Create a Retention Policy

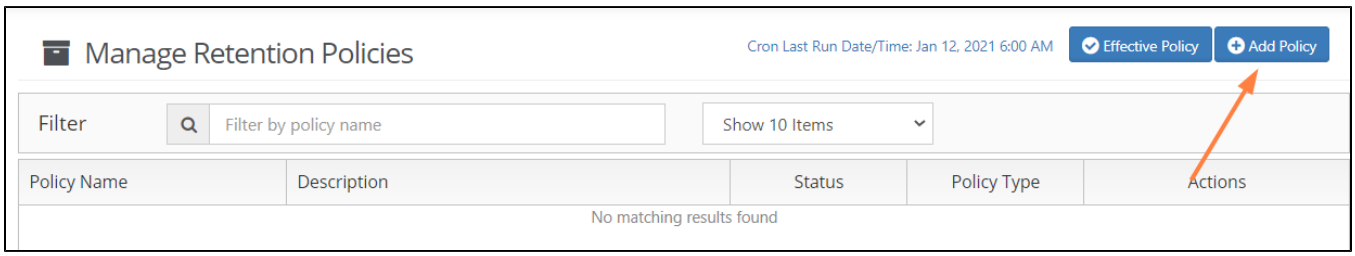
A Retention policy allows an organization to identify specific content that is required to be stored for a specific period of time before it can be accessed. During the retention period, the content cannot be deleted.

⚠ Retention policies cannot be removed once applied unless an expiration fixed date is set.

The following table identifies what actions are blocked for a retention policy.

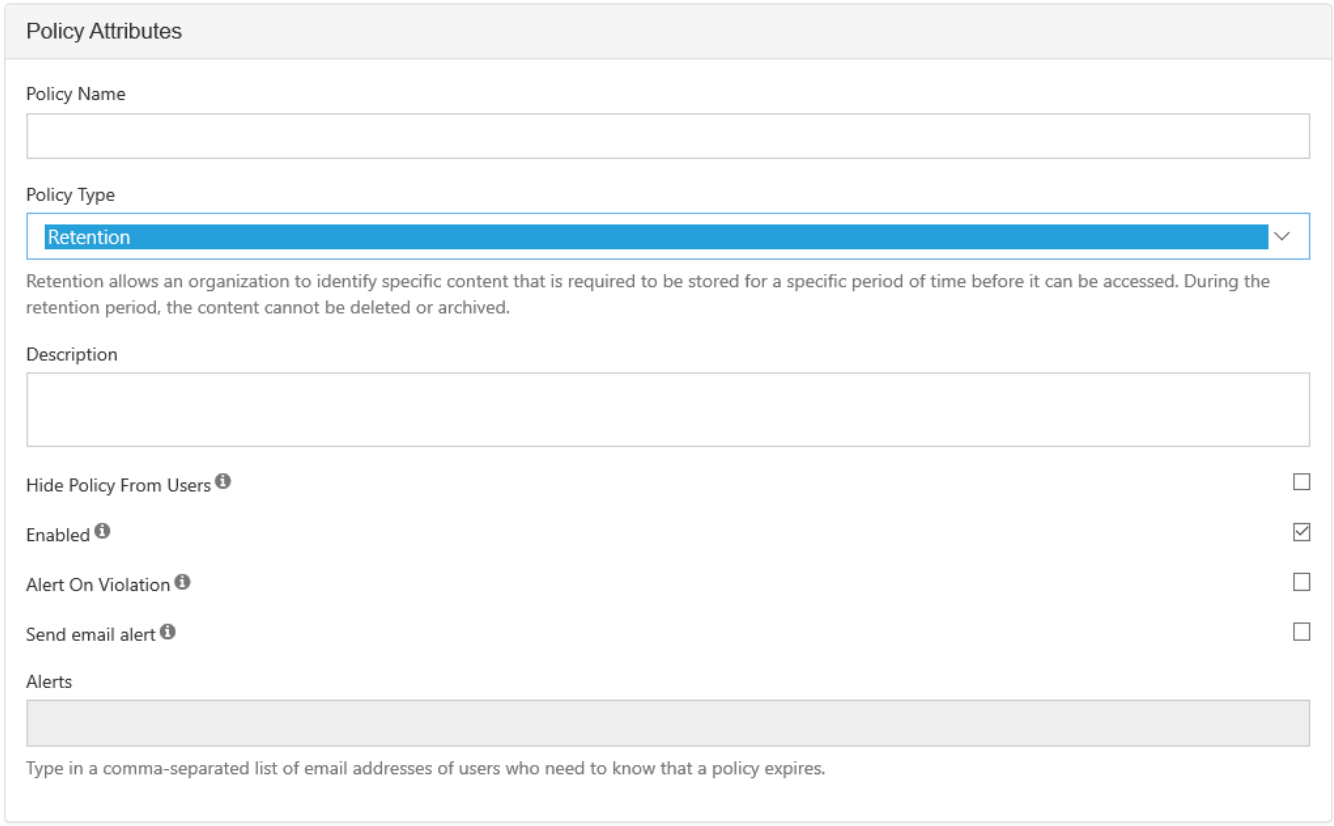
Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Retention	NO	NO	NO	NO	YES	• Time Period • Fixed Date • Indefinite	• Delete • No Action

