SECRETS MANAGER > YOUR SECRETS

Machine Accounts

Machine Accounts

> ⓘ **Note**
>
> As of the 2024.4.1 release, service accounts are now referred to as machine accounts in Bitwarden Secrets Manager. All of the feature functionality will remain the same.

Machine accounts represent non-human machine users, like applications or deployment pipelines, that require programmatic access to a discrete set of secrets. 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.

Machine accounts that your user account has access to can be viewed by selecting **Machine accounts** from the navigation:

Machine accounts

Opening a machine account will list the **Secrets** and **People** the service account has access to, as well as any generated **Access tokens** and **Event logs**:
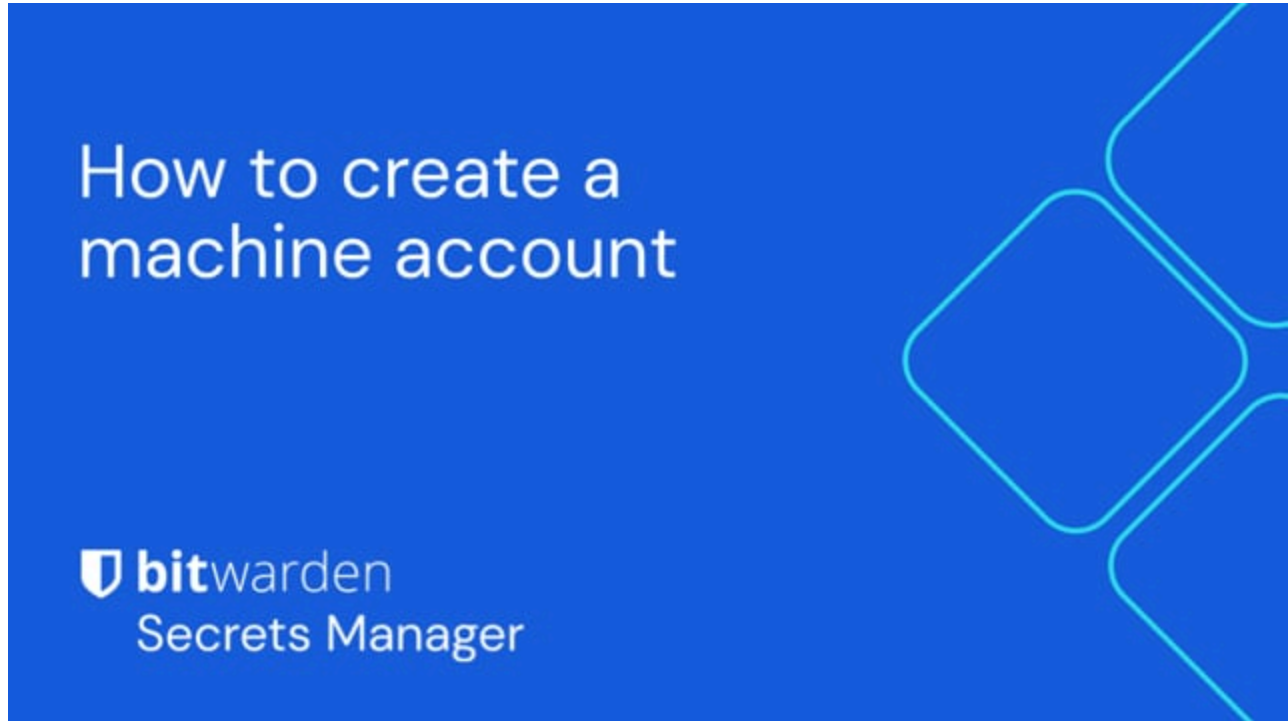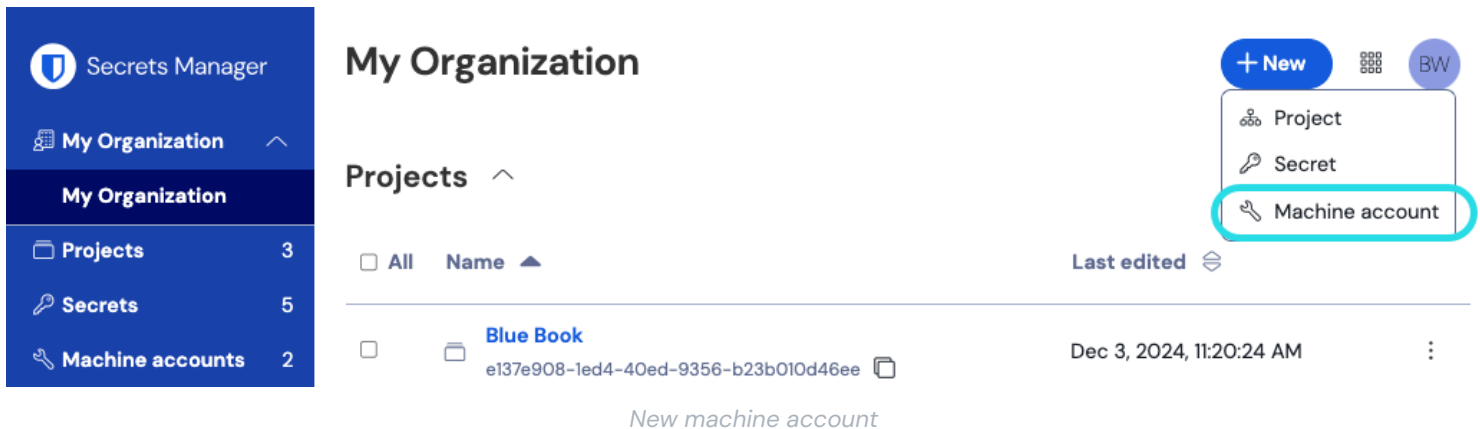

