

MCP SERVER

NO CODE

CLOUD HOSTED

Holded MCP

Manage invoices, contacts, and inventory via natural chat.

Holded MCP connects your entire business management system to any AI agent. Use this connector to manage invoicing, track contacts, and oversee projects directly through natural conversation. You can list all invoices, check product stock levels, retrieve client profiles, and monitor tasks without leaving your chat window.

A+ Quality Score 100/100

business-management

invoicing

contact-management

crm

financial-operations



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.

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.

Holded MCP

11 tools available
Cloud-hosted on Vinkius

Managing a modern business shouldn't require logging into five different portals just to answer one question. This MCP connects your Holded ERP platform straight to your agent, letting you handle everything—from billing records to inventory counts—using plain English. Need to know if Acme Corp paid their last bill? Ask. Want to update the stock count on a specific product line? Tell your agent. It performs those actions and gives you the data back. Because all this functionality is housed within one connector, it keeps your workflow focused. By connecting through Vinkius, your AI client gains instant access to a unified view of your entire operation, turning complex accounting modules into simple conversations.

Core Capabilities

01 — Get Contact Information

Pull detailed profiles for any customer, supplier, or lead you need.

02 — View Invoice Data

Retrieve full details on specific invoices and monitor their payment status.

03 — Track Projects and Tasks

List active projects or check the current status of tasks across your company's portfolio.

04 — Manage Inventory Stock

Access product catalog details and update stock levels for specific items.

05 — View Business Metadata

Get high-level data about your account or organization to keep a clear overview of operations.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP and provide your Holded API key (found in Settings > Developers).
- 02 Your agent accesses the connected ERP data via Vinkius, mapping natural language requests to specific business tools.
- 03 You get a conversational response with real-time data—whether it's an invoice status or a list of active projects.

The bottom line is you stop clicking through menus and start asking questions.

Built For

This MCP is for anyone who spends too much time switching between dashboards to manage core business data. If your job involves checking invoice status, updating inventory counts, or coordinating project tasks across different platforms, you need this.

Project Manager

Checks the current task list and verifies if all active projects are on track without opening the dedicated PM dashboard.

Operations Lead

Needs to check product stock levels or retrieve contact details for suppliers before placing a new order.

Business Owner

Wants an immediate overview of company performance, such as listing recent invoices and overall account metadata.

What Changes When You Connect

- 01 Stop manually navigating complex modules. You can list all invoices or get detailed invoice information simply by asking your agent a question.

-
- 02** Keep track of teams' progress instantly. Use the `list_all_tasks` tool to see every task across multiple projects without opening a single dashboard tab.
-
- 03** Manage inventory on the fly. When you need to update stock levels, just ask your agent instead of navigating through complex warehouse management screens; use `update_product_stock`.
-
- 04** Get full client context immediately. Instead of finding a contact ID first, ask the agent to list contacts and then get their details directly with `get_contact_details`.
-
- 05** Maintain business oversight effortlessly. You can pull account metadata using `get_api_profile` or check project status via `list_projects`, all from one chat interface.
-

Real-World Applications

Checking on a Late Client Payment

The finance team needs to know if 'Global Logistics' paid their last bill. They ask the agent, and it uses `list_contacts` first, then calls `get_invoice_details` for the specific contact ID, returning the payment status immediately.

On-the-fly Inventory Correction

The warehouse staff finds they miscounted a shipment. They ask their agent to update the stock for Product X, and the agent executes `update_product_stock`, confirming the change without needing manual access to the inventory system.

Coordinating a Product Launch

A project manager needs to confirm product readiness. They ask the agent to list active projects (`list_projects`) and then check if the core products have enough stock using `get_product_details`.

Reviewing Team Workloads

The team lead needs to know where everyone stands. They ask the agent to list all tasks (`list_all_tasks`), getting an instant overview of who owns what and when it's due across departments.

Patterns to Avoid

Using generic web searches

X AVOID

Searching Google for 'how to check invoice status in Holded,' which gives general guides but requires manual data entry and login.

✓ INSTEAD

Use the agent directly. Ask it, 'What is the payment status of my last invoice?' The agent handles the authentication and calls `get_invoice_details` for you.

Copying/Pasting IDs

X AVOID

The user has to first run a search tool like `list_contacts` just to get an ID, then manually paste that ID into another form.

✓ INSTEAD

Just ask the agent to find information. Say, 'Show me the invoices for Acme Corp.' The agent uses `list_contacts` internally and passes the ID automatically when calling `list_invoices`.

