MCP SERVER | NO CODE | CLOUD HOSTED

JustCall MCP

Audit Every Call, Text, and Contact Detail.

JustCall MCP manages all your company's communication data—calls, texts, and recordings. This connector gives your agent instant access to comprehensive history, allowing you to audit interactions, vet contacts, or track campaign performance without ever leaving your workflow.

A+ Quality Score 100/100

cloud-phone | sms-marketing | call-recording | contact-management | sales-engagement | telephony

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

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.

JustCall MCP

10 tools available
Cloud-hosted on Vinkius

This MCP connects your AI client directly to JustCall's cloud phone system records. Your agent can instantly pull complete communication histories, whether it's a full transcript of a call, the details of an SMS exchange, or a list of active contacts. It centralizes data that used to live across multiple dashboards and manual exports. Need to check on a client? You can retrieve detailed contact information right away. Tracking down every interaction for compliance is simple; your agent can pull lists of all completed calls or search through message logs. This gives you full visibility into sales cycles and support tickets, letting you automate complex communication workflows efficiently. By connecting this MCP via the Vinkius catalog, you give your AI client a complete 360-degree view of every customer touchpoint.

Core Capabilities

01 — Audit Call History

Retrieve detailed records for specific phone calls, including participants, timestamps, and notes.

02 — Manage Customer Profiles

Get full contact details—phones, emails, and metadata—for any individual customer or lead.

03 — Review Messaging Logs

List all SMS/MMS messages, showing content, who sent them, and if they were successfully delivered.

04 — Track Communication Volume

Pull lists of contacts, calls, recordings, or users to audit activity and measure performance metrics.

05 — Monitor Campaign Efforts

List details about active calling campaigns to monitor sales outreach and telemarketing activities.

One Click on Vinkius — From Prompt to Execution

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

01 Your AI client tells the MCP exactly what data it needs, like 'Find all calls associated with Jane Doe' or 'Show me last week's messages.'

02 The MCP translates that request into an API call and hits the JustCall system to pull raw records.

03 It returns structured data—call IDs, message content, contact details—ready for your agent to use in its response.

The bottom line is you get immediate access to a unified log of all communication activity without having to manually navigate the JustCall portal.

Built For

This MCP is essential for operations managers, sales directors, and support leads. It's perfect for anyone whose job involves reviewing customer history or auditing communication compliance. You need this if your team spends too much time jumping between CRM dashboards, call logs, and ticketing systems just to get a full picture of one client.

Customer Support Manager

Uses the MCP to retrieve specific communication records and list messages, quickly building a complete history for agents handling escalated tickets.

Sales Director

Runs reports using the MCP to monitor call volumes, identify successful campaigns, and verify contact details before major client pitches.

Operations Analyst

Audits system activity by listing all users or checking webhook configurations to ensure communication processes are running correctly across the organization.

What Changes When You Connect

01 Get a full audit trail immediately. Instead of manually checking separate logs for every interaction, you can use the `list_calls` tool to pull all call metadata in one go.

02 Never guess who you're talking to again. By using `get_contact`, your agent pulls verified names and multiple contact methods before a sale or support chat even starts.

03 Track communications across channels. You don't just see calls; you can use `list_messages` to pull SMS/MMS logs right alongside call history, giving one complete view.

04 Improve compliance reporting. Need proof of customer interaction? The MCP lets your agent quickly list all available recordings via the `list_recordings` tool for internal review.

05 Automate data gathering. When onboarding a new client, you can run multiple tools—like listing contacts and checking campaign status—to build a comprehensive profile instantly.

Real-World Applications

Investigating a Failed Deal

A sales rep needs to know why a deal stalled. Instead of digging through multiple CRM tabs, they ask their agent to use `get_call` for the last interaction and then run `list_messages` to see if any follow-up texts were missed. They get all the context immediately.

Compliance Audit

The compliance officer needs proof that every agent is following protocol. They ask their agent to use `list_users` and then cross-reference it with `list_calls` to ensure only authorized personnel handled sensitive calls.

Customer Onboarding

A marketing team needs a list of leads for a new campaign. They ask the agent to use `list_contacts` first, then check `list_numbers` to confirm which numbers are available for dialing before running a large-scale outreach.

Post-Incident Review

A support team is reviewing a major service outage. They use the agent to get all call data using `list_calls`, then run `get_call` on specific IDs, and check associated notes to determine if communications failed at a certain point.

Patterns to Avoid

Trying to find contact info manually

✗ AVOID

A user copies an email address from one system and pastes it into another dashboard, only to realize the phone number is missing or outdated.

✓ INSTEAD

Always use the `get_contact` tool. It pulls all verified data (emails, phones, metadata) for a single contact in one structured API call.

