MCP SERVER | NO CODE | CLOUD HOSTED

Superblocks MCP

Manage Your Internal Apps and Workflows Via Conversation

Superblocks MCP connects your AI agent directly to your low-code platform infrastructure. It lets you manage internal applications, monitor automated workflows, and handle full application lifecycle tasks—all using natural language commands. Need to audit configurations or generate secure session tokens for embedded apps? This MCP gives your agent the necessary tools to interact with every part of your Superblocks ecosystem without needing UI clicks.

A+ Quality Score 100/100

internal-tools | low-code | workflow-automation | api-integration | app-management | scheduled-jobs

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

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.

Superblocks MCP

7 tools available
Cloud-hosted on Vinkius

You can use this MCP connection to control your entire low-code environment through simple conversation. Instead of jumping between dashboards, you tell your AI client what you need done—whether it's listing all available applications or figuring out which workflows are failing.

It gives your agent the power to perform critical infrastructure tasks like creating a brand new internal application, updating an existing one, or deleting obsolete resources entirely. You can also pull up a full list of every active workflow running in the background so you know exactly what kind of automated logic is firing off across the company.

If you have end-users that need to access specific Superblocks tools, your agent can generate secure session tokens right on the fly, making SSO integration much simpler. When you subscribe through Vinkius, you give any MCP-compatible client instant access to this full suite of controls, letting you treat platform management like a natural conversation with an expert developer.

Core Capabilities

01 — Audit and list apps

Your agent can quickly list every application in your organization or fetch detailed configurations for one specific app.

02 — Manage the full app lifecycle

You can programmatically create, update, or delete entire Superblocks applications using simple commands.

03 — Monitor automated workflows

The agent retrieves a comprehensive list of all active background processes and scheduled jobs running across your platform.

04 — Generate secure access tokens

You can request authenticated session tokens for embedded applications, enabling single sign-on (SSO) for end-users.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP on Vinkius and provide your Superblocks API Key.

02 Next, prompt any AI client with a natural language request (e.g., 'List all apps that need updating').

03 The agent executes the necessary function call, retrieves the data payload, and presents the result back to you in conversation.

The bottom line is you manage complex internal tools using only chat commands, without ever leaving your preferred AI environment.

Built For

This MCP is for platform engineers and DevOps teams who are tired of manually checking multiple dashboards to see if their low-code applications and automated workflows are running correctly. It's essential for anyone managing internal tooling infrastructure at scale.

Platform Engineer

Uses the MCP to audit application settings, check resource lifecycles, and programmatically update configuration files.

DevOps Team Lead

Monitors active workflows and automates the deployment or full teardown of Superblocks applications.

Product Manager (Internal)

Lists available internal tools for stakeholder reviews and generates secure embed tokens for client integration testing.

What Changes When You Connect

01 Control the full app lifecycle: You can create, update, or delete applications directly through your agent. No more needing to navigate complex admin UIs just to make a quick config change.

02 Streamline SSO setup: Need temporary access for an auditor? Use the `create_embed_token` tool to instantly generate secure session tokens without touching any manual user management screens.

03 Deep visibility into operations: The agent can list all active workflows (`list_workflows`), letting you monitor scheduled jobs and backend logic without guessing which services are running.

04 Audit apps easily: Use `list_applications` or `get_application` to quickly audit configurations. You get the exact JSON payload, making it easy for engineers to validate settings.

05 Faster onboarding: Product teams can list available internal tools instantly via your agent, giving them a real-time inventory without needing developer help.

Real-World Applications

The forgotten app

A Platform Engineer suspects an old dashboard is leaking data. They ask their agent to list all applications and find the ID. Then, they use `get_application` to pull the full configuration payload and confirm it needs deletion via `delete_application`.

Client review access

A Product Manager needs a stakeholder to test an embedded dashboard in staging. They ask their agent, which uses `create_embed_token`, generating the necessary session token right in the chat for immediate testing.

Workflow debugging

The Ops team notices payments aren't processing overnight. They prompt their agent to list all workflows (`list_workflows`), identify the payment job, and check its last run status immediately.

Launching a new feature module

A developer is ready to build an internal tool but needs boilerplate setup. They use `create_application` via their agent, instantly spinning up the necessary Superblocks shell and configuration structure.

Patterns to Avoid

Treating it like a simple CRUD list

✗ AVOID

Thinking that just running 'list apps' is enough. You get names, but you don't know the current status or if they are configured correctly.

✓ INSTEAD

Always follow up listing with `get_application` for the specific ID you care about. This pulls the full configuration context, letting you audit the actual settings.

