MCP SERVER | NO CODE | CLOUD HOSTED

Emergency Digital Access Brief MCP

Execute secure credential recovery when it matters most.

Emergency Digital Access Brief MCP provides a structured framework for managing digital access during predefined emergency conditions. It helps you navigate complex security protocols by verifying permissions, locating secure credential storage, and ensuring notification sequences are followed correctly through your AI client.

A+ Quality Score 100/100

emergency | access-control | digital-legacy | security-protocol | credential-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/emergency-digital-access-brief

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.

Emergency Digital Access Brief MCP

4 tools available
Cloud-hosted on Vinkius

When a crisis hits, finding the right digital keys shouldn't be a guessing game. This MCP gives your AI client a set of tools to manage sensitive access protocols under pressure. Instead of digging through spreadsheets or unorganized files, you use your agent to walk through a pre-defined security framework. You can verify if a specific person has the right to request access, find exactly where a category of credentials lives, and confirm that the right people are being notified before anything is unlocked. It bridges the gap between high-stakes emergency needs and the rigid requirements of secure digital asset management. You aren't just searching for passwords; you are executing a controlled, audited activation process.

Core Capabilities

01 — Protocol Generation

Your agent creates structured activation guides for specific emergency scenarios.

02 — Permission Verification

The AI checks if a user has the legal or procedural right to request access.

03 — Credential Mapping

Your agent identifies the physical or digital location of specific credential sets.

04 — Notification Auditing

The tool ensures the contact chain is followed before any access is finalized.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/emergency-digital-access-brief** — connect your AI agent in three steps.

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

02 Provide the emergency scenario details to your agent.

03 The agent uses the tools to validate permissions and locate credentials.

04 Follow the generated step-by-step protocol to complete the access request.

Connecting this MCP to your AI client gives your agent immediate access to your security protocols.

Built For

This MCP is built for professionals managing high-security digital assets and sensitive family or corporate legacies.

Security Officers

They use the MCP to enforce strict access protocols during security incidents.

Estate Managers

They hand off the task of navigating digital legacy access to their AI agent.

IT Administrators

They use the tool to manage emergency credential recovery workflows.

What Changes When You Connect

01 Reduces decision fatigue during high-pressure emergency scenarios.

02 Ensures all notification sequences are strictly followed.

03 Provides a clear map to credential storage locations.

04 Prevents unauthorized access through automated permission checks.

Real-World Applications

Medical Incapacity

An agent helps a family member navigate financial account access when a primary holder is incapacitated.

Corporate Security Breach

Security teams use the protocol generator to execute emergency access for recovery teams.

Digital Legacy Planning

Users set up structured guides to ensure heirs can find necessary credentials later.

Emergency Credential Recovery

The AI identifies where specific identity credentials are stored during a lockout.

Patterns to Avoid

Bypassing the notification chain

AVOID

You try to grab credentials immediately because you are in a rush during a security breach.

✓ INSTEAD

Always run `verify_contact_chain` first to ensure the required parties are notified before you proceed.

Guessing credential locations

AVOID

You search through random folders hoping to find the right login details for a locked account.

✓ INSTEAD

Use `map_account_to_location` to find exactly where that specific category of credentials is stored.

Assuming authorization is automatic

AVOID

You assume a family member has the right to access an estate account just because they are listed in a will.

✓ INSTEAD

Run `validate_authorization` to confirm the person actually has the procedural right to start the request.

The Right Fit

Connect this MCP if you manage high-stakes digital assets or sensitive corporate legacies where access must be audited and controlled. Do not connect it if you are looking for a simple password manager for casual use. The decision depends on whether you need a structured protocol for high-pressure activation rather than just a list of passwords.

Emergency Digital Access Brief 4 Tools

These tools manage the transition from crisis to controlled access. They handle everything from permission checks to locating specific credential sets.

#	TOOL	DESCRIPTION
01	`generate_access_protocol`	This tool builds a step-by-step activation guide based on the specific emergency variables you provide.
02	`map_account_to_location`	Use this to identify the exact storage location for a specific category of credentials.
03	`validate_authorization`	This tool checks if a person is permitted to start an access request under current conditions.
04	`verify_contact_chain`	This tool confirms that the required notification protocol is being followed before access is granted.

See It in Action

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

U Generate an access protocol for a medical incapacity scenario involving Alice and Bob for Financial accounts.

The activation steps are: 1. Verify Alice's authorization. 2. Notify Bob as per the contact sequence. 3. Retrieve Financial credentials from the Secure Vault.

U Is Charlie authorized to access accounts during a High severity emergency?

No, Charlie is not in the authorized people list for this scenario.

U Where can I find the credentials for the Personal Identity category?

The credentials for Personal Identity are located in the Primary Digital Safe.

Frequently Asked Questions

01 **How does this MCP handle sensitive credentials?**

This MCP does not store your passwords. It provides the logic and maps to help your agent find where they are stored in your own secure locations.

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

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

03 **Can I use this for non-emergency access?**

The tool is specifically designed for predefined emergency conditions and structured activation protocols.

04 **Does it verify if a user is allowed to see data?**

Yes, the validate_authorization tool checks if a person is permitted to initiate an access request.

05 **How do I get started?**

You subscribe through Vinkius and connect your preferred AI client with one click.

06 **How do I generate a new access guide?**

You can use the `generate_access_protocol` tool by providing the emergency condition, authorized people, and account categories.

07 **Can I verify if someone is authorized to request access?**

Yes, the `validate_authorization` tool checks if a requester is on the permitted list based on the emergency severity.

08 **How are credentials located?**

The `map_account_to_location` tool identifies the specific secure vault or location where credentials for a category are stored.

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 `"emergency-digital-access-brief": { "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

Emergency Digital Access Brief 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

DOCUMENT INFORMATION

Generated	September 2026
MCP Server	Emergency Digital Access Brief MCP
Server ID	`01a0db77-62f9-70b9-984d-769af7875e34`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE