MCP SERVER | NO CODE | CLOUD HOSTED

Automate.io MCP for AI Agents

Monitor and Debug Complex Workflow Automation Runs

Automate.io gives your AI agent full command over complex integration workflows. Use this MCP to audit every bot, trace execution runs—whether they succeed or fail—and check API connections across your entire platform via natural conversation.

A+ Quality Score 100/100

workflow-automation | integration-platform | bot-management | trigger-actions | execution-tracing | api-connectivity

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

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.

Automate.io MCP

6 tools available
Cloud-hosted on Vinkius

Need deep visibility into your automation flows without logging into the dashboard? This MCP connects your Automate.io account directly to any AI agent, letting you manage and debug complex integration workflows using only conversation. You can inspect structural rules for all your bots, trace specific execution runs to pinpoint exactly where a workflow failed, and audit every OAuth token connected to external services. It's about gaining total control over platform boundaries through plain talk.

For instance, instead of manually checking dashboards, you ask your agent to list all active connections or retrieve live billing usage stats against your account quota. This deep level of operational oversight makes it easy for teams to maintain reliability. By connecting this MCP via Vinkius, you bring the platform's full set of monitoring tools directly into your AI workflow, letting your agent do the heavy lifting.

Core Capabilities

01 — List and inspect all bots

See a structural overview of every automated bot, including its triggers and actions.

02 — Trace execution history for specific workflows

Retrieve the chronological log of attempts—successes or failures—for any given workflow endpoint.

03 — Audit connected SaaS applications

List and verify all external app connections, checking attached API keys or OAuth tokens.

04 — Check billing usage quotas

Get real-time statistics showing how many workflow executions have occurred against your account allowance.

05 — View supported integrations

Discover a list of applications that the underlying Automate engine natively supports globally.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your unique Automate.io API Key.

02 Connect it to your preferred AI client (Claude, Cursor, etc.).

03 Ask your agent questions about your workflows; it retrieves the data from Automate.io.

The bottom line is you get instant access to critical operational metrics and debug logs without ever leaving your chat interface.

Built For

This MCP is built for technical roles that live in the intersection of systems engineering and operations. If you spend your time debugging failed integrations or auditing compliance, this tool saves hours of manual dashboard clicking.

Integration Engineer

Uses it to remotely debug failed execution runs, diagnosing issues without needing to log into the main platform dashboard.

Operations Team Lead

Checks billing quotas and traces structural integrity on critical workflows before they impact business processes.

IT Administrator

Audits all connected SaaS applications and active API endpoints to ensure compliance and security across the company account.

What Changes When You Connect

01 Instantly diagnose workflow failures: Use the `list_bot_runs` function to trace exactly why a specific automation failed, getting the error details without logging in.

02 Maintain security posture: Audit all connected external systems using `list_connections`, verifying which OAuth tokens or API keys are active and authorized.

03 Manage resources efficiently: The `get_usage` tool gives you live billing statistics, letting you know exactly how close your workflow executions are to hitting the quota limit.

04 Control platform complexity: Instead of digging through menus, ask the agent to `list_bots` and instantly review the structure, triggers, and rules for every bot.

05 Quickly assess connectivity: Use the tool that lists all supported integrations (`list_apps`) before trying to build a new workflow with an unknown service.

Real-World Applications

Pinpointing a Production Bug

A developer notices workflows are failing intermittently. They ask their agent to check the `list_bot_runs` for the affected bot, which immediately pinpoints that the failure only happens on runs from the East Coast region, saving hours of guesswork.

Quarterly Security Audit

An IT admin needs to confirm all connected systems are still valid. They use the connection listing tools (`list_connections`) to generate a definitive report on every authorized OAuth token and API key in one pass.

Quota Management Check

The Ops team leader is worried about exceeding their monthly budget. They ask for usage metrics, and the agent uses `get_usage` to confirm they have 20% quota remaining until the next billing cycle.

Onboarding New Services

A new team needs to know what services Automate.io supports. They ask the AI to list all available integrations, using `list_apps` to see if the necessary CRM or ERP platform is built-in.

Patterns to Avoid

Relying on Dashboard Filtering

✗ AVOID

Manually clicking through dozens of workflow logs, filtering by date range and status, hoping to catch the one error that happened last Tuesday.

✓ INSTEAD

Ask your agent to run `list_bot_runs` for a specific bot. This retrieves the full execution history immediately, letting you filter and diagnose failures instantly without manual clicking.

Guessing Connection Status

✗ AVOID

Assuming an external app connection (like Slack) is still valid because it worked last week, only to have the workflow fail with a generic 'Authentication Error.'

✓ INSTEAD

Use `list_connections` to audit your current credentials. The agent will show you exactly which OAuth tokens need refreshing or which API keys are flagged as degraded.

