RESOURCE CENTER

Setting up administrative accounts with lesser privileges

Get the full interactive view at
https://bitwarden.com/resources/setting-up-administrative-accounts-with-lesser-privileges/

bitwarden

Setting up administrative accounts with lesser privileges

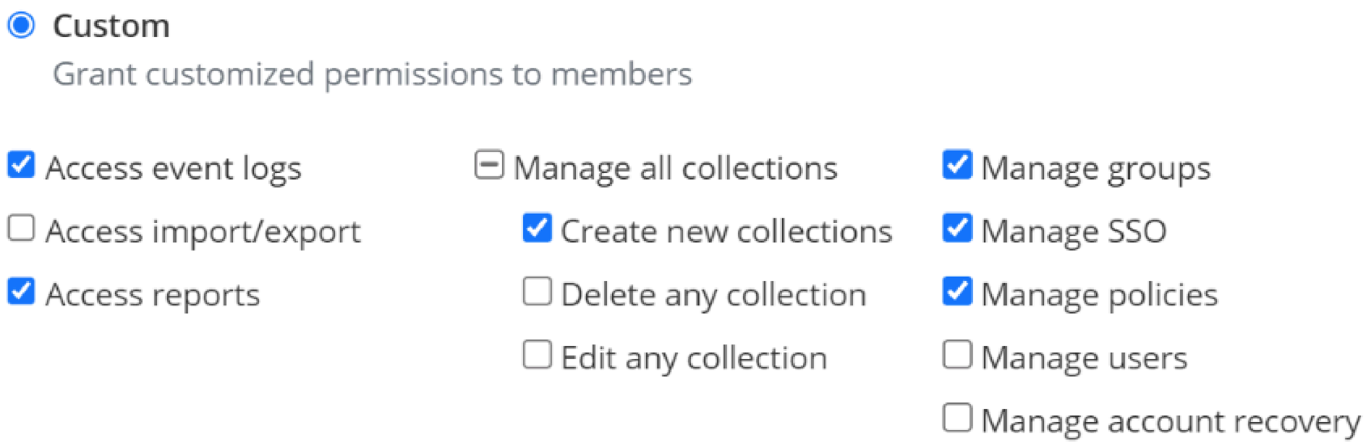
Bitwarden member roles include four pre-defined permissions sets including a configurable Custom member role (Enterprise only). Owners and Admins have full administrative access by default to prevent lockout and allow for user account administration.

To limit the day-to-day access a user has to the entire Organization, Owner account(s) can be set up with service account email addresses - these are not accessed regularly, but only to perform tasks that require access to all vault data at once - and Admin account(s) can be downgraded to the Custom member role with a specific permissions set.

This guide assumes that you have already determined a storage and approval mechanism for the Owner account(s). It is recommended to remain logged into an Owner account while modifying the Admin account(s) to Custom role(s).

Defining your custom member role

The below Custom member role will replace your users' Admin member role:



● Custom

Grant customized permissions to members

☑ Access event logs
☐ Access import/export
☑ Access reports

⊟ Manage all collections
- ☑ Create new collections
- ☐ Delete any collection
- ☐ Edit any collection

☑ Manage groups
☑ Manage SSO
☑ Manage policies
☐ Manage users
☐ Manage account recovery

Custom roles screenshot

Check any of the following boxes:

- Access event logs
- Access reports
- Create new collections
- Manage groups
- Manage SSO
- Manage policies

Note that none of the options above provide access to additional vault items.

Using the Owner member role as a service account

Now that the Admin users have been downgraded, several tasks can only be accomplished via the Owner account(s) due to the cryptographic or API permissions these tasks require. These tasks are:

- Import/Export of the organization vault
- Editing/Deleting unassigned collections
- Account recovery
- Manual user onboarding/offboarding
- Accessing the organization API key

Department Head/Manager permissions

Once you have changed your Admin users to this Custom member role, you will need to designate people to manage access to each collection. There are two ways to configure this, depending on how much access you want to give to the "department head".

