MCP SERVER | NO CODE | CLOUD HOSTED

Tactiq MCP

Turn meeting recordings into actionable knowledge.

Tactiq lets your AI agent manage every meeting transcript you've ever recorded. Pull summaries, pull out action items, track who talked the most, and search across all past recordings using natural conversation with any MCP-compatible client.

A+ Quality Score 100/100

transcription | meeting-notes | action-items | summarization | real-time-sync | speaker-analytics

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

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.

Tactiq MCP

6 tools available
Cloud-hosted on Vinkius

Connect your Tactiq account to your preferred AI client, and treat your entire library of meetings like a searchable database. You talk to your agent—'What did we decide about the budget in Q1?'—and it retrieves the answer across all recordings. It pulls full transcripts with speaker labels and timestamps, so you know exactly who said what. Need follow-up tasks? The system automatically extracts action items and deadlines from any conversation. Plus, you can view detailed reports on speaking time to see who contributed most often. All this meeting intelligence is accessible through the Vinkius Marketplace, making it easy for your agent to manage knowledge across multiple tools.

Core Capabilities

01 — Check connectivity status

Verifies if your AI client can talk to Tactiq's system.

02 — Fetch all meeting details

Retrieves specific information about any recording, like the date or participants involved.

03 — Get key insights and summaries

Provides an AI-generated breakdown of decisions and main points from a full transcript.

04 — Extract assigned tasks

Scans transcripts to automatically pull out specific follow-up actions, deadlines, and owners.

05 — List all meeting records

Gives you a list of every recording available in your account.

06 — Search across transcripts

Finds mentions of specific keywords or topics across your entire library of recordings.

One Click on Vinkius — From Prompt to Execution

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

01 First, you subscribe to the Tactiq MCP on Vinkius and grab your API Key from your Tactiq settings.

02 Next, you connect that key in your AI client. Your agent can now see all of your recorded meeting data.

03 Finally, you simply ask your agent a question—like 'What were the Q3 priorities?'—and it pulls the answer directly from the transcripts.

The bottom line is, instead of opening 20 separate meetings to find one fact, you just talk to your AI client and get the direct answer.

Built For

This MCP is built for knowledge workers who spend more time searching through notes than actually doing deep work. It's for product leads tired of context-switching between meeting apps, project managers who need instant summaries to track tasks, and developers needing raw transcript data for custom workflows.

Project Manager

Uses the agent to automatically pull out all assigned tasks and deadlines from a week's worth of meeting transcripts.

Product Lead

Checks past recordings for specific decision history, reviewing key insights without opening multiple dashboards.

Developer

Queries the MCP to retrieve full transcript details or list all meeting records to feed into a custom data pipeline.

What Changes When You Connect

01 Stop manually reading through hours of audio. Instead, use the agent to get a clean summary via `get_summary` and immediately know what was decided.

02 Never miss a follow-up task again. The `get_action_items` tool automatically pulls out deadlines and assigned tasks from any transcript, so nothing gets forgotten.

03 Deep dive into who contributed most: Use the tools to list speakers and track their talk time ratio, giving you analytics on participation.

04 Search instantly across your entire archive. Instead of jumping between meeting notes, use `search_transcripts` to find mentions of 'budget' or 'Q2 strategy' from years ago.

05 Review full context easily by getting the transcript details with `get_transcript`. You get speaker labels and timestamps, so you know exactly who said what.

06 View an overview of all your available data by running `list_meetings` to see a count and date range for every recording.

Real-World Applications

Finding the last mention of a key risk

A product manager needs to know if 'latency issues' came up during the Q1 planning session. They tell their agent, 'Search my transcripts for latency issues.' The agent uses `search_transcripts` and finds 3 mentions across 2 different meetings, allowing them to read the exact discussion section.

Building a task list from rambling notes

A team finishes a brainstorming session. Instead of forwarding dozens of emails with action items, they ask their agent to 'Get all follow-ups.' The agent uses `get_action_items` and returns a clean, formatted list of owners and due dates.

Onboarding new hires into project history

A developer needs to understand the original decision flow for a feature. They ask their agent to 'Get key insights from the initial meeting.' The agent uses `list_insights` and provides an immediate, high-level summary of decisions made months ago.

Tracking project scope creep

A product lead wants to compare what was planned versus what was decided. They ask the agent for 'The core goals from the initial sync.' The agent uses `get_meeting` and pulls up the original meeting details, providing a clear baseline.

Patterns to Avoid

Copying text snippets

✗ AVOID

Opening 15 different meeting notes, reading through paragraphs to find one specific date or name that was mentioned in passing.

✓ INSTEAD

Ask your agent to search transcripts using `search_transcripts` for the keyword. If you need a full record, use `get_transcript` and then ask the agent to filter it down.

Relying on memory

✗ AVOID

Trying to remember if the client agreed on the pricing model during last week's call. You spend time cross-referencing emails and Slack messages.

