

# FileCloud Online

## 23.253

# Governance Setup

17 December, 2025

# Table of Contents

Governance in FileCloud .....	1
Metadata, Smart Classification, and Smart DLP .....	2
Compliance .....	2
Retention Policies .....	2
Smart Classification .....	2
Smart Classification Classic.....	2
Smart DLP .....	2
(23.253) Import/Export DLP, CCE, and Metadata Settings.....	2
Example: Setting Up a Retention Policy to meet HIPAA Requirements .....	2
Monitor Retention and DLP: The Governance Dashboard .....	2
Secure Web Viewer for DRM.....	2
Metadata, Smart Classification, and Smart DLP .....	3
Metadata .....	3
Smart Classification .....	4
Smart DLP .....	4
Compliance .....	6
Compliance Center .....	6
Guide to HIPAA Rules in the Compliance Center .....	18
Guide to ITAR Rules in the Compliance Center .....	26
Guide to GDPR Rules in the Compliance Center .....	29
Guide to NIST Rules in the Compliance Center .....	33
Guide to PDPL Rules in the Compliance Center .....	39
FileCloud Web Accessibility (VPAT) Practices .....	43
Retention Policies .....	47
Are You Seeing This Screen? .....	47
Create a Type of Retention Policy .....	48
How Retention Policies Work.....	77
Applying a Retention Policy to All Files .....	97
Smart Classification .....	103

Smart Classification in FileCloud .....	103
Running content classification rules .....	105
Setting Up Smart Classification.....	106
Adding Smart Classification Regex Patterns.....	106
Creating Smart Classification Regex Pattern Groups .....	113
Creating a Smart Classification Rule.....	126
Running Smart Classification Rules .....	138
Testing a Smart Classification Rule .....	141
Guide to Classifiers .....	144
Editing a Smart Classification Rule .....	152
Deleting a Smart Classification Rule .....	154
Smart Classification Examples.....	154
Smart Classification Classic.....	164
Overview.....	164
Before You Start.....	165
Get Started with CCE .....	166
CCE Crawler .....	166
More Information:.....	167
Creating and Managing Content Classification Engine Rules .....	167
CCE Rule Examples .....	170
Creating a Pattern.....	176
Creating a Pattern Group.....	179
More CCE Rule Examples.....	181
Using ICAP DLP with CCE .....	186
Smart DLP .....	188
Overview.....	188
Creating Data Leak Prevention Rules .....	188
Example Rules .....	198
Rule Expressions .....	206
How to secure documents with Smart DLP & CCE.....	213
Troubleshooting DLP .....	227
Example: Setting Up a Retention Policy to meet HIPAA Requirements .....	229

Step 1: Enable the HIPAA retention policies rules in the Compliance Center. ....	229
Step 2: Create a metadata attribute to tag files with ePHI data .....	232
Step 3: Create a a pattern group that identifies file content as ePHI.....	236
Step 4: Set up a Smart Classification rule to locate and tag ePHI files .....	243
Step 5: Set up a 6 year retention policy .....	248
Step 6: Choose the retention policy in the Compliance Center .....	253
Monitor Retention and DLP: The Governance Dashboard .....	258
Secure Web Viewer for DRM.....	259
The Secure Web Viewer option.....	260

# Governance in FileCloud



DLP is only available in some versions of FileCloud Online.

Data governance encompasses the aspects of data management that ensure that data is valid, secure, accessible or inaccessible in the right circumstances, and compliant with regulations. FileCloud's data governance features include:

- **Smart classification** - Tags files with specific types of information, such as personally identifiable information (PII).
- **Smart DLP** - Prevents data leaks by controlling which files are uploaded, downloaded, and shared according to conditions you create. For example, download could be prevented in certain domains or file paths.
- **Retention policies** - Require certain files to be maintained in your system for specified time periods.
- **Compliance center** - Helps you make your system compliant and indicates where it is not compliant.
- **DRM** - Secures files by requiring that they be viewed through a secure viewer that can block downloading and printing or hide portions of content. See DRM for exporting secure documents.

To set up governance in your system, see the topics in this section:

## Metadata, Smart Classification, and Smart DLP

### Compliance

#### Retention Policies

#### Smart Classification

##### Smart Classification Classic

##### Smart DLP

#### (23.253) Import/Export DLP, CCE, and Metadata Settings

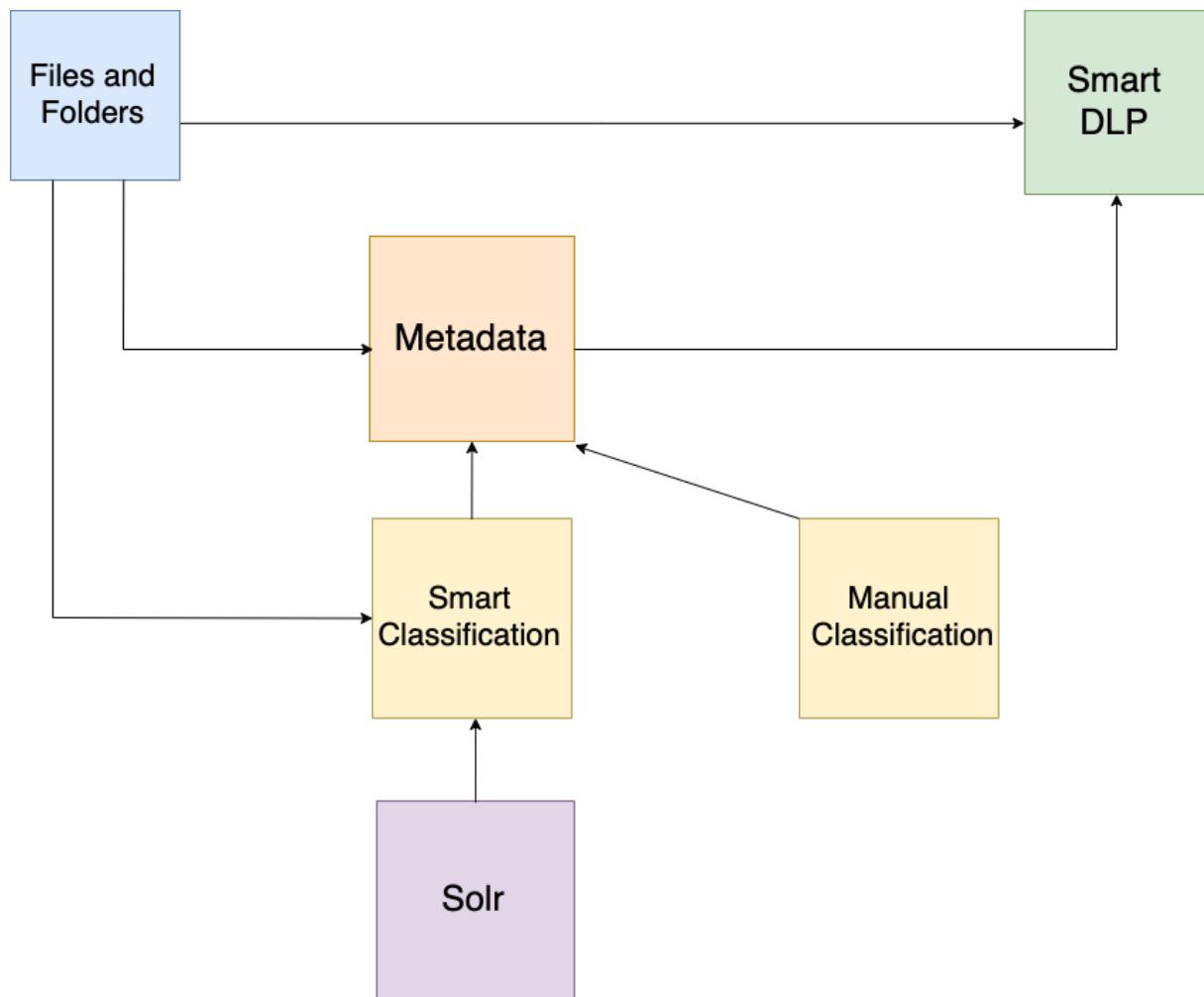
##### Example: Setting Up a Retention Policy to meet HIPAA Requirements

##### Monitor Retention and DLP: The Governance Dashboard

##### Secure Web Viewer for DRM

# Metadata, Smart Classification, and Smart DLP

Metadata, Smart Classification, and Smart DLP are all part of FileCloud's advanced security technology. However, there are distinct differences between these features that affect how they are used and how they interact with one another.



## Metadata

**Metadata** – information about files and folders – identifies what the file or folder contains and how much protection it should receive.

Examples of metadata include:

- Phone numbers
- Credit card numbers
- PII security priority

- EXIF image data
- Upload date
- Boolean values

Metadata can be created, edited, and applied with **no dependencies**.

Learn more about metadata.

## Smart Classification

The **Smart Content Classification Engine (CCE)** further refines how files are organized and tracked by FileCloud. With one or more sets of initial metadata, classification can **automatically** add or alter metadata. Examples of smart content classification rules include:

- For files containing nine-digit credit card numbers, mark PII security level as "HIGH"
- For images larger than 15MB, add the text attribute "PRINT PROOFS"
- For PDFs with the metadata text attribute "Holiday vacation requests" uploaded after October 1st, add the text attribute "HOLIDAY REQUESTS" and the number attribute "2019".

Smart Classification **relies on metadata** in order to operate. A minimum of **one set of metadata** is required to run CCE; using more than one smart classification rule allows for a greater degree of classification.

Learn more about [Smart Classification](#) (see page 103).



CCE scans **every file and folder** on the FileCloud installation. However, the parameters of the CCE rule determine which files undergo classification.

## Smart DLP

**Smart Data Leak Prevention (DLP)** applies user-created rules in order to strictly control who can access the FileCloud installation, in addition to restricting which files and folders they can download or share. DLP rules can control access based on many different parameters, including user name, IP address, file path, and applied metadata. Smart DLP can also return information about who is attempting to access the FileCloud installation. Examples of DLP include:

- Deny users of the group "accounting" from downloading or sharing files.
- Allow users with emails from the domain "[example.com](http://www.example.com)<sup>1</sup>" to login to the FileCloud installation and share files but **deny** users the ability to download files.
- Deny downloads of files with metadata attribute "GDPR" set to "YES".
- Return the usernames, IP addresses, user agents, and file paths for everyone accessing the FileCloud installation.

1. <http://www.example.com>

DLP can operate **with** or **without** metadata or prior classification.

Learn more about [Smart DLP](#) (see page 188).

# Compliance

- [Compliance Center \(see page 6\)](#)
- [Guide to HIPAA Rules in the Compliance Center \(see page 18\)](#)
- [Guide to ITAR Rules in the Compliance Center \(see page 26\)](#)
- [Guide to GDPR Rules in the Compliance Center \(see page 29\)](#)
- [Guide to NIST Rules in the Compliance Center \(see page 33\)](#)
- [Guide to PDPL Rules in the Compliance Center \(see page 39\)](#)
- [FileCloud Web Accessibility \(VPAT\) Practices \(see page 43\)](#)

## Compliance Center



NIST and PDPL compliance checks are available beginning in version 23.232 of FileCloud.

The **Compliance Center** enables you to check which regulatory requirements your system meets and which it fails to meet. It also provides information explaining why you haven't met certain requirements, and enables you to configure compliance settings.

### The Compliance Center

To open the Compliance Center, in the navigation panel, click **Compliance Center**.

#### The Overview tab

The **Compliance Center** opens to the **Overview** tab. This tab lists your enabled configurations and recent compliance events.

In the image below, the box under **Enabled Configurations** displays an icon for each compliance and a slider that currently indicates that it is enabled. The box for each compliance also indicates the number of total compliance rules that are being evaluated and how many of them failed the last

evaluation.

FILECLOUD

Admins

MANAGE

Team Folders

Network Share

User Share

Folder Permissions

Notifications

DEVICES

Device Management

GOVERNANCE

Dashboard

Retention

Smart DLP

Smart Classification

Compliance Center

MISC.

Audit

Alert

User Locks

Workflows

Reports

Federated Search

Metadata

SETTINGS

Settings

CUSTOMIZATION

Customization

SYSTEM

FILECLOUD Compliance Center

Overview

Enabled Configurations

5 of 5 configurations enabled

ITAR

HIPAA

GDPR

NIST

PDPL

Recent Events

Dec 19 2023

11:00 AM

11:15 AM

11:30 AM

12:00 AM

12:00 AM

12:00 AM

12:00 AM

12:00 AM

Events include failed rules, disabled/enabled rules, and configuration changes.

Click to export a CSV file of events.

Filter events listed.

Export Events

filters

Refresh Events

ITAR compliance checking is enabled for 13 of 14 rules. 9 of those rules failed the most recent check.

Compliance policy 'status' updated to enabled (HIPAA)

Compliance policy 'status' updated to disabled (HIPAA)

Share may not be public [/sarath/SARATH\_1/SampleCSVFile\_2kb.csv]

Share may not be public [/sarath/A/file\_example\_XLS\_10.xls]

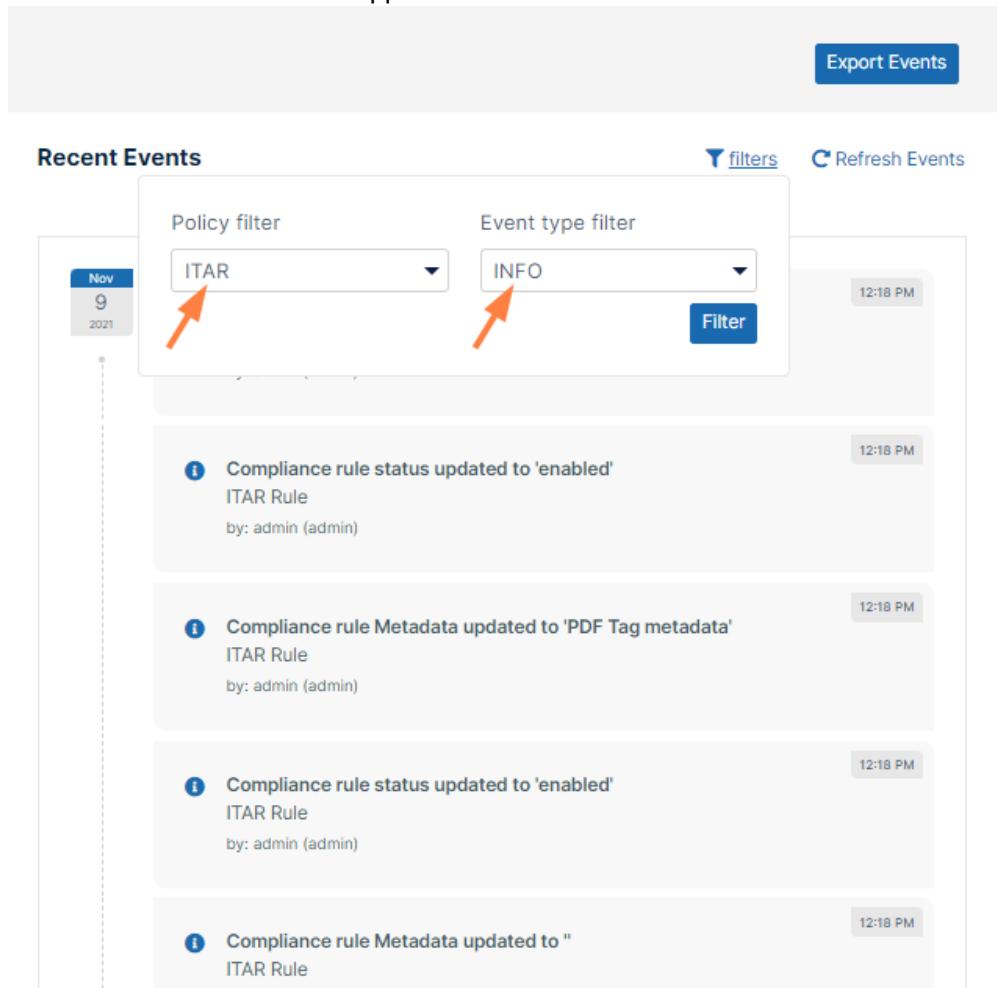
Share may not be public [/sarath/B]

Share may not be public [/sarath/A]

## Filtering Events

You can click **filters** above the **Recent Events** list to only display violation or information events, or to only display events for one compliance. In the following image, the filters are set so that only ITAR

events that are informational appear.



Recent Events

Policy filter: ITAR

Event type filter: INFO

Filter

Nov 9 2021

12:18 PM

12:18 PM

12:18 PM

12:18 PM

- Compliance rule status updated to 'enabled'  
ITAR Rule  
by: admin (admin)
- Compliance rule Metadata updated to 'PDF Tag metadata'  
ITAR Rule  
by: admin (admin)
- Compliance rule status updated to 'enabled'  
ITAR Rule  
by: admin (admin)
- Compliance rule Metadata updated to "  
ITAR Rule

## Compliance Tabs

There are currently compliance tabs for ITAR, HIPAA, GDPR, NIST, and PDPL. Each tab lists the rules for the particular regulation and whether the system is compliant with each rule or has issues. You can enable or disable each rule, change the settings that are evaluated, and manually mark a rule

as compliant in each tab.

Rules	FileCloud Configuration	Enable	Effective Date	Status	Actions
120.6	Click Edit to designate a metadata set to identify defense articles.	<input checked="" type="checkbox"/>	25-08-2021	<span>OK</span> 14-09-2023 12:00 AM	<span>Info</span>
120.10	Choose a metadata set for classifying technical data.	<input checked="" type="checkbox"/>	13-09-2021	<span>Issues</span> 14-09-2023 12:00 AM	<span>Info</span>
120.13	Choose a DLP rule that allows logins from within the US only.	<input checked="" type="checkbox"/>	13-09-2021	<span>Issues</span> 14-09-2023 12:00 AM	<span>Info</span>
120.15	Enable this rule as confirmation that all users are US residents.	<input checked="" type="checkbox"/>	31-08-2021	<span>OK</span> 14-09-2023 12:00 AM	<span>Info</span>
120.17	Choose a DLP rule that only allows private sharing.	<input checked="" type="checkbox"/>	24-08-2021	<span>Issues</span> 14-09-2023 12:00 AM	<span>Info</span>
120.25	Promote at least one user to an Admin role with access to the Compliance Dashboard.	<input checked="" type="checkbox"/>	18-08-2021	<span>OK</span> 14-09-2023 12:00 AM	<span>Info</span>
120.50	Use DRM when downloading/previewing files.	<input checked="" type="checkbox"/>	18-08-2021	<span>OK</span> 14-09-2023 12:00 AM	<span>Info</span>

Hover over the description under **FileCloud Configuration** for more details about how to configure the rule's setting. For even more information, click the row's information icon.

If **Status** indicates that there are issues, click the warning icon to see details of the issue.

## How to set up and check compliance

For each type of compliance that you want to manage, follow these steps to enable and configure compliance checking and review your compliance status.

### 1) Enable compliance checking

#### Enable compliance checking

1. In the Admin portal's navigation panel, click **Compliance Center**.  
The **Compliance Center** opens to the **Overview** tab.
2. Either:  
Under **Enabled Configurations**, click the slider for a compliance.

Enabled Configurations

5 of 5 configurations enabled

- ITAR: 13/14 rules enabled, 9 failed, 0 bypassed (Enabled)
- GDPR: 13/13 rules enabled, 5 failed, 0 bypassed (Enabled)
- HIPAA: 9/31 rules enabled, 5 failed, 1 bypassed (Enabled)
- NIST: 17/18 rules enabled, 3 failed, 0 bypassed (Enabled)
- PDPL: 15/22 rules enabled, 6 failed, 0 bypassed (Enabled)

Or:

Click the tab for a compliance, and click the slider at the top of the screen.

ITAR Compliance

Enable

#### Enable or disable compliance checking for a rule:

After checking has been enabled for a specific compliance, you can enable or disable checking for each of its rules by toggling the slider to the rule's right. Notice that compliance status is checked as soon as you enable the rule.

Some rules prompt you to enter settings when you enable them. See the next procedure.

Enable  
a rule  
that

### **prompts you for settings**

When you enable certain rules, a dialog box opens and prompts you to enter a setting before the rule is enabled and **Status** indicates if it is OK or there are issues. You are not required to enter the setting, but if you do not **Status** indicates there are issues.

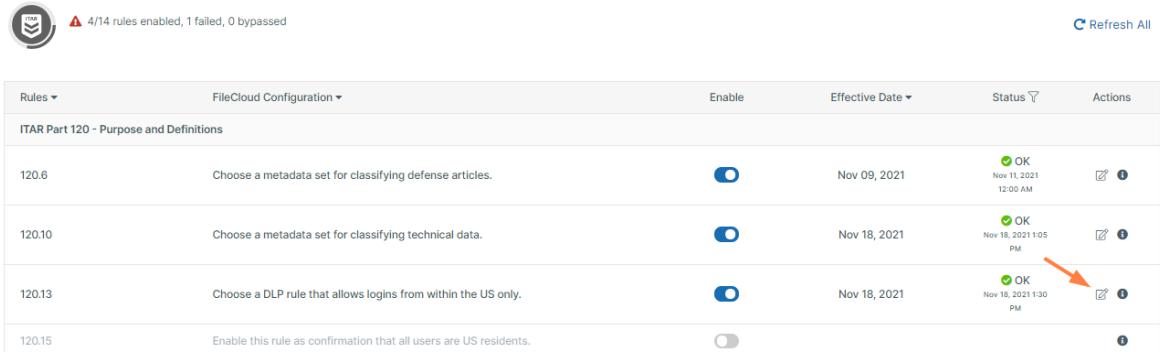
2)

## **Configure Compliance Settings**

### **Compliance settings you can configure while in the Compliance Center**

You can configure the compliance settings directly from the Compliance Center for any rules with an **Edit** icon under **Actions**. When you enable the rule, you are prompted to enter settings, but you are not required to enter them. See the video above, under **Enable a rule that prompts you for settings**.

After you configure the setting, you can change it by clicking the edit icon in the row for the rule:



Rules	FileCloud Configuration	Enable	Effective Date	Status	Actions
ITAR Part 120 - Purpose and Definitions					
120.6	Choose a metadata set for classifying defense articles.	<input checked="" type="checkbox"/>	Nov 09, 2021	<span>OK</span> Nov 11, 2021 12:00 AM	 
120.10	Choose a metadata set for classifying technical data.	<input checked="" type="checkbox"/>	Nov 18, 2021	<span>OK</span> Nov 18, 2021 1:05 PM	 
120.13	Choose a DLP rule that allows logins from within the US only.	<input checked="" type="checkbox"/>	Nov 18, 2021	<span>OK</span> Nov 18, 2021 1:30 PM	 
120.15	Enable this rule as confirmation that all users are US residents.	<input type="checkbox"/>			

### Compliance settings you must configure outside the Compliance Center

For many rules, you must navigate to other pages in FileCloud and configure settings. The compliance tool will verify that the settings are configured correctly when you enable the rule.

For instructions on how to configure the settings, click the Information icon in the row for the rule.



Rules you can mark as compliant

### compliant

Some rules only need your verification that you are complying with them. Simply enable the rule to confirm that you have complied.

Bypassing

### compliance checking

You have the option of bypassing FileCloud's compliance checking for most rules, so that whether or not the rule would be considered compliant by FileCloud's verification process, **Status** will display **BYPASSED** with a green check.

Note that you cannot bypass rules that only require you to enable them to make them compliant, as there is no validation to bypass.

To bypass a rule, enable it, then click the Information icon, and check **Bypass check for this rule and mark as passed**.

### 3) Run compliance checks

FileCloud automatically checks a rule for compliance when it is enabled and rechecks compliance for all rules in once per day. If you make changes in your system or want to make sure you have the most recent check, you can manually run a compliance check.

#### Manually running a compliance check

To manually run a compliance check, in the tab for the compliance, click **Refresh All**.

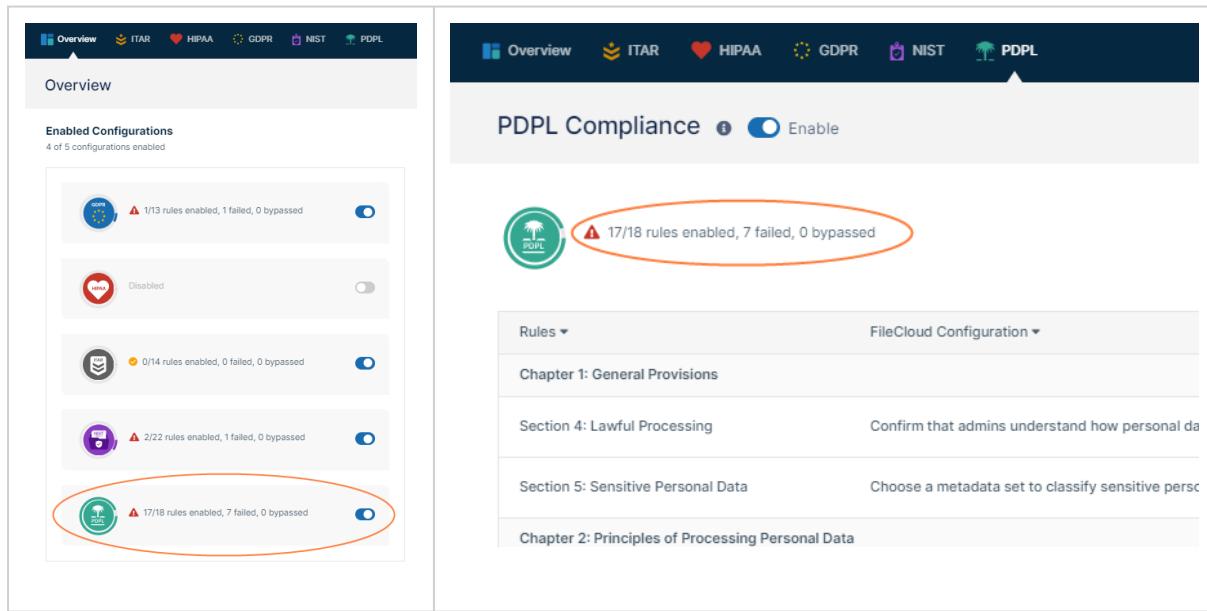
4)

#### Review compliance status

Review your compliance status regularly to make sure all of your rules remain compliant.

#### Viewing the status summary

You can view a summary of the number of rules you have enabled for checking, and how many of them failed or were bypassed on the **Overview** tab or at the top of the compliance tab.



The screenshot displays two panels of the FileCloud Online Governance Setup interface. The left panel, titled 'Overview', shows 'Enabled Configurations' with 4 of 5 configurations enabled. It lists five items: 'GDPR' (1/13 rules enabled, 1 failed, 0 bypassed), 'HIPAA' (Disabled), 'NIST' (0/14 rules enabled, 0 failed, 0 bypassed), 'ITAR' (2/22 rules enabled, 1 failed, 0 bypassed), and 'PDPL' (17/18 rules enabled, 7 failed, 0 bypassed). The 'PDPL' item is circled in orange. The right panel, titled 'PDPL Compliance', has an 'Enable' switch set to 'On'. It shows a summary: '17/18 rules enabled, 7 failed, 0 bypassed'. Below this, a section titled 'PDPL Compliance' lists several configuration items with dropdown menus for 'Rules' and 'FileCloud Configuration'. The items include 'Chapter 1: General Provisions', 'Section 4: Lawful Processing', 'Section 5: Sensitive Personal Data', and 'Chapter 2: Principles of Processing Personal Data'.

### Checking a rule's compliance status

On a compliance tab, you can review whether each enabled rule's compliance check was OK, had issues, or was bypassed by viewing its **Status**.

FileCloud Compliance Center

Overview ITAR HIPAA GDPR NIST PDPL

HIPAA Compliance  Enable Export Settings

5/31 rules enabled, 3 failed, 1 bypassed Refresh All

Rules	FileCloud Configuration	Enable	Effective Date	Status	Actions
Subpart C - 164.304 Definitions					
164.304 Definitions	Choose a metadata set to classify electronic protected health information.	<input checked="" type="checkbox"/>	Dec 18, 2023	<span>OK</span> Dec 18, 2023 2:23 PM	
164.306 Security standards: General rules					
164.306 Security standards: General rules	Give at least one admin access to the Compliance Center."	<input checked="" type="checkbox"/>	Dec 18, 2023	<span>Issues</span> Dec 18, 2023 2:23 PM	
164.308 Administrative safeguards					
164.308 Administrative safeguards.(a)(1)(ii)(A & B)	Enable this rule once all the other HIPAA rules are compliant	<input checked="" type="checkbox"/>	Dec 18, 2023	<span>BYPASSED</span>	
164.308 Administrative	Enable Governance Report Email to send the HIPAA admin an email	<input type="checkbox"/>	Dec 18, 2023	<span>Issues</span> Dec 18, 2023	

### Checking why a rule failed

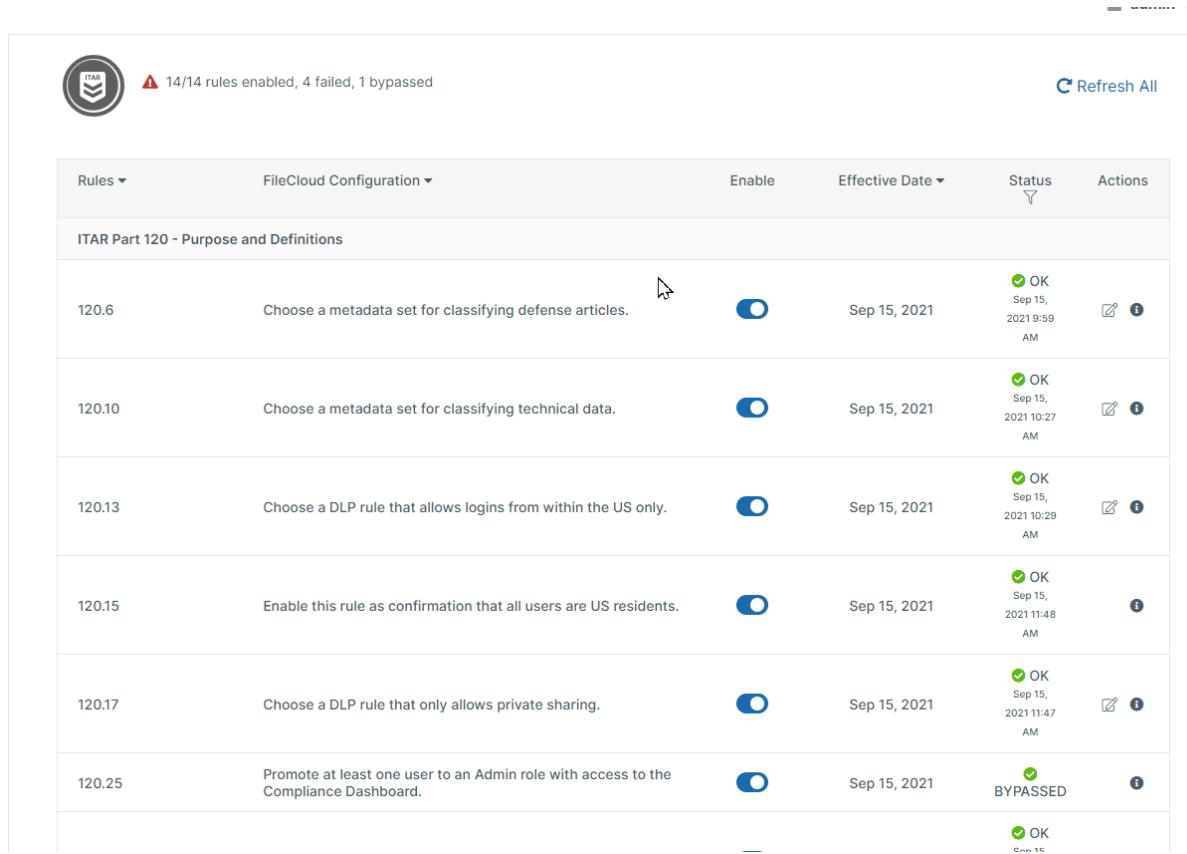
If the **Status** column for a rule displays **Issues** and an error icon, click on the status to view information about the problem.

Rules ▾	FileCloud Configuration ▾	Enable	Effective Date ▾	Status ▾	Actions
ITAR Part 120 - Purpose and Definitions					
120.6	Choose a metadata set for classifying defense articles.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 9:59 AM	
120.10	Choose a metadata set for classifying technical data.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 10:27 AM	
120.13	Choose a DLP rule that allows logins from within the US only.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 10:29 AM	
120.15	Enable this rule as confirmation that all users are US residents.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 11:48 AM	
120.17	Choose a DLP rule that only allows private sharing.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 11:47 AM	
120.25	Promote at least one user to an Admin role with access to the Compliance Dashboard.	<input checked="" type="checkbox"/>	Sep 15, 2021	BYPASSED	
120.50	Use DRM when downloading/previewing files.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 11:48 AM	
120.54(2)(3)	Remove any existing public shares or change them to private.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 11:48 AM	
120.54(5)	Use settings for SSL and enable encryption.	<input checked="" type="checkbox"/>	Sep 15, 2021	Issues Sep 15, 2021 11:48 AM	
120.55	Confirm decryption keys are confidential.	<input checked="" type="checkbox"/>	Sep 15, 2021	OK Sep 15, 2021 11:48 AM	
ITAR Part 123 - Licenses for the Export of Defense Articles					
123.1	Choose policy settings that permit private sharing only or do not permit sharing.	<input checked="" type="checkbox"/>	Sep 15, 2021	Issues Sep 15, 2021 11:48 AM	

## Getting more details on how to comply

### Getting more details on how to comply

For basic information on how to comply with a rule, hover over the description under **FileCloud Configuration**. For more specific instructions, click the Information icon in the row for the rule. To see the text of the rule in the regulation document, click the rule number.



Rules ▾	FileCloud Configuration ▾	Enable	Effective Date ▾	Status	Actions
<b>ITAR Part 120 - Purpose and Definitions</b>					
120.6	Choose a metadata set for classifying defense articles.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>OK</span> Sep 15, 2021 9:59 AM	 
120.10	Choose a metadata set for classifying technical data.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>OK</span> Sep 15, 2021 10:27 AM	 
120.13	Choose a DLP rule that allows logins from within the US only.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>OK</span> Sep 15, 2021 10:29 AM	 
120.15	Enable this rule as confirmation that all users are US residents.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>OK</span> Sep 15, 2021 11:48 AM	
120.17	Choose a DLP rule that only allows private sharing.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>OK</span> Sep 15, 2021 11:47 AM	 
120.25	Promote at least one user to an Admin role with access to the Compliance Dashboard.	<input checked="" type="checkbox"/>	Sep 15, 2021	<span>BYPASSED</span>	
<span>OK</span> Sep 15, 2021					

## Specific compliance rules and validation

For more details about the rules covered for each compliance and how they are handled in FileCloud, see:

[Guide to HIPAA Rules in the Compliance Center \(see page 18\)](#)

[Guide to ITAR Rules in the Compliance Center \(see page 26\)](#)

[Guide to GDPR Rules in the Compliance Center \(see page 29\)](#)

[Guide to NIST Rules in the Compliance Center \(see page 33\)](#)

[Guide to PDPL Rules in the Compliance Center \(see page 39\)](#)

## Guide to HIPAA Rules in the Compliance Center

This table defines the HIPAA rules covered in FileCloud's Compliance Center, explains what steps you must take to be in compliance, and describes how FileCloud validates each rule.

Rule (click to see text)	Description	Steps for complying	Validation
<a href="#">164.304 Definitions<sup>2</sup></a>	Identify which files have electronically protected health information (ePHI).	<p>In the Compliance Center, click the Edit button for the rule, and select a metadata set with a tag that identifies ePHI files.</p> <p>(To carry out compliance, you must use smart classification (see page 103) to apply the metadata tag to ePHI files.)</p>	If the metadata set exists and is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">164.306 Security standards: General rules<sup>3</sup></a>	Allow at least one user access to the Compliance system.	<p>To enable at least one user to manage the Compliance Center:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Admins</b> and create a role with <b>Compliance</b> access to the Compliance Center.</li> <li>2. In <b>Admins</b>, add at least one user to the role with access to the Compliance Center.</li> </ol>	If one or more Admin users have access to the Compliance Center, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">164.308 Administrative safeguards.<sup>4</sup> (a)(1)(ii)(A &amp; B)<sup>5</sup></a>	Confirm that all the FileCloud Compliance HIPAA rules are successful.	Enable this rule once all the other HIPAA rules are compliant.	If all rules are implemented and status of all rules is <b>OK</b> then the status of this rule <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">164.308 Administrative safeguards.<sup>6</sup> (a)(1)(ii)(D)<sup>7</sup></a>	Implement a procedure to regularly review system activity records.	In <b>Settings &gt; Admin</b> , enable <b>Send daily governance report to admin</b> .	If the <b>Send daily governance report to admin</b> setting is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">164.308 Administrative safeguards.<sup>8</sup> (a)(3)(ii)(A)</a>	Allow users to login to access FileCloud content based on location or IP address.	Click the Edit button and select a DLP rule that blocks users from logging in from outside locations.	If the DLP rule exists and is enabled and GeolP is not disabled, status is <b>OK</b> ; otherwise, status is <b>Issues</b> .

2. <https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.304>

3. <https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.306>

4. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(1\)\(ii\)}](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(1)(ii)})

5. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(1\)\(ii\)}](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(1)(ii)})

6. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(1\)\(ii\)\(D\)}](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(1)(ii)(D)})

7. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(1\)\(ii\)\(D\)}](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(1)(ii)(D)})

Rule (click to see text)	Description	Steps for complying	Validation
164.308 Administrative safeguards. (a)(5)(ii)(B) <sup>9</sup>	Configure antivirus protection against malicious file uploads.	<ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Third Party Integration &gt; Antivirus</b>.</li> <li>2. Configure an Antivirus.</li> </ol>	If an <b>Antivirus</b> is configured, status is <b>OK</b> ; if not, status is <b>Issues</b> .
164.308 Administrative safeguards. (a)(5)(ii)(C) <sup>10</sup>	Monitor log-in attempts.	<ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Admin</b>.</li> <li>2. Set <b>Audit Log Level</b> to <b>REQUEST</b> or <b>FULL</b>.</li> </ol>	If <b>Audit Log Level</b> is <b>REQUEST</b> or <b>FULL</b> status is <b>OK</b> ; if <b>Audit Log Level</b> is <b>OFF</b> , status is <b>Issues</b> .
164.308 Administrative safeguards. (a)(5)(ii)(D) <sup>11</sup>	Set up password management procedures.	<ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Password</b>.</li> <li>2. Configure the settings as follows: <ul style="list-style-type: none"> <li>• Set <b>Minimum password length</b> to 8 or more.</li> <li>• Enable <b>Enable strong passwords</b>.</li> <li>• Enable <b>Disallow commonly used passwords</b>.</li> <li>• Set <b>User password expiration in days</b> to a value greater than 0.</li> <li>• Set <b>Number of previous passwords that cannot be reused</b> to a value greater than 0.</li> <li>• Set <b>Reset password attempt interval</b> to a value greater than 0.</li> </ul> </li> </ol>	If the password settings are configured as indicated, status is <b>OK</b> ; if not, status is <b>Issues</b> .
164.308 Administrative safeguards. (a)(6)(ii) <sup>12</sup>	Confirm all (HIPAA) violations can be exported from the Compliance Center.	Enable this rule as confirmation that all FileCloud Compliance HIPAA violations can be exported.	None

---

8. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308\(a\)\(3\)\(ii\)\(A\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308(a)(3)(ii)(A))
9. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308\(a\)\(5\)\(ii\)\(B\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308(a)(5)(ii)(B))
10. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308\(a\)\(5\)\(ii\)\(C\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308(a)(5)(ii)(C))
11. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308\(a\)\(5\)\(ii\)\(D\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308(a)(5)(ii)(D))
12. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308\(a\)\(6\)\(ii\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-C/section-164.308#p-164.308(a)(6)(ii))

Rule (click to see text)	Description	Steps for complying	Validation
164.308 Administrative safeguards. (a)(7)(i) <sup>13</sup>	Implement a contingency plan in case systems containing ePHI are damaged.	<p>Enable this rule as confirmation that you have done the following:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; General</b>.</li> <li>2. Disable <b>Database backup interval</b> option should be disabled (by default it is disabled).</li> <li>3. Set <b>Database backup interval</b> to <b>daily</b>.</li> <li>4. Backup of the managed storage location should be planned and maintained by your team.</li> </ol>	None
164.308 Administrative safeguards. (a)(7)(ii)(B) <sup>14</sup>	Establish procedures to restore loss of data.	Enable this rule as confirmation that admins understand the procedures to restore data given at Backing Up and Restoring FileCloud Server.	None
164.308 Administrative safeguards. (a)(7)(ii)(C) <sup>15</sup>	Establish an emergency mode operation plan.	Enable this rule as confirmation that admins understand that they can configure a firewall proxy rule to prevent access to FileCloud to protect ePHI.	None
164.312 Technical safeguards. (a)(1) <sup>16</sup>	Implement policies and procedures to only allow access to ePHI to people and programs with access rights.	<p>To prevent data from being shared with unauthorized users:</p> <ol style="list-style-type: none"> <li>1. For each policy, go to <b>Settings &gt; Policies</b> and click the <b>General</b> tab. Set <b>Share Mode</b> to either <b>Allow Private Shares Only</b> or <b>Shares Not Allowed</b>.</li> <li>2. Remove any existing public shares, or change them to private.</li> </ol>	If <b>Share Mode</b> is <b>Allow All Shares</b> or any public shares exist, status is <b>Issues</b> .

13. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(7\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(7)(i))

14. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(7\)\(ii\)\(B\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(7)(ii)(B))

15. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308\(a\)\(7\)\(ii\)\(C\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.308#p-164.308(a)(7)(ii)(C))

16. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(a\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312(a)(1))

Rule (click to see text)	Description	Steps for complying	Validation
164.312 Technical safeguards. (a)(2)(i) <sup>17</sup>	Assign a unique name and/or number to each user.	Enable this rule as a confirmation that all users have unique usernames.	None
164.312 Technical safeguards. (a)(2)(iii) <sup>18</sup>	Terminate sessions after a certain amount of time automatically.	<p>To confirm automatic logoff of sessions:</p> <ul style="list-style-type: none"> <li>Go to <b>Settings &gt; Server</b>, and set <b>Session Timeout</b> to a value greater than 0.</li> </ul>	If <b>Session Timeout</b> is set to 0 or empty, status is <b>Issues</b> .
164.312 Technical safeguards. (a)(2)(iv) <sup>19</sup>	Implement encryption and decryption of ePHI.	<p>To set up ePHI encryption:</p> <ol style="list-style-type: none"> <li>Configure storage encryption. See <b>Setting Up Managed Storage Encryption</b>.</li> <li>Go to <b>Settings &gt; Storage &gt; Managed Storage</b> and click <b>Manage</b> next to <b>Encryption</b>; then enable encryption.</li> <li>Encrypt all existing files.</li> </ol>	If storage is not fully encrypted, or any existing files are not fully encrypted, status is <b>Issues</b> .
164.312 Technical safeguards. (b) <sup>20</sup>	Set up audit controls.	<p>To implement audit controls:</p> <ul style="list-style-type: none"> <li>Go to <b>Settings &gt; Admin</b>, and configure the following: <ul style="list-style-type: none"> <li><b>Audit Log Level</b> - Set to to <b>REQUEST</b> or <b>FULL</b>.</li> <li><b>Auto Archive Audit Database</b> - Enable.</li> <li><b>Auto Archive Records Frequency (in days)</b> - Enter a value.</li> <li><b>Storage Path For Archived Audit Records</b> - Enter a valid path.</li> </ul> </li> </ul>	If any of the audit settings is not set as specified, status is <b>Issues</b> .

17. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(a\)\(2\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312(a)(2)(i))

18. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(a\)\(2\)\(iii\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312(a)(2)(iii))

19. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(a\)\(2\)\(iv\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312(a)(2)(iv))

20. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(b\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.312#p-164.312(b))

Rule (click to see text)	Description	Steps for complying	Validation
164.312 Technical safeguards. (c)(1) <sup>21</sup>	Protect ePHI files from destruction.	<p>To protect ePHI files and folders from deletion:</p> <ul style="list-style-type: none"> <li>Click the Edit button, and select a retention policy to protect ePHI files and folders from deletion based on metadata.</li> </ul>	If the retention policy exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the retention policy allow file or folder deletion, status is <b>Issues</b> .
164.312 Technical safeguards. (d) <sup>22</sup>	Verify user identity of people seeking access to ePHI.	To confirm that all users have individual FileCloud user accounts, enable this rule.	None
164.312 Technical safeguards. (e)(1) <sup>23</sup>	Guard against unauthorized access of ePHI that is being transmitted.	<p>To guard against unauthorized access to ePHI:</p> <ol style="list-style-type: none"> <li>Click the Edit button, and select a DLP rule that blocks public shares.</li> <li>Change any existing public shares to private.</li> </ol>	If the DLP rule exists and is enabled and there are no existing public shares, status is <b>OK</b> ; if not, or if modifications to the rule allow public shares, status is <b>Issues</b> .
164.312 Technical safeguards. (e)(2)(i) <sup>24</sup>	Ensure that transmitted ePHI is not modified.	To confirm that users are educated about sharing permissions and folder level permissions, enable this rule.	None
164.316 Policies and procedures and documentation requirements (b)(2)(i) <sup>25</sup>	Retain files for 6 years.	<p>To retain files for 6 years:</p> <ul style="list-style-type: none"> <li>Click the Edit button, and select a retention policy to retain files for 6 years based on metadata. (The selected retention policy must have its expiry set to 2192 days (6 years with 2 leap years) and must not renew on expiry.)</li> </ul>	If the retention policy exists and is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .

21. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312\(c\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312(c)(1))

22. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312\(d\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312(d))

23. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312\(e\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312(e)(1))

24. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312\(e\)\(2\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.312#p-164.312(e)(2)(i))

25. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.316#p-164.316\(b\)\(2\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164 subpart-C section-164.316#p-164.316(b)(2)(i))

Rule (click to see text)	Description	Steps for complying	Validation
164.316 Policies and procedures and documentation requirements .(b)(2)(ii) <sup>26</sup>	Make documentation available and accessible.	To confirm that Admins and users have access to support documentation for all features, enable this rule.	None
164.316 Policies and procedures and documentation requirements .(b)(2)(iii) <sup>27</sup>	Maintain updated documentation.	To ensure the system is at the latest version, go to Upgrade screen in Admin and ensure there are no upgrades available	If the system is not upgraded to the latest available version, then status is <b>Issues</b> .
164.404 Notification to individuals. (b) <sup>28</sup>	Create timely notifications in case of breaches.	To confirm that admins can use Audit logs, Alerts and Violation reports to generate breach notifications, enable this rule.	None
164.502 Uses and disclosures of protected health information: General rules.(a)(1) <sup>29</sup>	Allow users to use and disclose ePHI according to regulations.	<p>To prevent data from being shared with non-associates without proper permission:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Policies</b>, and edit each policy.             <ol style="list-style-type: none"> <li>a. On the <b>General</b> tab, set <b>Share Mode</b> to either <b>Allow Private Shares Only</b> or <b>Shares Not Allowed</b>.</li> <li>b. Remove any existing public shares or change them to private.</li> </ol> </li> </ol>	If <b>Share Mode</b> is <b>Allow All Shares</b> or any public shares exist, status is <b>Issues</b> .

26. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.316#p-164.316\(b\)\(2\)\(ii\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(2)(ii))

27. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.316#p-164.316\(b\)\(2\)\(iii\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(2)(iii))

28. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-D/section-164.404#p-164.404\(b\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-D/section-164.404#p-164.404(b))

29. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-E/section-164.502#p-164.502\(a\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C/part-164/subpart-E/section-164.502#p-164.502(a)(1))

Rule (click to see text)	Description	Steps for complying	Validation
164.504 Uses and disclosures: Organizational requirements .(e)(1) <sup>30</sup>	Business associates must comply with standards.	To confirm that users who have access to ePHI are educated about sharing permissions, enable this rule.	None
164.504 Uses and disclosures: Organizational requirements .(e)(2)(ii)(J) <sup>31</sup>	At the termination of a contract, all info shared with business associate should be destroyed or returned.	<p>To confirm return or destruction of ePHI at the termination of contracts:</p> <ul style="list-style-type: none"> <li>Go to <b>Settings &gt; Misc &gt; Share</b> and configure these settings:           <ul style="list-style-type: none"> <li><b>Remove Expired Shares</b> - enable.</li> <li><b>Delete Files from Expired Shares</b> - enable.</li> </ul> </li> </ul>	If all the settings are as specified, status is <b>OK</b> ; if not, status is <b>Issues</b> .
164.508 Uses and disclosures for which an authorization is required. (a) <sup>32</sup>	Uses of ePHI requiring authorization.	<p>To implement authorization for use and disclosures of ePHI:</p> <ul style="list-style-type: none"> <li>Click the Edit button, and select a DLP rule that restricts sharing.</li> </ul>	If the DLP rule exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the rule allow public shares, status is <b>Issues</b> .
164.522 Rights to request privacy protection for protected health information. (a)(1) <sup>33</sup>	Right of individual to request restriction of disclosure of their ePHI.	<p>To implement the right of an individual to request restriction of uses and disclosures of ePHI:</p> <ol style="list-style-type: none"> <li>Go to <b>Settings &gt; Misc &gt; General</b>.</li> <li>If <b>Disable Locking</b> is enabled, disable it, and save.</li> </ol>	If <b>Disable Locking</b> is unchecked, status is <b>OK</b> ; if not, status is <b>Issues</b> .

30. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.504#p-164.504\(e\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.504#p-164.504(e)(1))

31. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.504#p-164.504\(e\)\(2\)\(ii\)\(J\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.504#p-164.504(e)(2)(ii)(J))

32. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.508#p-164.508\(a\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.508#p-164.508(a))

33. [https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.522#p-164.522\(a\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A subchapter-C part-164 subpart-E section-164.522#p-164.522(a)(1))

Rule (click to see text)	Description	Steps for complying	Validation
<a href="#">164.528 Accounting of disclosures of protected health information.<sup>34</sup></a>	Right of an individual to receive records of disclosures of PHI.	To confirm that admins understand how to use audit logs and reports to generate an account of disclosures of protected health information, enable this rule.	None

## Guide to ITAR Rules in the Compliance Center

This table defines the ITAR rules covered in FileCloud's Compliance Center, explains what steps you must take to be in compliance, and describes how FileCloud validates each rule.

Rule (click to see text)	Description	Steps for complying	Validation
<a href="#">120.6<sup>35</sup></a>	Identify which documents are defense articles.	In the Compliance Center, click the Edit button for the rule, and select a metadata set with a tag that identifies defense articles.  (To carry out compliance, you must use smart classification (see page 103) to apply the metadata tag to defense articles.)	If the metadata set exists and is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">120.1 0<sup>36</sup></a>	Identify which files contain technical data.	In the Compliance Center, click the Edit button for the rule, and select a metadata set with a tag that identifies technical data.  (To carry out compliance, you must use smart classification (see page 103) to apply the metadata tag to technical data.)	If the metadata set exists and is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">120.1 3<sup>37</sup></a>	Only allow access to the system from within the US.	In the Compliance Center, click the Edit button for the rule, and select a DLP rule (see page 188) that blocks users from logging in from outside locations. Only DLP rules for the LOGIN action are available for selection.	If the DLP rule exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the rule allow log in from outside the US, status is <b>Issues</b> .

34. <https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-E/section-164.528>

35. <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120#120.6>

36. <https://www.ecfr.gov/cgi-bin/text-idx?>

SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\_110

37. <https://www.ecfr.gov/cgi-bin/text-idx?>

SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\_113

Rule (click to see text)	Description	Steps for complying	Validation
120.1 5 <sup>38</sup>	Only allow US residents to access the system.	Enabling the rule to confirm that your system checks if all users are US residents is all that is necessary to pass the compliance check.	None
120.1 7 <sup>39</sup>	Do not permit public sharing.	<ol style="list-style-type: none"> <li>In the Compliance Center, click the Edit button for the rule, and select a DLP rule (see page 188) that blocks public shares. Only DLP rules for the SHARE action are available for selection.</li> <li>Change any existing public shares to private.</li> </ol>	If the DLP rule exists and is enabled and there are no existing public shares, status is <b>OK</b> ; if not, or if modifications to the rule allow public shares, status is <b>Issues</b> .
120.2 5 <sup>40</sup>	Allow at least one user access to the Compliance system.	<p>To enable at least one user to manage the Compliance Center:</p> <ol style="list-style-type: none"> <li>Go to <b>Admins</b> and create a role with <b>Compliance</b> access to the Compliance Center.</li> <li>In <b>Admins</b>, add at least one user to the role with access to the Compliance Center.</li> </ol>	If one or more Admin users have access to the Compliance Center, status is <b>OK</b> ; if not, status is <b>Issues</b> .
120.5 0 <sup>41</sup>	Prevent unauthorized access to data by non-US residents.	Install FileCloud with an enterprise license or a license that includes a Digital Rights Management (DRM) component.	If a proper license is installed, status is <b>OK</b> ; if not, status is <b>Issues</b> .
120.5 4(2) (3) <sup>42</sup>	Prevent data from being shared with non-US entities.	Remove any existing public shares or change them to private.	If any public shares exist, status is <b>Issues</b> .

38. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_115](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_115)39. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_117](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_117)40. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_125](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_125)41. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_150](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_150)42. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_154](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_154)

Rule (click to see text)	Description	Steps for complying	Validation
120.5 4(5) <sup>43</sup>	Confirm that data is only transferred between US entities.	<ol style="list-style-type: none"> <li>1. In the Admin portal, go to <b>Settings &gt; Server &gt; Server URL</b>. Use HTTPS for the <b>Server URL</b>.</li> <li>2. Configure storage encryption. See Setting up Managed Storage Encryption.</li> <li>3. Go to <b>Settings &gt; Storage &gt; Managed Storage</b> and enable <b>Encryption</b>.</li> <li>4. Encrypt all existing files.</li> </ol>	If HTTPS is not used, storage is not fully encrypted, or any existing files are not fully encrypted, status is <b>Issues</b> .
120.5 5 <sup>44</sup>	Keep decryption methods secure.	Enabling the rule to confirm that decryption keys are kept confidential in your system is all that is necessary to pass the compliance check.	None.
123.1 <sup>45</sup>	Ensure that proper permission is given if data is shared with non-US entities	<ol style="list-style-type: none"> <li>1. In the Admin portal, go to <b>Settings &gt; Policies &gt; General &gt; Share Mode</b>, and for <b>Share Mode</b> in all policies choose either <b>Allow Private Shares Only</b> or <b>Shares Not Allowed</b>.</li> <li>2. Remove any existing public shares or change them to private.</li> </ol>	If <b>Share Mode</b> is <b>Allow All Shares</b> or any public shares exist, status is <b>Issues</b> .
123.2 6 <sup>46</sup>	Maintain records of all data shared with non-US entities	In the Admin portal, go to <b>Settings &gt; Admin</b> and set the <b>Audit Log Level</b> to <b>FULL</b> .	If <b>Audit Log Level</b> is set to <b>OFF</b> or <b>REQUEST</b> , status is <b>Issues</b> .
126.1 <sup>47</sup>	Deny access to the system by prohibited countries	<p>In the row for the rule in the Compliance Center, click the Edit button and select a DLP rule (see page 188) that blocks users from logging in from those countries.</p> <p>Only DLP rules for the LOGIN action are available for selection.</p>	If the DLP rule exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the rule allow log in from those countries, status is <b>Issues</b> .

43. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_154](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_154)44. [https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120\\_155](https://www.ecfr.gov/cgi-bin/text-idx?SID=70e390c181ea17f847fa696c47e3140a&mc=true&node=pt22.1.120&rgn=div5#se22.1.120_155)45. [https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.123#se22.1.123\\_11](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.123#se22.1.123_11)46. [https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.123#se22.1.123\\_126](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.123#se22.1.123_126)

Rule (click to see text)	Description	Steps for complying	Validation
127.1 <sup>48</sup>	Confirm that reports of violations of compliance rules can be exported.	Enabling the rule to confirm that there is functionality to export reports of compliance rule violations from this page is all that is necessary to pass the compliance check.	None

## Guide to GDPR Rules in the Compliance Center

This table defines the GDPR rules covered in FileCloud's Compliance Center, explains what steps you must take to be in compliance, and describes how FileCloud validates each rule.

Rule (click to see text)	Description	Steps for complying	Validation
Art 5 <sup>49</sup>	Principles for processing personal data.	To set up data protection, customize Terms of Service: <ol style="list-style-type: none"> <li>1. Go to <b>Customization &gt; TOS</b>.</li> <li>2. Set up a TOS that is suitable for your organization.</li> </ol>	If the default TOS is not modified then status is <b>Issues</b> .

47. [https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.126#se22.1.126\\_11](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.126#se22.1.126_11)

48. [https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.127#se22.1.127\\_11](https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.127#se22.1.127_11)

49. <https://gdpr.eu/article-5-how-to-process-personal-data/>

Rule (click to see text)	Description	Steps for complying	Validation
Art. 6 & 7 <sup>50</sup>	Lawfulness of processing	<p>To confirm lawfulness of processing and conditions for consent:</p> <ol style="list-style-type: none"> <li>1. For each policy:             <ol style="list-style-type: none"> <li>a. Go to <b>Settings &gt; Policies</b>.</li> <li>b. Open the policy for editing.</li> <li>c. In the <b>General</b> tab, set <b>Enable Privacy Settings</b> to <b>YES</b>, and save.</li> </ol> </li> <li>2. After you have completed this configuration for each policy:             <ol style="list-style-type: none"> <li>a. Go to <b>Settings &gt; Misc &gt; Privacy</b>.</li> <li>b. Set <b>Force users to accept TOS when changed</b> to enabled.</li> <li>c. Enable <b>Show TOS for every login</b>.</li> </ol> </li> </ol>	If the settings are set as specified, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Art. 12 <sup>51</sup>	Rights of data subject - transparent information	<p>To maintain transparent information and communication:</p> <ul style="list-style-type: none"> <li>• Go to <b>Settings &gt; Misc &gt; General</b>, and if <b>Disable Action Panel</b> is enabled, disable it.</li> </ul>	If <b>Disable Action Panel</b> is disabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Art. 13 <sup>52</sup>	Rights of data subject - information about collecting of personal data	To confirm that <b>Terms of Service</b> indicate where personal data are collected about the data subject, enable this rule.	<b>None</b>
Art. 17 <sup>53</sup>	Rights of data subject - right to be forgotten	<p>To set up the right to be forgotten:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Privacy</b>.</li> <li>2. In <b>Anonymous User Consent Message for Accessing Shared Files</b> enter text that explains data subject's right to erasure.</li> <li>3. If a user requests to be forgotten, anonymize the data.</li> </ol> <p>Also see <b>Anonymizing User Data</b>.</p>	If the settings are configured as specified, status is <b>OK</b> ; if not, status is <b>Issues</b> .

50. <https://gdpr.eu/article-6-how-to-process-personal-data-legally/>51. <https://gdpr.eu/article-12-how-controllers-should-provide-personal-data-to-the-subject/>52. <https://gdpr.eu/article-13-personal-data-collected/>53. <https://gdpr.eu/article-17-right-to-be-forgotten/>

Rule (click to see text)	Description	Steps for complying	Validation
Art. 20 <sup>54</sup>	Rights of data subject - right to data portability	<p>To confirm the right to data portability, ensure the following options work in the Admin portal, and then enable this rule.</p> <ul style="list-style-type: none"> <li>• Exporting a user's file.             <ol style="list-style-type: none"> <li>a. In the navigation pane, click <b>Users</b>.</li> <li>b. Edit a user.</li> <li>c. In the <b>User Details</b> dialog box, click <b>Manage Files</b>, and then click <b>My Files</b>.</li> <li>d. Click <b>Download as Zip</b> for a file, and confirm that the zip download works.</li> </ol> </li> <li>• Exporting audit log records.             <ol style="list-style-type: none"> <li>1.                     <ol style="list-style-type: none"> <li>a. In the navigation pane, click <b>Audit</b>.</li> <li>b. In the upper-right corner of the screen, click <b>Manage</b>.</li> <li>c. In the <b>Manage Audit Logs</b> dialog box, enter a <b>Start Date</b> and an <b>End Date</b>.</li> <li>d. Click <b>Export</b>, and confirm that the file is exported correctly.</li> </ol> </li> </ol> </li> </ul>	None.

54. <https://gdpr.eu/article-20-right-to-data-portability/>

Rule (click to see text)	Description	Steps for complying	Validation
Art. 21 <sup>55</sup>	Rights of data subject - right to object	<p>To confirm users have right to object:</p> <ul style="list-style-type: none"> <li>• For each policy:           <ol style="list-style-type: none"> <li>1.               <ol style="list-style-type: none"> <li>a. Go to <b>Settings &gt; Policies</b>.</li> <li>b. Open the policy for editing.</li> <li>c. In the <b>General tab</b>, set <b>Enable Privacy Settings</b> to <b>Yes</b>.</li> </ol> </li> </ol> </li> </ul> <p>After you have completed this configuration for each policy:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc</b>.</li> <li>2. Click the <b>Privacy</b> tab.</li> <li>3. Check <b>Show TOS for every login</b>. This option forces users to accept the TOS for every login; if users do not want to accept the condition, they can close the TOS, but they will not be able to log in to the user portal.</li> </ol>	If the specified settings are set, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Art. 30 <sup>56</sup>	Controller and processor - Records of processing activities	<p>To maintain records of processing activities:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Admin</b>.</li> <li>2. Set <b>Audit Log Level</b> to <b>Request</b> or <b>Full</b>.</li> </ol>	If <b>Audit Log Level</b> is set to <b>Request</b> or <b>Full</b> , status is <b>OK</b> ; if <b>Audit Log Level</b> is set to <b>Off</b> , status is <b>Issues</b> .
Art. 32 <sup>57</sup>	Controller and processor - Security of processing	<p>Configure storage encryption.</p> <ol style="list-style-type: none"> <li>1. See <b>Setting Up Managed Storage Encryption</b> in the support document.           <ol style="list-style-type: none"> <li>a. Go to <b>Settings &gt; Storage &gt; Managed storage</b> and enable encryption.</li> <li>b. Encrypt all existing files.</li> </ol> </li> </ol>	If storage is not fully encrypted or any existing files are not fully encrypted, status is <b>Issues</b> .
Art. 33 <sup>58</sup>	Controller and processor - Notification of a personal data breach to the supervisory authority	To confirm that admins can use audit logs, alerts, and violation reports to generate breach notification, enable this rule.	None

55. <https://gdpr.eu/article-21-right-to-object/>56. <https://gdpr.eu/article-30-records-of-processing-activities/>57. <https://gdpr.eu/article-32-security-of-processing/>

Rule (click to see text)	Description	Steps for complying	Validation
Art. 35 <sup>59</sup>	Controller and processor - Data protection impact assessment	Enable all GDPR compliance rules, and ensure that they pass.	If all GDPR compliance rules are enabled and pass, <b>Status</b> is <b>OK</b> . If any rules are not enabled or do not pass, <b>Status</b> is <b>Issues</b> .
Art. 37 <sup>60</sup>	Controller and processor - Designation of the data protection officer	<p>To enable at least one user to manage the Compliance Center:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Admins</b> and create a role with <b>Compliance</b> access to the Compliance Center.</li> <li>2. In <b>Admins</b>, add at least one user to the role with access to the Compliance Center.</li> </ol>	If one or more users have access to the Compliance Center, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Art. 45 <sup>61</sup>	Transfers of personal data to third countries or international organisations - Transfers on the basis of an adequacy decision	To allow users to log in to access FileCloud content based on location or IP address, click the Edit button and select a DLP rule that blocks users from logging in from outside locations.	If the DLP rule exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the rule allow login from outside locations, status is <b>Issues</b> .

