MCP SERVER | NO CODE | CLOUD HOSTED

Persona MCP

Audit accounts and verifications instantly.

Persona MCP connects your AI agent directly to identity verification workflows. Handle KYC/AML compliance tasks—from managing user accounts and listing inquiries to approving or declining submissions—all through natural conversation. This tool lets you inspect verification results, process transactions, and permanently redact sensitive data without leaving your chat window.

F Quality Score 3.6/100

kyc | aml | identity-verification | risk-management | compliance | onboarding

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

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.

Persona MCP

27 tools available
Cloud-hosted on Vinkius

Connecting Persona through this MCP means your AI agent handles identity verification and KYC/AML compliance right where you work. You don't have to open a dozen browser tabs just to check if a user submitted their ID or what the status is on an old case file. Your agent acts as a dedicated compliance assistant, giving you instant access to critical data points like account records, transaction histories, and detailed verification results. Need to approve a pending submission? You can call `approve_inquiry` right away. Want to clean up sensitive data for GDPR compliance? Use the redaction tools. Because this MCP is hosted on Vinkius, your agent gets instant access to all these identity operations—list inquiries, get accounts, set case statuses, and much more. It makes auditing and acting on verifications immediate, letting you focus on risk management instead of dashboard clicking.

Core Capabilities

01 — Process Identity Submissions

You can approve or decline identity inquiries using dedicated tools.

02 — Manage User Records

Create, update, and retrieve full details on user accounts and associated data.

03 — Audit Compliance Data

List all inquiries, cases, and reports to audit compliance status or generate throughput metrics.

04 — Handle Sensitive Data Cleanup

Permanently delete PII from accounts, inquiries, or reports for privacy compliance (e.g., GDPR).

05 — Review Verification Statuses

Get detailed results and metadata on specific identity checks.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Persona API Secret Key.

02 Select your preferred AI client (Claude, Cursor, etc.) and authorize the connection.

03 Use natural language prompts with your agent; it executes the necessary functions like `get_inquiry` or `create_account` in the background.

The bottom line is you use your agent's chat interface to manage complex compliance workflows that used to require multiple manual dashboard logins.

Built For

Compliance Officers, Support Agents, and Developers need this. If your job involves manually checking user identity status or auditing large volumes of PII across different systems, this MCP cuts out the swivel-chair workflow entirely.

Compliance Officer

You use it to quickly review inquiry statuses and redact sensitive data from old records without running manual reports or spreadsheets.

Support Agent

During a customer call, you verify the user's account status and check their recent identity progress directly within your communication platform.

Development Engineer

You test new verification flows or write scripts that need to pull historical data by calling tools like `list_accounts` or `get_transaction` straight from your IDE.

What Changes When You Connect

01 Stop switching tabs. Instead of leaving your chat client to check an account's status, you use `get_account` or `list_inquiries` directly with your agent. It keeps all compliance data in one place.

02 Handle GDPR and CCPA requests easily. You can run specific redaction tools like `redact_account`, `redact_inquiry`, or `redact_verification` to prove permanent deletion of PII without manual database queries.

03 Accelerate decision-making. Need to approve a user? Use the `approve_inquiry` tool instantly, updating their status and completing the onboarding flow in one message exchange.

04 Build better reports. You can list all necessary records—from running `list_accounts` to calling `get_report`—to build complex audit trails without exporting CSV files first.

05 Maintain data integrity across systems. Use `create_transaction` or `set_case_status` to ensure that every action taken on a user record is logged and traceable for audits.

Real-World Applications

Onboarding a New Client

A Support Agent needs to confirm if a new client, Jane Doe, has finished her KYC. She asks the agent to list all inquiries for her ID. The agent uses `list_inquiries` and finds a pending status. The agent then retrieves the details using `get_inquiry`, sees everything is ready, and calls `approve_inquiry`. Done in three steps.

Handling Data Subject Requests

A Compliance Officer receives a request to delete all data on an inactive user. Instead of manually finding the account ID, they ask the agent to run the redaction tools. The agent executes `redact_account`, and the officer confirms permanent removal from their chat history.

Investigating Suspicious Activity

A risk analyst suspects an account is compromised. They use the agent to check for unusual activity by calling `list_events` across a range of dates, then fetching all associated transactions via `get_transaction` to build a full timeline.

Developer Testing and Integration

A developer needs to test their internal system's ability to process new users. They use the agent to call `create_account` with dummy data, then immediately follow up by calling `get_verification` to ensure the record was created correctly.

Patterns to Avoid

Manually tracking status changes

✗ AVOID

A support agent opens five different tabs—the inquiry dashboard, the account page, the case management portal, and the report generator—to figure out if a user is compliant.

✓ INSTEAD

Ask your AI client to run `list_inquiries` first. Then, use `get_account` on the resulting ID. Finally, use `get_verification` to confirm all necessary components are updated.

Confusing account and inquiry data

✗ AVOID

A user asks about a 'record' but means either the person (Account) or the verification attempt (Inquiry). The human has to guess which dashboard is correct.

✓ INSTEAD

Specify your request. If you mean the people, use `get_account` and `list_accounts`. If you mean the identity checks, use `get_inquiry` and `list_inquiries`.

Ignoring data retention policies

✗ AVOID

An employee just deletes a record from one dashboard but forgets to redact it in another system's log or report.

✓ INSTEAD

To ensure full compliance, always pair deletion with redaction. If you delete an account, call `redact_account` and then also run `redact_inquiry` for any related records.

