MCP SERVER | NO CODE | CLOUD HOSTED

Mitto MCP

Automate SMS, 2FA Verification, and Number Lookups.

Mitto automates global communication workflows directly from your AI agent. Send single or bulk SMS messages, secure accounts by sending and verifying Two-Factor Authentication (2FA) codes via SMS or voice, and validate phone numbers to ensure deliverability.

F Quality Score 3.6/100

sms-api | two-factor-authentication | otp-verification | global-messaging | number-lookup | telecom

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

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.

Mitto MCP

27 tools available
Cloud-hosted on Vinkius

Connecting Mitto through Vinkius lets your AI client handle complex messaging tasks right where you write code. You can trigger large-scale outreach campaigns with a single command, sending bulk SMS messages globally while tracking which countries see the most activity. If an account needs securing, your agent handles the entire 2FA process: it sends the One-Time Password (OTP) and then waits for you to feed back the verified code using specific tools. Beyond messaging, Mitto helps with phone number hygiene. You can look up any given phone number to check its carrier information before sending a message, making sure your campaigns don't fail due to invalid numbers. Developers use this MCP to integrate robust communication and authentication into applications without ever leaving their chat window or IDE.

Core Capabilities

01 — Global SMS Messaging

Send single messages or manage large-scale, bulk message campaigns across various countries.

02 — Two-Factor Authentication Management

Initiate the 2FA process by sending a verification code and completing the cycle by verifying the received OTP against an account.

03 — Number Validation and Lookup

Check if a phone number is valid, determine its carrier, or mask numbers for privacy before use in communications.

04 — Usage Reporting

Retrieve detailed metrics on SMS volume and 2FA attempts, grouped by country or date range.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the Mitto MCP and enter your specific API key.

02 Instruct your AI client to perform a communication task—like sending an SMS or requesting a code—using natural language.

03 Your agent executes the necessary tool calls, manages the data flow (e.g., waiting for confirmation of the OTP), and provides the final status update.

The bottom line is that your AI client acts as the orchestrator, managing the communication steps without you having to jump between a dashboard and an API call.

Built For

Marketing managers running campaigns across borders; support engineers who need instant, verifiable customer communications; or developers building secure, message-driven applications.

DevOps Engineer

Integrates SMS and 2FA flows into CI/CD pipelines so new microservices can verify users immediately upon deployment.

Support Specialist

Sends quick, verifiable account status updates or password reset codes directly to a customer chat thread instead of waiting for email confirmation.

Marketing Campaign Manager

Runs high-volume bulk SMS campaigns to segmented user lists and tracks the conversion rates from those messages in real time.

What Changes When You Connect

01 Saves time by handling multi-step processes. Instead of manually sending a code, waiting for confirmation, and then logging the result, your agent can execute `send_2fa` followed by `verify_2fa` in one sequence.

02 Ensures deliverability before you spend credits. Before running any campaign, use `lookup_number` to validate recipient numbers, preventing messages from failing due to simple formatting errors.

03 Manages complex privacy requirements automatically. You can establish a secure communication boundary by using tools like `create_masking_context` and `add_masked_number`, ensuring customer data is protected at the source.

04 Handles high volume effortlessly. Running marketing campaigns that require sending thousands of messages is simple with `send_bulk_sms`, which keeps your workflow moving without manual batch uploads.

05 Provides clear accountability. You don't just send a message; you get analytics, like using `get_sms_usage_by_country` or `track_sms_conversion`, so you know exactly where and how well your messaging efforts are working.

Real-World Applications

Handling High-Volume Account Onboarding

A developer needs to onboard 50 new users. Instead of writing a script that handles the request, wait time, and verification API calls separately, they prompt their agent: 'Run the full onboarding flow for these 50 numbers.' The agent uses `send_2fa` for every user and then waits for confirmation using `verify_2fa`, completing the entire process in one go.

Running Geo-Targeted Marketing Campaigns

A marketing manager needs to know if their latest campaign is working better in Germany versus France. They prompt the agent to run a report, which uses `get_sms_usage_by_country` to provide instant metrics showing where the highest engagement was.

Securing Customer Data for Support

A support team member needs to reset a customer's password. They tell their agent, 'Verify user John Doe.' The agent calls `send_2fa` and then prompts the agent to await confirmation, streamlining what was previously a three-step phone call process.

Auditing Communication Security

An audit team needs to prove that sensitive number data is correctly masked. They ask the agent to list all active masking tools using `list_masked_numbers` and check who has access with `list_masking_participants`, creating a complete security report.

Patterns to Avoid

Treating it like a simple messaging tool

✗ AVOID

Assuming you only need to send messages and ignoring the necessary steps for number validation or 2FA workflow setup.

✓ INSTEAD

Always check `lookup_number` first before sending bulk SMS. And remember that sensitive communications require setting up workflows using `set_2fa_workflows`, not just calling a single tool.

Trying to manage data outside of context

✗ AVOID

Attempting to modify an existing masked number without defining the scope of its use or purpose.

✓ INSTEAD

Start by creating a defined boundary. Use `create_masking_context` first, then update the boundaries with `update_masking_application`, keeping your data clean and auditable.

Forgetting to track results

✗ AVOID

Running a campaign and just assuming success because no immediate error message popped up.

✓ INSTEAD

After any send operation, prompt the agent to run `track_sms_conversion`. This provides measurable data on whether your messages actually drove action.

