

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

Coverage Gap Map is an insurance MCP.

Match expenses against policy terms to find coverage gaps.

Coverage Gap Map connects your AI agent to insurance policy data. It lets your agent check specific expenses against policy clauses, limits, and exclusions. You can use it to monitor category caps, verify incident eligibility, and pull together final adjuster reports without manual cross-referencing.

A+ Quality Score 100/100

insurance

claims

policy

coverage

audit



SCAN TO VIEW

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.

Coverage Gap Map MCP

4 tools available

Cloud-hosted on Vinkius

You can stop manually hunting through policy documents to see if a claim fits. This MCP gives your AI client direct access to policy clauses and expense data. When you feed a list of expenses to your agent, it compares every line item against the specific limits and exclusions in the policy. It catches when a requested amount hits a category cap or when an incident falls under a specific exclusion. Instead of spending hours auditing claims, you let your agent do the heavy lifting of matching data points. It identifies exactly where a claim stands, which items are covered, and where the gaps are. This makes the transition from raw expense data to a finished adjuster report much faster.

Core Capabilities

01 — Expense Matching

Your agent compares individual line items to policy clauses.

02 — Limit Monitoring

The agent flags when requested amounts exceed category caps.

03 — Exclusion Checking

Your agent verifies if an incident is barred by policy language.

04 — Report Generation

The agent compiles findings into summaries for adjusters.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/coverage-gap-map — connect your AI agent in three steps.

- 01 Connect your AI client to the Coverage Gap Map MCP via Vinkius.
- 02 Provide your agent with the policy terms and expense data.
- 03 The agent uses the tools to match expenses, check limits, and verify exclusions.
- 04 The agent produces a summary or identifies a gap based on your request.

You connect your AI client to the Vinkius hosted MCP and start querying policy data.

Built For

Insurance professionals use this MCP to automate the tedious parts of claim auditing.

Claims Adjusters

They hand off expense lists to the agent to generate summary reports.

Insurance Auditors

They use the agent to find policy limit violations and coverage gaps.

Policy Underwriters

They use the tool to verify how specific incidents align with policy terms.

What Changes When You Connect

- 01 Automates the comparison between expense data and policy text.
- 02 Flags limit violations without manual calculation.
- 03 Identifies policy exclusions automatically.

04 Produces adjuster-ready summaries from raw data.

Real-World Applications

Claim Auditing

Verify that every expense submitted in a claim is actually covered by the policy.

Limit Enforcement

Check if a claimant is asking for more money than their category limits allow.

Eligibility Verification

Confirm an incident is not excluded before proceeding with a claim.

Adjuster Reporting

Turn a set of analyzed expenses into a clean summary for final review.

Patterns to Avoid

Manual Policy Auditing

❌ AVOID

An adjuster reads through fifty pages of policy text to manually check if a specific medical expense is covered.

✓ INSTEAD

Feed the expense list and policy text to your agent and use ``analyze_expense_coverage`` to find the matches instantly.

Ignoring Category Caps

❌ AVOID

A team approves a claim where the total requested amount for a specific category exceeds the policy limit.

✓ INSTEAD

Run ``identify_policy_limit_violations`` to catch when a claimant asks for more than their established caps allow.

Missing Exclusion Clauses

❌ AVOID

A claim is processed for an incident that the policy explicitly excludes, leading to a loss for the insurer.

✓ INSTEAD

Use ``validate_incident_eligibility`` to confirm the incident isn't barred by specific policy language before you proceed.

The Right Fit

Insurance professionals handling high volumes of claims should connect this MCP. If your team manually audits every single expense line item against policy documents, you need this. If you only handle a handful of simple claims per month, the manual process is likely fine.

Coverage Gap Map Toolset for Claims Analysis

These tools automate the comparison between expense line items and policy language to find coverage gaps.

#	TOOL	DESCRIPTION
01	analyze_expense_coverage	This tool checks if specific expenses are covered under the policy terms.
02	generate_claim_action_summary	This tool aggregates all findings into a high-level report for adjusters.
03	identify_policy_limit_violations	This tool monitors whether total requested amounts exceed established policy caps.
04	validate_incident_eligibility	This tool determines if a specific incident is excluded by the policy language.

See It in Action

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

- U** Analyze these expenses against the policy: items: [{ 'itemId': '1', 'description': 'Water damage repair', 'amount': 500}], policy: [{ 'clauseId': 'C1', 'clauseText': 'Covers water damage', 'type': 'coverage', 'limitAmount': 1000}], incident: 'Pipe burst in kitchen'.



The expense for water damage repair is covered under clause C1.

- U** Check if the total for 'Mitigation Cost' exceeds the limit of 500. Expenses: [{ 'itemId': '2', 'category': 'Mitigation Cost', 'amount': 600}].



The total requested amount of 600 for Mitigation Cost exceeds the limit of 500 by 100.

- U** Is a claim for 'Flood damage' eligible if the policy excludes 'Natural disasters'?



No, the claim is not eligible because flood damage falls under the natural disasters exclusion.

Frequently Asked Questions

01 What does this MCP do?

It connects your AI agent to insurance policy data to identify coverage gaps, limit violations, and eligibility issues.

02 Can I use this with Claude or Cursor?

Yes, you can use this with any MCP-compatible client like Claude, Cursor, or Windsurf.

03 How does it handle policy limits?

It uses the `identify_policy_limit_violations` tool to check if requested amounts exceed the caps set in the policy.

04 Does it help with claim summaries?

Yes, the `generate_claim_action_summary` tool aggregates all findings into a summary for adjusters.

05 Do I need to host this myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start working.

06 How does the tool identify coverage gaps?

The tool uses ``analyze_expense_coverage`` to compare expense descriptions against policy clauses and incident details to find mismatches or exclusions.

07 Can I check if I have exceeded my policy limits?

Yes, the ``identify_policy_limit_violations`` tool sums expenses by category and compares them against defined policy limits.

08 Does this tool handle incident exclusions?

Yes, ``validate_incident_eligibility`` checks the incident description against policy exclusions to determine if the claim is eligible.

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>"coverage-gap-map": { "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

Coverage Gap Map 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 Coverage Gap Map. 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	Coverage Gap Map MCP
Server ID	01a0e04d-8227-7268-8321-7a9c339821e3
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/coverage-gap-map.