Setting Up an Ethical Wall

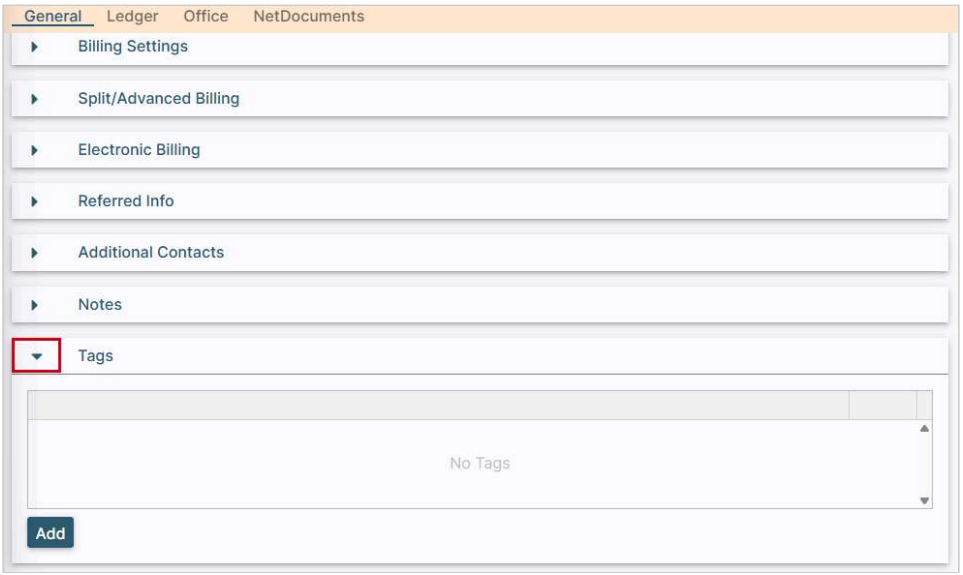
Modified on Tue, 20 May at 4:17 PM

To avoid conflicts of interest, files can be restricted so certain users won't have access to them. This article walks through the three parts to this process:

- Creating the tag.
- Creating a restricted user group.
- Setting access permission for a file.

Part 1: Creating the tag:

1. In Legal Accounting, go to **Contacts > File Manager**.
2. Expand the **Tags** section.

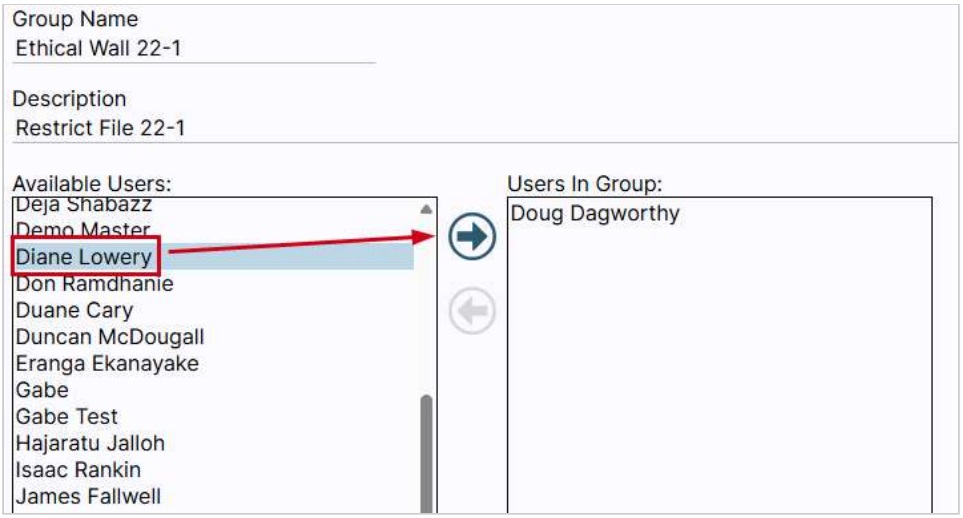


3. Click **Add**. The New Tag window appears.
4. Enter the name of the tag in the field (e.g., *Ethical Wall 22-1*) and click **OK**.
5. Click **Save** at the bottom of the page.

Part 2: Creating a restricted user group:

1. In Legal Accounting, click the **Administrator Settings** icon and go to **Users** > **Groups**.
2. Click **Add**. The Group Editor page appears.
3. Enter a **Group Name** and **Description**.

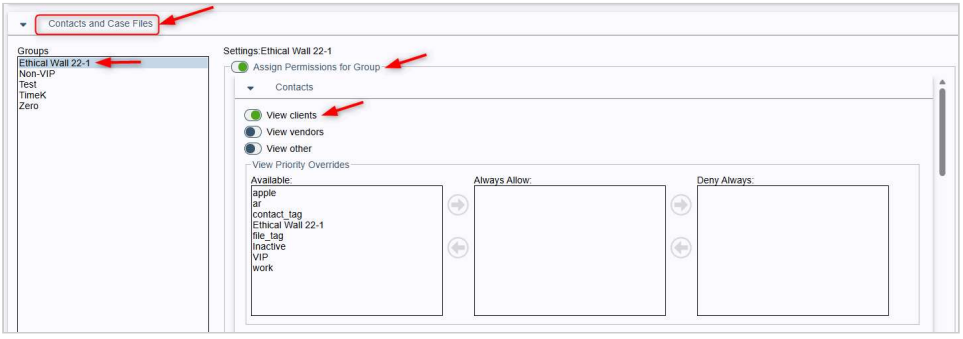
4. Select a user who should not have access to the file in the **Available Users** lists and click the right arrow to add them to the **Users in Group** list.



5. Click **Submit** to save your changes.

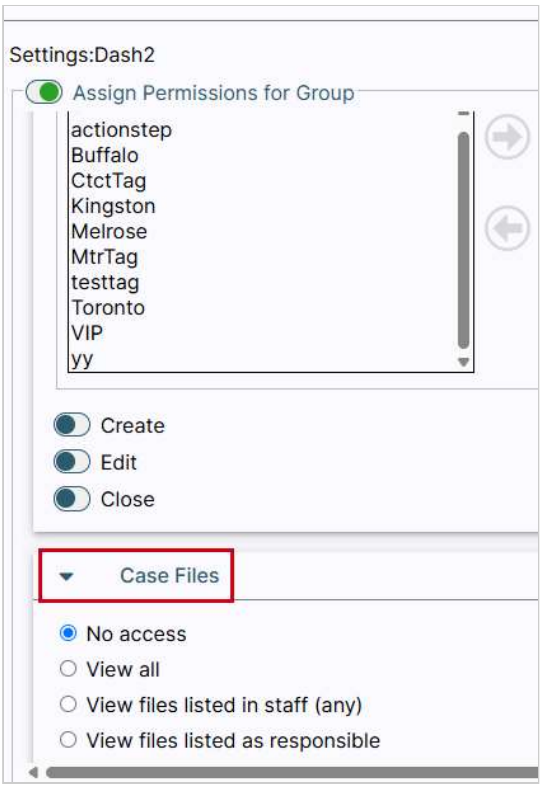
Part 3: Setting access permission for a file:

1. In Legal Accounting, click the **Administrator Settings** icon and go to **Users** > **Security**.
2. Expand the **Contact and Case Files** section.
3. In the **Groups** list, select the group that you created in Part 2.
4. Toggle **Assign Permissions for Group** so that it's enabled.
5. Click the arrow to expand the **Contacts** section.
6. Toggle **View clients** so that it's enabled.

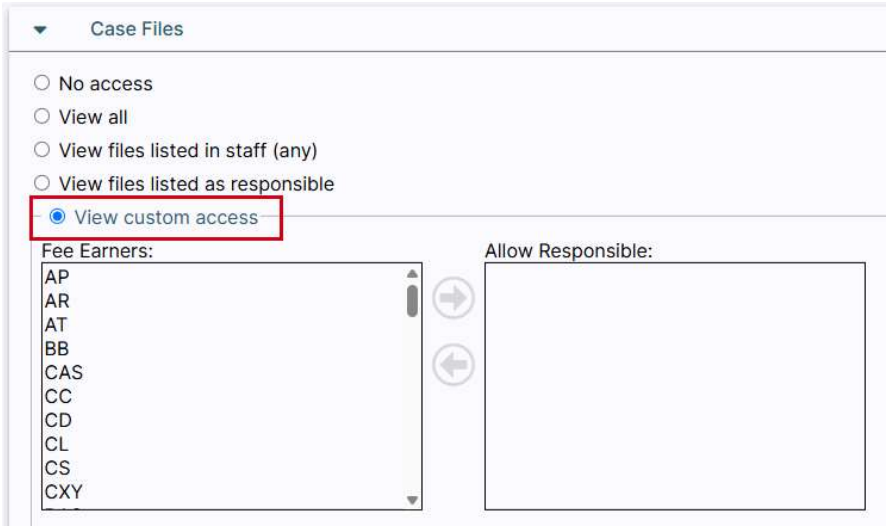


> **NOTE:** If you want the wall to be applied at client level, you can move the tag under **Contacts** from **Available** to **Deny Always**.

7. In this same section, click the arrow to expand the **Case Files** section.



8. Select **View custom access**.



9. Scroll down to view the **Available** section.
10. Select the tag you created in Part 2 and, using the arrows, move it from the **Available** list to to the **Deny Always** list.
11. Click **Save** at the bottom of the page.

> **NOTES:**
> - The steps outlined above assume the user is already part of another group that has access to File Manager.
> - If the user is an Admin and/or Power User, the ethical wall will not work since both of those groups are meant to have access to all files.
> - There are some cases that users are unable to access all other files that they

are supposed as an effect of other security restrictions in place. If this happens, move **Fee Earners** and **Areas of Practice** to the **Allow** list.