MCP SERVER | NO CODE | CLOUD HOSTED

Common Room MCP

Unify every community signal into one actionable source.

Common Room MCP unifies your entire community data—from Slack posts to GitHub commits—into one place. Stop juggling separate dashboards. Your agent connects to Common Room and gives you a single source of truth for every member's activity, relationship history, and current engagement score across all platforms.

A+ Quality Score 100/100

community-intelligence | identity-resolution | signal-processing | b2b-growth | customer-insights | cross-channel

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/common-room-alternative

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Common Room MCP

12 tools available
Cloud-hosted on Vinkius

Your AI client acts as a dedicated community intelligence analyst. Instead of manually checking Slack threads or downloading GitHub reports, your agent reads the data for you. You can ask it to find specific groups—like 'highly engaged power users who haven't talked in three weeks.' It resolves identities across platforms using Person360 technology, meaning it knows that John Doe on Discord is the same John Doe from Slack and GitHub. Need to manage a member? You can programmatically create new profiles or delete old ones if compliance requires it. The whole process happens through natural conversation. Vinkius makes this possible by providing access to Common Room's full catalog, letting your agent handle everything from listing community tags to ingesting brand-new activity signals from any social platform. It's total control over relationship intelligence without leaving your workspace.

Core Capabilities

01 — Build and manage member profiles

The MCP lets you create, update, or remove entire community member records programmatically.

02 — Track cross-platform activity

You can ingest new signals—like a Slack post or social interaction—into a member's timeline history.

03 — Determine community segments

It retrieves and monitors pre-defined groups of users, such as 'At Risk' or 'Highly Engaged,' to assess behavioral health.

04 — List all known tags and segments

You can list existing community tags or defined segment types to guide your analysis.

05 — Monitor API connection status

The MCP lets you check the health of the underlying API token, ensuring continuous data flow.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/common-room-alternative** — connect your AI agent in three steps.

01 First, subscribe to this Common Room MCP on Vinkius.

02 Next, retrieve your dedicated API Token from the platform settings and provide it to your AI client.

03 Finally, use natural language commands in your agent to manage profiles or ingest signals directly.

The bottom line is you tell your AI what data you need—whether it's a list of members or an activity report—and it executes the request across all connected community sources.

Built For

Community Managers who are tired of manually cross-referencing dozens of social channels. DevRel leads needing to track high-impact contributors without switching tabs. Operations staff tasked with maintaining data compliance and member records.

Community Manager

They use the MCP to instantly get complete profile details for a user, checking engagement levels across all platforms in one command.

DevRel Lead

They monitor social signals from multiple channels simultaneously to spot influential contributors and guide marketing outreach.

Operations Specialist

They automate member provisioning by creating new profiles or executing 'Right to be Forgotten' deletions when necessary for compliance.

What Changes When You Connect

01 Stop guessing who your best advocates are. Instead of manually checking multiple social platforms, you can use the MCP to list all members and instantly check their cross-channel engagement levels.

02 Compliance is easier when everything's centralized. When a deletion request comes in, your agent executes 'delete_member,' handling the process cleanly so you don't have to worry about GDPR manually.

03 Keep track of every interaction that matters. You can run 'ingest_activity' whenever new data pops up—whether it's from Discord or an internal tool—keeping member timelines fresh for your outreach team.

04 Target efforts precisely. Instead of sending mass emails, you ask the MCP to list segments, pulling out only the users who are 'At Risk,' so your DevRel team can intervene early.

05 Maintain a perfect record. You never lose context because the system aggregates everything, letting you get complete member details and metadata without any manual data scrubbing.

Real-World Applications

Finding top contributors before a conference

The DevRel team needs to know who their most influential users are for an event. They ask the agent to list segments, filtering only for 'Highly Engaged' members. The MCP replies with the complete profiles of the 20 best candidates, saving days of manual outreach.

Handling a data deletion request

An operational lead receives a legal order to delete a user's profile entirely. They use the agent to execute 'delete_member,' ensuring that all associated metadata is removed programmatically and logged for compliance.

Tracking new viral activity

A key member makes a major announcement on a third-party forum not connected directly. The Ops team uses the MCP to ingest_activity, updating that user's timeline immediately so they can respond with timely support.

Cleaning up old data streams

The company needs to retire an integration webhook. Instead of hunting through dashboard menus, the team uses the MCP to list webhooks and then delete_webhook in one query.

Patterns to Avoid

Treating signals as isolated events

✗ AVOID

A user sees a Slack post about User X's great idea, but has to switch to GitHub and manually search for more activity on that account.

✓ INSTEAD

Instead of switching tabs, ask your agent to get_member details for User X. It compiles the profile with cross-channel context (Slack + GitHub) immediately.

Updating profiles via multiple forms

✗ AVOID

A team member updates a user's role on Slack, then has to go into a separate CRM and manually update that same field.

