MCP SERVER | NO CODE | CLOUD HOSTED

Apideck MCP for AI Agents

Unified CRM and SaaS Data Orchestration

Apideck lets your AI agent talk to dozens of SaaS platforms—all from one place. It manages CRM contacts, handles user account connections in a secure 'Vault,' and runs proxy requests across services like Salesforce, HubSpot, and more. Stop writing custom code for every platform; connect everything through this single unified API.

A+ Quality Score 100/100

unified-api | crm-integration | vault | api-proxy | saas-orchestration

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

SCAN TO VIEW

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.

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.

Apideck MCP

6 tools available
Cloud-hosted on Vinkius

Apideck lets you build agents that interact with your entire software stack without needing to write boilerplate code for each service. Instead of connecting separately to dozens of CRMs or integrating accounts one by one, Apideck acts as a universal translator. Your AI agent uses the platform's unified APIs to read contacts from different sources and manage user connections in a secure Vault environment.

This means your agent can check if a customer's integration is healthy, list all connected services, or pull contact lists from Salesforce just as easily as it pulls them from Pipedrive. It drastically cuts down on the time spent writing platform-specific API calls. Because Vinkius hosts this MCP, you connect your preferred AI client once and immediately gain access to these powerful orchestration tools.

It's about unifying the data layer so your agent can work across boundaries, giving you one consistent way to manage user identity and CRM information.

Core Capabilities

01 — Retrieve contacts from multiple CRMs

The MCP pulls contact lists and filters them across various connected CRM providers.

02 — Manage user account links in the Vault

You can initiate new user sessions, list existing connections, or delete specific service integrations.

03 — Audit connection health

The system checks and reports on the status of any active integration to ensure data flow is working.

04 — Run custom API requests

When a specific function isn't covered by the standard tools, you can execute direct proxy calls to other endpoints.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your unique Apideck API Key, App ID, and Consumer ID credentials.

02 Your AI agent connects to the unified endpoint provided by the MCP.

03 The agent sends a request—for example, 'List all contacts from HubSpot'—and receives structured data back.

The bottom line is that you treat your entire SaaS ecosystem like one big database through Apideck's standardized API layer.

Built For

This MCP solves the headache of siloed data. It’s built for developers, product managers, and support engineers who spend too much time manually hopping between dashboards or writing repetitive integration code across multiple enterprise platforms.

Developer

Uses the MCP directly from their IDE to write agent logic that communicates with several APIs (like Salesforce and HubSpot) without needing separate authentication layers for each.

Product Manager

Needs a single point of view to audit user connections or check CRM data consistency across different business units or environments.

Support Engineer

Answers complex customer questions by verifying the status and configuration details of a client’s integration in the Vault using natural language prompts.

What Changes When You Connect

01 Stop writing custom code. Instead of building unique connection logic for every single service, Apideck lets your agent access all platforms through one standardized API.

02 Audit user connections instantly. Use `list_vault_connections` to see the status of every integrated platform and verify if data flow is healthy without manually checking dashboards.

03 Centralized contact management. You can pull contacts from multiple sources, like Salesforce or HubSpot, using `list_crm_contacts` in a single request for context building.

04 Maintain system integrity with confidence. The ability to use `get_vault_connection` lets your agent verify specific user setup details before taking action, reducing operational risk.

05 Flexible fallback. Need a function that doesn't have a dedicated tool? You can always execute it using the `execute_proxy` function.

Real-World Applications

Auditing CRM data for compliance

A product manager needs to confirm if every user who signed up last month has been correctly linked across Salesforce and Pipedrive. They ask the agent, which uses `list_crm_contacts` combined with `list_vault_connections` to generate a comprehensive report showing both data presence and connection status.

Onboarding new enterprise clients

A support engineer needs to get a client started. They ask the agent to use `create_vault_session`, generate the required redirect URL, and guide the user through linking their accounts securely in the Vault.

Cross-platform data migration

A developer needs to pull a list of key contacts from multiple systems before migrating them. They prompt the agent to use `list_crm_contacts` across all connected providers, consolidating the data set for transfer.

Fixing broken integrations

A team member notices a client is having issues. Instead of guessing, they ask the agent to run `get_vault_connection` on that specific service link to immediately report if the connection token or status is expired.

Patterns to Avoid

Writing code for every API endpoint

✗ AVOID

Attempting to write bespoke Python code to handle authentication and data retrieval for Salesforce, then rewriting it again for HubSpot. This creates massive maintenance overhead.

✓ INSTEAD

Use the unified `list_crm_contacts` tool. It handles the multi-provider complexity under a single function call, letting your agent abstract away the underlying platform differences.

Ignoring connection status

✗ AVOID

Assuming data is available simply because a user signed up. The agent might fail later when it attempts to read data from an unlinked service.

✓ INSTEAD

Always run `list_vault_connections` first. This confirms that the necessary integrations are active and healthy before your agent tries to retrieve any sensitive contact or account data.

Using raw API calls for general tasks

✗ AVOID

Trying to list contacts by calling a generic `execute_proxy` endpoint instead of using the dedicated, structured `list_crm_contacts` tool. This is harder to debug and less reliable.

