MCP SERVER | NO CODE | CLOUD HOSTED

Atera MCP for AI Agents

Managing IT Support Tickets and Device Status

Atera MCP gives your AI agent deep access into your IT management platform. You stop clicking through dashboards and start talking directly to your infrastructure data. Use it to list devices, create support tickets, audit customer records, and track system alerts—all from a single conversation with your preferred AI client.

F Quality Score 3.6/100

rmm | psa | it-management | remote-monitoring | ticket-tracking | device-management

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

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.

Atera MCP

9 tools available
Cloud-hosted on Vinkius

Atera lets you manage complex IT operations by connecting your AI agent directly to your monitoring platform's core functions. You don't have to navigate multiple tabs or copy-paste data between systems. Instead, you simply ask for what you need—like listing all devices running a specific OS, or finding the last five high-priority support tickets.

For example, if an agent reports an issue, your AI client can immediately pull up that customer's contact details and create a formal ticket, everything in one go. This capability radically changes how MSPs handle day-to-day work. When you connect Atera via Vinkius, your agent gains powerful tools to monitor hardware status, review organizational structures, and keep track of every alert without ever needing to log into the web dashboard manually.

Core Capabilities

01 — View Device Status

List all monitored devices (agents), getting detailed info like OS type, IP addresses, and current online/offline status.

02 — Create Support Tickets

Generate a new support ticket instantly when an issue is reported, ensuring it gets logged with the right details.

03 — Retrieve Account Details

Verify that your Atera account connection is active and ready to use by checking credentials.

04 — Manage Support Tickets

Get full details on a specific ticket or list all current tickets across the client base.

05 — Access Customer Data

Retrieve detailed information about any customer organization or individual end-user contact within your system.

06 — Monitor System Alerts

Pull a list of recent alerts, letting you proactively identify potential hardware failures or service outages.

One Click on Vinkius — From Prompt to Execution

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

01 Your AI client authenticates with the Atera MCP using your secure API key.

02 You prompt your agent with a natural language request, such as 'List all offline agents in the Northeast region.'

03 The MCP executes the relevant tool calls and returns structured data, which your AI client then presents to you in plain English.

The bottom line is that your AI client handles the complex back-and-forth with Atera so you just get a clean, conversational answer.

Built For

This MCP is built for IT Administrators and Managed Service Providers (MSPs) who spend too much time clicking between dashboards. If your day involves checking device statuses, logging tickets, or pulling customer records manually, this tool saves you hours.

Managed Service Provider Technician

They monitor system alerts and update ticket status directly from chat, instead of switching between the ticketing system and the monitoring dashboard.

IT Administrator

They quickly check the operational status of servers or workstations across multiple clients without needing to manually audit every device record.

Operations Manager

They retrieve customer and contact data for reporting, planning, and compiling reports for executive meetings.

What Changes When You Connect

01 You stop navigating complex web dashboards. Asking your agent to list all monitored agents or check specific device details is instant.

02 Need to know what's broken? By using the `list_alerts` tool, you immediately get a clear rundown of potential hardware or software failures, letting you fix things before they become major outages.

03 Never lose context again. Your agent can cross-reference customer data with current tickets. You can ask it to find all high-priority issues for 'Acme Corp' in one query.

04 Ticket handling gets faster. Instead of manually logging into the ticketing system, you use `create_ticket` and get a new ticket logged immediately from your chat interface.

05 Auditing is painless. You can quickly call `list_customers` or `list_agents` to pull comprehensive reports on who your clients are and what tech they run.

06 It saves time finding data points. The MCP allows you to consolidate knowledge about customer structure, agent status, and open tickets into one conversational flow.

Real-World Applications

Investigating a client outage

A user asks: 'What's wrong with the main office?' The agent responds by calling `list_alerts` first, finding a 'Disk Space Low' warning. It then uses `get_customer` to pull up the client's contact list and recommends who needs to be notified immediately.

Starting a new service contract

An operations manager asks: 'Show me all clients in Texas.' The agent runs `list_customers`, filters the results, and then uses `get_customer` on one specific entry to pull up contact details for sales follow-up.

Handling a sudden support surge

A tech needs to open a record. They ask: 'Log a new ticket for Agent ID 502.' The agent executes `create_ticket`, logging the issue and immediately returns the new ticket number.

Pre-audit preparation

A manager needs to report on device health. They ask: 'How many agents are online vs offline?' The agent runs `list_agents` and summarizes the full count, saving them from clicking through dozens of individual device dashboards.

Patterns to Avoid

Copying data between apps

✗ AVOID

The user finds a ticket ID in one system, copies it into an email, and then has to manually paste it into the monitoring dashboard to check status.

✓ INSTEAD

Instead of copy-pasting anything, tell your AI agent: 'Check ticket 1234.' The MCP uses `get_ticket` to pull up all related information (customer details, agent links) in one go.

Forgetting the client context

✗ AVOID

A user asks for a list of agents but doesn't specify which customer group they are working with, leading to irrelevant results.

✓ INSTEAD

Always ground your request. Say: 'List all agents for the Northwood Group.' This guides the agent to use `list_agents` against the correct organizational context.

Overlooking system health checks

✗ AVOID

A user only focuses on open tickets and misses critical hardware warnings that could cause new issues.

