

20.1 Set Permissions on Folders in the User Dashboard



Folders are the way your files are organized on the User Dashboard.

- Folder-level permissions can be used to allow or restrict access to a single folder and all of its contents.
- Folder-level permissions can only be set on the folders in [My Files](#).



[My Files](#) is your private store.

- Your administrator must first allow you to set folder-level permissions.
- If your administrator has granted you the ability to set permissions, you will see a [Manage Security](#) button when opening a folder in the right-side pane of User Dashboard.
- If your administrator has NOT granted you the ability to set permissions, you can [Share the folder](#) to grant or restrict access.

Securing a folder

- Setting folder-level permissions is more commonly used to secure one entire folder with access to only a small number of users
- The permissions granted are applied to all of the files inside the folder and cannot be set for just a specific file inside the folder
- You can allow or restrict sharing

Sharing a folder

- Sharing a folder is more about allowing a larger number of users to easily access your folders
- Access can be granted to anyone with the Share URL
- Sharing can also be used to provide access to a specific single file



When a folder contains more folders inside it, the top folder is the parent and the sub-folders are children.

Inherited permissions means that a parent's permissions are used for all the sub-folders too.

In general, a sub-**folder** can be in one of the following states:

- The child, or sub-folder has all of the same **permissions** as its parent folder
- The child, or sub-**folder** has all of the same **permissions** as its parent folder, plus additional **permissions**
- The child, or sub-**folder** has all of the same permissions as its parent, minus additional **permissions**
- **The child, or sub-folder's permissions are not connected in any way to the parent folder and the sub-folder retains a separate set of permissions**

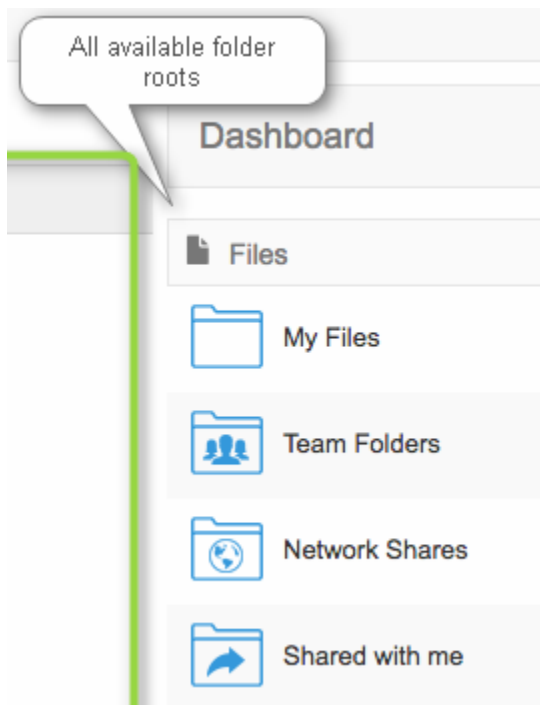
When setting folder-level permissions in FileCloud, you have the following options:

Option	Description
 Inherit Permissions	Permissions set in this folder are exactly the same as the top level folder's permissions
 Don't Inherit Permissions	Permissions set in this folder don't inherit from any top level folder's permissions and are specific to only this folder

When you set folder-level permissions, you can select one or more of the following options:

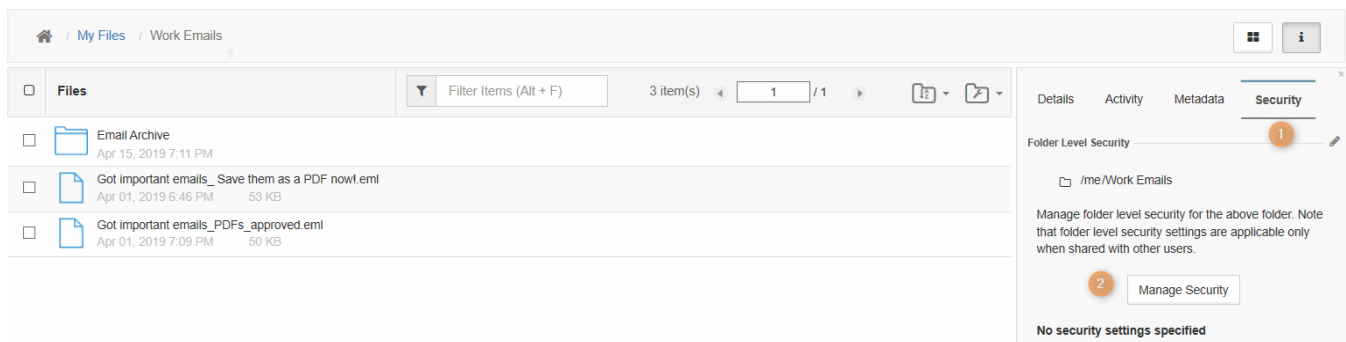
Read	Write	Delete	Share	Manage
<ul style="list-style-type: none">• Allows downloading• Allows previewing	<ul style="list-style-type: none">• Allows uploading and modifying• Allows creating files and folders• Allows renaming	Allows deleting	Allows sharing	Allows managing folder-level permissions

How do I secure access to my folders?



To set folder-level permissions:

1. Open a browser and log in to the [User Portal](#).
2. On the Home page of the User dashboard, click [My Files](#).
3. On the [My Files](#) window, click a folder.



4. On the right-side of the folder details window, click the [Security](#) tab, and then click the [Manage Security](#) button.

Manage Folder Level Security

×

Folder: /me/Work Emails

Security

Check Access

Permissions

Inherit Parent Folder Security:

☒ Inherit
☐ Don't Inherit

User

Group

Add User

User	Read	Write	Delete	Share	Manage
------	------	-------	--------	-------	--------

×

Close

5. In the Manage Folder Level Security window, decide if you want all sub-folders to have the same permissions by selecting either Inherit or Don't Inherit.
6. In the Manage Folder Level Security window, click Add User.

Search Users

×

Account or Email

Q Search

7. In the Search Users window, type in the email address of the user you want to allow access to your folder.
8. From the list of users, select the one you want to grant access.

Manage Folder Level Security

Folder:

/sat1/Class 3

Security

Check Access

Permissions

Inherit Parent Folder Security:

☒ Inherit
 ☐ Don't Inherit

User

Group

Add User

User	Read	Write	Delete	Share	Manage	
jane@codelathe.com						
joe@codelathe.com						

⏪

⏩

Page

1

of 1

⏪

⏩

9. By default, all permissions are granted. To restrict a permission, you must first restrict some of the previous permissions.

Permissions must be set in the following order:

Read	<ol style="list-style-type: none"> 1. Restrict MANAGE 2. Restrict SHARE 3. Restrict DELETE 4. Restrict WRITE
Write	<ol style="list-style-type: none"> 1. Restrict MANAGE 2. Restrict SHARE 3. Restrict DELETE
Delete	<ol style="list-style-type: none"> 1. Restrict MANAGE
Share	<ol style="list-style-type: none"> 1. Restrict MANAGE
Manage	Must be restricted first before anything else

10. To restrict any permissions, first restrict Manage by clicking its green check mark.

11. Now you can deny the permission to Delete or Share permissions by clicking their green check marks.

12. To restrict the Write permission, make sure the Manage, Delete, and Share permissions are first restricted.
13. To restrict the Read permission, make sure the Manage, Delete, Share, and Write permissions are first restricted.
14. To save your changes, click Close.