MCP SERVER | NO CODE | CLOUD HOSTED

Dynamic Web3 Auth MCP for AI Agents

Verify wallet sanctions and manage decentralized identity compliance.

Dynamic Web3 Auth MCP lets your AI agent handle complex blockchain security tasks. It gives you the power to check if a wallet address is sanctioned across multiple chains, fetch detailed user profiles, or instantly terminate active sessions—all without leaving your chat window.

A+ Quality Score 100/100

web3-authentication | wallet-security | user-management | sanction-screening | session-management | decentralized-identity

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/dynamic-web3-auth

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.

Dynamic (Web3 Auth) MCP

8 tools available
Cloud-hosted on Vinkius

Managing web3 users and ensuring compliance used to mean jumping between dashboards, running manual checks on block explorers, and calling support for session resets. Now, you connect this MCP to any compatible AI client and handle all that complexity through natural conversation. You can ask your agent to fetch a user's full profile or verify if an address is flagged as sanctioned across ETH, SOL, and other major chains. Need to secure an environment? Tell your agent to revoke a suspicious session instantly. For developers building complex systems, this makes managing the entire web3 authentication layer—from initial sign-up to compliance auditing—a single conversation. If you’re looking for robust security tooling, Vinkius hosts this MCP right in the catalog so you can connect once and get access to professional-grade Web3 identity management.

Core Capabilities

01 — Audit wallet sanctions across chains

Check if a given blockchain address is sanctioned or flagged on multiple networks (like Ethereum, Solana, etc.) using the check_sanctions tool.

02 — Manage user identity and profiles

Fetch complete details for a specific user account or permanently remove an account entirely from your environment using get_user and delete_user.

03 — Control active sessions instantly

Forcefully terminate any currently logged-in user session with the revoke_session tool, maintaining strict security boundaries.

04 — Monitor system configuration

List all configured webhooks or retrieve real-time token balances for users across different blockchains to audit setup integrity.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/dynamic-web3-auth** — connect your AI agent in three steps.

01 Subscribe to this MCP and enter your unique Dynamic API Token into the Vinkius catalog.

02 Select your preferred AI client (Claude, Cursor, etc.) and connect it using the MCP integration.

03 Ask your agent a question—for example, 'What is the current balance for user X?' or 'Check sanctions for 0x...'—and get an immediate, actionable answer.

The bottom line is that you turn complex security operations into simple natural language prompts.

Built For

This MCP is built for people who manage high-stakes digital identities and need instant compliance visibility. It's for the Security Engineer tired of manual dashboard checks, the Web3 Developer debugging user flows at 2 AM, or the Ops Team needing to audit suspicious sessions without logging into a separate portal.

Security Engineer

Using this MCP, you can audit wallet sanctions and revoke compromised user sessions instantly from your agent interface.

Web3 Developer

You debug complex user profiles or fetch token balances directly within your code editor by asking your AI client to run the necessary checks.

Operations Manager

You audit webhook configurations and monitor active embedded wallet versions to ensure platform stability during feature rollouts.

What Changes When You Connect

01 Stop manual checks. You can run `check_sanctions` to verify a wallet's status on ETH or SOL instantly, feeding the result directly into your agent workflow.

02 Maintain security control by using `revoke_session`. If an account is suspicious, you end the session in seconds without opening any dashboard.

03 Streamline user data access. Use `get_user` to pull a full profile and then run `get_token_balances` to get their current holdings, all in one prompt.

04 Improve auditability by running `get_webhooks`. You see exactly what events the system is monitoring and where that data goes.

05 Reduce compliance risk. By having tools like `delete_user`, you ensure that when an account needs to be permanently removed, it happens securely and completely.

Real-World Applications

Handling a Suspicious Login

An agent detects unusual activity. Instead of waiting for an admin, it uses the MCP to run `check_sanctions` on the user's wallet and then immediately calls `revoke_session` if any red flags appear.

Onboarding a New Partner

A developer needs to validate a new partner. They ask their agent to run `get_user` for the profile, check current token balances using `get_token_balances`, and ensure all webhooks are correctly configured.

Compliance Cleanup

The security team needs to purge old accounts. They use the MCP to identify users via `get_user` and then execute `delete_user` on those records, maintaining a clean audit trail.

Patterns to Avoid

Only checking dashboards

✗ AVOID

Manually logging into the web dashboard to check user profiles or sanctions status every time an event happens. This is slow and prone to human error.

✓ INSTEAD

Use your agent to call `get_user` for profile details, then run `check_sanctions` directly in conversation. This automates the entire audit process.

Ignoring session status

✗ AVOID

Assuming a user logged out just because they closed the tab. The session might still be active and vulnerable.

✓ INSTEAD

Always use `revoke_session` via your agent to forcefully end access, guaranteeing the environment is secure regardless of client-side actions.

Overlooking token data

✗ AVOID

Thinking a user's identity confirms their wealth. You might miss crucial financial context.