## Guide to NIST Rules in the Compliance Center

This table defines the NIST rules covered in FileCloud's Compliance Center, explains what steps you must take to be in compliance, and describes how FileCloud validates each rule.

58. <https://gdpr.eu/article-33-notification-of-a-personal-data-breach/>

59. <https://gdpr.eu/article-35-impact-assessment/>

60. <https://gdpr.eu/article-37-designation-of-the-data-protection-officer/>

61. <https://gdpr.eu/article-45-adequacy-decision-personal-data-transfer/>

Rule (click to see text)	Description		Validation
<a href="#">Access Control 3.1.1<sup>62</sup></a>	Choose a DLP rule to restrict public sharing of CUI.	<p>To guard against unauthorized access to CUI:</p> <ol style="list-style-type: none"> <li>1. Click the edit button, and select a DLP rule that blocks public shares.</li> <li>2. Change any existing public shares to private.</li> </ol>	If the DLP rule exists and is enabled and there are no existing public shares, status is <b>OK</b> ; if not, or if modifications to the rule allow public shares, status is <b>Issues</b> .
<a href="#">Access Control 3.1.8<sup>63</sup></a>	Configure password settings to limit unsuccessful logon attempts.	<p>To set a limit on unsuccessful logon attempts:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Password</b>.</li> <li>2. Configure the setting as follows: <b>Incorrect Password Attempts Before Account Lockout</b> - a value greater than 0.</li> </ol>	If the <b>Incorrect Password Attempts Before Account Lockout</b> setting is set as indicated, then status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">Access Control 3.1.18<sup>64</sup></a>	Set up a workflow that blocks the connection of a new mobile device until it is approved.	<p>To set up a workflow to block the connection of a new mobile device:</p> <ul style="list-style-type: none"> <li>• Go to <b>Workflow &gt; Add Workflow</b> and choose <b>If any new client app connects &gt; Block the device for admin approval</b>.</li> </ul> <p>For information about this workflow, see: <a href="#">Admin Approval Required Workflow</a></p>	If the workflow does not exist or is not enabled, the status is <b>Issues</b> .
<a href="#">Audit and Accountability 3.3.1<sup>65</sup></a>	Set the audit log level.	<p>To monitor log-in attempts:</p> <ul style="list-style-type: none"> <li>• Go to <b>Settings &gt; Admin</b>, and set <b>Audit Log Level</b> to <b>REQUEST</b> or <b>FULL</b>.</li> </ul>	If <b>Audit Log Level</b> is set to <b>OFF</b> , status is <b>Issues</b> .

62. <https://csf.tools/reference/nist-sp-800-171/r2/3-1/3-1-1/>63. <https://csf.tools/reference/nist-sp-800-171/r2/3-1/3-1-8/>64. <https://csf.tools/reference/nist-sp-800-171/r2/3-1/3-1-18/>65. <https://csf.tools/reference/nist-sp-800-171/r2/3-3/3-3-1/>

Rule (click to see text)	Description		Validation
Audit and Accountability 3.3.3 <sup>66</sup>	Confirm admin knows how to use and manage audit reports.	Enable this rule to confirm admin understands audit logs and has a process to regularly review audit records and remove unwanted records.	None
Audit and Accountability 3.3.8 <sup>67</sup>	Confirm admin understands how to disable the deletion of audit records.	To disable deletion of audit records see Delete Audit Log Entries.	None
Audit and Accountability 3.3.9 <sup>68</sup>	Give at least one admin user access to the Audit Reports.	To enable at least one admin user to access the Audit Reports: <ol style="list-style-type: none"> <li>1. Go to <b>Admins</b> and create a role with read access to the Audit Reports.</li> <li>2. Add at least one user to the role.</li> </ol>	If one or more users have access to the Audit Reports, the status is <b>OK</b> ; if not, the status is <b>Issues</b> .
Configuration Management 3.4.2 <sup>69</sup>	Confirm admin understands security settings and knows how to implement reCaptcha, 2FA, and password policies.	Enable this rule to confirm that admin can implement reCaptcha, 2FA, and password policies.	None
Configuration Management 3.4.7 <sup>70</sup>	Confirm admin knows how to disable or change non-essential ports and services.	Enable this rule to confirm that admin can disable or change non-essential ports and services. For information about changing default port or web server settings in FileCloud, see: <a href="#">Changing a Default Port or Web Server Setting</a> .	None

66. <https://csf.tools/reference/nist-sp-800-171/r2/3-3/3-3-3/>

67. <https://csf.tools/reference/nist-sp-800-171/r2/3-3/3-3-8/>

68. <https://csf.tools/reference/nist-sp-800-171/r2/3-3/3-3-9/>

69. <https://csf.tools/reference/nist-sp-800-171/r2/3-4/3-4-2/>

70. <https://csf.tools/reference/nist-sp-800-171/r2/3-4/3-4-7/>

Rule (click to see text)	Description		Validation
<a href="#">Identification and Authentication 3.5.2<sup>71</sup></a>	Configure and enable the <b>Authentication Type</b> as <b>Active Directory</b> or <b>LDAP</b> or enable SSO.	<p>To authenticate users during login:</p> <ul style="list-style-type: none"> <li>• Go to <b>Settings &gt; Authentication</b>, and set <b>Authentication Type</b> to <b>Active Directory</b> or <b>LDAP</b>.</li> </ul> <p>To enable SSO, see: SAML Single Sign-On Support</p>	If <b>Authentication Type</b> is set to <b>Default</b> and SSO is not enabled, status is <b>Issues</b> .
<a href="#">Identification and Authentication 3.5.7<sup>72</sup></a>	Set up strong password management.	<p>To set regulations for strong password management:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Password</b>.</li> <li>2. Configure the settings as follows:  <b>Minimum Password Length</b> - 8 or more.  <b>Enable Strong Passwords</b> - enable.  <b>Disallow Commonly Used Passwords</b> - enable.  <b>User Password Expiration In Days</b> - a value greater than 0. </li> </ol>	If the password settings are set as indicated, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">Identification and Authentication 3.5.8<sup>73</sup></a>	Disallow the reuse of previous passwords.	<p>To disallow the reuse of previous passwords:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Password</b>.</li> <li>2. Configure the setting as follows:  <b>Number of previous passwords that cannot be reused</b> - a value greater than 0. </li> </ol>	If <b>Number of previous passwords that cannot be reused</b> is set as indicated, then status is <b>OK</b> ; if not, status is <b>Issues</b> .

71. <https://csf.tools/reference/nist-sp-800-171/r2/3-5/3-5-2/>

72. <https://csf.tools/reference/nist-sp-800-171/r2/3-5/3-5-7/>

73. <https://csf.tools/reference/nist-sp-800-171/r2/3-5/3-5-8/>

Rule (click to see text)	Description		Validation
<a href="#">Identification and Authentication 3.5.9<sup>74</sup></a>	Require new accounts to change passwords.	<p>To require new accounts to change passwords:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Password</b>.</li> <li>2. Configure the setting as follows: <b>New accounts must change password</b> - enable.</li> </ol>	If <b>New accounts must change password</b> is set as indicated, then the status is <b>OK</b> ; if not, the status is <b>Issues</b> .
<a href="#">Incident Response 3.6.1<sup>75</sup></a>	Confirm admin knows how to use audit, alerts, violation reports, and event reports to create notification reports.	Enable this rule to confirm that admin knows how to use audit logs, alerts and violation reports to generate breach notifications.	None
<a href="#">Maintenance 3.7.4<sup>76</sup></a>	Configure antivirus protection against malicious file uploads.	<p>To protect CUI from malicious file uploads:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Third Party Integrations &gt; Antivirus</b>.</li> <li>2. Configure an <b>Antivirus</b> type.</li> </ol>	If <b>Antivirus</b> is configured, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">Media Protection 3.8.4<sup>77</sup></a>	Choose a metadata set to classify controlled unclassified information	<p>To indicate which files are CUI, click the edit button and select a metadata set with a tag for identifying them.</p> <p>(Use smart classification to apply the metadata tag to the CUI.)</p>	If the metadata set exists and is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .
<a href="#">Media Protection 3.8.6<sup>78</sup></a>	Configure and enable encryption.	<p>To maintain security:</p> <p>Configure storage encryption.</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Storage &gt; Managed Storage</b> and enable encryption.</li> <li>2. Encrypt all existing files.</li> </ol> <p>See Setting Up Managed Storage Encryption in the support document.</p>	If storage is not fully encrypted or any existing files are not fully encrypted, status is <b>Issues</b> .

74. <https://csf.tools/reference/nist-sp-800-171/r2/3-5/3-5-9/>75. <https://csf.tools/reference/nist-sp-800-171/r2/3-6/3-6-1/>76. <https://csf.tools/reference/nist-sp-800-171/r2/3-7/3-7-4/>77. <https://csf.tools/reference/nist-sp-800-171/r2/3-8/3-8-4/>78. <https://csf.tools/reference/nist-sp-800-171/r2/3-8/3-8-6/>

Rule (click to see text)	Description		Validation
Systems and Communi cations Protectio n 3.13.3 <sup>79</sup>	Give at least one user in an admin role access to the Compliance Center.	<p>To enable at least one user to manage the Compliance Center:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Admins</b> and create a role with <b>Compliance</b> access to the Compliance Center.</li> <li>2. In <b>Admins</b>, add at least one user to the role with access to the Compliance Center.</li> </ol>	If one or more users have access to the Compliance Center, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Systems and Communi cations Protectio n 3.13.4 <sup>80</sup>	Choose a DLP rule that only allows private sharing.	<p>To guard against unauthorized access to CUI:</p> <ol style="list-style-type: none"> <li>1. Click the edit button, and select a DLP rule that blocks public shares.</li> <li>2. Change any existing public shares to private.</li> </ol>	If the DLP rule exists and is enabled and there are no existing public shares, status is <b>OK</b> ; if not, or if modifications to the rule allow public shares, status is <b>Issues</b> .
Systems and Communi cations Protectio n 3.13.9 <sup>81</sup>	Set session timeout for the user portal.	<p>To confirm automatic logoff of sessions:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Server</b>, and set <b>Session Timeout</b> to a value greater than 0.</li> </ol>	If <b>Session Timeout</b> is set to <b>0</b> or empty, status is <b>Issues</b> .
Systems and Communi cations Protectio n 3.13.10 <sup>82</sup>	Confirm decryption keys are confidential.	To confirm that decryption keys are confidential, enable this rule.	None
System and Informati on Integrity 3.14.1 <sup>83</sup>	Enable <b>Governance Report Email</b> to send the admin an email reminder to check audit logs, reports, and security issues regularly.	<p>To implement procedures to regularly review records such as audit logs and violation report:</p> <ul style="list-style-type: none"> <li>• Enable <b>Send daily governance report to admin</b> option in <b>Admin</b> settings.</li> </ul>	If the <b>Send daily governance report to admin</b> setting is enabled, status is <b>OK</b> ; if not, status is <b>Issues</b> .

79. <https://csf.tools/reference/nist-sp-800-171/r2/3-13/3-13-3/>80. <https://csf.tools/reference/nist-sp-800-171/r2/3-13/3-13-4/>81. <https://csf.tools/reference/nist-sp-800-171/r2/3-13/3-13-9/>82. <https://csf.tools/reference/nist-sp-800-171/r2/3-13/3-13-10/>83. <https://csf.tools/reference/nist-sp-800-171/r2/3-14/3-14-1/>

## Guide to PDPL Rules in the Compliance Center

This table defines the PDPL rules covered in FileCloud's Compliance Center, explains what steps you must take to be in compliance, and describes how FileCloud validates each rule.

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 1, Section 4 Lawful Processing	Confirm that admins understand how personal data is processed.	<p>Enable this rule to confirm that admins understand how personal data is processed to create or perform the following:</p> <ul style="list-style-type: none"> <li>• Audit records</li> <li>• Alerts</li> <li>• Reports</li> <li>• Activity and share activity in user portal</li> <li>• Notifications</li> </ul>	None
Ch. 1 Section 5 Sensitive Personal Data	Choose a metadata set to classify sensitive personal data, and apply the metadata to files with a smart classification rule.	To indicate which files include sensitive personal data, click the edit button and select a metadata set with a tag for identifying them. Then confirm that a smart classification rule that applies the metadata is enabled.	If the metadata set and the classification rule both exist and are enabled, status is OK; if any part of the condition isn't met, status is Issues.
Ch. 2 Section 2 Withdrawal of Consent	Confirm admins and users understand the process for resetting consent information.	Enable this rule to confirm that admins understand the procedures for withdrawing user consent information.	None
Ch. 2 Section 8 Lawfulness, Fairness, and Transparency	Set up privacy regulations.	<p>To obtain explicit and informed consent from users before processing their data: For each policy:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Policies</b>.</li> <li>2. Open the policy for editing.</li> <li>3. In the <b>General</b> tab, set <b>Enable Privacy Settings</b> to <b>YES</b>, and save.</li> </ol> <p>After you have completed this configuration for each policy:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Privacy</b>.</li> <li>2. Enable <b>Force users to accept TOS when changed</b>.</li> <li>3. Enable <b>Show TOS</b> for every login.</li> </ol>	If the specified settings are set, status is <b>OK</b> ; if not, status is <b>Issues</b> .

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 2 Section 9 Purpose Limitation	Set up terms of service.	<p>To set up data protection principles:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Customization &gt; TOS</b>.</li> <li>2. Set up a TOS that is suitable for your organization.</li> </ol>	If the default TOS is not modified then status is <b>Issues</b> .
Ch. 2 Section 10 Data Minimizat ion	Confirm admins know how to use audit reports.	Enable this rule to confirm admins have a process to regularly review audit records and remove unwanted records.	None
Ch. 2 Section 11 Accuracy	Ensure that system date and time are updated to the user's regional time zone.	Enable this rule to confirm that admins and users understand how to check that records like audit, share activity, and global activity show the system date and time in the correct regional time zone.	None
Ch. 2 Section 12 Storage Limitation	Set up a retention policy to protect files and folders from deletion.	<p>To protect personal data files and folders from deletion:</p> <ul style="list-style-type: none"> <li>• Click the edit button, and select a retention policy to protect personal data files and folders from deletion based on metadata.</li> <li>• Confirm admins understand that after the retention period, files will be completely deleted from the recycle bin.</li> </ul>	If the retention policy exists and is enabled, status is <b>OK</b> ; if not, or if modifications to the retention policy allow file or folder deletion, status is <b>Issues</b> .
Ch. 2 Section 13 Integrity and Confidentiality	Configure and enable encryption.	<p>To maintain security:</p> <ol style="list-style-type: none"> <li>1. Configure storage encryption. See <a href="#">Setting Up Managed Disk Storage Encryption</a> in the support document.</li> <li>2. Go to <b>Settings &gt; Storage &gt; Managed Storage</b> and enable encryption.</li> <li>3. Encrypt all existing files.</li> </ol>	If storage is not fully encrypted, or any existing files are not fully encrypted, status is <b>Issues</b> .
Ch. 3 Section 15 Right of Access	Confirm terms of service indicates where personal data are collected.	To confirm that terms of service indicates where personal data are collected from the data subject, enable this rule.	There are no system checks to verify this; your confirmation is the only verification.

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 3 Section 16 Right of Correctio n	Confirm admins understand how to edit user accounts, and users are aware of the rectification request process.	Enable this rule to confirm that admins and users understand the process of amending personal data.	There are no system checks to verify this; your confirmation is the only verification.
Ch. 3 Section 17 Right to Erasure	Use Anonymize Data.	<p>To confirm the right to be forgotten:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc &gt; Privacy</b>.</li> <li>2. In <b>Anonymous User Consent Message for Accessing Shared Files</b> enter text that explains data subject's right to erasure.</li> <li>3. If a user requests to be forgotten, anonymize the data.</li> </ol> <p>Also see Anonymizing User Data.</p>	If the specified settings are set, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Ch. 3 Section 19 Right to Object to Processin g	Confirm that admins and users know privacy TOS behavior.	<p>To configure users' right to object:</p> <p>For each policy:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Policies</b>.</li> <li>2. Open the policy for editing.</li> <li>3. In the <b>General</b> tab, set <b>Enable Privacy Settings</b> to <b>Yes</b>.</li> </ol> <p>After you have completed this configuration for each policy:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Settings &gt; Misc</b>.</li> <li>2. Click the <b>Privacy</b> tab.</li> <li>3. Enable <b>Show TOS for every login</b>. This option forces users to accept the TOS for every login; if users do not want to accept the condition, they can close the TOS. Please note that on not accepting the TOS, the user will not be able to log in to the user portal.</li> </ol>	If the specified settings are set, status is <b>OK</b> ; if not, status is <b>Issues</b> .

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 3 Section 20 Right to Data Portability	Confirm admins understand option to Export User Files and User activity.	<p>To configure the right to data portability, ensure the following options work in the admin portal, and then enable this rule.</p> <p>Exporting a user's file.</p> <ol style="list-style-type: none"> <li>1. In the navigation pane, click <b>Users</b>.</li> <li>2. Edit a user.</li> <li>3. In the <b>User Details</b> dialog box, click <b>Manage Files</b>, and then click <b>My Files</b>.</li> <li>4. Click <b>Download as Zip</b> for a file, and confirm that the zip download works.</li> </ol> <p>Exporting audit log records.</p> <ol style="list-style-type: none"> <li>1. In the navigation pane, click <b>Audit</b>.</li> <li>2. In the upper-right corner of the screen, click <b>Manage</b>.</li> <li>3. In the <b>Manage Audit Logs</b> dialog box, enter a <b>Start Date</b> and an <b>End Date</b>.</li> <li>4. Click <b>Export</b>, and confirm that the file is exported correctly.</li> </ol>	None
Ch 3 Section 23 Right to be Informed of Data Breaches	Confirm Admin knows how to use audit, alerts, violation and event reports to create notification reports.	To confirm that admins can use audit logs, alerts, and violation reports to generate breach notifications, enable this rule.	None
Ch. 4 Section 29 Data Protection Officer	Give at least one admin access to the Compliance Center.	<p>To enable at least one user to manage the Compliance Center:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Admins</b> and create a role with <b>Compliance</b> access to the Compliance Center.</li> <li>2. In <b>Admins</b>, add at least one user to the role with access to the Compliance Center.</li> </ol>	If one or more users have access to the Compliance Center, status is <b>OK</b> ; if not, status is <b>Issues</b> .
Ch. 6 Section 33 Transfers to Third Countries	Confirm that users and admins understand how to use and manage sharing and folder permissions.	Enable this rule to confirm that users and admins are educated about sharing and folder-level permissions.	None

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 6 Section 34 Transfers to Internatio nal Organizati ons	Confirm admins understand how to set up encryption and anonymization of data.	To confirm that admins understand how to use anonymization and encryption, enable this rule.	None

## FileCloud Web Accessibility (VPAT) Practices

As of Version 20.2, FileCloud has complied with Voluntary Product Accessibility Template (VPAT) guidelines. Below is a list of the guidelines complied with. For a list of guidelines, see <https://www.w3.org/TR/WCAG21/>.

Guideline	Descriptions of requirement and FileCloud's compliance	File Clo ud Ver sio n
1.1 Text alternatives	<p><b>Requirement:</b> Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>Images are associated with alt tags to act as image descriptions.</li> <li>Controls like checkboxes have aria attributes to describe their usage.</li> </ul>	20.3

Guideline	Descriptions of requirement and FileCloud's compliance	File Cloud Version
1.3 Adaptable content	<p><b>Requirement:</b> Create content that can be presented in different ways (for example simpler layout) without losing information or structure.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>The labels for required fields are displayed in red.</li> <li>The labels for checkboxes can be programmatically determined, as they are associated with aria-label attributes.</li> <li>The rows of files are navigable through the keyboard.</li> <li>Keyboard support is included for forms.</li> <li>Screen reader provides context about content when format in which it is presented changes from the original, for example, by indicating the number of search results found or by giving instructions about how to navigate options. Information in interactive elements (like File Operations box) is not marked as a header.</li> </ul> <p><b>Note:</b> Added in FileCloud 23.1 for requirement 1.3.1.</p> <ul style="list-style-type: none"> <li>Wherever possible, data tables are programmatically marked to show relationships between table headers and table cells.</li> </ul> <p><b>Note:</b> Added in FileCloud 23.1 for requirements 1.3.1 and 1.3.2.</p>	20.3
1.4 Distinguishable	<p><b>Requirement:</b> Make it easier for users to see and hear content including separating foreground from background.</p> <p><b>FileCloud compliance:</b> The new UI enables high contrast mode, which makes the visual presentation of blocks of text and icons easily readable.</p>	
2.1 Keyboard Accessible	<p><b>Requirement:</b> Make all functionality available from a keyboard.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>Keyboard accessibility is supported in FileCloud, and enables users to submit forms or navigate using keyboard shortcuts and keyboard navigation.</li> <li>The <b>Details</b> section in My Files is keyboard accessible.</li> </ul> <p><b>Note:</b> Added in FileCloud 23.1 for requirement 2.1.1. See Guide to Keyboard Shortcuts.</p>	
2.2.5 Re-authenticating	<p><b>Requirement:</b> When an authenticated session expires, the user can continue the activity without loss of data after re-authenticating.</p> <p><b>FileCloud compliance:</b> When an authenticated session expires, the user can continue the activity after re-authenticating.</p>	

Guideline	Descriptions of requirement and FileCloud's compliance	File Cloud Version
2.4 Navigable	<p><b>Requirement:</b> Provide ways to help users navigate, find content, and determine where they are.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>• In FileCloud, keyboard accessibility enables users to navigate through file lists and tab through fields in forms. See Guide to Keyboard Shortcuts.</li> <li>• A link for skipping navigation enables users to skip repetitive navigation information on pages and directly access the main content.</li> </ul> <p><b>Note:</b> Added in FileCloud 23.1 for requirement 2.4.1.</p> <ul style="list-style-type: none"> <li>• Interactive elements such as table headers are read in tab order, and focus order of tables is top to bottom and left to right.</li> </ul> <p><b>Note:</b> Added in FileCloud 23.1 for requirement 2.4.3.</p>	
3.1 Readable	<p><b>Requirement:</b> Make text content readable and understandable.</p> <p><b>FileCloud compliance:</b> The lang attribute in HTML tags changes so that it can be easily read in the language of the site. Many non-text parts of the site are associated with alternative texts to make them readable.</p>	
3.2 Predictable	<p><b>Requirement:</b> Make Web pages appear and operate in predictable ways.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>• Drop-down lists are keyboard-navigable.</li> <li>• Focus is set to the first input field in forms.</li> </ul>	
3.3 Input Assistance	<p><b>Requirement:</b> Help users avoid and correct mistakes.</p> <p><b>FileCloud compliance:</b> All form input fields have proper labels and validation of inputs in place. Errors are shown if a form submission fails.</p>	

Guideline	Descriptions of requirement and FileCloud's compliance	File Cloud Version
4.1 Compatible	<p><b>Requirement:</b> Maximize compatibility with current and future user agents, including assistive technologies.</p> <p><b>FileCloud compliance:</b></p> <ul style="list-style-type: none"> <li>• Newest user interface uses well-formed HTML with proper Start and End tags. The tags have aria label, name, and role attributes associated with them.</li> <li>• Screen reader indicates whether elements are buttons or links. <b>Note:</b> Added in FileCloud 23.1 for requirement 4.1.2.</li> <li>• Screen reader informs users when new data is loaded on the page or dynamic content appears. <b>Note:</b> Added in FileCloud 23.1 for requirement 4.1.3.</li> </ul>	

# Retention Policies



Retention Policies are available for the Enterprise editions of FileCloud. Learn more about differences in features<sup>84</sup>between editions.

As an administrator, you can create Retention policies to automate some of the processing related to protecting files and their folder groupings. This policy-based automation is designed to help secure digital content for compliance, but it can also enhance the management of digital content for other business reasons.

- Retention policies are created and attached to files and folders.
- These special policies allow you to define the conditions that enforce a set of restrictions on how each file or folder can be manipulated.
- For example, you can create a Retention Policy that disables a user's ability to delete any of the files and folders named in the policy.

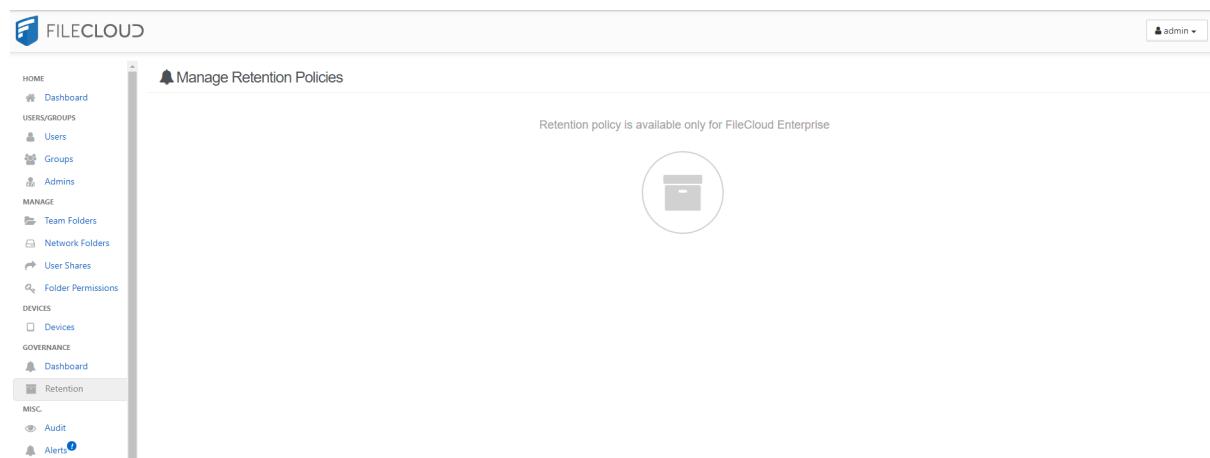
[How Retention Policies Function \(see page 77\)](#)

[Create a Type of Retention Policy \(see page 48\)](#)

## Are You Seeing This Screen?

This screen appears when the Retention features are not enabled for the system.

- Retention can be manually disabled by an Administrator. For more information, please contact Support
- Retention is available in Enterprises Licenses. To upgrade, please contact Support



84. <https://www.filecloud.com/pricing/>

## Create a Type of Retention Policy

There are five different types of retention policies that can be configured and assigned.

Policy Type	Description
<b>Admin Hold</b>	<ul style="list-style-type: none"> <li>Prevents any update or delete of digital content for an indefinite period of time</li> <li>Admin Hold policies applied to folders can be removed</li> <li>Admin policies applied to files can be removed</li> </ul> <p><a href="#">Create an Admin Hold policy (see page 53)</a></p>
<b>Legal Hold</b>	<ul style="list-style-type: none"> <li>Freezes digital content to aid discovery or legal challenges</li> <li>During a legal hold, file modifications are not allowed</li> <li>Holds cannot be reversed once applied</li> </ul> <p><a href="#">Create a Legal Hold policy (see page 48)</a></p>
<b>Retention</b>	<ul style="list-style-type: none"> <li>Identifies digital content to be kept around for an unlimited amount of time before being deleted or released</li> <li>Retention policies cannot be reversed once applied</li> </ul> <p><a href="#">Create a Retention policy (see page 66)</a></p>
<b>Archival</b>	<ul style="list-style-type: none"> <li>Moves and stores old organizational content, for example, to a more cost effective systems for long term</li> <li>No Deletion is allowed until a specific time period is reached</li> <li>After the specified time period is reached, content gets moved to a specific folder or location</li> </ul> <p><a href="#">Create an Archival policy (see page 58)</a></p>
<b>Trash Retention</b>	<ul style="list-style-type: none"> <li>Controls if files can permanently be deleted off the FileCloud Server system</li> <li>Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions</li> </ul> <p><a href="#">Create a Trash Retention policy (see page 71)</a></p>

## Create a Legal Hold Policy



A Legal Hold is designed to retain data, therefore, there is no deletion or move option available when this policy is in effect.

⚠ Legal Holds cannot be removed once applied unless an expiration fixed date is set.

The following table identifies what actions are blocked for a Legal Hold type of retention policy.

Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Legal Hold	NO	YES	NO	YES	YES	<ul style="list-style-type: none"> <li>• Fixed Date</li> <li>• Indefinite</li> </ul>	<ul style="list-style-type: none"> <li>• No Action</li> </ul>



Copies cannot be created if there is a retention hold on the destination folder that prevents updates.

## What is a Use Case for a Legal Hold?

In the world of litigation, a legal hold is a notification

- It is sent from an organization's legal team to employees
- It instructs them not to delete electronically stored information (ESI)
- It also instructs them not to discard any paper documents that may be relevant to a new or imminent legal case.

FileCloud allows administrators to place a legal hold on ESI.

- FileCloud's Legal Hold policy prevents any of the attached file to be moved
- FileCloud's Legal Hold policy prevents any of the attached file to be changed in any way
- FileCloud's Legal Hold policy prevents any of the attached file to be deleted (either for a fixed number of days or indefinitely)

## Creating the Policy

Manage Retention Policies

Cron Last Run Date/Time: Jan 12, 2021 6:00 AM  Effective Policy

Filter	Filter by policy name	Show 10 Items		
Policy Name	Description	Status	Policy Type	Actions

No matching results found

### To create a Legal Hold 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.

**4. Completely fill out the Policy Attributes section.**

Policy Attributes

Policy Name

Policy Type

**Legal Hold**

Locks digital content to aid discovery or legal challenges. This policy can be removed by the admin.

Description

Hide Policy From Users  ⓘ

Enabled  ⓘ

Alert On Violation  ⓘ

Send email alert  ⓘ

Alerts

Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select <i>Legal Hold</i>
Description	<ul style="list-style-type: none"> <li>Required</li> <li>A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab</li> </ul>

Property	Description
<b>Hide Policy from Users</b>	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
<b>Alert on Violation</b>	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
<b>Send email alert</b>	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>ℹ</b> The same information is available on the Governance dashboard. The Governance Dashboard lists 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.</p>
<b>Alerts</b>	<p>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.</p>

## 5. Attach folders or files in the Apply Policy To section.

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

Apply Policy To

Paths	Metadata
<b>Add Path</b>	
Path	Actions
/teams/Data Governance	<span style="color: red;">X</span>

Page 1 of 1

## 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
<ul style="list-style-type: none"> <li>Paths work for <i>managed storage</i> ONLY</li> <li>Since managed storage includes Team Folders, you CAN add a path to a Team Folder</li> <li>A Path takes the form of: <code>/username/sub-folder</code></li> <li>You can add more than 1 path</li> <li>You can set BOTH a path and specify metadata</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to <i>network folders</i></li> <li>You CANNOT add a path to <i>external folders</i></li> <li>You CANNOT add a path to <i>shared folders</i></li> <li>You CANNOT add a path to protected folders, such as <code>/boot</code>, <code>/root</code>, and <code>/var</code> in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy will be enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however.</p> <p>At a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist <code>/username/</code></li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist</li> </ul> <p>This will prevent you from saving the policy</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="margin: 0;">ERROR</p> <p style="margin: 0; color: #ccc;">Failed to add new retention policy. Failed to add new Retention policy definition.</p> <p style="margin: 0; background-color: #f0f0f0; padding: 2px;">Reason: Retention policy definition is invalid. conditions: Incorrect path specified - only paths for existing users / team folders are accepted</p> </div>

## 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 and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

For more information about metadata, see (23.253) Managing Metadata.

## 6. Set the Expiry Actions

Legal holds can expire in either a Fixed Date or be set to Indefinite.

The screenshot shows the 'Actions' section of a configuration interface. It includes the following elements:

- Expiry Date** (with a help icon):  
 Time Period  Fixed Date  Indefinite
- Expiry Date** (text input field)
- Policy Expiry Actions** (with a help icon):  
 No Action

### To set a fixed date:

1. In the Actions section, choose **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.

## Create an Admin Hold Policy

An Admin hold only blocks user access, it does not block other policies from expiring. However, if an Admin Hold is in place, any other policies will expire gracefully without completing any move or delete expiry options.

- For Admin Holds, a policy expiration date cannot be set

- The policy can only be removed by an administrator
- Since the policy does not expire on a specific date, there are no automatic actions on expiration

The following table identifies what actions are blocked for an Admin Hold type of retention policy.

Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Admin Hold	NO	YES	NO	YES	YES	• Indefinite	• No Action



Copies cannot be created if there is a retention hold on the destination folder that prevents updates.

## What is a Use Case for an Admin Hold?

For example:

1. An administrator looks at the Governance dashboard and sees that a Retention with Deletion policy is about to expire on files that have been kept for 3 years.
2. The Retention with Deletion policy will delete 200 files when it expires in 2 days.
3. However, the administrator notices that some of these files have been recently updated.
4. The Administrator puts an Admin Hold policy in place on the files in the Retention with Deletion policy that is about to expire.
5. The Administrator can now investigate the files without worrying about users updating them at the same time.
6. However, it takes the Administrator 3 days to identify which files should not be deleted and which can be deleted.
7. During this time, the Retention with Deletion policy expires, but because of the Admin Hold, no files are removed.
8. The Administrator removes the Admin Hold from the files.
9. The Administrator removes the files that don't need to be saved from FileCloud.
10. A new Retention with No Deletion policy is created for the remaining files that need to be saved.

## Creating the Policy

The screenshot shows the 'Manage Retention Policies' page. At the top, there is a header with a 'Manage Retention Policies' icon, the date 'Cron Last Run Date/Time: Jan 12, 2021 6:00 AM', a checked 'Effective Policy' checkbox, and a '+ Add Policy' button. Below the header is a search bar with a 'Filter' button and a 'Filter by policy name' input field. To the right of the search bar is a 'Show 10 Items' dropdown. The main area contains a table with columns: 'Policy Name', 'Description', 'Status', 'Policy Type', and 'Actions'. A message 'No matching results found' is displayed below the table. An orange arrow points to the '+ Add Policy' button.

**To create an Admin Hold 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.

**4. Completely fill out the Policy Attributes section.**

**Add Retention Policy** X

**Policy Attributes**

Policy Name  
DPO\_Admin

Policy Type  
Retention  
Archival  
Legal Hold  
Trash Retention  
**Admin Hold**

Suspend any action to files due to other retention policies that might affect them.

Description

Hide Policy From Users

Enabled

Alert On Violation

Send email alert

Alerts  
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Admin Hold

Property	Description
Description	<ul style="list-style-type: none"> <li>Required</li> <li>A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab</li> </ul>
Hide Policy from Users	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
Alert on Violation	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
Send email alert	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>ⓘ</b> The same information is available on the Governance dashboard. The Governance Dashboard lists 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.</p>
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.

## 5. Attach folders or files in the Apply Policy To section.

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

Apply Policy To

Paths	Metadata
<b>Add Path</b>	
Path	Actions
/teams/Data Governance	<span style="color: red;">X</span>

Page 1 of 1

## 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
<ul style="list-style-type: none"> <li>Paths work for <i>managed storage</i> ONLY</li> <li>Since managed storage includes Team Folders, you CAN add a path to a Team Folder</li> <li>A Path takes the form of: <code>/username/sub-folder</code></li> <li>You can add more than 1 path</li> <li>You can set BOTH a path and specify metadata</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to <i>network folders</i></li> <li>You CANNOT add a path to <i>external folders</i></li> <li>You CANNOT add a path to <i>shared folders</i></li> <li>You CANNOT add a path to protected folders, such as <code>/boot</code>, <code>/root</code>, and <code>/var</code> in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy will be enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however.</p> <p>At a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist / <code>username/</code></li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist</li> </ul> <p>This will prevent you from saving the policy</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="margin: 0;">ERROR</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc; margin-top: 5px;"> <p style="margin: 0;">Failed to add new retention policy. Failed to add new Retention policy definition. Reason: Retention policy definition is invalid. conditions: Incorrect path specified - only paths for existing users / team folders are accepted</p> </div> <p style="text-align: right; margin: 0;">Close</p> </div>

## 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:

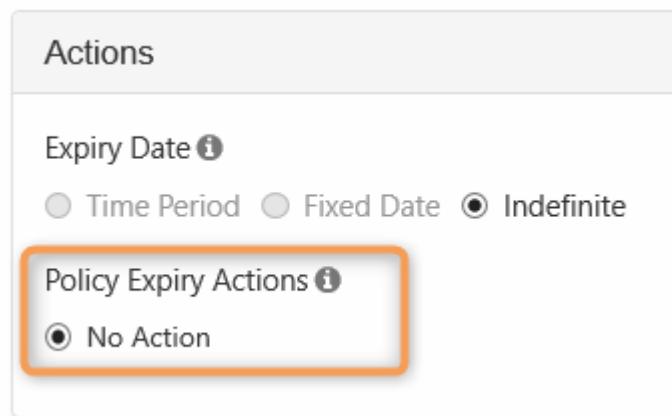
- Default sets = provided with FileCloud and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

For more information about metadata, see [Managing Metadata](#).

## 6. Set the Expiry Actions

An administrative hold is designed to help an administrator block access to files and folders so that they can determine what should happen next.

- For Admin Holds, a policy expiration date cannot be set
- The policy can only be removed by an administrator
- Since the policy does not expire on a specific date, there are no automatic actions on expiration



## Create an Archival Policy

An Archival policy type is designed to help you create a more cost effective systems for long term.

Therefore, you can create a policy to move and store old organizational content in the following ways:

- If you choose No Action, you will see an error that it is not supported and you will not be able to create the policy
- After the specified time period is reached, content gets moved to a specific folder or location (**Archive**)

The following table identifies what actions are blocked for an Archival type of retention policy.

Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Retention	NO	NO	NO	NO	YES	<ul style="list-style-type: none"> <li>• Time Period</li> <li>• Fixed Date</li> </ul>	<ul style="list-style-type: none"> <li>• Move files to a specific location</li> </ul>

### What is a use case for an Archival Policy?

This type of policy helps an administrator plan for the future by setting up a process to run automatically when the time comes.

For example:

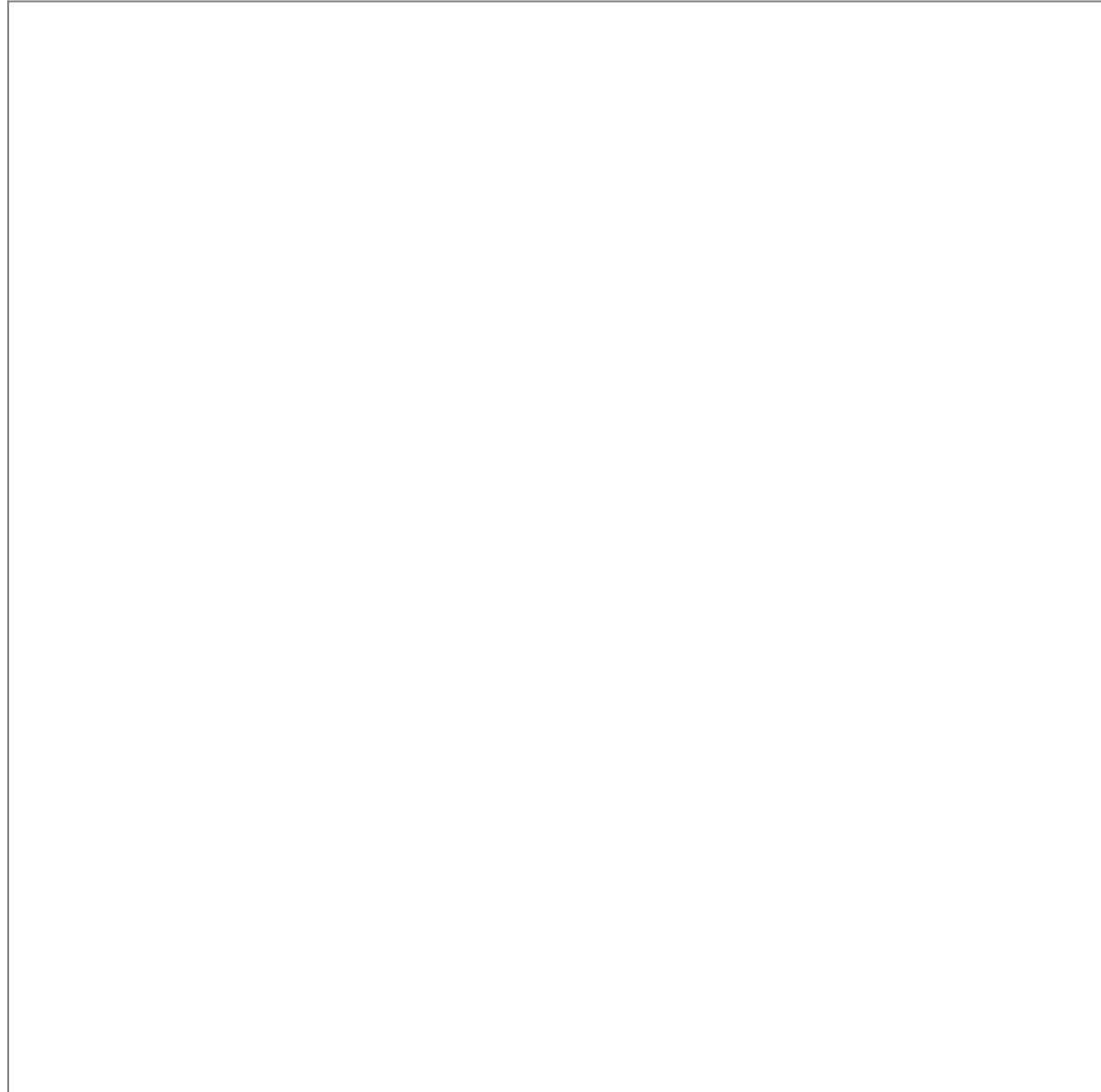
1. If phone records only have to be accessible in the system for 5 years, but stored for at least 10 years, then the Administrator doesn't have to just remember to move the current phone records in 5 years into storage.
2. The administrator can just create an Archival policy to move them automatically in 5 years.

This also allows a process to run independent of an employee's length of service.

For example:

If the same employee is no longer an Administrator in 5 years, but the old records still need to be moved, they will be.

## Creating the Policy



### **To create an Archival 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.

**4. Completely fill out the Policy Attributes section.**

### Policy Attributes

Policy Name

Policy Type

Archival

Moves and stores files in specified directories. This policy cannot be modified or removed once set by the admin.

Description

Hide Policy From Users 

Enabled 

Alert On Violation 

Send email alert 

Alerts

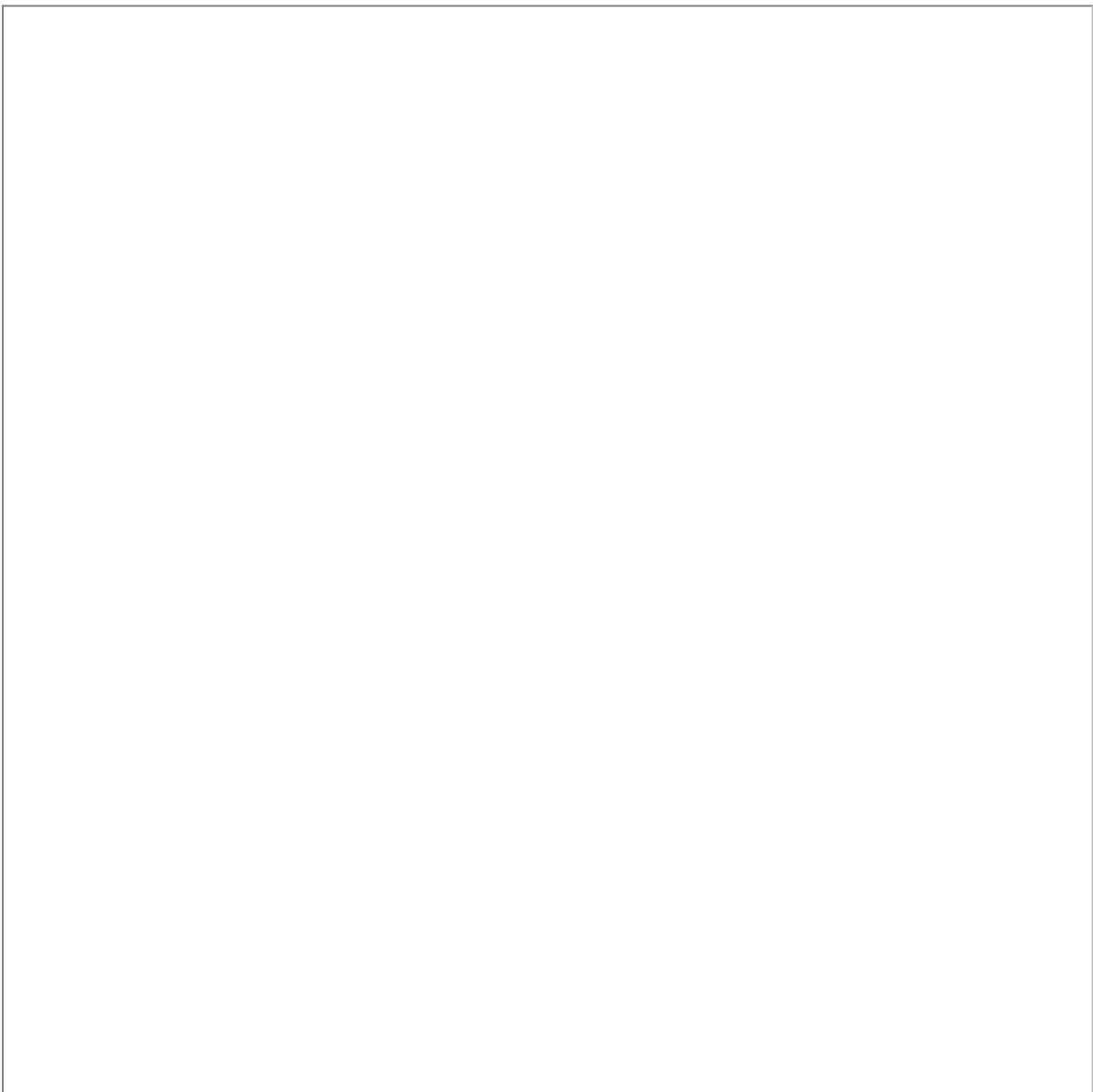
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select <i>Archival</i>
Description	<ul style="list-style-type: none"> <li>Required</li> <li>A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab</li> </ul>

Property	Description
<b>Hide Policy from Users</b>	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
<b>Alert on Violation</b>	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
<b>Send email alert</b>	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>ℹ</b> The same information is available on the Governance dashboard. The Governance Dashboard lists 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.</p>
<b>Alerts</b>	<p>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.</p>

## 5. Attach folders or files in the **Apply Policy To** section.

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
<ul style="list-style-type: none"> <li>Paths work for managed storage ONLY</li> <li>Since managed storage includes Team Folders, you CAN add a path to a Team Folder</li> <li>A Path takes the form of: /username/sub-folder</li> <li>You can add more than 1 path</li> <li>You can set BOTH a path and specify metadata</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to network folders</li> <li>You CANNOT add a path to external folders</li> <li>You CANNOT add a path to shared folders</li> <li>You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy will be enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however.</p> <p>At a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist / username/</li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist</li> </ul> <p>This will prevent you from saving the policy</p>

## 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 and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

For more information about metadata, see [Managing Metadata](#).

## 6. Set the Expiry Actions

You can configure an Archival policy to expire in a set Time Period or at a Fixed Date.

	<p><b>To set a Time Period:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, click <b>Time Period</b>.</li> <li>2. In <b>Time Period of Retention</b>, click the down arrow.</li> <li>3. From the list, you can select a built-in option:           <ol style="list-style-type: none"> <li>a. 30 days</li> <li>b. 60 days</li> <li>c. 1 year</li> <li>d. 2 years</li> </ol> </li> <li>4. From the list, you can also select <b>Custom</b>.           <ol style="list-style-type: none"> <li>a. In No. of days, type in a whole number greater than 0.</li> </ol> </li> </ol> <p><b>To set a fixed date:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, click <b>Fixed Date</b>.</li> <li>2. Click in the <b>Expiry Date</b> text box.</li> <li>3. A calendar will be shown with the current month.</li> <li>4. Select a date from the calendar.</li> </ol>				
	<p><b>Renew Expiry on Access:</b> this is a set number of days or years that is used to calculate when the policy expires based on the <u>last access date</u>.</p> <p><span style="color: yellow;">!</span> Available only if the <b>Time Period</b> option is set, and selected by default.</p> <table border="1" data-bbox="616 1343 1378 1709"> <thead> <tr> <th data-bbox="616 1343 1013 1410">Renew Expiry on Access</th><th data-bbox="1013 1343 1378 1410">Expiration Date</th></tr> </thead> <tbody> <tr> <td data-bbox="616 1410 1013 1709">           For example, if on March 2, 2019, for an X-ray, you set expiry to:           <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul> </td><td data-bbox="1013 1410 1378 1709">           Then the policy will expire on May 2, 2019 UNLESS:           <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul>           Then the 60-day time period will be reset to July 1, 2019.         </td></tr> </tbody> </table> <p><span style="color: yellow;">!</span> The ACTUAL date is reset by a user every time they access the file.</p> <p><b>To set Renew Expiry On Access:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, next to <b>Renew Expiry on Access</b>, make sure the checkbox is selected.</li> </ol>	Renew Expiry on Access	Expiration Date	For example, if on March 2, 2019, for an X-ray, you set expiry to: <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	Then the policy will expire on May 2, 2019 UNLESS: <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> Then the 60-day time period will be reset to July 1, 2019.
Renew Expiry on Access	Expiration Date				
For example, if on March 2, 2019, for an X-ray, you set expiry to: <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	Then the policy will expire on May 2, 2019 UNLESS: <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> Then the 60-day time period will be reset to July 1, 2019.				

	<p>When a Retention policy expires, you can configure it to allow access to or delete the attached files and folders.</p> <p><b>To set Policy Expiry Actions:</b></p> <ol style="list-style-type: none"> <li>1. In <b>Policy Expiry Actions</b>, select either:           <ol style="list-style-type: none"> <li>a. <b>No Action</b> : Although this option is available, if you select it you will get an error and will not be able to save the policy</li> <li>b. <b>Archive</b> : After the specified time period or fixed date is reached, content is moved to a specific folder or location</li> </ol> </li> <li>2. If you select <b>Archive</b>, in <b>Archive Path</b> you must type in a path to the location where the files are moved.</li> </ol>
--	--

## Create a Retention Policy

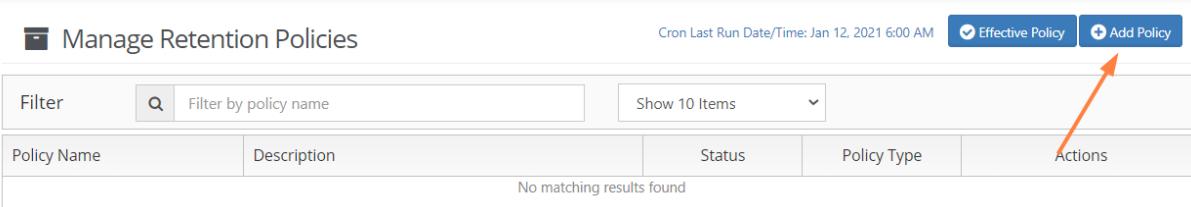
A Retention policy allows an organization to identify specific content that is required to be stored for a specific period of time before it can be accessed. During the retention period, the content cannot be deleted.

⚠ 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	<ul style="list-style-type: none"> <li>• Time Period</li> <li>• Fixed Date</li> <li>• Indefinite</li> </ul>	<ul style="list-style-type: none"> <li>• Delete</li> <li>• No Action</li> </ul>

## Creating the Policy



Manage Retention Policies

Cron Last Run Date/Time: Jan 12, 2021 6:00 AM  Effective Policy

Filter	Filter by policy name	Show 10 Items		
Policy Name	Description	Status	Policy Type	Actions
No matching results found				

### 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.

**4. Completely fill out the Policy Attributes section.**

**Policy Attributes**

Policy Name

Policy Type  
Retention ▼

Retention 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 or archived.

Description

Hide Policy From Users i

Enabled i

Alert On Violation i

Send email alert i

Alerts

Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Retention
Description	<ul style="list-style-type: none"> <li>Required</li> <li>A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>This description is displayed in the User Portal when the cursor hovers over the <b>Policy Name</b> in the Details tab</li> </ul>

Property	Description
<b>Hide Policy from Users</b>	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
<b>Alert on Violation</b>	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
<b>Send email alert</b>	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>ℹ</b> The same information is available on the Governance dashboard. The Governance Dashboard lists 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.</p>
<b>Alerts</b>	<p>A list of email addresses separated by a comma specifying who will receive the email notification that there are only 7 days until the policy expires.</p>

## 5. Attach folders or files in the **Apply Policy To** section.

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

Apply Policy To

Paths	Metadata
<b>Add Path</b>	
Path	Actions
/teams/Data Governance	<span style="color: red;">X</span>

Page 1 of 1

## 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
<ul style="list-style-type: none"> <li>Paths work for managed storage only</li> <li>Since managed storage includes Team Folders, you can add a path to a Team Folder</li> <li>A Path takes the form of: /username/sub-folder</li> <li>You can add more than 1 path</li> <li>You can both set a path and specify metadata</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to network folders</li> <li>You CANNOT add a path to external folders</li> <li>You CANNOT add a path to shared folders</li> <li>You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click <b>Add</b> to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy is enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however, at a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist /username/</li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist. This will prevent you from saving the policy</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="margin: 0;">ERROR</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc; margin-top: 5px;"> <p style="margin: 0;">Failed to add new retention policy. Failed to add new Retention policy definition. Reason: Retention policy definition is invalid. conditions: Incorrect path specified - only paths for existing users / team folders are accepted</p> </div> <p style="text-align: right; margin: 0;">Close</p> </div>

## 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.

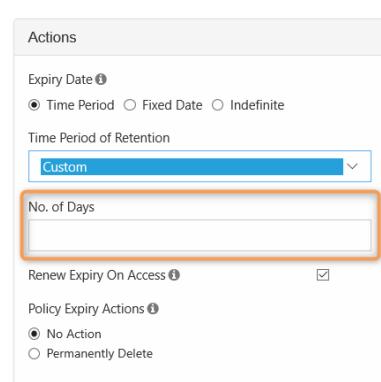
You can select metadata from the following existing attributes or sets:

- Default sets = provided with FileCloud and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

For more information about metadata, see [Managing Metadata](#).

## 6. Set the Expiry Actions

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



**To set a Time Period:**

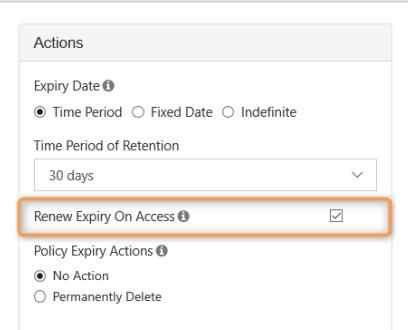
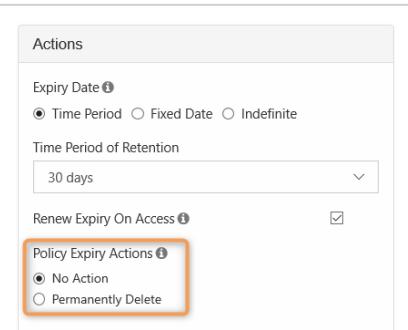
1. In the Actions section, click **Time Period**.
2. In **Time Period of Retention**, click the down arrow.
3. From the list, you can select a built-in option:
  - a. 30 days
  - b. 60 days
  - c. 1 year
  - d. 2 years
4. From the list, you can also select **Custom**.
  - a. In **No. of days**, type 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 is shown with the current month.
4. Select a date from the calendar.

**To set an Indefinite date:**

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

	<p><b>Renew Expiry on Access:</b> this is a set number of days or years that is used to calculate when the policy expires based on the <a href="#">last access date</a>.</p> <p><b>⚠ Available only if the Time Period option is set and selected by default.</b></p> <table border="1" data-bbox="609 467 1383 833"> <thead> <tr> <th data-bbox="609 467 1002 541">Renew Expiry on Access</th><th data-bbox="1002 467 1383 541">Expiration Date</th></tr> </thead> <tbody> <tr> <td data-bbox="609 541 1002 833">           For example, if on March 2, 2019, for an X-ray, you set expiry to:           <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul> </td><td data-bbox="1002 541 1383 833">           Then the policy will expire on May 2, 2019 UNLESS:           <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul>           Then the 60-day time period will be reset to July 1, 2019.         </td></tr> </tbody> </table> <p><b>💡 The ACTUAL date is reset by a user every time they access the file.</b></p> <p><b>To set Renew Expiry On Access:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, next to <b>Renew Expiry on Access</b>, make sure the checkbox is selected.</li> </ol>	Renew Expiry on Access	Expiration Date	For example, if on March 2, 2019, for an X-ray, you set expiry to: <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	Then the policy will expire on May 2, 2019 UNLESS: <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> Then the 60-day time period will be reset to July 1, 2019.
Renew Expiry on Access	Expiration Date				
For example, if on March 2, 2019, for an X-ray, you set expiry to: <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	Then the policy will expire on May 2, 2019 UNLESS: <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> Then the 60-day time period will be reset to July 1, 2019.				
	<p>When a Retention policy expires, you can configure it to allow access to or delete the attached files and folders.</p> <p><b>To set Policy Expiry Actions:</b></p> <ol style="list-style-type: none"> <li>1. In <b>Policy Expiry Actions</b>, select either:       <ol style="list-style-type: none"> <li>a. <b>No Action</b> : Allow users to access the files again and delete them if they want</li> <li>b. <b>Permanently Delete</b> : Delete all the files that have this policy attached from the system, without retaining them in the Trash bin</li> </ol> </li> </ol>				

## Create a Trash Retention Policy

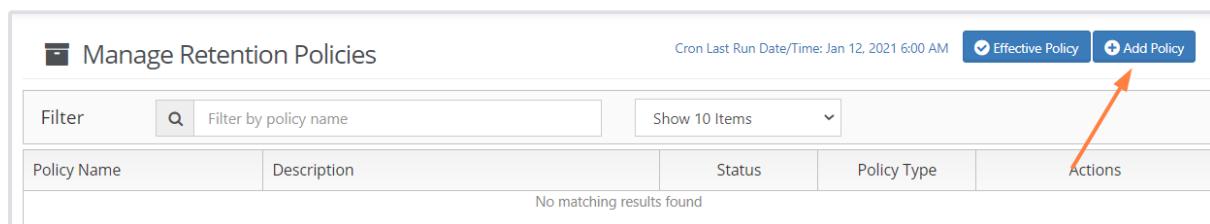
A Trash Retention policy is designed to help you control if files in the Trash Bin can be permanently deleted from FileCloud.

**⚠ If files in the Trash Bin are permanently deleted from FileCloud, they cannot be recovered.**

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

Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Trash Retention	NO	NO	NO	NO	YES	<ul style="list-style-type: none"> <li>Time Period</li> <li>Fixed Date</li> <li>Indefinite</li> </ul>	<ul style="list-style-type: none"> <li>Permanently Delete</li> <li>No Action</li> </ul>

## Creating the Policy



The screenshot shows the 'Manage Retention Policies' interface. At the top, there is a header with a trash icon, the title 'Manage Retention Policies', a Cron status message 'Cron Last Run Date/Time: Jan 12, 2021 6:00 AM', a checked checkbox for 'Effective Policy', and a blue 'Add Policy' button. Below the header is a search bar with a 'Filter' dropdown and a 'Show 10 Items' dropdown. The main area is a table with columns: 'Policy Name', 'Description', 'Status', 'Policy Type', and 'Actions'. A message 'No matching results found' is displayed below the table. An orange arrow points to the 'Add Policy' button.

### To create a Trash 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.
4. Completely fill out the Policy Attributes section.

### Policy Attributes

Policy Name

Policy Type

**Trash Retention** ▼

Trash Retention allows administrators to control who can permanently delete files off the system where they cannot be recovered.

Description

Hide Policy From Users

Enabled

Alert On Violation

Send email alert

Alerts

Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select <b>Trash Retention</b>
Description	<ul style="list-style-type: none"> <li>• Required</li> <li>• A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>• This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab</li> </ul>

Property	Description
Hide Policy from Users	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
Alert on Violation	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
Send email alert	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>ℹ</b> 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.</p>
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.

## 5. Attach folders or files in the Apply Policy To section.

The Path tab allows you to define the conditions that specify how the policy will be applied in the system.

Apply Policy To

Paths				
<input type="text" value="Path"/> <span>Add</span>				
<table border="1"> <thead> <tr> <th>Path</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td colspan="2">No results found</td> </tr> </tbody> </table>	Path	Actions	No results found	
Path	Actions			
No results found				

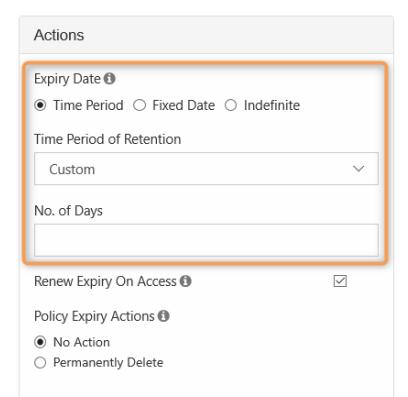
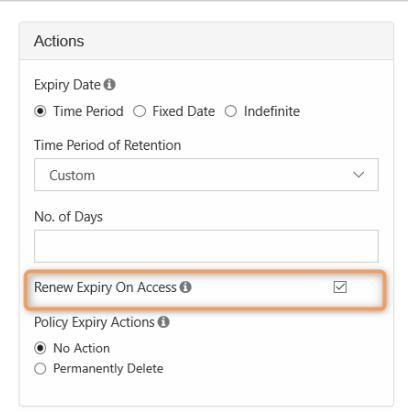
## Add a Path

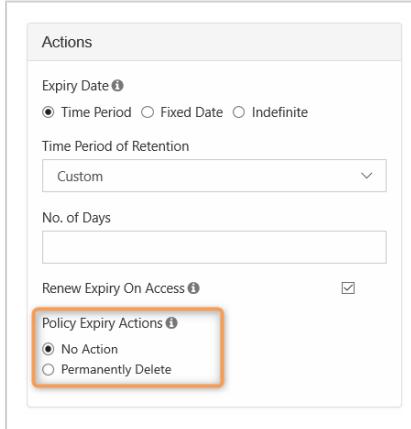
**Add Path** allows you to define a folder that a policy will apply to as well as all the files and sub-folders it contains.

