MCP SERVER | NO CODE | CLOUD HOSTED

Kaseya MCP

Monitor and manage your entire IT infrastructure from natural language.

Kaseya MCP connects your AI agent directly to Kaseya VSA 10, giving you full control over managed IT infrastructure and device health. Use this MCP to list all connected devices, track every asset, check active alarms, or review audit logs across multiple client organizations. It lets you manage the entire tech estate—from hardware inventory to security compliance checks—all through simple natural language commands.

A+ Quality Score 100/100

it-management | remote-monitoring | msp-tools | infrastructure-automation | device-management | vulnerability-scanning

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.

Kaseya MCP

10 tools available
Cloud-hosted on Vinkius

Need to know what's going on across your managed network? This MCP gives your agent direct access to Kaseya VSA 10, letting it monitor and interact with all your IT devices. You can check the status of every single agent, get a complete inventory list of assets, or quickly pull up recent audit logs for compliance checks. If an alarm goes off, your agent finds it using `list_alarms`. It also lets you inspect available scripts and workflows, so you never have to jump into a complex dashboard just to check status. By connecting this MCP through Vinkius, your AI client handles the heavy lifting of data retrieval, letting you focus on solving the problem, not clicking through tabs.

Core Capabilities

01 — Check Device Status and Visibility

List all managed agents to check their current online status or pull detailed information about a specific device.

02 — Manage Organizational Assets

Track your entire IT estate by listing organizations, groups, and individual hardware assets within the system.

03 — Review System Security Logs

Access recent audit logs or active alarms to quickly spot security issues or policy violations across your managed environments.

04 — Automate Maintenance Workflows

List and inspect available maintenance scripts and automation workflows ready for deployment on devices.

05 — Get System Health Data

Retrieve high-level system information, including metadata about your VSA 10 instance's current operational status.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to the Kaseya MCP and provide your unique Kaseya Instance Name, Token ID, and Token Secret credentials.

02 Then, tell your AI client exactly what you need—for example, 'What agents are offline?' or 'List all assets in the Finance group.'

03 Your agent executes the necessary API calls using the MCP's tools and returns plain English answers based on Kaseya data.

The bottom line is that you treat complex infrastructure monitoring like a simple conversation with your AI client, instead of navigating multiple dashboards.

Built For

This MCP is for the Ops Engineer who spends too much time clicking through dashboards at 2 AM. If manual checks are slowing down incident response, this tool cuts out the clicks and gives you direct access to operational truth.

IT Systems Administrator

Uses the MCP to quickly check device status across dozens of machines or trigger maintenance scripts without logging into a console.

Managed Service Provider (MSP)

Monitors multiple client organizations simultaneously, pulling up alarm lists and asset inventories from various groups in one conversational interface.

Security Analyst

Inspects system health indicators and reviews recent audit logs to investigate potential security breaches or compliance gaps instantly.

What Changes When You Connect

01 Stop bouncing between monitoring dashboards. Your agent aggregates device status, asset inventory, and alarm data into one conversation thread via `list_agents` and `list_assets`.

02 Cut down investigation time with security logs. Instead of manually filtering audit reports, you ask your agent to 'Show me the last 10 policy changes' using `list_audit_logs`.

03 Manage client groups efficiently. The MCP lets you list all organizations and machine groups (`list_organizations`, `list_groups`) so you can isolate problems without context switching.

04 Accelerate maintenance tasks. You don't need to know the script name; just ask your agent to 'Run patch deployment on Laptops,' which uses `list_scripts` under the hood.

05 Understand system scope immediately. Running `get_system_info` gives you a quick, accurate picture of your VSA 10 environment health without digging into setup menus.

Real-World Applications

The end-of-day status report.

An MSP needs to compile a summary for a client showing all offline devices and recent security alerts. They ask their agent, 'What are the current issues across the Accounting group?' The agent uses `list_agents` and `list_alarms`, giving a concise list of 7 offline machines and 3 critical alarms, saving the engineer 20 minutes of manual report generation.

Investigating unauthorized changes.

A Security Analyst suspects an admin changed a firewall rule. They instruct their agent to 'Show me all activity related to network policies.' The tool uses `list_audit_logs` to pull the precise timestamps and user IDs, confirming when the change happened and who made it.

Preparing for an audit.

An IT Admin needs proof of asset compliance. They prompt their agent: 'List all assets in the Production Servers group and verify they have current software versions.' The MCP uses `list_assets` combined with specific checks to generate a report proving compliance.

Deploying emergency fixes.

A critical bug is found, requiring an immediate patch. Instead of logging into the console and running scripts manually, the engineer asks their agent, 'Run the latest security patch on all Laptops.' The MCP uses `list_scripts` to locate and deploy the fix.

Patterns to Avoid

Assuming a tool does everything.

✗ AVOID

The user asks, 'Fix the network problem immediately,' expecting the AI agent to magically solve it. They don't specify *what* kind of fix or *where* the issue is.

✓ INSTEAD

You must narrow the scope by using specific tools. If the problem is device connectivity, ask first: 'Run `list_agents` and tell me which agents are offline.' This guides the agent to the right data.

