MCP SERVER | NO CODE | CLOUD HOSTED

Retool MCP Connector

Audit your entire internal tool stack via chat.

Retool MCP lets your AI agent inspect and audit internal applications directly. Instantly review who has access, what databases are connected, and how your entire suite of custom tools is structured—all from a simple chat prompt.

A+ Quality Score 100/100

internal-tools | app-building | database-management | audit-logs | workflow-monitoring | low-code

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

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.

Retool MCP

7 tools available
Cloud-hosted on Vinkius

Connect your conversational assistant to the Retool ecosystem for deep infrastructure insights. This connector allows your AI to look inside the complex web of internal applications built in Retool. You can ask it to map out your organizational structure, checking every tool and folder available without clicking through dozens of dashboards. Need to know who has access? Your agent reads the user list and checks current permission groups against those users. Want to audit what data powers your apps? It lists all connected databases and APIs for you. This ability to inspect infrastructure status—whether it's a PostgreSQL database or an external Stripe API—and monitor background automation tasks is incredibly powerful. Vinkius makes this whole catalog available, letting you connect once and instantly gaining the power to audit internal systems from any MCP-compatible client.

Core Capabilities

01 — Audit application structure

Lists all existing apps and folders in your Retool workspace so you can map out how tools are organized.

02 — Check user permissions

Retrieves the list of organization members and audits which permission groups they belong to.

03 — Review connected data sources

Lists every database, API, or external service wired into your Retool operational stack.

04 — Monitor system workflows

Checks for active background automation tasks and processes running within the environment.

One Click on Vinkius — From Prompt to Execution

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

01 Install the Retool module into your MCP environment and securely provide your Retool Access Token and Domain.

02 Your AI client receives permission to query the internal structure of your applications, users, and resources within Retool.

03 You simply ask a natural language question like, "List all active users and tell me what databases are connected," and get an immediate audit report.

The bottom line is you can use chat to run complex audits that used to require hours of manual clicking through multiple dashboards.

Built For

This MCP is for the IT Administrator or Engineering Lead who hates spending their day deep in click-heavy dashboards. It's for anyone whose job involves understanding system dependencies, user access rights, and application sprawl.

IT Administrator

Running quick audits on internal user privileges or checking database connections without having to navigate the main Retool dashboard.

Engineering Lead

Monitoring the overall landscape of internal tools and automation workflows while discussing operations with a team member.

Data Team Manager

Quickly verifying that essential data sources, like a specific PostgreSQL database, are correctly integrated into the Retool platform for development use.

What Changes When You Connect

01 Pinpoint access issues instantly. Instead of clicking through user menus, ask the agent to list all users and check their group assignments using `list_users` and `list_groups` for a quick audit.

02 Verify data connectivity in seconds. The `list_resources` tool lets you confirm if critical systems, like your PostgreSQL database or Stripe API, are actually wired into Retool when you need to know it.

03 Map the entire application landscape. Use `list_apps`, and then follow up with `list_folders` and `get_app` to understand how every single internal tool is organized without any manual navigation.

04 Check automation health easily. If a workflow fails, use `list_workflows` to list all active background tasks and see if anything unexpected has stopped running.

05 Reduce risk during handoffs. When onboarding new staff or changing roles, you can run an audit combining user listing, group checking, and resource review all in one chat session.

Real-World Applications

The database connection mystery

A data team member needs to confirm if the new regional PostgreSQL database is connected. Instead of logging into Retool and clicking through settings, they just prompt their agent: "Are all required databases available?" The agent runs `list_resources` and confirms the connection status immediately.

Onboarding a new team

An IT admin needs to check what access rights Bob has. Rather than trying to find his profile, they ask the agent: "What groups is Bob in?" The agent calls `list_users` and then cross-references permissions using `list_groups`, giving an instant answer.

Pre-launch infrastructure check

An engineering lead needs to verify if the payment module can process transactions. They ask the agent: "Show me all connected APIs and workflows." The agent runs `list_resources` and `list_workflows`, confirming both Stripe API connectivity and active automation tasks.

Understanding app sprawl

A manager wants to know which internal tools exist. They ask the agent: "What apps are built?" The agent responds with a list from `list_apps`, giving them a complete inventory of assets they never knew existed.

Patterns to Avoid

Manual dashboard clicking

✗ AVOID

Trying to audit permissions by navigating to User Management, then drilling down into Groups, and finally checking the linked database resources one by one.

✓ INSTEAD

Tell your agent to run a combined check. Ask it to use `list_users` alongside `list_groups` and follow up with `list_resources`. This combines three separate manual tasks into one chat command.

Assuming resource location

✗ AVOID

Thinking that because an app uses a database, the connection details are visible on the front end of the Retool dashboard.

✓ INSTEAD

The agent runs `list_resources`. This tool directly queries the backend configuration and shows you exactly which APIs or databases are attached to your entire environment, bypassing the visual layer.

Missing background tasks

✗ AVOID

Thinking that if a report is running slowly, it must be a database issue. You forget there might be an automation task slowing things down.

✓ INSTEAD

Always include `list_workflows` in your audit queries. This ensures you check the status of automated jobs, not just static resource connections.

The Right Fit

Use this MCP if your job requires auditing or inventorying internal infrastructure: Who can log into the Retool dashboard and needs to know what's connected? If you are mainly concerned with application *design* (e.g., how a specific button works), this isn't enough. But if you need to audit permissions (`list_groups`), check who is using it (`list_users`), or verify data flow (`list_resources`),

this is exactly what you need. Don't use this if you just need to build the application; use your native Retool client for that. This MCP is purely an inspection and governance tool, letting you read the system status without changing any settings.

The manual audit process takes hours of clicking.

Right now, checking the health of your internal tools means logging into Retool and manually hopping between User Management, Resource Connectors, and Workflow Automation. You click to see who is in a group, then copy names, paste them somewhere else to cross-reference with user lists, and finally open dozens of tabs just to check if the PostgreSQL connection is still active. It's slow, it's tedious, and you always feel like you missed one critical tab.

With this MCP, your agent does all that work for you in seconds. You ask a single question—like "What's connected?"—and it compiles the answer using tools like `list_resources` and `list_users`. You get an immediate, unified audit report right in your chat window.

Retool MCP: Get instant visibility into applications.

You no longer have to wait for a junior engineer to compile the list of active apps. Instead, you can prompt the agent using `list_apps` and `list_folders` to instantly map out the entire application sprawl. You get a clear, hierarchical view of everything built.

The result is that governance decisions are instantaneous. You don't just *think* about permissions; your AI client confirms them by running the checks for you.

Retool MCP Connector (7 Tools)

These tools allow you to systematically inspect every aspect of your Retool environment, covering applications, users, resources, and workflows.

#	TOOL	DESCRIPTION
01	`get_app`	Retrieves detailed information about one specific Retool application by name or ID.
02	`list_apps`	Provides a complete list of every custom application available in the Retool organization.
03	`list_folders`	Shows you the folder hierarchy used to organize tools within the Retool workspace.
04	`list_groups`	Retrieves a list of all existing permission groups that control user access rights.
05	`list_resources`	Lists every data source, API connector, or external service wired into the Retool platform.
06	`list_users`	Generates a comprehensive list of all currently active users in your Retool organization.
07	`list_workflows`	Shows the status and names of all automated background tasks running in Retool.

See It in Action

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

U List all users in my Retool workspace.

I invoked `list_users` successfully. I found 8 users in your organization, including `alice@example.com` and `bob@example.com`. Let me know if you need to know their group assignments using the associated permission tools.

U List all applications currently configured.

Running `list_apps`, I retrieved a total of 12 distinct internal tools within your environment. Popular examples include your 'Admin Dashboard', 'Customer Refund Portal', and 'Inventory Tracker'. Would you like the detailed properties for a specific one?

U Tell me what resources are connected to our Retool.

By querying `list_resources`, I can see 5 integrated services in your Retool account. This includes your production 'PostgreSQL Database', a 'Stripe API' connector, and an 'S3 Bucket' for file uploads. The connections are confirmed active.

Frequently Asked Questions

01 **How do I use Retool MCP to check user access?**

You simply ask the agent to list users and groups. It automatically uses `list_users` to get member names, then runs `list_groups` to show which permission sets those members belong to.

02 **Can I check if my database is connected using Retool MCP?**

Yes, use the agent to run `list_resources`. This tool checks every API and data source wired into Retool, confirming if your PostgreSQL or Stripe connections are active.

03 **Does Retool MCP only list apps, or can it show me details?**

It does both. You can start by listing all applications with `list_apps`, and then drill down into a specific app's properties using the `get_app` tool.

04 **How do I find out what background tasks are running?**

Ask the agent to check workflows. It uses the `list_workflows` tool to provide an overview of all automated background processes in your Retool environment.

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 `"retool": { "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

Retool 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 Retool. 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	Retool MCP
Server ID	`019d75ff-22b8-718f-a6ee-f19060fabfac`
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/retool.