MCP SERVER | NO CODE | CLOUD HOSTED

Mailsac MCP

Automate Email Testing & Data Extraction

Mailsac manages disposable and private email addresses, letting your AI client automate testing workflows without needing real accounts. This MCP lets you reserve new, isolated inboxes, search through messages across multiple domains, and reliably extract sensitive data like verification codes or links from both plain text and HTML bodies.

A+ Quality Score 100/100

disposable-email | email-testing | inbox-management | message-extraction | automated-testing | verification-codes

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

SCAN TO VIEW

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.

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.

Mailsac MCP

9 tools available
Cloud-hosted on Vinkius

Managing test emails used to be a nightmare of clicking tabs and manually copying codes. Now, your agent can handle the whole process directly. You connect this MCP via Vinkius and tell your AI client exactly what you need—whether it's checking if a new sign-up flow sends an email or grabbing a single verification code after a password reset. Your agent reserves a clean, private address for the test run, waits for the message to land, and then pulls out only the data you asked for, whether that's raw plain text or structured HTML content. You can also inspect your entire setup by listing all reserved addresses and checking which custom domains are linked to your account. Need cleanup? Your agent permanently deletes messages from an inbox or even clears out entire inboxes when testing is done. It’s pure automation for email-based operations.

Core Capabilities

01 — Reserve and Manage Addresses

Create new, isolated private addresses, list all reserved addresses, or delete old ones to keep your setup clean.

02 — Retrieve Message Content

Fetch the full plain text body or the sanitized HTML structure of any specific message in an inbox.

03 — Check Inbox Status and Contents

List all messages received by a given address, allowing you to inspect what came through your temporary mailbox.

04 — Search Across All Inboxes

Query messages across every registered address using advanced search parameters like sender or subject line (requires paid tier).

05 — Delete and Maintain Mailboxes

Permanently remove a single message from an inbox, or completely clear out an entire mailbox when testing is finished.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and enter your Mailsac API key.

02 Connect the credentials to your preferred AI client (like Cursor or Claude).

03 Instruct your agent using natural language commands, telling it exactly which action to perform—for example, 'Reserve a new address for testing' or 'Extract the code from the last email.'

The bottom line is that you tell your AI client what task needs doing with temporary emails, and this MCP executes the complex API calls on your behalf.

Built For

This MCP targets technical roles that spend time testing signup flows, password resets, or multi-step user journeys. It's for developers who need reliable data extraction and QA engineers tired of manual inbox checking.

QA Engineer

Automates the retrieval of verification codes from test emails, ensuring that every signup or workflow correctly sends a functional code.

Developer/DevOps Engineer

Inspects incoming integration test emails and manages temporary addresses directly from their IDE without leaving their coding environment.

Security Tester

Tests account isolation by reserving unique private email addresses for each simulated user to ensure no cross-contamination of data occurs.

What Changes When You Connect

01 Stop manually checking inboxes. Use the agent to reserve a clean address with `reserve_new_address` and then automatically wait for, read, and process incoming messages.

02 Extract data reliably. Instead of reading messy HTML, use `get_plain_text_body` to pull out only verification codes or tracking numbers into a simple text string.

03 Keep your environment clean. When testing is done, use `delete_inbox_message` or even clear the entire inbox to prevent test data from accumulating and causing clutter.

04 Track everything you own. You can always verify which addresses are active by running `list_reserved_addresses`, giving you full oversight of your email infrastructure.

05 Search complex histories easily. The `search_account_messages` tool lets you query messages across all domains using parameters like 'from' or 'to', saving hours of manual searching.

Real-World Applications

Testing a New Signup Flow

A QA engineer needs to test the password reset email. They ask their agent to `reserve_new_address` for 'test-user@mailsac.com'. The flow runs, sends the email, and the agent uses `get_plain_text_body` to pull out the unique reset code instantly, feeding it back into a testing script.

Debugging Email Triggers

A developer is debugging an integration that should send a confirmation email. They use their agent to `list_inbox_messages` for the test address, confirming the message arrived and then use `get_html_message_body` to check if all necessary tracking links are present in the source code.

Auditing Domain Usage

A DevOps engineer needs to know which custom domains are active for a new client project. They run `list_custom_domains` through their agent, getting an immediate list of all available and linked sender identities.

Investigating Failed Messages

A user suspects a message got lost in the shuffle. Instead of checking every single inbox, they ask their agent to use `search_account_messages` with date parameters, narrowing down potential messages across their entire account.

Patterns to Avoid

Trying to scrape live email services

✗ AVOID

Using a general web scraping tool on an actual inbox. This is brittle, violates terms of service, and requires complex handling for logins and rate limits.

✓ INSTEAD

Always use this MCP. The agent first uses `reserve_new_address` to create isolated test environments, then reads the data safely using tools like `get_plain_text_body`.

Manually listing addresses

✗ AVOID

Opening a dashboard and clicking through multiple tabs to see all reserved domains. This is tedious and prone to human error.

