bitwarden | Help Center Article

SECRETS MANAGER > GET STARTED

Manage your Organization

View in the help center:
https://bitwarden.com/help/manage-your-secrets-org/

Manage your Organization

> **Note**
> For a complete Bitwarden onboarding overview, please review this guide for more information.

As an organization using Secrets Manager, you'll share many of the tools originally used by Password Manager. This article covers these common areas and links to share documentation where appropriate.

> **Note**
> If you're brand new to Bitwarden organizations, we recommend checking out our article on getting started as an organization administrator.

Enterprise policies

Policies allow Enterprise organizations to enforce security rules for their members, for example mandating use of two-step login. While some policies apply primarily to Password Manager, there are a handful of policies that are broadly applicable to users of Secrets Manager:

- Require two-step login
- Master password requirements
- Master password reset
- Single organization
- Require single sign-on authentication
- Vault timeout

> **Tip**
> If you're new to Bitwarden, we recommend setting policies before onboarding your users.

User management

User management for Secrets Manager organizations is similar to organizations using Password Manager, however some Secrets Manager-specific elements include granting organization members access to Secrets Manager, member role differences, and specifying user seats and machine accounts.

Onboarding

There are a few different methods of onboarding users to your Bitwarden organization. Some of the commonly used methods are highlighted here:

Manual

The Bitwarden web vault provides a simple and intuitive interface for inviting new users to join your organization. This method is best for small organizations or those that aren't using directory services like Azure AD or Okta. Learn how to get started.

SCIM

Bitwarden servers provide a SCIM endpoint that, with a valid SCIM API Key, will accept requests from your identity provider for user and group provisioning and de-provisioning. This method is best for larger organizations using a SCIM-enabled directory service or IdP. Learn how to get started.

