MCP SERVER | NO CODE | CLOUD HOSTED

OFAC Sanctions Service MCP

Verify global sanctions lists and entity history

The OFAC Sanctions Service MCP connects your AI agent directly to the authoritative sanctions data published by OFAC. You can verify if individuals, groups, or entities appear on major lists like the SDN list, check historical versions of these records, and track when the underlying compliance data was last updated. It gives you deep, traceable insights into global financial risk.

A+ Quality Score 100/100

sanctions-screening | risk-management | regulatory-compliance | aml-checks | data-verification | watch-list

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/ofac-sanctions-service

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.

OFAC Sanctions Service MCP

10 tools available
Cloud-hosted on Vinkius

Need to know if a client or counterparty is sanctioned? This MCP lets your AI agent query the official OFAC Sanctions List Service (SLS) directly from within your workflow. Instead of downloading massive CSVs and manually cross-referencing data sheets, you ask your agent natural language questions about sanctions lists.

For example, you can list all available sanctions registries to know what data sets exist. You can also check the current status by calling `get_list_last_updated` to confirm that the information you're using is genuinely up-to-date. If compliance requires historical checks, the MCP allows deep diving into versions, letting you track both the full list metadata and only the specific changes (deltas) between versions.

This level of structured access makes manual audits faster. By connecting this service through Vinkius, your agent can handle complex data tasks—from getting total entity counts within a version to accessing detailed profiles for any specific sanctioned party. It turns what used to be a massive administrative chore into a simple conversational query.

Core Capabilities

01 — Verify Entity Status

Fetch detailed profile information on specific entities, including known aliases and addresses.

02 — Check List Currency

Determine the exact timestamp of when any sanctions list was last updated by OFAC.

03 — Audit List Scope

Retrieve a full catalog of all available sanctions lists, such as SDN or NONSDN.

04 — Track Data History

View the version history and metadata for any given sanctions list, including specific changes between versions.

05 — Count Records

Get an exact total count of entities contained within a specific version of a sanctions list for reporting purposes.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/ofac-sanctions-service** — connect your AI agent in three steps.

01 Subscribe to the OFAC Sanctions Service MCP and provide your API key, if required.

02 Connect this MCP to your preferred AI client (Claude, Cursor, etc.) in Vinkius.

03 Tell your agent exactly what you need—for instance, 'What are all the available sanctions lists?' or 'Check the entry count for version X'.

The bottom line is, you get real-time access to authoritative compliance data without ever leaving your chat window.

Built For

This MCP is built for professionals who deal with international financial risk and regulatory mandates. It's for the Compliance Officer needing instant verification, the Legal Team monitoring watchlist changes, or the Risk Analyst automating audit reports.

Compliance Officer

Quickly verifying entity details against multiple sanctions lists without manually downloading and comparing large government files.

Legal Counsel

Monitoring for new or historical additions to watchlists, specifically tracking changes in the SDN list version history.

Risk Analyst

Automating compliance reports by retrieving total entry counts and listing all available sanctions lists across different versions.

What Changes When You Connect

01 Stop wasting time manually checking if a list is current. Use `get_list_last_updated` to get the precise timestamp of the latest OFAC update, ensuring your compliance checks rely on fresh data.

02 Don't just check for existence; understand *why* an entity is flagged. With `get_entity_details`, you pull detailed profiles including aliases and addresses in one go.

03 Audit risk over time by listing all historical versions using `list_list_versions`. You can then track specific changes between two points in time with `get_delta_version_metadata`.

04 Need a quick count for reporting? Instead of manually counting lines, use `get_version_entry_count` to get the exact total number of entities contained within any list version.

05 Quickly understand your compliance scope by calling `list_sanctions_lists` to see every available registry, eliminating guesswork about which lists you need to check.

Real-World Applications

Screening a New Client Against Multiple Lists

A risk analyst needs to know if a client is flagged by OFAC. They ask their agent to call `list_sanctions_lists` first, then use the result to check for details using `get_entity_details`, providing a comprehensive and immediate risk report.

Preparing Quarterly Regulatory Reports

A compliance officer must prove that their checks are always based on current data. They use `get_list_last_updated` to document the exact time of the last official update for audit purposes, satisfying regulatory demands.

Investigating a Historical Sanction Change

A legal team needs to know exactly when an entity's status changed. They use `list_list_versions` and then `get_delta_version_metadata` to isolate the precise changes, rather than reviewing entire list versions.

Building a Data Validation Pipeline

A risk analyst needs to confirm that their dataset matches an official version. They use `list_version_entities` and then `get_version_entry_count` to validate the scope against the authoritative source.

Patterns to Avoid

Treating this like a simple database lookup

✗ AVOID

Assuming that just because an entity ID is known, its status hasn't changed since last month. Using general data retrieval tools for compliance checks.

✓ INSTEAD

You must use `get_list_last_updated` first to validate the list currency. Then, run `get_entity_details` to get current profile information. Never rely on stale data.

