bitwarden | Help Center Article

SECRETS MANAGER > YOUR SECRETS

Secret Decryption

View in the help center:
https://bitwarden.com/help/secret-decryption/

Secret Decryption

Secrets Manager can use access tokens, in addition to master passwords, to decrypt, edit, and create secrets. Specifically, this is done in secrets injection scenarios like the examples here.

Conceptually, access tokens consist of two component pieces:

- **An API key**, containing a client id and secret for authentication with Bitwarden servers.
- **A unique encryption key**, which will be used to decrypt an encrypted payload containing your organization symmetric encryption key.

When an access token is used, for example when authenticating a CLI command like `bws get secret`:

1. A request is sent to Bitwarden servers containing the API key's client id and client secret.
2. Bitwarden servers use these credentials to authenticate the client session, and send a response containing an encrypted payload. This encrypted payload contains the organization symmetric key.
3. Once received, the organization symmetric key is decrypted locally using the access token's unique encryption key.
4. A subsequent request is sent to Bitwarden APIs for the data called for in the `bws` command, for example a secret.
5. Bitwarden determines whether the called-for data can be provided based on a machine account identifier in the request. If yes, a response is sent to the client with the encrypted data.
6. The data is decrypted locally using the organization symmetric key. Relevant values are used however you're using Secrets Manager, for example saving a decrypted `"key": ""` value to an environment variable.