MCP SERVER | NO CODE | CLOUD HOSTED

Authing MCP for AI Agents

Manage User Accounts, Roles, and Access Control Permissions

Authing provides a cloud-native identity and access management platform. Connect it via an MCP and let your AI client manage all user accounts, organizational structures, roles, and security audit logs through natural conversation. Stop clicking dashboards to check permissions; just ask.

A+ Quality Score 100/100

idaas | user-roles | access-control | security-auditing | cloud-native

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/authing

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.

Authing MCP

10 tools available
Cloud-hosted on Vinkius

Authing lets your agent control your entire identity infrastructure. It turns complex tasks like user provisioning, compliance auditing, and access control into simple conversations with your AI client. You no longer need to jump between multiple consoles or manually cross-reference permission sets. With Authing connected through Vinkius, you can tell your agent to list all users, check an organizational unit's hierarchy, or pull the security audit logs from last week —all without leaving your chat window.

This means whether you're running a compliance review or simply onboarding a new team member, your AI acts as a real-time identity assistant. It keeps user data accurate and systems secure by handling complex queries like listing roles, groups, and permission resources instantly. You manage the whole lifecycle of who can access what.

Core Capabilities

01 — Manage User Accounts

You can create new users or retrieve specific user details to verify their current profile metadata.

02 — Audit Security Logs

Retrieve detailed security audit logs showing who did what and when, helping track administrative actions.

03 — Map Organizational Structure

Browse the entire company hierarchy by listing organizational units to understand reporting lines.

04 — Check Access Permissions

List all roles, groups, and specific permission resources to map out complex authorization patterns.

05 — Monitor System Settings

Access high-level security settings and metadata for your entire identity project pool.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the Authing MCP and provide your required User Pool ID, Access Key, and Domain credentials.

02 Connect this MCP to any compatible client like Claude or Cursor within Vinkius.

03 Use natural language prompts to ask your AI agent to perform identity tasks, such as listing users or checking audit logs.

The bottom line is you talk to your agent about user accounts and roles; the MCP handles the complex API calls to Authing for you.

Built For

Security Engineers, IT Administrators, and Compliance Leads. If your job involves auditing who has access to what, or if onboarding users requires coordinating multiple systems, this is for you. It takes the clicks out of identity management.

Security Engineer

Automates compliance audits and monitors system access by asking the agent to retrieve security audit logs and list permission resources.

IT Administrator

Manages user lifecycles, such as creating new users or updating organizational units, without needing to navigate multiple internal dashboards.

Compliance Lead

Retrieves detailed administrative logs and verifies group memberships via a unified AI interface for audit purposes.

What Changes When You Connect

01 Audit compliance effortlessly. Instead of manually checking logs, your agent can retrieve security audit logs to prove who accessed what and when.

02 Control user lifecycles completely. You use the `create_user` tool or `get_user` to onboard or verify employee details without leaving the chat interface.

03 Understand organizational flow instantly. Listing organizations gives you a real-time map of your company's structure, eliminating manual diagramming.

04 Audit permissions in bulk. By calling `list_roles`, `list_groups`, and `list_resources`, you can quickly identify potential authorization gaps across the entire system.

05 Maintain security posture proactively. Check high-level security settings using `get_security_settings` to ensure your pool remains compliant.

Real-World Applications

New Employee Onboarding Audit

An IT administrator needs to verify that a new hire has the correct access. They ask their agent, and it uses `get_user` for basic details, then calls `list_groups` to confirm role assignments across different departments.

Compliance Review of Sensitive Data

A compliance lead must prove who saw financial records last month. They ask the agent to pull all security audit logs via `get_audit_logs`, providing a verifiable timeline for auditors.

Re-structuring Departments

The company merges two divisions, requiring a full review of reporting lines. The user asks their agent to list organizations using `list_organizations` to map the new combined hierarchy instantly.

Role Permission Gap Analysis

A security engineer suspects over-permissioning. They ask the agent to list roles and resources, then use `list_resources` and `list_roles` in succession to pinpoint exact access bottlenecks.

Patterns to Avoid

Manual Role Cross-Referencing

✗ AVOID

The user prints out the list of users, then opens a spreadsheet, and manually compares roles against resource permissions.

✓ INSTEAD

Ask your AI client to list all available roles and resources. Then, ask it to compare them using `list_roles` and `list_resources`. The agent does the comparison work for you.

Checking User Status in Multiple Places

✗ AVOID

The administrator has to check the HR system for employment status, then log into Authing to see user accounts.

✓ INSTEAD

Just ask your AI client to get user details using `get_user`. It pulls all relevant profile metadata from one source. For new users, use the `create_user` tool.

