MCP SERVER | NO CODE | CLOUD HOSTED

CHATFLY MCP for AI Agents

Manage custom chatbot knowledge bases and support workflows

CHATFLY connects your AI agents directly to your custom knowledge base and chatbot environment. It lets you manage bot performance, retrieve full conversation histories, upload documents for training, and send live test messages—all through natural language commands from any compatible AI client.

A+ Quality Score 100/100

custom-ai-bots | knowledge-base | document-training | conversational-ai | data-source-integration | ai-training

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

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.

CHATFLY MCP

8 tools available
Cloud-hosted on Vinkius

If you're managing a team of specialized chatbots, you know the struggle: tracking down which data source trained which bot, or figuring out exactly why a customer conversation went off script. This MCP solves that by giving your agent direct access to your entire CHATFLY environment.

Instead of jumping through dashboards and clicking tabs, your AI client can list every chatbot in your account, check the full message history for any given thread, or even trigger retraining on new documents with a simple prompt. You can send test messages directly to verify bot responses instantly. It gives you complete oversight, letting you audit resource usage and manage complex knowledge bases without leaving your chat window.

Because this functionality is housed in Vinkius, you get access to CHATFLY's full suite of tools—from listing all uploaded documents to triggering the actual training process—all through one connection point. It puts enterprise-grade chatbot management right where you do your work.

Core Capabilities

01 — Inventory and Monitor Chatbots

List every custom AI bot in your account, check specific bot details, or retrieve core usage data like quotas.

02 — Manage Knowledge Sources

View a list of all documents currently uploaded to the knowledge base and trigger retraining on new source material.

03 — Audit Conversations and History

Retrieve recent chat conversations or pull up the full message history for any specific interaction.

04 — Simulate Live Interactions

Send test messages directly to a bot and receive an immediate, AI-generated response in real time.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and provide your CHATFLY API Key.

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

03 Use natural language prompts within your agent to manage bots, review data, or run tests.

The bottom line is: you talk to your bot management system using simple conversation prompts, and it handles the complex backend calls for you.

Built For

This MCP is essential for Support Managers who need constant visibility into chatbot performance. Content Strategists use it to manage knowledge documents without logging into a separate dashboard. Product Teams rely on this when they need to quickly test bot responses and audit customer interactions directly from their chat interface.

Support Manager

Reviewing customer chat logs or monitoring chatbot performance across different product lines using natural language queries.

Content Strategist

Triggering the retraining process for a bot when new policy documents are uploaded, without having to open the main CHATFLY dashboard.

Product Team Lead

Running quick test messages against a staging chatbot to verify that a recent feature update trained correctly before going live.

What Changes When You Connect

01 Audit bot performance immediately. Use the `get_conversation_history` tool to pull full message transcripts, letting you analyze exactly what was said in past customer interactions.

02 Keep your bots up-to-date instantly. You can trigger retraining using `trigger_bot_training` directly through your agent, eliminating the need to navigate a separate dashboard to update knowledge sources.

03 Maintain oversight of your entire system. The `list_chatfly_bots` tool gives you an instant roster of all available bots, and `get_chatbot_details` shows their specific status and configuration.

04 Test bot responses live. Use the `send_bot_message` action to send simulated customer queries and get real-time AI replies instantly, validating functionality before deployment.

05 Monitor resource limits without effort. The `get_chatfly_account_info` tool pulls core account data, so you always know your current usage quotas.

Real-World Applications

Investigating a Customer Complaint

A support manager needs to understand why an agent gave the wrong answer last week. They ask their agent to use `get_conversation_history`, instantly retrieving the full transcript so they can pinpoint the exact point of failure and fix the bot's underlying knowledge.

Adding New Product Knowledge

A content strategist adds a new white paper. Instead of waiting for manual updates, they ask their agent to use `list_uploaded_documents` first, confirm the file is there, and then immediately use `trigger_bot_training` so the bot knows about the new product data by morning.

Pre-launch Bot Testing

A product team lead needs to verify how a beta chatbot handles complex pricing questions. They prompt their agent, which uses `send_bot_message` to send five different scenarios, allowing the team to validate responses without needing test credentials.

Auditing System Health

A business owner wants a quick summary of system usage. They prompt their agent for account info, which uses `get_chatfly_account_info` to return total conversation counts and resource consumption in seconds.

Patterns to Avoid

Trying to manage bots via generic APIs

✗ AVOID

Writing a custom script that requires hardcoding bot IDs, document IDs, and API endpoint structures. This is slow, brittle, and needs constant maintenance.

✓ INSTEAD

Use the CHATFLY MCP within your agent. You can simply ask your AI client to 'list all my active chatbots' (using `list_chatfly_bots`) or 'get me the chat history for last week' (using `list_fly_conversations`). Your agent handles the complex API structure.

Manually copying conversation logs

✗ AVOID

A support manager has to manually go into the web dashboard, find a customer interaction from two weeks ago, and copy all the text into a spreadsheet for reporting.

✓ INSTEAD

Ask your agent to use `get_conversation_history` with specific date parameters. The MCP pulls the full transcript directly into your chat interface, ready for review or export.

Assuming data is automatically updated

✗ AVOID

A content team uploads a new policy document but forgets to manually tell the bot it exists, so the chatbot keeps answering with old, incorrect information.