Manual token generation

✗ AVOID

Having to go into a separate user management portal and manually generate an SSO link just to let someone view a dashboard.

✓ INSTEAD

Use `create_embed_token`. This tool handles the secure, authenticated session token generation directly through your agent.

Assuming app existence

✗ AVOID

Telling the agent 'Update the Marketing Dashboard' without knowing its ID. The call will fail because it can't find the resource.

✓ INSTEAD

First, use `list_applications` to get a list of IDs and confirm the exact name/ID. Then, pass that verified ID to `update_application`.

The Right Fit

Use this MCP if your job requires managing the entire infrastructure layer of Superblocks—that means you need to audit configurations (`get_application`), control the app lifecycle (create/delete), or monitor background jobs (`list_workflows`). This is for platform engineers and DevOps teams who treat their internal tools like code. Don't use this if all you need to do is read a single piece of public data, or if your requirement is only simple messaging; in those cases, a generic chat tool will suffice. However, if the task involves *making* changes—like setting up SSO via `create_embed_token` or fixing an app's settings using `update_application` —this MCP is non-negotiable.

Debugging internal tools means context switching and copy-pasting IDs all day.

Right now, finding out why a dashboard isn't working or if an old app needs to be decommissioned is a pain. You have to jump from the main Superblocks dashboard to the settings panel, then maybe open another tab for the workflow monitor. Every time you need to check an ID or copy a configuration payload, you lose momentum and waste time.

With this MCP, that entire manual process evaporates. You simply tell your agent what's wrong—'Check the status of the inventory app.' Your agent handles the deep dive, gathering all necessary details from Superblocks' backend and giving you one clean answer in chat.

Superblocks MCP Gives You Full App Control

Manual management requires running separate commands for every action: first, listing all applications to find the right ID; second, manually calling a different API endpoint just to get the configuration details; and finally, using another UI screen to trigger token generation.

Now, you use your agent once. You ask it to generate an embed token for a specific user role, and in return, you get the secure, working token immediately. It's all one conversation.

Superblocks MCP: 7 Tools for App Management

Use these tools to interact with every core function of your Superblocks instance—from listing available applications to generating secure user tokens.

#	TOOL	DESCRIPTION
01	`create_application`	This tool builds a brand new Superblocks application within your organization.
02	`create_embed_token`	It generates an authenticated session token for users embedding the Superblocks applications using SSO.
03	`delete_application`	The tool permanently removes a specific Superblocks application from your setup.
04	`get_application`	It pulls detailed configuration information for one app, using its unique identifier.
05	`list_applications`	This tool retrieves a paginated list of every application currently running in the organization.
06	`list_workflows`	It lists all active background workflows and scheduled jobs associated with your account.
07	`update_application`	You can use this tool to change the configuration details of an existing Superblocks application.

See It in Action

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

U List the first 10 applications in our Superblocks organization.

I've retrieved the first 10 applications. You have tools like 'Customer Support Dashboard' (ID: app_123) and 'Inventory Manager' (ID: app_456) active. Would you like details on any specific one?

U Show me the configuration for application ID app_789.

Fetching details for app_789... This is the 'Sales Analytics' app. It currently has 3 pages and connects to your Snowflake and Salesforce instances. Would you like to see the full JSON payload?

U Generate an embed token for user 'dev@example.com' for our embedded portal.

I've generated a secure session token for dev@example.com. You can now use this token to authenticate their session in your embedded Superblocks components.

Frequently Asked Questions

01 **How do I list applications using Superblocks MCP?**

You use the `list_applications` tool. This pulls a paginated inventory of every app in your organization, giving you an immediate overview without needing to navigate the UI.

02 **Can I update configurations with Superblocks MCP?**

Yes, you can use the `update_application` tool. Just provide the application ID and the new configuration data, and your agent handles making those changes programmatically.

03 **Does Superblocks MCP handle workflow monitoring?**

Absolutely. The `list_workflows` tool lets you retrieve a full list of all active background jobs so you can monitor scheduled tasks across your platform.

04 **How do I generate an embed token using Superblocks MCP?**

Use the `create_embed_token` tool. You pass the necessary user details, and the agent returns a secure session token ready for embedding in external systems.

05 **What if I want to delete an old app with Superblocks MCP?**

Use the `delete_application` tool. The agent executes the removal process on your behalf, allowing you to clean up obsolete resources from your chat interface.

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 `"superblocks": { "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

Superblocks 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 Superblocks. 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	Superblocks MCP
Server ID	`019e38f5-e79b-7137-b5f3-a483dee898cb`
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/superblocks.