

MCP SERVER

NO CODE

CLOUD HOSTED

Beekeeper MCP for AI Agents

Organize Internal Team Communications and User Data

Beekeeper MCP connects your agent directly to your internal communication platform. You can manage entire organizational structures—from listing employees and channels to sending private messages—all through natural conversation with your AI client.

A+ Quality Score 100/100

frontline-workers

internal-communications

employee-engagement

team-management

workplace-productivity



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.

Beekeeper MCP

10 tools available

Cloud-hosted on Vinkius

Managing a large, distributed workforce means juggling multiple tools: checking who's on the roster, figuring out which announcement channel is active, and then manually posting the update. This MCP changes that. It lets your agent talk directly to your Beekeeper account, giving you complete control over internal comms and team data right where you work. Instead of logging into a dashboard just to find contact details or check group membership, you simply ask your AI client. Your agent can list all active communication channels, retrieve the full chat history between two specific people, or post an urgent announcement across multiple streams—all without lifting a finger. When integrated via Vinkius, it gives your workflow access to thousands of tools, making internal communications management totally hands-free.

Core Capabilities

01 — Manage employee roster and groups

Get comprehensive lists of all users, specific details about individuals, and the organizational groups they belong to.

03 — Handle direct messaging

Send private messages or retrieve the full conversation history between any two users.

02 — Control communication channels

Discover active discussion streams and publish announcements to keep every team member updated instantly.

04 — Track organizational structure

Access system metadata and detailed tenant information for high-level administrative oversight.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP on Vinkius.
- 02 Provide your Beekeeper Subdomain and API Token credentials to connect the service.
- 03 Start interacting with your agent from any compatible client; you can now manage all workforce communication directly through natural conversation.

The bottom line is, once connected, your AI client handles the authentication and API calls so you never have to switch tabs or copy/paste credentials again.

Built For

This MCP is for HR Managers who spend hours manually verifying contact lists. It's for Operations Leads needing instant, guaranteed communication across specific teams. And it's perfect for Internal Communicators who need to monitor engagement and message flow without diving into the platform itself.

HR Manager

Needs to quickly find employee contact details or verify group membership when onboarding new staff.

Operations Lead

Must publish urgent safety alerts or policy changes to specific frontline streams instantly across the entire organization.

Internal Communicator

Monitors key messages and overall engagement by listing posts and retrieving message histories for reporting purposes.

What Changes When You Connect

- 01 Post announcements instantly: You can use the `create_post` tool to publish urgent updates to specific streams, making sure every relevant employee sees the notice immediately.

-
- 02** Never search manually again: Use `search_users` to find a person's ID or contact info by name or email in seconds. No more clicking through directories.
-
- 03** Keep comms private and tracked: Need to check up on a chat? The agent can use `list_messages` to pull the full conversation history for review.
-
- 04** Understand your team structure: Running reports? You can list all defined groups using `list_groups` or get an overview of every employee with `list_users`.
-
- 05** Get user specifics fast: Instead of guessing, you can use `get_user` to pull specific details on a single person's profile when needed.
-

Real-World Applications

Sending an urgent company-wide safety alert

An operations lead needs to notify everyone about new equipment protocols. Instead of manually navigating and selecting multiple channels, the agent uses `create_post` to publish a single announcement simultaneously across 'Operations Updates' and 'Company News'.

Summarizing a client discussion

A team member wants to check up on a project discussion they were absent for. They ask their agent to use `list_messages` within that specific thread, getting a bulleted summary of the last 20 exchanges.

Finding an employee's direct contact details

An HR manager needs to reach Sarah Miller but doesn't know her user ID. The agent uses `search_users` by name, instantly providing the correct User ID and confirming she belongs to the 'Logistics Team'.

Getting an organizational overview

A manager wants to know who's on the team and what channels exist. The agent first calls `list_groups` to see departmental structure, then uses `list_streams` to map out all active communication areas.

Patterns to Avoid

Treating comms as a database lookup

X AVOID

Trying to figure out who is in the 'Marketing' department by just listing every single user and manually checking group names. This is slow and error-prone.

✓ INSTEAD

Use ``list_groups`` first to verify the departmental structure, then use ``get_user`` on a specific person if you need their full profile details.

Posting updates in silos

X AVOID

Manually having to post an announcement three different times because it applies to 'HR', 'Ops', and 'Sales' teams. You risk missing one channel.

✓ INSTEAD

Use the agent to list all relevant channels with ``list_streams``, then use ``create_post`` once, targeting all necessary streams.

Ambiguous search queries

X AVOID

Just asking 'Find John' and getting too many results because your system has multiple people named John. You waste time filtering.

✓ INSTEAD

Always specify the criteria: use ``search_users`` with a combination of name AND email for the most accurate result.