Inside a machine account

Create a machine account

On the Admin Console **Billing → Subscription** page you are able to assign the number of machine accounts available for use in your organization. For additional information regarding your available machine accounts and machine account scaling, see here.

To create a new machine account:

https://player.vimeo.com/video/845933062

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

New 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, create new secrets in assigned projects, or create new projects altogether.

> 💡 **Tip**
>
> Fully utilizing write access for machine accounts is dependent on a forthcoming CLI release. For now, this simply makes the option available in the UI. Stay tuned to the Release Notes for more information.

Add people to a machine account

Adding organization members to a machine account will allow those people to generate access tokens for the machine account and interact with all secrets the machine account has access to. To add people to your machine account:

1. In the machine account, select the **People** tab.

2. From the people dropdown, type or select the members or groups to add to the machine account. Once you've selected the right people, select the **Add** button:


Add people to a machine account

Add projects to a machine account

Adding projects to a machine account will allow programmatic access to included secrets using access tokens. To add projects to a machine account:

1. Open the machine account and select the **Projects** tab.

2. From the Projects dropdown, type or select the project(s) to add to the machine account. Once you've chosen the right projects, select the **Add** button:
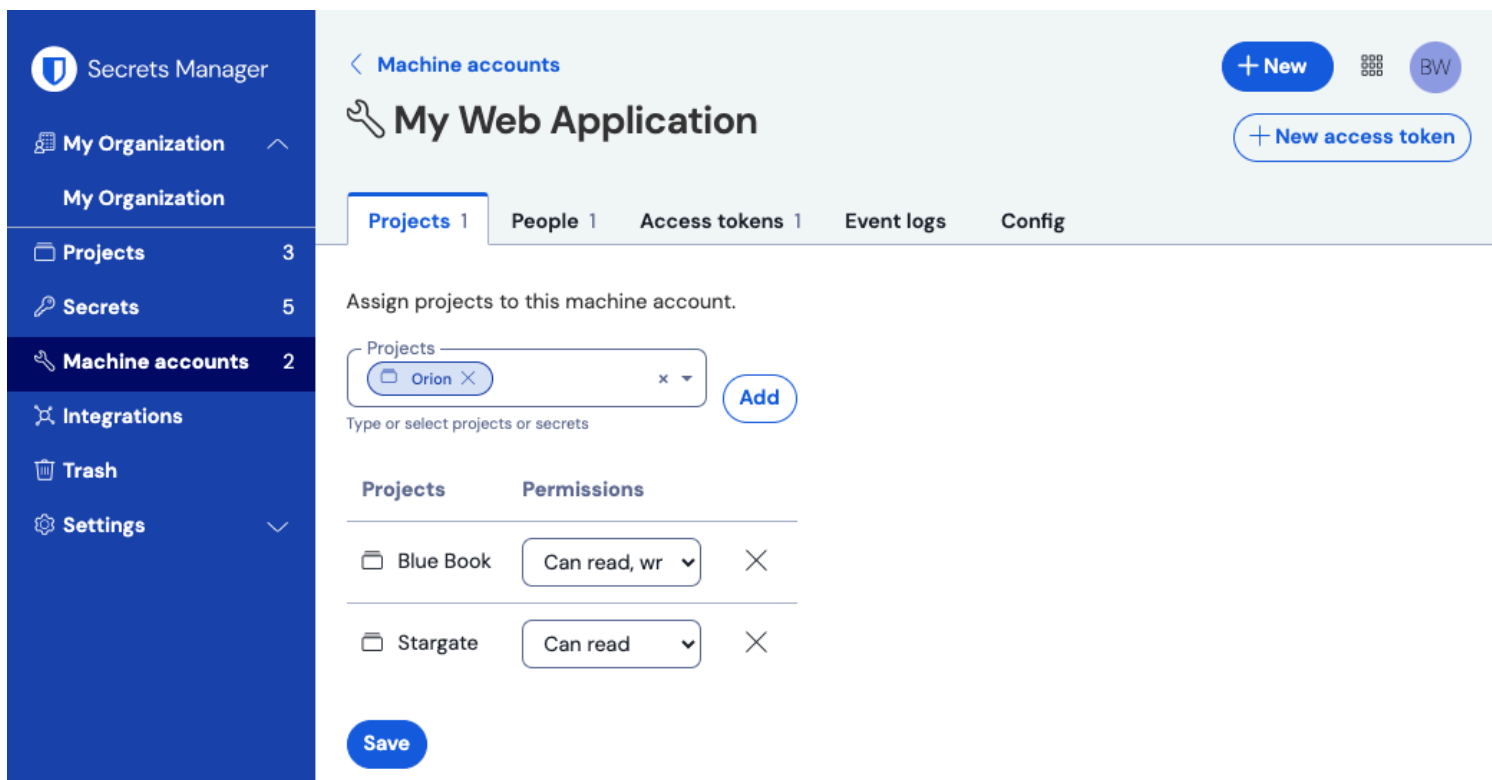
Add a project

3. 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.

Delete a machine account

To delete a machine account, use the (⋮) options menu for the machine account to delete to select **Delete machine account**. Deleting a machine account **will not** delete the secrets associated with it. Machine accounts are fully removed once deleted and **do not** get sent to the trash like secrets do.

Machine account events

Timestamped records of actions taken with each service account are available from the machine account's **Event logs** tab.

Any user that has access to a given machine account will be able to view events for that machine account. Events that are captured include:

- Accessed secret *secret–identifier*. (2100)

> ⓘ **Note**
>
> Each **Event** is associated with a type code (1000, 1001, etc.) that identifies the action captured by the event. Type codes are used by the Bitwarden Public API to identify the action documented by an event.

Event logs are exportable and are retained indefinitely. Exporting events will create a .csv of all events within the specified date range, which should not exceed 367 days.

Configuration information

The **Config** tab provides a quick view of information that might be required when configuring an application to use a machine account. **Identity server URL**, **API server URL**, **Organization ID**, and **Project IDs** are displayed and can be copied by selecting each field's respective ⎘ icon. For more information on Secrets Manager environments, see the Secrets Manager SDK documentation and CLI documentation.

Machine account config view