

MCP SERVER

NO CODE

CLOUD HOSTED

Gallabox MCP

Manage chats, contacts, and templates instantly.

Gallabox MCP handles all your WhatsApp Business communication through any AI client. Use this to automate outreach, manage shared inboxes, send templates, and track complete customer conversation history at scale. It lets agents interact with contacts and channels without needing a dashboard.

A+ Quality Score 100/100

whatsapp-automation

shared-inbox

chatbot

transactional-messaging

customer-engagement

notifications



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.

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.

Gallabox MCP

12 tools available

Cloud-hosted on Vinkius

Need to handle high-volume messaging for your business? This MCP connects your WhatsApp Business account directly to any AI agent, giving it deep access to your communication tools. You can use it to manage shared inboxes and deploy bots that act like trained support staff. Instead of logging into a separate platform, your AI client talks directly to Gallabox. It reads the full message history for specific conversations, verifies contact details, and lets you list all approved templates before sending anything out. This capability is critical because it keeps the entire communication flow within your agent's natural conversation, allowing real-time actions on things like listing active chats or checking which support teams are available. Because this MCP lives in Vinkius, your AI client gets instant access to these tools, making complex WhatsApp workflows feel as simple as asking a question.

Core Capabilities

01 — Monitor and retrieve chat history

Get the full context of any conversation by listing active chats or fetching detailed message threads for specific IDs.

03 — Automate messaging outreach

Send standard text messages to customers, or deploy pre-approved templates for transactional notifications at scale.

05 — Coordinate team support tasks

Access details about support teams and verify your own account metadata to assign chats efficiently.

02 — Manage contacts and profiles

View your contact database, get individual profile details, or even check if a phone number is valid.

04 — Organize communication assets

List all available message templates and identify configured WhatsApp channels by accessing channel IDs.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP through the Vinkius Marketplace.
- 02 Enter your Gallabox API Key and API Secret into the connection settings.
- 03 Your AI client now handles all WhatsApp workflows, allowing you to send messages or check histories via natural conversation.

The bottom line is that once connected, your AI agent treats your entire WhatsApp Business account like a set of functions it can call on demand.

Built For

This MCP is for operational teams and marketing leads whose jobs depend on constant communication. If you spend time manually switching between dashboards or copying IDs to build reports, this saves hours.

Support Lead

Uses the MCP to list all active chats or check message history for a specific conversation ID when they need to hand off a ticket quickly.

Marketing Manager

Automates follow-ups by listing approved templates and sending them out based on campaign status, without touching the WhatsApp web interface.

Customer Success Operations Specialist

Verifies contact metadata or lists support teams to ensure a customer is routed to the right person with all necessary background info.

What Changes When You Connect

- 01 Contextual replies are automatic. Instead of manually digging through logs, asking the agent to list thread messages gives it the full history needed to draft an accurate response.

-
- 02** Streamlined support triage. You can use list active chats or list support teams to immediately know who owns a conversation and if it's already flagged for attention.

 - 03** Compliance guaranteed. Before sending anything out, you can call list message templates to make sure the outreach uses only approved language and structure.

 - 04** Data accuracy on demand. Get contact details anytime by using get contact details to verify name or phone number before a critical communication.

 - 05** Full visibility across channels. List whatsapp channels identifies every unique ID so your agent knows exactly where to route messages, whether it's internal or external.

-

Real-World Applications

A customer asks about an order status update.

The Support Agent uses the MCP to list thread messages for the conversation ID. The agent reads the last five exchanges, sees the original order number mentioned, and then sends a simple text message to confirm the tracking link.

A new chat comes in with unclear contact info.

Instead of guessing, the Ops Specialist asks the agent to get contact details. The agent confirms the user's name and company before sending a personalized welcome message via send whatsapp text.

Marketing needs to launch an appointment reminder campaign.

The Marketing Manager asks the agent to list message templates. They select 'Appointment Reminder' and use send whatsapp template to execute the outreach instantly across 50 contacts.

The team needs to audit all open conversations today.

A Support Lead simply uses list active chats, which provides an immediate dashboard view of every conversation thread that is currently ongoing or waiting for attention.

Patterns to Avoid

Trying to manually copy IDs

X AVOID

The user spends ten minutes navigating the Gallabox dashboard, copying a chat ID, pasting it into their notes app, and then trying to feed that raw text snippet into the AI agent.

✓ INSTEAD

Just tell your AI client, 'Show me the message history for this conversation.' The agent uses list thread messages directly and provides the context without you ever touching an ID.

Sending random, unapproved messages

X AVOID

A marketing person drafts a quick, non-compliant follow-up message on the fly, risking brand inconsistency or policy violations.

✓ INSTEAD

Always check list message templates first. If you need to send an update, use send whatsapp template with the correct, pre-vetted format.

Assuming contact data is fresh

X AVOID

A sales rep sends a personalized follow-up email based on old notes because they forgot to check if the number changed.

