MCP SERVER | NO CODE | CLOUD HOSTED

Clerk MCP for AI Agents

Monitor B2B Organization Health and User Authentication Data

Clerk MCP lets your AI client manage and monitor authentication systems. You can track every user, check active sessions across platforms, audit B2B organizations, and review invitation statuses—all through natural conversation without opening a dashboard.

A+ Quality Score 100/100

authentication | user-management | session-tracking | b2b-organizations | user-onboarding

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

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

8 tools available
Cloud-hosted on Vinkius

Managing user data used to mean navigating multiple admin panels: checking signups in one tab, auditing sessions in another, and tracking organization memberships on a third. This MCP changes that. You connect your Clerk account once via Vinkius and give your AI client the authority it needs to manage core authentication functions using just chat commands.

Your agent can pull a complete picture of your user base instantly. Need to know if a specific domain is whitelisted? Ask for it. Want to audit how many B2B organizations are active or check the status of pending invitations? Your client handles it. You get immediate, actionable data—a full system health report on demand. It's about turning complex backend monitoring into a simple conversation.

Core Capabilities

01 — Get System Health Summary

Retrieve an instant summary of your total user count, active sessions, and overall authentication status.

02 — List All Users

Fetch a comprehensive list of every user in the application, including their specific metadata and account status.

03 — Check Active Sessions

Monitor all active user sessions across your platforms to identify potential security issues or inactive accounts.

04 — Manage Organizations

List and review all B2B organizations linked to the application, along with their member rosters.

05 — Audit Invitations

Access a history of both pending and completed user invitations for full onboarding visibility.

06 — Review Allowlist Identifiers

See exactly which emails and domains are currently approved on the authentication allowlist.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Clerk Secret Key, usually found in your API Keys dashboard.

02 Connect your preferred AI client (like Cursor or Claude) through the Vinkius platform.

03 Start asking questions. Tell your agent what you need—for instance, 'Show me all active sessions for B2B organizations.' — and it retrieves the data.

The bottom line is that you use natural language to access complex user and authentication data without ever logging into the Clerk dashboard.

Built For

This MCP is built for roles that live in the intersection of product operations and engineering. If your job involves auditing user accounts, verifying system health, or managing B2B onboarding logistics, you need this. It cuts out the dashboard clicking.

Developer

Checks user signups or verifies session status directly in their chat interface instead of writing boilerplate API calls.

Customer Support Agent

Quickly pulls up a full profile, organization membership list, and account details for a customer without having to open multiple internal tools.

Product Manager

Audits invitation success rates or checks active user counts to report on growth metrics straight from the chat interface.

Operations Team Lead

Verifies authentication allowlists and system health indicators across different platforms to ensure compliance before a release.

What Changes When You Connect

01 Check system health at a glance. Instead of digging through dashboards, use get_auth_dashboard_summary to instantly see total users and active sessions.

02 Audit user access quickly. Need details on a specific account? Use get_user_auth_details to pull up every piece of information about that user profile without leaving the chat window.

03 Manage B2B growth efficiently. List all organizations with list_clerk_organizations, giving you a clear picture of your enterprise client base and their members.

04 Stay secure by tracking sessions. Use list_active_sessions to monitor who is logged in right now, helping catch unauthorized or forgotten access points.

05 Simplify onboarding processes. You can review all pending and completed invitations using list_sent_invitations, giving product managers clear visibility into growth pipelines.

Real-World Applications

Investigating an Account Breach

A support agent suspects a compromised account. They ask the agent to check active sessions and then run get_user_auth_details on the affected user ID, immediately identifying unusual or geographically distant login points.

Quarterly B2B Audit

The operations team needs to confirm all organizational structures. They ask to list clerk organizations and then run list_clerk_users to cross-reference the total number of members across all accounts.

Tracking Marketing Campaigns

A product manager wants to measure referral success. They request a list of sent invitations, allowing them to audit who was invited and if the invitation status is still 'Pending'.

Verifying System Compliance

The developer needs proof that only authorized domains can connect. They use list_auth_allowlist to pull a definitive list of all approved emails and domains for compliance checks.

Patterns to Avoid

Trying to manually check user status

✗ AVOID

A developer needs to know if a user is active but has to jump between the main dashboard, the session log, and the organization panel. It takes five clicks and three minutes.

✓ INSTEAD

Ask your agent directly: 'Check the current status of user X.' This single command uses get_user_auth_details and returns all necessary info instantly.

Confusing roles with active users

✗ AVOID

A PM thinks that listing B2B organizations is enough to show growth, but they miss inactive accounts. They only see the organization count.

✓ INSTEAD

To get a full picture, ask your agent to list clerk organizations first, then follow up with a request for all users via list_clerk_users to cross-reference total user counts.

Ignoring tracking clients

✗ AVOID

The team only checks active sessions and misses that an old device is still logged in. They assume security is fine.

