bitwarden | Help Center Article

SECRETS MANAGER > YOUR SECRETS

Access Tokens

View in the help center:
https://bitwarden.com/help/access-tokens/

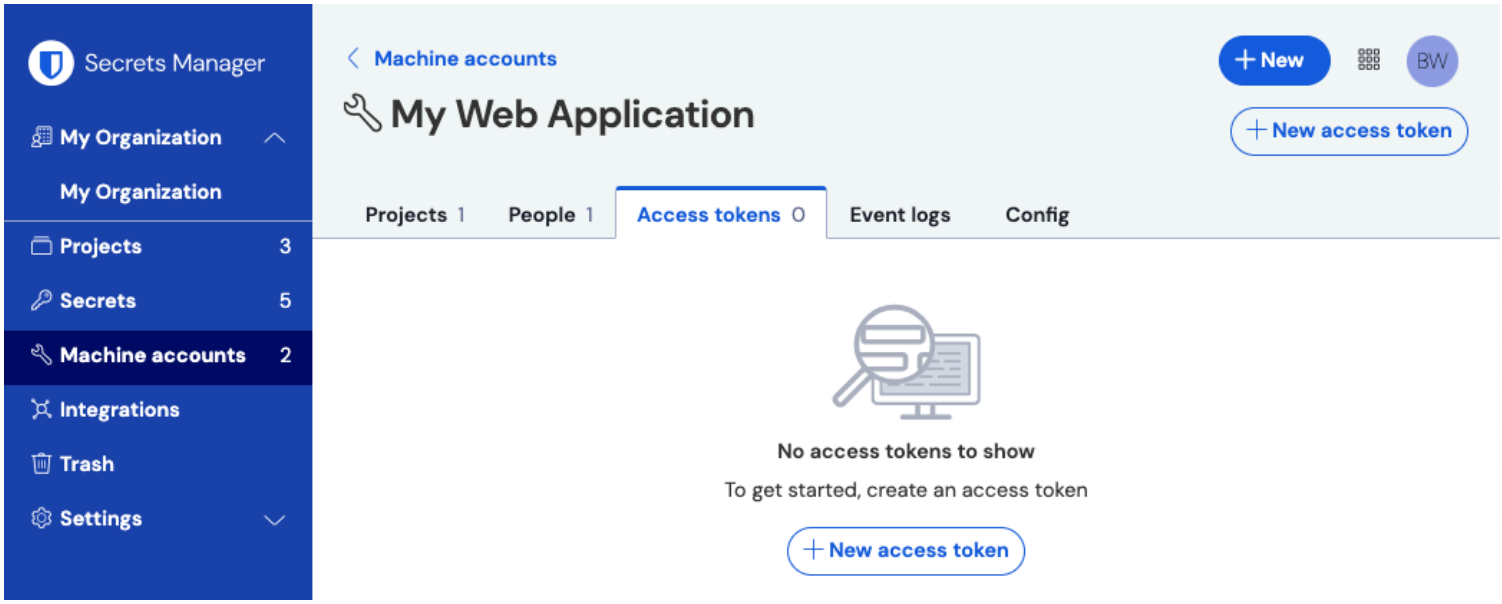
Access Tokens

Access tokens are objects that facilitate machine account access to, and the ability to decrypt, edit, and create secrets stored in Secrets Manager. Access tokens are issued to a particular machine account, and will give any machine they're applied to the ability to access **only the secrets associated with that machine account**.

Create an access token

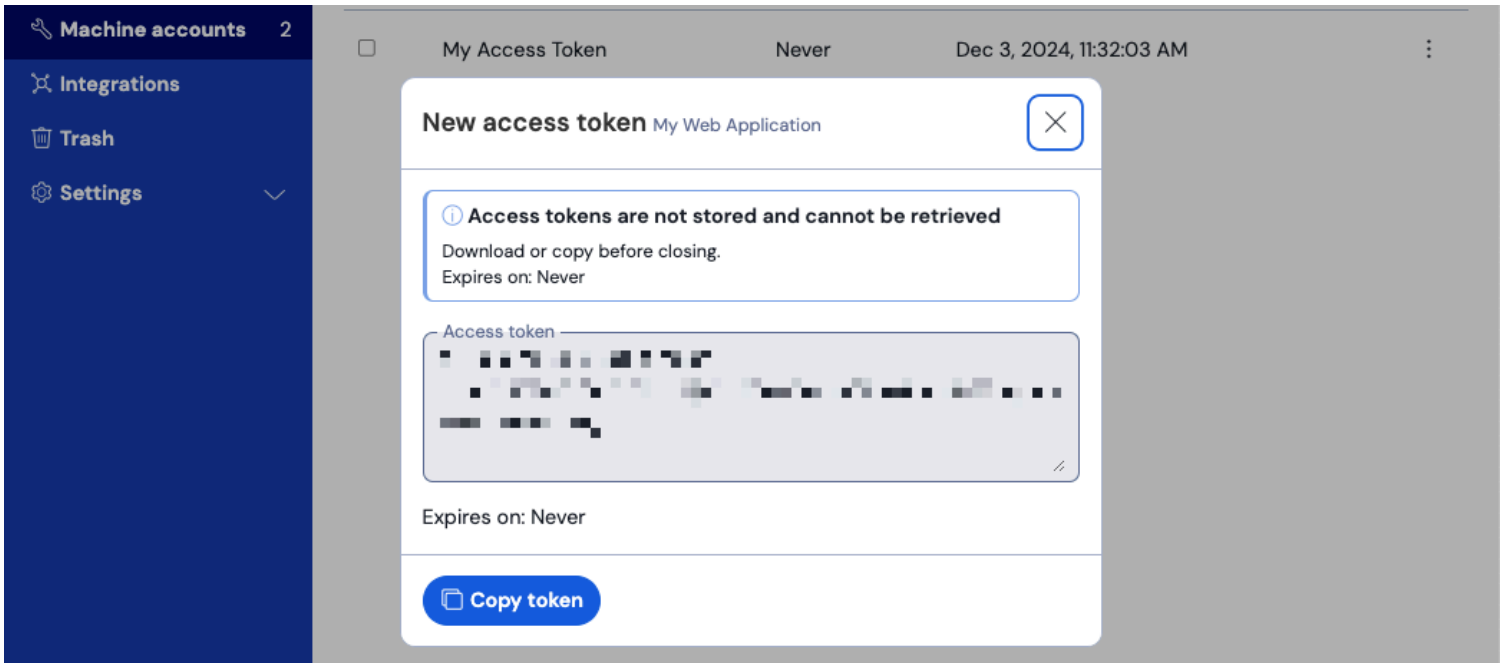
Access tokens are never stored in Bitwarden databases and cannot be retrieved, so take care to store your access tokens somewhere safe when you generate them. To create an access token:

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 window, provide:
    1. A **Name** for the token.
    2. 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. Save your token somewhere safe before closing this window, as your token **will not be stored and cannot be retrieved later**:



Access token example

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

Use an access token

Access tokens are used for authentication by the Secrets Manager CLI. Once you've created your access token and saved its value somewhere safe, use it to authenticate secret retrieval commands by the CLI for injection into your applications or infrastructure. This could be:

- Exporting the access token to a `BWS_ACCESS_TOKEN` environment variable on the host machine. CLI commands like the following will automatically check for a variable with that key for authentication:

```
Bash

bws project get e325ea69-a3ab-4dff-836f-b02e013fe530
```

- Using the `-access-token` option inline a script written to `get` and inject secrets, for example something that includes the lines:

```
Bash

...
export DB_PW=$(bws secret get fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff --access-token 0.48c78342-163
5-48a6-accd-afbe01336365.C0tMmQqHnAp1h0gL8bngprlPOYutt0:B3h5D+YgLvFiQhWkIq6Bow== | .jq '.value')
...
docker run -d database ... -env DB_PW=$DB_PW ... mysql:latest
```

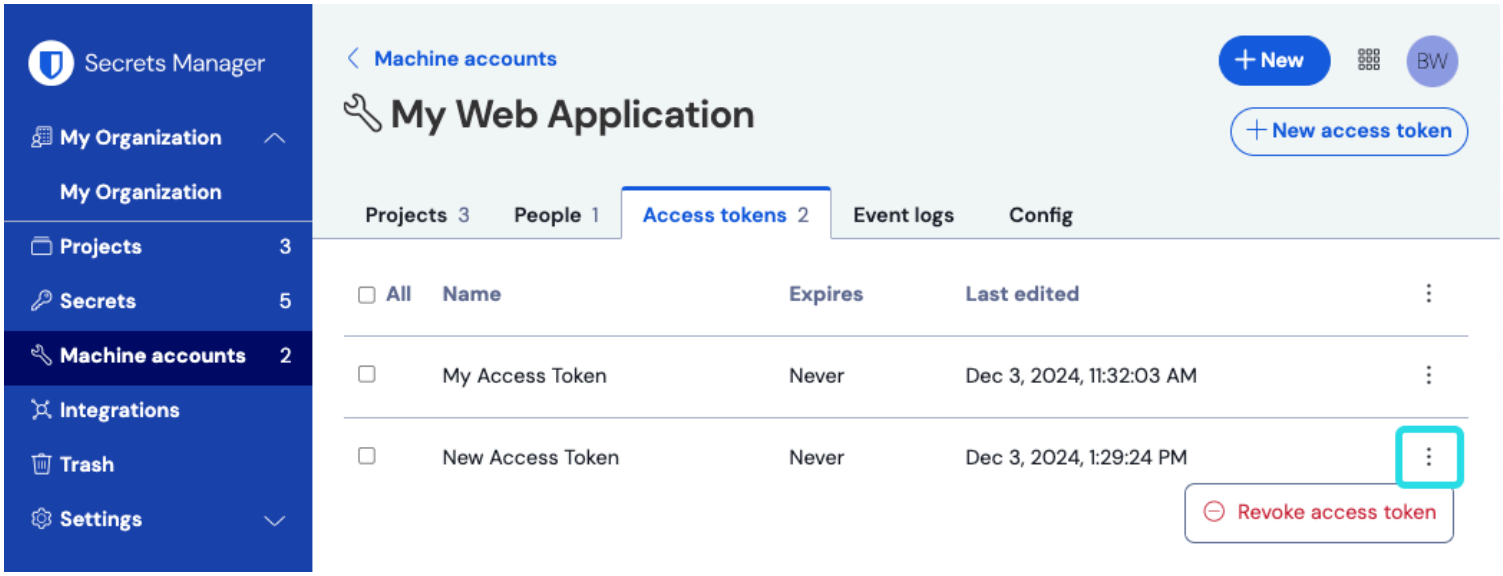
- Using our dedicated GitHub Actions integration to save the access token as a repository secret for use in your workflow files.

Revoke an access token

At any time, you can revoke an access token. **Revoking a token will break the ability of any machines currently using it to retrieve and decrypt secrets**. To revoke a token:

1. Select **Machine accounts** from the navigation, and open the **Access tokens** tab.

2. For the access token you want to revoke, use the (⋮) options menu to select **Revoke access token**:



Revoke access token