

MCP SERVER

NO CODE

CLOUD HOSTED

Memberstack MCP

Manage membership data from natural conversation.

Memberstack MCP gives your AI agent complete control over member authentication and e-commerce data. Use it to manage membership plans, look up user profiles, monitor promotions, and handle custom fields—all through natural conversation. It lets you query active coupons or pull detailed metadata on a specific user's subscription status without ever leaving your chat window.

A+ Quality Score 98.33/100

user-authentication

membership-management

access-control

subscription-billing

member-data



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.

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.

Memberstack MCP

10 tools available
Cloud-hosted on Vinkius

Need to track who belongs and what they paid for? This MCP connects your Memberstack account directly to your AI agent, letting you manage all member data through plain conversation. You can ask your agent to list every active member or search for a user by email to instantly check their subscription status. The system also lets you pull detailed information on all available membership plans and view which custom fields were set up for members. Plus, checking the latest coupons or monitoring marketing promotions is as simple as asking it. Getting this data stream through Vinkius makes sure your AI agent has access to everything needed, turning complex member workflows into simple conversations.

Core Capabilities

01 — Retrieve Member Profiles

Find and pull detailed records for specific members or search the entire user base by email address.

03 — Manage Promotions and Offers

Check the status of active coupons and list all ongoing marketing promotions to see what's running right now.

05 — Check Application Status

Get high-level information about your current Memberstack setup, verifying the app's configuration details.

02 — Audit Membership Plans

List all available membership plans, or get deep configuration details on a single plan's pricing structure.

04 — Handle Custom User Data

List, view, and manage any custom fields or metadata attached to specific member accounts.

One Click on Vinkius — From Prompt to Execution

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

- 01 Subscribe to this MCP and provide your unique Memberstack Secret Key.
- 02 Your AI agent connects using that key, establishing a direct link to your member data sources.
- 03 You ask the agent questions like, 'What is our annual plan?' or 'Find out John Doe's membership details,' and it returns actionable data.

The bottom line is you get real-time access to all your member records without needing to copy and paste anything into a dashboard.

Built For

E-commerce operations managers, product owners, and marketing teams need this. If you're constantly toggling between the CRM, the billing platform, and your internal database just to figure out one member's access level or plan status, this is for you.

E-commerce Operations Manager

Checks if a user has paid their subscription fee, verifying the current membership plan and checking associated custom fields to ensure proper system access.

Product Owner

Needs to enumerate all available membership plans or list members to verify that new features are correctly gated behind specific plan requirements.

Marketing Analyst

Queries the system to list active promotions and monitor coupon usage, allowing them to report on current marketing campaign effectiveness instantly.

What Changes When You Connect

- 01 Stop cross-referencing spreadsheets. You can use the `search_members` tool to instantly pull a user's full record, including their current plan and custom details, just by asking your agent.
- 02 Never forget what plans you offer. Your AI client can list all membership plans or fetch detailed configs using `get_plan`, ensuring every team member knows exactly what tiers exist.
- 03 Streamline promotional checks. Instead of navigating coupon tabs, ask the agent to use `list_coupons` and instantly see which discounts are active for your users' checkout process.
- 04 Full visibility into user data. The MCP lets you list all members or grab a single profile using `get_member`, giving you immediate access to plan connection details.
- 05 Keep track of unique data points. You can use `list_custom_fields` and related tools to manage metadata, making sure every niche piece of member info is accessible via conversation.

Real-World Applications

Verifying a High-Value Customer's Access

An e-commerce manager needs to confirm if VIP user 'ceo@corp.com' has the necessary 'Enterprise Annual' plan status before granting them access to beta features. They ask their agent, who uses ``search_members`` and then ``get_member``, confirming the correct subscription level in seconds.

Auditing Plan Changes After an Update

The product team needs to check if a new paid tier was correctly configured. They ask their agent to use ``list_plans`` and then query specific details with ``get_plan``, verifying the pricing structure before launching it.

Handling Support Queries on Discounts

A support agent needs to tell a user, 'Your discount code is active.' They ask their agent to use `list_coupons` and then verify the details with the resulting data, providing accurate, immediate information.

Onboarding New Data Fields

The ops team adds a new field for 'Industry Vertical'. Instead of manually updating every record, they use `list_custom_fields` to confirm the metadata structure is ready and available for agent interaction.

Patterns to Avoid

Treating member data as a simple database lookup

X AVOID

Trying to manually query every user's plan details by writing repetitive code blocks, one after the other.

✓ INSTEAD

Use the MCP. Ask your agent to `list_members` and then ask it to process that list using tools like `get_member_plans`. The AI handles the loop; you just talk to it.

