MCP SERVER | NO CODE | CLOUD HOSTED

# Commerce Layer MCP for AI Agents

## Managing E-commerce Orders, Inventory, and Customer Data

Commerce Layer lets your AI agent manage everything related to e-commerce operations. Use it to find specific customer details, check product stock by SKU, retrieve complete order histories, and track shipments across multiple markets.

A+ Quality Score 98.33/100

headless-commerce | api-first | inventory-management | multi-market | order-processing | sku-management

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

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.

# Commerce Layer MCP

9 tools available
Cloud-hosted on Vinkius

This MCP connects your AI client directly to the Commerce Layer API, giving your agent immediate access to all your commerce data. Instead of logging into a dashboard or running complex queries, you just ask your agent what you need—and it does it. You can quickly list recent orders and filter them by status, grab full details on any specific line item, or look up inventory levels for a product using its SKU code. Need to find a customer? Your agent can search records by email and even compile their total order history. Because Vinkius hosts this entire catalog, you connect your AI once from Claude, Cursor, or Windsurf and get all these capabilities instantly available.

## Core Capabilities

**01 — Get specific order details**

Retrieve complete financial and line-item information for a single order.

**02 — Search orders by customer email**

Locate and view all historical orders associated with a specific customer's email address.

**03 — Check product inventory status**

Get current pricing, stock counts, and metadata for any given SKU code.

**04 — View customer records and history**

Access a list of customers or find specific individuals to see their total order count and associated addresses.

**05 — Track shipments and analyze metrics**

Retrieve lists of recent shipments, or calculate basic performance statistics across a group of orders.

## One Click on Vinkius — From Prompt to Execution

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

01 Connect the Commerce Layer MCP to your AI client by providing your organization's subdomain, Client ID, and Client Secret.

02 Your agent uses natural language to determine what data you need—whether it's a list of all SKUs or a specific order number.

03 The MCP executes the required API call and returns structured commerce data directly into your chat window for immediate action.

The bottom line is, you get real-time access to complex backend e-commerce data without ever leaving your messaging interface.

## Built For

This MCP serves anyone whose job involves interacting with order, inventory, or customer records. It's for the Customer Support specialist who needs instant answers and the E-commerce Manager who wants to check stock without opening a browser.

**Customer Support Representative**

Uses the agent to look up an account by email and immediately pull their order history, cutting down on back-and-forth emails.

**E-commerce Manager**

Checks current inventory levels for multiple SKUs or calculates aggregate sales statistics across various orders in one prompt.

**Developer/Analyst**

Inspects specific API resources, like retrieving a list of shipments or checking order details, to debug workflows directly from the chat.

## What Changes When You Connect

01 Resolve customer inquiries faster by letting your agent run the search_orders_by_email tool. Instead of asking a user for an order ID, they just give their email address.

02 Check product availability instantly. Use get_sku to pull pricing and inventory levels on demand, eliminating manual navigation through product dashboards.

03 Gain immediate oversight into sales metrics by running get_order_stats across multiple recent orders. You get the summary without having to calculate it yourself.

04 Keep track of physical goods with list_shipments. Your agent pulls all tracking information and shipment details in one go, perfect for support teams.

05 Streamline customer research using list_customers or list_orders. These tools let your agent build a profile on any user right from the chat window.

## Real-World Applications

**A customer calls asking about their missing package.**

The support rep asks the agent to use search_orders_by_email with the caller's email. The agent instantly finds all related orders and pulls shipment details, allowing the rep to give a precise update without transferring calls.

**An e-commerce manager needs to know if they can sell an old product.**

The manager asks the agent for the SKU status. The agent runs get_sku using the product code and reports back on current pricing, stock availability, and metadata in seconds.

**A developer needs to debug why a specific order failed payment.**

The developer asks the agent to run get_order on the problematic ID. The agent returns the full order details, including line items and payment info, allowing for rapid debugging in chat.

**A marketing team wants a quarterly sales summary report.**

Instead of exporting data and running Pivot Tables, they ask the agent to get_order_stats across all orders from Q3. The resulting stats are delivered directly for immediate review.

# Patterns to Avoid

### Treating it like a simple database search

✗ AVOID

Asking the AI agent to just 'find the customer' without specifying they need order history or addresses. The agent only returns basic name data, which is useless.

✓ INSTEAD

Always scope your request using specific tools. To get full context on a user, ask the agent to run search_orders_by_email first, then use list_customers if you need general account details.

### Overloading one prompt with too many data points

✗ AVOID

Asking for 'all orders, all SKUs, and all customer addresses' in a single breath. The agent gets confused and returns an unusable dump of raw JSON that nobody reads.

✓ INSTEAD

Break it down into steps. Start by listing the needed resources (list_skus), then drill down using get_sku for specific analysis.

### Assuming real-time stock data is always available

✗ AVOID

Asking about a product that was discontinued months ago. The agent might return outdated pricing or inaccurate inventory counts if the system isn't fully updated.