Missing communication types

✗ AVOID

A user only checks the 'Calls' tab and misses critical follow-up texts or automated campaign status updates.

✓ INSTEAD

To get the full picture, run both `list_calls` (for voice) and `list_messages` (for text). Never assume one channel holds all the data.

Confusing activity logs with history

✗ AVOID

A manager thinks listing active users is the same as reviewing historical calls, leading to confusion about who handled what.

✓ INSTEAD

To see past actions, use `list_calls` or `get_call`. Use `list_users` only when you need a roster of people currently set up in your organization.

The Right Fit

Use this MCP if the core of your problem is auditing communication history across multiple channels (voice, SMS, recording). You need

to know *what* was said and *who* was involved. Don't use it if you only need to manage internal user roles—use the `list_users` tool specifically for that. If your goal is pure CRM record-keeping and you don't care about call logs or recordings, a dedicated contact management MCP might be cleaner. However, because this MCP handles everything from calls (`list_calls`) to texts (`list_messages`), it remains the best single source of truth for customer interactions.

The Pain of Fragmented Customer Records

Right now, gathering a full picture of one client is a nightmare. You open your CRM to see their name and basic details. Then you switch to the calling dashboard to check if they spoke to sales last week. Next, you jump to an SMS log just to verify follow-up texts, and finally, if there was trouble, you have to manually pull the call recording link. It's a dozen clicks and three systems just to answer one question: 'What happened with this client?'

With this MCP, your agent handles it all in one go. You simply ask for the full history of that customer ID. The system instantly pulls together the contact details, the call log (`list_calls`), and any associated messages (`list_messages`). You get a single, structured data packet that answers everything you need, without leaving your workflow.

Getting a 360-Degree View with JustCall MCP

The manual steps of cross-referencing the call history against the contact database and then searching for recordings are gone. You don't click between tabs or copy IDs; your agent just calls `get_contact` followed by `list_calls` , stitching the data together in real time.

What’s different now is speed and completeness. Instead of spending 15 minutes gathering scattered proof points, you get a complete, auditable record in seconds.

JustCall: 10 Tools for Communication Ops

These tools let your agent inspect every layer of customer interaction—from basic contacts to complex call records and message threads.

#	TOOL	DESCRIPTION
01	`get_call`	Retrieves comprehensive details for a specific phone call, including notes and participants.
02	`get_contact`	Pulls all associated contact information, like phones and emails, for a single person or company.
03	`list_calls`	Provides an overview of phone calls, listing the direction (inbound/outbound), duration, and status.
04	`list_campaigns`	Lists all defined calling campaigns in your account for monitoring outreach efforts.
05	`list_contacts`	Generates a list of all contacts available, including their names and IDs.
06	`list_messages`	Lists every SMS/MMS message in your account, detailing the content and delivery status.
07	`list_numbers`	Shows all phone numbers registered to your JustCall account for inventory checks.
08	`list_recordings`	Provides an index of available call recordings, useful for quality assurance and review.
09	`list_users`	Lists all user accounts within the organization to track who handled specific communications.
10	`list_webhooks`	Shows a list of configured webhooks for auditing system integrations.

See It in Action

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

U List all recent phone calls in JustCall.

I'll fetch the history of your recent phone calls from JustCall.

U Show me the latest SMS messages.

I'll retrieve the list of recent text messages from your JustCall account.

U Check the details for contact ID '123'.

I'll look up the full profile and history for that specific contact in JustCall.

Frequently Asked Questions

01 **How do I find out if an agent was authorized to make the call using JustCall MCP?**

You use `list_users` first to see who is set up in your organization, and then check `get_call` details to confirm which specific user ID handled that communication.

02 **Does JustCall MCP include old call recordings or just recent ones?**

The MCP uses the `list_recordings` tool to provide an index of available records. You should check your account settings within the API documentation to verify retention policies.

03 **Can I track a contact's phone number history with JustCall MCP?**

Yes, you use `get_contact` to pull associated numbers and metadata for that specific person. This is useful for vetting leads before outreach campaigns.

04 **What if I need to check both calls and texts from the same date? JustCall MCP?**

Run `list_calls` to get voice activity records, then immediately run `list_messages` to pull all SMS/MMS logs for that timeframe. Combining these two tools gives you a full picture.

05 **How do I audit which campaigns are running right now using JustCall MCP?**

Use the `list_campaigns` tool. This function provides an overview of all defined calling campaigns, helping you monitor sales outreach and telemarketing efforts.

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 `"justcall": { "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

JustCall 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 JustCall. 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	JustCall MCP
Server ID	`019d75be-b0a3-7232-81cc-baf536cde198`
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/justcall.