

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

App Permission Review MCP

Verify app permissions against official security requirements.

App Permission Review MCP lets your AI client audit application permission profiles. It compares requested permissions against a registry of approved sets to flag privacy risks and compliance gaps. Your agent can categorize permissions as keep, review, or revoke to ensure apps only access what they actually need.

A+ Quality Score 100/100

audit

permissions

security

compliance

privacy



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

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.

App Permission Review MCP

4 tools available

Cloud-hosted on Vinkius

You can use this MCP to stop apps from overreaching. Instead of manually checking every permission request, you let your AI client do the heavy lifting. It compares the permissions an app claims to need against a strict registry of approved permission sets. If an app asks for more than it should, your agent catches it immediately.

You'll get clear categorizations for every permission: keep, review, or revoke. This makes it easy to spot privacy risks or compliance failures before they become problems. Whether you're auditing a single app or scanning a whole directory, your agent uses this tool to ensure everything stays within official guidelines. It's a direct way to enforce security standards without digging through endless documentation yourself.

Core Capabilities

01 — Permission Auditing

Your agent compares app permission requests against a registry of approved sets.

02 — Requirement Verification

The AI checks if an app's requested access matches its official requirements.

03 — Risk Categorization

Your agent labels permissions as keep, review, or revoke to highlight risks.

04 — Registry Management

The AI accesses a directory of all managed applications and their permission rules.

05 — Permission Validation

Your agent verifies if specific permission strings are valid within the system.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/app-permission-review — connect your AI agent in three steps.

- 01
- Connect your AI client to the Vinkius-hosted MCP.
- 02
- Ask your agent to list apps or fetch requirements for a specific application.
- 03
- Instruct the agent to run an audit on a permission profile.
- 04
- Review the categorized results to identify risks.

You connect the MCP to your AI client and start asking questions about app permissions.

Built For

Security professionals and compliance officers use this MCP to automate the vetting of application access. You can hand off the tedious task of permission mapping to your AI agent.

Security Auditor

Uses the MCP to identify apps that request excessive or unauthorized permissions.

Compliance Officer

Relies on the tool to ensure application permissions meet regulatory standards.

App Developer

Checks their own app's permission profile against the official registry.

What Changes When You Connect

- 01
- Identifies privacy risks by flagging unapproved permission requests.
- 02
- Automates the comparison between requested and required permission sets.

- 03

Categorizes risks into actionable keep, review, or revoke statuses.
- 04

Provides a centralized registry of approved application requirements.

Real-World Applications

Security Auditing

Run a full audit on a new application to see if its permission profile matches its intended use.

Compliance Monitoring

Check if existing applications still adhere to the official permission registry.

Permission Validation

Verify if a specific permission string is valid before implementing it in a new app.

App Inventory Management

Use the app directory to see all applications currently being managed for permissions.

Patterns to Avoid

Manual Permission Comparison

❌ AVOID

You spend hours cross-referencing an app's requested access against a PDF of approved permissions.

✓ INSTEAD

Let your agent handle the comparison by using `analyze_app_permissions` to run a full audit against approved standards.

Guessing Permission Validity

❌ AVOID

You assume a permission string is valid and try to implement it in a new application build.

✓ INSTEAD

Verify the string is recognized in the global domain context first with `search_permission_by_name`.

Blind App Deployment

❌ AVOID

You deploy a new app without checking if its permission profile matches its intended use.

✓ INSTEAD

Use `get_app_requirements` to pull the official baseline for that specific application before you approve it.

The Right Fit

Security auditors and compliance officers should connect this MCP to automate permission vetting. General users without a need for strict access control or permission auditing won't find value here. The decision depends on whether you need to enforce a strict registry of approved permission sets.

App Permission Review Tools for Automated Auditing

These tools allow your agent to audit app profiles, check permission strings, and pull official requirement registries.

#	TOOL	DESCRIPTION
01	list_all_apps	This tool provides a directory of every application currently managed in the permission registry.
02	get_app_requirements	This tool pulls the official list of approved permissions for a specific application. It provides the baseline for your audit.
03	search_permission_by_name	This tool checks if a specific permission string exists in the global domain context. Use it to verify if a permission is recognized.
04	analyze_app_permissions	This tool runs a full audit on a specific application's permission profile. It compares the app's requested access against approved standards.

See It in Action

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

U Audit the permissions for 'PhotoEditorApp' with permissions: ['camera', 'location', 'contacts'].



The audit for PhotoEditorApp is complete. Keep: ['camera']. Review: ['location', 'contacts']. The app is marked as unapproved due to the extra permissions requested.

U What are the required permissions for 'WeatherService'?



The required permissions for WeatherService are: ['location', 'network'].

U Is 'biometric_auth' a valid permission?



Yes, 'biometric_auth' is a recognized permission under the 'Security' category.

Frequently Asked Questions

01 What does this MCP do?

This MCP audits application permissions by comparing them against a registry of approved permission sets to find security and privacy risks.

02 How are permissions categorized?

The tool categorizes permissions into three statuses: keep, review, or revoke.

03 Can I check if a permission is valid?

Yes, you can use the search tool to check if a specific permission string exists within the global domain context.

04 Which AI clients can use this MCP?

You can use this MCP with any compatible client like Claude, Cursor, Windsurf, or VS Code.

05 Do I need to host the MCP myself?

No, Vinkius hosts and manages the MCP for you. You just connect your client and start using the tools.

06 How do I audit a specific application?

You can use the `analyze\_app\_permissions` tool by providing the application name and the list of permissions you want to check.

07 What does 'Review' status mean?

A 'Review' status indicates that the application has requested a permission that is not found in its official required permission list, signaling a potential security risk.

08 Can I see all available apps in the registry?

Yes, use the `list\_all\_apps` tool to retrieve a directory of all applications currently managed within the permission registry.

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>"app-permission-review": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

App Permission Review 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 App Permission Review. 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	October 2026
MCP Server	App Permission Review MCP
Server ID	01a0ee75-799c-7314-8453-34d5c3736f22
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/en/ai-agent-connect/app-permission-review.