MCP SERVER | NO CODE | CLOUD HOSTED

Bandwidth MCP for AI Agents

Managing 10DLC Campaigns and High-Volume Messaging

Bandwidth connects your cloud communications stack directly to any AI agent. You manage SMS and MMS campaigns, validate 10DLC profiles, check toll-free number compliance, and audit message histories—all through natural conversation. Forget building complex webhook architectures; simply ask your agent to run the telecom operations you need.

A+ Quality Score 100/100

cpaas | sms-api | mms-messaging | 10dlc | telecom-automation | carrier-grade

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

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.

Bandwidth MCP

10 tools available
Cloud-hosted on Vinkius

This connector lets your AI client take full control of high-volume communication workflows without requiring you to write custom code or build complicated webhooks. You can manage everything from initial messaging blasts, sending both standard SMS and rich media MMS payloads, to validating entire 10DLC campaigns for carrier approval. Need to know if a toll-free number is compliant? Ask your agent to ping the verification headers. The system also lets you audit all message histories or clear out old media files when you're done with them. Because this MCP sits within the Vinkius catalog, you get access to reliable telecom infrastructure management right alongside hundreds of other operational tools for your AI agents.

Core Capabilities

01 — Send bulk SMS and MMS messages

Dispatch text alerts or rich media messages instantly to specific phone numbers.

02 — Manage 10DLC campaign compliance

Check the health of your messaging campaigns and validate required profiling data for carrier approval.

03 — Verify toll-free number status

Run checks on upstream headers to ensure your dedicated toll-free numbers are compliant before sending messages.

04 — Audit messaging activity and media storage

Review message logs, check API health, or delete stored media payloads from the system.

One Click on Vinkius — From Prompt to Execution

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

01 Connect your Bandwidth credentials (Account ID, Username, Password) to this MCP within your preferred AI client.

02 Tell your agent what you need—for example, 'Send an outage alert SMS to all users' or 'List the last 50 messages sent.'

03 The agent executes the necessary communication operation, and you receive a plain-language confirmation of the successful dispatch or data retrieval.

The bottom line is that your AI client handles complex telecom requirements, allowing you to manage messaging operations through simple conversation.

Built For

This MCP is for teams whose core job revolves around timely, reliable communication at scale. It's built for the marketing operator who gets frustrated with campaign failures due to carrier filtering, or the support engineer needing instant mass alerts during an outage.

Support Operations Engineer

Needs to immediately dispatch priority SMS blasts across large user bases during system outages and track message receipt confirmations.

Marketing Campaign Manager

Must constantly audit 10DLC campaign health, ensuring promotional texts never get flagged or blocked by carriers.

DevOps Engineer

Needs to execute structural health tests and ping the telecom backbone before scaling new services or deploying updates.

What Changes When You Connect

01 Avoid building custom webhook architectures. Your agent handles the underlying CPaaS complexity, letting you focus on messaging strategy.

02 Instantly send blast SMS/MMS payloads with rich media attachments while explicitly bypassing legacy SIP pipelines.

03 Validate 10DLC TCR profiling and approve messaging rules using `get_campaign` to prevent carrier-side filtering blocks.

04 Run compliance checks by calling `get_toll_free` to dynamically ping upstream toll-free approval headers.

05 Audit message history with `list_messages`, ensuring you always have a clear record of delivery footprints and communication logs.

Real-World Applications

Mass Outage Notification

During an unexpected system outage, the support engineer simply asks their agent to send a priority alert. The agent uses `send_sms` to dispatch the blast message instantly across all registered users.

Marketing Compliance Checkup

Before running a major holiday promotion, the marketing manager prompts the agent to check campaign health using `list_campaigns`, ensuring 10DLC rules are approved and ready for scale.

Media Storage Cleanup

A team needs to free up old assets. They tell their agent to list all stored media files using `list_media` and then use `delete_media` on any files older than six months.

Pre-deployment Network Check

A DevOps team needs assurance that the communication channels are clear. They ask the agent to ping the API health using `get_health`, confirming structural readiness before scaling services.

Patterns to Avoid

Trying to send messages manually

✗ AVOID

A user tries to compose and dispatch a critical alert message by navigating through the Bandwidth web console, which is slow and doesn't fit into their workflow.

✓ INSTEAD

Instead, ask your agent to use `send_sms` or `send_mms`. This executes the send command instantly from natural conversation, regardless of what interface you're using.

Ignoring campaign compliance rules

✗ AVOID

A marketer launches a large promotional batch without validating 10DLC profiles, resulting in messages being blocked by carriers.

✓ INSTEAD

Always run `list_campaigns` and use the details provided to confirm profiling is done. This validates your messaging rules before you send anything.

Assuming media assets persist forever

✗ AVOID

The team forgets about old images used for promotions, leading to unnecessary storage costs over time.

