

PASSWORD MANAGER > DEVELOPER TOOLS > CLI

CLI Authentication via API Key



View in the help center:

<https://bitwarden.com/help/personal-api-key/>

CLI Authentication via API Key

Your Bitwarden personal API key can be used as a method for authenticating into the command line interface (CLI).

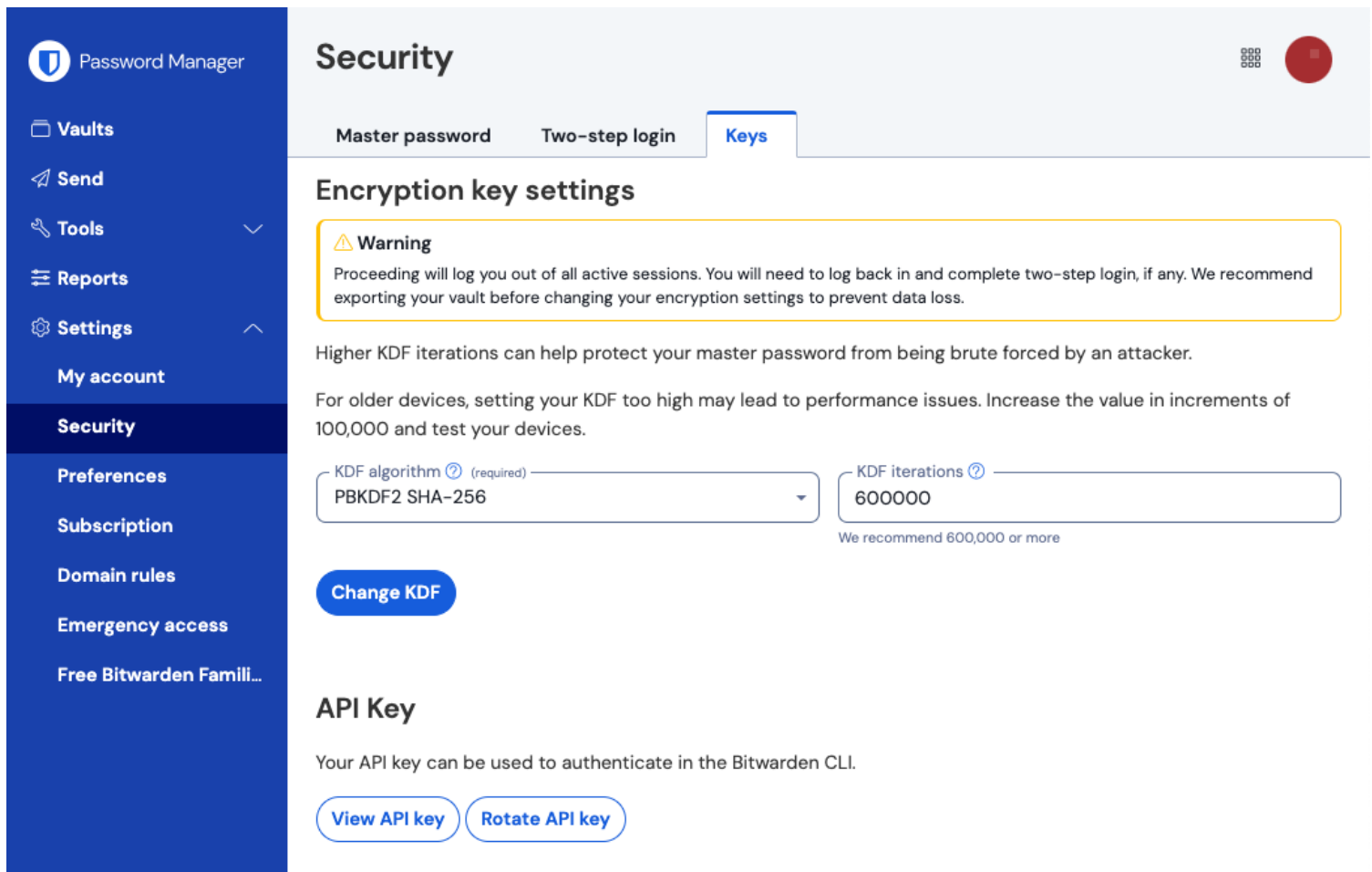
Note

Your personal API key is **not the same** as the [organization API key](#) used to access the [Bitwarden Public API](#) or [Directory Connector](#). Personal API keys will have a `client_id` with format `"user.clientId"`, while organization API keys will have a `client_id` with format `"organization.ClientId"`.

Get your personal API key

To get your personal API key:

1. In the Bitwarden web app, navigate to **Settings** → **Security** → **Keys**:



The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation links: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Subscription, Domain rules, Emergency access, and Free Bitwarden Famili... The main content area has a light blue header with the title 'Security' and a sub-header 'Keys'. Below the header are tabs for 'Master password', 'Two-step login', and 'Keys'. The 'Keys' tab is active. The main content area is titled 'Encryption key settings' and contains a yellow warning box with a triangle icon. The warning text reads: 'Warning: Proceeding will log you out of all active sessions. You will need to log back in and complete two-step login, if any. We recommend exporting your vault before changing your encryption settings to prevent data loss.' Below the warning, there is text explaining that higher KDF iterations can help protect the master password from brute force attacks. There are two input fields: 'KDF algorithm (required)' with a dropdown menu showing 'PBKDF2 SHA-256', and 'KDF iterations' with a text input showing '600000'. A blue button labeled 'Change KDF' is below the algorithm dropdown. At the bottom of the main content area, there is a section titled 'API Key' with the text 'Your API key can be used to authenticate in the Bitwarden CLI.' and two buttons: 'View API key' and 'Rotate API key'.

Keys

2. Select the **View API key** button and enter your master password to validate access. Once entered, you will be provided the following:

- `client_id: "user.clientId"` (This value is unique to your account and does not change.)
- `client_secret: "clientSecret"` (This value is unique and can be rotated).
- `scope: "api"` (This value will always be `"api"`).
- `grant_type: "client_credentials"` (This value will always be `"client_credentials"`).

Rotate your API key

Select the **Rotate API Key** button to rotate your personal API key. Rotating your key will only change your `client_secret`.

Rotating your key will invalidate your previous key and all active sessions using that key.

Authenticate using your API key

Logging in to the CLI with the personal API key is **recommended for automated workflows or providing access to an external application**. To log in with the API key:

Bash

```
bw login --apikey
```

This will initiate a prompt for your personal `client_id` and `client_secret`. Once your session is authenticated using these values, you'll be prompted to use the `unlock` command ([learn more](#)).

Using API key environment variables

In scenarios where automated work is being done with the Bitwarden CLI, you can save environment variables to prevent the need for manual intervention at authentication.

Environment variable name	Required value
BW_CLIENTID	<code>client_id</code>
BW_CLIENTSECRET	<code>client_secret</code>