FileCloud Online
Version 23.263
FileCloud Site Maintenance

12 October, 2026

Table of Contents

Admin Portal Dashboard 2
Setup Checklist 2
Quick Actions 3
Dashboard Widgets 4
Release Notifications 18
By Subscribing to the Mailing List 18
Managing Users 19
Listing FileCloud Users 19
Viewing User Properties 20
Disable a FileCloud User Account 29
Deleting a FileCloud User 30
Resetting a User Password 32
Manage A User's Policies 34
Manage a User's Profile Picture 37
Change a User's Email Address 38
Setting a User Account to Expire 38
Send Email from User Details 39
Managing Groups 41
Change a User Group Name 41
Delete a User Group 41
View and Change Group Members 42
Exporting a list of users in a group 43
View and Change Group Admins 44
View and Change a Group's Policy 45
View and Change an SSO-imported Group's Sync Options 46
Managing Admin Users 48
Check an admin user's permissions 48
Remove an admin role 49
Managing User Folders and Files 50

Add Folder-Level Permissions to User Folders ... 51
Copy and Move User Files ... 54
Download User Files and Folders ... 55
Cancel User Uploads in Progress ... 58
Delete User Folders and Files ... 59
Clear a Recycle Bin ... 60
Remove a User's Old File Versions ... 62
Remove Incomplete User Uploads ... 63
Restore a Previous File Version ... 65
Change the Name of the Zip File for Multiple File Downloads ... 67
Managing Team Folders ... 69
To view the breakdown of data in Team Folders: ... 71
To edit the Team Folders account fields: ... 71
To lock the Team Folder account: ... 72
To manage Team Folder shares: ... 73
To reset the Team Folder account password: ... 74
To manage Team Folder notifications ... 75
To delete the Team Folder account: ... 76
Search for a Team Folder ... 78
Recover Deleted Files ... 78
View and Restore Previous Versions in Team Folders ... 80
Managing User Shares ... 83
To manage user shares for an individual user: ... 83
To manage user shares for all users: ... 85
To export a list of all shares: ... 86
Transfer Ownership of a Reshare from a Team Folder or Network Share ... 87
Creating direct file download link from a public file share ... 89
Creating direct file download links from a public folder share ... 89
Managing Storage Space Usage ... 93
Related topics ... 93
Managing User Locks ... 94
Managing User-Defined Notifications ... 98

Editing individual user's file and folder notifications 98
Editing all users file and folder path notifications 101
Adding notifications for actions on user's files and folders 103
Managing Client Devices 105
FAQ's 106
How Do You Want to Manage a Device? 108
Centralized Device Management 111
iOS Device Management 155
Search in the Admin Portal 157
FileCloud's Federated Search 157
All search 159
Audit Logs 164
What do you want to do? 164
View Audit Logs 164
Filter Audit Log Views 166
Configure What is Logged 170
Export Audit Logs 171
Delete Audit Log Entries 171
FileCloud Alerts 173
File Content Heuristic Engine 174
Identifying a FileCloud Specific Path 179
Custom Reports 181
Add Reports 181
Download Reports 184
Available Reports 184
Specifying Y-M-d H:i:s values 190
Manage Folder Level Permissions 192
To Edit Folder-Level Permissions 192
Managing Metadata 194
Metadata for governance and other system processes 194
Metadata for users 196
Metadata Components and Types 197

Create a New Metadata Set 200
Edit an Existing Metadata Set 203
Managing Metadata Attributes 205
Managing Metadata Permissions 206
Working with Built-In Metadata 210
Working with Custom Metadata 239
Working with Default Metadata 240
Finding files without metadata 242
Metadata Limitations/Recommendations 246
Managing FileCloud Licenses 248
FileCloud - License Purchase And Renewal 248
Workflows - IFTTT 267
The Workflow Dashboard 267
Add a New Workflow 268
Define an IF Condition 269
Define a THEN Action 303
Edit a Workflow 316
Run a Workflow 317
Set Advanced Workflow Options 318
Workflow Recipes for FileCloud 324
Automated Workflow Management 372
Disabling Automated Workflows 372
Enable Sharing of Automated Workflows 373
Requiring a Share Approval Workflow 374
Reset Settings and Customizations 376
To return to default settings for options in Settings 376
To return to default settings for all options on the Settings pages: 376

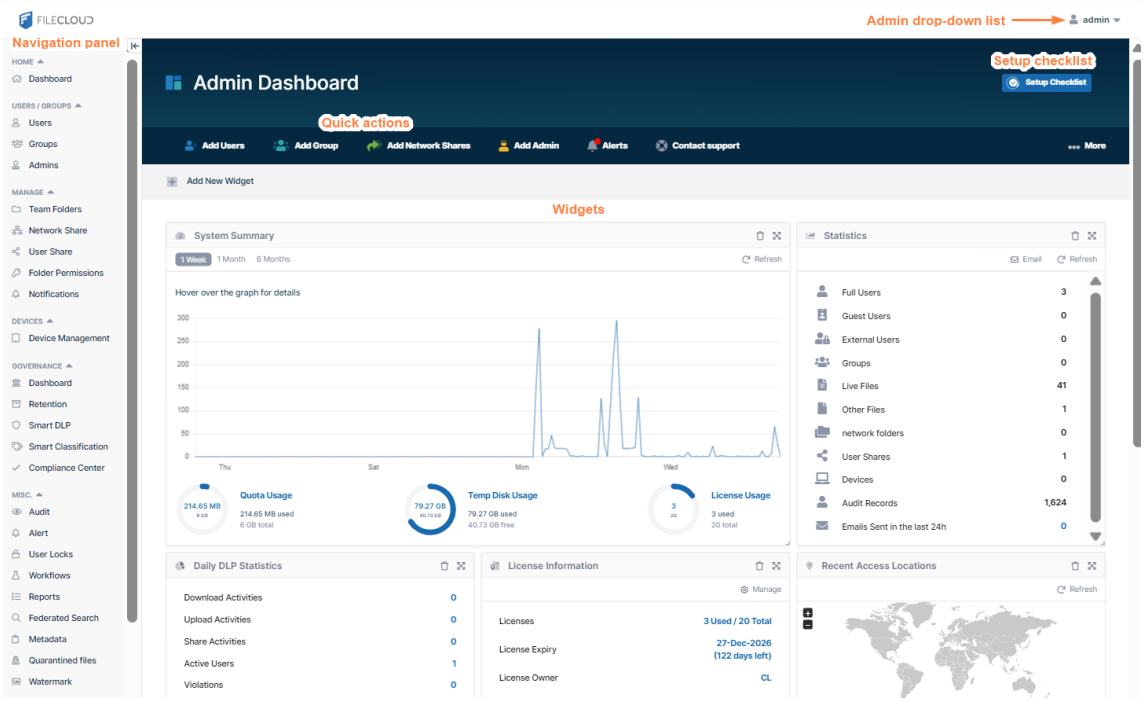
This section shows you how to monitor and maintain your FileCloud site, as well as how to edit and update its features and options.

Admin Portal Dashboard

The Admin dashboard, which is the first page you see when you log into FileCloud, is a Web console that provides a monitoring interface for your site.

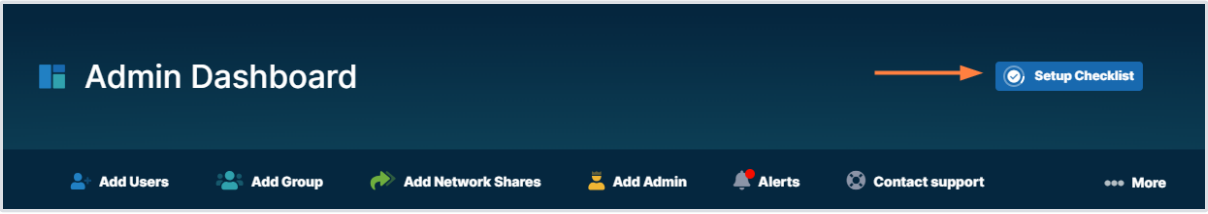
💡 The Admin dashboard displays several areas to help you manage your site.

- **Navigation pane** - The left pane includes a menu that allows you to access other screens where you configure site settings. It appears on all screens in the admin portal.
- **Setup Checklist** - This button opens a manually updatable checklist of the tasks generally required for setting up FileCloud.
- **Quick actions** - The ribbon near the top of the dashboard displays links to common actions such as adding a user and managing alerts.
- **Dashboard widgets -** The widgets on the dashboard allow you to see at a glance how your site is performing. Note: If you do not have access to a dashboard widget or its contents, it does not appear on your dashboard.
- **Admin drop-down list** - Includes options for switching to the user portal, accessing this documentation, signing out of the admin portal, and going to the FileCloud Knowledge Base for support. It appears on all screens in the admin portal.

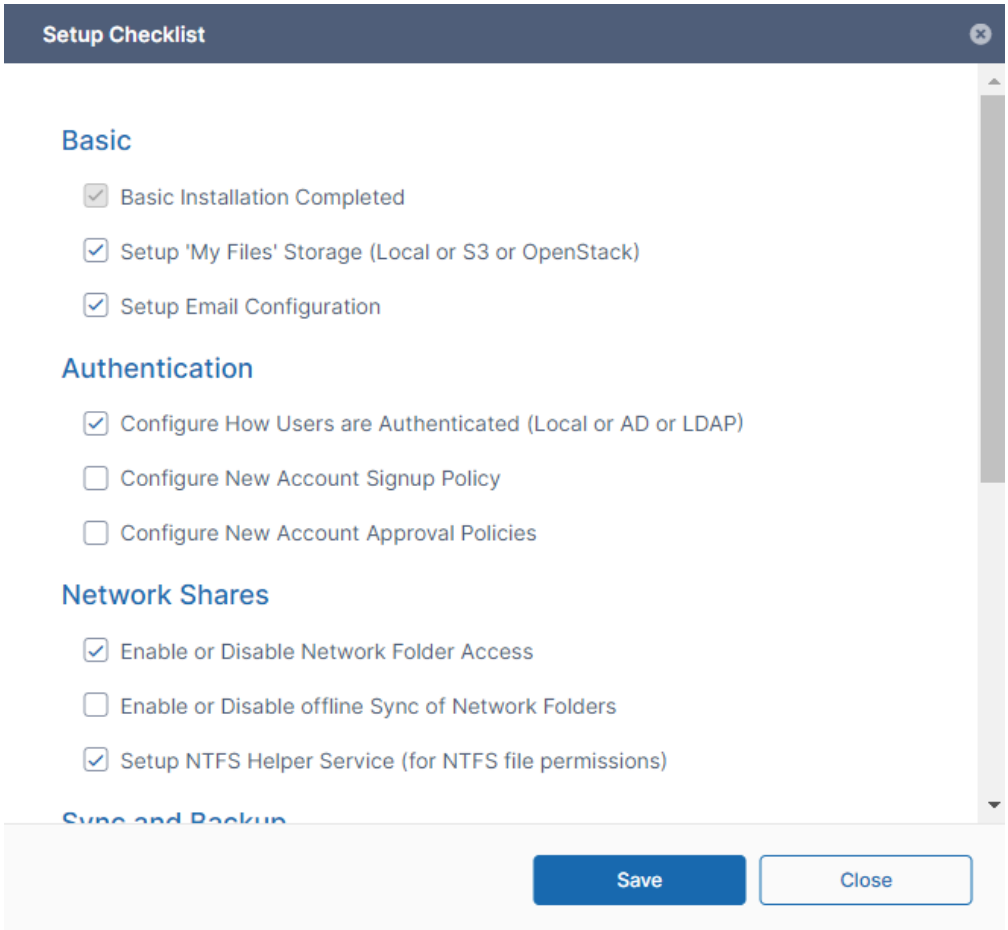


Setup Checklist

The **Setup Checklist** includes the tasks that are generally required for setting up FileCloud. Click the button in the header of the page to open the checklist.



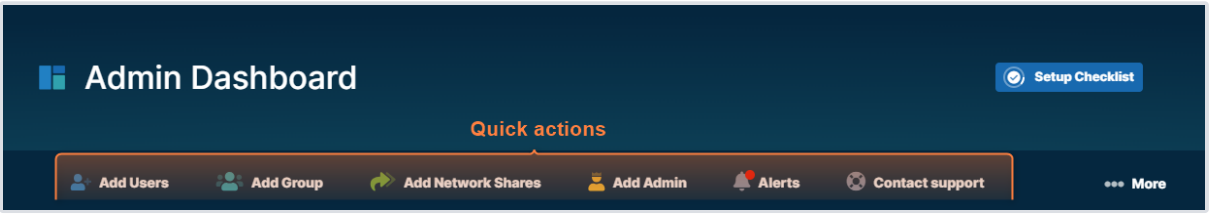
The **Setup Checklist** includes various tasks generally necessary for setting up FileCloud, although some tasks may not apply to you.
The tasks **Basic Installation Completed** and **Setup Cron Job** are automatically checked/unchecked for you, and you cannot modify them. All of the other tasks are not checked automatically, and you may check them manually to keep track of what you have completed.



Quick Actions

Links for quick actions are listed in a ribbon near the top of the page. They take you to the screen in the admin portal for the action, for example, the **Add Users** link takes you to the **Manage Users** screen.

The **Alerts** link takes you to the **Manage Alerts** screen. It displays a red dot if there are alerts listed on the **Manage Alerts** screen. You must clear all alerts from this screen to remove the red dot from the **Alerts** link.
If you are an Admin user, only those quick actions that you have access to are listed.



For help performing the quick actions, see:
Add a user
Add a group
Add Network Shares
Add Admin
Alerts
Contact FileCloud Support

Dashboard Widgets

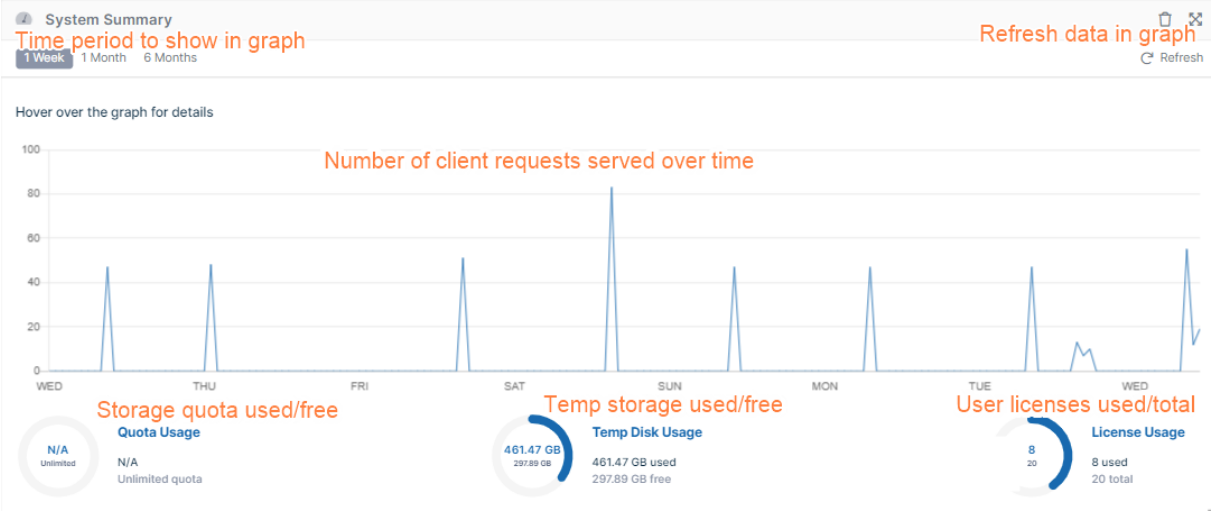
The FileCloud dashboard has widgets that display real-time information. If you are an Admin user, only those widgets involving actions you have access to are listed.

- Each widget accesses a particular set of data or performs a particular function and presents its information.
- Widgets allow you to visualize operational data with rich visualizations and fast performance.
- Widgets have menus or actions that allow you to access and manage the data quickly.
- Widgets can be rearranged on the screen, as well as removed and restored.

Widget descriptions

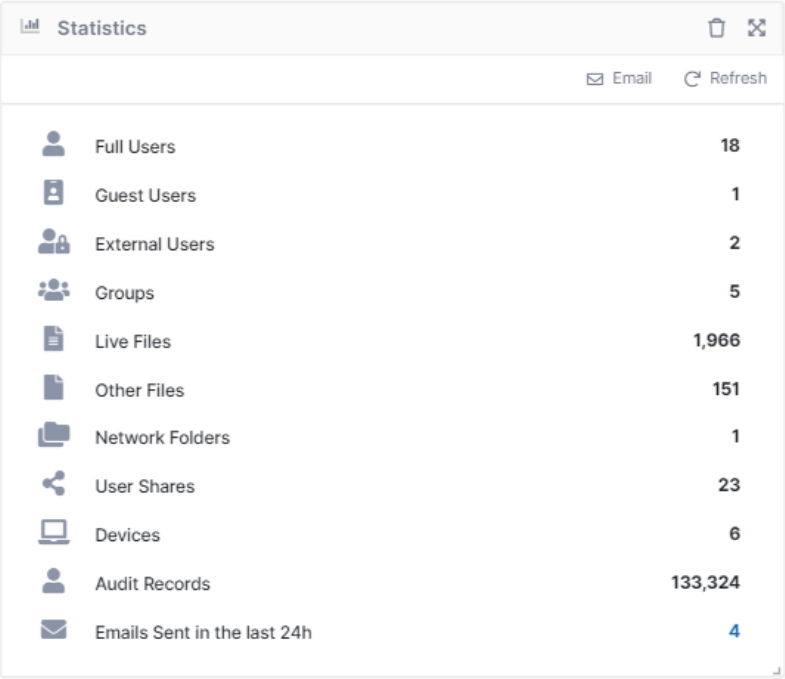
System Summary

This **System Summary** widget allows you to analyze overall site performance by visualizing relevant data for your site.



Statistics

This **Statistics** widget displays general statistics about your system:

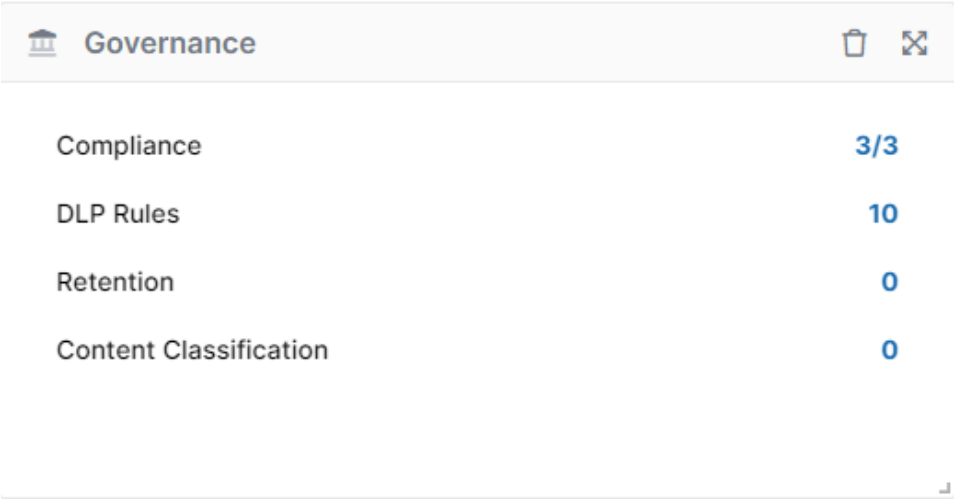


Icon	Function
	Sends an Admin Summary email to the admin. By default, an Admin Summary email is sent to the admin every 24 hours. Click number to view report.
	Refreshes the statistics.

Statistic	Description
Full / Guest / External Users	Number of full users, guest users, and external users.
Groups	Number of groups.
Live Files	Number of files stored locally by all users combined that users can access directly from FileCloud folders.
Other Files	Other files are additional versions of Live files that users access from the Previous Version option for a file.
Network Folders	Number of Network folders.
User Shares	Number of shares by each user. A share is counted each time a different user shares it, but only once per time shared, even if it is shared with multiple users.
Devices	Number of clients (other than the Web server) that use your system, such as FileCloud Drive, FileCloud Sync, MS Office plugin, MS Outlook plugin, mobile applications, ServerSync, and ServerLink.
Audit Records	Number of audit records in the entire system.
Emails Sent in the last 24h	Number of emails sent in your system in the last 24 hours. Click the number to view a report.

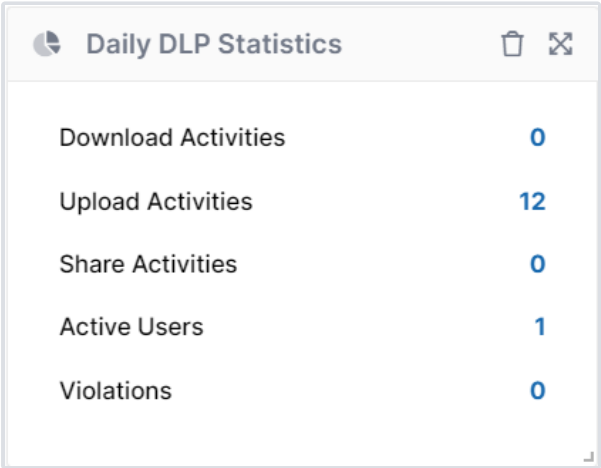
Governance

The Governance widget displays counts of your compliance configurations, DLP rules, retention policies and content classification rules. Each count is a link to the screen for configuring the feature.



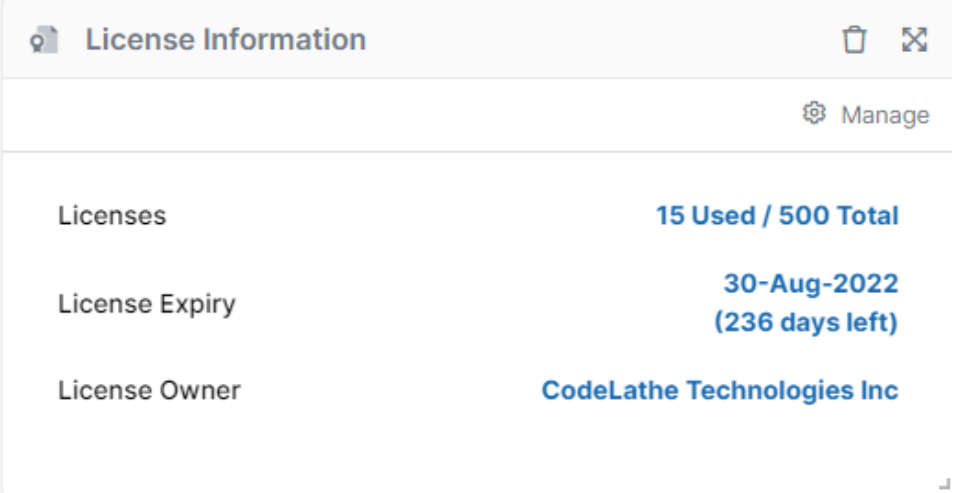
Daily DLP Statistics

This widget displays DLP statistics from the last 24 hours, including number of downloads, uploads, shares, and active users. When you click the number to the right of **Download Activities**, **Upload Activities**, **Share Activities**, and **Active Users**, a report listing the activities or users in the last 24 hours opens. When you click the number to the right of **Violations**, the Manage DLP Rules page opens.



License Information

This widget shows you basic information about your license.



In the upper-right corner of the widget, click **Manage** to go to the License settings page.
To update your license, see Viewing Your License Details.

Recent Access Locations

The **Recent Access Locations** report provides the total number of requests received from a geographical location. The countries that had any activities in the last 10 days are shown in blue color. The red points on the map indicate the cities. Moving the mouse over on the cities or countries

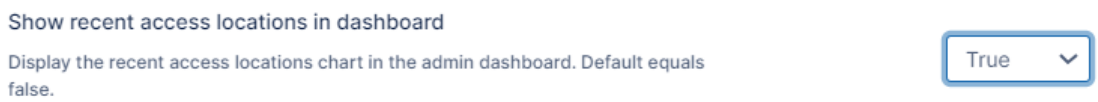
displays the total number of visits from that particular location in the last 10 days.

To refresh the report, in the upper-right corner of the **Statistics** widget, click refresh; then in the upper-right corner of the **Recent Access Locations** widget, click **Refresh**.

The **Recent Access Locations** report is not enabled by default.

To enable the Recent Access Location report:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin** .
   The **Admin** settings page opens.
2. Scroll down to **Show recent access locations in dashboard**, and set it to **True**.

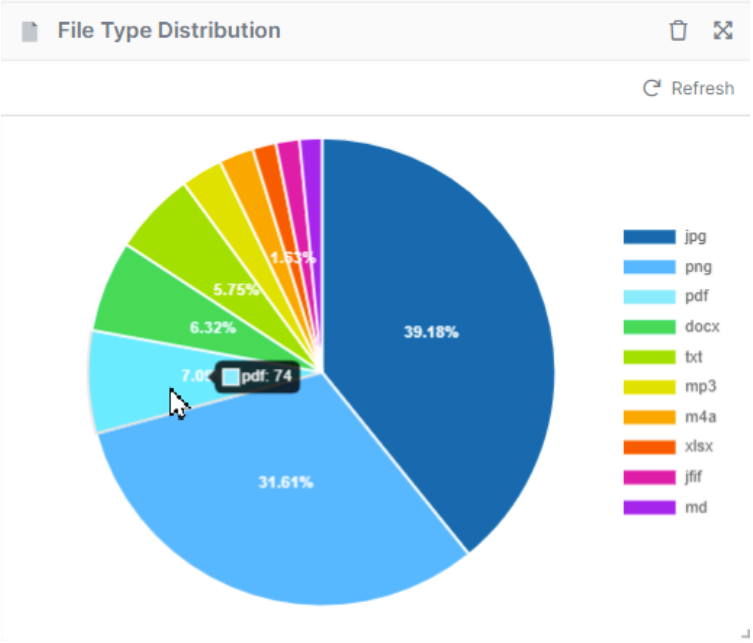


Settings	Value
Show recent access location in dashboard	TRUE - Show the Geo IP Map with data FALSE - Hide the Geo IP Map from the dashboard DEFAULT - Show the Geo IP Map with no data.
Access locations Server URL	Server URL that converts the IP address to Geo Location Data. Default URL: http://geoiplookup.codelathe.com/geoip.php To point this URL to a different location contact FileCloud support.
Recent access update frequency	The Frequency with which the GeoIP data is retrieved from the server. Default : 24.

NOTE: The **Recent Access Locations** map and report displays with proper data only when a Cron job is set up and running and the access IP address recorded in audit is an external IP.

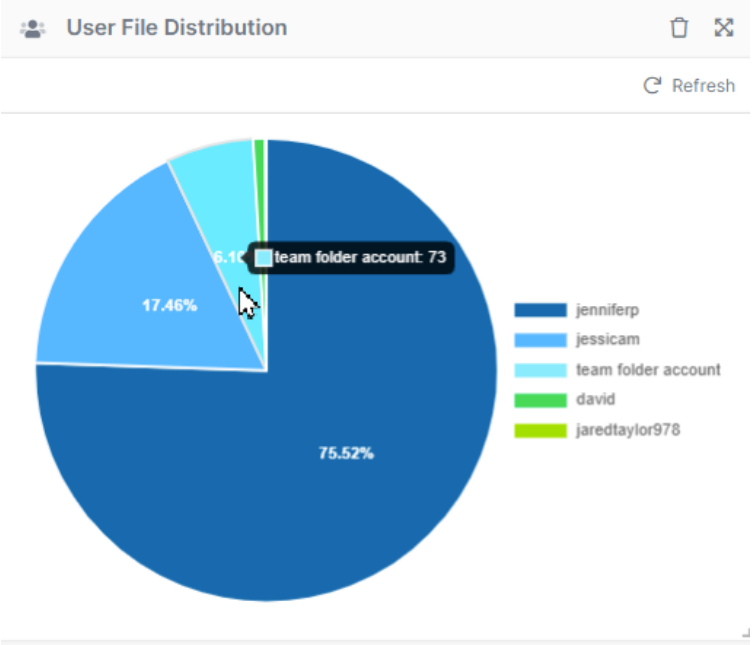
File Type Distribution

The File type distribution report displays the percentage of files that are stored in the FileCloud by file type extensions such as .PDF, .DOCX etc. Hover your cursor over a section of the chart to view the number of files of that type.



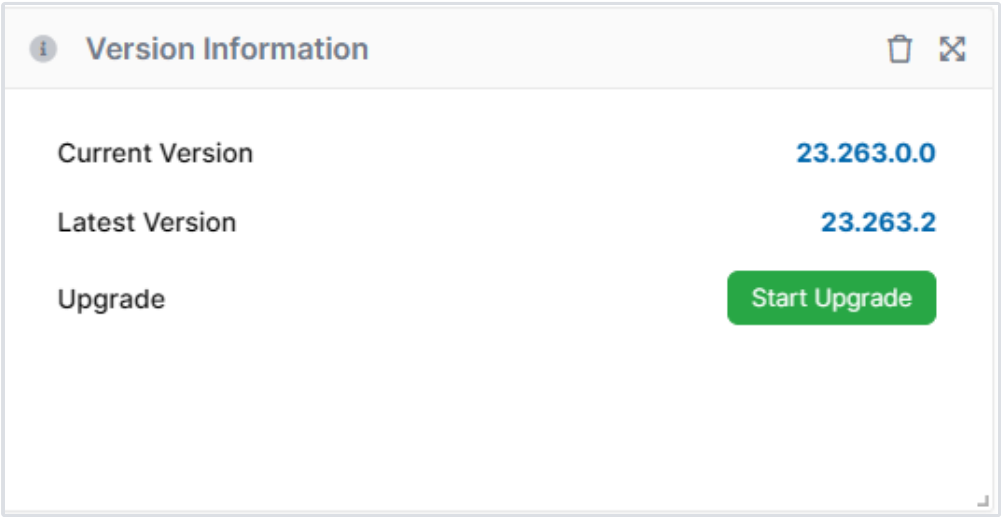
User File Distribution

The user file distribution report displays the total number of files that are stored in FileCloud by specific users in percentage. Hover your cursor over a segment of the chart to see the number of files the user is storing.

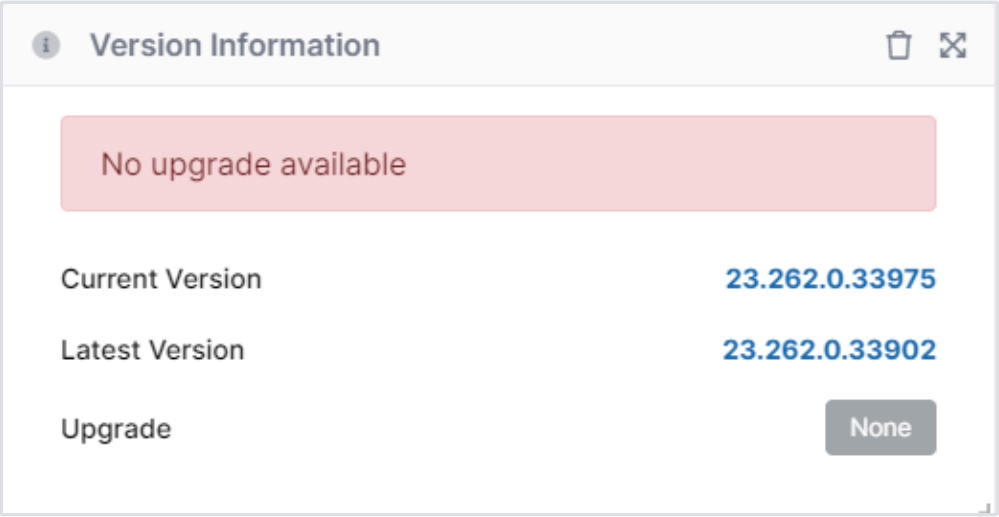


Version Information

The Version Information widget displays your currently installed version and the latest available version of the system. If there is a new version available, the widget displays a **Start Upgrade** button.

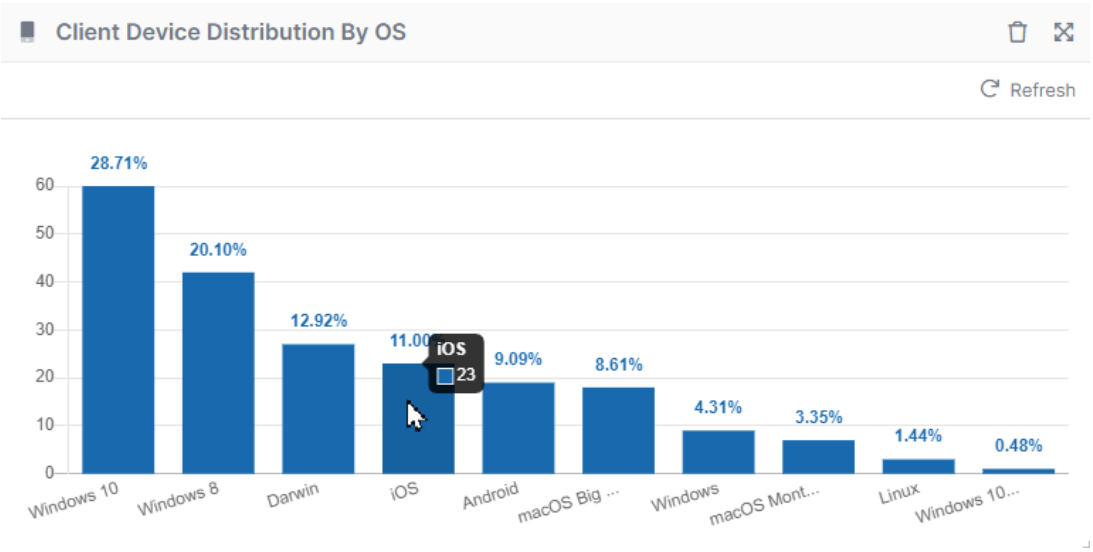


A banner indicates if there is no update available:



Client Device Distribution by OS

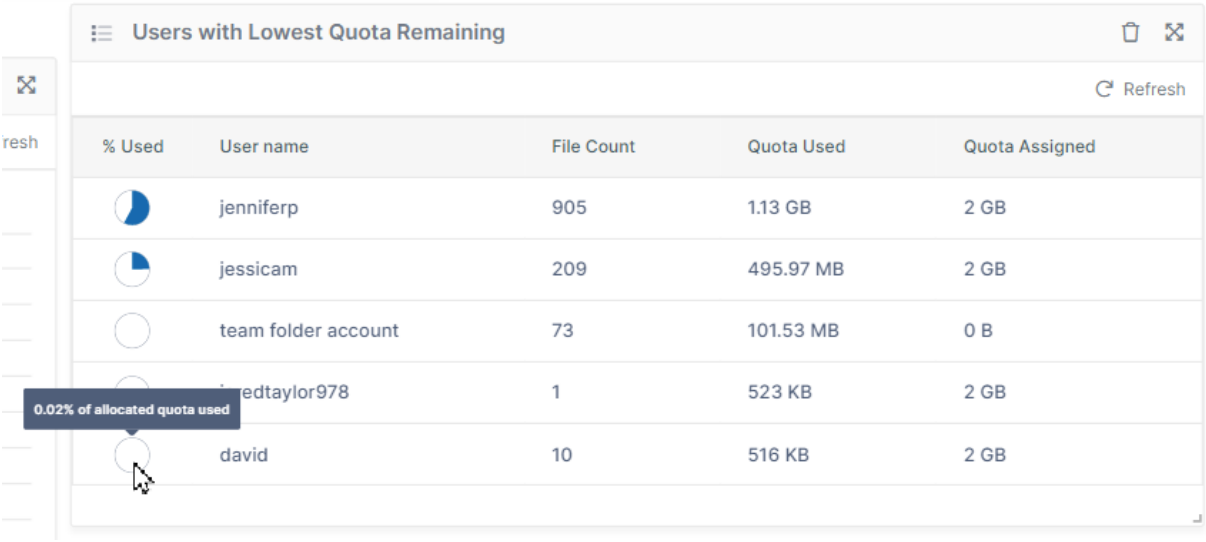
The client device distribution graph displays the total number of devices that are used to connect to FileCloud by OS type such as Windows, iOS, and Android. Hover over a bar to see the number of devices.



Users with Lowest Quota Remaining

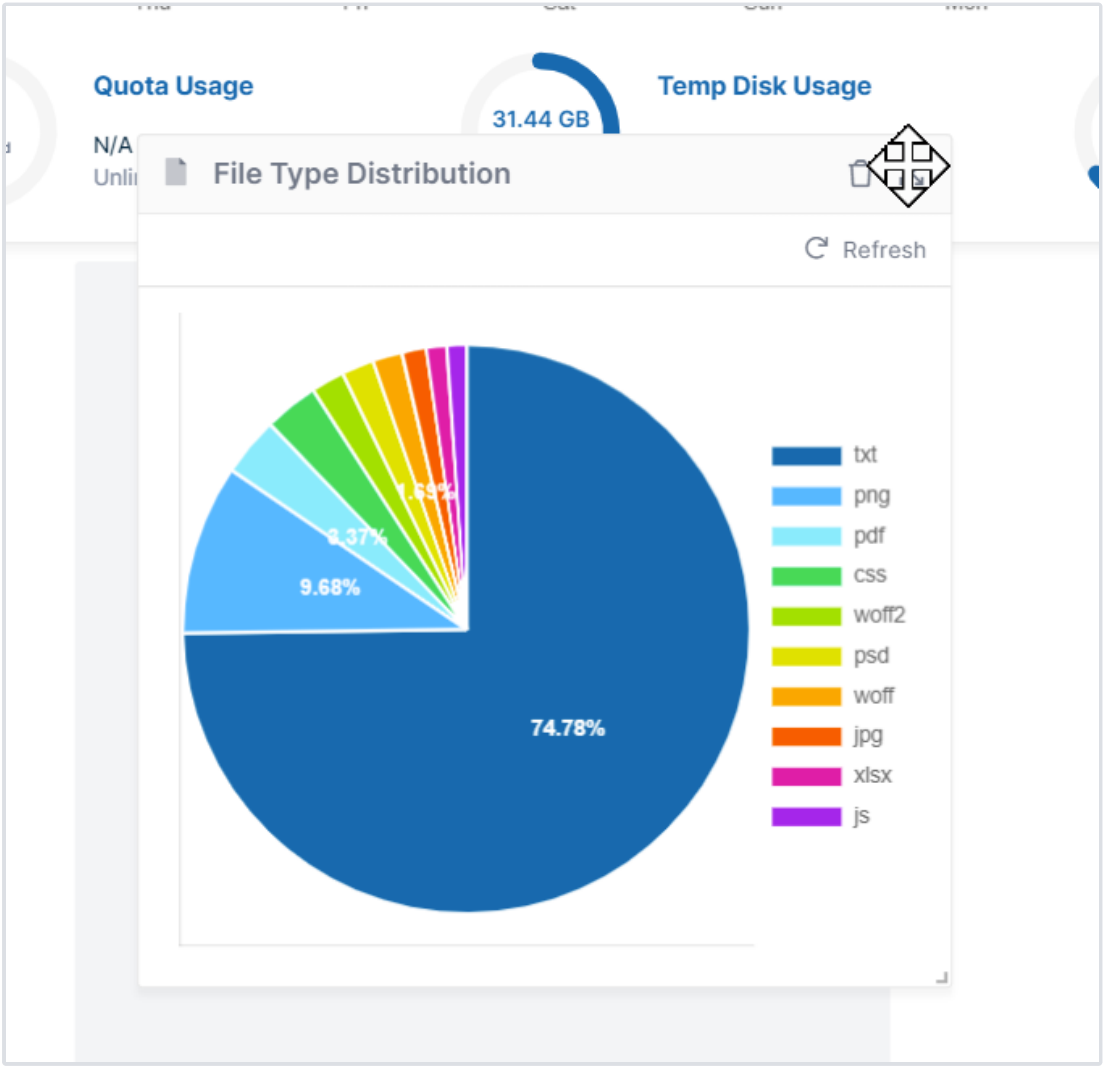
The **Users with Lowest Quota Remaining** widget displays the 10 users who have used the most disk quota. Hover your cursor over the icon in **% Used** to see the percent. The widget also gives the total files and the quota assigned for the user.

Please note that file count and size includes files in the user's deleted folder.

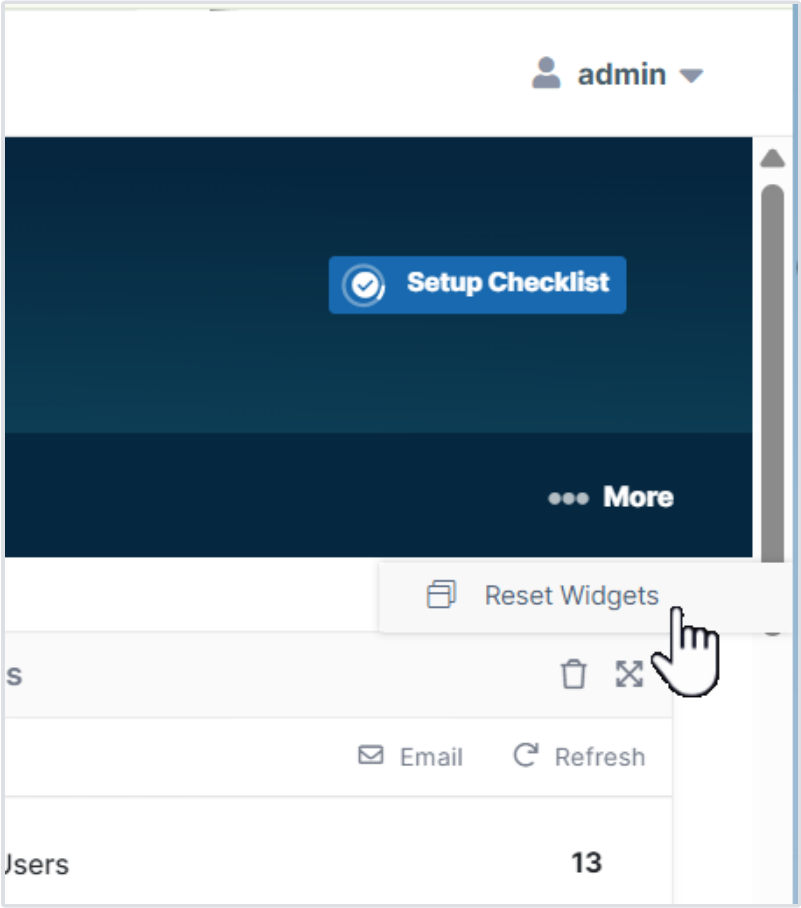


Rearranging and resetting widgets

To move a widget to a different location on the dashboard, click and hold the cross-arrow icon in the upper-right corner of the widget and drag and drop it to the new location.

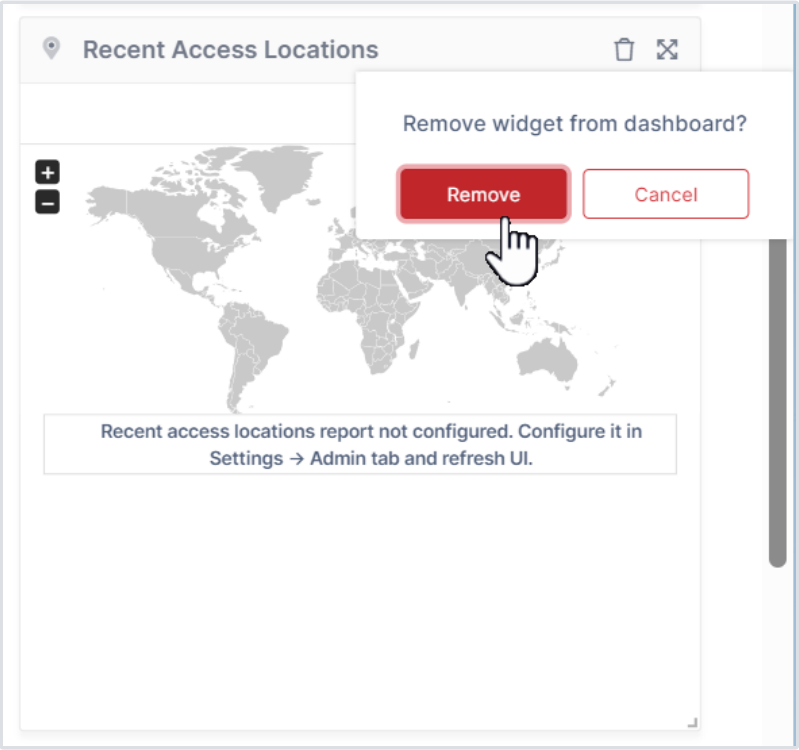


To move all widgets back to their original configuration, click **More** in the header ribbon and choose **Reset Widgets**.

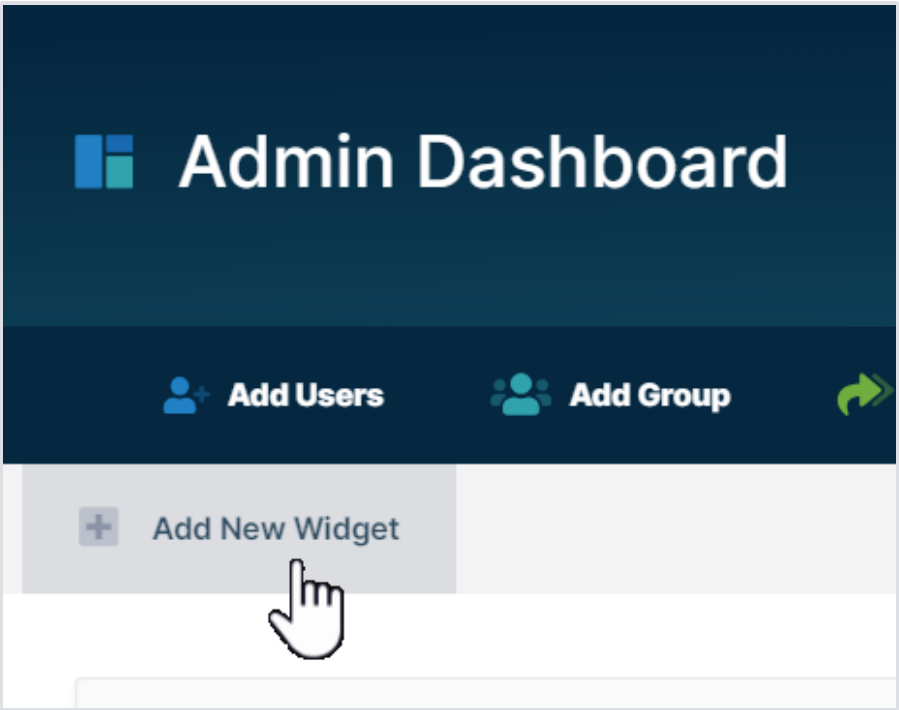


Removing and Restoring Widgets

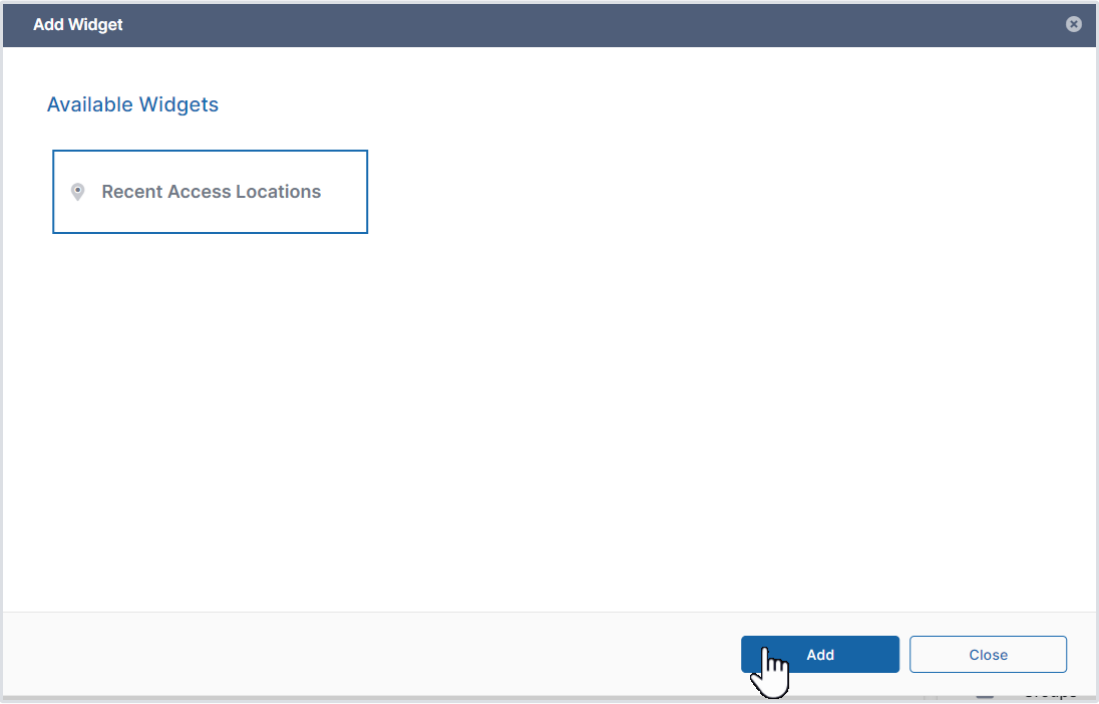
To remove a widget from the dashboard, click the delete icon in the upper-right corner of the widget, and then click **Remove**.



To restore a widget that has been removed, in the upper-left of the screen, click **Add New Widget**:



Then click the widget to restore, and click **Add**.



It is added to the bottom of the screen. To move widgets back to their original positions, click **More**, and choose **Reset Widgets** (see **Rearranging and resetting widgets**, above).

Release Notifications

You can learn about new FileCloud releases:

By Subscribing to the Mailing List

When you register with CodeLathe, you will automatically be added to the FileCloud Mailing List.

If you are not receiving FileCloud emails, you can Subscribe to the FileCloud Mailing List.

Managing Users

> The ability to update and remove a user's profile picture is available in FileCloud Server version 18.2 and later.

In this section:

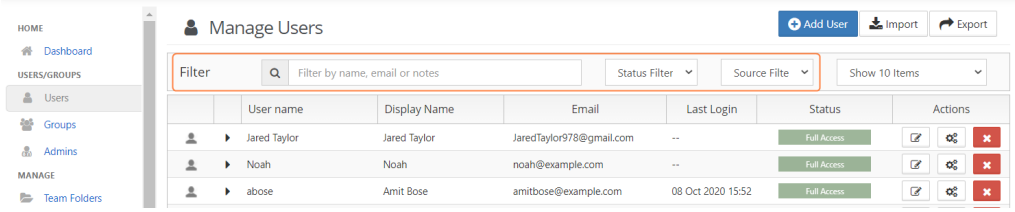
To add FileCloud users, see Create FileCloud Users.

Listing FileCloud Users

Listing Users

To list all users in FileCloud:

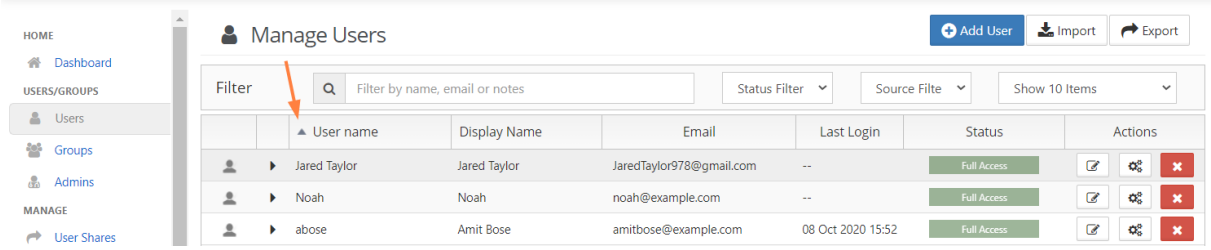
1. Log on to Administration Portal.
2. Click on **User** on the left navigation panel to list all users.
3. To find users:
    - by name or email,, use the **Filter by name, email or notes** box.
    - by status, use the **Status Filter** box.
    - by source, use the **Source Filter** box. Options are:
        - **All** - Default. Users in both of the following categories.
        - **DEFAULT** - Users created internally in FileCloud.
        - **SSO** - Users created externally using SSO.



Sorting the User List

To sort the user list, click on the column name. The list is sorted on that column, and an arrow indicating the direction of sort appears in the column header.
For example, the following screenshot shows the user list sorted by ascending user names.

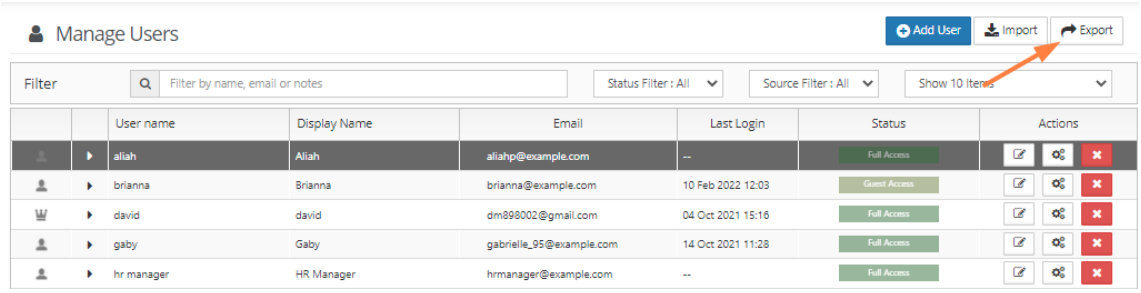
Notice that by default, all upper-case letters precede lower-case letters in alphabetical order.



Exporting a list of users

To export a list of FileCloud users:

1. In the navigation pane, click **Users**.
2. Click **Export** in the upper-right of the **Manage Users** screen.



A csv file of users displaying the following fields is exported:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotifications	LastLogin	Authentication Type	MobilePhone	Effective Policy	
2	david	dm898002@example.com		david	FULL		EVERYONE	YES	NO	10/4/2021 15:16	Default	15559992323	Group Management	
3	aliah	aliahp@example.com		Aliah	FULL		EVERYONE	YES	NO		Default	15556667777	Global Default Policy	
4	hr manager	hrmanager@example.com		HR Manager	FULL		EVERYONE	YES	NO		Default		Global Default Policy	
5	gaby	gabrielle_95@example.com		Gaby	FULL		EVERYONE	YES	NO	10/14/2021 11:28	Default		Global Default Policy	

Viewing User Properties

> The ability to update and remove a user's profile picture is available in FileCloud Server version 18.2 and later.

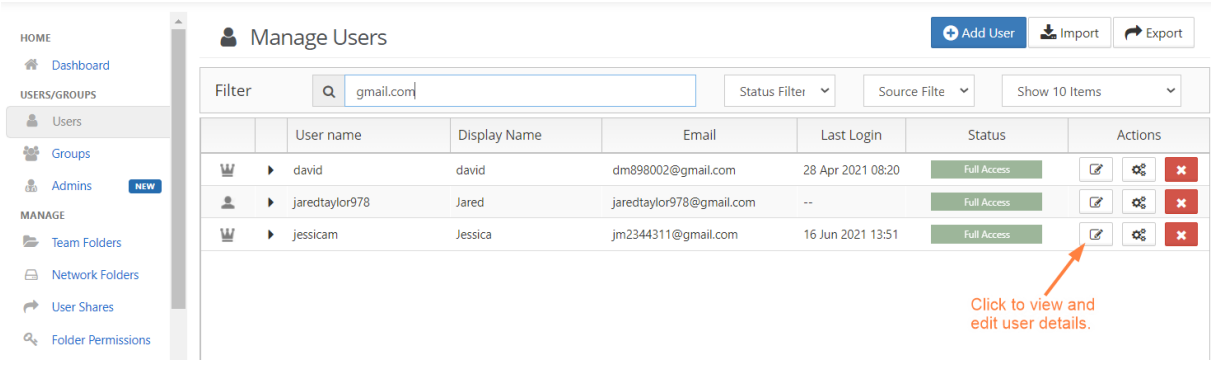
As a FileCloud administrator, you can see user properties and change them as needed.

To see a user's details and what they have permission to do:

1. Open a browser and log on to the admin portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user you want whose details you want to view.

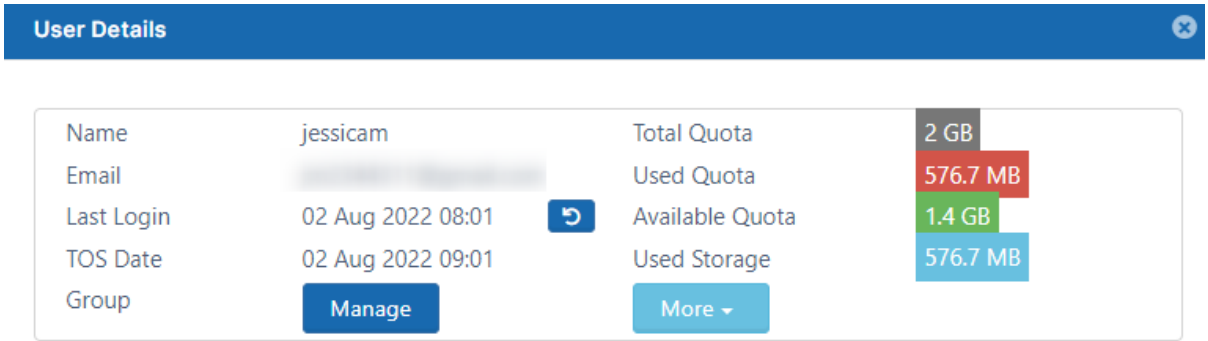
4. Click the **edit icon**.

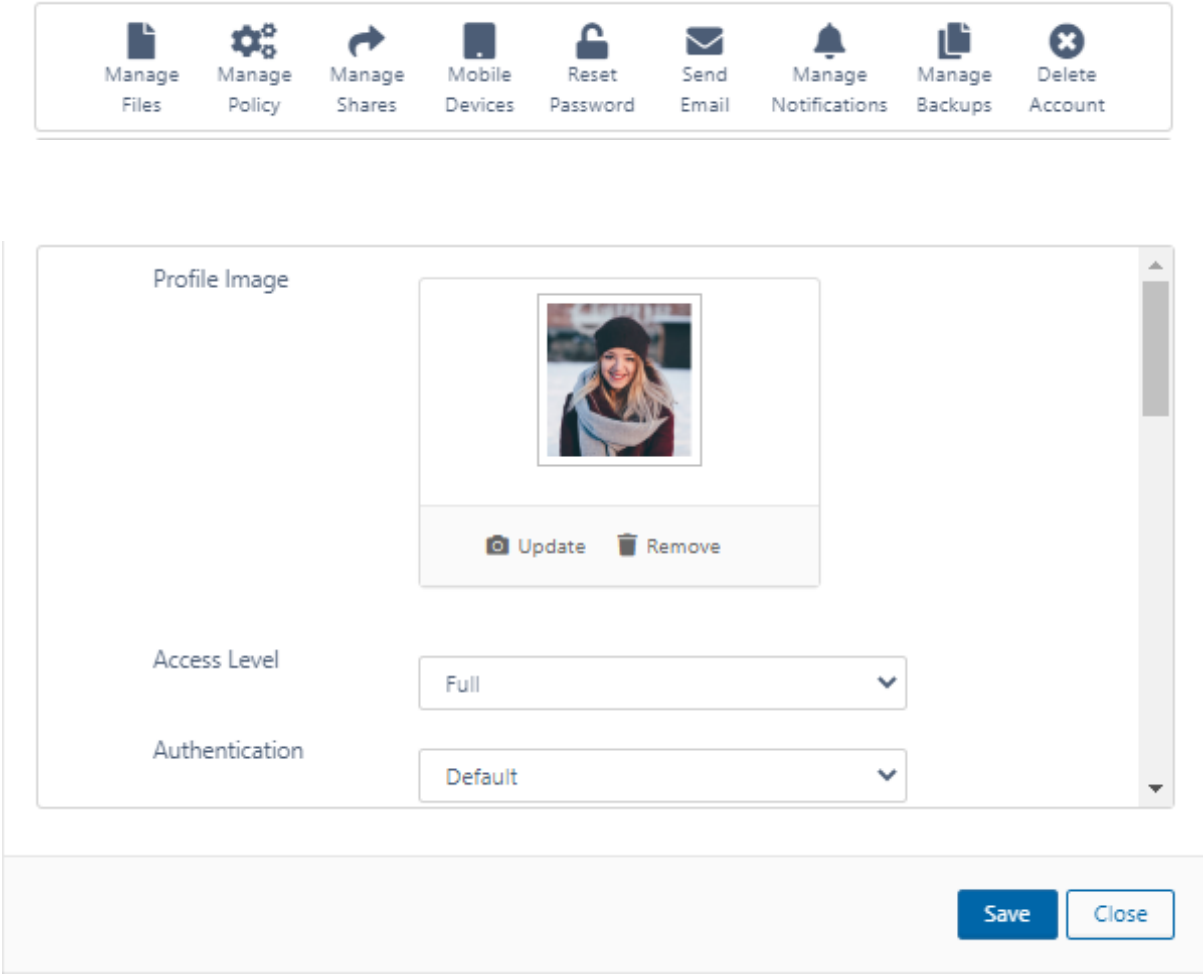
Show me



The **User Details** window opens showing you which user attributes you can set.

💡 Click on the section of the **User Details** window below to learn more about an option.



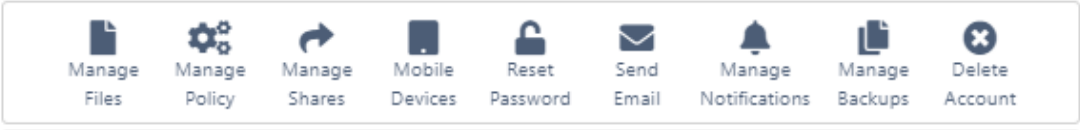


User Properties - Advanced Options

"As a FileCloud administrator, you can see user properties and change them as needed.

To see a user's details and what they have permission to do:

1. Open a browser and log on to the admin portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user whose details you want to view.
4. Click the **edit icon**.

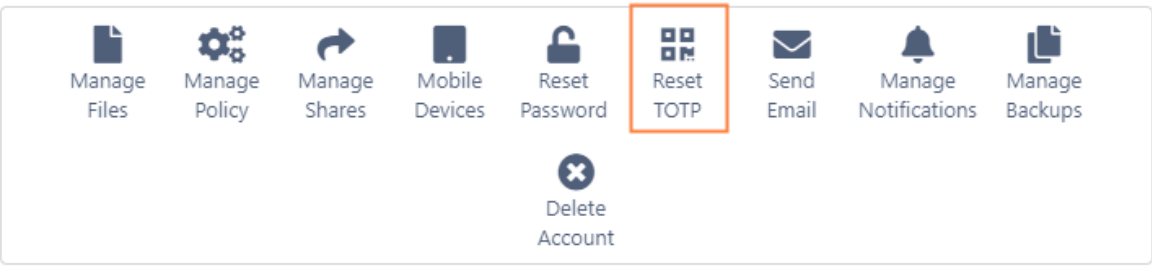


Options	Description	For more information
Manage Files	Manage the files that are stored on your FileCloud Server site. This allows you to protect and maintain your system in the following ways: • Remove user files infected with a virus • Remove files belonging to a user that no longer has an account • Move folders for teams • Download, copy and move files at a user's request • Manage your storage space limits by moving or deleting files • Copy and move files and folders between two FileCloud users	Managing User Files and Folders
Manage Policy	Manage client policy for this user (overrides global values)	
Manage Shares	View, modify or remove shares created by users with a FileCloud account and appropriate permissions.	Managing User Shares
Mobile Devices	Manage clients connecting to your FileCloud instance. This feature is called Remote Client Management (RCM) or Data Leak Prevention Control (DLPC)	Managing Client Devices
Reset Password	Reset the password for user accounts with Authentication Type set to Default. For user accounts with an Authentication Type set to AD or LDAP, the password management must be done in AD or LDAP admin portal.	Reset a User Password
Send Email	If the user does not have an AD account, this option either sends a forgot email message with the password newly generated by **Reset Password** or an account welcome message with an automatically generated new password. If the user has an AD account, there is no option to send a forgot email message. Clicking OK sends the user a welcome email without a new password. The option to send an account welcome message for accounts other than AD users is available beginning in FileCloud 20.1 The option to send an account welcome message to AD users is available beginning in FileCloud 20.3	Send Email
Manage Notifications	Edit notifications configured on the user's file and folder paths.	Editing individual user's file and folder notifications
Manage Backups	Manage backups for the user.	

Options	Description	For more information
Delete Account	Delete this user account from the command line or the admin portal.	Deleting a FileCloud User

The Reset TOTP button

A **Reset TOTP** button is included for admin users if a setting is included to configure their 2FA to use the admin configuration if the admin 2FA delivery method is TOTP. When the setting is included, the admin users' TOTP authorization cannot be reset by the given methods for users and the main admin, and must be reset using this button. For more information about the setting, see Two-Factor Authentication for Admin Portal.



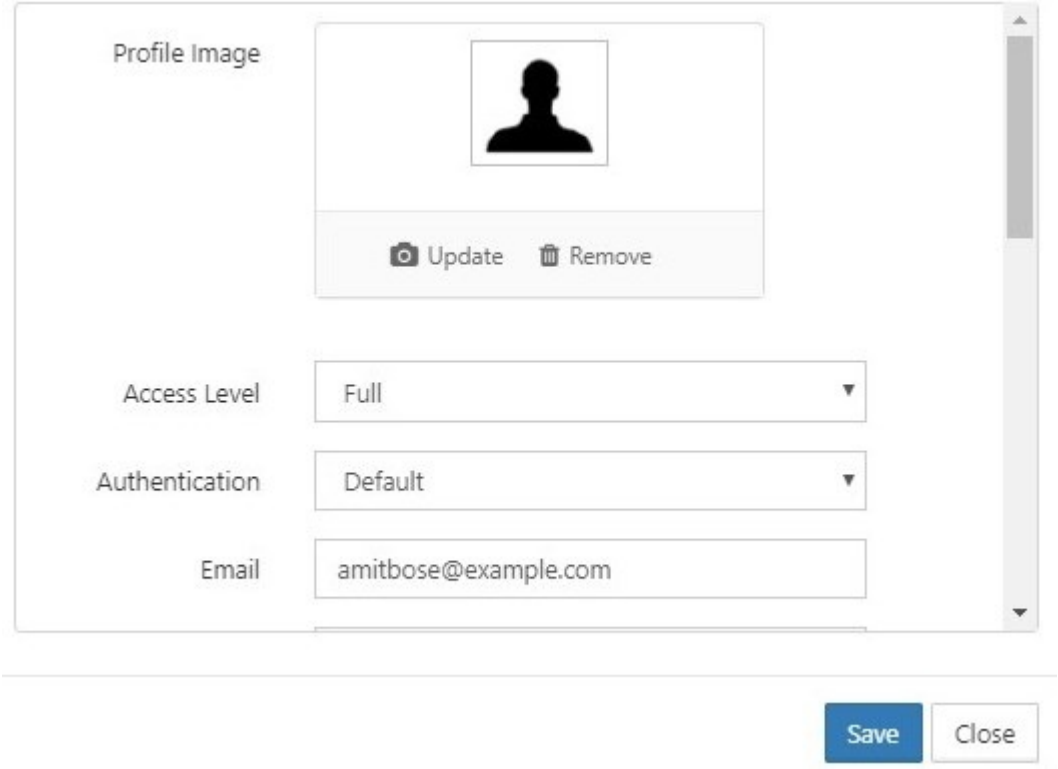
User Properties - Editable

> The ability to update and remove a user's profile picture is available in FileCloud Server version 18.2 and later.

As a FileCloud administrator, you can see user properties and change them as needed.

To see a user's details and what they have permission to do:

1. Open a browser and log on to Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user you want whose details you want to view.
4. Click the **edit icon**.



After you make any changes and save them, the new property will be in effect immediately.

For example, after an administrator increases the storage quota for an account, the increased storage is available to the user as soon as the administrator clicks Save.

Editable Property	Description
Profile Image	You can choose a new picture or remove the current one. • This is useful for IT Managers who also manage user images in Active Directory. • If no profile image is chosen, the default shown in the User Details panel is used by default.

Editable Property	Description
Access Level	This is the access level set for this user. The possible values are: • **Full Access** • **Guest Access** • **External Access** • **Enabled** • **Disabled** Only accounts with enabled status can login into their account irrespective of their access level. Disabled accounts do not count towards the License Limit. For more information: User Access Levels
Authentication	This is the type of authentication used to verify the user's account. The possible values are: **Default** **External (AD/LDAP)** For more information: Authentication
Total Quota (GB)	Field to set the total storage quota for the user account. The value set must be in GB.. This value will override the global storage quota settings.
Email	Field to set the email ID for the user account. This value has to be unique for the FileCloud installation.
Secondary Email	Additional email account.
Display Name	Field to set an user readable name that will be used in various places such as email notifications etc.
Account Expires On	If this is date is set and the current date is past, the account will be disabled automatically and user cannot log into the system
Password Expires On	If "User Password Expires in Days" field in Password settings is configured, then any new account will have this value setup automatically and will require password change after the expiration date elapses.This value can be overridden by the administrator. NOTE: An automatic email notification is sent to the user 7 days and 1 day before the actual password expiry date.
Email Verified	Indicates if the entered email has been verified. If email is not verified, then account cannot be logged in until the verification is completed.

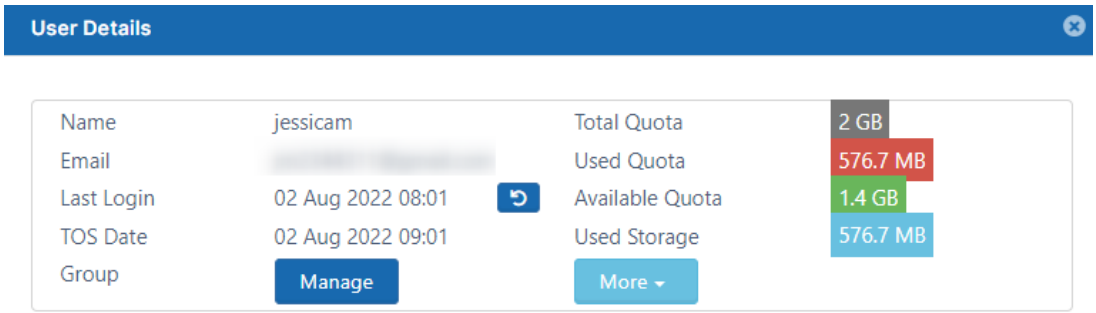
Editable Property	Description
Disable Sync (Automatic Sync of My Files and Network Folders)	Allow or disable Automatic sync of "My Files" location and Network Folders Location
Disable Sync (Offline Network Share Sync)	Allow or disable offline access of network folders in FileCloud Sync
Backup Path	Allows override of the backup folder that the user can backup files and folders using the sync app or the media files from mobile apps
Change Password on Login	Forces the user to change the login password on first login to the user portal. Note: This does not appear when the following setting, **Creation Source**, is set to **SSO**.
Creation Source	Where user was created. Options are: • Default (Admin user interface or import) • SSO (During SSO sign in) - When this is selected, the above setting, **Change Password on Login** is not applicable and does not appear.
Phone Number	The user's phone number. This phone number is used for SMS-based multi-factor authentication (MFA). When a user logs in for the first time with SMS MFA enabled, they are required to re-enter their phone number, even if it has already been configured by an administrator.
Notes	This filed allows the user to enter notes for the user and also search the user based on notes.

User Properties - Read Only

As a FileCloud administrator, you can see user properties and change them as needed.

To see a user's details and what they have permission to do:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user you want whose details you want to view.
4. Click the **edit icon**.



Most of the User Properties in the top portion of the User Details dialog box are for display only and cannot be changed in this window.

In this section of the User Details, you can manage the groups that a User belongs to by clicking the Manage button.
See Managing Groups

The User's read-only properties are described in the following table.

Read only Property	Description
Name	The unique name of the user account.
Email	Email id associated with the account (Can be changed editing the "**Email**" text box).
Last Login	Last login attempted on this account. Click the Reset icon to set **Last Login** to null. **Note**: When a disabled user is re-enabled, Last Login is set to null.
TOS Date	Date that terms of service was approved on login. If not approved, **Not Accepted** appears.
Group	Click **Manage** to view, add, and remove the user's groups.
Total Quota	Quota allocated for this account (This can be changed using "**Total Quota (GB)**" text box)

Read only Property	Description
Used Quota	This is the size of data this user has currently used. This includes all "Committed" Space by this user including file versions, files in recycle bin, partial files uploaded. Depending on the storage calculation setting, this quota might also include storage shared with this user by other users. For guest access users, this value calculated from the amount of data shared to that account.
Available Quota	Space available
Used Storage	Space taken by all this user content. This includes space used for **multiple file versions**, **files in Recycle bin** contents and **Partial files in progress.**

Storage Details
Additional storage details about the files stored in the user account can be viewed by clicking on the "**More**" button found in the read only section of the user properties popup.

Disable a FileCloud User Account

Disabled User Account Status

Any user account can be disabled by the Administrator.

If a user account is disabled, then the following rules apply

	Description
Log in using user id from browser or other clients	Disallowed. User will see explicit message when attempting to log in
User files	Not deleted.
License count	Disabled users do not count towards consumed license count

Disabling a User Account

Disable a user account by following the steps listed below

1. Log on to Administration Portal.
2. Click **Users** in the left navigation panel.
3. Click **Edit** in the user row.

4. Using the **Status** drop-down list, change the status to **Disabled**.

   UNKNOWN ATTACHMENT

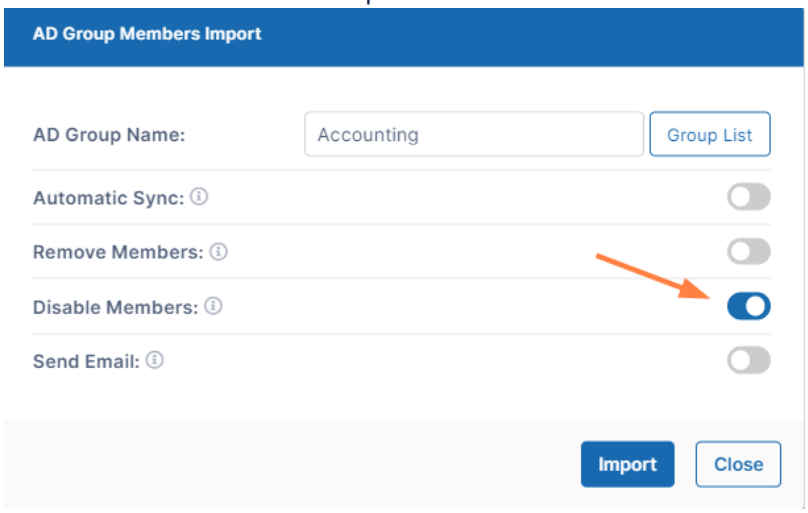
5. Click **Save**.

Import Disabled Users from Active Directory as Disabled

When a user account is disabled in AD, it may be imported as a disabled account into FileCloud.

To use this option:

1. Open a browser and log on to the admin portal.
2. In then navigation panel, click **Groups**.
3. Select the **group** that you want to add users to, and then click the Edit icon.
4. On the **Members** tab, click **Import Users from AD Group**.
5. In **AD Group Name**, enter the AD group to import.
6. Enable the **Disable Members** option.



If there are users with disabled accounts in the AD group, they are listed in the admin portal's **Manage Users** screen with **Disabled Access**.

Deleting a FileCloud User

As an administrator, you can delete a FileCloud user account.

When a user account is deleted

- By default, the user's data stored in My Files is deleted.
- The user can no longer log in via browser or connect using the Sync client or Drive client.
- The user's license account is released, and the available license count is incremented by 1.
- The user is removed from all shares.
- The user's workflows are deleted.

- Data shared by the user is no longer be available.

Account Type	Effect
User with "Default Authentication" (Local User)	Local user account is deleted.
User with "AD or LDAP Authentication"	Only the FileCloud account will be deleted. No change will be done to the user in the AD or LDAP server.

To move the user's data to a different user before deleting the account:

Use the admin portal to copy and move user files

To delete the user's account

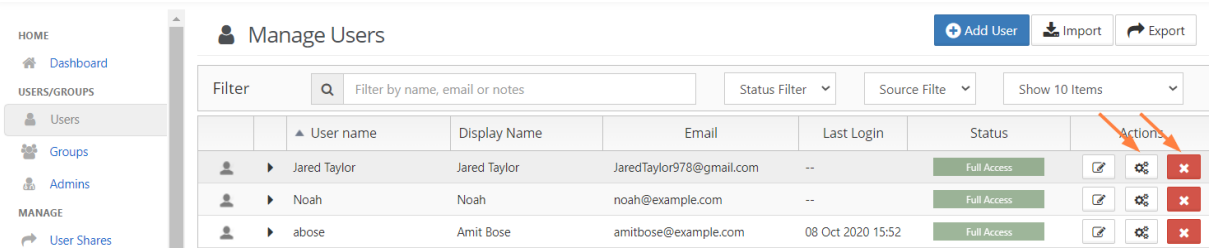
Delete the account

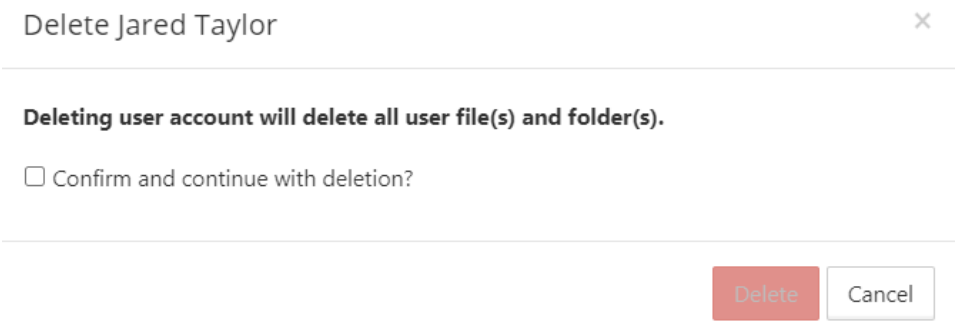
Deleting a FileCloud User From Admin Portal

To delete a user:

1. Open a browser and log on to Administration Portal.
2. From the left navigation panel, click **Users**.
3. Click the row containing the user to be deleted.
4. In the Actions column, click the delete icon ( ).
5. On the confirmation dialog, click the box next to "Confirm and continue with deletion?". Then click OK.

It is also possible to delete an account using the account properties panel by clicking on the settings icon .





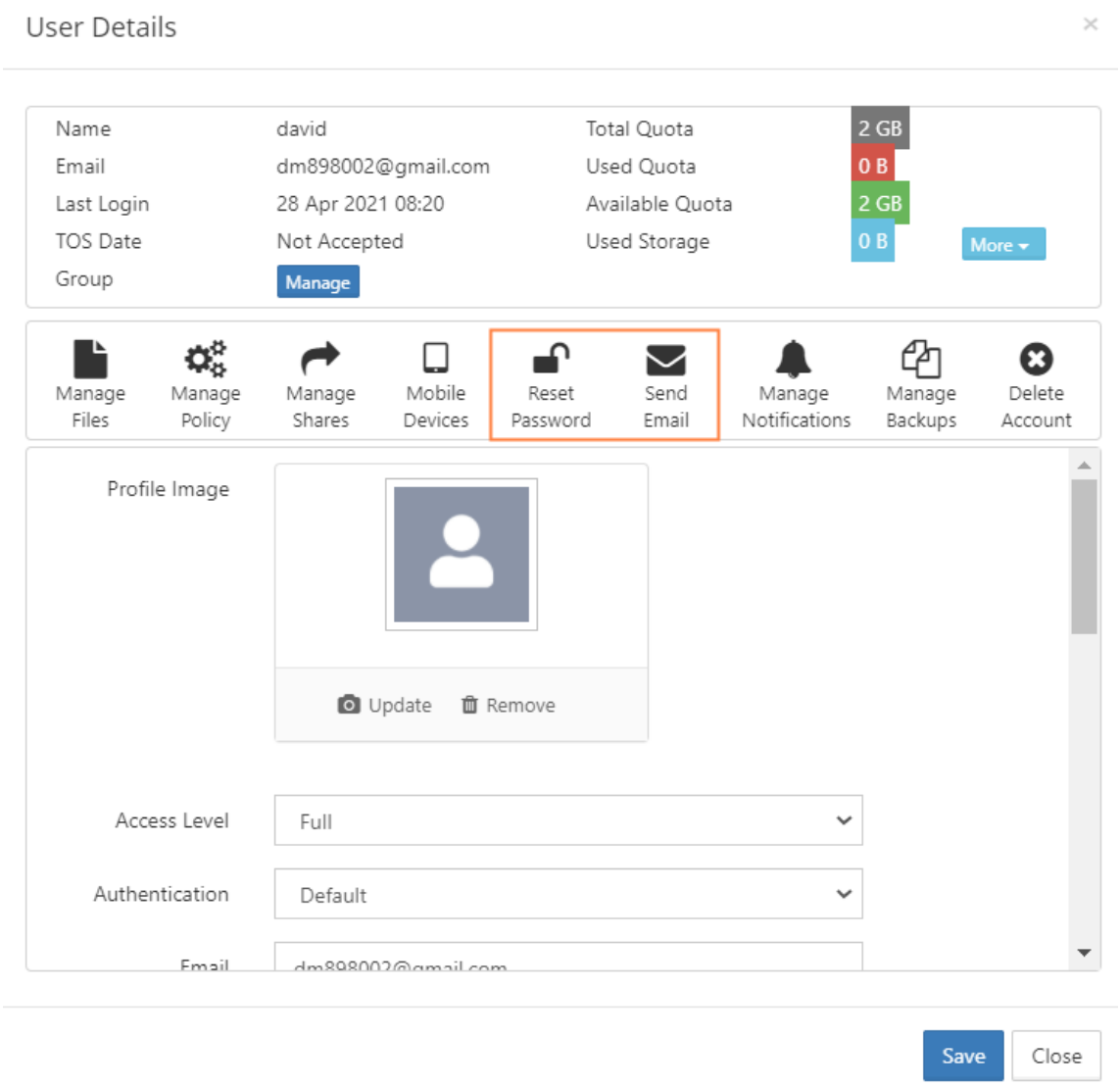
Resetting a User Password

As a FileCloud Administrator, you can reset password for accounts with Authentication Type set to Default.

> For user accounts with "Authentication Type" set to "AD or LDAP", password management must be done in AD or LDAP admin portal.
> Sending the Account Welcome email option is available beginning with FileCloud 20.1.

To reset password for user account:

1. Log on to Administration Portal.
2. Click on "**Users**" on left navigation panel.
3. Locate the user to reset the password using "**Filter Users**" or from the user list.
4. Click on "**Edit**" for the user row under the "**Actions**" column to launch the User Details window.

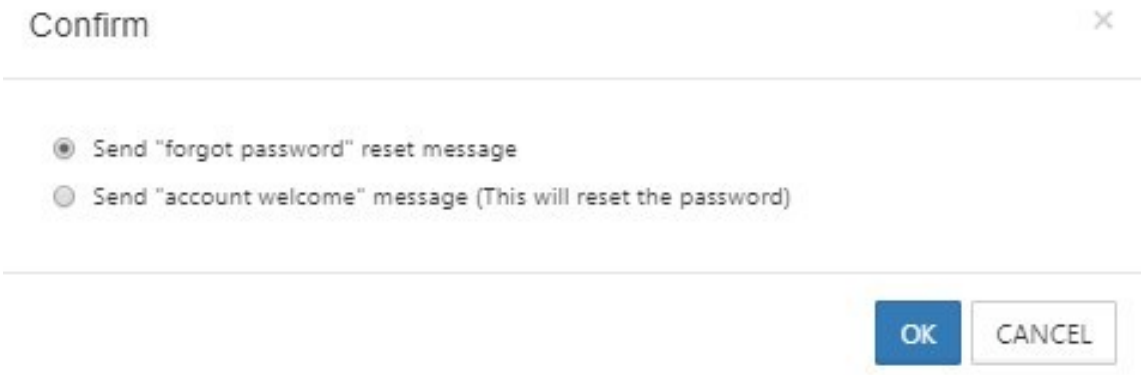


5. Click **Reset Password.**

6. Enter the new password in **Password** and **Confirm Password**.
7. Click **Save**.
   Note: If you want an email to be automatically sent to the user when you change their password, enable the **Send reset password email** setting in Password Settings and enter the text of the email.

OR

1. To change the password, and send the new password to the user, click **Send Email**.
   The following dialog box opens:



2. Choose **Send "forgot password" reset message**, and click **OK**.
   The new password is sent to the user

Manage A User's Policies

Administrators can manage users easily using policies.

- Policies provide a framework for managing settings at the user or group level
- One policy record manages multiple policy values
- The policy record can be associated with a user

Learn more about Policies

What do you want to do?

Select a Policy for a User

You can add a user to a policy to apply multiple settings at once and re-use settings for similar user scenarios.

For example, you can use a policy to set attributes for the following:

- Enable or Disable Printing in Mobile Apps
- Enable or Disable Configuration Changes in Clients
- Enable or Disable Two-Factor Authentication (2FA)

- Enable or Disable Notifications
- Enforce Session Timeout for Clients
- Set a Default Storage Quota
- Enable Privacy Settings

To select a policy for a user:

1. Open a browser and log on to the admin portal.
2. In the navigation panel, click **Users**.
3. In the **Manage Users** window, select a user, and then click the Edit icon.
4. In the **User Details** window, click **Manage Policy**.
5. Next to the **Selected Policy** box, click **Select**.
6. Choose a policy, and click **Select**.

Change or Remove a User's Policy

If you want to change a user's policy, you must remove the selected one first.

To remove a policy for a user:

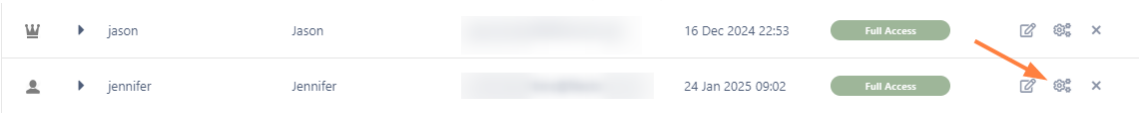
1. Open a browser and log on to the admin portal.
2. In the navigation panel, click **Users**.
3. In the **Manage Users** window, select a user, and then click the Edit icon.
4. In the **User Details** window, click **Manage Policy**.
5. Next to the **Selected Policy** box, click **Clear**.

Modifying a policy while managing a user

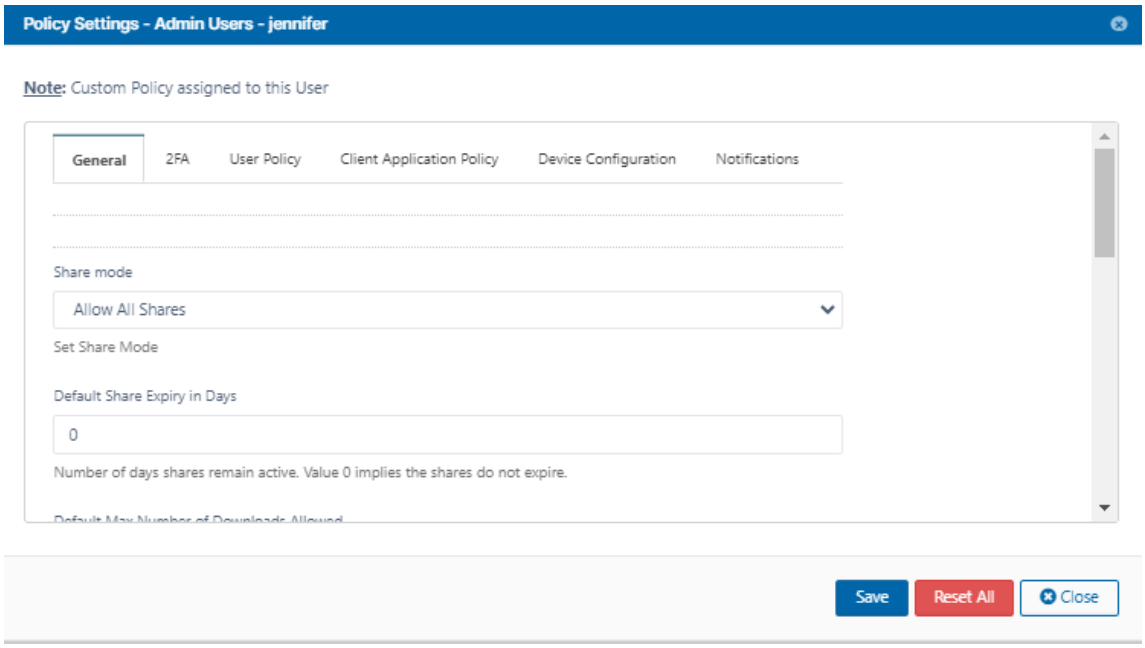
In the **Manage Users** page, in addition to viewing the details of the policy assigned to a user, you can edit the policy. However, if you edit the policy, the changes affect all users the policy is assigned to.

To edit a policy from a user account:

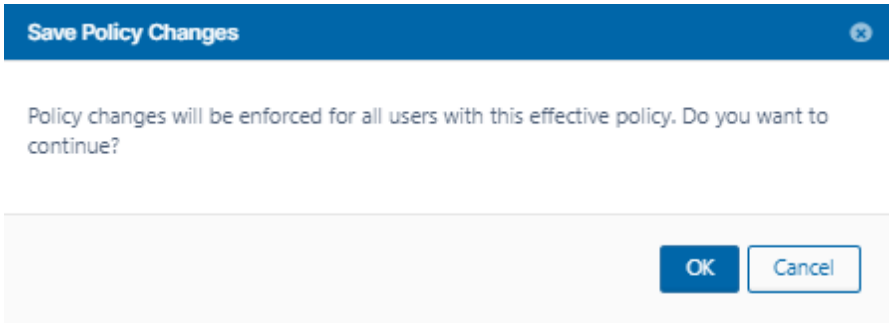
1. In the admin portal navigation panel, click **Users**.
   The **Manage Users** page opens.
2. Across from a user, click the Manage User Policy (gears) icon.



   The **Policy Settings** dialog box opens.
3. Change the settings on any of the tabs.



4. **Click Save.**
   A confirmation prompt warns you that this will change the policy for all users who are assigned to it.



5. Click **OK**.
   The policy is changed.

Calculate the Effectiveness of a User's Policy

An effective policy for a user is calculated on multiple factors.

This check is provided so you can see if group associations for this user changes how the policy you selected is enforced.

Learn more about Effective Policy Best Practices

To calculate the effectiveness of a policy for a user:

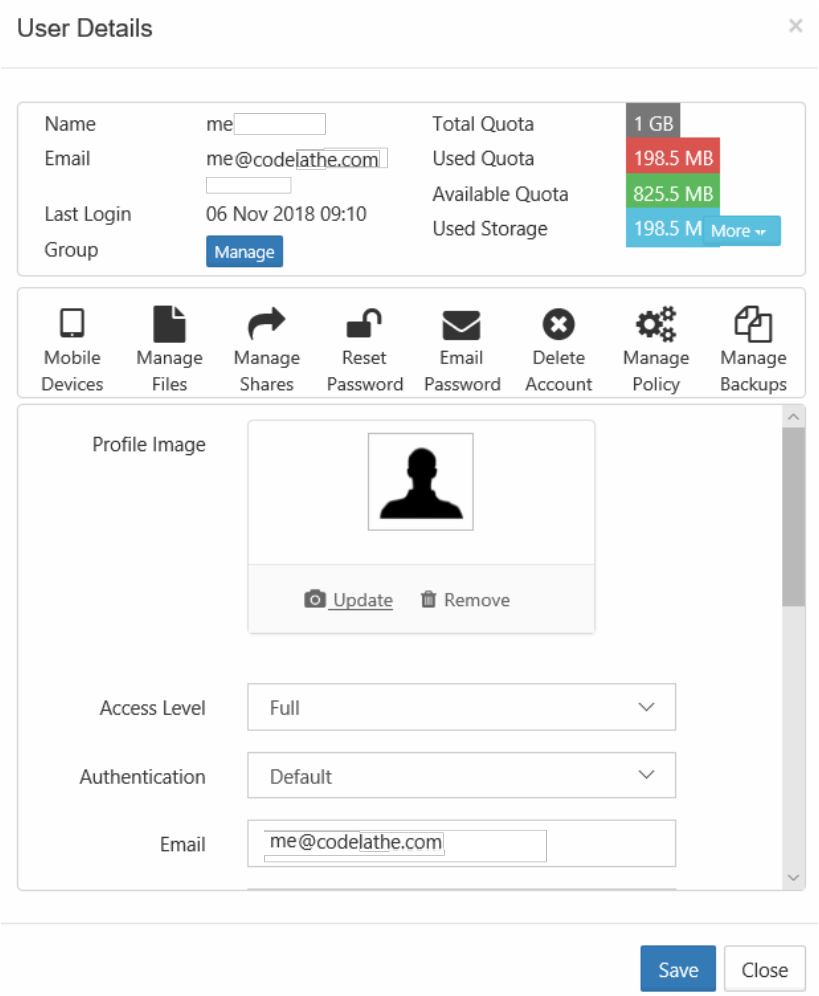
1. Open a browser and log on to the admin portal.
2. From the navigation panel, click **Users**.
3. In the **Manage Users** window, select a user, and then click the Edit icon.
4. In the **User Details** window, click **Manage Policy**.

5. Next to the **Effective Policy** box, click **Calculate**.
6. The most effective policy for this user is shown in the box next to the **Calculate** button.
7. To see the details of a policy, click **Open**.

Manage a User's Profile Picture

As a FileCloud administrator, you can update and remove a user's profile picture in the User Details screen.

If no profile image is chosen, the default is shown in the following figure:



To update a user's profile image:

1. Open a browser and log on to Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click the row containing the user whose picture you want to change.
4. Click the **edit icon.**

5. Next to **Profile Image**, to add an image, click **Update**.
6. Next to **Profile Image**, to remove an image, click **Remove**.

Change a User's Email Address

As a FileCloud administrator, you can update a user's email address when it changes.

- After you update the email address, the user's shared files and folder will be updated to display this new email address

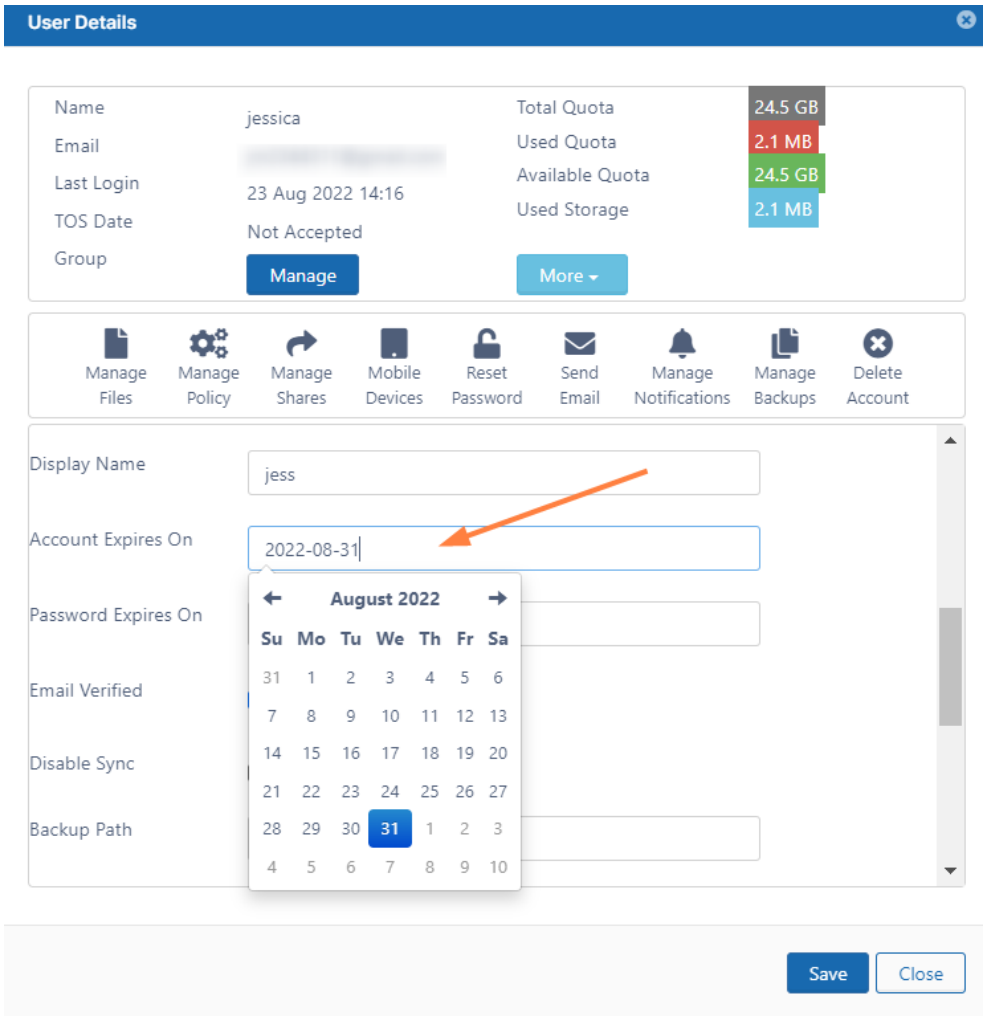
To change a user's email address:

1. Open a browser and log on to Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user.
4. Click the **edit icon** .
5. On the User Details screen, scroll down to the editable Email box.
6. Type in the new email address.
7. Click **Save**.

Setting a User Account to Expire

> The issue with an expiration date automatically changing to the day before has been fixed in FileCloud Server version 18.2 and later.

As a FileCloud administrator, you can set up a user account to be temporary, and configure it to expire.



To see a user's details and what they have permission to do:

1. Open a browser and log on to Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user.
4. Click the **edit icon** ( ).
5. Scroll down to see the **Account Expires On** field.
6. To see a calendar and select a date, click the text box.
7. To save your changes, click **Save**.

Send Email from User Details

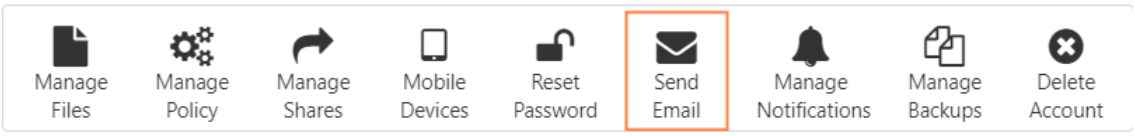
This option is available beginning in FileCloud 20.1

There are two types of emails you can send from the User Details window:

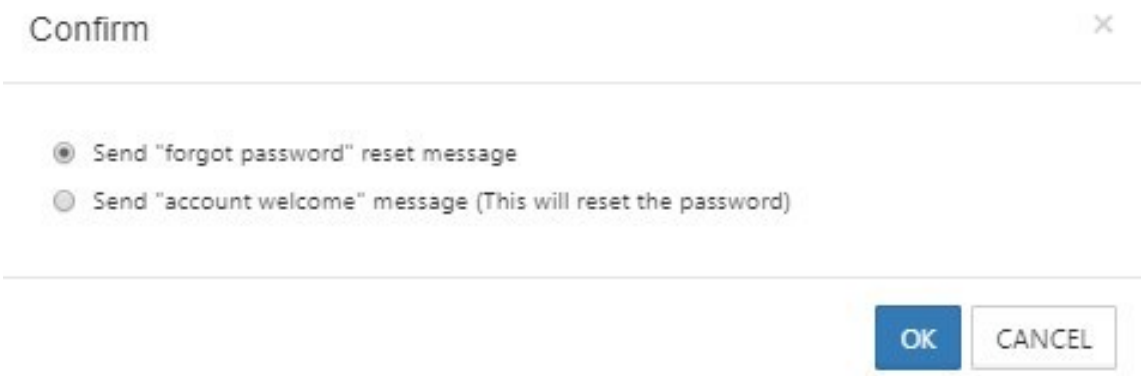
- A forgot password email that sends the user a password newly generated using the Reset Password option in User Details.
- An account welcome email that welcomes a new user to FileCloud. If the new user is not an AD user, the message includes a new password. If the new user is an AD user, the message does not include a new password.

To send an email from User Details:

1. Click **Users** in the navigation panel.
2. Locate the user in the user list.
3. Click the **edit** icon under **Actions** to the right of the user.
   The User Details window opens.
4. Click the **Send Email** icon.



   A dialog box for choosing the type of email opens.
   Note: If the user has an AD account, there is no option to send a "forgot password" message. The dialog box only sends an account welcome message that does not include a new password.



5. Select **Send "forgot password" reset message** or **Send "account welcome" message**
6. To send the message, click **OK.**

Managing Groups

A FileCloud Admin can manage User Groups.

Once a user group is created, the following operations can be performed:

- Change group details
- Delete a group
- View and Change Group members

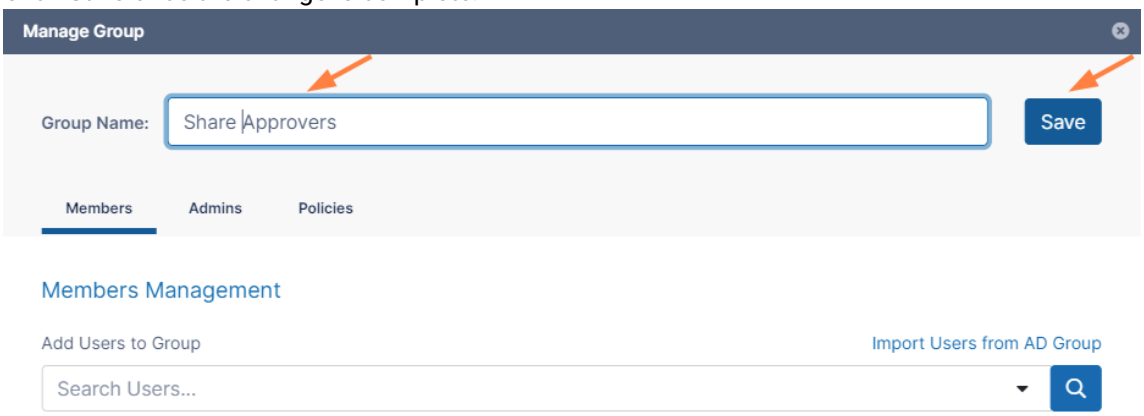
To add a group, see Group Settings.

Change a User Group Name

You can change any FileCloud group's name except for the **Everyone** and **Externals** groups.

To change a group's name:

1. Log on to admin portal.
2. In the navigation panel, click **Groups.**
3. Click the Edit icon for the desired group from the list of groups.
4. In the **Manage Group** dialog box, change the group name.
5. Click **Save** once the change is complete.

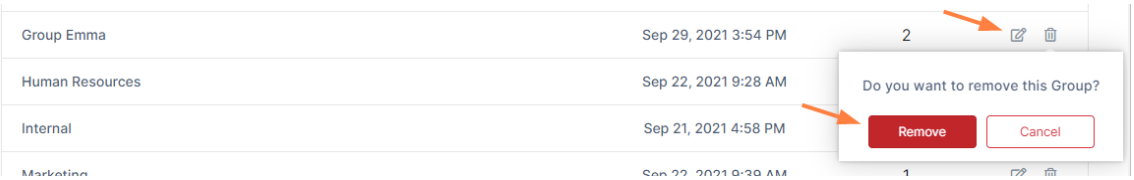


Delete a User Group

To delete a group:

1. Log on to the admin portal.
2. In the navigation panel, click **Groups.**
3. Click the Delete icon for a group to remove it from the list of groups.

4. Click **Remove** to confirm deletion.



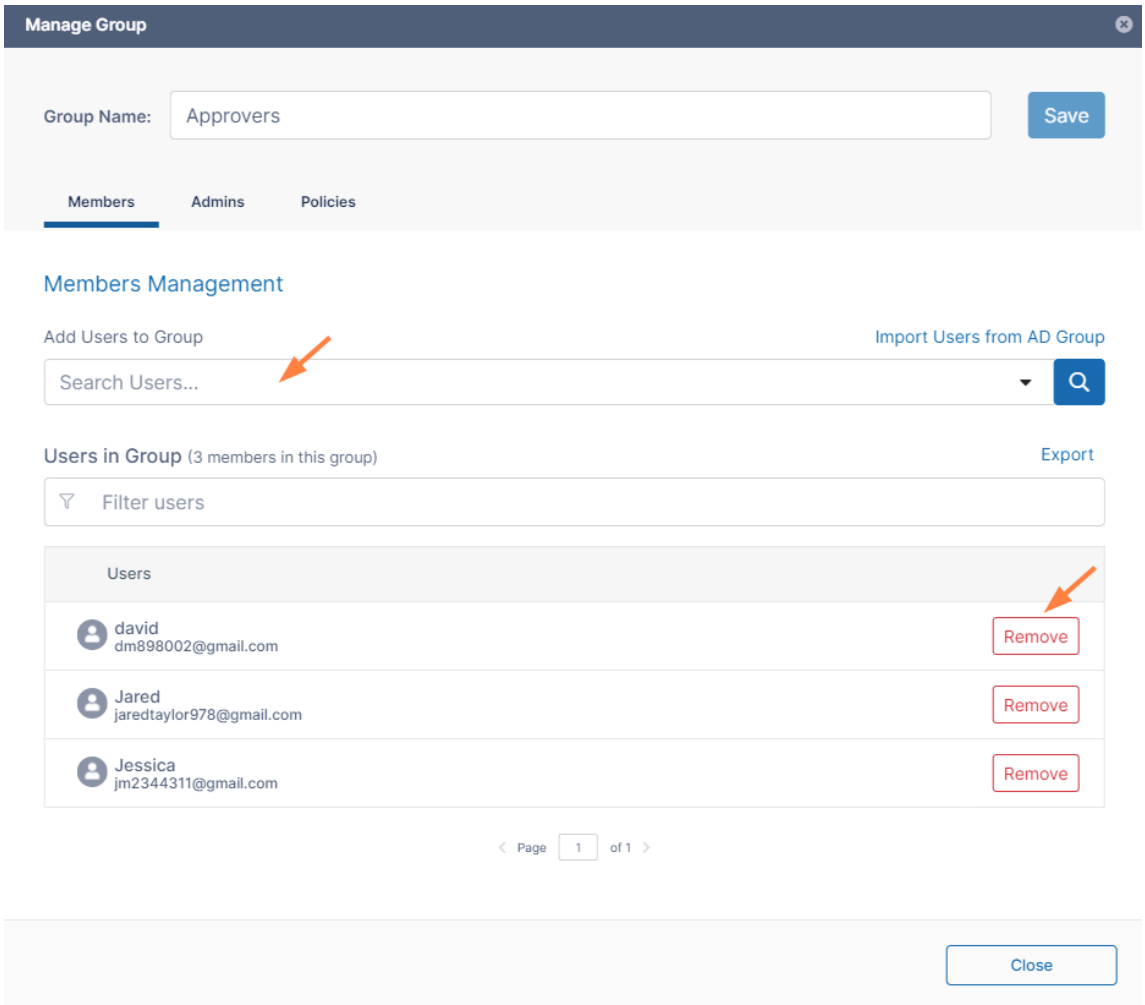
> Once a group is removed, network shares shared with that removed group will no longer be available to the former members of the group

View and Change Group Members

You can change the members in any FileCloud group except the **EVERYONE** and **EXTERNALS** groups.

To change a group's members:

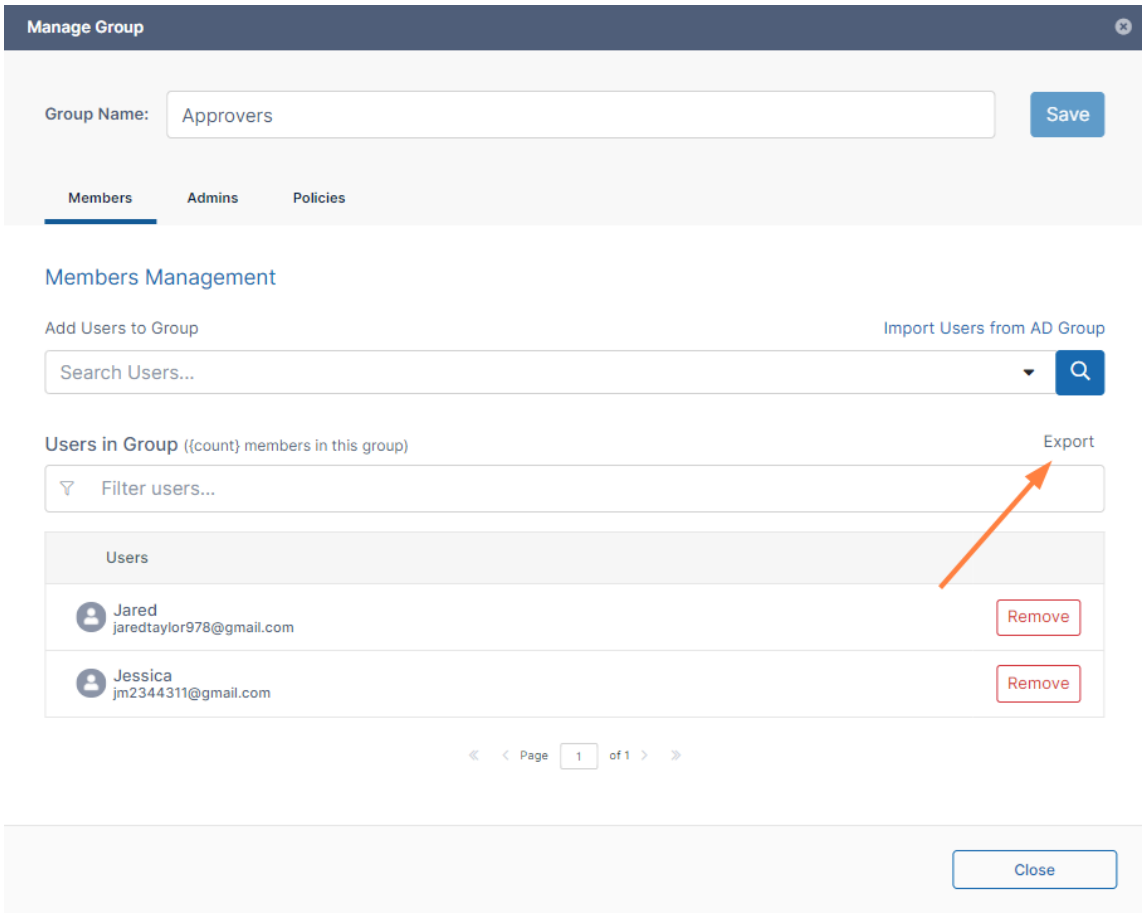
1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. In the **Members** tab, view the members of the group.
4. To add a member, enter an existing FileCloud user's name or email address in the search bar, and click **Add**.
5. To remove a user, click **Remove** next to the user's name.



Exporting a list of users in a group

To export a list of users in a group:

1. In the navigation pane, click **Groups**.
2. Click the Edit icon for a group.
3. In the **Members** tab of the **Manage Group** dialog box, click **Export**.



A csv file of users displaying the following fields is exported:

UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotific	LastLogin	Authentication	MobilePhone	Effective Policy
jaredtaylor978	[redacted]		Jared	FULL		EVERYONE, Human Resources Grou	YES	NO	10/18/2021 12:36	Default		Global Default Policy
jessicam	[redacted]		Jessica	FULL		EVERYONE, Internal, Human Resour	YES	NO	2/10/2022 14:08	Default		Global Default Policy

View and Change Group Admins

Group admins have the ability to add and/or remove users from the group. You can add, remove, and change the permissions of group admins in the Admins tab. A user's policy also may enable them to add and/or remove users from groups.

To modify group admin settings:

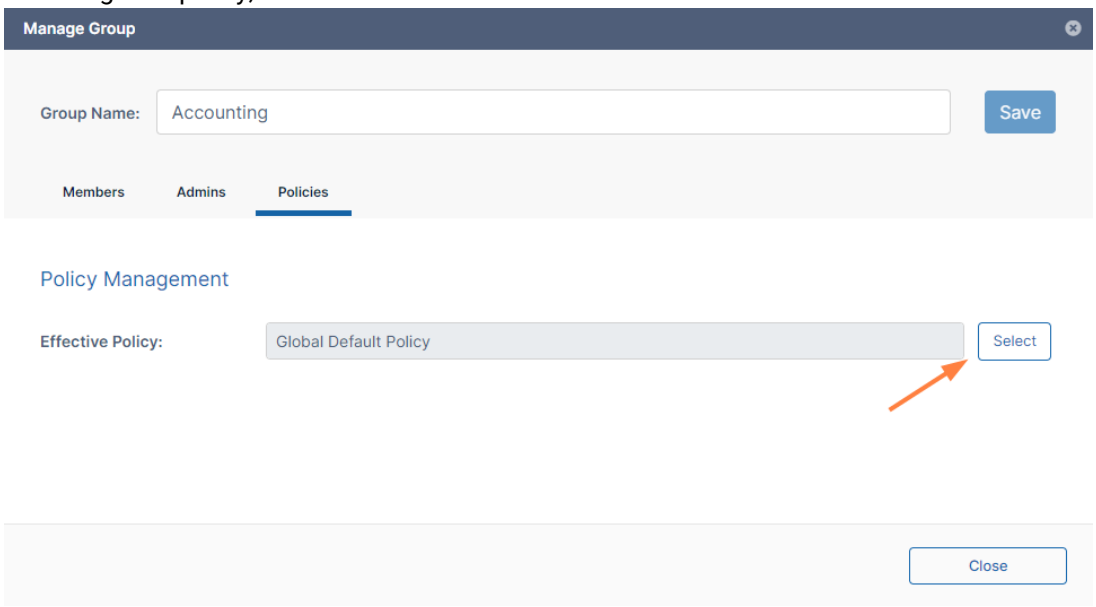
1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. In the **Admins** tab, view the admins of the group.
4. To add an admin, enter an existing FileCloud user's name or email address in the search bar, and click **Add**.
5. To remove an admin, click **Remove** next to the admin's name.
6. To change an admin's permissions, check or uncheck **Can add users** or **Can remove users**.

To import an AD group into a FileCloud group, see Group Settings

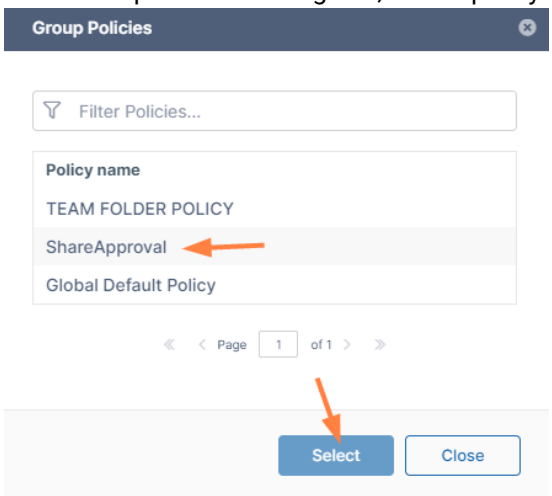
View and Change a Group's Policy

To change a group's policy:

1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. Click the **Policies** tab to view the group's policy.
4. To change the policy, click **Select**.



5. In the Group Policies dialog box, click a policy and click **Select**.



The policy is changed.