What you CAN do in the Path field	What you CANNOT do in the Path field
<ul style="list-style-type: none"> <li>Paths work for managed storage only</li> <li>Since managed storage includes Team Folders, you can add a path to a Team Folder</li> <li>A Path takes the form of: /username/sub-folder</li> <li>You can add more than 1 path</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to network folders</li> <li>You CANNOT add a path to external folders</li> <li>You CANNOT add a path to shared folders</li> <li>You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click <b>Add</b> to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy will be enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however, at a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist /username/</li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist</li> </ul> <p>This prevents you from saving the policy</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>ERROR</p> <p>Failed to add new retention policy. Failed to add new Retention policy definition. Reason: Retention policy definition is invalid. conditions: Incorrect path specified - only paths for existing users / team folders are accepted</p> <p><span style="float: right;">Close</span></p> </div>

## 6. Set the Expiry Actions

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

	<p><b>To set a Time Period:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, click <b>Time Period</b>.</li> <li>2. In <b>Time Period of Retention</b>, click the down arrow.</li> <li>3. From the list, you can select a built-in option:             <ol style="list-style-type: none"> <li>a. 30 days</li> <li>b. 60 days</li> <li>c. 1 year</li> <li>d. 2 years</li> </ol> </li> <li>4. From the list, you can also select <b>Custom</b>.             <ol style="list-style-type: none"> <li>a. In <b>No. of days</b>, type in a whole number greater than 0.</li> </ol> </li> </ol> <p><b>To set a fixed date:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, click <b>Fixed Date</b>.</li> <li>2. Click in the <b>Expiry Date</b> text box.</li> <li>3. A calendar will be shown with the current month.</li> <li>4. Select a date from the calendar.</li> </ol> <p><b>To set an Indefinite date:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, click <b>Indefinite</b>.</li> </ol>				
	<p><b>Renew Expiry on Access:</b> this is a set number of days or years that is used to calculate when the policy expires based on the <u>last access date</u>.</p> <p><b>⚠ Available only if the Time Period option is set and selected by default.</b></p> <table border="1" data-bbox="616 1185 1378 1556"> <thead> <tr> <th data-bbox="616 1185 1013 1260">Renew Expiry on Access</th> <th data-bbox="1013 1185 1378 1260">Expiration Date</th> </tr> </thead> <tbody> <tr> <td data-bbox="616 1260 1013 1556"> <p>For example, if on March 2, 2019, for an X-ray, you set expiry to:</p> <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul> </td><td data-bbox="1013 1260 1378 1556"> <p>Then the policy will expire on May 2, 2019 UNLESS:</p> <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> <p>Then the 60-day time period will be reset to July 1, 2019.</p> </td></tr> </tbody> </table> <p><b>💡 The ACTUAL date is reset by a user every time they access the file.</b></p> <p><b>To set Renew Expiry On Access:</b></p> <ol style="list-style-type: none"> <li>1. In the Actions section, next to <b>Renew Expiry on Access</b>, make sure the checkbox is selected.</li> </ol>	Renew Expiry on Access	Expiration Date	<p>For example, if on March 2, 2019, for an X-ray, you set expiry to:</p> <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	<p>Then the policy will expire on May 2, 2019 UNLESS:</p> <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> <p>Then the 60-day time period will be reset to July 1, 2019.</p>
Renew Expiry on Access	Expiration Date				
<p>For example, if on March 2, 2019, for an X-ray, you set expiry to:</p> <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul>	<p>Then the policy will expire on May 2, 2019 UNLESS:</p> <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> <p>Then the 60-day time period will be reset to July 1, 2019.</p>				



When a Trash Retention policy expires, you can configure it to allow access to or permanently 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

## How Retention Policies Work

Retention policy is a name that can apply to any of these types of policies:

- Admin Hold
- Legal Hold
- Archival
- Retention
- Trash Retention

Retention policy types allow you to:

1. Block specific actions on files and folders
2. Specify what happens when the policy expires

## What Do You Want to Understand?

[What All Policies Have In Common \(see page 77\)](#)

[How Policies Differ \(see page 86\)](#)

[How Policies Interact \(see page 92\)](#)

Monitor retention policy activity

## What All Policies Have In Common

All Retention Policy types have these attributes:

### Policies Inherit

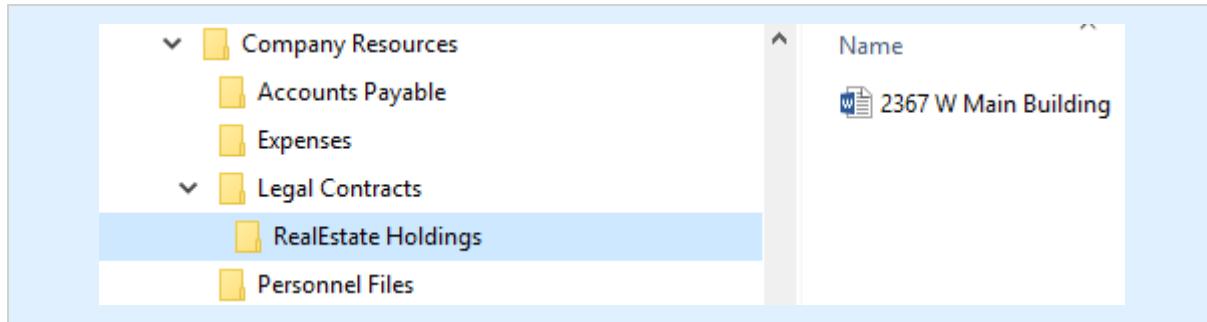
If you set a policy on a folder, all sub-files and sub-folders inherit the policy when it is enabled.

A policy setting inside a hierarchical structure is:

- passed from parent to children
- from children to grandchildren

This is termed *inheritance*. Inheritance will always occur, but it can be blocked or enforced based on the policies that are applied at each level.

For example, The Cherry Road Brokerage company creates this folder structure in FileCloud:



**PARENT to CHILD INHERITANCE**

**CHILDREN to GRANDCHILDREN INHERITANCE**

<p>In the folder for all of the company's real estate holdings, all of these contracts are for leases that last for 1 year.</p> <ul style="list-style-type: none"> <li>• This means the Administrator needs to keep all the files in the RealEstate Holdings folder for 1 year.</li> </ul> <p>To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 1 year.</p> <p>When the policy is created:</p> <ul style="list-style-type: none"> <li>• The RealEstate Holdings folder cannot be deleted for 1 year</li> <li>• The document in this folder cannot be deleted for 1 year: 2367 W Main Building.docx</li> <li>• Any new files added to the RealEstate Holdings folder cannot be deleted for 1 year</li> </ul> <p><b>To prevent a file with a longer retention period than its folder from being deleted when the folder's retention period is reached:</b></p> <ul style="list-style-type: none"> <li>• A folder with a retention policy on it can only be deleted when the file it contains with the longest retention period is deleted. Therefore, the retention policy on a folder can change when a file it contains is given a longer retention period. But the other files the folder contains maintain their original briefer retention period.</li> </ul> <p>For example, The RealEstate Holdings folder has a 1 year retention period which is applied to all its files. Then the retention policy on one file is increased to 5 years. As a result, the retention policy on the RealEstate Holdings folder is increased to 5 years, but the retention policies on the other files it contains remain at 1 year.</p>	<p>Now let's say that due to tax regulations, all legal contracts need to be retained for 5 years.</p> <ul style="list-style-type: none"> <li>• This means the Administrator needs to keep all the files in the Legal Contracts folder for 5 years.</li> </ul> <p>To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 5 years.</p> <p>When the policy is created:</p> <ul style="list-style-type: none"> <li>• No file in the Legal Contracts folder can be deleted for 5 years</li> <li>• The RealEstate Holdings folder now cannot be deleted for 5 years</li> <li>• No file in the RealEstate Holdings folder can be deleted for 5 years</li> <li>• The document in the RealEstate Holdings folder: 2367 W Main Building.docx now has 2 policies applied</li> <li>• On the 2367 W Main Building.docx file, the retention policy to block any files from being deleted for 5 years becomes effective and the policy to retain the file for 1 year is not effective</li> <li>• The document in the RealEstate Holdings folder: 2367 W Main Building.docx now cannot be deleted for 5 years</li> </ul>
--	--

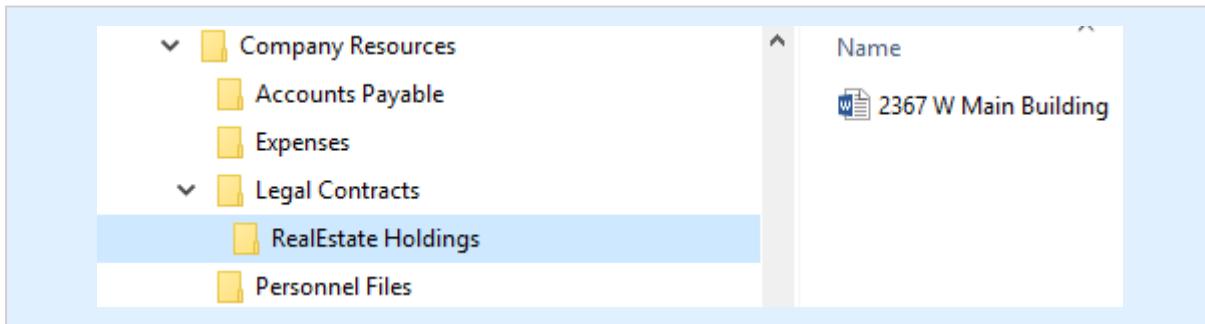
## Policies Stick

Once you apply a policy to a file or folder, no matter where that object goes in the FileCloud System, the policy information will be retained.

- The policy will be retained, but may not be in effect if a higher-ranking policy is inherited or applied

**Note:** When a file is restored from the recycle bin, it does not maintain the retention policy.

For example, The Cherry Road Brokerage company creates this folder structure in FileCloud:



ORIGINAL POLICY ASSIGNMENT	POLICY ASSIGNMENT AFTER MOVES
<p>In the folder for all of the company's real estate holdings, all of these contracts are for leases that last for 1 year.</p> <ul style="list-style-type: none"> <li>This means the Administrator needs to keep all the files in the RealEstate Holdings folder for 1 year.</li> </ul> <p>To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 1 year.</p> <p>When the policy is created:</p> <ul style="list-style-type: none"> <li>The RealEstate Holdings folder cannot be deleted for 1 year</li> <li>The document in this folder cannot be deleted for 1 year: 2367 W Main Building.docx</li> <li>Any new files added to the RealEstate Holdings folder cannot be deleted for 1 year</li> </ul>	<p>Now let's say that tenants at 2367 W Main pay their rent for the entire year.</p> <ul style="list-style-type: none"> <li>The administrator is asked to move the file to the Accounts Payable folder</li> <li>The building will still be occupied, so the file still needs to be retained for 1 year</li> <li>The Accounts Payable folder has a retention policy based on a custom metadata set for financial documents</li> </ul> <p>When the file is moved:</p> <ul style="list-style-type: none"> <li>The document 2367 W Main Building.docx now lives in the Accounts Payable folder</li> <li>The document 2367 W Main Building.docx keeps the retention policy for 1 year</li> <li>The document 2367 W Main Building.docx inherits the Accounts Payable retention policy based on metadata even though it does not meet the metadata condition of being a financial document</li> </ul>

## Files and Folders Are Attached to Policies

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

Apply Policy To

Paths	Metadata				
<a href="#">Add Path</a> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Path</th> <th style="text-align: center;">Actions</th> </tr> </thead> <tbody> <tr> <td style="text-align: center; padding: 5px;">/teams/Data Governance</td> <td style="text-align: center; padding: 5px; vertical-align: middle;"> <span style="color: red;">×</span> </td> </tr> </tbody> </table>		Path	Actions	/teams/Data Governance	<span style="color: red;">×</span>
Path	Actions				
/teams/Data Governance	<span style="color: red;">×</span>				

«
»
Page
1
of 1
»

## 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
<ul style="list-style-type: none"> <li>Paths work for managed storage only</li> <li>Since managed storage includes Team Folders, you can add a path to a Team Folder</li> <li>A Path takes the form of: /username/sub-folder</li> <li>You can add more than 1 path</li> <li>You can both set a path and specify metadata</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT add a path to network folders</li> <li>You CANNOT add a path to external folders</li> <li>You CANNOT add a path to shared folders</li> <li>You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX</li> <li>You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path</li> </ul>
<ul style="list-style-type: none"> <li>The full path must exist before the policy will be enforced</li> </ul> <p>When creating the policy the full path doesn't have to exist, however.</p> <p>At a minimum:</p> <ul style="list-style-type: none"> <li>The first component of the path has to already exist / username/</li> <li>This means that the username or team folder has to already exist before you can save the policy</li> </ul>	<ul style="list-style-type: none"> <li>You CANNOT specify a path that does not exist</li> </ul> <p>This will prevent you from saving the policy</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px; width: fit-content;"> <p style="margin: 0;">ERROR</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc; margin-top: 5px;"> <p style="margin: 0;">Failed to add new retention policy. Failed to add new Retention policy definition. Reason: Retention policy definition is invalid. conditions: Incorrect path specified - only paths for existing users / team folders are accepted</p> </div> <p style="text-align: right; margin-top: 5px; margin-right: 10px;">Close</p> </div>

## 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 and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

For more information about metadata, see [Managing Metadata](#).

For example, [The Cherry Road Brokerage](#) company creates this custom metadata in FileCloud:

Term	Description	Cherry Road Example
<b>Set</b>	A set of metadata attributes that might be logically grouped and can be attached as a single entity to File Objects.  In this example, The Cherry Road Brokerage company creates a set called Building Profile that contains 5 attributes	Building Profile <ul style="list-style-type: none"> <li>• Address</li> <li>• Photo</li> <li>• Square Feet</li> <li>• Leasing Status</li> <li>• Maintenance Status</li> </ul>
<b>Attribute</b>	A single piece of information that describes the File Object.  In this example, The Cherry Road Brokerage company creates an attribute called Address which identifies where the building is, such as 2367 W Main  A tag is also defined called State which allows searches for properties by State, such as Texas.	Address <ul style="list-style-type: none"> <li>• State</li> </ul>
<b>Attribute</b>	A single piece of information that describes the File Object.  In this example, The Cherry Road Brokerage company creates an attribute called Photo  A tag is also defined called Color which allows searches for properties that have color photos.	Photo <ul style="list-style-type: none"> <li>• Color</li> </ul>

Term	Description	Cherry Road Example
Attribute	<p>A single piece of information that describes the File Object.</p> <p>In this example, The Cherry Road Brokerage company creates an attribute called Square Feet</p> <p>Two tags are also defined to allow for property searches by a range of square feet.</p>	<p>Square Feet</p> <ul style="list-style-type: none"> <li>• 0-1500</li> <li>• 1500-3000</li> </ul>
Attribute	<p>A single piece of information that describes the File Object.</p> <p>In this example, The Cherry Road Brokerage company creates an attribute called Leasing Status which identifies the building as occupied or vacant.</p>	Leasing Status
Attribute	<p>A single piece of information that describes the File Object.</p> <p>In this example, The Cherry Road Brokerage company creates an attribute called Maintenance Status which identifies the building as In Repair or No Repair.</p>	Maintenance Status

Now, when an administrator needs to configure a Legal Hold policy for properties that are 1,500 square feet or larger in the state of Texas, they can use this metadata to apply the policy to all files that meet these conditions even if they are not in the same folder.

Apply Policy To

Paths Metadata

Building Profile Square Feet

Tags 1500-3000

Add

Set	Attribute	Value	Actions
Building Profile	State	Texas	<span style="border: 1px solid #ccc; padding: 2px 5px; background-color: #005a9c; color: white; text-decoration: none;">Edit</span>

Page 1 of 1

## General Attributes

The following properties exist for all retention policy types and do not change how the policy functions.

### Add Retention Policy

**Policy Attributes**

Policy Name  
DPO\_Admin

Policy Type  
Retention  
Archival  
Legal Hold  
Trash Retention  
**Admin Hold**

Suspend any action to files due to other retention policies that might affect them.

Description

Hide Policy From Users

Enabled

Alert On Violation

Send email alert

Alerts  
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Description	<ul style="list-style-type: none"> <li>Required</li> <li>A string of characters, letters, and numbers that provide details about why the policy is necessary</li> <li>This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab.</li> </ul>

Property	Description
<b>Hide Policy from Users</b>	<ul style="list-style-type: none"> <li>Prevents policy details from being shown and leaked.</li> <li>Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal.</li> <li>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.</li> <li>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.</li> </ul> <p><b>⚠</b> 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.</p>
<b>Alert on Violation</b>	<p>Displays an alert in the Admin portal on the Governance dashboard.</p> <p><b>⚠</b> 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.</p>
<b>Send email alert</b>	<p>Notifies all provided recipients that there are only 7 days until the policy expires.</p> <p><b>i</b> The same information is available on the Governance dashboard. The Governance Dashboard lists 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.</p>
<b>Alerts</b>	<p>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.</p>



#### Notes:

#### Retention Policies and Versioning

When a file is protected by any type of retention policy, file versions are updated using the following logic:

- Users will not have the option to 'Make version live' to protect the current file version from being deleted
- Files with a retention policy assigned will automatically work as if the 'Unlimited number of versions' setting is selected

Files without a retention policy applied will follow normal versioning behavior.

## How Policies Differ

The most important ways that policy types differ is:

1. What actions are blocked
2. How long the policy is effective
3. What happens when a policy expires

The following table identifies what actions are blocked for each type of retention policy.

Policy Type	Reads Blocked	Moves Blocked	Copies Blocked	Updates Blocked	Deletes Blocked	Policy Length	Expiration Actions
Admin Hold	NO	YES	NO	YES	YES	• Indefinite	• No Action
Legal Hold	NO	YES	NO	YES	YES	• Fixed Date • Indefinite	• No Action
Archival	NO	NO	NO	NO	YES	• Time Period • Fixed Date	• Archive to a path
Retention	NO	NO	NO	NO	YES	• Time Period • Fixed Date • Indefinite	• Delete • No Action
Trash Retention	NO	NO	NO	NO	YES	• Time Period • Fixed Date • Indefinite	• Permanently Delete • No Action

## How Policy Lengths Differ

**⚠** Any time you configure when a policy should expire, keep in mind that all expiration dates are dictated by when the next Cron job is run.

You can specify when a policy should expire.

- This helps an administrator set up a process to run automatically in the future. For example, if phone records only have to be kept for 5 years, then the Administrator doesn't have to remember to delete current records in 5 years.
- This allows a process to run independent of an employee's length of service. For example, if the same employee is no longer an Administrator in 5 years, but the old records still need to be deleted, they will be.

The following options can be selected depending on which type of Retention Policy you are creating:

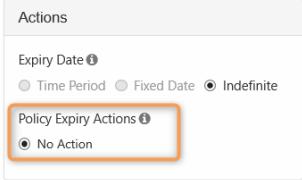
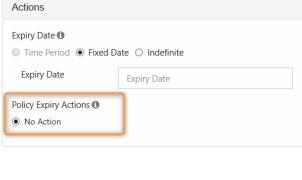
Policy Length	Available on Types	Description	
<b>Indefinite</b>	<ul style="list-style-type: none"> <li>• Admin Hold</li> <li>• Legal Hold</li> <li>• Retention</li> <li>• Trash Retention</li> </ul>	<p>A policy never expires.</p> <p>For example, if you are required to retain accounting records for the entire length of your company's existence, you can never delete your accounting records</p>	<p>Expiry Date </p> <p><input type="radio"/> Time Period <input checked="" type="radio"/> Fixed Date <input type="radio"/> Indefinite</p>
<b>Fixed Date</b>	<ul style="list-style-type: none"> <li>• Legal Hold</li> <li>• Archival</li> <li>• Retention</li> <li>• Trash Retention</li> </ul>	<p>The date a policy expires with no exceptions.</p> <p>This means you are locked out of the policy at 11:59:59 PM on that calendar date.</p> <p>Policy expiration is end of day (midnight), UTC adjusted.</p> <p>The ACTUAL expire time is the time of the next Cron run.</p> <ul style="list-style-type: none"> <li>• If the next Cron run isn't for another 24 hours, the policy will expire 24 hours later at midnight</li> <li>• If you want the policy to expire exactly at midnight, you can always force a Cron run</li> </ul>	<p>Expiry Date </p> <p><input type="radio"/> Time Period <input checked="" type="radio"/> Fixed Date <input type="radio"/> Indefinite</p> <p>Expiry Date <input type="text" value=""/></p>

Policy Length	Available on Types	Description	
<b>Time Period - not Renewed on Access</b>	<ul style="list-style-type: none"> <li>• Archival</li> <li>• Retention</li> <li>• Trash Retention</li> </ul>	<p>A set number of days or years that is used to calculate when the policy expires based on the <u>creation date</u>.</p> <p>For example, if a file is created on March 1, 2019 and you select 30 days, the policy on that file will expire on April 1, 2019.</p> <p>You can select from:</p> <ul style="list-style-type: none"> <li>• 30 days</li> <li>• 60 days</li> <li>• 90 days</li> <li>• 1 year</li> <li>• 2 years</li> <li>• Custom</li> </ul>	<p>Expiry Date  <input checked="" type="radio"/> Time Period <input type="radio"/> Fixed Date <input type="radio"/> Indefinite</p> <p>Time Period of Retention</p> <p>30 days </p> <p>Renew Expiry On Access  <input type="checkbox"/></p>
<b>Time Period - Renewed on Access</b>	<ul style="list-style-type: none"> <li>• Archive</li> <li>• Retention</li> <li>• Trash Retention</li> </ul>	<p>A set number of days or years that is used to calculate when the policy expires based on the <u>last access date</u>.</p> <p>For example, if on March 2, 2019, for an X-ray, you set expiry to:</p> <ul style="list-style-type: none"> <li>• Time Period = 60 days</li> <li>• Renew on Access = selected</li> </ul> <p>Then the policy will expire on May 2, 2019 UNLESS:</p> <ul style="list-style-type: none"> <li>• If a doctor previews the file before May 2, say on May 1, 2019</li> </ul> <p>Then the 60-day time period will be reset to July 1, 2019.</p> <p>The ACTUAL date is reset by a user every time they access the file.</p>	<p>Expiry Date  <input checked="" type="radio"/> Time Period <input type="radio"/> Fixed Date <input type="radio"/> Indefinite</p> <p>Time Period of Retention</p> <p>60 days </p> <p>Renew Expiry On Access  <input checked="" type="checkbox"/></p>

## How Expiration Actions Differ

When a policy expires, you can configure it to move or delete files. This is another way that policies interact with files.

Expiration actions allow you to provide any special instructions for use of the content after the policy expires.

Policy Type	Expiration Actions	Notes
Admin Hold	 <p>An administrative hold is designed to help an administrator block access to files and folders so that they can determine what should happen next.</p> <p><b>1</b> An Admin hold only blocks user access, it does not block other policies from expiring. However, if an Admin Hold is in place, any other policies will expire gracefully without completing any move or delete expiry options.</p> <ul style="list-style-type: none"> <li>• For Admin Holds, a policy expiration date cannot be set</li> <li>• The policy can only be removed by an administrator</li> <li>• Since the policy does not expire on a specific date, there are no automatic actions on expiration</li> </ul> <p>For example:</p> <ol style="list-style-type: none"> <li>1. An administrator looks at the Governance dashboard and sees that a Retention with Deletion policy is about to expire on files that have been kept for 3 years.</li> <li>2. The Retention with Deletion policy will delete 200 files when it expires in 2 days.</li> <li>3. However, the administrator notices that some of these files have been recently updated.</li> <li>4. The Administrator puts an Admin Hold policy in place on the files in the Retention with Deletion policy that is about to expire.</li> <li>5. The Administrator can now investigate the files without worrying about users updating them at the same time.</li> <li>6. However, it takes the Administrator 3 days to identify which files should not be deleted and which can be deleted.</li> <li>7. During this time, the Retention with Deletion policy expires, but because of the Admin Hold, no files are removed.</li> <li>8. The Administrator removes the Admin Hold from the files.</li> <li>9. The Administrator removes the files that don't need to be saved from FileCloud.</li> <li>10. A new Retention with No Deletion policy is created for the remaining files that need to be saved.</li> </ol>	
Legal Hold	 <p>A Legal Hold is designed to retain data, therefore, there is no deletion or move option available when the policy expires.</p> <p><b>⚠</b> Legal Holds cannot be reversed once applied unless they are set to expire after a fixed number of days</p>	

Policy Type	Expiration Actions	Notes
Retention		<p>Retention policies are designed to keep digital content around for a specified amount of time.</p> <p>When a retention policy expires, it can automatically:</p> <ul style="list-style-type: none"> <li>Allow users to access the files again and delete them if they want (<b>No Action</b>)</li> <li>Delete all the files that have this policy attached from the system, without retaining them in the Trash bin (<b>Permanently Delete</b>)</li> </ul> <p><b>⚠️</b> Retention policies cannot be reversed once applied</p>
Archival		<p>An Archival policy type is designed to help you create a more cost effective systems for long term.</p> <p>Therefore, you can create a policy to move and store old organizational content in the following ways:</p> <ul style="list-style-type: none"> <li>If you choose <b>No Action</b>, you will see an error that it is not supported and you will not be able to create the policy</li> <li>After the specified time period is reached, content gets moved to a specific folder or location (<b>Archive</b>)</li> </ul> <p>This type of policy helps an administrator plan for the future by setting up a process to run automatically when the time comes.</p> <p>For example:</p> <ol style="list-style-type: none"> <li>If phone records only have to be accessible in the system for 5 years, but stored for at least 10 years, then the Administrator doesn't have to just remember to move the current phone records in 5 years into storage.</li> <li>The administrator can just create an Archival policy to move them automatically in 5 years.</li> </ol> <p>This also allows a process to run independent of an employee's length of service.</p> <p>For example: if the same employee is no longer an Administrator in 5 years, but the old records still need to be moved, they will be.</p>
Trash Retention		<p>The Trash Retention policy is designed to help you control if files in the Trash Bin can be permanently deleted from FileCloud.</p> <ul style="list-style-type: none"> <li>You can allow the policy to automatically and permanently delete all files in the Trash bin when the policy expires</li> <li>You can allow the policy to expire with no actions - thereby using this policy to control how long files and folders are retained in the trash before being completely removed</li> </ul>

## Policy Types Cheat Sheet

As an administrator, you can create Retention policies to automate some of the processing related to protecting files and their folder groupings. This policy-based automation is designed to help secure digital content for compliance, but it can also enhance the management of digital content for other internal reasons.

- Retention policies are created and attached to files and folders.
- These special policies allow you to define the conditions that enforce a set of restrictions on how each file or folder can be manipulated.
- For example, you can create a Retention Policy that disables a user's ability to delete or edit any of the files and folders named in the policy.

To resolve the issue of conflicting policies, FileCloud ranks retention policies by what best protects and retains the digital content. There are five different types of retention policies that can be configured and assigned.

Policy Type	Rank	Description
<b>Admin Hold</b>	1	<ul style="list-style-type: none"> <li>• Outranks all other policies</li> <li>• Is outranked by no other policy</li> </ul> <p><a href="#">Create an Admin Hold policy (see page 53)</a></p>
<b>Legal Hold</b>	2	<ul style="list-style-type: none"> <li>• Outranks policies 3,4,5,6,7</li> <li>• Is outranked by Admin Hold</li> </ul> <p><a href="#">Create a Legal Hold policy (see page 48)</a></p>
<b>Retention - Indefinite</b>	3	<ul style="list-style-type: none"> <li>• Outranks policies 4,5,6,7</li> <li>• Is outranked by Admin and Legal Holds</li> </ul> <p><a href="#">Create a Retention policy (see page 66)</a></p>
<b>Archival</b>	4	<ul style="list-style-type: none"> <li>• Outranks policies 5,6,7</li> <li>• Is outranked by Admin Hold</li> <li>• Is outranked by Legal Hold</li> <li>• Is outranked by Retention -Indefinite</li> </ul> <p><a href="#">Create an Archival policy (see page 58)</a></p>

Policy Type	Rank	Description
Retention - No delete on expiry	5 <ul style="list-style-type: none"> <li>Outranks policies 6 and 7</li> <li>Is outranked by Admin Hold</li> <li>Is outranked by Legal Hold</li> <li>Is outranked by Retention - Indefinite</li> <li>Is outranked by Archival</li> </ul>	<ul style="list-style-type: none"> <li>Allows an organization to identify specific content that is required to be stored for a specific period of time before it can be disposed.</li> <li>During the retention period, the content cannot be deleted.</li> <li>Retention - No delete on expiry doesn't delete the content upon policy expiration</li> <li>Retention policies cannot be reversed once applied</li> </ul> <p>Create a Retention policy (<a href="#">see page 66</a>)</p>
Retention - Delete on expiry	6 <ul style="list-style-type: none"> <li>Outranks policy 7</li> <li>Is outranked by Admin Hold</li> <li>Is outranked by Legal Hold</li> <li>Is outranked by Retention - Indefinite</li> <li>Is outranked by Archival</li> <li>Is outranked by Retention - No delete on expiry</li> </ul>	<ul style="list-style-type: none"> <li>Allows an organization to identify specific content that is required to be stored for a specific period of time before it can be accessed.</li> <li>During the retention period, the content cannot be deleted.</li> <li>Retention - Delete on expiry deletes the content upon policy expiration</li> <li>Retention policies cannot be reversed once applied</li> </ul> <p>Create a Retention policy (<a href="#">see page 66</a>)</p>
Trash Retention	7 <ul style="list-style-type: none"> <li>Outranks no other policies</li> <li>Is outranked by all other policies</li> </ul>	<ul style="list-style-type: none"> <li>Controls if files can permanently be deleted completely from FileCloud</li> <li>Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions</li> </ul> <p>Create a Trash Retention policy (<a href="#">see page 71</a>)</p>

## How Policies Interact

As an administrator, you can configure how policies interact with file objects and each other in the following ways:

- Using the Enabled Setting to apply a policy to all files or only to keep it on existing files

- Using the Effective property to manage multiple policies attached to a single file or folder

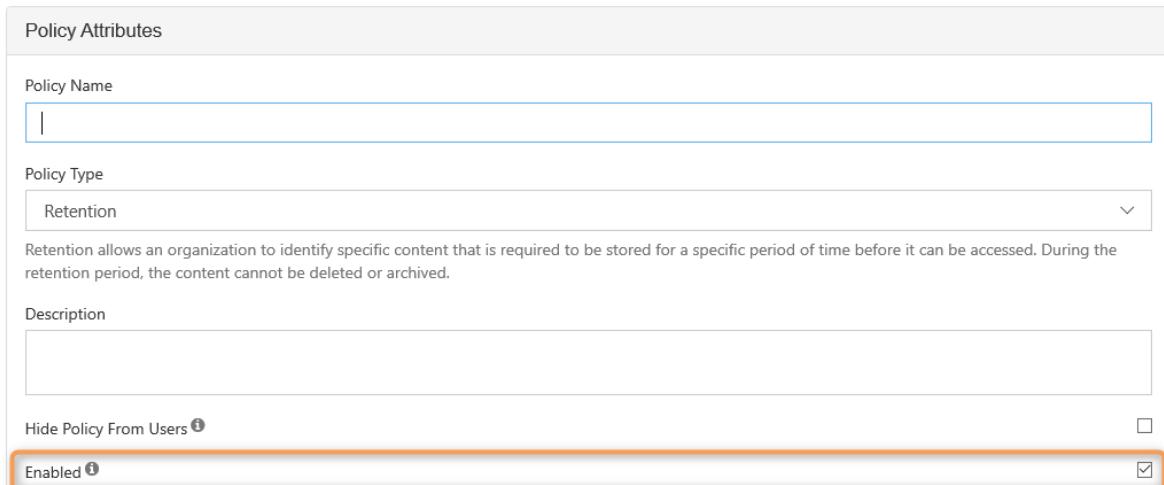
## Enabled Setting

Using the Enabled Setting, policies can interact with new and existing files differently.

This setting determines whether new files and folders that meet ANY of the policy conditions will have the policy assigned.

- ✓ If enabled, the policy is assigned to files and folders
- ✗ If not enabled, FileCloud will:
  - Stop applying the policy to new file objects
  - Keep the policy in place for file objects already attached

### The Enabled Setting

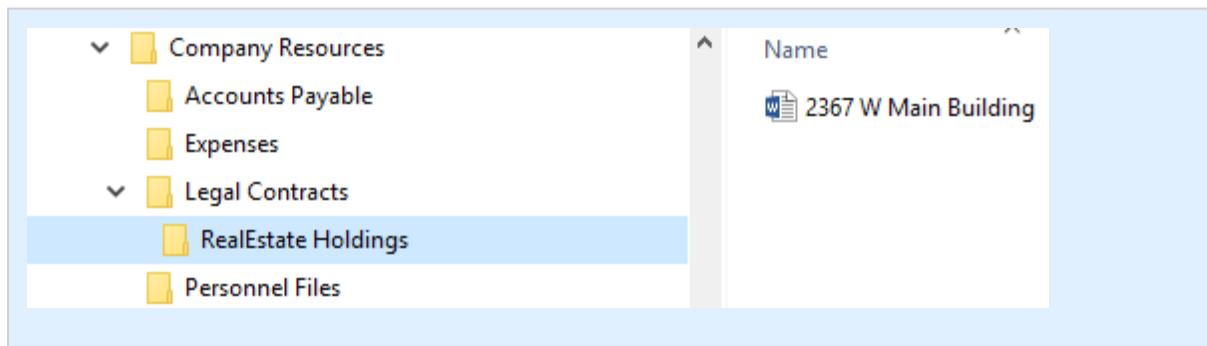


The screenshot shows the 'Policy Attributes' configuration screen. It includes fields for 'Policy Name' (empty), 'Policy Type' (set to 'Retention'), a description area (empty), and two checkboxes: 'Hide Policy From Users' (unchecked) and 'Enabled' (checked). The 'Enabled' checkbox is highlighted with a thick orange border.

- This option is available for all policy types
- By default, it is selected

The Enabled setting does not stop any currently assigned policies from being in effect, it only stops the application of the policy to any new file objects (files and folders).

For example, [The Cherry Road Brokerage](#) company creates this folder structure in FileCloud Server:



1. The administrator creates a retention policy to stop any file from being deleted in the RealEstate Holdings folder.
2. The file for 2367 W Main Building is added to the RealEstate Holdings folder, and the retention policy is applied to it.
3. Now, the administrator wants to allow any new files added to the RealEstate Holdings folder to be deleted.
4. The administrator edits the retention policy, and clears the checkbox for *Enabled*, thereby disabling the policy.

How does the original retention policy interact with files when DISABLED?

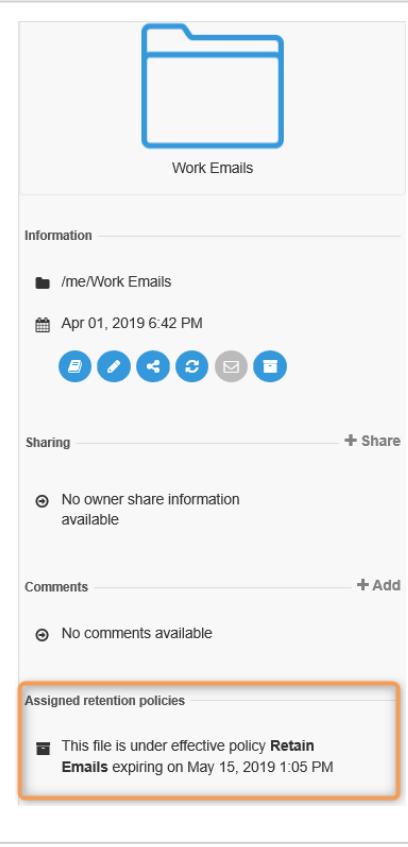
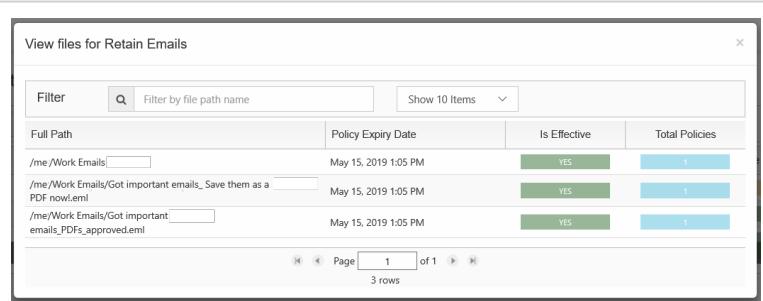
1. A new file called 98675 E Orchard Drive is added to the RealEstate Holdings folder, and the retention policy is NOT applied.
2. Since the new file, 98675 E Orchard Drive does not have the retention policy applied, it CAN be deleted.
3. However, the 2367 W Main Building file still has the policy applied and CANNOT be deleted.

How does the original retention policy interact with files when RE-ENABLED?

1. The administrator edits the retention policy, and selects the checkbox for *Enabled*, thereby re-enabling the policy.
2. FileCloud re-applies the policy to all files in the RealEstate Holdings folder.
3. The 2367 W Main Building file still has the policy applied and CANNOT be deleted.
4. The new file, 98675 E Orchard Drive now has the policy applied and CANNOT be deleted.
5. Now, another new file is added to the RealEstate Holdings folder for 3654 S Blossom Road, and the policy is applied and the file CANNOT be deleted.

To determine if a specific file has a policy applied to it:

In the USER Portal	In the ADMIN Portal
--------------------	---------------------

	 <p>When using the Admin portal, you will need to know the name of the policy that the file belongs to.</p> <p>Then you can view all files for the policy to check if it is attached.</p>
<ol style="list-style-type: none"> <li>1. Log in to the Admin Portal.</li> <li>2. From the left navigation pane, select <b>Retention</b>.</li> <li>3. On the Manage Retention Policies screen, select the policy row.</li> <li>4. In that row, click the Edit Policy icon (  ).</li> <li>5. Clear the checkbox for <b>Hide Policy from Users</b>.</li> <li>6. Log in to the User Portal.</li> <li>7. Browse to the file.</li> <li>8. Look in the Details tab for the Assigned retention policies.</li> </ol>	<ol style="list-style-type: none"> <li>1. Log in to the Admin Portal.</li> <li>2. From the left navigation pane, select <b>Retention</b>.</li> <li>3. On the Manage Retention Policies screen, select the policy row.</li> <li>4. In that row, click the View Files icon (  ).</li> <li>5. The View files for the policy screen opens.</li> </ol>

## Effective Property

You can attach multiple policies to a single file or folder, however, only one policy will be in effect at a time. You can tell which policy is active by the Effective label.

## Multiple Policies Interaction

Since you can create different types of policies and attach multiple types of policies to one file or folder, policies will interact with each other.

To manage this, FileCloud ranks retention policies by what best protects and retains the digital content.

- If a file or folder has more than one policy applied to it, only one policy will be in effect.
- This is determined by policy rankings and is displayed on the Retention dashboard as Effective.

### The Effective Property

The following table describes what will happen if multiple policies are applied to a file or folder. Once a policy expires or is removed, the next policy in order of rank, will become effective. However, some policies can never be removed and will block the other policies from becoming effective.

For example, [The Cherry Road Brokerage](#) company adds the file called [2367 W Main Building.docx](#) to FileCloud Server.

Let's see what happens when different policies are attached to it.

	Admin Hold	Legal Hold	Retention No Deletion	Archival	Retention with Deletion	Trash Bin Retention	Which Policy is Effective?
Rank	1	2	4	5	6	7	
Attached?	Yes	Yes expires = Indefinite	No	No	Yes expires = Indefinite Renew on Access is not selected	No	<ol style="list-style-type: none"> <li>1. Admin Hold - until it is removed</li> <li>2. Legal Hold - set to never expire</li> <li>3. Retention with Deletion - will never take effect unless the Legal Hold is removed by the admin</li> </ol>

No	No	Yes expires = 90 days Renew on Access is not selected	Yes expires = 30 days	No	No	<ol style="list-style-type: none"> <li>1. Retention No Deletion until it expires in 90 days</li> <li>2. Archival, although it was set to move files in 30 days, must wait for the Retention No Deletion policy to expire first, so it will actually take effect in 91 days</li> </ol>
Yes	No	No	No	Yes expires = 30 days Renew on Access is selected	Yes set to permanently Delete in 30 days Renew on Access is not selected	<ol style="list-style-type: none"> <li>1. Admin Hold - until it is removed</li> <li>2. Retention with Deletion - deletes files on next Cron run unless a file or folder with this policy attached is accessed, and then the expiration date is moved out 30 more days</li> <li>3. Trash Bin Retention - permanently deletes files off the system when the Retention with Deletion policy actually expires</li> </ol>

## Applying a Retention Policy to All Files

You may be required to apply a retention policy to all documents imported into FileCloud. If you have a large number of users in your system, the following method is especially useful, since it provides you with an alternative to putting a retention policy on each user's My Files path.

To use this method, you can take advantage of the fact that the Default metadata set is applied to every file, and add an attribute to the metadata set that will always be set to a certain value.

### To apply a retention policy to all files:

In the example shown here, a 7-day retention policy is applied to all uploaded files. 7 days after a file is uploaded, it is deleted from FileCloud.

1. In the admin portal navigation pane, click **Metadata**.  
The **Manage Metadata Sets** screen opens.
2. Click the **Edit** icon for the **Default** metadata set.

Manage Metadata Sets

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	1	1	 
Image metadata	Image metadata (EXIF)	Enabled	Built-in	1	1	 
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	1	1	 
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	1	1	 

3. In the **Edit Metadata Set Definition** dialog box, click **Add Attribute**.

Edit Metadata Set Definition

Metadata Set

Name\*  
Default

Description\*  
Default metadata set definition will be automatically bound to every single

Disabled

Permissions

Users Groups Paths

Add User

Name	Read Permission	Write Permission
jenniferp		

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	Actions
Tags	Array	Tags	Enabled	 

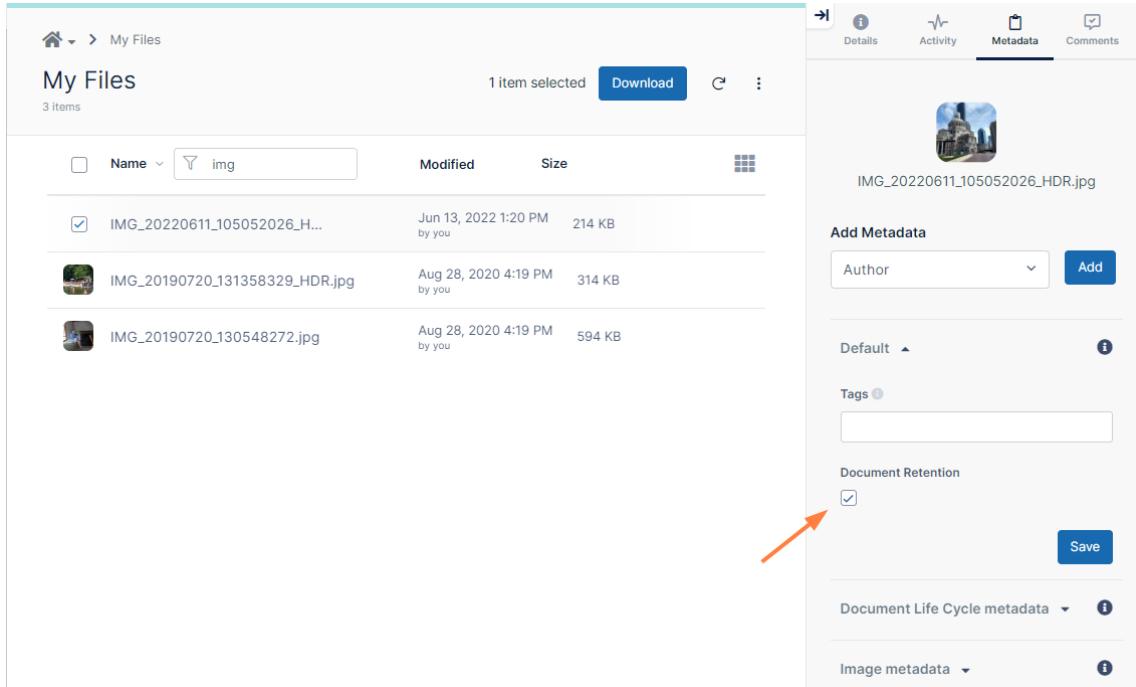
- As long as the attribute has a default value that you don't change, it can be any attribute type. In this example, create a **Boolean** attribute named **Document Retention** that has **Default Value** checked, which sets it to **true**.
- Click **Create**, and then click **Save** in the **Edit Metadata Set Definition** dialog box to save the attribute in the Default metadata set.

## Add Attribute

Name	Document Retention
Description	
Attribute Type	Boolean
Disabled	<input type="checkbox"/>
Required	<input type="checkbox"/>
Default Value	<input checked="" type="checkbox"/>
<span style="color: red; font-size: 2em;">→</span>	
<input style="background-color: #0070C0; color: white; border: none; padding: 5px 10px; border-radius: 5px; margin-right: 10px;" type="button" value="Create"/> <input style="border: none; padding: 5px 10px; border-radius: 5px;" type="button" value="Close"/>	

Now the **Document Retention** attribute, with a value of **true**, will be applied to every file that is uploaded to FileCloud.

6. To test that you have set up the metadata correctly, log in to the user portal as any user, upload a file, select it, and view the **Metadata** tab in the details pane, to make sure **Document Retention** has a value of **true**.



The screenshot shows the 'My Files' list on the left and the 'Metadata' tab details pane on the right. The 'Metadata' tab is active, showing the 'Add Metadata' section. An orange arrow points to the 'Document Retention' checkbox, which is checked. The 'Save' button is visible at the bottom of the metadata pane.

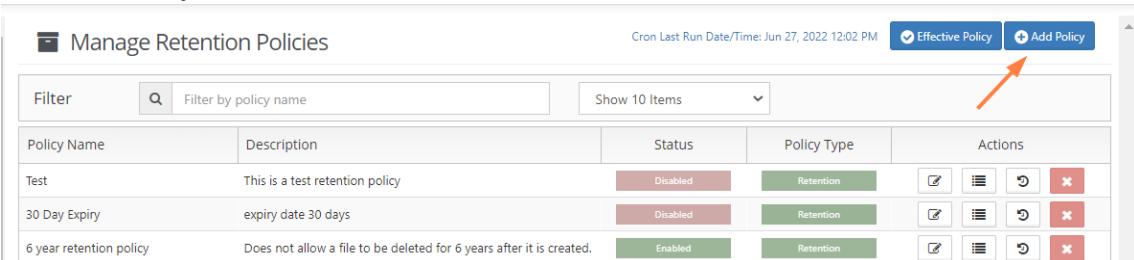
Name	Modified	Size
IMG_20220611_105052026_HDR.jpg	Jun 13, 2022 1:20 PM by you	214 KB
IMG_20190720_131358329_HDR.jpg	Aug 28, 2020 4:19 PM by you	314 KB
IMG_20190720_130548272.jpg	Aug 28, 2020 4:19 PM by you	594 KB

Once you have confirmed that the metadata is being applied correctly, create the retention policy.

7. In the admin portal navigation pane, click **Retention**.

The **Manage Retention Policies** screen opens.

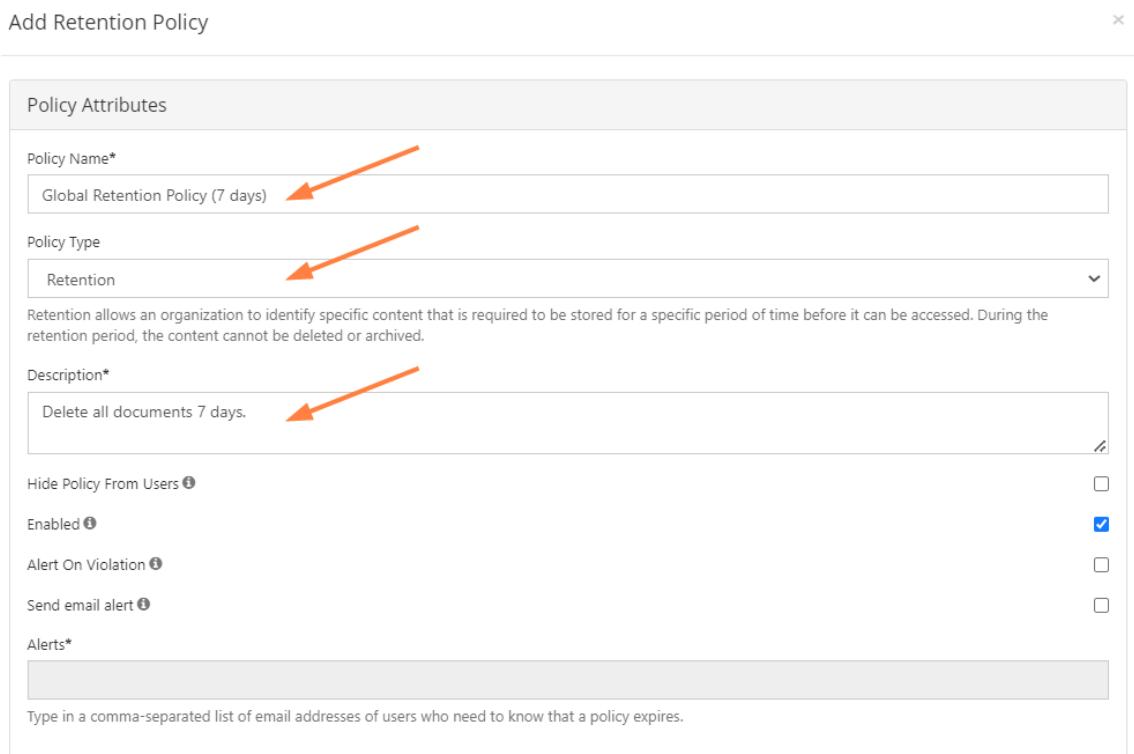
8. Click **Add Policy**.



The screenshot shows the 'Manage Retention Policies' interface. At the top, there are buttons for 'Effective Policy' and '+ Add Policy'. Below is a table with columns: Policy Name, Description, Status, Policy Type, and Actions. Three policies are listed: 'Test' (disabled, Retention), '30 Day Expiry' (disabled, Retention), and '6 year retention policy' (enabled, Retention).

The **Add Retention Policy** dialog box opens.

9. In the upper portion, give the policy a name and description and leave the **Type** of policy set to **Retention**.



The screenshot shows the 'Add Retention Policy' dialog. The 'Policy Attributes' section includes fields for 'Policy Name\*' (Global Retention Policy (7 days)), 'Policy Type' (Retention), and 'Description\*' (Delete all documents 7 days.). Below this are checkboxes for 'Enabled' (checked), 'Alert On Violation' (unchecked), 'Send email alert' (unchecked), and a 'Alerts\*' text input field.

10. In the middle portion, click the **Metadata** tab, and set the condition that the retention policy will apply to each uploaded file.
  - a. In the first drop-down list, choose **Default** to indicate the **Default** metadata set.
  - b. In the next drop-down list, choose **Document Retention** or the name you have given the new attribute.

c. Enter the default value you have given the new attribute. For this example, select the **Document Retention** check box to set it to **true**.

Apply Policy To

Paths **Metadata**

Default

Document Retention

Add

Set	Attribute	Value	Actions
Default	Document Retention	true	

No search conditions found

11. Click **Add**.

The condition is added.

Set	Attribute	Value	Actions
Default	Document Retention	true	

12. In the lower portion, enter the details of what the retention policy will do when the condition is true.

- In **Expiry Date**, choose an option. For this example, choose **Time Period** since we want all files to be deleted a specific number of days after they are uploaded.
- Since a preset option of 7 days does not exist, in **Time Period of Retention** choose **Custom**, and in **No. of Days**, choose **7**.
- In **Policy Expiry Options**, choose **Permanently Delete**.

Actions

Expiry Date\*

Time Period  Fixed Date  Indefinite

Time Period of Retention

Custom

No. of Days\*

7

Renew Expiry On Access

Policy Expiry Actions

No Action  Permanently Delete

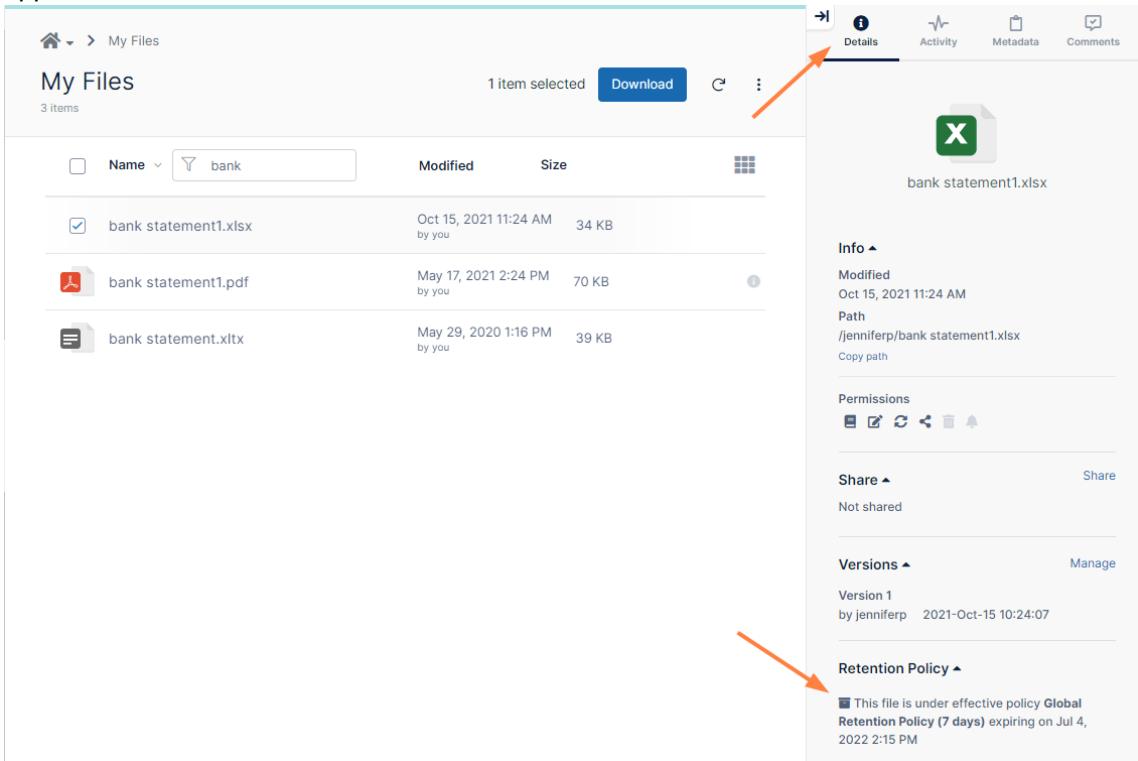
13. Click **Save**.

Manage Retention Policies

Cron Last Run Date/Time: Jun 27, 2022 12:02 PM Effective Policy Add Policy

Policy Name	Description	Status	Policy Type	Actions
Test	This is a test retention policy	Disabled	Retention	<span>Edit</span> <span>Preview</span> <span>Copy</span> <span>Delete</span>
30 Day Expiry	expiry date 30 days	Disabled	Retention	<span>Edit</span> <span>Preview</span> <span>Copy</span> <span>Delete</span>
6 year retention policy	Does not allow a file to be deleted for 6 years after it is created.	Enabled	Retention	<span>Edit</span> <span>Preview</span> <span>Copy</span> <span>Delete</span>
Global Retention Policy (7 days)	Delete all documents 7 days.	Enabled	Retention	<span>Edit</span> <span>Preview</span> <span>Copy</span> <span>Delete</span>

14. To test the the retention policy is working properly, log in to the user portal as any user, upload a file, select it, and view the **Details** tab in the details pane, to make sure the retention policy is applied to the document.



The screenshot shows the 'My Files' interface. On the left, a list of files is displayed, including 'bank statement1.xlsx', 'bank statement1.pdf', and 'bank statement1.xltx'. On the right, a detailed view is open for 'bank statement1.xlsx'. The 'Details' tab is selected. The 'Retention Policy' section shows a message: 'This file is under effective policy Global Retention Policy (7 days) expiring on Jul 4, 2022 2:15 PM'. Arrows point from the text 'Delete all documents 7 days.' in the retention policies table to the 'Retention Policy' message in the details view.

# Smart Classification

Beginning in FileCloud 23.232, an updated version of the Smart Classification user interface is available. This section of the documentation covers the new user interface. If you prefer to use the classic user interface, see [Smart Classification Classic](#) (see page 164).



Smart Classification is only available for Advanced licenses, or Essentials licenses with CCE+PATTERNSEARCH components. For information on the different license types, read about the key features on the [Pricing](#)<sup>85</sup> page.

## Smart Classification in FileCloud

FileCloud's Smart Classification system (also referred to as the content classification engine or CCE) searches for files with specific content or content patterns and tags them with metadata values. Once the files are marked with metadata, they can be identified for further actions, such as processing in FileCloud's data leak prevention (DLP) (see page 188) system.

To use Smart Classification, set up rules that search for content in files and apply metadata to them depending on the search results. When rules are initially enabled, they apply to files added before the rules were created. After that, they apply to newly added and uploaded files.

### Example:

You create a rule to mark all files that contain content with 6 consecutive numbers by setting their metadata field **CompanyID** to **yes**. Smart Classification tries to locate instances of 6 consecutive numbers in the content of each new and modified file in FileCloud, and when it finds a match, sets the file's **CompanyID** metadata field to **yes**. Now, FileCloud's Smart DLP (see page 188) can prevent files with **CompanyID=yes** from being read and downloaded.

## Setting up Smart Classification

To set up content classification, you create rules in the **Add Content Classification Rule** wizard. These rules specify the patterns to match and the metadata to apply to files if a pattern is matched or is not matched.

---

85. <https://www.filecloud.com/pricing/>

Update Content Classification Rule

1 General      2 Classifier      3 Action

**Classifier condition** [Switch to code editor](#)  
 After scanning the document for patterns, the match action is executed if the condition is satisfied.  
 Otherwise, the non-match action takes place.

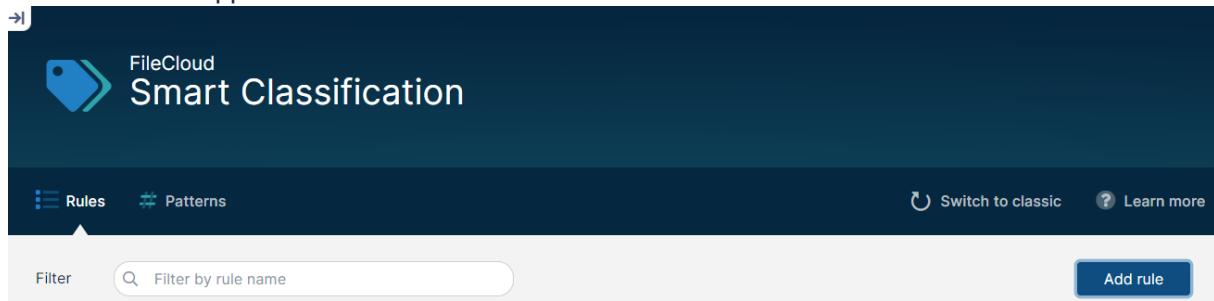
Number of matches is greater than 0 [Add condition](#) [Add group](#)

**Match action** [Switch to code editor](#)  
 Set metadata CompanyID > found to yes [Add action](#)

**Non-match action** [Switch to code editor](#)  
 Set metadata CompanyID > found to no [Add action](#)

[Back](#) [Save rule](#)

The saved rules appear in the Smart Classification screen.



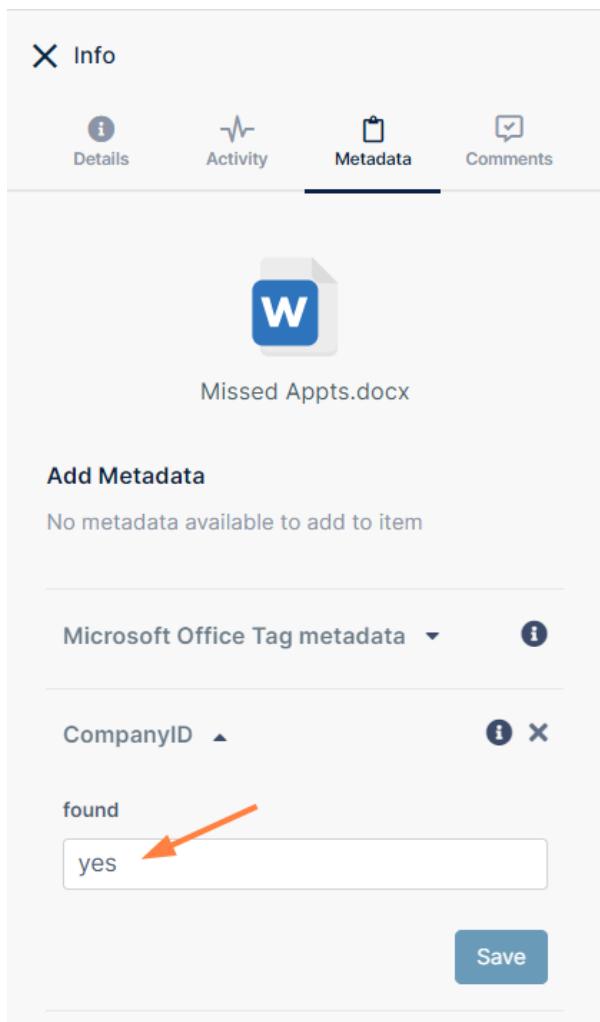
FileCloud Smart Classification

Rules Patterns [Switch to classic](#) [Learn more](#)

Filter  [Add rule](#)

Rule name	Status	Enabled	Last run	Actions
Company ID number	-	<input checked="" type="checkbox"/>	Never	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>
Patient names	✓	<input checked="" type="checkbox"/>	2 hours ago	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>
US ID data	✓	<input checked="" type="checkbox"/>	3 hours ago	<a href="#"></a> <a href="#"></a> <a href="#"></a> <a href="#"></a>

When a rule runs, it applies metadata to files with content that match its conditions:



Missed Appts.docx

Add Metadata

No metadata available to add to item

Microsoft Office Tag metadata ▾

CompanyID ▾

found

yes

Save

Other FileCloud operations look at this metadata to perform their actions. For example, Smart DLP can prevent a file from being downloaded if **CompanyID** is set to **yes**. Or a search can return all files where **CompanyID** is set to **no**.

## Running content classification rules

To automate and schedule running of content classification rules, you must set up a Cron Job. You can also run a rule manually from the **Smart Classification** screen..



### Requirements

- Files greater than 10 MB are not available for Smart Classification.
- Administrators must have created at least one set of metadata for the Smart Classification process to operate.

## Setting Up Smart Classification

To set up Smart Classification:

1. If you have not set up metadata for tagging your Smart Classification content, set it up.
2. If you plan to use the [ICAP DLP classifier \(see page 144\)](#), configure ICAP DLP integration in FileCloud.
3. If you plan to use the AI Classifier ([see page 144](#)), configure AI Integration in FileCloud.
4. Smart Classification has several predefined regex patterns that you can use in your rules. In addition, you may create and save regex patterns. For help creating your own regex patterns, see [Adding Smart Classification Regex Patterns \(see page 106\)](#).
5. To put your smart classification regex patterns into groups, so you can refer to multiple patterns at once, see [Creating Smart Classification Regex Pattern Groups \(see page 113\)](#).
6. [Create and Test Smart Classification Rules \(see page 126\)](#).

## Adding Smart Classification Regex Patterns

Smart Classification looks at a pattern you have added and checks if the content of uploaded and modified files includes that pattern. Patterns can be expressed in different ways - for example, in regex format, as text in a query, or as an AI match term.

In a large number of cases, the patterns to be matched are expressed in regex format and locate common identification information such as national ID numbers. To make it easier for you to set up rules, Smart Classification has predefined a number of these commonly-used regex patterns.

