

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

Claim Evidence Checklist MCP

Turn incident facts into organized, actionable evidence lists.

Claim Evidence Checklist MCP automates the heavy lifting of insurance claim processing. It analyzes incident details and policy requirements to build prioritized checklists, identify missing documentation, and verify if a claim is actually ready for a final decision. You can connect it to your AI client once and start managing claim workflows immediately.

A+ Quality Score 100/100

claims

insurance

evidence

checklist

workflow



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.

Claim Evidence Checklist MCP

4 tools available

Cloud-hosted on Vinkius

You can stop manually cross-referencing policy documents against incident reports. This MCP handles the comparison for you. When you feed incident facts and policy details into your AI client, the MCP identifies exactly what documentation is missing to satisfy the specific policy requirements. It doesn't just list items; it organizes them by urgency so you know what to chase first. You can use it to audit your current files to see if you have enough evidence to move to a decision phase, or you can use it to delegate tasks by grouping requirements by the person or department responsible. It turns a messy pile of claim data into a structured, prioritized roadmap for your adjusters and investigators.

Core Capabilities

01 — Gap Analysis

Your agent uses this to find missing documentation required by a specific policy.

02 — Urgency Sorting

The AI uses this to reorder checklists so you tackle the most critical evidence first.

03 — Readiness Audits

Your agent checks if the current file contains enough proof to finalize a claim decision.

04 — Task Delegation

The AI groups evidence requirements by the specific owner or department in charge.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/claim-evidence-checklist — connect your AI agent in three steps.

- 01 Connect the MCP to your preferred client like Claude or Cursor via Vinkius.
- 02 Provide the incident facts and policy details to your AI agent.
- 03 Ask the agent to identify missing evidence or check for sufficiency.
- 04 Use the agent to organize or delegate the resulting checklist.

Connect the MCP to your AI client and start managing claim requirements through natural language.

Built For

Insurance professionals who need to move claims through a structured pipeline without manual document auditing.

Claims Adjusters

They use the MCP to get clear, prioritized lists of what to collect for each file.

Claims Managers

They use the tool to verify if files are actually ready for final approval.

Insurance Investigators

They use the checklist to ensure all necessary proof is gathered before closing a case.

What Changes When You Connect

- 01 Reduces manual cross-referencing between incident reports and policy rules.
- 02 Identifies missing evidence before a claim hits a bottleneck.
- 03 Organizes tasks by owner to prevent duplicate requests.

04 Provides a clear signal when a claim is ready for a decision.

Real-World Applications

Automated Evidence Auditing

Run a check on a new claim to see immediately what documents are still outstanding.

Workflow Prioritization

Turn a long list of requirements into a prioritized task list for your team.

Decision Readiness Checks

Confirm a claim has sufficient evidence before presenting it for final settlement.

Departmental Task Assignment

Group required evidence by department to send clear instructions to different teams.

Patterns to Avoid

Manual policy cross-referencing

❌ AVOID

An adjuster spends hours reading through a 50-page policy to manually check if a specific incident report meets every requirement.

✓ INSTEAD

Feed the policy and incident details to your AI client and use ``get_required_evidence`` to instantly see what is missing.

Unorganized evidence lists

❌ AVOID

A claims manager receives a massive, unsorted list of missing documents and doesn't know which ones to request first.

✓ INSTEAD

Run the list through ``prioritize_checklist`` to organize the requirements by urgency so the team hits the most critical items first.

Premature decision making

❌ AVOID

A team moves a claim to the final settlement phase before realizing a key piece of proof is missing from the file.

✓ INSTEAD

Use ``validate_evidence_sufficiency`` to confirm the file actually has enough information to support a decision.

The Right Fit

Insurance professionals managing high-volume claims should connect this MCP to automate document auditing. Teams handling low-volume, simple claims with no policy complexity don't need it. The deciding factor is whether your current workflow relies on manual document comparison to move files forward.

Claim Evidence Checklist: 4 Specialized Tools

These tools automate the comparison between policy requirements and incident facts to identify missing documentation and prioritize tasks.

#	TOOL	DESCRIPTION
01	generate_owner_summary	This tool aggregates your checklist items by the specific person or department responsible for completing them.
02	prioritize_checklist	This tool takes your identified evidence list and organizes it into a logical, actionable order based on urgency.
03	get_required_evidence	This tool identifies exactly which pieces of evidence are missing or needed to satisfy a policy based on the specific incident details provided.
04	validate_evidence_sufficiency	This tool checks your current collection of records to determine if you have enough information to move a claim to the decision phase.

See It in Action

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

U What evidence do I need for this claim?



Based on the incident facts and policy, you need to collect the following: a police report, a repair estimate, and a signed claim form.

U Is the claim ready for a decision?



No, there are 2 high-priority items still missing: the medical report and the witness statement.

U Show me the tasks for the Adjuster.



The Adjuster has 3 tasks: verify the repair estimate, contact the claimant, and review the police report.

Frequently Asked Questions

01 How does this MCP help with insurance claims?

It automates the process of identifying, prioritizing, and validating the evidence needed to process a claim based on specific policy rules.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any compatible client including Claude, Cursor, and Windsurf.

03 How do I know if a claim is ready to be settled?

You can use the validation tool to check if your current collection of records is sufficient to move the claim to the decision phase.

04 Does this MCP host the data?

Vinkius hosts and manages the MCP, so you don't need to set up your own infrastructure to use these tools.

05 Can I assign tasks to specific people?

Yes, the tool can aggregate the evidence checklist by the person or department responsible for each item.

06 How do I identify what evidence is missing?

You can use the ``get_required_evidence`` tool by providing the incident facts, policy requirements, and any records you already have.

07 Can I see which person is responsible for each task?

Yes, the ``generate_owner_summary`` tool aggregates the checklist by owner so you can see exactly what each person needs to resolve.

08 How is the priority of evidence determined?

The ``prioritize_checklist`` tool sorts items based on their due date and their criticality to the claim's validity.

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>"claim-evidence-checklist": { "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

Claim Evidence Checklist 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 Claim Evidence Checklist. 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	Claim Evidence Checklist MCP
Server ID	01a0e04d-47e0-706e-b2d1-c787dc0d38d0
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/claim-evidence-checklist.