MCP SERVER | NO CODE | CLOUD HOSTED

Logto (Auth Platform) MCP

Manage who has access, roles, and organizations.

Logto (Auth Platform) MCP lets you manage user identities, roles, and organizational structures directly from your AI agent. Need to audit who has access or update a profile? You can list users, create new API resources, assign granular permissions using roles, and even handle complex multi-tenant organization setups. It's full identity control in one place.

A+ Quality Score 98.33/100

authentication | rbac | user-management | identity-provider | access-control | iam

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/logto-auth-platform

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.

Logto (Auth Platform) MCP

23 tools available
Cloud-hosted on Vinkius

This MCP gives you complete control over user identities and access rules within your Logto authentication system. Instead of jumping through multiple dashboards to manage who can do what, your agent handles the heavy lifting. You can look up specific users by ID or list everyone currently registered. If a team needs tighter security, you can create new global roles and API resources to enforce precise permissions across the board. For large companies using multi-tenant setups, this MCP lets you build and manage entire organizations, tracking memberships along the way. All of this is accessible through your AI client once you connect it via Vinkius, letting you automate complex identity workflows without writing boilerplate code.

Core Capabilities

01 — Manage user accounts

You can get details for a specific user, list all users in the tenant, or update basic profile information like names and avatars.

02 — Control organizational structure

Build out multi-tenant environments by listing existing organizations, creating new ones, and viewing which members belong to them.

03 — Define granular permissions (RBAC)

Create global roles, list available API resources, and assign specific permissions to users or groups.

04 — Handle password and MFA resets

Send verification codes via email or SMS, verify a user's password strength, or bind/remove Multi-Factor Authentication factors for account security.

05 — Update current user profile

Retrieve your own account details and update primary emails, passwords, or extended profile information using end-user tokens.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/logto-auth-platform** — connect your AI agent in three steps.

01 Subscribe to this MCP on Vinkius and provide your Logto Management API credentials (Endpoint, App ID, and App Secret).

02 Your agent authenticates with the necessary keys, giving it full read/write access to your identity management system.

03 You prompt your AI client, telling it exactly what needs changing—like 'Create a role called X' or 'List all users in organization Y.''

The bottom line is you manage complex auth infrastructure using natural conversation instead of logging into an internal dashboard.

Built For

This MCP is built for security engineers and developers who deal with user identity daily. If you're tired of manually auditing role assignments or updating test accounts across multiple dashboards, this saves hours.

Security Engineer

Auditing user lists, checking resource permissions, and ensuring compliance by verifying passwords or deleting old user accounts.

DevOps Engineer

Programmatically setting up new multi-tenant organizations and defining initial roles for deployment environments.

Full-stack Developer

Managing test users, creating dummy API resources for testing endpoints, or updating user profiles during local feature development.

What Changes When You Connect

01 Instead of manually calling APIs to check credentials, you can ask your agent to run a password verification using `verify_user_password` and get an immediate status update.

02 Need to audit permissions? You can list all users and then use `list_user_roles` to instantly see every role assigned to any account.

03 When setting up multi-tenant environments, you don't have to manually create structures; just call `create_organization`, and your agent handles the initial setup.

04 For security cleanup, if an employee leaves, your agent can run a simple prompt that executes `delete_user` right away, ensuring immediate deprovisioning.

05 You get granular control over system access by defining new permissions. Use `create_role` to build specific job titles and assign them using the MCP.

Real-World Applications

Auditing User Access After a Breach

A security engineer notices unusual activity. They prompt their agent: 'List all users who have access to API resources for finance.' The agent automatically runs `list_resources` and then checks the permissions, giving the engineer an immediate report on potential risks.

Onboarding a New Department

A manager needs to set up a new department. They tell their agent: 'Create a new organization called Marketing.' The MCP runs `create_organization`, and the agent confirms the new tenant is ready for users.

Patterns to Avoid

Treating it like a general database tool

✗ AVOID

Asking the agent to 'update user X' without specifying what kind of update. The system doesn't know if you mean name, password, or role.

✓ INSTEAD

Be specific: If you want to change an avatar, prompt for `update_user` and specify the field. To change a password, use `update_my_account_password`.

Assuming access rights

✗ AVOID

Trying to list all users without first checking if the account has permission to read user data. The request will fail or return incomplete info.

✓ INSTEAD

Always start by running `list_roles` and understanding what permissions your current service credentials possess before attempting large-scale operations.

The Right Fit

Use this MCP if your core problem involves identity, access control (RBAC), or user lifecycle management. You need to know *who* can do *what*, and you must be able to programmatically enforce those boundaries.

Don't use this if you simply need to read static data that isn't tied to a user profile—for example, listing general product catalog items would require a different MCP. Also, if your goal is just basic messaging or simple document retrieval (like fetching articles), an identity platform like this won't help; look for a message routing or knowledge base MCP instead. This tool is strictly about managing the users and their permissions.

User access management used to feel like juggling fifty different dashboards.

