MCP SERVER | NO CODE | CLOUD HOSTED

ORCID (Researcher IDs) MCP

Verify scholarly profiles and track research output.

ORCID (Researcher IDs) connects your AI agent directly to the global ORCID registry. Use this MCP to search for researchers, pull biographical data, and track scholarly work and funding history across academic records.

A+ Quality Score 98.33/100

researcher-search | academic-profile | solr-search | funding-data | scholarly-ecosystem | data-retrieval

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

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 (Researcher IDs) MCP

14 tools available
Cloud-hosted on Vinkius

This connector gives you immediate access to the massive network of researcher identifiers managed by ORCID. You can ask your AI client to find specific scholars using simple searches or dig deep into a full profile. It pulls everything from general life details—like institutional affiliations and biographical summaries—to highly specific data, such as listing an author's entire body of published works or tracking their grant funding history. When you connect this MCP via Vinkius, your agent handles all the complex queries, letting you work with validated scholarly records right where you are.

Core Capabilities

01 — Search for researchers

Find scholars by name, institution, or keywords using standard and expanded registry searches.

02 — Retrieve full profiles

Fetch comprehensive records that include biographical details and a summary of all associated activities for one researcher ID.

03 — List publications and works

Get a summary list of specific research outputs or scholarly articles tied to an ORCID profile.

04 — Review funding history

Access details about the grant funding associated with a researcher's work.

05 — Manage records (requires membership)

Add, update, or delete items on a record if your agent has the necessary API permissions.

One Click on Vinkius — From Prompt to Execution

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

01 First, connect this MCP by providing an ORCID Access Token (either Public or Member API) to Vinkius.

02 Next, tell your AI client exactly what you need—for example, 'Find the works for researcher X' or 'Search for all authors from University Y'.

03 Your agent executes the specific tool call and returns structured data containing the requested biographical details, publication lists, or funding information.

The bottom line is that you get reliable, standardized scholarly metadata without leaving your primary workflow.

Built For

This MCP serves academic researchers who need to verify their publication history; librarians handling institutional data; and grant officers verifying credentials. If your job involves tracing intellectual property or tracking scholar output, this is for you.

Academic Researcher

Uses the tool to quickly find collaborators' ORCID IDs and pull verifiable lists of their published works.

Librarian or Data Manager

Automates the retrieval of institutional research outputs and metadata, saving hours of manual database querying.

Grant Officer / Administrator

Verifies researcher credentials and tracks funding history against grant requirements directly within a case management system.

What Changes When You Connect

01 Instead of manually searching multiple databases, your agent uses the `expanded_search` tool to find researchers using advanced criteria like specific keywords or institutions across the entire global registry.

02 You stop copying text from profile pages. By calling `get_record`, you get a structured summary that feeds directly into your report without any formatting issues.

03 For tracking output, use `get_works` to immediately pull a list of publications associated with an ORCID ID, which is far faster than navigating institutional repositories one by one.

04 When managing data integrity, the agent can call `add_item` or `update_item` to ensure that records are kept current and accurate if you have the Member API permissions.

05 Need a snapshot of trust? The `get_summary` tool lets you access validated trust markers on a record in one step, which is critical for compliance reporting.

Real-World Applications

Verifying candidate credentials

A grant officer needs to confirm if a new applicant has published specific types of research. They ask their agent to use `get_works` and cross-reference the results with funding records using `get_activities`. The result immediately confirms eligibility.

Mapping departmental expertise

A librarian needs a list of all faculty who worked on 'quantum computing' in the last five years. They use `expanded_search` to gather initial IDs, then run `get_person` on each one to verify institutional affiliation.

Updating publication details

A researcher realizes a small detail is missing from their profile. Using the agent with Member API scope and calling `update_item`, they add the necessary information directly, avoiding manual web edits.

Bulk data export for analysis

A research team needs to analyze a list of 50 scholars' basic profiles. They use the `csv_search` tool to pull all the relevant names and summary data into one spreadsheet, ready for statistical modeling.

Patterns to Avoid

Treating ORCID as a simple name search

✗ AVOID

Typing 'Einstein' into your agent and expecting it to return all research outputs. It only returns the most basic matching records.

✓ INSTEAD

Use `expanded_search` or specify the full ID when searching by criteria like institution or keyword. Always start with a focused search before requesting a comprehensive summary via `get_record`.

Assuming all data is public

✗ AVOID

Trying to use simple retrieval calls for record management, which will fail because updates require specific token scopes.

✓ INSTEAD

For modifying records, you must explicitly mention that the agent needs Member API access and then utilize `add_item`, `update_item`, or `delete_item`.

Needing data from multiple sources

✗ AVOID

Trying to get publications from ORCID, funding details from a grant database, and bios from LinkedIn all in one prompt.

✓ INSTEAD

Use this MCP only for ORCID-specific data. If you need to link it to other systems, use the structured output of `get_record` as input for a separate integration tool.

