MCP SERVER | NO CODE | CLOUD HOSTED

Airship MCP for AI Agents

Manage Multi-Channel Communication and User Segmentation Data

Airship connects mobile and web engagement orchestration tools to your AI agent. This MCP lets you manage push notifications, audit subscriber segments, and map user devices across multiple channels using natural conversation. It turns complex multi-channel communication strategy into simple chat commands.

F Quality Score 3.6/100

mobile-engagement | push-notifications | omnichannel | customer-segmentation | user-retention | mobile-marketing

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

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.

Airship MCP

10 tools available
Cloud-hosted on Vinkius

You need to run a massive campaign that hits users across iOS, Android, and web, but managing all those touchpoints manually is a nightmare of dashboards and API calls. This MCP connects your Airship account directly to your AI agent, letting you handle multi-channel communication strategy through conversation.

Instead of logging into three different consoles to send alerts or check delivery status, you just ask your agent. You can tell it to trigger targeted push notifications for a specific group, audit the criteria behind an audience segment, or even see which devices are linked to a single customer profile. This gives you total control over your entire user lifecycle—from initial segmentation research to final delivery confirmation. When you connect this through Vinkius, all those complex communication tools become accessible via one simple interface for your AI agent.

Core Capabilities

01 — Send Targeted Push Alerts

Trigger a push notification message instantly to specific user groups, segments, or the entire audience.

02 — Audit Audience Segments

List and review the exact criteria—tags and attributes—that define your existing audience segments.

03 — Map User Devices to Profiles

Manage named users, linking multiple devices (like an iPhone and a web browser) back to one single customer account.

04 — Check Channel Metadata

List all active communication channels—iOS, Android, Web, Email—and retrieve technical details for each one.

05 — Monitor Delivery Status

Get a quick report on whether recent push notifications were successfully delivered to the target devices.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Airship App Key, Master Secret, and Region (US or EU) credentials.

02 Your agent uses these credentials to connect directly to the Airship platform's data sources.

03 You then issue natural language commands—like 'Send a sale alert to premium users'—and the agent executes the multi-step process using the necessary tools.

The bottom line is, your AI client handles all the secure authentication and complex API calls so you only have to talk conversationally to get things done.

Built For

This MCP is essential for Marketing Managers who manage multi-channel campaigns. It solves the pain of having to jump between segmentation tools, push platforms, and analytics dashboards just to run a simple campaign.

Marketing Manager

Runs high-priority push sends; they use this to send alerts to specific segments or check delivery status after a blast.

Product Owner

Audits channel configurations and verifies user associations, making sure all devices (iOS/Android) are mapped correctly to the right customer profile.

Growth Specialist

Researches segment criteria for new campaigns, managing multi-channel tags to execute precise lifecycle marketing funnels.

What Changes When You Connect

01 Run complex campaigns without leaving your chat interface. Instead of jumping between dashboards to send a targeted push notification, just ask the agent to execute it.

02 Understand exactly who you're talking to. You can use the `get_segment_details` tool to instantly audit segment criteria, ensuring your audience lists are accurate before launching any campaign.

03 Maintain clean customer records. Use the `associate_named_user` tool to map every device—whether it's an Android tablet or a web browser—to one consistent user profile.

04 Confirm delivery success immediately. After running a large push notification, use `get_push_status` to quickly confirm if the message was delivered across all intended channels.

05 Audit your tech stack on demand. You can list and check details for every communication channel (`list_channels` , `get_channel_details`) without needing to navigate complex platform menus.

Real-World Applications

Auditing Device Consistency After a Product Launch

A product owner needs to verify that all new users are correctly mapped across platforms. They ask their agent, 'Show me the details for this user's channels.' The agent uses `get_channel_details` and `list_named_users`, confirming that both the iOS app and web browser are linked to the single customer profile.

Launching a Time-Sensitive Sale Campaign

A marketing manager needs to hit high-value subscribers immediately. They prompt their agent, 'Send an urgent sale alert only to users tagged 'Premium' and who haven't logged in for 7 days.' The agent coordinates the `send_push_notification` using specific segment criteria.

Researching Segment Requirements

A growth specialist needs to build a new lifecycle campaign. They ask, 'What are the criteria behind our current 'High Potential' group?' The agent uses `get_segment_details` and `list_tags`, giving them the precise data structure needed for their next marketing push.

Verifying Static List Compliance

An operations lead is worried about outdated user lists. They ask, 'List all static audiences we maintain.' The agent uses `list_static_lists` to provide an inventory, letting the lead quickly verify if any old campaigns are still pointing to unmaintained groups.

Patterns to Avoid

Sending a notification without checking eligibility

✗ AVOID

Manually sending a push alert to 'all users' when you really only wanted to target people who opened the app last week. This wastes credits and annoys the whole base.

✓ INSTEAD

Don't just send it blindly. First, ask your agent to use `get_segment_details` on the specific segment (e.g., 'Opened App Last 7 Days'). Then, run the notification using `send_push_notification` against that precise group.

Assuming device linkage is automatic

✗ AVOID

A user sees an email alert but assumes their web session will also get it. If they haven't linked their accounts, the message fails on one channel.

✓ INSTEAD

Before running a campaign, check your setup. Use `list_named_users` and then run `associate_named_user` to explicitly link all relevant devices to that single user profile.

