

MCP SERVER

NO CODE

CLOUD HOSTED

Activepieces MCP for AI Agents

Automate complex business processes and manage integrations.

Activepieces lets your AI agent manage, monitor, and build complex automation workflows directly from natural language. You can programmatically create new flows, adjust existing connections, and track detailed execution results—all without needing a dedicated UI or jumping between tabs.

A+ Quality Score 98.33/100

workflow-automation

no-code

business-process

integration-platform

task-automation

self-hosted



The infrastructure that powers AI agents in the real world.



Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest
managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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 — 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.

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.

Activepieces MCP

32 tools available

Cloud-hosted on Vinkius

You're already using AI agents for writing code or summarizing documents. Activepieces lets you use them to build and maintain automated business processes too. Instead of manually logging into the platform to check if your lead-generation flow broke, you simply ask your agent to check its status. It can list all active workflows, pinpoint exactly which connection failed, and even apply a structural change like moving an entire automation block.

It takes complex, multi-step business logic—like 'When X happens in Slack, update the record in Google Sheets, then notify the team'—and lets your agent orchestrate it. All of this power is accessible through Vinkius, letting you connect Activepieces to any MCP-compatible client so you never have to switch context just to manage a routine process.

Core Capabilities

01 — Get Flow Details

Retrieves the complete blueprint and configuration details of a specific automation workflow by ID.

02 — List Projects

Displays an overview list of every distinct project you have created on the platform.

03 — List Users

Lists every user account that has access to the Activepieces platform.

One Click on Vinkius — From Prompt to Execution

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

- 01 First, subscribe to this MCP and provide your unique Activepieces API Key.
- 02 Next, connect that credential through Vinkius to any compatible AI client (Cursor, Claude, etc.).
- 03 Finally, tell your agent what you want done—like 'List all automation flows in the Marketing project'—and it handles the rest.

The bottom line is Activepieces turns manual dashboard management into a conversational command for your AI agent.

Built For

This MCP is built for Ops Engineers and Product Managers who are tired of manually checking execution logs or toggling flow switches. If you manage dozens of critical, multi-app automations that need constant oversight, this tool saves time by giving your agent direct control.

DevOps Engineer

Monitors flow health across multiple projects and triggers updates or status changes directly from the terminal.

Product Operations Manager

Verifies data consistency by listing records, managing app connections, and ensuring automated workflows are pointing to the correct sources.

Automation Specialist

Creates new automation flows, manages project structures (folders/projects), and handles user permissions like inviting team members into the platform.

What Changes When You Connect

- 01 Full control over workflow definitions: You don't need a GUI. Use `create_flow` or `get_flow` to generate, read, and modify entire automation blueprints via conversational commands.

-
- 02** Instant debugging capability: If something goes wrong, your agent doesn't just say 'failed.' It uses `list_flow_runs` and `get_flow_run` to pull detailed step-by-step logs so you know exactly where the process broke.
-
- 03** Centralized connection management: Stop hunting for API keys. Manage all external services—from Slack credentials to Google Sheets links—in one place using `upsert_app_connection`.
-
- 04** Project and user governance: Easily manage who can do what by listing or removing users (`list_users` , `delete_project_member`) and organizing work with tools like `create_folder`.
-
- 05** Immediate structural changes: Need to pause a flow or change its status? Use `apply_flow_operation` to make those high-level adjustments instantly, without manual clicks.
-

Real-World Applications

The Marketing Lead Follow-up Failure

A marketing specialist notices that leads coming from Discord aren't triggering the correct follow-up sequence. Instead of checking the flow status page, they ask their agent to ``list_flows`` and then use ``get_flow`` on the lead router process. The agent reports that a specific conditional step is misconfigured, allowing them to immediately fix it using ``apply_flow_operation``.

Debugging Critical Data Syncing

A DevOps engineer finds that a critical sales lead record isn't updating correctly. They ask their agent to check the runs for the relevant flow ID. The agent uses ``list_flow_runs`` and then ``get_flow_run``, showing failure in step 3 because the source data table needed an update, which they fix by manually using ``update_record``.

Onboarding a New App Integration

The Product Ops team needs to connect a brand-new CRM platform. They ask their agent to manage the credentials. The agent uses ``upsert_app_connection``, handles all the authentication types (OAuth2, etc.), and confirms the connection is live for use in upcoming workflows.