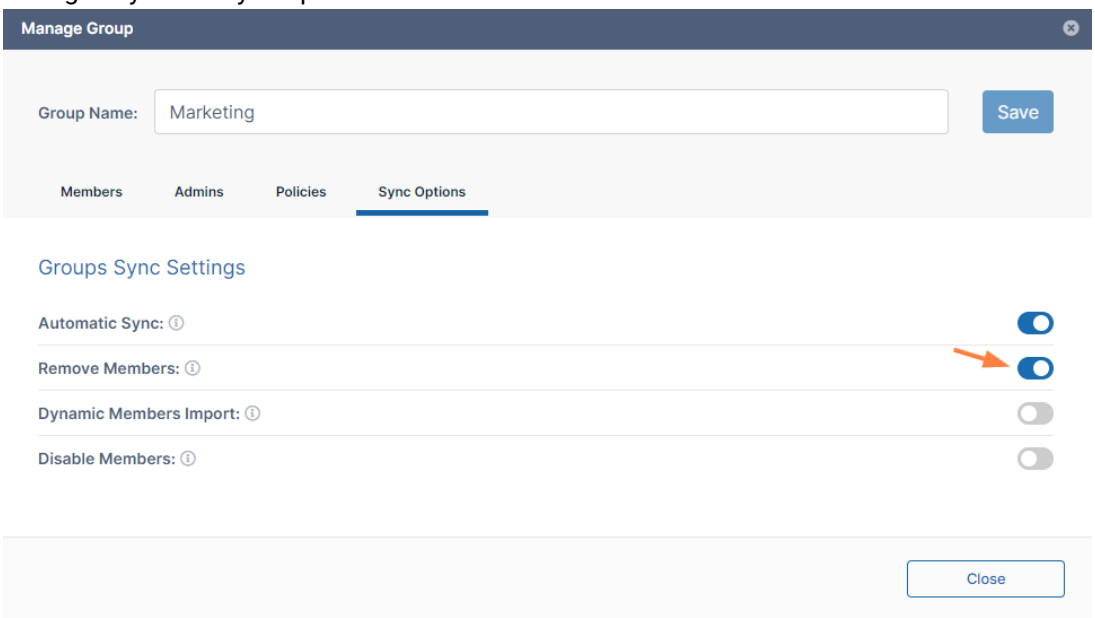
6. Click **Close**.

View and Change an SSO-imported Group's Sync Options

Groups that are imported from SSO providers have an additional tab in the **Manage Group** dialog box with options for syncing FileCloud with the SSO provider.

To change an SSO-imported group's synchronization options:

1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. Click the **Sync Options** tab to view the group's sync options.
4. Change any of the sync options.



Their functions are as follows:

Automatic Sync	Enabled by default. FileCloud periodically imports new users from the group in the SSO provider to the group in FileCloud.
Remove Members	Disabled by default. The group and its permissions are imported without its users. When a member of the group logs into FileCloud for the first time, the member is automatically placed into the group.
Dynamic Members Import	Disabled by default. Users are automatically placed into the correct groups when they are imported.
Disable Members	Disabled by default. FileCloud users that are disabled in the SSO group are also disabled in the FileCloud group.

5. Click **Close**.

Managing Admin Users

FileCloud enables you to create admin roles with a set of administrator permissions. Users assigned to any of the admin roles that you have created become admin users and have the permissions assigned to the role.

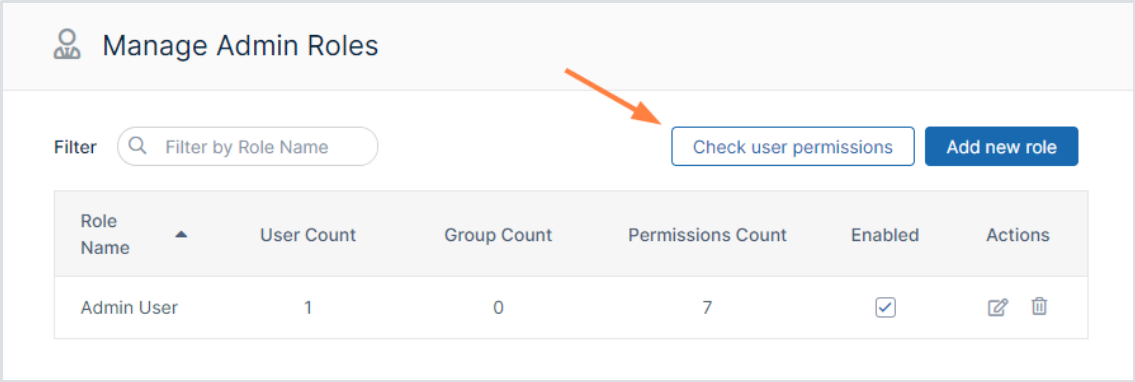
For information on about admin roles and admin users and instructions for setting them up, see Admin User and Role Settings.

Check an admin user's permissions

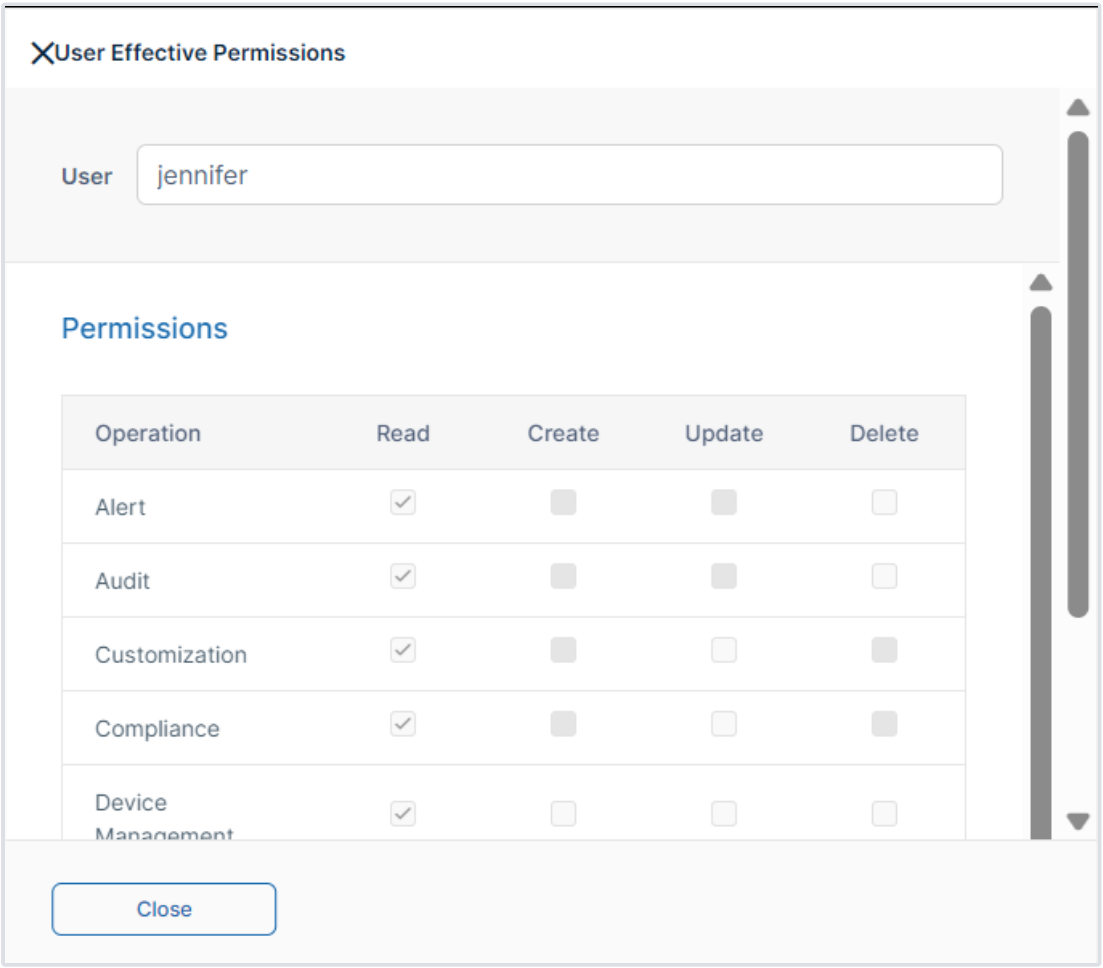
If an admin user has one role, the user has the permissions assigned to that role, but if an admin user has multiple roles, the user has the combined permissions of all of its roles.

To check all of a user's permissions:

1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Check user permissions.**



   The **User Effective Permissions** dialog box opens.
3. In **User**, enter the name of the user.
   The dialog box displays the user's combined permissions with checks next to them.



For definitions of the permissions, see page Admin User and Role Settings .

Remove an admin role

When you remove an admin role, you permanently delete it. To recreate it, you must create it, assign all permissions, and add users and groups again.

To remove an admin role:

1. Click **Admins** in the navigation panel.
2. Either
   - In the **Manage Admin Roles** screen, click the **Delete** button for the role, and then click Remove Role when you are prompted to confirm removal.
     Or:
   - In the **Manage Admin Roles** screen, click the **Edit** button for the role, and click **Remove Role** at the bottom of the dialog box.
3. Click **Remove** when you are prompted to confirm removal.

Managing User Folders and Files

As an administrator, you can manage the files that are stored on your FileCloud Server site.

This allows you to protect and maintain your system in the following ways:

- Remove user files infected with a virus
- Remove files belonging to a user that no longer has an account
- Move folders for teams
- Download, copy and move files at a user's request
- Manage your storage space limits by moving or deleting files
- Copy and move files and folders between two FileCloud users

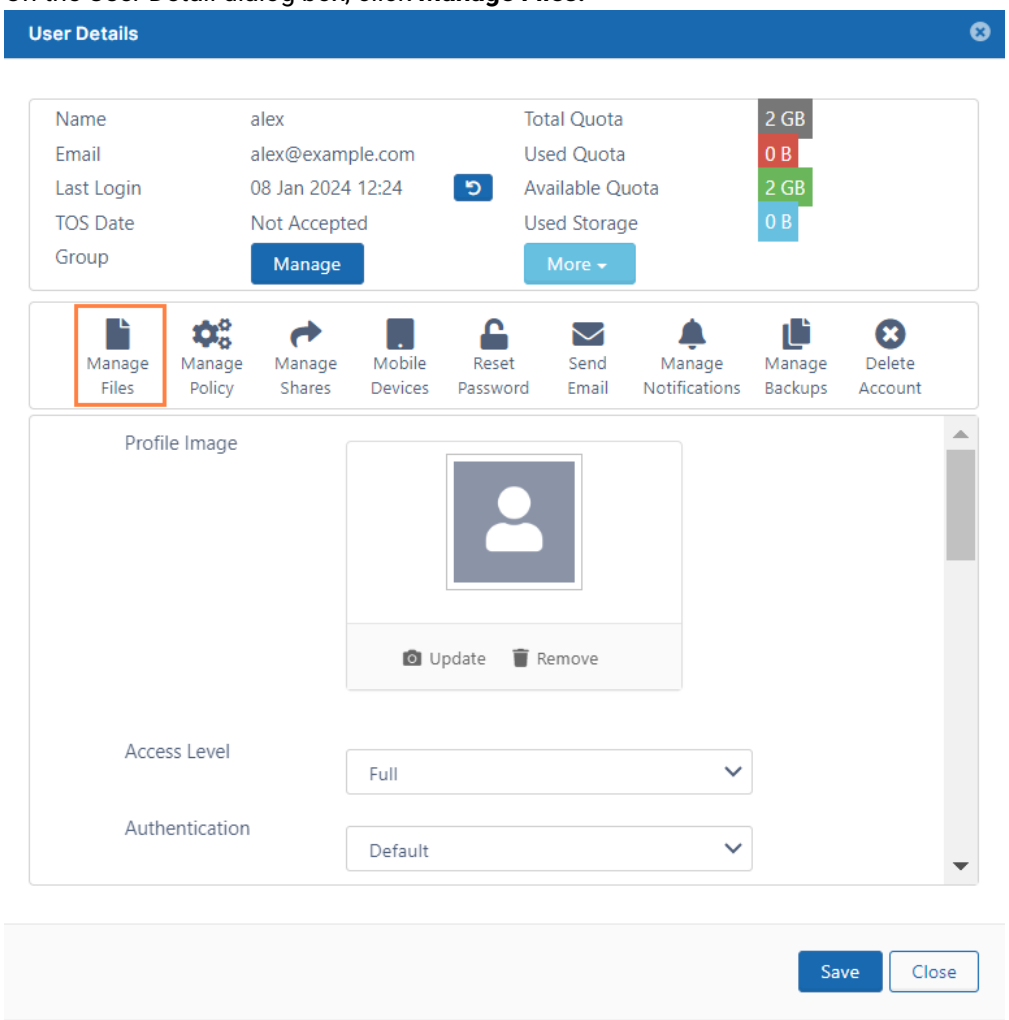
How do I access user storage management settings?

To access user folder and files settings:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon

   .

4. On the User Detail dialog box, click **Manage Files.**



5. The Manage Files for <User> window opens.

In this section:

Add Folder-Level Permissions to User Folders

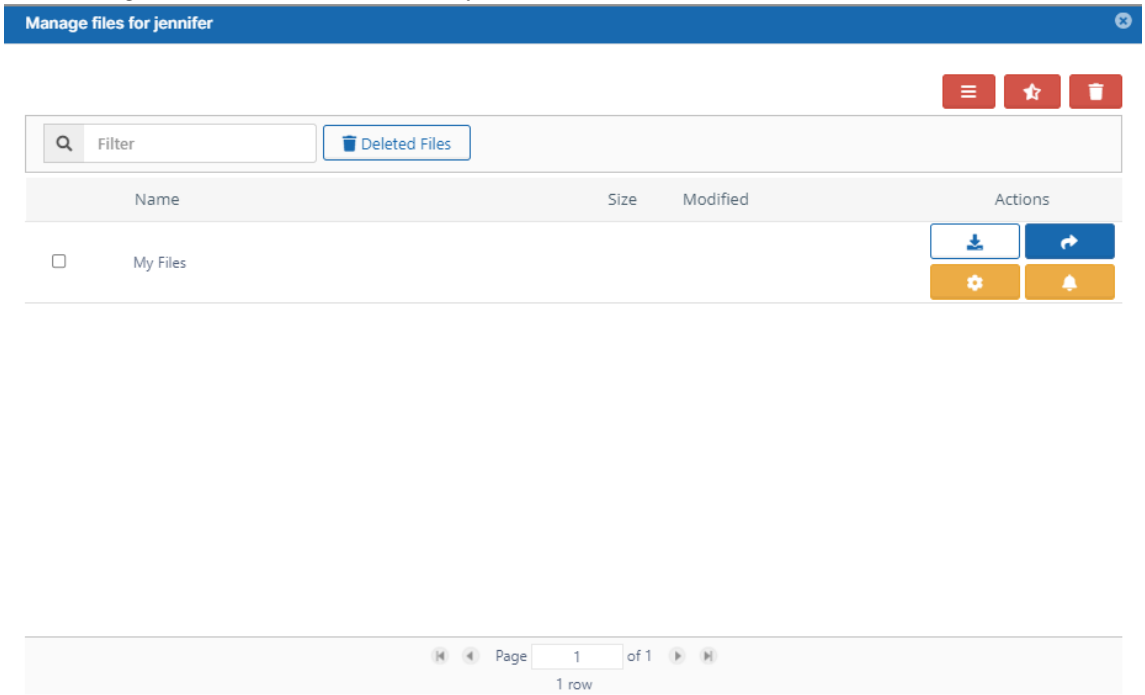
Folder-level permissions are permissions that are applied directly to a folder. They add additional restrictions to the share permissions when the folder is shared. Note that whatever is more restrictive, folder-level or share permissions, apply. For more information, see Folder-Level Permissions.

From the **Manage Users** page, you can access a user's details and edit permissions that are applied directly to a folder.

To assign folder-level permissions to users' folders:

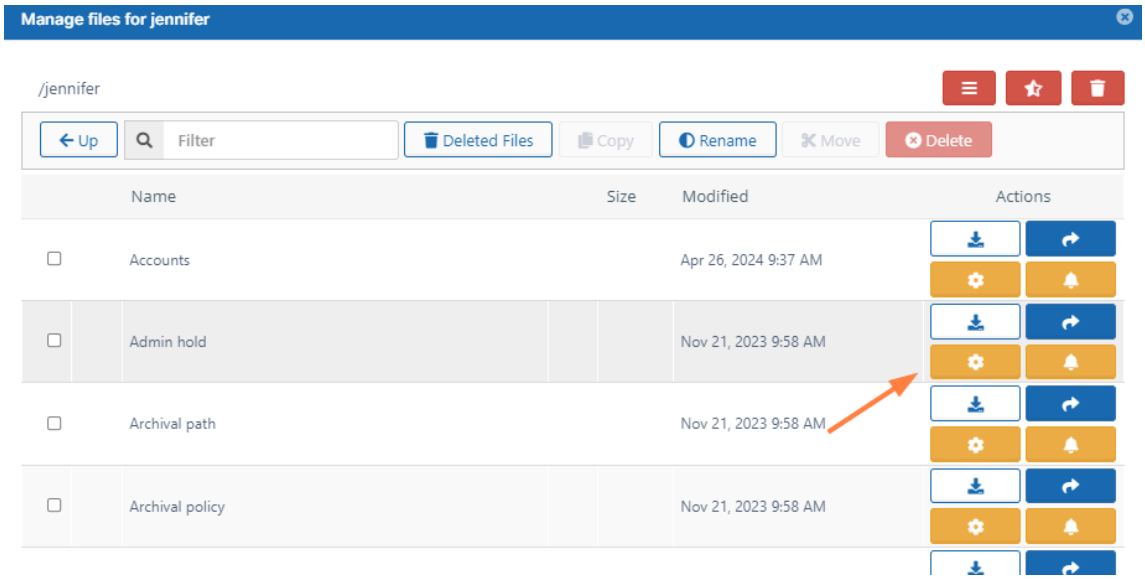
1. In the admin portal's left navigation panel, click **Users**.

2. On the **Manage Users** page, select a user, and then click the Edit icon.
3. On the **User Details** dialog box, click **Manage Files.**
   The **Manage Files for <User>** window opens.



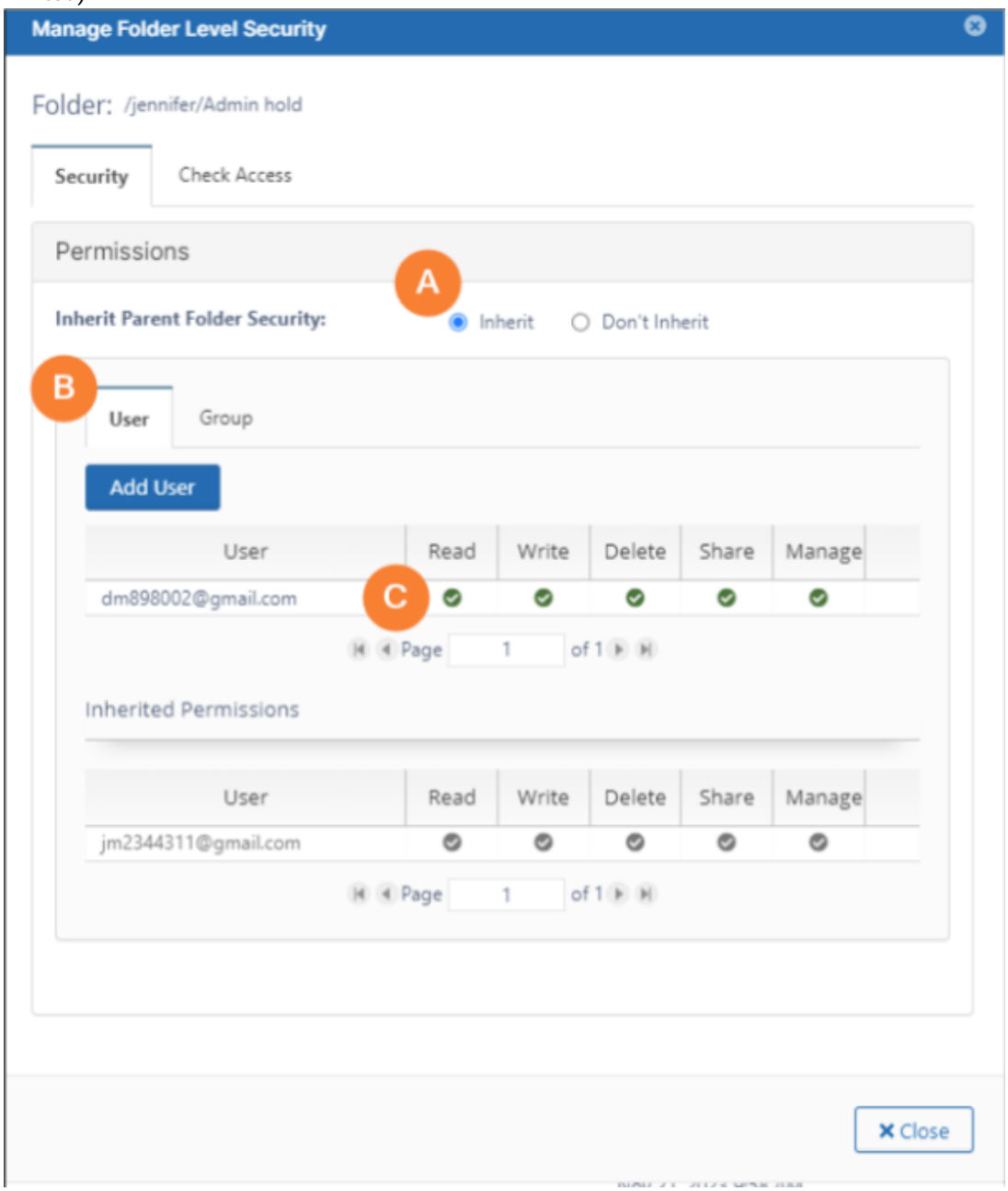
4. Expand **My Files** and locate the folder that you want to set folder-level permissions for.
5. Click the **Manage Access**

   button in the folder's row.



The **Manage Folder Level Security** dialog box opens. Any folder-level permissions that are already effective appear.

6. Follow the steps below to assign and change user and group folder-level permissions. Users who do not appear
on the list have all folder-level permissions to the folder (unless their group permissions are limited)



A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.
B Click **Add User** to add a user and limit their access to the folder, or click the Group tab and add a group.
C In the top list of users, check or uncheck levels of permissions.

Copy and Move User Files

> This action will be recorded in the Audit log as:
> "Action performed by ADMIN"

As an administrator, you can copy and move user files that are stored on your FileCloud Server site.

This allows you to protect and maintain your system in the following ways:

- Move folders for teams
- Download, copy and move files at a user's request
- Manage your storage space limits by moving or deleting files
- Copy and move files and folders between folder locations for the same user account

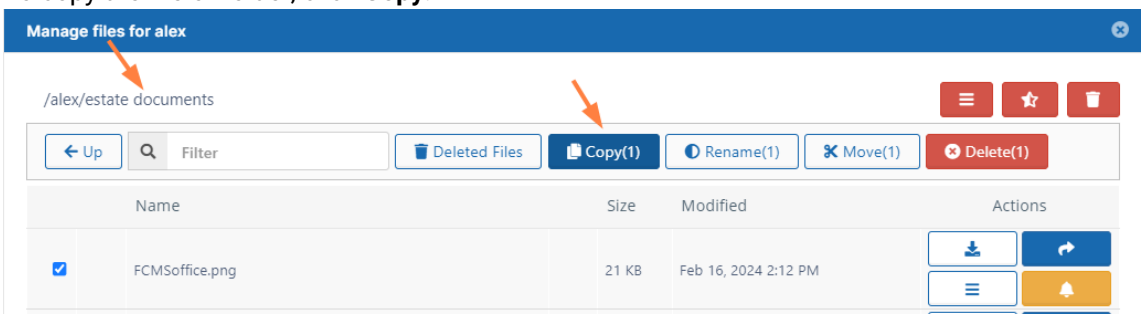
What is the difference between copy and move?

Copying a file will allow you to have the same file in two different locations.

Moving a file will allow you to put the file in a new location so it can be removed from the original location.

To copy and paste files and folders between a user's folder locations:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon .
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the folder or file you want to copy.
6. To select the file or folder, click the checkbox next to the name.
7. To copy the file or folder, click **Copy**.

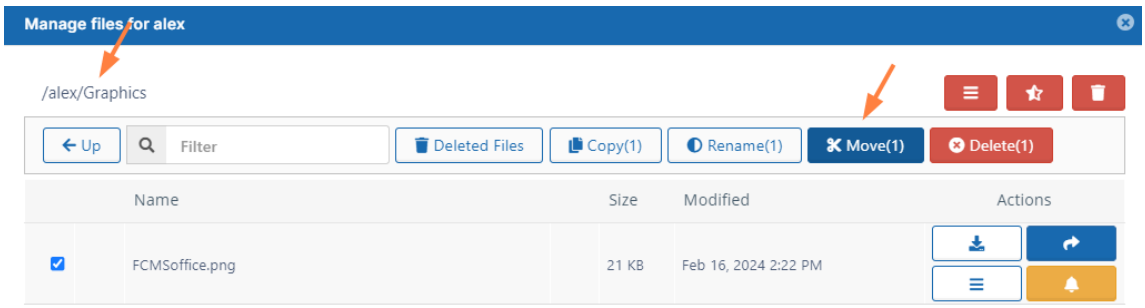


8. Navigate to the folder where you want to paste the copy.
9. Click **Paste**.

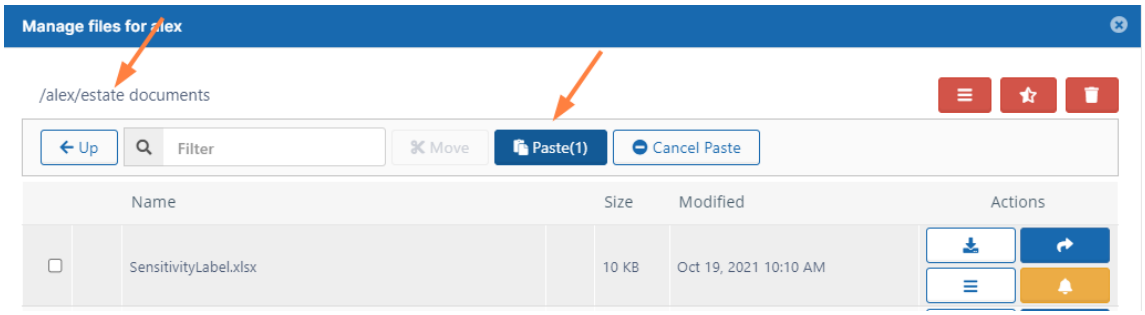
To move and paste files and folders between a user's folder locations:

1. Open a browser and log on to the Admin Portal.

2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the folder or file you want to move.
6. To select the file or folder, click the checkbox next to the name.
7. To move the file or folder, click the **Move** button.



8. Navigate to the folder where you want to paste the original file or folder.
9. Click **Paste**.



Download User Files and Folders

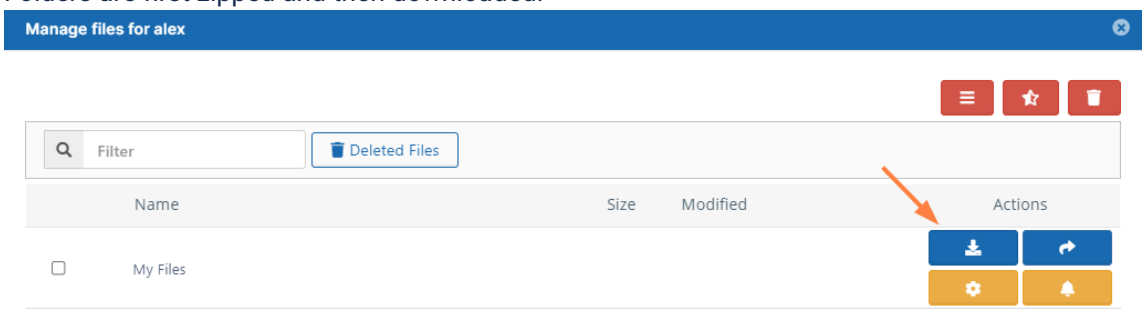
> To disable users' ability to download folders from the user portal, see the setting **Disable Folder Download** at General Customization.

As an administrator, you can manage the files that are stored on your FileCloud Server site. This allows you to protect and maintain your system.

Can I download all of a user's files at once?

- You can easily download all of a user's files by downloading the My Files folder.

- Folders are first zipped and then downloaded.

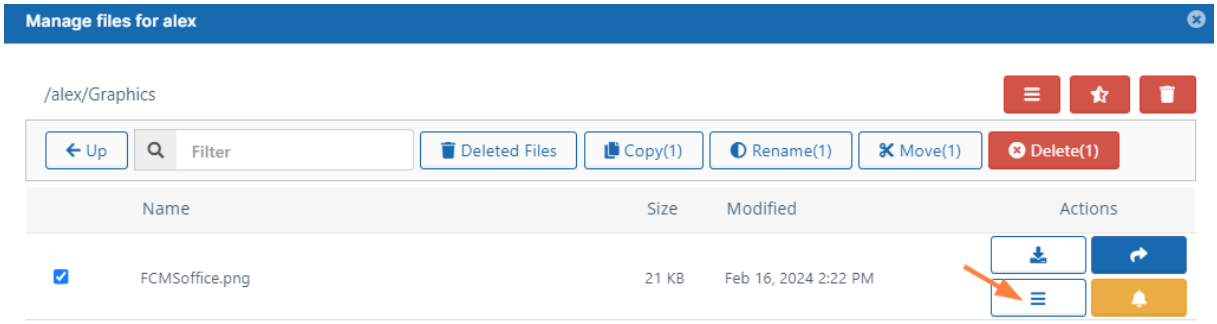


Can I download an older version of a file?

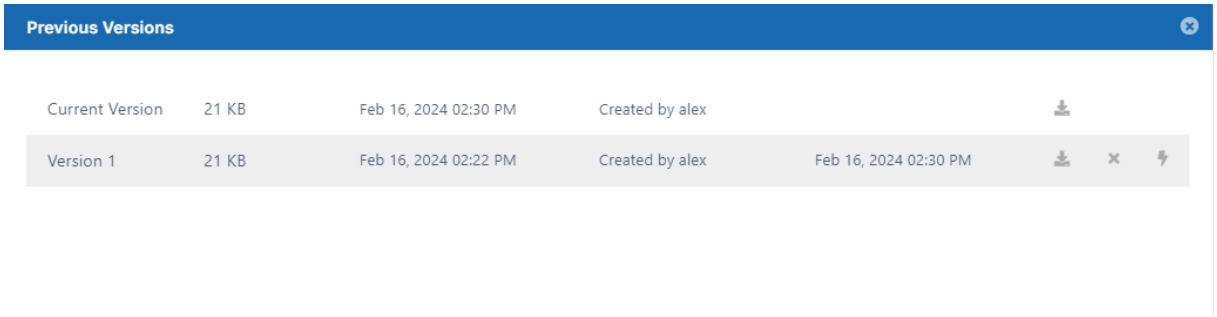
If the user has uploaded changes to a file, you can:

- download the latest version
- download a previous version

In the **Manage files** dialog box, click the **Versions** button.



Find the version you want to download and click its **Download** icon.

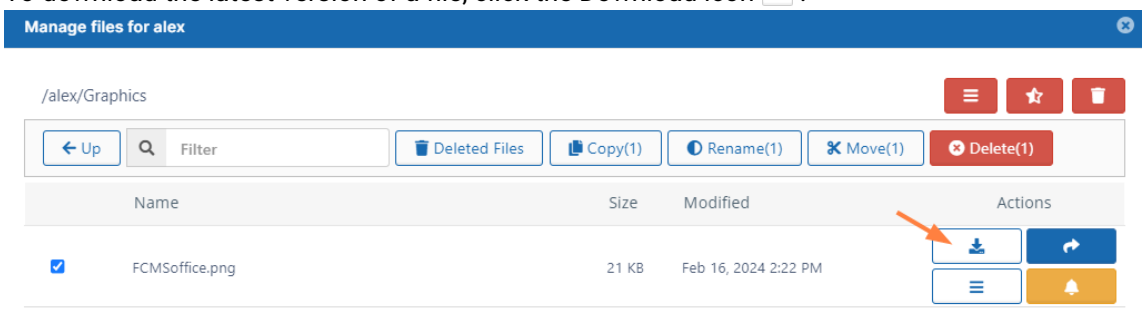


If you have older versions on your site, you may:

- Restore the previous version of a file and make it live
- Remove previous versions to save space

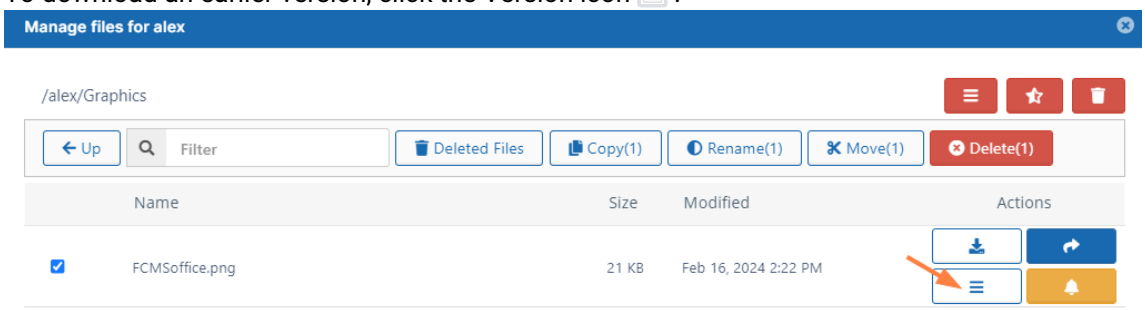
To download user folder and files:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon .
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the folder or file you want to download.
6. To download the latest version of a file, click the Download icon .

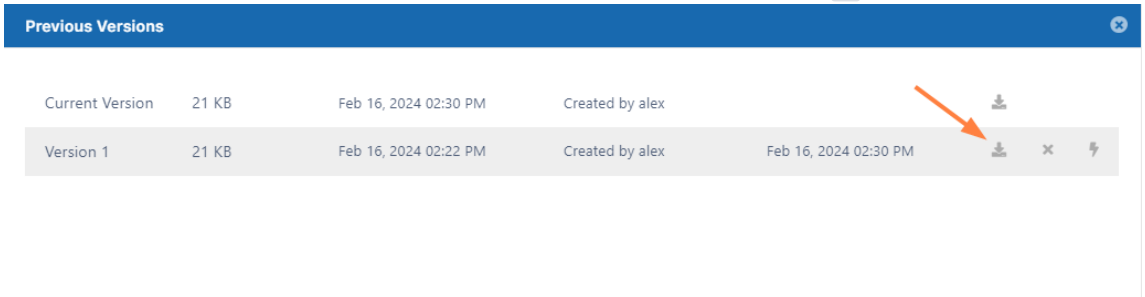


OR

To download an earlier version, click the Version icon .



Then select the version from the list and then click the Download icon .



Cancel User Uploads in Progress

This action:

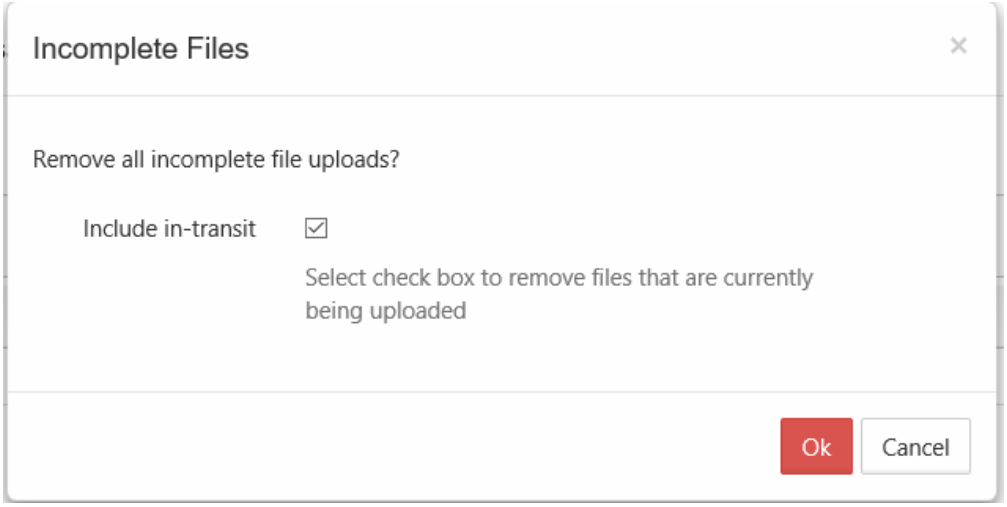
- Is recorded in the Audit log as: "Action performed by ADMIN"
- Cannot be undone

As an administrator, when a user is uploading a file and you want to cancel the upload, if it is only partially completed, you can cancel it using the Remove All Incomplete Uploads button using the Include in-transit option.

- This is useful if you discover the file is infected and want to stop the upload
- If the file is too large or contains inappropriate content, you can cancel the upload before it completes

To stop all partial user uploads from completing:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Click the Remove all incomplete uploads icon .
6. On the Incomplete Files dialog box, select the Include in-transit checkbox.



7. Click OK.

Delete User Folders and Files

> This action is recorded in the Audit log as:
> "Action performed by ADMIN"

As an administrator, you can manage the files that are stored on your FileCloud Server site.

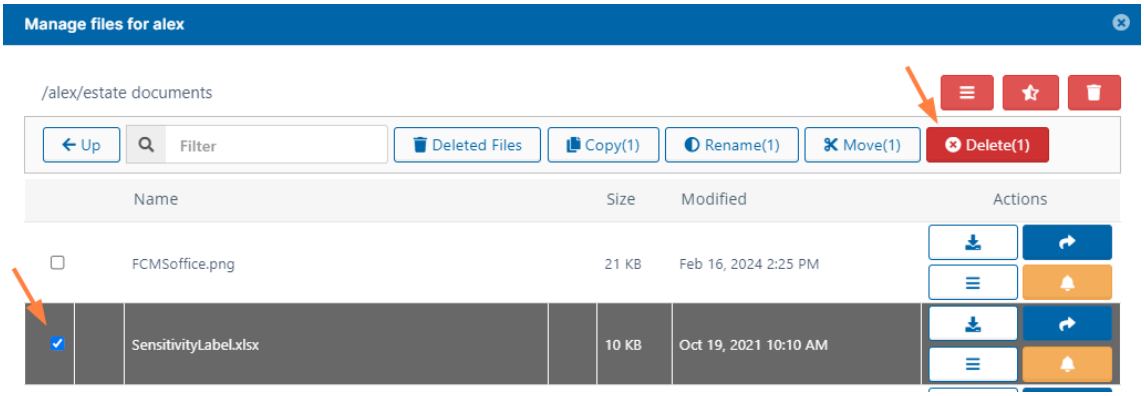
This allows you to protect and maintain your system in the following ways:

- Remove user files infected with a virus
- Remove files belonging to a user that no longer has an account
- Manage your storage space limits by moving or deleting files

Deleting a file or folder moves it to the Deleted Files recycle bin. To permanently remove a file, you must clear if from the recycle bin.

To delete files and folders:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the folder or file you want to delete.
6. To select the file or folder, click the checkbox next to the name.
7. Click the **Delete** button.



8. On the **Confirm** dialog box, click **OK**.

Clear a Recycle Bin

This action:

- Is recorded in the Audit log as: "Action performed by ADMIN"
- CANNOT be undone

As an administrator, you can delete a user's files and folders.

After you delete files and folders, they are normally placed in the user's Recycle Bin, which you can also manage.

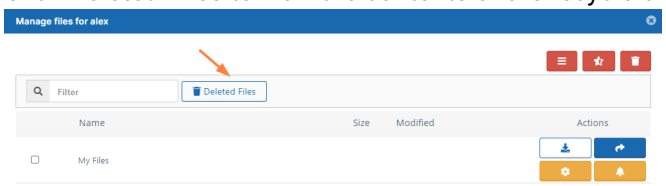
- If you have a policy that stores deleted files, they are saved in the Recycle Bin
- This means that they can be recovered if deleted by mistake or are needed again at a later time
- You can also set the Recycle Bin to automatically delete through a policy

Manage the Recycle Bin Using a Policy

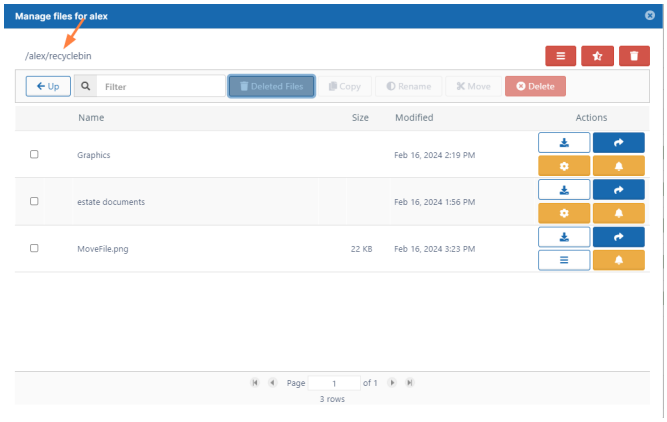
Go the the recycle bin

To go to a user's recycle bin:

1. In the Admin portal, go to the **Users** page, select a user, and click the edit icon. In the **User Details** dialog box, click **Manage Files.**
2. Click **Deleted Files** to view the contents of the recycle bin:



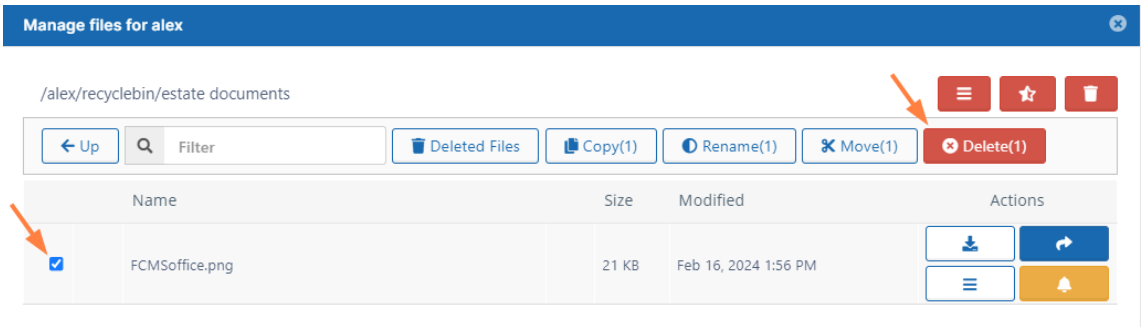
The recycle bin opens and displays deleted files. If the deleted files are in subfolders, navigate into the subfolders to locate them.



Clear a deleted file or folder

To clear a deleted file or folder from a user's recycle bin:

1. Follow the steps above to go to the recycle bin.
2. Navigate to the file or folder you want to delete from the recycle bin.
3. Check the file or folder.



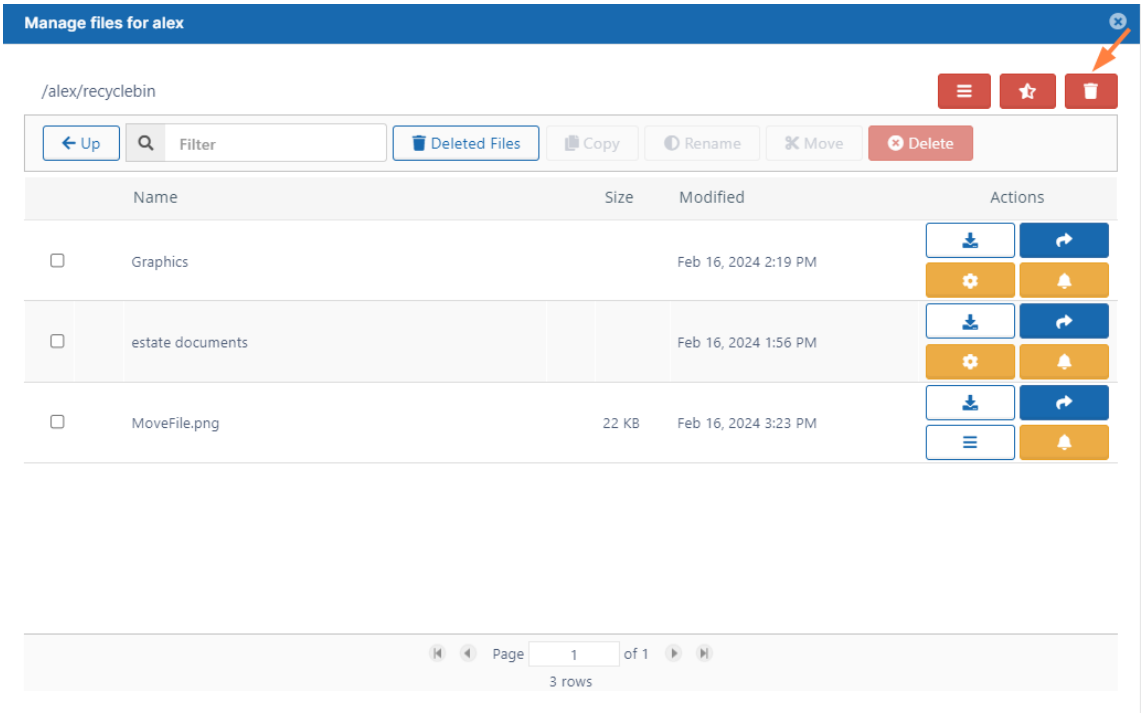
4. Click **Delete**.
5. In the **Confirm** dialog box, click **Yes**.
   The file or folder is deleted from the recycle bin (permanently removed from FileCloud).

Clear all deleted files

> Only recycle bins with contents less than 16 MB of data can be cleared using this method.

To clear all files and folders from a user's recycle bin:

1. Follow the steps above to go to the recycle bin.
2. Click the trash icon in the upper right corner.



3. In the **Confirm** dialog box, click **OK**.
   All files and folders are deleted from the recycle bin (permanently removed from FileCloud).

Remove a User's Old File Versions

> This action:
> - Is recorded in the Audit log as: "Action performed by ADMIN"
> - CANNOT be undone

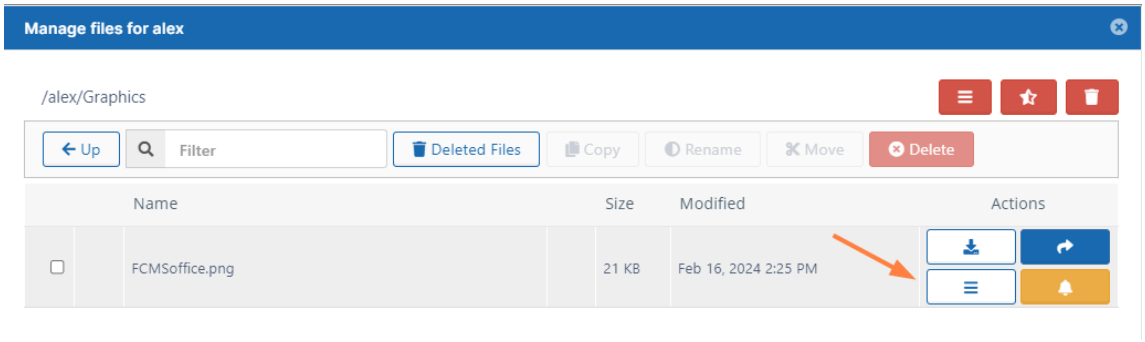
As an administrator, you can delete older versions of files that are stored on your FileCloud Server site.

- This allows you to free up space when previous versions of a file are not needed anymore.
- This can also be used to clean up storage space for users who no longer have a FileCloud Server account for your site.

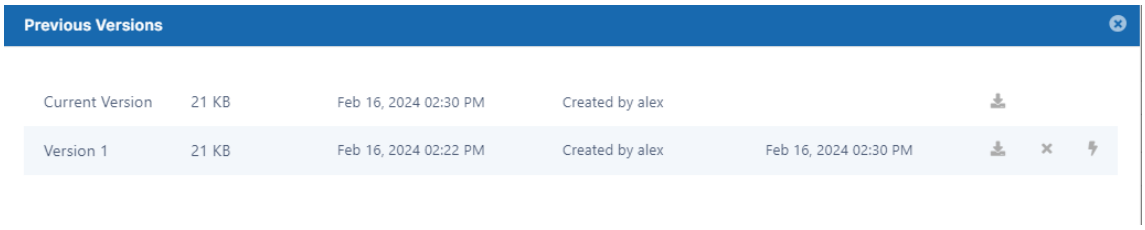
This action does not remove the current version of a file, only all older versions saved on the FileCloud Server.

How do I know if there are previous versions of a file?

1. Open a browser and log on to the admin portal.
2. From the left navigation menu, select **Users**.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the file.
6. Click the Previous Versions button.

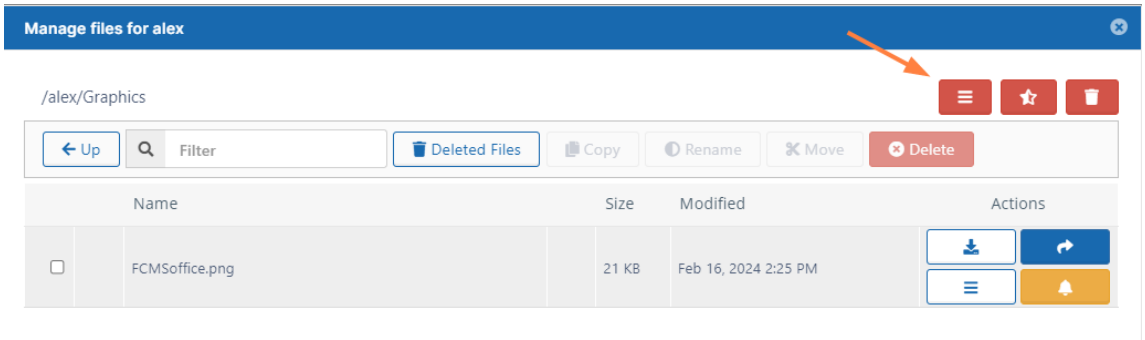


If there are previous versions they appear in the listing that opens:



To remove all old versions of a file:

1. Open a browser and log on to the admin portal.
2. From the left navigation menu, select **Users**.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   The Manage Files for <User> window opens.
5. Navigate to the file.
6. Click the Remove All Old Versions icon.



7. In the **Confirm** dialog box, click **OK**.
   All old versions of the file are deleted.

Remove Incomplete User Uploads

This action:

- Is recorded in the Audit log as: "Action performed by ADMIN"
- CANNOT be undone

As an administrator, you can remove files that were not completely uploaded. This can free up storage space.

If a user tries to upload a file and for some reason the action is only partially completed, the file is saved in a folder for partial uploads.

- Partial uploads are saved in case a network connection is lost and the user wants to continue the upload when connectivity is restored.
- Incomplete user uploads are never shown in the Manage Files listing.
- Over a period of time, these partial uploads can occupy lots of space.
- Admins can easily remove these partial uploads with the click of one button.

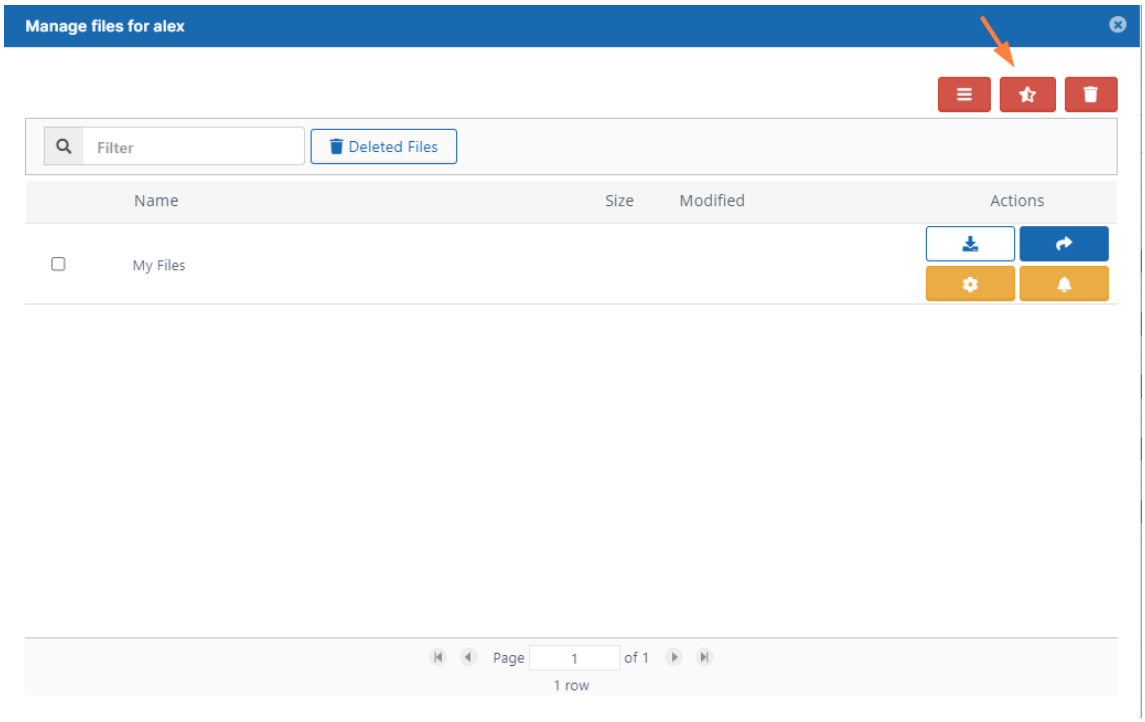
💡 If a file upload is in progress:

- It will not be removed, even if it only partially uploads, unless you use the In-transit option when removing partial uploads
- You can use the In-transit option to cancel a partial upload in progress

Cancel a Partial Upload

To remove all incomplete user uploads:

1. Open a browser and log in to the admin portal.
2. From the left navigation menu, select **Users**.
3. On the **Manage Users** page, select a user, and then click the Edit icon.
4. In the **User Detail** dialog box, click **Manage Files.**
   The **Manage Files for <User> window opens.**
5. Click the Remove All Incomplete Uploads icon
   .



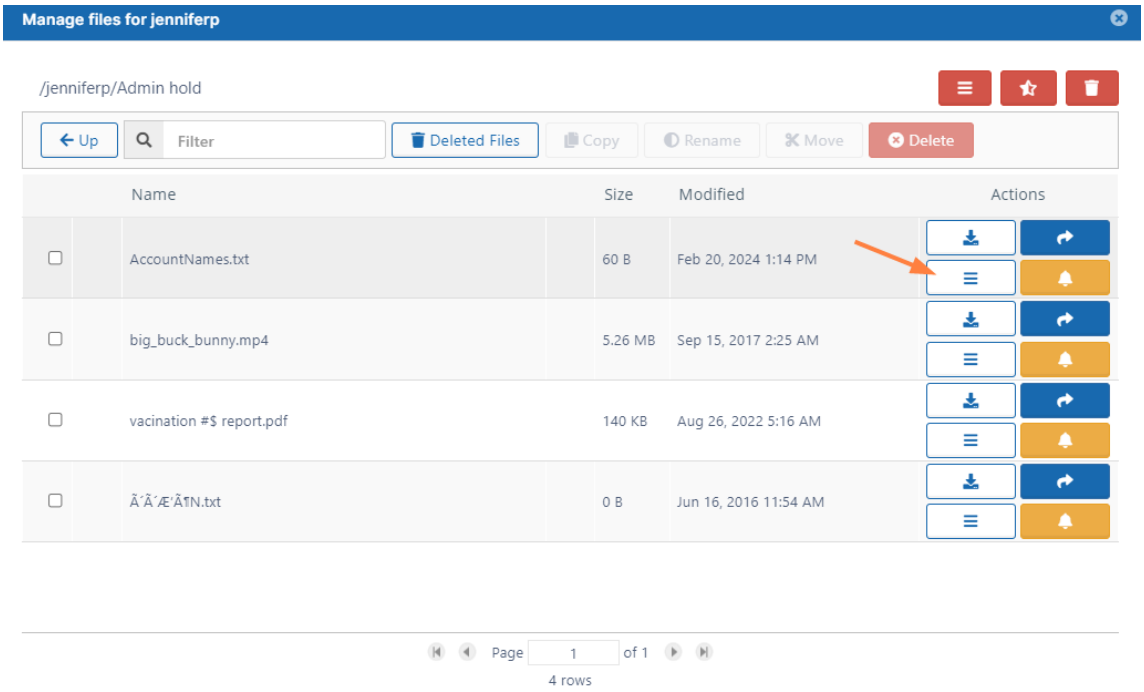
6. On the **Incomplete Files** dialog box, to also remove incomplete uploads in progress, select Include in-transit.
7. Click **OK**.
   Incomplete downloads are removed.

Restore a Previous File Version

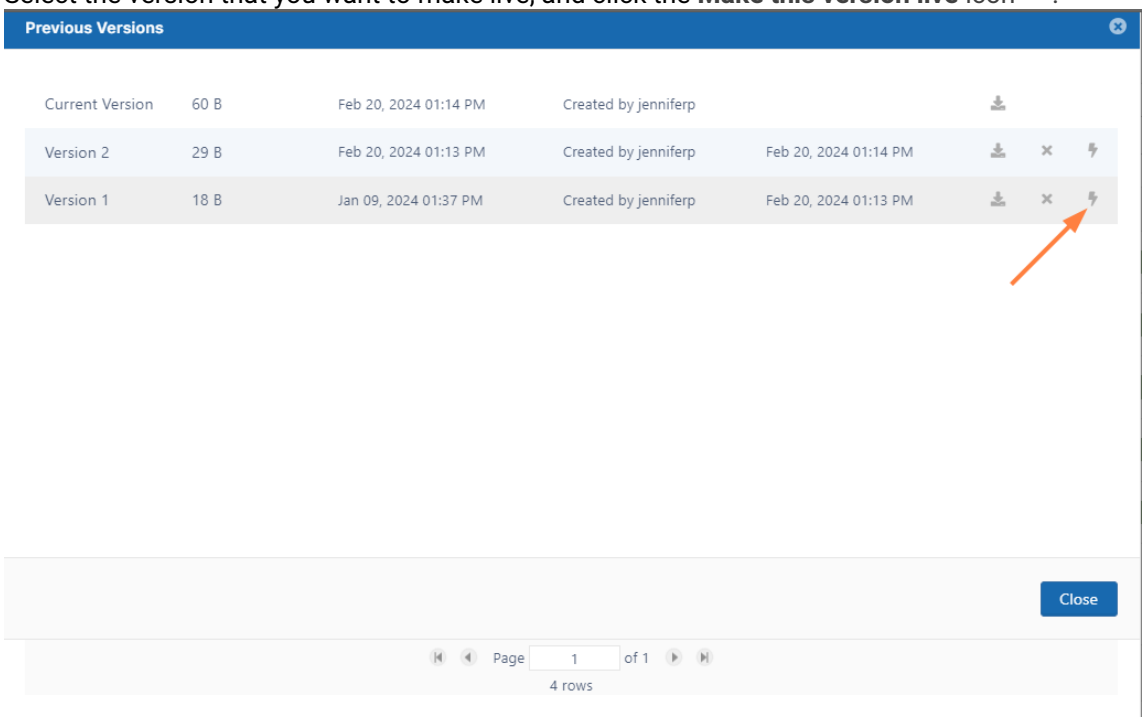
If a user has uploaded changes to a file, you can restore the previous version of a file and make it live.

To restore a previous version of a user's file:

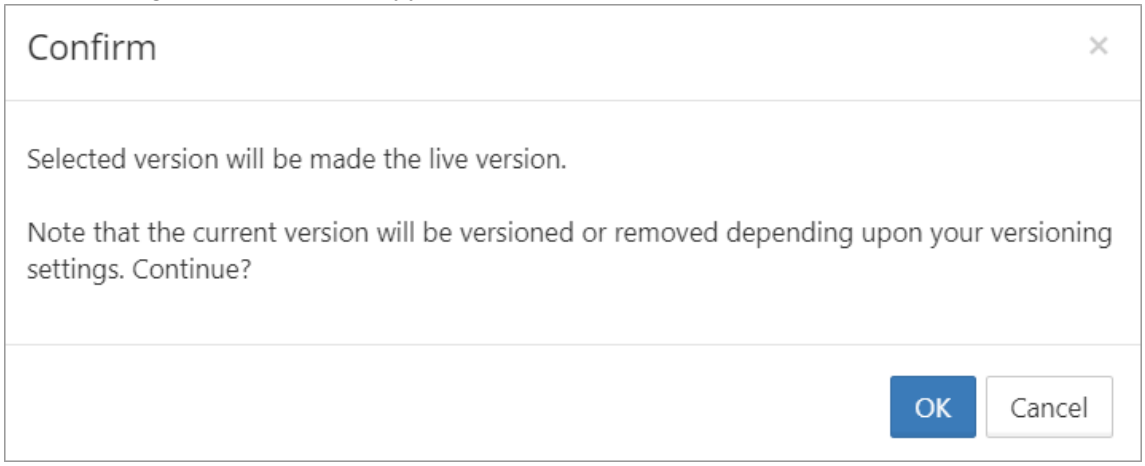
1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select **Users**.
3. On the **Manage Users** page, select a user, and then click the edit icon .
4. On the **User Detail** dialog box, click **Manage Files.**
   The **Manage Files for <User>** window opens.
5. Navigate to the file.
6. To see a list of earlier versions, click the Version icon.



7. Select the version that you want to make live, and click the **Make this version live** icon .

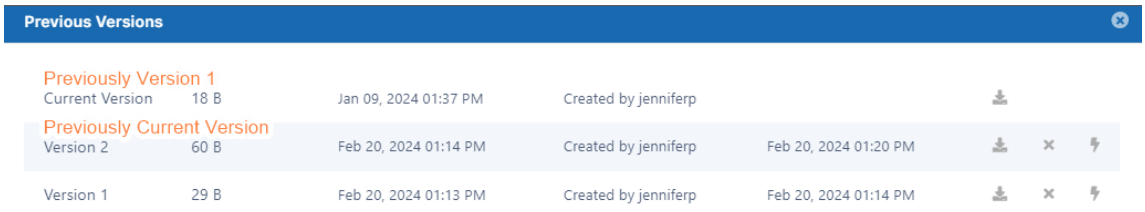


The following confirmation box appears.



> In versions of FileCloud prior to 20.2, current versions are always removed when another version is restored. Beginning with Version 20.2, by default, the current version is saved when another version is restored.

8. Click **OK**. A message telling you that the selected version has been made live appears.
   If the current version remains, it becomes the version directly preceding the current one.



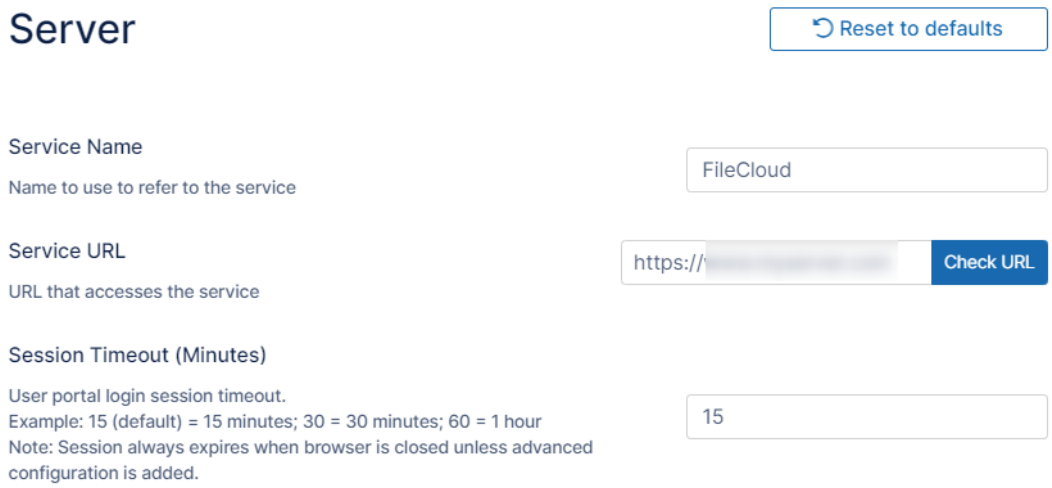
Change the Name of the Zip File for Multiple File Downloads

When multiple files and folders are downloaded from FileCloud, they are downloaded as a zip file with the name **<Service Name>-<download datetime>**. In addition to the downloaded files and folder, the zip file contains a text file named **downloadzip.log** which includes the line **Generated by <Service Name>**.

Service Name is used to refer to your FileCloud server throughout your system, on the user interface and in email messages and other notifications as well as in the download zip file name. By default, its value is FileCloud.

To change the Service Name:

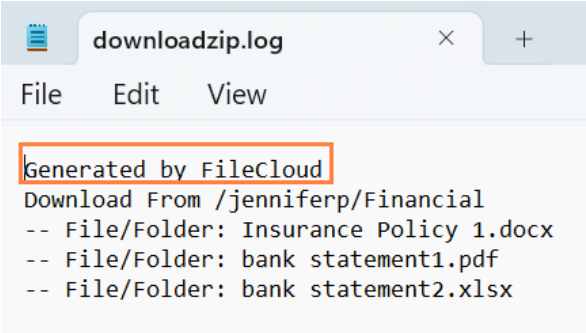
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server** .
   The **Server** settings page opens.



   At this point, if a user downloads multiple files at the same time, the zip file has a name similar to:

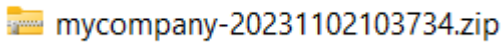
   filecloud-20231101141022.zip

and **downloadzip.log** has the line **Generated by FileCloud**:

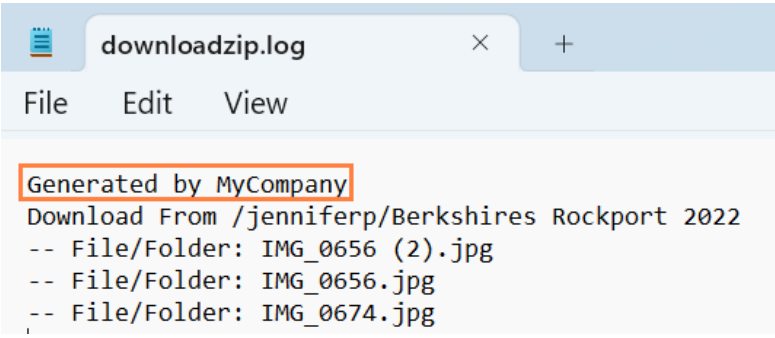


2. Change the value in **Service Name** to your own name for your server:

Now, if a user downloads multiple files at the same time, the zip file include the new **Service Name** instead of **FileCloud**:



and downloadzip.log has the line **Generated by <new Service Name>**:



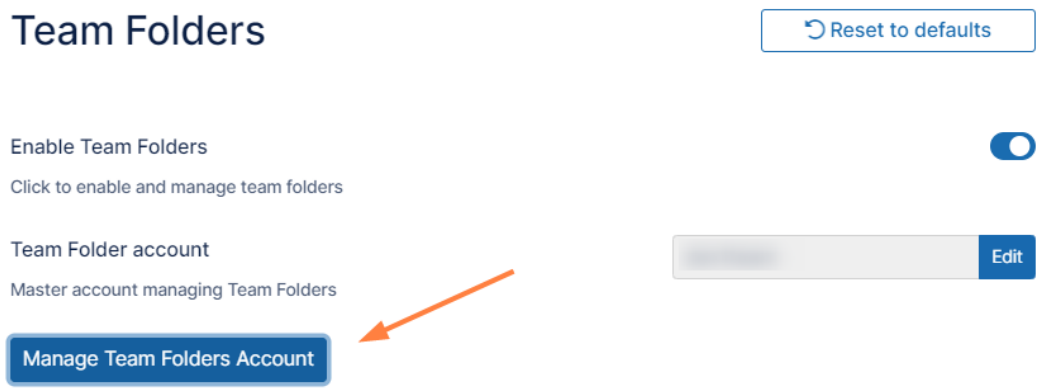
Managing Team Folders

> Beginning in FileCloud 23.242, you can manage and view details of Team Folders through the Team Folder Account Details dialog box.

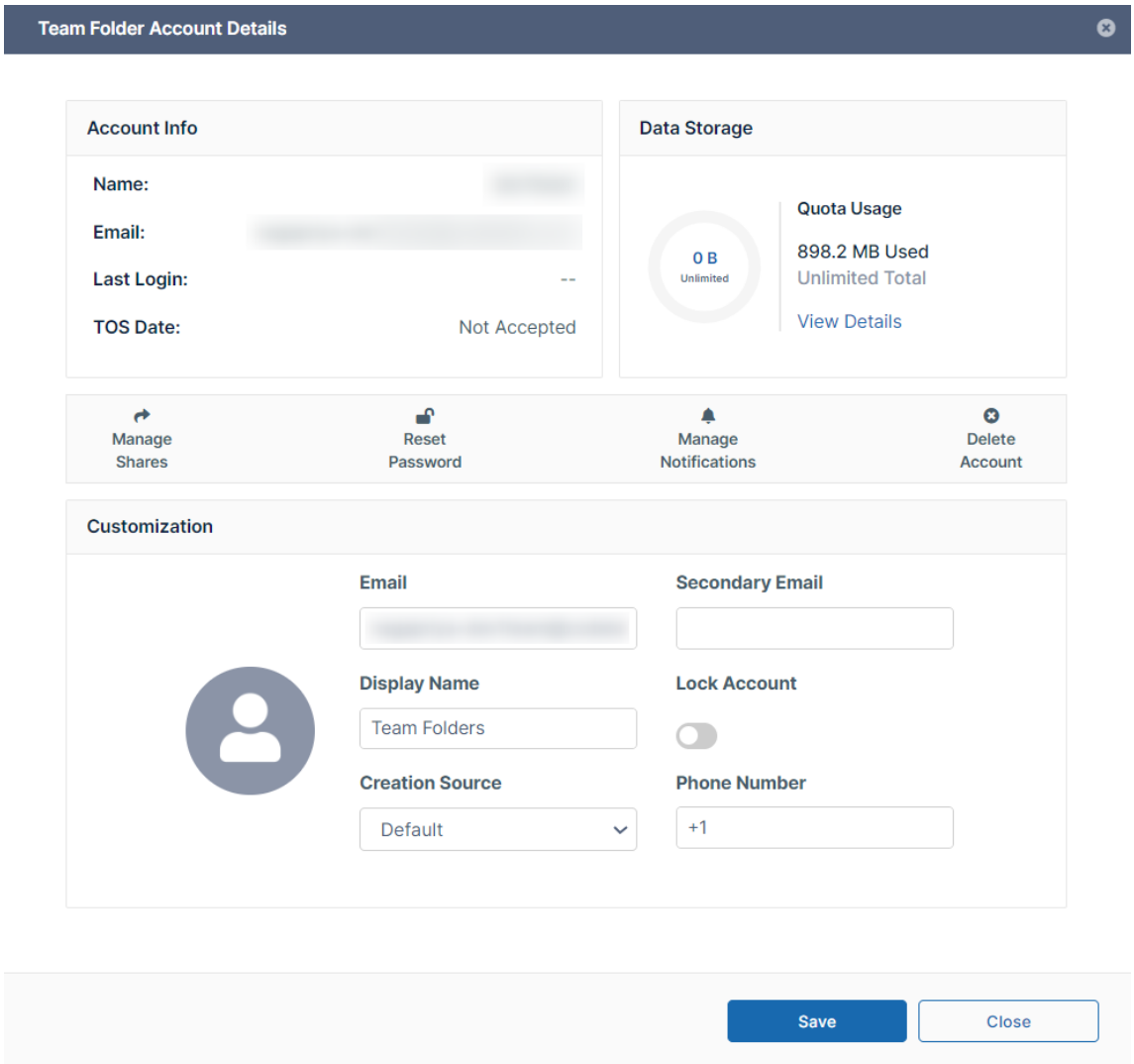
To access the **Team Folder Account Details**, you must have already set up your Team Folders account. If you have not set it up yet, see Configure the Team Folders Account.

To manage and view details of Team Folders:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Team Folders** .
   The **Team Folders** settings page opens.

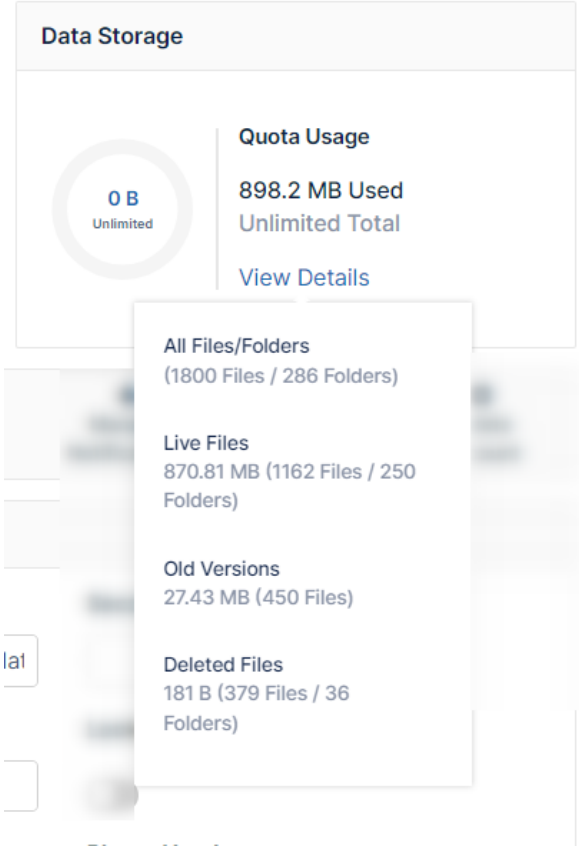


2. To see details of the Team Folders account, click **Manage Team Folders Account**.
   The Team Folder Account Details dialog box opens.
   The dialog box gives you account and data information, and enables you to manage Team Folder shares and notifications, reset the Team Folder account password, edit some account fields, and perform other Team Folder actions.


Team Folder Account Details
Account Info
Name:
Email:
Last Login:
--
TOS Date:
Not Accepted
Data Storage
0 B
Unlimited
Quota Usage
898.2 MB Used
Unlimited Total
View Details
Manage Shares
Reset Password
Manage Notifications
Delete Account
Customization
Email
Secondary Email
Display Name
Team Folders
Lock Account
Creation Source
Default
Phone Number
+1
Save
Close

To view the breakdown of data in Team Folders:

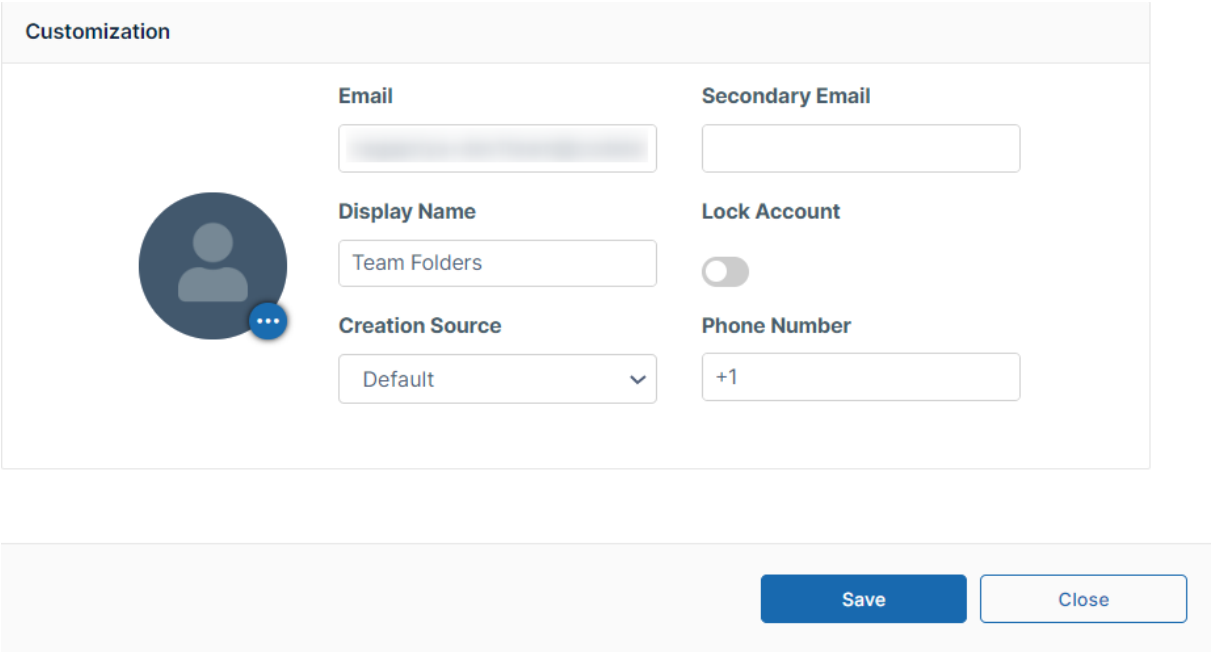
In the Data Storage section, click **View Details**.
You are shown a breakdown of the files and folders by live versions, old versions, and deleted files.



To edit the Team Folders account fields:

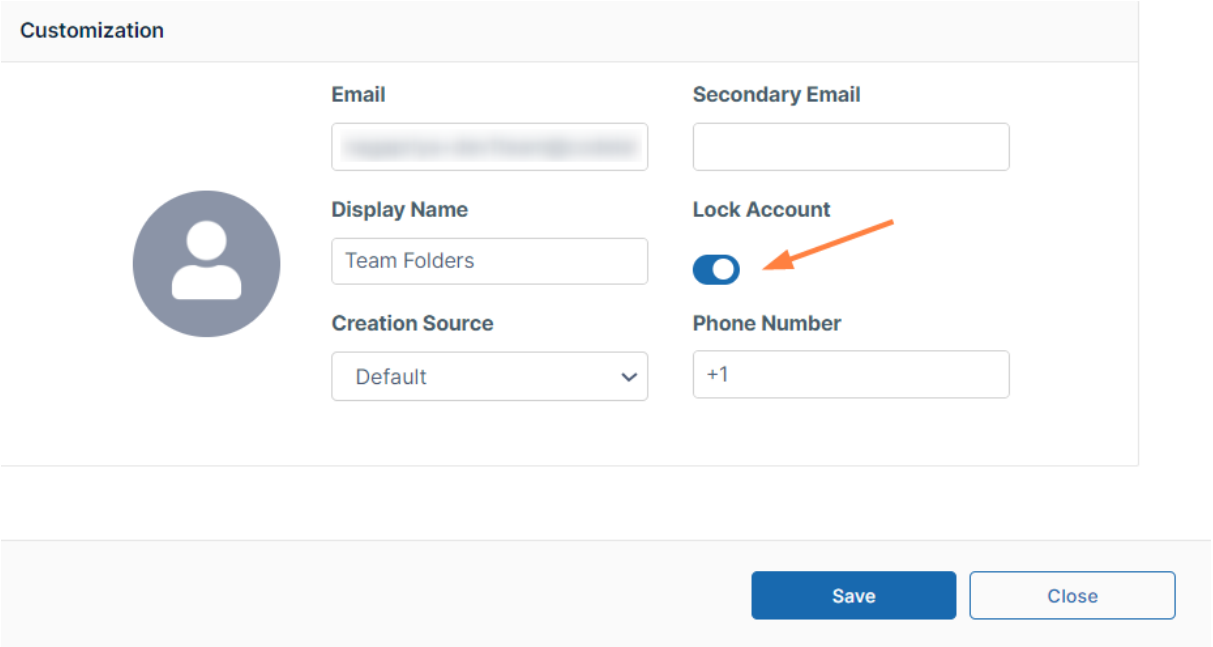
In the customization section, click the image, to upload a photo or graphic, or modify the **Email**, **Secondary Email**, **Display Name**, **Creation Source**, or **Phone Number** fields and click **Save** to save your changes.
Lock Account is automatically checked when too many login errors occur. Click to remove the check

and unlock the account.



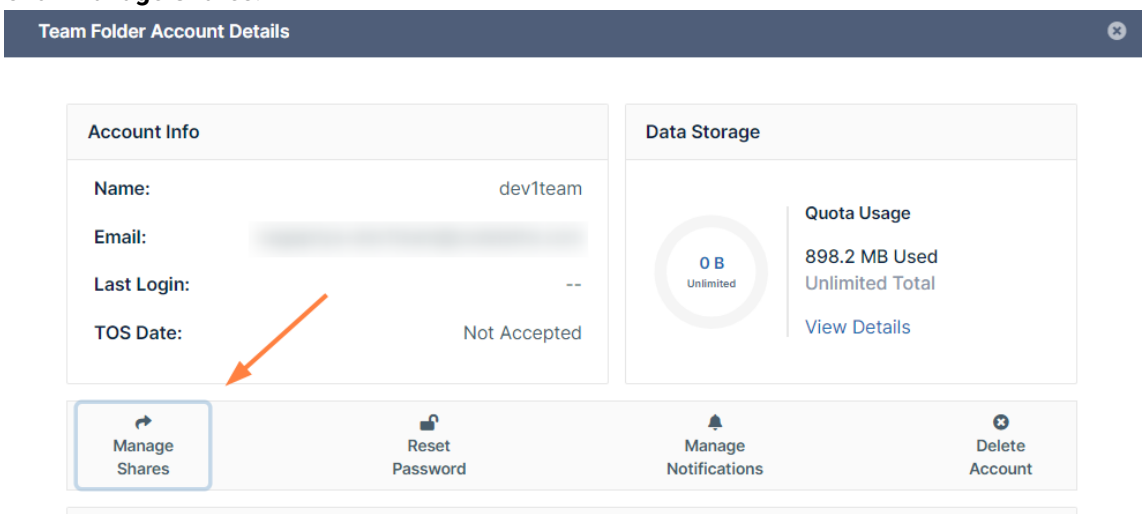
To lock the Team Folder account:

The **Lock Account** field is automatically enabled when the account is locked.
Unlock the account by clicking the enabled **Lock Account** control so that it appears disabled.

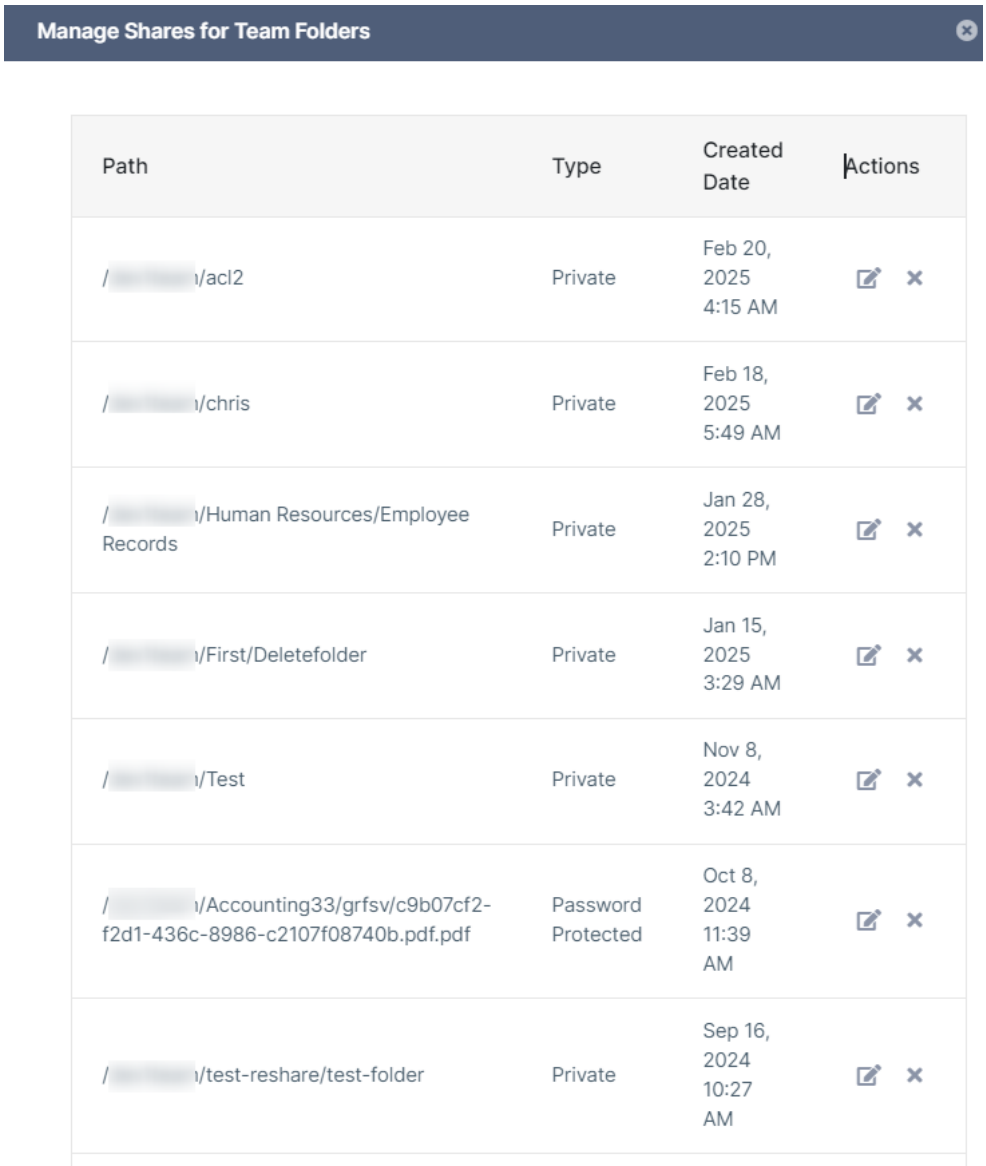


To manage Team Folder shares:

1. Click **Manage Shares**.

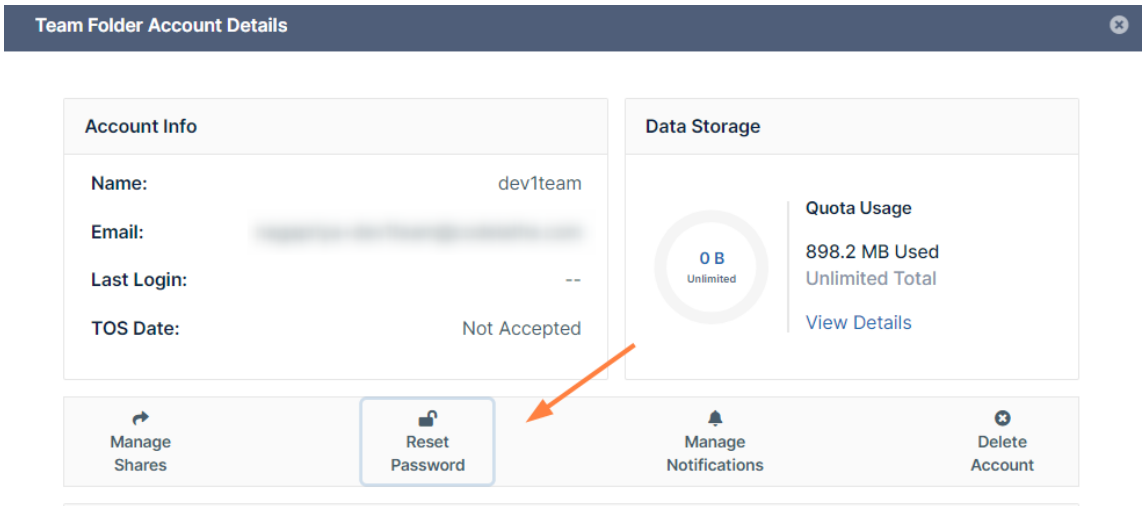


   A list of your Team Folder shares opens.
2. Click the edit icon to modify the options or permissions of a share.
3. Click the x icon to remove a share.

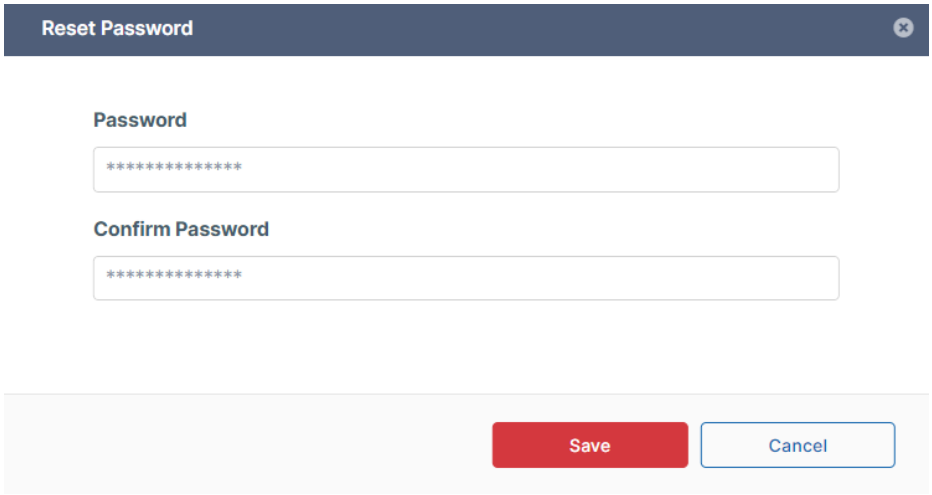


To reset the Team Folder account password:

1. Click **Reset Password**.

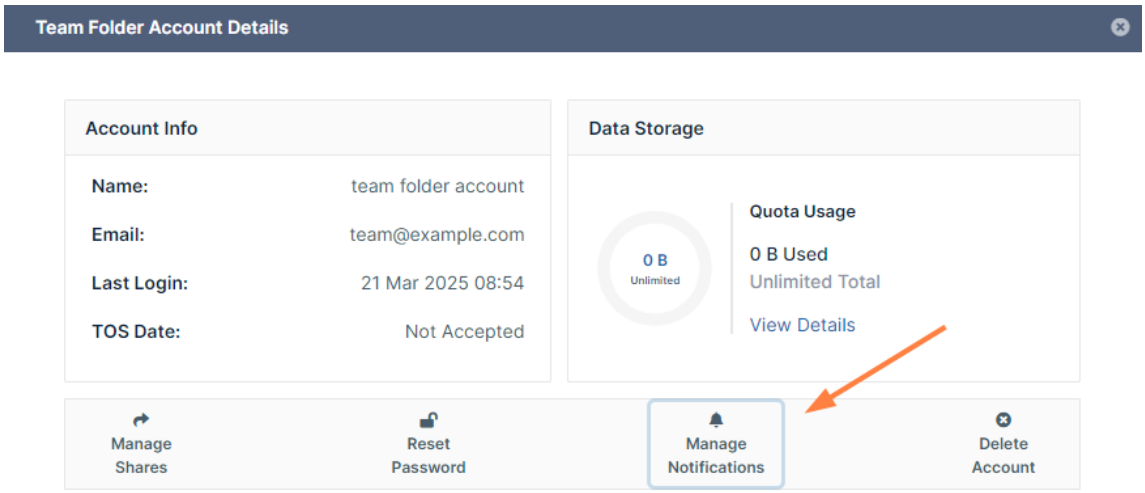


2. Enter and re-enter a new password, and click **Save**.

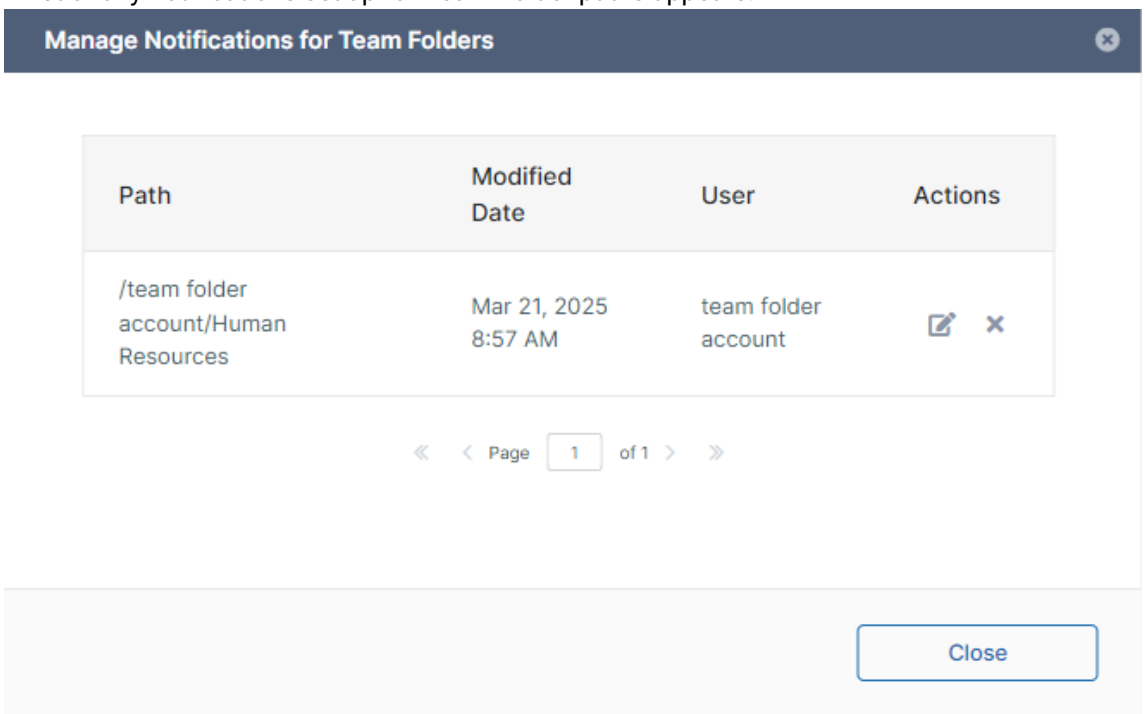


To manage Team Folder notifications

1. Click **Manage Notifications**.



A list of any notifications set up for Team Folder paths appears.



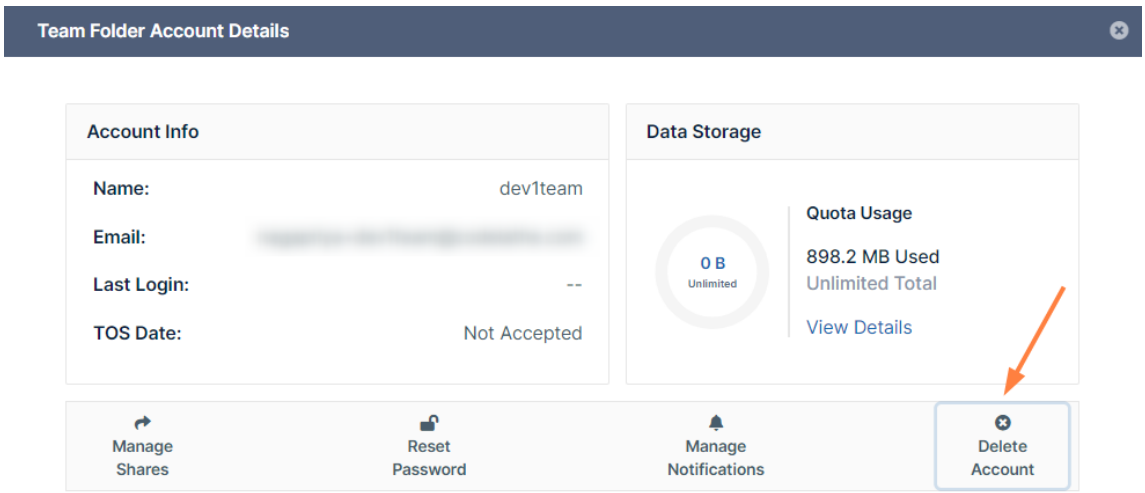
2. Click the Edit icon to change a notification's settings, or click the delete icon to delete the notification.

To delete the Team Folder account:

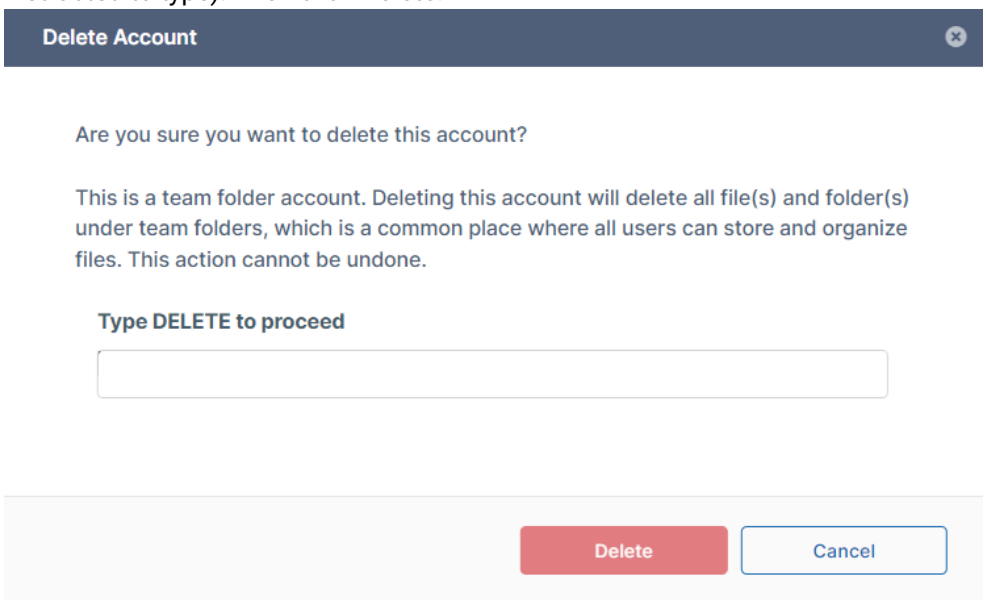
Check which files and folders will be deleted before you delete your Team Folder account. Deleting the account causes the following to be permanently deleted:

- All files and folders you have stored and shared with users in Team Folders
- Any files or folders users have stored in Team Folders

1. Click **Delete Account**.



2. To confirm that you want to delete the Team Folder account, enter **DELETE** (or the word you are instructed to type). Then click **Delete**.



Search for a Team Folder

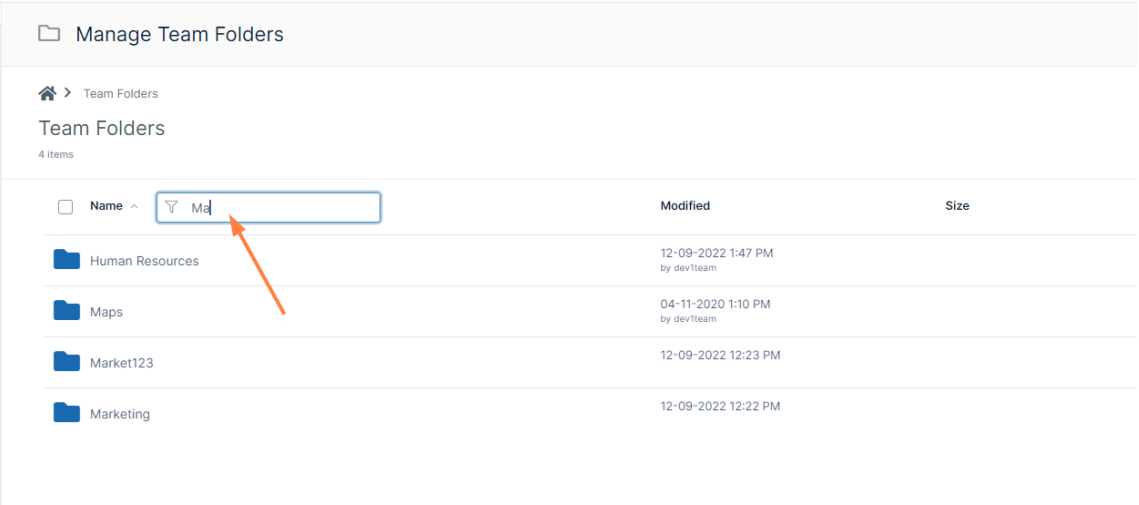
> The ability to search for a specific Team Folder is available in FileCloud Server version 19.1 and later.

If you manage so many Team Folders that you have to look through multiple pages of folder listings to find a Team Folder, you can use the search box to find the folder you need quickly.

- In some cases, enterprises might see multiple pages of team folders
- To help you filter the Team Folder list, a search box allows you to filter the list of folders on the Manage Team Folders page.
- You can also locate files by clicking the **Name**, **Size**, and **Modified** columns to sort on them.

To search for a Team Folder:

1. Open a browser and log on to the *Admin Portal*.
2. From the left navigation menu, under *MANAGE*, select *Team Folders*.
3. On the *Manage Team Folders* page, In the *Filter* box, type in the name of your folder or part of the name, and press ENTER.
   Matching folders appear in the Team Folders list.



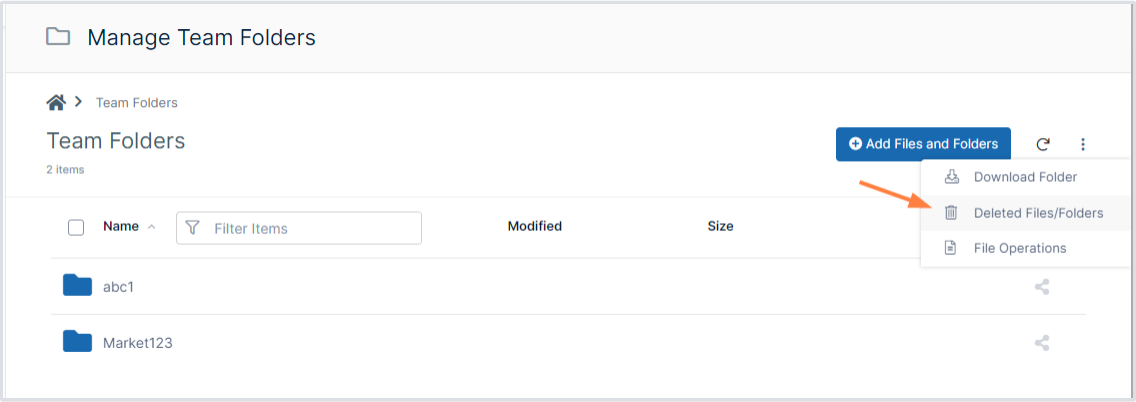
Recover Deleted Files

> The **Restore** button for deleted files and folders in Team Folders is available in FileCloud version 22.1 and later.

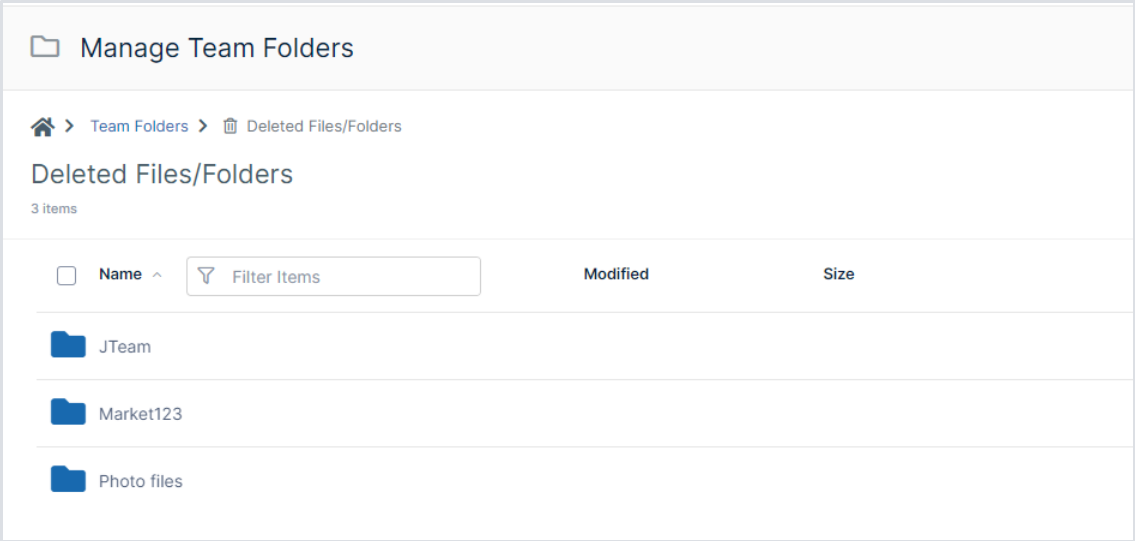
After you delete files and folders, they are placed in the Team Folder's recycle bin so that they can be recovered if deleted by mistake or are needed again at a later time.

To recover a deleted folder or file:

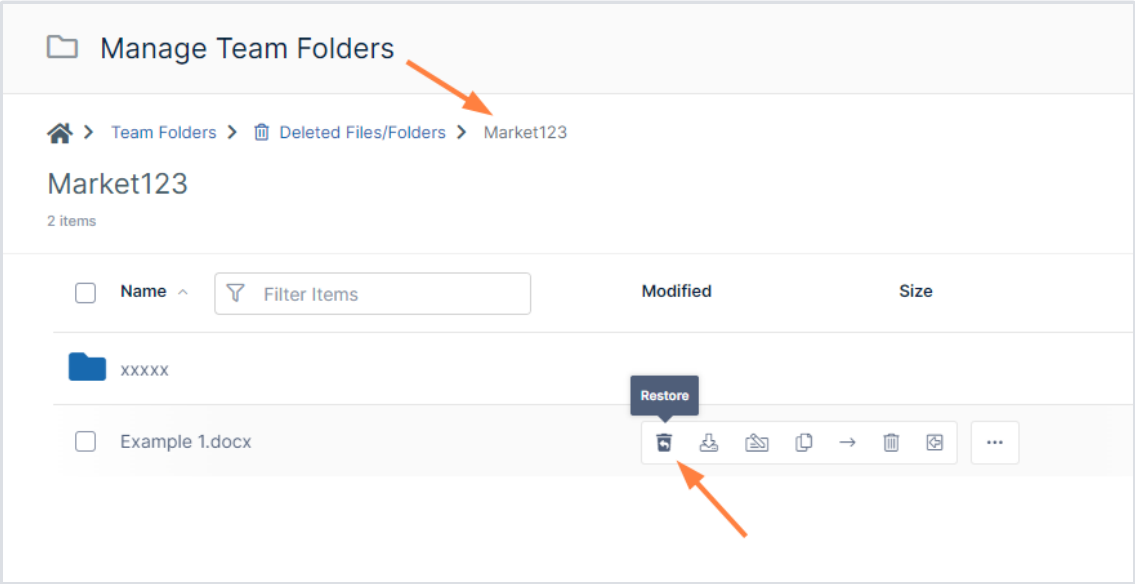
1. Open a browser and log in to the admin portal.
2. In the navigation panel, click **Team Folders**.
3. To open the **Deleted Files/Folders** page, in the upper-right corner, click the more icon and choose **Deleted Files/Folders**.



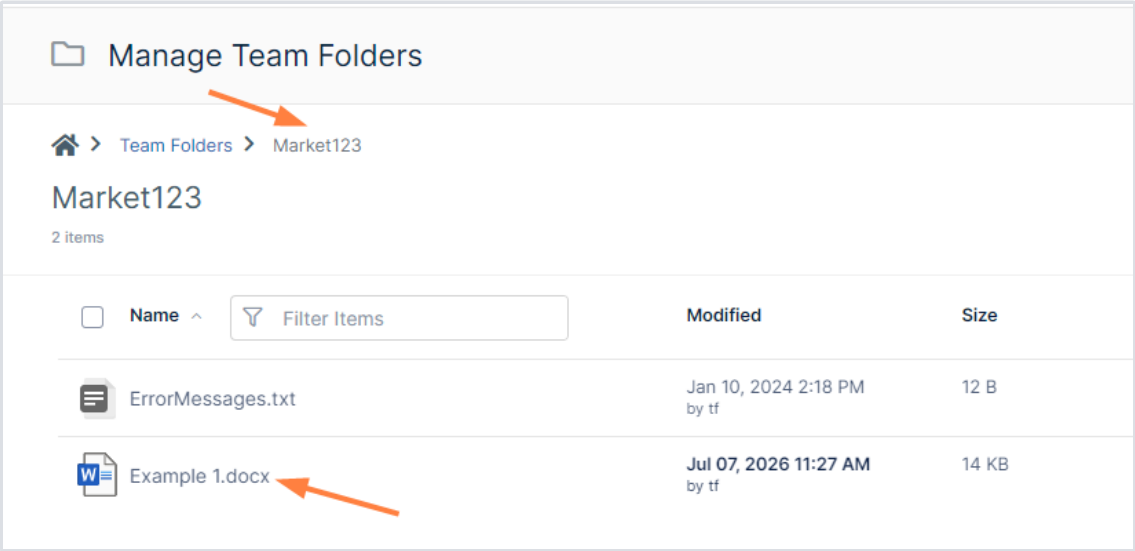
The **Deleted Files/Folders** page opens. The top level of folders includes deleted team folders as well as non-deleted parent team folders of deleted files. For example, in the following screenshot, the **JTeam** and **Photo files** team folders are deleted team folders, but the **Market123** team folder is a non-deleted team folder that contains deleted files.



4. Navigate to the folder or file you want to recover.
5. Hover over the folder or file, and click the **Restore** button.



6. The file or folder is restored. If it is a Team Folder, it is restored to the top level of Team Folders. If it is a file within a Team Folder, it is restored within the Team Folder.



View and Restore Previous Versions in Team Folders

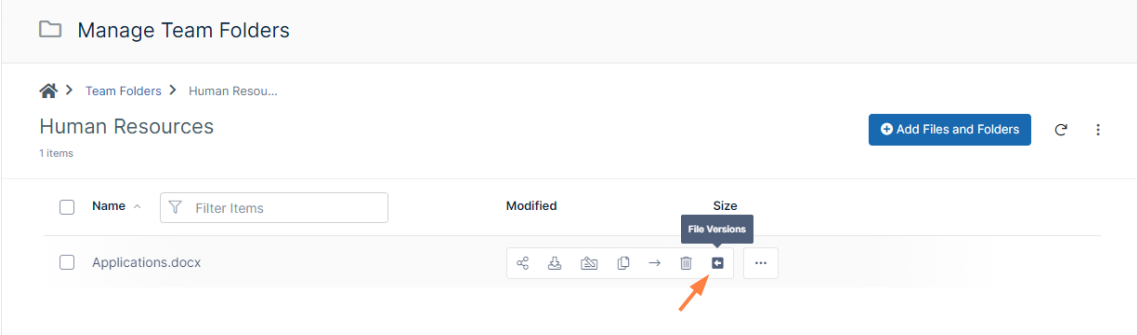
> The ability to restore a previous version of a file in Team Folders is available in FileCloud Server version 18.2 and later.

If you need to revert changes made to a file, you can restore the previous version and make it live.

To restore a previous version of a file in Team Folders:

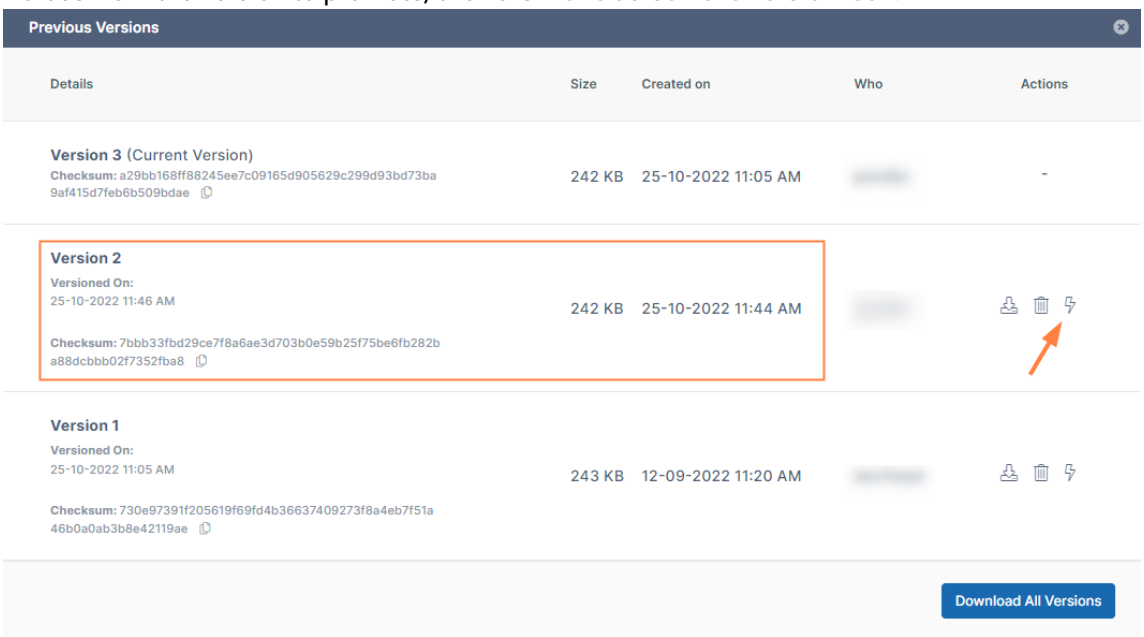
1. Open a browser and log in to the admin portal.

2. In the navigation pane, select **Team Folders.**
3. On the **Manage Team Folders** page, navigate to the file you want to revert to a previous version.
4. Click the version icon.

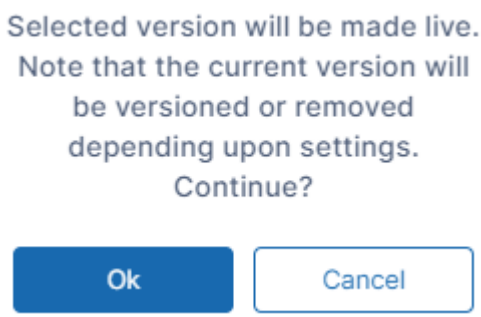


A list of the previous versions opens.

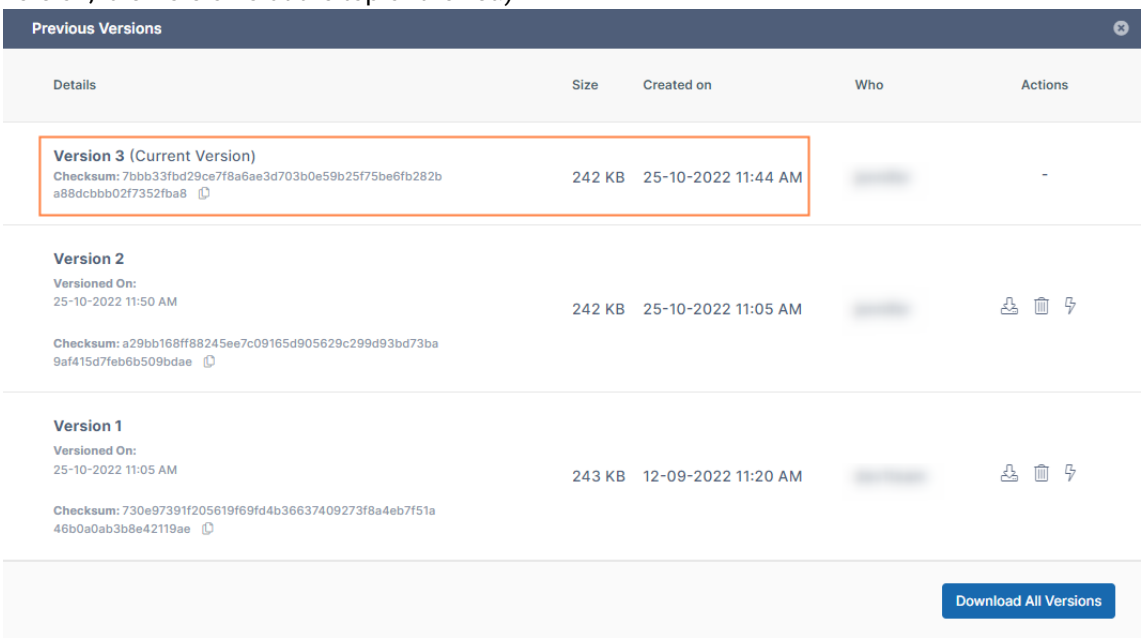
5. Across from the version to promote, click the **Make as Current Version** icon.