✓ INSTEAD

Always run list_clerk_clients after checking sessions. This identifies every single browser or device instance currently maintaining a connection, providing deeper security context.

The Right Fit

Use this MCP if your workflow requires monitoring and reporting on user lifecycle events, B2B organizational structure, or core authentication metrics. It's perfect for operations teams who need to audit credentials or product managers tracking adoption rates. Don't use it if you just need simple data storage; this isn't a database substitute. If your primary goal is generating reports based on *transactional* data (like payments processed), look for a dedicated financial MCP instead, as this focuses purely on identity and access.

Clerk MCP: Auditing User Authentication in B2B SaaS

Today, checking user status is a clicking nightmare. You open the admin panel to see who signed up (list_clerk_users), then you have to switch tabs to check if they are currently active (list_active_sessions). If you're managing B2B clients, finding out which organization they belong to requires another deep dive into member rosters.

With this MCP, your agent handles all of that. You simply ask it to 'Give me the status for John Doe.' The response pulls together user details, session status, and organizational membership in one clean block of text. It turns a 5-minute manual audit into five seconds of conversation.

Clerk MCP: Managing User Onboarding Logistics

Onboarding users used to mean manually checking the invitation queue, confirming who was invited (list_sent_invitations), and then verifying if the domain they came from was approved on the allowlist. This process is slow and highly prone to human error.

Now, you just ask your agent: 'What's the status of invitations for this quarter?' It aggregates all that data—pending invites, completion dates, and even the system health summary—into one report. You get immediate oversight on your entire growth pipeline.

8 Tools for User & Session Data Monitoring

These tools let you retrieve specific, actionable information about your users, sessions, and organizational structure instantly.

#	TOOL	DESCRIPTION
01	`get_auth_dashboard_summary`	Retrieves key metrics, including total user count and current active sessions, for an overview of system health.
02	`get_user_auth_details`	Fetches specific details about one user account using their identity.
03	`list_auth_allowlist`	Provides a list of all approved identifiers, such as emails and domains, on the authentication allowlist.
04	`list_clerk_clients`	Lists all tracking clients, which are instances identifying where users are currently logged in (e.g., browser or device).
05	`list_sent_invitations`	Retrieves a full list of user invitations, showing both those that are pending and those already completed.
06	`list_clerk_organizations`	Lists all B2B organizations within the application and details their member rosters.
07	`list_active_sessions`	Pulls a list of every currently active user session across all connected platforms.
08	`list_clerk_users`	Retrieves the complete directory and details for every registered user in your application.

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 quick snapshot: how many total users do we have, and are there any high-risk active sessions running right now?

Authentication Dashboard Summary

- 👤 **Total Users:** 1,240
- 🟢 **Active Sessions (Current):** 78
- ⚠️ **Suspicious Activity:** 3 sessions detected from new geographic areas. Review recommended.

The system health looks good, but those three sessions should be checked immediately.

U Can you list all the B2B organizations we manage and tell me who belongs to 'Acme Corp'?

Organization Overview

- 🏢 **Total Organizations:** 45
- 💡 **Example Organization:** Acme Corp (ID: org_987)
- 👥 **Members of Acme Corp:** John Smith, Jane Doe, Mike Brown. Status: All active.

U Show me the full list of users who signed up last week and their current session status.

Here are 5 new accounts from the past seven days:

USER	EMAIL	LAST ACTIVE SESSION	STATUS
Alex P.	alex@biz.com	Yesterday (10:30 AM)	Active
Sarah K.	sarah@corp.net	Today (9:00 AM)	Active
Ben R.	ben@test.co	Never logged in	Pending/Inactive

Frequently Asked Questions

01 **How does the Clerk MCP help me monitor user accounts without logging into the dashboard?**

It lets your AI client pull all necessary user and session data directly through natural conversation. You can check total users, find specific profiles using get_user_auth_details, and audit organization memberships instantly.

02 **Can I use the Clerk MCP to see which B2B organizations are active?**

Yes. The MCP lets you list all connected B2B organizations (list_clerk_organizations) and check their full roster of members, giving you a clear picture of your enterprise client base.

03 **What if I need to audit who is logged in right now?**

You can use the MCP to list all active sessions (list_active_sessions). This gives you real-time visibility into every device or browser instance currently accessing your application, which is critical for security.

04 **Does Clerk MCP help me track new signups and invitations?**

Absolutely. You can review both pending and completed user invitations (list_sent_invitations) and list all registered users to get a comprehensive view of your growth pipeline and onboarding funnel.

05 **Is the Clerk MCP good for developers needing quick session data?**

Yes. Developers can use this MCP to run commands like getting the authentication dashboard summary, providing immediate metrics on user counts and system health without writing boilerplate code.

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": { "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	`019d7571-c76b-72ac-92e2-b133526f0b5a`
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.