MCP SERVER | NO CODE | CLOUD HOSTED

Hudu MCP

Access all company assets and IT documentation via your AI agent.

Hudu connects your AI client directly to your IT documentation, asset records, and company data. Your agent can list companies, retrieve specific asset details, find stored passwords, or pull knowledge base articles—all without you logging into Hudu manually. It gives your AI the immediate operational context it needs for MSP workflows and technical support.

A+ Quality Score 100/100

it-documentation | asset-management | password-management | msp-tools | knowledge-base | it-operations

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

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.

Hudu MCP

10 tools available
Cloud-hosted on Vinkius

Your AI client now talks directly to Hudu, giving it visibility across all your IT operations data. Instead of needing a human to run reports or search multiple systems, your agent handles that work immediately. You can ask it to find the asset details for a specific device, list contacts associated with a company, or even pull out stored passwords if needed. This MCP exposes everything from general knowledge base articles and documented procedures to lists of network devices and websites you monitor.

When you connect this through Vinkius, your agent gets access to all these operational tools in one place. It lets you automate complex IT management tasks—like gathering an initial report on a client's assets or listing all associated contacts—all via natural conversation. No more switching between tabs or copying data from different dashboards. You just ask for the information, and your AI agent gets it directly from Hudu.

Core Capabilities

01 — Find Company Information

Retrieves specific details about a company using its identifier.

02 — Review Operational Logs

Lists historical activity logs to see who did what and when within the system.

03 — Search Documentation

Finds knowledge base articles, documented procedures, or specific assets based on keywords or scope.

04 — Manage Contacts and Networks

Lists contacts across all companies or retrieves details about documented network structures.

05 — Handle Credentials

Retrieves lists of stored passwords for quick access by the agent.

One Click on Vinkius — From Prompt to Execution

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

01 Connect your AI client to Vinkius and enable the Hudu MCP. This gives your agent secure, read-only access credentials.

02 Instruct your agent using natural language (e.g., 'List all contacts for Company X').

03 The MCP translates that request into a specific API call, fetches the data from Hudu, and returns it to your agent as clean context.

The bottom line is you tell your AI what information you need, and it executes the necessary database queries against Hudu for you.

Built For

This MCP is essential for IT Operations Managers and MSP technical staff who are tired of spending hours manually gathering client data from disparate systems. If your job involves auditing assets, managing passwords, or building initial reports on client infrastructure, this saves serious time.

Managed Service Provider (MSP) Technician

Needs to quickly pull a list of all known company contacts and associated assets when onboarding a new client, instead of logging into five different portals.

IT Operations Analyst

Must audit system activity logs or retrieve documented procedures for compliance checks without writing complex SQL queries.

Technical Consultant

Often needs to list all companies and their associated websites, networks, and assets to scope a new IT project quickly.

What Changes When You Connect

01 Stop manual data gathering. With the `list_companies` tool, you instantly get a full list of every client managed in Hudu, giving you an immediate scope overview for any project.

02 Instant compliance checks. By running the `list_activity_logs`, your agent can pull records of who changed what and when, saving hours of manual auditing.

03 Centralized credential access. You don't need to memorize logins; simply ask to use `list_passwords` and have your AI client retrieve the necessary credentials securely.

04 Better documentation recall. Instead of digging through shared drives, you can request a search of knowledge base articles using `list_articles`, getting direct answers from Hudu's content library.

05 Full IT Picture. Combining calls like `list_assets` and `list_networks` lets your agent build a complete infrastructure picture for a client in one go.

Real-World Applications

Auditing Client Security Protocols

A compliance officer needs to prove that all critical assets are tracked. Instead of pulling reports from the asset management system, they ask their agent to use `list_assets` and then cross-reference those results with `list_procedures` to ensure every device has an up-to-date handling protocol.

Onboarding a New Client

A technician starts onboarding. They ask the agent for all initial data: 'List companies, and get me contacts.' The agent uses `list_companies` and `list_contacts` to pull the core organizational structure immediately.

Investigating a Breach

A security team needs to know what happened yesterday. They ask their AI client to run `list_activity_logs` for the last 24 hours, instantly generating an audit trail instead of manually reviewing log files.

Scope Creep Prevention

A project manager is scoping a network upgrade. They ask the agent to use `list_networks`, which gives them all documented connections and endpoints right away, preventing scope creep later in the month.

