Per-server rules

MCP Inventory lists every MCP server Sentilai has seen — discovered on developer machines by the Endpoint Suite, and independently observed in Gateway traffic. Nothing here is typed in by hand; the list is what your team actually runs.

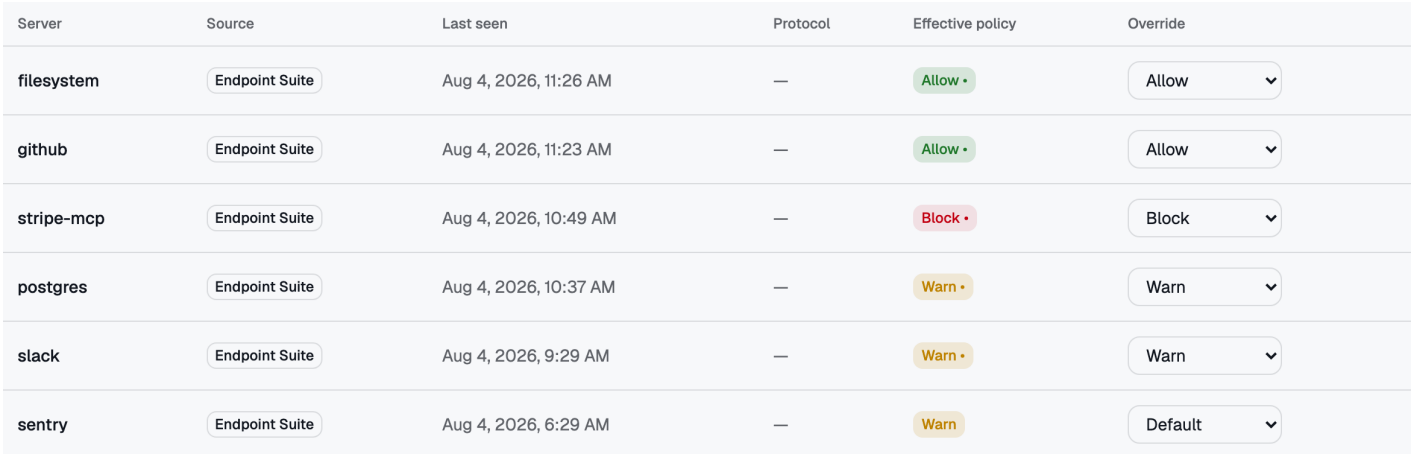
Each row shows:

- **Server** — the name as the tool declares it.
- **Source** — how we know about it (Endpoint Suite discovery, or Gateway traffic).
- **Last seen** — the most recent request.
- **Protocol** — the MCP protocol version it speaks, when it reports one.
- **Effective policy** — the rule in force right now.
- **Override** — the per-server rule you set: `Allow`, `Warn`, `Report`, `Block`, or `Default` (fall back to the MCP default action).

Changing the override takes effect within seconds — the Endpoint Suite caches decisions briefly (see **Local MCP decision cache** under Policy).

A practical order of work

1. Recognise the servers you expect — `github`, `filesystem`, your database — and set `Allow`.
2. Set `Warn` on anything that touches production data.
3. Set `Block` on anything with payment, billing or admin reach that developers don't need day to day.
4. Leave the rest at `Default` and let your MCP default action decide.



Server	Source	Last seen	Protocol	Effective policy	Override
filesystem	Endpoint Suite	Aug 4, 2026, 11:26 AM	—	Allow •	Allow
github	Endpoint Suite	Aug 4, 2026, 11:23 AM	—	Allow •	Allow
stripe-mcp	Endpoint Suite	Aug 4, 2026, 10:49 AM	—	Block •	Block
postgres	Endpoint Suite	Aug 4, 2026, 10:37 AM	—	Warn •	Warn
slack	Endpoint Suite	Aug 4, 2026, 9:29 AM	—	Warn •	Warn
sentry	Endpoint Suite	Aug 4, 2026, 6:29 AM	—	Warn	Default

MCP Inventory — every server your developers use, with the rule in force and a per-server override.

Revision #12
Created 2026-08-01 13:06:40 UTC by Sentilai Docs
Updated 2026-08-05 06:29:11 UTC by Sentilai Docs