MCP SERVER | NO CODE | CLOUD HOSTED

Code Climate MCP for AI Agents

Monitor Code Quality and Engineering Metrics Across Repositories

Code Climate MCP lets your AI client govern code quality metrics directly from chat. It connects to Code Climate data, giving you immediate visibility into repository grades, test coverage percentages, and technical debt across all your projects. Stop clicking through dashboards; start asking questions about how healthy your codebase is.

F Quality Score 3.11/100

engineering-metrics | code-maintainability | test-coverage | software-intelligence | repository-analytics | dev-productivity

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/code-climate

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.

Code Climate MCP

8 tools available
Cloud-hosted on Vinkius

Managing code quality shouldn't require a dozen open tabs or deep dives into complex CI/CD dashboards. This MCP connects Code Climate to any AI agent you use, giving you natural language control over your engineering metrics. You can ask your client things like, 'What is the maintainability grade for our payment service?' and get an instant answer based on historical data. It lets you audit test coverage reports or list all technical debt issues found in a specific commit snapshot without ever logging into the Code Climate dashboard itself.

This connection turns complex code analysis into a simple conversation. Whether you're checking compliance grades, reviewing recent snapshots, or monitoring webhook status for DevOps tasks, your AI agent handles the heavy lifting. It’s one of the most useful tools in the Vinkius catalog for any development team that needs real-time visibility into their codebase health.

Core Capabilities

01 — Check repository grade and overall quality

Get a summary of code quality information, including grades and metrics, for an entire project.

02 — Review specific analysis snapshots

Access detailed insights from historical or current Code Climate analyses to track how quality changes over time.

03 — Audit technical debt issues

List all specific code problems and findings identified within a particular snapshot, helping developers prioritize fixes.

04 — Monitor test coverage reports

Retrieve comprehensive lists of test coverage data to ensure your software meets quality standards across the board.

05 — View and manage webhooks

List all configured webhooks for a repository, allowing quick auditing of real-time notification setup.

06 — Retrieve user account details

Fetch metadata about the authenticated user profile and organizational settings within your workspace.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and provide your Code Climate Personal API Token (found in User Settings).

02 Your AI client connects using the token, granting it direct access to all your monitored repositories' code quality data.

03 You ask a question—like 'What was the test coverage for project X?'—and your agent pulls the specific report details directly into your chat.

The bottom line is that you get immediate, conversational access to deep engineering metrics without needing to navigate complex web dashboards.

Built For

This MCP is for development teams where code quality isn't a manual process but a constant source of stress. It helps Engineering Managers who need high-level grade reports, DevOps Engineers who are tired of opening multiple dashboards just to check webhook status, and Software Developers who want instant lookups on specific issues or test coverage.

Engineering Manager

Uses the MCP to monitor repository grades and overall maintainability trends across different teams using natural language queries.

DevOps Engineer

Audits configured webhooks and analysis status for multiple repositories directly in chat, eliminating manual dashboard checks.

Software Developer

Quickly looks up specific code issues or test coverage percentages related to a feature branch without leaving their coding environment.

What Changes When You Connect

01 Stop opening multiple dashboards. You ask your agent, 'What's the status of Project X?' and get immediate data using `get_repository_code_quality`.

02 Track how code quality evolves over time by accessing historical analyses through `list_repository_snapshots`, giving you a full audit trail.

03 Prioritize technical debt instantly. Use `list_snapshot_code_issues` to pull up all identified problems for a specific commit, letting your team focus on the highest-impact fixes.

04 Verify test safety easily. Run `list_repository_test_reports` to confirm your branch meets minimum coverage requirements before merging.

05 Audit system connections without logging in. Use `list_codeclimate_webhooks` to confirm that real-time notifications are set up correctly for every project.

Real-World Applications

Checking if a feature branch is safe to merge

A developer asks, 'What's the test coverage on the 'checkout' repository?' Your agent uses `list_repository_test_reports` and reports that it's at 82%, which is above the required minimum of 75%. The merge can proceed.

Investigating a sudden dip in code quality

An Engineering Manager asks, 'Show me all issues found after the last deployment.' Your agent uses `list_snapshot_code_issues` to pull up 15 critical findings from the snapshot taken yesterday.

Understanding historical maintainability

A team lead asks, 'How did Project Alpha's grade change last quarter?' Your agent uses `list_repository_snapshots` to compare the current grade against the one found six months ago.

Verifying deployment readiness for a microservice

A DevOps Engineer asks, 'Are all webhooks set up for Project Beta?' Your agent uses `list_codeclimate_webhooks` and confirms that the webhook is active and pointing to the correct CI/CD endpoint.

Patterns to Avoid

Manually checking every repository

✗ AVOID

Having to visit 12 different project dashboards just to check if all repositories are above an 'A' grade. This takes hours of clicking and copying data.

✓ INSTEAD

Ask your agent to run `list_codeclimate_repositories` first, then ask for the quality status of any specific one. You get a summary instantly.

Confusing general metrics with specific issues

✗ AVOID

Seeing that 'Project Gamma' has a low grade but not knowing *why*. The dashboard shows 50 issues, but you don't know which ones are critical.

