MCP SERVER | NO CODE | CLOUD HOSTED

CM.com MCP for AI Agents

Managing Customer Communications Across Multiple Channels

CM.com MCP connects your AI agents directly to a unified messaging platform for conversational commerce. It lets you manage customer outreach across WhatsApp, SMS, RCS, and voice channels using natural conversation. Handle everything from sending bulk alerts and verifying two-factor authentication codes to distributing complex HTML emails—all without writing dedicated integration code.

A+ Quality Score 100/100

sms-notifications | omnichannel-messaging | whatsapp-business | otp-verification | conversational-commerce | voice-api

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

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.

CM.com MCP

11 tools available
Cloud-hosted on Vinkius

This MCP connects your AI agent to CM.com's robust communication system, giving it control over all your customer outreach channels. You can manage communications across WhatsApp, SMS, RCS, voice calls, and email from a single conversational flow. For example, an automated workflow can first use the capability to send an OTP via SMS, and if verification is needed, the agent handles that entire loop using the `verify_otp` tool. Beyond security, you'll handle bulk campaigns by sending multiple SMS messages or running comprehensive marketing blasts. The system also supports rich messaging formats for platforms like WhatsApp and Viber, meaning your messages look professional, not just like plain text alerts. Since Vinkius hosts this MCP, you don't need to worry about complex API setups; you just connect your preferred AI client and start sending messages.

Core Capabilities

01 — Send multi-channel notifications

Dispatch personalized or bulk alerts using SMS, rich WhatsApp messages, RCS, or automated voice calls.

02 — Manage authentication flows

Automate security protocols by sending temporary OTP codes via SMS and verifying the correct code against your account.

03 — Broadcast marketing campaigns

Send large batches of personalized text messages to multiple recipients simultaneously for promotions or updates.

04 — Deliver complex emails

Send professional HTML formatted emails using CM.com's dedicated email delivery infrastructure.

05 — Handle voice communications

Place automated calls or send voice notifications, useful for delivering audio codes or reminders.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP and enter your CM.com Product Token from your Channels dashboard.

02 Next, instruct your AI agent on the communication goal, specifying the channel (e.g., SMS or WhatsApp) and recipient details.

03 Finally, your agent executes the required action—whether that's sending a single message, initiating an OTP flow, or checking your credit balance—and reports the outcome.

The bottom line is you use natural language prompts to trigger complex, multi-step messaging and delivery processes across multiple communication channels.

Built For

This MCP is essential for Operations Teams who need automated, reliable customer alerts. It's perfect for Security Teams implementing robust two-factor authentication flows directly into AI workflows, or Marketing Teams running large-scale campaigns without needing a dedicated dev team.

Operations Coordinator

Sends transactional updates, like shipment confirmations or appointment reminders, via SMS and WhatsApp based on system triggers.

Security Analyst

Builds automated login verification systems by triggering OTP messages and confirming the received codes within an AI workflow.

Marketing Manager

Deploys bulk SMS campaigns or sends rich, template-based WhatsApp messages to segmented customer lists for promotions.

What Changes When You Connect

01 You can run full authentication flows, from sending an OTP via SMS to verifying the code using `verify_otp`, all within a single agent workflow.

02 The platform handles multi-channel delivery. You don't have to write separate logic for WhatsApp rich messages (`send_rich_message`) versus standard text alerts (`send_sms`).

03 Marketing teams gain efficiency by executing massive, simultaneous broadcasts using the `send_bulk_sms` tool, updating customer records instantly.

04 Security workflows become simpler. You can mandate two-factor authentication steps that use both `send_otp_sms` and the subsequent verification step.

05 The agent manages diverse media types. Whether you need a formal HTML email (`send_email`) or an automated voice alert (`send_voice_message`), it's covered.

Real-World Applications

Handling Post-Login Security Checks

A user attempts to log in. The agent detects no session, triggering the flow: first using `send_otp_sms` to send a code, then waiting for the user input, and finally confirming success with `verify_otp`. This completes the authentication cycle automatically.

Running International Sales Campaigns

The marketing agent needs to contact 500 leads. Instead of writing a loop in code, it uses `send_bulk_sms` to hit every number instantly and checks the current credit balance first using `get_balance`.

Confirming Appointment Details

A user books an appointment. The agent automatically sends a rich WhatsApp message (`send_rich_message`) confirming details, ensuring all required formatting and namespaces are correct for the platform.

Dispatching System Alerts to Employees

The operations team needs to notify multiple departments about an outage. They use `list_numbers` to pull all necessary contacts and then execute a series of targeted alerts using standard SMS messages (`send_sms`).

Patterns to Avoid

Hardcoding Channel Logic

✗ AVOID

Writing separate code blocks for WhatsApp, plain SMS, and email whenever you need to send a simple alert. This makes updates painful.

✓ INSTEAD

Use the agent to abstract the channel choice. If an alert needs sending, let your AI client decide whether to use `send_rich_message` or `send_sms`, keeping your workflow clean regardless of the delivery medium.

Forgetting Balance Checks

✗ AVOID

Trying to send a large batch of messages without first checking if you have enough credits, leading to failure and unexpected costs.

✓ INSTEAD

Always check account status first. Start your workflow by calling `get_balance` before initiating any bulk sending using `send_bulk_sms`.

Treating OTP as a single action

✗ AVOID

Only writing code to send the initial SMS, but forgetting the necessary step to capture and confirm the user's response.