✓ INSTEAD

Run the `list_reserved_addresses` tool with your agent. It immediately provides a comprehensive list of every active inbox you manage.

Assuming message content format

✗ AVOID

Treating all email data as raw text when it actually contains structured HTML elements like buttons and tables.

✓ INSTEAD

If structure matters, use `get_html_message_body`. If you only need the code or link, use `get_plain_text_body` for a cleaner, more predictable output.

The Right Fit

Use this MCP if your job requires interacting with temporary, disposable, or private email addresses within a programmatic flow. Specifically, if you need to reserve an address, wait for a message, and then extract structured data like codes from that message (use `get_plain_text_body` for simple extraction). You must use it when testing automated workflows involving emails, such as signups or password resets.

Don't use this if you need to send mass marketing campaigns (that requires a dedicated bulk sender service) or if you just need a general email client interface. If your goal is simply to write an email from scratch and hit 'send,' then a standard messaging tool works better. But for testing, data extraction, and inbox maintenance, this MCP is the only thing you need.

Manually tracking test emails slows down development.

Today, when your app sends a new email trigger—say, a welcome message or a failed payment alert—you have to manually open the inbox for that test address. Then you copy the content, paste it into a notepad, and sift through the HTML junk until you find the one piece of data, like an API key or verification code, you actually needed.

With this MCP, your agent handles all that noise. You tell your client to wait for the message; it retrieves the full body using `get_plain_text_body` and gives you nothing but the clean, actionable string. It saves you the copy-paste cycle every single time.

Mailsac MCP Gives You Full Control Over Inbox Data.

The biggest manual step that goes away is the guesswork. You no longer have to wonder if you're looking at plain text or a messy HTML version of the data, because your agent can decide which view—using `get_plain_text_body` or

It’s not just about reading emails; it's about treating them like a predictable resource. You control the entire lifecycle, from reserving the address to deleting the message with `delete_inbox_message`. That level of automation is a game-changer.

`get_html_message_body` —will give you what you need for that specific step.

Mailsac: 9 Tools for Inbox & Domain Control

These tools let your agent list reserved addresses, search messages across all domains, and perform specific content extractions from emails.

#	TOOL	DESCRIPTION
01	`list_reserved_addresses`	Retrieves a list of all the enhanced or custom email addresses you have reserved in your account.
02	`delete_inbox_message`	Permanently removes a specific message from an inbox, ensuring clean test environments.
03	`list_custom_domains`	Shows all the custom domains that have been linked to and are active within your Mailsac account.
04	`get_html_message_body`	Pulls out the complete, sanitized HTML code from a specific message for deep inspection.
05	`get_plain_text_body`	Extracts only the readable plain text content from a message body, perfect for grabbing codes or simple links.
06	`list_inbox_messages`	Fetches a list of all messages currently sitting in a specified inbox.
07	`release_reserved_address`	Deletes and releases an email address that you no longer need, freeing up the reserved slot.
08	`reserve_new_address`	Programmatically secures a new, unique private email address for isolated testing flows.
09	`search_account_messages`	Searches for messages across all your reserved addresses using advanced search parameters like sender or subject (paid tier required).

See It in Action

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

U List all my reserved email addresses in Mailsac.

I've retrieved your reserved addresses. You have 3 active inboxes: 'test-user@mailsac.com', 'service-dev@mailsac.com', and 'alert-prod@mailsac.com'.

U Fetch the plain text content of the last email sent to 'test-user@mailsac.com'.

I've retrieved the text body. The message contains a verification code: '123-456'. Would you like me to extract any other specific information?

U Reserve a new private address 'automation-flow@mailsac.com'.

Successfully reserved 'automation-flow@mailsac.com'. This inbox is now private and enhanced, allowing you to capture messages exclusively.

Frequently Asked Questions

01 **How does the Mailsac MCP work for testing?**

The agent first uses `reserve_new_address` to create an isolated, clean inbox. When your application sends a test email, the agent detects it in that specific address and retrieves the content using tools like `get_plain_text_body`.

02 **Can I search my entire Mailsac account history?**

Yes, you can use `search_account_messages` to query messages across all your addresses. This requires a paid tier but is essential for auditing old test data.

03 **Is the content I get from Mailsac safe to use in my code?**

Yes, since this MCP runs through controlled API calls on Vinkius, the extracted data is passed directly as a clean string or object to your agent, making it ready for your application logic.

04 **How do I delete an email message using Mailsac?**

You use the `delete_inbox_message` tool. You just need to specify which inbox and which message ID you want permanently removed, keeping your test data clean.

05 **Can I check what domains are available for my account?**

Absolutely. The `list_custom_domains` tool lets you see all the custom email domains that have been linked to your Mailsac account, helping you plan new test setups.

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 `"mailsac": { "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

Mailsac 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 Mailsac. 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	Mailsac MCP
Server ID	`019d75cd-1878-7253-bd65-c14fcb48f235`
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/mailsac.