

Bring AI into your lab. With a trail you can trust.

A self-hosted proxy that records every AI tool call in a tamper-evident audit trail and lets through only the calls you allow. Designed to support GLP, 21 CFR Part 11 and EU GMP Annex 11 workflows.

 ChatGPT Claude Copilot

Your infrastructure. Your policies. Your control.

You decide what information can be sent to external AI providers.

The challenge

AI assistants are starting to query lab, research and business systems directly, through the Model Context Protocol (MCP). In regulated and research settings every action needs to be traceable. Yet plain logs can be edited or deleted without anyone noticing, and many AI set-ups have no audit trail at all.



Which tool was called, when, and what was done?



Can you show the record has not been changed?



Can you stop an assistant doing what it shouldn't?

How it works

1

Connect



Place the proxy between your AI assistant and your systems (over MCP). A setup wizard configures it and checks the configuration.

**2**

Check & record



Every tool call is recorded: what, when, which tool. Calls not on your allowlist are blocked, and the block is logged.

**3**

Verify



Each entry is hash-chained to the one before. The verify tool shows if anything was altered or deleted.

Key benefits



Complete, automatic trace

What, when and which tool, for every call, with no manual effort.



Tamper-evident

Any alteration or deletion of the trail is detectable.



Read-only by default

Plus an allowlist: other calls are blocked, and every block is logged.



No friction for your team

Never waits for anyone and never changes message content.



Self-hosted, no phone-home

The audit trail stays on your own infrastructure.



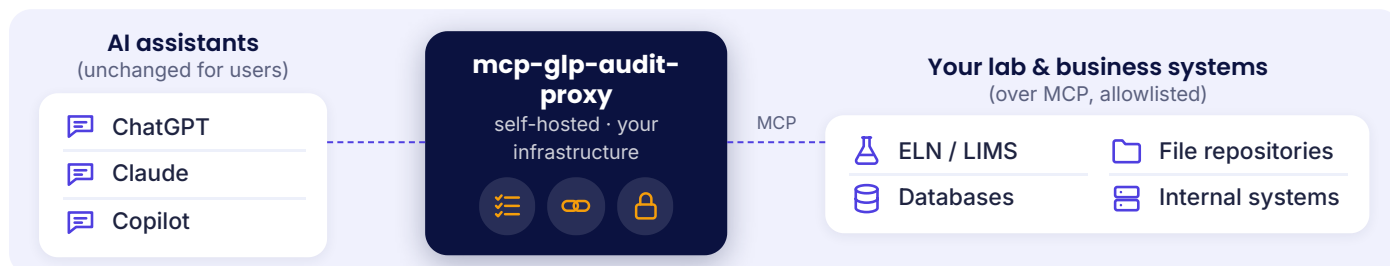
Free to start

Open-source Community edition (MIT), available now, with a setup wizard.

Same AI assistants. Every call on the record.

One self-hosted proxy between your AI tools and your systems: unchanged for users, traceable for your teams.

Where it sits



How it differs

	No audit trail	Generic logging	mcp-glp-audit-proxy
Every AI tool call recorded automatically	✗ No	– Depends on setup	✓ Yes: what, when, which tool
Alteration or deletion is detectable	✗ No	✗ Not by design	✓ Hash chain + verify tool
Only approved calls get through	✗ No	✗ No, logs only observe	✓ Read-only default + allowlist
Runs on your own infrastructure	– n/a	– Varies	✓ Self-hosted, no phone-home
Designed to support GLP, 21 CFR Part 11 and EU GMP Annex 11 workflows	✗ No	✗ No	✓ Yes

Unlike typical AI gateways, which offer logs or observability, mcp-glp-audit-proxy is built around a hash-chained, tamper-evident audit trail and is positioned for GxP and research workflows.

Two editions



Community edition

AVAILABLE NOW

Free, open source (MIT), v0.3.0 · PyPI, MCP Registry, GitHub.

- ✓ Hash-chained JSONL log
- ✓ Verify tool with pinning
- ✓ Allowlist
- ✓ Setup wizard

```
pip install mcp-glp-audit-proxy
```



Pro edition

COMING SOON

For regulated teams that need more.

- ✦ SQL/MSSQL and S3 Object Lock storage
- ✦ PDF/CSV reports
- ✦ Before/after values
- ✦ IQ/OQ validation pack



Designed to support GLP, 21 CFR Part 11 and EU GMP Annex 11 workflows. It does not by itself guarantee regulatory compliance and does not replace the validation of your systems.

Contact us / Request a demo

Try the free Community edition today, or write to us to request a demo for your lab, company or university.

Email antonio@castellon.ch

Antonio Castellon · Castellon.CH

antonio@castellon.ch

+41 76 689 13 69

castellon.ch

Biel/Bienne, Switzerland