MCP SERVER | NO CODE | CLOUD HOSTED

Clerk MCP for AI Agents

Manage Multi-Tenant User Authentication and Profiles

Clerk lets your AI agent manage complex user authentication and multi-tenant environments directly from natural conversation. Pull up directories of every registered user, check organization boundaries, or send targeted invitations without opening a dashboard. It puts full control over your application's identity layer right into your workflow.

A+ Quality Score 100/100

authentication | user-management | sso | multi-factor-auth | session-handling | user-profiles

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

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.

Clerk MCP

6 tools available
Cloud-hosted on Vinkius

Managing user accounts and organizational structures used to mean clicking through multiple dashboards just to find the right ID or status update. Now, you can talk to your AI agent and have it handle that complexity for you. Your agent acts like a dedicated auth architect, pulling up detailed profiles and handling multi-tenant coordination on demand. You'll pull user directories using `list_auth_users` or check out organization setups with `list_auth_organizations`. Need to bring someone new onto the team? Just ask your AI client to send an invitation via email; it manages that entire lifecycle for you. This MCP lets you manage account integrity and coordinate team access in real time, making complex user provisioning feel as simple as asking a question.

Getting this integration from Vinkius means you connect once, and your agent gains full control over these core authentication workflows.

Core Capabilities

01 — List all active users

Your agent retrieves a complete directory of every registered user in the application.

02 — Manage organizational structures

You can list and monitor multi-tenant environments to coordinate team access control boundaries.

03 — Generate new invitations

The agent programmatically sends email invites with custom redirect URLs for streamlined user onboarding.

04 — Get detailed user profiles

Retrieve high-fidelity user metadata, contact information, and current authentication status instantly.

05 — Track invitation statuses

Your agent lists all pending invitations to check the onboarding pipeline's progress.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and retrieve your secret key from the Clerk dashboard.

02 Connect that secret key to your preferred AI client (like Claude or Cursor).

03 Ask your agent to perform a specific action, like listing users or creating an organization invitation.

The bottom line is: you talk to your AI agent, and it executes the complex user management commands against Clerk for you.

Built For

This MCP is built for developers and operations teams who manage SaaS applications with multiple clients or departments. If your job involves coordinating access rights, onboarding users, or troubleshooting authentication issues across different organizational units, this tool saves you hours of manual dashboard work.

Developer

You use the agent to programmatically pull user profiles and verify complex multi-tenant setups before writing a single line of backend code.

Operations Engineer

Your job is automating team growth; you'll ask the agent to dispatch invitations or check organization boundaries for compliance reporting.

Customer Success Manager

You need visibility into user accounts. You can use the agent to check authentication history and manage invitation lifecycles through simple, conversational queries.

What Changes When You Connect

01 Instant access to user directories. Instead of navigating through tables, your agent runs `list_auth_users` and gives you a clean summary of every account.

02 Simplified onboarding workflow. You can ask the agent to send an invitation using `create_auth_invitation`, handling custom redirects without manual API calls.

03 Full organizational visibility. Need to know how many tenants exist? The MCP lets your agent list organizations via `list_auth_organizations` instantly, helping you track multi-tenancy growth.

04 Deep user data retrieval. You don't just get an ID; using `get_auth_user_details` pulls the full profile metadata and authentication history right into your chat window.

05 Audit trail management. Easily list all pending invites or check specific account statuses using `list_auth_invitations`, making compliance checks faster than ever.

Real-World Applications

Onboarding a new client department

An ops engineer needs to set up a brand-new, isolated team for a major corporate client. Instead of manually clicking through setup forms, they ask their agent to use the `create_auth_organization` tool, instantly provisioning a secure, dedicated environment.

Auditing user access after a security incident

A developer needs to verify which users have accessed sensitive data and what roles they hold. They prompt their agent to run `list_auth_users`, getting an immediate, verifiable list of all accounts for investigation.

Scaling team expansion with controlled invites

Customer success needs to onboard ten new contractors simultaneously without leaving the chat interface. They ask their agent to send out multiple invitations using `create_auth_invitation`, and then check status using `list_auth_invitations`.

Cross-checking identity across departments

A developer needs to confirm if a specific user's profile is correct and active. They ask the agent to run `get_auth_user_details`, pulling all necessary contact info and authentication statuses in one query.

Patterns to Avoid

Trying to manage access manually

✗ AVOID

The developer spends an hour digging through the web portal, clicking 'Users' then 'Organization Settings,' copying IDs, and pasting them into a spreadsheet.

✓ INSTEAD

Use your agent with this MCP. Simply ask it to pull up all users via `list_auth_users` or check organizational boundaries using `list_auth_organizations`. The agent handles the deep portal navigation for you.

Assuming user data is always current

✗ AVOID

The operations team assumes a user account exists because they remember the name, but the account has been deactivated or changed ownership.

✓ INSTEAD

Always verify status. Use `get_auth_user_details` to pull the full metadata and authentication status directly through your agent before making any changes.

