MCP SERVER | NO CODE | CLOUD HOSTED

Atlassian Crowd MCP for AI Agents

Manage User Directory and Group Access Control

Atlassian Crowd gives your AI client the power to manage corporate user directories and group memberships. Use it to provision new accounts, search for specific employee attributes, or audit who belongs to which security group—all through natural language conversation.

F Quality Score 3.6/100

sso | user-provisioning | directory-services | iam | group-management | access-control

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

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.

Atlassian Crowd MCP

10 tools available
Cloud-hosted on Vinkius

Managing identities is a constant headache. Trying to figure out if someone has the right access level usually means clicking through five different dashboards and running multiple manual checks. This MCP connects your AI agent directly into Atlassian Crowd, letting you handle complex directory tasks via chat.

You can ask your agent things like, 'Which users in engineering don't have Jira access?' or 'Create an account for Jane Doe with these attributes.' Your agent handles the API calls and returns clean lists. It takes identity management from a series of tedious clicks to simple conversation. When you connect this MCP through Vinkius, you get one central place to manage your entire corporate user lifecycle.

Core Capabilities

01 — Search for specific users

Find employee profiles using names or complex attributes instead of relying on manual searches.

02 — Manage group membership lists

Get comprehensive lists of all users belonging to a specified security group, making audits simple.

03 — Audit user roles and permissions

Determine exactly which groups an individual user belongs to by checking their current memberships.

04 — Provision new employee accounts

Create full, operational accounts for new staff members directly through the chat interface.

05 — View directory status reports

Retrieve lists of all active or disabled users to help with cleanup and compliance checks.

One Click on Vinkius — From Prompt to Execution

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

01 Connect the Atlassian Crowd integration using your preferred AI client.

02 Authorize the connection by providing your specific Crowd Base URL, Application Name, and Application Password.

03 Use natural language to instruct your agent on identity tasks—for example, asking it to 'List all users in the sales department who aren't active.' The agent executes the necessary API calls and gives you a clear data report.

The bottom line is that this MCP turns complex directory lookups into simple conversation prompts.

Built For

This is for IT Administrators, Security Teams, and DevOps Engineers who spend too much time navigating multiple dashboards to manage user access. If you're tired of manual audits and provisioning delays, this MCP gives your agents the control they need.

IT Administrator

Audits group memberships for compliance checks or quickly verifies if a specific account needs to be reset or deactivated.

Security Team Member

Searches user attributes across the directory and monitors access patterns to spot potential security risks or unauthorized accounts.

DevOps Engineer

Provisions new application-specific user accounts with detailed attribute definitions, integrating identity management directly into development workflows.

What Changes When You Connect

01 Automate account setup. Instead of manually running provisioning steps, your agent uses `create_new_user` to provision accounts instantly.

02 Simplify audits. Use `list_group_memberships` or `get_user_details` to quickly confirm who has access and why, cutting down audit time significantly.

03 Improve search accuracy. You can use `search_users_by_attribute` to find users based on department or role, not just names.

04 Control group visibility. The MCP gives you the ability to run through `list_all_groups` and get a clear picture of your entire organizational structure.

05 Handle lifecycle events. Quickly identify stale accounts by running `list_inactive_users`, ensuring directory hygiene.

Real-World Applications

A new hire needs immediate access

An HR manager asks their agent to set up a worker's account. The agent uses `create_new_user` and automatically adds them to the required initial groups, ensuring zero downtime.

Compliance audit for privileged accounts

A security analyst needs to verify who has admin access to a sensitive system. They ask the agent to run `list_group_members` on the 'Admins' group and review every single member.

Finding an employee's current role

A manager needs to know which groups a specific employee belongs to. They ask the agent, and it uses `list_user_memberships` to give them a definitive list of all group roles.

Cleaning up old accounts

The IT team suspects many people left without deactivating their records. They run `list_inactive_users` to get a full report and tackle cleanup in bulk.

Patterns to Avoid

Searching by name only

✗ AVOID

Asking the agent, 'Find all people named John.' This usually returns too many results or misses people whose records are incomplete.

✓ INSTEAD

To get accurate results, use `search_users_by_attribute` and narrow your search down. For example: 'Search for users where department=Sales AND status=Active.'

Assuming group structure

✗ AVOID

Telling the agent to just check a group without knowing its full scope, which can lead to missing dependencies.

✓ INSTEAD

Always start by running `list_all_groups` first. Then, use `get_group_details` on specific groups to confirm their purpose before auditing membership.

Manually listing all users

✗ AVOID

Running a prompt like 'List everyone.' This is inefficient and doesn't help with compliance checks.

✓ INSTEAD

If you need an active user count, use `list_active_users`. If you need to check for old accounts, always run `list_inactive_users` instead.

