MCP SERVER | NO CODE | CLOUD HOSTED

WordPress Plugin Auditor MCP

Audit Site Plugins Securely. No Admin Passwords Needed.

WordPress Plugin Auditor provides your agent with secure, read-only access to list every plugin on a WordPress site. It returns the name, version number, author, and whether each plugin is active or inactive. Use this MCP for quick security sweeps, compliance checks, and generating detailed maintenance reports without ever needing full admin credentials.

A+ Quality Score 100/100

plugin-management | security-audit | maintenance | vulnerability-scanning | site-health

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/wordpress-plugin-auditor

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.

WordPress Plugin Auditor MCP

1 tools available
Cloud-hosted on Vinkius

Managing multiple client websites means juggling dozens of plugins. You don't want to give your AI agent the master admin password just to check if a couple of things are outdated or inactive. This MCP solves that risk by giving your agent specific, read-only access.

It lets you ask questions like, "Which plugins haven't been used in three months?" and instantly get a structured list detailing every plugin’s status and version. It works entirely on the assumption that the data is for viewing—the AI client can check inventory, but it cannot delete anything or change settings. This secure scoping is vital when dealing with sensitive client sites.

If you're used to manually logging into WordPress dashboards just to pull a list of plugins, this changes that. You connect your preferred agent through Vinkius, and the auditing capability becomes an immediate tool in your workflow, letting you gather all necessary plugin metadata for maintenance reporting or vulnerability assessments without touching a single core file.

Core Capabilities

01 — Generate Plugin Inventory

Lists every installed WordPress plugin, providing its name, version number, author, and operational status.

02 — Identify Inactive Plugins

Checks the site to pinpoint plugins that are currently disabled or unused, helping focus cleanup efforts.

03 — Create Maintenance Reports

Gathers structured data on all active and inactive components needed for client-facing status reports.

04 — Audit Security Status

Performs a quick sweep to check plugin statuses, assisting in vulnerability or cleanup planning.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/wordpress-plugin-auditor** — connect your AI agent in three steps.

01 Your agent sends a request asking for a site audit, specifying which plugins' data it needs.

02 The MCP securely executes the read-only query against the WordPress environment.

03 You receive a structured list containing all plugin names, versions, authors, and their current active/inactive status.

The bottom line is: you get an instant, comprehensive inventory of every installed plugin's details without needing to log in or risk making changes.

Built For

This MCP is for web agencies, security consultants, and technical leads. It helps people who spend too much time jumping between dashboards just to compile a simple list of installed software.

Web Development Agency Owner

Uses this to run pre-audit checks when onboarding a new client, ensuring all legacy plugins are accounted for before migration.

Security Consultant

Runs quick audits on client sites to identify outdated or inactive components that could pose a security risk.

Technical Operations Manager (DevOps)

Uses it for routine maintenance reporting, automatically generating the data needed to update clients on their site's overall plugin health status.

What Changes When You Connect

01 Avoid using full admin passwords for simple checks. This MCP uses native WordPress Application Passwords, ensuring the AI client only reads data and never touches core settings or deletes plugins.

02 Stop manual reporting. You can automatically gather a detailed monthly report of all active and inactive plugins, making client communication faster and more reliable.

03 Instantly check for security gaps. Quickly identify unused or outdated plugins that pose a vulnerability risk, giving you a clear list for cleanup.

04 Speed up the audit process significantly. Instead of clicking through multiple plugin menus, your agent retrieves all necessary metadata in one go.

05 Better project scoping. Before building anything, run an audit to understand exactly what components are already active on the client's site.

Real-World Applications

Client Onboarding Audit

A development team needs to know every component on a legacy client site before migration. They use `audit_wordpress_plugins` to get an exhaustive list of all plugins, versions, and statuses. This report allows them to scope the migration effort accurately without ever requesting high-level credentials.

Security Health Check

A security consultant suspects a client has abandoned several old plugins that could be exploited. They run an audit using `audit_wordpress_plugins` and immediately filter the results to show all inactive components, flagging them for immediate removal.

Routine Maintenance Reporting

A web agency owner needs to send a quarterly report detailing site health. They use the MCP's capabilities to generate a structured summary of all active plugins and their versions, making the process automated rather than manual data entry.

Pre-Deployment Readiness Check

Before launching a new feature set, the team needs confirmation that no critical dependencies were accidentally disabled. They run an audit to verify all necessary plugins are listed as active and correctly versioned.

