MCP SERVER | NO CODE | CLOUD HOSTED

IPinfo MCP

Audit IPs, ASNs, and network metadata instantly.

IPinfo lets you conduct deep network audits instantly. Your agent can geolocate IPs, check Autonomous System Numbers (ASN) for ownership details, and determine if an IP is a proxy or VPN exit node—all without needing to touch a terminal or read documentation. Use this MCP to analyze vast amounts of IP data for security research, infrastructure planning, and risk management.

A+ Quality Score 100/100

ip-geolocation | asn-lookup | network-intelligence | privacy-metadata | cybersecurity | data-enrichment

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

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

IPinfo MCP

6 tools available
Cloud-hosted on Vinkius

Need to understand where an IP address really comes from? This MCP connects your AI agent to industry-leading network intelligence, letting you query complex geographical and ownership data conversationally. Instead of jumping between spreadsheets and specialized lookup tools, you ask your agent a question—'Is this range associated with known proxy networks?'—and it handles the whole audit process. You get instant answers on city location, ISP details, or if the IP is flagged as private or VPN-related.

When you connect this MCP via Vinkius, your AI client acts like a full-time network analyst for you. You can analyze an entire CIDR block to see where all its IPs land geographically, or check the historical data on a single address. The result is immediate, high-fidelity intelligence that helps ground your work in verifiable facts, whether you're monitoring user traffic or building secure infrastructure.

Core Capabilities

01 — Audit IP location and network details

Retrieves full geographic data for a specific IP address, including city, region, and ISP.

02 — Identify ownership via ASNs

Looks up Autonomous System Numbers (ASN) to determine the corporate or network entity that owns the IP range.

03 — Check for privacy masking

Determines if an IP address is linked to VPN, proxy, or Tor exit nodes.

04 — Analyze entire IP ranges

Gathers metadata across a CIDR block or specified range of IP addresses.

05 — Audit current system connection

Pulls specific network details about the IP address currently running your agent.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your IPinfo Access Token.

02 Connect the MCP to your preferred AI client (Claude, Cursor, etc.) via Vinkius.

03 Ask your agent a question like, 'Check the location and ASN details for 10.0.0.1' to execute the network audit.

The bottom line is that you tell your AI client what network information you need, and it handles all the complex data lookups using this MCP.

Built For

This MCP is essential for security researchers who hunt threats, data engineers building reliable systems, risk managers auditing compliance, or ops leads needing real-time network visibility. Stop relying on partial reports and start asking your agent deep questions about connectivity.

Security Researcher

Identifies malicious IPs or suspicious traffic patterns by checking for proxy usage or unusual ASNs.

Data Engineer

Verifies user geolocation accuracy and audits network routing data to ensure performance standards are met.

Risk Manager

Performs rapid, automated audits of IP privacy settings or compliance requirements using natural language prompts.

Operations Lead

Automates network data querying to maintain strict control over the organization's infrastructure environment.

What Changes When You Connect

01 Stop guessing about data source location. Use get_ip_details to pinpoint the exact city, region, or ISP for any IP address in seconds.

02 Automate ownership checks with get_asn_details. You can immediately verify which large organization owns a network block without leaving your workflow.

03 Audit user traffic integrity using get_privacy_details. Quickly spot if an IP is masked by a proxy or VPN, improving threat detection.

04 Manage infrastructure risk by running get_ip_range. Check entire CIDR blocks at once to understand regional allocations and compliance boundaries.

05 Maintain full control over your setup. Use get_own_ip_details whenever you need absolute certainty about the connection environment your agent is operating from.

Real-World Applications

Investigating Suspicious User Traffic

A security analyst notices a spike in traffic from an unknown source. The agent uses get_ip_details and get_privacy_details to confirm the IP isn't using common VPN exit nodes, narrowing the investigation scope immediately.

Verifying New Infrastructure Deployments

A data engineer needs to ensure a new regional deployment uses IPs from an approved block. They run get_ip_range on the CIDR and use get_asn_details to confirm the ownership aligns with corporate records.

Auditing Compliance for Third Parties

A risk manager needs proof that a vendor's connection IPs are not masked. The agent executes multiple checks using get_privacy_details across various IP ranges to generate an audit trail.

Troubleshooting Connection Failures

An ops lead suspects connectivity issues. Instead of manual diagnostics, they run get_own_ip_details to confirm the current server connection is operating from the expected physical location and ISP.

