MCP SERVER | NO CODE | CLOUD HOSTED

# break-time-total is a break management MCP.

## Keep your workforce compliant and track break durations accurately.

break-time-total handles the math and logic for workforce break tracking. It lets your AI client calculate total durations, check against labor regulations, and flag unusually long breaks. Instead of manual spreadsheets, you use your agent to audit time logs and ensure everyone stays within legal limits.

A+ Quality Score 100/100

time-tracking | compliance | breaks | workforce | statistics

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · SEPTEMBER 2026
vinkius.com/en/ai-agent-connect/break-time-total

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.

# break-time-total MCP

4 tools available
Cloud-hosted on Vinkius

Managing break times shouldn't be a manual math problem. This MCP gives your AI client the ability to process break logs and turn them into actionable compliance data. You can hand over a list of timestamps or durations, and your agent will immediately tell you if a worker has exceeded their allowed time or if certain breaks are hitting a threshold that needs attention. It is built for anyone managing shifts who needs to ensure labor laws are followed without spending hours on a calculator. Whether you are looking for a quick summary of daily breaks or need to find specific outliers in a large dataset, this tool handles the heavy lifting. You just provide the data, and your agent provides the answers.

## Core Capabilities

**01 — Duration Aggregation**

Your agent uses this to add up multiple break periods into a single total.

**02 — Compliance Auditing**

The AI checks total break times against specific legal or company limits.

**03 — Outlier Detection**

Your agent identifies individual breaks that exceed a specific length.

**04 — Statistical Reporting**

The tool provides a high level summary of break patterns in a dataset.

## One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/break-time-total** — connect your AI agent in three steps.

01 Connect your preferred MCP client to Vinkius.

02 Provide your break duration data to your AI agent.

03 Ask the agent to calculate totals or check compliance.

04 Receive the processed results directly in your chat interface.

Connect your AI client to Vinkius and start querying your break data immediately.

## Built For

This MCP is for managers and HR professionals who need to monitor time logs for compliance.

**Operations Managers**

They hand off shift logs to the AI to check for labor law violations.

**HR Specialists**

They use the tool to audit employee break patterns and compliance.

**Payroll Administrators**

They use the math tools to verify break durations before processing pay.

## What Changes When You Connect

| | |
|---|---|
| 01 | Automates the math for cumulative break durations. |
| 02 | Flags breaks that exceed specific time thresholds. |
| 03 | Validates total break times against regulatory limits. |
| 04 | Provides statistical summaries of break data instantly. |

## Real-World Applications

**Labor Law Compliance**

Check if employee break totals stay within legal requirements for your region.

**Shift Auditing**

Identify specific employees who are taking breaks that exceed company policy.

**Payroll Verification**

Confirm that total break times match the logged hours for a pay period.

**Workforce Analytics**

Get a statistical overview of how much time is being spent on breaks across a team.

## Patterns to Avoid

### Manual math errors

✕ AVOID

You try to manually add up a spreadsheet of timestamps to see if a worker went over their limit.

✓ INSTEAD

Let your agent do the math by using calculate_total_break_time to get an exact sum of all durations.

### Ignoring specific outliers

✕ AVOID

You look at a general summary but miss the one employee who took a three hour break.

✓ INSTEAD

Use filter_breaks_by_threshold to isolate only the specific break periods that exceed your set limits.

### Guessing compliance status

AVOID

You assume a shift was compliant because the total time looks okay at a glance.

✓ INSTEAD

Run validate_break_compliance to confirm the total time actually stays within your specific regulatory limits.

## The Right Fit

Operations managers and HR professionals should connect this MCP if they handle shift logs and need to ensure labor law compliance. If you don't manage time-sensitive break data or don't need to audit employee patterns, you don't need this.

# break-time-total MCP Tools

These tools handle the math and logic for analyzing break logs. Your agent uses them to aggregate durations, find outliers, and check for compliance.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `calculate_total_break_time` | This tool sums up a list of break durations to find the total time spent away from work. |
| 02 | `filter_breaks_by_threshold` | Use this to pull out specific break periods that are longer than a set limit. |
| 03 | `get_break_summary` | This tool generates a statistical overview of all provided break data. |
| 04 | `validate_break_compliance` | This tool checks if the total break time stays within a specific regulatory limit. |

# See It in Action

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

**U** What is the total time for breaks of 10, 15, and 25 minutes?

The total duration is 50 minutes (00:50).

**U** Are my breaks compliant if I took 60 minutes of breaks and the limit is 45?

No, you have exceeded the limit by 15 minutes.

**U** Find any breaks longer than 20 minutes in this list: 5, 25, 10, 30.

The breaks exceeding the threshold are 25 and 30 minutes.

# Frequently Asked Questions

01 **How do I use this MCP with Claude?**

You connect your Claude client to Vinkius once, and the break-time-total tools become available for your agent to use in any conversation.

02 **Can I check if a specific employee is compliant?**

Yes. You can provide the employee's break durations to your agent and use the validation tool to check them against a limit.

03 **Does this MCP handle the math for me?**

Yes. The calculate_total_break_time tool performs the summation of all provided break durations.

04 **Can I find long breaks in a large list?**

Yes. You can use the filter tool to identify any break periods that exceed a specific threshold you set.

05 **What kind of data does the tool need?**

The tools require lists of break durations or timestamps to perform calculations and compliance checks.

06 **How do I calculate the total time spent on breaks?**

You can use the `calculate_total_break_time` tool by providing a list of break durations in minutes.

07 **Can I check if my breaks comply with labor laws?**

Yes, the `validate_break_compliance` tool allows you to check if your total break time is within a specific maximum limit.

08 **How can I see a summary of all breaks taken?**

The `get_break_summary` tool provides a full statistical overview, including the count, total time, average duration, and the longest break.

# 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 `"break-time-total": { "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

# break-time-total 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 →**

## INDEPENDENT PLATFORM DISCLAIMER



## DOCUMENT INFORMATION

| | |
|---|---|
| Generated | September 2026 |
| MCP Server | break-time-total MCP |
| Server ID | `01a0c7cd-9e00-715b-950e-630f30c785ff` |
| Platform | Vinkius Cloud for AI Agents |
| Endpoint | `https://edge.vinkius.com/{token}/mcp` |

## LICENSE & USAGE