MCP SERVER | NO CODE | CLOUD HOSTED

Middesk MCP

Verify any business's legal standing and tax compliance.

Middesk MCP connects your AI client to comprehensive Business Identity (KYB) and compliance verification. It lets you verify corporate entities, access Secretary of State documents, manage tax registrations, and auto-complete business details using real-time data.

A+ Quality Score 100/100

kyb | business-verification | identity-verification | compliance | corporate-records

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

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.

Middesk MCP

9 tools available
Cloud-hosted on Vinkius

This MCP gives your agent the ability to handle complex identity checks for businesses. You can start by asking it to populate core business data just from an EIN or a website address. Need to know if a company is properly registered? It retrieves official Secretary of State filings and documents, so you don't have to check multiple state websites. The system also lets you manage tax registrations and track payroll compliance across states. When the information is complex, linking up through Vinkius makes it easy; your agent gets access to all these tools in one place. You can monitor verification requests live or search for businesses using suggestions based on existing SOS records.

Core Capabilities

01 — Verify Business Entities

You send a request and get real-time status updates while creating and tracking new business verification jobs.

02 — Retrieve Corporate Filings

The MCP fetches official documents directly from the Secretary of State, like Articles of Incorporation.

03 — Auto-Populate Business Details

It takes a single identifier, like an EIN or URL, and automatically fills in core business information fields.

04 — Track State Tax Compliance

You can manage and track specific state tax registrations and overall payroll compliance status for multiple entities.

05 — Search Business Records

The system searches existing records, offering live suggestions for businesses based on Secretary of State data.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and enter your Middesk API Key into your client.

02 Ask your agent to perform an identity check or retrieve a specific document for the business you're investigating.

03 The MCP executes the lookup, pulls the data from official sources, and returns verified records directly to your workflow.

The bottom line is that you stop hopping between compliance tools and run all your KYC checks in one place.

Built For

Anyone who deals with corporate onboarding, due diligence, or financial compliance. If your job involves verifying a company's legal standing before making a deal, you need this.

Compliance Officer

Needs to run full Know Your Business (KYB) checks on new partners and track their state tax registrations for regulatory audits.

Legal Operations Specialist

Requires the ability to pull official corporate documents, like articles of incorporation, and validate entity existence quickly during M&A due diligence.

Financial Analyst

Often needs to verify a company's legal details or check its status against Secretary of State records before running financial models.

What Changes When You Connect

01 Instead of manually checking state websites for documents, this MCP lets your agent retrieve official Secretary of State filings instantly using the `get_document` tool. You get verified history in seconds.

02 When onboarding a client, you can use `prefill_business` to populate basic details from just one identifier. This saves hours of copy-pasting and initial data gathering.

03 Compliance checks are simpler. Use `list_tax_registrations` to see every state tax registration tied to an entity in one API call, instead of running multiple searches.

04 You can monitor the full lifecycle of a check. Start with `create_business`, which kicks off a request you then track until it's fully verified, providing clear status updates.

05 Need to find an unknown company? Use `autocomplete_identity` first. This provides live suggestions based on SOS data, guiding your investigation before you even know the full name.

Real-World Applications

Due diligence for a potential acquisition.

The M&A team needs to validate the target company's legal standing. They ask their agent to use `list_documents` and `get_document` on the primary business ID, instantly retrieving all articles of incorporation and annual reports needed for the pitchbook.

Onboarding a new vendor from another state.

The procurement officer needs to know if the vendor is compliant everywhere. They use `list_tax_registrations` to check all known states, ensuring tax compliance before signing any purchase order.

Investigating a suspicious business name online.

Instead of searching Google for conflicting addresses, the user asks their agent to use `autocomplete_identity`. The MCP provides live, accurate suggestions based on official Secretary of State records immediately.

Validating a client's primary corporate identity.

The sales team receives an EIN and needs basic facts. They ask the agent to run `prefill_business`, which quickly pulls verified legal names, addresses, and other core details, allowing the pitch to move forward immediately.

Patterns to Avoid

Treating it like a general search engine

✗ AVOID

Asking your agent: 'Tell me everything about Acme Corp.' This returns random links and requires you to sift through non-official data, wasting time.

✓ INSTEAD

Be specific. Tell the MCP exactly what you need, like: 'Use `get_document` to find the Articles of Incorporation for Acme Corp's ID.' Use specific tools for precise results.

