

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



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.

The **Secrets Manager web app** will be your home for setting up your secrets management infrastructure. You'll use it to add and organize [secrets](#), create [systems of permissions](#) to fit your needs, and [generate access tokens](#) for use by your applications. Once complete, you'll move on to the [Developer Quick Start](#) guide to learn how to inject secrets into your machines and applications.

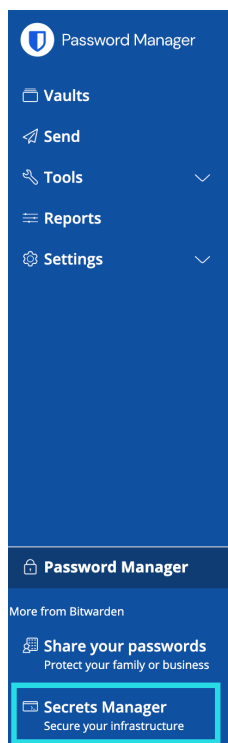
Getting to Secrets Manager

To navigate to Secrets Manager, select **Secrets Manager** from the product switcher located on the navigation menu:

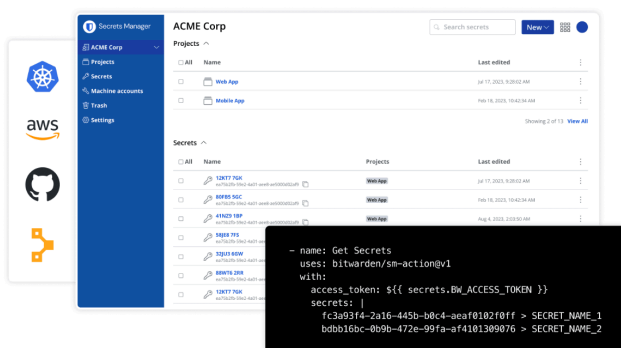


<https://player.vimeo.com/video/840459200>

If you or your organization are not active Secrets Manager users, the Secrets Manager page will provide information about the product. Owners and users can click **Try it now** to be redirected:



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** will be redirected to the Secrets Manager section of the organization's subscription page.
- **Users** will be redirected to a pre-generated email where the user may request Bitwarden Secrets Manager access. The email can be edited before being sent to the organization administrator.

 Password Manager

 Vaults

 Send

 Tools 

 Reports

 Settings 

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

Activating Secrets Manager

You must be an organization owner to enable Secrets Manager. To start using Secrets Manager:

1. In the Admin Console, navigate to your organization's **Billing → Subscription** page or click **Try it now** on the Secrets Manager screen.
2. In the **More from Bitwarden** section, select the **Subscribe to Secrets Manager** checkbox.

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](#)

Once activated, Secrets Manager will be available through the web app using the product switcher:

Product switcher

Before you take your first steps with Secrets Manager, you will need to explicitly invite a few organization members to join.


Give members access



Before proceeding, we recommend setting up one or more groups for users of Secrets Manager. You will need to give members access to Secrets Manager through the **Members** page, but you can use groups to scaleably assign access to secrets once your vault is populated.

To give members access to Secrets Manager you must be an organization owner or admin:

1. Open your organization's **Members** view and select the members you want to give access to Secrets Manager.
2. Using the **:** menu, select **Activate Secrets Manager** to grant access to selected members:



- My Organization
- Collections
- Members**
- Groups
- Reporting
- Billing
- Settings

Members

+ Invite member

All 4
Invited
Needs confirmation
Revoked

<input type="checkbox"/>	All	Name	Groups	Role	Policies
<input type="checkbox"/>		Brett Warden dec24sm@bitwarden.com		Owner	
<input checked="" type="checkbox"/>		Betty Warden dec24sm1@bitwarden.com		User	<div> <div>Activate Secrets Manager</div> <div> + Restore access - Revoke access </div> <div>✗ Remove</div> </div>
<input type="checkbox"/>		Bob Warden dec24sm2@bitwarden.com		User	
<input type="checkbox"/>		Bill Warden dec24sm3@bitwarden.com		User	

Add Secrets Manager users

Note

Once Secrets Manager access has been granted to a user (or yourself), you may need to refresh the vault in order for Secrets Manager to appear in the product switcher.

User seats and machine account scaling

From your organization's **Billing** → **Subscription** page you will be able to assign total allowed user seats and machine accounts for your Secrets Manager organization.

