MCP SERVER | NO CODE | CLOUD HOSTED

Atlan MCP for AI Agents

Discover and Govern Enterprise Data Assets & Business Glossaries

Atlan MCP connects your AI agent directly to the Atlan Data Catalog, turning metadata discovery and governance into a conversation. Your agent can search thousands of data assets, verify business terms from organizational glossaries, and check data sensitivity classifications (like PII) instantly—all without you having to click through dozens of dashboards.

F Quality Score 3.6/100

metadata-management | data-governance | data-catalog | business-glossary | data-stewardship | asset-discovery

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

SCAN TO VIEW

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.

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.

Atlan MCP

6 tools available
Cloud-hosted on Vinkius

Atlan MCP lets your AI client become a master data steward for your organization. Instead of manually logging into different systems just to figure out where a piece of data lives or what it means, your agent handles the heavy lifting. It connects conversational governance and instant cataloging directly into your workflow. By subscribing through Vinkius, you give your AI agent deep context about every table, column, and business definition across your entire data estate.

Your agent can locate assets using natural language search, retrieve verified terms from internal glossaries, or list active security tags like Confidentiality or GDPR compliance. It's governance on demand. You'll stop wasting time hunting down the right dataset and start working with trusted information.

Core Capabilities

01 — Search Across Data Assets

Find any data asset, whether it's a table, dashboard, or column, by querying its name or topic directly.

02 — Verify Business Definitions

Retrieve comprehensive organizational glossaries that hold verified business terms and acronyms used company-wide.

03 — Check Data Policies and Tags

List all configured data classifications (like PII) or review the sharing policies applied across your datasets.

04 — Inspect User Roles and Access Rights

View registered users in the workspace and check the specific access control profiles assigned to different business roles.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this secure MCP connection on Vinkius.

02 Provide your Atlan API URL and corresponding API Key credentials.

03 Start talking to the catalog via any compatible AI client, letting your agent do the searching and governance work.

The bottom line is that your AI client talks to the metadata layer directly, giving it full visibility into what data exists, who owns it, and how sensitive it is.

Built For

This MCP is essential for any role drowning in enterprise data complexity. If you're a Data Analyst tired of guessing which dataset to use, or a Governance Specialist who spends all day auditing metadata tags, this tool gives your agent the institutional knowledge it needs.

Data Steward

Auditing metadata completeness and systematically checking for PII tags and glossary consistency across different data sources.

Data Analyst

Quickly discovering the right verified tables or dashboards by asking natural questions, instead of manually browsing the catalog.

Security Architect

Inspecting broad access personas and data-sharing purposes to ensure compliance with internal policies before a new project begins.

What Changes When You Connect

01 Find the right data without clicking through menus. Use `search_assets` to query your entire connected data ecosystem using plain text, instantly revealing lineage and trusted datasets.

02 Stop arguing over definitions. The agent uses `list_glossaries` to pull verified business terms and acronyms from organizational glossaries, ensuring everyone speaks the same technical language.

03 Stay compliant by design. You can call `list_classifications` to see every active data tag (like PII or Confidential) applied across your assets, guaranteeing proper handling.

04 Understand who sees what. By running `list_personas`, you get a clear map of configured access control profiles, allowing security teams to audit permissions quickly.

05 Improve trust in the data by listing all defined sharing purposes (`list_purposes`), showing exactly why and how your data can be used.

Real-World Applications

A new project needs a reliable KPI definition

Instead of asking five different domain experts, the analyst asks their agent to check for verified business terms. The agent uses `list_glossaries` and immediately returns the official definition and owner for 'Monthly Recurring Revenue,' solving weeks of debate in minutes.

Preparing for a compliance audit

The security officer asks their agent to list all data classifications. The agent uses `list_classifications` and confirms that every asset containing customer names is tagged as 'PII,' generating an immediate, auditable report.

Finding the source of truth for a dashboard

A data scientist needs to know which tables feed the executive summary dashboard. They ask the agent to search assets, and it uses `search_assets` to trace the lineage back to the original production schema, identifying the authoritative source.

Onboarding a new team member

The manager needs to know who has access to sensitive HR data. They ask the agent to list all users and then check the relevant Personas using `list_personas`, giving an immediate overview of role-based permissions.

Patterns to Avoid

Searching for assets manually

✗ AVOID

A user has to navigate through the Atlan UI, clicking into 'Tables', then filtering by 'Owner,' and finally using a search bar. This takes too much time.

✓ INSTEAD

Just ask your agent: 'Show me all tables owned by Marketing related to Q3 sales.' The agent uses `search_assets` and instantly pulls the results without any clicks.

Assuming definitions are consistent

✗ AVOID

Two teams use different internal definitions for 'Customer Lifetime Value' because they aren't checking the central repository.

✓ INSTEAD

Ask your agent to run `list_glossaries`. It immediately provides the single, verified definition used across the entire organization.

