

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

Location History Retention Plan MCP

Organize and manage geographic telemetry data lifecycle policies.

Location History Retention Plan MCP acts as a classification engine for your sensitive geographic telemetry data. It lets your AI client apply specific lifecycle policies to location records by filtering through dates, providers, or devices. You can organize data into Keep, Review, or Delete-On buckets to maintain control without accidental deletions.

A+ Quality Score 100/100

location

retention

telemetry

data-lifecycle

privacy-compliance



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.

Location History Retention Plan MCP

4 tools available

Cloud-hosted on Vinkius

Managing large volumes of geographic telemetry data is a headache, especially when privacy and compliance are on the line. This MCP gives your AI client the ability to act as a data lifecycle manager. Instead of manually sorting through thousands of coordinates, you can instruct your agent to categorize records based on your specific retention rules.

You can isolate data by provider or device before running analysis, ensuring you only touch the subsets that matter. The system organizes records into three distinct buckets: Keep, Review, or Delete-On. This approach lets you stage data for deletion without actually performing destructive actions, giving you a safety net to verify records before they are gone. It turns raw telemetry into a structured, actionable dataset that follows your exact compliance requirements.

Core Capabilities

01 — Data Categorization

Your agent sorts telemetry into Keep, Review, or Delete-On buckets.

02 — Granular Filtering

The AI isolates specific data subsets using provider or device identifiers.

03 — Expiration Tracking

Your agent calculates precise dates for when records should be flagged.

04 — Statistical Summaries

The tool provides counts and breakdowns of the current retention status.

05 — Non-Destructive Management

The MCP organizes data into buckets without performing immediate deletions.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/location-history-retention-plan — connect your AI agent in three steps.

- 01
- Connect your MCP-compatible client to the Vinkius platform.
- 02
- Define your retention rules and policies.
- 03
- Instruct your agent to filter or analyze specific telemetry subsets.
- 04
- Review the categorized buckets and expiration dates provided by the agent.

Connect your client to Vinkius and start managing telemetry through natural language.

Built For

This MCP is built for professionals managing large-scale geographic datasets who need to automate data lifecycle policies.

Data Privacy Officers

They hand off the task of auditing telemetry data against compliance rules to the AI.

Data Engineers

They use the tool to automate the categorization of telemetry streams.

Compliance Managers

They rely on the tool to verify that data retention policies are being followed.

What Changes When You Connect

- 01
- Prevents accidental data loss by using non-destructive buckets.
- 02
- Reduces manual sorting through automated provider and device filtering.

-
- 03 Provides clear visibility into data expiration through precise date calculations.
 - 04 Automates the classification of telemetry into actionable lifecycle stages.
-

Real-World Applications

Privacy Compliance

Automatically flag old location data for deletion to meet regulatory requirements.

Telemetry Auditing

Filter records by specific devices to check how different hardware handles data retention.

Data Lifecycle Automation

Set up rules that move records from Keep to Review as they age.

Storage Optimization

Identify large volumes of data in the Delete-On bucket to manage storage costs.

Patterns to Avoid

Blindly deleting raw telemetry

❌ AVOID

You run a script to wipe all old coordinates immediately to save space without checking them first.

✓ INSTEAD

Use the non-destructive buckets to stage data first. Use `analyze\_retention\_plan` to sort records into Review or Delete-On buckets so you can verify them before they are gone.

Analyzing the entire dataset at once

❌ AVOID

You try to run a full retention audit on millions of records across every single device in your fleet.

✓ INSTEAD

Narrow your scope first to save time and compute. Use `filter\_by\_provider\_device` to isolate the specific hardware or provider you need to audit.

Guessing expiration timelines

❌ AVOID

You assume all data is safe for 90 days and manually track when it needs to be purged.

✓ INSTEAD

Let the agent do the math. Use ``calculate_retention_expiration`` to find the exact date a specific record is scheduled to be flagged.

The Right Fit

Data engineers and privacy officers managing high-volume telemetry should connect this MCP. Teams handling small, static datasets or those without formal data lifecycle policies will find it unnecessary. The decision rests on whether you need to automate the classification of geographic records into actionable buckets.

4 Tools for Managing Location History Retention

These tools handle the heavy lifting of sorting, filtering, and auditing geographic telemetry data against your specific lifecycle rules.

#	TOOL	DESCRIPTION
01	analyze_retention_plan	This tool evaluates location records against your specific retention rules to sort them into categories.
02	calculate_retention_expiration	Use this to find the exact date a specific record is scheduled to be flagged for deletion.
03	filter_by_provider_device	This tool narrows down your records to a specific provider or device before you start the retention analysis.
04	summarize_retention_status	Get a statistical breakdown and a high-level count of how many records sit in each bucket.

See It in Action

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

U Analyze these location records using a 30-day retention policy.



The analysis is complete. 45 records are marked to Keep, 12 are in Review, and 5 are flagged as Delete-On.

U How many records are scheduled for deletion based on my current plan?



There are currently 8 records in the Delete-On bucket.

U Calculate the expiration date for a record from January 1st, 2024, with a 90-day retention period.



The record is scheduled to be flagged for deletion on March 31st, 2024.

Frequently Asked Questions

01 Does this MCP delete my data automatically?

No. The MCP organizes data into Keep, Review, or Delete-On buckets without performing destructive deletions.

02 Can I filter data by specific hardware?

Yes. You can use the filter tool to narrow down records to a specific device or provider.

03 How does the agent know when to delete a record?

The agent uses the expiration tool to calculate the exact date a record is scheduled to be flagged based on your rules.

04 What kind of data does this work with?

This MCP is designed for geographic telemetry and location history records.

05 Can I see a summary of my data status?

Yes. You can request a statistical breakdown of how many records fall into each retention bucket.

06 Does this tool delete my location data?

No. This tool is a classification engine. It flags records for future deletion using the ``analyze_retention_plan`` tool, but it does not perform the actual deletion.

07 How can I filter records by a specific device?

You can use the ``filter_by_provider_device`` tool to narrow down your records to a specific device ID before running a full retention analysis.

08 What are the different retention buckets?

Records are categorized into Keep (preserved), Review (gray area/approaching expiration), or Delete-On (ready for removal).

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>"location-history-retention-plan": { "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

Location History Retention Plan 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 Location History Retention Plan. 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	October 2026
MCP Server	Location History Retention Plan MCP
Server ID	01a0ef42-538f-71ea-8e0f-94555f943411
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/location-history-retention-plan.