MCP SERVER | NO CODE | CLOUD HOSTED

AT&T 5G MCP for AI Agents

Managing 5G Network Slicing and Device Location Data

The AT&T 5G MCP gives your AI agent deep access to Open Gateway network APIs. You can run fraud checks like SIM swap detection, provision private network slices, verify user phone numbers without sending SMS codes, and monitor device location using AT&T's live 5G infrastructure data.

A+ Quality Score 100/100

5g-api | network-slicing | device-location | number-verification | camara-api | telecom-infrastructure

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/att-5g

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 5G MCP

9 tools available
Cloud-hosted on Vinkius

Stop writing custom HTTP clients just to check a few API endpoints. This MCP connects your AI agent directly to the full suite of AT&T's Open Gateway network capabilities. Instead of navigating developer portals or building complex integration layers, you talk naturally to your client—Claude, Cursor, or any compatible tool—and it executes advanced network commands.

For example, need to onboard a new enterprise client? Your agent can automatically provision a dedicated 5G network slice with specific performance guarantees. Worried about account takeover? You just ask the system to run a SIM swap detection check. If your application needs location data for geo-fencing or emergency services routing, it's available—all without you touching any code. It makes your AI agent act like a full network operations console. By connecting through Vinkius, this MCP becomes one of thousands of specialized tools ready to augment whatever workflow you're building.

Core Capabilities

01 — Checking device roaming status

Determines if a phone is connected to an outside network, which helps with billing and routing.

02 — Running SIM swap detection checks

Compares recent account activity to detect signs of fraud or unauthorized access attempts.

03 — Creating a new 5G network slice

Deploys an isolated, dedicated virtual segment of the network for private enterprise use cases.

04 — Deleting an existing network slice

Removes a provisioned network segment to stop associated costs and clean up resources.

05 — Getting approximate device location

Returns the general coordinates of a device based on cell tower triangulation, requiring user consent.

06 — Retrieving network slice details

Pulls comprehensive information about an existing network segment, including its performance SLAs and connected devices.

07 — Listing active service sessions

Generates a detailed log of all premium or high-usage network sessions for auditing purposes.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/att-5g** — connect your AI agent in three steps.

01 Subscribe to this MCP and provide your AT&T 5G API Access Token.

02 Your AI client connects the token, giving it full access to the network APIs.

03 You query for specific network information—like running a SIM swap check or creating a new slice—using natural language prompts.

The bottom line is: your agent handles all the complex API calls and data interpretation so you just get clear answers about the network status.

Built For

This MCP targets specialized technical roles that deal with high-stakes connectivity, security, and massive infrastructure. If your job involves guaranteeing uptime, detecting fraud across state lines, or optimizing mission-critical device performance, you need this.

Security Engineer

Needs to enforce geo-fencing policies, confirm user identities without relying on SMS OTPs, and proactively block SIM swap fraud attempts.

Network Architect

Must provision dedicated 5G network slices for private enterprise use or monitor the health of existing service level agreements (SLAs).

Product Manager (IoT/Mobile)

Needs to integrate location-aware features into a mobile app, optimize real-time performance, or manage complex international roaming billing.

What Changes When You Connect

01 Fraud Mitigation: Instead of relying on slow SMS methods, you can use the `verify_number` tool to confirm a user's identity instantly, improving login security.

02 Resource Control: You gain full control over network capacity. With `create_network_slice`, architects can deploy private 5G networks for critical operations, guaranteeing performance where it matters most.

03 Operational Visibility: The `list_network_sessions` tool gives you a clear audit trail of premium service usage, making billing and troubleshooting straightforward.

04 Enhanced User Experience: By using `request_quality_on_demand`, product teams can ensure that high-priority tasks—like video calls or AR experiences—always get the low latency they need.

05 Proactive Security: The `check_sim_swap` tool lets you build fraud prevention directly into your user flow, catching account takeovers before they happen.

Real-World Applications

Onboarding a New Enterprise Client

A network architect needs to set up a private campus network. They prompt their agent: 'Create a low-latency slice for 50 devices.' The agent uses `create_network_slice` and reports the new Slice ID and provisioning status, letting them confirm the deployment immediately.

Mitigating Account Takeovers

A security engineer detects suspicious login attempts. They ask the AI to run a SIM swap check on the user's number using `check_sim_swap`. If recent swaps are found, they can immediately flag the account and prevent password resets.

Optimizing Live Video Conferencing

A product team needs to test a new video feature. They ask their agent to run `request_quality_on_demand` with 'high_throughput' profile for the session, guaranteeing stable bandwidth during testing.

Auditing Roaming Costs

A product team member needs to check billing rules for a user traveling abroad. They use `check_roaming_status` and get an instant answer on whether the device is roaming, allowing them to apply correct international rates.

Patterns to Avoid

Using Location Data for GPS

✗ AVOID

Assuming that calling `get_device_location` provides precise, real-time GPS coordinates like a dedicated mapping API. This will fail or return wildly inaccurate data.

✓ INSTEAD

Remember this service uses network cell tower triangulation; it's for approximate geography only. Use the location to define a general area (geo-fencing), not to track specific movements.

Over-relying on SMS Authentication

✗ AVOID

Forcing users through an OTP flow just because they logged in from a new device, which is frustrating and often fails due to network issues.

✓ INSTEAD

Use the `verify_number` tool instead. It silences the process by confirming the number matches the device currently connected on the AT&T 5G network.

Ignoring Resource Cleanup

✗ AVOID

Creating a temporary, high-cost network slice for testing and then forgetting to decommission it, leading to unexpected monthly bills.