The Right Fit

Use this MCP if your primary pain point is understanding *what* data exists and *how* it should be treated. You need conversational access to metadata—for example, you must use `list_classifications` when compliance tags are the core issue. However, don't rely on Atlan for running complex SQL queries or performing ETL transformations; this MCP only handles discovery and governance information. If your goal is pure code execution, look for a different type of integration that focuses on runtime actions rather than metadata context.

Atlan MCP: Solving Data Discovery Pain with Atlan's Metadata Catalog

Today, finding the right data is a manual nightmare. You start by knowing what you need—say, customer retention metrics—but then you waste hours clicking through multiple

With this MCP, your AI agent takes over the detective work. You simply ask it to search for assets related to 'customer retention.' It uses `search_assets` across the whole catalog,

departmental dashboards and disparate databases just to find out which schema has the most reliable version of that metric.

returning a list of all potential sources—tables, dashboards, and glossaries—and tells you exactly where to look.

Atlan MCP: Governing Data Assets with Atlan's Business Glossaries

The biggest risk isn't finding the data; it's trusting its definition. Often, different teams use different terms for the same concept—one calls it 'Active Users,' another calls it 'Monthly Active Count.' This ambiguity breaks every report.

This MCP solves that by giving your agent access to verified business terms. It uses `list_glossaries` to pull up the single source of truth, ensuring every person working with the data is using the exact same definition.

6 Atlan Tools for Data Discovery & Governance

Use these tools to search for assets, list classifications, check user roles, or retrieve verified business terms from the data catalog.

#	TOOL	DESCRIPTION
01	`search_assets`	Searches the entire Atlan Data Catalog for specific data assets by name or keyword.
02	`list_glossaries`	Retrieves a list of all business glossaries defined within your organization's metadata.
03	`list_classifications`	Lists every active data classification tag, such as Confidential or PII, configured in Atlan.
04	`list_purposes`	Shows all defined sharing purposes and policies for your data assets within the platform.
05	`list_personas`	Retrieves a list of configured access control profiles, known as Personas, used in Atlan.
06	`list_users`	Lists all individual users registered within the Atlan workspace.

See It in Action

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

U What are the most sensitive types of data we have?

Data Sensitivity Report

We currently have 7 active classification tags applied across our assets. These dictate how the data must be handled:

- 🛡️ **PII:** Personal Identifiable Information (High Risk)
- 🔒 **Confidential_Tier_1:** Internal use only, restricted access.
- 🌐 **Public_Domain:** Safe for external reporting.

If you want to check which tables contain PII specifically, let me know.

U List all the official business metrics we use?

Verified Business Glossaries

Our organization maintains 4 primary active glossaries. These define our core KPIs and concepts:

- `Core Finance KPIs` : Defines 'EBITDA' (Earnings Before Interest, Taxes, Depreciation, and Amortization).
- `Marketing Attribution Rules` : Provides the official definition for 'First Touch Conversion.'
- `Engineering Data Contracts` : Specifies how data fields should be named.
- `Regulatory Policies` : Tracks definitions related to regional compliance mandates.

U Who has access to the executive dashboard?

Access Profile Summary

The following Personas are currently configured for high-level visibility:

- `Executive Tier` : Read-only access across all core dashboards.
- `Data Steward` : Full metadata read/write rights, limited data access.
- `Finance Analyst` : Limited to Finance schemas and reporting tools.

You can see the full list of users under the `list_users` tool if needed.

Frequently Asked Questions

01 **How does Atlan MCP help me find data assets I don't know exist?**

It acts like a universal search engine for your entire company data catalog. Instead of guessing names, you ask your agent a question about the business problem, and it uses `search_assets` to surface every potential dataset that matches the context.

02 **I need to know if my data is compliant; can Atlan MCP check classifications?**

Yes. Your agent runs classification checks by listing all tags (like PII or GDPR). This gives you a clear, auditable view of your compliance posture across the entire estate.

03 **What is the difference between Atlan MCP and just using an internal wiki?**

A wiki only stores text; this MCP connects to live metadata. It doesn't just tell you *what* a term means, it tells you *where* that term is used in actual production tables and dashboards.

04 **Can Atlan MCP help me understand the company's official metrics?**

Absolutely. It accesses your business glossaries via `list_glossaries`. This means you get the single, verified definition for any KPI—like 'Net Revenue' or 'Churn Rate'—so everyone is on the same page.

05 **I need to know which teams can use a specific dataset. Can Atlan MCP check access rights?**

Your agent lists configured Personas and users, showing you exactly what roles exist and what level of access they have been granted across your catalog.

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 `"atlan": { "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

Atlan 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 Atlan. 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	Atlan MCP
Server ID	`019d7554-2193-7133-bdf0-f6b5371dab72`
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/atlan.

© 2026 Vinkius · vinkius.com · support@vinkius.com