MCP SERVER | NO CODE | CLOUD HOSTED

Cisco Meraki MCP for AI Agents

Monitor Network and Device Statuses in Cloud-Managed Infrastructure

Cisco Meraki MCP connects your AI agent directly to your cloud-managed IT infrastructure. It lets you monitor network health, track connected devices, and manage configurations—all through natural conversation. Stop clicking dashboards; start asking questions about your entire enterprise network.

A+ Quality Score 98.33/100

network-management | it-infrastructure | hardware-inventory | cloud-networking | device-monitoring

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/cisco-meraki-1

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.

Cisco Meraki MCP

10 tools available
Cloud-hosted on Vinkius

Managing a large corporate network means jumping between dozens of tabs, running reports, and cross-referencing status data across multiple screens. This MCP puts all that knowledge into one conversational layer. Your agent can query the Meraki dashboard directly to give you real-time answers about your infrastructure. For example, instead of checking device statuses in three different places, you ask your AI client, and it compiles a single report detailing everything from which organizations you manage to the specific signal strength of connected clients across all sites. You just subscribe through Vinkius and connect your API key; the conversation does the heavy lifting.

Core Capabilities

01 — Check organization details

Retrieve metadata for any defined corporate entity or site.

02 — Review network configurations

Get detailed settings and configurations for a specific Meraki network.

03 — Audit hardware inventory

List all networking devices, like APs and switches, and check their current operational status across your sites.

04 — Monitor client activity

Track connected clients on a network, including how strong their signal is and if they are connecting properly.

05 — Manage wireless settings

Review all configured SSIDs and inspect specific details about your wireless setup.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/cisco-meraki-1** — connect your AI agent in three steps.

01 Subscribe to this MCP on Vinkius and provide your Cisco Meraki API Key.

02 Your AI agent uses the key to connect to the Meraki cloud dashboard.

03 You talk naturally to your AI client, asking it questions about network status or configurations. It retrieves and formats the data for you.

The bottom line is you get conversational control over complex networking tasks without needing to manually navigate the web console.

Built For

This MCP is built for Network Engineers, IT Operations Managers, and System Administrators. If you spend your day logging into dashboards just to find out if a specific piece of gear is online or what SSID was accidentally misconfigured, this is for you.

Network Engineer

Using the MCP to pull device details and monitor real-time client connectivity across multiple sites without leaving their primary workflow.

IT Operations Manager

Running bulk checks, like listing all organizations or retrieving network configurations for compliance audits, quickly through natural language prompts.

System Administrator

Investigating connectivity issues by asking the agent to track connected clients and their signal strength at a specific location.

What Changes When You Connect

01 Audit device health instantly. Use `get_device_statuses` to get a single report showing the status of all hardware across your entire organization, eliminating manual dashboard checks.

02 Pinpoint connectivity issues fast. With `list_clients`, you can ask about connected clients—including their signal strength and type—without having to run complex reports in the web console.

03 Manage configuration changes conversationally. Use `get_appliance_settings` to pull specific network configurations for a device, allowing your agent to draft necessary change tickets immediately.

04 Understand your whole footprint. The MCP allows you to list all organizations and networks using tools like `list_organizations` and `list_networks`, giving you an immediate map of every managed site.

05 Review wireless settings efficiently. Instead of hunting through menus, asking the agent to use `list_wireless_ssids` pulls up all configured network names in one prompt.

Real-World Applications

Finding a failing AP after hours

A technician notices an employee reports poor Wi-Fi. The agent is asked to use `get_device` and `list_clients` for the specific site, immediately identifying that a key access point is reporting low signal strength and high client drop rates.

Auditing organizational scope

An auditor needs proof of all managed sites. The agent uses `list_organizations`, providing an immediate, verifiable list of every corporate entity that must be included in the compliance report.

Checking a new network deployment

A project manager wants to confirm that the new branch office is set up correctly. The agent runs `list_networks` and then uses `get_appliance_settings` to verify all required security parameters are active.

Diagnosing a widespread outage

After an outage, the operations team asks for a full status report. The agent executes `list_devices` and `get_device_statuses`, providing an instant count of how many devices are online versus alerting across all sites.

Patterns to Avoid

Confusing network scope

✗ AVOID

Asking the agent to check device status without specifying the organization or network ID, leading to vague or incomplete reports.

✓ INSTEAD

Always start by identifying your scope. Use `list_organizations` first, then select a specific entity, and finally use `get_device_statuses` against that defined target.

Misunderstanding client data

✗ AVOID

Assuming the agent can list *all* clients ever connected to a network. The tool only shows currently active connections.

✓ INSTEAD

To see current users, use `list_clients`. Remember that this tracks live connection metrics for your troubleshooting.

Overloading the query

✗ AVOID

Asking for device status, client list, and wireless settings all in one massive prompt. This can confuse the agent or lead to timeouts.

✓ INSTEAD

Break it down. Check hardware first with `list_devices`, then check clients with `list_clients`, and finally review SSIDs using `list_wireless_ssids` in separate steps.

The Right Fit

Use this MCP if your core pain point is navigating the sheer volume of data across a complex, multi-site network. If you frequently find yourself running status checks, cross-referencing device IDs with client lists, or comparing configurations between different branch offices, this connector saves time by centralizing that knowledge base in conversation.

However, don't use it if your primary need is deep packet inspection or advanced firewall rule writing. This MCP focuses on inventory, basic status reporting, and configuration retrieval (like `get_appliance_settings`). If you need to build a complex automation script based on specific Meraki events, you might be better off using a dedicated scripting tool that integrates directly with the API payload rather than relying solely on conversational summaries.

Cisco Meraki MCP for AI Agents: Solving Network Visibility Pain Points

Right now, checking network health is a click-heavy nightmare. You have to jump into the dashboard, navigate to 'Devices,' then check statuses; if you need client data, you go back and filter by SSID. This means constant context switching, manually copying IDs, and piecing together reports across five different views just to answer one basic question: Is everything working?

With this MCP, your agent handles the clicks. You ask a plain language question—like 'Show me all APs with low signal strength in the downtown office.' It runs `list_devices` and filters the results internally, giving you an immediate, actionable summary without you ever touching a single dashboard menu.

Cisco Meraki MCP for AI Agents: Simplifying Device Inventory Management

Before this MCP, getting a comprehensive picture of your hardware meant running multiple reports—one for the organization list, one for network configurations, and another just for device types. It was slow, prone to human error, and often lagged behind the actual state of the physical infrastructure.

Now you simply ask the agent to 'List all hardware and their current status.' The MCP handles `list_devices` and `get_device_statuses`, providing a single, synthesized list that instantly maps your entire operational footprint. It's reliable, fast, and always up-to-date.

10 Cisco Meraki Tools for Network Monitoring Data

Use these tools to list organizations, retrieve hardware statuses, monitor connected clients, and manage specific network settings via natural language prompts.

#	TOOL	DESCRIPTION
01	`get_device`	Pulls detailed information for one specific network device.
02	`get_device_statuses`	Gathers the current operational status of all devices within your organization.
03	`get_organization`	Fetches detailed metadata about a specific corporate entity or branch.
04	`get_appliance_settings`	Retrieves the operational settings for networking gear within an organization.
05	`list_clients`	Lists all clients connected to a specific network and their current status.
06	`list_devices`	Provides a list of all hardware devices located within your specified network.
07	`list_networks`	Lists all available networks connected to an organization.
08	`list_organizations`	Provides a comprehensive list of every managed organization you have access to.
09	`list_wireless_ssids`	Shows all configured network names (SSIDs) for the wireless system.
10	`search_organizations`	Finds specific organizations using a name search query.

See It in Action

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

U Which organizations do I manage and what are their current network setups?

🏢 **Managed Organizations Overview**

• Global HQ (ID: 1234):
* Networks: Production, Guest Wi-Fi
* Key Devices: 50 APs, 8 Switches
* SSIDs available: `HQ_Staff`, `Guest`
• Regional Branch (ID: 5678):
* Networks: Local LAN Only
* Key Devices: 20 APs, 4 Switches
* SSIDs available: `Branch_Local`

Frequently Asked Questions

01 **How can I use the Cisco Meraki MCP to check device statuses?**

You simply ask your AI agent, 'What is the status of my networking devices?' The agent runs diagnostics across all connected hardware and gives you a single summary report detailing which APs or switches are online versus those that are alerting.

02 **Does the Cisco Meraki MCP help me see who is currently connected to my Wi-Fi?**

Yes. You can ask the agent about connected clients in a specific network. It pulls real-time data, showing you how many devices are active and their reported signal strength.

03 **What if I need to find out all my different office locations?**

The MCP allows you to list every organization tied to your Meraki account. If you know the name of a location, you can even search for it directly by name.

04 **Can this MCP help me audit network configurations?**

Absolutely. You can ask the agent to retrieve detailed settings for specific networks or appliances, letting you verify that crucial security parameters are set correctly across all sites.

05 **Is the Cisco Meraki MCP better than just looking at my web console?**

It's a huge time saver. Instead of clicking into multiple sections to piece together an answer, you talk to your AI agent and get a single, synthesized report that instantly answers complex questions about device health.

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 `"cisco-meraki-1": { "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

Cisco Meraki 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 Cisco Meraki. 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	Cisco Meraki MCP
Server ID	`019d75d2-807d-701f-9ca4-5663e14d9069`
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/cisco-meraki-1.