MCP SERVER | NO CODE | CLOUD HOSTED

Postmark MCP

Automate transactional email delivery and template management.

Postmark MCP handles high-deliverability email workflows directly through your agent. Send single emails, manage complex templates, and track open/click metrics without leaving your IDE. It's built for reliable transactional communication and programmatic template control.

F Quality Score 48.02/100

transactional-email | email-api | template-management | postmark | email-delivery

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.

Postmark MCP

72 tools available
Cloud-hosted on Vinkius

Think about sending critical automated messages—password resets, welcome packets, or account alerts. Getting those emails out reliably isn't just about hitting 'send'; it’s about making sure they land in the inbox and that your templates actually work every time.

This MCP connects your agent to Postmark's infrastructure. Instead of jumping into a separate dashboard, you manage your entire email lifecycle from one place. You can send massive batches of emails or just single messages using full control over content, attachments, and metadata. You also get deep visibility into performance metrics, letting you check open counts or spam complaint totals. Plus, you can manage the underlying templates—creating them, editing variables, or even validating their syntax before a campaign goes live. This makes it powerful for anyone managing communication at scale; just connect this MCP through Vinkius and your agent handles the rest.

Core Capabilities

01 — Send various emails

Dispatch single, batch, or bulk emails with full control over content and metadata.

02 — Manage templates

Programmatically list, create, edit, validate, and delete email templates.

03 — Audit domain health

Verify and rotate DNS keys like DKIM and Return Paths to maintain high sender reputation.

04 — Track performance metrics

Retrieve detailed stats on opens, clicks, bounces, and spam complaints for outbound messages.

05 — Handle message streams

Create, read, edit, or archive dedicated message streams for organization.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/postmark-extended-1** — connect your AI agent in three steps.

01 Subscribe to this MCP and provide your Postmark Server Token (and optionally your Account Token).

02 Connect the credentials to your preferred AI client—Claude, Cursor, or any MCP-compatible client.

03 Your agent uses natural language prompts to execute email actions, like sending a message using `send_email` or listing available templates with `list_templates`.

The bottom line is that your agent handles the API calls and data formatting automatically, so you just tell it what communication job needs doing.

Built For

This MCP is for technical teams and operations professionals who manage communications at scale. If you're tired of jumping between a CMS, a dashboard, and your code editor to send an email or check stats, this is what you need.

Software Developer

Integrating transactional emails (like password resets) directly into application logic without needing dedicated API calls in the codebase.

Marketing Operations Specialist

Using natural language to validate template syntax or update campaign assets, saving time previously spent navigating complex web interfaces.

Support Engineer

Automating personalized follow-up messages based on user interaction data by running AI-driven workflows.

What Changes When You Connect

01 Never switch tabs to manage communication. You can send a single email using `send_email`, validate templates with `validate_template`, and check analytics, all through your agent's chat interface.

02 Maintain perfect domain health effortlessly. If you need to rotate keys or verify records, use tools like `rotate_domain_dkim` or `verify_domain_return_path` right from your development flow.

03 Scale your reporting without writing custom queries. Get comprehensive metrics—like total open counts via `get_outbound_opens_stats` or spam complaint numbers using `get_outbound_spam_stats` —instantly in conversation.

04 Build complex, automated campaigns. You can use templates and variables to send personalized messages by calling `send_email_with_template`, ensuring consistency across thousands of users.

05 Handle compliance tasks with simple prompts. When data removal is necessary, you can execute `request_data_removal` directly via your agent, tracking the status until complete.

Real-World Applications

Handling a User Onboarding Flow

A developer needs to send a welcome email and then follow up with an invoice link three days later. They use `send_email_with_template` for the welcome, schedule the reminder through their agent, and if the recipient fails to click a link, they ask the agent to check `get_outbound_clicks_stats` before sending a human-written nudge.

Fixing Sending Reputation

A marketing team notices bounce rates spiked. Instead of checking three separate dashboards, they prompt their agent to run `search_bounces`, followed by `get_bounce` for the worst offenders, and then use `rotate_domain_dkim` to immediately improve sending reputation.

Updating a Core System Template

A support manager needs to change the disclaimer text in all password reset emails. They first run `list_templates`, find the alias, and use `edit_template` to update it, then they call `validate_template` to confirm the syntax is still good.

Bulk Communications Audit

A compliance officer needs to verify that all old user data can be removed. They trigger `request_data_removal`, and later use `get_data_removal_status` to confirm the process finished successfully, documenting the audit trail.

Patterns to Avoid

Over-relying on dashboards

✗ AVOID

Having to open the Postmark dashboard, navigate to 'Analytics,' and manually cross-reference bounce numbers with template versions.