Creating the Policy



To create a Retention Policy:

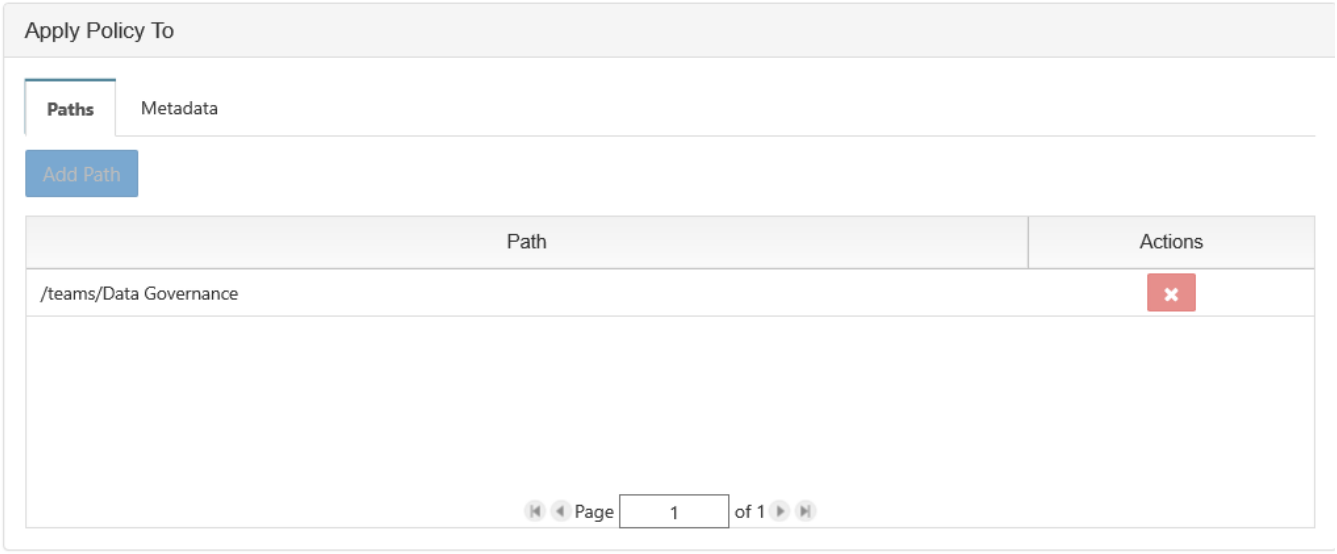
1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Retention*.
3. On the *Manage Retention Policies* screen, click the *Add Policy* button.



Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select *Retention*
Description	• Required • A string of characters, letters, and numbers that provide details about why the policy is necessary • This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠️ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.

Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

The Path and the Metadata tabs allow you to define the conditions that specify how the policy will be applied in the system.



Add a Path

Add Path allows you to define a folder that a policy will apply to AS WELL AS all the files and sub-folders it contains

What you CAN do in the Path field	What you CANNOT do in the Path field
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path

- The full path must exist before the policy will be enforced

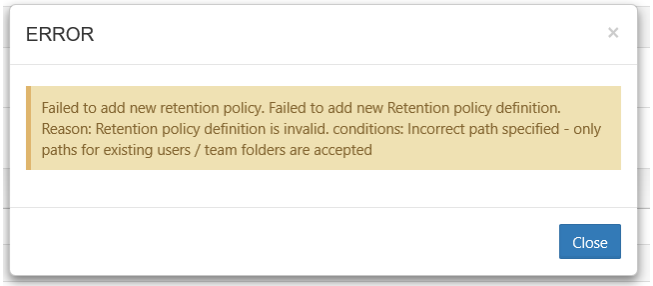
When creating the policy the full path doesn't have to exist, however.

At a minimum:

- The first component of the path has to already exist /username/
- This means that the username or team folder has to already exist before you can save the policy

- You CANNOT specify a path that does not exist

This will prevent you from saving the policy



Configure Metadata

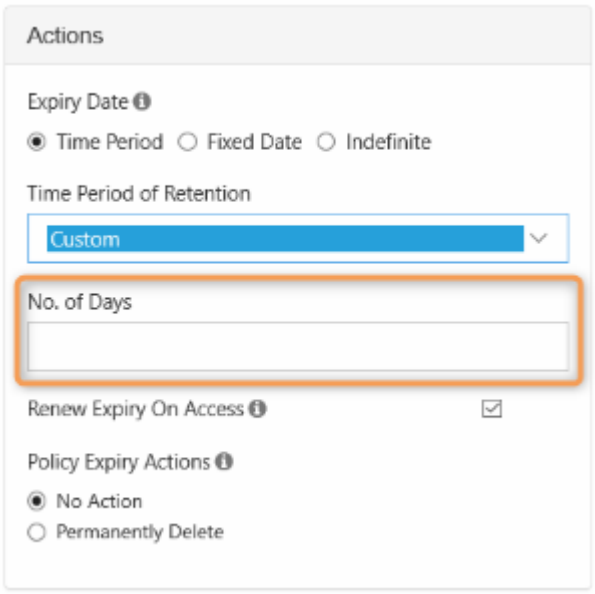
Data that provides additional information about files and folders is called **Metadata.**

