MCP SERVER | NO CODE | CLOUD HOSTED

Authorized Device Retirement Plan MCP

Securely decommission hardware while protecting data sovereignty.

Authorized Device Retirement Plan MCP handles the heavy lifting of hardware decommissioning. It helps you manage the entire lifecycle of retiring assets, from checking if data is safely backed up to verifying that the person receiving the device is actually authorized to take it. You get a clear, chronological checklist for every device to ensure nothing is missed during physical destruction or transfer.

A+ Quality Score 100/100

hardware | decommissioning | data-security | compliance | asset-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/authorized-device-retirement-plan

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.

Authorized Device Retirement Plan MCP

4 tools available
Cloud-hosted on Vinkius

Retiring hardware shouldn't be a guessing game of whether you backed up the right files. This MCP gives your AI client the specific tools needed to manage the hardware retirement lifecycle without skipping critical security steps. You can use it to verify that every data category is accounted for before a device leaves your control, ensuring total data sovereignty. Instead of manual checklists, your agent generates a step by step decommissioning plan for each piece of equipment. It also handles the logistics of custody transfers, making sure the person or department receiving the hardware is legally cleared to do so. Whether you are shredding drives or transferring assets to another department, this MCP keeps the process documented and predictable. You can even estimate how long the entire retirement project will take, helping you plan your resource allocation more effectively.

Core Capabilities

01 — Data Sovereignty Verification

Your agent checks if all required data categories are backed up before any hardware is destroyed.

02 — Automated Task Generation

The MCP builds a chronological decommissioning checklist for every individual device.

03 — Custody Validation

Your AI client verifies that recipients are authorized to take possession of the hardware.

04 — Timeline Estimation

The tool calculates the expected duration for the retirement process based on the number of devices.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/authorized-device-retirement-plan** — connect your AI agent in three steps.

01 Connect your preferred MCP client to Vinkius.

02 Provide your device details and data requirements to your AI client.

03 The agent uses the MCP to check readiness or generate task lists.

04 Follow the resulting chronological checklist to complete the retirement.

Connecting this MCP to your AI client gives your agent immediate access to hardware management tools.

Built For

This MCP is built for organizations that need to manage hardware lifecycles with strict security and compliance standards.

IT Asset Managers

They use the MCP to track device status and generate decommissioning checklists.

Security Compliance Officers

They rely on the tool to ensure data sovereignty and authorized custody transfers.

System Administrators

They use the generated task lists to execute physical hardware decommissioning.

What Changes When You Connect

01 Prevents data loss by verifying backups before hardware destruction.

02 Reduces human error with chronological, device specific task lists.

03 Ensures legal compliance through authorized custody verification.

04 Provides predictable scheduling with retirement timeline estimates.

Real-World Applications

Bulk Hardware Decommissioning

Manage the retirement of dozens of laptops at once by generating timelines and task lists.

Secure Data Disposal

Verify that all sensitive data categories are backed up before authorizing physical shredding.

Asset Transfer Auditing

Validate that a specific department is authorized to receive hardware during a custody transfer.

Compliance Readiness Checks

Use the readiness status tool to confirm a device meets all data requirements for disposal.

Patterns to Avoid

Manual checklist guessing

AVOID

An IT manager tries to remember every security step for a batch of laptops without a written plan.

✓ INSTEAD

Use generate_device_tasks to get a specific, chronological list of every step required for each individual unit.

Blindly shredding hardware

AVOID

A technician sends a drive to the shredder before confirming all sensitive files were moved to the cloud.

✓ INSTEAD

Run get_retirement_readiness_status first to ensure the device meets all data requirements before disposal.

Unverified asset transfers

AVOID

Handing over a fleet of tablets to a third party without checking if they are legally cleared to take them.

✓ INSTEAD

Always use validate_custody_transfer to confirm the recipient is authorized to handle the hardware.

The Right Fit

IT Asset Managers and Security Officers should connect this MCP if they handle hardware lifecycles with strict compliance needs. Organizations with loose, informal disposal processes don't need this. The deciding factor is whether you require documented, verifiable proof of data sovereignty and authorized custody.

Authorized Device Retirement Plan Tools

These tools handle the heavy lifting of decommissioning hardware, from verifying data backups to validating legal custody transfers.

#	TOOL	DESCRIPTION
01	`generate_device_tasks`	This tool creates a specific, chronological list of tasks for a single device to ensure the decommissioning process is complete.
02	`get_retirement_readiness_status`	Use this to check if a specific device is cleared for final disposal based on its specific data requirements.
03	`validate_custody_transfer`	This tool verifies that the planned recipient is legally or procedurally authorized to handle the hardware.
04	`calculate_retirement_timeline`	This tool estimates the window of time you will need to complete the entire retirement process.

See It in Action

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

U Is device DEV-992 ready for disposal? It has User Profiles and System Logs, and only User Profiles are backed up.

No, the device is not cleared for disposal. The missing category is: System Logs.

U Generate a task list for device DEV-101 with Financial Records and User Profiles. Both are backed up. The recipient is IT Department and the method is Physical Shredding.

1. Verify backup of Financial Records and User Profiles. 2. Perform Physical Shredding. 3. Transfer custody to IT Department.

U How long will it take to retire 50 devices starting on 2025-01-01?

The estimated completion is 2025-01-11, with a duration of 10 days.

Frequently Asked Questions

01 **How does this MCP ensure data is not lost?**

The get_retirement_readiness_status tool checks if all required data categories are backed up before a device is cleared for disposal.

02 **Can I use this with Claude or Cursor?**

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 **What happens if a recipient is not authorized?**

The validate_custody_transfer tool will verify the recipient against authorized protocols to ensure they are legally allowed to handle the device.

04 **Does it provide a schedule for decommissioning?**

Yes, the calculate_retirement_timeline tool provides an estimate of the time needed to finish the process.

05 **Is the task list the same for every device?**

No, the generate_device_tasks tool produces a specific, chronological list tailored to the individual device's requirements.

06 **How do I know if a device is ready to be destroyed?**

You can use the `get_retirement_readiness_status` tool. It compares the required data categories against confirmed backups to ensure no data is left behind.

07 **Can I generate a checklist for the entire decommissioning process?**

Yes, the `generate_device_tasks` tool produces a chronological list of tasks including backup verification, destruction, and custody transfer.

08 **How is the retirement timeline calculated?**

The `calculate_retirement_timeline` tool estimates the duration based on the number of devices and a complexity factor related to data volume.

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 `"authorized-device-retirement-plan": { "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

Authorized Device Retirement Plan 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 Authorized Device Retirement Plan. 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	Authorized Device Retirement Plan MCP
Server ID	`01a0dabe-570d-701d-bab6-ff73293f57a6`
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/authorized-device-retirement-plan.