MCP SERVER | NO CODE | CLOUD HOSTED

IP2WHOIS MCP

Find ownership and status data for any domain.

IP2WHOIS delivers instant domain intelligence by querying comprehensive WHOIS data at scale. Look up full registration records, determine ownership contacts, calculate domain age, and monitor expiration dates for any TLD. It also helps you identify all domains attached to a specific IP address or confirm if a domain is available for immediate registration.

A+ Quality Score 100/100

whois | domain-intelligence | dns-lookup | registration-data | domain-age | api-integration

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/ip2whois

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.

IP2WHOIS MCP

10 tools available
Cloud-hosted on Vinkius

Running domain intelligence checks used to mean opening dozens of browser tabs, copy-pasting URLs into multiple lookup sites, and cross-referencing spreadsheets. Now your agent handles it all in one go. This MCP connects deep domain data directly from IP2WHOIS. You can ask your AI client to run a full WHOIS lookup on several domains simultaneously or check the exact expiration date for renewal monitoring. Need to know if a name is free? Just ask it to check availability, and you get an instant answer. The system also pulls key registrar details and nameserver configurations so you always know where a domain points. Because Vinkius hosts this MCP, your agent gets immediate access to all these powerful tools without needing separate credentials or complex integrations.

Core Capabilities

01 — Analyze multiple domains at once

Send up to 10 different domain names in a single query and receive key registration details for every one.

02 — Check domain availability instantly

Determine right away if a specific domain name is free to register.

03 — Get full ownership records

Retrieve complete WHOIS information, including registration dates and the registrar for any domain.

04 — Track expiration timelines

Check when a domain expires and how many days are left until renewal is needed.

05 — Identify hosting infrastructure

Find all other domains that share the same IP address, which is useful for auditing shared hosts.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/ip2whois** — connect your AI agent in three steps.

01 You subscribe to this MCP and enter your unique API key.

02 Your AI client sends a prompt—for example, asking for the WHOIS data on five specific domains.

03 The MCP executes the necessary lookups and returns structured domain intelligence directly into your chat or workflow.

The bottom line is that you get complex internet infrastructure data delivered through simple conversation prompts.

Built For

This MCP is essential for security researchers, domain investors, and IT administrators who need to audit network assets or investigate ownership structures quickly. Stop juggling tabs; let your agent do the heavy lifting.

Security Researcher

Uses this to investigate domain ownership history, map out potential infrastructure targets, and check for suspicious name server configurations.

Domain Investor

Runs checks on multiple domains simultaneously and monitors expiration dates to identify names that are about to drop or become available.

IT Administrator

Audits shared hosting environments by running lookups against a specific IP address to see every domain attached to it.

What Changes When You Connect

01 Saves time by running bulk lookups. Instead of checking domains one by one, use `bulk_whois_lookup` to process up to 10 names instantly, getting key registration details for all at once.

02 Better risk management through expiry monitoring. You can set up workflows that regularly check domain expiration using `check_domain_expiry`, ensuring no critical asset is forgotten.

03 Deep infrastructure analysis when combined with other tools. Run `lookup_hosted_domains` to map out every single domain connected to a suspicious or shared IP address.

04 Immediate market intelligence for investors. Use `check_domain_availability` before proposing a name, and use `get_domain_contacts` to understand who owns the current records.

05 Comprehensive record keeping. Combine `lookup_domain_whois` with `get_registrar_info` to build a complete audit trail of ownership, status, and registration dates for any target.

Real-World Applications

A security researcher needs to map an entire subnet.

The agent runs the `lookup_hosted_domains` tool against a given IP address block. It receives a list of every domain name hosted there, allowing the researcher to instantly scope the size and scope of the attack surface.

A domain investor is vetting a cluster of potential names.

Instead of manual checks, the agent executes `bulk_whois_lookup` on 10 target domains. It filters the results to find those with unusual ownership patterns or long-term availability.

An IT admin needs to audit a shared hosting account.

The administrator uses `get_nameservers` to confirm which nameservers are authoritative for all client domains, verifying that the hosting environment is configured correctly and securely.

A business owner wants to know if their target domain name is available.

The agent first runs `check_domain_availability` on a new name. If it's free, they then run `get_domain_contacts` to see what kind of registration data the registrar requires for purchase.

Patterns to Avoid

Treating domain lookup like general web search

✗ AVOID

Asking your agent, 'Tell me everything about this website.' You get a generic summary that misses key technical data points like the registrar or ownership dates.

✓ INSTEAD

Be specific. If you want WHOIS details, use `lookup_domain_whois`. If you only care about who owns it, run `get_domain_contacts`.

Forgetting to check domain age

✗ AVOID

Assuming a newly registered site is safe just because the owner contact info looks clean. You don't know how old the underlying name is.