Restructuring Automation Projects

The Product Manager needs to overhaul how their marketing automations are organized. They ask the agent to create a new folder structure and delete old ones. The agent uses ``create_folder``, ``delete_folder``, and confirms all related flows have been correctly moved or archived.

Patterns to Avoid

Trying to troubleshoot using only the UI

X AVOID

Manually clicking through flow run logs, switching between tabs to see connection status, and copying IDs into a separate spreadsheet.

✓ INSTEAD

Use your agent to ``list_flow_runs`` for an overview, then ask it to ``get_flow_run`` on the specific failed instance. If you need credentials fixed, use ``upsert_app_connection`` instead of navigating deep into settings.

Modifying flows without knowing dependencies

X AVOID

Manually editing a critical flow and accidentally breaking it because they didn't realize another project relied on that same connection or step.

✓ INSTEAD

First, ask your agent to ``list_flows`` to see what exists. Then use ``get_flow`` to review the whole blueprint before using ``apply_flow_operation`` or making any structural changes.

Forgetting organizational boundaries

X AVOID

Attempting to delete a folder while another project still has flows referencing its structure, causing an error.

✓ INSTEAD

Always check the directory first. Use `list_folders` and then ask your agent to manage the hierarchy by using `delete_folder`, ensuring no active flows depend on that path.

The Right Fit

Use this MCP if you need direct, programmatic control over the entire lifecycle of a business automation—from creation and connection management down to debugging individual runs. You should connect it when your team needs an AI agent to act as a dedicated Flow Operations Engineer.

Don't use it if your primary need is just viewing static data or generating simple reports; for that, a basic database connector will suffice. Also, don't rely on this MCP to build the actual business logic itself—it only gives you the tools to manage and execute flows built elsewhere. If you only need to view users without managing their connections, listing project members (`list_project_members`) is simpler than using the full capability set.

Activepieces MCP: Managing Workflow Automation in Business Processes

Today, managing cross-platform automations feels like juggling a dozen browser tabs. You have to check one dashboard for flow status, another for connection credentials (like Slack or Google Sheets), and yet another for error logs. Every time the process breaks—even if it's just a forgotten API key—you waste 15 minutes manually diagnosing which piece failed.

With this MCP, your AI agent handles that entire operational headache. You simply tell it to 'Check the status of the lead capture flow.' It instantly accesses all necessary details, listing runs and pinpointing failure points with `get_flow_run`. What you gain is immediate oversight, turning hours of manual monitoring into a single chat prompt.

Activepieces MCP: Governing Integrations Across Enterprise Workflows

The manual steps that disappear are the credential hunts and the structural updates. Instead of going through complex menus to update a connection, you ask your agent to refresh it using `upsert_app_connection`. Similarly, instead of manually moving an entire segment of code, you use `apply_flow_operation` to reposition blocks instantly.

This MCP gives your team the power of a dedicated Ops Engineer built right into your chat interface. It means your automations run reliably and your team spends time on strategy, not debugging.

32 Activepieces Tools for Business Process Orchestration

These tools give your agent granular control over every aspect of your automation platform, from creating new flows to managing user accounts and connections.

#	TOOL	DESCRIPTION
01	<code>add_piece</code>	Adds a specific custom component or action block to an automation flow.
02	<code>delete_app_connection</code>	Removes a credential connection for a single external service like Slack or Google Sheets.
03	<code>delete_flow</code>	Completely removes an automation flow from the platform using its unique ID.
04	<code>list_flow_runs</code>	Retrieves a list of recent executions for multiple workflows to quickly gauge overall system health.
05	<code>update_folder</code>	Changes the name or structure of an existing folder in your automation workspace.
06	<code>apply_flow_operation</code>	Applies structural changes to a flow, such as changing its status or moving it within the project hierarchy.
07	<code>configure_git_repo</code>	Sets up automatic synchronization between your Activepieces projects and an external Git repository.
08	<code>create_flow</code>	Generates a brand new, blank automation workflow ready for building out steps.
09	<code>create_folder</code>	Adds a new organizational folder to keep your project structures clean and segmented.
10	<code>upsert_app_connection</code>	Creates or modifies an external service connection, supporting various authentication types like OAuth2 or Basic Auth.
11	<code>upsert_global_connection</code>	Creates or updates a company-wide connection that can be used across multiple projects.
12	<code>create_project_release</code>	Marks and creates a specific version release point for a project's automation status.
13	<code>create_project</code>	Establishes an entirely new, dedicated workspace or project container.