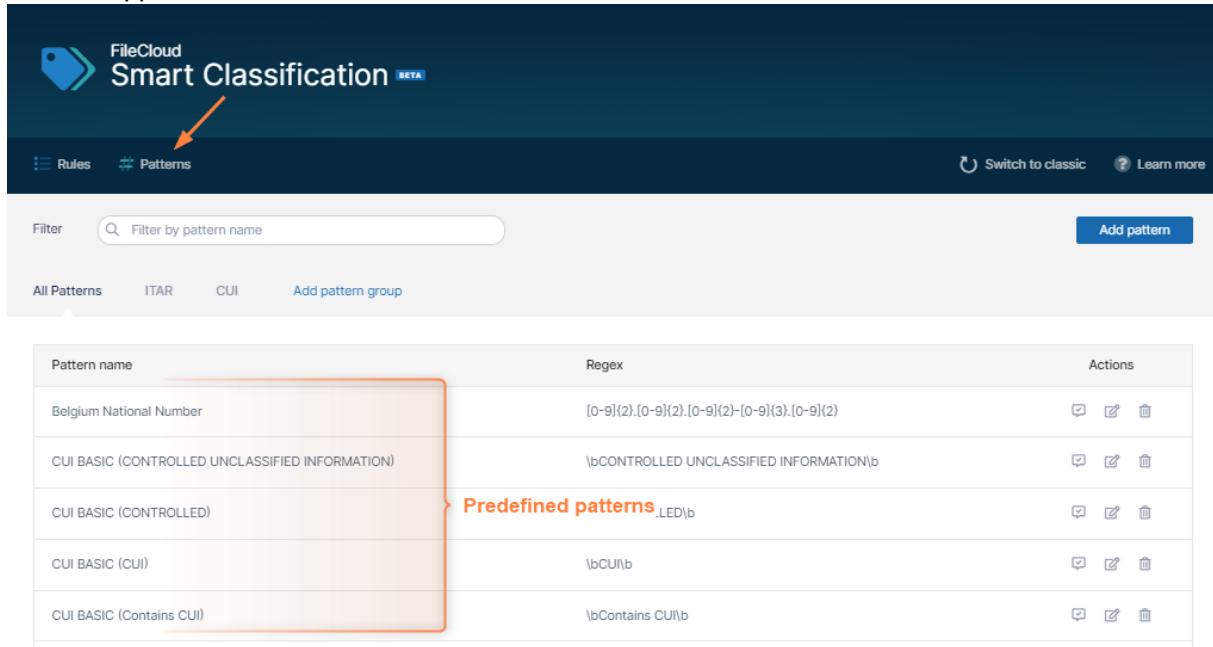
There may be regex patterns that are common in your organization but are not included in the predefined patterns, so Smart Classification enables you to define and save any number of regex patterns so you don't have to type them manually each time you enter them in a rule.

You also have the option of entering a regex pattern manually into a rule, which may be efficient for patterns that you are planning to use only once or infrequently.

### Selecting from predefined regex patterns

The predefined patterns in Smart Classification are all in regex format. You can view all of them by clicking the **Patterns** link in the **Smart Classification** page menu bar. If you add your own patterns, they

will also appear here.

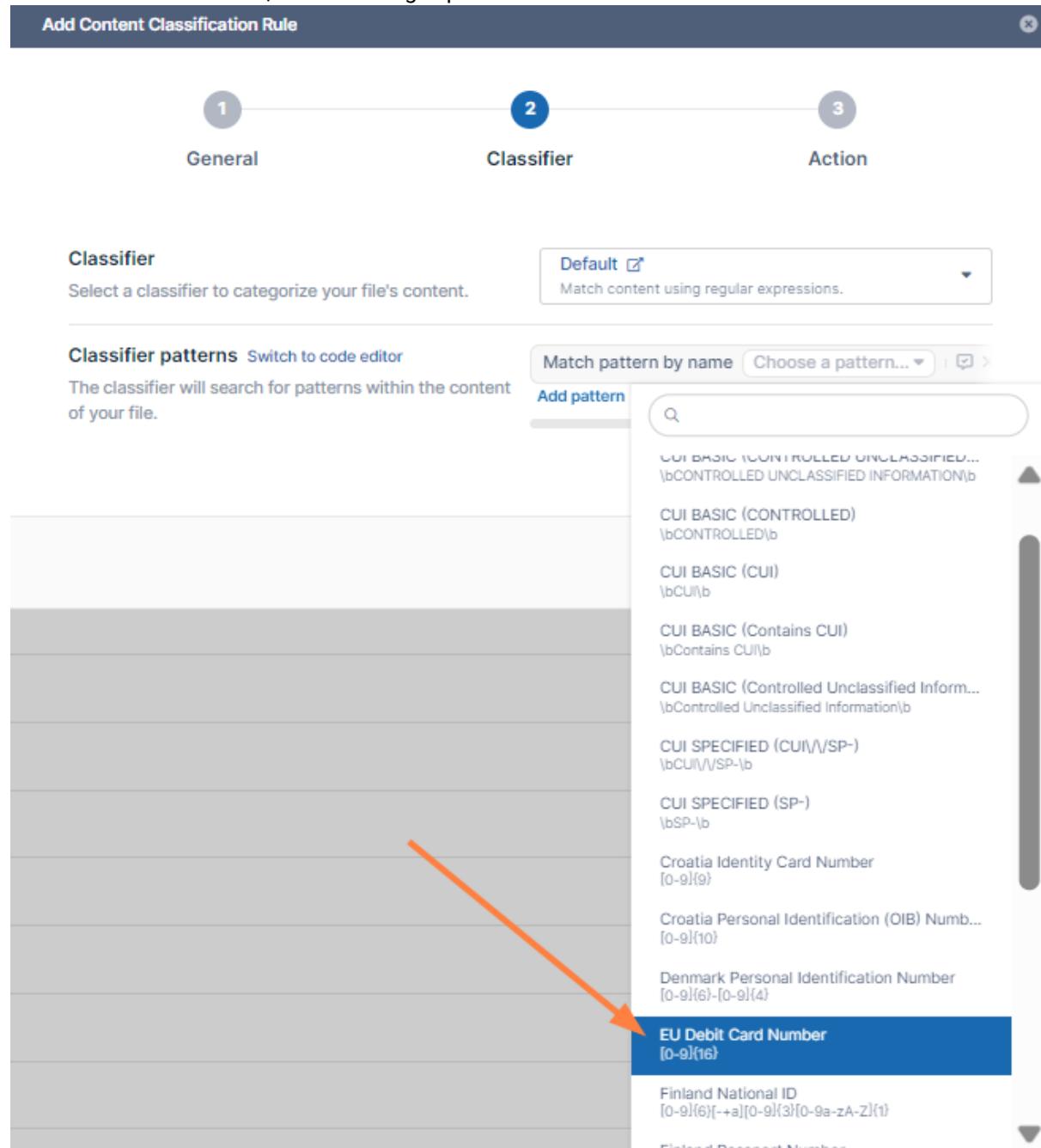


Pattern name	Regex	Actions
Belgium National Number	[0-9]{2}.(0-9){2}.(0-9){2}-[0-9]{3}.(0-9){2}	 
CUI BASIC (CONTROLLED UNCLASSIFIED INFORMATION)	\bCONTROLLED UNCLASSIFIED INFORMATION\b	 
CUI BASIC (CONTROLLED)	\bCUI\b	 
CUI BASIC (CUI)	\bContains CUI\b	 
CUI BASIC (Contains CUI)		 

Next to the name of each pattern is the regex for the pattern. For example, if you choose to match on the **EU Debit Card Number**, Smart Classification looks for files with content that matches the regex **[0-9]{16}** (which is equivalent to any 16 numerals in a row).

If you are looking for a pattern that matches one of the predefined patterns, choose it in the **Add Content Classification Rule** wizard as the **Classifier pattern** by selecting **Match pattern by name** and choosing the pattern name. **Note:** You can only choose regex patterns with the **Default** and **Solr**

**Pattern Match** classifiers, which use regex patterns.



The screenshot shows the 'Add Content Classification Rule' wizard with three steps: General, Classifier, and Action. The Classifier step is active, showing a 'Classifier' section with a dropdown set to 'Default' and a note to 'Select a classifier to categorize your file's content.' To the right is a 'Patterns' list with a search bar and a 'Match pattern by name' dropdown. An orange arrow points from the 'Classifier' section to the 'EU Debit Card Number [0-9]{16}' pattern in the list.

Step	Section	Content
1	General	Content of the General step
2	Classifier	<p><b>Classifier</b> Select a classifier to categorize your file's content.</p> <p><b>Classifier patterns</b> <a href="#">Switch to code editor</a> The classifier will search for patterns within the content of your file.</p>
3	Action	Content of the Action step

**Patterns List:**

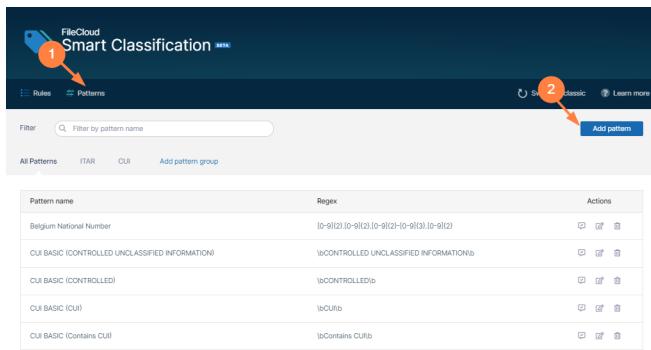
- CUI BASIC (CONTROLLED UNCLASSIFIED...) \bCONTROLLED UNCLASSIFIED INFORMATION\b
- CUI BASIC (CONTROLLED) \bCONTROLLED\b
- CUI BASIC (CUI) \bCUI\b
- CUI BASIC (Contains CUI) \bContains CUI\b
- CUI BASIC (Controlled Unclassified Inform... \bControlled Unclassified Information\b
- CUI SPECIFIED (CUI|/|SP-) \bCUI|/|SP-\b
- CUI SPECIFIED (SP-) \bSP-\b
- Croatia Identity Card Number [0-9]{9}
- Croatia Personal Identification (OIB) Numb... [0-9]{10}
- Denmark Personal Identification Number [0-9]{6}-[0-9]{4}
- EU Debit Card Number [0-9]{16}**
- Finland National ID [0-9]{6}[-+a][0-9]{3}[0-9a-zA-Z]{1}

## Creating your own regex pattern before adding it to a rule

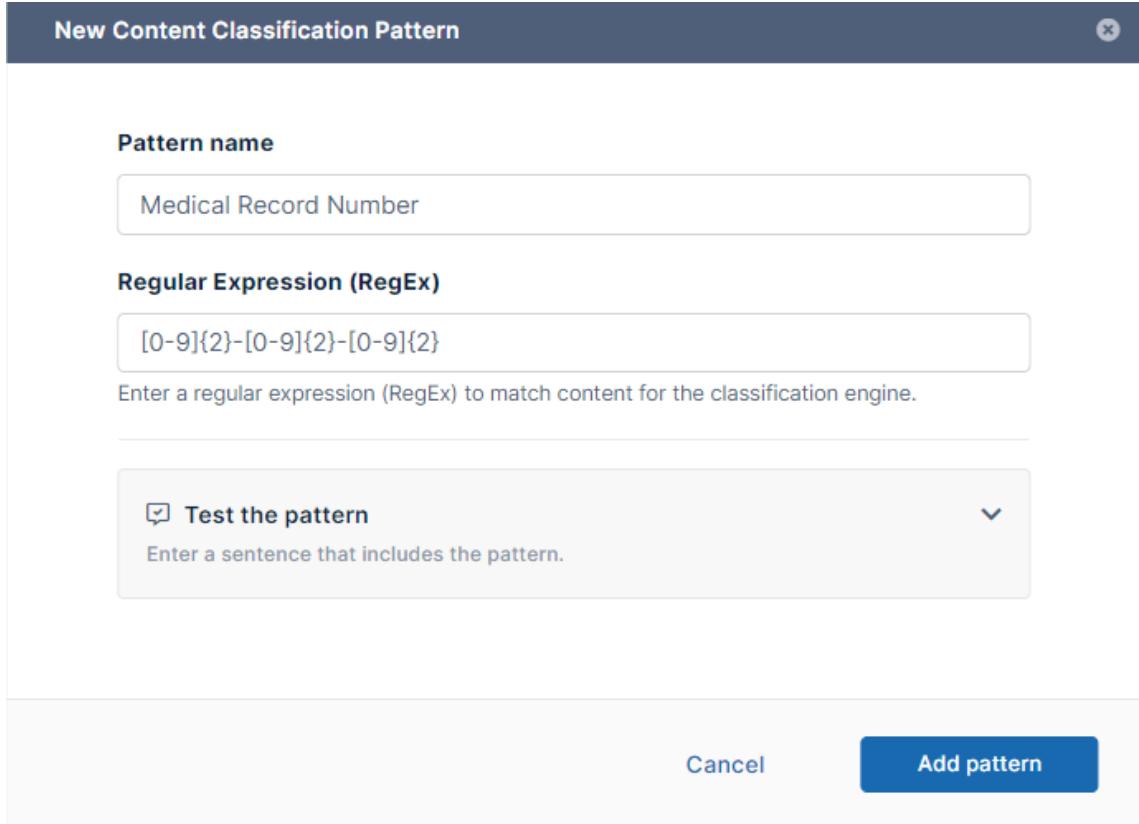
The following procedure for creating and saving your own regex pattern uses the example of medical record numbers in the format of 6 digits in pairs of 2 separated by dashes, such as 12-34-56.

### To create your own pattern:

1. In the menu bar of the **Smart Classification** screen, click **Patterns** to open the **Patterns** screen, and then click **Add Pattern**.



The **New Content Classification Pattern** dialog box opens:



2. In **Pattern name**, enter a name for a pattern.
3. In **Regular Expression (RegEx)** enter the regex for the pattern.  
If you're not familiar with writing regular expressions, you can find a number of sites with information online, such as those at <https://www.geeksforgeeks.org/write-regular-expressions/> and <https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>.
4. To see if your regex matches the correct patterns, click **Test the pattern**.  
The field expands.
5. Type in some text that contains content matching your regex into the box and click **Check**.

New Content Classification Pattern ×

**Pattern name**

**Regular Expression (RegEx)**

Enter a regular expression (RegEx) to match content for the classification engine.

**Test the pattern** ^

**Default** **PatternMatch**

Please send me the files for 12-34-56 and 78-91-00

Enter a sentence that includes the pattern.

**Check**

**Cancel** **Add pattern**

If your regex is working as expected, the matches you entered are highlighted and a count of the matches appears below the box.

### New Content Classification Pattern

**Pattern name**  
Medical Record Number

**Regular Expression (RegEx)**  
[0-9]{2}-[0-9]{2}-[0-9]{2}

Enter a regular expression (RegEx) to match content for the classification engine.

**Test the pattern**

**Default**      **PatternMatch**

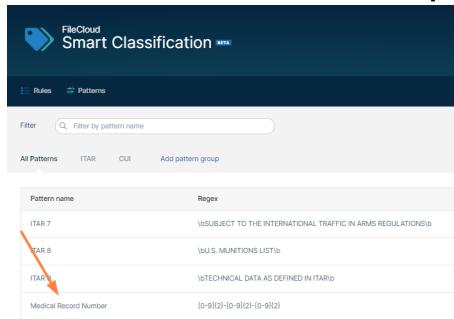
Please send me the files for 12-34-56 and 78-91-00

Enter a sentence that includes the pattern.

✓ 2 matches      **Check**

**Add pattern**

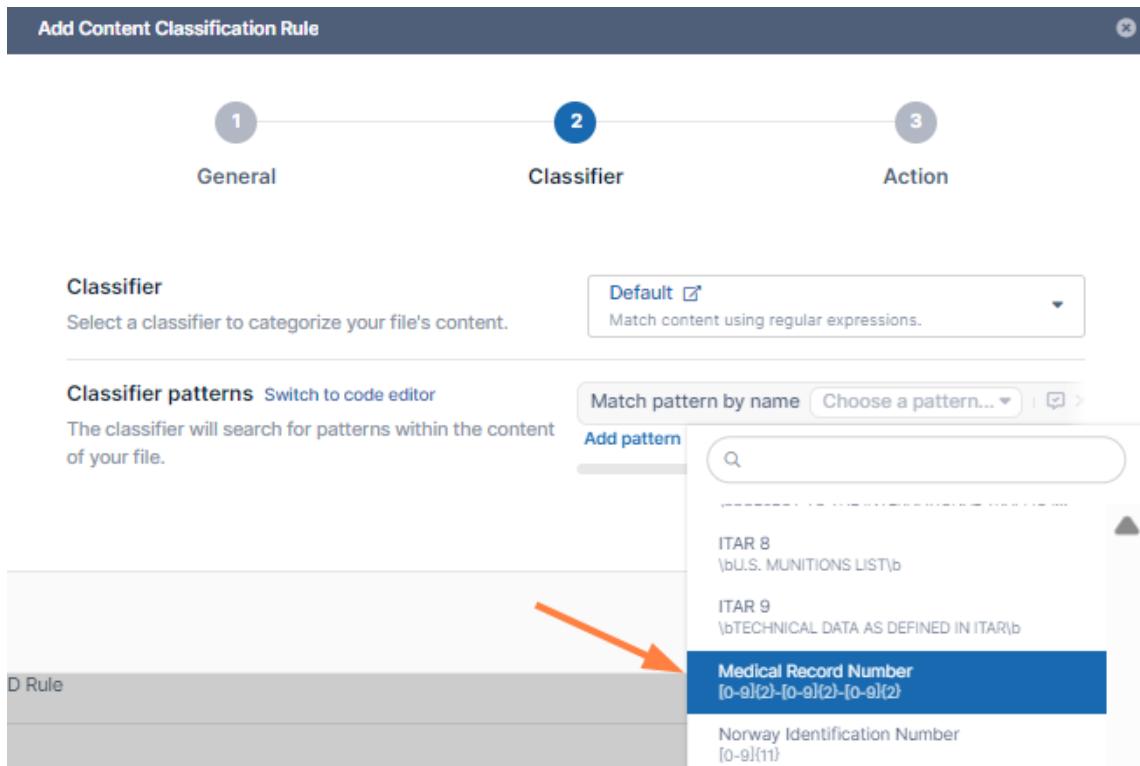
6. If the test for your pattern was successful, click **Add pattern**.  
 The pattern appears in the list of patterns and in the drop-down list of the **Add Content Classification Rule** wizard when you choose a **Classifier pattern** for the **Default** or **Solr Pattern Match** classifier and choose **Match pattern by name**.



The screenshot shows the 'Smart Classification' interface with the 'Patterns' tab selected. A new pattern, 'Medical Record Number', has been added and is visible in the list. The pattern name is 'Medical Record Number' and the regular expression is '[0-9]{2}-[0-9]{2}-[0-9]{2}'. An orange arrow points to the 'Medical Record Number' entry in the list.

Pattern name	Regex
ITAR 7	\b(SUBJECT TO THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS\b)
ITAR 8	\b(U.S. MUNITIONS LIST\b)
ITAR 9	\b(TECHNICAL DATA AS DEFINED IN ITAR\b)
Medical Record Number	[0-9]{2}-[0-9]{2}-[0-9]{2}

The new **Medical Record Number** pattern appears in the list of patterns on the **Patterns** tab.



The new **Medical Record Number** pattern appears in the **Choose a pattern** drop-down list in the **Add Content Classification Rule** wizard.

## Adding a pattern as you create a rule

You are not required to give regex patterns names and add them to the list of saved patterns to use them in a content classification rule; instead, you can enter the regex manually when you create a rule that uses the **Default** or **Solr Pattern Match** classifier.

For instructions on adding a regex pattern manually to a rule, see the **Match with Regex** videos for the

Default and Solr Pattern Match classifiers in [Guide to Classifiers \(see page 144\)](#).

The screenshot shows the 'Add Content Classification Rule' wizard in progress, specifically Step 2: Classifier. The 'Classifier' tab is active. A dropdown menu is open, showing 'Default' as the selected option. A red arrow points to this selection. Below the dropdown, there is a 'Match RegEx' input field containing the pattern '[0-9]{2}-[0-9]{2}-[0-9]{2}'. There is also an 'Add pattern' button. At the bottom of the screen, there are 'Back' and 'Next' navigation buttons.

## Creating Smart Classification Regex Pattern Groups

You can group regex patterns together in pattern groups, which enables you to add them to Content Classification Rules together. This is useful if you have multiple regex patterns that you frequently add together to rules, for example, if you have multiple rules that search for personally identifiable information (PII), you could add a regex pattern group that includes patterns for national ID number, passport number, and driver's license numbers, and add the group each time you add a new PII rule.

When you create a regex pattern group, you can either create new patterns and add them to the group as you create it or you can add existing patterns to the group.



There are two default pattern groups, ITAR and CUI, that correspond with the ITAR and CUI built-in metadata. These include the default patterns to use when searching for content to classify for the ITAR and CUI compliances. If your content includes different values than the default ones, you can modify the patterns here and in the metadata sets.

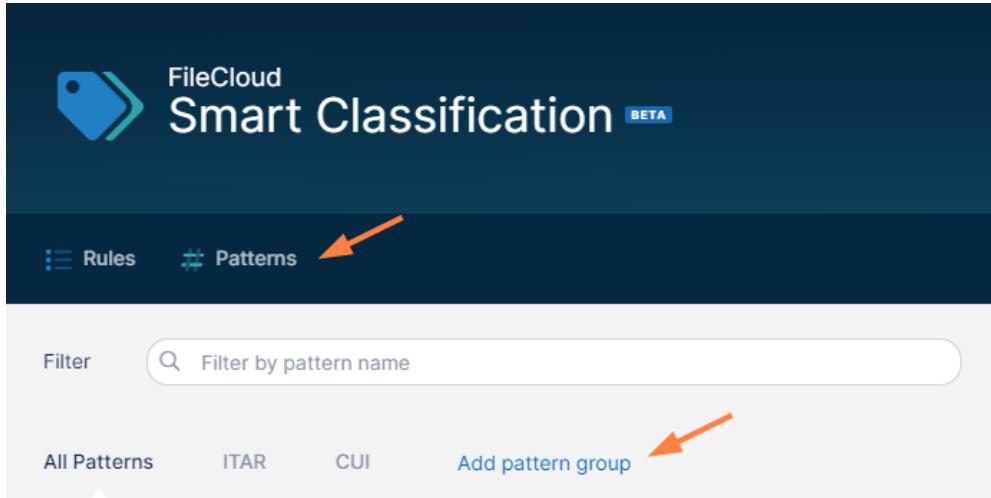
### Creating a regex pattern group

The steps for creating a regex pattern group below use the example of a company that is creating a pattern group for PII that includes:

- The predefined patterns **France Driver's License Number**, **France National ID Card**, and **France Passport Number**
- The new pattern **Company ID**, a 6 digit numerical pattern.

**To add a regex pattern group:**

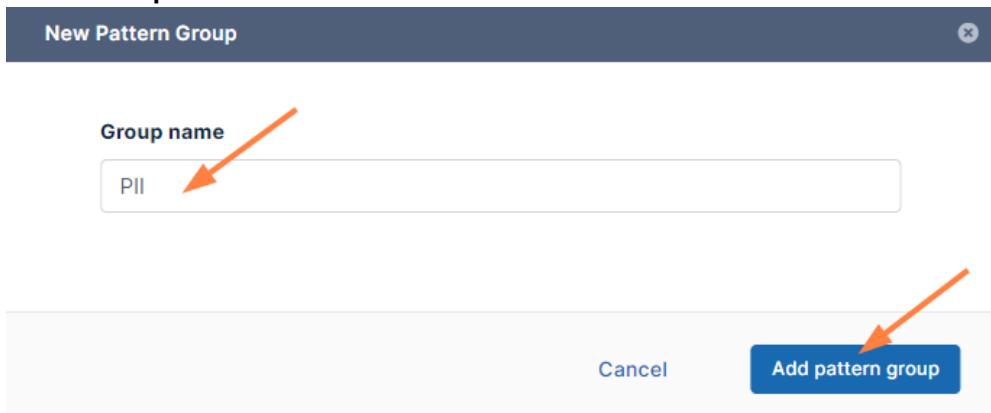
1. In the **Smart Classification** screen, click **Patterns** in the menu bar, and then click **Add pattern group**.



The screenshot shows the 'Smart Classification' interface. At the top, there is a 'FileCloud Smart Classification' header with a 'BETA' badge. Below the header, there are two main navigation buttons: 'Rules' and 'Patterns'. An orange arrow points to the 'Patterns' button. Below these buttons is a search bar labeled 'Filter by pattern name' with a magnifying glass icon. Underneath the search bar, there are three filter tabs: 'All Patterns', 'ITAR', and 'CUI'. To the right of these tabs is a blue button labeled 'Add pattern group', which is also highlighted with an orange arrow. The main content area displays a list of pattern names in a table format. The first few items in the list are: 'Belgium National Number', 'CUI BASIC (CONTROLLED UNCLASSIFIED INFORMATION)', 'CUI BASIC (CONTROLLED)', and 'CUI BASIC (CUI)'. Each item is a row in the table.

The **New Pattern Group** dialog box opens.

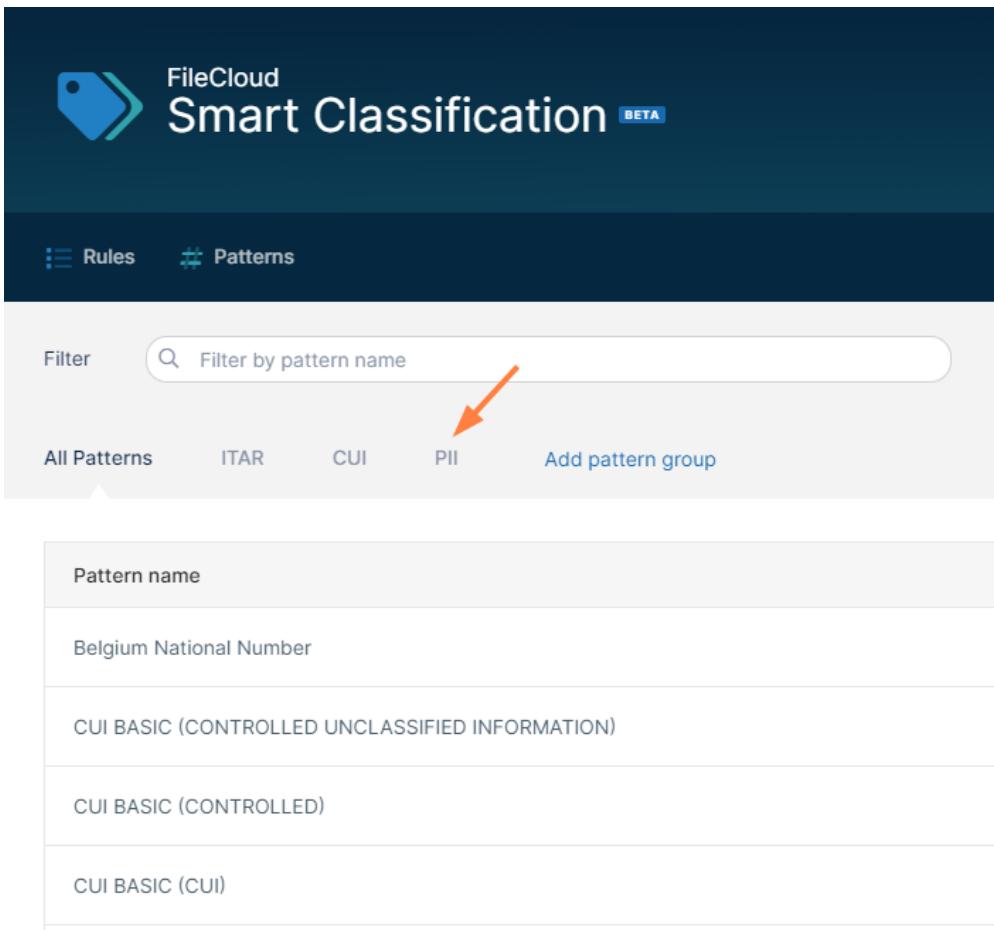
2. Enter a **Group name**.



The screenshot shows the 'New Pattern Group' dialog box. At the top, it has a title bar with the text 'New Pattern Group' and a close button. Below the title bar is a text input field labeled 'Group name' with the placeholder text 'PII'. An orange arrow points to this input field. At the bottom of the dialog box are two buttons: 'Cancel' on the left and a blue 'Add pattern group' button on the right. An orange arrow points to the 'Add pattern group' button.

3. Click **Add pattern group**.

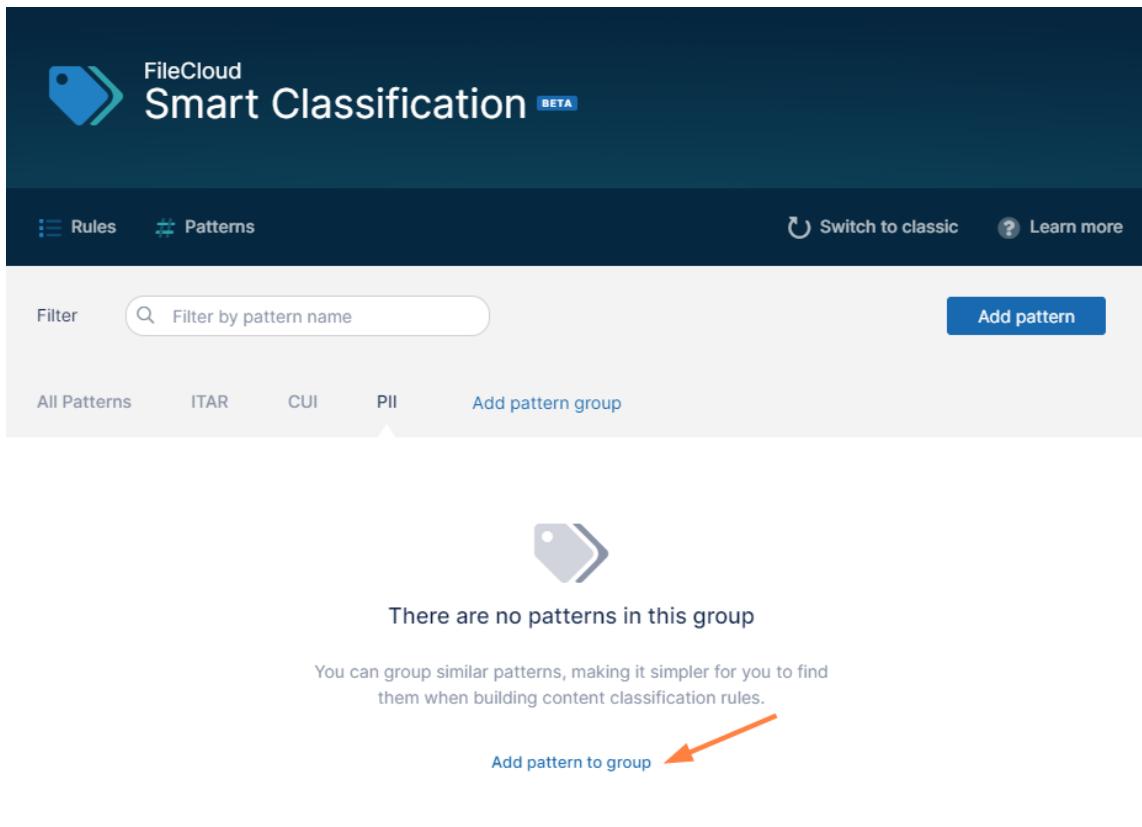
The new pattern group name is added above the list of patterns.



The screenshot shows the FileCloud Smart Classification interface. At the top, there is a logo and the text "FileCloud Smart Classification BETA". Below the header, there are two navigation tabs: "Rules" and "Patterns". The "Patterns" tab is selected. A search bar labeled "Filter by pattern name" is present. Below the search bar, there are four filter buttons: "All Patterns", "ITAR", "CUI", and "PII". An orange arrow points to the "PII" button. To the right of the filter buttons is a blue "Add pattern group" button. The main content area displays a list of pattern names. The first item in the list is "Belgium National Number". Below it are three CUI categories: "CUI BASIC (CONTROLLED UNCLASSIFIED INFORMATION)", "CUI BASIC (CONTROLLED)", and "CUI BASIC (CUI)".

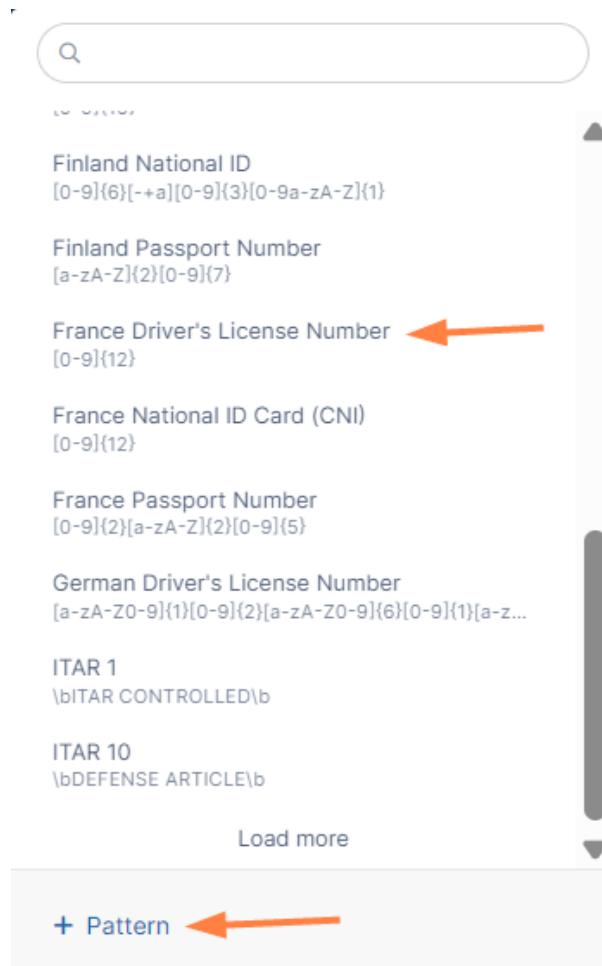
Pattern name
Belgium National Number
CUI BASIC (CONTROLLED UNCLASSIFIED INFORMATION)
CUI BASIC (CONTROLLED)
CUI BASIC (CUI)

4. Click the pattern group name.  
At this point, the pattern group is empty.
5. Click **Add pattern to group**.



The screenshot shows the FileCloud Smart Classification interface. At the top, there is a navigation bar with the FileCloud logo, the text "Smart Classification", and a "BETA" badge. Below the navigation bar, there are two tabs: "Rules" and "Patterns", with "Patterns" being the active tab. To the right of the tabs are "Switch to classic" and "Learn more" buttons. Below the tabs is a search bar with the placeholder "Filter by pattern name" and an "Add pattern" button. Under the search bar, there are four filter buttons: "All Patterns", "ITAR", "CUI", and "PII". A "Add pattern group" button is also present. The main content area displays a message: "There are no patterns in this group" with a small icon of a tag. Below this message, a note says: "You can group similar patterns, making it simpler for you to find them when building content classification rules." An "Add pattern to group" button is located at the bottom of this note, with a red arrow pointing to it.

A drop-down list opens. It lists existing pattern groups for you to choose and enables you to add new pattern groups and include them.



Finland National ID  
[0-9]{6}[-+a][0-9]{3}[0-9a-zA-Z]{1}

Finland Passport Number  
[a-zA-Z]{2}[0-9]{7}

France Driver's License Number ←  
[0-9]{12}

France National ID Card (CNI)  
[0-9]{12}

France Passport Number  
[0-9]{2}[a-zA-Z]{2}[0-9]{5}

German Driver's License Number  
[a-zA-Z0-9]{1}[0-9]{2}[a-zA-Z0-9]{6}[0-9]{1}[a-zA-Z0-9]{1}

ITAR 1  
\\bITAR CONTROLLED\\b

ITAR 10  
\\bDEFENSE ARTICLE\\b

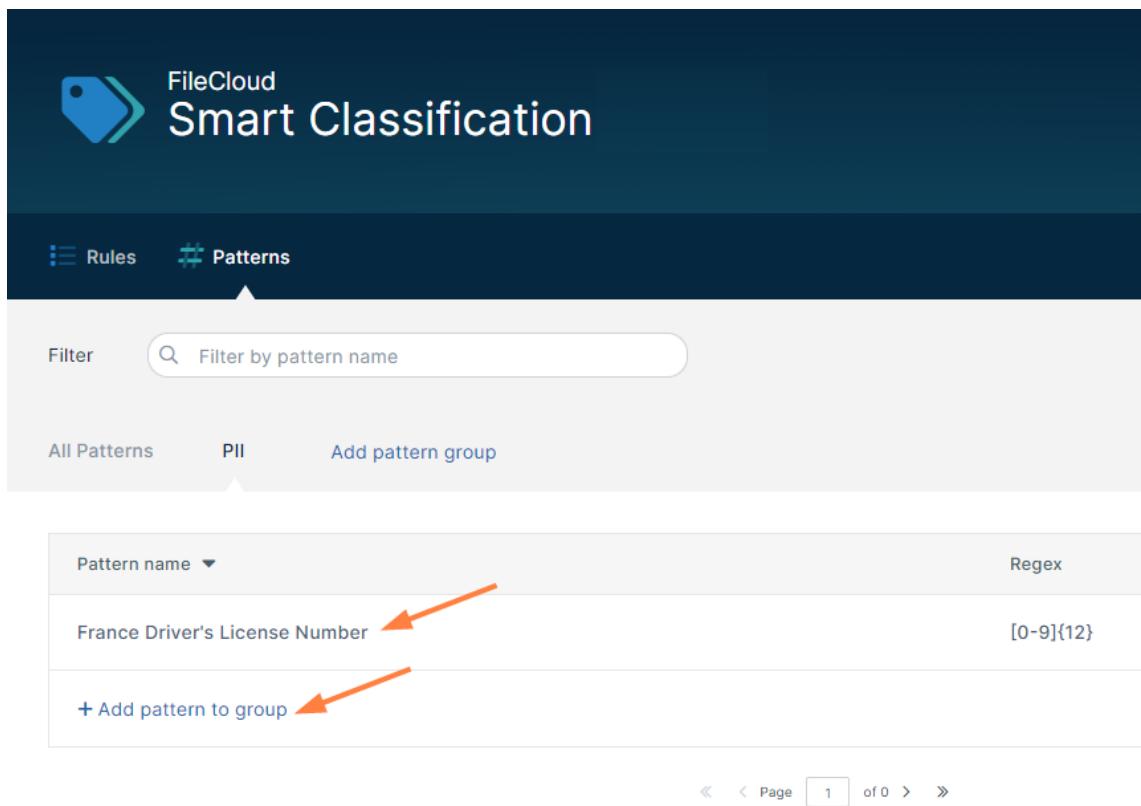
Load more

+ Pattern ←

6. Click **France Driver's License Number**.

The dialog box closes and **France Driver's License Number** is added to the list for the group.

Another **Add pattern to group** link appears below it.



FileCloud Smart Classification

Rules Patterns

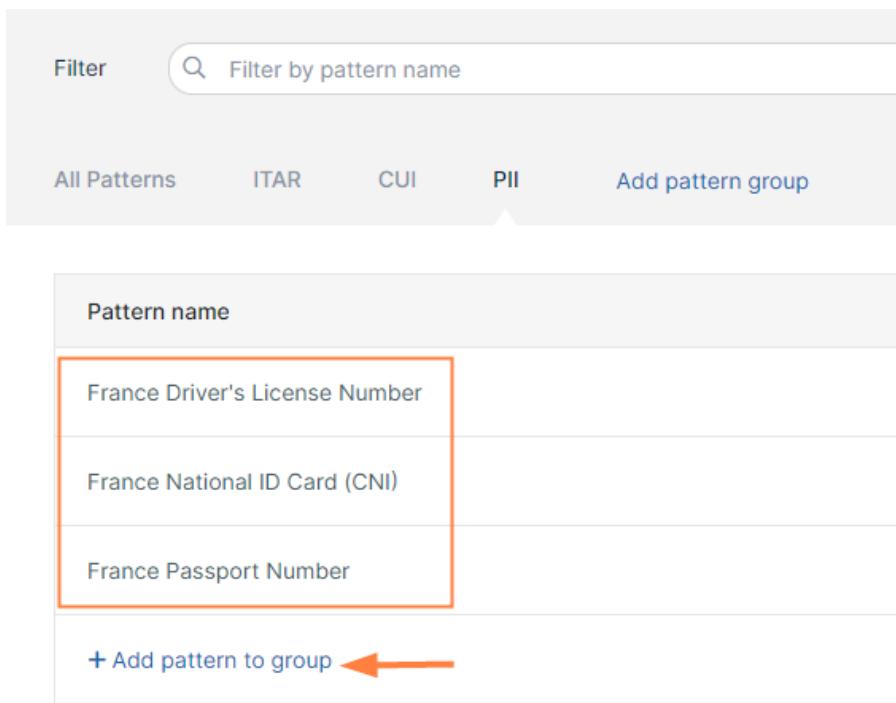
Filter Filter by pattern name

All Patterns PII Add pattern group

Pattern name	Regex
France Driver's License Number	[0-9]{12}
<a href="#">+ Add pattern to group</a>	

Page 1 of 0

7. Click the **Add pattern to group** link and click **France National ID Card**.  
**France National ID Card** is added to the group.
8. Click the **Add pattern to group** link below it, and click **France Passport Number**.  
Now all three of the predefined patterns are added to the **PII** pattern group.



Filter

All Patterns ITAR CUI PII Add pattern group

Pattern name

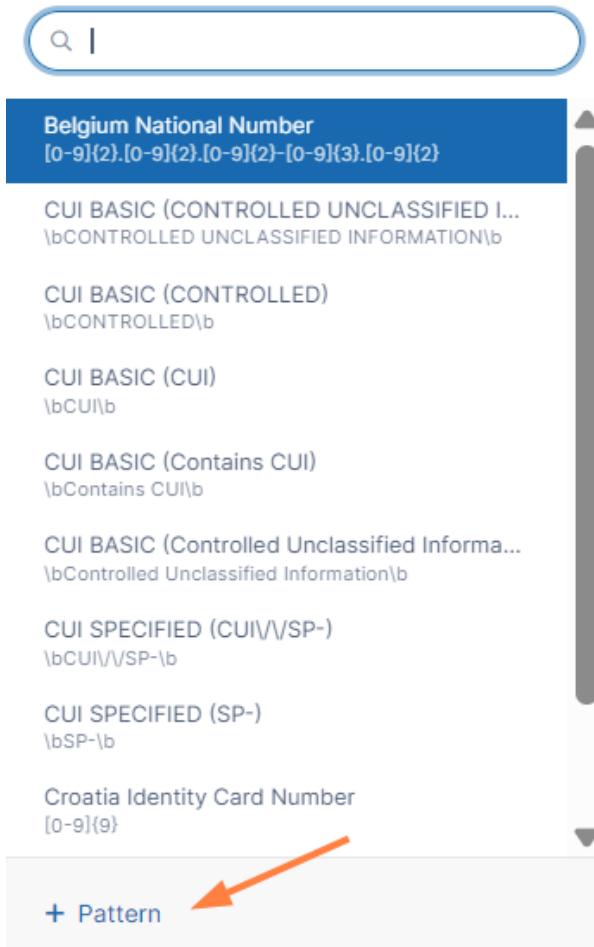
France Driver's License Number

France National ID Card (CNI)

France Passport Number

+ Add pattern to group

9. Below the three patterns, click **Add pattern to group**.
10. To create the new **Company ID** pattern, click **+ Pattern** at the bottom of the drop-down list.



Belgium National Number  
[0-9]{2}.[0-9]{2}.[0-9]{2}-[0-9]{3}.[0-9]{2}

CUI BASIC (CONTROLLED UNCLASSIFIED I...  
\bCONTROLLED UNCLASSIFIED INFORMATION\b

CUI BASIC (CONTROLLED)  
\bCONTROLLED\b

CUI BASIC (CUI)  
\bCUI\b

CUI BASIC (Contains CUI)  
\bContains CUI\b

CUI BASIC (Controlled Unclassified Informa...  
\bControlled Unclassified Information\b

CUI SPECIFIED (CUI\|/SP-)  
\bCUI\|/SP-\b

CUI SPECIFIED (SP-)  
\bSP-\b

Croatia Identity Card Number  
[0-9]{9}

+ Pattern

A **New Content Classification Pattern** dialog box opens. Check the box with the pattern group's name in the bottom left corner to add the pattern and include it in the group at the same time.

New Content Classification Pattern ✖

**Pattern name**

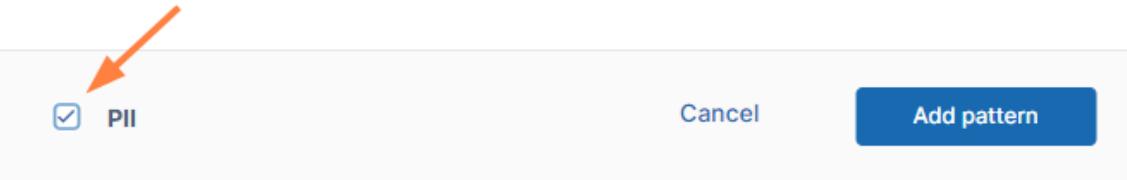
**Regular Expression (RegEx)**

Enter a regular expression (RegEx) to match content for the classification engine.

**Test the pattern** ▼

Enter a sentence that includes the pattern.

**PII** Cancel **Add pattern**



11. In **Pattern name**, enter **Company ID**.
12. In **Regular Expression (RegEx)** enter **[0-9]{6}**.
13. To open a test box, click **Test the pattern**.  
Notice that the box has two tabs: **Default** and **PatternMatch** which correspond to the **Default** and **Solr Pattern Match** classifiers. Test it in the tab that corresponds with the classifier you plan to use, or test it in both. For descriptions of the classifiers, see [Guide to Classifiers](#) (see page 144).
14. Type text that includes a 6-digit number into the **Test the pattern** box.

New Content Classification Pattern ×

**Pattern name**  
Company ID (arrow)

**Regular Expression (RegEx)**  
[0-9]{6} (arrow)

Enter a regular expression (RegEx) to match content for the classification engine.

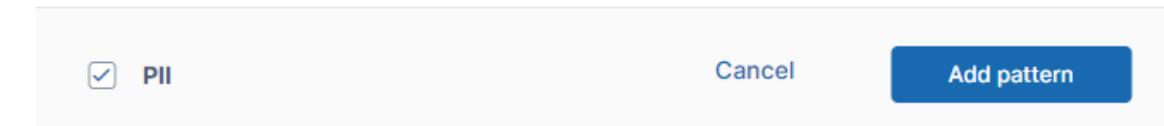
**Test the pattern** ^

**Default** **PatternMatch**

Please add **123456** to the company list. (highlighted)

Enter a sentence that includes the pattern.

**Check** (arrow)



15. To test the pattern, click **Check**.

If the test is successful, the dialog box is similar to the following, with the 6-digit number highlighted and a message below it indicating the number of matches.

New Content Classification Pattern

**Pattern name**

**Regular Expression (RegEx)**

Enter a regular expression (RegEx) to match content for the classification engine.

**Test the pattern**

**Default**      **PatternMatch**

Please add **123456** to the company list.

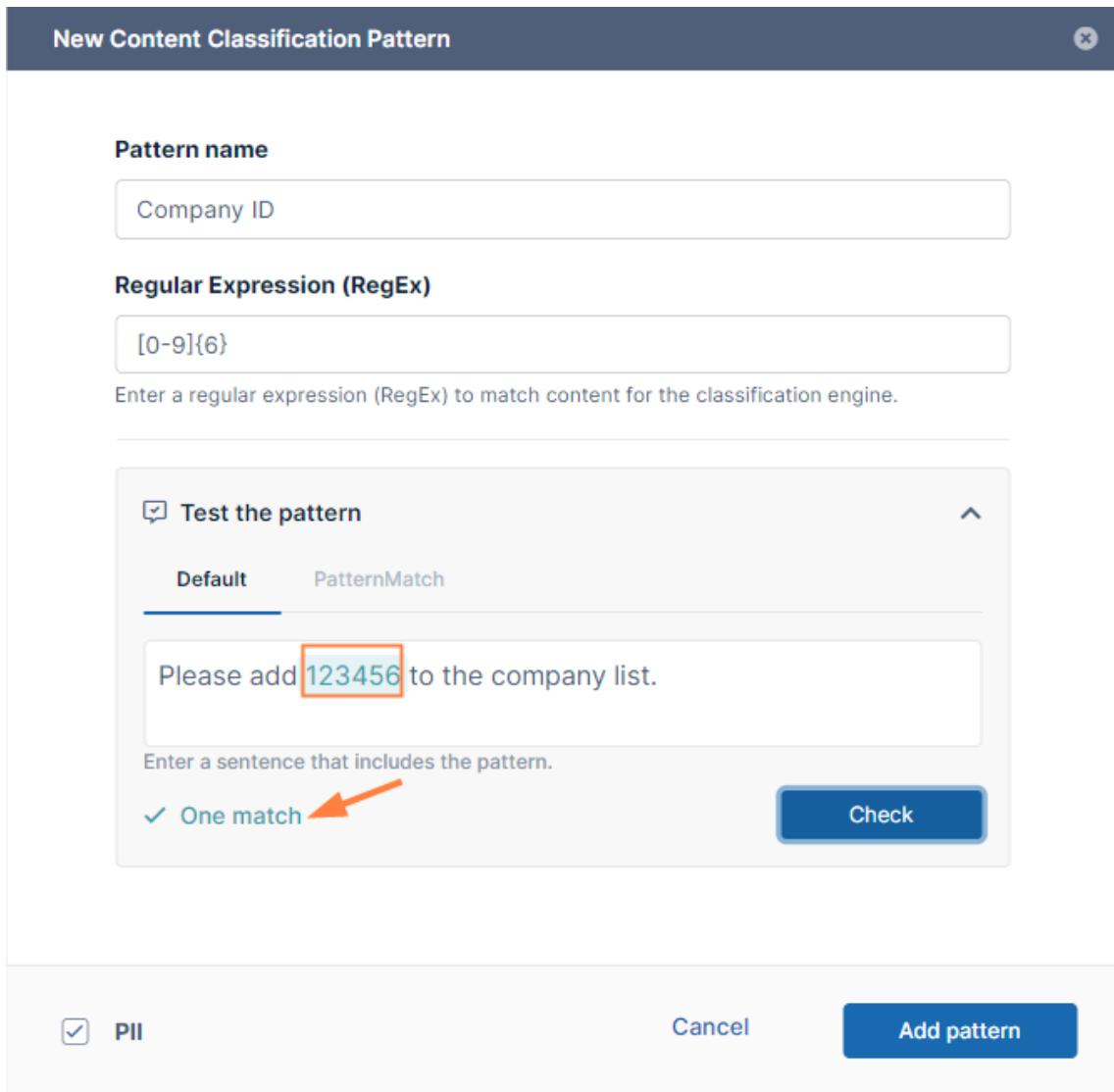
Enter a sentence that includes the pattern.

**✓ One match** 

**Check**

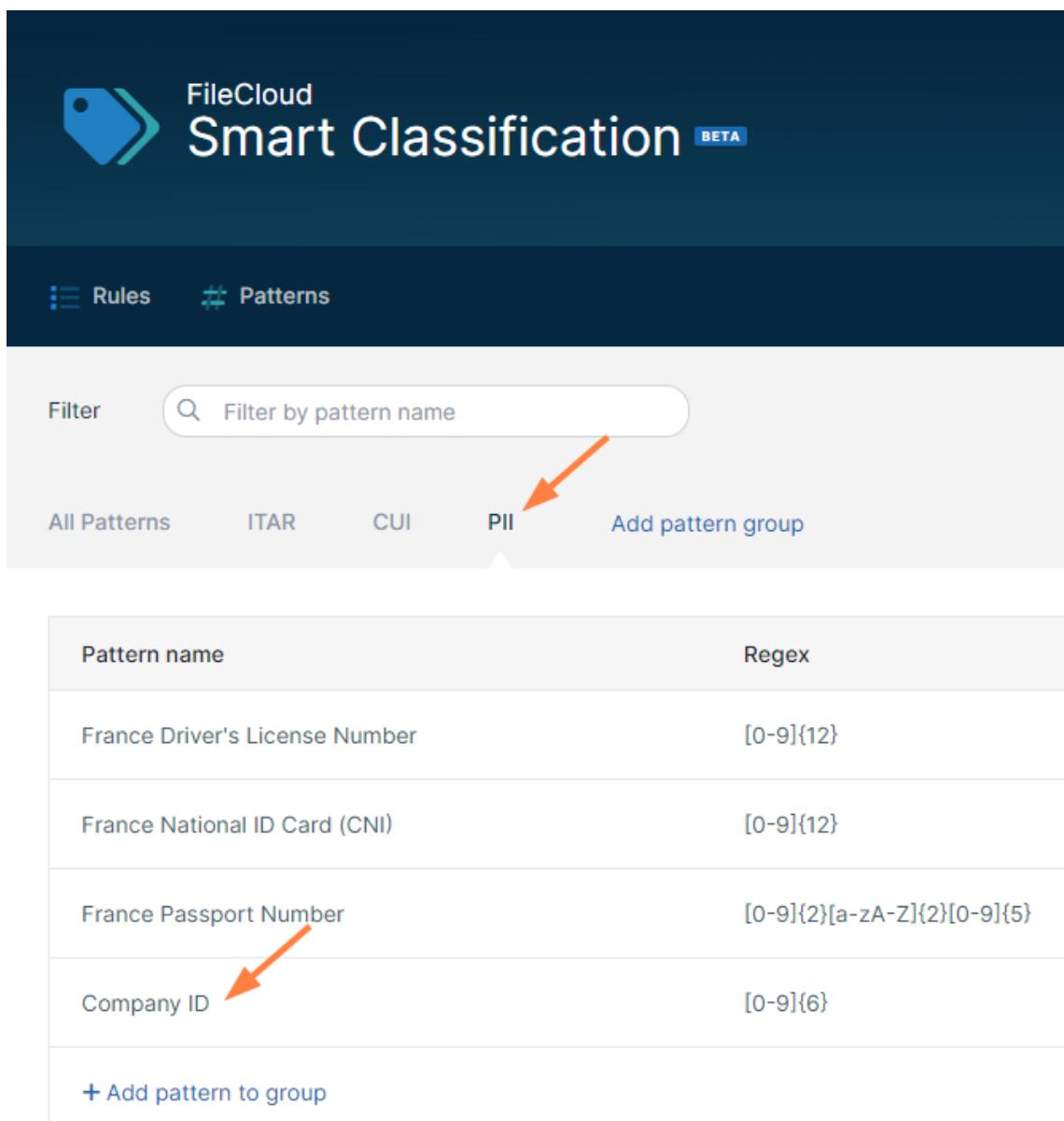
**PII**

**Cancel**      **Add pattern**



16. If the test is successful, click **Add pattern**.

The pattern is added to the pattern group.



The screenshot shows the FileCloud Smart Classification interface. At the top, there is a logo and the text "FileCloud Smart Classification BETA". Below the header, there are two navigation buttons: "Rules" and "Patterns". The "Patterns" button is selected, indicated by a blue background and white text. Underneath the buttons, there is a "Filter" section with a search bar labeled "Filter by pattern name". Below the filter, there are four categories: "All Patterns", "ITAR", "CUI", and "PII". An orange arrow points from the text "PII" to the "Add pattern group" button, which is located to the right of the PII category. The main content area displays a table of patterns. The table has two columns: "Pattern name" and "Regex". The patterns listed are:

Pattern name	Regex
France Driver's License Number	[0-9]{12}
France National ID Card (CNI)	[0-9]{12}
France Passport Number	[0-9]{2}[a-zA-Z]{2}[0-9]{5}
Company ID	[0-9]{6}

At the bottom of the table, there is a blue link labeled "+ Add pattern to group".

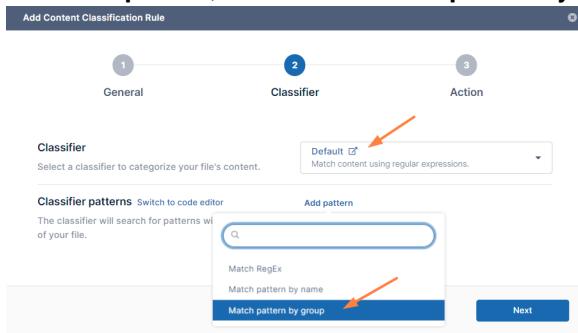
It is also added to the list **All Patterns**, so you can add it to a rule individually or as part of the pattern group.

## Adding a regex pattern group to a rule

The following procedure shows you how to add a regex pattern group to a rule on the second page of the rule wizard. For full instructions on adding a rule, see [Creating a Smart Classification Rule](#) (see page 126).

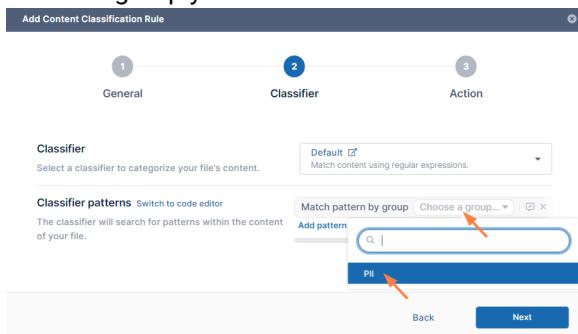
### To add a regex pattern group to a rule:

1. On the second page of the **Add a Content Classification Rule** wizard, choose either of the regex classifiers, **Default** or **Solr Pattern Match**.
2. Click **Add pattern**, and choose **Match pattern by group**.



Match pattern by group is now listed in **Classifier patterns**.

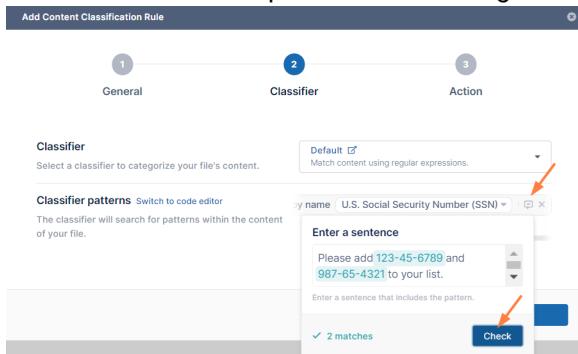
3. Click the drop-down list next to it.
- Any groups you have added are listed under the search box.
4. Click the group you want to use for the rule:



Once the group is selected, you can test the different patterns in the group together.

5. To test the pattern group, click the comment check icon next to the group name.
6. Enter a sentence or phrase that includes any number of patterns from the group, and click check.

The test verifies if the patterns are working and how many times matching patterns appear:



## Creating a Smart Classification Rule

A Smart Classification rule specifies:

- The classifier that categorizes your content a certain way (for example, by regex or by AI)
- The pattern to match
- The metadata to apply to the file depending on whether a pattern match is found

For example, a rule could specify that Smart Classification should attempt to match an ID number pattern in the content of a file, and to set the metadata variable **PII** to **yes** or **no** depending on whether or not there is a match.

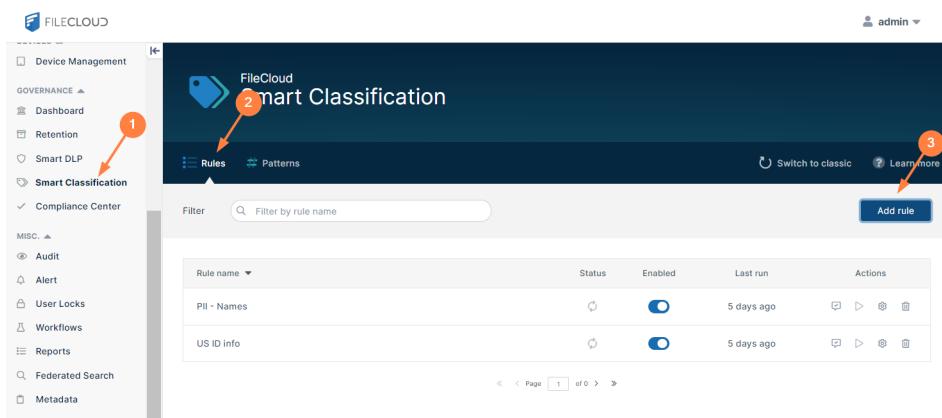


When you automate running of a Smart Classification rule, it classifies all existing files in FileCloud, and then runs on each file that is added or updated. The initial run may be lengthy since many files may have to be classified. If you don't automate running of a rule, and only run it manually, during each manual run it classifies all content in FileCloud. If you have a large number of files, each manual run may take a long time.

The following procedure uses an example in which the **Default** classifier, a regex classifier, is used with the predefined pattern for U.S. social security number.

### To create a smart classification rule:

1. In the navigation panel, click **Smart Classification**.  
The **Smart Classification** screen opens.
2. In the menu bar, click **Rules** if it is not already selected.
3. Click **Add rule**.



The **General** screen of the **Add Content Classification Rule** wizard opens.

4. In **Rule name**, enter a name for the rule.
5. In most cases, you will enable **Automatic execution** so the rule runs automatically on a schedule on files added and updated since the last run.  
If you only want to run the rule manually, leave it disabled.

Add Content Classification Rule

1 General      2 Classifier      3 Action

**Rule name** PII 

Describe the new rule so it's easier for you to find it later.

**Automatic execution** 

If enabled, the classification rule will be executed whenever a file is created or updated. Otherwise, it will only run manually.

**Filters** [Switch to code editor](#) [Add filter](#) [Add group](#)

Set filters that determine if the classifier runs.

Cancel **Next**

- Click **Add Filter**, and choose a predefined condition, and set the numerical value.
- Note:** The final filter value in the drop-down list, **Anything**, applies no filter (allows all files to be classified).

Add Content Classification Rule

1 General      2 Classifier      3 Action

**Rule name** PII 

Describe the new rule so it's easier for you to find it later.

**Automatic execution** 

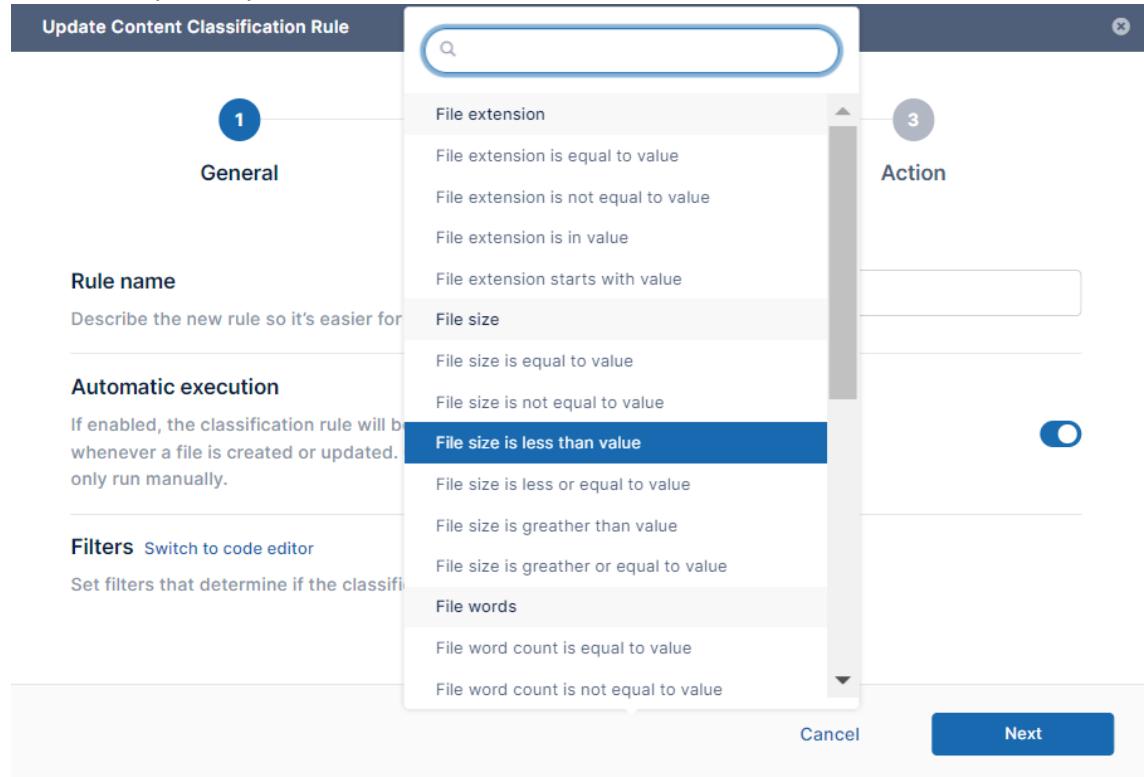
If enabled, the classification rule will be executed whenever a file is created or updated. Otherwise, it will only run manually.

