MCP SERVER | NO CODE | CLOUD HOSTED

AT&T IoT MCP for AI Agents

Manage entire IoT SIM fleets and connectivity diagnostics by conversation

AT&T IoT provides total control over your entire fleet of connected SIM devices. Connect this MCP to any AI client to check device inventory, monitor real-time connectivity status, manage data usage across shared pools, and instantly activate or suspend thousands of remote sensors via natural conversation.

A+ Quality Score 100/100

sim-management | fleet-management | connectivity-diagnostics | device-inventory | iot-data-plans

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/att-iot

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.

AT&T IoT MCP

10 tools available
Cloud-hosted on Vinkius

Connecting your AT&T IoT account gives your agent full command over every single SIM card in your fleet. You stop logging into complex web portals just to check a device's health or its current data allowance. Now, you talk to your AI client, and it handles the API calls for you.

Your agent can list all devices with their status (active, suspended, etc.), run automated diagnostics on offline units, and even update settings like APN configurations across groups of sensors. Need to contain costs? You instruct the device suspension process immediately. Want to audit billing? Your agent pulls historical data usage reports and tracks shared pool consumption, letting you forecast when capacity will run low. By connecting this MCP through Vinkius Catalog, your AI client becomes a complete IoT operations console, eliminating manual clicks and keeping your entire network running smoothly.

Core Capabilities

01 — Audit Device Inventory and Status

List all connected SIMs with their ICCIDs, current status, data plans, and last recorded activity date.

02 — Monitor Real-Time Connectivity

Get live diagnostics, including signal strength, IP address, data used/remaining, and the specific reason if a device is suspended.

03 — Control Device Lifecycle

Instantly activate deactivated SIMs or suspend compromised ones to prevent unauthorized network access and limit costs.

04 — Optimize Data Pool Management

View shared data pools, monitor total consumption across the fleet, and identify which devices are draining resources quickly.

05 — Update Device Configurations

Modify critical device settings like rate limits or APN values to optimize performance for different use cases.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the AT&T IoT MCP and provide your specific API Key and Client ID.

02 Authorize the connection through any compatible AI client (Claude, Cursor, etc.).

03 Ask your agent a question—like 'What's wrong with device X?'—and it runs diagnostics and provides actionable answers.

The bottom line is that your AI agent handles all the complex API calls so you can focus on solving operational problems instead of navigating developer documentation.

Built For

This MCP is essential for anyone running a large-scale, distributed fleet of connected hardware. If manual checks across multiple portals slow down your team, this tool gives you the centralized control needed to keep operations moving.

IoT Fleet Manager

You use this MCP to monitor device health at scale, check shared data pool usage against consumption forecasts, and prevent SIM exhaustion before it impacts service.

Field Engineer

When a sensor goes offline miles from the office, you ask your agent to run diagnostics or suspend a lost unit instantly, saving time and preventing unnecessary costs.

Network Operations Specialist

You use this MCP to troubleshoot connectivity issues by checking APN configurations and running automated diagnostics on suspected outages across the network area.

What Changes When You Connect

01 Instantly control device lifecycles. With the `suspend_device` tool, you can block a lost unit's network access in seconds—no manual ticket system required.

02 Eliminate guesswork on data spending. Use `get_pool_usage` to track shared pool consumption and identify top-spending devices before budget overruns happen.

03 Solve connectivity problems fast. Instead of guessing, you run automated checks with `diagnose_connectivity` to pinpoint if the issue is an APN mismatch or a network outage.

04 Keep your inventory accurate. The `list_devices` tool gives you a real-time audit of every SIM card's status, whether it's active, suspended, or deactivated.

05 Optimize settings remotely. You can use `update_device_settings` to adjust rate limits and APN values on dozens of devices without logging into the control portal.

Real-World Applications

Identifying all inactive hardware

An audit team needs a full list of every SIM card, especially those that haven't reported data in months. Asking your agent to run `list_devices` generates an immediate report, saving hours of manual database querying.

Containing costs after theft

A site reports a stolen sensor. Instead of waiting for physical retrieval or billing cycles, the agent uses `suspend_device` immediately on that specific ICCID to stop all network charges and contain losses.

Recovering service after maintenance

After a group of sensors undergo necessary servicing, you need to restore their connection. Running the agent's `resume_device` tool brings them back online instantly without complex reprovisioning steps.

Pre-deployment network checks

Before rolling out a new fleet in a specific area, your team runs diagnostics using `diagnose_connectivity`. This quickly verifies the local APN settings and flags potential regional outages before deployment begins.

Patterns to Avoid

Checking every device individually

✗ AVOID

A user tries to check 50 different SIM cards by manually entering their ICCID into a separate dashboard page for each one.

✓ INSTEAD

Instead, ask your agent to use `list_devices` and then filter the resulting list by status or data plan name. You get all the necessary data in one conversation.

Ignoring shared resource limits

✗ AVOID

The operations team overlooks that multiple small deployments are collectively draining a shared data pool, leading to unexpected service interruptions.

✓ INSTEAD

Always check the aggregate usage first. Use `list_data_pools` then run `get_pool_usage` on the specific pool name to see total consumption and remaining capacity.

Assuming device settings are correct

✗ AVOID

A device fails to connect, and the technician simply restarts it, assuming the issue is physical, when the real problem is outdated network parameters.

✓ INSTEAD

Use `diagnose_connectivity` first. If the diagnosis points to configuration issues, use `update_device_settings` to correct APN or rate limits programmatically.

The Right Fit

You should use this MCP if your workflow requires immediate, programmatic control over a large number of remote IoT assets—think thousands of sensors that need continuous monitoring. It's perfect for tasks like bulk diagnostics, mass status checks, or emergency device suspension.

