Extension security

An extension can have the following optional parts:

- A user interface in HTML or JavaScript, displayed in Docker Desktop Dashboard
- A backend part that runs as a container
- Executables deployed on the host machine.

Extensions are executed with the same permissions as the Docker Desktop user. Extension capabilities include running any Docker commands (including running containers and mounting folders), running extension binaries, and accessing files on your machine that are accessible by the user running Docker Desktop. Note that extensions are not restricted to execute binaries that they list in the host section of the extension metadata: since these binaries can contain any code running as user, they can in turn execute any other commands as long as the user has rights to execute them.

The Extensions SDK provides a set of JavaScript APIs to invoke commands or invoke these binaries from the extension UI code. Extensions can also provide a backend part that starts a long-lived running container in the background.

> [!IMPORTANT]
>
> Make sure you trust the publisher or author of the extension when you install it, as the extension has the same access rights as the user running Docker Desktop.

□□□ #2
□ □□□ □□□ 2026-10-31 19:32:29 UTC
□ □□□ □□□ 2026-10-31 19:32:30 UTC