

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 Transport Disruption Plan MCP

Automate contingency plans for mobility-dependent travelers during transport failures.

Accessible Transport Disruption Plan MCP handles contingency management for users with mobility requirements. When transport providers fail or delay, your AI client uses this MCP to trigger response protocols, check provider status, and validate that fallback routes meet strict accessibility standards.

A+ Quality Score 100/100

mobility

contingency

transport

accessibility

disruption



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 Transport Disruption Plan MCP

4 tools available

Cloud-hosted on Vinkius

When transport networks fail, users with mobility needs face much higher risks than the general public. This MCP gives your AI agent the logic needed to manage these disruptions in real time. Instead of manual troubleshooting, your agent can instantly check if a provider is running late, verify if a new route is actually wheelchair accessible, and execute a pre-planned fallback sequence. You can use it to build reliable, automated safety nets for recurring journeys. It moves beyond simple navigation by focusing on the specific constraints of accessibility, ensuring that a delay doesn't turn into a stranded passenger situation. Your agent handles the heavy lifting of checking provider availability and validating that every contingency plan stays compliant with mobility requirements.

Core Capabilities

01 — Contingency Generation

Your agent creates specific response protocols when a transport failure is detected.

02 — Real-time Status Monitoring

The AI checks for delays or availability issues with specific transport providers.

03 — Accessibility Validation

Your agent verifies that new journey configurations meet necessary mobility requirements.

04 — Fallback Testing

The AI simulates disruptions to confirm that fallback rules actually work before a real event occurs.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/accessible-transport-disruption-plan — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Grant the agent access to the Accessible Transport Disruption Plan MCP.
- 03 The agent uses the tools to monitor providers or validate routes.
- 04 The agent executes contingency plans or notifies contacts when disruptions occur.

Connect the MCP to your AI client to start managing transport contingencies.

Built For

This MCP is built for developers and operators managing specialized transport services for people with disabilities.

Mobility Service Operators

They hand off disruption management and provider status checks to the AI.

Accessibility Coordinators

They use the agent to validate that journey configurations remain compliant.

Logistics Developers

They integrate these tools into automated dispatch and contingency systems.

What Changes When You Connect

- 01 Automates the transition from primary to secondary transport providers.
- 02 Reduces manual verification of accessibility compliance for new routes.

-
- | | |
|-----------|--|
| 03 | Validates fallback plans through simulation before disruptions happen. |
| <hr/> | |
| 04 | Provides instant status updates on transport provider delays. |
-

Real-World Applications

Emergency Transport Switching

When a primary vehicle is delayed, the agent automatically triggers a secondary provider.

Route Compliance Auditing

The AI checks if a proposed recurring route meets specific wheelchair accessibility needs.

Proactive Plan Testing

Operators simulate transport failures to ensure their fallback rules are actually functional.

Real-time Delay Monitoring

The agent monitors provider status to anticipate disruptions before they impact the user.

Patterns to Avoid

Manual route checking

❌ AVOID

You manually check every single route change to see if a wheelchair can still fit on the new vehicle.

✓ INSTEAD

Let your agent handle the heavy lifting by using ``validate_journey_parameters`` to confirm accessibility compliance instantly.

Reactive disruption response

❌ AVOID

Waiting until a passenger is already stranded to figure out which backup provider is available.

✓ INSTEAD

Use ``get_disruption_plan`` to have a ready-to-go contingency response the moment a delay is detected.

Blind fallback reliance

❌ AVOID

Assuming your secondary transport provider will actually be able to pick up the user during a peak delay.

✓ INSTEAD

Run a ``simulate_fallback_sequence`` first to make sure your backup rules actually work under pressure.

The Right Fit

Connect this MCP if you manage specialized transport services where mobility constraints make standard rerouting impossible. Do not connect it if you only handle general passenger transit where any available vehicle suffices. The deciding factor is whether your service requires strict adherence to specific accessibility requirements during service failures.

4 Tools for Managing Accessible Transport Disruptions

These tools give your agent the ability to monitor provider status, validate accessibility, and run contingency simulations.

#	TOOL	DESCRIPTION
01	get_disruption_plan	Generates a complete contingency response for a specific journey when a disruption occurs.
02	get_provider_status	Checks the current availability or delay status of a specific transport provider.
03	simulate_fallback_sequence	Tests a user's fallback rules against a hypothetical disruption to ensure the plan is viable.
04	validate_journey_parameters	Ensures a new recurring journey configuration is logically sound and meets accessibility requirements.

See It in Action

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

U My primary transport provider is delayed by 20 minutes. What is the contingency plan?



The disruption trigger has been activated. The system will notify your primary contact via SMS and then attempt to book your secondary provider, Provider B.

U Check if my current transport provider is available for my 10:00 AM trip.



Provider Alpha is currently available and is running on schedule for your 10:00 AM trip.

U Is my new journey configuration valid for someone using a wheelchair?



The journey configuration is valid. All selected pickup points are marked as accessible and the fallback providers are correctly prioritized.

Frequently Asked Questions

01 What does this MCP do?

It provides tools for managing transport disruptions specifically for users with mobility needs. It handles contingency planning, provider status checks, and accessibility validation.

02 How do I use this with my AI agent?

You connect your AI client, such as Claude or Cursor, to the Vinkius platform. Once connected, your agent can immediately call the tools provided by this MCP.

03 Can I test my contingency plans before they are needed?

Yes. You can use the `simulate_fallback_sequence` tool to test your fallback rules against hypothetical disruptions to ensure they work.

04 Does it check for wheelchair accessibility?

Yes. The `validate_journey_parameters` tool is specifically designed to ensure journey configurations meet accessibility requirements.

05 Which clients are compatible?

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

06 How does the system handle a provider delay?

The system uses `'get_disruption_plan'` to evaluate if a delay exceeds the user's maximum acceptable limit and then triggers the pre-defined fallback rules.

07 Can I test my fallback rules before a real disruption occurs?

Yes, you can use the `'simulate_fallback_sequence'` tool to run hypothetical failure scenarios and verify that the replacement actions are viable.

08 How are accessibility requirements enforced?

The `'validate_journey_parameters'` tool ensures that all pickup points are explicitly marked as accessible and that the journey configuration is logically sound.

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-transport-disruption-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 Transport Disruption 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 Transport Disruption 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 Transport Disruption Plan MCP
Server ID	01a0d239-c88d-73a2-8c42-61933b554d27
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-transport-disruption-plan.