

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

Cold Plunge Protocol Generator MCP

Build safe, personalized cold therapy routines in seconds.

Cold Plunge Protocol Generator MCP uses Wim Hof principles to build custom cold water immersion plans. Your AI client can generate specific breathing patterns, check if temperatures are safe for your health profile, and map out long-term training milestones. It turns your agent into a specialized cold therapy coach.

A+ Quality Score 100/100

cold-plunge

wim-hof

resilience

recovery

biohacking



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.

Cold Plunge Protocol Generator MCP

4 tools available

Cloud-hosted on Vinkius

You can stop guessing about water temperature and immersion times. This MCP gives your AI client the specific logic needed to design cold therapy routines that follow Wim Hof principles. Instead of following generic internet advice, you get plans tailored to your specific goals, whether that is building physical resilience or speeding up muscle recovery.

Your agent can act as a safety filter by checking your health profile against specific temperatures and durations before you get in the water. It also handles the math for your progression, helping you move from beginner sessions to advanced training without hitting a plateau. You can also use it to coordinate your breathing, ensuring your respiratory patterns match the intensity of your plunge. It's a direct way to bring structured biohacking protocols into your existing AI workflow.

Core Capabilities

01 — Personalized Planning

Your agent creates custom immersion durations and breathing steps based on your specific profile.

02 — Safety Validation

The AI checks your planned temperature and time against your health data to flag high-risk sessions.

03 — Training Roadmaps

Your client can outline long-term milestones to help you advance your cold exposure training.

04 — Breathing Coordination

The tool calculates specific breathing patterns to use before and during your plunge.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/cold-plunge-protocol-generator — connect your AI agent in three steps.

- 01 Connect the MCP to Claude, Cursor, or Windsurf via Vinkius.
- 02 Provide your health profile and cold exposure goals to your AI client.
- 03 Ask your agent to generate a protocol or check a specific temperature.
- 04 Receive a detailed plan including breathing steps and immersion times.

Connect the MCP to your AI client and start asking for specific cold therapy guidance.

Built For

This MCP is built for individuals practicing biohacking and cold water immersion. It helps users move from random experimentation to structured, data-driven training.

Biohackers

Users who want to automate the creation of structured cold therapy routines.

Athletes

People using cold exposure for recovery who need specific breathing and timing protocols.

Resilience Trainers

Individuals focused on long-term adaptation and progressive cold exposure milestones.

What Changes When You Connect

- 01 Reduces guesswork by providing specific immersion times and temperatures.
- 02 Adds a safety layer by checking health profiles against planned exposure.

- 03 Automates the progression logic for long-term training.
- 04 Syncs breathing patterns with immersion intensity.

Real-World Applications

Beginner Onboarding

A new user asks for a starting protocol at a moderate temperature to build initial resilience.

Recovery Optimization

An athlete requests a breathing and immersion plan specifically designed to aid muscle recovery.

Safety Checking

A user with a specific health condition checks if a planned deep freeze is safe for them.

Long-term Tracking

A regular practitioner asks for the next milestone in their training roadmap to keep progressing.

4 Tools Available

#	TOOL	DESCRIPTION
01	calculate_breathing_routine	This tool defines the exact breathing patterns you should use before and during your immersion. It matches your respiratory steps to your specific cold therapy goals.
02	get_progression_milestones	This tool provides a structured roadmap for your training. It shows you how to advance your cold exposure over time.
03	get_protocol	This tool generates a full, personalized cold plunge plan. It uses your profile and goals to set immersion times and breathing steps.
04	validate_safety	This tool checks if your planned temperature and duration are safe. It compares your parameters against your specific health profile.

See It in Action

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

U Generate a protocol for a beginner looking for resilience at 10 degrees Celsius.



Your protocol includes 2 minutes of immersion at 10°C, preceded by 3 cycles of controlled breathing with 30-second breath holds.

U Is it safe to plunge at 5 degrees for 5 minutes if I have high blood pressure?



No, a 5-minute immersion at 5°C with high blood pressure is considered high risk. It is recommended to consult a medical professional first.

U What breathing pattern should I use for recovery?



For recovery, use a moderate breathing pattern with 4 cycles of deep inhalations and controlled exhalations to manage physiological stress.

Frequently Asked Questions

01 How does this MCP handle safety?

The `validate_safety` tool compares your planned temperature and duration against your personal health profile to identify high-risk scenarios.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any compatible client like Claude, Cursor, or Windsurf once you subscribe through Vinkius.

03 Does it include breathing instructions?

Yes, the `calculate_breathing_routine` tool provides specific patterns to use before and during your plunge.

04 Is it based on specific methods?

The protocols are designed using Wim Hof principles for cold water immersion.

05 Can it help me advance my training?

Yes, the `get_progression_milestones` tool provides a roadmap to help you advance your training over time.

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>"cold-plunge-protocol-generator": { "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

Cold Plunge Protocol Generator 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 Cold Plunge Protocol Generator. 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	Cold Plunge Protocol Generator MCP
Server ID	01a0b61c-d6fa-7081-9352-fb2301b06552
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/cold-plunge-protocol-generator.