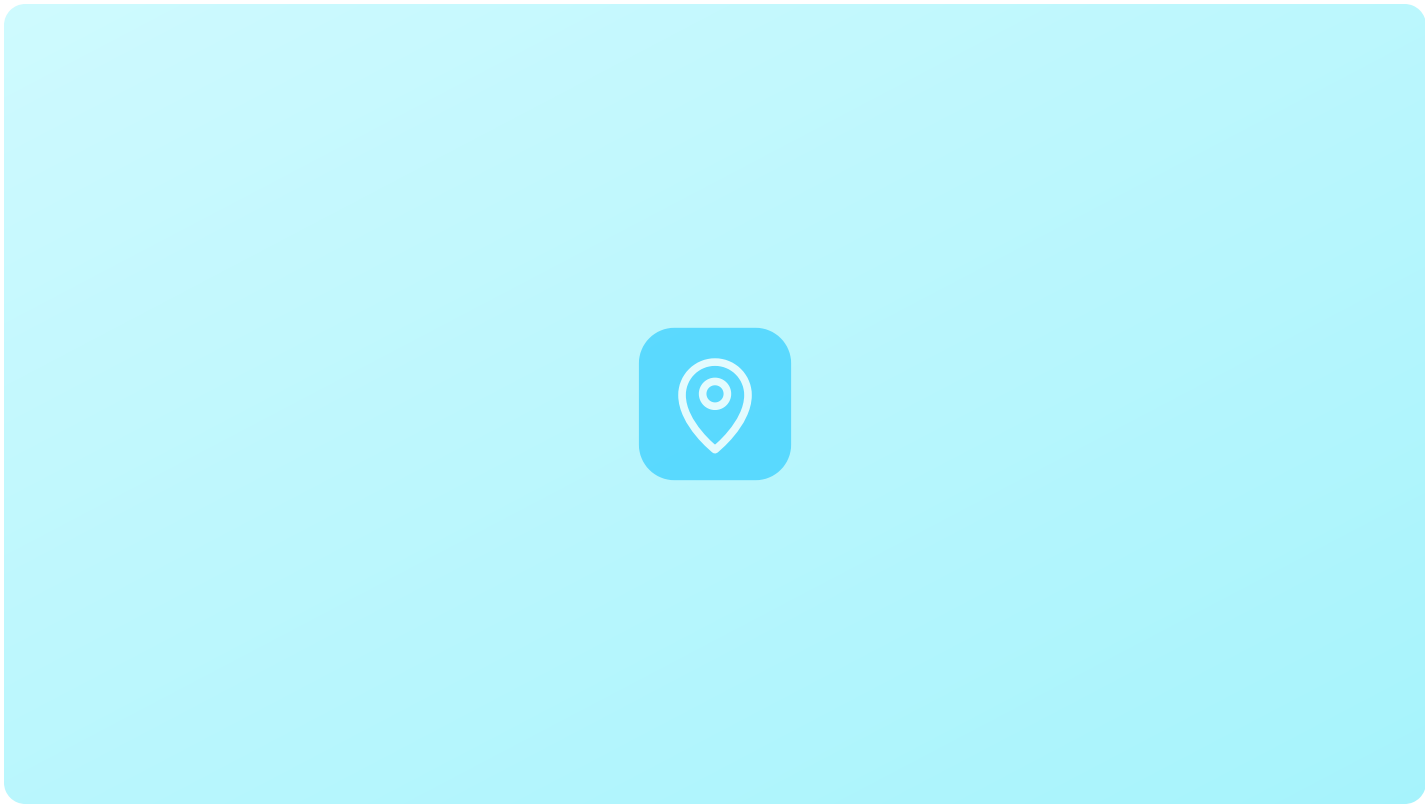
URTRAVELPRO



TRIPS

Passport collection workflow

The right way to collect passport details and scans from clients: a trip-attached form with passport identity fields plus a file-upload field routed to the encrypted passport vault. End-to-end encryption, per-agency keys, audited every access.

Prepared by System Generated · June 10, 2026

On this page

Collecting passport information is the highest-stakes data exchange a travel agency does — name, date of birth, passport number, scanned ID document. Trips bakes a purpose-built pipeline for it: a trip-attached form captures the structured fields, a file-upload field routes the scan straight into an encrypted passport vault, and every later access is audit-logged.

> IMPORTANT
>
> **Don't collect passports by email.** A passport scan attached to a Gmail thread sits unencrypted in two inboxes (yours and the client's) forever. The Trips form pipeline stores the scan encrypted at rest with a key derived per agency, and an audit row is written every time anyone — even you — looks at it.