The following confirmation box appears:



6. Click **OK**.
   The version that was made the current version now appears at the top, and the previous current version appears under it.
   (Note that above, the 11:44 AM version was Version 2, but below, after it was made the current version, it is Version 3 at the top of the list.)



> In versions of FileCloud prior to 20.2, current versions are always removed when another version is restored. Beginning with Version 20.2, by default, the current version is saved when another version is restored.

To view and restore previous versions of files in the user portal, see View Previous Versions Of Files

Managing User Shares

All Folder and File shares of FileCloud Users can be managed by the FileCloud Administrator.

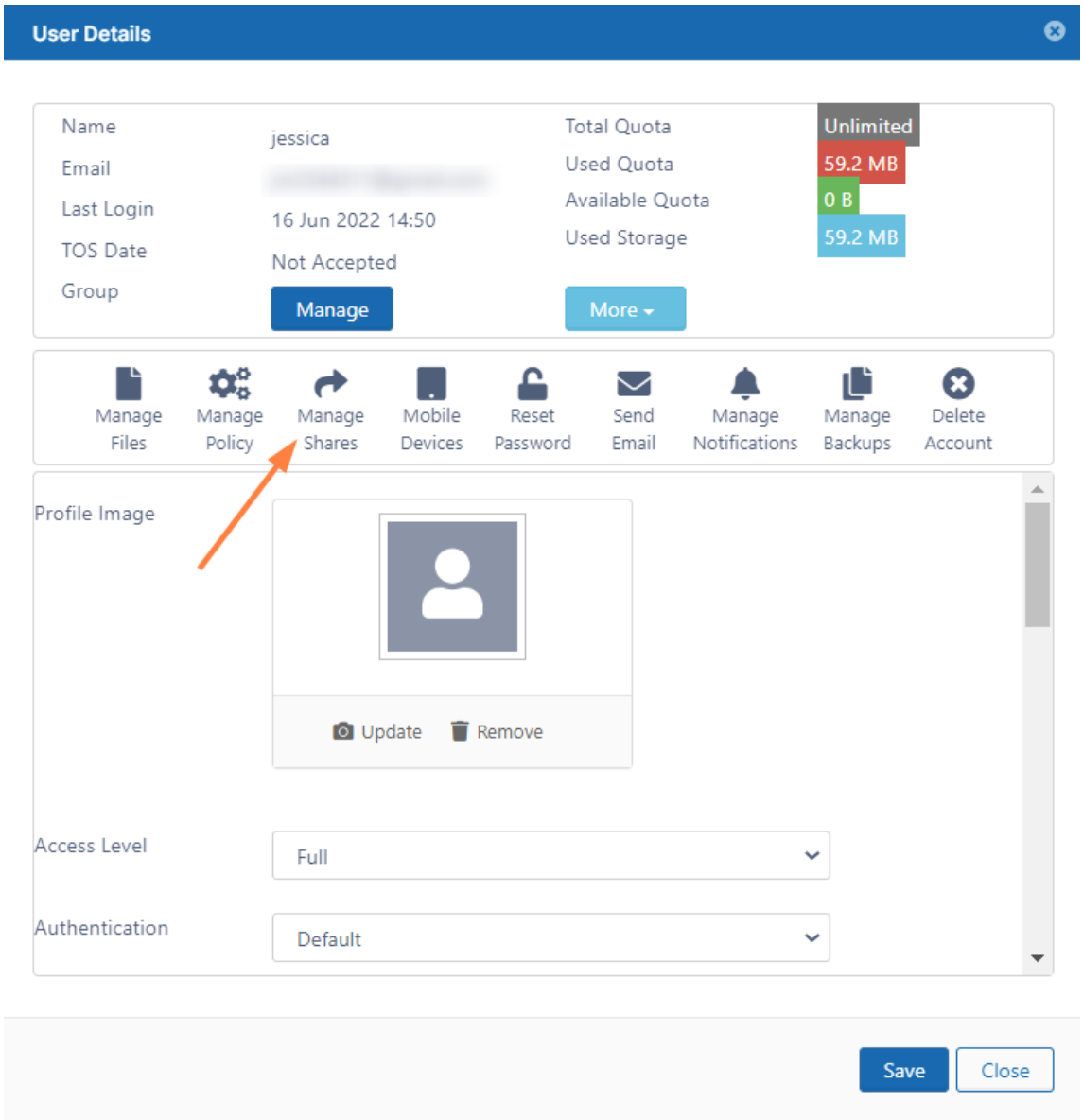
The Administrator is able to view, modify or remove shares done by users of the system.

The admin can open either an individual user's list of shares from the **User Details** dialog box or a list of all shares by all users in the system through the **User Shares** screen.
The admin can also export a file listing all shares and their details from the **User Shares** screen.

To set up file sharing, see Share Settings.

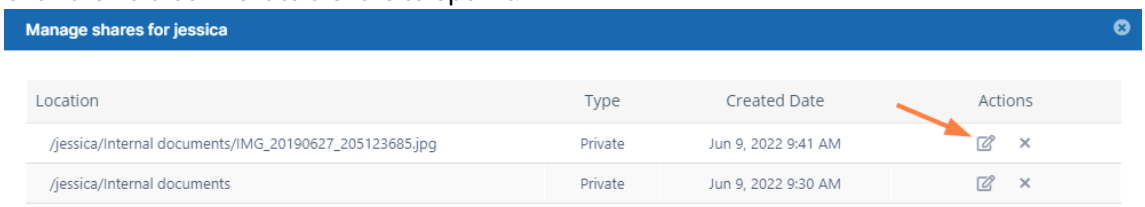
To manage user shares for an individual user:

1. Log on to Administration Panel
2. Click **Users** on the left navigation panel, then click the **Edit** icon for a user, and click **Manage Shares** in the **User Details** dialog box.



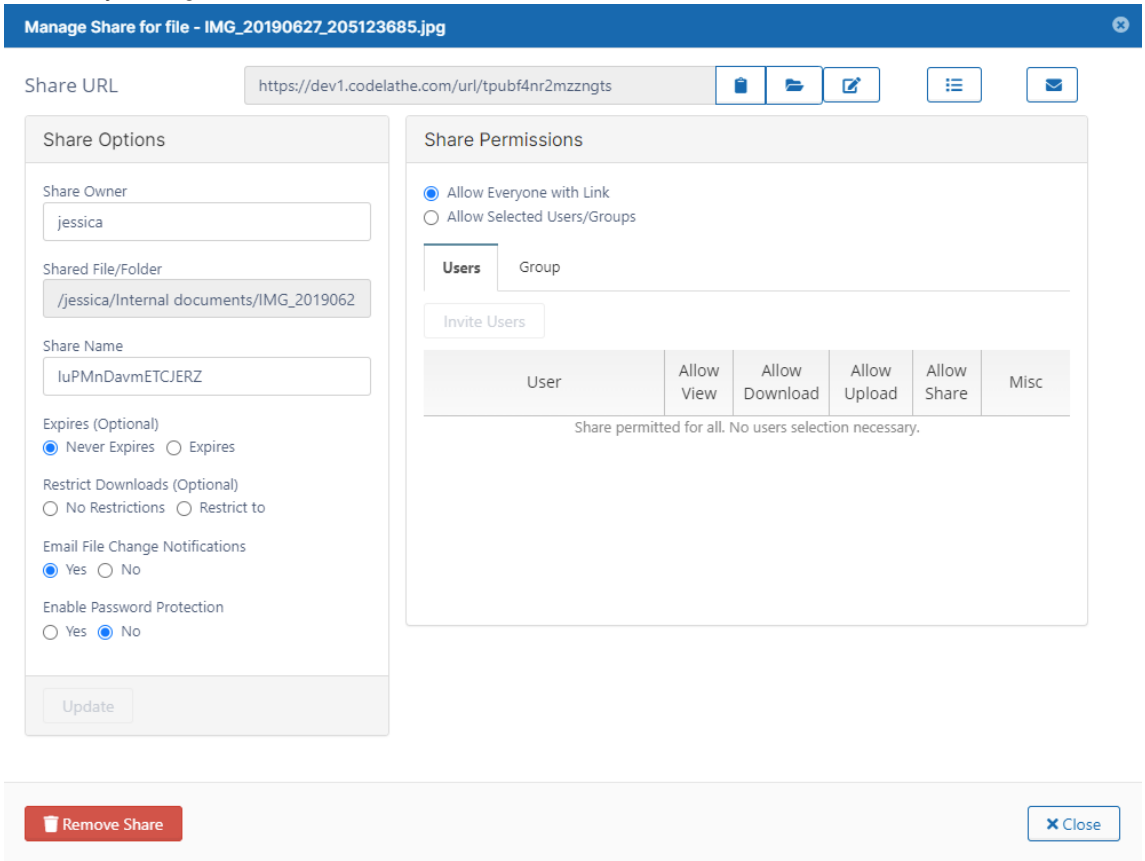
A **Manage shares for [user]** dialog box opens.

3. Click the Edit icon next to a share to open it.



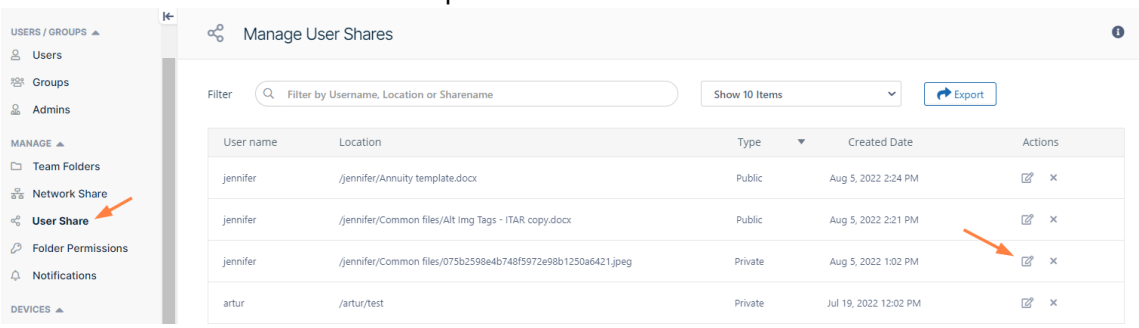
The **Manage Share** dialog box opens.

4. Make any changes to the share.

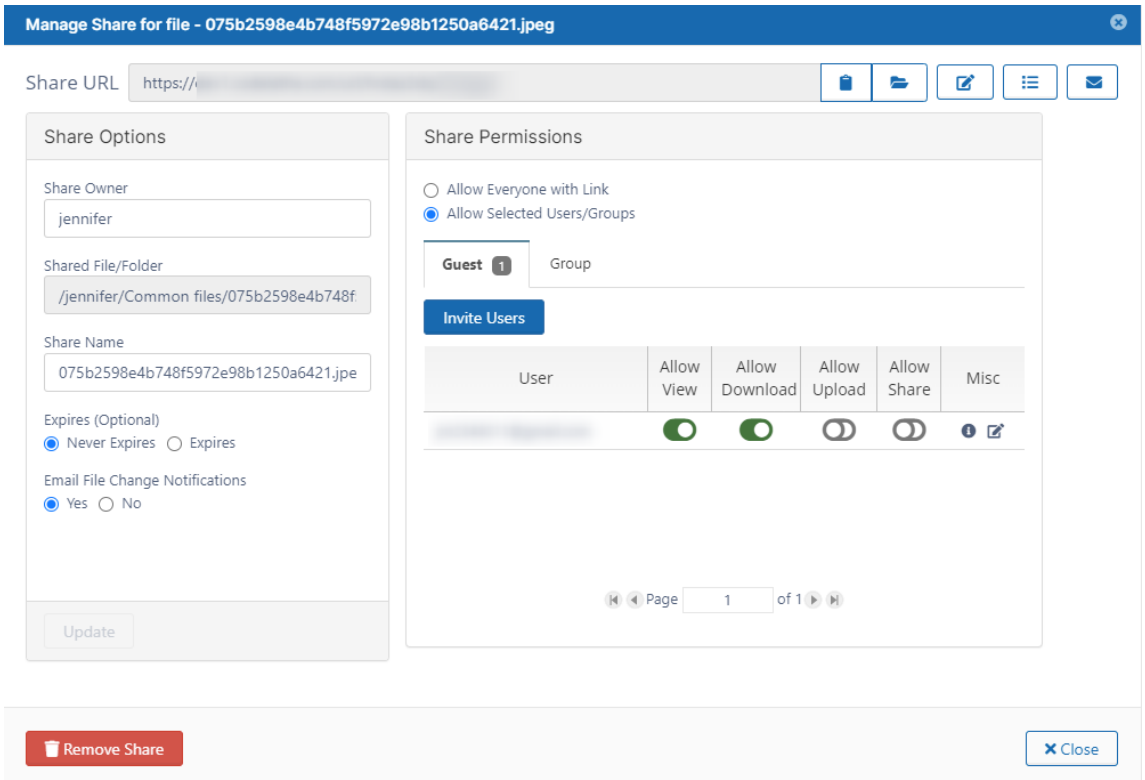


To manage user shares for all users:

1. Log on to Administration Panel.
2. Click **User Shares** in the navigation panel.
   The **Manage User Shares** screen opens.
3. Click the Edit icon next to a share to open it.

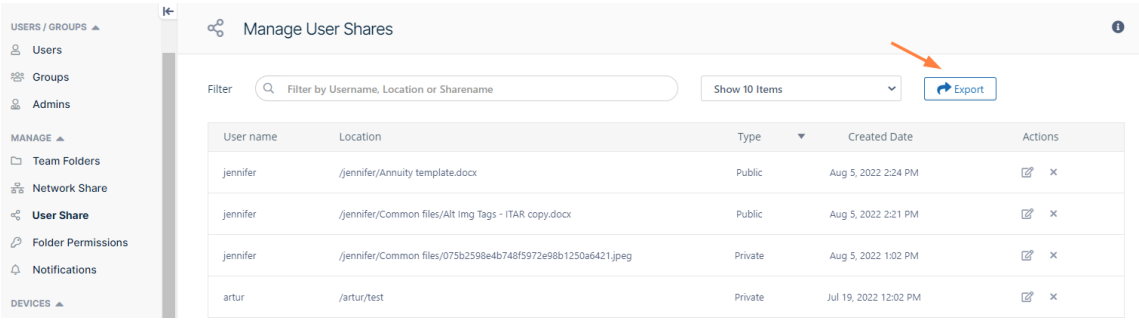


4. The **Manage Share** dialog box opens.
5. Make any changes to the share.



To export a list of all shares:

1. Log on to Administration Panel.
2. Click **User Shares** in the navigation panel.
   The **Manage User Shares** screen opens.
3. Click **Export**.



A csv file named **shares** is exported with the following fields:

	A	B	C	D	E	F	G	H	I
1	UserName	Share Location	TYPE	Created Date	Expiry Date	Users	Groups		
2	jennifer	/jennifer/Annuity ter	Public	8/5/2022 14:24	8/31/2022 0:00				
3	jennifer	/jennifer/Common fi	Public	8/5/2022 14:21					
4	jennifer	/jennifer/Common fi	Private	8/5/2022 13:02		No Users	No Groups		
5	artur	/artur/test	Private	7/19/2022 12:02			No Groups		

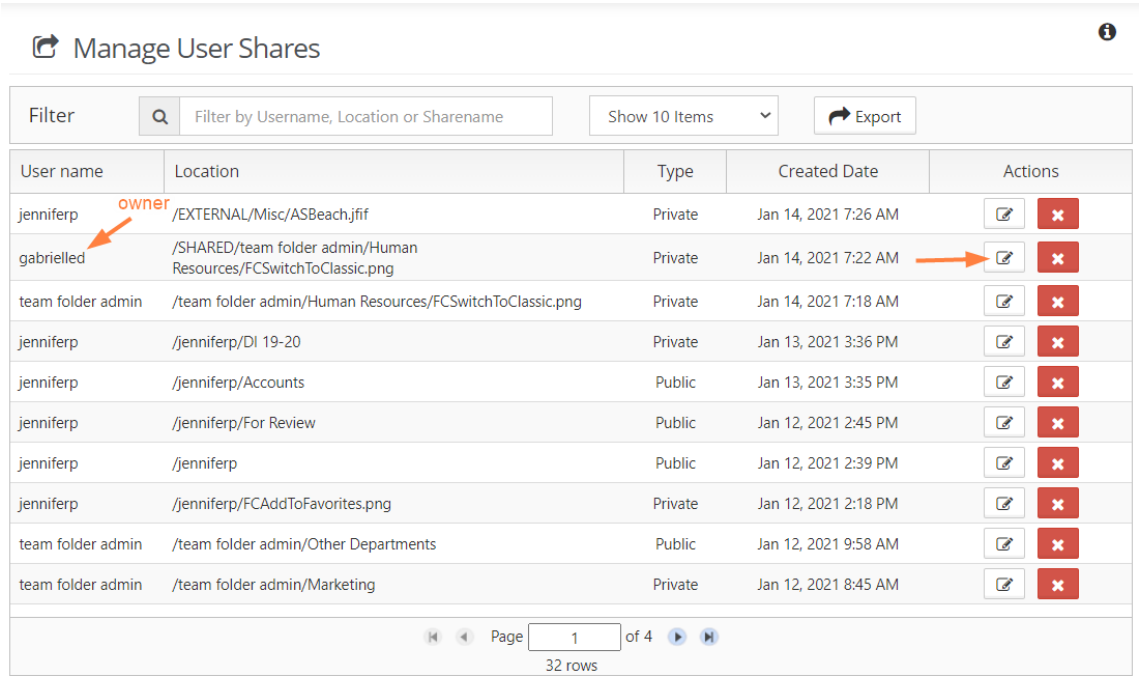
Transfer Ownership of a Reshare from a Team Folder or Network Share

In FileCloud version 20.3 and later, administrators have the ability to change the owner of a reshare from a Team Folder or a Network Share.

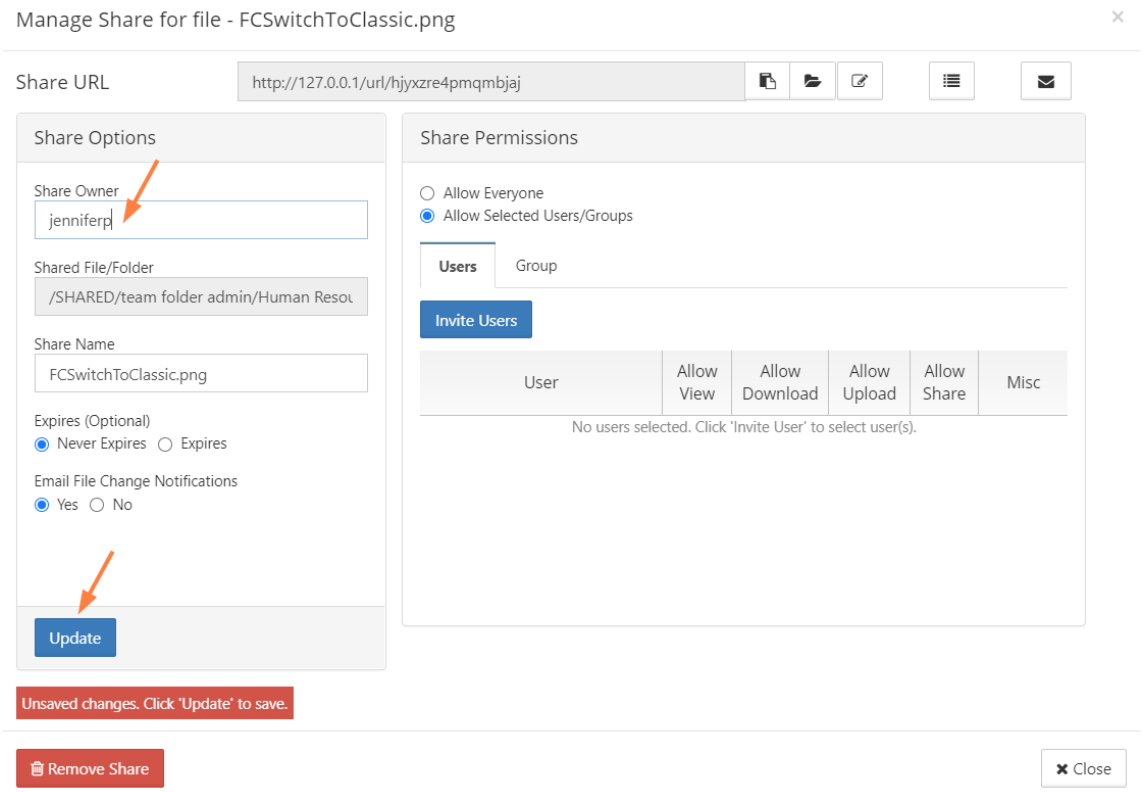
Reshared content from Team Folders and Network Shares is content that a user already has access to and has shared with another user.
In the **Manage User Shares** dialog box, its root is **/EXTERNAL** or **/SHARED**.

To change the owner of a reshare

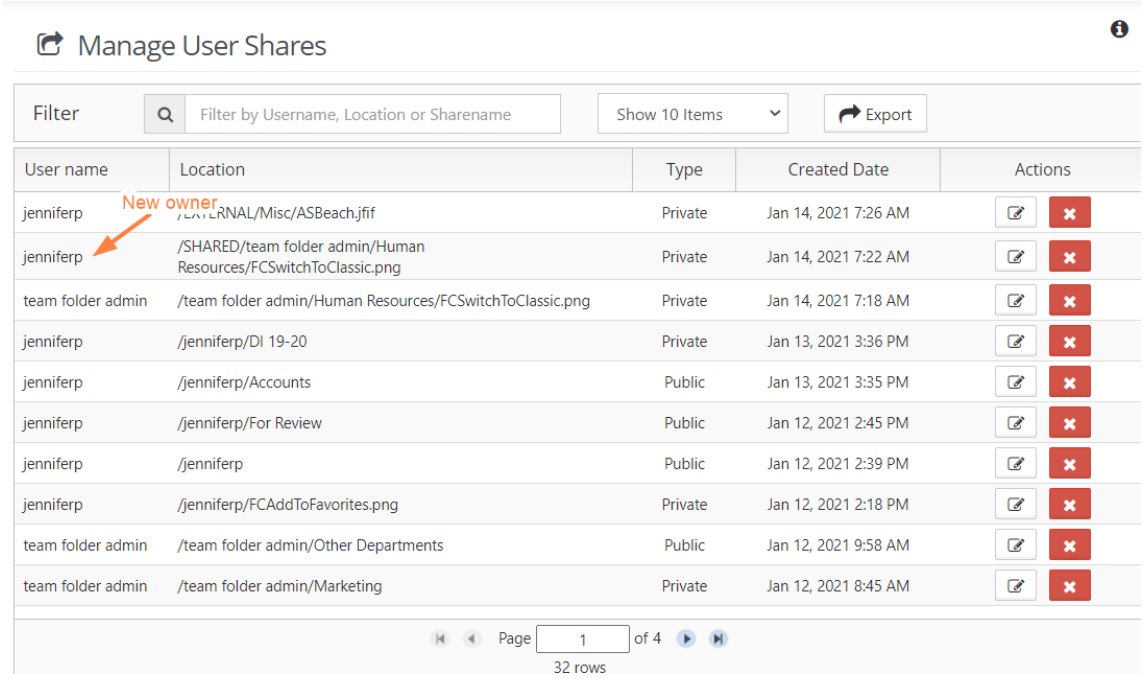
1. Follow the steps in Managing User Shares to open the list of shares.
2. To open the **Manage Share for File** dialog box, click the Edit button for a Team Folder share or a Network Share.



3. In the **Manage Share for file** or **Manage Share for folder** dialog box, type in the user name of a new **Share Owner**, and click **Update.**



4. Click **Close**.
   Now the listing for the share shows the new owner.



Creating direct file download link from a public file share

Creating direct download link for public shares

Public file shares by default opens a landing page, from where user can download the shared file. Sometimes it is preferable to have a direct downloadable links. By making minor changes to the share link, a direct downloadable link can be created.

By default the public share link looks like this:

> https://abc.company.com/ui/core/index.html?mode=single&path=/SHARED/tester/MMQj5gqRymicnDib

In the above link, replace the string "**ui/core/index.html?mode=single&**" with "**app/websharepro/share?**" to the URL and remove the mode parameter.
Making these two changes the above link becomes:

> https://abc.company.com/app/websharepro/share?path=/SHARED/tester/MMQj5gqRymicnDib"

Now, this link can be can be used to download the files directly from browser, download managers or Linux utilities such as wget.

Creating direct file download links from a public folder share

Public folder shares provide a share link that opens a page listing the contents of the folder. By making minor changes to the share link, a direct downloadable link for any file in the folder can be created.

After you create the share, copy the share link and modify it to link to a download page for a file in the folder. Then send the new link to share users.

The procedure for creating direct file download links is the same from public folder shares of folders in My Files and folders in Team Folders.

To copy the share link:

1. Hover over the folder and click the share icon.

2. In the **Share link for folder** dialog box, click the **Copy link to clipboard** button.
   If you open the link in a browser, FileCloud displays the folder's contents.
   The following video shows you the process.

To create a direct link to a file in the shared folder:

In our example, the link to the shared folder is:
http://127.0.0.1/ui/core/index.html?mode=public&shareto=#expl-tabl./SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1
We would like the link to open a download page for the file customers.docx, which is located in the folder.

This video shows you the steps, which are also listed below.

Copy the link to a text editor in order to modify it.

1. Remove the portion of the URL that takes you to the FileCloud page, and replace it with a path to a download page.
   (Remove /ui/core/index.html?mode=public&shareto=#expl-tabl and replace it with core/downloadfile.)
2. Add a **filepath** parameter after core/downloadfile and set it equal to the /SHARED/ portion of the path. Then add the filename, customers.docx, to the end of the path.
   (At this point, the path is http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1/customers.docx
3. After the filepath parameter, add a filename parameter, and set it equal to customers.docx.
   (The final link in the example looks like http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1/customers.docx&filename=customers.docx)
4. Send the link to share users. When clicked, it opens a download page for the customers.docx file.

To create a direct link to a file in a sub-folder of the share:

If the file is embedded in a folder within the shared folder, make the same changes as above, but include the path to the file including the sub-path(s). For example if you are linking to the file **background.png** which is in the sub-folder **images** in the shared folder, the link should appear as:

http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1/images/background.png&filename=background.png

Sample links before and after

Link to the **customers.docx** file in the top-level of the shared My Files folder

Original link
https://www.mycompany.com/ui/core/index.html?mode=public&shareto=#expl-tabl./SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1

Modified link
https://www.mycompany.com/core/downloadfile?filepath=/SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1/customers.docx&filename=customers.docx

Link to the **background.png** file in the **images** folder in the shared My Files folder

Original link
https://www.mycompany.com/ui/core/index.html?mode=public&shareto=#expl-tabl./SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1

Modified link
https://www.mycompany.com/core/downloadfile?filepath=/SHARED/!bIi3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1/images/background.png&filename=background.png

Link to the **Announcement.txt** file in the shared HR Misc folder of the Human Resources Team Folder (same format as link from My Files)

Original link
https://www.mycompany.com/ui/core/index.html?mode=public&shareto=#expl-tabl./SHARED/!b0ipSLCEtKoRQT47yiNpKOSyi/dWPDFohwRIjdOj7v

Modified link
https://www.mycompany.com/core/downloadfile?filepath=/SHARED/!b0ipSLCEtKoRQT47yiNpKOSyi/dWPDFohwRIjdOj7v/Announcement.txt&filename=Announcement.txt

Managing Storage Space Usage

Administrators can configure settings to control the space needed to keep FileCloud Server sites running.

Related topics

A User's Storage

Change the Storage Quota for a User or Group

Delete User Files and Folders

Clear a User's Recycle Bin

Remove a User's Incomplete Uploads

Remove Old File Versions

All Managed Storage

Clear Deleted Files Automatically

All Managed Storage Options

Protecting Your Storage

Set Up Encryption for Managed Storage

Managing User Locks

As an administrator, you can have full control over file locking:

- Decide whether you want to give users the ability to lock a folder or a file
- See a list of all locked files and folders system-wide
- Remove a lock on user's file or folder

💡 To learn more about managing locks, click on a subject:

How Locking Works

Locking can be set on both files and folders and signifies that a user is actively working that file or folder.

- Locking has to be enabled by the Administrator before the user has the option to lock a file or folder.
- FileCloud LOCKING is designed to prevent opening/accessing files between DIFFERENT USER ACCOUNTS.
- If you access a file whose lock is owned by you, then the file access will be ALLOWED.

When a file or folder is locked:

- A lock icon will be shown in the file listing
- The owner of the lock will also be shown in the details panel on the right hand side
- The owner of the lock has full access to that file or folder and can modify it
- Administrators can always override a lock in the Admin Portal
- A lock can be set up to prevent other users from reading the file or seeing the folder contents.
- If read permissions are not allowed, then other users cannot download or view the locked file or folder

The following table shows the behavior depending on the type of lock.

Lock with read allowed	Access by lock owner	Access by others
Yes	Full access to the file is available. Share/Sync/Edit/Deletes allowed	Only read is allowed. No modification is allowed
No	Full access to the file is available. Share/Sync/Edit/Deletes allowed	No access is provided . All access using all clients are blocked.

Turn Off All File Locking

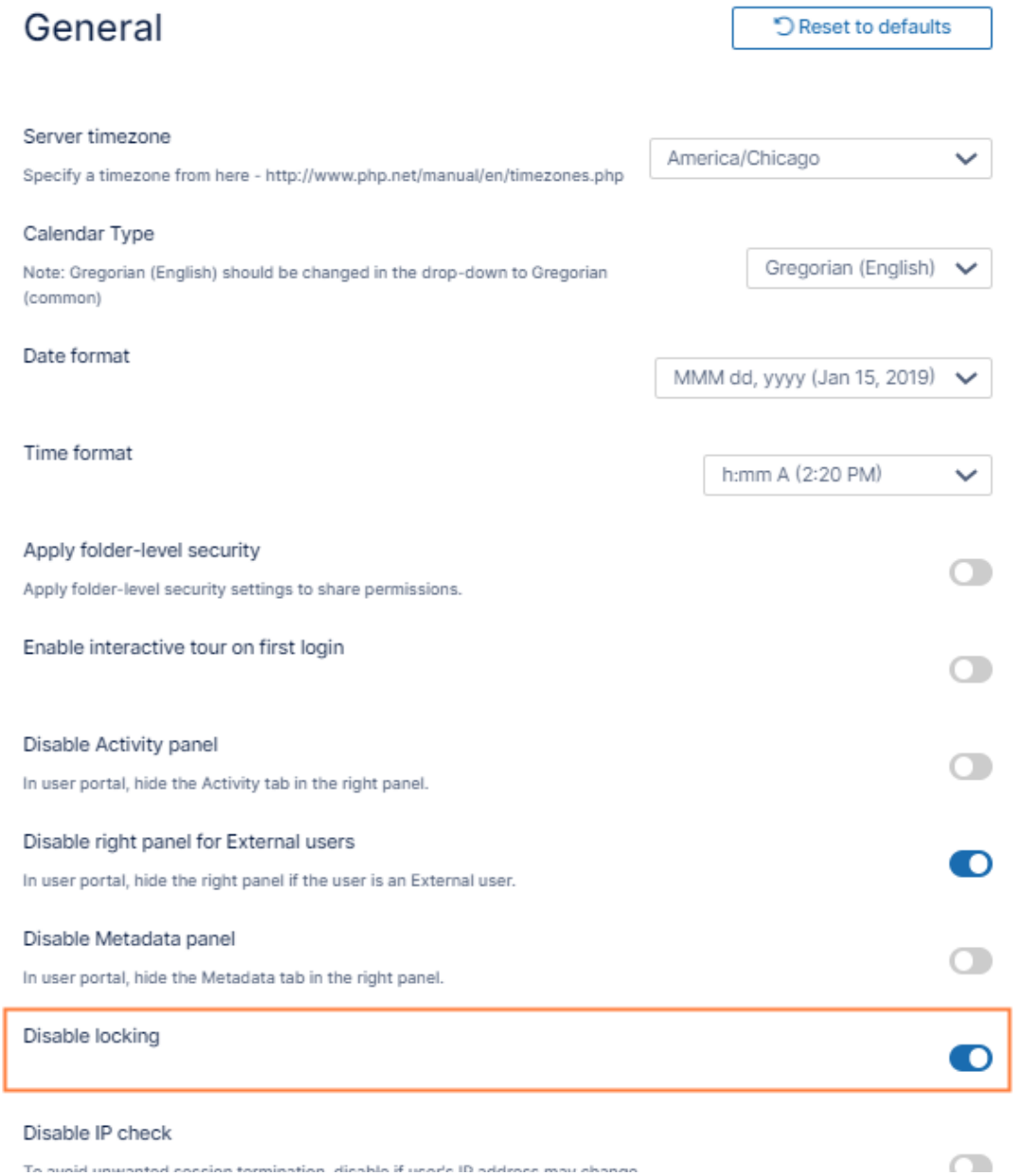
You can disable locking so that users are never given this option in the User Portal.

- This is a system-wide setting

- To release a lock on a single file or folder, see the topic for Releasing a Single Lock

To disable locking:

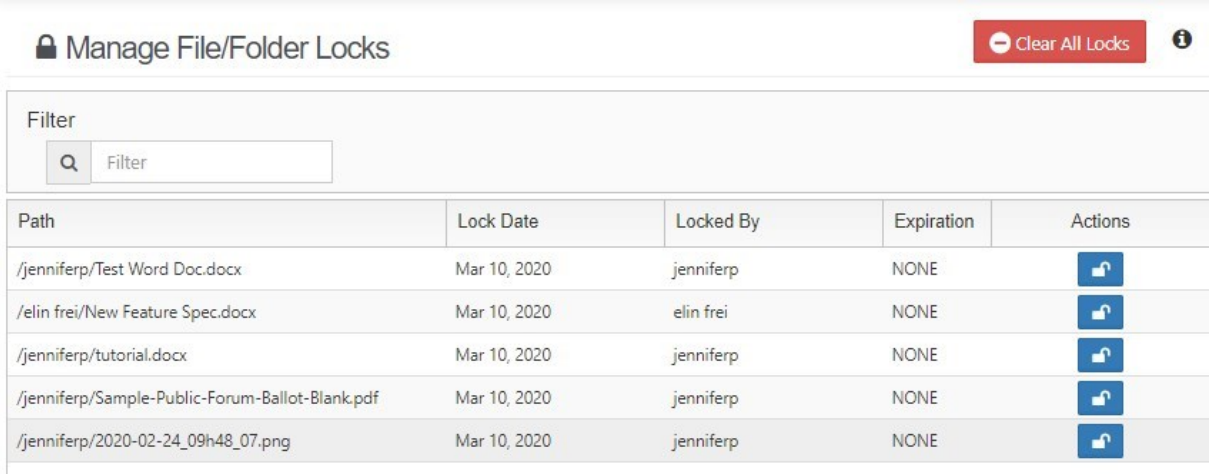
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   By default, **General** settings are opened.
2. Locate the setting **Disable locking**, and enable it.



3. Click **Save**.

How to View Which Files or Folders are Locked

Viewing a list of files and folders that are currently locked by FileCloud users helps you to manage locks.



To view a list of locked files and folders:

1. Log on to admin portal.
2. From the left navigation pane, click **User Locks**.
3. On the **Manage File/Folder Locks** screen, view the list of all files and folders currently locked.

You can use the **Filter** entry box to limit the list. To view only the locked files and folders, type in a string of characters. Only the files and folders that match the string will be displayed. To clear the filter, delete the string of characters from this box.

For example:

- You can filter the results by lock owner. To do this, type in the user account name.
- You can see all files that are locked in a particular folder. To do this, type in the name of the folder.

Release a Single Lock

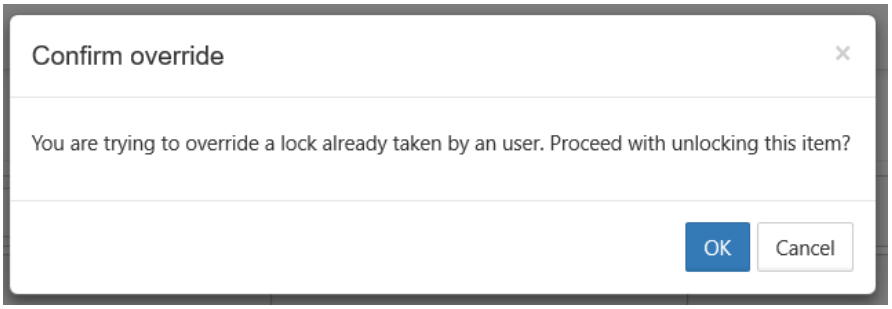
There are times when you may need to unlock a file for a user.

- A user no longer has a FileCloud account but has left a file locked
- A project folder can be used as a staging area that can be unlocked when the files are ready to be viewed
- Another user needs access to the file and the lock owner cannot be reached
- No one remembers why the file is locked

To release the lock on a single file or folder:

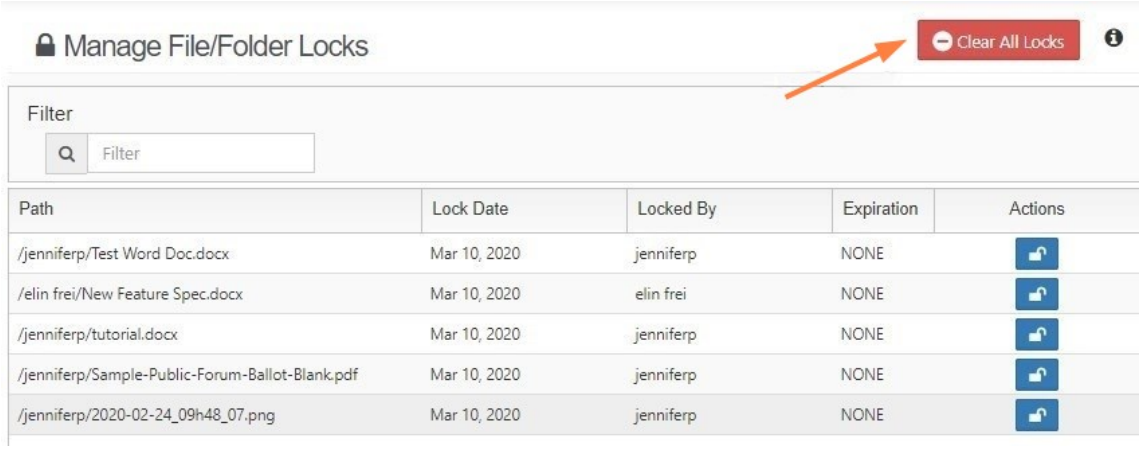
1. Log on to admin portal.
2. From the left navigation pane, click **User Locks**.
3. On the **Manage File/Folder Locks** screen, find the file or folder whose lock you want to remove.

4. In the row containing that file or folder name, under the **Actions** column, click the unlock button ( ).
5. On the **Confirm Override** screen, click **OK**.



To release the lock on all locked files and folders:

1. Log on to admin portal.
2. From the left navigation pane, click **User Locks**.
3. On the **Manage File/Folder Locks** screen, click **Clear All Locks**.



A confirmation dialog box opens.

4. Click **OK**.

Managing User-Defined Notifications

Users can configure notifications on their file and folder paths or admins can configure notifications on the paths for them. As an admin, you can add and edit these notifications.

Unless you check the **Disable User Override** setting in the policy assigned to a user, they can override your changes to their notification settings in the user interface.
See the page Notifications for file changes for information on disabling user overrides.

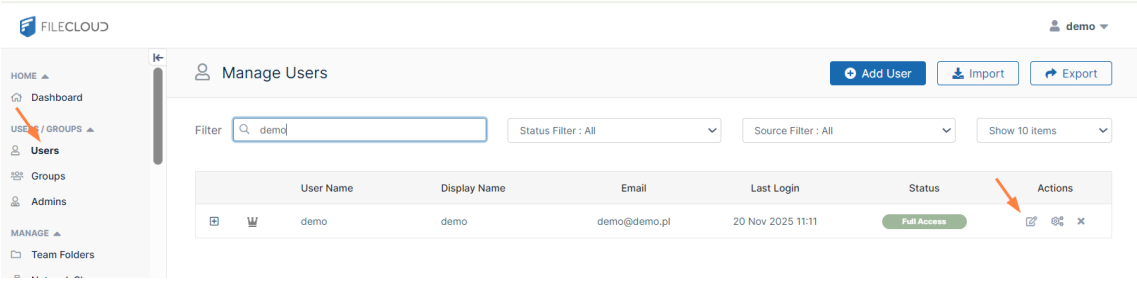
In this section:

Editing individual user's file and folder notifications

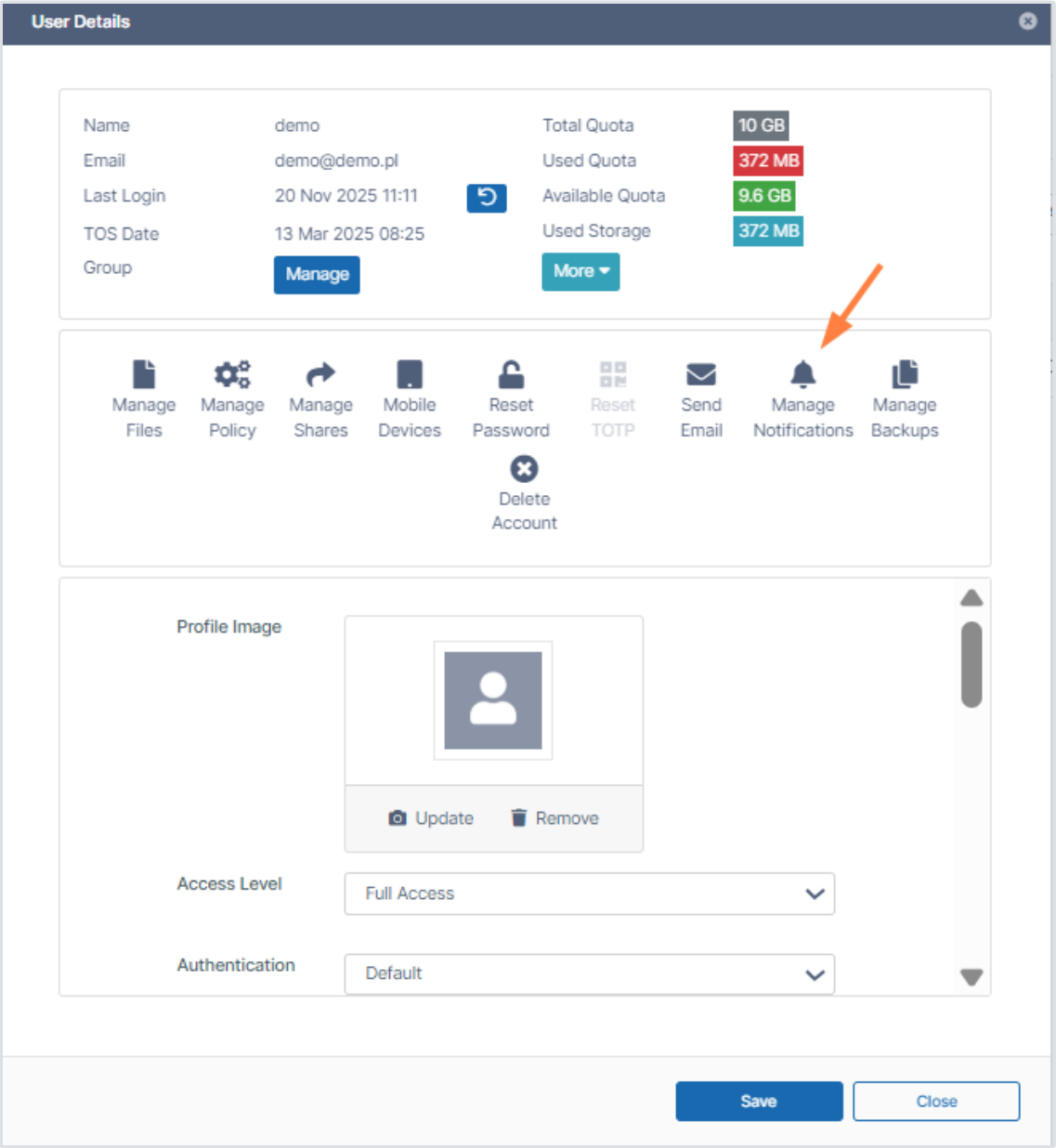
As an admin, you can edit notifications on a specific user's file and folder paths by clicking the **Manage Notifications** icon in the user's details.

To edit a user's file and folder notifications:

1. To open the **Manage Users** screen, In the navigation panel, click **Users**.
2. Click the edit icon across from the user.

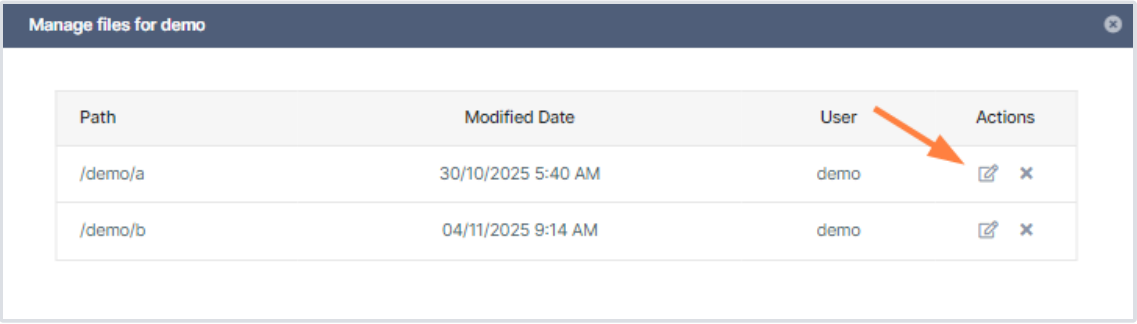


   The User Details dialog box opens.
3. Click the **Manage Notifications** icon.

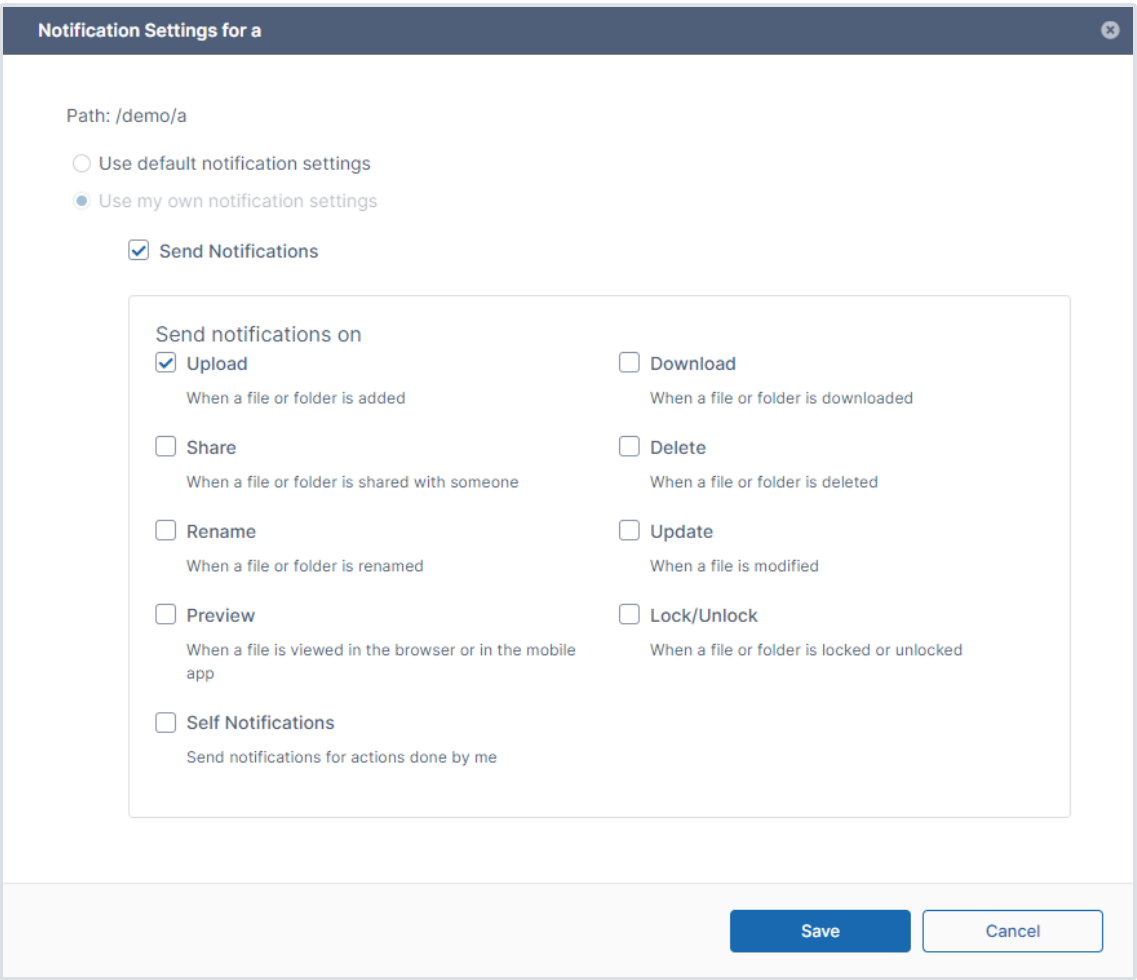


The **Manage Notifications for <user>** dialog box opens. All of the paths to files or folders with notifications defined on them are listed.

4. Click the edit icon in the row for path.



The **Notification Settings for <file/folder>** dialog box opens.



5. Edit the notification settings:
   - If you want to reset the user's settings to the defaults, check **Use default notification settings. Use my own notification settings** and all of the settings below it become unselected. If the user is permitted to override your settings, they may turn back on **Use my own notification settings** but will have to reset the individual settings.
   - If you want to to turn off notifications temporarily, uncheck **Send Notifications**; otherwise, leave it checked.

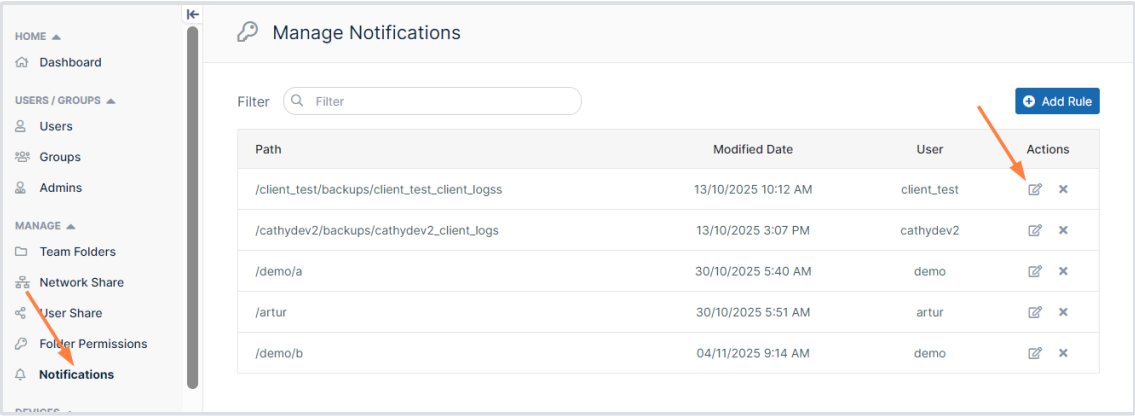
- If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
- If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications** box**.**
- If the user has **Use default notification settings** checked you can select **Use my own notification settings** and check **Send Notifications** and then check the boxes of the actions you want users notified about.

Editing all users file and folder path notifications

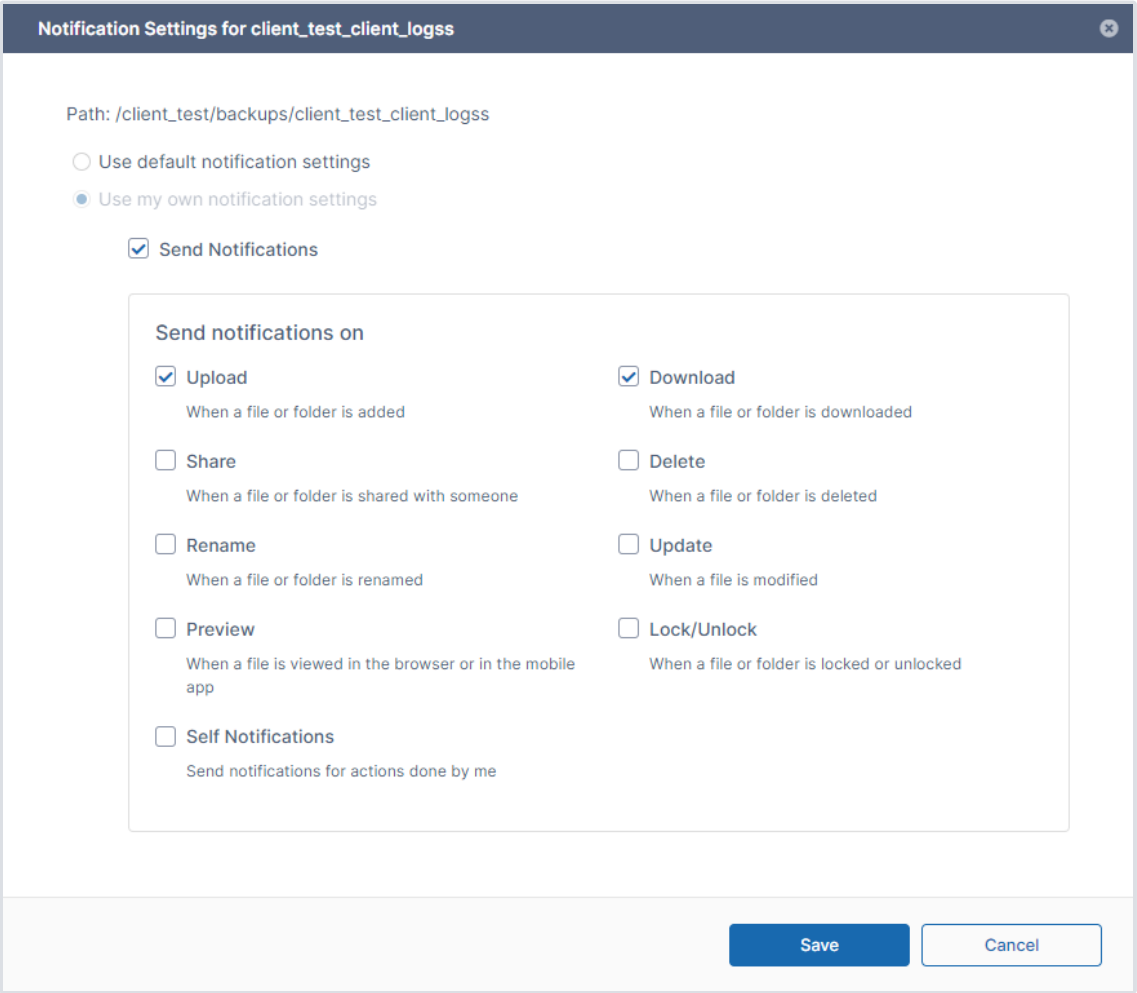
You can edit the notifications that users have defined for file and folder paths on the **Manage Notifications** screen. The screen shows all notifications assigned to paths for all users in your system.

To edit user-defined notifications on file and folder paths:

1. To open the **Manage Notifications** screen, in the navigation panel, click **Notifications**.
2. Click the edit icon in the row for the file or folder.



The Notification Settings for <file/folder> dialog box opens:



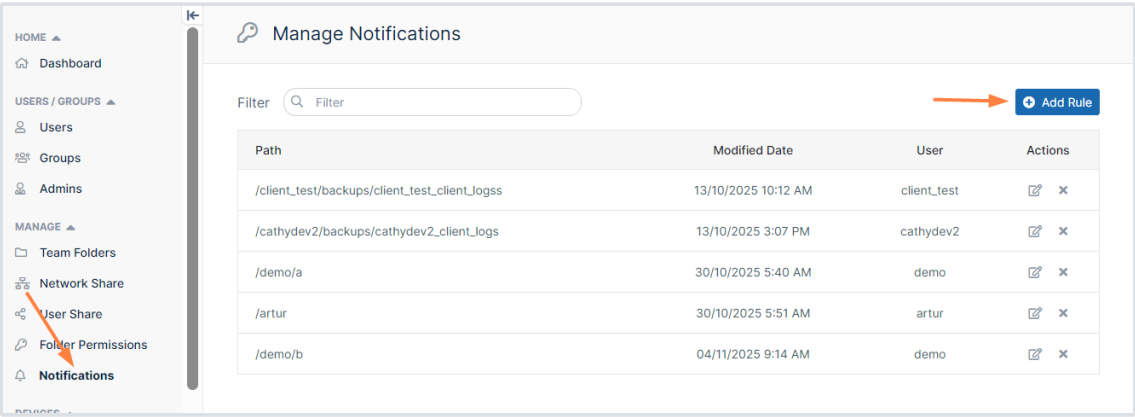
3. Edit the notification settings:
   - If you want to reset the user's settings to the defaults, check **Use default notification settings. Use my own notification settings** and all of the settings below it become unselected. If the user is permitted to override your settings, they may turn back on **Use my own notification settings** but will have to reset the individual settings.
   - If you want to to turn off notifications temporarily, uncheck **Send Notifications**; otherwise, leave it checked.
   - If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
   - If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications box.**
   - If the user has **Use default notification settings** checked you can select **Use my own notification settings** and check **Send Notifications** and then check the boxes of the actions you want users notified about.

Adding notifications for actions on user's files and folders

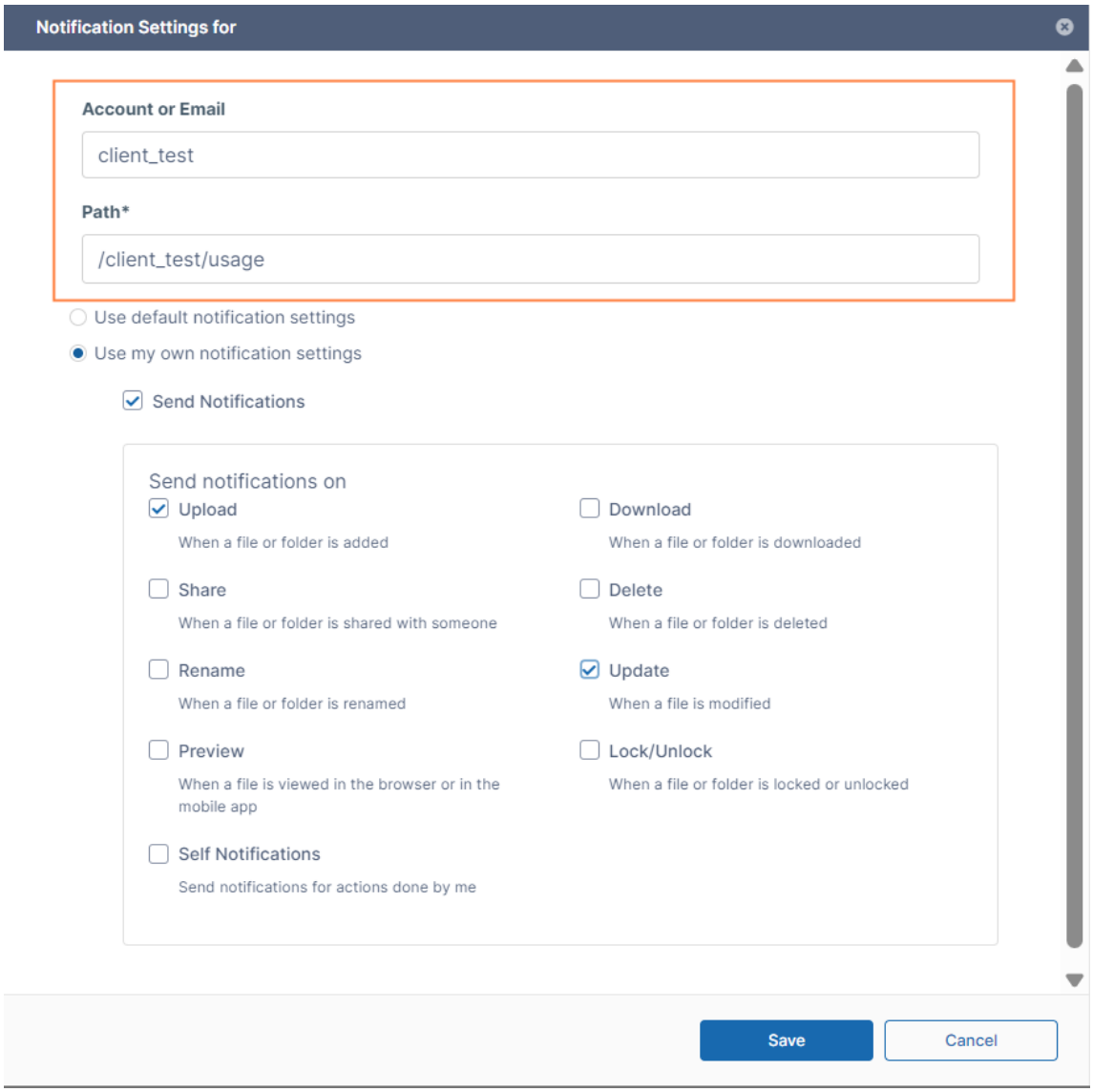
You can add notifications for actions performed on users' file and folder paths.

To add notifications to users files or folder

1. To open the **Manage Notifications** screen, in the navigation panel, click **Notifications**.
2. In the upper-right corner of the screen, click **Add Rule**.



The **Add Custom User Notifications Rule** dialog box opens:



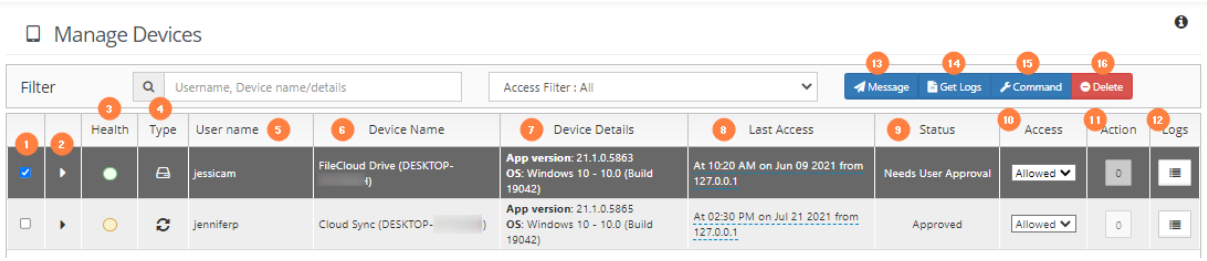
3. In **Account** or **Email**, enter the username or email address of the user.
4. In **Path**, enter the path to the file or folder in the user's storage.
5. Select **Use my notification settings**.
6. Check **Send Notifications**.
7. Below **Send Notifications on** check the actions for which you want to send share users notifications.
8. If you want the user who owns the file or folder to receive notifications about their own actions on it, check **Self Notifications**.
9. Click **Save**.

Managing Client Devices

> **Remote Device Management**
> You must be logged on as an Administrator or be a member of the Administrators group in order to perform Device Management actions.

As an administrator, you can manage the various clients connecting to the FileCloud instance.

- This feature is called Remote Client Management (RCM) or Data Leak Prevention Control (DLPC)



What Do All These Columns Mean?

Column	Title	Description
1	☐	Checkbox to identify the client device record you are working with
2	▸	Arrow to expand or collapse device details
3	**Health**	Health icon displayed as a color Green = Healthy Yellow = Needs Attention
4	**Type**	Client device icon
5	**User Name**	The account name that user logged in with on the client device
6	**Device Name**	The device name as setup by the client device. • This can be generic like "Cloud Sync" or "Client Drive" or specific like "Anis' iPhone 5"
7	**Device Details**	Displays the OS type, OS version and the Client App's version.

8	**Last Access**	Displays the last time this device connected to the FileCloud server • Also displays the location where the client connected from
9	**Status**	Indicates whether the device has been Approved or Not Approved for Access by the administrator
10	**Access**	Indicates if the device can connect or not. • Allow • Block • Remote wipe
11	**Action**	The list of queued actions for that client device, such as the number of messages.
12	**Logs**	Folder to view uploaded logs from the client
13	**Message**	Opens a window to send a message to the selected client
14	**Get Logs**	Retrieves the logs from the selected client
15	**Command**	Sends a configuration command to the selected client
16	**Delete**	Removes the selected client from the list of connect clients • Logs the user out of their account • Closes the connection • Removes data associated with the device • Removes any connection permissions associated with the device

FAQ's

What Devices Can Connect?

By Default, FileCloud will not allow non RCM Compliant clients to connect into FileCloud service. You can change this behavior in Server Settings page.

The following devices can connect to FileCloud Server and can be managed from the Admin Portal:

- **FileCloud iOS App**
- **FileCloud Android App**
- **FileCloud Windows Store App**
- **FileCloud Sync**
- **FileCloud Drive**
- **FileCloud Desktop for Windows**
- **FileCloud Desktop for macOS**
- **FC Outlook AddIn**
- **FC Office AddIn**
- **FC Desktop Edit**
- **FC File Browser**

Admin user will be able to see all devices that connected to a FileCloud server using the Admin Control Panel.

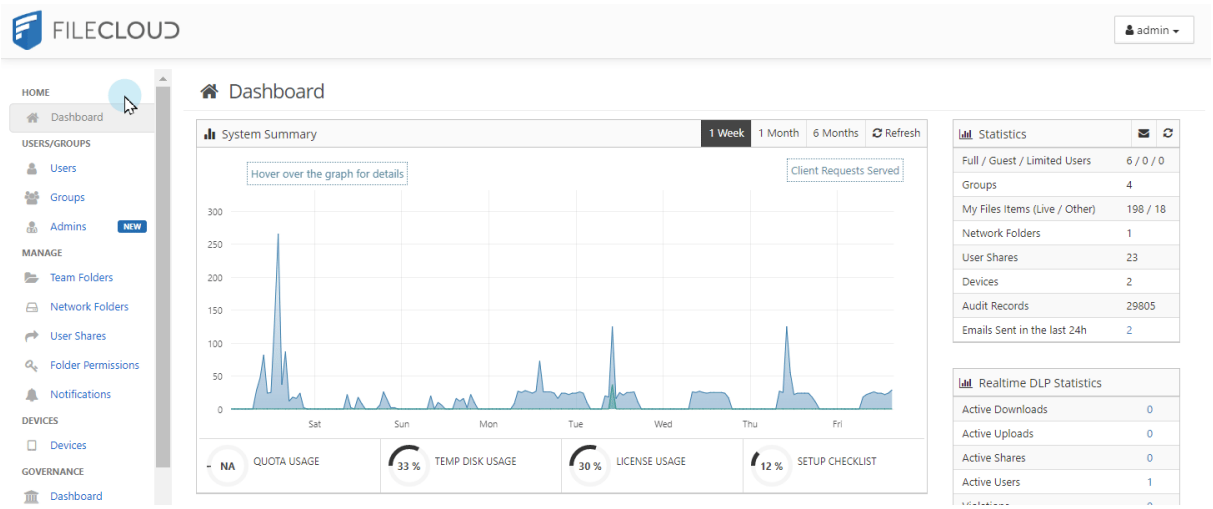
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

Where Can I See a List of Connected Devices?

An administrator can open the list of devices to manage using one of the following ways:

- Look on the Home dashboard of the Admin Portal
- Look on the **Devices dashboard in the Admin Portal**
- On a User Properties Popup, click **Manage Mobile Devices**

💡 Sometimes a list may start out empty. However, as users connect devices to the FileCloud Server by logging in, the devices will appear.



How Do You Want to Manage a Device?

The following operations are available from the Device Management panel:

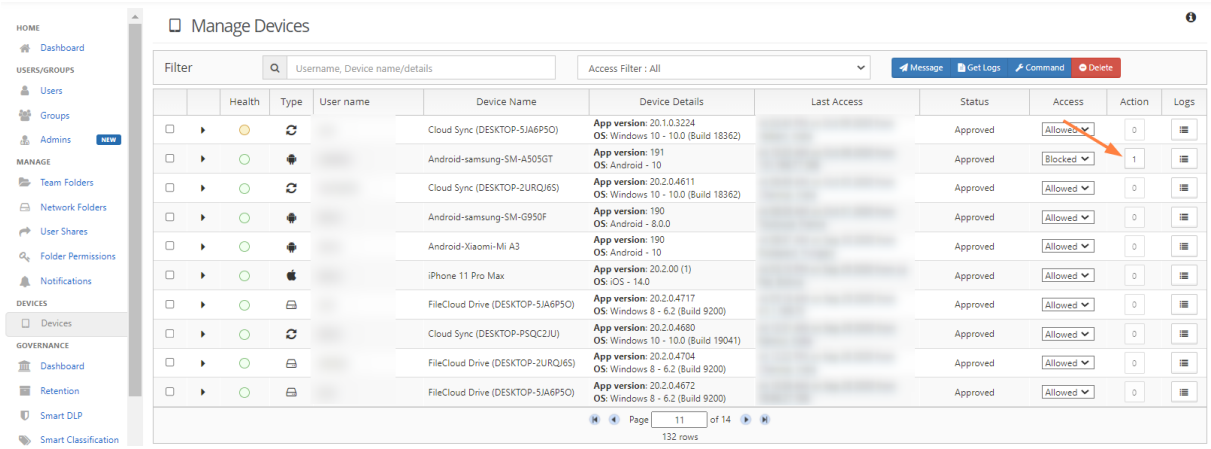
View Details of a Client Device

To see the details of a connected device:

1. Log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices***.
3. **On the *Manage Devices* screen, select the device you want details for.**
4. **In the second column, click the expand arrow (▶).**

View and Manage Actions Queued

If a message is queued to a device, it is possible to view them using the Admin Portal.



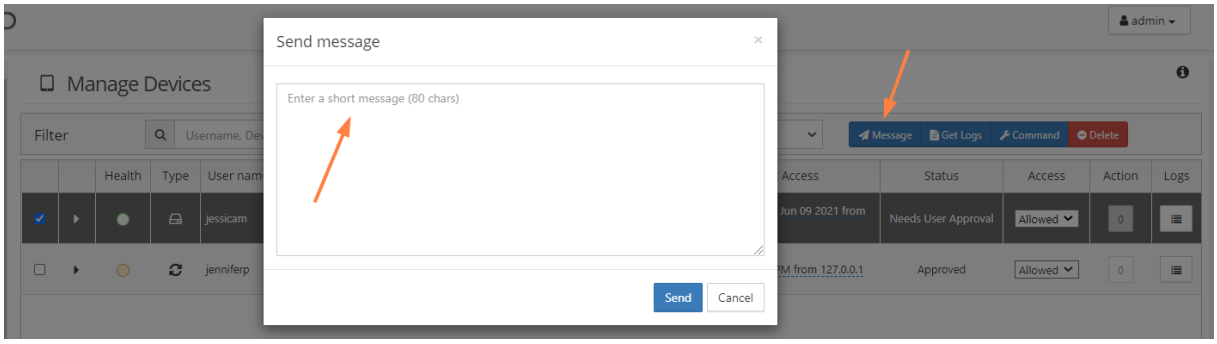
To view Actions:

1. Log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices*.**
3. **On the *Manage Devices* screen, select the device you want details for.**
4. In the *Actions* column, click the button.
5. Any queued action can be deleted from the pending actions list by clicking the Trash icon.

Add a Message to the Client's Display

An Admin can display a short message on the remote client using the "Add message" feature.

- The entered message(s) will be displayed when the remote client is connected to the FileCloud instance.
- If more than one message is queued to a device, they will be displayed in the order they were created.
- The messages will be shown only once per client
- The messages will be shown when the client connects to the FileCloud server (as a part of login operation)
- If the client is already connected, then it will retrieve the message periodically and display it to the user



To send a message:

1. Log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices*.**
3. On the *Manage Devices* screen, select the device to send a message to.
4. Click **Add Message**, type in the message, and then click **Send.**

Blocking and Remote Wiping

FileCloud's RMC function allows the Administrator to selectively block a specific client device from logging into the FileCloud server.

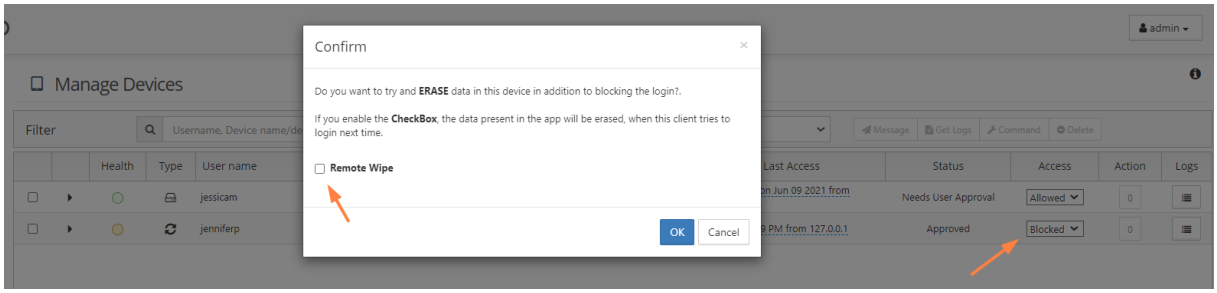
When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

- If the client is not connected, the block (and remote wipe) will happen when it tries to log into the server
- If the client is connected, the block and remote wipe will occur and the client will automatically exit out

💡 In addition to Blocking a Client Device from logging in, Administrator can also wipe FileCloud folders in the remote device.

The remote wipe will have the following effect on each of the clients

1.
    - FileCloudDrive: Cache folder data will be deleted and application will logout
    - FileCloudSync: Synced data will be deleted and application will logout
    - iOS and Android: Downloaded data in "This Device" will be deleted and will log out of the server



To block (but not wipe remote data):

1. Open a browser and log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices***.
3. On the *Manage Devices* screen, select the device you want to block.
4. In the ***Permissions*** column, select ***Blocked***.
5. On the ***Confirm*** dialog, to just block but not remote wipe the client device, clear the *Remote Wipe* checkbox.
6. Click *OK*.

To block and wipe remote data in a client device:

1. Open a browser and log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices***.
3. On the *Manage Devices* screen, select the device you want to block and wipe.
4. In the ***Permissions*** column, select ***Blocked***.
5. On the ***Confirm*** dialog, select the *Remote Wipe* checkbox.

6. Click *OK*.

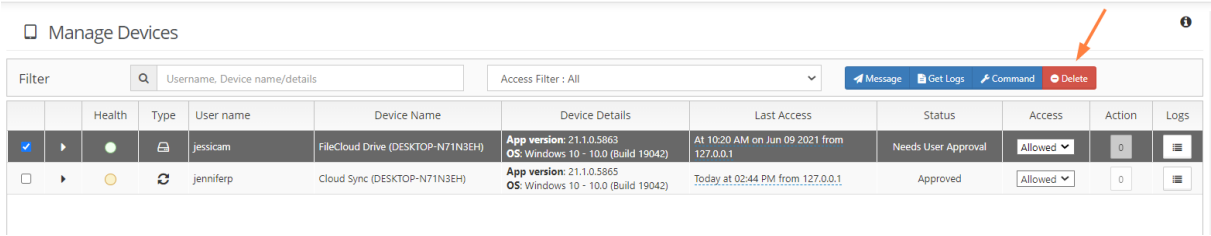
Delete a Client Device Record

It is possible to delete a client record from the FileCloud system.

You might want to use this feature when:

- The userid is no longer valid
- The associated client record no longer needs to be managed

💡 If you want to keep the device record but do not want to allow it to connect for a period of time, you can use the Block action.



To delete a client device record:

1. Open a browser and log into *Admin Portal*.
2. From the left navigation panel, under *DEVICES*, select ***Devices***.
3. On the *Manage Devices* screen, select the device you want to delete.
4. At the top of the screen, click the Delete button.

Centralized Device Management

Administrators can manage devices from the Admin Portal after remote management is enabled in FileCloud Sync.

You can use Device Management features to configure device settings like client configurations and apply them all-at-once to users or groups.

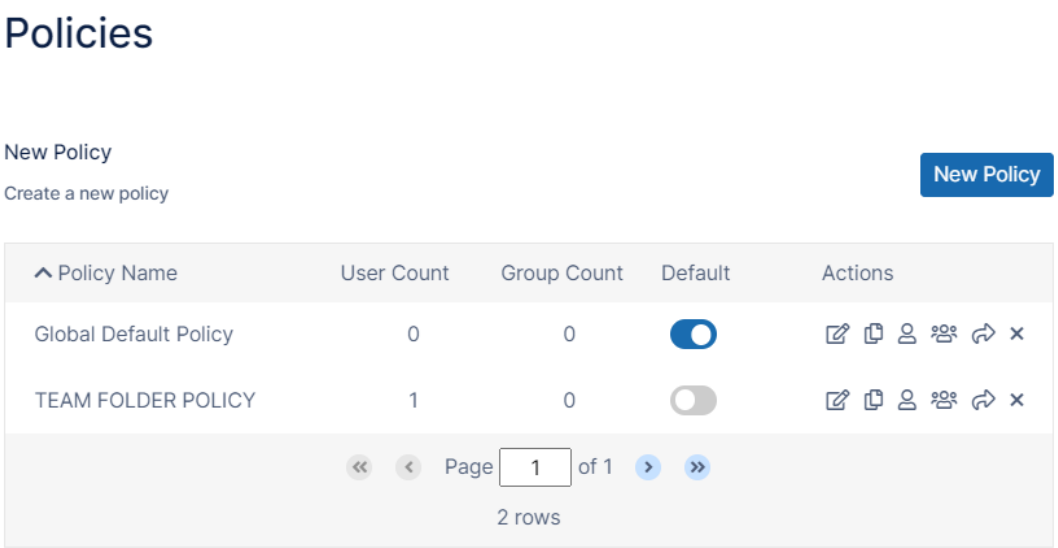
Configure Centralized Device Management

Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.
For the Sync client, when an Admin sets a remote client policy, a user working in the Sync app cannot modify the settings. Sync will display a message saying "Centralized Configuration is being applied. Settings cannot be changed.".

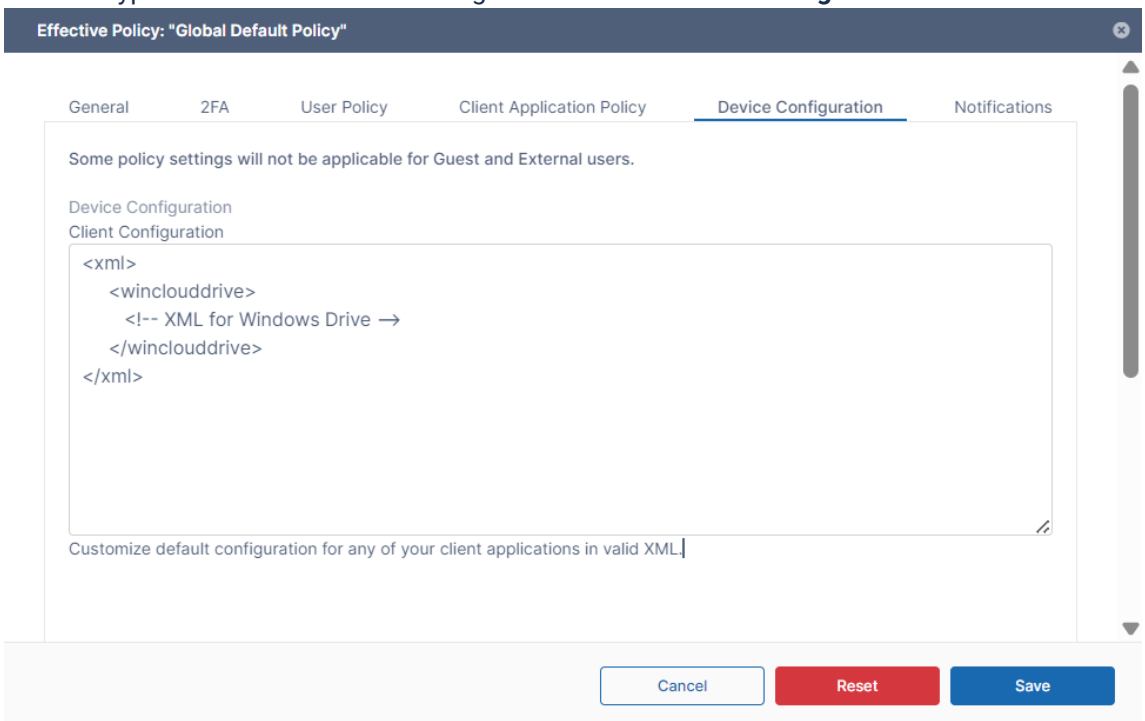
To set a device configuration for a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.

4. Paste or type in the remote device configuration XML in **Device Configuration**.



5. Click **Save**.

Device configuration is specified via XML, the general format of the XML is as follows

```
<xml>


     <wincloudrive>
        <!-- XML for Windows Drive -->
     </wincloudrive>


     <macclouddrive>
        <!-- XML for Mac Drive -->
      </macclouddrive>


     <cloudsync>
        <!-- XML for Sync App -->
     </cloudsync>


      <fssync>
        <!-- XML for ServerSync App -->
      </fssync>


      <filecloudesktopmac>
         <setting>
```

```
            <key>runatstartup</key>
            <value>1</value><
            <default>1</default>
        </setting>
    </filecloudesktopmac>


    <filecloudesktopwindows>
        <setting>
            <key>runatstartup</key>
            <value>1</value>
            <default>1</default>
        </setting>
    </filecloudesktopwindows>



</xml>
```

What do you want to configure?

Device Configuration XML For Drive for Mac

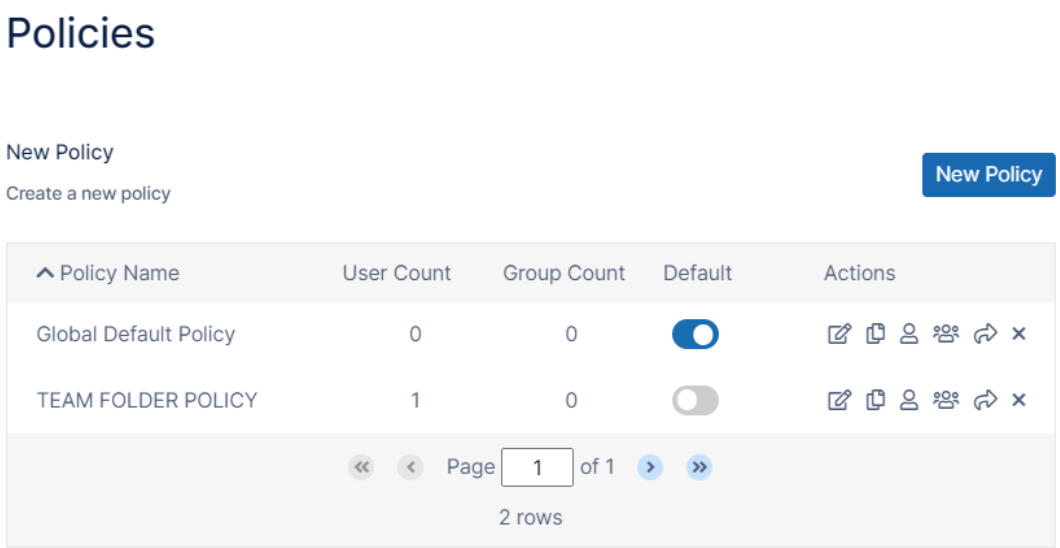
Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set FileCloud Drive for mac device configuration in a policy:

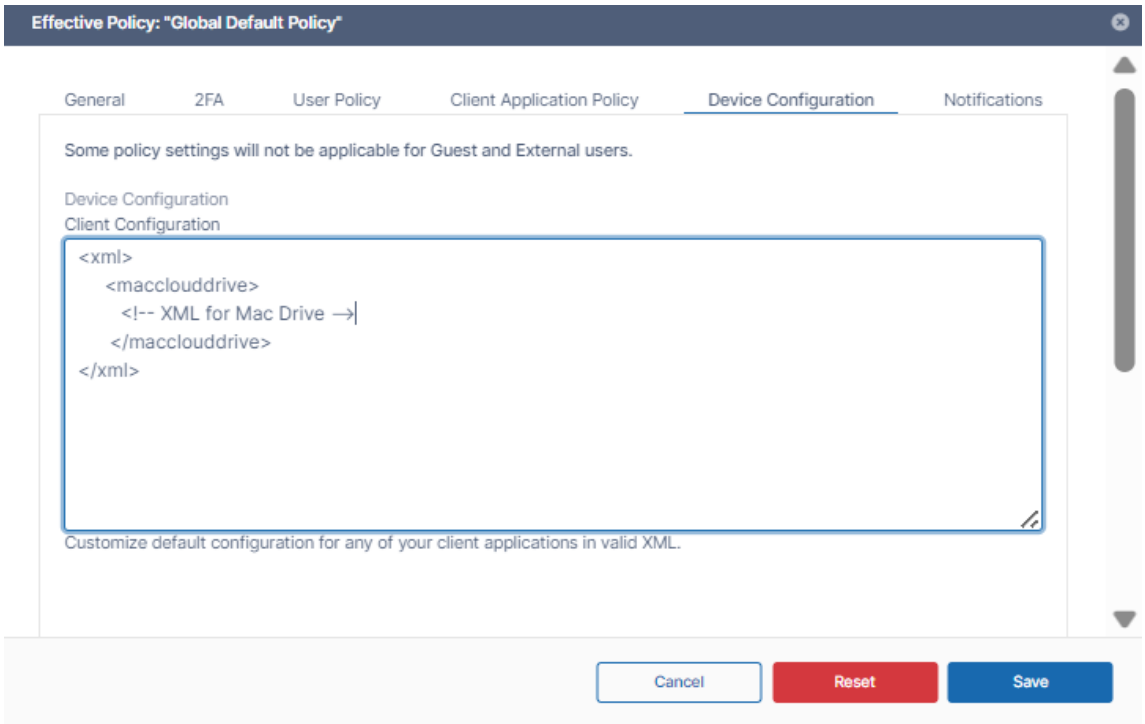
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for Mac Drive -->** with any parameters from the table below.

```
<xml>
     <macclouddrive>
        <!-- XML for Mac Drive -->
      </macclouddrive>
</xml>
```



Supported parameters for FileCloud Drive for Mac. All parameters are optional. Add one of more of these parameters (as XML tags) in the <maccloudrive> tags in the XML.

Parameter (XML Tag)	Value	Example
maxdownloadsizeinmb	Assigns the maximum single file download limit to the supplied value. The download limit does not apply to the following file types: .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .indd.	<maxdownloadsizeinmb>100</maxdownloadsizeinmb>
driveloginmode	Setting this to "0" will cause filecloud drive to use username/password to log into the Filecloud server. Setting this value to "1" will cause drive to use device code authentication mode	<driveloginmode>1</driveloginmode>
drivelocknupdate	Setting this value to 1 will enable automatic lock on edit function in FileCloud Drive. Setting this to 0 will disable the drive's lock on edit function	<drivelocknupdate>1</drivelocknupdate>

Parameter (XML Tag)	Value	Example
drivemutemessages	Setting this value to 1 will disable system tray notifications being shown to the user.	<drivemutemessages>1</drivemutemessages>
driveopenexplorerononstartup	Setting this value to 1 will automatically open finder when drive starts up and 0 will disable it.	<driveopenexplorerononstartup>1</driveopenexplorerononstartup>
checkupdates	Setting this value to 1 will enable automatic checking for new versions of FileCloud Drive for Mac and setting this value to 0 will disable it.	<checkupdates>1</checkupdates>
disableprecaching	Setting this value to 1 disables precaching. If many Drive users have access to a large data structure, the FileCloud server may experience a high load. This can be avoided by deactivating precaching. However, folder contents will no longer be cached in Drive which can lead to longer response times.	<disableprecaching>1</disableprecaching>
disableautologin	By default, once a drive is mounted, the authentication will be reused on every FileCloud Drive for Mac start ups. Setting this key to 1 will require authentication from user on every start up.	<disableautologin>1</disableautologin>
currentlanguage	Currently available languages.	<currentlanguage>english</currentlanguage>

Device Configuration XML For Outlook Add-in

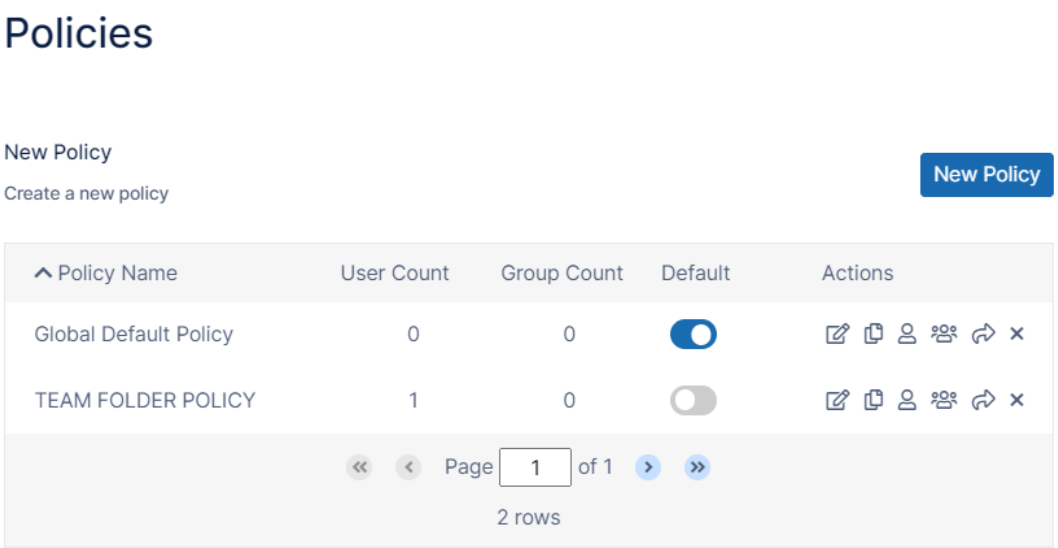
FileCloud for Outlook Add-in configuration settings can be configured remotely by specifying the configuration XML using policies.

For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set FileCloud's Outlook add-in device configuration for a policy:

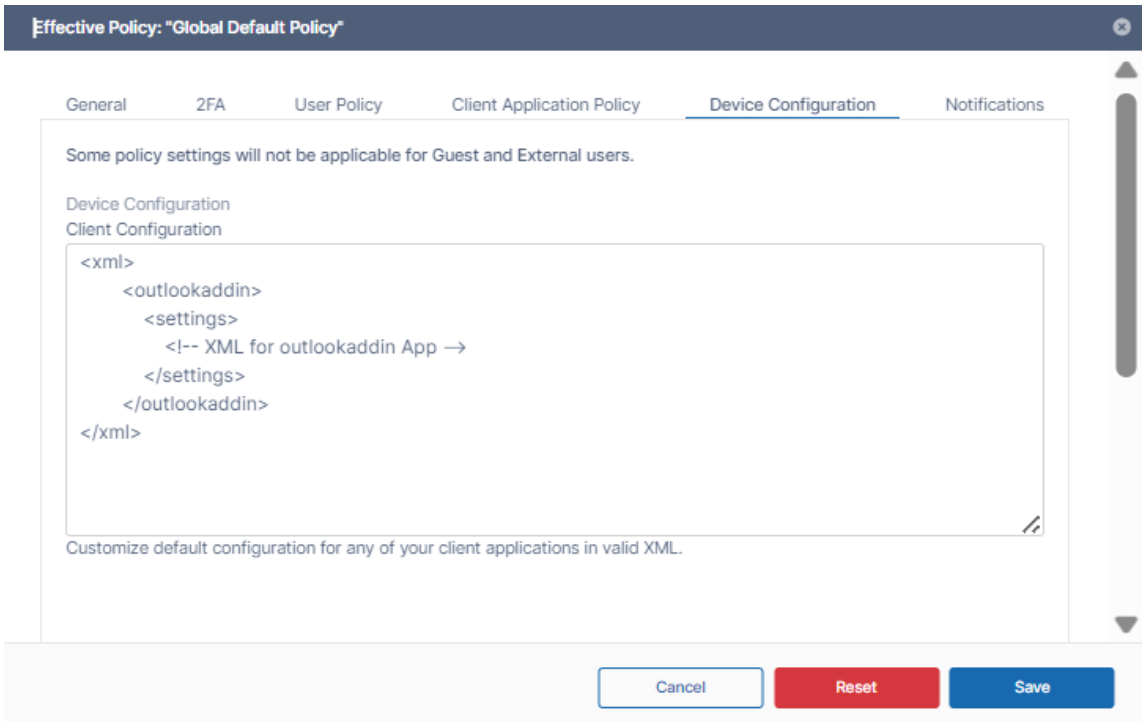
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for outlookaddin App -->** with any parameters from the table below.

```
<xml>
    <outlookaddin>
            <settings>
            <!-- XML for outlookaddin App -->
            </settings>
    </outlookaddin>
</xml>
```



Supported parameters for the FileCloud Outlook add-in. All parameters are optional. Add one of more of these parameters (as XML tags) in the <settings> tags in the above XML.

Parameter (XML Tag)	Value	Example
autoupload	Whether autoupload is on or off. 0 = off, 1= on	<autoupload>1</autoupload>
autouploadsize	The minimum size in MB an attachment must be to be automatically uploaded	<autouploadsize>3</autouploadsize>
serverurl	FileCloud server URL	<serverurl>http://www.yourdomain.com</serverurl>
sharetype	Share Type 0 = Public Share, 1= Password Protected Share	<sharetype>0</sharetype>
sharetext	Share Text in HTML. Ensure to use CDATA to accomodate special characters in xml	<sharetext><![CDATA[Attachment: #filename# Download link: #filename# #password#]]></sharetext>

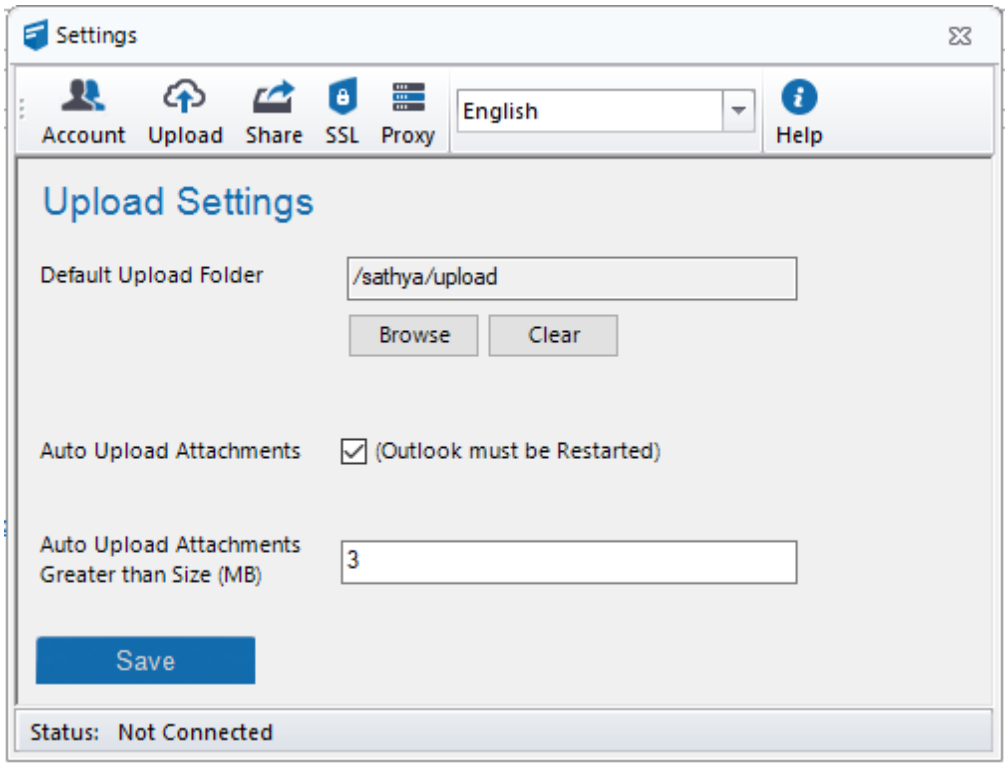
Parameter (XML Tag)	Value	Example
proxyserver	Proxy Server URL	<proxyserver>http://proxyserverurl.com</proxyserver>
proxyusername	Proxy Server Username	<proxyusername>proxyserverusername</proxyusername>
proxypassword	Proxy Server Password	<proxypassword>proxyserverpassword</proxypassword>
proxyport	Proxy Server Port	<proxyport>9000</proxyport>
ssllevel	Require strict SSL verification of VERIFY_STRICT or VERIFY_NONE	<ssllevel>VERIFY_STRICT</ssllevel>
sslverify	Connect only TLS 1.2 server. Empty string or TLSV1_2_CLIENT_USE	<sslverify><sslverify>

To set default values for auto upload:

In the Outlook add-in device configuration, you can set the default values for **Auto Upload Attachments** and **Auto Upload Attachments Greater than Size (MB)**.
Follow the instructions above for setting the device configuration, and enter values: for <autoupload> and <autouploadsize>, for example:

```
<xml>
    <outlookaddin>
            <settings>
                <autoupload>1</autoupload>
                <autouploadsize>3</autouploadsize>
            </settings>
    </outlookaddin>
</xml>
```

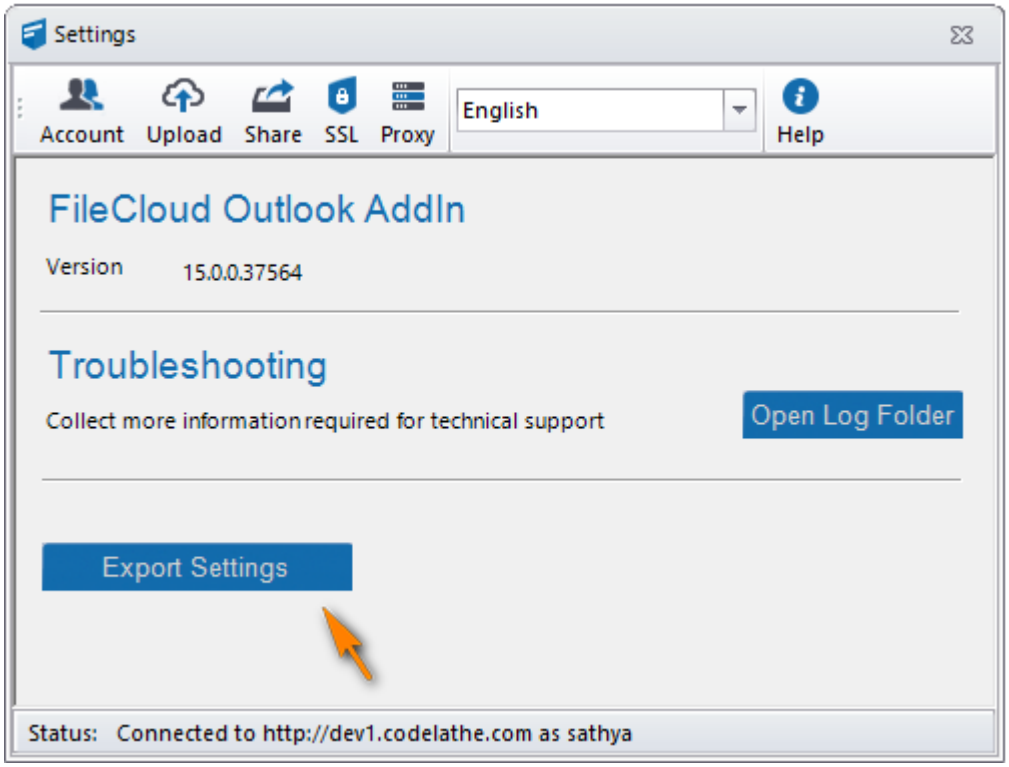
When the Outlook Add-in is opened, and **Settings > Upload** is accessed, the **Auto Upload Attachments** and **Auto Upload Attachments Greater than Size (MB)** settings appear as:



Tips and Tricks

The easiest way to get the configuration XML for sync apps is by configuring an Outlook Add-in as needed and then exporting the configuration.

Show me how...



Device Configuration XML For Server Sync

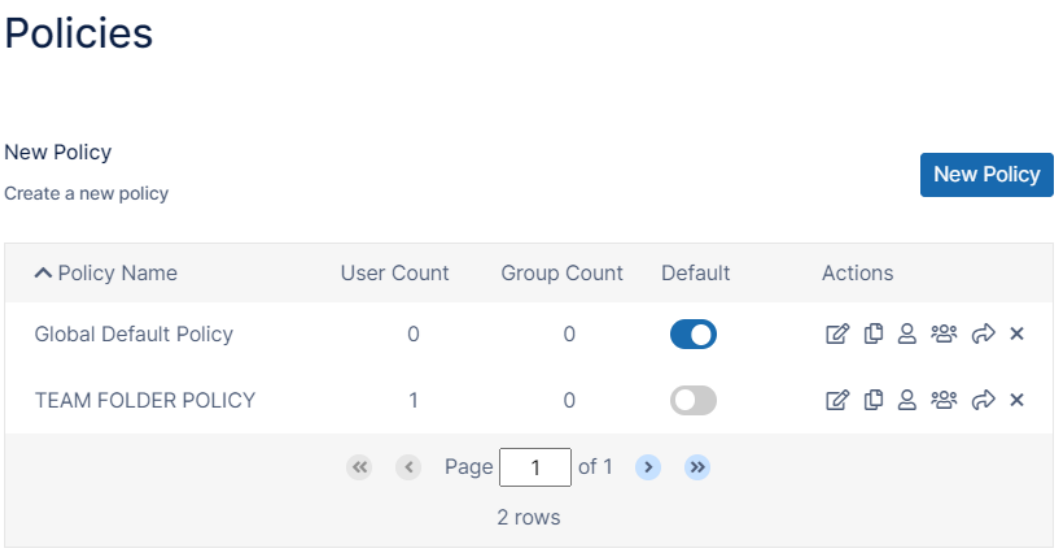
Client Device configuration settings can be configured remotely using policies.

> For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set a ServerSync device configuration in a policy:

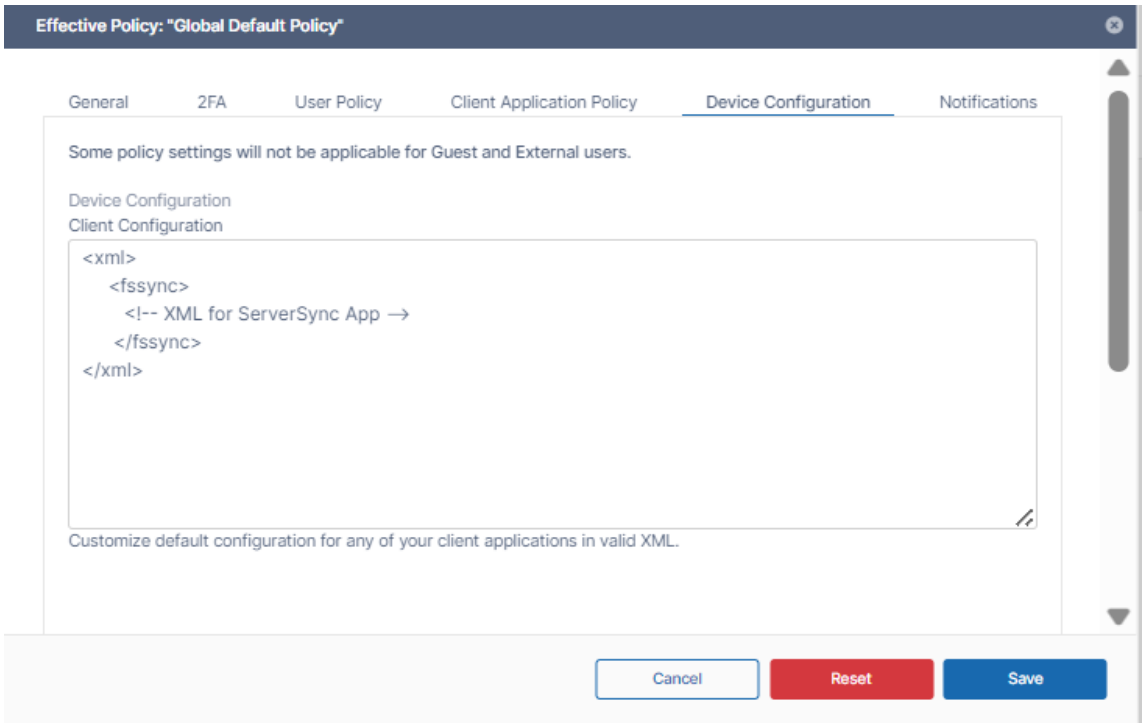
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for ServerSync App -->** with any parameters from the table below.

```
<xml>
     <fssync>
        <!-- XML for ServerSync App -->
      </fssync>
</xml>
```



Supported parameters for FileCloud ServerSync. All parameters are optional. Add one of more of these parameters (as XML tags) in the <fssync> tags in the XML.

XML Tag	Value	Example
limit_folder_count	Number of folders to sync. If key is not specified, then there are no folders to sync.	<limit_folder_count>0</limit_folder_count>
limit_folder_1 limit_folder_2 limit_folder_3 ...	Depending upon the number of folders specified in the limit_folder_count, you will need to have the appropriate number of entries. The folder value is specified using 5 parameters using the following format ***<REMOTE FOLDER>|<LOCAL FOLDER>|<PERMISSIONS>|<SYNC TYPE>|<SYNC DISABLED>*** ***<REMOTE FOLDER>*** = E.g.: /john/folder1 ***<LOCAL FOLDER>*** = E.g: C:\data\localfolder ***<PERMISSION>*** = 1 - Allow NTFS permissions to be applied to local folder as per permissions of the folder on the remote Server, 0 - Deny NTFS permissions to be applied ***<SYNC TYPE>*** = 0 (2-way sync) or 1 (remote to local sync). ***<SYNC DISABLED>*** = 0 (enabled) or 1 (disabled).	<limit_folder_1>/john/folder1|C:\data\local|0|1|0</limit_folder_1>

XML Tag	Value	Example
disablenotifications	0/1 - Enable or Disable sync notifications	<disablenotifications>1</disablenotifications>
syncfrequency	number - Number in seconds to sync to the server (default is 120 seconds)	<syncfrequency>100</syncfrequency>
checkmodtime	0/1 - Advanced: check modification time in addition to size when checking for changes. Default is disabled.	<checkmodtime>1</checkmodtime>
checkcrc	0/1 - Advanced: check CRC in addition to size when checking for changes. Default is disabled.	<checkcrc>1</checkcrc>
deleteapprovalpct	Number from 0 to 100, which indicates what % of files being deleted requires approval. Default is 10. This applies only to file deletions in the local sync folder.	<deleteapprovalpct>20</deleteapprovalpct>
skipdeleteapproval	0/1 - Whether approvals are needed for bulk sync deletions. Default is disabled. When set to 1, approval is required if > 50 files are deleted AND percent of files being deleted is > **deleteapprovalpct**. This applies only to file deletions in the local sync folder.	<skipdeleteapproval>1</skipdeleteapproval>
currentlanguage	Allows changing the current language of the Server sync app	<currentlanguage>dutch</currentlanguage>

Device Configuration XML For Sync

Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

For the Sync client, when an Admin sets a remote client policy, a user working in the Sync app cannot modify the settings. Sync will display a message saying "Centralized Configuration is being applied. Settings cannot be changed."
Any Sync settings in the config xml block the user's ability to configure selective sync, network folder, and backup folder settings. If you want users to be able to continue to change these settings, set the allowuserconfigforlimitsync, allowuserconfigfornwfolders, and allowuserconfigforbackup tags to 1 in the policy.

- allowuserconfigforlimitsync - enables users to select selective sync folders
- allowuserconfigfornwfolders - enables users to select network folders
- allowuserconfigforbackup - enables users to select backup folders

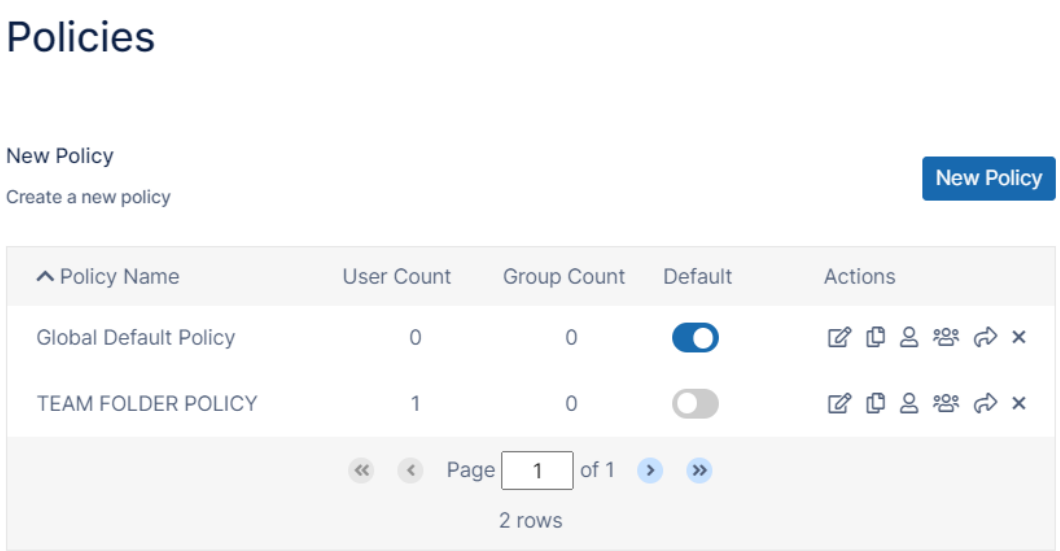
See What XML settings allow users to modify folders? below.

FAQs

How do I enter device configuration XML for Sync?

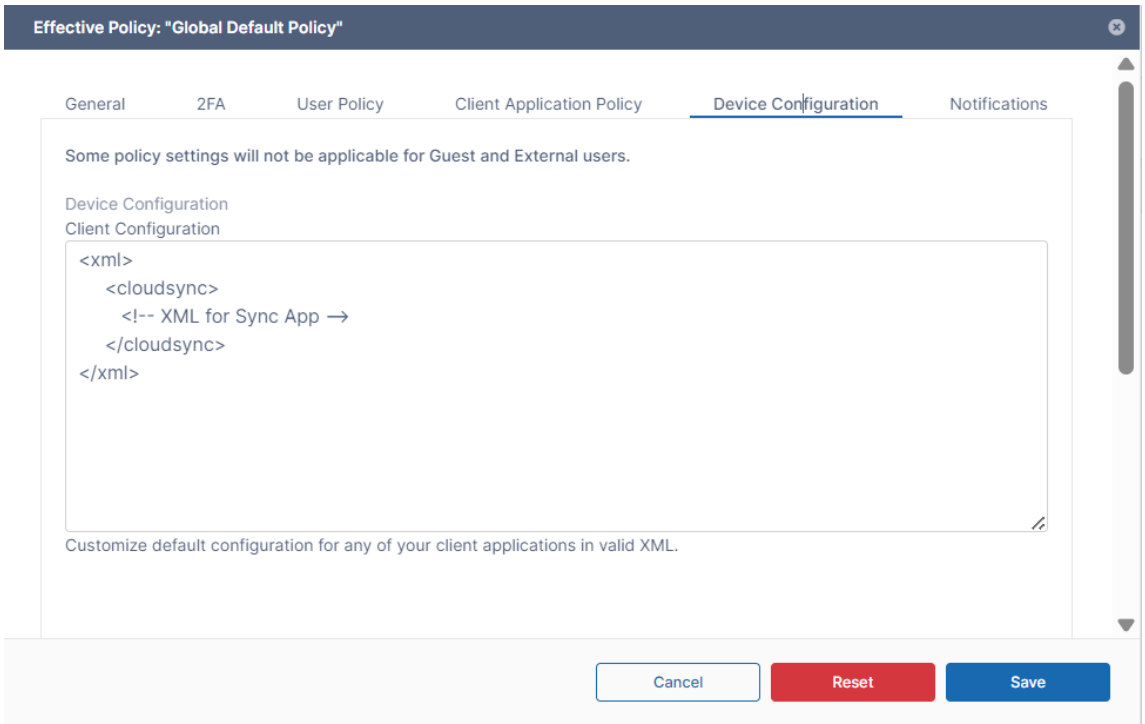
To set a FileCloud Sync device configuration in a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for Sync App -->** with any parameters from the table below.

```
<xml>
     <cloudsync>
        <!-- XML for Sync App -->
     </cloudsync>
</xml>
```



Supported parameters for FileCloud Sync. All parameters are optional. Add one of more of these parameters (as XML tags) in the <cloudsync> tags in the XML.

