MCP SERVER | NO CODE | CLOUD HOSTED

Codacy MCP for AI Agents

Monitor repository grade, security, and technical debt metrics

Codacy MCP lets you manage automated code reviews and track quality metrics using natural conversation. Instead of diving into dashboards, your AI client pulls up a repository's grade, finds specific security issues, or lists all organizations associated with your account instantly.

F Quality Score 11.43/100

code-quality | static-analysis | security-scanning | automated-reviews | repository-monitoring | technical-debt

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

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.

Codacy MCP

8 tools available
Cloud-hosted on Vinkius

Stop switching between tabs just to check if the latest commit broke something. This MCP lets you take full control of code quality and maintainability by talking to your agent. You can ask it to pull up the current grade for any repository, search across multiple orgs for specific vulnerability types, or even see which languages Codacy supports natively.

It’s about moving complex audit work into a simple conversation. Your AI client connects through Vinkius, giving you deep visibility into your codebase's health without ever needing to open the main web portal. You can quickly monitor configured webhooks for real-time alerts or list out all members across an entire organization roster.

Core Capabilities

01 — Assess overall repository grade and metrics

Get the current quality score and detailed analysis for any specific code repository.

02 — Search for precise security or technical issues

Find code quality problems by filtering on criteria like severity level, category, or programming language.

03 — Map out your entire organizational structure

List all organizations connected to your account and retrieve the full membership roster for any of them.

04 — Audit repository setup and webhooks

View which webhooks are currently configured for a given repository, ensuring you get real-time quality notifications.

05 — Determine supported coding standards

List every programming language that the Codacy analysis engine can process and grade.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius.

02 Input your Codacy Account API Token (you'll find this in User Settings > API).

03 Use the connection through your preferred AI client (Cursor, Claude, etc.) to start asking questions about code quality.

The bottom line is you use natural language conversation to pull detailed code metrics and audit information without opening a browser tab.

Built For

This MCP is for the DevOps Engineer who needs an instant audit of webhooks; the Security Team that must verify compliance across multiple repos; or the Engineering Manager who wants to track quality trends using only conversation. It cuts out the clicks.

DevOps Engineer

Auditing repository webhook status and checking overall analysis status without logging into the main dashboard.

Security Team Lead

Verifying repository compliance by searching for specific vulnerability findings across different services.

Software Developer

Quickly looking up specific code quality issues or security alerts directly from their chat interface while writing code.

What Changes When You Connect

01 Instantly check any repo's status. Instead of navigating to a dashboard, you ask the agent for `get_repository_quality_analysis` and get the current grade in one go.

02 Audit compliance across teams. Use `list_codacy_organizations` to map out every connected organizational unit without manual enumeration.

03 Pinpoint security flaws fast. You can use `search_repository_issues` to filter for 'Critical' vulnerabilities by category or language instantly.

04 Understand your scope. Quickly run `list_organization_repositories` to see a full inventory of all analyzed codebases in an organization.

05 Stay current with integrations. Use `list_repository_webhooks` to verify that real-time quality notifications are correctly configured.

Real-World Applications

Need to check the compliance status for a new team

An Engineering Manager needs to know if all ten microservices have passed their required security checks. They ask the agent, and it runs `list_organization_repositories`, then uses `get_repository_quality_analysis` on each one, delivering a single summary report.

Finding hardcoded secrets across multiple services

A Security Team member needs to audit ten repos for specific secret leaks. They use `search_repository_issues`, filtering by 'hardcoded' and 'Critical' severity, getting a list of exact locations they need to fix.

Onboarding new team members quickly

A DevOps Engineer needs to verify which teams are part of the project. They run `list_organization_members` to get the full roster, and then use `get_my_codacy_profile` to confirm their own access level.

Confirming all necessary alerts are firing

A DevOps Engineer suspects a repository is missing webhook notifications. They check this by running `list_repository_webhooks` and confirming the status for quality analysis updates.

Patterns to Avoid

Checking grades repo-by-repo

✗ AVOID

Manually logging into Codacy, selecting Repo A, checking grade. Logging out, going to Repo B, checking grade, repeating this process for every service.

✓ INSTEAD

Instead of repetitive checks, use the agent to first run `list_organization_repositories`, gather the list, and then ask it to check the quality metrics for all listed repositories in one call.

Searching issues without filters

✗ AVOID

Running a general issue search that returns thousands of results, forcing you to scroll through low-priority warnings just to find the two critical bugs.

✓ INSTEAD

Use `search_repository_issues` and specify advanced filters. For example, filter by 'level: Critical' AND 'category: Security' for immediate focus.

Missing organizational context

✗ AVOID

Assuming all teams are under one umbrella and missing the roster or identifying which organization owns a specific piece of code.

