

MCP SERVER

NO CODE

CLOUD HOSTED

# Cisco Meraki MCP for AI Agents

Monitor network devices and track client connectivity across multiple sites

Cisco Meraki MCP connects your AI client to your cloud-managed networking dashboard. It lets you check device status, track connected clients, and audit network health by simply talking to your agent. Stop opening dashboards; get real-time infrastructure insights instantly.

**A+** Quality Score 100/100

network-management

cloud-networking

device-monitoring

it-infrastructure

wireless-management

network-security



# 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.

### 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.

### 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.

### 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**

Encryption at rest

**Ed25519**

PKI vault signatures

**24h TTL**

Ephemeral session keys

**V8 Isolate**

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.

### 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.

### 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.

### 06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

**FinOps**

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

**Firewall & DLP**

PII redaction activity, sensitive data protection counters, and security event timeline.

**Agent Activity**

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

**Tool Health**

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

**Incident Log**

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

Get started at [cloud.vinkius.com](https://cloud.vinkius.com) — connect your AI agent in under 60 seconds.

# Cisco Meraki MCP

8 tools available

Cloud-hosted on Vinkius

Managing a large network means juggling dozens of dashboards—one for wireless, one for switches, another for security logs. This MCP changes that. Instead of clicking through multiple portals just to figure out if the London office's switch is online or how many clients are logged in, you talk to your AI agent. It pulls all the data from Cisco Meraki into a single conversation thread.

Your agent can list every organization you manage, then drill down to check real-time status on specific hardware like APs and firewalls. You can audit device inventory by serial number or quickly get a high-level summary of network health across multiple sites. It's about getting actionable answers immediately, without the clickbait fluff of a traditional IT portal.

If you're using Vinkius to connect multiple services for your AI agent, adding this MCP means all your networking data—from client counts to admin access levels—is available in one place. You get deep visibility into cloud-managed IT infrastructure directly from your chat interface.

---

## Core Capabilities

**01 – List all managed organizations**

Retrieves a full list of every corporate network and organization linked to the dashboard.

**03 – Review current network health summaries**

Provides a high-level overview of configuration details and overall operational status for a chosen network.

**05 – Audit device inventory by type**

Generates a complete list of every physical piece of networking equipment in the entire organization's inventory.

**02 – Get detailed device information by serial number**

Looks up specific hardware details, including status and metadata for any given serial number.

**04 – Track connected clients across networks**

Lists all active users and devices currently connected to your wireless or wired infrastructure.

**06 – Review administrator access levels**

Lists all users who have administrative rights across different Meraki organizations.

# One Click on Vinkius — From Prompt to Execution

Available at [vinkius.com/mcp/cisco-meraki](https://vinkius.com/mcp/cisco-meraki) — connect your AI agent in three steps.

- 01** Subscribe to this MCP on Vinkius and obtain your Cisco Meraki Dashboard API Key from the platform's settings.
- 02** Provide that API key to your AI client (like Cursor or Claude) within the connection setup process.
- 03** Once connected, you simply ask your agent a question—for example, 'What is the status of all APs in Site B?'—and it executes the necessary calls.

The bottom line is that once set up, you manage complex cloud networks using natural language commands instead of clicking through multiple vendor portals.

---

## Built For

This MCP is built for IT professionals who spend too much time context-switching between dashboards. If you're an admin constantly logging into a web portal just to pull basic status reports, this saves hours of repetitive clicking.

### Network Administrator

Checks device uptime and client connectivity across multiple sites without leaving their chat interface.

### IT Manager

Audits overall network health, reviews hardware inventory, and verifies admin access levels for compliance checks.

### Support Technician

Quickly looks up a specific client's connection details or an AP's status simply by asking their AI agent.

---

## What Changes When You Connect

- 01** Stop logging into dashboards. Use the agent to get a live overview of device status, including APs and switches, directly in your chat.

