

SECRETS MANAGER > GET STARTED

Secrets Manager Quick Start

View in the help center:

<https://bitwarden.com/help/secrets-manager-quick-start/>

Secrets Manager Quick Start

Tip

If you're a developer, you may prefer [Developer Quick Start](#). The article you're currently on will cover Secrets Manager from an administrative and setup point of view.

Bitwarden Secrets Manager enables developers, DevOps, and cybersecurity teams to centrally store, manage, and deploy secrets at scale. Use the **Secrets Manager web app** to add and organize [secrets](#), create [systems of permissions](#) to fit your needs, and [generate access tokens](#) for your applications.

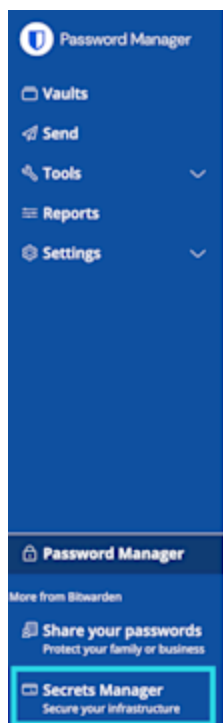
Once Secrets Manager is set up, learn how to inject secrets into your machines and applications with the [Developer Quick Start](#) guide.

Access Secrets Manager

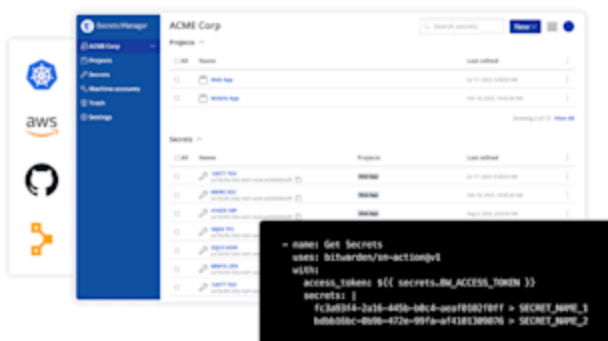
Log in to the Bitwarden web app and select **Secrets Manager** from the product switcher in the navigation menu:



If you or your organization are not active Secrets Manager users yet, click **Try it now**:



More products from Bitwarden



Bitwarden Secrets Manager

Development, DevOps, and IT teams choose Bitwarden Secrets Manager to securely manage and deploy their infrastructure and machine secrets.

- **Centralize secrets management.** Securely store and manage secrets in one location to prevent secret sprawl across your organization.
- **Prevent secret leaks.** Protect secrets with end-to-end encryption. No more hard coding secrets or sharing through .env files.
- **Enhance developer productivity.** Programmatically retrieve and deploy secrets at runtime so developers can focus on what matters most, like improving code quality.
- **Strengthen business security.** Maintain tight control over machine and human access to secrets with SSO integrations, event logs, and access rotation.

[Try it now](#)

[Learn more](#)

Secrets Manager Homepage

- **Owners** are taken to their organization's **Subscription** page for Secrets Manager.
- **Users** are asked if they want to send their organization owner an email requesting Bitwarden Secrets Manager access. They can edit the email before sending.



Request access to Secrets Manager

You need approval from your administrator to try Secrets Manager.

Add a note (required)

Hi,

I am requesting a subscription to Bitwarden Secrets Manager for our team. Your support would mean a great deal!

Bitwarden Secrets Manager is an end-to-end encrypted secrets management solution for securely storing, sharing, and deploying machine credentials like API keys, database passwords, and authentication certificates.

Secrets Manager will help us to:

- Improve security
- Streamline operations
- Prevent costly secret leaks

To request a free trial for our team, please reach out to Bitwarden.

Thank you for your help!

