

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Saleor MCP for AI Agents

Manage your headless e-commerce store and product inventory directly.

Saleor MCP lets you connect your AI agent directly to your headless e-commerce store. You can manage your product catalog, audit recent orders, and pull customer details instantly. It's the fast way to give your agent real-time access to your retail data without manual exports.

A+ Quality Score 100/100

graphql-api

product-catalog

inventory-management

digital-commerce

order-processing

storefront-management



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.

Saleor MCP

10 tools available

Cloud-hosted on Vinkius

If you're running a store, you know the pain of jumping between tabs just to see if an order shipped or if a specific SKU is out of stock. This MCP gives your AI agent a direct line to your Saleor backend. You can ask your agent to pull up a receipt, check a category list, or find a customer's profile in seconds. Instead of you doing the manual digging, your agent does the work. It handles the work of checking your inventory and order history so you can stay focused on actually running the business. Since Vinkius hosts this, you can get it connected and ready to go in minutes. It's about giving your AI the data it needs to be a useful part of your daily retail operations.

Core Capabilities

01 — Pull full product details

Get specific info like pricing and stock levels for any item in your store.

02 — Audit recent orders

See a list of the latest purchases and grab full receipt details instantly.

03 — Search customer profiles

Find registered users and their specific order histories in your database.

04 — Manage store categories

Browse how your products are organized without opening a dashboard.

05 — Check store configuration

Access global settings like currencies and active sales channels.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/mcp/saleor — connect your AI agent in three steps.

- 01 Create an internal App Token in your Saleor backend with the right permissions.
- 02 Add the Saleor Cloud GraphQL API Endpoint and your token to the connection.
- 03 Ask your agent to find an order, check stock, or list your products.

The bottom line is you get a live bridge between your AI agent and your e-commerce backend.

Built For

This is for e-commerce managers and retail ops who are tired of manual data entry and want their AI to actually interact with their store data.

E-commerce Manager

Uses the AI to check inventory levels and update product categories without leaving the chat.

Customer Support Lead

Pulls up customer order histories instantly to resolve tickets faster.

Retail Operations Specialist

Audits recent sales and monitors store configurations across different channels.

What Changes When You Connect

- 01 Faster order auditing: Use `list_orders` and `get_order` to see exactly what customers bought and where it's headed without manual searching.
- 02 Real-time inventory checks: Use `get_product` to see precise stock configurations for any item instantly.
- 03 Better customer service: Use `get_customer` to pull up a shopper's history the moment they message you.

-
- | | |
|----|---|
| 04 | Easy catalog management: Use <code>list_categories</code> and <code>list_collections</code> to see how your store is organized at a glance. |
| 05 | Rapid store setup: Use <code>list_channels</code> and <code>get_shop_info</code> to verify your global settings and active sales pipelines. |
| 06 | Customer list access: Use <code>list_customers</code> to see a full list of everyone registered in your shop. |
-

Real-World Applications

Checking an order's location

A customer asks 'Where is my package?' The agent uses `get_order` to find the shipping status and billing address.

Customer lookup

A support agent asks 'Who is customer 502?' The agent uses `get_customer` to pull their full profile and history.

Stock verification

A shopper asks 'Is the red dress available in size medium?' The agent uses `get_product` to check the specific variant's stock.

Catalog browsing

A user asks 'What categories do you have?' The agent uses `list_categories` to show the store's organization.

Patterns to Avoid

Guessing order details

✗ AVOID

Telling a customer 'I'm not sure' instead of looking it up.

✓ INSTEAD

Use `get_order` to give them the exact status of their purchase.

Manual stock updates

✗ AVOID

Wasting time checking your dashboard every time someone asks about a product.

✓ INSTEAD

Use `get_product` to see live stock levels instantly.

Searching for customers by name

X AVOID

Guessing which profile is correct when multiple people have similar names.

✓ INSTEAD

Use `list_customers` to find the right person and `get_customer` for the details.

The Right Fit

Use this if you have a Saleor-based headless store and want your AI to interact with your live inventory, orders, and customer data. It's the right choice if you need your agent to perform actual tasks like checking order status or pulling customer histories. Don't use it if you're on a different platform or if you only need to do basic web scraping. This is a deep integration for Saleor users who want their AI to act as a functional retail assistant.

Saleor MCP for Headless E-commerce Inventory Management

If you're running a retail business, you know how tedious it is to jump between different tabs just to see if an order shipped or to check if a specific SKU is out of stock. You're constantly copy-pasting IDs, refreshing dashboards, and hunting through spreadsheets to give your customers the right answers.