Ignoring Historical Activity

✗ AVOID

The team only checks current roles and forgets that a sensitive change happened weeks ago.

✓ INSTEAD

Don't just check roles; always ask to retrieve security audit logs using `get_audit_logs`. This provides the full, historical record of changes.

The Right Fit

Use this MCP if your primary bottleneck is coordinating identity data across multiple systems. You need one single interface that lets you query user accounts, organizational structure, and access controls—for example, checking who can see a specific resource using `list_resources`. Don't use it if you just need to send a simple email or manage calendar invites; those are messaging tools. If your problem is tracking physical assets or inventory, look for an asset management MCP instead.

Authing MCP: Simplifying User Identity Management

Today, managing user access feels like a scavenger hunt across half a dozen dashboards. You check the HR portal for status, then log into the identity platform to list users, and finally open the audit console just to see if someone updated permissions last week. The process involves constant copy-pasting and jumping between screens.

With Authing connected via this MCP, you simply ask your agent to verify a user's access level. It combines checking organizational units (`list_organizations`), pulling profile metadata (`get_user`), and listing roles—and gives you the answer instantly in natural language.

Authing MCP: Auditing Security Logs and Roles

The manual process for auditing is brutal. You have to filter audit logs by date range, then export them, then manually check every entry against the list of defined roles and groups. It's slow, tedious work prone to human error.

Now, your agent handles that whole workflow. Ask it to retrieve security audit logs (`get_audit_logs`) for a specific time frame, and simultaneously request all relevant permission resources (`list_resources`). You get a clean report combining history and potential gaps.

Authing MCP: 10 Tools for User Roles & Access Control Auditing

Use these tools to control everything about your identity infrastructure, from creating new accounts to reviewing historical access permissions.

#	TOOL	DESCRIPTION
01	`create_user`	This tool handles the creation of a brand new user account within your system.
02	`get_audit_logs`	Retrieves historical security audit logs detailing actions taken across the platform.
03	`get_security_settings`	Fetches current high-level security settings for your user pool.
04	`get_user`	Retrieves specific, detailed profile metadata for any existing user.
05	`list_applications`	Lists all registered third-party applications that are connected to your identity system.
06	`list_groups`	Provides a list of defined user groups within the organization.
07	`list_organizations`	Lists all primary organizational units and branches established in your company structure.
08	`list_resources`	Provides a list of defined permission resources that require access control.
09	`list_roles`	Lists all available roles, defining what permissions different user types have.
10	`list_users`	Retrieves a list of all application users currently registered in the system pool.

See It in Action

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

U Who are the admins in the Engineering department?

Engineering Department Admins

- John Doe (Role: Admin)
- Jane Smith (Role: SuperUser)

These users were identified by checking both organizational units and current role assignments. Do you need their email addresses?

U Show me all the security changes from yesterday.

Here are the top 3 actions logged yesterday:

- `[2026-06-11]` : Role updated for UserID: X987 (Admin → ReadOnly).
- `[2026-06-11]` : Application 'BillingTool' registered.
- `[2026-06-11]` : Attempted access to restricted resource R45 failed.

Need more detail on any of these?

U What are the main departments and who reports into them?

Company Organizational Structure

The company is structured around 3 primary units:

1. **Engineering:** (5 teams, including Frontend & Backend)
2. **Marketing:** (Product Launch, Content Creation)
3. **HR:** (Recruitment, Payroll)

You can ask me to dive deeper into any of those branches.

Frequently Asked Questions

01 **How does the Authing MCP help me check user roles?**

The Authing MCP lets you instantly list all defined roles and groups, or get details on a specific user's profile. You don't have to navigate complex role trees; just ask your agent for a summary of who can do what.

02 **Can I use the Authing MCP to audit permission changes?**

Yes, you can retrieve detailed security audit logs using this MCP. It provides a chronological record of all administrative and user actions across your system for full compliance checks.

03 **What if I need to add a new employee account?**

You use the `create_user` tool through your agent. You simply tell it the details, and it handles creating the account record in Authing without you needing to log into the main console.

04 **Is this MCP good for large organizations?**

Absolutely. It's built for enterprise identity management. You can map complex organizational units and access control patterns across thousands of users, making it ideal for growing companies.

05 **Does Authing MCP only list current permissions?**

No, this MCP is designed for deep auditing. It lets you retrieve historical data via the security audit logs, giving you a full picture of past and present access rights.

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 `"authing": { "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

Authing 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 Authing. 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	Authing MCP
Server ID	`019d8419-bb2d-7134-84cc-ae5b2262d7f3`
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/authing.