MCP SERVER | NO CODE | CLOUD HOSTED

Tencent Youtu / 腾讯优图 MCP

Verify Identities and Audit Visual Assets Instantly

Tencent Youtu / 腾讯优图 provides professional-grade computer vision, giving your agent instant facial recognition and analysis. Detect faces in images, calculate identity similarity scores, check liveness, and manage secure person libraries—all from one authorized source.

A+ Quality Score 100/100

computer-vision | facial-recognition | biometrics | image-analysis | liveness-detection | person-management

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/tencent-youtu

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.

Tencent Youtu / 腾讯优图 MCP

8 tools available
Cloud-hosted on Vinkius

Complex image analysis used to verify identities or audit content used to be a nightmare of specialized software logins and manual comparison sheets. Now, your agent handles it all. You can connect this MCP to your preferred AI client and simply talk through visual intelligence workflows. Your agent detects faces in image URLs, pulls out details like age or beauty scores, and compares identities across multiple photos. It even performs static liveness checks for compliance needs. If you're building a Know Your Customer (KYC) system or auditing digital assets, the platform manages person libraries and groups without you ever having to open the Tencent Cloud Console. Using Vinkius, your agent acts as an instant computer vision specialist, giving fast, accurate results directly within your workflow.

Core Capabilities

01 — Analyze facial attributes

The system processes a face and returns detailed metrics like gender, estimated age, or beauty scores.

02 — Compare two identities

It calculates a precise similarity score between two uploaded images to determine the likelihood that they belong to the same person.

03 — Identify faces in an image

The system scans any image URL and reports exactly where faces are located within it.

04 — Verify live presence

It performs a liveness check on a face to confirm the person is physically present, not using a photo or video loop.

05 — Manage user groups and records

You can list existing groups of people or retrieve specific members registered within those defined groups.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and enter your necessary Tencent Cloud SecretId and SecretKey.

02 Connect the credential set to your AI client (like Claude or Cursor).

03 Tell your agent what you need. For example, 'Analyze face attributes for this image' or 'Compare these two photos.' The system runs the check and gives you a direct answer.

The bottom line is that it lets you turn complicated biometrics into simple conversational commands.

Built For

This connector is essential for security teams, compliance officers, and developers who routinely deal with identity verification or content auditing. If your job involves checking if a photo belongs to someone specific, this tool saves you hours of manual comparison work.

Security Analyst

Uses the MCP to automate identity verification workflows and monitor visual access logs by detecting faces and confirming person details.

Compliance Officer

Runs liveness checks and compares identities across documents, ensuring that every piece of submitted data meets strict regulatory standards.

App Developer

Integrates world-class facial analysis into the application's core logic by calling functions like list group members or register person programmatically.

What Changes When You Connect

01 Eliminate manual image review. Instead of logging into a separate console, your agent uses the `detect_face` tool to find every face in an image and provide immediate attributes.

02 Speed up compliance checks. Use `live_face_check` whenever you need proof that a person is physically present, making your KYC process much faster than manual video review.

03 Simplify identity matching. The `compare_faces` tool instantly tells you if two photos are of the same person with a numerical score, eliminating guesswork in asset audits.

04 Centralize data management. Instead of keeping spreadsheets for who belongs where, use `list_persons_in_group` and `register_person` to manage your entire identity database within your agent's conversation flow.

05 Streamline search operations. If you need to audit assets, the `search_face_in_groups` tool lets you pinpoint specific people across massive libraries without running complex queries.

Real-World Applications

Auditing Content for Copyright and Identity

A content moderator needs to check thousands of uploaded images for faces belonging to a restricted group. Instead of downloading everything and using desktop software, the agent detects faces in image URLs and uses `search_face_in_groups` to flag any matches within the designated 'restricted' person library.

Automating Customer Onboarding (KYC)

A new user submits a profile photo. The agent first runs the `live_face_check` to confirm identity, then uses `analyze_face` to gather demographic data, and finally calls `register_person` to index them into the 'active_clients' group.

Investigating Suspects in a Breach

A security team needs to know if an unknown face is related to any known bad actors. They use `detect_face` on the suspect image, then run it through `compare_faces` against all records retrieved via `list_persons_in_group` to find potential matches.

Maintaining Employee Records

The HR department needs a current list of staff members in the 'field_sales' group. They ask the agent to use `list_persons_in_group`, instantly getting a vetted, up-to-date roster without touching any backend dashboard.

Patterns to Avoid

Comparing faces in Excel

✗ AVOID

Manually taking two photos, running them through an external biometric checker, recording the score, and then cross-referencing that data across multiple sheets.

✓ INSTEAD

Use `compare_faces` to get the similarity score directly within your agent's conversation. Then use `analyze_face` on both images sequentially to gather all needed attributes in one go.

