

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

Altitude Sickness Risk Assessment MCP

Plan safer high-altitude expeditions with physiological data.

Altitude Sickness Risk Assessment MCP gives your AI client the physiological modeling needed to manage high-altitude risks. It calculates your probability of Acute Mountain Sickness, suggests how many days you need to spend acclimatizing, and provides specific hydration targets and emergency safety protocols based on your specific trip profile.

altitude

ams

physiology

safety

mountain



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.

Altitude Sickness Risk Assessment MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to turn your AI agent into a specialized high-altitude safety planner. Instead of guessing how your body might react to thin air, you provide your trip details and get specific physiological insights. It handles the math behind Acute Mountain Sickness (AMS) risk, helping you decide if your planned ascent rate is too aggressive. You can use it to build out a full itinerary that includes necessary acclimatization buffers and daily hydration targets to keep you stable. When you're planning an expedition, it also generates emergency checklists so you aren't scrambling for protocols if someone shows symptoms. It's a practical way to add a layer of data-driven safety to your mountain travel planning.

Core Capabilities

01 — AMS Risk Modeling

Your agent calculates the probability and severity of sickness for any specific ascent profile.

02 — Acclimatization Scheduling

The AI determines how many days you need to spend at altitude to adjust safely.

03 — Hydration Planning

Your agent provides daily fluid targets to manage physiological stress.

04 — Emergency Protocol Generation

The AI creates checklists of warning signs and actions based on your risk level.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/altitude-sickness-risk-assessment — connect your AI agent in three steps.

- 01 Connect your preferred MCP-compatible client to Vinkius.
- 02 Provide your trip details like altitude, fitness, and susceptibility to your AI agent.
- 03 The agent calls the specific tools to run the physiological models.
- 04 You receive specific risk scores, hydration targets, or safety checklists.

Connect your client to Vinkius and start asking your agent about altitude safety.

Built For

This MCP is built for anyone planning travel to high altitudes who needs data-backed safety guidelines.

Expedition Planners

They hand off trip profiles to the AI to generate safety protocols and ascent schedules.

Mountain Guides

They use the tool to assess the risk levels of their clients based on fitness and susceptibility.

High-Altitude Travelers

They use it to get personalized hydration and acclimatization advice for their personal trips.

What Changes When You Connect

- 01 Reduces guesswork in ascent planning through physiological modeling.
- 02 Provides specific daily hydration targets to prevent dehydration.

-
- 03** Creates actionable emergency checklists based on individual risk scores.
-
- 04** Calculates necessary acclimatization buffers to prevent AMS.
-

Real-World Applications

Trip Risk Assessment

You input your starting altitude and target summit to see your AMS risk score.

Daily Health Management

You check your specific fluid requirements for your current altitude.

Itinerary Building

You use the tool to figure out how many rest days to add to your climbing schedule.

Safety Preparation

You generate a list of warning signs to watch for during a high-altitude push.

4 Tools Available

#	TOOL	DESCRIPTION
01	get_acclimatization_recommendation	This tool calculates the number of days you need to stay at certain altitudes to safely adjust. It uses your planned ascent rate to suggest a safe schedule.
02	get_ams_risk_score	This tool determines your probability and severity of Acute Mountain Sickness. It analyzes your specific trip profile to give you a risk score.
03	get_hydration_guidelines	This tool provides specific fluid intake targets. It helps you mitigate physiological stress caused by altitude through precise hydration goals.
04	get_safety_protocol	This tool generates a checklist of emergency actions. It creates specific response steps and warning signs based on your calculated risk level.

See It in Action

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

U What is my AMS risk if I go from 1500m to 4000m with 3 days of acclimatization, a susceptibility of 5, hydration of 8, and fitness of 7?



Your AMS risk score is 6, which is categorized as High Risk. You should monitor for symptoms like headache or nausea.

U How many days should I spend acclimatizing for a summit at 5000m starting from 2000m with standard susceptibility?



You should plan for at least 5 days of acclimatization, with an additional 2 days suggested as a safety buffer.

U What are my hydration needs at 4500m with a fitness level of 8?



You should aim for 4.5 liters of fluid daily and prioritize electrolyte intake to maintain fluid balance.

Frequently Asked Questions

01 What is this MCP used for?

It is used to calculate AMS risk, determine acclimatization needs, and provide hydration and safety guidelines for high-altitude travel.

02 Which AI clients can use this?

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

03 How does it calculate AMS risk?

It uses the `get_ams_risk_score` tool to analyze your specific trip profile, including altitude changes and personal susceptibility.

04 Can it help with hydration planning?

Yes, the `get_hydration_guidelines` tool provides specific fluid targets to help manage physiological stress at altitude.

05 Does it provide emergency instructions?

Yes, the `get_safety_protocol` tool generates checklists of emergency actions and warning signs based on your risk level.

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>"altitude-sickness-risk-assessment": { "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

Altitude Sickness Risk Assessment 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 Altitude Sickness Risk Assessment. 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	Altitude Sickness Risk Assessment MCP
Server ID	01a0a25f-fff7-7396-9b9b-126e0afb7138
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/altitude-sickness-risk-assessment.