

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 Photo Sharing Logic Engine MCP

Automate photo privacy and access permissions for your family.

Family Photo Sharing Logic Engine MCP handles the complex math of photo privacy. It lets your AI client evaluate consent flags, group memberships, and time-based rules to decide exactly who can see specific albums. Instead of manually checking permissions, you let your agent handle the logic of who is allowed in and when access expires.

A+ Quality Score 100/100

photo-sharing

permissions

privacy-logic

audience-management

temporal-rules



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 Photo Sharing Logic Engine MCP

4 tools available

Cloud-hosted on Vinkius

You shouldn't have to manually cross-reference permission lists every time you share a photo album. This MCP acts as a dedicated logic engine that your AI client uses to enforce privacy rules. It looks at consent settings, audience groups, and even how much time has passed since an album was created to determine access. If you need to know if a specific relative is in the right group, the agent can check that instantly. If you want to see when a shared link will stop working, the engine provides a clear schedule. It handles the heavy lifting of temporal constraints, ensuring that albums aren't shared outside of their intended windows. You get a reliable way to manage digital boundaries without the manual guesswork.

Core Capabilities

01 — Permission Auditing

Your agent uses this to identify which users are currently blocked or allowed for a specific album.

02 — Group Membership Verification

The AI checks if a user is part of a permitted audience group before suggesting a share.

03 — Expiration Tracking

Your agent calculates when access rights will lapse using the expiration calendar.

04 — Time-based Validation

The engine checks if an album's creation date allows for sharing under current temporal rules.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/family-photo-sharing-logic-engine — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 The agent receives a request to check or share an album.
- 03 The MCP runs the specific logic tool like permission analysis or temporal checks.
- 04 The agent receives the result and tells you who can or cannot see the photos.

The MCP connects your AI client to your photo permission database to run logic checks.

Built For

This MCP is built for anyone managing large-scale digital photo libraries where privacy and time-limited access are critical.

Digital Asset Managers

They hand off permission auditing and expiration scheduling to the agent.

Privacy Officers

They use the engine to verify that audience access aligns with consent flags.

Family Tech Coordinators

They use the tool to manage shared family albums and expiration dates.

What Changes When You Connect

- 01 Removes manual permission checks by automating consent evaluation.
- 02 Prevents accidental over-sharing through strict temporal constraint checks.

-
- | | |
|-----------|---|
| 03 | Provides a clear schedule of access expirations to prevent stale permissions. |
| <hr/> | |
| 04 | Centralizes privacy logic so your AI client can make consistent decisions. |
| <hr/> | |
-

Real-World Applications

Automated Privacy Audits

Your agent scans an album to see if any unauthorized users have access based on current group settings.

Managing Temporary Access

You use the expiration calendar to plan when to revoke access for seasonal event photos.

Enforcing Consent Rules

The engine blocks sharing requests if a user's consent flag is set to private.

Validating Sharing Windows

The AI checks if an old album is still eligible for sharing based on its original creation date.

Patterns to Avoid

Manual Permission Guessing

❌ AVOID

You try to remember if Aunt Mary is in the 'Extended Family' group before sending a link to a new album.

✓ INSTEAD

Let your agent handle the verification. Use ``validate_audience_access`` to confirm if a user belongs to a permitted group before you share anything.

Ignoring Expiration Dates

❌ AVOID

You share a folder of holiday photos and forget that the access window is supposed to close after the New Year.

✓ INSTEAD

Stay ahead of stale permissions. Use ``get_share_expiration_calendar`` to see exactly when access rights will lapse for different recipients.

Overlooking Temporal Rules

❌ AVOID

You attempt to share an old archive that has been locked due to its original creation date.

✓ INSTEAD

Check the validity of the album first. Use ``check_temporal_constraints`` to see if the current date allows for sharing under existing rules.

The Right Fit

Connect this MCP if you manage large digital photo libraries where privacy and time-limited access are non-negotiable. Do not connect it if you only manage small, single-user folders. The decision rests on whether you need to automate the enforcement of complex consent and expiration rules.

Family Photo Sharing Logic Engine: 4 Essential Tools

These tools handle the heavy lifting of privacy audits, group verification, and temporal access scheduling.

#	TOOL	DESCRIPTION
01	validate_audience_access	This tool checks if a specific user belongs to an audience group that has permission to view an album.
02	analyze_sharing_permissions	This tool evaluates all privacy rules and preference flags to identify exactly which recipients can view an album.
03	check_temporal_constraints	This tool verifies if an album is still within its valid date range for sharing based on the current date.
04	get_share_expiration_calendar	This tool generates a schedule showing when access to specific albums will expire for various recipients.

See It in Action

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

U Who is allowed to see album 'vacation_2023' among users 'user_1', 'user_2', and 'user_3'?



The allowed recipients for album 'vacation_2023' are 'user_1' and 'user_3'. 'user_2' is blocked due to privacy settings.

U Is the album created on '2023-01-01' still valid for sharing today, '2024-05-20'?



Yes, the album is within its valid sharing window.

U When will access to album 'family_reunion' expire for recipient 'user_99'?



Access for 'user_99' to the 'family_reunion' album is set to expire on 2024-12-31.

Frequently Asked Questions

01 How does this MCP handle photo privacy?

It uses a logic engine to evaluate consent flags and audience group memberships to determine access.

02 Can I see when a photo share will expire?

Yes, you can use the expiration calendar tool to get a schedule of when access will cease.

03 What clients can use this MCP?

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

04 Does it check if an album is too old to share?

Yes, the temporal constraints tool verifies if an album is within its valid sharing window.

05 How are audience permissions verified?

The `validate_audience_access` tool checks if a user is a member of a permitted group.

06 How does the system handle blocked users?

The `analyze_sharing_permissions` tool identifies blocked recipients by checking the user's explicit block list and individual consent flags.

07 Can I see when a user's access will expire?

Yes, you can use `get_share_expiration_calendar` to retrieve a schedule of all upcoming expiration dates for an album.

08 How are audience groups verified?

The `validate_audience_access` tool verifies if a specific user is a member of a permitted audience group.

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-photo-sharing-logic-engine": { "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 Photo Sharing Logic Engine 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 Photo Sharing Logic Engine. 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	October 2026
MCP Server	Family Photo Sharing Logic Engine MCP
Server ID	01a0ef42-1365-71d9-a590-062db7ef05ef
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-photo-sharing-logic-engine.