FileCloud Server Version 23.252

Governance Setup

Printed on 10/08/2025

Copyright Notice

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

FileCloud

Phone: U.S: +1 (888) 571-6480

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

Governance in FileCloud

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

Import/Export DLP, CCE, and Metadata Settings

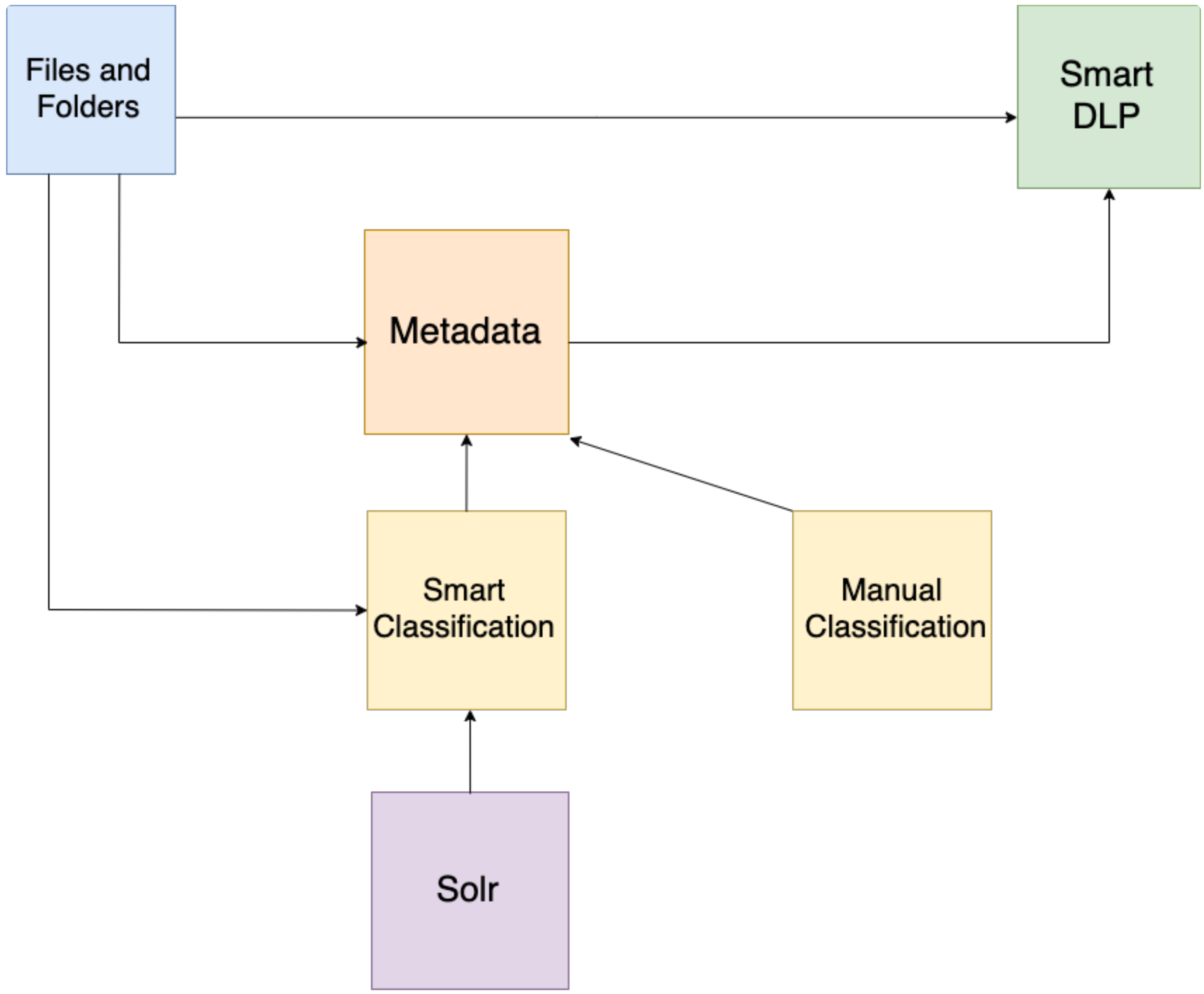
Example: Setting Up a Retention Policy to meet HIPAA Requirements

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.

> ℹ 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” 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.

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

Learn more about Smart DLP.

Compliance

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.

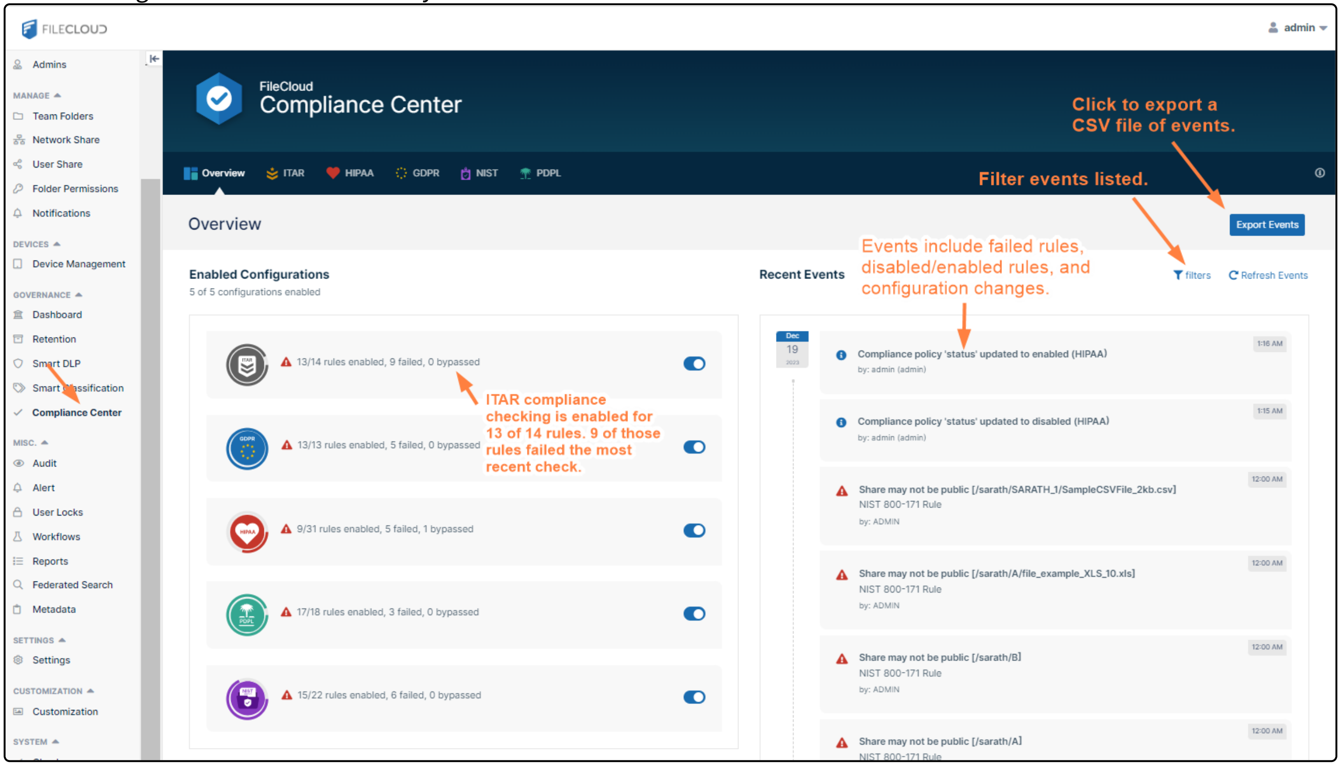
The Compliance Center

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.



Overview

Enabled Configurations

5 of 5 configurations enabled

13/14 rules enabled, 9 failed, 0 bypassed

13/13 rules enabled, 5 failed, 0 bypassed

9/31 rules enabled, 5 failed, 1 bypassed

17/18 rules enabled, 3 failed, 0 bypassed

15/22 rules enabled, 6 failed, 0 bypassed

Recent Events

Compliance policy 'status' updated to enabled (HIPAA)
by: admin (admin)
1:16 AM

Compliance policy 'status' updated to disabled (HIPAA)
by: admin (admin)
1:15 AM

Share may not be public [/sarath/SARATH_1/SampleCSVFile_2kb.csv]
NIST 800-171 Rule
by: ADMIN
12:00 AM

Share may not be public [/sarath/A/file_example_XLS_10.xls]
NIST 800-171 Rule
by: ADMIN
12:00 AM

Share may not be public [/sarath/B]
NIST 800-171 Rule
by: ADMIN
12:00 AM

Share may not be public [/sarath/A]
NIST 800-171 Rule
12:00 AM

Click to export a CSV file of events.

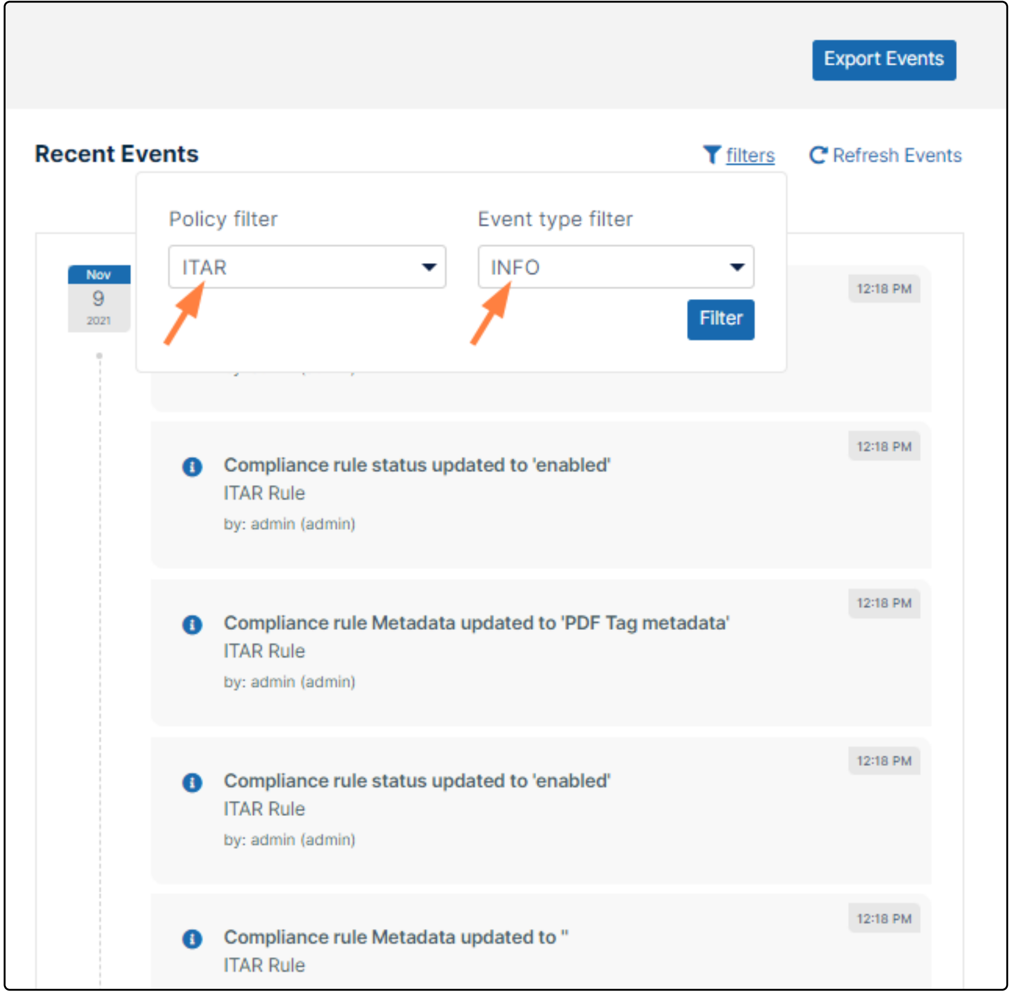
Filter events listed.

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

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

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.



Policy filter: ITAR

Event type filter: INFO

12:18 PM
Compliance rule status updated to 'enabled'
ITAR Rule
by: admin (admin)

12:18 PM
Compliance rule Metadata updated to 'PDF Tag metadata'
ITAR Rule
by: admin (admin)

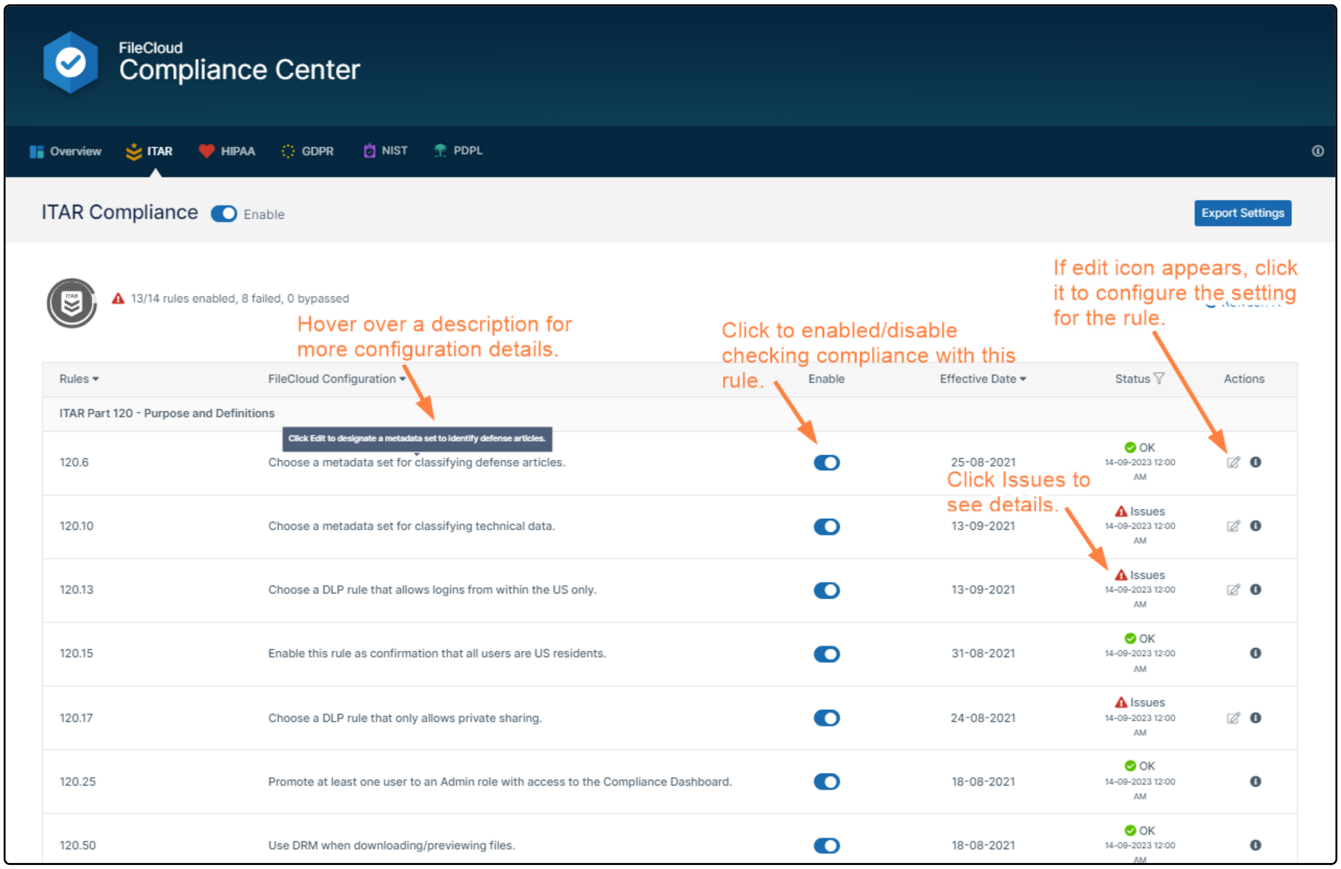
12:18 PM
Compliance rule status updated to 'enabled'
ITAR Rule
by: admin (admin)

12:18 PM
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.


FileCloud
Compliance Center
Overview
ITAR
HIPAA
GDPR
NIST
PDPL
ITAR Compliance
Enable
Export Settings
Hover over a description for more configuration details.
Click to enabled/disable checking compliance with this rule.
If edit icon appears, click it to configure the setting for the rule.
Click Issues to see details.

13/14 rules enabled, 8 failed, 0 bypassed

Rules	FileCloud Configuration	Enable	Effective Date	Status	Actions
ITAR Part 120 - Purpose and Definitions					
120.6	Click Edit to designate a metadata set to identify defense articles. Choose a metadata set for classifying defense articles.	●	25-08-2021	✓ OK 14-09-2023 12:00 AM	✎ ⓘ
120.10	Choose a metadata set for classifying technical data.	●	13-09-2021	⚠ Issues 14-09-2023 12:00 AM	✎ ⓘ
120.13	Choose a DLP rule that allows logins from within the US only.	●	13-09-2021	⚠ Issues 14-09-2023 12:00 AM	✎ ⓘ
120.15	Enable this rule as confirmation that all users are US residents.	●	31-08-2021	✓ OK 14-09-2023 12:00 AM	ⓘ
120.17	Choose a DLP rule that only allows private sharing.	●	24-08-2021	⚠ Issues 14-09-2023 12:00 AM	✎ ⓘ
120.25	Promote at least one user to an Admin role with access to the Compliance Dashboard.	●	18-08-2021	✓ OK 14-09-2023 12:00 AM	ⓘ
120.50	Use DRM when downloading/previewing files.	●	18-08-2021	✓ OK 14-09-2023 12:00 AM	ⓘ

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.

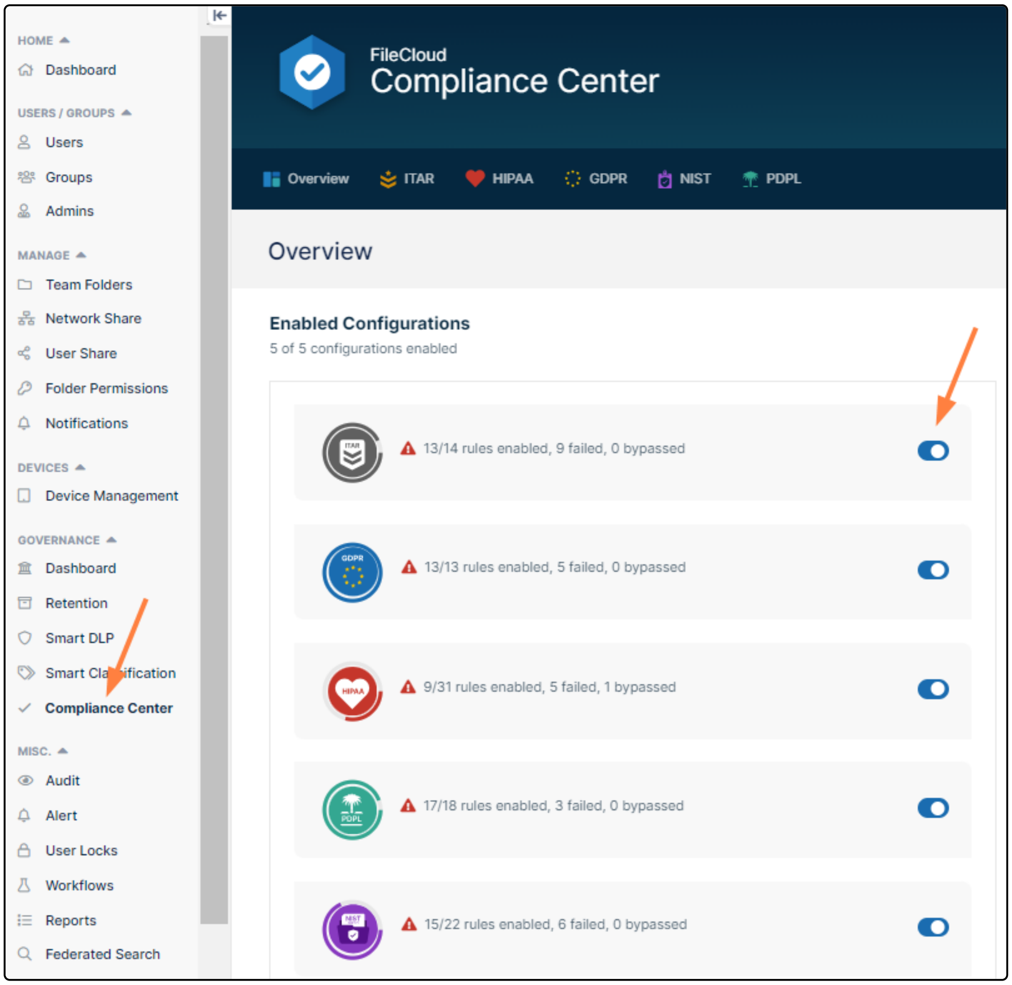
How to set up and check compliance

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.



Overview

Enabled Configurations

5 of 5 configurations enabled

13/14 rules enabled, 9 failed, 0 bypassed

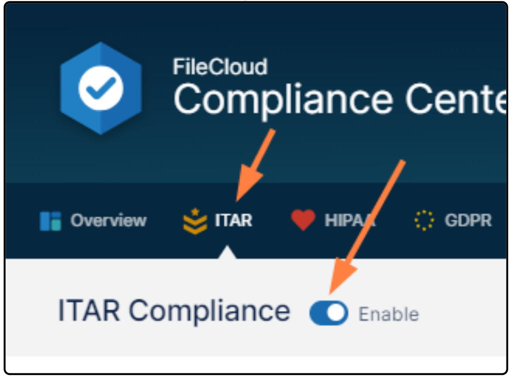
13/13 rules enabled, 5 failed, 0 bypassed

9/31 rules enabled, 5 failed, 1 bypassed

17/18 rules enabled, 3 failed, 0 bypassed

15/22 rules enabled, 6 failed, 0 bypassed

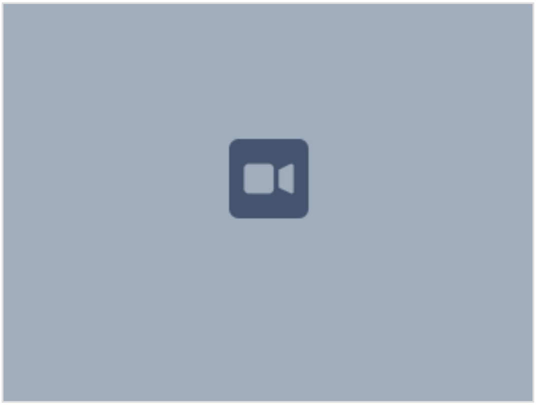
Or:
Click the tab for a compliance, and click the slider at the top of the screen.



ITAR Compliance

Enable or disable compliance checking for a rule:

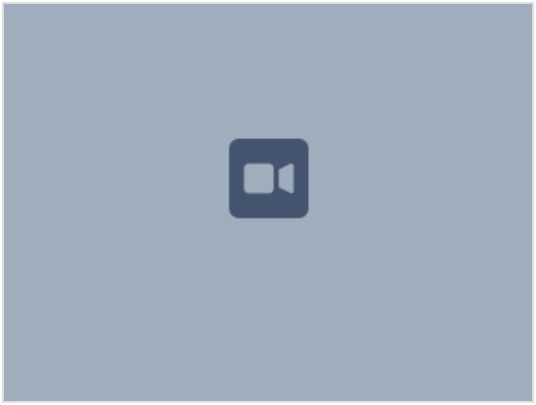
After checking has been enabled for a specific compliance, you can enable or disable checking for each of its rules by toggling the slider to the rule's right. Notice that compliance status is checked as soon as you enable the rule.



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.

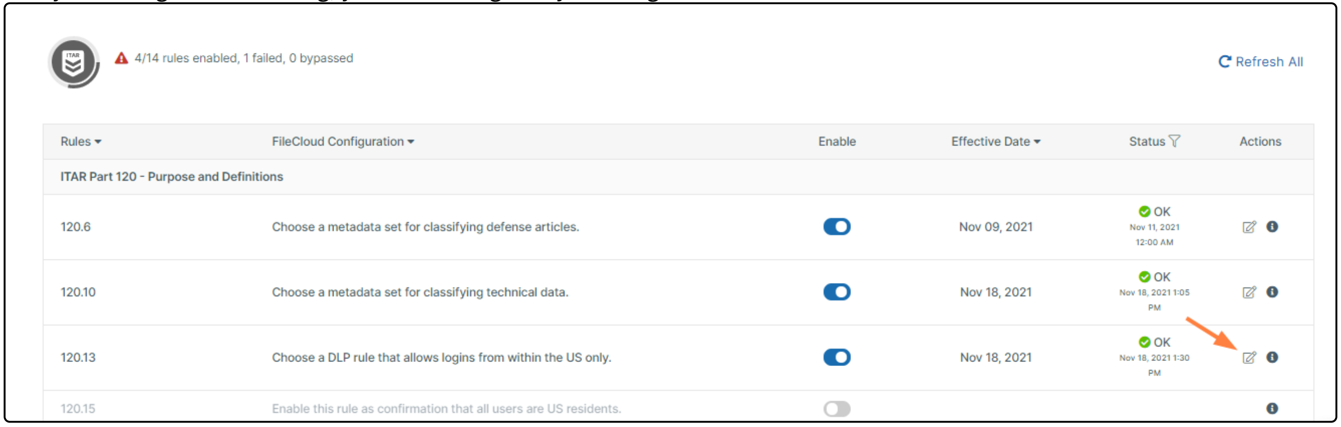


2) Configure Compliance Settings

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:



4/14 rules enabled, 1 failed, 0 bypassed

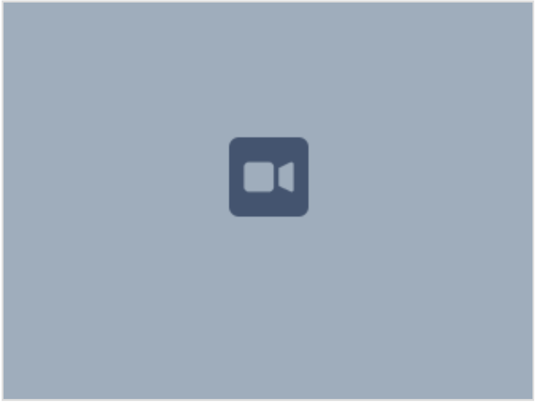
Refresh All

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

Compliance settings you must configure outside the Compliance Center

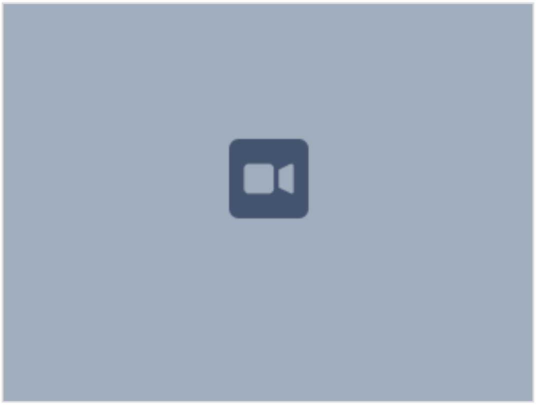
For many rules, you must navigate to other pages in FileCloud and configure settings. The compliance tool will verify that the settings are configured correctly when you enable the rule.

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



Rules you can mark as compliant

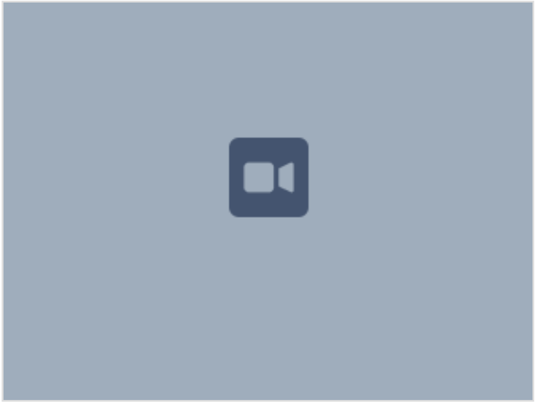
Some rules only need your verification that you are complying with them. Simply enable the rule to confirm that you have complied.



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 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.**

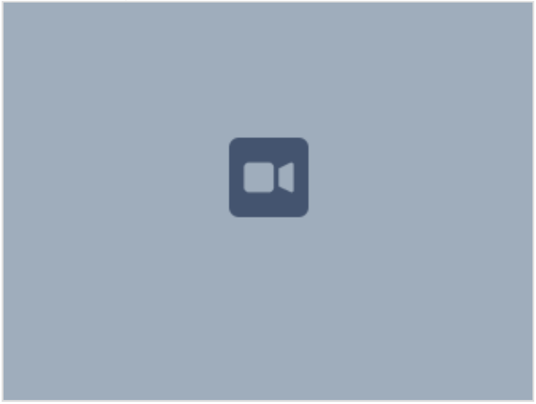


3) Run compliance checks

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**.

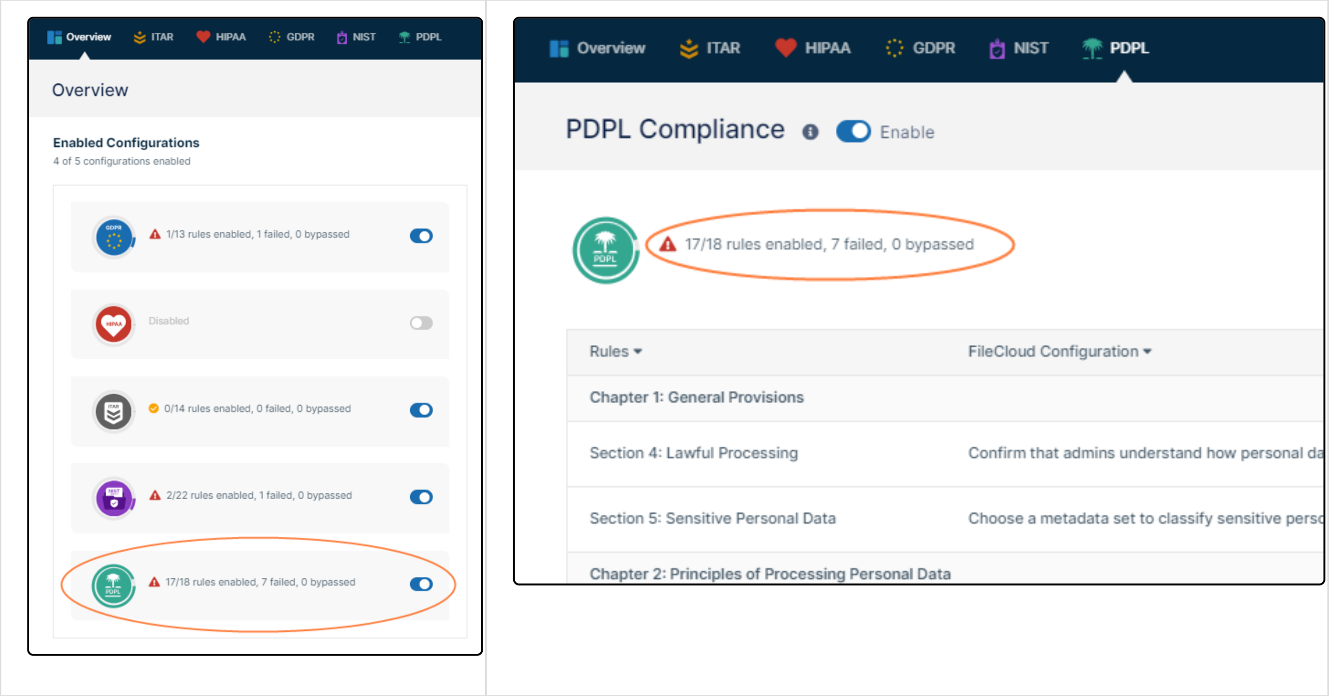


4) Review compliance status

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.



Overview

Enabled Configurations

4 of 5 configurations enabled

1/13 rules enabled, 1 failed, 0 bypassed

Disabled

0/14 rules enabled, 0 failed, 0 bypassed

2/22 rules enabled, 1 failed, 0 bypassed

17/18 rules enabled, 7 failed, 0 bypassed

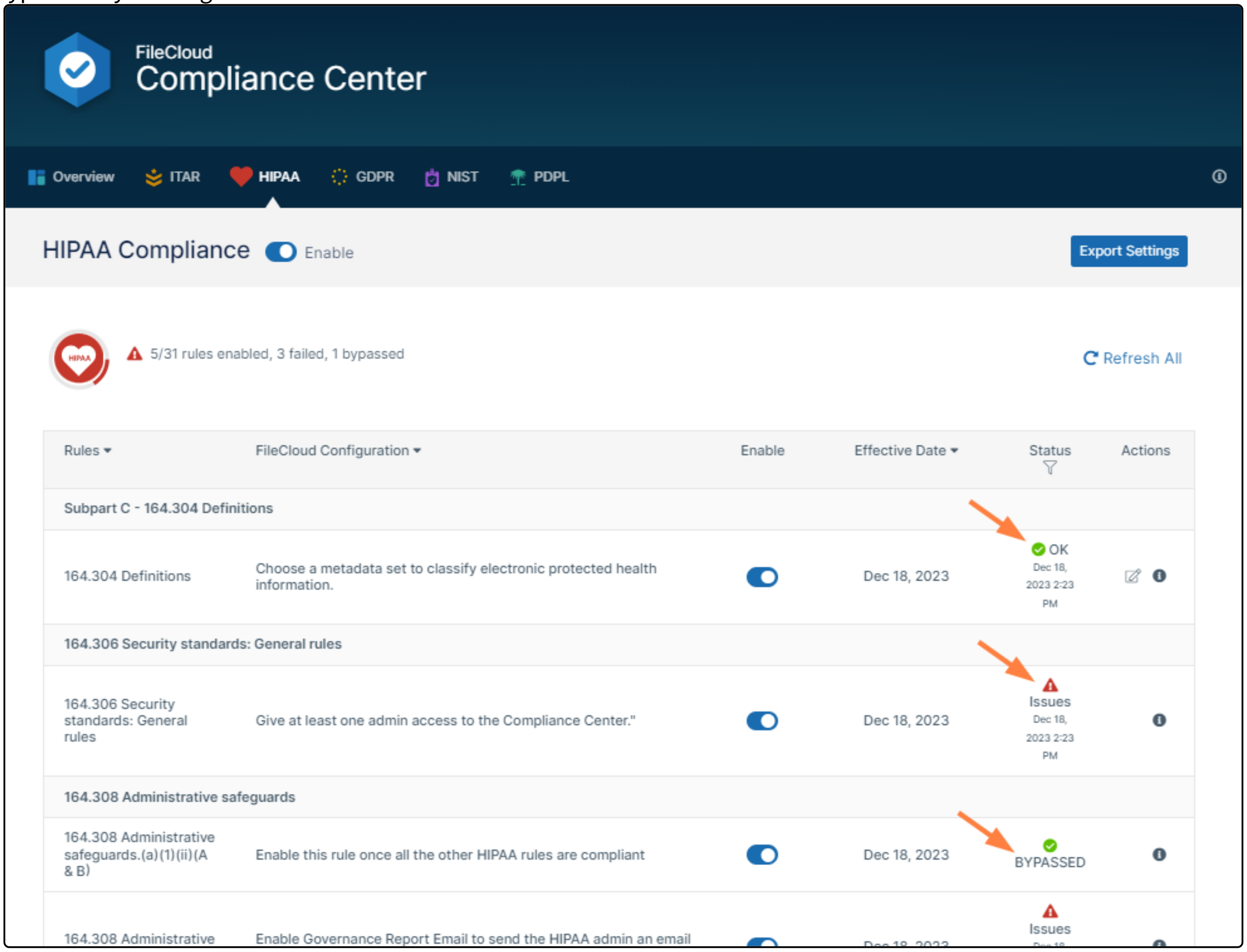
PDPL Compliance ● Enable

17/18 rules enabled, 7 failed, 0 bypassed

Rules ▾	FileCloud Configuration ▾
Chapter 1: General Provisions	
Section 4: Lawful Processing	Confirm that admins understand how personal da
Section 5: Sensitive Personal Data	Choose a metadata set to classify sensitive perso
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**.



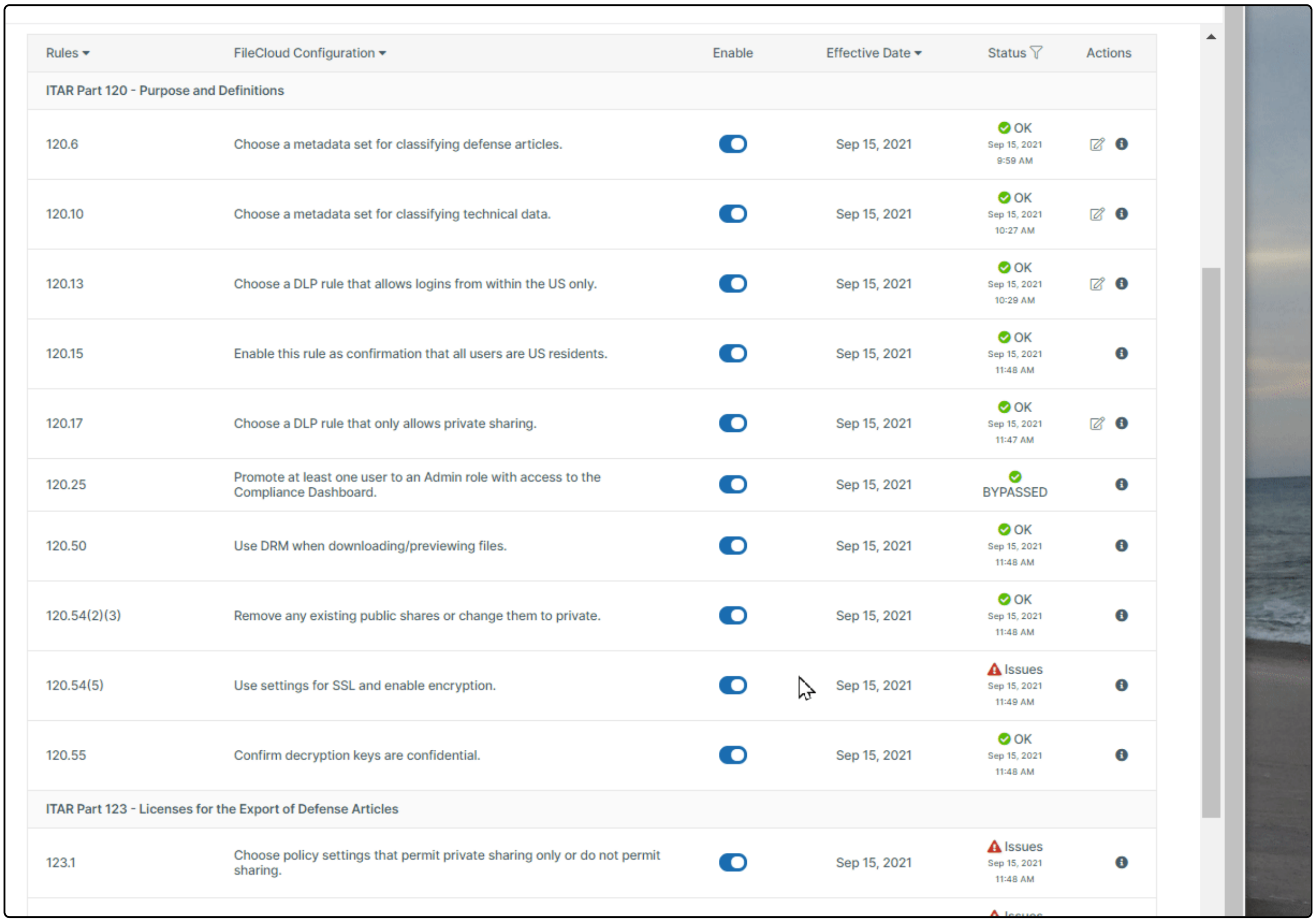
HIPAA Compliance

5/31 rules enabled, 3 failed, 1 bypassed

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.	●	Dec 18, 2023	OK 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."	●	Dec 18, 2023	Issues 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	●	Dec 18, 2023	BYPASSED	
164.308 Administrative	Enable Governance Report Email to send the HIPAA admin an email	●	Dec 18, 2023	Issues	

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.

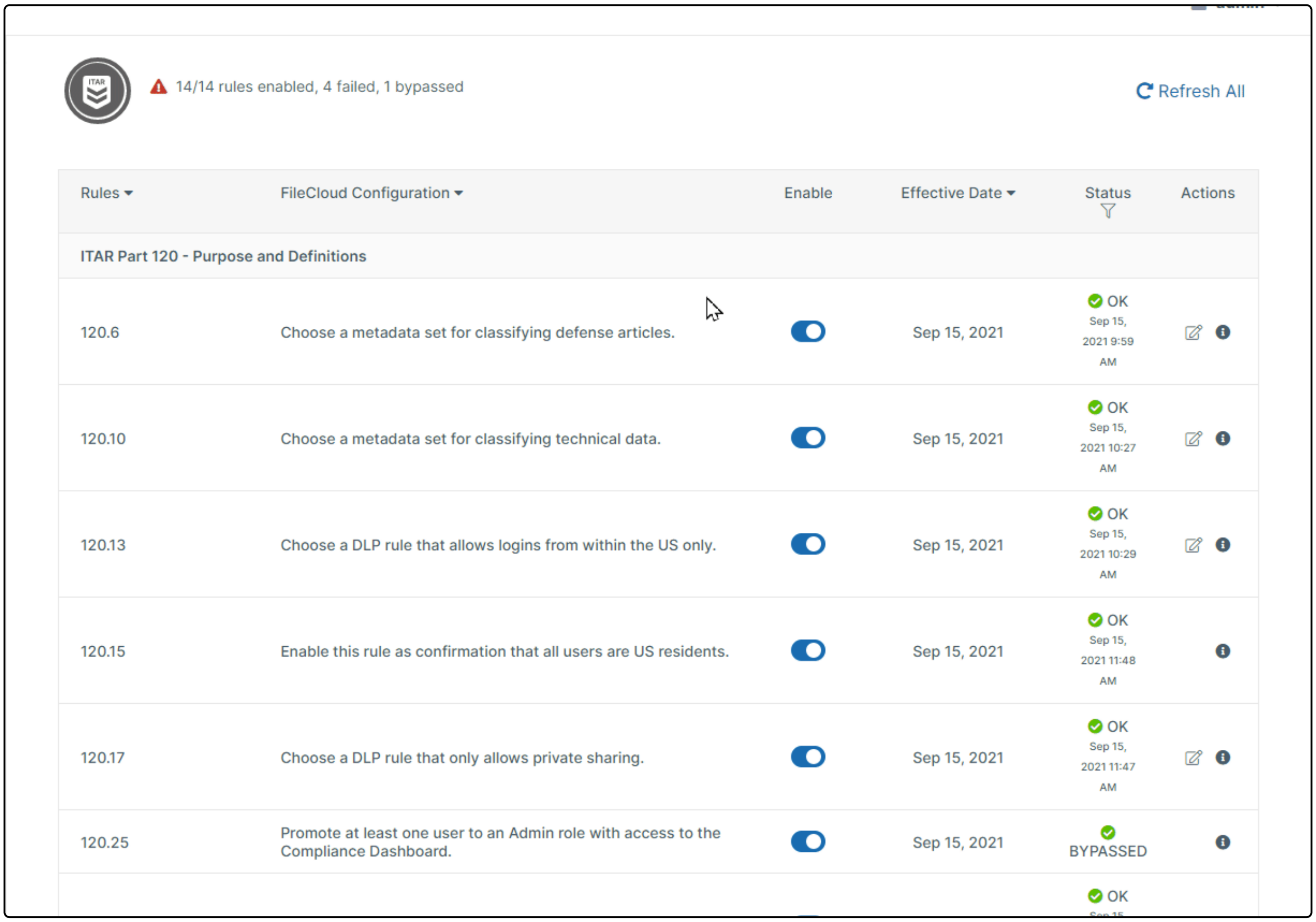


Rules ▾	FileCloud Configuration ▾	Enable	Effective Date ▾	Status ▽	Actions
ITAR Part 120 - Purpose and Definitions					
120.6	Choose a metadata set for classifying defense articles.	●	Sep 15, 2021	✓ OK Sep 15, 2021 9:59 AM	✎ ⓘ
120.10	Choose a metadata set for classifying technical data.	●	Sep 15, 2021	✓ OK Sep 15, 2021 10:27 AM	✎ ⓘ
120.13	Choose a DLP rule that allows logins from within the US only.	●	Sep 15, 2021	✓ OK Sep 15, 2021 10:29 AM	✎ ⓘ
120.15	Enable this rule as confirmation that all users are US residents.	●	Sep 15, 2021	✓ OK Sep 15, 2021 11:48 AM	ⓘ
120.17	Choose a DLP rule that only allows private sharing.	●	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.	●	Sep 15, 2021	✓ BYPASSED	ⓘ
120.50	Use DRM when downloading/previewing files.	●	Sep 15, 2021	✓ OK Sep 15, 2021 11:48 AM	ⓘ
120.54(2)(3)	Remove any existing public shares or change them to private.	●	Sep 15, 2021	✓ OK Sep 15, 2021 11:48 AM	ⓘ
120.54(5)	Use settings for SSL and enable encryption.	●	Sep 15, 2021	⚠ Issues Sep 15, 2021 11:49 AM	ⓘ
120.55	Confirm decryption keys are confidential.	●	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.	●	Sep 15, 2021	⚠ Issues Sep 15, 2021 11:48 AM	ⓘ
				⚠ Issues	

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.



14/14 rules enabled, 4 failed, 1 bypassed

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

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

Guide to ITAR Rules in the Compliance Center

Guide to GDPR Rules in the Compliance Center

Guide to NIST Rules in the Compliance Center

Guide to PDPL Rules in the Compliance Center

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
164.304 Definitions	Identify which files have electronically protected health information (ePHI).	In the Compliance Center, click the Edit button for the rule, and select a metadata set with a tag that identifies ePHI files. (To carry out compliance, you must use smart classification to apply the metadata tag to ePHI files.)	If the metadata set exists and is enabled, status is **OK**; if not, status is **Issues**.
164.306 Security standards: General rules	Allow at least one user access to the Compliance system.	To enable at least one user to manage the Compliance Center: 1. Go to **Admins** and create a role with **Compliance** access to the Compliance Center. 2. In **Admins**, add at least one user to the role with access to the Compliance Center.	If one or more Admin users have access to the Compliance Center, status is **OK**; if not, status is **Issues**.
164.308 Administrative safeguards. (a)(1)(ii)(A & B)	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 **OK** then the status of this rule **OK**; if not, status is **Issues**.
164.308 Administrative safeguards. (a)(1)(ii)(D)	Implement a procedure to regularly review system activity records.	In **Settings > Admin**, enable **Send daily governance report to admin**.	If the **Send daily governance report to admin** setting is enabled, status is **OK**; if not, status is **Issues**.
164.308 Administrative safeguards.(a)(3)(ii)(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 GeoIP is not disabled, status is **OK**; otherwise, status is **Issues**.
164.308 Administrative safeguards.(a)(5)(ii)(B)	Configure antivirus protection against malicious file uploads.	1. Go to **Settings > Third Party Integration > Antivirus.** 2. Configure an Antivirus.	If an **Antivirus** is configured, status is **OK**; if not, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
164.308 Administrative safeguards .(a)(5)(ii)(C)	Monitor log-in attempts.	1. Go to **Settings > Admin**. 2. Set **Audit Log Level** to **REQUEST** or **FULL**.	If **Audit Log Level** is **REQUEST** or **FULL** status is **OK**; if **Audit Log Level** is **OFF**, status is **Issues**.
164.308 Administrative safeguards .(a)(5)(ii)(D)	Set up password management procedures.	1. Go to **Settings > Misc > Password**. 2. Configure the settings as follows: - Set **Minimum password length** to 8 or more. - Enable **Enable strong passwords**. - Enable **Disallow commonly used passwords**. - Set **User password expiration in days** to a value greater than 0. - Set **Number of previous passwords that cannot be reused** to a value greater than 0. - Set **Reset password attempt interval** to a value greater than 0.	If the password settings are configured as indicated, status is **OK**; if not, status is **Issues**.
164.308 Administrative safeguards .(a)(6)(ii)	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
164.308 Administrative safeguards .(a)(7)(i)	Implement a contingency plan in case systems containing ePHI are damaged.	Enable this rule as confirmation that you have done the following: 1. Go to **Settings > Misc > General**. 2. Disable **Database backup interval** option should be disabled (by default it is disabled). 3. Set **Database backup interval** to **daily**. 4. Backup of the managed storage location should be planned and maintained by your team.	None
164.308 Administrative safeguards .(a)(7)(ii)(B)	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

Rule (click to see text)	Description	Steps for complying	Validation
164.308 Administrative safeguards .(a)(7)(ii)(C)	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)	Implement policies and procedures to only allow access to ePHI to people and programs with access rights.	To prevent data from being shared with unauthorized users: 1. For each policy, go to **Settings > Policies** and click the **General** tab. Set **Share Mode** to either **Allow Private Shares Only** or **Shares Not Allowed**. 2. Remove any existing public shares, or change them to private.	If **Share Mode** is **Allow All Shares** or any public shares exist, status is **Issues**.
164.312 Technical safeguards .(a)(2)(i)	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)	Terminate sessions after a certain amount of time automatically.	To confirm automatic logoff of sessions: - Go to **Settings > Server**, and set **Session Timeout** to a value greater than 0.	If **Session Timeout** is set to 0 or empty, status is **Issues**.
164.312 Technical safeguards .(a)(2)(iv)	Implement encryption and decryption of ePHI.	To set up ePHI encryption: 1. Configure storage encryption. See Setting Up Managed Storage Encryption. 2. Go to **Settings > Storage > Managed Storage** and click **Manage** next to **Encryption**; then enable encryption. 3. Encrypt all existing files.	If storage is not fully encrypted, or any existing files are not fully encrypted, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
164.312 Technical safeguards .(b)	Set up audit controls.	To implement audit controls: - Go to **Settings > Admin**, and configure the following: - **Audit Log Level** - Set to to **REQUEST** or **FULL**. - **Auto Archive Audit Database** - Enable. - **Auto Archive Records Frequency (in days)** - Enter a value. - **Storage Path For Archived Audit Records** - Enter a valid path.	If any of the audit settings is not set as specified, status is **Issues**.
164.312 Technical safeguards .(c)(1)	Protect ePHI files from destruction.	To protect ePHI files and folders from deletion: - Click the Edit button, and select a retention policy to protect ePHI files and folders from deletion based on metadata.	If the retention policy exists and is enabled, status is **OK**; if not, or if modifications to the retention policy allow file or folder deletion, status is **Issues**.
164.312 Technical safeguards .(d)	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)	Guard against unauthorized access of ePHI that is being transmitted.	To guard against unauthorized access to ePHI: 1. Click the Edit button, and select a DLP rule that blocks public shares. 2. Change any existing public shares to private.	If the DLP rule exists and is enabled and there are no existing public shares, status is **OK**; if not, or if modifications to the rule allow public shares, status is **Issues**.
164.312 Technical safeguards .(e)(2)(i)	Ensure that transmitted ePHI is not modified.	To confirm that users are educated about sharing permissions and folder level permissions, enable this rule.	None

Rule (click to see text)	Description	Steps for complying	Validation
164.316 Policies and procedures and documentation requirements.(b)(2)(i)	Retain files for 6 years.	To retain files for 6 years: - Click the Edit button, and select a retention policy to retain files for 6 years based on metadata. (The selected retention policy must have it's expiry set to 2192 days (6 years with 2 leap years) and must not renew on expiry.)	If the retention policy exists and is enabled, status is **OK**; if not, status is **Issues**.
164.316 Policies and procedures and documentation requirements.(b)(2)(ii)	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)	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 **Issues**.
164.404 Notification to individuals. (b)	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

Rule (click to see text)	Description	Steps for complying	Validation
164.502 Uses and disclosures of protected health information: General rules.(a)(1)	Allow users to use and disclose ePHI according to regulations.	To prevent data from being shared with non-associates without proper permission: 1. Go to **Settings > Policies**, and edit each policy. a. On the **General** tab, set **Share Mode** to either **Allow Private Shares Only** or **Shares Not Allowed**. b. Remove any existing public shares or change them to private.	If **Share Mode** is **Allow All Shares** or any public shares exist, status is **Issues**.
164.504 Uses and disclosures: Organizational requirements.(e)(1)	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)	At the termination of a contract, all info shared with business associate should be destroyed or returned.	To confirm return or destruction of ePHI at the termination of contracts: - Go to **Settings > Misc > Share** and configure these settings: - **Remove Expired Shares** - enable. - **Delete Files from Expired Shares** - enable.	If all the settings are as specified, status is **OK**; if not, status is **Issues**.
164.508 Uses and disclosures for which an authorization is required.(a)	Uses of ePHI requiring authorization.	To implement authorization for use and disclosures of ePHI: - Click the Edit button, and select a DLP rule that restricts sharing.	If the DLP rule exists and is enabled, status is **OK**; if not, or if modifications to the rule allow public shares, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
164.522 Rights to request privacy protection for protected health information. (a)(1)	Right of individual to request restriction of disclosure of their ePHI.	To implement the right of an individual to request restriction of uses and disclosures of ePHI: 1. Go to **Settings > Misc > General**. 2. If **Disable Locking** is enabled, disable it, and save.	If Disable Locking is unchecked, status is **OK**; if not, status is **Issues**.
164.528 Accounting of disclosures of protected health information.	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
120.6	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 to apply the metadata tag to defense articles.)	If the metadata set exists and is enabled, status is **OK**; if not, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
120.10	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 to apply the metadata tag to technical data.)	If the metadata set exists and is enabled, status is **OK**; If not, status is **Issues**.
120.13	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 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 **OK**; if not, or if modifications to the rule allow log in from outside the US, status is **Issues**.
120.15	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
120.17	Do not permit public sharing.	1. In the Compliance Center, click the Edit button for the rule, and select a DLP rule that blocks public shares. Only DLP rules for the SHARE action are available for selection. 2. Change any existing public shares to private.	If the DLP rule exists and is enabled and there are no existing public shares, status is **OK**; if not, or if modifications to the rule allow public shares, status is **Issues**.
120.25	Allow at least one user access to the Compliance system.	To enable at least one user to manage the Compliance Center: 1. Go to **Admins** and create a role with **Compliance** access to the Compliance Center. 2. In **Admins**, add at least one user to the role with access to the Compliance Center.	If one or more Admin users have access to the Compliance Center, status is **OK**; if not, status is **Issues**.
120.50	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 **OK**; if not, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
120.54(2)(3)	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 **Issues**.
120.54(5)	Confirm that data is only transferred between US entities.	1. In the Admin portal, go to **Settings > Server > Server URL**. Use HTTPS for the **Server URL**. 2. Configure storage encryption. See Setting up Managed Storage Encryption. 3. Go to **Settings > Storage > Managed Storage** and enable **Encryption**. 4. Encrypt all existing files.	If HTTPS is not used, storage is not fully encrypted, or any existing files are not fully encrypted, status is **Issues**.
120.55	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	Ensure that proper permission is given if data is shared with non-US entities	1. In the Admin portal, go to **Settings > Policies > General > Share Mode**, and for **Share Mode** in all policies choose either **Allow Private Shares Only** or **Shares Not Allowed**. 2. Remove any existing public shares or change them to private.	If **Share Mode** is **Allow All Shares** or any public shares exist, status is **Issues**.
123.26	Maintain records of all data shared with non-US entities	In the Admin portal, go to **Settings > Admin** and set the **Audit Log Level** to **FULL**.	If **Audit Log Level** is set to **OFF** or **REQUEST**, status is **Issues**.
126.1	Deny access to the system by prohibited countries	In the row for the rule in the Compliance Center, click the Edit button and select a DLP rule that blocks users from logging in from those countries. Only DLP rules for the LOGIN action are available for selection.	If the DLP rule exists and is enabled, status is **OK**; if not, or if modifications to the rule allow log in from those countries, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
127.1	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	Principles for processing personal data.	To set up data protection, customize Terms of Service: 1. Go to **Customization > TOS**. 2. Set up a TOS that is suitable for your organization.	If the default TOS is not modified then status is **Issues**.
Art. 6 & 7	Lawfulness of processing	To confirm lawfulness of processing and conditions for consent: 1. For each policy: a. Go to **Settings > Policies**. b. Open the policy for editing. c. In the **General** tab, set **Enable Privacy Settings** to **YES**, and save. 2. After you have completed this configuration for each policy: a. Go to **Settings > Misc > Privacy**. b. Set **Force users to accept TOS when changed** to enabled. c. Enable **Show TOS for every login**.	If the settings are set as specified, status is **OK**; if not, status is **Issues**.

Rule (click to see text)	Description	Steps for complying	Validation
Art. 12	Rights of data subject - transparent information	To maintain transparent information and communication: - Go to **Settings > Misc > General**, and if **Disable Action Panel** is enabled, disable it.	If **Disable Action Panel** is disabled, status is **OK**; if not, status is **Issues**.
Art. 13	Rights of data subject - information about collecting of personal data	To confirm that **Terms of Service** indicate where personal data are collected about the data subject, enable this rule.	**None**
Art. 17	Rights of data subject - right to be forgotten	To set up the right to be forgotten: 1. Go to **Settings > Misc > Privacy**. 2. In **Anonymous User Consent Message for Accessing Shared Files** enter text that explains data subject's right to erasure. 3. If a user requests to be forgotten, anonymize the data. Also see Anonymizing User Data.	If the settings are configured as specified, status is **OK**; if not, status is **Issues**.
Art. 20	Rights of data subject - right to data portability	To confirm the right to data portability, ensure the following options work in the Admin portal, and then enable this rule. - Exporting a user's file. a. In the navigation pane, click Users. b. Edit a user. c. In the **User Details** dialog box, click **Manage Files**. and then click **My Files**. d. Click **Download as Zip** for a file, and confirm that the zip download works. - Exporting audit log records. a. In the navigation pane, click **Audit**. b. In the upper-right corner of the screen, click **Manage.** c. In the **Manage Audit Logs** dialog box, enter a **Start Date** and an **End Date**. d. Click **Export**, and confirm that the file is exported correctly.	None.

Rule (click to see text)	Description	Steps for complying	Validation
Art. 21	Rights of data subject - right to object	To confirm users have right to object: • For each policy: a. Go to **Settings > Policies**. b. Open the policy for editing. c. In the **General tab**, set **Enable Privacy Settings** to **Yes**. After you have completed this configuration for each policy: 1. Go to **Settings > Misc**. 2. Click the **Privacy** tab. 3. Check **Show TOS for every login**. 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.	If the specified settings are set, status is **OK**; if not, status is **Issues**.
Art. 30	Controller and processor - Records of processing activities	To maintain records of processing activities: 1. Go to **Settings > Admin**. 2. Set **Audit Log Level** to **Request** or **Full**.	If **Audit Log Level** is set to **Request** or **Full**, status is **OK**; if **Audit Log Level** is set to **Off**, status is **Issues**.
Art. 32	Controller and processor - Security of processing	Configure storage encryption. 1. See Setting Up Managed Storage Encryption in the support document. a. Go to **Settings > Storage > Managed storage** and enable encryption. b. Encrypt all existing files.	If storage is not fully encrypted or any existing files are not fully encrypted, status is **Issues**.
Art. 33	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

Rule (click to see text)	Description	Steps for complying	Validation
Art. 35	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, **Status** is **OK**. If any rules are not enabled or do not pass, **Status** is **Issues**.
Art. 37	Controller and processor - Designation of the data protection officer	To enable at least one user to manage the Compliance Center: 1. Go to **Admins** and create a role with **Compliance** access to the Compliance Center. 2. In **Admins**, add at least one user to the role with access to the Compliance Center.	If one or more users have access to the Compliance Center, status is **OK**; if not, status is **Issues**.
Art. 45	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 **OK**; if not, or if modifications to the rule allow login from outside locations, status is **Issues**.

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.

Rule (click to see text)	Description		Validation
Access Control 3.1.1	Choose a DLP rule to restrict public sharing of CUI.	To guard against unauthorized access to CUI: 1. Click the edit button, and select a DLP rule that blocks public shares. 2. Change any existing public shares to private.	If the DLP rule exists and is enabled and there are no existing public shares, status is **OK**; if not, or if modifications to the rule allow public shares, status is **Issues**.

Rule (click to see text)	Description		Validation
Access Control 3.1.8	Configure password settings to limit unsuccessful logon attempts.	To set a limit on unsuccessful logon attempts: 1. Go to **Settings > Misc > Password**. 2. Configure the setting as follows: **Incorrect Password Attempts Before Account Lockout** - a value greater than 0.	If the **Incorrect Password Attempts Before Account Lockout** setting is set as indicated, then status is **OK**; if not, status is **Issues**.
Access Control 3.1.18	Set up a workflow that blocks the connection of a new mobile device until it is approved.	To set up a workflow to block the connection of a new mobile device: • Go to **Workflow > Add Workflow** and choose **If any new client app connects > Block the device for admin approval**. For information about this workflow, see: Admin Approval Required Workflow	If the workflow does not exist or is not enabled, the status is **Issues**.
Audit and Accountability 3.3.1	Set the audit log level.	To monitor log-in attempts: • Go to **Settings > Admin**, and set **Audit Log Level** to **REQUEST** or **FULL**.	If **Audit Log Level** is set to **OFF**, status is **Issues**.
Audit and Accountability 3.3.3	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	Confirm admin understands how to disable the deletion of audit records.	To disable deletion of audit records see Delete Audit Log Entries.	None

Rule (click to see text)	Description		Validation
Audit and Accountability 3.3.9	Give at least one admin user access to the Audit Reports.	To enable at least one admin user to access the Audit Reports: 1. Go to **Admins** and create a role with read access to the Audit Reports. 2. Add at least one user to the role.	If one or more users have access to the Audit Reports, the status is **OK**; if not, the status is **Issues**.
Configuration Management 3.4.2	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	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: Changing a Default Port or Web Server Setting.	None
Identification and Authentication 3.5.2	Configure and enable the **Authentication Type** as **Active Directory** or **LDAP** or enable SSO.	To authenticate users during login: - Go to **Settings > Authentication**, and set **Authentication Type** to **Active Directory** or **LDAP**. To enable SSO, see: SAML Single Sign-On Support	If **Authentication Type** is set to **Default** and SSO is not enabled, status is **Issues**.
Identification and Authentication 3.5.7	Set up strong password management.	To set regulations for strong password management: 1. Go to **Settings > Misc > Password**. 2. Configure the settings as follows: **Minimum Password Length** - 8 or more. **Enable Strong Passwords** - enable. **Disallow Commonly Used Passwords** - enable. **User Password Expiration In Days** - a value greater than 0.	If the password settings are set as indicated, status is **OK**; if not, status is **Issues**.

Rule (click to see text)	Description		Validation
Identification and Authentication 3.5.8	Disallow the reuse of previous passwords.	To disallow the reuse of previous passwords: 1. Go to **Settings > Misc > Password**. 2. Configure the setting as follows: **Number of previous passwords that cannot be reused** - a value greater than 0.	If **Number of previous passwords that cannot be reused** is set as indicated, then status is **OK**; if not, status is **Issues**.
Identification and Authentication 3.5.9	Require new accounts to change passwords.	To require new accounts to change passwords: 1. Go to **Settings > Misc > Password**. 2. Configure the setting as follows: **New accounts must change password** - enable.	If **New accounts must change password is** set as indicated, then the status is **OK**; if not, the status is **Issues**.
Incident Response 3.6.1	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
Maintenance 3.7.4	Configure antivirus protection against malicious file uploads.	To protect CUI from malicious file uploads: 1. Go to **Settings > Third Party Integrations > Antivirus**. 2. Configure an **Antivirus** type.	If **Antivirus** is configured, status is **OK**; if not, status is **Issues**.
Media Protection 3.8.4	Choose a metadata set to classify controlled unclassified information	To indicate which files are CUI, click the edit button and select a metadata set with a tag for identifying them. (Use smart classification to apply the metadata tag to the CUI.)	If the metadata set exists and is enabled, status is **OK**; if not, status is **Issues**.

Rule (click to see text)	Description		Validation
Media Protection 3.8.6	Configure and enable encryption.	To maintain security: Configure storage encryption. 1. Go to **Settings > Storage > Managed Storage** and enable encryption. 2. Encrypt all existing files. See Setting Up Managed Storage Encryption in the support document.	If storage is not fully encrypted or any existing files are not fully encrypted, status is **Issues**.
Systems and Communications Protection 3.13.3	Give at least one user in an admin role access to the Compliance Center.	To enable at least one user to manage the Compliance Center: 1. Go to **Admins** and create a role with **Compliance** access to the Compliance Center. 2. In **Admins**, add at least one user to the role with access to the Compliance Center.	If one or more users have access to the Compliance Center, status is **OK**; if not, status is **Issues**.
Systems and Communications Protection 3.13.4	Choose a DLP rule that only allows private sharing.	To guard against unauthorized access to CUI: 1. Click the edit button, and select a DLP rule that blocks public shares. 2. Change any existing public shares to private.	If the DLP rule exists and is enabled and there are no existing public shares, status is **OK**; if not, or if modifications to the rule allow public shares, status is **Issues**.
Systems and Communications Protection 3.13.9	Set session timeout for the user portal.	To confirm automatic logoff of sessions: 1. Go to **Settings > Server**, and set **Session Timeout** to a value greater than 0.	If **Session Timeout** is set to **0** or empty, status is **Issues**.

Rule (click to see text)	Description		Validation
Systems and Communications Protection 3.13.10	Confirm decryption keys are confidential.	To confirm that decryption keys are confidential, enable this rule.	None
System and Information Integrity 3.14.1	Enable **Governance Report Email** to send the admin an email reminder to check audit logs, reports, and security issues regularly.	To implement procedures to regularly review records such as audit logs and violation report: • Enable **Send daily governance report to admin** option in **Admin** settings.	If the **Send daily governance report to admin** setting is enabled, status is **OK**; if not, status is **Issues**.

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.	Enable this rule to confirm that admins understand how personal data is processed to create or perform the following: • Audit records • Alerts • Reports • Activity and share activity in user portal • Notifications	None

Rule (click to see text)	Description	Steps for complying	Validation
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.	To obtain explicit and informed consent from users before processing their data: For each policy: 1. Go to **Settings > Policies**. 2. Open the policy for editing. 3. In the **General** tab, set **Enable Privacy Settings** to **YES**, and save. After you have completed this configuration for each policy: 1. Go to **Settings > Misc > Privacy**. 2. Enable **Force users to accept TOS when changed**. 3. Enable **Show TOS** for every login.	If the specified settings are set, status is **OK**; if not, status is **Issues**.
Ch. 2 Section 9 Purpose Limitation	Set up terms of service.	To set up data protection principles: 1. Go to **Customization > TOS**. 2. Set up a TOS that is suitable for your organization.	If the default TOS is not modified then status is **Issues**.
Ch. 2 Section 10 Data Minimization	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

Rule (click to see text)	Description	Steps for complying	Validation
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.	To protect personal data files and folders from deletion: • Click the edit button, and select a retention policy to protect personal data files and folders from deletion based on metadata. • Confirm admins understand that after the retention period, files will be completely deleted from the recycle bin.	If the retention policy exists and is enabled, status is **OK**; if not, or if modifications to the retention policy allow file or folder deletion, status is **Issues**.
Ch. 2 Section 13 Integrity and Confidentiality	Configure and enable encryption.	To maintain security: 1. Configure storage encryption. See Setting Up Managed Disk Storage Encryption in the support document. 2. Go to **Settings > Storage > Managed Storage** and enable encryption. 3. Encrypt all existing files.	If storage is not fully encrypted, or any existing files are not fully encrypted, status is **Issues**.
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.
Ch. 3 Section 16 Right of Correction	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.

Rule (click to see text)	Description	Steps for complying	Validation
Ch. 3 Section 17 Right to Erasure	Use Anonymize Data.	To confirm the right to be forgotten: 1. Go to **Settings > Misc > Privacy**. 2. In **Anonymous User Consent Message for Accessing Shared Files** enter text that explains data subject's right to erasure. 3. If a user requests to be forgotten, anonymize the data. Also see Anonymizing User Data.	If the specified settings are set, status is **OK**; if not, status is **Issues**.
Ch. 3 Section 19 Right to Object to Processing	Confirm that admins and users know privacy TOS behavior.	To configure users' right to object: For each policy: 1. Go to **Settings > Policies**. 2. Open the policy for editing. 3. In the **General** tab, set **Enable Privacy Settings** to **Yes**. After you have completed this configuration for each policy: 1. Go to **Settings > Misc**. 2. Click the **Privacy** tab. 3. Enable **Show TOS for every login**. 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.	If the specified settings are set, status is **OK**; if not, status is **Issues**.

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.	To configure the right to data portability, ensure the following options work in the admin portal, and then enable this rule. Exporting a user's file. 1. In the navigation pane, click **Users**. 2. Edit a user. 3. In the **User Details** dialog box, click **Manage Files**. and then click **My Files**. 4. Click **Download as Zip** for a file, and confirm that the zip download works. Exporting audit log records. 1. In the navigation pane, click **Audit**. 2. In the upper-right corner of the screen, click **Manage**. 3. In the **Manage Audit Logs** dialog box, enter a **Start Date** and an **End Date**. 4. Click **Export**, and confirm that the file is exported correctly.	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.	To enable at least one user to manage the Compliance Center: 1. Go to **Admins** and create a role with **Compliance** access to the Compliance Center. 2. In **Admins**, add at least one user to the role with access to the Compliance Center.	If one or more users have access to the Compliance Center, status is **OK**; if not, status is **Issues**.
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 International Organizations	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	FileCloud Version
1.1 Text alternatives	**Requirement:** 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. **FileCloud compliance:** • Images are associated with alt tags to act as image descriptions. • Controls like checkboxes have aria attributes to describe their usage.	20.3

Guideline	Descriptions of requirement and FileCloud's compliance	FileCloud Version
1.3 Adaptable content	**Requirement:** Create content that can be presented in different ways (for example simpler layout) without losing information or structure. **FileCloud compliance:** • The labels for required fields are displayed in red. • The labels for checkboxes can be programmatically determined, as they are associated with aria-label attributes. • The rows of files are navigable through the keyboard. • Keyboard support is included for forms. • 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. **Note**: Added in FileCloud 23.1 for requirement 1.3.1. • Wherever possible, data tables are programmatically marked to show relationships between table headers and table cells. **Note**: Added in FileCloud 23.1 for requirements 1.3.1 and 1.3.2.	20.3
1.4 Distinguishable	**Requirement**: Make it easier for users to see and hear content including separating foreground from background. **FileCloud compliance:** The new UI enables high contrast mode, which makes the visual presentation of blocks of text and icons easily readable.	
2.1 Keyboard Accessible	**Requirement**: Make all functionality available from a keyboard. **FileCloud compliance:** • Keyboard accessibility is supported in FileCloud, and enables users to submit forms or navigate using keyboard shortcuts and keyboard navigation. • The **Details** section in My Files is keyboard accessible. **Note**: Added in FileCloud 23.1 for requirement 2.1.1. See Guide to Keyboard Shortcuts.	

Guideline	Descriptions of requirement and FileCloud's compliance	FileCloud Version
2.2.5 Re-authenticating	**Requirement**: When an authenticated session expires, the user can continue the activity without loss of data after re-authenticating. **FileCloud compliance:** When an authenticated session expires, the user can continue the activity after re-authenticating.	
2.4 Navigable	**Requirement**: Provide ways to help users navigate, find content, and determine where they are. **FileCloud compliance:** • In FileCloud, keyboard accessibility enables users to navigate through file lists and tab through fields in forms. See Guide to Keyboard Shortcuts. • A link for skipping navigation enables users to skip repetitive navigation information on pages and directly access the main content. **Note**: Added in FileCloud 23.1 for requirement 2.4.1. • Interactive elements such as table headers are read in tab order, and focus order of tables is top to bottom and left to right. **Note**: Added in FileCloud 23.1 for requirement 2.4.3.	
3.1 Readable	**Requirement**: Make text content readable and understandable. **FileCloud compliance:** 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.	
3.2 Predictable	**Requirement**: Make Web pages appear and operate in predictable ways. **FileCloud compliance:** • Drop-down lists are keyboard-navigable. • Focus is set to the first input field in forms.	
3.3 Input Assistance	**Requirement**: Help users avoid and correct mistakes. **FileCloud compliance:** All form input fields have proper labels and validation of inputs in place. Errors are shown if a form submission fails.	

Guideline	Descriptions of requirement and FileCloud's compliance	FileCloud Version
4.1 Compatible	**Requirement**: Maximize compatibility with current and future user agents, including assistive technologies. **FileCloud compliance:** • 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. • Screen reader indicates whether elements are buttons or links. **Note**: Added in FileCloud 23.1 for requirement 4.1.2. • Screen reader informs users when new data is loaded on the page or dynamic content appears. **Note**: Added in FileCloud 23.1 for requirement 4.1.3.	

Retention Policies

> Retention Policies are available for the Enterprise editions of FileCloud. Learn more about differences in features 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.

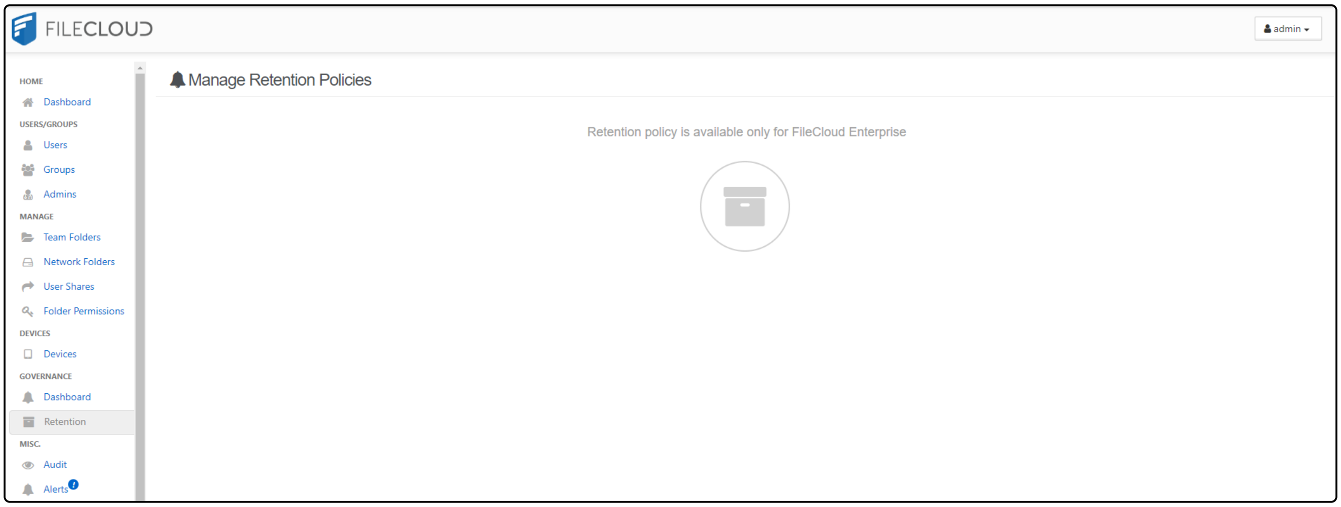
How Retention Policies Function

Create a Type of Retention Policy

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



Manage Retention Policies

Retention policy is available only for FileCloud Enterprise

Create a Type of Retention Policy

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

Policy Type	Description
Admin Hold	• Prevents any update or delete of digital content for an indefinite period of time • Admin Hold policies applied to folders can be removed • Admin policies applied to files can be removed Create an Admin Hold policy
Legal Hold	• Freezes digital content to aid discovery or legal challenges • During a legal hold, file modifications are not allowed • Holds cannot be reversed once applied Create a Legal Hold policy
Retention	• Identifies digital content to be kept around for an unlimited amount of time before being deleted or released • Retention policies cannot be reversed once applied Create a Retention policy
Archival	• Moves and stores old organizational content, for example, to a more cost effective systems for long term • No Deletion is allowed until a specific time period is reached • After the specified time period is reached, content gets moved to a specific folder or location Create an Archival policy
Trash Retention	• Controls if files can permanently be deleted off the FileCloud Server system • Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions Create a Trash Retention policy

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	• Fixed Date • 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 a Legal Hold?

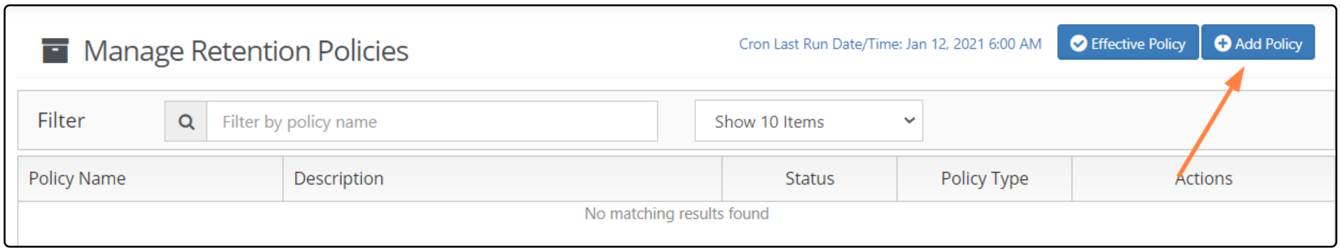
In the world of litigation, a legal hold is a notification

- It is sent from an organization's legal team to employees
- It instructs them not to delete electronically stored information (ESI)
- It also instructs then 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

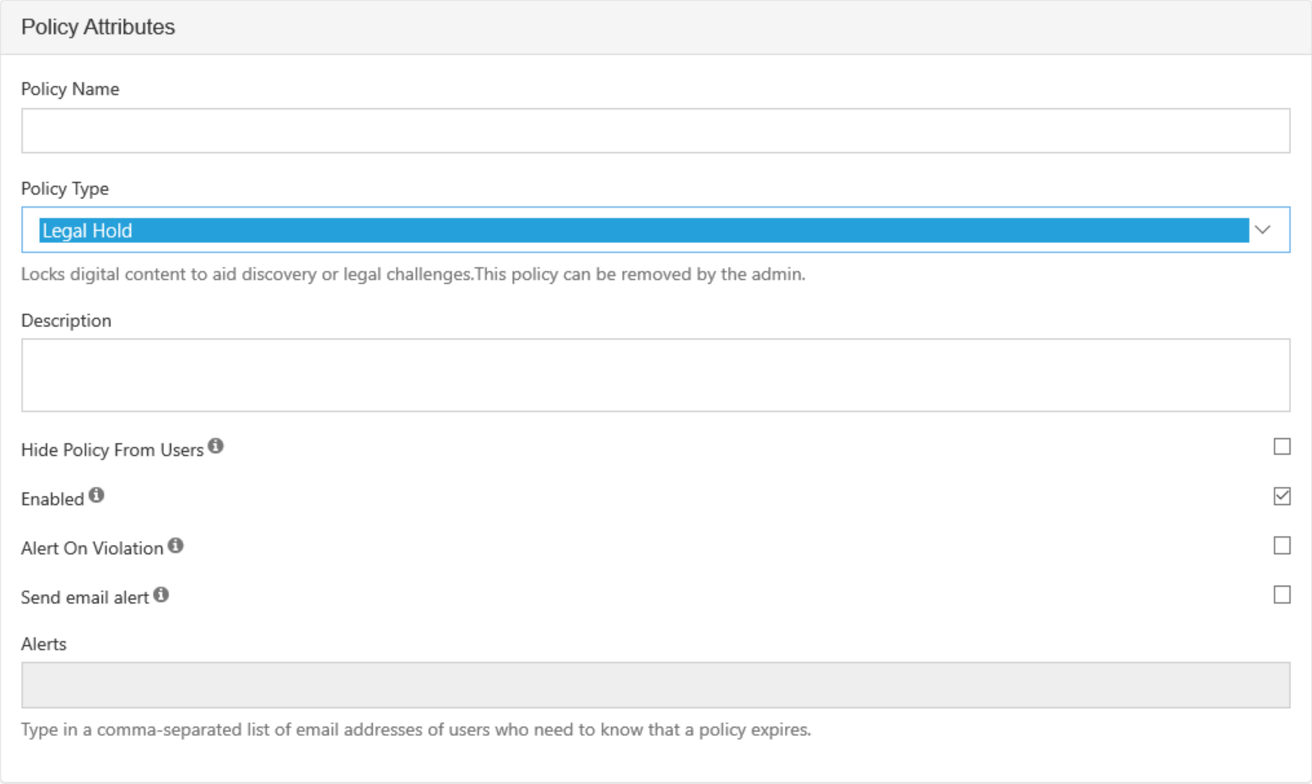

Manage Retention Policies
Cron Last Run Date/Time: Jan 12, 2021 6:00 AM
Effective Policy
Add Policy
Filter
Filter by policy name
Show 10 Items

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

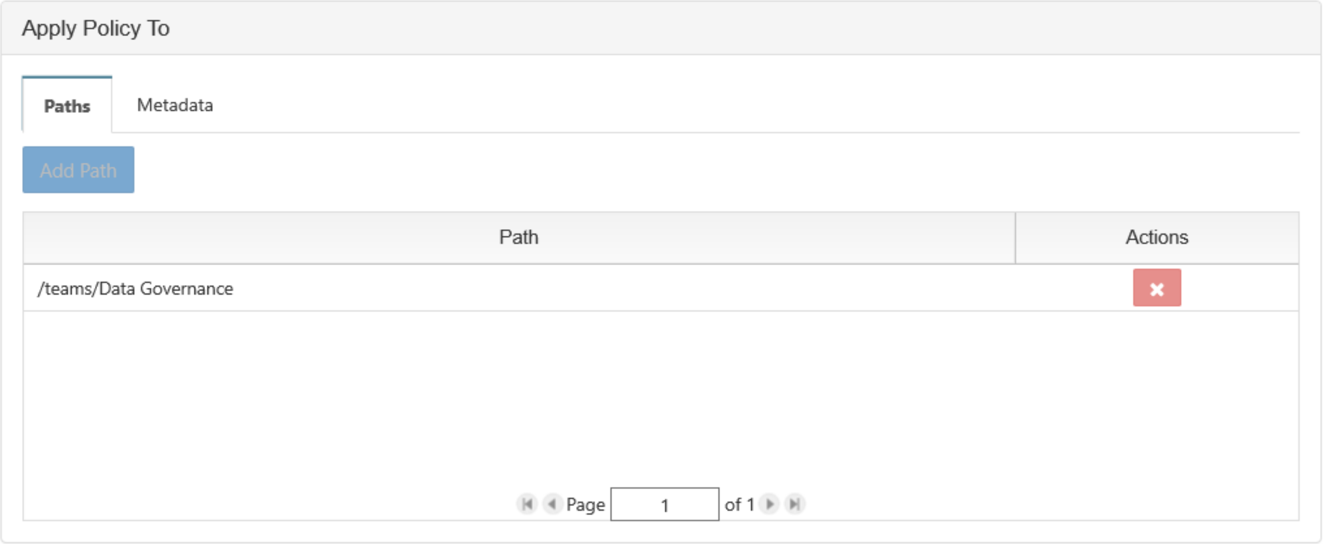
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select *Legal Hold*
Description	- Required - A string of characters, letters, and numbers that provide details about why the policy is necessary - This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab

Property	Description
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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.

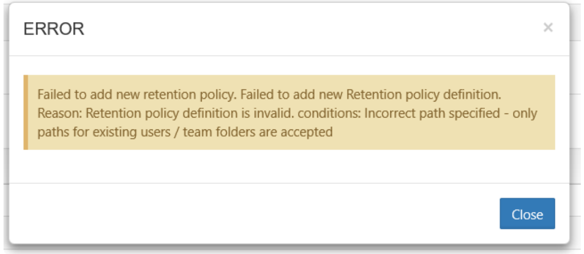


Apply Policy To

Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
• The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: • The first component of the path has to already exist /username/ • This means that the username or team folder has to already exist before you can save the policy	• You CANNOT specify a path that does not exist This will prevent you from saving the policy  ERROR 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

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.

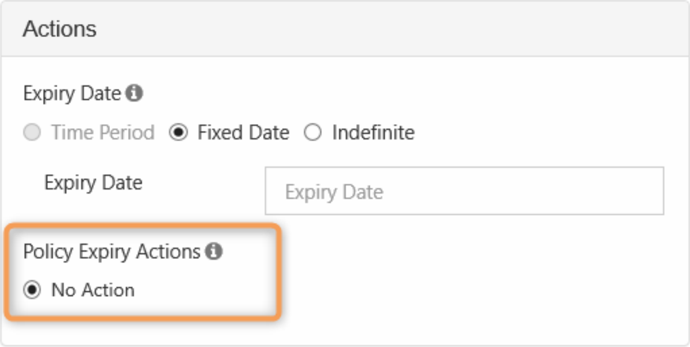
You can select metadata from the following existing attributes or sets:

- 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

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



Actions

Expiry Date

○ Time Period ● Fixed Date ○ Indefinite

Expiry Date: Expiry Date

Policy Expiry Actions

● No Action

To set a fixed date:

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

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

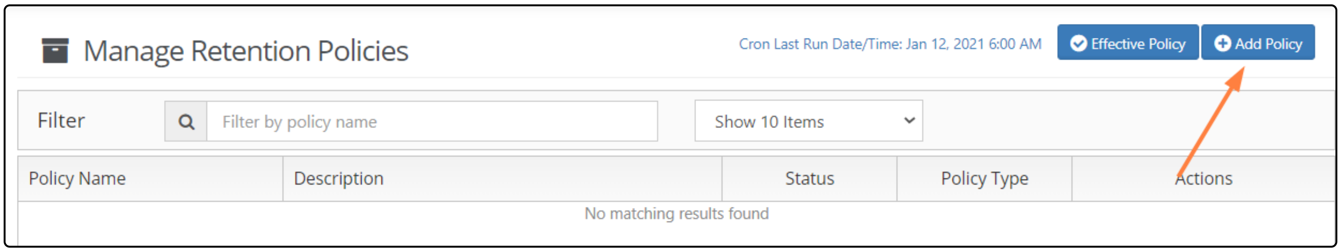
Copies cannot be created if there is a retention hold on the destination folder that prevents updates.

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.

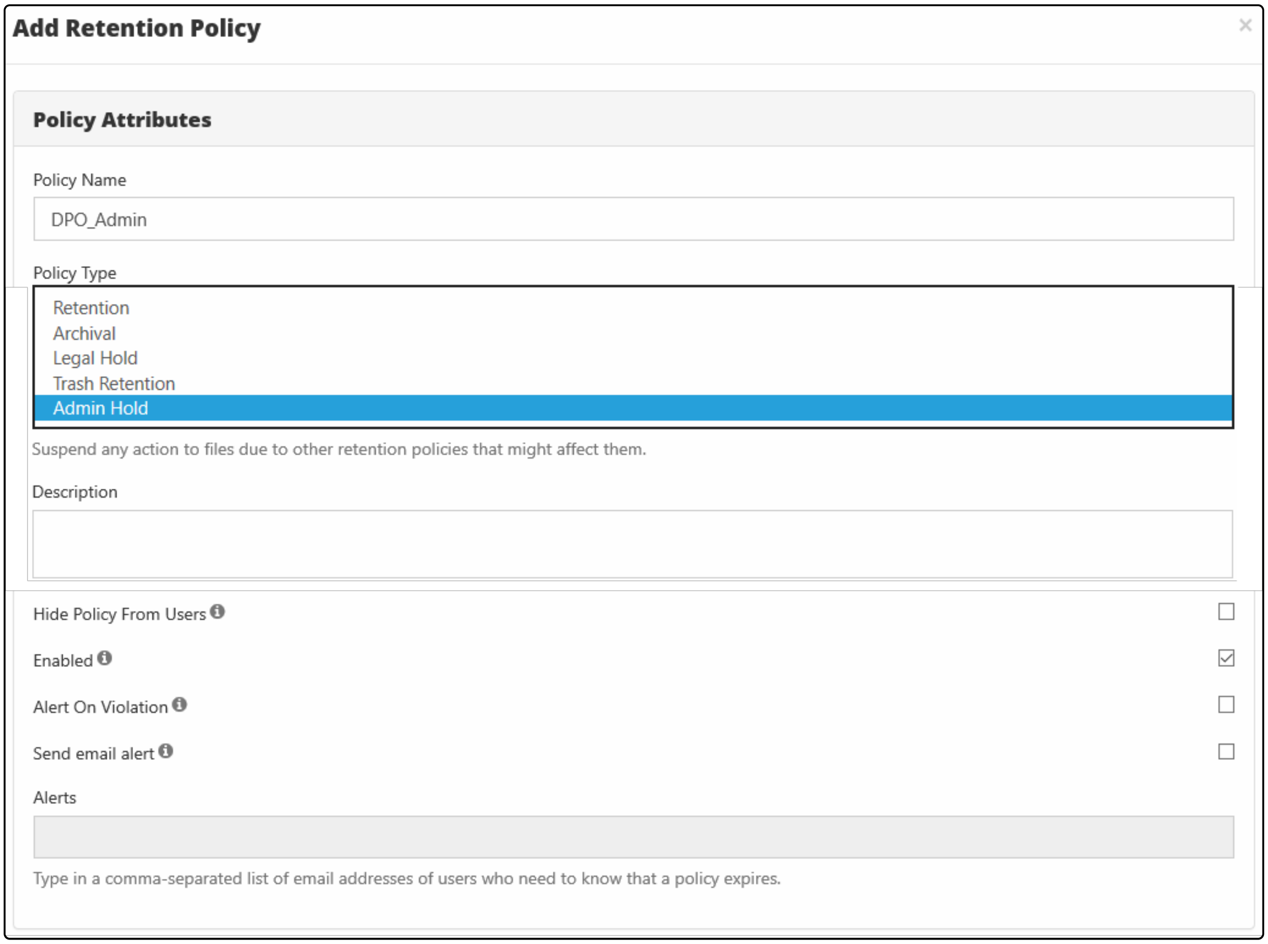
Creating the Policy



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

Policy Attributes

Policy Name: DPO_Admin

Policy Type: 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

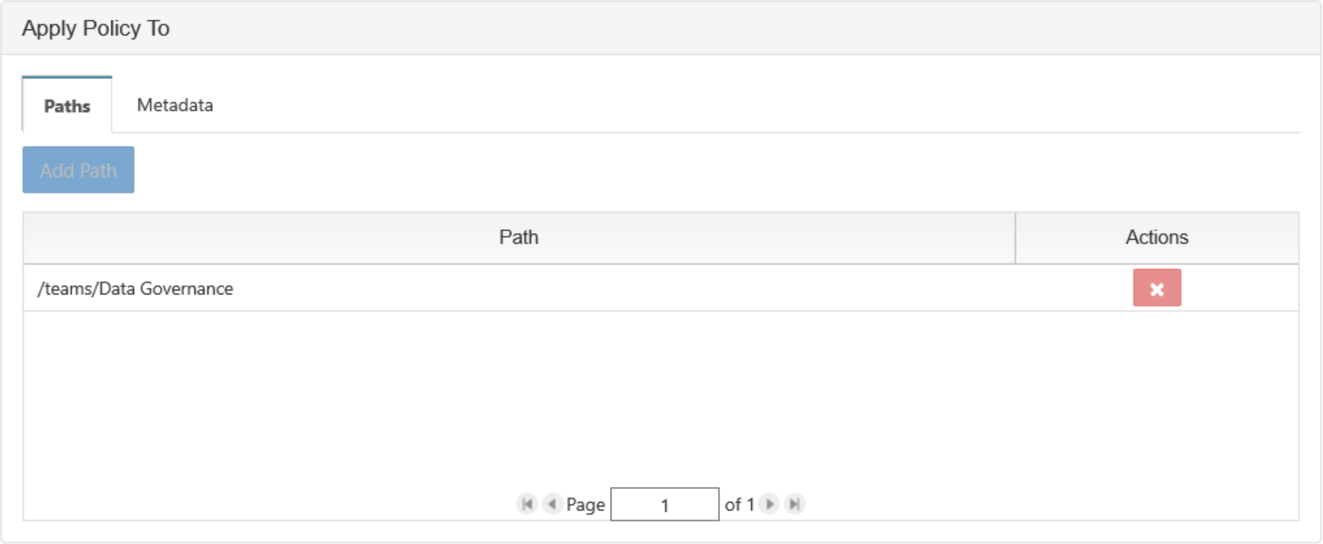
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select Admin Hold
Description	• Required • A string of characters, letters, and numbers that provide details about why the policy is necessary • This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab

Property	Description
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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.

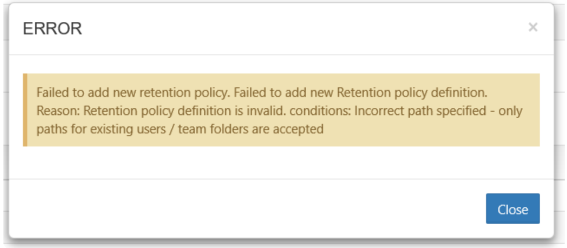


Apply Policy To

Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
• The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: • The first component of the path has to already exist /username/ • This means that the username or team folder has to already exist before you can save the policy	• You CANNOT specify a path that does not exist This will prevent you from saving the policy  ERROR 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

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:

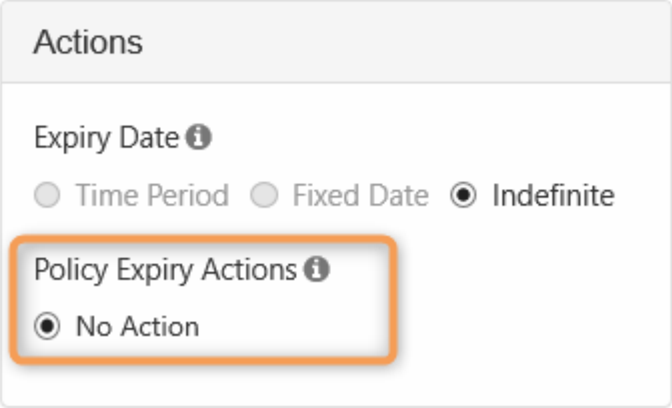
- Default sets = provided with FileCloud and applies to every folder and cannot be modified
- Built-In sets = provided with FileCloud and includes the Document Life Cycle and Image metadata sets
- Custom attributes and sets = created by administrators in the Admin Portal

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



Actions

Expiry Date

○ Time Period ○ Fixed Date ● Indefinite

Policy Expiry Actions

● No Action

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	• Time Period • Fixed Date	• Move files to a specific location

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.

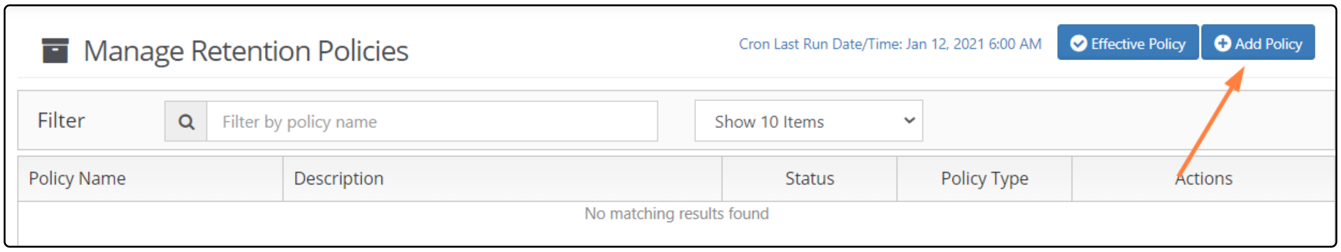
For example:

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.

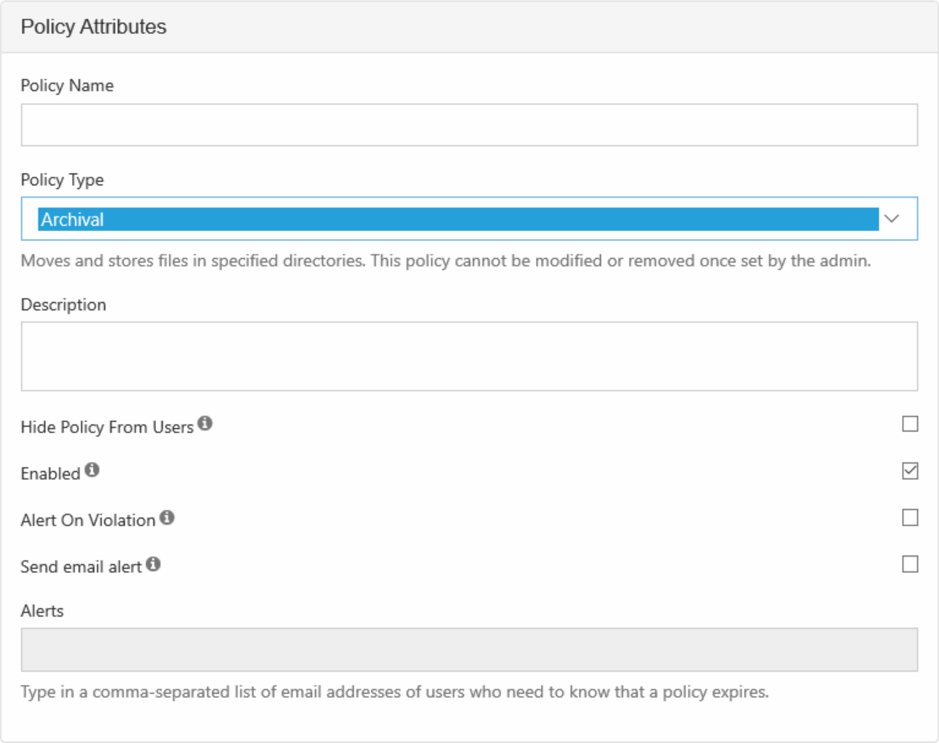
Creating the Policy



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

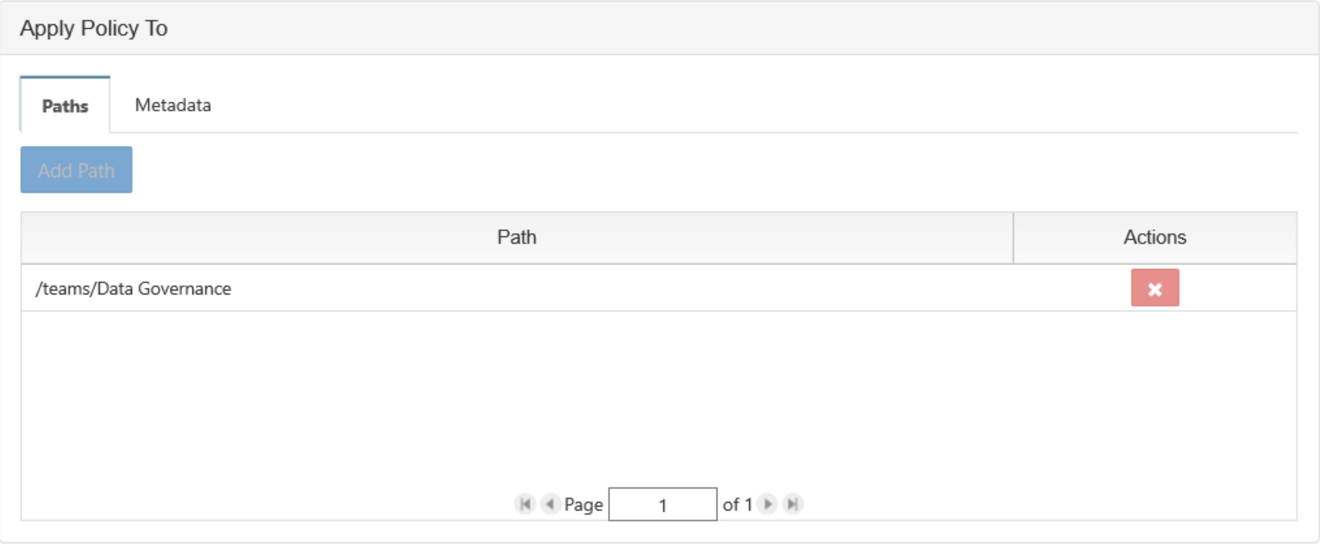
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select *Archival*
Description	• Required • A string of characters, letters, and numbers that provide details about why the policy is necessary • This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab

Property	Description
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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.

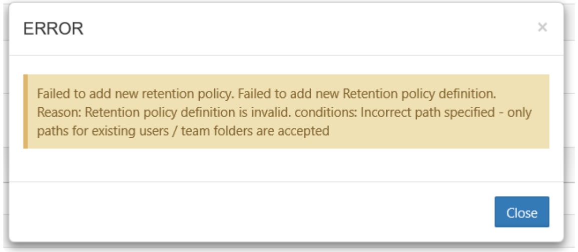


Apply Policy To

Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
• The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: • The first component of the path has to already exist /username/ • This means that the username or team folder has to already exist before you can save the policy	• You CANNOT specify a path that does not exist This will prevent you from saving the policy  ERROR 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

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.

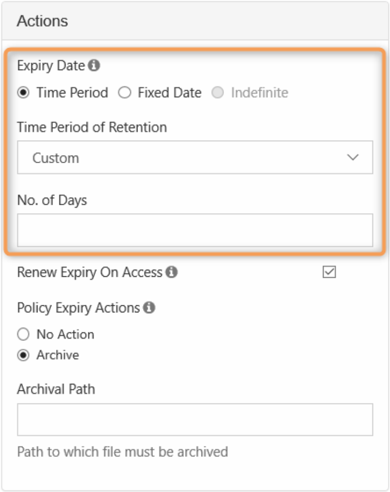
You can select metadata from the following existing attributes or sets:

- 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.



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention: Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions

○ No Action

● Archive

Archival Path

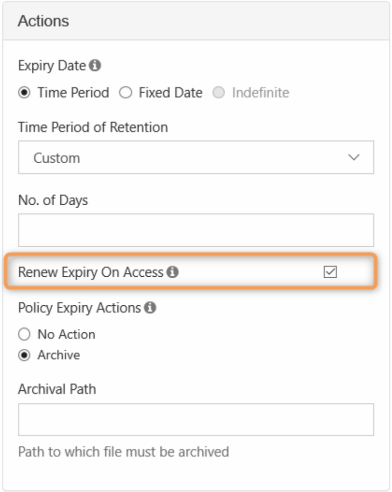
Path to which file must be archived

To set a Time Period:

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

To set a fixed date:

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



Actions

Expiry Date
● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention
Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions
○ No Action
● Archive

Archival Path

Path to which file must be archived

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

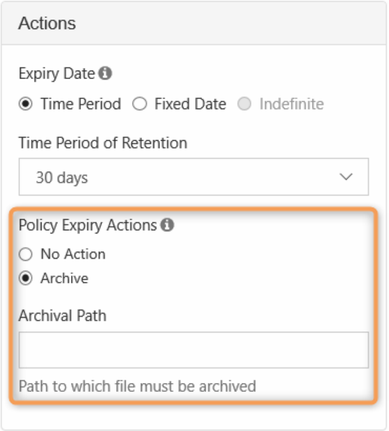
⚠ Available only if the *Time Period* option is set, and selected by default.

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

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

To set Renew Expiry On Access:

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



Actions

Expiry Date
● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention
30 days

Policy Expiry Actions
○ No Action
● Archive

Archival Path

Path to which file must be archived

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

To set Policy Expiry Actions:

1. In *Policy Expiry Actions*, select either:
   a. *No Action* : Although this option is available, if you select it you will get an error and will not be able to save the policy
   b. *Archive* : After the specified time period or fixed date is reached, content is moved to a specific folder or location
2. If you select *Archive*, in *Archive Path* you must type in a path to the location where the files are moved.

Create a Retention Policy

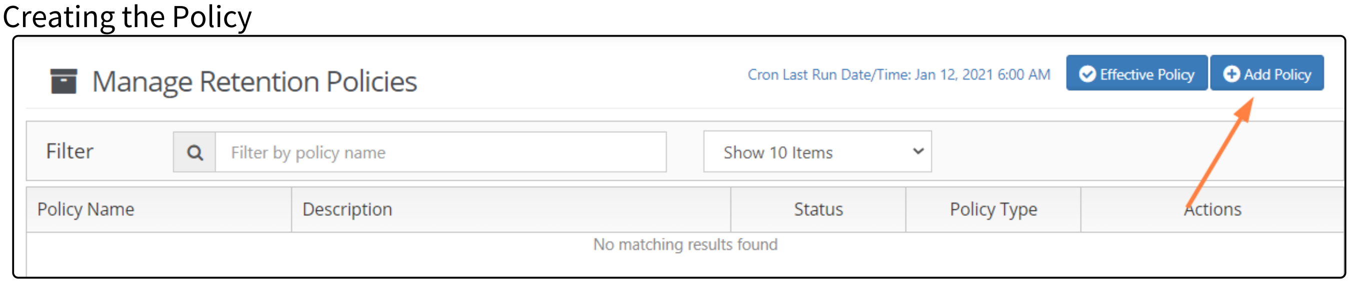
🚫 A Retention policy allows an organization to identify specific content that is required to be stored for a specific period of time before it can be accessed. During the retention period, the content cannot be deleted.

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

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

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

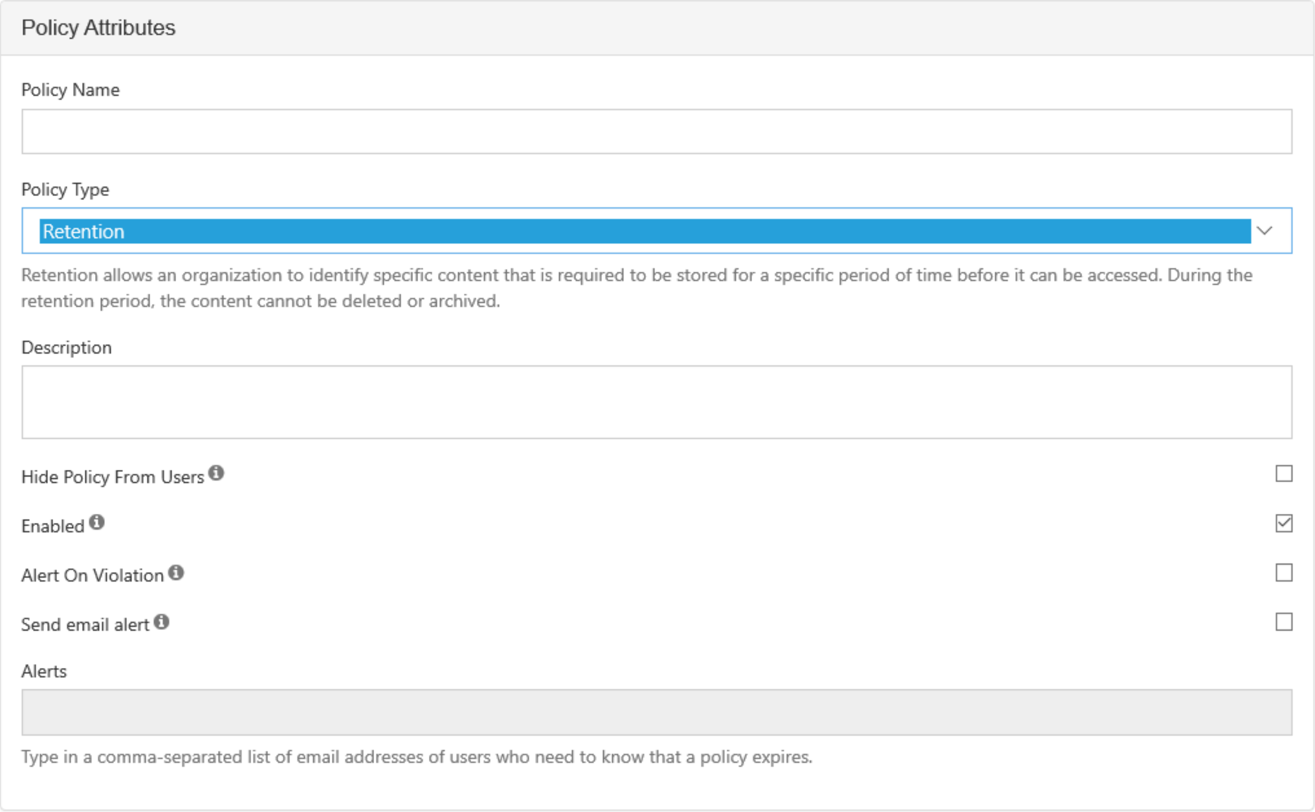
Creating the Policy



To create a Retention Policy:

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

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 □

Enabled ☑

Alert On Violation □

Send email alert □

Alerts

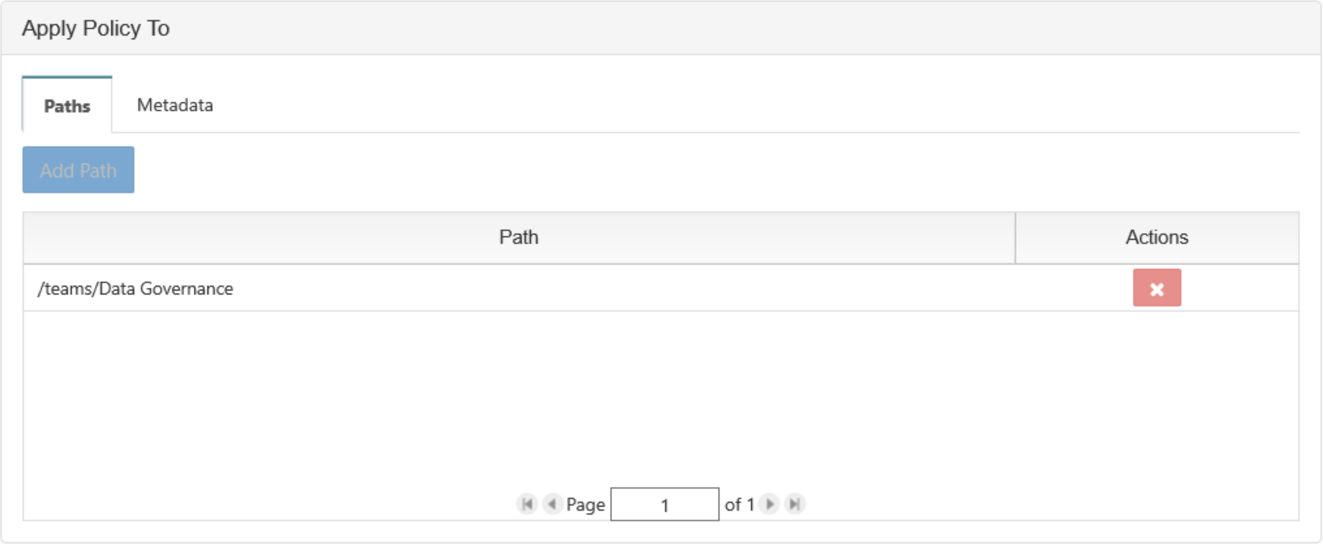
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select *Retention*
Description	• Required • A string of characters, letters, and numbers that provide details about why the policy is necessary • This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab

Property	Description
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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

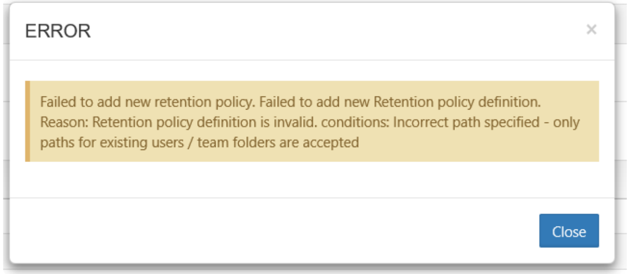
The Path and the Metadata tabs allow you to define the conditions that specify how the policy will be applied in the system.



Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
• The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: • The first component of the path has to already exist /username/ • This means that the username or team folder has to already exist before you can save the policy	• You CANNOT specify a path that does not exist This will prevent you from saving the policy  ERROR 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

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.

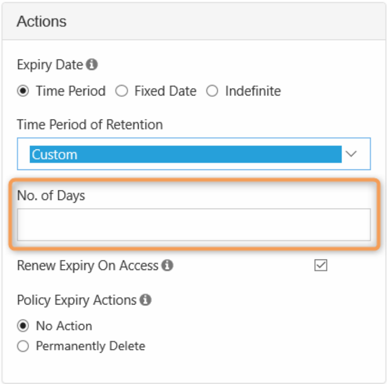
You can select metadata from the following existing attributes or sets:

- 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.



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention

Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions

● No Action

○ Permanently Delete

To set a Time Period:

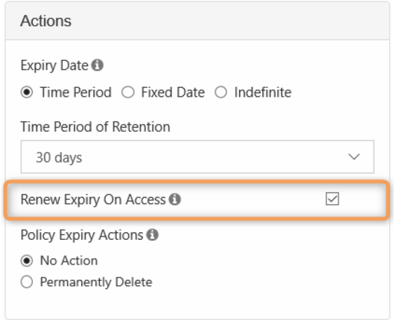
1. In the *Actions* section, click *Time Period*.
2. In Time Period of Retention, click the down arrow.
3. From the list, you can select a built-in option:
   a. *30 days*
   b. *60 days*
   c. *1year*
   d. *2years*
4. From the list, you can also select *Custom*.
   a. In No. of days, type in a whole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

To set a fixed date:

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

To set an Indefinite date:

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



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention

30 days

Renew Expiry On Access ☑

Policy Expiry Actions

● No Action

○ Permanently Delete

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

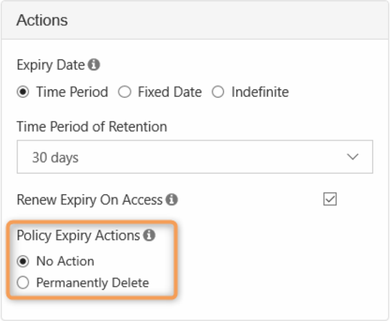
⚠ Available only if the *Time Period* option is set, and selected by default.

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

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

To set Renew Expiry On Access:

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



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention

30 days

Renew Expiry On Access ☑

Policy Expiry Actions

● No Action

○ Permanently Delete

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

To set Policy Expiry Actions:

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

Create a Trash Retention Policy

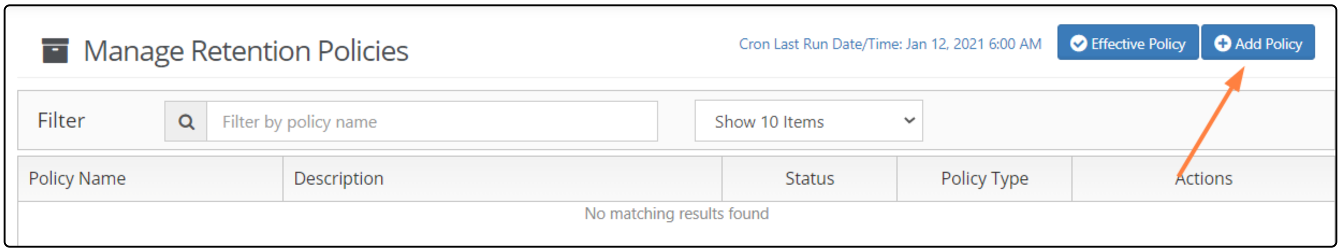
A Trash Retention policy is designed to help you control if files in the Trash Bin can be permanently deleted from FileCloud.

⚠ 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	• Time Period • Fixed Date • Indefinite	• Permanently Delete • No Action

Creating the Policy



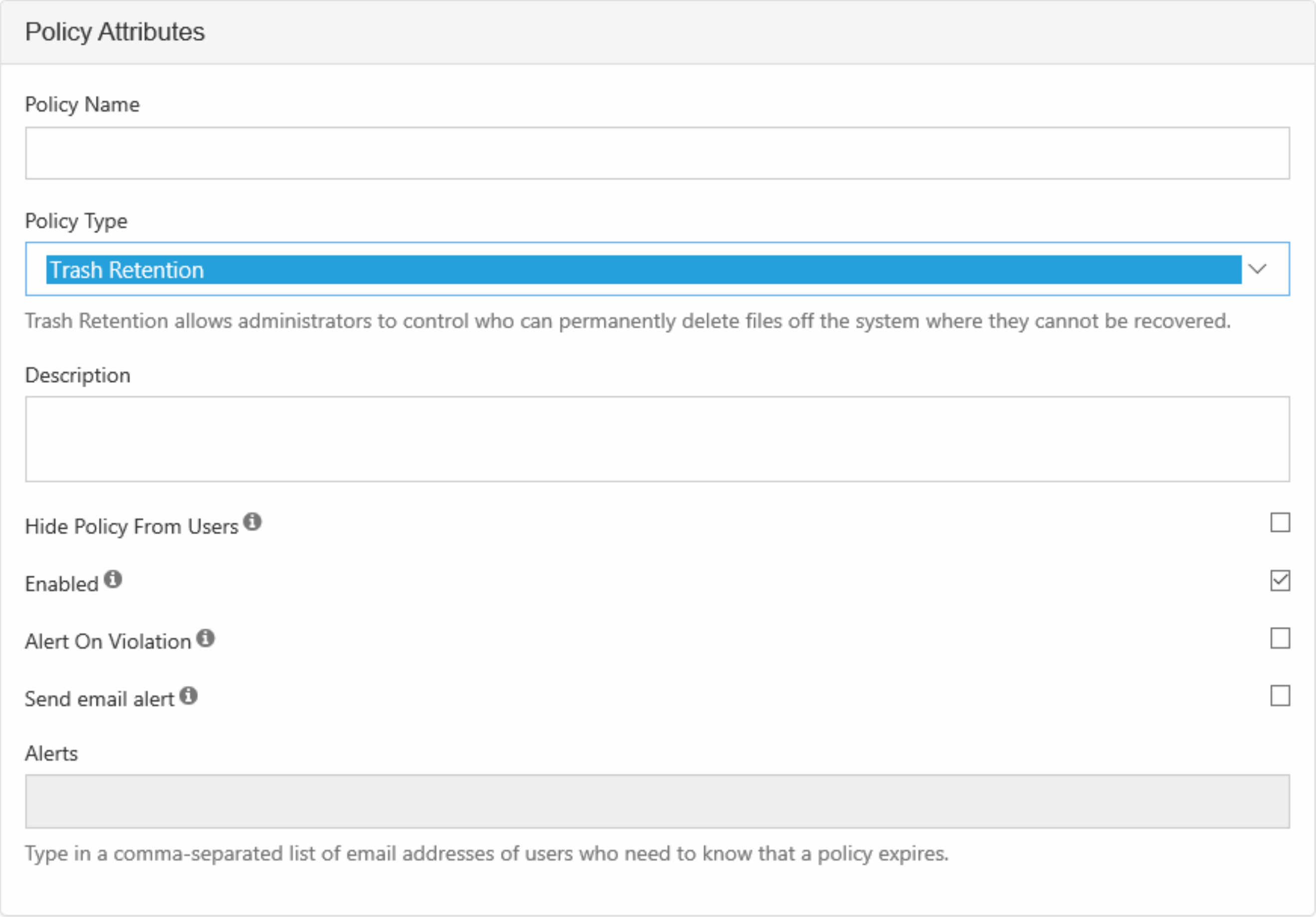
Manage Retention Policies

Policy Name	Description	Status	Policy Type	Actions
No matching results found				

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

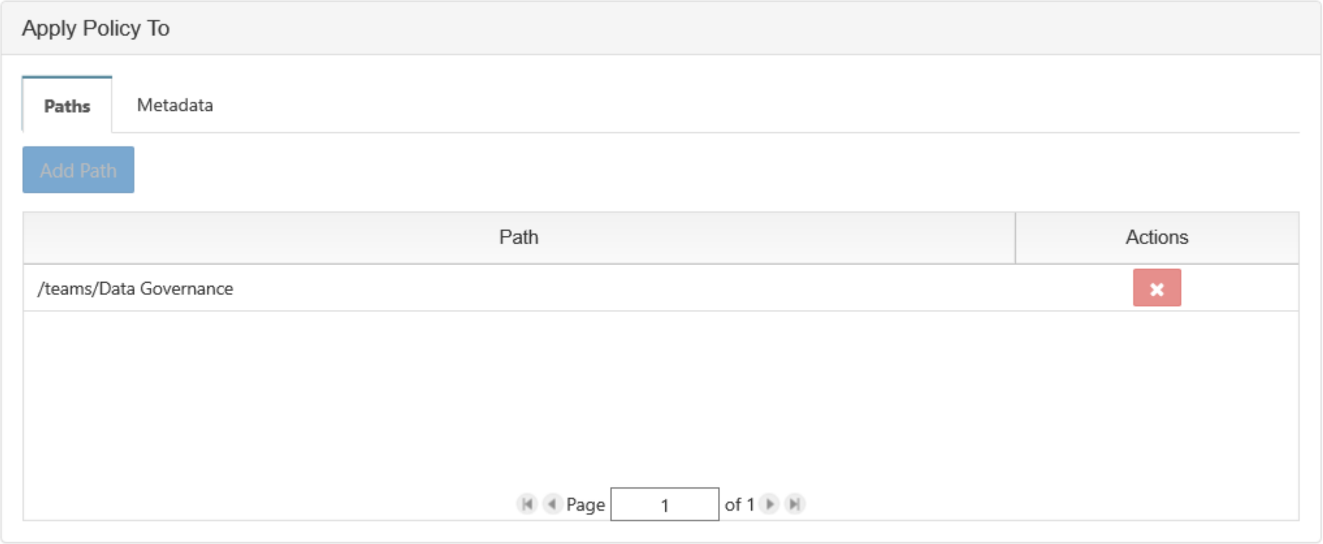
Type in a comma-separated list of email addresses of users who need to know that a policy expires.

Property	Description
Policy Name	A string of characters, letters, and numbers that provide a title for the policy
Policy Type	Select *Trash Retention*
Description	• Required • A string of characters, letters, and numbers that provide details about why the policy is necessary • This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab

Property	Description
Hide Policy from Users	- Prevents policy details from being shown and leaked. - Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. - Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. - Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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

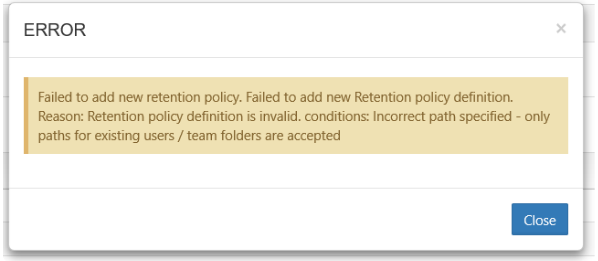
The Path and the Metadata tabs allow you to define the conditions that specify how the policy will be applied in the system.



Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
• Paths work for *managed storage* ONLY • Since managed storage includes Team Folders, you CAN add a path to a Team Folder • A Path takes the form of: /username/sub-folder • You can add more than 1 path • You can set BOTH a path and specify metadata	• You CANNOT add a path to *network folders* • You CANNOT add a path to *external folders* • You CANNOT add a path to *shared folders* • You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX • You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
• The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: • The first component of the path has to already exist /username/ • This means that the username or team folder has to already exist before you can save the policy	• You CANNOT specify a path that does not exist This will prevent you from saving the policy  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

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.

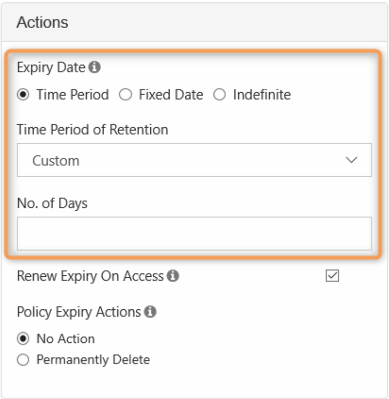
You can select metadata from the following existing attributes or sets:

- 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.



Actions

Expiry Date
● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention
Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions
● No Action
○ Permanently Delete

To set a Time Period:

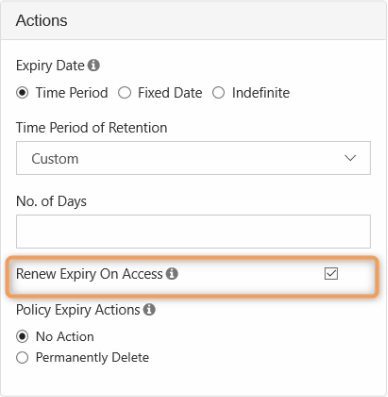
1. In the *Actions* section, click *Time Period*.
2. In Time Period of Retention, click the down arrow.
3. From the list, you can select a built-in option:
   a. *30 days*
   b. *60 days*
   c. *1year*
   d. *2years*
4. From the list, you can also select *Custom*.
   a. In No. of days, type in a whole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

To set a fixed date:

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

To set an Indefinite date:

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



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention

Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions

● No Action

○ Permanently Delete

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

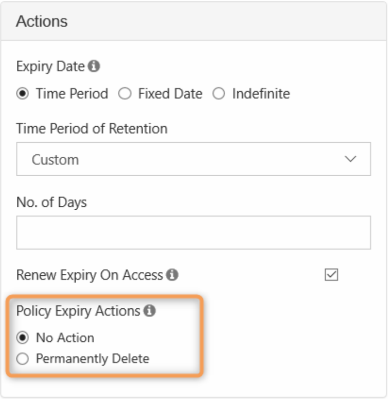
⚠ Available only if the *Time Period* option is set, and selected by default.

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

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

To set Renew Expiry On Access:

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



Actions

Expiry Date

● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention

Custom

No. of Days

Renew Expiry On Access ☑

Policy Expiry Actions

● No Action

○ Permanently Delete

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

How Policies Differ

How Policies Interact

Monitor retention policy activity

What All Policies Have In Common

All Retention Policy types have these attributes:

Policies Inherit

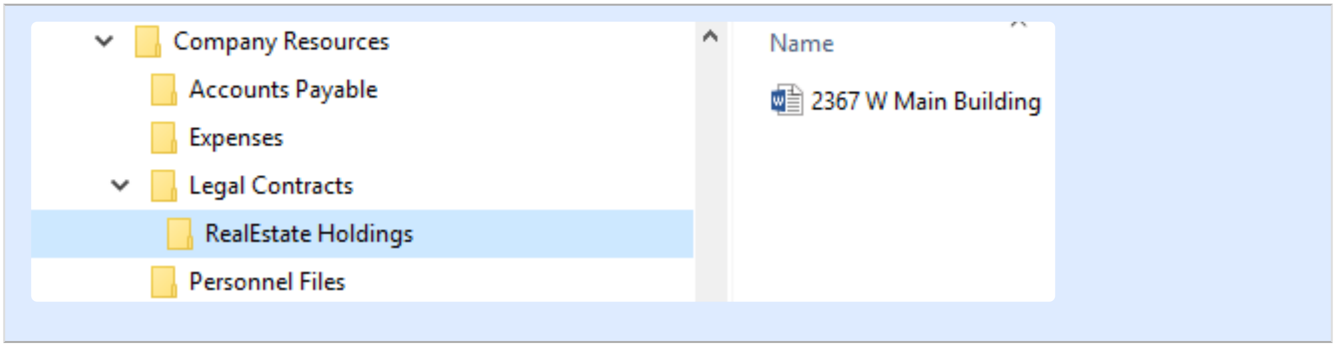
If you set a policy on a folder, all sub-files and sub-folders inherit the policy when it is enabled.

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

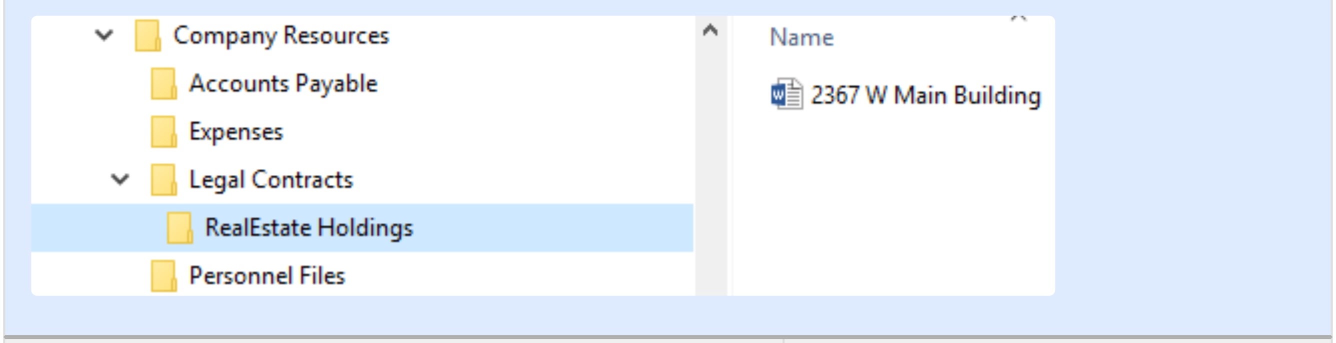
In the folder for all of the company's real estate holdings, all of these contracts are for leases that last for 1 year. • This means the Administrator needs to keep all the files in the RealEstate Holdings folder for 1 year. To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 1 year. When the policy is created: • The RealEstate Holdings folder cannot be deleted for 1 year • The document in this folder cannot be deleted for 1 year: 2367 W Main Building.docx • Any new files added to the RealEstate Holdings folder cannot be deleted for 1 year **To prevent a file with a longer retention period than its folder from being deleted when the folder's retention period is reached:** • 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. 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.	Now let's say that due to tax regulations, all legal contracts need to be retained for 5 years. • This means the Administrator needs to keep all the files in the Legal Contracts folder for 5 years. To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 5 years. When the policy is created: • No file in the Legal Contracts folder can be deleted for 5 years • The RealEstate Holdings folder now cannot be deleted for 5 years • No file in the RealEstate Holdings folder can be deleted for 5 years • The document in the RealEstate Holdings folder: 2367 W Main Building.docx now has 2 policies applied • 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 • The document in the RealEstate Holdings folder: 2367 W Main Building.docx now cannot be deleted for 5 years

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.*

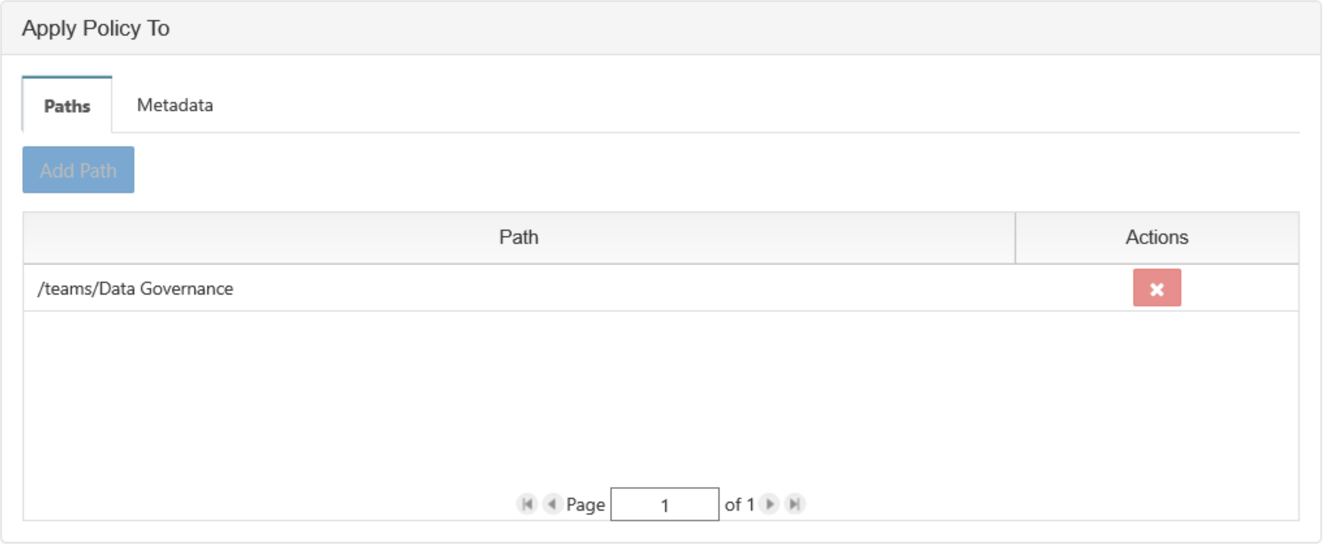
For example, The Cherry Road Brokerage company creates this folder structure in FileCloud:



ORIGINAL POLICY ASSIGNMENT	POLICY ASSIGNMENT AFTER MOVES
In the folder for all of the company's real estate holdings, all of these contracts are for leases that last for 1 year. • This means the Administrator needs to keep all the files in the RealEstate Holdings folder for 1 year. To do this, the Administrator creates a retention policy that blocks any file in this folder from being deleted for 1 year. When the policy is created: • The RealEstate Holdings folder cannot be deleted for 1 year • The document in this folder cannot be deleted for 1 year: 2367 W Main Building.docx • Any new files added to the RealEstate Holdings folder cannot be deleted for 1 year	Now let's say that tenants at 2367 W Main pay their rent for the entire year. • The administrator is asked to move the file to the Accounts Payable folder • The building will still be occupied, so the file still needs to be retained for 1 year • The Accounts Payable folder has a retention policy based on a custom metadata set for financial documents When the file is moved: • The document 2367 W Main Building.docx now lives in the Accounts Payable folder • The document 2367 W Main Building.docx keeps the retention policy for 1 year • 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

Files and Folders Are Attached to Policies

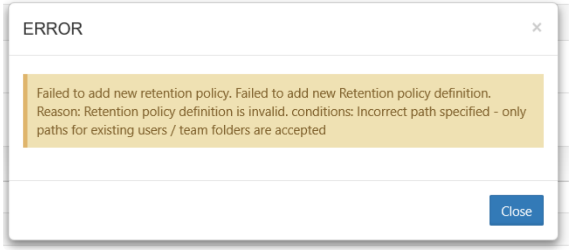
The Path and the Metadata tabs allow you to define the conditions that specify how the policy will be applied in the system.


Apply Policy To

Path	Actions
/teams/Data Governance	✖

Add a Path

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

What you CAN do in the Path field	**What you CANNOT do in the Path field**
- Paths work for *managed storage* ONLY - Since managed storage includes Team Folders, you CAN add a path to a Team Folder - A Path takes the form of: /username/sub-folder - You can add more than 1 path - You can set BOTH a path and specify metadata	- You CANNOT add a path to *network folders* - You CANNOT add a path to *external folders* - You CANNOT add a path to *shared folders* - You CANNOT add a path to protected folders, such as /boot, /root, and /var in LINUX - You CANNOT edit a path. If you make a mistake, you must first remove the path and click Add to specify the correct path
- The full path must exist before the policy will be enforced When creating the policy the full path doesn't have to exist, however. At a minimum: - The first component of the path has to already exist / username/ - This means that the username or team folder has to already exist before you can save the policy	- You CANNOT specify a path that does not exist This will prevent you from saving the policy  ERROR 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

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

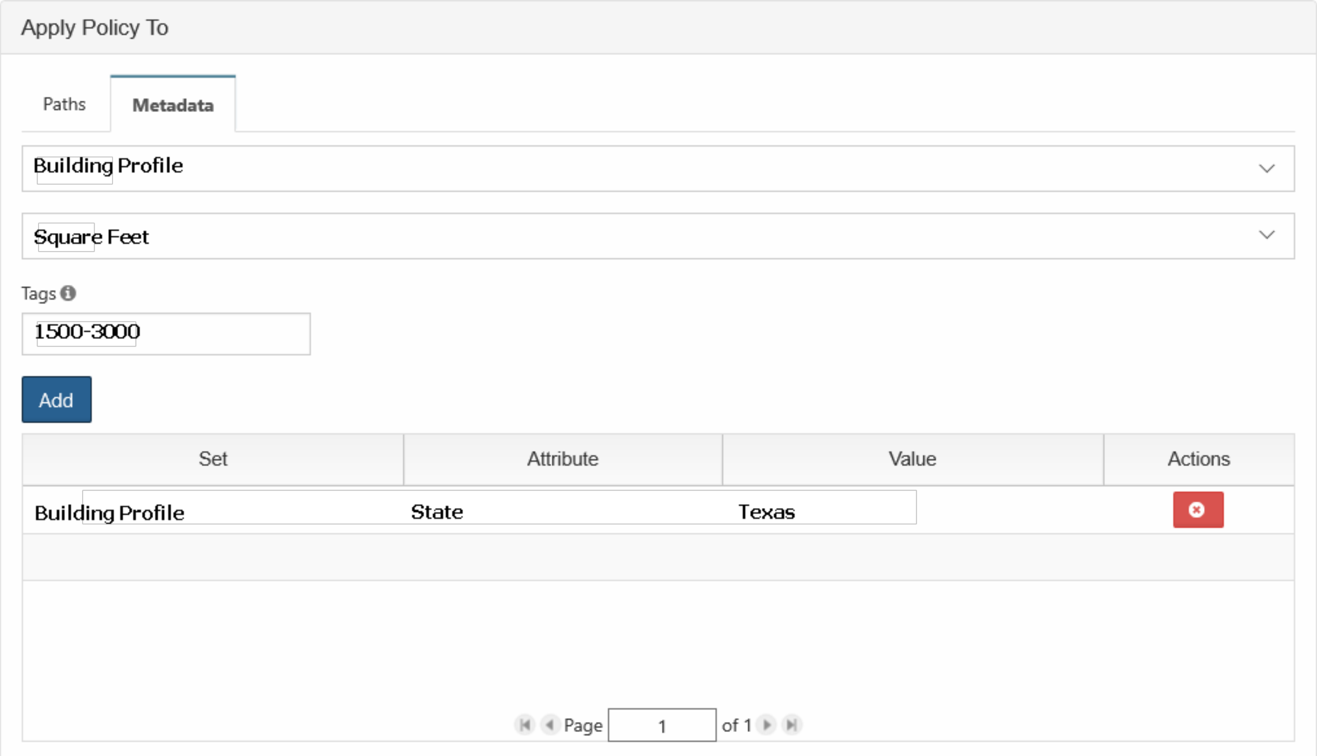
For more information about metadata, see Managing Metadata.

For example, The Cherry Road Brokerage company creates this custom metadata in FileCloud:

Term	Description	Cherry Road Example
Set	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 • Address • Photo • Square Feet • Leasing Status • Maintenance Status
Attribute	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 • State
Attribute	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 • Color
Attribute	A single piece of information that describes the File Object. In this example, The Cherry Road Brokerage company creates an attribute called *Square Feet* Two tags are also defined to allow for property searches by a range of square feet.	Square Feet • 0-1500 • 1500-3000

Term	Description	Cherry Road Example
Attribute	A single piece of information that describes the File Object. In this example, The Cherry Road Brokerage company creates an attribute called *Leasing Status* which identifies the building as occupied or vacant.	Leasing Status
Attribute	A single piece of information that describes the File Object. In this example, The Cherry Road Brokerage company creates an attribute called *Maintenance Status* which identifies the building as In Repair or No Repair.	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

Building Profile

Square Feet

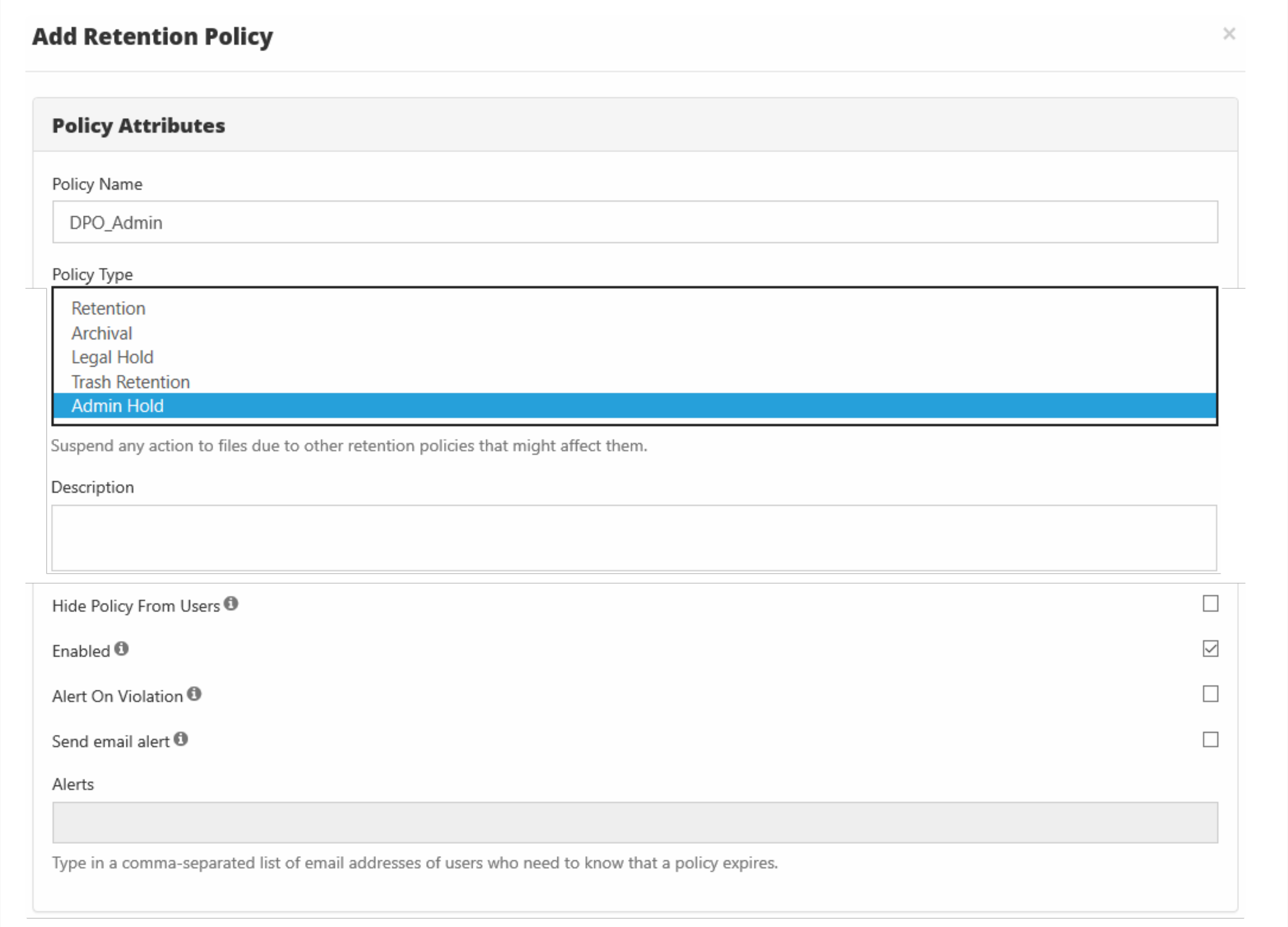
Tags

1500-3000

Set	Attribute	Value	Actions
Building Profile	State	Texas	⊗

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 (selected)

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	- Required - A string of characters, letters, and numbers that provide details about why the policy is necessary - This description is displayed in the User Portal when the cursor hovers over the Policy Name in the Details tab.

Property	Description
Hide Policy from Users	• Prevents policy details from being shown and leaked. • Selecting this option removes the display of applied policies and their expiration dates from the Details tab in the User Portal. • Selecting this option also blocks the API call to the backend to find out which policies are applied. This is how data leaks are prevented. • Although the policy name and expiration date are not shown, the restrictions are still enforced. For example, if the policy you are hiding from users prevents them from deleting the file, although the policy information is not shown, the user will not be able to delete the file. ⚠ Administrators need to be aware that users might report issues with the system when a retention policy is blocking their ability to access or delete a file or folder. The user will not be aware of why certain options are greyed out if they don't see the policy restrictions listed. However, if the user is able to select the option and it is restricted by a policy, they will see an error message telling them why when they try to select the option.
Alert on Violation	Displays an alert in the Admin portal on the Governance dashboard. ⚠ Administrators need to be aware that not all violations are logged here. The reason for this is that all permissions for a file are collected in one file- including user permissions and sharing permissions. In some cases, a sharing permission that was set first might stop a file from being deleted before a retention policy that was added later. The reason why the file cannot be deleted, or which set of permissions or policy is stopping the deletion, is not FileCloud's main priority. FileCloud's main concern is protecting the file and finding out if it cannot be deleted. This is why you might not always see a violation in the Dashboard, but the file will always be protected. If a user is constantly trying to delete a file that is protected by a retention policy then the chances of seeing the violation in the Governance Dashboard increase.
Send email alert	Notifies all provided recipients that there are only 7 days until the policy expires. ℹ The same information is available on the Governance dashboard. The Governance Dashboard list each file individually, and displays the date and time when a policy will expire so the Admin knows and can take action if any is needed.
Alerts	A list of email addresses separated by a comma who will receive the email notification that there are only 7 days until the policy expires.

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

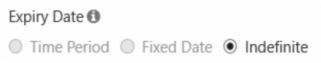
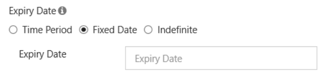
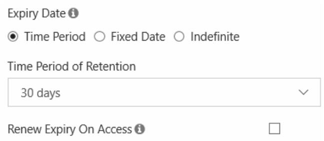
How Policy Lengths Differ

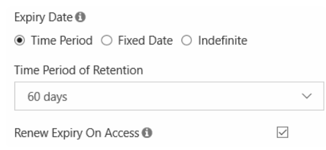
⚠ Any time you configure when a policy should expire, keep in mind that all expiration dates are dictated by when the next Cron job is run.

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:

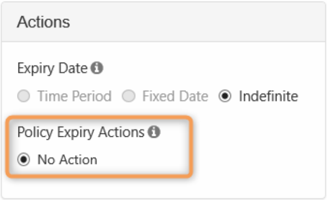
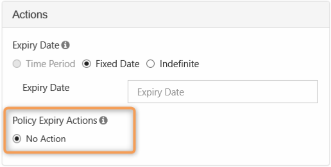
Policy Length	**Available on Types**	**Description**	
Indefinite	• Admin Hold • Legal Hold • Retention • Trash Retention	A policy never expires. For example, if you are required to retain accounting records for the entire length of your company's existence, you can never delete your accounting records	 Expiry Date ○ Time Period ○ Fixed Date ● Indefinite
Fixed Date	• Legal Hold • Archival • Retention • Trash Retention	The date a policy expires with no exceptions. This means you are locked out of the policy at 11:59:59 PM on that calendar date. Policy expiration is end of day (midnight), UTC adjusted. The ACTUAL expire time is the time of the next Cron run. • If the next Crom run isn't for another 24 hours, the policy will expire 24 hours later at midnight • If you want the policy to expire exactly at midnight, you can always force a Cron run	 Expiry Date ○ Time Period ● Fixed Date ○ Indefinite Expiry Date: Expiry Date
Time Period - not Renewed on Access	• Archival • Retention • Trash Retention	A set number of days or years that is used to calculate when the policy expires based on the creation date. 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. You can select from: • 30 days • 60 days • 90 days • 1 year • 2 years • Custom	 Expiry Date ● Time Period ○ Fixed Date ○ Indefinite Time Period of Retention: 30 days Renew Expiry On Access □

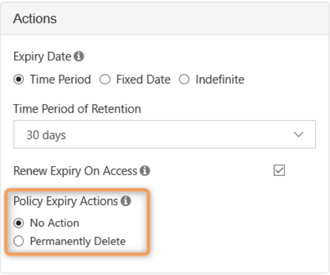
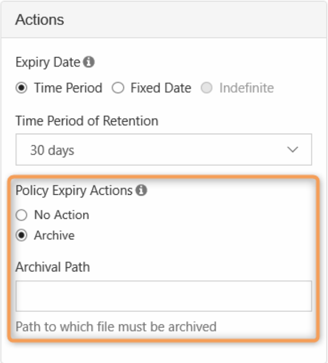
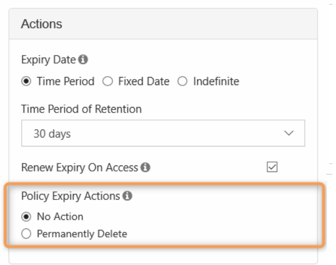
Policy Length	Available on Types	Description	
Time Period - Renewed on Access	- Archive - Retention - Trash Retention	A set number of days or years that is used to calculate when the policy expires based on the last access date. For example, if on March 2, 2019, for an X-ray, you set expiry to: - Time Period = 60 days - Renew on Access = selected Then the policy will expire on May 2, 2019 UNLESS: - If a doctor previews the file before May 2, say on May 1, 2019 Then the 60-day time period will be reset to July 1, 2019. The ACTUAL date is reset by a user every time they access the file.	 Expiry Date ● Time Period ○ Fixed Date ○ Indefinite Time Period of Retention 60 days Renew Expiry On Access ☑

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	 Actions Expiry Date ℹ ○ Time Period ○ Fixed Date ● Indefinite Policy Expiry Actions ℹ ● No Action	An administrative hold is designed to help an administrator block access to files and folders so that they can determine what should happen next. ℹ 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 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.
Legal Hold	 Actions Expiry Date ℹ ○ Time Period ● Fixed Date ○ Indefinite Expiry Date: Expiry Date Policy Expiry Actions ℹ ● No Action	A Legal Hold is designed to retain data, therefore, there is no deletion or move option available when the policy expires. ⚠ Legal Holds cannot be reversed once applied unless they are set to expire after a fixed number of days

Policy Type	Expiration Actions	Notes
Retention	 Actions Expiry Date ● Time Period ○ Fixed Date ○ Indefinite Time Period of Retention 30 days Renew Expiry On Access ☑ Policy Expiry Actions ● No Action ○ Permanently Delete	Retention policies are designed to keep digital content around for a specified amount of time. When a retention policy expires, it can automatically: • Allow users to access the files again and delete them if they want (No Action) • Delete all the files that have this policy attached from the system, without retaining them in the Trash bin (Permanently Delete) ⚠ Retention policies cannot be reversed once applied
Archival	 Actions Expiry Date ● Time Period ○ Fixed Date ○ Indefinite Time Period of Retention 30 days Policy Expiry Actions ○ No Action ● Archive Archival Path Path to which file must be archived	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) 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.
Trash Retention	 Actions Expiry Date ● Time Period ○ Fixed Date ○ Indefinite Time Period of Retention 30 days Renew Expiry On Access ☑ Policy Expiry Actions ● No Action ○ Permanently Delete	The Trash Retention policy is designed to help you control if files in the Trash Bin can be permanently deleted from FileCloud. • You can allow the policy to automatically and permanently delete all files in the Trash bin when the policy expires • 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

Policy Types Cheat Sheet

An as 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
Admin Hold	1 • Outranks all other policies • Is outranked by no other policy	• Prevents any update or delete of digital content for an indefinite period of time • Admin Hold policies applied to folders can be removed • Admin policies applied to files can be removed Create an Admin Hold policy
Legal Hold	2 • Outranks policies 3,4,5,6,7 • Is outranked by Admin Hold	• Freezes digital content to aid discovery or legal challenges • During a legal hold, file modifications are not allowed • Holds cannot be reversed once applied Create a Legal Hold policy
Retention - Indefinite	3 • Outranks policies 4,5,6,7 • Is outranked by Admin and Legal Holds	• Allows an organization to identify specific content that is required to be stored for a specific period of time before it can be disposed. • During the retention period, the content cannot be deleted. • Retention - Indefinite keeps the content indefinitely • Retention policies cannot be reversed once applied Create a Retention policy
Archival	4 • Outranks policies 5,6,7 • Is outranked by Admin Hold • Is outranked by Legal Hold • Is outranked by Retention -Indefinite	• Moves and stores old organizational content, for example, to a more cost effective systems for long term • No Deletion is allowed until a specific time period is reached • After the specified time period is reached, content gets moved to a specific folder or location Create an Archival policy

Policy Type	Rank	Description
Retention - No delete on expiry	5 - Outranks policies 6 and 7 - Is outranked by Admin Hold - Is outranked by Legal Hold - Is outranked by Retention - Indefinite - Is outranked by Archival	- Allows an organization to identify specific content that is required to be stored for a specific period of time before it can be disposed. - During the retention period, the content cannot be deleted. - Retention - No delete on expiry doesn't delete the content upon policy expiration - Retention policies cannot be reversed once applied Create a Retention policy
Retention - Delete on expiry	6 - Outranks policy 7 - Is outranked by Admin Hold - Is outranked by Legal Hold - Is outranked by Retention - Indefinite - Is outranked by Archival - Is outranked by Retention - No delete on expiry	- 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 - Delete on expiry deletes the content upon policy expiration - Retention policies cannot be reversed once applied Create a Retention policy
Trash Retention	7 - Outranks no other policies - Is outranked by all other policies	- Controls if files can permanently be deleted completely from FileCloud - Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions Create a Trash Retention policy

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.

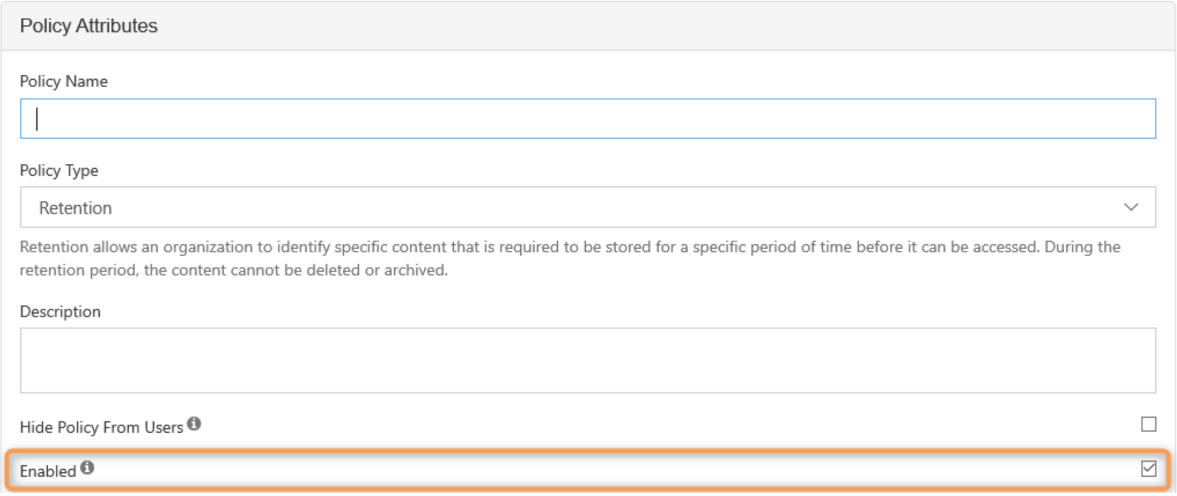
This setting determines whether new files and folders that meet ANY of the policy conditions will have the policy assigned.

✓ If enabled, the policy is assigned to files and folders

⛔ If not enabled, FileCloud will:

1. Stop applying the policy to new file objects
2. Keep the policy in place for file objects already attached

The Enabled Setting



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

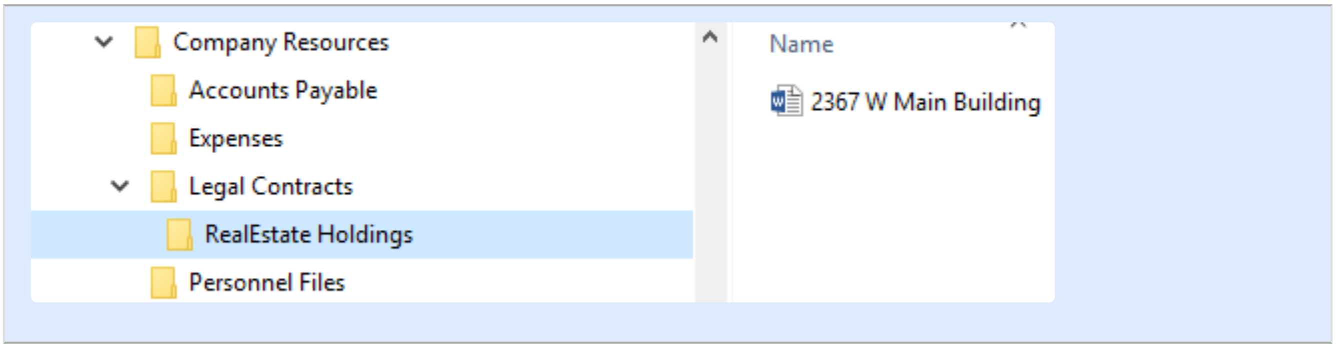
Hide Policy From Users ℹ □

Enabled ℹ ☑

- 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:



Company Resources
Accounts Payable
Expenses
Legal Contracts
RealEstate Holdings
Personnel Files

Name
2367 W Main Building

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?

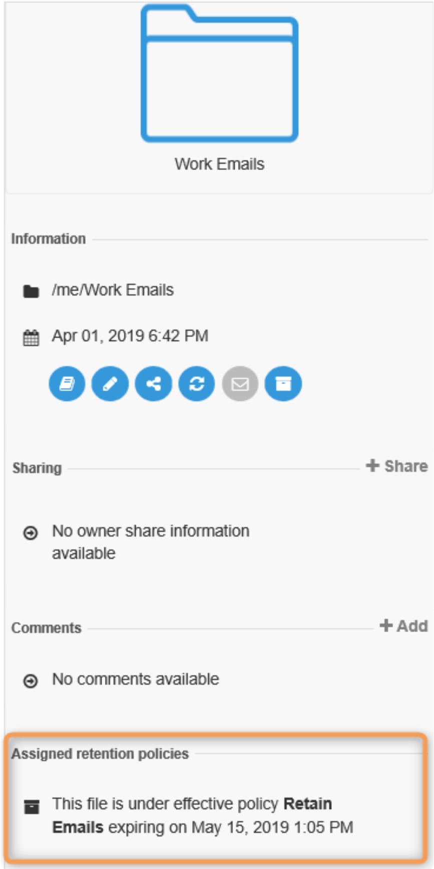
1. A new file called 98675 E Orchard Drive is added to the RealEstate Holdings folder, and the retention policy is NOT applied.
2. Since the new file, 98675 E Orchard Drive does not have the retention policy applied, it CAN be deleted.
3. However, the 2367 W Main Building file still has the policy applied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



Work Emails

Information

/me/Work Emails

Apr 01, 2019 6:42 PM

Sharing — + Share

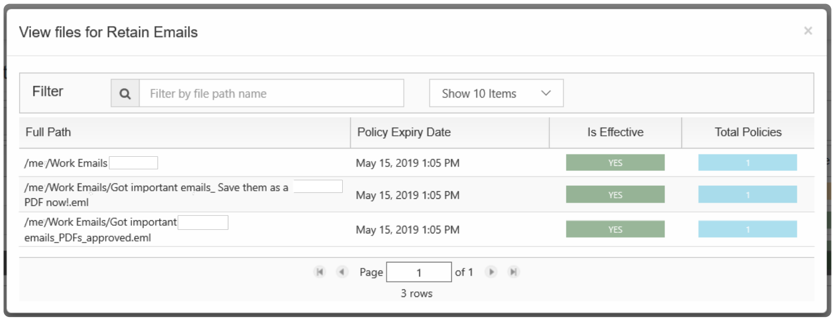
No owner share information available

Comments — + Add

No comments available

Assigned retention policies

This file is under effective policy **Retain Emails** expiring on May 15, 2019 1:05 PM



View files for Retain Emails

Filter: Filter by file path name — Show 10 Items

Full Path	Policy Expiry Date	Is Effective	Total Policies
/me /Work Emails	May 15, 2019 1:05 PM	YES	1
/me /Work Emails/Got important emails_ Save them as a PDF now!.eml	May 15, 2019 1:05 PM	YES	1
/me /Work Emails/Got important emails_PDFs_approved.eml	May 15, 2019 1:05 PM	YES	1

Page 1 of 1

3 rows

When using the Admin portal, you will need to know the name of the policy that the file belongs to.

Then you can view all files for the policy to check if it is attached.

1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Retention*.
3. On the *Manage Retention Policies* screen, select the policy row.
4. In that row, click the *Edit Policy* icon (✎).
5. Clear the checkbox for *Hide Policy from Users*.
6. Log in to the *User Portal*.
7. Browse to the file.
8. Look in the *Details* tab for the *Assigned retention policies*.

1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Retention*.
3. On the *Manage Retention Policies* screen, select the policy row.
4. In that row, click the *View Files* icon (☰).
5. The View files for the policy screen displays.

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	1. Admin Hold - until it is removed 2. Legal Hold - set to never expire 3. Retention with Deletion - will never take effect unless the Legal Hold is removed by the admin

	No	No	Yes expires = 90 days Renew on Access is not selected	Yes expires = 30 days	No	No	1. Retention No Deletion until it expires in 90 days 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
	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	1. Admin Hold - until it is removed 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 3. Trash Bin Retention - permanently deletes files off the system when the Retention with Deletion policy actually expires

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.

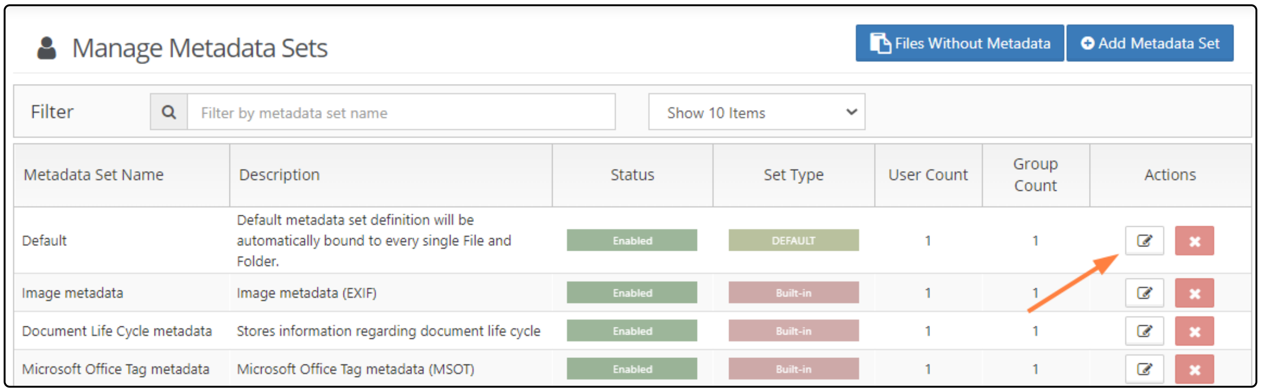
To use this method, you can take advantage of the fact that the Default metadata set is applied to every file, and add an attribute to the metadata set that will always be set to a certain value.

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.

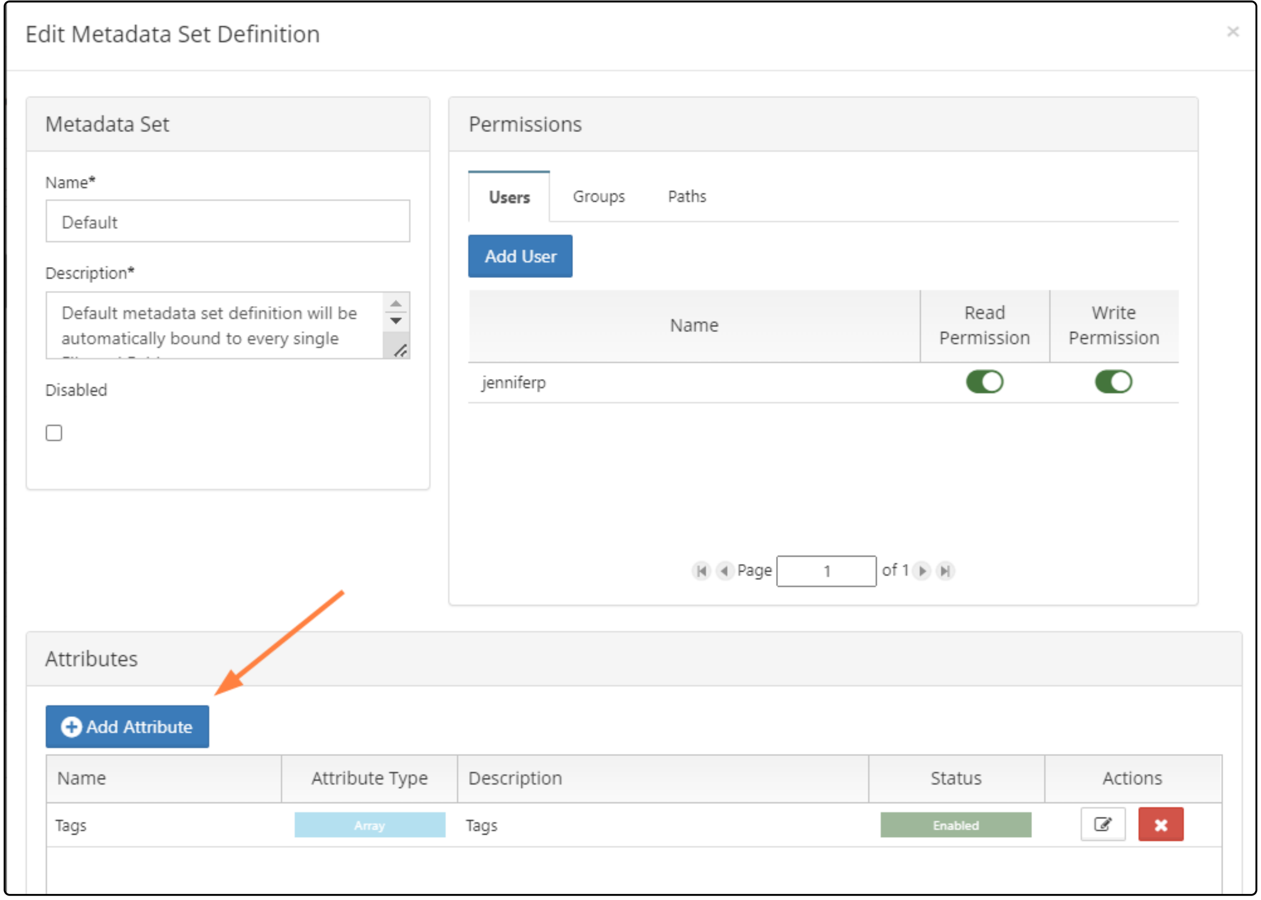
1. In the admin portal navigation pane, click **Metadata**.
   The **Manage Metadata Sets** screen opens.

2. Click the **Edit** icon for the **Default** metadata set.



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**.



Name*: Default

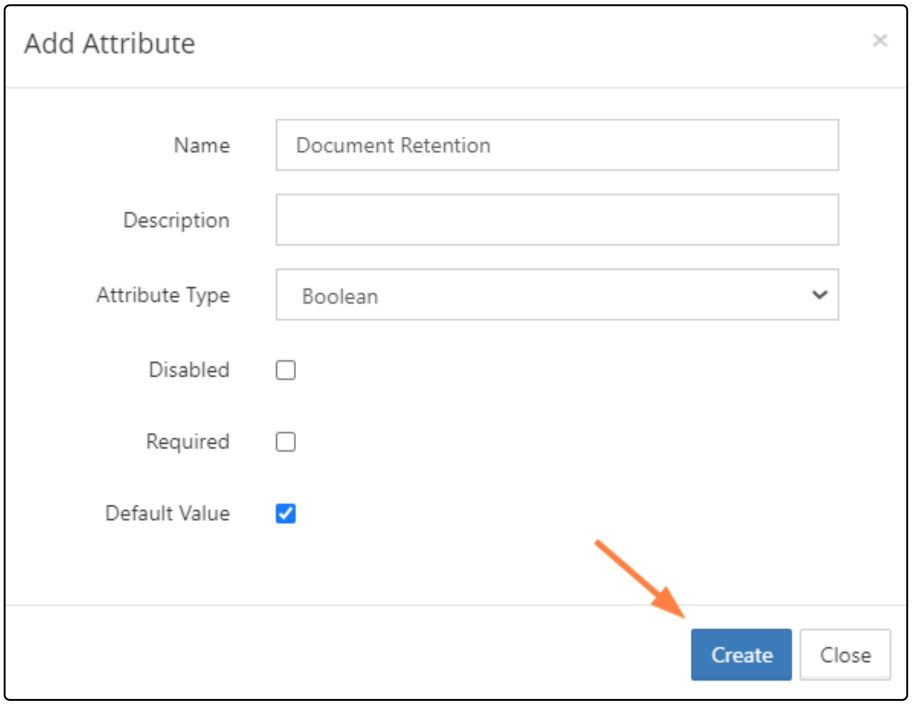
Description*: Default metadata set definition will be automatically bound to every single

Disabled ☐

Name	Read Permission	Write Permission
jenniferp	●	●

Name	Attribute Type	Description	Status	Actions
Tags	Array	Tags	Enabled	

4. 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**.
5. 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 □

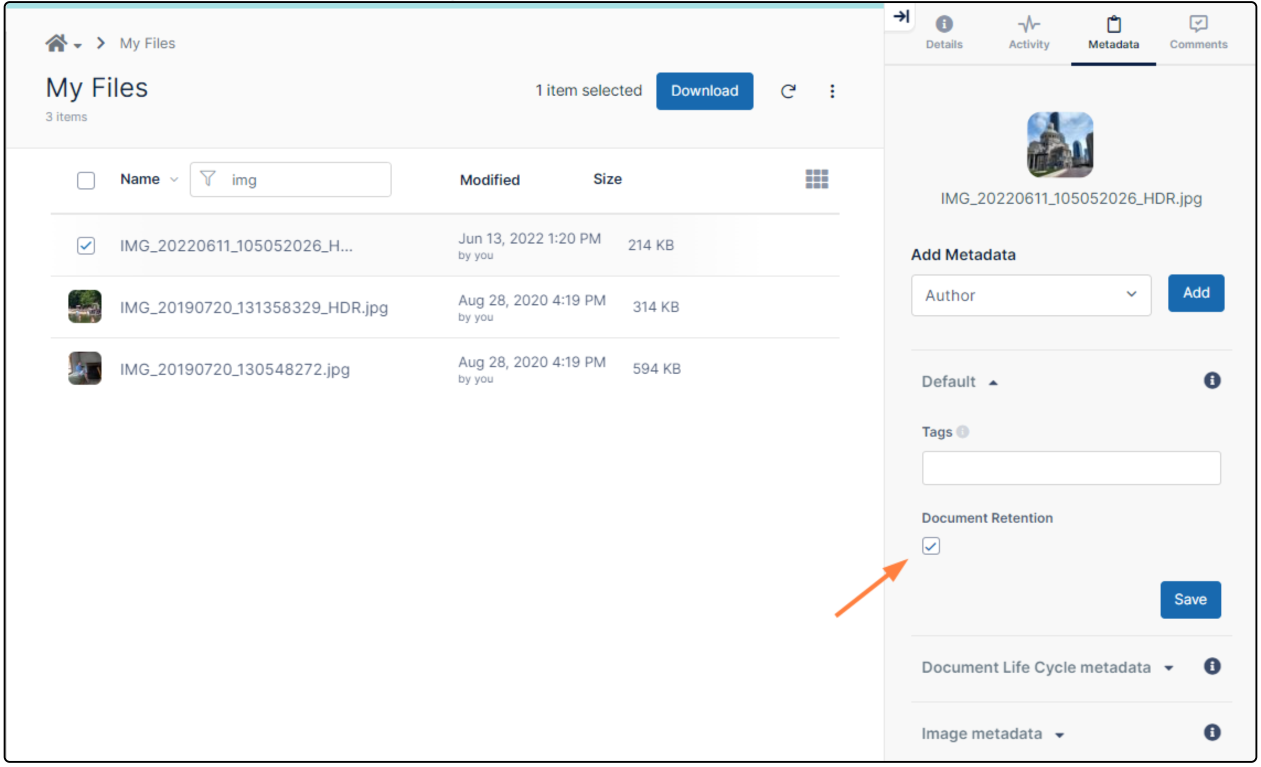
Required □

Default Value ☑

Create | 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**.



My Files

My Files

3 items

1 item selected | Download

□	Name	Modified	Size
☑	IMG_20220611_105052026_H...	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

Details | Activity | Metadata | Comments

IMG_20220611_105052026_HDR.jpg

Add Metadata

Author | Add

Default

Tags

Document Retention

☑

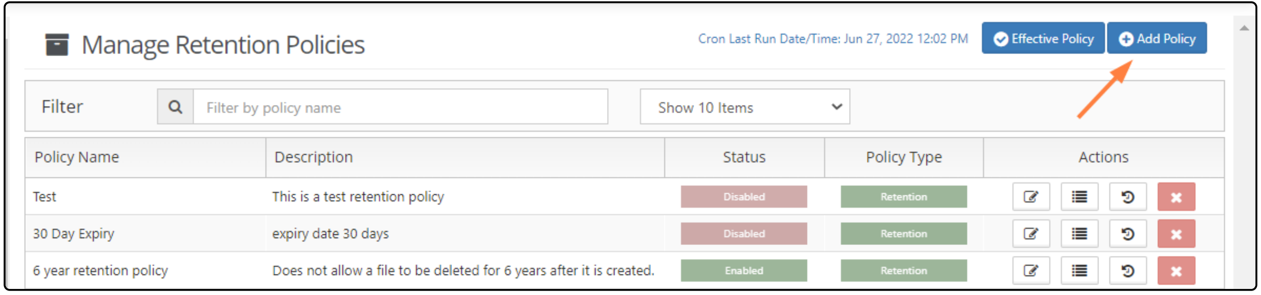
Save

Document Life Cycle metadata

Image metadata

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**.



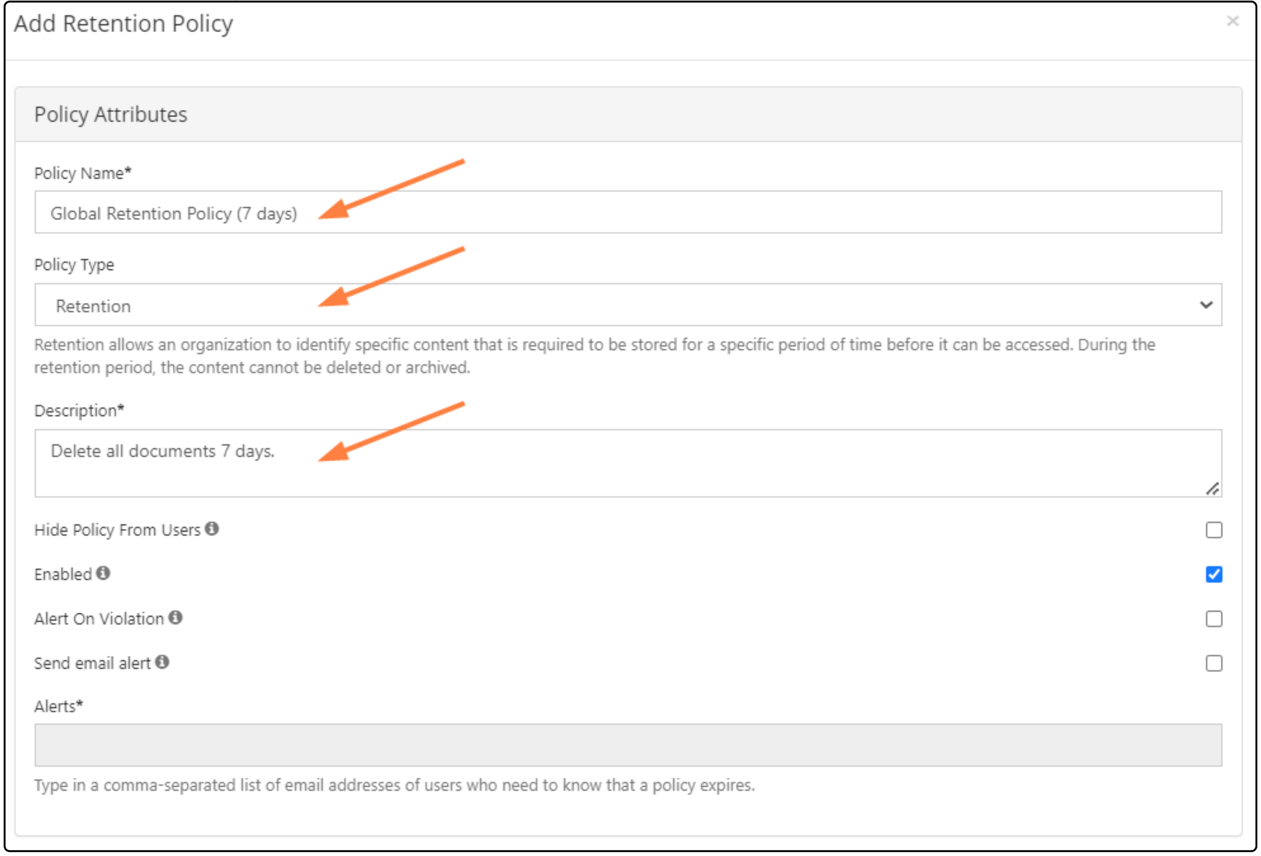
Manage Retention Policies

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

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 retention policy	Does not allow a file to be deleted for 6 years after it is created.	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**.



Add Retention Policy

Policy Attributes

Policy Name*
Global Retention Policy (7 days)

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*
Delete all documents 7 days.

Hide Policy From Users ☐

Enabled ☑

Alert On Violation ☐

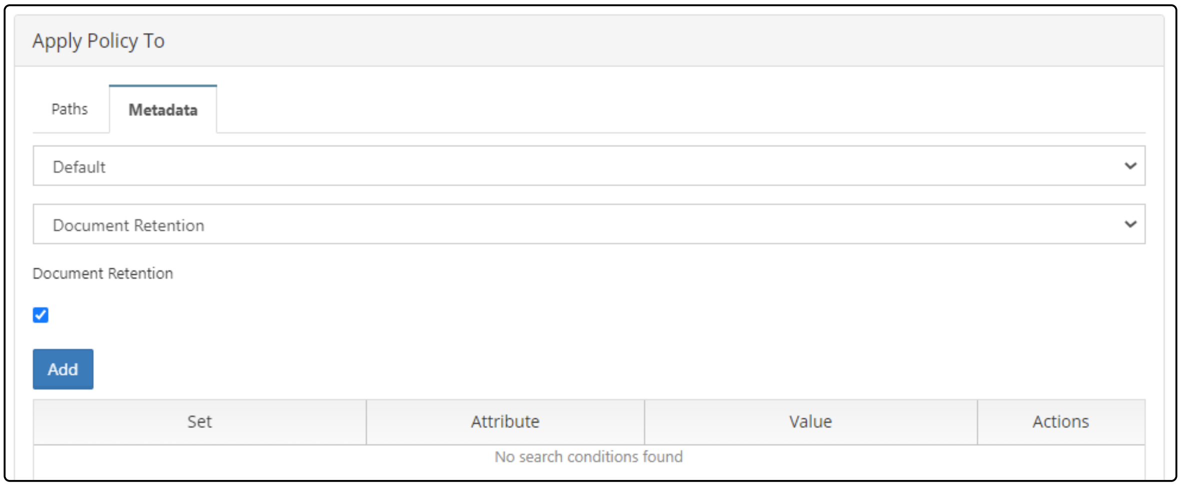
Send email alert ☐

Alerts*

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

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

Default

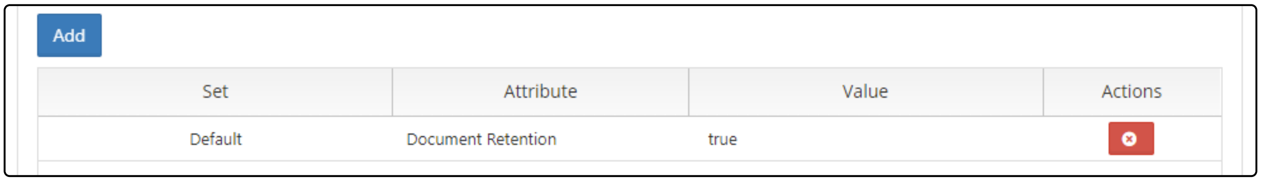
Document Retention

Document Retention

☑

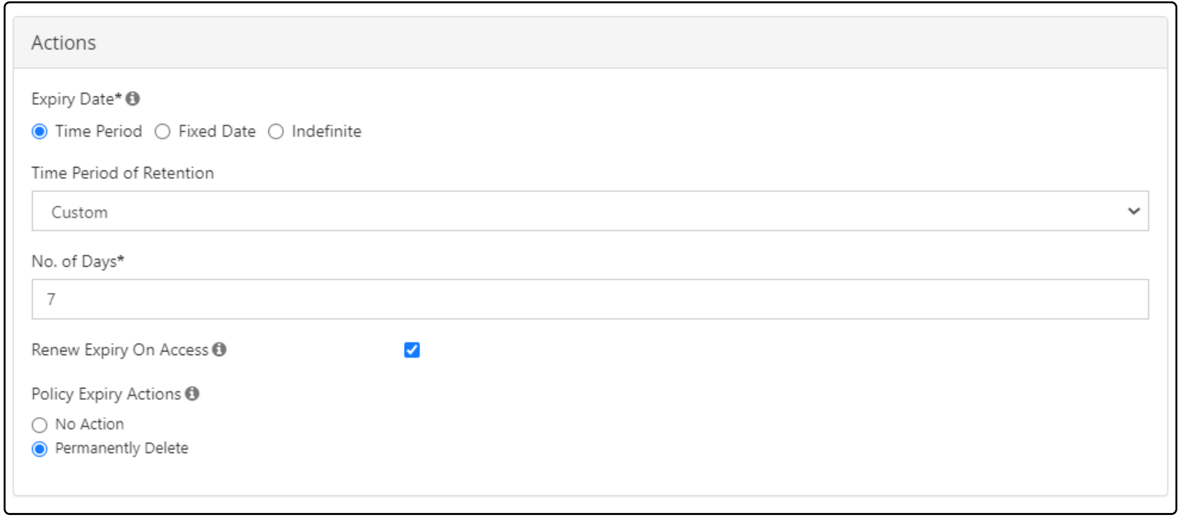
Set	Attribute	Value	Actions
No search conditions found			

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.
   a. 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.
   b. Since a preset option of 7 days does not exist, in **Time Period of Retention** choose **Custom**, and in **No. of Days**, choose **7**.
   c. In **Policy Expiry Options**, choose **Permanently Delete**.



Actions

Expiry Date* ℹ
● Time Period ○ Fixed Date ○ Indefinite

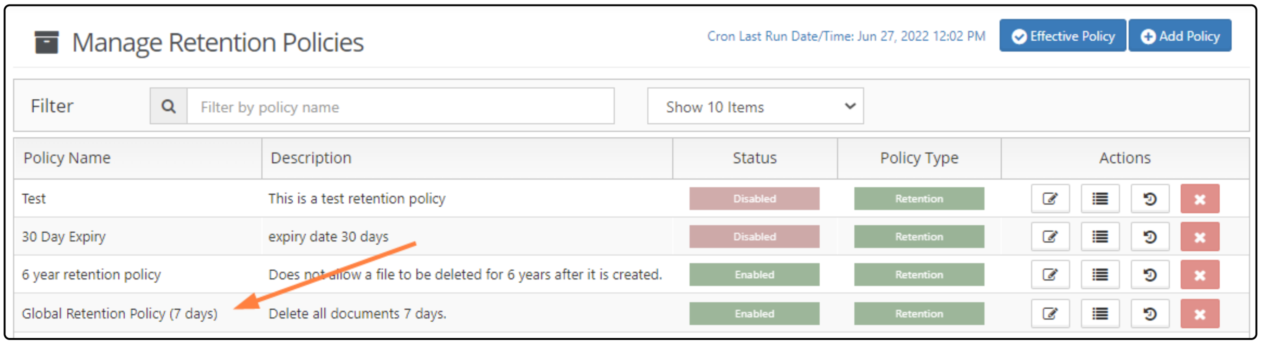
Time Period of Retention
Custom

No. of Days*
7

Renew Expiry On Access ℹ ☑

Policy Expiry Actions ℹ
○ No Action
● Permanently Delete

13. Click **Save**.

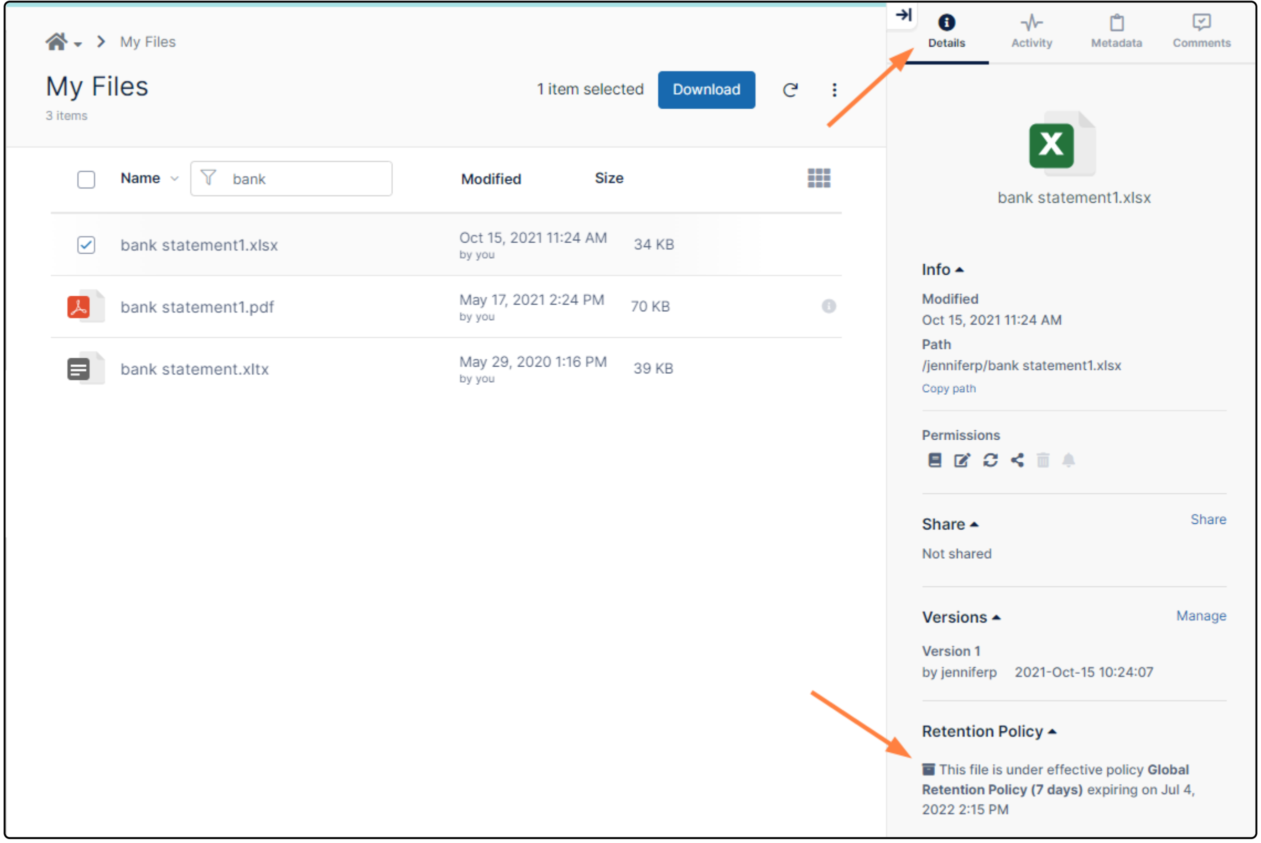


Manage Retention Policies

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

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 retention policy	Does not allow a file to be deleted for 6 years after it is created.	Enabled	Retention	
Global Retention Policy (7 days)	Delete all documents 7 days.	Enabled	Retention	

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.



My Files

3 items

1 item selected

Name	Modified	Size
☑ bank statement1.xlsx	Oct 15, 2021 11:24 AM by you	34 KB
bank statement1.pdf	May 17, 2021 2:24 PM by you	70 KB
bank statement.xltx	May 29, 2020 1:16 PM by you	39 KB

bank statement1.xlsx

Info

Modified
Oct 15, 2021 11:24 AM

Path
/jenniferp/bank statement1.xlsx

Copy path

Permissions

Share — Share

Not shared

Versions — Manage

Version 1
by jenniferp 2021-Oct-15 10:24:07

Retention Policy

This file is under effective policy **Global Retention Policy (7 days)** expiring on Jul 4, 2022 2:15 PM

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.

> ℹ 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 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) system.

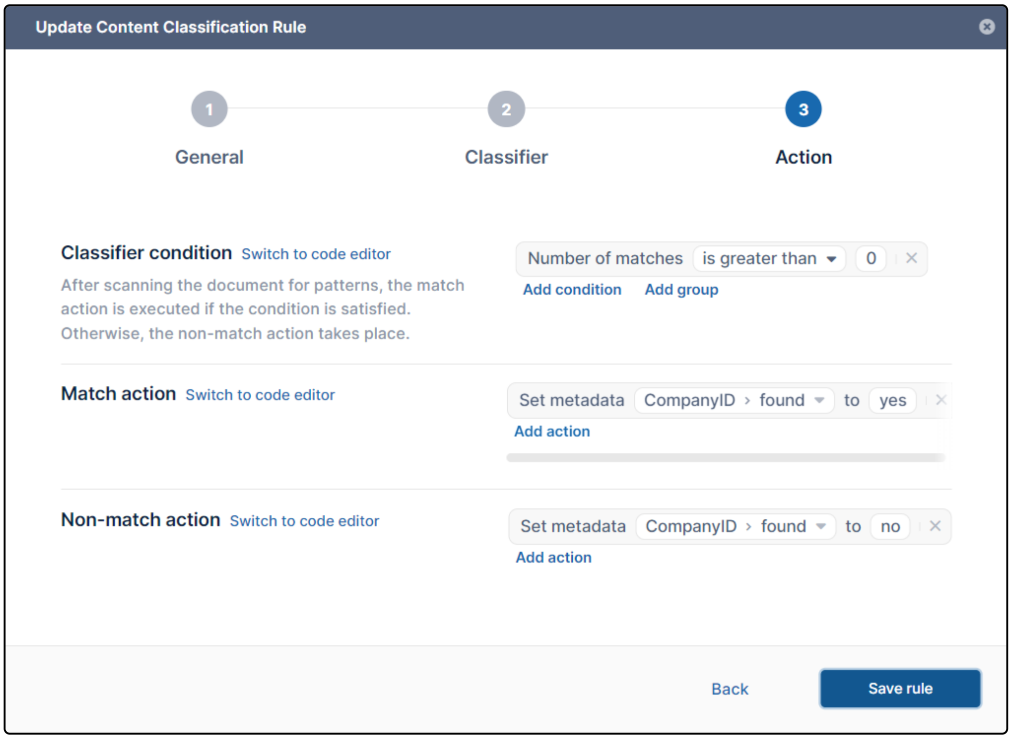
To use Smart Classification, set up rules that search for content in files and apply metadata to them depending on the search results. When rules are initially enabled, they apply to files added before the rules were created. After that, they apply to newly added and uploaded files.

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 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.



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

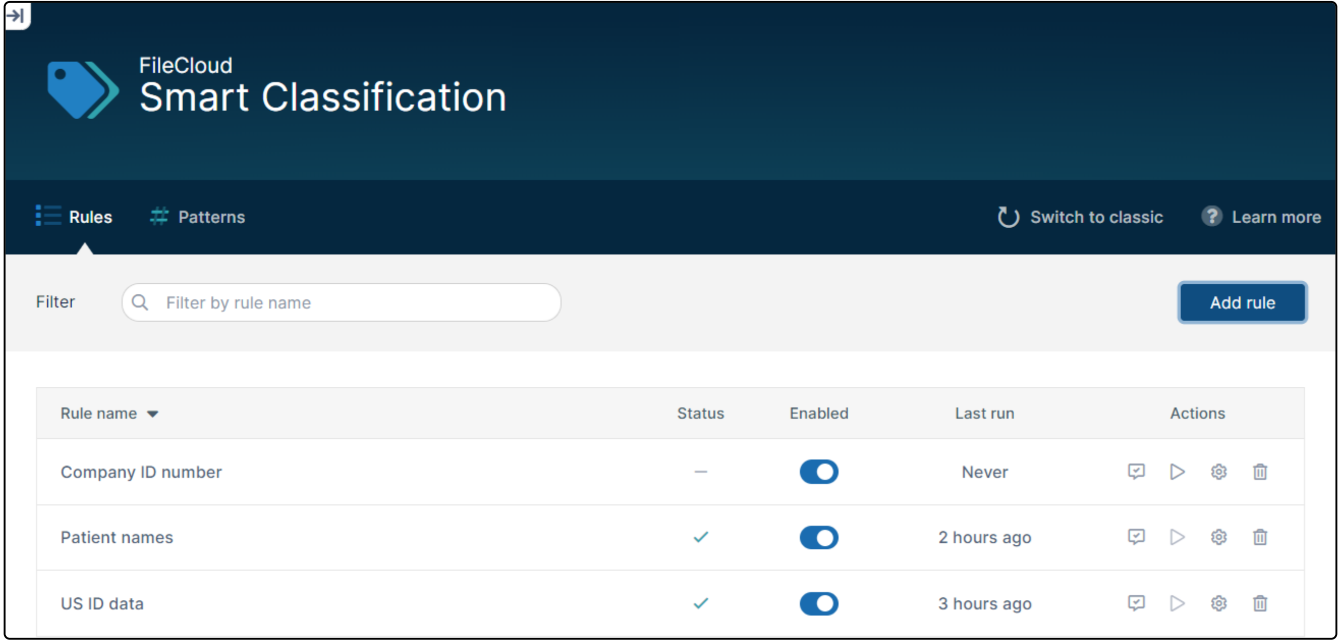
Add action

Non-match action Switch to code editor

Set metadata | CompanyID › found | to | no

Add action

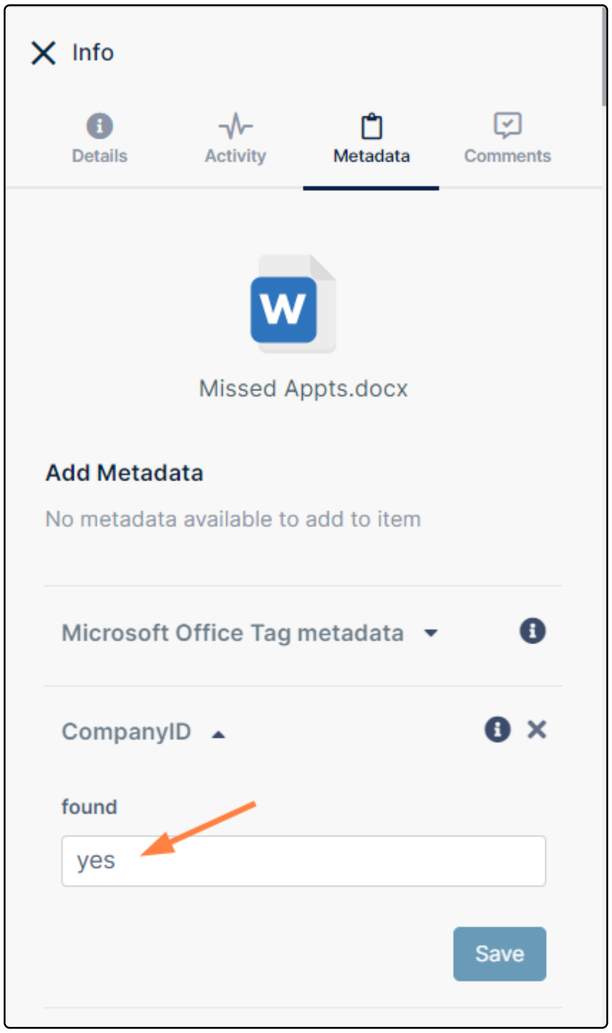
The saved rules appear in the Smart Classification screen.



FileCloud
Smart Classification

Rule name	Status	Enabled	Last run	Actions
Company ID number	–	●	Never	
Patient names	✓	●	2 hours ago	
US ID data	✓	●	3 hours ago	

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



Add Metadata

No metadata available to add to item

Microsoft Office Tag metadata

CompanyID

found: yes

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

- Smart classification will only function properly if Solr is configured in your system and your storage has been indexed.
- Since files greater than 10 MB cannot be indexed by Solr, 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

If you have not enabled Solr, enable it, and index your content before completing the following steps.

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, configure ICAP DLP integration in FileCloud.
3. If you plan to use the AI Classifier, 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.
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.
6. Create and Test Smart Classification Rules.
7. Schedule automatic running of Smart Classification Rules.
   See Setting Up a Cron Job or Scheduled Task for help.

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.

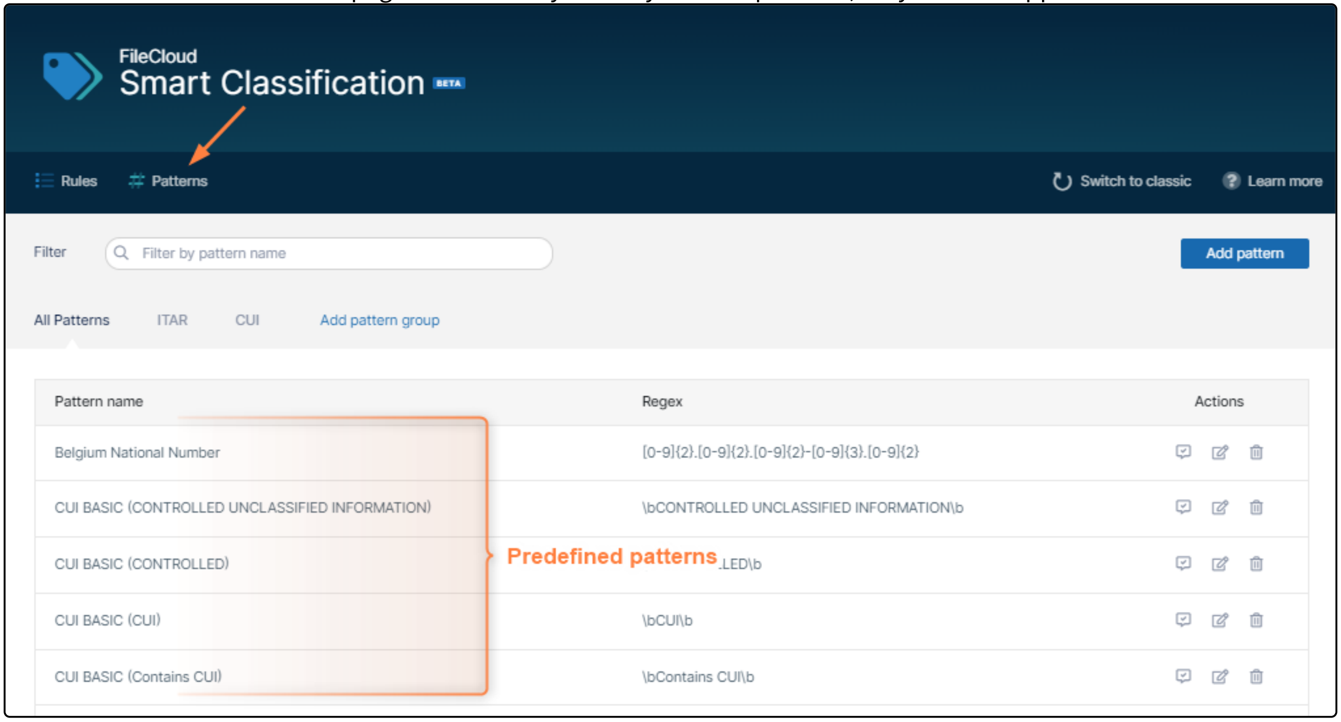
In a large number of cases, the patterns to be matched are expressed in regex format and locate common identification information such as national ID numbers. To make it easier for you to set up rules, Smart Classification has predefined a number of these commonly-used regex patterns.

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

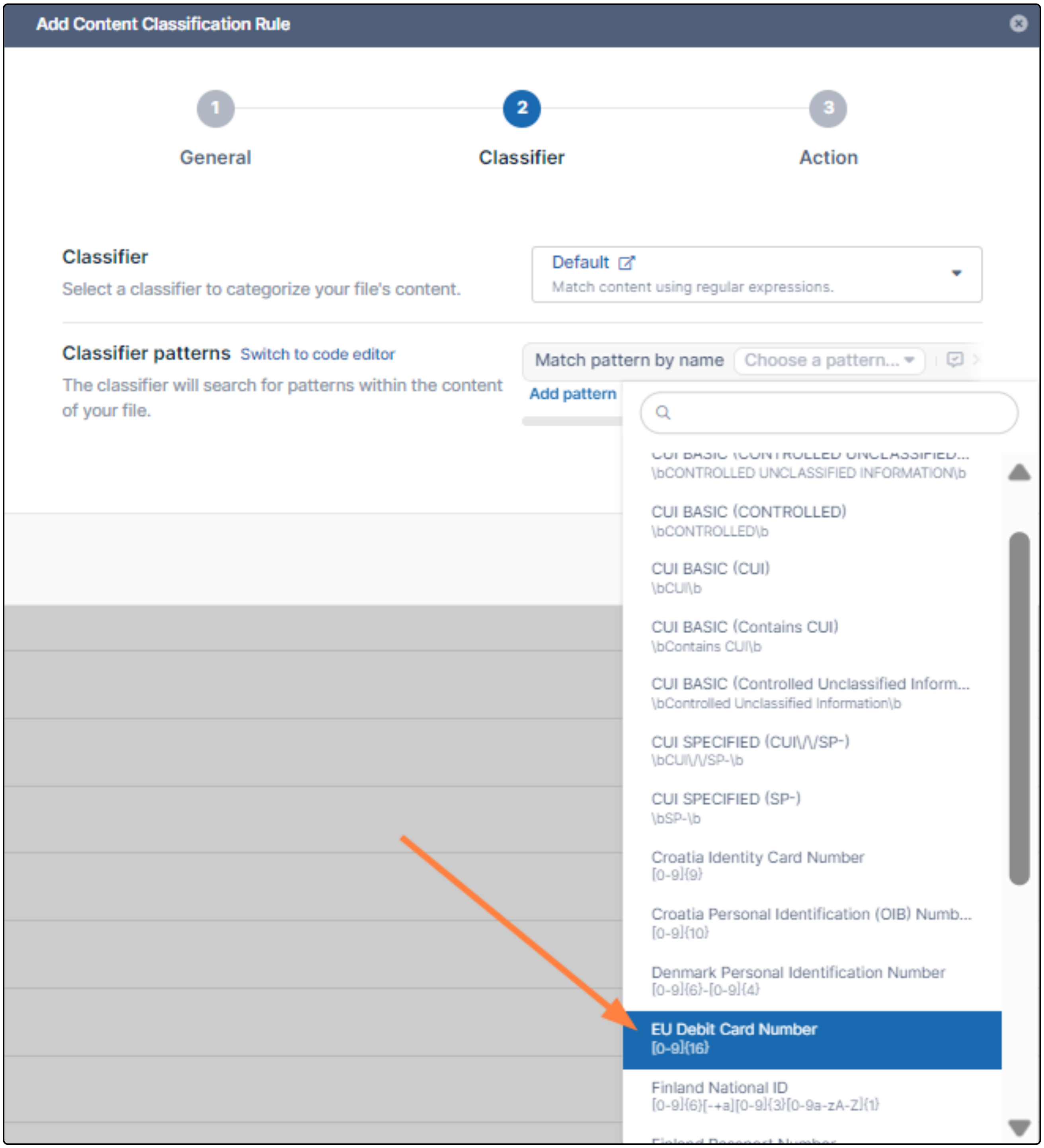
The predefined patterns in Smart Classification are all in regex format. You can view all of them by clicking the **Patterns** link in the **Smart Classification** page menu bar. If you add your own patterns, they will also appear here.



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)	LED\b	
CUI BASIC (CUI)	\bCUI\b	
CUI BASIC (Contains CUI)	\bContains CUI\b	

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.



Classifier
Select a classifier to categorize your file's content.

Default
Match content using regular expressions.

Classifier patterns Switch to code editor
The classifier will search for patterns within the content of your file.

Match pattern by name | Choose a pattern...

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}

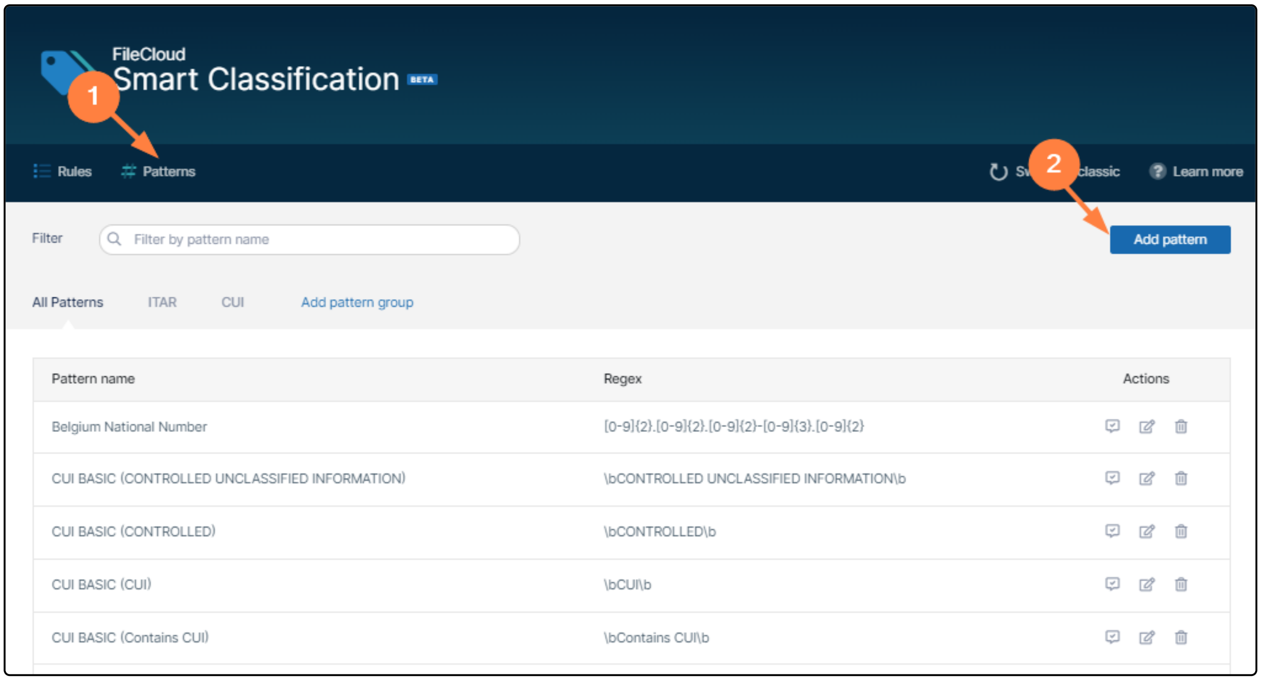
Finland Passport Number

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.

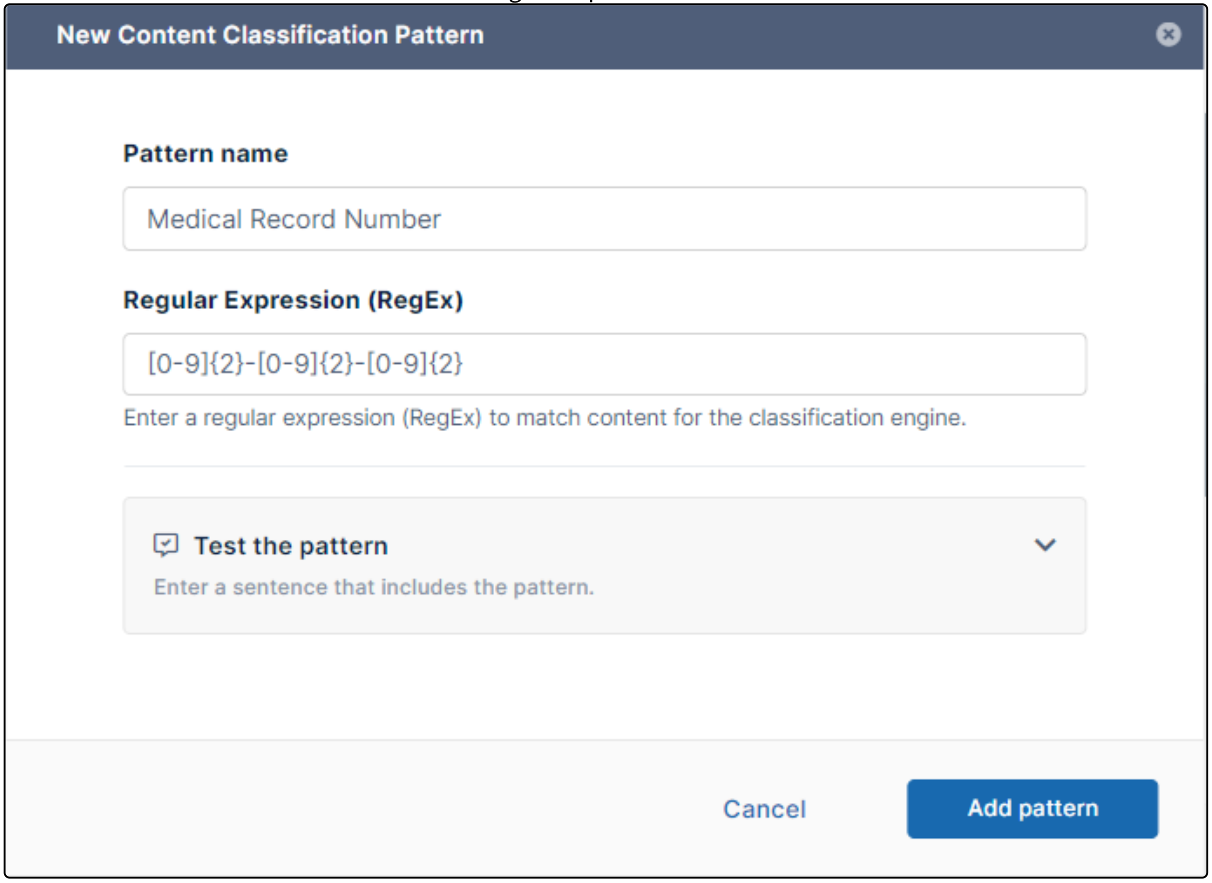
To create your own pattern:

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



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)	\bCONTROLLED\b	
CUI BASIC (CUI)	\bCUI\b	
CUI BASIC (Contains CUI)	\bContains CUI\b	

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



New Content Classification Pattern

Pattern name

Medical Record Number

Regular Expression (RegEx)

[0-9]{2}-[0-9]{2}-[0-9]{2}

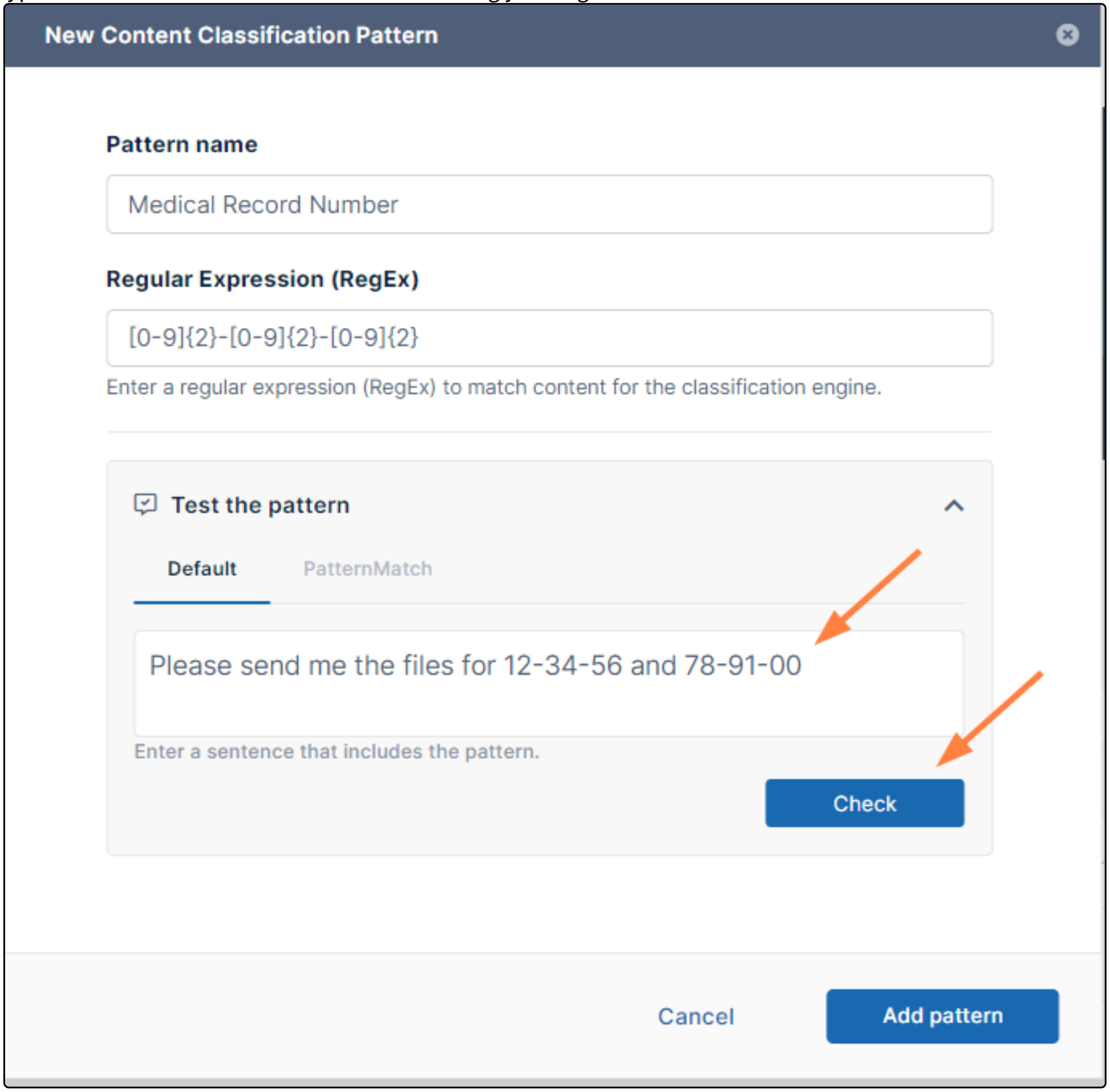
Enter a regular expression (RegEx) to match content for the classification engine.

Test the pattern

Enter a sentence that includes the pattern.

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

Medical Record Number

Regular Expression (RegEx)

[0-9]{2}-[0-9]{2}-[0-9]{2}

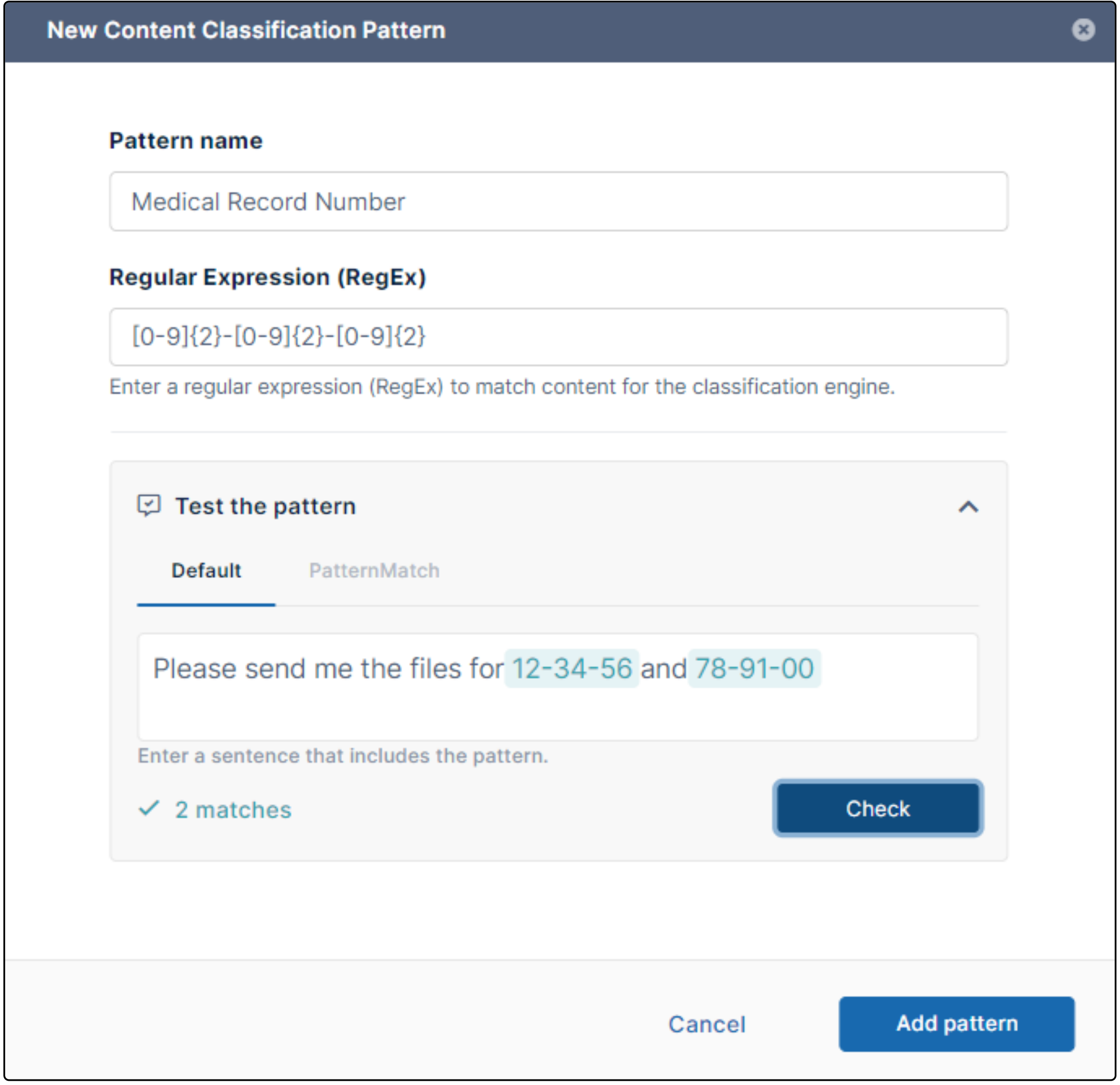
Enter a regular expression (RegEx) to match content for the classification engine.

Test the pattern

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

Enter a sentence that includes the 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.

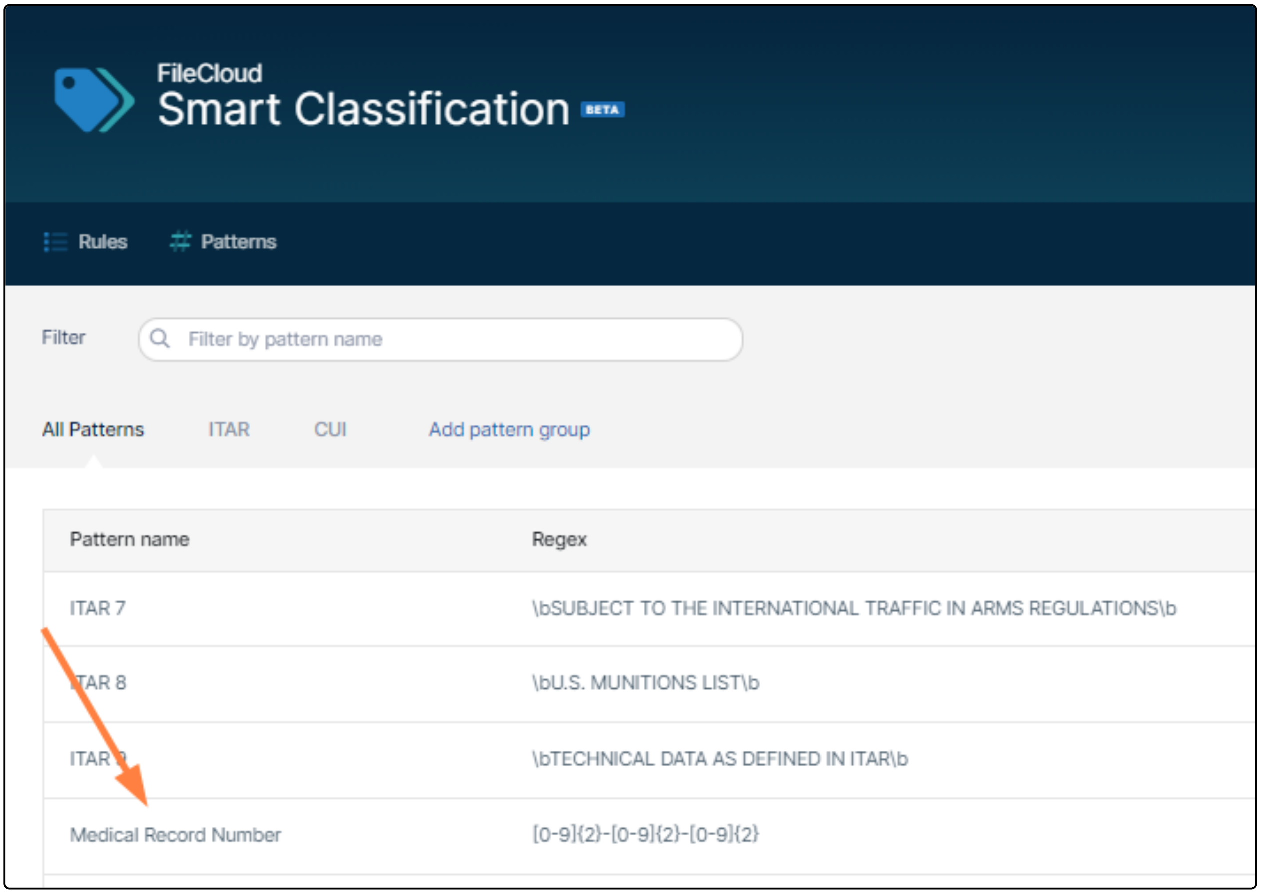
Test the pattern

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

Enter a sentence that includes the pattern.

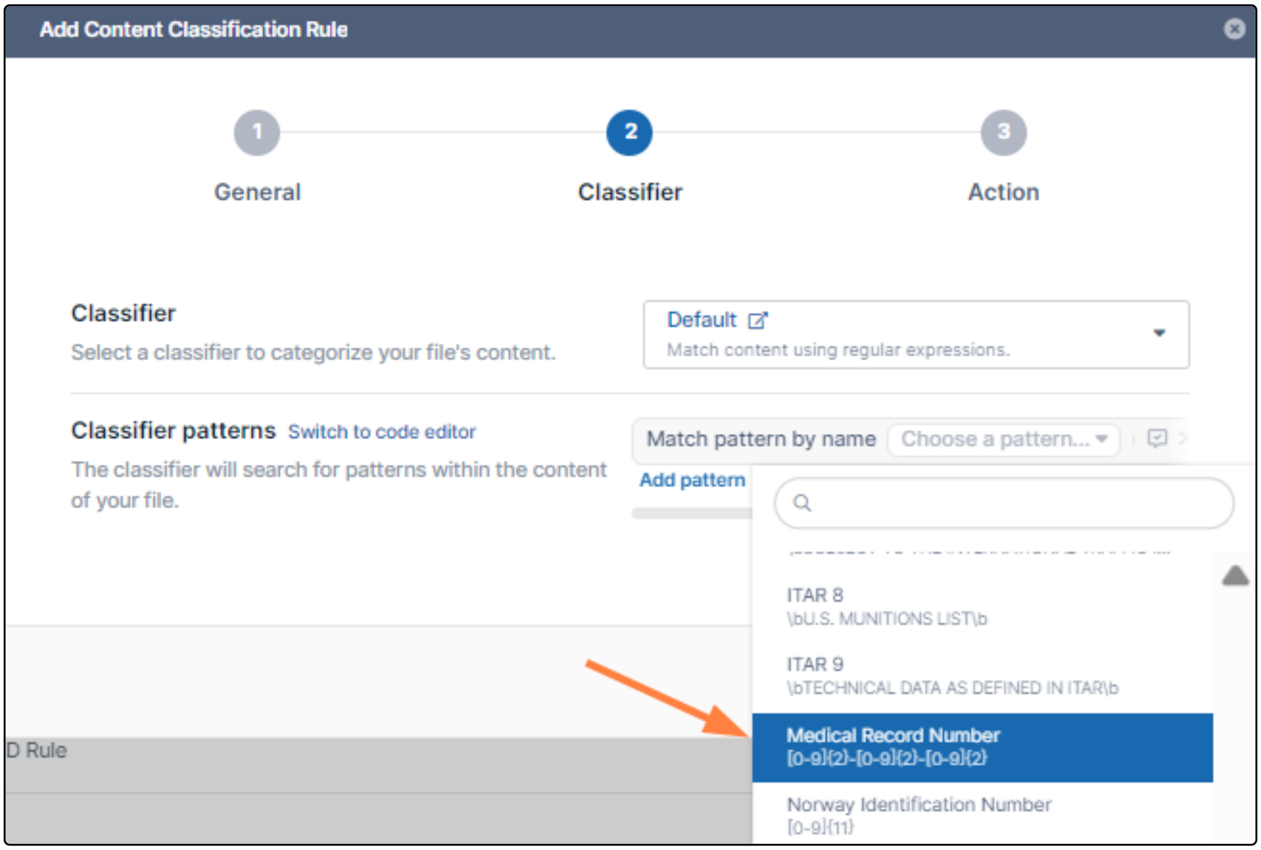
✓ 2 matches

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**.



Pattern name	Regex
ITAR 7	\bSUBJECT TO THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS\b
ITAR 8	\bU.S. MUNITIONS LIST\b
ITAR 9	\bTECHNICAL 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.



Add Content Classification Rule

Classifier

Select a classifier to categorize your file's content.

Default

Match content using regular expressions.

Classifier patterns Switch to code editor

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

Match pattern by name Choose a pattern...

Add pattern

ITAR 8
\bU.S. MUNITIONS LIST\b

ITAR 9
\bTECHNICAL DATA AS DEFINED IN ITAR\b

Medical Record Number
[0-9]{2}-[0-9]{2}-[0-9]{2}

Norway Identification Number
[0-9]{11}

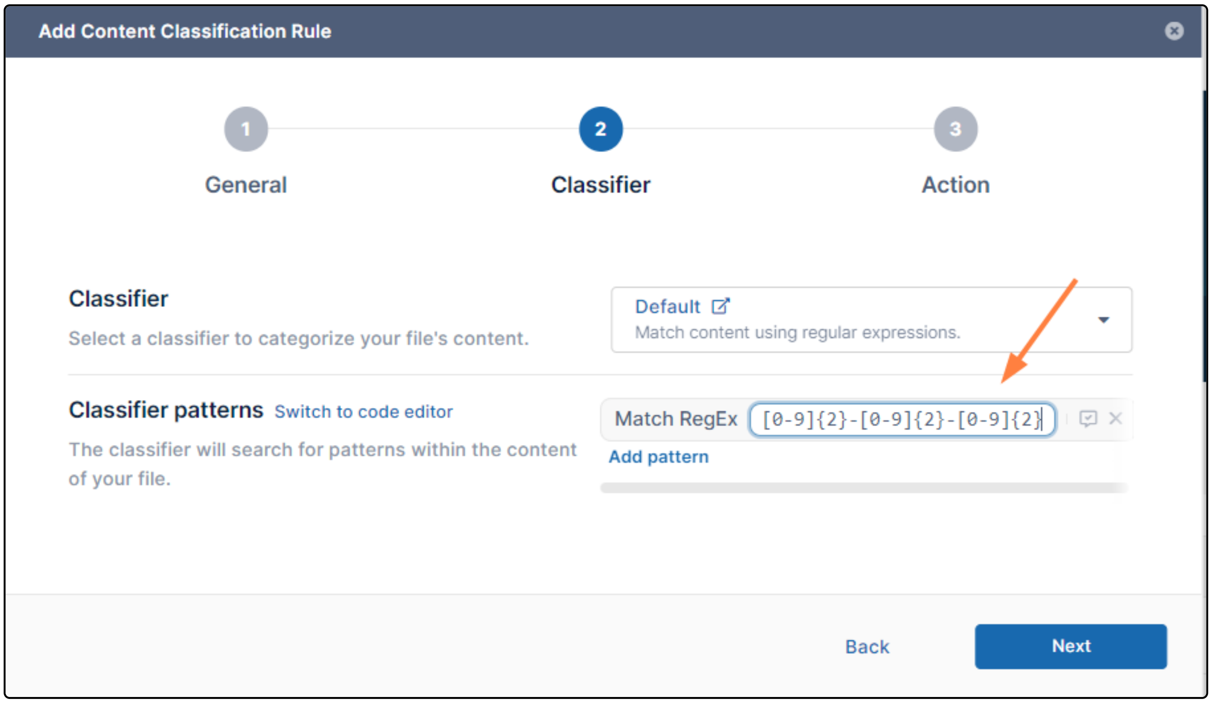
The new **Medical Record Number** pattern appears in the **Choose a pattern** drop-down list in the **Add Content Classification Rule** wizard.

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.



Add Content Classification Rule

Classifier

Select a classifier to categorize your file's content.

Default — Match content using regular expressions.

Classifier patterns

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

Match RegEx `[0-9]{2}-[0-9]{2}-[0-9]{2}`

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.

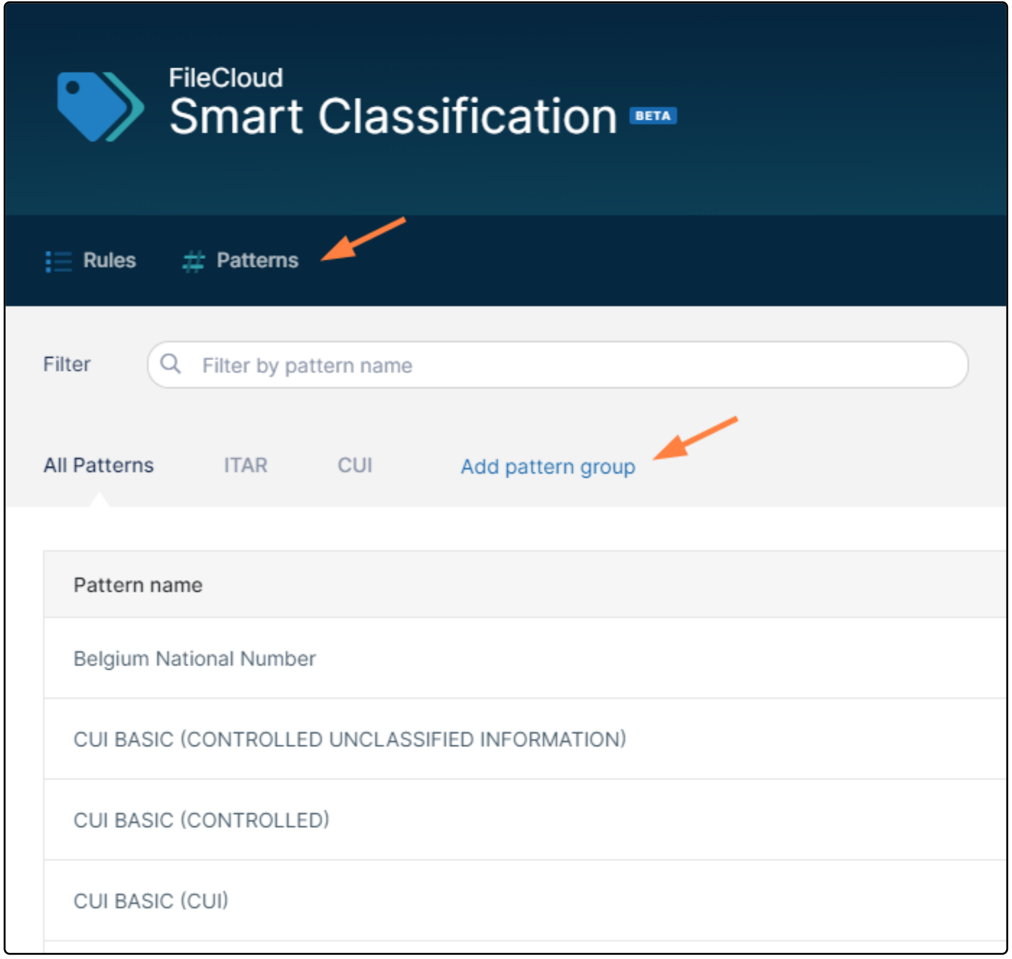
Creating a regex pattern group

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:

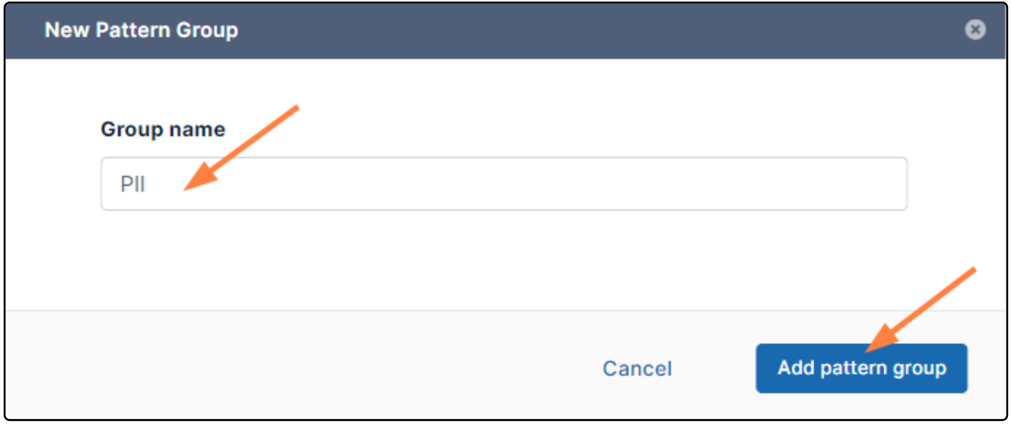
1. In the **Smart Classification** screen, click **Patterns** in the menu bar, and then click **Add pattern group**.



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

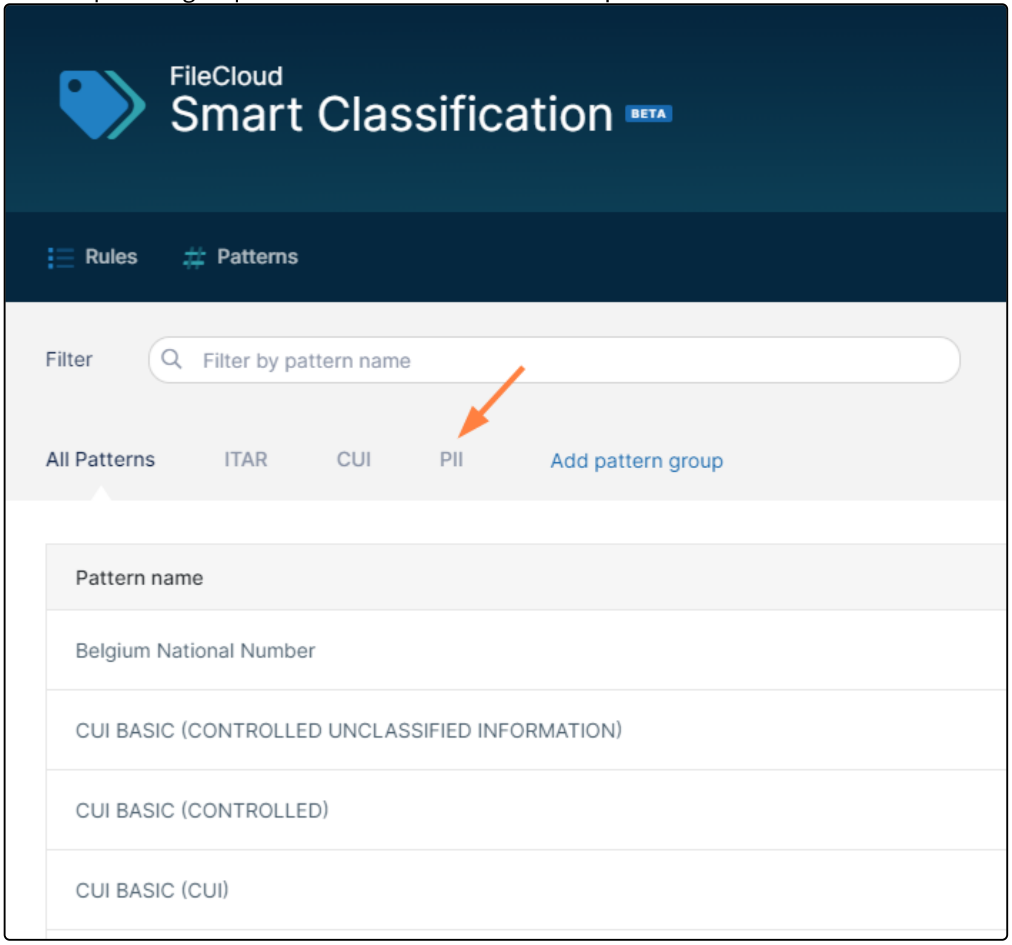
   The **New Pattern Group** dialog box opens.

2. Enter a **Group name**.



Group name: PII

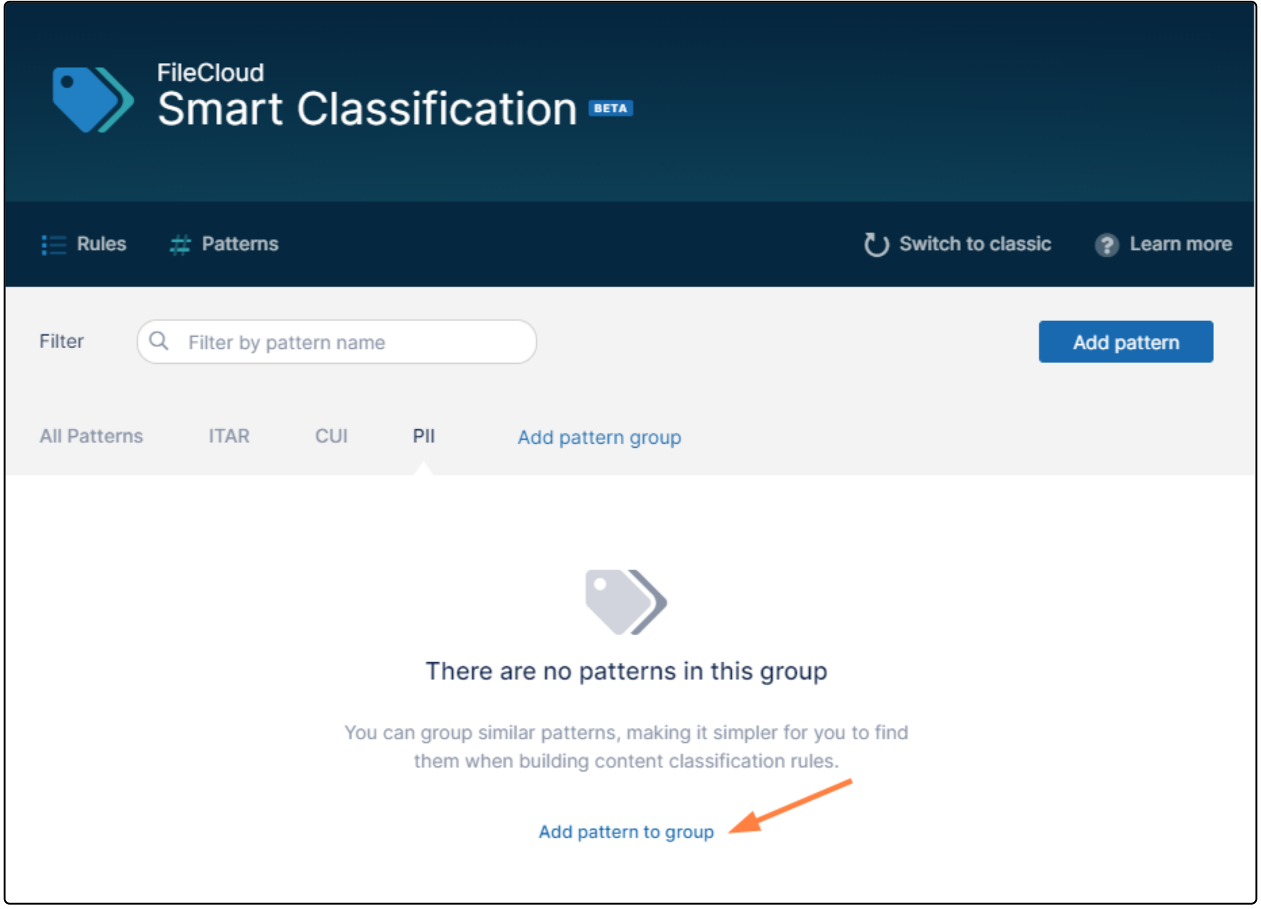
3. Click **Add pattern group**.
   The new pattern group name is added above the list of patterns.



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.

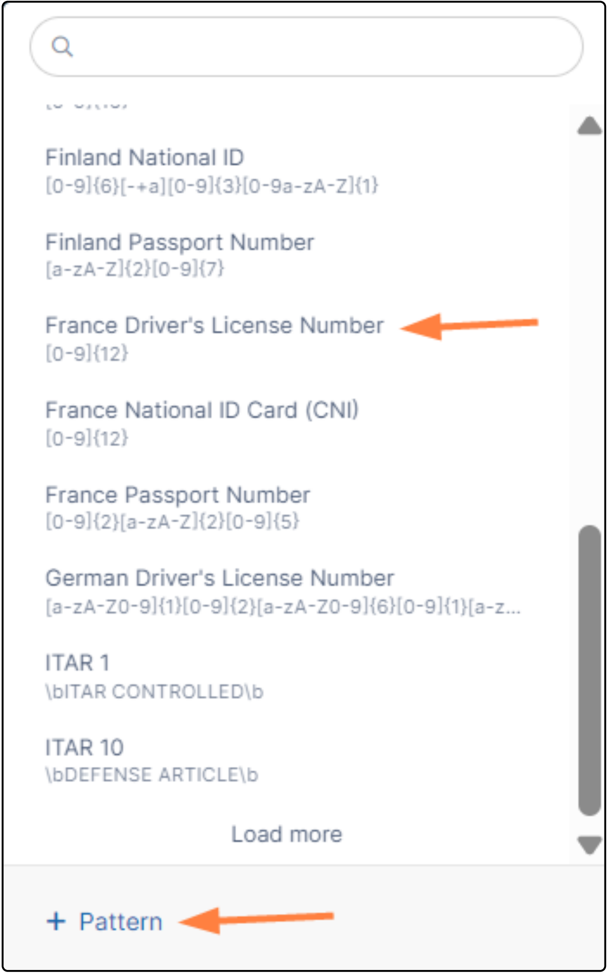
5. Click **Add pattern to group**.



There are no patterns in this group

You can group similar patterns, making it simpler for you to find them when building content classification rules.

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}

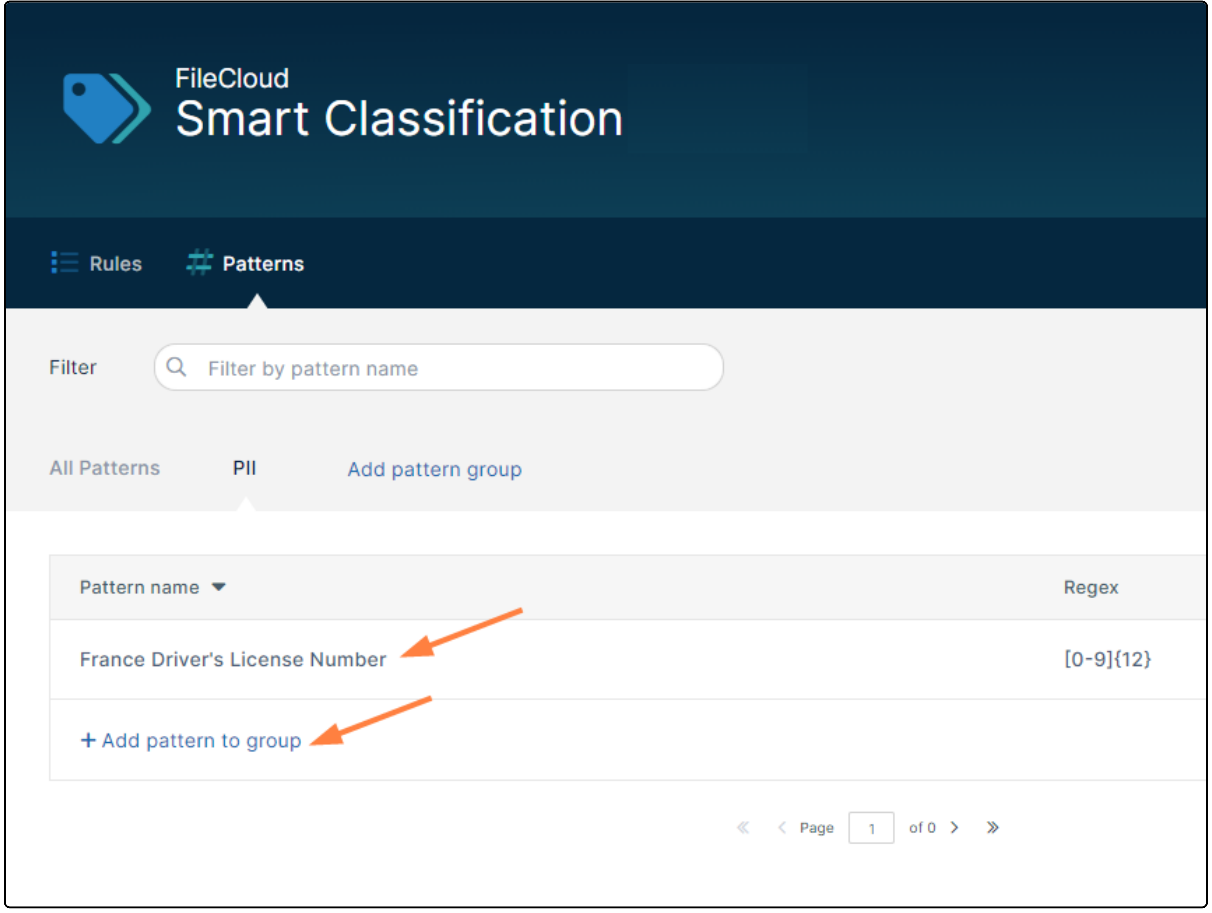
German Driver's License Number
[a-zA-Z0-9]{1}[0-9]{2}[a-zA-Z0-9]{6}[0-9]{1}[a-z...

ITAR 1
\bITAR CONTROLLED\b

ITAR 10
\bDEFENSE ARTICLE\b

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**

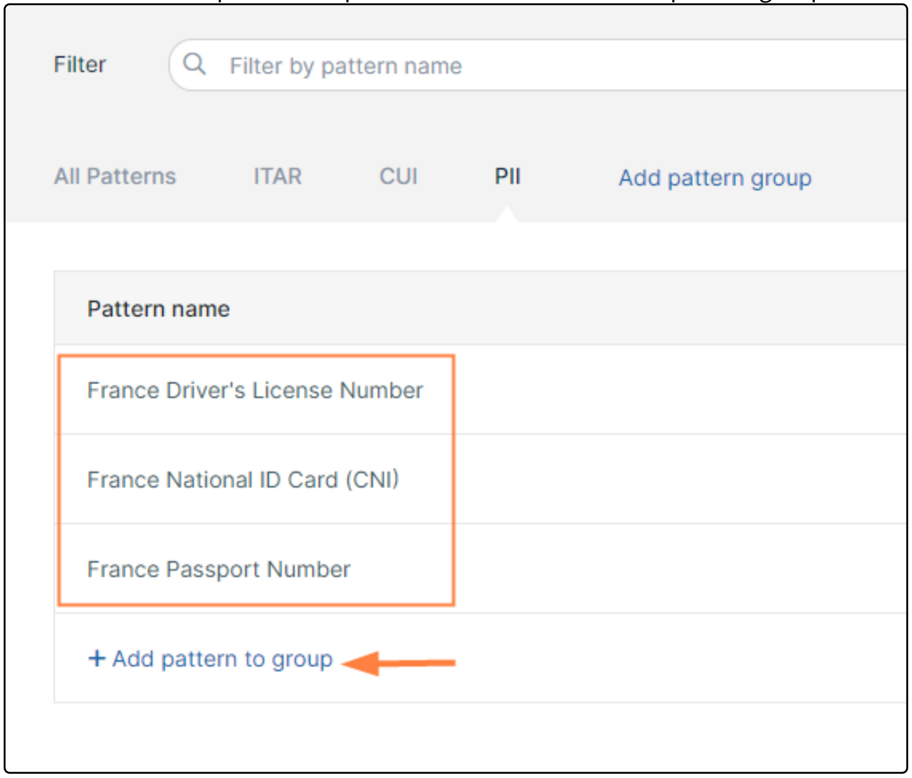
pattern to group link appears below it.



Pattern name	Regex
France Driver's License Number	[0-9]{12}

7. Click the **Add pattern to group** link and click **France National ID Card**.
   France National ID Card is added to the group.

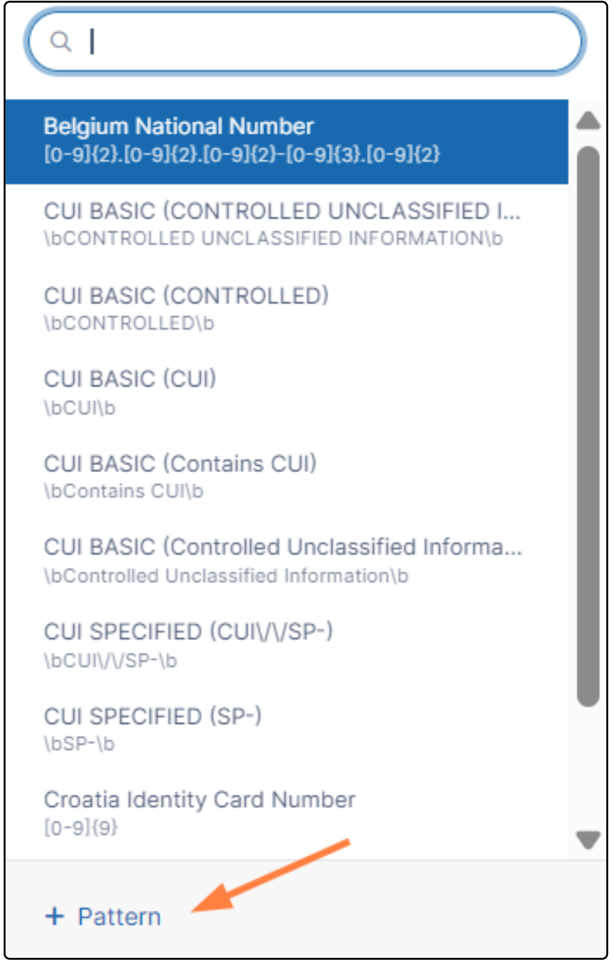
8. Click the **Add pattern to group** link below it, and click **France Passport Number**. Now all three of the predefined patterns are added to the **PII** pattern group.



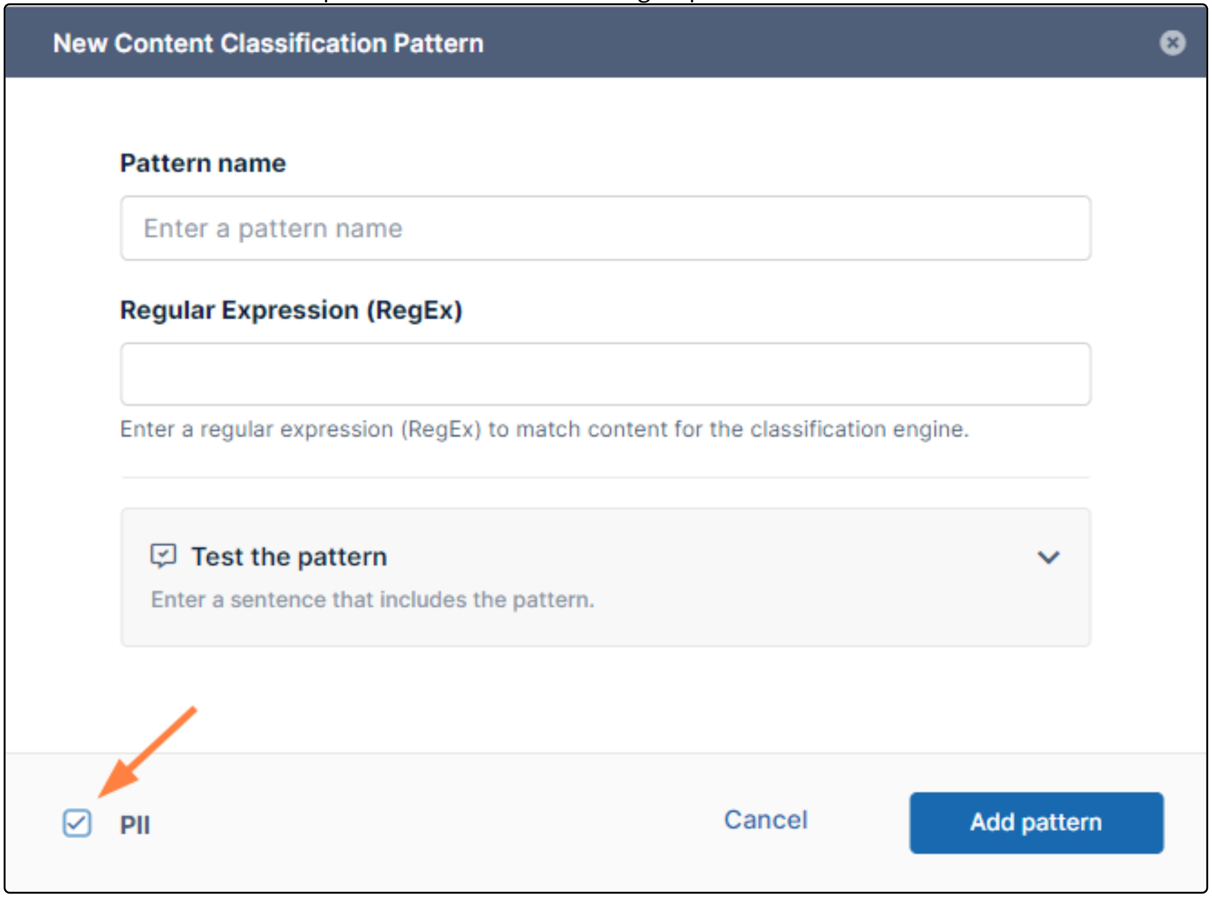
Pattern name
France Driver's License Number
France National ID Card (CNI)
France Passport Number

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.



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.



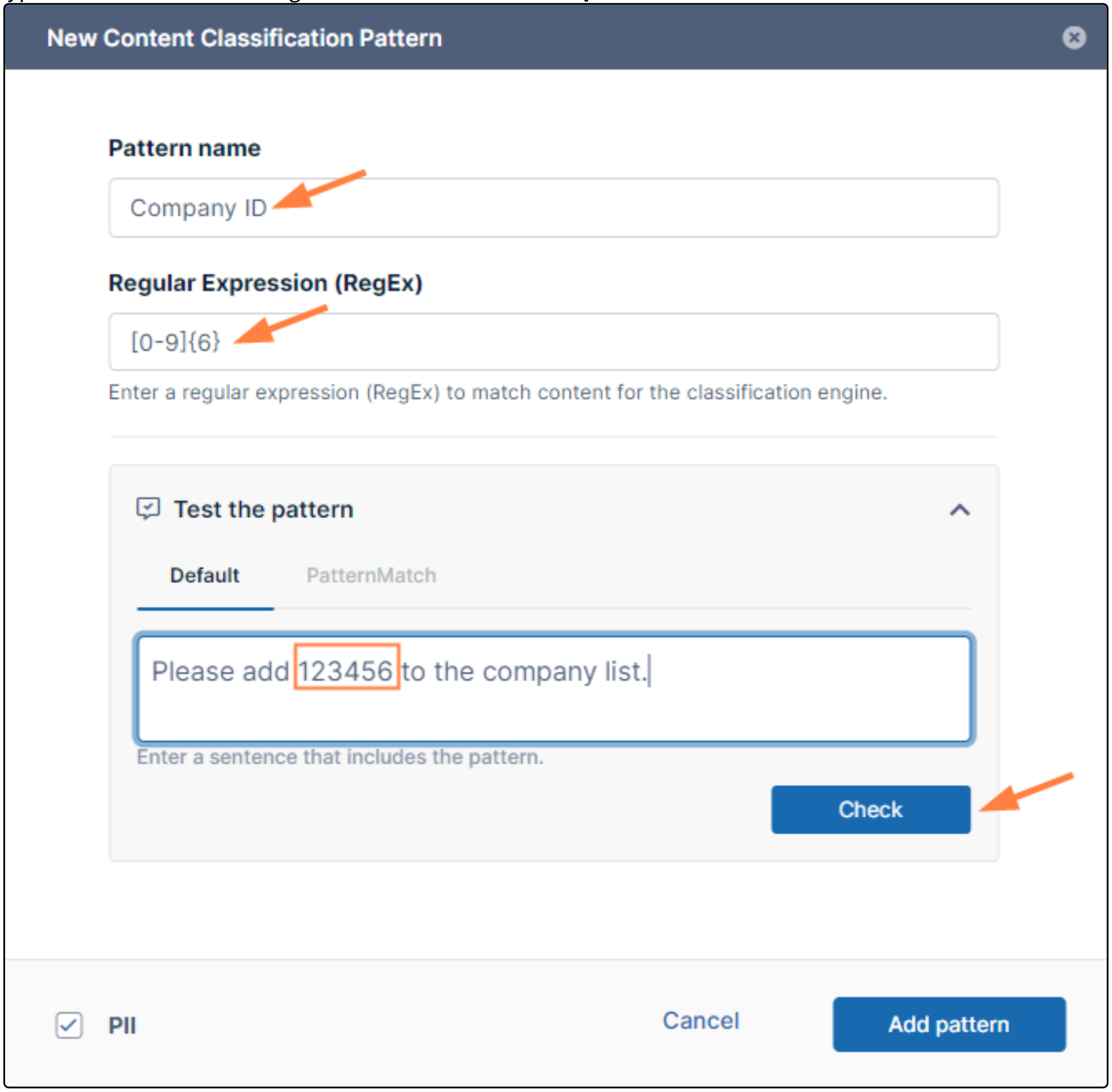
Enter a regular expression (RegEx) to match content for the classification engine.

Enter a sentence that includes the pattern.

☑ PII

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.

14. Type text that includes a 6-digit number into the **Test the pattern** box.



New Content Classification Pattern

Pattern name

Company ID

Regular Expression (RegEx)

[0-9]{6}

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

Test the pattern

Default

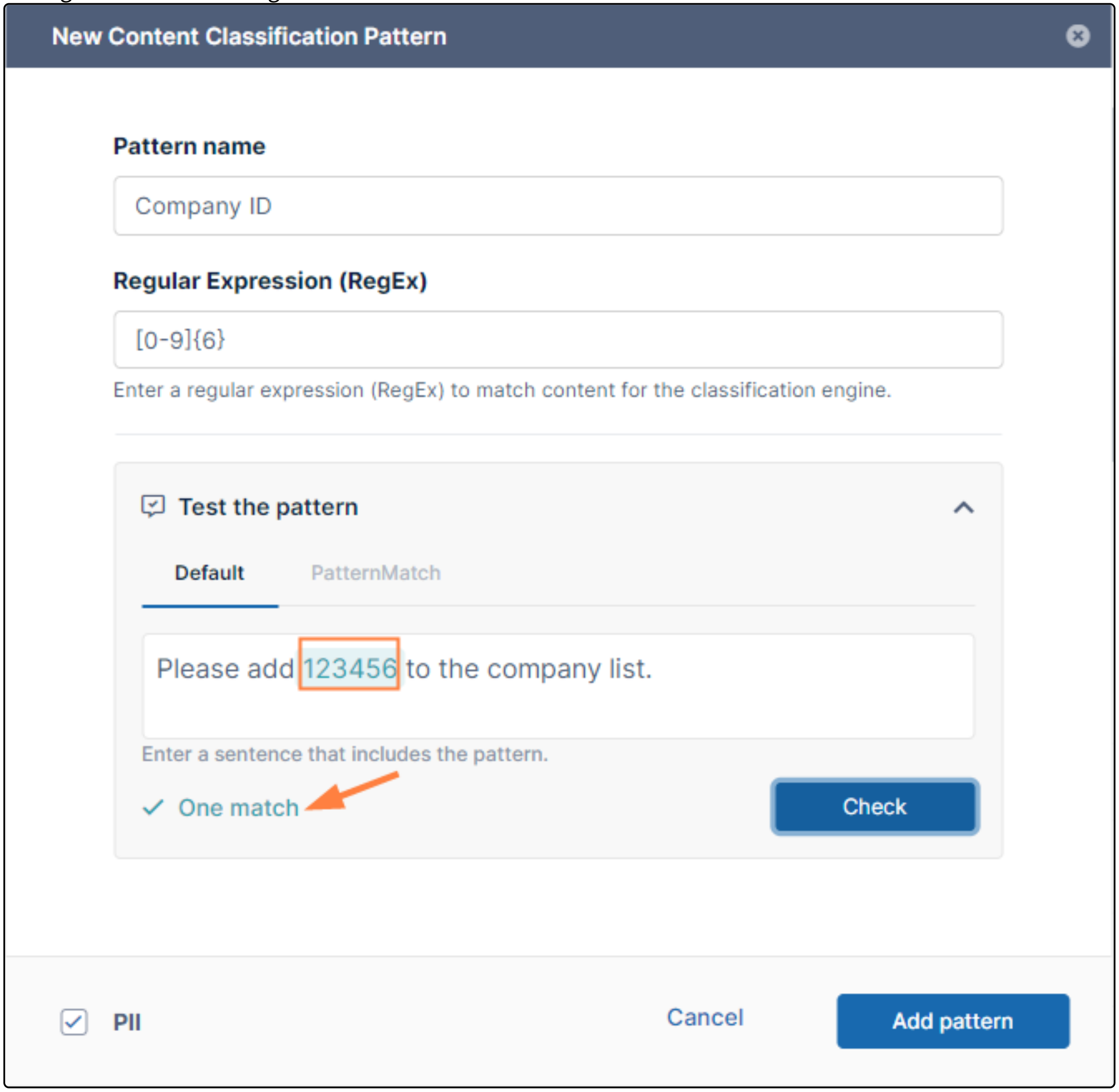
PatternMatch

Please add 123456 to the company list.

Enter a sentence that includes the pattern.

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

Company ID

Regular Expression (RegEx)

[0-9]{6}

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

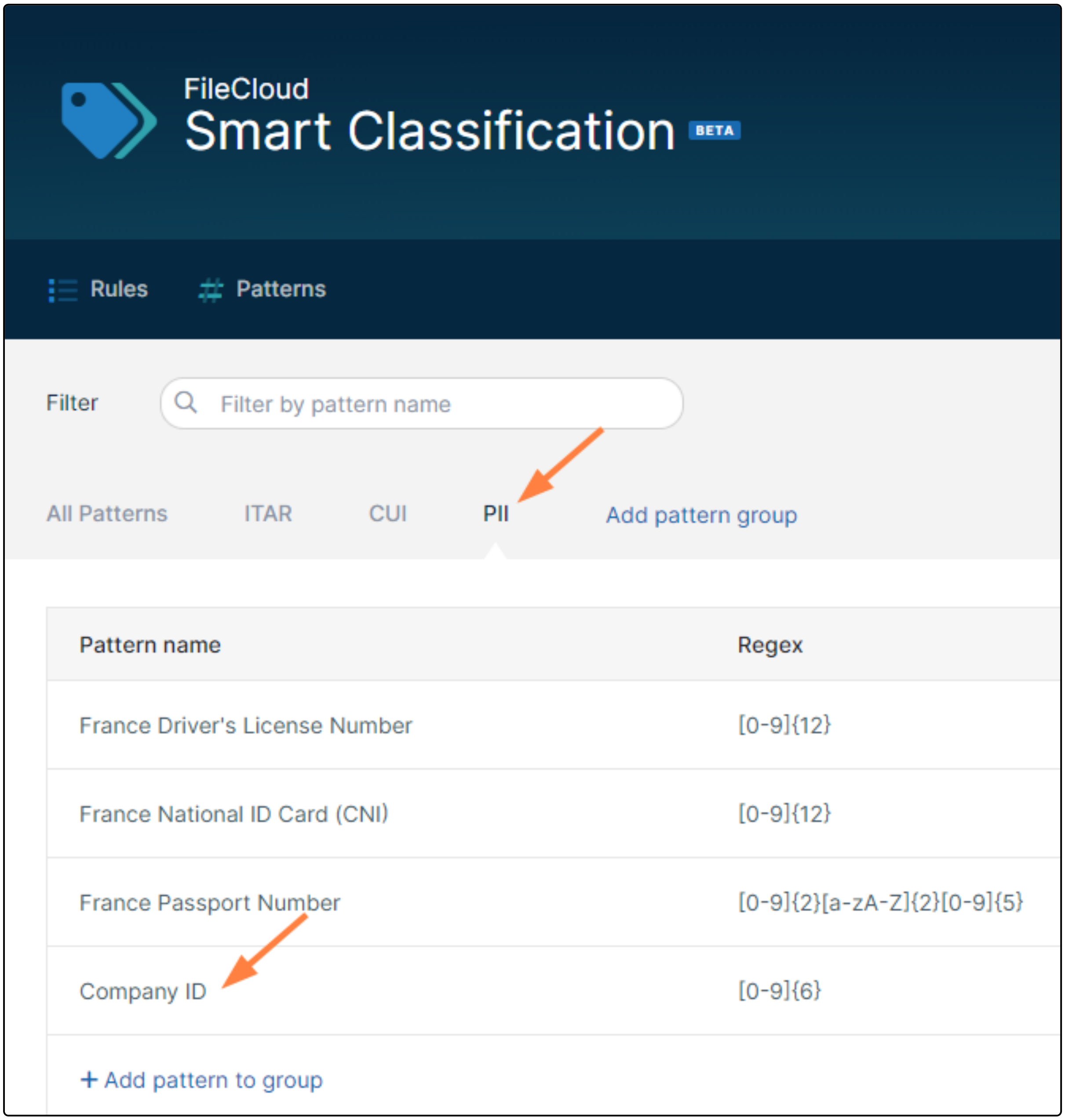
Test the pattern

Please add 123456 to the company list.

Enter a sentence that includes the pattern.

✓ One match

16. If the test is successful, click **Add pattern**.
    The pattern is added to the pattern group.



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}

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.

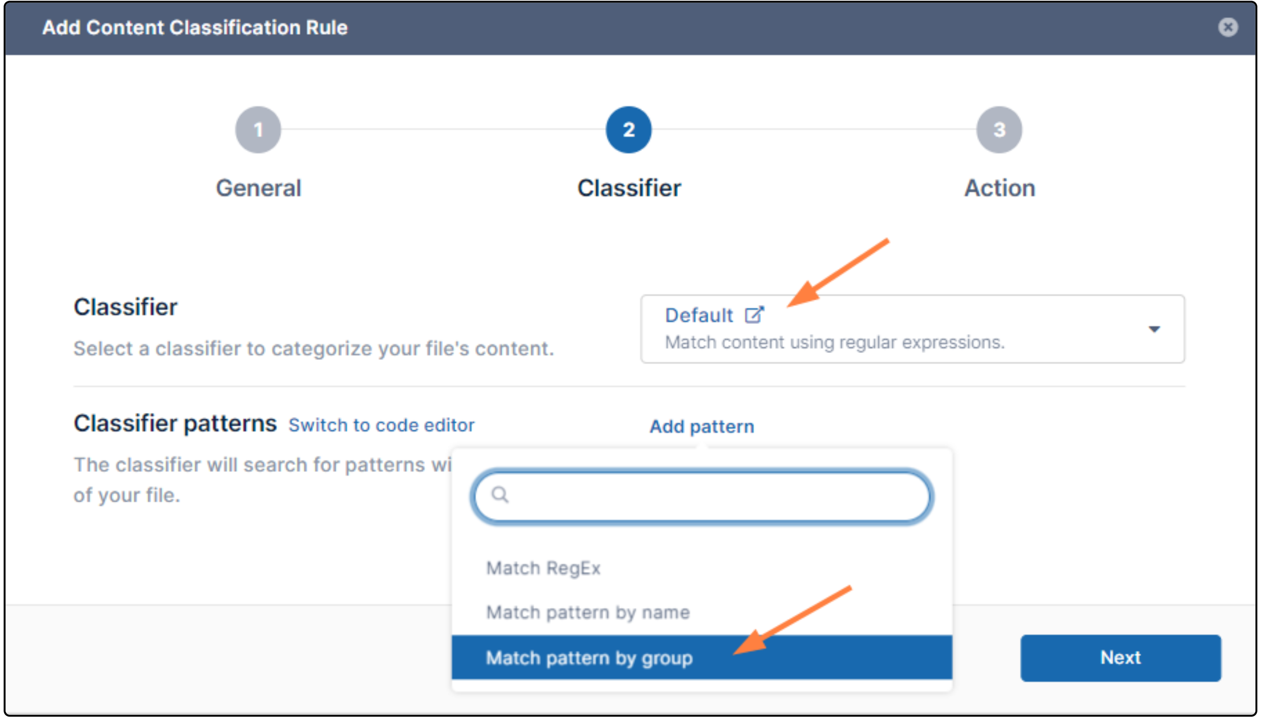
Adding a regex pattern group to a rule

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.

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**.



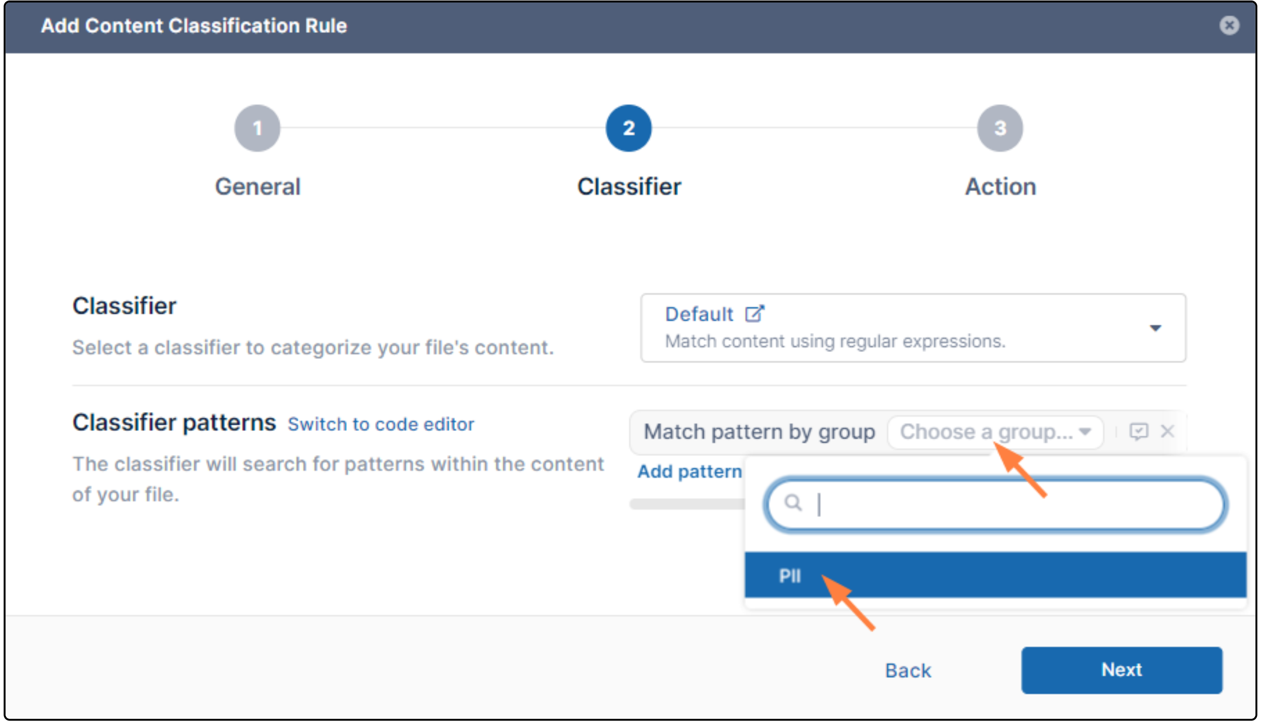
Add Content Classification Rule
1
General
2
Classifier
3
Action
Classifier
Select a classifier to categorize your file's content.
Default
Match content using regular expressions.
Classifier patterns
Switch to code editor
Add pattern
The classifier will search for patterns wi
of your file.
Match RegEx
Match pattern by name
Match pattern by group
Next

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:

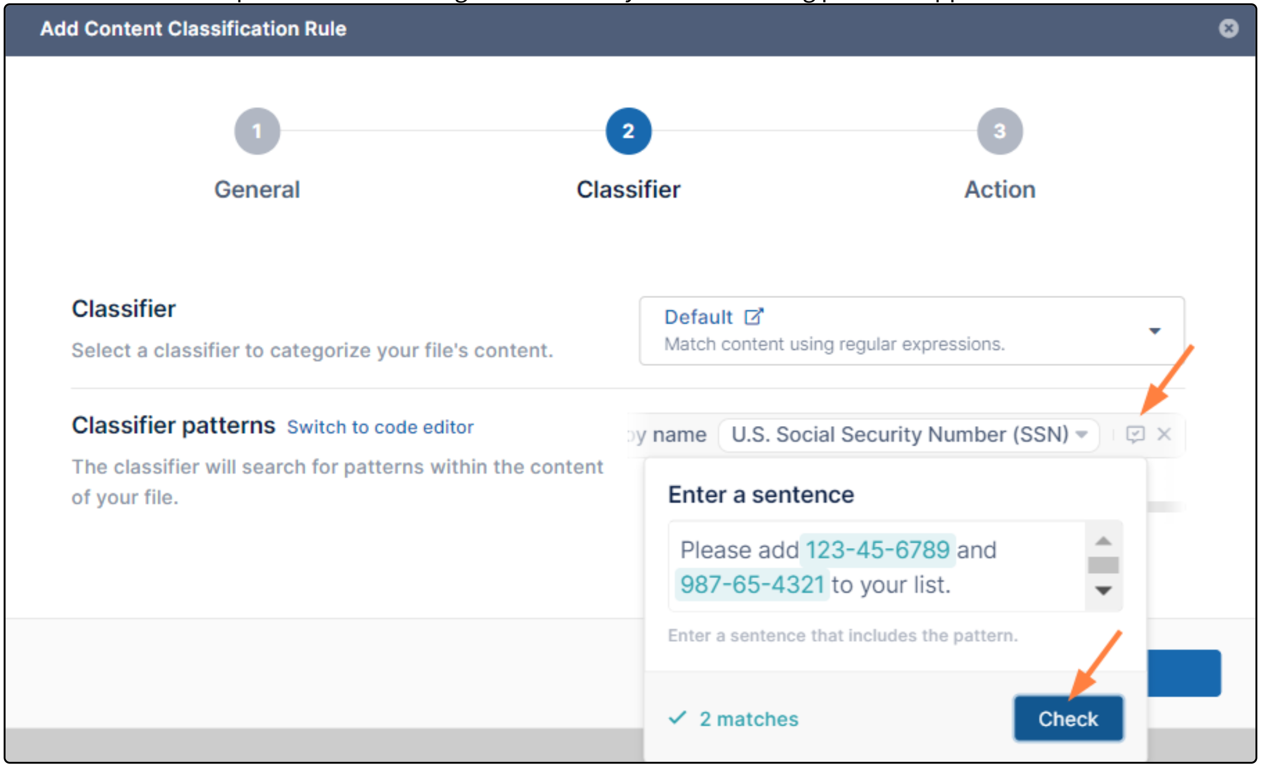


Add Content Classification Rule
1
General
2
Classifier
3
Action
Classifier
Select a classifier to categorize your file's content.
Default
Match content using regular expressions.
Classifier patterns
Switch to code editor
The classifier will search for patterns within the content of your file.
Match pattern by group
Choose a group...
Add pattern
PII
Back
Next

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:


Add Content Classification Rule
1
General
2
Classifier
3
Action

Classifier

Select a classifier to categorize your file's content.

Default

Match content using regular expressions.

Classifier patterns Switch to code editor

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

y name
U.S. Social Security Number (SSN)

Enter a sentence

Please add 123-45-6789 and 987-65-4321 to your list.

Enter a sentence that includes the pattern.

✓ 2 matches

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.

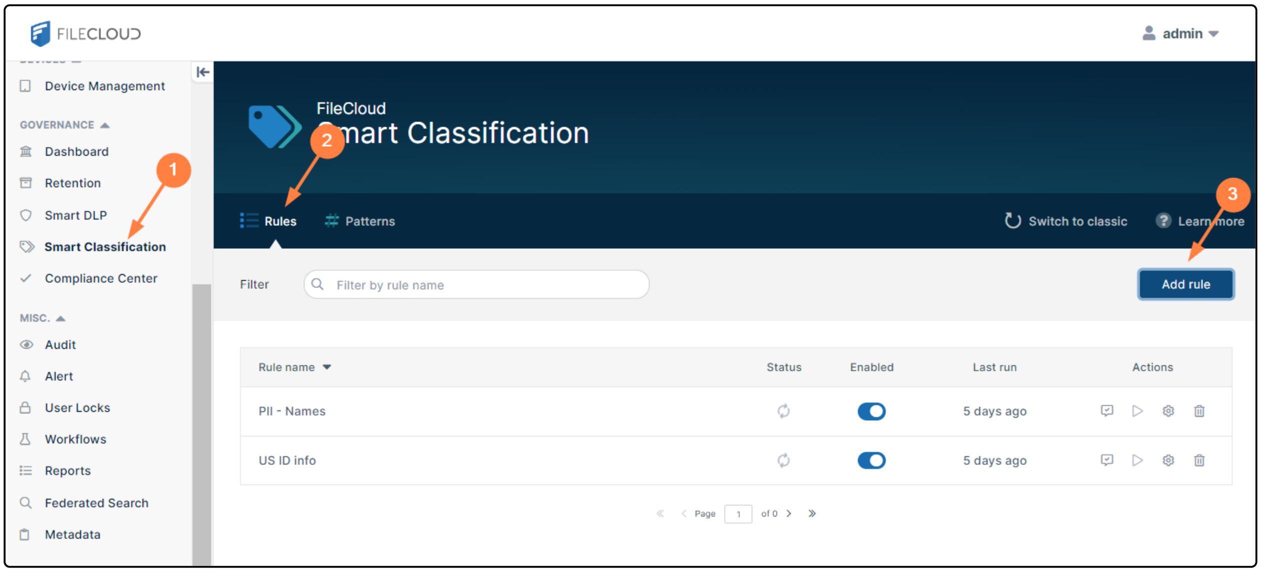
When you automate running of a Smart Classification rule, it classifies all existing files in FileCloud, and then runs on each file that is added or updated. The initial run may be lengthy since many files may have to be classified. If you don't automate running of a rule, and only run it manually, during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

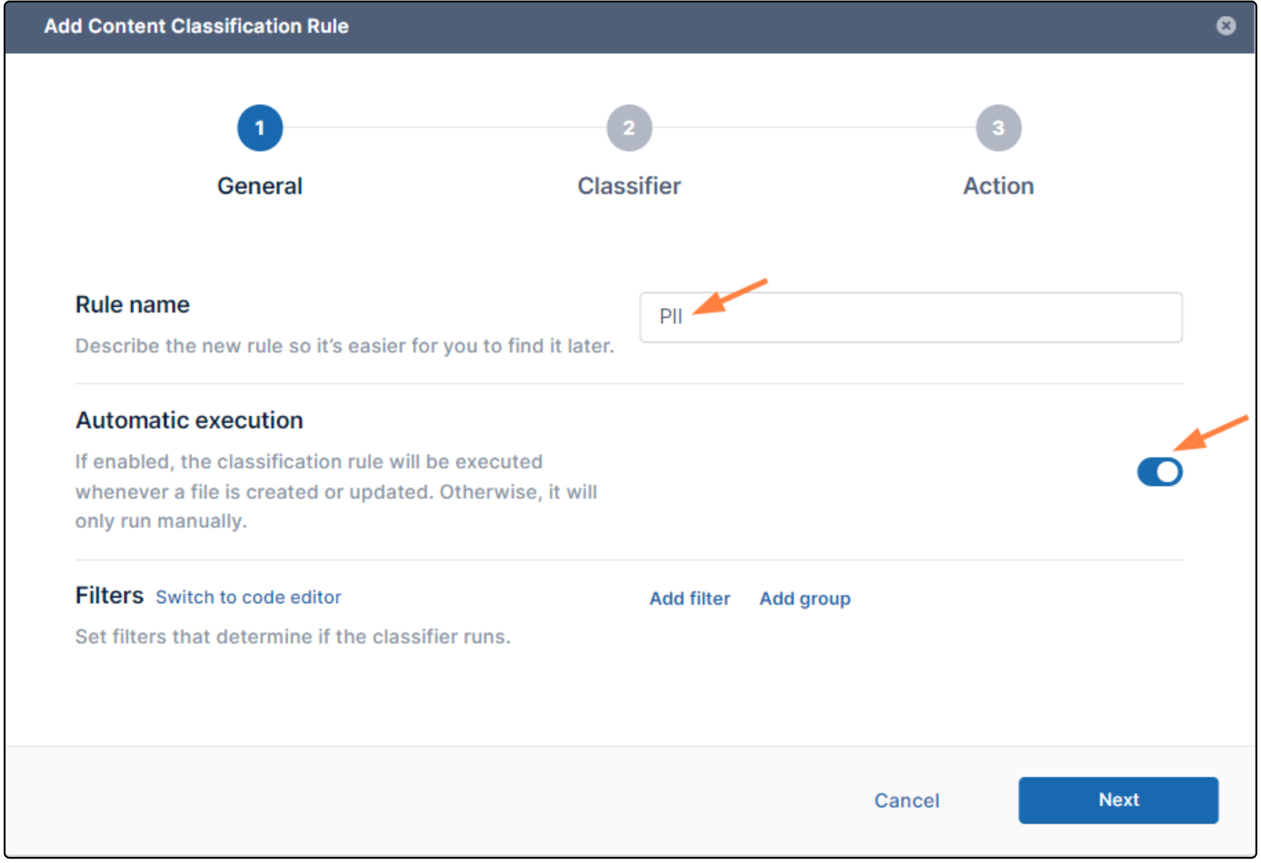
3. Click **Add rule**.



Rule name	Status	Enabled	Last run	Actions
PII - Names		●	5 days ago	
US ID info		●	5 days ago	

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.

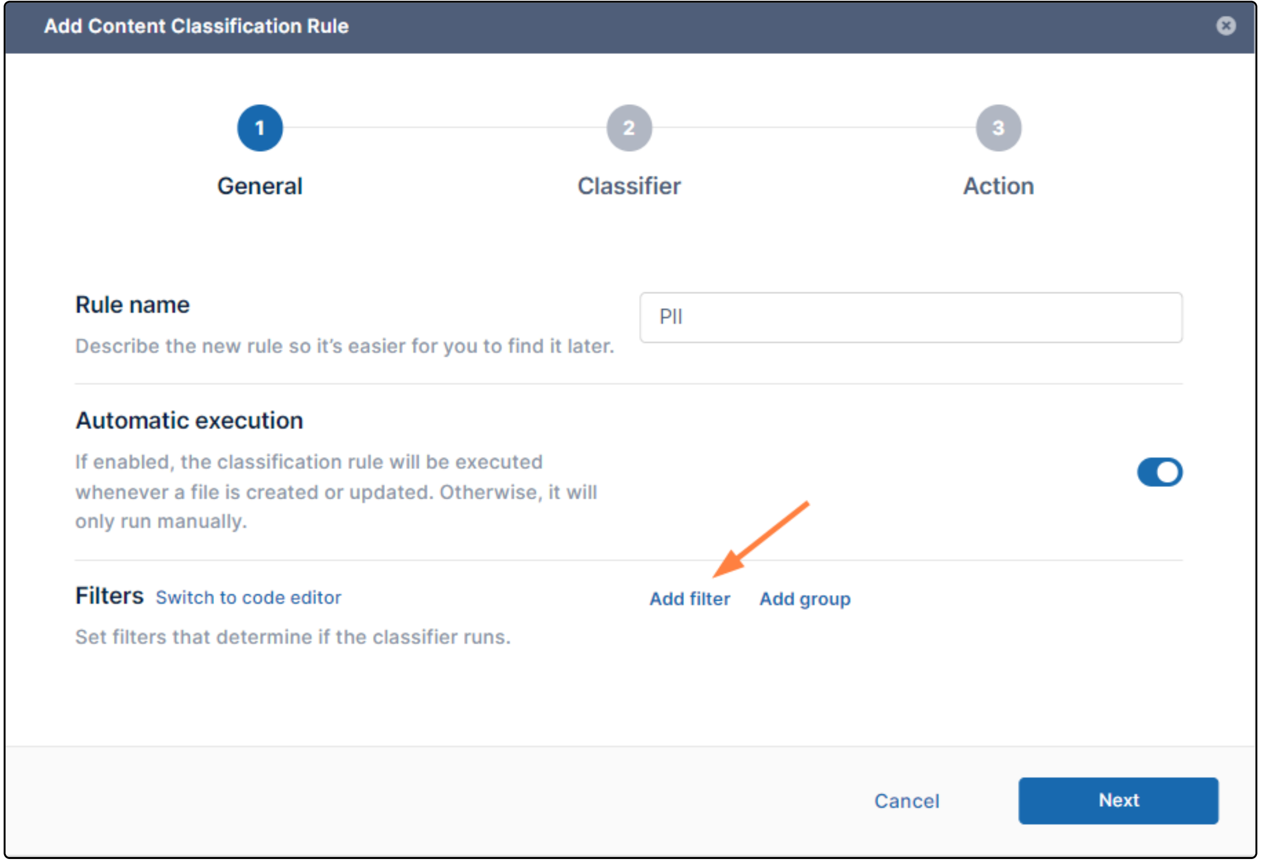


Rule name: PII
Describe the new rule so it's easier for you to find it later.

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.

6. 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).



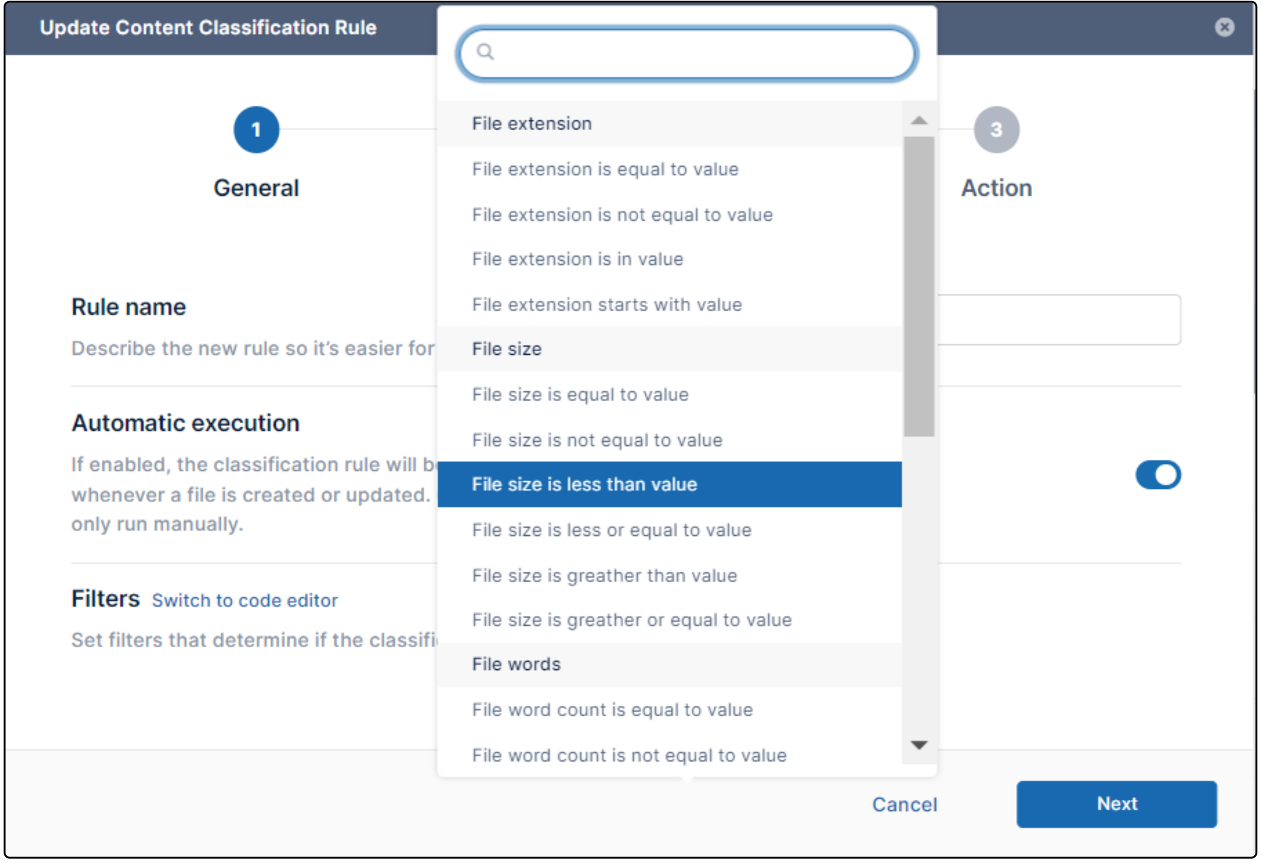
Add Content Classification Rule

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

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.

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



Update Content Classification Rule

1 General

3 Action

Rule name

Describe the new rule so it's easier for

Automatic execution

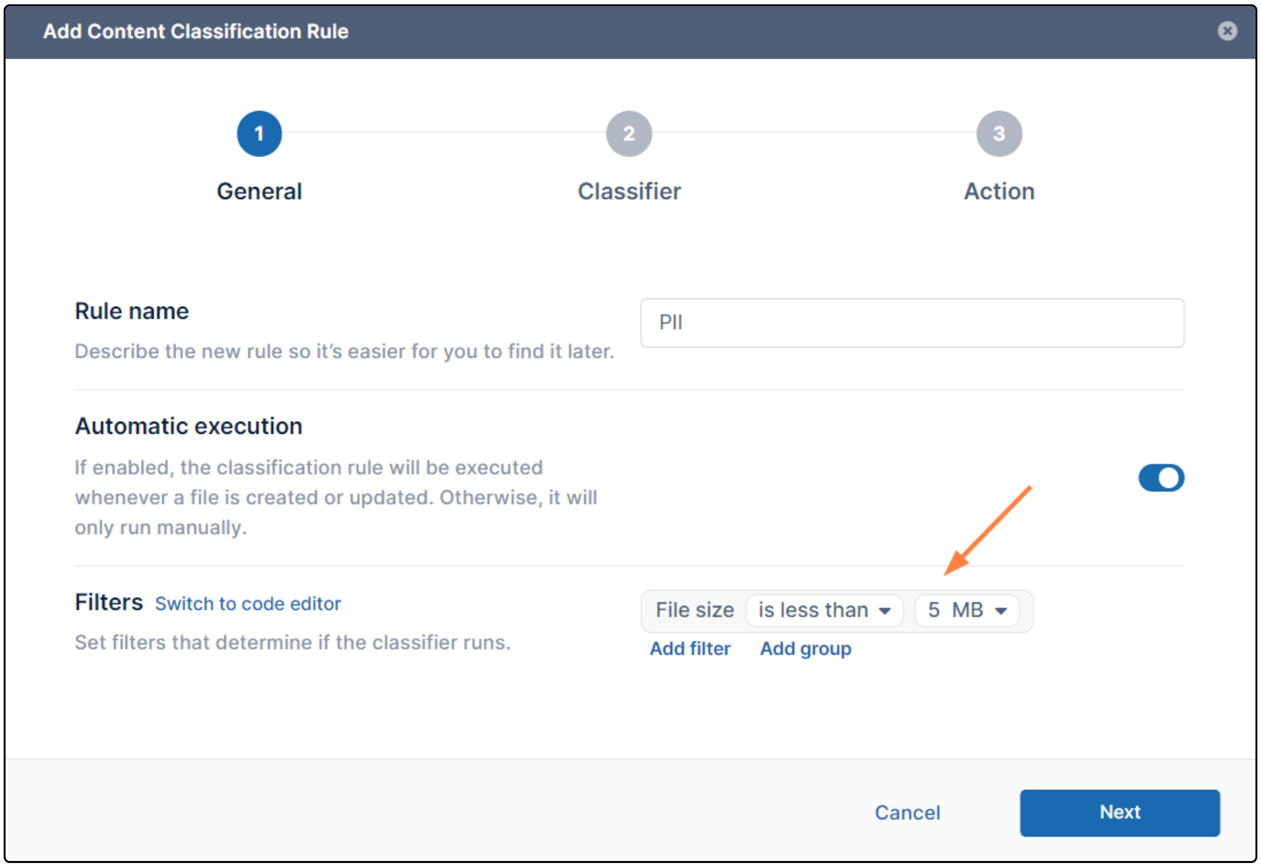
If enabled, the classification rule will b whenever a file is created or updated. only run manually.

Filters Switch to code editor

Set filters that determine if the classifi

File extension
File extension is equal to value
File extension is not equal to value
File extension is in value
File extension starts with value
File size
File size is equal to value
File size is not equal to value
File size is less than value
File size is less or equal to value
File size is greather than value
File size is greather or equal to value
File words
File word count is equal to value
File word count is not equal to value
Cancel
Next

7. For this example, the value is set to **5 MB**.
   Note: Files greater than **10 MB** are not available to be classified.



Rule name

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

PII

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

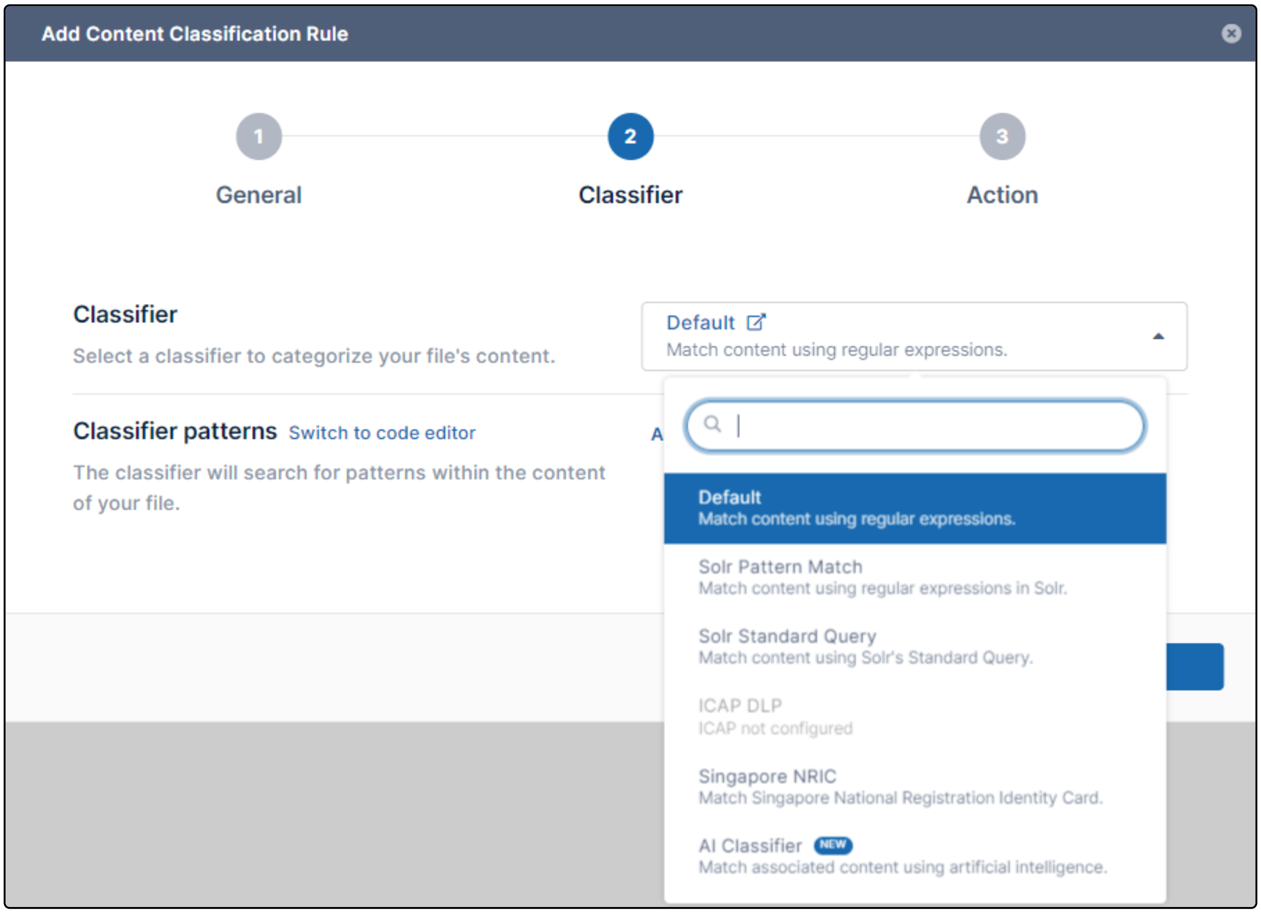
Set filters that determine if the classifier runs.

File size is less than 5 MB

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.
- 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.

Default
Match content using regular expressions.

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.

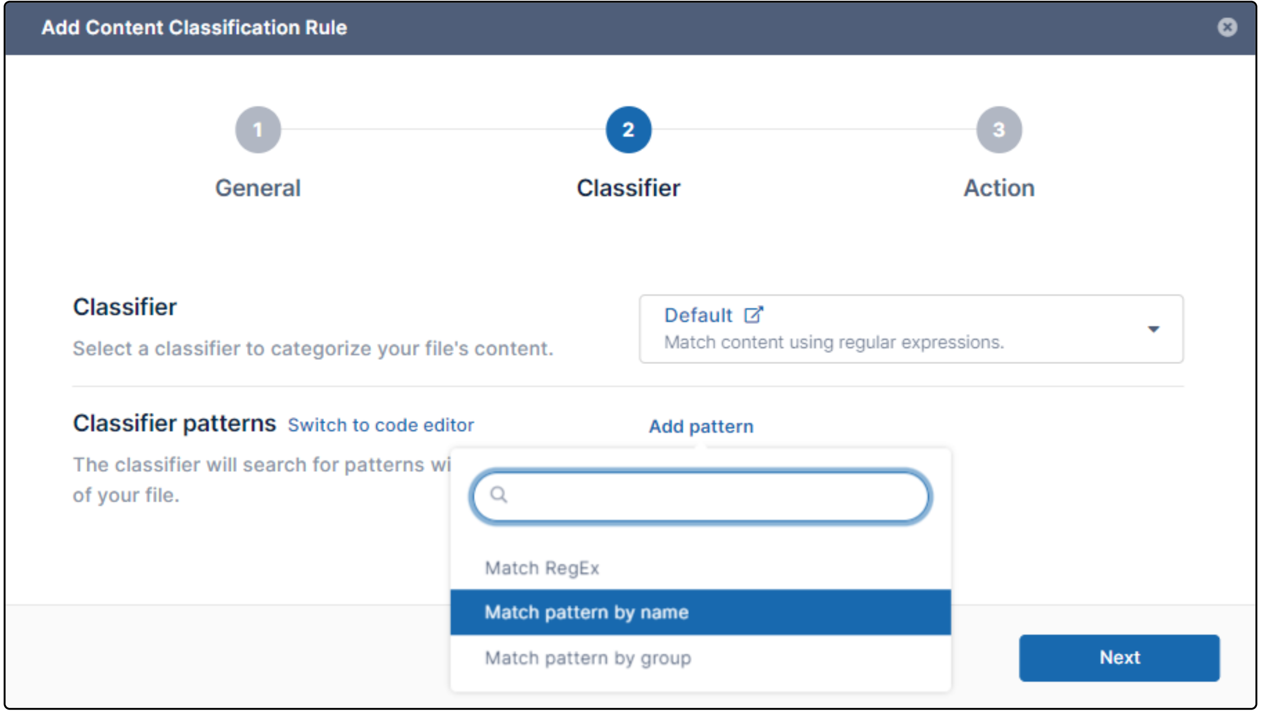
AI Classifier NEW
Match associated content using artificial intelligence.

For help using classifiers, see Guide to Classifiers

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.
    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.



Add Content Classification Rule

Classifier

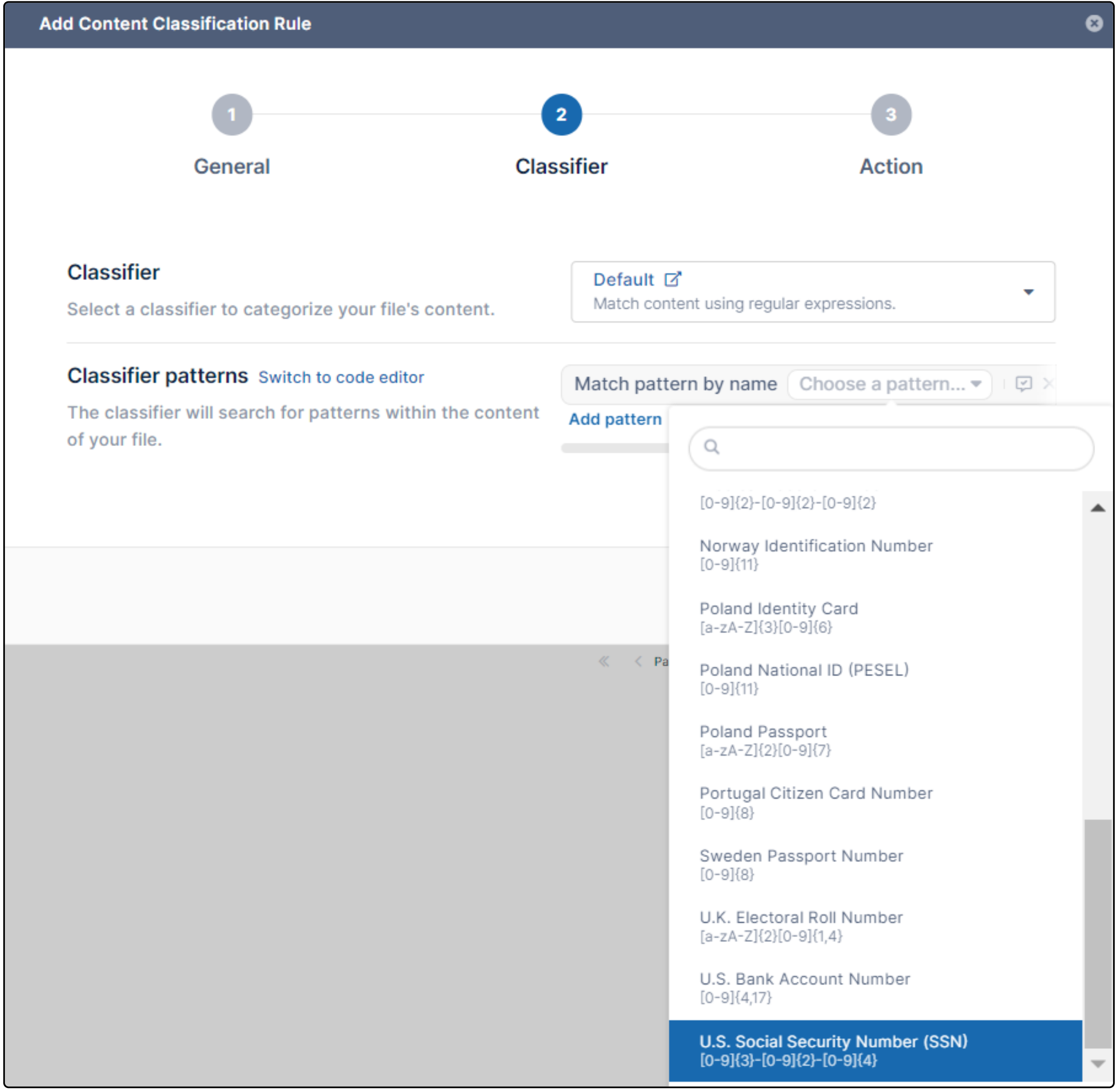
Select a classifier to categorize your file's content.

Default
Match content using regular expressions.

Classifier patterns

The classifier will search for patterns wi
of your file.

12. Choose a predefined pattern in the **Choose a pattern** drop-down list.
U.S. Social Security Number is chosen.



Add Content Classification Rule

Classifier

Select a classifier to categorize your file's content.

Default
Match content using regular expressions.

Classifier patterns Switch to code editor

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

Match pattern by name Choose a pattern...

Add pattern

[0-9]{2}-[0-9]{2}-[0-9]{2}

Norway Identification Number
[0-9]{11}

Poland Identity Card
[a-zA-Z]{3}[0-9]{6}

Poland National ID (PESEL)
[0-9]{11}

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

Portugal Citizen Card Number
[0-9]{8}

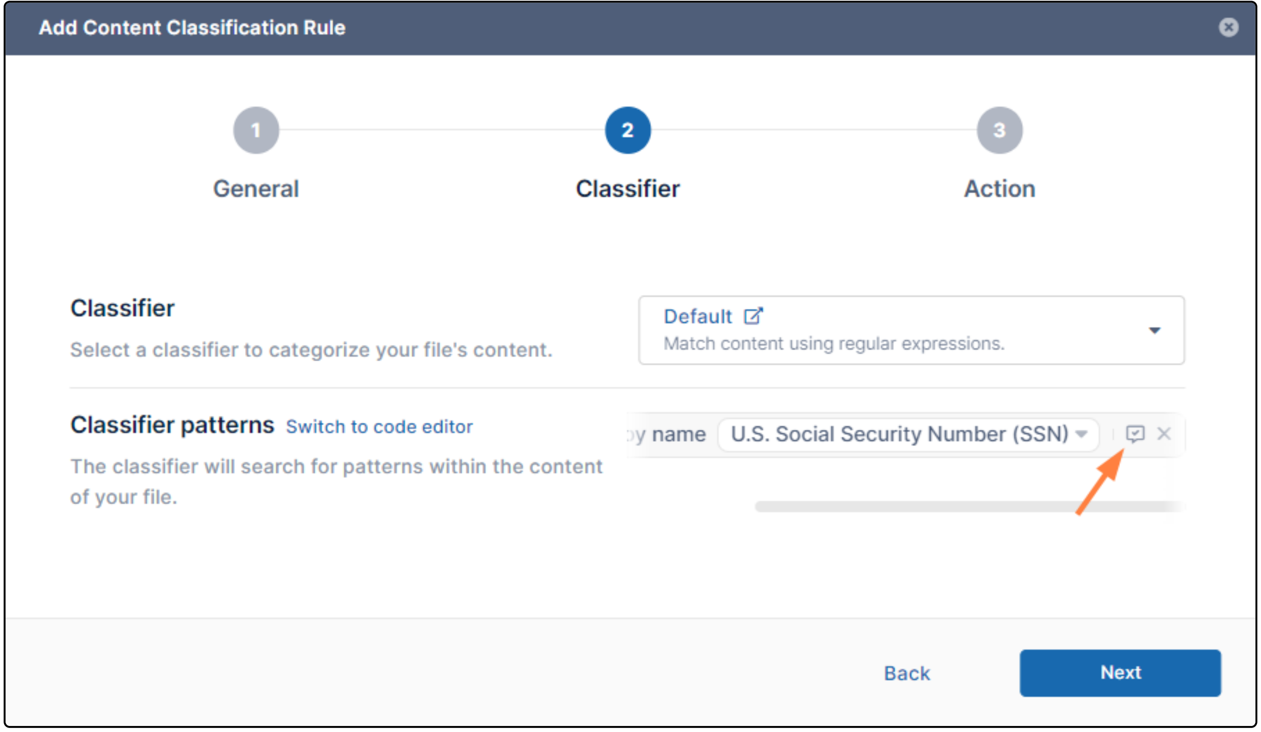
Sweden Passport Number
[0-9]{8}

U.K. Electoral Roll Number
[a-zA-Z]{2}[0-9]{1,4}

U.S. Bank Account Number
[0-9]{4,17}

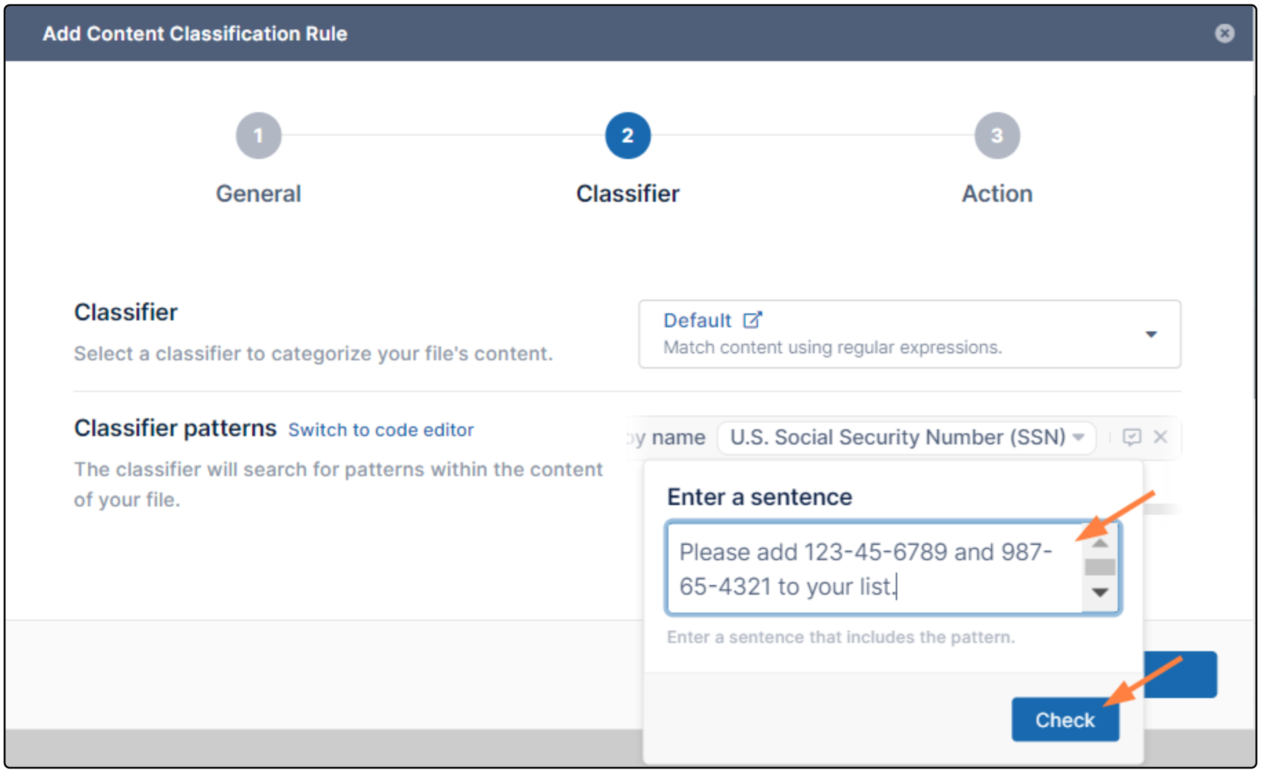
U.S. Social Security Number (SSN)
[0-9]{3}-[0-9]{2}-[0-9]{4}

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



Add Content Classification Rule
1
General
2
Classifier
3
Action
Classifier
Select a classifier to categorize your file's content.
Default
Match content using regular expressions.
Classifier patterns
Switch to code editor
The classifier will search for patterns within the content of your file.
by name
U.S. Social Security Number (SSN)
Back
Next

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

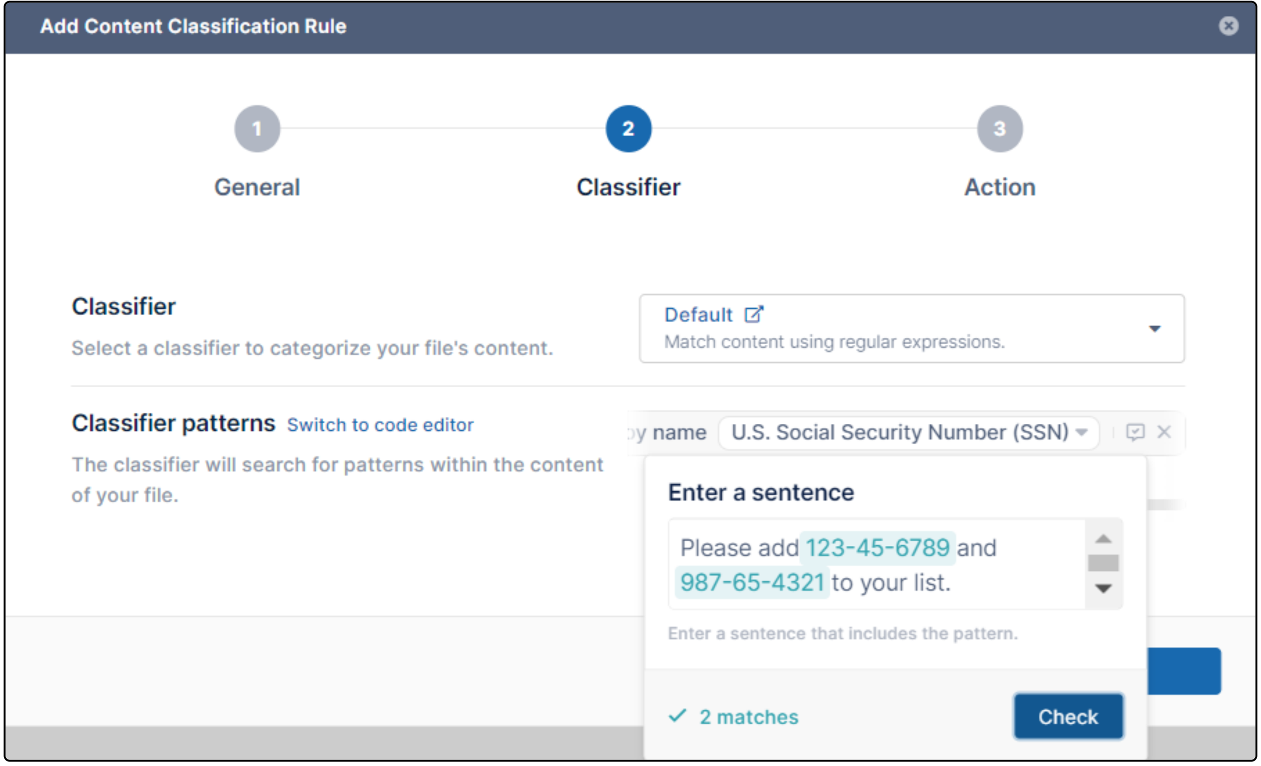


Add Content Classification Rule
1
General
2
Classifier
3
Action
Classifier
Select a classifier to categorize your file's content.
Default
Match content using regular expressions.
Classifier patterns
Switch to code editor
The classifier will search for patterns within the content of your file.
by name
U.S. Social Security Number (SSN)
Enter a sentence
Enter a sentence that includes the pattern.
Check

Please add 123-45-6789 and 987-65-4321 to your list.

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.



Classifier

Select a classifier to categorize your file's content.

Default

Match content using regular expressions.

Classifier patterns Switch to code editor

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

by name U.S. Social Security Number (SSN)

Enter a sentence

Please add 123-45-6789 and 987-65-4321 to your list.

Enter a sentence that includes the pattern.

✓ 2 matches

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

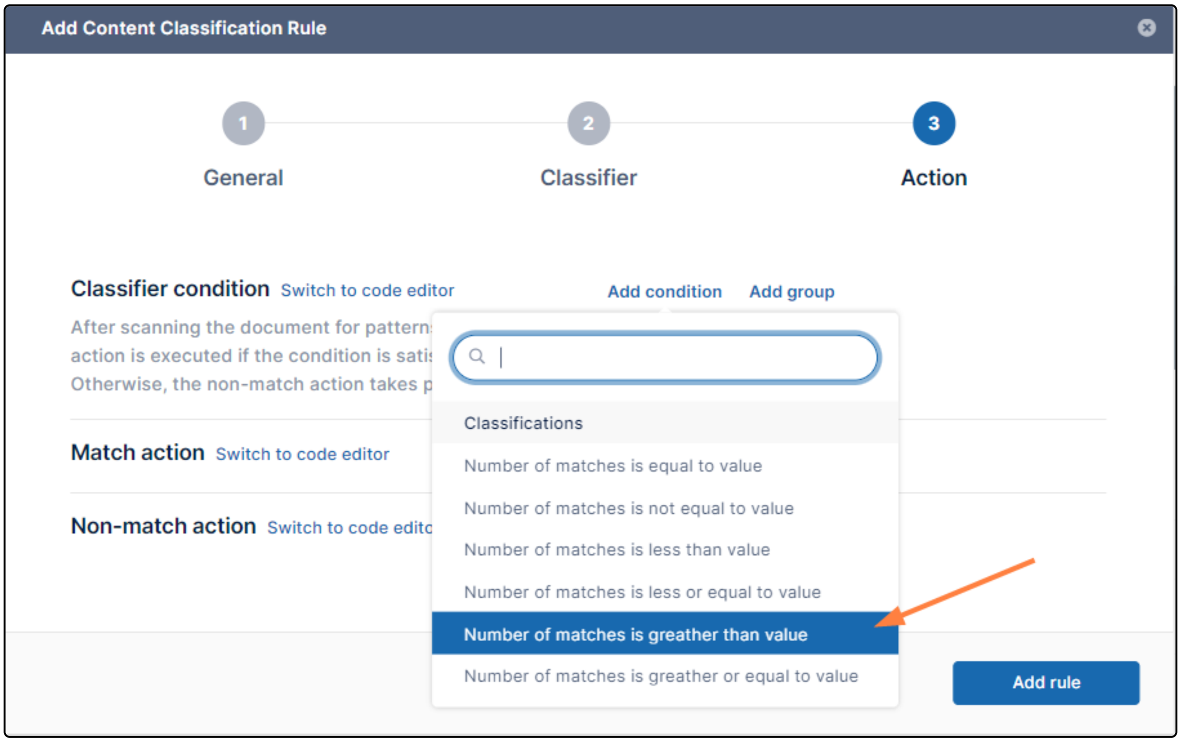
    The **Action** screen of the **Add Content Classification Rule** wizard opens.

16. Add a **Classifier condition**.

    Notes:

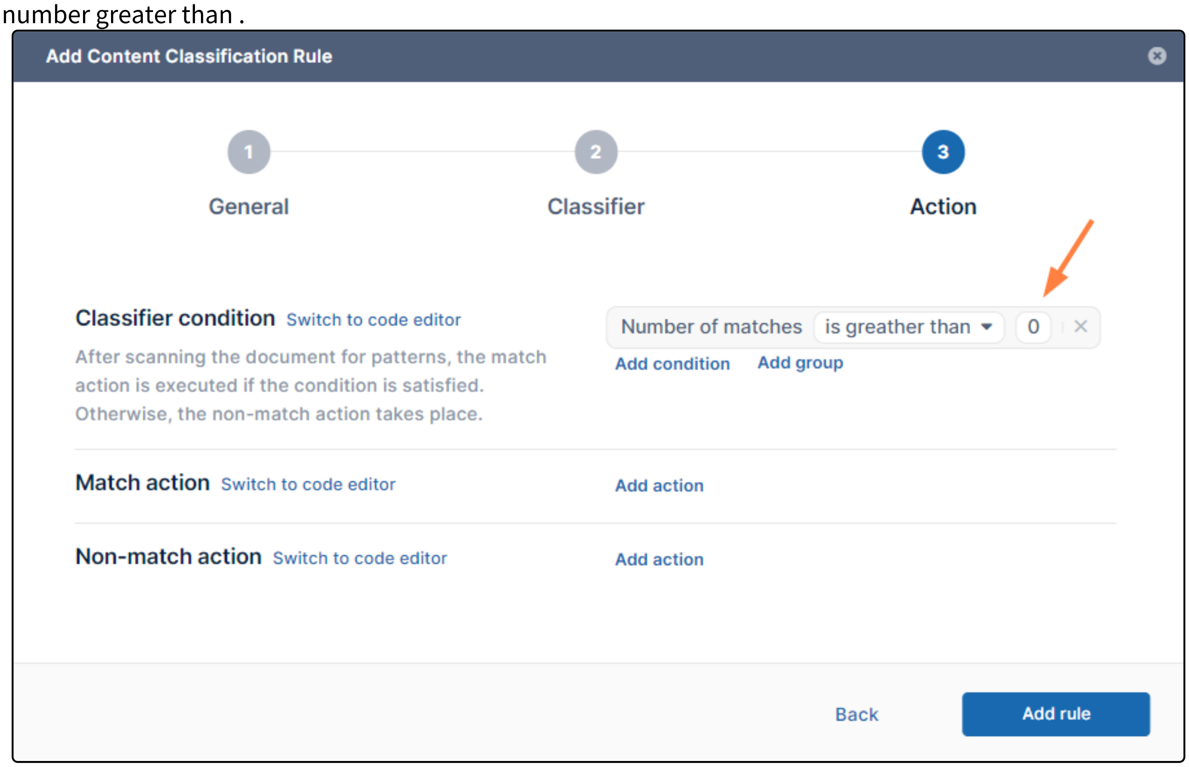
    - In many cases you can click **Add condition** and choose **Number of matches is greater than value**, and set value to **0.**
    - In most cases, there is no need for a complex condition, and choosing **Add group** is not necessary.
    - If you add multiple **Classifier conditions**, you can switch 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**.**


Add Content Classification Rule
1
General
2
Classifier
3
Action
Classifier condition
Switch to code editor
Add condition
Add group
Match action
Switch to code editor
Non-match action
Switch to code edito
Classifications
Number of matches is equal to value
Number of matches is not equal to value
Number of matches is less than value
Number of matches is less or equal to value
Number of matches is greather than value
Number of matches is greather or equal to value
Add rule

After scanning the document for pattern
action is executed if the condition is satis
Otherwise, the non-match action takes p

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 .



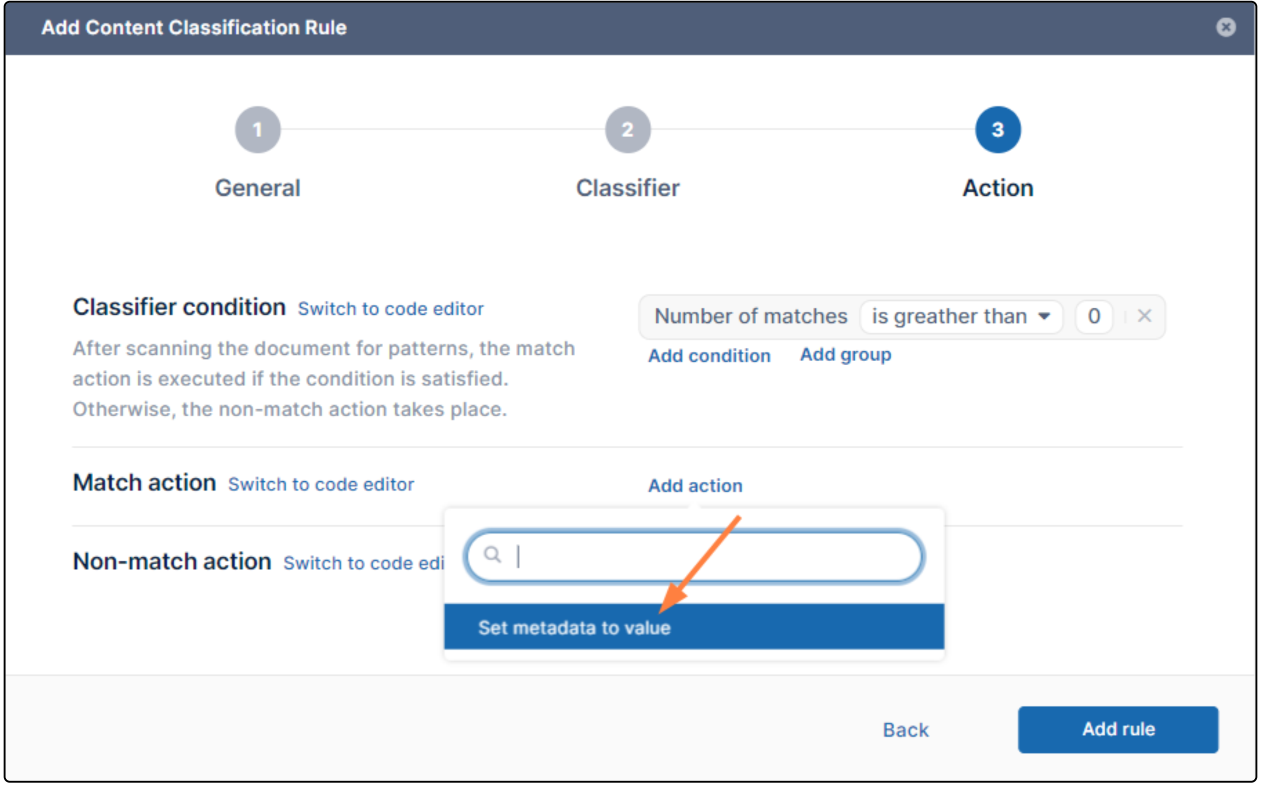
Number of matches is greather than 0

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

0

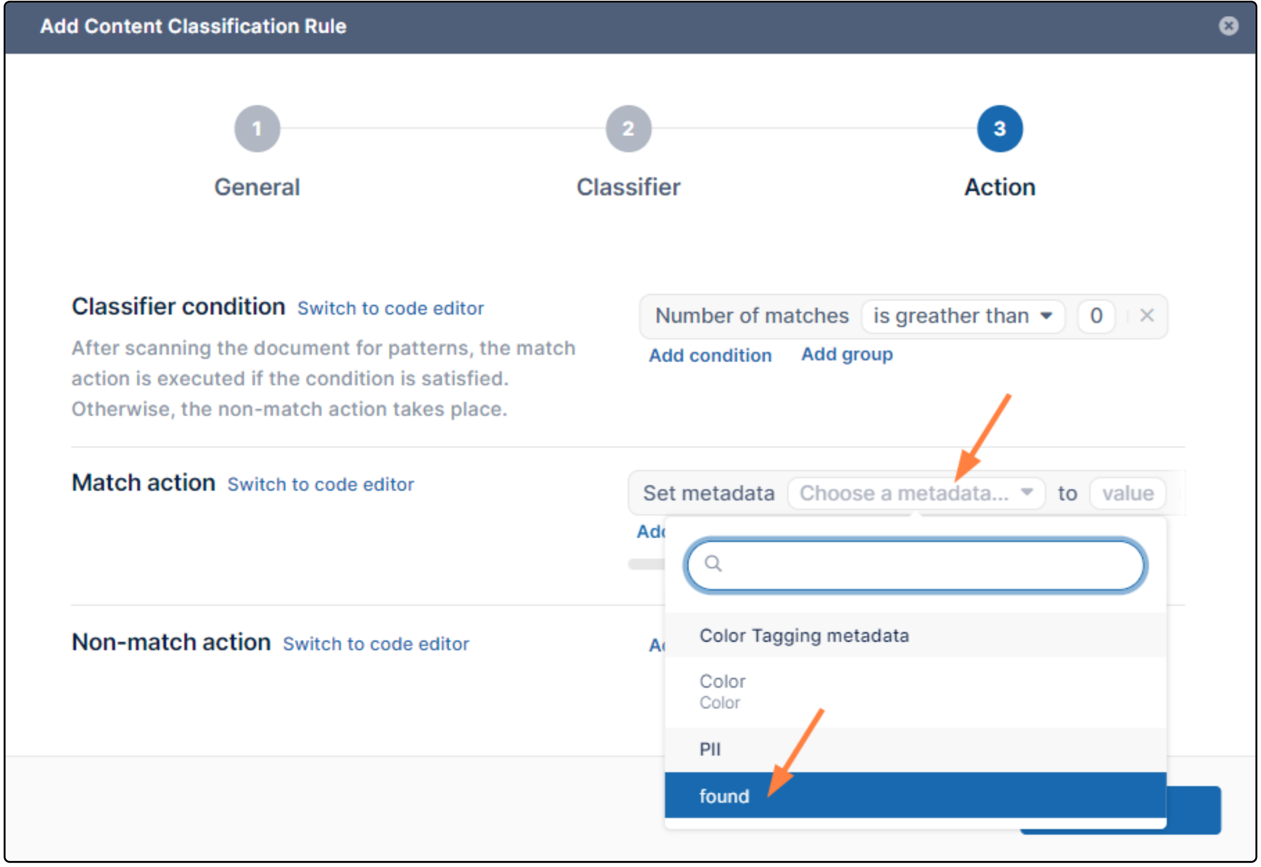
17. Add a **Match action** either by clicking **Add action** and choosing **Set metadata to value**, or, if you are familiar with JSON, by clicking **Switch to code editor**, and adding an action in JSON.

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.

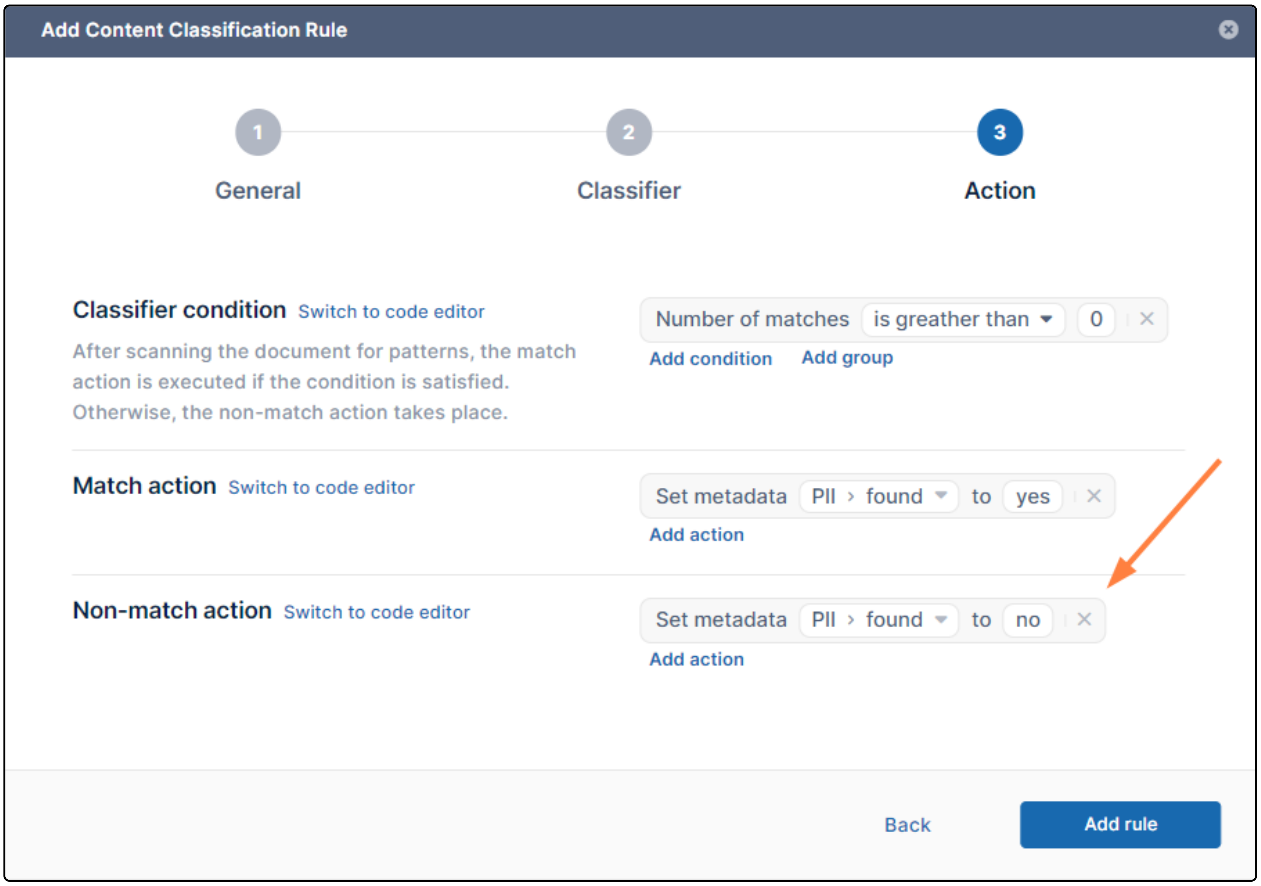


18. Click in the **Choose a metadata** field. **Color Tagging metadata** and any custom metadata you have created is listed with its attributes below it.

19. Click one of the metadata attributes.
    In this example, the **PII** metadata attribute **found** is selected.



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**.



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 greather than | 0

Match action Switch to code editor

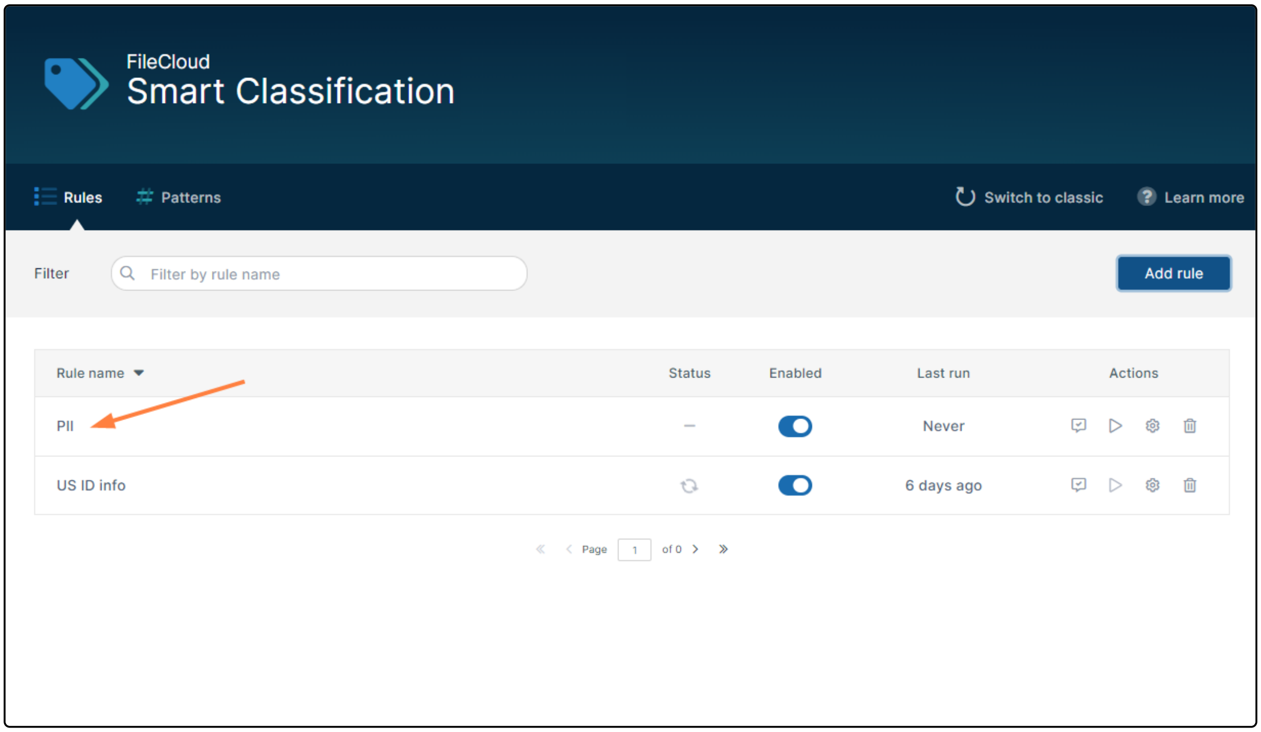
Set metadata | PII › found | to | yes

Non-match action Switch to code editor

Set metadata | PII › found | to | no

Your rule is complete.

22. Click **Add rule**.
    The wizard closes and your rule is added to the Smart Classification page.

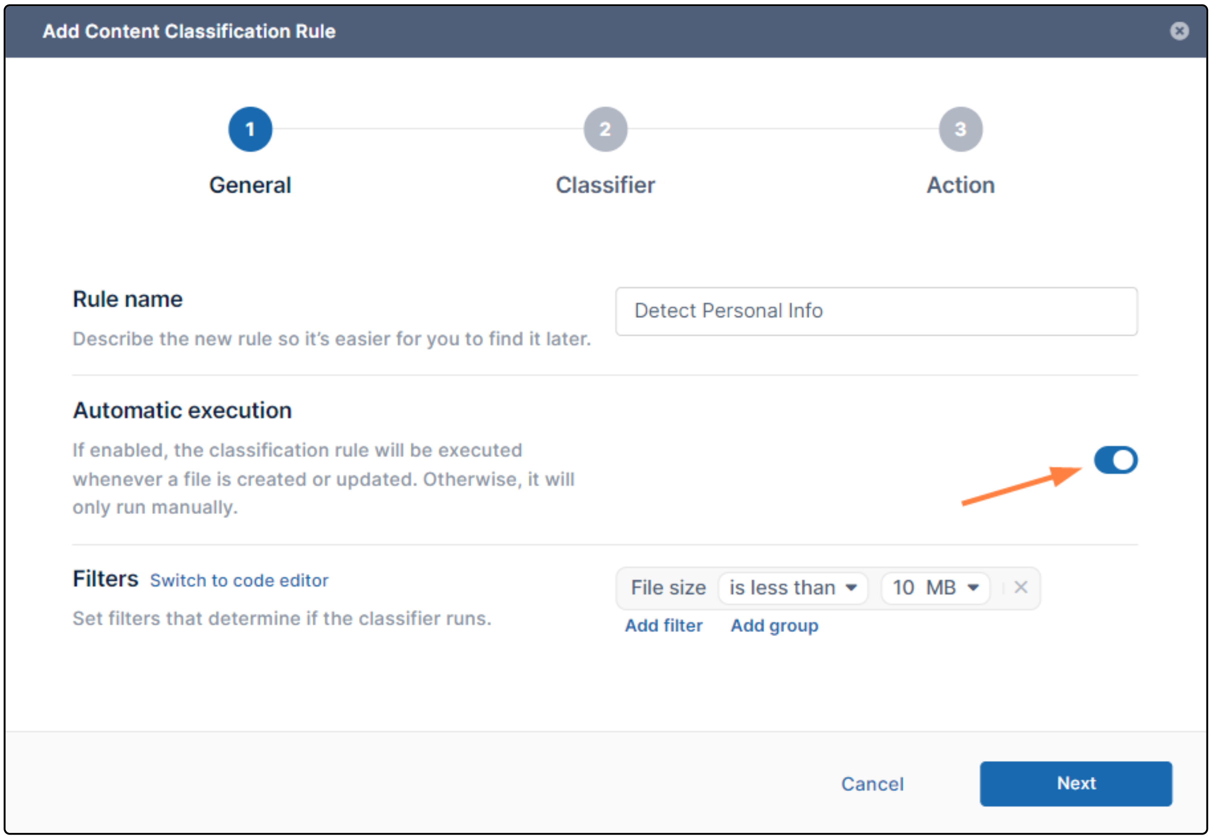


Rule name	Status	Enabled	Last run	Actions
PII	–	●	Never	
US ID info		●	6 days ago	

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 as long as you have set up a Cron job to run at the scheduled intervals. 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).



Rule name

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

Detect Personal Info

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

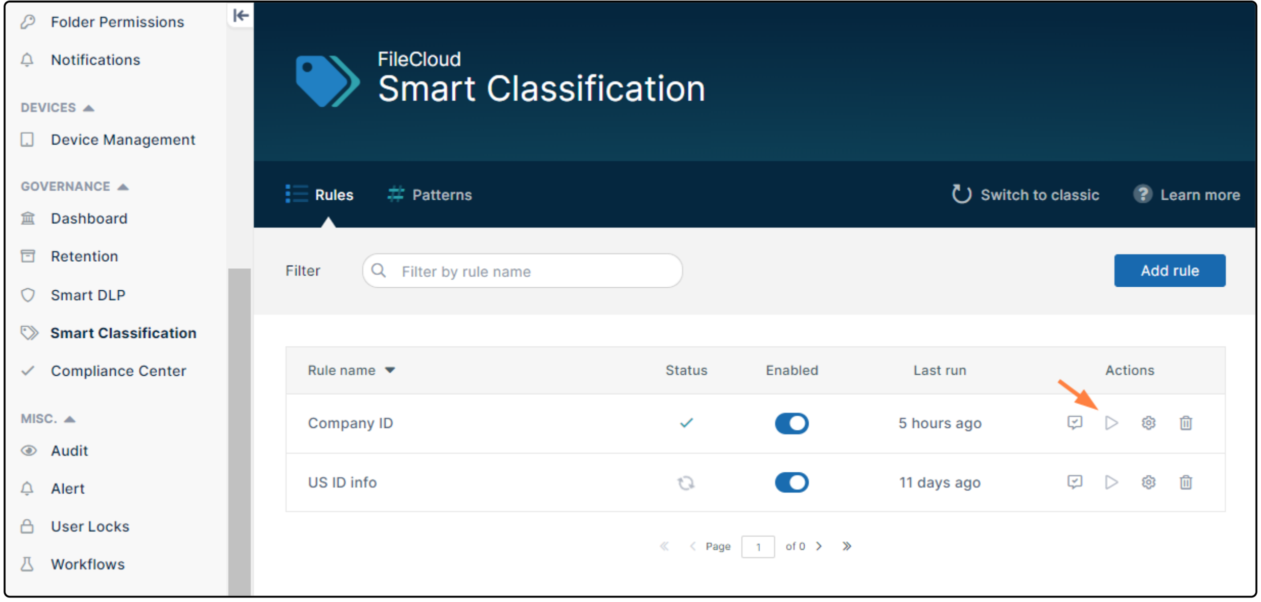
Set filters that determine if the classifier runs.

File size | is less than | 10 MB

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

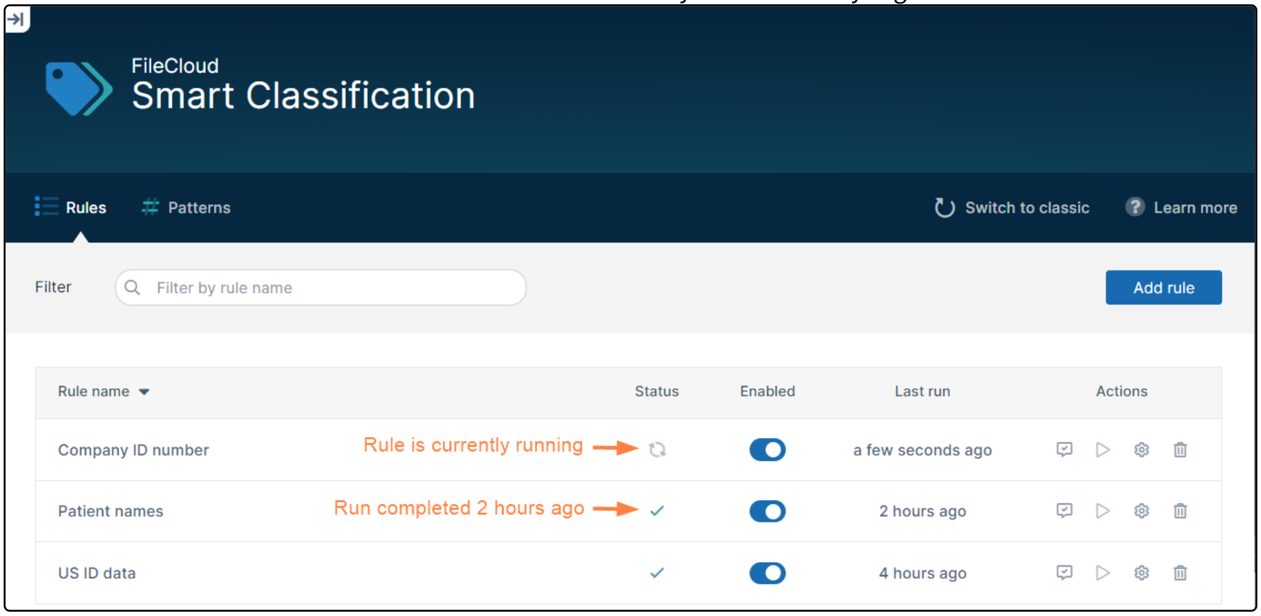
To run a Smart Classification rule manually:

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.

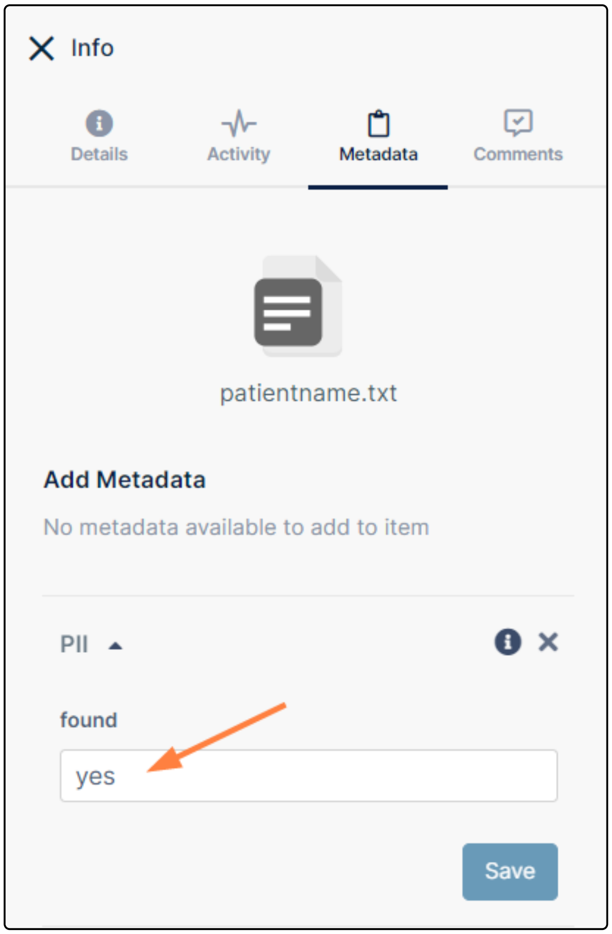


Rule name	Status	Enabled	Last run	Actions
Company ID number	↻	●	a few seconds ago	
Patient names	✓	●	2 hours ago	
US ID data	✓	●	4 hours ago	

Rule is currently running

Run completed 2 hours ago

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



patientname.txt

Add Metadata

No metadata available to add to item

PII

found

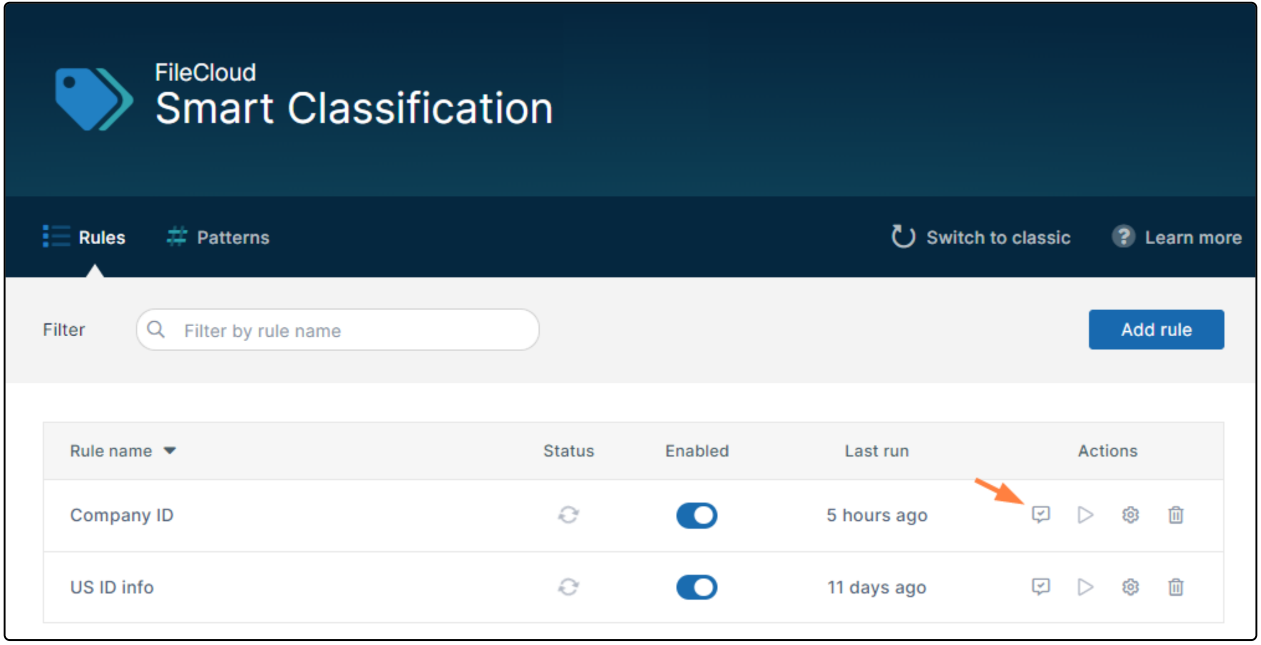
yes

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.

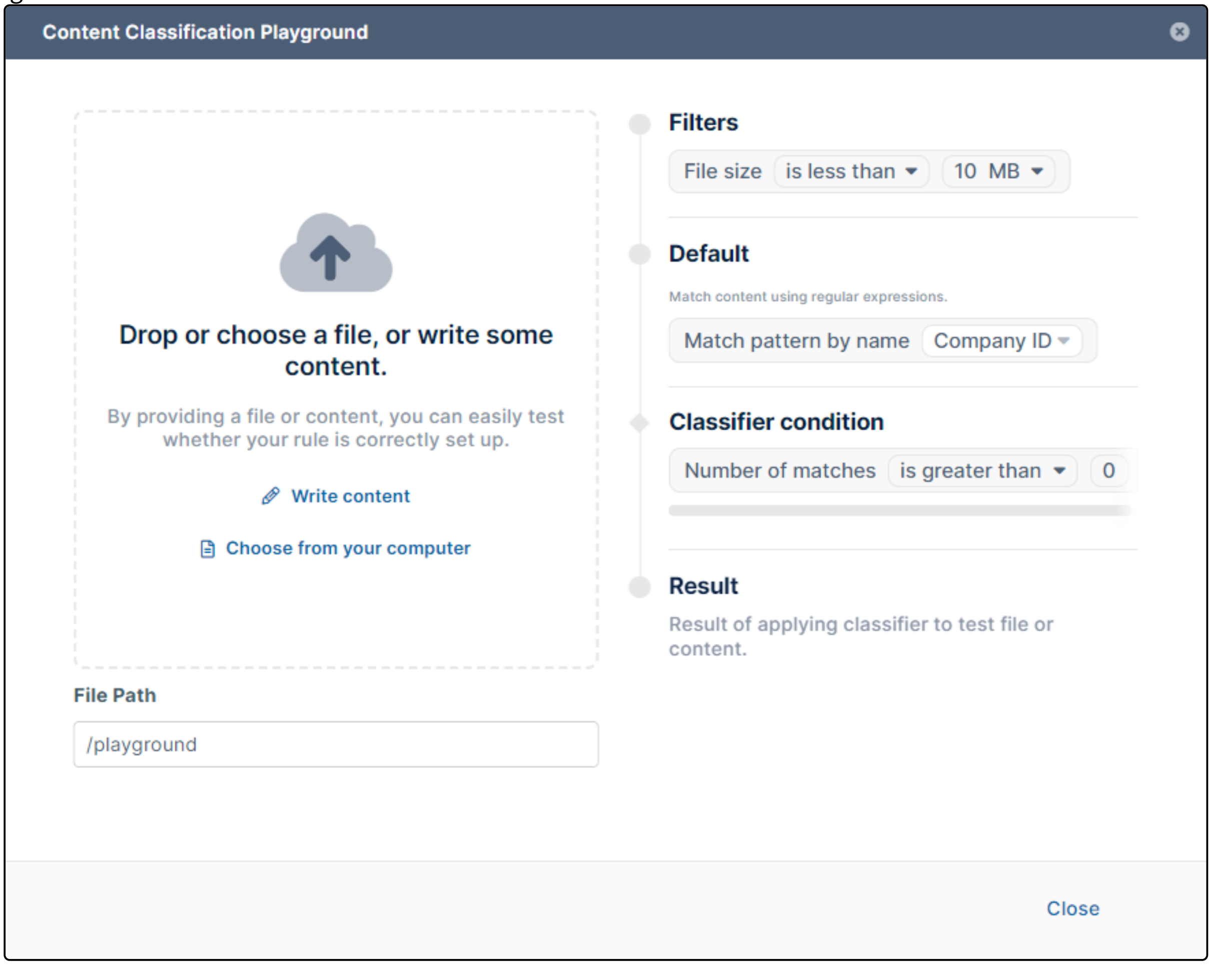
To test a Smart Classification rule:

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.



Drop or choose a file, or write some content.

By providing a file or content, you can easily test whether your rule is correctly set up.

File Path: /playground

Filters

File size is less than 10 MB

Default

Match content using regular expressions.

