

MCP SERVER

NO CODE

CLOUD HOSTED

CS-Cart MCP for AI Agents

Manage e-commerce products and multi-vendor marketplace operations

CS-Cart connects your entire e-commerce or multi-vendor marketplace to any AI agent. Use this MCP to manage products, track complex orders, audit vendor accounts, and check tax rules—all through natural conversation. It gives you direct control over store operations without logging into the admin panel.

A+ Quality Score 100/100

online-store

marketplace

product-management

order-tracking

vendor-management

retail-operations



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.

CS-Cart MCP

10 tools available

Cloud-hosted on Vinkius

Your AI client can treat your CS-Cart platform like a conversational employee. Instead of navigating deep menu structures or copying IDs from various tabs, you just talk to it. You get full command over everything: listing inventory details, finding out why an order is stuck, or verifying if a vendor meets operational limits.

Need to know the tax structure for goods shipped to France? Ask the agent. Need to check which users have admin permissions? Ask the agent. This MCP pulls all that data together from your backend. You connect this through Vinkius and give your AI client the power it needs to run complex e-commerce checks on demand. It's like having a real-time, searchable database of every piece of information in your store—without needing an IT person to write custom scripts.

Core Capabilities

01 — Product Data Lookup

Retrieve detailed product information, including current stock levels, pricing options, and feature combinations.

03 — Vendor & User Auditing

List all active marketplace vendors, check their operational statuses, or manage user accounts by listing administrators and customer roles.

02 — Order Status Investigation

Get a complete overview of recent sales or drill down into specific order details like payment status, shipping methods, and line-item costs.

04 — Financial Rule Verification

Look up configured tax rates, VAT rules, and available shipping carrier rates to verify compliance for any transaction.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP on Vinkius. You'll need your CS-Cart Store URL, Admin Email, and API Key.
- 02 Enter those credentials into your preferred AI client (like Cursor or Claude).
- 03 Your agent can now access all the defined tools to answer complex questions about your store data.

The bottom line is that you set up the connection once, and then use natural language in your AI client to manage everything else.

Built For

This MCP solves headaches for anyone managing a multi-vendor marketplace or large online store. It's perfect for operations teams who hate clicking through dozens of admin panels, support staff needing instant order data, and accountants who need quick tax verification.

Marketplace Operator

Auditing vendor accounts to confirm which sellers are active and what their operational limits are across the platform.

Customer Support Specialist

Looking up order #987's full history, checking the billing address, and identifying the specific shipping method used for delivery.

Store Owner/Administrator

Running reports to list all products or verifying the current VAT settings before a major sale launch.

What Changes When You Connect

- 01 Audit vendor lists instantly. Instead of going to the Vendor tab, you can use `list_vendors` to check seller statuses across thousands of storefronts using natural language.

-
- 02 Handle complex order queries faster. Get a full picture of any sale by running `get_order`, which immediately provides line items, taxes, and shipping costs in one go.

 - 03 Stay compliant with tax rules. Never guess on pricing again; `list_taxes` gives you the exact percentage rate and geographic application rule needed for accurate billing.

 - 04 Simplify inventory management. Use `list_products` to quickly check product IDs, current stock levels, or even find out which vendor owns a specific item.

 - 05 Resolve customer issues immediately. Need to know what shipping options are available? `list_shippings` gives you the carrier names and rates right away.
-

Real-World Applications

A Support Agent Needs Order Details

A support agent needs to resolve a billing dispute for order #456. They ask their AI client, which uses `get_order`, and instantly receive the line-item breakdown, confirming that the tax applied was correct according to the customer's region.

Product Pricing Audit

The purchasing manager needs to know the full price options for a new product line. They ask the agent to use `get_product`, which returns not only the base price but also all associated feature combinations and tax rules.

The Ops Team Checks Vendor Compliance

A marketplace operator suspects a vendor might be inactive. They run `list_vendors` via their agent and quickly identify all active seller companies, cross-referencing them with current operational limits to flag potential issues.

New User Onboarding

A team member needs to know who is allowed to perform what actions. They simply ask for a list of users via `list_users`, which immediately distinguishes between 'Customer', 'Admin', and 'Vendor' roles.

Patterns to Avoid

Assuming Vendor Status

X AVOID

A team member sees an order from a new seller but doesn't know if the seller is fully approved or limited. They waste time manually checking multiple vendor pages.

✓ INSTEAD

Instead of digging through pages, use `list_vendors` to get a centralized view of all sellers and their current operational status in one prompt.

Ignoring Tax Complexity

X AVOID

A sales rep quotes a client a price without confirming the local VAT rates for that state. They risk under-billing or over-charging.

✓ INSTEAD

Before quoting, run `list_taxes` to get all configured tax names and their precise geographic application rules. This ensures accurate pricing every time.

Missing Order Context

X AVOID

A support rep finds an order number but can't tell if the payment status is 'Pending' or 'Paid,' making it hard to advise the customer.

✓ INSTEAD

Use `get_order` on the specific ID. This tool returns the full line items, billing addresses, and crucial payment details alongside the shipping costs.