✓ INSTEAD

First, use `list_repository_snapshots` to find the relevant time period, then run `list_snapshot_code_issues` to get a prioritized list of technical debt.

Relying on stale coverage numbers

✗ AVOID

Assuming the test coverage is good because it was last week's number. You need to know if the tests are still current.

✓ INSTEAD

Use `list_repository_test_reports` to ensure you are looking at the most recent, relevant report data.

The Right Fit

Use this MCP when your primary pain point is visibility across multiple code repositories. If you need to compare maintainability grades or audit test coverage against historical benchmarks, this tool is essential. However, don't use it if you only need basic information about a single file structure or local environment variables; those are outside its scope. Also, understand that while `list_codeclimate_repositories` gives you the list of projects, running actual quality checks requires subsequent calls to tools like `get_repository_code_quality`. This MCP is for auditing and reporting, not for writing code itself.

Code Climate MCP: Auditing Code Quality Metrics in Software Engineering

Today, checking the health of your codebase means logging into a dashboard, navigating to the correct repository, finding the right snapshot, and manually comparing grades, coverage percentages, and issue counts. It's tedious work that breaks focus and slows down decision-making.

With this MCP, you simply ask your agent, 'What is the technical debt status of the auth service?' Your AI client executes the necessary tools like `list_snapshot_code_issues` and delivers a concise report in plain language. You get immediate answers without clicking through any dashboards.

Code Climate MCP: Managing Test Coverage and Compliance Audits

Manually tracking whether every component meets the minimum test coverage threshold is a constant chore. You have to wait for CI/CD reports, then manually cross-reference those numbers across multiple repositories.

This MCP lets you confirm compliance on demand. By running `list_repository_test_reports`, your agent pulls the precise, latest data and confirms if the repository meets its coverage goals right in your chat window. You know instantly if you're safe to merge.

8 Tools in Code Climate for Repository Analytics & Code Quality Metrics

Use these tools to list repositories, check specific code quality scores, audit technical debt, or review historical analysis snapshots.

#	TOOL	DESCRIPTION
01	`get_my_codeclimate_profile`	Retrieves basic information about your own user account profile on Code Climate.
02	`get_repository_code_quality`	Fetches detailed code quality metrics, including grades and maintainability scores, for a specific repository.
03	`get_snapshot_quality_details`	Provides comprehensive information about a single analysis snapshot from the Code Climate history.
04	`list_snapshot_code_issues`	Lists all identified code issues and technical debt findings for a given analysis snapshot.
05	`list_codeclimate_repositories`	Retrieves a list of every repository that Code Climate is currently analyzing.
06	`list_repository_snapshots`	Gets a chronological list of all available analysis snapshots for a specific project.
07	`list_repository_test_reports`	Retrieves and lists the test coverage reports associated with a particular repository.
08	`list_codeclimate_webhooks`	Displays all webhooks that are currently configured for real-time analysis notifications on a repository.

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 current grade for our main API gateway?

Code Quality Report: Main API Gateway

- **Overall Grade:** B+
- **Maintainability Score:** 78/100 (Up from 75 last month)
- **Critical Issues Found:** 4 (Requires immediate attention)

Need a deep dive on those critical issues? Just ask me to list them.

U Show me the test coverage for 'user-profile' last week.

Checking historical reports for user-profile...

The most recent report (Snapshot ID: abc1234) shows 91% overall coverage. This is a solid improvement of 3% from the previous month's analysis. Good work!

U List all technical debt issues for the payments module.

Technical Debt Report: Payments Module

Found 8 total issues in the last snapshot:

- **Critical:** Missing unit tests (2 instances)
- **Major:** Outdated dependencies (3 instances)
- **Minor:** Code smell detected (3 instances)

Focusing on those critical test gaps should be the top priority for this sprint.

Frequently Asked Questions

01 **How does Code Climate MCP help me check code quality metrics?**

This MCP gives you immediate, natural language access to your codebase health. Instead of opening dashboards, you simply ask your agent for the repository grade or maintainability score and get a direct answer.

02 **Can I use Code Climate MCP to track test coverage reports?**

Yes. You can retrieve and monitor test coverage data instantly by asking about specific repositories. It shows you percentage increases or drops, which is critical for compliance.

03 **What if I need historical code quality data from Code Climate MCP?**

You can access past analyses using the MCP. By referencing snapshot details, your agent pulls up how the grade or issue count looked months ago, making long-term trend analysis simple.

04 **Does Code Climate MCP help me manage technical debt?**

Absolutely. The MCP lets you list all identified code issues for any snapshot. This helps teams prioritize which technical debt needs fixing first, turning massive dashboards into actionable lists.

05 **What kind of role is Code Climate MCP best for?**

It's perfect for Engineering Managers and DevOps Engineers who need high-level oversight across dozens of projects without spending all day clicking buttons in separate tools.

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 `"code-climate": { "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

Code Climate 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 Code Climate. 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	Code Climate MCP
Server ID	`019d7576-330f-7028-8748-25278968e156`
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/code-climate.