MCP SERVER | NO CODE | CLOUD HOSTED

Cloudflare MCP for AI Agents

Automating DNS Records and CDN Security Audits

The Cloudflare MCP gives your AI agents full control over your edge infrastructure, including DNS records, Workers, KV storage, and WAF rules. You can audit CDN performance, deploy configurations, and manage load balancers entirely through natural conversation, eliminating the need to click through dashboards.

A+ Quality Score 98.33/100

dns-management | cdn | edge-computing | firewall | serverless | network-security

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

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.

Cloudflare MCP

15 tools available
Cloud-hosted on Vinkius

Managing a modern web stack means juggling multiple services: DNS changes, updating serverless functions, adjusting firewall policies. This MCP lets your AI agent handle all of it. Instead of opening 10 different tabs in the Cloudflare dashboard, you talk to your client and tell it what needs fixing or changing. It handles everything from listing basic records (A, CNAME, MX) to writing configuration data into KV namespaces for Workers. Need to check if traffic is coming through the CDN? You can run those analytics reports instantly. Want to audit who's calling your services? The agent reviews every firewall rule and even checks which workers are deployed across your account. This level of deep control over DNS, edge computing, and security was once reserved for dedicated DevOps tooling; now you get it right inside any MCP-compatible client through Vinkius. It turns complex infrastructure management into a simple conversation.

Core Capabilities

01 — Manage Domain Name System (DNS) Records

You can list, create, update, and delete all types of DNS records while controlling settings like TTL and whether traffic is proxied through the CDN.

02 — Audit Network Security and Firewall Rules

Review every Web Application Firewall (WAF) rule, checking filter expressions, actions, and enabled status to keep your site secure.

03 — Control Edge Computing Workers

List all deployed serverless Worker scripts across your account, including their last deployment time and resource bindings.

04 — Handle Key-Value (KV) Data Storage

Browse KV namespaces or read and write specific key-value pairs needed for feature flags, configuration settings, or cached data.

05 — Monitor CDN Performance Analytics

View comprehensive traffic data, including request counts, bandwidth usage, threat mitigation efforts, and cache ratios.

06 — Inspect Load Balancer Configurations

Check the health status of load balancers, reviewing origin pools and traffic steering policies to ensure high availability.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and provide your Cloudflare API Token.

02 Connect the token via any MCP-compatible client (like Cursor or Claude).

03 Ask your agent for the specific action, like 'List all A records for my main domain' or 'Update the rate limit rule'.

The bottom line is that your AI client uses your API credentials to speak directly with Cloudflare services and execute infrastructure changes on your behalf.

Built For

This MCP is built for technical roles who spend too much time clicking through complex, multi-page vendor dashboards. If you're a Security Engineer tired of manually checking every WAF rule, or a DevOps specialist needing to deploy DNS changes without leaving your terminal, this tool saves serious time.

DevOps Engineer

Manages complex infrastructure tasks, such as deploying Workers, auditing firewall rules, and updating critical DNS records from a single command line.

Security Analyst

Reviews WAF configurations and CDN analytics to quickly identify potential threats or suspicious traffic patterns at the edge.

Full-Stack Developer

Reads and writes KV data for Worker configuration, checks Pages deployments, and inspects load balancer health before committing code.

What Changes When You Connect

01 Audit your entire network stack without leaving the chat window. You can view everything from `list_dns_records` to `list_firewall_rules`, all in one go.

02 Speed up deployment cycles by automating changes. Use `create_dns_record` or `update_dns_record` instantly instead of manually logging into a web dashboard.

03 Keep your edge secure and compliant. Review WAF settings using `list_firewall_rules` to ensure all security policies are correctly implemented at the source.

04 Manage configuration data reliably. Quickly read or write feature flags and cached content using `get_kv_value` and `put_kv_value` for Workers.

05 Understand traffic flow instantly. View detailed CDN metrics via `list_zone_analytics`, giving you clear data on performance and threat mitigation.

Real-World Applications

Debugging DNS Failures

A developer notices a service is unreachable. Instead of checking multiple records, they ask their agent to run `list_dns_records` for the zone and compare the result against the expected setup, pinpointing which record type or proxy status needs fixing.

Responding to Security Alerts

The security team gets a warning about potential bot traffic. They prompt their agent to run `list_firewall_rules` and check the current WAF action, then use `update_dns_record` to implement an immediate block if needed.

Updating Worker Feature Flags

The product manager needs to activate a new feature flag for testing. They ask their agent to read the current namespace via `list_kv_namespaces`, and then use `put_kv_value` to flip the required boolean switch.

Initial Infrastructure Audit

A new team member takes over a project. They ask their agent to run `list_zones` first, and then gather all active Workers using `list_workers`, getting a full inventory of the current edge setup.

Patterns to Avoid

Manual Dashboard Crawling

✗ AVOID

Trying to check DNS records, firewall rules, and KV data separately by clicking between different tabs in the Cloudflare dashboard. This is slow and prone to human error.

✓ INSTEAD

Use your agent to run `list_dns_records` for a full list of domain pointers, then use `list_firewall_rules` next. By chaining these calls, you get all necessary audit data without leaving the chat.

Assuming Records Are Correct

✗ AVOID

A developer assumes an old record is still active and doesn't check its current status or proxy setting before deploying new code.

✓ INSTEAD

Always use `list_dns_records` first. This lets you verify the type, name, content, and proxied status of existing records before attempting any writes with `update_dns_record`.

Writing Credentials Manually

✗ AVOID

Typing API tokens or credentials into code blocks to test connectivity, which is a major security risk.

✓ INSTEAD

Connect your account once and securely through Vinkius. Your agent handles the token management, allowing you to focus purely on the infrastructure commands like `create_dns_record`.