Right now, updating user accounts means opening the admin panel, finding the user by email, clicking 'Edit Profile,' changing a field, and then saving. If you need to audit roles or check MFA status for ten people, that's ten separate logins and dozens of clicks.

With this MCP, your agent handles it all in one prompt. You tell your AI client what needs fixing—maybe listing users who lack the 'Admin' role—and it runs the necessary checks (`list_users` then `list_user_roles`) and spits out a clean report.

Achieving Full Identity Control with Logto (Auth Platform)

The ability to define new roles, such as 'Billing Viewer' or 'Support Agent,' used to require coordination between engineering and security teams just to create a permission template. Now, you can use `create_role` directly through the MCP.

This means your team moves from manual audits and slow ticket resolution to instant, self-service identity management right inside your coding environment.

Logto (Auth Platform) MCP - 23 Tools

These tools give you direct access to Logto's backend functions, letting your agent perform any identity management action needed.

#	TOOL	DESCRIPTION
01	`create_organization`	Sets up an entirely new, isolated organizational structure within your Logto tenant.
02	`create_resource`	Defines a brand new API resource that services will use to authorize specific actions.
03	`create_role`	Builds and names a global role, which dictates what permissions users can inherit.
04	`delete_user`	Permanently removes a user account from the system.
05	`get_user`	Retrieves all specific details for any given Logto user ID.
06	`list_mfa_verifications`	Lists every MFA factor currently registered and associated with the current user's account.
07	`get_my_account`	Pulls your own profile data, including names and details, using end-user tokens.
08	`list_organization_users`	Fetches a roster of all users who are currently members of a specified organization.
09	`list_organizations`	Provides a list of every organizational container set up in the Logto tenant.
10	`remove_mfa_verification`	Deletes an existing Multi-Factor Authentication factor from the user's profile for security reasons.
11	`list_resources`	Shows all existing API resources that are currently defined in your system.
12	`list_roles`	Retrieves a list of every global role available for assignment across the entire platform.
13	`send_verification_code`	Triggers an email or SMS code delivery to verify user ownership of an account.
14	`update_my_account`	Updates basic personal information, such as changing your username or avatar image.

#	TOOL	DESCRIPTION
15	update_user	Modifies details for any existing user account in the tenant.
16	list_user_roles	Shows exactly which roles have been assigned to a specific user ID.
17	list_users	Pulls a comprehensive list of every single user account in the Logto tenant.
18	verify_password	Checks a password's validity to generate a temporary ID used for verification purposes.
19	verify_user_password	Verifies the strength and correctness of a user-supplied password using management credentials.
20	bind_mfa_verification	Links a new Multi-Factor Authentication factor like TOTP or WebAuthn to the current user's account.
21	update_my_account_primary_email	Changes or links the main primary email address associated with your own profile.
22	update_my_account_profile	Modifies extended personal details for your account, like physical addresses or phone numbers.
23	update_my_account_password	Changes the password for your own user account.

See It in Action

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

U List the first 10 users in my Logto tenant.

I've retrieved the user list. You have users like 'admin_user' (ID: user_1) and 'dev_test' (ID: user_2). Would you like to see the full details for any of them?

U Create a new User role called 'Support Agent' with a description.

The role 'Support Agent' has been successfully created. It is now available for assignment to your users.

U Show me all members of the organization with ID 'org_999'.

Fetching members for organization 'org_999'... I found 3 members: Alice, Bob, and Charlie. Would you like to inspect Alice's specific permissions?

Frequently Asked Questions

01 **How do I list all users in my Logto tenant using the Logto (Auth Platform) MCP?**

You run the `list_users` tool. This immediately provides a comprehensive roster of every account, letting you see who needs attention or auditing.

02 **Can I reset a user's password with the Logto (Auth Platform) MCP?**

Yes. You can use `send_verification_code` to trigger an email or SMS code delivery, allowing the user to securely reset their credentials.

03 **What is the difference between `get_user` and `list_users` in the Logto (Auth Platform) MCP?**

`list_users` gives you a high-level list of all accounts. `get_user` requires a specific ID to pull deep, detailed information for just one person.

04 **Do I need elevated permissions to use the Logto (Auth Platform) MCP?**

You must provide API credentials that grant management access. The agent uses these credentials to perform actions like `create_role` or `delete_user`.

05 **Can I see which roles are assigned to a specific user?**

Yes! Use the `list_user_roles` tool with the target User ID to retrieve all global roles associated with that account.

06 **Is it possible to manage multi-tenant organizations through this server?**

Absolutely. You can use `list_organizations` to see existing ones, `create_organization` to add new ones, and `list_organization_users` to audit membership.

07 **Can I update user profiles or suspend accounts?**

Yes, the `update_user` tool allows you to modify the username, name, avatar, and the `isSuspended` status of any user.

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 `"logto-auth-platform": { "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

Logto (Auth Platform) 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 Logto (Auth Platform). 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	Logto (Auth Platform) MCP
Server ID	`019e38ba-5d7f-73a9-9a9a-4ced52526cb4`
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/logto-auth-platform.