bitwarden | Help Center Article

SECRETS MANAGER

Secrets Manager Overview

View in the help center:
https://bitwarden.com/help/secrets-manager-overview/

Secrets Manager Overview

Bitwarden Secrets Manager enables developers, DevOps, and cybersecurity teams to centrally store, manage, and deploy secrets at scale. Use Secrets Manager to:

- **Manage and deploy secrets across the development lifecycle**. Develop a secure and systematic approach to creating and automating secrets for all your resources and applications.

- **Boost productivity, collaborate securely**. Safely share, retrieve, and assign secrets across your development teams - no more hard-coding secrets or sharing them through email, git, or messaging systems.

- **Level up your protection**. For full enterprise security coverage, combine the capabilities of secrets management with password management.

Key concepts

The core paradigm used by Secrets Manager is the relationship between:

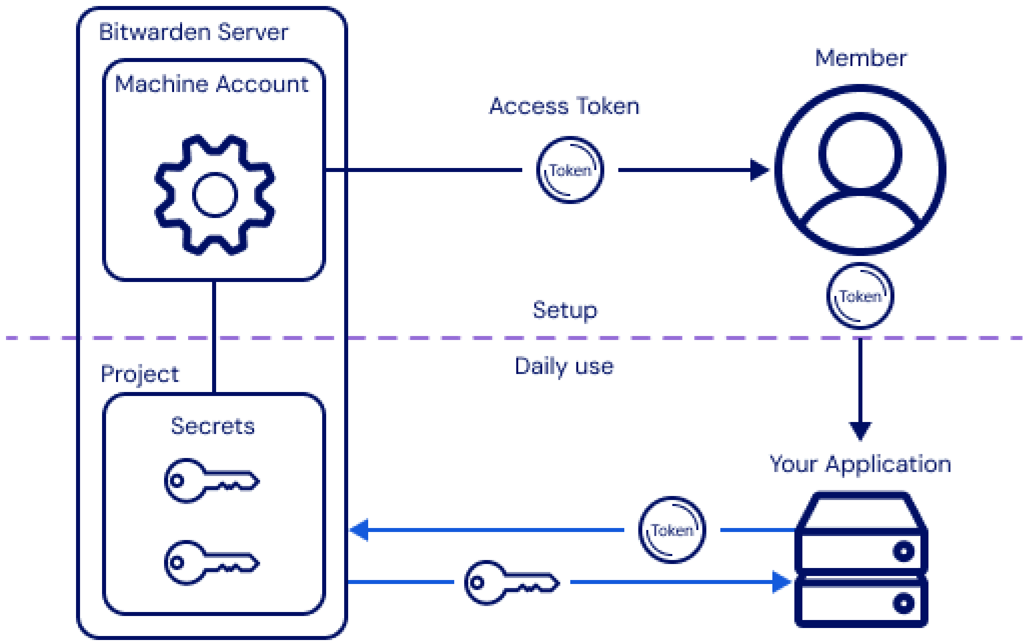
- **Secrets**: Sensitive key-value pairs, like API keys, that your organization needs securely stored and should never be exposed in plain code or transmitted over unencrypted channels.

- **Projects**: Collections of secrets logically grouped together for management access by your DevOps and cybersecurity teams.

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

- **Access tokens**: A set of keys that facilitates machine account access to, and the ability to decrypt, secrets stored in your vault.

Secrets Manager is designed to secure and manage your highly sensitive credentials within privileged developer environments. Multi-directional layers of access and levels of permission will ensure that only authenticated machines and persons with the correct permissions will be able to see or manipulate secrets stored within your vault:



Secrets Manager Diagram

Security-first principles

Bitwarden is committed to building security-first products. Secrets Manager, like Password Manager, is:

- **Open source**: All source code is hosted on GitHub and is free for anyone to review and audit. Third-party auditing firms and security researchers are paid to do so regularly.
- **End-to-end encrypted**: All encryption and decryption of secrets data is done client-side, meaning no sensitive data ever hits our servers unencrypted.
- **Zero-knowledge encrypted**: Bitwarden team members can't see your secrets, your passwords, or your master password.

> **Tip**
>
> Bitwarden Secrets Manager can also be self-hosted. Learn more here.

Clients

Secrets Manager offers a web app, CLI, and SDK. In the future, more SDK libraries will be supported.

Web vault

The Secrets Manager web app is your home for setting up your secrets management infrastructure. You'll use it to add and organize secrets, create systems of permission to fit your needs, and generate access tokens for use by your applications.

CLI

The Secrets Manager CLI is your primary vehicle for injecting secrets into your applications and infrastructure. You'll use it to script secrets injection into your applications through an authenticated machine account.

SDK

The Secrets Manager software development kit (SDK) helps developers create applications for secrets management. The Secrets Manager SDK is used by the Bitwarden team to build discreet integrations with popular products, like GitHub Actions, and can be used by the community to build applications of their own.

Get started today

We're excited to be a part of your secrets management journey, and pleased that you'll be joining us in this new adventure. Sign up for Secrets Manager today.

Bitwarden offers Secrets Manager subscriptions for Free, Teams, and Enterprise organizations. If you have a Families plan and would like to use Bitwarden Secrets Manager, simply create a new Free organization and sign up for Secrets Manager following these steps.

> **Tip**
>
> For a deep dive into the product, check out the on-demand Secrets Manager demo.