MCP SERVER | NO CODE | CLOUD HOSTED

Claro Antifraud (Open Gateway) MCP

Verify mobile line security and device location instantly.

Claro Antifraud (Open Gateway) provides direct access to the official Claro Brasil gateway. Your AI client uses this MCP to perform critical security checks like SIM swap detection, device location verification, and number recycling audits. It's built for risk agents and fintechs who need to validate the legitimacy of a mobile line before approving high-value actions.

A+ Quality Score 96.67/100

claro | sim-swap | account-takeover | antifraud | device-location | number-recycling

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/claro-antifraud-open-gateway

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.

Claro Antifraud (Open Gateway) MCP

7 tools available
Cloud-hosted on Vinkius

You can use this MCP to pull real-time security signals from the Claro Brasil network. Instead of guessing if a user is legitimate, your agent can check if a SIM card was swapped just minutes before a password reset attempt. You can also verify if a phone number has been recycled to a new owner, ensuring your customer database remains accurate. For location-based security, the MCP lets your agent confirm if a device is within a specific geographic radius or retrieve its last known cell-level position. This is essential for preventing account takeovers and validating physical presence during sensitive transactions. All authentication and token management happen in the background, so you just connect your client and start querying.

Core Capabilities

01 — Account Takeover Detection

Your agent identifies recent SIM swaps to block unauthorized password resets.

02 — Geofencing and Verification

The MCP confirms if a user's device is physically located within a required area.

03 — Database Hygiene

Your agent flags recycled phone numbers to prevent contacting the wrong individuals.

04 — Forensic Auditing

You retrieve exact timestamps of line changes to build detailed fraud investigation reports.

05 — Automated Authentication

The MCP handles OAuth token minting and refreshing automatically in the background.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/claro-antifraud-open-gateway** — connect your AI agent in three steps.

01 Register your application in the Claro Insight marketplace to get your credentials.

02 Connect your MCP-compatible client to Vinkius.

03 Provide your Client ID, Client Secret, and Customer ID to the MCP.

04 Your agent sends requests to tools like check_sim_swap or verify_device_location.

05 The MCP automatically handles OAuth token minting and header injection.

Connecting to this MCP gives your AI client immediate access to Claro's security tools.

Built For

This MCP is built for professionals managing digital risk and identity verification in the Brazilian market.

Antifraud Analysts

They use the tool to flag suspicious SIM swaps before approving high-value transactions.

Fintech Risk Engineers

They integrate these signals into automated onboarding flows to validate user identity.

Database Managers

They use number recycling checks to maintain the integrity of customer contact lists.

What Changes When You Connect

01 Direct access to official Claro Brasil gateway data.

02 Automated OAuth credential management and token refreshing.

03	Real-time signals for SIM swaps and device movements.
04	Reduced manual investigation time through precise forensic timestamps.

Real-World Applications

High-Value Transaction Security

An agent checks for recent SIM swaps before allowing a large bank transfer to proceed.

User Onboarding Validation

A fintech verifies that a phone number hasn't been recycled to a stranger during sign-up.

Delivery Verification

A logistics agent confirms a device is within a specific radius to validate a delivery attempt.

Account Recovery Protection

The system blocks password resets if the SIM card was changed within the last few hours.

7 Tools Available

#	TOOL	DESCRIPTION
01	`check_sim_swap`	Checks if a Claro number had a SIM card swap within a specified hour window. Use this to catch account takeover attempts during sensitive sessions.
02	`get_sim_swap_date`	Retrieves the exact timestamp of the last SIM change for a Claro number. This provides the forensic detail needed for fraud case reviews.
03	`get_line_change_alerts`	Monitors recent operational changes on a mobile line including SIM swaps, device changes, or subscription cancellations. It's a primary signal for detecting hijacked accounts.
04	`check_number_recycling`	Verifies if a phone number was reassigned to a new owner after a specific date. Use this to clean up stale contact lists and prevent sending data to the wrong person.
05	`verify_device_location`	Confirms if a device is located within a specific lat/long radius. This requires user consent under LGPD and works while the device is on the Claro data network.
06	`retrieve_device_location`	Fetches the last known location area and timestamp for a device on the Claro network. It provides a specific area rather than a simple yes/no verification.
07	`get_lbs_device_location`	Provides cell-level location data including coordinates and accuracy radius. This is a lightweight way to perform regional checks or asset monitoring.

See It in Action

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

U Has the SIM of +5511999999999 been swapped in the last 24 hours?

SIM Swap check for +5511999999999: The response shows the SIM was swapped within the 24-hour window, which is a high-risk signal for account takeover. I can also pull the exact timestamp using get_sim_swap_date if you need it for your records.

U Was the number 5521912345678 recycled since January 2025?

Number Recycling check for 5521912345678: This number was reassigned to a new owner after 2025-01-01. Any existing customer data tied to this number is likely outdated and belongs to a different person.

U Is the device of 5511974129777 within 5 km of -23.627, -46.655?

Device Location check for 5511974129777: The device is confirmed to be within the 5 km radius of the specified coordinates. Note that this check requires the device to be on the Claro network and requires LGPD consent.

Frequently Asked Questions

01 **How do I authenticate this MCP?**

You need to register an app in the Claro Insight marketplace to obtain a Client ID, Client Secret, and Customer ID. The MCP handles the OAuth token generation and automatic refreshing for you.

02 **Does device location tracking require user permission?**

Yes, all device location tools require user consent to comply with LGPD regulations.

03 **What happens if I get a 429 error during location checks?**

A 429 error means you have hit the per-MSISDN rate limit for the LBS service. You should slow down your requests for that specific number rather than retrying immediately.

04 **Can I check if a number was reassigned to someone else?**

Yes, the check_number_recycling tool allows you to verify if a number has been assigned to a new owner since a specific date.

05 **Which clients can I use with this MCP?**

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

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 `"claro-antifraud-open-gateway": { "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

Claro Antifraud (Open Gateway) 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 Claro Antifraud (Open Gateway). 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	Claro Antifraud (Open Gateway) MCP
Server ID	`01a08a8b-2a78-72ef-b504-ecff7f77de7b`
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/claro-antifraud-open-gateway.