MCP SERVER | NO CODE | CLOUD HOSTED

Household Key Custody Log MCP

Keep a clear record of who holds your physical keys.

Household Key Custody Log MCP lets your AI client manage the lifecycle of physical keys. You can record when keys are handed out, track who has them right now, and close out custody events when items are returned. It turns your agent into a precise log keeper for physical security and accountability.

A+ Quality Score 100/100

household | keys | custody | audit | log

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/household-key-custody-log

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Household Key Custody Log MCP

4 tools available
Cloud-hosted on Vinkius

Managing physical keys shouldn't rely on messy paper logs or memory. This MCP gives your AI client the ability to act as a digital custodian for your household or facility keys. You can use it to document exactly when a key leaves your possession and who is responsible for it. When a person brings a key back, you simply tell your agent to close the loop. This creates a reliable, searchable history of every handoff. If you ever need to know which keys are currently out in the field, your agent can pull that list instantly. It's a straightforward way to maintain accountability for physical access without manual bookkeeping.

Core Capabilities

01 — Issuance Tracking

Your agent logs the exact time and person receiving a key.

02 — Return Processing

Your agent marks keys as returned to clear them from active custody.

03 — Real-time Status Checks

Your agent identifies all current key holders on demand.

04 — Audit Reporting

Your agent generates summary tables of finished key transactions.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/household-key-custody-log** — connect your AI agent in three steps.

01 Connect your preferred MCP-compatible client to Vinkius.

02 Tell your agent to log a new key issuance for a specific person.

03 Ask your agent to check who currently holds keys when needed.

04 Instruct your agent to log a return once the key is back.

05 Request a signoff report to see your completed audit history.

Setting up key tracking with your AI client is a direct process.

Built For

This MCP is built for anyone managing physical access to a property or facility.

Property Managers

They hand off key handoff details to the agent to maintain tenant records.

Estate Managers

They use the agent to track service providers holding house keys.

Facility Coordinators

They rely on the agent to audit key movements across a site.

What Changes When You Connect

01 Eliminates manual paperwork for key tracking.

02 Prevents duplicate issuance of the same key.

03 Provides instant visibility into current key holders.

04 Creates a clean audit trail of completed transactions.

Real-World Applications

Maintenance Access

Log when a plumber or electrician takes a spare key and when they return it.

Tenant Turnovers

Track key handoffs during move-in and move-out periods.

Security Audits

Generate summary reports to verify all keys are accounted for.

Staff Management

Monitor which employees are currently carrying specific facility keys.

Patterns to Avoid

Manual paper log entry

AVOID

You write down that a contractor took the master key on a sticky note and hope you remember to record it later.

✓ INSTEAD

Tell your agent to use log_key_issuance immediately when the handoff happens to ensure the record is instant and accurate.

Ignoring active key holders

AVOID

You assume all keys are back in the safe because the maintenance window ended.

✓ INSTEAD

Ask your agent to run query_active_custody to see exactly who still has keys in their possession.

Duplicate issuance attempts

AVOID

You try to log a key as being given to a second person while the first person still has it.

✓ INSTEAD

The log_key_issuance tool prevents this by checking if the key is already out before it saves the new entry.

The Right Fit

Connect this MCP if you manage physical access to a property and need a digital trail for keys. Do not connect it if you only manage digital credentials or software permissions. The decision rests on whether you need to track physical objects moving between people.

Household Key Custody Log 4 Tools

These tools handle the entire lifecycle of a key handoff, from the initial issuance to final return and auditing.

#	TOOL	DESCRIPTION
01	`generate_signoff_report`	Creates a high-level summary table for auditing. This report only includes completed transaction cycles.
02	`log_key_issuance`	Records the moment a key is handed over to a specific person. The tool checks to make sure the key isn't already marked as issued before saving the entry.
03	`log_key_return`	Closes a custody event when a key is handed back to the primary custodian. It requires the key to be in an active issued state to work.
04	`query_active_custody`	Identifies everyone who currently has keys in their possession. You can filter the results by the holder's name.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U Record that the Front Door key was given to John Doe on 2023-10-01 for maintenance.

The issuance for the Front Door key to John Doe has been recorded for 2023-10-01.

U Who is currently holding any keys?

John Doe is currently holding the Front Door key issued on 2023-10-01.

U John Doe returned the Front Door key today.

The return of the Front Door key from John Doe has been successfully logged.

Frequently Asked Questions

01 **How do I track who has my keys?**

You can ask your AI client to query active custody to see a list of all individuals currently holding keys.

02 **Can I see a history of past key handoffs?**

Yes, you can use the tool to generate a signoff report which provides a summary table of all completed transactions.

03 **What happens if I try to issue a key that is already out?**

The issuance tool includes a check to ensure a key is not already marked as issued before it records the new event.

04 **Which AI clients can use this MCP?**

This MCP works with any compatible client including Claude, Cursor, Windsurf, and VS Code.

05 **Do I need to host this myself?**

No, Vinkius hosts and manages the MCP for you, so it is ready to use immediately after connection.

06 **How do I record a new key assignment?**

Use the `log_key_issuance` tool with the key label, holder name, and date.

07 **Can I see who currently has a key?**

Yes, use the `query_active_custody` tool to list all current key holders.

08 **How do I generate an audit report?**

Use the `generate_signoff_report` tool by providing a start and end date.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"household-key-custody-log": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Household Key Custody Log is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Household Key Custody Log. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	Household Key Custody Log MCP
Server ID	`01a0dd81-3d6e-72e1-8185-a79b88b3597e`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/en/ai-agent-connect/household-key-custody-log.