Confusing API documentation

X AVOID

Reading dense developer docs to figure out which endpoint needs what parameters (e.g., 'Do I need warehouseid or just product code?').

✓ INSTEAD

Don't read the docs. Just ask your agent, 'Change the stock for Product X in Warehouse Y.' The agent handles the complex JSON structure required by `update_product_stock`.

The Right Fit

Use this MCP if you need to execute core business actions—like checking billing history or adjusting inventory counts—without navigating multiple, specific ERP screens. It's your centralized chat interface for operations. Don't use it if you are trying to build a completely custom data pipeline that needs advanced scripting logic; those cases might require dedicated integration tools. However, if your goal is simply to read public-facing information or view general reports already exported somewhere else, this connector won't help. This MCP excels at making the backend of your accounting and operations system talk directly to your natural conversation.

The constant clicking between tabs kills productivity.

Right now, checking on a client payment status means logging into Holded, navigating through the CRM, finding their record, then going to the 'Invoicing' tab, filtering by date, and finally reading the payment notes. This process takes three minutes of focused clicking and copying.

With this MCP, you just ask your agent: 'What is the status of Acme Corp's last invoice?' It performs all those internal steps—finding the client, checking the invoices, and pulling the data—and gives you a clean answer in seconds.

Get Project Visibility with Holded MCP

Before this, tracking overall project health meant opening the main dashboard, clicking into each active workflow, and manually checking the task list for every team member. It was a massive chore that often led to missing deadlines.

Now you ask your agent to 'List all tasks across my projects.' You get an immediate, consolidated view of everything due, so you never miss a deadline again.

Holded with 11 Tools

Use these eleven tools to manage everything from client contacts and project statuses to detailed invoice records directly within your chat agent.

#	TOOL	DESCRIPTION
01	<code>get_contact_details</code>	Retrieves a complete profile with detailed information about one specific contact.
02	<code>get_invoice_details</code>	Pulls comprehensive details for a single, specified invoice.
03	<code>get_api_profile</code>	Retrieves basic information about the Holded account that is connected to your agent.
04	<code>get_product_details</code>	Gets detailed specifications and current status for a particular product.
05	<code>get_project_details</code>	Fetches the full setup and current operational status of an entire project.
06	<code>list_contacts</code>	Provides a master list of all contacts, including clients, suppliers, and leads in your system.
07	<code>list_invoices</code>	Generates a list of every invoice to help you track billing records and find necessary IDs.
08	<code>list_products</code>	Lists all products or services available in your inventory for review.
09	<code>list_projects</code>	Shows a summary of both active and past projects running through the business.
10	<code>list_all_tasks</code>	Gathers a comprehensive list of every task across all your operational projects.
11	<code>update_product_stock</code>	Adjusts and updates the current stock quantity for an item in the warehouse.

See It in Action

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

U List all active projects and show the last task for each.



I've retrieved your projects. You have 3 active workflows: 'Website Launch' (ID: proj_102), 'Q2 Campaign', and 'Product Beta'. For the Website Launch, the latest task is 'Final QA Check' (ID: task_992). Would you like to see the details for any of these?

U Find contact 'Acme Corp' and show their recent invoices.



I've found Acme Corp (ID: contact_552). They have 2 recent invoices: INV-2024-01 (\$1,250.00 - Paid) and INV-2024-05 (\$3,000.00 - Pending). Would you like to see the items included in the pending invoice?

U Show me the details for product ID 'prod_992' and its stock level.



Accessing inventory... Product 'prod_992' (Wireless Mouse) currently has 45 units in stock across 2 warehouses. The main warehouse has 30 units and the secondary has 15. Should I update the stock level for any specific location?

Frequently Asked Questions

01 How do I find my Holded API Key?

Log in to your Holded account, click on the **Settings** icon (top right), go to **Developers**, and you will find your unique **API Key** listed there. You can create multiple keys for different integrations.

02 What document types are supported in the invoicing tools?

This integration currently focuses on the `invoice` document type. For other types like sales orders or purchase orders, you can use the generic `list_invoices` logic if they are mapped under the same module in your instance.

03 Can I update stock levels through this integration?

Yes! Use the `update_product_stock` tool. You must provide the product ID and a JSON string containing the warehouse ID and the new quantity to update your inventory.

04 Is the integration secure for ERP data?







Absolutely. The integration uses official Holded API keys in the request header over HTTPS. Your credentials and business data are encrypted and stored securely within the Vinkius Cloud infrastructure.

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>"holded": { "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

Holded 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 Holded. 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	Holded MCP
Server ID	019d75b1-f232-73ba-b52c-ae40a9666edc
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/holded.