

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

Accessible Personal Assistance Handoff Plan MCP

Coordinate shifts and safety protocols through your AI client.

Accessible Personal Assistance Handoff Plan MCP provides a structured framework for managing transitions between personal assistants. It helps your agent handle formal shift handoffs, task briefings, and routine change notifications while respecting user-defined boundaries and consent checkpoints. Use it to maintain safety and continuity in care or personal support environments.

A+ Quality Score 100/100

assistance

handoff

safety

coordination

protocol



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.

Accessible Personal Assistance Handoff Plan MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to manage the handoff between different assistants or caregivers. It acts as a coordination layer that ensures no critical information is lost during shift changes. Instead of relying on messy notes or verbal messages, your AI client uses this tool to access formal transition documents and task summaries.

When a new assistant starts their shift, they can check for any unresolved questions or safety-critical ambiguities that need immediate attention. The system keeps everything within the boundaries you set, ensuring that tasks are only performed when they fall within authorized limits. It also handles routine updates, so if a user's environment or schedule changes, the notification is broadcasted clearly. This keeps the workflow predictable and keeps safety at the forefront of every transition.

Core Capabilities

01 — Shift Transitions

Your agent uses this to pass critical information from one person to the next.

02 — Task Authorization

The AI checks this to ensure it only discusses or suggests tasks within set boundaries.

03 — Safety Monitoring

Your agent pulls the question log to find ambiguities that could cause safety issues.

04 — Routine Updates

The system broadcasts notifications when a user's environment or schedule changes.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/accessible-personal-assistance-handoff-plan — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 The MCP becomes available as a set of tools in your agent's interface.
- 03 Your agent calls specific tools like `get_task_briefing` to access data.
- 04 Information is processed according to the user's established protocols and boundaries.

Connect your AI client to the Vinkius-hosted MCP to start managing assistance workflows.

Built For

This MCP is designed for professional or personal coordination environments where continuity of care is vital.

Caregivers

They use it to receive handoff protocols and task briefings during shift changes.

Personal Assistants

They rely on it to stay within authorized task boundaries and receive routine updates.

Care Coordinators

They use the tool to manage safety-critical ambiguities and formal notifications.

What Changes When You Connect

- 01 Reduces errors during shift changes through formal handoff protocols.
- 02 Enforces user-defined boundaries for task performance.

-
- | | |
|-----------|---|
| 03 | Identifies safety-critical ambiguities through a dedicated question log. |
| <hr/> | |
| 04 | Maintains clear communication regarding routine or environmental changes. |
-

Real-World Applications

Caregiver Shift Changes

An incoming caregiver uses the handoff protocol to see exactly what happened during the previous shift.

Boundary Enforcement

An AI agent checks the task briefing to ensure it doesn't suggest actions outside of authorized limits.

Safety Management

A coordinator reviews the unresolved question log to fix issues before they become problems.

Routine Monitoring

The system sends a notification when a user's daily schedule is modified.

Patterns to Avoid

Relying on verbal handoffs

❌ AVOID

A new caregiver walks into a room and asks the outgoing staff what happened during their shift. This leads to missed details and confusion.

✓ INSTEAD

Use `get_shift_handoff_protocol` to access a formal transition document that captures all necessary details from the previous shift.

Ignoring task boundaries

❌ AVOID

An AI agent suggests a medical task that the user hasn't authorized, potentially creating a safety risk.

✓ INSTEAD

Always call `get_task_briefing` to verify which specific tasks are currently allowed before your agent takes any action.

Overlooking safety ambiguities

❌ AVOID

A coordinator assumes everything is fine and moves to the next task without checking for pending issues.

✓ INSTEAD

Check the `get_unresolved_question_log` to identify any pending questions or safety-critical ambiguities that need to be solved first.

The Right Fit

Connect this MCP if you manage professional caregivers or personal assistants in environments where continuity of care is a safety requirement. Do not connect it if your workflow is purely administrative and lacks a need for strict task authorization or shift transitions. The deciding factor is whether a gap in information during a handoff could lead to a safety incident.

4 Tools for Managing Caregiver Handoffs and Safety

These tools manage the flow of information between assistants, enforce task boundaries, and track unresolved safety questions.

#	TOOL	DESCRIPTION
01	get_change_notification	Use this to create or receive formal notifications regarding changes in a user's routine or environment.
02	get_shift_handoff_protocol	This tool generates a formal transition document to pass information between outgoing and incoming assistants.
03	get_task_briefing	This tool provides a concise summary of specific tasks that are currently authorized for performance.
04	get_unresolved_question_log	This tool retrieves a list of pending questions or ambiguities that require resolution before proceeding.

See It in Action

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

U Generate a handoff protocol for the transition between assistant A and assistant B.



The transition protocol is ready. It includes completed task statuses, pending items for the incoming assistant, and all active safety checkpoints.

U What tasks am I permitted to perform right now?



You are authorized for meal preparation and light housekeeping. Note that any changes to the medication schedule require a specific consent trigger.

U Are there any unresolved questions preventing me from starting my shift?



Yes, there is one high-priority question regarding the specific location of the user's mobility equipment.

Frequently Asked Questions

01 What can this MCP do for my personal assistant workflow?

It provides a structured way to handle shift handoffs, task briefings, and safety notifications through your AI client.

02 How does it handle safety?

It uses a specific tool to log unresolved questions and ambiguities, allowing you to address safety-critical issues immediately.

03 Can I restrict what my AI agent suggests?

Yes, the task briefing tool filters information based on authorized boundaries and consent checkpoints.

04 Which AI clients work with this MCP?

This MCP works with any compatible client, including Claude, Cursor, Windsurf, and VS Code.

05 Do I need to host this myself?

No, Vinkius hosts and manages the MCP for you, so it is ready to use as soon as you connect.

06 How does this server ensure safety during transitions?

Safety is maintained through ``get_shift_handoff_protocol`` and ``get_task_briefing``, which enforce user-defined consent checkpoints and task boundaries, ensuring no unauthorized actions are taken.

07 Can I use this to receive task instructions?

Yes, assistants can use ``get_task_briefing`` to receive a summary of permitted tasks and specific consent triggers required for their role.

08 What happens if there is a change in the user's routine?

Changes are managed via ``get_change_notification``, which broadcasts updates regarding routine, equipment, or communication to all affected authorized assistants.

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>"accessible-personal-assistance-handoff-plan": { "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

Accessible Personal Assistance Handoff 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 Accessible Personal Assistance Handoff 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	Accessible Personal Assistance Handoff Plan MCP
Server ID	01a0d312-7772-728c-a21f-c1babc277967
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/accessible-personal-assistance-handoff-plan.