Parameter (XML Tag)	Value	Example
limitfolders	'|' separated list of folders for selective sync. If Limitfolders is not specified, then there are no folders for selective sync.	<limitfolders>/john/folder1|/john/folder2</limitfolders>
offline_folder_count	Number of offline folders to sync. If key is not specified, then there are no offline folders.	<offline_folder_count>0</offline_folder_count>

Parameter (XML Tag)	Value	Example
offline_folder_1 offline_folder_2 offline_folder_3 ...	Depending upon the number of offline folders specified in the offline_folder_count, you will need to have the appropriate number of entries. The folder value is specified using 6 parameters using the following format **<LOCAL FOLDER>|<REMOTE FOLDER>|<SYNCTYPE>|<SCHEDULE>|<RECURSE INTO DIRECTORIES>|<ALLOW REMOTE DELETION>|<SENDEMAIL>** **<LOCAL FOLDER>** = E.g: C:\data\localfolder **<REMOTE FOLDER>** = E.g.: /john/folder1 **<SYNC TYPE>** = 0 - 2 Way Sync, 1 - Backup from Local to Remote, 2 - Read only copy of remote files to local **<SCHEDULE>**= 1h (every 1 hour), 2h (every 2 hours), 4h (every 4 hours), 8h (every 8 hours), 24h (every 24 hours), 30m (every 30 minutes), manual (Manual), realtime (Real-time syncing) **<RECURSE INTO DIRECTORIES>** = 1 - Recurse (top level and sub folders are synced), 0 - Not Recurse (only top level folder is synced) **<ALLOW REMOTE DELETION>** = 1- Allowed (Local deletes are not propagated to server) , 0-Disallowed (Local deletes are not propagated to server) **<SENDEMAIL>** = 1 - Send Email after backups, 0-No Email	<offline_folder_1>C:\data\local|/john/folder1|0|30m|1|0|0</offline_folder_1>
disablenotifications	0/1 - Enable or Disable sync notifications.	<disablenotifications>1</disablenotifications>
showlocks	0/1 - Enable or Disable if lock information is shown in icon overlay	<showlocks>1</showlocks>
syncfrequency	number - Number in seconds to sync to the server (default is 120 seconds)	<syncfrequency>100</syncfrequency>
checkmodtime	0/1 - Advanced: check modification time in addition to size when checking for changes. Default is disabled.	<checkmodtime>1</checkmodtime>
checkcrc	0/1 - Advanced: check CRC in addition to size when checking for changes. Default is disabled.	<checkcrc>1</checkcrc>
removeunshared	0/1 - Delete locally synced folders that are unshared. Default is disabled	<removeunshared>1</removeunshared>
deleteapprovalpct	Number from 0 to 100, which indicates what % of files requires deletion approval. Default is 10. This applies only to file deletions in the local sync folder.	<deleteapprovalpct>20</deleteapprovalpct>

Parameter (XML Tag)	Value	Example
skipdeleteapproval	0/1 - Whether approvals are needed for bulk sync changes. Default is disabled. When set to 1, approval is required if > 50 files are deleted AND percent of files being deleted is > **deleteapprovalpct**. This applies only to file deletions in the local sync folder.	<skipdeleteapproval>1</skipdeleteapproval>
currentlanguage	Allows changing the current language of the Sync app	<currentlanguage>dutch</currentlanguage>
globalbwforupload	Specifies the bandwidth limit when uploading files from the client to the server in terms of KB only. This limit can be different from the download limit.	<globalbwforupload>100</globalbwforupload>
globalbwfordownload	Specifies the bandwidth limit when downloading files from the server to the client in terms of KB only. This limit can be different from the upload limit.	<globalbwfordownload>50</globalbwfordownload>
altbwforupload	Specifies that alternative settings should be used instead of the global bandwidth limit when uploading files from the client to the server in terms of KB only. ⚠️ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set.	<altbwforupload></altbwforupload>
altbwfordownload	Specifies that alternative settings should be used instead of the global bandwidth limit when downloading files from the server to the client in terms of KB only. ⚠️ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set.	<altbwfordownload></altbwfordownload>
altbwfromtime	Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit. Time must be expressed in the format HH:MM:SS ⚠️ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set.	<altbwfromtime>16:45:00</altbwfromtime>

Parameter (XML Tag)	Value	Example
altbwtotime	Specifies the ending time when the alternative settings should be used instead of the global bandwidth limit. Time must be expressed in the format HH:MM:SS ⚠️ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set.	<altbwtotime>24:00:00</altbwtotime>
altbwschedule_dayofweek	Specifies the days of the week when the alternative settings should be used instead of the global bandwidth limit. This value can be any number such as: {-1, 0, 1, 2, 3, 4, 5, 6} where: • -1 means every day • 0 means Sunday • 1 means Monday • and so on...	<altbwschedule_dayofweek>3</altbwschedule_dayofweek>
timeactivecontrolsset	Enables/Disables the Active Sync Hours settings 1 = enabled 0 = disabled	<timeactivecontrolsset>1</timeactivecontrolsset>
activesync_daysofweek	Specifies the days of the week when a client can run the Sync app Any number {-1, 0, 1, 2, 3, 4, 5, 6} where: • -1 = Everyday • 0 = Sunday • 1 = Monday • and so on...	<activesync_daysofweek>5</activesync_daysofweek>
activesync_timeofday	Specifies the times during the days of the week when a client can run the Sync app Use the format HH:MM:SS-HH:MM:SS	<activesync_timeofday>8:00:00-20:00:00</activesync_timeofday>
allowuserconfigforlimitsync	0 = cannot modify the folder and any *limitfolder* setting is applied 1 = can modify the folder and overrules any *limitfolder* setting This value works in combination with: • *limitfolders*	<allowuserconfigforlimitsync>1</allowuserconfigforlimitsync>

Parameter (XML Tag)	Value	Example
allowuserconfigfornwfolders	Allows user to configure network folders 0 = cannot modify the folder and any *offlinefolder* setting is applied 1 = can modify the folder and overrules any *offlinefolder* setting This value works in combination with: • *offlinefolders*	<allowuserconfigfornwfolders>1</allowuserconfigfornwfolders>
allowuserconfigforbackup	0 = cannot modify the folder and any *offlinefolder* setting is applied 1 = can modify the folder and overrules any *offlinefolder* setting This value works in combination with: • *offlinefolders*	<allowuserconfigforbackup>1</allowuserconfigforbackup>
checkupdates (available in FileCloud 22.1)	0 = Sync does not check for updates on startup 1 = (default) Sync checks for updates on startup, and notifies user if there is an update	<checkupdates>1</checkupdates>

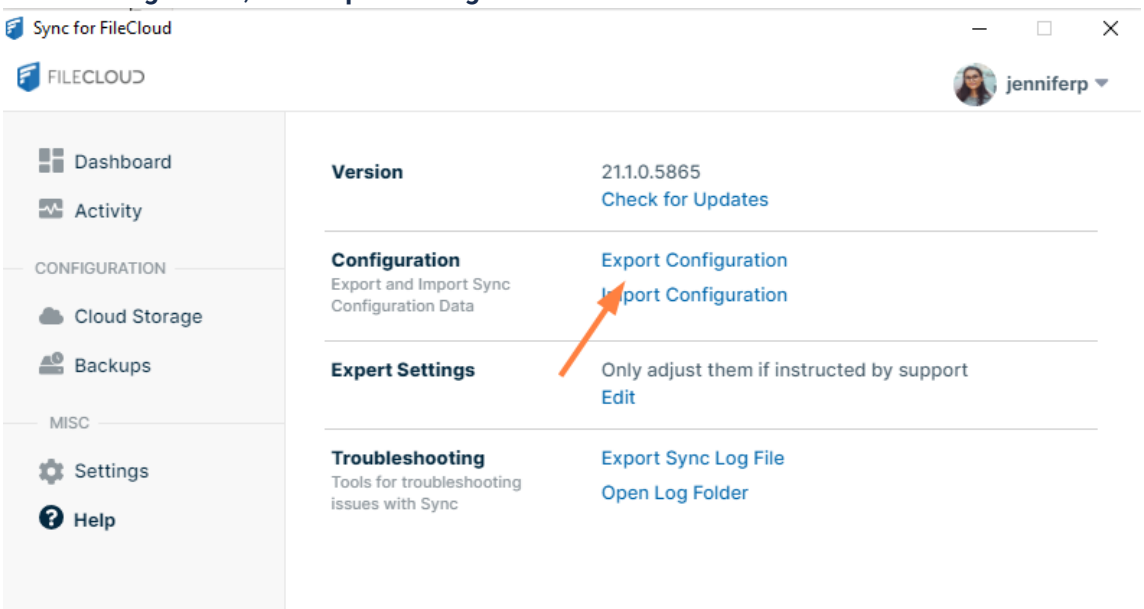
How do I get the configuration XML for Sync?

The easiest way to get the configuration XML for Sync is by installing a copy of Sync and configuring it as needed, and then exporting the configuration.

To export Sync configuration settings:

1. Install and Log In to FileCloud Sync.
2. From the system tray, right-click the FileCloud Sync icon, and choose **Open**.
   The mini-dashboard opens.
3. Click **Dashboard**.
   The main dashboard opens..
4. Click **Help**.
   The **Help** window opens.

5. Under **Configuration**, click **Export Configuration**.



What variables are supported?

When specifying values, variables can be used as well. The following variables are currently supported.

Variable	Notes
${USER}	Replaces with current logged in user name from the Operating System
${HOME}	Replaces with the location of the current user's Home Path
${USERID}	Replaces with the currently logged in FileCloud user account name

What is the XML code for limiting bandwidth rates?

If your users are running the FileCloud Sync app on a slow network, when Sync transfers files it can quickly use up all the network bandwidth.

You can have your users set individual bandwidth rates by following instructions in the Users Guide:

➡

Set Bandwidth Rate Limits for Sync

Or you can use centralized device management to limit bandwidth rates for all clients.

⚠️ If Centralized Device Configuration is set, the user will not be allowed to change the settings from the User Portal. The user will see the following message:

Centralized Configuration is being applied. Bandwidth Settings cannot be changed. Please contact your administrator for assistance.

The XML code will include the following lines:

```
<cloudsync>
      <globalbwforupload></globalbwforupload>
   <globalbwfordownload></globalbwfordownload>
   <altbwforupload></altbwforupload>
   <altbwfordownload></altbwfordownload>
   <altbwfromtime></altbwfromtime>
   <altbwtotime></altbwtotime>
   <altbwschedule_dayofweek></altbwschedule_dayofweek>
 </cloudsync>
```

XML Tag	Value	Example
globalbwforupload	Specifies the bandwidth limit when uploading files from the client to the server in terms of KB only. This limit can be different from the download limit.	<globalbwforupload>100</globalbwforupload>
globalbwfordownload	Specifies the bandwidth limit when downloading files from the server to the client in terms of KB only. This limit can be different from the upload limit.	<globalbwfordownload>50</globalbwfordownload>
altbwforupload	Specifies that alternative settings should be used instead of the global bandwidth limit when uploading files from the client to the server in terms of KB only.	<altbwforupload></altbwforupload>
altbwfordownload	Specifies that alternative settings should be used instead of the global bandwidth limit when downloading files from the server to the client in terms of KB only.	<altbwfordownload></altbwfordownload>
altbwfromtime	Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit. Time must be expressed in the format HH:MM:SS	<altbwfromtime>16:45:00</altbwfromtime>
altbwtotime	Specifies the ending time when the alternative settings should be used instead of the global bandwidth limit. Time must be expressed in the format HH:MM:SS	<altbwtotime>24:00:00</altbwtotime>

XML Tag	Value	Example
altbwschedule_dayofweek	Specifies the days of the week when the alternative settings should be used instead of the global bandwidth limit. This value can be any number such as: {-1, 0, 1, 2, 3, 4, 5, 6} where: • -1 means every day • 0 means Sunday • 1 means Monday • and so on..	<altbwschedule_dayofweek>3</altbwschedule_dayofweek>

If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set.
A "Missing RMC params" message will be displayed in the log file.

What is the XML code for Active Sync Hours?

As an administrator, you can enable or disable a client's ability to set a schedule for when the Sync app runs.
Users set their schedule from the Sync dashboard. See Limit Sync To a Schedule.

⚠️ If Active Sync Hours is disabled, Sync will be active and function normally unless the user clicks the Pause button to stop it.

Use the following XML code to allow or disable the Active Sync Hours checkbox and settings.

```
<cloudsync>
  <timeactivecontrolsset></timeactivecontrolsset>
  <activesync_daysofweek></activesync_daysofweek>
  <activesync_timeofday></activesync_timeofday>
</cloudsync>
```

XML Tag	Value	Example
timeactivecontrolsset	1 = enabled 0 = disabled	<timeactivecontrolsset>1</timeactivecontrolsset>

XML Tag	Value	Example
activesync_daysofweek	Any number {-1, 0, 1, 2, 3, 4, 5, 6} -1 = Everyday 0 = Sunday 1 = Monday ...etc.	<activesync_daysofweek>5</activesync_daysofweek>
activesync_timeofday	Use the format HH:MM:SS-HH:MM:SS	<activesync_timeofday>8:00:00-20:00:00</activesync_timeofday>

What XML settings allows users to modify folders?

When device configuration xml is included for Sync, whether or not the settings included affect selective Sync folder, network folder, or backup folders, by default, users are prevented from configuring these folder types in the Sync application.

As an administrator, you can override this, and allow Sync users to modify the following folders:

- Selective Sync folders
- Network folders
- Backup folders

The XML Settings for enabling or disabling the ability to modify these folders are:

XML Tag	Value	Example
allowuserconfigforlimitsync	0 = user cannot modify Selective Sync folders and any *limitfolder* setting, if present in xml, is applied. 1 = user can modify Selective Sync folders and this overrules any *limitfolder* settings.	<allowuserconfigforlimitsync>1<allowuserconfigforlimitsync>
allowuserconfigfornwfolders	0 = user cannot modify Network folders and any *offlinefolder* setting configured for Network folders, if present, is applied. 1 = user can modify Network folders and this overrules any *offlinefolder* setting configured for Network folders.	<allowuserconfigfornwfolders>1<allowuserconfigfornwfolders>
allowuserconfigforbackup	0 = user cannot modify the Backup folder and any *offlinefolder* setting configured for Backup folders, if present, is applied. 1 = user can modify the folder and this overrules any *offlinefolder* setting configured for Backup folders	<allowuserconfigforbackup>1</allowuserconfigforbackup>

Scenarios

If xml device config settings are present, whether or not they apply to selective sync or offline folders, they must be overridden to allow users to modify folder settings in the Sync client app.

Controlling modifications to selective sync folders

limitfolders	allowuserconfigforlimitsync	Sync User's Access
/john/folder1|/john/folder2	1	Although limit folders are present, because *allowuserconfigforlimitsync* is set to allow modifications: • *limitfolder* settings will NOT be applied • Users CAN modify their selective sync folders
/john/folder1|/john/folder2	0	Because limit folders are present, AND *allowuserconfigforlimitsync* is set to disable modifications: • *limitfolder* settings will BE applied • Users CANNOT modify their selective sync folders
None set but other settings are present	1	Because *allowuserconfigforlimitsync* is set to allow modifications: • Users CAN modify their selective sync folders, irrespective of any other settings in the config
None set but other settings are present	0	Because *allowuserconfigforlimitsync* is set to disable modifications: • Users CANNOT modify their selective sync folders

Controlling modifications to selective network folders

offline folders	allowuserconfigfornwfolders	Sync User's Access
/EXTERNAL/folderA	1	Because offline folders (configured as Network Folders) are present, AND *allowuserconfigfornwfolders* is set to enable modifications: • *offlinefolder* setting configured for Network Folders, will NOT be applied • Sync users CAN modify Network Folders
/EXTERNAL/folderA	0	Because offline folders (configured as Network Folders) are present AND *allowuserconfigfornwfolders* is set to disable modifications: • *offlinefolder* setting configured for Network folders, will BE applied • Sync users CANNOT modify Network Folders

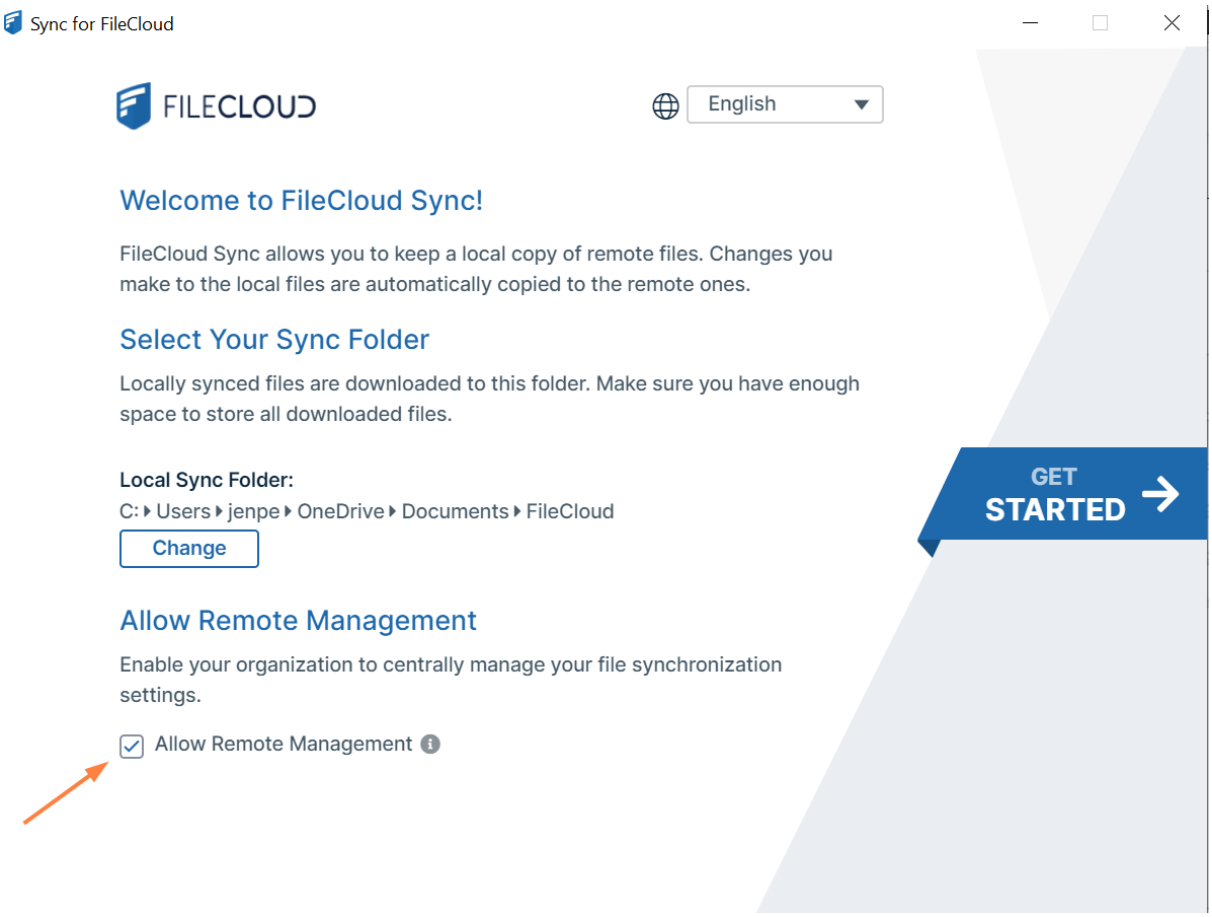
None set but other settings are present	1	Because *allowuserconfigfornwfolders* is set to enable modifications: • Sync users CAN modify Network Folders, irrespective of any other settings in the config.
None set but other settings are present	0	Because *allowuserconfigfornwfolders*is set to disable modifications: • Sync users CANNOT modify Network Folders

Controlling modifications to selective backup folders

offline folders	allowuserconfigforbackup	Sync User's Access
C:\data\local	1	Because offline folders (configured for backup) are present, AND *allowuserconfigforbackup* is set to enable modifications: • *offlinefolder* setting configured for Backup folders, will NOT be applied • Sync users CAN modify backup folders
C:\data\local	0	Because offline folders (configured for backup) are present AND *allowuserconfigforbackup* is set to disable modifications: • *offlinefolder* setting configured for Backup folders, will BE applied • Sync users CANNOT modify backup folders
None set but other settings are present	1	Because *allowuserconfigforbackup* is set to enable modifications: • Sync users CAN modify backup folders, irrespective of any other settings in the config.
None set but other settings are present	0	Because *allowuserconfigforbackup* is set to disable modifications: • Sync users CANNOT modify backup folders

How do I prevent users from overriding remote management?

In the Sync client, by default, there is a setting on the initial window of the log-in wizard: Allow Remote Management.



This setting is also available in the Settings window.

- It allows Sync users to manage their Sync application by overriding an Administrator's settings
- In some cases, administrators want to disable the toggle by hiding it.
- In FileCloud Server version 19.1 and later, an administrator can hide the setting by adding a registry key called *allowcentralmgmtusermodify*
- When set to 0, the central management option is disabled and can no longer be changed by users

To add the registry key:

1. Add a registry key under:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg
```

2. Name the registry key:

```
allowcentralmgmtusermodify
```

3. Restart the computer.

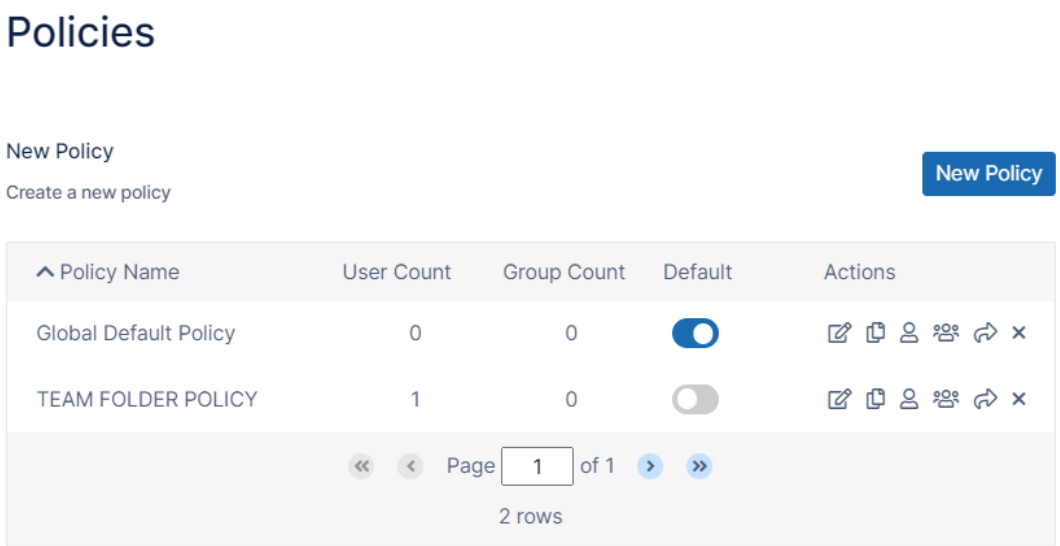
Device Configuration XML For Windows Drive

Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

> For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set a FileCloud Drive device configuration in a policy:

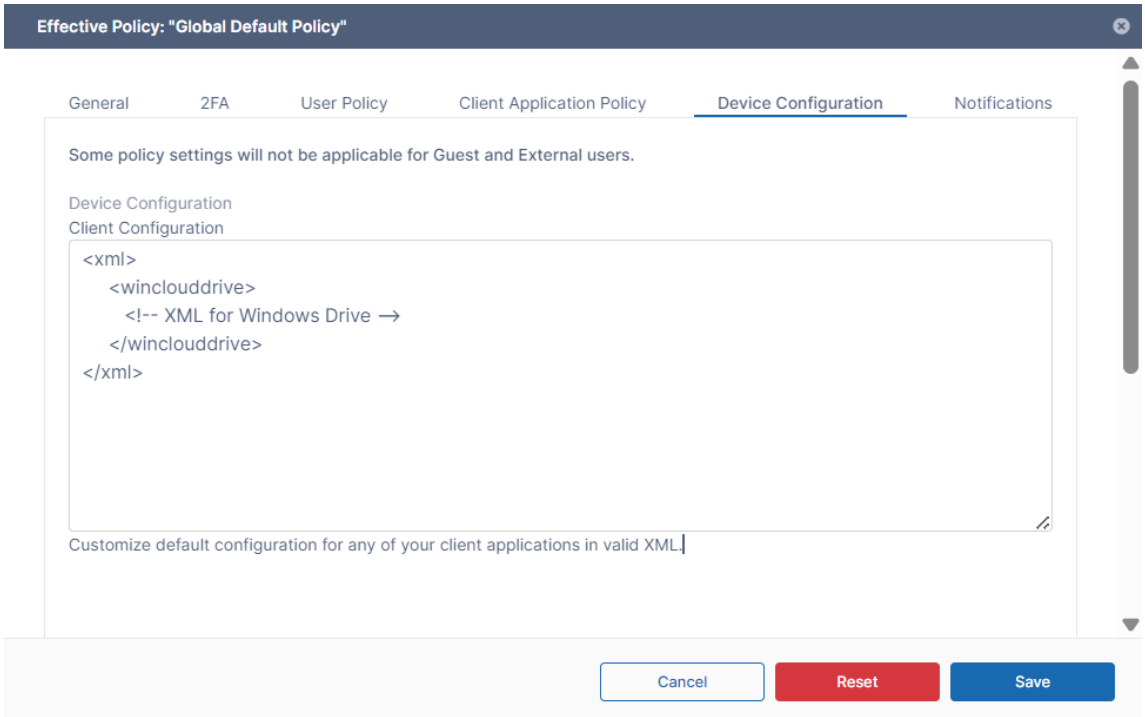
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for Windows Drive -->** with any parameters from the table below.

```
<xml>
```

```
    <winclouddrive>
       <!-- XML for Windows Drive -->
    </winclouddrive>
</xml>
```



Supported parameters for FileCloud Drive. All parameters are optional. Add one of more of these parameters (as XML tags) in the <winclouddrive> tags in the XML.

Parameter (XML Tag)	Value	Example
maxdownloadsizeinmb	Assigns the maximum single file download limit to the supplied value. The download limit does not apply to the following file types: .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .indd.	<maxdownloadsizeinmb>100</maxdownloadsizeinmb>
mountpoint	Set the mount point to use to mount filecloud drive in windows. This will only take effect on drive restart	<mountpoint>H:</mountpoint>

Parameter (XML Tag)	Value	Example
drivelogin mode	Setting this to "0" will cause filecloud drive to use username/password to log into the Filecloud server. Setting this value to "1" will cause drive to use device code authentication mode	<driveloginmode>1</driveloginmode>
drivelockonupdate	Setting this value to 1 will enable automatic lock on edit function in FileCloud Drive. Setting this to 0 will disable the drive's lock on edit function	<drivelockonupdate>1</drivelockonupdate>
drivemutemessages	Setting this value to 1 will disable system tray notifications being shown to the user.	<drivemutemessages>1</drivemutemessages>
driveopenexploreronstartup	Setting this value to 1 will automatically open explorer window when drive starts up and 0 will disable it.	<driveopenexploreronstartup>1</driveopenexploreronstartup>
drivedefaultstoragingb	Increases the storage space of the FileCloud Drive user. Default = 15. The configuration becomes effective after FileCloud Drive is restarted. **Note**: The FileCloud user must have unlimited storage (User Storage Quota is set to 0 in user policy) for the value to be applied.	<drivedefaultstoragingb>15</drivedefaultstoragingb>
checkupdates	Setting this value to 1 will enable automatic checking for new versions of FileCloudDrive and setting this value to 0 will disable it.	<checkupdates>1</checkupdates>
cachelocation	The default cache path is %APPDATA%/FileCloudDrive/ . This path can be changed to a different location using this key. Any path set must be a valid path on the computer where FileCloudDrive runs.	<cachelocation>E:\DriveCache<cachelocation> or <cachelocation>${HOME}\DriveCache<cachelocation> or <cachelocation>C:\somepath\${USERID}\DriveCache</cachelocation>

Parameter (XML Tag)	Value	Example
disableprecaching	Setting this value to 1 disables precaching. If many Drive users have access to a large data structure, the FileCloud server may experience a high load. This can be avoided by deactivating precaching. However, folder contents will no longer be cached in Drive which can lead to longer response times.	<disableprecaching>1</disableprecaching>
disableautologin	By default, once a drive is mounted, the authentication will be reused on every FileCloudDrive start ups. Setting this key to 1 will require authentication from user on every start up.	<disableautologin>1</disableautologin>
currentlanguage	By default English will be the default language. This key can be used to set the default language for FileCloudDrive. The current values that are supported are english, dutch, french	<currentlanguage>french</currentlanguage>

Variable	Notes
${USER}	Replaced with current logged in user name from the Operating System
${HOME}	Replaced with the location of the current user's Home Path
${USERID}	Replaced with the currently logged in FileCloud user account name

Device Configuration XML for Desktop Edit

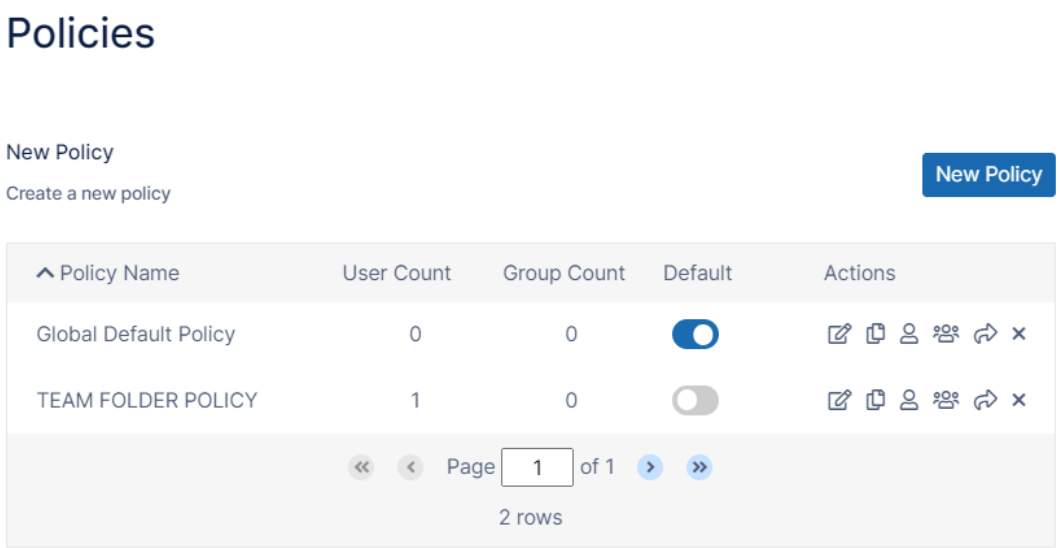
Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set FileCloud Desktop Edit device configuration in a policy:

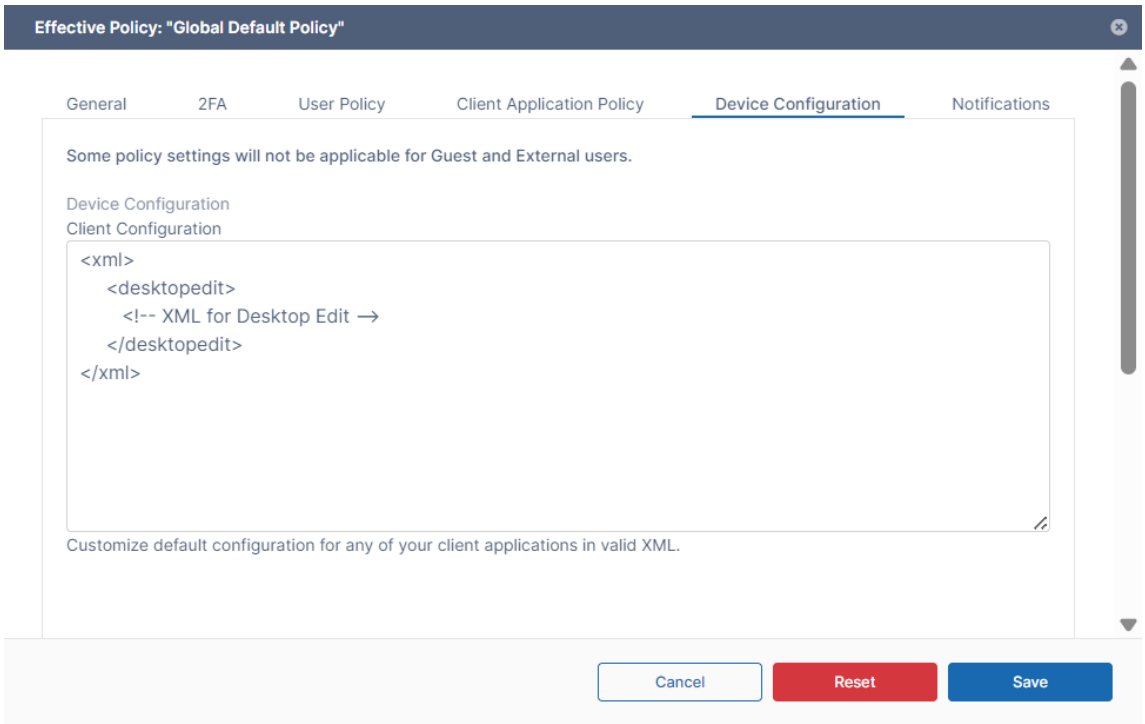
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the following remote device configuration XML in **Device Configuration** replacing **<!-- XML for Desktop Edit -->** with any parameters from the table below

```
<xml>
     <desktopedit>
        <!-- XML for Desktop Edit -->
     </desktopedit>
</xml>
```



Supported parameters for FileCloud Desktop Edit. All parameters are optional. Add one of more of these parameters (as XML tags) in the <desktopedit> tags in the XML.

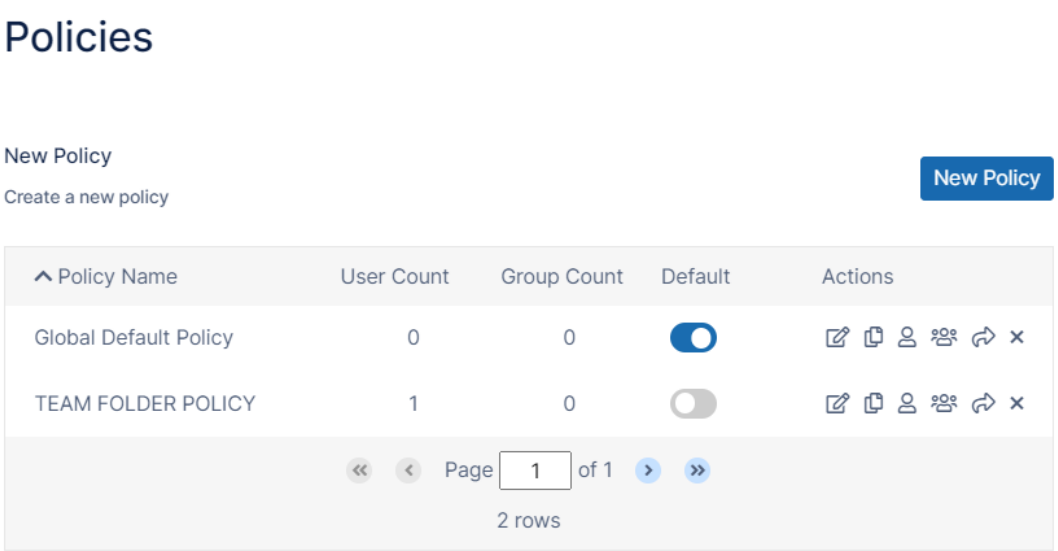
Parameter (XML Tag)	Value	Example
lockfiles	0/1 - Enable or Disable autolocking of files	<lockfiles>1</lockfiles>
runatstartup	0/1 - Enable or Disable running application at OS startup	<runatstartup>1</runatstartup>
mutenotifications	0/1 - Enable or Disable notifications	<mutenotifications>1</mutenotifications>

Device Configuration XML for FileCloud Desktop for macOS

You can configure client device settings for FileCloud Desktop for macOS remotely by specifying the configuration XML in the **Device Configuration** tab of FileCloud policies.

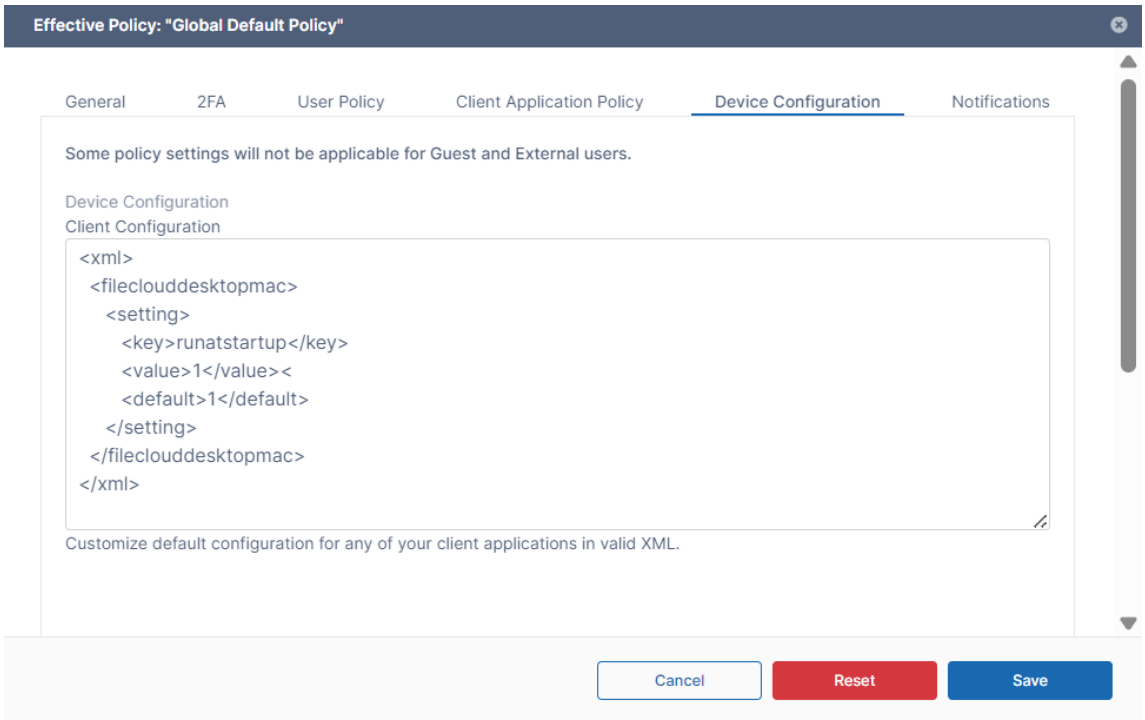
For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the remote device configuration XML in **Device Configuration** using any number of parameters from the table below.

```
<xml>
  <fileclouddesktopmac>
     <setting>
        <key>runatstartup</key>
        <value>1</value><
        <default>1</default>
     </setting>
  </fileclouddesktopmac>
</xml>
```



<default> is an optional tag that indicates if the setting can be changed through the user interface.
A value of 1 indicates the setting is a default and can be changed by the user through the user interface.
A value of 0 (or omission of <default>) indicates that the setting is overridden and cannot be changed by the user through the user interface.

Supported parameters for FileCloud Desktop for macOS. All parameters are optional. Add one of more of these parameters (using <key>, <value>, and <default> tags) in the <setting> tags in the XML.

Parameter (Key)	Description	Values
lockonopen	Automatically lock files when they are opened.	0 (disabled) 1 (enabled) default
runatstartup	Run FileCloud Desktop for macOS on system startup.	0 (disabled) 1 (enabled) default
loglevel	Level of details stored in log files, where **information** is the least detailed, and **trace** is the most detailed.	"information" default "debug" "trace"

<table>
<tr><th>Parameter (Key)</th><th>Description</th><th>Values</th></tr>
<tr><td>language</td><td>Language of the FileCloud Desktop for macOS user interface.</td><td>
<table>
<tr><th>Value</th><th>Language</th></tr>
<tr><td>nl</td><td>Dutch</td></tr>
<tr><td>en (default)</td><td>English</td></tr>
<tr><td>de</td><td>German</td></tr>
<tr><td>es</td><td>Spanish</td></tr>
<tr><td>pt</td><td>Portuguese</td></tr>
<tr><td>fr</td><td>French</td></tr>
<tr><td>ar</td><td>Arabic</td></tr>
<tr><td>it</td><td>Italian</td></tr>
<tr><td>ru</td><td>Russian</td></tr>
</table>
</td></tr>
<tr><td>mutenotifications</td><td>Suppress all notifications on FileCloud Desktop.</td><td>0 (disabled, notifications are shown) default
1 (enabled, notifications are not shown)</td></tr>
</table>

Example:

The code below shows example settings:

```
<xml>
<filecloudesktopmac>
  <setting>
    <key>lockonopen</key>
    <value>1</value>
  </setting>
  <setting>
    <key>runatstartup</key>
    <value>1</value>
```

```
    <default>1</default>
  </setting>
  <setting>
    <key>loglevel</key>
    <value>debug</value>
  </setting>
  <setting>
    <key>language</key>
    <value>en</value>
  </setting>
  <setting>
    <key>mutenotifications</key>
    <value>0</value>
  </setting>
 </fileclouddesktopmac>
</xml>
```

In this example:

- Files are automatically locked when they are opened by FileCloud Desktop (lockonopen = 1). Default value.
- The application runs at startup (runatstartup = 1, default = 1). Default value.
- The log level is set to "debug" (loglevel = debug). Overridden value.
- The language is set to "en" (language = en). Default value.
- Notifications are not muted (mutenotifications = 0). Default value.

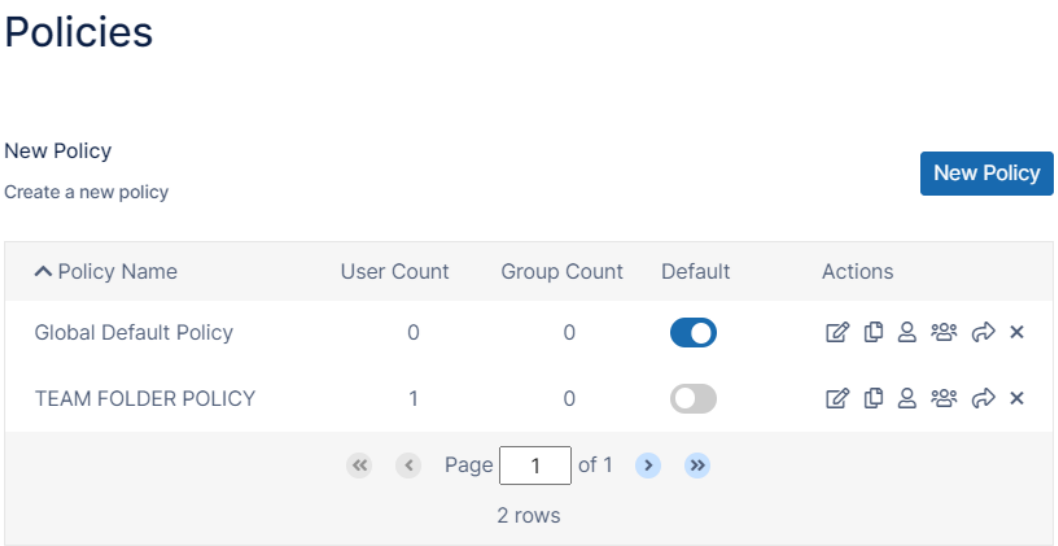
If a key is not supported or a value is incorrect, the application skips it and logs a warning message.

Device Configuration XML for FileCloud Desktop for Windows

You can configure client device settings for FileCloud Desktop for Windows remotely by specifying the configuration XML in the **Device Configuration** tab of FileCloud policies.

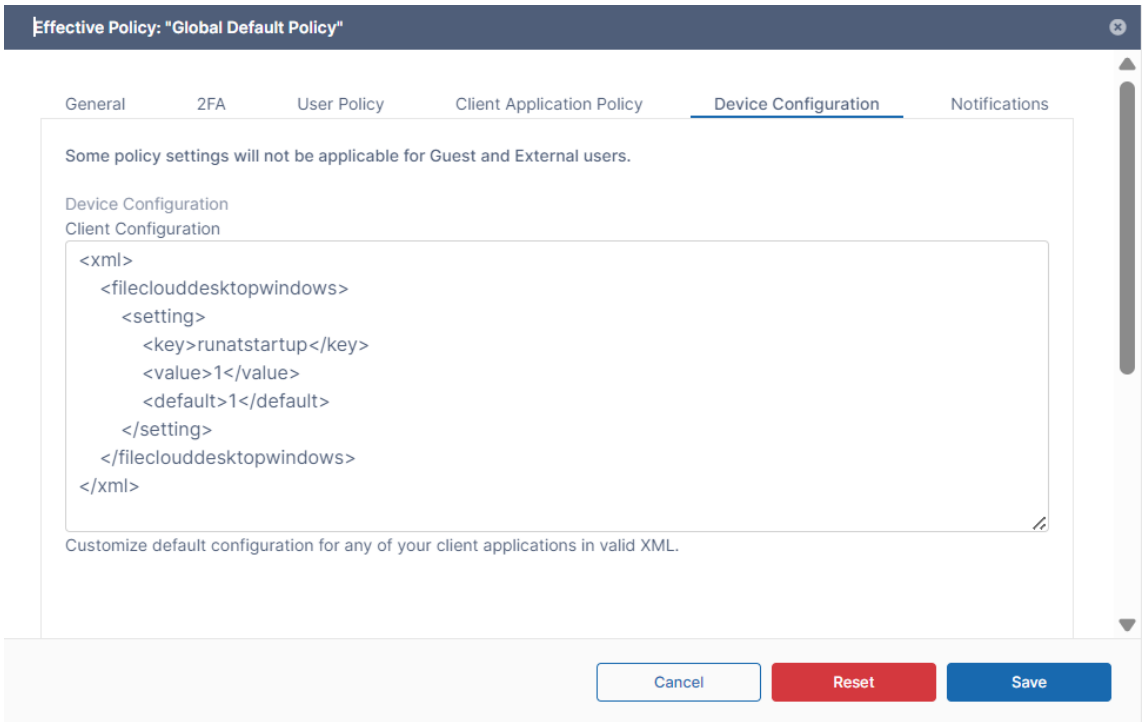
For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.



2. Edit the policy of the users whose client device settings you want to modify.
3. Click the **Device Configuration** tab.
4. Paste or type in the remote device configuration XML in **Device Configuration** using any number of parameters from the table below.

```
<xml>
    <fileclouddesktopwindows>
        <setting>
            <key>runatstartup</key>
            <value>1</value>
            <default>1</default>
        </setting>
    </fileclouddesktopwindows>
</xml>
```



<default> is an optional tag that indicates if the setting can be changed through the user interface.
A value of 1 indicates the setting is a default and can be changed by the user through the user interface.
A value of 0 (or omission of <default>) indicates that the setting is overridden and cannot be changed by the user through the user interface.

Supported parameters for FileCloud Desktop for Windows. All parameters are optional. Add one of more of these parameters (using <key>, <value>, and <default> tags) in the <setting> tags in the XML.

Key	Description	Values
runatstartup	Run FileCloud Desktop for Windows on system startup.	0 (disabled) 1 (enabled) default
loglevel	Level of details stored in log files, where **information** is the least detailed, and **trace** is the most detailed.	"information" default "debug" "trace"

<table>
<tr><td>language</td><td>Language of the FileCloud Desktop for Windows user interface.</td><td><table><tr><th>Value</th><th>Language</th></tr><tr><td>nl</td><td>Dutch</td></tr><tr><td>en (default)</td><td>English</td></tr><tr><td>de</td><td>German</td></tr><tr><td>es</td><td>Spanish</td></tr><tr><td>pt</td><td>Portuguese</td></tr><tr><td>fr</td><td>French</td></tr><tr><td>ar</td><td>Arabic</td></tr><tr><td>it</td><td>Italian</td></tr><tr><td>ru</td><td>Russian</td></tr></table></td></tr>
<tr><td>mutenotifications</td><td>Suppress all notifications on FileCloud Desktop.</td><td>0 (disabled, notifications are shown) default
1 (enabled, notifications are not shown)</td></tr>
</table>

Example:

The code below shows example settings:

```
<xml>
<filecloudesktopwindows>
  <setting>
    <key>runatstartup</key>
    <value>1</value>
    <default>1</default>
  </setting>
  <setting>
    <key>loglevel</key>
    <value>debug</value>
  </setting>
  <setting>
    <key>language</key>
    <value>en</value>
  </setting>
```