**Filters** [Switch to code editor](#) [Add filter](#) [Add group](#)

Set filters that determine if the classifier runs.

Cancel **Next**

In this example, the predefined condition **File size is less than value** is chosen.



7. For this example, the value is set to **5 MB**.

**Note:** Files greater than **10 MB** are not available to be classified.

1 General 2 Classifier 3 Action

**Rule name** PII  
Describe the new rule so it's easier for you to find it later.

**Automatic execution**  
If enabled, the classification rule will be executed whenever a file is created or updated. Otherwise, it will only run manually.

**Filters** Switch to code editor  
Set filters that determine if the classifier runs.

File size is less than 5 MB  
Add filter Add group

Cancel Next

**Notes:**

- You can add complex conditions by using the **Add filter** and **Add group** options together. Clicking **Add filter** ANDs another condition to the first. Clicking **Add group** adds a group of conditions that are ANDed to each other, and as a whole, ANDed to the previous condition.
- Alternately, you can click **Switch to code editor**, and write your condition in Expression Language if you are familiar with it. For help with expression language, see [https://symfony.com/doc/current/reference/formats/expression\\_language.html](https://symfony.com/doc/current/reference/formats/expression_language.html).
- If you want to switch an **AND** condition to an **OR** condition click the word **AND** (and click **OR** to toggle it back to **AND**).

8. Click **Next**.  
The **Classifier** screen of the wizard opens.

9. In the **Classifier** drop-down list, choose a classifier.  
In the example below, the classifier **Default** is chosen.

**Classifier**

Select a classifier to categorize your file's content.

**Classifier patterns** [Switch to code editor](#)

The classifier will search for patterns within the content of your file.

**Default**  Match content using regular expressions.

**Solr Pattern Match**  
Match content using regular expressions in Solr.

**Solr Standard Query**  
Match content using Solr's Standard Query.

**ICAP DLP**  
ICAP not configured

**Singapore NRIC**  
Match Singapore National Registration Identity Card.

**AI Classifier** NEW  
Match associated content using artificial intelligence.

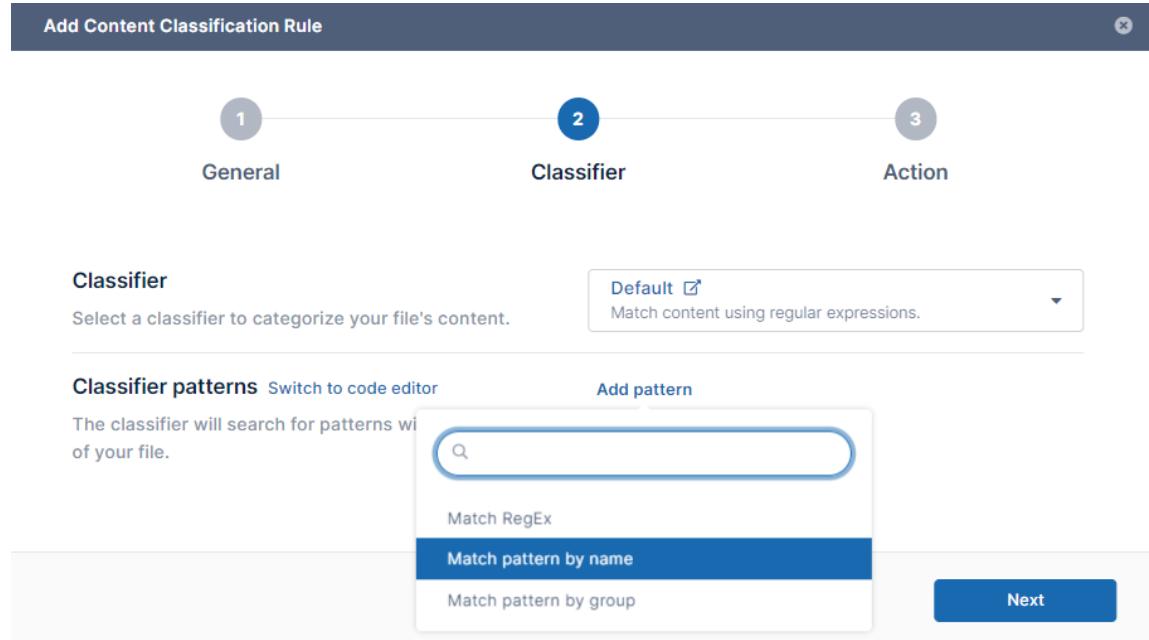
For help using classifiers, see [Guide to Classifiers](#) (see page 144)

**Note:** If you choose the **ICAP DLP** or the **Singapore NRIC** classifiers, the classifier pattern is preset, so the **Add Pattern** option below no longer appears on the screen.

10. After you choose a Classifier, if **Classifier patterns** still appears below it, click **Add Pattern**. The options vary depending on the classifier you have chosen. For help entering the pattern for each option, see [Guide to Classifiers](#) (see page 144). In this example where the **Default** classifier is used, when **Add Pattern** is clicked, the options **Match RegEx**, **Match pattern by name**, and **Match pattern by group** are shown.

11. Click one of the options.

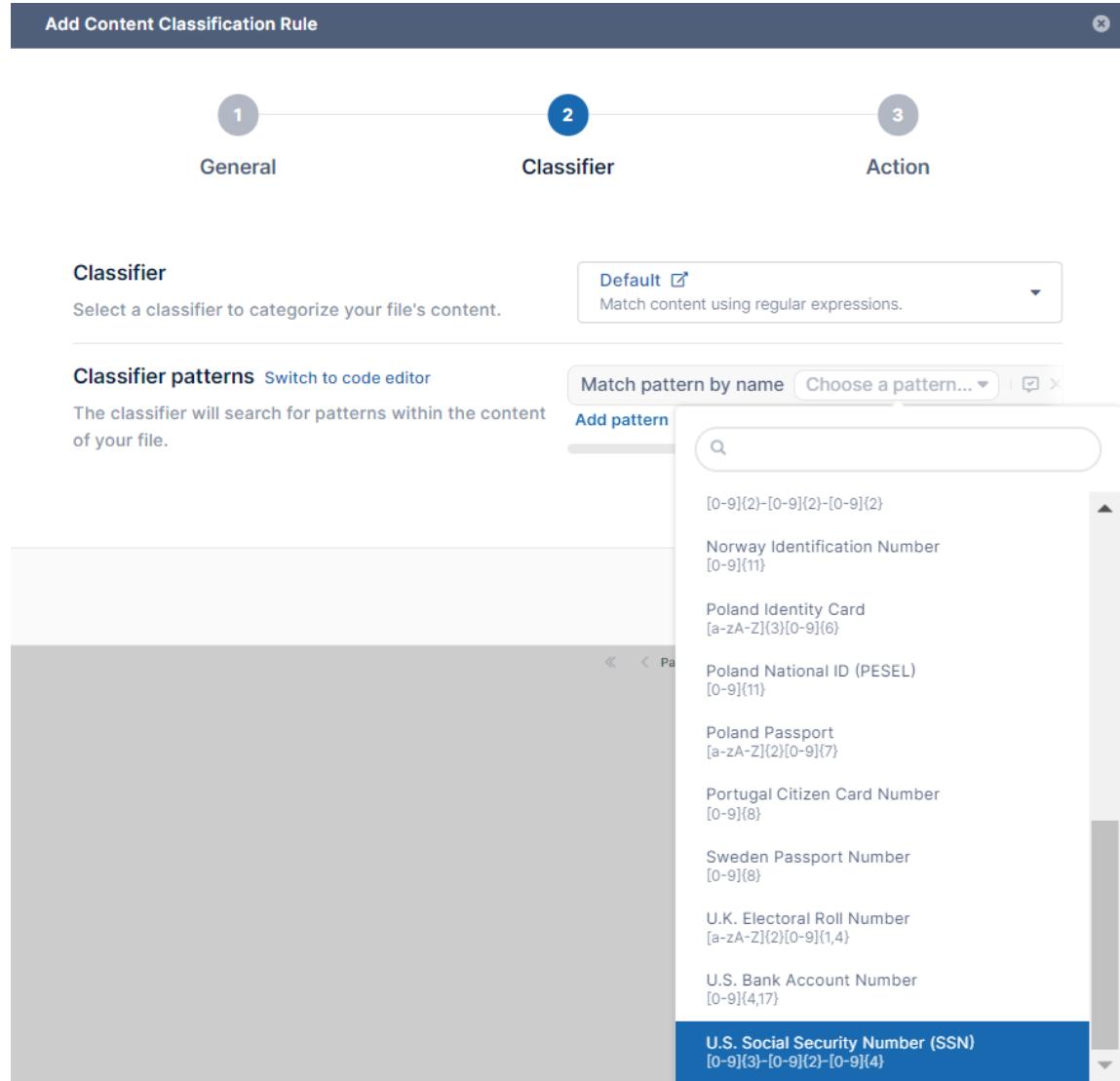
Here, **Match pattern by name**, which enables you to choose a predefined pattern, is chosen.



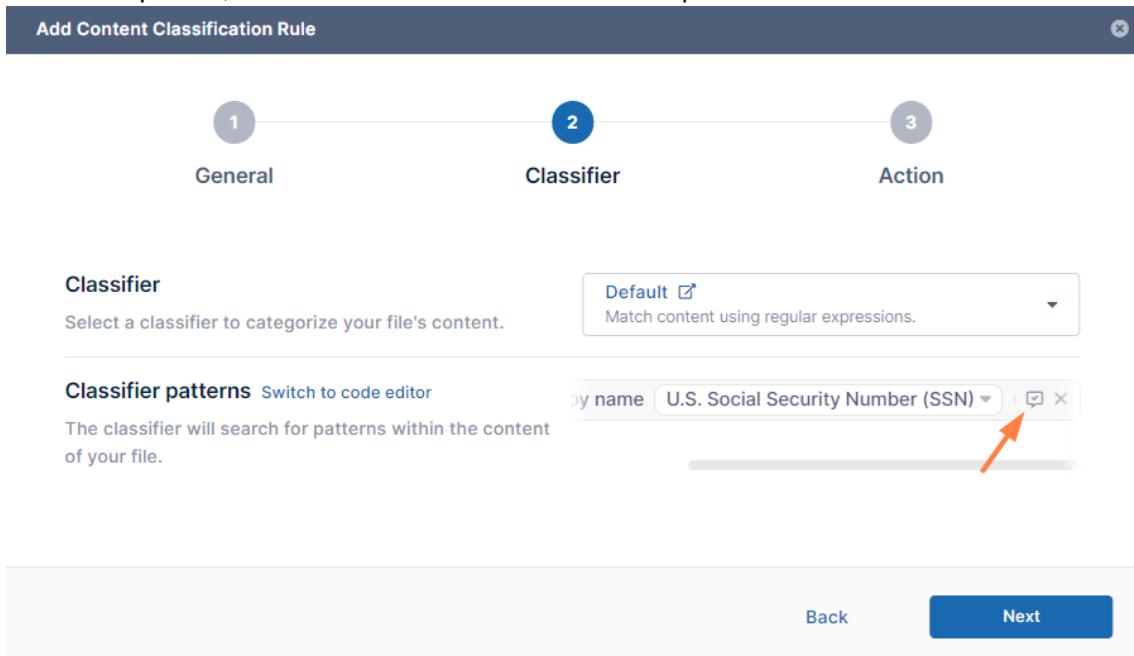
The screenshot shows the 'Add Content Classification Rule' wizard, step 2: Classifier. The steps are numbered 1 (General), 2 (Classifier, highlighted in blue), and 3 (Action). The 'Classifier' section shows a dropdown menu with 'Default' selected and 'Match content using regular expressions.' The 'Classifier patterns' section includes a search bar, a 'Match RegEx' button, and a 'Match pattern by name' button, which is highlighted with a blue background. A 'Match pattern by group' button is also present. A 'Next' button is located at the bottom right.

12. Choose a predefined pattern in the **Choose a pattern** drop-down list.

**U.S. Social Security Number** is chosen.

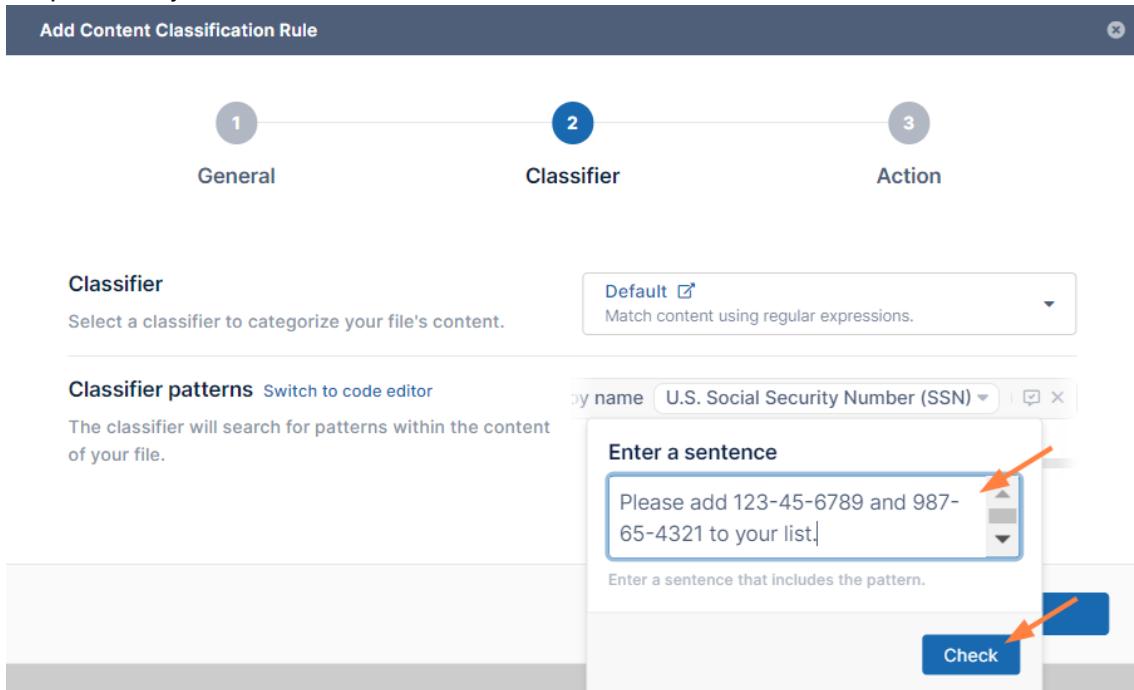


13. To test the pattern, click the Test Pattern icon next to the pattern.



The screenshot shows the 'Add Content Classification Rule' interface. It is on step 2, 'Classifier'. The 'Classifier' section is selected. A pattern 'U.S. Social Security Number (SSN)' is listed. A red arrow points to the 'Test' icon (a small blue square with a white checkmark) to the right of the pattern name.

You are prompted to enter a sentence that includes your pattern in the box that opens. Include the pattern any number of times.

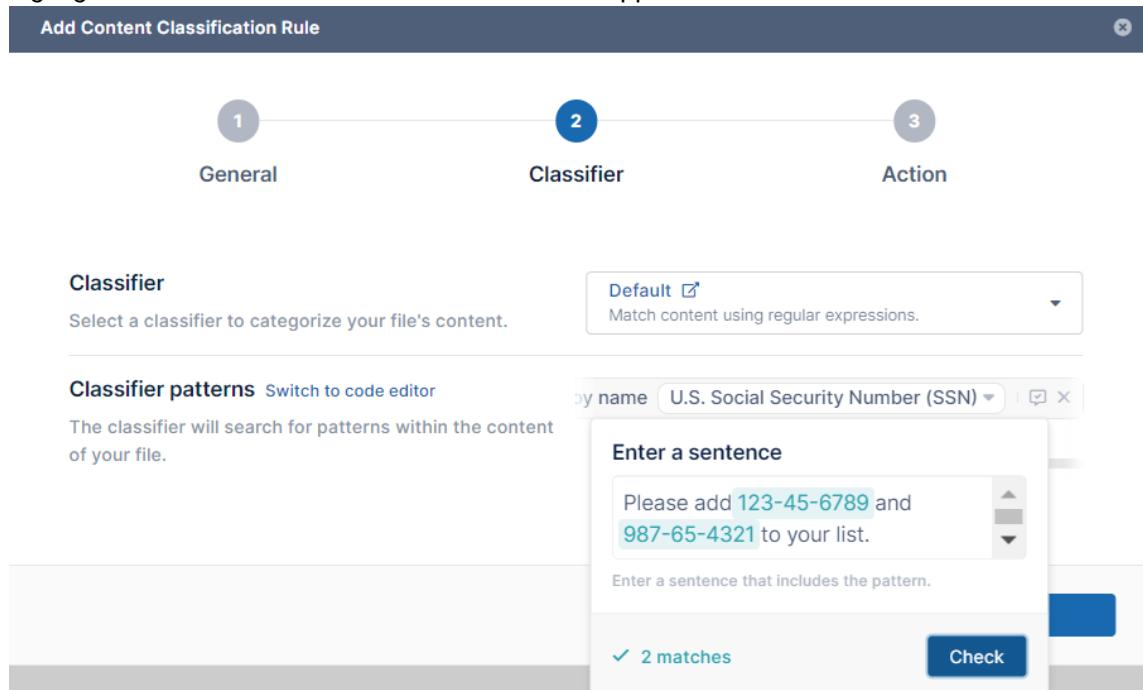


The screenshot shows the 'Add Content Classification Rule' interface. It is on step 2, 'Classifier'. The 'Classifier' section is selected. A pattern 'U.S. Social Security Number (SSN)' is listed. Below it, a test sentence 'Please add 123-45-6789 and 987-65-4321 to your list.' is entered in a text area. A red arrow points to the 'Check' button at the bottom right of the test area. Another red arrow points to the text area where the sentence is entered.

14. Click **Check**.

If the **Classifier pattern** is working, the terms that match the pattern in your sentence are

highlighted and a count of the number of matches appears below the sentence.



15. If the pattern is successful, click **Next**.

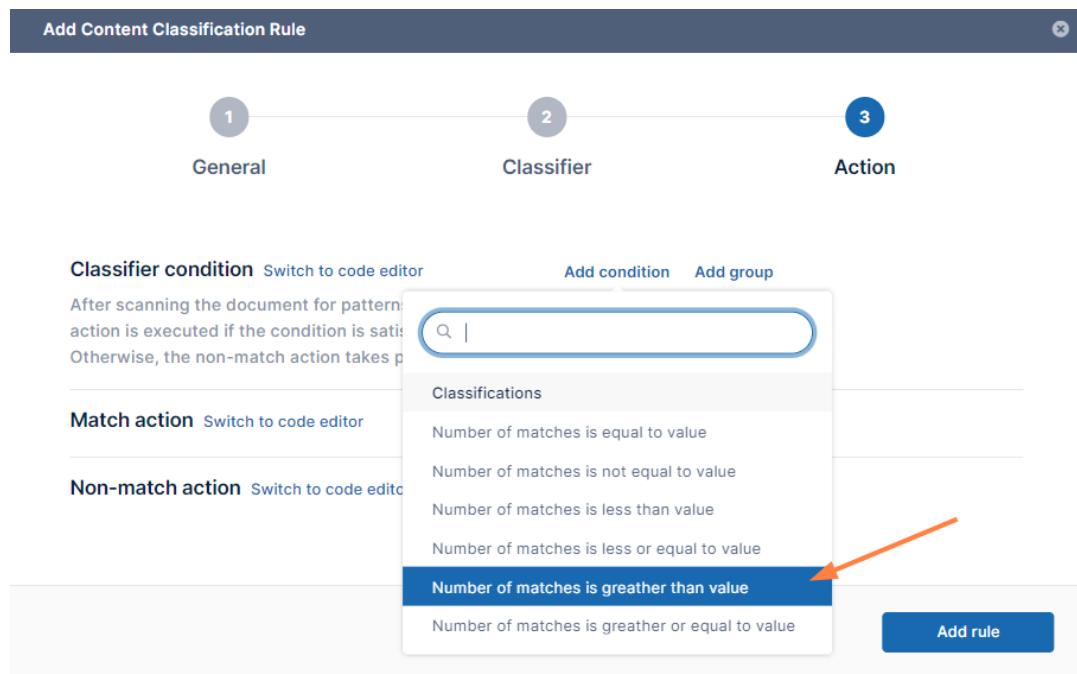
The **Action** screen of the **Add Content Classification Rule** wizard opens.

16. Add a **Classifier condition**.

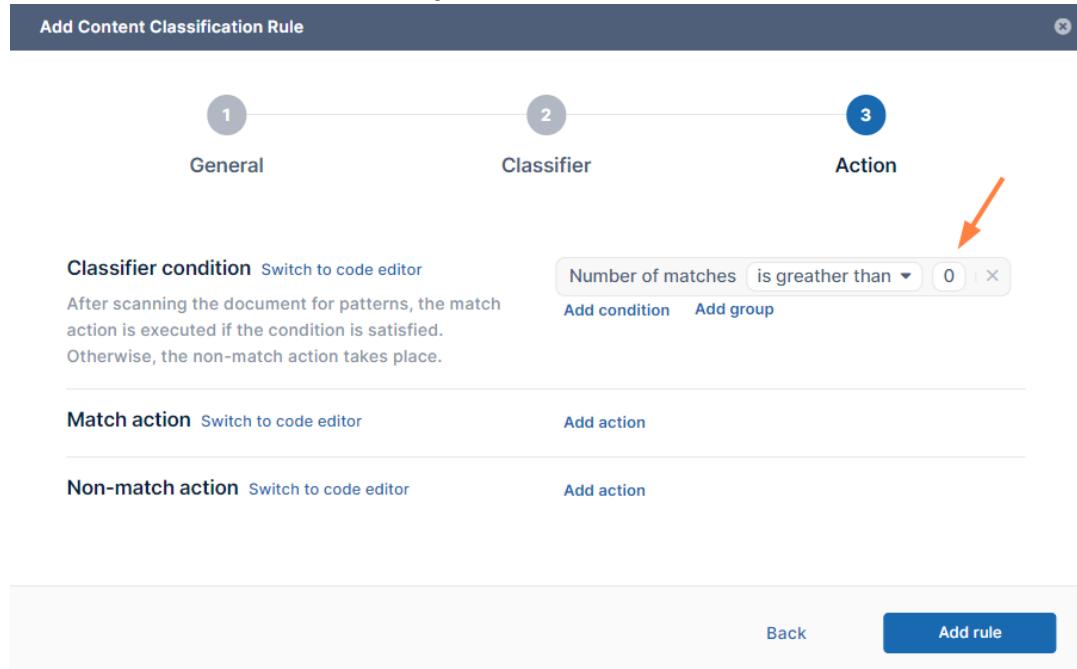
**Notes:**

- In many cases you can click **Add condition** and choose **Number of matches is greater than value**, and set value to **0**.
- In most cases, there is no need for a complex condition, and choosing **Add group** is not necessary.
- If you add multiple **Classifier conditions**, you can switch an **AND** condition to an **OR** condition by clicking the word **AND**. Click **OR** to toggle it back to **AND**.
- If you are familiar with Expression Language, you can click **Switch to code editor** and add a condition in Expression Language.

In this example the condition **Number of matches is greater than value** is added.

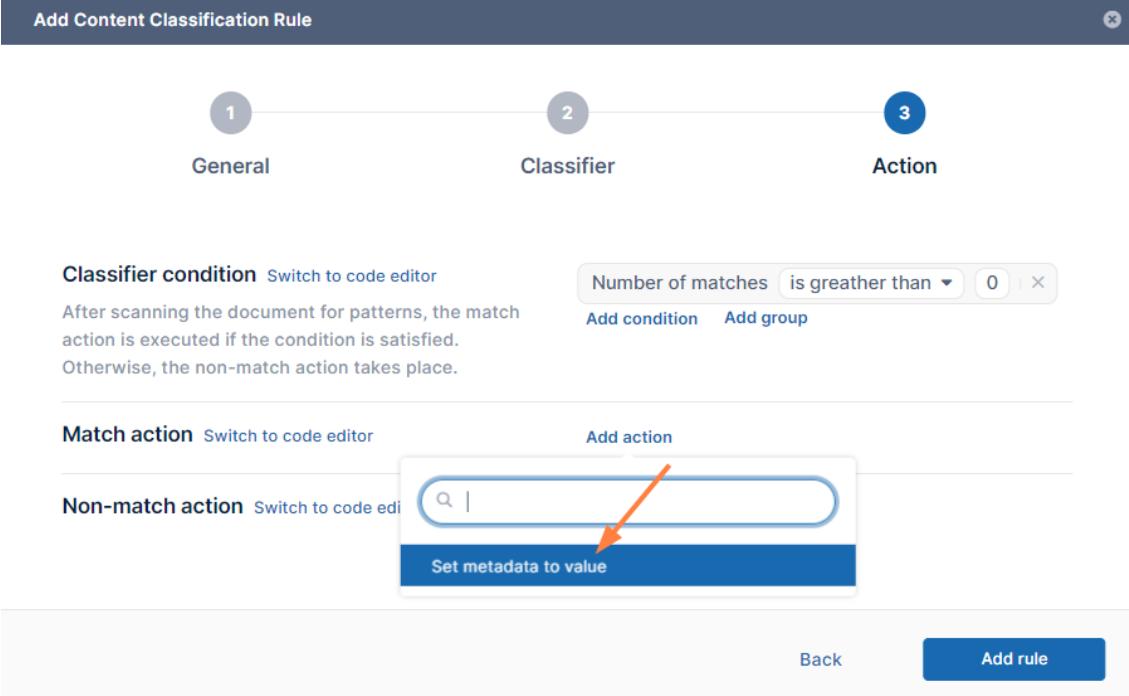


The classifier condition is added and by default set to **0**. In most cases, you can leave the value of **0**, but if you only want the classifier to treat the result as a match if more than 1 matches are found, enter a number greater than .



17. Add a **Match action** either by clicking **Add action** and choosing **Set metadata to value**, or, if you are familiar with JSON, by clicking **Switch to code editor**, and adding an action in JSON. Any number of actions may be added. In this example, **Add action** is clicked and the only current option, **Set metadata to value**, is

chosen.



**Classifier condition** Switch to code editor

After scanning the document for patterns, the match action is executed if the condition is satisfied. Otherwise, the non-match action takes place.

**Number of matches** is greater than 0

**Match action** Switch to code editor

**Non-match action** Switch to code editor

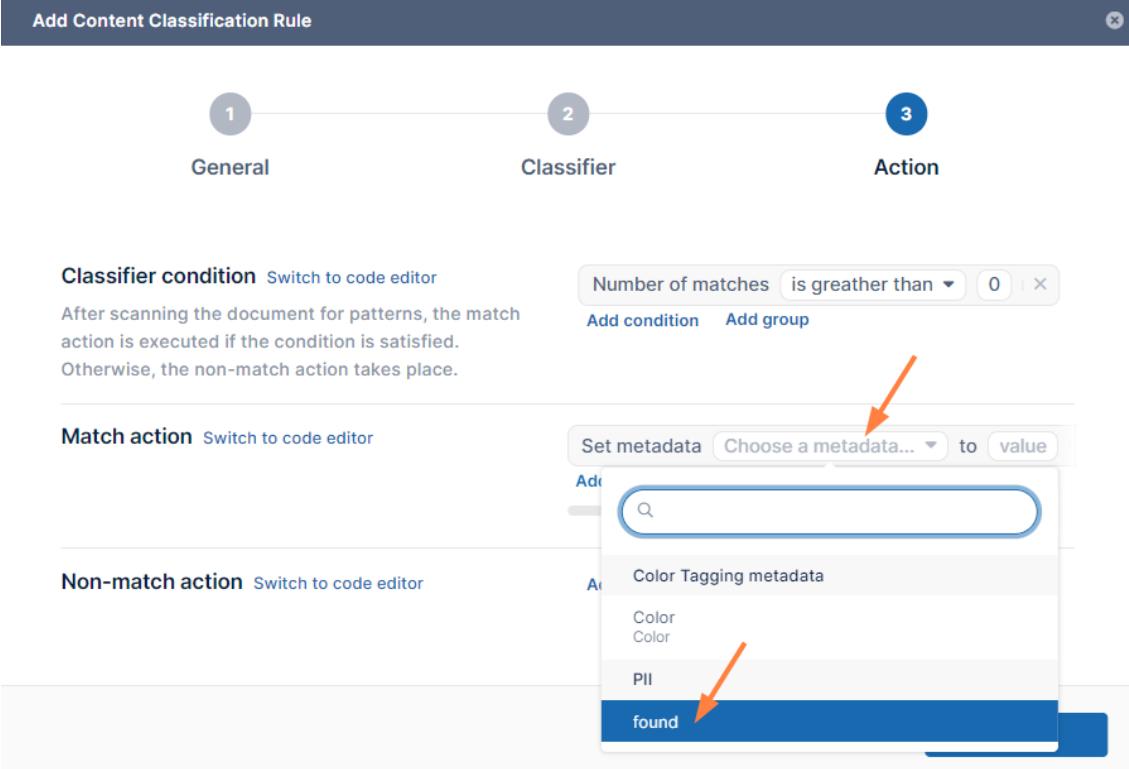
**Add action**

**Set metadata to value**

**Back** **Add rule**

18. Click in the **Choose a metadata** field. **Color Tagging metadata** and any custom metadata you have created is listed with its attributes below it.
19. Click one of the metadata attributes.

In this example, the **PII** metadata attribute **found** is selected.



**Classifier condition** Switch to code editor

After scanning the document for patterns, the match action is executed if the condition is satisfied. Otherwise, the non-match action takes place.

**Number of matches** is greater than 0

**Match action** Switch to code editor

**Non-match action** Switch to code editor

**Set metadata** Choose a metadata... to value

**Color Tagging metadata**

**Color**

**Color**

**PII**

**found**

20. Set a value for the metadata attribute.

Here **found** is set to **yes**.

In another process, such as DLP or a search, this enables FileCloud to locate files with PII information in them by looking for files with **PII.found** set to **yes**.

21. To include an action that occurs when the condition is not met, repeat the process for **Non-match action**. However, you may leave **Non-match action** blank.

In this example, the same metadata attribute is chosen, but it is set to **no**.

Add Content Classification Rule

1 General      2 Classifier      3 Action

**Classifier condition** [Switch to code editor](#)

Number of matches is greater than 0 [Add condition](#) [Add group](#)

**Match action** [Switch to code editor](#)

Set metadata PII > found to yes [Add action](#)

**Non-match action** [Switch to code editor](#)

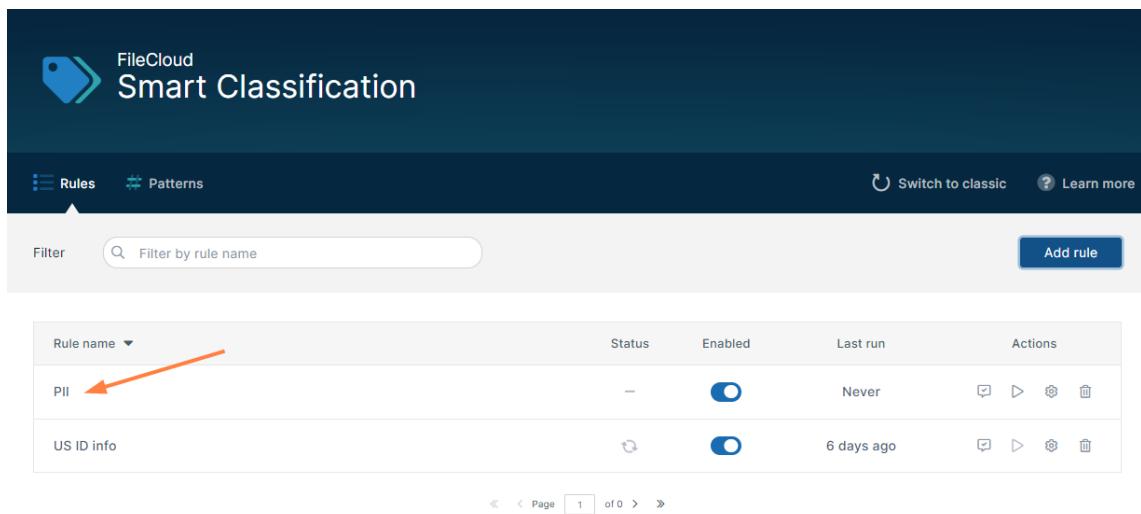
Set metadata PII > found to no [Add action](#)

Your rule is complete.

Back [Add rule](#)

22. Click **Add rule**.

The wizard closes and your rule is added to the Smart Classification page.



Rule name	Status	Enabled	Last run	Actions
PII	—	<input checked="" type="checkbox"/>	Never	<span>Run</span> <span>Run now</span> <span>Details</span> <span>Delete</span>
US ID info	⌚	<input checked="" type="checkbox"/>	6 days ago	<span>Run</span> <span>Run now</span> <span>Details</span> <span>Delete</span>

Since you created the rule to run automatically, it appears as enabled, and will run according to the Cron schedule. However, you can run it manually at any time by clicking the arrow under **Actions**.

## Running Smart Classification Rules

If you set the **Automatic Execution** switch on when you create a Smart Classification rule, the rule will run at scheduled times. If you have left the **Automatic Execution** switch off, you can only run the rule manually. At any time, you can also manually run a rule that is set to automatically execute (and it will continue to run on schedule as well).

Add Content Classification Rule

1 General      2 Classifier      3 Action

**Rule name** Detect Personal Info  
Describe the new rule so it's easier for you to find it later.

**Automatic execution**  
If enabled, the classification rule will be executed whenever a file is created or updated. Otherwise, it will only run manually. 

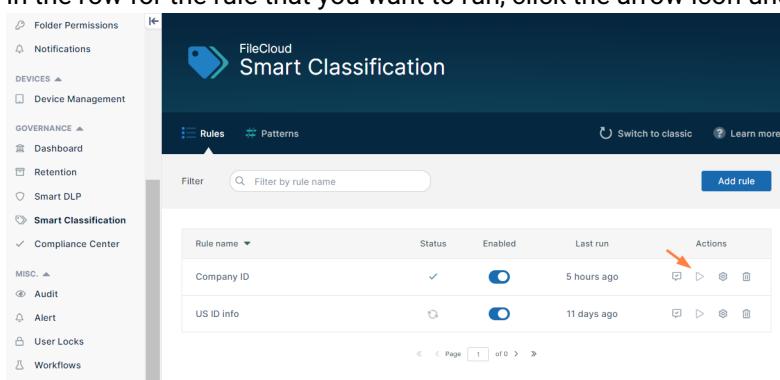
**Filters** Switch to code editor  
Set filters that determine if the classifier runs.  

Cancel 

The **Automatic execution** switch is in the on position.

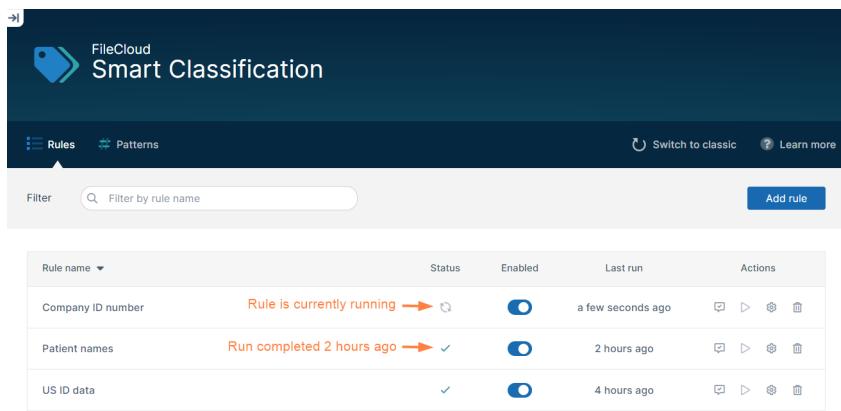
#### To run a Smart Classification rule manually:

1. In the navigation panel, click **Smart Classification**  
The **Smart Classification** screen opens to the **Rules** page.
2. In the row for the rule that you want to run, click the arrow icon under **Actions**.



Rule name	Status	Enabled	Last run	Actions
Company ID	✓		5 hours ago	
US ID Info	✗		11 days ago	

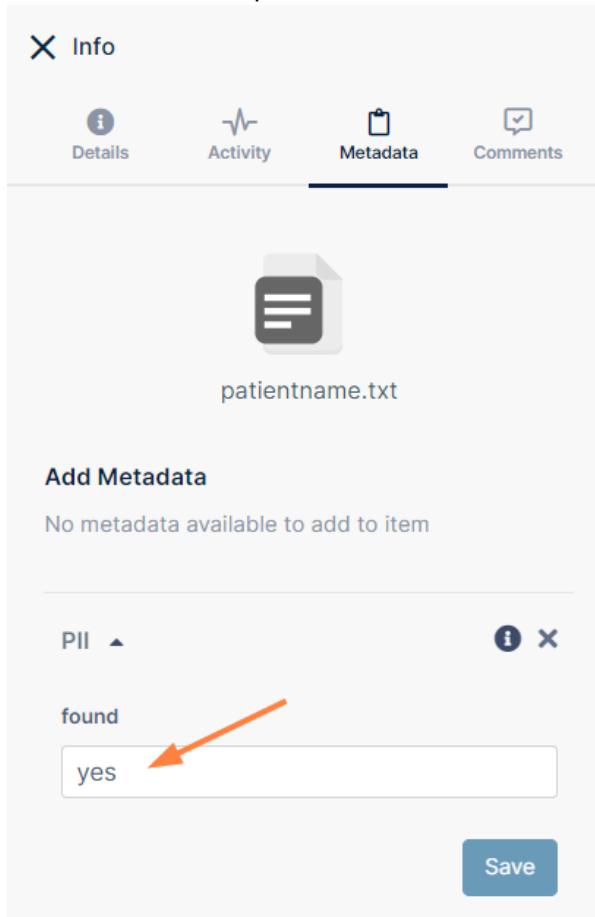
While the rule is running, the **Status** column shows a rotating arrow icon. When running is complete, the **Status** column shows a check. The **Last Run** column shows how many minutes or days ago the rule was last run.



The screenshot shows the FileCloud Smart Classification interface. At the top, there is a navigation bar with the FileCloud logo, the title 'Smart Classification', and tabs for 'Rules' and 'Patterns'. Below the navigation bar is a search bar with the placeholder 'Filter by rule name' and a 'Add rule' button. The main area displays a table of rules with columns: 'Rule name', 'Status', 'Enabled', 'Last run', and 'Actions'. The table contains three rows:

Rule name	Status	Enabled	Last run	Actions
Company ID number	Rule is currently running	<input checked="" type="checkbox"/>	a few seconds ago	<span>⋮</span> <span>▶</span> <span>⚙</span> <span>trash</span>
Patient names	Run completed 2 hours ago	<input checked="" type="checkbox"/>	2 hours ago	<span>⋮</span> <span>▶</span> <span>⚙</span> <span>trash</span>
US ID data		<input checked="" type="checkbox"/>	4 hours ago	<span>⋮</span> <span>▶</span> <span>⚙</span> <span>trash</span>

If the rule ran successfully, files containing the pattern searched for should now be tagged with the metadata value specified in the rule.



The screenshot shows the 'Info' page for a file named 'patientname.txt'. The page has a navigation bar with tabs: 'Info' (selected), 'Details', 'Activity', 'Metadata' (selected), and 'Comments'. Below the navigation bar is a preview of the file (a small icon of a text document) and the file name 'patientname.txt'. The 'Metadata' tab is selected, showing a table with a single row:

PII	found
	yes

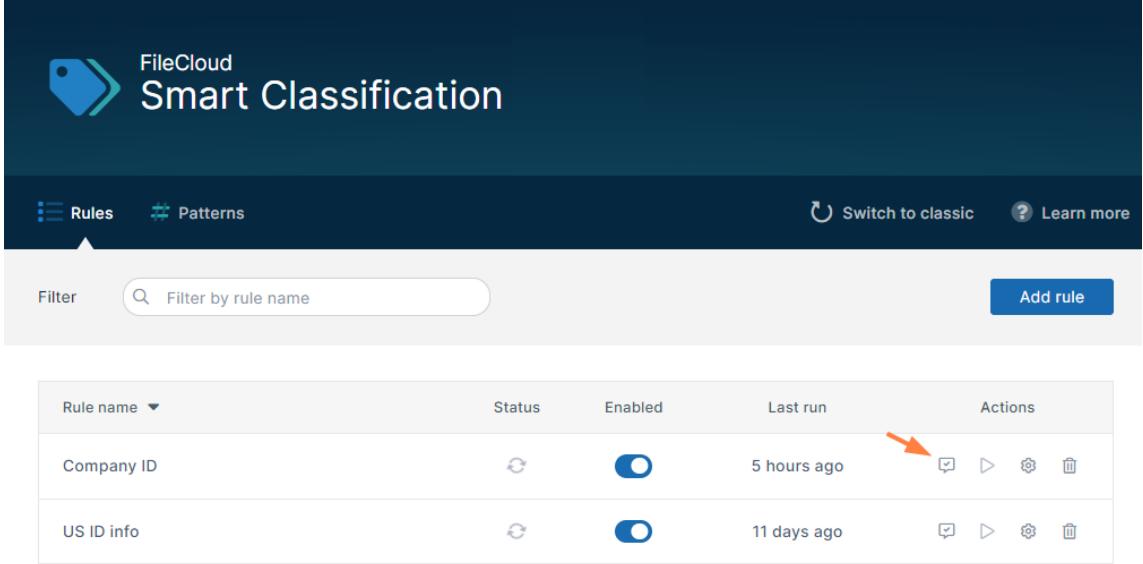
An orange arrow points to the 'yes' value in the 'found' column. At the bottom of the page is a 'Save' button.

## Testing a Smart Classification Rule

You can test a rule that is listed on the **Rules** tab of the **Smart Classification** page and see what metadata tags the rule would apply to a file containing your test content.

### To test a Smart Classification rule:

1. In the row for the rule, click the Test Pattern icon.



Rule name	Status	Enabled	Last run	Actions
Company ID	⌚	●	5 hours ago	   
US ID info	⌚	●	11 days ago	   

The **Content Classification Playground** opens and shows the content of the rule in the bulleted steps on the right.

2. You may either:

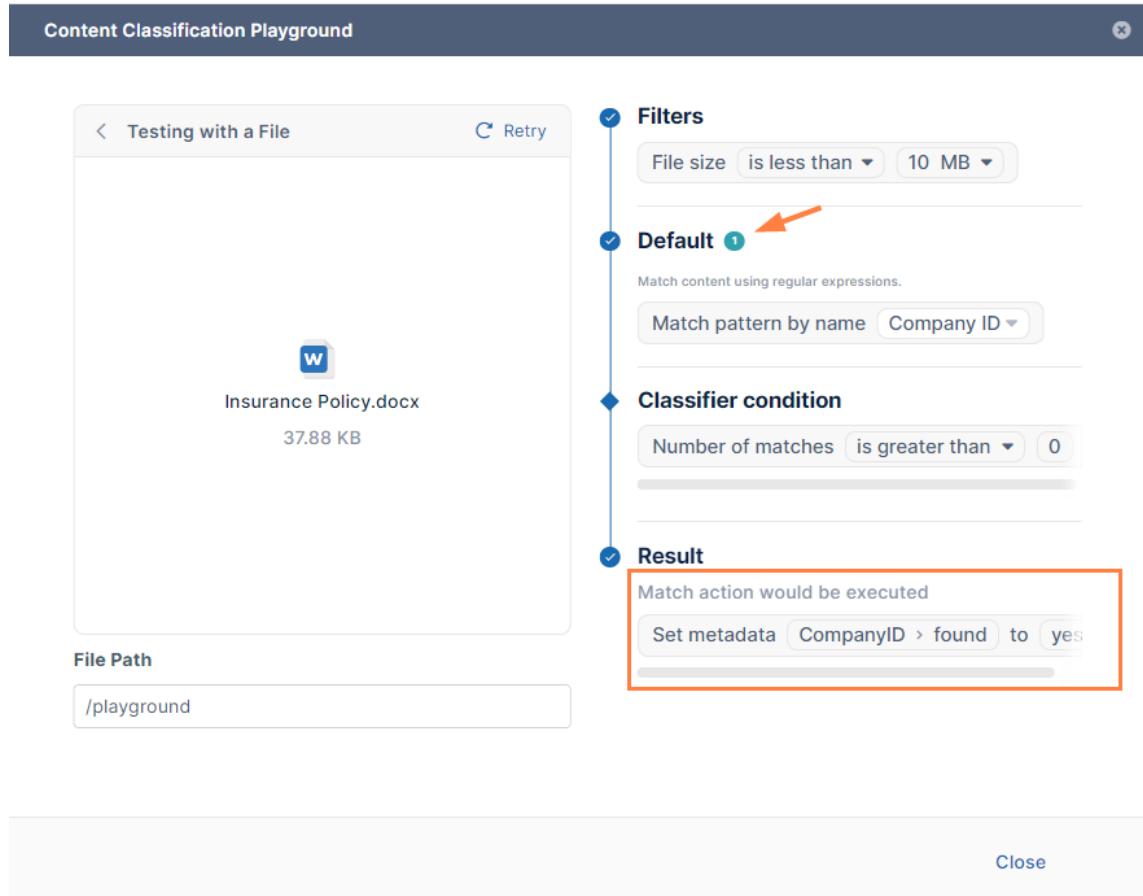
- Drop a file with content that you want to test into the box on the left
- Click **Write content** to manually write the test text
- Click **Choose from your computer** to open file explorer and choose a file.

**Note:** If you drop a file or choose it from your computer, the test begins running automatically, but if you write content manually, you must click the **Execute** link at the top of the box:

3. As the test runs through each step it highlights it.

When the test is complete, the second step shows the number of matches, and the final step, **Result**, shows the outcome. In the following screenshot, the test finds one match, **Default** shows

1 and **Result** displays **Match action would be executed** and lists the result of the match action, **Set metadata CompanyID.found to yes**.



The screenshot shows the 'Content Classification Playground' interface. On the left, under 'Testing with a File', a file named 'Insurance Policy.docx' (37.88 KB) is listed. On the right, a classification rule is defined:

- Filters:** File size is less than 10 MB.
- Default 1:** Match content using regular expressions. (An orange arrow points to this step.)
- Classifier condition:** Number of matches is greater than 0.
- Result:** Match action would be executed. Set metadata CompanyID > found to yes. (This step is highlighted with an orange box.)

At the bottom right of the main window is a 'Close' button.

## Examples

The first example test the same rule as the one shown in the procedure above. The rule uses the **Default** (regex) classifier. The admin drags and drops a file with text that contains one instance of the pattern (a 6-digit Company ID). The test begins automatically. Each bulleted test step on the right is highlighted when it is reached. The number 1 appears next to **Default** to indicate that there was one match. **Result** states that the **Match action would be executed** and that the rule would **Set metadata Company ID.found to Yes**.

The  
next

example tests a rule that uses the **AI Classifier**. The admin clicks **Write Content** and first enters text that does not include the match term **first or last names**. Since the text is entered manually, the admin must click **Execute**. **0** appears next to **AI Classifier** to indicate that there were no matches. **Result** states that **Match action would not be executed** and that the rule would **Set metadata PII.found to No**. Then the admin changes the text to include two first and last names, and clicks **Execute** again. Now **4** appears next to **AI Classifier** to indicate that there were 4 matches (2 first names and 2 last names). **Result** states that **Match action would be executed** and that the rule would **Set metadata PII.found to Yes**.

Gui  
de  
to

## Classifiers

### Default

## Default

### Definition

Classifies by whether content is an exact match for a regex PCRE pattern or is not an exact match for a regex PCRE pattern.

### Comparison to Solr Pattern Match

A more powerful classifier that can match patterns with spaces and special characters and returns the text that has been matched as well as the number of times the text was matched.

### Result schema to use if using code editor:

```
(_classifications): [{term: "term that matched a regex", count: "number of times the term appears in the doc"}, ...]
```

### Pattern options:

Any number of patterns may be added. Each pattern is connected to the previous pattern with OR.

- **Match RegEx** - Match with a manually-entered regular expression
- **Match pattern by name** - Match with predefined regular expression
- **Match pattern by group** - Match with a predefined group of regular expressions

### Examples:

#### Match with RegEx:



**Match pattern by name:**

	<b>Match</b>
--	--------------

**pattern by group:**

	<b>Code</b>
--	-------------

**editor example:**

```
{"SEARCH_PATTERN_SET": "[0-9]{6}"]}
```

**Solr Pattern Match**

## Solr Pattern Match

### Definition

Classifies by whether content is an exact match for a Solr regex pattern or is not an exact match for a Solr regex pattern.

### Comparison to Default

Not as powerful as Default, but faster. Cannot match patterns with spaces and special characters. Does not return the text that has been matched.

### Result schema to use if using code editor:

```
(_classifications): ["regex pattern", ...]
```

### Pattern options:

Any number of patterns may be added. Each pattern is connected to the previous pattern with OR.

- **Match RegEx** - Match with a manually-entered regular expression
- **Match pattern by name** - Match with predefined regular expression
- **Match pattern by group** - Match with a predefined group of regular expressions

### Examples:

#### Match with RegEx:



**Match pattern by name:**



**Match**

**pattern by group:**



**Code editor**

**example:**

```
{"SEARCH_PATTERN_SET": "[0-9]{16}"]}
```

**Solr Standard Query**

## Solr Standard Query

### Definition

Classifies by whether content matches a Solr standard query.

For help writing Solr standard queries, see [https://solr.apache.org/guide/6\\_6/the-standard-query-parser.html](https://solr.apache.org/guide/6_6/the-standard-query-parser.html)

### Result schema to use if using code editor:

```
(_classifications): ["expression"] or []
```

### Pattern option:

Any number of patterns may be added. Each pattern is connected to the previous pattern with OR.

**Match Standard Query expression** - Match with a specific term or number such as **confidential** or **514367A**

### Example:



#### example:

```
{"STANDARD_QUERY_EXPRESSION":["confidential"]}
```

### ICAP DLP

## ICAP DLP

To enable selection of the the ICAP DLP classifier, you must enable ICAP DLP in FileCloud.

For the ICAP DLP classifier to function properly in FileCloud, you must [set up rules in ePolicy Orchestrator](#)<sup>86</sup>that specify if a file is authorized or not authorized.

### Definition

Classifies by results on file authorization returned from ICAP DLP. ICAP DLP either authorizes or does not authorize a file, so the metadata you define for the rule should indicate if the file was authorized or not.

Your actions might appear as:

Update Content Classification Rule

1 General      2 Classifier      3 Action

**Classifier condition** [Switch to code editor](#)

Number of matches is greater than 0 [x](#)

[Add condition](#) [Add group](#)

**Match action** [Switch to code editor](#)

Set metadata DLP allowed > dlp-allowed to [off](#)

[Add action](#)

**Non-match action** [Switch to code editor](#)

Set metadata DLP allowed > dlp-allowed to [on](#)

[Add action](#)

Back [Save rule](#)

### Result schema to use if using code editor:

(\_classifications): []

<sup>86</sup> <https://docs.trellix.com/bundle/epolicy-orchestrator-landing>

## Example



## Example:



## AI Classifier

To enable selection of the the AI Classifier, you must integrate FileCloud with an AI-based provider.

## Definition

Classifies content into terms that match an AI prompt

### Pattern option:

Any number of patterns may be added. Each pattern is connected to the previous pattern with OR.

**Match instances of prompt** - Match with a manually entered prompt, such as **PII** or **first or last names**

### Example:



#### example:

```
{"SEARCH_AI_MATCHES":["PII"]}
```

## Editing a Smart Classification Rule

To edit a Smart Classification rule, change any of the settings you entered in the wizard when you created it. For information about the fields in the wizard, see [Creating a Smart Classification Rule \(see page 126\)](#)

### To edit a Smart Classification rule:

1. Click the gear icon to the right of the rule.

The screenshot shows the 'Smart Classification' interface with the 'Rules' tab selected. A table lists a single rule: 'Company ID number'. The 'Actions' column for this rule contains several icons, with a red arrow pointing to the 'Edit' icon (pencil).

The **Update Content Classification Rule** wizard opens to the **General** screen.

The screenshot shows the 'Update Content Classification Rule' wizard. The title bar says 'Update Content Classification Rule'. The navigation bar at the top has three steps: 1 General (highlighted with a blue circle), 2 Classifier, and 3 Action.

**General** screen details:

- Rule name:** Company ID number
- Automatic execution:** Enabled (switch is blue)
- Filters:** File size is less than 10 MB

At the bottom right of the wizard window are 'Cancel' and 'Next' buttons.

2. Make any changes to the values on the screen.
3. Click **Next**, and make any changes to the **Classifier** screen.
4. Click **Next**, and make any changes to the **Action** screen.
5. Click **Save Rule**.  
The rule now applies the changed settings when it runs.

**Note:** Metadata added to files and folders when the rule ran previously is not removed when the rule is edited.

## Deleting a Smart Classification Rule

### To delete a smart classification rule:

1. Click the delete icon to the right of the rule.

The screenshot shows the 'Smart Classification' section of the FileCloud interface. At the top, there are tabs for 'Rules' and 'Patterns', and buttons for 'Switch to classic' and 'Learn more'. Below this is a search bar with 'Filter by rule name' and an 'Add rule' button. The main area displays a table with two rows of rules. Each row includes a 'Rule name', 'Status' (Enabled), 'Last run' (14 days ago), and an 'Actions' column with several icons. An orange arrow points to the delete icon (trash can) in the 'Actions' column for the second rule, 'Patient names'.

Rule name	Status	Last run	Actions
US ID data	Enabled	14 days ago	
Patient names	Enabled	14 days ago	

You are prompted to confirm that you want to delete the rule.

2. Click **Delete**.

The rule is deleted.

**Note:** Metadata added to files and folders when the rule was run previously is not deleted.

## Smart Classification Examples

The following examples refer to custom metadata that would have to be created before creating the Smart Classification rule; a Smart Classification rule cannot be saved unless you specify which metadata field to set.

### Identifying files less than 5 MB containing US social security numbers

Rule name	Tag files <5 MB with US social security numbers
Automatic execution	Enable
Filters	File size is less than [5 MB]
Classifier	Default
Classifier patterns	Match pattern by name [U. S. Social Security Number (SSN)]

<b>Classifier condition</b>	<b>Number of matches is greater than [0]</b>
<b>Match action</b>	Set metadata <b>[SSN.found]</b> to <b>yes</b>
<b>Non-match action</b>	Set metadata <b>[SSN.found]</b> to <b>no</b>

## Identifying files with extensions .txt and .pdf containing US social security numbers

<b>Rule name</b>	<b>Tag txt and pdf files with US social security numbers</b>
<b>Automatic execution</b>	<b>Enable</b>
<b>Filters</b>	<b>File extension is equal to [txt] OR File extension is equal to [pdf]</b> Note: Click <b>AND</b> to change it to <b>OR</b> .
<b>Classifier</b>	<b>Default</b>
<b>Classifier patterns</b>	<b>Match pattern by name [U. S. Social Security Number (SSN)]</b>
<b>Classifier condition</b>	<b>Number of matches is greater than [0]</b>
<b>Match action</b>	Set metadata <b>[SSN.found]</b> to <b>yes</b>
<b>Non-match action</b>	Set metadata <b>[SSN.found]</b> to <b>no</b>

## Identifying all files containing US social security numbers

<b>Rule name</b>	<b>Tag all files with US social security numbers</b>
<b>Automatic execution</b>	<b>Enable</b>
<b>Filters</b>	<b>Anything</b>

<b>Classifier</b>	<b>Default</b>
<b>Classifier patterns</b>	<b>Match pattern by name [U. S. Social Security Number (SSN)]</b>
<b>Classifier condition</b>	<b>Number of matches is greater than [0]</b>
<b>Match action</b>	<b>Set metadata [SSN.found] to yes</b>
<b>Non-match action</b>	<b>Set metadata [SSN.found] to no</b>

## Identifying files in the Team Folder HumanResources containing US social security numbers

<b>Rule name</b>	<b>Tag all Human Resources files containing US social security numbers</b>
<b>Automatic execution</b>	<b>Enable</b>
<b>Filters</b>	<b>File path starts with [TeamFolderAdmin/HumanResources]</b> Note: See Identifying a FileCloud Specific Path for help writing FileCloud folder paths.
<b>Classifier</b>	<b>Default</b>
<b>Classifier patterns</b>	<b>Match pattern by name [U. S. Social Security Number (SSN)]</b>
<b>Classifier condition</b>	<b>Number of matches [is greater than 0]</b>
<b>Match action</b>	<b>Set metadata [SSN.found] to yes</b>
<b>Non-match action</b>	<b>Set metadata [SSN.found] to no</b>

## Identifying files containing any pattern in the custom pattern group France ID numbers

<b>Rule name</b>	<b>France ID numbers</b>
------------------	--------------------------

Automatic execution	Enable
Filters	Anything
Classifier	Default
Classifier patterns	Match pattern by group [France ID numbers]
Classifier condition	Number of matches [is greater than 0]
Match action	Set [metadata ID.found] to yes
Non-match action	Set [metadata ID.found] to no

## Identifying files with Singapore National Registry Identity Card (NRIC)

Rule name	Tag files with Singapore NRIC
Automatic execution	Enable
Filters	Anything
Classifier	Singapore NRIC
Classifier condition	Number of matches [is greater than 0]
Match action	Set [metadata ID.found] to yes
Non-match action	Set [metadata ID.found] to no

## Identifying files with patterns matching American Express credit cards

Rule name	Tag files with American Express card numbers
Automatic execution	Enable

<b>Filters</b>	<b>Anything</b>
<b>Classifier</b>	<b>Default</b>
<b>Classifier patterns</b>	<p><b>Match RegEx [3[47]{1}[0-9]{13}]</b>  <b>OR</b>  <b>Match RegEx [3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}]</b>  <b>OR</b>  <b>Match RegEx [3[47]{1}[0-9]{2} [0-9]{4} [0-9]{4} [0-9]{3}]</b></p> <p>Note: Smart Classification automatically inserts <b>OR</b> when you add multiple <b>Classifier</b> patterns.</p>
<b>Classifier condition</b>	<b>Number of matches [is greater than 0]</b>
<b>Match action</b>	<b>Set [metadata ID.found] to yes</b>
<b>Non-match action</b>	<b>Set [metadata ID.found] to no</b>

## Identifying files with the exact phrase "Confidential - for internal use only"

<b>Rule name</b>	<b>Tag files marked as confidential</b>
<b>Automatic execution</b>	<b>Enable</b>
<b>Filters</b>	<b>Anything</b>
<b>Classifier</b>	<b>Default</b>
<b>Classifier patterns</b>	<b>Match RegEx [Confidential - for internal use only]</b>
<b>Classifier condition</b>	<b>Number of matches [is greater than 0]</b>
<b>Match action</b>	<b>Set [IncludesText.Confidential] to yes</b>
<b>Non-match action</b>	<b>Set [IncludesText.Confidential] to no</b>

## Mark files with different tags depending on the number of matches

In this rule, if a file has 0-2 five-digit numbers, it is marked as having a low possibility of personal ID information. If it has >2 five-digit numbers, it is marked as having a high possibility of personal ID information. This enables you to perform different operations on files with low and high likelihood of having a match. For example, you might choose to manually review files with low possibility, but automatically block files with high possibility.

Rule name	Tag files based on number of 5-digit numbers
Automatic execution	Enable
Filters	Anything
Classifier	Default
Classifier patterns	Match RegEx <code>[[0-9]{5}]</code>
Classifier condition	Number of matches [is greater than 2]
Match action	Set [ID.found] to high
Non-match action	Set [ID.found] to low

## Identifying files with a phrase that is the same or similar to "Confidential - for internal use only"

Rule name	Tag files with confidentiality phrases
Automatic execution	Enable
Filters	Anything
Classifier	Solr Standard Query

<b>Classifier patterns</b>	<b>Match Standard Query ["Confidential - for internal use only"~4]</b> (include "" around phrase)
	<b>Note:</b> ~4 indicates that all words in the phrase must appear, but may be within 4 words of each other. For example "Confidential - use for internal only" would be a match.
<b>Classifier condition</b>	<b>Number of matches [is greater than 0]</b>
<b>Match action</b>	<b>Set [IncludesText.Confidential] to yes</b>
<b>Non-match action</b>	<b>Set [IncludesText.Confidential] to no</b>

## Identifying files with a word that matches or is one letter different from "Confidential"

<b>Rule name</b>	<b>Tag files with words spelled similarly to confidential</b>
<b>Automatic execution</b>	<b>Enable</b>
<b>Filters</b>	<b>Anything</b>
<b>Classifier</b>	<b>Solr Standard Query</b>
<b>Classifier patterns</b>	<b>Match Standard Query [Confidential~1]</b> (do not include "" around word)
	<b>Note:</b> ~1 indicates that there may be 1 letter different in the spelling, for example "Confidential" and "Confidentials" would match, but "Confidentail" would not.
<b>Classifier condition</b>	<b>Number of matches [is greater than 0]</b>
<b>Match action</b>	<b>Set [Spelling.similar] to yes</b>
<b>Non-match action</b>	<b>Set [Spelling.similar] to no</b>

## Identifying files with the word "classified" and not the word "declassified"

Rule name	Tag classified files
Automatic execution	Enable
Filters	Anything
Classifier	Solr Standard Query
Classifier patterns	Match Standard Query ["CLASSIFIED" NOT "DECLASSIFIED"]
Classifier condition	Number of matches [is greater than 0]
Match action	Set [Classified.found] to yes
Non-match action	Set [Classified.found] to no

## Identifying files marked for blocking by ICAP-DLP

In the case of the ICAP-DLP classifier, the pattern is checked by ICAP-DLP, which tags the file if it is sensitive and does not tag it if it is not sensitive. Therefore, if the file is tagged by ICAP-DLP as sensitive, it is a match, and the following rule sets **File.allowed** to **false**, indicating that the file is not allowed to be downloaded, uploaded, or shared.

Rule name	Identifying files flagged by ICAP-DLP
Automatic execution	Enable
Filters	Anything
Classifier	ICAP-DLP
Classifier condition	Number of matches [is greater than 0]
Match action	Set [File.allowed] to false
Non-match action	Set [File.allowed] to true

## Identifying files with the names or addresses (AI Classifier example)

Rule name	Tag files with names or addresses
Automatic execution	Enable
Filters	Anything
Classifier	AI Classifier
Classifier patterns	Match instances of [people names] OR Match instances of [addresses]
Classifier condition	Number of matches [is greater than 0]
Match action	Set [Personal Info.found] to yes
Non-match action	Set [Personal Info.found] to no

## Identifying files with company names (AI Classifier example)

Rule name	Identify files with company names
Automatic execution	Enable
Filters	Anything
Classifier	AI Classifier
Classifier patterns	Match instances of [company names]
Classifier condition	Number of matches [is greater than 0]
Match action	Set [CompanyName.detected] to yes
Non-match action	Set [CompanyName.detected] to no

## Identifying files with contact information (AI Classifier example)

Rule name	Identify files with contact information
Automatic execution	Enable
Filters	Anything
Classifier	AI Classifier
Classifier patterns	Match instances of [phone numbers] OR Match instances of [email addresses]
Classifier condition	Number of matches [is greater than 0]
Match action	Set [ContactInfo.detected] to yes
Non-match action	Set [ContactInfo.detected] to no

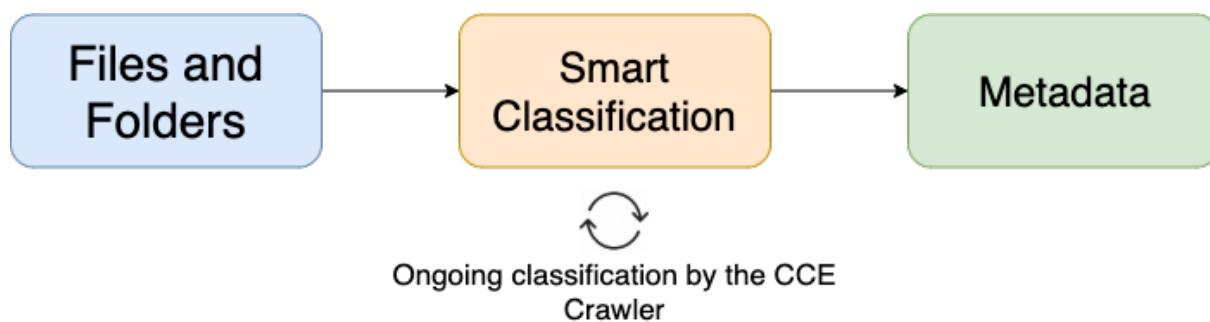
# Smart Classification Classic



Beginning in FileCloud 23.232, an updated version of the Smart Classification user interface is available. Please see [Smart Classification \(see page 103\)](#) to view instructions for the new user interface.

