

MCP Server Setup

Wire one local server. Validate it sees only what you scoped.

The frontier of the operator's stack in this era is connecting AI to your own tools and files under your own control — and the Model Context Protocol is how that's done safely. This week you install one local MCP server (Filesystem, Git, or Playwright), wire it to Claude Code or your workflow, and validate that it can see only what you scoped — nothing more. Security as the default, not the afterthought.

THE ACTION

- Pick one MCP server to start: Filesystem, Git, or Playwright.
- Install it and wire it to Claude Code or your local workflow.
- Scope it deliberately — point it at exactly one folder or repo, not your whole drive.
- Validate the scope: ask it to reach outside the boundary and confirm it can't.

SCOPE TIGHT, THEN LOOSEN

Give a tool the narrowest access that lets it do the job, and widen only when you must. The watchman grants ground deliberately — he doesn't hand over the keys to the whole city to save a few minutes.

SCRIPTURE

Luke 16:10 — "He who is faithful in what is least is faithful also in much." Faithful scoping of a small server is the same muscle as faithful stewardship of everything larger.