MCP SERVER | NO CODE | CLOUD HOSTED

Adjust MCP for AI Agents

Measure mobile app installs and campaign performance attribution

Adjust MCP handles mobile measurement and attribution for your AI client. Connect it to track app installs, monitor key performance indicators, audit technical settings, and verify device attribution using natural conversation with agents like Claude or Cursor.

A+ Quality Score 100/100

mobile-attribution | app-analytics | kpi-tracking | event-measurement | campaign-optimization | data-auditing

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/adjust

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Adjust MCP

3 tools available
Cloud-hosted on Vinkius

When you connect this Adjust MCP, your AI agent turns complex growth data into simple conversations. Instead of logging into multiple dashboards to check if your campaigns are working, you just talk to your client. Your agent handles the heavy lifting—auditing technical app settings, checking attribution status for specific devices using their advertising IDs, and pulling performance reports like total installs or clicks.

It lets you see exactly which networks and campaigns deliver high-value users without leaving your chat window. This makes monitoring mobile growth data immediate and actionable. Since Vinkius hosts this MCP, all of your mobile measurement tools are available through one connection point, giving your agent access to a massive catalog of services.

It's about getting real numbers—like understanding what event tokens are active or reviewing last week's total sessions—and having that data delivered instantly. Your team gets immediate clarity on app performance.

Core Capabilities

01 — Audit App Configuration Settings

Retrieve and audit technical settings for your mobile applications, including event tokens and partner parameters.

02 — Verify Device Attribution Status

Check the attribution history of a specific device using its advertising ID (ADID) for support or testing.

03 — Generate Performance Reports

Pull aggregated performance metrics like total installs, clicks, and sessions, filterable by date ranges.

04 — Track Event Tokens

List active event tokens to verify that all in-app events are correctly set up for measurement.

05 — Identify Campaign Sources

Pinpoint which marketing networks and campaigns are driving the most valuable users directly from a chat conversation.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/adjust** — connect your AI agent in three steps.

01 Subscribe to this MCP on Vinkius.

02 Provide your Adjust API Token to connect the service.

03 Ask your AI client (Claude, Cursor, etc.) to run a specific report or check an app setting.

The bottom line is that you give your agent the access token, and it handles all the data calls and reporting for you.

Built For

This MCP targets anyone responsible for mobile growth and campaign performance. It's essential for User Acquisition Managers who need instant attribution data, Mobile Developers needing to test event configurations, and Growth Analysts running daily ROI audits.

User Acquisition (UA) Manager

Monitoring how different campaigns are performing in real-time and identifying which source networks bring the highest quality users.

Mobile Developer

Running integration tests by verifying that specific device IDs correctly attribute installs or checking if an event token is configured right before a release.

Growth Analyst

Pulling weekly KPI reports (installs, sessions) to analyze trends and prepare data for board-level ROI presentations.

What Changes When You Connect

01 Get immediate visibility into campaign success. Instead of sifting through complex backend reports, your agent tells you which networks are driving the most valuable users instantly.

02 Eliminate manual data checks. Use `inspect_device` to quickly verify a device's attribution status using just its ADID for support or QA testing.

03 Streamline performance tracking. Pull aggregated KPI metrics with `get_kpi_report`, filtering by date ranges to compare weekly growth trends effortlessly.

04 Ensure development accuracy. Run `get_app_settings` to audit technical event tokens and partner parameters, ensuring your app tracks data correctly before a launch.

05 Keep documentation current. Audit all active event tokens and configurations through the MCP, making sure no critical in-app events are missed.

Real-World Applications

Diagnosing sudden performance dips

A UA Manager notices a drop in installs on Tuesday. They ask their agent to run `get_kpi_report` for the last 30 days, immediately spotting that the decline started after a specific partner was added. This pinpoints the failure source instantly.

Support tickets requiring attribution checks

A customer support agent receives a ticket asking about a user's install path. They use `inspect_device` with the provided ADID, and the agent returns the exact campaign name and source network that brought the user in.

Pre-launch QA validation

A Mobile Developer needs to confirm a new feature's tracking. They use `get_app_settings` to audit event tokens, verifying that the new 'checkout complete' event is correctly listed before pushing code.

Quarterly ROI analysis

A Growth Analyst needs historical context. They instruct their agent to run a filtered `get_kpi_report` for Q1, allowing them to build a precise comparison of sessions and clicks against previous quarters.

Patterns to Avoid

Comparing data across tools

✗ AVOID

Manually running reports in the Adjust web console, then copying those numbers into Google Sheets, and cross-referencing them with a separate analytics platform.

✓ INSTEAD

Use the MCP to get all necessary metrics (like installs and sessions) via `get_kpi_report` and feed that data directly to your agent. The agent consolidates it for you.

Guessing app configuration

✗ AVOID

Assuming an event token is active because the dev team said so, but failing to verify if it's properly configured or live in the current build.

