MCP SERVER | NO CODE | CLOUD HOSTED

Collibra MCP for AI Agents

Managing Data Assets and Governance Policies Across Your Enterprise

Collibra MCP connects your AI agent directly to the Collibra data intelligence platform. It lets you search, inspect, and manage an organization's entire data catalog via natural language conversation. You can retrieve metadata for specific assets, list all available communities, or even create new data records without needing to navigate complex UIs.

A+ Quality Score 100/100

data-governance | metadata-management | data-catalog | compliance | data-assets | enterprise-data

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

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.

Collibra MCP

10 tools available
Cloud-hosted on Vinkius

Collibra helps organizations build trust in their data by providing a centralized intelligence platform. With this MCP, your AI agent gets direct access to that deep catalog knowledge. Instead of spending hours clicking through dozens of tabs just to find out who owns 'Customer ID' or what classifications it has, you ask the question and get an answer instantly. You can list all domains, check asset relationships, or pull up detailed governance policies for any piece of data. This capability means data stewards and compliance teams operate faster, making manual audits a thing of the past. Vinkius hosts this MCP, giving your AI client access to Collibra's full suite of tools right alongside other enterprise services.

Core Capabilities

01 — Search and Retrieve Metadata

Finds data assets by name, type, or domain and pulls all associated metadata into conversation.

02 — Map Organizational Structure

Lists all communities and domains to provide a comprehensive view of the entire governance hierarchy.

03 — Inspect Asset Details

Retrieves full attributes, ownership roles, and relationships for any specific data asset identifier.

04 — Create New Data Assets

Allows the agent to programmatically generate a new record in the Collibra catalog when needed.

05 — List Available Domain Types

Provides an exhaustive list of classification standards, ensuring data is categorized correctly upon creation or review.

One Click on Vinkius — From Prompt to Execution

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

01 First, add the Collibra integration to your AI client's toolset and provide the required instance details.

02 Next, tell your agent what you need. You can ask it to search for a specific asset or list all available communities using plain language.

03 The MCP executes the request against the data platform and sends back structured metadata, which your agent then presents in conversational format.

The bottom line is that your AI client treats the complex data catalog like a simple search engine, giving you instant answers instead of endless clicks.

Built For

This MCP is built for anyone who spends time in data governance. Think Data Stewards manually checking ownership records or Compliance Officers trying to track down a single policy across dozens of systems. It’s for the people tired of spending half their day just *finding* what they need.

Data Steward

Uses the MCP to find and inspect asset metadata, quickly verifying ownership and classification details without navigating deep into the main Collibra UI.

Data Engineer

Leverages the tool to look up table or column definitions and determine data ownership directly through chat conversations while building pipelines.

Compliance Analyst

Verifies data classifications, governance policies, and asset relationships across different communities to prepare for audits much faster than manual checks allow.

What Changes When You Connect

01 Saves time on audits: Instead of navigating complex UI paths to verify data lineage, you can use the agent to check specific asset relationships instantly.

02 Quickly understand ownership: Use the tool to retrieve detailed information about any single asset, immediately showing who is responsible for it and what its attributes are.

03 Map your entire structure: You can list all communities and domains, giving you a high-level view of where data assets reside without needing administrative access to every section.

04 Automate documentation: Easily look up table/column definitions or ownership from chat. Data engineers get actionable metadata instantly, speeding up development time.

05 Build new records fast: Need to log a new piece of governed data? The `create_asset` tool lets you programmatically add assets without manual form filling.

Real-World Applications

Checking compliance status for sensitive data

A Compliance Analyst needs to prove that all 'PII' assets are correctly classified. The agent uses the tool to retrieve detailed information about specific assets, verifying their assigned governance policies and relationships against regulatory standards.

Discovering unknown data sources for a project

A Data Engineer starts a new model and needs input tables. They ask the agent to list all available assets in 'Data Engineering' community, narrowing down potential sources without manually browsing hundreds of entries.

Structuring an internal data governance wiki

A Data Steward wants to document best practices for a new department. They use the tool to list all domains and communities available in Collibra, creating a structured map that guides future users on where to store governed knowledge.

Validating data definitions before deployment

A team needs to ensure two separate tables both refer to the same 'Customer ID' definition. They use the agent to get asset details for both, instantly confirming they share consistent attributes and responsibilities.

Patterns to Avoid

Assuming a single search works

✗ AVOID

Trying to find all assets related to 'Customer' using only the name search will miss assets that are classified under different domains but share keywords.

✓ INSTEAD

For comprehensive searches, first use `list_communities` and then guide your agent to run targeted queries or use `search_assets` combined with community context.

Manually updating records

✗ AVOID

A steward manually logging a new asset into the system because they forget which tool to use, leading to incomplete metadata.

✓ INSTEAD

Use the `create_asset` tool. This method ensures that when you add a record, it is automatically logged and structured correctly within Collibra's governance model.

Ignoring asset types

✗ AVOID

Running a general listing of assets without knowing if the results include policies, tables, or business terms. The output becomes overwhelming.

