MCP SERVER | NO CODE | CLOUD HOSTED

Jibble MCP

Audit Time Logs, Personnel Data & Projects.

Jibble MCP connects your AI client directly to Jibble's full time tracking, attendance, and workforce management system. Your agent can list people, check specific time entries, track projects, or audit organization details using one simple connection. Stop switching tabs—manage all your team data through natural conversation.

A+ Quality Score 100/100

time-tracking | attendance-management | workforce-management | project-tracking | payroll-support

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

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.

Jibble MCP

10 tools available
Cloud-hosted on Vinkius

Jibble helps you move beyond viewing dashboards. Instead of manually compiling reports across multiple spreadsheets, your AI client uses this MCP to pull precise workforce data directly from Jibble's platform. Need to know if a specific person clocked in at the right location? Your agent can get that detail instantly. Want to see how many billable hours were logged against a specific project last month? That’s just one query away. This connection lets your agent analyze who worked where, when they worked it, and what type of activity was recorded—all without you writing a single API call. It's powerful workforce management built into the Vinkius catalog so any MCP-compatible client can use it.

Core Capabilities

01 — Audit organizational settings

Retrieve core details about your entire Jibble organization account.

02 — Look up employee records

Fetch comprehensive profiles for individual team members, including contact and ID information.

03 — Review specific time logs

Get detailed data on a single recorded time entry, including location and notes for auditing purposes.

04 — List configured resources

Pull lists of all defined groups, clients, projects, activities, or locations used across the company.

05 — Query historical time activity

Retrieve a list of all existing time entries to monitor total hours worked by the workforce.

One Click on Vinkius — From Prompt to Execution

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

01 Your AI client first authenticates with your Jibble account using Vinkius.

02 You ask your agent a question, like 'Show me all time entries for Q3.'

03 The MCP executes the necessary tool calls (e.g., list_time_entries) and returns clean, structured data to your client.

The bottom line is, you tell your agent what you need in plain English, and it handles all the complex data pulling from Jibble's systems for you.

Built For

HR Operations Managers who are sick of manual compliance checks; Payroll Specialists needing accurate time logs for billing; or Project Leads who struggle to prove billable hours by cross-referencing multiple spreadsheets. If your job involves verifying 'who did what, where, and when,' this is for you.

HR Operations Manager

Uses the MCP to verify employee details (get_person) or check if groups (list_groups) are correctly set up before a large company policy change.

Payroll Specialist

Runs checks on all time entries using list_time_entries and get_time_entry to ensure hours match pay periods accurately.

Project Manager

Queries the MCP to pull project details (list_projects) and correlate them with employee activities (get_person, list_activities) to measure utilization rates.

What Changes When You Connect

01 Stop guessing about who logged hours. Use list_people and get_person to build a definitive directory of all employees, ensuring your agent always has the correct IDs for time entry queries.

02 Never lose track of billing data again. By listing clients (list_clients) and projects (list_projects), you can instantly correlate work done against revenue-generating accounts.

03 Audit compliance faster than ever. Running list_time_entries allows your agent to pull the full history of time logged, letting you quickly verify dates and durations for payroll checks.

04 Identify team bottlenecks using list_groups and list_activities. You can programmatically check if a certain group is consistently clocking into non-standard activities, flagging potential policy issues.

05 Verify physical work locations effortlessly. List_locations allows your agent to confirm if an employee's recorded time entry (get_time_entry) matches the expected site for that project.

06 Centralize all workforce data. Instead of checking separate reports, you can query list_organization and get_organization details to verify account-wide settings in one go.

Real-World Applications

Investigating Time Discrepancies

A manager suspects an employee's time log is wrong. They ask their agent, 'Check the time entry for John Smith last Tuesday.' The agent uses get_time_entry and get_person to pull all relevant details—location, notes, and device info—immediately showing if the record is suspicious.

Generating Project Utilization Reports

A PM needs to prove how much time was spent on a specific client project. They ask their agent to cross-reference list_projects with list_time_entries, linking every logged hour back to the correct billing source.

Onboarding and Role Mapping

HR needs to update access for new hires. They first use list_people to find existing users, then check list_groups and list_locations to ensure the new employee is assigned to the correct department and site.

Compliance Auditing

An auditor needs proof that employees are only clocking in at authorized sites. They run a query comparing all entries from list_time_entries against the list_locations tool, flagging any site outside the approved network.

Patterns to Avoid

Treating it like a simple directory lookup

✗ AVOID

Asking only for 'list_people' and assuming that gives you project allocation data. You get names, but no context on what they worked on.

✓ INSTEAD

To link people to projects, first use list_people to identify the IDs, then run list_time_entries or list_projects to pull the associated time logs. Never rely on a single tool for complex reports.