- 
- 02** Audit compliance instantly. You can run `list_organization_inventory` to pull every single serial number across all corporate sites for auditing purposes.
- 
- 03** Check user access levels without opening anything. The agent reviews administrators using `list_organization_admins`, letting you verify who has elevated permissions immediately.
- 
- 04** Deep dive into connectivity. Need to know if a specific client is connected? Use the tool's ability to list network clients, giving you MAC addresses and usage details.
- 
- 05** Get instant summaries. Instead of clicking through five different tabs for status checks, ask the agent to run `get_network_summary` for an immediate health report.
- 

---

## Real-World Applications

### Finding a missing asset during a site audit

A manager needs to know if a specific piece of hardware was deployed. Instead of physically checking inventory, they ask their agent to run `list_organization_inventory` and narrow the search by model or serial number, getting instant confirmation.

### Comparing site health metrics

An IT manager needs to compare the operational status of two different branch offices. They ask the agent to run `get_network_summary` for both sites sequentially, allowing a direct comparison in one chat window.

### Investigating suspicious client activity

A security team member suspects unauthorized access. They prompt the agent to use `list_network_clients` across a specific network to identify unusual MAC addresses or high connection counts instantly.

### Onboarding and role verification

A new team member needs access rights verified. They ask their agent to use `list_organization_admins` to confirm who is currently authorized across the parent organization, saving time otherwise spent in HR/IT ticketing.

---

# Patterns to Avoid

---

## Checking device status one by one

### X AVOID

Manually going into the dashboard and checking the status of 50 individual APs to see if they are online.

### ✓ INSTEAD

Tell your agent to use `list_network_devices` for a whole network, which generates a list showing all hardware types and their current operational statuses in one go.

---

## Auditing inventory across multiple systems

### X AVOID

Switching between the asset management system and the Meraki portal to verify if serial numbers match up.

### ✓ INSTEAD

Use `list_organization_inventory` through this MCP. It aggregates all device serial numbers into your chat interface, making comparison immediate.

---

## Guessing which network is affected

### X AVOID

Trying to remember if the issue occurred in the 'East Wing' or the 'Warehouse' network.

### ✓ INSTEAD

Use `list_organization_networks` first. This lists all potential networks, letting you accurately scope your problem before asking for a summary using `get_network_summary`.

---

## The Right Fit

You should use this MCP if your primary pain point is context switching between networking dashboards to gather basic status reports, inventory details, or client counts. If your workflow requires querying network health data (like running a summary check with `get_network_summary`) and then immediately cross-referencing that against who has administrative rights (`list_organization_admins`), this connector saves you time.

Don't use this if you need to make configuration changes—this tool is read-only. If your goal is actually changing a firewall rule or updating firmware, you still have to go into the Meraki dashboard directly. It's purely for viewing data and generating reports.

---

---

## Cisco Meraki MCP: Solving Network Device Status Checks with AI Agents

Today, checking a few critical devices feels like an archaeological dig. You open the dashboard, navigate to 'Devices', then you have to filter by site, model, and status just to see if your APs are online. Then you repeat that process for switches, and maybe security appliances—it's tedious clicking, copying statuses into a spreadsheet, and praying nothing breaks while you do it.

With this MCP, you simply ask: 'Show me the operational status of all network devices in the West Wing.' The agent pulls data from Meraki's entire system and gives you an immediate, consolidated list of every device type and its current health. You get clean, actionable status reports without opening a single web tab.

---

## Cisco Meraki MCP: Auditing Network Client Connections with AI Agents

When an issue arises, the manual process is always the same. You have to jump into the client list portal, filter by date range, scroll through hundreds of MAC addresses, and manually count how many devices are active or what their last known location was. It's a time sink that slows down incident response.

This MCP lets you query all connected users directly. By asking your agent to 'List all clients for the main office,' it compiles the list instantly. You get immediate client counts and connection details, letting your team jump straight into diagnosis instead of data gathering.

---

## 8 Tools for Cisco Meraki: Device Inventory, Clients, and Network Data

Use these tools to check specific device details, get network summaries, list connected clients, or audit the entire organization's hardware inventory from your AI agent.

