MCP SERVER | NO CODE | CLOUD HOSTED

# Business Interruption Claim Log MCP

## Turn disruption data into audit-ready insurance claim logs.

Business Interruption Claim Log MCP automates the forensic accounting needed to reconcile business closures with revenue and expense records. Your AI client uses this MCP to define indemnity windows, calculate lost income, and aggregate disruption costs into a single, actionable ledger for insurance purposes.

A+ Quality Score 100/100

forensic-accounting | insurance-claims | business-interruption | audit-log | revenue-reconciliation

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/business-interruption-claim-log

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.

**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.

**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.

**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 | Ed25519 | 24h TTL | V8 Isolate |
|---|---|---|---|
| Encryption at rest | PKI vault signatures | Ephemeral session keys | 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.

**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.

**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.

**06 — Honeytoken Trap System**

Phantom credentials are injected into isolated environments. If a honeytoken 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.

**Agent Activity**

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

**FinOps**

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

**Tool Health**

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

**Firewall & DLP**

PII redaction activity, sensitive data protection counters, and security event timeline.

**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.

# Business Interruption Claim Log MCP

4 tools available
Cloud-hosted on Vinkius

You can stop manually chasing spreadsheets to prove lost revenue. This MCP handles the heavy lifting of forensic accounting by connecting your business disruption data to insurance requirements. When a closure occurs, your AI client uses this MCP to pinpoint the exact indemnity window and compare what you expected to earn against what actually hit your bank account. It doesn't just stop at revenue; it also tracks the specific extra expenses you incurred because of the disruption. Once the math is done, the MCP organizes everything into a chronological audit trail. This ledger is ready for submission, complete with notes on any missing evidence you still need to collect. It turns a messy pile of disruption data into a structured, defensible claim.

## Core Capabilities

**01 — Indemnity Window Mapping**

Your agent uses this to match disruption dates against your insurance policy coverage.

**02 — Revenue Gap Analysis**

Your agent calculates the difference between projected earnings and actual income during a closure.

**03 — Expense Aggregation**

Your agent identifies specific costs that only occurred because of the business interruption.

**04 — Audit Trail Generation**

Your agent compiles all findings into a chronological ledger for insurance adjusters.

## One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/business-interruption-claim-log** — connect your AI agent in three steps.

01 Connect your preferred MCP-compatible client to Vinkius.

02 Provide your disruption dates and revenue data to your agent.

03 The agent uses the MCP tools to calculate gaps and extra expenses.

04 The agent generates a final, chronological claim log for your review.

The process moves from raw data to a finished ledger through your AI client.

## Built For

This MCP is built for professionals managing financial recovery after business disruptions.

**Forensic Accountants**

They hand off raw revenue and expense data to the AI to automate the reconciliation process.

**Insurance Adjusters**

They use the generated logs to verify the validity of business interruption claims.

**Business Owners**

They use the tools to quickly quantify their losses and prepare documentation for their insurers.

## What Changes When You Connect

01 Reduces manual math errors by automating revenue and expense reconciliation.

02 Shortens the time between a business disruption and a completed claim log.

| | |
|---|---|
| 03 | Creates a structured audit trail that follows insurance requirements. |
| 04 | Identifies missing evidence needed to finalize a claim. |

## Real-World Applications

**Natural Disaster Recovery**

Quantify lost revenue and extra costs following a storm or flood that forced a facility closure.

**Supply Chain Disruptions**

Calculate the financial impact when a vendor failure causes a temporary halt in production.

**Policy Compliance Audits**

Verify that a claim falls within the specific indemnity windows defined by an insurance policy.

**Expense Verification**

Isolate specific emergency costs from standard operating expenses to prove they are claimable.

## Patterns to Avoid

### Manual Spreadsheet Reconciliation

✗ AVOID

You try to manually compare every single bank transaction against your projected earnings in a massive Excel sheet. This leads to math errors and missed expense entries.

✓ INSTEAD

Let your agent handle the math. Use `reconcile_revenue_gap` to find the exact difference between expected and actual income automatically.

### Vague Claim Windows

✗ AVOID

You submit a claim based on a general idea of when the disruption happened without checking policy dates. This causes adjusters to reject the filing.

✓ INSTEAD

Use `get_claim_period_summary` to pin down the specific indemnity dates that match your insurance coverage.

### Mixing Standard and Extra Costs

AVOID

You include your regular monthly rent and utility bills in the claim for extra expenses. Adjusters will flag these as standard operating costs.

✓ INSTEAD

Use `calculate_extra_expenses` to isolate only the specific costs triggered by the disruption from your normal overhead.

## The Right Fit

Connect this MCP if you are a forensic accountant or business owner needing to turn messy disruption data into a defensible audit trail. Do not use this if you are just tracking routine daily sales. The decision depends on whether you have a specific business interruption event that requires insurance reimbursement.

# Business Interruption Claim Log Tools

These tools handle the heavy lifting of forensic accounting by reconciling revenue gaps and isolating extra expenses.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `generate_claim_log` | This tool pulls all your reconciled data into a final, actionable audit trail. It organizes your findings into a chronological ledger for submission. |
| 02 | `get_claim_period_summary` | This tool identifies the active window for a claim. It uses your business disruption events to set the specific dates for indemnity. |
| 03 | `reconcile_revenue_gap` | This tool calculates lost income. It compares your expected revenue against actual revenue to find the exact gap caused by the disruption. |
| 04 | `calculate_extra_expenses` | This tool finds and totals the specific costs you incurred due to the disruption. It isolates these extra expenses from your standard operating costs. |

# See It in Action

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

**U** Calculate the active claim period for a closure from 2024-01-01 to 2024-01-10 with a policy covering 2024-01-01 to 2024-01-15.

The active period is from 2024-01-01 to 2024-01-10, totaling 10 days of interruption within policy coverage.

**U** Compare expected revenue of 5000 against actual revenue of 3000 for the period 2024-02-01 to 2024-02-02.

The total revenue loss for the period is 2000.

**U** Identify extra expenses of 500 for equipment rental on 2024-03-01 with a policy limit of 1000.

Total extra expenses are 500, leaving a remaining policy capacity of 500.

# Frequently Asked Questions

01 **What does this MCP do?**

This MCP automates forensic accounting for business interruption claims. It calculates lost revenue, identifies extra expenses, and builds an audit log.

02 **Which AI clients can I use with this MCP?**

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

03 **How does it calculate lost revenue?**

It uses the reconcile_revenue_gap tool to compare your expected revenue against the actual revenue recorded during the disruption period.

04 **Can it help with insurance documentation?**

Yes. The generate_claim_log tool creates a chronological, actionable ledger designed to meet insurance audit requirements.

05 **Do I need to host the MCP myself?**

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

06 **How does the tool determine the claim period?**

The `get_claim_period_summary` tool calculates the intersection between the actual business closure dates and the policy's indemnity period.

07 **What is a collection action?**

A collection action is a specific instruction generated by `generate_claim_log` to retrieve missing evidence, such as a vendor receipt, needed to substantiate a claim entry.

08 **Can I use this with Claude Desktop?**

Yes, this MCP server can be connected to Claude Desktop, Cursor, VS Code, Windsurf, and any other MCP-compatible client via Vinkius Edge.

# 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 `"business-interruption-claim-log": { "url": "…" }` |
| Windsurf | MCP Settings → `mcp_settings.json` → 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

# Business Interruption Claim Log 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 Business Interruption Claim Log. 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 | Business Interruption Claim Log MCP |
| Server ID | `01a0e15c-29c9-7383-be68-271430efee09` |
| 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/business-interruption-claim-log.