MCP SERVER | NO CODE | CLOUD HOSTED

Hexomatic MCP

Run complex web scraping and automation tasks via chat.

Hexomatic brings web scraping and no-code automation into your AI agent. Manage complex data extraction and workflow runs entirely through natural conversation. You can list active workflows, trigger manual executions by passing variables like target URLs, retrieve detailed configuration settings for any process, and access comprehensive logs to troubleshoot failures. It lets you treat your agent like a dedicated Data Scraping Specialist.

A+ Quality Score 100/100

no-code | workflow-automation | lead-generation | market-research | data-extraction | automation-logs

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

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Hexomatic MCP

11 tools available
Cloud-hosted on Vinkius

Using this MCP means you're giving your AI client full control over web scraping and automation workflows. Instead of navigating complex dashboards or writing code every time you need data, you just talk to your agent about what you need done. Your agent acts as the conductor for all your automated processes. Need to find a competitor's tech stack? Just ask. Want to run a lead-generation workflow on a list of URLs? Tell it to do it. The power comes from the ability to manage everything, from listing available recipes and checking current usage credits to manually triggering runs and pulling back detailed logs for review. By connecting this Hexomatic MCP through Vinkius, you instantly transform your AI client into a powerful, hands-on automation architect that handles all the messy details of data collection.

Core Capabilities

01 — Manage workflow processes

You can list available automated workflows and view their specific configuration settings.

02 — Run automations on demand

Manually kick off a workflow execution from the chat, supplying necessary data like target URLs as variables.

03 — View scraping recipes

List all point-and-click web scraping blueprints and retrieve the structured output data after an execution finishes.

04 — Audit process failures

Access detailed, step-by-step logs for any workflow run to find exactly where things broke.

05 — Check account limits

Instantly check your current automation credit usage and plan status without logging into a portal.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Hexomatic API Key within Vinkius.

02 Your AI client recognizes the connection, making all automation tools available for natural conversation.

03 You simply prompt your agent: 'Run the Tech Stack Discovery workflow on example.com,' and it executes the task.

The bottom line is that you manage complex, multi-step web scraping tasks using plain language prompts instead of clicking through multiple dashboards.

Built For

This MCP is built for anyone whose job relies on gathering data from the live internet. If your day involves checking competitor websites, compiling lead lists, or monitoring market trends, this connector saves you hours of manual dashboard work.

Data Analyst

Runs automated workflows to extract specific datasets from target websites and then uses the logs to audit data quality.

Growth Marketer

Triggers lead-generation campaigns instantly, passing lists of potential prospects to automate scraping and enrichment.

Product Researcher

Analyzes competitor tech stacks or industry news by running specific recipes and comparing the collected data points.

What Changes When You Connect

01 Stop switching between dashboards. Your agent handles listing workflows, getting their details, and running them all without you needing to copy an ID or navigate a menu.

02 Troubleshoot instantly by using the `get_execution_logs` tool. Instead of wading through vague error messages in a web UI, your agent gives you the specific log output needed.

03 Save time on data collection by using built-in automation like Tech Stack Discovery. Just prompt for it, and your agent handles the full lifecycle: run, retrieve results (`get_workflow_results`), and summarize the findings.

04 Manage resources without hassle. Use `get_account_usage` to check credits before running a major job, preventing unexpected billing issues.

05 It treats you like an expert operator. You don't just get data; your agent acts as a specialist that knows exactly which automation (`list_automations`) or recipe (`list_scraping_recipes`) to apply.

Real-World Applications

Tracking Competitor Moves

A product researcher needs to know what tech a rival used six months ago. Instead of manually checking old reports, they prompt their agent: 'Show me the results from running the Tech Stack Discovery workflow on that site.' The agent runs `run_workflow` and immediately returns enriched data.

Validating Lead Lists

A growth marketer collects a list of URLs. They ask their agent to 'Run the LinkedIn Lead Finder workflow using this JSON array.' The agent executes the task, and they use `get_workflow_results` to pull back clean, structured data ready for CRM import.

Debugging Data Failures

The data analyst runs a complex pricing scraper but gets bad numbers. They prompt: 'Check the logs for the last run.' The agent uses `get_execution_logs` to pinpoint whether the failure was due to an expired API key or a website layout change.

Quickly Assessing Workflow Options

A new team member needs to know what's possible. They ask their agent, 'What automations do we have?' The agent uses `list_automations` and presents the options instantly, guiding them toward the correct workflow ID.

Patterns to Avoid

Treating it like a simple API call

✗ AVOID

Attempting to pass a URL and expecting raw HTML output. This is inefficient because you lose structure, forcing you to clean data manually later.

✓ INSTEAD

You must use the `run_workflow` tool. By passing the URL as an input variable in the body JSON, the system executes the entire configured process, ensuring structured output that can be immediately retrieved via `get_workflow_results`.

Forgetting which workflow to audit

✗ AVOID

Receiving a general 'Error' message and not knowing if the problem was in the scraping setup or the run itself.