Relying on partial information without context

✗ AVOID

Just sending a name and saying, 'Is this company real?' The system can't tell if it needs state, federal, or corporate records.

✓ INSTEAD

Start with `autocomplete_identity` to get the official ID first. Once you have that ID, use tools like `get_business` for comprehensive data.

Assuming all compliance data is in one place

✗ AVOID

Thinking a single search will show tax status for every state.

✓ INSTEAD

Use `list_tax_registrations` to gather *all* known registrations first. Then, use `get_tax_registration` on the specific numbers you need to confirm compliance.

The Right Fit

Use this MCP if your job requires verifiable proof of a company's legal status or tax standing. If due diligence involves checking corporate records, state filings, EIN validation, or multi-state tax IDs, this is your tool. Don't use it if you just need general business contact information—other directories are fine for that. Also, don't rely on it to find internal company documents; it only accesses public and official government records. If you simply need to draft an email based on a name, use a standard text generator instead.

Compliance checks shouldn't feel like detective work.

Today, verifying a company's identity is a mess. You start with the corporate website, which gives you a name. Then you have to open State A's Secretary of State portal and manually search for filings. If that doesn't work, you move to State B, then maybe the IRS site to check tax status. It's hours of clicking through different portals and copy-pasting IDs into forms just to establish basic legitimacy.

With this MCP, that entire sequence vanishes. You give your agent a simple prompt. The system handles the routing: it checks the corporate records, pulls necessary filings from multiple states, and compiles everything for you in one clean response. You get verified, actionable data instantly.

Middesk MCP Provides Verified Business Identity Data

You no longer have to copy-paste a name into three different state websites just to confirm incorporation status. The agent can use the `get_business` tool, which pulls verified data from multiple sources simultaneously.

The result is immediate confirmation of legitimacy and compliance across jurisdictions. You stop wasting time on redundant manual checks and start making decisions with certainty.

Middesk: 9 Tools for Compliance Data

These tools let your agent perform specific, verifiable actions like searching business lists or retrieving single corporate documents based on official identifiers.

#	TOOL	DESCRIPTION
01	`autocomplete_identity`	Suggests complete business identities based on partial information you provide.
02	`create_business`	Initiates a new, monitored request to verify an entire business entity using its legal name.
03	`get_business`	Retrieves all available public and official records for a specific, known company ID.
04	`get_document`	Fetches the content of one specific corporate filing or document by its unique identifier.
05	`get_tax_registration`	Retrieves all compliance details for a single state tax registration number.
06	`list_businesses`	Searches and returns lists of multiple businesses based on general criteria you specify.
07	`list_documents`	Returns a list of all available official documents associated with a specific business ID.
08	`list_tax_registrations`	Lists all state tax registrations linked to a particular corporate entity.
09	`prefill_business`	Quickly populates common business details when you provide an identifier, like a website or EIN.

See It in Action

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

U Verify the business 'Acme Corp' located in Delaware.

Initiating verification for Acme Corp... Submission ID #99882. I will monitor the status for you.

U Find SOS filings for business ID 'bus_123'.

Retrieving documents... Found 2 filings: Articles of Incorporation and Statement of Information.

Frequently Asked Questions

01 **Does the Middesk MCP verify private business information?**

No, this MCP only accesses official public records like those maintained by Secretary of State offices. It won't provide internal financial data or non-public employee info.

02 **How do I use the `autocomplete_identity` tool with Middesk MCP?**

To use it, just ask your agent to autocomplete an identity using a partial detail like a website. The tool returns live suggestions based on existing Secretary of State records.

03 **Can I check tax compliance for multiple states using the Middesk MCP?**

Yes. You can use `list_tax_registrations` to find all known state registrations, then confirm specific statuses with `get_tax_registration`.

04 **What if I don’t know the company ID for a business?**

You can start by using `prefill_business`. Providing an EIN or website will often allow the system to look up and confirm core details without needing the specific internal ID.

05 Is this MCP better than manually checking corporate records?

Yes. It automates the multi-step process of gathering data from multiple, disparate government sources into a single structured response.

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 `"middesk": { "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

Middesk 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 Middesk. 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	Middesk MCP
Server ID	`019d75d4-8478-731a-b654-e26c92daf8cd`
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/middesk.