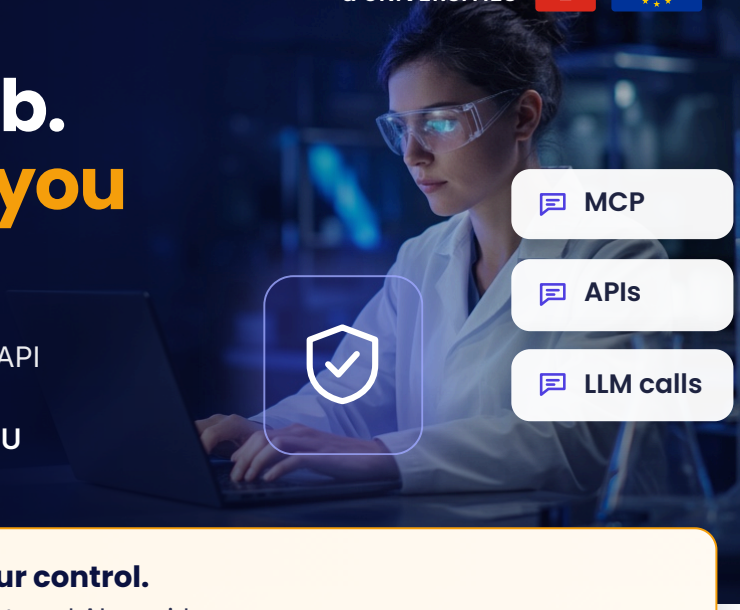
Castellon.CH | GxP Gateway Audit

FOR LABS, LIFE SCIENCE & UNIVERSITIES

Bring AI into your lab. Every call on a trail you can trust.



A self-hosted gateway that records MCP tool calls, API calls and LLM calls in a tamper-evident audit trail. **Designed to support GLP/GxP, 21 CFR Part 11 and EU GMP Annex 11 workflows.**

Your infrastructure. Your policies. Your control.
You decide what information can be sent to external AI providers.

The challenge

AI assistants, agents and scripts now reach lab and business systems through MCP, HTTPS APIs, gateways and LLM calls. In regulated and research settings every action needs to be traceable, yet plain logs can be edited or deleted without anyone noticing.

- **Which call was made, when, and what was done?**
- **Can you show no record was changed or deleted?**
- **Can you stop a call that shouldn't go through?**

How it works

1 Connect
Runs as a reverse proxy over TLS. Clients only change their base URL. Flows: mcp2mcp, mcp2api, api2mcp, api2api, mcp2llm, api2llm.

2 Check & record
Every call is recorded in a hash-chained trail. Authentication by mTLS and/or token; body storage: hash only (default), redacted or full.

3 Verify
Fail-closed: if a record is deleted or the chain breaks, it stops and alerts with which record and when.

Key benefits

MCP and HTTPS
One audit layer for MCP tools, APIs, gateways and LLM calls.

Tamper-evident, fail-closed
A broken or deleted record stops the gateway and raises an alert.

You choose what is stored
Hash only by default, or redacted or full bodies.

No client rewrite
Reverse proxy: clients only change the base URL.

Offline regulatory report
Lists regulations by type and country and whether your config supports them.

Free to start
Community edition, open source (MIT), 240 tests.

Overleaf: how it differs, editions and contact →

info@castellon.ch castellon.ch

Castellon.CH | GxP Gateway Audit

FOR LABS, LIFE SCIENCE & UNIVERSITIES



Same AI, same APIs. Every call on the record.

A complement to your systems' own audit trail: one self-hosted gateway, unchanged for users, traceable for your teams.

Where it sits

Clients
(only the base URL changes)

- AI assistants
- Agents & scripts
- Applications

GxP Gateway Audit
self-hosted reverse proxy · TLS

MCP/HTTPS

Your systems & services
(MCP or HTTPS)

- MCP servers
- HTTPS APIs
- Gateways
- LLM endpoints

How it differs

	No audit trail	Generic logging	GxP Gateway Audit
MCP, API and LLM calls recorded automatically	✗ No	– Depends on setup	✓ Yes, one trail for all six flows
Alteration or deletion is detectable	✗ No	✗ Not by design	✓ Hash chain, fail-closed alert
You control what bodies are stored	✗ No	– Varies	✓ Hash only, redacted or full
Shows which regulations your config supports	✗ No	✗ No	✓ Offline regulatory report
Designed to support GLP/GxP, 21 CFR Part 11 and EU GMP Annex 11 workflows	✗ No	✗ No	✓ Yes

Unlike typical AI gateways, which offer logs or observability, GxP Gateway Audit is built around a hash-chained, tamper-evident, fail-closed audit trail, as a complement to your systems' own audit trail.

Two editions

Community edition

AVAILABLE NOW

Free, open source (MIT), v0.4.0 · PyPI, GitHub.

- ✓ Hash-chained trail, schema 1.3.0
- ✓ mTLS and/or token auth
- ✓ Archive manifests, review
- ✓ Offline regulatory report

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

Pro edition

DEMO ON REQUEST

Paid edition for regulated teams.

- Signed records
- SSO, approvals
- WORM storage, SIEM
- Reports, IQ/OQ pack

Designed to support GLP/GxP, 21 CFR Part 11 and EU GMP Annex 11 workflows. It complements your systems' own audit trail, 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 Pro demo for your lab, company or university.

Email info@castellon.ch

Antonio Castellon · Castellon.CH
info@castellon.ch
+41 76 689 13 69
castellon.ch
Biel/Bienne, Switzerland

GxP Gateway Audit (package mcp-glp-audit-proxy). Community records are tamper-evident (hash-chained), not signed.
github.com/antonio-castellon/mcp-glp-audit-proxy · pypi.org/project/mcp-glp-audit-proxy