Manually listing group members

✗ AVOID

Having to log into a separate person management system just to see who is part of the 'admin' team. This takes multiple clicks and navigating different tabs.

✓ INSTEAD

Simply tell your agent to use `list_persons_in_group` for the 'admin' group. The list shows up immediately, no dashboard required.

Checking liveness separately

✗ AVOID

Getting a photo from one service and running it through another specialized tool just to confirm it wasn't a printout or deepfake.

✓ INSTEAD

Use the `live_face_check` tool. It handles both detection and verification in a single, conversational step.

The Right Fit

You need this MCP if your core business process revolves around verifying identity using visual data, or maintaining structured records of people's identities. Use it when you must compare faces, check liveness, or manage large groups of registered individuals. Don't use this if you only need to extract simple text from an image, like reading a name off a sign (you'd need an OCR tool). Also, don't use it just because you have photos; you must be performing one of the core biometrics tasks, such as identity confirmation or group management. If your task is simply 'tell me what color this car is,' this MCP won't help—it's specialized for faces only.

The headache of visual content auditing today

Right now, if you need to audit a batch of photos, you open the platform's console. You click through folders, download images one by one, and then run each image through an analysis tool to check for faces or attributes. This process is slow, involves constant context switching, and takes hours of highly specialized labor just to gather basic metadata.

With this MCP connected via Vinkius, you talk to your agent like you're talking to a coworker. You point to the batch of images and ask: 'Find me all faces in these pictures that belong to Group X.' The agent handles the detection, comparison, and retrieval instantly, giving you a clean report without ever needing to click through a single dashboard.

Tencent Youtu / 腾讯优图 gives you identity verification.

You no longer have to manually check if two people in different photos are the same. The agent uses `compare_faces` and delivers a single, actionable similarity score right into your chat window. It’s like having instant forensic comparison data available on demand.

This changes everything. Your AI client doesn't just process text; it processes visual truth. You get accurate biometrics as part of your natural workflow.

Tencent Youtu / 腾讯优图 - 8 Tools

These eight tools allow you to perform everything from basic face detection to complex identity comparisons, all through conversational commands.

#	TOOL	DESCRIPTION
01	analyze_face	Analyzes an image and returns detailed metrics about the face, such as estimated age, gender, and beauty score.
02	compare_faces	Compares two specific faces and generates a numerical similarity score to determine identity matches.
03	detect_face	Scans an image URL and identifies the precise location of any face present in that picture.
04	list_face_groups	Retrieves a list of all defined person groups within your registered system library.
05	list_persons_in_group	Pulls a list of every individual registered and associated with a specific group name.
06	live_face_check	Verifies if the person in an image is genuinely alive and present, preventing fraud from static media.
07	register_person	Adds a brand new individual to your secure library by associating them with a photo and group.
08	search_face_in_groups	Searches through the entire person library, looking for matches based on specific facial features or groups.

See It in Action

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

U Detect faces in this image: [URL] and show me their attributes.

I've analyzed the image. I detected one face belonging to a male, approximately 28 years old, with a beauty score of 82/100. Should I search for this person in your registered groups?

U Compare these two face images: [URL_A] and [URL_B].

The facial comparison is complete. The similarity score is 94.5, indicating a very high probability that these are the same person. Would you like me to check if this identity is already registered in your person library?

U Register a new person 'Alice' in group 'staff_01' with image [URL].

Alice has been successfully registered in group `staff_01` with ID `alice_8821`. Her facial features have been indexed for future recognition. Should I list all members currently in this group?

Frequently Asked Questions

01 **How does Tencent Youtu / 腾讯优图 handle identity verification?**

It compares two faces using the `compare_faces` tool, which generates a specific similarity score. A high score indicates a very strong probability that both photos depict the same person.

02 **Can I use Tencent Youtu / 腾讯优图 to check if someone is real?**

Yes, you can run a liveness check using `live_face_check`. This confirms whether the face in the picture or video stream belongs to a living person and isn't just a static image.

03 **What if I need to add new people to my system?**

You use the `register_person` tool. This function lets you create a brand-new identity record, linking them to specific photos and assigning them to an official person group.

04 **Does Tencent Youtu / 腾讯优图 help with large datasets?**

Absolutely. You can use `search_face_in_groups` to scan through massive person libraries and automatically find matching faces based on criteria or groups you define.

05 **Do I need technical skills to use Tencent Youtu / 腾讯优图?**

No. Because it's connected via MCP, you simply ask your agent what you need—for example, 'Analyze face attributes for this image.' The tool handles the complexity.

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 `"tencent-youtu": { "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

Tencent Youtu / 腾讯优图 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 Tencent Youtu / 腾讯优图. 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	Tencent Youtu / 腾讯优图 MCP
Server ID	`019d848b-74b8-71c6-98c9-9d1fcdfd38ed`
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/tencent-youtu.