MCP SERVER | NO CODE | CLOUD HOSTED

ORCID MCP

Verify and map professional research identities.

ORCID connects your AI client directly to the Open Researcher and Contributor ID registry. It lets you search, retrieve, and manage professional academic data for any researcher globally. Quickly access biographical details, track publications, and map complex research affiliations across multiple institutions.

A+ Quality Score 98.33/100

researcher-id | academic-publishing | data-attribution | scholarly-records | biographical-data | persistent-identifier

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

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.

ORCID MCP

13 tools available
Cloud-hosted on Vinkius

Need to verify who a scholar is or what they've published? This MCP connects your AI client directly to the ORCID registry. You can find researchers anywhere in the world by searching names, emails, or specific identifiers. Once you have an ID, you can retrieve full summaries of their professional profiles—including everything from institutional affiliations to publications and funding sources.

It's more than just a profile viewer; it lets you track all activity associated with that researcher. For advanced users, the MCP also allows direct management: creating, updating, or deleting items on a record if you have the necessary access tokens. By connecting this through Vinkius, your AI agent gains visibility into scholarly records across disciplines and borders—all without needing to navigate complex academic databases manually.

Core Capabilities

01 — Search the global registry

Find specific researchers or groups of scholars using name, email, or keyword searches.

02 — Retrieve full professional profiles

Fetch complete biographical records and summaries for a given ORCID ID.

03 — Track academic activity

Gather detailed lists of all associated works, funding grants, and institutional affiliations.

04 — Manage researcher items

Authorized users can create, update, or delete specific sections on a record to keep data current.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your ORCID Access Token (either Public or Member API).

02 Tell your AI client the researcher's identifier, name, or email.

03 The agent executes a query against the registry and returns structured academic data.

The bottom line is that you get verifiable, standardized scholarly records directly into your workflow.

Built For

University administrators who struggle to compile accurate faculty reports or data scientists building bibliometric models. If your job involves mapping academic networks or validating a researcher's credentials, you need this.

Academic Administrator

Automate the collection of faculty activity and affiliation records for annual reporting and grant submissions.

Bibliometric Data Scientist

Search and analyze researcher metadata across large datasets to map scientific connections or track field growth.

Research Librarian

Verify profile data for authors or departments, ensuring accurate citation records and institutional alignment.

What Changes When You Connect

01 Verification: Use `get_person` to instantly pull a researcher's verified name, email, and associated IDs, eliminating manual data entry.

02 Tracking: Run `get_activities` to get a complete list of all publications, grants, and institutional roles tied to one ID.

03 Deep Data Dive: Need more than a summary? Use `expanded_search` or `get_item` to pull granular metadata on specific works or funding sources.

04 Bulk Processing: Run `csv_search` when you need to analyze hundreds of records at once, getting the data ready for spreadsheet analysis.

05 Data Maintenance: If your system needs to correct an entry, use `update_item` or `create_item` (if authorized) to keep the profile accurate.

Real-World Applications

Onboarding a New Faculty Member

A University Administrator needs to build a department directory. Instead of emailing every faculty member for CVs, they use `search` with known departmental emails and then run `get_record` on the top results. This instantly compiles verified names, past affiliations, and key publications into one source.

Tracking a Citation Chain

A Data Scientist finds an old paper cited in their work. They use `search` with keywords from that paper to find the original author's ORCID ID, then run `get_activities` to see all subsequent works and funding records by that researcher.

Creating a Program Report

A Research Librarian needs to prove which authors contributed to a multi-institutional project. They use the ORCID ID of each major contributor to run `get_section` for 'Works', guaranteeing they capture every publication listed against that specific ID.

Validating Grant Eligibility

A funding body must verify a PI's history. They use `search` and then `get_summary` to ensure the researcher's current institutional affiliation matches the grant application requirements, validating their professional standing.

Patterns to Avoid

Relying on name searches alone

✗ AVOID

Asking your agent to 'find all papers by John Smith and Jane Doe'. This is too vague; the registry has thousands of Johns Smiths.

✓ INSTEAD

Always start with a specific identifier. Use `search` combining names *and* an email, or better yet, use the known ORCID ID, then run `get_activities` to list works.

Assuming public data is current

✗ AVOID

Copying old affiliation details from a website and assuming they're right. Profiles change constantly.

✓ INSTEAD

To get the most reliable, validated status, use `get_summary` or `get_person`. This pulls the official record directly from ORCID.

Using general database searches

✗ AVOID

Searching a local university directory that might miss international collaborations or recent grants.

✓ INSTEAD

This MCP accesses the global ORCID registry. Use `search` to ensure you are viewing the complete, globally recognized record.