✓ INSTEAD

Ask your agent to 'Get key insights from the meeting.' The agent uses `list_insights` to summarize decisions, giving you a documented answer.

Manual task extraction

✗ AVOID

After every call, manually creating a list of tasks and sending them out in a follow-up email.

✓ INSTEAD

Immediately ask your agent to 'Extract the action items.' The agent uses `get_action_items` right after the call ends to get you that clean, structured list.

The Right Fit

Use this MCP if your biggest pain point is information retrieval from massive amounts of recorded audio. You need a system that treats every meeting like an indexable document library. Use it when you must know who said what (using `get_transcript`) or when you need to consolidate all assigned tasks into one view (`get_action_items`). Don't use this if you just want to schedule meetings; for scheduling, use a dedicated calendar tool. If your goal is simply to analyze the overall health of the connection between systems, running `check_tactiq_status` confirms everything is good to go.

The problem isn't recording meetings; it's finding anything after they end.

Today, getting key information means clicking through multiple platforms. You open the meeting platform, download the transcript, copy-paste it into a notes document, and then try to highlight every single action item or decision point. It's tedious work that turns an hour of focus into two hours of administrative searching.

With this MCP, you talk to your agent directly. Instead of manual highlighting or searching across multiple tabs, the agent processes everything for you. You ask a direct question—like 'What did we decide about the budget?'—and you get the answer instantly.

Tactiq MCP: Structured knowledge from unstructured meetings

The manual steps that vanish are the need to manually list, search for keywords, and summarize decisions. You never have to open 10 different records just to get a general overview; you simply ask the agent to pull the key insights.

This MCP changes things because it gives your agent a structured way of understanding conversation. It doesn't just give you text; it extracts *meaning*—action items, decisions, and speaker contributions.

Tactiq: 10 Tools for Meeting Intelligence

These tools allow your agent to perform specific actions like listing meetings, extracting tasks, or searching keywords across all recorded transcripts.

#	TOOL	DESCRIPTION
01	`list_meetings`	Provides a complete list of all meeting recordings available in the Tactiq system.
02	`list_meeting_artifacts`	Requires Tactiq Team plan or higher. List AI artifacts from a meeting
03	`check_generation_status`	Useful when a summary is still being processed by Tactiq AI. Returns the current processing state. Check if meeting summary is ready
04	`get_artifact`	Artifacts include action items, email drafts, slide outlines, and more. Read a specific AI artifact
05	`get_meeting_summary`	Requires Tactiq Team plan or higher. Returns key takeaways, decisions, and context. Get AI-generated meeting summary
06	`search_meetings`	Use to find specific discussions: "Find my calls with the design team from last month" or "What was decided about Q1 roadmap?" Search meetings by keyword, participant, or date

See It in Action

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

U Show all meetings from this week.

You had 8 meetings this week. The longest was 'Q2 Planning' (62 min, 5 participants). Would you like to see the summary or action items from any meeting?

U Get the summary and action items from transcript TR-5021.

Summary: The team agreed on Q2 priorities, assigned 3 tasks (proposal draft by Friday, budget review next Monday, client follow-up by Sarah). 4 key decisions were made. Want me to format these as tasks?

U Search my transcripts for mentions of 'pricing strategy'.

Found 5 mentions across 3 meetings. The most detailed discussion was in 'Sales Review' (March 18), where the team spent 12 minutes on pricing tiers. Would you like to read that section?

Frequently Asked Questions

01 **How does the Tactiq MCP handle searching across all my meetings?**

The agent uses `search_transcripts` to scan your entire transcript library. You only need to provide a keyword or topic, and it finds every relevant mention across multiple recordings.

02 **Can I get who talked the most using the Tactiq MCP?**

Yes, you can use the speaker tools to list speakers and view their participation metrics. This gives you a clear breakdown of contribution time for every meeting.

03 **Does the Tactiq MCP only give me plain text summaries?**

No, the system provides AI-generated insights and key decision lists via `list_insights`, which goes beyond just summarizing the main topics.

04 **How many types of information can I pull from a transcript using Tactiq MCP?**

You can get full transcripts, summaries, action items, speaker data, and general meeting details—all through different tools like `get_transcript` and `get_action_items`.

05 **Do I need to do anything with the Tactiq MCP after connecting it?**

No. After you subscribe and connect your API key, you just talk to your agent. It handles retrieving all the data for you.

06 **How do I access meeting transcripts via AI?**

Use `list_transcripts` to see all recorded meetings, then `get_transcript` with the transcript ID for the full text with speaker labels and timestamps.

07 **Can I extract action items from meetings?**

Yes. Use `get_action_items` with a transcript ID to retrieve all AI-detected follow-ups, deadlines, and assigned tasks.

08 **How do I search across all my transcripts?**

Use `search_transcripts` with any keyword or phrase to find matching content across all recorded meetings.

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 `"tactiq": { "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

Tactiq 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 Tactiq. 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	Tactiq MCP
Server ID	`019dd16d-560a-71b4-97eb-49770f80b973`
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/tactiq.