✓ INSTEAD

Always run `check_domain_age` first. Knowing if a domain was active for 10 years or 1 week changes your entire interpretation of its ownership.

Ignoring potential IP sharing

✗ AVOID

Only checking the WHOIS record for one specific domain, missing out on other unrelated domains hosted on the same physical server.

✓ INSTEAD

Run `lookup_hosted_domains` against the IP address to get a full picture of everything running from that location.

The Right Fit

Use this MCP when your primary goal is investigating internet infrastructure, ownership data, or domain status. You need concrete facts: Who registered it? When does it expire? Is it available?

Don't use this if you are trying to find general information about a website (like 'What services do they offer?') — that requires a search engine tool. Don't use it for content generation or writing code.

If your job is pure discovery and auditing, run `bulk_whois_lookup` or `lookup_hosted_domains`. If you are doing targeted research on one name, start with `lookup_domain_whois` to get the full picture.

The Domain Due Diligence Headache

Today, vetting a domain is a tedious process. You copy a URL into Google, then open a separate WHOIS site and paste it in again. If you need to check ten names, that's ten tabs, ten lookups, and three hours of manual cross-referencing across different sites just to get basic ownership data.

With this MCP, you simply prompt your agent. You tell it which domains to investigate, and it runs the necessary checks—from determining if a domain is available using `check_domain_availability` to finding all related assets via `lookup_hosted_domains`. You get structured data in seconds.

IP2WHOIS: Comprehensive Domain Data Retrieval

You no longer have to manually check the registrar and nameservers for every single domain name. The agent gathers this technical metadata, combining `get_registrar_info` with `get_nameservers` automatically.

What changes is that you move from being a data collector to an analyst. You spend your time interpreting what the WHOIS data means, not gathering it.

IP2WHOIS: 10 Tools for Domain Data Retrieval

These tools let your agent perform specific actions like checking domain age or finding nameservers, giving you granular control over domain data retrieval.

#	TOOL	DESCRIPTION
01	`check_domain_availability`	Determines if a specified domain name is currently available for registration.
02	`bulk_whois_lookup`	Returns key WHOIS details when you need to check the ownership records of multiple domains at once.
03	`get_domain_contacts`	Retrieves registrant and admin contact information for a domain, if privacy protection hasn't been applied.
04	`check_domain_age`	Calculates the exact age of any given domain name in days or years.
05	`check_domain_expiry`	Checks the expiration date of a domain, which is useful for renewal planning and monitoring.
06	`lookup_hosted_domains`	Finds all domains that are currently hosted on a specific IP address range or block.
07	`get_nameservers`	Retrieves the authoritative nameserver information for any given domain name.
08	`get_registrar_info`	Gathers registrar details and status codes associated with a specific domain registration.
09	`check_ip2whois_status`	Verifies that the IP2WHOIS API connection is properly authenticated and working.
10	`lookup_domain_whois`	Performs a complete, detailed WHOIS lookup on any single domain name.

See It in Action

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

U Look up the WHOIS information for github.com.

Here's the WHOIS record for github.com: Registered on October 9, 2007 (18+ years old), expires October 9, 2026. Registrar: MarkMonitor Inc. Nameservers: dns1.p08.nsone.net, dns2.p08.nsone.net, and more. The domain status is 'clientDeleteProhibited' (protected).

U Check if the domain coolstartup2026.com is available.

The domain coolstartup2026.com appears to be available for registration! No WHOIS record was found, which indicates it has not been registered yet.

U When does google.com expire?

google.com expires on September 14, 2028. That's approximately 866 days from now — no immediate renewal concern. The registrar is MarkMonitor Inc.

Frequently Asked Questions

01 **How do I check if multiple domains are available using IP2WHOIS?**

You use the `check_domain_availability` tool. You just need to list the domain names you want tested, and the MCP will confirm which ones are free for registration.

02 **Can I get ownership information for a large batch of domains with IP2WHOIS?**

Yes. Use `bulk_whois_lookup` to query multiple domains in one operation, saving you from having to run the full lookup individually.

03 **What is the difference between `lookup_domain_whois` and `get_registrar_info`?**

`lookup_domain_whois` provides the entire record (contacts, dates, nameservers). `get_registrar_info` focuses specifically on the registrar details and status of that domain.

04 **How does IP2WHOIS help me analyze shared hosting?**

You run the `lookup_hosted_domains` tool against an IP address. This reveals every single other domain name using that same infrastructure, which is key for auditing purposes.

05 **Does IP2WHOIS only work with public TLDs?**

No. The MCP handles full WHOIS lookups and general domain intelligence regardless of the top-level domain type you are investigating.

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 `"ip2whois": { "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

IP2WHOIS 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 IP2WHOIS. 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	IP2WHOIS MCP
Server ID	`019dd10d-4bfa-729f-bbec-c957e2f3740a`
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/ip2whois.