The Right Fit

Use this MCP if your core task involves verifying academic identity, mapping publication history, or tracking affiliations for a scholar. If your data set is already contained within one institution's local database and doesn't need global validation, you don't need ORCID. You should only use ORCID when the provenance of the researcher—who they are globally, what they have published across borders, and where their work originated—is critical to your output. If you just need a name or department phone number, that's fine for general search tools; but if you need proof of scholarly identity, this MCP is essential. Never use ORCID if you only want basic contact info without any academic context.

The Problem with Disconnected Research Records

Today, compiling a complete profile for an academic requires juggling five different systems: the university's HR portal, institutional publication databases, grant funding sites, and personal CV websites. You spend hours copy-pasting names, cross-referencing affiliations, and guessing if a paper was listed under the correct primary author.

With this MCP, you bypass all that manual work. Your agent queries ORCID directly, gathering verified data points—publications, roles, funding—into one clean stream. You get a unified view of scholarly life instantly.

ORCID: Standardizing Academic Identity

The manual steps that fall away include searching multiple institutional databases and reconciling conflicting author names (e.g., 'J. Smith' vs. 'Johnathan J. Smith'). You never have to worry about which John Smith you are looking at again.

You now work with a single, persistent identifier for every scholar. This changes everything; it means your output is verifiable and globally consistent.

ORCID: 13 Tools for Academic Data Management

These tools let you search the ORCID registry, pull biographical details, list works, or even manage records directly using your AI agent.

#	TOOL	DESCRIPTION
01	`create_item`	Adds a new piece of information to a specific section of a researcher's record (requires Member API access).
02	`csv_search`	Searches the ORCID registry and returns all results in CSV format for easy bulk download.
03	`delete_item`	Removes an existing item from a researcher's record section (requires Member API access).
04	`expanded_search`	Searches the ORCID registry and returns detailed, expanded metadata for matching records.
05	`get_activities`	Retrieves a summary list of all activities linked to an ORCID ID, including works and funding.
06	`get_item`	Gets the full metadata for one specific piece of data using its unique put-code.
07	`get_person`	Fetches the basic biographical section containing names and email addresses for a researcher.
08	`get_record`	Retrieves a high-level summary view of the entire ORCID profile record.
09	`get_section`	Gets a summary of one specific section (like Works or Funding) on an ORCID record.
10	`get_summary`	Retrieves the validated and self-asserted summary data for a researcher's profile (requires Member API access).
11	`register_webhook`	Sets up a callback URL so ORCID can notify you when a record changes (requires Premium Member API).
12	`search`	Searches the entire ORCID registry using specific criteria like names, emails, or keywords.
13	`update_item`	Modifies an existing piece of information within a researcher's section (requires Member API access).

See It in Action

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

U Search the ORCID registry for researchers with the family name 'Einstein'.

I've searched the registry. I found several records, including 'Albert Einstein' (ORCID: 0000-0001-XXXX-XXXX). Would you like me to fetch the full record summary for this iD?

U Get the biographical details for ORCID iD 0000-0002-1825-0097.

Fetching biographical data using `get_person` ... The record belongs to Josiah Carberry. It includes verified names, associated email addresses, and a list of other identifiers like Scopus Author ID.

U List all the works associated with ORCID 0000-0002-1825-0097.

I've retrieved the 'works' section. There are 12 items listed. Notable titles include 'Toward a Unified Theory of High-Energy Metrology'. Would you like the full details for any specific work?

Frequently Asked Questions

01 **How do I search the ORCID registry using the ORCID MCP?**

You use the `search` tool by providing criteria like a name, email address, or family name. The agent returns potential matches, which you can then use to fetch specific records.

02 **Does the ORCID MCP allow me to see all of a researcher's publications?**

Yes, running `get_activities` gathers summaries of works and grants associated with the ID. You can also run `get_section` specifically for 'Works'.

03 What is the difference between `get_record` and `expanded_search` in ORCID?

`get_record` provides a quick, high-level summary view of the profile. `expanded_search` gives you much deeper metadata for more detailed analysis.

04 Can I use the ORCID MCP to update a researcher's information?

Yes, tools like `create_item`, `update_item`, and `delete_item` allow authorized users to manage sections of the record. Note that these require specific Member API access.

05 Do I need an ORCID ID to use this MCP?

While you can search using names or emails, having the specific 16-digit ORCID iD and running `get_record` is the most direct and accurate way to pull a full profile.

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 `"orcid": { "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

ORCID 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 ORCID. 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	ORCID MCP
Server ID	`019e38d0-9b54-715c-bf35-c1674736b6db`
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/orcid.