#	TOOL	DESCRIPTION
01	<code>get_device_details</code>	Pulls detailed information, including current operational status, for a single networking device using its serial number.
02	<code>get_network_summary</code>	Retrieves an immediate health summary and key configuration details for a specified network location.
03	<code>list_organization_admins</code>	Generates a complete list of all users who have elevated administrative permissions within a given organization.
04	<code>list_network_clients</code>	Lists every client device currently connected to the network, including their MAC address and connection status.
05	<code>list_network_devices</code>	Retrieves a list of all physical hardware (APs, switches, firewalls) installed in a specific network location.
06	<code>list_organization_inventory</code>	Provides an exhaustive audit of every device serial number registered across the entire organization's assets.
07	<code>list_organization_networks</code>	Retrieves a list of all distinct network sites and operational areas within one corporate entity.
08	<code>list_meraki_organizations</code>	Lists every organization the connected API key has visibility into, helping scope the current check.

---

## 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?



I found 4 distinct Meraki organizations associated with this API key:

- **Acme Corp:** (ID: 123456) - Primary HQ Site.
- **Global Distribution:** (ID: 789012) - Warehouse Network.
- **Beta Testing Group:** (ID: 334455) - Dev Environment.
- **Jane Doe's Dept:** (ID: 667788) - Small Office Site

Which of these should I check for network summaries?

### U Show me the status and inventory list for the 'Global Distribution' site.



#### Network Summary: Global Distribution

- **Health Score:** 98/100 (Minor firmware updates recommended)
- **Device Count:** APs: 45, Switches: 12, Firewalls: 3

**Inventory Check:** The serial numbers for all three firewalls are:

- FXW1: SN-A1B2C3D4
- FXW2: SN-E5F6G7H8
- FXW3: SN-I9J0K1L2

## U How many users are connected to the main office wireless network right now?



Checking the 'Primary HQ Site' for active connections...

There are currently **68** clients logged in. This includes:

- Staff Devices (Internal SSID): 55
- Visitor Passports (Guest SSID): 13

The top three MAC addresses observed are: `00:1A:2B:3C:4D:E1` , `FF:EE:DD:CC:BB:AA` and `A1:B2:C3:D4:E5:F6` .

---

## Frequently Asked Questions

---

### 01 How can the Cisco Meraki MCP help me check if my devices are online?

You can ask your agent to list all physical network devices in a specific location. It pulls real-time status data for every AP, switch, and firewall, letting you know instantly which pieces of hardware are up or down.

### 02 Do I have to open the Meraki dashboard to audit device serial numbers?

No. You just ask your agent to generate a full organization inventory list. It pulls every registered device's unique serial number into your chat, providing an immediate asset audit.

### 03 What if I want to see who the network administrators are?

You can tell your agent to list all users with admin rights across your organizations. It provides a clean roster of every authorized administrator's name and access level, helping you verify compliance.

### 04 How does using the Cisco Meraki MCP make troubleshooting easier?

It centralizes data retrieval. Instead of checking five different tabs for symptoms like 'high client count' or 'slow bandwidth,' you ask your agent to run a network summary, getting all critical metrics in one response.

### 05 Can I use the Cisco Meraki MCP to track connected devices?

Absolutely. You can prompt it to list all currently connected clients across any of your networks. It gives you real-time counts and details, which is perfect for incident response.

---

# Go Live in 60 Seconds

Get your connection token from [cloud.vinkius.com](https://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": { "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](https://cloud.vinkius.com) →

[vinkius.com](https://vinkius.com) · [support@vinkius.com](mailto: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	019d7570-52db-71cb-8727-d09f80a02210
Platform	Vinkius Cloud for AI Agents
Endpoint	<a href="https://edge.vinkius.com/{token}/mcp">https://edge.vinkius.com/{token}/mcp</a>

### 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](https://vinkius.com/mcp/cisco-meraki).