## Overview

The Content Classification Engine (CCE) is a rule-driven content classification system that enables the generic labeling of files with metadata. This labeling enables key operations within FileCloud such as contextual file search and Data Leak Prevention.



CCE automates, streamlines, and strengthens the overall level of data leak prevention for an organization. Administrators and users can upload files and folders with the knowledge that they can be automatically classified according to their content, which helps ensure that sensitive data is immediately covered by the criteria outlined in the DLP plan. CCE rules are also applied retroactively to data that was uploaded before the rules were created, helping organizations protect legacy data.



Smart Classification is only available for files that are 1MB or larger.

Read more about managing metadata.

Read more about Smart DLP ([see page 188](#)).

## Before You Start

CCE will only function properly if Solr has been configured and your storage has been indexed. Additionally, administrators must have created at least one set of metadata in order for the classification process to operate.



### Caution

Understand these Limitations before you begin using CCE or update it

1. Since rules that apply to the same metadata attribute often result in unexpected classification, each rule should have a unique metadata attribute.
2. To prevent overwriting metadata intentionally added by users, CCE does not overwrite metadata it didn't add itself. Users must remove manually added metadata set values to allow CCE to add its own metadata.
3. CCE uses Perl Compatible Regular Expressions (PCRE), which enables it to support a richer set of regular expressions. For example, the character class \d which represents a single number, is now usable.

If you upgrade from a previous version of FileCloud, review your CCE rules and existing patterns to confirm that they still classify as expected.

4. CCE updates classification if a file no longer meets the condition of a rule after it is updated and re-uploaded. For example, if a file with a credit card number that is classified as PII is re-uploaded without the credit card number, the PII classification is removed.
5. Empty files cannot be indexed and classified.
6. The default maximum size for indexed files is 10MB; therefore, by default, files larger than 10MB are not classifiable by CCE and are not available for content search.
7. As of FileCloud Version 20.3, if you have OCR enabled, CCE scans image and PDF files for matching patterns. To enable OCR, see [Enabling Solr OCR](#).

## Create New Metadata Set

## Get Started with CCE

[Creating and Managing Content Classification Engine Rules \(see page 167\)](#)

[CCE Rule Examples \(see page 170\)](#)

[Creating a Pattern \(see page 176\)](#)

[Creating a Pattern Group \(see page 179\)](#)

## CCE Crawler

The CCE Crawler is an automated tool that classifies files and folders after a rule has been enabled. This helps to ensure that all content is classified according to the defined **and** enabled rules regardless of when the upload occurred or will occur.



The CCE crawler **will not run** unless manually enabled or executed by a Cron job.

## Manually Run the Crawler

To manually run the crawler, click the blue button on the row of the rule you would like the crawler to use for classification. The amount of time needed for the completion of the crawl will depend on the number and size of files being classified, as well as the complexity of enabled CCE rules.

Manage Content Classification Rules					
Rules					<a href="#">+ Add rule</a> <span style="margin: 0 10px;">☰ Manage Pattern Group</span>
Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
Confidential Documents	{"Confidential Documents": {"Confidential": "Yes"}}	UNEXECUTED	YES		<span style="color: orange;">→</span> <span style="color: blue;">▶</span> <span style="color: grey;">⚙</span> <span style="color: red;">✖</span>



You may manually execute a rule that is not enabled (**Auto-classification Enabled** is **FALSE**). After you click the arrow, your screen displays the message *This rule is disabled but it can classify files when manually executed. Proceed to execute the rule? Click OK to execute the rule.*



If you edit a currently executing rule and click **Save**, rule execution is aborted and **Status** is set to **Unexecuted**.

## More Information:

- [Classify Documents in FileCloud using Smart Classification](#)<sup>87</sup>

## Creating and Managing Content Classification Engine Rules

### Keyword Definitions

Below are the keywords used in creating the rule definition:

---

87. <https://www.filecloud.com/blog/2021/06/classify-documents-in-filecloud-using-smart-classification/#.YMzZK2hKhIA>

Classifier	<p>Classifier used to classify the file content.</p> <p><i>Note: Classification is not case sensitive.</i></p> <p>In most cases, you can use:</p> <ul style="list-style-type: none"> <li>• <b>Default</b> - Classify content into terms that match the supplied regex patterns.</li> </ul> <p>Supported parameters: SEARCH_PATTERN_SET, SEARCH_PATTERN_NAME or SEARCH_PATTERN_GROUP</p> <p>Result Schema (_classifications): [{term: "term that matched a regex", count: "number of times the term appears in the doc"}, ...]</p> <p>Also supported are:</p> <ul style="list-style-type: none"> <li>• <b>PatternMatch</b> - Classify content into regex patterns found.</li> </ul> <p>Supported parameters: SEARCH_PATTERN_SET, SEARCH_PATTERN_NAME or SEARCH_PATTERN_GROUP</p> <p>Result Schema (_classifications): ["regex pattern", ...]</p> <ul style="list-style-type: none"> <li>• <b>StandardQuery</b> - Classify content as matching the query or not.</li> </ul> <p>Supported parameters: STANDARD_QUERY_EXPRESSION</p> <p>Result Schema (_classifications): ["expression"] or []</p> <ul style="list-style-type: none"> <li>• <b>ICAPDLP</b> - Classify content based on results returned from ICAP DLP.</li> </ul> <p>Supported parameters: none</p> <p>Result Schema (_classifications): []</p> <ul style="list-style-type: none"> <li>• <b>SingaporeNRIC</b> - Classify content into terms that match a Singapore NRIC.</li> </ul> <p>Supported parameters: none</p> <p>Result Schema (_classifications): [{term: "NRIC term", count: "number of times the NRIC term appears in the doc"}, ...]</p>
Pre-condition	Rules that must be met by a file before the file is evaluated through the classifier.
Condition	Criteria to take a match action or default action on the files. Currently it must be count(_classifications) > 0 that indicates the file contains the search pattern, or the file must have applied metadata based on the presence of unique numbers or values.
Parameters	Regular Expression search criteria. Regular Expressions can be specified using SEARCH_PATTERN_SET, SEARCH_PATTERN_NAME or SEARCH_PATTERN_GROUP.
SEARCH_PATTERN_SET	Any Valid Regular Expressions e.g. /[0-9]{9}/

SEARCH_PATTERN_NAME	Regular Expression assigned a name through Manage Pattern Group - Available Patterns
SEARCH_PATTERN_GROUP	Regular Expressions grouped through Manage Pattern Group - Pattern Group.
Match Action	Actions taken when the classifier finds a file based on precondition, condition and parameters. For example, assign metadata set PII and metadata attribute Confidential to 1.
Default Action	Actions taken when the classifier finds a file based on precondition but did not meet the condition based on parameters. For example, assign metadata set PII and metadata attribute Confidential to 0.

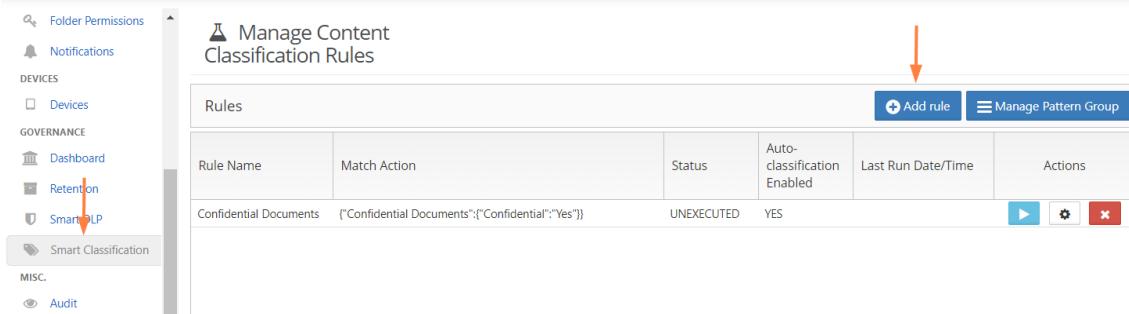
## Creating and Editing CCE Rules



A CCE Rule is a **self-contained specification** for classifying **one or more files**.

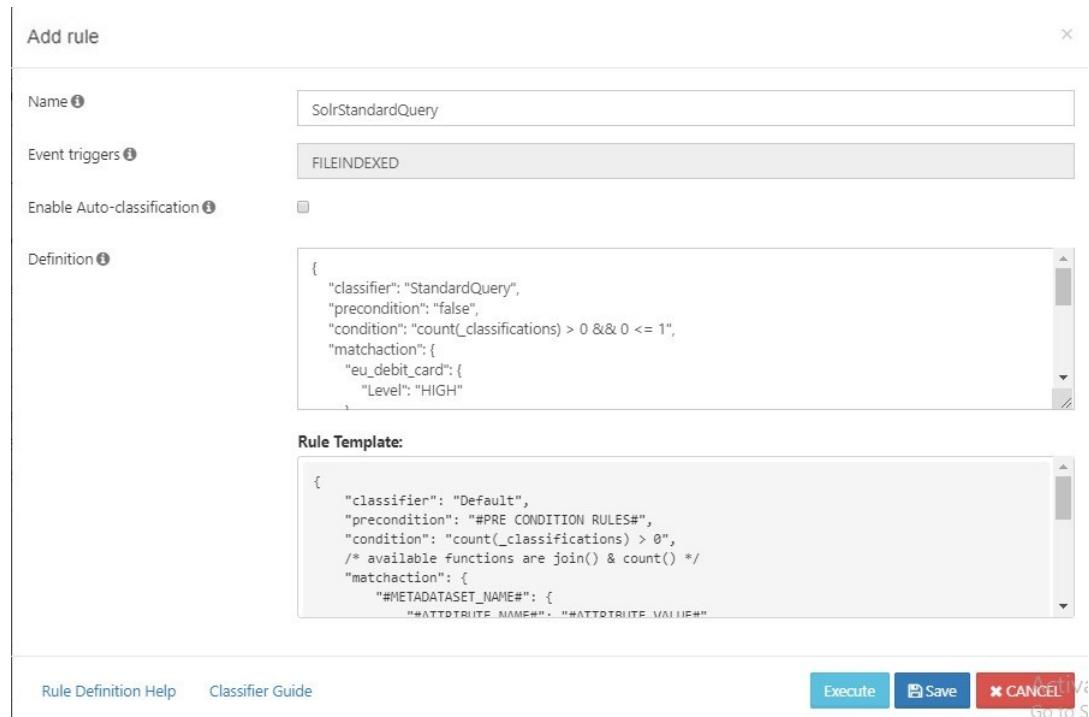
### To create a CCE rule:

1. To open the **Manage Content Classification Rules** page, in the Admin portal's navigation pane, click **Smart Classification**.
2. To add or create a new rule, click **Add Rule**.



3. In the **Add Rule** dialog box, fill in the fields:

- **Name:** Naming detail for the rule to be created.
- **Event Triggers:** Criteria that enables the CCE to automatically execute rules for certain events.
- **Enable Auto-classification:** When enabled, the rule defined will start classifying files based on the definition.
- **Definition:** Set of rules which defines the action to be taken.



#### 4. Click **Save**.

See [Example Rules](#) (see page 170).



If you want the rule to immediately begin auto-classifying files when you save it, be sure to check the **Enable Auto-classification** box.

## CCE Rule Examples



**Note:** Allowed paths defined for a metadata do not prevent CCE classification from applying that metadata.

### How to identify files based on size containing U.S Social Security Numbers

Criteria:

- Files under 5MB
- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW"

Pre-Requisite:

- Have Metadata set PII defined with Level attribute

- Have Pattern defined with the name "US Social Security Number"

```
{
  "classifier": "Default",
  "precondition": "_file.size < 5000000",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Level": "HIGH"
    }
  },
  "defaultaction": {
    "PII": {
      "Level": "LOW"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_NAMES": [
      "US Social Security Number"
    ]
  }
}
```

## How to identify files based on extensions and containing US Social Security Numbers

Criteria:

- Apply to files with extensions .txt & .pdf
- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW"

Pre-Requisite:

- Have Metadata set PII defined with Level attribute
- Have RegExp pattern for US Social Security Numbers

```
{
  "classifier": "Default",
  "precondition": "_file.ext in ['txt', 'pdf']",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Level": "HIGH"
    }
  },
}
```

```

"defaultaction": {
  "PII": {
    "Level": "LOW"
  }
},
"parameters": {
  "SEARCH_PATTERN_SET": [
    "/[0-9]{9}/"
  ]
}
}

```

## How to identify files containing US Social Security Numbers

Criteria:

- Apply to all files
- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW"

Pre-Requisite:

- Have Metadata set PII defined with Level attribute
- Have Pattern defined with the name "US Social Security Numbers"

```

{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Level": "HIGH"
    }
  },
  "defaultaction": {
    "PII": {
      "Level": "LOW"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_NAMES": [
      "US Social Security Number"
    ]
  }
}

```

```

    }
}
```

## How to identify files containing one of the patterns in the pattern group

Criteria:

- Apply to all files
- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW"

Pre-Requisite:

- Have Metadata set PII defined with Level attribute
- Have Pattern Group - GDPR defined

```

{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "GDPR": {
      "Level": "HIGH"
    }
  },
  "defaultaction": {
    "GDPR": {
      "Level": "LOW"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_GROUPS": [
      "GDPR"
    ]
  }
}
```

## How to identify files containing US Social Security Numbers inside the user folder `/my.user/PII/`

Criteria:

- Apply to all files inside `/my.user/PII/`

- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW"

Pre-Requisite:

- Have Metadata set PII defined with Level attribute
- Have Pattern defined with the name "US Social Security Number"

```
{  
  
  "classifier": "Default",  
  
  "precondition": "starts_with(_file.fullPath, '/my.user/PII/')",  
  
  "condition": "count(_classifications) > 0",  
  
  "matchaction": {  
  
    "PII": {  
  
      "Level": "HIGH"  
  
    }  
  
  },  
  
  "defaultaction": {  
  
    "PII": {  
  
      "Level": "LOW"  
  
    }  
  
  },  
  
  "parameters": {  
  
    "SEARCH_PATTERN_NAMES": [  
  
  ]
```

```

    "US Social Security Number"

]
}


```

## How to identify files containing white spaces within words or sentences

Criteria:

- Apply to text and pdf files
- Set Metadata PII.Level = "HIGH" if there is a pattern match or as PII.Level = "LOW" otherwise

Pre-Requisite:

1. Have Metadata set PII defined with Level attribute.

```

{
  "classifier": "Default",
  "precondition": "_file.ext in ['txt', 'pdf']",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Level": "HIGH"
    }
  },
  "defaultaction": {
    "PII": {
      "Level": "LOW"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_SET": [
      "\/[0-9]{4} [0-9]{4} [0-9]{4} [0-9]{4}\/"
    ]
  }
}

```

## How to identify files containing Singapore National Registry Identity Card (NRIC)

Criteria:

- Apply to all files

- Set metadata NRIC.Confidentiality Level = "HIGH" if there is a pattern match or NRIC.Confidentiality Level = "LOW"

Pre-Requisite:

- Have metadata set NRIC defined with Confidentiality Level attribute

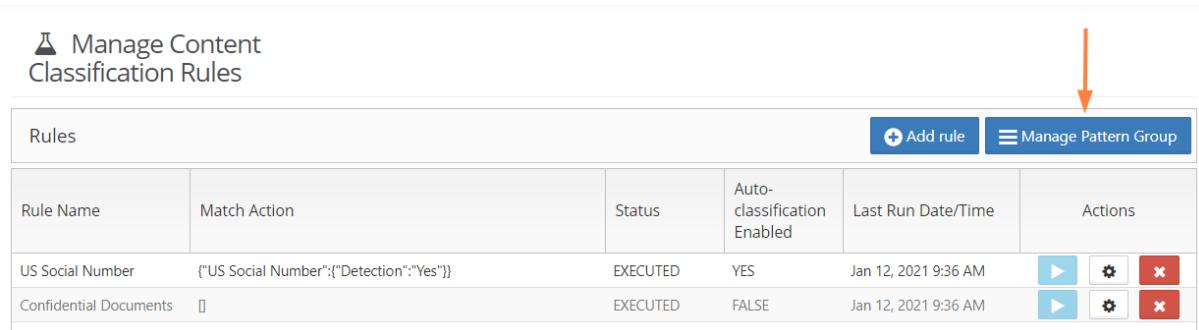
```
{
  "classifier": "SingaporeNRIC",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "NRIC": {
      "Confidentiality Level": "HIGH"
    }
  },
  "defaultaction": {
    "NRIC": {
      "Confidentiality Level": "LOW"
    }
  },
  "parameters": []
}
```

## Creating a Pattern

Patterns are named sets of regular expressions that allow administrators to easily label and identify commonly used or important regexes.

## Creating and Modifying a Pattern

### 1. Click on 'Manage Pattern Group'



The screenshot shows the 'Manage Content Classification Rules' interface. At the top, there is a title bar with the text 'Manage Content Classification Rules'. Below the title bar, there is a blue button labeled 'Manage Pattern Group'. A red arrow points to this button. The main area of the interface is a table titled 'Rules'. The table has columns for 'Rule Name', 'Match Action', 'Status', 'Auto-classification Enabled', 'Last Run Date/Time', and 'Actions'. There are two rows in the table. The first row is for 'US Social Number' with the match action '{"US Social Number":{"Detection":"Yes"}}', status 'EXECUTED', auto-classification 'YES', last run date 'Jan 12, 2021 9:36 AM', and actions buttons. The second row is for 'Confidential Documents' with the match action '[]', status 'EXECUTED', auto-classification 'FALSE', last run date 'Jan 12, 2021 9:36 AM', and actions buttons.

Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
US Social Number	{ "US Social Number": { "Detection": "Yes" } }	EXECUTED	YES	Jan 12, 2021 9:36 AM	 
Confidential Documents	[]	EXECUTED	FALSE	Jan 12, 2021 9:36 AM	 

### 2. To create a new Pattern, click on Add New Pattern.

## Manage Pattern Groups : GDPR



Pattern Group

GDPR

New Pattern Group

Available Patterns
Belgium National Number
Croatia Identity Card Number
Croatia Personal Identification (OIB) Number
Denmark Personal Identification Number
EU Debit Card Number
Finland National ID
Finland Passport Number
France Driver's License Number
France National ID Card (CNI)
France Passport Number

 Page  of 2 20 rows

Member Patterns
Belgium National Number
Denmark Personal Identification Number

 Page  of 1 2 rows

Add New Pattern

Delete

Close

3. Click on +Add button and enter the pattern details in the modal that pops up.



New Pattern



Manage PII Patterns		Add	
Name	Regex	Actions	
Belgium National Number	[0-9]{2}.[0-9]{2}.[0-9]{2}-[0-9]{3}.[0-9]{2}		
Croatia Identity Card Number	[0-9]{9}		
Croatia Personal Identification (OIB) Number	[0-9]{10}		
Denmark Personal Identification Number	[0-9]{6}-[0-9]{4}		
EU Debit Card Number	[0-9]{16}		
Finland National ID	[0-9]{6}[-+a][0-9]{3}[0-9a-zA-Z]{1}		
Finland Passport Number	[a-zA-Z]{2}[0-9]{7}		
France Driver's License Number	[0-9]{12}		
France National ID Card (CNI)	[0-9]{12}		
France Passport Number	[0-9]{2}[a-zA-Z]{2}[0-9]{5}		

Page 1 of 2 20 rows

New PII Search Pattern

Name	<input type="text" value="Enter Pattern Name"/>
Regex	<input type="text" value="Enter Pattern Regex"/>
<input type="button" value="Create"/> <input type="button" value="CANCEL"/>	

4. Once you have created your pattern, you should now be able to use it in a Content Classification rule or group it together with other patterns in a Pattern Group.

## Creating a Pattern Group

Pattern groups allow administrators and users to save information identification patterns in order to streamline the classification process.

### Creating and Modifying a Pattern Group

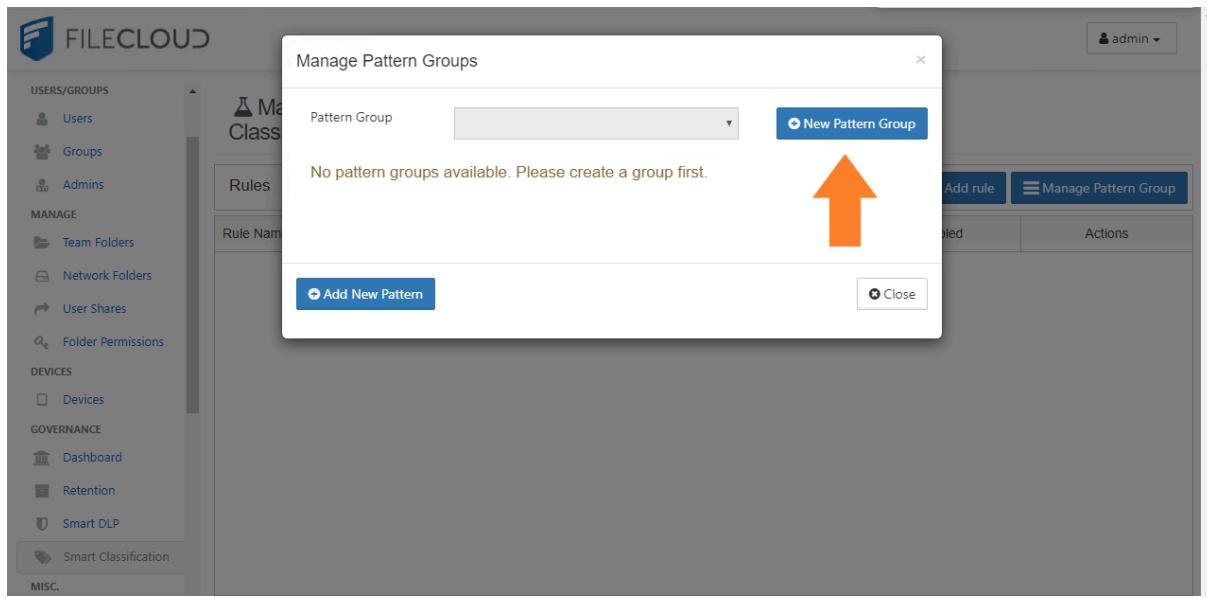
1. Click on 'Manage Pattern Group'

Manage Content Classification Rules



Rules						<input type="button" value="Add rule"/>	<input type="button" value="Manage Pattern Group"/>
Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions		
US Social Number	{"US Social Number":{"Detection":"Yes"}}	EXECUTED	YES	Jan 12, 2021 9:36 AM			
Confidential Documents	[]	EXECUTED	FALSE	Jan 12, 2021 9:36 AM			

2. To add or create a new rule Pattern Group, click on New Pattern Group.



3. Click on New Pattern Group, enter a Group Name and click Save.



4. Once you have created your group, you can add Available Patterns by selecting them from the left-side panel and moving them with the middle arrows to the Members Patterns on the right. Once completed, click Close.

In the below example, we have created the Pattern Group **GDPR** that includes patterns such as Belgian National Numbers and Denmark Personal Identification Numbers.

Manage Pattern Groups : GDPR

Pattern Group GDPR + New Pattern Group

**Available Patterns**

- Belgium National Number
- Croatia Identity Card Number
- Croatia Personal Identification (OIB) Number
- Denmark Personal Identification Number
- EU Debit Card Number
- Finland National ID
- Finland Passport Number
- France Driver's License Number
- France National ID Card (CNI)
- France Passport Number

Page 1 of 2 ◀ ▶ ◀ ▶  
20 rows

**Member Patterns**

- Belgium National Number
- Denmark Personal Identification Number

Page 1 of 1 ◀ ▶ ◀ ▶  
2 rows

+ Add New Pattern Delete ✖ Close

**Step 5.** Once saved, you can add your new group to a Content Classification Rule.

## More CCE Rule Examples

Generally, CCE can be used for a number of classification purposes such as:

- Identification of files containing certain patterns of textual content e.g. credit card numbers, employee numbers, and social security numbers
- Identification of files containing exact phrases
- Classification of files into different tiers of security, privacy, etc.
- Setting default values for custom metadata or Color Tagging metadata
- Classification of files based on word proximity

- Classification of files based on word similarity
- Classification of files based on a boolean combination of SOLR queries

## Identifying text patterns.

E.g. identifying files with Amex credit card numbers:

```
{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Credit Card": "Amex"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_SET": [
      "3[47]{1}[0-9]{13}",
      "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}",
      "3[47]{1}[0-9]{2} [0-9]{4} [0-9]{4} [0-9]{3}"
    ]
  }
}
```

## Identifying exact phrases.

E.g. identifying files containing confidentiality phrases

```
{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Confidentiality": "CONFIDENTIAL"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_SET": [
      "CONFIDENTIAL - FOR CODELATHE PERSONNEL ONLY"
    ]
  }
}
```

## Classification into tiers:

### (1) Classifying files into different tiers of security using pattern occurrence

```

/* Tier 1 */
{
    "classifier": "Default",
    "precondition": "true",
    "condition": "count(_classifications) < 5 && count(_classifications) > 0",
    "matchaction": {
        "PII": {
            "Security": "MONITOR"
        }
    },
    "defaultaction": [],
    "parameters": {
        "SEARCH_PATTERN_SET": [
            "3[47]{1}[0-9]{13}",
            "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}"
        ]
    }
}

/* Tier 2 */
{
    "classifier": "Default",
    "precondition": "true",
    "condition": "count(_classifications) >= 5",
    "matchaction": {
        "PII": {
            "Security": "RESTRICT"
        }
    },
    "parameters": {
        "SEARCH_PATTERN_SET": [
            "3[47]{1}[0-9]{13}",
            "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}"
        ]
    }
}

```

### (2) Classifying files into different tiers of security using pattern match

```

/* Tier 1 */
{
    "classifier": "PatternMatch",
    "precondition": "true",
    "condition": "count(_classifications) == 1",
    "matchaction": {

```

```

        "PII": {
            "Security 2": "MONITOR"
        }
    },
    "defaultaction": [],
    "parameters": {
        "SEARCH_PATTERN_SET": [
            "3[47]{1}[0-9]{13}",
            "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}"
        ]
    }
}

/* Tier 2 */
{
    "classifier": "PatternMatch",
    "precondition": "true",
    "condition": "count(_classifications) == 2",
    "matchaction": {
        "PII": {
            "Security 2": "RESTRICT"
        }
    },
    "parameters": {
        "SEARCH_PATTERN_SET": [
            "3[47]{1}[0-9]{13}",
            "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}"
        ]
    }
}
}

```

## Setting default metadata.

CCE can set custom metadata parameters values for files. Beginning in FileCloud 21.1, CCE can also set color tag metadata values for files.

Ensure file has been classified

```

{
    "classifier": "Default",
    "precondition": "true",
    "condition": "count(_classifications) == 0",
    "matchaction": {
        "PII": {
            "Status": "Classified"
        }
    },
    "parameters": {
        "SEARCH_PATTERN_SET": [
            "3[47]{1}[0-9]{13}",
            "3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}"
        ]
    }
}

```

```

        ]
    }
}
```

## Classifying files based on word proximity (phrase similarity)

```
{
  "classifier": "StandardQuery",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Confidentiality %": 99.9
    }
  },
  "defaultaction": [],
  "parameters": {
    "STANDARD_QUERY_EXPRESSION": "\"CONFIDENTIAL - FOR CODELATHE PERSONNEL
ONLY\"~2"
  }
}
```

## Classifying files based on word similarity

```
{
  "classifier": "StandardQuery",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Confidentiality 2 %": 99.9
    }
  },
  "defaultaction": [],
  "parameters": {
    "STANDARD_QUERY_EXPRESSION": "CONFIDENTIAL~1"
  }
}
```

## Classifying files based on a boolean combination of SOLR queries

```
{
  "classifier": "StandardQuery",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "PII": {
      "Confidentiality 3 %": 99.9
    }
  },
  "defaultaction": [],
  "parameters": {
    "STANDARD_QUERY_EXPRESSION": "\"CONFIDENTIAL\" NOT \"NOT CONFIDENTIAL\""
  }
}
```

## Using ICAP DLP with CCE

If you have integrated ICAP DLP with FileCloud, you can create a content classification rule that flags files, thereby enabling DLP to prevent downloading or sharing of those files.

### To set up your system to use ICAP DLP with CCE:

1. In [ePolicy Orchestrator](#)<sup>88</sup>, add rules for flagging files to block from downloads or shares. For example if file contains 10 or more bank account numbers, flag it for blocking (since it may be a data leak).
2. Add custom metadata that can be set to true or false depending on whether or not McAfee authorizes the file. For example add the metadata parameter **dlp-allowed** with possible values of **true** and **false**.
3. Set up a [FileCloud CCE rule](#) (see page 167) that uses the classifier **ICapDLP**. The CCE rule is applied each time a file is uploaded. It sets **dlp-allowed** to **true** or **false** depending on whether or not McAfee authorizes it.
  - a. To go to the **Manage Content Classification Rules** screen, in the Admin portal navigation panel, click **Smart Classification**.
  - b. Click **Add rule**. The **Add rule** dialog box opens.
  - c. In **Name**, enter a name for the rule.
  - d. In **Event triggers**, enter **ADDFILE,UPDATEFILE**.
  - e. In **Definition**, enter a rule similar to:

```
{
```

88. <https://docs.trellix.com/bundle/epolicy-orchestrator-landing>

```

"classifier": "IcapDLP",
"precondition": "true",
"condition": "count(_classifications) > 0",
"matchaction": {
    "DLP allowed": {
        "dlp-allowed": "false"
    }
},
"defaultaction": {
    "DLP allowed": {
        "dlp-allowed": "true"
    }
},
"parameters": []
}

```

Add rule

Name 	ICAP DLP
Event triggers 	ADDFILE,UPDATEFILE
Enable Auto-classification 	<input checked="" type="checkbox"/>
Definition 	<pre> {     "classifier": "IcapDLP",     "precondition": "true",     "condition": "count(_classifications) &gt; 0",     "matchaction": {         "DLP allowed": {             "dlp-allowed": "false"         }     } } </pre>
Rule Template:	<pre> "#METADATASET_NAME": {     "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#" }, "parameters": {     "SEARCH_PATTERN_SET": "[#"REGULARE EXPRESSION#, "#REGULARE EXPRESSION#"]",     "SEARCH_PATTERN_NAMES": "[#"PATTERN NAME#", "#PATTERN NAME#"]",     "SEARCH_PATTERN_GROUPS": "[#"PATTERN GROUP#"" </pre>

Rule Definition Help  Classifier Guide 

 Save  Cancel

#### f. Click Save.

 Manage Content Classification Rules

Rules						 Add rule 
Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions	
Confidential Documents	{"Confidential Documents": {"Confidential": "Yes"}}	EXECUTED	YES	May 6, 2021 1:10 PM	  	
ICAP DLP	{"DLP allowed": {"dlp-allowed": "false"}}	UNEXECUTED	YES		  	

Now, in FileCloud [Smart DLP](#) (see page 188), add rules that prevent download or sharing for files with the **dlp-allowed** metadata parameter set to false.

# Smart DLP



Data leak prevention (DLP) features are only available in some versions of FileCloud Online.



DLP crawlers run on all daily cron jobs and remove shares that violate any SHARE ENFORCE rules.

## Overview

Due to increasing privacy requirements, it is important for organizations to be able to monitor neglectful or malicious activity that can result in the loss of confidential data. The data leak or loss can occur at end points due to user actions, during transit, or while at rest. Data at rest leak prevention relies on encryption technologies and physical security of media, whereas endpoint leak prevention refers to the ability to prevent data leak from an application's end point (e.g. the recipient of a data transfer).

Data leak prevention (DLP) is a FileCloud feature that enables administrators to closely control the degree to which users can access, edit, download, and transfer their organization's files and folders. While DLP can be useful for many different kinds of data, it can be especially critical for the secure handling of Personal Identification Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI). DLP also offers greater security to organizations that are required to operate in compliance with HIPAA or GDPR.

Smart Classification (see page 103) works in conjunction with DLP to streamline, automate, and strengthen data security.

### In this section

- [Creating Data Leak Prevention Rules \(see page 188\)](#)
- [Example Rules \(see page 198\)](#)
- [Rule Expressions \(see page 206\)](#)
- [How to secure documents with Smart DLP & CCE \(see page 213\)](#)
- [Troubleshooting DLP \(see page 227\)](#)

## Creating Data Leak Prevention Rules



Only administrators with DLP privileges are able to create, modify, and delete DLP rules.



DLP DOWNLOAD rules may affect file preview functionality, which requires the previewed file to be downloaded to the browser or client application.

To create and edit DLP rules, follow the steps below:

1. Access FileCloud's Admin portal > Governance > Smart DLP

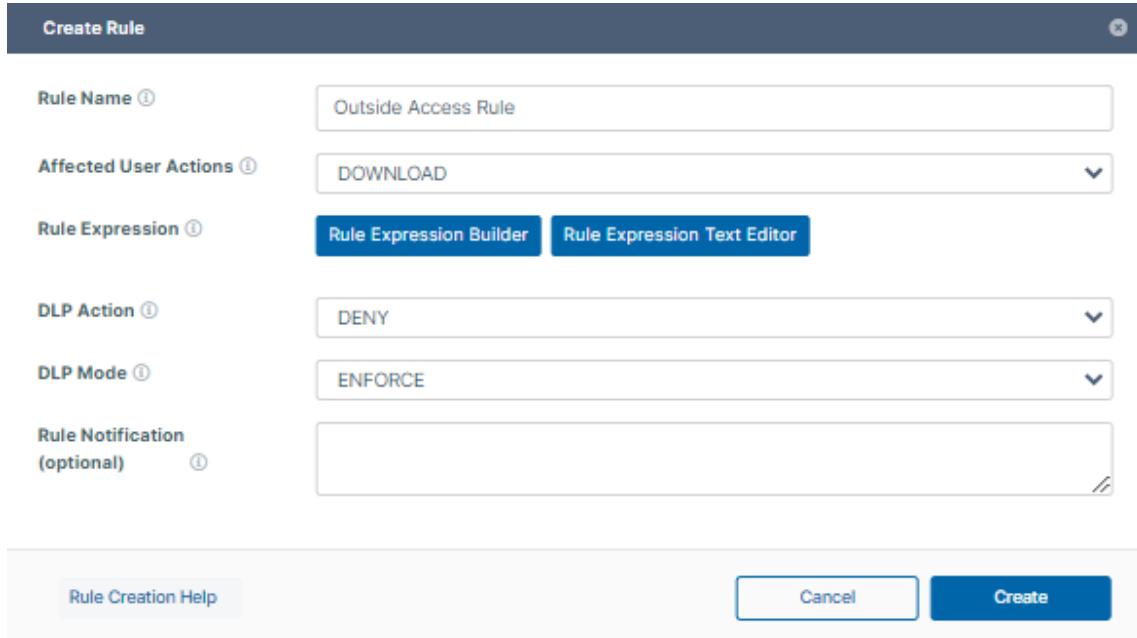


The screenshot shows the FileCloud Admin portal interface. The left sidebar has a tree structure with categories like HOME, USERS / GROUPS, MANAGE, DEVICES, and GOVERNANCE. Under GOVERNANCE, the 'Smart DLP' link is highlighted with a red arrow. The main content area is titled 'Smart DLP' and shows a table of existing rules. The table columns are: Rule Name, WHEN (Affected User Action), IF (Rule Expression), THEN (DLP Action), MODE, Recent Violations, Active, and Actions. The rules listed are:

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	<code>\$_user.inGroup('Company XYZ') and _request.remoteip in ['43.12.45.78'] or \$_user.inGroup('Internal')</code>	DENY	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>
Confidential Documents	SHARE	<code>\$_metadata.existsWithValue('Confidential Documents.Confidential', 'Yes') and _share.onlyUsersFromDomain('codelalthe.com') or \$_metadata.existsWithValue('Confidential Documents.Confidential', 'No')</code>	ALLOW	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>
US Social Number	SHARE	<code>\$_metadata.existsWithValue('US Social Number.Detection', 'Yes') and _share.onlyUsersFromDomain('codelalthe.com') or \$_metadata.existsWithValue('US Social Number.Detection', 'No')</code>	ALLOW	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>
Public Sharing Allowed	SHARE	<code>\$_share.hasUsersFromDomain('gmail.com')</code>	DENY	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>
Private Sharing Only	SHARE	<code>\$_metadata.existsWithValue('cce.pdf')</code>	DENY	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>
Login US only	LOGIN	<code>\$_request.remoteCountryCode == 'US'</code>	DENY	ENFORCE	0	<input type="checkbox"/>	<span>⚠️</span> <span>🔗</span> <span> ⓘ</span>

2. To create a new rule, click **Add DLP Rule**.

The **Create Rule** dialog box opens:



The 'Create Rule' dialog box is open. The fields are:

- Rule Name:** Outside Access Rule
- Affected User Actions:** DOWNLOAD
- Rule Expression:** Rule Expression Builder (selected)
- DLP Action:** DENY
- DLP Mode:** ENFORCE
- Rule Notification (optional):** (empty text area)

At the bottom are 'Rule Creation Help', 'Cancel', and 'Create' buttons.

3. Fill in the fields.

- **Rule Name:** A name that identifies the DLP rule.

- **Affected User Actions:** User actions that trigger the DLP rule (DOWNLOAD, SHARE, or LOGIN).
- **Rule Expression:** Criteria for triggering the DLP rule. A minimum of one expression is required in order to create a DLP rule.  
You can either use the **Rule Expression Builder** to help you construct a rule expression or type it in manually using the **Rule Expression Text Editor**.  
For help using the **Rule Expression Builder**, see [Create a rule with the rule expression builder](#), below.  
See a list of [Rule Expressions \(see page 206\)](#).
- **DLP Action:** Allow or Deny the user action if the parameters of the rule expression are triggered.
- **DLP Mode:** If a rule is violated, whether or not the action will be prevented. Regardless of the mode, the system creates an audit log.  
Options are:
  - **Enforce** - (Default) The action will be prevented.
  - **Permissive** - The action will not be prevented.
- **Rule Notification:** Message displayed to users when a rule is violated. Does not apply to log-in rules.  
The following HTML tags are supported: <a>, <br>, and <p>. Only full urls (those beginning with <http://> or <https://>) can be rendered.

#### 4. Click **Create**.

The rule appears in the **DLP Rules** table.

Manage DLP Rules								<a href="#">+ Add DLP Rule</a>
Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions	
Outside Access Rule	DOWNLOAD	<code>file.path == '/myuser/mydir/myfile.pdf'</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>		

## Create a rule with the rule expression builder

The Rule Expression Builder helps you ensure that your rules have the right parameters and correct formatting. The first example demonstrates how to use the expression builder to create a simple single-condition rule. The second example shows how to create a more complex rule that contains several conditions.

### To create a rule with a simple condition

This rule blocks downloading of files with metadata indicating that they contain personal identification information (PII).

1. Go to the DLP page and click **Add DLP**.
2. In the **Create Rule** dialog box, enter a **Rule Name**, and choose **DOWNLOAD** in **Affected User Actions**.
3. Click **Rule Expression Builder**.

Rule Name ⓘ

Affected User Actions ⓘ

Rule Expression ⓘ

DLP Action ⓘ

DLP Mode ⓘ

Rule Notification (optional) ⓘ

Rule Creation Help

The **Rule Expression Builder** opens.

4. Click **ADD**.

Rule Expression Builder

+ ADD

You are given two choices: **New Rule** and **New Rule Group**.

5. Since this is a simple rule, choose **New Rule**.
- Fields for creating a rule appear.
6. The top field shows options based on the **Affected User Action**. Since the **Affected User Action** is **DOWNLOAD**, the options are **Request**, **File**, **Metadata**, and **User**.

Rule Expression Builder

Request

ip equals True  False

43.12.45.78

Example: 43.12.45.78 (i)

Cancel Save

+ ADD

Cancel Update

7. Choose **Metadata**.
8. In the next field, choose **exists**, and in the last field, choose the metadata set and the parameter that indicates that the file contains PII.  
For this example, the metadata set is **cce** and the parameter is **pii**.

Rule Expression Builder

Metadata

exists True  False

cce.pii

Example: cce.pii (i)

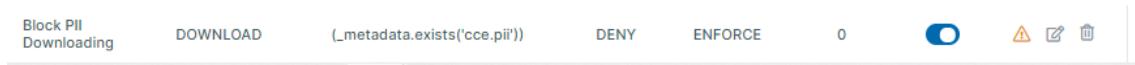
Cancel Save

+ ADD

Cancel Update

9. Click **Save**, and then click **Update**.
10. In the **Rule Update** dialog box, choose a **DLP Action**, **DLP Mode**, and optionally enter a **Rule Notification**, and click **Create**.

The rule appears in the **Smart DLP** list.



### To create a rule with multiple conditions

This rule blocks downloading of a file either:

- Sent from a user in the group **User**  
OR
- Sent from a user in the group **Manager** and sent from the Server address **1.1.1.1**.

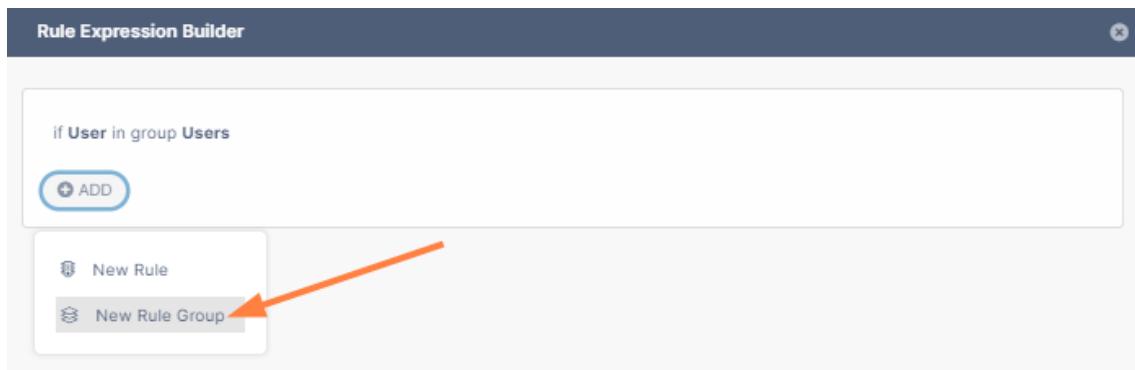
1. Go to the DLP page and click **Add DLP**.
2. In the **Rule Update** dialog box, enter a **Rule Name**, and choose **DOWNLOAD** in **Affected User Actions**.
3. Click **Rule Expression Builder**.
4. Click **Add**.

You are given two choices: **New Rule** and **New Rule Group**.

5. To add the condition that only checks if the user is in the **User** group, choose **New Rule**.
6. Fill the fields with **User, in group**, and **Users**.



7. Click **Save**.



8. Click **ADD** again.

9. Since you are adding a two-condition rule, click **New Rule Group**.

Clicking **New Rule Group** will enclose the conditions that follow in parentheses and embed it one level.

You may embed up to four levels of rule groups.

10. Choose the indented **ADD** directly under **AND**.

Make sure you click the correct **ADD** link.

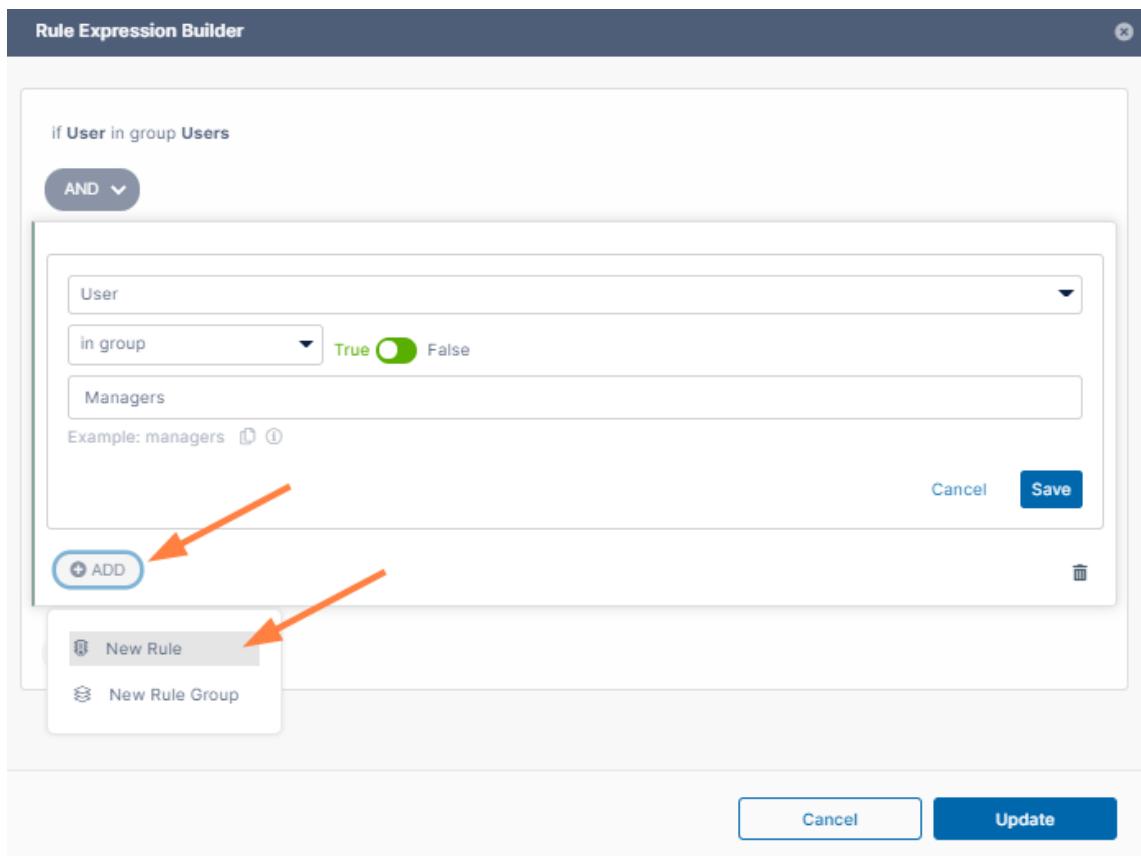


11. Click **New Rule**.



12. Fill in the fields with **User**, **in group**, and **Managers**.

13. Click **ADD** directly under the fields for this condition, and choose **New Rule**.



14. Enter the fields **Request, ip equals**, and **1.1.1.1**.
15. Click **Save** for each of the conditions.

Rule Expression Builder

if User in group Users

AND

User  
in group True False

Managers  
Example: managers

Cancel Save

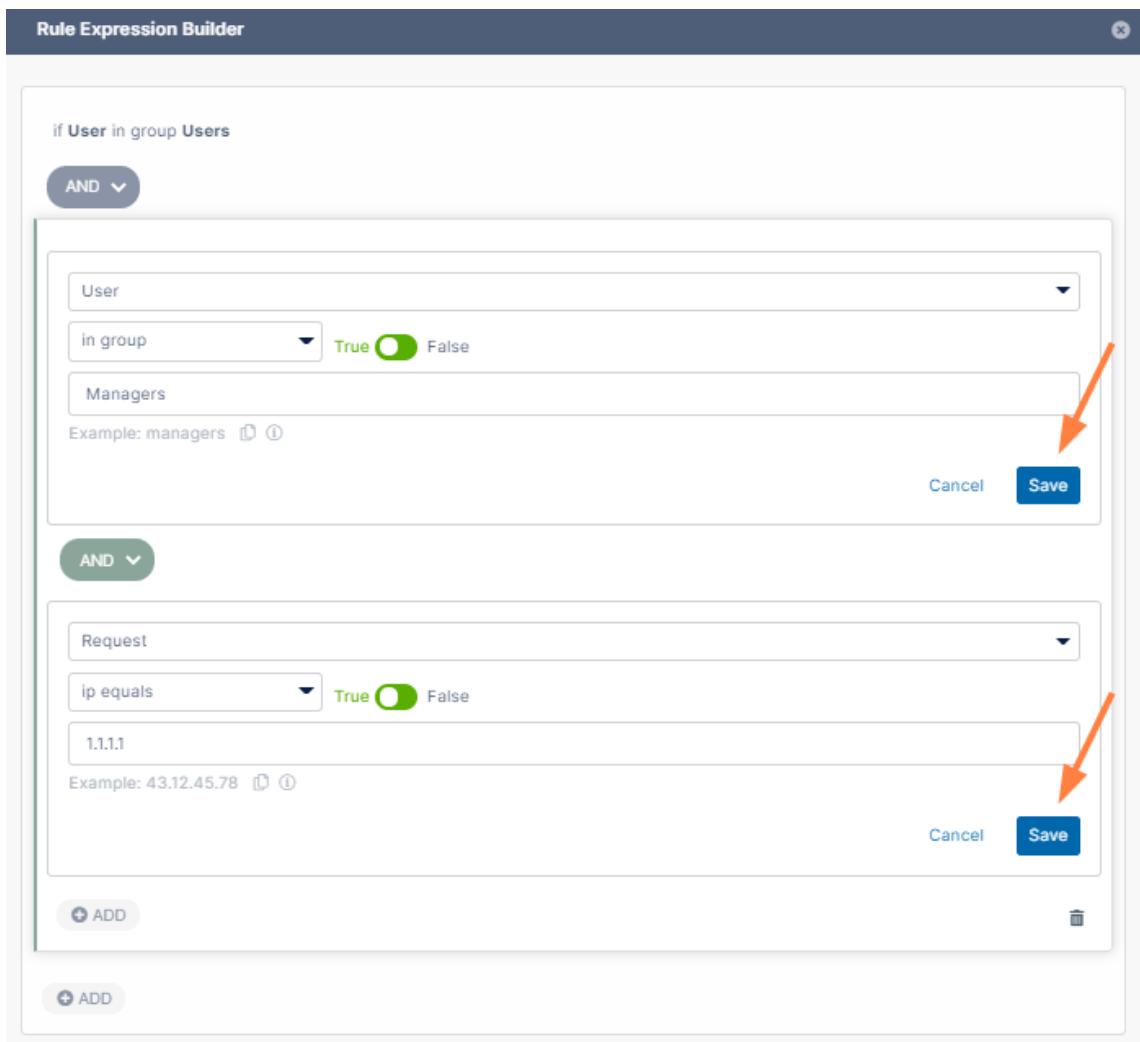
AND

Request  
ip equals True False

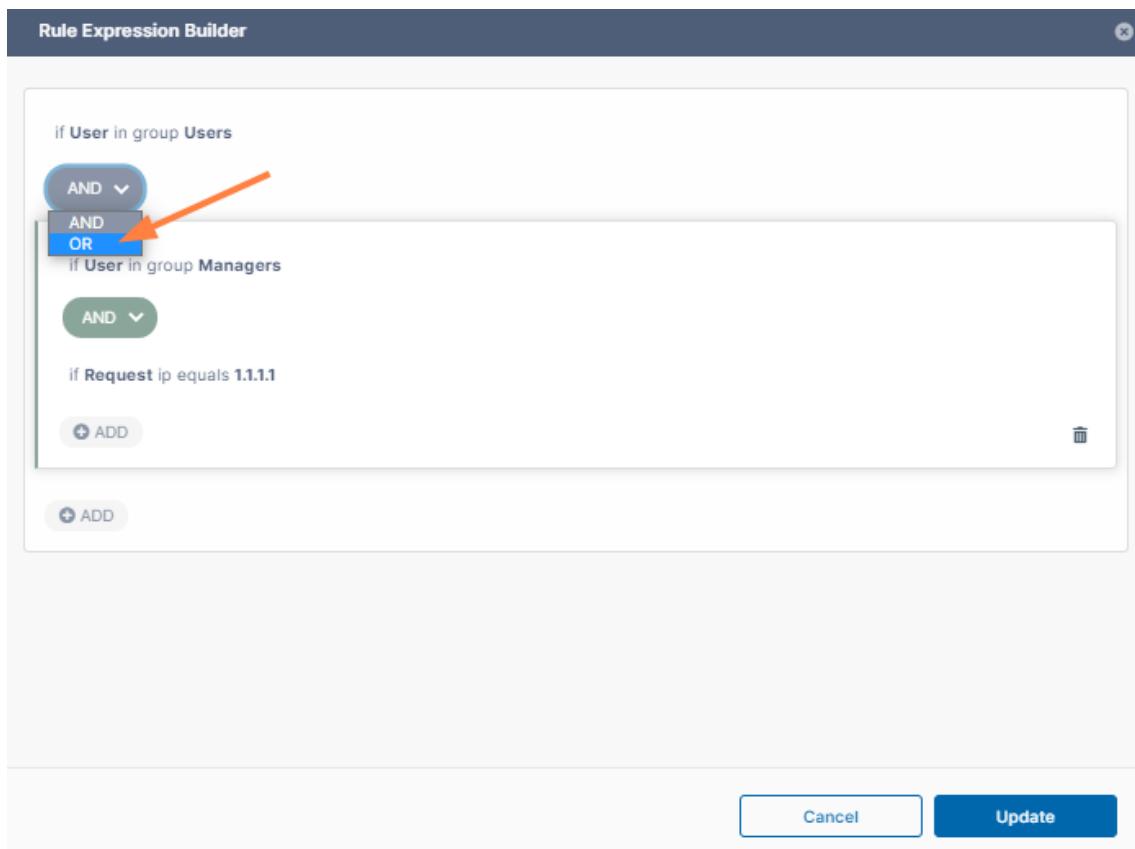
1.1.1.1  
Example: 43.12.45.78

Cancel Save

ADD ADD



16. The rule expression is saved.
17. Since the expression is checking if one condition OR the other condition exists, change the top **AND** to **OR**.



18. Click **Update**.
19. Make sure your **Rule Expression** is correct, then fill in values for **DLP Action**, **DLP Mode**, and **Rule Notification**, and click **Create**.

The rule appears in the **Smart DLP** list.

Download by internal managers only	DOWNLOAD	<code>_user.inGroup('Users')    (_user.inGroup('Managers') &amp;&amp; _request.remoteip == '1.1.1.1')</code>	DENY	ENFORCE	0				
------------------------------------	----------	--	------	---------	---	--	--	--	--

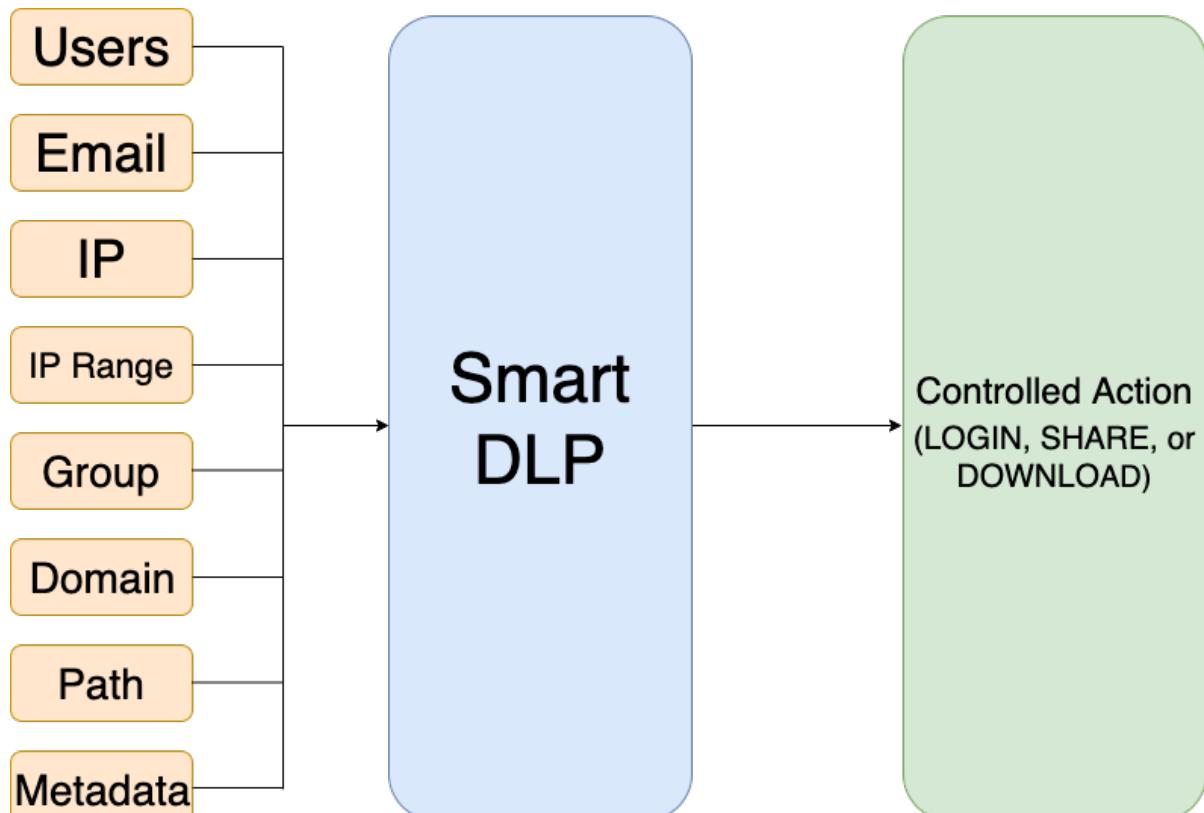


If the Rule Expression is not valid, an error will be thrown.



DLP crawlers run on all daily cron jobs and remove shares that violate any SHARE ENFORCE rules.

## Example Rules



### Multiple DLP Actions

Each affected user action requires its own individual DLP rule. For instance, if an admin wanted to use the same Rule Expressions to control both DOWNLOAD and SHARE, two rules using the same Rule Expressions would be required.



DLP crawlers run on all daily cron jobs and remove shares that violate any SHARE ENFORCE rules.

Read how to create your own [DLP rules](#) (see page 188)

Learn more about DLP [Rule Expressions](#) (see page 206)

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control download of files	DO WN LOA D	<ul style="list-style-type: none"> <li>• <code>_file.path</code></li> <li>• <code>_file.pathStartsWith</code></li> <li>• <code>_file.ext</code></li> <li>• <code>_file.pathContains</code></li> <li>• <code>_file.pathMatches</code></li> <li>• <code>_file.fileNameContains</code></li> </ul>	<pre> _file.path == '/myuser/mydir/myfile.pdf'  OR  _file.pathStartsWith('/myuser/mydir')  OR  _file.ext == 'pdf'  OR  _file.pathContains('/myuser/mydir')  OR  _file.pathMatches('/myuser/mydir')  OR  _file.fileNameContains('mrn') </pre>	DENY	Users cannot download files from the path expressed in the rule or with the extension or term in the filename.

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control download and shares of files based on metadata	DOWNLOAD SHARE	<ul style="list-style-type: none"> <li>• <code>_metadata.exists('metadataValue')</code></li> <li>• <code>_metadata.existsAll('metadataValue')</code></li> <li>• <code>_metadata.existsWithValue(metadataValue, value)</code></li> <li>• <code>_metadata.existsWithValueInArray(metadataValue, value)</code></li> <li>• <code>_metadata.existsWithCondition(metadataValue, operator, value)</code></li> </ul> <p><b>Note:</b> The metadata set and the attribute specified cannot contain periods within their names. For example, <code>cce.pii</code> is valid, but <code>cce.x.pii.y</code> is not valid.</p>	<pre> _metadata.exists('cce.pii')  OR  _metadata.existsAll('cce.pii')  OR  _metadata.existsWithValue('content.category', 'confidential')  OR  _metadata.existsWithValueInArray('content.categories', 'pii')  OR  _metadata.existsWithCondition('content.Risk_Level', '&gt;', 6) </pre>	ALLOW	Users can download and share files with associated metadata.

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control login/ access and download of files based on IP/ Device/ IP Range/ country code	DO WN LOA D LOG IN	<ul style="list-style-type: none"> <li>• <code>_request.remoteIp</code></li> <li>• <code>_request.agent</code></li> <li>• <code>_request.inIpv4Range(lowIp, highIp)</code></li> <li>• <code>_request.remoteCountryCode</code> <b>Note:</b> To use this expression, the <b>Show Geo IP Chart</b> setting in the <b>Settings &gt; Admin</b> screen must be set to <b>TRUE</b>.</li> <li>• <code>_request.inIpv4CidrRange(cidrRange)</code></li> </ul>	<pre> _request.remoteIp == '43.12.45.78'  OR  _request.agent == 'Unknown'  OR  _request.inIpv4Range('138.204.26.1', '138.204.26.254')  OR  _request.remoteCountryCode == 'US'  OR  _request.inIpv4CidrRange('10.2.0.0/16') </pre>	DENY	Users from the given IP, agent, IP range, country code, or CIDR ip range will not be permitted to login or download.
	LOG IN	<ul style="list-style-type: none"> <li>• <code>_request.isAdminLogin</code></li> </ul>	<code>_request.isAdminLogin</code>	DENY	If the

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control login/ access, download and sharing of files based on user attributes	DO WN LOA D LOG IN SH ARE	<ul style="list-style-type: none"> <li>• <code>_user.username</code></li> <li>• <code>_user.email</code></li> <li>• <code>_user.userType</code></li> <li>• <code>!_user.inGroup</code></li> <li>• <code>_user.isMasterAdmin</code></li> </ul>	<pre> _user.username == 'FileCloudUser1' OR  _user.email == 'john.Doe@mail.com'  OR  user.userType == 'Guest Access'  OR  !_user.inGroup('managers')  OR  _user.isMasterAdmin  DLP Action:  ALLOW/DENY </pre>	ALLOW	Users with the given username, email address, user type, any user <b>not</b> in the group 'managers', and the master Admin will be permitted to login, as well as download and sharing files.

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control file sharing	DO WN LOA D SH ARE	<ul style="list-style-type: none"> <li>• <code>_share.path</code></li> <li>• <code>_share.public</code></li> <li>• <code>_share.onlyAllowedEmails</code></li> <li>• <code>_share.allowedUsers</code></li> <li>• <code>_share.allowedGroups</code></li> <li>• <code>_share.hasUsersFromDomain(domain)</code></li> <li>• <code>_share.onlyUsersFromDomain(domain)</code></li> <li>• <code>_share.pathStartsWith(start)</code></li> <li>• <code>_share.pathContains(text)</code></li> <li>• <code>_share.pathMatches(pattern)</code></li> </ul> <p><b>Note:</b> In any of the expressions including <code>share.path</code>, specify the original path of the shared file (for example <code>/user1/textfile1.txt</code>), not the path in the Shared with Me folder (for example, <code>/SHARED/user1/textfile1.txt</code>)</p> <p><b>Note:</b> <code>share.pathMatches(pattern)</code> supports the wildcards:</p> <ul style="list-style-type: none"> <li>`*` - any sequence of characters</li> <li>`#` - a single character</li> </ul>	<p>Rule Expression:</p> <pre><code>_share.public</code></pre> <p>OR</p> <pre><code>_share.onlyAllowedEmails</code></pre> <p>OR</p> <pre><code>_share.allowedUsers</code></pre> <p>OR</p> <pre><code>_share.allowedGroups</code></pre> <p>OR</p> <pre><code>_share.hasUsersFromDomain('gmail.com')</code></pre> <p>OR</p> <pre><code>_share.onlyUsersFromDomain('mycompany.com')</code></pre> <p>OR</p> <pre><code>_share.pathStartsWith('/myuser/mydir')</code></pre> <p>OR</p> <pre><code>_share.pathContains('sometext')</code></pre> <p>OR</p> <pre><code>_share.pathMatches('*sometext*')</code></pre>	ALLOW	Select users select groups, and users coming from a particular domain can access a specified or matching path.