✓ INSTEAD

Always start by running `list_codacy_organizations` to get the full scope, then use `list_organization_repositories` to drill down into ownership.

The Right Fit

Use this MCP if your job involves frequent auditing, compliance checks, or needing a unified view of code health across many repositories. You need to know *what* the grade is and *why*. Don't use it if you just want to write some simple documentation; those tasks are better handled by general knowledge retrieval tools. If your primary goal is simply writing new code without auditing concerns, you don’t need this MCP. But if you frequently run into issues like 'Where do I check the grade for 50 repos?' or 'What was the last security finding in the billing service?', then `get_repository_quality_analysis` and `search_repository_issues` are exactly what you need.

Codacy MCP: Auditing Code Quality and Technical Debt

Today, checking the overall health of a codebase feels like detective work. You have to open the dashboard, click through multiple repositories, manually compare grades, and cross-reference different security findings. It’s slow, tedious, and you often miss the 'why' behind a low score.

With this MCP, you talk to your agent instead. You ask it to run `get_repository_quality_analysis` for a whole suite of services. The agent handles the manual clicks, gathers all the grades and metrics, and hands you a clean summary report. It turns hours of clicking into a simple question.

Codacy MCP: Managing Code Security and Vulnerability Findings

Manually tracking down specific vulnerabilities is a nightmare. You have to remember if the issue was categorized as 'SQL Injection,' or if it hit a certain development branch, making comprehensive auditing nearly impossible.

This MCP fixes that with `search_repository_issues`. You tell your agent: 'Show me all Critical SQL injection issues in the marketing repo.' It filters everything down instantly and gives you actionable data. Your focus shifts from searching to fixing.

Codacy MCP: 8 Tools for Code Quality Analysis

Use these tools to get repository grades, search specific issues, list organizations, and manage user details via chat commands.

#	TOOL	DESCRIPTION
01	`get_repository_quality_analysis`	Retrieves the current grade and key metrics for a specified repository.
02	`list_supported_languages`	Returns a list of all programming languages supported by Codacy analysis.
03	`get_my_codacy_profile`	Pulls user profile information for the authenticated Codacy account.
04	`list_codacy_organizations`	Provides a list of all organizations associated with the connected account.
05	`list_organization_members`	Retrieves the names and profiles of users belonging to a specific organization.
06	`list_organization_repositories`	Lists all repositories that have been analyzed within a given organization.
07	`list_repository_webhooks`	Shows the currently configured webhooks for quality notification purposes on a repository.
08	`search_repository_issues`	Searches and filters code quality issues within a specific repository based on criteria like level or category.

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 overall quality grade for our core services?

Codacy Quality Report

REPOSITORY	GRADE	PRIMARY CONCERN
`core-api`	A	Minor refactoring needed
`web-frontend`	B	High count of Medium security issues
`billing-service`	C+	Critical vulnerability found (SQL)

Summary: The billing service needs immediate attention due to a critical finding. I recommend starting with `search_repository_issues`.

U I need to know what languages are supported for analysis.

Supported Languages List

Codacy analyzes over 40 programming languages, including:

- JavaScript
- TypeScript
- Python
- Go
- Java
- PHP
- Ruby
- C#
- And many configuration files (Dockerfile, Terraform).

U Show me all repos in the 'vinkius' org and their current grades.

Organization Repository Status

I found 5 analyzed repositories under the 'vinkius' organization:

- `core-api` : Grade A (Excellent)
- `web-frontend` : Grade B (Needs Review)
- `mcp-servers` : Grade A (Excellent)
- `auth-service` : Grade C+ (Action Required)
- `logging-tool` : Grade N/A (No analysis found)

Frequently Asked Questions

01 **How does the Codacy MCP help me monitor code quality?**

It lets you ask about your codebase's health using natural language. You can get the current grade for any repository, search for specific security flaws, or audit which languages are supported by Codacy.

02 **Is this MCP useful for auditing compliance?**

Yes. It allows you to list all organizations and repositories connected to your account, letting you systematically check the status of every service against your internal quality standards.

03 **Can I find specific security vulnerabilities using Codacy?**

Absolutely. You can run advanced searches that filter issues by severity level (like 'Critical') or category, helping you pinpoint exactly where the code needs fixing.

04 **What if my team is working on a new service I haven't connected yet?**

You can first use the MCP to list all available organizations and repositories in your account. This gives you a full map of what services are already being monitored.

05 **What kind of information does Codacy provide about users?**

The MCP lets you retrieve member rosters for any organization, giving you the names and profile details of everyone associated with your project.

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 `"codacy": { "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

Codacy 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 Codacy. 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	Codacy MCP
Server ID	`019d7576-17b4-712c-881e-c24764c50575`
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/codacy.