MCP SERVER | NO CODE | CLOUD HOSTED

Alation MCP for AI Agents

Audit Data Lineage and Discover Enterprise Data Assets

Alation MCP brings enterprise data governance directly to your AI agent. Use this connector to search, audit, and query complex data assets across massive catalogs using plain conversation. It lets you discover metadata, trace lineage, and retrieve schema details without writing a single SQL command.

F Quality Score 3.6/100

data-catalog | data-governance | metadata-management | data-discovery | sql-querying | data-intelligence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/alation

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Alation MCP

10 tools available
Cloud-hosted on Vinkius

Working with large data environments means spending way too much time just trying to find the right data set or figuring out who owns it. This MCP changes that by connecting your AI agent directly to your Alation instance. You can ask natural language questions—like, 'Show me all tables related to Q3 sales figures'—and the system handles the complexity for you.

It lets you go beyond simple searches. Your agent can audit table schemas, trace data lineage back to its source, and even pull saved queries from Alation Compose. Everything is exposed through a clean chat interface managed by Vinkius. You get enterprise-grade data intelligence without needing specialized SQL knowledge or navigating dozens of dashboards.

Core Capabilities

01 — Search the Data Catalog

You can search across all your catalog data sources using keywords and advanced filters to locate relevant schemas, tables, and data assets.

02 — Inspect Object Metadata

Retrieve detailed information about any data object, including its official description, assigned data steward, or specific governance tags.

03 — Trace Data Lineage

Follow the path of your data. This capability shows exactly where a table originated and which downstream dashboards or systems rely on it.

04 — Audit Governance Fields

List and examine custom governance fields attached to catalog objects, helping you ensure compliance details are properly filled out.

05 — Query Saved SQL Results

List saved SQL queries and retrieve cached execution results from Alation Compose so you don't have to run the same report twice.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/alation** — connect your AI agent in three steps.

01 First, subscribe to this MCP on Vinkius. You'll need your specific Alation Instance URL and an API Access Token.

02 Next, connect your preferred AI client (like Cursor or Claude) using the credentials you entered. This links your agent to the entire Alation catalog.

03 Finally, just ask your agent a question—for example, 'What is the lineage for the Customer ID table?' The MCP uses its tools to pull the data and present the answer in conversation.

The bottom line is you talk to your AI client naturally, and it does the heavy lifting of querying and interpreting your complex data catalog structure.

Built For

This MCP is for anyone whose job involves understanding where data comes from or proving its trustworthiness. If you're tired of spending hours clicking through dashboards just to find a schema definition, this tool saves you time. Data Analysts and Engineers especially benefit from having instant access to lineage and metadata.

Data Analyst

You use this MCP to quickly search for relevant tables or schemas when building reports, eliminating guesswork about data location.

Data Governance Officer

You audit metadata completion and manage custom field values across the entire catalog to ensure compliance standards are met everywhere.

Software Engineer

You trace data lineage when implementing new features, ensuring that changes won't break downstream systems or reports.

What Changes When You Connect

01 Stop guessing where data lives. Use the `search_catalog` tool to instantly pinpoint schemas, tables, or entire sources using natural language prompts.

02 Eliminate manual metadata checks. With `get_object_metadata`, you can ask your agent for stewardship details and definitions on demand, ensuring compliance right away.

03 Understand data trust immediately. The `get_lineage` tool maps out the complete journey of any dataset, showing exactly what feeds into it or depends on it.

04 Save time running reports. You can use `list_saved_queries` to see past work and `get_query_results` to retrieve cached output without re-execution.

05 Maintain governance integrity by using the `list_custom_fields` tool, allowing you to audit specific compliance details attached to every data object.

Real-World Applications

A new analyst needs a report on customer churn rates.

Instead of asking a domain expert for the right table name, the agent uses `search_catalog` and identifies 'Customer Metrics'. The analyst then runs `get_lineage` to confirm that this dataset comes from the approved source system before building their dashboard.

The compliance team needs to prove data residency.

They instruct their agent to use `list_custom_fields` across all tables in the 'Production' schema. The agent audits every object, verifying that the required 'Jurisdiction Tag' field has been populated everywhere.

An engineer is modifying a core reporting dashboard.

They use the agent to run `get_lineage` on the key metric table. The output immediately warns them that three critical downstream dashboards ('Global Sales', 'Finance Forecast') depend on this data, preventing a major outage.

A BI lead wants to reuse last quarter's complex financial analysis.

Rather than recreating the query manually, they ask the agent to `list_saved_queries`. They find 'Q2 Revenue by Region', and with one prompt, retrieve its cached results using `get_query_results`.

Patterns to Avoid

Over-relying on basic SQL searches

✗ AVOID

Trying to manually track down the source of a column by running multiple, disjointed SELECT statements. This is slow and only tells you what's happening right now.

✓ INSTEAD

Use the agent to run `get_lineage` on that specific column name. It automatically maps the entire flow, showing the full history from the raw data source to the final report.

Ignoring governance definitions

✗ AVOID

Assuming a column is safe for use in an external system because it's easy to query. This ignores whether critical stewardship tags or custom fields are present.

✓ INSTEAD

Always check the object details using `get_object_metadata` before trusting the data, ensuring you know who owns it and what its purpose is.

Confusing source code with catalog assets

✗ AVOID

Attempting to manually list every schema or table by running generic commands. This misses context and governance details.

