MCP SERVER | NO CODE | CLOUD HOSTED

# Termii MCP

## Verify Users and Send Messages Globally.

Termii connects your AI agent to a unified communication platform, letting you manage global outreach across SMS, WhatsApp, and voice channels. It handles secure user onboarding by sending and verifying One-Time Passwords (OTP). You can also check account balances and list authorized Sender IDs, all without leaving your conversational interface.

A+ Quality Score 100/100

multi-channel-messaging | otp-verification | whatsapp-business | voice-messaging | customer-engagement | api-messaging

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

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.

# Termii MCP

6 tools available
Cloud-hosted on Vinkius

You use this MCP to handle every part of customer communication, from initial contact to final verification. Instead of jumping between a messaging dashboard, an SMS portal, and a security console, you talk directly to your agent. Your agent executes complex tasks like sending a WhatsApp notification, immediately followed by triggering an OTP code via SMS, all in one conversation thread. You manage the entire lifecycle—the message delivery, the identity check, even monitoring if you have enough credit—using natural language commands. This capability makes global engagement reliable and fast. By connecting Termii through Vinkius, your agent gains access to a powerful communication layer that supports everything from simple broadcast texts to complex, multi-step verification flows.

## Core Capabilities

**01 — Send targeted messages**

You send standard text messages via SMS or richer media formats through WhatsApp.

**02 — Secure user identity**

The MCP programmatically sends and confirms One-Time Passwords (OTP) to verify new users during onboarding.

**03 — Check account resources**

You check your current credit balance and list which Sender IDs are registered for use.

**04 — Manage communication channels**

The MCP routes messages across multiple formats, including SMS, WhatsApp, and voice channels globally.

## One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Termii API Key in the Vinkius settings.

02 Direct your AI client to perform a communication task, such as sending an OTP or checking balance.

03 Your agent executes the request through Termii and returns the real-time status of the transaction.

The bottom line is that you get global messaging and secure verification built into your natural conversation flow.

## Built For

This MCP is essential for companies focused on rapid, verifiable customer growth. It's for the product owner who can't afford friction in onboarding, or the marketing director who needs real-time visibility into message campaign performance across multiple channels.

**DevOps Engineer**

Uses the MCP to quickly test message delivery flows and integrate OTP verification steps into a deployment script.

**Customer Success Manager**

Automates proactive outreach campaigns, sending follow-up messages via WhatsApp or SMS based on customer activity status.

**Security Analyst**

Monitors and verifies identity tokens by triggering OTP codes for high-security user accounts and auditing communication history.

## What Changes When You Connect

01 Automate secure user sign-ups. Instead of having users manually enter codes, your agent can trigger the `send_otp` tool to send a code, followed by using `verify_otp` to confirm identity in a single workflow.

02 Manage all global messaging from one place. You can use `send_sms`, `send_whatsapp`, or other channels without switching tools or dashboards. Your agent handles the routing.

03 Never run out of visibility into costs again. Use `check_balance` to instantly verify your current account credit, stopping unexpected overages before they happen.

04 Maintain brand consistency across all messages. Run `list_sender_ids` to confirm which authorized IDs you can use for outgoing campaigns, ensuring users recognize your brand name.

05 Reduce friction in outreach. Send targeted marketing updates or alerts using the appropriate channel—whether it's a quick SMS or a richer WhatsApp message.

## Real-World Applications

**Onboarding a new user base**

A company needs to onboard 500 users rapidly. The agent first uses `send_otp` to deliver the verification code, then calls `verify_otp` with the response. This ensures every new account is instantly secured and ready for use.

**Running a multi-stage marketing campaign**

A sales team needs to follow up with leads who haven't opened an email. The agent first checks `check_balance` to ensure funds are available, then sends the targeted reminder using `send_whatsapp`, ensuring maximum visibility.

**Auditing message history and branding**

A security team needs to confirm allowed communication channels. They start by running `list_sender_ids` to see all authorized sender names, then use this list when initiating a high-priority alert via `send_sms`.

**Crisis communication and alerts**

A service provider needs to instantly notify customers about an outage. The agent uses its ability to send messages across channels, sending critical updates using the most reliable method available (SMS or WhatsApp) without manual intervention.

# Patterns to Avoid

### Juggling different platform dashboards

✗ AVOID

Manually checking your balance on one portal, then going to a second dashboard to send the message, and finally using a third system just to verify the code.

✓ INSTEAD

Connect Termii MCP. Let your agent handle the entire sequence: first `check_balance` for funds, then use `send_otp`, and finally confirm with `verify_otp`. It keeps everything in one chat.

