

MCP protocol versions

The **Protocol** column on MCP Inventory shows which version of the Model Context Protocol each server actually negotiated with the tool that called it.

Where the number comes from

The Sentilai shim observes the handshake between the AI tool and the local server and reports the negotiated version. It is observed, not asserted — this is what the two ends actually agreed on, not what the server's documentation claims.

A dash with a tooltip means no handshake has been observed yet: usually the server is known only from a chat-request declaration or from Gateway traffic, with no shim in the path.

Why it matters

The protocol has changed meaningfully between versions, including in how tool calls are framed and what a server may assert about itself. A server pinned to an old version is not necessarily dangerous, but it is a signal worth having when you are deciding whether to approve something.

It is also useful in reverse: if a server you expect to be governed shows no protocol at all, the shim is probably not in its path, and your per-tool rules will not apply to it.

What Sentilai enforces

The Gateway checks that the request's headers and body agree about which MCP method and server are being addressed, and rejects requests where they do not. A mismatch is either a broken client or an attempt to have the policy engine and the server read the same request differently.

Revision #5

Created 2026-08-02 10:19:53 UTC by Sentilai Docs

Updated 2026-08-02 16:29:01 UTC by Sentilai Docs