

How to use the case workspace

A preview for partner shops. One encrypted place for your customer cases: every tech opens the shop's shared cases, hands a case on or takes one from the queue, and saves recovery reports to it. Only your shop can read them: Family Security Playbook can't, and can't recover them without your passphrase or recovery kit.

Before you start

- It's a **preview** (beta), switched on for your organization by Family Security Playbook. Until it has had an outside security review, use it with made-up test cases, not real customers.
- Everyone uses **their own login** with a second step. The shared organization password can't open it. Each login is for one person: don't share it, your second step or your passphrase.
- It needs a current Chrome, Edge, Firefox or Safari. Open it from **Recovery reports** on your organization page: **Open the case workspace**.

Set it up (owner, once)

1. **Choose the shop passphrase.** At least 16 characters; a few unrelated words with spaces work well. The meter shows its strength, and it's checked against passwords known from breaches (only the first five characters of a fingerprint of it leave your browser). **Suggest five random words** makes one for you. There are no hints and no reset by email.
2. **Your recovery kit.** 24 words appear once. Write them down in order or press **Print the recovery kit**, and keep the page somewhere safe and offline. Anyone with them can read your shop's cases. We have no copy.

3. **Check your kit.** Type the three words it asks for, then press **Create the workspace**. Nothing is saved until this check passes.
4. Every owner on your organization's people list unlocks with the same shop passphrase, each signed in as themselves.

Add your techs (owner)

1. First invite them on your organization page (**Your account, People**) so they have their own login.
2. In the case workspace, open **People**, type their email and press **Add to the case workspace**.
3. They open the case workspace, press **Set up my key** and choose a passphrase of their own (the same rules). If they forget it, remove them and add them again.
4. The next time you unlock, your browser shares the **shop key** with them. Ask them to read you the **fingerprint** on their **Your key** tab and check it matches the one next to their name under People: that's how you know nobody swapped their key on the way.

Unlock and lock

- Enter your passphrase and press **Unlock**. It stays unlocked in that browser while you move between the workspace and the recovery report.
- It locks itself after **30 minutes** without use, when you sign out, or when you press **Lock now**. Locking in one tab locks every tab.
- Lost the shop passphrase? Press **Use the recovery kit instead**, type all 24 words, then set a new passphrase.

Open a case and save to it

1. On **Cases**, type the customer's name, choose who has it (you, another tech, or **The queue**) and press **Open a case**. The name is encrypted too: we see only a random id.
2. Open the recovery report, press **Open case** and choose the case. **Load** opens its latest saved job, or starts one with the customer's name filled in.
3. **Save to case** encrypts what's on screen and saves it as a new version. Nothing is overwritten: if someone saved a newer version after you opened yours, choose **Load theirs** or **Keep mine as a new version on top**.
4. If another tech is editing the same case, it opens read-only and says who and since when. Their lock lapses after 10 minutes without activity; an owner can press **Break the lock** sooner.
5. Under **History and files**, attach the customer's own record (the what-happened file their record page saves), a photo or a PDF, up to 6 MB, and download any saved file.

Hand a case on, or take one from the queue

1. In a case's row, choose a tech under **Hand to...** (or **The queue**), add a short note such as "waiting on customer callback", and press **Hand off**. The note is encrypted; the case's history shows it to your shop.
2. Anyone in the shop can hand on a shared case, or press **Take it** on a case in the queue. If two techs take the same case at once, one gets it and the other is told who.
3. A case can't be moved while someone else is editing it. Ask them to save first.
4. Press **Close the case** when the job is done (the tech who has it, or an owner). **Reopen** brings it back.

Follow-ups and colours

Every new case starts with your shop's follow-up dates, counted from the day the case starts. These are the defaults; an owner can change them for the whole shop under **Your account, Follow-up defaults** (and press **Reset to default** to go back):

Follow-up	Due after the case starts	Time to do
Change remaining passwords	7 days	1 day
Check bank and card statements	14 days	1 day
Confirm credit freeze or fraud alert	30 days	1 day
Second statement review	60 days	1 day
Close-out call	90 days	1 day

The **warning buffer** is **3 days** by default. Each follow-up gets a colour, worked out in your browser from the case's own (encrypted) dates:

- **Green** (on track): more days left than its time to do plus the warning buffer.
- **Yellow** (due soon): within its time to do plus the warning buffer.
- **Red**: fewer days left than its time to do, and not started. Tick **Started** and it shows yellow instead.
- **Black** (past due): its due date has passed and it isn't marked **Done**.

A case's colour is its worst follow-up. Open a case's **History and files** to change its dates, its time to do, tick **Started** or **Done**, add a follow-up, or tick the services you offered, then press **Save follow-ups**.

The dashboard and the calendar

- **Dashboard:** every open case, who has it, its next follow-up and its colour, worst first. Owners see the whole shop and **Who's behind:** each tech's open cases by colour. Filter by tech or colour. Techs see their own cases, with the same colours.
- **Calendar:** every follow-up not done yet, by month or as a list. Filter by tech, or tick **My calendar** for yours.
- **Download for my calendar app (.ics)** makes a calendar file in your browser, with the customers' names in it. Add it to your own calendar, not a shared one.

Your services

- An owner lists the shop's own services under **Your account, Your services:** a name, a short description, the price as you'd say it, and what it uses (the incident record, the recovery report, the family playbook, the follow-up checklist and so on).
- They show as next steps on your free tools page and on the customer's record sheet, with your phone number, and in the recovery report, where a tech ticks what was offered. Staff see them but can't change them.

Private cases and removing someone (owner)

1. Cases are **shared** with the whole shop by default. Press **Make private to** a tech and only that tech and owners can open it; it gets a new key. **Share with the shop** undoes it. Only owners can move a private case.
2. Press **Remove** under People (or remove them from your organization's people list) and their access stops at once. Your shop gets a new shop key, their cases go to the queue, and each shared case's files get a new key the next time someone saves.

Seats and your plan

- The case workspace comes with every paid plan. Its **seats** are your plan's techs: **Shop 5, Team 20, Unlimited** any number; plans without a tech limit have no seat limit. Every owner and every person added to the workspace (set up or not) takes a seat. The People tab shows **N of M seats used**.
- When every seat is in use, nobody new can be added: remove someone, or move up a plan. Moving up adds seats at once; nothing is re-encrypted.
- If your shop has more people than seats (after moving to a smaller plan), nothing is removed. Nobody new can be added, and after **14 days** the most recently added extra techs become **read-only** (they can open and download, not save) until someone is removed or the plan has more seats. Owners and the backup owner are never made read-only.
- On a plan with only one seat, there's no one to be a backup owner: a second seat is what makes a backup owner possible.

If your plan ends

Nothing is deleted the day a plan ends. This is the timeline:

1. **The plan ends:** the workspace becomes **read-only** for **30 days**. Everyone can still open and download cases; nobody can save, open new cases or add people. Removing someone still works.
2. **30 days after:** the workspace **closes**. Nobody can open it. Everything in it is kept.
3. **90 days after it closes:** everything in it is **deleted for good:** every case, file and note. Nobody can bring it back, Family Security Playbook included.

Your organization's owners and contact address get an email **30, 7 and 1 day** before the deletion, with the date (never anything from a case). **Renewing at any time before**

the deletion opens everything again, exactly as it was. If you need more time, reply to one of those emails: Family Security Playbook can hold it.

A backup owner (owner)

1. If your shop has more than one person, name a **backup owner**: an active tech who can unlock the workspace as owner with their own passphrase, and take over if you can't. On **People**, under **Backup owner**, choose the tech, type your shop passphrase and press **Make them the backup owner**. Your browser wraps the shop's master key for them, made with your owner key, so nobody else can slip them a key of their own.
2. The backup owner unlocks with their own passphrase as usual; the page says **Unlocked in this browser, as the backup owner**. They can do what an owner does, except change the shop passphrase.
3. Changing or removing the backup owner: they held the master key, so make a new one afterwards (**Make a new master key** on People). The page reminds you.