Secrets Manager

Subscription seats (required)

Total: $5 \times \$144.00 = \720.00 / year

☐ 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)

Your plan comes with 50 machine accounts. You can add additional machine accounts for \$1.00 per month.

Total: $0 \times \$12.00 = \0.00 / year

☐ 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

Secrets Manager User Management

Secrets Manager will automatically scale your user seats and machine accounts when new users or machine accounts are added. A limit can be set by selecting the **Limit subscription** and **Limit machine accounts** boxes.

Note

In the **User seats** field, the specified number must be lower than or equal to the number of seats specified for your Password Manager subscription.

You can also use the **Additional machine accounts field** to explicitly add machine accounts above your plans pre-packaged number; 20 for Teams and 50 for Enterprise.

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

<input type="checkbox"/>	<div>Blue Book</div> <div>e137e908-1ed4-40ed-9356-b23b010d46ee</div>	Dec 3, 2024, 11:20:24 AM	
<input type="checkbox"/>	<div>Orion</div> <div>f8b02375-aa51-42cb-bfbf-b23b010d5168</div>	Dec 3, 2024, 11:20:33 AM	
<input type="checkbox"/>	<div>Stargate</div> <div>bde574f7-bf02-410c-8463-b23b010d5832</div>	Dec 3, 2024, 11:20:39 AM	

Showing 3 of 3 [View all](#)

Secrets

All

Name

Project

Last edited

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

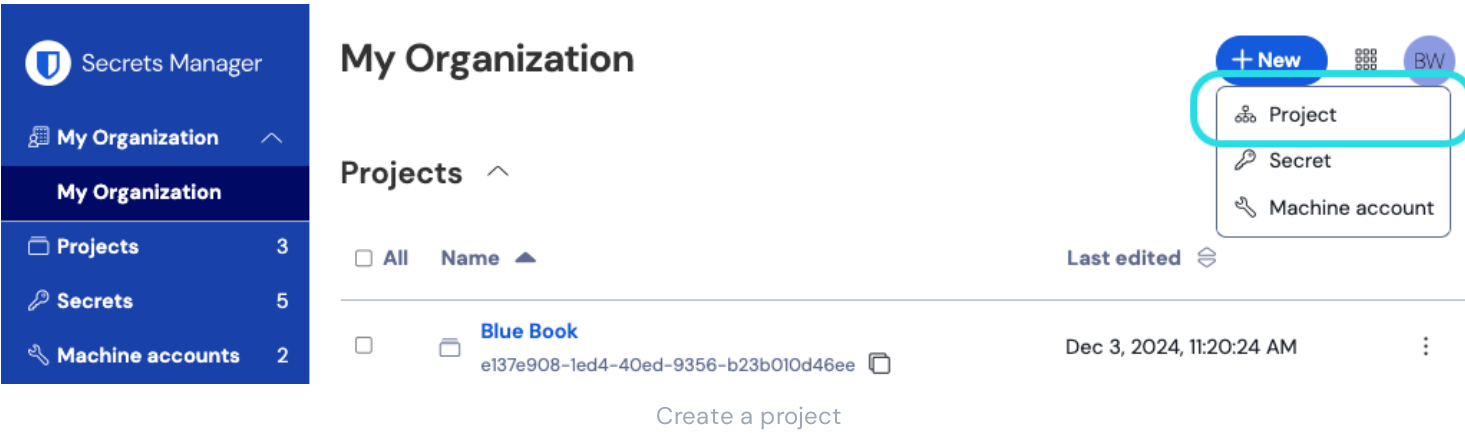
Secrets vault

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**:

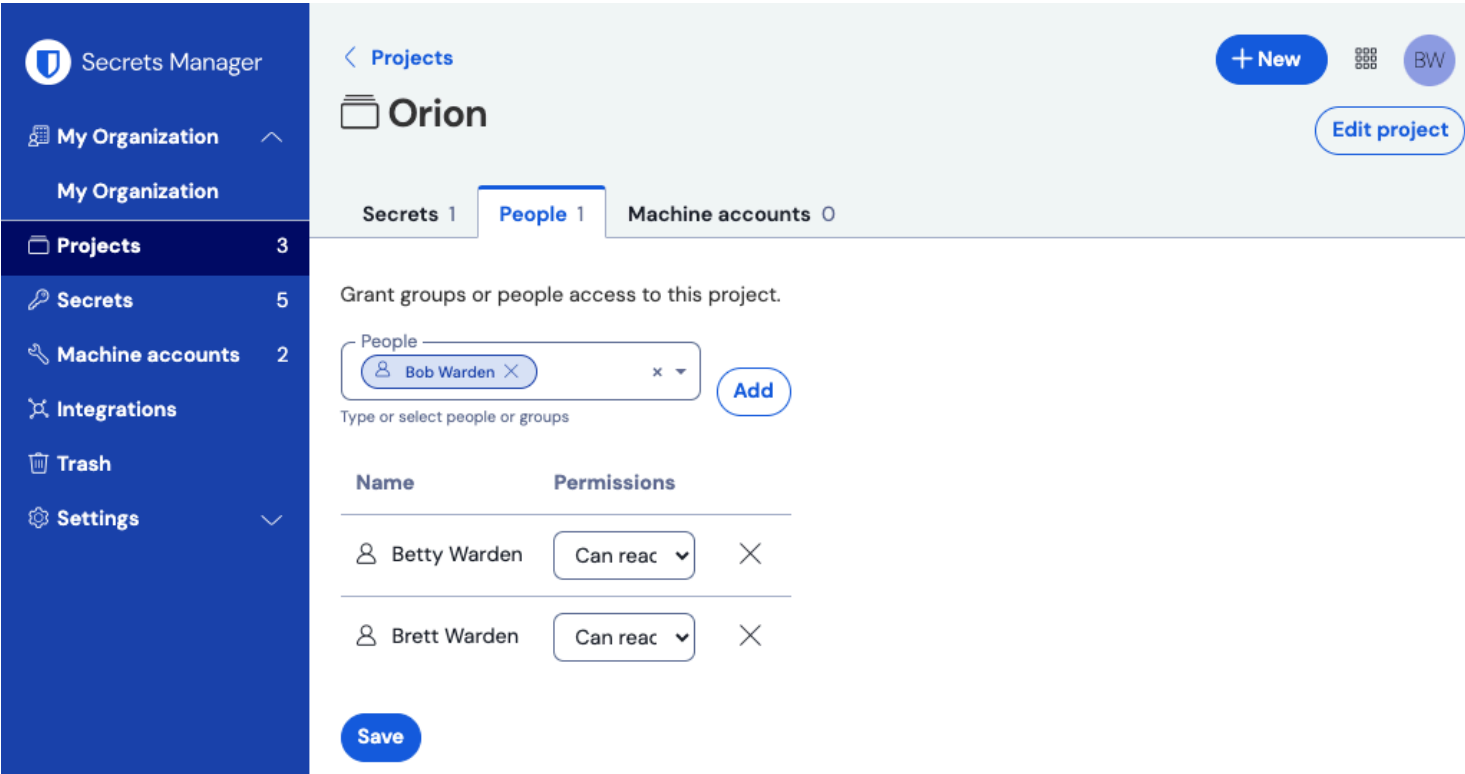


- 2. Enter a **Project name**.
- 3. Select the **Save** button.

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:

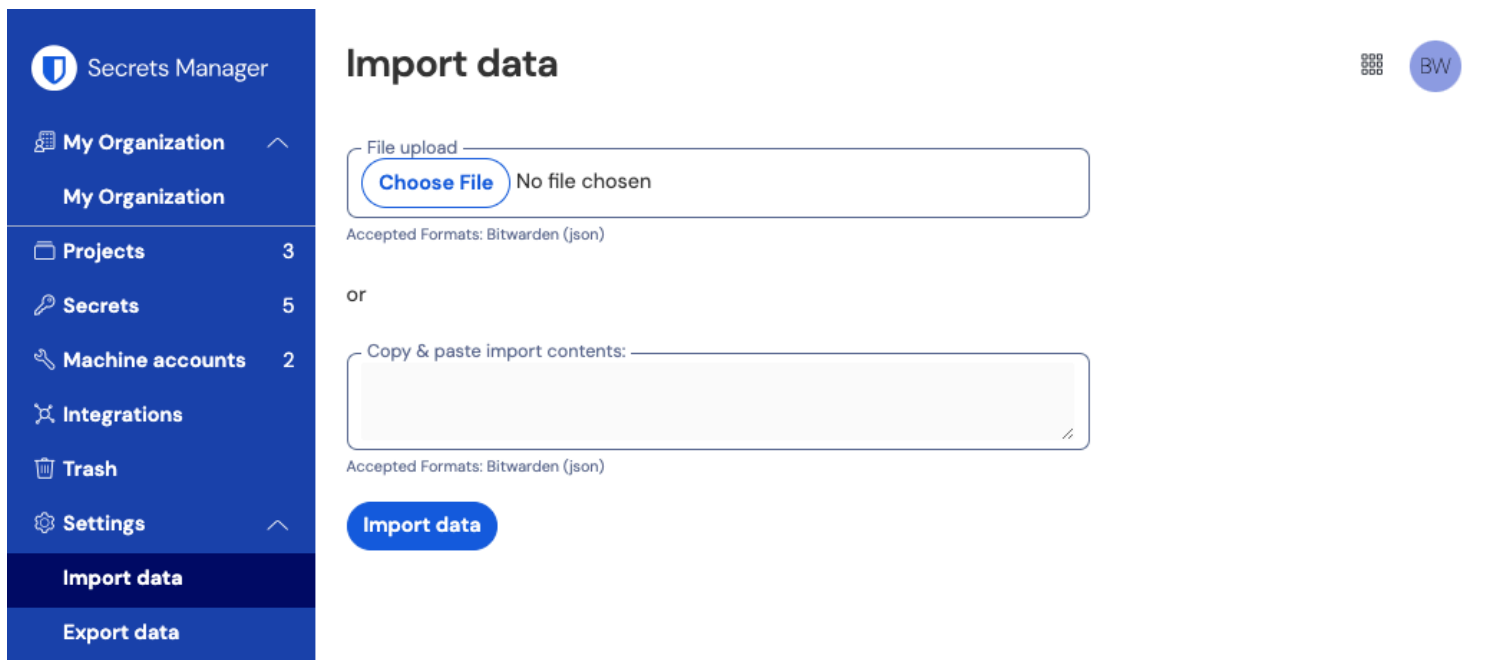
- API Keys
- Application Configurations
- Database Connection Strings
- Environment Variables

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:



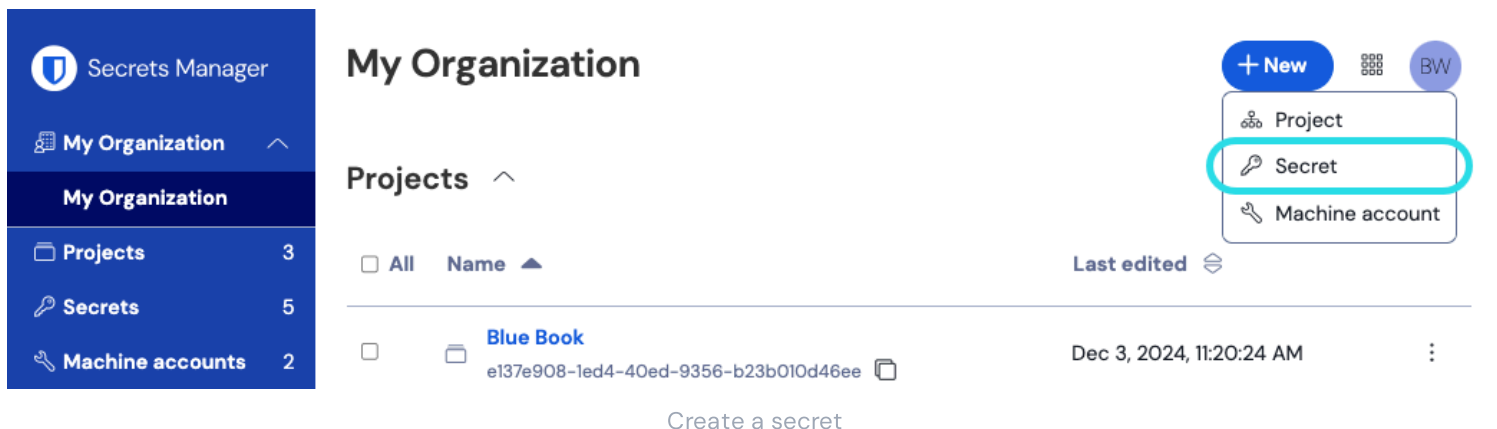
Import data

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.

