MCP SERVER | NO CODE | CLOUD HOSTED

Flock MCP

Control team comms and audit groups via natural language.

Flock MCP gives your AI client full control over team communications inside Flock. It lets you manage private groups, list public channels, audit who is a member of any group or channel, and send rich, formatted messages directly from natural conversation. You can also pull historical chat logs and retrieve employee metadata by alias.

A+ Quality Score 100/100

team-chat | instant-messaging | rich-messaging | workspace-management | channel-automation | roster-management

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

SCAN TO VIEW

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.

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.

Flock MCP

10 tools available
Cloud-hosted on Vinkius

This MCP connects your AI agent to the full power of Flock, letting you manage every aspect of team communication without leaving your chat interface. Forget switching between dashboards or running manual reports just to confirm who needs to know what. Instead, you use natural language to get answers about your organization's roster and group structures.

Need to announce a policy change? You can send formatted, rich messages using advanced layouts straight into any channel. Want to audit security? Your agent can identify private groups or check which users are active members of specific channels. It even handles the messy work of mapping user aliases (like @john_doe) to their permanent UUIDs. When you connect through Vinkius, you get access to this full catalog of Flock tools, letting your AI client handle everything from checking chat logs to retrieving employee time zones and LDAP properties.

It means your agent doesn't just talk about your team; it actively manages the flow of information across your entire organization.

Core Capabilities

01 — Sending Rich Messages

Send formatted messages, including rich attachments and styled layouts, to any established Flock chat.

02 — Auditing Group Memberships

Identify members for specific channels or audit the explicit active UUIDs attached to a group to verify who can see sensitive content.

03 — Managing Private Groups

List all private groups and inspect their internal credentials to understand exactly how they operate within your company's structure.

04 — Listing Public Channels

Get a complete list of every public channel available in the workspace, along with details about its banners and descriptions.

05 — Roster Mapping & User Details

Find precise user metadata (like time zones or emails) for any employee by their alias, or get a directory mapping all active users to their UUIDs.

06 — Retrieving Chat History

Pull chronological logs and raw JSON objects from any specific room's chat history for auditing purposes.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius, then enter your Flock Bot Token in the developer dashboard.

02 Connect your preferred AI client (like Cursor or Claude).

03 Tell your agent what you need—for example, 'List all public channels and check who belongs to #announcements.' — and it executes the actions.

The bottom line is that your AI agent becomes a natural language interface for complex team communication tasks.

Built For

IT Admins who spend hours running membership reports, Operations Teams managing cross-departmental announcements, and Team Leads who need to coordinate private group updates without leaving their chat client.

IT Administrator

Audits channel memberships or verifies organizational roster mappings using natural language commands instead of running multiple manual reports.

Team Manager

Coordinates sensitive announcements or sends updates to private groups directly from the chat interface without needing IT help.

Product Operations Specialist

Monitors public channels and checks historical logs to track when specific features were discussed, pulling raw data into a database.

What Changes When You Connect

01 Stop manually listing users. With the `roster_list_directory` tool, your agent gets a definitive map of every employee's alias to their UUID, making targeting messages accurate every time.

02 Audit permissions without fear. You can use `groups_list_members` to check who has read access to a sensitive group, guaranteeing that only the intended audience sees critical information.

03 Send better announcements. The `chat_send_message` tool lets you bypass basic Markdown and send richly formatted messages with enterprise attachments straight into any channel.

04 Track conversations historically. Need proof of what was said? Use `chat_fetch_messages` to pull raw, chronological JSON logs from a room for deep auditing.

05 Understand the structure. You can use `groups_list_private` and `channels_get_info` together to map out your entire communication topology—public channels, private groups, and their specific rules.

06 Get user context instantly. The `users_get_metadata` tool retrieves essential profile details for any employee, including their time zone or LDAP properties.

Real-World Applications

Handling an executive announcement

A manager needs to send a critical policy update only to the core leadership team. Instead of manually listing every group and sending messages, they ask their agent: 'Send this memo to all members in the Executive Steering Group.' The agent uses `groups_list_members` then `chat_send_message`, ensuring perfect delivery.

Onboarding a new cross-functional team

An HR specialist needs to confirm who belongs to three different project channels (Product, Marketing, Engineering). They simply ask their agent: 'List all members in these three channels.' The agent runs `channels_list_members` for each, providing one consolidated list of active UUIDs.

Investigating a data leak

A security analyst must determine if sensitive client data was shared outside the intended group. They ask their agent to pull all chat logs from the relevant room using `chat_fetch_messages`, providing raw JSON objects for forensic review.

Updating user contact info

A developer needs to verify if a contractor's time zone or email address has changed. They use their agent to run the `users_get_metadata` tool on the alias, getting real-time profile details without logging into HR systems.

Patterns to Avoid

Assuming a user's UUID

✗ AVOID

A user tries to send a message by guessing the target person's ID or using an old alias, which results in a failed delivery error.

✓ INSTEAD

Always use the `roster_list_directory` tool first. It guarantees you get the current, accurate mapping of every active @ alias to their absolute UUID before sending anything.

Missing group membership checks

✗ AVOID

A team lead tries to post an announcement to a private group, but doesn't know if certain departmental members are actually allowed to read it, risking visibility issues.

