

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

Sigma Computing MCP for AI Agents

Map your BI workbook metadata and data lineage without clicking through dashboards.

Sigma Computing MCP lets your AI agent navigate your BI environment. It pulls workbook lists, maps out data connections, and audits team structures without you having to click through the web UI. It's designed for teams who need to see their data landscape clearly.

A+ Quality Score 100/100

data-lineage

workbook-management

cloud-bi

data-stewardship

analytical-metadata

database-integration



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.

Sigma Computing MCP

7 tools available

Cloud-hosted on Vinkius

Sigma Computing MCP gives your AI agent a direct line into your organization's data analytics metadata. Instead of hunting through heavy browser tabs to find which workbooks belong to a specific department or figuring out which datasets power a dashboard, you can just ask your agent. It acts like a data steward that knows where everything lives. You can see the connections between your Snowflake or BigQuery sources and the final reports they feed into. It's a huge time saver when you're trying to map out data lineage or find out who owns a specific set of analytics. If you're looking for a way to make your BI environment more searchable, this is how you do it. It fits right into your workflow on Vinkius, making it easy to keep your data governance on track. You can get a full inventory of workbooks or see every team in your organization with a single prompt. This takes the manual work out of auditing your BI stack.

Core Capabilities

01 — List all workbooks

Get a full inventory of every workbook in your Sigma organization.

02 — Audit data connections

See every backend data source connection configured in the platform.

03 — Map dataset lineage

Identify which datasets are available across your entire organization.

04 — Track team structures

See every team and member within your Sigma organization.

05 — Drill into workbook pages

View the specific pages contained within a single workbook.

06 — Inspect workbook details

Pull specific metadata for a single workbook.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/mcp/sigma-computing — connect your AI agent in three steps.

- 01 Add your SIGMA_CLIENT_ID and SIGMA_CLIENT_SECRET to your environment variables.
- 02 Connect the Sigma Computing MCP through the Vinkius catalog to your agent.
- 03 Ask your agent to find specific workbooks, teams, or data connections.

The bottom line is you get instant visibility into your BI metadata without opening a browser.

Built For

Data engineers and BI analysts who are tired of manual metadata audits and searching through hundreds of dashboards to find the right data source.

Data Steward

Audits team structures and dataset permissions to ensure company compliance.

BI Analyst

Finds existing workbooks and pages to avoid duplicating work on a Tuesday afternoon.

Data Engineer

Maps out backend connections to understand how data flows into the BI layer.

What Changes When You Connect

- 01 Stop hunting for reports. Use `list_workbooks` to get a complete inventory of every workbook in seconds.
- 02 Audit your data sources quickly. `list_connections` lets you see every backend pipe without digging into settings.
- 03 Map your data lineage easily. Use `list_datasets` to see the building blocks of your entire analytics stack.

04 Manage your team topology. `list_organization_teams` and `list_organization_members` give you a bird's eye view of your users.

05 Save time on report audits. Use `get_workbook_details` and `list_workbook_pages` to see report content instantly.

Real-World Applications

Audit Data Lineage

A data engineer needs to see where a specific report gets its data. They ask the agent to list all datasets and connections to find the source.

Report Discovery

An analyst wants to see if a North America report already exists. They use `list_workbooks` to check the current inventory.

Team Onboarding

A manager wants to know who is in the Marketing team. The agent uses `list_organization_teams` and `list_organization_members` to provide a list.

Metadata Extraction

A developer needs to know how many pages are in a specific workbook. They use `list_workbook_pages` to get the count.

Patterns to Avoid

Trying to edit data

✗ AVOID

Users might think they can write data to the database.

✓ INSTEAD

This MCP is for reading metadata, not for editing records. Use it to find the workbooks and datasets, not to modify the rows.

Searching for specific rows

✗ AVOID

Asking the agent to find a specific customer's revenue.

✓ INSTEAD

This tool doesn't query the actual data in your tables. Use it to find the workbooks and datasets that contain that information.

Manual clicking

X AVOID

Opening 10 tabs to find one database connection.

✓ INSTEAD

Use `list_connections` to see everything at once instead of clicking through several different menus.

The Right Fit

Use this if you need to audit your BI environment, map out data lineage, or manage team structures in Sigma Computing. It's perfect for data stewards and engineers who need to see the big picture of what's built. It helps you find existing reports and see how they connect to your backend sources like Snowflake or BigQuery. Don't use this if you need to run SQL queries against your actual production data or if you need to create new workbooks. This MCP is for reading metadata, not for active data manipulation. If you need to write data or perform complex queries on specific rows, you'll need a different tool that interacts with your database directly. This tool is about visibility and organization, not execution.

Sigma Computing MCP for BI Metadata Audits

Right now, finding out which workbooks are actually used or which datasets power them involves a lot of manual clicking. You have to open your browser, navigate through heavy dashboards, and keep tabs open just to see what's connected to what. It's a slow process that makes data lineage hard to track.

