MCP SERVER | NO CODE | CLOUD HOSTED

# Katana MCP

## Automate order tracking and inventory counts.

Katana MCP automates your manufacturing ERP workflow by letting your AI agent interact with core business data—including sales, purchasing, and inventory—through natural conversation. You can generate new customer orders, check real-time stock counts for specific product variants, or pull detailed lists of all active manufacturing jobs directly from your client. This eliminates manual logins and spreadsheet cross-referencing across multiple systems.

A+ Quality Score 100/100

manufacturing-erp | production-planning | shop-floor-control | inventory-tracking | supply-chain-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/katana

SCAN TO VIEW

# The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

# Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

# Katana MCP

11 tools available
Cloud-hosted on Vinkius

This MCP connects your AI agent to Katana Cloud Manufacturing, giving it direct access to the data that runs a factory floor. Instead of logging into a separate ERP dashboard every time you need information, your agent handles the request in plain conversation. You can ask it to check if 'Acme Corp' has enough material for their next big order or pull up all outstanding purchase orders needing attention. It uses tools like `list_customers` and `get_inventory_by_variant` to gather precise data, so you don't have to jump through tabs. Whether you need the status of a product run via `list_manufacturing_orders`, or you just want to know what materials are available in your catalog using `list_materials`, this MCP handles it all. By connecting this capability through Vinkius, you get one access point for every critical piece of operational data.

## Core Capabilities

**01 — Manage Sales and Purchasing Flow**

Create new sales orders using `create_sales_order` or pull comprehensive lists of both customer accounts (`list_customers`) and purchase orders (`list_purchase_orders`).

**02 — Check Real-Time Stock Levels**

Get immediate inventory status for the entire facility via `list_inventory`, or drill down to check specific stock counts using `get_inventory_by_variant`.

**03 — Track Production Status**

View and pull lists of all active manufacturing orders (`list_manufacturing_orders`) to monitor job progress across the shop floor.

**04 — Query Product Data**

Access a full database view by listing available products or materials using `list_products` and `list_materials`, including metadata needed for planning.

**05 — Handle Supplier and Client Info**

Pull lists of all suppliers (`list_suppliers`) and sales orders (`list_sales_orders`), keeping a clear view of your external partners.

## One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and input your Katana API key.

02 Your AI client sends a natural language request (e.g., 'What's the stock for Model X?').

03 The agent executes the relevant tool (like `get_inventory_by_variant`) and returns structured data directly to your chat interface.

The bottom line is you get instant, actionable answers about your factory operations without writing or running code yourself.

## Built For

This MCP is for operational staff—the Production Manager who needs live status updates before calling a client, and the Inventory Specialist who can't afford to wait for an afternoon report. If your job involves cross-referencing order details with current material availability, you need this.

**Production Planner**

Uses `list_manufacturing_orders` and `get_inventory_by_variant` to determine if raw materials are ready for the next production run.

**Sales Account Manager**

Pulls customer details using `list_customers` or checks existing order status via `list_sales_orders` during a client call.

**Supply Chain Coordinator**

Checks material availability (`list_materials`) and pulls supplier lists (`list_suppliers`) to manage procurement timelines.

## What Changes When You Connect

01 Stop manually cross-referencing sheets. You can check current stock levels using `get_inventory_by_variant` and immediately know if a sales order is viable, all in one chat session.

02 Faster client calls mean better sales. Instead of searching through old records, simply ask your agent to use `list_customers` or `list_sales_orders` for instant account history.

03 Production visibility happens instantly. You can pull up a list of active jobs using `list_manufacturing_orders` and get an immediate status update without opening the full ERP dashboard.

04 Never lose track of what needs buying again. Your agent handles listing all purchase orders ( `list_purchase_orders` ) or checking material requirements against your product catalog using `list_materials` .

05 Process order creation in seconds. Instead of filling out forms, you tell your AI client to use `create_sales_order` , and it routes the request directly into Katana.

## Real-World Applications

**The Rush Order Check**

A sales rep needs to confirm if a customer's large order is possible. They ask their agent, which uses `list_sales_orders` and then checks the material availability with `get_inventory_by_variant`. The agent reports back: 'Yes, 50 units are available, but they will be committed by the job listed under SO-123.' This avoids a panicked phone call to operations.

**Quarterly Inventory Audit**

The inventory specialist needs an overall picture of stock. Instead of running five different reports, they ask the agent to run `list_inventory`. The system immediately returns a comprehensive status report across all product variants and materials.

**Starting New Production**

A planner decides to start a new item. They first use `list_products` to check if the base model exists, then ask for suppliers using `list_suppliers` to find sources for necessary components, and finally run `create_sales_order` once everything is confirmed.

**Understanding Past Purchases**

A coordinator needs to know why a specific job stalled. They ask the agent to list all manufacturing orders (`list_manufacturing_orders`) and then check the associated purchase order status using `list_purchase_orders` to find the missing component.

# Patterns to Avoid

### Treating it like a search engine

✗ AVOID

Typing 'Show me all sales orders and inventory.' The agent gets confused because you asked for two separate data types in one query, resulting in an incomplete or unusable summary.