Organization (required)

My_Organization

Send request

Cancel

Request access to Secrets Manager

Set up Secrets Manager

Add Secrets Manager to your organization

Only owners can add Secrets Manager to their organization. To start using Secrets Manager:

1. In Admin Console for your organization, go to **Billing** → **Subscription**.
2. In the **More from Bitwarden** section, check **Subscribe to Secrets Manager**:

More from Bitwarden

 **Secrets Manager**

Secrets Manager for Enterprise
For engineering and DevOps teams to manage secrets throughout the software development lifecycle.

- Unlimited secrets
- Unlimited projects
- 50 machine accounts included
- \$1.00 per month for additional machine accounts

\$12.00 per user /month

☐ **Subscribe to Secrets Manager**

[Add Secrets Manager](#)

3. Depending on your organization's plan:

- If you are on the Free plan, select **Submit**.
- If you are on an upgraded plan, enter the desired number of **Subscription seats** (up to your Password Manager subscription's total) and **Additional machine accounts** beyond your plan's included amount (20 for Teams and 50 for Enterprise). Select **Save**.

Note

Secrets Manager will automatically scale your user seats and machine accounts when new users or machine accounts are added. At any time, you can go to **Billing** → **Subscription** to change the total allowed user seats and machine accounts. To set a scaling limit, select **Limit subscription** and **Limit machine accounts**:

Secrets Manager

Subscription seats (required)

2

Total:

**Limit subscription (optional)**

Set a seat limit for your Secrets Manager subscription. Once this limit is reached, you will not be able to invite new members.

Additional machine accounts (required)

30

Your plan comes with 50 machine accounts. You can add additional machine accounts for per month.

Total:

**Limit machine accounts (optional)**

Set a limit for your machine accounts. Once this limit is reached, you will not be able to create new machine accounts.

Save

Limit subscription seats and machine accounts

Once activated, you can open Secrets Manager from the product switcher:

Product switcher

 Tip

Before proceeding, we recommend [creating groups](#) for Secrets Manager users. Groups let you to quickly assign access to secrets once users have Secrets Manager access.

Organization owners and admins can grant access to Secrets Manager. To give members access:

1. In Admin Console for your organization, go to **Members**.
2. Select which users you want to add to the Secrets Manager.
3. Click the  icon and select **Activate Secrets Manager**:

bitwarden
Admin Console

My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Members

Search members

Invite member

All 4

Invited

Needs confirmation

Revoked

☐	All	Name	Groups	Role	Policies
☐		Brett Warden dec24sm@bitwarden.com		Owner	
☒		Betty Warden dec24sm1@bitwarden.com		User	Activate Secrets Manager Restore access Revoke access Remove
☐		Bob Warden dec24sm2@bitwarden.com		User	
☐		Bill Warden dec24sm3@bitwarden.com		User	

Add Secrets Manager users

Alternatively, go to **Members** → **Member role** and select **This user can access Secrets Manager**:

Edit member

Role

Groups

Collections

Member role

☒ User

Access and add items to assigned collections

☐ Admin

Manage organization access, all collections, members, reporting, and security settings

☐ Owner

Manage all aspects of your organization, including billing and subscriptions

☐ Custom

Grant customized permissions to members

Secrets Manager

Activate user access to Secrets Manager.

☐ This user can access Secrets Manager

Save

Cancel

Revoke

Remove

Edit member role to grant Secrets Manager access

Note

Once Secrets Manager access is granted to a user (or yourself), you may need to refresh your browser for Secrets Manager to appear.

First steps

Your secrets vault

Use the product switcher to open the Secrets Manager web app. If this is your first time opening the app you'll have an empty vault, but eventually it'll be full of your projects and secrets:

Secrets Manager

My Organization

My Organization

Projects3

Secrets5

Machine accounts2

Integrations

Trash

Settings

Password Manager

Secrets Manager

Admin Console

My Organization

+ New

BW

Projects

☐ All	Name	Last edited	
☐	Blue Book e137e908-1ed4-40ed-9356-b23b010d46ee	Dec 3, 2024, 11:20:24 AM	
☐	Orion f8b02375-aa51-42cb-bfbf-b23b010d5168	Dec 3, 2024, 11:20:33 AM	
☐	Stargate bde574f7-bf02-410c-8463-b23b010d5832	Dec 3, 2024, 11:20:39 AM	

