MCP SERVER | NO CODE | CLOUD HOSTED

Onfido MCP

Automate KYC, check IDs, and onboard users instantly.

Onfido connects your AI agent to identity verification services, automating KYC and compliance checks. You can create new applicant profiles, trigger complex multi-step verification workflows, run specific document comparisons, and pull detailed reports—all through natural conversation. This MCP lets you manage the entire user onboarding process without leaving your chat interface.

F Quality Score 3.6/100

identity-verification | kyc | applicant-screening | compliance | document-verification | biometrics

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

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.

Onfido MCP

6 tools available
Cloud-hosted on Vinkius

Running compliance checks used to mean logging into a dedicated dashboard, filling out forms, clicking 'start,' waiting for an email, and then manually cross-referencing results. Now, connecting Onfido through Vinkius changes that. You talk to your AI agent, tell it the task (like checking a new applicant's ID), and the system handles everything. The MCP lets you start by creating a profile using `create_applicant`. Next, you initiate the full process with `create_workflow_run`, which manages every step—document validation, face matching, etc.—in the background. You don't need to worry about the status; your agent tracks it and uses `get_workflow_run` to tell you exactly where things stand. When everything clears, you pull a full breakdown using `get_report`. It's all conversational. Your agent manages identity verification from start to finish.

Core Capabilities

01 — Manage Applicant Records

Create and track new profiles for individuals undergoing compliance checks.

02 — Run Full Verification Workflows

Start and monitor complex, multi-step identity verification processes automatically.

03 — Perform Specific Document Checks

Execute classic, targeted checks, such as comparing a photo to an uploaded ID document.

04 — Retrieve Detailed Reports

Pull comprehensive reports containing granular identity data and verification results.

05 — Get Status Updates

Check the real-time status of a running workflow run, like 'processing' or 'approved'.

06 — Set Up Status Alerts

Register webhooks to get immediate notifications when verification statuses change.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and enter your Onfido API Token within Vinkius.

02 Your AI agent authenticates the connection, making identity services available through natural language prompts.

03 You simply tell your agent what needs doing—like 'Start a verification for John Doe'—and it executes the necessary steps.

The bottom line is: you get to treat complex compliance tasks like simple chat commands.

Built For

Compliance Officers who are tired of digging through dashboards for audit trails.
Fintech developers needing to test identity flows directly in their code editor.
Operations teams that need to automate user onboarding and verification triggers.

Compliance Officer

Quickly checking the status of a pending applicant's verification or reviewing detailed report breakdowns without clicking through multiple tabs.

Fintech Developer

Integrating and testing identity verification flows directly from their IDE or terminal, treating it like any other API call.

Operations Manager

Automating the initial creation of applicants and triggering entire verification workflows as part of a new user's sign-up process.

What Changes When You Connect

01 Eliminate manual dashboard searching. Instead of clicking into a portal just to see if an applicant is ready, you ask your agent for the status using `get_workflow_run` and get instant answers.

02 Build robust onboarding flows that handle multi-step checks automatically. Using `create_workflow_run` means you don't have to manually trigger document validation followed by face matching—it's one command.

03 Speed up developer testing. You can integrate identity verification into code or scripts, using the MCP tools to test specific report retrievals via `get_report` without needing a live sandbox environment.

04 Maintain continuous compliance awareness. By setting up webhooks with `register_webhook`, you ensure your systems get immediate alerts when critical verification milestones are hit, eliminating manual checks.

05 Streamline user intake by automating record keeping. You can instantly initiate the process for a new person using `create_applicant` right from your chat client.

Real-World Applications

Onboarding a high-value contractor

The Ops Manager needs to verify a new contract employee. They tell their agent, 'Start the full onboarding check for Jane Doe.' The agent uses `create_applicant` first, then triggers `create_workflow_run`. When finished, they pull the final audit trail using `get_report`.

Checking compliance status during an audit

A Compliance Officer needs to know if 50 applicants are ready. Instead of running 50 manual checks, they ask their agent to check the status of multiple runs using `get_workflow_run` and get a compiled list of 'approved' or 'declined.'

Testing identity logic in a script

A Fintech Developer needs to test if their code correctly handles a failed document check. They use the MCP tools, specifically `create_check`, and feed the expected failure report directly into their testing environment.

System integration for real-time alerts

The system needs to know when an applicant moves from 'awaiting input' to 'approved.' Instead of polling a database, the developer uses `register_webhook` with the agent to guarantee instant, push-based notification.