The Right Fit

Use this MCP if your core task is identifying, summarizing, or managing scholarly records tied specifically to an ORCID ID. You need verifiable, standardized data about publications, affiliations, and funding history.

Don't use it if you are looking for general professional networking information (use a dedicated CRM tool) or if you need real-time internal company data (use your company's internal API). If your goal is simply to check if an author exists, the standard `search` tool works fine. But if you need their complete scholarly history, including works and activities, then this MCP's depth is necessary.

Collecting scholar data means juggling five different systems.

Today, getting a full picture of an academic involves logging into multiple sites: the university directory for bios, one journal database for publications, a separate grant portal for funding, and another site just to check affiliations. You spend hours copy-pasting IDs and manually cross-referencing dates.

With this MCP, your agent handles that entire process behind the scenes. You ask it to find everything about a researcher, and you get one clean output containing their profile details, all their works, and their funding records—no jumping between tabs needed.

ORCID (Researcher IDs) MCP delivers verifiable, structured profiles.

The manual steps that disappear are the repetitive searches for 'works' and the tedious effort of summarizing disparate data points. You don't have to manually check if a record has valid trust markers or compile a list of all their associated activities.

Now, you simply state your need—for example, 'Give me the works summary for this ID.' The agent retrieves the precise information using `get_works`, giving you instant, actionable data.

ORCID (Researcher IDs): 14 Tools for Research Data Access

These tools allow your AI client to interact with every facet of the ORCID registry, from basic searches to managing complex records and exporting data.

#	TOOL	DESCRIPTION
01	get_works	Gets a summary list of all research works and publications tied to the ORCID profile.
02	register_webhook	Sets up automated notifications for an ORCID record, requiring premium Member API access.
03	search	Performs a standard search against the main ORCID registry database.
04	unregister_webhook	Removes previously set up automated notifications for an ORCID record (premium access).
05	update_item	Changes the details of an existing item on a researcher's profile, requiring elevated Member API access.
06	add_item	Adds a new item to an existing ORCID record, but requires elevated Member API access.
07	delete_item	Removes an item from an ORCID record, but requires elevated Member API access.
08	expanded_search	Performs a deep search across the entire ORCID registry for broader results.
09	get_activities	Retrieves a high-level summary of every activity associated with a specific researcher record.
10	get_person	Fetches the basic biographical section and details for an ORCID profile.
11	get_record	Retrieves the full, comprehensive summary of a complete ORCID record.
12	get_section_item	Gets detailed information for one specific piece of content or item within an ORCID record.
13	get_summary	Retrieves validated trust markers on a record, requiring elevated Member API access.
14	csv_search	Searches the ORCID registry and returns all resulting data in a CSV file format.

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 for 'Einstein'. The most prominent is Albert Einstein (ORCID: 0000-0001-5109-3700). Would you like to see his full record summary?

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

Retrieving biographical data... For ORCID 0000-0002-1825-0097, the researcher is Josiah Carberry. He is affiliated with Brown University and his research focuses on psychoceramics. Would you like to see his list of works?

U List all research works for ORCID 0000-0003-1415-9265.

Fetching works summary... I found 12 research works for this ORCID iD. Notable titles include 'Advanced Quantum Computing' and 'Neural Network Optimization'. Would you like the full details for any of these using their put-code?

Frequently Asked Questions

01 **How do I use ORCID (Researcher IDs) to search for people?**

You can use either the standard `search` tool or the more powerful `expanded_search` tool. The expanded version gives you broader results, allowing you to filter by keywords or institution.

02 **Does ORCID (Researcher IDs) include funding data?**

Yes, it includes funding history. You can use the agent to retrieve details about associated grant funds and activities via `get_activities`.

03 **Can I update a researcher's record using ORCID (Researcher IDs)?**

You can, but you must have Member API access. Use tools like `add_item`, `update_item`, or `delete_item` when your agent has the necessary permissions.

04 **What is the difference between get_record and expanded_search?**

`expanded_search` finds potential candidates across the whole registry. `get_record` takes a specific ID and returns the complete, detailed profile summary for that single record.

05 **Is ORCID (Researcher IDs) suitable for large-scale data exports?**

Yes. For bulk retrieval of simple records, use `csv_search` to get all results into a CSV format, making it easy to process in spreadsheet software.

06 **Can I search for researchers by their institution or specific keywords?**

Yes! Use the `expanded_search` tool with a Solr query like `affiliation-name:"University of Oxford"` to find researchers associated with specific organizations along with their profile details.

07 **How do I retrieve the full list of publications for a specific ORCID iD?**

You can use the `get_works` tool by providing the researcher's ORCID iD. This will return a summary of all research works associated with that record.

08 **Is it possible to add new research items to an ORCID profile using this server?**

Yes, if you have a Member API access token with the appropriate scopes, you can use the `add_item` tool to add works, funding, or other activities to a record.

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-researcher-ids": { "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 (Researcher IDs) 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

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	ORCID (Researcher IDs) MCP
Server ID	`019e38d1-0537-72ce-b82c-eed669b3434a`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE