MCP SERVER | NO CODE | CLOUD HOSTED

ChatBot.com MCP for AI Agents

Manage bot workflows and conversational story data

ChatBot.com lets your AI agent take full control of conversational automation and bot workflows. It gives you a single point of access to monitor every user interaction, track complex story paths, and audit bot performance directly from any compatible AI client.

A+ Quality Score 100/100

conversational-ai | bot-workflows | customer-service-automation | chat-automation | interaction-tracking | ai-agents

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

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.

ChatBot.com MCP

8 tools available
Cloud-hosted on Vinkius

Stop switching between the chat interface, the analytics dashboard, and the training log just to understand what your customer service bot is doing. This MCP connects ChatBot.com's full suite of conversational data directly into your agent. You can monitor entire story paths, list every user who has interacted with the bot, or even retrieve specific unrecognized phrases that signal a gap in your knowledge base. It's about getting intelligence on conversation flow—the whole picture—without ever leaving your chat window. If you're managing multiple systems for bot performance, Vinkius makes it simple: connect once and get access to this full catalog of conversational tools. You can use the agent to look up user profiles or check webhook settings, letting you manage complex automation tasks using natural conversation.

Core Capabilities

01 — Audit Bot Workflows

List all existing bot stories and retrieve detailed information for any specific conversational workflow.

02 — Track User Activity

Pull lists of every user who has interacted with the bot, or get a deep profile on individual users by their unique ID.

03 — Analyze Conversation Flow

Review all recorded interactions within a specific story to follow exactly how a conversation unfolded and where it went wrong.

04 — Identify Training Gaps

Access the list of unrecognized phrases, telling you precisely what users are saying that your bot doesn't understand yet.

05 — Manage Integrations and Data

Review all configured webhook integrations or examine core system metadata like entity definitions to audit how the bot is connected.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and enter your ChatBot Developer Access Token.

02 Connect your preferred AI client, such as Cursor or Claude, using the token.

03 Ask your agent to perform a task, like 'List all users who chatted with the bot today,' and it executes the necessary data retrieval.

The bottom line is that you treat complex back-end data management—like checking user records or training logs—as if it were just another natural conversation prompt for your AI client.

Built For

This MCP targets people who own the bot workflow, not just the content. If you're a Customer Experience Manager spending hours cross-referencing dashboards to figure out why user X got stuck on step 3, this is for you. It gives your team an immediate operational view of bot performance.

Customer Experience Manager

Monitors overall bot health by listing stories and running reports to see which parts of the journey are failing or confusing users.

Conversational Designer

Audits existing story paths and interactions directly through their chat interface, allowing them to spot flow issues without opening a complex content management system.

Support Team Lead

Quickly looks up user details and specific chat histories for troubleshooting or compliance checks straight from the agent's prompt window.

Product Manager

Analyzes unrecognized phrases to identify where the bot needs new training data, guiding the roadmap for improvements.

What Changes When You Connect

01 Instead of manually checking dashboards, your agent can list all stories via `list_chatbot_stories` and give you an instant overview of the entire bot's capabilities.

02 You instantly get context by using `list_story_interactions`, letting your agent trace a user through every single chat message to pinpoint where the confusion happened.

03 The ability to use `list_training_data` means you don't have to guess what the bot doesn't know; your agent reports the exact phrases that need adding to the training set.

04 When troubleshooting, running `get_chatbot_user_details` lets you pull a full user profile and conversation history without jumping between multiple internal tabs.

05 Audit connections easily. Use `list_chatbot_webhooks` or review system metadata with `list_chatbot_entities` to ensure your bot's external data links are correct.

Real-World Applications

Diagnosing a Failed Customer Journey

A user asks their agent: 'Why did the refund request fail for User 90210?' The agent runs `get_chatbot_user_details` and then uses `list_story_interactions` to show the exact sequence of messages, pinpointing where the bot gave incorrect information.

Updating Bot Knowledge Base

A product manager asks their agent: 'What are we missing in our FAQ flow?' The agent runs `list_training_data` and returns a list of unrecognized phrases, immediately giving the PM actionable items for bot retraining.

Auditing Bot Connections

A development team needs to check all outgoing data points. They ask their agent: 'Show me all webhook connections.' The agent runs `list_chatbot_webhooks` and displays the full list of active external integrations for review.

Reviewing Bot Scope

A CX manager asks their agent: 'What are our current bot flows?' The agent uses `list_chatbot_stories` to present a complete catalog, allowing the manager to see every defined workflow at a glance.

Patterns to Avoid

Treating Bot Data Like Static Reports

✗ AVOID

A user tries to manually copy conversation logs from an internal dashboard into a spreadsheet to analyze flow, which takes hours and is prone to formatting errors.

✓ INSTEAD

Instead, ask your agent to run `list_story_interactions` or `get_story_details`. The MCP gathers the entire sequence of events and presents it structured data that you can immediately use in your workflow.

Ignoring Bot Performance Gaps

✗ AVOID

The team assumes the bot is working fine because most chats succeed, but critical edge cases are failing silently.

✓ INSTEAD

Use `list_training_data` to actively surface those gaps. The agent retrieves phrases that users typed but the bot failed to recognize, showing you exactly where retraining is needed.

Confusing User Data with System Metadata

✗ AVOID

A user needs to know if a specific data type (like a shipping zip code) is properly defined for the bot's logic, but they don't know which system setting to check.

✓ INSTEAD

Use `list_chatbot_entities` to list and review custom entities. This tells you what structured information the bot recognizes and relies on.

The Right Fit

You should use this MCP if your main goal is operational visibility into how your chatbot performs in a live environment, especially when tracking complex conversations or needing to audit who talks to the bot. Use it if you need to understand *why* a conversation failed—was it the story path, insufficient user data, or poor training? Don't use this MCP if all you need is basic content editing for a single workflow; that requires direct access to the chatbot platform itself. If you just want to list users, while `list_chatbot_users` works, remember that running `get_story_details` provides much richer context about *why* those users interacted.

ChatBot.com MCP for AI Agents: Managing Customer Service Bot Stories

Today, checking bot performance means logging into the chat platform, navigating to the analytics tab, and manually clicking through story logs, user data lists, and training reports. It’s a fragmented process that forces you to switch context constantly just to get one clear answer about customer failure points.

With this MCP, your agent pulls all of that information together. You ask it to 'Audit the refund flow for yesterday,' and it runs through `list_chatbot_stories` and `list_story_interactions`, returning a single, comprehensive data set detailing every step, interaction, and deviation—giving you immediate, actionable answers.

ChatBot.com MCP for AI Agents: Tracking Conversational User Data

Without this tool, finding out if a specific customer provided an email or what their name was requires querying multiple databases and manually correlating user IDs across different chat sessions.

Now, your agent handles it. You simply ask for 'The details on User 543,' and the MCP uses `get_chatbot_user_details` to pull the secure profile data instantly. It simplifies complex customer record retrieval into a simple conversation.

ChatBot.com: 8 Tools for Bot Workflow Analysis

These tools let you list all stories, check user details, audit interactions, and identify gaps in bot training.

#	TOOL	DESCRIPTION
01	`get_story_details`	Retrieves detailed information about a specific conversational story or workflow path.
02	`get_chatbot_user_details`	Pulls and displays detailed profile information for one specific user who interacted with the bot.
03	`list_chatbot_entities`	Lists all custom entities that the bot uses to understand and match specific data types, like names or product codes.
04	`list_story_interactions`	Generates a full list of every single interaction that took place within a defined story path.
05	`list_chatbot_stories`	Provides an overview and list of all active bot workflows or conversational stories configured in the system.
06	`list_training_data`	Compiles a report of unrecognized phrases, highlighting areas where the chatbot needs immediate training updates.
07	`list_chatbot_users`	Gathers and lists every user who has ever initiated a conversation with your bot.
08	`list_chatbot_webhooks`	Reviews all configured webhook integrations, helping you audit how the chatbot sends data to other services.

See It in Action

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

U List all bot workflows we have set up right now.

Bot Story Audit Report

Here are the 6 active conversational stories:

- `Main Greeting` : The initial customer touchpoint.
- `Product FAQ` : Handles billing and feature questions.
- `Lead Generation` : Collects contact info for sales follow-up.
- `Customer Support Flow` : Escalation path to human agents.
- `Billing Inquiry` : Specific flow for invoice issues.
- `Account Update` : For changing passwords or addresses.

Which story should I dive into? Just name it.

U What phrases are users typing that the bot doesn't understand?

Training Data Gap Report

We found 18 unrecognized phrases since last week. These require immediate training:

- 'How do I cancel my subscription?' (Frequency: 12)
- 'Talk to a human agent now.' (Frequency: 8)
- 'Is there an alternative product?' (Frequency: 5)

Please review these and add them as new intents to the `Product FAQ` story.

U Show me all users who opened a chat yesterday.

Yesterday's User Activity Log

We found **34 unique users** interacting with the bot yesterday. Key insights:

- 12 users came from 'Product FAQ'.
- 5 users completed the `Lead Generation` workflow.
- The top source of traffic was the main website, generating 7 new interactions.

Frequently Asked Questions

01 **How can I check if my chatbot is losing performance or needs retraining?**

You can use ChatBot.com MCP to list unrecognized phrases and get a report on what users are saying that the bot doesn't understand yet. This tells you exactly where your conversational flows need immediate attention.

02 **Can I see every single conversation path for a specific customer?**

Yes, by connecting ChatBot.com MCP, you can retrieve all interactions within a story. It gives you the full history—every message exchanged—so you know exactly how and why the user reached their current point.

03 **How do I audit who has used my bot? Does it track every person?**

You can list all users who interacted with your bot through ChatBot.com MCP. It provides a complete roster of unique users, helping you measure overall adoption and usage patterns.

04 **Does this help me find out what my bot's current workflows are?**

Absolutely. The MCP lets your agent list all active stories (bot workflows). This gives you a full map of every conversation path the chatbot knows how to handle, perfect for scope review.

05 **What if I need to know what external systems my bot talks to?**

You can use ChatBot.com MCP to list all configured webhook integrations and audit your system's metadata. This confirms every connection point, ensuring your data routes are secure and correct.

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 `"chatbotcom": { "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

ChatBot.com 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 ChatBot.com. 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	ChatBot.com MCP
Server ID	`019d756d-67e7-7200-8a74-094b189bdea8`
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/chatbotcom.