Match pattern by name Company ID

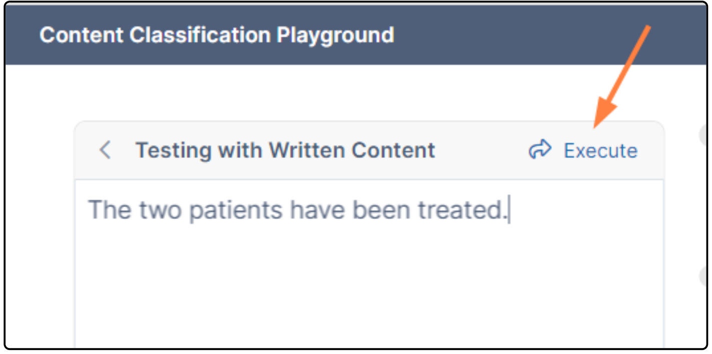
Classifier condition

Number of matches is greater than 0

Result

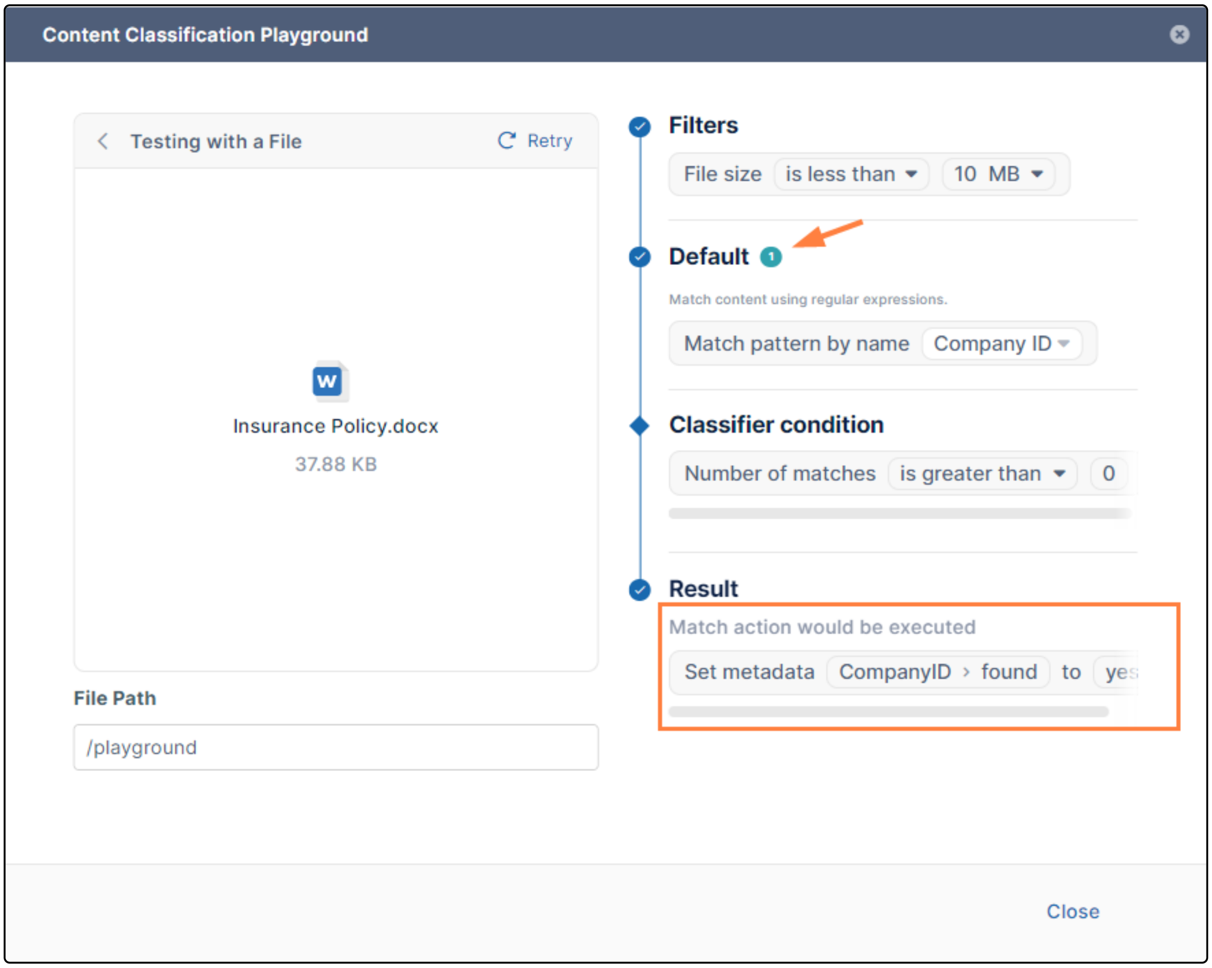
Result of applying classifier to test file or content.

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:


Content Classification Playground
Testing with Written Content
Execute

The two patients have been treated.

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**.



Insurance Policy.docx
37.88 KB

File Path
/playground

Filters
File size is less than 10 MB

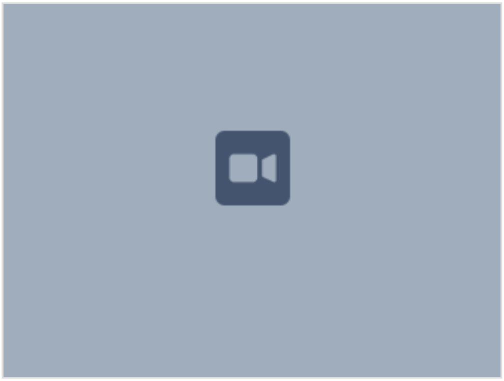
Default 1
Match content using regular expressions.
Match pattern by name Company ID

Classifier condition
Number of matches is greater than 0

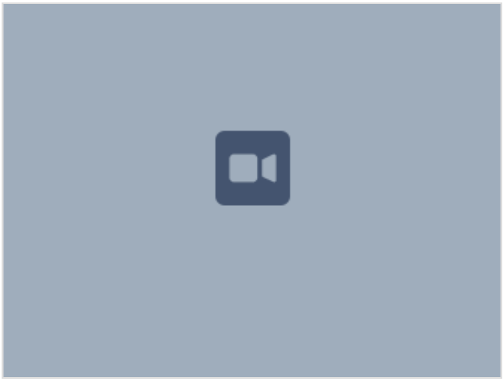
Result
Match action would be executed
Set metadata CompanyID › found to yes

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**.



Guide 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"}, ...]

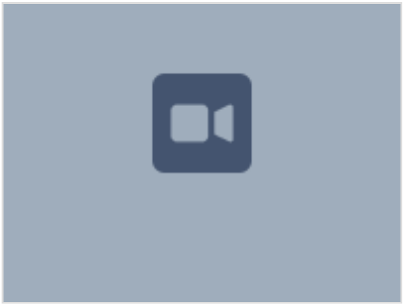
Pattern options:

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

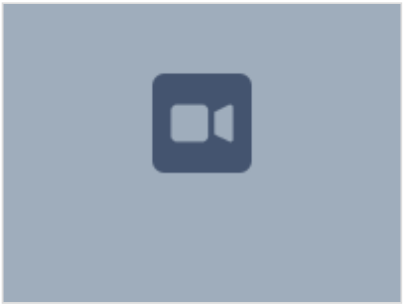
- **Match RegEx** - Match with a manually-entered regular expression
- **Match pattern by name** - Match with predefined regular expression
- **Match pattern by group** - Match with a predefined group of regular expressions

Examples:

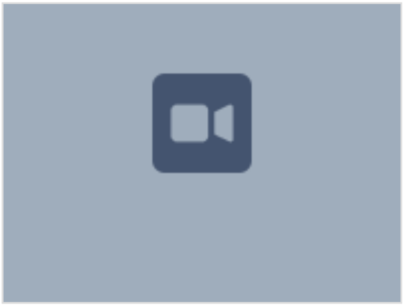
Match with RegEx:



Match pattern by name:



Match pattern by group:



Code 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", ...]
```

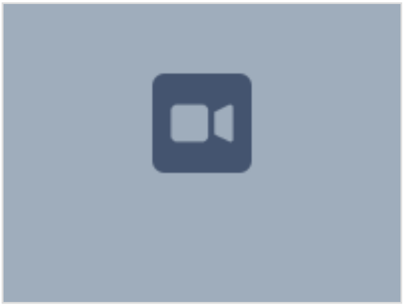
Pattern options:

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

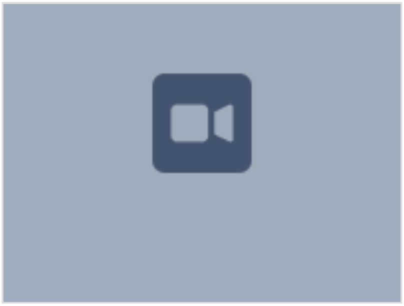
- **Match RegEx** - Match with a manually-entered regular expression
- **Match pattern by name** - Match with predefined regular expression
- **Match pattern by group** - Match with a predefined group of regular expressions

Examples:

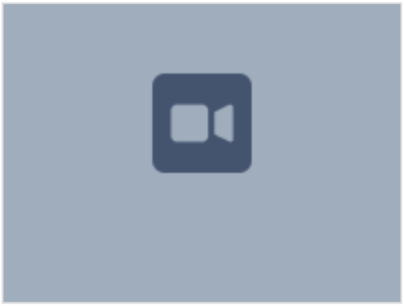
Match with RegEx:



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

Result schema to use if using code editor:

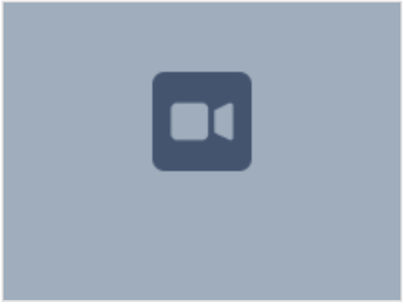
```
(_classifications): ["expression"] or []
```

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:



Code editor example:

{"STANDARD_QUERY_EXPRESSION":["confidential"]}

ICAP DLP

ICAP DLP

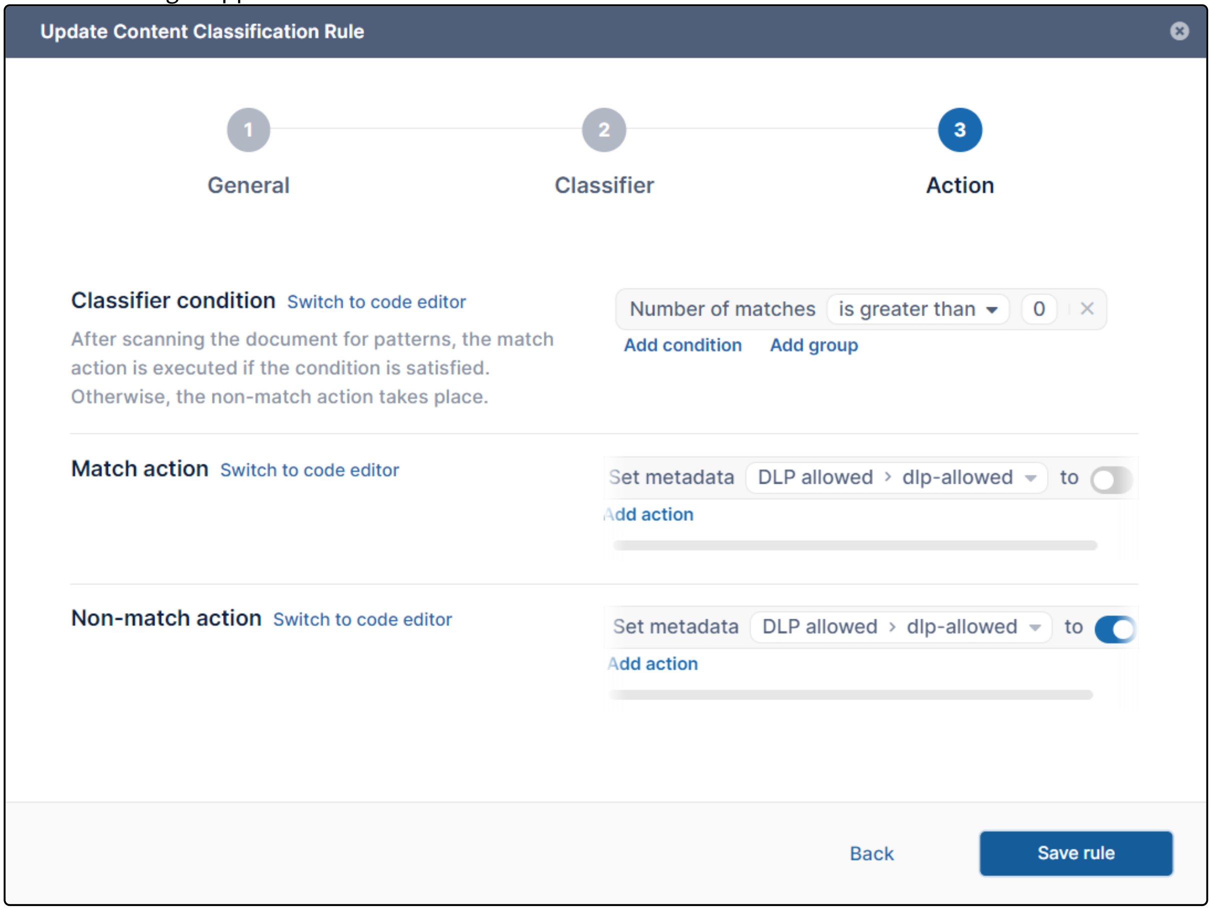
To enable selection of the the ICAP DLP classifier, you must enable ICAP DLP in FileCloud.

For the ICAP DLP classifier to function properly in FileCloud, you must set up rules in ePolicy Orchestrator 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

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

Set metadata | DLP allowed › dlp-allowed | to ○

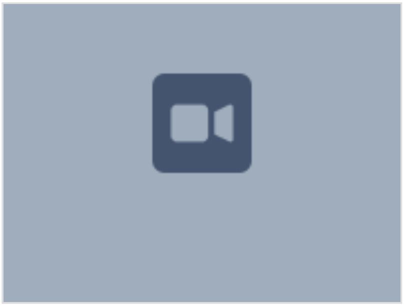
Non-match action Switch to code editor

Set metadata | DLP allowed › dlp-allowed | to ●

Result schema to use if using code editor:

(_classifications): []

Example



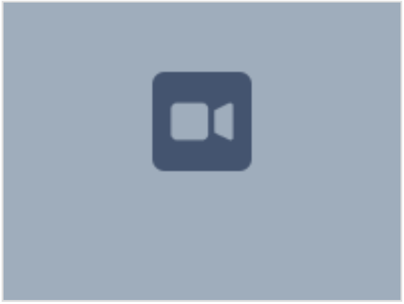
SingaporeNRIC

SingaporeNRIC

Definition

Classifies content by whether or not it matches a Singapore National Registration Identity Card.

Example:



AI Classifier

AI Classifier

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

Definition

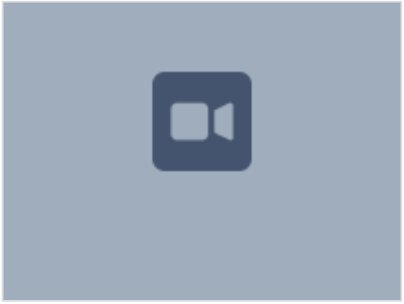
Classifies content into terms that match an AI prompt

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:



Code editor example:

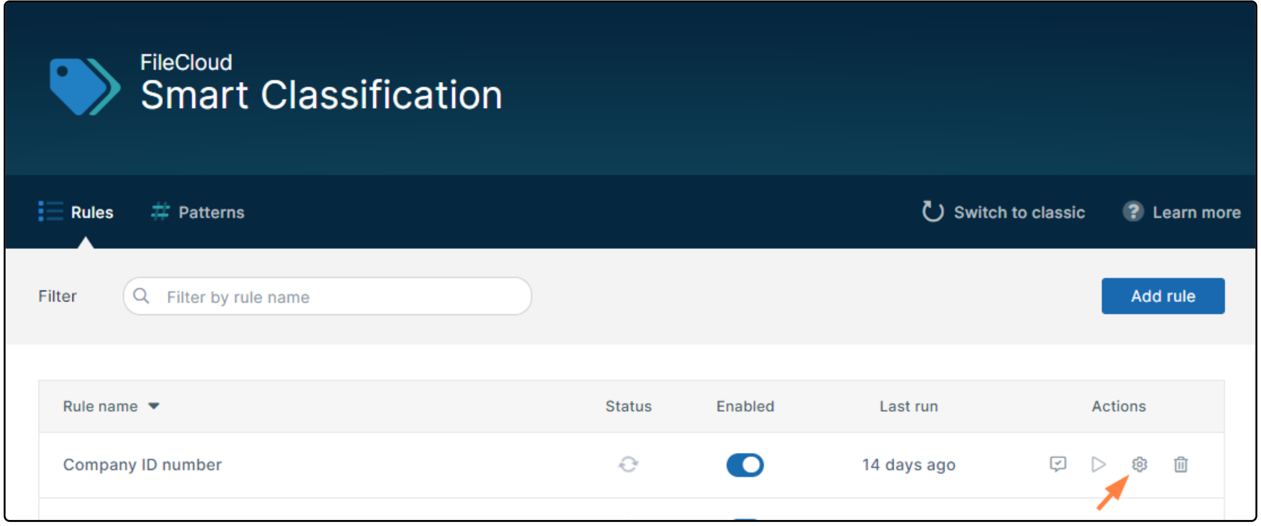
{"SEARCH_AI_MATCHES":["PII"]}

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

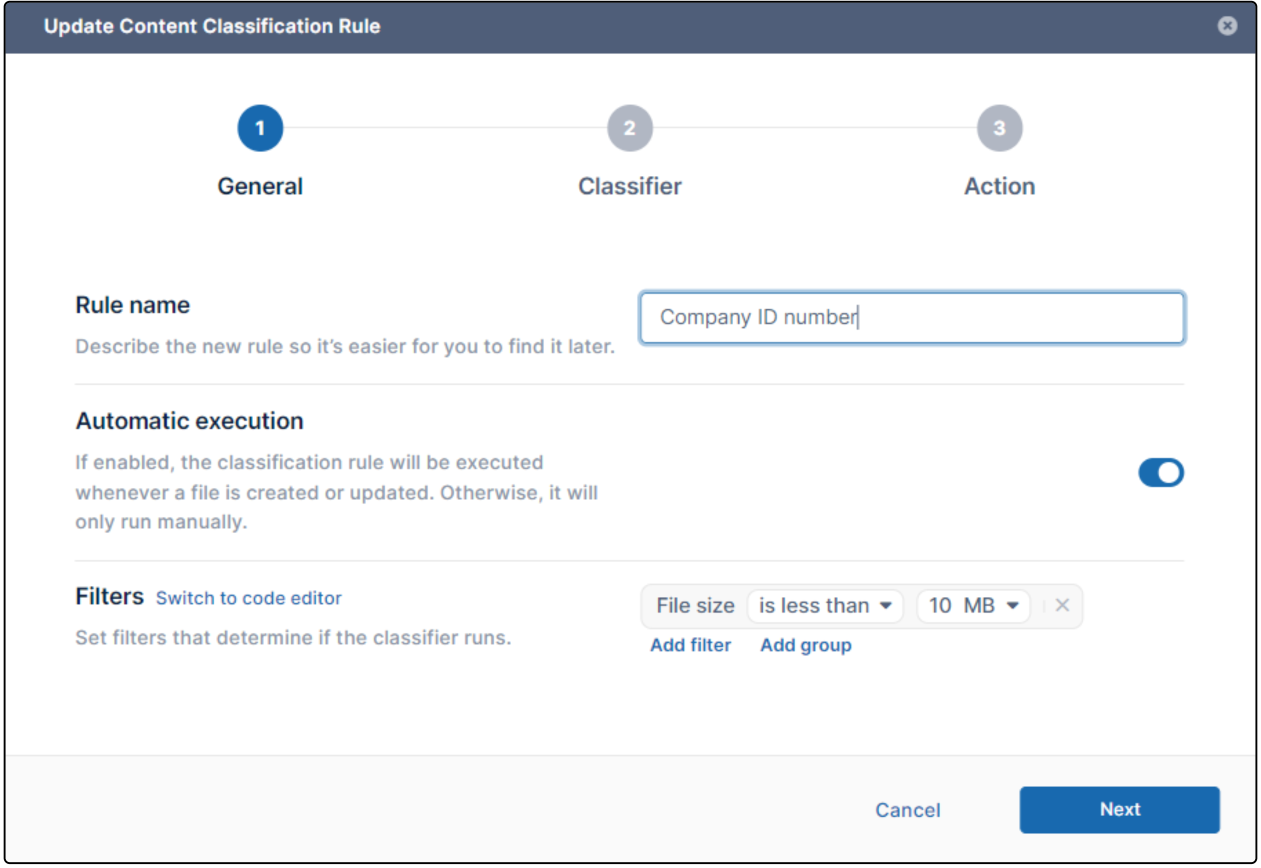
To edit a Smart Classification rule:

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



Rule name	Status	Enabled	Last run	Actions
Company ID number			14 days ago	

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



Update Content Classification Rule

Rule name: Company ID number

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: File size is less than 10 MB

Set filters that determine if the classifier runs.

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**.

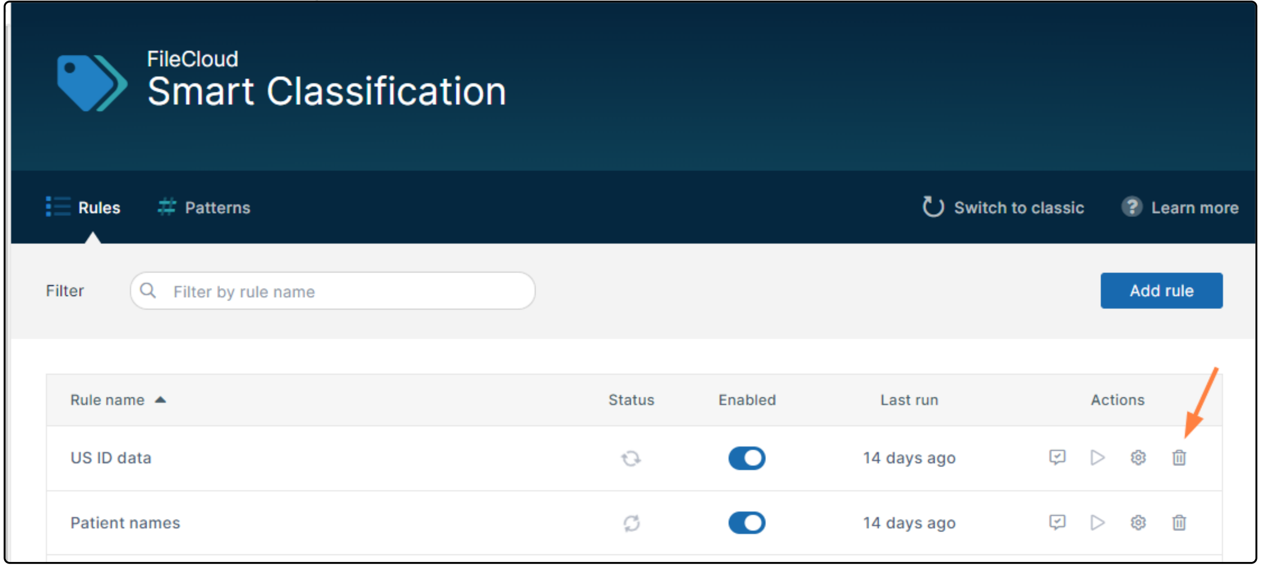
   The rule now applies the changed settings when it runs.

   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.



Rule name ▲	Status	Enabled	Last run	Actions
US ID data		●	14 days ago	
Patient names		●	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)]**

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

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

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

Identifying all files containing US social security numbers

Rule name	**Tag all files with US social security numbers**
Automatic execution	**Enable**
Filters	**Anything**
Classifier	**Default**

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

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

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

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

Rule name	**France ID numbers**
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**
Filters	**Anything**

Classifier	**Default**
Classifier patterns	**Match RegEx** [3[47]{1}[0-9]{13}] **OR** **Match RegEx** [3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}] **OR** **Match RegEx** [3[47]{1}[0-9]{2} [0-9]{4} [0-9]{4} [0-9]{3}] Note: Smart Classification automatically inserts **OR** when you add multiple **Classifier** patterns.
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 the exact phrase "Confidential - for internal use only"

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

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 [[0-9]{5}]**
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**
Classifier patterns	**Match Standard Query ["Confidential - for internal use only"~4]** (include "" around phrase) **Note**: ~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.

Classifier condition	**Number of matches [is greater than 0]**
Match action	**Set [IncludesText.Confidential] to yes**
Non-match action	**Set [IncludesText.Confidential] to no**

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

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

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**

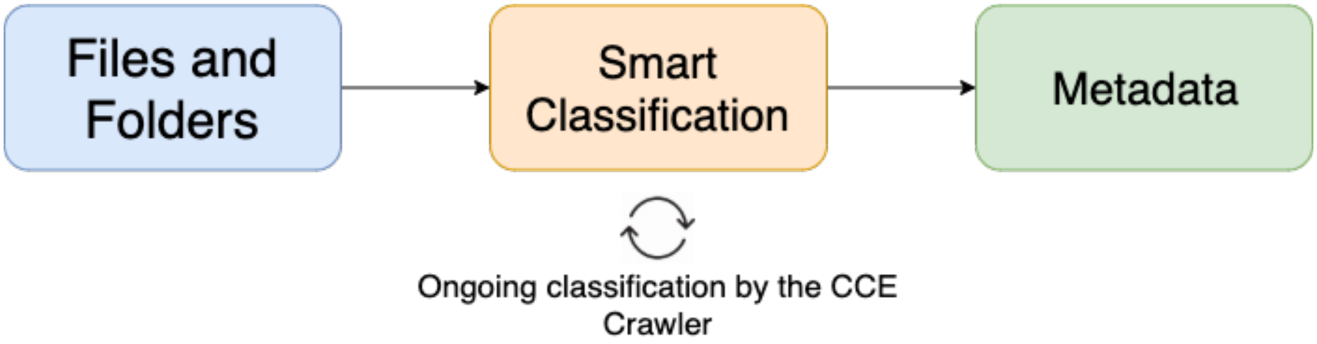
Classifier	**AI Classifier**
Classifier patterns	**Match instances of [phone numbers]** **OR** **Match instances of [email addresses]**
Classifier condition	**Number of matches [is greater than 0]**
Match action	**Set [ContactInfo.detected] to yes**
Non-match action	**Set [ContactInfo.detected] to no**

Smart Classification Classic

Beginning in FileCloud 23.232, an updated version of the Smart Classification user interface is available. Please see Smart Classification 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.

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.

Configure Content Search for Managed Storage

SOLR Configuration Tips

Create New Metadata Set

Get Started with CCE

Creating and Managing Content Classification Engine Rules

CCE Rule Examples

Creating a Pattern

Creating a Pattern Group

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.

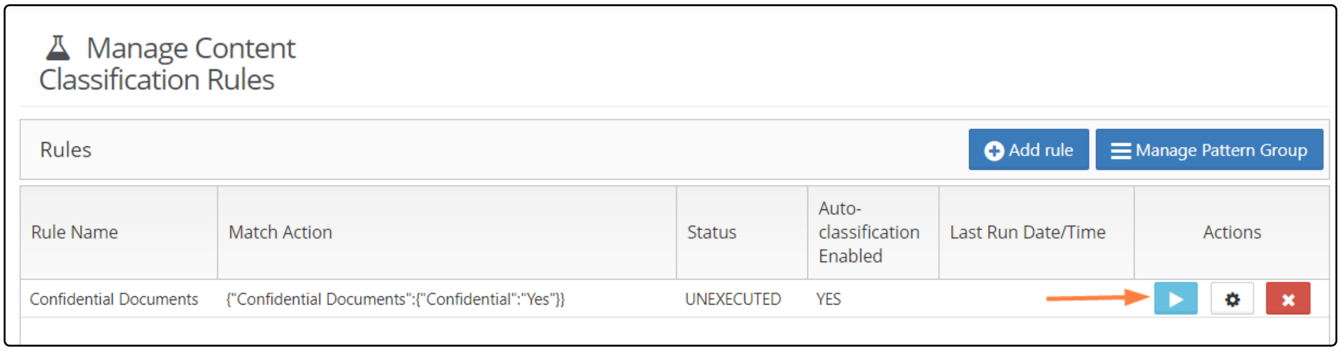
Automating the Crawler

To control the automation of the classification process, as well as choosing when the crawler runs, administrators can use Cron Jobs.

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

Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
Confidential Documents	{"Confidential Documents":{"Confidential":"Yes"}}	UNEXECUTED	YES		▶ ⚙ ✖

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:

FileCloud Videos	FileCloud Blogs
	- Classify Documents in FileCloud using Smart Classification

Creating and Managing Content Classification Engine Rules

Keyword Definitions

Below are the keywords used in creating the rule definition:

Classifier	Classifier used to classify the file content.
	Note: Classification is not case sensitive.
	In most cases, you can use:
	• **Default** - Classify content into terms that match the supplied regex patterns.
	`Supported parameters: SEARCH_PATTERN_SET, SEARCH_PATTERN_NAME or SEARCH_PATTERN_GROUP`
	`Result Schema (_classifications): [{term: "term that matched a regex", count: "number of times the term appears in the doc"}, ...]`
	Also supported are:
	• **PatternMatch** - Classify content into regex patterns found.
	`Supported parameters: SEARCH_PATTERN_SET, SEARCH_PATTERN_NAME or SEARCH_PATTERN_GROUP`
	`Result Schema (_classifications): ["regex pattern", ...]`
	• **StandardQuery** - Classify content as matching the query or not.
	`Supported parameters: STANDARD_QUERY_EXPRESSION`
	`Result Schema (_classifications): ["expression"] or []`
	• **IcapDLP** - Classify content based on results returned from ICAP DLP.
	`Supported parameters: none`
	`Result Schema (_classifications): []`
	• **SingaporeNRIC**- Classify content into terms that match a Singapore NRIC.
	`Supported parameters: none`
	`Result Schema (_classifications): [{term: "NRIC term", count: "number of times the NRIC term appears in the doc"}, ...]`

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}/

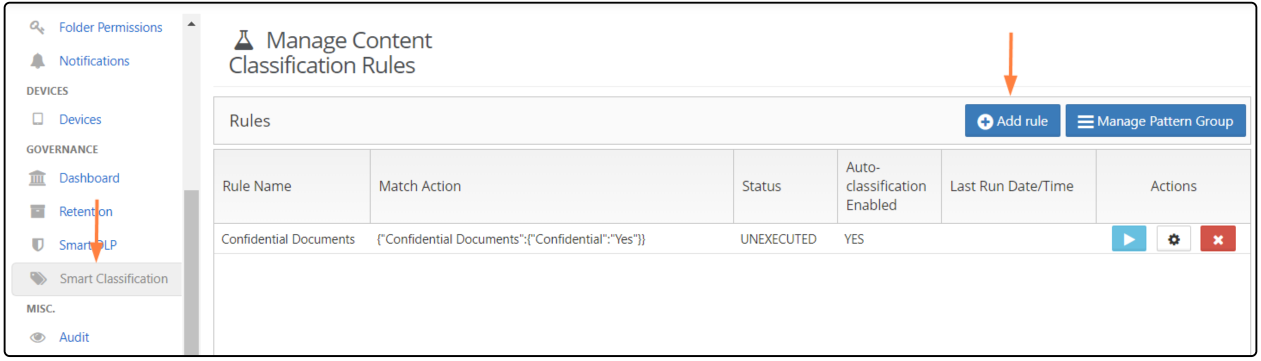
SEARCH_PATTERN_NAME	Regular Expression assigned a name through Manage Pattern Group - Available Patterns
SEARCH_PATTERN_GROUP	Regular Expressions grouped through Manage Pattern Group - Pattern Group.
Match Action	Actions taken when the classifier finds a file based on precondition, condition and parameters. 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:

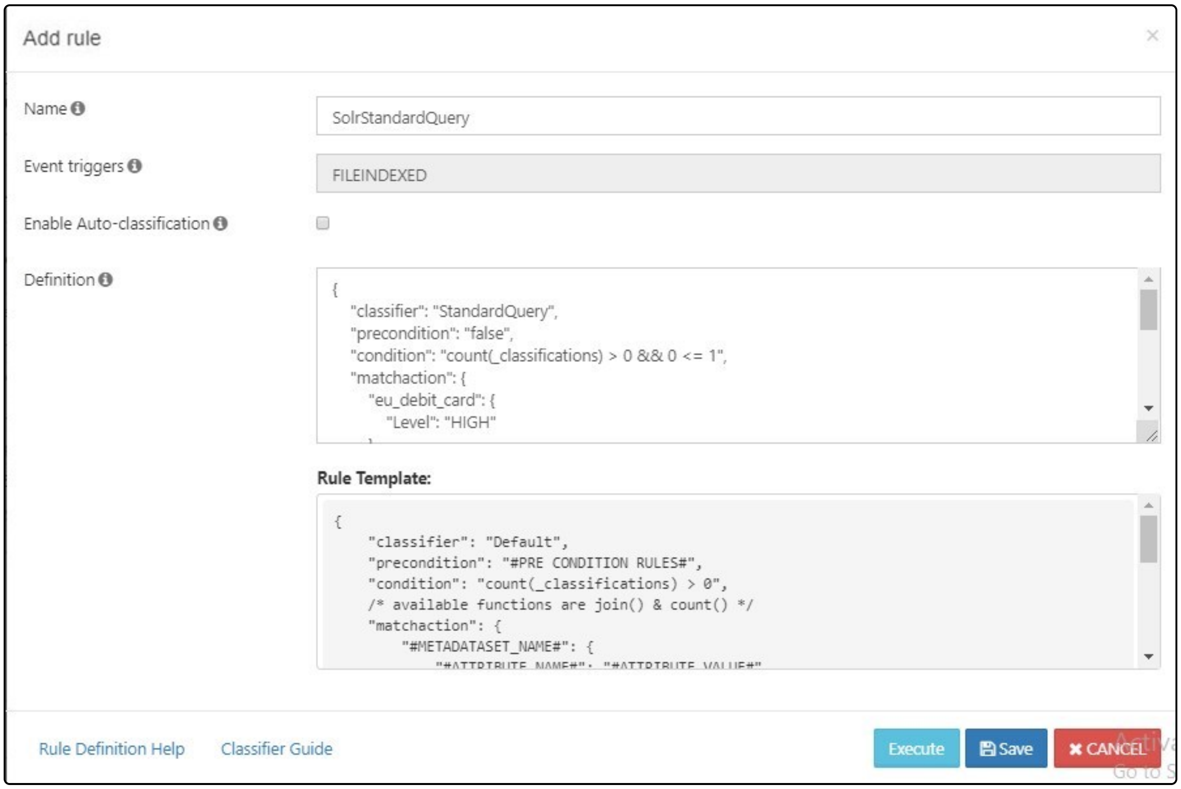
1. To open the **Manage Content Classification Rules** page, in the Admin portal's navigation pane, click **Smart Classification.**
2. To add or create a new rule, click **Add Rule**.



Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
Confidential Documents	{"Confidential Documents":{"Confidential":"Yes"}}	UNEXECUTED	YES		

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.



Name: SolrStandardQuery

Event triggers: FILEINDEXED

Enable Auto-classification: □

Definition:

```
{
   "classifier": "StandardQuery",
   "precondition": "false",
   "condition": "count(_classifications) > 0 && 0 <= 1",
   "matchaction": {
      "eu_debit_card": {
         "Level": "HIGH"
```

Rule Template:

```
{
    "classifier": "Default",
    "precondition": "#PRE CONDITION RULES#",
    "condition": "count(_classifications) > 0",
    /* available functions are join() & count() */
    "matchaction": {
        "#METADATASET_NAME#": {
            "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#"
```

4. Click **Save**.

See Example Rules.

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.Confidentialilty 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":  []
```

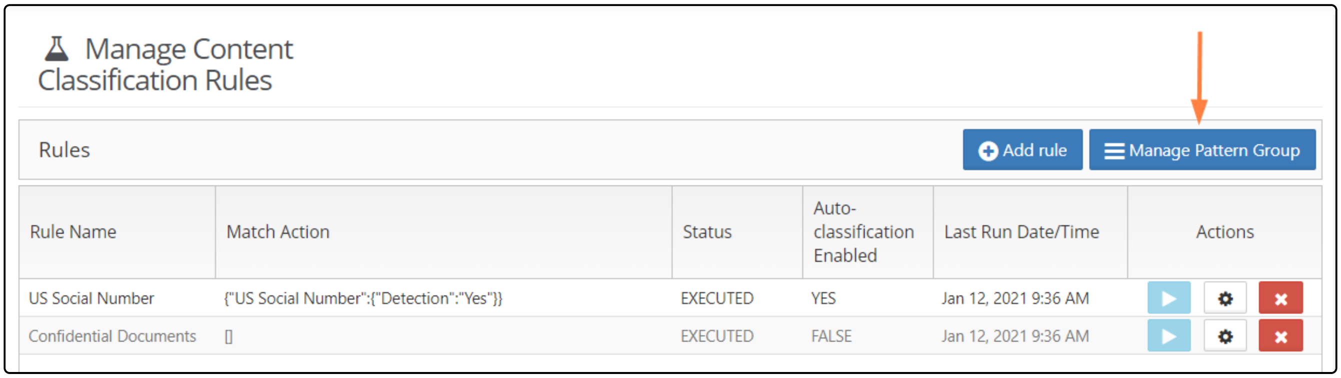
```
    }
}
```

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'

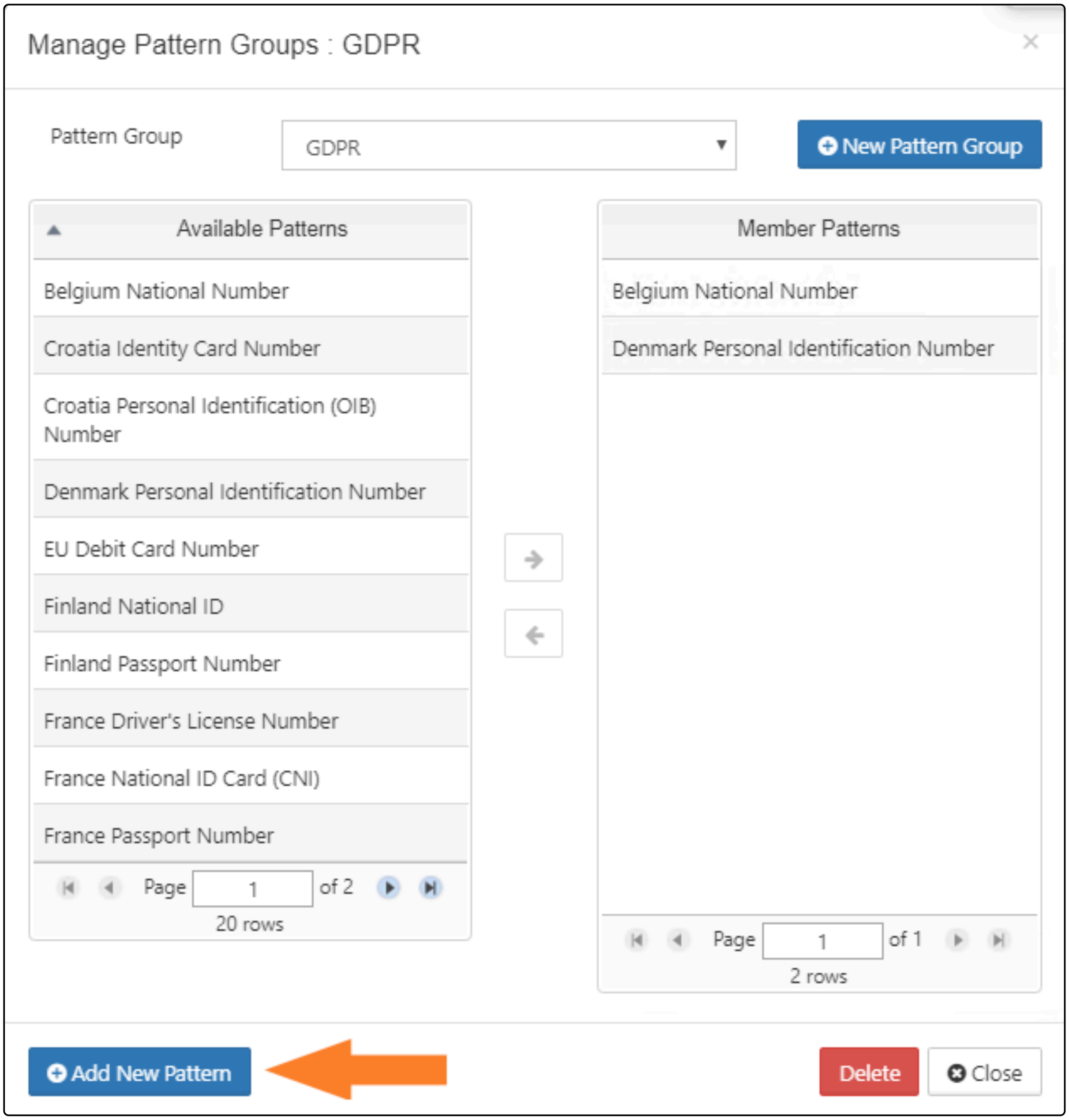


Manage Content Classification Rules

Rules

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

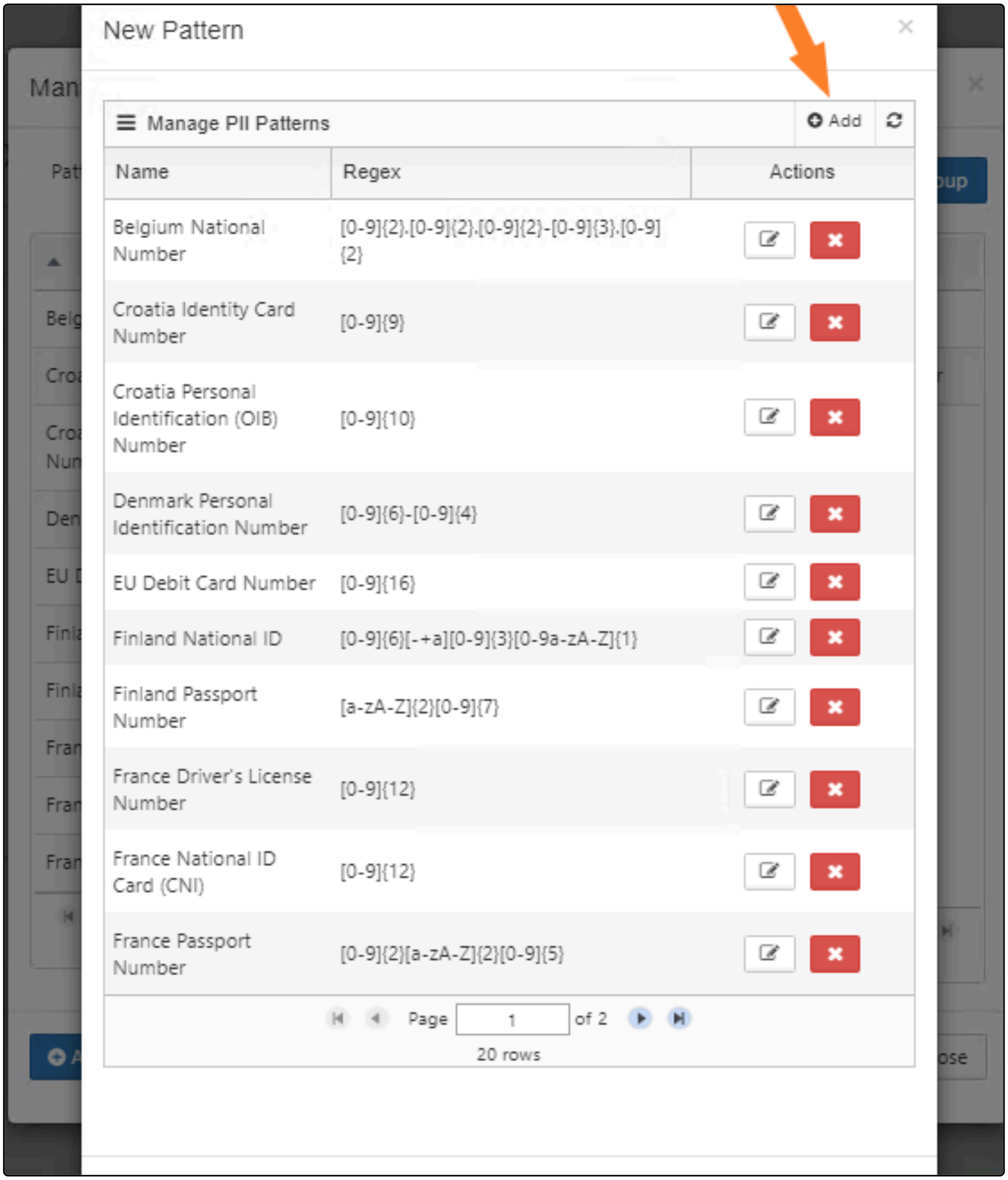
Available Patterns
Belgium National Number
Croatia Identity Card Number
Croatia Personal Identification (OIB) Number
Denmark Personal Identification Number
EU Debit Card Number
Finland National ID
Finland Passport Number
France Driver's License Number
France National ID Card (CNI)
France Passport Number

Page 1 of 2
20 rows

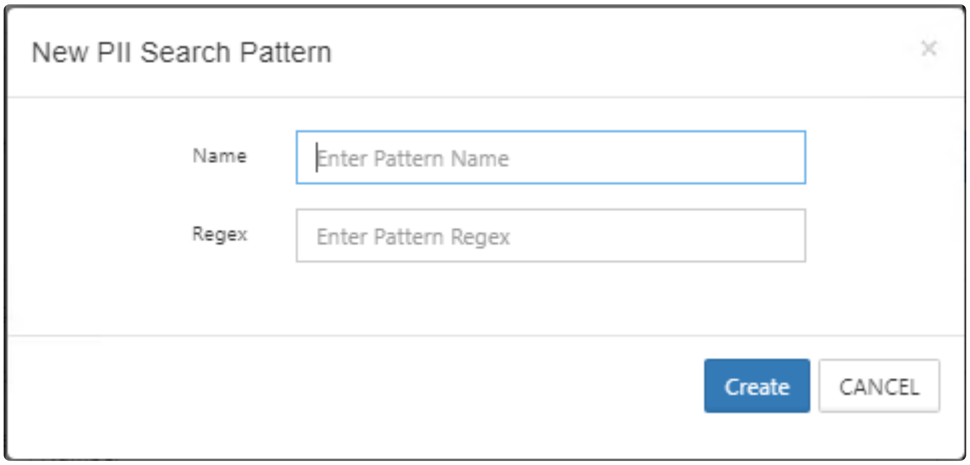
Member Patterns
Belgium National Number
Denmark Personal Identification Number

Page 1 of 1
2 rows

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



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}	✎ ✖



New PII Search Pattern

Name: Enter Pattern Name

Regex: Enter Pattern Regex

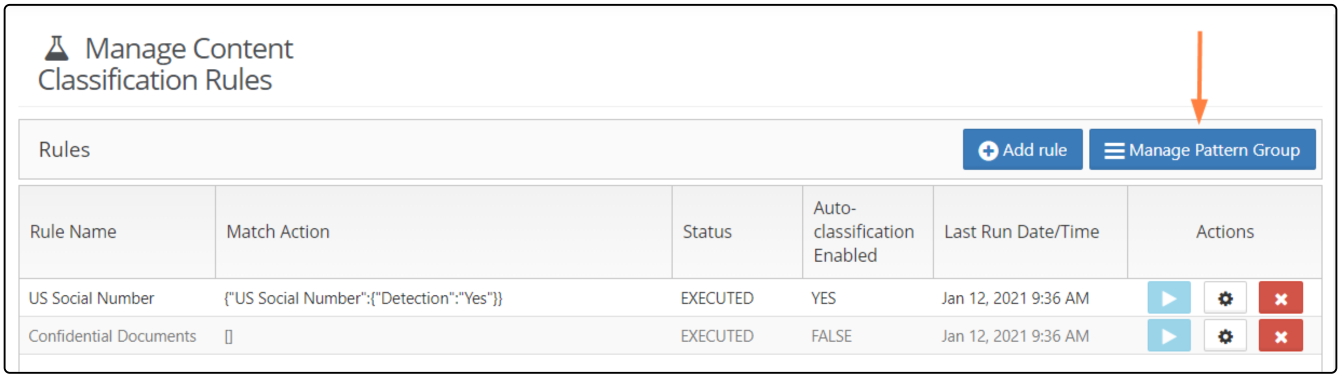
4. Once you have created your pattern, you should now be able to use it in a Content Classification rule or group it together with other patterns in a Pattern Group.

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'

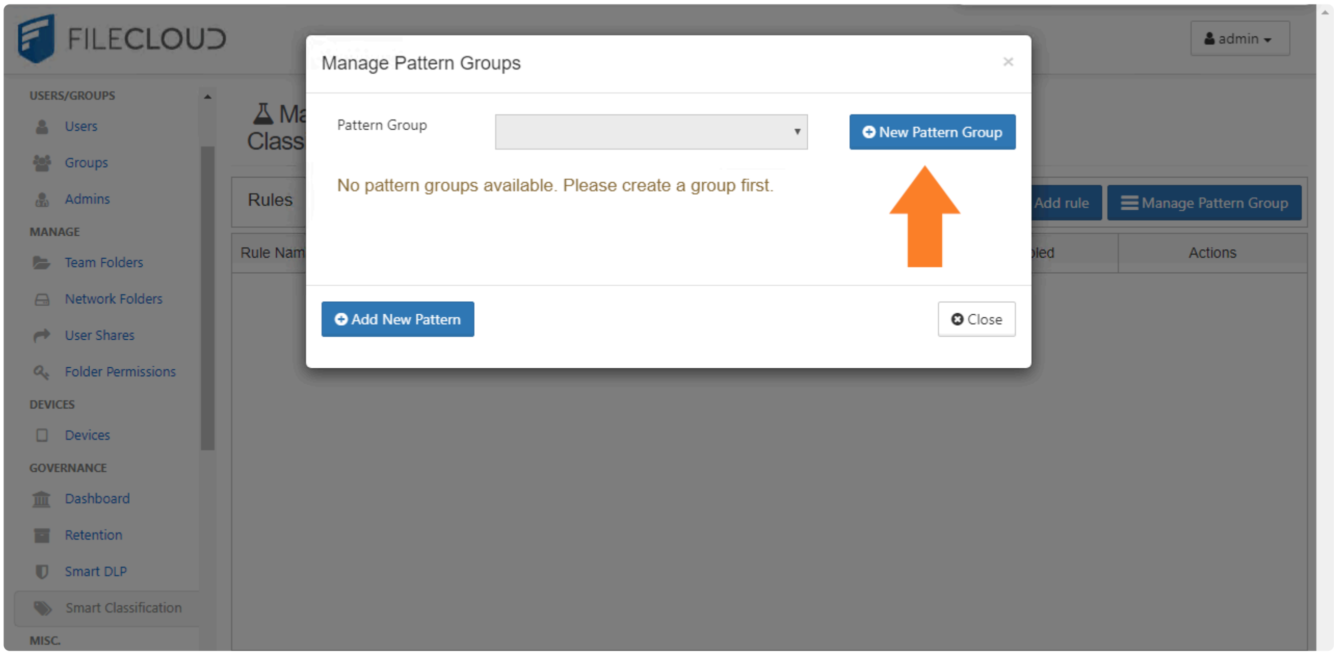


Manage Content Classification Rules

Rules

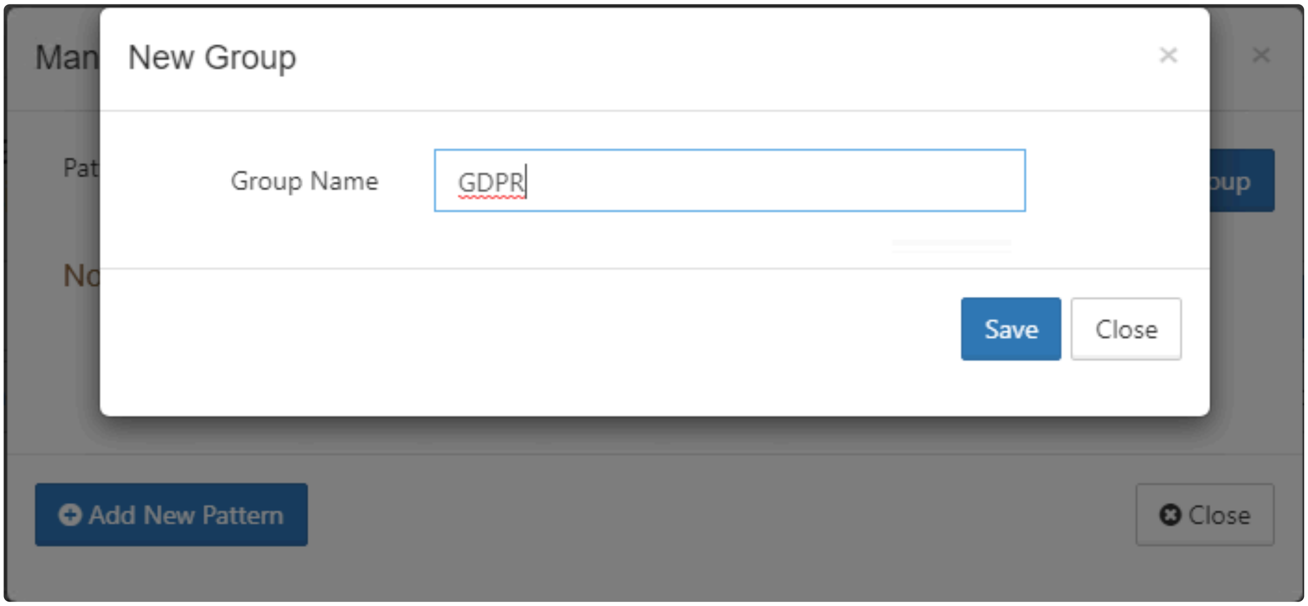
Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
US Social Number	{"US Social Number":{"Detection":"Yes"}}	EXECUTED	YES	Jan 12, 2021 9:36 AM	▶ ⚙ ✖
Confidential Documents	[]	EXECUTED	FALSE	Jan 12, 2021 9:36 AM	▶ ⚙ ✖

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



No pattern groups available. Please create a group first.

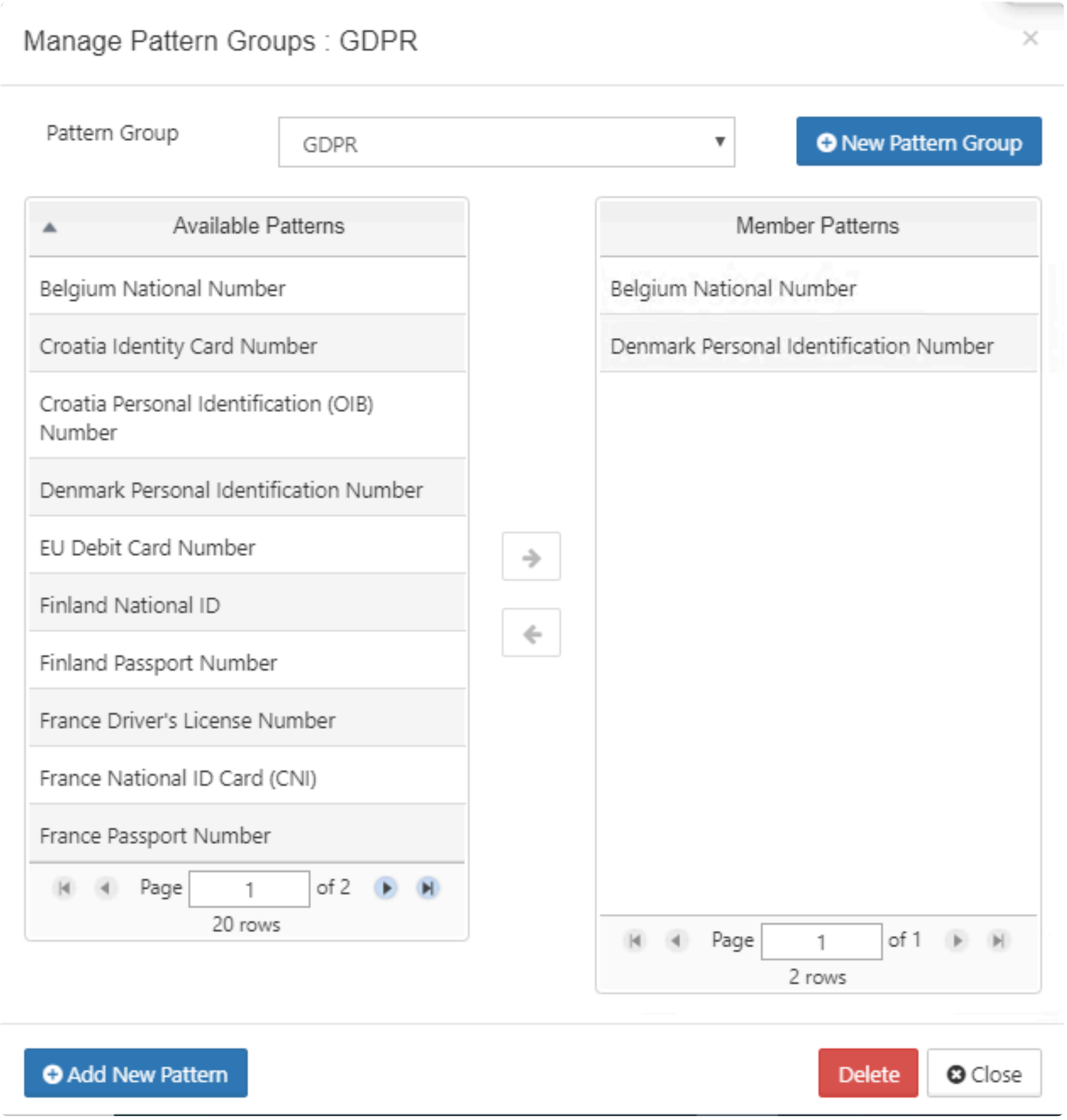
3. Click on New Pattern Group, enter a Group Name and click Save.



Group Name: GDPR

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 Patters 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

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

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\"" } }
```

Metadata in Log Files

As of FileCloud 20.1, custom metadata is included in audit logs of share and download operations.

Metadata is stored in the field *metadata* and appears in the format:

```
{
    "metadataName": {
        "attributeName": "value",
        "attributeName2": "value",
    }
}
```

To include non-custom metadata in logs, in

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define('TONIDOCLOUD_LOG_CUSTOM_METADATA_VALUES_ONLY', false);
```

Metadata is logged for the following actions:

- downloadfilemulti - Download multiple files.
- downloadfile - Download a single file.
- getaudio - Play an audio file.
- getvideo - Play a video file.
- getfsslideimage - View an image file.
- docconvert - Open or view a file.
- quickshare - Quick share.
- addusertoshare - Add specific users to a share.
- addgrouptoshare - Add specific groups to a share.
- setallowpublicaccess - Make a share public (after sharing only with certain users/groups).

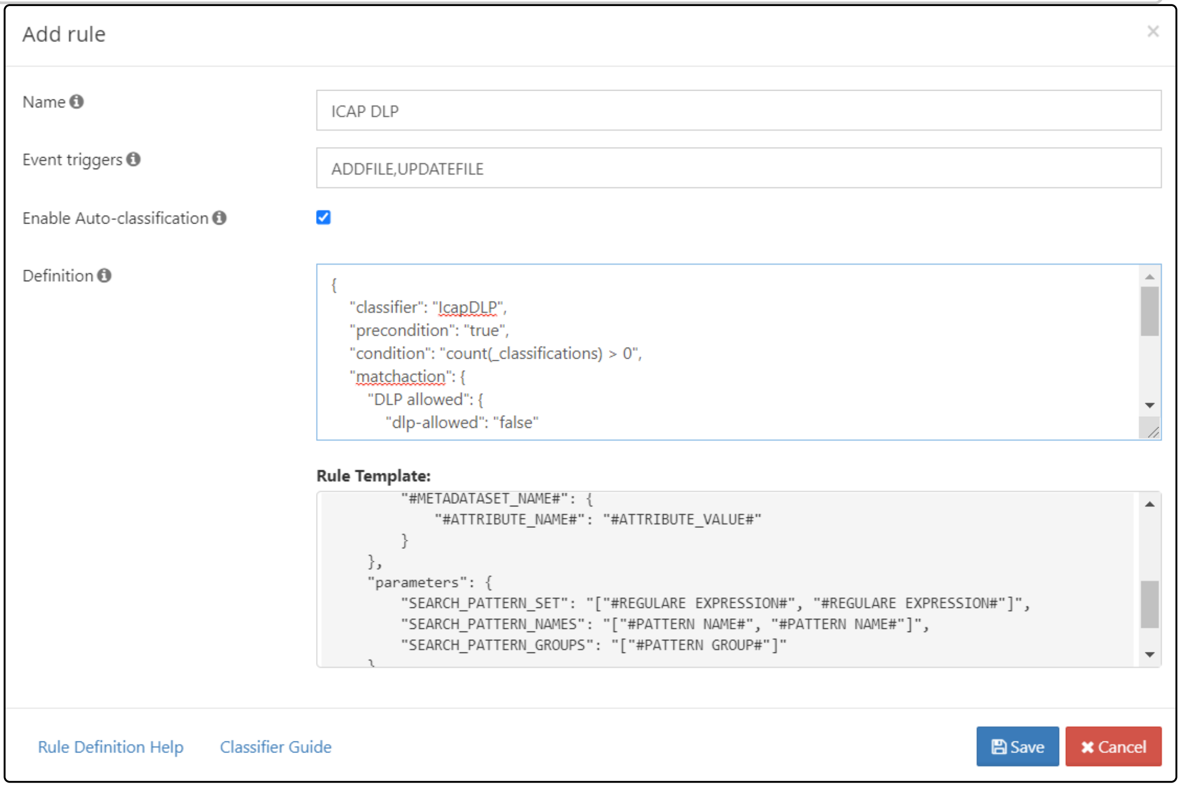
Using ICAP DLP with CCE

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, 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 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:

```
{
    "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: ☑

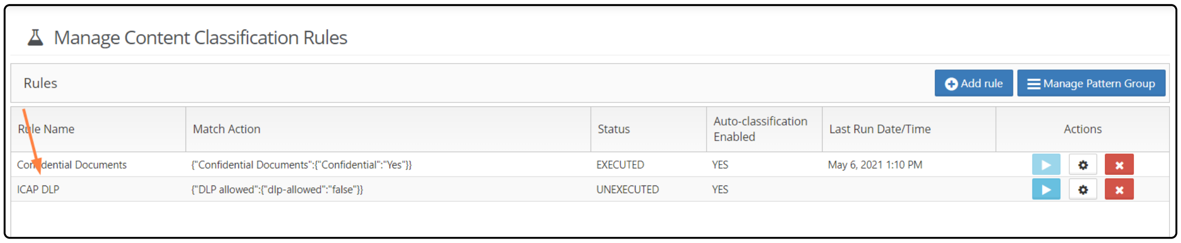
Definition:

```
{
    "classifier": "IcapDLP",
    "precondition": "true",
    "condition": "count(_classifications) > 0",
    "matchaction": {
      "DLP allowed": {
        "dlp-allowed": "false"
```

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#"]"
```

f. Click **Save**.



Manage Content Classification Rules

Rules

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, add rules that prevent download or sharing for files with the **dlp-allowed** metadata parameter set to false.

Smart DLP

✖ 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 works in conjunction with DLP to streamline, automate, and strengthen data security.

In this section

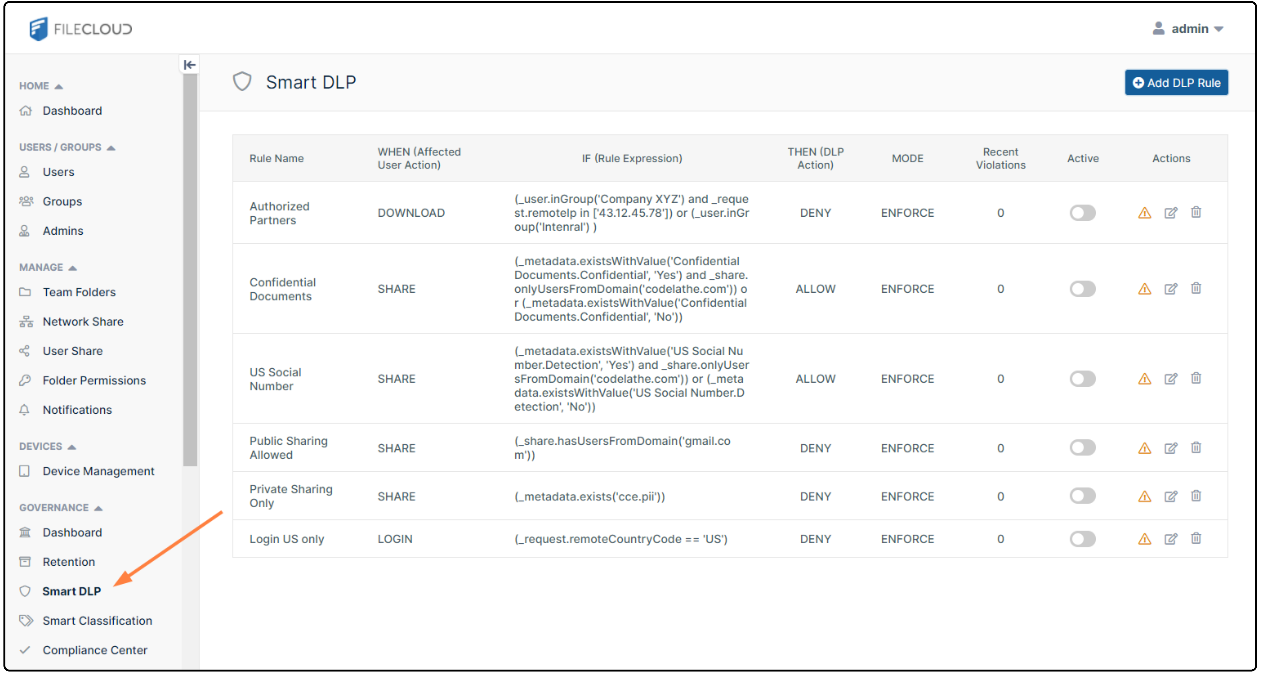
Creating Data Leak Prevention Rules

ℹ 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.

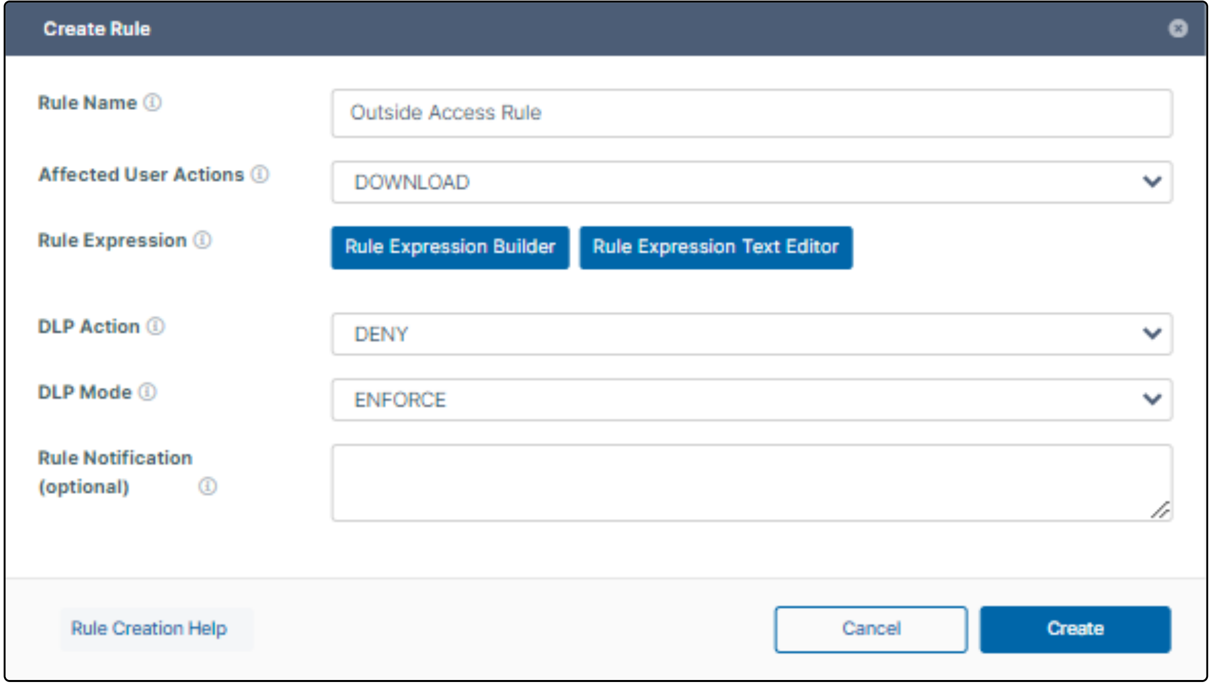
To create and edit DLP rules, follow the steps below:

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



Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	(_user.inGroup('Company XYZ') and _request.remoteIp in ['43.12.45.78']) or (_user.inGroup('Intenral'))	DENY	ENFORCE	0	○	⚠ ✎ 🗑
Confidential Documents	SHARE	(_metadata.existsWithValue('Confidential Documents.Confidential', 'Yes') and _share.onlyUsersFromDomain('codelathe.com')) or (_metadata.existsWithValue('Confidential Documents.Confidential', 'No'))	ALLOW	ENFORCE	0	○	⚠ ✎ 🗑
US Social Number	SHARE	(_metadata.existsWithValue('US Social Number.Detection', 'Yes') and _share.onlyUsersFromDomain('codelathe.com')) or (_metadata.existsWithValue('US Social Number.Detection', 'No'))	ALLOW	ENFORCE	0	○	⚠ ✎ 🗑
Public Sharing Allowed	SHARE	(_share.hasUsersFromDomain('gmail.com'))	DENY	ENFORCE	0	○	⚠ ✎ 🗑
Private Sharing Only	SHARE	(_metadata.exists('cce.pii'))	DENY	ENFORCE	0	○	⚠ ✎ 🗑
Login US only	LOGIN	(_request.remoteCountryCode == 'US')	DENY	ENFORCE	0	○	⚠ ✎ 🗑

2. To create a new rule, click **Add DLP Rule.**
The **Create Rule** dialog box opens:



Rule Name: Outside Access Rule

Affected User Actions: DOWNLOAD

Rule Expression

DLP Action: DENY

DLP Mode: ENFORCE

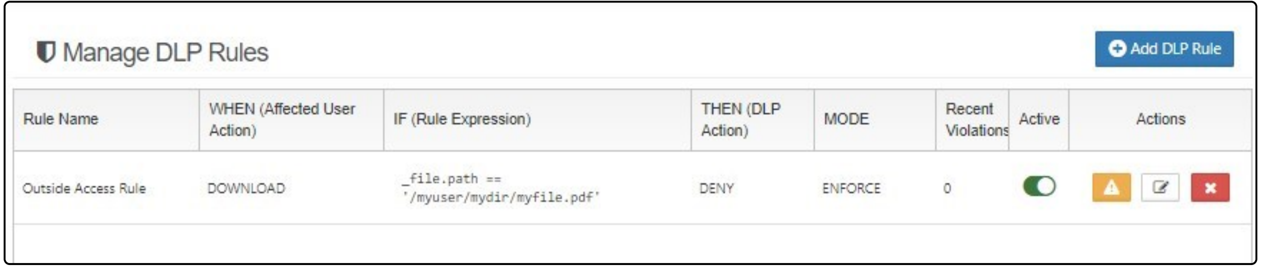
Rule Notification (optional)

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.

- **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.



Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Outside Access Rule	DOWNLOAD	`_file.path == '/myuser/mydir/myfile.pdf'`	DENY	ENFORCE	0	●	⚠ ✎ ✖

Create a rule with the rule expression builder

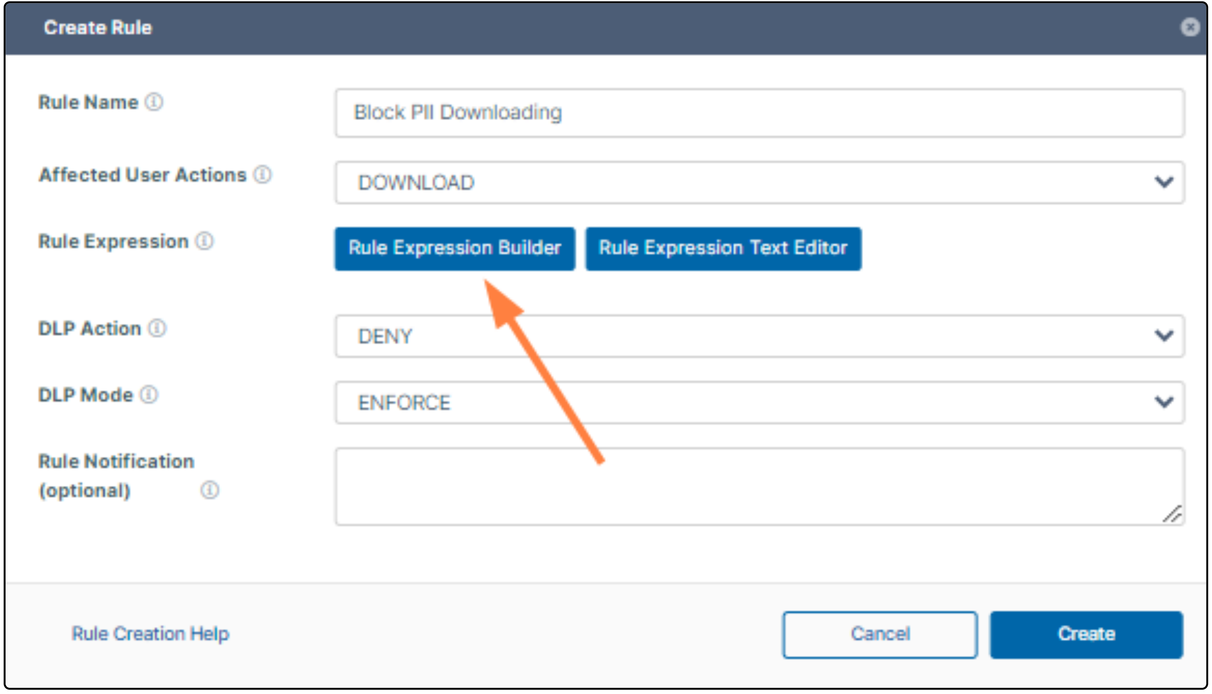
The Rule Expression Builder helps you ensure that your rules have the right parameters and correct formatting. The first example demonstrates how to use the expression builder to create a simple single-condition rule. The second example shows how to create a more complex rule that contains several conditions.

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**.



Create Rule

Rule Name: Block PII Downloading

Affected User Actions: DOWNLOAD

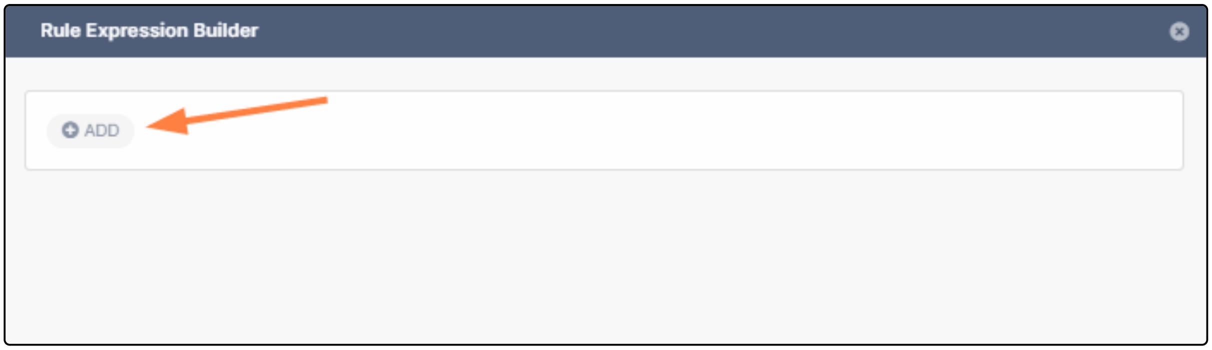
DLP Action: DENY

DLP Mode: ENFORCE

Rule Notification (optional):

The **Rule Expression Builder** opens.

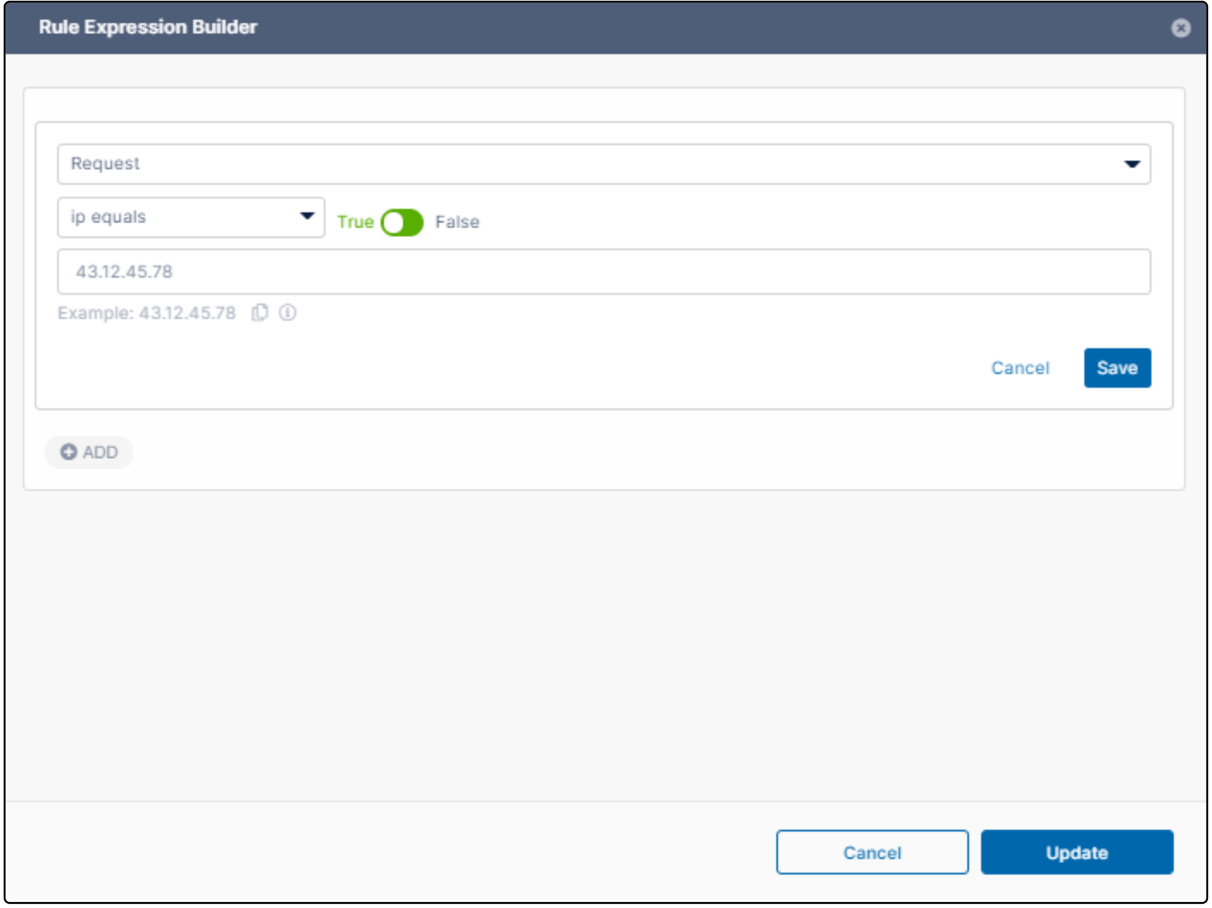
4. Click **ADD**.



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

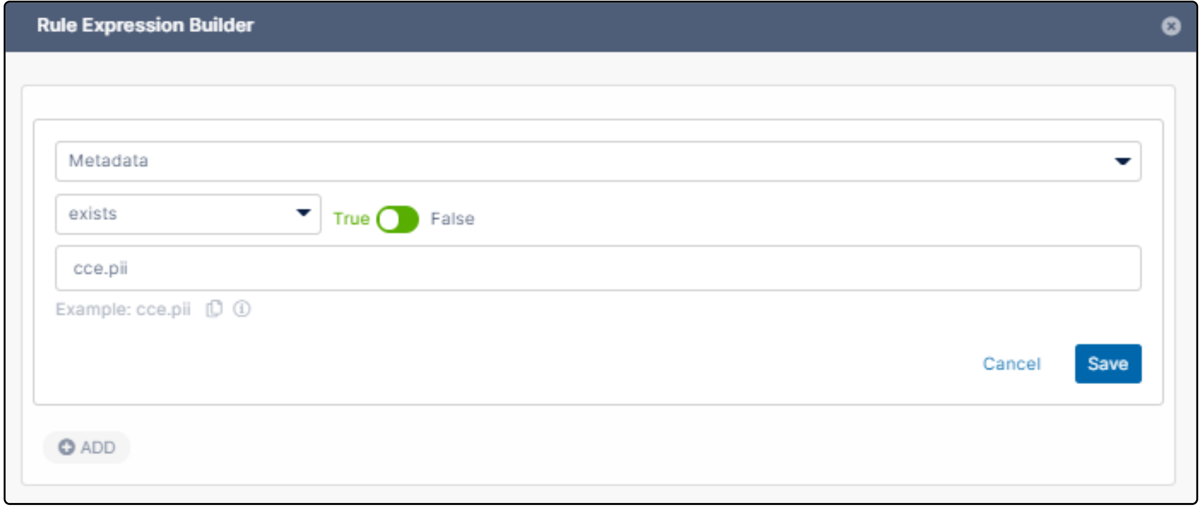
ip equals

True False

43.12.45.78

Example: 43.12.45.78

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

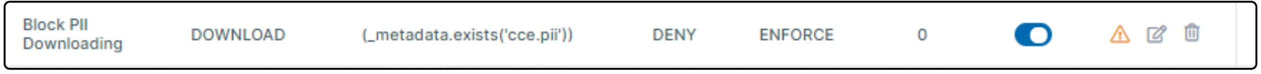
True False

cce.pii

Example: cce.pii

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.



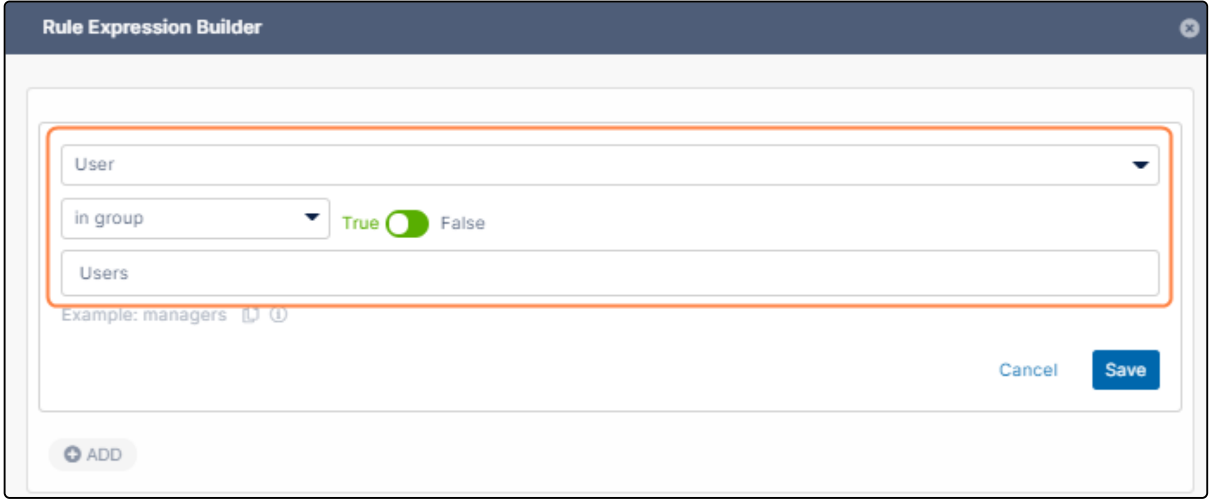
Block PII Downloading	DOWNLOAD	(_metadata.exists('cce.pii'))	DENY	ENFORCE	0

To create a rule with multiple conditions

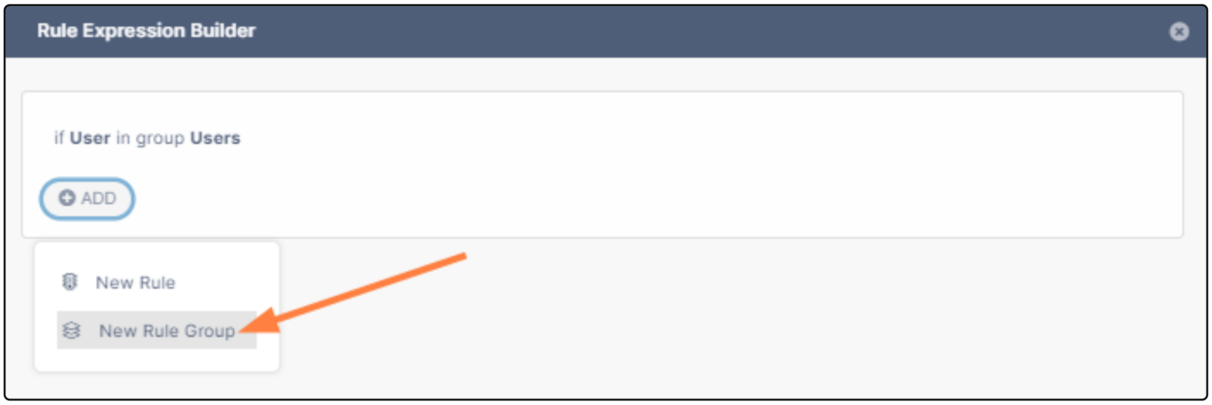
This rule blocks downloading of a file either:

- 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 group **User** group, choose **New Rule**.
6. Fill the fields with **User**, **in group**, and **Users**.



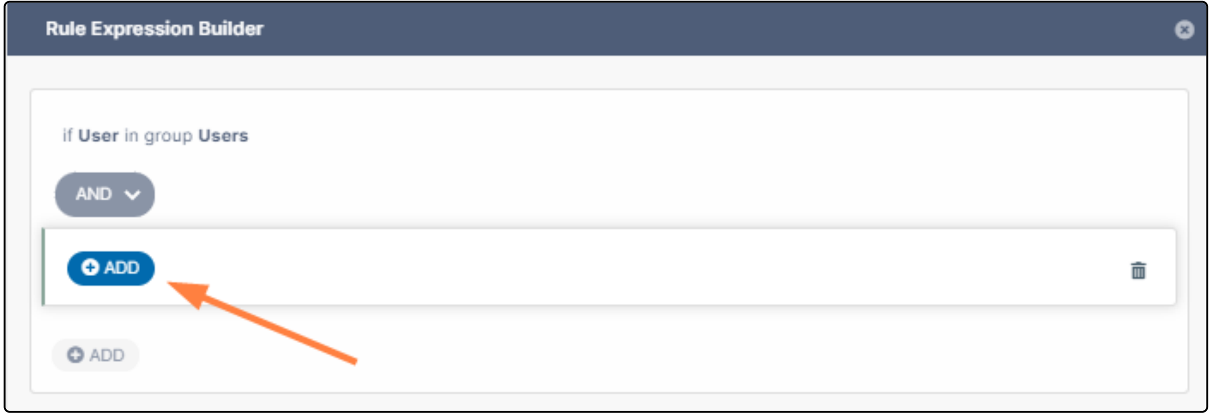
7. Click **Save**.



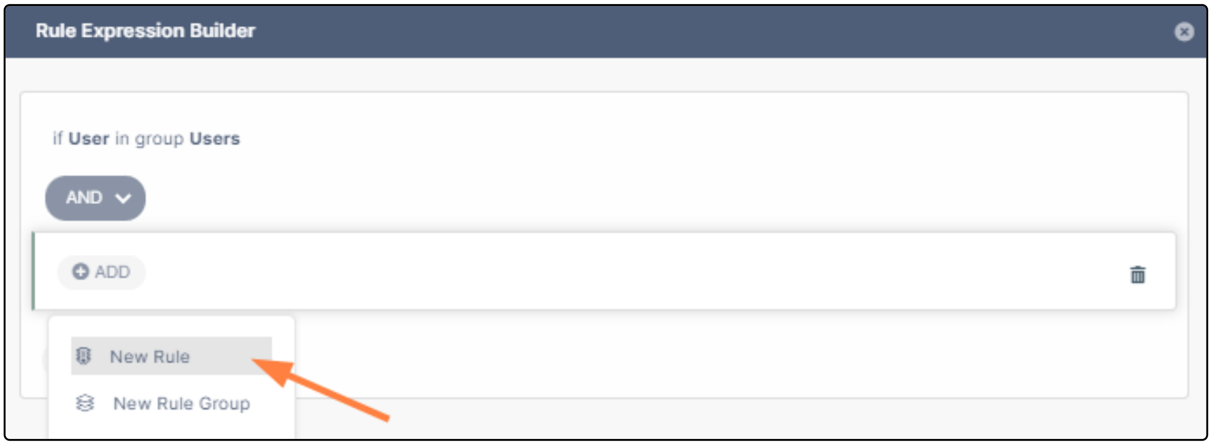
if **User** in group **Users**

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.

