

MCP SERVER

NO CODE

CLOUD HOSTED

1Password SaaS Manager MCP.

Give your AI agent control over your 1Password organization.

1Password SaaS Manager MCP connects your 1Password organization to any MCP-compatible client. Your agent can now inspect your SaaS catalog, audit logs, and team structures. It can also interact with automation workflows by firing signals to advance or gate specific steps in a run.

A+ Quality Score 96.67/100

1password

saas-manager

saas-catalog

audit-log

workflows



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

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.

1Password SaaS Manager MCP

8 tools available

Cloud-hosted on Vinkius

You can now give your AI agent a seat at the table for 1Password administration. This MCP connects directly to the 1Password SaaS Manager API, allowing your agent to reason about your organization's software footprint and user structure. Instead of clicking through dashboards, you can ask your agent to pull a list of active SaaS apps or check who belongs to a specific team. It can even dig into the audit log to find specific permission changes or sign-in anomalies. For teams using 1Password automations, your agent can inspect the status of a workflow run and fire signals to move a process forward or hold it for review. It turns your AI client into a functional extension of your security and identity operations.

Core Capabilities

01 — SaaS Inventory Management

Your agent can list and inspect every application tracked in your 1Password catalog.

03 — Team Oversight

Your agent can map out your organization's team structure and user memberships.

02 — Identity Auditing

Your agent can pull audit logs to track user actions and permission changes.

04 — Workflow Control

Your agent can monitor automation runs and trigger signals to advance them.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/1password-saas-manager — connect your AI agent in three steps.

- 01 Generate API client credentials in your 1Password organization.
- 02 Select your specific region, such as US or EU.
- 03 Enter your Client ID and Client Secret into the Vinkius credential fields.
- 04 Set the base URL to match your chosen region.
- 05 Connect your preferred MCP-compatible client to start using the tools.

Setting up the connection is a straightforward process through the 1Password SaaS Manager API.

Built For

This MCP is built for technical professionals managing identity and software access at scale.

Security and Compliance Teams

They use the agent to maintain SaaS inventories and surface audit events for review.

Identity Administrators

They use the agent to verify team structures and membership before changing access.

What Changes When You Connect

- 01 Reduces manual clicks by letting your agent query the SaaS catalog directly.

- 02

Speeds up troubleshooting stuck automations by inspecting workflow runs.
- 03

Simplifies compliance checks by pulling filtered audit logs via natural language.
- 04

Enables direct interaction with 1Password workflows through signal firing.

Real-World Applications

Automated Compliance Audits

Ask your agent to find all permission changes that happened over the weekend.

Workflow Troubleshooting

Identify exactly why an onboarding or offboarding automation has stalled.

SaaS Inventory Checks

Quickly verify which software applications are currently active in your organization.

Team Membership Verification

Confirm if a user belongs to a specific team before granting them new access.

Patterns to Avoid

Blindly trusting manual audits

AVOID

You spend hours manually checking user lists in a dashboard to find permission changes. This is slow and prone to human error.

✓ INSTEAD

Use ``list_audit_events`` to pull specific permission changes or security events within a set timeframe through your agent.

Guessing workflow status

AVOID

You assume an onboarding process finished because no one complained, but it actually stalled halfway through.

✓ INSTEAD

Check the exact status and details of the process using ``get_workflow_run`` to see where it stopped.

Manual team mapping

❌ AVOID

You try to manually verify if a new hire belongs to the DevOps team by scrolling through a massive user list.

✓ INSTEAD

Ask your agent to verify membership or pull the organization hierarchy using `'list_teams'` and `'list_people'`.

The Right Fit

Connect this MCP if you manage identity or security for a large organization and need to audit SaaS usage. Do not connect it if you are a solo user with no team structure or automation needs. The decision rests on whether you need to move beyond manual dashboard clicking for your security operations.

8 Tools for 1Password SaaS Management

These tools give your agent direct access to your SaaS catalog, organization hierarchy, and automation workflows.

#	TOOL	DESCRIPTION
01	fire_workflow_signal	Sends a signal to a specific activity within a 1Password workflow run. Use this to advance or unblock a process when you explicitly tell your agent to do so.
02	list_teams	Retrieves the list of teams within your 1Password organization. This helps your agent understand team hierarchy and group-level access.
03	list_workflows	Shows all automation workflows configured in the 1Password SaaS Manager. Your agent uses this to find specific workflows before inspecting their runs.
04	get_application	Fetches detailed information about a specific SaaS application from your catalog. Use this to inspect an app after finding it in the list.
05	get_workflow_run	Provides the status and details of a specific automation workflow run. This is how your agent checks why a process might be stuck.
06	list_applications	Returns the full list of SaaS applications tracked in your 1Password organization. It supports pagination via cursors for large catalogs.
07	list_audit_events	Reads the 1Password audit log. Your agent uses this to track user actions, permission changes, or security events within a specific timeframe.
08	list_people	Lists the users present in your 1Password organization. This allows your agent to verify headcount or check individual membership status.

See It in Action

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

U Which SaaS applications are active in our organization right now?



I found 14 active SaaS apps: Slack, Confluence, Salesforce, Okta, Datadog, Jira, Linear, Notion, GitHub, AWS, GCP, Zendesk, Intercom, and Retool. Do you need details on any of them?

U Show me audit log events from the last 48 hours where admin permissions changed.



I checked the audit log for the last 48 hours. Three admin permission events occurred: a service account was granted admin on Slack, two people left the Security team, and an admin added a new app to the catalog. Should I pull the full details for the service account grant?

U Our onboarding workflow is stuck on step 3. Check that run and tell me what it's waiting for.



The workflow run is stuck at the access-grant activity in step 3. It is waiting for a manual 'continue' signal because a manager needs to approve the new person's team access. Do you want me to fire the signal to unblock it?

Frequently Asked Questions

01 How do I connect this MCP to my 1Password account?

You need to create API client credentials in your 1Password SaaS Manager settings. Once you have the Client ID and Secret, you provide them to Vinkius, and you can connect your AI client immediately.

02 Can my AI agent actually change things in 1Password?

Yes, specifically through the `fire_workflow_signal` tool. This allows your agent to advance or unblock specific steps in an automation workflow when you tell it to.

03 Does this work with any AI client?

It works with any MCP-compatible client, including Claude, Cursor, Windsurf, and VS Code.

04 How does the agent handle large lists of users or apps?

The tools use pagination and cursors. Your agent can request specific limits or use the 'after' parameter to move through large datasets without overwhelming the context.

05 Is my data secure?

The MCP uses short-lived tokens generated by the server to interact with the 1Password API, ensuring your credentials remain protected.

06 Which parts of 1Password does this manage?

The SaaS Manager organization surface: the SaaS application catalog, people, teams, the audit log, and automation workflows. It does not read or manage personal vault items or individual secrets — those are out of scope for this server.

07 How does authentication work?

Machine-to-machine OAuth 2.0 client-credentials. The server exchanges your Client ID and Client Secret for a short-lived bearer token and signs its own requests — no human login, no user session. The base URL selects the region: app.trellica.com (US) or eu.trellica.com (EU).

08 Can it change the organization, or only read it?

Mostly read. The read tools cover the catalog, people, teams, audit log, workflow definitions, and runs. The one state-changing tool is `fire_workflow_signal`, which advances or gates a step of an automation run — use it only when explicitly asked.

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 <code>"1password-saas-manager": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

1Password SaaS Manager 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 1Password SaaS Manager. 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	September 2026
MCP Server	1Password SaaS Manager MCP
Server ID	01a0bb24-9f83-72a7-bf3f-7f382ce81122
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/en/ai-agent-connect/1password-saas-manager.