The Right Fit

You should use this MCP if your primary pain point is managing complex, multi-departmental internal communications or needing instant access to employee roster data. Specifically, if you need to read chat logs (using `list_messages`) or publish time-sensitive announcements across multiple groups, this is the right tool. Don't use it if you only ever check a single user profile; then maybe just using standard platform search is enough. However, if your needs are administrative—like checking global tenant metadata (`get_tenant_info`)—this MCP gives you that oversight through natural language interaction.

Beekeeper MCP for AI Agents: Managing Internal Workforce Communication

Right now, if an urgent message needs to go out, your process is manual. You have to open the platform, check which streams are relevant (Is it 'Ops' or 'Company News?'); then you copy the text, navigate back and forth, and hit 'post' multiple times. If you miss one channel, the message fails.

With this MCP, your agent handles that entire sequence. You tell it, 'Post the new policy update to all relevant teams.' It uses its tools to list every necessary stream, then publishes the announcement once. What you get is guaranteed, complete communication coverage.

Beekeeper MCP for AI Agents: Controlling Employee Directory and User Data

When onboarding or troubleshooting, your time gets eaten up by basic data retrieval. You spend minutes searching the directory to find a person's ID, then maybe another minute checking which groups they belong to just to verify their role.

This MCP eliminates that friction. Your agent can search for users directly using `search_users` or retrieve all group memberships instantly. It hands you exactly the data point you need—the user ID, the contact details, or the full roster list—in a single step.

Beekeeper: 10 Tools for Team Communication Management

Use these tools to list posts in streams, search contacts, create announcements, send direct messages, and retrieve conversation histories with your agent.

#	TOOL	DESCRIPTION
01	<code>list_posts</code>	Retrieves all the content written in a specific communication stream (channel).
02	<code>search_users</code>	Finds employee profiles using either a name or an email address.
03	<code>list_streams</code>	Lists every active discussion channel available across your organization.
04	<code>list_users</code>	Generates a complete roster of all users within the platform.
05	<code>create_post</code>	Publishes an announcement or update to a designated communication stream.
06	<code>send_message</code>	Initiates private, one-on-one chats with any user in the system.
07	<code>get_tenant_info</code>	Gathers administrative data about your entire company's Beekeeper account setup.
08	<code>get_user</code>	Pulls detailed profile information for a single specified employee.
09	<code>list_groups</code>	Retrieves a list of all defined functional groups (e.g., 'Sales', 'Logistics').
10	<code>list_messages</code>	Fetches the conversation history for a specific chat thread.

See It in Action

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

U Can you show me who is on the Sales team and what their email addresses are?



Sales Team Roster

- John Smith (ID: u_123): john.smith@corp.com
- Maria Garcia (ID: u_456): maria.garcia@corp.com
- David Lee (ID: u_789): david.lee@corp.com

You can also view their full group membership list by calling the `list_groups` tool.

U What was the outcome of last week's meeting in the Operations Updates stream?



I pulled the latest messages from 'Operations Updates'. Key takeaways include:

- **New Protocol:** Safety protocols start Monday (Posted by HR).
- **Equipment Status:** The forklift maintenance is scheduled for Tuesday afternoon.
- **Follow-up:** Team needs to submit their updated shift schedules by end of day.

U Send a quick message to Sarah Miller and ask her about the Q3 budget.



✓ Message sent to Sarah Miller (ID: u_99283).

Subject: Q3 Budget Check-in

Hi Sarah, could you send over an update on the Q3 budget projections when you get a minute?
Thanks!

Frequently Asked Questions

01 How does the Beekeeper MCP help me manage company announcements?

It lets your agent publish urgent updates across multiple channels simultaneously. Instead of manually posting to every stream, you send one command and it broadcasts the message everywhere it needs to go.

02 Can I use the Beekeeper MCP to find employee contact info?

Yes, absolutely. You can search for users by name or email, and the agent will pull up their full details right away. This saves you from manually searching through directories.

03 Is the Beekeeper MCP good for tracking conversations?

It's great for that. You can ask your agent to retrieve message histories between any two users, giving you a full record of what was discussed in that specific chat thread.

04 Does the Beekeeper MCP connect to all my company departments?

Yes, it gives you visibility into every defined group and communication stream. You can list all channels and groups within your organization using the agent's tools.

05 What if I need administrative data about my Beekeeper account?







The MCP includes functions to retrieve tenant information, so you get system-level metadata for high-level oversight. It helps administrators verify the overall health of the connection.

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>"beekeeper": { "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

Beekeeper 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 Beekeeper. 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	Beekeeper MCP
Server ID	019d755a-5d39-7221-a301-839fe5bf2826
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/beekeeper.