MCP SERVER | NO CODE | CLOUD HOSTED

Defective Delivery Report MCP

Turn damaged shipment evidence into actionable claim strategies.

Defective Delivery Report MCP handles the heavy lifting of delivery disputes. It helps your agent document damage, preserve physical evidence, and determine if the fault lies with the carrier, the seller, or the product itself. You can use it to build structured reports and follow specific seller protocols to get your claims processed correctly.

A+ Quality Score 100/100

delivery | damage-report | logistics | claims | evidence

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · OCTOBER 2026
vinkius.com/en/ai-agent-connect/defective-delivery-report

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.

Defective Delivery Report MCP

4 tools available
Cloud-hosted on Vinkius

Dealing with damaged goods is a headache, especially when you have to prove who is actually at fault. This MCP gives your AI client the tools to manage the entire dispute process. Instead of guessing how to document a crushed box or a broken component, you can use this MCP to generate objective, factual reports that sellers can't easily ignore. It doesn't just describe the damage; it helps you protect your evidence by providing specific preservation instructions so your physical proof stays valid for a formal dispute. You can also stop wasting time on rejected claims by using the tool to build submission strategies tailored to a specific seller's rules. Whether you need to figure out if the carrier dropped the package or if the packaging was just insufficient, this MCP provides the logic to analyze liability factors and move your claim forward.

Core Capabilities

01 — Damage Documentation

Your agent creates structured reports that describe defects objectively.

02 — Evidence Protection

The AI provides instructions to ensure physical evidence remains valid for disputes.

03 — Liability Assessment

Your agent determines if the carrier, seller, or product is at fault.

04 — Claim Strategy

The tool builds custom submission guides based on specific seller requirements.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/defective-delivery-report** — connect your AI agent in three steps.

01 Connect your preferred MCP-compatible client to Vinkius.

02 Provide your agent with order details and evidence of the damage.

03 Run tools to generate reports, preservation plans, or liability analyses.

04 Follow the generated strategy to submit your claim to the seller.

Connect your AI client to Vinkius and start managing claims immediately.

Built For

This MCP is built for anyone managing e-commerce logistics and shipping disputes.

E-commerce Managers

Hand off the task of documenting damaged inventory and drafting claim reports to your agent.

Logistics Coordinators

Use the tool to analyze whether carriers or sellers are responsible for shipping errors.

Customer Support Teams

Let your agent follow specific seller protocols to resolve customer delivery issues quickly.

What Changes When You Connect

01 Reduces claim rejection rates by following seller-specific protocols.

02 Protects physical evidence through guided preservation plans.

03	Speeds up dispute resolution with structured, factual defect reports.
04	Removes guesswork from determining carrier or seller liability.

Real-World Applications

Damaged Shipment Claims

Generate a formal report when a customer receives a broken item.

Carrier Liability Disputes

Determine if a shipping company mishandled a package by analyzing the damage type.

Seller Protocol Compliance

Create a custom submission guide to match a specific retailer's claim process.

Evidence Management

Get instructions on how to handle a damaged item so it can be used in a formal dispute.

Patterns to Avoid

Vague damage descriptions

AVOID

You tell your agent the box arrived looking a bit beat up and the item inside is broken.

✓ INSTEAD

Use generate_defect_report to create a structured, factual account of the damage based on your specific order details.

Ignoring retailer rules

AVOID

You send a generic claim to a major retailer without checking their specific filing requirements first.

✓ INSTEAD

Run create_submission_strategy to build a guide that follows the exact protocols that specific seller requires.

Discarding damaged goods too early

AVOID

You throw away the crushed packaging before you have finished the dispute process.

✓ INSTEAD

Use create_preservation_plan to get a list of actions that keep your physical evidence valid for the claim.

The Right Fit

Connect this MCP if you manage e-commerce logistics or handle high volumes of shipping disputes. Do not connect it if you only ship small batches of goods where manual claims are easier. The deciding factor is whether your current claim rejection rate is high enough to justify automated, protocol-driven reporting.

Defective Delivery Report MCP Tools

These tools handle everything from documenting physical damage to building custom claim strategies for specific retailers.

#	TOOL	DESCRIPTION
01	`create_preservation_plan`	This tool generates a specific list of actions to keep your physical evidence valid for formal disputes.
02	`create_submission_strategy`	Use this to build a step-by-step guide for submitting claims based on a seller's specific protocols.
03	`generate_defect_report`	This tool creates a structured, factual description of product damage using your order details and evidence.
04	`analyze_liability_factors`	This tool evaluates whether the carrier, the seller, or the product itself is responsible for the damage.

See It in Action

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

U Generate a defect report for order #12345 where the box was crushed and the item inside is broken.

Defect Report ID: DR-98765. Summary: The external packaging was crushed upon arrival, resulting in a broken internal product component. Severity: High.

U How do I submit a claim for order #54321 via the web portal?

To submit your claim via the web portal for order #54321, follow these steps: 1. Log in to the seller's portal. 2. Navigate to 'My Orders'. 3. Select 'Report Issue'. 4. Upload the required photos and submit.

U Analyze liability for order #11223 where the packaging was intact but the product failed.

The likely fault party is the Seller or Product Quality, as the packaging remained intact while the product was damaged.

Frequently Asked Questions

01 **What can this MCP do for my e-commerce business?**

It helps you manage delivery disputes by generating defect reports, analyzing liability, and creating submission strategies for claims.

02 **How does the MCP help with evidence?**

It uses the create_preservation_plan tool to give you specific instructions on how to maintain physical evidence so it stays valid for a formal dispute.

03 **Can I use this with Claude or Cursor?**

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

04 **How does it determine who is at fault?**

The analyze_liability_factors tool evaluates the evidence to see if the fault lies with the carrier, the seller's packaging, or the product itself.

05 **Does it handle different seller requirements?**

Yes, the create_submission_strategy tool develops a step-by-step guide tailored to the specific protocols of a seller.

06 **How do I generate a formal report?**

Use the `generate_defect_report` tool with the order ID, damage photos, packaging notes, and a description of the defect.

07 **Can I find out who is responsible for the damage?**

Yes, the `analyze_liability_factors` tool evaluates whether the fault lies with the carrier, the seller, or the product.

08 **What should I do with the damaged packaging?**

Run the `create_preservation_plan` tool to get specific instructions on which items and packaging components you must keep to satisfy the seller's requirements.

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 `"defective-delivery-report": { "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

Defective Delivery Report 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 Defective Delivery Report. 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	October 2026
MCP Server	Defective Delivery Report MCP
Server ID	`01a0eb97-9eff-7365-92d1-03b5a42986db`
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/defective-delivery-report.