Ignoring which channels are active

✗ AVOID

Writing code to send a message to an unsupported channel type (like an old OS version) because you forgot to check its status.

✓ INSTEAD

Always start by calling `list_channels`. This ensures your agent knows exactly which communication methods—iOS, Android, Web—are active and ready for deployment.

The Right Fit

Use this Airship MCP if your primary pain point is complexity across multiple messaging channels. If you run campaigns that rely on combining audience segmentation (who the user is) with specific device data (what they use), this is what you need. You'll gain immediate conversational access to tools like `send_push_notification`, `list_segments`, and `get_push_status`. However, don't connect it if your needs are limited only to basic, single-channel email blasts that don't depend on user device mapping or segment auditing; a simpler messaging connector might suffice. This MCP is for sophisticated, multi-touchpoint customer journeys.

Airship MCP: Managing Multi-Channel Messaging Campaigns

Today, launching a proper campaign means jumping between at least three systems: the segmentation tool to define your audience; the push platform to write and send the message; and a separate analytics dashboard just to see if it landed correctly. This copy-paste mess makes coordinating urgency nearly impossible.

With this MCP, you talk to your agent like talking to an employee who knows all the systems. You ask for a segment audit, get the data, confirm the channel details, and then trigger the push notification—all without leaving your chat window.

Airship MCP: Auditing User Segmentation and Device Data

Manually verifying user associations is a deep dive into multiple internal dashboards. You have to check if the web tag matches the app's device ID, which takes hours of cross-referencing.

Now, you simply prompt your agent. It pulls all necessary data by calling tools like `list_named_users` and `associate_named_user`, giving you a consolidated view that tells you exactly where every user is represented.

Airship: 10 Tools for Audience Segmentation and Push Notifications

Use these tools to send alerts, audit audience groups, map devices, and check the delivery status of your mobile marketing campaigns.

#	TOOL	DESCRIPTION
01	`send_push_notification`	Sends a push alert message out to the targeted audience.
02	`list_segments`	Retrieves a list of all existing audience segments defined in your account.
03	`get_segment_details`	Pulls the specific criteria—the tags and attributes—used to build a chosen segment.
04	`list_named_users`	Displays a list of all named users set up in your system.
05	`associate_named_user`	Links a specific device (like an iPhone or Android) to a known customer profile.
06	`list_channels`	Lists all available communication channels, such as iOS, Android, and Web.
07	`get_channel_details`	Retrieves technical details about a specific device or channel type.
08	`list_static_lists`	Lists pre-defined static audience groups, often created from CSV uploads.
09	`list_tags`	Shows all the custom tags available to categorize your audience members.
10	`get_push_status`	Checks the delivery status and success rate of recent push notifications sent out.

See It in Action

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

U Send an urgent push alert to everyone who hasn't opened the app in 30 days. The message should be 'We miss you! Check out our new features.'

✅ **Push Notification Triggered**

- **Target Segment:** Inactive Users (Last 30 Days)
- **Status:** Scheduled
- **Channels Affected:** iOS, Android, Web
- **Operation ID:** ABC-9876

A delivery status report is pending. I recommend checking the `get_push_status` tool in about 5 minutes to confirm successful distribution.

U What are the criteria for our 'Platinum Tier' segment? Also, list all active channels.

📈 **Segment & Channel Audit**

Segment Details: Platinum Tier

- `Membership Level`: Platinum
- `Total Spend`: > $1000
- `Last Purchase Date`: Within 90 days

Active Channels:

- 📱 iOS (Metadata: Version 17, Registered: Yes)
- 🤖 Android (Metadata: Build 34, Registered: Yes)
- 🌐 Web (Metadata: Browser type, Last Active: Today)

U Map my laptop and phone to the same account. My devices are listed as 'laptop-xyz' and 'phone-abc'.

User Profile Update

The two devices have been successfully linked to a single user profile.

- **User ID:** U12345678
- **Associated Devices:** [laptop-xyz, phone-abc]
- **Tags Added:** 'Multi-Device User'

You can now send communications that target the user, regardless of which device they open it on.

Frequently Asked Questions

01 **How do I use Airship MCP to manage my multi-channel push campaigns?**

You simply ask your agent. Instead of manually navigating the platform, you tell the system what message to send and who needs to receive it across iOS, Android, or web. The agent handles the complex orchestration.

02 **Can Airship MCP help me check if my audience segments are accurate?**

Yes. You can ask the agent to pull segment details using criteria and tags. This confirms that your target groups—like 'Premium Subscribers'—are built using the exact rules you intended.

03 **What is the best way to link my physical devices to a single user profile?**

You use the MCP to map named users. This process links multiple specific devices (like your phone and tablet) back to one consistent customer record, ensuring all messages hit the right person.

04 **If I run a push notification, how do I know if it actually got delivered?**

The MCP lets you check delivery status. You ask for a report on recent sends, and the agent provides a clear audit showing which channels received the message and whether they were successful.

05 **Does Airship MCP help me find out what tags I have available?**

Absolutely. You can request a list of all current audience tags and attributes, giving you an immediate inventory of how your customers are segmented within the platform.

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 `"airship": { "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

Airship 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 Airship. 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	Airship MCP
Server ID	`019d754b-486d-70c2-bdf8-acc6ec11fe84`
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/airship.

© 2026 Vinkius · vinkius.com · support@vinkius.com