MCP SERVER | NO CODE | CLOUD HOSTED

BoxyHQ MCP for AI Agents

Automating Enterprise Single Sign-On and Directory Synchronization

Manage enterprise Single Sign-On (SSO) and user provisioning through BoxyHQ's MCP. This tool lets your AI agent automate complex identity workflows, handling everything from SAML/OIDC connection setup to SCIM directory synchronization. Get instant visibility into security configurations and manage user lifecycles without leaving the chat interface.

F Quality Score 3.6/100

sso | saml | oidc | scim | user-provisioning | enterprise-auth

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/boxyhq-enterprise-sso

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.

BoxyHQ (Enterprise SSO) MCP

8 tools available
Cloud-hosted on Vinkius

Running enterprise authentication is complicated. You're dealing with multiple tenants, different protocols (SAML, OIDC), and a constant need for an accurate audit trail. With this MCP, you connect your BoxyHQ instance to your preferred AI client and treat identity management like any other workflow.

Your agent handles the tedious parts of enterprise authentication and user lifecycle control. Need to prove who has access? Ask it to list all SSO connections or check connection metadata by tenant ID. Setting up a new product requires automated user provisioning? The MCP creates SCIM 2.0 directories instantly, managing user creation and de-provisioning automatically. It also lets you update existing security setups or delete stale credentials when they're no longer needed. Because Vinkius hosts this catalog, your AI client can access BoxyHQ's full suite of identity tools from one place, so you don't have to switch dashboards just to verify connection health.

Core Capabilities

01 — Manage SSO Connections

Add, view, or modify SAML and OIDC connections for specific products and tenants.

02 — Automate User Provisioning Directories

Create SCIM 2.0 directories to manage user accounts across your enterprise applications.

03 — Audit Identity Connections

Retrieve detailed metadata about existing connections using client, product, or tenant IDs.

04 — Monitor Service Health

Check the overall operational status and health of the BoxyHQ service.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/boxyhq-enterprise-sso** — connect your AI agent in three steps.

01 Subscribe to this MCP on Vinkius, providing your specific BoxyHQ Instance URL and API Key.

02 Tell your AI agent exactly what you need—for example, 'Add a new OIDC connection for client X.'

03 The agent executes the required action against BoxyHQ and reports back the status, connection ID, or user list.

The bottom line is: you manage complex enterprise identity workflows using plain English prompts instead of navigating multiple web dashboards.

Built For

This MCP is built for security and infrastructure teams dealing with the day-to-day friction of multi-tenant authentication. It saves the Security Engineer from manually clicking through dozens of compliance portals and gives DevOps staff immediate automation during customer onboarding.

Security Engineer

Quickly auditing, updating, or deleting SSO connections across multiple products to maintain a clean security posture.

DevOps/SRE Engineer

Automating the creation of SCIM directories and SAML connections as part of automated customer onboarding pipelines.

Product Manager

Verifying the live status and health of enterprise integrations directly within a chat window without logging into the backend console.

What Changes When You Connect

01 Audit security configurations instantly. Instead of jumping through dashboard menus, your agent uses `get_connections` to list all SSO links across tenants.

02 Eliminate manual provisioning steps. Use `create_directory` to set up SCIM 2.0 directories and automate user lifecycle management during onboarding.

03 Maintain a clean security posture by using `delete_connection` to remove stale or unused credentials when a product is retired.

04 Speed up deployments with metadata control. The agent can configure Identity Provider metadata using raw XML, bypassing complex GUI inputs.

05 Handle changes without downtime. If an existing connection needs tweaking, use `update_connection` instead of rebuilding the whole thing.

Real-World Applications

Onboarding a New Client Product

A DevOps engineer needs to integrate a new SaaS offering for a client. Instead of logging into multiple consoles, they prompt their agent: 'Create an Okta SCIM directory for tenant X and product Y.' The MCP uses `create_directory` to automate the entire provisioning foundation.

Compliance Audit of Credentials

A Security Engineer needs to prove which products are using SAML. They prompt: 'List all SSO connections for tenant Acme Corp.' The agent runs `get_connections` and returns a structured list, immediately flagging any non-compliant or unmanaged credentials.

User Access Review

A Product Manager needs to know who is currently active in the system. They ask the agent to 'List all users for the main directory.' The MCP runs `get_directory_users` and provides a real-time list, solving the question of user access immediately.

Emergency Cleanup

The team discovers several old product tenants that were decommissioned months ago. Rather than manually finding them, they ask the agent to 'Delete all connections for product Z.' The MCP uses `delete_connection` instantly.

Patterns to Avoid

Dashboard Clicking Fatigue

✗ AVOID

Having to open 15 separate browser tabs, navigate to the 'Connections' section of each one, and copy/paste IDs just to get a full inventory list.

✓ INSTEAD

Ask your agent to run `get_connections` with specific filters (tenant ID or product ID). The MCP aggregates the necessary metadata and presents it in a single, consumable output.

Manual Provisioning Delays

✗ AVOID

A new client comes on board. The team spends hours setting up SCIM directories and manually verifying user sync permissions across different apps.

✓ INSTEAD

Use the `create_directory` tool to automate the setup of the entire directory structure. This process is repeatable, instant, and auditable via the MCP.

The Right Fit

You should use this MCP if your team's pain point is managing complex, multi-tenant authentication credentials or automating user lifecycle processes. Specifically, if you need to audit connectivity across many products using `get_connections`, or if you are integrating a new directory service and require automated provisioning via `create_directory`. Don't use it if you only need simple API calls (like reading a single database record). For that, a direct data read MCP is better. This tool focuses on the high-level state management of enterprise identity.

BoxyHQ and SAML/OIDC Connection Management via AI Agents

Managing SSO connections today is a headache of tabs, copy-pasting metadata URLs, and navigating complex security dashboards. When an employee leaves or a product changes its identity provider,

With this MCP, your agent handles the heavy lifting. You can simply ask it to 'Add a new SAML connection' using just a metadata URL. It manages the complex protocol handshake behind the

manually updating every single connection across multiple tenants is time-consuming and prone to human error.

scenes, giving you immediate confirmation that the connection was established correctly.

BoxyHQ and SCIM Directory Synchronization Automation with AI Agents

The manual process for onboarding a new customer often involves setting up a directory sync, then verifying user creation rules, then manually confirming that the connection is active. This cycle takes hours of hands-on work from an SRE.

Now, you ask your agent to 'Create a Directory Sync (SCIM) connection.' It executes the entire provisioning setup in seconds and provides the necessary base URL for the customer to start syncing users immediately.

BoxyHQ (Enterprise SSO) MCP: 8 Tools for Directory Synchronization

Use these tools to manage connections, list users, set up SCIM directories, audit credentials, and maintain the health of your enterprise identity systems.

#	TOOL	DESCRIPTION
01	`add_connection`	Programmatically adds a new Single Sign-On (SSO) connection, either SAML or OIDC.
02	`create_directory`	Sets up and configures a Directory Sync (SCIM) connection for user provisioning.
03	`delete_connection`	Removes an existing, outdated SSO connection from the system.
04	`get_connections`	Retrieves a list of all active Single Sign-On connections for a given product or tenant.
05	`get_directory_groups`	Lists every group belonging to a specific user directory within a client's tenancy.
06	`get_directory_users`	Retrieves a list of all active users associated with a given SCIM directory.
07	`health_check`	Performs an immediate check on the overall operational health and status of BoxyHQ services.
08	`update_connection`	Modifies settings for an already established SSO connection, like changing credentials or metadata.

See It in Action

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

U I need to check which products are using SAML authentication right now.

SSO Connection Report

We found 4 active connections:

- `Globex Corp` : Protocol (SAML), Last Updated (2024-11-01)
- `Internal Portal` : Protocol (SAML), Last Updated (2023-05-20)
- `Acme SaaS` : Protocol (OIDC), Last Updated (2024-06-15)
- `Client X` : Protocol (Unknown), Status (**Needs Review**)

I recommend reviewing the Client X connection details immediately.

U Can you set up a new user directory for my client, 'TechCorp'? I need it to sync users right away.

Directory Sync Status

The SCIM 2.0 directory for TechCorp has been created successfully.

- **Base URL:** `https://sso.boxyhq.com/api/scim/v2.0/techcorp`
- **Status:** Active
- **Next Step:** Provide this URL to the client's IdP team for immediate user synchronization.

Please let me know if you need a different tenant ID.

U What are all the active connections in the 'enterprise-portal' product?

Connections Found for enterprise-portal

You have 3 connected services:

CLIENT NAME	PROTOCOL	STATUS	ACTION
Globex Corp	SAML	Active	Inspect Details
Initech	OIDC	Active	Update Credentials
Umbrella	SAML	Deprecated	Delete Connection

Which connection would you like to inspect or delete?

Frequently Asked Questions

01 **How do I use the BoxyHQ MCP for AI Agents to audit my SSO setup?**

You ask your agent to list all connections, specifying the tenant or product ID. It will retrieve detailed metadata, letting you see which credentials are active, when they were last updated, and if anything is stale. This gives you a full security picture without manual clicks.

02 **Can I use BoxyHQ MCP for AI Agents to add new SSO connections?**

Yes, your agent can establish new SAML or OIDC links by accepting connection details like metadata URLs. It handles the technical setup and confirms the link is active, saving you from manual configuration.

03 **What if I need to automate user creation for a new client? Does BoxyHQ MCP support that?**

Absolutely. You use the MCP to create an SCIM directory connection. This sets up the foundational link, allowing you and your team to automatically provision users into the application from your central identity source.

04 **Is BoxyHQ MCP for AI Agents better than just using a GUI?**

It's faster and more reliable. Instead of navigating through multiple dashboards, you describe the action in plain English, and the agent executes the correct tool call instantly. You get structured data right back in your chat window.

05 **Can I delete old or unused connections using BoxyHQ MCP for AI Agents?**

Yes, you can safely decommission credentials. By having the agent run a deletion command on an outdated connection, you maintain a clean and compliant security posture instantly.

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 `"boxyhq-enterprise-sso": { "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

BoxyHQ (Enterprise SSO) 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 BoxyHQ (Enterprise SSO). 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	BoxyHQ (Enterprise SSO) MCP
Server ID	`019e386f-c220-732d-b0c9-db6a7568ec0c`
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/boxyhq-enterprise-sso.