This MCP changes that by letting your agent do the heavy lifting. You can just ask for a list of all workbooks or see every connection in your organization instantly. You get a clear map of your data stack without ever opening a browser tab.

Sigma Computing MCP for Data Lineage Mapping

Mapping out how data flows from a source like Snowflake into a final report usually requires manual documentation. You have to cross-

You can now automate this. Your agent can pull all connections and datasets to show you exactly how

reference connections, datasets, and workbooks one by one to build a map that's actually accurate.

your data moves. It turns a multi-hour audit into a few seconds of conversation.

Sigma Computing 7-Tool BI Metadata Explorer

Use these tools to list workbooks, map data connections, and audit your organization's team structure.

#	TOOL	DESCRIPTION
01	get_workbook_details	Retrieves details for a specific workbook. Use this to see the metadata of a single report.
02	list_workbook_pages	Lists all pages within a specific workbook. This shows you the layout of a specific report.
03	list_connections	Lists data source connections configured in Sigma. Use this to see what databases are linked.
04	list_organization_members	Lists all users in the Sigma organization. This gives you a full view of your user base.
05	list_organization_teams	Lists all teams in the Sigma organization. This helps you see how the company is structured.
06	list_datasets	Lists all datasets available in the organization. Use this to find the raw data building blocks.
07	list_workbooks	Lists all workbooks in the Sigma organization. This helps you see every available report at once.

See It in Action

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

U Show me all the workbooks we have for the sales team.



Sales Team Workbooks

I found the following workbooks associated with the sales department:

WORKBOOK NAME	WORKBOOK ID
Q3 Sales Performance	wb_9921
Regional Revenue Map	wb_8832
Lead Conversion Tracker	wb_7741

Would you like to see the specific pages for any of these?

U Who are the members of our data engineering team?



Data Engineering Team

The following members are currently assigned to the **Data Engineering** team:

- Alex Rivera
- Jordan Smith
- Casey Chen
- Morgan Lee

There are **4** members total in this group.

What datasets are currently available in our organization?



Available Datasets

I've pulled the full list of datasets available in your Sigma organization:

- **Marketing_Leads_Master**
- **Finance_Quarterly_Actuals**
- **Product_Inventory_Sync**
- **User_Engagement_Metrics**
- **Churn_Risk_Score_v2**

Let me know if you'd like to see which workbooks depend on a specific one.

Frequently Asked Questions

01 Can the Sigma Computing MCP help me find specific reports?

Yes, it lists all workbooks so you can see what's already built. This helps you identify existing reports quickly without browsing every dashboard manually.

02 How do I see what databases are connected to Sigma?

You can ask the agent to list all your data source connections. This provides a clear view of every backend pipe linked to your BI platform.

03 Can I use this to see who is in my organization?

Yes, it lists all members and teams within your Sigma account. This is great for getting a bird's eye view of your user base and team structures.

04 Does the Sigma Computing MCP show me the actual data in my tables?

No, it only shows metadata like workbooks and datasets. It's designed for exploring the structure of your BI environment rather than querying individual rows.

05 Can I use this to map out our data lineage?

Yes, it helps you see the connection between sources, datasets, and reports. You can use it to audit how data flows from your backend into your final dashboards.

06 How does this help with data governance?

It helps with governance by providing a fast way to audit your entire BI environment. You can quickly verify which teams have access and what datasets are being used.

07 Can the integration forcefully modify datasets or override workbook queries directly?

No. By structured intent, this module is strictly bounded as an observational and auditing matrix targeting specifically organizational discovery heavily optimized securely natively. Explicit write protocols structurally enabling queries, mutation mappings, or data modifications systematically inherently simply completely systematically bypassed unconditionally directly universally.

08 Why construct this manually over leveraging the standard platform web UI interfaces?

The native IDE integration context decisively grants explicitly your agent prompt active unadulterated runtime authority seamlessly querying real-time underlying arrays dynamically without latency immediately directly mapping structurally uniquely native taxonomies avoiding graphical interface lags flawlessly intrinsically seamlessly definitively completely.

09 Does my client credentials require explicit specific elevated Admin privileges exclusively natively?

Yes explicitly securely seamlessly thoroughly definitively successfully extensively confidently conclusively exactly absolutely entirely solidly reliably exactly correctly perfectly. Creating API keys unequivocally cleanly exactly simply strongly thoroughly decisively distinctly clearly strictly conclusively intrinsically locally essentially requires inherently specifically explicit Administrative credentials securely internally distinctly correctly clearly deeply directly exclusively purely successfully thoroughly fully permanently precisely cleanly comprehensively successfully locally correctly definitively safely reliably directly cleanly seamlessly successfully seamlessly efficiently essentially firmly seamlessly inherently strictly smoothly uniquely.

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>"sigma-computing": { "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

Sigma Computing 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 Sigma Computing. 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	July 2026
MCP Server	Sigma Computing MCP
Server ID	019d7607-ef5a-72e7-a501-546c2cb1718c
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/mcp/sigma-computing.