SECRETS MANAGER > YOUR SECRETS

Secrets

Secrets

Secrets are sensitive key-value pairs that your organization needs securely stored and should never be exposed in plain code or transmitted over unencrypted channels, for example:

- API Keys

- Application Configurations

- Database Connection Strings

- Environment Variables

Secrets that your user account has access [through assigned projects](#) are listed in the primary Secrets Manager view as well as by selecting **Secrets** from the navigation:

Secrets

Create a secret

To create a new secret:

1. Use the **New** dropdown to select **Secret**:
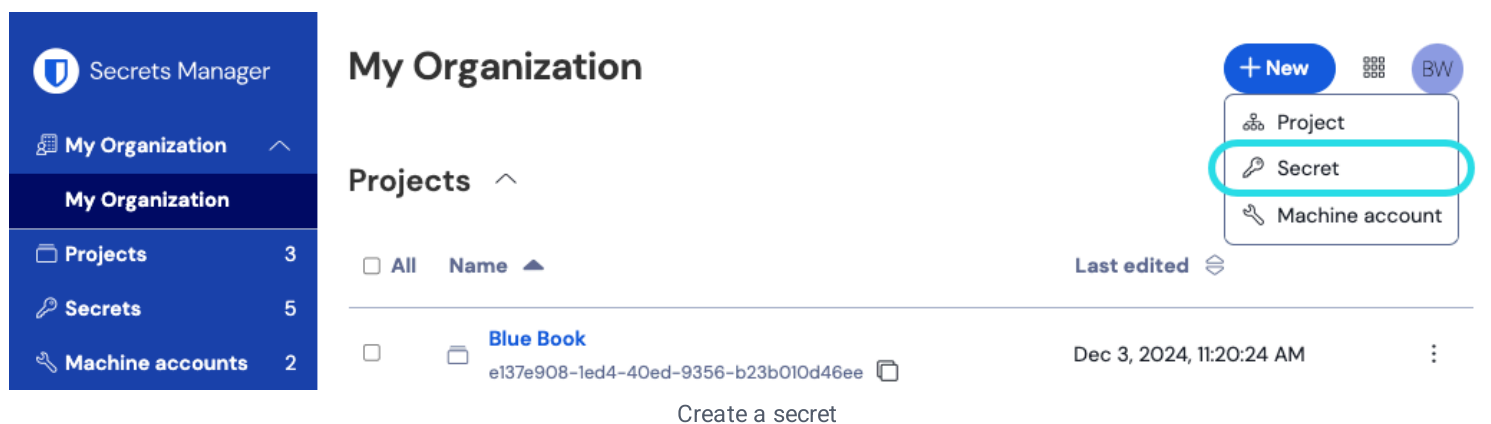
Create a secret

2. On the New Secret window's top-most section, enter a **Name** and **Value**. Adding **Notes** is optional.

3. Within **Project**, pick an existing project to associate with the secret or create a new project to that will include the secret. Each secret can only be associated with a single project at a time.

4. Optionally, use the **People** and **Machine accounts** tabs to grant people or machine accounts direct access to the secret.

5. When you're finished, select the **Save** button.

Add secrets to a project

Secrets may only be assigned to one project at a time. By adding a secret to a project:

- Organization members with access to the project will be able to see or manipulate this secret.

- Machine accounts with access to the project will be able to create a pathway for injecting and editing this secret.

To add your secrets to a project:

1. Go to **Secrets** and select the secret to add.

2. In the Edit Secret window, in the **Project** section, type or select the project to associate the secret with. Each secret can only be associated with a single project at a time.

3. When you're finished, select the **Save** button.

Assign secrets to people or machine accounts

From the same window, you can grant secret access directly to people and machine accounts:

- Granting secret access directly to users will allow them to interact with it from the **Secrets** view.

- Granting secret access directly to machine accounts will grant programmatic access to the secret using the machine account's access token(s).

Delete a secret

When you delete a secret, it moves to **Trash** for 30 days. After that time, it will be permanently deleted.

> ⚠ **Warning**
>
> Once a secret is permanently deleted, it cannot be recovered.

To delete a secret:

1. Go to **Secrets**.

2. On the same line as the secret, select the ⋮ **icon**.

3. Select **Delete secret**:

Delete secret

To undo a deletion or permanently delete a secret before 30 days:

1. Go to **Trash**.

2. On the same line as the secret, select the ⋮ **icon**.

3. Select **Restore secret** or **Permanently delete**:

Permanently delete secret

4. Select **Delete secret** to confirm.