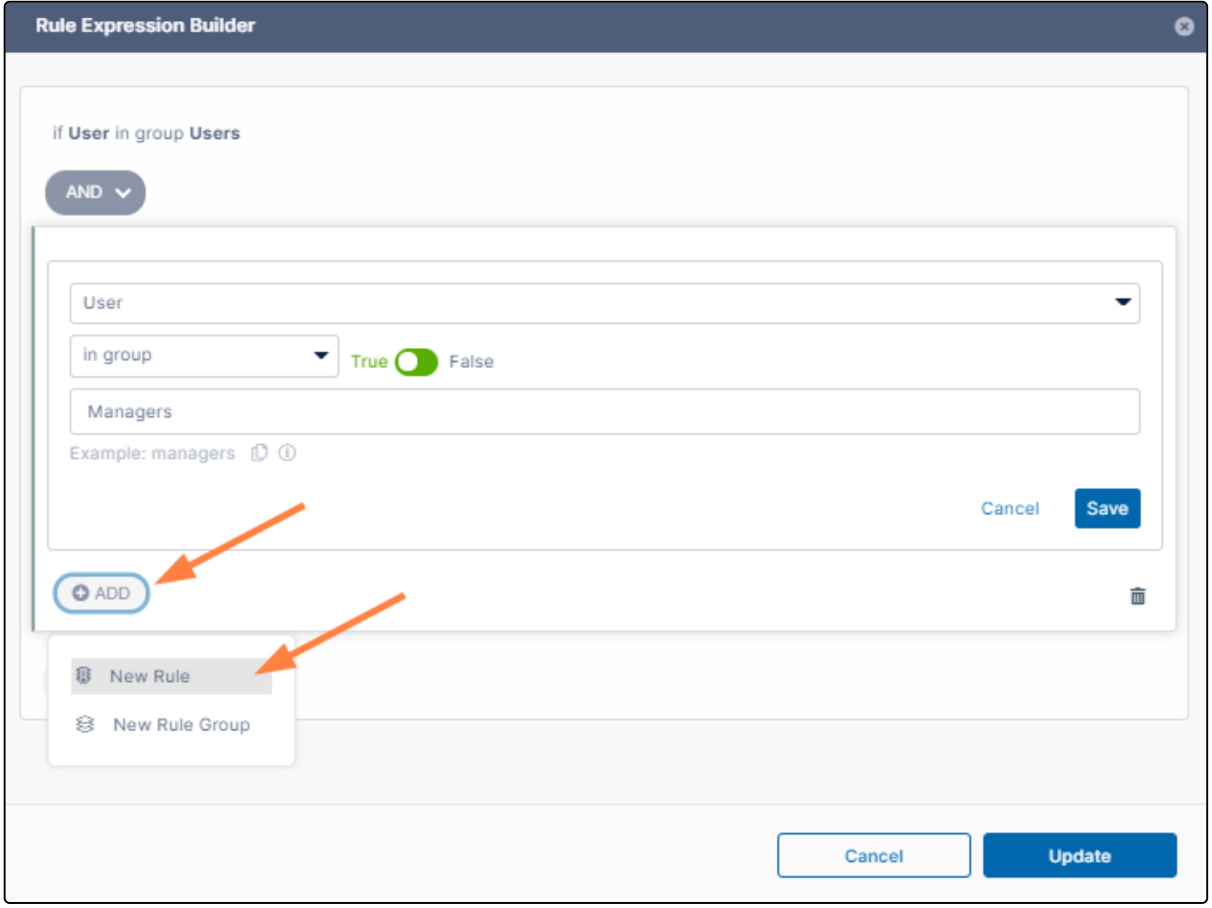


11. Click **New Rule**.



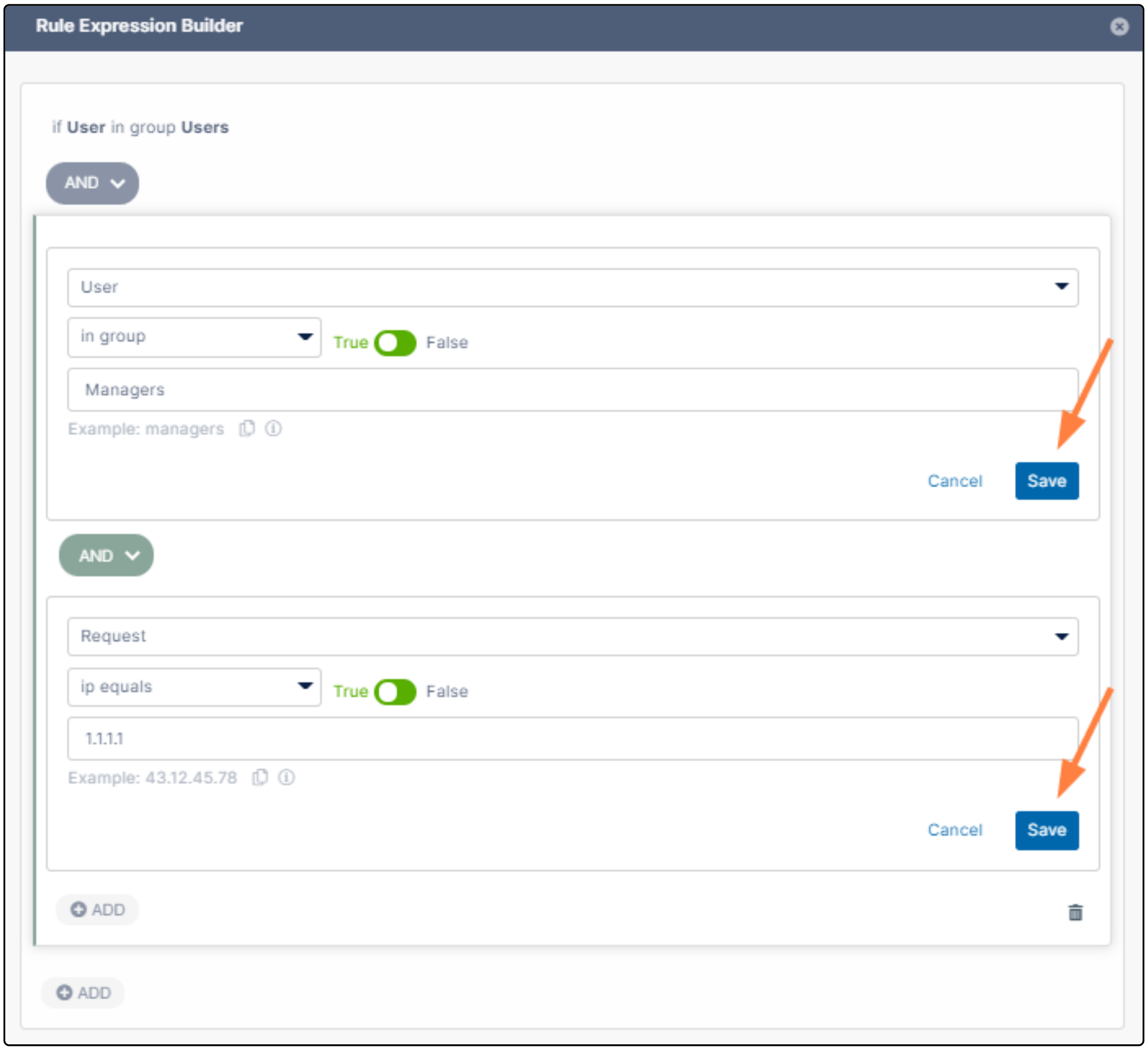
12. Fill in the fields with **User**, **in group**, and **Managers**.

13. Click **ADD** directly under the fields for this condition, and choose **New Rule**.



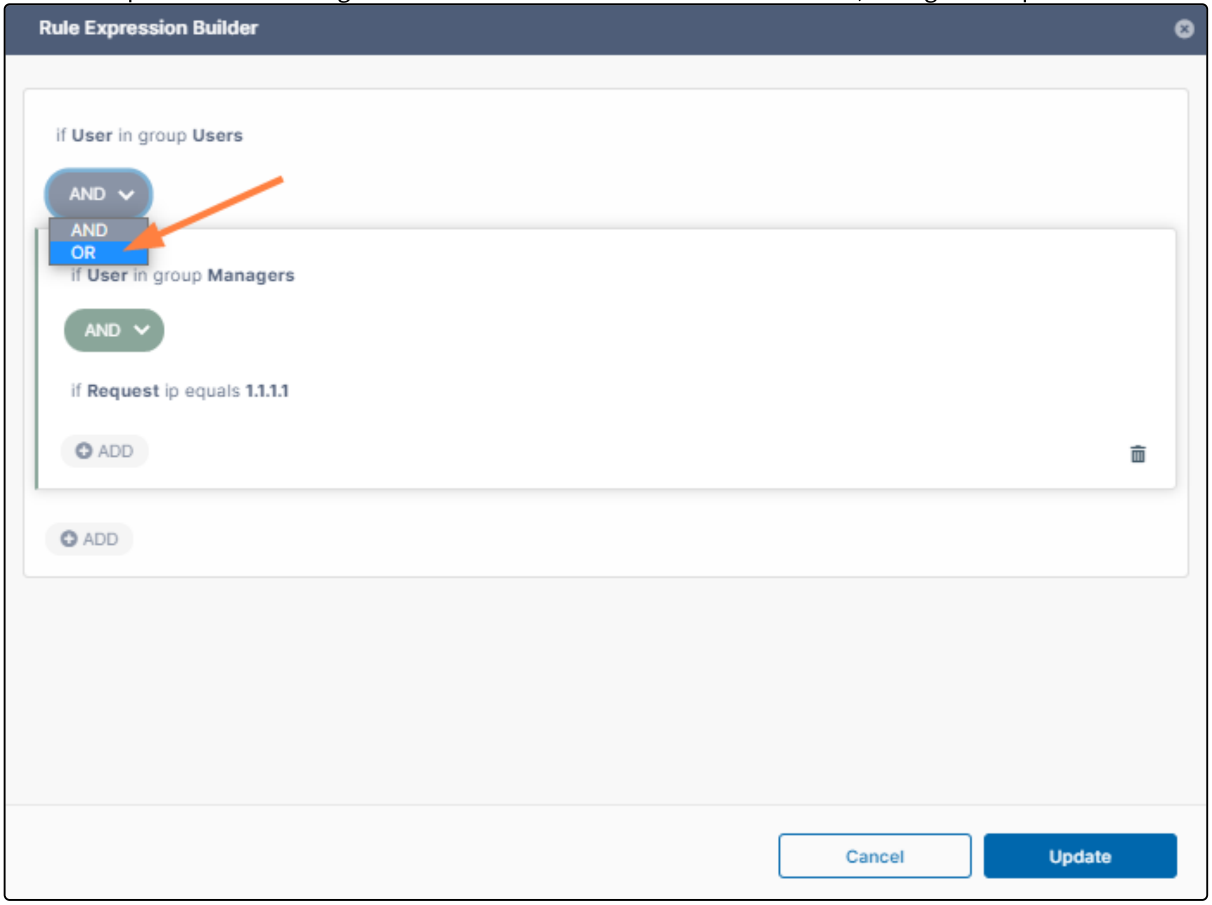
14. Enter the fields **Request**, **ip equals**, and **1.1.1.1**.

15. Click **Save** for each of the conditions.



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**.



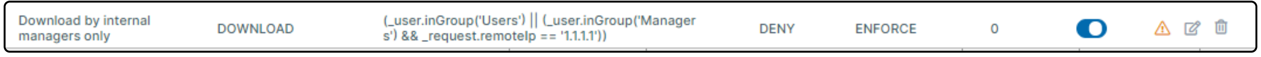
if **User** in group **Users**

if **User** in group **Managers**

if **Request** ip equals **1.1.1.1**

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.

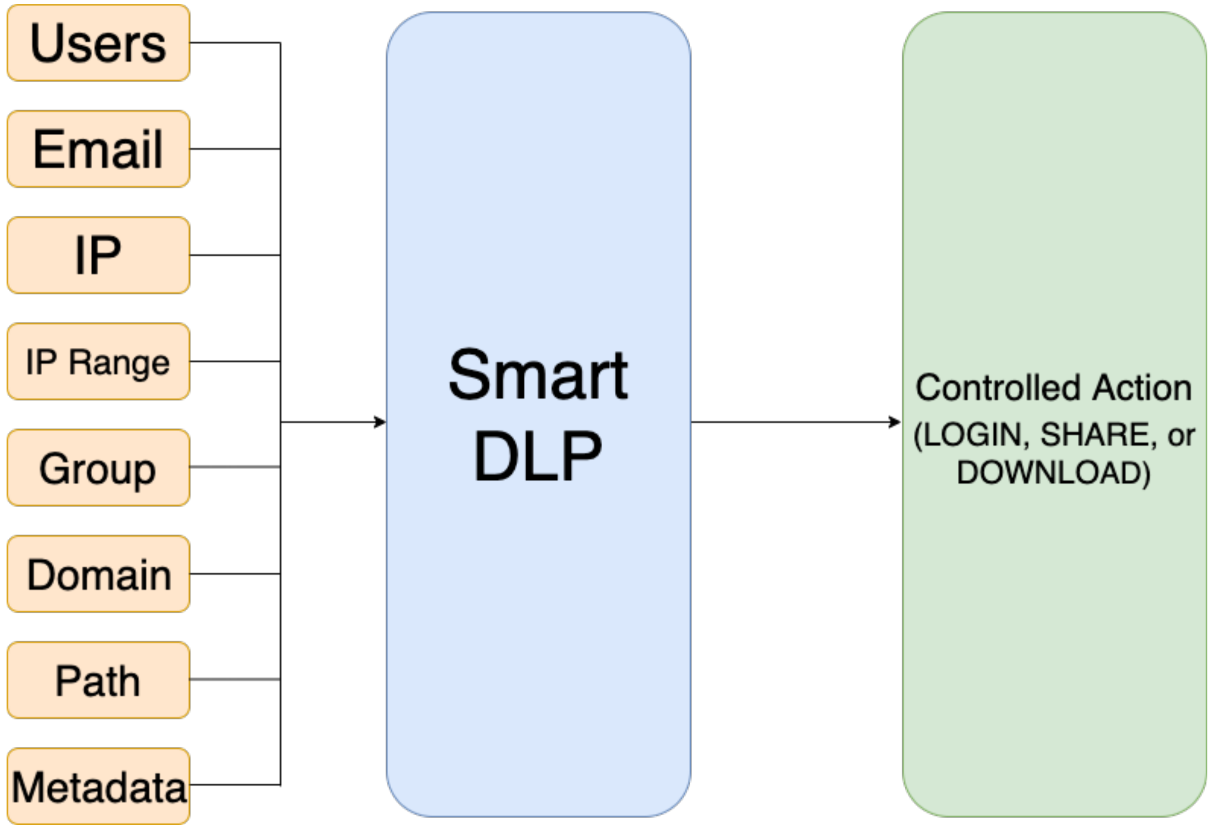


Download by internal managers only	DOWNLOAD	(_user.inGroup('Users') || (_user.inGroup('Managers') && _request.remoteIp == '1.1.1.1'))	DENY	ENFORCE	0	●	⚠ ✎ 🗑

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

Learn more about DLP Rule Expressions

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT

Control download of files	DOWNLOAD	- _file.path
		- _file.pathStartsWith
		- _file.ext
		- _file.pathContains
		- _file.pathMatches
		- _file.fileNameContains
			`_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')`
				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 downloads and shares of files based on metadata	DOWNLOAD
	SHARE
		• _metadata.exists('metadataValue")
		• _metadata.existsAll('metadataValue")
		• _metadata.existsWithValue(metadataValue, value)
		• _metadata.existsWithValueInArray(metadataValue, value)
		• _metadata.existsWithCondition(metadataValue, operator, value)
		Note: 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('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', '>', 6)`
				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 downloading of files based on IP/Device/IP Range/country code	DOWNLOAD
	LOGIN
		• _request.remoteIp
		• _request.agent
		• _request.inIpv4Range(lowIp, highIp)
		• _request.remoteCountryCode
		Note: To use this expression, the **Show Geo IP Chart** setting in the **Settings > Admin** screen must be set to **TRUE**.
		• _request.inIpV4CidrRange(cidrRange)
			`_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')`
				DENY	Users from the given IP, agent, IP range, country code, or CIDR ip range will not be permitted to login or download.

	LOGIN	• _request.isAdminLogin	_request.isAdminLogin	DENY	If the

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT

Control login/access, downloading and sharing of files based on user attributes	DOWNLOAD
	LOGIN
	SHARE
		• _user.username
		• _user.email
		• _user.userType
		• !_user.inGroup
		• _user.isMasterAdmin
			`_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`
				ALLOW	Users with the given username, email address, user type, any user **not** in the group 'managers', and the master Admin will be permitted to login, as well as downloading and sharing files.

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT

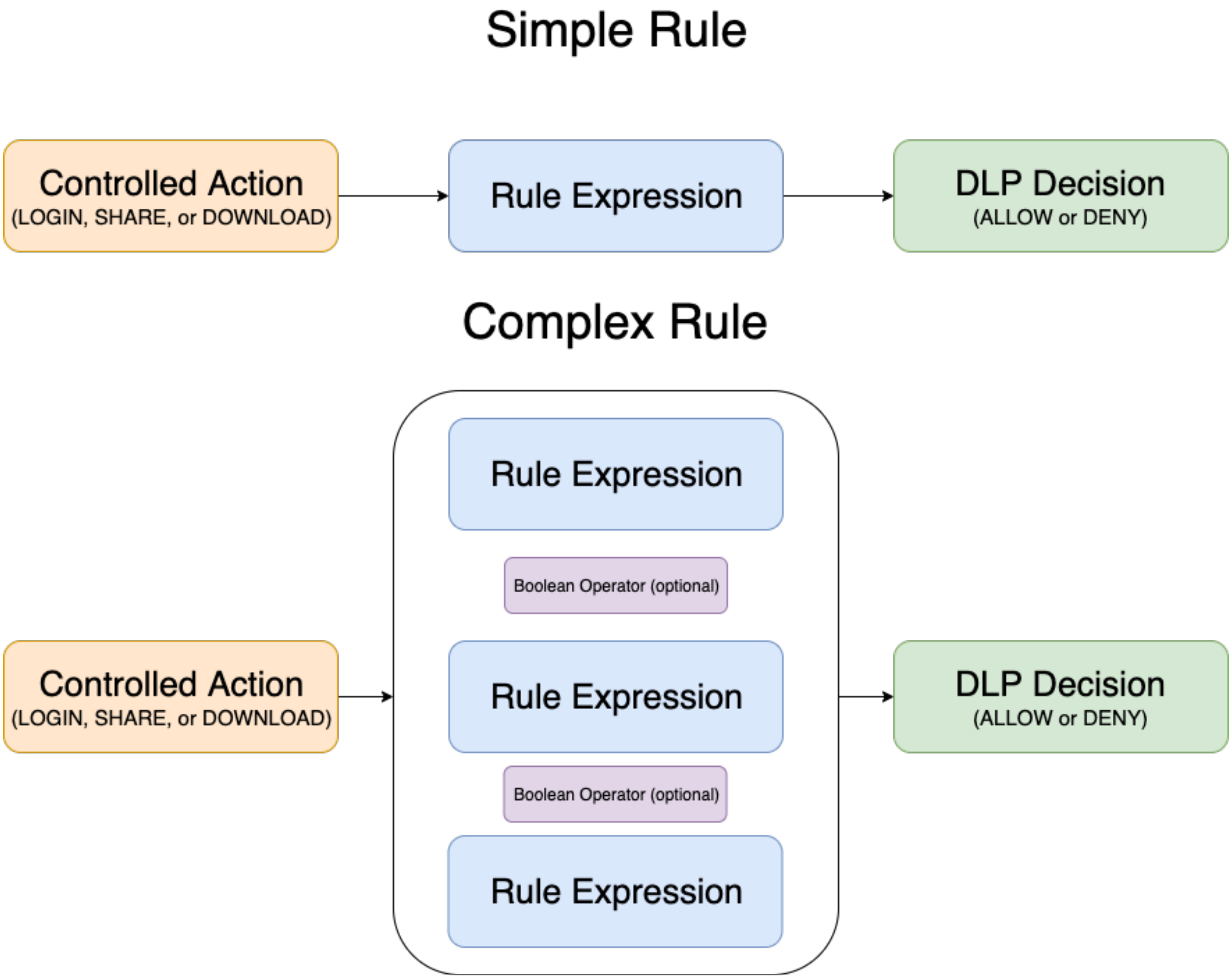
Control file sharing	DOWNLOAD
	SHARE
		• _share.path
		• _share.public
		• _share.onlyAllowedEmails
		• _share.allowedUsers
		• _share.allowedGroups
		• _share.hasUsersFromDomain(domain)
		• _share.onlyUsersFromDomain(domain)
		• _share.pathStartsWith(start)
		• _share.pathContains(text)
		• _share.pathMatches(pattern)
		Note: In any of the expressions including **share.path**, specify the original path of the shared file (for example /user1/textfile1.txt) , not the path in the Shared with Me folder (for example, /SHARED/user1/textfile1.txt)
		Note: **share.pathMatches(pattern)** supports the wildcards:
		`*` - any sequence of characters
		`#` - a single character
			`Rule Expression:`
			`_share.public`
			`OR`
			`_share.onlyAllowedEmails`
			`OR`
			`_share.allowedUsers`
			`OR`
			`_share.allowedGroups`
			`OR`
			`_share.hasUsersFromDomain('gmail.com')`
			`OR`
			`_share.onlyUsersFromDomain('mycompany.com')`
			`OR`
			`_share.pathStartsWith('/myuser/mydir')`
			`OR`
			`_share.pathContains('sometext')`
			`OR`
			`_share.pathMatches('*sometext*')`
				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	DOWNLOAD
	LOGIN
		- !_user.inGroup
		- _metadata.existsWithValue
		- _request.remoteIp
		- _request.isAdminLogin
		- !_request.inIpV4CidrRange
			Rule Expression:
			`!_user.inGroup('superadmin') and _metadata.existsWithValue('PII.Confidentiality Level', 'HIGH')`
			OR
			`_user.inGroup('external') or _request.remoteIp in ['45.45.45.1', '45.45.45.2', '45.45.45.7']`
			OR
			`_request.isAdminLogin && ! _request.inIpV4CidrRange('10.2.0.0/16')`
			DLP Action:
			ALLOW/DENY
				DENY	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'
					OR
					Users logging into the admin portal in the

Objective	Affected User Action	Rule Expressions	Example Rule Expression	DLP Action	RESULT
					given IP range will not be able to download files or log in.
Control sharing based on domain of user doing the sharing	SHARE	- _user.isEmailInDomain(domainsToCheck)	**Rule Expression:** `_user.isEmailInDomain('example.com', 'mail.com')`	ALLOW	Users with one of the specified email domains are permitted to share files.

Rule Expressions



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 '!'.

➡ Learn more about logical operators.

DLP Rule Expressions

Expression	What does the expression do?	Sample returned value	Applicable actions
_request.remoteIp	Returns the IP address that was used to execute the action.	_request.remoteIp == '43.12.45.78'	DOWNLOAD, 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'	DOWNLOAD, 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')	DOWNLOAD, LOGIN
_request.remoteCountryCode	Returns the two-character uppercase ISO country code. Returns "Unknown" if country could not be determined. **Note**: To use this expression, the **Show Geo IP Chart** setting in the **Settings > Admin** screen must be set to **TRUE**.	_request.remoteCountryCode == 'US'	DOWNLOAD, 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')	DOWNLOAD, LOGIN
_user.username	Returns the name of the user trying to execute an action. **Note:** This cannot be used to identify the master Admin since "admin" is not stored as a user. Instead use **user.isMasterAdmin** (see below).	_user.username == 'FileCloudUser'	DOWNLOAD, 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'	DOWNLOAD, LOGIN, SHARE
_user.userType	Returns the type of user that is trying to execute the action. The available types are: 'Full Access', 'Limited Access', 'Guest Access'. **Note**: Prior to FileCloud 22.1, the three user types were **Full**, **Limited**, and **Guest**. Beginning in FileCloud 22.1 **Limited** users are referred to as **External** users; however, the DLP rule expression still requires the use of the value 'Limited Access' to refer to these users.	_user.userType == 'Guest Access'	DOWNLOAD, LOGIN, SHARE
_user.inGroup(groupName)	Checks if a user is part of a given group.	!_user.inGroup('managers')	DOWNLOAD, LOGIN, SHARE
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', 'mail.com')	SHARE
user.isMasterAdmin	Checks if user is the master Admin. **Note:** _user.username =='admin' cannot be used in place of this to identify the master Admin since "admin" is not stored as a user.	user.isMasterAdmin	DOWNLOAD, LOGIN, SHARE
_file.path	Returns the path that was accessed.	_file.path == '/myuser/mydir/myfile.pdf'	DOWNLOAD

Expression	What does the expression do?	Sample returned value	Applicable actions
_file.pathStartsWith(start)	Returns true when the path has been accessed. Starts with the given `start` parameter.	_file.pathStartsWith('/myuser/mydir')	DOWNLOAD
_file.ext	Checks if the file has the extension specified.	_file.ext == 'pdf'	DOWNLOAD
_file.pathContains(path)	Checks if the file path contains the sub-path specified.	_file.pathContains('/myuser/mydir')	DOWNLOAD
_file.pathMatches(path)	Checks if the file path matches the path specified.	_file.pathMatches('/myuser/mydir')	DOWNLOAD
_file.fileNameContains(text)	Checks if the filename includes the given text.	_file.fileNameContains('mrn')	DOWNLOAD
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')	DOWNLOAD, 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.pii')	DOWNLOAD, SHARE
_metadata.existsWithValue(metadataValue, value)	This function is similar to the _metadata.exists(metadataValue) function, but it checks if the metadata attribute (first parameter) exists, and if its value is equal to a given value (second parameter).	_metadata.existsWithValue('content.category', 'confidential')	DOWNLOAD, SHARE

Expression	What does the expression do?	Sample returned value	Applicable actions
_metadata.existsWithValueInArray(metadataValue, value)	This function is similar to the `_metadata.existsWithValue(metadataValue, value) function, but checks whether an array metadata attribute contains the specified value.	_metadata.existsWithValueInArray('content.categories', 'pii')	DOWNLOAD, SHARE
_metadata.existsWithCondition(metadataValue, operator, value)	This function is similar to the _metadata.existsWithValue(metadataValue, value) 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.	_metadata.existsWithCondition('content.Risk Level', '>', 6)	DOWNLOAD, SHARE
Note: In any of the expressions including **share.path**, specify the original path of the shared file (for example /user1/textfile1.txt), not the path in the Shared with Me folder (for example, /SHARED/user1/textfile1.txt)			
_share.path	Returns the path of the share.	_share.path == '/myuser/mydir/myfile.pdf'	SHARE
_share.public	Returns true or false if the share is public or not.	_share.public	SHARE
_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

Expression	What does the expression do?	Sample returned value	Applicable actions
_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' 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 **matches** 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')	SHARE

Expression	What does the expression do?	Sample returned value	Applicable actions
_share.onlyUsersFromDomain(domain)	Similar to the _share.hasUsersFromDomain(domain) function, but checks if the allowed users list has any user with an email domain that **doesn't match** the given domain. In the provided sample, the expression only returns true if all users have their emails in the `mycompany.com` domain. This method only makes sense with ALLOW rules. ⚠ Do not use this expression in an OR condition with another expression; this could cause shares to be denied unintentionally. Instead use _share.onlyAllowedEmails with a wildcard. For example, instead of: (_share.onlyUsersFromDomain('gmail.com') || _share.onlyAllowedEmails('testuser@test.com')) use: _share.onlyAllowedEmails('*@gmail.com','testuser@test.com')	_share.onlyUsersFromDomain('mycompany.com')	SHARE
_share.pathStartsWith(start)	Returns true when the shared path starts with the given `start` parameter.	_share.pathStartsWith('/myuser/mydir')	SHARE
_share.pathContains(text)	Returns true when the shared path contains the given `text` parameter.	_share.pathContains('sometext')	SHARE

Expression	What does the expression do?	Sample returned value	Applicable actions
_share.pathMatches(pattern)	Returns true when the shared path matches the given `pattern` parameter. Wildcards are supported: `*` for any sequence of characters and `#` for a single character.	_share.pathMatches('*some text*')	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	_user.username == 'john' && _user.inGroup('engineers')	User 'john' in group 'engineers' will not be permitted to download any files.
DOWNLOAD	ALLOW	_user.inGroup('accounting') || _request.remoteIp == '69.89.31.226.'	Users in group 'accounting' **or** users from the listed IP will be permitted to download files, but **no other users** will be permitted.
SHARE	DENY	!_user.inGroup('designers')	Users who are **not** 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
- Detect confidential documents with PII and allow internal shares only
- Detect documents with US Social Security Number and allow sharing only with specific domains
- Limit Web Login to a specific group of users

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.

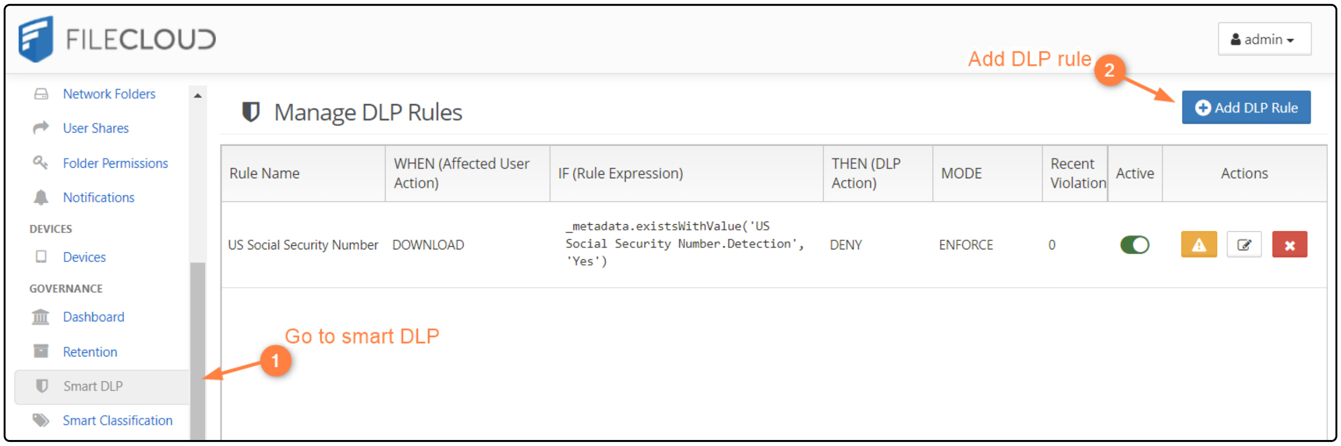
In the example, a FileCloud group is named after the partner company, "Company XYZ", and contains users from this company.

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.remoteIp in ['IP1', 'IP2', 'IP3'])**
- In the image below, **(_user.inGroup('Internal'))** allows downloads from users in group "Internal" initiated from any IP.

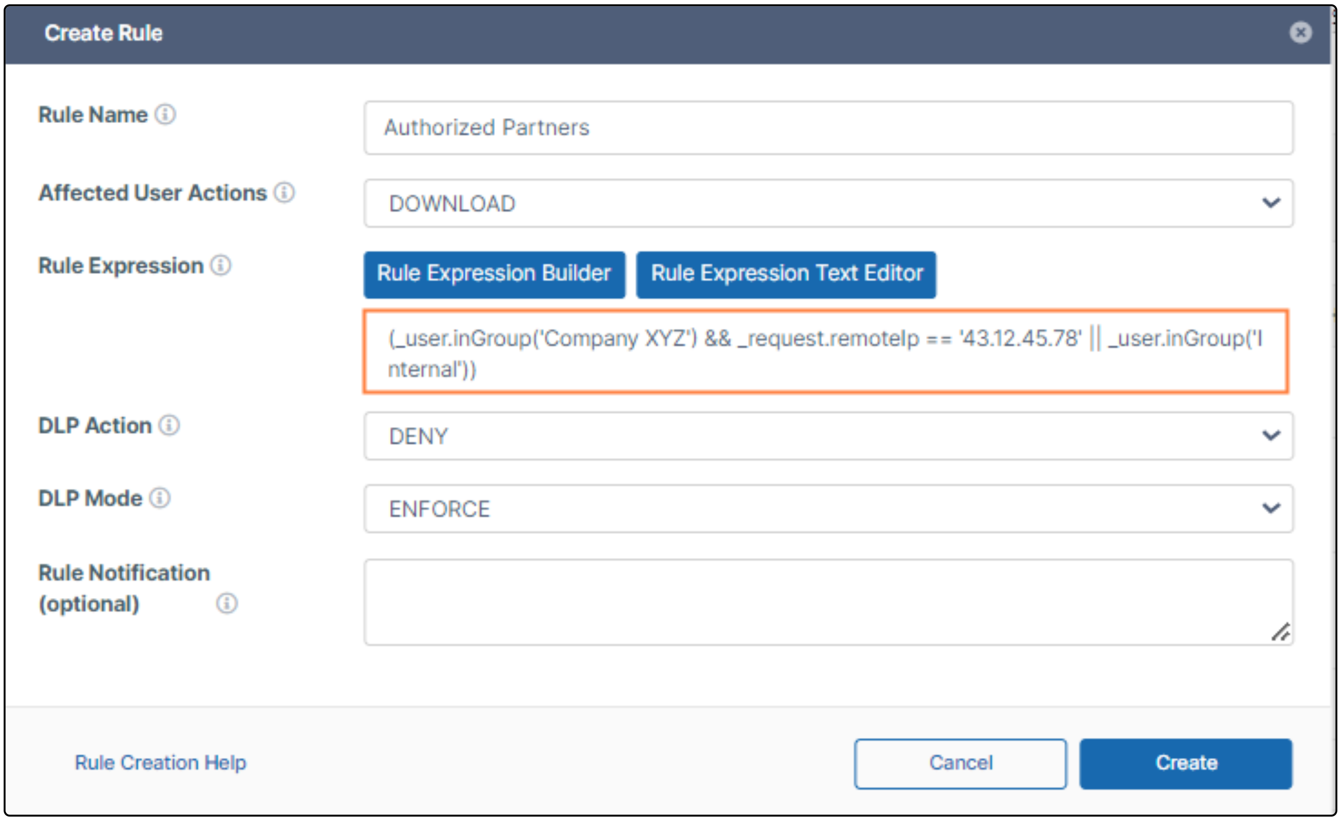


Add DLP rule

Manage DLP Rules

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violation	Active	Actions
US Social Security Number	DOWNLOAD	_metadata.existsWithValue('US Social Security Number.Detection', 'Yes')	DENY	ENFORCE	0	●	⚠ ✎ ✖

Go to smart DLP



Create Rule

Rule Name: Authorized Partners

Affected User Actions: DOWNLOAD

Rule Expression:

```
(_user.inGroup('Company XYZ') && _request.remoteIp == '43.12.45.78' || _user.inGroup('Internal'))
```

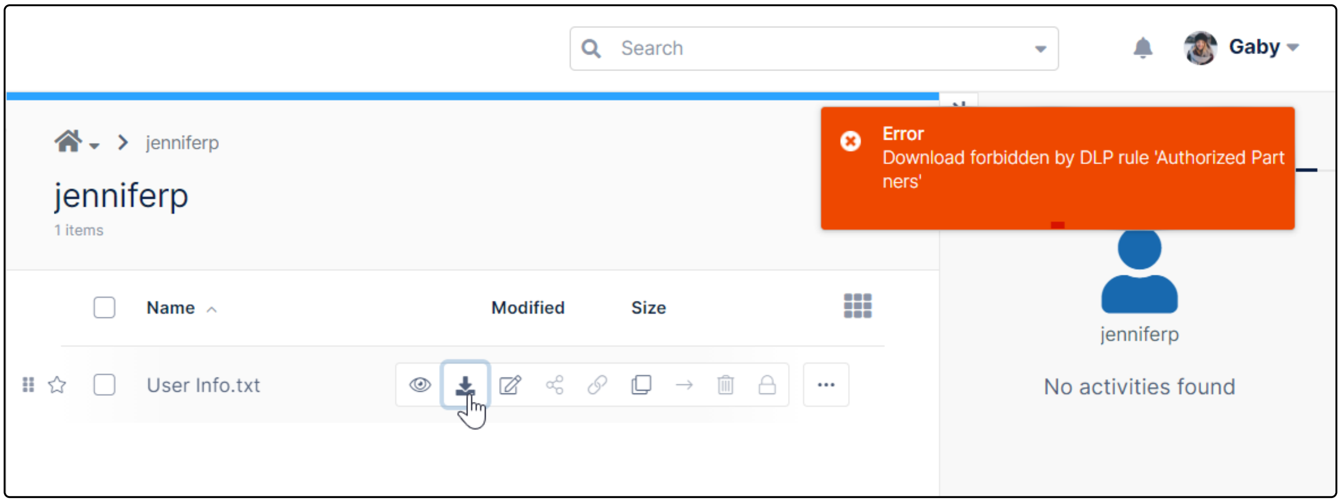
DLP Action: DENY

DLP Mode: ENFORCE

Rule Notification (optional):

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.



Error
Download forbidden by DLP rule 'Authorized Partners'

Detect confidential documents with PII and allow internal shares only

Overview:

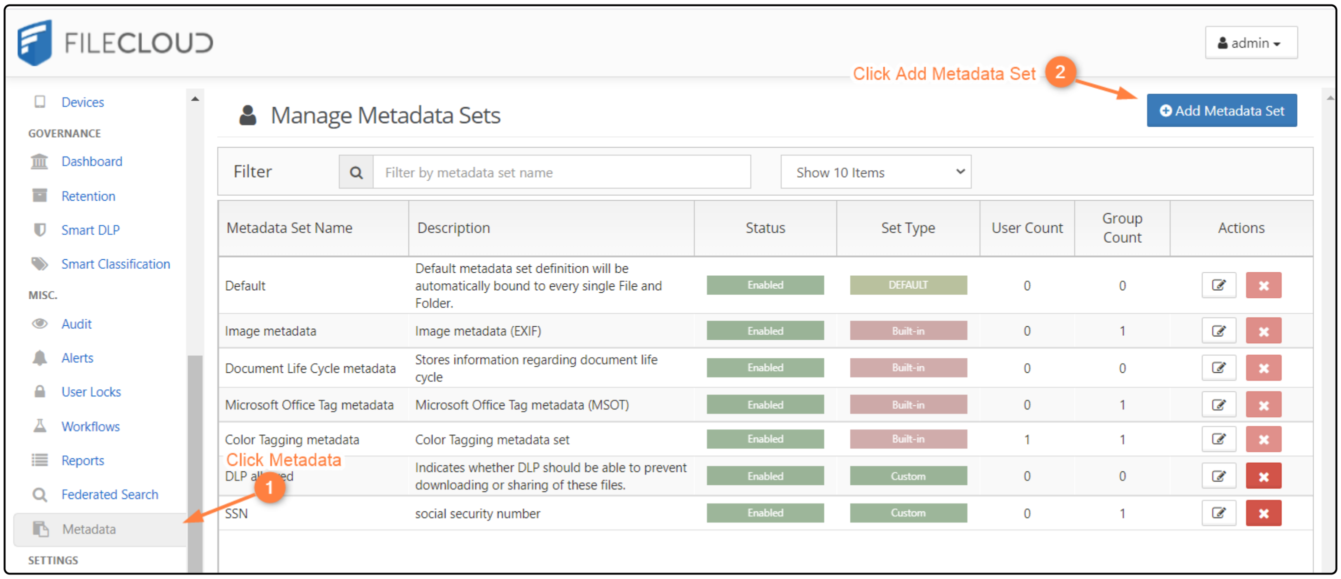
The purpose of this example is to:

- Create a classification rule that detects confidential documents using a group of personally identifiable information (PII) patterns.
- Tag the documents with attributes that specify if they are marked confidential.
- Create a DLP rule that allows only internal sharing of documents tagged as confidential, but allows external sharing of documents not tagged as confidential.

Configuration Steps:

1. Create Metadata Set

- Log in to the FileCloud Admin portal, and in the navigation panel, click **Metadata**, then click **Add Metadata Set**.



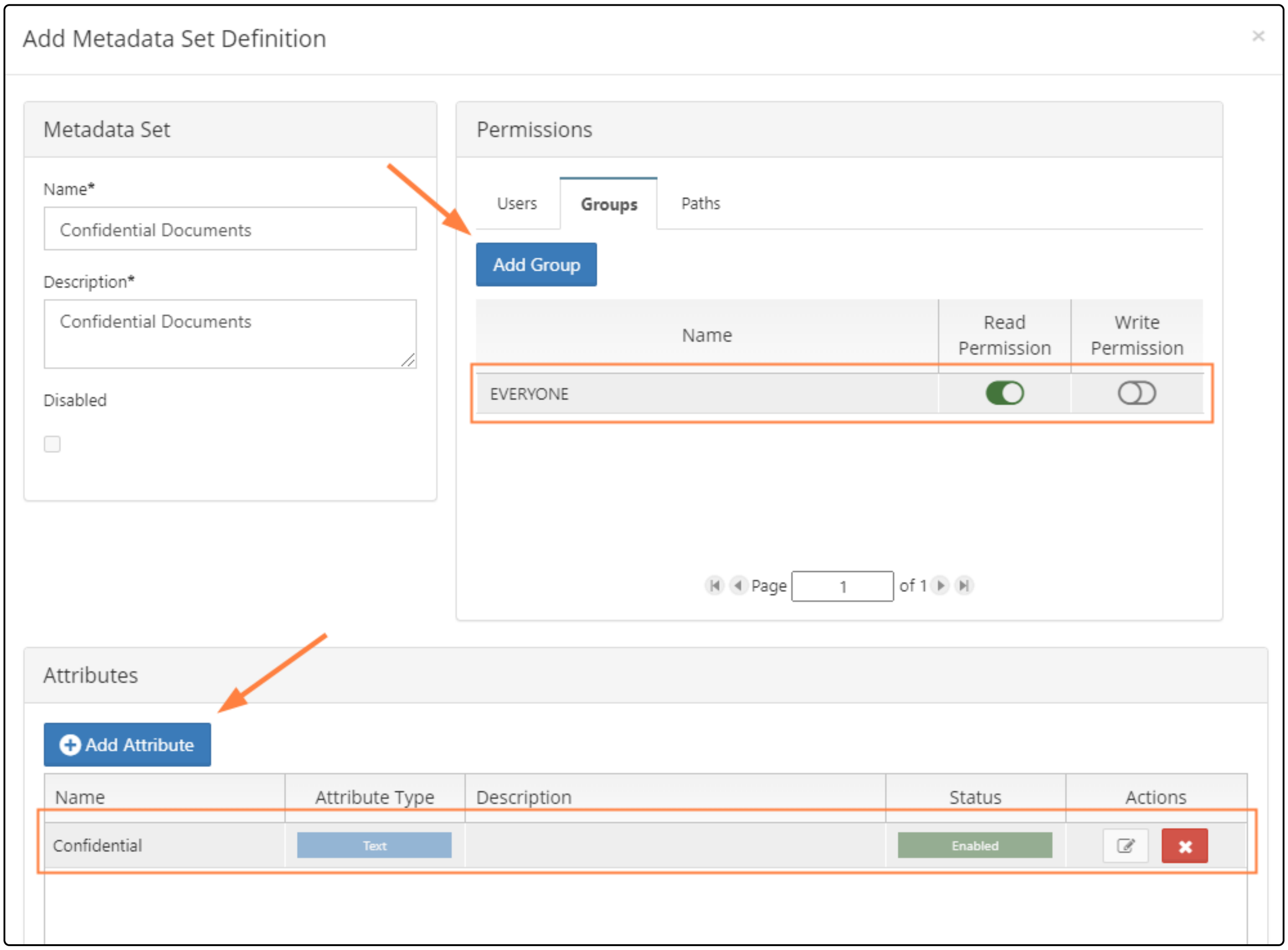
Click Add Metadata Set 2

Click Metadata 1

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	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	✎ ✖
SSN	social security number	Enabled	Custom	0	1	✎ ✖

- Create a metadata set named **Confidential Documents** with the attribute **Confidential** of type text.
- Choose the Users/Groups that can see this metadata and provide them with read permission.



Name*: Confidential Documents

Description*: Confidential Documents

Disabled □

Name	Read Permission	Write Permission
EVERYONE	● on	○ off

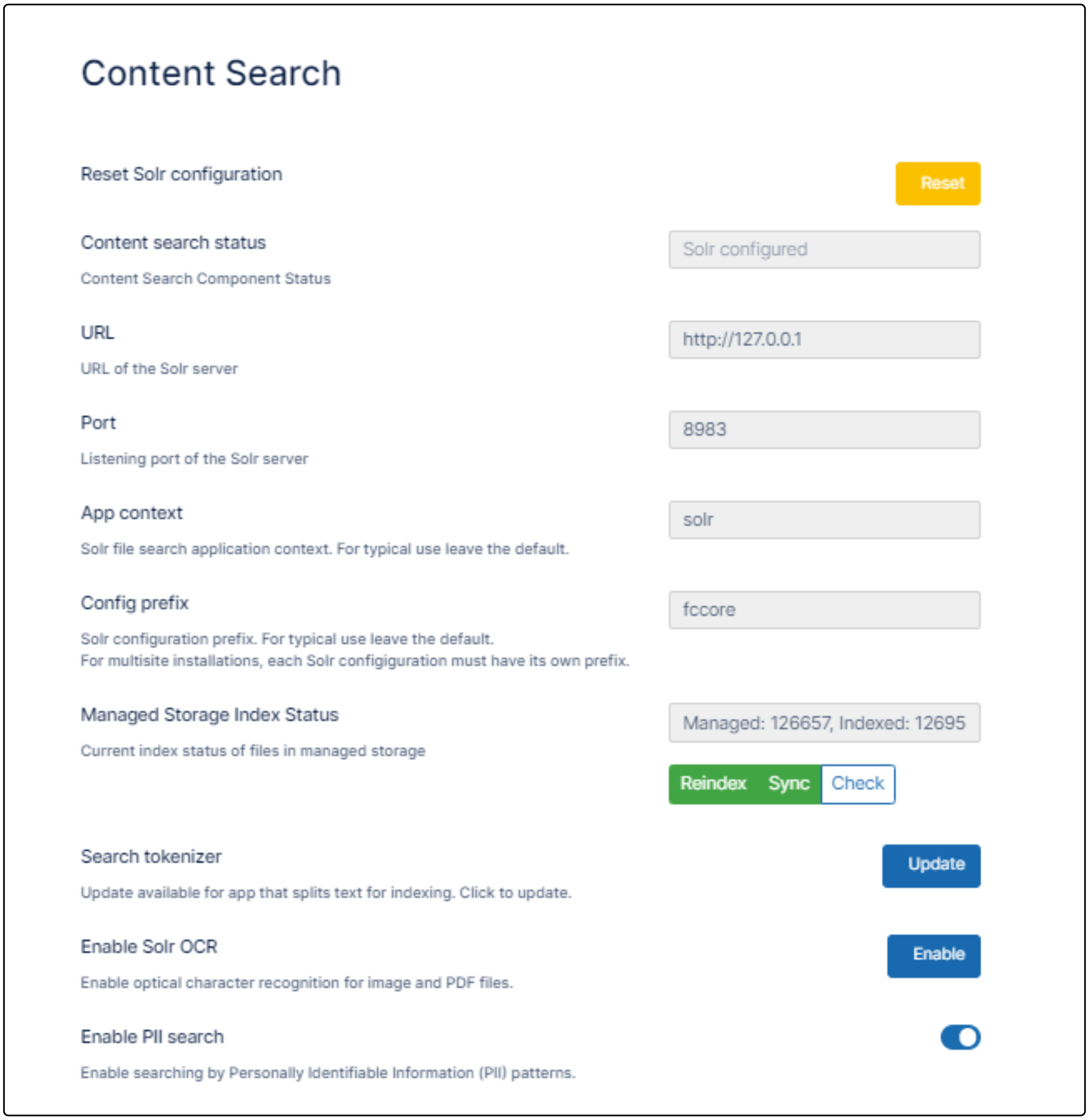
Page 1 of 1

Name	Attribute Type	Description	Status	Actions
Confidential	Text		Enabled	

2. Create the PII Regex Patterns Group

- 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.

- Check **Enable PII Search**.



Content Search

Reset Solr configuration

Content search status

Content Search Component Status

Solr configured

URL

URL of the Solr server

http://127.0.0.1

Port

Listening port of the Solr server

8983

App context

Solr file search application context. For typical use leave the default.

solr

Config prefix

Solr configuration prefix. For typical use leave the default.
For multisite installations, each Solr configiguration must have its own prefix.

fccore

Managed Storage Index Status

Current index status of files in managed storage

Managed: 126657, Indexed: 12695

Search tokenizer

Update available for app that splits text for indexing. Click to update.

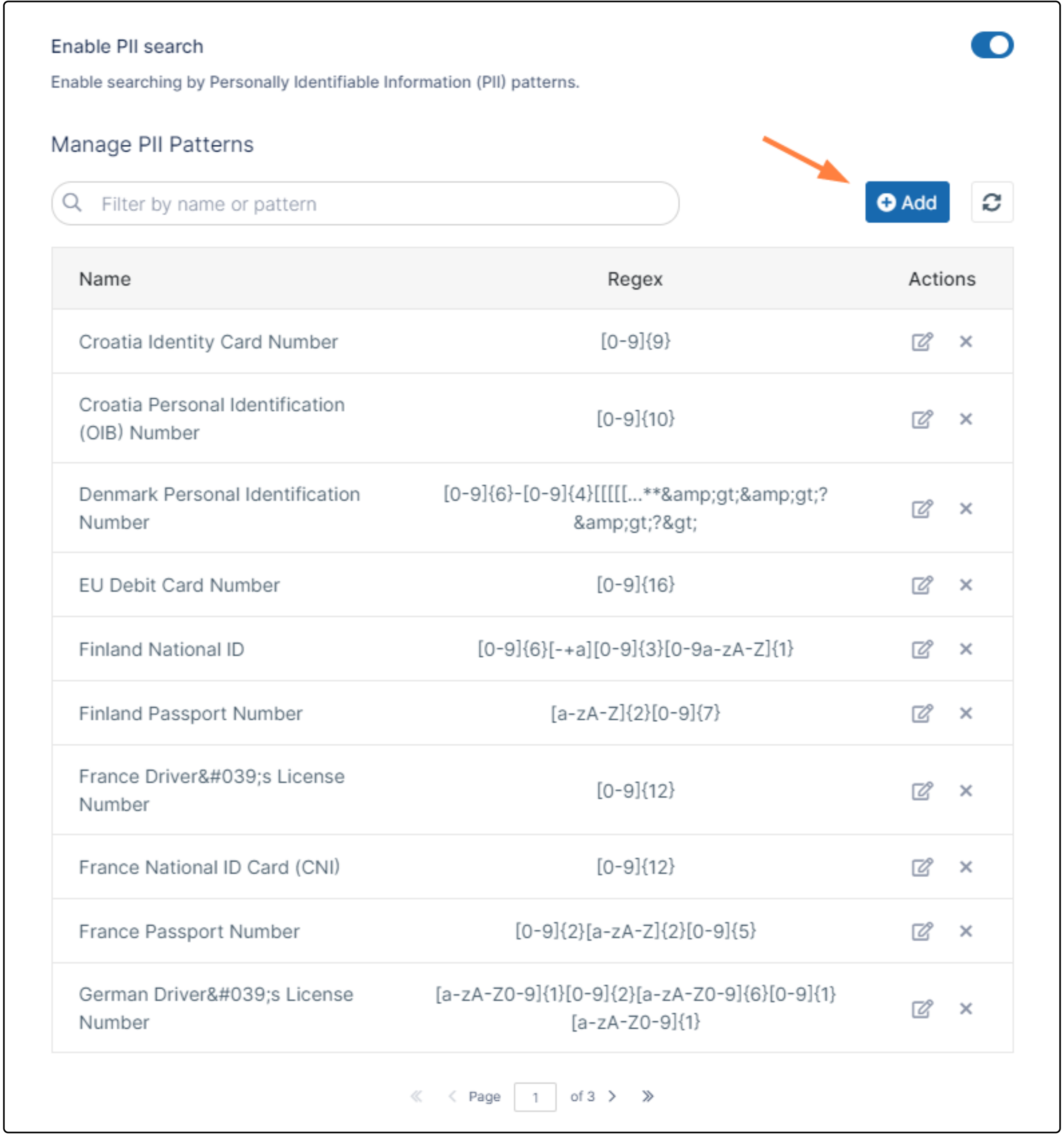
Enable Solr OCR

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 patten for your confidential Information.



Enable PII search

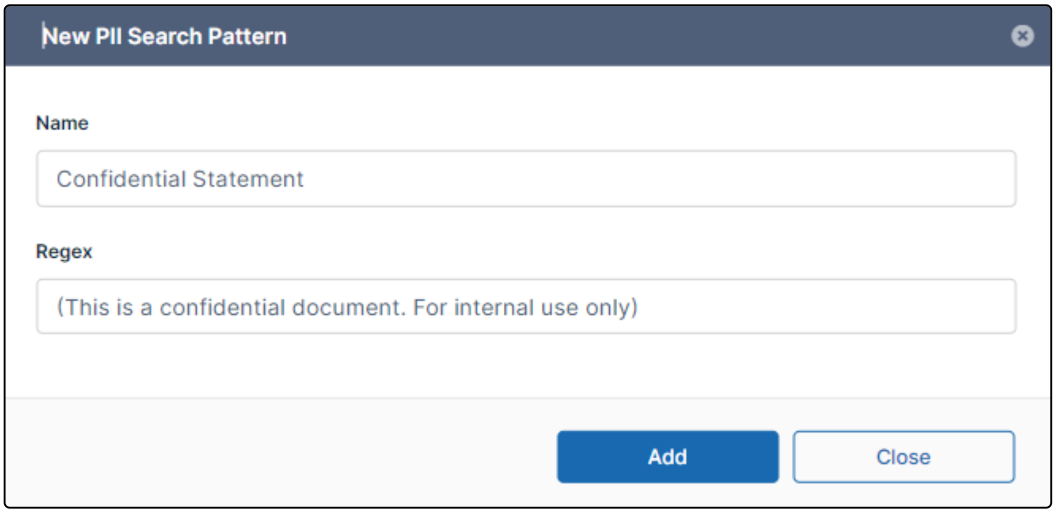
Enable searching by Personally Identifiable Information (PII) patterns.

Manage PII Patterns

Name	Regex	Actions
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}[[[[[...**&gt;&gt;?&gt;?&gt;	✎ ×
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&#039;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&#039;s License Number	[a-zA-Z0-9]{1}[0-9]{2}[a-zA-Z0-9]{6}[0-9]{1}[a-zA-Z0-9]{1}	✎ ×

Enter the new PII search pattern, and set **Regex** to the confidential statement to detect inside your documents, for example, "(This is a confidential document, For internal use only)". Note that statement should be inside (). If you have multiple statements to detect in your document you can use (statement1) | (statement2) | (statement3) . In this example, you are also adding the pre-defined patterns with personally identifiable information listed below.

- Confidential Statement Pattern:



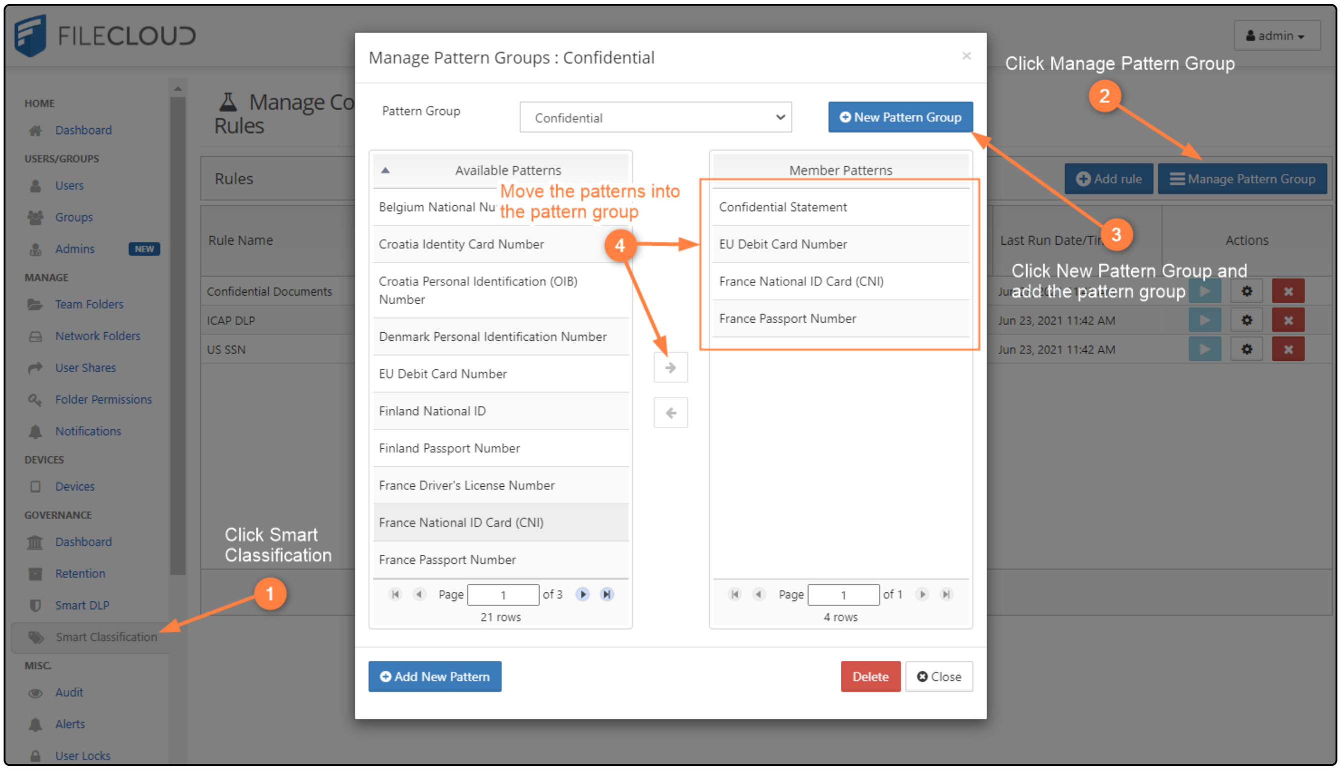
New PII Search Pattern

Name: Confidential Statement

Regex: (This is a confidential document. For internal use only)

Also select:
European Debit Card number Pattern
France National ID Card (CNI)
France Passport Number

- Add the different patterns into a pattern group:



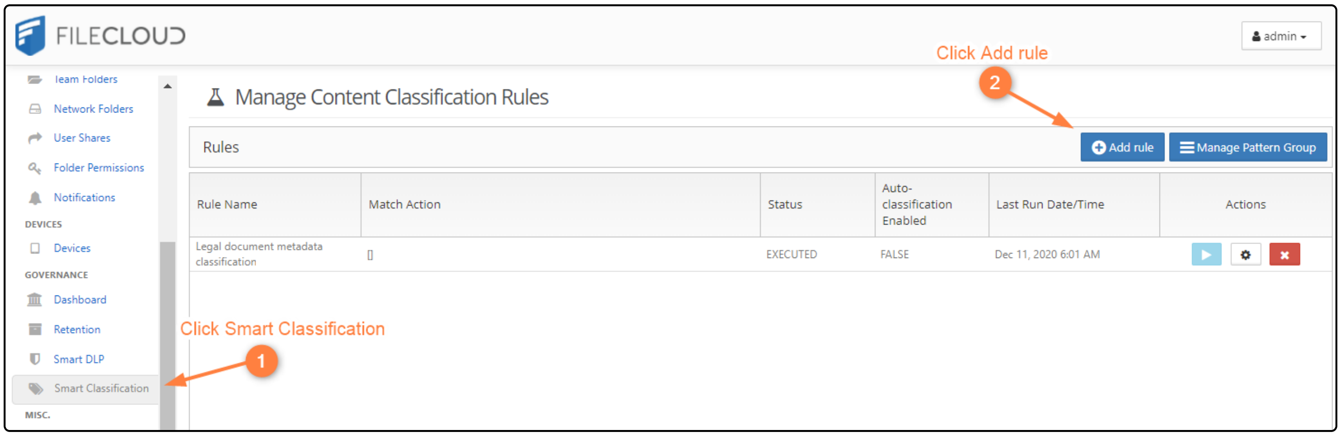
Manage Pattern Groups : Confidential

Pattern Group: Confidential

Available Patterns	Member Patterns
Belgium National Nu	Confidential Statement
Croatia Identity Card Number	EU Debit Card Number
Croatia Personal Identification (OIB) Number	France National ID Card (CNI)
Denmark Personal Identification Number	France Passport 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	Page 1 of 1, 4 rows

3. Create the Smart Classification Rule

- Log in to the FileCloud Admin portal, and in the navigation panel, click **Smart Classification.**
- Add a new classification rule



Click Add rule

Click Smart Classification

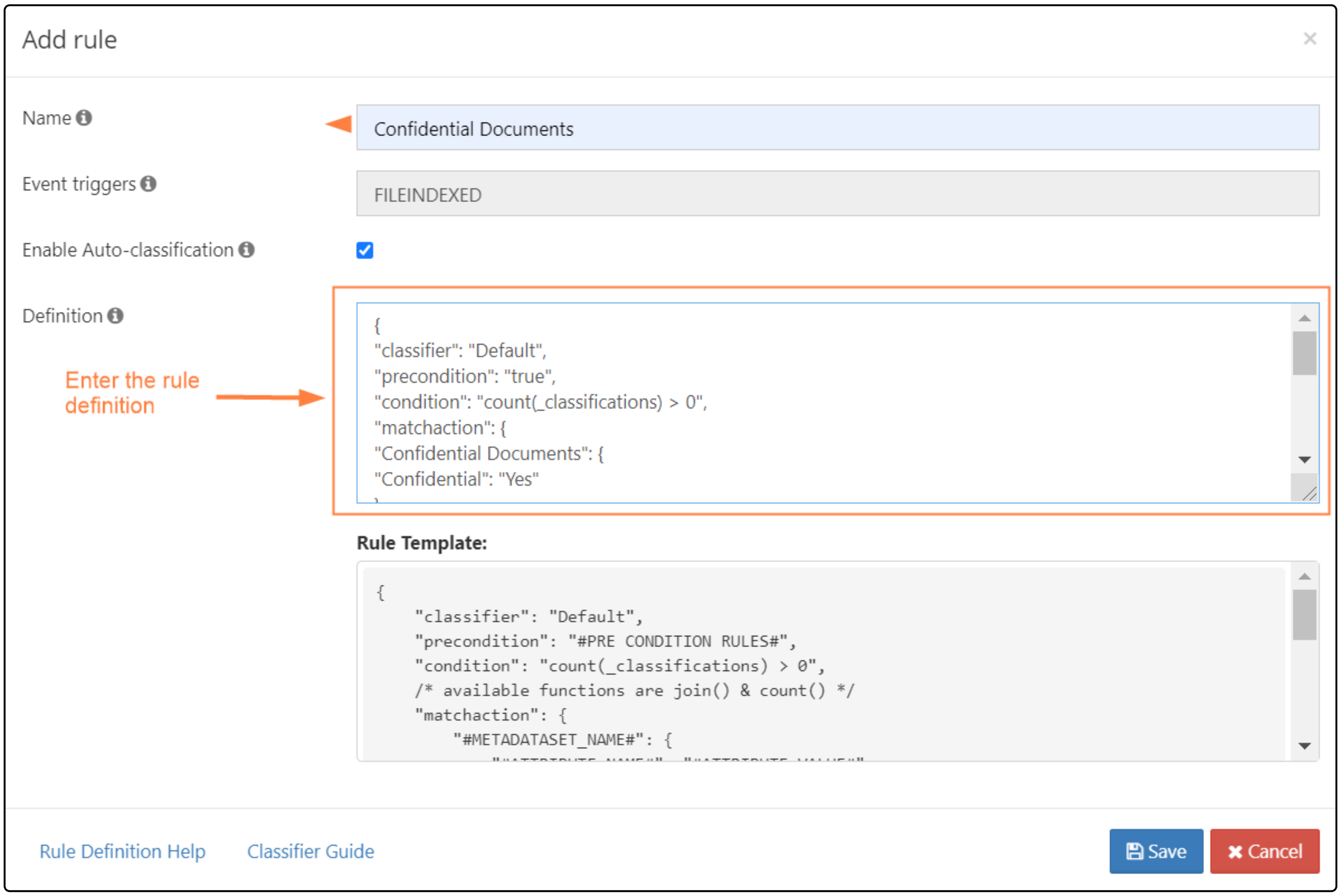
Manage Content Classification Rules

Rules

Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
Legal document metadata classification	[]	EXECUTED	FALSE	Dec 11, 2020 6:01 AM	▶ ⚙ ✖

- 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": {
  "Confidential Documents": {
    "Confidential": "Yes"
}
},
"defaultaction": {
  "Confidential Documents": {
    "Confidential": "No"
}
},
"parameters": {
  "SEARCH_PATTERN_GROUPS": [
    "Confidential Info"
]
}
}
```



Name: Confidential Documents

Event triggers: FILEINDEXED

Enable Auto-classification: ☑

Definition:

Enter the rule definition

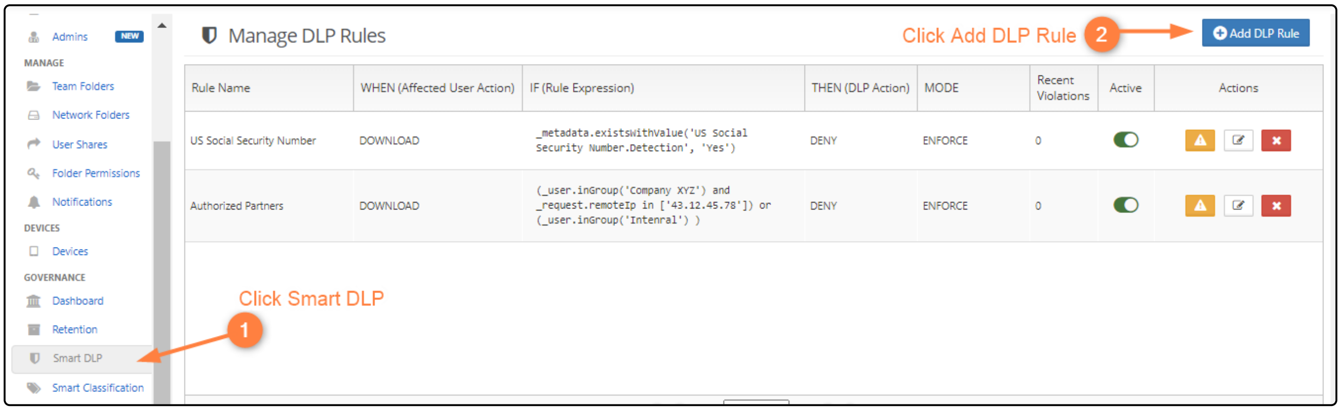
```
{
"classifier": "Default",
"precondition": "true",
"condition": "count(_classifications) > 0",
"matchaction": {
"Confidential Documents": {
"Confidential": "Yes"
```

Rule Template:

```
{
    "classifier": "Default",
    "precondition": "#PRE CONDITION RULES#",
    "condition": "count(_classifications) > 0",
    /* available functions are join() & count() */
    "matchaction": {
        "#METADATASET_NAME#": {
            "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#"
```

4. Create the 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 are confidential, the rule checks for metadata attribute "Confidential" = "Yes" and allows sharing with only domain "codelathe.com".
- For documents that are non-confidential, the rule checks for metadata attribute "Confidential" = "No" and allows sharing with all domains.

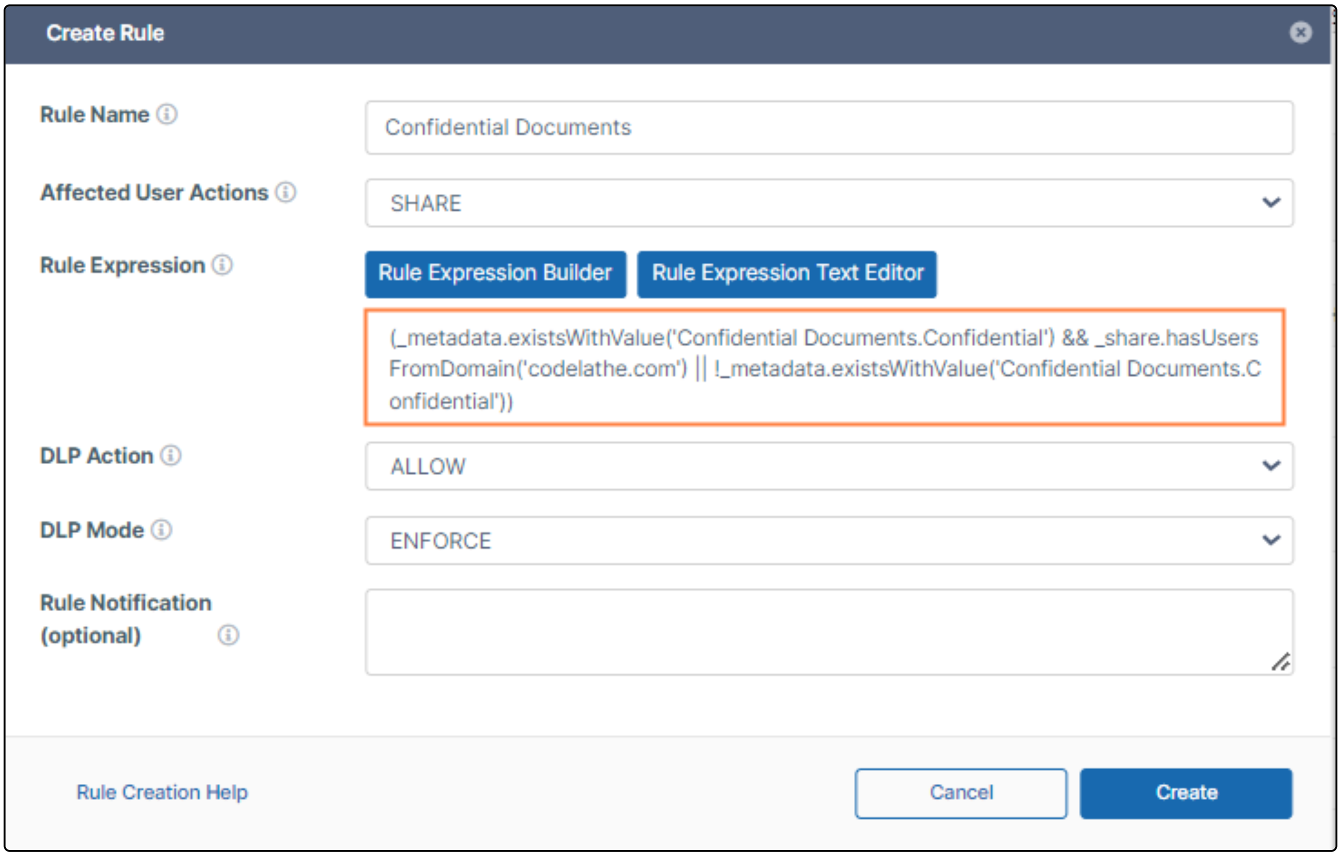


Manage DLP Rules

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
US Social Security Number	DOWNLOAD	`_metadata.existsWithValue('US Social Security Number.Detection', 'Yes')`	DENY	ENFORCE	0		
Authorized Partners	DOWNLOAD	`(_user.inGroup('Company XYZ') and _request.remoteIp in ['43.12.45.78']) or (_user.inGroup('Intenral') )`	DENY	ENFORCE	0		

Click Add DLP Rule 2

Click Smart DLP 1



Create Rule

Rule Name: Confidential Documents

Affected User Actions: SHARE

Rule Expression:

```
(_metadata.existsWithValue('Confidential Documents.Confidential') && _share.hasUsersFromDomain('codelathe.com') || !_metadata.existsWithValue('Confidential Documents.Confidential'))
```

DLP Action: ALLOW

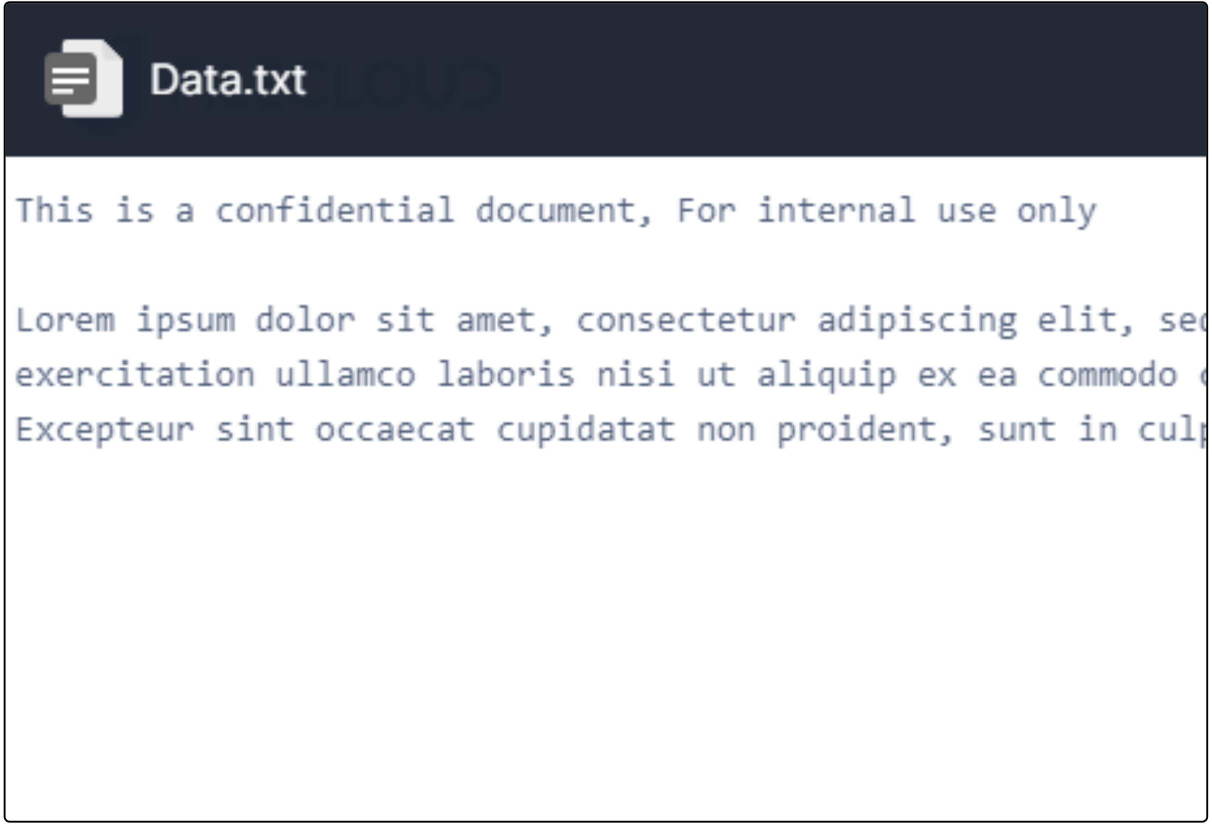
DLP Mode: ENFORCE

Rule Notification (optional):

5. Upload documents to Filecloud's user portal

- Log in to the FileCloud user portal.
- Upload multiple documents to My Files or to a Team Folder. Some of the files should contain confidential information.
- The classification rule will detect documents that contain confidential information and set the attribute "Confidential" to "Yes".
- The classification rule will detect documents that do not contain confidential information and set the attribute "Confidential" to "No".

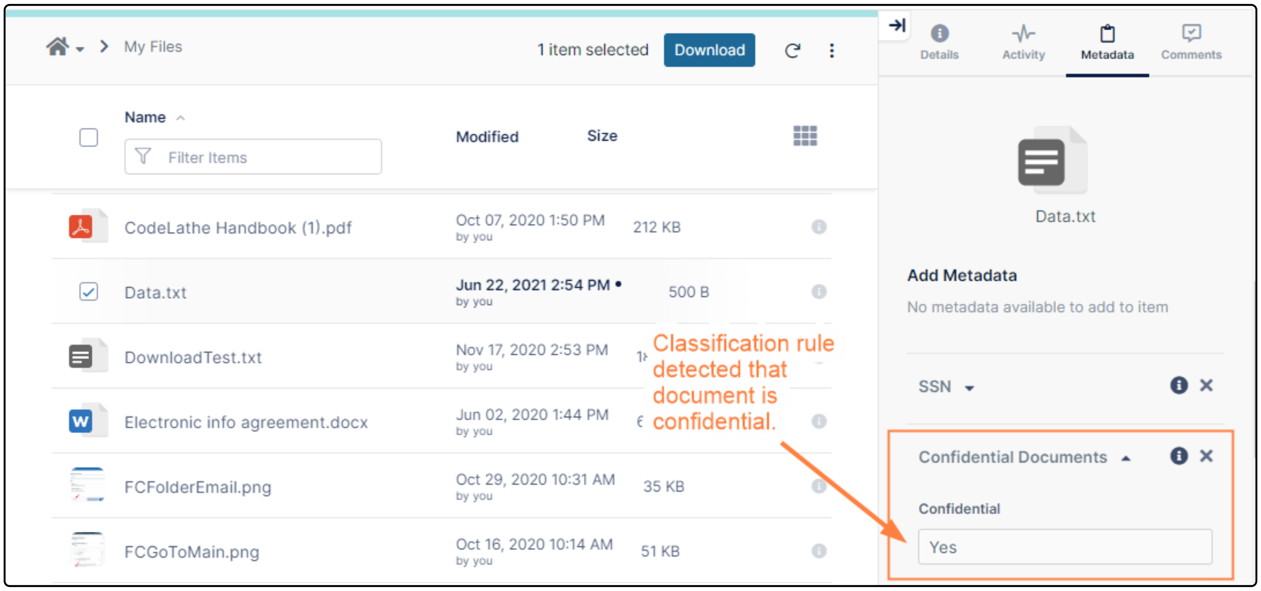
Content of uploaded document with confidential statement in it:



Data.txt

