MCP SERVER | NO CODE | CLOUD HOSTED

DataRobot MCP for AI Agents

Monitor Model Performance and Audit ML Deployments

DataRobot MCP manages your entire automated machine learning lifecycle from natural language prompts. Use this connector to monitor live model performance, audit complex projects, track deployments across cloud environments, and extract raw metrics directly through any AI client.

A+ Quality Score 100/100

automl | ml-lifecycle | model-deployment | predictive-analytics | model-monitoring | data-science

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

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.

DataRobot MCP

6 tools available
Cloud-hosted on Vinkius

Need full visibility into your AutoML workflows? This DataRobot MCP lets you manage the complete machine learning lifecycle using simple conversation with your preferred agent. You stop clicking through dashboards just to check a metric or verify a deployment status. Instead, you simply ask your AI client to perform an audit, and it pulls real-time data right into the chat. Whether you're comparing training metrics across several models or checking which components are running in production, you get definitive answers instantly. Because Vinkius hosts this DataRobot MCP within its catalog, you can connect once from any compatible agent (Claude, Cursor, etc.) and gain access to all your ML governance tools without needing multiple integrations. This connector provides the full control required for rigorous data science operations.

Core Capabilities

01 — Audit DataRobot Projects

List and retrieve specific nested elements across projects in your workspace.

02 — View Machine Learning Models

Get a list of available models or inspect the details of a specific model within a project.

03 — Check Current Deployments

List and review global configurations for DataRobot nodes deployed into scalable cloud environments.

04 — Inspect Datasets and Metrics

View available datasets or retrieve raw metrics from completed data extractions.

05 — Monitor ML Configurations

Audit specific model versions and AI configurations stored on your platform for governance checks.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your DataRobot API Key and Endpoint URL (found in Profile > API Keys).

02 Connect the credential set to any MCP-compatible client, like Claude or Cursor.

03 Ask your agent a natural language question, such as 'List all active deployments running on AWS.' The data appears instantly.

The bottom line is you manage complex AutoML workflows and governance tasks using conversational prompts instead of navigating multiple web UIs.

Built For

This MCP targets data platform teams, ML engineers, and senior data scientists who are tired of manually switching between the DataRobot console, dashboard tools, and documentation. If your job involves auditing model health or ensuring compliance across multiple deployed models, this is for you.

ML Engineer

Verifies AI configurations and audits deployments in real-time using natural language prompts to ensure production readiness.

Data Scientist

Compares training metrics across multiple experimental models or quickly retrieves discrete logical properties during the prototyping phase.

MLOps Architect

Monitors project-wide dataset usage and tracks model metadata to maintain an organization's ML governance standards.

What Changes When You Connect

01 Audit model performance instantly. You can ask the agent to retrieve raw training metrics or compare validation scores across multiple models using `get_model` without leaving your chat interface.

02 Manage deployments from a single source. Use `list_deployments` to intercept and trace global configurations for every DataRobot node deployed into scalable clouds, keeping your production stack visible.

03 Maintain full project visibility. Quickly identify physical boundaries within your workspace by listing nested elements using `get_project`, simplifying governance audits.

04 Streamline data lineage checks. Use `list_datasets` to inspect which raw metrics are executing global data extractions, ensuring models rely on mapped and secure sources.

05 Simplify lifecycle oversight. The MCP allows you to audit specific model versioning and AI configurations stored directly in your platform by monitoring the ML lifecycle.

Real-World Applications

Auditing Model Drift Before Production

An engineer needs to verify if a new model deviates from historical performance. They ask the agent to use `get_model` on the staging environment's latest build, instantly getting raw metrics and comparison scores without logging into the dashboard.

Inventorying All Live ML Services

A platform team needs a count of every running service. They instruct their agent to use `list_deployments`, receiving an immediate, structured list of all active nodes and where they are operating (e.g., AWS, Azure).

Understanding Project Scope Boundaries

A data scientist is unsure which datasets a project relies on. They prompt the agent to `list_datasets` for that project, immediately seeing all mapped sources and their logical boundaries.

Patterns to Avoid

Ignoring deployment status

✗ AVOID

Assuming all deployed models are healthy because they were configured last week. Checking manually requires clicking into multiple cloud consoles.

✓ INSTEAD

Use the MCP to run `list_deployments`. This tool provides a centralized view of active nodes and their current health status across your scaled clouds.

Confusing datasets with projects

✗ AVOID

Thinking that just because a project exists, all its underlying data sources are visible. You might miss deprecated or unmapped source metrics.