✓ INSTEAD

Never rely on just an error code. Use `get_execution_logs` immediately after failure. This provides the detailed, step-by-step history needed to diagnose if it's a credentials issue or a data parsing mistake.

Ignoring resource limits

✗ AVOID

Running multiple large workflows back-to-back without realizing you hit your monthly credit cap, leading to job failures.

✓ INSTEAD

Always start by calling `get_account_usage`. This shows your current plan status and remaining credits before initiating any costly automation runs.

The Right Fit

Use this MCP if your core workflow involves gathering dynamic data from websites or running multi-step, pre-configured processes. You need the AI agent to act as a wrapper around complex web scraping logic, allowing you to interact with it purely through conversation.

Don't use this if all you need is simple text generation (use a standard LLM) or if your data already lives in a structured database (use a standard database connector). If you just want to list websites you scraped last month, stick to basic file storage—you don't need the full automation layer. This MCP shines when you need execution and auditing power.

Manually managing web data is tedious.

Right now, getting a comprehensive view of your market requires jumping between tabs: opening the main dashboard to list workflows, clicking into each one to check its configuration details, then manually triggering the run, and finally downloading the logs file just to find out what went wrong. It's copy-pasting IDs and managing status codes across multiple screens.

With this MCP, you skip the interface entirely. Your agent handles the entire lifecycle in natural conversation. You simply tell it, 'List all workflows,' or 'Run X on Y.' The system does the heavy lifting of routing and executing the task for you.

Hexomatic MCP delivers automated data intelligence.

You don't have to navigate 10 different settings pages or remember specific API keys. Your agent handles listing recipes, confirming your usage with `get_account_usage`, and then triggering the complex task using `run_workflow` —all in sequence.

The result is immediate control. You get structured data results directly back into your chat window, turning a hours-long manual process into a single conversation turn.

Hexomatic: 11 Tools for Data Extraction

These tools let you manage everything from listing available automations to triggering complex web scraping jobs and retrieving detailed execution logs.

#	TOOL	DESCRIPTION
01	`get_workflow_results`	Pulls the final structured output data from a workflow once it has completed its tasks.
02	`get_execution_logs`	Retrieves the complete step-by-step log file for a specific workflow run, useful for debugging.
03	`get_account_usage`	Shows your current plan details and how many automation credits you have left.
04	`get_workflow_details`	Gets the full, specific setup configuration for any single workflow ID.
05	`list_automations`	Shows a list of all pre-built Hexomatic automations, like Tech Stack Discovery.
06	`list_scraping_recipes`	Lists every available point-and-click web scraping template you can use immediately.
07	`list_account_teams`	Displays the names of all teams and collaborators connected to your account.
08	`list_workflows`	Lists every defined automation workflow in your Hexomatic account, helping you find the ID for running it.
09	`run_workflow`	Manually starts an execution of a chosen workflow using input variables like URLs.
10	`search_workflows`	Finds specific workflows by searching their name or title.
11	`update_workflow_status`	Changes whether a workflow is active (on) or inactive (off).

See It in Action

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

U List all active automation workflows.

I've retrieved your workflows. You have 4 active automations: 'Competitor Pricing Scraper', 'Tech Stack Discovery', 'LinkedIn Lead Finder', and 'Product News Tracker'. Which one would you like to run or inspect?

U Show me the results from the latest 'Tech Stack Discovery' run.

Accessing workflow results... The latest run for 'Tech Stack Discovery' (ID: hex_992) found that 'example.com' uses AWS, React, and Intercom. 'target-app.io' uses Google Cloud and Vue.js. Should I export these results to a summary for you?

U Run workflow ID 'hex_5501' with the target URL 'https://vinkius.com'.

Workflow triggered! I've successfully started the execution of workflow hex_5501 with the provided URL. You can check the progress using the `get_execution_logs` tool in a few minutes.

Frequently Asked Questions

01 **How do I check if my Hexomatic credits are running low using the Hexomatic MCP?**

You use `get_account_usage`. This tool quickly retrieves your current plan details and how many automation credits you have left, so you can avoid unexpected service interruptions.

02 **I need to run a workflow but don't know its ID. Which tool should I use?**

First, use `list_workflows` or `search_workflows`. These tools list all available automations so you can find the exact name or ID required before calling `run_workflow`.

03 **What is the difference between running a workflow and getting its results?**

Running the workflow starts the process. After it finishes, you use `get_workflow_results` to pull back the final, clean output data. You can't do both with one tool.

04 **Can I view old runs and see where they failed?**

Yes. If a workflow fails or you need an audit trail, use `get_execution_logs`. This provides detailed step-by-step logs for that specific run ID.

05 **Does the Hexomatic MCP support Tech Stack Discovery?**

Yes. You can find this built-in automation by listing all automations using `list_automations` and then running it via `run_workflow`.

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 `"hexomatic": { "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

Hexomatic 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 Hexomatic. 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	Hexomatic MCP
Server ID	`019d75b0-a2fc-7352-a467-7aa2b3670ce8`
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/hexomatic.