- To specify files and folders that this policy should apply to, you can use metadata sets, attributes, and tags.
- You can use metadata to apply a policy to all files that meet the metadata conditions even if they are not in the same folder.

You can select metadata from the following existing attributes or sets:

- Default sets = provided with FileCloud Server and applies to every folder and cannot be modified Tell me more about the Default set
- Built-In sets = provided with FileCloud Server and includes the Document Life Cycle and Image metadata sets, NEW for 19.1 Tell me more about these new sets
- Custom attributes and sets = created by administrators in the Admin Portal

When you configure a Retention policy's expiration actions, all of the options are available.



To set a Time Period:

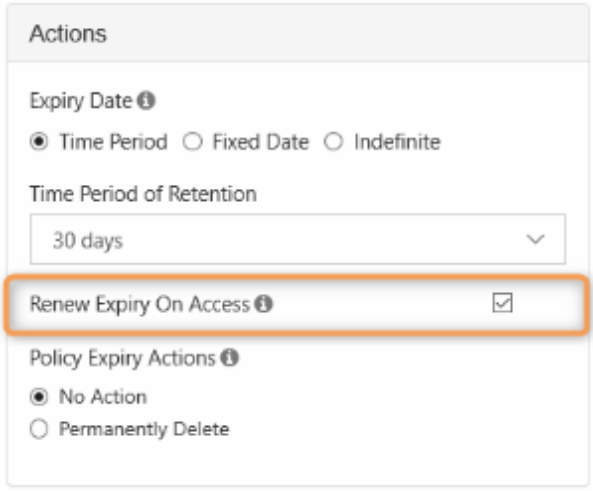
1. In the *Actions* section, click *Time Period*.
2. In Time Period of Retention, click the down arrow.
3. From the list, you can select a built-in option:
   a. *30 days*
   b. *60 days*
   c. *1year*
   d. *2years*
4. From the list, you can also select *Custom*.
   a. In No. of days, type in a whole number greater than 0.

To set a fixed date:

1. In the *Actions* section, click *Fixed Date*.
2. Click in the *Expiry Date* text box.
3. A calendar will be shown with the current month.
4. Select a date from the calendar.

To set an Indefinite date:

1. In the *Actions* section, click *Indefinite*.



Renew Expiry on Access: this is a set number of days or years that is used to calculate when the policy expires based on the last access date.

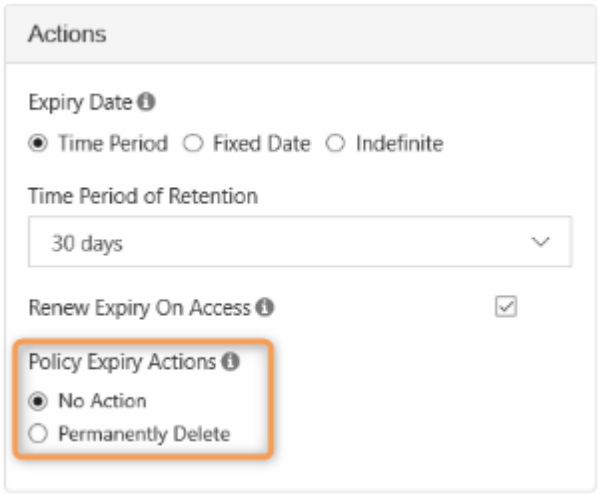
⚠️ Available only if the *Time Period* option is set, and selected by default.

Renew Expiry on Access	Expiration Date
For example, if on March 2, 2019, for an X-ray, you set expiry to: • Time Period = 60 days • Renew on Access = selected	Then the policy will expire on May 2, 2019 UNLESS: • If a doctor previews the file before May 2, say on May 1, 2019 Then the 60-day time period will be reset to July 1, 2019.

💡 The ACTUAL date is reset by a user every time they access the file.

To set Renew Expiry On Access:

1. In the *Actions* section, next to Renew Expiry on Access, make sure the checkbox is selected.



When a Retention policy expires, you can configure it to allow access to or delete the attached files and folders.

To set Policy Expiry Actions:

1. In Policy Expiry Actions, select either:
   a. *No Action* : Allow users to access the files again and delete them if they want
   b. *Permanently Delete* : Delete all the files that have this policy attached from the system, without retaining them in the Trash bin