

Give Claude the keys. Keep the locks.

JobLog's MCP server lets Claude read the platform and take real action in it, with the authorization, audit, and guardrails a security review expects.

JobLog is my construction-site security platform. Operators can ask Claude what happened overnight, then acknowledge and resolve incidents by voice.

ON A JOBSITE, BY VOICE

You: Resolve 42. It was the foreman, he's authorized.

Claude: Resolving incident 42 as Authorized Person Confirmed, noted as the site foreman. Go ahead?

You: Yes.

Claude: Done. Logged under your name, in your words.

You: Close it out too.

Claude: I can resolve the incident, but final closure isn't available through MCP. That remains a separate workflow.

Illustrative exchange. Every write previews first, then commits as a separate step.

I4 TOOLS, READ AND WRITE	4 ADDRESSABLE RESOURCES	2 OPERATOR PROMPTS	Entra ID OAuth 2.0 SIGN-IN
--	---	--	--

Claude works inside JobLog.

Live site, device, incident, and evidence state across every site you can see, plus real actions: acknowledge, annotate, resolve, escalate, create.

Actions an operator can say yes to.

Every write previews, then commits as a separate call carrying the user's verbatim request. The audit trail records the acting principal. The riskiest actions aren't exposed at all.

Access that fits an enterprise.

Clients self-register against an allowlist, sign in through Entra ID, and see only what their membership allows. Revoke someone and their next call fails.

morning-brief

Overnight incidents, coverage gaps, and silent devices, ranked by what needs a decision today.

incident-triage

Walks the evidence in order and recommends a priority, citing the frames it rests on.

WHAT THE BUILD DECIDED

Whether to pass Entra's token through or mint JobLog's own, and what each costs in revocation latency. Which annotations actually make a client gate an action, versus which are merely semantically correct. Which operations to expose at all: read first, writes after a separate policy decision, closure not at all.

Christopher J. Wolff
cwolfftechnologies.com

UNDER THE HOOD

The complete JobLog MCP surface.

All three MCP primitives (tools, resources, and prompts), served over Streamable HTTP and scoped exactly as the application is.

READ TOOLS

- get_site_status**
Per site: protected, coverage gap, or offline
- list_active_incidents**
Open incidents by site and priority, by number
- get_incident**
State, owner, next action, timeline, legal hold
- list_device_status**
Reporting, silent, or never live, with coverage gaps
- search_events**
Detections in a window, and why each opened an incident or not

- get_evidence_metadata**
Provenance and content hash, never a storage path
- get_recent_activity**
Timeline entries across visible sites, up to seven days
- get_camera_snapshot**
One frame, never a stream; stale after five minutes
- list_checkins**
Authorized workers on site, in site-local time
- get_profile_version**
The server's own profile version

WRITE TOOLS

- acknowledge_incident**
Stops escalation. A repeat is a safe no-op that reports who acted first.
- add_incident_note**
Appends to the incident timeline.

- Every write: preview, then commit. Attributed to the signed-in person, or to the service identity.
- update_incident_status**
Resolve with a reason code, or escalate without a new notification blast. Assign refuses by design.
- create_incident**
Notifies the roster for real, and says so before you confirm.

RESOURCES

- joblog://organizations/{id}
- joblog://sites/{id}
- joblog://incidents/{id}
- joblog://devices/{id}

PROMPTS

- morning-brief**
Overnight incidents, coverage gaps, and silent devices, ranked by what needs a decision today.
- incident-triage**
Walks the evidence in order and recommends a priority, labeled as AI, without setting it.

BUILT TO PASS A SECURITY REVIEW

- Standards-based sign-in.** Dynamic client registration (RFC 7591), PKCE, RFC 9728, 8414, and 9207 metadata, Entra ID.
- Instant revocation.** Revoke access in JobLog and the next call fails at every endpoint. Lookup errors fail closed.

- Two-step writes.** A five-minute, single-use, argument-bound token, then a commit carrying the user's own words.
- Honest data.** No evidence storage paths, stale frames flagged, AI recommendations labeled.