Confusing membership status with general user data

X AVOID

Assuming a basic email search gives enough information, only finding the username and nothing else.

✓ INSTEAD

Always use `get_member` or `search_members`. These tools provide comprehensive records including active plan connections and custom metadata.

Bypassing promotion checks

X AVOID

Relying on the marketing team's spreadsheet for coupon codes, which might be outdated.

✓ INSTEAD

Use `list_promotions` or `list_coupons`. This MCP gives you real-time access to your live campaign data.

The Right Fit

Use this MCP if your core workflow revolves around user identity, billing cycles, and membership status. You need to know: Does User X belong? What plan are they on? Are they eligible for a discount?

Don't use it if you only need general user data that isn't tied to payments or specific plans (like basic contact lists). For those cases, a generic CRM connector might be better. However, because this MCP handles both the core membership state and

supplementary custom fields (`list_custom_fields`), it covers almost all e-commerce access control needs.

If you need to write code that *uses* member data (e.g., running complex financial models), you'll want a specialized Python agent framework; if you just need the *data itself* pulled into a script or conversation, this MCP is perfect.

The pain of checking membership status across systems

Today, figuring out what a member can access requires jumping between three places. You start in the CRM to find their email, then you log into your billing platform to see their plan level, and finally, you check a spreadsheet or internal dashboard just to verify if they have a custom field that grants them early access. It's a painful loop of tabs, logins, and copy-pasting.

With this MCP, all that friction vanishes. You simply ask your agent for the status. It automatically pulls together details from member profiles, plan records, and custom data points into one conversational answer. You get immediate context without touching another dashboard.

Memberstack MCP gives you complete access control through conversation

You no longer have to manually verify if a user's account has an active promotion or what their specific plan configuration is. You can use the agent to `list_promotions` and confirm the details, then check the member record using `get_member` all in one flow.

The difference now is that your AI client handles the complex orchestration of data retrieval. It combines membership status, billing records, and custom fields into a single stream of usable information.

Memberstack: 10 Tools for Membership Data

Use these tools to query everything from specific user details and membership plans to active coupons and custom metadata.

#	TOOL	DESCRIPTION
01	<code>get_member_plans</code>	Retrieves all possible membership plans associated with a specific user.
02	<code>get_plan</code>	Fetches comprehensive details about one particular membership plan by its identifier.
03	<code>list_coupons</code>	Displays a list of all discount coupons that are currently available for use.
04	<code>list_custom_fields</code>	Lists every custom data field you have set up to track unique member information.
05	<code>list_members</code>	Retrieves a list of all user accounts registered in your system.
06	<code>list_plans</code>	Shows an overview of every membership plan currently configured in Memberstack.
07	<code>list_promotions</code>	Provides a list and summary of all active promotional campaigns running right now.
08	<code>search_members</code>	Searches for members by entering their email address to locate the correct user profile.
09	<code>get_application_info</code>	Gathers high-level information about your overall Memberstack application configuration.
10	<code>get_member</code>	Retrieves the full, detailed record for one specific member ID or profile.

See It in Action

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

U List the last 5 members who joined.



Retrieving members... I found your most recent users, including 'john.doe@example.com' and 'jane.smith@domain.com'.

U Show details for member ID 'mem_12345'.



Inspecting member... Member 'mem_12345' is currently on the 'Pro Plan' and has been active since last month.

U What are my available membership plans?



Querying plans... You have 3 plans configured: 'Free Tier', 'Monthly Pro', and 'Annual Enterprise'.

Frequently Asked Questions

01 How does Memberstack MCP help me find a specific user's plan?

You use the `search_members` tool first to locate the user by email. Then, you can ask for the member details using `get_member`, which provides their current membership status and associated plans.

02 Can I check if a coupon is working with Memberstack MCP?

Yes. You use the `list_coupons` tool to see all available discount codes, ensuring that any promotion you mention is currently active in your system.

03 What kind of data can I pull about membership plans using this MCP?

You can list every plan offered using ``list_plans`` or get deep configuration details for one specific plan with the ``get_plan`` tool.

04 Is Memberstack MCP only for e-commerce billing?

No. While it handles payments, you can also use tools like ``list_custom_fields`` to manage non-billing metadata and track unique information about your member base.

05 Does the Memberstack MCP help me list all my members?







Yes. You use the ``list_members`` tool, which retrieves a roster of every user account registered in your system for auditing or reporting.

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>"memberstack": { "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

Memberstack 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](https://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 Memberstack. 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	Memberstack MCP
Server ID	019d75d2-4bc4-70bc-a1bd-f88abff52211
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/memberstack.