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
Control file download and login combinations	DO WN LOA D LOG IN	<ul style="list-style-type: none"> <li>!_user.inGroup</li> <li>_metadata.existsWithValue</li> <li>_request.remoteIp</li> <li>_request.isAdminLogin</li> <li>!</li> <li>_request.inIpV4CidrRange</li> </ul>	<p>Rule Expression:</p> <pre>!_user.inGroup('superadmin') and _metadata.existsWithValue('PII Confidentiality Level', 'HIGH')</pre> <p>OR</p> <pre>_user.inGroup('external') or _request.remoteIp in ['45.45.45.1', '45.45.45.2', '45.45.45.7']</pre> <p>OR</p> <pre>_request.isAdminLogin &amp;&amp; ! _request.inIpV4CidrRange('10.2.0.0/16')</pre> <p>DLP Action:</p> <p>ALLOW/DENY</p>	<p>DENY</p> <p>Users in (or not in) the given groups or IP ranges will not be able to download files or access paths with the given metadata (in this case, a HIGH value for the attribute 'PII Confidentiality Level')</p> <p>OR</p> <p>Users logging into the admin portal in the given IP</p>	

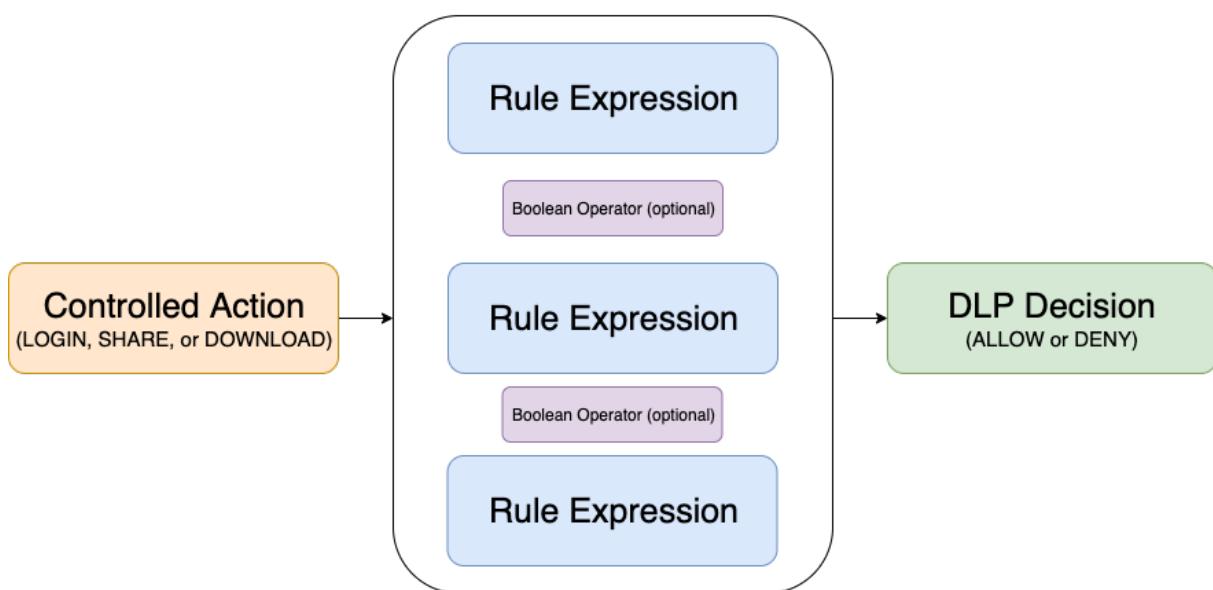
Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
					range will not be able to download files or log in.
Control sharing based on domain of user doing the sharing	SHARE	<ul style="list-style-type: none"> <li>• <code>_user.isEmailInDomain(domainToCheck)</code></li> </ul>	<p>Rule Expression:</p> <pre><code>_user.isEmailInDomain('example.com', 'mail.com')</code></pre>	ALLOW	Users with one of the specified email domains are permitted to share files.

## Rule Expressions

### Simple Rule



### Complex Rule



Rule Expressions are the parameters by which DLP policies determine a user or group's ability to login into the FileCloud system, as well as to download or share files. Rule Expressions also enable administrators to access detailed information about user activity on their FileCloud installations.



#### Logical operators

DLP permits users to implement two or more rules using the logical operators '&&', '||', and '!'.

[UNKNOWN ATTACHMENT](#) Learn more about [logical operators](#).

## DLP Rule Expressions

Expression	What does the expression do?	Sample returned value	Applicable actions
_request.remotelp	Returns the IP address that was used to execute the action.	_request.remotelp == '43.12.45.78'	DOW NLOAD, LOGIN
_request.isAdminLogin	Returns true for admin login request.	_request.isAdminLogin	LOGIN
_request.agent	Returns the user agent that was used to execute the action. The possible values are: 'Cloud Drive', 'Cloud Sync', 'Unknown', 'Web browser', 'Android', 'iOS', 'MS Outlook' and 'MS Office'.	_request.agent == 'Unknown'	DOW NLOAD, LOGIN
_request.inIpv4Range(lowIp, highIp)	Checks if the IP address that was used to execute the action is part of a given IP range, represented by limits of the range (given with the parameters).	_request.inIpv4Range('138.204.26.254', '138.204.26.1')	DOW NLOAD, LOGIN
_request.remoteCountryCode	<p>Returns the two-character uppercase ISO country code. Returns "Unknown" if country could not be determined.</p> <p><b>Note:</b> To use this expression, the <b>Show Geo IP Chart</b> setting in the <b>Settings &gt; Admin</b> screen must be set to <b>TRUE</b>.</p>	_request.remoteCountryCode == 'US'	DOW NLOAD, LOGIN
_request.inIpV4CidrRange(cidrRange)	Checks if the IP address used to execute the action matches the given CIDR range.	_request.inIpV4CidrRange('10.2.0.0/16')	DOW NLOAD, LOGIN
_user.username	<p>Returns the name of the user trying to execute an action.</p> <p><b>Note:</b> This cannot be used to identify the master Admin since "admin" is not stored as a user. Instead use <b>user.isMasterAdmin</b> (see below).</p>	_user.username == 'FileCloudUser'	DOW NLOAD, LOGIN, SHARE

Expression	What does the expression do?	Sample returned value	Applicable actions
_user.email	Returns the email of the user trying to execute an action.	_user.email == 'john.doe@mail.com' <sup>89</sup>	DOW NLOA D, LOGI N, SHAR E
_user.userType	<p>Returns the type of user that is trying to execute the action. The available types are: 'Full Access', 'Limited Access', 'Guest Access'.</p> <p><b>Note:</b> Prior to FileCloud 22.1, the three user types were <b>Full</b>, <b>Limited</b>, and <b>Guest</b>. Beginning in FileCloud 22.1 <b>Limited</b> users are referred to as <b>External</b> users; however, the DLP rule expression still requires the use of the value 'Limited Access' to refer to these users.</p>	_user.userType == 'Guest Access'	DOW NLOA D, LOGI N, SHAR E
_user.inGroup(groupName)	Checks if a user is part of a given group.	!_user.inGroup('managers')	DOW NLOA D, LOGI N, SHAR E
user.isEmailInDomain(domainsToCheck)	Checks if a user's email id matches a given list of domains. The 'domainsToCheck' parameter can be a single domain, or a comma-separated domains list.	_user.isEmailInDomain('example.com' <sup>90</sup> , 'mail.com' <sup>91</sup> )	SHAR E
user.isMasterAdmin	<p>Checks if user is the master Admin.</p> <p><b>Note:</b> _user.username == 'admin' cannot be used in place of this to identify the master Admin since "admin" is not stored as a user.</p>	user.isMasterAdmin	DOW NLOA D, LOGI N, SHAR E

89. <http://mail.com>90. <http://example.com>91. <http://mail.com>

Expression	What does the expression do?	Sample returned value	Applicable actions
_file.path	Returns the path that was accessed.	_file.path == '/myuser/mydir/myfile.pdf'	DOW NLOAD
_file.pathStartsWith(start)	Returns true when the path has been accessed. Starts with the given `start` parameter.	_file.pathStartsWith('/myuser/mydir')	DOW NLOAD
_file.ext	Checks if the file has the extension specified.	_file.ext == 'pdf'	DOW NLOAD
_file.pathContains(path)	Checks if the file path contains the sub-path specified.	_file.pathContains('/myuser/mydir')	DOW NLOAD
_file.pathMatches(path)	Checks if the file path matches the path specified.	_file.pathMatches('/myuser/mydir')	DOW NLOAD
_file.fileNameContains(text)	Checks if the filename includes the given text.	_file.fileNameContains('mr n')	DOW NLOAD

**Note:** When you set a \_metadata rule, the metadata set and the attribute specified cannot contain periods within their names. For example, cce.pii is valid, but cce.x.pii.y is not valid.

_metadata.exists(metadataValue)	Checks if the path or one of its children, have the given metadata attribute set. The metadata attribute must be provided using the `metadataSet.attribute` notation.	_metadata.exists('cce.pii')	DOW NLOAD, SHARE
_metadata.existsAll(metadataValue)	Checks if the path or all of its children, have the given metadata attribute set. The metadata attribute must be provided using the `metadataSet.attribute` notation.	_metadata.existsAll('cce.pi i')	DOW NLOAD, SHARE

Expression	What does the expression do?	Sample returned value	Applicable actions
_metadata.existsWithValue(metadataValue, value)	This function is similar to the <code>_metadata.exists(metadataValue)</code> function, but it checks if the metadata attribute (first parameter) exists, and if its value is equal to a given value (second parameter).	<code>_metadata.existsWithValue('content.category', 'confidential')</code>	DOW NLOA D, SHAR E
_metadata.existsWithValueInArray(metadataValue, value)	This function is similar to the <code>_metadata.existsWithValue(metadataValue, value)</code> function, but checks whether an array metadata attribute contains the specified value.	<code>_metadata.existsWithValueInArray('content.categories', 'pii')</code>	DOW NLOA D, SHAR E
_metadata.existsWithValueCondition(metadataValue, operator, value)	This function is similar to the <code>_metadata.existsWithValue(metadataValue, value)</code> function, but it takes an operator parameter (second parameter) that will be used to compare the metadata attribute value (first parameter) with the provided value (third parameter). The available operators are: `==` (equals), `!=` or `<>` (not equal), `>` (greater than), `<` (less than), `>=` and `<=`. When the metadata and the third operator are numbers, they'll be compared as numbers. If any parameter is not a number, it will be compared alphabetically (dates, for example, cannot be compared using `>`, `<`, `>=`, `<=`). The sample checks if the risk level of a document is greater than 6.	<code>_metadata.existsWithValueCondition('content.Risk Level', '&gt;', 6)</code>	DOW NLOA D, SHAR E
<p><b>Note:</b> In any of the expressions including <code>share.path</code>, specify the original path of the shared file (for example <code>/user1/textfile1.txt</code>), not the path in the Shared with Me folder (for example, <code>/SHARED/user1/textfile1.txt</code>)</p>			
_share.path	Returns the path of the share.	<code>_share.path == '/myuser/mydir/myfile.pdf'</code>	SHAR E
_share.public	Returns true or false if the share is public or not.	<code>_share.public</code>	SHAR E

Expression	What does the expression do?	Sample returned value	Applicable actions
_share.onlyAllowedEmails	Checks if all users receiving a share match one of the emails or one of the domains specified in the rule. A domain may be specified instead of an email by using *, for example *@gmail.com. If any recipients do not match an email or domain specified, the share is denied.	'true' if all share recipients are in a domain or email in the onlyAllowedEmails list. 'false' if any share recipient is not in any of the domains or emails in the onlyAllowedEmails list.	SHARE
_share.allowedUsers	Returns a list of the allowed users of the share (including the users in an allowed group). The list contains the users' email addresses.	'john.snow@mail.com <sup>92</sup> ' in _share.allowedUsers	SHARE
_share.allowedGroups	Returns a list of the allowed groups of the share.	'EVERYONE' in _share.allowedGroups	SHARE
_share.hasUsersFromDomain(domain)	Checks if the allowed users list has any users with an email domain that <b>matches</b> the given domain. In the provided sample, the expression will return true if any user with a gmail domain is included as an allowed user (directly or through a group). This method only makes sense with DENY rules.	_share.hasUsersFromDomain('gmail.com <sup>93</sup> ')	SHARE

92. <http://mail.com>93. <http://gmail.com>

Expression	What does the expression do?	Sample returned value	Applicable actions
_share.onlyUsersFromDomain(domain)	<p>Similar to the <code>_share.hasUsersFromDomain(domain)</code> function, but checks if the allowed users list has any user with an email domain that <b>doesn't match</b> the given domain. In the provided sample, the expression only returns true if all users have their emails in the <code>'mycompany.com'</code><sup>94</sup> domain. This method only makes sense with ALLOW rules.</p>	<code>_share.onlyUsersFromDomain('mycompany.com')</code> <sup>95</sup>	SHARE
	<p><b>⚠</b> Do not use this expression in an OR condition with another expression; this could cause shares to be denied unintentionally. Instead use <code>_share.onlyAllowedEmails</code> with a wildcard.</p> <p>For example, instead of:</p> <pre data-bbox="620 1185 922 1298">(_share.onlyUsersFromDomain('gmail.com')    _share.onlyAllowedEmails('testuser@test.com'))</pre> <p>use:</p> <pre data-bbox="620 1394 922 1484">_share.onlyAllowedEmails('*@gmail.com','testuser@test.com')</pre>		
_share.pathStartsWith(start)	Returns true when the shared path starts with the given `start` parameter.	<code>_share.pathStartsWith('/myuser/mydir')</code>	SHARE
_share.pathContains(text)	Returns true when the shared path contains the given `text` parameter.	<code>_share.pathContains('someText')</code>	SHARE

94. <http://mycompany.com>95. <http://mycompany.com>

Expression	What does the expression do?	Sample returned value	Applicable actions
<code>_share.pathMatches(pattern)</code>	Returns true when the shared path matches the given `pattern` parameter. Wildcards are supported: `*` for any sequence of characters and `#` for a single character.	<code>_share.pathMatches('*someText*')</code>	SHARE

## Logical Operators

DLP allows users to implement logical operators to further refine and specify their data leak prevention rules.

### Logical Operator Examples

Applicable Action	DLP Ruling	Rule Expressions	Result
DOWNLOAD	DENY	<code>_user.username == 'john' &amp;&amp; _user.inGroup('engineers')</code>	User 'john' in group 'engineers' will not be permitted to download any files.
DOWNLOAD	ALLOW	<code>_user.inGroup('accounting')    _request.remoteip == '69.89.31.226.'</code>	Users in group 'accounting' <b>or</b> users from the listed IP will be permitted to download files, but <b>no other users</b> will be permitted.
SHARE	DENY	<code>!_user.inGroup('designers')</code>	Users who are <b>not</b> a member of group 'designers' will not be permitted to share files.

## How to secure documents with Smart DLP & CCE

- [Allow downloading files from authorized partners only \(see page 214\)](#)
- [\(23.253\) Detect confidential documents with PII and allow internal shares only](#)
- [Detect documents with US Social Security Number and allow sharing only with specific domains \(see page 216\)](#)
- [Limit Web Login to a specific group of users \(see page 224\)](#)

## Allow downloading files from authorized partners only

### Overview:

The purpose of this example is to create a Smart DLP rule that allows downloading of files from authorized partners of your company initiated from a specific public IP address or a list of public IP addresses.

In the example, a FileCloud group is named after the partner company, "Company XYZ", and contains users from this company.

Another FileCloud group named "Internal" contains all the internal users from your company.

### Configuration Steps:

#### 1. Create Smart DLP Rule

- Open the FileCloud Admin portal, and in the navigation panel, click **Smart DLP**.
- Add a new DLP rule.
- Configure the rule to allow downloads from users in the group "Company XYZ" when requests are initiated from a specific IP or multiple specific IPs. In the second image below, multiple specific IPs would appear as `_request.remotelp in ['IP1', 'IP2', 'IP3']`
- In the image below, `(_user.inGroup('Internal'))` allows downloads from users in group "Internal" initiated from any IP.

The screenshot shows the 'Manage DLP Rules' page. The left sidebar has a 'Smart DLP' button highlighted with a red circle and an arrow pointing to it with the text 'Go to smart DLP'. The top right corner has an 'Add DLP rule' button highlighted with a red circle and an arrow pointing to it with the text 'Add DLP rule'.

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violation	Active	Actions
US Social Security Number	DOWNLOAD	<code>_metadata.existsWithValue('US Social Security Number.Detection', 'Yes')</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>

**Create Rule**

Rule Name <i>(i)</i>	Authorized Partners
Affected User Actions <i>(i)</i>	DOWNLOAD
Rule Expression <i>(i)</i>	<a href="#">Rule Expression Builder</a> <a href="#">Rule Expression Text Editor</a> <div style="border: 2px solid orange; padding: 5px; margin-top: 10px;"> <code>(_user.inGroup('Company XYZ') &amp;&amp; _request.remoteip == '43.12.45.78'    _user.inGroup('Internal'))</code> </div>
DLP Action <i>(i)</i>	DENY
DLP Mode <i>(i)</i>	ENFORCE
Rule Notification (optional) <i>(i)</i>	
<a href="#">Rule Creation Help</a> <span style="border: 1px solid #ccc; padding: 2px 10px; margin: 0 10px;">Cancel</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px;">Create</span>	

## 2. Test Smart DLP rule

- As a user in the "Internal" group, log in to the FileCloud user portal.
- Share a file with a user from the group "Company XYZ".
- Log in to the user portal as a user from the group "Company XYZ" from a public IP that is allowed by the DLP rule. Confirm that the file downloads successfully.
- Log in to the user portal as a user from the group "Company XYZ" from a public IP that is not allowed by the DLP rule. Confirm that file download is forbidden.

The screenshot shows the FileCloud user portal interface. At the top, there is a search bar and a user profile for 'Gaby'. Below the header, the user is navigating to the 'jenniferp' folder. Inside the folder, there is a single item named 'User Info.txt'. The file's download icon is highlighted with a blue box and a cursor, indicating an attempt to download the file. A prominent orange error message box appears, stating: 'Error Download forbidden by DLP rule 'Authorized Partners''. To the right of the file list, there is a sidebar with a user icon and the text 'No activities found'.

## Detect documents with US Social Security Number and allow sharing only with specific domains

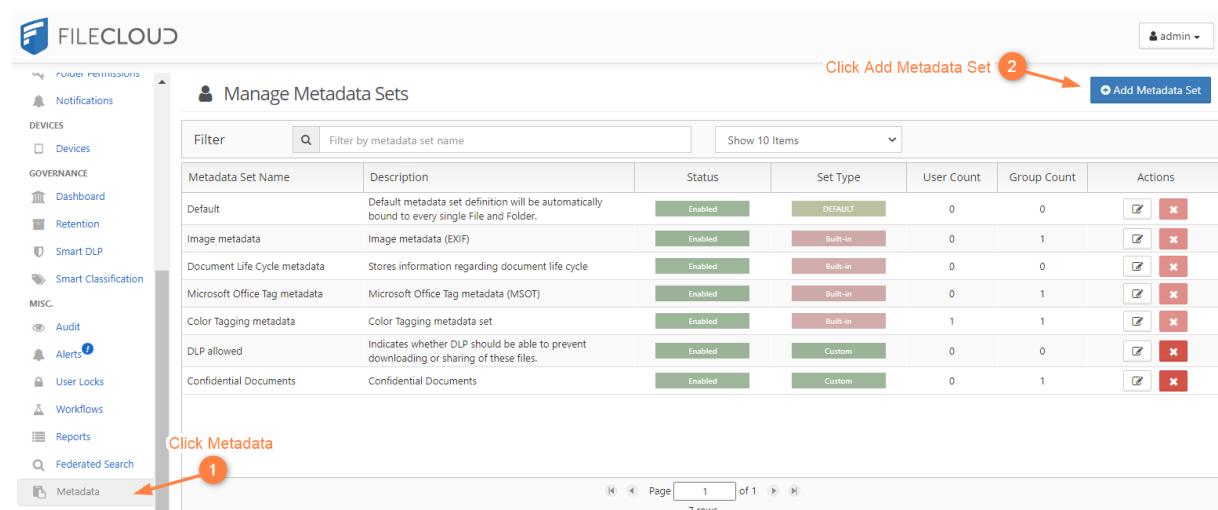
### Overview:

The purpose of this example is to create a classification rule that detects and tags documents with US Social Security Numbers, and then create a DLP rule to prevent sharing the tagged documents with email addresses other than those using your company domain. For documents that do not contain US Social Security Numbers, sharing is allowed with all domains.

### Configuration Steps:

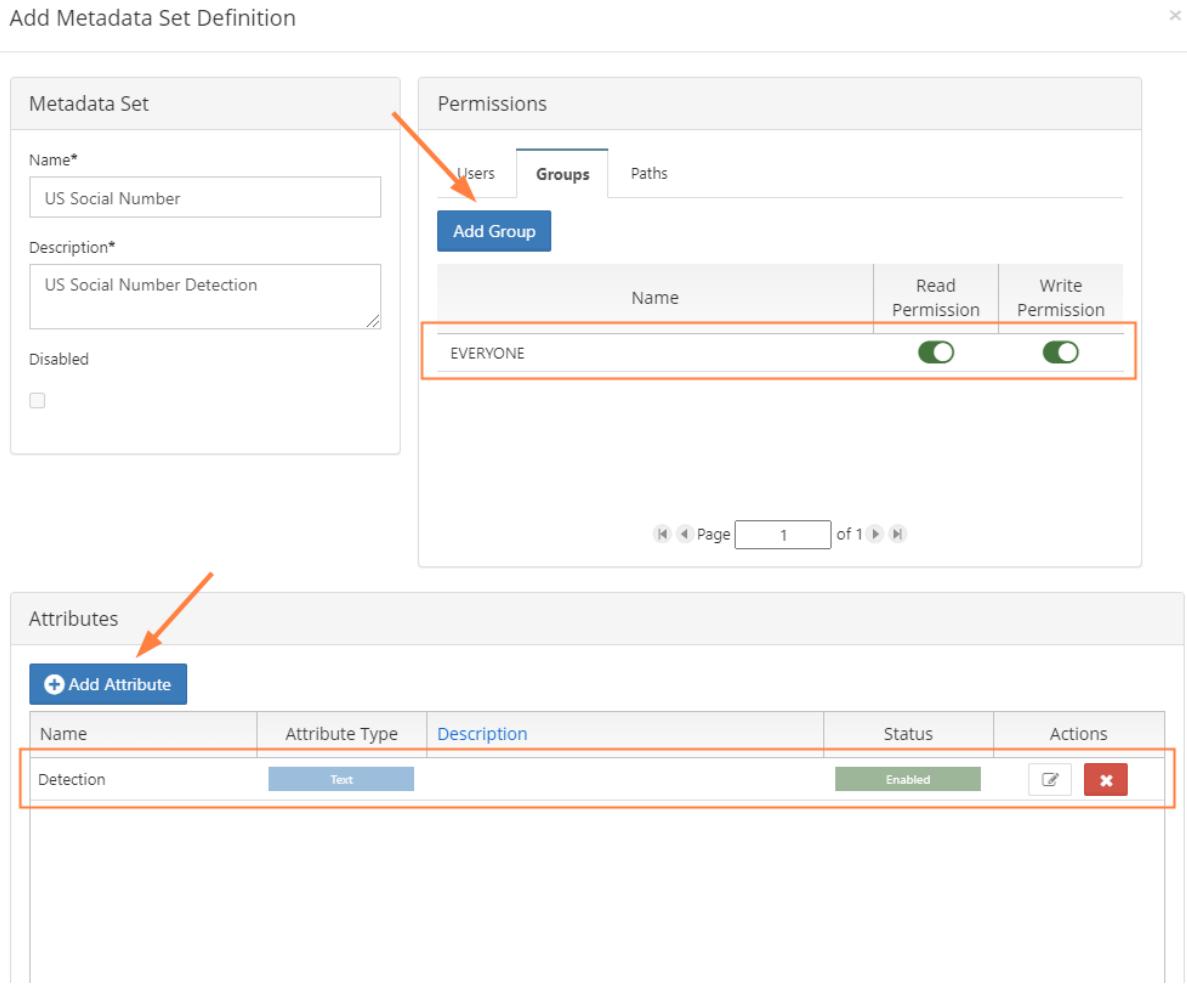
#### 1. Create Metadata Set

- In the navigation pane, click **Metadata**, then click **Add Metadata Set**.



Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	0	0	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	1	1	
DLP allowed	Indicates whether DLP should be able to prevent downloading or sharing of these files.	Enabled	Custom	0	0	
Confidential Documents	Confidential Documents	Enabled	Custom	0	1	

- Create a metadata set with the attribute **Detection** of type text.
- Choose the Users/Groups that can see this metadata and provide read permission.



The screenshot shows the 'Add Metadata Set Definition' dialog. On the left, the 'Metadata Set' section is visible with fields for 'Name\*' (US Social Number) and 'Description\*' (US Social Number Detection). The 'Disabled' checkbox is checked. On the right, the 'Permissions' section is shown with the 'Groups' tab selected. An orange arrow points to the 'Add Group' button. A table shows a single row for 'EVERYONE' with both 'Read Permission' and 'Write Permission' checkboxes checked. Below the table, a page navigation bar shows '1 of 1'. At the bottom left, the 'Attributes' section is visible with an 'Add Attribute' button. An orange arrow points to the 'Add Attribute' button. A table shows a single row for 'Detection' with 'Attribute Type' set to 'Text', 'Status' set to 'Enabled', and 'Actions' showing edit and delete icons. The entire 'Attributes' section is also highlighted with an orange border.

## 2. Create US Social Number regex pattern

- In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the Settings navigation page, click **Content Search** . The **Content Search** page opens.
- Locate the **Enable PII Search** setting at the bottom of the page and enable it:

## Content Search

Reset Solr configuration

[Reset](#)

Content search status

Solr configured

Content Search Component Status

URL

http://127.0.0.1

URL of the Solr server

Port

8983

Listening port of the Solr server

App context

solr

Solr file search application context. For typical use leave the default.

Config prefix

fccore

Solr configuration prefix. For typical use leave the default.

For multisite installations, each Solr configuration must have its own prefix.

Managed Storage Index Status

Managed: 126657, Indexed: 12695

Current index status of files in managed storage

[Reindex](#) [Sync](#) [Check](#)

Search tokenizer

[Update](#)

Update available for app that splits text for indexing. Click to update.

Enable Solr OCR

[Enable](#)

Enable optical character recognition for image and PDF files.

Enable PII search

Enable searching by Personally Identifiable Information (PII) patterns.

- Click Add to add a PII pattern for US Social Number.

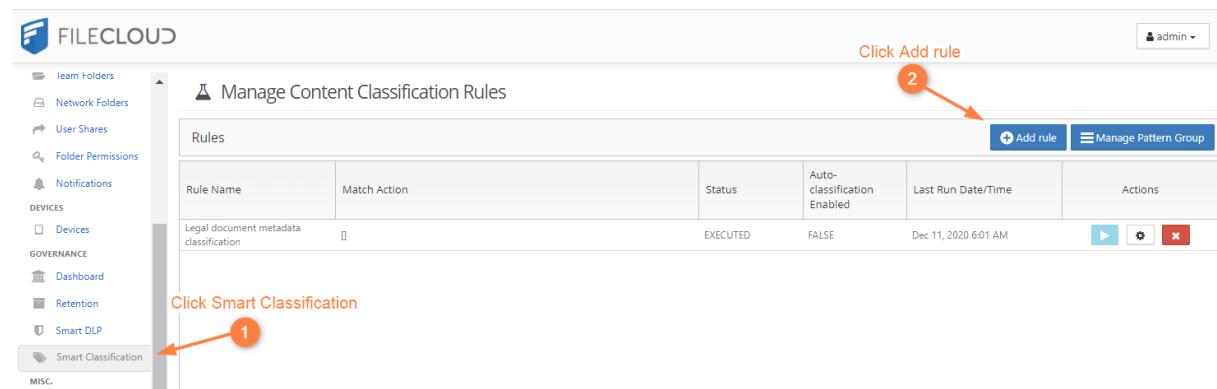
## Edit PII Search Pattern

Name	U.S. Social Security Number (SSN)
Regex	[0-9]{3}-[0-9]{2}-[0-9]{4}

Update
CANCEL

### 3. Create Smart Classification Rule

- Log in to the FileCloud Admin portal, and in the navigation panel, click **Smart Classification**.
- Add a new classification rule



The screenshot shows the 'Manage Content Classification Rules' interface. On the left, a sidebar lists various navigation items. The 'Smart Classification' item is highlighted with a red circle and an arrow labeled '1'. In the main content area, there is a table titled 'Rules' with one row. The 'Actions' column for this row contains three buttons: a blue play button, a gear icon, and a red X. Above the table, a button labeled 'Add rule' is highlighted with a red circle and an arrow labeled '2'.

- Make sure to specify the exact name of the metadata along with attribute name and PII Regex pattern. In the **Add Rule** dialog box, enter the following into **Definition**:

```
{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "US Social Number": {
      "Detection": "Yes"
    }
  },
  "defaultaction": {
    "US Social Number": {
      "Detection": "No"
    }
  },
  "parameters": {
    "SEARCH_PATTERN_NAMES": [

```

```

    "U.S. Social Security Number (SSN)"
]
}
}
}

```

Add rule

Name: US Social Number

Event triggers: FILEINDEXED

Enable Auto-classification:

Definition:   
Enter the rule definition

```

{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  "matchaction": {
    "US Social Number": {
      "Detection": "Yes"
    }
  }
}

```

Rule Template:

```

{
  "classifier": "Default",
  "precondition": "#PRE CONDITION RULES#",
  "condition": "count(_classifications) > 0",
  /* available functions are join() & count() */
  "matchaction": {
    "#METADATASET_NAME#": {
      "Detection": "Yes"
    }
  }
}

```

Rule Definition Help Classifier Guide

Save Cancel

#### 4. Create Smart DLP Rule

- Log in to the FileCloud Admin portal. In the navigation panel, click **Smart DLP**.
- Add a new DLP rule
- For Documents that contain US Social Number, the rule will check for metadata attributes "Detection" = "Yes" and allow sharing with only domain "codelathe.com"
- For Documents that do not contain US Social Number, the rule will check for metadata attributes "Detection" = "No" and allow sharing with all domains.

Manage DLP Rules

Click Add DLP Rule 2 → Add DLP Rule

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	( <code>_user.inGroup('Company XYZ')</code> and <code>_request.remoteIp in ['43.12.45.78']</code> ) or ( <code>_user.inGroup('Internal')</code> )	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	<span>!</span> <span>edit</span> <span>remove</span>
Confidential Documents	SHARE	( <code>_metadata.existsWithValue('Confidential Documents.Confidential', 'Yes')</code> and <code>_share.onlyUsersFromDomain('codelathe.com')</code> ) or ( <code>_metadata.existsWithValue('Confidential Documents.Confidential', 'No')</code> )	ALLOW	ENFORCE	0	<input checked="" type="checkbox"/>	<span>!</span> <span>edit</span> <span>remove</span>

1 Smart DLP

**Create Rule**

Rule Name <small>(i)</small>	US Social Number
Affected User Actions <small>(i)</small>	SHARE
Rule Expression <small>(i)</small>	<a href="#">Rule Expression Builder</a> <a href="#">Rule Expression Text Editor</a> <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> <code>!_metadata.existsWithValue('US Social Number.Detection') &amp;&amp; !_share.hasUsersFromDomain('codelathe.com')    !_metadata.existsWithValue('US Social Number.Detection')</code> </div>
DLP Action <small>(i)</small>	ALLOW
DLP Mode <small>(i)</small>	ENFORCE
Rule Notification <small>(optional)</small> <small>(i)</small>	

[Rule Creation Help](#) [Cancel](#) [Create](#)

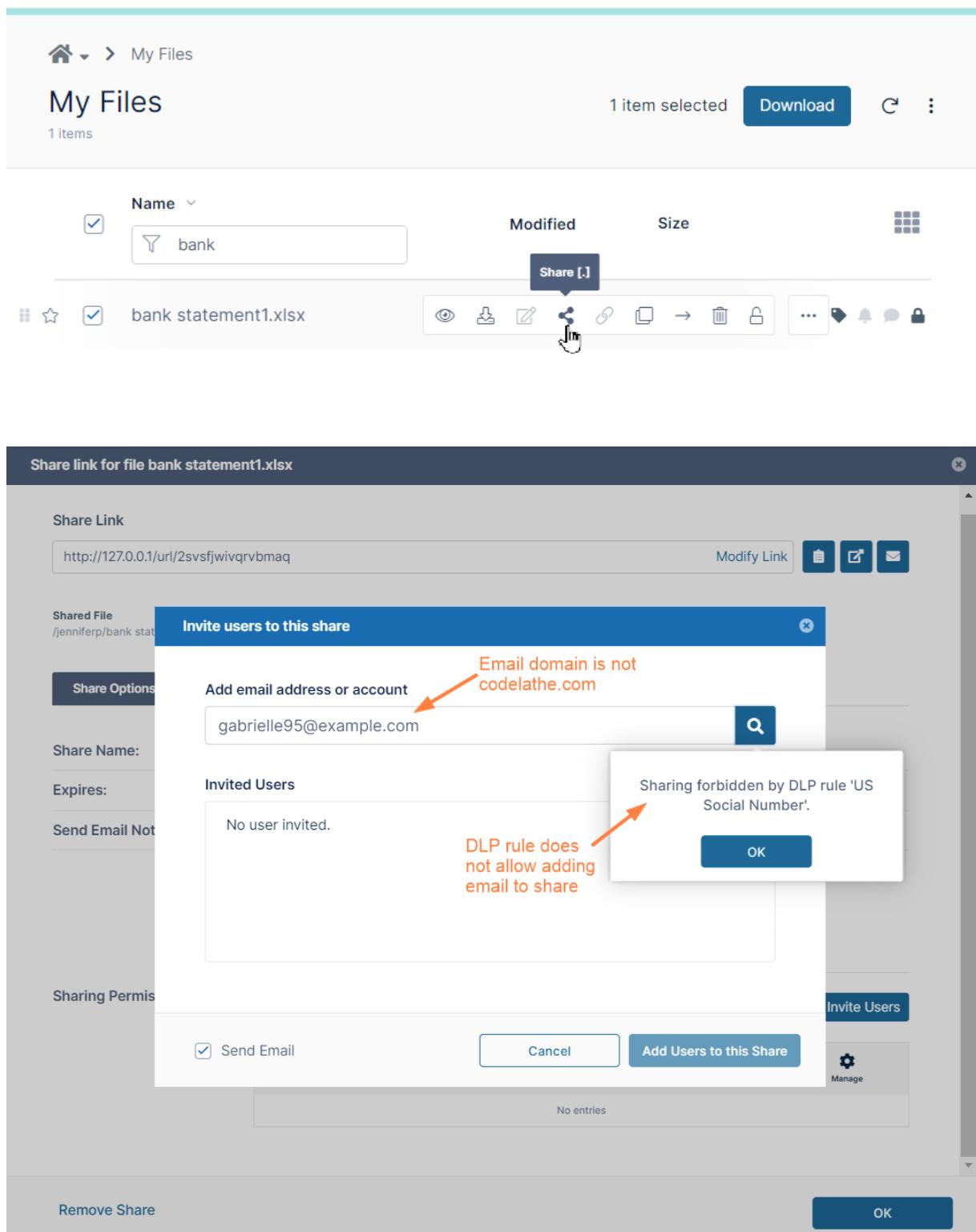
## 5-Upload documents to Filecloud's User interface

- Log in to the FileCloud user portal.
- Upload multiple documents to My Files or to a Team Folder. Some of the files should contain US Social Number examples.
- The classification rule will detect document that contains US Social Numbers and tag them with the attribute "Detection" = "Yes".
- The documents that do not contain US Social Numbers will be tagged with "Detection" = "No".

The screenshot shows the FileCloud interface with a sidebar on the left containing navigation links like 'All Files', 'My Files', 'Team Folders', 'Network Shares', 'Shared with Me', 'Recent Documents', 'Starred', 'Shared by Me', 'File Operations', and 'Notice'. The main area shows a list of files in 'My Files' with one item selected, 'bank statement1.xlsx'. A tooltip message 'Classification detected US Social Number in the document' is overlaid on the screen. On the right, a 'Metadata' panel is open, showing a single entry for 'US Social Number' with the value 'Yes'.

## 6-Test Smart DLP rule

- Log in to the FileCloud User Portal.
- Share a file that contains US Social Number
- Confirm that sharing is only allowed only with users from the domain "codelathe.com"



The screenshot shows the 'My Files' interface in the FileCloud User Portal. A file named 'bank statement1.xlsx' is selected, indicated by a checkmark in the header and a checkmark next to the file name in the list. The file is filtered by the text 'bank'. The 'Share [.]' button is highlighted with a blue box and a downward arrow. The file list includes icons for star, checkmark, and a grid.

**Share link for file bank statement1.xlsx**

**Share Link**  
http://127.0.0.1/url/2svsfjwivqrvbmaq

**Shared File**  
/jenniferp/bank stat

**Invite users to this share**

**Add email address or account**  
gabrielle95@example.com

**Invited Users**  
No user invited.

**Sharing forbidden by DLP rule 'US Social Number'.**

**DLP rule does not allow adding email to share**

**OK**

**Sharing Permissions**

**Send Email**

**Cancel**

**Add Users to this Share**

**Remove Share**

**OK**

Annotations in the screenshot highlight the following:
 

- An orange arrow points from the text 'Email domain is not codelathe.com' to the email address 'gabrielle95@example.com'.
- An orange arrow points from the text 'Sharing forbidden by DLP rule 'US Social Number''. to the 'OK' button of the error dialog.
- An orange arrow points from the text 'DLP rule does not allow adding email to share' to the same 'OK' button.

## Limit Web Login to a specific group of users

### Overview:

The purpose of this Example is to create a Smart DLP rule that allows login to Filecloud account for a certain group from only the web browser. Users from another group will be able to login to their Filecloud account using different methods.

Assuming that a partner company name is "Company XYZ", we created a FileCloud group called "Company XYZ" containing users from this company.

Another group called "Internal" which contains all the internal users from your company.

Users from the group "Company XYZ" will be limited to log in only through the Web browser.

Users from group "Internal" will be able to log in through the web browser, Filecloud Sync, Drive, mobile phone applications ...etc

### Configuration Steps:

#### 1-Create Smart DLP Rule

- Access FileCloud's Admin portal > Smart DLP
- Add a new Dlp rule
- The rule allows downloads from users in the group "Company XYZ" and requests must be initiated from the web browser.
- The second part of the rule allows downloads from users in group Internal from any client.

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	<code>(_user.inGroup('Company XYZ') and _request.remoteip in ['43.12.45.78']) or (_user.inGroup('Internal'))</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	<span style="color: orange;">⚠</span> <span style="color: orange;">🔗</span> <span style="color: orange;">✖</span>
Confidential Documents	SHARE	<code>(_metadata.existsWithValue('Confidential Documents Confidential', 'Yes') and _share.onlyUsersFromDomain('codelathe.com')) or (_metadata.existsWithValue('Confidential Documents Confidential', 'No'))</code>	ALLOW	ENFORCE	0	<input checked="" type="checkbox"/>	<span style="color: orange;">⚠</span> <span style="color: orange;">🔗</span> <span style="color: orange;">✖</span>

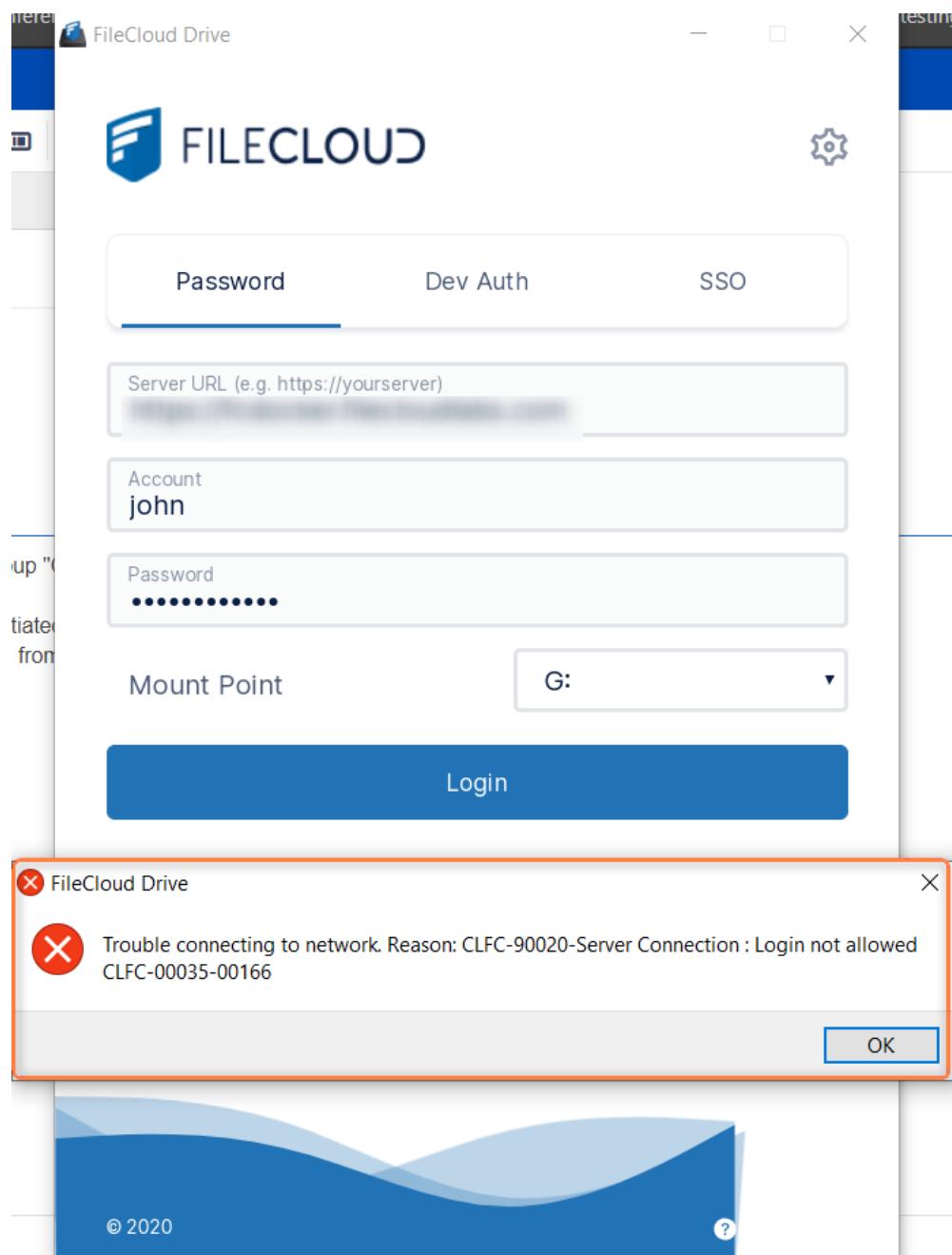
**Create Rule**

<b>Rule Name</b> ⓘ	Limited login methods for external users
<b>Affected User Actions</b> ⓘ	LOGIN
<b>Rule Expression</b> ⓘ	<a href="#">Rule Expression Builder</a> <a href="#">Rule Expression Text Editor</a> <div style="border: 2px solid orange; padding: 5px; margin-top: 10px;"> <code>(_user.inGroup('Company XYZ') &amp;&amp; _request.agent == 'Web browser'    (_user.inGroup('Internal') &amp;&amp; _request.agent == 'FileCloud Drive','Cloud Sync','Web browser','Android','iOS','MS Outlook','MS Office'))</code> </div>
<b>DLP Action</b> ⓘ	ALLOW
<b>DLP Mode</b> ⓘ	ENFORCE
<b>Rule Notification (optional)</b> ⓘ	<div style="border: 1px solid #ccc; padding: 5px; height: 40px; margin-top: 10px;"></div> <p>* Does not apply to login rules * Does not apply to permissive rules.</p>
<a href="#">Rule Creation Help</a> <span style="border: 1px solid #ccc; padding: 2px 10px; margin: 0 10px;">Cancel</span> <span style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; font-weight: bold;">Create</span>	

## 2-Test Smart DLP rule

### Test case 1:

- Open the Filecloud Drive application.
- Try to login with user John who is part of the group "Company XYZ".
- User John will not be able to log in using the Filecloud Drive application.

**Test case 2 :**

- Access FileCloud's User Interface .
- Try to login with user John which is part of the group "Company XYZ".
- User John will be able to log in to the web interface.

**Test case 3:**

- Open the Filecloud Drive application.
- Try to login with user Wail which is part of the group "Internal".

- User Wail will not be able to log in using the Filecloud Drive application.

#### Test case 3:

- Access FileCloud's User Interface.
- Try to login with user Wail which is part of the group "Internal".
- User Wail will be also able to log in to the web interface.

## Troubleshooting DLP

### Problem: Combined rules don't deny or allow actions as expected.

#### Possible cause:

##### Incorrect use of combined expressions in different rules

Use of multiple rules leads to their expressions being combined, and there is a misunderstanding about the results they achieve.

The following clarifies how combined expressions work together:

- **When you use multiple DENY expressions in different rules:**

If any of the DENY expressions is true, the action is blocked.

If none of the DENY expressions is true, the action is allowed.

In other words, DENY expressions coming from different rules have an **OR** combination:

##### Example:

Download DENY expression rule 1: `_file.pathStartsWith('/teamaccount/TeamFolder_01/FolderA')`

Download DENY expression rule 2: `_file.pathStartsWith('/teamaccount/TeamFolder_01/FolderB')`

To clarify how these work together, imagine them in a single rule, combined. These would appear as:

`_file.pathStartsWith('/teamaccount/TeamFolder_01/FolderA') || _file.pathStartsWith('/teamaccount/TeamFolder_01/FolderB')`

Download is blocked from FolderA **OR** FolderB, but downloads from other folders are allowed.

- **When you use multiple ALLOW expressions in different rules:**

The ALLOW expressions must be different or the combined expression can never be true (that is, you cannot use 2 or more `_file.pathStartsWith` expressions, 2 or more `request.remotelp` expressions, and so on, that you set to different values.)

ALLOW expressions coming from different rules have an **AND** combination:

##### Example:

Download ALLOW expression rule 1: `_file.pathStartsWith('/teamaccount/TeamFolder_01')`

Download ALLOW expression rule 2: `_user.inGroup('internalUsers')`

To clarify how these work together, imagine them in a single rule, combined. These would appear as:

`_file.pathStartsWith('/teamaccount/TeamFolder_01') && _user.inGroup('internalUsers')`

Only downloads in the TeamFolder\_01 directory for users in the internalUsers group are

allowed. All other downloads are blocked.

# Example: Setting Up a Retention Policy to meet HIPAA Requirements

The customer we'll look at in this example is Community HMO, a health maintenance organization whose FileCloud users are both health care professionals and administrative personnel. In this example, your role is the FileCloud admin.

To meet the requirements for passing two of the rules in the Compliance Center's HIPAA screen, you must choose a retention policy that ensures you retain ePHI data. These rules are:

- [164.312\(c\)\(1\)](#)<sup>96</sup>- Technical Safeguards - Set up a retention policy to protect files and folders from deletion.
- [164.316\(b\)\(2\)\(i\)](#)<sup>97</sup>- Policies and procedures and documentation requirements - Use Retention Policy to retain files for 6 years.

This example will walk you through the process necessary to pass these requirements. The broader steps involve:

1. Enabling the HIPAA retention policy rules in the Compliance Center.
2. Creating a metadata attribute to tag files with ePHI data.
3. Creating a pattern group that identifies file content as ePHI.
4. Setting up a Smart Classification rule to locate and tag ePHI files.
5. Setting up a retention policy that prevents these files from being deleted for 6 years after their creation.
6. Choosing the retention policy in the Compliance Center for each of the requirements listed above.

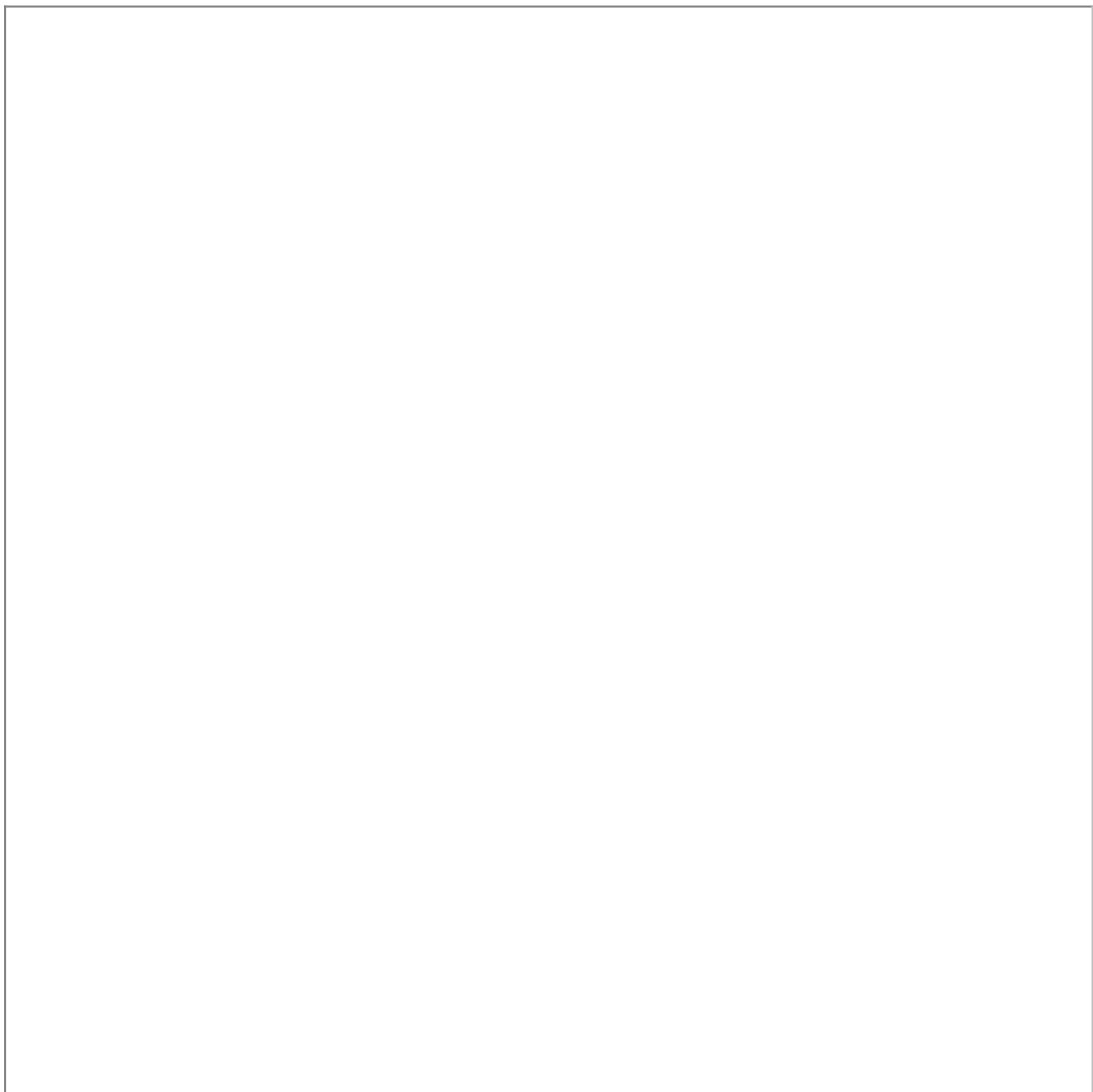
## Step 1: Enable the HIPAA retention policies rules in the Compliance Center.

1. In the Admin portal's navigation panel, click **Compliance Center**.  
The **Compliance Center** opens to the **Overview** tab.
2. Under **Enabled Configurations**, click the slider next to the HIPAA icon.
3. To go to the **HIPAA Compliance** page, click the **HIPAA** link in the menu bar.

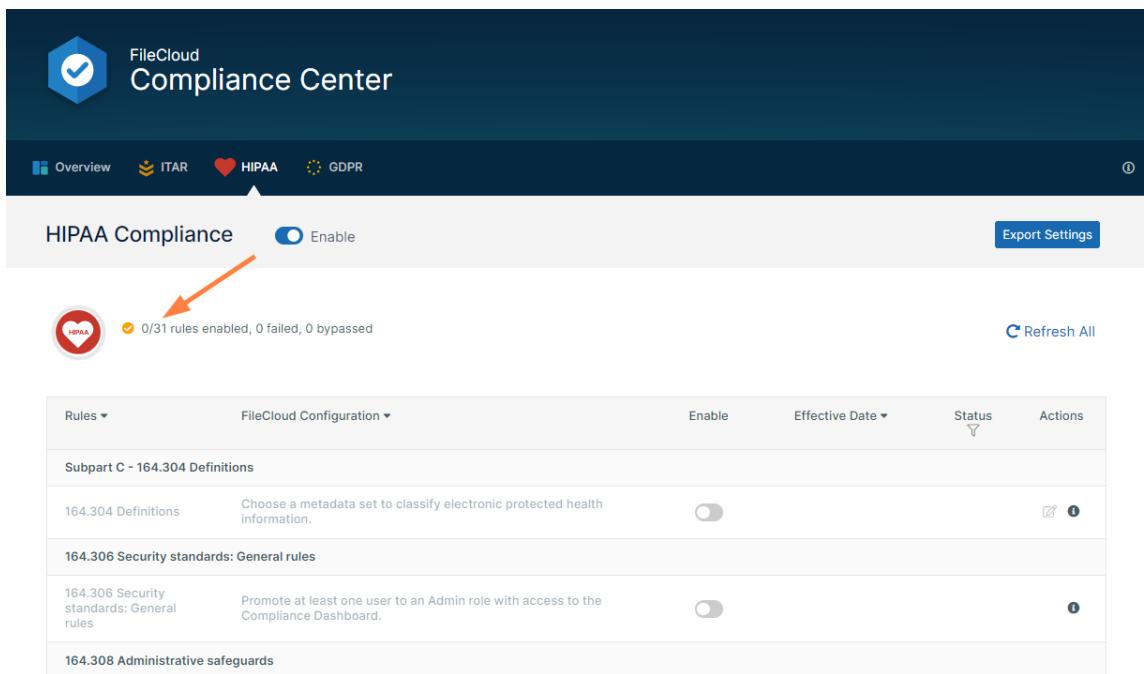
---

96. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.312#p-164.312\(c\)\(1\)](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.312#p-164.312(c)(1))

97. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316\(b\)\(2\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(2)(i))



The HIPAA page opens. In this example, you have not enabled any of your HIPAA rules yet.



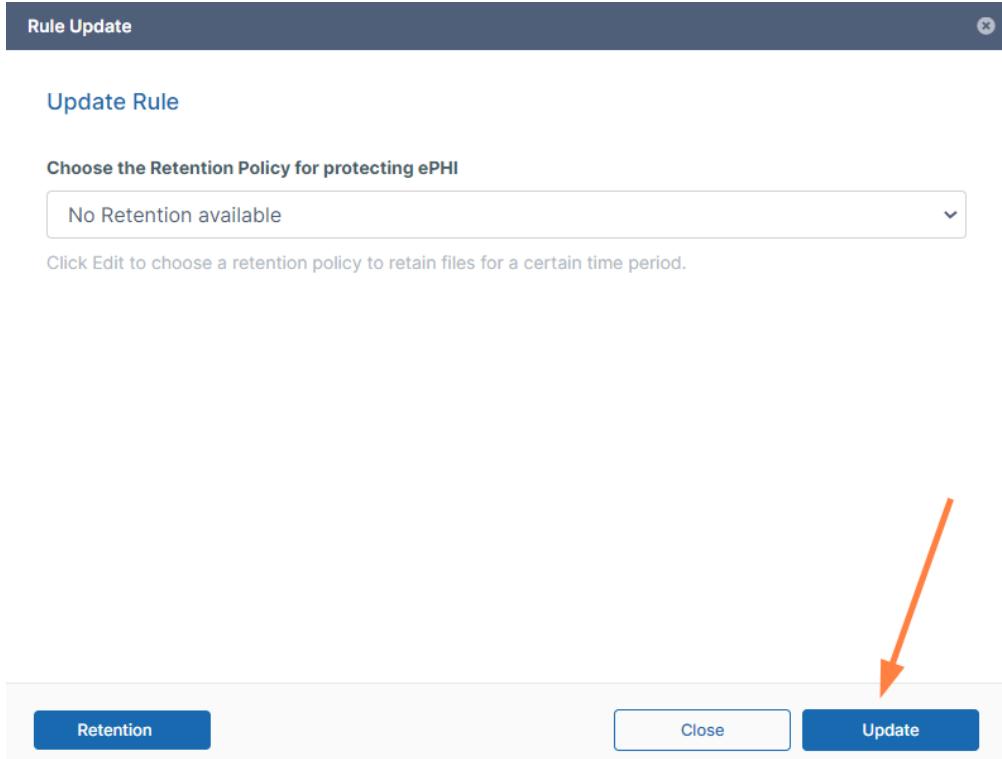
HIPAA Compliance Enable Export Settings

 0/31 rules enabled, 0 failed, 0 bypassed Refresh All

Rules ▾	FileCloud Configuration ▾	Enable	Effective Date ▾	Status	Actions
Subpart C - 164.304 Definitions					
164.304 Definitions	Choose a metadata set to classify electronic protected health information.	<input checked="" type="checkbox"/>			
164.306 Security standards: General rules					
164.306 Security standards: General rules	Promote at least one user to an Admin role with access to the Compliance Dashboard.	<input checked="" type="checkbox"/>			
164.308 Administrative safeguards					

4. Scroll down so you can see rules **164.312(c)(1)** and **164.316(b)(2)(i)**.  
These are the two rules that you will set up retention policies for.
5. Enable each rule.

For each rule, you are prompted to choose a retention policy that enables you to pass the rule.



Rule Update ×

Update Rule

Choose the Retention Policy for protecting ePHI

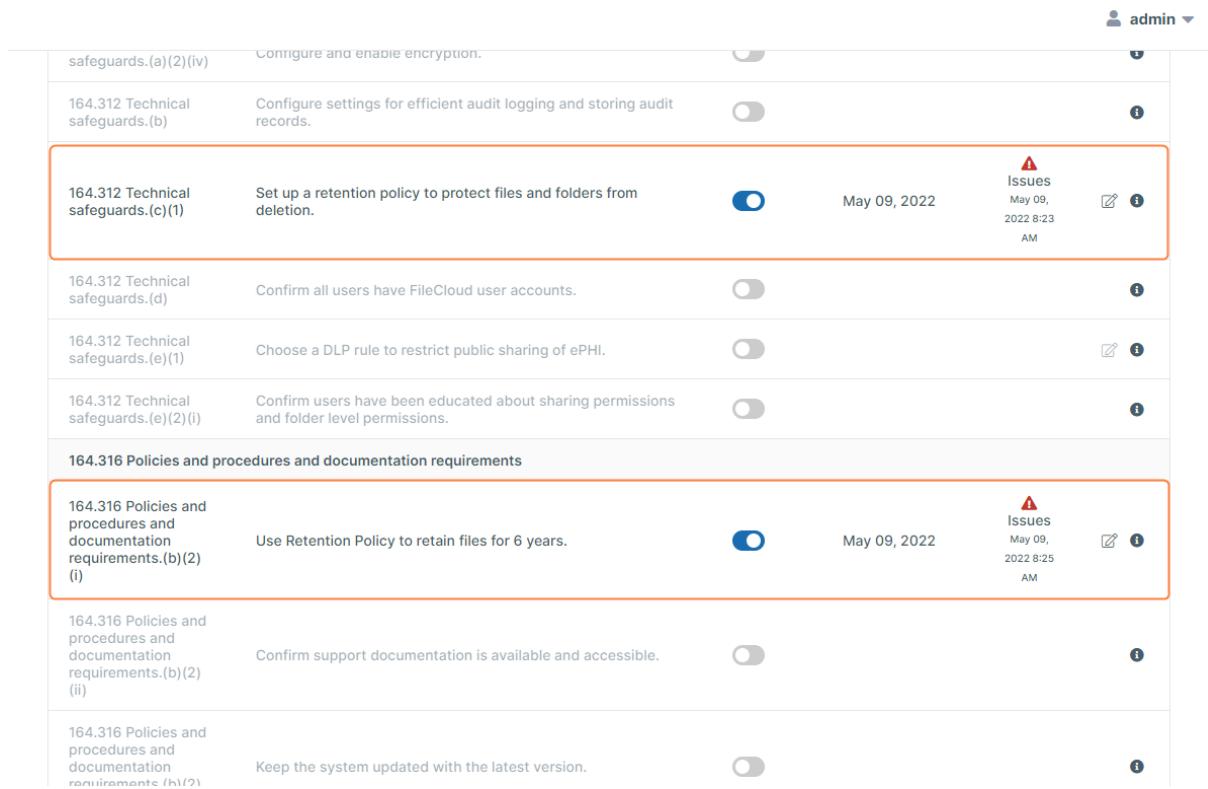
No Retention available

Click Edit to choose a retention policy to retain files for a certain time period.

Retention Close Update

6. Since you have not set up the retention policy yet, click **Update** without attempting to select a retention policy.

The row for each rule will indicate that FileCloud has failed the rule.



Configure and enable encryption.			
safeguards.(a)(2)(iv)	Configure settings for efficient audit logging and storing audit records.	<input type="checkbox"/>	
164.312 Technical safeguards.(b)	Set up a retention policy to protect files and folders from deletion.	<input checked="" type="checkbox"/>	May 09, 2022  Issues May 09, 2022 8:23 AM
164.312 Technical safeguards.(c)(1)	Confirm all users have FileCloud user accounts.	<input type="checkbox"/>	
164.312 Technical safeguards.(d)	Choose a DLP rule to restrict public sharing of ePHI.	<input type="checkbox"/>	
164.312 Technical safeguards.(e)(1)	Confirm users have been educated about sharing permissions and folder level permissions.	<input type="checkbox"/>	
164.316 Policies and procedures and documentation requirements			
164.316 Policies and procedures and documentation requirements.(b)(2) (i)	Use Retention Policy to retain files for 6 years.	<input checked="" type="checkbox"/>	May 09, 2022  Issues May 09, 2022 8:25 AM
164.316 Policies and procedures and documentation requirements.(b)(2) (ii)	Confirm support documentation is available and accessible.	<input type="checkbox"/>	
164.316 Policies and procedures and documentation requirements.(b)(2) (iii)	Keep the system updated with the latest version.	<input type="checkbox"/>	

## Step 2: Create a metadata attribute to tag files with ePHI data

The function of HIPAA compliance is to protect electronic protected health information, such as individuals' medical records and insurance information. Before you can place safeguards on this information, it's necessary that you identify which files contain it. You can do this by configuring FileCloud's smart classification system to flag files that contain the wide range of information considered ePHI, for example, medical diagnoses and insurance policy numbers.

When the smart classification system finds a file with ePHI, it tags it with metadata to let FileCloud know that the file contains ePHI.

To identify a file as containing ePHI, you must tell the content search engine what patterns (character strings) to look for in the file's contents. For example, if the file contains the pattern "**Ins Policy ID**" that could indicate that the file contains ePHI. You must include all of the possible patterns that indicate a file contains ePHI, and then flag each of these files with a metadata tag.