The Right Fit

Use this MCP if your workflow involves making structured changes across multiple Cloudflare services: DNS records, Workers configuration (KV data), and security policies (WAF/CDN). It's perfect for DevOps teams that need to audit or deploy entire stacks from a single interface. Don't use it if you only need simple information retrieval about a non-Cloudflare service—you'd be better off with a dedicated platform tool. If your goal is just reading basic domain status, `list_zones` works great, but if you plan on writing records or checking firewall rules, this MCP is what you need.

Cloudflare MCP for AI Agents: Auditing DNS Records and CDN Security

Today, auditing your domain's pointers means jumping into the Cloudflare dashboard. You check DNS records for typos, then open another tab to view WAF rules, and maybe a third to inspect traffic analytics. It’s a frustrating cycle of clicking through pages just to confirm basic operational health.

With this MCP, you ask your agent to run `list_dns_records` and immediately get all current pointers in one response. Then, running `list_firewall_rules` provides the security context right below it. You get a complete picture of your domain's setup without ever leaving your terminal.

Cloudflare MCP for AI Agents: Managing Workers and KV Data

Managing edge data requires logging into the Worker dashboard to see what namespaces are used, then opening a separate console to read or write key-value pairs. This manual process is slow, especially if you're trying to debug why a feature flag isn't flipping.

The agent lets you first run `list_kv_namespaces` to know where the data lives, and then use simple commands like `get_kv_value` or `put_kv_value`. You manage your entire edge data layer—the configuration, the flags, the cache—with conversational precision.

Cloudflare Alternative: 15 Tools for Edge Computing and DNS Management

These tools allow your agent to perform every major infrastructure task, from creating a simple record to auditing complex load balancer configurations.

#	TOOL	DESCRIPTION
01	get_zone_analytics	Audits CDN performance by retrieving traffic analytics to identify spikes or review threat mitigation statistics.
02	create_dns_record	Creates a new DNS record in a zone, allowing you to define the type, hostname, content, and proxy status.
03	delete_dns_record	Permanently removes an existing DNS record from the specified cloudflare zone.
04	list_dns_records	Retrieves a list of all configured records for a zone, including their type and proxy status.
05	list_firewall_rules	Lists every Web Application Firewall rule in a zone, showing its filter expression and defined action (block, challenge, allow).
06	get_kv_value	Reads the value associated with a specific key name within a designated KV namespace.
07	get_zone	Fetches detailed information about a specific Cloudflare zone using its ID.
08	list_cloudflare_ips	Retrieves the official IP address ranges for Cloudflare, useful for setting up origin firewall allow-lists.
09	list_kv_namespaces	Lists all available KV namespaces used for edge data and configuration storage within your account.
10	list_load_balancers	Displays load balancer details, including target pools and current health status across a zone.
11	list_pages_projects	Lists all Cloudflare Pages deployments connected to Git repositories, showing their build status and source branch.
12	put_kv_value	Writes or updates a value in a specific KV namespace using the required key name.
13	update_dns_record	Modifies existing DNS records by updating fields like content, TTL, or proxy status.

#	TOOL	DESCRIPTION
14	list_workers	Lists all deployed Worker scripts in your account, showing deployment times and resource usage.
15	list_zones	Retrieves a comprehensive list of every domain zone managed by Cloudflare.

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 my A records and tell me which ones are using the proxy.

DNS Records for example.com

- `app` : 203.0.113.10 (Proxied)
- `api` : 203.0.113.11 (Proxied)
- `staging` : 203.0.113.20 (DNS only)

Three records found. Do you want to update the proxy status for any of these?

U What are the top three security rules and what do they do?

Active WAF Rules

The following rules define your current web application firewall policy:

1. **Block known bots**: Blocks traffic from recognized bad actors (Action: Block, Status: Enabled).
2. **Rate limit /api**: Challenges IPs hitting the API endpoint over 1000 requests/5min (Action: Challenge, Status: Enabled).
3. **Allow internal IP range**: Permits your team's IP addresses globally (Action: Allow, Status: Enabled).

U I need to set the feature flag for beta users in my worker.

KV Storage Update

Namespace `worker-config` :
Key: `beta_enabled`
 Value: `true` (Successfully written)

The update is complete. Beta features are now active across your edge network.

Frequently Asked Questions

01 **How can I check my DNS records using the Cloudflare MCP for AI Agents?**

You simply ask your agent to list all records or filter by type. It will show you every A, CNAME, and MX record currently configured in your zone, letting you confirm pointers are correct without manually visiting the dashboard.

02 **Can this MCP help me manage my Workers configuration?**

Yes. You can list all deployed workers to see their status, or use KV functions to read and write feature flags and configuration data used by those worker scripts.

03 **Does the Cloudflare MCP for AI Agents help with security auditing?**

It's perfect for security. You can review every single firewall rule, see who is blocked or challenged, and audit your CDN analytics to spot unusual traffic spikes or threat activity.

04 **What if I need to change a DNS record? Is it safe?**

The agent allows you to update specific records by providing the necessary IDs. It's highly controlled, letting you only modify fields like TTL or content, minimizing the risk of breaking your site.

05 **Is this MCP for AI Agents compatible with my current development environment?**

Since it runs through Vinkius and utilizes the open Model Context Protocol (MCP), it connects to any client that speaks the standard language, including Cursor, Claude, or VS Code extensions.

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 `"cloudflare-alternative": { "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

Cloudflare 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 Cloudflare. 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	Cloudflare MCP
Server ID	`019d8426-d134-725f-b107-c354b0453ab9`
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/cloudflare-alternative.