The Right Fit

Use this MCP if your core business function revolves around reliable communication and identity verification. Specifically, you need tools that manage global SMS delivery, handle the multi-step process of 2FA authentication (sending a code AND verifying it), or require phone number validation before sending any message. Don't use this if your primary need is simple data storage; for instance, if you just need to list users, other catalog MCPs are better suited. If your problem is purely about internal document management, avoid this tool entirely. However, if the core pain point involves 'Can I trust this number?' or 'How do I prove this user is who they say they are?', then Mitto's tools like `lookup_number` and `send_2fa` make it an absolute necessity.

Managing customer communications used to mean jumping between four different systems.

Think about the old way: You log into your CRM to find a user's number. Then you open a separate telecom dashboard to check if that number is active and what carrier they use. If everything looks good, you copy the number into a different marketing tool just to send a single test SMS. It's a messy cycle of logging in, copying data, waiting for multiple pages to load, and manually confirming every step.

Now, your agent handles it all. You tell your AI client: 'Verify this user's contact info and send them a status update.' The MCP runs `lookup_number` instantly, validates the number type, and then uses `send_sms`. The entire sequence happens in one conversation thread, giving you immediate confirmation that both the data was good *and* the message went out.

Mitto provides complete control over SMS and 2FA through this MCP.

Before this MCP, setting up a secure authentication flow meant developing complex webhooks or relying on brittle email integrations.

Now you just describe the workflow: 'Send an OTP, then confirm it.' The agent orchestrates `send_2fa` followed by `verify_2fa`. It eliminates

You had to write specific code for sending the initial OTP, another block of code to wait for user input, and a final block to check that input against the service's records.

complex conditional logic from your codebase and makes authentication reliable, regardless of whether the user is communicating via SMS or Voice.

Mitto: Messaging & Authentication Tools (27)

These tools let your agent manage everything from simple message delivery to complex security protocols like Two-Factor Authentication and number masking.

#	TOOL	DESCRIPTION
01	`add_masked_number`	Attaches a privacy mask to an existing phone number record.
02	`add_masking_participant`	Adds a new user or entity that needs its communication identity masked.
03	`cancel_2fa`	Stops an ongoing Two-Factor Authentication code request for a specific user.
04	`create_masking_application`	Sets up a dedicated application layer to manage how numbers are masked and used.
05	`create_masking_context`	Creates a specific operational context for grouping related masking data.
06	`delete_masking_application`	Removes an established number masking application entirely.
07	`delete_masking_context`	Clears out a previously defined grouping of masked communication data.
08	`delete_masked_number`	Deletes a phone number that has been masked by the system.
09	`delete_masking_participant`	Removes a specified user from the list of participants involved in masking operations.
10	`get_2fa_usage`	Retrieves historical records detailing how often 2FA codes were requested and used.
11	`get_sms_usage_by_country`	Generates a breakdown of SMS message usage, grouped by the destination country.
12	`list_masking_applications`	Shows all currently active number masking applications set up in your account.
13	`list_masking_contexts`	Lists the available, defined grouping contexts for masked numbers.
14	`list_masked_numbers`	Retrieves a list of all phone numbers currently under a masking protocol.
15	`list_masking_participants`	Displays the names and IDs of every participant involved in number masking.

#	TOOL	DESCRIPTION
16	`lookup_number`	Checks a phone number to validate its format, type (mobile/landline), and carrier information.
17	`search_2fa`	Searches historical records for specific Two-Factor Authentication details.
18	`search_masking_interactions`	Finds records of interactions related to number masking activities.
19	`send_2fa`	Triggers the sending of a One-Time Password code to a user's phone number.
20	`send_bulk_sms`	Sends messages to multiple recipients simultaneously in one batch operation.
21	`send_sms`	Sends a single, specific text message to one recipient.
22	`set_2fa_limits`	Defines the operational rules and limits for how many times 2FA can be requested.
23	`set_2fa_workflows`	Configures multi-channel paths for 2FA delivery, such as routing a code from SMS to Voice.
24	`track_sms_conversion`	Measures the success rate of your SMS messages in achieving a desired outcome or click.
25	`update_masking_application`	Modifies existing number masking parameters without deleting them.
26	`update_masking_context`	Changes the rules or scope of an already established communication context.
27	`verify_2fa`	Confirms a user's identity by submitting and validating a received 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 an SMS to +1234567890 saying 'Your order is ready for pickup!' from 'MyStore'.

I've sent the SMS to +1234567890. The message ID is `msg_987654`. You can track its delivery status using this ID.

U Send a 2FA verification code to +447700900123.

The 2FA code has been sent to +447700900123. Please provide the code once the user receives it, along with the Request ID: `req_abc123`.

U Lookup the phone number +4915123456789 to see the carrier info.

I've looked up the number. It is a mobile number in Germany, currently served by 'Deutsche Telekom'. The number is valid and active.

Frequently Asked Questions

01 **How does Mitto MCP handle bulk messaging?**

You use the `send_bulk_sms` tool. This function allows you to send messages to many recipients at once, streamlining your marketing efforts without manually sending each one.

02 **Can I check if a phone number is valid using Mitto MCP?**

Yes. The `lookup_number` tool validates the phone number's format and provides carrier information to ensure it's ready for communication.

03 What tools are available for Two-Factor Authentication with Mitto MCP?

You can use `send_2fa` to initiate the code, and then use `verify_2fa` once you have the user's response. You can also set rules using `set_2fa_limits`.

04 Is Mitto MCP useful for masking sensitive data?

Yes, it provides full control over masking through tools like `create_masking_context`, allowing you to group and manage numbers under a specific privacy application.

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 `"mitto": { "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

Mitto 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 Mitto. 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	Mitto MCP
Server ID	`019e38c2-b00a-739b-a2b2-40898937d5ae`
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/mitto.