Ignoring Quotas Until Failure

✗ AVOID

Letting workflows run unchecked until the platform sends an 'Exceeded Limit' warning, resulting in lost productivity and potential downtime.

✓ INSTEAD

Proactively ask for usage metrics using `get_usage`. This gives you a real-time view of your consumption against your allowance before you hit zero.

The Right Fit

Use this MCP if your pain is visibility into platform performance, not building the workflows themselves. You need to check logs (`list_bot_runs`), audit credentials (`list_connections`), or track spending (`get_usage`). Don't use it if you primarily need help drafting workflow logic; that requires a dedicated development environment. If your goal is simply listing available applications and nothing else, the `list_apps` tool handles that specific check. But for comprehensive operational control—the full lifecycle of monitoring, auditing, and debugging—this MCP is essential.

Automate.io MCP: Debugging Workflow Execution Runs

Debugging automation flows today means opening the dashboard, navigating to the specific bot, finding the run history tab, setting date filters, and scrolling through pages of mixed success/failure logs just to find that one cryptic error message. It's slow, tedious, and you risk missing context.

With this MCP, your agent pulls all the execution chronologies into a single conversation thread. You ask for the run history for 'Slack to CRM,' and it surfaces every attempt, detailing the specific failure point—like an expired API token—in plain language. It cuts out the dashboard clicks.

Automate.io MCP: Auditing SaaS Connections

Manually auditing external connections is a mess; you have to jump between the platform's settings, check every integration card, and try to confirm if the associated credentials (OAuth or API Key) are still valid and haven't degraded.

This MCP consolidates that view. You ask your agent to audit your integrations, and it provides a clear list of all attached apps and their current status. It’s immediate verification of connectivity across every platform.

Automate.io: 6 Tools for Bot Management & Workflow Auditing

These six tools let your AI agent list, audit, retrieve history, and check the status of all bots and connections in Automate.io.

#	TOOL	DESCRIPTION
01	`list_bots`	Lists every automated bot configured within your Automate.io account.
02	`get_usage`	Retrieves the current billing usage statistics for your entire Automate.io account.
03	`get_bot`	Fetches specific configuration details for a single, named bot.
04	`list_bot_runs`	Provides the full history of execution runs for any specific bot you name.
05	`list_connections`	Lists all external applications that have been authorized and connected to your Automate.io account.
06	`list_apps`	Discovers the full metadata list of integrations supported by the core Automate engine.

See It in Action

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

U Summarize my Automate usage numbers and tell me if I'm close to hitting the limit.

Usage Report:
- **Total Runs This Cycle:** 8,402
- **Quota Limit:** 10,000 runs
- **Remaining Quota:** ~15% (approx. 1,500 runs)

You're safe for now. You have about a week before the usage hits a critical threshold.

U What happened with the 'Salesforce to Trello' bot yesterday?

Bot Run History: Salesforce to Trello
- ✅ 2026-06-23 @ 10:00 AM: Success. Created 5 cards.
- ❌ 2026-06-23 @ 9:45 AM: **Failure.** Error Code: `Invalid User Scope`. The API key needs permission for Trello card creation.
- ✅ 2026-06-22 @ 11:00 AM: Success. Created 3 cards.

U Show me all the external apps we're connected to right now.

Active Connections Audit
We currently have four connections mapped:
- 🟢 Salesforce (OAuth Active)
- 🟢 Slack (OAuth Active)
- 🟡 Google Sheets (Warning: Token Degradation detected. Refresh recommended.)
- 🔑 Mailchimp (API Key Valid)

Frequently Asked Questions

01 **How can the Automate.io MCP help me debug failed workflows?**

You simply ask your agent to list the run history for a bot. It pulls up every execution log, detailing exactly when and why it broke—whether it's an expired token or a structural rule issue.

02 **Does Automate.io MCP help me check my usage quota?**

Yes, you can get live billing statistics using the MCP. It tells you exactly how many workflow executions you've used against your account limit right now.

03 **What is the best way to audit all my connected services with Automate.io?**

You ask the agent to list connections. It gives you a comprehensive report on every external app, verifying if their OAuth tokens or API keys are still active and authorized for use.

04 **Can I see what structural rules my bots have?**

Yes, by asking the agent to list bots. You get an overview of all triggers and actions attached to every bot, helping you understand how the automation is built.

05 **Is Automate.io MCP useful for IT teams doing compliance audits?**

Absolutely. It lets you audit your entire connected app portfolio easily. You can verify all endpoints and credentials in one place, which is critical for maintaining security logs.

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 `"automateio": { "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

Automate.io 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 Automate.io. 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	Automate.io MCP
Server ID	`019d7556-2a41-7028-b427-b24c74924318`
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/automateio.