Patterns to Avoid

Trying to delete or update plugins

✗ AVOID

Asking the agent to 'delete old plugins' or 'update plugin X'. This MCP is strictly read-only, so those commands will fail.

✓ INSTEAD

Use `audit_wordpress_plugins` first. Get the list of names and versions. Then, you can pass that structured data to a separate system for manual review or action.

Manually cross-referencing plugin lists

✗ AVOID

Opening three different client dashboards, logging into each one, and copying the list of installed plugins into a spreadsheet.

✓ INSTEAD

Use this MCP to run a single audit across all necessary sites. It aggregates the data automatically, saving hours of tedious clicking.

Assuming full administrative control

✗ AVOID

Treating the result as permission to make changes. The agent can list components, but it cannot modify their status or settings.

✓ INSTEAD

Always remember this is a diagnostic tool. Use `audit_wordpress_plugins` purely for data gathering; any required actions must happen outside of the MCP.

The Right Fit

Use this MCP if your primary need is *knowing* what's installed on a WordPress site, and you absolutely do not want to risk making changes. If your goal is simply auditing status—listing names, versions, and activity—this is exactly right. Don't use it if you need to actually change plugin settings, deactivate components, or install new ones; for those tasks, you require an MCP with write permissions, which this one doesn't provide.

Think of it like checking the contents of a safe without opening it. You get a perfect inventory report every time using `audit_wordpress_plugins`. If you need to actually *take* items out of the safe (i.e., modify data), then look for an MCP with write permissions.

The Plugin Inventory Nightmare

When a client asks, "What plugins do we have?" you usually end up logging into multiple dashboards, navigating through the 'Installed Plugins' screen repeatedly. You copy names and versions from one tab, then switch to another dashboard for a different site, only to find yourself with half-copied data and hours wasted.

With this MCP, your agent handles that tedious work instantly. One prompt retrieves all plugin metadata—name, version, author, status—from every site you connect it to. You get clean, structured data ready for a report in seconds.

Get the Full Plugin Status Report with WordPress Plugin Auditor MCP

The manual steps that vanish are the logins, the dashboard clicks, and the copy-pasting across multiple sites. You no longer have to maintain a personal checklist of every single plugin status.

Now, you simply ask your agent what's wrong with the plugins, and it gives you an immediate, actionable list. The process shifts from tedious data collection to quick diagnosis.

WordPress Plugin Auditor with 1 Tool

Use this single tool to gather comprehensive, read-only data on all plugins across any connected WordPress site.

#	TOOL	DESCRIPTION
01	`audit_wordpress_plugins`	Lists all installed WordPress plugins, returning the name, version, author, and current active or inactive status for each one.

See It in Action

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

U **Can you audit my WordPress site and tell me which plugins are currently inactive?**

I've audited your site. You have 12 plugins installed, and 2 are currently inactive:

1. Hello Dolly (v1.7.2)
2. Classic Editor (v1.6.3)

I recommend deleting these if you no longer use them to improve security.

Frequently Asked Questions

01 **Can WordPress Plugin Auditor MCP delete inactive plugins?**

No, this is a purely read-only tool. It can only audit and report the names, versions, and statuses of installed plugins; it cannot perform any deletion or modification actions.

02 **Does WordPress Plugin Auditor MCP require full admin credentials?**

No. The MCP is designed for secure scoping using native WordPress Application Passwords, meaning you don't have to risk giving out your main administrator password just to read the data.

03 **What information does audit_wordpress_plugins provide?**

The tool provides four key pieces of metadata for every plugin: its name, version number, who wrote it (author), and whether it is currently active or inactive on the site.

04 **Can I use WordPress Plugin Auditor MCP for vulnerability scanning?**

Yes. By providing a complete inventory of names and versions, you can feed that data into other security tools to check for known vulnerabilities associated with those specific plugin versions.

05 **Is this safe for multiple client sites?**

Yes. Because it operates in a read-only capacity using secure scoping methods, it is designed to audit many different WordPress environments without risking data integrity.

06 **Can the AI install or delete plugins with this tool?**

No. This MCP only calls the `GET` endpoint for plugins. It cannot modify your site's plugin configuration.

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 `"wordpress-plugin-auditor": { "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

WordPress Plugin Auditor 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 WordPress Plugin Auditor. 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	WordPress Plugin Auditor MCP
Server ID	`019e390d-33ab-73b7-9a4d-20a63079d645`
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/wordpress-plugin-auditor.