Showing 3 of 3 [View all](#)

Secrets

☐ All	Name	Project	Last edited	
☐	DB Connection String 3c5c82ef-952a-4ce9-8ea6-b23b010d9725	Blue Book	Dec 3, 2024, 11:22:30 AM	
☐	Imported Secret a723853a-c041-4f2a-aa19-b23b010dbf84	Unassigned	Dec 3, 2024, 11:22:07 AM	
☐	PKI Certificate c7c93bc1-470c-4643-96fb-b23b010dd248	Blue Book	Dec 3, 2024, 11:22:23 AM	
☐	Port Variable 76e6d9f0-f2f5-47e3-a032-b23b010df11a	Orion	Dec 3, 2024, 11:22:49 AM	
☐	SSH Key 16cdb8d-1112-48d7-9b0a-b23b010e02f3	Stargate	Dec 3, 2024, 11:23:04 AM	

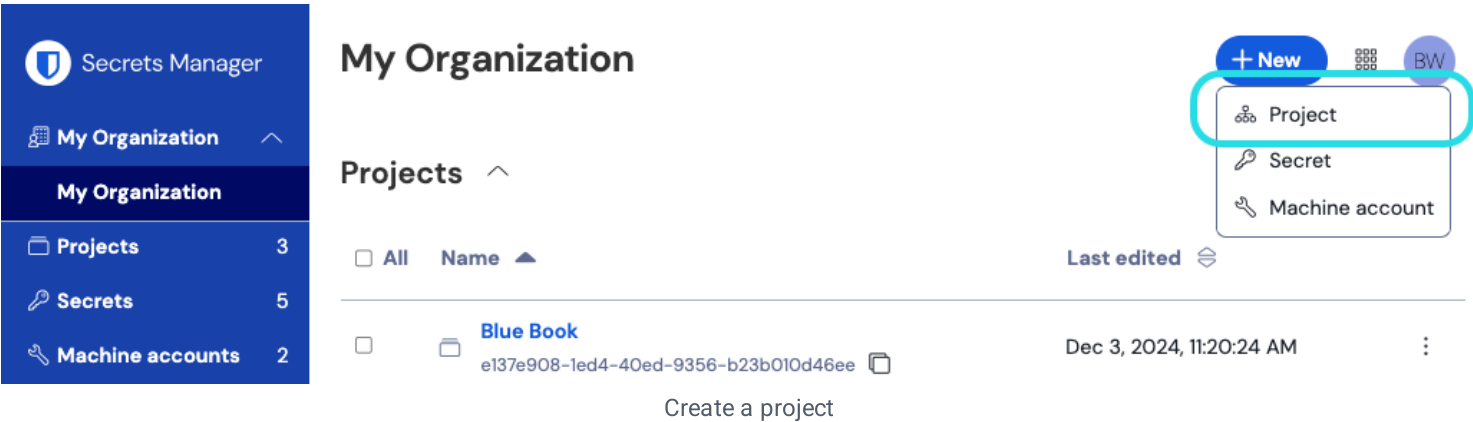
Secrets vault

Let's start filling your vault.

Add a project

Projects are collections of secrets logically grouped together for management access by your DevOps, cybersecurity, or other internal teams. It's important to take into account, when creating your projects, that projects will be **the primary structures through which you assign members access to secrets**. To create a project:

1. Use the **New** dropdown to select **Project**:

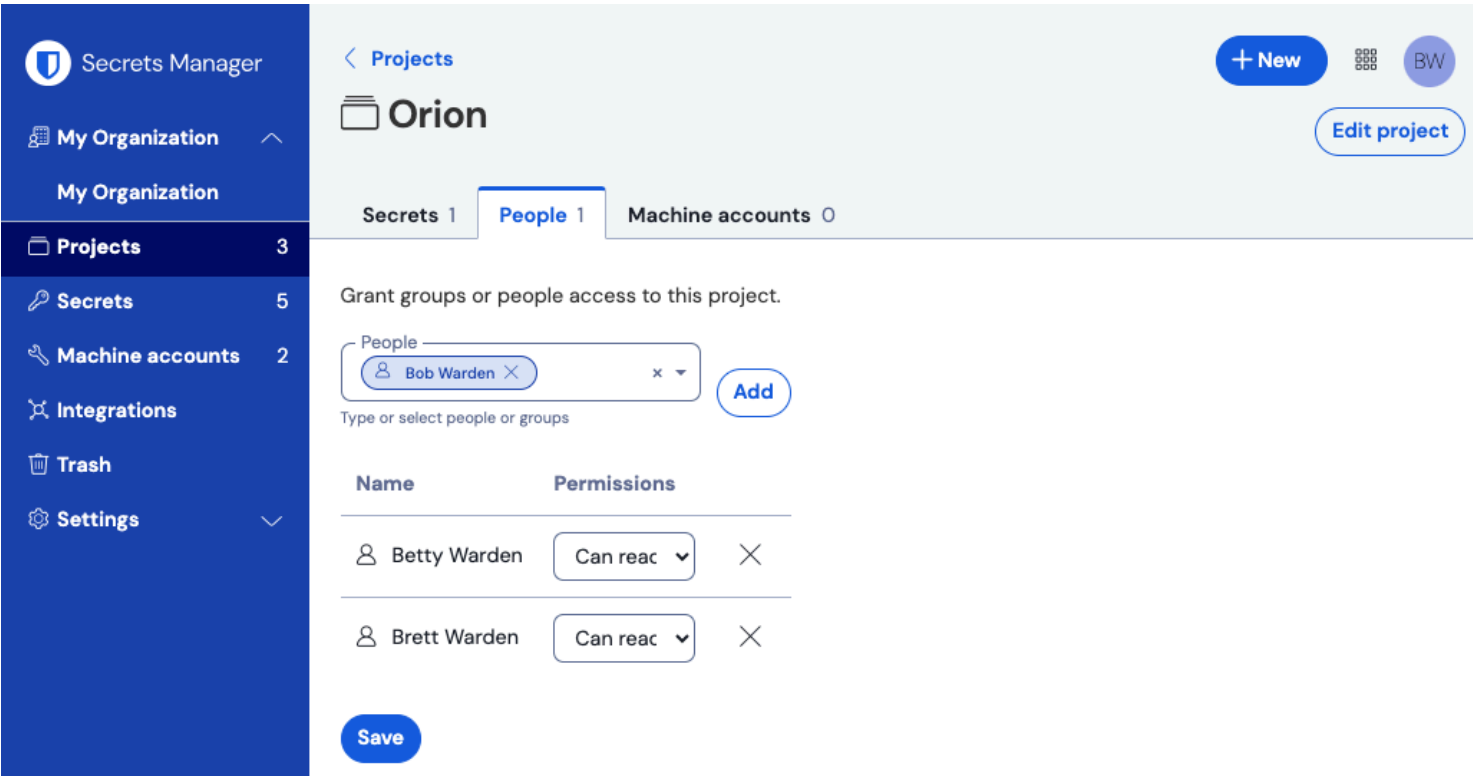


- 2. Enter a **Project name**.
- 3. Select the **Save** button.

Assign members to your project

Adding organization members to your project will allow those users to interact with the project's secrets. To add people to your project:

- 1. In the new project, select the **People** tab.
- 2. From the People dropdown, type or select the member(s) or group(s) to add to the project. Once you've selected the right people, use the **Add** button:



Add people to a project

3. Once members or groups are added to the project, set a level of **Permissions** for those members or groups. Members and groups can have one of the following levels of permission:

- **Can read:** Members/groups will be able to view existing secrets in this project.
- **Can read, write:** Members/groups will be able to view existing secrets and create new secrets in this project.

