MCP SERVER | NO CODE | CLOUD HOSTED

Huawei Push Kit MCP

Send Targeted Alerts to HMS Devices

Huawei Push Kit / 华为推送服务 lets your AI agent manage all device notifications for the Huawei Mobile Services (HMS) ecosystem. You can send targeted alerts to unique devices, broadcast messages to large topic groups, or create specific notification flows based on complex user criteria—all by talking to your agent.

A+ Quality Score 100/100

push-notifications | mobile-engagement | hms-ecosystem | message-orchestration | targeted-messaging | real-time-alerts

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/huawei-push-kit

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.

Huawei Push Kit / 华为推送服务 MCP

6 tools available
Cloud-hosted on Vinkius

Managing device communication used to mean navigating massive developer consoles and writing complex API calls just to send a simple alert. This MCP changes that. It connects the full power of Huawei Push Kit directly to your AI client, letting you handle everything from basic announcements to highly specific user targeting through natural conversation. Instead of logging into AppGallery Connect, telling your agent what needs to happen—like sending an update only to users who are subscribed to both 'sales' and 'beta' topics—is enough. Your agent acts as a real-time push coordinator for your whole business. You can manage subscriptions by checking which topics devices follow or even adding new ones using the `subscribe_to_topic` tool. Whether you need to send an immediate alert to a single user via `push_to_token`, broadcast a global update with `push_to_topic`, or execute complex targeting logic with `push_to_condition`, all those actions are available from one, authorized source through Vinkius.

Core Capabilities

01 — Send messages to single devices

Deliver a push notification directly to a unique device token.

02 — Broadcast updates by topic

Push the same message out simultaneously to all subscribers of a specific content topic.

03 — Target messages with conditions

Send notifications only if devices match multiple, complex criteria defined by topics.

04 — Manage device subscriptions

Add or remove specific content topics from a device's list of interests.

05 — Verify system connectivity

Check if your App ID and connection gateways are working correctly, helping you troubleshoot alerts before deployment.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/huawei-push-kit** — connect your AI agent in three steps.

01 Subscribe to this MCP in Vinkius and provide your Huawei HMS App ID and App Secret.

02 Connect the MCP to your preferred AI client (like Cursor or Claude).

03 Use natural language instructions, like 'Send an alert for X topic' or 'List topics for token Y', to trigger the desired action.

The bottom line is you manage complex device communications using plain English prompts instead of developer console clicks and API code.

Built For

This MCP serves marketing managers who need to launch timely, targeted campaigns without waiting for dev resources. It's also perfect for backend engineers who want to automate system alerts or DevOps teams needing instant push delivery confirmation.

Marketing Manager

Launching a flash sale requires sending an alert only to users subscribed to 'discounts' and located in the 'west_region', which they can specify via topic conditions.

Backend Engineer

Automating system status updates, like notifying all devices that a new API endpoint is live, using `push_to_topic` to hit an 'all_users' group.

DevOps Specialist

Running diagnostic checks to validate token formats or confirm that the connection status of the push gateway is active before a major release.

What Changes When You Connect

01 Targeted messaging gets you precise results. Instead of blasting everyone, you can use `push_to_token` to send an alert only to a single user's device.

02 Mass communication is simple too. To reach all users interested in system updates, just prompt your agent to use the `push_to_topic` tool on a known group topic.

03 Complex logic becomes conversational. Use `push_to_condition` to send messages that only fire when devices meet specific criteria, like 'Topic A' AND 'Topic B'.

04 Managing user interest is easy. Need to stop sending alerts? Prompt the agent to use `unsubscribe_from_topic`. Want them interested in something new? Use `subscribe_to_topic`.

05 You gain full operational visibility. The MCP lets you run diagnostics and check token validity, saving time previously spent debugging connectivity issues.

Real-World Applications

The product launch announcement

A marketing team needs to tell 50,000 users about a new feature. They ask their agent to 'Broadcast the release notes to all active beta testers.' The agent uses `push_to_topic` on the designated 'beta_testers' topic, ensuring rapid, reliable delivery without manual API calls.

The abandoned cart reminder

An e-commerce backend needs to remind a specific user who left items in their cart. They prompt the agent: 'Send an alert to token XYZ about the cart.' The agent executes `push_to_token`, ensuring the message hits that single, critical device immediately.

The regional sales promotion

A sales team only wants to promote a deal in Europe. They ask their agent to 'Send an alert for discounts, but only to users subscribed to both 'discounts' and 'europe_region'.' The agent uses `push_to_condition`, guaranteeing the message reaches the right segment.

The content cleanup

A developer needs to remove old topics because they are no longer relevant. They prompt: 'Remove the 'old_guide' topic from all tokens.' The agent executes `unsubscribe_from_topic`, maintaining clean, accurate device subscriptions.

Patterns to Avoid

Assuming a message reached everyone

✗ AVOID

Running a mass alert and assuming that every single user gets it because the API call succeeded. The message might fail for specific tokens.

✓ INSTEAD

After running `push_to_topic`, follow up by asking your agent to run diagnostic checks or use `list_topic_subscriptions` on known tokens to confirm device status.