✓ INSTEAD

Always run `list_datasets` to get an accurate inventory of every dataset mapped to your workspace and understand the physical boundaries.

The Right Fit

Use this MCP if you need deep, operational visibility into deployed ML systems. Specifically, if tracking model performance metrics, auditing configuration versions, or managing multi-cloud deployments is part of your daily job, this connector works for you. Don't use it if your primary need is just initial data cleaning; that requires a dedicated ETL tool. If you only need to view static, completed training results and never worry about deployment status or version control, the complexity might be overkill. This MCP provides MLOps governance at scale.

DataRobot MCP: Centralized ML Model Performance Auditing

Today, checking an active model's performance is a mess of tabs and copies. You have to log into the console, navigate to the specific project, find the model version, drill down into validation scores, and then copy those raw metrics into a spreadsheet for comparison. It's slow, prone to human error, and you often lose context across different deployment stages.

With this MCP, the process changes entirely. You just ask your agent to compare models. The connection handles the retrieval of detailed performance reports using `get_model`, presenting structured comparisons instantly in text format. You get a clean, actionable audit trail without ever opening the DataRobot UI.

DataRobot MCP: Governing Dataset Lineage and Deployment Status

Manually verifying data sources is risky business. Teams often struggle to prove exactly which version of a dataset (and what its physical boundaries are) was used for a model that went live six months ago, making compliance audits nearly impossible.

This MCP fixes the governance gap. You can ask the agent to `list_datasets` and map out all available sources or audit deployments using `list_deployments`. Now you have an always-up-to-date, auditable record of your entire ML asset inventory.

6 Tools for DataRobot Project & Dataset Auditing

Use these tools to list projects, check dataset boundaries, retrieve specific model metrics, or monitor live deployment status in conversation.

#	TOOL	DESCRIPTION
01	`list_projects`	Retrieves a list of all projects available in your DataRobot workspace.
02	`get_project`	Fetches detailed information about a specific project ID within the system.
03	`list_models`	Lists all machine learning models associated with a given project.
04	`get_model`	Retrieves full performance metrics and details for a single, specified model.
05	`list_deployments`	Provides an inventory of currently deployed DataRobot nodes and their status.
06	`list_datasets`	Lists all datasets that are mapped or available for use in your projects.

See It in Action

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

U Show me the top three models for my fraud detection project and their recent validation scores.

Model Performance Report: Fraud Detection

MODEL NAME	VALIDATION SCORE	STATUS
XGBoost Classifier	0.92	Active
Random Forest Regressor	0.89	Staging
Linear Regression	0.75	Deprecated

Note: The scores above are based on the last run cycle.

U What deployments are currently running in production and what cloud platform do they use?

Deployment Overview

The following services are live and actively processing requests:

- **Pricing Engine:** Running on AWS nodes. Status: Healthy.
- **Fraud Scanner:** Running on Azure nodes. Status: Warning (High latency detected).
- **Forecasting Service:** Running on GCP nodes. Status: Healthy.

U List all projects and tell me which one uses the 'Client_Master' dataset.

Workspace Projects Found

1. Churn Analysis v2 (Uses: Client_Master, Transaction_Log)
2. Predictive Maintenance POC (Uses: Sensor_Data only)
3. Sales Forecasting 2024 (Uses: Client_Master)

Frequently Asked Questions

01 **How does the DataRobot MCP help me audit my ML models?**

The DataRobot MCP gives you a conversational way to audit your models. You can ask it to compare validation scores, retrieve raw metrics for deep dives, or check specific model versions without navigating complex UIs.

02 **I need to know what is deployed in production—how does the DataRobot MCP handle that?**

The MCP provides a simple way to list all active deployments. You can get an immediate, structured overview of every running node and its current health status across different cloud platforms.

03 **Can I use the DataRobot MCP to check data sources for my projects?**

Yes, you can easily see what datasets are mapped or available. You can list all datasets associated with your workspace and understand their exact logical boundaries before training a model.

04 **Does using the DataRobot MCP mean I don't need to use the web interface?**

Not necessarily, but it means you don't have to. It lets you pull key operational data—like deployment statuses or metrics—into a chat conversation instantly, saving time and eliminating context switching.

05 **What if I need to compare old model results with new ones?**

The MCP allows you to retrieve detailed historical performance reports. You can get the raw training metrics for different versions of a model side-by-side, making comparisons straightforward and auditable.

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 `"datarobot": { "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

DataRobot 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 DataRobot. 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	DataRobot MCP
Server ID	`019d7582-64b7-7288-a8dc-785da5ed532d`
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/datarobot.

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