Patterns to Avoid

Using Onfido via only the web UI

✗ AVOID

Manually logging into the Onfido dashboard every time a new user signs up just to start a verification process and check the status later.

✓ INSTEAD

Use your AI agent. Start by calling `create_applicant` to log the person, then trigger `create_workflow_run`. The MCP handles all subsequent steps and status checks for you.

Attempting manual data retrieval

✗ AVOID

If a user changes their profile information, manually searching through old reports or workflows to find the correct historical record.

✓ INSTEAD

Use `get_report` to pull the specific verification report you need. If you need history, use `get_workflow_run` and specify the timeline.

Assuming a single check is enough

✗ AVOID

Thinking that running just one document comparison (`create_check`) covers all compliance requirements for a new user.

✓ INSTEAD

Don't run individual checks. Use `create_workflow_run` to start the full process; this ensures all necessary, complex steps are executed in sequence.

The Right Fit

Use this MCP if your compliance needs involve multi-step processes that require managing state (e.g., 'Start X, wait for Y, then check Z'). You need to automate the entire lifecycle of identity verification—from initial record creation to final report retrieval. Don't use it if all you need is a simple data lookup or basic CRUD operation; those might be better handled by generic database connectors. If your goal is only to run single, isolated document comparisons without tracking history, then `create_check` handles that, but for full lifecycle management, this MCP is necessary.

Identity verification used to be a manual pain point.

Before tools like this MCP, onboarding someone was a headache. You'd have to click through three different tabs: one for applicant data, one for the workflow start button, and another just to check the status of your last report. Then you'd copy IDs from one dashboard and paste them into another system.

Now, those steps disappear. You talk to your agent, giving it a simple instruction like 'Verify John Doe.' The agent handles creating the applicant record, running all necessary background checks, monitoring every stage of the workflow, and finally providing you with everything in one clean response.

Onfido MCP: Getting structured verification status instantly

The most tedious part used to be checking if a process was stuck. You'd have to manually query the system repeatedly, hoping that the workflow hadn't stalled in 'pending' limbo for hours.

With this MCP, you simply ask your agent to check the run status using `get_workflow_run`. It gives you immediate feedback on where the process stands—is it waiting for input? Is it approved? You get confidence and speed without ever leaving your chat window.

Onfido: 6 Tools for Compliance and Verification

These six tools give you granular control over every stage of the identity verification process, from creating records to pulling final audit reports.

#	TOOL	DESCRIPTION
01	`create_applicant`	Makes a brand new record for an individual who needs identity verification.
02	`create_check`	Runs a classic, targeted check by combining specific document types or data points.
03	`create_workflow_run`	Starts an entire complex verification process that handles multiple steps automatically.
04	`get_report`	Pulls the final, detailed report for a completed identity verification run.
05	`get_workflow_run`	Retrieves the current status and history of an active or completed workflow process.
06	`register_webhook`	Sets up a system notification to alert you when a verification status changes.

See It in Action

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

U Create a new Onfido applicant for John Doe (john.doe@example.com).

I've created the applicant John Doe. The Applicant ID is 'app_12345'. You can now use this ID to start a verification workflow or a check.

U Start a verification workflow 'wf_abc' for applicant 'app_12345'.

Workflow run 'wr_999' has been started for applicant 'app_12345'. The current status is 'awaiting_input'.

U Retrieve the details for report ID 'rep_xyz789'.

I've fetched the report 'rep_xyz789'. The result is 'clear' with a breakdown showing document validity and image integrity are confirmed.

Frequently Asked Questions

01 **How do I start a new verification workflow using Onfido MCP?**

You initiate the process by calling `create_workflow_run`. This single action tells the system to run all necessary, multi-step checks required for compliance.

02 **What is the difference between create_check and create_workflow_run?**

`create_check` runs a specific, isolated comparison (like face matching). `create_workflow_run` starts the full, multi-stage identity onboarding process that includes multiple checks.

03 **Can I retrieve the final report details with Onfido MCP?**

Yes. After a workflow completes successfully, you use `get_report` to pull all the detailed verification data into your chat conversation for easy review.

04 **How do I get notified when an applicant's status changes?**

You set up an alert using `register_webhook`. This tells your system to send a notification immediately whenever the Onfido verification status shifts.

05 **Does Onfido MCP help with record keeping for new users?**

Absolutely. You first use `create_applicant` to establish the person's profile in the system, making them ready for subsequent checks and workflow runs.

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 `"onfido": { "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

Onfido 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 Onfido. 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	Onfido MCP
Server ID	`019e38cc-2ec8-7119-bd4b-b945267d6e11`
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/onfido.