MCP SERVER | NO CODE | CLOUD HOSTED

Digital Legacy Message Library MCP

Securely schedule and manage messages for future delivery.

Digital Legacy Message Library lets you build a structured system for sensitive, timed, or event-based communications. You can register messages for specific recipients, set delivery triggers, and choose how they are sent. Your AI client handles the heavy lifting of managing metadata and checking if conditions are met for release.

A+ Quality Score 100/100

legacy | messaging | scheduling | privacy | automation

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/digital-legacy-message-library

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.

Digital Legacy Message Library MCP

4 tools available
Cloud-hosted on Vinkius

You can use this MCP to organize messages that shouldn't be sent until a specific time or event occurs. It works as a central repository for sensitive content that needs to stay dormant until the right moment. Instead of manually tracking dates or triggers, you let your AI client manage the registry and monitor the status of every entry.

You can register new content with `create_message_entry` to ensure all delivery metadata is captured correctly. If you need to see what is currently waiting in the queue, `list_pending_messages` shows you everything that hasn't hit its trigger yet. You can also use `validate_delivery_conditions` to check if a specific message is actually ready to go based on its rules. For authorized senders needing a full breakdown, `get_message_delivery_manifest` produces a complete report for a single entry.

Core Capabilities

01 — Message Registration

Your agent can log new messages with specific metadata and recipient info.

02 — Trigger Monitoring

The AI checks if specific conditions or timeframes have been met for a message.

03 — Queue Management

You can view all messages currently waiting for their delivery triggers.

04 — Report Generation

Authorized users can pull full delivery manifests for individual messages.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/digital-legacy-message-library** — connect your AI agent in three steps.

01 Connect your AI client to the Vinkius hosted MCP.

02 Register a message using the create tool with its metadata.

03 Monitor the status of scheduled items using the list tool.

04 Verify readiness with the validation tool.

05 Generate a manifest once the message is ready for release.

Setting up your timed messaging system is a direct process through your AI client.

Built For

This MCP is built for individuals and professionals managing sensitive communications that require delayed or event-based delivery.

Estate Planners

They use the agent to organize messages intended for beneficiaries.

Digital Asset Managers

They manage the release of information based on specific lifecycle events.

Privacy Advocates

They use the tool to schedule data releases that must remain dormant for a set period.

What Changes When You Connect

01 Automates the monitoring of delivery triggers.

02 Centralizes sensitive message metadata in one place.

03	Provides clear reports for authorized message release.
04	Reduces manual tracking of scheduled communications.

Real-World Applications

Posthumous Communication

Schedule messages to be sent to family members at a later date.

Timed Information Release

Hold sensitive data until a specific time or condition is met.

Event-Based Messaging

Trigger a message to a recipient when a specific event occurs.

Audit and Reporting

Generate manifests to verify message contents and instructions for authorized senders.

Patterns to Avoid

Manual Trigger Tracking

AVOID

You keep a separate spreadsheet to track which messages are ready to be sent to beneficiaries.

✓ INSTEAD

Let your agent monitor the queue for you. Use `list_pending_messages` to see exactly what is waiting for its trigger.

Blind Release Attempts

AVOID

You try to send a message without checking if the specific conditions for its release have actually been met.

✓ INSTEAD

Always run a check first. Use `validate_delivery_conditions` to confirm a message meets its rules before you act.

Incomplete Metadata Entry

AVOID

You skip adding delivery details because you want to save time during the setup process.

✓ INSTEAD

Ensure all delivery metadata is captured during the initial setup by using `create_message_entry`.

The Right Fit

Connect this MCP if you manage sensitive information that requires strict, time-based, or event-based release. Do not connect it if you need real-time, instant communication tools. The decision depends on whether your data needs to stay dormant until a specific trigger occurs.

Digital Legacy Message Library 4 Tools

These tools handle the full lifecycle of dormant messages, from initial registration to trigger validation and final reporting.

#	TOOL	DESCRIPTION
01	`get_message_delivery_manifest`	This tool generates a detailed, labeled report for a single message for authorized senders.
02	`list_pending_messages`	This tool pulls a list of all messages currently marked as scheduled that haven't met their triggers.
03	`validate_delivery_conditions`	Use this to check if a specific message meets its triggers and expiration rules for release.
04	`create_message_entry`	This tool registers a new message into the library along with its required delivery metadata.

See It in Action

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

U Register a message for recipient 'user_123' with the content 'Hello from the past' to be sent via email when a timed trigger occurs.

Message successfully registered with ID: msg_98765. Status: Scheduled.

U Is the message with ID 'msg_12345' ready to be delivered?

The message is eligible for release. The trigger condition has been met.

U Generate a delivery manifest for message 'msg_555' for authorized sender 'admin_01'.

Manifest generated: Recipient: John Doe; Content: 'Remember me'; Instructions: Send via SMS; Expiration: Valid.

Frequently Asked Questions

01 **How do I add a new message to the library?**

You use the create_message_entry tool to register the content and all necessary delivery metadata.

02 **Can I see which messages are waiting to be sent?**

Yes, the list_pending_messages tool shows all messages that are currently scheduled but haven't met their triggers.

03 **How does the AI know when to release a message?**

The AI uses the validate_delivery_conditions tool to check if the specific triggers and expiration rules for a message have been satisfied.

04 **What information is in a delivery manifest?**

A manifest includes the recipient, the message content, delivery instructions, and expiration status.

05 **Which AI clients can use this MCP?**

You can use this with any MCP-compatible client like Claude, Cursor, or Windsurf.

06 **Can I check if a message is ready to be sent?**

Yes, use the `validate_delivery_conditions` tool to verify if a message's triggers have been met and if it is still within its validity period.

07 **How can I see all messages waiting to be delivered?**

The `list_pending_messages` tool allows you to retrieve all messages that are currently scheduled but have not yet met their delivery triggers.

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 `"digital-legacy-message-library": { "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

Digital Legacy Message Library 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 Digital Legacy Message Library. 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	September 2026
MCP Server	Digital Legacy Message Library MCP
Server ID	`01a0dabf-2833-72da-9a0a-ea316dab6cd4`
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/en/ai-agent-connect/digital-legacy-message-library.