The Right Fit

Use this MCP if your primary pain points revolve around managing identities: provisioning accounts, auditing group access, or finding users based on non-name attributes. It's perfect for IT Security and DevOps teams that need a single source of truth for user directories. Don't use it if you just need to read general company news or manage project tickets—you'll need a different type of connector. If your goal is purely workflow automation (like sending emails), focus on messaging integration instead. This MCP specializes in the *who* and *what* of access control.

Atlassian Crowd MCP: Solving Directory Management Pain

Today, checking a user's true access level is painful. You have to navigate the user profile, check group memberships in one tab, and then manually cross-reference that list with application permissions spread across different systems. It’s copy-pasting data between three or four windows just to answer: 'Does this person actually have permission X?'

With Atlassian Crowd MCP, you simply ask your agent about the user's access. You can tell it to check a specific user's groups and attributes in one conversation turn. The result is clean data that tells you exactly what they can do—no more clicking through five different tabs.

Atlassian Crowd MCP: Streamlining User Provisioning Workflows

The old way of onboarding a new employee meant multiple tickets: one for the IT team to create the account, another for HR to add them to groups, and a third for the manager to assign roles. It was slow, error-prone, and required constant manual handoffs.

Now, you can tell your agent in one go, 'Provision a new user for John Smith who reports to Mary.' The MCP handles account creation (`create_new_user`) and group assignment with a single command. You get the full record updated instantly.

Atlassian Crowd: 10 Tools for Directory Access Control

Use these tools to provision accounts, audit group roles, search user data, and manage the entire corporate identity lifecycle via your AI agent.

#	TOOL	DESCRIPTION
01	`create_new_user`	Creates a complete user account within the Crowd directory.
02	`get_group_details`	Retrieves specific information about an organizational group.
03	`get_user_details`	Fetches the full profile and attributes for any specified user.
04	`list_group_members`	Lists every single user who belongs to a given group.
05	`list_all_groups`	Provides a complete list of all security and organizational groups available in the directory.
06	`list_inactive_users`	Retrieves a comprehensive list of users who have been disabled or are marked as inactive.
07	`list_user_memberships`	Lists every group that a specific user has joined.
08	`list_active_users`	Gets a list of all users currently marked as active in Crowd.
09	`search_users_by_name`	Searches for users whose names start with a specific text prefix.
10	`search_users_by_attribute`	Performs detailed user searches using complex criteria strings, like filtering by department or manager.

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 active users in the 'Engineering' department who haven't logged in for 90 days.

Active User Report: Engineering

We found 42 users matching your criteria. These accounts are currently marked as active but require review.

- `jdoe@corp.com` (Last Login: 10/15/2023)
- `tchen@corp.com` (Last Login: 10/28/2023)
- `mgarcia@corp.com` (Last Login: 10/01/2023)

Please confirm if these users should be deactivated.

U What groups does user 'jsmith' belong to? Also, check his full profile details.

User Profile: John Smith (jsmith)

- **Title:** Senior Developer
- **Department:** Engineering
- **Email:** jsmith@corp.com
- **Status:** Active

Group Memberships:

1. `jira-users` (Read/Write)
2. `engineering-leads` (Admin)
3. `company-all-staff` (View Only)

U Search for all users with the attribute 'Manager' and whose department is Marketing.

Marketing Managers Found

I found 6 users matching your search criteria:

NAME	EMAIL	GROUP MEMBERSHIPS
Sarah Lee	slee@corp.com	`marketing-leads` , `all-staff`
David Kim	dkim@corp.com	`marketing-leads` , `sales-read`

Do you want to see the details for any of these individuals?

Frequently Asked Questions

01 **How does Atlassian Crowd MCP help me audit user access?**

It gives your AI agent the ability to check every group a user belongs to using `list_user_memberships`. You can quickly verify who has access and ensure compliance without opening dozens of tabs.

02 **Can I use Atlassian Crowd MCP to add new users?**

Yes, you can. Using the agent's capabilities, you tell it exactly what attributes a new hire needs (department, title) and it uses `create_new_user` to provision the full account.

03 **Is Atlassian Crowd MCP better than just searching by name?**

Absolutely. Instead of relying only on names, you can use advanced searches that look at attributes like department or manager using `search_users_by_attribute`, giving you much more precise results.

04 **What if I need a list of all potential groups?**

You can run a command to get a complete overview by listing all security and organizational groups via `list_all_groups`. This helps map out your entire directory structure for audits.

05 **Does Atlassian Crowd MCP handle inactive accounts too?**

Yes. You can easily run reports on disabled or retired staff using the `list_inactive_users` function, helping you keep your user directory clean and secure.

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 `"atlassian-crowd": { "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

Atlassian Crowd 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 Atlassian Crowd. 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	Atlassian Crowd MCP
Server ID	`019d7554-57ee-70e8-9360-fc03413c7b4a`
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/atlassian-crowd.