Don't use it if you only need basic viewing access; if reading simple reports is enough and you never have to change settings (e.g., just view a static CSV), then a simpler data export tool will suffice. If your primary need is troubleshooting network infrastructure that isn't tied to an individual SIM, look for general telecom diagnostic tools instead of this specific device-focused MCP.

AT&T IoT: Monitoring Device Health and Data Pools with AT&T IoT

Today, managing a modern sensor fleet requires jumping between an inventory portal, a billing dashboard, and a separate diagnostics page. You manually check the status of 30 devices on one screen, then copy data usage to a spreadsheet for cost review, and finally open a third tab just to run network diagnostics on a single offline unit.

With this MCP, you simply ask your agent: 'Which units are failing or running low?' It compiles the inventory list, checks real-time status, identifies depleted pools using `get_pool_usage`, and flags connectivity issues—all in one conversation. You get immediate, actionable answers.

AT&T IoT: Streamlining SIM Activation and Network Access with AT&T IoT

Manually onboarding new hardware means logging into the control center, finding the device by serial number, and clicking through activation forms. If a unit is lost or needs to be decommissioned, you must remember to manually suspend it everywhere.

Now, your agent handles the entire lifecycle. You tell it which units need service, and it runs `activate_device` for new deployments. When assets are retired or stolen, it executes `suspend_device`, guaranteeing instant network cutoff without any manual clicks.

AT&T IoT: 10 Tools for SIM Management and Connectivity Diagnostics

Use these tools to audit fleet inventory, diagnose connectivity issues, monitor usage, and control device lifecycle settings across your AT&T IoT network.

#	TOOL	DESCRIPTION
01	activate_device	Restores service or brings new devices online, returning the activation time and assigned IP address.
02	diagnose_connectivity	Runs automated troubleshooting checks on a device to identify connectivity issues and suggest fixes for offline units.
03	get_data_usage	Retrieves detailed records of current and historical data consumption for any specific IoT SIM card.
04	get_device_status	Provides a live snapshot of an IoT SIM's connectivity, showing its data allowance and real-time status.
05	get_pool_usage	Shows detailed usage metrics for a specific shared data pool to help prevent overspending.
06	list_data_pools	Provides an overview of all configured enterprise data pools used across your device fleet.
07	list_devices	Generates a full inventory list of every managed IoT SIM, helping you audit status and provisioning records.
08	resume_device	Restores network access to a suspended device after troubleshooting or policy clearance has been completed.
09	suspend_device	Blocks the network connection for an IoT SIM immediately, typically used when a unit is reported lost or stolen.
10	update_device_settings	Changes critical settings like rate limits and APN configurations on a specific device to optimize its performance.

See It in Action

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

U List all my devices and tell me which ones need attention right now.

IoT Fleet Status Report

- **Total Devices:** 412
- **Active/Healthy:** 398 (96%)
- **Needs Attention:** 14

* ⚠️ **Suspended for Cost Containment:** 7 units. These are currently blocking access to save money.
* 🔴 **Offline/Diagnostic Required:** 5 units. Diagnostics show APN configuration mismatch on three of these.
* 🟡 **Data Pool Warning:** 2 units. They used up the remaining 10% capacity in Pool Alpha and need reassignment.

U We just deployed a new batch of sensors; can you get them ready to go?

✅ **New Deployment Status**

I've successfully processed the activation request for 35 devices. Here are the results:

ICCID	STATUS	ASSIGNED IP	ACTIVATION TIME
...1234	Active	192.168.1.5	2026-06-12 10:01 AM
...5678	Active	192.168.1.6	2026-06-12 10:01 AM
...9012	Active	192.168.1.7	2026-06-12 10:01 AM

All units are reporting strong network registration and full connectivity.

U What's our current data usage on the main enterprise pool?

Data Pool Usage Report

- **Pool Name:** Enterprise-Fleet-A
- **Total Allocated:** 100 GB
- **Used:** 78.3 GB (78.3% utilization)
- **Remaining:** 21.7 GB
- **Renewal Date:** April 28th

Top 5 Consumers:
1. ICCID ...3456: 8.2 GB
2. ICCID ...7891: 6.7 GB
3. ICCID ...2345: 5.1 GB

Recommendation: Consider reallocating capacity or suspending non-critical devices to extend the pool life.

Frequently Asked Questions

01 **How do I use the AT&T IoT MCP to check every device's status?**

You can ask your agent to list all connected SIM cards. It gives you a full inventory, showing which devices are active, suspended, or deactivated, along with their last activity date for easy auditing.

02 **Can I suspend multiple devices using the AT&T IoT MCP?**

Yes. You simply ask your agent to suspend a list of ICCIDs or all units associated with a specific location. This is much faster and more reliable than doing it manually in the portal.

03 **Is data usage tracking available through the AT&T IoT MCP?**

Absolutely. The MCP pulls current and historical consumption reports for any SIM, helping you predict when your shared data pools will run out so you can plan for billing cycles ahead of time.

04 **What if a device is offline? Can the AT&T IoT MCP help troubleshoot it?**

Yes. You ask your agent to diagnose connectivity issues. It runs automated checks, identifies problems like APN misconfigurations or network registration failures, and tells you exactly what needs fixing.

05 **Does the AT&T IoT MCP let me change device settings?**

Yes, it allows advanced configuration changes. You can update things like rate limits or APN settings across multiple devices programmatically to optimize their performance without manual intervention.

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 `"att-iot": { "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

AT&T IoT 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 AT&T IoT. 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	AT&T IoT MCP
Server ID	`019d7554-c1fd-730e-b1d5-2ae57d54d3ca`
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/att-iot.