MCP SERVER | NO CODE | CLOUD HOSTED

Autho MCP for AI Agents

Manage user identities and security logs in your Autho tenant.

Auth0 MCP lets your AI agent handle identity and access management tasks directly. You can manage users, audit security logs, and check client configurations without switching between your terminal and the Auth0 dashboard. It is built for security teams and developers who need to move fast on IAM operations.

A+ Quality Score 100/100

iam | authentication | user-management | sso | identity-provider | security-logs

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JULY 2026
vinkius.com/mcp/auth0

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.

Autho MCP

10 tools available
Cloud-hosted on Vinkius

Auth0 MCP lets you connect your tenant to an AI agent so you can manage identities without leaving your chat interface. Instead of hunting through nested menus to find a specific user or digging through logs to see why a login failed, you just ask your agent to do it. This MCP handles the heavy lifting of identity and access management, like deleting user data for privacy compliance, checking OAuth client boundaries, and listing active connections, all through natural conversation. It takes the friction out of security audits and developer workflows. You'll find it's a huge time saver when you're using the Vinkius catalog to bridge your favorite tools with your core infrastructure. Because Vinkius hosts the entire catalog, you only have to connect once from your favorite AI client to get access to this and every other tool in the library. Your AI agent eliminates the need to navigate the verbose dashboard while debugging identity flows or verifying permissions. You can check if a specific app has the right token durations or look for a blocked login IP, getting direct access to the data you need without the manual overhead of the web console. It makes the complex parts of identity management feel like a simple chat. You can quickly verify if a specific client is configured correctly or check the metadata on a high-value account. It handles the tedious parts of the job, like pulling the system-level chronology of actions or identifying tripped rate limits. This means you spend less time on manual data entry and more time actually securing your application.

Core Capabilities

01 — Delete user profiles

Permanently remove user data to meet privacy compliance requirements.

02 — Audit OAuth clients

Inspect application configurations and token lifetimes.

03 — Inspect IdP connections

View details for social and enterprise authentication strategies.

04 — Fetch user metadata

Retrieve unified JSON profiles for specific accounts.

05 — List serverless actions

View the Javascript logic executing in your pipelines.

06 — Query security logs

Retrieve a chronological stream of all tenant events.

07 — Manage RBAC roles

List and audit authorization roles within the core engine.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/auth0** — connect your AI agent in three steps.

01 Subscribe to the Auth0 MCP through the Vinkius catalog.

02 Provide your Auth0 Domain and Management API Token.

03 Ask your AI client to perform tasks like listing users or checking logs.

The bottom line is you get a conversational interface for your entire Auth0 identity stack.

Built For

This is for the engineers and security pros who spend half their day in the Auth0 dashboard but would rather just get the answers they need instantly.

IAM Engineer

Audits logs and manages RBAC roles to keep the production environment secure.

App Developer

Checks OAuth client scopes and user metadata while building new features.

Compliance Officer

Ensures PII is deleted correctly and audits connection mappings for audits.

What Changes When You Connect

01 Handle right-to-be-forgotten requests instantly by using delete_user to wipe data without manual intervention.

02 Audit your security posture faster by pulling real-time events with list_logs to identify blocked IPs.

03 Verify OAuth boundaries and JWT lifetimes without manual checks using get_client to ensure app security.

04 Manage complex permissions across your app by listing and checking list_roles for RBAC.

05 See all your active IdPs and social wrappers in one list using list_connections for a clear overview.

Real-World Applications

Identifying a brute-force attack

A security engineer sees a spike in failed logins and asks the agent to fetch the list_logs to identify the source IP and frequency.

Verifying user metadata

A developer needs to know if a specific user has premium status and asks the agent to get_user to check the metadata.

Privacy compliance cleanup

A compliance officer needs to verify that a specific user's data was wiped and asks the agent to confirm the delete_user action.

Auditing tenant applications

An admin wants to see every app connected to the tenant and asks the agent to list_clients for a security audit.

Patterns to Avoid

Manual ID hunting

✗ AVOID

Trying to find a user's unique identifier by scrolling through the Auth0 dashboard.

✓ INSTEAD

Use list_users to find the correct ID first, then perform your actions.

Guessing block reasons

✗ AVOID

Wondering why a specific IP is being blocked without checking the logs.

✓ INSTEAD

Use list_logs to see exactly why a login or request failed in real time.

Hardcoding client scopes

✗ AVOID

Guessing the correct OAuth scopes for a new application integration.

✓ INSTEAD

Use get_client to see the exact configuration and allowed origins for an existing client.

The Right Fit

Use this if you need to perform frequent, repetitive IAM tasks like user lookups, log auditing, or client configuration checks. It's perfect for developers and security teams who want a conversational way to interact with Auth0 data. Don't use it if you need to build complex, custom UI components for your end users; this is for internal management and debugging. If you only need to manage simple web logins without an identity provider, a basic auth library might be enough, but for full IAM lifecycle management, this is the right choice.

Autho IAM Management: Ending the Dashboard Fatigue

Right now, if you need to find a user's metadata or check a client's OAuth scope, you have to log into the Auth0 dashboard, navigate through several menus, and filter through tables. It's a lot of clicks for a simple check, especially when you're in the middle of a deployment or a security incident.