```
  <setting>
    <key>mutenotifications</key>
    <value>0</value>
  </setting>
</fileclouddesktopwindows>
</xml>
```

In this example:

- The application runs at startup (runatstartup = 1, default = 1). Default value.
- The log level is set to "debug" (loglevel = debug). Overridden value.
- The language is set to "en" (language = en). Default value.
- Notifications are not muted (mutenotifications = 0). Default value.

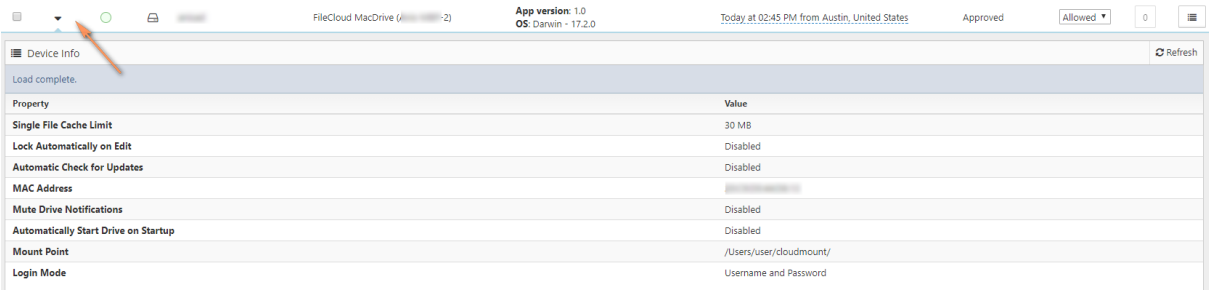
If a key is not supported or a value is incorrect, the application skips it and logs a warning message.

Viewing Client Information

Managing client devices requires the ability to view client information about:

- Health
- State

Figure 1. Device Information



What do you want to view?

Client Health Information

The information shown for each client will depend upon the client type (Sync, Drive, Outlook Add In, iOS, Android, etc.)

To show information related to a device:

1. In the Devices table, click the device.

Client State Information

Each client now has health information represented by the icon in the client table.

	Health color	Information
	Green	Healthy client
	Yellow	Some problems reported by client
	Red	Critical problem reported by client

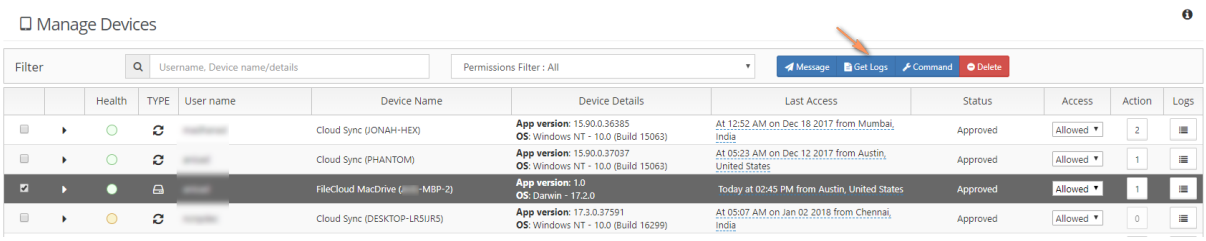
Requesting Client Log Files

Administrators can request clients to upload their latest log files to the server so the administrator can view any errors for troubleshooting.

To get logs, select the device in the list and click on "Get Logs" button.

The logs are uploaded by the client

- When the client connects to the FileCloud server (as a part of login operation)
- If the client is already connected, then it processes the get logs command periodically and uploads the logs to the server.



The get logs request is queued to the client the next time the client is online and processes server commands it will upload the logs to it's logs folder.

Blocking and Remotely Wiping a Client Device

Administrators can selectively block a specific client device from logging into the FileCloud server using FileCloud's RMC function.

In addition to Blocking a Client Device from logging in, Administrator can also wipe FileCloud folders in the remote device.

When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

1. If the client is not connected, the block (and remote wipe) will happen when it tries to log into the server
2. If the client is connected, the block and remote wipe will occur and the client will automatically exit out.

Steps to block (but not wipe remote data) in a client device

1. Log on to Administration Portal
2. Click on "**Devices**" on the left navigation panel
3. Locate the client device to be blocked and under the "**Permissions**" column, Change the value to "**Blocked**"
4. In the "**Confirm**" dialog, select "**NO**" to just block but not remote wipe the client device

Steps to block and wipe remote data in a client device

1. Log on to Administration Portal
2. Click on "**Devices**" on the left navigation panel
3. Locate the client device to be blocked and under the "**Permissions**" column, Change the value to "**Blocked**"
4. In the "**Confirm**" dialog, Check the "Remote Wipe" button to block and remote wipe downloaded data in the client device

The remote wipe will have the following effect on each of the clients

- FileCloud Drive: Cache folder data will be deleted and application will log out
- FileCloud Sync: Synced data will be deleted and application will log out
- iOS and Android: Downloaded data in "This Device" will be deleted and will log out of the server

Sending a Message to a Client's Display

Administrators can display a short message on the remote client using the "Add message" feature.

The entered message(s) will be displayed when the remote client is connected to the FileCloud instance. If more than one message is queued to a device, they will be

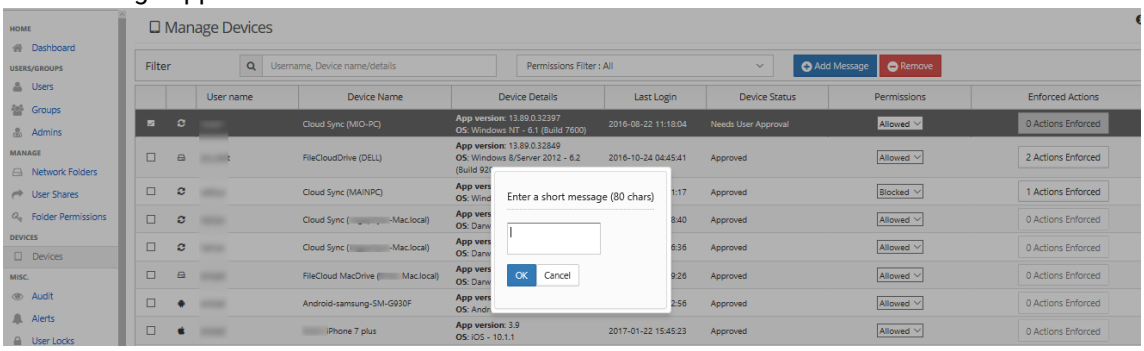
displayed in the order it was entered. The messages will be shown only once per client and during

Message will be shown

- When the client connects to the FileCloud server (as a part of login operation)
- If the client is already connected, then it will retrieve the message periodically and display it to the user

Steps to add message

1. Log on Administration Panel
2. Select one or more devices using the checkbox on the left most column of a device record
3. Click the "**Add Message**" button.
   The message appears on the remote client.



iOS Device Management

Administrators can configure how mobile users with an iOS device interact with FileCloud.

Configuring Automatic Camera Uploads

iOS users can automatically upload photos and videos from their mobile device without manually having to upload.

⚠️ As an administrator, you must first enable this feature before users can configure it on their mobile device.

Why would I enable this feature?

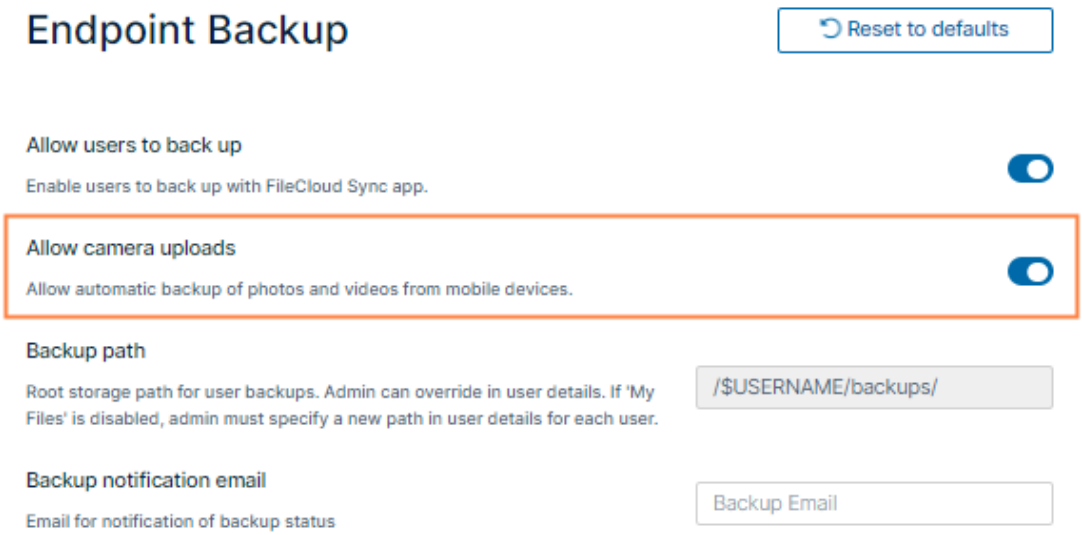
- This is a very convenient feature and it mobile users to know that your photos and videos are always saved in a safe location.
- Instead users saving all of their work files on their mobile device, they can save them to the FileCloud.
- Mobile users can spend time constantly managing their images/videos to free up more space unless they are able to save them to FileCloud.
- If you are concerned about privacy and security, work-related files and photos are stored securely in FileCloud.

💡 Keep in mind that with the amount of photos and videos generated by the mobile devices, the storage size can run out quickly.

To enable automatic camera uploads:

Note: The **Allow Sync Apps** setting in Server Settings must be enabled for **Allow camera uploads** to work. By default **Allow Sync Apps** is enabled.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Endpoint Backup** .
   The **Endpoint Backup** settings page opens.
2. Enable **Allow camera uploads**.



Search in the Admin Portal

FileCloud's Federated Search

In the Admin Portal, FileCloud includes a federated search that looks for matches in file names, folder names, file content, and metadata. It is also capable of searching for complex strings using regular expressions.

> The ability to search the entire FileCloud system for files and folders is available in FileCloud Server version 17.3 and later.
> The PCRE search is available in FileCloud Version 21.1 and higher.

As an administrator, you may need to find a file or folder quickly in a large data set.

- FileCloud supports searching the entire FileCloud system for files and folders with the Federated Search feature.
- The search may be a basic file or folder name search.
- Search results may contain matches from both managed storage and network folders.
- Search results can be downloaded, and if applicable, previewed.
- Search results cannot be copied, moved or deleted.

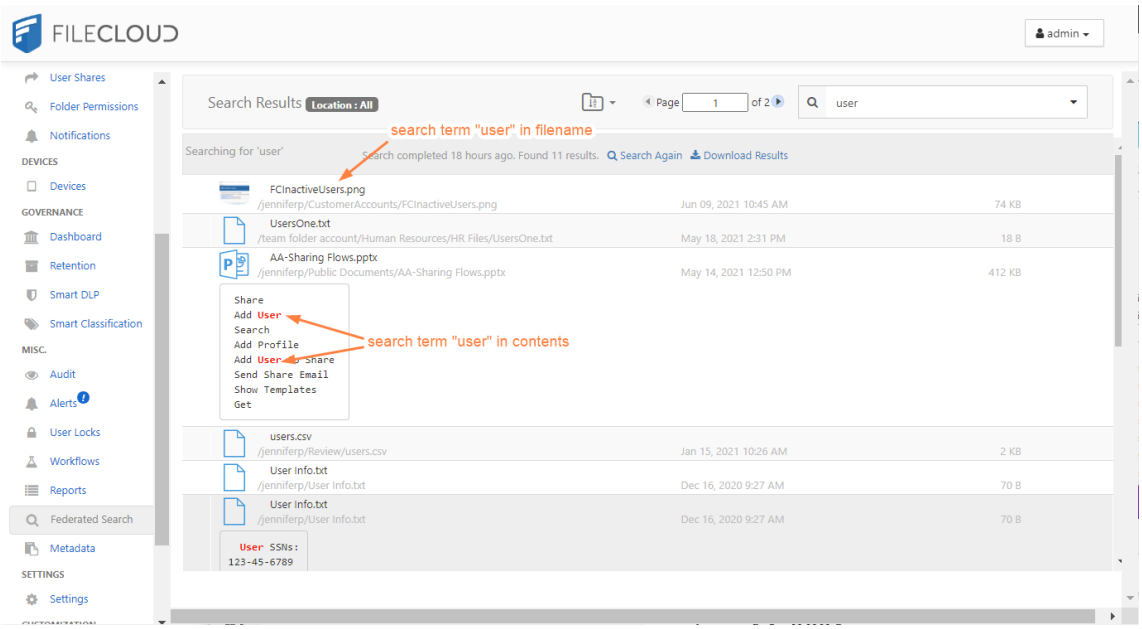
Basic Search

A basic search searches for the search term in file and folder names, and if content search is enabled, in the content of files.

The following procedure assumes that you have enabled full content search for documents.

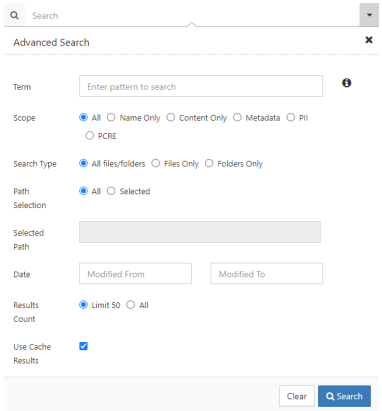
To perform a basic search on the entire site:

1. From the left navigation panel of the Admin Portal, under **Misc.**, click **Federated Search**.
2. On the search screen, in the search box, type the search term and press enter.
   Files and folders with the search term in their names as well as files containing text that contains the search term are listed as search results. Text in files containing the search terms is shown.



Advanced Searches

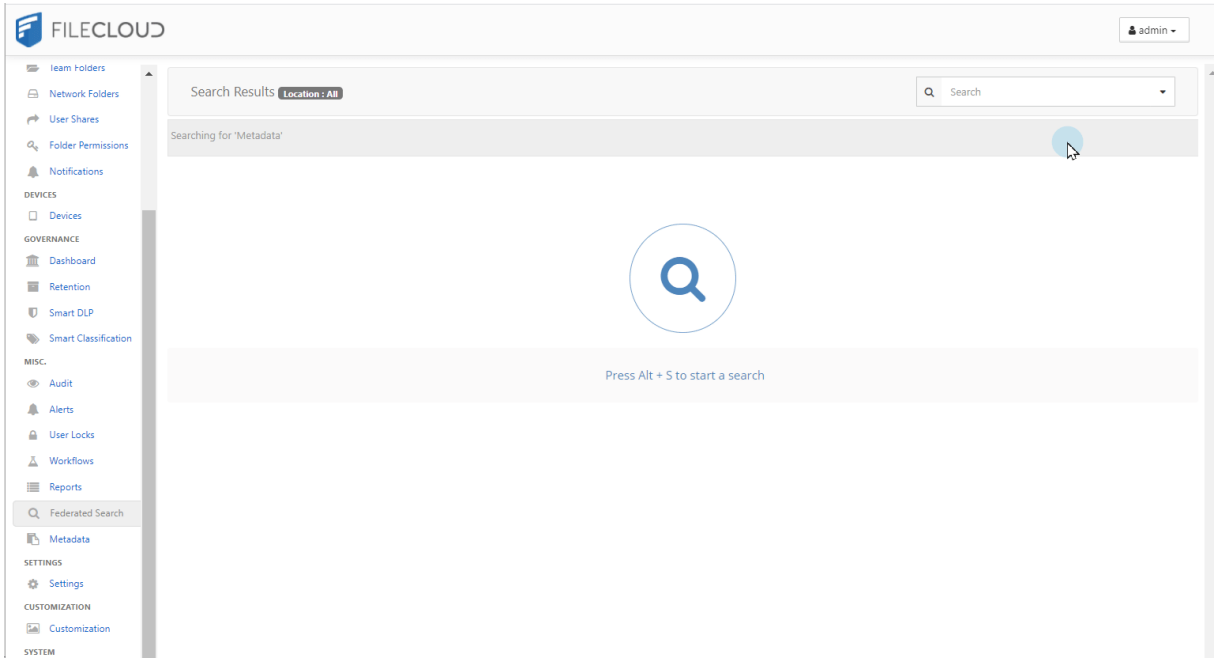
An advanced search lets you search on the search term and any of the options shown and listed below:

Advanced search box	Search options
	**Term** - (required) The string to search for. **Scope** - Which content to search. **All** - File and folder names if content search is not enabled. File and folder names and content in files when content search is enabled. See **All search**, below. **Name Only** - File and folder names only. See **Name only search**, below. **Content Only** - Content in files only. See **Content only search**, below. **Metadata** - Content stored in metadata fields only. You must define conditions to search for instead of entering a search term. See **Metadata search**, below. **PII** - Personally identifiable information in content only. You must select a PII type instead of entering a search term. See **PII and PCRE searches**, below. **PCRE** - Only appears when the **PCRE mode** setting is enabled. Searches on regular expressions. See **PII and PCRE searches**, below. **Search Type** - Options are **All files/folders**, **Files Only**, and **Folders Only**. Not applicable for Metadata search. **Path Selection** - Either **All** or **Selected**. If **Selected** is chosen, **Selected Path** is enabled for you to enter a path. **Selected Path** - When **Selected** is chosen for **Path Selection**, this is enabled. Enter the path to search on. **Date** - Range of Last Modified dates to search on. **Results Count** - Number of results to return. Choose **Limit 50** or **All**. Use **Limit 50** to reduce lengthy search times. **Use Cache Results** - When checked, this returns any saved results of the same search instead of performing the search again. This gives you faster results but does not take into account changes since the previous search.

All search

All search

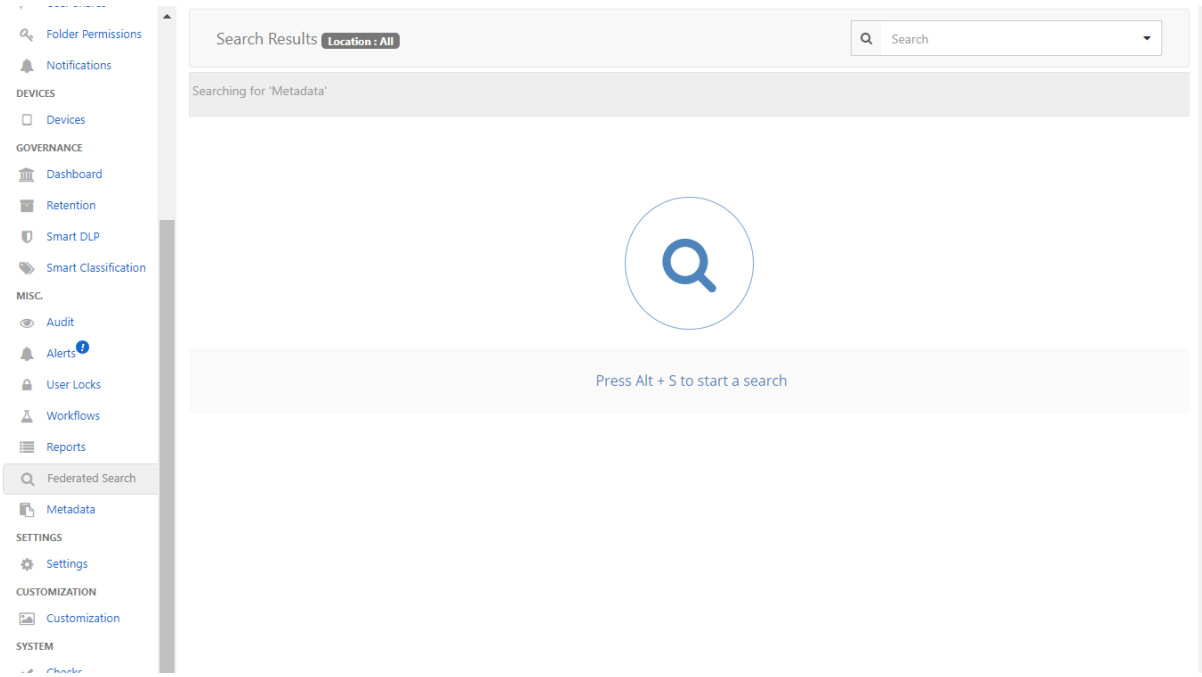
All is selected by default. This search looks for matches in file and folder names when content search is not enabled. It looks for matches in file and folder names and in the content of files when content search is enabled.



Name only search

Name Only search

When **Name Only** is selected, the search only looks for matches in file and/or folder names.



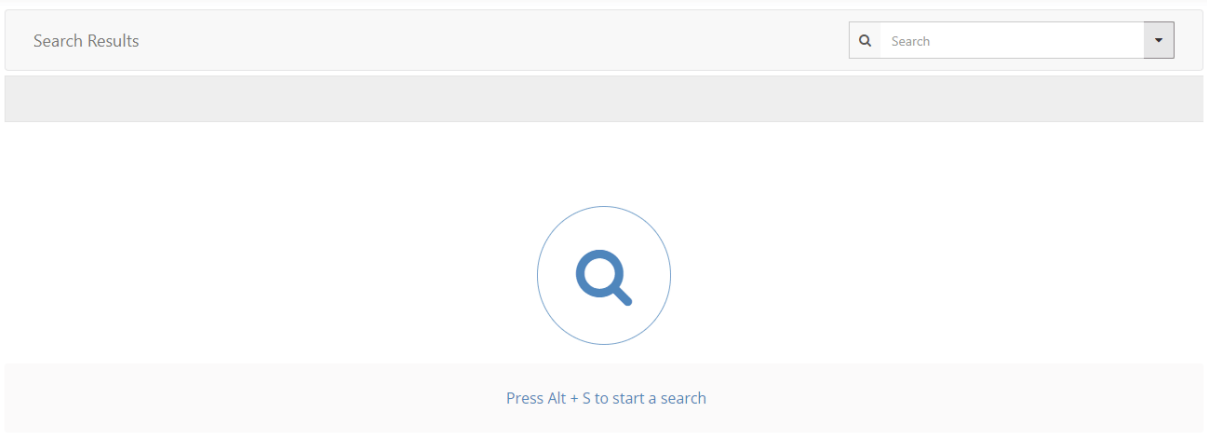
Content only search

Content Only search

When **Content Only** is selected, the search only looks for matches in the text of files.

To perform this search, your system must have full content search capability.

> Content search hits are returned with the matching string highlighted except in the case of lengthy search results, where omitting highlighting achieves quicker response time.

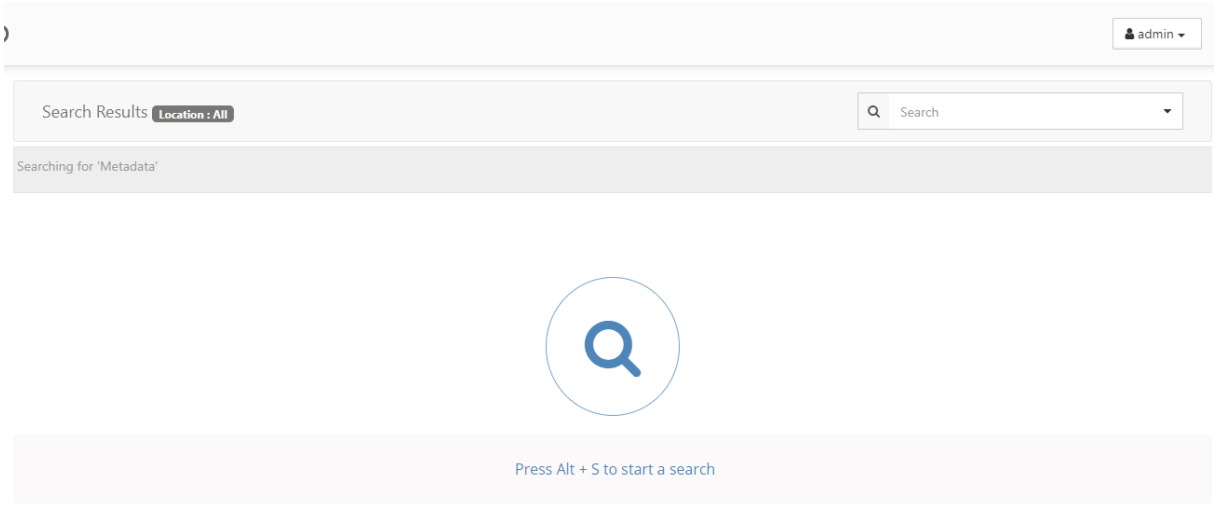


Metadata search

Metadata search

To perform a metadata search, select **Metadata** and define a condition specifying the metadata field value that you are searching for. In the example below, the search is configured to look for content

with the image orientation field set to horizontal.



Audit Logs

FileCloud has extensive auditing support and every operation is logged.

As an administrator, you can use audit logs to quickly see what has changed on your FileCloud site, such as:

- Were any new accounts created recently
- How many clients are logged in
- What are users commonly searching for on the site
- How many files are being uploaded and downloaded

Since every operation is logged, the audit database entries can grow very large very quickly.

To manage log file growth, you can:

- Remove log entries using the Admin dashboard
- Limit what operations are logged
- Export log files to CSV as an archive

Note: You can configure your system to prevent administrators from deleting audit log entries. See Delete Audit Log Entries below.

💡 It is important to keep in mind that removing log entries from the Admin dashboard does removes them from the database. However, MongoDB does not release the space but keeps it for new entries to be added in the future. If you need to reclaim the space, you should compact the database.

What do you want to do?

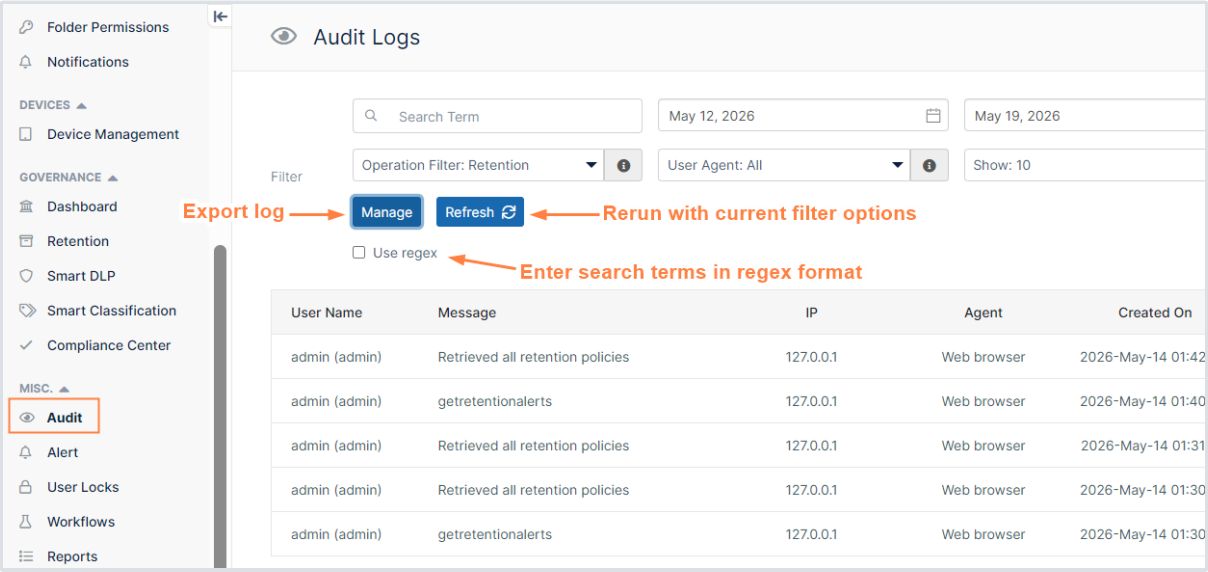
View Logs	View Audit Logs Filter Audit Log Views
Manage Logs	Delete Audit Log Entries Configure What is Logged Export Audit Logs

View Audit Logs

As an administrator, you can read log files as an important part of maintaining proper operation and ensuring system security of your FileCloud site.

- Log files can be extremely useful in troubleshooting issues
- Only an Administrator can read FileCloud log files

To view the audit log, in the navigation panel, click **Audit**.



At the top of the Audit Logs screen are fields that enable you to filter log results. Below them, a **Manage** button opens a dialog box for exporting the log to a csv file and downloading it. A **Refresh** button regenerates the log with the current filter settings. When checked, **Use regex** enables you to enter search terms in regex format.

The main portion of the Audit Log screen lists the audit log entries. Each entry includes the following information:.

User Name	Name of the user account
Message	The descriptive message for the audit record For example, *USER1 logged in FAIL*
IP	The IP address from which the event occurred
Agent	Indicates how FileCloud was accessed. For example: • Web browser • Sync • Drive • Mobile device
Created On	The date and time when the event was logged

Filter Audit Log Views

Since every operation is logged and displayed in the Audit screen, there may be times when you want to filter the events shown.

💡 The audit log can also be sorted, trimmed, or filtered after exporting it to a CSV file. Exporting the audit log can also reduce the size taken up in the database.

> Filtering your view of log entries does not trim or decrease the size of your log database.
> If your log database is growing too large, you can:
> Export Audit Logs
> Configure What is Logged
> Delete Audit Log Entries

How do you want to filter the Audit log?

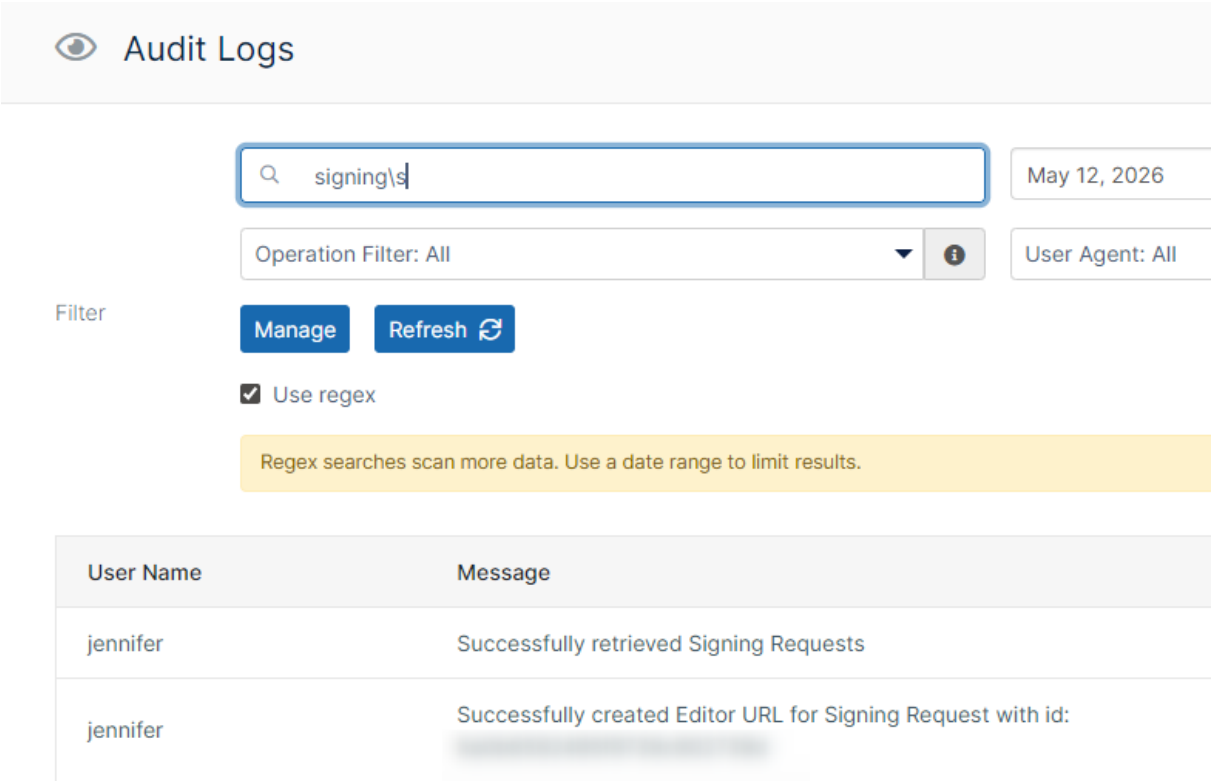
> Searches without a date range entered default to the last 7 days.

By a search term

To filter the audit log by searching:

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Audit**.
3. In the Search box, type in your key words.

By a regular expression search term



To filter the audit log by searching on a regular expression:

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Audit**.
3. Check **Use regex**.
4. Enter a date range.
   Use regex requires a date range because it searches on more data and is resource-intensive. In addition, the regex function does not search on the create date, so to filter by a date or date range, you must enter it in the date fields.
5. In the Search box, enter your regular expression.

By start and end dates

To filter the audit log by date:

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click Audit.
3. In the Filter Start Date box, select a date or type in a date in the following format: YYYY-MM-DD.
4. In the Filter End Date box, select a date or type in a date in the following format: YYYY-MM-DD.

By an operation

The Audit log can be filtered by the following operations or actions that occur on the FileCloud server:

Operation	Description
All	Displays all operations logged by FileCloud Server This is the default filter.
Common	Displays 6 of the most commonly logged operations: • create new account • login • create file or folder • upload file • download file or folder • share file or folder
Deleted	Displays logs created when a file or folder was moved to the recycle bin on the FileCloud Server site
Uploaded	Displays logs created when a file or folder was uploaded to the FileCloud Server site
Downloaded	Displays logs created when a file or folder was downloaded from the FileCloud Server site
Metadata	Displays logs created when a file or folder's metadata was added, edited or removed
Files	Displays logs created when a change is made to all the files on the FileCloud Server site
Retention	Displays logs of retention policy actions.
DLP	Displays logs for failed DLP rules.
Moved	Displays logs created when a file or folder was moved to another location in FileCloud.
Virus removed	Displays logs created when antivirus scanned an upload and removed a virus.
No virus found	Displays logs created when antivirus scanned an upload and found no virus.

Operation	Description
Automation Workflow	Displays logs created when a share approval request created by an automation workflow was approved or rejected. The log message includes the details: share owner, share path, share link, share type, share date, and share approver or rejector.

To filter the audit log by operation:

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Audit**.
3. In **Operation Filter**, select an action or group of actions.

By an agent

An agent is any client or device that connects or communicates with FileCloud Server.

You can select from the following user agents:

- Web browser
- Sync
- Drive
- Outlook
- Office
- iOS
- Android
- Workflow
- Mqworker
- FileCloud Desktop

To filter the audit log by agent:

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Audit**.
3. In **User Agent**, select a client or device.

Configure What is Logged

There might be some operations that that you do not want logged because they fill your audit log with unnecessary information.

To configure what is logged:

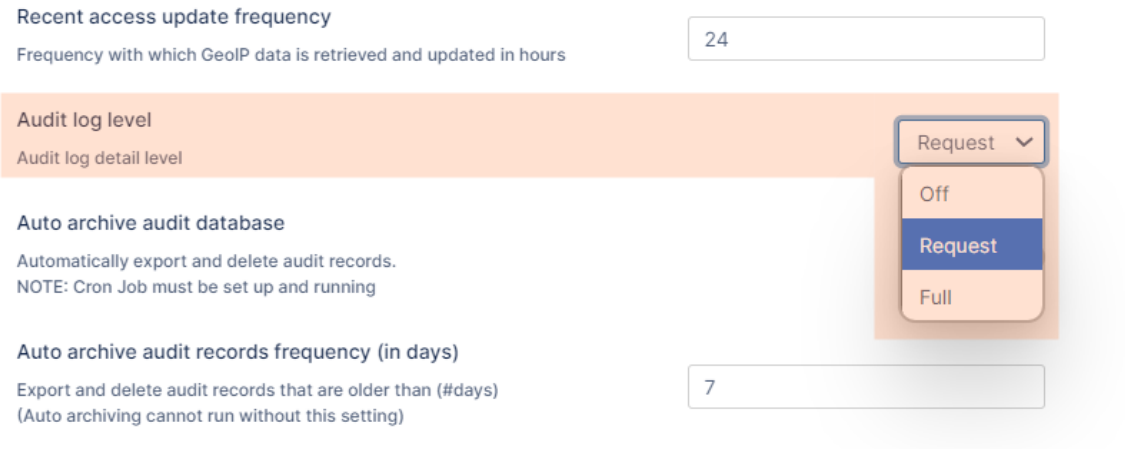
Set a logging level

You can choose to set logging to one of the following levels:

- **Off** - Records nothing in the audit log files
- **Request** - Limits the logging to requests from agents or clients and the results of a request. Does not record the full response to the agent or client.
- **Full** - Records entries for all requests from agents or clients, the full response, and the and the results of the request.

To set a log level:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin** .
   The **Admin** settings page opens.
2. Scroll down and locate **Audit log level**. Set it to **Off**, **Request**, or **Full**.



3. Click **Save**.

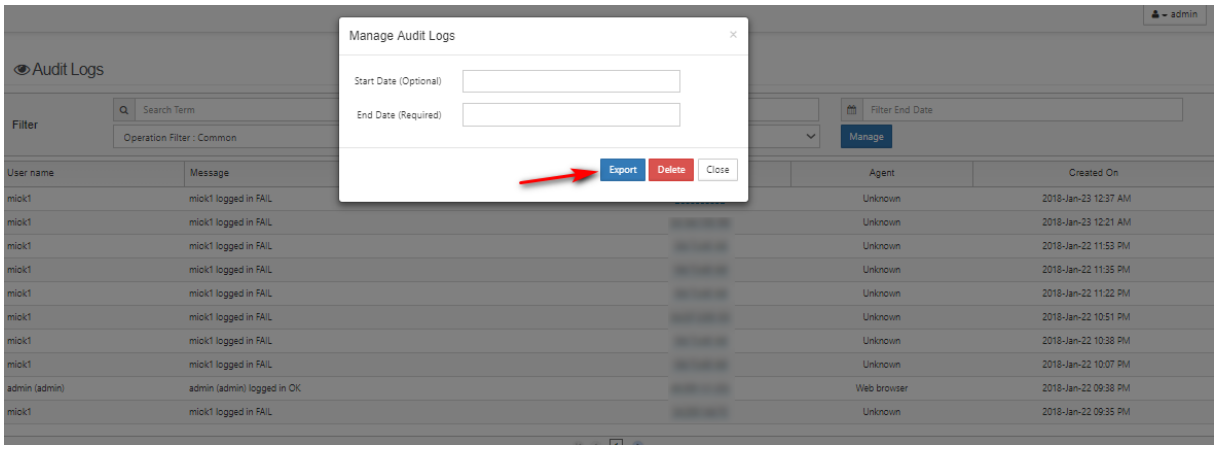
⚠️ Remember that the information in audit logs can be extremely important for troubleshooting. Be careful not to exclude too much information from your log files.

Export Audit Logs

You can export FileCloud Server audit logs as CSV files.

To export the audit logs:

1. Open a browser and log in to the Admin Portal.
2. From the left navigation panel, click **Audit**.
3. To open the Manage Audit Logs window, click **Manage**.
4. In **Start Date** and **End Date**, select dates or type in dates in the format YYYY-MM-DD.
5. Click **Export**.



Delete Audit Log Entries

> **Admin Audit Log Deletion**
> Admins can prohibit other admins from deleting audit logs.

If you need to you can remove entries from the log file manually or contact FileCloud Support to enable automatic archival and removal.

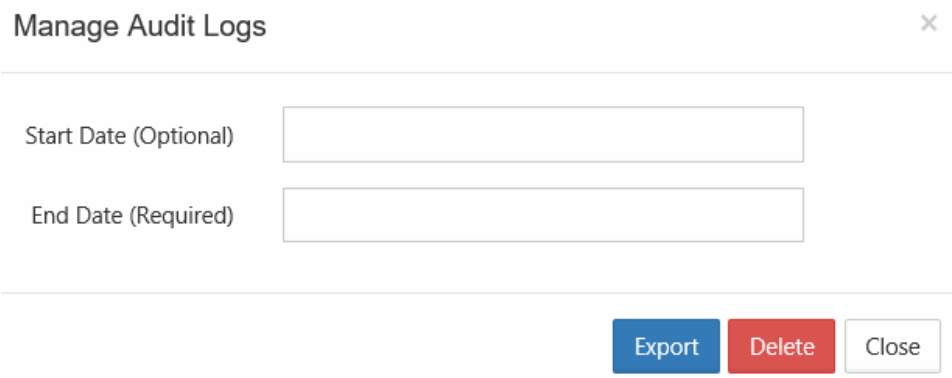
> It is important to keep in mind that removing log entries from the Admin dashboard also removes them from the database. However, the database does not release the space but keeps it for new entries to be added in the future.
> Some reports, such as reports on file actions and failed logins, get their data from the audit log. These reports only include events that are in the audit logs when you run the report. See Custom Reports for information about specific reports

How do you want to remove Audit log entries?

Manually delete entries

To manually remove audit log entries:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Misc > Audit**.
2. On the **Audit Logs** window, click **Manage**.



3. In **Start Date**, select a date or type in a date in the following format: YYYY-MM-DD. If you do not specify a start date, the deletion will occur for the very first log entry until specified End Date.
4. In **End Date**, select a date or type in a date in the following format: YYYY-MM-DD.
5. Click **Delete**.
6. On the **Confirm** dialog box, click **OK**.

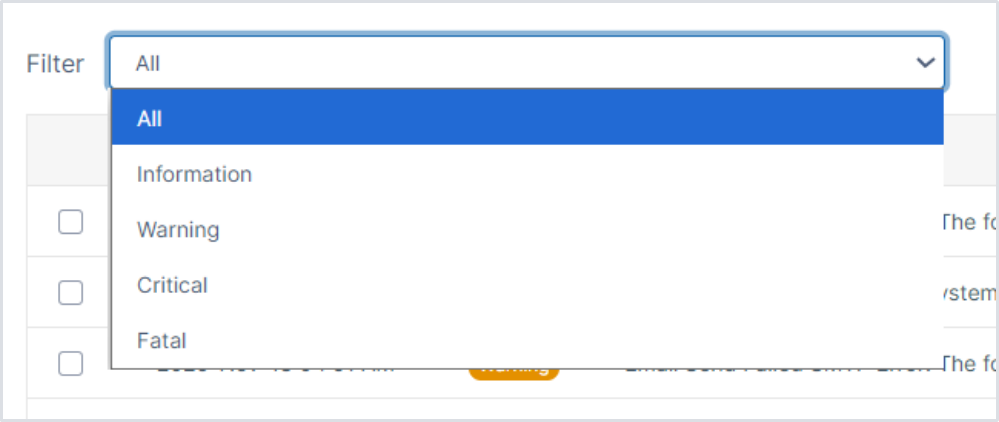
FileCloud Alerts

FileCloud Alerts are available in FileCloud's Admin portal.

This page tracks all unhandled exceptions, system error messages generated in FileCloud. The Alerts page shows information about the various errors encountered.

Depending on the error, you may need to take steps to correct the problem. For example, if alerts indicate that system is frequently running out of memory, then system memory may need to be increased.

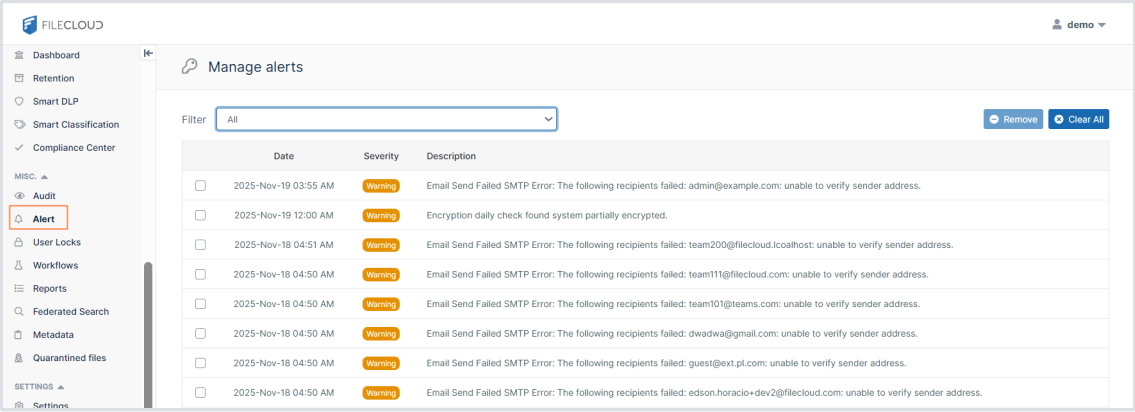
On the Manage alerts page, you can filter by type of alert:



You can also remove individual or all alerts from the screen.

To view alerts:

1. Log into the Administration portal.
2. On the left navigation panel, click **Alerts**.
   The Manage alerts page opens:



File Content Heuristic Engine

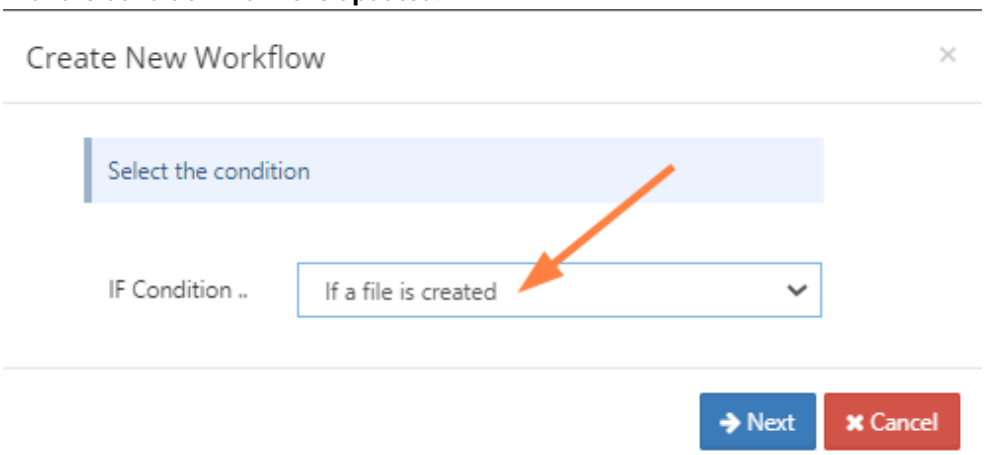
Ransomware is a type of malware that an attacker uses to infiltrate your system and make your files inaccessible, usually by encrypting them. The attacker then demands that you pay a ransom to decrypt your files.

A heuristic engine can help prevent ransomware from entering your system by scanning files for characteristics that are often present in malicious files. FileCloud includes a heuristic engine that looks for files that identify their content inaccurately, a method sometimes used to trick users into opening files containing ransomware. For example, FileCloud's heuristic engine can detect if a file identifies itself as a basic text or image file, but includes code that is not normally present in these types of files.

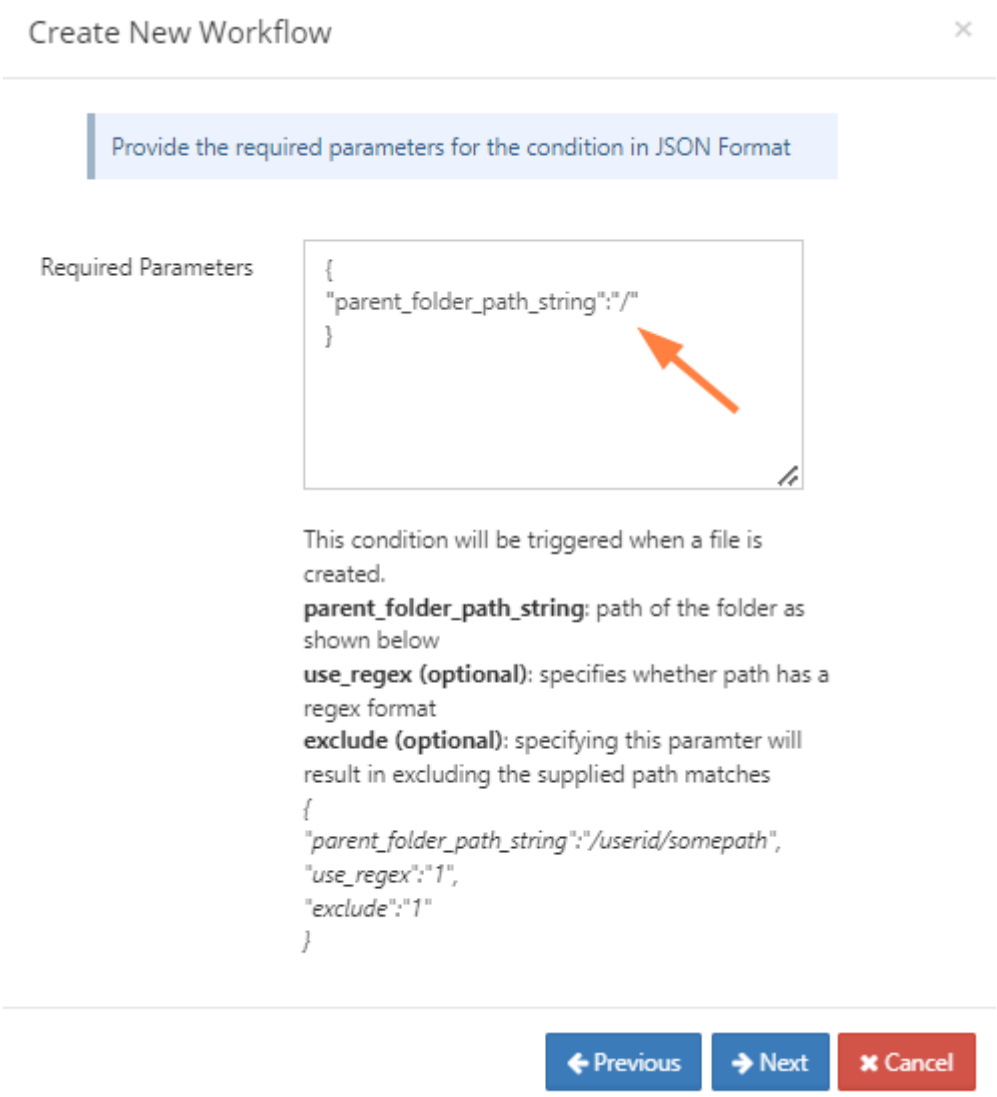
The FileCloud heuristic engine is available to you, but to use it, you must add it to a workflow in your system by choosing a **Verify file integrity** action. When a file fails the integrity check, the workflow can either delete the file or send a notification.

To create a workflow that uses the heuristic engine to validate uploaded files:

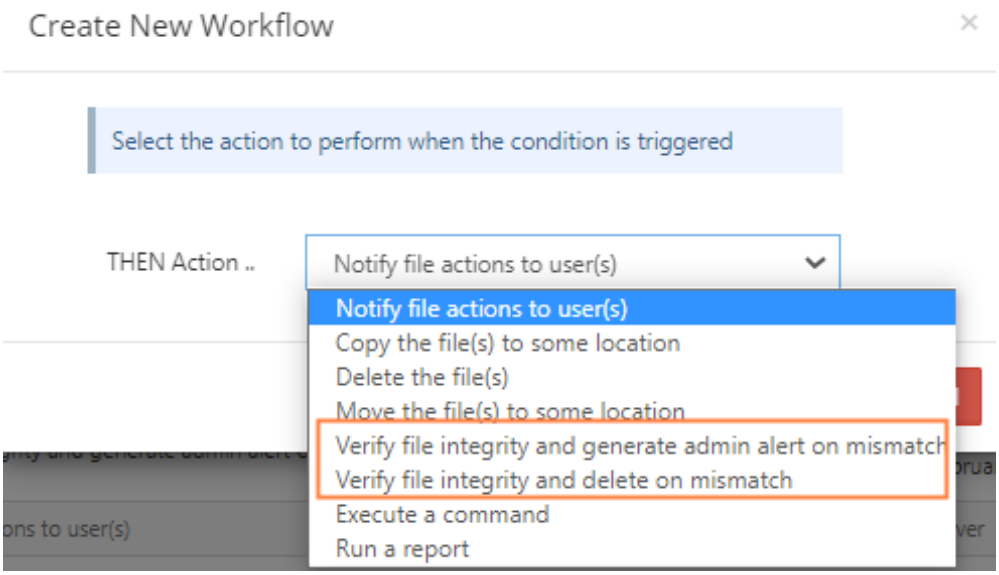
1. In the admin portal, in the navigation panel, click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
   The **Create New Workflow** dialog box opens.
3. To perform the check on every file that is uploaded for the first time, in the **IF Condition** drop-down list, choose **If a file is created**.
   Note: To also apply the condition to files that are re-uploaded, add a verify file integrity action with the condition **If a file is updated**.



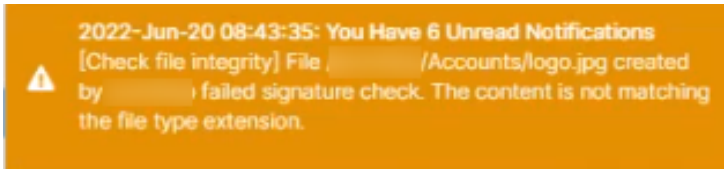
4. Click **Next**.
   The next window prompts you to enter parameters for the workflow.
5. Since you want to scan all uploaded files, set **parent_folder_path_string** to **/**, which indicates all files. The other parameters are optional, and you can exclude them.



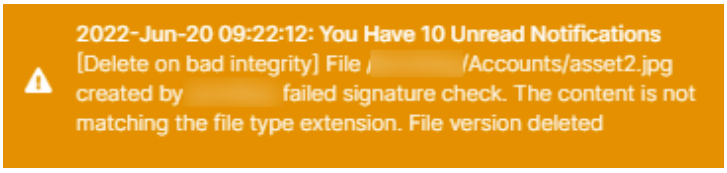
6. Click **Next**.
   You are prompted to choose an action.
7. Choose one of the **Verify file integrity** actions depending on what you want the system to do when a mismatch is detected. The possible actions are:
   - **Verify file integrity and generate admin alert on mismatch**: Detects the mismatch and adds an entry to the **Alerts** screen of the admin portal. However, the file is uploaded into FileCloud, and if it is determined that it should be deleted, this must be done as a separate action.
   - **Verify file integrity and delete on mismatch**: Detects the mismatch, adds an entry to the **Alerts** screen of the admin portal, and deletes the file from FileCloud. An audit entry is added in the admin portal to indicate that the file has been deleted by the workflow.



In both cases, a pop-up in the user interface notifies the user that the content and file type extension do not match, either:

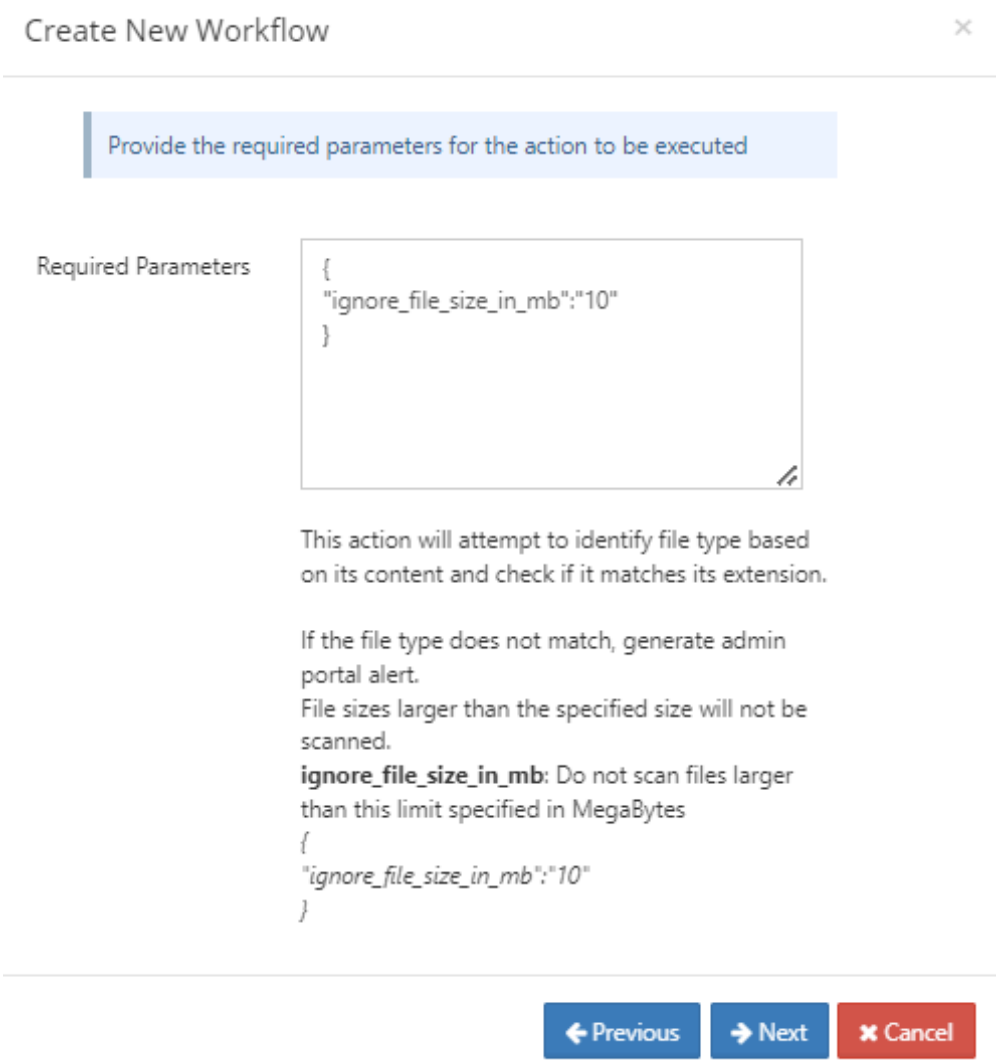


or

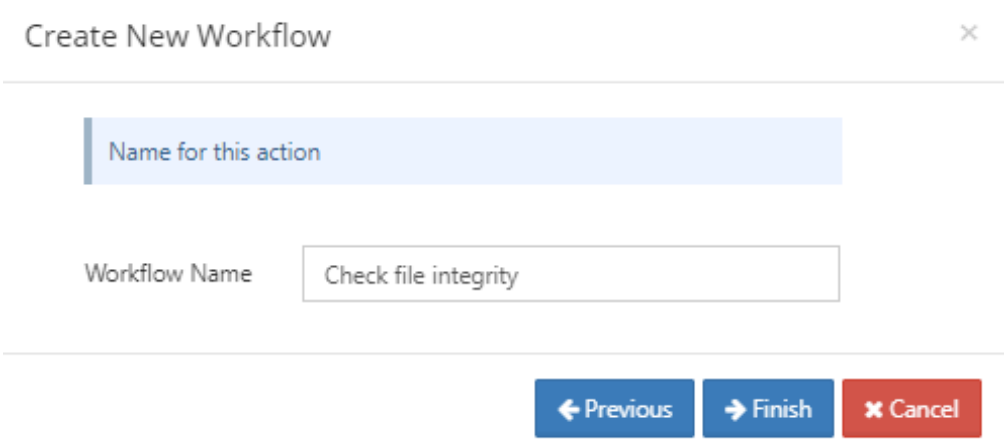


In both cases, alerts also appear in the **Manage Alerts** screen of the admin portal.

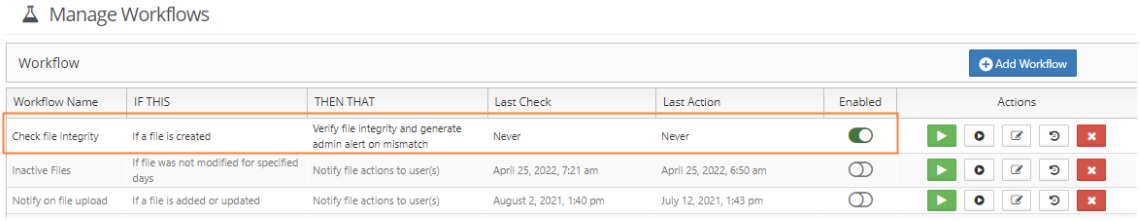
8. After you choose one of the actions, click **Next**.
9. Add the **ignore_file_size_in_mb** parameter. The purpose of this parameter is to prevent the system from slowing down by scanning the content of large files.
   In the following example, the parameter is set to **10**.



10. Click **Next**.
11. Enter a name for the workflow.



12. Click **Finish**.
    The workflow appears in the list on the Manage Workflows screen.



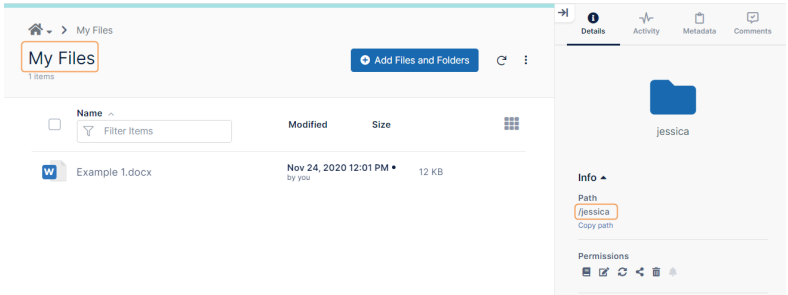
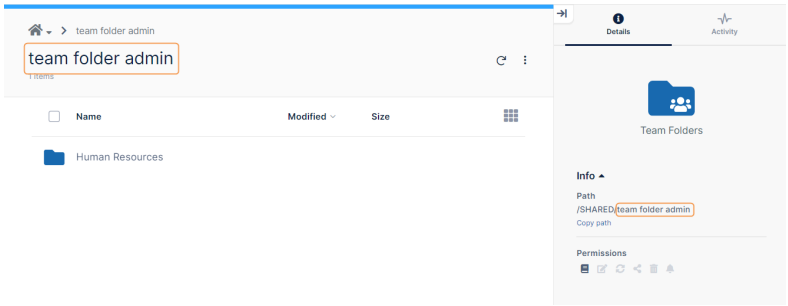
    Since the workflow is enabled, now each time a file is uploaded for the first time into FileCloud, its content and file extension are checked for a mismatch.

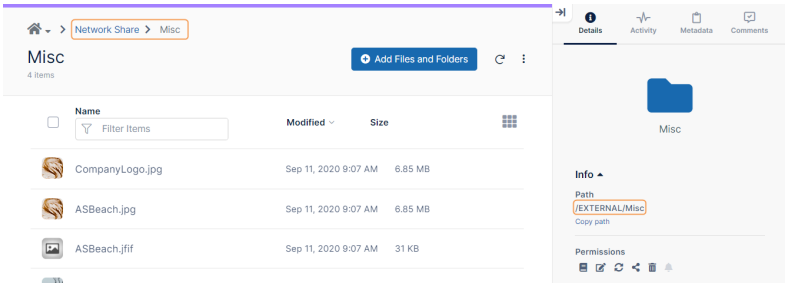
> By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check.

Identifying a FileCloud Specific Path

For many operations and configurations, FileCloud requires that you specify the FileCloud system path name. For example, when you are configuring a report or a workflow, if you want to specify a path, you must use the path's system name.

The following table lists the correct way to specify paths for files and folders in **My Files**, **Team Folders**, **Network Shares**, and **Shared with Me**.

Folder	How to specify path	Example
My Files	/username	In this example, to specify the **My Files** folder of the user with username **jessica**, use: **/jessica** If **jessica** were logged in, and she selected **My Files**, she would see the exact path in the **Details** tab in the right panel. 
Team Folders	/teamfolderaccount	In this example, to specify the **Team Folders** folder use the name of the account that manages Team Folders: **/team folder admin** An end user who selected **Team Folders** could look in the **Details** tab in the right panel and copy the portion of the path after /SHARED 

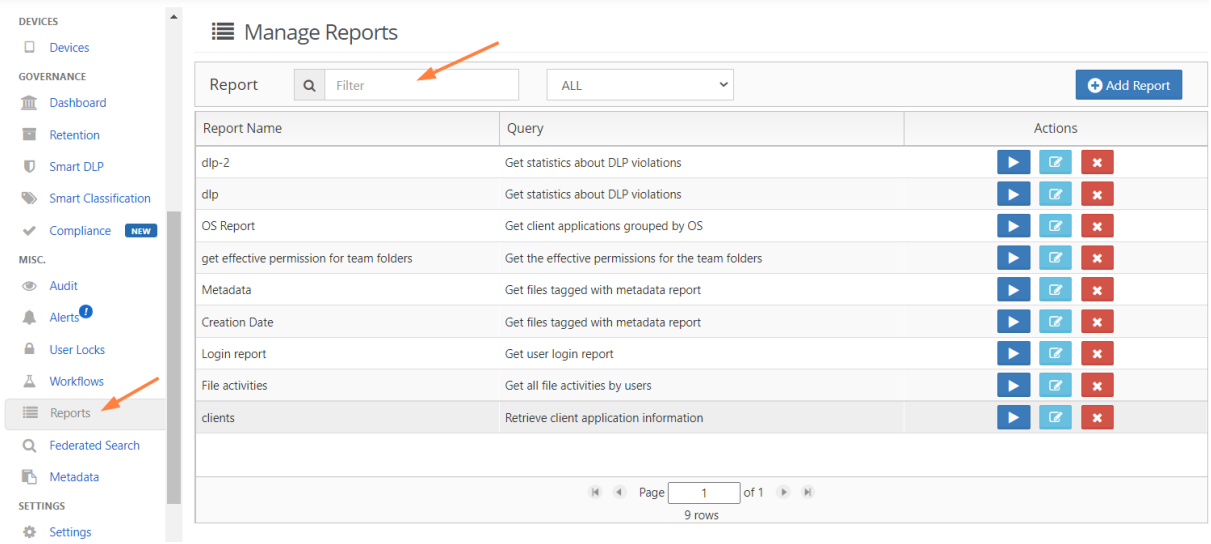
Network Shares	/EXTERNAL/foldername	In this example, to specify the **Network Shares** folder **Misc**, use: /EXTERNAL/Misc An end user who selected **Network Shares/Misc** could look in the **Details** tab in the right panel and copy the exact path. 
Shared with Me	Can't be done. You must specify the path from the owner's My Files (use the owner's username)	

Custom Reports

> The **folder_path** parameter was added to the **Get downloaded files** report in FileCloud version 23.242.

FileCloud enables you to create custom reports and download them in an Excel format. To get started with the reporting system, go to the Reports menu item in the left navigation menu in admin interface. In order to view the reports, the admin user must be the master admin or must have access to the reports system. An admin user can be granted access to the reports system through the Admins menu item on the left navigation menu.

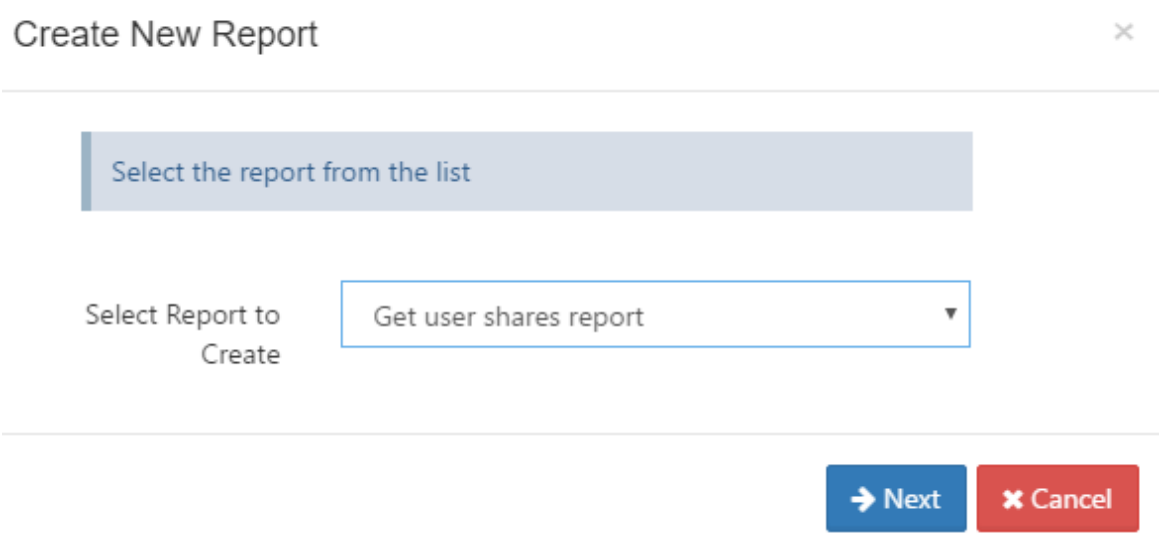
The reports screen displays the list of existing reports. The filter text box can be used to filter reports by name. The individual reports on the report list can be viewed, downloaded, edited and deleted. New reports can be added by clicking the Add Report button.



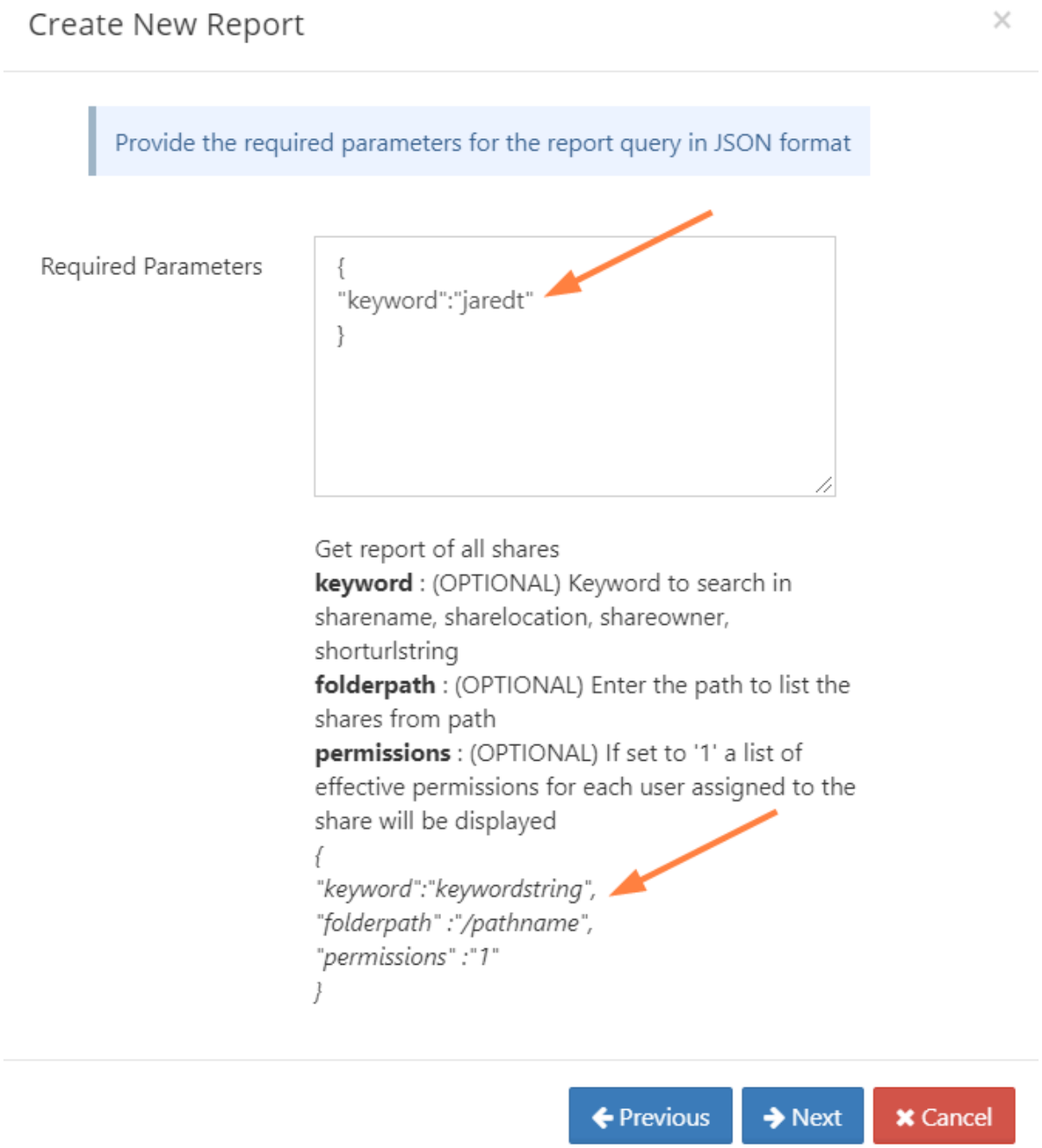
> Some reports, such as reports on file actions and failed logins, get their data from the audit log. These reports only include events that are in the audit logs when you run the report.

Add Reports

Click the add report button and Select the report to create from the drop down list.



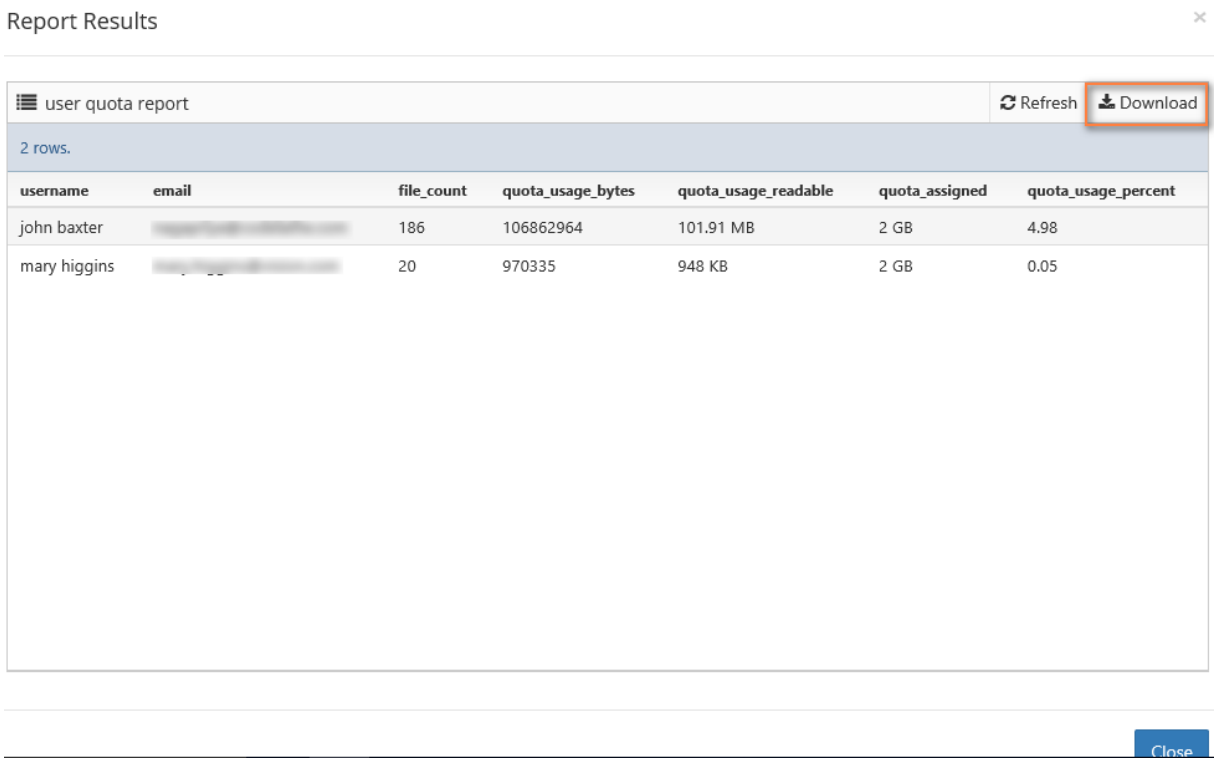
The next step is the set the parameters. The parameters can be entered in the text box. The format for the parameters are given on the bottom of the screen. The screen also indicates whether the parameters are optional or required.



The final step is to set a report name. The same report can be created multiple times with different parameters and named differently. This enables you to execute and download the reports quickly.

Download Reports

From the report list, run the report to view the report results in a separate window. First 30 rows are displayed on the screen. The download button can be used to download the data in csv format.



username	email	file_count	quota_usage_bytes	quota_usage_readable	quota_assigned	quota_usage_percent
john baxter	[redacted]	186	106862964	101.91 MB	2 GB	4.98
mary higgins	[redacted]	20	970335	948 KB	2 GB	0.05

Available Reports

Report Name	Description
Retrieve client application information	Report of all remote client devices connected to FileCloud and their details. **Data Retrieved**: userid, client display name, client os type, client OS version, client api level, client last login **Parameters**: None
Get client application grouped by OS	Report of total client devices that are connected to FileCloud grouped by client OS. **Data Retrieved**: client OS type(Windows, Android etc), total devices connected. **Parameters**: None

Report Name	Description
Get client apps grouped by TYPE	Report of total client devices that are connected to FileCloud grouped by TYPE. **Data Retrieved**: Client Type(Sync, Drive etc), total devices connected. **Parameters**: None
Get all file activities by users	Report of all add, update, share, download, and delete actions for files. If date parameters are not supplied, actions from last 7 days are retrieved. **Data Retrieved**: Timestamp of action, username, file name, action. **Parameters**: • user: (OPTIONAL) Enter the username to list the file activities of the user • from_date: (OPTIONAL) From date in Y-M-d H:i:s • to_date: (OPTIONAL) To date in Y-M-d H:i:s This report is available beginning in FileCloud 20.1.
Get file type distribution in managed storage	Report of File types stored in FileCloud along with the total count of each type **Data Retrieved**: File Type, total files stored. **Parameters**: None
Get storage usage by file type	Report of amount of storage space used by each file type. **Data Retrieved**: File type, sizeraw (file size in bytes), size (formatted file size) **Parameters**: None
Get users who have most files in managed storage	Report of users who have the most files stored under FileCloud in managed storage **Data Retrieved**: username, total files stored. **Parameters**: None
Get user quota usage report	Report of users who use the maximum quote in FileCloud managed storage **Data Retrieved**: username, email, file count, quote usage, quote assigned, quote usage percentage. Beginning with FileCloud version 20.3, the CSV file that is downloaded also displays the groups the user belongs to, the user's effective policy, and the user's last log-in date and time. **Parameters**: None
Get number of active files in managed storage	Report of total number of files that were changed in the last 1 day, 1 week, 1 month and 6 months **Data Retrieved**: days, total files changed, percent of files changed. **Parameters**: None

Report Name	Description
Get uploaded files report	Report on what files were uploaded during a given period, or files uploaded by a user or group of users during a particular period. **Data Retrieved:** Timestamp of upload, user name, user agent, IP address, file path, bytes of file uploaded **Parameters:** • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified • ignore_from_owner: (OPTIONAL) Define if the uploads made from folders owned by the user are ignored (YES or NO, defaults to NO)
Get downloaded files report	Report on what files were downloaded during a given period, or files downloaded by a user or group of users during a particular period. **Data Retrieved:** Timestamp of download, user name, user agent, IP address, file path, bytes of file downloaded **Parameters:** • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • folder_path : (OPTIONAL) Restrict report to files inside specified path. • username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified • ignore_from_owner: (OPTIONAL) Define if the downloads made from folders owned by the user are ignored (YES or NO, defaults to NO)
Get files tagged with metadata report	Report listing files/folders and their value for a specified metadata field. **Data Retrieved:** path of folder or file, username, metadata field, value of metadata field **Parameters:** • metadata_name : (REQUIRED) Name of the metadata set • attribute_name : (REQUIRED) Name of the metadata attribute • attribute_value: (OPTIONAL) Metadata attribute value
Get shares report	Report listing shares created. **Data Retrieved:** Timestamp of download, user name, user agent, IP address, file path, password **Parameters:** • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified

Report Name	Description
File query report	Report listing files or folders filtered by specified parameters if included. **Data Retrieved:** file or folder name, path, type (file or folder), size, last modification date, create date Note: Prior to FileCloud version 21.3, the year for the modification and create dates is returned in 2 digits (for example **Parameters**: • userid : (OPTIONAL) User id to retrieve listing. If not supplied, all user listings are generated • sort : (OPTIONAL) Sort criteria can be "SIZE" or "MODDATE" or "CREATEDDATE" • limit : (OPTIONAL) the total number of results • searchterm : (OPTIONAL) Match keyword in file or folder name • type : (OPTIONAL) Type can be "file" or "folder", default is "file" • path : (OPTIONAL) Restrict report to files inside specified path. For help specifying the path correctly, see Identifying a FileCloud Specific Path.
File count report	Report of file count in paths specified in parameters. **Data Retrieved**: number of files in each specified path. **Parameters**: List of paths. For help specifying the path correctly, see Identifying a FileCloud Specific Path. **Note**: This report does not include versions, deleted files and thumbnails; however, these files are considered in quota calculations in other reports, so file counts throughout reports may not be the same.
Get deleted files report	Report of deleted files. **Data Retrieved:** Timestamp of delete, user name, user agent, IP address, file path **Parameters:** • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s
Get bandwidth usage for this instance of FileCloud	Report of the total bandwidth (upload and download) as tracked by this instance of the file cloud server. **Data Retrieved:** upload bandwidth and download bandwidth **Parameters:** • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s
Managed Storage File, Folder Count, and Size report	Report of all folders and sub folders within a given path, showing each file count and total size of the folder **Data Retrieved**: folder and sub folder path, file count and size **Parameters**: • path: (REQUIRED) Location path. For help specifying the path correctly, see Identifying a FileCloud Specific Path. This report is available in FileCloud version 20.3 and later.

Report Name	Description
Get all exported secure docs report	Report of all files exported securely. **Data Retrieved**: folder path, user performing the download, options enabled (screenshot/screenshare, secure view, or enable print), # times accessed, max access times, last access date **Parameters**: None
Get user shares report	Report of all the shares created in FileCloud and their details. **Data Retrieved**: share name, share owner, share URL, share type, share location, created on, last access, expiry date **Parameters**: • keyword - search keyword in share name, share owner, share url string (string following /url/) • folderpath - location path. For help specifying the path correctly, see Identifying a FileCloud Specific Path. The CSV file that is downloaded contains additional information about users and groups that have access to each share. This update is available in FileCloud Server version 18.2 and later.
Get the advanced share activity of users	Report showing extensive details about the activity on a share. If no parameters are entered, the period reported is the last 7 days. **Data Retrieved**: timestamp of action, action, action details (share permissions), folder name, path, affected user, affected user email address, author (person performing the action), author email address, change source IP, additional info (indicates if share is a folder), share URL For multiple entries of the same share, the Action Details column on the report shows the most recent share's permissions. If a user shares a folder and shares a file in that folder during the period reported on, the report displays separate entries for the folder and the file. **Parameters**: from_date: (OPTIONAL) From date in Y-M-d H:i:s to_date: (OPTIONAL) To date in Y-M-d H:i:s owner: (OPTIONAL) Owner name This report is available beginning in FileCloud 20.1.

Report Name	Description
Get files/folders shared with user	Report listing the files and folders shared with a specific user **Data Retrieved**: share name, share owner, share url, share location, type (private or public), expiry date, creation date **Parameter**:email of share recipient This report is available beginning in FileCloud 21.1.
Get effective permissions for team folders	Report on the permission level of each user who has access to a team folder. **Data Retrieved**: folder, type (private or public), share location, user, permission **Parameters**: • paths: (OPTIONAL) List of the names of the team folders to include on the report. For help specifying the path correctly, see Identifying a FileCloud Specific Path. • users : (OPTIONAL) List of users to be included in the report.
Get anonymous/ unauthorized login geolocation report	Report of unauthenticated and anonymous users who accessed FileCloud showing users' IP addresses and location. To view location, **Show Geo IP Chart** in **Settings > Admin** must be set to **TRUE**. **Data Retrieved**: IP address, operation, username, user agent, geo area, city, country, create date **Parameters**: • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • group_by_ip : (OPTIONAL) Set to "1" to group result by IP address
Get user login report	Report of all logins to FileCloud and their details. If no parameters are entered, the period reported on is the last 7 days. **Data Retrieved**: login time, username, useragent, IP **Parameters**: • from_date: (OPTIONAL) login from date • to_date: (OPTIONAL) login to date OR • last_number_of_hours : (OPTIONAL) number of hours before the present time to begin retrieving login records. The last_number_of_hours parameter is available beginning in FileCloud 20.1. If from_date, to_date, and last_number_of_hours are entered together, last_number_of_hours is ignored.
Get number of emails sent, grouped by sender	Report of the number of emails sent in the last X hours **Data Retrieved:** sender, number of emails sent **Parameters:** • hours: number of hours ago to begin retrieving sent email records.

Report Name	Description
Get statistics about DLP violations	Report of DLP violations by rule. **Data Retrieved:** user, time of violation, user action, rule violated **Parameters:** • **rule_name** : (OPTIONAL) Name of the rule • **minutes** : (OPTIONAL) How many minutes ago to begin looking at violations The CSV file that is downloaded also displays the files subjected to the rule violation and, beginning in FileCloud 20.1, the metadata and attributes tagged to those files.
Get a report of active users	Report of active users in the last 15 minutes or for the time defined in minutes **Data Retrieved:** user name **Parameters:** • **minutes** : (OPTIONAL) How many minutes ago to consider users as active
Get file movement statistics	Report of last file uploads, downloads, and shares (or share changes) **Data Retrieved:** number of files downloaded, number of files uploaded, number of files shared and share changes **Parameters:** None

Specifying Y-M-d H:i:s values

Many of the report parameters require a date/time value in **Y-M-d H:i:s** format. The following table indicates the allowed values in this format.

Format	Description	Example/Possible values
Y	Year, in 4-digit format	2021
M	Month, in 2-digit format, with leading 0 if necessary	00 to 12
d	Day, in 2-digit format, with leading 0 if necessary	01 to 31
H	Hour, in 2-digit 24-hour format	00 to 23
i	Minute, in 2-digit format, with leading 0 if necessary	00 to 59
s	Second, in 2-digit format, with leading 0 if necessary	00 to 59

Including the **H:i:s** settings for time is not required.

Manage Folder Level Permissions

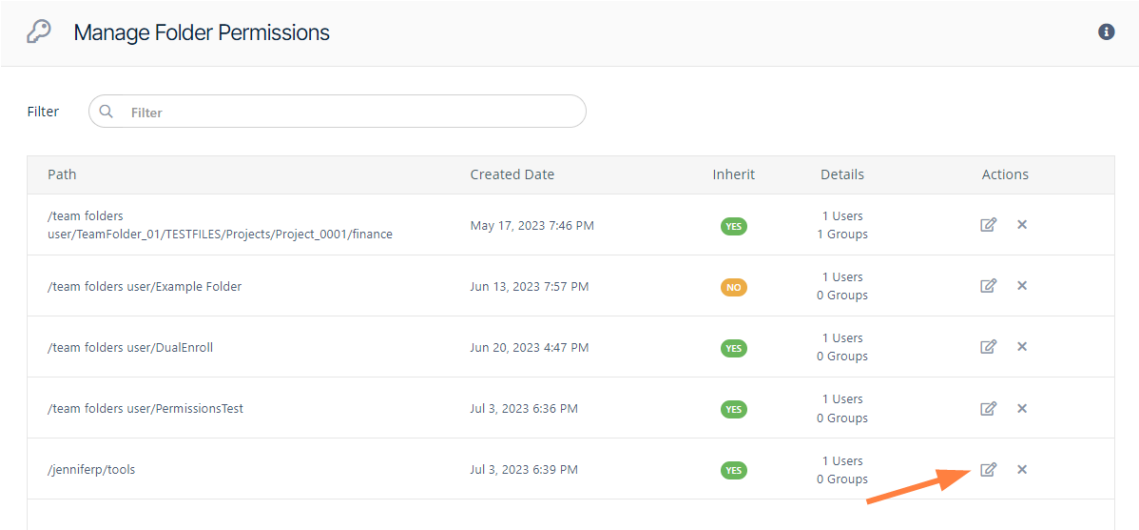
Administrators can manage folder-level permissions assigned to folders. In order to view these folder-level permissions, the admin must be the main admin or an admin user with access to the folder permissions enabled. An admin user can be granted access to the Folder permissions system through the Admins menu item on the left navigation panel (see Managing Admin Users).

The screen displays the list of existing folder-level permissions set in the system. This includes folder-level permissions set on Team Folders in the admin portal and folder-level permissions set on user folders in the user portal.
Use the **Filter** box to filter folder permissions on the folder path. Individual permissions can then be viewed, edited and deleted.

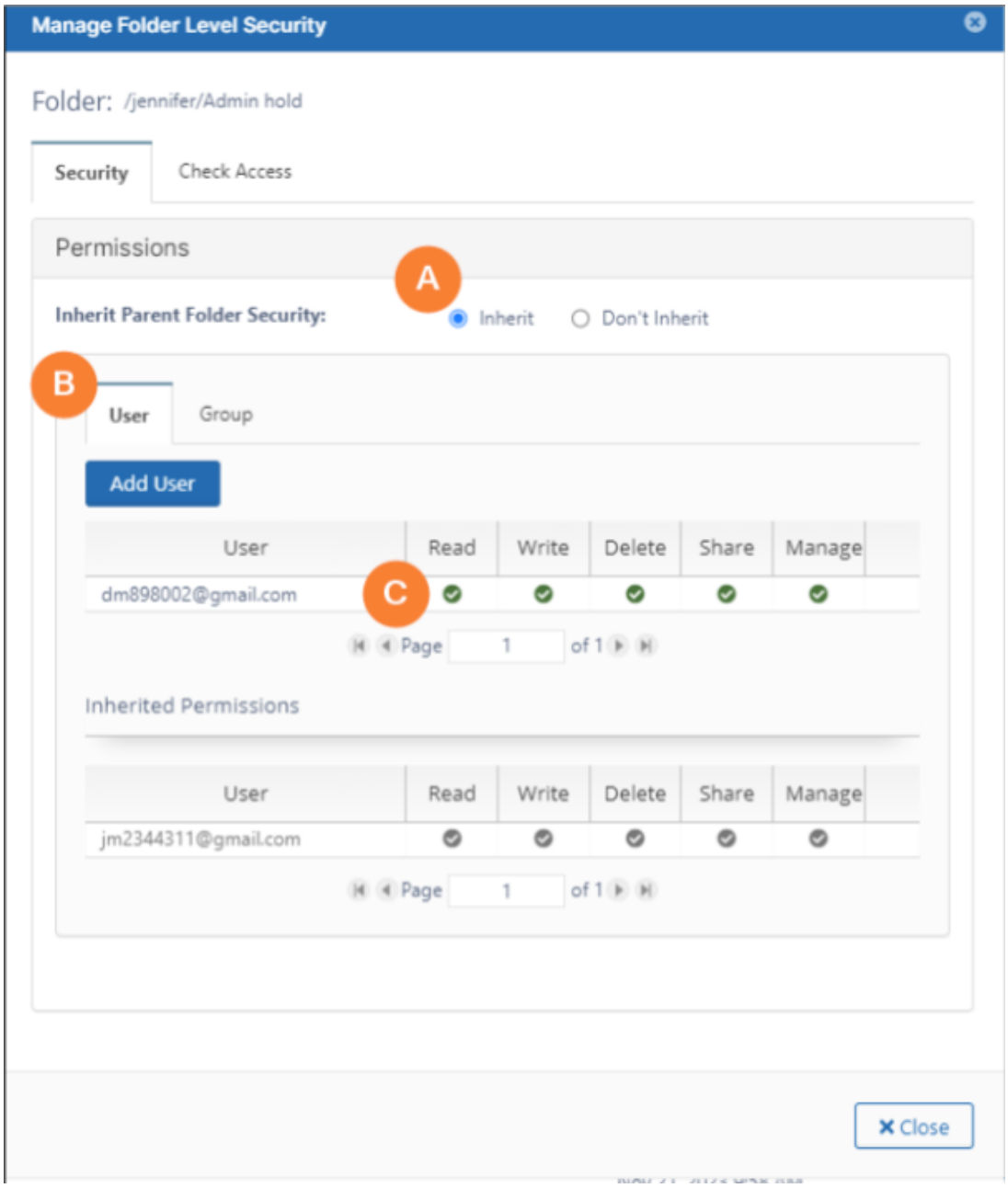
For more information about folder-level permissions, see Folder-Level Permissions.

To Edit Folder-Level Permissions

1. To open the **Manage Folder Permissions** screen, In the navigation panel, click **Folder Permissions**.



2. To open the **Manage Folder Level Security** dialog box, click the edit button.
3. Follow the steps below to assign and change user and group folder-level permissions. Users who do not appear
on the list have all folder-level permissions to the folder (unless their group permissions are limited)



A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.
B Click **Add User** to add a user and limit their access to the folder, or click the Group tab and add a group.
C In the top list of users, check or uncheck levels of permissions.

Managing Metadata

As an administrator, you can manage **metadata** to provide additional information about files and folders in FileCloud and to use the information when performing actions on them. FileCloud includes built-in metadata sets that include information such as image properties, file create dates, and metadata tags from other applications. FileCloud also allows you to build any number of custom metadata sets.

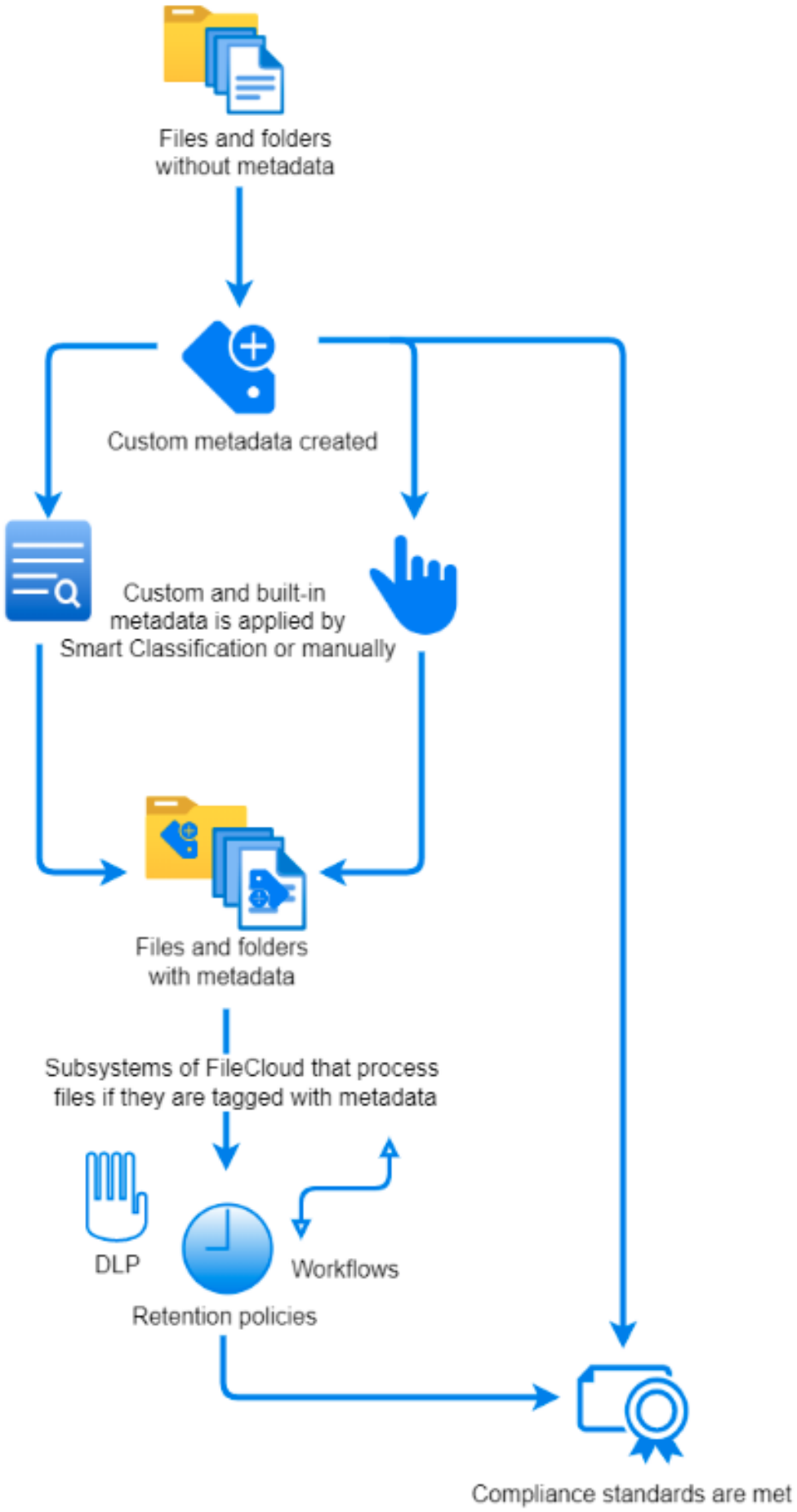
Metadata for governance and other system processes

Metadata serves an important role in the functioning of many processes in FileCloud, including compliance, data leak prevention (DLP), retention policies, and workflows. You can configure these processes to look for files and folders with certain metadata values and then act on matching files and folders accordingly.

The following diagram shows you how metadata is applied and used in FileCloud. First, create your metadata, if necessary. FileCloud includes built-in metadata, but for some purposes, such as identifying confidential or secure information, you must create custom metadata. After your custom metadata is created, Smart Classification automatically applies the correct metadata to files and folders. In addition, users can apply metadata manually.

After files and folders are marked with metadata, the DLP, retention, and workflow sub-systems of FileCloud use metadata to identify content to act on. Some examples are described below the diagram.

Once the necessary metadata, DLP rules, and retention policies have been configured, compliance standards can be met.


Files and folders
without metadata
Custom metadata created
Custom and built-in
metadata is applied by
Smart Classification or manually
Files and folders
with metadata
Subsystems of FileCloud that process
files if they are tagged with metadata
DLP
Workflows
Retention policies
Compliance standards are met

Here are some examples of the way the different sub-systems in FileCloud can use metadata:

- **DLP**: If a file's **Confidential** metadata attribute is equal to **Yes**, DLP prevents it from being shared externally.
- **Retention policies**: If a file's **Sensitivity Label** attribute is equal to **general,** then a retention policy of 3 years is applied to it.
- **Workflows**: If a file's **Modified** attribute is equal to a date over 3 months ago, then a workflow sends an email to the email address in **Last Modified By**.

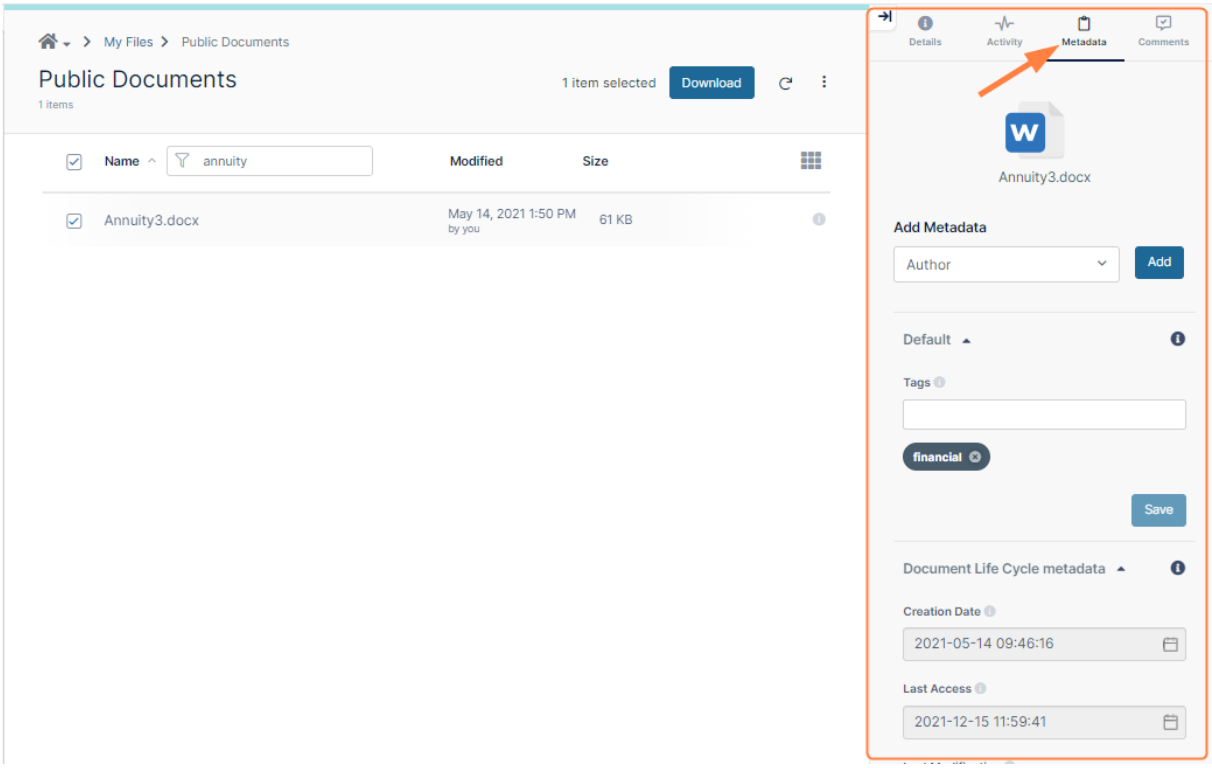
Here are some examples of the way compliance rules are met by metadata:

- The HIPAA section of the Compliance Center requires that your system include metadata that identifies PHI data.
- The ITAR section requires your system to use content classification to apply metadata tags to defense and technical articles, and then use DLP to block public sharing of the tagged articles.

Example of the process: In a medical facility's system, a new file is uploaded. Smart Classification searches its contents for the string **Medical Record Number**. It finds the string and applies the **PHI** metadata tag to the file. When an external user attempts to upload the file, a DLP rule identifies the **PHI** metadata tag, and therefore, does not allow the upload. In 2 weeks, a user attempts to delete the file, but a 6-year retention policy identifies the **PHI** metadata tag, and does not allow the file to be deleted.

Metadata for users

Metadata is also useful to your users, who can view the information it provides about files and folders in the Metadata tab in the side panel of the user portal. In the Metadata tab, users can view the metadata applied to a file or folder, and depending on their permissions, can add and change metadata.



Users can also search on metadata and apply color tag metadata to files and folders for categorization and identification purposes.

In this section

Metadata Components and Types

FileCloud defines two levels of metadata definition:

1. **Attribute** - defines a single piece of information that user can specify for file or folder.
2. **Metadata set** - a group of related attributes with additional properties and settings. It works as a container for attributes.

See a Description of Metadata Terms

Figure 1. Metadata Terms

File Object	Metadata	Attribute	Metadata Set	Tag
Every file and folder that exists in FileCloud.	Information about the file data. Describes files and folders available in the system.	A single piece of information that describes the File Object. In FileCloud attributes are defined as a part of the metadata set.	A set of metadata attributes that might be logically grouped and can be attached as a single entity to File Objects.	a special type of attribute (referred to as the Array attribute type) that allows users to provide multiple custom values for each File Object.

For example:
• a resume
	For example:
	• Lives in the Human Resources Folder
	• Has a created date
	• Has a modified date
		For example:
		• the candidate's photo in their resume
			For example, resumes will always have:
			•
			  • Photo
			  • Name
			  • Address
			  • Experience
			  • Education
				For example:
				HR wants to tag a resume status as:
				• Candidate
				• New Hire
				• OnBoarding

Metadata Set Types

FileCloud supports the following types of Metadata Sets:

TYPE	DESCRIPTION	SETS AVAILABLE
Default	This a special type of metadata set that is automatically associated with every single File Object when it is created, copied, uploaded, etc. • For already existing File Objects it will be associated when the file / folder is accessed for the first time. • Exactly one Default Set exists in FileCloud - it cannot be deleted, renamed or disabled, but administrators can customize attributes and permissions. • Out of the box it is shipped with a single predefined attribute of Array type - Tags.	• Default

TYPE	DESCRIPTION	SETS AVAILABLE
Built-In	These are metadata sets that have been created for you. • Administrators can edit the attributes • Administrators can choose to disable the use of this metadata	• Image metadata • Document Life Cycle metadata • Microsoft Office Tag metadata • Color Tag metadata • PDF Tag metadata • AIP Sensitivity Label metadata • CDR metadata (added in FileCloud 23.241.4) • Signority eSignature metadata (added in FileCloud 23.241.4) • ITAR metadata (added in FileCloud 23.252) • CUI metadata (added in FileCloud 23.252) • Extended metadata (added in FileCloud 23.262)
Custom Metatdata Set	This is a fully customizable set of metadata, defined by the administrator.	As many as you want to create

How do I allow users to tag their files?

You must specify which users can access the Metadata attributes. If you do not add them, then the user will not be able to add a tag to their file.

Manage Metadata Permissions

More Information:

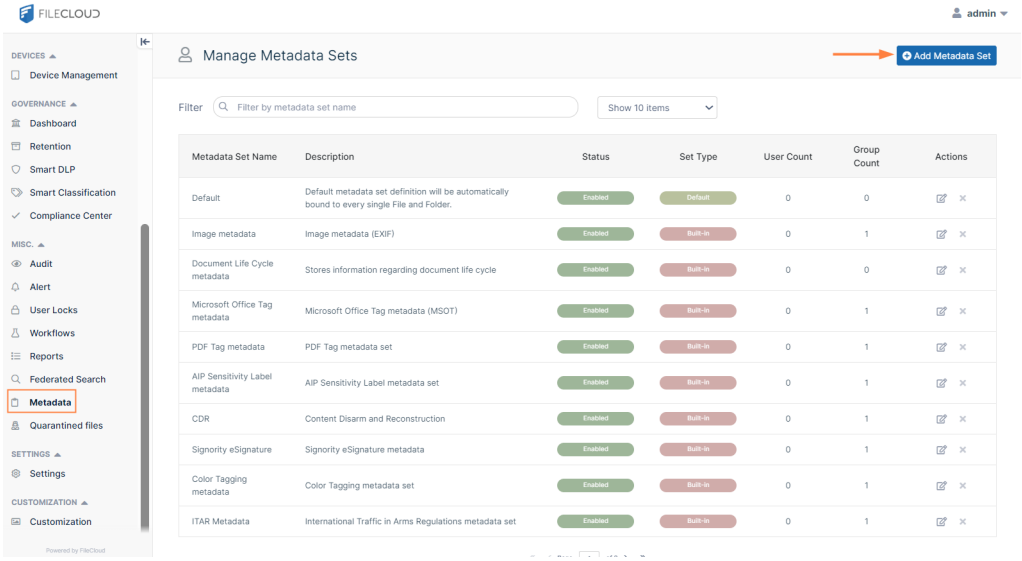
FileCloud Blogs
• **How to Best Utilize FileCloud's Metadata**

Create a New Metadata Set

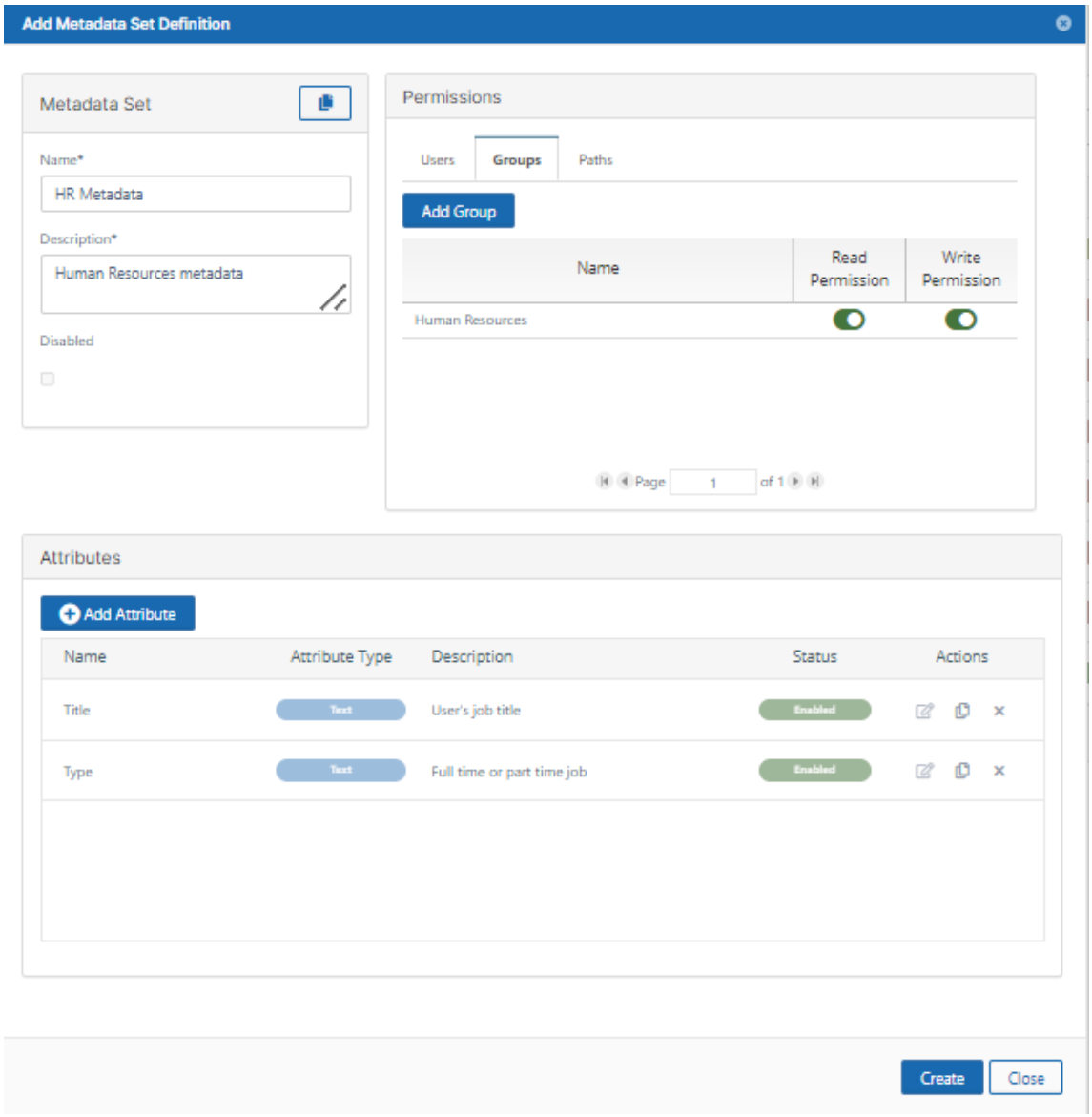
Add a new metadata set definition

To add new metadata:

1. In the navigation panel, click **Metadata.**

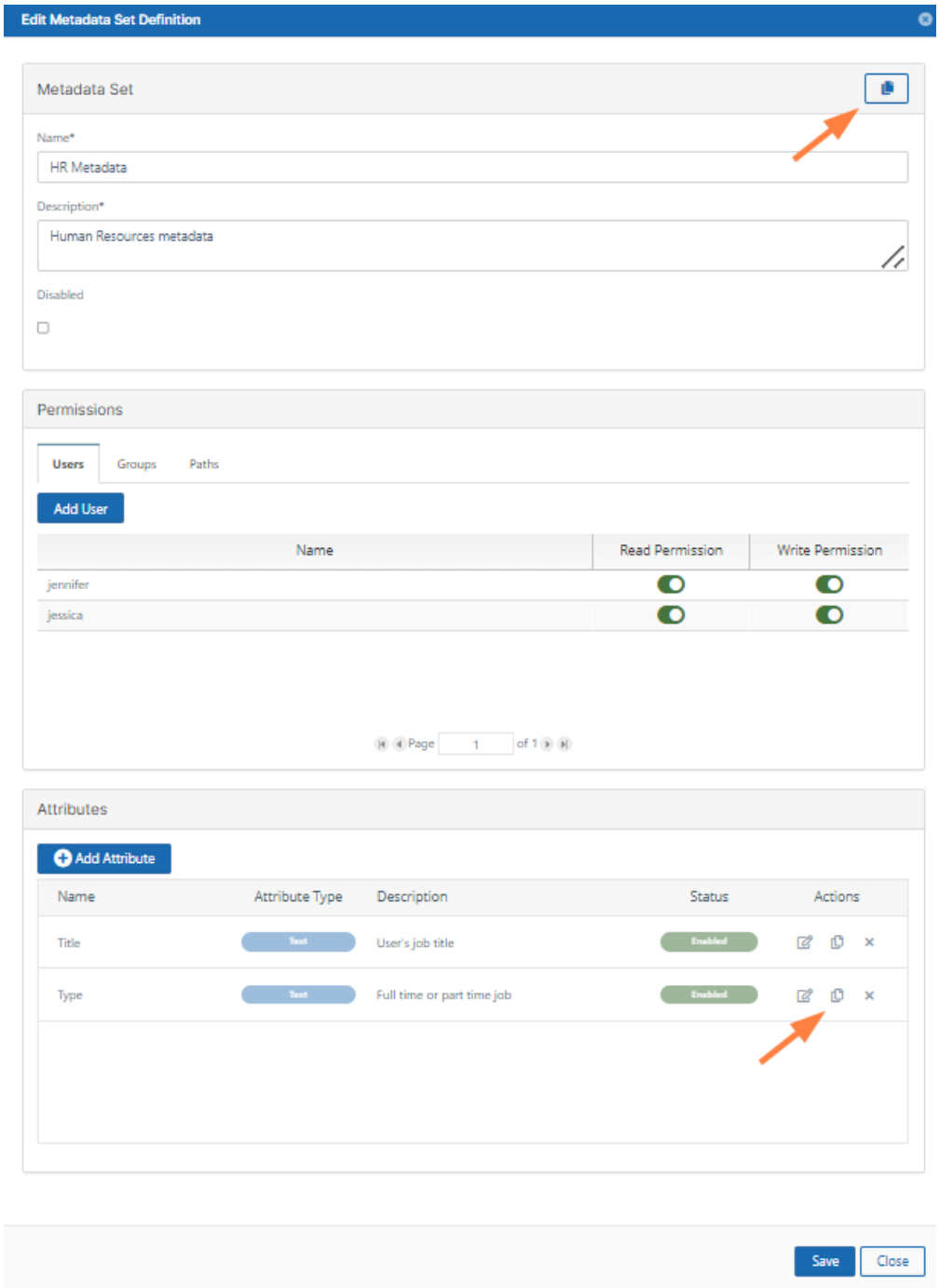


2. To open the **Add Metadata Set Definition** dialog box, click **Add Metadata Set**.



3. Enter **Name** and **Description** and check **Disabled** if you don't want the metadata set to be enabled when you save. it.
4. Add users or groups and specify permissions for them. Define FileCloud paths (locations) that have access to the metadata set. For more details, see Managing Metadata Permissions.
5. Click **Add Attribute** and add at least one metadata attribute definition. For more details, see Managing Metadata Attributes.
6. Click **Create**.

Note: If you need the metadata set id, click the copy icon in the **Metadata Set** box. If you need a metadata attribute id, click the copy icon in the row for the attribute:



Edit an Existing Metadata Set

Propagating changes

Once changes to the metadata set definition are saved the background process runs, which propagates changes made to the set definition to metadata_values collection that stores user provided attribute values. This is done to keep both collections in-sync and to increase performance for end-user metadata actions. Metadata info properties (name, description, status) are updated, permissions are omitted as they're not used in the metadata_values collection and the main task is to keep attributes in sync. There are three main use cases that are served by the task:

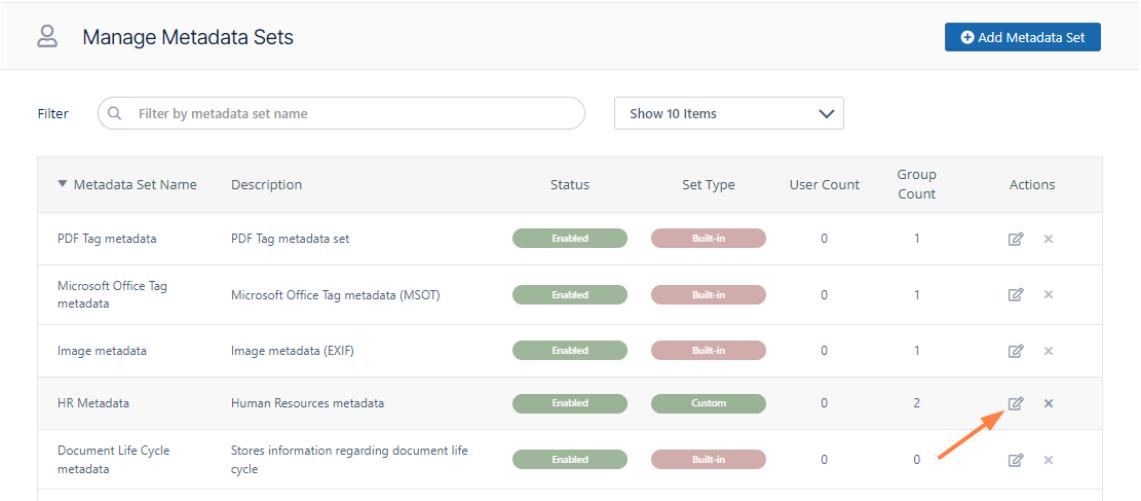
1. **New attribute is added** - attribute definition is added to each associated metadata_values document. Default value provided for this attribute is used.
2. **Existing attribute is changed** - attribute definitions is updated for each associated metadata_values document. **Existing values remain untouched** even when default value was updated (the new value will be used for newly associated file objects but not for existing records).
3. **Attribute was deleted** - attribute definition is removed for all associated file objects. **Values are removed** accordingly**.** This operation cannot be reverted so all values for this attribute **will be lost**.

Notes:

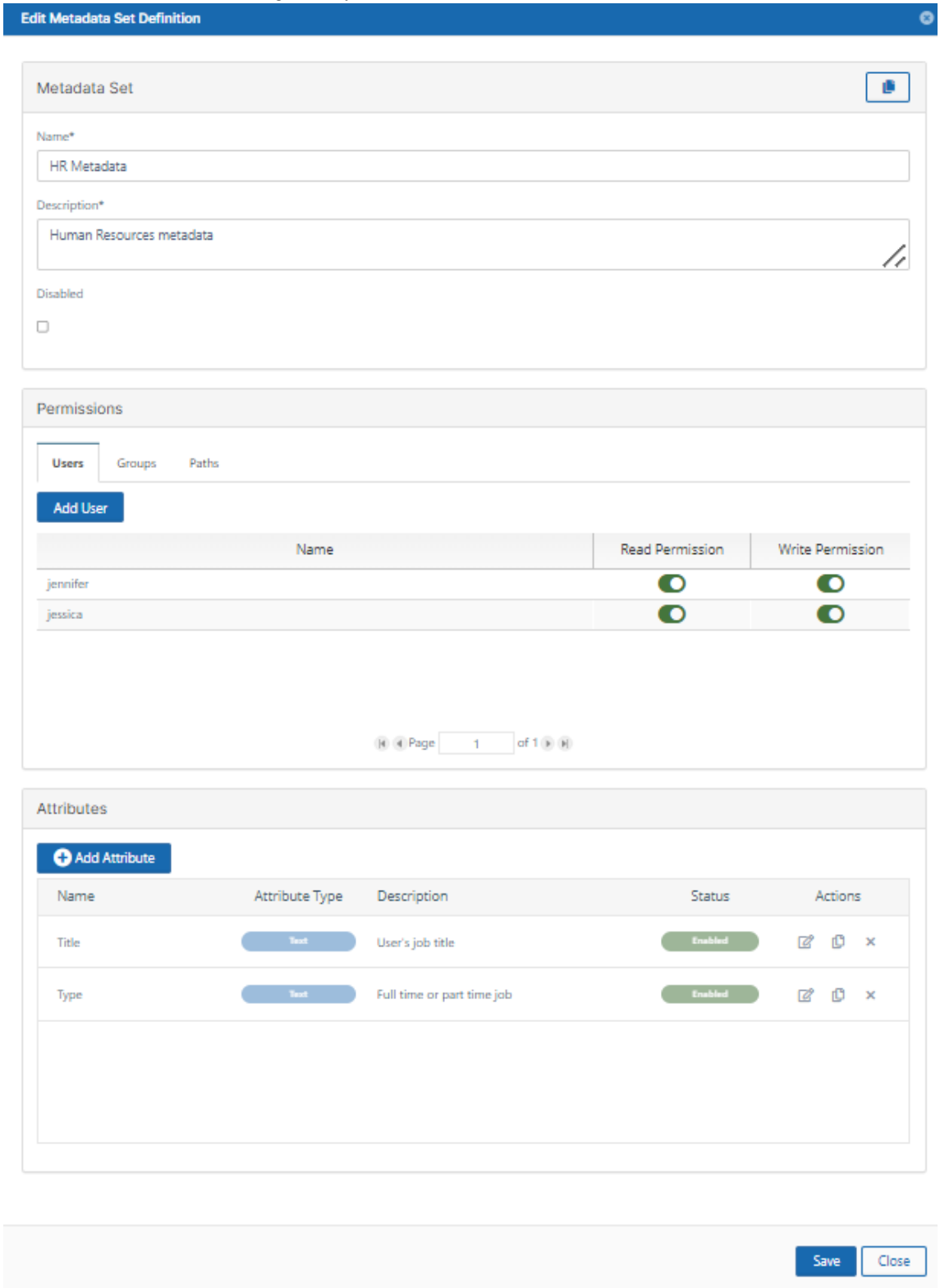
- The Default Metadata set is a special type and cannot be renamed.
- When an existing attribute is removed **all** associated values will be removed. This operation cannot be reverted.

To edit an existing metadata set:

1. Open a browser and log in to the admin portal.
2. From the left navigation pane, under **Misc.**, click **Metadata**.
3. In the row of the set you want to edit, under **Actions**, click the edit button.



The **Edit Metadata Set** dialog box opens.



4. Edit properties, permissions and attributes.

5. Click **Save**.

Managing Metadata Attributes

Administrators can manage metadata tags in FileCloud.

Attribute Types

Each attribute can have one of the following types:

Attribute type	Accepted values	UI editor type	Values validation
Text	Regular text value	TextBox	-
Integer	Integer numbers	TextBox	Type validation
Decimal	Decimal numbers	TextBox	Type validation
Boolean	True / False value	CheckBox	-
Date	Date value	Date picker	-
Enumeration	One value from a list of predefined values	Drop down / Select	-
Array (Tag)	A number of custom values provided by user	Tag Input - custom editor	-

⚠️ Attribute type cannot change once the definition is saved.

How do I add or delete attributes?

You can use the following ways to manage attributes:

- Edit Metadata Set Definition window
  - A new attribute can be added by clicking the "Add Attribute" button in the Attributes section of the Metadata definition widget.
  - Existing attributes can be edited by clicking the "Edit Attribute Definition" icon.
  - Existing attributes can be removed by clicking the "Delete Attribute Definition" icon.
- Tag Input Editor
- Tag input is a custom editor that allows users to provide multiple values for a single attribute with a better experience.

- It looks like a regular TextBox but supports multiple values.
- When user writes a string and presses the Enter or enters a comma a new value is added to the control.
- It's called a Tag and appears as a text in a blue rectangle. Values can be removed by pressing the cross icon.
- It is used as the editor for the Array attribute type (in the User Core UI) and as the editor for Predefined values for enumeration attribute type (in the Admin UI).

See a video on Managing Attributes.

⚠️ All attribute definition changes take effect when the whole set definition is saved.

Video of Managing Metadata Attributes

After creating the metadata set, you can add, edit and delete its attributes.

Managing Metadata Permissions

Administrators can use FileCloud Server to set the following Metadata types of permissions:

- User/group permissions (read/write) - these grant access to specific users and
- Allowed paths support - which affects File Objects based on their location.

What are effective permissions?

When setting Metadata permissions, you need to consider additional permissions on the File Object such as:

- lock permissions,
- share permissions,
- network folder permissions,

Effective permissions include all of these considerations. For example, on a shared file, if a user has write permission to the metadata set but read-only access to share then the effective metadata permission would be read-only.

Table 1. Permissions Examples

User permissions	Group permissions	Allowed Paths	File Object	Additional permissions	Read/Write	Comment
Write	Readonly	All	/USERNAME/assets	-	y/y	Write permission is granted based on the user permissions
Write	-	All	/USERNAME/assets/image1.png	write lock	y/n	As lock is applied, readonly access to metadata will only be granted
Readonly	Write	All	/SHARED/user1/assets	view only access for share	y/n	Share permissions will narrow metadata permissions to readonly
Readonly	Write	/USERNAME/assets	/USERNAME/assets/images	-	y/y	As file path is a subpath of one of the allowed paths user will be granted write access for metadata
Write	-	/USERNAME/assets	/USERNAME/images	-	n/n	The path isn't allowed so no metadata permissions are granted at all

How do I grant users permission to access Metadata?

The process of adding group permissions is similar to adding user permissions. The main difference is that when you use the *Add Group* button, all available groups are listed immediately. The rest of the process is exactly the same.

To grant a user access to the Metadata field:

1. Log in to the Admin Portal.
2. In the *Home* navigation panel on the left side, under *Misc.*, select *Metadata*.
3. In the *Manage Metadata Sets* section, select the one you want to grant access, and then click on the edit icon.
4. In the *Edit Metadata Set Definition* window, in *Permissions*, select the *Users* tab, and then click *Add User*.
5. In the *Search Users* window, in *Account or Email*, type in the user's information, and then click *Search*.
6. Select a user, and then you are returned to the *Edit Metadata Set Definition* window.
7. By default, the user is granted both *Read* and *Write* permissions.
8. Select the *Read* checkbox to grant or deny the user Read permissions.
9. Select the *Write* checkbox to grant or deny the user Read permissions.
10. At the bottom of the *Edit Metadata Set Definition* window, click *Save*.

⚠️ It is very important to remember that all changes made to permissions are not saved until "Save" button is clicked and the validation is successful.

Watch a video on granting users permission to access Metadata.

How do I allow paths on which the metadata sets can be added?

All paths have to have one of the following formats:

- /USERNAME/...
- /EXTERNAL/...

Administrators can choose to allow all paths or specific paths on which the metadata sets can be added.

- By default all paths are allowed.
- When an administrator wants to provide a specific set of allowed paths:
  - the "Allow Selected Paths" option has to be selected and
  - all allowed paths have to be specified via the Add Allowed Path dialog.

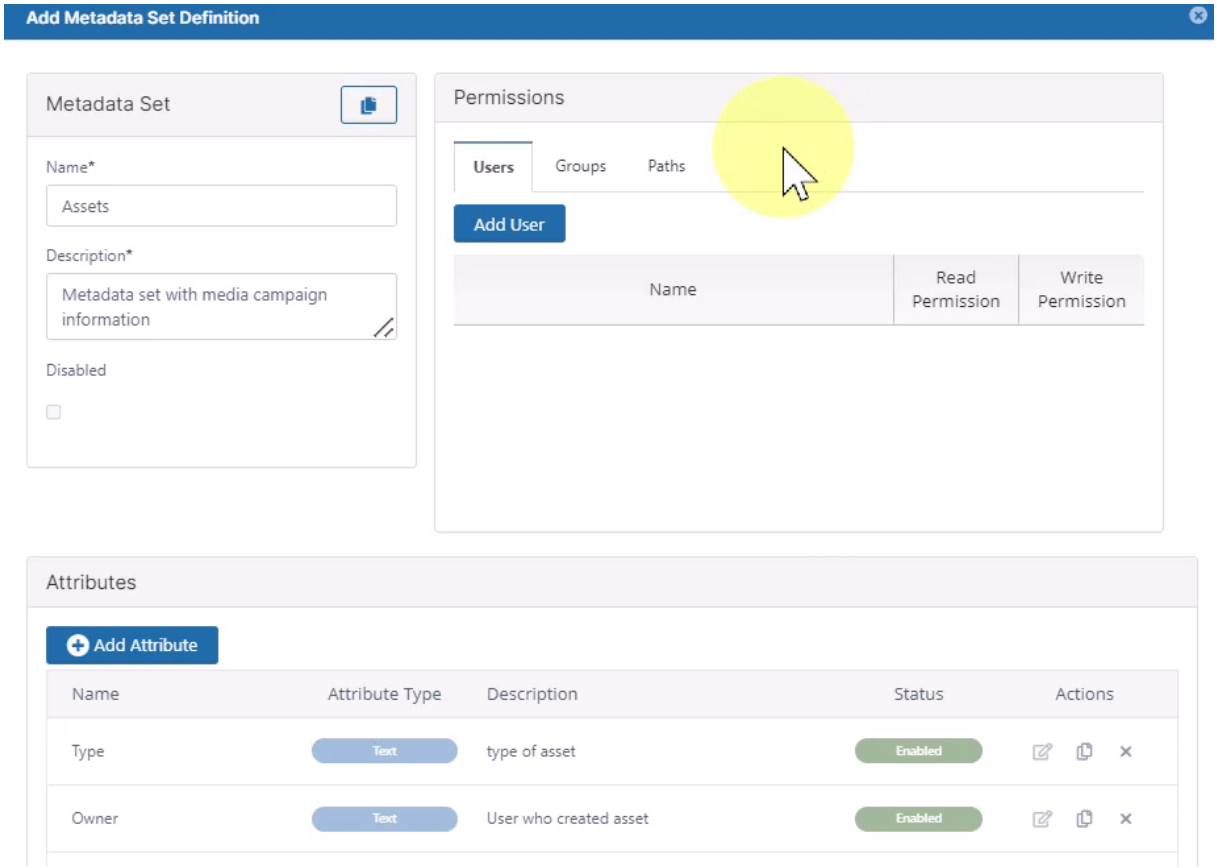
- When the path is added it will be displayed on the list.
- A path can be removed from the list by clicking on the "Remove Allowed Path" icon.

> When path is allowed all sub-paths are automatically allowed as well. For example, when path: /USERNAME/assets is allowed than automatically the sub-paths /USERNAME/assets/images, /USERNAME/assets/videos/HD, etc are allowed.

Watch a video on creating allowed paths.

Video of Allowing Paths for Metadata Permissions

Administrators can use FileCloud Server to set the paths that metadata applies to. The metadata can only be applied to files and folders located on that path.



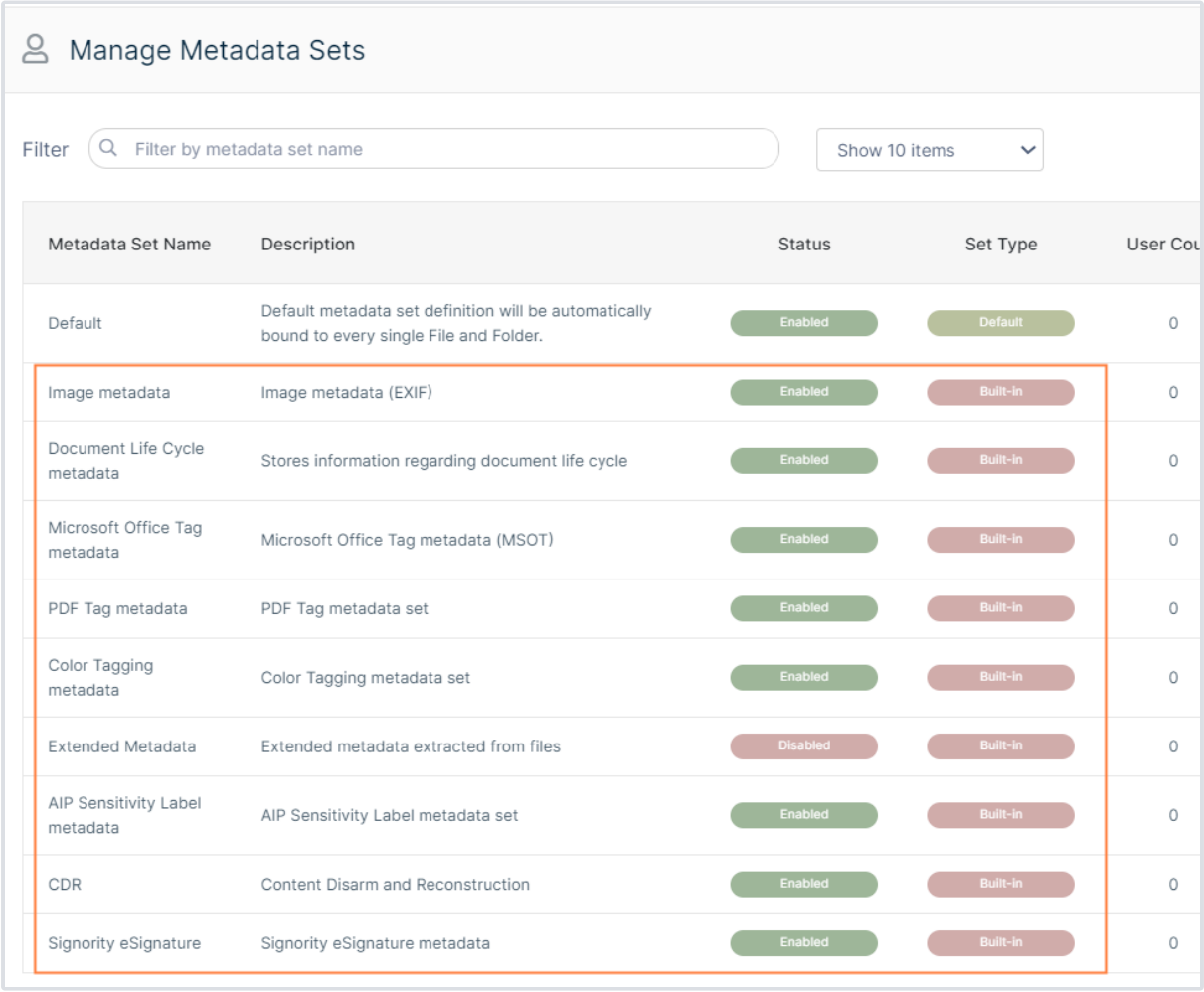
Video of Granting a User Metadata Permissions

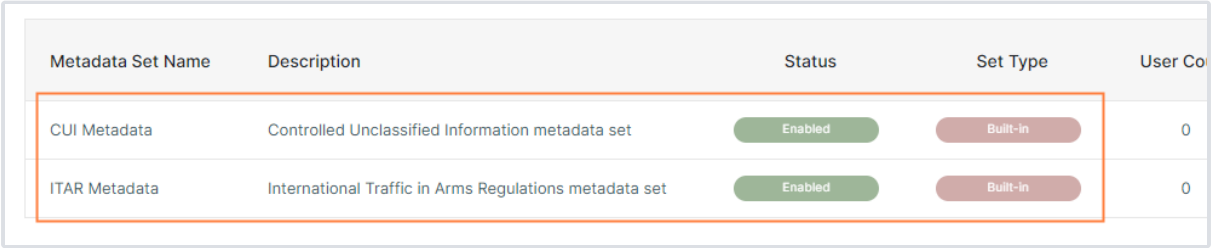
When you add a user to a metadata set, you can choose whether the user has write permission. If you remove read permission, the user is removed from the list.

Wor
king
with

Built-In Metadata

Built-in is a special type of metadata set that is automatically created for you.





Unlike the **Default** metadata set:

- Built-In sets cannot be renamed
- Built-In sets are not limited to paths

The versions of FileCloud in which each built-in metadata set and its attributes became available are listed in the following table:

Built-in Metadata Set	FileCloud Version
Image	18.1
Document Life Cycles	18.1
Microsoft Office Tag	20.1
Color Tagging	20.3
PDF Tag	21.2
AIP Sensitivity Label	21.2
CDR	23.241.4
Signority eSignature	23.241.4
ITAR	23.252
CUI	23.252
Extended	23.262

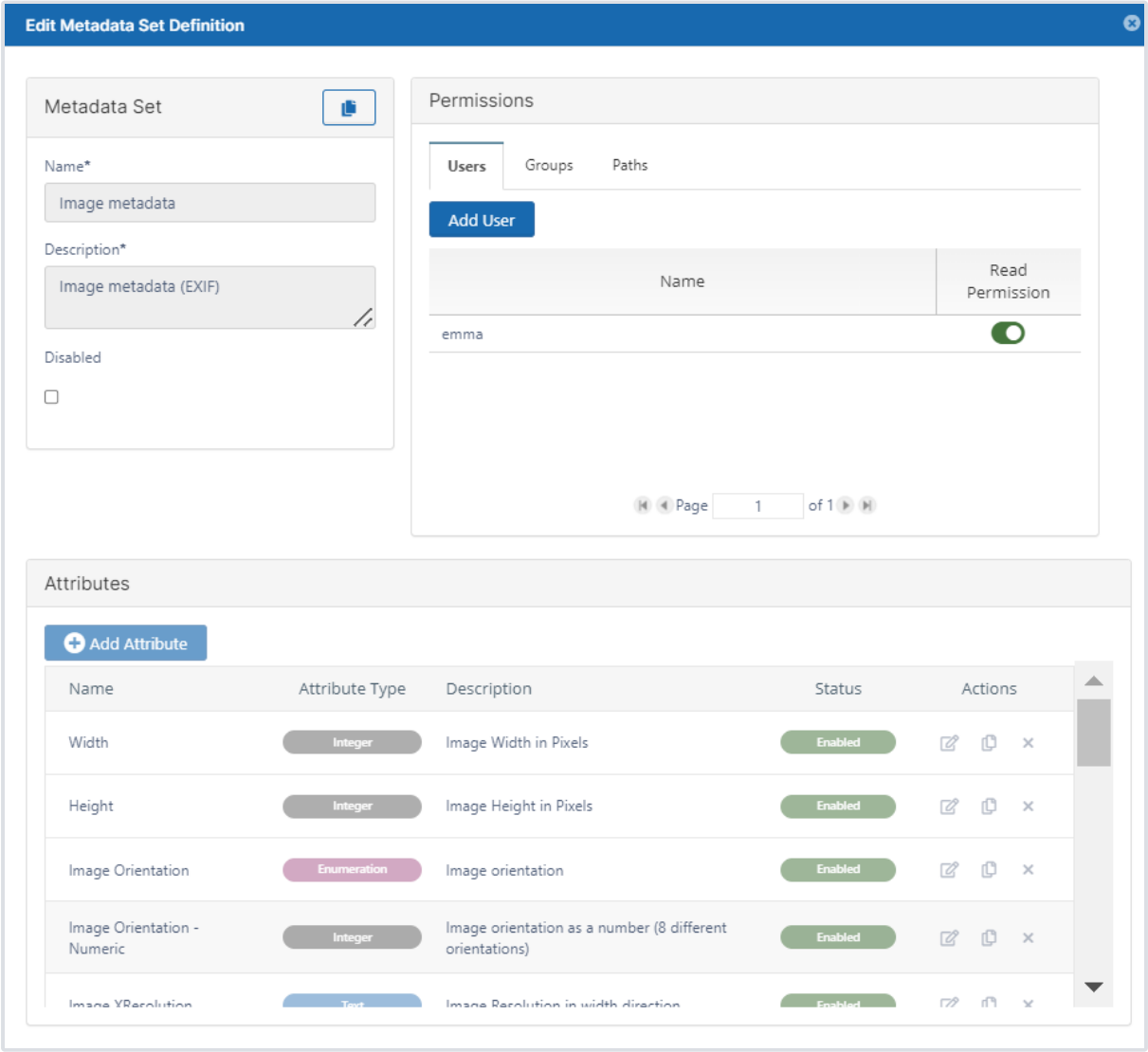
The **Color Tagging** metadata set differs from the other built-in metadata sets because its Tag attribute can be edited (but not deleted).
The attributes of all other built-in metadata sets cannot be edited or deleted.

The sets that have been created for you include:

Image Metadata

The **Image** metadata set is based on the Exchangeable Image File Format (Exif) and is a standard that records the important data on image files such as shutter speed, aperture, ISO Speed, lens type etc.

- The Exif data provides valuable information to organize photographs, perform searches and provide vital information to photos stored in FileCloud.
- This set is provided to you so that you can allow users to store and search image attributes using metadata.
- FileCloud does not apply Image metadata for Azure/S3 Network Folders.



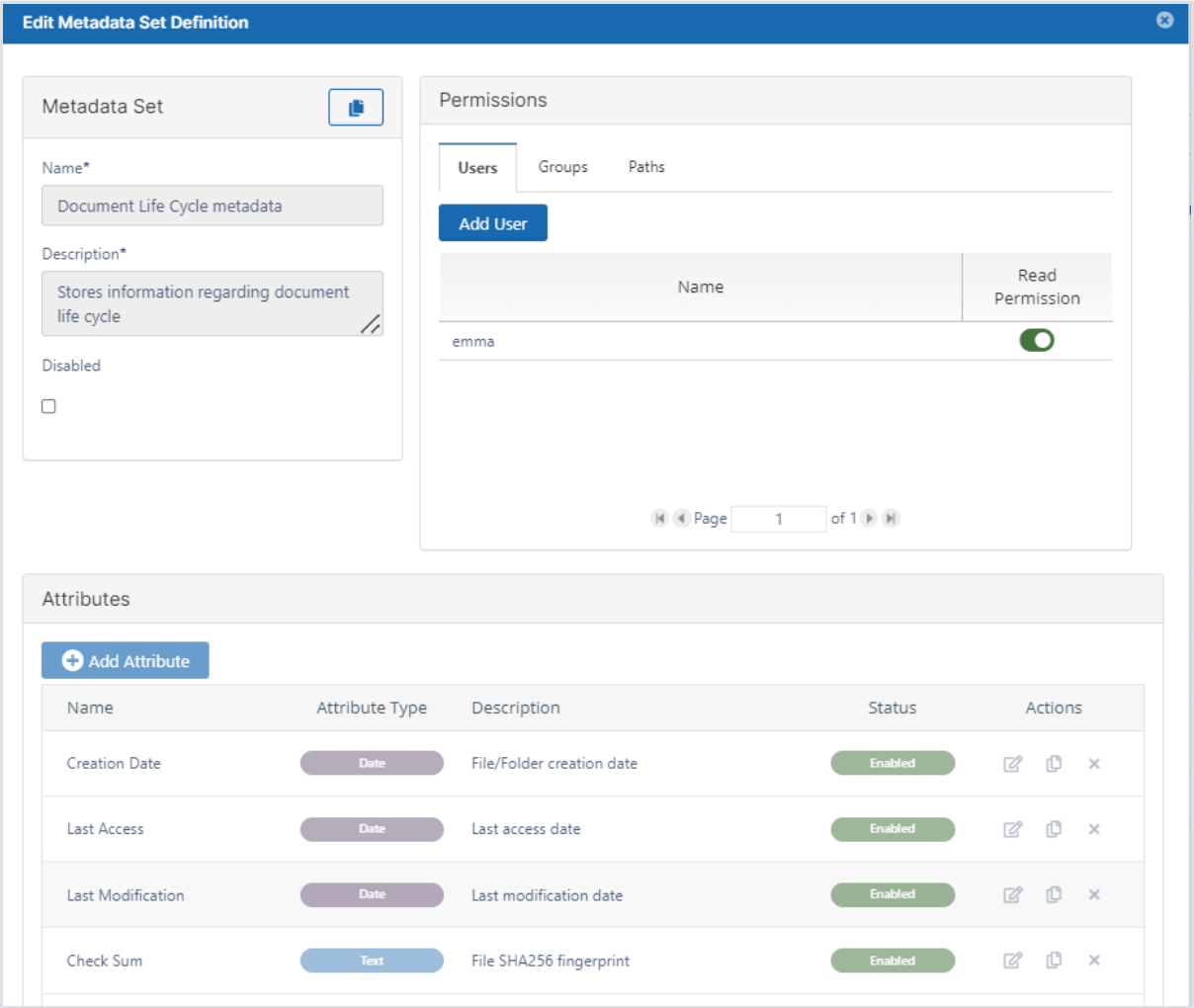
The following attributes exist in the **Image** built-in metadata set:

	Description	Options
Name	Title for the metadata set: Image metadata	• Required • This cannot be changed
Description	By default, says: Image metadata (Exif)	• Required • This cannot be changed
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	• Not selected • This cannot be changed

	Description	Options
User Permissions	Grant access to specific users to: • Read: this permission displays the metadata to the user in the User Portal For more information, read Managing Metadata Permissions	• Not Required • Read
Group Permissions	Grant access to specific groups to: • Read: this permission displays the metadata to the user in the User Portal For more information, read Managing Metadata Permissions	• Not Required • Read
Path Permissions	File Objects in this location will have the metadata set applied	• Not available • This cannot be changed
Attributes	A number of tags that are built-in for image files	• Width: Image width in pixels • Height: Image Height in pixels • Image Orientation • Image Orientation - Numeric: orientation as a number • Image XResolution: width direction • Image YResolution: height direction • Unit of Resolution

Document Life Cycle Metadata

This set stores information about a document's life cycle.



The following attributes are included in the **Document Lifecycle** metadata set:

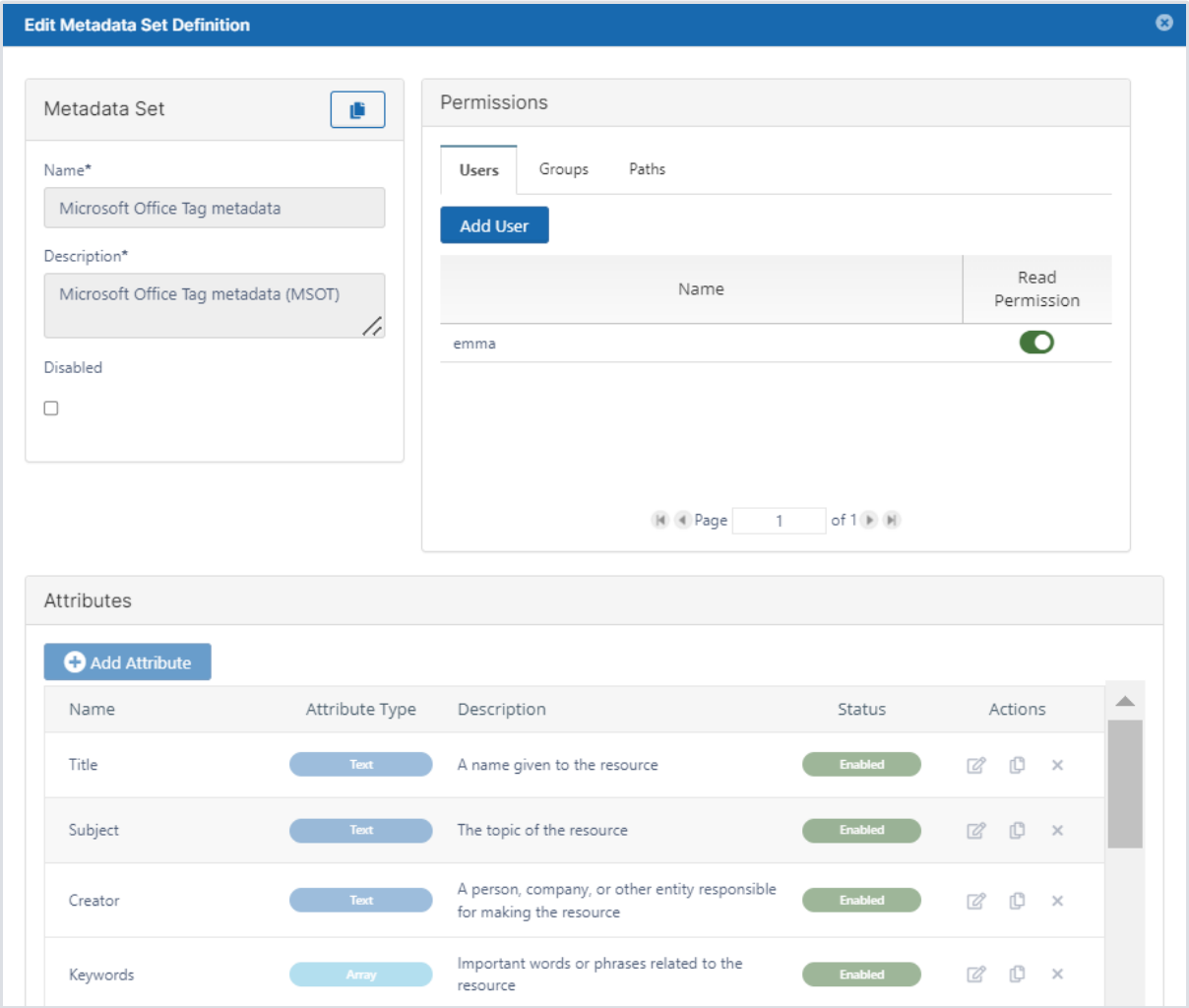
	Description	Options
Name	Title for the metadata set: Document Life Cycle Metadata	• Required • This cannot be changed
Description	By default, says: Stores information regarding document life cycle	• Required • This cannot be changed
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	• Not selected • This cannot be changed

	Description	Options
User Permissions	Grant access to specific users to: • Read: this permission displays the metadata to the user in the User Portal For more information, read Managing Metadata Permissions	• Not Required • Read
Group Permissions	Grant access to specific groups to: • Read: this permission displays the metadata to the user in the User Portal For more information, read Managing Metadata Permissions	• Not Required • Read
Path Permissions	File Objects in this location will have the metadata set applied	• Not available • This cannot be changed
Attributes	A number of custom values (tags) extracted from the file. One of these attributes is a SHA256 Fingerprint (file checksum). • This is a unique text string generated by the SHA-1 hash algorithm. • It is a standard for the implementation of a secure hash algorithm. • It is a one-way cryptographic function that can be used to act as a 'signature' of a sequence of bytes. • It is very unlikely that 2 different byte sequences would produce the same value (though not impossible)	• Creation Date • Last Access • Last Modification • Check Sum: File SHA256 Fingerprint

Microsoft Ofiice Tag metadata

Microsoft Office Tag metadata enables the system to apply FileCloud tags that match existing tags in MS Office documents (.docx, .xlsx and .pptx files) when they were uploaded to FileCloud.

Note: FileCloud does not apply **Microsoft Office Tag** metadata for Azure/S3 Network Folders.



The following attributes are included in FileCloud's **Microsoft Office Tag** metadata set:

	Description	Options
Title	Name of file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Subject	Topic of file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Creator	User who created file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)

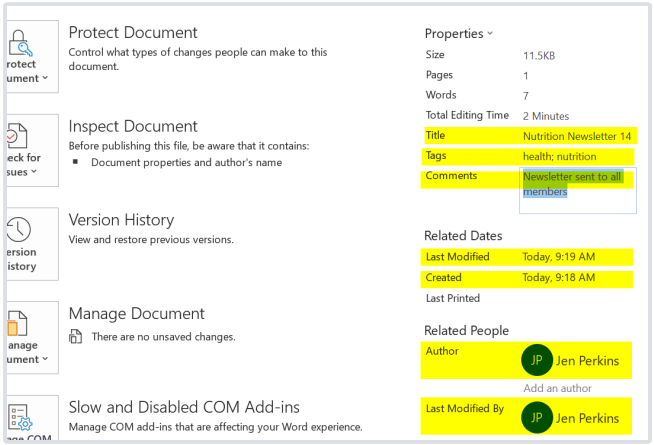
	Description	Options
Keywords	Keyword tags assigned to file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Description	Description of file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Last Modified By	Last user who modified file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Created	Date file was created.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Modified	Date file was last modified.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Category	Category of file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Sensitivity Labels	Sensitivity level of data in file, such as **Public** or **Confidential**.	• Not required • Read (can only be changed in Microsoft Office file before uploading) ***Note: You can only view and capture sensitivity labels if you have enabled them in Office. They are disabled by default. Please see the following note regarding them.***

MSOT Sensitivity Labels
By default, FileCloud does not capture MSOT sensitivity label data even if sensitivity labels are enabled in Office.
Prior to FileCloud 21.2, enabling the Sensitivity Label field was the only way to extract sensitivity label data. In FileCloud 21.2, AIP Sensitivity Label metadata, which captures more details and applies to more file types was added to replace this method; however, the MSOT sensitivity label is still available for backwards compatibility.

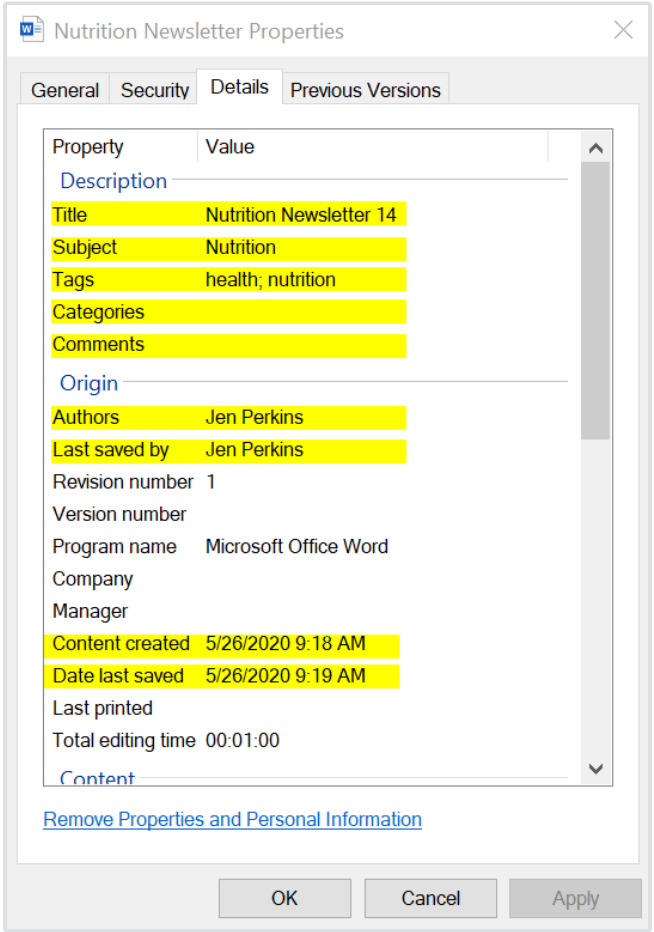
To enable FileCloud to capture MSOT sensitivity label data and to display the **Sensitivity Label** field in the **Metadata** panel, please contact FileCloud Support.

There are several ways in MS Office that you can view, add, and modify the properties:

From within an Office document by clicking **Properties** in the toolbar:

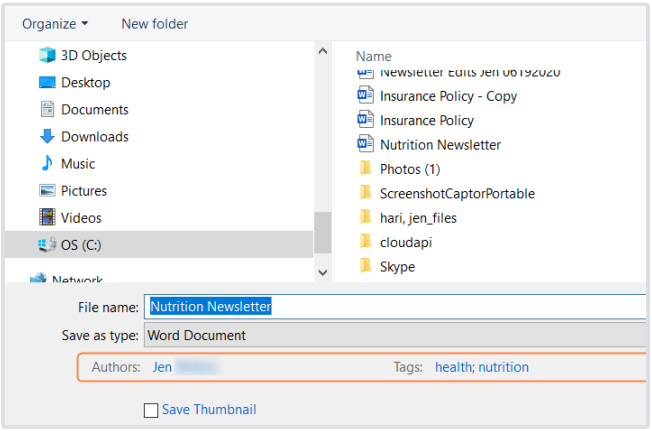


When you right-click an Office document in file explorer and select Properties > Details tab:



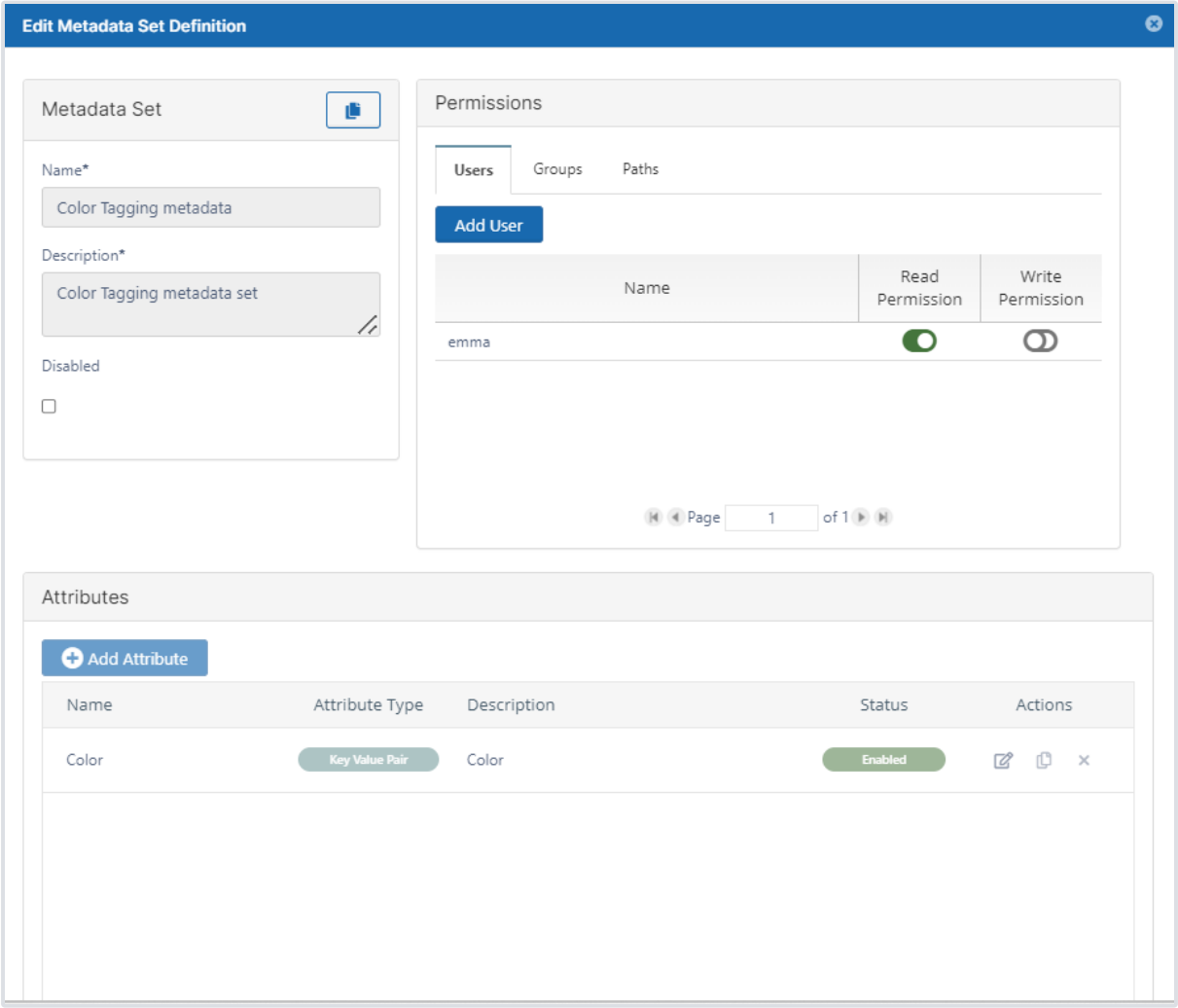
Or when you save an Office document:

Microsoft Office property	Corresponding FileCloud metadata attribute
Title	Title
Subject	Subject
Tags	Keywords
Categories	Category
Comments	Description
Author	Creator
Last saved by/Last modified by	Last modified by
Content created/Created	Created
Date last saved/Last modified	Modified
Sensitivity	Sensitivity Label



Color Tagging Metadata

The **Color Tagging** metadata set enables you to apply color tags to files and folders. It includes a single **Color** attribute that has six default values: **Red**, **Yellow**, **Green**, **Aqua**, **Blue**, and **Purple**. Admins can add other color values to the attribute.



Color is the only attribute included in the **Color Tagging** metadata set.

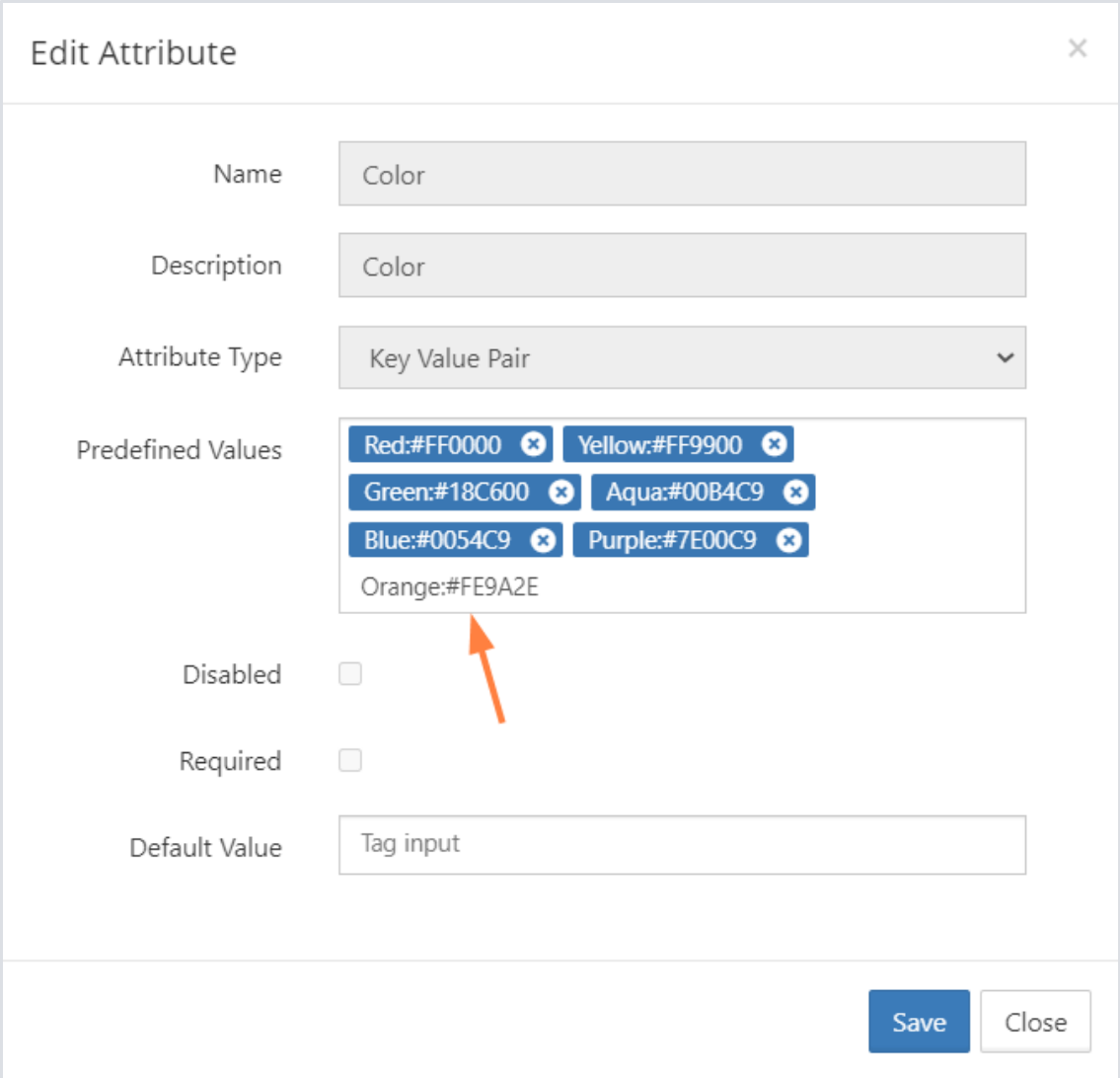
Name	Description	Options
Color	An array of color tags in the format **Color:Hexadecimal value**	• Not required • Color tags can be added and deleted.

Color values are added to the **Color** attribute with the name of the color and its hexadecimal value. To find hexadecimal codes for colors, see https://html-color-codes.info/.

To add values to the Color attribute:

1. To open the **Edit Metadata Set Definition** dialog box, click the Edit button for Color Tagging metadata.
2. Under **Attributes**, click the Edit button for **Color**.
   The **Edit Attribute** dialog box opens.

3. Click in the **Predefined Values** box, and type the name of a color followed by **:#** and then the hexadecimal color code.



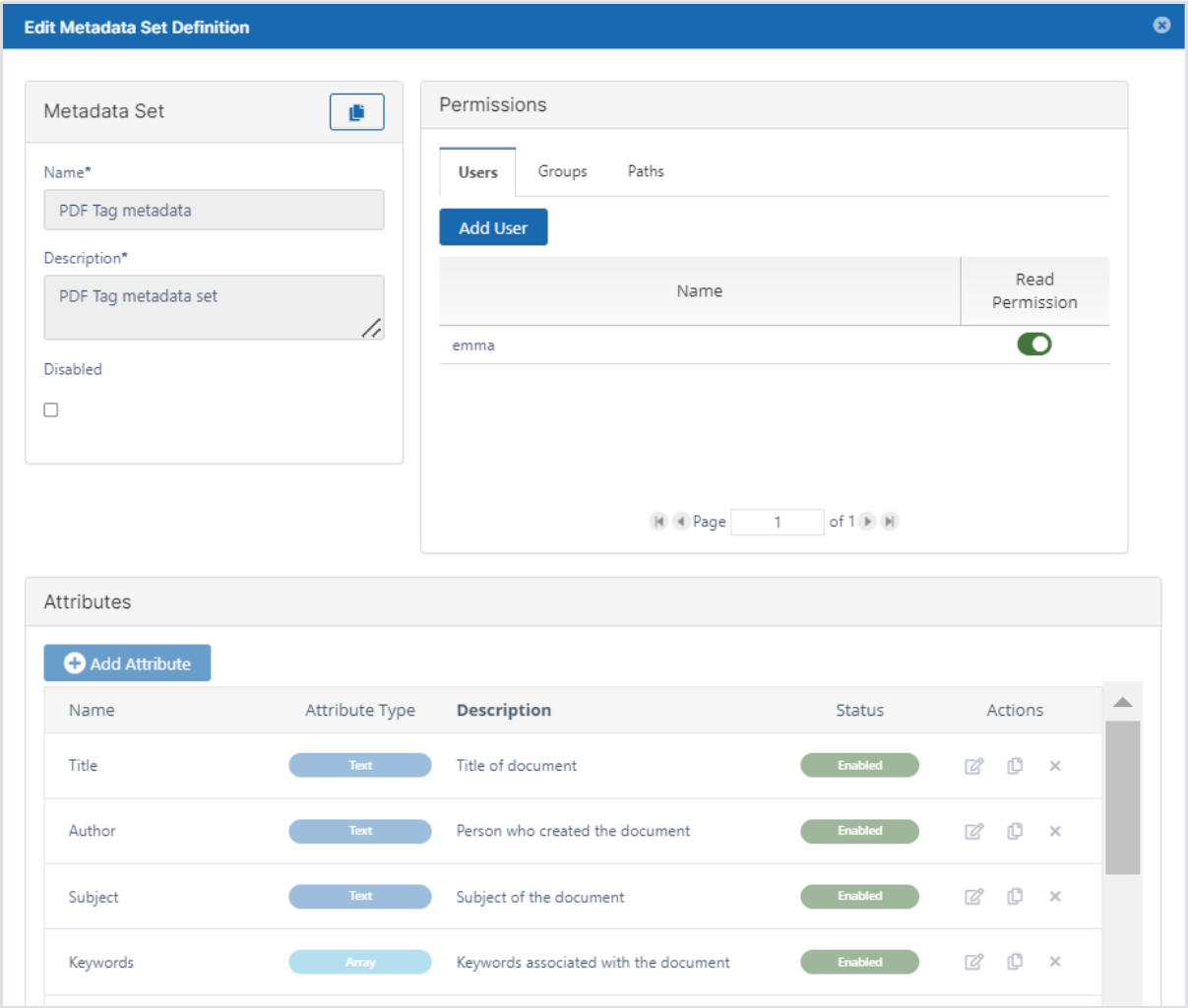
4. Click Enter.
   The color is saved and formatted with white letters on a blue background.
5. Add any number of custom colors and click **Save**.
   The colors now appear as options to users when they apply color tags to files or folders.

For information on applying color tags to files, see Color Tag Metadata.

Beginning with FileCloud 21.1, the Smart Classification can apply color tag values to files.
Note: Although users can search on color metadata in both the new and classic user interfaces, they can only apply color tags to files and folders in the new interface.

PDF Tag metadata

The **PDF Tag** metadata set enables FileCloud to apply FileCloud tags that match default and custom tags in PDF files when they are uploaded.



The following attributes are included by default in FileCloud's **PDF Tag** metadata set:

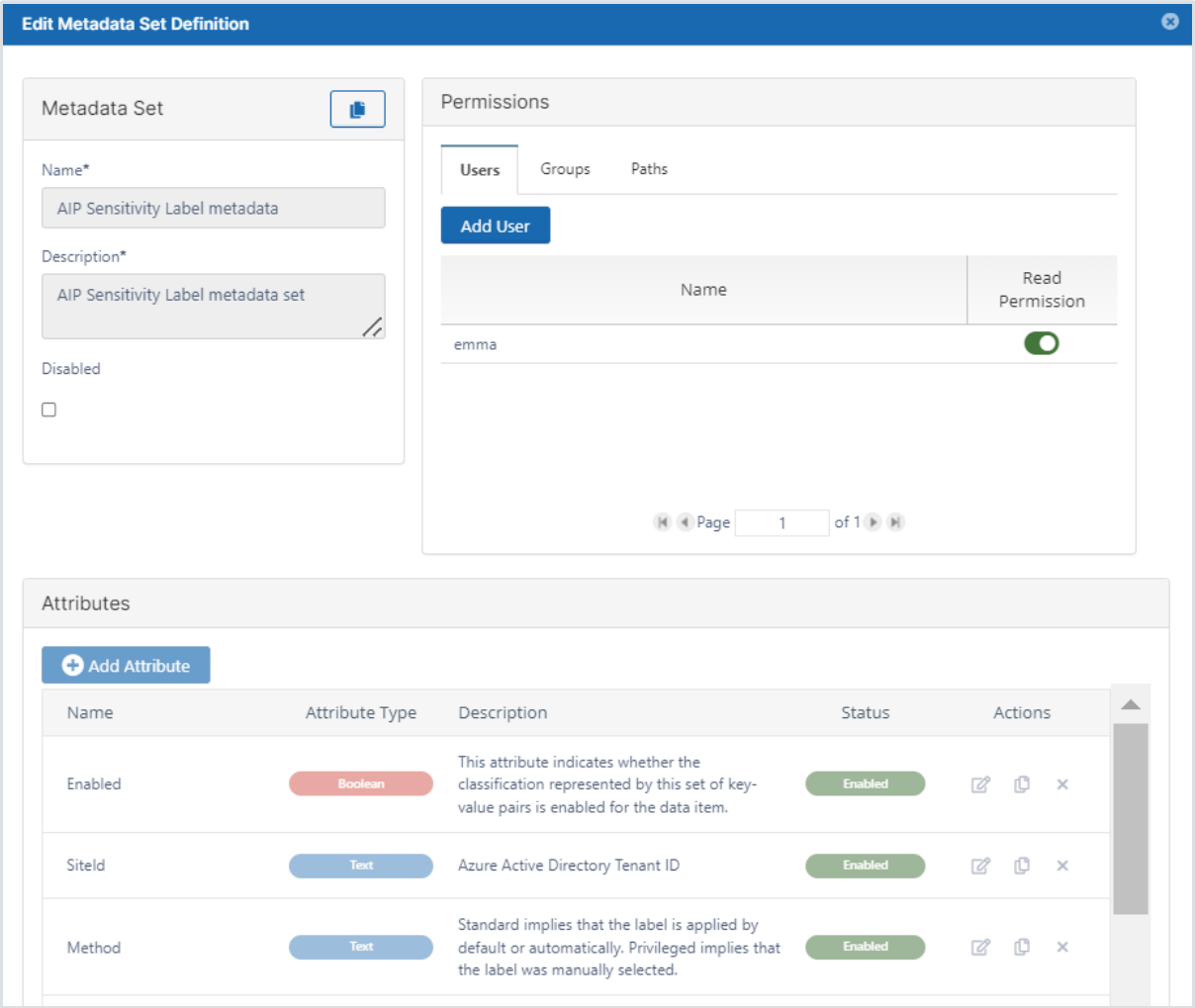
	Description	**Options**
Title	Title of document.	Read only
Author	Author of document	Read only
Subject	Subject of document.	Read only
Keywords	Keywords associated with document.	Read only
Creator	Application used to create file before it was converted to PDF.	Read only

Producer	Application used to convert this file to PDF.	Read only
Created	Date created.	Read only
Modified	Date last modified.	Read only

AIP Sensitivity Label metadata

Note: **AIP Sensitivity Label** metadata was added in FileCloud Version 21.2 and currently applies only to Microsoft Office Word, Excel, and PowerPoint files. In the future, it will be applied to additional file types.

AIP Sensitivity Label metadata stores sensitivity label information applied to files using Azure Information Protection when the files are uploaded to FileCloud.



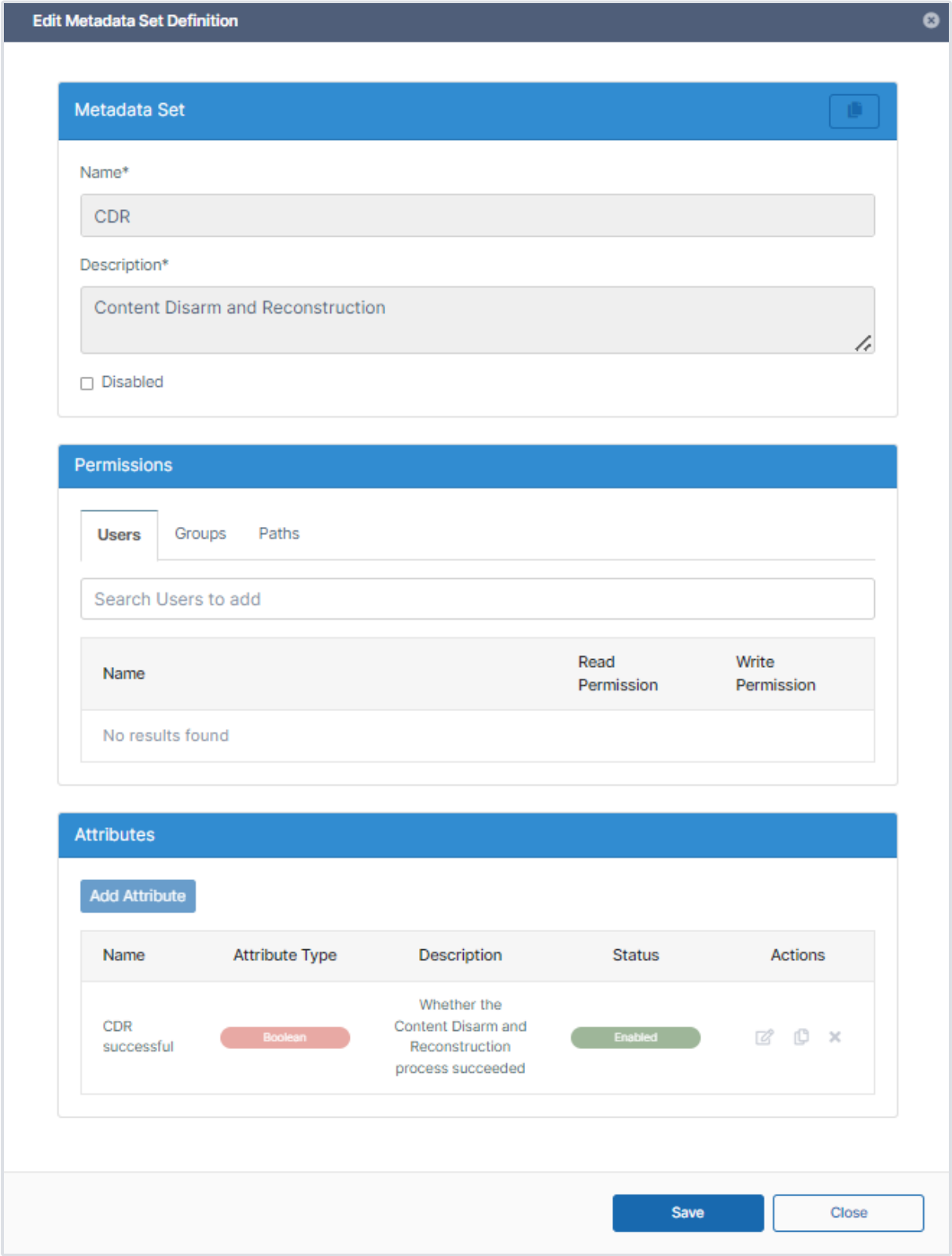
The following attributes are included in FileCloud's **AIP Sensitivity Label** metadata set:

	Description	Options
Enabled	Whether the sensitivity label is enabled for this item.	Read only
SiteID	Azure Active Directory tenant ID.	Read only
Method	Indicates whether label was applied by default/automatically or if the label was applied manually. Value may be: **Standard** - Label was applied by default or automatically. **Privileged** - Label was applied manually.	Read only
SetDate	Timestamp when label was set.	Read only
Name	Unique label name (may differ from display name).	Read only
ContentBits	Bitmask that describes the types of visual marking that should be applied to the file to identify the sensitivity category. See https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-markings for more information.	Read only

CDR metadata

Note: **CDR** metadata was added in FileCloud Version 23.241.4

CDR metadata stores a Boolean attribute that indicates whether or not CDR was successful.



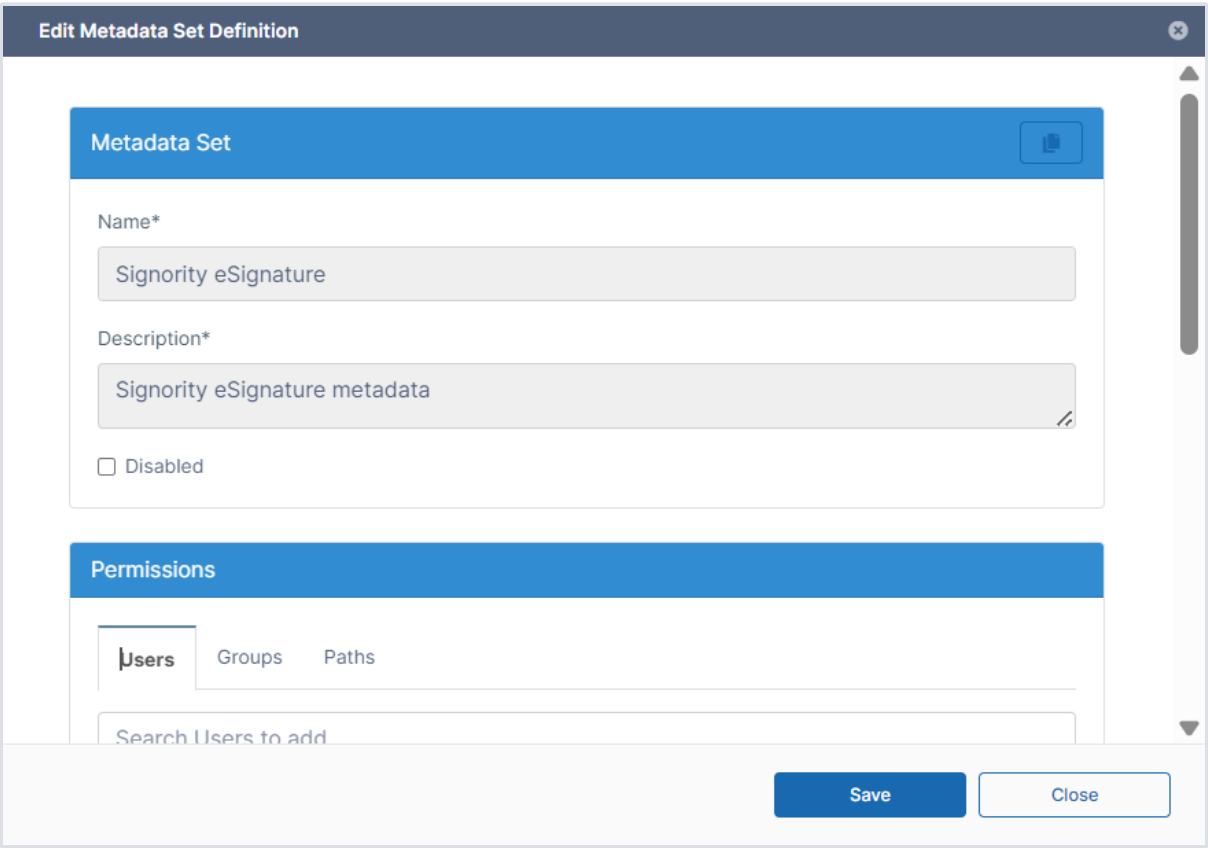
The following attribute is included in FileCloud's **CDR** metadata set:

	Description	Options
CDR successful	Whether content disarm and reconstruction was successful for this file.	Read only

Signority eSignature metadata

Note: **Signority eSignature** metadata was added in FileCloud Version 23.241.4.

Signority eSignature metadata stores information about eSignatures applied to the file.



The following attributes are included in FileCloud's **AIP Sensitivity Label** metadata set:

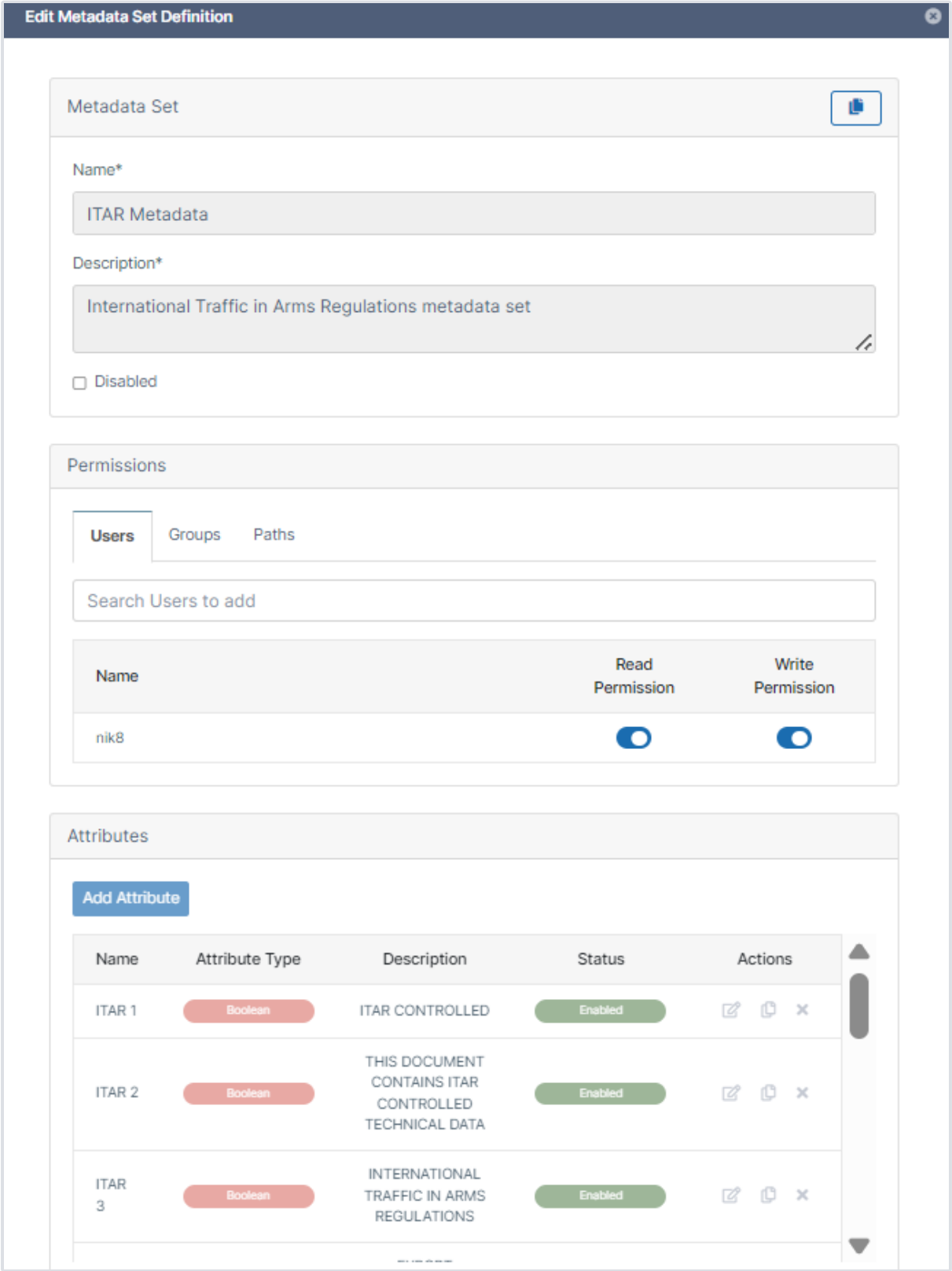
	Description	Options
Completion Date	Date signing was completed.	Read only

	Description	Options
Total Signers	Total number of people who received signing requests.	Read only
Total Rejections	Total number of signers who rejected the document.	Read only
Digital Signature	Whether the signature is a digital signature.	Read only
Signing Request ID	ID of the request to begin the eSignature process.	Read only

ITAR metadata

Note: **ITAR** metadata was added in FileCloud Version 23.252

ITAR (International Traffic in Arms Regulations) metadata enables you to identify the presence of phrases indicating that a file contains ITAR information. This enables you to apply an appropriate rule or workflow to the file.



The following attributes are included in FileCloud's **ITAR** metadata set.

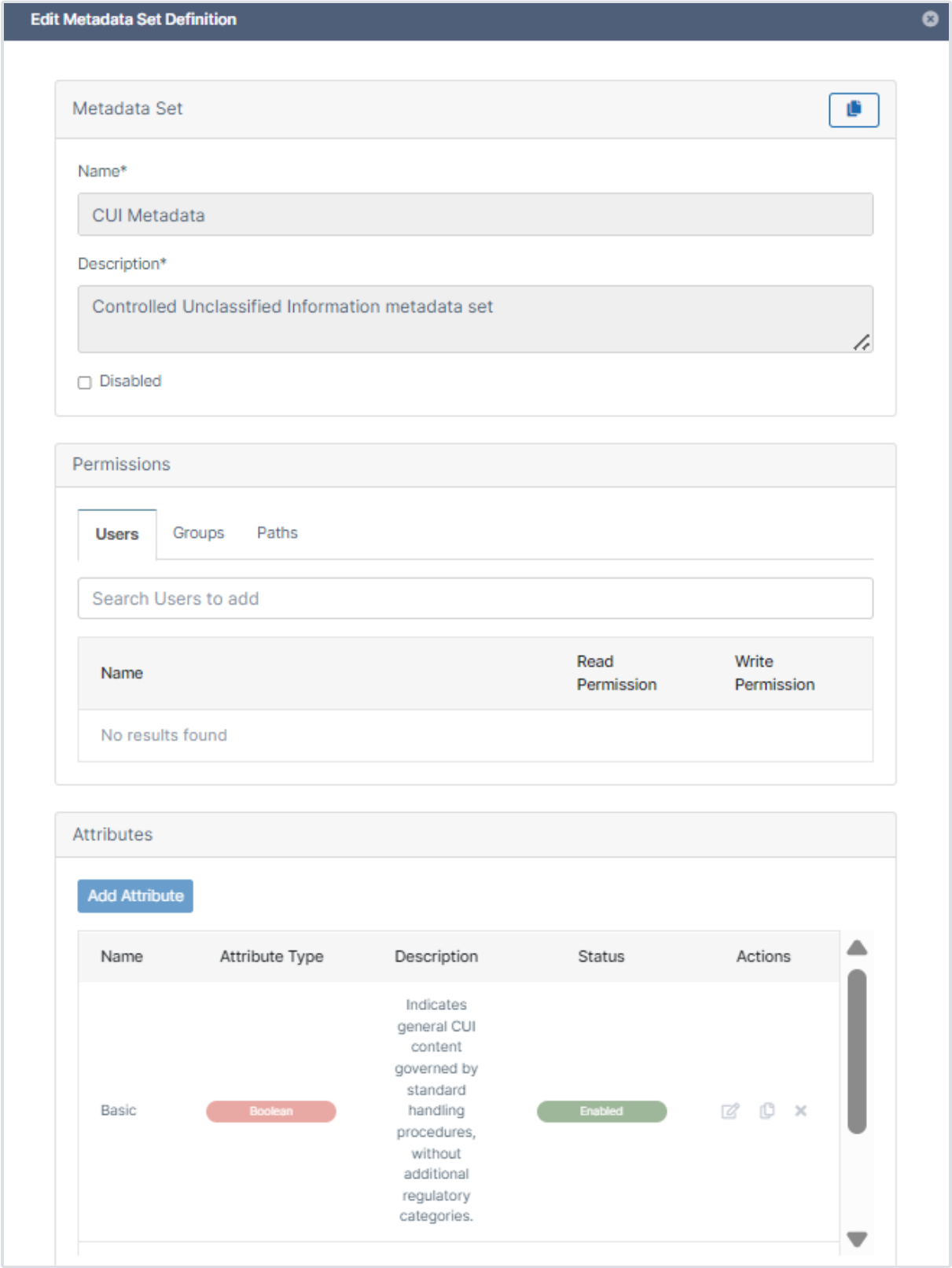
Note that the descriptions are phrases that commonly appear in ITAR documents. If other phrases are used in your ITAR documents, search for those phrases.

	Description	Options
ITAR 1	ITAR CONTROLLED	Read only
ITAR 2	THIS DOCUMENT CONTAINS ITAR CONTROLLED TECHNICAL DATA	Read only
ITAR 3	INTERNATIONAL TRAFFIC IN ARMS REGULATIONS	Read only
ITAR 4	EXPORT CONTROLLED INFORMATION	Read only
ITAR 5	EXPORT CONTROLLED	Read only
ITAR 6	SUBJECT TO ITAR	Read only
ITAR 7	SUBJECT TO THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS	Read only
ITAR 8	U.S. MUNITIONS LIST	Read only
ITAR 9	TECHNICAL DATA AS DEFINED IN ITAR	Read only
ITAR 10	DEFENSE ARTICLE	Read only
ITAR 11	DDTC EXPORT AUTHORIZATION	Read only
ITAR 12	AUTHORIZED EXPORT ONLY	Read only
ITAR 13	NOT FOR PUBLIC RELEASE	Read only
ITAR 14	NO FOREIGN NATIONALS	Read only
ITAR 15	DISTRIBUTION STATEMENT	Read only

CUI metadata

Note: CUI metadata was added in FileCloud Version 23.252

CUI (controlled unclassified information) metadata enables you to identify the presence of phrases indicating that a file contains CUI information. This enables you to apply an appropriate rule or workflow to the file.



The following attributes are included in FileCloud's **CUI** metadata set:

	Description	Options
Basic	Indicates general CUI content governed by standard handling procedures, without additional regulatory categories.	Read only
Specified	Identifies CUI content tied to specific legal or regulatory requirements, marked with SP- designations.	Read only

Extended metadata

> Extended metadata enables you to work with custom tags have been applied to PDF or Microsoft Office files by a third-party application that is exporting them, such as Forcepoint CDR.

How metadata attributes are added

Extended metadata contains custom metadata attributes that can be added in two ways:

- Manually created by admins in the Extended metadata set.
- Automatically extracted from uploaded PDF and Microsoft Office files when automatic extraction is enabled.

Metadata attributes are extracted and added to the Extended metadata set if they match regex filters that you have supplied.
Manually created attributes are always available in the Extended metadata set, and if a manually created attribute matches a tag in the file, it is applied to the uploaded file.

Setting an auto extraction limit

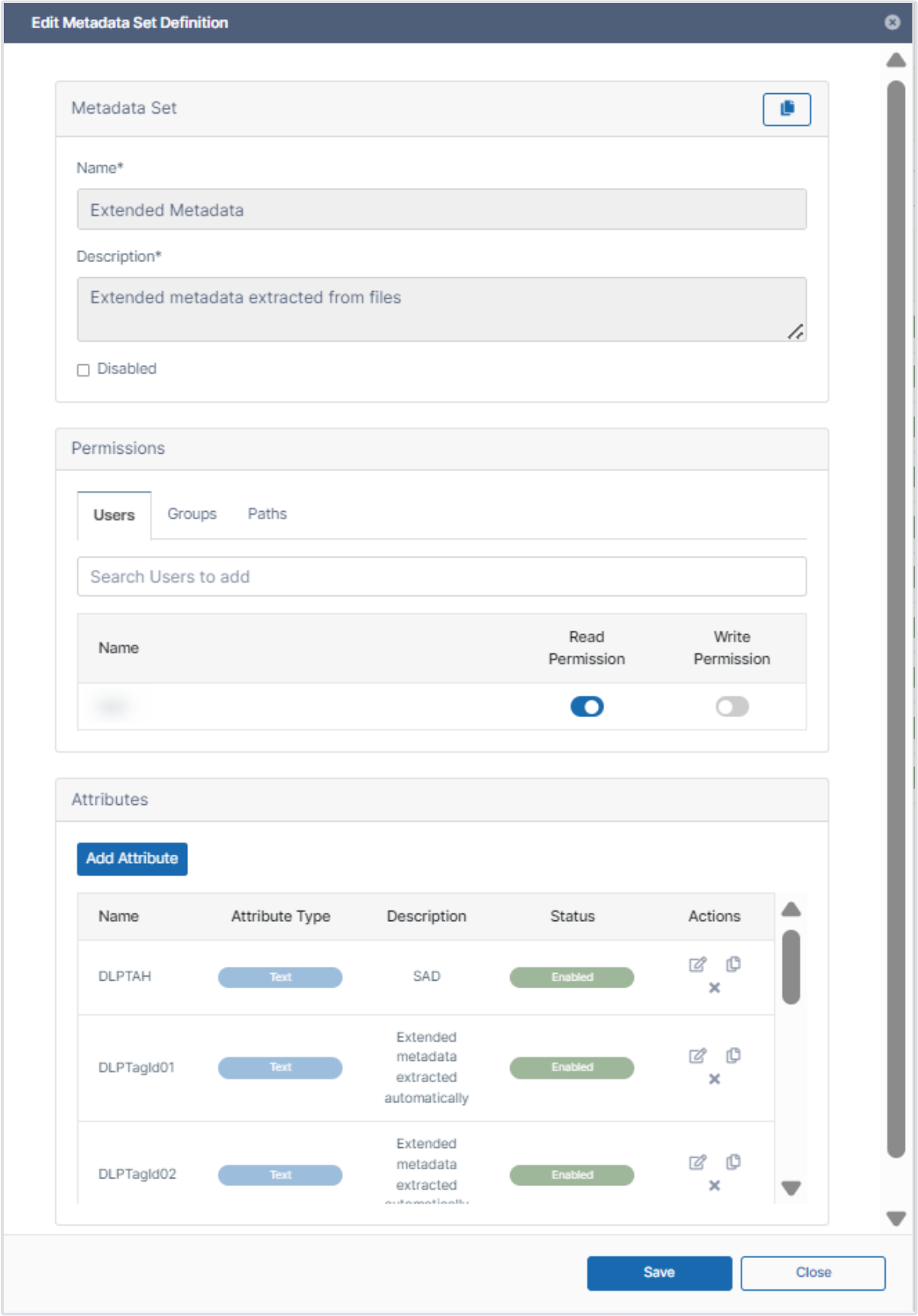
You set a limit that determines how much metadata can be automatically extracted. The limit depends on the amount of metadata already manually created, as explained in the procedure below. The limit prevents an excessive number of metadata attributes matching the regex filter and being added unintentionally.

Why full set of attributes are not added to every file

Note that when other FileCloud metadata is applied to files, all of its metadata attributes are added to each file whether or not each attribute is given a value. Extended metadata differs in that the full set of attributes may not be added to every file. Only those attributes that already exist in the uploaded files are applied. This prevents extraneous attributes and excessive numbers of attributes being applied to files.

Example

In the following example, the attribute DLPTAH was added manually, and the DLPTagId01 and DLPTagId02 attributes were extracted automatically from uploaded files. When each file is uploaded the Extended metadata attributes it contains already are added to it from the Extended set. These attributes are given the values that exist for them on the uploaded file.

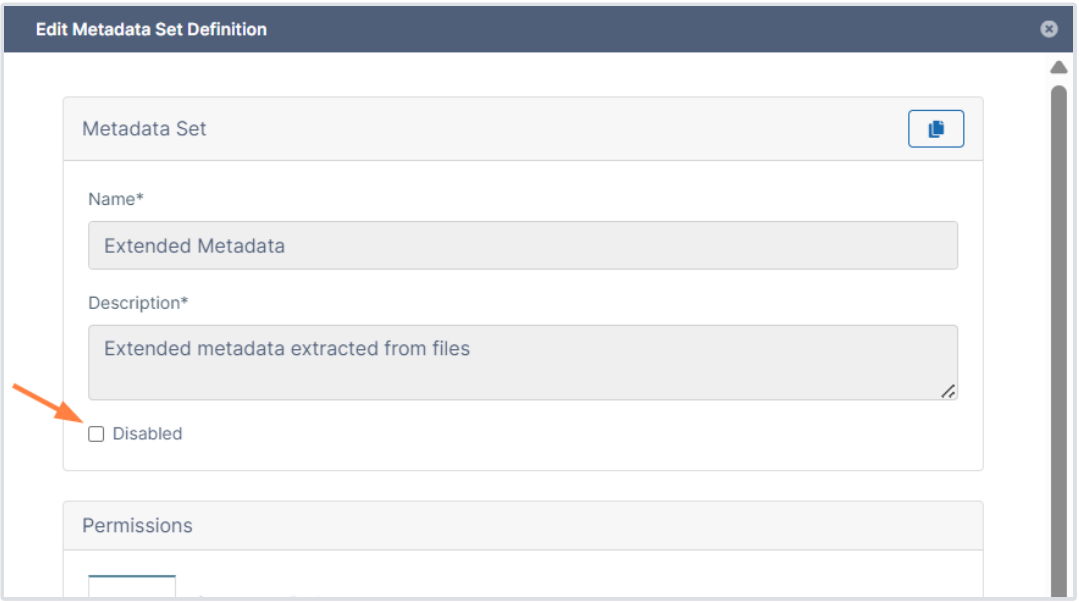

Edit Metadata Set Definition
Metadata Set
Name*
Extended Metadata
Description*
Extended metadata extracted from files
Disabled
Permissions
Users
Groups
Paths
Search Users to add
Name
Read Permission
Write Permission
Attributes
Add Attribute
Name
Attribute Type
Description
Status
Actions
DLPTAH
Text
SAD
Enabled
DLPTagId01
Text
Extended metadata extracted automatically
Enabled
DLPTagId02
Text
Extended metadata extracted
Enabled
Save
Close

⚠️ Files that were uploaded before Extended metadata was configured do not have it applied to them after it is created.

⚠️ After upload, files that are modified to include tags matching the Extended metadata attributes do not have those attributes applied to them.

To configure the Extended metadata set:

1. In the admin portal, in the navigation pane, click **Metadata** to go to the Manage Metadata Sets page.
   The Extended metadata set is disabled by default and must be opened for edit to manually enable it.
2. Enable Extended metadata:
   a. In the **Extended Metadata** row, click the Edit icon.
      The **Edit Metadata Set Definition** dialog box opens.
   b. Uncheck **Disabled**.



3. Manually add any attributes to the Extended metadata set. If they match any tags in uploaded PDF and Office files, they are added to the files.
4. Add the two required settings to the cloudconfig.php file:
   a. Open cloudconfig.php:
      Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
      Linux Location: /var/www/config/cloudconfig.php
   b. To enable automatic extraction and add the regular expression filter, set TONIDOCLOUD_METADATA_AUTO_TAG_REGEX to a regular expression matching the attributes you want to extract.
      For example, to extract the attributes **Sensitive** and **Restricted** from the first uploaded files containing them, add:

```
define('TONIDOCLOUD_METADATA_AUTO_TAG_REGEX', 'Sensitive|Restricted');
```

Or to extract attributes that begin with the word **Custom** followed by an uppercase letter, add:

```
define('TONIDOCLOUD_METADATA_AUTO_TAG_REGEX', '/^Custom[A-Z]/');
```

c. To add the per file extraction limit for automatically extracted tags, set TONIDOCLOUD_METADATA_AUTO_TAG_LIMIT to the limit value.
About the limit:
   - It applies to the number of automatically extracted attributes, but manually added attributes are added to the extraction limit.
   - It does not apply to manually added attributes. In other words, once the limit is reached, additional automatically extracted attributes are not added, but manually added attributes can continue to be added.
   - Example: If this limit is 10 and 3 attributes have been created manually, only 7 more can be auto-created. However, additional attributes can be added manually.
   - By default, its value is 10.

     To limit the number of attributes (automatically extracted + manually added) to 15, add the following to the cloudconfig.php file:

```
define('TONIDOCLOUD_METADATA_AUTO_TAG_LIMIT', 15);
```

Note: The Extended metadata set only accepts attributes of type text.

Now your Extended metadata is configured, and as PDF and Office files are uploaded they will be checked for the matching regex strings. If there is a matching string, it is extracted and an Extended metadata attribute is created. In addition, the metadata attribute is assigned to the file with the value it contained in the file.

Once the number of attributes in the limit is reached:

- If an uploaded file has a matching string that does not have a corresponding Extended metadata attribute, an attribute is not automatically created and is not added to the file.
- If an uploaded file has a matching string that has a corresponding Extended metadata attribute, the attribute is added to the file and given the value originally contained in the file.

Working with Custom Metadata

FileCloud allows you to create fully customizable sets of metadata, defined by the administrator.

Managing Metadata Sets

Create a new Set Definition

Manage Metadata Permissions

Edit an existing Set Definition

Delete a Set Definition

⚠️ The **Default** metadata Set cannot be removed.

⚠️ You cannot undo or revert deletions.

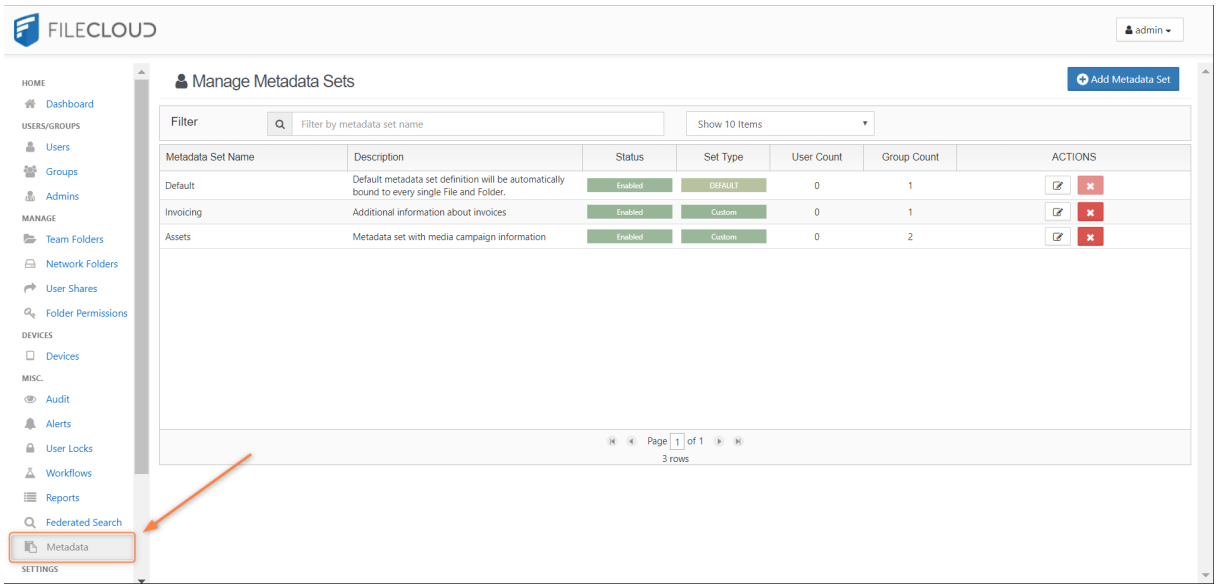
To delete an existing Custom metadata set definition:

1. Log in to the Admin Portal.
2. In the *Home* navigation panel on the left side, under *Misc.*, select *Metadata*.
3. In the *Manage Metadata Sets* section, select the one you want to grant access, and then click the delete icon .

View the Set Definition List

The metadata set definitions screen displays the list of defined metadata sets.

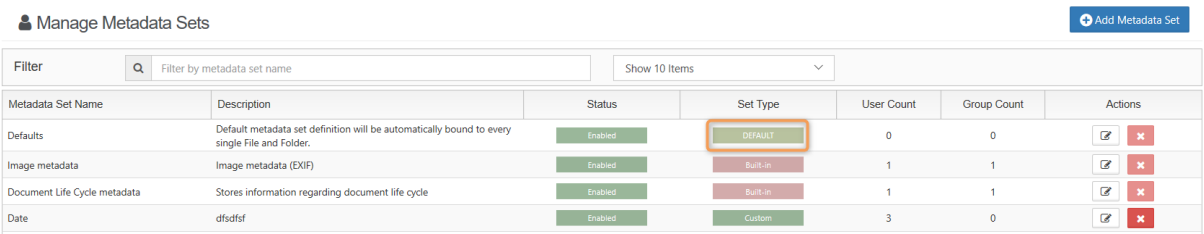
- The filter text box can be used to filter the metadata sets based on the metadata name.
- The individual metadata set on the metadata list can be viewed, edited and deleted.
- New metadata sets can be added by clicking the Add Metadata Set button and filling in the metadata set definition form.



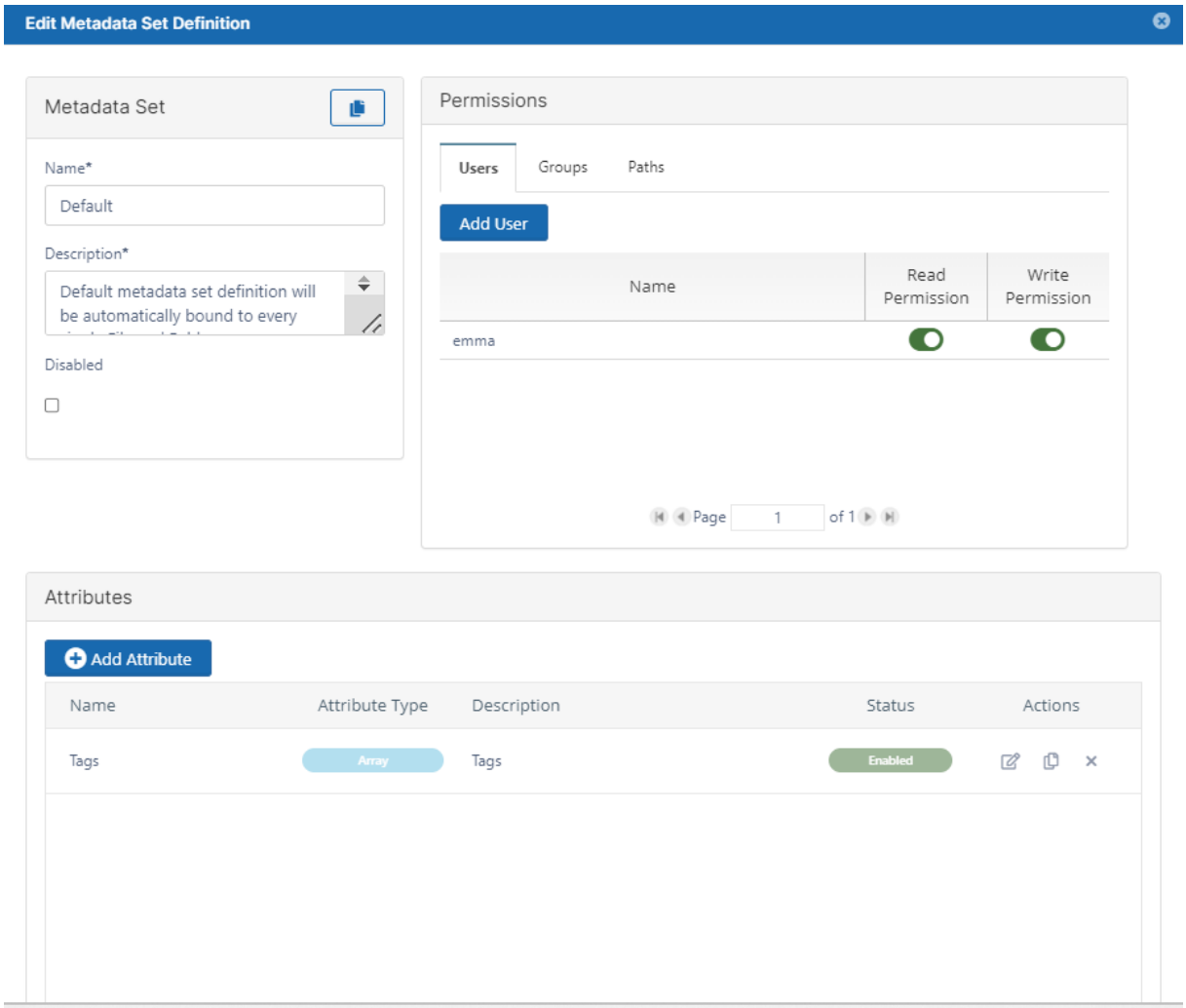
Working with Default Metadata

Default is a special metadata set that is automatically associated with every File Object when it is created, copied, uploaded, etc.

- For already existing File Objects it will be associated when the file or folder is accessed for the first time.
- Exactly one Default Set exists in FileCloud - it cannot be deleted, but administrators can customize attributes and permissions or disable it.
- Out of the box it is shipped with a single predefined attribute of Array type - Tags.



The following attributes can be edited in the DEFAULT metadata set:



	Description	Options
Name	Title for the metadata set.	• Required • This can be changed • Validated on Creation
Description	By default, says: Default metadata set definition will be automatically bound to every single File and Folder.	• Required • This can be changed • Validated on Creation
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	• By default this is not selected • You can choose to disable this set

	Description	Options
User Permissions	Grant access to specific users to: • Read: this permission displays the metadata to the user in the User Portal • Write: this permission allows the user to add, edit, copy, or paste a value For more information, read Managing Metadata Permissions	• Not Required • Read • Write
Group Permissions	Grant access to specific groups to: • Read: this permission displays the metadata to the user in the User Portal • Write: this permission allows the user to add, edit, copy, or paste a value For more information, read Managing Metadata Permissions	• Not Required • Read • Write
Path Permissions	File Objects in this location will have the metadata set applied For more information, read Managing Metadata Permissions	• Not Required
Array	A number of custom values (tags) provided by the administrator	• Name • Description • Disabled • Required • Tag Input
How To Edit a Metadata Set		

Finding files without metadata

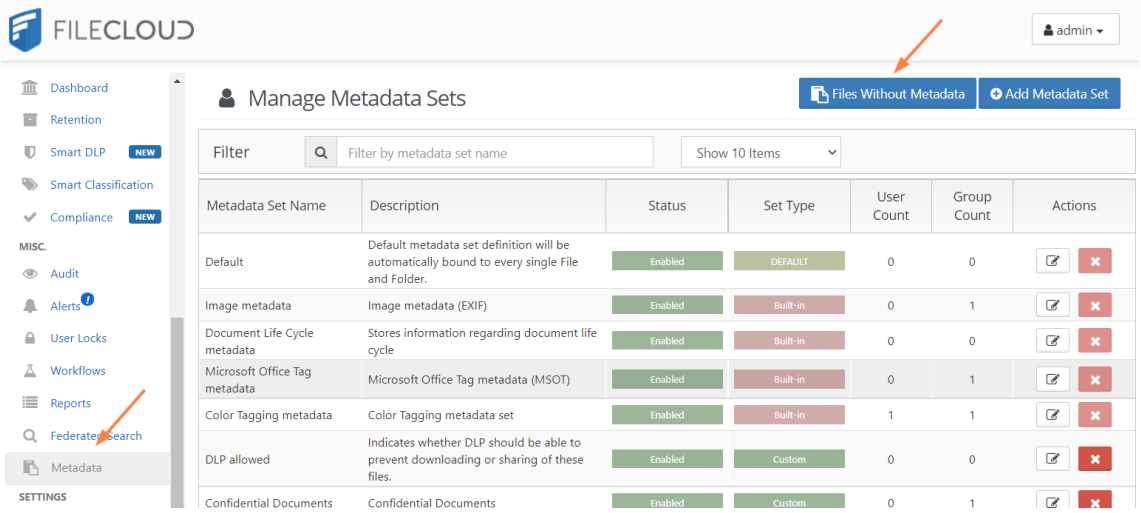
Smart Classification does not apply metadata to files over a specified size, but you can add metadata to those files manually. Beginning in FileCloud 20.1, you can configure your system to search for files without metadata.

Find files without metadata:

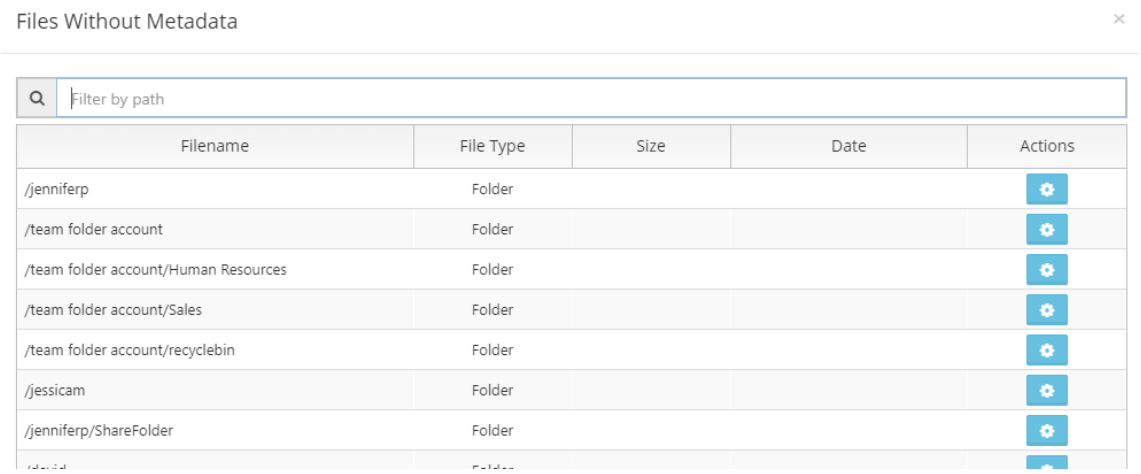
1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define('TONIDOCLOUD_SHOW_FILES_WITHOUT_METADATA', true);
```

3. In the navigation bar, click **Metadata**.
   Now the upper-right corner of the Manage Metadata Sets screen displays a **Files Without Metadata** button.

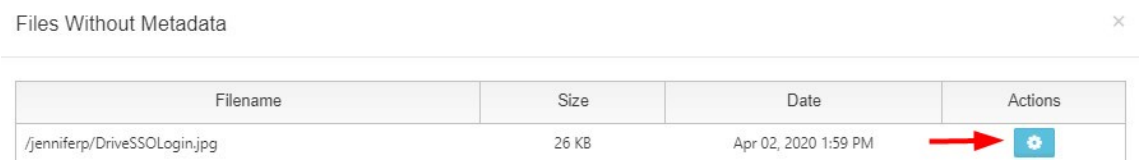


4. To display a list of files without metadata, click **Files Without Metadata**.

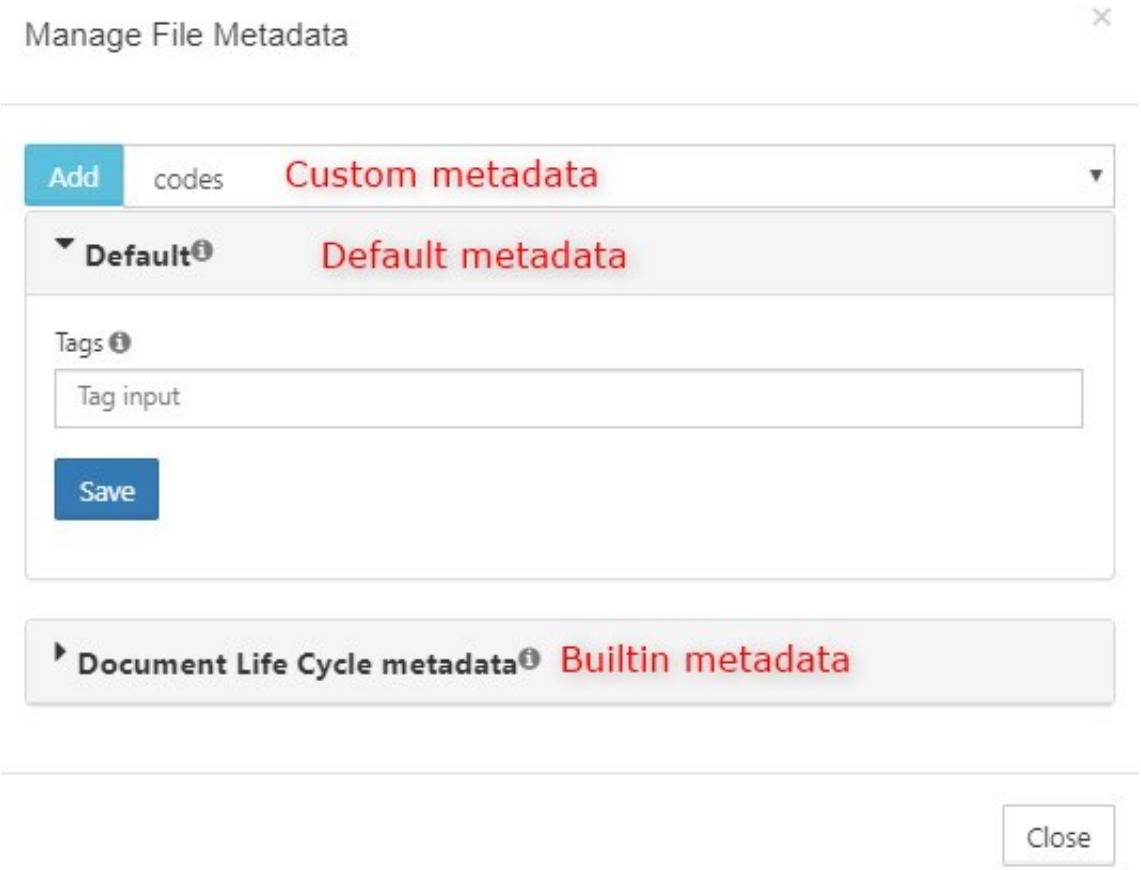


Add metadata from the Files Without Metadata list

1. Follow the procedure above to access your **Files Without Metadata** list.
2. Across from a file, click the button under **Actions**.

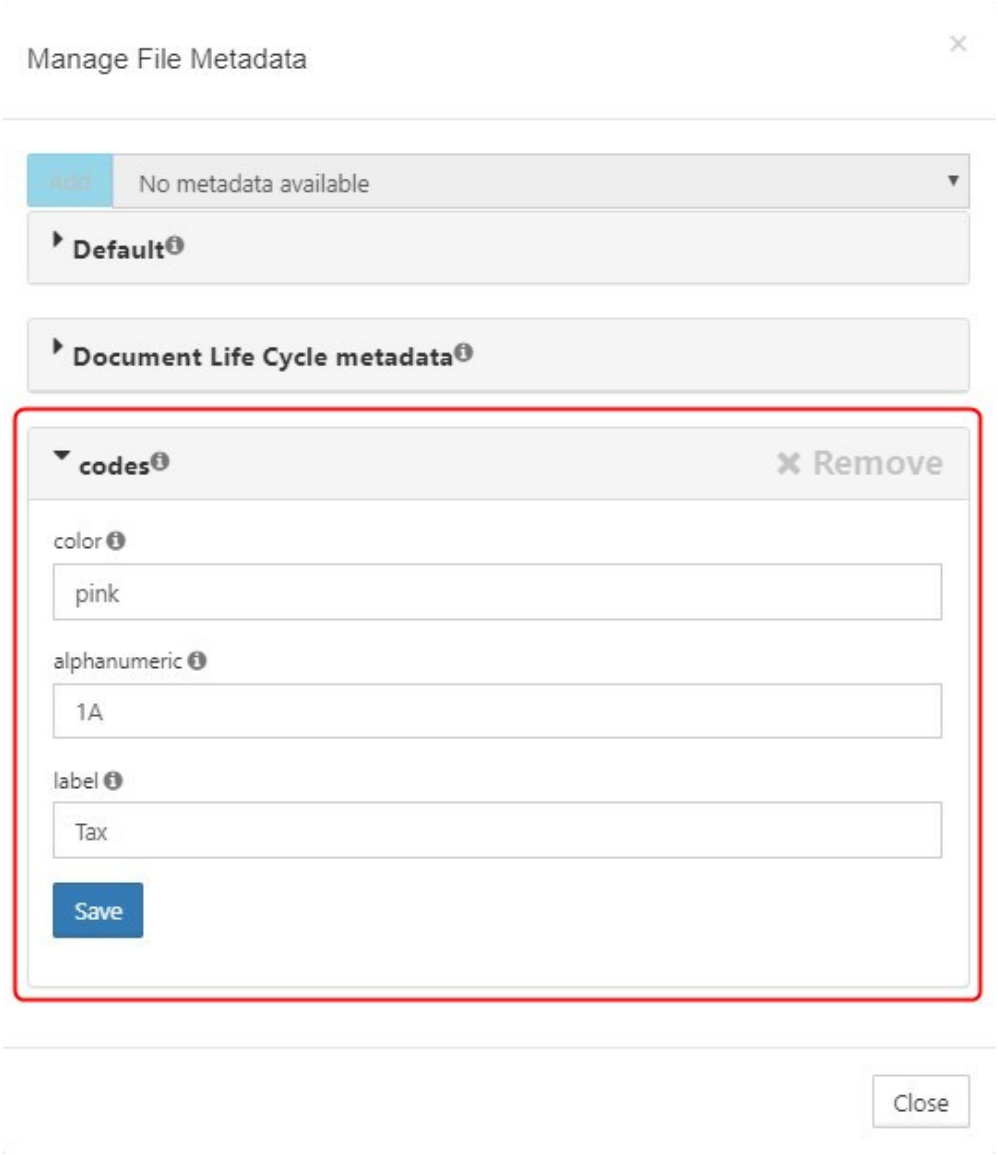


The Manage File Metadata window opens.

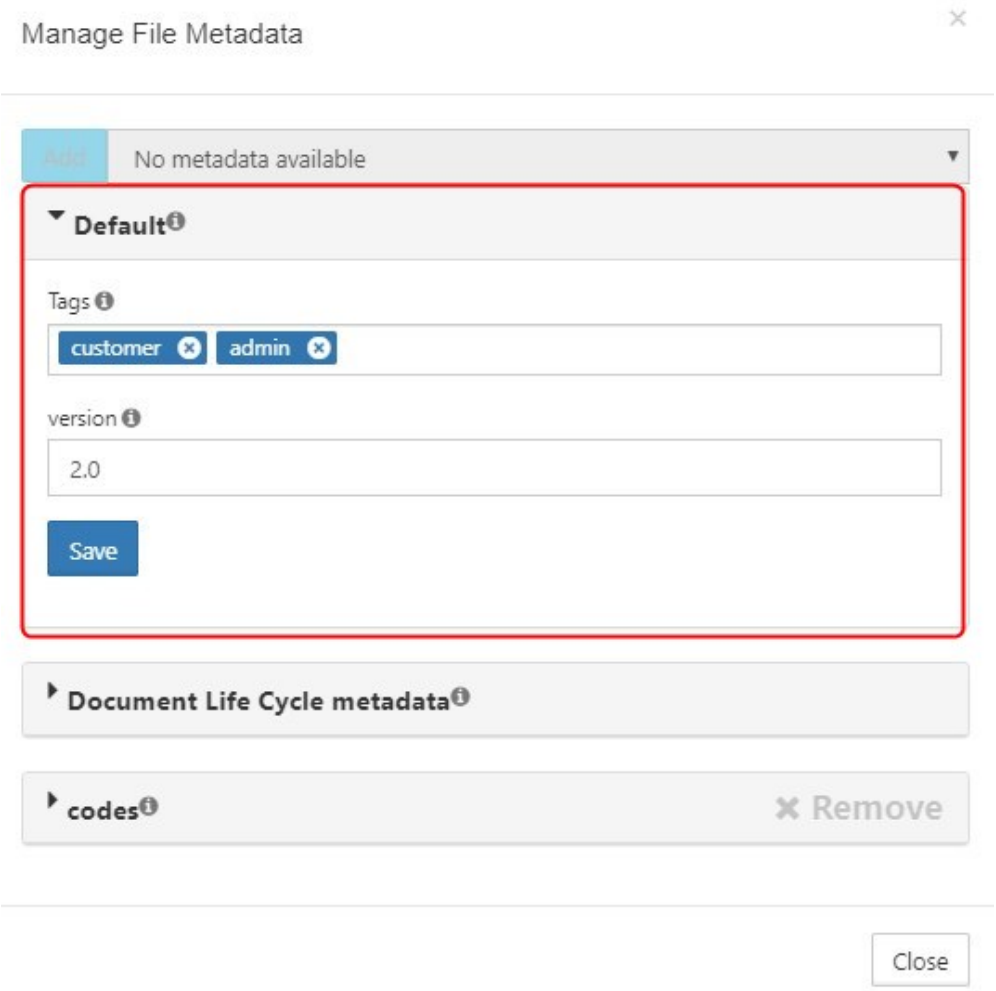


The top drop-down list holds custom metadata, the drop-down list below that holds default metadata, and any drop-down lists below that hold built-in metadata.

3. To add a custom metadata set, choose it in the drop-down list and click **Add**.
   It is added below the other metadata sets.
4. Add or change values in any of the metadata fields.



5. You can update the value of fields that appear in **t**he **Default** metadata set**.**. Expand the section, and add or change the values in the metadata fields, and click **Save**.



6. You can view, but not update the values in built-in metadata sets. Expand the sections to view the metadata and any values they have.

Metadata Limitations/Recommendations

Metadata feature	Recommended maximum
Metadata set name	128 characters
Metadata set description	128 characters
Attributes per metadata set	99

Metadata feature	Recommended maximum
Attribute name	128 characters
Attribute description	128 characters
Values per enum/array	99
Predefined value (enum)	128 characters
Default value	128 characters
Actual value	128 characters

Managing FileCloud Licenses

Your FileCloud license provides legally binding guidelines on your use and distribution of FileCloud.

In this section:

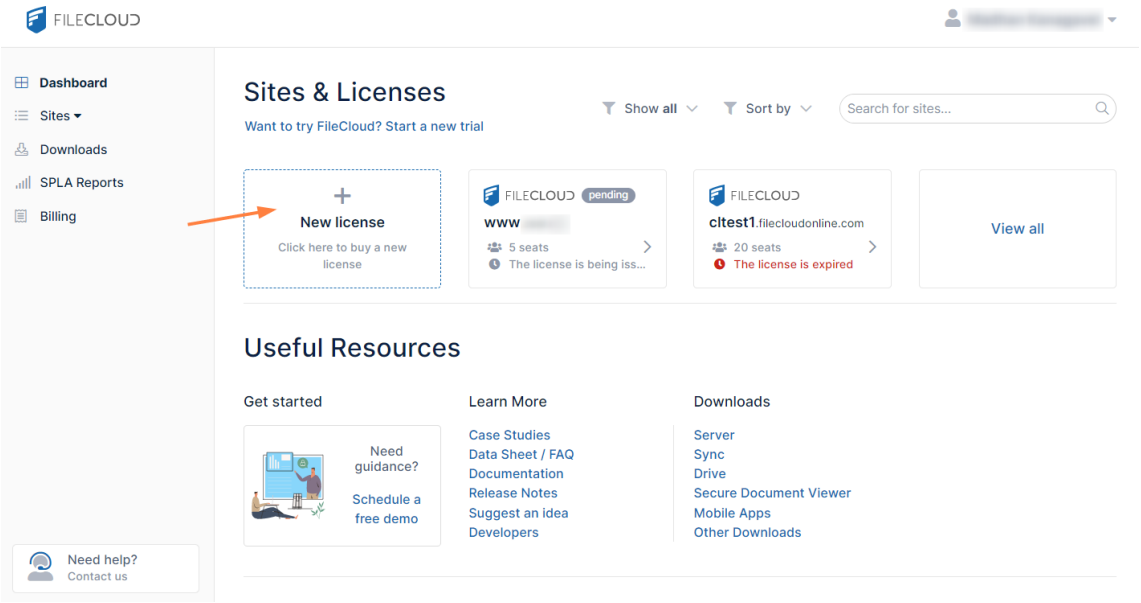
FileCloud - License Purchase And Renewal

Purchase a new license

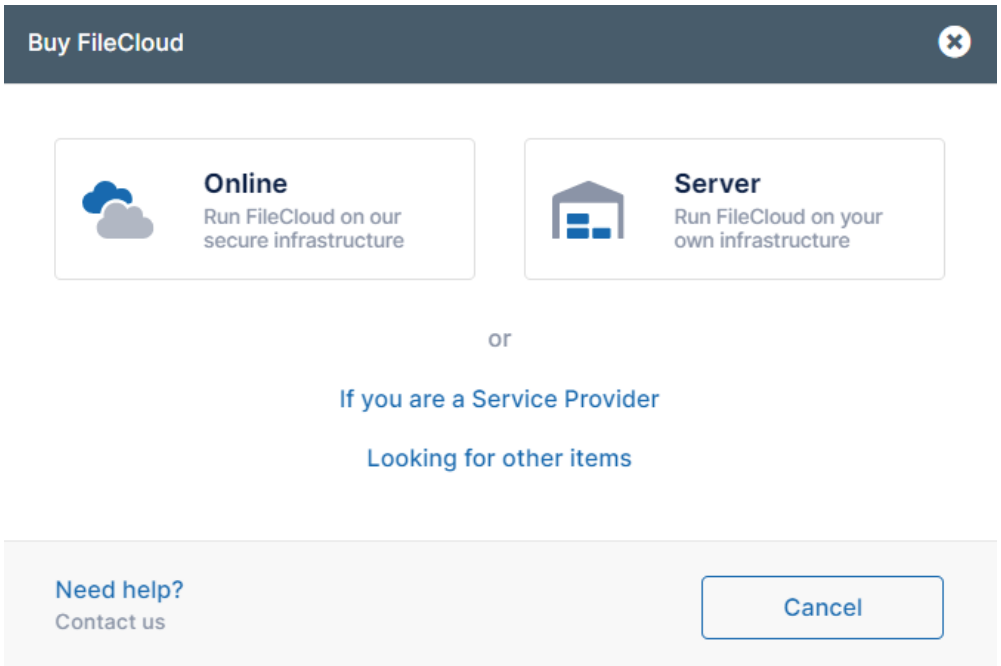
First

Choose a server or online license

1. Log into https://portal.getfilecloud.com
2. Click the **New license** icon.



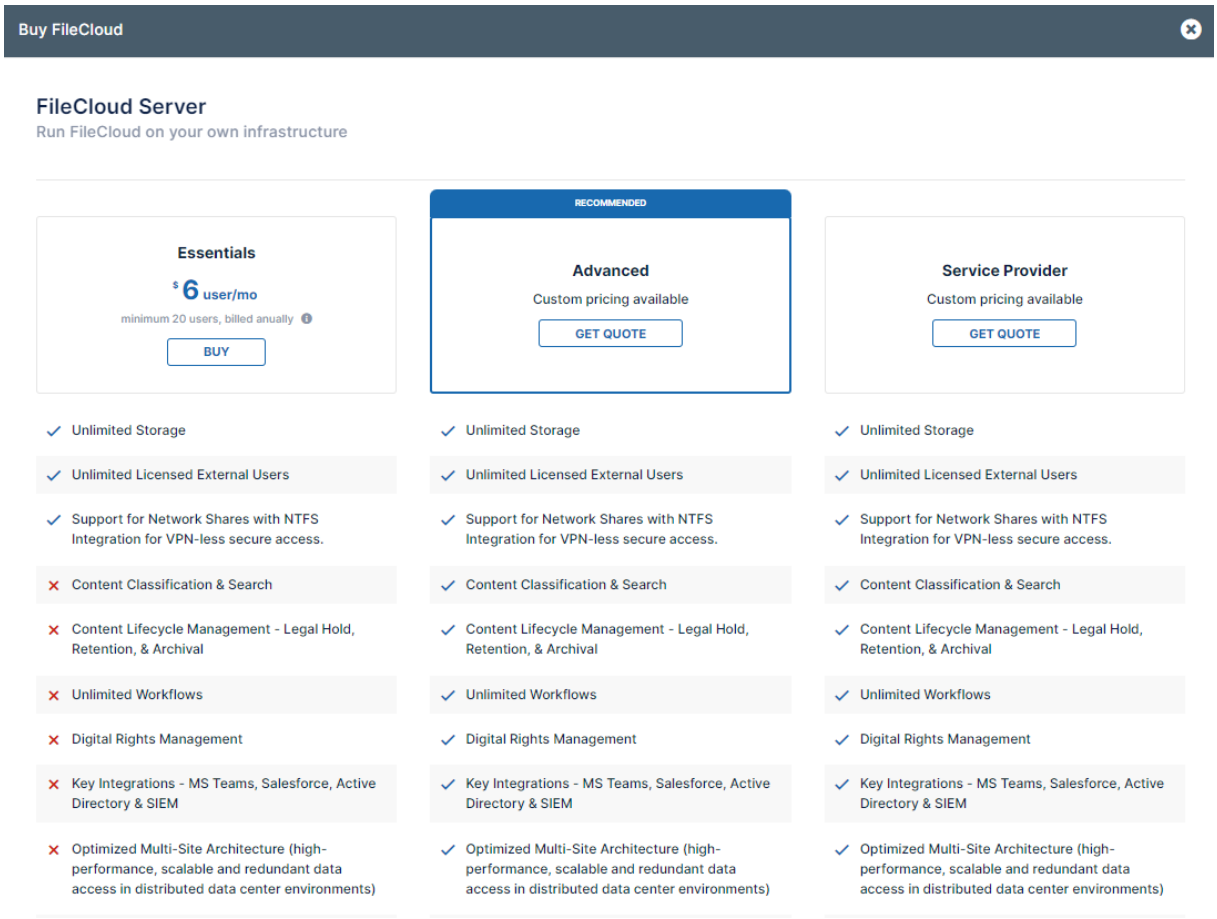
3. In the **Buy FileCloud** window, click **Online** or **Server**.



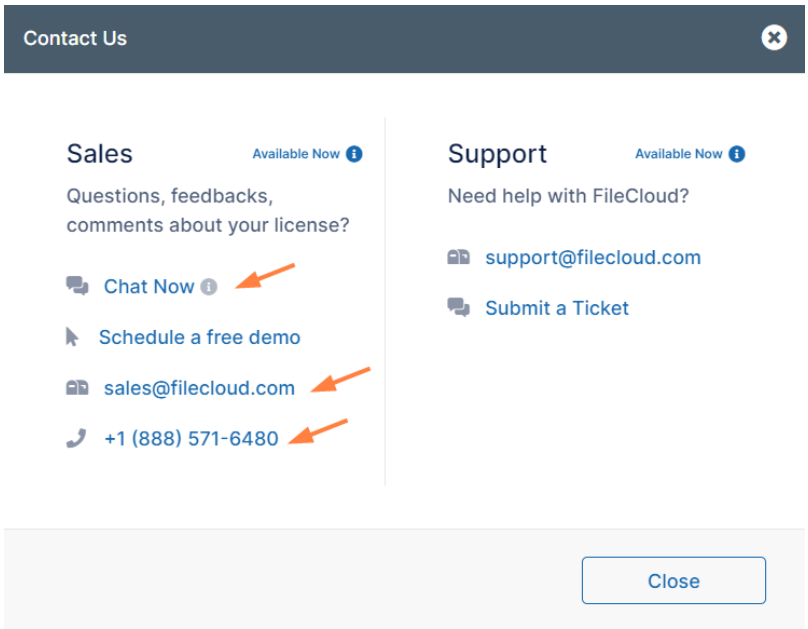
Then

Purchase the server license

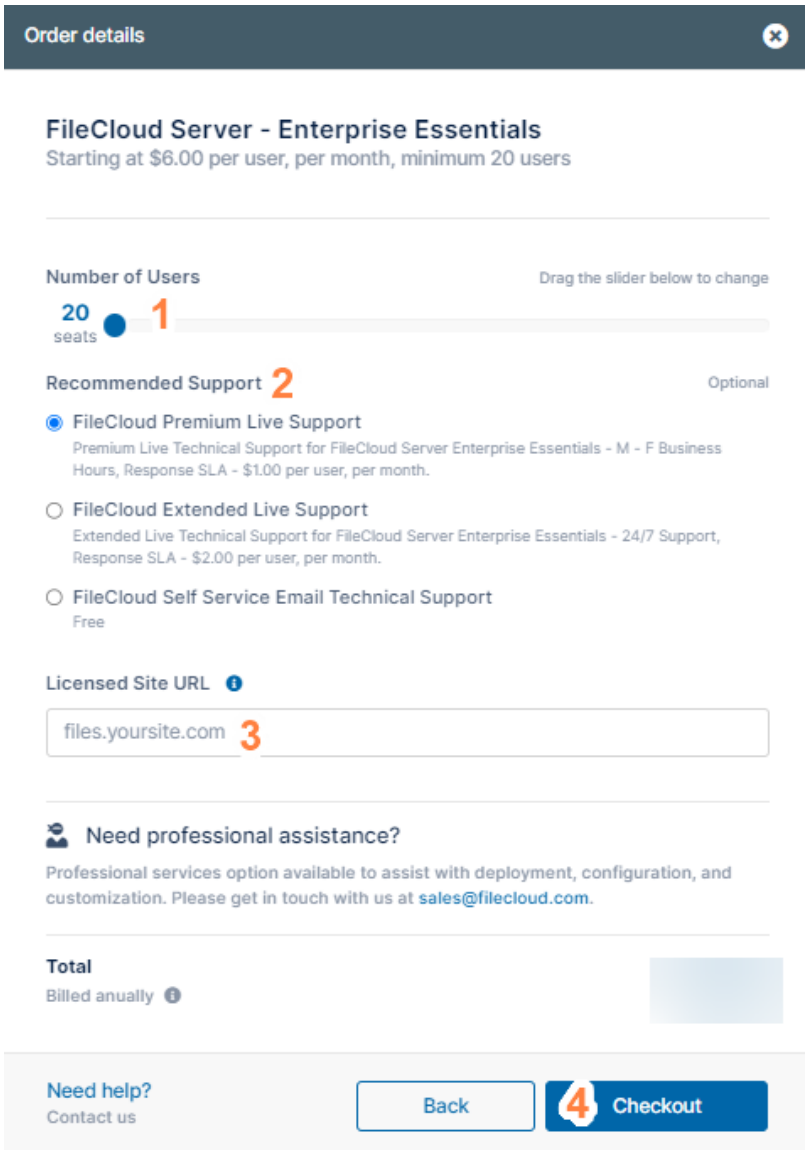
If you choose **Server**, the next window prompts you to choose **Essentials, Advanced,** or **Service Provider**.



If you click **Advanced** or **Service Provider,** in the window that opens, choose an option for contacting Sales and making your purchase.



If you choose **Essentials**, an **Order details** window opens.

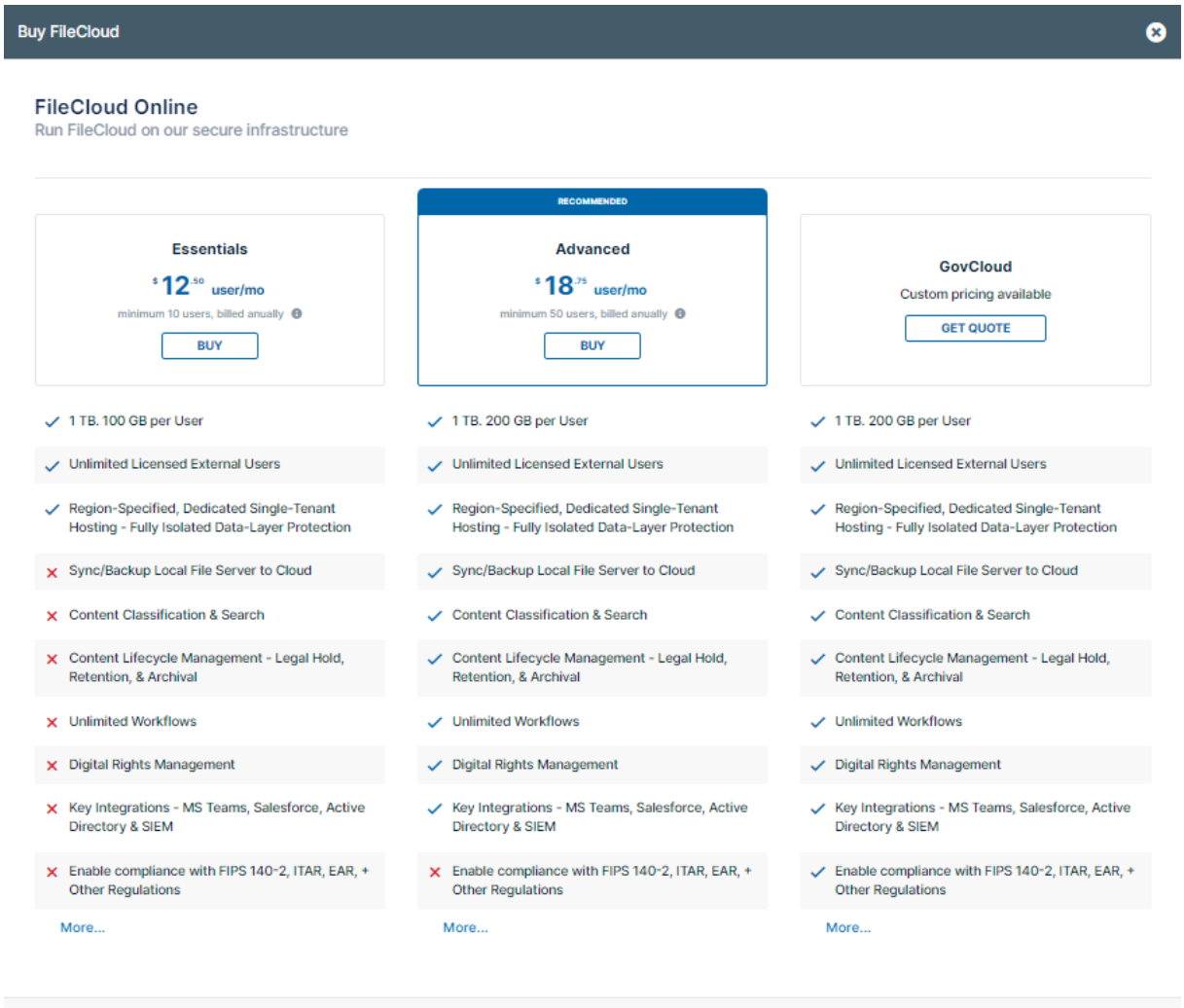


1. Move the **Number of Users** slider to indicate the number of users to include on the license.
2. Choose a support option.
3. In **Licensed Site URL**, enter your site address.
4. Click **Checkout**.
5. Perform the checkout process, below.

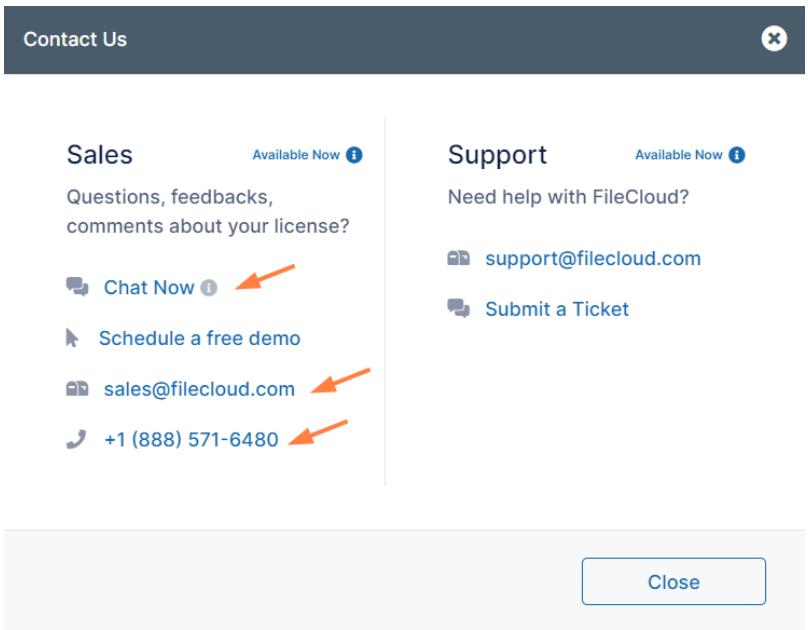
or

Purchase the online license

If you choose **Online**, the next window prompts you to choose **Essentials, Advanced, or GovCloud.**

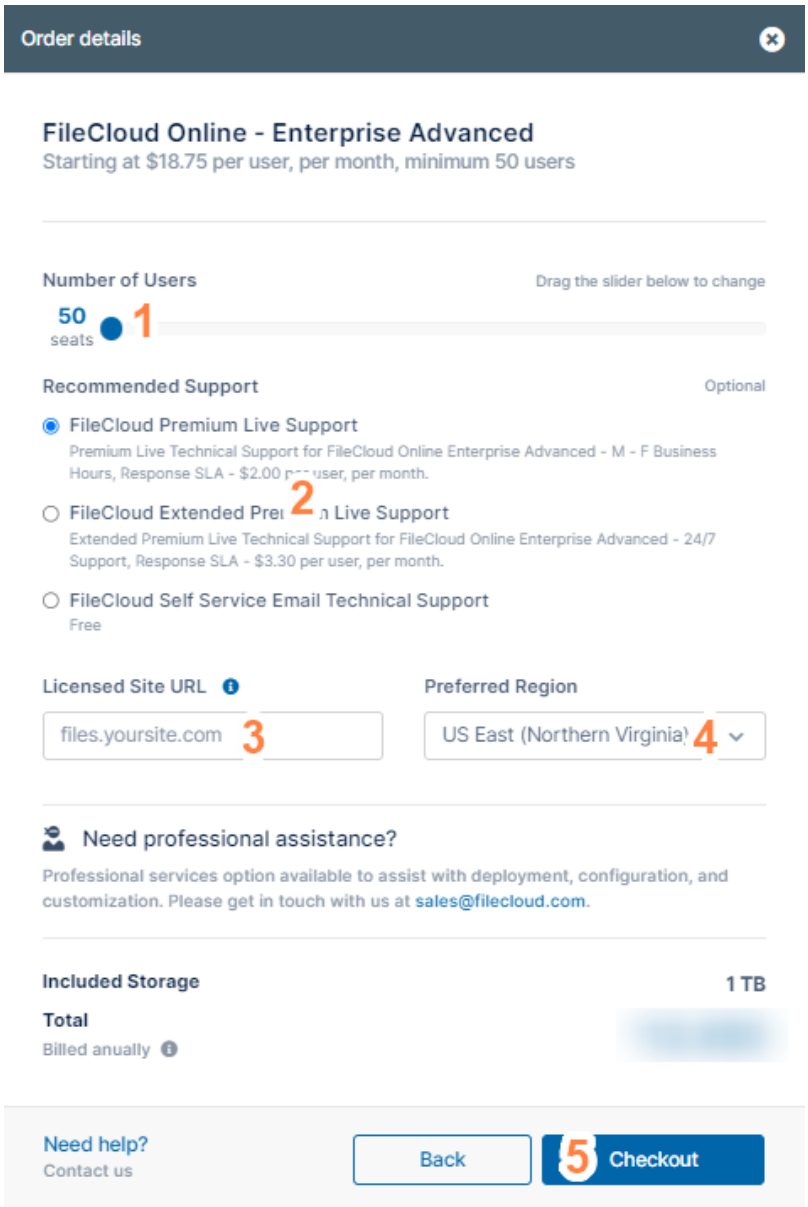


If you click the **GovCloud,** in the window that opens, choose an option for contacting Sales and making your purchase.



If you choose **Essentials** or **Advanced**, an **Order details** window opens. It is similar for both options,

but shows different minimum number of users and support options.



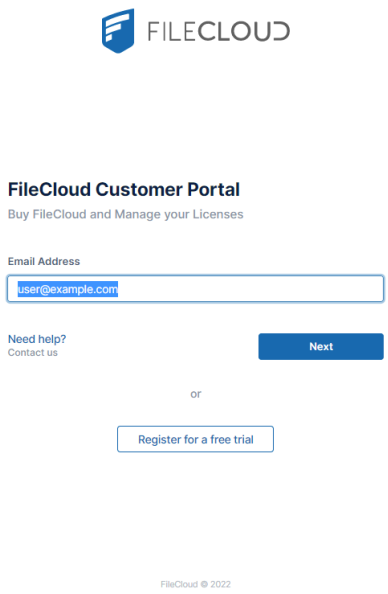
1. Move the **Number of Users** slider to indicate the number of users to include.
2. Choose a support option.
3. In **Licensed Site URL**, enter your site address.
4. In **Preferred Region**, choose the region where you want your server located.
5. Click **Checkout**.
6. Perform the checkout process, below.

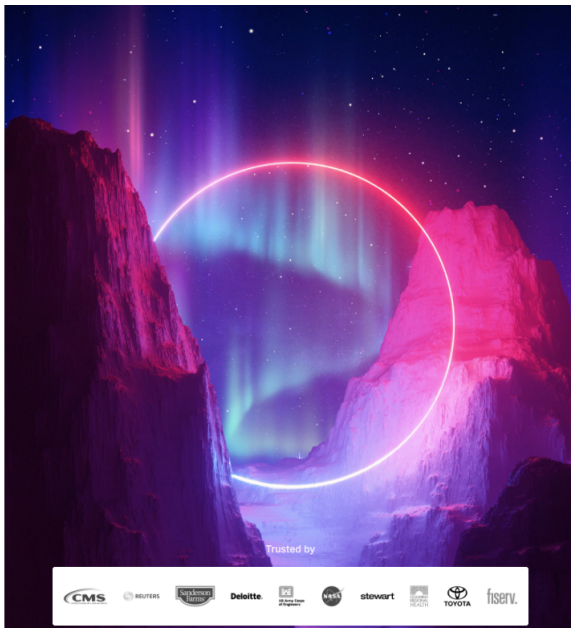
Renew an existing license

Renew a license

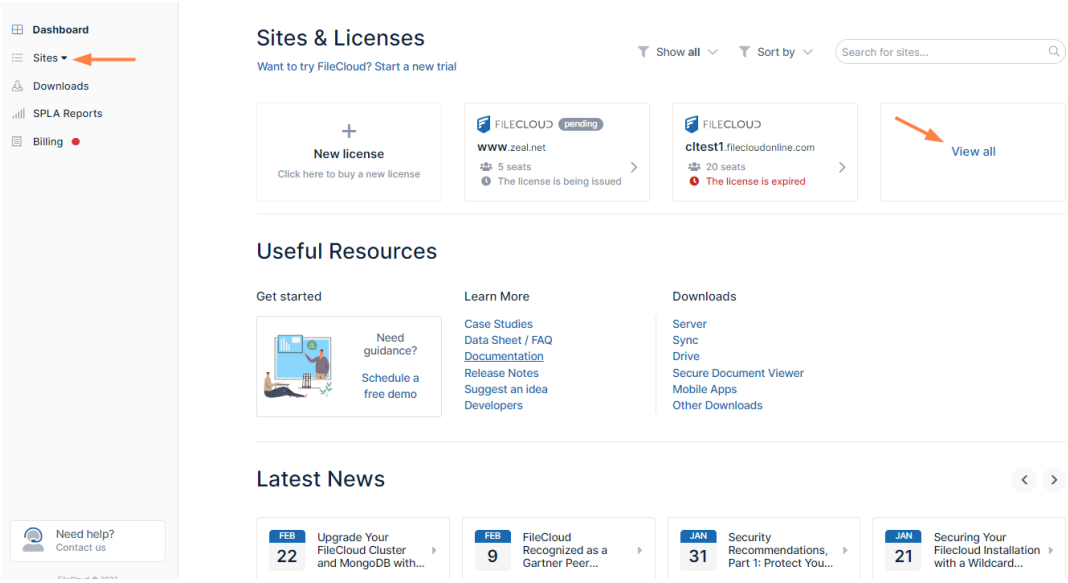
Note: If you are an MSP and want to renew an SPLA License, please follow the purchase a new license instructions, above.

1. Log into https://portal.getfilecloud.com
   Note: Enter the email of the license holder. To change the license holder email, please contact sales@codelathe.com.

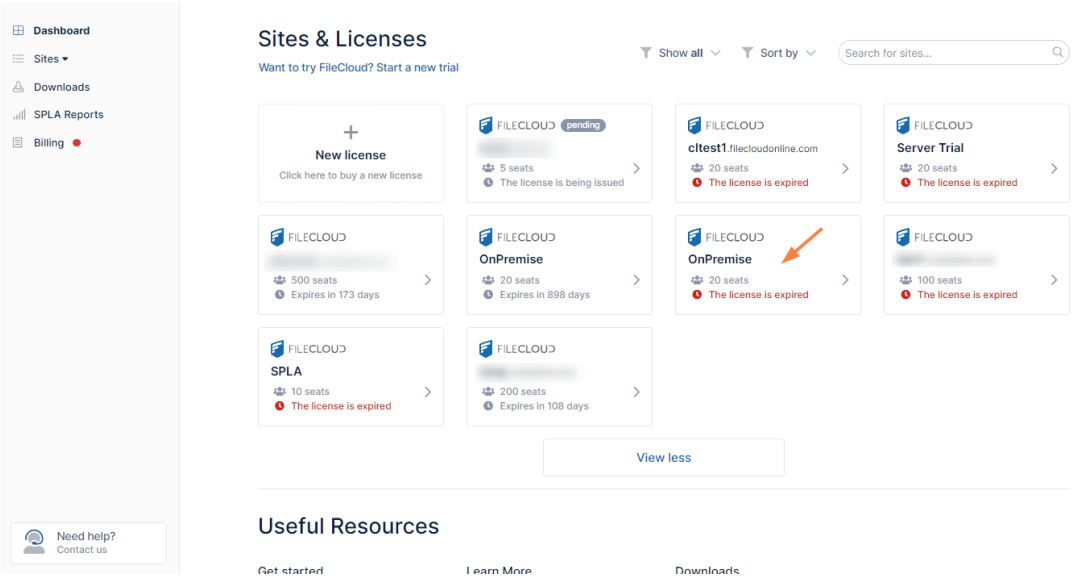




2. If you don't see the license you want to renew on the initial dashboard page, click **View all** to view all of your licenses.
   (You can also expand the **Sites** link in the navigation pane to see navigation links to all of your licenses.)

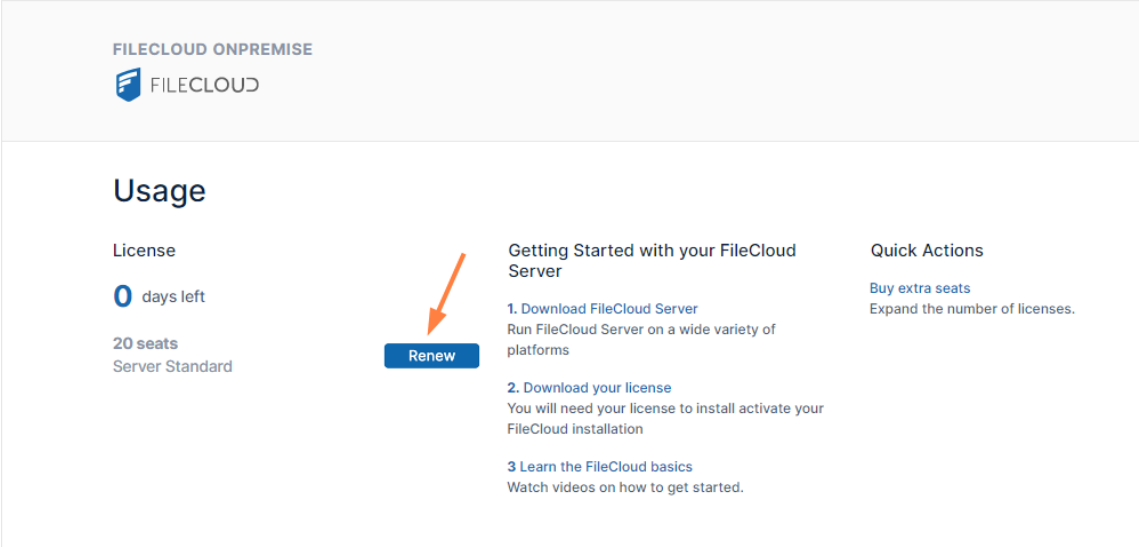


3. Find and click the license that you want to renew.



A screen that displays the license details opens.

4. Click the **Renew** button.



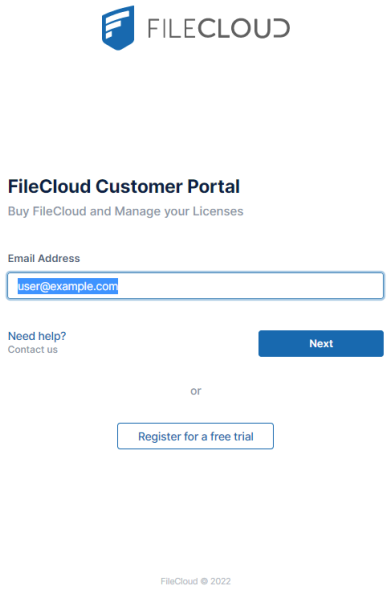
An **Order Summary** opens.

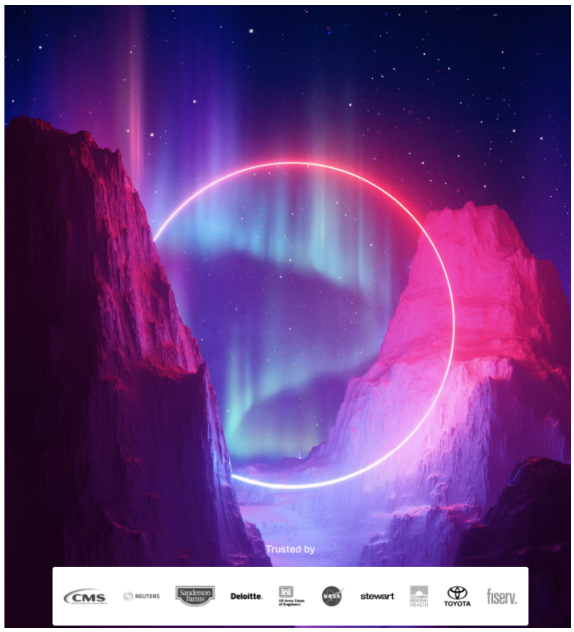
5. Follow the checkout process, below.

Add additional users to an existing license

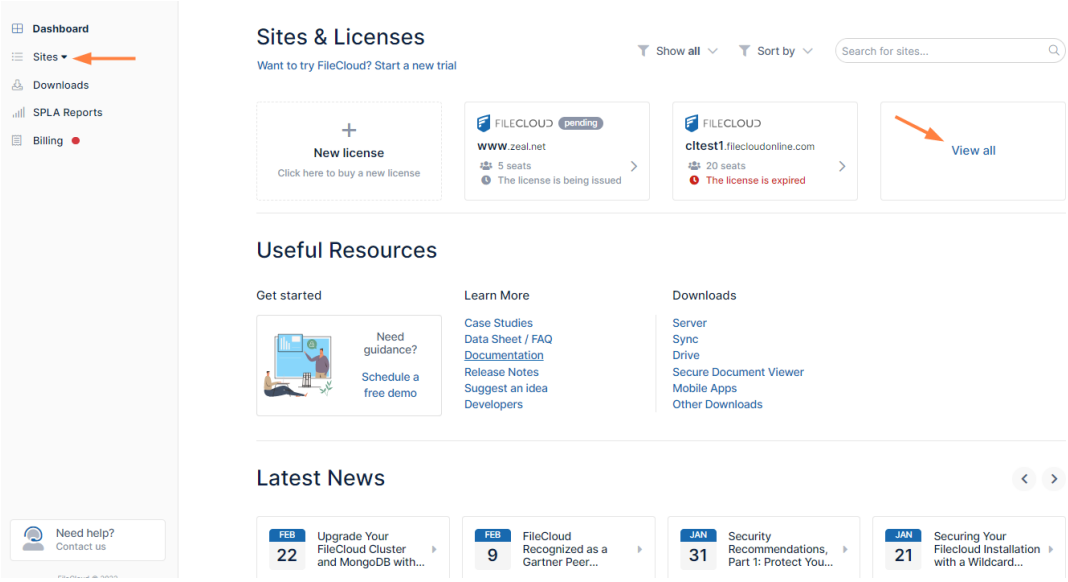
Add additional users to a license

1. Log into https://portal.getfilecloud.com
   Notes: Enter the email of the license holder. To change the license holder email, please email sales@codelathe.com.

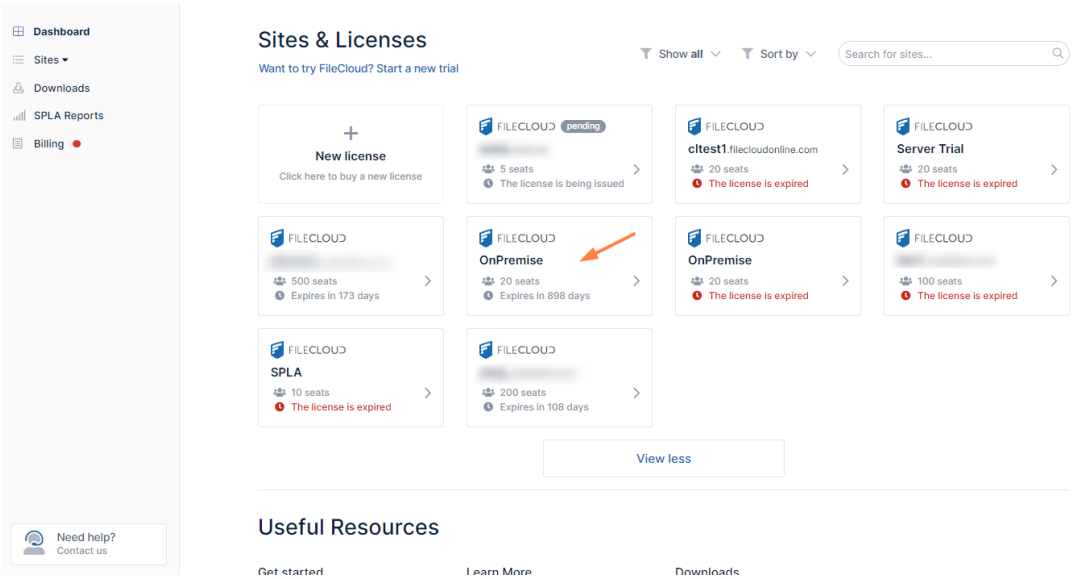




2. If you don't see the license you want to add users to on the initial dashboard page, click **View all** to view all of your licenses.
   (You can also expand the **Sites** link in the navigation pane to see navigation links to all of your licenses.)

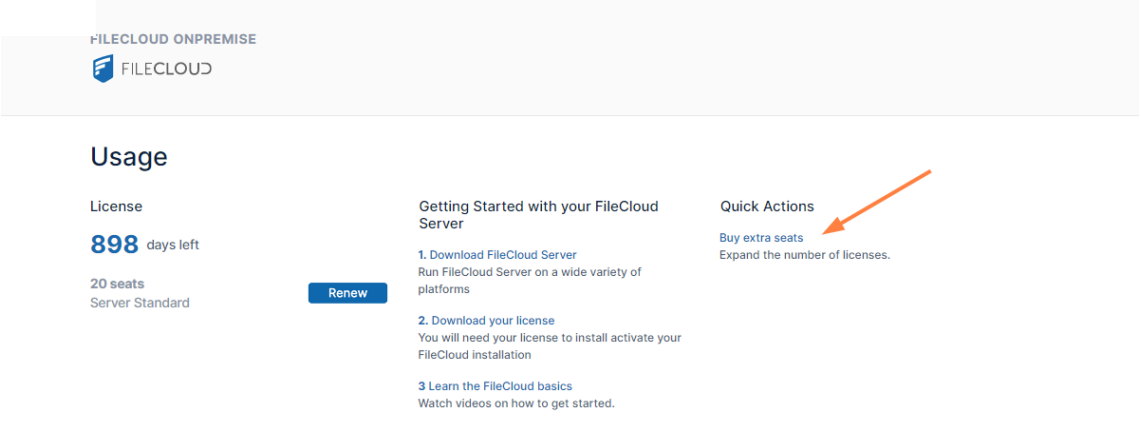


3. Find and click the license that you want to add additional users to.
   .



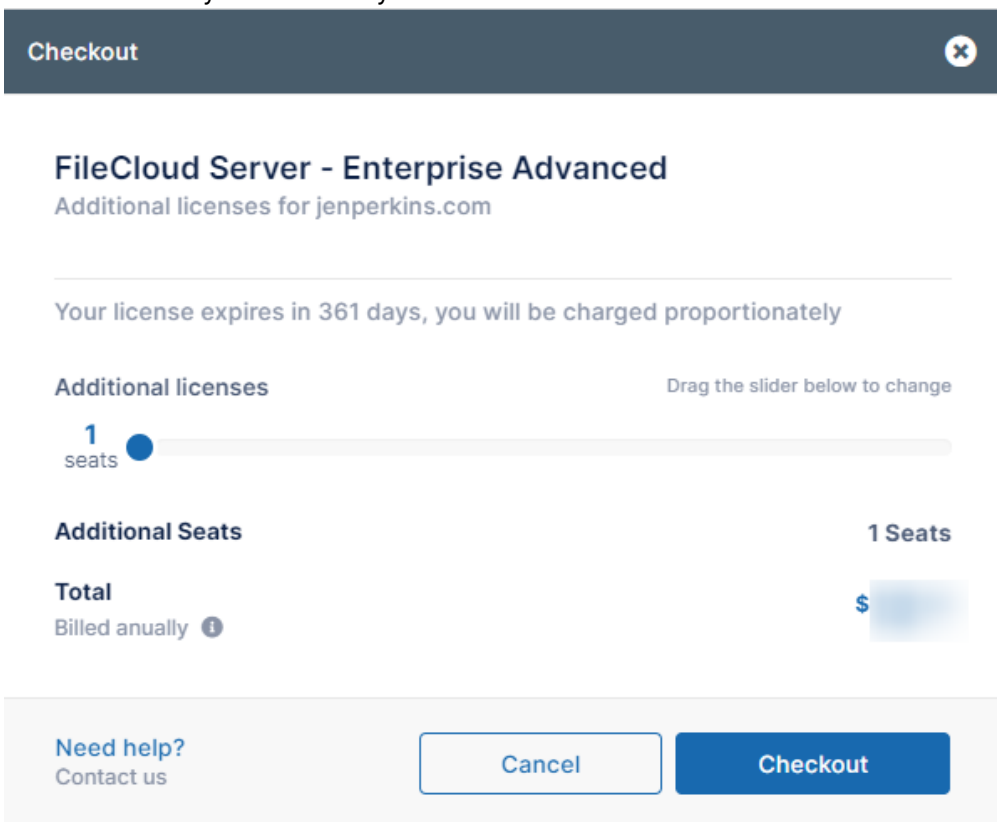
   A screen that displays the license details opens.

4. Click **Buy extra seats**.



A checkout window opens. The number of extra seats is set to 1 by default.

5. If you want to purchase more than 1 extra seat, move the **Number of Users** slider to indicate the number of seats you want to buy.

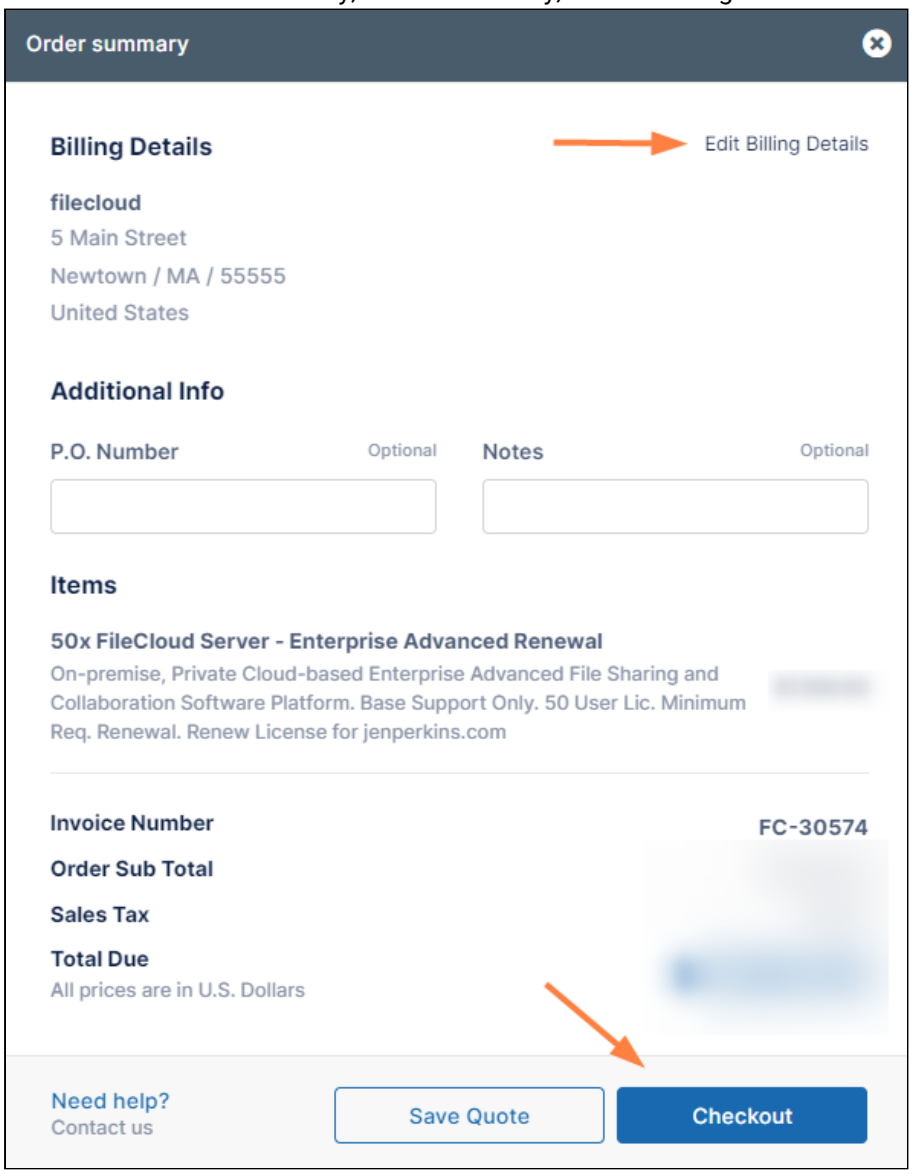


6. Click **Checkout**.
   An **Order Summary** opens.
7. Follow the checkout process.

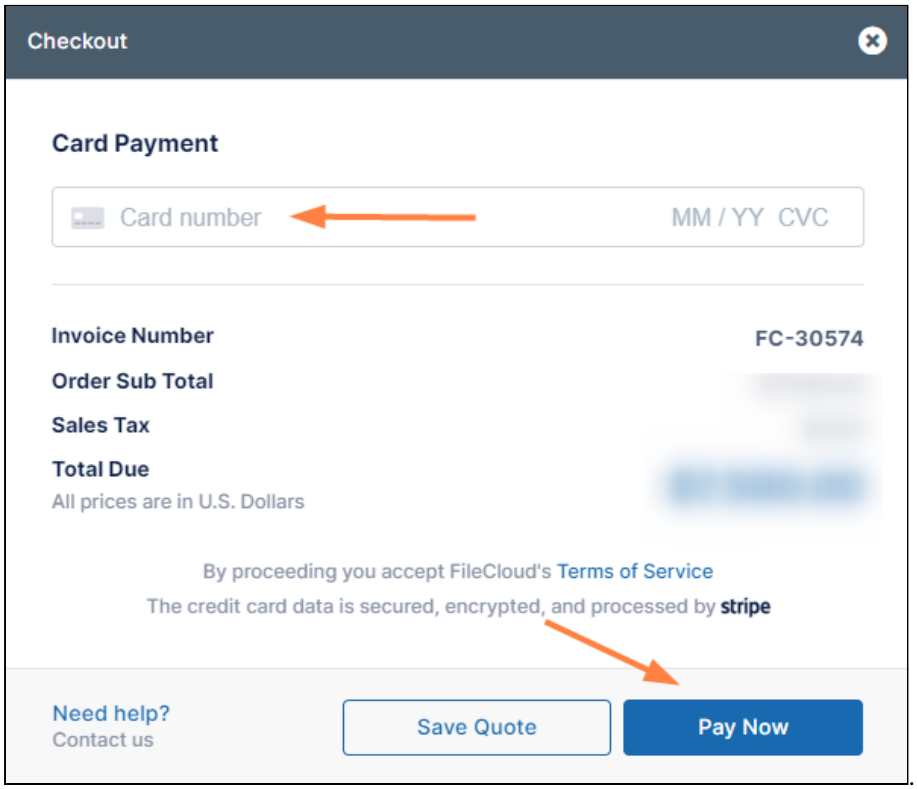
Checkout process

Pay now

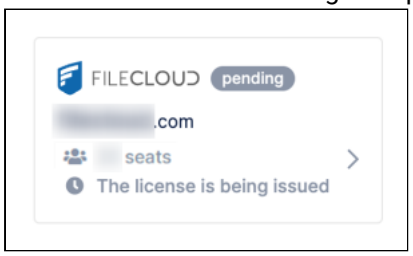
1. Look over the order summary, and if necessary, edit the billing details:



2. Click **Checkout.**



3. Enter your credit card number, and click **Pay Now**.
   A confirmation window appears.
4. Click **Dashboard** in the navigation pane to see an icon for your new pending license:

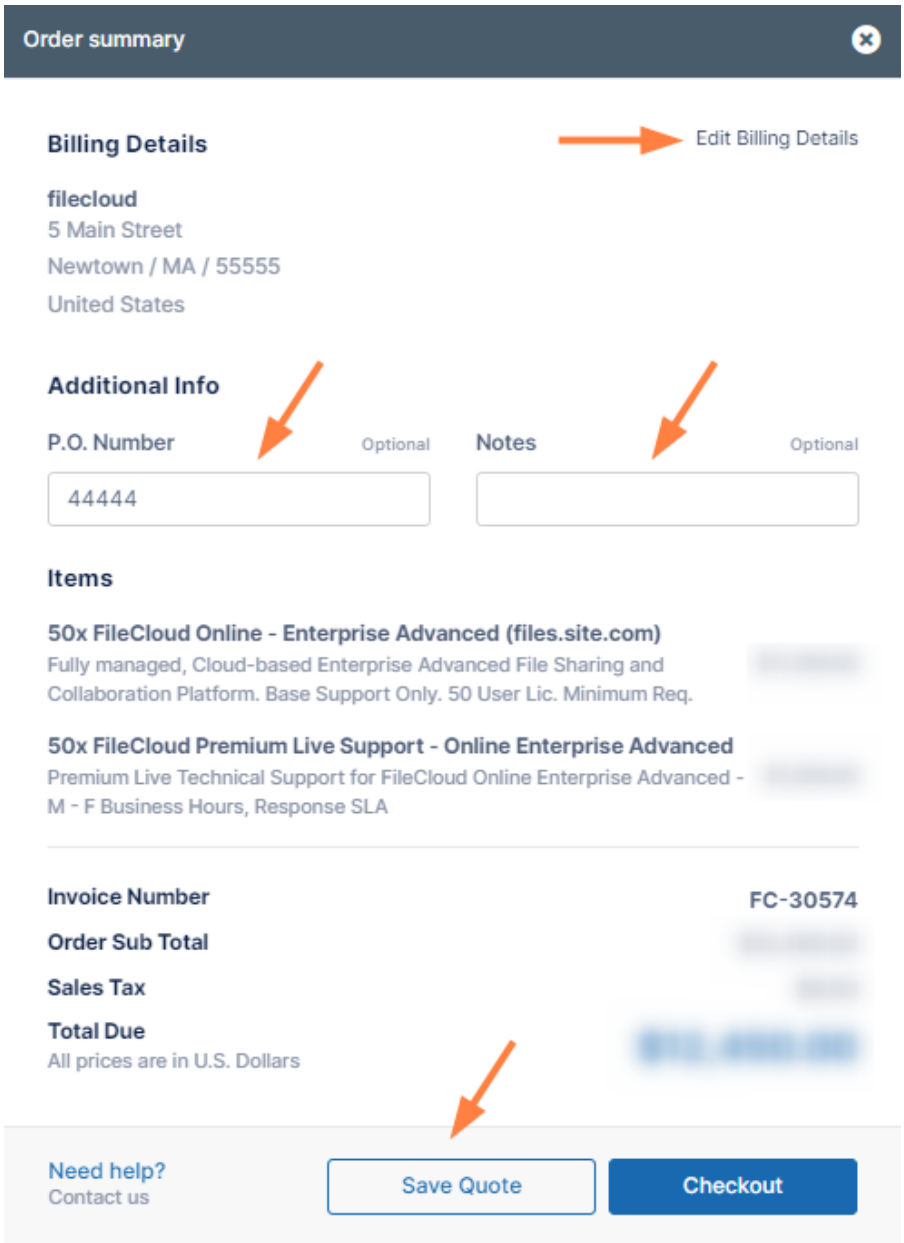


5. When processing of the license is complete and the new license has been installed for you, the pending icon disappears.

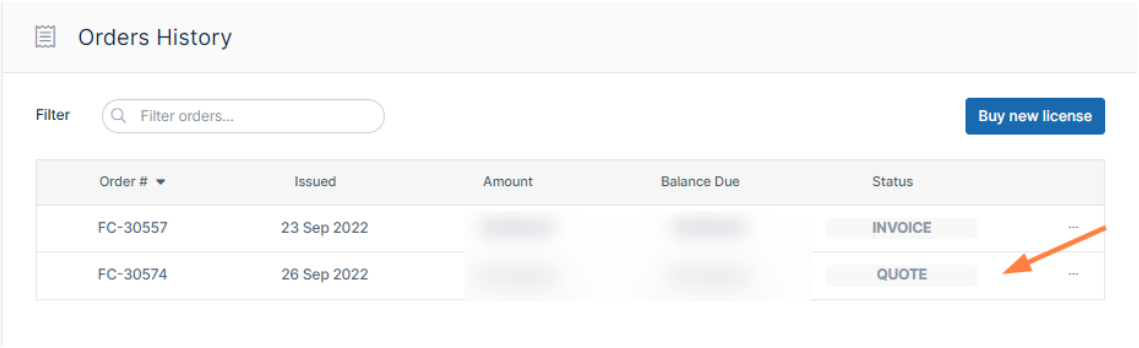
or

Send a purchase order

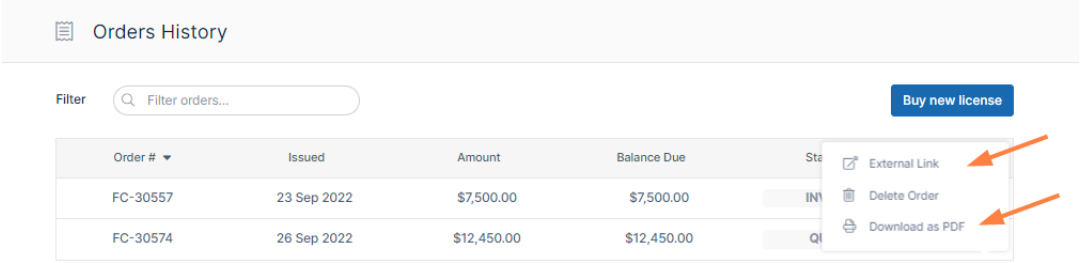
1. Look over the order summary, and if necessary, edit the billing details:



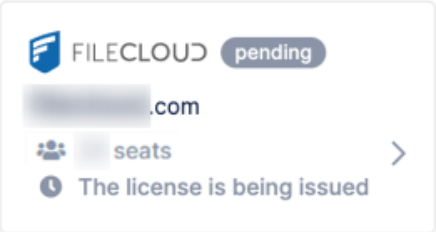
2. Optionally, enter a **P.O. Number** and any **Notes** for FileCloud Sales.
3. Click **Save Quote**.
   The **Billing** screen opens.
4. Your order appears under **Orders History** with the status **QUOTE**.



5. Click the **More** (triple-dot) icon in the row for the order, and either:
   - choose **External Link** and copy the link,
     or
   - choose **Download as PDF** and save the PDF.



6. Send a purchase email to sales@codelathe.com with the quote link included or the PDF attached.
7. Once FileCloud begins to process the license, it is overlaid with a pending icon.

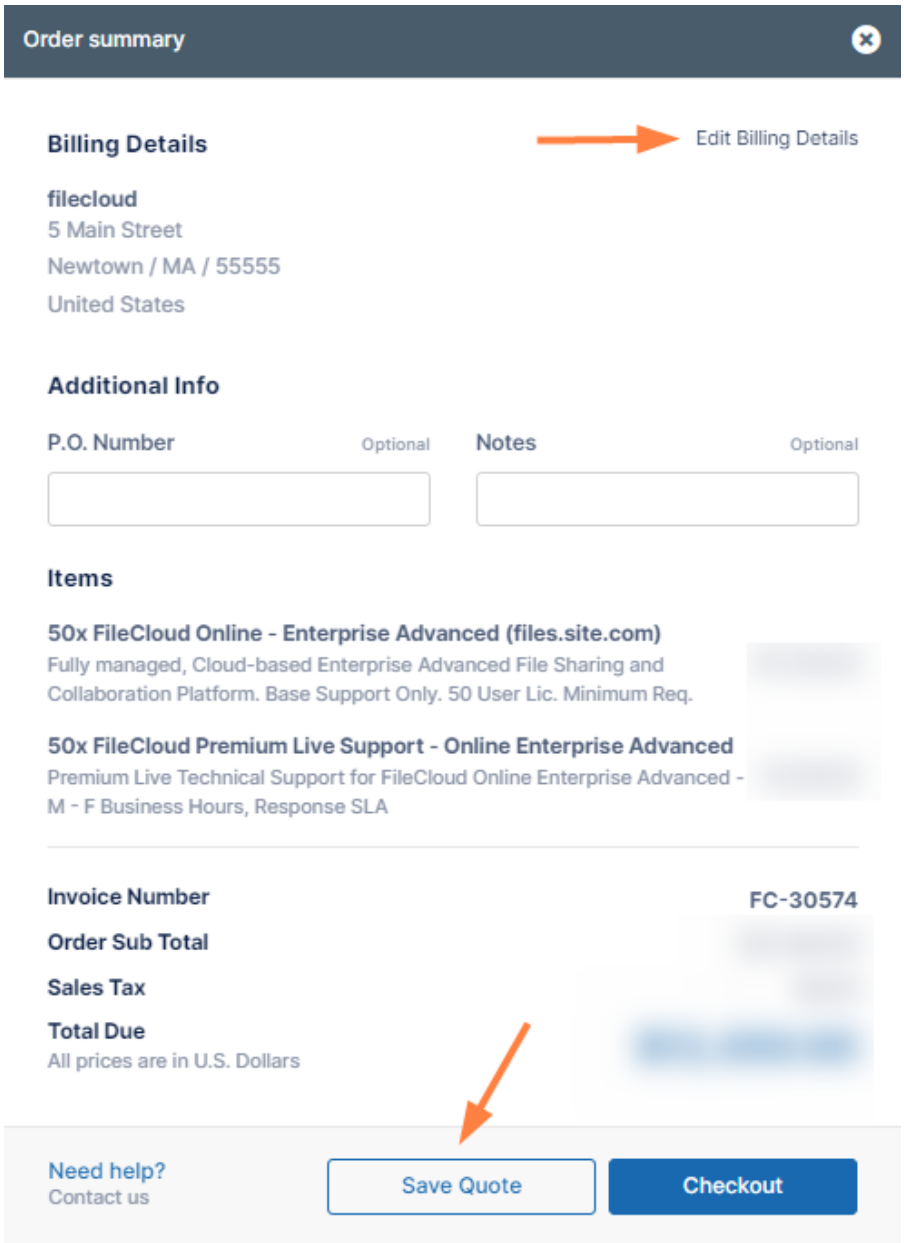


When processing of the license is complete and the new license has been installed for you, the pending icon disappears.

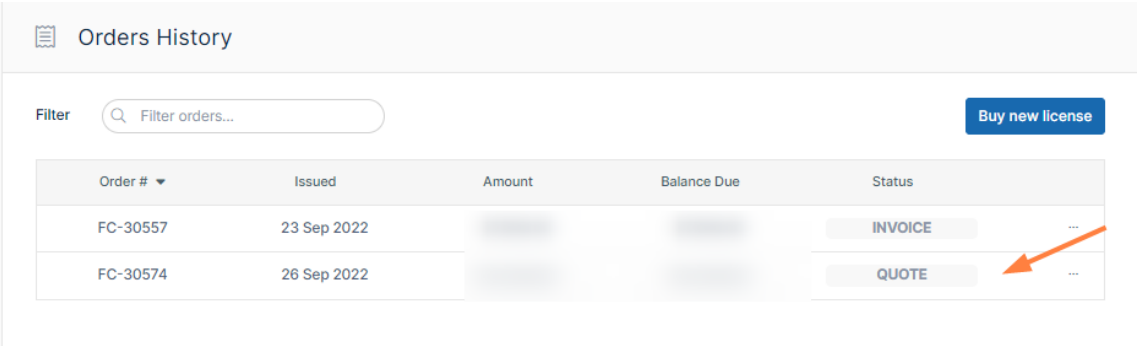
or

Save quote and continue later

1. Look over the order summary, and if necessary, edit the billing details:



2. Click **Save Quote**.
   The **Billing** screen opens. Your order appears under **Orders History** with the status **QUOTE**, and remains there unless you delete it.

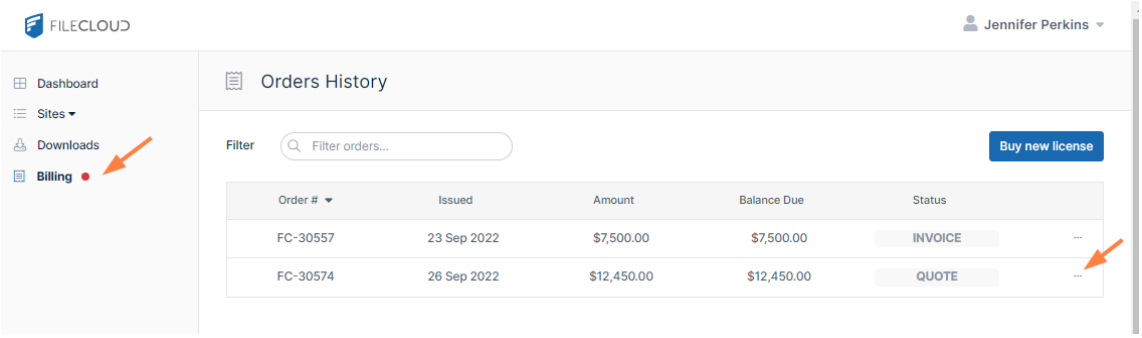


3. When you are ready to continue, return to the **Billing** screen and perform one of the actions in Manage orders, below.

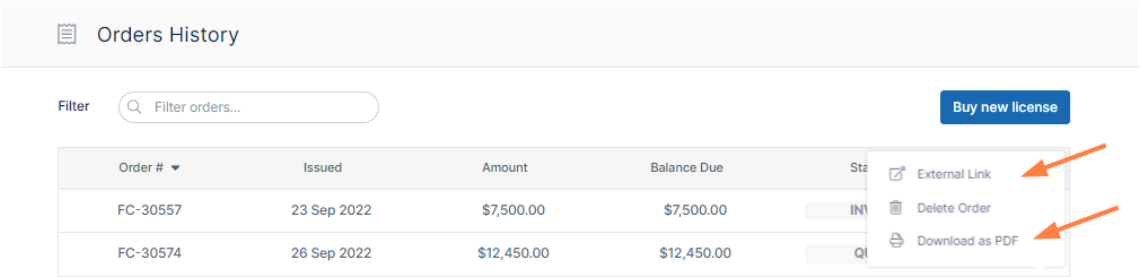
Manage orders

View order, save order link, save to pdf or delete order history

1. Log into https://portal.getfilecloud.com
2. In the navigation pane, click the **Billing** link.
3. To the right of the order, click the **More** (triple-dot) icon.



4. You are given options to view the order in another link, delete it, or download it as a PDF.
   If you click **External Link**, you can copy the link and send it to another user to view the order or you can send it to FileCloud to purchase it. You can also send a copy of the PDF to FileCloud to purchase the order.



Workflows - IFTTT

Administrators can use workflows to automate certain standard operations within FileCloud.

Workflows operate using the following model:

```
IF "CONDITION" - THEN "ACTION" (IFTTT)
```

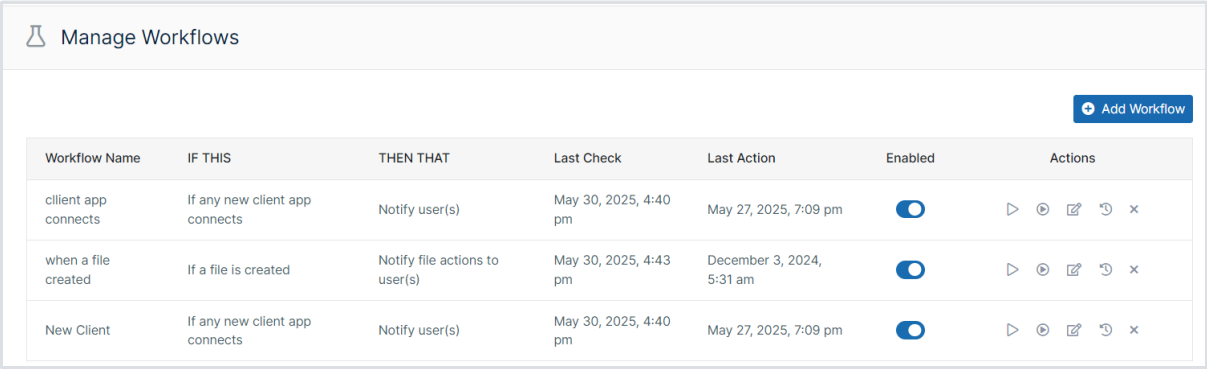
You can setup specific triggers to run when the following conditions occur:

- A system event
- A specific date and time
- A variety of actions

💡 Each of the Conditions and Actions may require a parameter in JSON format.

The Workflow Dashboard

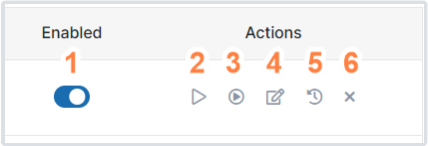
All workflows are created and managed on the Workflows dashboard.



To access the Workflows dashboard:

1. Open a browser and log into the admin portal.
2. On the left hand navigation panel, under **MISC.**, click **Workflows**.

The actions you can perform on a workflow you have created include:

	1. Enable or Disable the workflow 2. Run the workflow (once, on-demand) 3. Simulate the workflow. Displays the list of users or files that a workflow will affect. The Simulate option is only available to workflows that are configured to run on demand and not to run automatically at scheduled times. 4. Edit the workflow 5. See activity. (Shows the date of an event, and a description of the event, such as file upload, move, and deletion. 6. Delete the workflow

In this section:

Add a New Workflow

> It is important to note that not all actions are compatible with all conditions. Please see the table on the page Define a THEN Action for compatible settings.

Administrators can add Workflows in the Admin Portal.

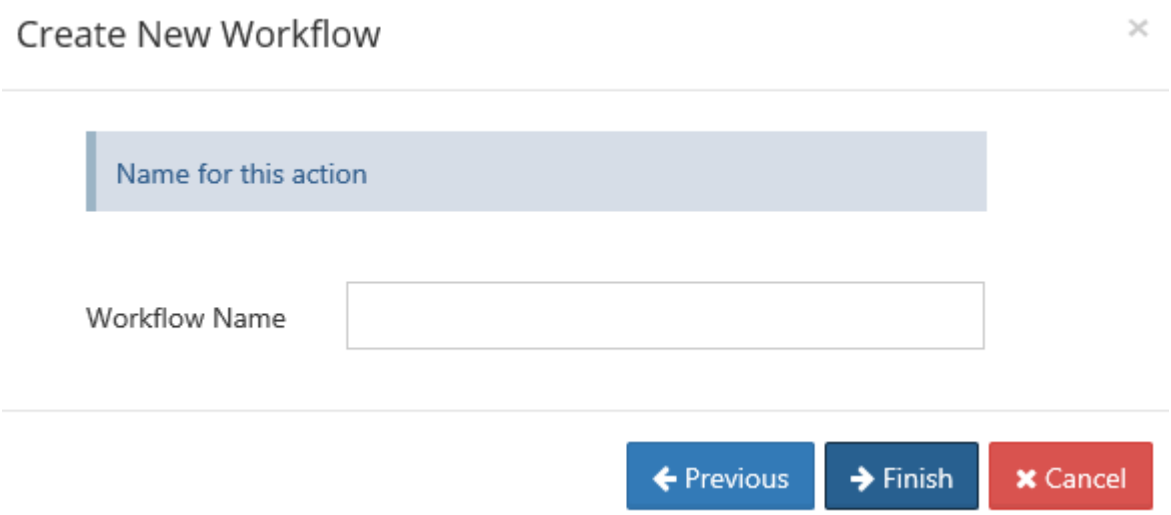
You will need to choose a condition, and specify what action should be taken when that condition occurs.

- Define an IF Condition
- Define a THEN Action

To add a new workflow:

1. Open a browser and log into the Admin Portal.
2. On the left hand navigation panel, click **Workflows**.
3. On the top right, click the Add Workflow button.
4. In the Create New Workflow window, select an IF Condition, and then click Next.
5. If a condition requires you to specify a value for something, for example a date or time, type in the values in the Required Parameters, and then click Next. Information about what is required is described below this box.
6. In the Create New Workflow window, select a THEN Action, and then click Next.
7. If an Action requires you to specify a value for something, for example a date or time, type in the values in the Required Parameters, and then click Next. Information about what is required is described below this box.

8. In Workflow Name, type in a unique word or phrase that describes the workflow, and then click Finish.



Define an IF Condition

Beginning in version 23.253, FileCloud supports expressions, special conditions based on user and path owner properties.

The workflow **If a user's account is near its expiration date** is available in FileCloud 23.251 and later.

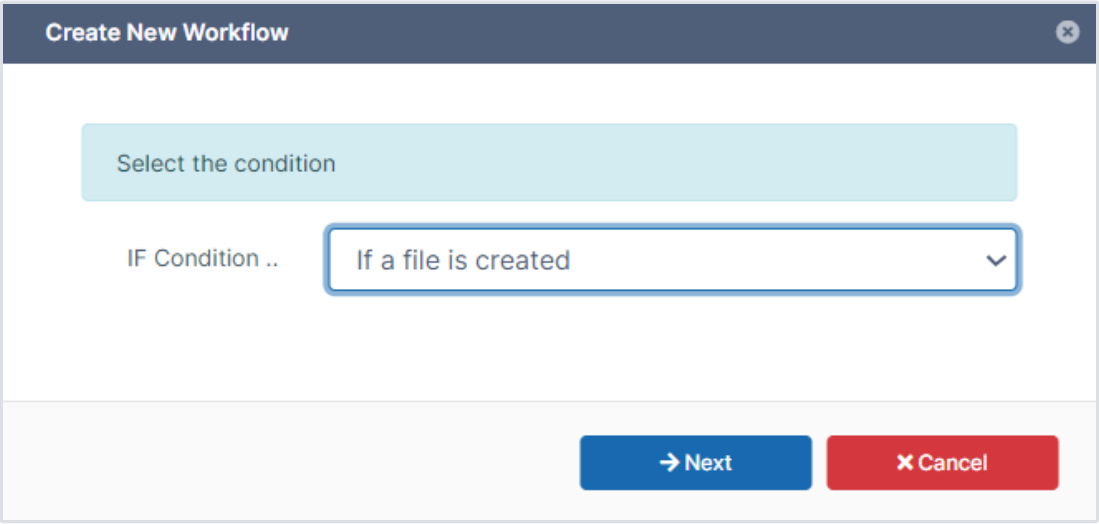
Not all actions are compatible with all conditions.

When you create a workflow, you must select a condition to act as a trigger.

- Depending on the trigger, additional parameters may be required.
- Once a Condition is selected, compatible Actions can be selected.

Where do I set up the condition?

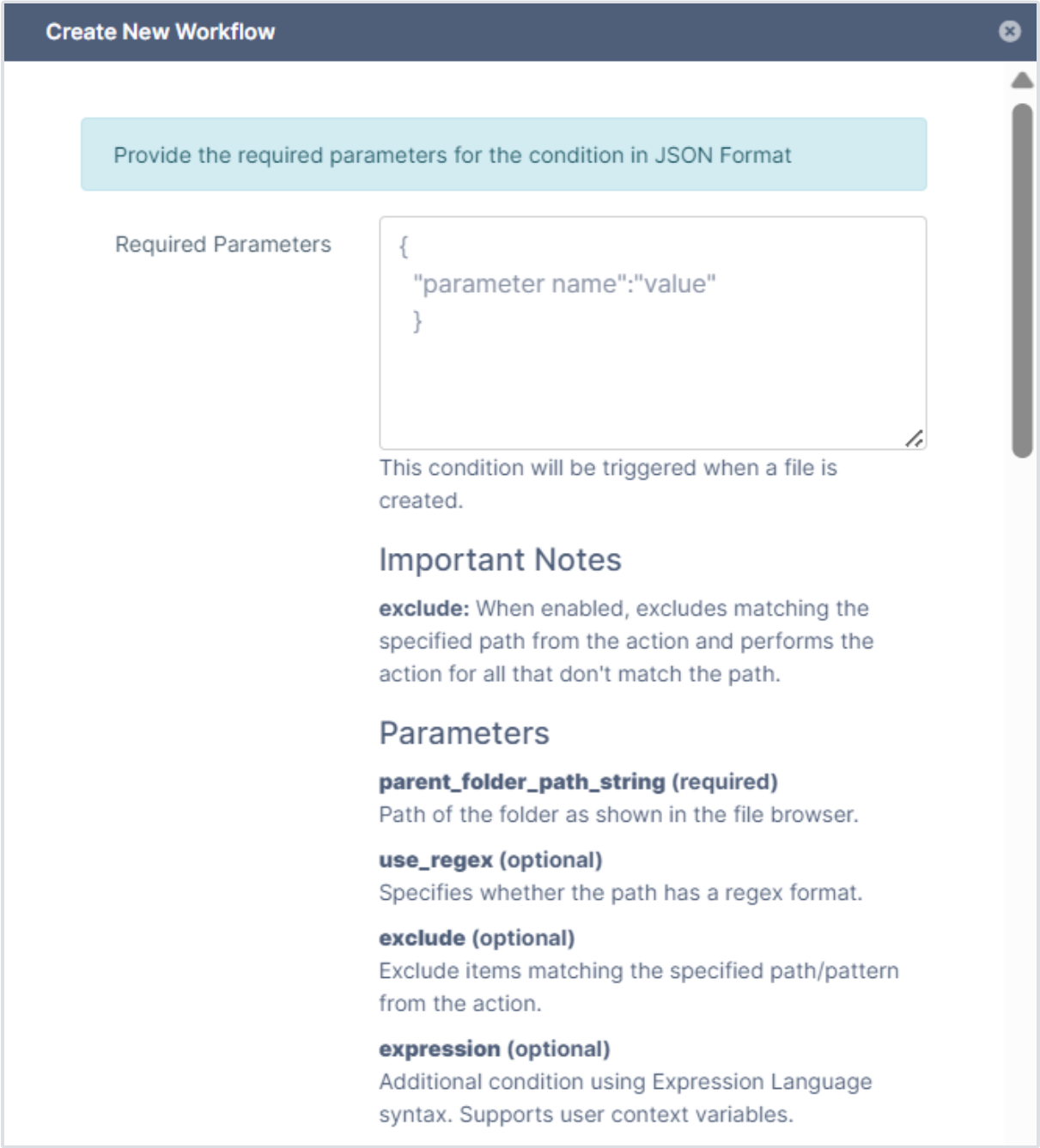
When you create a new Workflow, you will be able to select a condition.



