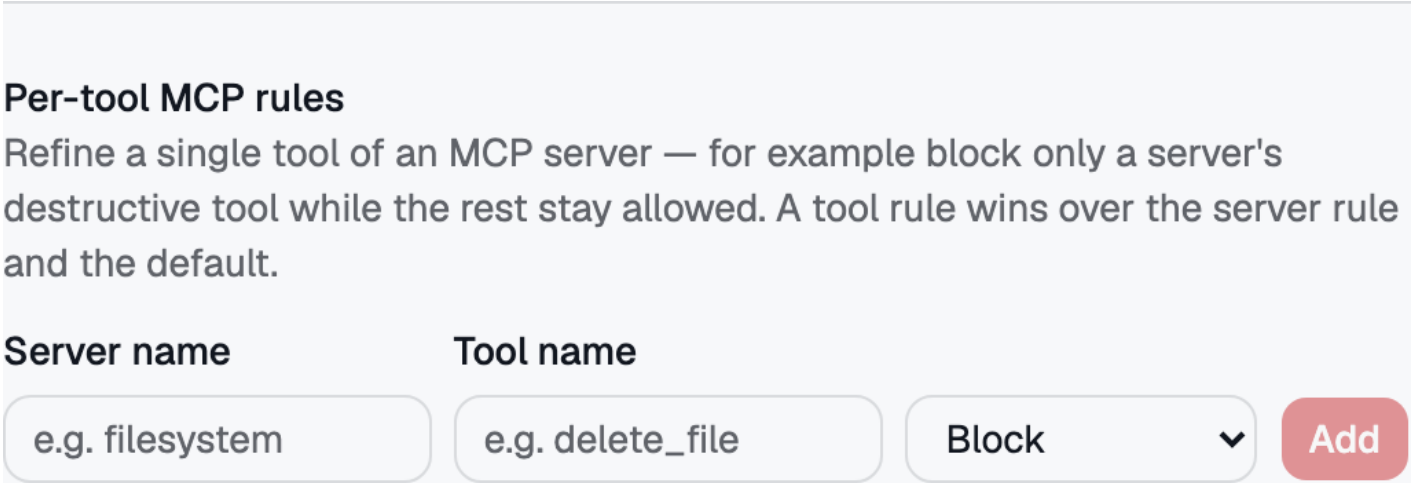
Per-tool rules

A per-server rule is sometimes too blunt: you want `github` available, but not `delete_repository`. Per-tool rules let you allow a server while blocking individual tools inside it.

Open a server's row on **MCP Inventory** to set rules for the individual tools that server exposes. The most specific rule wins: a tool rule beats its server's rule, which beats the MCP default action.

Why this matters more than it sounds

An MCP server's tool list is not fixed. A server you approved can add a tool later, or change what an existing tool's description tells the model to do — the "rug pull" pattern. Sentilai fingerprints tool definitions and flags changes, so an approved server that starts behaving differently re-enters review instead of silently inheriting your trust.



Per-tool MCP rules — refine a single tool of a server, for example block only the tool that writes.

Revision #11
Created 2026-08-01 13:06:41 UTC by Sentilai Docs
Updated 2026-08-06 04:31:38 UTC by Sentilai Docs