

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Digital Legacy Update Log MCP

Keep a precise, auditable record of your digital asset transitions.

Digital Legacy Update Log MCP provides the tools to maintain a chronological audit trail for digital assets. It tracks account status changes, manages custodian shifts, and versions instructional documents. Your AI client can use this to monitor compliance and ensure every change to a digital legacy is recorded and verifiable.

A+ Quality Score 100/100

audit

legacy

account-management

compliance

digital-assets



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

Digital Legacy Update Log MCP

4 tools available

Cloud-hosted on Vinkius

Managing digital assets requires a paper trail that doesn't rely on memory. This MCP gives your AI client the ability to act as a digital registrar for your legacy planning. Instead of manually tracking when a custodian changed or when an account status shifted, you let your agent handle the logging.

You can use it to keep a clean history of every instruction version and account movement. It's built for people who need to ensure that their digital estate management is transparent and follows a strict timeline. Whether you are updating a custodian or checking if a mandatory review is due, the MCP keeps the data organized and ready for audit. It turns your AI into a reliable bookkeeper for your digital legacy, ensuring that no status change or instructional update goes unrecorded.

Core Capabilities

01 — Audit Trail Creation

Your agent records every change to an account or custodian to build a timeline.

02 — Status Monitoring

The AI checks the current state of any digital account on demand.

03 — Compliance Verification

Your agent identifies accounts that are due for a mandatory review cycle.

04 — Instruction Versioning

The MCP tracks different versions of instructional documents for your assets.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/digital-legacy-update-log — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Grant the client access to the Digital Legacy Update Log MCP.
- 03 Ask your agent to log a change or check an account status.
- 04 The agent executes the specific tool to update or retrieve the audit data.

Connecting this MCP to your AI client gives your agent immediate access to your legacy audit tools.

Built For

This MCP is designed for professionals managing digital estates and sensitive asset transitions.

Estate Planners

They use the MCP to log changes in custodians and instruction versions for clients.

Digital Asset Managers

They rely on the audit history to track the movement and status of digital holdings.

Compliance Officers

They use the review cycle tool to ensure all accounts meet mandatory audit requirements.

What Changes When You Connect

- 01 Maintains a chronological record of all digital asset changes.
- 02 Automates the detection of overdue account reviews.
- 03 Provides a verifiable history of custodian and instruction updates.

04 Centralizes account status tracking within your AI client.

Real-World Applications

Custodian Transitions

Record when a new person or entity takes over the management of a digital account.

Compliance Scheduling

Check which accounts require a periodic review to stay compliant with estate protocols.

Account Status Audits

Pull a full history of an account to see exactly when its status changed from active to frozen.

Instruction Version Control

Track updates to digital legacy instructions to ensure the most recent version is always known.

Patterns to Avoid

Manual Log Entry Errors

❌ AVOID

You try to remember every custodian change and manually type them into a spreadsheet at the end of the month.

✓ INSTEAD

Use `log_legacy_update` to record every change the moment it happens so your audit trail stays perfect.

Missing Compliance Deadlines

❌ AVOID

You assume an account is still compliant and realize too late that it missed its mandatory review window.

✓ INSTEAD

Run `verify_review_cycle` to see exactly which accounts need attention right now.

Outdated Instruction Versions

❌ AVOID

You act on an old set of instructions because you didn't realize the custodian had updated the document.

✓ INSTEAD

Check the history using `get_audit_history` to confirm you are looking at the most recent version.

The Right Fit

Connect this MCP if you manage digital estates or sensitive asset transitions that require a strict, verifiable timeline. Do not connect it if you are managing simple, low-stakes personal accounts that don't require formal auditing. The decision rests on whether you need a tamper-proof paper trail for your digital assets.

Digital Legacy Update Log 4 Tools

These tools handle the heavy lifting of recording asset changes, checking account status, and managing compliance timelines.

#	TOOL	DESCRIPTION
01	get_audit_history	This tool provides a full, chronological list of all events tied to an account for auditing purposes.
02	log_legacy_update	Use this to record a new event, such as a change in an account, a custodian, or an instruction, directly into the audit log.
03	verify_review_cycle	This tool checks if an account needs a mandatory review based on its last recorded review date.
04	get_account_summary	This tool pulls the most recent status and core details for a specific digital account.

See It in Action

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

U What is the current status of account ACC-123?



Account ACC-123 is currently Active, and the latest instruction version is v2.1.

U Log a status change for account ACC-456 to Frozen.



The status change for account ACC-456 has been recorded in the audit log.

U Show me the history for account ACC-789.



The history for account ACC-789 includes three events: a status change, a custodian update, and a recent review confirmation.

Frequently Asked Questions

01 How do I use this MCP with Claude or Cursor?

You connect your client to the Vinkius platform, which hosts the MCP. Once connected, your AI client can immediately call the tools provided by this MCP.

02 Can I see a full history of account changes?

Yes, you can use the `get_audit_history` tool to retrieve a chronological list of all events associated with a specific account.

03 How does the MCP handle account reviews?

The `verify_review_cycle` tool checks the last recorded review date for an account to determine if it is due for a mandatory check.

04 What kind of data is recorded in the audit log?

The log records changes to account status, custodian shifts, and updates to instructional document versions.

05 Do I need to manage my own credentials?

No, Vinkius hosts the MCP and manages the necessary credentials so you can use it with one click.

06 How do I record a change in a custodian?

You can use the `log_legacy_update` tool with the `CUSTODIAN_CHANGE` update type and provide the `newCustodianId`.

07 How can I check if an account needs a review?

Use the `verify_review_cycle` tool by providing the account ID and the required review frequency in days.

08 Can I see the full history of an account?

Yes, the `get_audit_history` tool provides a complete chronological list of all recorded events for a specific account.

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 <code>"digital-legacy-update-log": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Digital Legacy Update 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 Digital Legacy Update 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	Digital Legacy Update Log MCP
Server ID	01a0db08-5cb8-71c1-bea1-b795984e0988
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/digital-legacy-update-log.