

MCP SERVER

NO CODE

CLOUD HOSTED

WooCommerce MCP

Audit orders and manage your store data via AI.

WooCommerce MCP connects your AI agent directly to your entire e-commerce store backend. You stop logging into dashboards and start asking questions. Your agent can list products, audit historical orders, monitor live system status, and check customer purchase histories—all from a single conversation. Manage everything from sales reports to coupon governance without ever touching the WooCommerce admin panel.

A+ Quality Score 100/100

store-management

sales-reporting

product-catalog

order-tracking

inventory-management

open-source-ecommerce



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

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.

WooCommerce MCP

10 tools available

Cloud-hosted on Vinkius

Running an online shop means juggling dozens of moving parts: inventory levels, pending shipments, marketing promotions, and complex sales data. This MCP turns that entire operational mess into simple commands for your AI client. You tell your agent what you need—like 'What are my top 5 selling products this month?' or 'Check the status of order #90210.' Your agent executes those requests against your live WooCommerce store data and delivers a clean, conversational report back to you. It acts like having an expert operations manager sitting with you, ready to pull up any record instantly. Because Vinkius manages this connection point, all these capabilities are available through one single subscription, letting you focus purely on running the business, not managing the tools.

Whether it's verifying if a new product category was published correctly or finding out why an order is stuck in 'pending,' your agent handles the data retrieval and reporting. It keeps your entire e-commerce workflow visible and actionable right inside your preferred AI chat window.

Core Capabilities

01 — Audit Order History

Retrieve detailed information about specific, recent, or historical orders, including customer details and current status.

03 — Analyze Customer Data

Look up customer profiles and view their complete purchase history to understand buying patterns.

05 — Govern Promotions and Sales

List all active coupons and retrieve detailed sales performance metrics by accessing system reports.

02 — Manage Product Catalog

List all available products and categories to verify product availability, check draft items, or confirm pricing structures.

04 — Check System Health

Get real-time status reports on the store's backend, ensuring everything from database connections to core functions is running smoothly.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP on Vinkius, then provide your store's URL along with the necessary Consumer Key and Secret credentials.
- 02 Connect your preferred AI client (like Claude or Cursor) to the MCP. Your agent now has secure access to the e-commerce backend tools.
- 03 Ask your agent a direct question—for example, 'Show me all orders placed yesterday.' The agent executes the query and presents the results in plain text.

The bottom line is you get immediate, conversational access to deep operational data without ever needing to navigate a complex dashboard.

Built For

This MCP is essential for e-commerce professionals who are tired of manually clicking through dashboards just to answer simple questions. It's perfect for the operations manager, the support agent, or the marketing lead who needs real-time data across products, orders, and customers without logging into a separate admin portal.

Support Specialist

When a customer calls with an order question, you use this MCP to quickly check order status or pull up purchase history for immediate resolution.

Operations Manager

You monitor system health and audit entire categories of products or orders at the end of the day, ensuring fulfillment teams have accurate data before starting work.

Marketing Lead

You verify that new coupons are active and correctly configured across all product lines, or you list available reports to prove campaign ROI.

What Changes When You Connect

-
- 01 Stop clicking through multiple tabs to get a simple answer. You can ask your agent, 'What is the status of order #XYZ?' and immediately get the full details using `get_order`, making customer service faster.

 - 02 Don't waste time manually checking if everything is up-to-date. Use `list_system_status` to confirm the store environment is healthy before a major sale starts, giving you peace of mind.

 - 03 Need to know what products are ready for sale? Instead of browsing product dashboards, simply use `list_products` and get a clean list of everything currently active in your catalog.

 - 04 Marketing campaigns require constant vigilance. You can instantly check all promotions by calling `list_coupons`, ensuring no expired or misconfigured codes affect sales.

 - 05 When an order needs manual status changes, you don't need admin access. Your agent handles the workflow using `update_order` and logs it correctly for your team.
-

Real-World Applications

Investigating a Missing Order

A customer reports they never got an item. Instead of manually checking every record, you ask the agent to find all recent orders and use `get_order` on the relevant IDs to pull up tracking numbers and confirmation details instantly.

Verifying New Inventory

The warehouse team just processed 50 new items. You ask the agent to list all products and check specific ones using `get_product` to confirm they are correctly categorized before listing them for sale.

Quarterly Performance Review

You need data for a board meeting. You instruct your agent to list reports using `list_reports`, then use that information to query sales metrics, building a comprehensive performance summary without ever leaving the chat window.

Handling a Promotion Error

A customer complains that their discount code isn't working. You use the agent to list all coupons and check the rules using `list_coupons` to see exactly why the promotion might be failing.

Patterns to Avoid

Trying to find a product price

X AVOID

Going into the dashboard, clicking 'Products,' filtering by category, and then manually opening each item to check its current cost.

✓ INSTEAD

Just ask your agent to get details for a specific product using `get_product`. It skips all the clicks and gives you the price directly.

Listing customer names

X AVOID

Running a report that takes 10 minutes, exporting it to CSV, then opening Excel just to find one person's purchase history.

✓ INSTEAD

Better yet, ask your agent to list all customers using `list_customers`, and then immediately use `get_order` on their account ID to see the transaction details.

Updating an order status manually

X AVOID

Logging into the admin panel, finding the order, changing the status from 'Processing' to 'Shipped,' and then having to save it.

✓ INSTEAD

Tell your agent to update the order using `update_order`. It executes the change securely on the backend for you.

The Right Fit

Use this MCP if your workflow requires fetching specific, structured data points from an existing e-commerce store (like product prices, customer IDs, or order statuses). If you need to know 'What were

my sales last quarter?'—you should use the `list_reports` tool. But don't use it if all you need is general advice on marketing strategy; this MCP provides data access, not strategic consulting. Also, if you only need a simple list of categories and nothing else, listing them with `list_categories` might be faster than involving your agent. However, if the data retrieval needs to be part of a multi-step process—like 'Find customer X's orders, then update their status,'—this MCP is exactly what you need.

The Dashboard Black Hole

Today, finding basic information requires navigating a labyrinth of tabs and dropdown menus. You open the dashboard, click 'Orders,' filter by date range, then drill down into individual orders to confirm details. If you need product data, you switch tabs again to the catalog, which often doesn't show real-time inventory updates.

With this MCP, all that manual clicking disappears. Your agent reads your request—like 'What was the status of order #123?'—and pulls the answer instantly from the source database and delivers it in plain conversation. You get immediate answers without ever leaving your chat.

WooCommerce MCP: Instant Operational Visibility

The tedious process of compiling reports, cross-referencing customer records against product lists, and verifying coupon rules across multiple admin screens is eliminated. All that complex coordination happens silently in the background.

Now you can manage your entire e-commerce data set with simple conversational prompts. You own the conversation; the MCP handles the complexity.

WooCommerce MCP with 10 Tools

Use these tools to programmatically read and write core store data like customer profiles, order details, product listings, and system reports.

#	TOOL	DESCRIPTION
01	<code>get_order</code>	Pulls specific details for a single order using its unique ID.
02	<code>get_product</code>	Retrieves all information about one particular product by its identifier.
03	<code>get_system_status</code>	Checks the overall operational health and current version of the WooCommerce platform.
04	<code>list_coupons</code>	Lists every active coupon code so you can check promotion rules and expiration dates.
05	<code>list_customers</code>	Provides a list of all registered customers in the store database.
06	<code>list_orders</code>	Generates a summary list of multiple orders, allowing you to see who ordered and when.
07	<code>list_categories</code>	Shows all the major product categories used on your website for organization.
08	<code>list_products</code>	Lists every single product available in your catalog, useful for inventory checks.
09	<code>list_reports</code>	Retrieves a list of all available sales and performance reports from the platform.
10	<code>update_order</code>	Changes the status of an order, such as marking it as 'shipped' or 'cancelled'.

See It in Action

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

U List my last 5 orders in WooCommerce.



I've retrieved your recent orders. You have 5 new transactions, including order #1234 for \$45.00 by John Smith. Would you like the full details for any of them?

U Show me all my draft products.



I've found 3 products in draft status: 'New Hoodie', 'Limited Poster', and 'Demo Shirt'. I can provide category and pricing info for each if you like.

U What is the system status of my store?



Your WooCommerce system status is healthy. Environment: Production, WooCommerce version: 8.5.0, Database status: OK. Is there anything specific you'd like to check?

Frequently Asked Questions

01 Can WooCommerce MCP only list products?

No, it does much more than just listing products. It lets you audit orders using ``list_orders``, check customer history via ``list_customers``, and even update an order's status with ``update_order``.

02 How do I get system health info with WooCommerce MCP?

You use the ``get_system_status`` tool. This function checks the overall operational integrity of your store, telling you if the database connection or platform version is running correctly.

03 What is the difference between list_orders and get_order?

The `list_orders` tool gives you a summarized overview—a quick list of many transactions. You use `get_order` when you need the deep, detailed metadata for one specific order ID.

04 Does WooCommerce MCP handle inventory tracking?

Yes. By using `list_products` and `get_product`, your agent can give you real-time visibility into product availability and catalog status.

05 Can I change an order's status with this MCP?







Absolutely. The `update_order` tool lets your agent modify the current status of any specific order, allowing you to move it from 'Processing' to 'Shipped,' for example.

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 <code>"woocommerce-alternative": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

WooCommerce 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](https://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 WooCommerce. 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	WooCommerce MCP
Server ID	019d849e-f2e6-7369-a7c9-8c1d57d4982e
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/woocommerce-alternative.