✓ INSTEAD

Use the purpose-built tools first. If those fail or are incomplete, then use `execute_proxy` as a last resort for highly specific, undocumented needs.

The Right Fit

You need this MCP if your team's workflow requires data coordination across more than two distinct SaaS platforms, especially when dealing with user identity and CRM records. If you frequently ask agents to 'check the contact list from both HubSpot AND Salesforce,' this is for you.

Don't use it if all of your required functionality comes from a single, isolated service (e.g., only using Pipedrive). In that case, connecting directly might be simpler. But if your goal is cross-platform orchestration and robust auditing, Apideck's unified APIs are essential.

Apideck MCP for AI Agents: Solving CRM Data Silos

Right now, pulling a complete picture of an account means jumping through hoops. You have to log into Salesforce, copy the list; then jump to HubSpot and repeat it. If you need to check Pipedrive as well, that's three separate logins and at least fifteen minutes of tedious copy-pasting just to get a single source of truth.

With this MCP, your agent handles all that complexity behind the scenes. You ask for 'all contacts in the US,' and it uses `list_crm_contacts` to pull and normalize those leads from every connected CRM into one clean data set. The result is immediate context for your AI workflow.

Apideck MCP for AI Agents: Managing SaaS Connection Auditing

Checking user permissions or connection health used to be a nightmare of manual checks. A support person would have to check the dashboard, look for expiration dates, and confirm if all necessary integrations were linked up—a process that was slow, error-prone, and impossible at scale.

Now, your agent handles it. You just ask about the 'Vault connections,' and it runs `list_vault_connections` or checks a specific link with `get_vault_connection`. It instantly tells you if an integration is healthy, expired, or needs attention.

Apideck: 6 Tools for Multi-SaaS CRM Orchestration

These tools let you manage everything from listing contacts to auditing specific user integrations using a single, unified API endpoint.

#	TOOL	DESCRIPTION
01	`list_crm_contacts`	Retrieves and filters contact lists from all connected CRM providers using one unified call.
02	`delete_vault_connection`	Removes a specific, pre-existing connection link within the secure Vault environment.
03	`get_vault_connection`	Checks and retrieves detailed status information for one particular service integration in the Vault.
04	`execute_proxy`	Sends a direct API request to an arbitrary external endpoint when standard tools don't cover the needed functionality.
05	`list_vault_connections`	Generates a comprehensive list of every active and inactive integration connected through the Vault.
06	`create_vault_session`	Initiates a new, secure session link in the Vault so users can connect their own accounts.

See It in Action

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

U Can you pull all leads who interacted last week but aren't fully set up in the Vault?

📊 CRM Lead Status Report

I pulled data from your connected CRMs and cross-referenced it with current Vault connections. Here are 5 leads needing attention:

CONTACT NAME	SOURCE CRM	LAST ACTIVITY DATE	CONNECTION STATUS
Jane Doe	HubSpot	2024-06-10	Needs Linkage
Mark Smith	Salesforce	2024-06-15	Active (OK)
Alex Jones	Pipedrive	2024-06-08	Missing Vault Session

Next Steps: I recommend initiating a new session for Jane Doe and Alex Jones.

U What is the current status of our integrations across all connected platforms?

✅ Vault Connection Audit Summary

You have 7 active connections. All are reported as healthy, but here's a breakdown:

- **Salesforce:** Active (Last checked: 5 mins ago)
- **HubSpot:** Active (Data sync OK)
- **Slack:** Active (Permissions confirmed)
- **Jira:** Warning (Token expires in 3 days. Consider re-auth.)

Overall, the system is stable, but you should check the Jira credentials soon.

U I need a list of all contacts from both Salesforce and HubSpot who have never logged into the Vault.

Unlinked High-Value Contacts

Based on your criteria, I found 14 contacts. They are active in CRM but lack an established Vault session.

- Alice Smith (alice@example.com) - Last Seen: Salesforce
- Bob Jones (bob@example.com) - Last Seen: HubSpot
- ... (and 12 others)

You can use this list to target them with a manual onboarding email.

Frequently Asked Questions

01 **How does the Apideck MCP help me manage data across different CRMs?**

The Apideck MCP standardizes your connection layer, so you don't have to write custom code for every single CRM. It lets your agent pull contacts from Salesforce and HubSpot into one structured list using a unified API call.

02 **Is the Apideck MCP useful if I only use one type of software?**

No, it's designed for multi-platform orchestration. If you only use a single app, connecting directly is simpler. But if your workflow involves multiple services, this MCP provides the necessary glue.

03 **What does 'Vault connection' mean when I use Apideck MCP?**

The Vault is the secure place where you manage user identity and service links. It lets your agent check if a customer has correctly linked their accounts, which is key for data integrity.

04 **Can Apideck help me onboard new users automatically?**

Yes. The MCP provides tools to create secure Vault sessions and generate the necessary links. Your agent can guide a user through linking their own accounts using these tools.

05 **Does the Apideck MCP require writing any API code myself?**

No, you don't write the integration boilerplate. You just connect your AI client to the MCP, and then use natural language prompts to ask for data or actions.

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 `"apideck": { "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

Apideck 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 Apideck. 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	Apideck MCP
Server ID	`019e3865-e908-7319-82b2-6e97b370a642`
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/apideck.