✓ INSTEAD

Combine `get_user` with `get_token_balances`. This gives your agent the full picture: who they are, and what assets they control.

The Right Fit

Use this MCP if your core business function relies on real-time identity validation, compliance auditing, or immediate session control in a decentralized environment. You need to know *who* the user is, *if* their wallet is clean, and *if* they are currently allowed access. Don't use it if you simply need to read static documentation or perform generic CRUD operations on non-web3 data. If your goal is just listing available event types (using `get_event_types`), this MCP covers that, but if you need deeper integration with external databases not related to web3 identity, look at a general API connector instead.

Dynamic Web3 Auth MCP: Managing Wallet Sanctions and Identities

Today, vetting user identities in web3 is an administrative nightmare. You have to open multiple tabs—one for the profile data, one for the blockchain explorer, and a third just to check if their wallet has been flagged by compliance lists. This process requires constant context switching and manual copy-pasting of addresses.

With this MCP, you simply ask your agent to verify an address's status. It runs checks across multiple chains using `check_sanctions` and provides a clean pass/fail verdict immediately. The result is actionable intelligence without the painful dashboard dance.

Dynamic Web3 Auth MCP: Controlling User Sessions and Data Access

Before this tool, securing an account meant relying on manual logouts or waiting for a timeout. If you suspected unauthorized access, the only option was often to call an admin team and wait.

Now, your agent can use `revoke_session` instantly. You execute the command, confirm the session is dead, and move on. It gives you granular control over every active connection point.

8 Tools for Dynamic Web3 Auth: Sanctions & User Management

These tools let your agent perform specific actions like checking token balances or deleting users directly within the chat interface.

#	TOOL	DESCRIPTION
01	`check_sanctions`	Verifies if a specific blockchain wallet address is listed as sanctioned across multiple chains.
02	`delete_user`	Permanently removes an existing user account from the system environment.
03	`get_embedded_wallet_versions`	Retrieves a list of all active embedded wallet versions configured in your current setup.
04	`get_event_types`	Lists the specific types of user or session events available for webhook subscriptions.
05	`get_token_balances`	Pulls real-time token balance data for a specified user across various connected networks.
06	`get_user`	Retrieves comprehensive profile details for an identified user within a specific environment.
07	`get_webhooks`	Shows the current list of configured webhooks and their status settings.
08	`revoke_session`	Immediately ends an active user session, ensuring that only authorized parties maintain access.

See It in Action

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

U What are the current balances for user ID 'usr-789'? I need to check ETH and SOL.

User: usr-789

- 🌐 **Ethereum (ETH):** 12.45 ETH
- 🌞 **Solana (SOL):** 450 SOL
- 💰 **Stablecoins:** $1,230 USD equivalent

Last updated: Moments ago.

U Please check if the wallet address 0xabc... is sanctioned on any major chain.

Sanctions Check Results

CHAIN	STATUS
Ethereum (ETH)	✅ Clear
Polygon (MATIC)	✅ Clear
Solana (SOL)	❌ Flagged

Action required: Block all transactions from this address until manual review.

U I need to know what event types I can subscribe to for webhooks.

You can set up webhook subscriptions for the following key events:

- `user.created` : When a new user signs up.
- `wallet.authenticated` : Every time a wallet successfully connects.
- `session.started` : A session begins, indicating active usage.
- `email.verified` : Confirms the user has provided and verified an email address.

Each event payload contains detailed metadata you can use for advanced logic.

Frequently Asked Questions

01 **How does the Dynamic Web3 Auth MCP help me manage user identity and security?**

It lets your AI agent handle critical tasks like checking if a wallet is sanctioned or instantly revoking sessions. You get enterprise-grade compliance controls without ever leaving your chat interface.

02 **Can the Dynamic Web3 Auth MCP check token balances for multiple chains?**

Yes, you can use this MCP to retrieve real-time token balances for a user across different major networks. This provides an immediate view of their total assets.

03 **What if I need to remove a user's account entirely? Does the Dynamic Web3 Auth MCP handle that?**

The MCP includes dedicated tools to permanently delete users from your environment, ensuring full compliance when an account needs to be removed.

04 **How do I use the Dynamic Web3 Auth MCP for auditing purposes?**

You can audit your setup by listing all configured webhooks or checking which embedded wallet versions are active. This gives you a clear picture of your current security posture.

05 **Is the Dynamic Web3 Auth MCP better than just using the native dashboard?**

Absolutely. The MCP allows you to run complex, multi-step workflows—like checking sanctions and revoking sessions in one go—which is much faster and more reliable than navigating a dashboard.

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 `"dynamic-web3-auth": { "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

Dynamic (Web3 Auth) 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 Dynamic (Web3 Auth). 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	Dynamic (Web3 Auth) MCP
Server ID	`019e388f-445a-712b-a72b-54dc65d62c86`
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/dynamic-web3-auth.