✓ INSTEAD

Just ask your agent: 'What were the total open counts for last week?' or 'Show me all messages that bounced yesterday' using `get_outbound_opens_stats` or `search_bounces`. It brings the data to you.

Manual credential management

✗ AVOID

Writing boilerplate API calls in Python just to send a simple test email because the credentials aren't easily available.

✓ INSTEAD

Connect your agent and run `send_email` or `send_batch_emails`. Your agent handles the token passing, so you only write the prompt.

Ignoring domain health

✗ AVOID

Sending a major campaign without verifying DKIM records first, risking immediate blacklisting.

✓ INSTEAD

Always start with `get_domain` to check current status, and if necessary, run `verify_domain_dkim` before any large send.

The Right Fit

Use this MCP if your primary need is programmatic control over email delivery mechanics—things like managing templates, rotating DNS records (DKIM), or querying granular event data. If you just want to *view* a report that already exists in one place and don't need to act on the underlying structure, then a simple read-only stats tool might suffice. However, if you need your agent to perform an action —like sending 50 emails with variables, validating template syntax

via `validate_template`, or searching for specific message IDs using `search_outbound_messages`—this is the right choice. Don't use this if you simply want a general mailing list provider; this is specifically for transactional reliability and deep technical auditing.

The Headache of Email Deliverability

Today, managing email communication feels like juggling. You might start by building the message copy in a CMS, then jump to another dashboard to check your domain's DKIM status. If you need to make it personalized, you have to switch again to edit variables within a template previewer. Then, when the campaign is live and someone asks 'Why did this fail?', you end up digging through cryptic logs trying to figure out if it was a bounce or just bad formatting.

With this MCP, that friction vanishes. You tell your agent exactly what needs to happen—'Send the welcome email using template X and include John Doe's name.' The agent handles the entire chain of events: validating the template structure first with `validate_template`, then sending the message via `send_email_with_template`. You just get the confirmation.

Sending Emails with Postmark MCP

The manual steps that disappear are the repeated checks: validating syntax, updating sender signatures manually via `edit_sender_signature`, and running separate reports to check open counts. These tasks used to require dedicated UI time or multiple API calls just to get a simple status update.

Now, your agent handles the complexity. You can send bulk emails using `send_bulk_emails` and immediately ask for the results—'What were the total opens?' The process is integrated; you write code or natural language prompts, and the delivery stats come back instantly.

Postmark Extended: 72 Tools for Email Management

Use these tools to control every aspect of email communication, from sending single messages to managing domain records and fetching deep performance statistics.

#	TOOL	DESCRIPTION
01	activate_bounce	Reactivates an email address that previously bounced.
02	add_domain	Adds a new domain to the account level for sending emails.
03	archive_message_stream	Archives an existing message stream.
04	bypass_inbound_message	Allows messages to pass rules if they were previously blocked upon arrival.
05	create_message_stream	Sets up a new message stream for organizing communications.
06	create_sender_signature	Creates a sender signature at the account level.
07	create_server	Sets up a new sending server for the account.
08	create_suppressions	Creates suppressions for a message stream, limiting recipients to 50.
09	create_template	Generates an entirely new email template.
10	create_webhook	Sets up a webhook endpoint for notifications.
11	delete_domain	Removes a domain from the account level.
12	delete_sender_signature	Removes an existing sender signature at the account level.
13	delete_server	Deletes a sending server configuration from the account level.
14	delete_suppressions	Removes suppressions (and reactivates recipients) for a message stream.
15	delete_template	Deletes an existing email template.
16	delete_webhook	Removes a configured webhook.
17	edit_current_server	Changes the configuration settings for the active sending server.

#	TOOL	DESCRIPTION
18	edit_domain	Updates an existing domain setting at the account level.
19	edit_message_stream	Modifies settings for a message stream.
20	edit_sender_signature	Updates an existing sender signature at the account level.
21	edit_server	Edits core server settings across the entire account.
22	edit_template	Makes changes to the content or variables of a specific template.
23	edit_webhook	Modifies an existing webhook configuration.
24	get_bounce_dump	Retrieves the raw SMTP data for a failed email bounce.
25	get_bounce	Fetches detailed information about a specific bounced email address.
26	get_bulk_request_status	Checks the status of large-scale, bulk email requests.
27	get_current_server	Retrieves the current configuration details for the sending server.
28	get_data_removal_status	Checks the status of a data removal request (GDPR/CCPA compliance).
29	get_delivery_stats	Retrieves overall statistics on email delivery and bounces.
30	get_domain	Fetches detailed information about a specific sending domain.
31	get_inbound_message_details	Gets full details for an email that was sent to your domain.
32	get_message_stream	Retrieves specific details about a message stream.
33	get_outbound_bounces_stats	Gathers bounce count statistics for all outgoing emails.
34	get_outbound_clicks_stats	Gets click-through rate counts and stats for outbound messages.
35	get_outbound_message_details	Retrieves full event history and details for a single sent email.
36	get_outbound_message_dump	Gets the raw source code of an outbound message.
37	get_outbound_opens_clients_stats	Calculates open usage metrics, broken down by email client used by recipients.

#	TOOL	DESCRIPTION
38	get_outbound_opens_platforms_stats	Calculates open usage metrics, grouped by the recipient's platform (e.g., iOS, Android).
39	get_outbound_opens_stats	Gets total counts for when outbound messages were opened.
40	get_outbound_sends_stats	Retrieves the total count of emails successfully sent out.
41	get_outbound_spam_stats	Gets the number of spam complaints received for outbound messages.
42	get_outbound_stats	Provides a general statistical overview of all sent messages.
43	get_outbound_tracked_stats	Retrieves counts for emails that were tracked after being sent out.
44	get_sender_signature	Fetches details about the current sender signature setup.
45	get_server	Retrieves configuration settings for the overall sending server.
46	get_template	Gets specific details and content of a single template by name or alias.
47	get_webhook	Retrieves the configuration settings for an existing webhook.
48	list_domains	Lists all domains configured for sending emails at the account level.
49	list_message_streams	Retrieves a list of existing message streams.
50	list_sender_signatures	Lists all sender signatures available at the account level.
51	list_servers	Retrieves a list of all configured sending servers for the account.
52	list_suppressions	Lists current suppressions set for a specific message stream.
53	list_templates	Retrieves a list of all templates available on the server.
54	list_webhooks	Lists webhooks associated with a specific message stream.
55	push_templates	Transfers template definitions from one sending server to another.

#	TOOL	DESCRIPTION
56	request_data_removal	Initiates a formal request to remove recipient data for compliance (GDPR/CCPA).
57	resend_sender_signature	Resend confirmation email for a sender signature
58	retry_inbound_message	Tries again to process an inbound message that failed processing the first time.
59	rotate_domain_dkim	Triggers the rotation of DKIM keys for a specific sending domain.
60	search_bounces	Searches historical records for bounced emails.
61	search_inbound_messages	Queries received messages sent to your domain.
62	search_outbound_clicks	Searches historical records for specific click events on outbound emails.
63	search_outbound_messages	Queries all sent outbound messages by various criteria.
64	search_outbound_opens	Searches historical records for when specific outbound emails were opened.
65	send_batch_emails	Sends multiple, predefined emails in a single batch operation.
66	send_bulk_emails	Initiates the sending of a large volume of emails to many recipients.
67	send_email	Sends one single email message immediately.
68	send_email_with_template	Sends an email using a specific, pre-defined template and variables.
69	unarchive_message_stream	Restores a message stream that was previously archived.
70	validate_template	Checks an email template's syntax to ensure it is valid before sending.
71	verify_domain_dkim	Triggers a verification check for the domain's DKIM records.
72	verify_domain_return_path	Triggers a verification check for the domain's Return-Path record.

See It in Action

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

U Send an email from 'sales@company.com' to 'client@example.com' with the subject 'Meeting Follow-up' and a simple thank you message.

I've sent the email using `send_email`. The Message ID is 'abc-123' and the status is 'Submitted'.

U List all the email templates available on my Postmark server.

I found 3 templates: 'Welcome Email' (Alias: welcome), 'Password Reset' (Alias: reset), and 'Invoice' (Alias: invoice).

U Send a welcome email to 'newuser@gmail.com' using the template alias 'welcome-pack' and set the 'name' variable to 'John'.

Processing `send_email_with_template`... The email has been successfully queued for delivery to John.

Frequently Asked Questions

01 **How do I send a one-off email using Postmark MCP?**

You use the `send_email` tool. You just provide the recipient, subject, and body content, and your agent handles getting it out immediately.

02 **Can I check if my domain is ready for bulk sending with Postmark MCP?**

Yes, you can use `get_domain` to review current settings. If needed, run `rotate_domain_dkim` or `verify_domain_return_path` first to ensure your records are fresh.

03 **What if I need to change a template variable in Postmark MCP?**

You use the `edit_template` tool. This lets you modify the content or variables of an existing template without affecting other parts of your system.

04 **How do I get detailed failure reports from Postmark MCP?**

Use `search_bounces` to look up bounce records, and then use `get_bounce` to fetch specific details about a single bounced address.

05 **Is it possible to track clicks using the Postmark MCP?**

Yes. You can search for click events using `search_outbound_clicks`, or get aggregate data with `get_outbound_clicks_stats`.

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 `"postmark-extended-1": { "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

Postmark 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 Postmark. 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	Postmark MCP
Server ID	`019e5d4a-b8fa-7379-a0c4-003ad9729784`
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/postmark-extended-1.