MCP SERVER | NO CODE | CLOUD HOSTED

WorkOS MCP

Manage identity and audit systems without leaving your chat client.

WorkOS connects your enterprise identity platform to your AI agent, letting you manage complex organizations, audit security logs, and monitor Single Sign-On (SSO) connections via natural chat. Use this MCP to handle directory sync status checks and user roster lookups without ever logging into the WorkOS dashboard.

A+ Quality Score 100/100

sso | saml | oidc | directory-sync | audit-logs | enterprise-ready

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

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.

WorkOS MCP

10 tools available
Cloud-hosted on Vinkius

Managing an enterprise's identity infrastructure shouldn't feel like navigating a decade-old web portal. This MCP connects your WorkOS account to any AI agent, letting you treat your entire organization setup as just another conversation. Instead of clicking through multiple tabs to check if a directory sync is active or finding the unique ID for a specific tenant, you simply ask your agent. You can instantly list and audit all connected SSO services like SAML and OIDC links, or retrieve detailed metadata about any synced user group or organization. The Vinkius catalog makes it easy: connect once from your preferred AI client and gain full control over governance tasks—from creating new organizational records to streaming security audit logs—all through simple chat commands.

Core Capabilities

01 — Audit Security Events

The agent streams detailed historical events, letting you monitor who accessed what and when across any organization.

02 — Manage Organization Structure

You can list all existing organizations or create new ones by specifying the name and authorized domains.

03 — Monitor SSO Health

The MCP lists all active Single Sign-On connections, allowing you to check the status of critical enterprise authentication links.

04 — Check Directory Sync Status

You get metadata and sync details for connected directories from providers like Okta or Azure AD.

05 — List User Rosters and Groups

The agent retrieves complete lists of users and groups synced into WorkOS from your external directory.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius, then provide your API Key.

02 Connect the credential to your preferred AI client (like Cursor or Claude).

03 Ask your agent a question, like 'List all organizations' or 'Check SSO status for Acme Corp', and get immediate answers.

The bottom line is that your AI agent becomes your identity administrator, eliminating the need to manually browse WorkOS dashboards.

Built For

This MCP targets security and operations staff who spend too much time switching between administrative consoles. If you're an engineer who needs real-time audit status or a compliance team needing historical proof of access control, this is for you.

Security Engineer

Uses the MCP to retrieve audit logs and verify SSO connection health across all connected tenants.

Product Manager

Audits the list of organizations and verified domains to plan new product features or market rollouts.

Support Operations Specialist

Quickly looks up specific organization details or user rosters when providing technical assistance to enterprise clients.

What Changes When You Connect

01 Audit logs: Instead of navigating through complex security dashboards to find an event, you ask for it. The agent streams detailed audit log events instantly.

02 Directory Sync: You can check the metadata and status of all connected directory instances (like Okta or Azure AD) without clicking into each one individually.

03 User Rosters: Needing a list of users? Use the MCP to pull complete user lists or specific group rosters from your synced directories, saving minutes of manual data compilation.

04 SSO Management: Quickly get a full count and status update on all active Single Sign-On connections using `list_sso_connections`, keeping your authentication links healthy.

05 Organization Mapping: When you're planning a new deployment, use the MCP to list all existing organizations or even create new ones with specific authorized domains.

Real-World Applications

Investigating Unauthorized Access

A security team member needs to know if a particular client's account was accessed last month. Instead of manually building complex queries, they ask the agent to `get_audit_log_events` for that organization ID and immediately see the stream of access attempts.

Pre-launch Governance Check

A Product Manager is launching a new enterprise feature. They first use `list_workos_organizations` to confirm every tenant is accounted for, then call `get_directory_details` on the primary directory ID to ensure sync readiness.

Troubleshooting Sync Breakage

An engineer notices user groups are missing. They use `list_directories` to confirm which sync source is down, and then call `list_directory_groups` using the correct directory ID to verify group membership.

Client Onboarding Setup

A support specialist needs to set up a new client. They use `create_workos_organization`, providing the necessary name and authorized domains, completing the initial setup in seconds.

Patterns to Avoid

Manual Dashboard Checks

✗ AVOID

A user has to open the WorkOS dashboard, click 'Audit Logs,' filter by date range, then manually copy and paste event IDs into a spreadsheet for review.

✓ INSTEAD

Ask your agent directly using `get_audit_log_events`. The MCP handles the filtering and streaming of data, giving you the raw information instantly.

Guessing Organization IDs

✗ AVOID

A user doesn't know if 'Client Alpha' or 'Alpha Corp' is the correct ID for a sync test and spends 15 minutes searching through multiple tenant lists.

✓ INSTEAD

First, run `list_workos_organizations` to see all available names. Then use `get_organization_details` with the specific ID you find.

Forgetting Connection Status

✗ AVOID

A team member assumes an SSO link is active because it hasn't thrown an error yet, but doesn't know if OIDC or SAML is actually configured.

✓ INSTEAD

Run `list_sso_connections` to get a comprehensive list of every connection. Then use `get_sso_connection_details` on the specific link you need to verify.

The Right Fit

Use this MCP if your primary pain point is operational governance—you need to audit, monitor status (SSO/Directory), or manage identity records at scale. If you frequently ask questions like 'What's the sync status for Tenant X?' or 'Show me all users in Group Y,' this tool handles that complexity. Don't use it if your only goal is simply viewing a single static piece of data; other, more focused connectors might be better. Also, if you don't need to audit logs or manage SSO connections, but just listing basic tenants is enough, confirm the scope of `list_workos_organizations` meets your needs before committing.

The Pain of Administrative Overload

Today, checking your enterprise identity infrastructure means logging into WorkOS. You navigate to the SSO tab to check connection health. Then you jump to Directory Sync to see if users are syncing correctly. If you need an audit, you have to find a different section entirely. It’s a painful sequence of clicking through multiple dashboards just to get one status update.

With this MCP, that entire process shrinks down to conversation. Your agent handles the clicks for you. You ask about SSO health or directory sync status, and it gives you the full picture in plain text—no dashboard required.

Get Full Visibility with WorkOS MCP

The manual steps that vanish are: manually switching between SSO links and directory sync monitors; piecing together user lists from multiple sources; and building complex audit reports by exporting data piece by piece.

Now, you treat your entire identity platform like a conversational database. You ask, it delivers the comprehensive report. That's how modern ops teams work.

WorkOS MCP: Directory & Governance Tools (10 tools)

Use these ten tools to control everything from creating new organizational accounts to retrieving detailed user rosters and auditing security events.

#	TOOL	DESCRIPTION
01	`create_workos_organization`	Creates a new organizational record by requiring the name and authorized domains.
02	`get_audit_log_events`	Retrieves a stream of security events tracked within a specific organization.
03	`get_sso_connection_details`	Fetches detailed information for one particular Single Sign-On connection.
04	`get_directory_details`	Retrieves metadata about a specific directory instance, such as Okta or Azure AD connections.
05	`get_organization_details`	Fetches detailed information for a given organization ID.
06	`list_sso_connections`	Lists every active Single Sign-On connection configured across the account.
07	`list_directories`	Provides a list of all currently running directory synchronization instances.
08	`list_directory_groups`	Lists every group that has been synced from an external directory source.
09	`list_workos_organizations`	Retrieves a comprehensive list of all organizations managed in the WorkOS account.
10	`list_directory_users`	Lists every user that has been synced from an external directory source.

See It in Action

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

U List all organizations in my WorkOS account.

I found 5 organizations: 1. 'Acme Corp' (ID: org_01E...), 2. 'Global Tech' (ID: org_01F...), 3. 'Stark Industries' (ID: org_01G...), and 2 others. Which one would you like to see details for?

U Check the status of SSO connections for 'Acme Corp'.

Acme Corp (org_01E...) has 2 active SSO connections: 1. Okta SAML (Status: ACTIVE, ID: conn_01H...) and 2. Azure AD OIDC (Status: ACTIVE, ID: conn_01I...). Both links are healthy and operational.

U List all users synced from the directory 'dir_01J...'.

I found 120 users in directory dir_01J.... The most recently synced users are: 1. John Doe (john@acme.com), 2. Jane Smith (jane@acme.com), and 3. Robert Brown (robert@acme.com). Would you like to see the full roster or filter by group?

Frequently Asked Questions

01 **How do I list all organizations using WorkOS MCP?**

You use `list_workos_organizations` to get a complete roster of every tenant in your account. This is the fastest way to see how many organizational records you're dealing with.

02 **Can I check SSO connections status with WorkOS MCP?**

Yes, running `list_sso_connections` gives you a full list of all configured SAML and OIDC links. You can follow up by using `get_sso_connection_details` for deeper troubleshooting.

03 What is the difference between listing users and groups in WorkOS MCP?

Use `list_directory_users` when you need a roster of individual accounts (like John Doe). Use `list_directory_groups` if you only care about membership lists, such as 'IT Admin Group'.

04 Does WorkOS MCP help with compliance auditing?

Absolutely. You use `get_audit_log_events` to stream historical security data for any organization, which is crucial for proving who did what and when.

05 How do I create a new organization record via the MCP?

You run the `create_workos_organization` tool. You must provide both the desired name and the list of authorized domains to complete the process.

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 `"workos": { "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

WorkOS 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 WorkOS. 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	WorkOS MCP
Server ID	`019d7624-976b-70fd-a7c1-f593259f9d95`
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/workos.