### Using generic messaging tools

✗ AVOID

Relying on basic email systems that don't offer real-time delivery tracking or multi-channel support, leading to lost messages and poor user experience.

✓ INSTEAD

Use this MCP. It supports SMS, WhatsApp, and voice channels, giving you reliable delivery reporting for every message sent.

### Forgetting sender identification

✗ AVOID

Sending mass communications without verifying your Sender ID first, which can result in messages being flagged as spam or rejected entirely.

✓ INSTEAD

Before a campaign, run `list_sender_ids`. This ensures you use an authorized and recognized brand name for all outgoing traffic.

## The Right Fit

Use this MCP if your core business function revolves around secure, multi-channel communication: user onboarding (OTP verification), transaction alerts, or high-volume customer outreach. You need a single point of interaction that can handle SMS, WhatsApp, and manage the associated costs using `check_balance`. Don't use it if you are only sending internal employee memos; in that case, a simple ticketing system integration might suffice. However, if your requirement involves verifying user identities or ensuring messages reach outside email systems, this MCP is necessary because it combines secure verification ( `send_otp` / `verify_otp` ) with global messaging capabilities.

## Messaging and Verification Used to Be a Mess.

Today, managing customer communications means logging into three different places. You check your balance in one dashboard; you send the actual SMS or WhatsApp message from another; and then, when a user responds with their code, you have to manually copy that code into a third verification portal just to confirm they are legitimate. It's slow, prone to human error, and takes way too much time.

With this MCP connected via Vinkius, the entire process runs through your agent's conversational flow. You simply ask your agent to 'Verify user X,' and it handles checking the balance, sending the code using `send_otp`, waiting for the reply, and confirming validity using `verify_otp`. The result is immediate, audited communication.

## The Termii MCP Gives You Full Communication Control.

Specific steps that disappear include manually switching between SMS and WhatsApp interfaces, separately checking credit usage by running `check_balance`, and piecing together the verification status from multiple logs. The agent does all of this automatically in the background.

It's not just sending a message; it's controlling a complex communication workflow end-to-end. You own the process, which is a massive operational improvement.

# Termii: Communication Tools (6)

Use these tools through your agent to send messages across multiple channels, manage account credits, and securely verify user identities.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `check_balance` | Gets a real-time reading of your current account credit balance. |
| 02 | `list_sender_ids` | Retrieves all the Sender IDs that are authorized and registered to your account. |
| 03 | `send_otp` | Initiates delivery of a unique one-time password (OTP) to a specified phone number. |
| 04 | `send_sms` | Sends a standard text message via the SMS channel. |
| 05 | `send_whatsapp` | Delivers a business-grade message through WhatsApp. |
| 06 | `verify_otp` | Checks if a submitted OTP code is valid for the target phone number. |

# See It in Action

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

**U** Send a verification code (OTP) to +15550199.

Verification initiated! I've triggered the OTP code delivery to +15550199 via Termii. The request reference ID is pin_88231. I'll let you know when the user provides the code to verify.

**U** Check my account balance.

Fetching balance... You currently have $45.50 in your Termii account. This balance is sufficient for your upcoming automated SMS and WhatsApp campaigns.

**U** List all Sender IDs registered for my account.

I've retrieved your Sender IDs. You have 3 authorized IDs: 'VINKIUS', 'ALERT_MS', and 'AUTH_MSG'. Which one would you like to use for your next campaign?

# Frequently Asked Questions

01 **How does Termii MCP handle WhatsApp messages?**

You use the `send_whatsapp` tool to send business-grade messages directly through WhatsApp. This allows you to reach customers where they prefer to communicate, maintaining a high engagement rate.

02 **Can I verify users using Termii MCP?**

Yes, identity verification is handled by the `send_otp` tool to trigger the code and the `verify_otp` tool to validate it. This ensures secure user onboarding for your platform.

03 **Is there a way to check my spending limits with Termii MCP?**

You run the `check_balance` tool, which provides an accurate, real-time reading of your current account credit balance. This keeps you from running into unexpected billing issues.

04 **Does Termii MCP support multiple sender names?**

Absolutely. Use the `list_sender_ids` tool to retrieve all registered Sender IDs, ensuring that every message is sent with your recognized brand name.

05 **What types of messages can I send with Termii MCP?**

You can use dedicated tools for SMS (`send_sms`), WhatsApp (`send_whatsapp`), and manage voice channels, giving you multi-channel coverage globally.

# 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 `"termii": { "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

# Termii 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 Termii. 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 | Termii MCP |
| Server ID | `019dd171-2ae3-721d-8cf7-e6eb628823e5` |
| 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/termii.