Over-relying on a single sanctions list

✗ AVOID

Checking only against the SDN list and assuming that covers all potential regulatory concerns for a multinational client.

✓ INSTEAD

Always start by calling `list_sanctions_lists` to get a complete view of available lists. This ensures you cross-reference the entity across every relevant registry.

Ignoring version control

✗ AVOID

Using only the latest list data without knowing if the source was updated today or last week, leading to compliance failure.

✓ INSTEAD

Always verify currency using `get_list_last_updated`. If history is needed, use `list_list_versions` before checking any status.

The Right Fit

Use this MCP if your core need involves validating an entity's existence or status against official, version-controlled government watchlists. You must be tracking *compliance* risk—is the data current? Did the status change recently? If you just need to search a private database of internal client names or look up general company contact info (non-sanction related), don't use this. Use your standard database lookup MCP instead. Only when regulatory accuracy and official list sourcing are paramount should you connect to OFAC via this service.

Dealing with Sanctions Data is a Paperwork Nightmare

Compliance teams spend hours downloading massive, multi-gigabyte data dumps from government sites. They then open spreadsheets, manually filter by client name or ID, and cross-reference the results against dozens of internal records just to answer one simple question: 'Is this person sanctioned?' It’s tedious, error-prone clicking through tabs until 2 AM.

With this MCP, you simply ask your agent. You prompt it to check an entity's status using `get_entity_details`. The system executes the complex API calls and hands you a clean, summarized answer showing exactly where they stand on official watchlists. It turns a multi-hour audit into seconds.

Accessing Sanctions List Data via OFAC Sanctions Service MCP

You eliminate the manual steps of visiting multiple government websites, downloading zip files, unzipping them, and running comparison scripts. The agent handles all that complexity for you.

Now, checking global financial risk is part of your conversation flow. You get auditable, authoritative answers immediately.

OFAC Sanctions Service: 10 Tools for Compliance

These tools allow you to programmatically interact with the OFAC Sanctions List Service. You can retrieve metadata, list entities, or check update statuses through precise API calls.

#	TOOL	DESCRIPTION
01	`get_sls_about`	Retrieves general information about the OFAC Sanctions List Service API.
02	`get_delta_version_metadata`	Gets metadata detailing only the changes (deltas) between two specific versions of a list.
03	`get_entity_details`	Accesses detailed profile information for any specific sanctioned entity ID.
04	`get_version_entry_count`	Returns the total number of entities present in a specified version of a sanctions list.
05	`get_full_version_metadata`	Retrieves complete metadata for an entire, specific version of a sanctions list.
06	`get_list_last_updated`	Checks the exact date and time that any given sanctions list was last updated by OFAC.
07	`list_version_entities`	Lists all entity identifiers contained within a specific version of a sanctions list.
08	`list_sanctions_lists`	Provides a catalog of all available sanctioned lists, such as SDN or NONSDN.
09	`list_version_tags`	Fetches descriptive tags and labels applied to a specific sanctions list version.
10	`list_list_versions`	Lists all available historical versions for any given sanctions list.

See It in Action

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

U When was the SDN sanctions list last updated?

Checking update status... The SDN sanctions list was last updated today at 10:15 AM UTC. Would you like to see the entry count for the latest version?

U Get the details for entity ID '12345' in the latest SDN version.

Inspecting entity 12345... This record belongs to 'Example Global Group'. It has 3 known aliases and is associated with 2 addresses in Zurich. Shall I retrieve the full version metadata for this list?

U List all historical versions available for the SDN list.

Retrieving version history... I found 12 historical versions for the SDN list, ranging from January 2023 to the current version published today. Would you like to check the delta (changes) between the last two versions?

Frequently Asked Questions

01 **How do I check if an entity is on any sanctions list using the OFAC Sanctions Service MCP?**

You use `list_sanctions_lists` to see all available lists, then provide a name or ID. The agent handles the full screening process across the appropriate registries.

02 **What is the difference between full and delta metadata using OFAC Sanctions Service MCP?**

Full version metadata (`get_full_version_metadata`) provides everything in a list for that date. Delta metadata (`get_delta_version_metadata`) only shows what changed since the previous official release, saving you time.

03 **Can I find out when the SDN sanctions list was last updated with OFAC Sanctions Service MCP?**

Yes, calling `get_list_last_updated` provides the exact date and time the specific sanctioned list was modified by OFAC.

04 **How do I list all historical versions using this MCP?**

Use the `list_list_versions` tool. This gives you a catalog of every archived version, allowing you to pick and choose which date range you need for your audit.

05 **Is the data from OFAC Sanctions Service MCP real-time?**

The data reflects the most current versions published by OFAC. Always confirm currency using `get_list_last_updated` to ensure you're working with the latest official release.

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 `"ofac-sanctions-service": { "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

OFAC Sanctions Service 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 OFAC Sanctions Service. 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	OFAC Sanctions Service MCP
Server ID	`019d75e3-3edf-7282-8b84-60a6ff19a6ea`
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/ofac-sanctions-service.