Where do I add my parameters?

After you select a Condition, then you can enter any parameters, such as a date or time.

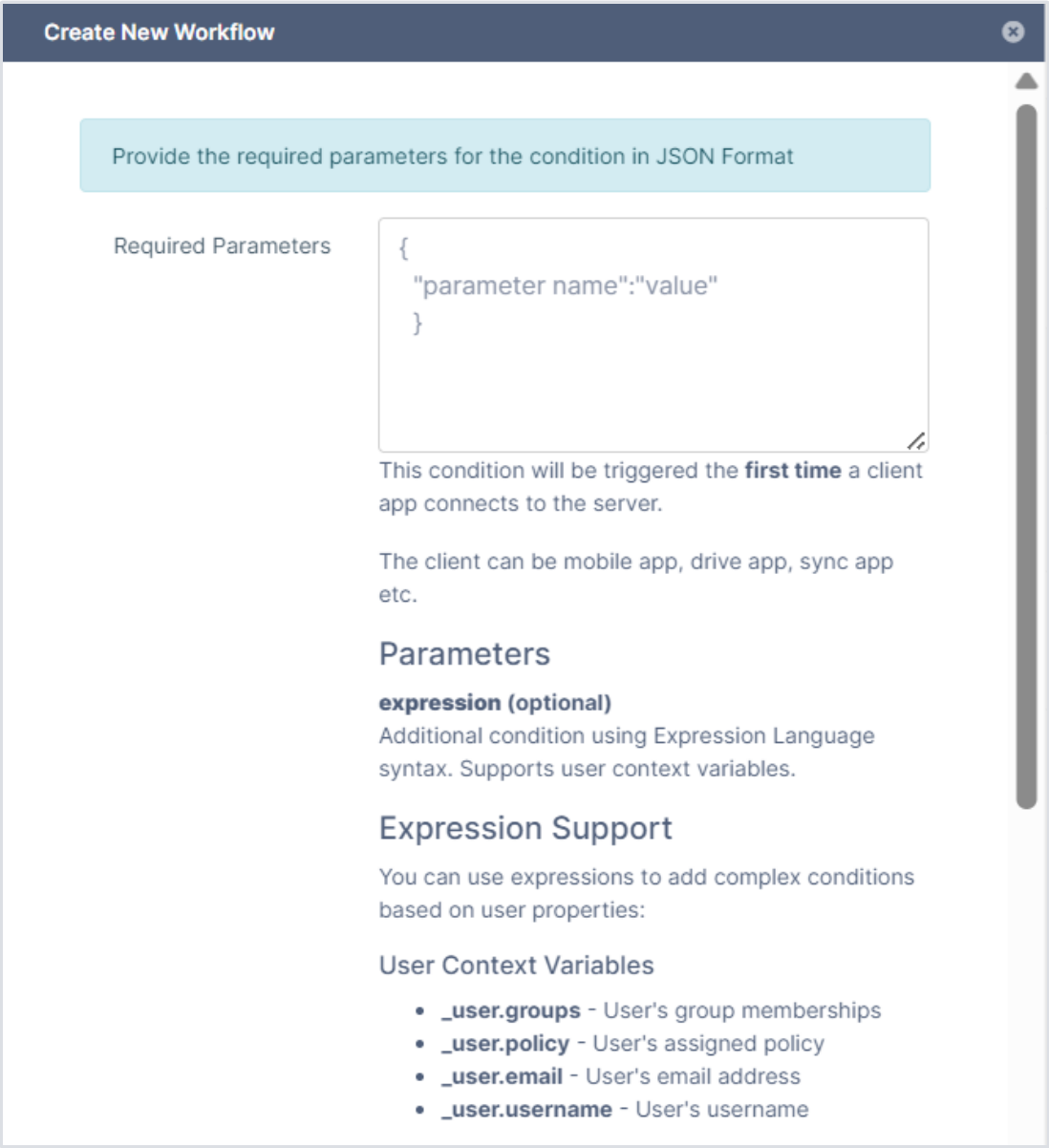
If you need more information about what parameters are required, look below the Required Parameters box.



Available Conditions

Client App Conditions

If any new client app connects

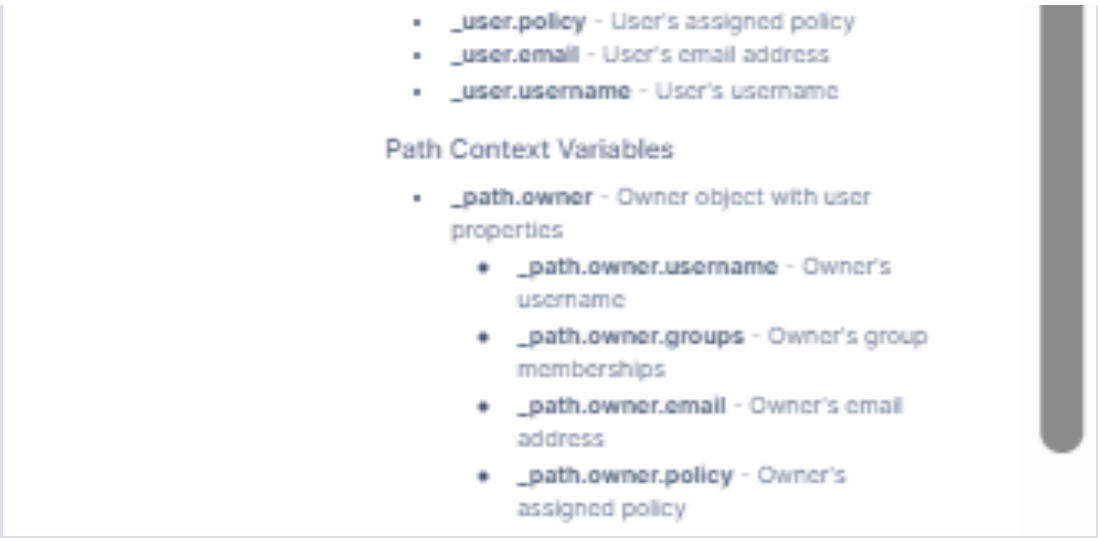


Workflow Condition	Parameters	Description
If any new client app connects	**No parameters required**	This condition is triggered when an external (non-browser) client connects to FileCloud Server. For example, this condition will trigger for clients such as: • FileCloudSync • FileCloudDrive • iOS • Android App

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

File Conditions

If a file is created



Workflow Condition	Parameters	Description
If a file is created	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered if a file is created via any means (Browser, Clients, etc.) **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a file is updated

Workflow Condition	Parameters	Description

If a file is updated.	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered if a file is updated. **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a file is deleted

Workflow Condition	Parameters	Description
If a file is deleted	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered if a file is deleted. **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If file is downloaded

Workflow Condition	Parameters	Description

If a file is downloaded	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered if a file is downloaded **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

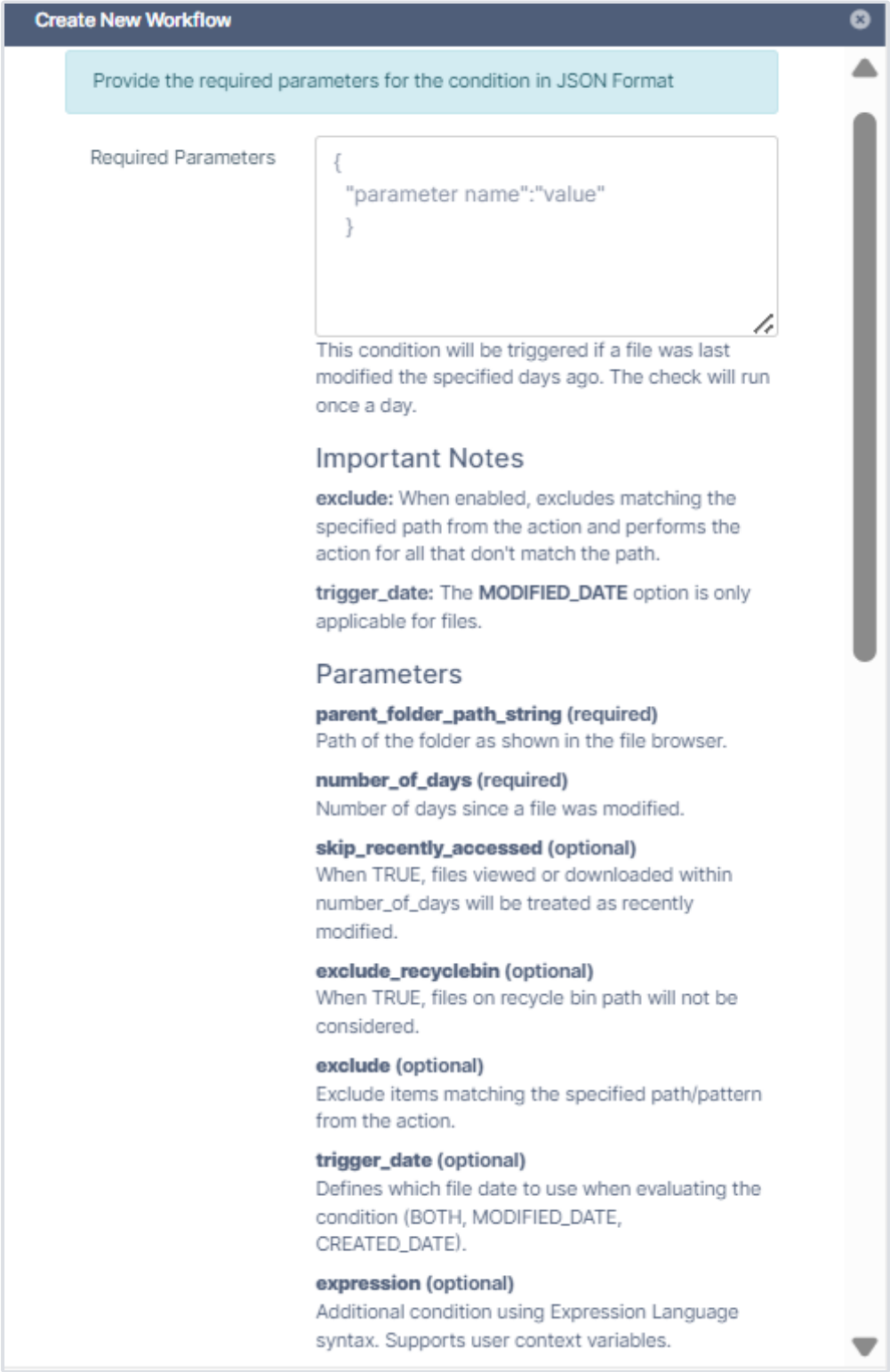
Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a file is added or updated

Workflow Condition	Parameters	Description
If a file is added or updated	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered if a file is added or updated **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If file was not modified/created in specified days

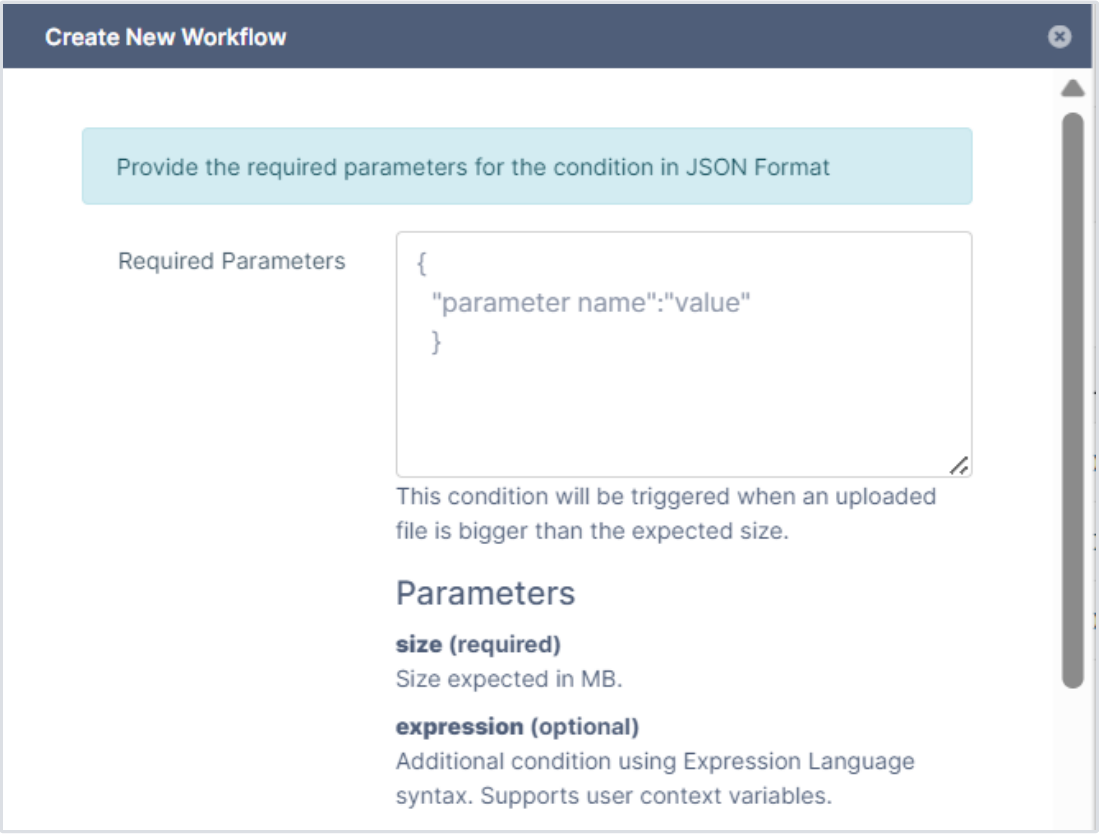


Workflow Condition	Parameters	Description

If a file was not modified/ created in specified days	`{`
	`"parent_folder_path_string": "/johndoe",`
	`"number_of_days": 7,`
	`"skip_recently_accessed": 1,`
	`"exclude_recyclebin": 1,`
	`"exclude": ".*secret.*"`
	`}`
		This condition will be triggered if a file was not created [specified days] ago or has not been updated for [specified days].
		• This is useful for removing old files that are no longer being used
		• This check will run once a day
		parent_folder_path_string - required as a parameter for this condition to trigger.
		• If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path.
		• NOTE: ONLY Managed storage paths are supported for this condition.
		number_of_days - required to specify the number of days before the current date that a file was last modified.
		• This will be checked once a day and all files that match this condition will be subject to the THEN action you choose.
		• For example, if you specify the number of days as 15, all files in the specified folder that have not been modified in the last 15 days will subject to the the THEN action you configure.
		skip_recently_accessed - required to specify whether files that were viewed or downloaded during the number of days are considered modified. Default is *false*, viewed or downloaded files are not considered recently modified. When *true*, files viewed or downloaded within number_of_days are considered modified and will not be included in the *Then* action.
		exclude_recyclebin - (added in FileCloud version 21.3) optional (default is false) When true, files in recycle bin are not considered.
		exclude - (added in FileCloud version 22.1) optional - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).
		trigger_date - (added in FileCloud version 23.253) optional (default is BOTH) - specifies which field to use as the date the file was last modified. Use one of the following values:
		BOTH - (default) Check if the CREATED_DATE and the MODIFIED_DATE are the specified number of days ago or more.
		CREATED_DATE - Check if the CREATED_DATE is the specified number of days ago or more.
		MODIFIED_DATE - Check if the CREATED_DATE is the specified number of days ago or more.

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If the file uploaded is bigger than the expected size



Workflow Condition	Parameters	Description
If the file uploaded is bigger than expected size.	*{ "size":"4" }*	This condition will be triggered when an uploaded file is bigger than the size specified. **size** - specifies the maximum expected file size in MB.

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If the file downloaded is bigger than the expected size

Workflow Condition	Parameters	Description
If the file downloaded is bigger than expected size.	*{ "size":"4" }*	This condition will be triggered when a downloaded file is bigger than the size specified. **size** - specifies the maximum expected file size in MB.

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

Folder Conditions

If a folder is created

Workflow Condition	Parameters	Description
If a folder is created	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered when a folder is created in the system **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a folder is deleted

Workflow Condition	Parameters	Description
If a folder is deleted	*{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }*	This condition will be triggered when a folder is deleted **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

User Account Conditions

If a user's last login is older than...

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
 "parameter name":"value"
 }
```

This condition is triggered if a user's last login is older than specified days. This check will run based on the day interval configured.

Parameters

last_login_days_ago (required)
Number of days since last login.

user_account_type (required)
Type of user account (USER_ACCOUNT_ANY, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS, USER_ACCOUNT_DISABLED).

day_interval (required)
Days interval (For daily operation, specify this value to be 1).

skip_users_not_logged_in (optional)
Skip users who have never logged in to the system.

skip_admin_users (optional)
Skip promoted admins. Default is true.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

	Workflow Condition	Parameters	Description

If a user's last login is older than ...	`{`	`"last_login_days_ago": 30,`
		`"user_account_type": "USER_ACCOUNT_LIMITED_ACCESS",`
		`"day_interval": 1,`
		`"skip_users_not_logged_in": 1,`
		`"skip_admin_users": 0,`
		`"include_domain": "domain.com",`
		`"exclude_domain": "subdomain.domain.com,@otherdomain.com"`
		`}`
		
		For example, every five days to check for full access users who have not logged in for the last 30 days. Omit them from this check if they have never logged in or are promoted admins.
		`{ "last_login_days_ago": 30,`
		`"user_account_type": "USER_ACCOUNT_FULL_ACCESS",`
		`"day_interval": 1,`
		`"skip_users_not_logged_in": 1,`
		`"skip_admin_users": 1,`
		
		`}`
			If a user's last login is older than the specified number of days, then the THEN condition you configure will be run.
			last_login_days_ago: Number of days since last login.
			user_account_type - type of account. You must use one of the following values:
			• USER_ACCOUNT_ANY
			• USER_ACCOUNT_FULL_ACCESS
			• USER_ACCOUNT_GUEST_ACCESS
			• USER_ACCOUNT_LIMITED_ACCESS (for external users)
			• USER_ACCOUNT_DISABLED
			day_interval - the number of days between checks
			• For daily operation, specify a value of 1
			skip_users_not_logged_in (optional): Skip users who have never logged in to the system. This enables you to only apply the action to users who are already using the system. Values are **true** and **false**.
			skip_admin_users (added in FileCloud 23.251) Optional. Do not include promoted admins.
			0 (default) - Include promoted admins
			1 - Do not included promoted admins

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a new user is created

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
 "parameter name":"value"
 }
```

This condition will trigger the proper action depending on the security state of a created user.

Parameters

auth_type (optional)
Type of authentication (DEFAULT, ACTIVEDIRECTORY, LDAP).

user_access_level (optional)
Account access level (USER_ACCOUNT_ANY_ACCESS, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS). Default is "USER_ACCOUNT_ANY_ACCESS".

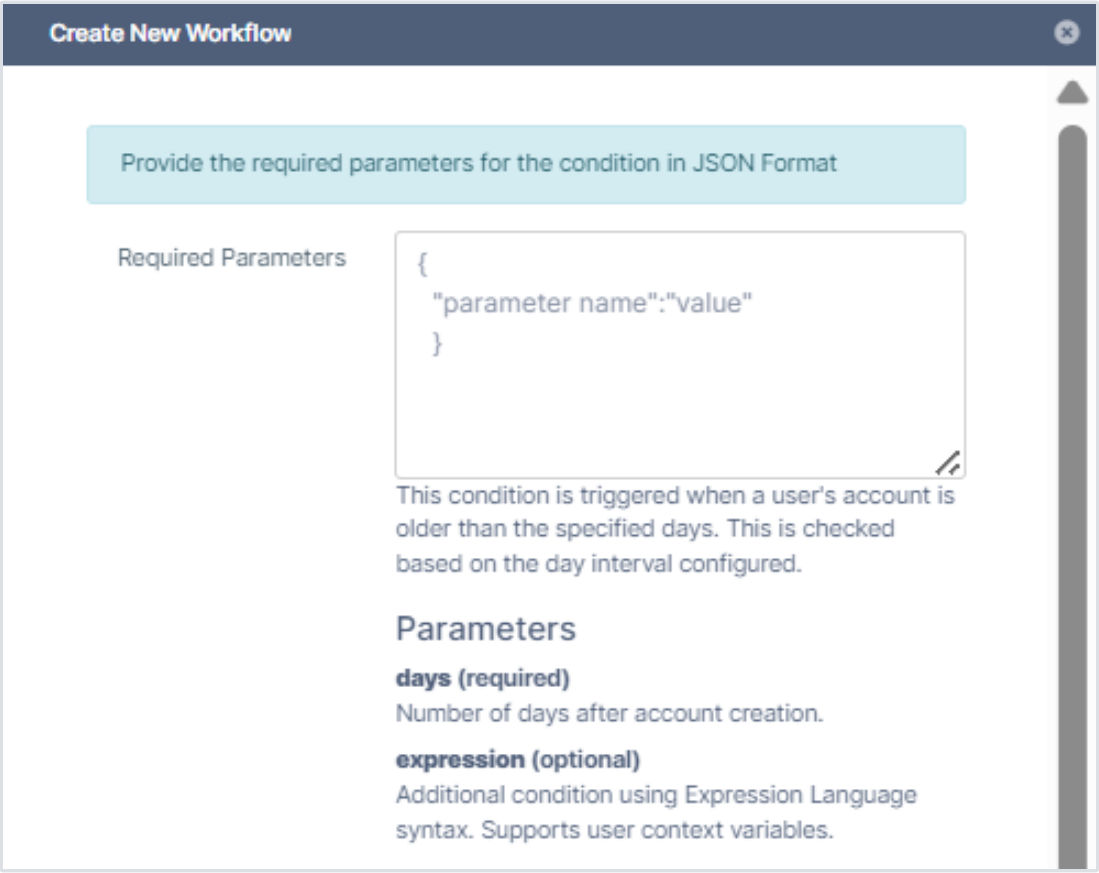
user_login_method (optional)
How user authenticates (LOGIN_METHOD_ANY, LOGIN_METHOD_DEFAULT, LOGIN_METHOD_SSO). Default is "LOGIN_METHOD_ANY".

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Parameters	Description
If a new user is created ...	*None*	When a new user account is created, the THEN action you configure will be triggered. Optional Parameters **auth-type** - Type of authentication. This is **optional** and can be: • DEFAULT • ACTIVEDIRECTORY • LDAP **user_access_level:** Account access level. This is **optional** and can be: • USER_ACCOUNT_ANY_ACCESS (default) • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (for external users) **user_login_method:** How user authenticates. This is **optional** and can be: • LOGIN_METHOD_ANY (default) • LOGIN_METHOD_DEFAULT • LOGIN_METHOD_SSO

Available expression variables: **User Context variables** (_user.email, _user.username)
For instructions on including expressions, see Using Expressions in IF Conditions

If a user's account is older than

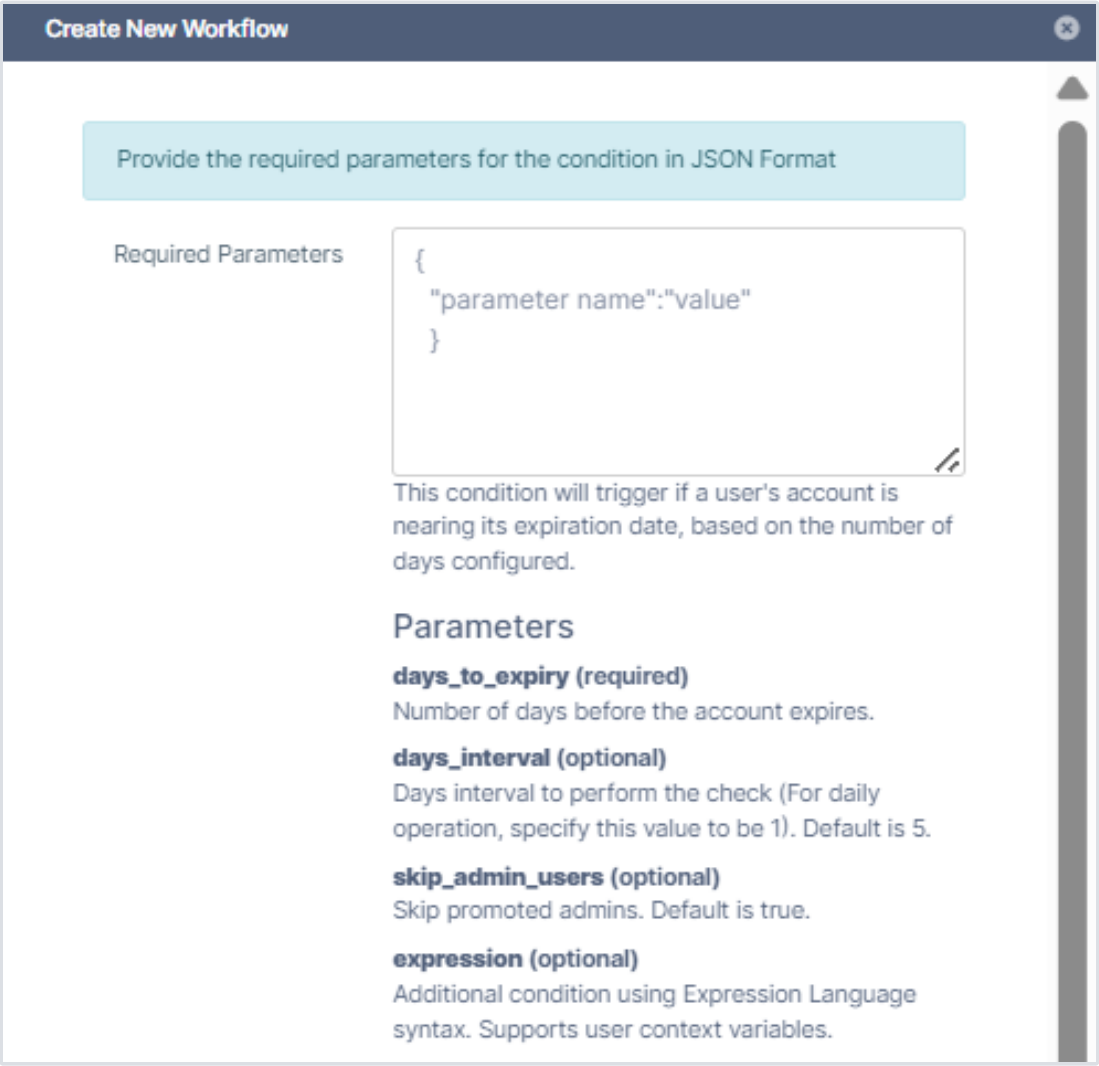


Workflow Condition	Parameters	Description

If a user's create date is older than
 	
Available in FileCloud Version 23.232
	`{`
	`"days": 30,`
	`"include_domain": "contractor.com",`
	`"exclude_domain": "subdomain.domain.com,@otherdomain.com"`
	`}`
	
	`For example, if a user's account was created more than 60 days ago and it is in the domain contractor.com`
	
	`{`
	`"days": 60,`
	`"include_domain": "contractor.com",`
	`}`
		This condition is triggered when a user's create date is older than the number of days specified in **days**.
		
		Parameters
		
		days - Required. When a user's create date is older than this number of days, the condition is triggered.

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

If a user's account is near its expiration date


Create New Workflow
Provide the required parameters for the condition in JSON Format
Required Parameters
{
"parameter name":"value"
}
This condition will trigger if a user's account is nearing its expiration date, based on the number of days configured.
Parameters
days_to_expiry (required)
Number of days before the account expires.
days_interval (optional)
Days interval to perform the check (For daily operation, specify this value to be 1). Default is 5.
skip_admin_users (optional)
Skip promoted admins. Default is true.
expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

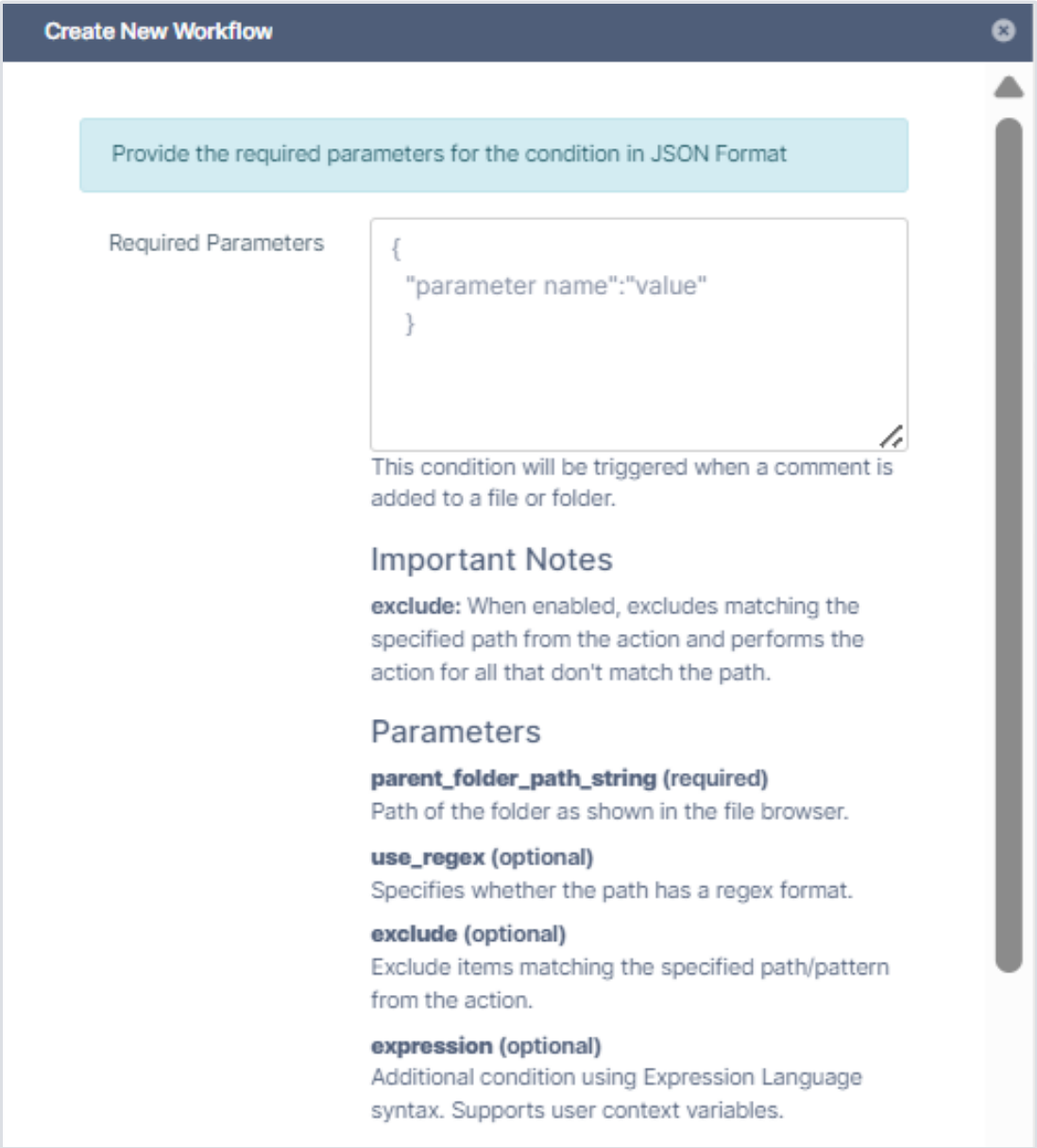
Workflow Condition	Parameters	Description

If a user's account is near its expiration date	`{`
	`"days_to_expiry": 10,`
	`"days_interval": 5,`
	`"skip_admin_users": 1`
	`}`
	
	For example, When a user's account is set to expire in 15 days, perform an action such as sending the user an email. Send the email again every 5 days, but the last 5 days, send the email every day. Do not perform the action on promoted admins.
	`{`
	`""days_to_expiry": 15,`
	`"days_interval": 5,`
	`"skip_admin_users": 1`
	`}`
		days_to_expiry - Number of days before account expiration
		days_interval - (optional)
		At what interval to perform the action again after it is performed the first time. During the last interval, the action is performed every day. Default is 5 days. For example:
		• Action is "Send an email"
		• days_to_expiry = 15
		• days_interval = 5
		An email is sent at 15 days before account expiration, 10 days before account expiration and 5, 4, 3, 2, and 1 days before account expiration.
		skip_admin_users Optional. Do not include promoted admins.
		0 (default) - Include promoted admins
		1 - Do not included promoted admins
		
		Interval Logic
		During the last interval, the action is executed every day. For example:
		• Action: "Send an email"
		• days_to_expiry = 15
		• days_interval = 5
		An email is sent at 15 days before account expiration, 10 days before account expiration and 5, 4, 3, 2, and 1 days before account expiration.

Other Conditions

If a comment is added

💡 **Comments can be added to files and folders.**



Workflow Condition	Required Parameters	Description

If a comment is added	*{ "parent_folder_path_string": "/userid/somepath", "use_regex":"1", "exclude":"1" }* Available expression variables: **User Context variables**. For instructions on including expressions, see Using Expressions in IF Conditions	This condition will be triggered when a comment is added **parent_folder_path_string** - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. **use_regex (optional)** - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") **exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

Perform an action periodically at specified time and interval

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
"parameter name":"value"
}
```

This condition will be triggered when the current time matches the supplied time.
day_interval : Days interval (For daily operation, specify this value to be 1)
time_string : (OPTIONAL) Time in format H:i:s (If not specified, it will run at 00:00:00)
start_date : (OPTIONAL) Start date in format yyyy-mm-dd (If not specified, it will start from today)
end_date : (OPTIONAL) End date in format yyyy-mm-dd (If not specified, it will run indefinitely)

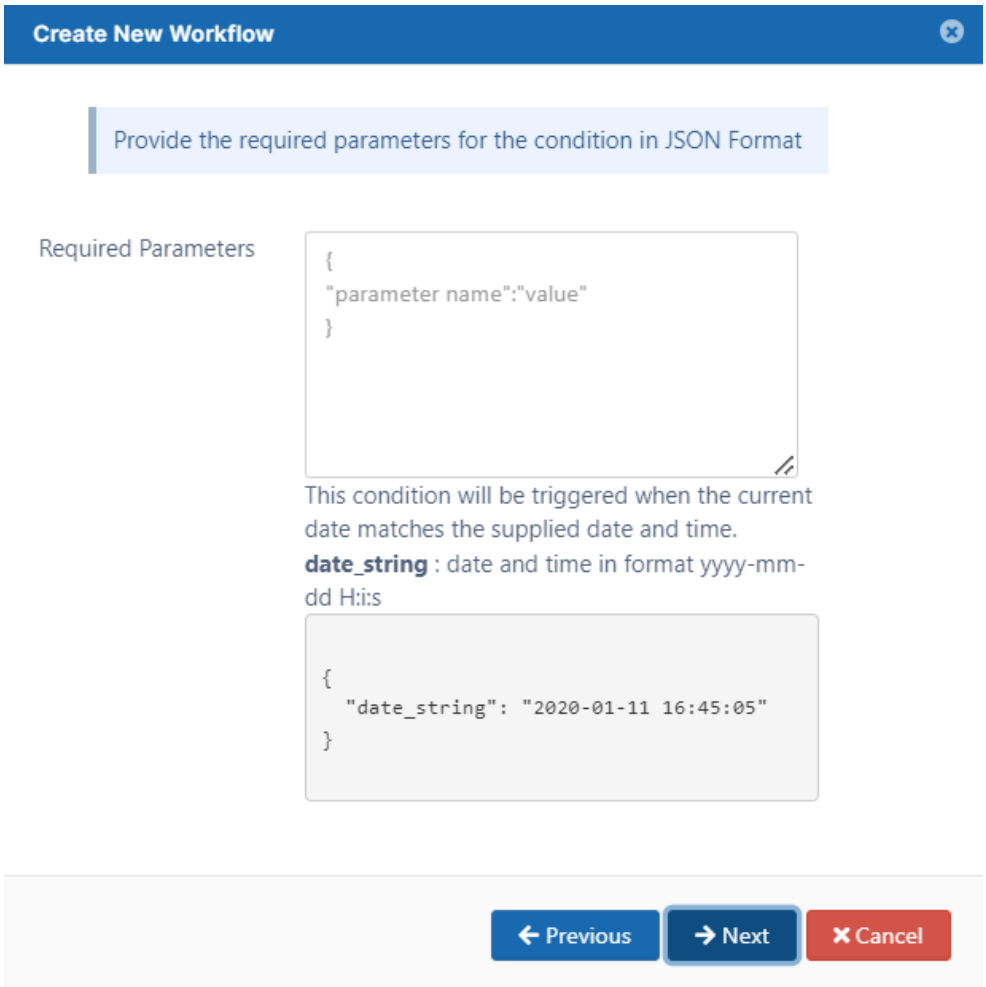
```
{
  "day_interval": 7,
  "time_string": "08:00:00",
  "start_date": "2020-01-01",
  "end_date": "2020-01-31"
}
```

Previous Next Cancel

Workflow Condition	Parameters	Description
Perform an action periodically at specified time and interval	*{ "time_string":"16:45:05", "day_interval":"7" }*	This condition will be triggered when the current time on the FileCloud Server matches the supplied time. **day_interval** - number of days that passes after a THEN action before it is triggered again. • The THEN action you choose will be triggered every "day_interval" days. • If the "day_interval" is 1, it is done daily **time_string** - the time of day when you want the THEN action triggered • The matching time includes the time zone • The time is specified in a 24-hour format of Hours, minutes, seconds **start-date** - Date that FileCloud begins checking for the condition **end-date** - Last date that FileCloud checks for the condition.

Available expression variables: **None.**

Perform an action on the specified date



Workflow Condition	Parameters	Description
Perform an action on the specified date	*{ "date_string":"2020-01-11" }*	When the date matches the supplied date and time, the THEN action you configure will be run. **date_string** - date and time in a 24-hour format • yyyy-mm-dd H:i:s

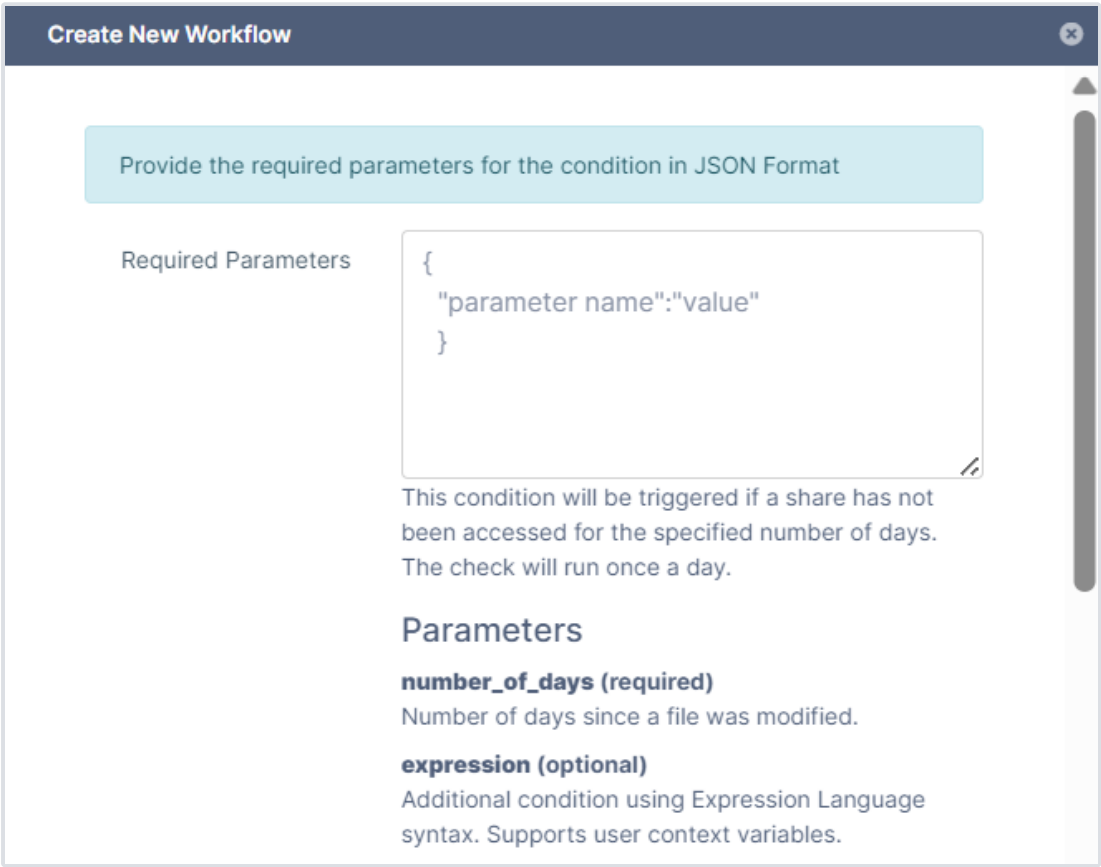
Available expression variables: **None.**

Perform an action periodically

Workflow Condition	Parameters	Description
Perform an action periodically	**None. The frequency depends on how you configure the cron or task scheduler frequency.**	This requires you to set up one of the following: • cron job • task scheduler

Available expression variables: **None.**

If share has not been accessed for specified days



Workflow Condition	Parameters	Description
If a share has not been accessed for specified days	*{ "share_permission": ["PUBLIC", "PRIVATE"], "number_of_days":"180", }*	This condition will be triggered when a shared file or folder has not been accessed for the specified number of days. • NOTE: The only supported action is *Delete share*. • This is useful for removing shared files that are no longer being used • This check will run once a day **number_of_days** - required to specify the number of days before the current date that a shared file was accessed. • This will be checked once a day and all files that match this condition will be subject to the THEN action you choose. • For example, if you specify the number of days as 15, all shared files or folders that have not been accessed in the last 15 days will subject to the the THEN action you configure.

Available expression variables: **Share Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions

Using Expressions in IF Conditions

> Expressions are available in FileCloud beginning in version 23.253.

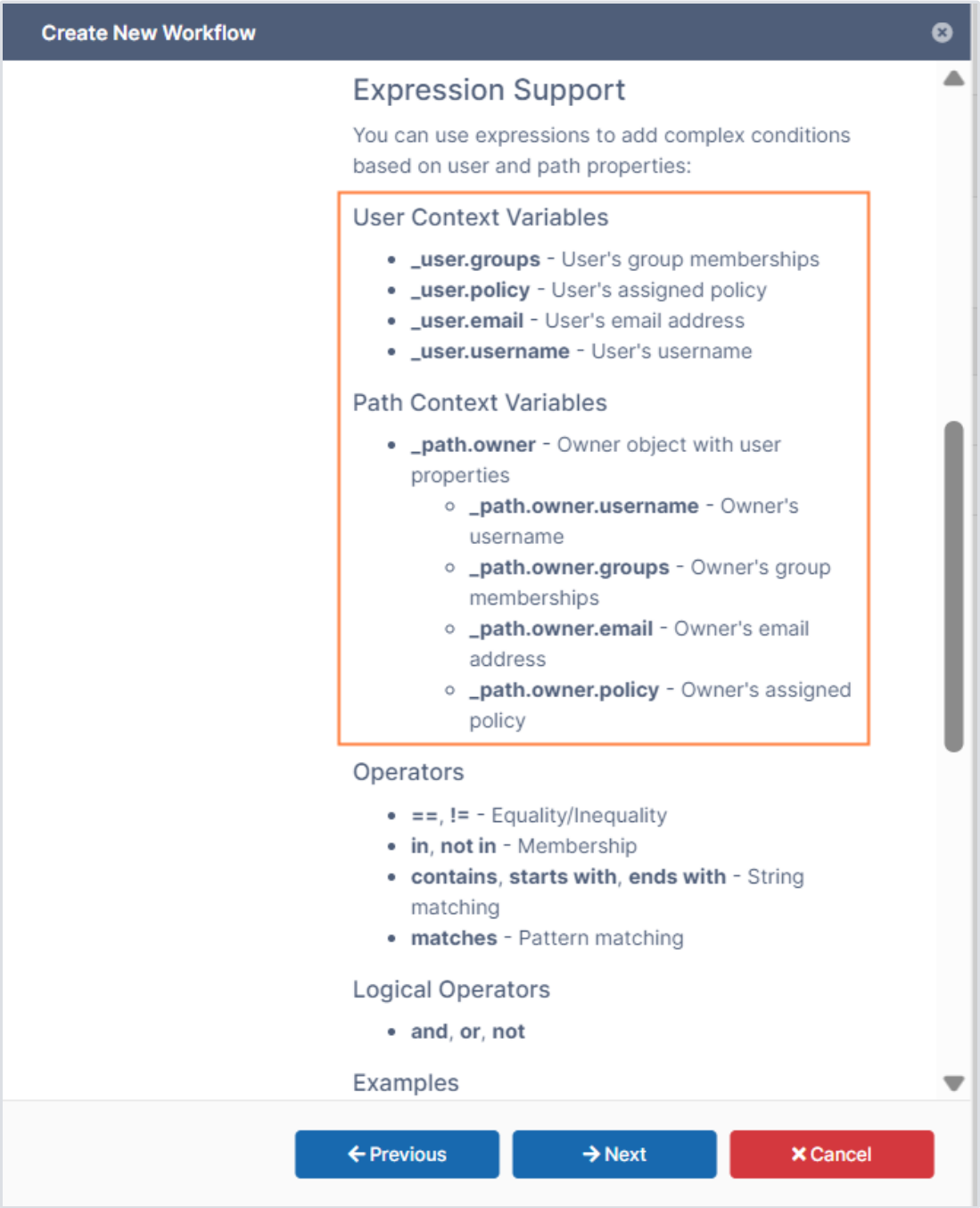
Many admin workflows allow you to set up custom conditions in workflows based on user, path owner, and share properties. These conditions (referred to as expressions) must be written in regular expression syntax. They greatly expand your ability to customize workflows.

For example, you can expand the IF statement in a workflow to check if a user is a member of a certain group or has a certain policy, or to check if a share is a folder or file share.

Specifically, the additional conditions available for you to include can be based on:

- the user's or the path owner's **group**, **policy**, **email (or domain)**, or **name**
- the share owner's **group**, **policy**, **email (or domain)**, or **name**, the type of share (**public or private)**, and the type of item shared (**folder vs. file**).

  The list of available expression variables for each workflow is shown in its wizard. You can view a list of all available variables in the tables under Guide to expression variables and operators, below.
  As an example, in the following workflow, which uses the IF condition **If a file is added or updated**, the user and path context variables are supported, but not the share context variables. Below the variables, the available regular expression operators and examples are listed.



The examples help you use the proper syntax when adding conditions:

Examples

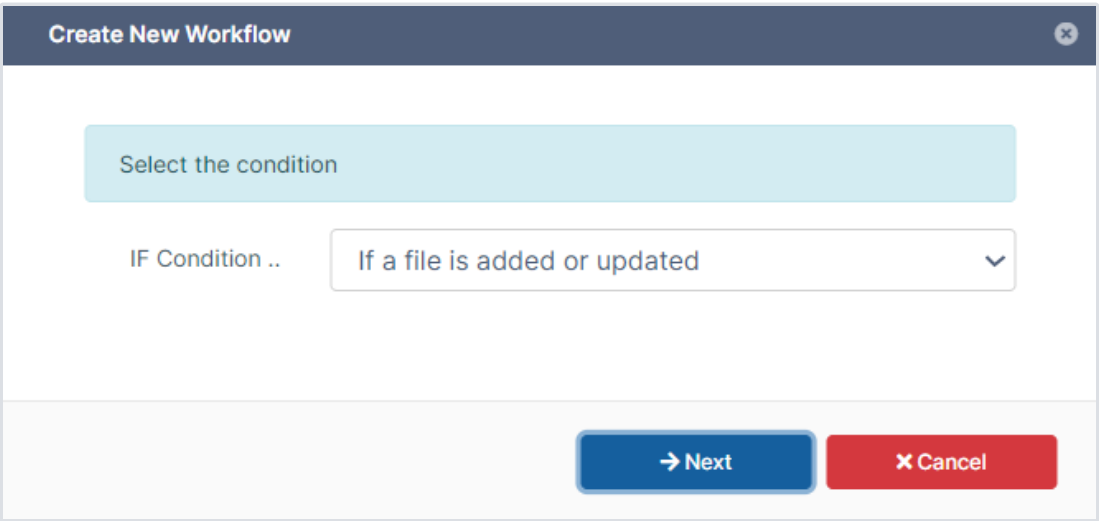
- **'Admin Group' in _user.groups** - User must be in Admin Group
- **_user.policy == 'AdminPolicy'** - User must have Admin Policy
- **'Admin' in _path.owner.groups** - Path owner must be in Admin group
- **_path.owner.policy == 'AdminPolicy'** - Path owner must have Admin policy
- **_user.username == _path.owner.username** - Current user is the path owner
- **_path.owner.email ends with '@company.com'** - Owner must be from company domain
- **'Manager' in _user.groups and _path.owner.username != 'admin'** - Complex condition example

The variables available depend on the workflow, and not all workflows have variables available.

To create an IF statement with an expression condition

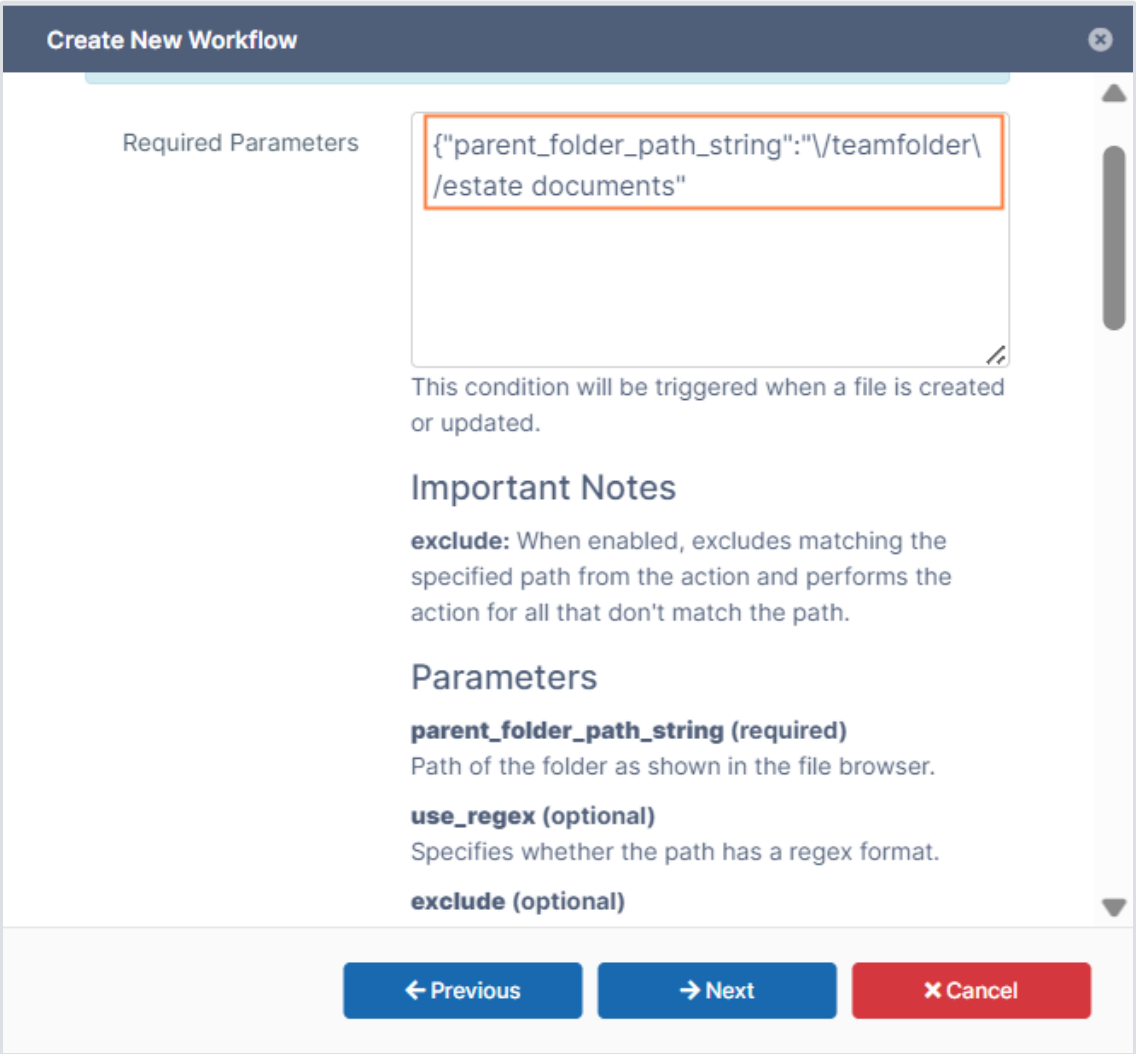
The IF statement we are setting up in this example uses an expression to specify a user's group and policy. The IF statement requires that the user who added or updated a file must also be in the group **TeamMember** and have the policy **Staff**.

1. In the admin portal, go to the Workflows page, and click **Add Workflow**.
2. In the Create New Workflow dialog box, choose an IF condition.
   This example uses the condition **If a file is added or updated**.

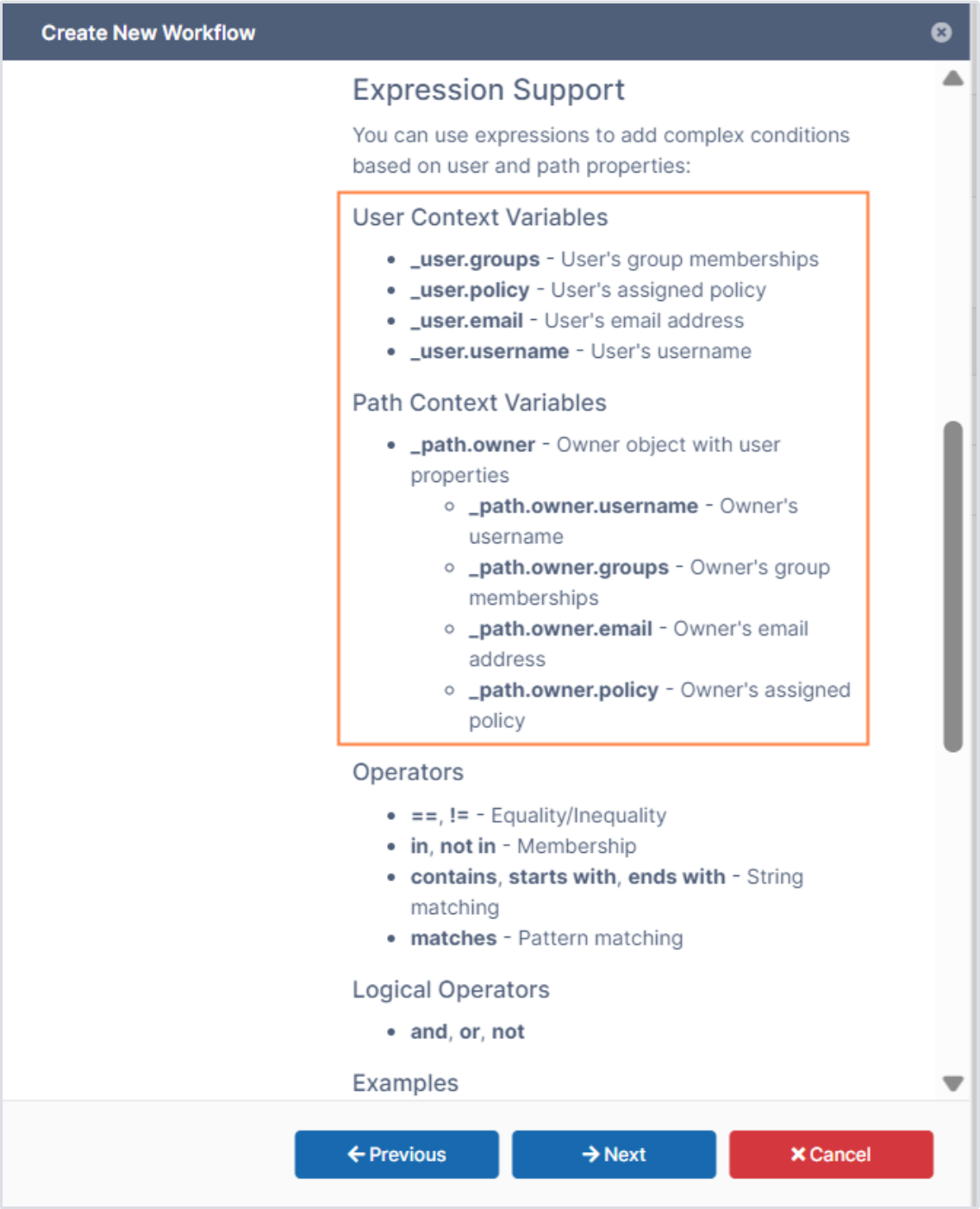


3. Click **Next**.

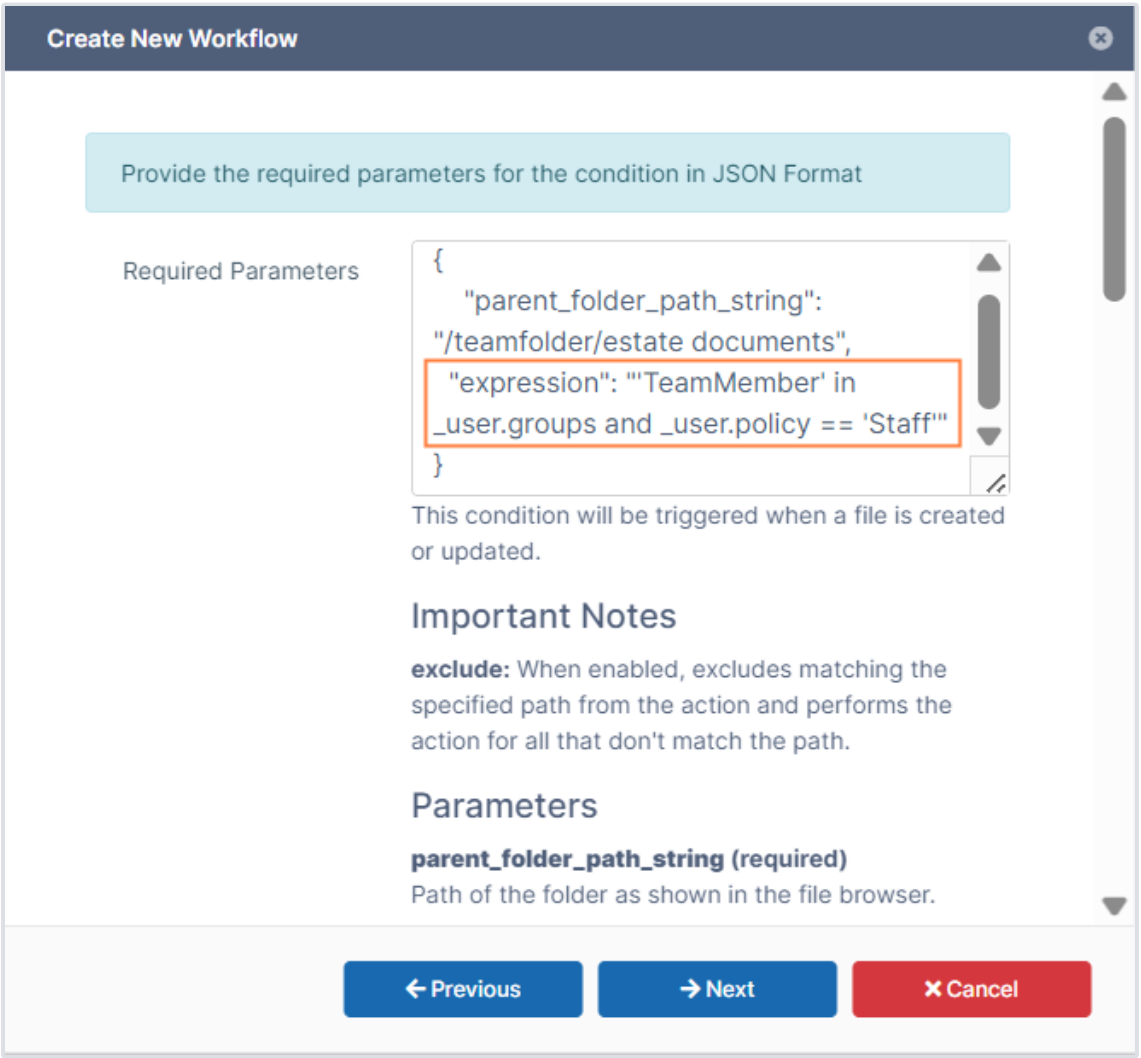
4. The only required parameter is **parent_folder_path_string**, so begin by entering it into the **Required Parameters** box.
   This example uses the Team Folder **estate documents**.



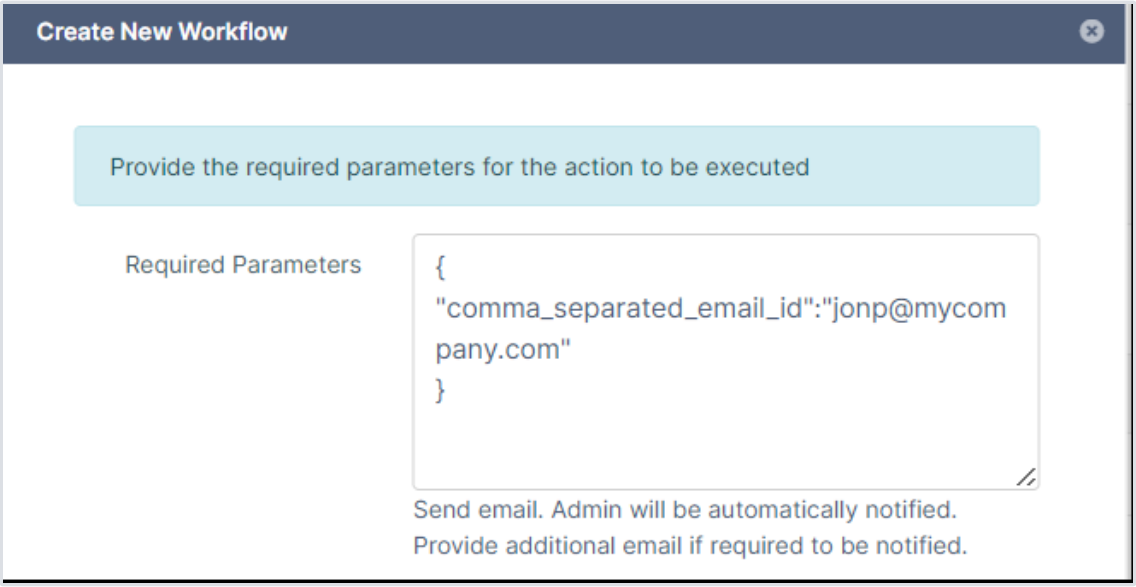
   Scroll down to **Expression Support** to see the supported context variables. In this case the user and path context variables are supported.
   To specify the user's group and policy, use the variables **_user.groups** and **user.policy**.



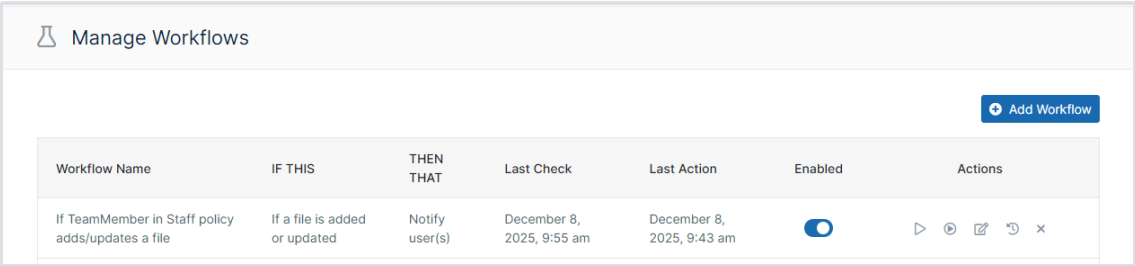
5. Add the variables and values.



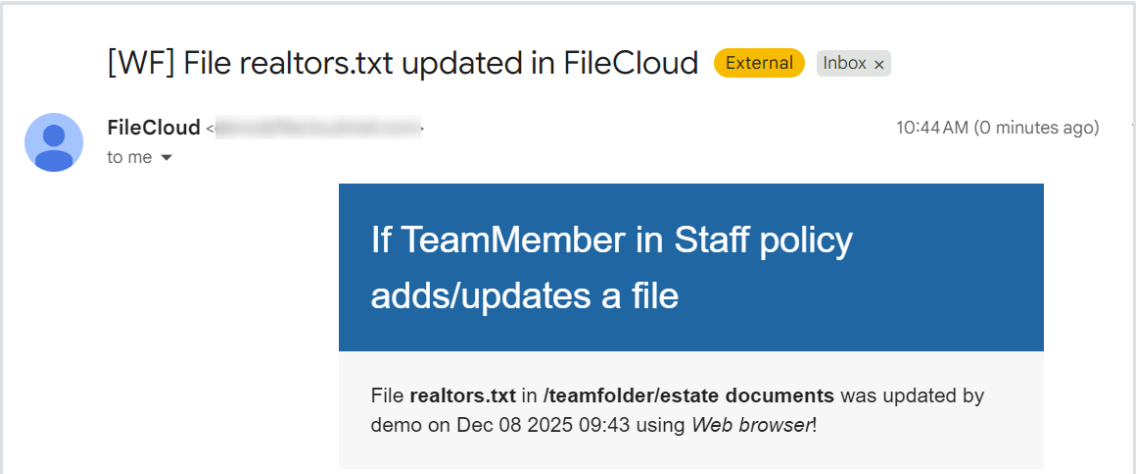
6. Click **Next**.
7. Choose the appropriate THEN action, and add the parameters.
   This example uses a THEN action that sends an email to a specific user, and specifies the user's email address.



8. Click **Next**, and enter a name for the workflow, then click **Finish**.
   The workflow is saved.



9. Test the workflow by having a user in the **TeamMember** group who has the policy **Staff** add or update a file in the Team Folder **estate documents**.
   The user specified will receive an email notification similar to the following one if the workflow is effective:



Guide to expression variables and operators

The tables below show the variables and operators supported in regular expressions when used with IF/THEN workflows in FileCloud. For examples using regular expression syntax with these variables and operators, see the wizard for adding each workflow.

User Context Variables	
_user.groups	User's groups
_user.policy	User's policy
_user.email	User's email address
_user.username	User's username
Path Owner Context Variables	
_path.owner.username	Path owner's username
_path.owner.groups	Path owner's groups
_path.owner.email	Path owner's email
_path.owner.policy	Path owner's policy
Share Context Variables	
_share.owner.username	Share owner's username
_share.owner.groups	Share owner's groups
_share.owner.email	Share owner's email
_share.owner.policy	Share owner's policy
_share.public	If share is public, true; if share is not public, false.
_share.private	If share is private, true; if share is not private, false.
_share.is_dir	If this is a folder share, true; if this is a file share, false.

Operators	
==, !=	equal/not equal
in, not in	is a member of/is not a member of
contains, starts with, ends with	string contains, string starts with, string ends with
matches	pattern matches

Logical Operators
and
or
not

Define a THEN Action

> Not all THEN actions are compatible with all IF conditions. Please see the table below for compatible settings.

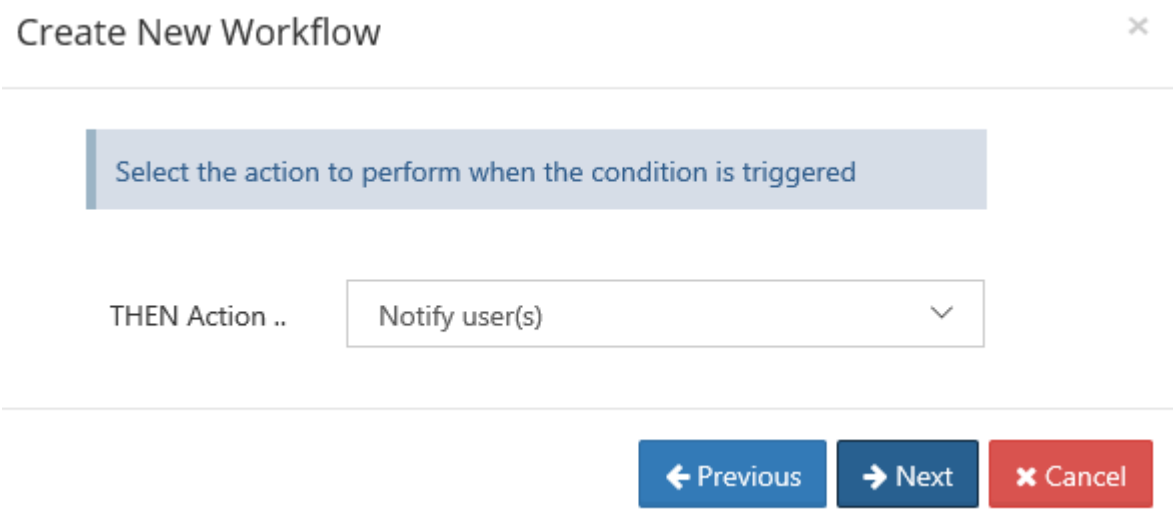
Once you select an IF Condition, compatible THEN Actions can be selected.

- Actions are performed if the associated Condition is triggered.

Some Actions may require you to specify parameters, such as a specific date or time.

Where do I set up the Action?

When you create a new Workflow, after you select a condition and specify parameters, then you can select an Action.



Where do I add my parameters?

After you select an Action, then you can enter any parameters, such as a date or time.

If you need more information about what parameters are required, look below the Required Parameters box.

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{
"parameter name":"value"
}
```

Send email. Admin and user will be automatically notified. Provide additional email if required to be notified.
comma_separated_email_id:Email ids in comma separated format as shown below
{
"comma_separated_email_id":"xyz@a.com,abc@b.com"
}

Previous Next Cancel

THEN Actions

Notifications

Action and		Details	Compatible IF conditions
Notify the user that the account may be deactivated soon	None	Notifies the user that the account may be disabled or deleted due to inactivity.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Notify user(s)	{ "comma_separated_email_id":"xyz@a.com,abc@b.com" , "comma_separated_group_name":"Group A,Group B" }	Sends email notifications to the emails listed and to the users in the groups listed. **comma_separated_email_id** - email ids in comma separated format **comma_separated_group_name**: Group names in comma separated format.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date If a new client app connects If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created

Action and		Details	Compatible IF conditions

Send an email	{
	"subject": "Subject of the email",
	"body": "Body of the email in HTML format.",
	"is_html": 1,
	"users": "user1,user2",
	"groups": "group1,group2",
	"notify": 0
	}
		Sends a customized email to the users and/or groups indicated
		subject - Subject of the email
		body - Body of the email
		is_html (optional) - 1 if the body is in HTML format; 0 if the body is in plain text format. Default is 0. **Note**: If **is_html=1**, HTML tags are interpreted and the body of the email is formatted. For example, you can insert tags to make text bold.
		users (optional) - Comma separated list of users to send the email to.
		groups (optional) - Comma separated list of groups to send the email to.
		notify (optional) - 1 to automatically send the email to users impacted by the related action; 0 to not automatically send them the email. Default is 0.
			Click to see if conditions
			If a file is created
			If a folder is created
			If a file is updated
			If a file is deleted
			If a folder is deleted
			If a file is downloaded
			If a comment is added
			If a file was not modified for specified days
			If a file is added or updated
			If the file uploaded is bigger than the expected size
			If the file uploaded is bigger than the expected size
			Perform an action periodically at specified time and interval
			Perform an action on the specified date
			Perform an action periodically
			If a new user is created
			If a user's account is older than
			If a user's last login is older than
			If a user's account is near its expiration date

File actions

Action	Parameters	Details	Compatible IF conditions
Copy the file(s) to some location	{ "target_path": "/usera/folderb/", "allow_overwrite": 1, "keep_folder_structure": 1 }	Copies files. **target_path** - path to copy the file to. • This path must be in the same storage type • Files cannot be copied from managed storage to network shares or vice versa. **allow_overwrite** - (Added in FileCloud 20.1) Optional. Allow file to overwrite existing files with the same name in the target path. If allow_overwrite is not included, overwrites are allowed. **keep_folder_structure** (Optional): Keep folder structure while copying files. Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided. The placeholders. %who, %when, %path, %how, %filename are available for this action.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a comment is added

Action	Parameters	Details	Compatible IF conditions
Delete the file(s)	{ "delete_empty_folders":1, "notify_owner":0, "comma_separated_email_id":"email1@email.com,email2@email.com", "comma_separated_group_name":"Group A,Group B" }	Deletes matching files. **delete_empty_folders (Optional)**: When files are deleted, delete the parent folder as well if it is empty. **notify_owner (Optional)**: When the files are deleted, send an email to the owners. **comma_separated_email_id (Optional)**: Email ids in comma separated format. **comma_separated_group_name (Optional)**: Group names in comma separated format.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a comment is added

Action	Parameters	Details	Compatible IF conditions
Move the file(s) to some location	{ "target_path": "/usera/folderb/", "allow_overwrite": 1, "keep_folder_structure": 1 }	Moves files. **target_path** - Path to the new file location (where it should be moved). • This path must be in the same storage type • Files cannot be moved from managed storage to network shares or vice versa. **allow_overwrite** - (Added in FileCloud 20.1) Optional. Allow file to overwrite existing files with the same name in the target path. If allow_overwrite is not included, overwrites are allowed. **keep_folder_structure** (Optional): Keep folder structure while moving files. Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided. The placeholders. %who, %when, %path, %how, %filename are available for this action. ⚠️ Currently, if creation/update of a file in FileCloud via WOPI triggers a move file workflow, the move fails.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is deleted If a comment is added
Release locks (added in FileCloud 22.1)	{ "days": 7 }	Releases locks on files and folders. **days** - Number of days after a lock was created on a file or folder to release it.	Click to see if conditions Perform an action periodically at specified time and interval Perform an action on the specified date Perform an action periodically If a user's create date is older than

Action	Parameters	Details	Compatible IF conditions
Verify file integrity and generate admin alert on mismatch	{ "ignore_file_size_in_mb": 10 }	Attempts to identify the file type based on its content and checks if it matches the extension. • If the file type does not match, then generate admin portal alert. Optional **ignore_file_size_in_mb**: - Do not scan files larger than this limit specified in megabytes. **Note:** By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deletedIf a comment is added

Verify file integrity and delete on mismatch	{ "ignore_file_size_in_mb": 10 }	Attempts to identify file type based on its content and checks if it matches its mime type.
		• A MIME type is a string identifier composed of two parts: a "type" and a "subtype".
		• If the file type does not match, then
		  • the latest version is deleted
		  • users listed in the parameter are notified
		Optional
		ignore_file_size_in_mb: - Do not scan files larger than this limit specified in megabytes.
		
		Note: By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check.
			Click to see If conditions
			If a file is created
			If a file is updated
			If a file is deleted
			If a file is downloaded
			If a file was not modified for specified days
			If a file is added or updated
			If a file uploaded is bigger than expected size
			If a file downloaded is bigger than expected size
			If a folder is created
			If a folder is deleted
			If a comment is added

Reporting

Action	Parameters	Details	Compatible IF conditions
Run a report	{ "report_name": "my_report", "comma_separated_email_id": "a@x.com,b@y.com", "comma_separated_group_name": "Group A,Group B" }	Opens a saved report, runs it, and then sends the results in email. 💡 This action requires you to have already created the report from the Admin dashboard. Create a Custom Report **report_name**: Name of the report to run. The report must already be created in the reports section and that exact report name must be provided here. **comma_separated_email_id**: Comma separated email ids to be notified after report is run **comma_separated_group_name (Optional)**: Group names in comma separated format.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date If a comment is added Perform an action periodically at specified time and interval Perform an action on the specified date Perform an action periodically

Action	Parameters	Details	Compatible IF conditions
Generate an email report	{ "comma_separated_email_id":"xyz@a.com,abc@b.com" , "comma_separated_group_name":"Group A,Group B" }	Sends an email to the specified addresses with information about the users matching the criteria. **comma_separated_email_id** - email ids in comma separated format **comma_separated_group_name**: Group names in comma separated format.	Click to see If conditions If a user's last login is older than . . . If a new user is created (if the user account was created by the user; not applicable if the user account was created by an admin) If a user's create date is older than If a user's account is near its expiration date

Modifying users

Action	Parameters	Details	Compatible IF conditions
Disable user account	{ "comma_separated_email_id":"xyz@a.com,abc@b.com" , "comma_separated_group_name":"Group A,Group B", "donot_email_user": 0 }	Disables the user account and then sends an email with information about the action performed. **comma_separated_email_id** - email IDs in comma separated format **comma_separated_group_name**: Group names in comma separated format. **donot_email_user (optional)**: Do not send email to the user affected (1 or 0). Default 0. **Note**: To customize the email sent to the user, go to Customization > Email Templates and edit the template **Workflow Auto Disable Account Email Template**.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Action	Parameters	Details	Compatible IF conditions
Delete user account	{ "comma_separated_email_id":"xyz@a.com,abc@b.com", "comma_separated_group_name":"Group A,Group B", "donot_email_user": 0 }	Deletes the user account and then sends an email with information about the action performed. **comma_separated_email_id** - email IDs in comma separated format **comma_separated_group_name**: Group names in comma separated format. **donot_email_user (optional)**: Do not send email to user affected (1 or 0). Default 0.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Change user status	{ "user_status": "USER_ACCOUNT_LIMITED_ACCESS", "mark_as_verified": 0, "comma_separated_email_id": "xyz@a.com,abc@b.com", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }	**user_account_type -** type of account. You must use one of the following values: • USER_ACCOUNT_DISABLED_ACCESS • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (external access) **mark_as_verified** (optional) - marks the account as verified, so that the user can log in immediately without waiting for the admin to send the verification email. **comma_separated_email_id** - email IDs in comma separated format **comma_separated_group_name**: Group names in comma separated format. **donot_email_user** (optional) - prevents an email from being sent to the user affected when the status is changed • 1 = Does not send an email • 0 = Sends an email • If nothing is specified, the default is 0	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Action	Parameters	Details	Compatible IF conditions
Set user group	{ "group_name":"Group1,Group2" }	Assigns user to groups. **group_name** - Comma separated list of groups to assign user to.	If a new user is created If a user's create date is older than If a user's account is near its expiration date
Set user policy	{ "policy_name":"SamplePolicyName", "comma_separated_email_id": "", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }	Sends an email notification to the listed users that the user's policy was set as the specified policy **policy_name** - Name of policy to set **comma_separated_email_id** - email ids in comma separated format **comma_separated_group_name**: Group names in comma separated format. **donot_email_user** **0** (default) send the emails **1** do not send the emails	If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Set user properties	{ "policy_name":"SamplePolicyName", "user_status":"USER_ACCOUNT_LIMITED_ACCESS", "comma_separated_email_id": "", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }	Sends an email notification to the listed users that the user's policy was set as specified and the user access was set as specified **policy_name**: Name of policy to set. **user_status (optional)**: User status to set. (USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS (external access)) **comma_separated_email_id (optional)**: Comma separated emails to notify of workflow action. **comma_separated_group_name (Optional)**: Group names in comma separated format. **donot_email_user (optional)**: Set to 1 to prevent system from notifying user.	If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Share actions

Action	Parameters	Details	Compatible IF conditions
Delete the share(s)	*None*	Delete the share.	Click to see If conditions If a share has not been accessed for specified days

Device actions

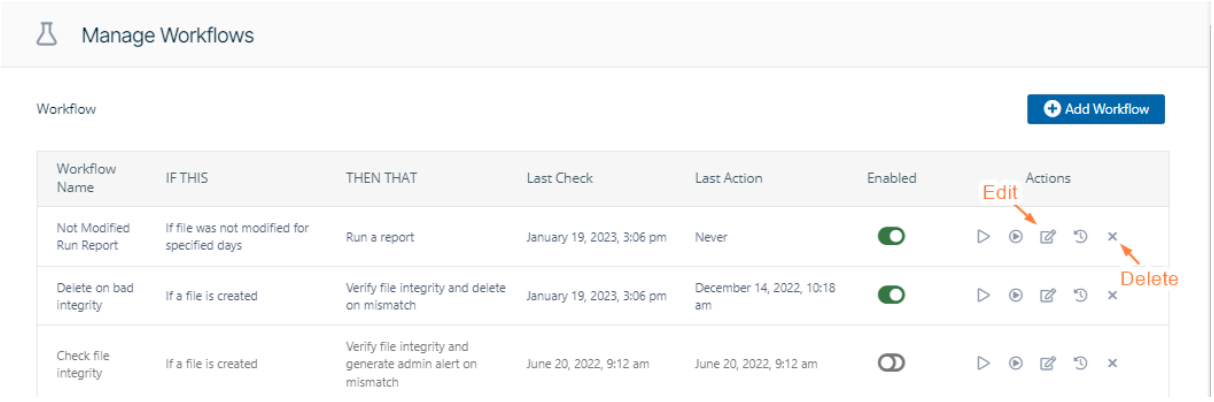
Action	Parameters	Details	Compatible IF conditions
Block the device for admin approval	*None*	Blocks the device and marks it with "Needs Approval" on the Manage Devices screen	Click to see If conditions If a new client app connects

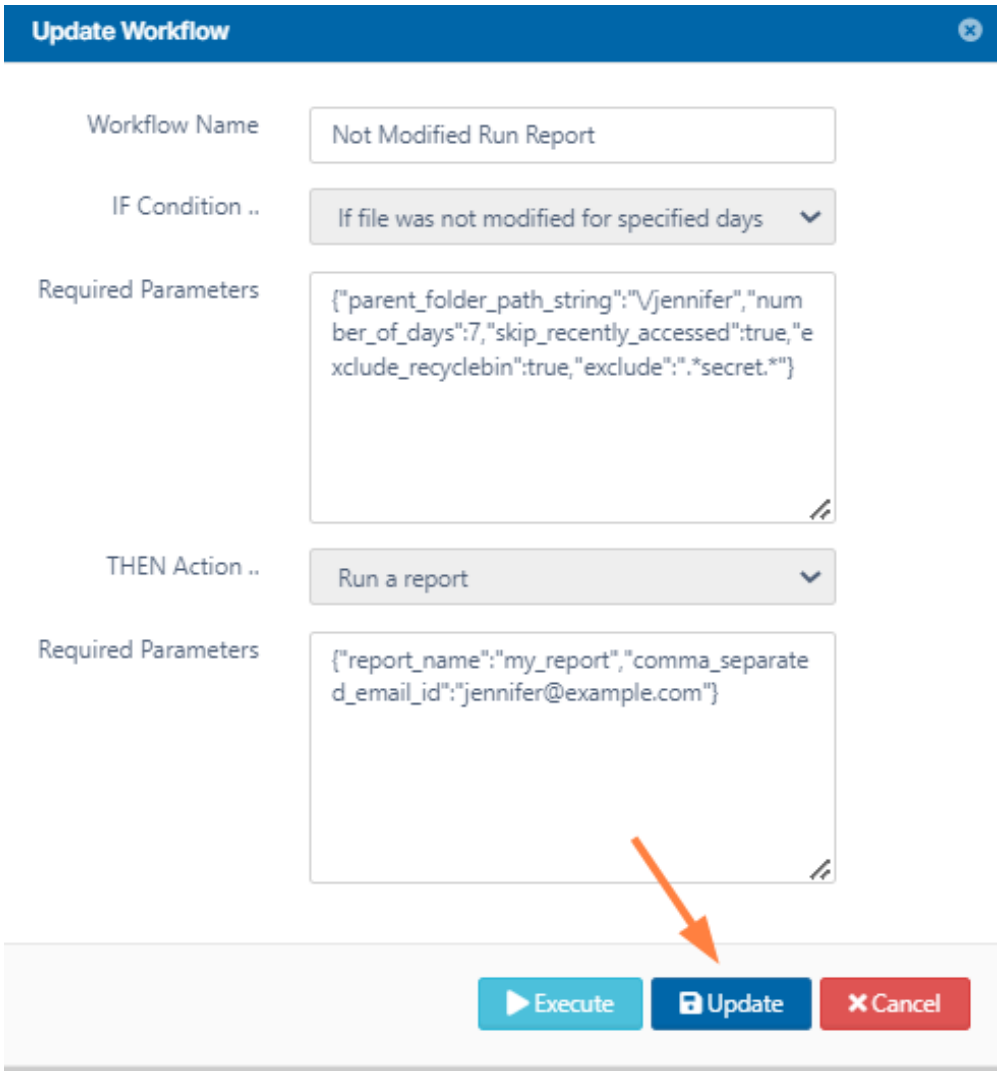
Edit a Workflow

It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and set up correct workflows.

Administrators can edit workflows to change the name or parameters of the conditions and action.

To edit, click on the Edit button; to delete, click on the Delete button.





Run a Workflow

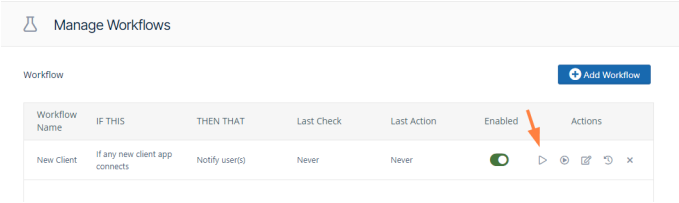
> It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

Administrators can run a workflow manually from the **Manage Workflows** screen.

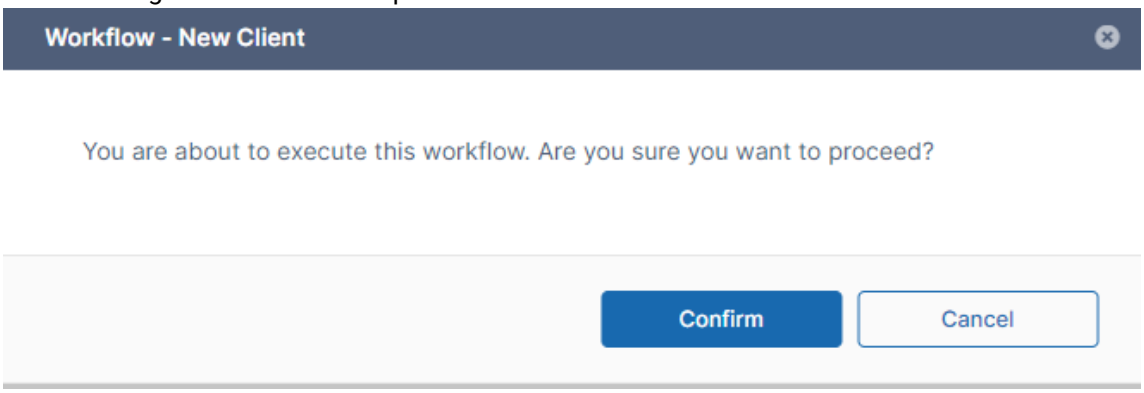
To run a workflow manually:

1. In the FileCloud admin portal's navigation panel, click **Workflows**.

2. In the Manage Workflows screen, in the row for the workflow you want to run, click the first arrow under **Actions**.



The following confirmation box opens.



3. Click **Confirm**.
   A screen notification confirms that the workflow ran successfully.

Set Advanced Workflow Options

> It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

Administrators can create and run more advanced scenarios., such as:

- regular expression in path matching
- the ability to pass additional, runtime-resolved data between conditions and actions

What scenario do you want to use?

Regular Expressions and Path Matching

You can enable regular expression matching in workflows by setting the **use_regex** parameter to **"1"** in the condition definition. This is an optional parameter and by default is **"0"** (don't use regular expressions - use strict match instead). If regular expressions are enabled you must provide a valid regular expression pattern as the **parent_folder_path_string** value. This pattern is used in the condition resolution process to find all matching paths (files / folders).

Regular expressions are supported by the following workflow conditions:

- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated

Parameters definition - example

Strict match

```
{
"parent_folder_path_string":"/userid/somepath",
}
```

or

```
{
"parent_folder_path_string":"/userid/somepath",
"use_regex":"0"
}
```

Regular expression

```
{
"parent_folder_path_string":"/userid/somepath",
"use_regex":"1"
}
```

Usage - Example

For simplicity sake assume that Administrator wants to send email notifications whenever someone downloads a file from a given location. The following example shows the difference between *strict match* and *regular expression match*

Strict match

Parameters are defined as follows:

```
{
"parent_folder_path_string":"/userA/downloads",
}
```

For such defined condition action will be triggered whenever a files is downloaded directly from the "/userA/downloads" directory and only from this one.

Regular expression

In this case the definition might look something like:

{
*"parent_folder_path_string":"**~/.*/downloads~**",*
"use_regex":"1"
}

For this condition action will be triggered for **all** directories that match the /user/download format, i.e. /userA/downloads, /userB/downloads, etc. This is a huge change that enables Administrators to define much more universal workflow scenarios.

Important
Regular expression patterns aren't validated for correctness. Please double check them, especially when dealing with the data-changing actions (i.e. delete files / move files, etc.).

RegEx Patterns
Regular expression definition has to start and end with one of the following characters:
'/', '~', '@', ';', '%', '`'
We strongly advise against the / usage as it adds confusion to the pattern definition.

Reversed Path Matching

The **Exclude** parameter enables the "reversed" path matching. That means that the specified action will be triggered for all files / folders whose path **doesn't match**. It's another huge change that allows administrators to define a new set of workflow. This is a very flexible and poweful feature, especially when combined with regular expressions.

Exclude parameter is supported by the following conditions:

- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated

Example

Administrator wants to delete all files that were downloaded form the FileCloud, but wants to keep files in one particular location - /userA/prevented. Condition should be then defined as:

{
"parent_folder_path_string":"/userA/prevented",
"exclude":"1"
}

The match condition will be reversed, so action will be triggered for all files, except the ones located in this particular directory.

Regular Expressions
For a regular expression it is very important to understand that if it is invalid it will return a **NOT MATCH** result for all paths. Administrators have to be very careful when using exclude parameter with regular expressions, especially for a data sensitive operations.

Runtime Resolved Parameters

Runtime resolved parameters are available in Workflows.

The runtime resolved parameters can be specified in the following IF conditions:

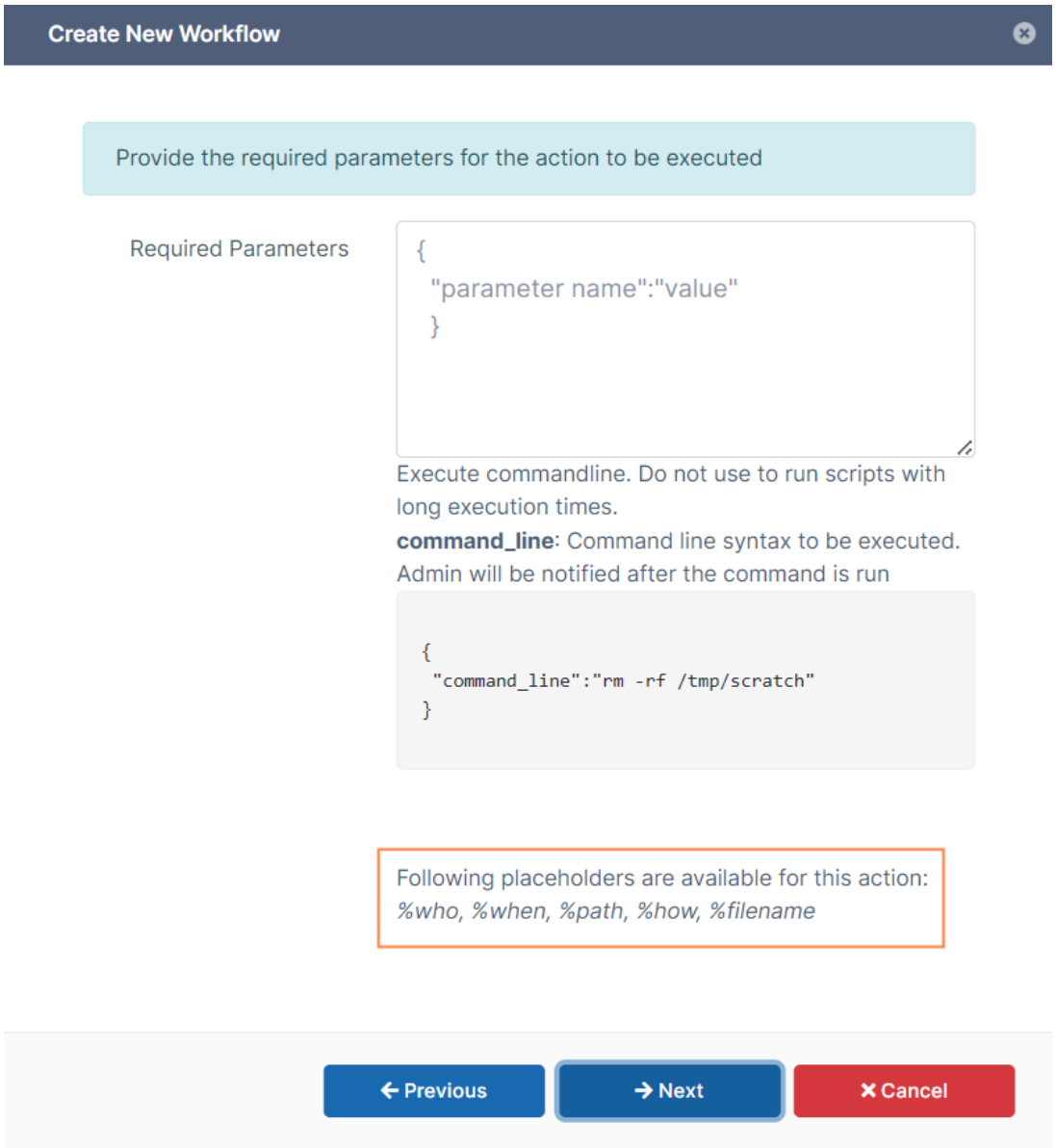
- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated
- if the file updated is bigger than the expected size
- if the file downloaded is bigger than the expected size

and then used in all compatible THEN actions.

Currently FileCloud supports the following placeholders only for file/folder related conditions.

- **%who** - user who performed the action that triggered the condition (for example, file upload or download)
- **%when** - time of the action
- **%path** - path of the file/folder
- **%how** - user agent of the performed action (for example, a browser type)
- **%filename** - name of the file

If the selected IF condition is able to implement runtime resolved parameters they are listed in the THEN action dialog box.



Example - how condition resolves parameters
Assume that **user1** downloaded a file **file1.pdf** from the **/user1/test** folder through a **Firefox** browser on **4pm** on the **01.01.2018**.
Condition will resolve all the parameters and pass it to the action:

- **%who** - user1
- **%when** - 2018-01-01 16:00:00
- **%path** - /user1/test/file1.pdf
- **%how** - Web browser

- **%filename** - file1.pdf

Recommended usage
Although it is possible to use resolved parameters in all compatible actions, this feature was designed and implemented mainly for the **command execution** action.

Workflow Recipes for FileCloud

You can create custom workflows to perform a variety of actions.

Workflows operate using the following model:

- IF CONDITION - THEN ACTION (IFTTT)

Since there are many different ways to create custom workflows, this page provides you with some simple recipes to create a specific workflow.

- Using some of these recipes will help you learn how a workflow functions
- After using some recipes you should be able to understand how to create your own workflows

In this section:

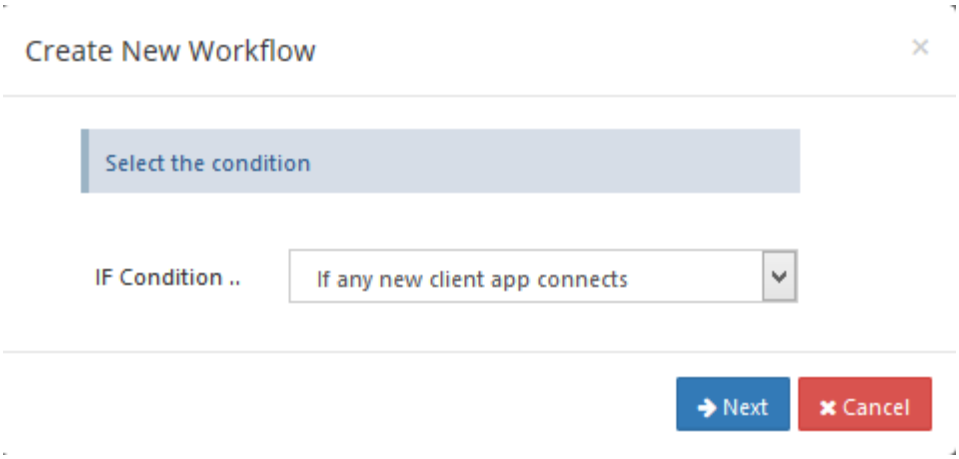
Admin Approval Required Workflow

This workflow recipe blocks the connection of a new app or device until it is approved by an administrator.

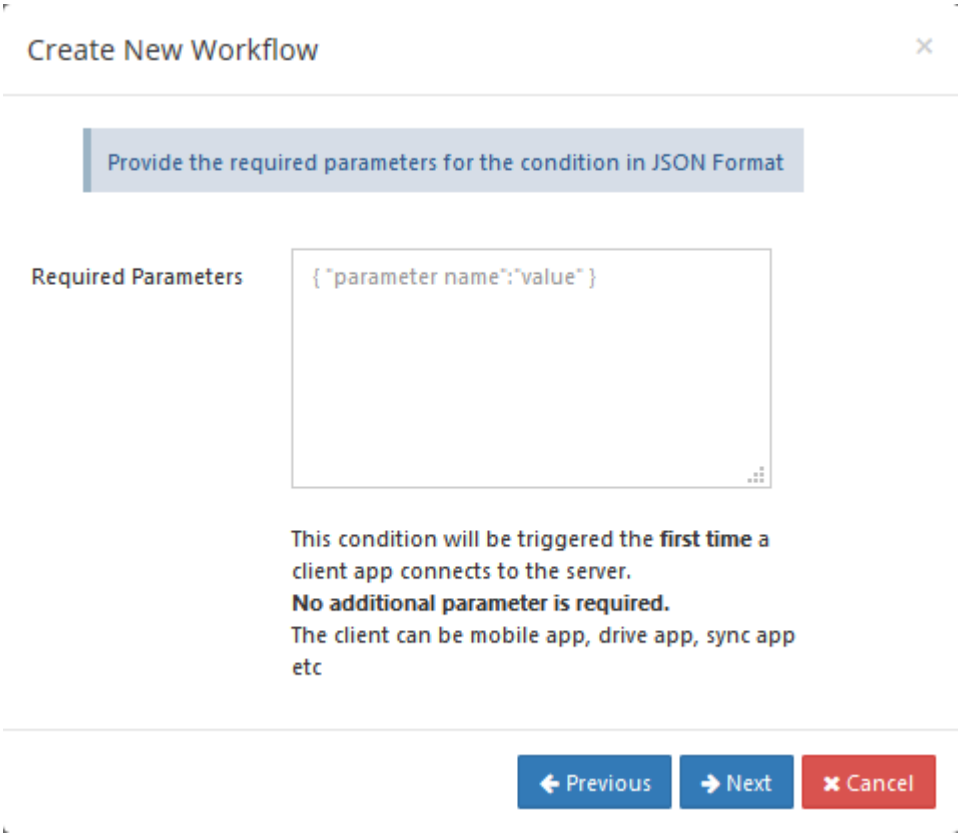
- When a new app or device tries to connect to FileCloud, the action is unblocked ONLY after admin approval.
- In the Admin Portal, you can see the devices in BLOCKED status, awaiting ADMIN approval.

To create a workflow that requires admin approval for all clients:

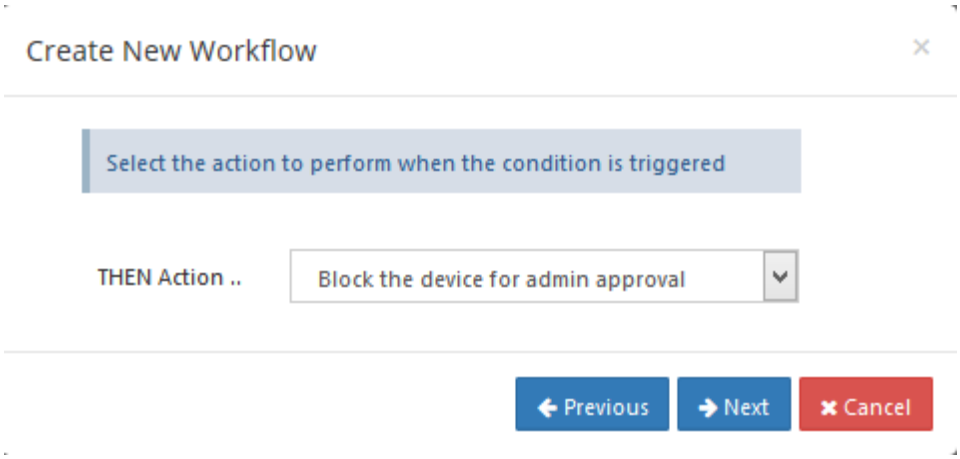
1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition "**If any new client app connects**"



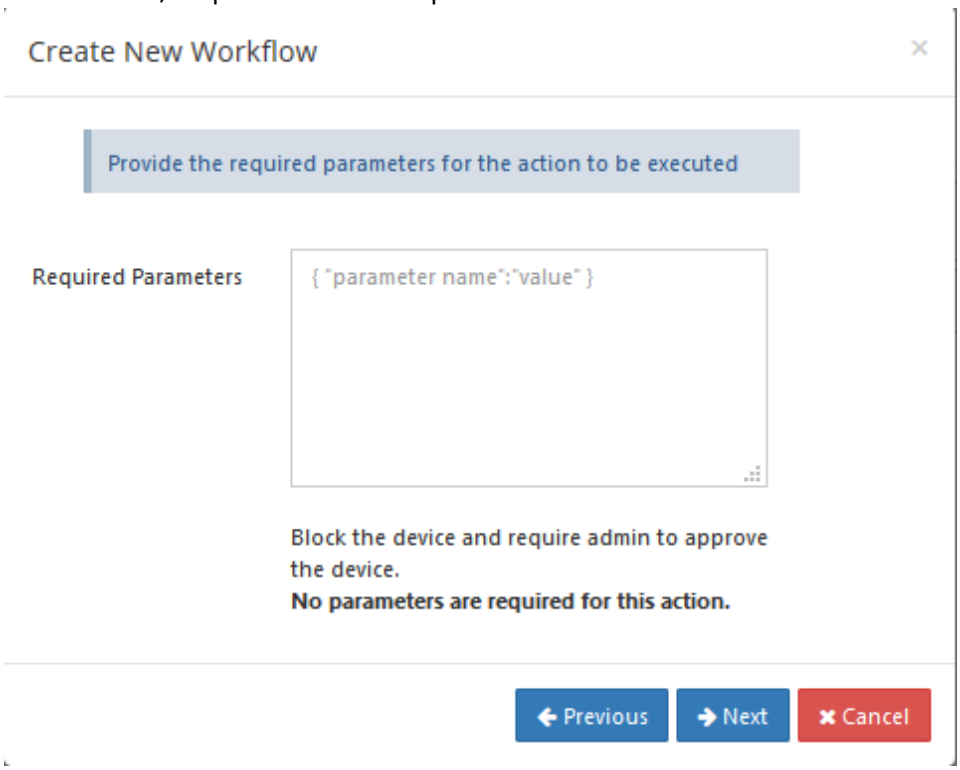
5. Click Next, no required parameters are to be given as ,the condition triggers for any client app that connects to FileCloud.



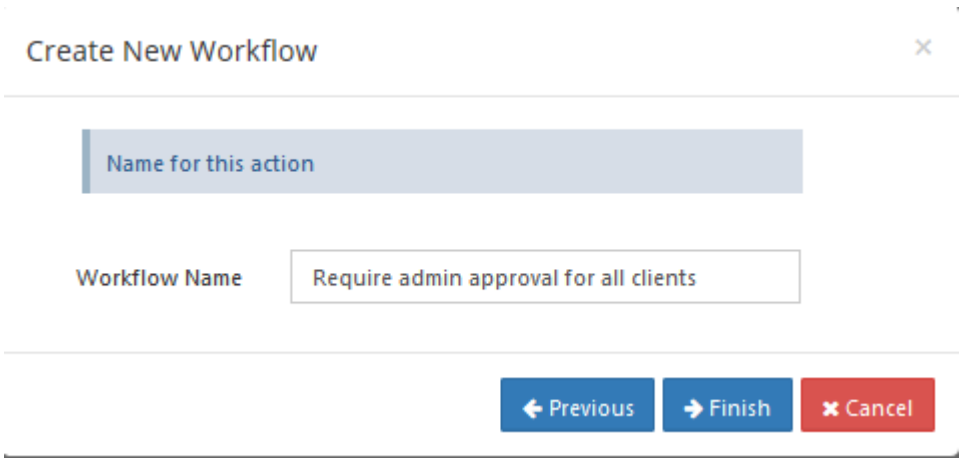
6. Click Next, to give the THEN action



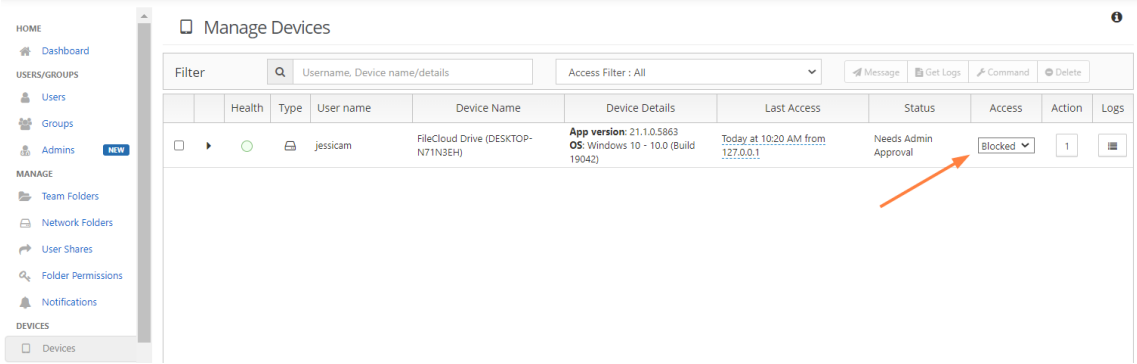
7. Click on Next, No parameters are required for this action



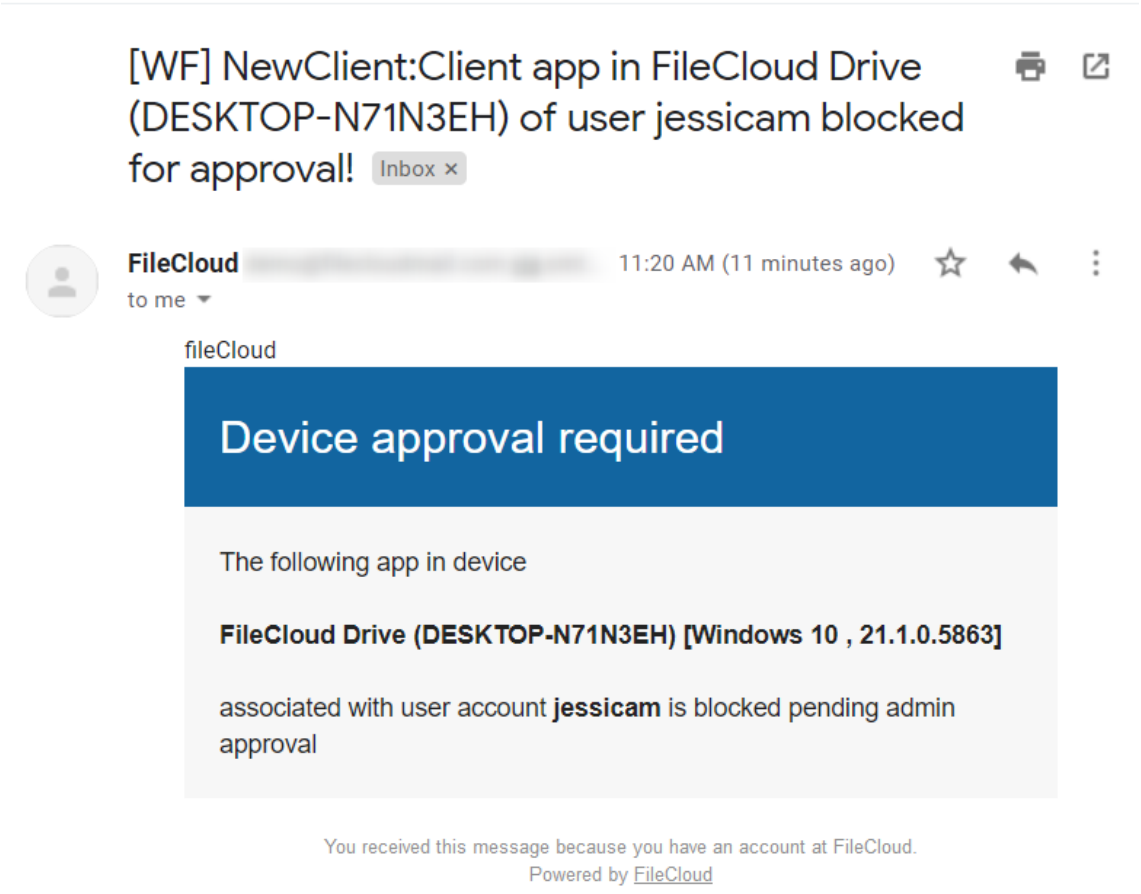
8. Click on Next, to give workflow name



9. In the admin dashboard, the Devices tab will show the status of the devices awaiting Admin approval. The Admin is also sent an email.



10. An email will be sent to the user trying to connect to FileCloud notifying the user that the device needs to be approved by the admin.



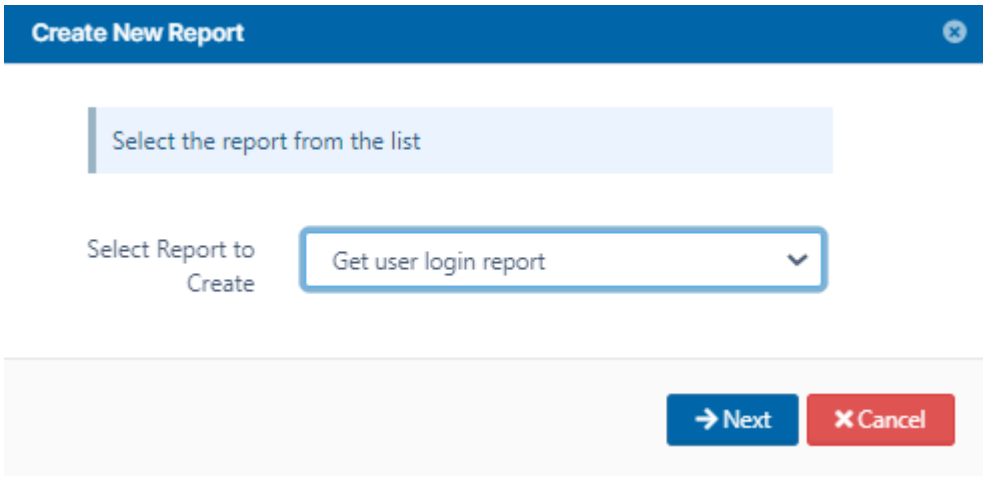
Create Report and Send Email Workflow

This workflow recipe creates a specific report and sends the result to specified emails once a day.

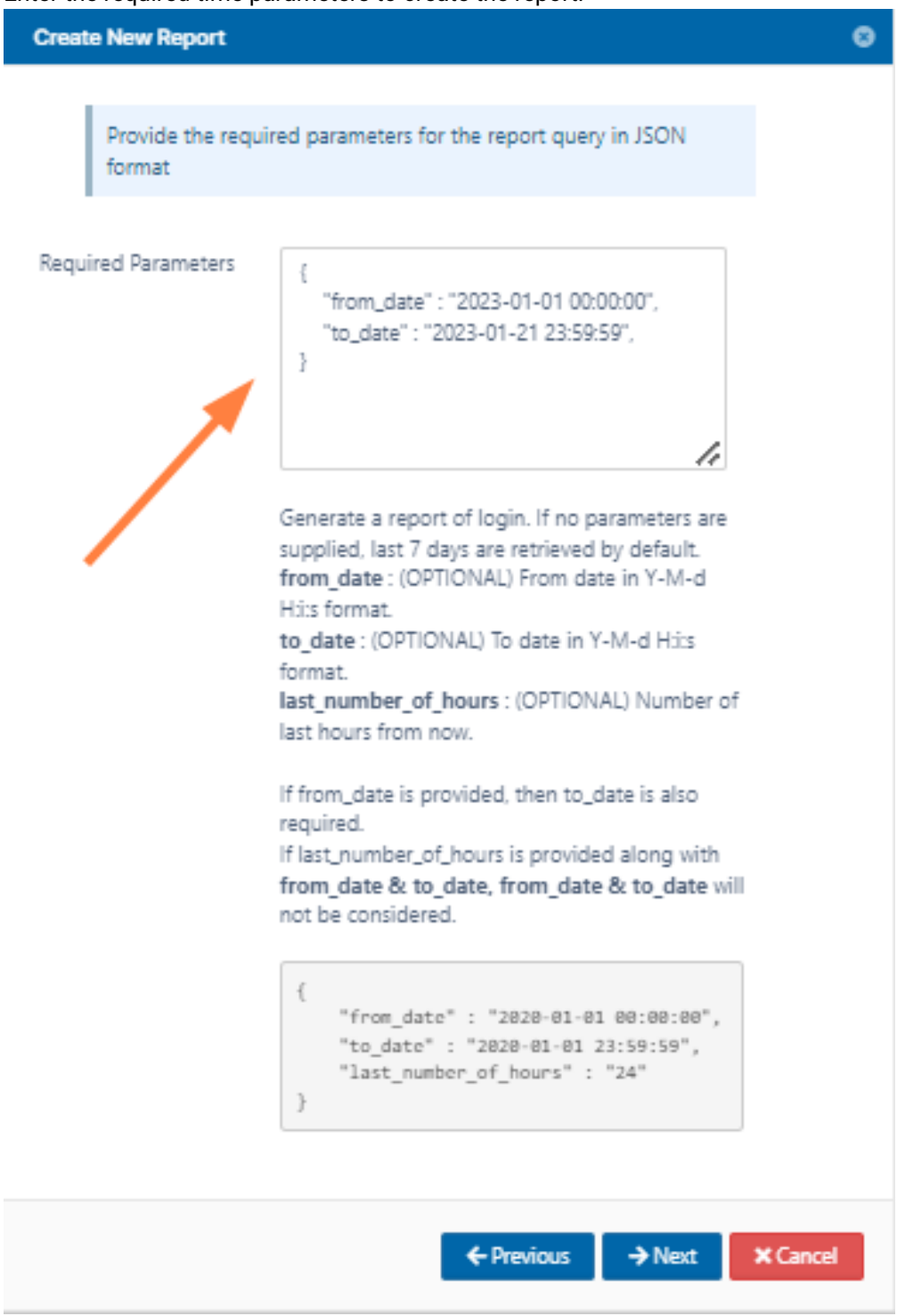
- The email can be configured to be sent at a specific time in the day, and the day interval can be set to daily.