```
This is a confidential document, For internal use only

Lorem ipsum dolor sit amet, consectetur adipiscing elit, se
exercitation ullamco laboris nisi ut aliquip ex ea commodo 
Excepteur sint occaecat cupidatat non proident, sunt in cul
```



☐	Name	Modified	Size
	CodeLathe Handbook (1).pdf	Oct 07, 2020 1:50 PM by you	212 KB
☑	Data.txt	Jun 22, 2021 2:54 PM • by you	500 B
	DownloadTest.txt	Nov 17, 2020 2:53 PM by you	1
	Electronic info agreement.docx	Jun 02, 2020 1:44 PM by you	6
	FCFolderEmail.png	Oct 29, 2020 10:31 AM by you	35 KB
	FCGoToMain.png	Oct 16, 2020 10:14 AM by you	51 KB

Classification rule detected that document is confidential.

Data.txt

Add Metadata

No metadata available to add to item

SSN

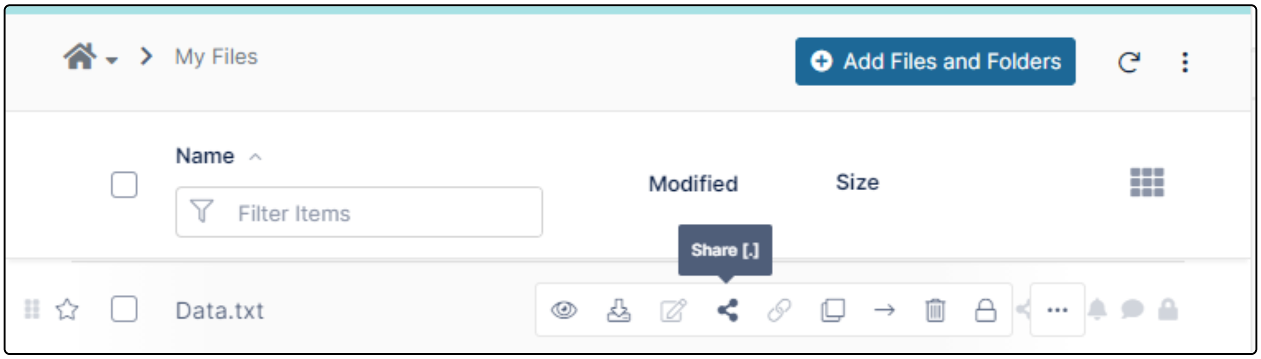
Confidential Documents

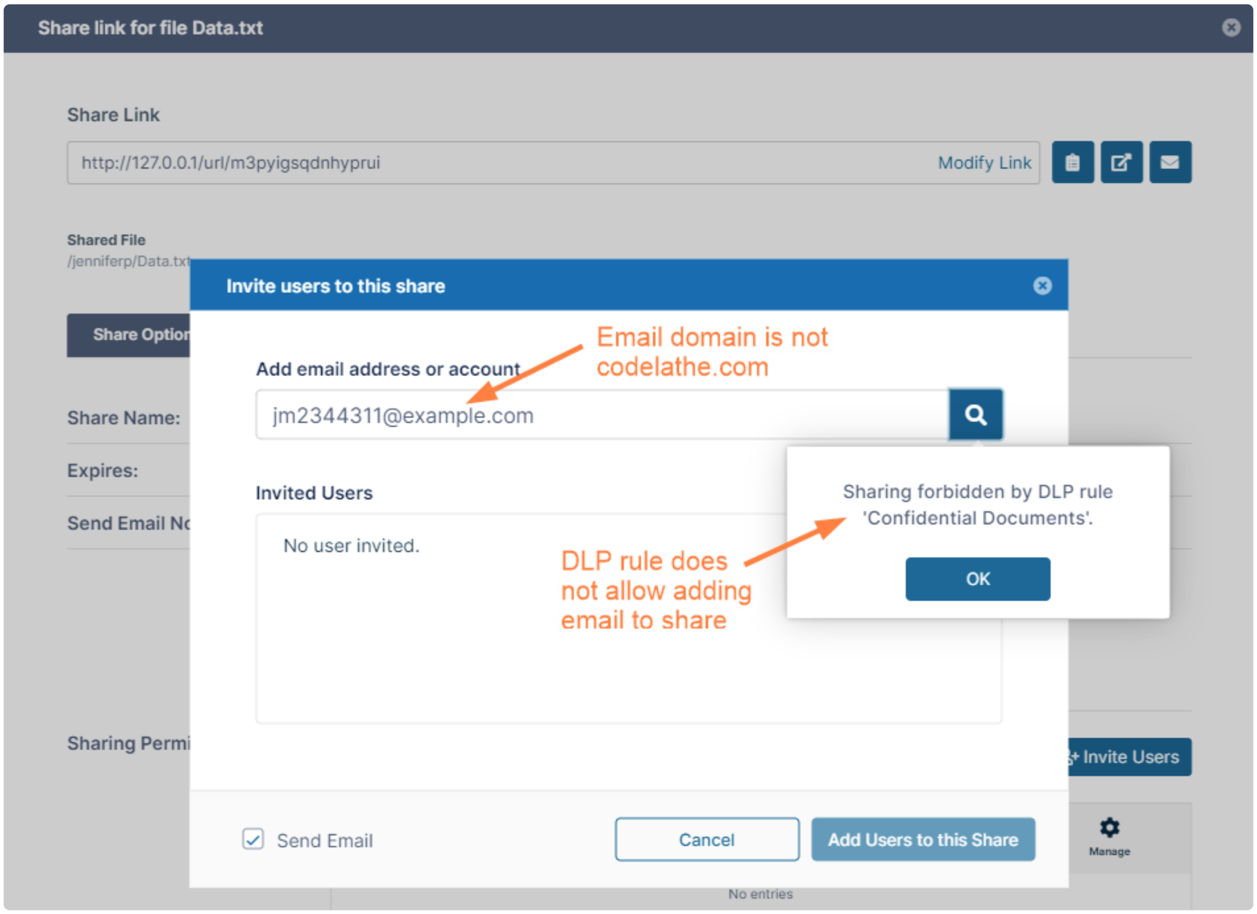
Confidential: Yes

6. Test the Smart DLP rule

- Log in to the FileCloud user portal and share a file that contains confidential information.

- Confirm that sharing is only allowed with users from the domain "codelathe.com".




Share link for file Data.txt

Share Link: http://127.0.0.1/url/m3pyigsqdnhyprui

Shared File: /jenniferp/Data.txt

Invite users to this share

Add email address or account: jm2344311@example.com

Invited Users: No user invited.

Sharing forbidden by DLP rule 'Confidential Documents'.

Email domain is not codelathe.com

DLP rule does not allow adding email to share

Detect documents with US Social Security Number and allow sharing only with specific domains

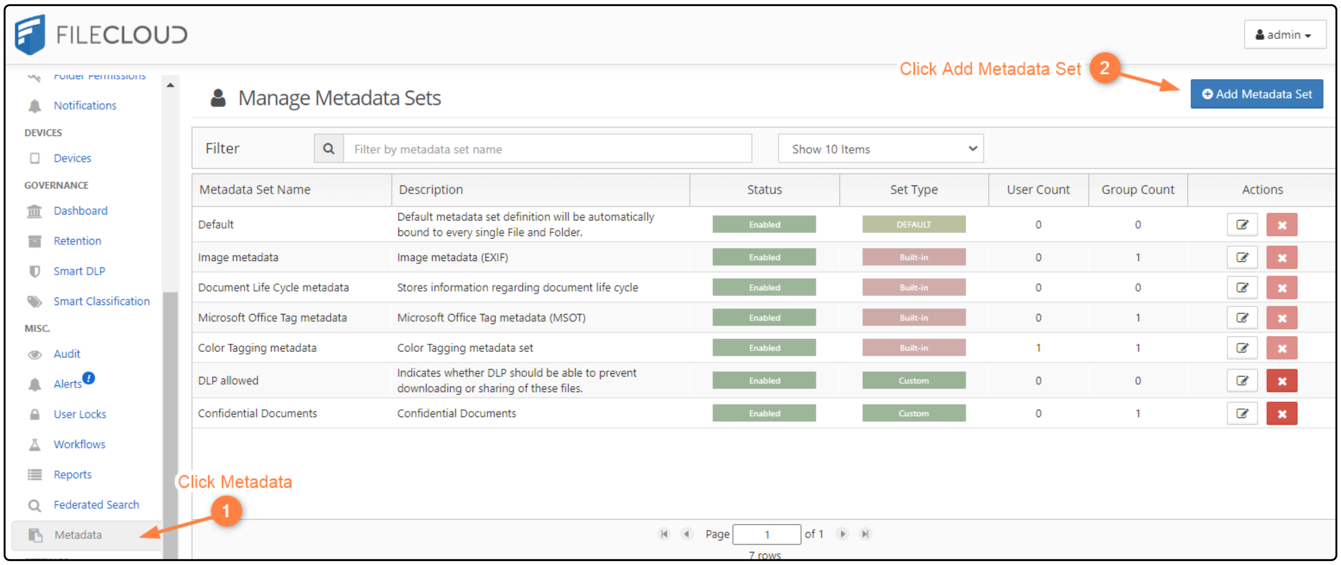
Overview:

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**.

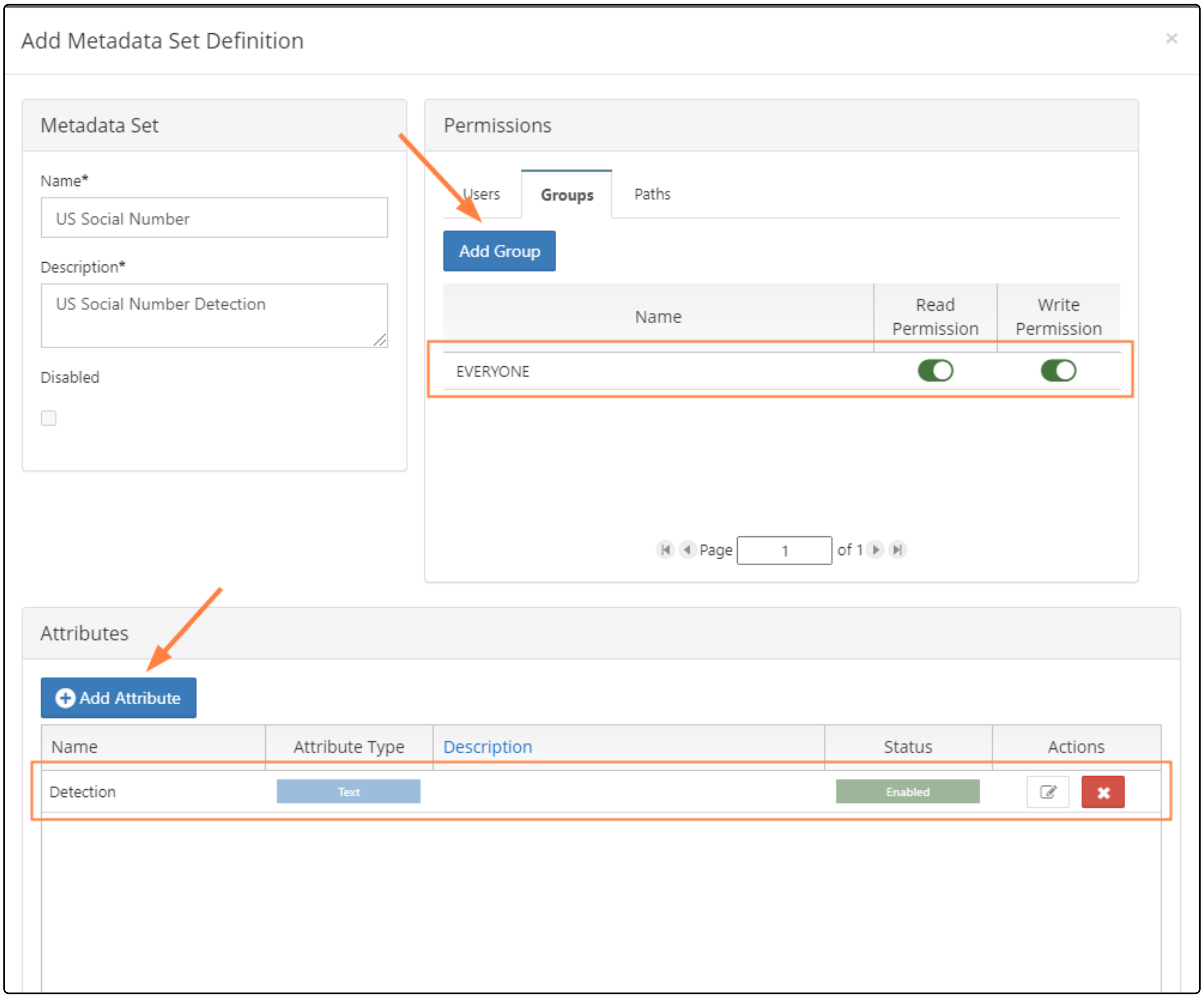


Click Add Metadata Set 2

Click Metadata 1

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.



Add Metadata Set Definition

Metadata Set

Name*: US Social Number

Description*: US Social Number Detection

Disabled □

Permissions

Name	Read Permission	Write Permission
EVERYONE	●	●

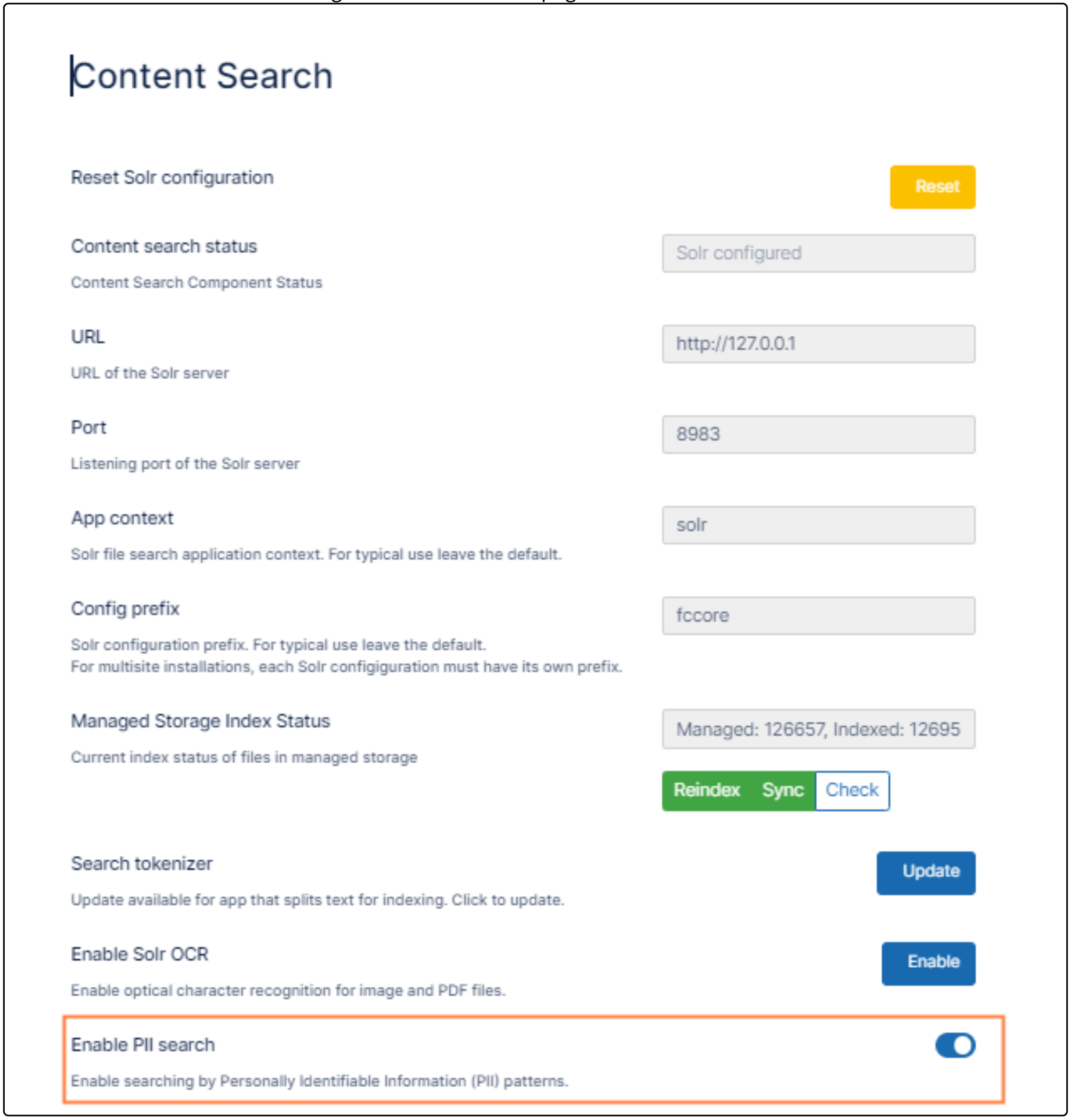
Attributes

Name	Attribute Type	Description	Status	Actions
Detection	Text		Enabled	

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

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 configigguration must have its own prefix.

Managed Storage Index Status: Managed: 126657, Indexed: 12695

Current index status of files in managed storage

Search tokenizer

Update available for app that splits text for indexing. Click to update.

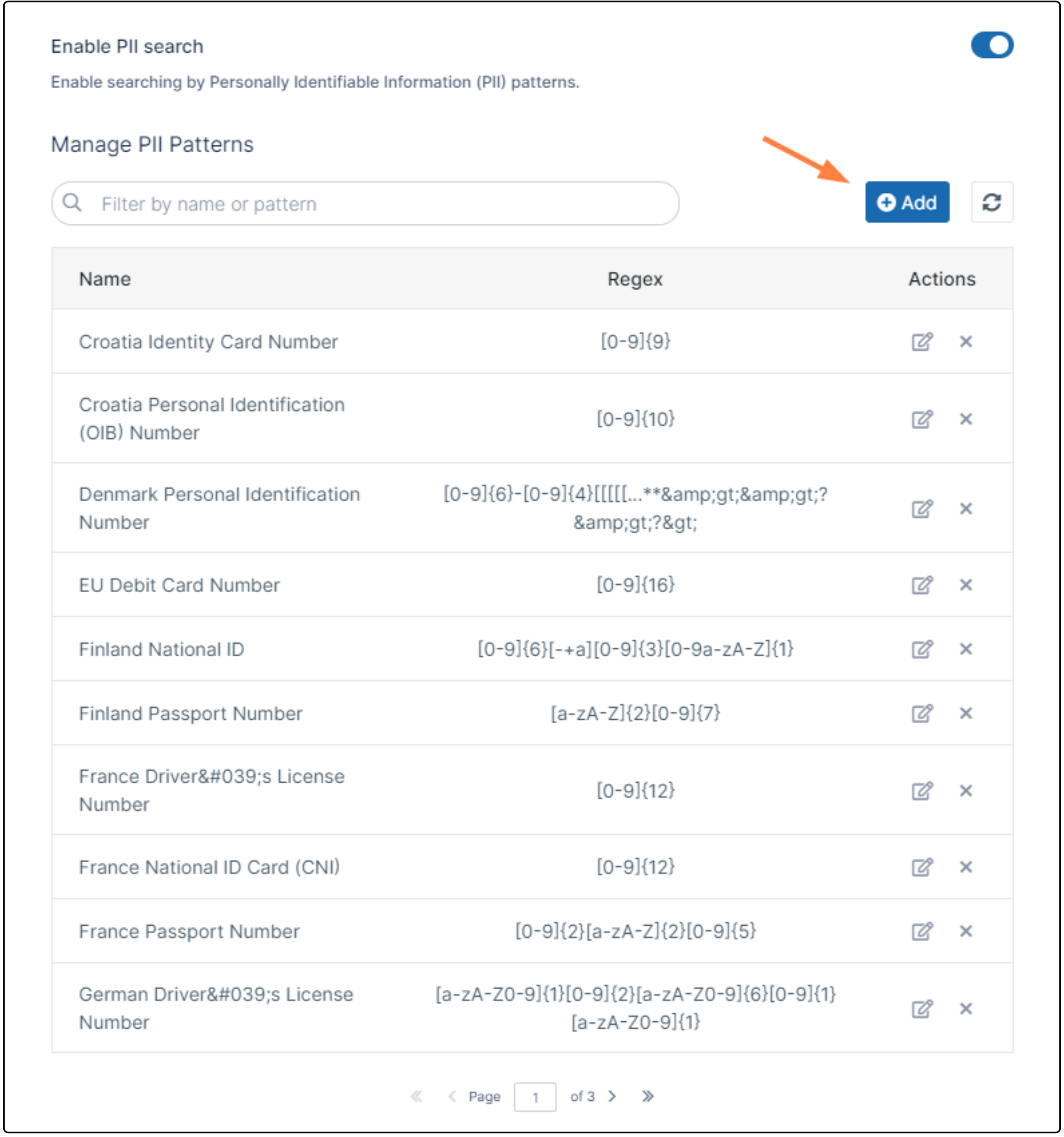
Enable Solr OCR

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.

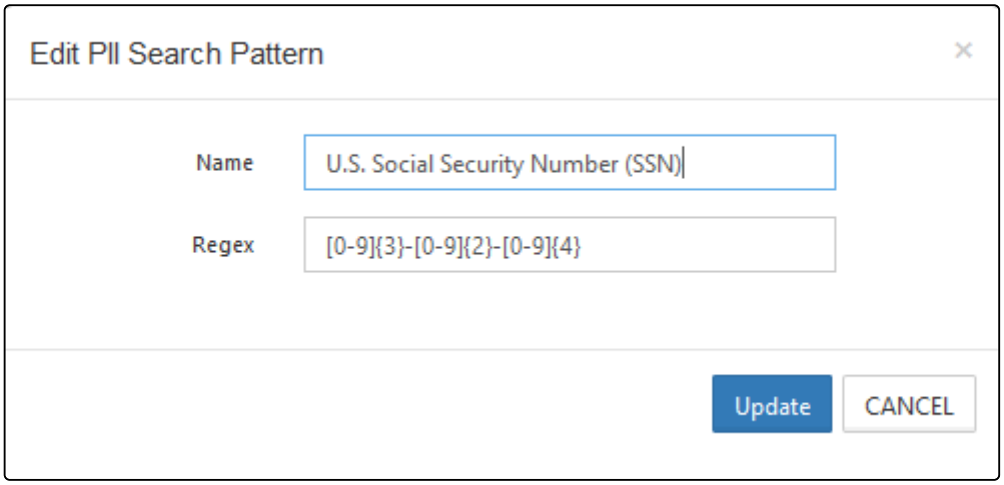


Enable PII search

Enable searching by Personally Identifiable Information (PII) patterns.

Manage PII Patterns

Name	Regex	Actions
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}[[[[[...**&gt;&gt;?&gt;?&gt;	✎ ×
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&#039;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&#039;s License Number	[a-zA-Z0-9]{1}[0-9]{2}[a-zA-Z0-9]{6}[0-9]{1}[a-zA-Z0-9]{1}	✎ ×



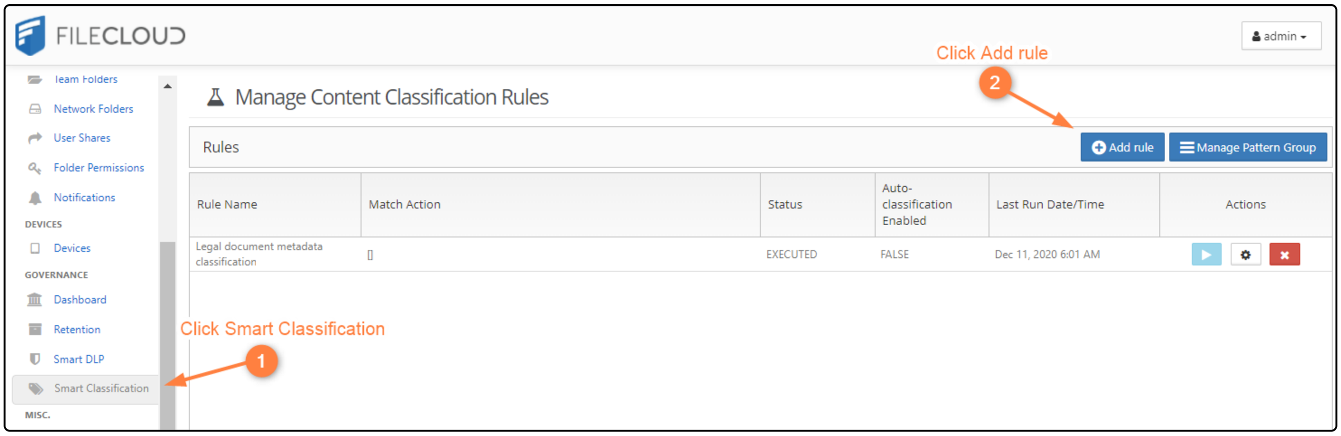
Edit PII Search Pattern

Name: U.S. Social Security Number (SSN)

Regex: [0-9]{3}-[0-9]{2}-[0-9]{4}

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



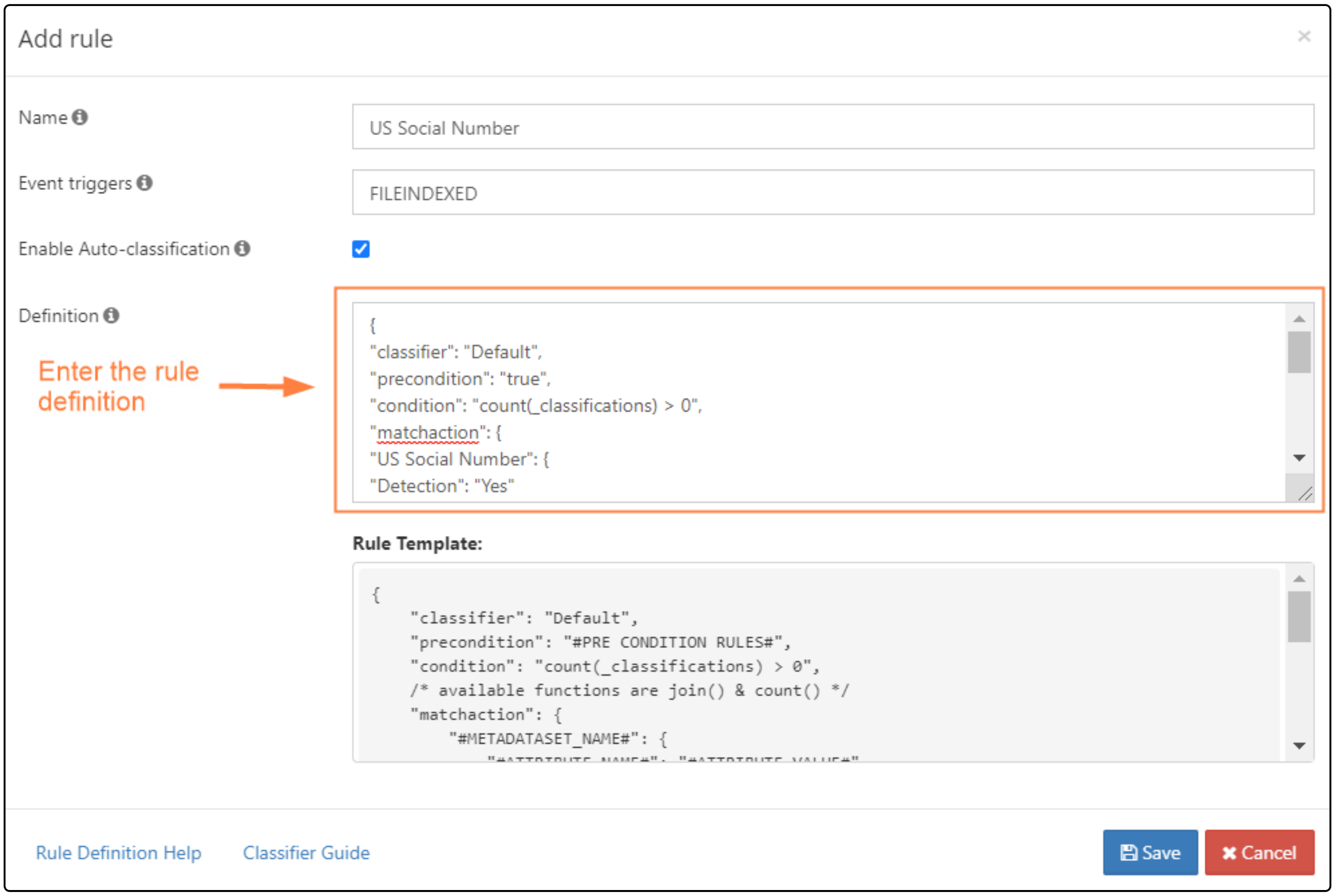
Manage Content Classification Rules

Rules

Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
Legal document metadata classification	[]	EXECUTED	FALSE	Dec 11, 2020 6:01 AM	▶ ⚙ ✖

- 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)"
]
}
}
```



Name: US Social Number

Event triggers: FILEINDEXED

Enable Auto-classification: ☑

Definition:

Enter the rule definition

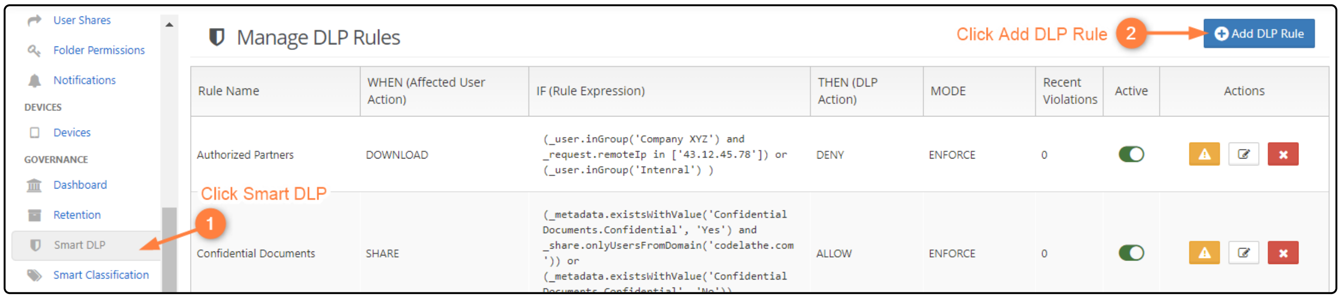
```
{
"classifier": "Default",
"precondition": "true",
"condition": "count(_classifications) > 0",
"matchaction": {
"US Social Number": {
"Detection": "Yes"
```

Rule Template:

```
{
    "classifier": "Default",
    "precondition": "#PRE CONDITION RULES#",
    "condition": "count(_classifications) > 0",
    /* available functions are join() & count() */
    "matchaction": {
        "#METADATASET_NAME#": {
            "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#"
```

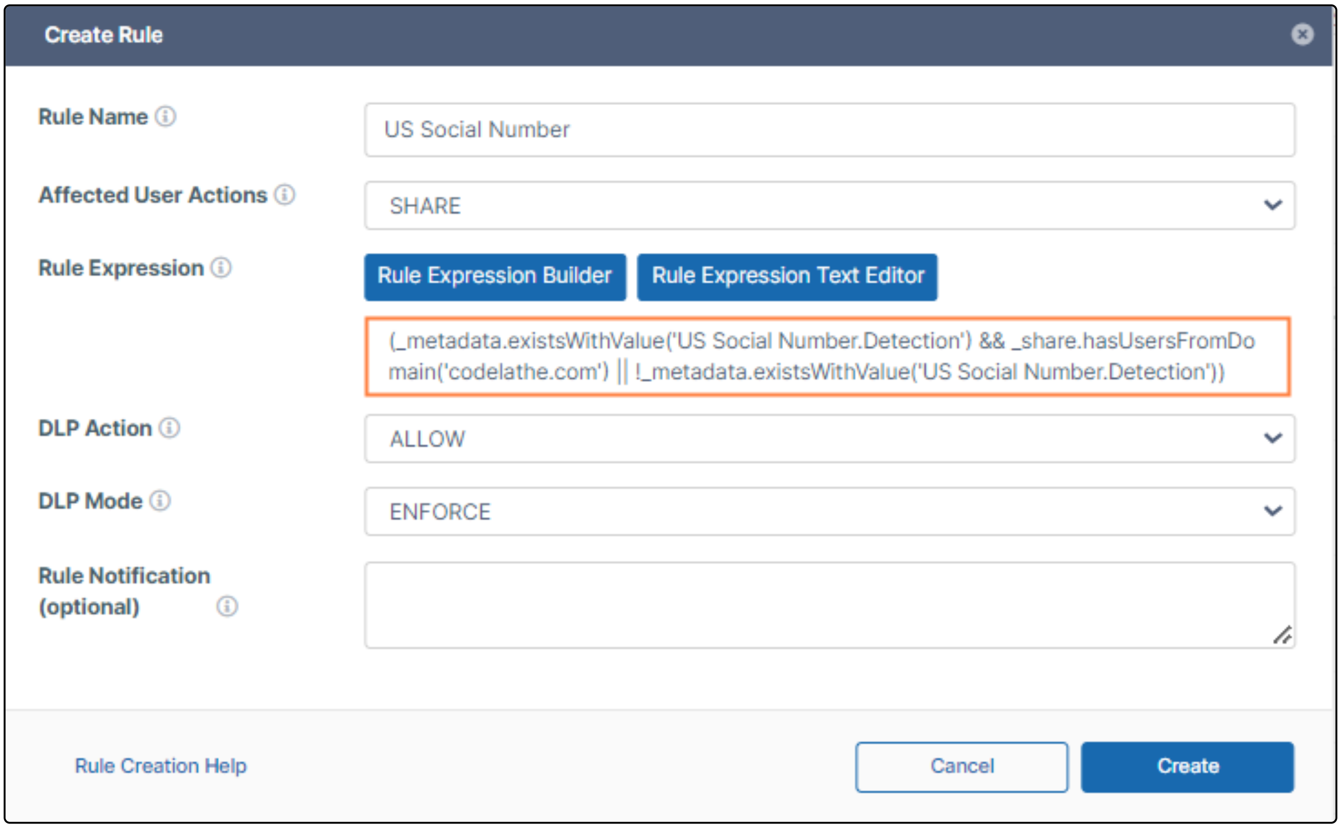
4. Create Smart DLP Rule

- 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

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	`(_user.inGroup('Company XYZ') and _request.remoteIp in ['43.12.45.78']) or (_user.inGroup('Intenral') )`	DENY	ENFORCE	0		
Confidential Documents	SHARE	`(_metadata.existsWithValue('Confidential Documents.Confidential', 'Yes') and _share.onlyUsersFromDomain('codelathe.com')) or (_metadata.existsWithValue('Confidential Documents.Confidential', 'No'))`	ALLOW	ENFORCE	0		



Create Rule

Rule Name: US Social Number

Affected User Actions: SHARE

Rule Expression:

```
(_metadata.existsWithValue('US Social Number.Detection') && _share.hasUsersFromDomain('codelathe.com') || !_metadata.existsWithValue('US Social Number.Detection'))
```

DLP Action: ALLOW

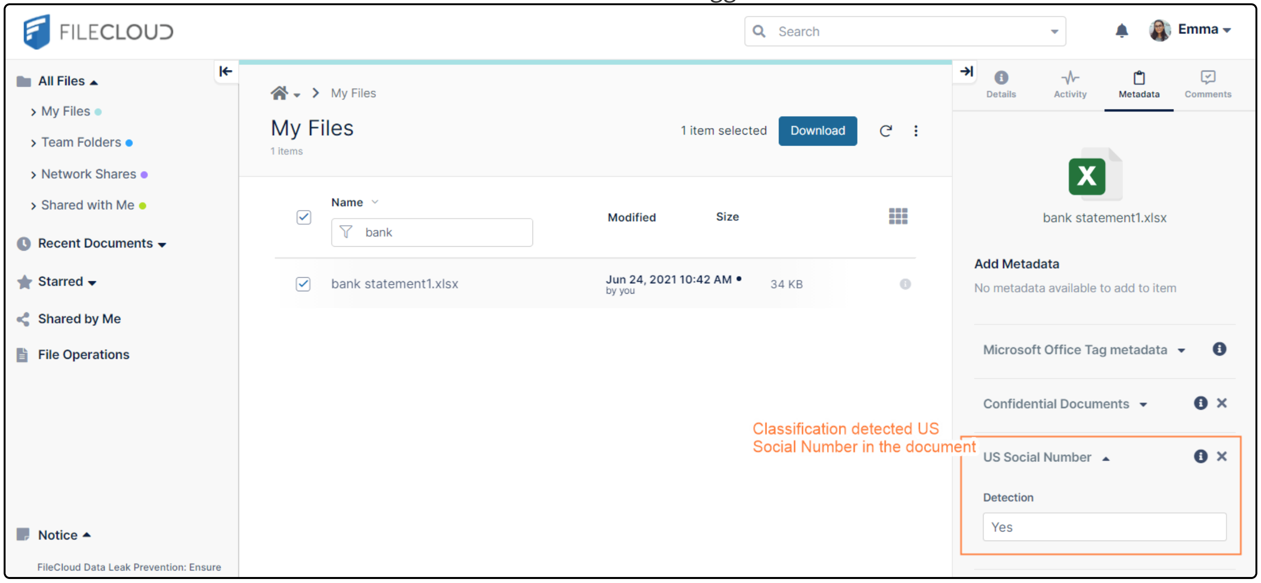
DLP Mode: ENFORCE

Rule Notification (optional):

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".

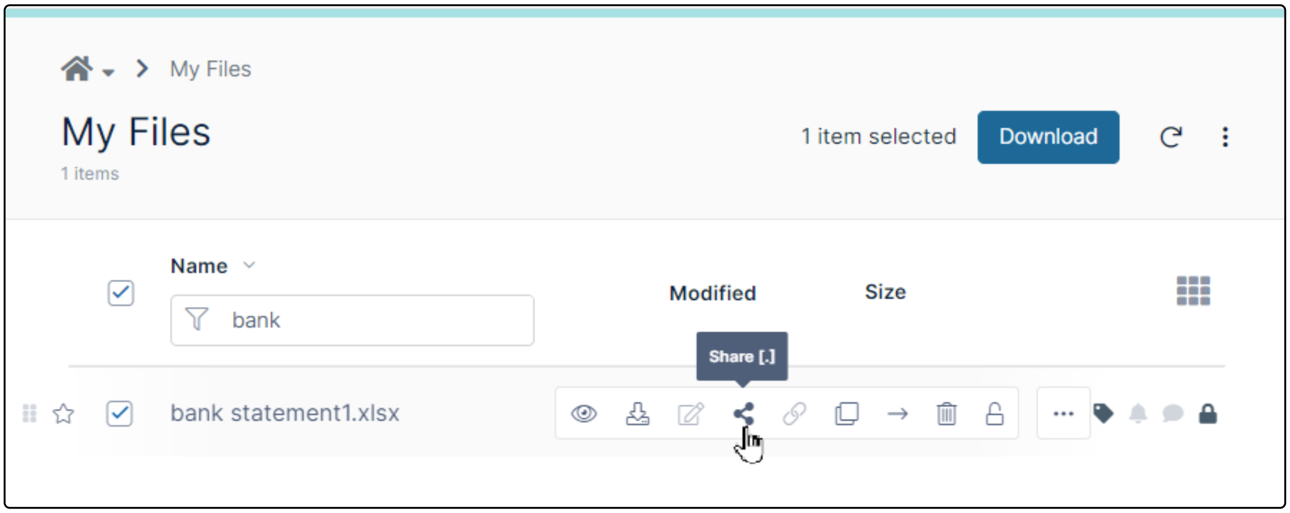
- The documents that do not contain US Social Numbers will be tagged with "Detection" = "No".

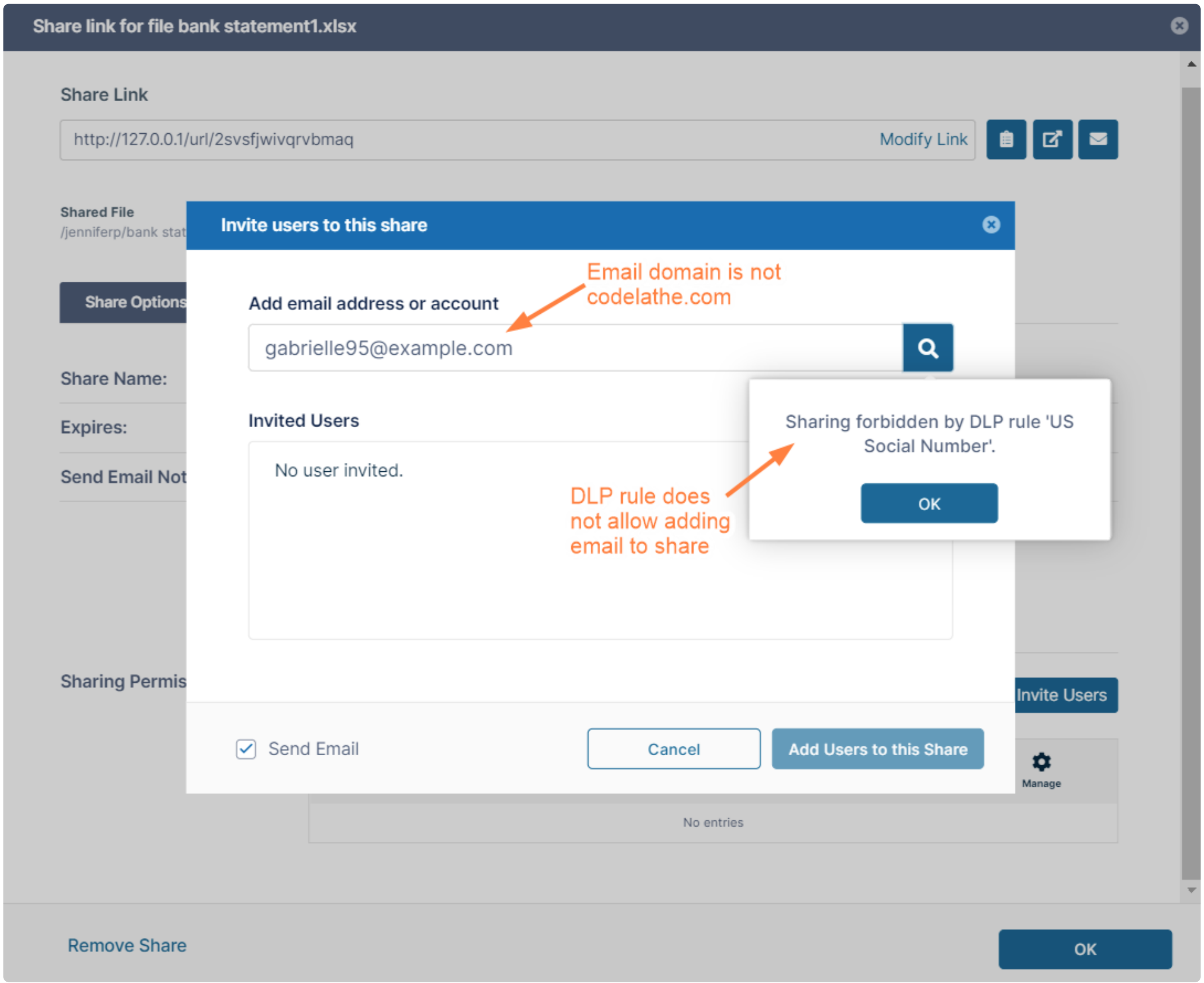


Classification detected US Social Number in the document

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"





Sharing forbidden by DLP rule 'US Social Number'.

Email domain is not codelathe.com

DLP rule does not allow adding email to share

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.

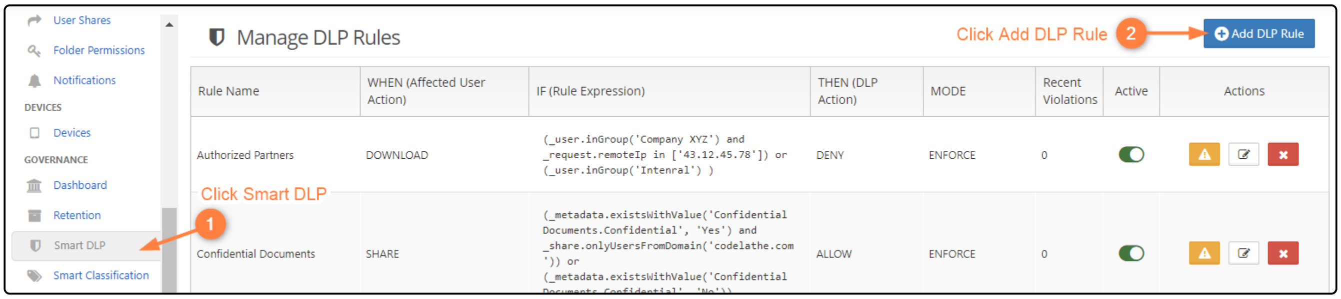
Users from the group "Company XYZ" will be limited to log in only through the Web browser.

Users from group "Internal" will be able to log in through the web browser, Filecloud Sync, Drive, mobile phone applications ...etc

Configuration Steps:

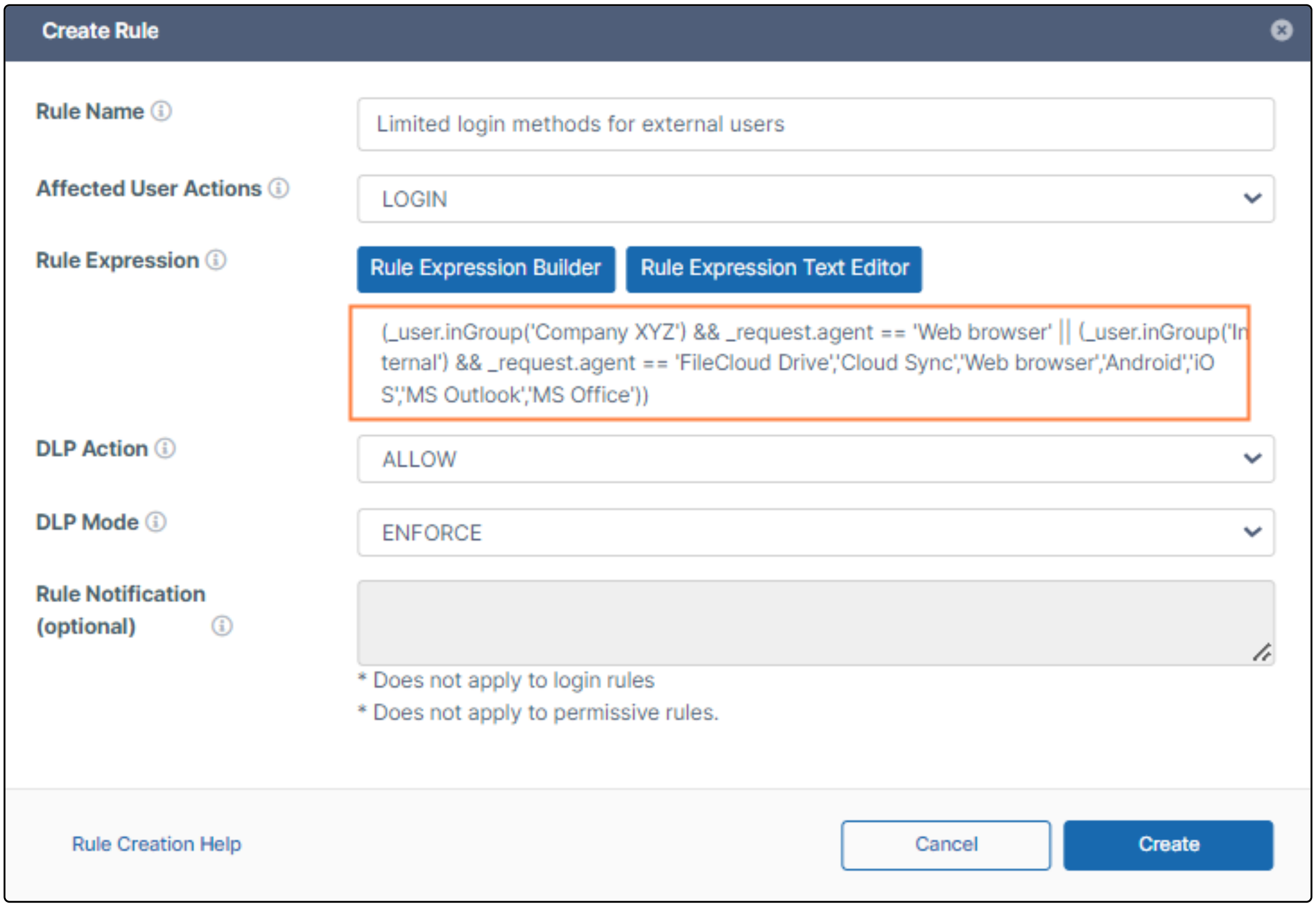
1-Create Smart DLP Rule

- AccessFileCloud'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.



Manage DLP Rules

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Authorized Partners	DOWNLOAD	`(_user.inGroup('Company XYZ') and _request.remoteIp in ['43.12.45.78']) or (_user.inGroup('Intenral') )`	DENY	ENFORCE	0	●	⚠ ✎ ✖
Confidential Documents	SHARE	`(_metadata.existsWithValue('Confidential Documents.Confidential', 'Yes') and _share.onlyUsersFromDomain('codelathe.com ')) or (_metadata.existsWithValue('Confidential Documents.Confidential', 'No'))`	ALLOW	ENFORCE	0	●	⚠ ✎ ✖



Rule Name: Limited login methods for external users

Affected User Actions: LOGIN

```
(_user.inGroup('Company XYZ') && _request.agent == 'Web browser' || (_user.inGroup('In
ternal') && _request.agent == 'FileCloud Drive','Cloud Sync','Web browser','Android','iO
S','MS Outlook','MS Office'))
```

DLP Action: ALLOW

DLP Mode: ENFORCE

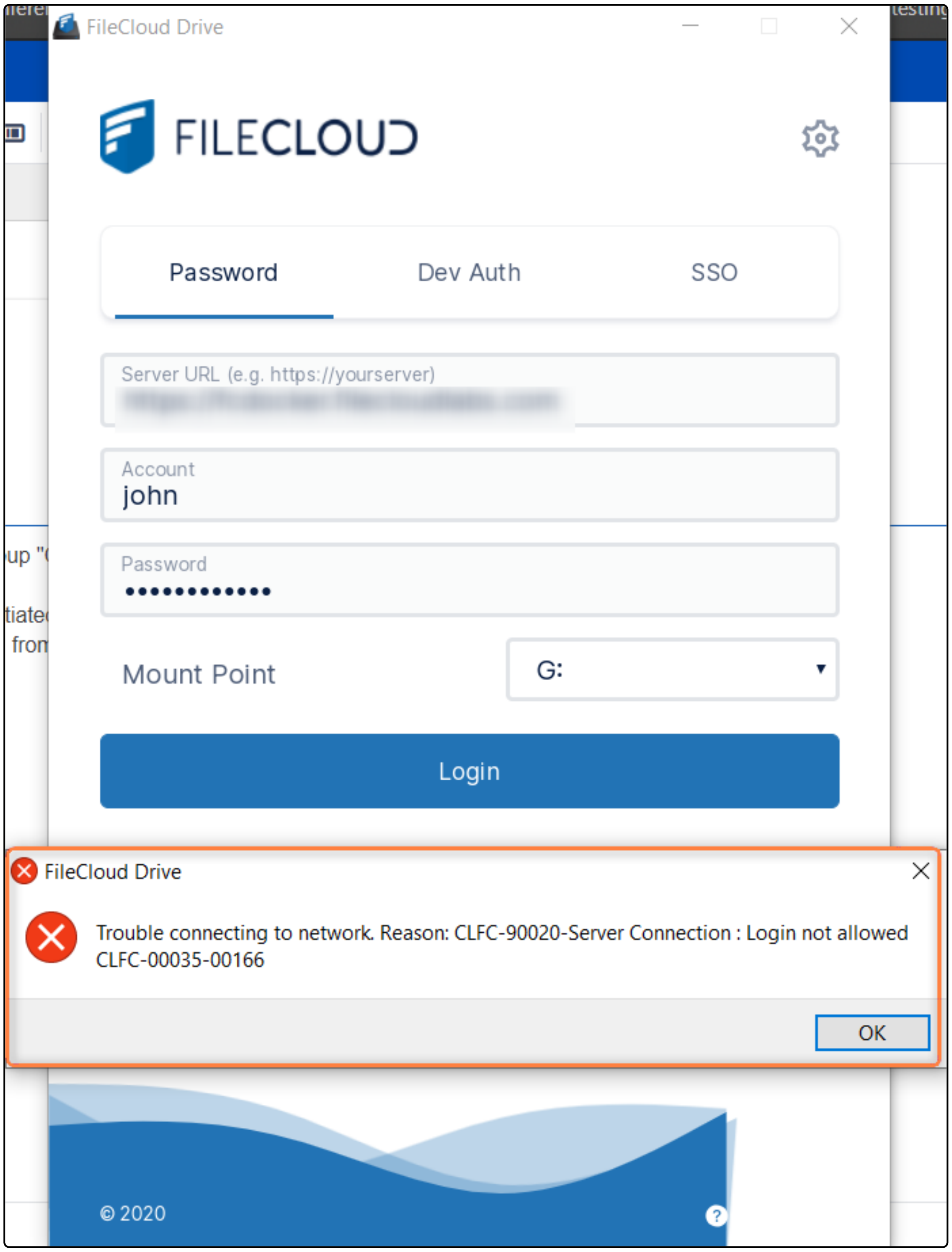
Rule Notification (optional)

* Does not apply to login rules
* Does not apply to permissive rules.

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.



Server URL (e.g. https://yourserver) [redacted]

Account john

Password •••••••••••••

Mount Point G:

FileCloud Drive

Trouble connecting to network. Reason: CLFC-90020-Server Connection : Login not allowed CLFC-00035-00166

OK

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.remoteIp 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.

Import/Export DLP, CCE, and Metadata Settings

The FIleCloud Import/Export Settings tool is available in FileCloud version 20.3 and later.

FileCloud's Import/Export Settings tool enables you to import or export content classification rules, DLP rules, and metadata set definitions.

Location and Syntax

The Import/Export Settings tool is located at **C:\xampp\htdocs\resources\tools\ruleset\RuleSetTool.php**.

The tool enables you to import and export the following collections:

Collection name	Collection in command line format	Import/export file name
metadata set definitions	`metadata_set_definitions`	metadata_set_definitions.txt
content classification rules	`content_classification_rules`	content_classification_rules.txt
dlp rules	`dlp_rules`	dlp_rules.txt
search patterns	`searchpattern`	searchpattern.txt
search pattern groups	`searchpattern_group`	searchpattern_group.txt

On import, the file storing the collection must have the exact name specified in the table above under **Import/export file name** or the command will not know which file to import. On export, the tool will export to the specified filename.

The syntax for **RulesSetTool** is:

```
{-i|-e} -c COLLECTION,...  [-d "directory path"] [-o]
```

where:

Parameter	Function	Notes
-i	import the collections	

Parameter	Function	Notes
-e	export the collections	

-c COLLECTION,...	A list of the collections to import or export.
	Either in the format:
	-c COLLECTION1 -c COLLECTION2 . . .
	Or:
	-c COLLECTION1, COLLECTION2, . . .
		Specify one or more of the collections listed in the table above. You can also list the collection in its file format.
		For example, both of the following are valid:
		`-c searchpattern`
		or
		`-c searchpattern.txt`

-d "directorypath"	The directory path to export to or import from.	Optional. If this is not included, the current directory is used.
-o	Used with -i (import) only. Overwrite the existing collections of the same type in FileCloud.	Optional. If -o is not included, all rules and settings of the specified collections are added (so if you already have any of the rules or settings in FileCloud, after import you will have duplicates). If -o is included, the rules and settings of the specified collections are deleted from FileCloud before the rules and settings of the collections from the files are imported. See the recommended sequence below if you are importing updated collections that have duplicate rules or settings in your database.

Command examples

Action	Command	example

Import a specific collection from the current directory to FileCloud	`-i -c [collection]`	`php ./RuleSetTool.php -i -c metadata_set_definitions`
		`OR`
		`php ./RuleSetTool.php -i -c metadata_set_definitions.txt`
		Import metadata set definitions from the current directory to the FileCloud database.

Export a specific collection from FileCloud to the current directory	`-e -c [collection]`	`php ./RuleSetTool.php -e -c content_classification_rules` Export content classification rules from the FileCloud database to the current directory.
Import multiple specified collections from the current directory to FileCloud. Include any number of collections.	`-i -c [collection1], [collection2], . . .`	`php ./RuleSetTool.php -i -c metadata_set_definitions,searchpattern,searchpatterngroup,content_classification_rules, dlp_rules` Import all collections from the current directory to the FileCloud database.
Export multiple specified collections from FileCloud to the current directory. Include any number of collections.	`-e -c [collection1], [collection2], . . .`	`php ./RuleSetTool.php -e -c dlp_rules,content_classification_rules` Export DLP rules and CCE rules from the FileCloud database to the current directory.

Action	Command	example
Import the specified collection(s) from a specific directory to FileCloud.	`-i -c [collection1], [collection2] , . . . -d "directorypath"`	`php ./RuleSetTool.php -i -c metadata_set_definitions,searchpattern -d "C:/Users/joe/Desktop/rules"` Import metadata set definitions and searchpatterns from the directory C:/Users/joe/Desktop/rules to the FileCloud database.
Export specified collection(s) from FileCloud to a specific directory.	`-e -c [collection1], [collection2] , . . . -d "directorypath"`	`php ./RuleSetTool.php -e -c dlp_rules,content_classification_rules -d "C:/Users/joe/Desktop/rules"` Export DLP rules and CCE rules from the FileCloud database to the directory C:/Users/joe/Desktop/rules.
Import specified collection(s) from the current directory to FileCloud and overwrite the existing collections (of the same type) in FileCloud.	`-i -c [collection1], [collection2] , . . . -o`	`php ./RuleSetTool.php -i -c metadata_set_definitions -o` Import metadata set definitions from the current directory to the FileCloud database, but first delete the existing metadataset definitions in the FileCloud database.
Import specified collection(s) from a specific directory to FileCloud and overwrite the existing collections (of the same type) in FileCloud.	`-i -c [collection1], [collection2] , . . . -d "directorypath" -o`	`php ./RuleSetTool.php -i -c dlp_rules,content_classification_rules -d "C:/Users/joe/Desktop/rules" -o` Import DLP rules and CCE rules from the FileCloud database to the directory C:/Users/joe/Desktop/rules, but first delete the existing DLP rules and CCE rules in C:/Users/joe/Desktop/rules.

Importing updated versions of collections

If you want to import an updated collection with rules or settings that are already in FileCloud, export the FileCloud collection first, and then import the updated collection with the overwrite parameter so you don't end up with duplicate entries. The overwrite parameter causes the tool to delete the collection in FileCloud before it imports the updated one.

For example, to update your DLP rules and CCE rules in FileCloud:

1. Export your DLP rules and CCE rules from FileCloud by running:

```
php ./RuleSetTool.php -e -c dlp_rules,content_classification_rules
```

2. Update the collections that you just exported into your current directory (or replace the collections with updated files)
3. Run the RuleSetTool with **-o** so that it deletes your FileCloud DLP rules and CCE rules, and then replaces them with the updated files:

```
php ./RuleSetTool.php -i -c dlp_rules,content_classification_rules -o
```

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) - Technical Safeguards - Set up a retention policy to protect files and folders from deletion.
- 164.316(b)(2)(i)- Policies and procedures and documentation requirements - Use Retention Policy to retain files for 6 years.

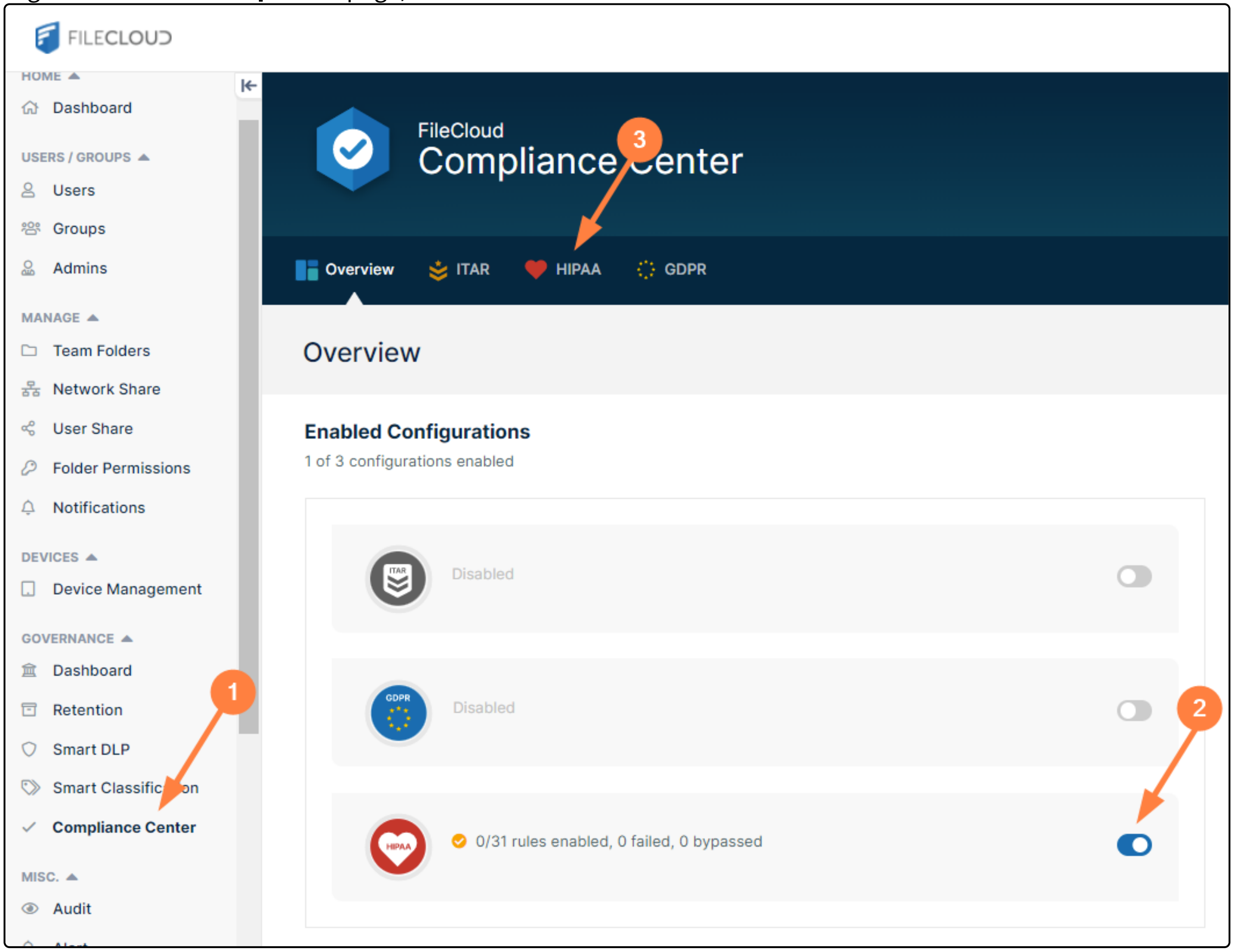
This example will walk you through the process necessary to pass these requirements. The broader steps involve:

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.



Overview

Enabled Configurations

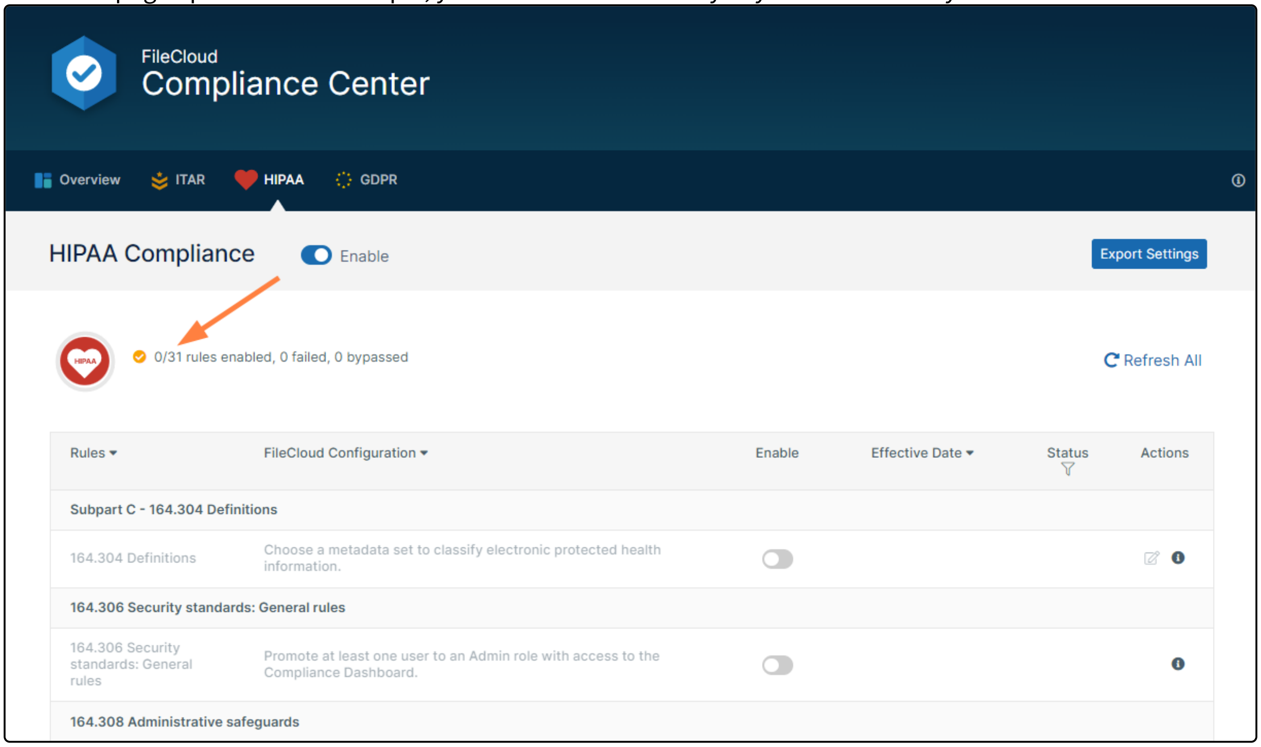
1 of 3 configurations enabled

Disabled

Disabled

0/31 rules enabled, 0 failed, 0 bypassed

The HIPAA page opens. In this example, you have not enabled any of your HIPAA rules yet.



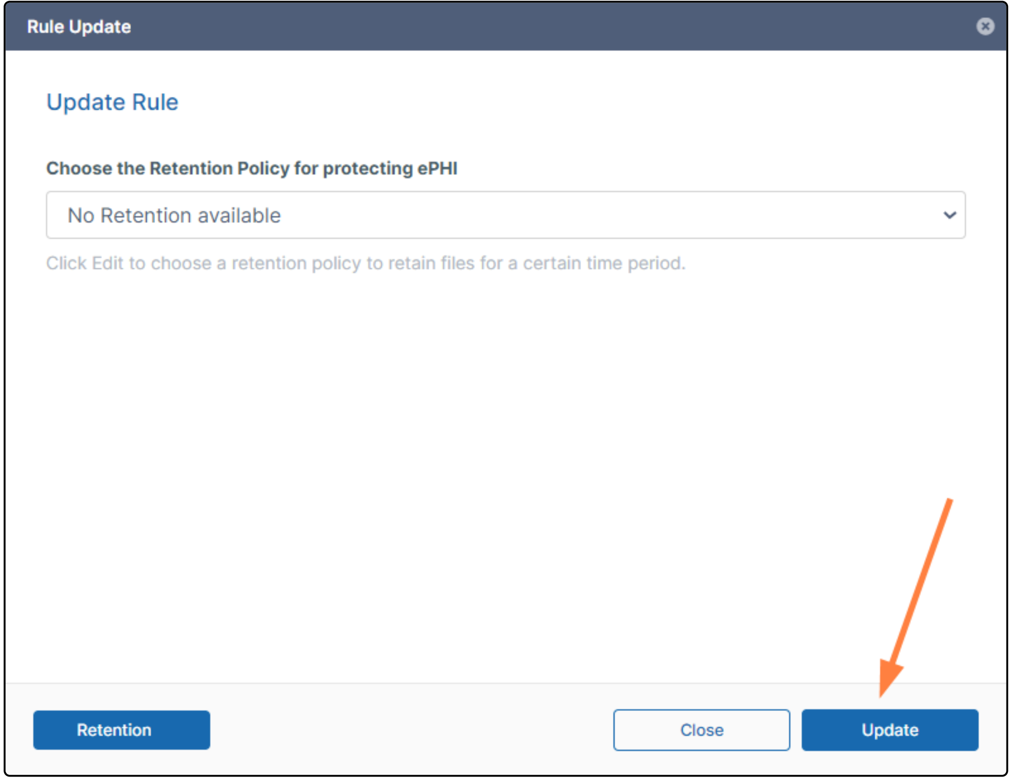
HIPAA Compliance

0/31 rules enabled, 0 failed, 0 bypassed

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.	○			
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.	○			
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.

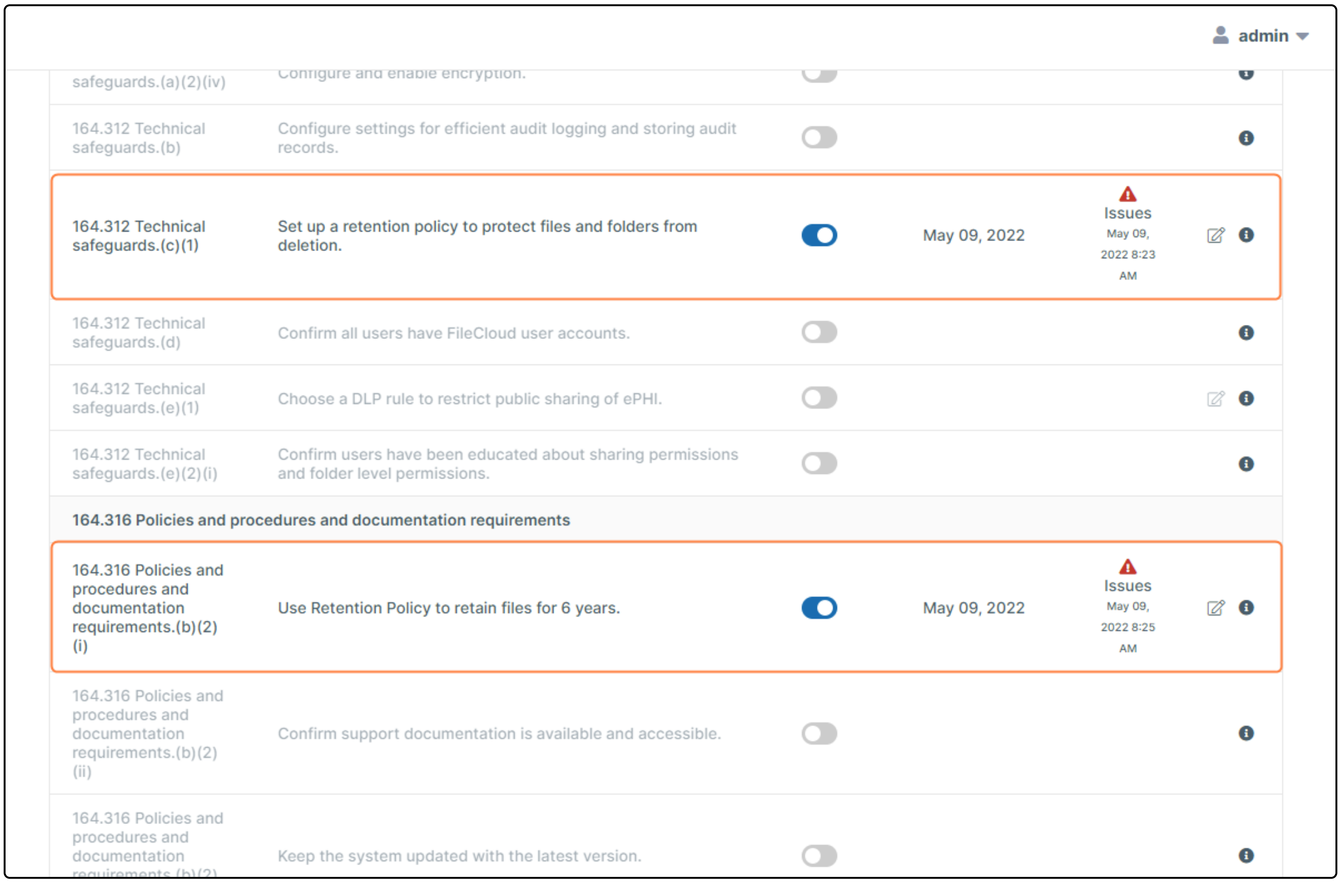


Choose the Retention Policy for protecting ePHI

No Retention available

Click Edit to choose a retention policy to retain files for a certain time period.

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.



safeguards.(a)(2)(iv)	Configure and enable encryption.	○			
164.312 Technical safeguards.(b)	Configure settings for efficient audit logging and storing audit records.	○			
164.312 Technical safeguards.(c)(1)	Set up a retention policy to protect files and folders from deletion.	●	May 09, 2022	Issues May 09, 2022 8:23 AM	
164.312 Technical safeguards.(d)	Confirm all users have FileCloud user accounts.	○			
164.312 Technical safeguards.(e)(1)	Choose a DLP rule to restrict public sharing of ePHI.	○			
164.312 Technical safeguards.(e)(2)(i)	Confirm users have been educated about sharing permissions and folder level permissions.	○			
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.	●	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.	○			
164.316 Policies and procedures and documentation requirements.(b)(2)	Keep the system updated with the latest version.	○			

Step 2: Create a metadata attribute to tag files with ePHI data

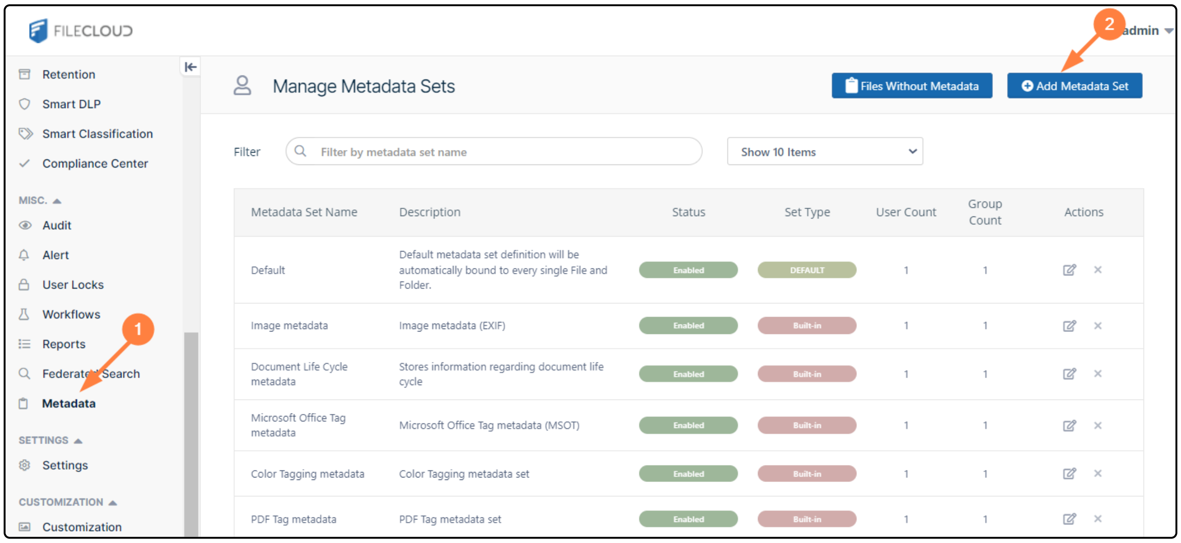
The function of HIPAA compliance is to protect electronic protected health information, such as individuals' medical records and insurance information. Before you can place safeguards on this information, it's necessary that you identify which files contain it. You can do this by configuring FileCloud's 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**.



Manage Metadata Sets

Filter: Filter by metadata set name

Show 10 Items

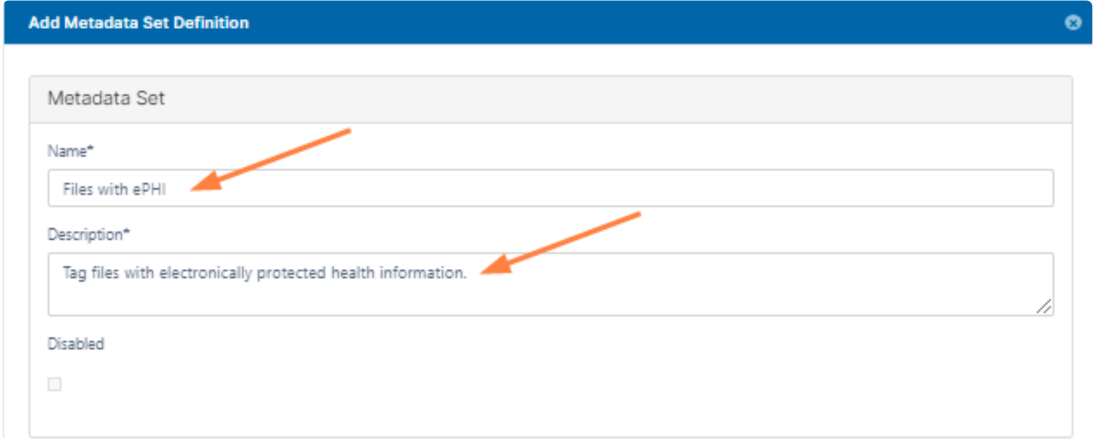
Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	1	1	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	1	1	
Document Life Cycle metadata	Stores information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



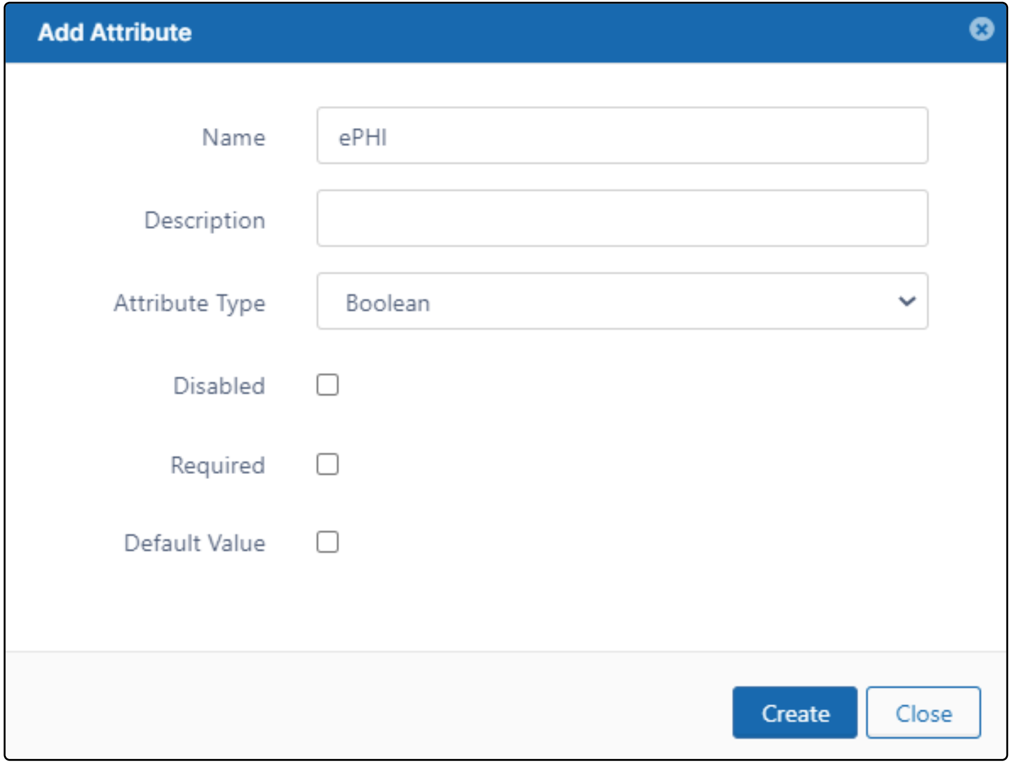
Name*: Files with ePHI

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**.

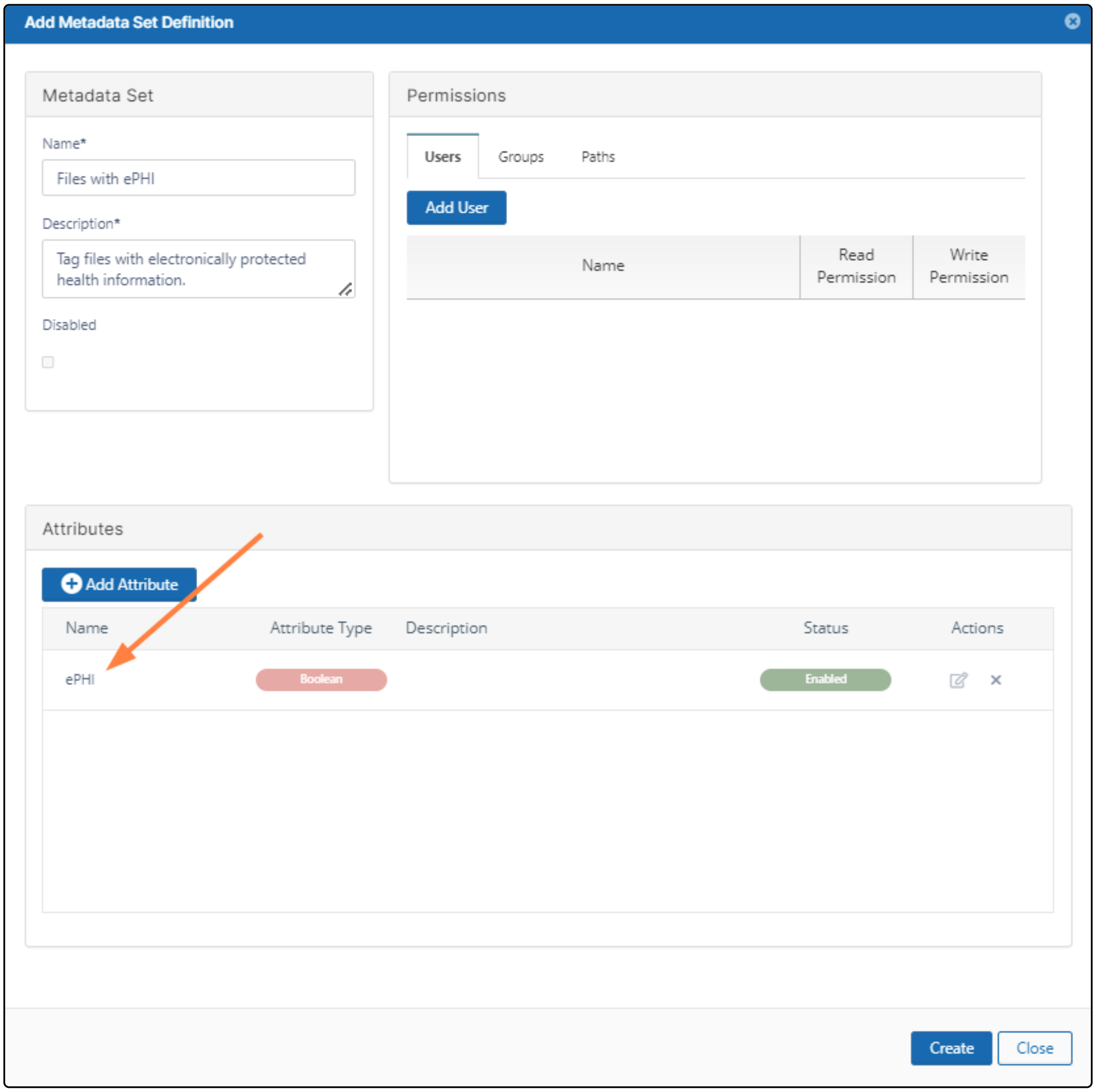
Whenever a file has ePHI, this Boolean value will be set to **1**.



Add Attribute

Name	ePHI
Description	
Attribute Type	Boolean
Disabled	□
Required	□
Default Value	□

d. Click **Create**.



Add Metadata Set Definition

Metadata Set

Name*

Files with ePHI

Description*

Tag files with electronically protected health information.

Disabled

☐

Permissions

Name	Read Permission	Write Permission

Attributes

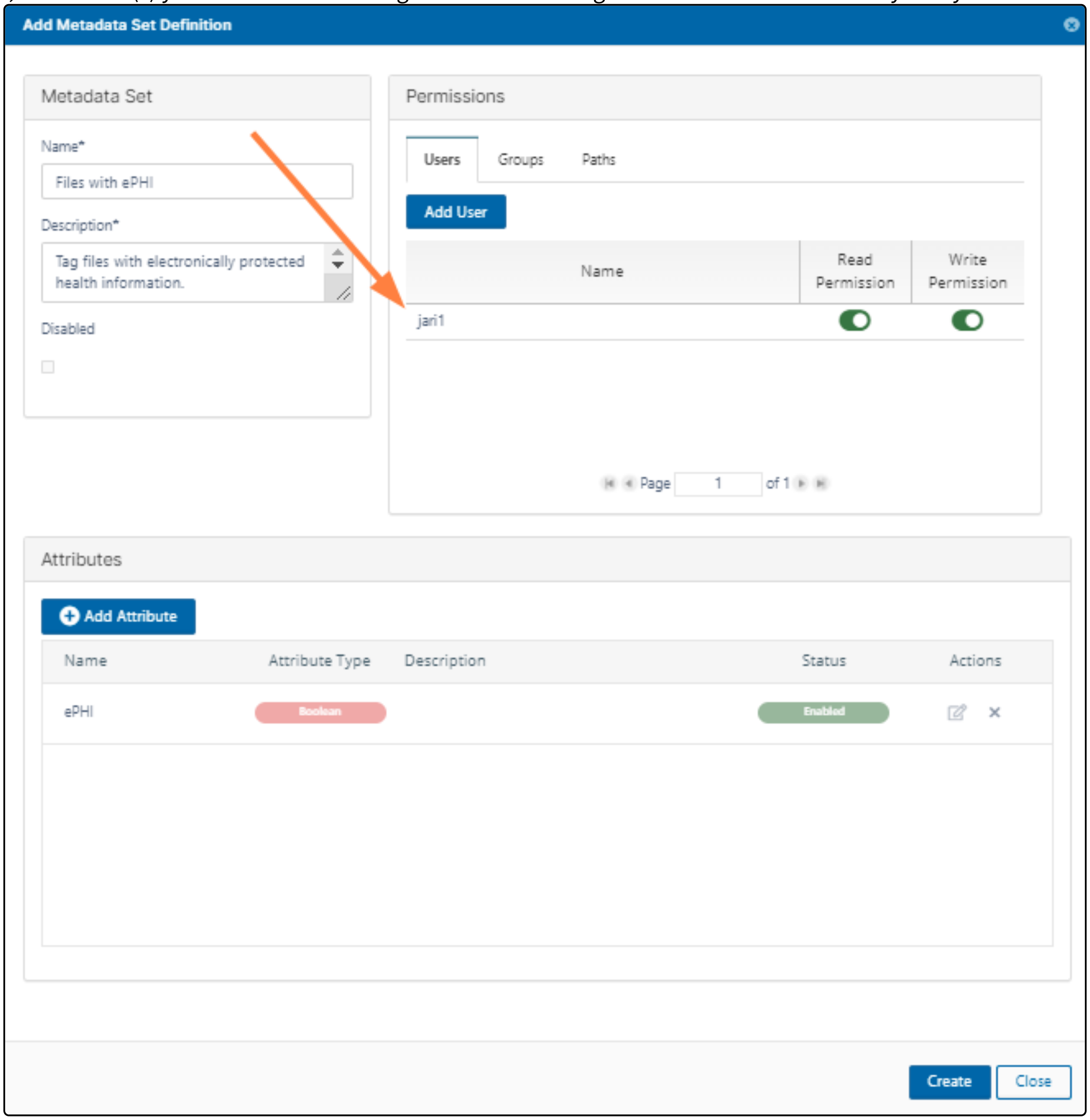
Name	Attribute Type	Description	Status	Actions
ePHI	Boolean		Enabled	✎ ×

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.



Name*: Files with ePHI

Description*: Tag files with electronically protected health information.

Disabled □

Name	Read Permission	Write Permission
jari1	●	●

Name	Attribute Type	Description	Status	Actions
ePHI	Boolean		Enabled	

Step 3: Create a a pattern group that identifies file content as ePHI

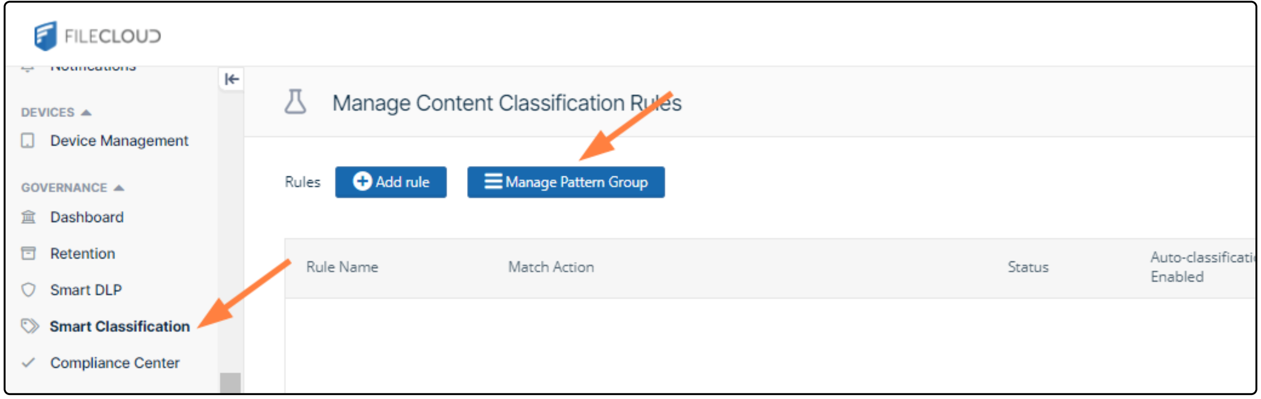
Community HMO has the following types of files that contain PHI:

- 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.

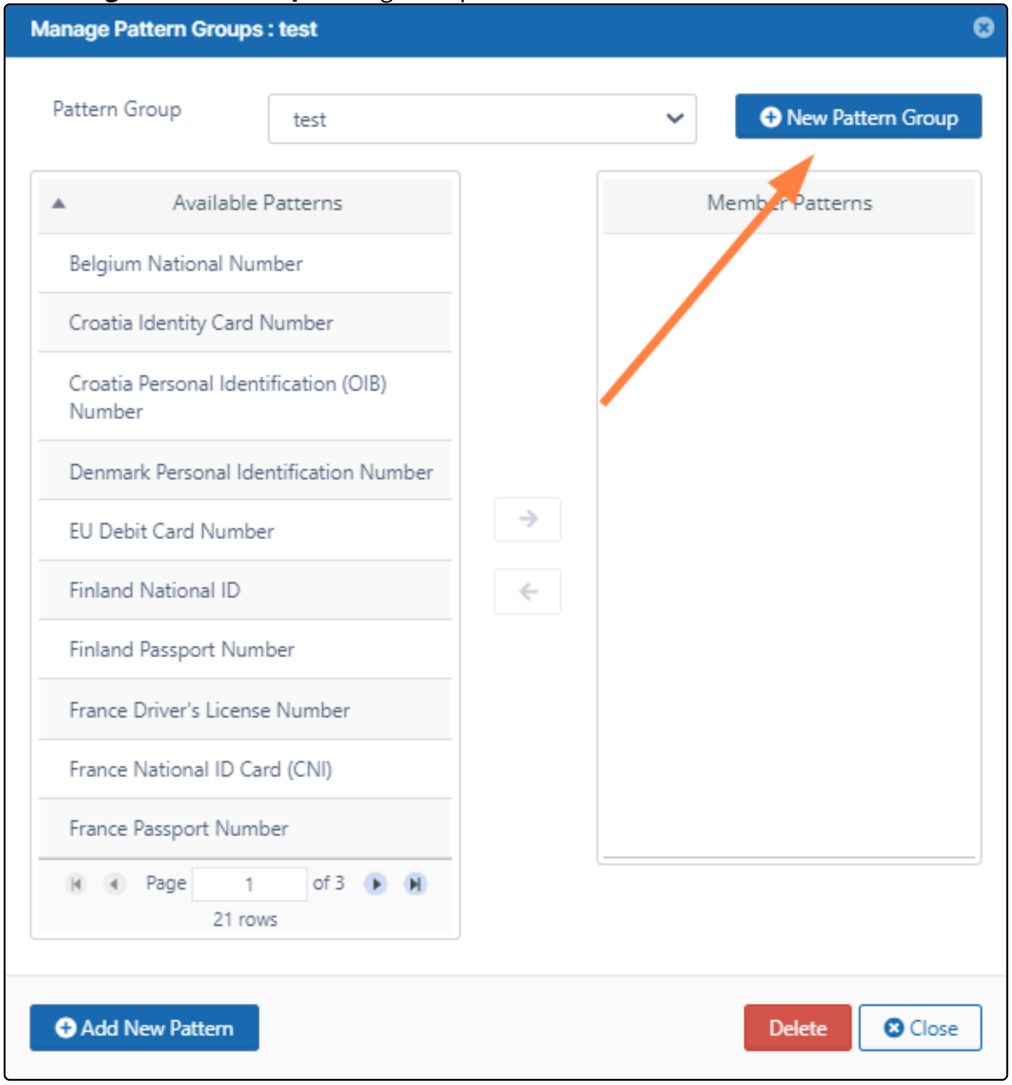
You have determined that the scanned doctor diagnosis notes will have to be tagged with metadata manually, and that smart classification can automatically search for the identifying strings in the medical records and insurance records.

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**.



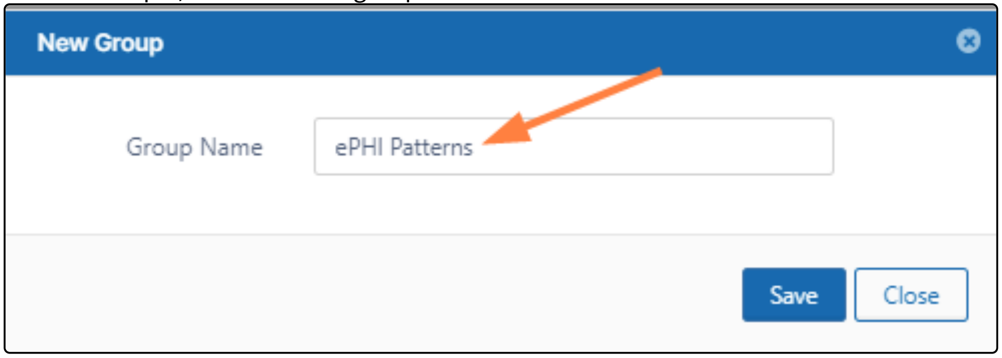
The **Manage Pattern Groups** dialog box opens.



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

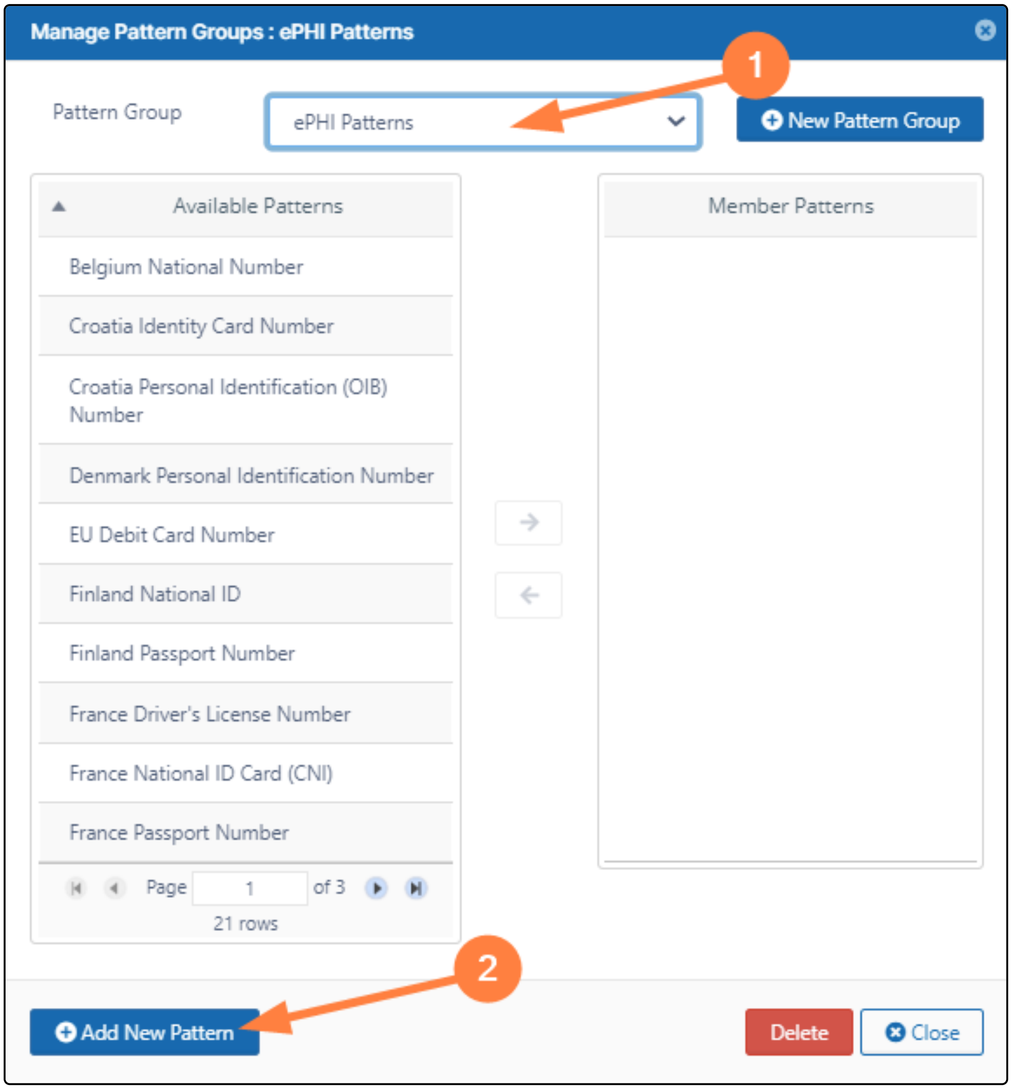
3. Click **New Pattern Group.**
4. For this example, name the new group **ePHI Patterns**.



New Group

Group Name: 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

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

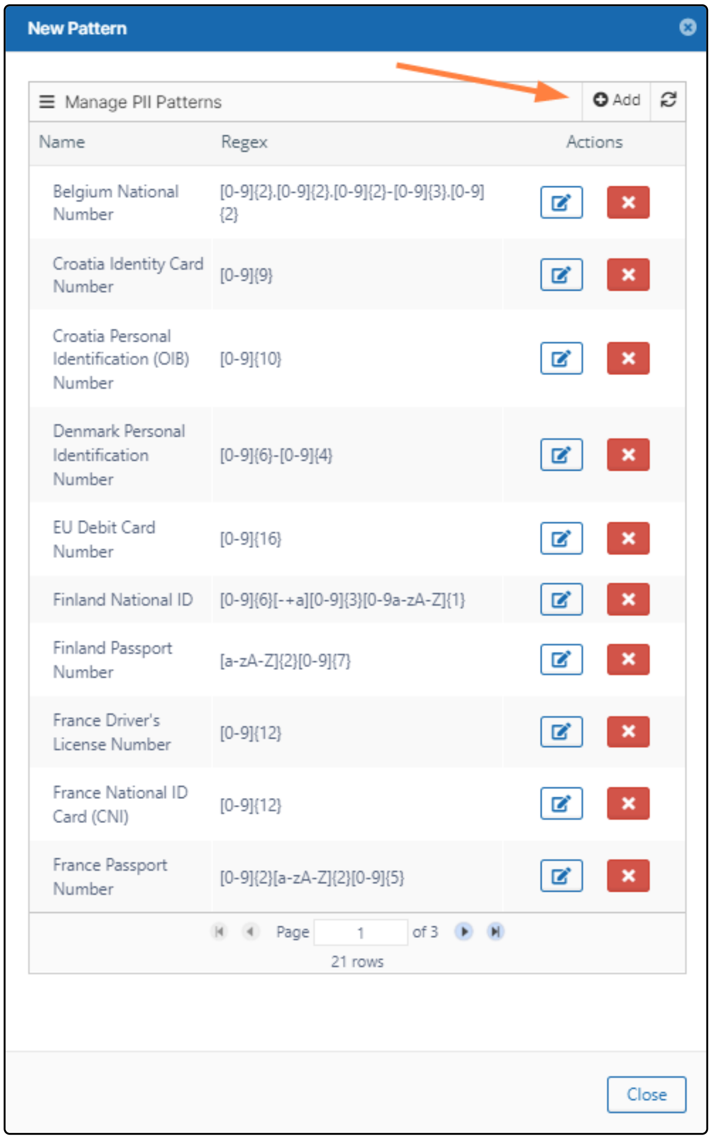
Page 1 of 3

21 rows

Member Patterns

The **New Pattern** dialog box opens.