✓ INSTEAD

Always run `get_app_settings` first. This confirms exactly what tokens and parameters are currently audited and available for use.

Relying on memory during support

✗ AVOID

Telling a client, 'I think they came from Google Ads,' without any proof or source attribution data to back up the claim.

✓ INSTEAD

Use `inspect_device` with the ADID. The MCP provides documented attribution status, showing exactly which network and campaign is responsible for that device.

The Right Fit

You should use this Adjust MCP if your primary problem is tracking *why* a user installed an app or what specific actions they took inside it. If you need to audit event tokens, verify ad attribution, or pull historical KPI metrics by date, this is the tool for you. Don't use it if all you need is simple session counting without knowing the campaign source; in that case, basic web logging tools might suffice. Crucially, never rely on manual data entry when checking device history; always run `inspect_device` to get accurate attribution status.

Adjust MCP for AI Agents: Solving Mobile App Attribution Pain

Today, tracking mobile growth is a nightmare. You jump between ad platforms, internal dashboards, and analytics tools just to answer one question: where did the user come from? You spend hours piecing together data points—some are tokens, some are campaign names, and most of it requires manual cross-referencing.

With this MCP, your agent handles the entire process. Instead of clicking through five different tabs or copy/pasting IDs, you ask a question like, 'What did my latest ad spend generate?' The system runs `get_kpi_report` and gives you an instant, synthesized answer, showing total installs and clicks in one go.

Adjust MCP for AI Agents: Validating Event Tracking Accuracy

Manually verifying event tokens is tedious. You have to check configuration files, ask the dev team if a token is active, and then manually confirm it hasn't expired or been changed on another platform.

Now, you simply prompt your agent to run `get_app_settings`. It delivers an audited list of all active event tokens and partner parameters. You get immediate confirmation that your tracking setup is accurate for launch day.

3 Tools: App Analytics & KPI Tracking with Adjust

These tools let you retrieve app settings, check device attribution status, and pull filtered performance reports using natural language commands.

#	TOOL	DESCRIPTION
01	`get_app_settings`	Retrieves the current technical configuration of your mobile application, including active event tokens and partner details.
02	`inspect_device`	Verifies what campaigns or networks are attributed to a specific device using its unique advertising ID (ADID).
03	`get_kpi_report`	Pulls aggregated performance reports for key metrics like total installs, clicks, and sessions, allowing you to filter by date.

See It in Action

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

U What were the total installs last week compared to the one before?

KPI Report: Installs & Sessions

- **Last Week:** 15,400 total installs (Source breakdown below)
- **Previous Week:** 13,200 total installs
- **Change:** +8% increase in installs.

The primary driver was the 'Summer Campaign' on Google Ads. You can see a detailed platform breakdown if needed.

U Check the attribution for this ADID: 12345-67890.

Device Attribution Status

- **ADID:** `12345-67890`
- **Source Campaign:** Summer Campaign (Google Ads)
- **Attribution Window:** 7 Days
- **Last Seen:** 2 hours ago

This device is healthy and properly attributed to a high-value campaign. Great to know.

U List all active event tokens for the app.

✅ **App Event Token Audit**

The system found 6 active, configured tokens:

- `event_purchase`: Status: Active | Window: 30 days
- `event_login`: Status: Active | Window: 7 days
- `event_signup`: Status: Active | Window: 14 days
- ... and 3 others.

The `get_app_settings` report confirms all parameters are currently set.

Frequently Asked Questions

01 **How can I use the Adjust MCP to track user campaign sources?**

You can check device attribution status using an ADID. The agent tells you exactly which network or campaign is credited with bringing that specific user into your app, providing immediate clarity for support tickets.

02 **Does Adjust MCP help me audit my mobile event tokens?**

Yes. You can run a full audit of your application's technical settings to list all active event tokens and verify that every crucial in-app action is correctly configured for tracking.

03 **Can I get weekly reports on app installs using the Adjust MCP?**

Absolutely. You can pull aggregated KPI reports, filtering by date ranges to easily compare total installs, clicks, and sessions week over week for growth analysis.

04 **What if a device's attribution status is unclear?**

The MCP allows you to inspect the device directly. It provides documentation on which campaigns are currently attributed to that specific advertising ID, helping you resolve confusion quickly.

05 **Is Adjust MCP better than using the native reporting dashboard?**

It's faster and more conversational. Instead of clicking through multiple tabs in a dashboard, you ask your agent a question—like 'Show me total installs for last month'—and get an immediate, summarized answer.

06 **Does the Adjust MCP help with app development QA?**

Yes. Developers use it to confirm that event configurations are correct via `get_app_settings`, guaranteeing that new features track data properly before going live.

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 `"adjust": { "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

Adjust 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 Adjust. 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	June 2026
MCP Server	Adjust MCP
Server ID	`019d7547-6057-72fc-8e2f-21684fc81528`
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/mcp/adjust.