

MCP default action

This is the rule the Gateway applies to an MCP server that has **no explicit rule of its own**. Set it under **Policy ? MCP default action**.

Action	What developers experience	When to use it
Allow	Nothing changes	You want visibility first, controls later
Warn	A warning before the server is used	The usual starting point
Report	Nothing; usage is logged for review	You want a quiet audit trail
Block	The request is rejected	Locked-down environments

Per-server rules on **MCP Inventory** always override this default — so a strict default with a few allowed servers, or a permissive default with a few blocked ones, are both sensible shapes.

Where it applies

Enforced for Claude Code traffic today. Other tools are audited and appear in Activity; their MCP enforcement follows.

Recommended path

Start at **Warn**, watch **MCP Inventory** fill up with what your team actually uses for a week, set explicit rules for the servers you recognise, then decide whether to tighten the default. Starting at **Block** works but generates support requests on day one.

MCP default action

☐ **Allow**

MCP servers run without restriction.

☒ **Warn**

Developers see a warning before using an MCP server.

☐ **Report**

Usage is logged for review; developers are not interrupted.

☐ **Block**

The Gateway rejects any request that declares an MCP tool.

Per-server rules on MCP Inventory override this default — allow specific servers through a strict default, or block individual ones under a permissive default. Enforced for Claude Code traffic today.

☐ **Require approval for new MCP servers **

Servers nobody has reviewed yet are held at the pending action below.

“Reviewed” means any explicit per-server rule on MCP Inventory — setting one always takes over from this pending action.

AI risk classifier sensitivity

How aggressively the AI risk classifier acts on what it finds in outbound prompts. Medium (recommended) records medium- and high-severity findings as warnings; Low suppresses low-confidence signals for a quieter feed; High is the strictest. Findings appear on the Activity screen either way.

Policy ? MCP default action. Per-server rules on MCP Inventory override this default.

Revision #13

Created 2026-08-01 13:06:37 UTC by Sentilai Docs

Updated 2026-08-05 06:29:13 UTC by Sentilai Docs