✓ INSTEAD

Before any outreach, ask your agent to get contact details. This verifies that the phone number and profile metadata are current.

The Right Fit

Use this MCP if managing WhatsApp communication is a core part of your business process, requiring automation or complex context retrieval. Specifically, you need to reliably list message templates, check thread histories (list thread messages), and send structured notifications via send whatsapp template.

Don't use it if all you need is simple data viewing without action. For example, if you only want a static list of contacts for an external spreadsheet, using the MCP might be overkill. If your needs are purely internal process management (like managing ticketing queues in Jira), look at dedicated workflow automation tools instead.

This MCP excels when combining retrieval and execution: use list active chats to find problems, then use get chat details to understand them, and finally use send whatsapp text to fix them.

The Manual Headache of Customer Communication

Right now, running a shared inbox means living in a series of tabs. You see a notification pop up for an important customer message; you jump over to the dashboard, manually search for the thread ID, click into it, copy the last five messages just to understand what happened, and then switch back out to your AI agent—only to paste that raw, messy text block into the prompt.

With this MCP integrated via Vinkius, the entire process collapses. You tell your agent about the customer, and it handles the heavy lifting behind the scenes. It pulls the complete message history using list thread messages and feeds the clean context directly to its memory. The result is immediate: you get actionable intelligence without ever opening a dashboard or copying an ID.

Gallabox MCP Gives You Full Control Over Your Messaging

Forget manually checking which channels are live, or wondering if the right team is available. The

What changes is your ability to trust the system. You're no longer guessing; you're executing based

MCP lets you query list whatsapp channels for routing IDs and use list support teams to verify who can take the chat. This stops guesswork before it starts.

on verified data. Your AI client simply needs permission to access these tools, giving you enterprise-grade control over every message sent.

Gallabox: 12 Tools for WhatsApp Automation

These tools allow your AI client to interact with every aspect of your WhatsApp Business account, from listing active chats to sending templated messages.

#	TOOL	DESCRIPTION
01	<code>verify_api_connection</code>	Checks if your API credentials are valid and connected correctly.
02	<code>get_contact_details</code>	Retrieves detailed profile information for a specific contact.
03	<code>get_chat_details</code>	Fetches metadata about an entire conversation thread.
04	<code>get_my_profile</code>	Retrieves the account profile information for your current user.
05	<code>list_whatsapp_channels</code>	Lists all active WhatsApp Business channels configured in your account.
06	<code>list_whatsapp_contacts</code>	Retrieves a list of contacts available within your chat records.
07	<code>list_active_chats</code>	Lists all current, ongoing WhatsApp conversations in your shared inbox.
08	<code>list_thread_messages</code>	Retrieves the complete message history for any given conversation ID.
09	<code>list_support_teams</code>	Lists all support teams configured within your Gallabox account.
10	<code>list_message_templates</code>	Shows you every approved message template available for sending out.
11	<code>send_whatsapp_template</code>	Sends a pre-approved, structured message using one of your saved templates.
12	<code>send_whatsapp_text</code>	Sends a simple, freeform text message to any contact.

See It in Action

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

U Send a WhatsApp message to '+1234567890' saying 'Hello from AI!'.



Message sent! I've successfully queued your WhatsApp message to +1234567890 via Gallabox. The message will appear in your open conversations inbox.

U List all my approved WhatsApp templates.



Retrieving templates... I found 5 approved templates, including 'Order Confirmation', 'Welcome Message', and 'Appointment Reminder'. Which one would you like to use?

U Show the message history for conversation 'conv_987'.



Fetching thread... For conversation conv_987, I found 3 recent messages. The customer asked about 'shipping times' and the bot replied with the standard '2-4 days' policy.

Frequently Asked Questions

01 How do I list all active conversations using Gallabox MCP?

Use the list active chats tool. This immediately provides a comprehensive list of currently running conversation threads, letting your agent know exactly what attention is needed.

02 Can Gallabox MCP send messages if I don't have a template?

Yes. You can use the send whatsapp text tool for simple, freeform messaging to any contact. For structured or branded outreach, you should use send whatsapp template.

03 What is the difference between list_whatsapp_contacts and get_contact_details?

list whatsapp contacts provides a general directory of names available in your chat history. However, get contact details fetches specific metadata for one person, verifying their current profile information.

04 Does Gallabox MCP handle support team assignments?

Yes. You can use list support teams to see which groups are available and verify your own account profile with get my profile before assigning a chat for optimal handoff.

05 Is it safe to let the AI client send messages via Gallabox MCP?







The system is designed around pre-approved templates. The tool list message templates ensures you only deploy compliant messaging, minimizing risk when using send whatsapp template.

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>"gallabox": { "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

Gallabox 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 Gallabox. 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	Gallabox MCP
Server ID	019d75a2-48a5-7134-a399-f615234c0a9c
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/gallabox.