MCP SERVER | NO CODE | CLOUD HOSTED

Okta MCP for AI Agents

Manage user identities and group permissions in your Okta Identity Cloud.

Okta MCP lets your AI agent manage users, groups, and authentication in your Okta Identity Cloud without you having to click through a dashboard.

A+ Quality Score 100/100

authentication | user-provisioning | sso | identity-management | access-control | security-policy

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JULY 2026
vinkius.com/mcp/okta

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.

Okta MCP

10 tools available
Cloud-hosted on Vinkius

Okta MCP connects your AI agent directly to your identity cloud so you can handle user management through simple conversation. Instead of hunting through complex administrative menus to find a locked account or manually assigning a new hire to a dozen different groups, you just tell your agent what needs to happen. It handles the heavy lifting of provisioning identities, revoking access for departing employees, and auditing your current app integrations. You can ask it to pull a list of everyone in a specific department or check the sign-in logs for a suspicious spike in activity. By adding this to your setup through the Vinkius catalog, you turn a multi-click administrative chore into a quick request. It is about getting the right people into the right systems without the friction of traditional dashboard navigation. You can quickly see which applications are mapped to your user base or check the specific SSO configurations for your core tools. If a device is stolen, you can tell your agent to kill all active sessions for that person immediately. It removes the need to keep multiple tabs open for basic identity tasks, letting you focus on higher level security strategy instead of manual data entry. You can also use it to see which users were automatically granted licenses through directory mapping. This means you spend less time on the "how" of identity and more time on the "who" of your organization.

Core Capabilities

01 — Provision new identities

Create new user accounts and assign them to the correct departments instantly.

02 — Revoke user access

Deprovision employees and kill all active sessions to secure company data.

03 — Terminate active sessions

Force a logout for any user across all connected applications from a single command.

04 — Audit group memberships

Query which users belong to specific security or application groups.

05 — Review application configs

Check SSO bindings, secrets, and token lifespans for your integrated apps.

06 — Monitor sign-in logs

Retrieve recent audit events to spot malicious activity or configuration changes.

07 — List all directory users

Get a complete list of everyone in your Okta Universal Directory for reporting.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the Okta MCP via the Vinkius catalog.

02 Provide your Okta domain and organizational API Key.

03 Ask your agent to perform tasks like 'block user X' or 'list all admins'.

The bottom line is you get a conversational interface for your entire Okta identity directory.

Built For

This is for the IT admin who's tired of clicking through dashboards at 2am to unlock accounts, or the SecOps analyst hunting for compromised sessions.

Helpdesk Technician

Responding to 'I'm locked out' tickets by quickly resetting credentials or clearing sessions via chat.

Security Operations Analyst

Identifying and terminating hazardous sessions or auditing app permissions during an active security incident.

IT System Administrator

Handling bulk user onboarding and offboarding without manual CSV uploads or tedious manual entry.

What Changes When You Connect

01 Shut down compromised accounts instantly with `deactivate_user` to stop unauthorized access before it causes damage.

02 Kill all active sessions for a user with `clear_user_sessions` when a laptop or phone goes missing.

03 Audit your entire app footprint by using `list_apps` to see every OIDC, SAML, and SCIM connection in one place.

04 Identify permission gaps quickly by using `list_groups` to see exactly how your security and dynamic groups are organized.

05 Verify specific user statuses and profile details using `get_user` without having to search through a large directory manually.

06 Monitor security events in real-time by pulling recent logs with `list_system_logs` to spot suspicious activity.

Real-World Applications

Emergency session termination

A laptop is stolen and you need to kill all sessions immediately. The agent uses `clear_user_sessions` to lock down the account and protect company data.

Automated new hire onboarding

A new employee joins and needs access to the Engineering group. The agent uses `list_group_users` and `get_group` to verify permissions and assign access.

Security audit of a specific app

You need to audit who has access to Jira. The agent uses `list_apps` and `list_groups` to identify all users with relevant permissions.

Rapid user status verification

An admin needs to see if a specific user is still active. The agent uses `get_user` to pull the profile and status in one second.

Patterns to Avoid

Deleting users without checking group membership

✗ AVOID

Asking the agent to delete a user without checking their groups first.

✓ INSTEAD

Use `list_group_users` first to see who is affected by the group mapping before taking action.

Attempting to manage non-Okta applications

✗ AVOID

Trying to use the MCP to manage a standalone app that isn't integrated with Okta.

✓ INSTEAD

This MCP only interacts with your Okta Identity Cloud. Ensure your apps are integrated with Okta first.

Requesting bulk audits in a single command

✗ AVOID

Asking the agent to audit 10,000 users in one single request.

✓ INSTEAD

Use `list_users` to get the full list, then ask for specific details on smaller batches to avoid timeout issues.

The Right Fit

Use this if you need to perform identity tasks like user provisioning, session termination, or group auditing within Okta. It's perfect for helpdesk automation and SecOps incident response. Don't use it if you need to manage non-Okta applications or if you're looking for deep configuration of the Okta platform itself, like setting up complex policies. For those tasks, you'll still need to use the Okta admin console. This MCP is for the actions you do every day, not the high-level infrastructure setup.

