



DATASHEET • DATA APIS • DEVICE FINGERPRINT

Same device, new account? Now you recognize the device.

Device Fingerprint recognizes browsers and devices through a browser SDK and returns a stable visitor_id per device, first and last seen, risk factors and a bot signal. For sign-in, checkout and account protection: via SDK, REST API and MCP.

AT A GLANCE

One visitor_id per device, stored separately per organization. At the next login, /fingerprint/verify checks whether it is the same device and shows which signals match.

01 · WHAT IT IS ABOUT

New email, new account? The device stays the same.

People who create several accounts or use someone else's login change email and name, but rarely the device. Device Fingerprint gives every browser a stable ID and reports when it was first and last seen and what stands out about the session.

SIGNALS

Canvas, WebGL, audio, fonts, hardware and screen via SDK, plus IP and user agent

RESULT

visitor_id, visits, first and last seen, device, risk 0–100 with factors, bot signal

ACCESS

Browser SDK with a publishable key, REST API /fingerprint, MCP in the /mcp-full catalog

PRIVACY

Device data separated per organization, deletion per ID with POST /privacy/forget

**Stable ID**

The SDK builds hashes from canvas, WebGL, audio and fonts. If a browser arrives with a new ID but the same values, its history continues.

Verify at login

/fingerprint/verify compares JA4, user agent, IP, canvas and WebGL with the stored device and returns verified and matchScore.

Risk with reasons

risk.factors names what stands out: VPN, proxy, Tor, data center, relay, impossible travel speed or a known bot.

Bot detection

bot returns is_bot, a score and signals, calculated on the server: headless browsers, automation, software rendering, missing interaction.

Similar devices

/fingerprint/similar finds devices with similar hashes in your data, with similarity in percent and an adjustable threshold.

Devices on the same network

/fingerprint/linked shows which other devices came from the same networks, for example several devices in one home or office.

02 · HOW IT WORKS

Add the SDK, get the ID. Compare at login.

The SDK runs on your website and talks to the API directly with a publishable key. Your backend compares later with the API key.

1

Create a publishable key

Under `API & Developer > API Keys`, choose `Create New Key`, then the type `Publishable Key`, and enter your website's domains.

2

Add the SDK

Load `/fingerprint/sdk` with a script tag, call `PaperOfficeFingerprint.load` with your key and then `get()`.

3

Store the ID

The result contains the `visitor_id`. Store it in your system with the login or order.

4

Compare and evaluate

At the next login, `POST /fingerprint/verify` checks the device. `risk.factors` and `bot` show what stands out.

TECHNICAL DATA

FEATURE	DETAILS
SDK	<code>https://api.paperooffice.ai/latest/fingerprint/sdk</code> , as an ES module at <code>/fingerprint/sdk.esm</code>
Endpoints	<code>POST /fingerprint/identify</code> , <code>POST /fingerprint/verify</code> , <code>GET /fingerprint/device</code> , <code>/similar</code> , <code>/linked</code>
Response fields	<code>visitor_id</code> , <code>visits</code> , <code>first_seen</code> , <code>last_seen</code> , <code>device</code> , <code>ip</code> , <code>risk (score, level, factors)</code> , <code>bot</code>
Access	Browser: publishable key (<code>po_pk_</code>); backend: API key; MCP in the <code>/mcp-full</code> catalog
Deletion	<code>POST /privacy/forget</code> with <code>visitor_id</code> or <code>identifier_hash</code> ; response with tombstone
Tenant separation	Device data is stored and queried separately per organization
Billing	Pay as you go

03 · IN PRACTICE

Where the device matters. Three typical flows.

Protect sign-in

When a known account signs in from an unfamiliar device or with impossible travel speed, your application asks for a second factor.

Spot multiple sign-ups

When one device creates new accounts, your system shows the same visitor_id on several accounts. /fingerprint/linked adds devices from the same network.

Tell bots from people

During sign-up or a voucher campaign, your application holds back sessions with bot.is_bot, such as headless browsers or automation without interaction.

FREQUENTLY ASKED QUESTIONS

Which signals does the SDK use?

Canvas, WebGL, audio, fonts, hardware and screen properties, plus mouse, keyboard and touch patterns for bot detection. On the server, IP and user agent are added.

How do I handle deletion requests?

POST /privacy/forget deletes the device profile, links, history and alerts for the ID in your organization. A tombstone keeps the same ID from being captured again.

How do I recognize a known device?

identify reports is_new and visits. GET /fingerprint/device returns first and last seen, visits, browser, platform and country for a visitor_id.

Who is responsible for the data?

As the controller, you set purpose and legal basis. The identify response lists data categories, purposes and the recommended legal basis in its compliance block.

GET STARTED

Recognize devices from the next login on

Create an account, generate a publishable key for your domain under [API & Developer › API Keys](#) and add the SDK to your sign-in page.

paperoffice.ai/en/ai-device-fingerprint-browser-tracking-fraud-prevention



MORE ABOUT THE MODULE

paperoffice.ai/en/ai-device-fingerprint-browser-tracking-fraud-prevention

PRICING

paperoffice.ai/en/pricing

CONTACT

paperoffice.ai/en/contact