Add secrets

Now that you have a project with a handful of members who can help you manage it, let's add some **secrets** to the project. Secrets are sensitive key-value pairs stored in your vault, typically things that should never be exposed in plain code or transmitted over unencrypted channels, for example:

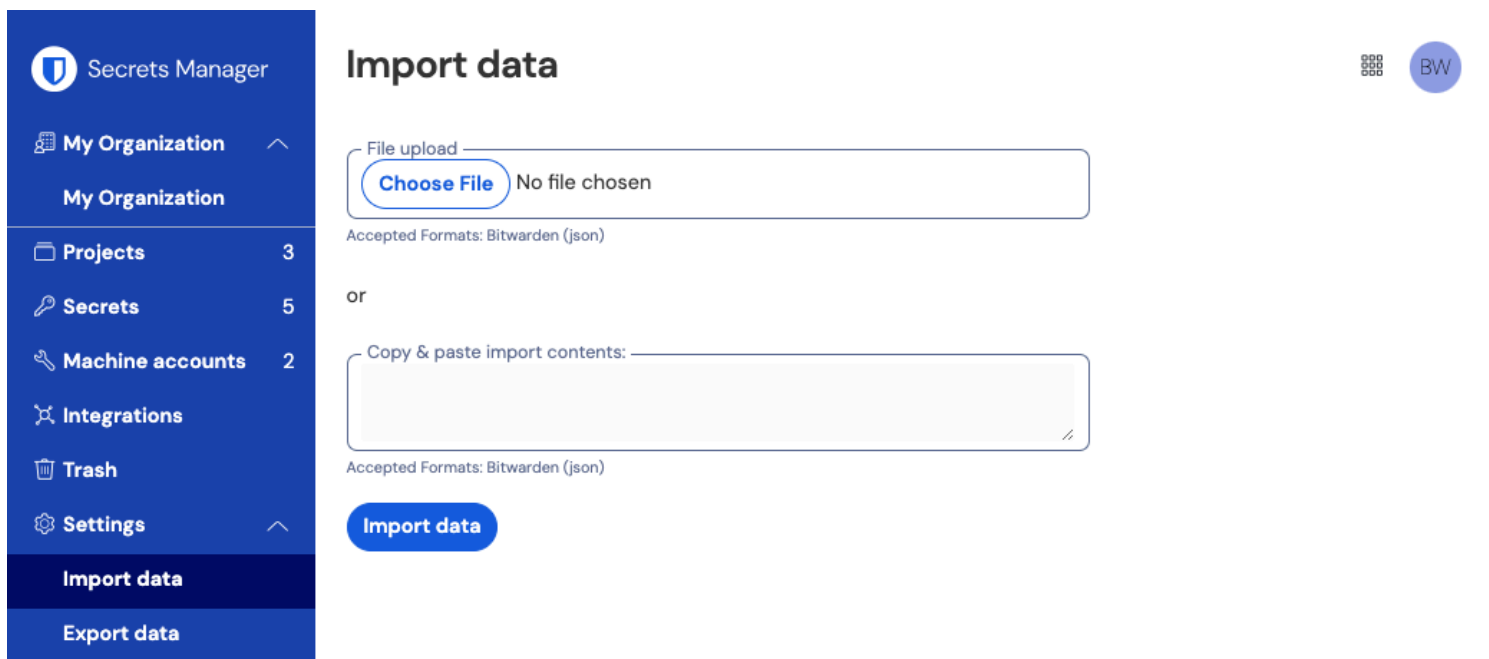
- API Keys
- Application Configurations
- Database Connection Strings
- Environment Variables

You can import secrets directly to your vault as a `.json` file or add secrets manually:

⇒Import secrets

To import your secrets:

1. Review [this document](#) for help properly formatting an import file.
2. Select **Settings** → **Import data** from the left-hand navigation:



The screenshot shows the Bitwarden web interface. On the left is a dark blue sidebar with the 'Secrets Manager' header and a list of navigation items: 'My Organization', 'Projects' (3), 'Secrets' (5), 'Machine accounts' (2), 'Integrations', 'Trash', 'Settings', 'Import data' (highlighted), and 'Export data'. The main content area is titled 'Import data' and features two methods for importing secrets. The first method, 'File upload', includes a 'Choose File' button and indicates that accepted formats are Bitwarden (json). The second method, 'Copy & paste import contents:', includes a large text area for pasting content and also lists accepted formats as Bitwarden (json). A blue 'Import data' button is positioned at the bottom of the main content area. In the top right corner of the interface, there is a QR code icon and a circular profile icon labeled 'BW'.

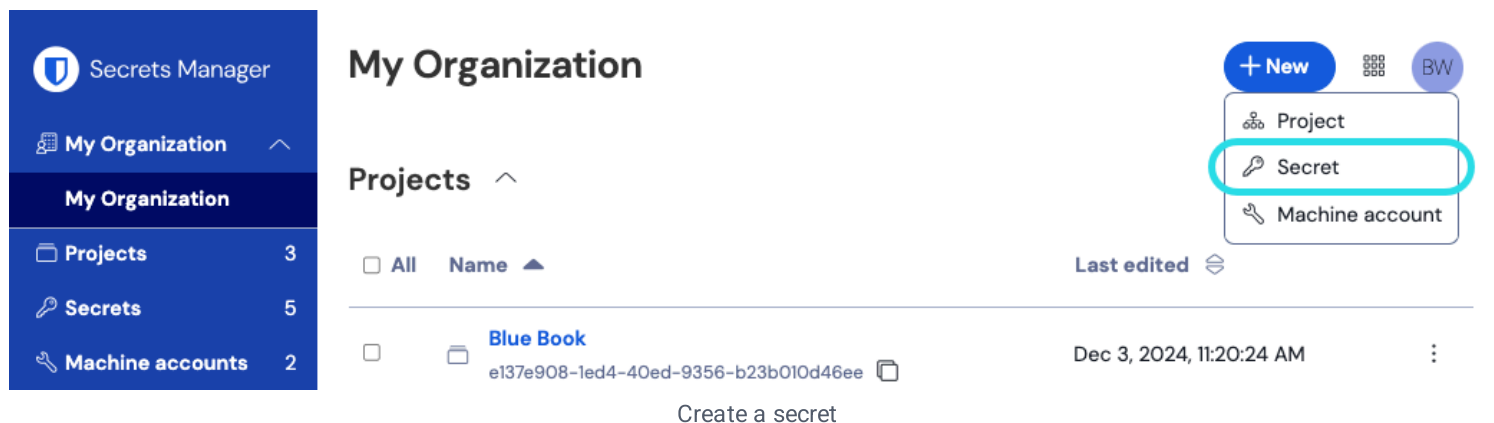
Import data

3. Select **Choose File** and choose a `.json` file for import.

⇒Add secrets manually

To add secrets manually:

1. Use the **New** dropdown to select **Secret**:



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

3. In the Project section, type or select the project to associate the secret with. A few key points:

- Each secret can only be associated with a single project at a time.
- Only organization members with access to the project will be able to see or manipulate this secret.
- Only machine accounts with access to the project will be able to create a pathway for injecting this secret ([more on that soon](#)).

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

Repeat this process for as many secrets as you want to add to your vault.

Add a machine account

Now that you've got a project full of secrets, it's time to start constructing machine access to those secrets. **Machine accounts** represent non-human machine users, or groups of machine users, that require programmatic access to some of the secrets stored in your vault. Machine accounts are used to:

- Appropriately scope the selection of secrets a machine user has access to.
- Issue access tokens to facilitate programmatic access to, and the ability to decrypt, edit, and create secrets.

