MCP SERVER | NO CODE | CLOUD HOSTED

Family Account Permission Matrix MCP

Control who accesses which family services and when.

Family Account Permission Matrix MCP provides a structured way to govern service access for your household. You can map family members to specific services, define what they can or cannot do, and use secure identifiers to verify permissions. It handles the heavy lifting of permission mapping, security audits, and identifying authorized approvers for any service you manage.

A+ Quality Score 100/100

access-control | family-management | permission-matrix | security-audit | identity-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/family-account-permission-matrix

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.

Family Account Permission Matrix MCP

4 tools available
Cloud-hosted on Vinkius

Managing shared household accounts often becomes a mess of shared passwords and unclear boundaries. This MCP gives you a formal way to govern those permissions. You can build a clear map of which family members have access to specific services like streaming, utilities, or banking. Instead of guessing who can pay a bill or change a setting, you use this MCP to generate a permission matrix that defines permitted and prohibited actions for every person in the house.

Security stays tight because you can generate unique access references to validate permissions on the fly. If you need to check if a specific person is allowed to perform an action, your AI client can verify it instantly. You also get built in oversight. You can schedule regular permission reviews to ensure your access lists stay current and use the workflow tools to find out exactly who has the authority to approve changes for a specific service. It turns messy family account sharing into a structured, auditable system.

Core Capabilities

01 — Access Mapping

Your agent creates a formal document linking people to specific service permissions.

02 — Permission Validation

Your AI client checks if a specific access reference is valid for a requested action.

03 — Security Auditing

Your agent tracks and schedules periodic reviews of all service permissions.

04 — Approver Identification

Your agent finds the correct person to contact for permission changes.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/family-account-permission-matrix** — connect your AI agent in three steps.

01 Connect the MCP to your preferred client like Claude or Cursor via Vinkius.

02 Generate your initial permission matrix by defining users and their service rights.

03 Use access references to verify permissions whenever a question arises.

04 Set up recurring audits to keep your permission data accurate and secure.

Connecting this MCP to your AI client gives you immediate control over your household permission structure.

Built For

This MCP is built for heads of households and family managers who need to organize shared digital lives.

Household Managers

They use the MCP to delegate service access to children or extended family members.

Digital Organizers

They use the tool to maintain a clean, auditable record of shared account permissions.

Security Conscious Users

They use the audit tools to ensure no one has unnecessary access to sensitive services.

What Changes When You Connect

01 Eliminates guesswork by providing a clear map of who can do what.

02 Reduces security risks through scheduled permission audits.

03	Provides instant verification of user rights using access references.
04	Identifies the correct decision makers for service changes.

Real-World Applications

Managing Teenager Access

Set up a matrix where a teenager can use streaming services but cannot access utility billing accounts.

Shared Utility Management

Verify if a spouse or roommate has the permission to pay a specific monthly bill.

Security Maintenance

Schedule a monthly review to ensure old permissions for former household members are removed.

Permission Change Requests

Quickly find out which family member needs to approve a new service permission request.

Patterns to Avoid

Manual Permission Tracking

AVOID

You keep a messy spreadsheet of who has the Netflix password and try to remember if your teenager can access the utility portal.

✓ INSTEAD

Use `generate_permission_matrix` to build a formal document that clearly maps every person to their specific allowed actions.

Guessing Access Rights

AVOID

You wonder if a roommate has the authority to change a service setting and just hope they don't break anything.

✓ INSTEAD

Run `get_access_verification` to instantly check if a specific access reference allows that person to perform the action.

Ignoring Security Rot

AVOID

You forget to remove access for an old tenant or a former family member, leaving your accounts vulnerable.

✓ INSTEAD

Stay on top of your security by using `schedule_permission_review` to set and track regular audit dates.

The Right Fit

Connect this MCP if you manage a household with multiple people sharing digital services. Do not connect it if you live alone or have no shared accounts. The decision comes down to whether you need a formal way to govern shared access instead of just sharing passwords.

Family Account Permission Matrix Tools

These tools let you map, verify, and audit access rights for every person in your household.

#	TOOL	DESCRIPTION
01	audit_approval_workflow	This tool identifies the specific contact person who holds the authority to change permissions for a given service.
02	generate_permission_matrix	This tool creates your primary access document by mapping family members to services and their specific allowed actions.
03	get_access_verification	This tool uses an access reference to confirm if a person is authorized to perform a specific action on a service.
04	schedule_permission_review	This tool manages your security oversight by recording or retrieving the next scheduled audit date for service permissions.

See It in Action

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

U Generate a permission matrix for Alice and Bob for Netflix and Utilities, where Alice can do everything and Bob can only view.

The permission matrix has been generated. Alice has full access to Netflix and Utilities, while Bob is restricted to viewing only.

U Can I verify if the access reference 'ref_123' is allowed to 'Pay Bill' on the 'Utilities' service?

Yes, the access reference 'ref_123' is authorized to 'Pay Bill' for the Utilities service.

U Who is the authorized contact to change permissions for the Banking service?

The authorized approver for the Banking service is the Primary Account Holder.

Frequently Asked Questions

01 **How do I use this MCP with my AI client?**

You connect to the MCP through the Vinkius platform. Once connected, your AI client can immediately call the tools to manage permissions.

02 **Can I use this to manage business permissions?**

The tool is designed for family service access and household governance, though the logic applies to any structured permission needs.

03 **What is an access reference?**

An access reference is a secure identifier used to validate whether a person is authorized to perform a specific action on a service.

04 **How do I know who can change my service settings?**

You can use the audit approval workflow tool to identify the specific contact authorized to change permissions for any service.

05 **Does this MCP host my data?**

Vinkius hosts and manages the MCP, allowing you to use the tools through your AI client without managing the underlying infrastructure.

06 **How do I create a new permission grid?**

Use the `generate_permission_matrix` tool by providing the list of services, family members, and the specific actions allowed or forbidden.

07 **How can I schedule a security audit?**

You can use the `schedule_permission_review` tool to set a future date for auditing a specific service's permissions.

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 `"family-account-permission-matrix": { "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

Family Account Permission Matrix 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 Account Permission Matrix. 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 Account Permission Matrix MCP
Server ID	`01a0db08-ccf7-70e5-a80a-3b031c82d092`
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-account-permission-matrix.