MCP SERVER | NO CODE | CLOUD HOSTED

Granola MCP

Search, summarize, and track meeting actions instantly.

Granola helps you manage meeting notes directly through your AI agent. It lists all documents in your workspace, retrieves full transcripts, and finds summaries or specific action items instantly. Instead of manually sifting through hours of conversation, you can search across every document to pull out exactly what you need.

A+ Quality Score 100/100

meeting-notes | transcription | summarization | action-items | searchable-memory | ai-assistant

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

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.

Granola MCP

12 tools available
Cloud-hosted on Vinkius

Connecting Granola means taking control of all the meeting data generated by your team. Your AI agent gains access to a searchable memory of every discussion, allowing you to retrieve full transcripts and summaries using natural language queries. You don't have to manually organize notes; this MCP lists documents in your workspace so your agent can find primary entry points for everything from last week's sync to last month's planning session.

It doesn't just summarize; it isolates specific action items, pulling out targeted next steps right after the meeting ends. You can also look at participant details by cross-referencing calendar arrays attached to a session. If you need context from multiple meetings, you can even fetch several documents by their IDs in one request. This makes Granola invaluable when integrated through Vinkius's catalog of tools, making your agent smarter about organizational knowledge.

Core Capabilities

01 — Search all meeting discussions

Perform a full-text search across every document to find specific topics or conversations.

02 — Extract key tasks and owners

Identify and isolate action items from recorded meetings, automatically setting up post-meeting follow-ups.

03 — Retrieve transcripts and summaries

Get full speaker-detected transcripts or concise AI-generated overviews of any meeting document.

04 — View all workspace documents

List every available meeting document, or narrow the search by date range or folder structure.

05 — Identify attendees and content

Get participant lists for a specific meeting, or access the full structured content of a document.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP on Vinkius and enter your Granola API Key (found in your account settings).

02 Next, prompt your AI agent with a request like 'Show me the meeting notes about Q3 spending last month'.

03 Your agent uses the available tools to search documents, retrieve the necessary content, and present you with actionable summaries or specific data points.

The bottom line is that your AI agent handles all the complexity of navigating organizational memory for you.

Built For

Managers who spend their afternoons trying to piece together decisions from dozens of meeting notes, or Product Managers who need to audit conversation history across multiple teams. This MCP helps stop that endless search through shared drives.

Project Manager

Needs to summarize back-to-back meetings and track every assigned action item without having to take manual notes.

Product Owner

Must audit collaborative meeting documents, searching across conversation history using natural language prompts for specific feature mentions.

Operations Analyst

Monitors organizational knowledge by verifying meeting results and dependencies in real-time through the chat interface.

What Changes When You Connect

01 Stop manually reading long transcripts. With the `get_summary` tool, you get AI-generated overviews that cut down hours of content into key takeaways in seconds.

02 Never miss a follow-up task again. The dedicated `get_action_items` tool isolates specific next steps and owners directly from meeting notes.

03 Need to compare ideas across several sessions? Use `get_documents_batch` to pull multiple documents by their IDs in one go, letting your agent analyze cross-meeting dependencies securely.

04 Finding old info used to mean guessing which folder it was in. Now, use the `search_documents` tool for full-text searching across everything, no matter where it lives.

05 You can see exactly who was there and what they did. Use `get_participants` to list attendees, or run `list_by_date` to focus only on meetings from last quarter.

Real-World Applications

Auditing a failed project.

A Product Owner needs to know why the 'Phoenix' feature was shelved. They ask their agent to `search_documents` for mentions of 'Phoenix scope reduction'. The agent finds three key documents and uses `get_summary` on each, giving the PO a quick breakdown of the decisions made across different teams.

Preparing for an executive review.

A Project Manager needs to prove team progress. They use `list_documents` to find all meeting notes from the last month and then run `get_action_items` on each one, compiling a single list of completed tasks and outstanding items for their boss.

Onboarding a new team member.

A manager needs to give a new hire context. Instead of sending 20 links, the manager asks the agent to `list_recent` meetings from the past month and then uses `get_metadata` to pull participant lists for the last three key sessions.

Comparing competitor strategy.

An analyst needs to compare notes from two separate vendor calls. They use `get_documents_batch` by providing the IDs of both meetings, allowing their agent to analyze and synthesize side-by-side comparisons in one prompt.

Patterns to Avoid

Asking for vague context.

✗ AVOID

Prompting: 'What did we talk about last month?' The AI client fails because it doesn't know where to look or what documents are relevant, giving only a list of links.

✓ INSTEAD

Be specific. Use `list_by_date` first to narrow the scope to the correct time period, then use `search_documents` with keywords like 'Q3 budget review' for precise results.

Treating notes as single files.

✗ AVOID

Assuming that all meeting info is in one giant document and trying to copy-paste everything into a spreadsheet, leading to data loss and misattribution.

✓ INSTEAD

Use `get_documents_batch` if you need multiple sources for comparison. If you only need the next steps, always use `get_action_items` rather than reading the full content.