Overlooking tenant separation

✗ AVOID

A developer forgets which organization a new user belongs to, leading to potential data access mix-ups between clients.

✓ INSTEAD

Start by listing all organizations using `list_auth_organizations`. This ensures you know exactly which multi-tenant boundaries you're working within.

The Right Fit

Use this MCP if your application's core function revolves around complex, multi-tenant identity management. If you need to coordinate access control across different organizational units or automate the full user lifecycle—from invitation to profile retrieval—this is what you need. However, don't use it if all you need is a simple form submission tool (like just creating a single record). For basic data entry that doesn't involve authentication status or complex relationships, look for a dedicated database connector instead. This MCP excels when your task requires coordinating multiple pieces of user-centric information: list users, check organization membership, and then get specific details on one person.

Clerk MCP for AI Agents: Automating Multi-Tenant User Identity Management

Right now, managing your user base means jumping between the dashboard, API documentation, and support forums. You have to copy a user ID from one place, check their organization status on another tab, and then manually dispatch an email invite through a third workflow. It's tedious, prone to human error, and slows down every single onboarding process.

With this MCP, your agent takes over the whole flow. Instead of manual clicks, you just ask your client: 'Send invites for these five people and confirm their new organization.' The AI handles the complex choreography using tools like `create_auth_invitation` and `list_auth_organizations`. You get instant confirmation and accurate data without leaving your chat.

Clerk MCP for AI Agents: Controlling User Provisioning Workflows

The most time-suck steps that disappear are the repetitive checks. You don't have to manually list every user just to find one person's current status, or check if an organization already exists before creating a new one.

This MCP gives your agent direct control over the entire identity lifecycle. You can ask it to get detailed profiles using `get_auth_user_details`, giving you instant operational reports that used to take minutes of clicking and searching.

Clerk: 6 Tools for AI Agents' User Authentication Management

Use these tools to list users, create organizations, manage invitations, and pull detailed user profiles using your agent.

#	TOOL	DESCRIPTION
01	`create_auth_invitation`	Sends a new user invitation email with custom redirect links.
02	`create_auth_organization`	Sets up an entirely new, self-contained organizational environment.
03	`get_auth_user_details`	Fetches specific user data, including detailed profiles and contact information.
04	`list_auth_invitations`	Retrieves a list of all current or past user invitations.
05	`list_auth_organizations`	Lists all active and existing organizations managed by the application.
06	`list_auth_users`	Provides a comprehensive list of every user registered in the system.

See It in Action

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

U I need a list of all users in the system, specifically showing their organization ID and if they have an active account.

User Directory Report

USER NAME	ID	ORGANIZATION SLUG	STATUS
John Doe	user_123	vinkius-corp	Active
Jane Smith	user_456	beta-testers	Suspended
Mark Lee	user_789	acme-solutions	Active

Total Users Found: 3

U Can you set up a new department for 'Global Retail' and invite two key leads?

✅ **Invitation Dispatch Complete**

I successfully created the organization 'global-retail'. I then sent invitations to:

- `sara@store.com` (ID: inv_101)
- `tom@store.com` (ID: inv_102)

The leads are now in the pipeline. You'll be notified when they complete registration.

U Show me all organizations we have and list any pending invitations for them.

Multi-Tenant Overview

Organizations Found:

1. Vinkius Enterprise (Slug: vinkius-ent)
2. Beta Testers (Slug: beta-testers)

Pending Invitations Check:

- **Vinkius Enterprise:** 3 pending invites.
- **Beta Testers:** 0 pending invites.

Please let me know if you want to check the full user directory for any of these organizations.

Frequently Asked Questions

01 **How does using Clerk MCP help with multi-tenant architecture?**

It lets you manage the boundaries between different client accounts (tenants) without manually switching views. You can list all organizations and ensure that actions only affect the correct isolated environment.

02 **Is this better than just using a standard database connector for user data?**

Yes, because it understands authentication concepts like SSO, MFA status, and organization ownership. It doesn't just read rows; it understands 'user profile.' This adds crucial context to the data you get back.

03 **Can I use Clerk MCP to onboard users programmatically?**

Absolutely. You can automate the entire onboarding flow by having your agent dispatch invitations, track their status, and even create an organization for them all in one session.

04 **What if I need to see a user's full profile history?**

You can ask the MCP to get detailed user profiles. This pulls together not just basic info but also critical metadata and authentication status, giving you a complete picture of that account.

05 **What is the main benefit of using Clerk MCP with my AI agents?**

The biggest gain is speed and accuracy. You eliminate the need to switch between dashboards or run multiple manual queries by having your agent coordinate all the user management tasks for you.

06 **Does Clerk MCP help me manage roles and permissions?**

While it doesn't set the roles, it gives you the necessary data to manage access control. You can list users and organizations to confirm who belongs where before making any changes.

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 `"clerk-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

Clerk 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 Clerk. 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	Clerk MCP
Server ID	`019dd0ce-c3f0-73b3-b778-ae7b3c0abfa7`
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/clerk-alternative.