Patterns to Avoid

Treating it like a simple search query

✗ AVOID

Just pasting an IP address into a general chat prompt and hoping for full network context. This only gives partial, often outdated data.

✓ INSTEAD

Structure your request to use specific tools. To get the best results, ask the agent to run both get_ip_details AND get_asn_details on the target IP.

Checking single IPs only

✗ AVOID

Only checking a few random addresses when diagnosing a large-scale network problem. This misses the scope of the issue.

✓ INSTEAD

For comprehensive coverage, use get_ip_range to analyze the entire CIDR block instead of just spot-checking individual addresses.

The Right Fit

Use this MCP if your task requires verifiable data about network ownership, physical location, or connection masking. Think 'network forensics' or 'infrastructure auditing.' You need to know *who* owns the IP (use get_asn_details) and *where* it is physically located (use get_ip_details). Don't use this if you are trying to retrieve internal document knowledge or summarize unstructured text; those tasks require general retrieval tools. If your goal is simply writing code,

stick to standard programming libraries; if the goal is understanding network topology, this MCP is what you need.

The headache of manual IP investigation

Right now, auditing a single connection means opening three different browser tabs: one for geolocation, one for ASN lookup, and another to check if it's flagged as a proxy. You copy the IP, paste it into each tool, wait for page loads, then manually cross-reference city names and ownership IDs before you even start writing a report.

With this MCP, your agent handles the whole process in one conversation. You ask a question—for example, 'What's the privacy status of 192.0.2.1?'—and it executes all necessary lookups behind the scenes. The answer is instant, complete, and ready for you to use.

IPinfo MCP: Network Intelligence at Your Fingertips

You ditch the copy-pasting across multiple services. You skip opening separate terminal windows just to run a basic lookup. The AI client manages all the complexity, running tools like get_ip_details and get_asn_details automatically.

It’s not just faster; it's more reliable. You are getting comprehensive, verified network intelligence delivered directly into your natural language workflow.

IPinfo: 6 Tools for Network Analysis

These tools let you perform every type of deep network audit imaginable, from checking a single IP's location to analyzing vast CIDR blocks.

#	TOOL	DESCRIPTION
01	`get_asn_details`	Retrieves specific ownership and details for any given Autonomous System Number (ASN).
02	`get_ip_details`	Gets the full geographic, network, and ISP information for a single IP address.
03	`get_ip_historical`	Retrieves past data points or changes associated with an IP address (requires proper plan).
04	`get_ip_range`	Gathers metadata and details for a defined range of IPs or CIDR block.
05	`get_own_ip_details`	Fetches the specific network and location data for the machine running your agent right now.
06	`get_privacy_details`	Checks if a given IP address is known to belong to a VPN, proxy, or Tor service.

See It in Action

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

U Geolocate the IP address 1.1.1.1 using IPinfo.

I've geolocated the IP! It is located in Research, Victoria, Australia. The provider is identified as Cloudflare. Would you like the full network and ASN details?

U Check if IP 8.8.8.8 is using a VPN.

I've checked the privacy settings for 8.8.8.8. It is not identified as a VPN, proxy, or Tor exit node. It is a public DNS IP provided by Google. Would you like to see the ASN info?

U Show ASN details for AS15169.

I've retrieved the details for AS15169. It belongs to Google LLC and has over 15 million IPs allocated. Would you like to see the domains associated with this ASN?

Frequently Asked Questions

01 **How does IPinfo MCP help with geolocation?**

The get_ip_details tool retrieves the full geographic information for any IP address, providing city, region, and ISP data points right away.

02 **Can I check if an entire range of IPs is private or masked using IPinfo MCP?**

Yes. You can use get_ip_range to analyze a CIDR block, and then leverage the privacy checking capabilities to audit the whole spectrum for VPNs or proxies.

03 **What is the difference between get_ip_details and getting my own IP?**

get_ip_details works on any arbitrary IP you provide. If you want to know details about the machine running your agent, use get_own_ip_details.

04 **Is this MCP useful for checking network ownership?**

Absolutely. Use the get_asn_details tool whenever you need to confirm which corporation or entity owns a specific Autonomous System Number (ASN).

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 `"ipinfo": { "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

IPinfo 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 IPinfo. 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	IPinfo MCP
Server ID	`019d8449-355c-7135-ae8c-fe0cf4765323`
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/ipinfo.