Targeting based only on one topic

✗ AVOID

Sending a message that should only go out during sale events, but it goes out anytime because you didn't specify multiple criteria.

✓ INSTEAD

Always use `push_to_condition` when your target audience requires matching two or more specific topics (e.g., 'sale' AND 'premium').

Forgetting credentials

✗ AVOID

Trying to run any push command without properly providing the required App ID and Secret keys.

✓ INSTEAD

Remember that you must first subscribe the MCP in Vinkius with your specific Huawei HMS App ID and App Secret before running any tool.

The Right Fit

Use this MCP if your core problem is *real-time, push-based communication* to devices within the Huawei Mobile Services ecosystem. This is for alerts, timely reminders, or immediate system updates where the user must be notified on their phone right now. Don't use it if you need complex data storage, like managing customer profiles; those belong with database tools. Also, don't rely solely on this MCP for internal chat communication; that needs a dedicated messaging tool. If your goal is simply to retrieve historical log files or general analytics, look for a logging or reporting-type MCP instead.

Managing device alerts used to be a console nightmare.

Before this MCP, sending out an alert meant jumping into the AppGallery Connect portal. You'd spend time figuring out which specific topic IDs were active, manually checking if your token list was correct, and then building a complex request just to hit 'send.' It required multiple clicks and deep knowledge of the HMS structure.

Now, you just tell your agent what you want done. Need to update 50,000 users? You say, 'Broadcast this announcement.' Done. The entire process—from targeting logic to sending the alert—happens in a single conversation. It cuts out all the clunky manual steps.

Huawei Push Kit / 华为推送服务 MCP Gives You True Communication Control

The biggest time sink was figuring out how to combine targeting rules. Did I need a single topic push, or did I need the complex logic that only triggers when 'Topic X' is active AND 'Topic Y' is also active? Writing these boolean conditions used to take hours of API testing.

Now you simply ask your agent: 'Send this message if both topics are true.' The MCP handles the complexity behind the scenes. You get precise, reliable push delivery without ever needing to write a condition string or touch a console.

Huawei Push Kit / 华为推送服务: 6 Tools

These tools give you granular control over every aspect of your device communication, allowing you to subscribe users, send alerts, and verify status all through conversation.

#	TOOL	DESCRIPTION
01	`list_topic_subscriptions`	Retrieves and lists all content topics that a specific device is currently registered to receive updates from.
02	`push_to_condition`	Sends an alert only if the target device matches complex criteria based on multiple subscribed topics.
03	`push_to_token`	Delivers a direct, high-priority message to one specific device using its unique token identifier.
04	`push_to_topic`	Sends an update simultaneously to every single device currently subscribed to a named content topic.
05	`subscribe_to_topic`	Adds a new interest topic for a device, ensuring it receives future messages related to that subject matter.
06	`unsubscribe_from_topic`	Removes a specific content topic from a device's subscriptions, stopping all future alerts on that subject.

See It in Action

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

U Send a push notification to token 'ABCD...1234' with title 'Good Morning' and body 'Don't forget your tasks today'.

I've successfully sent the notification to the device token. The Huawei request ID is `1234567890`. Should I also send this update to your global announcement topic?

U Broadcast a system update notification to the 'all_users' topic for version '2.5.0'.

I've initiated the broadcast to all devices subscribed to the `all_users` topic. The message 'Version 2.5.0 is now ready for download' has been successfully submitted to Huawei Push Kit. Would you like me to monitor the delivery status?

U Check the connectivity status of our Huawei Push and OAuth gateways.

I've performed a diagnostic check. Both the Huawei OAuth authentication gateway and the Push Kit API are responding normally. Your App ID is correctly configured. Is there anything else you'd like to audit?

Frequently Asked Questions

01 **How do I send an alert using Huawei Push Kit / 华为推送服务 MCP?**

You simply prompt your agent with the details, such as 'Send a message to token XYZ.' The agent handles connecting and sending the push notification for you.

02 **Can I use Huawei Push Kit / 华为推送服务 MCP for mass marketing?**

Yes. You can use `push_to_topic` to broadcast updates to large groups of subscribers, making it ideal for global campaigns or product announcements.

03 **Does Huawei Push Kit / 华为推送服务 MCP support complex targeting?**

Absolutely. Use the `push_to_condition` tool to target devices that satisfy multiple topic requirements simultaneously (e.g., users in both 'premium' and 'europe').

04 **What is the difference between push_to_token and push_to_topic?**

Sending via `push_to_token` targets one specific device directly, guaranteeing a personal alert. Sending via `push_to_topic` hits every device subscribed to that general topic.

05 **How do I check if my tokens are valid?**

You can use the MCP's diagnostic capabilities or prompt your agent to validate token formats and check overall API connectivity status, ensuring your alerts won't fail unexpectedly.

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 `"huawei-push-kit": { "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

Huawei Push Kit / 华为推送服务 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 Huawei Push Kit / 华为推送服务. 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	Huawei Push Kit / 华为推送服务 MCP
Server ID	`019d8446-c807-7392-ace7-ee351a64e631`
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/huawei-push-kit.