Forgetting about organizational scope

✗ AVOID

Running a query without first verifying account settings using get_organization, resulting in vague errors because your agent doesn't know what data is available.

✓ INSTEAD

Always start by calling get_organization. This verifies the full configuration and ensures that subsequent calls (like list_groups or list_locations) are scoped correctly for the entire organization.

Confusing activity with project type

✗ AVOID

Assuming 'list_activities' will tell you which client a meeting was for. Activities only track *what* they were doing, not *who paid* for it.

✓ INSTEAD

To get billing context, you must combine list_clients and list_projects with the time data from list_time_entries. Activities just categorize the work.

The Right Fit

Use this MCP if your primary need is auditing or reporting on *time* and *workforce allocation*. You need to know who logged hours, against which project, and at what location. Don't use it if you only need simple CRM functions; for example, if you just want to update a client's phone number without any time tracking context, a standard CRM connector is better.

However, don't use it either if your core pain point is managing payroll calculations itself—this MCP provides the raw data (list_time_entries) that *feeds* into payroll systems; it doesn't execute the calculation. If you need to manage internal knowledge bases or document retrieval alongside time logs, look for a dedicated indexing tool instead of relying on Jibble.

The Payroll Report Nightmare

Right now, generating an accurate payroll report means juggling three different sources: the timesheet system, the project management board, and the internal HR roster. You spend hours exporting CSVs from each, then manually merging them in Excel—checking if employee IDs match, if locations are correct, and if every time entry links back to a valid client.

With this MCP, your agent handles that entire mess. Instead of clicking through five separate dashboards and copy-pasting into one master sheet, you simply ask the question: 'Give me all billable hours for Q2.' You get clean, structured data instantly.

Accessing Project Data with list_time_entries

Previously, if you wanted to know the total time logged on 'Project Alpha' for a specific employee, you had to search through every single entry record manually. You couldn't easily filter by both project and person simultaneously.

Now, your agent uses list_time_entries to pull all relevant records and filters them down instantly. The data shows exactly how long the person worked on that project, making audit trails immediate.

Jibble: Workforce Management Tools (10)

Use these ten tools to analyze every facet of your workforce, from listing all employees to auditing specific time entries against defined projects.

#	TOOL	DESCRIPTION
01	`get_organization`	Retrieves basic configuration settings for your entire Jibble account.
02	`get_person`	Pulls detailed profile information for a single employee or team member.
03	`get_time_entry`	Fetches location data, activity notes, and device info for one specific time record.
04	`list_activities`	Lists every possible task type (like 'Meeting' or 'Break') an employee can select when clocking in.
05	`list_clients`	Provides a list of all external clients tracked by the organization for billing purposes.
06	`list_groups`	Lists all defined teams or work units (like 'Sales Team' or 'Remote Workers') within the company.
07	`list_locations`	Retrieves a list of all physical sites or offices where employees can clock in.
08	`list_people`	Returns a comprehensive directory listing every employee by name, email, and internal ID.
09	`list_projects`	Lists all current and inactive projects set up in the system for time tracking breakdowns.
10	`list_time_entries`	Gathers a list of every recorded time entry, including who logged it and how long they worked.

See It in Action

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

U List all people in my Jibble organization.

I'll fetch the list of all members in your Jibble organization.

U Show me the recent time entries.

I'll retrieve the latest time tracking entries from Jibble.

U What are the active projects in Jibble?

I'll look up the list of configured projects in your account.

Frequently Asked Questions

01 **How do I find out what activities employees can select using Jibble MCP?**

You use list_activities. This tool retrieves a complete list of all predefined work categories, like 'Meeting' or 'Break,' that staff members have available when clocking in.

02 **Can I check if an employee exists before querying their time using Jibble MCP?**

Yes. You should run list_people first to get the comprehensive directory and confirm the correct internal ID. Then, use that ID when calling get_person or list_time_entries.

03 **What data does get_time_entry return for auditing purposes?**

get_time_entry returns detailed information about a single time log, including the location where it was clocked and any notes attached to the entry. This is key for discrepancy checks.

04 **How do I find out which clients are available in my Jibble organization?**

Just call list_clients. This tool retrieves a comprehensive list of every client that the company tracks, which is vital when auditing billable hours.

05 **Is there a way to see all configured projects using Jibble MCP?**

Yes, you use list_projects. It pulls a full record of every project setup in your account, allowing you to track work against existing initiatives.

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 `"jibble": { "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

Jibble 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 Jibble. 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	Jibble MCP
Server ID	`019d75bc-f6c3-72d7-b600-4d7e149658b2`
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/jibble.