

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 Home Visitor Protocol MCP

Manage visitor access while protecting resident privacy and needs.

Accessible Home Visitor Protocol MCP bridges the gap between residents with specific accessibility requirements and their incoming visitors. It turns household boundaries and building entry rules into structured communication flows. Your AI client uses this to prepare visitors, manage arrival transitions, and ensure resident consent is respected throughout the visit.

A+ Quality Score 100/100

accessibility

privacy-preserving

visitor-management

household-safety

protocol-engine



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 Home Visitor Protocol MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to manage how visitors interact with residents who have specific accessibility or privacy needs. Instead of manual coordination, your AI client handles the heavy lifting of preparing visitors for what to expect when they arrive. It translates complex household requirements, such as lighting preferences or quiet periods, into clear instructions for service providers or guests.

When a visitor arrives, the MCP manages the handoff from the building entrance to the resident's door. It ensures that people like medical professionals or maintenance workers follow specific boundaries, such as staying in certain rooms or following verbal cues. Most importantly, it keeps the resident in control. You can use it to facilitate post-visit reviews to confirm that all privacy protocols were followed. This keeps the home environment predictable and safe without sacrificing the resident's autonomy.

Core Capabilities

01 — Visitor Preparation

Your agent generates briefings so visitors know exactly what to expect before they reach the door.

03 — Arrival Transitions

Your agent manages the handoff between a visitor's arrival and their meeting with the resident.

02 — Entry Management

The AI provides specific navigation instructions for building entrances and gates.

04 — Privacy Enforcement

The MCP facilitates feedback loops to ensure residents can verify that their boundaries were respected.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/accessible-home-visitor-protocol — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Input the resident's specific needs and building rules into your AI client.
- 03 Use the tools to generate briefings or entry instructions for visitors.
- 04 Manage the arrival handoff through the agent.
- 05 Complete the process with a privacy feedback check.

You connect your AI client to the Vinkius-hosted MCP to start managing visitor flows.

Built For

This MCP is designed for caregivers, household managers, and accessibility coordinators who need to coordinate visits safely.

Caregivers

They use the MCP to relay specific resident needs to visiting medical or support staff.

Home Managers

They use the tool to manage entry protocols and household boundaries for service workers.

Accessibility Coordinators

They use the protocol to ensure visitor behavior aligns with resident requirements.

What Changes When You Connect

- 01 Reduces friction during visitor arrival through structured briefings.
- 02 Protects resident privacy by facilitating post-visit feedback.

- 03

Ensures household boundaries are communicated clearly to external workers.
- 04

Standardizes how visitors navigate building entry points.

Real-World Applications

Medical Visits

A nurse receives a briefing about a resident's need for low lighting and quiet environments before arriving.

Secure Building Entry

A delivery person or guest gets the exact gate code and contact instructions needed to enter the property.

Home Maintenance

A repair technician is given specific instructions to stay in the kitchen and avoid certain bedrooms.

Privacy Auditing

A resident uses the feedback tool to confirm a visitor respected their personal space after the visit ends.

Patterns to Avoid

Manual instruction delivery

❌ AVOID

A caregiver texts a long list of lighting and noise requirements to a nurse right before they arrive at the house.

✓ INSTEAD

Use ``generate_pre_visit_briefing`` to send a structured information package that the visitor can review before they even leave their previous location.

Unstructured entry coordination

❌ AVOID

A delivery person arrives at a gated community and has to call the resident repeatedly to get the gate code.

✓ INSTEAD

Provide the exact gate codes and navigation steps ahead of time using ``get_entry_protocol``.

Ignoring post-visit compliance

❌ AVOID

A maintenance worker enters a bedroom they weren't supposed to, but the resident doesn't report it because they don't have a process.

✓ INSTEAD

Run a formal check after the worker leaves by using ``initiate_privacy_feedback`` to confirm all boundaries were respected.

The Right Fit

Caregivers and household managers should connect this MCP if they manage frequent visits from external staff. If you only have visitors once a month, you probably don't need this. The deciding factor is whether you need to standardize how service providers interact with a resident's specific environment.

Accessible Home Visitor Protocol Tools

These tools manage the entire visitor lifecycle, from initial arrival instructions to post-visit privacy checks.

#	TOOL	DESCRIPTION
01	get_entry_protocol	This tool provides visitors with specific instructions for navigating building exteriors and entry points.
02	generate_pre_visit_briefing	This tool creates a complete information package for visitors to read before they arrive at the residence.
03	initiate_privacy_feedback	This tool starts a post-visit review process so residents can confirm that all privacy rules were respected.
04	orchestrate_handoff	This tool manages the transition period from the moment a visitor arrives to their actual interaction with the resident.

See It in Action

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

- U** Prepare a briefing for a medical professional arriving at 2 PM, noting that the resident needs low lighting and there is a quiet period scheduled.



The briefing is ready. The visitor will be notified about the low lighting requirement and the scheduled quiet period to ensure they comply upon arrival.

- U** The visitor has arrived at the gate. How should they enter and contact the resident?



The visitor should use gate code 1234 and then send a text message to the resident as requested.

- U** The maintenance worker is inside. Remind them of the boundaries and the resident's needs.



The worker is instructed to stay in the kitchen, avoid the second bedroom, and provide verbal cues as requested by the resident.

Frequently Asked Questions

01 What does this MCP actually do?

It manages the communication between residents with accessibility needs and their visitors by providing briefings, entry instructions, and privacy checks.

02 Which AI clients can I use with this?

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

03 How does it protect resident privacy?

It uses a specific tool to initiate privacy feedback, allowing residents to confirm that visitors followed all established protocols.

04 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 your client.

05 Can I use this for medical professionals?

Yes, you can generate briefings that include specific medical-related environmental needs like lighting or noise levels.

06 How does this protocol protect resident privacy?

The protocol uses a tiered information system and the ``initiate_privacy_feedback`` tool to ensure only necessary context is shared with visitors, masking sensitive data.

07 Can I use this for delivery personnel?

Yes. By using ``get_entry_protocol``, you can provide couriers with specific building rules and contact methods without revealing sensitive household details.

08 What happens if a visitor ignores household boundaries?

Residents can use the ``initiate_privacy_feedback`` tool after a visit to report if the protocol was followed, helping to refine future instructions.

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-home-visitor-protocol": { "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 Home Visitor Protocol 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 Home Visitor Protocol. 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 Home Visitor Protocol MCP
Server ID	01a0d239-3c0e-7264-925a-a453796898b2
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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-home-visitor-protocol.