

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Family Records Transfer List MCP

Maintain a verifiable chain of custody for sensitive archives.

Family Records Transfer List MCP handles the secure movement of sensitive family archives between custodians. It provides your AI client with the tools to build inventories, generate verification checklists, and confirm that every file arrives exactly as it was sent. You can track the history of every custodian to ensure nothing is lost during handoffs.

A+ Quality Score 100/100

chain-of-custody

records-management

family-archives

data-integrity

custodian-tracking



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

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.

Family Records Transfer List MCP

4 tools available

Cloud-hosted on Vinkius

Moving sensitive family archives between family members or legal custodians shouldn't rely on guesswork. This MCP gives your AI client the ability to manage a strict chain of custody for digital or physical records. Instead of just moving files, you're creating a documented trail that proves exactly what was sent and who received it.

You can use your agent to build master inventories of files intended for transfer, ensuring nothing is overlooked. To prevent errors during the handoff, you can generate step-by-step checklists that guide the recipient through the verification process. If you need to confirm that a transfer was successful, your AI can compare the original inventory against the received files to check for any missing or altered data. It also keeps a chronological log of all past transfers, so you always know the history of how specific custodians have handled your family's records.

Core Capabilities

01 — Inventory Creation

Your agent builds a master list of all files designated for a specific transfer.

02 — Verification Checklists

The AI generates step-by-step instructions to guide custodians through the verification process.

03 — Integrity Auditing

Your client compares received files against the original list to detect any changes or losses.

04 — Custodian Tracking

The AI maintains a chronological log of all transfers involving specific individuals.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/family-records-transfer-list — connect your AI agent in three steps.

- 01
- Connect the MCP to Claude, Cursor, or Windsurf via Vinkius.
- 02
- Ask your agent to generate a transfer list for your files.
- 03
- Have the AI create a verification checklist for the recipient.
- 04
- Use the integrity tool to confirm the files arrived safely.

You connect the MCP to your preferred AI client and start managing transfers through natural language.

Built For

This MCP is built for individuals and professionals managing sensitive historical or legal family documentation.

Estate Executors

They use the AI to document the movement of assets and records between beneficiaries.

Family Historians

They rely on the tool to maintain the integrity of digital archives during handoffs.

Legal Custodians

They use the checklists and logs to prove a verifiable chain of custody.

What Changes When You Connect

- 01
- Creates a verifiable paper trail for every file movement.
- 02
- Prevents data loss by comparing intended lists against actual receipts.
- 03
- Standardizes the handoff process with structured checklists.

04 Maintains a clear history of custodian activity.

Real-World Applications

Estate Record Handoff

An executor moves digital estate documents from a deceased relative's account to a beneficiary.

Digital Archive Migration

A family historian moves a collection of scanned photos from one storage medium to another.

Legal Document Transfer

A custodian moves sensitive legal files between different family members or lawyers.

Custodian Auditing

A user reviews the history of a specific custodian to ensure all previous transfers were handled correctly.

Patterns to Avoid

Blind file transfers

❌ AVOID

You send a folder of scanned estate documents to a beneficiary via email and assume everything arrived intact.

✓ INSTEAD

Use ``generate_transfer_list`` first to create a master inventory, then use ``verify_transfer_integrity`` to confirm the recipient actually got what you sent.

Unstructured handoffs

❌ AVOID

A legal custodian tells a family member to 'check the files' without providing any specific guidance on what to look for.

✓ INSTEAD

Run ``create_coc_checklist`` to give the recipient a clear, step-by-step guide for the verification process.

Ignoring custodian history

❌ AVOID

You notice a discrepancy in a file but don't check if the person handling it has a history of missing data.

✓ INSTEAD

Use ``get_custodian_history`` to review the past activity of specific individuals and identify patterns in how they handle transfers.

The Right Fit

Connect this MCP if you are an executor, historian, or legal custodian managing high-stakes digital archives. Do not connect it if you are just moving casual personal photos. The decision rests on whether you need a verifiable chain of custody for your records.

Family Records Transfer List MCP Tools

These tools handle the heavy lifting of inventorying, verifying, and auditing the movement of sensitive family archives.

#	TOOL	DESCRIPTION
01	create_coc_checklist	This tool produces a structured, step-by-step checklist for the recipient. It ensures the chain of custody is followed correctly during the handoff.
02	generate_transfer_list	This tool builds a complete inventory of every file you intend to move. It serves as the master list for your transfer batch.
03	get_custodian_history	This tool retrieves a chronological log of all previous transfers. You can use it to audit the activity of specific custodians over time.
04	verify_transfer_integrity	This tool compares the original inventory against what was actually received. It confirms that no files were lost or changed during the move.

See It in Action

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

U Create a transfer list for 3 files from John Doe to Jane Smith on 2024-12-01 with Private access.



The transfer batch has been created with ID TR-9928. It includes 3 files assigned to the designated owners, scheduled for December 1st, 2024.

U Generate a checklist for transfer TR-9928 using a Digital Hash verification method.



The checklist CL-4412 has been generated. It includes steps to verify file counts and perform digital hash matching for the 3 files in batch TR-9928.

U Verify if the transfer TR-9928 was successful. 3 files were received and the checksum matches.



The transfer is valid. The received file count matches the original batch and the integrity score is 100%.

Frequently Asked Questions

01 How does this MCP ensure files aren't lost?

The `verify_transfer_integrity` tool compares the original inventory list against the files actually received to ensure the counts and data match.

02 Can I track who has handled my files in the past?

Yes, the `get_custodian_history` tool provides a chronological log of all past transfers involving specific custodians.

03 What AI clients can I use with this MCP?

You can use this MCP with any compatible client, including Claude, Cursor, Windsurf, and VS Code.

04 Do I need to host this myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start using the tools.

05 What is a chain of custody in this context?

It is a documented, verifiable trail that proves how sensitive files were moved from one person to another without being altered.

06 How do I ensure the records were not tampered with?

You can use the ``verify_transfer_integrity`` tool to compare the intended transfer list against the actual receipt, checking both file counts and digital checksum matches.

07 Can I track the history of a specific custodian?

Yes, the ``get_custodian_history`` tool provides a chronological log of all past transfers involving a specific custodian to audit their reliability.

08 What is a Chain of Custody (CoC) checklist?

A CoC checklist is a structured set of verification steps generated by ``create_coc_checklist`` to track the movement of files and confirm they were handled correctly.

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 <code>"family-records-transfer-list": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Family Records Transfer List 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 Family Records Transfer List. 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	Family Records Transfer List MCP
Server ID	01a0de0a-c038-72df-a579-1825b8e60e8d
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/family-records-transfer-list.