MCP SERVER | NO CODE | CLOUD HOSTED

Courier MCP for AI Agents

Monitor multi-channel message delivery status and user profiles

Courier connects your AI agent directly to multi-channel notification infrastructure. Use this MCP to send messages across email, SMS, push alerts, and chat apps, while also monitoring their real-time delivery status. It gives you full visibility into whether a message was sent, delivered, opened, or clicked by the recipient.

A+ Quality Score 100/100

notifications | multi-channel | api-integration | message-delivery | real-time-sync | workflow-automation

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

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.

Courier MCP

10 tools available
Cloud-hosted on Vinkius

Managing communications across different channels used to mean jumping between multiple dashboards—checking email sends here, looking up phone numbers there, and manually tracking status updates in a third system. This MCP changes that. Instead of dealing with siloed data, your AI agent handles complex notification workflows using natural conversation.

It lets you trigger messages through any channel (email, SMS, push) and, critically, gives you real-time visibility into the message life cycle. You can monitor who received a message and when they opened it or clicked a link. Need to check user details? The MCP provides tools to list user profiles and even audit previous communication history. If your current system makes tracking deliveries feel like a job for an intern, Vinkius hosts this Courier integration so your agent handles it all automatically. You just tell the AI what needs to be sent, and it manages the rest.

Core Capabilities

01 — Send notifications via various channels

Sends messages using templates across email, SMS, push alerts, and chat apps.

02 — Check message delivery history

Retrieves detailed logs showing if a sent message was delivered, opened by the user, or clicked on.

03 — Get specific user contact details

Pulls basic contact information like email or phone number for a specific user ID.

04 — Segment users into target groups

Retrieves specific saved audience groups and subscription lists for targeted marketing efforts.

One Click on Vinkius — From Prompt to Execution

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

01 Connect the Courier MCP to your AI client using an API token. This authorizes your agent to access message logs, user profiles, and sending capabilities.

02 Your agent identifies the necessary data points—like the target recipient's profile or a specific audience list ID—and calls the relevant tools within this MCP.

03 The MCP executes the request against the Courier system, returning structured data that your AI client uses to formulate a final answer for you.

The bottom line is: You talk to your agent in plain English, and it translates that into specific API calls to manage communications for you.

Built For

This MCP helps marketing ops leads who are tired of checking five different dashboards just to see if a campaign email landed. It's essential for support managers needing instant access to user history, and developers building reliable notification systems.

Customer Support Specialist

Checks a customer's profile data or message history instantly when they call in, giving the customer a full view of their communication trail.

Marketing Automation Manager

Sends welcome sequences to new users and audits if those multi-step notifications actually reached the intended recipients.

Software Developer

Builds reliable notification features into an application, needing to track delivery logs and user preferences programmatically.

What Changes When You Connect

01 Verify critical system notifications instantly. Instead of guessing if a password reset email worked, use the Send API to trigger messages and monitor their success.

02 Pinpoint why communications fail. If users are complaining about emails not arriving, audit message history or get message details to find out if the issue was delivery failure or simply not opened.

03 Stop manual list management. You can use list_audiences and list_subscription_lists to target campaigns precisely without manually sorting through spreadsheets.

04 Better support interactions. With get_user_profile, your agent pulls all necessary contact details and channel preferences in one step, making customer service faster.

05 Build reliable workflows. By listing available notification templates using list_templates, you ensure that every message sent adheres to proper branding and messaging standards.

Real-World Applications

Tracking a failed onboarding sequence

The marketing team needs to know if the welcome email and subsequent SMS reminder actually went out. Asking the agent to list messages allows them to see which steps succeeded (using list_messages) and where the process stalled.

Investigating a user complaint

A customer claims they never received a critical alert. The support specialist asks the agent to get message details for that specific ID, instantly showing whether the platform recorded a 'DELIVERED' status or if it failed entirely.

Segmenting users for a promotion

The sales team wants to run a special campaign only on premium subscribers. The agent uses list_subscription_lists and then combines that data with get_user_profile to build the precise target group.

Validating system alerts post-update

A developer needs to confirm that a new critical alert (like an account lock) is properly sent. They use send_notification, and then follow up with list_messages to check the immediate delivery status.

Patterns to Avoid

Relying on single-channel checks

✗ AVOID

Assuming that if you sent an email notification, it must have been seen. You might only check the 'sent' status in a basic client.

✓ INSTEAD

Don't just send it; ask your agent to list messages and then use get_message_history on the resulting IDs. This confirms not just the send time, but also if it was delivered or opened.

Manual user data compilation

✗ AVOID

Copying a customer's email from one CRM screen into another system to manually verify their preferences and contact details.

✓ INSTEAD

Ask the agent to get_user_profile. It pulls all necessary contact info and channel-specific delivery preferences in one clean query, saving you multiple clicks.

Using generic message sending

✗ AVOID

Sending out a general alert without remembering which templates or brands are appropriate for the campaign.

✓ INSTEAD

First, use list_templates to see what's available. Then, when you send a notification using send_notification, your agent ensures the correct template and brand settings apply.

The Right Fit

Use this MCP if your core problem is visibility into communication failure points. Specifically, if you need to know *if* an alert reached the user (delivery status) or *how many* people can receive it (audience lists), this is for you.