The shape of a passport form

Build a **Trip-attached** form (kind = trip_attached) with three categories of field:

Identity (Core slot)

- `first_name`
- `last_name`
- `middle_name`
- `date_of_birth`
- `email`
- `phone`

Passport (Trips column)

- `trips:passport_number`
- `trips:passport_country`
- `trips:passport_expiry_date`
- `trips:passport_issued_date`
- `trips:passport_place_of_birth`
- `trips:passport_issuing_authority`
- `trips:passport_type`
- `trips:passport_gender`

The third category is the **File upload** field with `routeTo: contact` set. That single setting is what lands the scan in the passport vault rather than the trip's general Files tab. Without it, the scan is just another attachment — useful, but not in the right encryption bucket.

Add a signature field at the bottom if your release of liability requires one — once signed, the submission locks (it can't be re-edited by the client) and stamps a typed name + signed-at timestamp + IP + user agent. ESIGN-compliant.

> **ADVISOR TIP**
>
> **There's a starter template.** Open **Forms → + New form** and pick the seeded *Passport collection* template — every field above is pre-built with the right `contactKey` and `routeTo` set. Customize the cover photo and intro copy, publish, share.

Sharing the form

From the published form's detail page, click **Share** and pick the trip. Two things happen automatically when you share a trip-attached form:

- The link expires in **14 days** by default — passports are time-sensitive, no reason to leave the link live forever. Override at mint time if a client needs more.
- Existing contact data on the trip's primary traveler is **prefilled** on the form. Identity slots and any passport columns we already have come pre-filled; the client edits what's stale and submits.

Send the link by Gmail (from Trips) or paste it into your usual client channel. The form lives on your branded portal host — `your-agency.urtravelpro.com` or your custom domain.

What happens on submission

When the client clicks **Submit**, four things happen in order:

1. **reCAPTCHA v3** scores the session. Bot-shaped submissions are rejected before they touch the database.
2. **Identity fields** (the Core slots) write through to Core, the platform-wide contact authority. Other UrTravelPro apps (Books, Marketing, Compass) see the update too.
3. **Passport columns** (the trips:* fields) write to the Trips contact extension. The columns are on a strict allowlist — typos or unrecognized passport keys are silently dropped so a misnamed field can't break the submission.
4. **The uploaded scan** runs through the encryption pipeline: ClamAV virus scan, then AES-256-GCM encryption with a per-agency key derived via HKDF-SHA256 from a platform master, then write to

encrypted blob storage. Filename + size are stored unencrypted (so the UI can list them); the bytes are not.

The scan lands in the contact's passport vault. Open the contact, go to the **Passport** tab, and you see the structured fields above plus a thumbnail of each scan with download / view actions.

Who can see passports

Anyone with agent access to your agency in Trips can view passport scans for contacts in that agency. On the client side, a portal user can view and download **only the scans attached to their own contact record** — never anyone else's. The portal enforces the contact-scoping at the route level: a request for another contact's scan returns 404, not a permission error.

Every portal-side access is audit-logged the same way agent-side access is, with the source clearly marked as the portal so staff can tell them apart on the access log.

ADVISOR TIP

Every view and download is logged. The **passport access log** records who looked at which scan, when, from which IP, with which browser. Agents see their own log on the contact's Access tab; full org logs are available for compliance review on request. This is intentional friction — passports deserve it.

Files, limits, and rejections

The passport upload field accepts **JPG, PNG, HEIC, WebP, and PDF** up to **10 MB** per file. The allowlist is narrower than the trip-files one (no Office docs, no plain text) because a passport scan is always a photo or a single-page PDF. If the client tries to upload a Word doc or a 20 MB scan, the submission fails with a clear error and they retry; nothing is stored until validation passes.

If our virus scanner is unreachable when the upload arrives (clamd down for maintenance), the pipeline **fails open** — the upload is accepted relying on the MIME allowlist + size cap as fallback. Encryption still happens. This is the same behavior across every attachment path in Trips.

Frequently asked

My client wants to send the passport by encrypted email instead.

No. The form pipeline is the supported path. "Encrypted email" usually means PGP or a vendor-portal link that's a worse audit posture than this one — we have no record on the trip, no audit log, no per-agency encryption envelope. Use the form.

Can two travelers on the same trip use the same form link?

Only the primary traveler's data is prefilled. For multi-traveler trips, the cleanest path is to mint a separate share link per traveler (each one trip-attached but with a different traveler resolved on submit), or build a multi-row form that captures all travelers in one pass. The latter is what the seeded multi-traveler template does.

I need to delete a passport scan — does it really get wiped?

Yes. Deleting from the contact's Passport tab writes a `delete` audit row and removes the encrypted blob from storage. The metadata row goes too. There's no undelete — the bytes are gone.

Does Core (the identity hub) see the passport number?

No. Passport columns live on Trips' contact extension — they don't round-trip through Core. Core sees only the identity fields (name, DOB, email, phone, anniversary). Passport columns are Trips-only and stay on this app.

Related

- Forms (intake, traveler info, passport)
- Trip files
- Contacts
- My file won't upload