



TRIPS

Trip files (encrypted attachments)

How the Files section of a trip works: uploading documents, the 25 MB limit and supported file types, the client-visible toggle that controls what your traveler sees in the portal, virus scanning, encryption, and the access log we keep for every file.

On this page

- [Where it lives](#)
- [Uploading a file](#)
- [Controlling what the client sees](#)
 - [Safe to share](#)
 - [Keep hidden](#)
- [Opening, downloading, deleting](#)
- [How your files are kept safe](#)
- [The access log](#)
- [Troubleshooting](#)
- [Related](#)

The Files section on a trip holds booking confirmations, supplier PDFs, signed waivers, ID photos — anything that belongs with the trip but doesn't fit a proposal or invoice. Uploads are scanned for malware, encrypted at rest, and audit-logged on every access.

Where it lives

Open any trip and click the **Attachments** tab. The Files block sits below Proposals & Itineraries and Invoices, with its own header reading *"Encrypted at rest. Visible to your agency team only."* Files are agent-only by default — clients see nothing on their portal until you mark a file as client-visible.

Uploading a file

Click **Upload file** in the Files header. Pick one file — the button flips to *"Uploading..."* while it's scanned, encrypted, and stored. Failures show a red banner above the list.

- **Maximum size: 25 MB.**
- **Allowed types:** PDFs; images (JPEG, PNG, HEIC, WebP, GIF); Office documents (Word, Excel, PowerPoint — old .doc/ .xls/ .ppt and modern XML); plain text; CSV.
- **One file per upload.**

ADVISOR TIP

No HTML, no zip files, no executables. The allowed file-type list is intentionally narrow — if your computer's file picker lets you pick a file but Trips rejects it on upload, the type isn't on the allowed list. Re-save it as a PDF and upload that instead.

Controlling what the client sees

Every file has a **client-visible** flag that defaults to **off** — agent view only until you say otherwise. To share, click the **eye** icon on the file's row. Crossed-out eye = hidden; open green eye = visible. Click again to revoke. The toggle is instant — no save button.

Safe to share

- Signed contracts.
- Final itinerary PDFs and confirmation pages.
- Boarding passes and supplier vouchers the traveler needs on the trip.

Keep hidden

- Supplier commission statements and net-rate sheets.
- Internal call notes saved as a PDF.
- Anything you wouldn't want the client reading over your shoulder.

IMPORTANT

Default is hidden — and that's by design. You have to opt each file in. There is no bulk "share all" button, and a re-upload starts fresh with the flag off again.

Opening, downloading, deleting

Every file row has three actions on the right:

- **Open.** For images and PDFs, an inline viewer pops up over the page. The viewer footer reads *"Encrypted in storage · every view is audit-logged."* For other types the viewer falls back to a download link.
- **Download.** Streams the decrypted bytes as an attachment. Cache-Control is set to no-store so the file doesn't linger in the browser cache.
- **Delete.** Opens a confirm dialog. On confirm the file is removed from the trip and from storage, and the delete is recorded in the access log. There's no undo from the UI; if you need a file back, open a support ticket quickly.

How your files are kept safe

Here's what happens between clicking **Upload file** and the file appearing in the list:

1. **Size and type check.** Anything over 25 MB or not on the supported-type list is rejected before it touches storage.

2. **Virus scan.** Every file is scanned for known viruses on upload. If anything's found, the file is rejected on the spot and never saved.
3. **Encryption.** The file is encrypted before being saved. Each agency has its own encryption key, so files from one agency can't be read using another agency's key.
4. **Private storage.** Encrypted files are kept in private storage with no public links. The only way to read one is through Trips, signed in, on a trip you have access to.
5. **Access logging.** Every upload, view, download, and delete is recorded with who did it and when.

ADVISOR TIP

What encryption means here. Encryption protects the files from anyone who isn't inside Trips — at the storage layer they're unreadable without the key. Inside Trips, any teammate with access to the trip can open the file normally. This isn't zero-knowledge storage; it's protection against the file being readable if it ever left our systems.

The access log

Every upload, view, download, and delete on a file is recorded — who did it, from which device, and when. Deleted files keep their history. There's no in-app log viewer yet; if you need a "who downloaded this" report for a specific file, open a support ticket and we'll pull it for you.

Troubleshooting

My upload says "Unsupported file type" but the file is a PDF.

The check is on the actual content type, not the extension. A .docx renamed to .pdf is still seen as Word and rejected. Re-save as a real PDF.

I got "failed our virus scan." Was something wrong with my computer?

Not necessarily — the scanner flagged the file before it was written. Macros in old Office documents and bundled installers in PDFs are common triggers. The bytes were discarded; nothing to clean up.

I shared a file with the client by accident. How do I un-share?

Click the eye icon on the row again. The flag flips back to hidden and the file disappears from the portal on the next page load. The file itself is not deleted.

Can the client see what else is on the file list?

No. The portal only shows files marked client-visible. Hidden files aren't listed at all — no filenames, no counts, no indication other files exist.

Related

- [The Trip page, top to bottom](#)
- [Trips — Getting Started](#)
- [What is a Trip?](#)
- [Passport collection \(encrypted contact attachments\)](#)