✓ INSTEAD

Always pair `create_network_slice` with a cleanup step. Use the `delete_network_slice` tool immediately after your test is complete.

The Right Fit

Use this MCP if your core business logic relies on deep, real-time network status checks or device connectivity validation. You need to know *where* a device is, *if* its connection is secure, or *what kind* of dedicated bandwidth it needs for a specific service (e.g., gaming vs. video). However, don't use this if your primary goal is simple data storage or general mapping; you can get basic location approximations from other APIs. If you just need to list users and check emails, stick with a CRM MCP instead. This tool is purely for telecommunications infrastructure control.

AT&T 5G MCP: Managing Network Slices and Fraud Detection

Today, managing enterprise connectivity feels like playing whack-a-mole. You have to jump between billing systems to check roaming rules, then log into a separate security console just to run a SIM swap detection audit, and finally use an entirely different dashboard just to confirm if the network slice you paid for is actually running at the guaranteed low latency. It’s manual, slow, and prone to human error.

With this MCP, your agent handles it all in one conversation. You don't click through tabs; you ask a question. The system runs `check_sim_swap` alongside checking the network status via `check_roaming_status`, giving you an immediate, consolidated verdict on security and cost compliance.

AT&T 5G MCP: Ensuring Guaranteed Bandwidth Performance

Before this, guaranteeing performance meant over-provisioning—paying for massive excess capacity just in case a critical session spiked. You’d run tests manually and have to wait hours for network engineers to audit the usage logs using `list_network_sessions` before you knew if your SLA was actually being met.

Now, you can tell your agent, 'Guarantee us ultra-reliable transmission for this hour.' The system executes `request_quality_on_demand`, provisions exactly what's needed, and lets you monitor the health in real time. It cuts out guesswork; it gives you guaranteed performance.

AT&T 5G MCP with 9 Tools for Network Slicing

These tools let your agent monitor connectivity, audit usage logs, detect fraud, and build custom network segments across the AT&T 5G infrastructure.

#	TOOL	DESCRIPTION
01	`check_roaming_status`	Checks if an AT&T device is connected to a foreign network, which helps apply the right billing rules or reroute traffic.
02	`check_sim_swap`	Determines if a SIM card has been recently swapped for fraud prevention purposes by looking at recent account activity.
03	`create_network_slice`	Builds and deploys an entirely new, private 5G network segment optimized for specific enterprise needs or IoT devices.
04	`delete_network_slice`	Decommissions and removes a dedicated 5G network slice to stop incurring unnecessary costs.
05	`get_device_location`	Gets an approximate geographic position of the device using cell tower data, useful for localized content or emergency services.
06	`get_network_slice_info`	Retrieves detailed specifications and current status (SLAs, resources) of a specific 5G network slice you've deployed.
07	`list_network_sessions`	Provides an audit log listing all active or historical premium service sessions for usage tracking and troubleshooting.
08	`request_quality_on_demand`	Guarantees a specific network quality profile (low latency, high bandwidth) for the duration of a critical user session.
09	`verify_number`	Confirms a user's phone number matches their device without requiring an SMS code, making login frictionless.

See It in Action

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

U Does user 555-1234 have any fraud flags or recent SIM swap activity?

SIM Swap Audit Report

- **Target Number:** +1 (555) 123-4567
- **Last Detected Swap:** N/A (Clean)
- **Fraud Risk Score:** Low.

Status: The number shows no recent swap activity, and the last recorded change was over 90 days ago. It's safe to proceed with identity verification.

U We need to run a high bandwidth test for our new video feature. Can you set up the network slice?

Network Slice Provisioning Initiated

The following dedicated slice is being provisioned:

- **Slice Name:** VideoTest-Alpha
- **SLA Profile:** High Throughput (Video)
- **Status:** Pending Deployment.
- **Estimated ID:** NS-b4c2e9

Please wait 15 seconds for the slice to become fully active and ready for testing.

U What is the approximate location of this device and how much does it cost to operate in this country?

Device Location & Billing Check

- **Location:** 34.0522, -118.2437 (Los Angeles Area)
- **Accuracy:** +/- 200 meters.
- **Roaming Status:** No. Device is on a domestic AT&T network.
- **Billing Implication:** Standard US rates apply. No special international fees are triggered.

Frequently Asked Questions

01 **How do I prevent my account from being taken over using the AT&T 5G MCP?**

You can proactively audit for fraud by checking SIM swap history. This tool detects if a card has been recently swapped, allowing you to block suspicious login attempts before they succeed.

02 **Can I guarantee bandwidth for my real-time app using the AT&T 5G MCP?**

Yes. You can request guaranteed network quality profiles (like low latency or high throughput) for specific sessions, ensuring your critical application always performs optimally.

03 **What is the best way to verify a user's phone number without asking them for an SMS code?**

You can use the dedicated number verification tool. It confirms that the phone number matches the device currently active on the AT&T 5G network, providing secure login paths without sending texts.

04 **How do I set up a private 5G network for my company's campus?**

You use the dedicated slicing tools to provision your own isolated network segment. This gives you full control over performance and security, perfect for enterprise deployments.

05 **Does AT&T 5G MCP help me track billing when users travel internationally?**

Yes. It checks the device's roaming status instantly, allowing your system to apply the correct international billing rates or flag potential overage fees immediately.

06 **What is network slicing and why do I need it for my IoT devices?**

Network slicing builds dedicated digital lanes on the 5G network. For IoT, this means you isolate critical deployments from general traffic, guaranteeing connectivity even during peak usage.

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-5g": { "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 5G 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 5G. 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 5G MCP
Server ID	`019d7554-a87c-70ca-bf68-ea92d0048637`
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-5g.