

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

Confined Space Entry Program MCP

Automate OSHA safety protocols and atmospheric monitoring requirements.

Confined Space Entry Program MCP handles the heavy lifting for industrial safety compliance. It uses OSHA Permit-Required Confined Space (PRCS) standards to run safety calculations, classify hazards, and build out rescue and ventilation plans. You can connect it to your AI client to turn raw site data into actionable, compliant safety documentation.

A+ Quality Score 100/100

osha

safety

confined-space

industrial-safety

compliance-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.

Confined Space Entry Program MCP

4 tools available

Cloud-hosted on Vinkius

Managing confined space entries requires strict adherence to OSHA standards to prevent accidents. This MCP acts as a compliance engine that processes your site data to ensure every entry meets safety requirements. Instead of manually calculating airflow or gas testing frequencies, you give your agent the space dimensions and known hazards, and it handles the math.

You can use it to classify whether a space is a Permit-Required Confined Space (PRCS) based on its geometry or potential for engulfment. Once the space is identified, the MCP determines how often you need to test the air, what specific gases to watch for, and how much mechanical ventilation is needed to keep the atmosphere safe. It also builds out the human element of the safety plan by defining exactly who needs to be on-site and what the specific rescue protocols should look like. It's a direct way to move from a physical hazard to a documented safety plan without the manual guesswork.

Core Capabilities

01 — Hazard Classification

Your agent uses this to identify if a space meets PRCS criteria.

02 — Atmospheric Planning

The AI calculates gas testing frequencies and specific gas targets.

03 — Ventilation Math

Your agent determines the mechanical airflow needed for a specific volume.

04 — Rescue Staffing

The MCP defines the required personnel and rescue protocols for an entry.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/confined-space-entry-program — connect your AI agent in three steps.

- 01 Connect your AI client to the MCP via Vinkius.
- 02 Provide the space dimensions and known hazards to your agent.
- 03 The agent runs the necessary calculations for hazards, air, and ventilation.
- 04 Review the generated safety protocols and rescue plans.

You connect the MCP to your AI client and feed it site-specific data to generate safety plans.

Built For

Safety professionals and industrial managers use this to automate the technical side of OSHA compliance.

Safety Officers

They hand off site dimensions and hazard data to get compliant safety protocols.

Industrial Managers

They use the tool to verify that their entry plans meet regulatory standards.

Compliance Auditors

They use the calculations to validate that ventilation and monitoring plans are sufficient.

What Changes When You Connect

- 01 Reduces manual calculation errors for ventilation and gas monitoring.
- 02 Standardizes safety protocols based on OSHA PRCS requirements.

- 03

Speeds up the creation of entry permits and rescue plans.
- 04

Provides consistent hazard classification across different job sites.

Real-World Applications

Tank Entry Preparation

A manager provides tank dimensions to determine if it requires a permit and what ventilation is needed.

Gas Monitoring Setup

A safety officer uses the tool to decide which gases to test for in a space with known contaminants.

Rescue Plan Drafting

An engineer uses the MCP to define the specific staffing and rescue steps for a high-risk entry.

Ventilation Verification

A technician checks if their current mechanical ventilation meets the calculated requirements for a specific volume.

Patterns to Avoid

Manual Hazard Guessing

❌ AVOID

A supervisor looks at a tank and decides it doesn't need a permit because it looks empty and clean.

✓ INSTEAD

Input the specific dimensions and known contaminants into the MCP to let it accurately classify the space using ``evaluate_space_hazard``.

Estimating Airflow Needs

❌ AVOID

A technician assumes a single standard fan is enough to clear a large vessel without checking the volume.

✓ INSTEAD

Use ``determine_ventilation_strategy`` to get the exact mechanical airflow required for that specific volume and contaminant level.

Vague Safety Protocols

❌ AVOID

Writing a generic safety plan that doesn't specify who is on-site or what the rescue steps are.

✓ INSTEAD

Run ``generate_entry_roles_and_rescue`` to build a specific staffing plan and rescue protocol tailored to the job.

The Right Fit

Safety officers and industrial managers should connect this MCP if they need to automate technical OSHA compliance math. It is not for general administrative staff. The decision depends on whether you need to move from raw site data to a documented safety plan without manual calculation errors.

Confined Space Entry Program 4 Tools

These tools handle the technical math and regulatory logic for OSHA-compliant entry planning. Your agent uses them to classify hazards, calculate ventilation, and set monitoring schedules.

#	TOOL	DESCRIPTION
01	calculate_atmospheric_monitoring	This tool sets your gas testing protocols. It tells you which specific gases to monitor and how often you need to run tests.
02	determine_ventilation_strategy	This tool handles airflow math. It calculates the mechanical ventilation needed to keep the atmosphere safe based on the space volume and contaminant levels.
03	evaluate_space_hazard	This tool classifies your workspace. It determines if a space qualifies as a Permit-Required Confined Space (PRCS) and identifies the primary hazards present.
04	generate_entry_roles_and_rescue	This tool builds your staffing plan. It defines the necessary entry roles and the specific rescue protocols required for the job.

See It in Action

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

U Is this tank a permit-required confined space? It has a tapering bottom and potential for engulfment.



The space is classified as a Permit-Required Confined Space (PRCS) due to the tapering geometry and engulfment hazard.

U What is the required ventilation for a 500 cubic meter space with a contaminant generation rate of 2?



The required airflow rate is calculated based on the volume and contaminant rate to maintain safe levels.

U What gases should I monitor in a space with known flammable vapors?



The monitoring protocol requires testing for oxygen levels, flammable gases, and specific toxic contaminants.

Frequently Asked Questions

01 Does this MCP follow OSHA standards?

Yes, the engine is built specifically around OSHA Permit-Required Confined Space (PRCS) standards.

02 Which AI clients can I use with this MCP?

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

03 Can it calculate ventilation requirements?

Yes, it calculates the necessary mechanical ventilation based on the space volume and contaminant generation rates.

04 How does it help with gas monitoring?

It determines the specific gases you need to monitor and how frequently you must perform tests.

05 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you, so it is ready to use immediately after connection.

06 How does this tool ensure OSHA compliance?

The engine is built directly upon the OSHA Permit-Required Confined Space (PRCS) standard, ensuring that hazard classification, monitoring, and rescue planning follow regulatory requirements.

07 Can I use this to determine if a space needs a permit?

Yes. By using the `evaluate\_space\_hazard` tool with specific space attributes and hazard profiles, the system will determine if the space qualifies as a Permit-Required Confined Space.

08 What happens if rescue equipment is not available on-site?

If you indicate that rescue equipment is not available, the `generate\_entry\_roles\_and\_rescue` tool will automatically set the rescue plan to 'External Emergency Response'.

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>"confined-space-entry-program": { "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

Confined Space Entry Program 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 Confined Space Entry Program. 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	Confined Space Entry Program MCP
Server ID	01a092f1-d2a8-724f-9612-3221a86663b8
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/confined-space-entry-program.