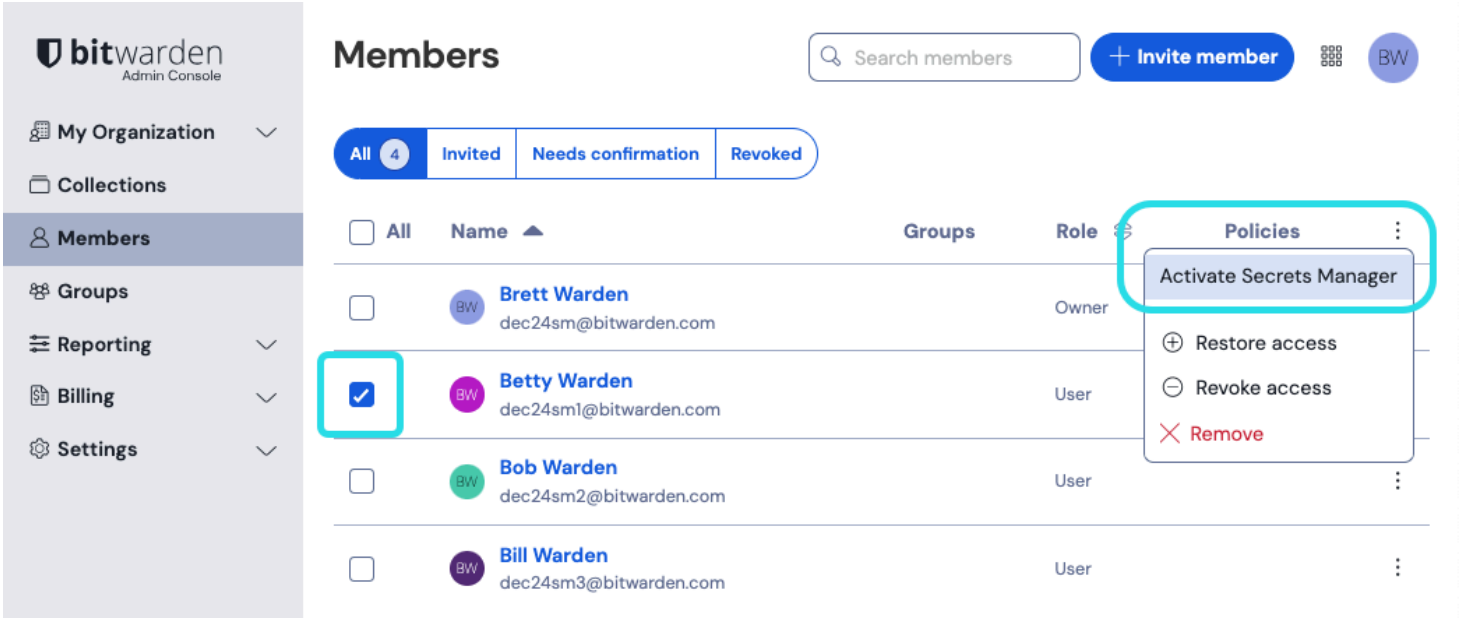
Directory Connector

Directory Connector automatically provisions users and groups in your Bitwarden organization by pulling from a selection of source directory services. This method is best for larger organizations using directory services that don't support SCIM. Learn how to get started.

Access to Secrets Manager

Once onboarded, give individual members of your organization access to Secrets Manager:

1. Open your organization's **Members** view and select the members your want to give access to Secrets Manager.
2. Using the ⋮ menu, select **Activate Secrets Manager** to grant access to selected members:
   - For organizations self-hosting, this step must be repeated in the self-hosted instance as well.



Add Secrets Manager users

> **Tip**
>
> Giving members access to Secrets Manager won't automatically give them access to stored projects or secrets. You'll need to assign people or groups access to the projects next.

Member roles

The following table outlines what each member role can do within Secrets Manager. During the beta, users have the same member role for Secrets Manager that they're assigned for Password Manager:

Member role	Description
User	Users can create their own secrets, projects, machine accounts, and access tokens. They can edit these objects once created. Users must be assigned to projects or machine accounts in order to interact with existing objects, and can be given **Can read** or **Can read, write** access.
Admin	Admins automatically have **Can read, write** access to all secrets, projects, machine accounts, and access tokens. Admins can assign themselves access to Secrets Manager and assign other members access to Secrets Manager.
Owner	Owners automatically have **Can read, write** access to all secrets, projects, machine accounts, and access tokens. Owners can assign themselves access to Secrets Manager and assign other members access to Secrets Manager.

> **Note**
> Custom roles are not currently scoped with options for Secrets Manager, however can still be used to assign specific Password Manager or broader organization capabilities.

Groups

Groups relate together individual members and provide a scaleable way to access access to and permissions for specific projects. When adding new members, add them to a group to have them automatically inherit that group's configured permissions. Learn more.

Once groups are created in the admin console, assign them to projects from the Secrets Manager web app.

Single sign-on

Login with SSO is the Bitwarden solution for single sign-on. Using login with SSO, Enterprise organizations can leverage their existing Identity Provider to authenticate users with Bitwarden using the SAML 2.0 or Open ID Connect (OIDC) protocols. Learn how to get started.

Account recovery administration

Account recovery allows designated administrators to recover enterprise organization user accounts and restore access in the event that an employee forgets their master password. Account recovery can be activated for an organization by enabling the Account recovery administration policy. Learn how to get started.

Event logs

Event logs are timestamped records of events that occur within your Teams or Enterprise organization. Secrets Manager events are available both from the **Reporting** → **Event logs** of your organization vault and from the machine account Event logs page.

Event logs are exportable and are retained indefinitely. While many events are applicable to all Bitwarden products and some are specific to Password Manager, Secrets Manager will specifically log the following:

- Secret accessed by a machine account

Self-hosting

Enterprise organizations can self-host Bitwarden Secrets Manager using Docker on Linux and Windows machines. If you haven't self-hosted Bitwarden before, use this guide to set yourself on the right track.

If you are already self-hosting an Enterprise Bitwarden organization and want to get access to Secrets Manager on that server:

1. Sign up for a Secrets Manager subscription in your cloud-hosted Bitwarden organization.
2. Update your self-hosted server to, at a minimum, 2023.10.0
3. Retrieve a new license file from your cloud-hosted organization and upload it to your self-hosted server.
4. Give individual users access to Secrets Manager in the self-hosted instance.

> **Note**
>
> Self-hosting Secrets Manager is not supported for the Bitwarden unified self-hosted deployment option. Enterprise organizations should use a standard Linux or Windows installation.