To add a machine account for this project:

1. Use the **New** dropdown to select **Machine account**:



2. Enter a **Machine account name** and select **Save**.

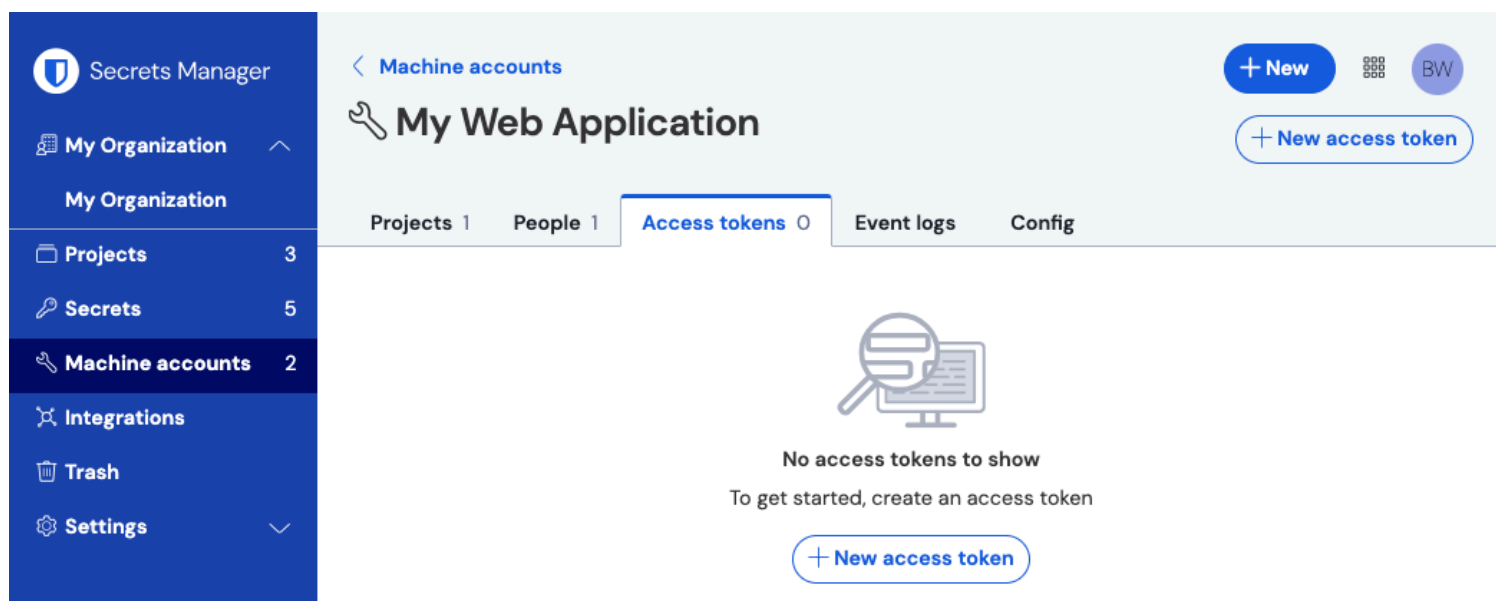
3. Open the machine account and, in the **Projects** tab, type or select the name of the project(s) that this machine account should be able to access. For each added project, select a level of **Permissions**:

- **Can read**: Machine account can retrieve secrets from assigned projects.
- **Can read, write**: Machine account can retrieve and edit secrets from assigned projects, as well as create new secrets in assigned projects or create new projects.