The Right Fit

Use this MCP if your primary workflow involves querying interconnected data points across e-commerce modules—like checking an order's status *and* verifying its associated tax rate. It's ideal for deep administrative audits, like running `list_vendors` to check seller compliance or using `get_product` to verify pricing options against tax rules. Don't use this if you just need a simple mailing list; for that, a dedicated CRM integration is better. Also, don't rely on it for making changes; it's read-only data retrieval.

CS-Cart MCP: Solving Marketplace Vendor Auditing Pain Points

Managing a multi-vendor marketplace means dealing with thousands of independent storefronts. Today, checking vendor compliance is pure manual labor. You have to open the admin panel, navigate to 'Vendors,' and then click into multiple individual profiles just to verify if they're active and operating within their defined limits.

With this MCP, you simply tell your agent what you need—for example, 'List all vendors that are currently restricted.' The tool uses `list_vendors` to pull the live data and gives you a clean, actionable report instantly. You get immediate clarity on who's available without opening a single browser tab.

CS-Cart MCP: Streamlining Order Fulfillment Data Retrieval

When an order comes in, the typical flow requires jumping between multiple pages. You check `list_orders` for status, then open `get_order` to see items and shipping costs, and finally run `list_taxes` just to confirm the rate. This constant context switching is slow and error-prone.

Now, your agent handles it all. By combining tools like `get_order` with tax checks, you get one single answer: a complete breakdown of everything from initial payment status to final calculated cost. The data speaks for itself.

CS-Cart: 10 Tools for Marketplace Order & Product Data

Use these tools to retrieve specific product details, track orders, list vendors, or check tax rates from your CS-Cart store through natural conversation.

#	TOOL	DESCRIPTION
01	<code>list_products</code>	Retrieves product IDs, names, prices, stock levels, and associated vendor identifiers across your store.
02	<code>get_product</code>	Fetches full details for a single product ID, including feature options, tax rules, and pricing boundaries.
03	<code>list_orders</code>	Generates an overview of recent orders, showing totals, payment statuses, shipping methods, and transaction timestamps.
04	<code>get_order</code>	Retrieves detailed line items for a specific order ID, including applied taxes, shipping costs, and customer addresses.
05	<code>list_users</code>	Lists all user accounts (Customers, Admins, Vendors), providing roles, email addresses, and account creation dates.
06	<code>list_categories</code>	Provides a list of product categories, including their IDs, names, parent/child relationships, and SEO identifiers.
07	<code>list_vendors</code>	Lists all registered marketplace vendors or companies, providing contact info, profiles, and current operational status.
08	<code>list_shippings</code>	Shows available shipping methods configured in your store, along with carrier names and supported delivery regions.
09	<code>list_taxes</code>	Retrieves a list of tax rules and rates applied to the store, including their percentage rate and geographic application details.
10	<code>list_statuses</code>	Lists all defined order statuses used in your system, mapping human-readable names to internal code identifiers.

See It in Action

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

U Show me the details and current stock levels for product ID 1024.



Product Details: Modern Desk Lamp

- **Price:** \$45.00 (MSRP)
- **Stock Level:** Available (Qty: 187 units)
- **Features:** Includes LED base and USB charging port.
- **Tax Applied:** 7% (State rate).

This item is ready to ship.

U What are the total contents and status for order #987?



Order Summary: #987

- **Status:** Paid (P)
- **Total Billed:** \$120.00
- **Items:** 2 units (Item A: \$50.00; Item B: \$70.00)
- **Shipping Method:** FedEx Ground (\$10.00).
- The customer's billing address is confirmed in the system.

U Who are all the active sellers and what's their status?



Active Marketplace Vendors (3 found):

1. TechWorld Solutions: *Status:* Active, Full Capability.
2. Green Garden Supplies: *Status:* Restricted (Requires Tax Audit).
3. Fashion Hub: *Status:* Dormant.

Frequently Asked Questions

01 How does the CS-Cart MCP help with general marketplace operations?

It centralizes all your core e-commerce data into one conversational interface. You can list active vendors, check product stock levels, and audit user roles without ever having to navigate the complex admin menus.

02 Can I use this MCP to verify taxes for a new sale?

Yes. The MCP lets you look up configured tax rules using `list_taxes`. You can confirm the correct percentage rate and check if any geographic restrictions apply before finalizing a quote.

03 Is CS-Cart MCP only for viewing data, or can I do more?

It is designed entirely for reading and auditing data. You can retrieve comprehensive reports on orders (`get_order`), inventory, and vendor details using natural language prompts.

04 What if I need to find the total number of products in my store?

You can list products to get a count and overview. The MCP pulls product IDs, names, and stock counts instantly, letting you survey your whole catalog quickly.

05 Does this tool help with customer support inquiries about shipping?







Absolutely. You can use the agent to list available shipping methods (`list_shippings`) or get a specific order's details to confirm which carrier and rate was applied during checkout.

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>"cs-cart": { "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

CS-Cart 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 CS-Cart. 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	CS-Cart MCP
Server ID	019d757f-b82a-739b-b76c-22f9bc0e6820
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/cs-cart.