

CHECK YOUR AGENT'S BOUNDARIES

Permissions should match the task you actually want it to do.

GitHub's local sandboxing restricts agent-run tools and commands according to developer or organisation policies. Tool isolation and the location of model execution are separate concerns.

Review the policy

1. Identify the project folder the agent can read and edit. Keep unrelated files and credential folders outside the allowed scope.
2. Check allowed network destinations and access to Git or GitHub CLI credentials. Start with the smallest access that can complete your task.
3. Read the current client setup guide and confirm sandboxing is active in the session; do not rely on a prompt alone.
4. In a disposable sample project, test an allowed file edit and an attempted read of a dummy file outside the allowed folder. Check that the latter is blocked.

Your boundary checklist

1. Allowed files: _____ Allowed network destinations: _____
2. Credential access: _____ Actions requiring approval: _____
3. Policy confirmed active: _____ Dummy boundary test result: _____

When a task is blocked

1. Check which permission the specific action needs. Adjust only that scope, then re-run the boundary check.
2. Review the diff and test the result even when every command ran inside the sandbox.

ORIGINAL RESOURCE

[GitHub's local sandboxing announcement](https://github.blog/changelog/2026-10-07-local-sandboxing-for-github-copilot-now-generally-available/)

<https://github.blog/changelog/2026-10-07-local-sandboxing-for-github-copilot-now-generally-available/>

An independent companion by Huzaifa Shoukat. Check the original project for current setup and availability. Prepared 12 October 2026.