✓ INSTEAD

Use the MCP's update_member tool. Your agent changes the profile detail in one command, updating the record across all connected systems.

Assuming data consistency

✗ AVOID

A new team member starts and gets added to a group, but their profile is missing key identifiers or metadata.

✓ INSTEAD

Use the create_member tool. This ensures the user's record is fully initialized with all necessary fields from day one.

The Right Fit

Use this MCP if your core pain point is fragmented data across multiple communication channels (Slack, Discord, GitHub). You need to see a single, unified view of a person's history and current engagement level. This tool excels at identity resolution and signal aggregation. Don't use it if you simply need to send a one-off message or just log an event; those are simple messaging tasks handled by other tools. If your only requirement is listing members without needing context like 'At Risk' segmentation, basic directory services might suffice. But if the intelligence layer—the ability to combine signals and manage relationships—is what you need, this MCP is essential.

The Signal Mess: Keeping track of who talks to whom.

Right now, your team wastes hours clicking between Slack, Discord, GitHub, and marketing CRMs. You see a great conversation happen on one platform, but when you need the full picture—the person's history, their other interests, or if they are part of an 'At Risk' segment—you have to copy IDs, open five different tabs, and stitch the narrative together yourself.

With this MCP, that whole process vanishes. Your agent reads all those signals and weaves them into a single profile view. You don't piece together data; you ask for insight. It hands you the complete, organized story of your community member in plain language.

Get Complete Identity Resolution with Common Room MCP

Manually cross-referencing identities is a nightmare: Is 'johndev' on Discord the same person as 'John Doe' in Slack? You have to run multiple manual searches and verify metadata across different systems just to confirm basic identity.

The MCP solves this by using Person360 technology. It resolves those cross-channel identities automatically, giving you a single source of truth for every user relationship without the guesswork.

Common Room with 12 Tools

These tools give your agent direct control over the entire lifecycle of community data, from creating profiles to ingesting signals and managing webhooks.

#	TOOL	DESCRIPTION
01	`create_member`	This tool creates a brand-new profile entry for a community member.
02	`create_webhook`	It sets up a new webhook endpoint to send data notifications from the platform.
03	`delete_member`	This tool permanently removes a member's record, fulfilling GDPR compliance requests.
04	`delete_webhook`	It deletes a previously configured webhook endpoint.
05	`get_member`	You can fetch all detailed information about any specific community member using their identifier.
06	`get_token_status`	This checks the current status and validity of your API access token.
07	`ingest_activity`	It reports a specific activity, like a Slack post or social interaction, to update a member’s timeline.
08	`list_members`	This retrieves a comprehensive list of all community members stored in the system.
09	`list_segments`	It fetches a list of defined user groups, such as 'Highly Engaged' or 'At Risk'.
10	`list_tags`	This retrieves all custom tags currently applied to the community members.
11	`list_webhooks`	It provides a list of all webhooks that are actively configured for data streaming.
12	`update_member`	You can modify specific details, like names or roles, on an existing member's profile.

See It in Action

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

U List all members in the 'Highly Engaged' segment.

I've retrieved the 'Highly Engaged' segment. You have 15 members in this category, including top contributors from GitHub and Slack. Would you like the Person360 profiles for the top 3?

U Get the community profile for 'john@example.com'.

I've located John's Person360 profile. He is active on Slack and GitHub (username: john_dev). His current sentiment is 'Positive' and he is tagged as a 'Power User'. Shall I check his latest activity signals?

U Report a new Slack activity for member ID 'abc-123'.

Activity ingested! I've successfully registered the new Slack signal for member abc-123. The interaction is now visible in their community timeline and engagement score. Need help with other members?

Frequently Asked Questions

01 **How does Common Room MCP resolve different user accounts?**

It uses Person360 technology to link identifiers. It means that even if 'john@example.com' appears on three different platforms, your agent knows it's the same person.

02 **Can Common Room MCP track activities from non-listed sites?**

Yes, you can ingest custom activity signals. The MCP allows you to programmatically feed new interactions into a member's timeline, keeping records current even if they don't use the core platforms.

03 **What is the difference between list_members and get_member?**

list_members gives you a directory of every user. get_member pulls all deep details for one specific user, including their full metadata history.

04 **Is Common Room MCP compliant with GDPR deletion rules?**

Yes. The delete_member tool allows you to execute permanent member removal programmatically, which is necessary for managing data compliance requirements.

05 **How do I set up webhooks using Common Room MCP?**

You use the create_webhook tool to configure a new endpoint. This ensures that when something happens in the community, your system gets an automated notification.

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 `"common-room-alternative": { "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

Common Room 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 Common Room. 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	Common Room MCP
Server ID	`019dd0d5-89f3-71a4-9712-8cf119502e17`
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/common-room-alternative.