Handing the workspace to a new owner

1. If you're leaving the shop, hand the workspace on while you can. On **People**, under **Hand the workspace to a new owner**, choose an active tech (or another owner), choose whether you stay on the people list as staff or leave it, type your shop passphrase and press **Start the handoff**.
2. The new owner opens the case workspace within **7 days** and presses **Accept and become the owner**. They choose a new shop passphrase, print the new recovery kit and check three of its words. Their browser makes a new master key, a new shop key and a new owner key, and re-wraps every case's keys.
3. Then your passphrase and recovery kit stop working, they become the owner on your organization's people list, you become staff (or leave the list), and everyone involved gets an email. Your cases go to the queue for them to hand out. Techs

keep their own keys: the first time each one unlocks, their browser checks a link from the old owner key to the new one and updates their key. Every case gets a new key the next time it's saved.

4. One handoff at a time. **Cancel the handoff** stops it; the person it's for can **Decline**. Any other owners need the new shop passphrase from the new owner.
5. After a change of owner, contact Family Security Playbook at jeff@jcady.org to update the billing contact on your plan; we update it in Stripe for you.

If the owner has gone

- **With a backup owner:** they unlock, open **People** and press **Take over as owner**, with a new shop passphrase and recovery kit. It happens at once: they become the owner, every other owner becomes staff (the new owner can make them owners again on the organization page), everyone is emailed, and the audit log records it. Then contact us to update the billing contact, as above.
- **With the recovery kit:** the kit is for owners. Another owner on your organization's people list unlocks with **Use the recovery kit instead** and sets a new passphrase, takes the owner who has gone off the people list, then presses **Make a new master key** on People. If whoever holds the kit isn't an owner, an owner makes them one first; if no owner is left, Family Security Playbook can make them the owner after checking who you are, and then they unlock with the kit.
- **With neither:** nobody can open the cases, Family Security Playbook included: they're encrypted with keys only your shop had. Family Security Playbook can move the account and billing to a new owner after checking who you are, but the cases stay locked. They're kept, not deleted, unless you ask us in writing to delete them so you can start a new workspace.

Bring in recovery jobs saved before the workspace

1. Before the workspace, the recovery report kept each job on your computer as a job file (**Recovery-job-....json**, from **Save job file**). On **Cases**, under **Import saved recovery jobs**, choose one or many of those files.
2. Choose what happens when a customer already has a case: **Add it to their case as a new version**, **Open a separate case**, or **Skip the file**. A job that's already saved exactly is always skipped.
3. Press **Import**. Each file is encrypted in your browser before it's saved, and you get a line for each one: a new case, added to a case, skipped, or why it couldn't be imported. The files on your computer are only read, never changed or deleted: delete them yourself once you've checked the workspace has them.

What Family Security Playbook can and can't see

- **Can see:** who is in your workspace, the random id of each case, whether it's shared or private, who has it, who handed it to whom and when, how many versions there are, their sizes and times and who saved them, who is editing, and the audit log.
- **Can't see:** customer names, anything in your files, handoff notes, your passphrases, your recovery words, or any key that opens them.
- **Can see too:** who the backup owner is, any owner handoff waiting, and when your plan's seats or end date change what the workspace allows.
- The **Audit log** (owners) shows who added, set up keys, opened, handed on, took, moved, made private, removed, re-keyed, failed to unlock or broke a lock, named a backup owner, handed on or took over the workspace, and made a new master key. It never holds content.

If something doesn't work

- **"The Argon2id library couldn't be loaded"**: the page loads its key-derivation library from cdn.jsdelivr.net. Reload, and check your network doesn't block it. It never unlocks with a weaker method instead.
- **"You don't have your shop's key yet"**: your owner shares it the next time they unlock.
- **"The key Family Security Playbook shows for ... isn't the one you shared cases with before"**: nothing was shared. If that person reset their key, remove and add them again; otherwise email us.
- **"The case workspace needs your own login"**: sign out of the shared password and sign in with your own login.
- **"Your shop's owner key changed, and the change couldn't be confirmed"**: nothing was opened. Ask your owner to remove and add you again, and email us.
- **"Your plan has lapsed, so the case workspace is read-only" or "...closed"**: see **If your plan ends** above. Renewing opens it again.

Stuck?

Email jeff@jcady.org or call (520) 223-9878 ext. 800, and say which page you're on. We'll never ask for a password, a code from your phone, or a card number.