There are also files with handwritten diagnostic information that doctors scan into your system. This is ePHI that smart classification cannot locate, and must be flagged with metadata manually. Therefore, you must give some users permission to add the metadata manually when you create it.

1. Create the metadata to tag the file with.

- a. To open the **Metadata** page, in the admin portal navigation pane, click **Metadata**.

b. Click **Add Metadata Set**.

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	1	1	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	1	1	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	1	1	
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	1	1	
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	1	1	
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	1	1	

The **Add Metadata Set Definition** dialog box opens.

c. Enter the values for the metadata set.

For this example:

- In **Name**, enter **Files with ePHI**.
- In **Description**, enter **Tag files with electronically protected health information**.

**Metadata Set**

**Name\***  
Files with ePHI

**Description\***  
Tag files with electronically protected health information.

**Disabled**

- In the **Attributes** box, click **Add Attribute**.

For this example, in the **Add Attribute** dialog box, in **Name**, enter **ePHI** and in **Attribute type**, choose **Boolean**.

Whenever a file has ePHI, this Boolean value will be set to **1**.

**Add Attribute**

Name	<input type="text" value="ePHI"/>
Description	<input type="text"/>
Attribute Type	<input type="text" value="Boolean"/>
Disabled	<input type="checkbox"/>
Required	<input type="checkbox"/>
Default Value	<input type="checkbox"/>

**Create** **Close**

d. Click **Create**.

**Metadata Set**

Name\*  
Files with ePHI

Description\*  
Tag files with electronically protected health information.

Disabled

**Permissions**

Users   Groups   Paths

**Add User**

Name	Read Permission	Write Permission

**Attributes**

**+ Add Attribute**

Name	Attribute Type	Description	Status	Actions
ePHI	Boolean		Enabled	

**Create** **Close**

Now add a user who can manually flag files with the ePHI metadata:

- e. In the **Permissions** box, click **Add User**.
- f. Enter the user or users who will be manually marking scanned doctor notes as having ePHI data, and give them **Read** and **Write** permissions.

**Read** permission enables the user(s) to view the metadata, but **Write** permission enables them to change it, so the user(s) you add should have a good understanding of what constitutes ePHI in your system.

**Metadata Set**

Name\*  
Files with ePHI

Description\*  
Tag files with electronically protected health information.

Disabled

**Permissions**

Users Groups Paths

Add User

Name	Read Permission	Write Permission
jari1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Page 1 of 1

**Attributes**

Add Attribute

Name	Attribute Type	Description	Status	Actions
ePHI	Boolean		Enabled	

**Create** **Close**

### Step 3: Create a pattern group that identifies file content as ePHI

Community HMO has the following types of files that contain PHI:

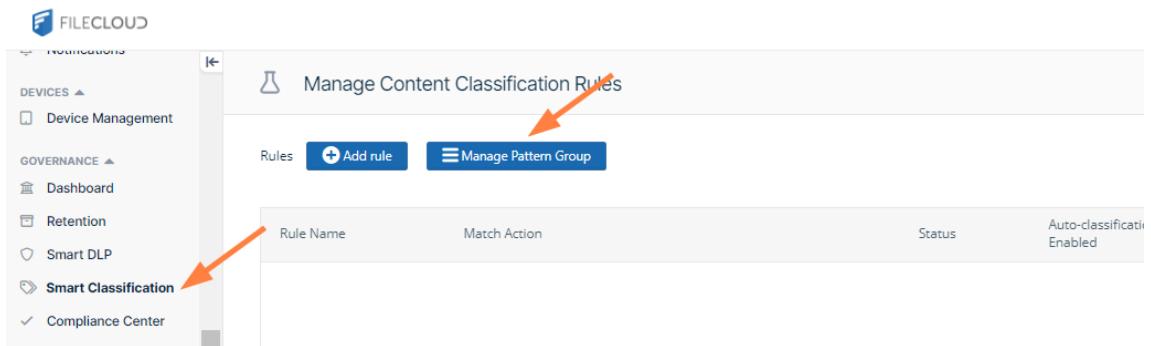
- Medical records that all have the string **Medical Record Number** in them.
- Insurance records that all have the string **Insurance Policy ID** in them.
- Scanned doctor diagnosis notes.

You have determined that the scanned doctor diagnosis notes will have to be tagged with metadata manually, and that smart classification can automatically search for the identifying strings in the medical records and insurance records.

To configure the pattern group for identifying PHI:

1. In the admin portal navigation pane, click **Smart Classification**.  
The **Manage Content Classification Rules** screen opens.

## 2. Click Manage Pattern Group



The **Manage Pattern Groups** dialog box opens.

Manage Pattern Groups : test

Pattern Group: test

**Available Patterns**

- Belgium National Number
- Croatia Identity Card Number
- Croatia Personal Identification (OIB) Number
- Denmark Personal Identification Number
- EU Debit Card Number
- Finland National ID
- Finland Passport Number
- France Driver's License Number
- France National ID Card (CNI)
- France Passport Number

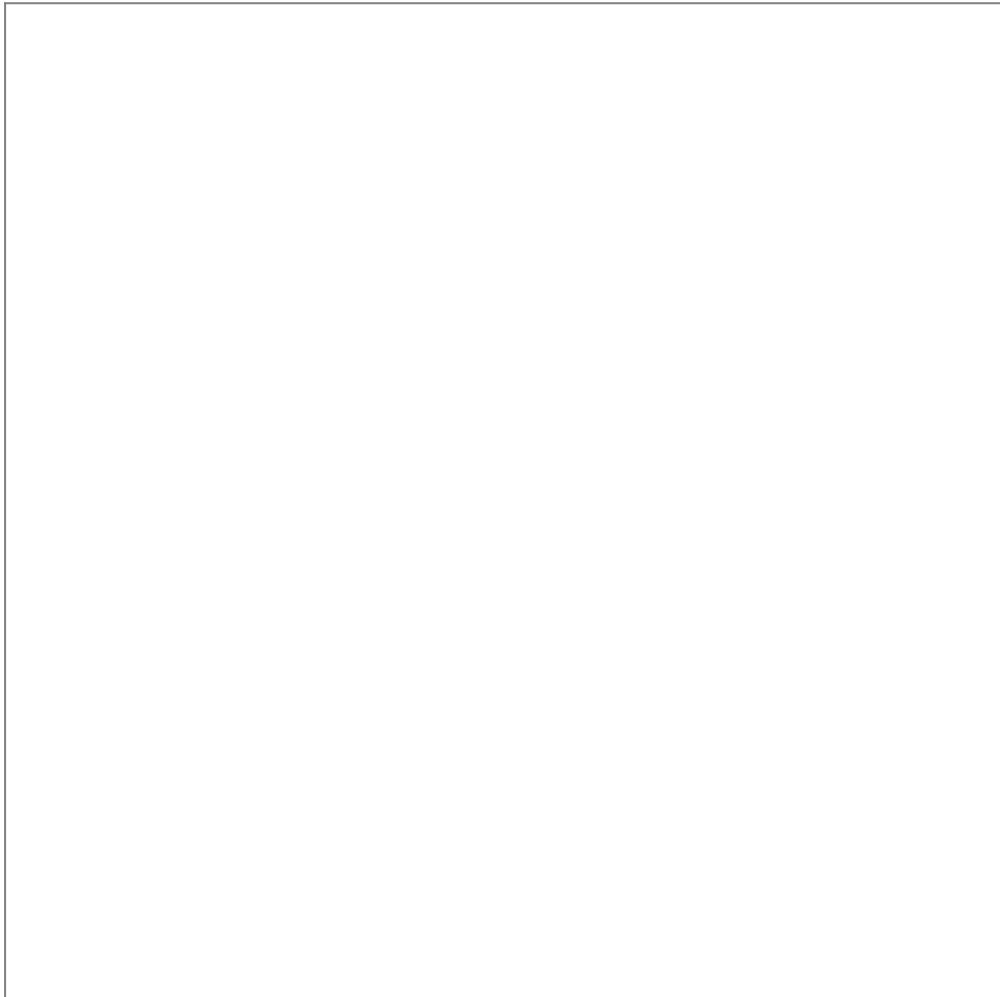
Page: 1 of 3    21 rows

**Member Patterns**

**Buttons:**

- + Add New Pattern
- Delete
- Close

3. Click **New Pattern Group**.
4. For this example, name the new group **ePHI Patterns**.



5. Click **Save**, and in the **Pattern Group** drop-down list, choose **ePHI Patterns**.

Now, you are ready to add the patterns that smart classification will search for in your files. When it finds any of these patterns in a file, it will tag it with the **ePHI** metadata attribute.

6. Click **Add New Pattern**.

Manage Pattern Groups : ePHI Patterns

Pattern Group ePHI Patterns 1 New Pattern Group

Available Patterns

- Belgium National Number
- Croatia Identity Card Number
- Croatia Personal Identification (OIB) Number
- Denmark Personal Identification Number
- EU Debit Card Number
- Finland National ID
- Finland Passport Number
- France Driver's License Number
- France National ID Card (CNI)
- France Passport Number

Page 1 of 3 21 rows

Member Patterns

2

Add New Pattern Delete Close

The **New Pattern** dialog box opens.

7. Click **Add**.

**New Pattern**



Manage PII Patterns		
Name	Regex	Actions
Belgium National Number	[0-9]{2}.[0-9]{2}.[0-9]{2}-[0-9]{3}.[0-9]{2}	 
Croatia Identity Card Number	[0-9]{9}	 
Croatia Personal Identification (OIB) Number	[0-9]{10}	 
Denmark Personal Identification Number	[0-9]{6}-[0-9]{4}	 
EU Debit Card Number	[0-9]{16}	 
Finland National ID	[0-9]{6}[+-a][0-9]{3}[0-9a-zA-Z]{1}	 
Finland Passport Number	[a-zA-Z]{2}[0-9]{7}	 
France Driver's License Number	[0-9]{12}	 
France National ID Card (CNI)	[0-9]{12}	 
France Passport Number	[0-9]{2}[a-zA-Z]{2}[0-9]{5}	 
Page <input type="text" value="1"/> of 3  21 rows		

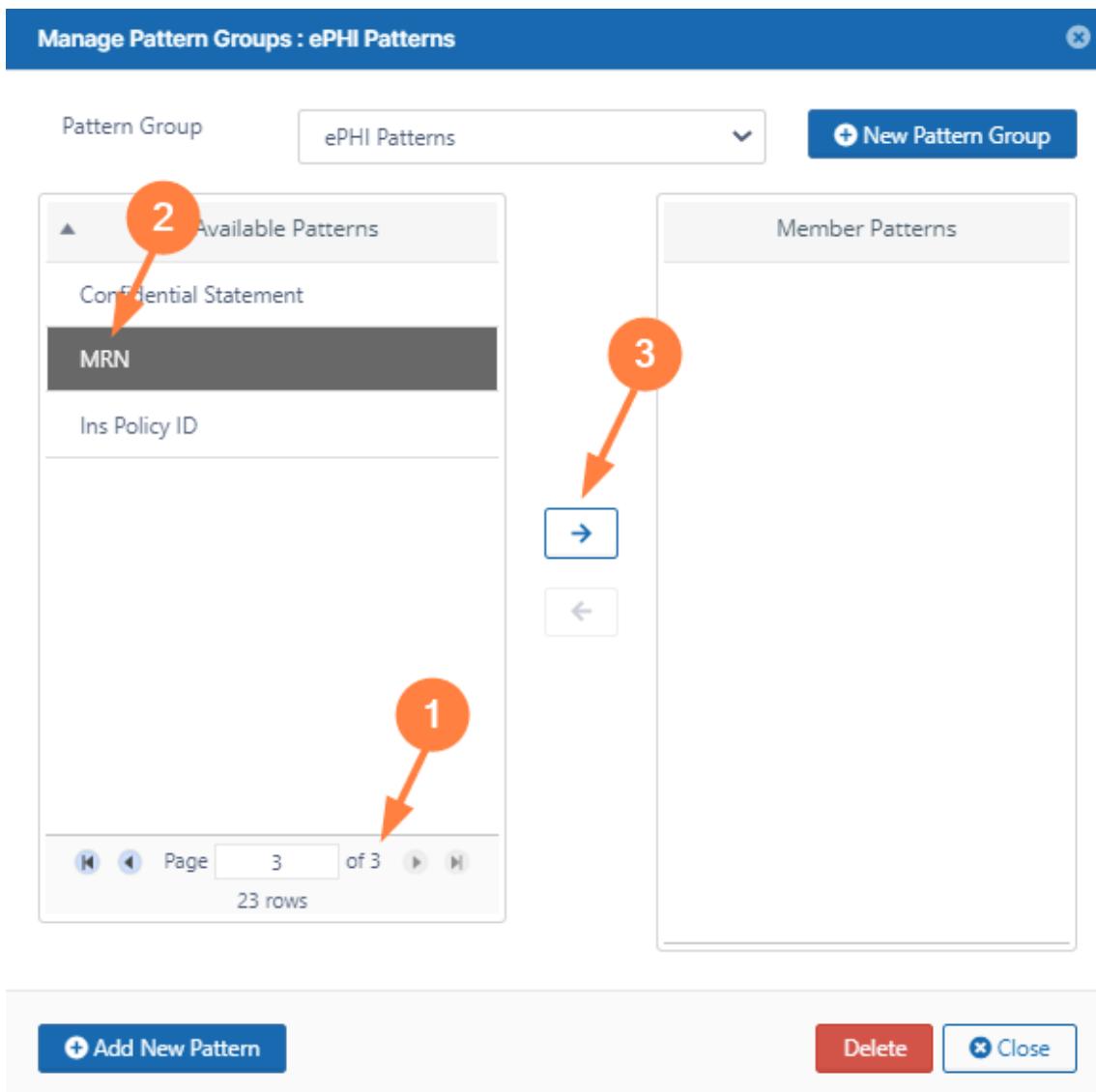
 Close

The **New PII Search Pattern** dialog box opens.

8. Enter **MRN** in **Name**, and enter **MRN** in **Regex**.



9. Click **Create**.
10. Click **Add** again, and in the **New PII Search Pattern** dialog box enter **Ins Policy ID** in both **Name** and **Regex**.
11. Click **Create**.
12. Close the **New Pattern** dialog box.
13. In the **Manage Pattern Groups** dialog box, confirm that you still have **ePHI Patterns** selected in the **Pattern Group** field.
14. In the **Available Patterns** box, scroll to the last page, and click **MRN**, then click the right arrow.



The pattern appears in the **Member Patterns** box.

15. In the **Available Patterns** box, click **Ins Policy Number**, and then click the right arrow. Both patterns now appear in the **Member Patterns** box.

Manage Pattern Groups : ePHI Patterns

Pattern Group: ePHI Patterns

**New Pattern Group**

**Available Patterns**

- Confidential Statement
- MRN
- Ins Policy ID

**Member Patterns**

- MRN
- Ins Policy ID

**Add New Pattern** **Delete** **Close**

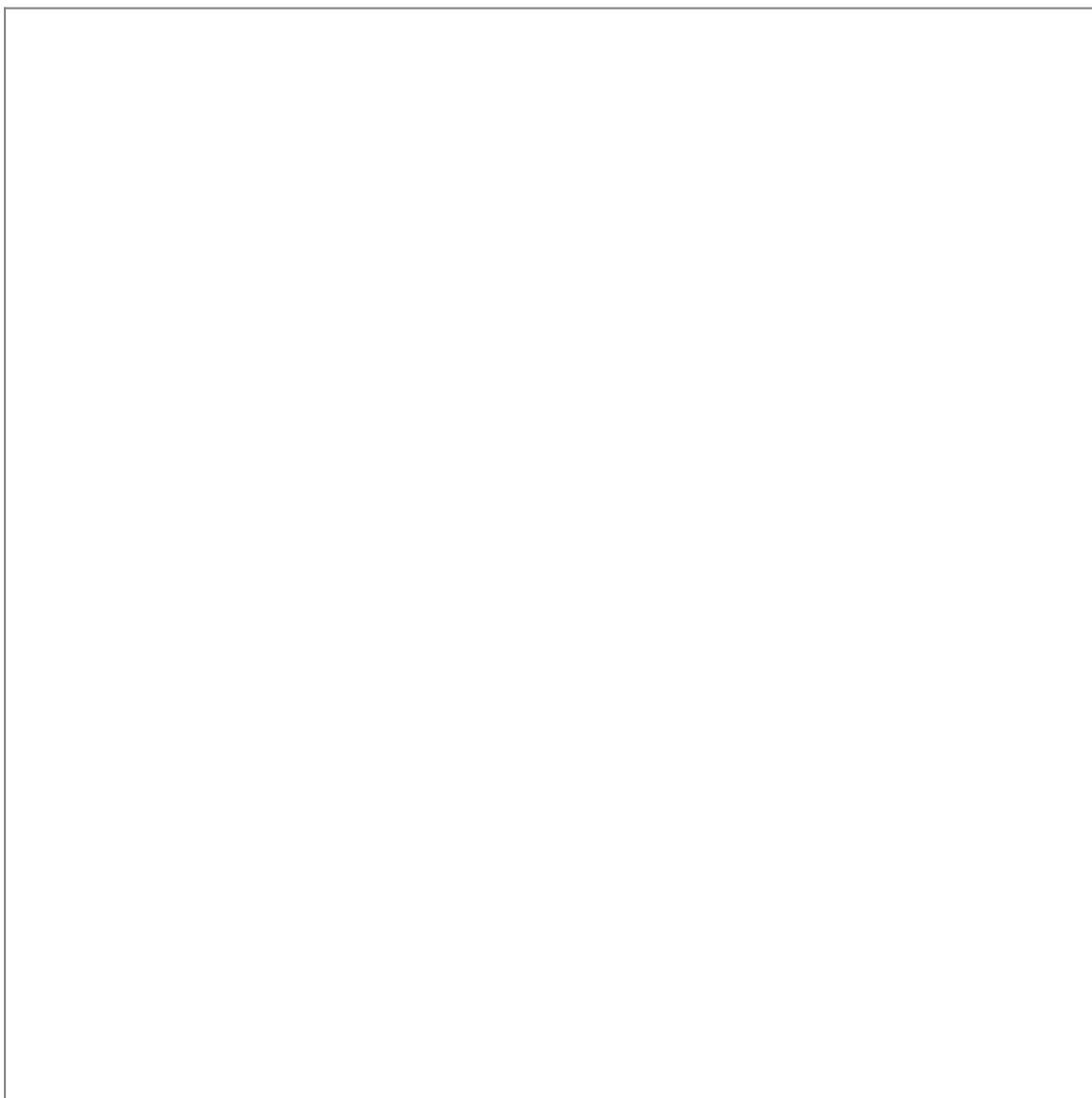
16. Click **Close**.

## Step 4: Set up a Smart Classification rule to locate and tag ePHI files

Now that you have configured the search patterns for identifying ePHI in files, you can set up a smart classification rule that uses the patterns to find and tag the files.

**To set up the smart classification rule:**

1. In the admin portal navigation pane, click **Smart Classification**.  
The **Manage Content Classification Rules** screen opens.
2. Click **Add Rule**.



An **Add Rule** dialog box opens.

3. Fill in values for the fields.
  - a. In **Name**, enter **Classify files with PHI**.
  - b. In **Event triggers**, choose **FILEINDEXED**. This indicates that when the file is indexed, smart classification should apply this rule (that is, set the **ePHI** metadata attribute to **true**).
  - c. Check **Enable Auto-classification**.
  - d. In **Definition**, define the rule. To simplify setting it up, copy and paste the **Rule Template** from the space under it, and modify the template.

Enter the rule as:

```
{  
  "classifier": "Default",  
  "precondition": "true",  
  "condition": "count(_classifications) > 0",
```

```

"matchaction": {
    "Files with ePHI": {
        "ePHI": true
    }
},
"defaultaction": [],
"parameters": {
    "SEARCH_PATTERN_GROUPS": [
        "ePHI Patterns"
    ]
}
}

```

The rule indicates that if either of the search patterns (**MRN** and **Ins Policy ID**) in the search pattern group **ePHI Patterns** are found in the file being indexed, the metadata attribute **ePHI** is set to **true**.

Add rule

Name: Classify files with PHI

Event triggers: FILEINDEXED

Enable Auto-classification:

Definition:

```

{
    "classifier": "Default",
    "precondition": "true",
    "condition": "count_(classifications) > 0",
    /* available functions are join() & count() */
    "matchaction": {
        "Files with ePHI": {

```

Rule Template:

```

#METADATASET_NAME# : {
    "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#"
}
},
"parameters": {
    "SEARCH_PATTERN_SET": "[#REGULARE EXPRESSION#", "#REGULARE EXPRESSION#"]",
    "SEARCH_PATTERN_NAMES": "[#PATTERN NAME#", "#PATTERN NAME#"]",
    "SEARCH_PATTERN_GROUPS": "[#PATTERN GROUP#]"
}

```

Rule Definition Help Classifier Guide Save Cancel

#### 4. Now, test the smart classification rule.

- Obtain or create some files that contain the ePHI patterns.

We include:

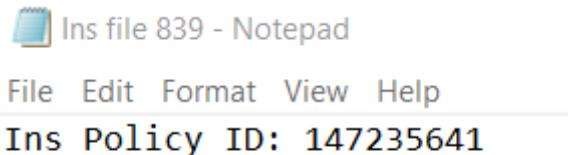
- a test file with an MRN, **Patient 2457.txt**:



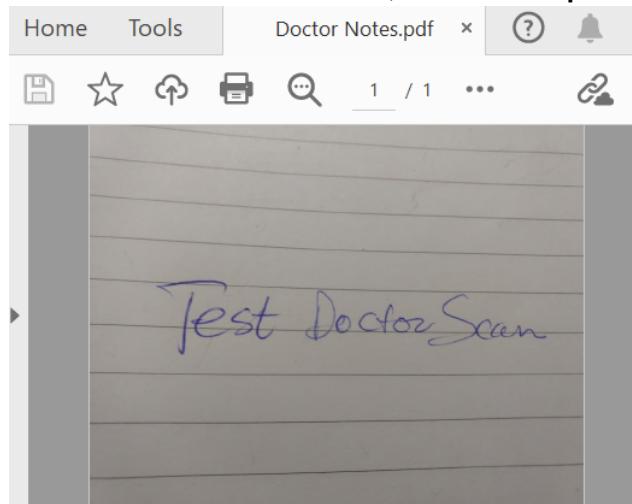
File Edit Format View Help

MRN: 356223190

- a test file with and insurance policy id, **Ins file 839.txt**:



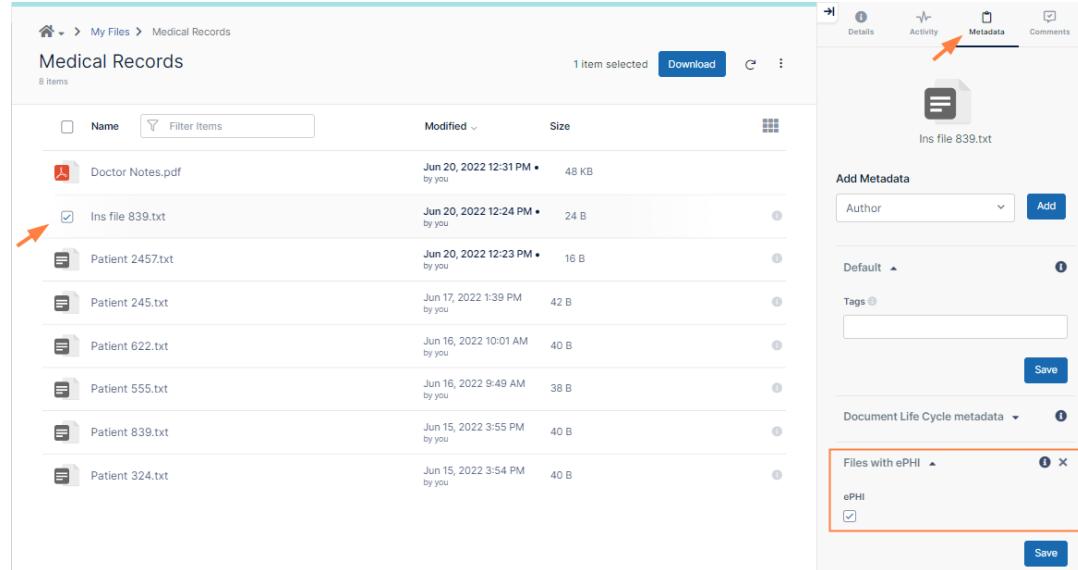
- a test scanned handwritten note, **Doctor Notes.pdf**:



- Log in to the FileCloud user portal as the user you gave permissions to read and write the **Files with ePHI** metadata.
- Upload the files into FileCloud.
- Check the checkbox for the file **Patient 2457.txt** and click **Metadata** in the details pane. Confirm that **Files with ePHI** is listed and that the **ePHI** metadata attribute is checked.

The screenshot shows the FileCloud user portal interface. On the left, a list of files in 'Medical Records' is displayed, including 'Doctor Notes.pdf', 'Ins file 839.txt', 'Patient 2457.txt' (with a red arrow pointing to its checkbox), 'Patient 245.txt', 'Patient 622.txt', 'Patient 555.txt', 'Patient 839.txt', and 'Patient 324.txt'. On the right, the 'Metadata' tab is selected in the details pane for 'Patient 2457.txt'. The 'Add Metadata' section shows 'Author' and 'Default' fields. The 'Document Life Cycle metadata' section shows a 'Files with ePHI' attribute with a checked 'ePHI' checkbox. A blue arrow points to the 'ePHI' checkbox in this section.

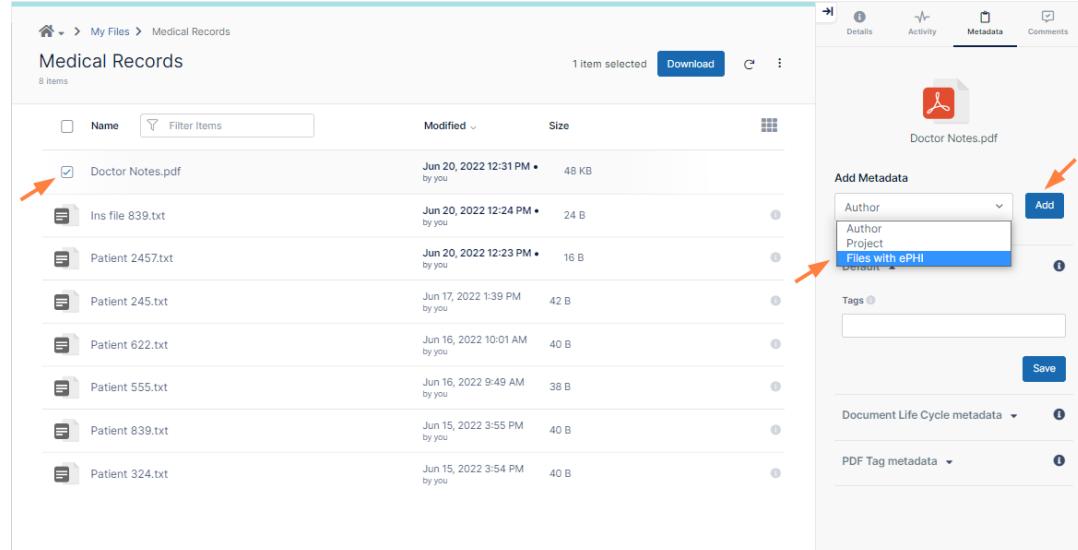
e. Then check the checkbox for the file **Ins file 839.txt**, and click **Metadata** in the details pane. Confirm that **Files with ePHI** is listed and that the **ePHI** metadata attribute is checked.



The screenshot shows the 'Medical Records' list on the left and the 'Metadata' pane on the right for the file 'Ins file 839.txt'. In the list, 'Ins file 839.txt' is selected, indicated by a red arrow. In the 'Metadata' pane, the 'ePHI' checkbox is checked, and the 'Files with ePHI' attribute is listed under 'Document Life Cycle metadata'.

f. Next, check the checkbox for the file **Doctor Notes.pdf**, and click **Metadata** in the details pane. **Files with ePHI** is not yet listed since you are required to check it manually.

g. In the **Add Metadata** drop-down list, choose **Files with ePHI** and click **Add**.



The screenshot shows the 'Medical Records' list on the left and the 'Metadata' pane on the right for the file 'Doctor Notes.pdf'. In the list, 'Doctor Notes.pdf' is selected, indicated by a red arrow. In the 'Metadata' pane, the 'ePHI' checkbox is checked. In the 'Add Metadata' section, 'Files with ePHI' is selected in the dropdown menu, and the 'Add' button is highlighted with a red arrow.

**Files with ePHI** is added to the list of included metadata.

h. Check **ePHI** to indicate that the file has ePHI.

The screenshot shows a list of files in the 'Medical Records' folder. The 'Metadata' tab is active. In the bottom right corner, there is a section titled 'Files with ePHI' with a checkbox labeled 'ePHI' which is checked. A red arrow points to this checkbox.

## Step 5: Set up a 6 year retention policy

The next step is to create the 6 year retention policy that is applied to files with an **ePHI** metadata attribute of **true**.

### To create the 6 year retention policy:

1. In the admin portal navigation pane, click **Retention**.  
The **Manage Retention Policies** screen opens.
2. Click **Add Policy**.

The screenshot shows the 'Manage Retention Policies' screen. The left sidebar has a 'Retention' link highlighted with a red arrow labeled '1'. In the top right corner, there is a '+ Add Policy' button highlighted with a red arrow labeled '2'.

The **Add Retention Policy** form opens.

3. Fill out the **Policy Attributes** section of the form.
  - a. In **Policy Name**, enter **6-year expiry**.
  - b. In **Policy Type**, leave **Retention** selected.  
A **Retention** type policy prevents a file from being deleted, and this fulfills our requirements.
  - c. In **Description**, enter, **Files are kept for at least 6 years**.

d. Leave the checkboxes in this section at their default values (only **Enabled** should be checked).

Add Retention Policy ×

**Policy Attributes**

Policy Name\*  
6-year expiry

Policy Type  
Retention

Retention 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 or archived.

Description\*  
Files are kept for at least 6 years.

Hide Policy From Users

Enabled

Alert On Violation

Send email alert

Alerts\*  
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

4. Add the metadata condition to the **Apply Policy To** section:

- a. Click the **Metadata** tab.
- b. In the drop-down list of metadata sets, choose the metadata set you created for personal health information, **Files with ePHI**.  
A drop-down list of metadata attributes appears.
- c. Choose **ePHI**.  
**ePHI** is listed below the drop-down list with a checkbox.
- d. Select the checkbox to indicate that the retention policy should be applied if **ePHI** is **true**.

**Apply Policy To**

Paths Metadata

Files with ePHI

ePHI

ePHI

**Add**

Set	Attribute	Value	Actions
No search conditions found			

e. Click **Add**.

The condition is added:

5. Fill out the **Actions** section.

- Leave **Time Period** selected.
- In **Time Period of Retention** choose custom so you can set a period that is more than 6 years.
- The time period required in rule [164.316\(b\)\(2\)\(i\)](#)<sup>98</sup> is over six years, so in **No. of Days** enter **2193** [2190 (365 x 6 years) + 2 (for 2 possible leap years) + 1 (to make the period over, not equal to 6 years)].
- Uncheck **Renew Expiry on Access** since the HIPAA rule requires that the records be saved 6 years after creation, not 6 years after access.
- For **Policy Expiry Actions** leave **No Action** selected since files must be saved for a minimum of 6 years, but are not required to be deleted after that.

6. At the bottom of the form, click **Save**.

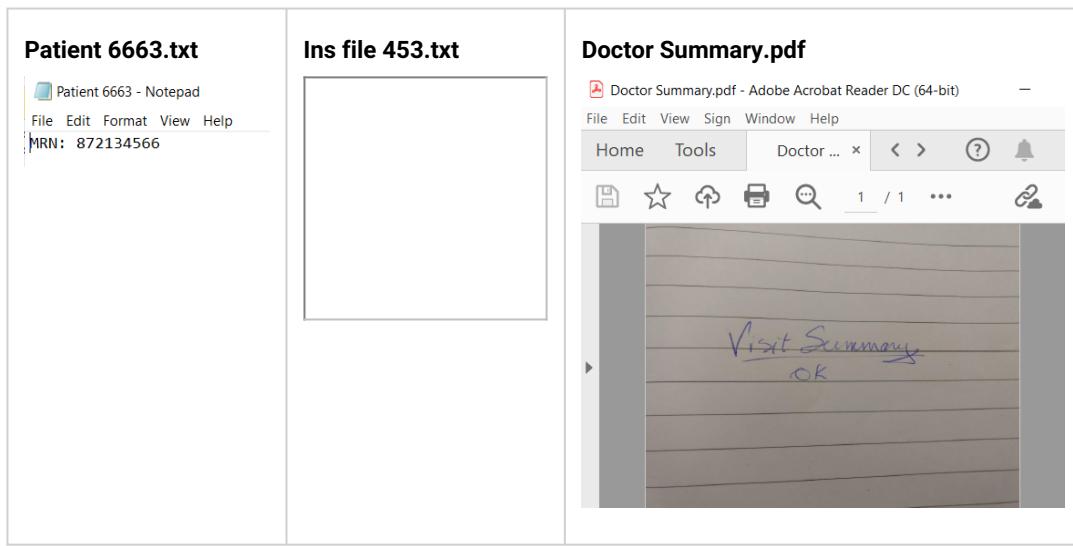
The retention policy is added and enabled by default. Now, each time a file is indexed, FileCloud will check if **ePHI** is true, and if it is, it will apply the 6-year retention policy to the file.

Policy Name		Description	Status	Policy Type	Actions
Test		This is a test retention policy	Disabled	Retention	
30 Day Expiry		expiry date 30 days	Disabled	Retention	
6-year expiry		Files are not deleted for over 6 years.	Enabled	Retention	

7. Now test the retention policy.

- Obtain some files with ePHI content, like the ones you used for testing in Step 4. Our examples include the content **MRN** and **Ins Policy ID**, and a scanned file that must be tagged manually:

98. [https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316\(b\)\(2\)\(i\)](https://www.ecfr.gov/current/title-45 subtitle-A/subchapter-C/part-164/subpart-C/section-164.316#p-164.316(b)(2)(i))



- Log in to the user portal as the user you gave permissions to read and write the **Files with ePHI metadata**.
- Upload the files into FileCloud.
- Select the checkbox for the file **Patient 6663.txt** and click **Details** in the details pane. Confirm that the retention policy is listed at the bottom of the details.

The screenshot shows the FileCloud interface with the following details:

- Medical Records** folder: 11 items.
- Patient 6663.txt** is selected (indicated by a checked checkbox).
- Details** button is highlighted with an orange arrow.
- Details pane content:**
  - Info** section: Modified Jun 20, 2022 1:34 PM, by you, Path /jennifer/Medical Records/Patient 6663.txt.
  - Permissions** section: Standard file permissions.
  - Share** section: Not shared.
  - Versions** section: Version 1 by jenniferp 2022-Jun-20 12:57:57.
  - Retention Policy** section: A box highlights the text "This file is under effective policy 6-year expiry expiring on Jun 28, 2028 12:57 PM".

- Next select the checkbox for the file **Ins file 453.txt** and click **Details** in the details pane. Confirm that the retention policy is listed at the bottom of the details.

- f. Next, select the file **Doctor Summary.pdf**. It does not have a retention policy attached to it yet because you have not manually added an **ePHI** metadata tag yet.
- g. Click **Metadata** in the details pane.
- h. Follow the same steps you completed in **Step 4** to add the ePHI tag to the file:
  - In the **Add Metadata** drop-down list, choose **Files with ePHI** and click **Add**. **Files with ePHI** is added to the list of included metadata.
  - Check **ePHI** to indicate that the file has ePHI.

- i. Click the **Details** tab.
- j. Confirm that the retention policy is now listed at the bottom of the details.

## Step 6: Choose the retention policy in the Compliance Center

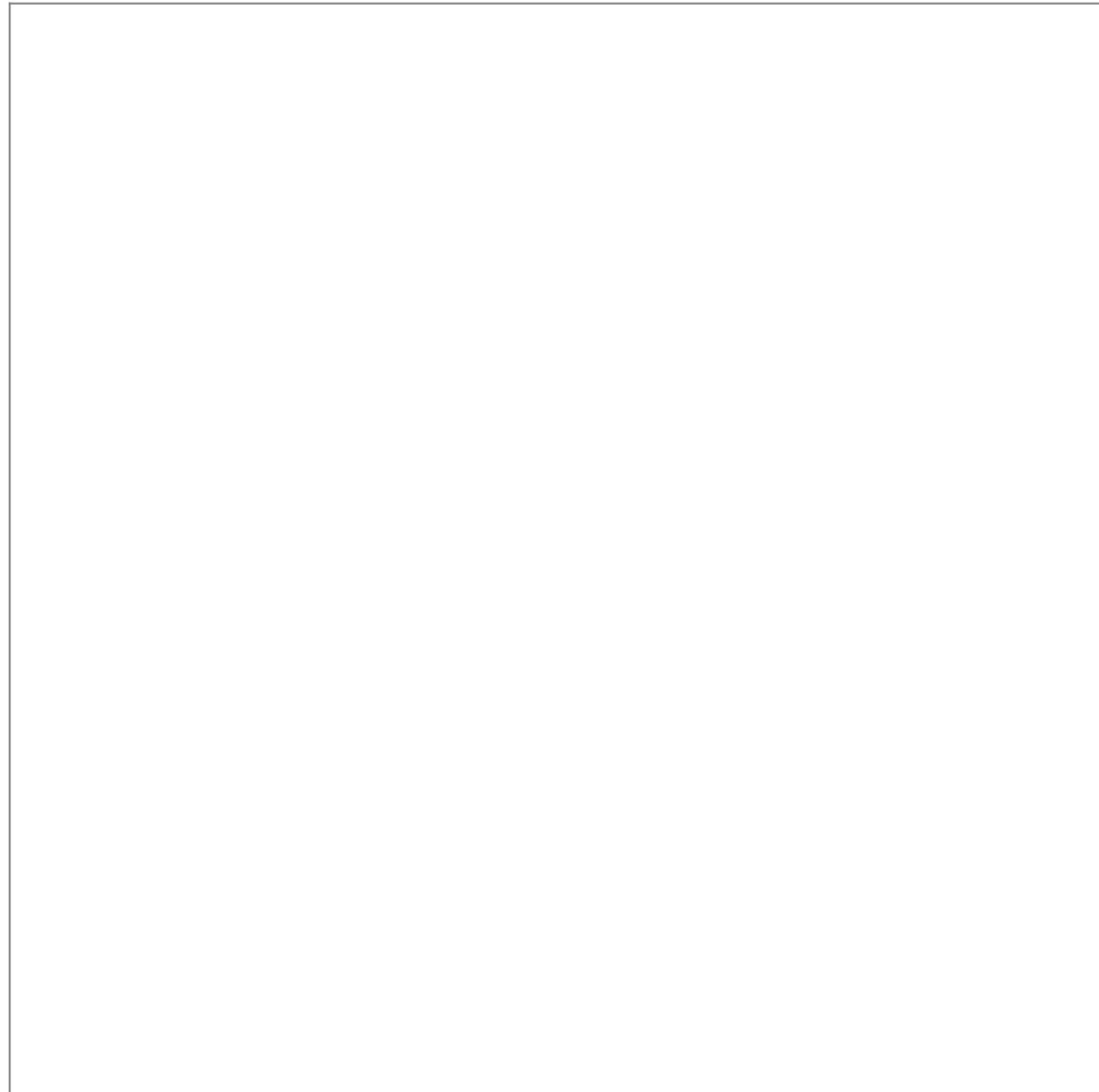
You have now reached the last step, adding the retention policy to rules in the Compliance Center as proof that you are in compliance.

To add the retention policy to compliance rules:

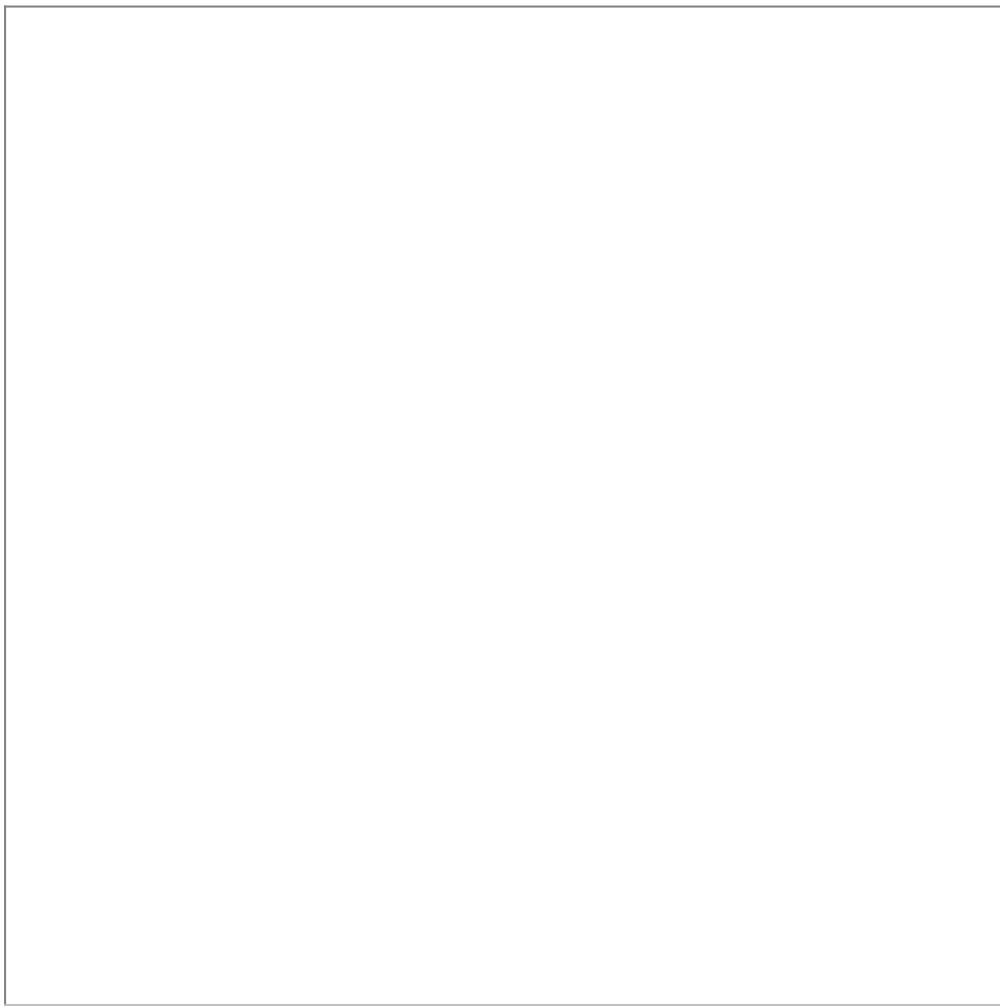
1. In the Admin portal's navigation panel, click **Compliance Center**.  
The **Compliance Center** opens.
2. To go to the **HIPAA Compliance** page, click the **HIPAA** link in the menu bar.

3. Scroll down so you can see rules **164.312(c)(1)** and **164.316(b)(2)(i)**.

You enabled them in Step 1, but since there were no retention policies that you could associate with them, they both fail.

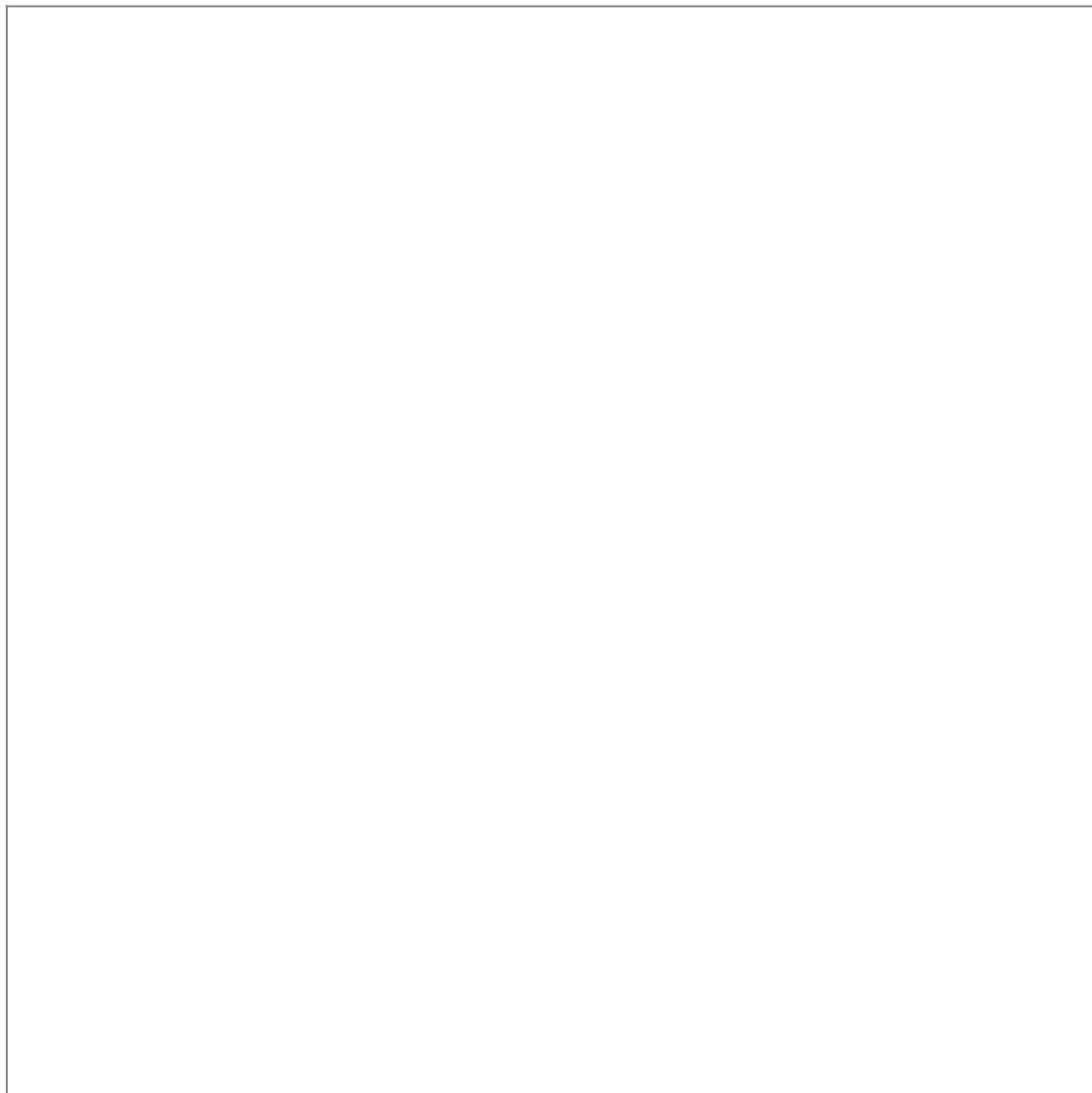


4. Click the edit button for rule **164.312 (c) (1)**.  
The **Rule Update** dialog box opens.
5. In the drop-down list, choose the 6-year policy that you just created.



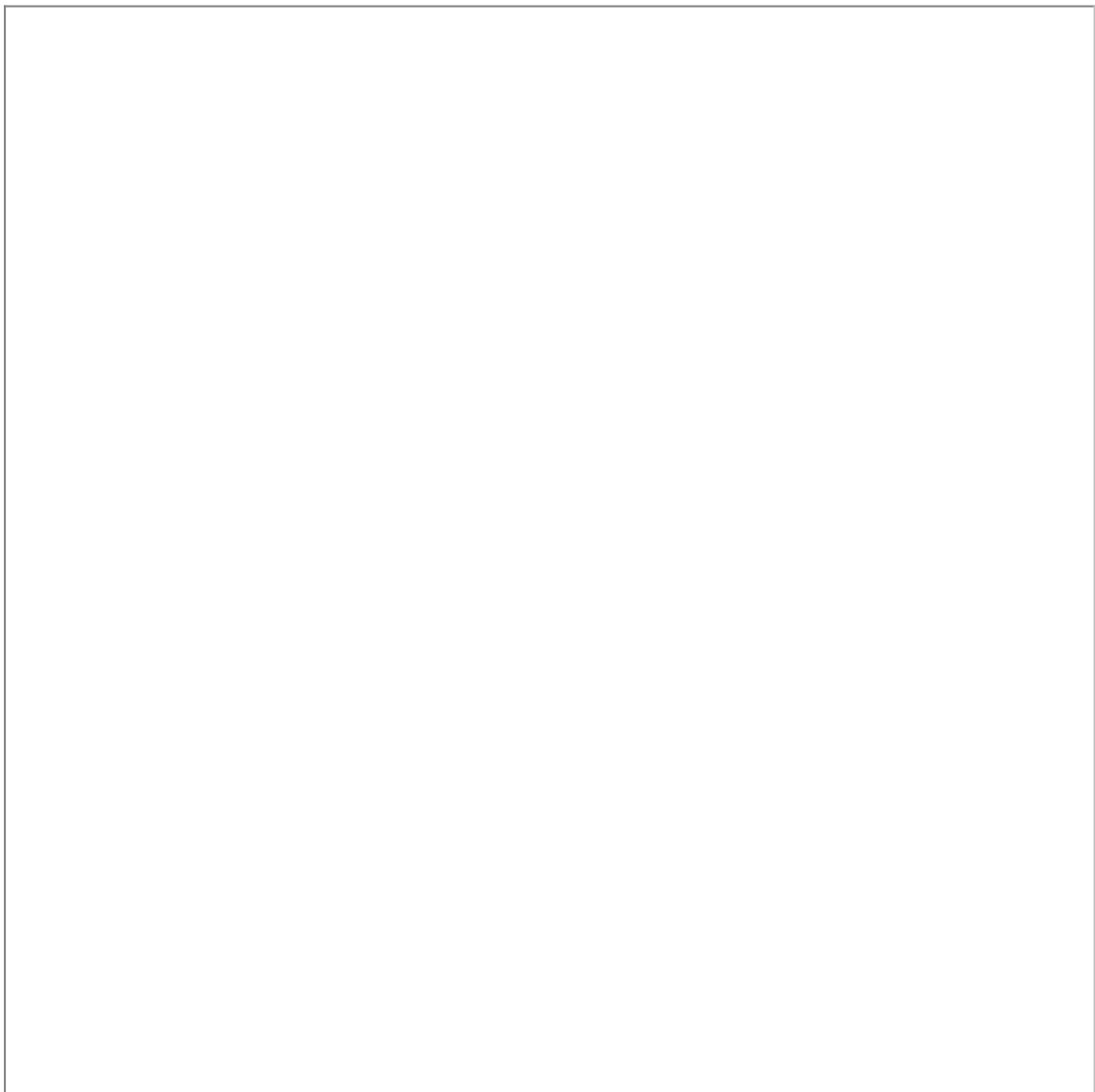
6. Click **Update**.

The rule now passes.



7. Now edit rule **164.316 (b)(2)(i)**, and choose the same retention policy.

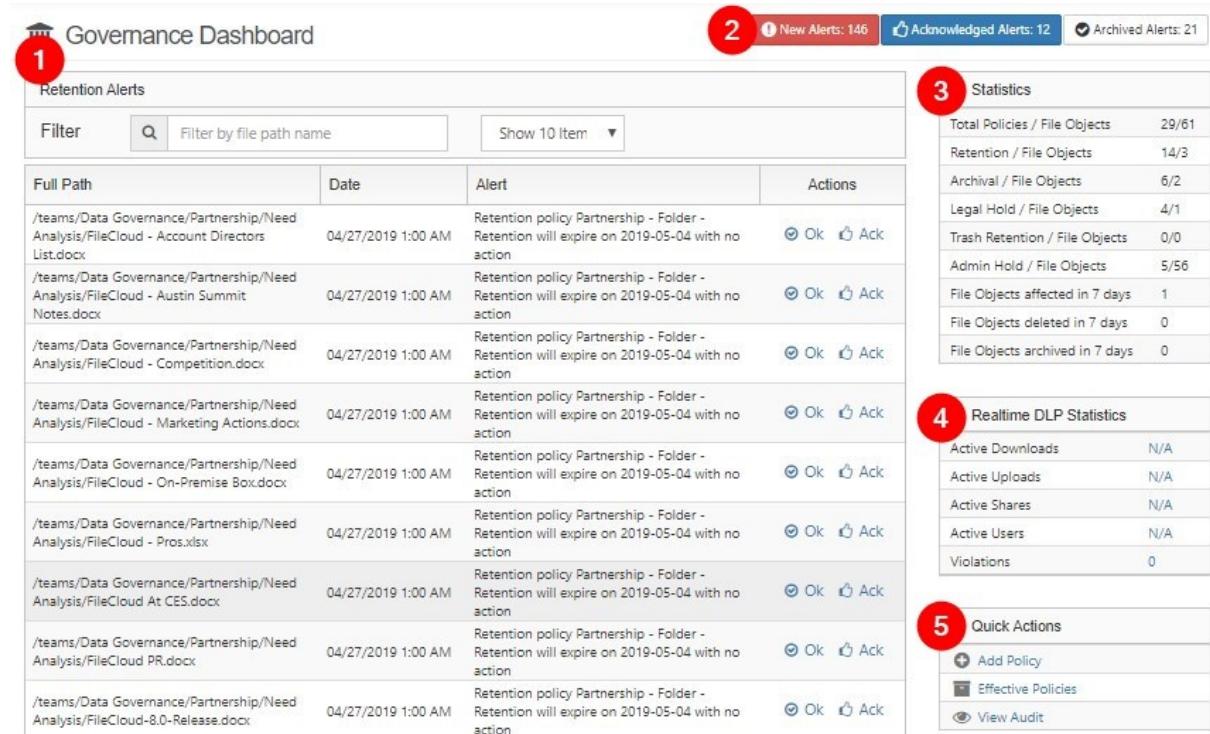
Both rules now pass:



By creating and applying the 6-year retention policy and selecting it for the two requirements, you have demonstrated that you are in compliance with the two rules, which now indicate that you have passed.

# Monitor Retention and DLP: The Governance Dashboard

The Governance Dashboard displays retention alerts as well as retention and DLP statistics to help you keep track of [retention policies](#) (see page 47) and violations of [DLP rules](#) (see page 188).



The screenshot shows the Governance Dashboard with the following sections:

- 1 Retention Alerts:** A table listing retention alerts for various files and folders. Each row includes the full path, date, alert details, and action buttons (Ok, Ack).
- 2 Alert type buttons:** Buttons for New Alerts (146), Acknowledged Alerts (12), and Archived Alerts (21).
- 3 Statistics:** A table showing retention statistics across different categories.
- 4 Realtime DLP Statistics:** A table showing active DLP violations.
- 5 Quick Actions:** Buttons for Add Policy, Effective Policies, and View Audit.

Retention Alerts			
Full Path	Date	Alert	Actions
/teams/Data Governance/Partnership/Need Analysis/FileCloud - Account Directors List.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud - Austin Summit Notes.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud - Competition.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud - Marketing Actions.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud - On-Premise Box.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud - Pros.xlsx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud At CES.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud PR.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack
/teams/Data Governance/Partnership/Need Analysis/FileCloud 8.0-Release.docx	04/27/2019 1:00 AM	Retention policy Partnership - Folder - Retention will expire on 2019-05-04 with no action	<input checked="" type="button"/> Ok <input type="button"/> Ack

Statistics	
Total Policies / File Objects	29/61
Retention / File Objects	14/3
Archival / File Objects	6/2
Legal Hold / File Objects	4/1
Trash Retention / File Objects	0/0
Admin Hold / File Objects	5/56
File Objects affected in 7 days	1
File Objects deleted in 7 days	0
File Objects archived in 7 days	0

Realtime DLP Statistics	
Active Downloads	N/A
Active Uploads	N/A
Active Shares	N/A
Active Users	N/A
Violations	0

Quick Actions	
<input type="button"/> Add Policy	
<input type="button"/> Effective Policies	
<input type="button"/> View Audit	

<b>1) Retention Alerts</b>	Lists current alerts for files and folders that have retention policies added to them. To the right of an alert:
	<ul style="list-style-type: none"> <li>Click <b>OK</b> to archive the alert and move it to the <b>Archived Alerts</b> listing.</li> <li>Click <b>Ack</b> to acknowledge the alert and move it to the <b>Acknowledged Alerts</b> listing.</li> </ul>
<b>2) Alert type buttons</b>	Clicking each button displays a list of the alert type ( <b>New</b> , <b>Acknowledged</b> , or <b>Archived</b> ) in the <b>Retention Alerts</b> table.
<b>3) Statistics</b>	Statistics of : <ul style="list-style-type: none"> <li>Number of retention policies of each type and how many files and folders they are added to.</li> <li>Number of files and folders receiving a certain action in the last 7 days.</li> </ul>
<b>4) Realtime DLP Statistics</b>	DLP violations occurring currently.
<b>5) Quick Actions</b>	<b>Add Policy</b> - Add a retention policy, and apply it to files and folders. <b>Effective Policies</b> - View a list of retention policies and the files and folders they affect. <b>View Audit</b> - View system audit logs. Defaults to displaying retention audit logs.

## Secure Web Viewer for DRM



The Secure Web Viewer (Beta version) is available in FileCloud versions 23.232 and later.

Note: The Secure Web Viewer is not included with some licenses, such as the FileCloud Community Edition license and the FileCloud Essentials license.

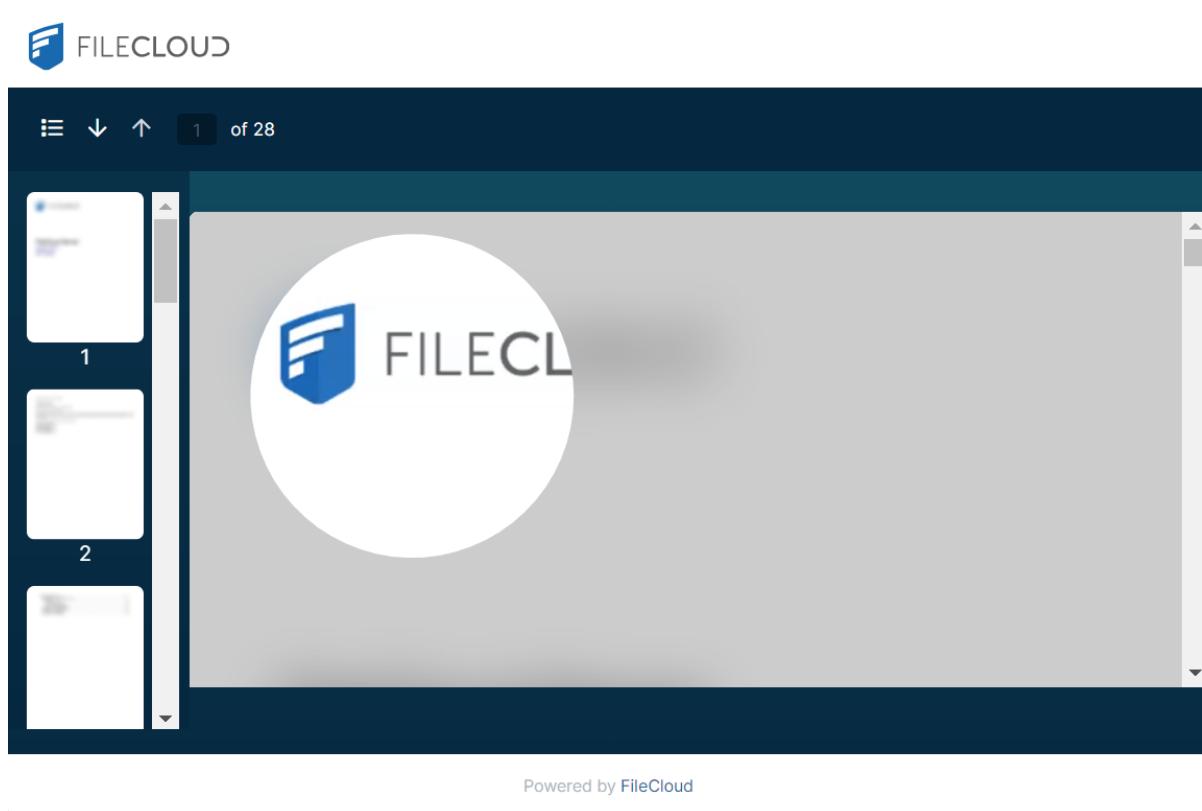
Users have the ability to publicly or privately share certain file types (jpg, png, pdf, docx, and pptx) with the protection of digital rights management (DRM) by requiring them to be viewed through FileCloud's Secure Web Viewer. The Secure Web Viewer requires public share recipients to enter a password to view the share. It can also limit access in other ways for both private and public shares, such as only permitting small portions of the file to be viewed at a time.



FileCloud's Secure Web Viewer for viewing securely shared files is not the same as FileCloud's Secure Document Viewer for viewing securely exported files. The Secure Document Viewer is a stand-alone app, while the Secure Web Viewer is web-based, and open to further refinement based on user input.

Only files of 20MB or less can be viewed through the Secure Web Viewer.

For more information about how a Secure Web Viewer share is created, see [Public File Sharing with Secure Web Viewer Protection](#) and [Private File Sharing with Secure Web Viewer Protection](#).



File viewed through the Secure Web Viewer with limited view (partial file viewing) enabled.

## The Secure Web Viewer option

When **Enable WebDRM** is enabled, an option for creating public or private shares that must be viewed through the Secure Web Viewer is available in the **Share link** dialog box for jpg, png, pdf, docx, and pptx files of 20 MB or less. For other file types and files greater than 20 MB, the option appears

disabled.

Share Link

https:// /url/sitky5rhpktpaj Modify Link

Shared File  
/jennifer/estate documents/Example 2.docx

Share Options Share History

Share Name: 9hk6AMCPNw5eXNzB Change

Expires: Never Expires Change

Sharing Permissions:

- Allow anyone with link
- Allow anyone with link and a password
- Allow selected users or groups
- Secure Web Viewer
  - Allow selected users or groups

This share is password protected public share with enhanced protection. Only users with the secure web viewer link and password can access.

Password:  Save

Enable Protected View

Max Access Time:  Unlimited  Limited

Remove Share OK

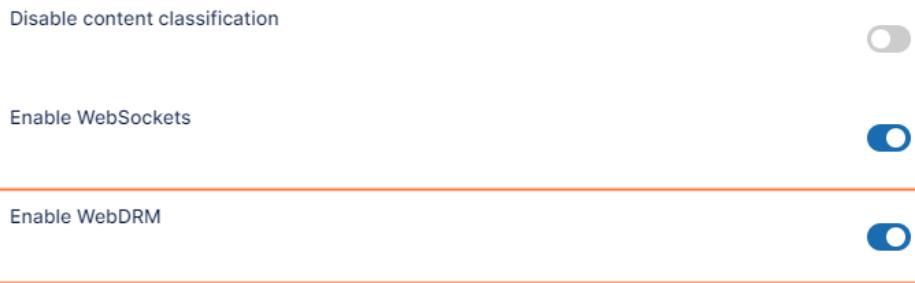
## Prerequisites for use of the Secure Web Viewer:

1. The **Enable WebDRM** option in the Misc settings page is enabled. Note that it is enabled by default; if it has been disabled, see the steps to re-enable it below.
2. A valid SSL connection is configured.
3. Document Preview is installed.  
For Windows installation, see [Installing and Running Document Converter for Windows](#).  
For Linux installation, see [LibreOffice Ubuntu/RHEL Instructions](#).

## To disable/re-enable use of the Secure Web Viewer option:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Misc** . By default, **General** settings are opened.

2. Scroll down to the setting **Enable WebDRM** and disable or re-enable it.



3. Click **Save**.