Can manage Collection permission

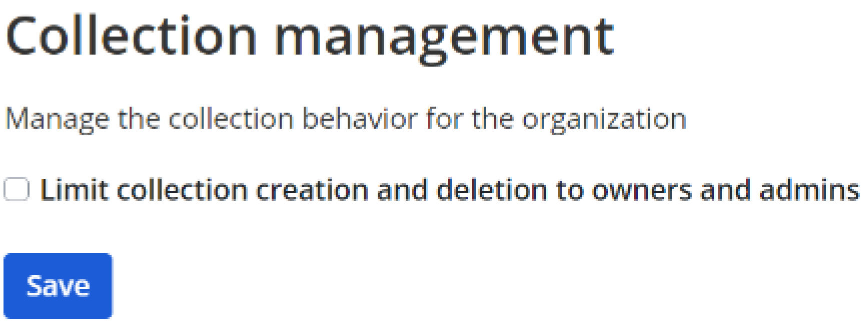
Grant the department heads the can manage permission for any collection you would like them to manage.

Allowing Department Heads to create new collections

If your "department head" needs to be able to create new collections in addition to managing their currently assigned collections, you will have two options.

Allow all users to create collections

Within the Admin Console, navigate to **Settings > Organization info**. From there, you will be able to decide whether you want Collection creation and deletion restricted to owners and admins. If you would like all users to be able to create collections, uncheck this box and save.



Collection management

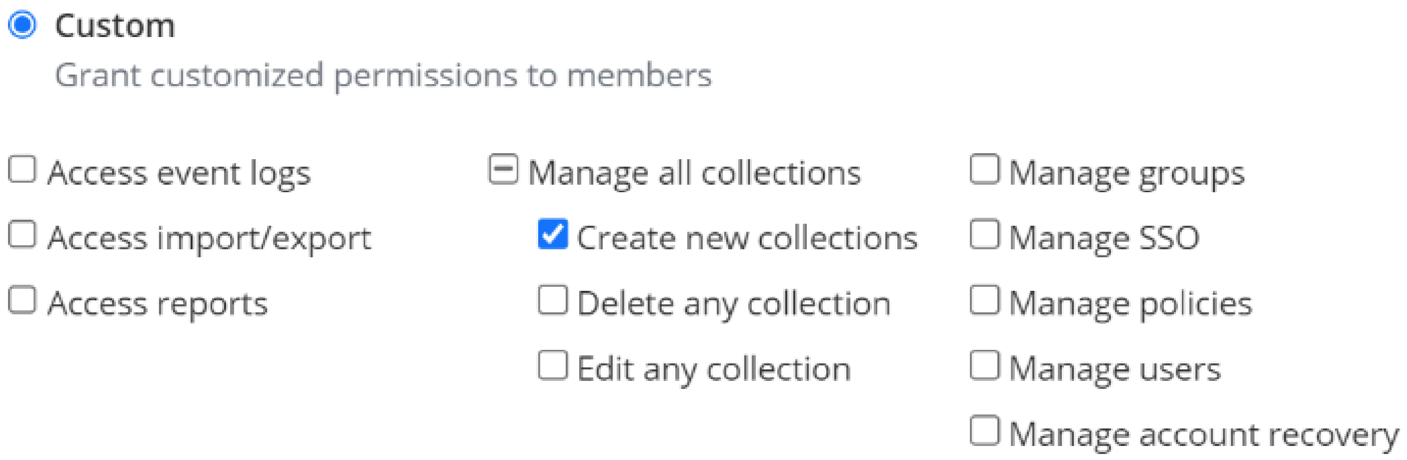
Manage the collection behavior for the organization

□ Limit collection creation and deletion to owners and admins

Organization Settings - Limiting Collection Management to Owners and Admins

Restrict collection creation to designated members

To allow department heads to create new collections when the Collection management option is checked, you will need to additionally grant those members the following Custom role:



● Custom
Grant customized permissions to members

□ Access event logs
□ Access import/export
□ Access reports

⊟ Manage all collections
- ☑ Create new collections
- □ Delete any collection
- □ Edit any collection

□ Manage groups
□ Manage SSO
□ Manage policies
□ Manage users
□ Manage account recovery

Custom Role - Create New Collections Selected

These members will still need to be granted the Can manage permission for any existing collections, but will immediately be granted Can manage for any new collection they create.

Additional Resources

Learning Center Modules

- Video Series: Getting started as an administrator
- Scaling Members, Groups, and Collections

Help Articles

- Member Roles and Permissions