

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

Claro Insight is a Brazil identity MCP.

Verify users and assess credit risk using carrier-grade data.

Claro Insight provides direct access to Claro Brasil's official API marketplace. Your agent can perform SIM tenure checks, GSMA KYC matching, and credit scoring via the Claro Score. It handles the OAuth authentication and token management automatically, letting you focus on building secure onboarding and antifraud workflows in Brazil.

A+ Quality Score 98.33/100

claro

kyc

identity-verification

credit-score

facial-biometrics

onboarding



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.

Claro Insight (Marketplace API Claro) MCP

7 tools available

Cloud-hosted on Vinkius

You can now give your AI agent direct access to Claro Brasil's carrier-grade identity and scoring suite. This MCP acts as a bridge to the official Claro Insight marketplace, allowing your agent to pull real-time data for identity verification, fraud prevention, and credit assessment. Instead of building complex OAuth flows for the GSMA Open Gateway suite, you connect this MCP to your client and start making calls immediately.

When you're building fintech apps or digital onboarding flows in Brazil, you need more than just basic data. This MCP lets your agent verify if a phone number actually belongs to a specific CPF, check if a user's address matches their mobile network footprint, and even pull credit scores for unbanked consumers. It's built for high-stakes automation where identity certainty is the priority. Whether you're running a KYC match to prevent account takeover or using facial biometric lookups to confirm a user's identity, this MCP handles the heavy lifting of communicating with Claro's infrastructure.

Core Capabilities

01 — Identity Verification

Your agent uses KYC tools to match user data against carrier records.

03 — Credit Assessment

Your agent pulls Claro Scores to evaluate creditworthiness for unbanked individuals.

05 — Biometric Validation

Your agent checks for existing facial biometrics to streamline identity workflows.

02 — Fraud Prevention

The agent checks SIM tenure and address proximity to flag high-risk users.

04 — Automated Onboarding

The agent uses KYC Fill-In to populate user profiles from carrier data.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/claro-insight-marketplace-api-claro — connect your AI agent in three steps.

- 01 Register your app in the Claro Insight marketplace to get credentials.
- 02 Connect the MCP to your AI client via Vinkius.
- 03 The MCP automatically handles OAuth token minting and refreshing.
- 04 Your agent calls specific tools to perform identity or credit checks.
- 05 The agent receives structured data to make real-time decisions.

Connecting to this MCP gives your agent immediate access to Claro's API suite.

Built For

This MCP is designed for organizations operating in Brazil that require high-assurance identity and credit data.

Fintech Developers

They hand off identity verification and credit scoring tasks to the agent.

Antifraud Analysts

They use the agent to run real-time checks on phone ownership and address proximity.

Product Managers

They implement automated onboarding flows that use carrier data to reduce friction.

What Changes When You Connect

- 01 Accesses official Claro Brasil carrier data directly.
- 02 Automates OAuth token management and refreshing.

03 Provides credit scoring for the unbanked population.

04 Reduces onboarding friction through automated data filling.

Real-World Applications

Digital Bank Onboarding

Use KYC Match and KYC Fill-In to verify new customers and populate their profiles instantly.

Account Takeover Prevention

Run `validate_phone` and `check_face_biometrics` to ensure the person accessing an account is the legitimate owner.

Credit Risk Triage

Apply Claro Score to new loan applicants to assess risk based on mobile payment history.

Delivery Verification

Use `validate_address` to ensure a customer's location matches their registered mobile footprint.

7 Tools Available

#	TOOL	DESCRIPTION
01	validate_phone	This tool checks if a specific CPF is the registered owner of a Claro mobile line. It helps you catch mis-typed numbers or borrowed lines during onboarding.
02	kyc_match	This tool compares user-provided identity data like name, birthdate, and ID against verified Claro records. It provides a per-field verdict to help identify fraud during account opening.
03	kyc_fill_in	This tool pulls authorized registration data like full name, CPF, and address directly from Claro records. You can use it to pre-fill onboarding forms and increase conversion rates.
04	validate_address	This tool uses antenna-proximity scoring to confirm if a CPF and phone number actually belong to a specific address. It's a reliable way to flag fake addresses in credit or delivery flows.
05	get_credit_score	This tool retrieves a Claro Score from 0 to 1000 based on actual payment behavior. It provides credit risk data even for consumers who are unbanked.
06	check_face_biometrics	This tool checks if a CPF has a registered facial biometric in the Claro database. You can use the result to decide whether to proceed with a face comparison or fall back to document checks.
07	get_sim_tenure	This tool checks how long a Claro Brasil number has been active and identifies the associated plan. It serves as a strong trust signal for assessing the risk of a new account.

See It in Action

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

Check how long the phone 5511999999999 has been a Claro customer



The tenure check for 5511999999999 shows the activation period on the Claro network and the current plan. This data can be used as a trust signal during onboarding.

Validate that CPF 12345678909 is the owner of the Claro line 5521987654321



The Valida Telefone check confirms whether CPF 12345678909 matches the registered owner of line 5521987654321. A mismatch indicates a borrowed or incorrect number.

Validate that CPF 12345678909 with name João da Silva and birthdate 1990-01-01 matches Claro records for +5511999999999



The KYC Match tool has compared the provided name, CPF, and birthdate against Claro's verified records for +5511999999999. The payload contains the per-field match verdict.

Frequently Asked Questions

01 How do I handle authentication for this MCP?

You need to register an app in the Claro Insight marketplace to get a Client ID and Client Secret. The MCP manages the OAuth client_credentials flow and token refreshes for you.

02 Do I need a Customer ID for all tools?

Some legacy customer APIs require a Customer ID in the header, which is an optional credential you can provide in this MCP.

03 What happens if a KYC match fails?

A failed field in a KYC match is a strong signal of identity fraud. If a response says a customer is not found, it means the data is not in the Claro base, not necessarily a mismatch.

04 Can this MCP score people without bank accounts?

Yes, the Claro Score is built from mobile payment behavior, allowing it to score unbanked consumers.

05 Is the data provided by this MCP official?

Yes, this MCP provides access to the official Claro Brasil API marketplace.

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>"claro-insight-marketplace-api-claro": { "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

Claro Insight (Marketplace API Claro) 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 Insight (Marketplace API Claro). 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 Insight (Marketplace API Claro) MCP
Server ID	01a08a8b-bcb5-7347-895b-ee3d3d128660
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/claro-insight-marketplace-api-claro.