7. Click **Add**.



New Pattern

☰ Manage PII Patterns

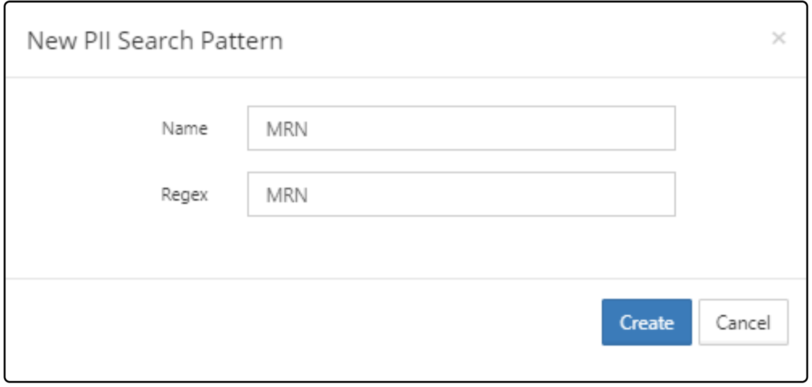
Name	Regex	Actions
Belgium National Number	[0-9]{2}.[0-9]{2}.[0-9]{2}-[0-9]{3}.[0-9]{2}	
Croatia Identity Card Number	[0-9]{9}	
Croatia Personal Identification (OIB) Number	[0-9]{10}	
Denmark Personal Identification Number	[0-9]{6}-[0-9]{4}	
EU Debit Card Number	[0-9]{16}	
Finland National ID	[0-9]{6}[-+a][0-9]{3}[0-9a-zA-Z]{1}	
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 1 of 3

21 rows

The **New PII Search Pattern** dialog box opens.

8. Enter **MRN** in **Name**, and enter **MRN** in **Regex**.



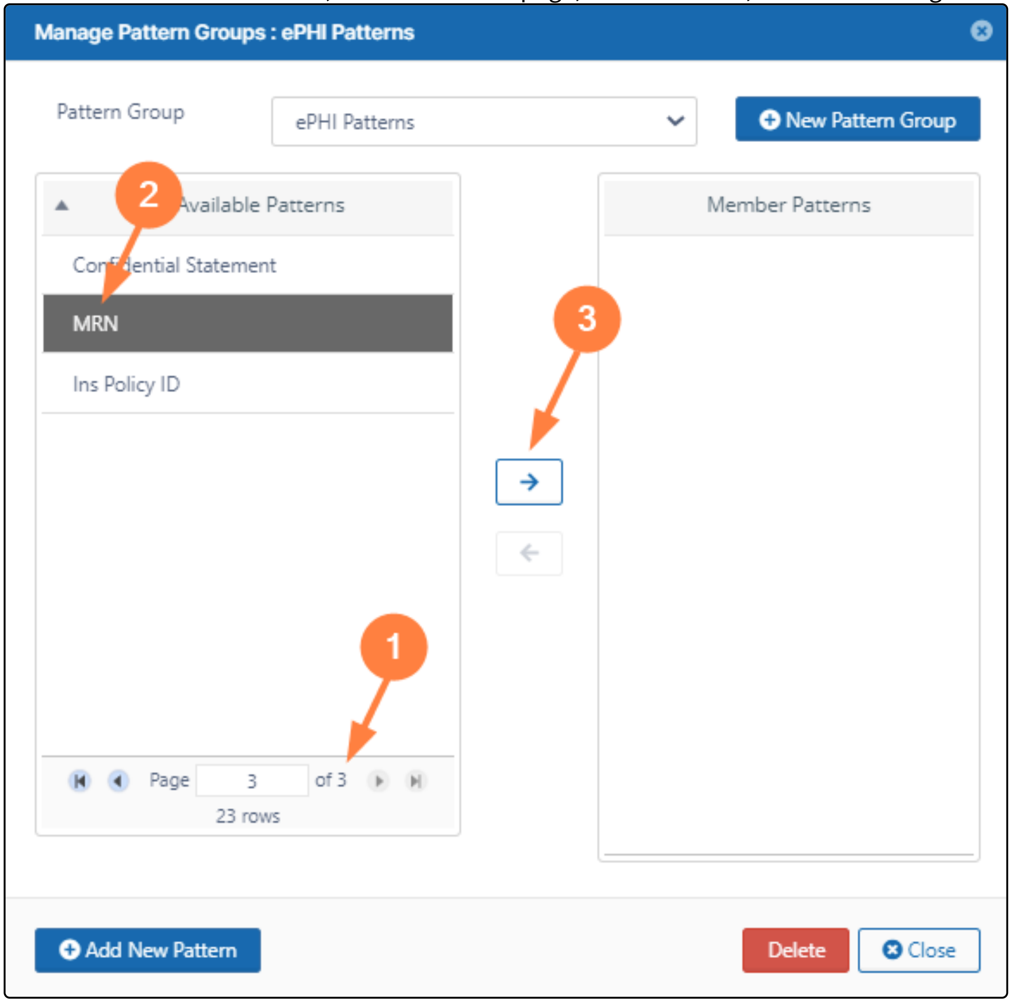
New PII Search Pattern

Name: MRN

Regex: MRN

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.

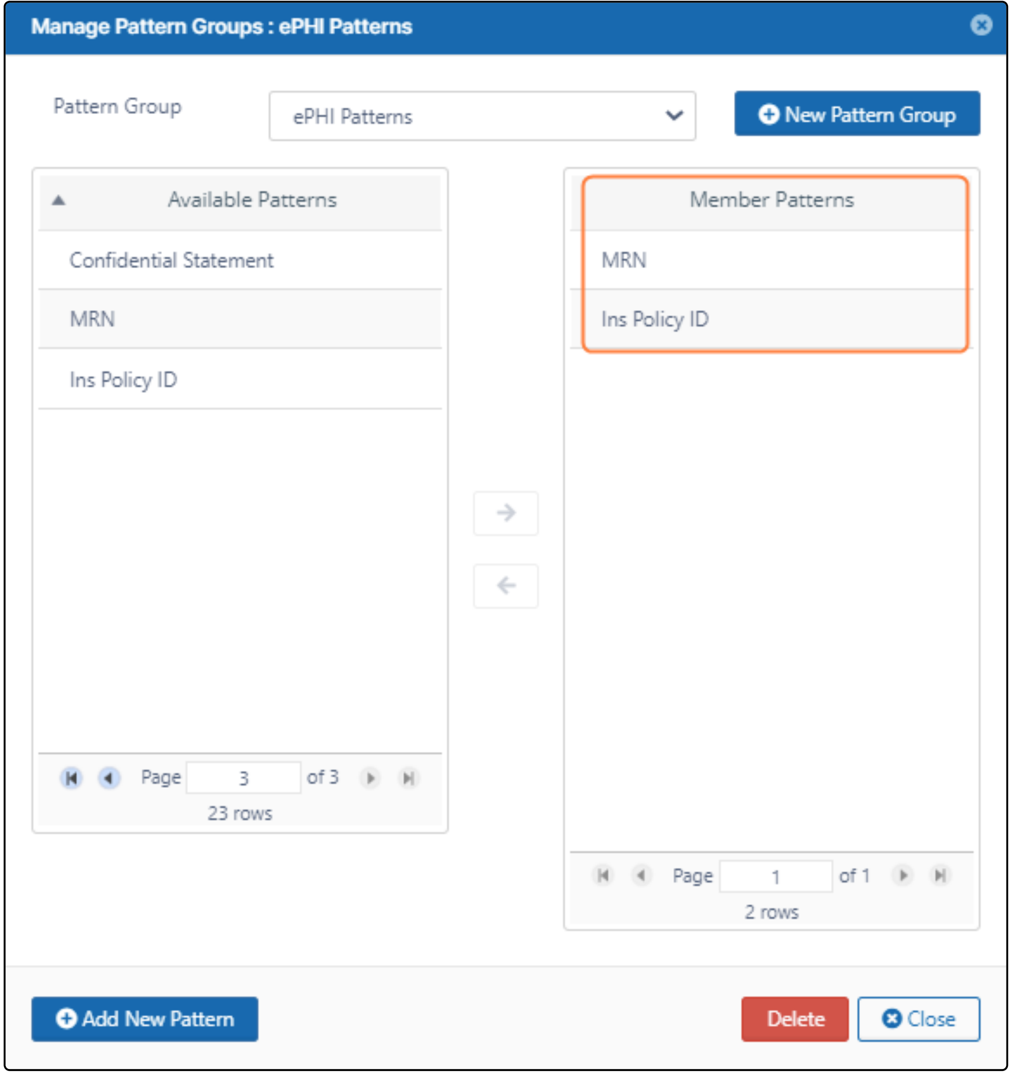


Manage Pattern Groups : ePHI Patterns

Pattern Group: ePHI Patterns

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.



16. Click **Close**.

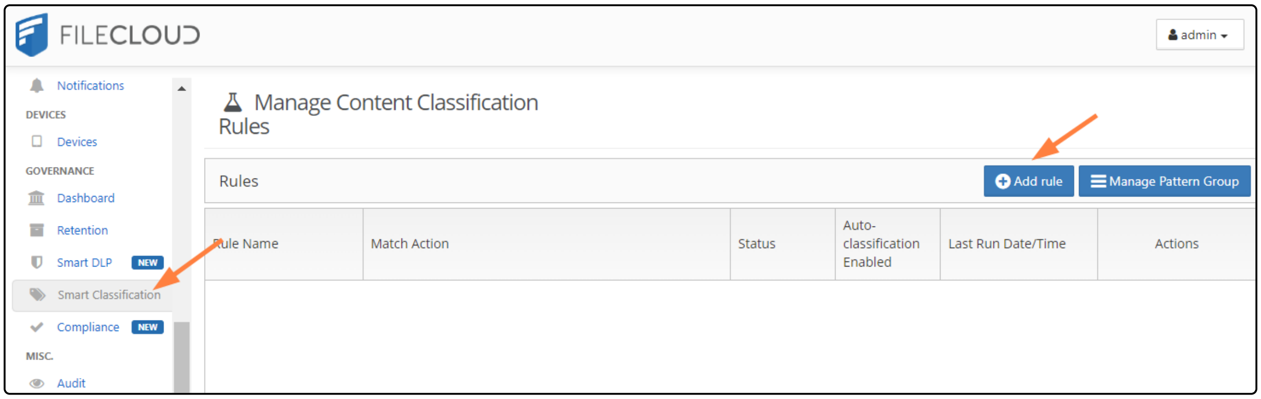
Step 4: Set up a Smart Classification rule to locate and tag ePHI files

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**.



Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions

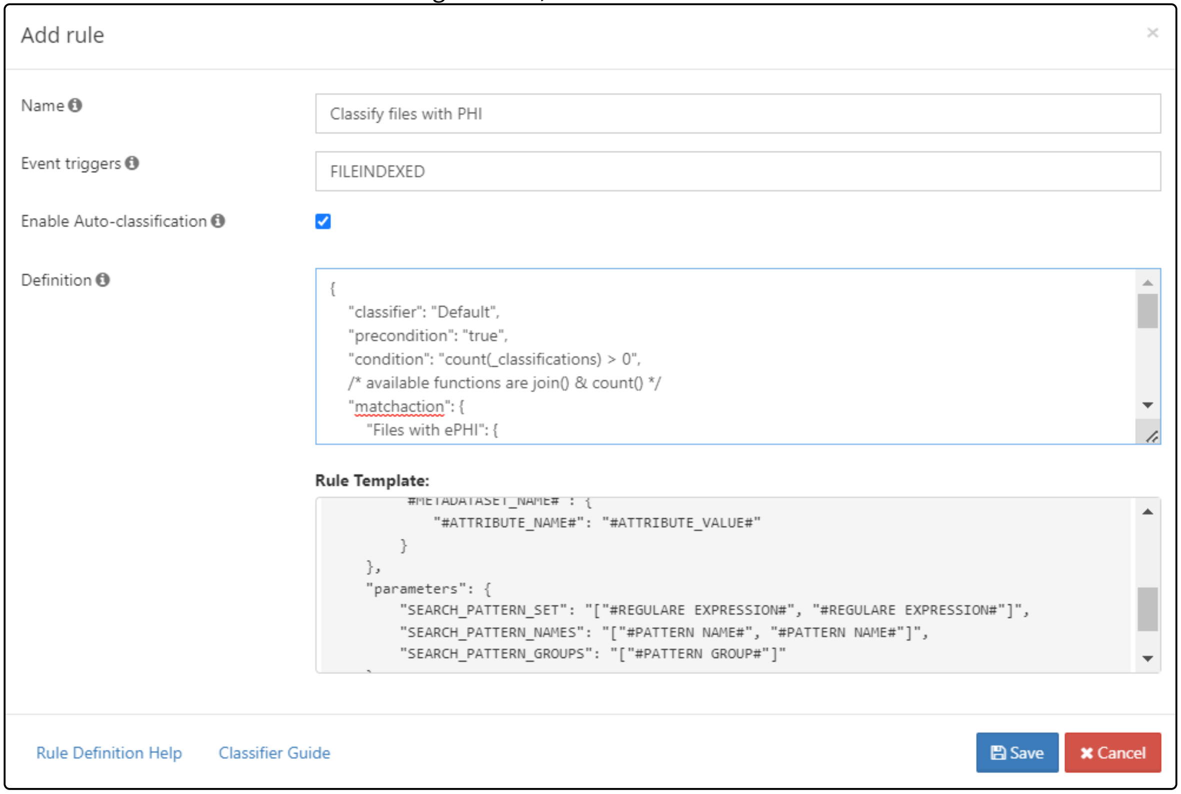
An **Add Rule** dialog box opens.

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**.



Name: Classify files with PHI

Event triggers: FILEINDEXED

Enable Auto-classification: ☑

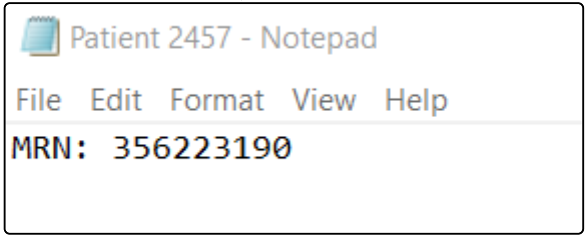
Definition:

```
{
  "classifier": "Default",
  "precondition": "true",
  "condition": "count(_classifications) > 0",
  /* available functions are join() & count() */
  "matchaction": {
    "Files with ePHI": {
```

Rule Template:

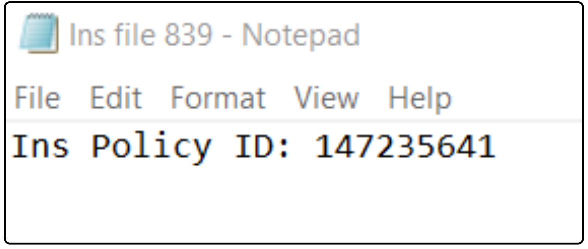
```
          #METADATASET_NAME#": {
              "#ATTRIBUTE_NAME#": "#ATTRIBUTE_VALUE#"
          }
      },
      "parameters": {
          "SEARCH_PATTERN_SET": "["#REGULARE EXPRESSION#", "#REGULARE EXPRESSION#"]",
          "SEARCH_PATTERN_NAMES": "["#PATTERN NAME#", "#PATTERN NAME#"]",
          "SEARCH_PATTERN_GROUPS": "["#PATTERN GROUP#"]"
```

4. Now, test the smart classification rule.
   a. Obtain or create some files that contain the ePHI patterns.
      We include:
      - a test file with an MRN, **Patient 2457.txt**:



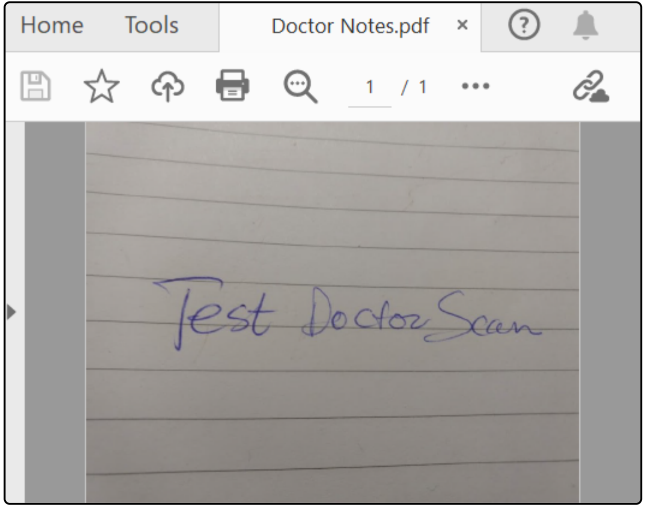
MRN: 356223190

      - a test file with and insurance policy id, **Ins file 839.txt**:



Ins Policy ID: 147235641

- a test scanned handwritten note, **Doctor Notes.pdf**:

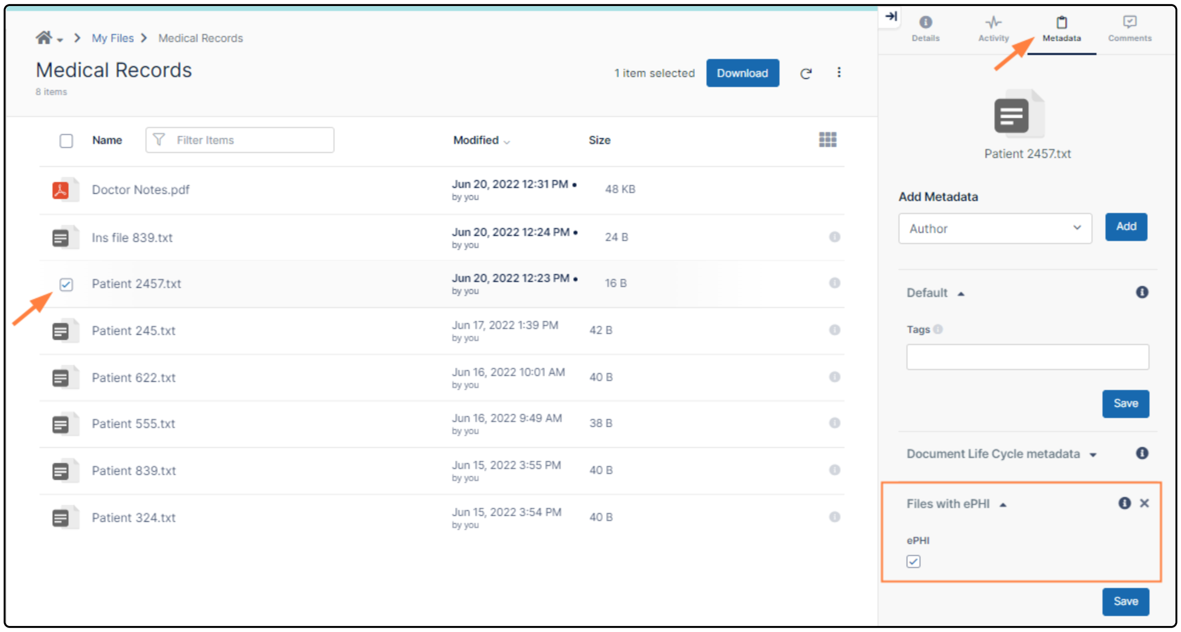


Test Doctor Scan

b. Log in to the FileCloud user portal as the user you gave permissions to read and write the **Files with ePHI** metadata.

c. Upload the files into FileCloud.

d. 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.



Medical Records

8 items

	Name	Modified	Size
	Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
	Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
☑	Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
	Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
	Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
	Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
	Patient 839.txt	Jun 15, 2022 3:55 PM by you	40 B
	Patient 324.txt	Jun 15, 2022 3:54 PM by you	40 B

Patient 2457.txt

Add Metadata

Author [Add]

Default

Tags

[Save]

Document Life Cycle metadata

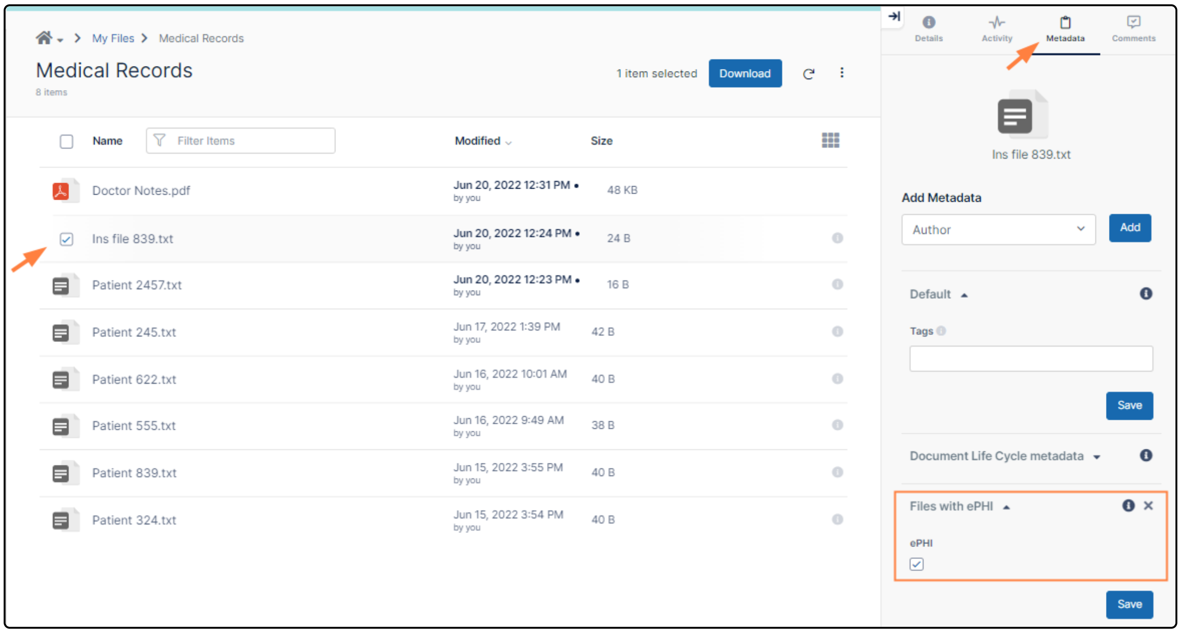
Files with ePHI

ePHI

☑

[Save]

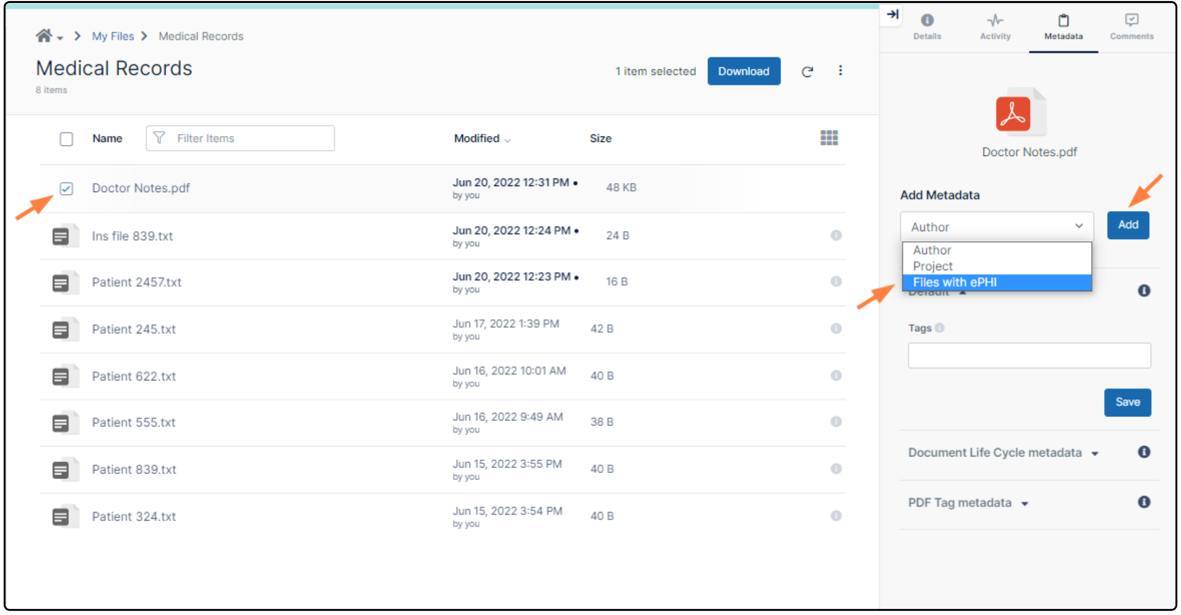
e. Then check the checkbox for the file **Ins file 839.txt**, and click **Metadata** in the details pane. Confirm that **Files with ePHI** is listed and that the **ePHI** metadata attribute is checked.



Name	Modified	Size
Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
☑ Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM by you	40 B
Patient 324.txt	Jun 15, 2022 3:54 PM by you	40 B

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.

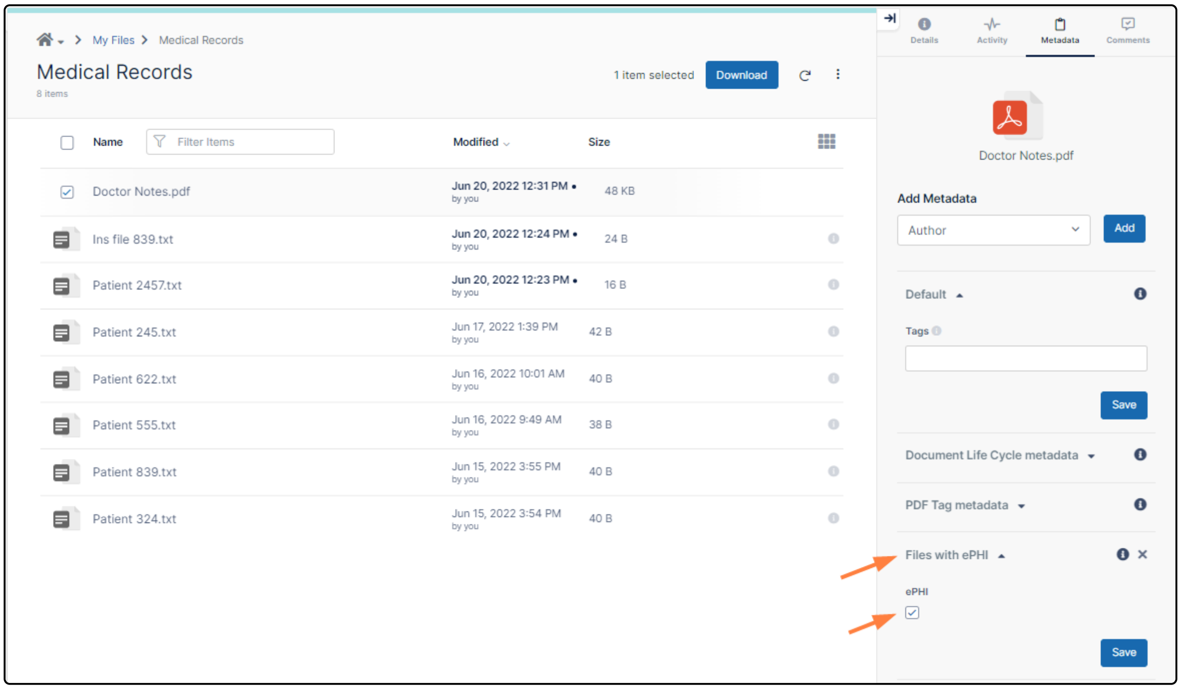
g. In the **Add Metadata** drop-down list, choose **Files with ePHI** and click **Add**.



Name	Modified	Size
☑ Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM by you	40 B
Patient 324.txt	Jun 15, 2022 3:54 PM by you	40 B

Files with ePHI is added to the list of included metadata.

h. Check **ePHI** to indicate that the file has ePHI.



Medical Records
8 items

Name	Modified	Size
☑ Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM by you	40 B
Patient 324.txt	Jun 15, 2022 3:54 PM by you	40 B

Doctor Notes.pdf

Add Metadata: Author — Add

Default
Tags
Save

Document Life Cycle metadata

PDF Tag metadata

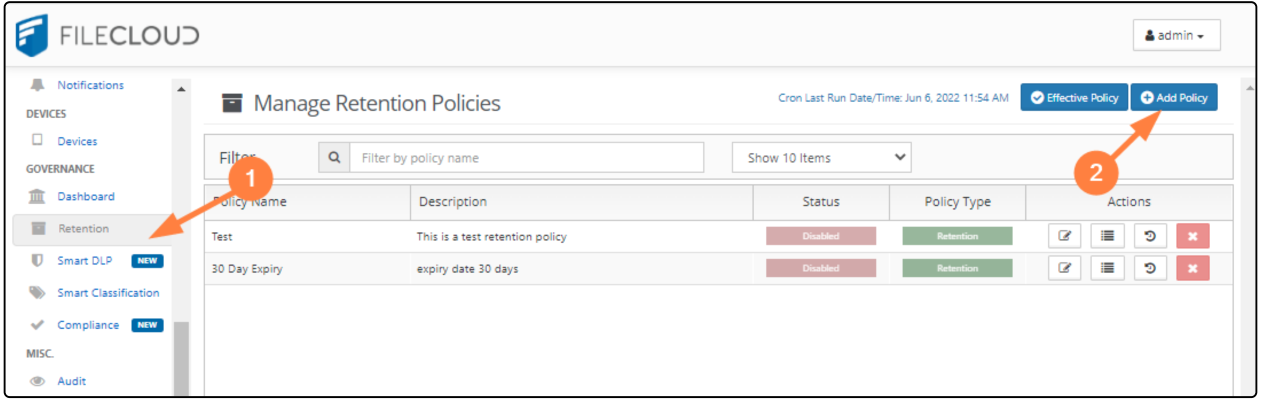
Files with ePHI
ePHI ☑
Save

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**.



Manage Retention Policies

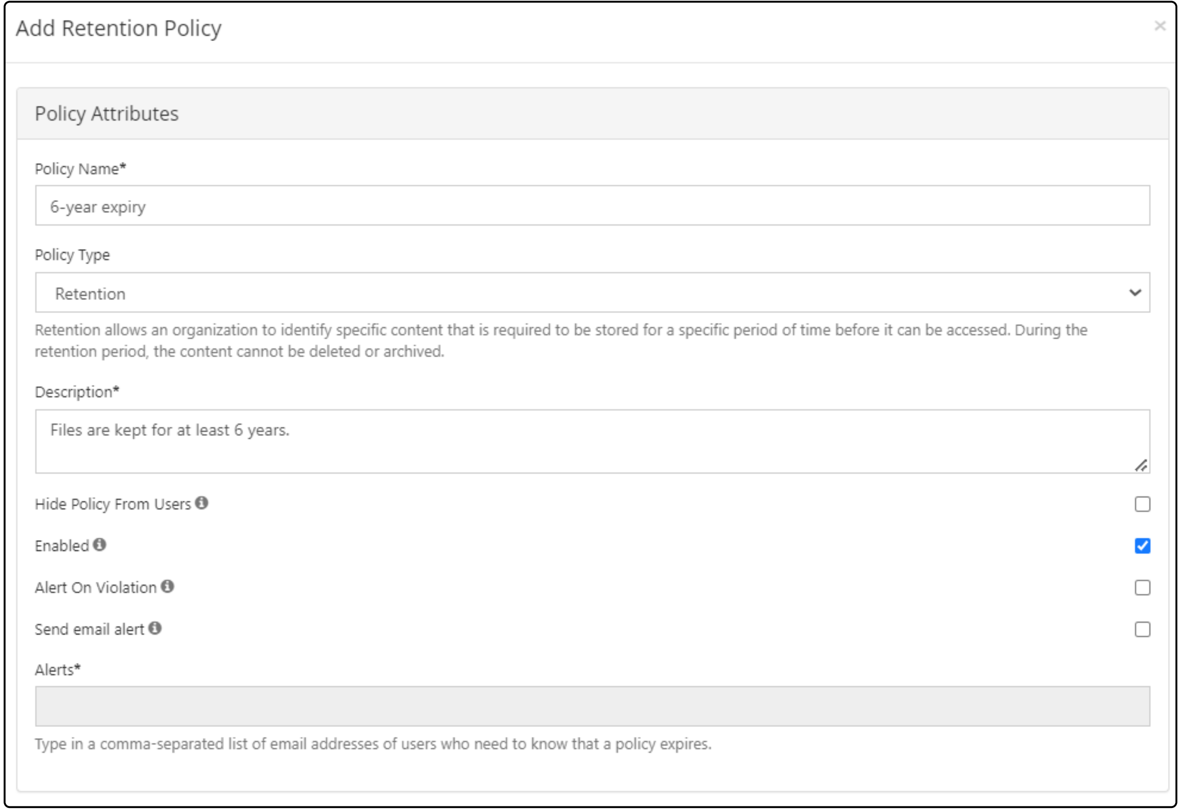
Cron Last Run Date/Time: Jun 6, 2022 11:54 AM

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	

   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.

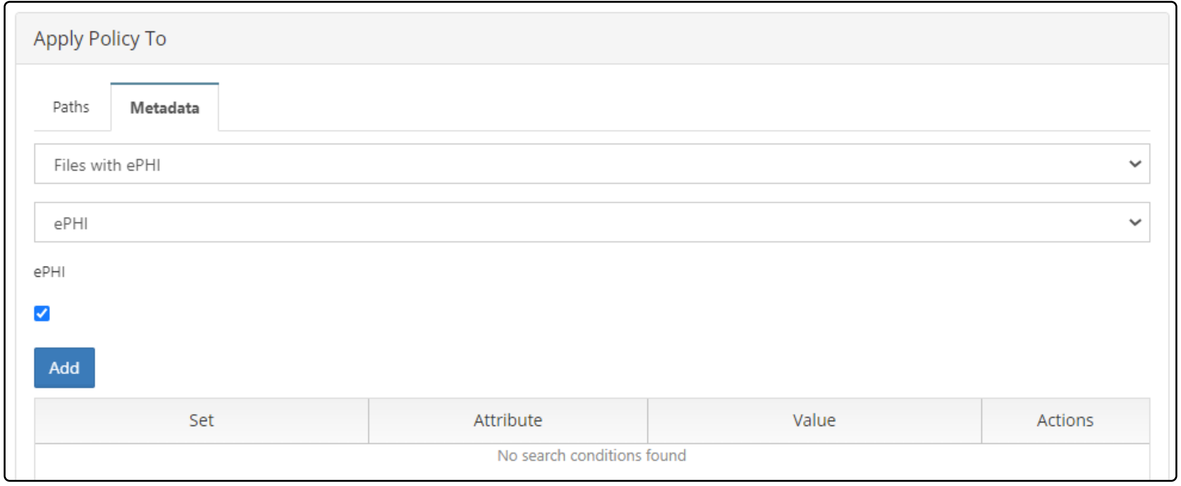
4. Add the metadata condition to the **Apply Policy To** section:

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

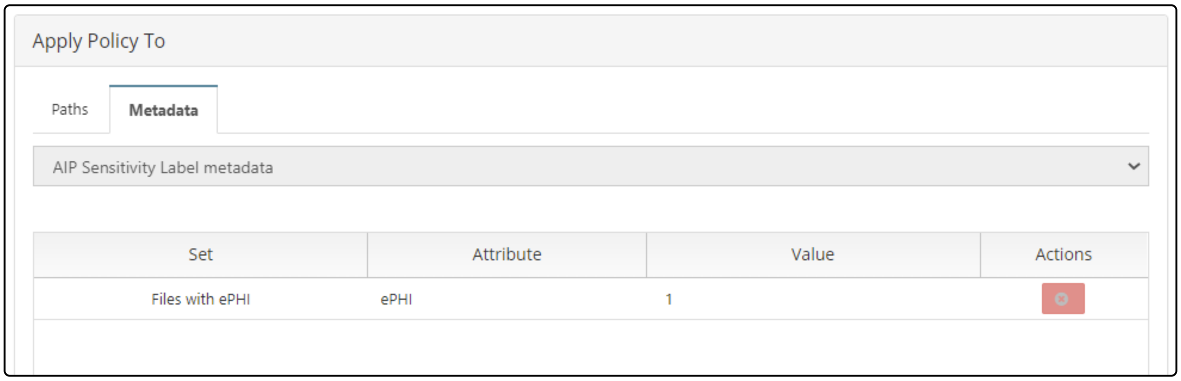
ePHI

☑

Add

Set	Attribute	Value	Actions
No search conditions found			

e. Click **Add**.
The condition is added:



Apply Policy To

AIP Sensitivity Label metadata

Set	Attribute	Value	Actions
Files with ePHI	ePHI	1	⊗

5. Fill out the **Actions** section.

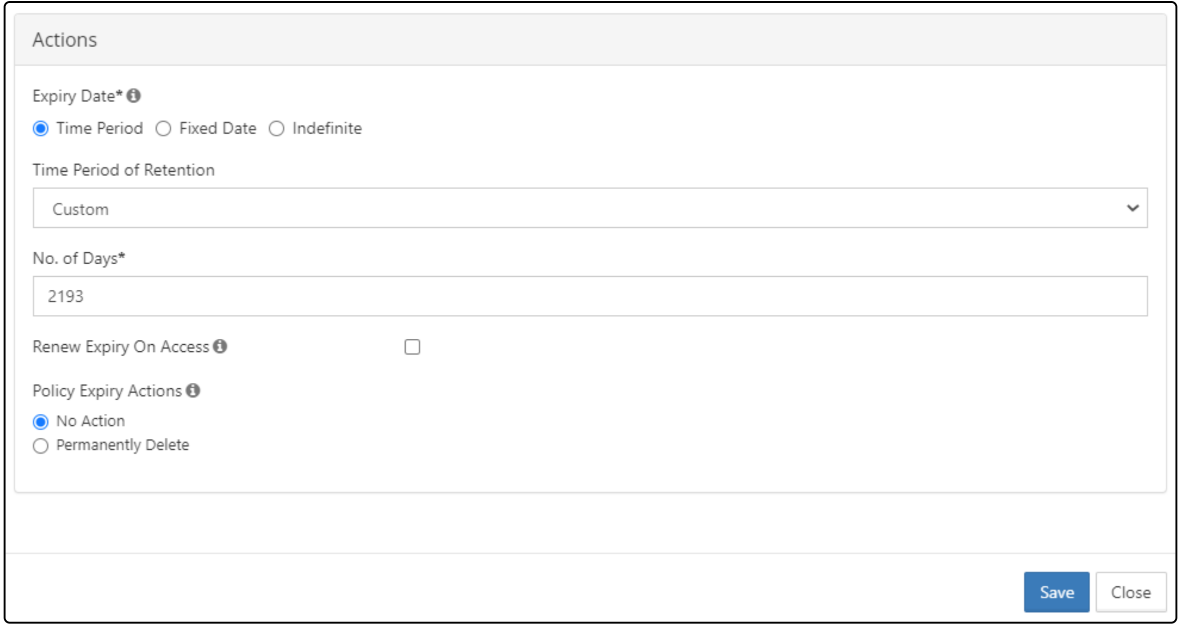
a. Leave **Time Period** selected.

b. In **Time Period of Retention** choose custom so you can set a period that is more than 6 years.

c. The time period required in rule 164.316(b)(2)(i) 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).

d. Uncheck **Renew Expiry on Access** since the HIPAA rule requires that the records be saved 6 years after creation, not 6 years after access.

e. 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.



Actions

Expiry Date*
● Time Period ○ Fixed Date ○ Indefinite

Time Period of Retention
Custom

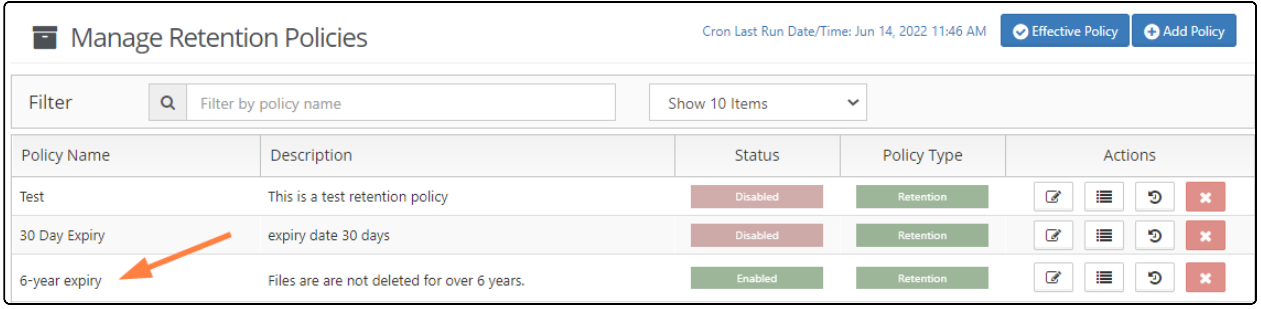
No. of Days*
2193

Renew Expiry On Access □

Policy Expiry Actions
● No Action
○ Permanently Delete

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.



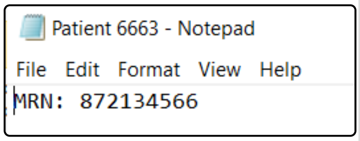
Manage Retention Policies

Cron Last Run Date/Time: Jun 14, 2022 11:46 AM

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 are not deleted for over 6 years.	Enabled	Retention	✎ ☰ ↺ ✖

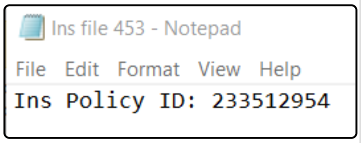
7. Now test the retention policy.
   a. Obtain some files with ePHI content, like the ones you used for testing in Step 4.
   Our examples include the content **MRN** and **Ins Policy ID**, and a scanned file that must be tagged manually:

Patient 6663.txt



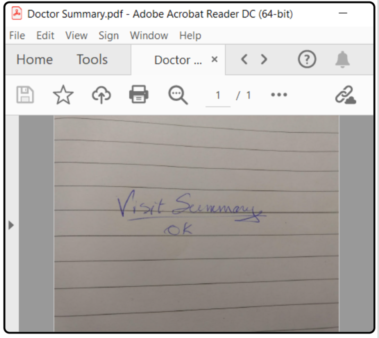
```
MRN: 872134566
```

Ins file 453.txt



```
Ins Policy ID: 233512954
```

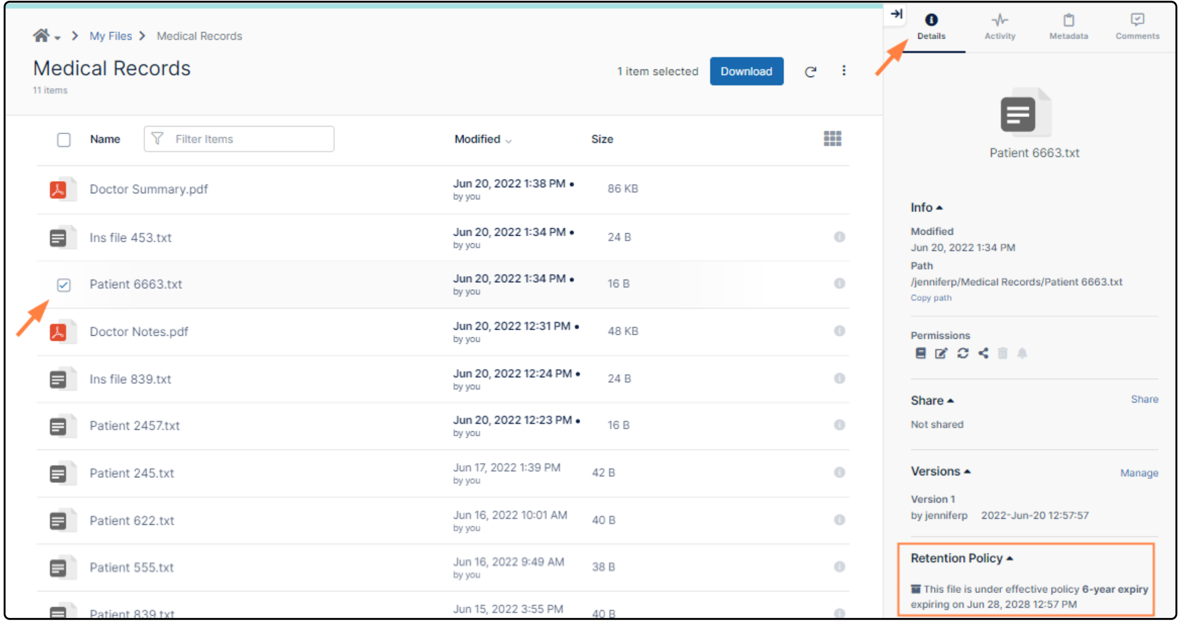
Doctor Summary.pdf



Doctor Summary.pdf - Adobe Acrobat Reader DC (64-bit)
File Edit View Sign Window Help
Home Tools Doctor ... ×
1 / 1
Visit Summary
ok

   b. Log in to the user portal as the user you gave permissions to read and write the **Files with ePHI** metadata.
   c. Upload the files into FileCloud.

d. 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.



Medical Records
11 items

Name	Modified	Size
Doctor Summary.pdf	Jun 20, 2022 1:38 PM • by you	86 KB
Ins file 453.txt	Jun 20, 2022 1:34 PM • by you	24 B
☑ Patient 6663.txt	Jun 20, 2022 1:34 PM • by you	16 B
Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM	40 B

Patient 6663.txt

Info
Modified
Jun 20, 2022 1:34 PM
Path
/jenniferp/Medical Records/Patient 6663.txt
Copy path

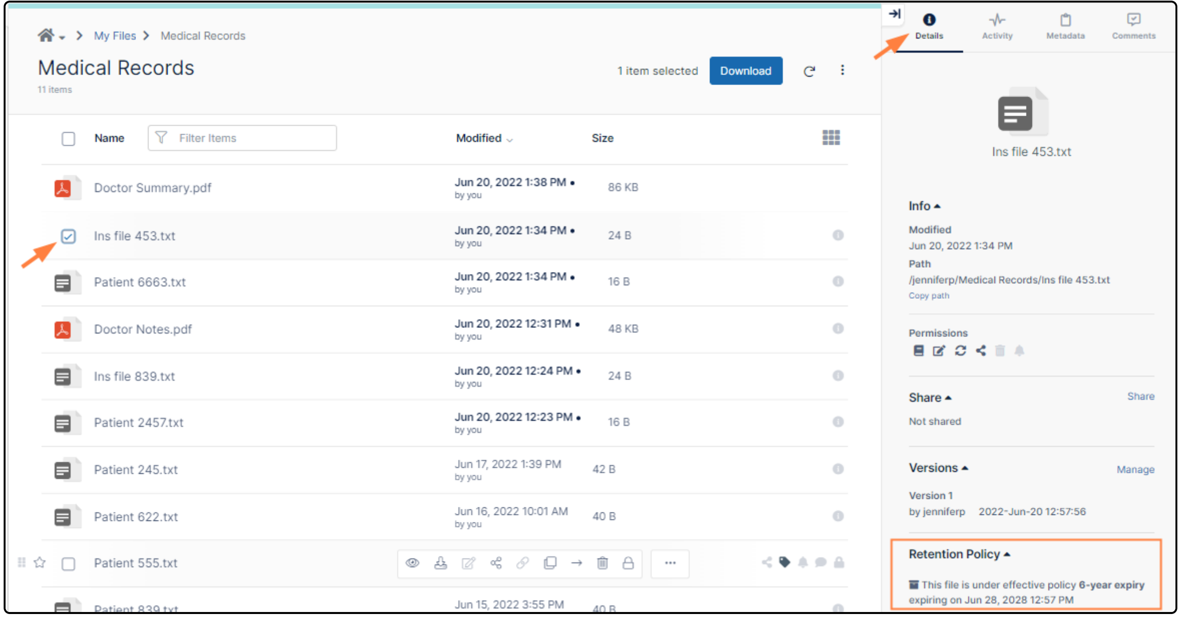
Permissions

Share Share
Not shared

Versions Manage
Version 1
by jenniferp 2022-Jun-20 12:57:57

Retention Policy
This file is under effective policy **6-year expiry** expiring on Jun 28, 2028 12:57 PM

e. 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.



Medical Records
11 items

Name	Modified	Size
Doctor Summary.pdf	Jun 20, 2022 1:38 PM • by you	86 KB
☑ Ins file 453.txt	Jun 20, 2022 1:34 PM • by you	24 B
Patient 6663.txt	Jun 20, 2022 1:34 PM • by you	16 B
Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
□ Patient 555.txt		
Patient 839.txt	Jun 15, 2022 3:55 PM	40 B

Ins file 453.txt

Info
Modified
Jun 20, 2022 1:34 PM
Path
/jenniferp/Medical Records/Ins file 453.txt
Copy path

Permissions

Share Share
Not shared

Versions Manage
Version 1
by jenniferp 2022-Jun-20 12:57:56

Retention Policy
This file is under effective policy **6-year expiry** expiring on Jun 28, 2028 12:57 PM

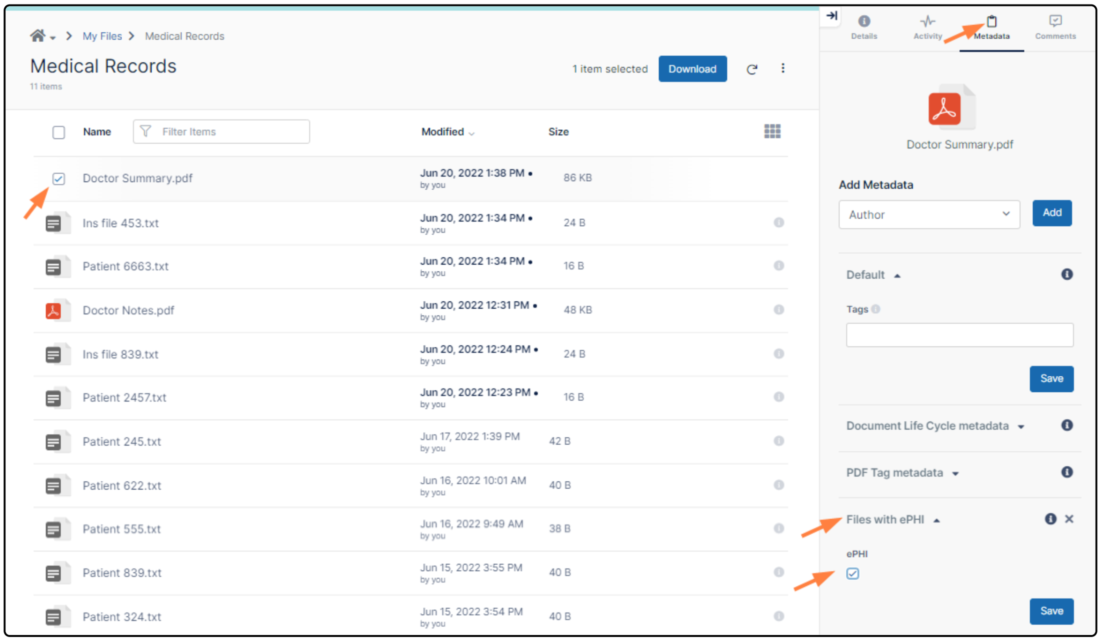
f. Next, select the file **Doctor Summary.pdf**. It does not have a retention policy attached to it yet because you have not manually added an **ePHI** metadata tag yet.

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.



My Files > Medical Records

Medical Records
11 items

1 item selected Download

Name	Modified	Size
☑ Doctor Summary.pdf	Jun 20, 2022 1:38 PM • by you	86 KB
Ins file 453.txt	Jun 20, 2022 1:34 PM • by you	24 B
Patient 6663.txt	Jun 20, 2022 1:34 PM • by you	16 B
Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM by you	40 B
Patient 324.txt	Jun 15, 2022 3:54 PM by you	40 B

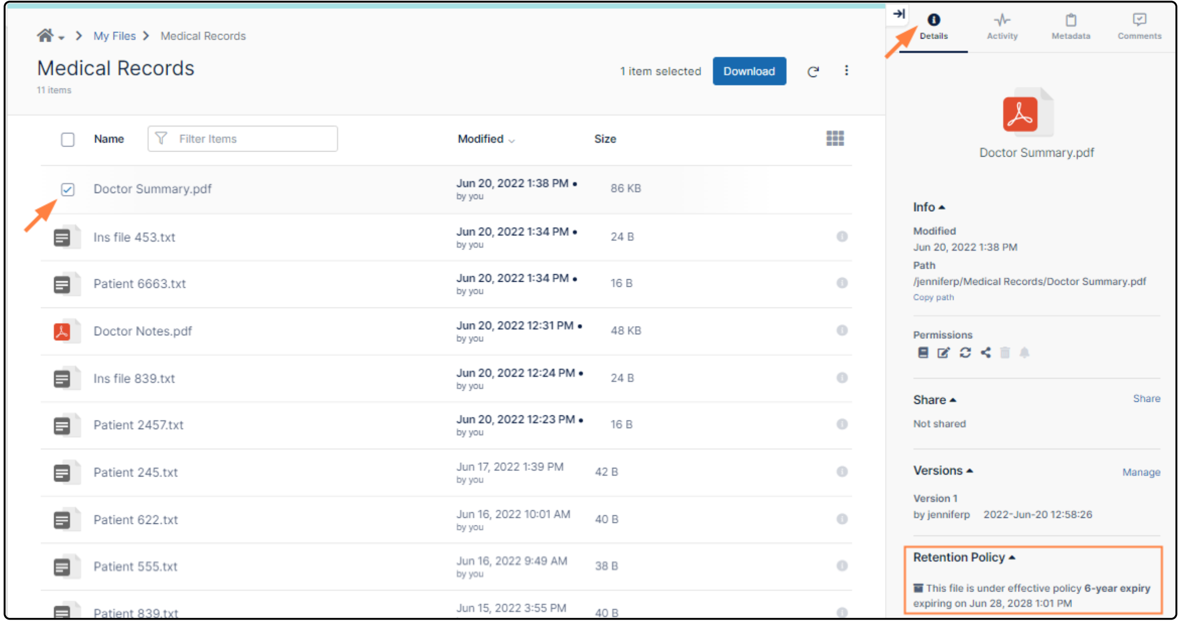
Doctor Summary.pdf

Add Metadata
Author Add

Default
Tags
Save

Document Life Cycle metadata
PDF Tag metadata
Files with ePHI
ePHI
☑
Save

i. Click the **Details** tab.
j. Confirm that the retention policy is now listed at the bottom of the details.



My Files > Medical Records

Medical Records
11 items

1 item selected Download

Name	Modified	Size
☑ Doctor Summary.pdf	Jun 20, 2022 1:38 PM • by you	86 KB
Ins file 453.txt	Jun 20, 2022 1:34 PM • by you	24 B
Patient 6663.txt	Jun 20, 2022 1:34 PM • by you	16 B
Doctor Notes.pdf	Jun 20, 2022 12:31 PM • by you	48 KB
Ins file 839.txt	Jun 20, 2022 12:24 PM • by you	24 B
Patient 2457.txt	Jun 20, 2022 12:23 PM • by you	16 B
Patient 245.txt	Jun 17, 2022 1:39 PM by you	42 B
Patient 622.txt	Jun 16, 2022 10:01 AM by you	40 B
Patient 555.txt	Jun 16, 2022 9:49 AM by you	38 B
Patient 839.txt	Jun 15, 2022 3:55 PM	40 B

Doctor Summary.pdf

Info
Modified
Jun 20, 2022 1:38 PM
Path
/jenniferp/Medical Records/Doctor Summary.pdf
Copy path

Permissions

Share Share
Not shared

Versions Manage
Version 1
by jenniferp 2022-Jun-20 12:58:26

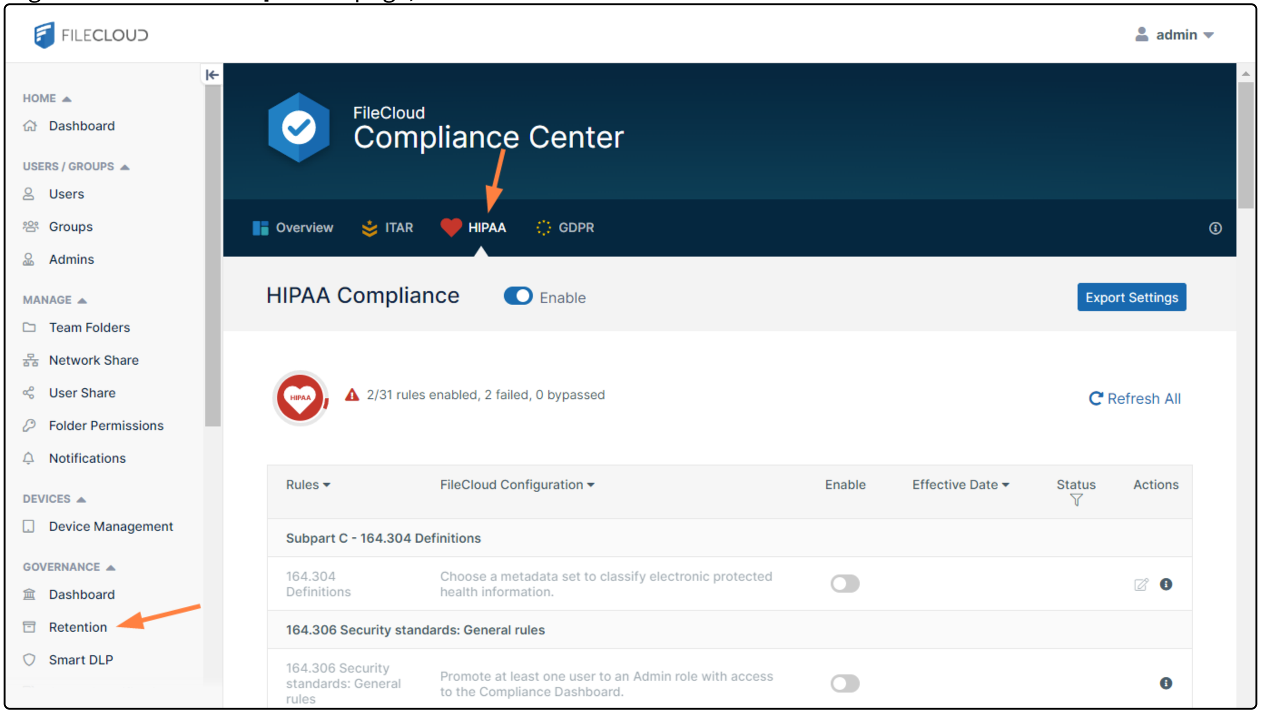
Retention Policy
This file is under effective policy **6-year expiry** expiring on Jun 28, 2028 1:01 PM

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.

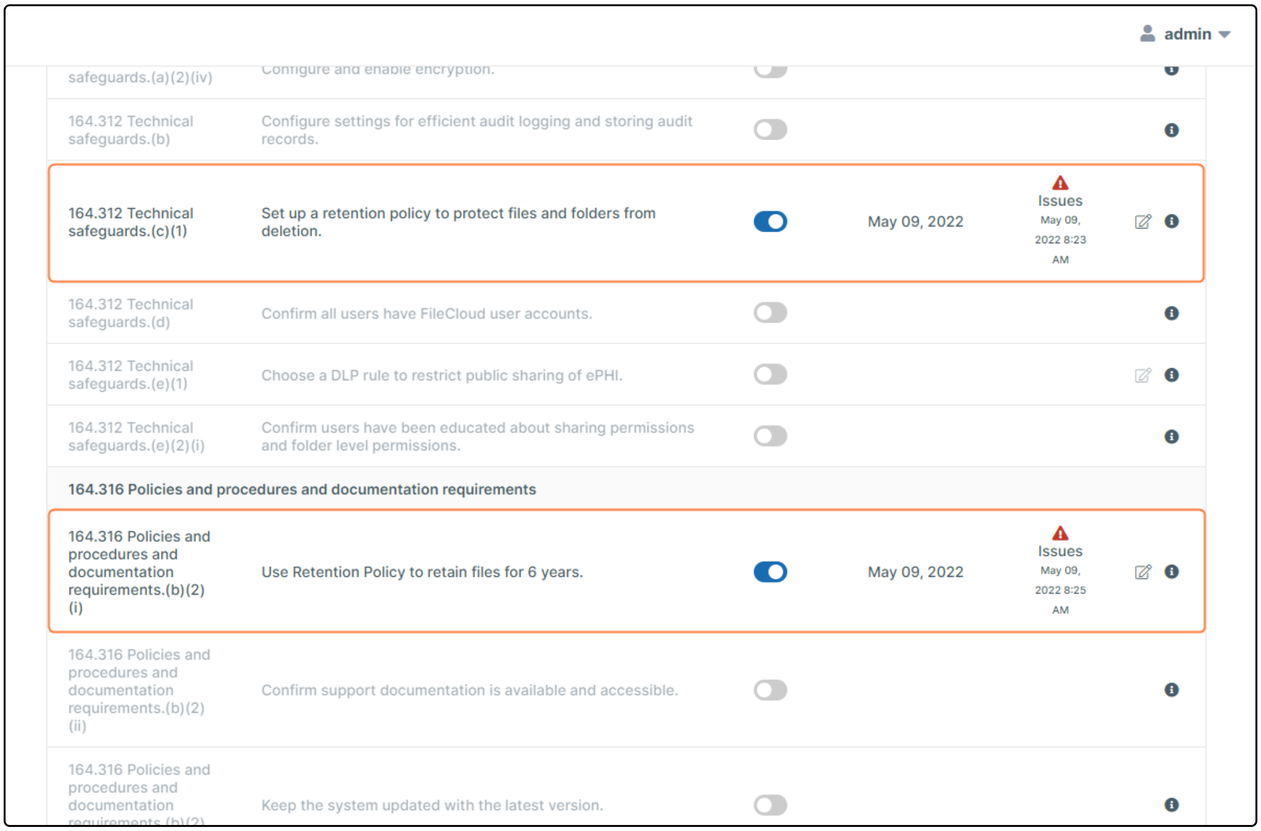


2/31 rules enabled, 2 failed, 0 bypassed

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.				
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.				

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 associated with them, they

both fail.

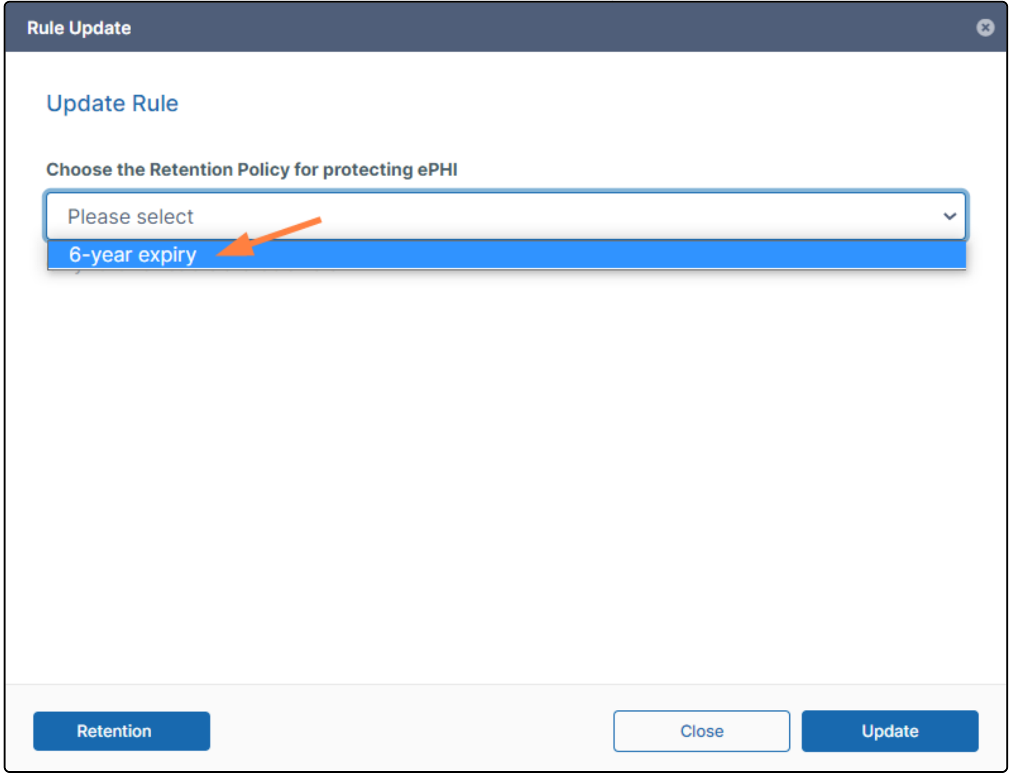


admin

safeguards.(a)(2)(iv)	Configure and enable encryption.	○			
164.312 Technical safeguards.(b)	Configure settings for efficient audit logging and storing audit records.	○			
164.312 Technical safeguards.(c)(1)	Set up a retention policy to protect files and folders from deletion.	●	May 09, 2022	Issues May 09, 2022 8:23 AM	
164.312 Technical safeguards.(d)	Confirm all users have FileCloud user accounts.	○			
164.312 Technical safeguards.(e)(1)	Choose a DLP rule to restrict public sharing of ePHI.	○			
164.312 Technical safeguards.(e)(2)(i)	Confirm users have been educated about sharing permissions and folder level permissions.	○			
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.	●	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.	○			
164.316 Policies and procedures and documentation requirements.(b)(2)	Keep the system updated with the latest version.	○			

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.



Rule Update

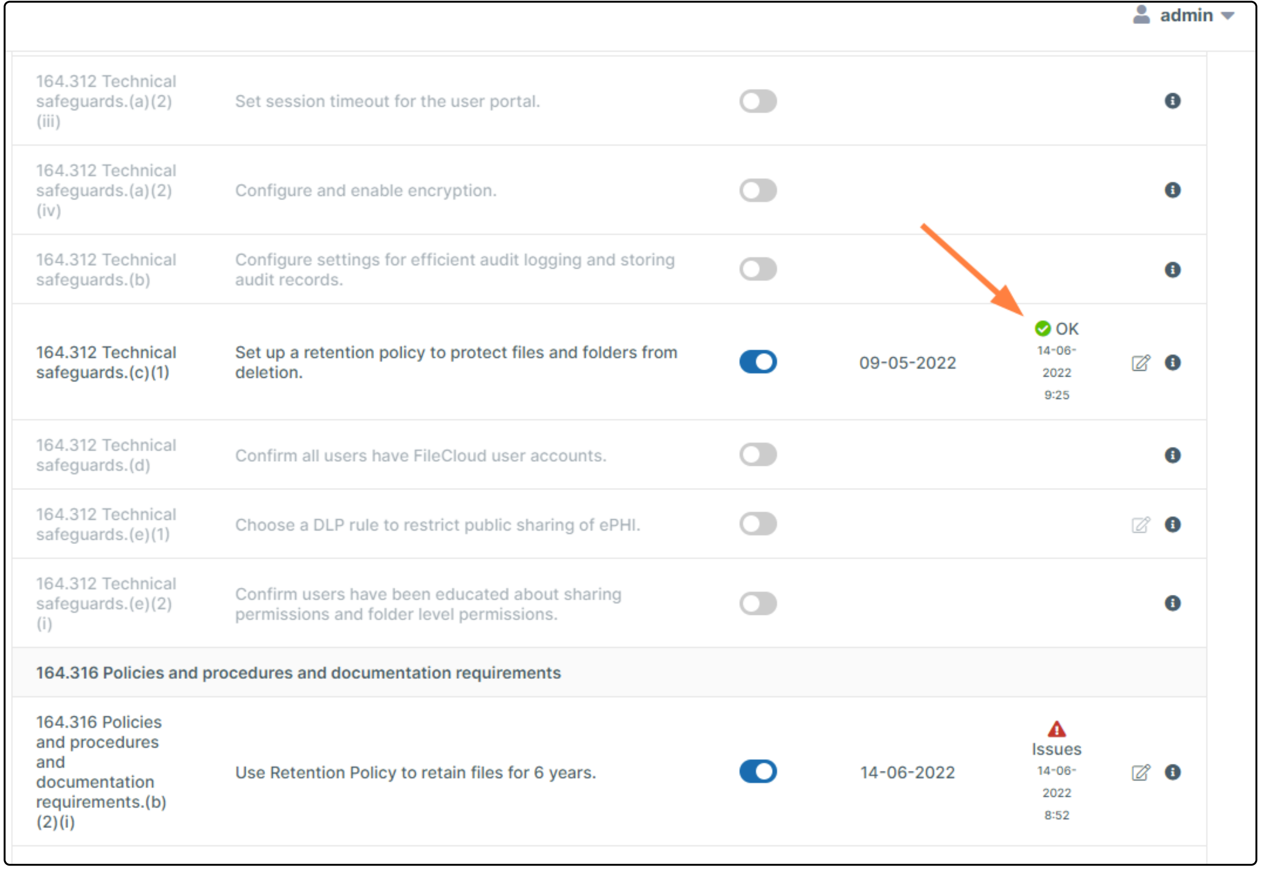
Update Rule

Choose the Retention Policy for protecting ePHI

Please select

6-year expiry

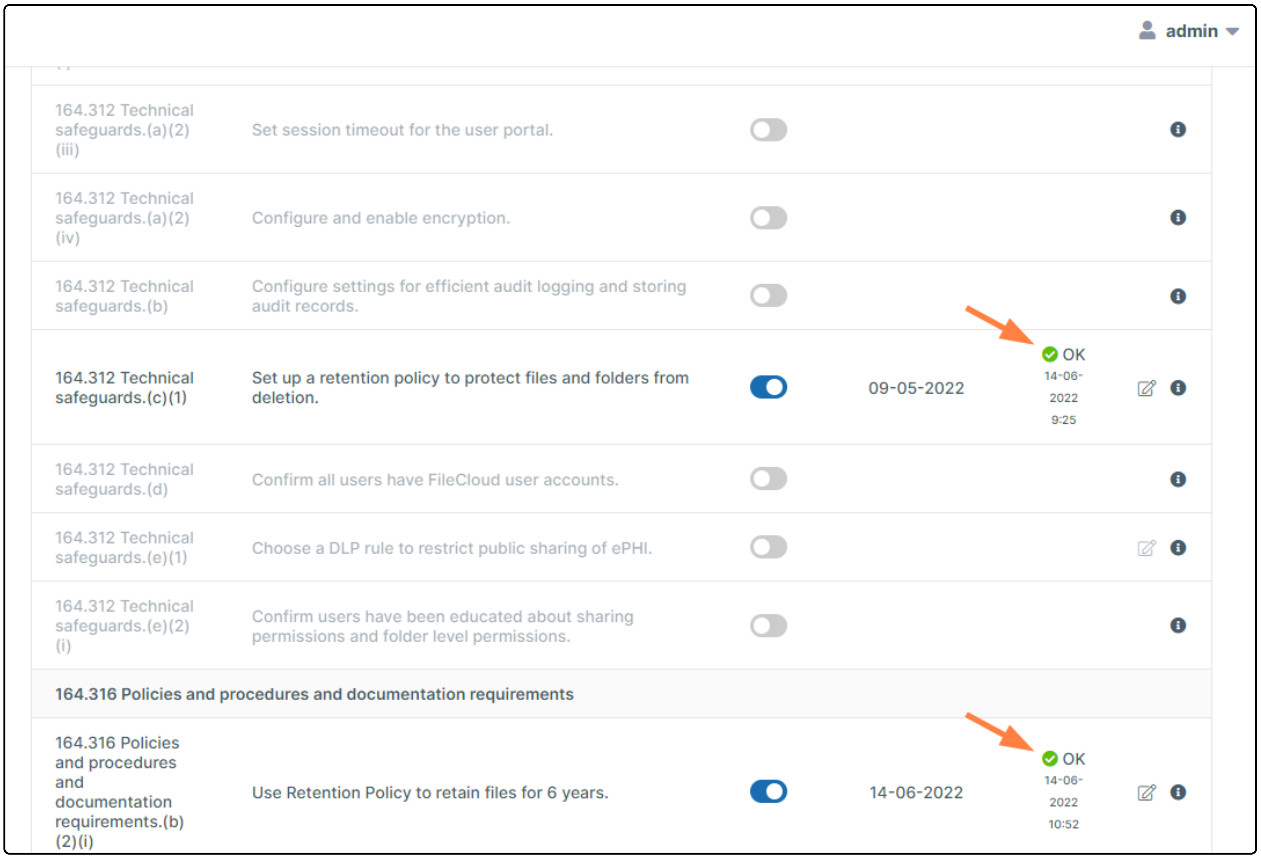
6. Click **Update**.
   The rule now passes.



admin

164.312 Technical safeguards.(a)(2)(iii)	Set session timeout for the user portal.	○			ⓘ
164.312 Technical safeguards.(a)(2)(iv)	Configure and enable encryption.	○			ⓘ
164.312 Technical safeguards.(b)	Configure settings for efficient audit logging and storing audit records.	○			ⓘ
164.312 Technical safeguards.(c)(1)	Set up a retention policy to protect files and folders from deletion.	●	09-05-2022	✓ OK 14-06-2022 9:25	✎ ⓘ
164.312 Technical safeguards.(d)	Confirm all users have FileCloud user accounts.	○			ⓘ
164.312 Technical safeguards.(e)(1)	Choose a DLP rule to restrict public sharing of ePHI.	○			✎ ⓘ
164.312 Technical safeguards.(e)(2)(i)	Confirm users have been educated about sharing permissions and folder level permissions.	○			ⓘ
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.	●	14-06-2022	⚠ Issues 14-06-2022 8:52	✎ ⓘ

7. Now edit rule **164.316 (b)(2)(i)**, and choose the same retention policy.
   Both rules now pass:

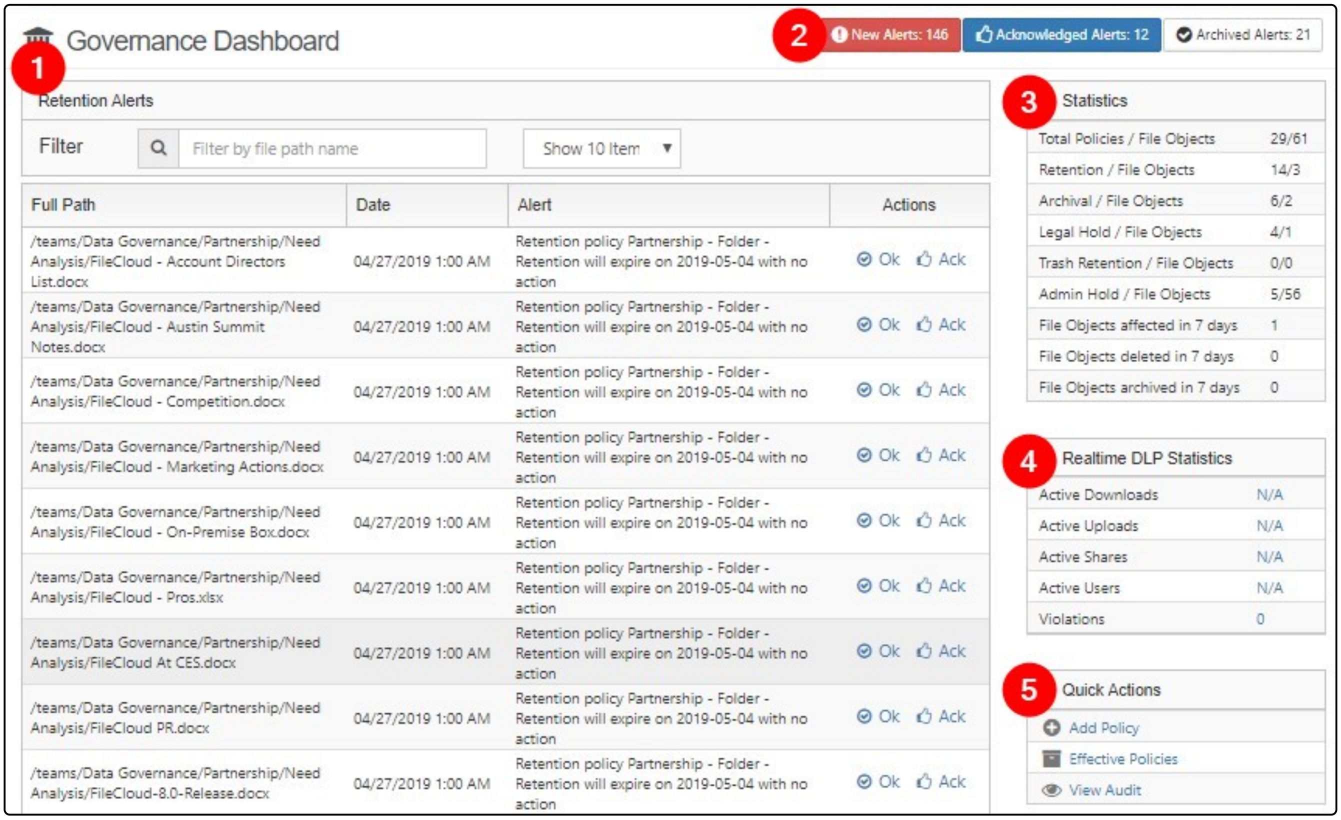


164.312 Technical safeguards.(a)(2)(iii)	Set session timeout for the user portal.	○			
164.312 Technical safeguards.(a)(2)(iv)	Configure and enable encryption.	○			
164.312 Technical safeguards.(b)	Configure settings for efficient audit logging and storing audit records.	○			
164.312 Technical safeguards.(c)(1)	Set up a retention policy to protect files and folders from deletion.	●	09-05-2022	✓ OK 14-06-2022 9:25	
164.312 Technical safeguards.(d)	Confirm all users have FileCloud user accounts.	○			
164.312 Technical safeguards.(e)(1)	Choose a DLP rule to restrict public sharing of ePHI.	○			
164.312 Technical safeguards.(e)(2)(i)	Confirm users have been educated about sharing permissions and folder level permissions.	○			
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.	●	14-06-2022	✓ OK 14-06-2022 10:52	

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 and violations of DLP rules.



Governance Dashboard

New Alerts: 146 | Acknowledged Alerts: 12 | Archived Alerts: 21

Retention Alerts

Filter | Filter by file path name | Show 10 Item ▾

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	Ok 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	Ok 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	Ok 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	Ok 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	Ok 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	Ok 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	Ok 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	Ok 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	Ok 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

- Add Policy
- Effective Policies
- View Audit

1) Retention Alerts	Lists current alerts for files and folders that have retention policies added to them. To the right of an alert: • Click **OK** to archive the alert and move it to the **Archived Alerts** listing. • Click **Ack** to acknowledge the alert and move it to the **Acknowledged Alerts** listing.
2) Alert type buttons	Clicking each button displays a list of the alert type (**New**, **Acknowledged**, or **Archived**) in the **Retention Alerts** table.
3) Statistics	Statistics of : • Number of retention policies of each type and how many files and folders they are added to. • Number of files and folders receiving a certain action in the last 7 days.
4) Realtime DLP Statistics	DLP violations occurring currently.

5) Quick Actions	**Add Policy** - Add a retention policy, and apply it to files and folders. **Effective Policies** - View a list of retention policies and the files and folders they affect. **View Audit** - View system audit logs. Defaults to displaying retention audit logs.

Secure Web Viewer for DRM

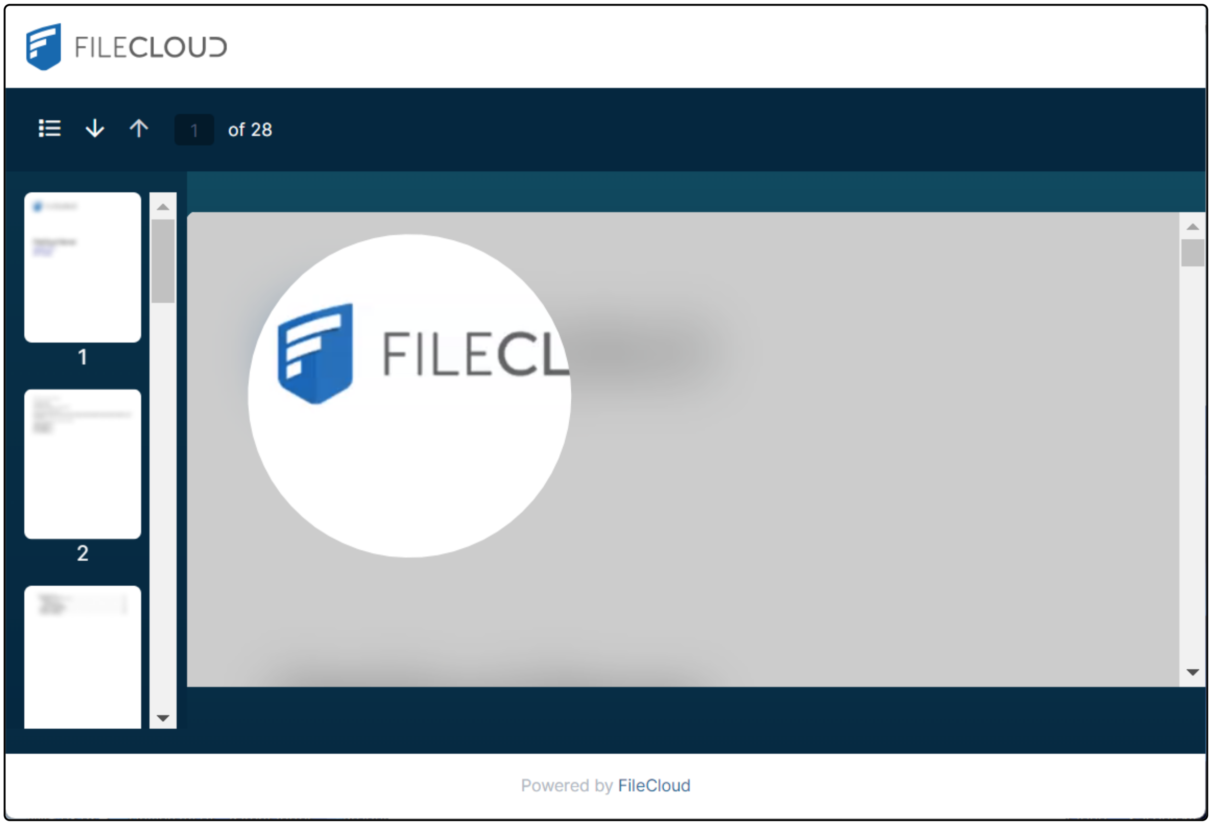
The Secure Web Viewer (Beta version) is available in FileCloud versions 23.232 and later.
Note: The Secure Web Viewer is not included with some licenses, such as the FileCloud Community Edition license and the FileCloud Essentials license.

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.

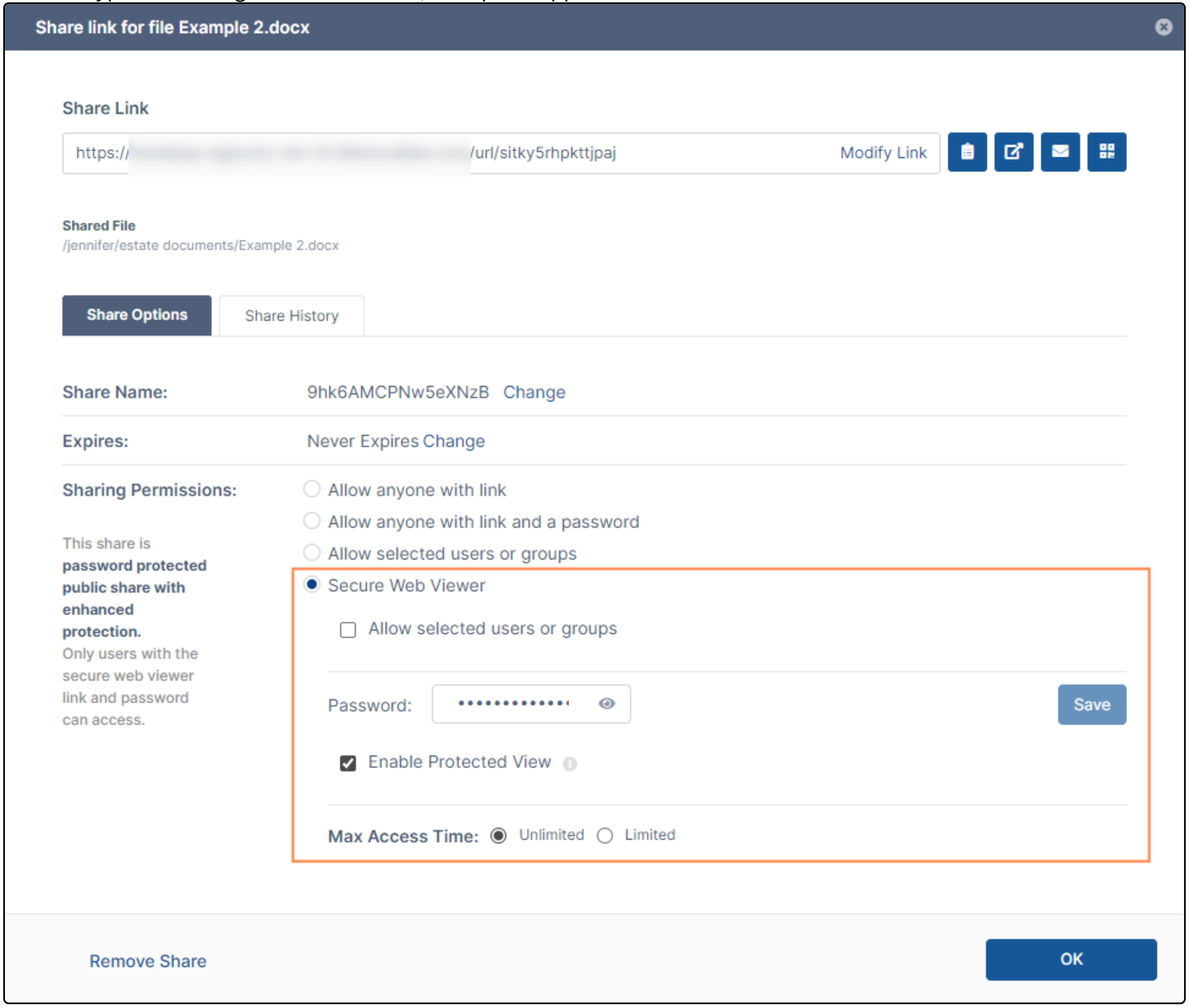
For more information about how a Secure Web Viewer share is created, see Public File Sharing with Secure Web Viewer Protection and Private File Sharing with Secure Web Viewer Protection.



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 for file Example 2.docx

Share Link

https://[redacted]/url/sitky5rhpkttjpaj 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
Password: ••••••••••••• Save
☑ Enable Protected View
Max Access Time: ● Unlimited ○ Limited

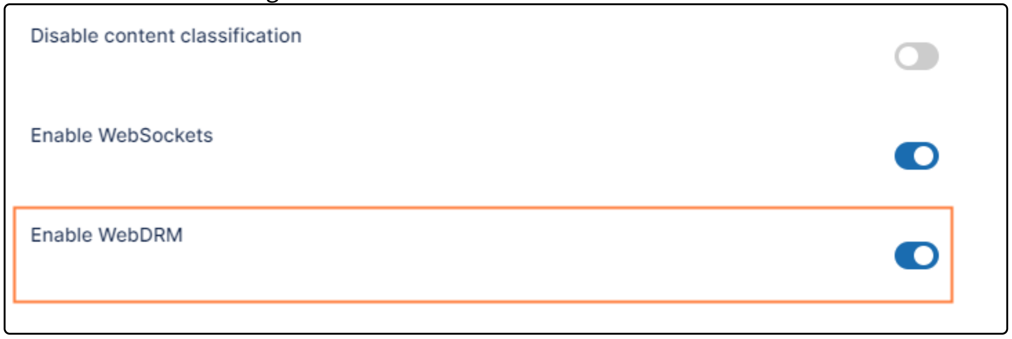
This share is **password protected public share with enhanced protection.** Only users with the secure web viewer link and password can access.

Remove Share OK

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.



Disable content classification

Enable WebSockets

Enable WebDRM

3. Click **Save**.