This MCP gives your AI agent a direct line to your Saleor backend. Instead of you doing the manual digging, your agent does the work. It handles the heavy lifting of checking your inventory and order history so you can stay focused on actually running the business.

Saleor MCP for Real-time Order Fulfillment Auditing

Manually auditing every receipt and checking billing addresses across different sales channels is a drain on your time. It makes it harder to catch errors before they become problems for your customers.

With this connection, your agent can pull up full order details and shop configurations in seconds. You get a clear view of your operations without the manual overhead.

Saleor MCP: 10 Tools for E-commerce Inventory

Use these tools to manage your Saleor products, orders, and customer data through your AI agent.

#	TOOL	DESCRIPTION
01	<code>get_customer</code>	Pulls a specific customer's profile and their full order history. Use this to check past purchases during a support call.
02	<code>get_order</code>	Grabs every detail for a single order, including line items and billing info. Use this to verify shipping addresses or fulfillment status.
03	<code>get_product</code>	Fetches specific details like variants and stock for a single product ID. This helps you check exact inventory counts for specific items.
04	<code>get_shop_info</code>	Retrieves your global store configuration and high-level settings. Use it to see your active regions and default currencies.
05	<code>list_categories</code>	Shows you every category in your store to see how items are organized. It's a quick way to browse your catalog structure.
06	<code>list_channels</code>	Lists all active sales channels and their configurations. Use this to see where your products are currently being sold.
07	<code>list_collections</code>	Pulls a list of all product collections in your directory. This helps you see how you've grouped your merchandise.
08	<code>list_customers</code>	Finds all registered customers in your store's database. Use this to get a broad view of your user base.
09	<code>list_orders</code>	Shows a list of the most recent orders placed on your platform. It's perfect for a quick pulse check on daily sales.
10	<code>list_products</code>	Returns a list of all products currently in your Saleor store. Use this to get a high-level view of your entire catalog.

See It in Action

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

List all products in my store.



I've pulled the current product list from your Saleor store. Here are the top items:

PRODUCT NAME	STATUS	PRICE
Classic Fedora	In Stock	\$85.00
Wool Overcoat	Low Stock	\$240.00
Leather Gloves	Out of Stock	\$45.00

Would you like more details on any of these?

Find out order specifics and shipping details for order number '334'.



I've retrieved the details for **Order #334**:

- **Status:** Unfulfilled
- **Customer:** customer@example.com
- **Shipping Address:** 123 Maple St, CA
- **Items:** 1x Classic Fedora
- **Total:** \$85.00

It looks like this is still awaiting fulfillment.

U What currencies does the store utilize in the available sales channels?



I checked your high-level store configuration. You currently have three active pipelines:

- **US Store:** USD
- **UK Store:** GBP
- **Continental Node:** EUR

All three channels are functioning correctly.

Frequently Asked Questions

01 Can the Saleor MCP help me manage my inventory?

Yes, it allows your AI agent to check live stock levels and pull specific product details for any item in your store.

02 How does the Saleor MCP handle customer order history?

Your agent can pull up a specific customer's full profile and every order they've ever placed in your shop.

03 Can I use Saleor MCP to check my store's global settings?

Yes, it can retrieve your global configuration, including active regions and default currencies.

04 Does Saleor MCP work with my existing headless setup?

It is designed specifically for Saleor's headless GraphQL backend, making it a perfect fit for your existing architecture.

05 How can I use Saleor MCP to help with customer support?

It lets your agent quickly find order statuses and customer information so you can provide faster, more accurate help.

06 Can I see my sales channels using Saleor MCP?

Yes, it can list all your configured sales channels and their specific settings.

07 Can the AI forcefully complete, modify, or delete existing customer orders in my Saleor shop?

No. The integration focuses securely on read-only queries. It fetches critical information such as stock numbers, recent sales, and product characteristics without actively overwriting, resolving, or destroying records to protect e-commerce transactional integrity.

08 Does it require a specific Saleor Cloud paid plan to use this integration?

A specific plan is not heavily mandated by the tool itself as long as your environment successfully exposes the standard backend GraphQL endpoint and permits the creation of standard administrative App Tokens within your environment policies.

09 Why do some commands ask for a 'GraphQL ID' specifically?

Saleor's core architecture uses unique Base64-encoded strings (like 'UHJvZHVjdDoxMjM=') as identifiers natively, rather than typical numeric database IDs. Always use the `list\_orders` or `list\_products` tools first to discover these exact encoded IDs natively, then seamlessly pass them to the exact fetching tools to pull their full snapshots.

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>"saleor": { "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

Saleor 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 Saleor. 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	July 2026
MCP Server	Saleor MCP
Server ID	019d7601-70dd-733a-9ebe-42eee26bb8b8
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/saleor.