Don't use this if your only goal is to write a nice-sounding message in a vacuum; you still need another tool for drafting. Also, don't use it just because your current system sends notifications—you must be able to audit the history using get_message_history or check user details with get_user_profile.

If you are only building simple one-time alerts and never care about tracking if they were opened, then a basic communication tool might suffice. But if auditing is part of your job, this MCP provides the necessary depth.

Courier MCP for AI Agents: Auditing multi-channel message delivery history

Currently, checking notification status involves a tedious mess. You open your email dashboard to see if it was sent, then switch to the SMS portal to check if that landed, and finally log into your CRM just to verify the user's current contact preferences. It’s constant context switching, making troubleshooting slow and painful.

With this MCP, you simply ask your agent about a message. It instantly checks the entire event timeline using list_messages or get_message_history. You don't waste time jumping between tabs; you just get the full status report—delivered, opened, clicked—right away.

Courier MCP for AI Agents: Managing targeted user communication lists

Building a campaign list manually is a headache. You have to export data from different sources,

The agent handles this complex filtering for you. By listing audiences or using get_user_profile, your

then cross-reference IDs and names just to ensure you're only sending the promotion to active, premium subscribers. It’s error-prone work.

AI client automatically compiles a clean list of eligible recipients ready for mass notification sends. You go from data chaos to actionable targets instantly.

Courier: 10 Tools for Multi-Channel Message Tracking

Use these tools to list users, check profiles, send notifications, and get deep logs on every message sent across all channels.

#	TOOL	DESCRIPTION
01	`get_message_history`	Retrieves detailed event logs showing the full status (sent, delivered, opened) of a specific message ID.
02	`get_message_details`	Gets deep details about a single message, including provider responses and rendering metadata.
03	`get_user_profile`	Pulls basic contact information like email or phone number for a specific user ID.
04	`list_audiences`	Lists the names and IDs of saved groups used to target notifications, helping segment your recipients.
05	`list_brands`	Retrieves a list of custom brands configured in Courier for white-labeling purposes.
06	`list_subscription_lists`	Lists the IDs and names of subscriber groups, useful for managing large lists of potential recipients.
07	`list_messages`	Lists all messages sent by ID, providing current statuses like DELIVERED or CLICKED along with timestamps.
08	`list_templates`	Retrieves a list of available notification templates and the channels they support for sending.
09	`list_users`	Lists all user accounts registered within your Courier workspace environment.
10	`send_notification`	Sends a new notification to the specified recipient, routing it through the best available channel and template.

See It in Action

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

U What was the delivery status of the alert sent last Tuesday to user 456?

Message Status Report

The message (ID: XYZ-987) was successfully **DELIVERED** on June 10th, 2024. It shows a history of:

- `SENT` : 2024-06-10T09:00:00Z
- `DELIVERED` : 2024-06-10T09:05:12Z (via Email)
- `OPENED` : 2024-06-10T09:07:30Z
- `CLICKED` : Link to pricing page @ 2024-06-10T09:07:30Z

The last action was a link click. Do you want me to check the full event log?

U Send a welcome message with template ID 'welcome_v2' to user john@testcorp.com.

Action Taken:

A 'Welcome' notification has been queued for john@testcorp.com.

- **Template Used:** Welcome Series v2
- **Target Channel:** Email and Push Alert (Best available)
- **Status Check:** We are monitoring the delivery status in real time. You will receive an alert when we confirm 'Delivered' or if any error occurs.

U List all notification templates and tell me which ones support SMS.

Available Notification Templates

TEMPLATE NAME	ID	SUPPORTED CHANNELS
Password Reset	TPL-100	Email, Push
New Login Alert	TPL-205	Email, SMS
Monthly Digest	TPL-330	Email only

SMS support is currently limited to the 'New Login Alert' and other system alerts. The 'Monthly Digest' must be sent via email.

Frequently Asked Questions

01 **How can I check if a message actually got delivered using the Courier MCP for AI Agents?**

You don't have to guess. The agent checks the full history of that specific message, confirming its delivery status (delivered, opened, etc.). This is critical for knowing your communication actually made it to the user.

02 **Do I need technical skills to use the Courier MCP for AI Agents?**

No. You just talk to your agent in natural language. Tell it what you want—like 'Check the status of my last campaign'—and the MCP handles all the complex API calls behind the scenes.

03 **What if I need to send a notification through multiple channels?**

The MCP makes that easy. You can ask your agent to send one message, and it routes it automatically across email, SMS, or push notifications based on what's best for the recipient.

04 **Can I use Courier MCP for AI Agents to find out user details?**

Yes. You can ask your agent to get a user profile by ID. It pulls contact info, like email and phone number, plus their specific channel preferences all in one place.

05 **How does Courier MCP for AI Agents help with marketing campaigns?**

It lets you run highly segmented campaigns. You can list saved audiences or subscription lists to ensure your messages only go out to the right people, saving time and avoiding mistakes.

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 `"courier": { "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

Courier 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 Courier. 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	Courier MCP
Server ID	`019d757d-58c4-73d0-9f1d-857592131488`
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/courier.