MCP SERVER | NO CODE | CLOUD HOSTED

Casdoor (IAM) MCP for AI Agents

Audit and manage identity access control across all systems

Casdoor (IAM) connects your identity services directly to any AI agent. It lets you manage user accounts, audit organizational structures, and control registered applications—all via natural conversation. You can provision users, check permissions, and maintain compliance without leaving your coding environment.

A+ Quality Score 98.33/100

iam | authentication | user-management | casdoor | access-control

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

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.

Casdoor (IAM) MCP

10 tools available
Cloud-hosted on Vinkius

Managing identities used to mean jumping between dashboards: one for users, another for groups, and a third for application keys. This MCP changes that by giving your AI client direct access to your Casdoor IAM instance. You can now handle the entire user lifecycle through chat prompts alone. Need to create a new employee account? Your agent handles it. Want to check if an app still needs its credentials updated? Just ask. Because this connector manages everything from individual profiles to complete organization oversight, you get a single point of control for your identity infrastructure. By connecting via Vinkius, you gain access to robust identity and access management tools directly in the conversational layer of your favorite AI client.

Core Capabilities

01 — Provisioning and Updating Users

Add new user accounts or modify existing profiles by providing specific details like the owner organization and username.

02 — Auditing Organizations

List all organizations within your Casdoor account and pull specific configuration data for any given IAM hierarchy.

03 — Managing Applications

Query a list of registered applications or fetch the full details for one specific application instance.

04 — Viewing User Details

Instantly retrieve the profile and current status of any user by providing their unique ID.

05 — Checking Authentication Status

Get a real-time view of the currently authenticated user's full profile to confirm permissions immediately.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and provide your Casdoor Endpoint, Client ID, and Client Secret credentials.

02 Your AI client authenticates with the connection details, establishing a secure link to your IAM instance.

03 You simply ask your agent—'Show me all users in the marketing department'—and it executes the required actions using the connected tools.

The bottom line is: you use natural language prompts to trigger structured administrative tasks, letting your AI client do the heavy lifting across your identity systems.

Built For

This MCP is built for technical roles who spend too much time clicking through dashboards and executing repetitive admin tasks. If you're tired of manually auditing user permissions or provisioning new accounts via a web UI, this is what you need.

Security Analyst

You check user access rights and application configurations for compliance audits without logging into three different consoles.

DevOps Engineer

You automate the creation, modification, or deletion of test accounts across various organizational units directly from your terminal or IDE.

Full-stack Developer

You manage application settings and user roles for testing environments while keeping your development flow uninterrupted.

What Changes When You Connect

01 Automate user provisioning: Use the `add_user` tool to create new accounts, or `update_user` to modify profiles, eliminating manual dashboard logins.

02 Centralize auditing: Quickly list every organization using `list_organizations`, giving you a complete map of your IAM structure in one go.

03 Secure credential management: Use `list_applications` and `get_application` to maintain an accurate inventory of all linked services.

04 Instant compliance checks: The `get_userinfo` tool lets you confirm the permissions and profile of any authenticated user on demand.

05 Simplify user discovery: Need to find a specific account? Use `list_users` or `get_user` to pull detailed records without guessing usernames.

Real-World Applications

Onboarding a new team member

A DevOps engineer needs to provision five temporary test accounts for a project. Instead of running through the web UI multiple times, they prompt their agent: 'Create five dev users in the engineering organization.' The agent uses `add_user` repeatedly and reports success.

Quarterly Security Audit

A security analyst must verify who has access to critical systems. They ask the agent to list all organizations (`list_organizations`) and then check application ownership by listing every registered app using `list_applications`.

Revoking Old Credentials

A developer needs to terminate an employee's access immediately. They instruct their agent to find the user's record via `get_user` and then execute a full deletion using `delete_user`, logging the action instantly.

Reviewing Service Dependencies

A team needs to know which applications are running on an old platform. The agent uses `list_applications` to get the names, then runs `get_application` for each one to check its current status and owner.

Patterns to Avoid

Manual Role Checks

✗ AVOID

A user manually logs into the web portal, navigates deep into settings, and clicks through several tabs just to confirm a single permission setting.

✓ INSTEAD

Ask your agent directly. Use `get_userinfo` or prompt for specific permissions checks against the Casdoor instance. It gives you the answer immediately.

Forgetting Scope

✗ AVOID

When trying to update a user, forgetting which organization they belong to and receiving an 'invalid scope' error.

✓ INSTEAD

Always confirm your target with `get_organization` first. Then use the full path format required for `update_user`, like `<org>/<username>`.

Over-relying on UI Filters

✗ AVOID

Using a web interface's search bar, which often fails to surface users or applications that are miscategorized or inactive.

✓ INSTEAD

Use `list_users` and `list_applications`. These tools pull the comprehensive data directly from the source of truth, guaranteeing you see everything.