✓ INSTEAD

Build the full security loop. Use `send_otp_sms` followed immediately by incorporating `verify_otp` into your workflow logic.

The Right Fit

Use this MCP if your core need is reliable, multi-channel customer communication—specifically handling transactional alerts and authentication flows across WhatsApp, SMS, RCS, or voice. This includes scenarios where you must verify a code after sending an OTP via SMS. Don't use it if you only need to send one type of message (e.g., just email). For isolated tasks like purely managing contact lists without messaging capabilities, another dedicated directory tool might work better. However, if the goal is communicating *with* customers and proving delivery status, this MCP is necessary.

CM.com Messaging: Automating Transactional Alerts with CM.com MCP

Today, sending a simple transaction alert—like 'Your password reset link is here' or 'Your order has shipped'—requires multiple manual steps. You might copy the message body into an email client, then switch to your SMS dashboard for a text version, and finally send a rich media update through WhatsApp. This means jumping between three different interfaces just to get one piece of information out.

With this MCP, you tell your agent once: 'Alert the user about X.' The system handles choosing whether that needs an email via `send_email`, a standard SMS using `send_sms`, or a rich message through WhatsApp. You get reliable delivery across all channels without ever touching a dashboard.

CM.com Messaging: Implementing Secure OTP Workflows with CM.com MCP

Manual security flows are complex and error-prone. You have to manually trigger the code send, wait for a human to receive it, copy it down, paste it into another system, and then confirm it worked—a process that slows everything down.

Now, your agent manages the entire sequence: It sends the initial code via `send_otp_sms`, captures the user's response, and completes the verification using `verify_otp`. The whole flow is automated, making security checks instantaneous.

CM.com: 11 Tools for Conversational Commerce Messaging

You can send bulk messages, trigger OTP verification flows, dispatch rich media updates, or check your account balance using these specific tools.

#	TOOL	DESCRIPTION
01	`get_balance`	Checks the current credit balance of your CM.com account.
02	`list_numbers`	Retrieves a list of all virtual phone numbers associated with your CM.com account.
03	`send_bulk_sms`	Sends text messages to multiple recipients in a single request for mass communication.
04	`send_email`	Sends an HTML formatted email using the CM.com delivery infrastructure.
05	`send_otp_sms`	Triggers the sending of a One-Time Password code via SMS to a specified phone number.
06	`send_rich_message`	Sends a message using rich media formats available on platforms like WhatsApp or Viber.
07	`send_sms`	Sends a standard text message to a single recipient.
08	`send_voice_message`	Initiates an automated call to deliver a voice notification or alert.
09	`send_voice_otp`	Sends an audio recording containing a One-Time Password code.
10	`send_whatsapp`	Dispatches a pre-approved WhatsApp Business template message to a recipient.
11	`verify_otp`	Confirms and validates a user-provided One-Time Password code.

See It in Action

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

U Send a bulk SMS notification to all customers in the 'Bronze Tier' group about our sale today.

SMS Campaign Report

- **Target Group:** Bronze Tier (1,240 contacts)
- **Message Body:** Don't miss out! 💸 30% off everything until midnight. Use code SALE30.
- **Status:** ✅ Bulk SMS initiated successfully.
- **Details:** 1,240 messages queued for sending. Estimated credit usage: 1,240 credits.

U We need to authenticate a new user. Send an OTP code to +1555987654 and then wait for them to confirm the code is 482910.

Authentication Flow Log

- **Step 1: Code Sent:** SMS sent to +1555987654. (ID: ver_xyz)
- **Step 2: Verification Attempt:** Input code 482910.
- **Result:** ✅ SUCCESS. The user account is now authenticated. Flow complete.

U Email our partners a weekly summary of sales and the current credit balance.

Weekly Summary Email Report

- **Recipient:** partners@company.com
- **Subject:** Weekly Sales Performance & Account Update
- **Body Sent:** (HTML format applied)
- **Attachment Status:** Attached PDF report.
- **Account Check:** Current Credit Balance: 4,231 credits remaining.

Frequently Asked Questions

01 **How do I send different types of alerts (SMS, WhatsApp, email) using the CM.com MCP for AI Agents?**

You tell your agent what you need to communicate; it handles which channel is best. You can trigger SMS text messages, rich media updates on WhatsApp, or formal HTML emails all from the same prompt.

02 **Can I use CM.com MCP for AI Agents to build a secure login process?**

Yes. You can automate two-factor authentication by having your agent send an OTP code via SMS and then waiting until you confirm that the code is correct.

03 **What if I need to reach many people for marketing? Does CM.com MCP support this?**

It does. You can use bulk messaging tools to send out thousands of SMS alerts or rich campaign messages simultaneously, making large-scale campaigns easy.

04 **Does the CM.com MCP for AI Agents handle voice notifications?**

Yes, you can trigger automated calls or send audio alerts using the MCP. This is useful when a simple text message won't cut it, like delivering an important reminder.

05 **Do I need to write custom code for every channel? Is CM.com MCP for AI Agents helpful?**

No. By using this MCP, you interact with the platform through natural conversation. You don't write separate integration code; you just tell your agent what needs to happen.

06 **How do I check if my messaging account has enough credits before a big campaign?**

You can start any workflow by asking the MCP to retrieve your current credit balance. This ensures you know exactly how many messages you can send before running a bulk blast.

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 `"cmcom": { "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

CM.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 CM.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	CM.com MCP
Server ID	`019dd0d3-4cfd-7207-9062-5cd5b9705681`
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/cmcom.