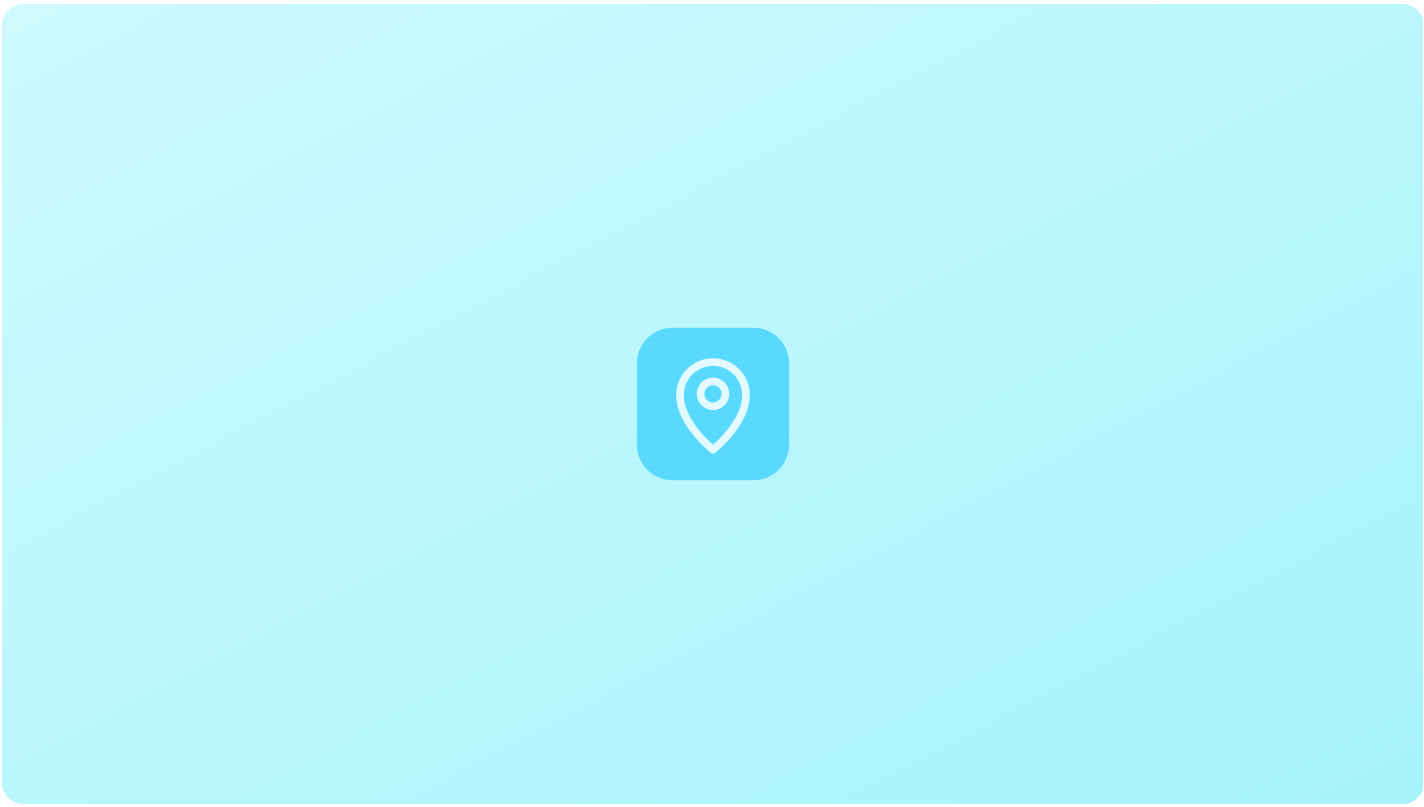
URTRAVELPRO



TRIPS

# Passport access log

The append-only audit trail of every passport upload, view, download, and delete across your agency. Why it exists, who can read it, how to filter by action / agent / date, and what each row contains.

Prepared by System Generated · June 10, 2026

On this page



The Passport access log (at `/reports/passport-access-log`) is the audit trail for every passport scan stored in Trips. Each upload, view, download, and delete writes a row — the agent who did it, their IP address and browser, the contact whose passport it was, and the exact timestamp. Append-only, owner / admin only, never purged.

> **IMPORTANT**
>
> **Owners and admins only.** Passport access history is itself sensitive — it reveals which travelers have passports on file and who has been looking at them. Members and viewers cannot reach this page.

## Why it exists

Travel agencies routinely handle scanned passports for visa support, cruise check-in, and international flight bookings. That is personal identity data — under most consumer-protection regimes (GDPR, CCPA, your professional E&O policy), if a client ever asks *"who at your agency has looked at my passport?"* you need a defensible answer. The log gives you one — without anyone in your agency needing direct database access or having to file a ticket with us.

## What each row contains

Four actions are logged, one row each. Every row carries:

- **Action** — `upload`, `view`, `download`, or `delete`.
- **Actor** — the agent's name if a logged-in user did it, or *"Client (portal)"* if the traveler uploaded their own scan from the client portal.
- **Contact** — whose passport. Resolved through Core so the name is current even if the contact has been renamed.
- **Attachment** — the kind (main scan, second page) and the original filename when uploaded.
- **IP address + user agent** — captured at the moment of the action. User agents are truncated to 80 chars in the UI; the full string is in the database.
- **Timestamp** — `occurred_at` in your org's timezone.

## Filtering

Three filters across the top, all optional:

- **Action** — narrow to one of upload / view / download / delete. Audit a deletion specifically by filtering to `delete`.
- **Agent** — the dropdown lists every agent who has at least one logged action in the org. Picking one scopes the table to "what did this person see this month?"
- **Date range — from / to** — defaults to the last 30 days because the log can grow large for older agencies. Widen as needed.

Four counters above the table — Uploads, Views, Downloads, Deletes — update with the filters so you can read the shape of the window at a glance.

> **ADVISOR TIP**
>
> **Client portal uploads count too.** When a traveler uploads their own passport from the client portal, the row is labeled *"Client (portal)"* instead of an agent name. That is by design — you want to be able to attribute the action even when no member of your agency did it.

## Retention

The log is **append-only**. Trips never deletes rows; there is no "older than 90 days" purge. The row stays even if the passport scan itself is later deleted — the `delete` action shows up as its own row, and the upload + every view that came before it stays in place. That is what makes the log defensible after the fact.

## Related

- Reports overview
- Passport collection
- Trip files
- Team management + roles