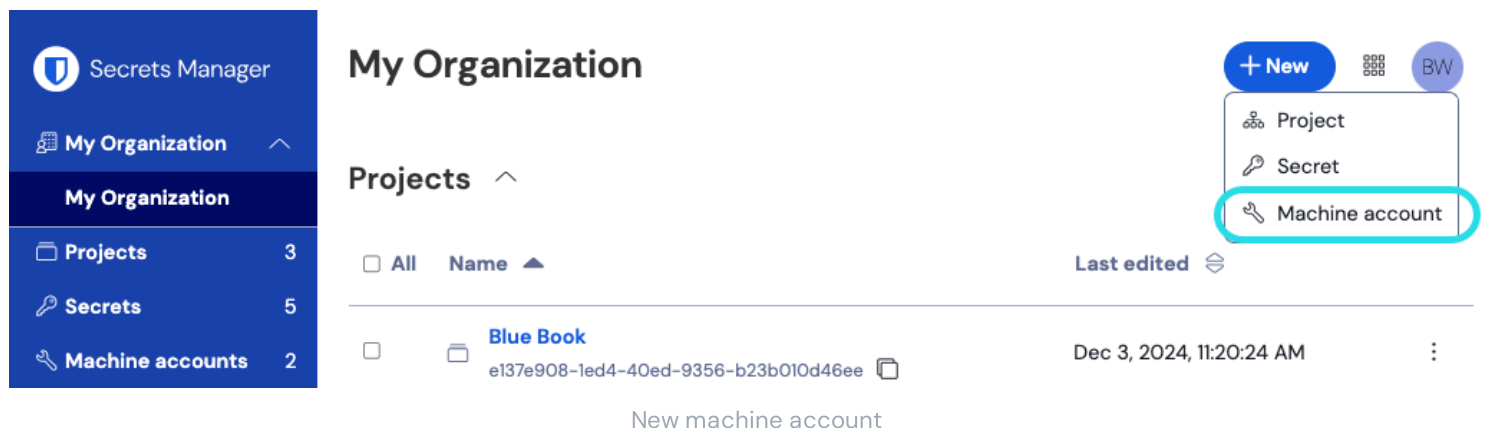
Add a machine account

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**.

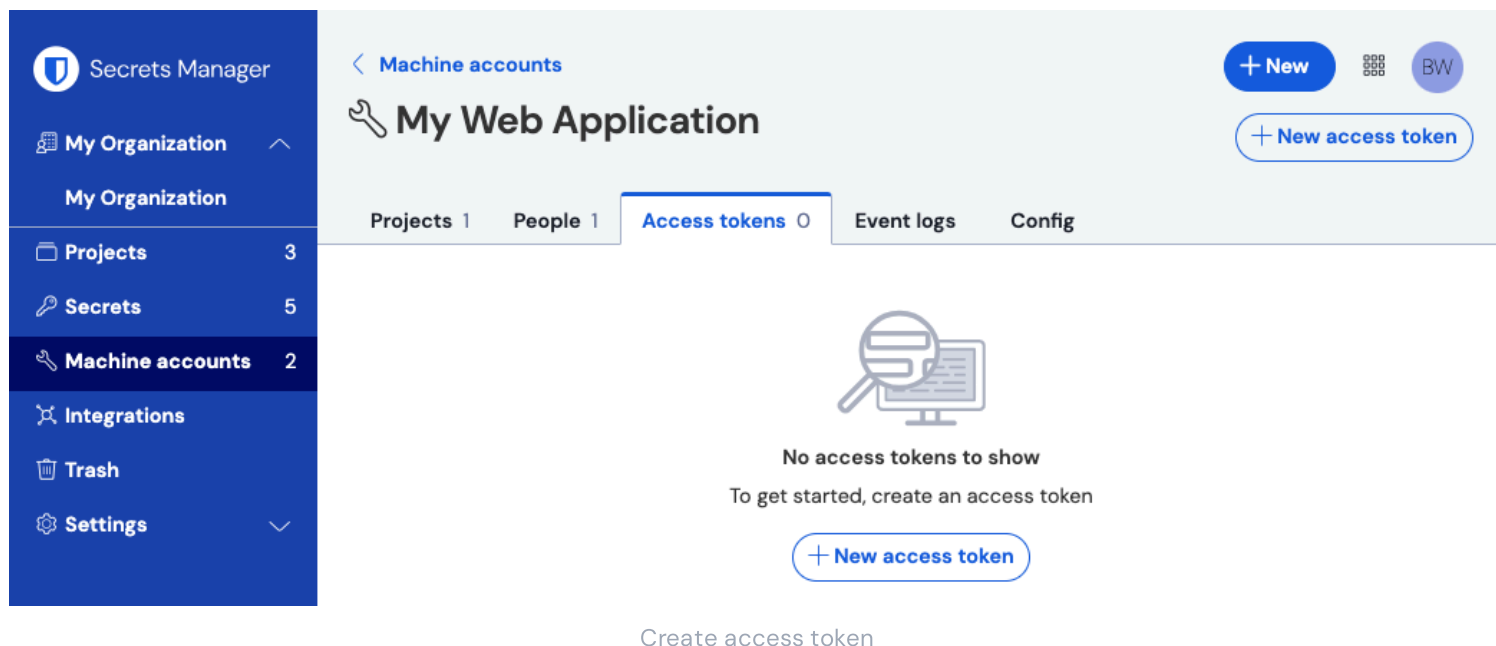
3. Open the machine account and, in the **Projects** tab, type or select the name of the project(s) that this machine account should be able to access. For each added project, select a level of **Permissions**:

- **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:



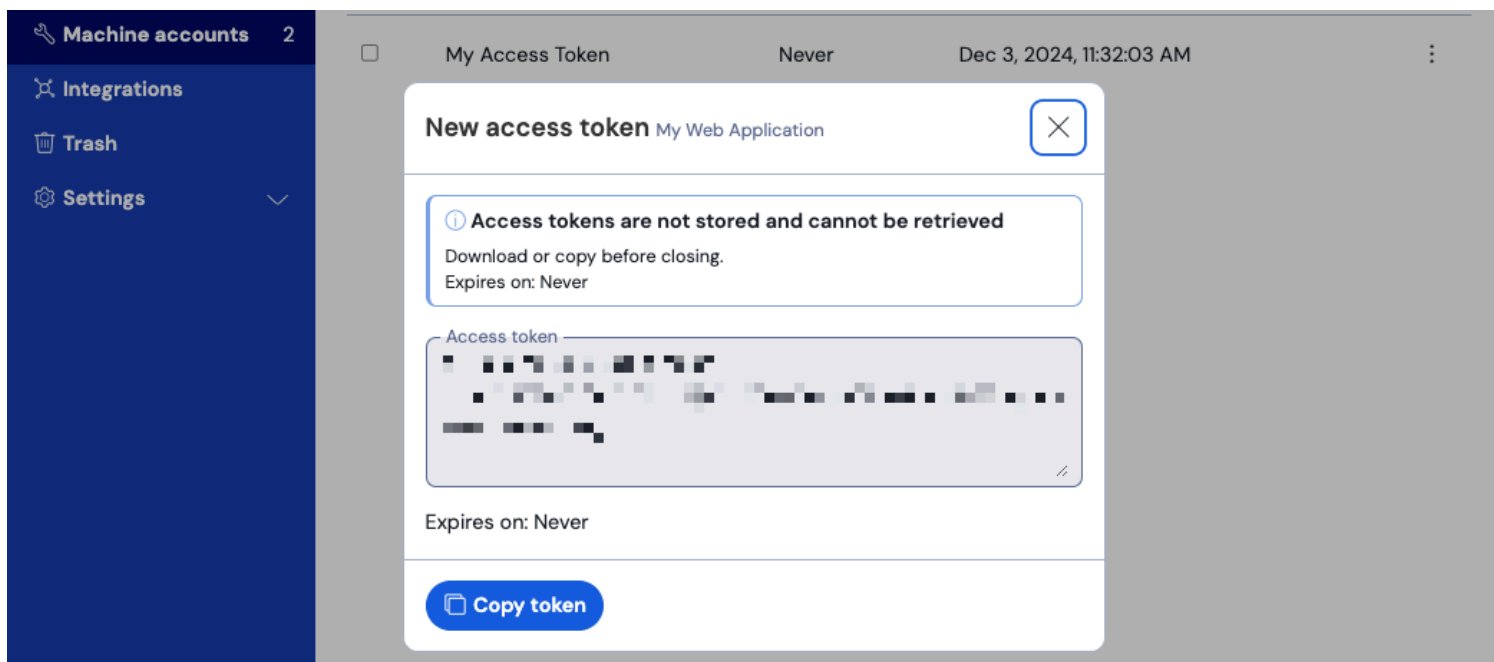
3. Select the **Create access token** button.

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](#)