Give an Auditor Read-Only Access

Last Modified on 09/04/2026 11:10 am EDT

An auditor needs to look, not touch. Add them as a user for the length of the audit, then take the access back when it's over.

Introduction

Most auditors would rather browse your files themselves than wait on a folder of downloads, and plenty of offices are happy to let them. We usually discourage giving account access to outside contacts — auditors are the exception.

The setup is a temporary user with as little granted to it as possible, put on exactly the transactions the audit covers, and switched off the day it ends. It's the closest thing Pipeline has to a read-only account, and knowing exactly how close it gets is part of doing this well.

When to Use This

- Your state auditor wants to look at the files themselves rather than take a stack of downloads.
- The auditor asked for more transactions than you can download in a day.
- The audit covers dual-sided deals and the auditor needs to see both sides of each one.
- The auditor needs to see when each document was uploaded and when your broker reviewed it.
- The audit is finished and you need the access gone.

Why This Is as Close to Read-Only as Pipeline Gets

Read-only is the right instinct and the wrong expectation. There is no view-only permission level in Pipeline — no box you check that turns someone into a spectator. Strip every permission from a user and they still aren't inert: an agent who's been added to a transaction can edit certain fields on it while it's Active, Listing, or Pending, and can still agent-check tasks, download and email documents, and add notes.

So build read-only out of restraint instead of out of a setting. Grant the auditor nothing, put them only on the transactions the audit actually covers, and end the access when the audit does. That combination is what makes this safe — not a permission, but a small blast radius and a short clock.

1. Decide Whether the Auditor Needs to Be in Pipeline at All

Live access is one of two good answers, and it isn't automatically the right one. If the audit covers a handful of transactions, downloading those files and handing them over is simpler, needs no account, and ends nothing that has to be undone. Ask your auditor which they'd prefer — many will tell you plainly.

Choose live access when the list is long, when the auditor wants to browse rather than receive, or when you'd otherwise be fighting the daily download limit.

An auditor asked for six transactions. Your account holds six hundred. Only the six need to leave.

See Give an Auditor What They Need, Not Your Whole Account

2. Add the Auditor as a User

The auditor gets their own profile, like anyone else who logs in. Use the email address they give you — their access ties to it, and so does the record of everything they opened.

Add the agents and staff on your team so each person can log in and work in Pipeline under their own account.

See Adding a User

3. Grant Them Nothing

Work down the permission list and leave all of it unchecked. An auditor is reading, so there is no permission they need — every box you check is reach you'd have to justify later, and none of them buy you anything the audit requires.

Leave **View all transactions for this location** clear in particular. It's the tempting one, because it saves you the work of the next step, and it's the one that opens your entire office to an outsider.

Decide exactly what each person can see and do in Pipeline, location by location.

See User Permissions

> Granting nothing gets you close to read-only, not all the way. An auditor added to a transaction can still edit some of its fields while it's in an Active, Listing, or Pending status, and can agent-check tasks, download or email documents, and add notes. Keep the access short and scoped, and if a file absolutely cannot be touched, hand that one over as a download instead.

4. Put Them on the Transactions the Audit Covers

With no permissions granted, the auditor sees a transaction only when you add them to it — which is exactly the control you want. Add them to each transaction in the audit as an agent, and they can open those files and nothing else in your account.

Put the right agents on each side of a transaction so Pipeline credits the deal correctly and everyone can open the file and work it.

See Assign Agents

> On a dual-sided deal, add the auditor as **both** the listing and the selling agent. Each side carries its own documents, and an auditor added to only one side quietly misses half the file.

> If the audit genuinely covers everything and adding them file by file is unrealistic, granting **View all transactions for this location** is the alternative — accepting that it makes the auditor a location admin

> there and shows them every deal in that office.
>
> A location admin runs the day-to-day inside the locations they're given — reviewing docs, managing checklists, and seeing every transaction there.
>
> See Admin / Staff (Location Admin)

5. Deactivate the Auditor When the Audit Is Over

This is the step that makes the whole approach defensible, and it's the one that gets forgotten — an auditor profile left live is an outside party with a standing login to your brokerage. Do it the day the audit closes.

Deactivating doesn't erase anything. Their profile and every trace of what they did stays in your history; they can't log in anymore. If a follow-up question arrives next quarter, you can bring the same profile back.

Turn off a user's access when they leave — without losing any of the work tied to their name.

See User Deactivation