This MCP changes that by letting you just ask. You can query your tenant logs or list your RBAC roles directly from your chat interface. You get the information you need in seconds without ever opening a new tab.

Autho Security Auditing: Faster Log Analysis

Manually searching through thousands of logs to find a specific blocked IP or a failed JWT validation is a nightmare. You usually end up exporting CSVs or squinting at a crowded console

With this MCP, your agent can scan the list_logs stream for you. You can ask it to find specific anomalies or summarize recent login failures,

to piece together what happened during a security event.

making security audits a conversation rather than a manual hunt.

Autho MCP: 10 IAM & Identity Tools

Manage users, audit logs, and inspect client configurations directly via your AI agent.

#	TOOL	DESCRIPTION
01	delete_user	Permanently delete a user profile directly from Auth0. This ensures complete privacy compliance during active right-to-be-forgotten requests.
02	get_client	Retrieve OIDC and configuration details for a single Auth0 application. This includes JWT lifetimes and allowed web origins.
03	get_connection	View details and strategies of a single authentication connection. This includes password strength and auto-routing triggers.
04	get_user	Retrieve the unified JSON profile for a specific Auth0 user. This includes sensitive identifiers and user metadata.
05	list_actions	List serverless Javascript logic executing dynamically in pipelines. This helps you monitor real-time authorization flows.
06	list_clients	List all logical applications and clients spanning this Auth0 tenant. This is crucial for auditing global grant types.
07	list_connections	List all Identity Provider connections attached to Auth0. This shows configurations for social wrappers and enterprise firewalls.
08	list_logs	Retrieve the chronological stream of all executed Auth0 tenant logs. This captures successful logins and failed JWT validations.
09	list_roles	List RBAC roles defined intrinsically within the Auth0 Core Engine. Use this to decouple authorization scopes from authentication.
10	list_users	List all users registered in the Auth0 tenant. This includes core attributes and customized app metadata mappings.

See It in Action

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

U Show me the last 5 failed login attempts in our logs.

Reviewing the last 5 failed attempts:

TIMESTAMP	IP ADDRESS	REASON
10:04 AM	192.168.1.45	Invalid Password
10:05 AM	192.168.1.45	Invalid Password
10:06 AM	192.168.1.45	Invalid Password
10:07 AM	192.168.1.45	Brute-force Block
10:08 AM	172.16.0.12	Expired Token

It looks like a brute-force attempt from `192.168.1.45` triggered a block.

U Does user auth0|5ecc9f1... have any custom metadata?

Extracting profile for `auth0|5ecc9f1...`.

User Metadata:
- **Tier:** Premium
- **_internal_id:** 99283
- **last_login_region:** Toronto
- **verified_email:** true

The `app_metadata` confirms this user is on a premium subscription tier.

U List all our active social connections.

I found 4 active connections in your Auth0 tenant:

- **Google** (OAuth2)
- **Facebook** (OAuth2)
- **Apple** (OIDC)
- **Enterprise AD** (LDAP Proxy)

Frequently Asked Questions

01 **Can I use the Auth0 MCP to delete users for GDPR?**

Yes, this MCP allows you to delete user profiles directly. Your AI agent can handle these requests instantly to ensure you meet privacy compliance requirements.

02 **Does the Auth0 MCP work with my custom Actions?**

Yes, the MCP can list the serverless Javascript logic currently running in your pipelines. This helps you audit and manage your custom authorization flows.

03 **Can I use this to check my OAuth clients?**

Yes, you can ask your agent to retrieve the configuration details for any specific client. This includes checking token lifetimes and allowed web origins.

04 **Is my Auth0 data safe with this MCP?**

Yes, the MCP uses your Auth0 Management API Token. This ensures that your agent only performs the actions you've authorized within your secure tenant.

05 **Can I list all my RBAC roles?**

Yes, the MCP can fetch and list all RBAC roles defined within your Auth0 Core Engine. This makes it easy to audit your authorization scopes.

06 **How do I see my tenant logs?**

You can simply ask your agent to pull the logs. It will retrieve the chronological stream of actions, including failed logins and administrative mutations.

07 **Can the agent show me the exact cause of a user’s failed login attempt?**

Absolutely. By asking the agent to search the tenant logs for the user's specific interactions, you receive exact JSON artifacts mapping the failure trigger—whether it was a brute-force IP rate limitation or an explicitly thrown error from a deployed Custom Action pipeline.

08 **Are user passwords exposed or compromised through this integration?**

Never. The Auth0 Management API strictly strips raw authentication secrets and passwords from all JSON payloads by default. The agent can only interpret profile structures (metadata, log times, associated connections), ensuring top-tier infrastructure security.

09 **Does it support identifying all connections tied to one user (Social + DB)?**

Yes. When retrieving a single user's profile, the agent parses the `identities` array object. This object arrays each distinct identity provider mapping—meaning you can see if the user signed in natively, merged to a Google account later, and the precise times of those connection lifecycle updates.

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 `"auth0": { "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

Autho 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 Auth0. 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	July 2026
MCP Server	Auth0 MCP
Server ID	`019d7555-9059-72a6-9284-264b380fa0c5`
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/auth0.