✓ INSTEAD

Always check the metadata and confirm the SKU status using get_sku to ensure the listed information is current before making a business decision.

## The Right Fit

Use this MCP when your primary goal involves accessing live, transactional data from an e-commerce back end. If you need to know 'What was sold?' or 'How much stock do we have?', this is the right tool. For instance, if a user needs to check order status, use get_order or search_orders_by_email. Don't use it if your goal is simply generating marketing copy or summarizing general industry trends; for that, you need a pure LLM client without external API access. If you only need basic contact information and nothing about their purchases, querying the list_customers tool might be enough, but if any transaction data (like shipments) is involved, use this MCP.

## Commerce Layer: Managing Order Status and Customer History via AI

Today, checking an order's status or finding a customer’s purchase history means jumping through hoops. You open the admin dashboard, search by email, navigate to the specific order ID, then click on line items and payment details. It takes clicks, context switching, and multiple browser tabs just to answer a simple 'Where is my stuff?' question.

With Commerce Layer connected via this MCP, the process changes entirely. You ask your agent, 'What's the status of Jane Doe's last order?' The agent uses search_orders_by_email instantly retrieves all necessary data and presents it back to you in a clean chat summary, saving minutes on every single interaction.

## Commerce Layer: Analyzing Product Inventory and Shipments with AI

Manually checking inventory requires running separate reports for dozens of SKUs. You're juggling pricing sheets, stock spreadsheets, and shipment logs. If you need to know the combined status across different markets or if a specific product is ready to ship, it’s a manual, error-prone process.

Now, your agent handles the complexity. You ask about stock levels for 'TSHIRT-BLUE-L', and get_sku gives you real-time metrics immediately. Similarly, asking about recent shipments consolidates list_shipments records into one view. It’s instant data aggregation that eliminates manual reporting.

# Commerce Layer: 9 Tools for E-commerce Data Retrieval

These tools let your agent find specific order details, list customers, calculate stats, or look up product information directly from the platform's backend.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `get_order` | Retrieve details of a specific order |
| 02 | `get_order_stats` | Calculate basic stats for a set of orders |
| 03 | `get_sku` | Retrieve details of a specific SKU |
| 04 | `list_customers` | Retrieve a list of customers |
| 05 | `list_orders` | Retrieve a list of orders from Commerce Layer |
| 06 | `list_prices` | Retrieve a list of product prices |
| 07 | `list_skus` | Retrieve a list of SKUs (products) |
| 08 | `list_shipments` | Retrieve a list of shipments |
| 09 | `search_orders_by_email` | Find orders belonging to a specific customer email |

# See It in Action

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

**U** What were the total sales and how many orders we processed last month?

**Order Metrics for Last Month:**

- **Total Orders Count:** 1,245
- **Gross Revenue:** $389,500.00
- **Average Order Value (AOV):** $313.70

(These stats were calculated using data from your recent orders.)

**U** Check the inventory for SKU TSHIRT-BLUE-L and see if we have enough to fulfill 50 units.

**SKU Details: TSHIRT-BLUE-L**

- Name: Blue T-Shirt (Large)
- Price: $29.99
- Stock Available: 142 units
- Weight: 200g

Yes, you have enough stock to fulfill 50 units right now.

**U** Find all orders for the email john.smith@example.com and tell me their total value.

I found 3 recent orders for John Smith:

1. #ORD-4521: $89.99 (Fulfilled)
2. #ORD-4520: $142.50 (Pending)
3. #ORD-4519: $35.00 (Cancelled)

The total value of these three orders is **$267.49**.

# Frequently Asked Questions

01 **How does the Commerce Layer MCP help me with customer lookups?**

It allows your agent to find customers by email or retrieve their entire order history, so you don't have to manually search multiple records. This speeds up support calls and gives a full view of their purchasing life cycle.

02 **Can I use the Commerce Layer MCP to check product stock levels?**

Yes, it lets you query any specific SKU code to get real-time details on pricing, current inventory counts, and overall product metadata. It’s great for quickly confirming availability before promising a date.

03 **Does the Commerce Layer MCP help me manage my shipments?**

Absolutely. You can ask your agent to pull all recent shipment records. This means you get tracking numbers and delivery status updates in one place, without needing the shipping portal.

04 **How does this MCP handle bulk order analysis?**

Instead of downloading massive CSV files for reporting, your agent can calculate basic statistics across a set of orders. You just ask for 'total sales' or 'average item count,' and the result appears instantly.

05 **What kind of data does the Commerce Layer MCP give me access to?**

It provides full e-commerce data: order details, customer contact info, product SKUs, pricing lists, and shipment records. Everything needed to run an operation from chat.

# 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 `"commerce-layer": { "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

# Commerce Layer 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 Commerce Layer. 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 | Commerce Layer MCP |
| Server ID | `019d7578-612d-71bc-84e9-cedc7372d961` |
| 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/commerce-layer.