Ignoring speaker context.

✗ AVOID

Reading a transcript and forgetting who said what because it's just a wall of text.

✓ INSTEAD

Use the `get_transcript` tool, which provides full transcripts with speaker detection markers, so you know exactly who said what.

The Right Fit

Use this MCP if your core workflow is built around synthesizing information from multiple meeting discussions. You need to ask questions like, 'What were the tasks assigned during the Q2 planning sessions?' or 'Who was supposed to follow up on the marketing sync?'. Don't use it if you just need simple file storage; those are dedicated document management systems. Also, don't rely solely on its summary features for legal compliance; always cross-reference with `get_content` to validate key passages. This MCP is a knowledge layer built *on top of* your existing files, not a replacement for them.

The manual effort of piecing together meeting decisions is exhausting.

Think about it: You finish a week of back-to-back calls. You have 20 different documents, each with hours of audio and notes. To get the full picture—who agreed to what, who owns which task—you open Document A, scroll through the transcript, copy three action points into your tracker. Then you jump to Document B, manually search for names, find the summary block, and copy those details too. It’s a cycle of clicking, scrolling, and copy-pasting that takes half a workday.

With this MCP connected via Vinkius, that manual effort evaporates. You simply ask your agent: 'What did John commit to during the Q2 budget review?' The system runs `get_action_items`, pulls the relevant data from all necessary sources, and presents a clean list of commitments without you touching a single cursor.

Granola MCP. Get immediate action items and summaries.

Specific manual steps that disappear include the need to open multiple files just to confirm details, or spending time trying to distinguish key decisions from general chatter within a full transcript. You don't have to manually cross-reference calendars; your agent handles participant lookups instantly.

Now, getting project context is instantaneous. Your team moves faster because the knowledge base isn’t trapped in PDF archives and old meeting notes; it’s immediately accessible and structured for action.

Granola: 12 Tools for Document Ops

Use these 12 tools to list, search, retrieve content, extract tasks, and manage every aspect of your organizational meeting notes.

#	TOOL	DESCRIPTION
01	`list_documents`	Lists all available meeting documents within your workspace, managing pagination automatically.
02	`get_metadata`	Pulls basic information (metadata) for a single specified meeting document.
03	`get_transcript`	Retrieves the entire transcript of a meeting, including speaker detection markers.
04	`get_documents_batch`	Fetches multiple documents using their IDs in just one request for comparative analysis.
05	`list_folders`	Retrieves a list of high-level folder labels that organize your entire document workspace.
06	`get_content`	Retrieves the full, structured content from an entire meeting document.
07	`list_by_date`	Lists all meeting documents that fall within a specific date range you define.
08	`get_participants`	Retrieves the names and details of attendees for any given meeting.
09	`get_summary`	Generates a concise, AI-powered summary of an entire meeting document.
10	`list_recent`	Lists the 20 most recently created or modified meeting documents in your workspace.
11	`get_action_items`	Extracts and lists specific tasks that were identified as next steps during a meeting.
12	`search_documents`	Performs a full-text search across all your stored meeting documents to find keywords.

See It in Action

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

U Show me the 5 most recent meeting documents

Retrieving your recent documents... I found 5 meetings including 'Product Design Workshop', 'Q2 Budget Review', and 'Weekly Sync'. Would you like the AI summary or the list of participants for the design workshop?

U What were the action items from meeting 'abc-123'?

Action items extracted! For meeting abc-123, I found 3 tasks: 1. John to update the landing page copy. 2. Sarah to finalize the pricing model. 3. Mike to schedule the stakeholder demo. Would you like the due dates for these?

U Search for meeting notes mentioning 'competitor analysis'

Searching documents... I found 2 meeting documents mentioning 'competitor analysis'. The most relevant is 'Marketing Strategy Sync' from March 20. I can retrieve the full structured content or transcript for you.

Frequently Asked Questions

01 **How does Granola MCP handle transcripts?**

The `get_transcript` tool retrieves the full meeting transcript and includes speaker detection, so you know exactly which person said every line of dialogue.

02 **Can I find action items from multiple meetings using Granola MCP?**

Yes. You can use the `get_documents_batch` tool to fetch several documents and then ask your agent to run `get_action_items` across the entire set for comprehensive tracking.

03 **What if I only want notes from a specific time frame using Granola MCP?**

Use the `list_by_date` tool. It lets you filter your workspace and list only documents that fall within a precise date range, narrowing down your focus instantly.

04 **Does Granola MCP help me find specific keywords across years of meetings?**

Absolutely. The `search_documents` tool performs full-text detection across all available meeting documents, giving you highly targeted results regardless of when the discussion happened.

05 **What is the easiest way to get a quick overview of a massive document?**

Use the `get_summary` tool. It retrieves an AI-generated summary that boils down bulk meeting content into concise overviews and key takeaways.

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 `"granola": { "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

Granola 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 Granola. 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	Granola MCP
Server ID	`019d75aa-db58-73fd-92a0-f00fd6fd4006`
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/granola.