

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

Account Closure Evidence Register MCP

Maintain a verifiable audit trail for every account closure.

Account Closure Evidence Register MCP manages the entire lifecycle of your account closure audits. It lets you register new requests, track their progress, and store formal proof once a service confirms a closure. You can use it to identify overdue tasks and keep your compliance records organized in one central place.

A+ Quality Score 100/100

account-closure

audit-trail

compliance-tracking

data-privacy

verification



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.

Account Closure Evidence Register MCP

4 tools available

Cloud-hosted on Vinkius

Managing account closures shouldn't be a manual guessing game. This MCP gives you a centralized way to track every closure request from the moment it's initiated until you have hard evidence that the account is actually gone. Instead of digging through old emails or chat logs to prove a service was terminated, you record the formal evidence directly in the register.

You can use your AI client to monitor the status of all pending requests or quickly pull up a list of accounts that need immediate attention because their follow-up date has passed. It's built to ensure nothing slips through the cracks during the offboarding or data privacy cleanup process. By keeping a structured log of requests and verified proofs, you maintain a clean, ready-to-use audit trail for compliance requirements.

Core Capabilities

01 — Request Registration

Your agent adds new closure attempts to the log with specific follow-up dates.

03 — Status Monitoring

Your agent pulls high-level counts to show how many closures are in progress.

02 — Evidence Logging

Your agent attaches formal verification to pending requests to close the loop.

04 — Overdue Detection

Your agent identifies accounts that missed their scheduled follow-up date.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/account-closure-evidence-register — connect your AI agent in three steps.

- 01 Connect the MCP to your client via Vinkius.
- 02 Register a new closure request through your agent.
- 03 Monitor the status or check for overdue items using the summary and follow-up tools.
- 04 Record the formal evidence once the closure is confirmed.

Connecting this MCP to your AI client gives your agent direct access to the closure register.

Built For

This MCP is designed for teams managing sensitive data lifecycles and compliance workflows.

Compliance Officers

They use the MCP to maintain a verifiable audit trail for regulatory requirements.

IT Administrators

They use it to track the decommissioning of software accounts and cloud services.

Data Privacy Managers

They use it to ensure account deletions are completed according to privacy policies.

What Changes When You Connect

- 01 Centralizes all closure-related data in one place.
- 02 Eliminates manual tracking of overdue follow-ups.
- 03 Creates a verifiable record of closure evidence.

04 Reduces the risk of forgotten account terminations.

Real-World Applications

Cloud Service Offboarding

Track the deletion of AWS or Azure accounts to ensure no lingering costs or security risks remain.

SaaS License Cleanup

Manage the removal of user access across various subscription services.

Compliance Auditing

Generate a list of verified closures to present during a data privacy audit.

Employee Offboarding

Ensure every tool an employee used is properly decommissioned and documented.

Patterns to Avoid

Manual Spreadsheet Tracking

❌ AVOID

You keep a separate Excel sheet to track which accounts are closed and which are still active.

✓ INSTEAD

Use ``register_closure_request`` to log the attempt immediately so your agent can manage the follow-up dates for you.

Ignoring Overdue Requests

❌ AVOID

You wait until the end of the month to check if any account deletions failed or were ignored.

✓ INSTEAD

Run ``get_followup_list`` regularly to catch accounts that missed their scheduled follow-up date.

Vague Audit Records

❌ AVOID

You tell an auditor that an account is closed based on a verbal confirmation from a teammate.

✓ INSTEAD

Always use ``record_closure_evidence`` to attach formal, verifiable proof to the request in the register.

The Right Fit

Compliance officers and IT admins managing sensitive data lifecycles should connect this MCP. Teams with low-volume, non-regulated account changes don't need it. The decision depends on whether you need a verifiable audit trail to prove account terminations actually happened.

Account Closure Evidence Register: 4 Essential Tools

These tools handle the full lifecycle of a closure request, from initial registration to final evidence logging and status monitoring.

#	TOOL	DESCRIPTION
01	record_closure_evidence	This tool updates a pending request with the formal proof of closure. Use it once you have received confirmation that an account is officially closed.
02	get_register_summary	This tool provides a high-level overview of all current account closure request statuses. It's the quickest way to see how many requests are pending or verified.
03	register_closure_request	This tool adds a new account closure attempt to your register. It ensures your follow-up date is set correctly after the initial request date.
04	get_followup_list	This tool identifies all accounts requiring immediate attention. It pulls a list of requests where the follow-up date has already arrived.

See It in Action

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

U Give me a summary of all pending account closure requests.



There are currently 5 pending account closure requests in the register.

U Which account closures need my attention today?



The following requests are overdue: AWS (Full Deletion) and Slack (Subscription Stop).

U I have received confirmation for the AWS closure. The reference is REF-12345.



The request for AWS has been successfully updated to VERIFIED with confirmation reference REF-12345.

Frequently Asked Questions

01 How do I add a new account closure to the list?

You can use the `register_closure_request` tool through your AI client to add a new entry.

02 Can I prove that an account was actually closed?

Yes, you use the `record_closure_evidence` tool to attach formal proof to a pending request.

03 How do I find accounts that I forgot to follow up on?

Use the `get_followup_list` tool to see all accounts where the follow-up date has arrived.

04 What kind of clients can I use this with?

This MCP works with any compatible client like Claude, Cursor, Windsurf, or VS Code.

05 Does this MCP host my data?

Vinkius hosts and manages the MCP, making it ready to use immediately after you connect.

06 How do I see how many requests are still pending?

You can use the ``get_register_summary`` tool and filter by the PENDING status to see the current count of requests awaiting verification.

07 What should I do if a follow-up date has passed?

Use the ``get_followup_list`` tool to identify all requests that are overdue and require immediate verification or action.

08 How do I mark a closure as successful?

Once you receive a confirmation reference from the service, use ``record_closure_evidence`` to update the request status to VERIFIED.

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>"account-closure-evidence-register": { "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

Account Closure Evidence Register 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 Account Closure Evidence Register. 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	Account Closure Evidence Register MCP
Server ID	01a0db08-4089-705d-94af-3288fd5e05d4
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/account-closure-evidence-register.