✓ INSTEAD

Use the `groups_list_members` tool before posting. This audits who has explicit read permissions for that specific group.

Over-relying on plain text messaging

✗ AVOID

A manager tries to share a complex spreadsheet and formats it with basic Markdown, losing the rich visual context.

✓ INSTEAD

When sending updates via `chat_send_message`, instruct your agent to use FlockML capabilities. This ensures the payload renders as a proper, formatted enterprise attachment.

The Right Fit

Use this MCP if your workflow requires managing or querying structured team communication data within Flock. Specifically, you need to audit membership (using `channels_list_members` or `groups_list_members`), map user identities (`roster_list_directory`, `users_get_metadata`), or send rich content directly into the chat. Don't use this if you simply need to read a document stored in Dropbox, because this MCP only handles communication data. If your goal is just general task automation (like creating Trello cards), look for an external project management tool integration instead.

The pain of manual team communication audits

Right now, checking who belongs to a group or what was discussed last week is a multi-step nightmare. You jump between the main chat interface and internal reporting dashboards. You run one report for public channels, another for private groups, then you copy lists of user IDs—it's slow, error-prone clicking across half a dozen tabs.

With this MCP, your agent handles it all in one go. Instead of running reports, you just ask the question: 'Who is in the finance group?' The agent runs `groups_list_members`, pulls the UUIDs, and gives you a direct answer. It changes auditing from tedious report generation to instant query response.

Getting immediate control with Flock MCP

You don't have to manually find every single user ID or check the system settings for group permissions anymore. The agent runs `roster_list_directory` and `groups_get_info` in the background, giving you structured data that a human would spend hours compiling.

It's simple: your AI client talks directly to Flock's core functions. You stop managing reports and start making decisions based on real-time, accurate information.

Flock MCP with 10 Tools

These tools let you manage everything from listing public channels to auditing private group memberships, all through natural language commands.

#	TOOL	DESCRIPTION
01	channels_get_info	Retrieves the description and banner configuration for any specific channel.
02	channels_list_public	Gets a list of every public channel active in your Flock workspace.
03	channels_list_members	Identifies and lists the UUIDs of all members attached to a specific channel.
04	groups_list_members	Audits group boundaries to list members with read permissions, crucial for verifying sensitive targets.
05	roster_list_directory	Provides a directory mapping every active user's direct @ alias to their absolute UUID for accurate routing.
06	chat_send_message	Sends formatted messages using advanced layouts directly into an existing Flock chat room.
07	chat_fetch_messages	Pulls recent chat history for a room, returning raw JSON objects with chronological messages.
08	users_get_metadata	Retrieves structured profile metadata (like time zone and email) linked to any Flock user identity.
09	groups_get_info	Inspects the deep internal credentials needed to understand a specific private group's operation.
10	groups_list_private	Returns an array of all bounded private groups, helping you find the correct routing UUIDs.

See It in Action

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

U Send a message to group 'g:123': 'Project update is live!'

Message dispatched! 'Project update is live!' has been sent to group g:123. I've used your bot token to route the payload through the Flock API synchronously.

U List all public channels in my Flock workspace

Retrieving channels... I found 5 public environments: '#general', '#product-news', '#marketing', '#announcements', and '#engineering'. Which one would you like to see the members for?

U Get the metadata for user '@john_doe'

Retrieving identity... For alias '@john_doe' (UUID: u:456), I found: Name: John Doe, Email: john@example.com, Time Zone: America/New_York. He is currently an active member of 3 private groups.

Frequently Asked Questions

01 **How do I send a message using the Flock MCP?**

You use the `chat_send_message` tool. Simply ask your agent to 'Send an announcement about the new deadline' and it handles routing the rich payload into the correct chat.

02 **Can I see who is in a private group using Flock MCP?**

Yes, you use `groups_list_members`. This tool audits the IAM boundaries of the specific group to list every active UUID that has read access, keeping your data secure.

03 **What if I need a user's time zone for an announcement?**

Use `users_get_metadata`. This tool retrieves structural profile metadata linked to any Flock identity, including their current time zone and LDAP properties.

04 **How do I find all the public channels available?**

Run the `channels_list_public` tool. It enumerates every public channel in your workspace, giving you a full map of your accessible communication areas.

05 **Is it possible to get historical chat logs with Flock MCP?**

Yes, use `chat_fetch_messages`. This tool pulls chronological records and raw JSON objects from any specific room's history for thorough review.

06 **Can my agent send formatted messages using FlockML?**

Yes. Use the 'chat_send_message' tool and provide your XML string in the 'flockml' parameter. The agent will bypass standard Markdown limits to render rich enterprise attachments and layouts natively in Flock.

07 **How do I list all members of a specific private group via chat?**

Use the 'groups_list_members' tool. Provide the Group UUID. Your agent will surface the explicitly mapped profiles within that group, helping you verify sensitive message targets securely.

08 **Can I search for a user's UUID using their '@' alias through the agent?**

Absolutely. The 'roster_list_directory' tool discovers global identity blocks mapping direct aliases to absolute string UUIDs, ensuring you can route messages accurately to anyone in your company.

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 `"flock": { "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

Flock 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 Flock. 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	Flock MCP
Server ID	`019d759b-89c1-71a8-9059-e9d374a66606`
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/flock.