Okta MCP for Identity Management and User Provisioning

Managing identities usually means jumping between multiple browser tabs, searching for specific user IDs, and clicking through deep administrative menus to find the right settings. You might spend twenty minutes just trying to find which groups a new hire needs to join or checking if a specific account was compromised.

With the Okta MCP, you just tell your agent what to do. You can ask it to deprovision a user or list every person in a security group in seconds. You get your work done in one sentence instead of a dozen clicks.

Okta MCP for SecOps and Automated Access Audits

You no longer have to manually audit your application integrations or scroll through endless system logs to find a single sign-in anomaly. The

You move from manual data entry to high-level oversight. It's the difference between being a button-pusher and a security strategist.

MCP pulls this data instantly, giving you a clear view of your security posture.

Okta MCP and 10 Identity Management Tools

Use these tools to manage users, audit groups, and monitor security logs in your Okta directory.

#	TOOL	DESCRIPTION
01	clear_user_sessions	Terminate all active login sessions for a specific user. This is necessary to protect data if a device is compromised or stolen.
02	deactivate_user	Instantly convert a user status to deprovisioned and revoke all active sessions. Use this for emergency offboarding to block all future app access.
03	get_group	View the details of a specific Okta group. This helps you see who is part of a group and what permissions they have.
04	get_user	Get a detailed profile and state for a specific Okta user. Use this to check a user's account status or department mapping.
05	get_app	View the detailed SSO configuration for a specific application. This includes security bindings, secrets, and token lifespans.
06	list_groups	List all security, app, and dynamic Okta groups. Use this to audit permissions and see how users are organized.
07	list_users	List all users configured in your Okta Universal Directory. This is useful for organization-wide identity reporting.
08	list_system_logs	Retrieve the most recent 100 Okta system and audit log events. This helps you identify malicious password spraying or configuration tweaks.
09	list_apps	List all applications integrated within your Okta dashboard. Use this to identify all OIDC, SAML, and SCIM connections.
10	list_group_users	List all users currently assigned to an Okta group. Use this to see exactly who was granted licenses or access via directory mapping.

See It in Action

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

U Retrieve the user profile for 'mark@example.com'.

I found the profile for ID `00u12xxxxxxx`: Mark Johnson. The account status is currently **ACTIVE** and mapped to the 'Engineering' department.

Would you like to check his group associations?

U Clear all active sessions for user 'mike@example.com' immediately.

Success. I've sent the termination command to Okta.

All active sessions for `mike@example.com` **have been cleared and closed**, forcing a re-login for any connected service.

U List all active application mappings for the 'Contractors' group.

Scanning Group mapping ID `00xxxx` ('Contractors'): I found 3 provisioned apps tied to this cohort:

- **Slack** (Provisioning Active)
- **Atlassian Jira Server** (SAML)
- **Zoom** (SAML)

Do you want me to revoke any permissions immediately?

Frequently Asked Questions

01 **How can Okta MCP help my helpdesk team?**

It lets your team handle 'I'm locked out' tickets via chat. Your agent can quickly reset credentials or clear sessions without the tech needing to open the Okta dashboard.

02 **Can I use Okta MCP to offboard employees?**

Yes, it can instantly deactivate users and kill all active sessions. This ensures that access is revoked across all integrated apps the moment an employee leaves.

03 **Does Okta MCP work with my existing apps?**

It manages the Okta integrations for your apps. If your apps are connected to Okta via SAML, OIDC, or SCIM, your agent can manage those permissions.

04 **Is Okta MCP safe for security audits?**

It's a great tool for audits because it can pull system logs and group memberships. You can quickly see who has access to what and spot any suspicious sign-in attempts.

05 **How do I connect Okta MCP to my AI agent?**

You subscribe to the MCP via the Vinkius catalog and provide your Okta domain and API Key. From there, your agent can start performing identity tasks for you.

06 **Where do I retrieve my Okta Domain and API Token?**

Log in to your Okta Admin Console. The Okta domain is simply the URL you use (e.g., `company.okta.com`). To get the API Key, navigate to **Security** → **API**, then select the **Tokens** tab. Click **Create Token**, assign it a name, and securely copy the generated string.

07 **Can the agent clear active sessions for a compromised user?**

Yes! If you suspect an ongoing security incident, you can promptly ask the agent to clear user sessions (`clear_user_sessions`) by simply stating the user's ID or email. The integration talks back to Okta and terminates persistent connections instantaneously.

08 **Is the administrator API key shared globally with anyone else?**

No, your setup is extremely private and BYOC (Bring Your Own Credentials). The token is entered locally inside your private environment or workspace instance and injected tightly and exclusively into your isolated runtime execution. It is never exposed publically.

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 `"okta": { "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

Okta 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 Okta. 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	July 2026
MCP Server	Okta MCP
Server ID	`019d75e4-0470-7139-8db4-8eb4403df914`
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/okta.