✓ INSTEAD

Always start by calling `list_asset_types` to understand the scope and categories available. This helps you filter your subsequent requests for precision.

The Right Fit

Use this MCP if your primary need is understanding data context, ownership, or compliance status within a defined catalog structure. You want an AI agent to talk to your metadata layer—that's what it does best.

Don't use this if you are trying to perform actions outside of the existing Collibra framework, like migrating data between systems or running complex ETL jobs. For those tasks, you need a dedicated integration for workflow orchestration, not just catalog viewing.

If your goal is merely to write documentation that *describes* governance processes without querying actual asset details, this MCP might be overkill. But if you need the agent to verify data classifications using `get_asset` or map out domain relationships using `list_domains`, then this is exactly what you need.

Collibra: Centralizing Data Governance Metadata with Collibra

Today, data governance professionals waste huge amounts of time. They have to jump between the main UI, domain dashboards, and separate compliance reports just to build a complete picture of where sensitive information lives. It's slow, it involves copying attributes from one screen to another, and you almost always end up missing key relationships.

With this MCP, your AI agent becomes the centralized dashboard. Instead of navigating five different tabs to check ownership, you simply ask: 'Who owns the customer data in the Compliance community?' The tool returns the answer immediately, giving you a single source of truth right where you're working.

Collibra: Improving Data Asset Discovery via Collibra

Before this MCP, finding assets meant running multiple searches by name and type, often getting conflicting results. You had to manually cross-

Now you can ask your agent to list all available asset types or search for a dataset simply by its conceptual name. The result is not just a file name;

reference lists of domains and communities just to understand the data's scope.

it’s a structured, actionable piece of metadata that tells you exactly what the data is used for.

Collibra: 10 Tools for Managing Data Assets & Governance Metadata

Use these tools to search the catalog, list structures, create new records, and retrieve detailed governance information about your data assets.

#	TOOL	DESCRIPTION
01	`create_asset`	Creates a new record for a data asset within the Collibra catalog.
02	`get_asset`	Pulls all detailed information regarding one specific, known data asset.
03	`get_community_details`	Retrieves comprehensive details for a single, identified community within the platform.
04	`list_asset_types`	Returns an exhaustive list of all types of assets available in the system.
05	`list_assets`	Generates a full listing of data assets across the entire catalog.
06	`list_communities`	Provides a list of all organizational communities available in Collibra.
07	`list_domain_types`	Returns an exhaustive list of all types of data domains that can be used for classification.
08	`list_domains`	Generates a full listing of all organizational domains within the platform.
09	`list_statuses`	Provides a list of all available status tags that can be applied to data assets.
10	`search_assets`	Searches for metadata about multiple assets based only on the asset's name.

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 top 3 communities and how many assets are in each?

Data Catalog Summary

Here's a breakdown of the largest communities:

1. **Engineering:** (15 Domains, 1,204 Assets)
Focus: Raw data pipelines and ETL definitions.
2. **Business Intelligence:** (8 Domains, 532 Assets)
Focus: Reporting layers and aggregated metrics.
3. **Data Governance:** (12 Domains, 845 Assets)
*Focus: Policy documents and business terms.

You can dive deeper into any of these domains.

U Show me the owner and classification for 'Customer Transaction History'.

Asset Details Found

FIELD	VALUE
Name	Customer Transaction History
Domain	Financial Data
Owner	Jane Doe (jane.doe@corp.com)
Classification	Restricted - PII/PCI

This asset belongs to the Finance community and must adhere to PCI-DSS guidelines.

U I need a list of all possible data domain types we use.

Available Domain Types:

The system supports these classifications:

- **Customer Identity**: For all PII related assets.
- **Financial Metrics**: Assets tied to revenue, costs, and budgets.
- **Operational Logs**: Data from application usage and activity tracking.
- **Product Inventory**: Cataloging physical or digital goods.

These types help keep our data governance consistent across the enterprise.

Frequently Asked Questions

01 **How does Collibra MCP help me find data ownership?**

It quickly finds and reports the owner (Data Steward) for any asset you reference. You no longer have to hunt through departmental contacts; the metadata gives you a direct answer, saving hours of manual investigation.

02 **Can I use Collibra MCP to map out my entire data structure?**

Yes. By listing all available communities and domains, your agent provides a clear, high-level map of the entire data catalog. This is vital for understanding scope before starting any major project.

03 **Is Collibra MCP useful for compliance audits?**

Absolutely. It allows you to verify specific asset classifications and relationships instantly, providing auditable proof that governance policies are consistently applied across your data assets without manual checks.

04 **What if I need to add a new data asset record?**

You can use the MCP to create new records directly in Collibra. This means you don't have to manually fill out forms; your agent handles the structured entry, keeping your catalog clean and up-to-date.

05 **Can I search for data assets using natural language?**

Yes. You just ask your AI agent what you're looking for—by name or type—and it translates that into a metadata query, bringing the relevant results to you in plain conversation.

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 `"collibra": { "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

Collibra 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 Collibra. 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	Collibra MCP
Server ID	`019d7577-aeba-72e9-84b9-c80a40d71660`
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/collibra.