✓ INSTEAD

After uploading documents (verified via `list_uploaded_documents`), you must explicitly ask your agent to use `trigger_bot_training` on that specific bot. This ensures the knowledge base is actively updated.

The Right Fit

You should connect this MCP if your workflow requires conversational intelligence for managing internal chatbots and knowledge bases. Use it when you need your AI client to act as an operational layer, checking usage quotas (`get_chatfly_account_info`), auditing specific conversations (`get_conversation_history`), or initiating critical maintenance tasks like bot retraining (`trigger_bot_training`). Don't use this if you only need simple data retrieval; for instance, if you just want to view a list of bots, the `list_chatfly_bots` tool handles that. However, if your goal is complex workflow orchestration—like sending messages and then updating records in a CRM—you might need multiple MCPs connected together.

CHATFLY MCP: Automating Chatbot Knowledge Base Updates

Right now, when your company policy changes or you add a new product line, someone has to manually log into the chatbot dashboard. They find the correct bot, upload the new document, and then hit 'Start Training.' This process is slow; it's prone to human error, and those critical knowledge updates often get delayed or forgotten.

With this MCP, you tell your agent: 'Update the Support Assistant with the Q3 pricing guide.' The system handles the entire sequence. It checks the document list (`list_uploaded_documents`), confirms the file is ready, and triggers the retraining process using `trigger_bot_training` . You get a confirmed update status directly in your chat.

CHATFLY MCP: Monitoring Support Conversation Performance

Without this direct connection, reviewing performance means logging into the analytics dashboard and sifting through pages of data to find a specific conversation thread. To check if an

Now, your agent gives you full conversational oversight. You can ask it to 'Show me the full history of all pricing calls from Tuesday.' It uses `list_fly_conversations` and

agent handled a certain query correctly last week, you have to manually search for that user's ID or date range—a tedious chore.

`get_conversation_history` to pull up exactly what happened, letting you analyze performance in minutes instead of hours.

CHATFLY: 8 Tools for Chatbot Knowledge Base Management

Use these tools to list documents, retrieve chat histories, manage bot details, and trigger training cycles through natural language commands.

#	TOOL	DESCRIPTION
01	`list_uploaded_documents`	Retrieves a list of all files currently housed in the knowledge base.
02	`get_chatbot_details`	Provides detailed information about a single, specific chatbot instance.
03	`get_conversation_history`	Pulls up the complete message transcript for a given conversation thread.
04	`get_chatfly_account_info`	Fetches core account details and current AI usage quotas.
05	`list_chatfly_bots`	Lists every active chatbot configured within the account.
06	`list_fly_conversations`	Provides a list of the most recent chat sessions that occurred.
07	`send_bot_message`	Sends an immediate message to a chatbot and receives the resulting AI response.
08	`trigger_bot_training`	Initiates the data ingestion process, retraining a specific chatbot using new sources.

See It in Action

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

U List all my active bots and tell me if they're trained on the new marketing guides.

Chatbot Inventory Report

BOT NAME	STATUS	LAST TRAINED ON
Support Assistant	Ready	2026-05-15 (Policies)
Sales Closer	Needs Review	2026-03-01 (Old Pricing)
Internal FAQ Bot	Operational	2026-06-19 (HR Updates)

The 'Sales Closer' bot needs retraining on the latest guides. I can trigger that now if you want.

U Show me what the Sales Closer bot would say about returns over $500.

Sending test message to Sales Closer...

The AI responded: 'For high-value returns exceeding $500, please ensure you have your original receipt and proof of purchase. We recommend contacting our dedicated Returns department at 1-800-XYZ for immediate assistance.'

U What were the last few conversations about billing issues?

Billing Conversation Summary

- **[User A]**: Questioned the $29 fee. (History retrieved: 2026-06-18)
- **[User B]**: Asked how to dispute a charge. (History retrieved: 2026-06-17)
- **[User C]**: Needed clarification on the annual billing cycle. (History retrieved: 2026-06-15)

I found three recent threads focusing on billing, detailing the specific issues discussed.

Frequently Asked Questions

01 **How can CHATFLY MCP help me audit my chatbot’s performance?**

You can use this MCP to pull full message transcripts for any conversation. This lets you review exactly what was said, helping you pinpoint knowledge gaps or incorrect responses in your bot's training data.

02 **Do I need to manually update my bots when policies change?**

Not anymore. You can use the MCP to trigger retraining on new documents directly from your chat interface, ensuring your chatbot uses the latest company policies immediately after you upload them.

03 **Can I test my chatbot responses before showing them to customers?**

Yes. The MCP allows you to send simulated messages to any bot and receive a live AI response in real time, letting you verify the accuracy of its answers instantly.

04 **What happens if I add new documents to my knowledge base?**

The system lists all uploaded files. To make sure the chatbot uses them, you must use the MCP to explicitly trigger a training run on the specific bot that needs the update.

05 **How do I check how much of my AI usage quota is left?**

The MCP has an account info tool. You simply ask your agent for 'account details,' and it retrieves your core resource usage information, keeping you aware of any spending limits.

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 `"chatfly": { "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

CHATFLY 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 CHATFLY. 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	CHATFLY MCP
Server ID	`019d756d-813d-736b-8c19-f51a480c3f0d`
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/chatfly.