Approval for new MCP servers

Turn on **Require approval for new MCP servers** when you want unknown servers held back until someone has looked at them.

How it behaves

A server nobody has reviewed — meaning it has no explicit per-server rule on **MCP Inventory** — is enforced at the **pending action** you choose, instead of the MCP default action. Setting any explicit rule for that server counts as reviewing it, and takes over from the pending action immediately.

So the workflow is:

1. A developer starts using a new MCP server.
2. It appears in **MCP Inventory** with a *Pending approval* badge.
3. Until you set a rule, it's held at the pending action (typically `block` or `warn`).
4. You set `allow`, `warn`, `report` or `block` — and the badge disappears.

Why this exists

The MCP ecosystem is young and unvetted; a server added on Tuesday can do anything its tools describe. This setting turns "anyone can add anything" into "anything new waits for a human", without blocking the servers your team already relies on.

Revision #8
Created 2026-08-01 13:06:38 UTC by Sentilai Docs
Updated 2026-09-29 14:39:30 UTC by Sentilai Docs