Create an access token

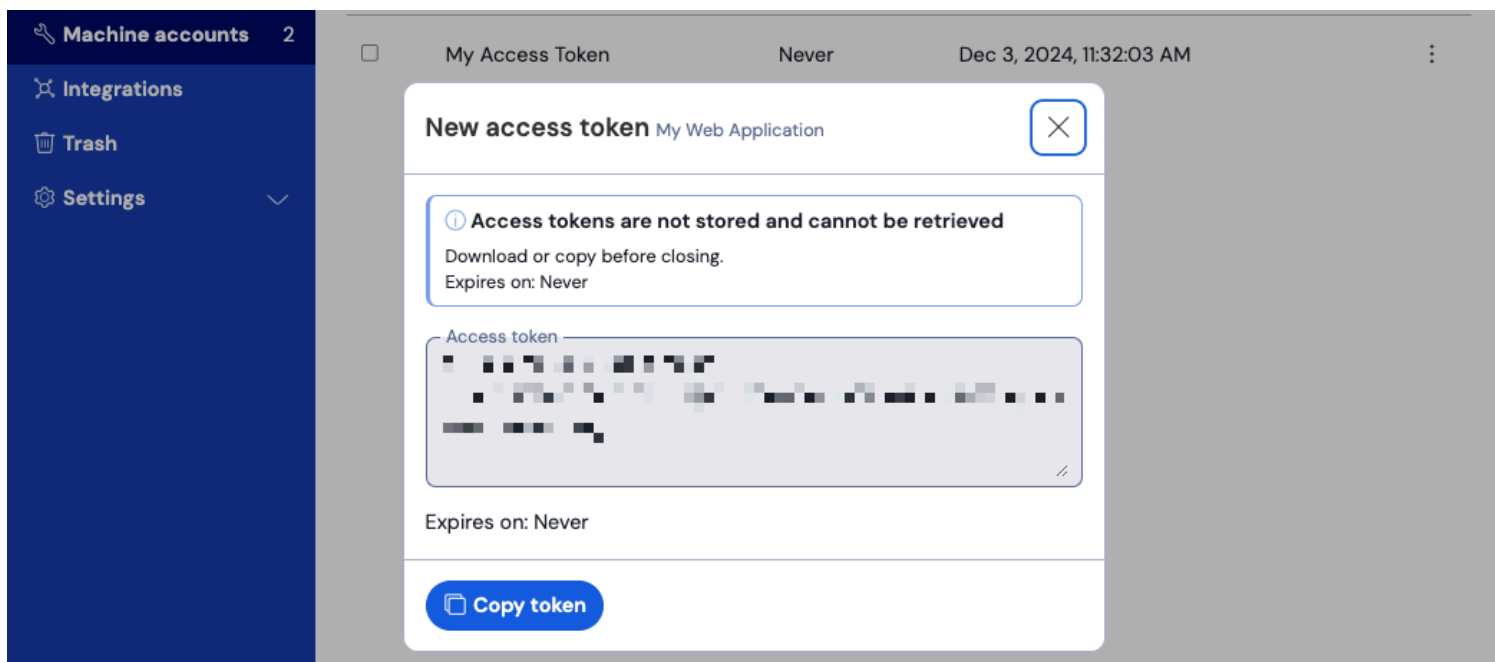
Access tokens facilitate programmatic access to, and the ability to decrypt and edit, secrets stored in your vault. Access tokens are issued to a particular machine account, and will give any machine that they're applied to the ability to access **only the secrets associated with that machine account**. To create an access token:

1. Select **Machine accounts** from the navigation.
2. Select the machine account to create an access token for, and open the **Access tokens** tab:



Create access token

3. Select the **Create access token** button.
4. On the Create Access Token panel, provide:
 - A **Name** for the token.
 - When the token **Expires**. By default, Never.
5. Select the **Create access token** button when you're finished configuring the token.
6. A window will appear printing your access token to the screen. Copy your token to somewhere safe before closing this window, as your token **cannot be retrieved later**:



Access token example

This access token is the authentication vehicle through which you'll be able to script secret injection to your machines and applications.

Next steps

Now that you've got the hang of creating the infrastructure for securely managing secrets, and of creating pathways for machine access to secrets, let's continue on to the [Developer Quick Start](#) guide.

Or, for more information about Secrets Manager:

- [Bitwarden brings open source security and zero knowledge encryption to secrets management](#)
- [Why does my development team need a secrets manager?](#)
- [Why end-to-end encryption is crucial for developer secrets management](#)