The Right Fit

You should use this MCP if your job requires checking user identity or managing access control across multiple systems. If auditing is a core part of your routine—whether it's provisioning accounts, reviewing organizational boundaries with `list_organizations`, or ensuring an application is up to date via `get_application`—this tool saves massive amounts of time. However, don't use this if you only need simple messaging or data storage; those tasks require different types of connectors. If your problem is just 'I need a list of all departments,' and that department structure isn't tied to IAM roles, then another catalog MCP will work better.

Casdoor (IAM) for AI Agents: Managing User Access Control

Today, managing user access is a nightmare of clicks. You have to log into the CASDOOR portal, navigate to 'Users,' filter by department, and then copy/paste usernames into a spreadsheet just to start an audit. If you need to check if an application has been decommissioned, you're stuck opening a separate dashboard for that service.

With this MCP, your agent handles the whole sequence in one chat window. You simply ask it to list all users and then verify their roles or manage them using `add_user` or `delete_user`. It brings the entire identity lifecycle into conversation.

Casdoor (IAM) for AI Agents: Auditing Organization Structure

Without this MCP, mapping out your company's organizational units is a manual process. You have to click through 'Root,' then 'Division A,' then 'Team 1,' and hope you haven't missed any subsidiaries just because the UI didn't link them correctly.

Now, simply ask your agent to list all organizations using `list_organizations`. It pulls the entire hierarchy instantly. You get a clear map of who belongs where without clicking through twenty different menus.

Casdoor (IAM) 10 Tools for User Management and Access Control

Use these tools to list, create, delete, and modify user profiles, track organizations, or audit connected applications using natural language commands.

#	TOOL	DESCRIPTION
01	`add_user`	Creates a new user account, requiring the organization owner and the desired username.
02	`delete_user`	Removes an existing user account after confirming both the organization and the specific username.
03	`get_application`	Retrieves all defined details for a single, specified application within Casdoor.
04	`get_organization`	Fetches the full configuration and details for one specific organization unit.
05	`get_user`	Pulls detailed profile information for a user when given their unique ID.
06	`list_applications`	Generates a list of every application registered within the current organization scope.
07	`list_organizations`	Returns a comprehensive list of all organizational units managed by your Casdoor instance.
08	`list_users`	Lists every user account belonging to a specific organization unit.
09	`update_user`	Modifies existing details for an account, requiring the owner/organization and username format.
10	`get_userinfo`	Immediately retrieves the profile information for the user who is currently logged in or authenticated.

See It in Action

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

U Show me all user accounts in the 'marketing-dept' and list their current roles.

Marketing Department User Audit

- `john.doe` : Active | Role: Marketing Lead | Last Login: 2024-10-15
- `jane.smith` : Inactive | Role: Content Writer | Last Login: N/A
- `test_user_mktg` : Active | Role: Trainee | Last Login: Today

Next Steps: Would you like to update John Doe's permissions or archive Jane Smith's account?

U What applications are currently linked and who owns them?

Registered Applications Summary

APP NAME	OWNER ORG	STATUS
Billing API	built-in	Active
Auth Service v2	engineering-team	Needs Review
CMS Gateway	marketing-dept	Active

Note: The 'Auth Service v2' owner needs to update their credentials.

U I need a new user for the QA team. Can you set it up?

Okay, I can create that account right away. Please confirm the username and whether this belongs in the 'engineering-team' organization.

Confirmation Needed: Username & Organization

Once confirmed, I'll use the appropriate tool to add them and report back with their new profile details.

Frequently Asked Questions

01 **How can I use Casdoor (IAM) MCP to audit my user accounts?**

You connect this MCP, then ask your agent to list all users in a specific organization. The agent uses the necessary tools to pull comprehensive data on every account and their current status.

02 **Does Casdoor (IAM) MCP let me delete user accounts?**

Yes, it does. If you confirm the owner and the username, your agent executes a secure deletion command, removing the user from your identity system instantly.

03 **What kind of organizations can Casdoor (IAM) MCP manage?**

The tool manages all organizational units within your Casdoor instance. You simply ask the agent to list them, and you get a full breakdown of every department or division you've set up.

04 **Can I check my own permissions using this MCP?**

Absolutely. By asking the agent for your user info, it instantly fetches your profile details, letting you verify exactly what access rights are assigned to your account right now.

05 **If I need to change a username or role, can Casdoor (IAM) MCP help?**

Yes. You use the update function by giving the agent the required details for both the organization and the user's current ID. It handles modifying existing accounts seamlessly.

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 `"casdoor-iam": { "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

Casdoor (IAM) 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 Casdoor (IAM). 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	Casdoor (IAM) MCP
Server ID	`019e3874-e2e1-73fc-afa3-3c85d9af2b4c`
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/casdoor-iam.