Patterns to Avoid

Treating it like a general search engine

✗ AVOID

Asking the agent to 'Find me information about networking' and expecting narrative answers. The MCP is structured for data retrieval, not free-form writing.

✓ INSTEAD

Be specific: Use `list_networks` first to get a list of documented network structures. Then, if needed, use `list_articles` with keywords related to those networks.

Relying on memory

✗ AVOID

Trying to recall a specific company's assets from scratch without using the tool. This is slow and error-prone.

✓ INSTEAD

Start by listing all companies with `list_companies` to narrow down your scope, then use `get_company` to pull the exact details for that entity.

Forgetting credentials exist

✗ AVOID

Assuming a system administrator knows all necessary passwords off the top of their head. This leads to delays and service interruptions.

✓ INSTEAD

Use `list_passwords` when you need immediate access to stored, secured credentials for any given company.

The Right Fit

You should use this MCP if your core IT operations data—assets, contacts, passwords, documentation, and procedures—resides within the Hudu platform. It's a necessity when you need an AI agent to act as a universal search terminal for structured operational records.

Don't use it if your primary goal is purely generative writing, like drafting marketing copy or summarizing meeting notes that aren't

tied to recorded data. For those tasks, you need a general LLM connection. Also, don't rely on this MCP if the critical data lives in an unlisted system (e.g., Jira tickets or SharePoint sites). In those cases, you must look for a dedicated connector for that specific platform instead.

The headache of compiling client reports by hand is real.

Today, compiling an initial report on a client requires hopping between systems. You pull the contact list from one tab, run an asset inventory query in another, then manually search for relevant procedures and passwords across three different dashboards. It’s clicking, copy-pasting, and cross-referencing data until your eyes blur.

With this MCP, the process flips. Your agent gets everything it needs through natural conversation. You just ask: 'Give me the full contact list, all associated assets, and any key passwords for Acme Corp.' The information is assembled and returned to you instantly.

Hudu MCP gives your AI client total visibility into documentation and assets.

You eliminate the need to manually run separate reports. You no longer have to click through the asset inventory, then switch screens to check network details, and finally open a third tab for stored passwords. All that data is now accessible via simple commands.

What changes is this: you stop being an operator running queries and start being a decision-maker relying on immediate, consolidated truth.

Hudu: 10 Tools for IT Operations Management

These tools allow your agent to perform every essential function needed to manage documentation, track assets, and access company data stored in Hudu.

#	TOOL	DESCRIPTION
01	`get_company`	Pulls detailed information for one specific company by ID.
02	`list_activity_logs`	Generates a list of all recent actions taken within Hudu.
03	`list_articles`	Retrieves a list of available knowledge base articles.
04	`list_assets`	Lists every documented piece of IT hardware or software asset.
05	`list_companies`	Returns a comprehensive list of all companies managed in Hudu.
06	`list_contacts`	Gets a list of every contact associated with any company.
07	`list_networks`	Retrieves details about all documented network structures.
08	`list_passwords`	Provides a list of stored passwords for secured access.
09	`list_procedures`	Lists the documented operational procedures used by staff.
10	`list_websites`	Retrieves a list of monitored websites associated with companies.

See It in Action

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

U List all companies documented in Hudu.

I'll fetch the list of companies for you.

U Show me assets for company ID 123.

I'll retrieve the assets documented for that company.

U Find knowledge base articles related to backup procedures.

I'll search your knowledge base for backup procedures.

Frequently Asked Questions

01 **Can the Hudu MCP list all my companies?**

Yes. Using the `list_companies` tool, your AI agent can retrieve a comprehensive roster of every company documented in Hudu immediately.

02 **How do I find stored passwords using the Hudu MCP?**

You instruct your agent to use the `list_passwords` tool. The agent will then securely pull and present a list of all stored credentials for you to review.

03 **What if I only need details on one company, not all of them?**

Use the `get_company` tool; it allows your AI client to retrieve specific, detailed information using a known company ID, narrowing down the scope effectively.

04 **Does Hudu MCP help with compliance and auditing?**

Absolutely. The agent can use the `list_activity_logs` tool to pull recent system activity, giving you an immediate audit trail for compliance purposes.

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 `"hudu": { "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

Hudu 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 Hudu. 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	Hudu MCP
Server ID	`019d75b4-e597-72c6-a58e-7c79cd544faa`
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/hudu.