#	TOOL	DESCRIPTION
14	<code>delete_folder</code>	Deletes an empty or unused folder structure from your automation environment.
15	<code>delete_global_connection</code>	Permanently removes a company-wide global connection, revoking access across all projects.
16	<code>delete_project_member</code>	Removes another team member's account from the current project scope.
17	<code>get_flow_run</code>	Pulls all the detailed execution data for a single, specific flow run instance.
18	<code>get_flow</code>	Retrieves the complete blueprint and configuration details of a specific automation workflow by ID.
19	<code>get_mcp_server</code>	Fetches the current MCP server configuration for use in your AI client setup.
20	<code>invite_user</code>	Sends an invitation to a specific user's email address to join the platform or project.
21	<code>list_app_connections</code>	Provides a list of all external service connections currently set up within your active projects.
22	<code>list_flows</code>	Lists every available automation workflow defined within the current project scope.
23	<code>list_folders</code>	Retrieves a directory of all organizational folders that structure your projects.
24	<code>list_global_connections</code>	Lists all the global connections available across every project in your organization.
25	<code>list_project_members</code>	Shows who is currently a member of the active project and what their roles are.
26	<code>list_projects</code>	Displays an overview list of every distinct project you have created on the platform.
27	<code>list_records</code>	Pulls a dataset of entries from a specified internal data table for review.
28	<code>list_tables</code>	Shows all the available, named internal data tables within your workspace environment.
29	<code>list_users</code>	Lists every user account that has access to the Activepieces platform.
30	<code>rotate_mcp_token</code>	Generates a new, refreshed security token for the project's MCP connection.

#	TOOL	DESCRIPTION
31	update_project	Modifies general settings or parameters for an existing automation project.
32	update_record	Changes specific data points within a single record in one of your internal tables.

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 if my main customer support flow is running correctly after the API change.



Flow Run Status Report

- **Project:** Customer Support Intake
- **Latest Run ID:** `run_abc123` (Succeeded)
- **Previous Run ID:** `run_xyz789` (Failed: Timeout Error)

Failure Details:

The last run failed at the 'Data Validation' step. The error indicates an expired credential for the external database connection. Please review and update the credentials using the proper management tools to resolve this.

U Can you list all my active projects and see who is on them?



I found 3 distinct automation projects:

- **Project: Sales Intake:** Members include Alice (Admin), Bob (Editor).
- **Project: HR Onboarding:** Members include Carol (Viewer), David (Admin).
- **Project: Marketing Sync:** Only you are currently listed as a member.

You can invite new users or remove existing ones via the management tools.

U Create a new flow to handle incoming support emails and name it 'Email Triage'.



Success. I've created a blank automation workflow named 'Email Triage.' The ID is `flow_new_101`. You can now begin adding steps, like integrating the email source or defining the routing logic. Do you want me to list all available folder IDs so you know where to put it?

Frequently Asked Questions

01 How does Activepieces MCP help manage complex integrations without logging in?

It lets your agent act like a dedicated operations specialist. You can list and update external credentials, or even create new connections using ``upsert_app_connection``, all through chat commands instead of the web UI.

02 Can I use Activepieces MCP to debug why my automation workflow failed?

Absolutely. If a flow breaks, you don't have to guess. Your agent can list recent runs and pull detailed logs using ``get_flow_run``, showing exactly which step threw the error and why.

03 What if I need to change how my automation works? Can I modify it?

Yes, you can programmatically adjust workflows. You can get a flow's current structure using ``get_flow``, and then use tools like ``apply_flow_operation`` to move blocks or change status without touching the platform interface.

04 Is Activepieces MCP only for single projects, or can it manage multiple ones?

It manages your entire workspace. You can list all available projects and monitor flows across different business units, ensuring consistency everywhere you need it.

05 How do I organize my automation flows using Activepieces MCP?







You control the structure by managing folders. Your agent lets you create new folders (``create_folder``), list existing ones, and delete empty organizational containers to keep everything tidy.

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>"activepieces": { "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

Activepieces 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](https://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 Activepieces. 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	Activepieces MCP
Server ID	019e3860-7a7d-71ef-b884-e518f1a812d3
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/activepieces.