✓ INSTEAD

Break the request into specific steps. First, ask the agent to `list_sales_orders`. Then, follow up with, 'Now check the stock level for the product mentioned on that last order' using `get_inventory_by_variant`.

### Manual data transfer

✗ AVOID

Pulling a customer list from one screen and then copying IDs into another system to create an order. This is slow, error-prone, and interrupts workflow.

✓ INSTEAD

Use the agent to first `list_customers` for verification, and then tell it directly: 'Please use this customer ID' followed by the command to `create_sales_order`. It handles the data flow.

### Over-relying on one tool

✗ AVOID

Only checking the current list of materials (`list_materials`) without knowing if a purchase order exists for them. You think you're ready, but supplies are stuck in transit.

✓ INSTEAD

Always cross-reference your material needs by first running `list_purchase_orders` to see what is currently on its way before making production decisions.

## The Right Fit

Use this MCP if your daily work requires reading, creating, or updating core ERP records—specifically sales orders, purchase orders, and inventory counts. If you need to know 'How much stock do we have?' or 'Can I submit an order for Client X?', this is what you need. Don't use it if all you need is a simple report that doesn't change data; those are better suited for dedicated reporting tools. Also, don't rely on this MCP to manage payroll or HR records—that falls outside the scope of manufacturing operations. If your task involves querying basic product definitions and materials, however, using `list_products` and `list_materials` is exactly what it was built for.

## The headache of switching between operational screens.

Today, if you want to know the status of a big order, you log into the ERP. Then you open the inventory module to check stock levels. Next, you switch to the sales tab just to confirm the customer ID before emailing anyone. You're clicking through five different screens and copying three different numbers—all just for one conversation.

With this MCP, your agent handles that entire sequence in plain English. It combines checking `list_sales_orders` status with verifying real-time stock via `get_inventory_by_variant`. You get the final answer immediately, without ever leaving your chat window.

## Katana MCP: Immediate access to full order and material data.

The manual steps of opening separate dashboards for inventory checks, listing suppliers, and viewing purchase orders vanish. Your agent consolidates the output from tools like `list_materials` and `list_suppliers` into one readable response.

You don't just get data; you get a complete picture of your operational status. The speed is the biggest difference now.

# Katana MCP: 11 Tools for Operations Management

These tools allow your AI client to perform specific actions like creating orders or checking stock levels directly within the Katana ERP system.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `create_sales_order` | Generates a brand new sales order for a customer, provided you give the customer's ID. |
| 02 | `list_customers` | Retrieves a complete list of every registered customer in your system. |
| 03 | `get_sales_order` | Fetches all specific details for one designated sales order number. |
| 04 | `list_inventory` | Provides a high-level, overall view of the entire inventory status across all locations. |
| 05 | `get_inventory_by_variant` | Checks the specific stock count for one designated product variant ID to know exactly what's available. |
| 06 | `list_manufacturing_orders` | Pulls a list of every currently active and pending manufacturing job or work order. |
| 07 | `list_materials` | Lists all raw materials available in your Katana catalog, including metadata. |
| 08 | `list_products` | Retrieves a complete list of every finished or semi-finished product defined in the system. |
| 09 | `list_purchase_orders` | Lists all purchase orders that have been created, detailing what needs to be bought. |
| 10 | `list_sales_orders` | Retrieves a list of all sales orders, allowing you to see recent activity and status updates. |
| 11 | `list_suppliers` | Lists every external supplier connected to your manufacturing process. |

# See It in Action

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

**U** Show me all active sales orders in Katana.

I've retrieved your sales orders. You have 15 active orders, including SO-101 for 'Acme Corp' and SO-102 for 'Tech Solutions'.

**U** Check the inventory level for variant ID 'VAR_987'.

For variant 'VAR_987', there are currently 45 units in stock, with 10 units committed to existing sales orders.

**U** List all my manufacturing orders.

I've fetched 8 manufacturing orders. Current jobs include production of 'Wooden Table' and 'Office Chair'.

# Frequently Asked Questions

01 **How do I create a sales order using Katana MCP?**

To create an order, simply ask your agent to use `create_sales_order`. You just need to make sure you provide the correct customer ID when you submit the request.

02 **Does Katana MCP only show finished goods inventory?**

No. The system handles both finished products and raw components. Use `list_materials` or `get_inventory_by_variant` to see stock for every variant type.

03 **Can I check production status with Katana MCP?**

Yes, you can list all current jobs by asking the agent to run `list_manufacturing_orders`. This gives you a real-time view of what's currently running on the line.

04 **What if I need more data than just sales orders?**

You can pull far more. Use tools like `list_purchase_orders` to see incoming supplies or run `list_customers` to get a full client roster.

05 **Is Katana MCP only for American businesses?**

No, it connects directly to your specific Katana Cloud Manufacturing account. It works with whatever data and structure you already have set up in the ERP.

# 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 `"katana": { "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

# Katana 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 Katana. 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 | Katana MCP |
| Server ID | `019d75bf-d7e6-720b-a6a3-fa389b581d6d` |
| 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/katana.