✓ INSTEAD

Use `list_media` to see what's stored and then use `delete_media` immediately after a campaign concludes to keep your account clean.

The Right Fit

You should connect Bandwidth if your core pain point is reliably sending high-volume, compliant messages at scale. Use this MCP when you need your AI agent to take over the technical complexity of telecommunications—for example, running compliance checks via `get_toll_free` or dispatching alerts using `send_sms`. Don't use it if you only need basic email functionality; those are handled by dedicated mail service tools. Likewise, don't rely on this MCP for complex audience segmentation based on web behavior; that requires a CRM integration. This is purely about the reliable transport and management of messages (SMS/MMS) and their associated compliance infrastructure.

Bandwidth Messaging: Automating Compliance Checks with AI Agents

Today, managing high-volume messaging requires jumping between multiple platforms. You have to manually check if your 10DLC campaigns are properly profiled and then verify if the target number is compliant before hitting 'send.' This process takes time, introduces human error, and risks message failure.

With this MCP, you just talk to your agent. You ask it to validate campaign health or ping a toll-free header. The agent handles all those backend checks, giving you immediate confirmation that the communication path is clear for deployment.

Bandwidth: Managing Media and Campaign Data with AI Agents

Manually auditing message history or deleting old media assets means opening multiple dashboard tabs, filtering by date range, and clicking through logs. It's tedious data cleanup that slows down the team.

Now you can ask your agent to list all messages using `list_messages` or delete specific assets with `delete_media`. You get immediate, actionable results without ever leaving the chat interface.

Bandwidth: 10 Tools for Messaging Campaign Operations

Use these tools to manage message sending, campaign validation, media storage cleanup, and API health checks within your agent.

#	TOOL	DESCRIPTION
01	`delete_media`	Removes a stored media asset from your Bandwidth account.
02	`get_campaign`	Retrieves detailed information for one specific 10DLC campaign.
03	`get_toll_free`	Lists all the verification statuses of your toll-free numbers.
04	`get_health`	Pings the Bandwidth API to check overall system health and status.
05	`list_applications`	Retrieves a list of all your active messaging applications.
06	`list_campaigns`	Lists all available 10DLC messaging campaigns you manage.
07	`list_media`	Shows a list of media files currently stored in your Bandwidth account.
08	`list_messages`	Generates a log showing all sent and received messages.
09	`send_mms`	Sends an MMS message that includes attached rich media content.
10	`send_sms`	Sends a standard SMS text message via the Bandwidth API.

See It in Action

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

U We had a major service interruption. Send an urgent SMS update to our entire user base telling them we're back online.

Outage Alert Sent

The system successfully dispatched the emergency payload to 4,521 recipients across three regions. The outbound carrier queue confirmed receipt of the message by Bandwidth and scheduled delivery through the primary application ID.

Confirmation: All high-priority alerts are processed immediately.

U List all my uploaded media files and delete any promotional image named 'Q1-sale.jpg'.

✅ **Media Audit Complete**

I found 23 media blocks in your storage instance. I located and deleted the asset `Q1-sale.jpg`, freeing up its allocated quota immediately. The remaining files are listed below:

- `logo_v2.png` (Uploaded: 2024-01-15)
- `manual_guide.pdf` (Uploaded: 2023-11-01)

U Check the overall status of our toll-free number +1-800-CALL-NOW.

Toll-Free Verification Report

The check returned a 'Compliant' status. The upstream approval headers are active and match current carrier requirements for US service. You can send high-volume traffic using this line without risk of rejection.

Frequently Asked Questions

01 **How do I use the Bandwidth MCP to send a bulk SMS alert?**

You simply ask your agent to dispatch an SMS, providing the target numbers and message body. The system handles the complex messaging payload and ensures it gets into the carrier queue immediately.

02 **Should I use Bandwidth MCP for marketing campaigns that require compliance checks?**

Yes. Before launching any campaign, you can ask your agent to validate the 10DLC profiles. This proactive check confirms your messaging rules are approved and ready to avoid carrier filtering.

03 **Can I use Bandwidth MCP to manage media files?**

You can list all uploaded media using `list_media` and then delete specific assets like old images or guides. This keeps your storage clean and helps you track usage effectively.

04 **Is the Bandwidth MCP good for checking if my toll-free number is active?**

It is excellent for that. The agent can ping upstream headers to dynamically check compliance, giving you confidence that your dedicated line will work reliably for messaging.

05 **Does the Bandwidth MCP help me audit past messages?**

Yes. You can request a list of sent or received messages using `list_messages`. This gives you a full, auditable log of every interaction that went through your account.

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 `"bandwidth": { "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

Bandwidth 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 Bandwidth. 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	Bandwidth MCP
Server ID	`019d7558-42a7-7146-bed3-50322cc71f68`
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/bandwidth.