The Right Fit

Use this MCP if your job requires cross-referencing identity data across multiple compliance stages: accounts, inquiries, transactions, and reports. Specifically, if you need to approve submissions (`approve_inquiry`), or permanently delete PII (`redact_account`), this is the right tool. Don't use it if all you need is a simple list of emails; basic CRM tools are fine for that. Also, don't rely on it as your sole data source; always verify critical decisions by running multiple calls (e.g., `list_accounts` then `get_account`). This MCP gives you the operational hooks, but you still need human judgment to interpret the results and make the final call.

The Friction of Identity Compliance

Today, confirming a user's identity status is a nightmare of context switching. You open your CRM for account details. Then you jump to the KYC dashboard to see if their documents cleared. Next, you might have to go into a separate case management system just to check the last audit report. Copy-pasting IDs between these three or four tabs and systems takes minutes per user, slowing down everything.

With this MCP, that entire process collapses into one chat conversation. Your agent pulls all necessary data—account status from `get_account`, inquiry history from `list_inquiries`, and transaction logs using `list_transactions`—and presents it to you instantly. You get a single source of truth without ever leaving the conversational interface.

Identity & Account Operations

The biggest manual step that vanishes is status updating. Instead of logging into a separate portal just to change an inquiry's state from 'Pending' to 'Approved,' you simply ask the agent to run `approve_inquiry`. It does the work and updates the record immediately.

This changes everything. You stop being a dashboard jockey and start being a decision-maker. The entire compliance process flows directly through your AI agent, making it faster, auditable, and infinitely less frustrating.

Persona: 27 Tools for Identity Ops

These tools let you manage every step of identity verification, from creating new users to redacting sensitive data. Use them with your AI client to automate compliance tasks.

#	TOOL	DESCRIPTION
01	approve_inquiry	Marks a pending identity inquiry as approved.
02	create_account	Initializes a new user account record in the system.
03	create_inquiry	Starts a new identity verification request for a user.
04	create_transaction	Logs a new financial or operational transaction record.
05	create_webhook	Sets up automated webhooks to notify other services of status changes.
06	decline_inquiry	Marks an identity inquiry as declined, halting the verification process.
07	get_account	Retrieves all specific details for a single user account ID.
08	get_case	Fetches detailed information about a specific compliance case file.
09	get_event	Retrieves records of important system events that occurred for an account or inquiry.
10	get_inquiry	Gets the current status and data for a specific identity inquiry ID.
11	get_report	Retrieves detailed compliance reports, often covering watchlists or adverse media checks.
12	get_transaction	Fetches the full details for a specific transaction record.
13	get_verification	Retrieves the complete results and metadata for an identity verification attempt.
14	list_accounts	Generates a list of all existing user accounts in the system.
15	list_cases	Provides a comprehensive list of open and closed compliance cases.
16	list_events	Lists historical events that have occurred across the system's records.
17	list_inquiries	Retrieves a list of all identity verification inquiries, allowing filtering and pagination.
18	list_reports	Generates a bulk list of compliance reports available for review.

#	TOOL	DESCRIPTION
19	`list_transactions`	Provides a paginated list of all recorded transactions.
20	`list_webhooks`	Lists the current webhooks configured to notify other services.
21	`redact_account`	Permanently removes Personally Identifiable Information (PII) from a specific user account record.
22	`redact_inquiry`	Performs permanent data deletion of sensitive PII associated with an inquiry.
23	`redact_report`	Cleans up and permanently redacts PII from a specific report document.
24	`redact_verification`	Deletes sensitive data points associated with an identity verification check.
25	`set_case_status`	Updates the active status of a compliance case (e.g., open, closed).
26	`trigger_workflow`	Starts a predefined workflow run for a specific purpose.
27	`update_account`	Modifies existing data points on an account, such as changing contact details or status.

See It in Action

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

U List the most recent 10 identity inquiries.

I've retrieved the latest inquiries. There are 10 records found, including Inquiry inq_123abc (Status: completed) and inq_456def (Status: pending). Would you like to inspect the details of the pending one?

U Get the account details for account ID acc_789ghi.

Fetching account acc_789ghi... This account is associated with user 'Jane Doe', created on 2023-10-12, and currently has 2 completed verifications linked to it.

U Approve inquiry inq_456def.

Processing approval for inq_456def... The inquiry has been successfully approved. The user's status has been updated in the Persona dashboard.

Frequently Asked Questions

01 **How do I check if an account has been redacted using Persona MCP?**

You use the `get_account` tool to retrieve the record. If PII was successfully removed, the returned data fields will be null or replaced with redaction markers, confirming compliance.

02 **Can I list all pending inquiries using Persona MCP?**

Yes, you use `list_inquiries`. You can filter this list by status (e.g., 'pending') and then select specific IDs to fetch full details with `get_inquiry`.

03 What is the difference between `create_account` and `update_account`?

`create_account` establishes a brand new user record. `update_account`, however, modifies an existing account's data—like changing their phone number or status.

04 Do I need to manually approve every inquiry after using Persona MCP?

No. While the tool provides the action via `approve_inquiry`, you still must review the details retrieved by `get_inquiry` first, confirming that all necessary checks passed before giving approval.

05 How do I ensure my data is compliant with GDPR using Persona MCP?

You use the dedicated redaction tools like `redact_account`, `redact_inquiry`, and `redact_report`. These calls permanently delete PII, providing an auditable trail of compliance.

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 `"persona": { "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

Persona 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 Persona. 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	Persona MCP
Server ID	`019e38d6-13b6-7295-9481-16eb71bcc74f`
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/persona.