✓ INSTEAD

Start by letting the agent `list_data_sources`, then use it to systematically browse all schemas, tables, and columns in a guided manner.

The Right Fit

Use this MCP if your primary bottleneck is data discovery or governance auditing. If you need to know *what* data exists, *where* it came from, or *who* is responsible for it, this connector is essential. You should connect it when compliance requires tracking metadata completion (`list_custom_fields`) or when cross-departmental reporting relies on reliable historical queries (`get_query_results`).

Don't use this if your problem is simply running a single, isolated SELECT statement that you already know the exact table and column names for. In those cases, a simple database client might suffice. If you only need to check one schema without context, an ad-hoc tool might work. But when you need the full picture—the relationship between assets, their ownership, and their history—you need Alation MCP.

Alation MCP for AI Agents: Solving Data Discovery Pain Points

Right now, finding a specific data asset is a pain. You spend hours clicking through the UI, checking different tabs, and running disjointed searches just to figure out if 'Customer ID' means two different things in two different systems. It's manual, it's slow, and you often end up building reports on questionable, unverified sources.

With this MCP, that process disappears. You simply ask your agent for the data asset by name or function. The system uses its tools to search the catalog, audit metadata, and present a definitive list of options, saving you hours every single week.

Alation MCP for AI Agents: Mastering Data Lineage and Governance

Manually tracking data flow is nearly impossible. When a report breaks, figuring out which source table caused the failure—and who needs to fix it—

The agent handles this by tracing data lineage for you. You tell it the target table, and the MCP immediately maps its entire life cycle, showing all

is an archaeological dig involving emails and ticket systems.

upstream dependencies and downstream consumers instantly.

Alation MCP: 10 Tools for Metadata Management

Use these specific tools to search the catalog, retrieve object details, map data lineage, or audit governance fields through your agent.

#	TOOL	DESCRIPTION
01	`search_catalog`	Searches your entire catalog for specific data assets using keywords.
02	`list_data_sources`	Retrieves a list of all available data sources within the catalog.
03	`list_schemas`	Lists all schemas contained within a specific data source.
04	`list_tables`	Displays all tables associated with a selected schema.
05	`list_columns`	Provides an inventory of columns for a specified table.
06	`get_object_metadata`	Pulls detailed metadata, including descriptions and stewards, for any object in the catalog.
07	`list_saved_queries`	Shows a list of previously saved SQL queries stored in the system.
08	`get_query_results`	Fetches cached results from executed SQL queries, so you don't have to re-run them.
09	`list_custom_fields`	Lists and audits custom governance fields applied across the catalog objects.
10	`get_lineage`	Maps out data lineage, showing how a table is populated from its source systems.

See It in Action

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

U I need to know which systems feed into the 'Global Sales' dashboard.

Lineage Report: Global Sales Dashboard

This dashboard relies on three primary data feeds:

- `Sales_Transactions`: Primary source, last updated 2026-06-12.
- `Regional_Adjustments`: Used for currency conversion.
- `Product_Master`: Provides current product taxonomy.

Next Steps: Would you like me to audit the governance metadata for any of these three sources?

U Show me all tables that contain customer PII and are marked as sensitive.

Sensitive Data Audit Results

The following 4 tables were found matching both 'PII' keywords and the 'Sensitive' custom governance tag:

TABLE NAME	SCHEMA	STEWARD	LAST AUDITED
`customer_master`	Prod	Alice K.	2026-05-01
`user_login_history`	Audit	Bob L.	2026-06-10
`billing_details`	Finance	Carol R.	N/A

Note: The 'billing_details' table requires an immediate steward assignment.

U List the saved queries and pull the results for the one that checks user signups.

Query Retrieval Report

Found 12 saved SQL items. Here are your recent ones:

- `Monthly Churn Report` (Last run: yesterday)
- `Revenue by Region` (Last run: week ago)
- `Active User Audit` (Saved for Signups):

Cached Results for 'Active User Audit':

```json
[{"date": "2026-06-11", "count": 1450}, {"date": "2026-06-12", "count": 1610}]
```

The results show a steady growth in active users.

Frequently Asked Questions

01 **How does the Alation MCP help me find data I need for reporting?**

It turns searching into conversation. Instead of sifting through endless UI menus, you ask your agent what you need (e.g., 'sales figures') and it uses its tools to pinpoint all relevant tables and sources in the catalog.

02 **Can I use Alation MCP to check if my data is compliant?**

Yes. You can audit metadata completion by listing custom fields or getting object details, letting you confirm that required governance tags are applied before publishing reports.

03 **What if I need to know where a specific column of data came from?**

You use the lineage tool. It traces the entire journey of that single column, showing every source table and system it passed through—it's like seeing the full pedigree.

04 **Does Alation MCP save me time running reports?**

Yes. You can list saved SQL queries and retrieve cached results. This means if you ran a complex report yesterday, you don't have to re-run the query; your agent just pulls the old numbers for you.

05 Is Alation MCP only for data engineers?

No. While it’s powerful for engineers, analysts use it constantly. You can search and audit metadata simply using natural conversation, making complex governance tasks accessible to everyone.

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 `"alation": { "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

Alation 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 Alation. 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	June 2026
MCP Server	Alation MCP
Server ID	`019d754b-934c-72da-837c-f7e53c9a9d7c`
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/mcp/alation.