MCP SERVER | NO CODE | CLOUD HOSTED

Kolide MCP

Audit device security and compliance status.

Kolide helps you audit fleet security posture in seconds. Connect your AI agent to get full visibility into every managed device, track active vulnerabilities across your entire hardware inventory, and check user compliance states instantly. Audit logs, device details, and issue tracking—all available through one MCP.

A+ Quality Score 100/100

endpoint-security | device-management | fleet-inventory | vulnerability-scanning | security-auditing

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

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.

Kolide MCP

10 tools available
Cloud-hosted on Vinkius

Connect Kolide via Vinkius to gain complete oversight of your organization's fleet security and device health. You can use your AI agent to audit every managed device and track specific vulnerabilities or misconfigurations across the entire hardware inventory. It lets you see which users are linked to which devices and whether those individuals meet compliance standards. Need a deeper dive? You can pull up detailed reports on available security checks, view chronological administrative logs, or get high-level fleet statistics at a glance. This MCP handles all that complex data retrieval, letting your agent do the heavy lifting so you don't have to.

Core Capabilities

01 — Inventory Device Status

List every device in the fleet and check its current security status.

02 — Check for Security Vulnerabilities

Pull a list of active security issues or misconfigurations across the entire device pool.

03 — Review User Compliance

See which users are assigned to devices and whether they meet required compliance policies.

04 — Audit System Events

Access a complete, chronological history of security and administrative actions taken on the fleet.

05 — View High-Level Metrics

Get immediate statistics like total device count, online status percentage, and current issue counts.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and generate a Bearer Token from the Kolide settings.

02 Configure your AI client with that token so it can authenticate against the service.

03 Tell your agent exactly what you need—for example, 'What are the top three security issues affecting my MacBooks?'

The bottom line is: your agent uses the connection to query Kolide directly and spits out the answers in natural language.

Built For

Security Operations Center (SOC) analysts, IT managers, or compliance officers who are tired of manually cross-referencing dashboards to build a single security picture. You need instant, comprehensive visibility into every asset.

Security Analyst

Running automated audits across the fleet using the agent's ability to list devices and check for specific vulnerabilities.

IT Manager

Tracking compliance status by listing users and checking if their associated devices adhere to policy, or pulling high-level fleet statistics.

Compliance Officer

Generating reports on device ownership and accessing audit logs to prove adherence to regulatory standards.

What Changes When You Connect

01 You stop guessing about your network. By running `list_kolide_devices`, you get a clear, actionable list of every asset ID and its current security posture in one query.

02 Instead of digging through ten different dashboards, you use the MCP to pull all active vulnerabilities by calling `list_kolide_issues` and immediately know what needs patching.

03 Compliance checks are faster. Use the toolset to list users via `list_kolide_people`, then check individual compliance using `get_person_details` —all without switching tabs.

04 You get immediate answers about system changes by calling `list_kolide_audit_logs`. You don't have to manually sift through days of event records to find one key incident.

05 High-level overviews are instant. `get_kolide_fleet_stats` gives you a summary (total devices, compliance rate) so fast it feels like magic.

Real-World Applications

Investigating an alleged data leak

The agent runs through the audit logs using `list_kolide_audit_logs` to trace who accessed a sensitive resource and when. It then uses `get_person_details` to identify that user's role, pinpointing the source of the risk.

Quarterly compliance review

The team runs `list_kolide_people` followed by checks on each individual. They use this data to confirm every employee's assigned device is compliant and properly owned, satisfying auditors instantly.

Post-incident analysis

After a breach alert, the agent first calls `get_kolide_fleet_stats` for an overall picture. Then it uses `list_kolide_issues` to determine if other devices were affected by the same vulnerability.

Onboarding a new department

The IT manager runs `list_kolide_checks` to see what standards apply, and then uses `get_check_details` to confirm that every new device meets those exact criteria before it goes live.

Patterns to Avoid

Checking security status piecemeal

✗ AVOID

Calling one tool for devices, another tool for issues, and a third service for user names. This requires manual aggregation in a spreadsheet.

✓ INSTEAD

Use the Kolide MCP to chain these calls together. For instance, list all devices via `list_kolide_devices`, then immediately query those IDs against `list_kolide_issues` to get one comprehensive report.

Ignoring device ownership

✗ AVOID

Finding a vulnerability but not knowing which user or department is responsible for patching the machine.

✓ INSTEAD

Always pair your security checks. After finding an issue with `list_kolide_issues`, follow up by listing people via `list_kolide_people` to assign accountability.

Relying on raw logs only

✗ AVOID

Getting a massive dump of text from the audit log without context, making it impossible to pinpoint the actual risk.

✓ INSTEAD

Use `list_kolide_audit_logs` in conjunction with `get_check_details`. This lets your agent filter the noise and only present high-risk events relevant to specific compliance checks.

The Right Fit

You need this MCP if your job requires constant visibility across multiple, distinct security domains: physical device inventory, user identity, active vulnerabilities, and historical audit trails. If you're trying to build a single source of truth for 'How healthy is our fleet right now?'—this is the tool. Don't use it if you only need one piece of data; for example, just listing users. In that case, calling `list_kolide_people` alone works fine. But when you need to connect *who* (user) has *what* (device) and *if* that combination is safe (issues/logs), this MCP connects those dots automatically.

The constant headache of security visibility

Today, getting a full picture of your fleet means jumping between the device management dashboard, the vulnerability scanner portal, and the user directory. You copy IDs here, paste them there, run three different reports, then spend hours manually merging Excel sheets just to see who is non-compliant.

With this MCP, you tell your agent what you need —say, 'Give me a compliance report for all MacBooks.' The AI client handles the multi-step process: it checks device IDs, finds linked users, cross-references vulnerabilities, and delivers the final, clean answer directly to you.

Kolide MCP gives you comprehensive fleet security reporting

The manual steps that disappear are the data transfers. You won't have to run `list_kolide_devices` and then take those IDs to manually query for issues using a separate tool. The agent handles both calls sequentially, passing the results along.

You finally get one consistent view of your entire security posture. It’s not just data; it’s actionable intelligence that lets you patch vulnerabilities and correct compliance gaps in minutes.

Kolide: 10 Tools for Endpoint Security

These tools allow you to inspect every facet of your fleet—from listing device IDs to auditing historical security events.

#	TOOL	DESCRIPTION
01	`list_kolide_devices`	Lists every managed device in the fleet for a full security posture check.
02	`get_device_details`	Retrieves specific, granular details about one particular device ID.
03	`list_kolide_issues`	Pulls a list of all active security vulnerabilities and misconfigurations across the fleet.
04	`get_issue_details`	Provides deep information about one specific, reported security issue.
05	`list_kolide_people`	Lists all users associated with the system for compliance review.
06	`get_person_details`	Retrieves specific details about a single user account.
07	`list_kolide_checks`	Shows all the available security checks you can run against your fleet.
08	`get_check_details`	Gets detailed information about a specific type of security check.
09	`list_kolide_audit_logs`	Retrieves the full, chronological history of all administrative and security events.
10	`get_kolide_fleet_stats`	Generates a high-level summary of the entire fleet's current health metrics.

See It in Action

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

U List all devices currently online in Kolide

Retrieving online devices... I've found 42 devices currently active. Most are MacBooks running macOS 14. Would you like to see if any of these have pending security issues?

U What are the most common security issues in my fleet?

The most frequent issues are 'Outdated OS' (12 devices) and 'Full Disk Encryption Disabled' (5 devices). I can provide the names of the affected users if you'd like.

U Show fleet statistics for today

Current fleet stats: 150 total devices, 92% compliance rate, 12 active issues, and 5 new devices enrolled this week. Overall health is 'Good'.

Frequently Asked Questions

01 **How do I use the list_kolide_devices tool?**

You ask your agent to 'list all devices.' The system uses `list_kolide_devices` and returns a comprehensive roster of every asset ID in the fleet.

02 **Can Kolide MCP tell me who owns a problematic device?**

Yes. After running `list_kolide_issues`, you can follow up by asking for details on affected users. The agent uses tools like `get_person_details` to pinpoint ownership.

03 **Is Kolide MCP only good for current issues?**

No, it handles history too. By listing fleet audit logs using `list_kolide_audit_logs`, you get a chronological record of every security event that has happened previously.

04 **What is the best way to check overall compliance?**

Run `get_kolide_fleet_stats` first for a summary, then follow up with `list_kolide_people` and run checks on the most critical users to verify their status.

05 **Do I need to know specific vulnerability names?**

Not at all. You can ask your agent generally about 'security issues.' It will use `list_kolide_issues` and then offer options for deeper dives using `get_issue_details`.

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 `"kolide": { "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

Kolide 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 Kolide. 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	Kolide MCP
Server ID	`019d75c2-7fbc-73cf-91bc-6ac1c6fdf882`
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/kolide.