✓ INSTEAD

Always start by asking: 'Are there any active alerts?' Using `list_alerts` ensures you see the infrastructure problems before dealing with human-reported tickets.

The Right Fit

Use this MCP if your IT workflow involves constant context switching—jumping from a ticketing system to a monitoring dashboard, and then checking customer records. If your team needs an AI agent that can synthesize data about device status (`list_agents`), support history (`get_ticket`), and client details (`get_customer`) all in one conversation, this is the right fit.

Don't use it if you only need to perform single functions, like just reading a static list of customer names. For those isolated tasks, simple data retrieval tools might suffice. But if your goal is operational intelligence—connecting the dots between alerts and tickets—this Atera MCP gives you that unified view.

Atera MCP for IT Support Ticket Management

Right now, handling a support request means opening the ticketing system to get the ID. Then, switching tabs to check if the customer is on a high-priority account. You copy details and send them into another chat window just to see the latest device status or audit which agents are online.

With this MCP, that whole manual dance disappears. Your agent takes your request—say, 'Check client XYZ's ticket history.' It automatically pulls the customer data, then fetches all associated tickets, giving you a complete picture without ever leaving your chat window.

Atera MCP for Remote Device Monitoring

The manual process of checking device health is brutal. You have to visit the monitoring dashboard and manually check OS status, IP addresses, and alert logs for every client you manage.

Now, ask your agent: 'List all devices running Windows that are offline.' It runs `list_agents` and instantly filters the results, providing a targeted list of exactly what needs attention. You get actionable data, not just raw metrics.

9 Atera Tools for IT Operations and Monitoring

Use these tools to list devices, create support tickets, manage customer records, and track system alerts through natural conversation.

#	TOOL	DESCRIPTION
01	`create_ticket`	Creates a brand new support ticket in your system.
02	`get_account_check`	Verifies that the Atera account connection is working correctly.
03	`get_agent`	Retrieves detailed information for one specific monitored device (agent).
04	`get_customer`	Gets all the details for a single customer organization.
05	`get_ticket`	Pulls all the details associated with one specific ticket ID.
06	`list_agents`	Lists every monitored device (agent) currently connected to Atera.
07	`list_alerts`	Pulls a list of all recent system alerts that need attention.
08	`list_customers`	Lists every customer organization managed by Atera.
09	`list_tickets`	Retrieves a list of all support tickets currently in the system.

See It in Action

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

U Show me all agents for Acme Corp that are showing high CPU usage.

Agent Status Report: Acme Corp

- **Total Devices:** 45
- **High Usage Detected:** 3 devices (Requires immediate attention)

DEVICE ID	IP ADDRESS	OS TYPE	ALERT LEVEL
DEV-012	192.168.1.5	Windows 10	HIGH (CPU > 90%)
DEV-345	192.168.1.10	MacOS Ventura	MEDIUM (Memory Low)
DEV-789	192.168.1.15	Linux Kernel	HIGH (Disk Space < 5%)

U What's the status of the last ticket for client Beta Inc?

I found the details on Ticket ID: **9034**.

- **Status:** Pending Client Response
- **Priority:** Medium (Tier 2)
- **Created For:** John Doe (Contact ID: C-55)
- **Last Action:** Assigned to Tier 1 Support on 2026-06-12.

The issue relates to a VPN connection failure, which is consistent with the alerts found for their gateway devices.

U List all customers that have open high priority tickets.

I've checked the current queue and found 3 clients with active high-priority issues:

1. **Acme Corp:** Ticket ID 1234 (VPN Connection Issue). Requires immediate network review.
2. **Global Solutions Inc.:** No open tickets, but 5 agents are showing 'Offline' status.
3. **Beta Inc.:** Ticket ID 9034 (System Access Failure). Needs credentials reset.

Frequently Asked Questions

01 **How does Atera MCP help manage my IT support tickets?**

Atera MCP lets your AI agent read, list, and create new support tickets directly. You can ask it to show the last five issues or generate a ticket instantly for an issue found during monitoring.

02 **I need to check device status across multiple clients using Atera MCP?**

Yes. By listing agents, you can pull comprehensive data on OS types and IP addresses for all monitored devices without manual dashboard navigation. This is great for large MSP accounts.

03 **What kind of customer information can I get with Atera MCP?**

You can retrieve full details about individual customers and their associated contacts. It helps you build a complete picture of the organization structure before starting any troubleshooting.

04 **Can Atera MCP help me plan for audits or reporting?**

Absolutely. You can ask your agent to list all customer accounts, allowing you to pull comprehensive data sets on who you serve and their current operational status for quarterly reports.

05 **Is Atera MCP just for viewing alerts, or can it do more?**

It does much more. While checking recent system alerts is key, the MCP also lets you cross-reference those alerts with customer data and create new tickets based on what's found.

06 **What if I need to find a specific device detail using Atera MCP?**

You simply ask your agent for details about the agent. It pulls all the technical specs, including IP addresses and OS information, right into the conversation window for you.

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 `"atera": { "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

Atera 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 Atera. 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	Atera MCP
Server ID	`019d7554-055b-7354-bffd-9b3a9d776931`
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/atera.