Over-relying on a single tool.

✗ AVOID

The user only runs `list_assets`, getting just names and serial numbers. They assume this list is complete and accurate for compliance purposes.

✓ INSTEAD

Always cross-reference asset data. After running `list_assets`, follow up with, 'And what are the active alarms associated with those assets?' This uses `list_alarms` to provide context.

Asking for too much at once.

✗ AVOID

The user asks: 'Check all logs, list every group, and tell me about system updates.' The agent gets overwhelmed or provides a massive, unusable block of text.

✓ INSTEAD

Break the task into focused steps. First, ask to `list_groups`. Then, in a separate prompt, use `list_workflows` to see what automation is available for those groups.

The Right Fit

Use this MCP if your primary need is comprehensive visibility and command execution across many disparate IT systems. You should connect it when you want to treat infrastructure monitoring like talking to a highly knowledgeable colleague—you ask questions, and the tool provides data from dozens of sources (agents, assets,

logs) without requiring CLI syntax or dashboard navigation.

Don't use this if your goal is simply writing code or generating text. If you just need help drafting a policy document or summarizing meeting notes, stick with general-purpose chat models. Also, don't use it for financial data analysis; that requires specialized tools. This MCP excels at operational reality: knowing *what* is online, *if* it's safe, and *how* to fix it using the available scripts and workflows.

The Manual Burden of Infrastructure Monitoring

Right now, checking your network status means juggling a dozen tabs. You jump into the Asset Management dashboard for inventory. Then you switch to the Alarm Panel to see what's red. Next, you open the Audit Log viewer just to confirm who changed a setting last week. It’s tedious clicking, copying data from one screen, and pasting it into an email.

With this MCP, all that manual hopping vanishes. You simply tell your agent, 'Give me the status of the whole department.' The tool pulls together device statuses, checks for active alarms, and compiles a single, actionable summary for you.

Kaseya MCP: Direct Access to System Truth

You no longer have to manually cross-reference which group an asset belongs to before checking its status. You can ask your agent, 'What scripts are available for the Accounting group?' and it uses `list_scripts` against the correct scope.

The MCP gives you a single conversational point of truth. It means faster troubleshooting and zero context switching—you just get the answer.

Kaseya: System & Asset Management (10 Tools)

Use these ten tools to check system health, pull asset details, manage groups, or list scripts directly through your AI agent.

#	TOOL	DESCRIPTION
01	`get_agent_details`	Retrieves specific, detailed information about a single managed device agent.
02	`list_agents`	Checks the current availability and status of all connected devices in Kaseya.
03	`list_alarms`	Generates a list of currently active system alarms that need attention.
04	`list_assets`	Pulls up the complete roster and details of all managed hardware assets.
05	`list_groups`	Displays a list of machine groups to help you narrow down your search area.
06	`list_audit_logs`	Gathers recent system activities and actions taken within the environment for review.
07	`list_organizations`	Lists all distinct organizations managed under one Kaseya instance.
08	`list_scripts`	Provides a catalog of available maintenance scripts that can be run on agents.
09	`get_system_info`	Retrieves general operational metadata and status information about the VSA 10 system itself.
10	`list_workflows`	Lists pre-built automation workflows that can be deployed across multiple devices or groups.

See It in Action

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

U List all agents that are currently offline in Kaseya.

I've scanned your managed devices. Out of 150 agents, 12 are currently offline, including 'Server-PROD-01' and 'WS-MARKETING-05'. Would you like more details on any of them?

U Show me the recent audit logs for my VSA instance.

I've retrieved the latest audit logs. Recent actions include a policy update by 'Admin_User' and 3 successful script deployments to the 'Accounting' group.

U List all machine groups in the organization.

I found 8 machine groups in your Kaseya instance, including 'Laptops', 'Production Servers', and 'Retail POS Systems'.

Frequently Asked Questions

01 **How does Kaseya MCP help with compliance?**

It helps by allowing your agent to run `list_audit_logs` easily. Instead of sifting through massive log files, you can ask for specific actions (e.g., 'Show me all policy changes in the last month') and get a summary.

02 **Can I use Kaseya MCP to find missing devices?**

Yes. You run `list_agents` to check device availability, which immediately flags any managed agents that are currently offline or unreachable on the network.

03 **Does the Kaseya MCP only list assets, or can it do more?**

It does much more. Beyond `list_assets`, you can check active alarms using `list_alarms` and even view available maintenance scripts via `list_scripts`.

04 **What if I need to monitor multiple client groups?**

You list all organizations first with `list_organizations`. Then, you can scope your subsequent checks—like listing alarms or assets—to specific groups across those different clients.

05 **Is Kaseya MCP better than just using the Kaseya UI?**

It's faster. The UI requires knowing where to click; this MCP lets you talk to the data directly. You skip the navigation and go straight to the answer.

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 `"kaseya": { "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

Kaseya 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 Kaseya. 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	Kaseya MCP
Server ID	`019d75bf-a19a-70cd-b13c-a0b601ca9e38`
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/kaseya.