To create a workflow that generates a specific report and sends the result to specified emails:

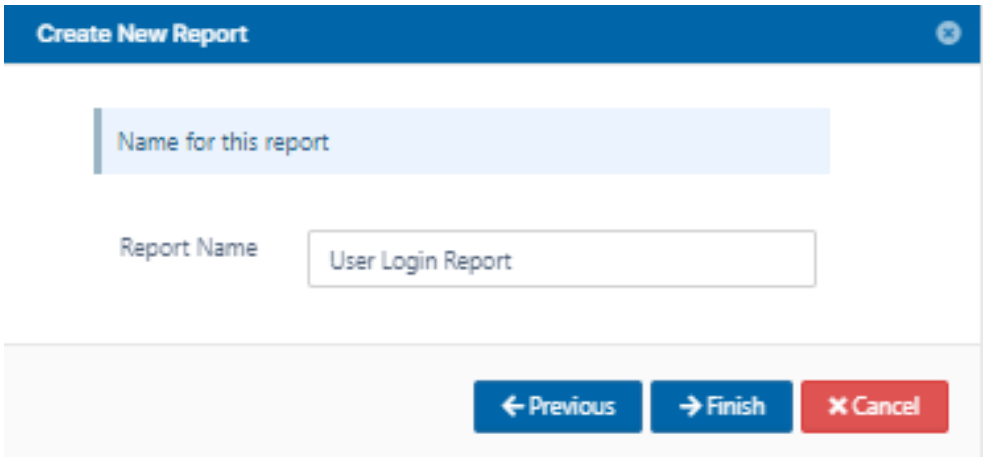
1. Log in to the admin portal
2. In the navigation panel, click **Reports**.
3. Click **Add Report**.
4. In **Select Report to Create**, choose **Get user login report**.


Create New Report
Select the report from the list
Select Report to Create
Get user login report
Next
Cancel

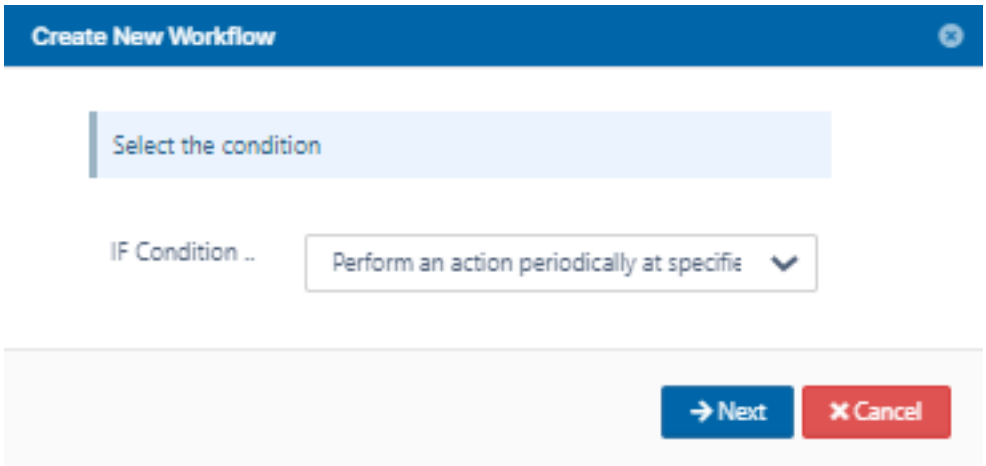
5. Enter the required time parameters to create the report.



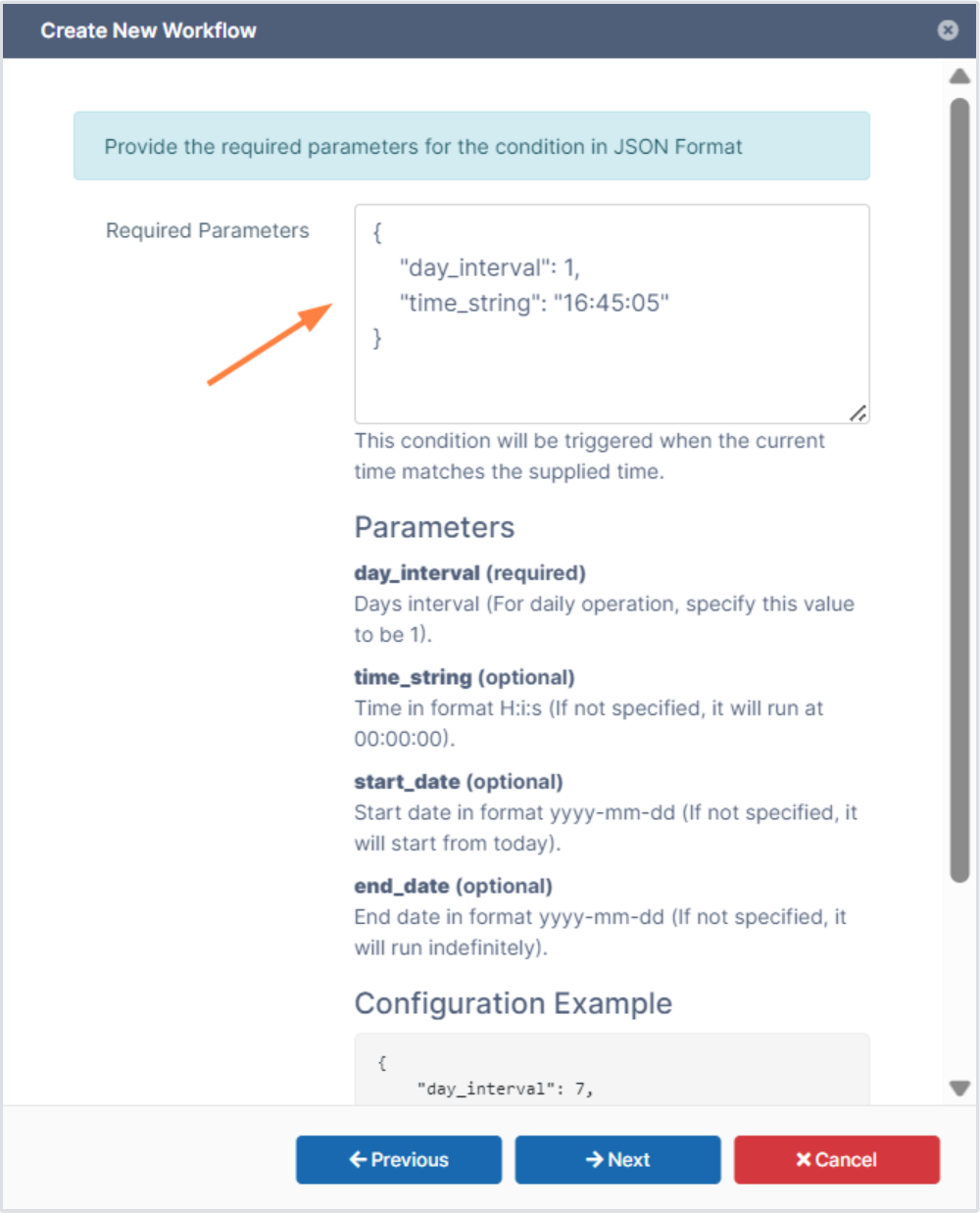
6. Save the report with an appropriate name, and click **Finish**.



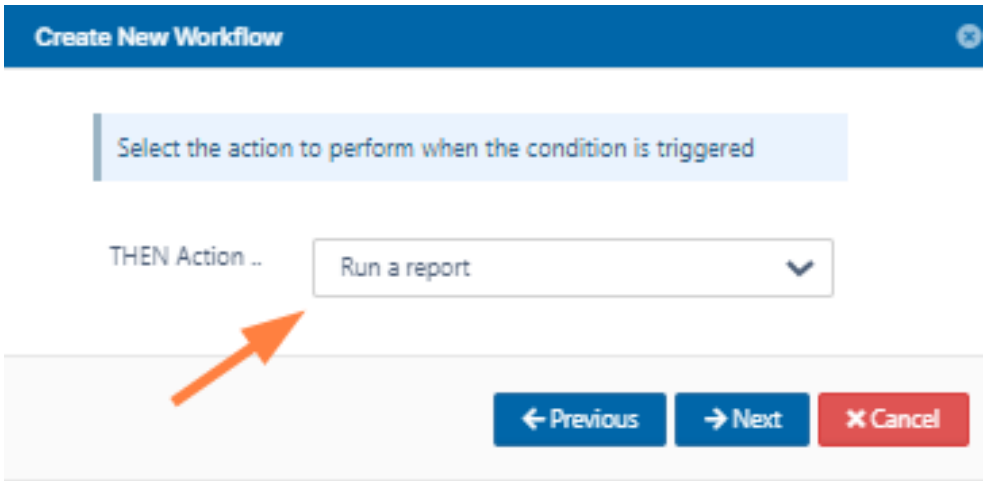
7. Click **Workflows** in the navigation panel.
8. Click **Add Workflow** and set the **If condition** as **Perform an action periodically at specified time and interval**.



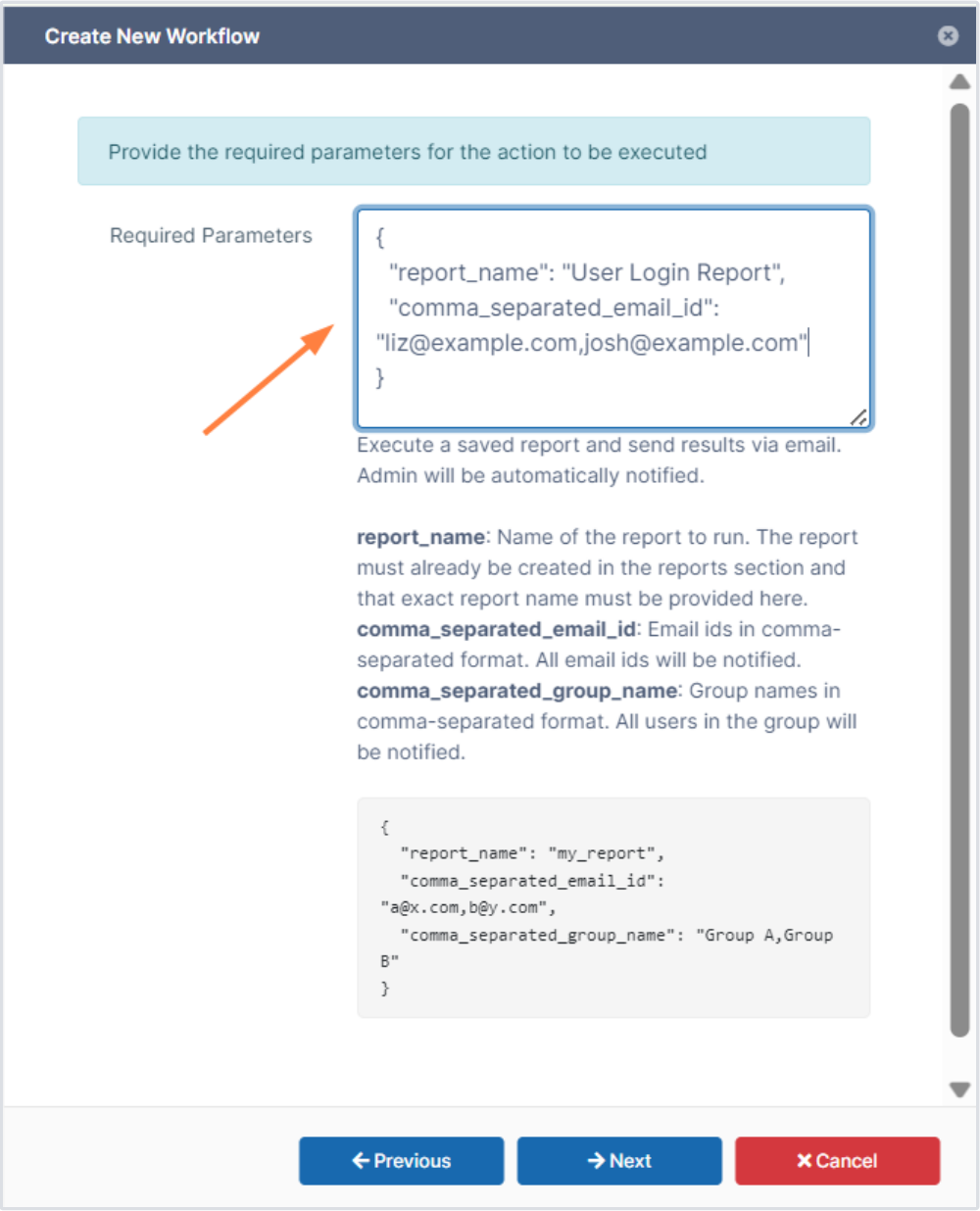
9. Specify the time in the format given in the template. Specify the day interval as 1 to indicate that the workflow should be triggered daily.



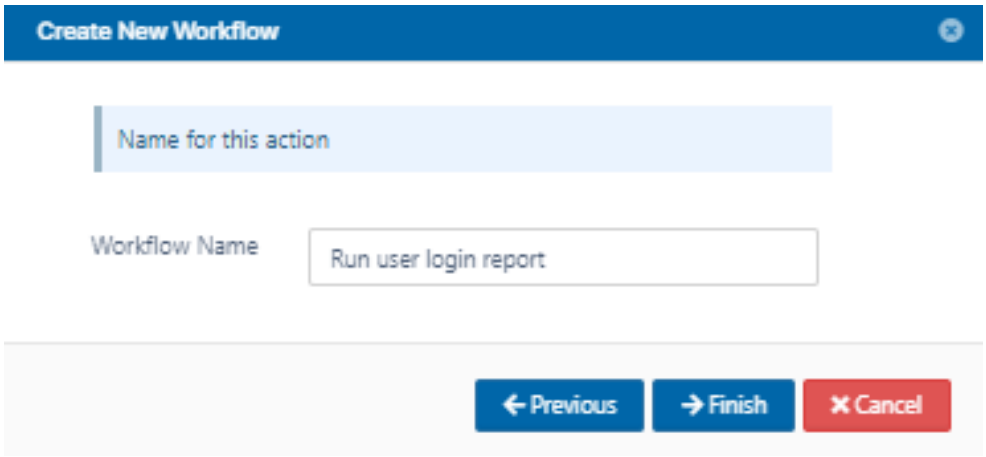
10. Set the **THEN Action** as **Run a report.**



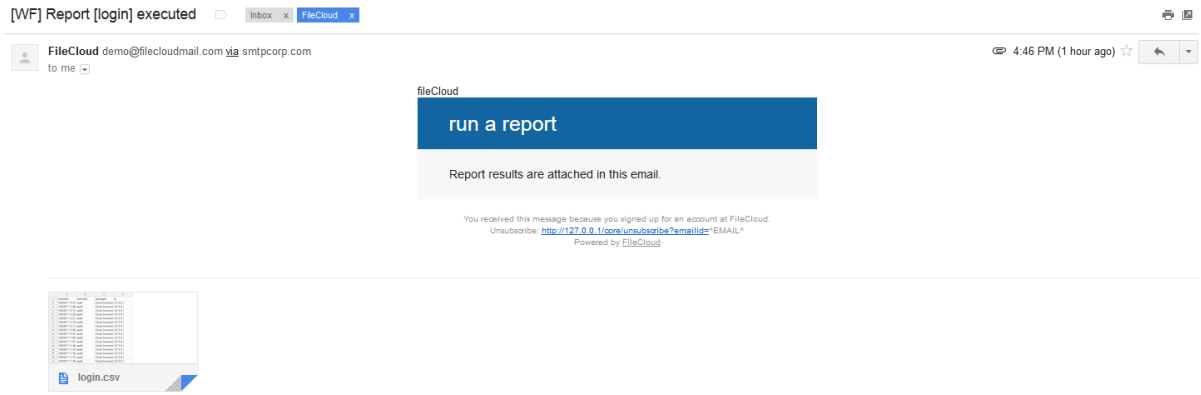
11. Specify the report name created previously and the emails or group of the users who will receive the report in the format given in the template.



12. Save the workflow with an appropriate name.



13. Once the workflow is run the report results are sent to the email ids specified.



Similar workflows can be created to run reports with THEN conditions like:
- **Perform an action on the specified date**
- **Perform an action periodically**

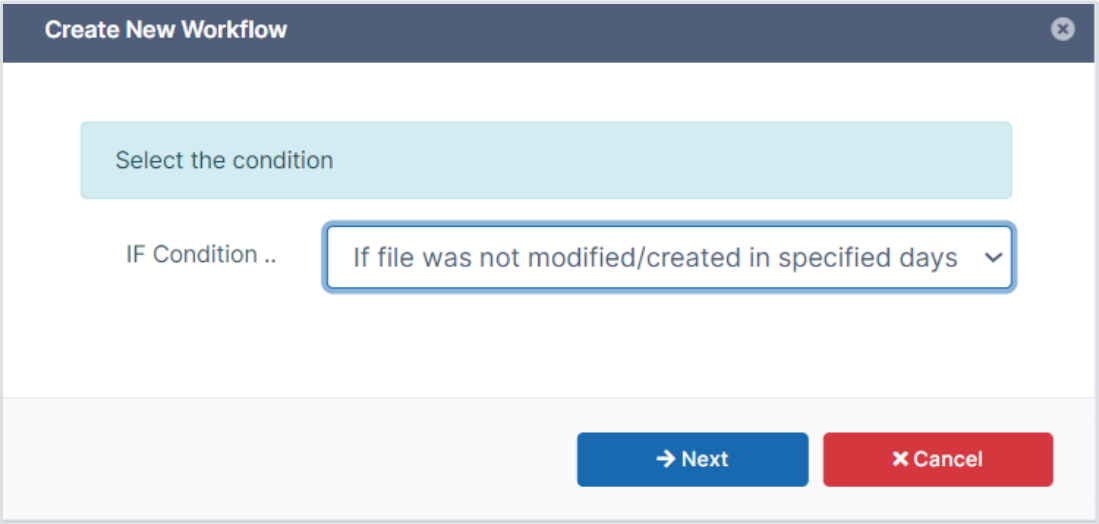
Detect and Delete Inactive Files Workflow

This workflow recipe deletes all unused files.

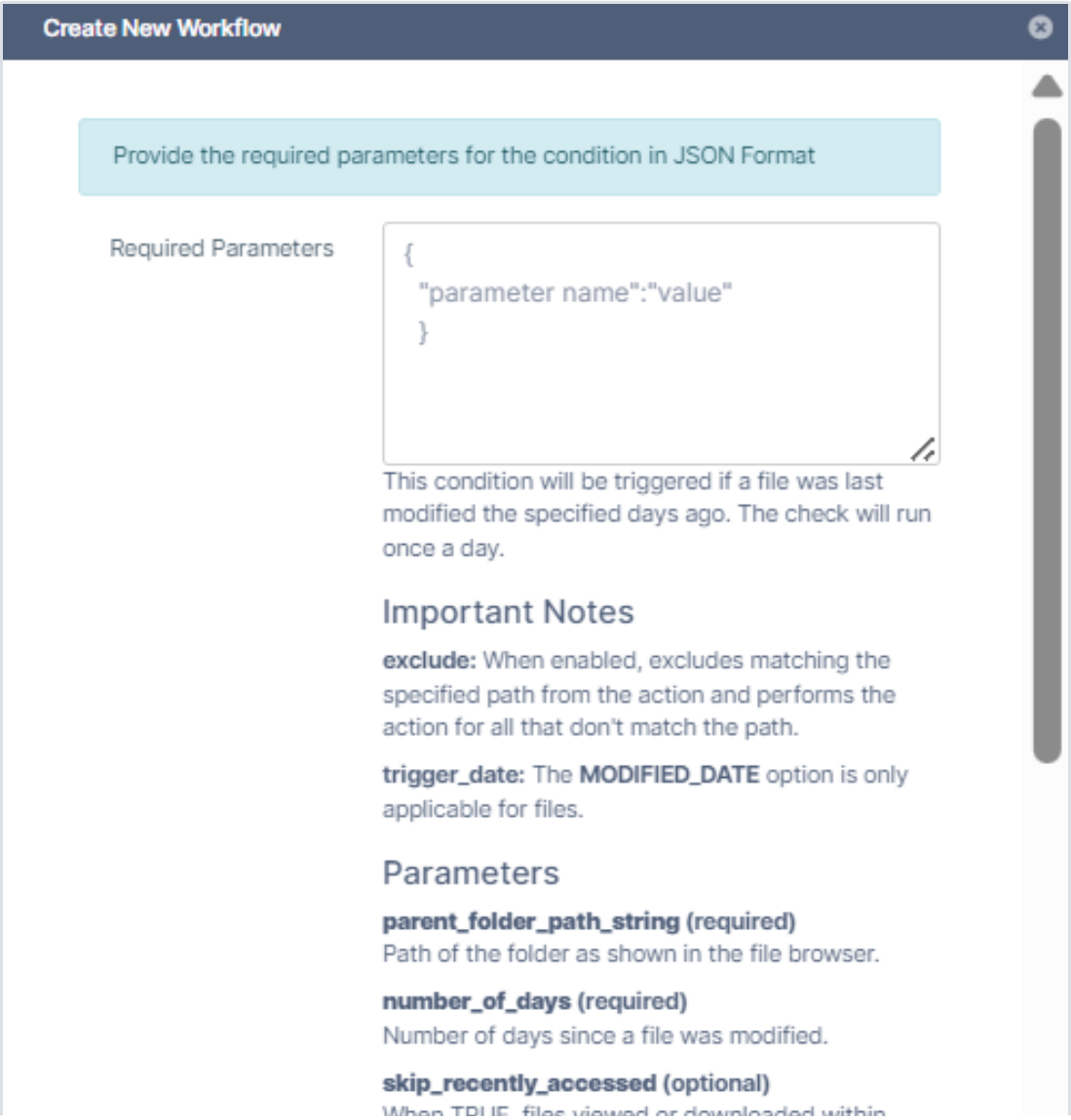
- The workflow checks the number of days a file was unused and deletes those files.
- You can provide a set of email ID's to send the generated report to.

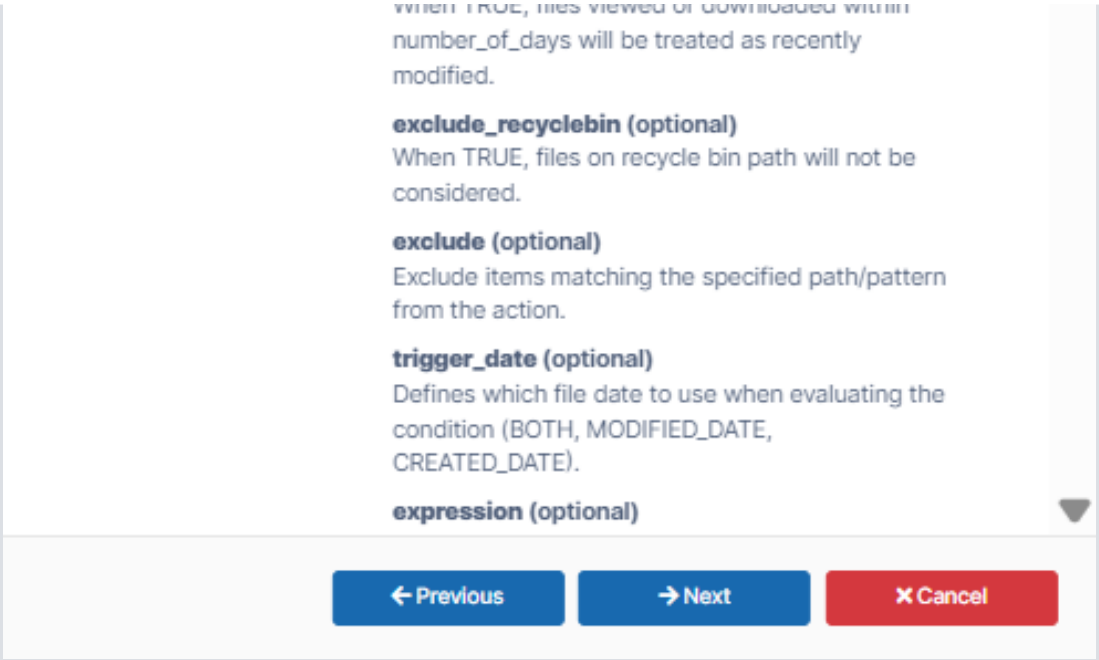
To create a workflow that detects and deletes inactive files:

1. Log in to the admin portal.
2. Click **Workflow** on the left navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified for specified days**, and click **Next.**



5. Enter the parameters in the given format.





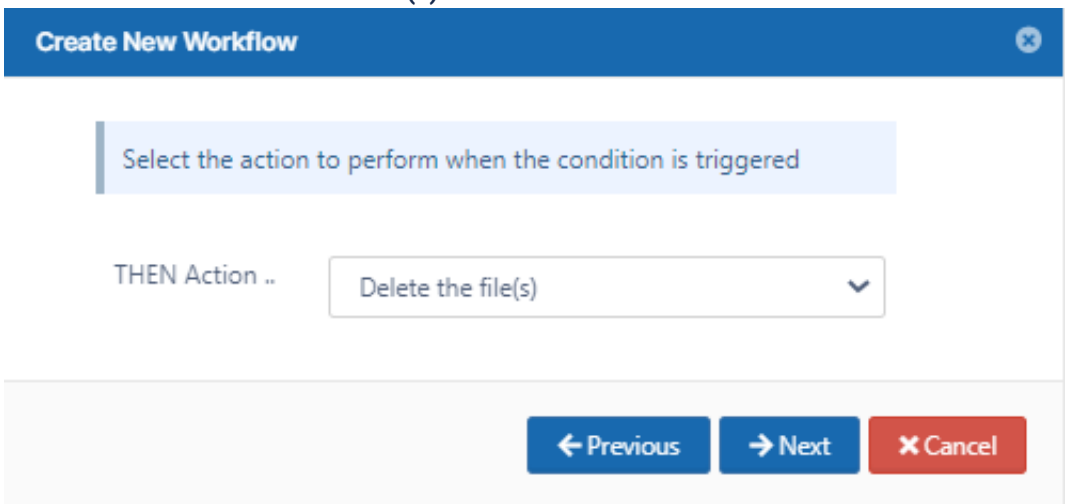
For example:

```
{
  "parent_folder_path_string": "/johndoe",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*",
  "trigger_date": "BOTH"
}
```

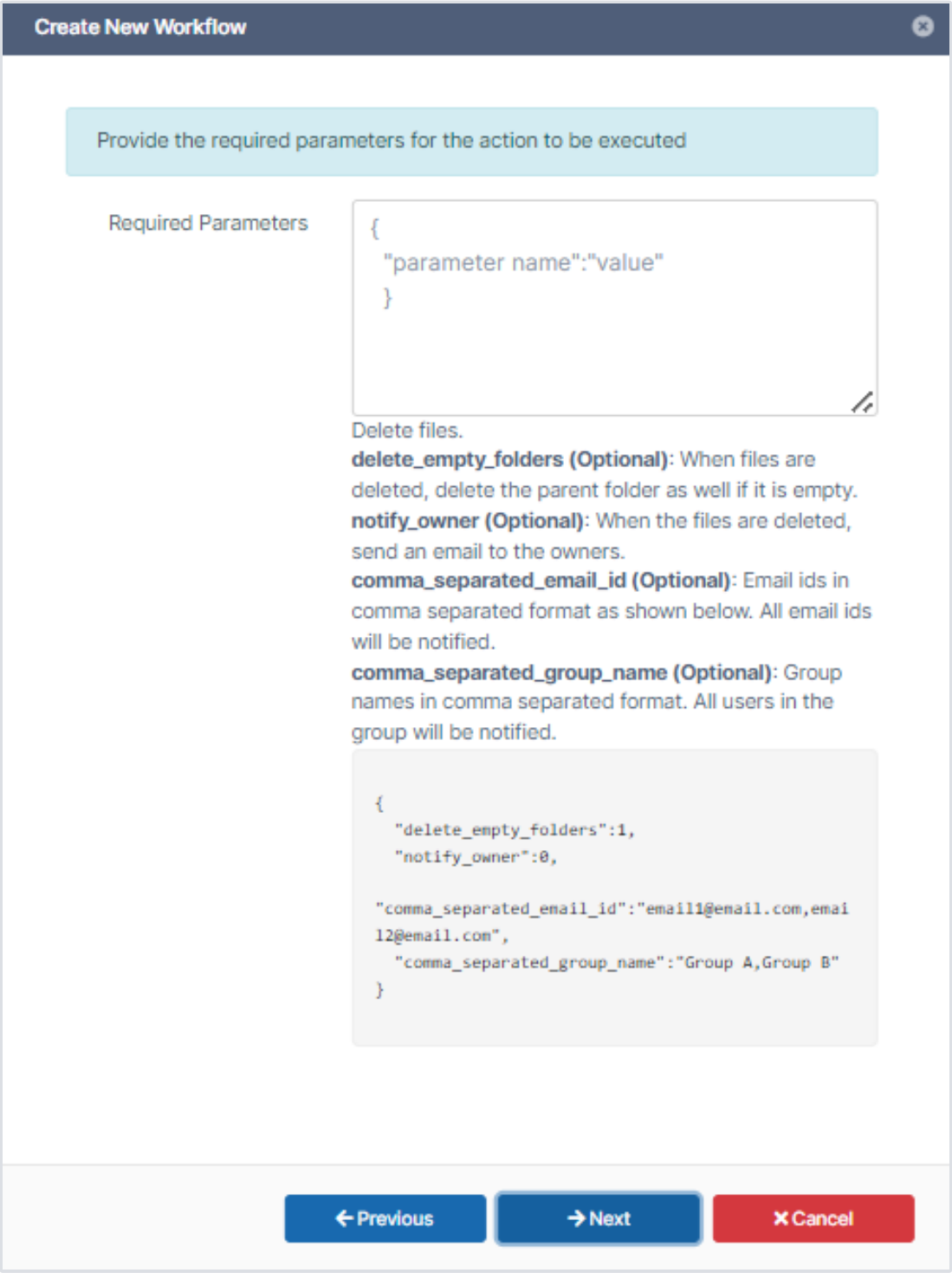
Note - This workflow only applies to Managed Storage and not to Network Folders.
To identify a FileCloud specific path for a folder, see Identifying a FileCloud Specific Path.

6. Click **Next.**

7. Set **THEN Action** to **Delete the file(s)**.



8. Click **Next**.
   Set any of the parameters. They are all optional.

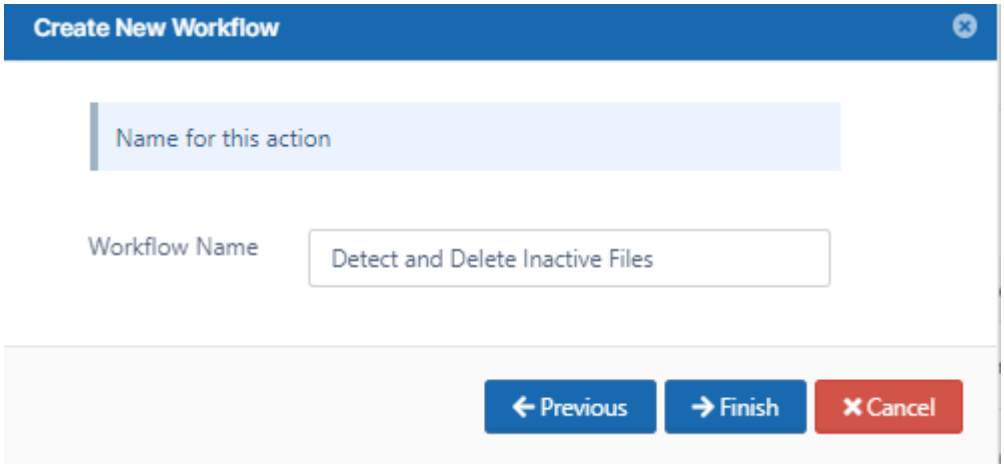


For example:

```
{
"delete_empty_folders":true
```

```
}
```

9. Click **Next**.
10. Enter a **Workflow Name** and click **Finish**.



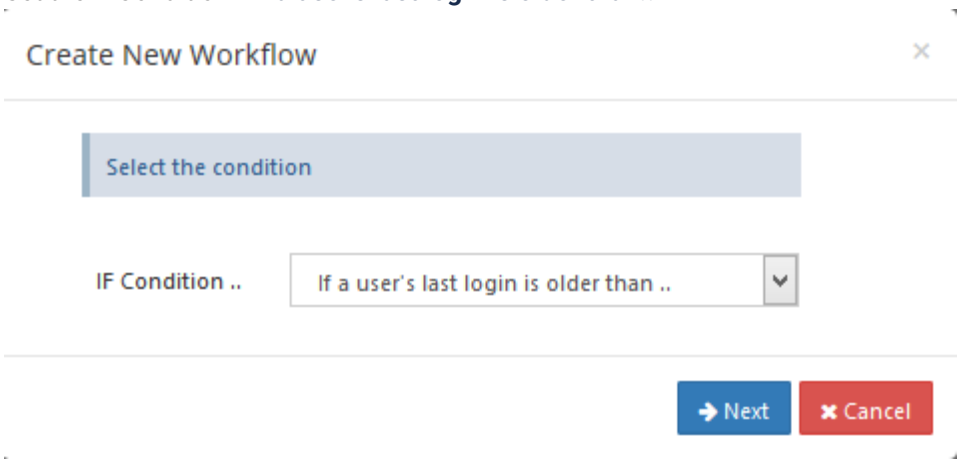
Detect and Disable Inactive Users Workflow

This workflow recipe disables a user when the user is no longer active and notifies the user through email once the account is deactivated.

- The last login date of the user is used to know if the user is Active or Inactive.
- You can avoid looking at users who have not begun using FileCloud.
- You provide the email ID's to which a report of disabled users is sent.

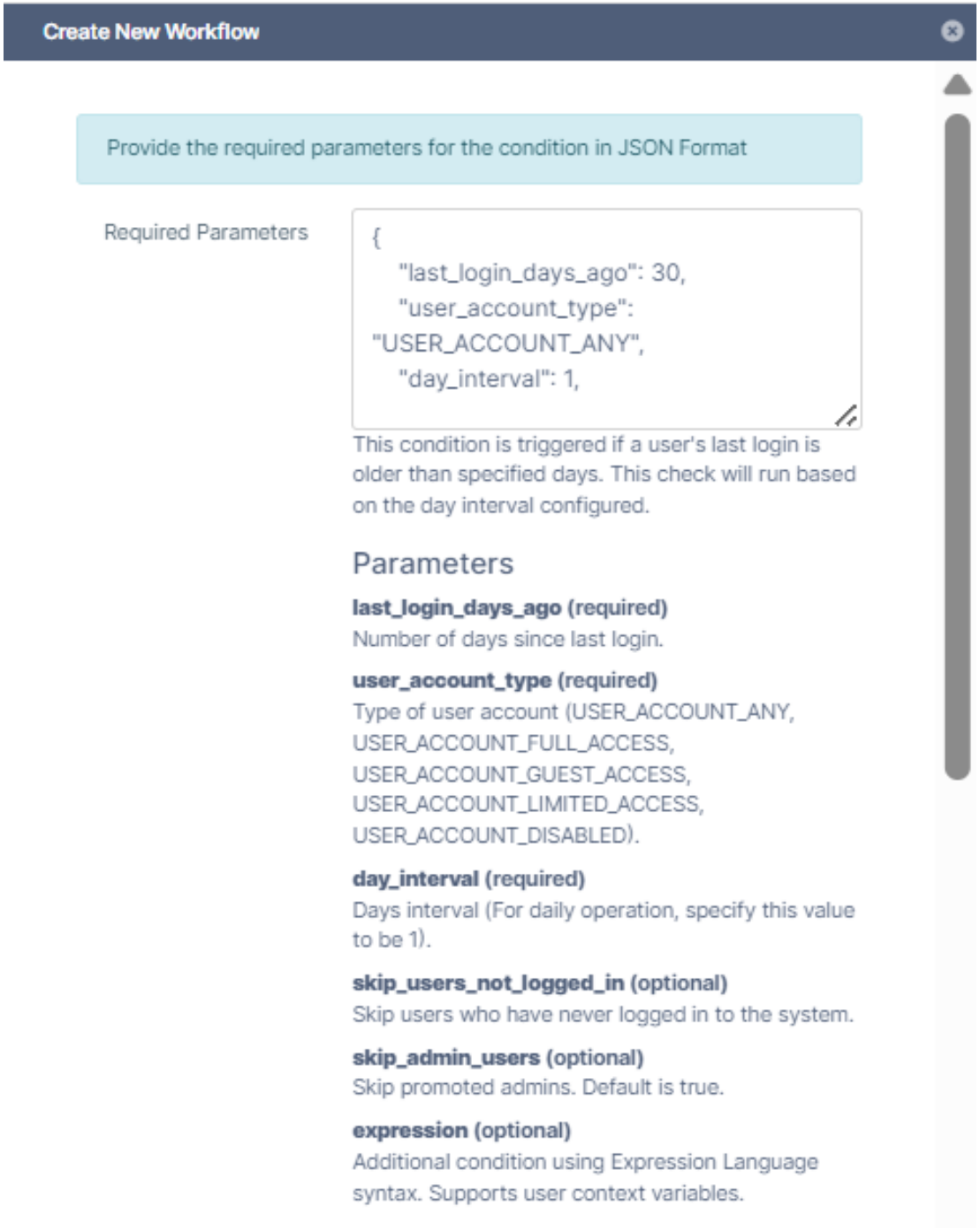
To create a workflow that detects and disables inactive users:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Click the **Add Workflow** button
4. Set the If Condition " **If a user's last login is older than..** "



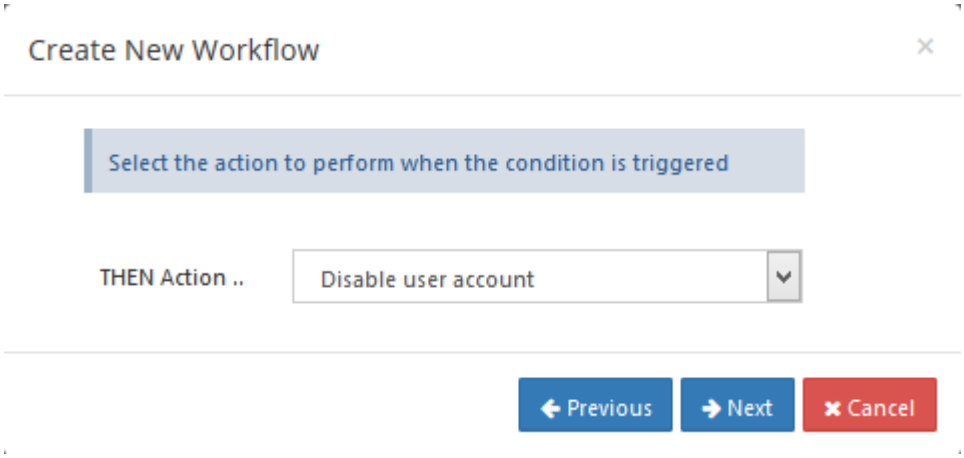
5. Enter the required parameters in the given format.

```
{
"last_login_days_ago":30,
"user_account_type":"USER_ACCOUNT_ANY",
"day_interval":1
}
```



6.

Click **Next**, and set the **Then Action** to " Disable user account ".



7. Enter the Required parameters in the given format.

```
{
"comma_separated_email_id":"admin@abccompany.com,hr@management.com"
  }
```

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

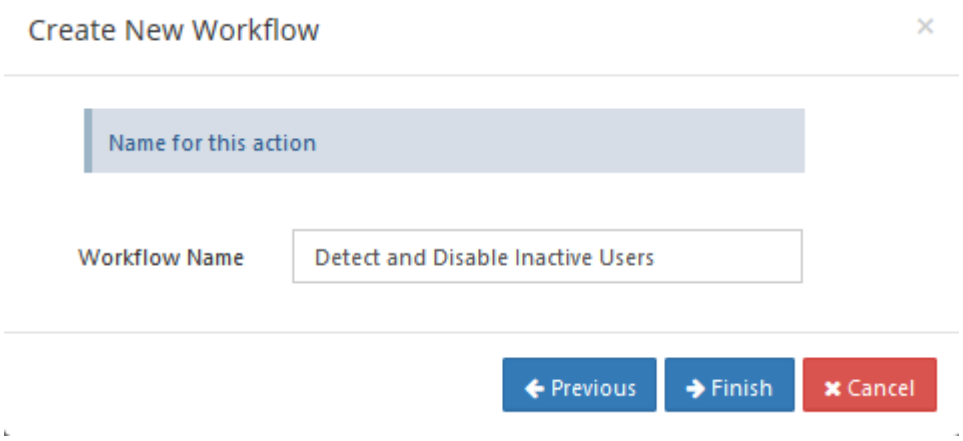
```
{

"comma_separated_email_id":"admin@abc.com,hr@management.com",
```

Disable user and send email after performing this action.
comma_separated_email_id: Email ids in comma separated format as shown below
comma_separated_group_name (optional): Group names in comma separated format. All email ids will be notified.
donot_email_user (optional): Do not send email to user affected (1 or 0). Default 0

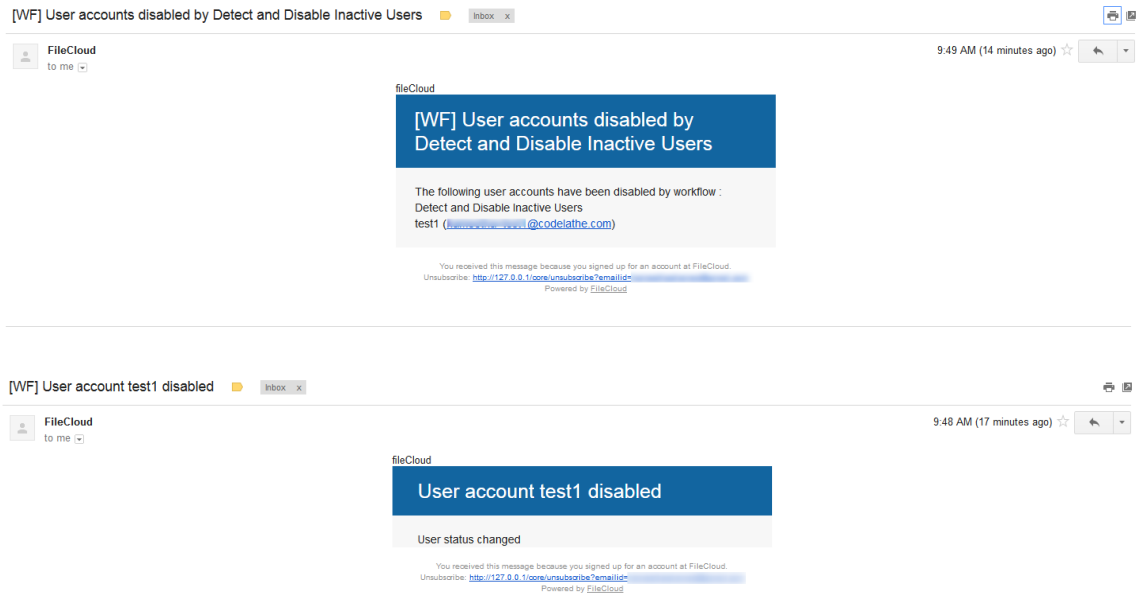
```
{

"comma_separated_email_id":"xyz@a.com,abc@b.com",
  "comma_separated_group_name":"Group A,Group B",
  "donot_email_user": 0
}
```

← Previous → Next ✕ Cancel

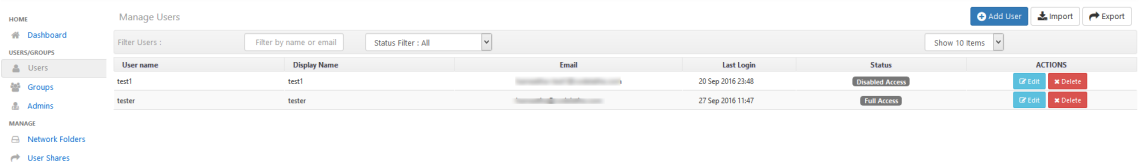
8. Click **Next**, give an appropriate workflow name and click **Finish**.



9. The user accounts are disabled and the notifications are sent once the workflow is executed.



10. Go to the users list to confirm that the users are disabled.



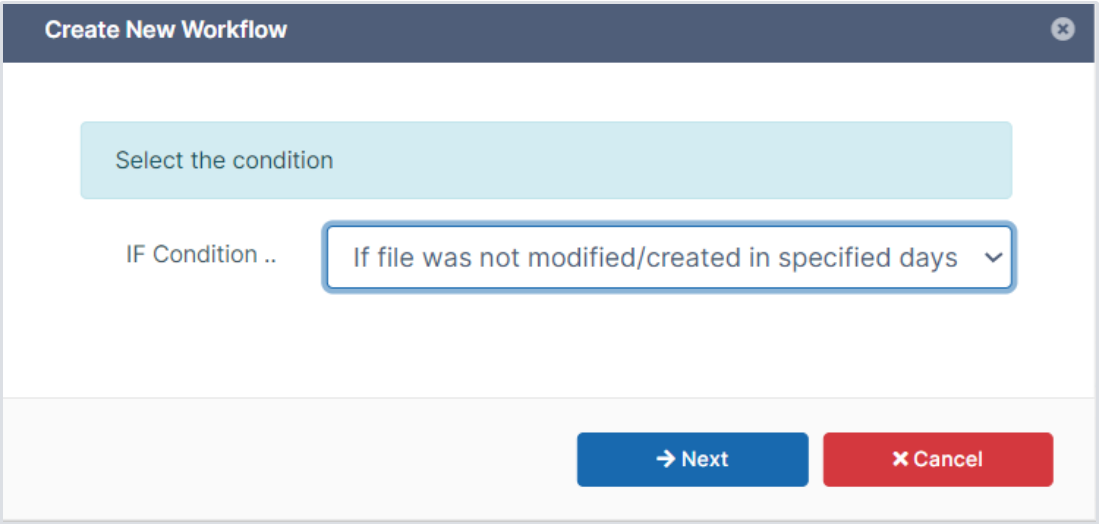
Detect and Generate Inactive File List Workflow

This workflow recipe sends an email report with a list of inactive files.

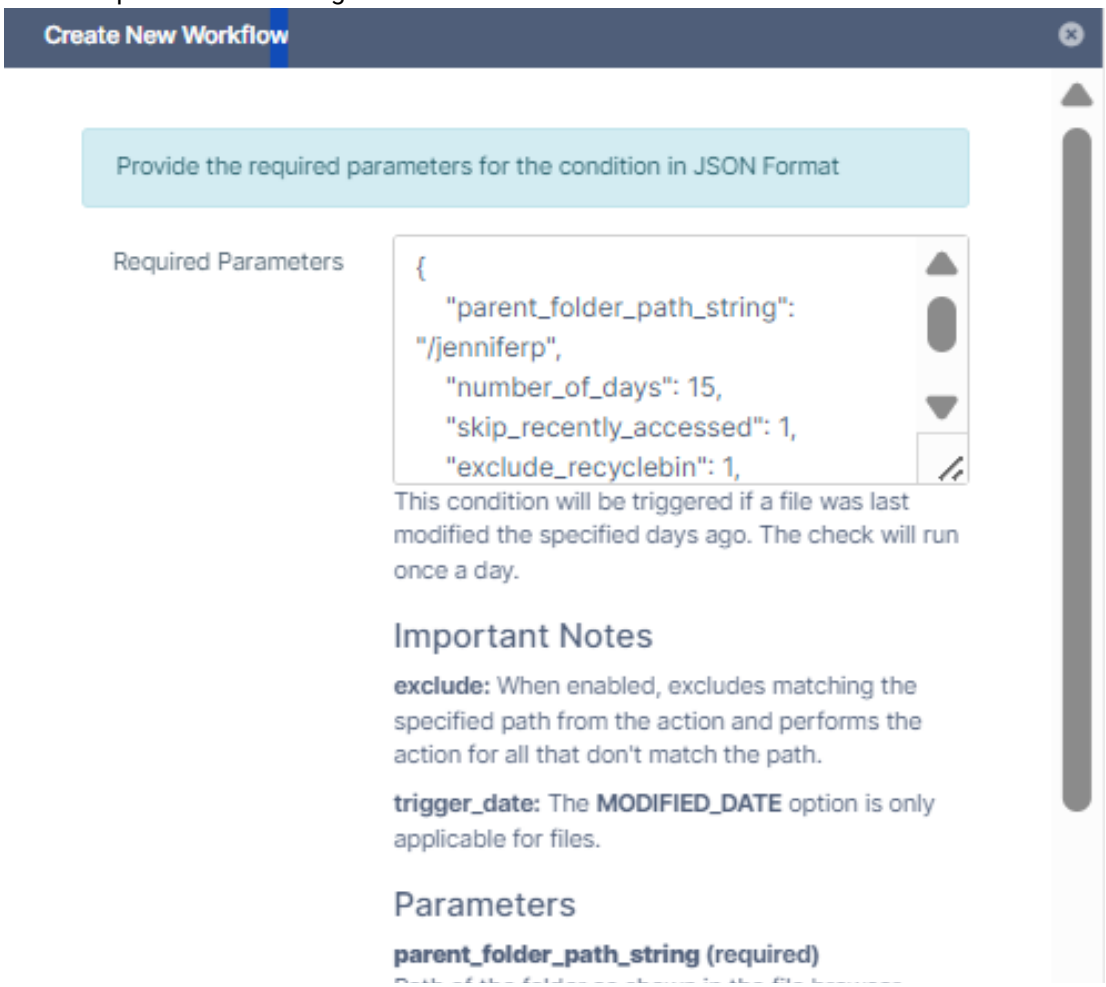
- The workflow checks the number of days a file was unused and generates a report.
- You can provide a set of email IDs the generated report will be emailed to.

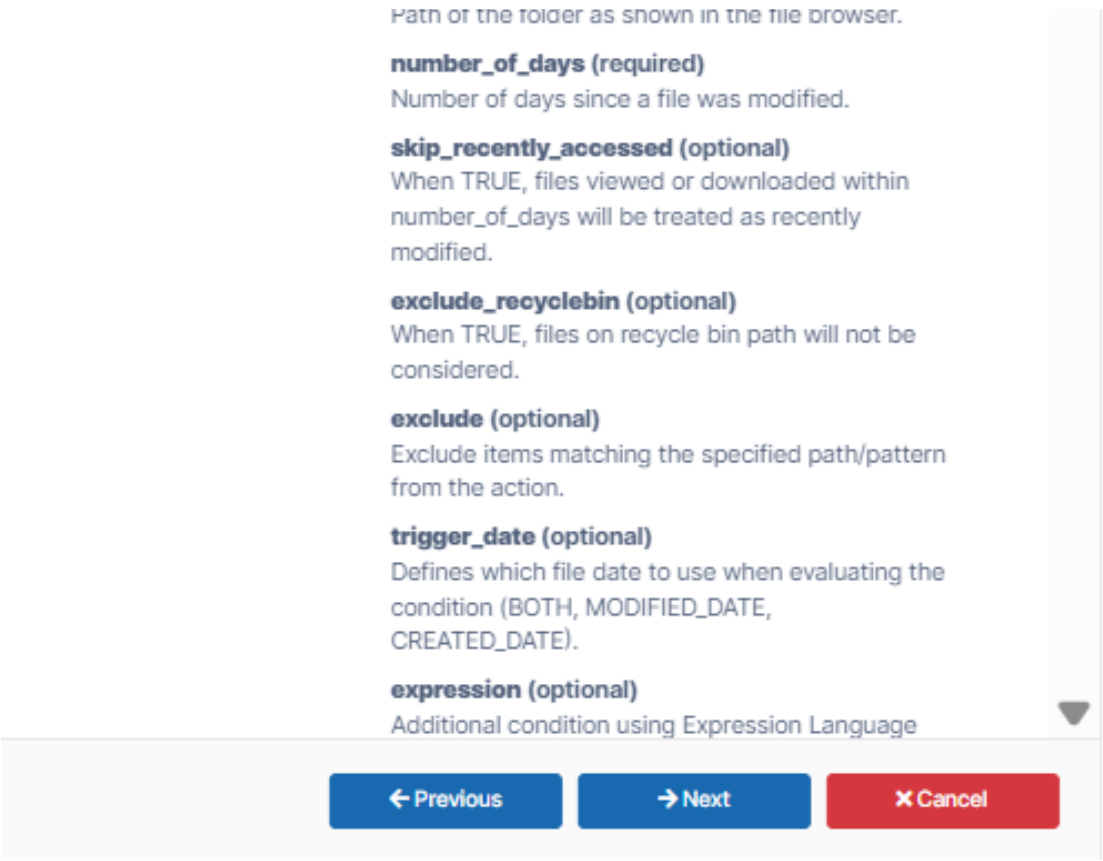
To create a workflow that detects and generates a list of inactive files:

1. Log in to the admin portal.
2. Click **Workflow** in the navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified/created for specified days**, and click **Next**.



5. Enter the parameters in the given format.



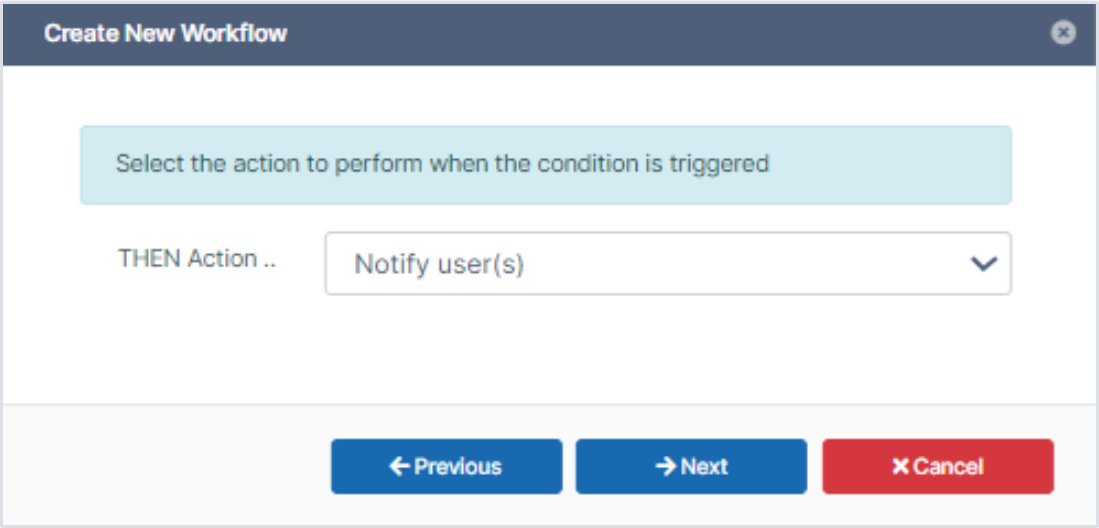


For example:

```
{
    "parent_folder_path_string": "/jenniferp",
    "number_of_days": 15,
    "skip_recently_accessed": 1,
    "exclude_recyclebin": 1,
    "exclude": ".*secret.*",
    "trigger_date": "BOTH",
}
```

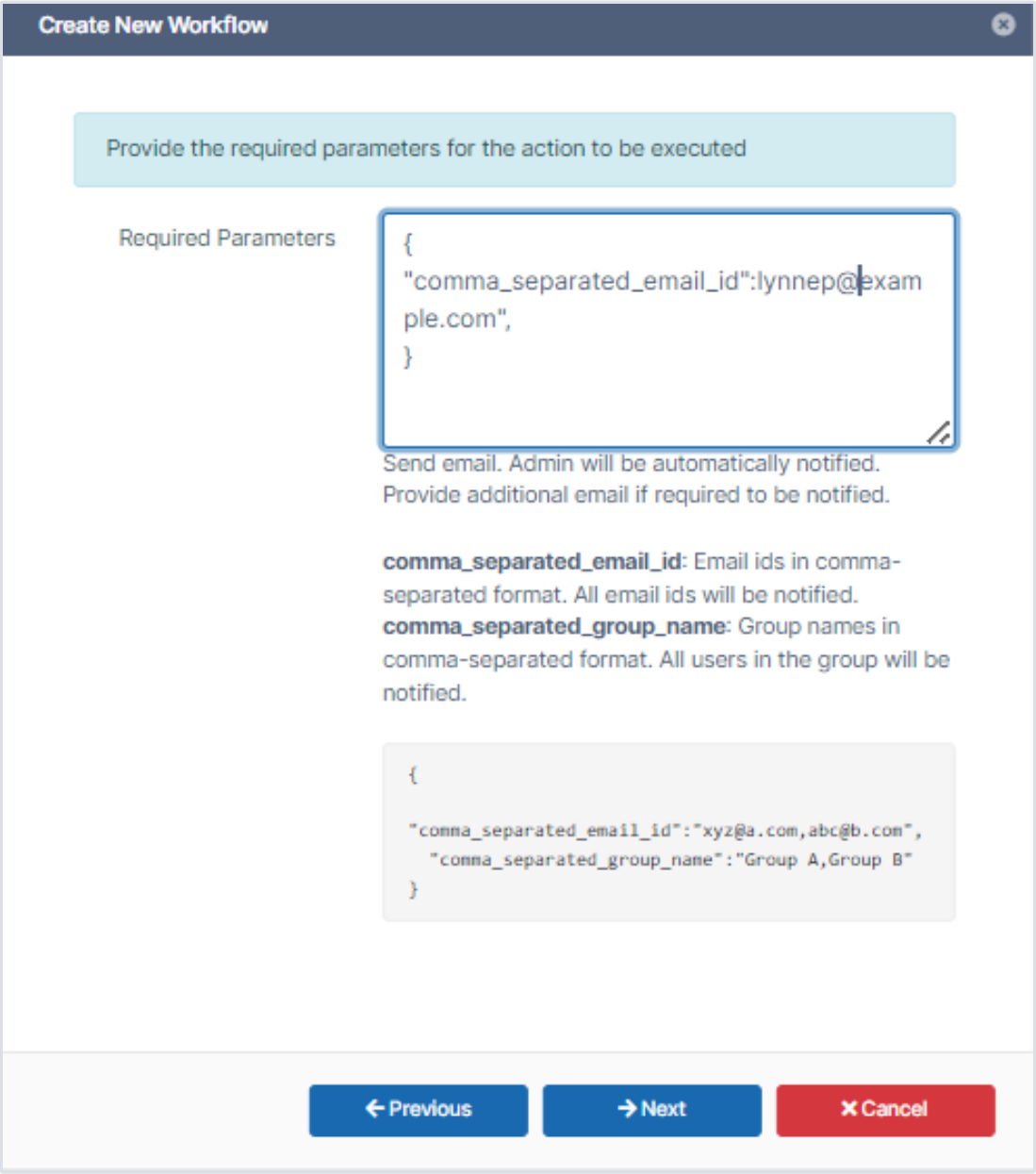
Note: This workflow applies only to Managed Storage and not to Network Folders.
To identify a FileCloud specific path for a folder please refer to Identifying a FileCloud Specific Path.

6. Click **Next.**
7. Set **THEN Action** to **Notify user(s)**.

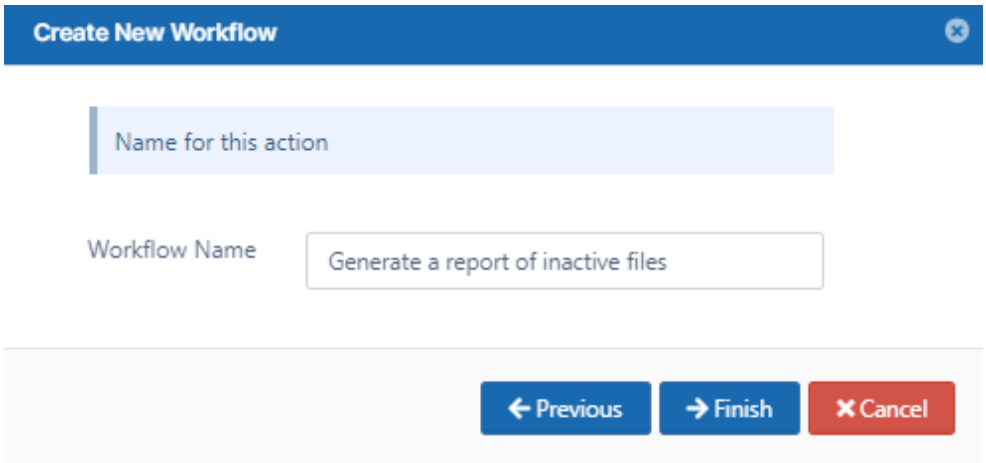


8. Click **Next**.
9. Enter the parameters in the given format.
   For example,

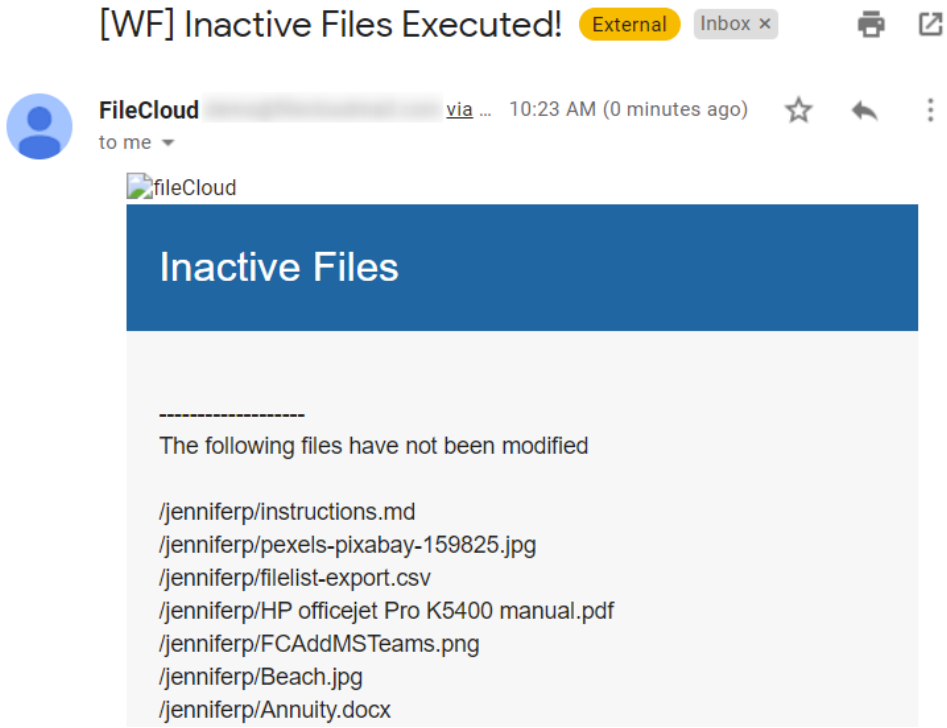
```
{
"comma_separated_email_id":"lynnep@example.com"
}
```



10. Click **Next**.
11. Enter a **Workflow Name**, and click **Finish**.



When you run the workflow, the emails specified receive an email with a list of inactive files.



Detect and Notify Failed Signatures Workflow

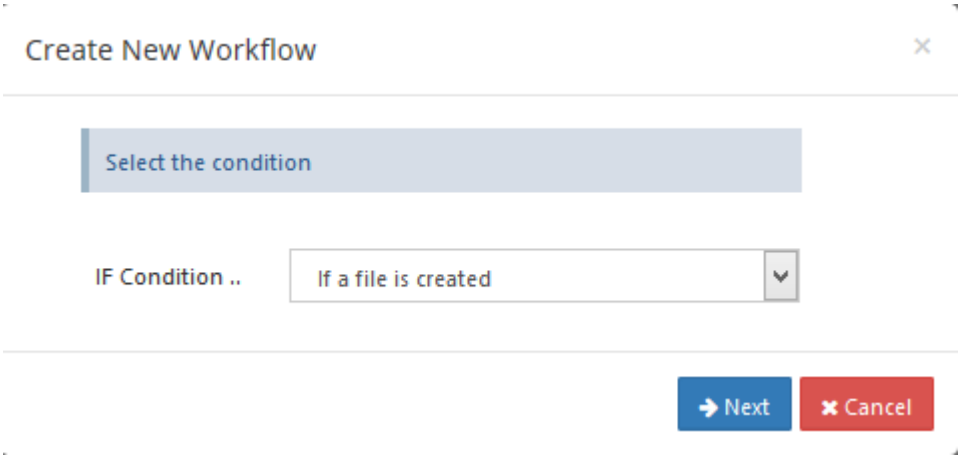
This workflow recipe creates an ALERT notification when a file is created or uploaded to FileCloud with a signature mismatch.

- This ALERT notification can be set for a specific folder location only.
- You can view the alerts on the Admin Portal in the alert panel.

To create a workflow to detect and notify when a file with a signature mismatch is uploaded:

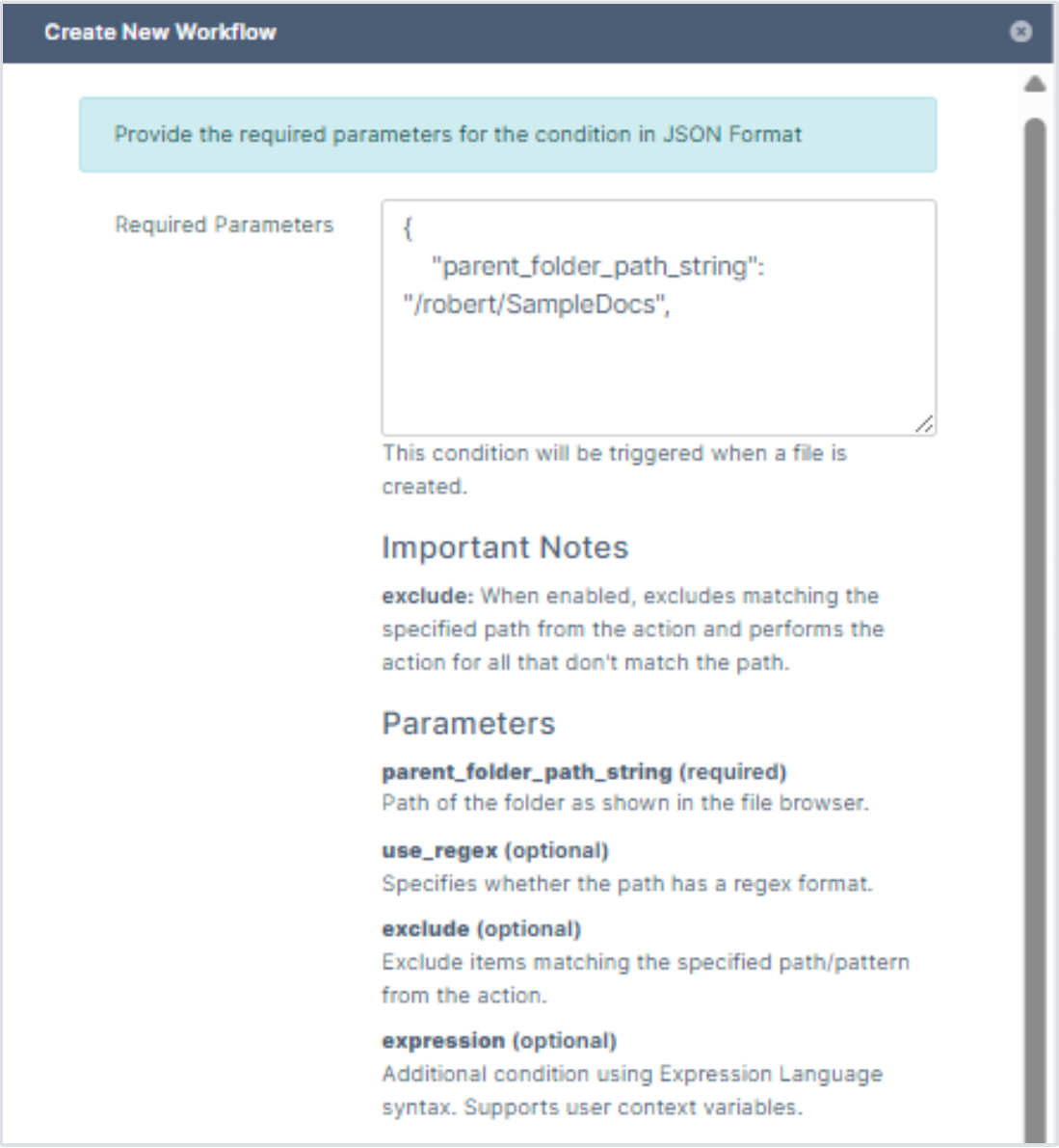
1. Login to Admin Portal

2. Navigate to **Workflow** on the left navigation panel.
3. Click the **Add Workflow** button.
4. Set the **If Condition** to **If a file is created.**

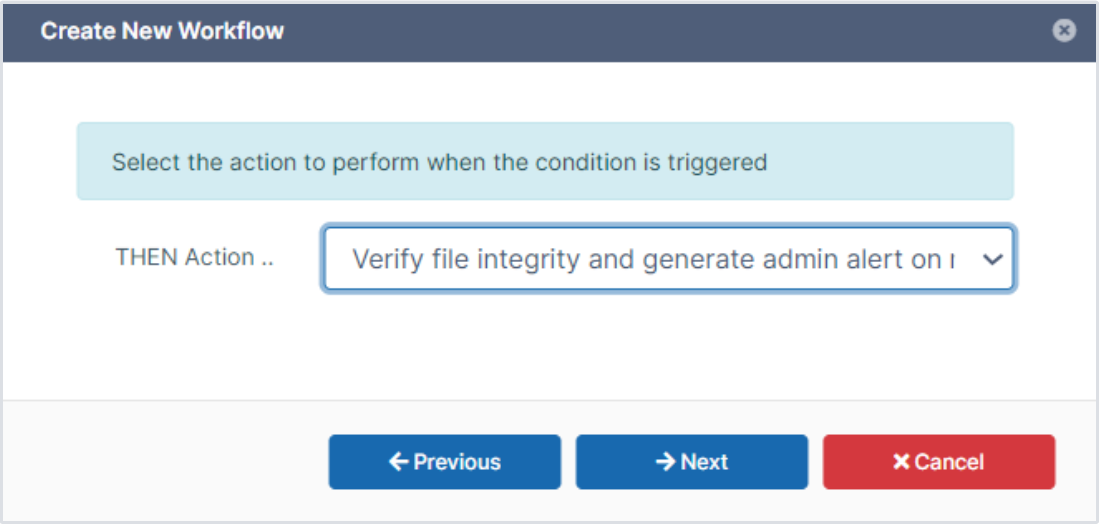


5. Click **Next.**
6. **Set the parameters as shown in the following screenshot.**
   To identify a FileCloud specific path for a folder please refer to Identifying a FileCloud Specific Path.

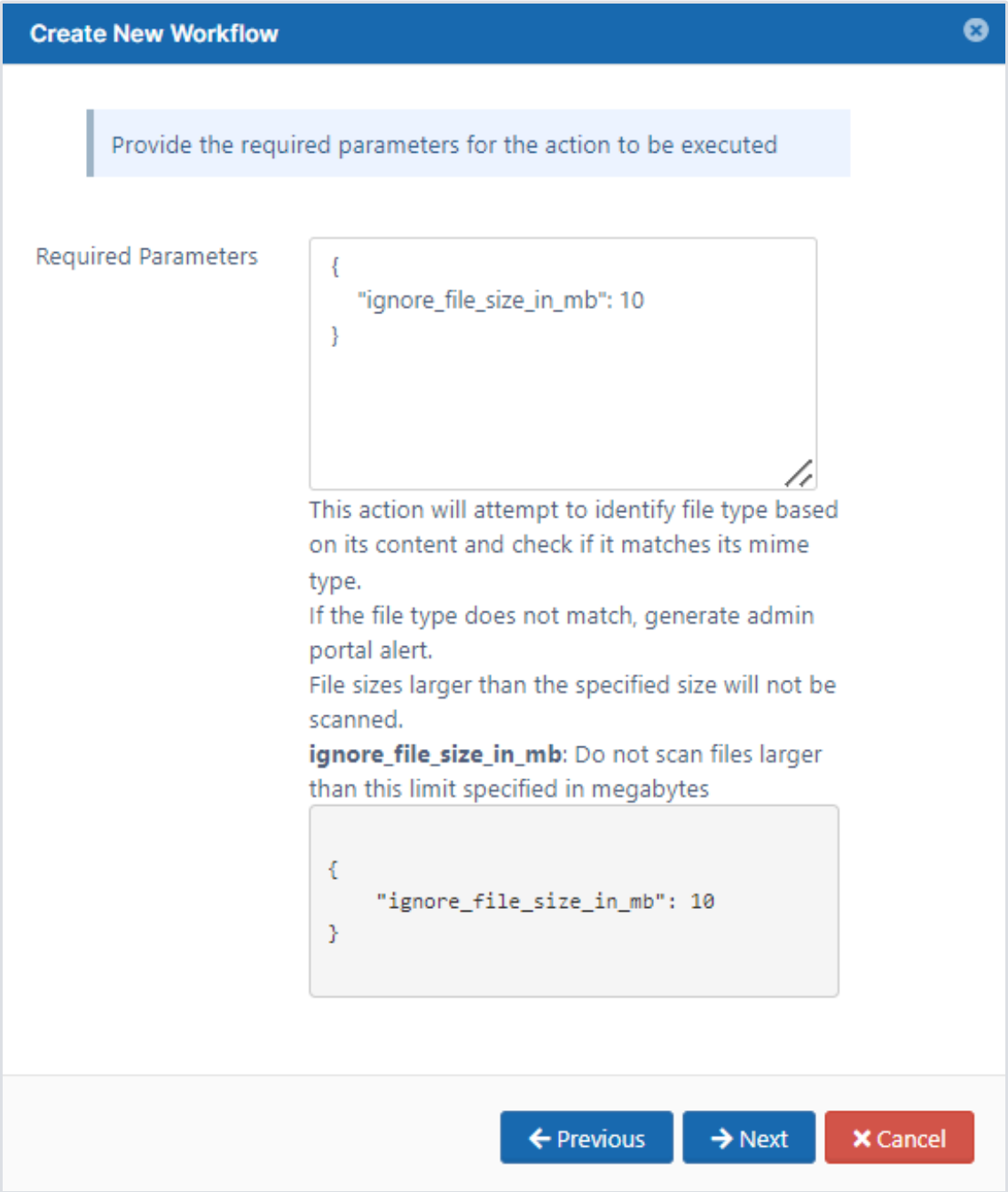
> Set the path to "/" if you want to monitor all the folders in the system.

7. 

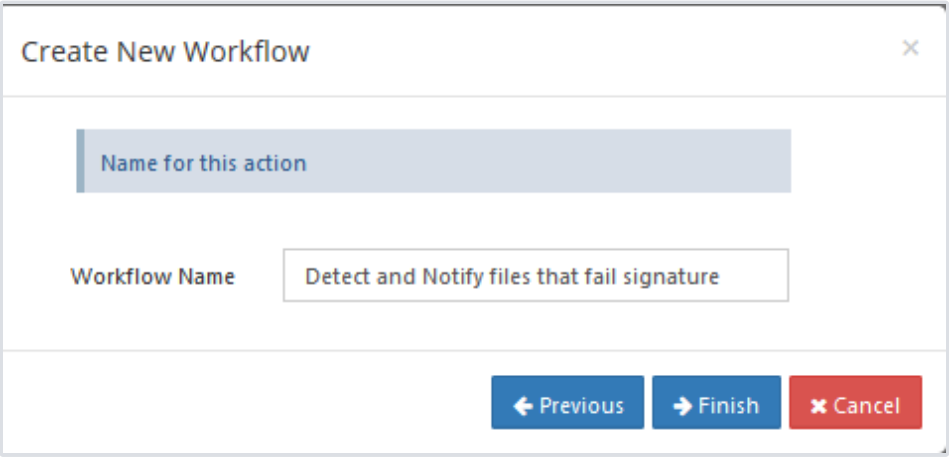
Click **Next**, and set **Then Action** to **Verify file integrity and generate admin alert on mismatch**



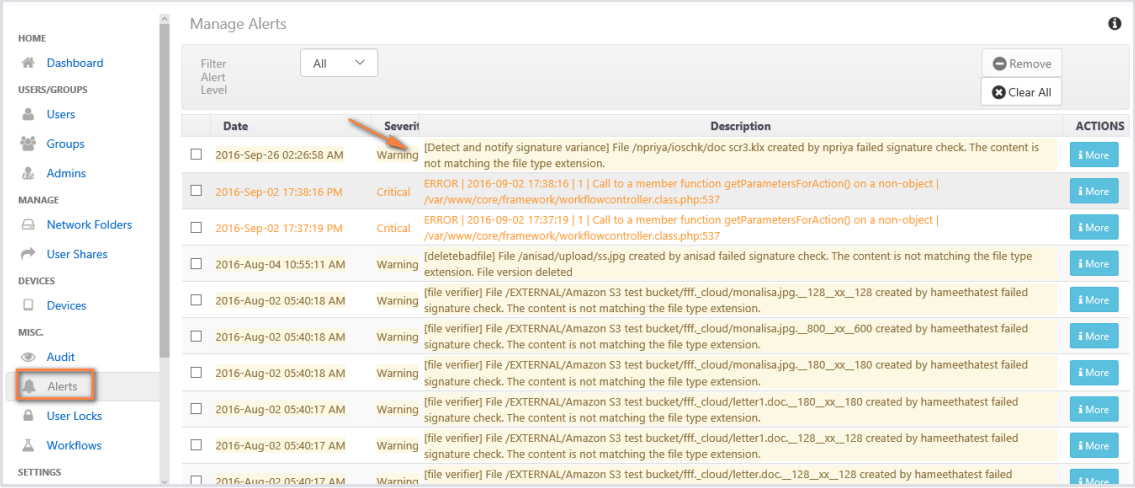
8. **Click Next**, and **enter the size limit of files to scan.**



9. **Click Next**, and give **a name to this workflow.**



Once this workflow is set, the Admin receives alert messages in the **Alerts** page.



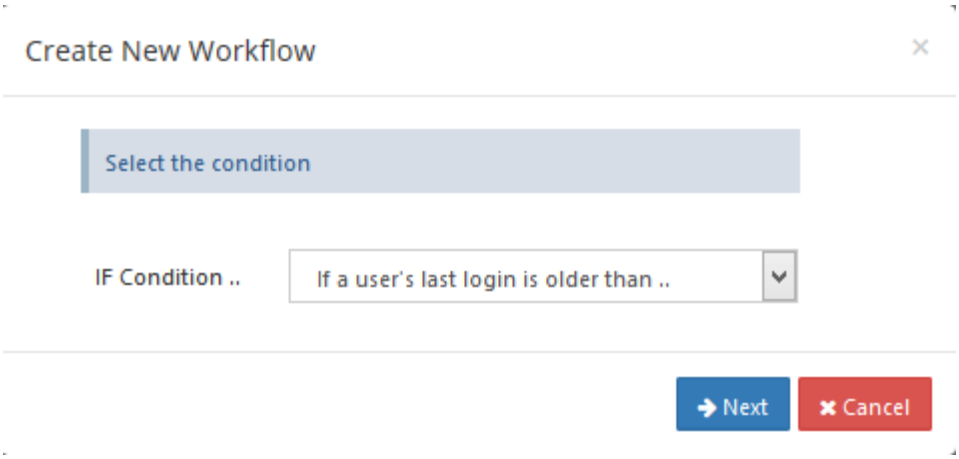
Detect and Notify Inactive Users Workflow

This workflow recipe sends an email report with a list of all the inactive users.

- The last login date of the user is used to determine if the user is Active or Inactive
- You can avoid looking at users who have not begun using FileCloud
- You provide a set of email ID's to which the generated report will be mailed

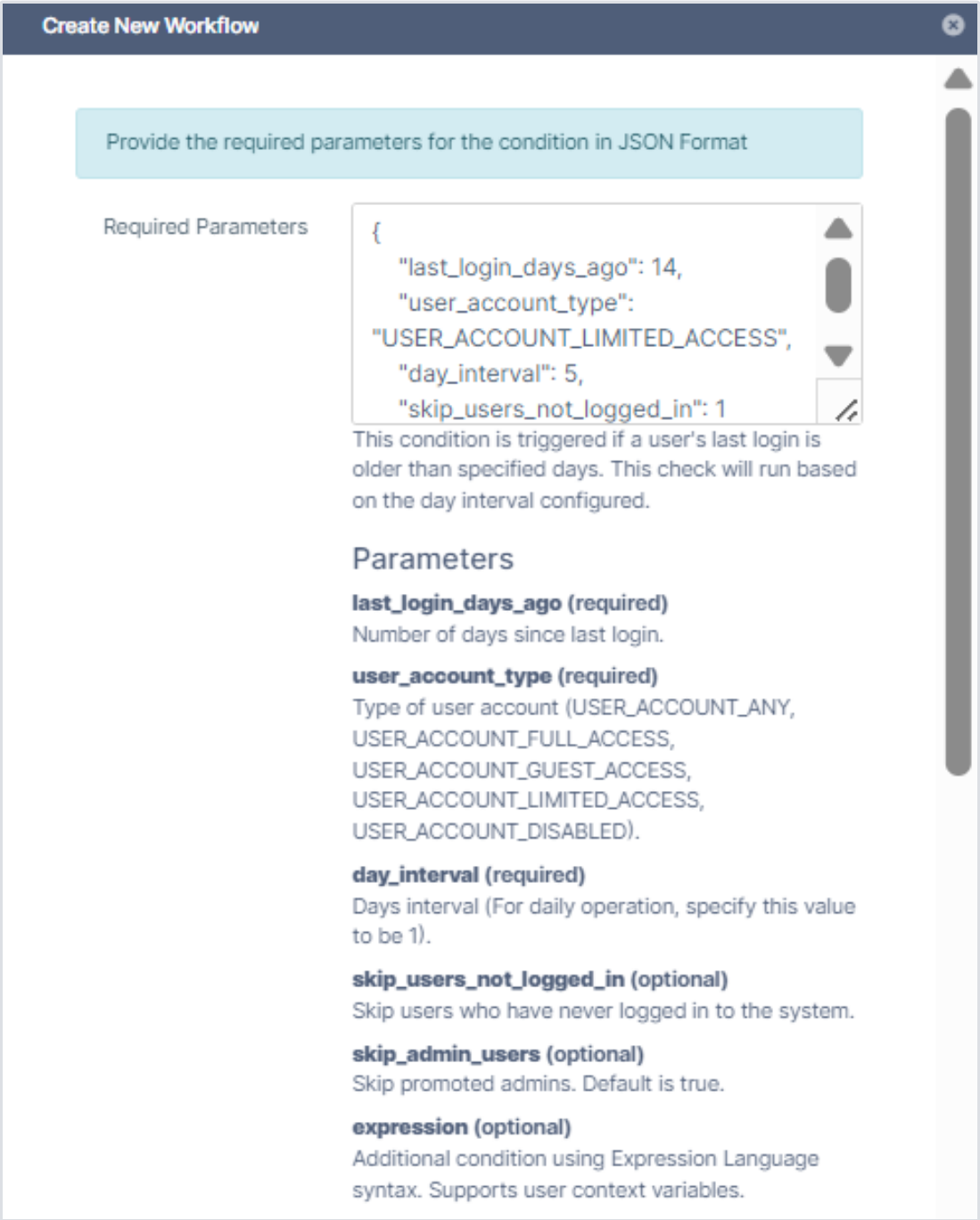
To create a workflow that sends an email report with a list of all the inactive users:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition **If a user's last login is older than..**, and click **Next**.

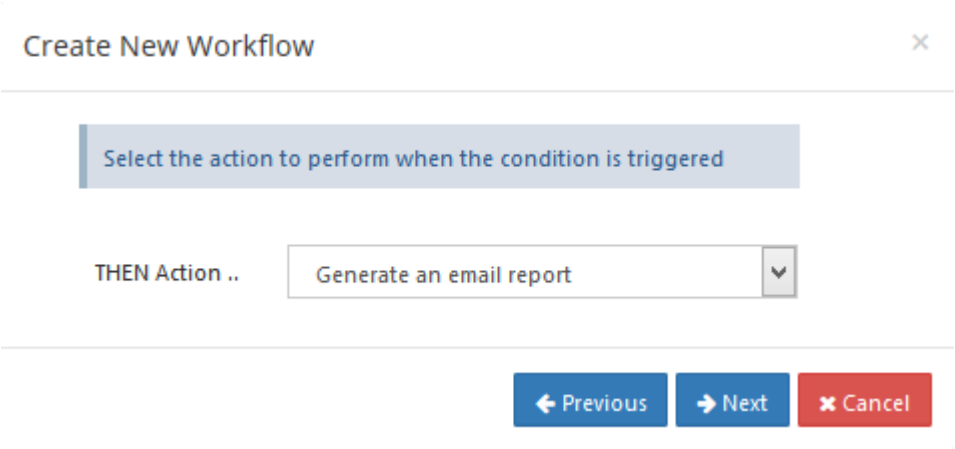


5. Enter the required parameters in the given format

```
{
    "last_login_days_ago": 14,
    "user_account_type": "USER_ACCOUNT_LIMITED_ACCESS",
    "day_interval": 5,
    "skip_users_not_logged_in": 1
}
```

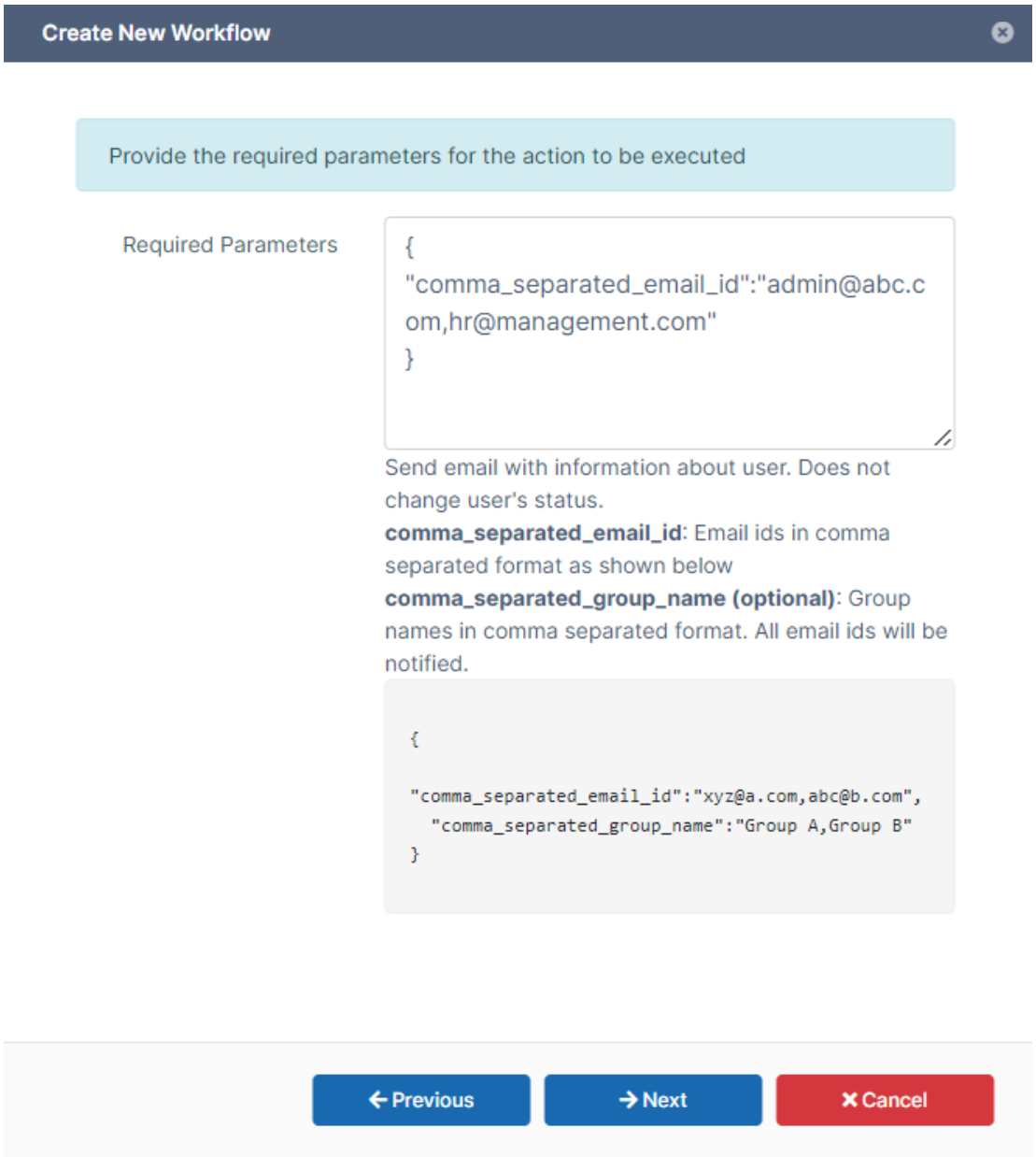


6. Click Next, set Then Action **Generate an email report**.



7. Enter the Required parameters in the given format

```
{
"comma_separated_email_id":"admin@abc.com,hr@management.com"
}
```



8. Click **Next**, give an appropriate workflow name, and click **Finish**.

Notify on File Upload Workflow

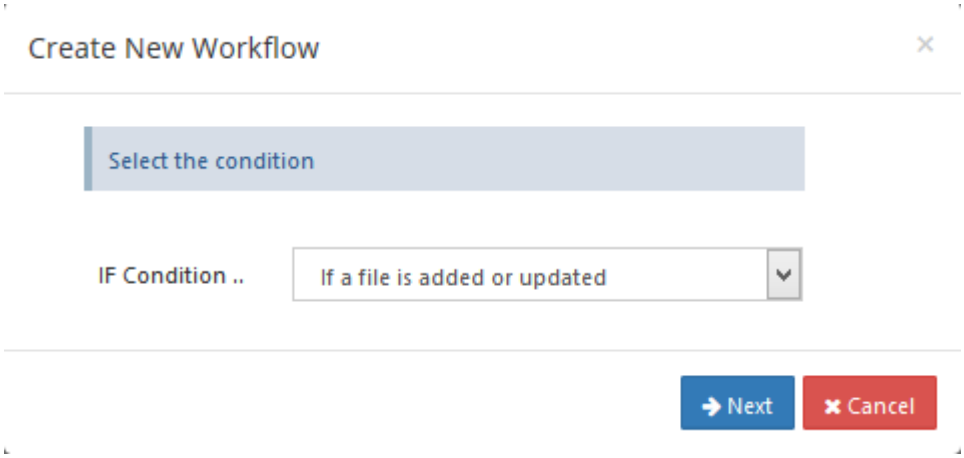
This workflow recipe sends an email notification when a file is created or uploaded to FileCloud.

- This notification can be set for a specific folder location only
- The admin can provide a set of email ids to which the notification email has to be sent

To create a workflow to notify when a file is uploaded:

1. Login to Admin Portal

2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition to **If a file is added or updated** and click **Next**

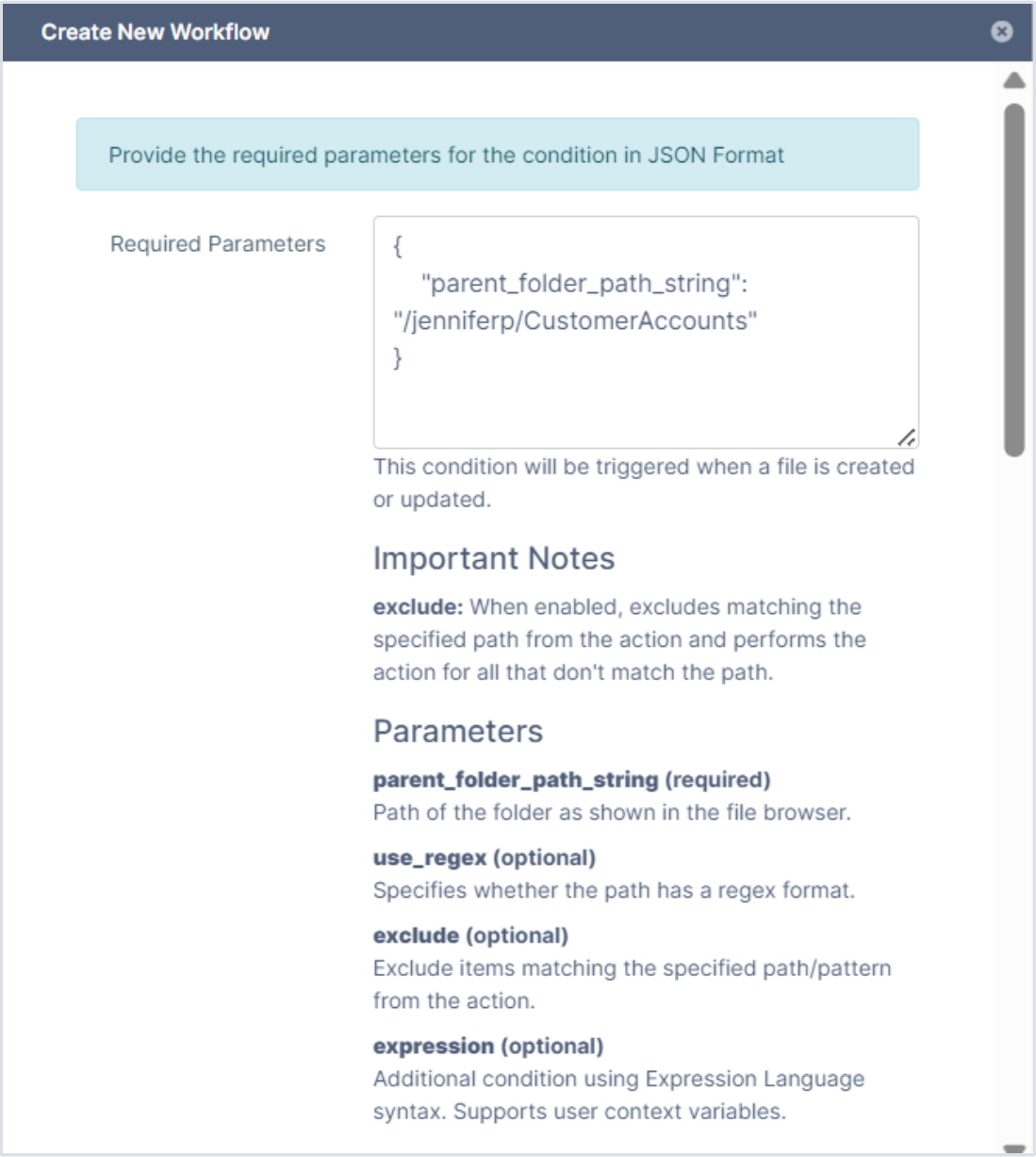


5. Enter the Required parameters in the given format, and click **Next**.

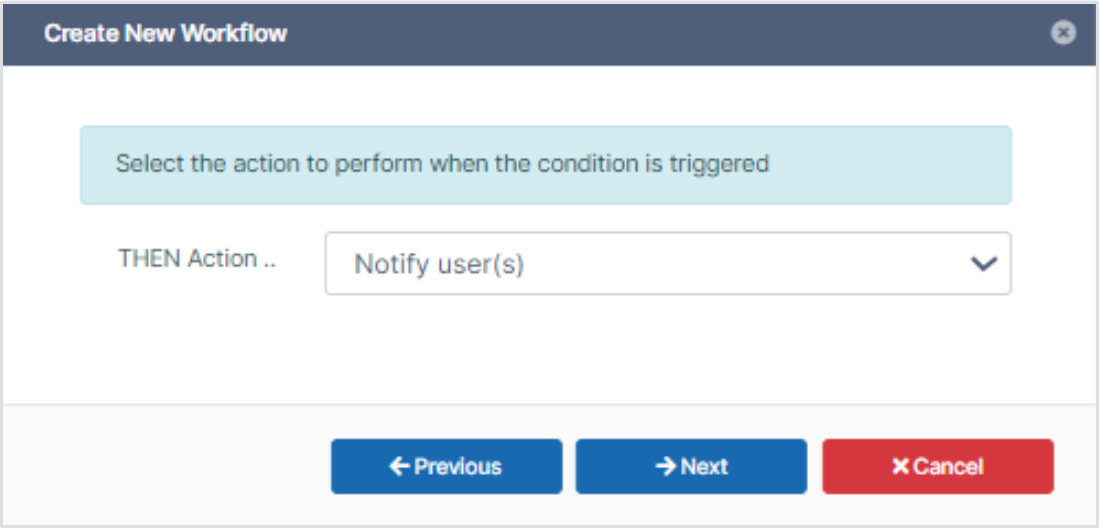
```
eg: Path : My Files Location (/jenniferp/CustomerAccounts)
{
"parent_folder_path_string":"/jenniferp/CustomerAccounts"
}
```

To identify FileCloud specific path for a folder please refer this Identifying a FileCloud Specific Path.

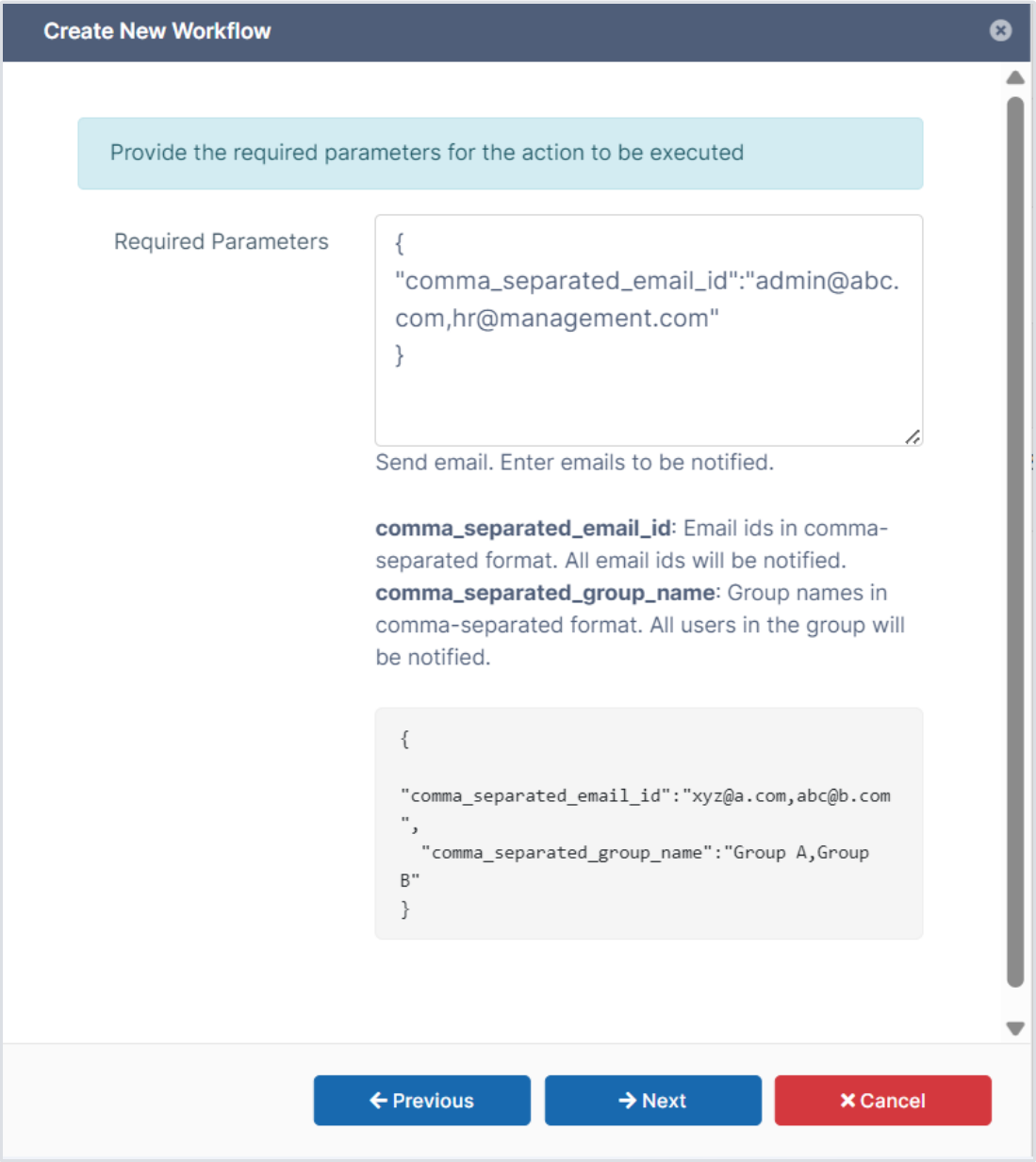
> `Set the path to "/" if you want to monitor all the folders in the system.`



6. Set the then action to **Notify user(s)**, and click **Next.**

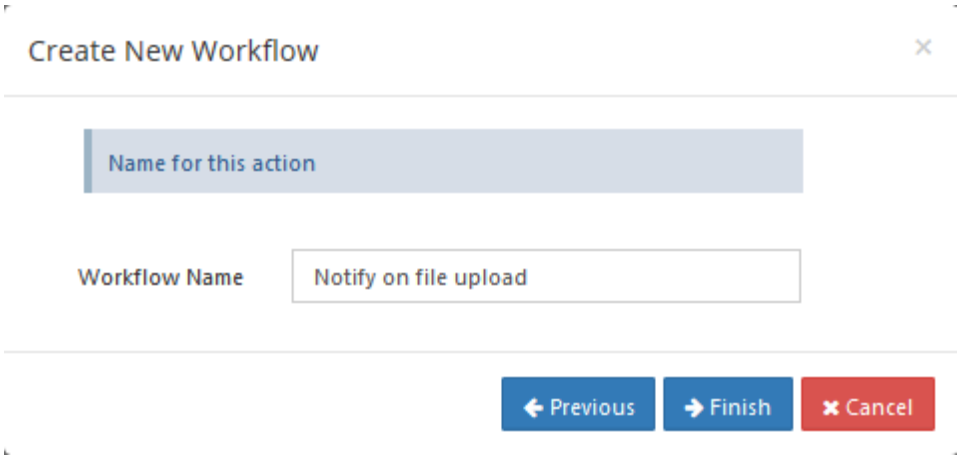


7. Enter the Required parameters in the given format

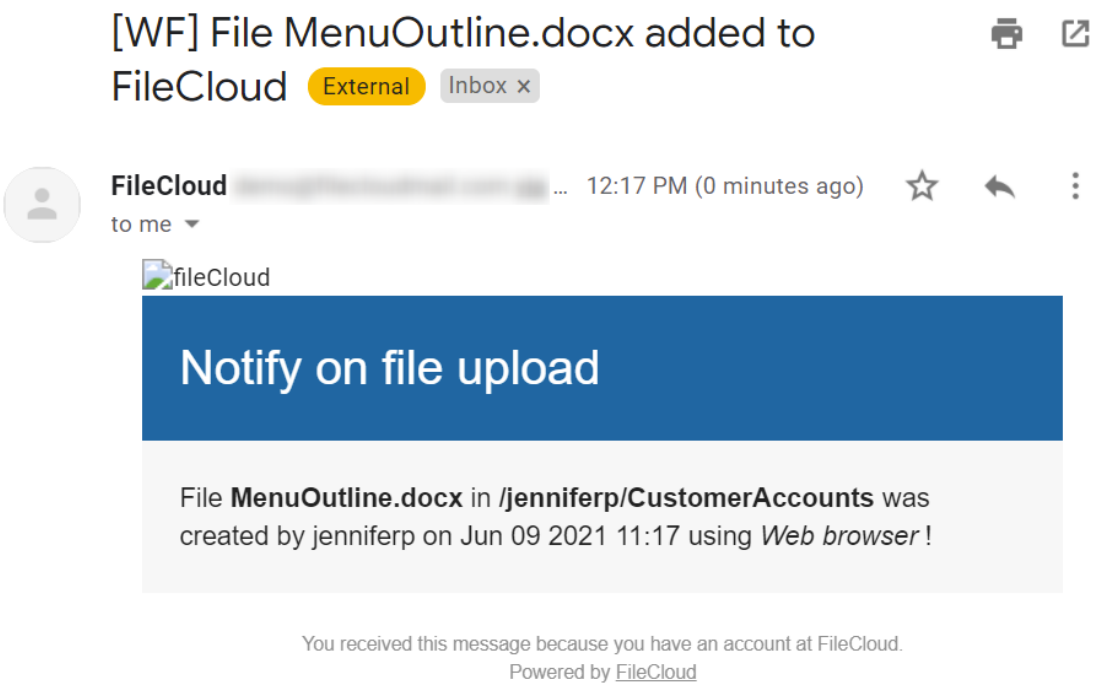



```
{
"comma_separated_email_id":"admin@abccompany.com,hr@management.com"
}
```

8. Click **Next**, then give an appropriate workflow name and click **Finish**.



9. Sample notification email on a file upload.



Periodic Script Workflow

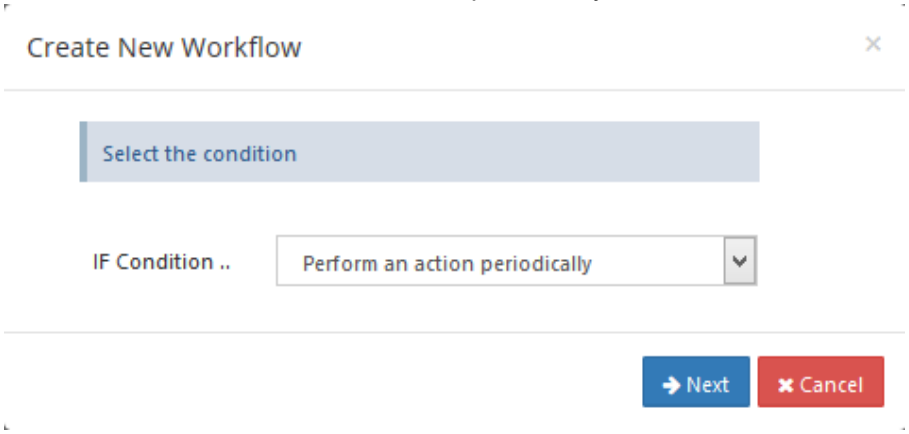
This workflow recipe runs a specified command at a periodic interval.

- This requires you to set up cron job or task scheduler to run the command.

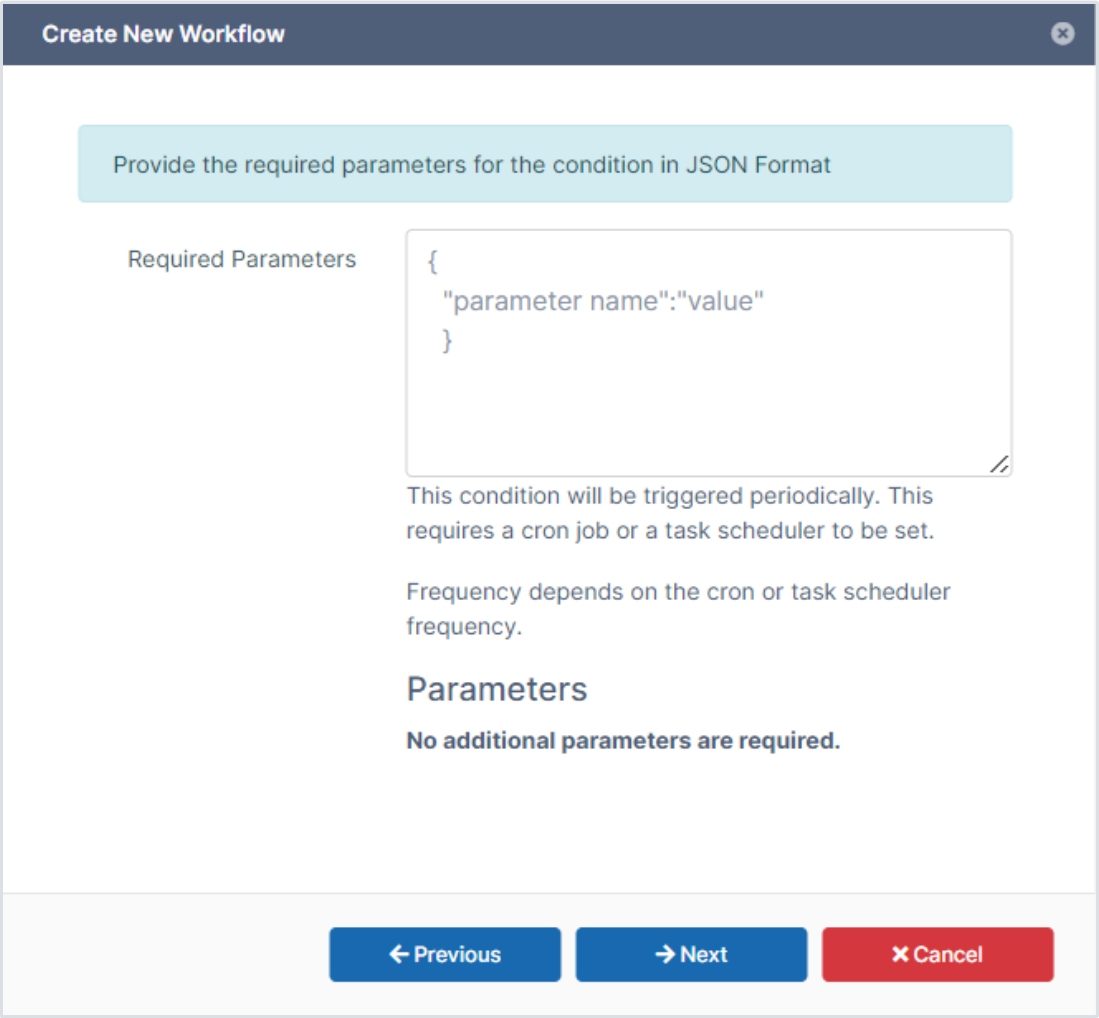
- The frequency depends on the cron or task scheduler frequency you set

To create a workflow that performs a periodic script:

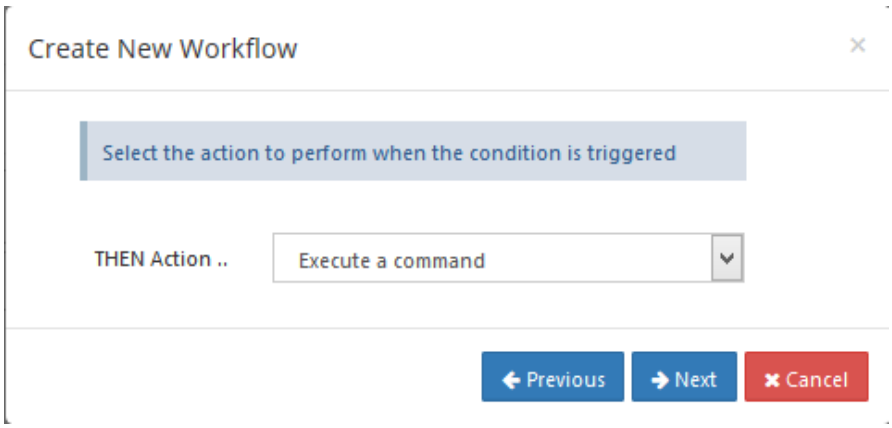
1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition " Perform an action periodically "



5. Click on Next, This condition does not require any parameters



6. Set the Then Action "Execute a command"

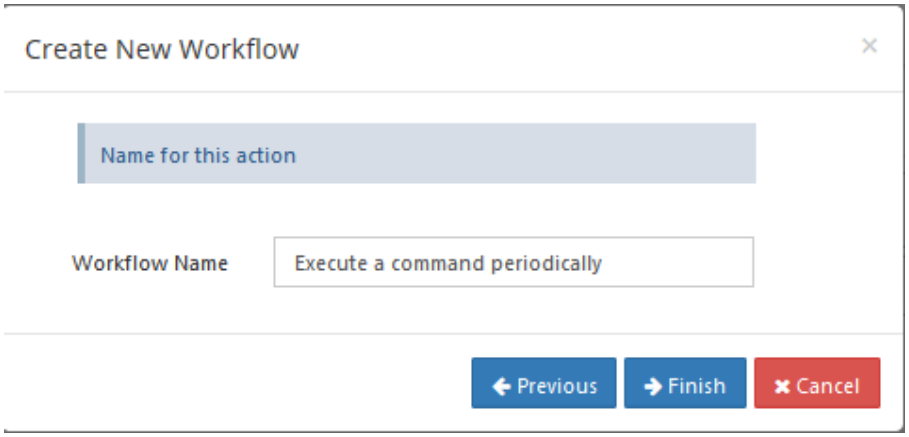


7. Enter the required Command.
   In the following example, ls causes all files and folders to be listed.:

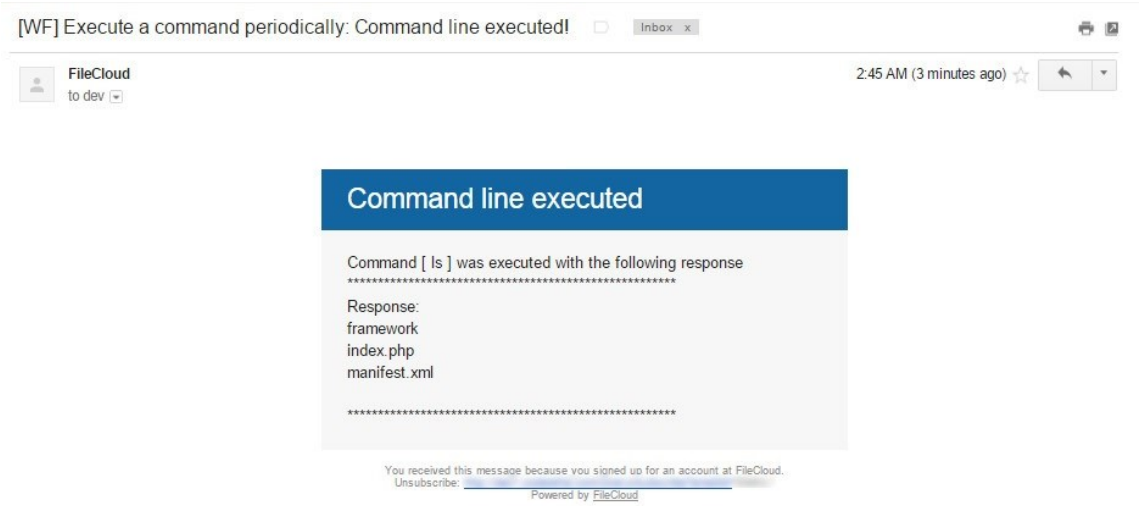
```
{
"command_line":"ls"
```

```
}
```

8. Enter the Workflow name and Finish.



9. A notification email will be sent to the Admin, with the response information of command line execution.



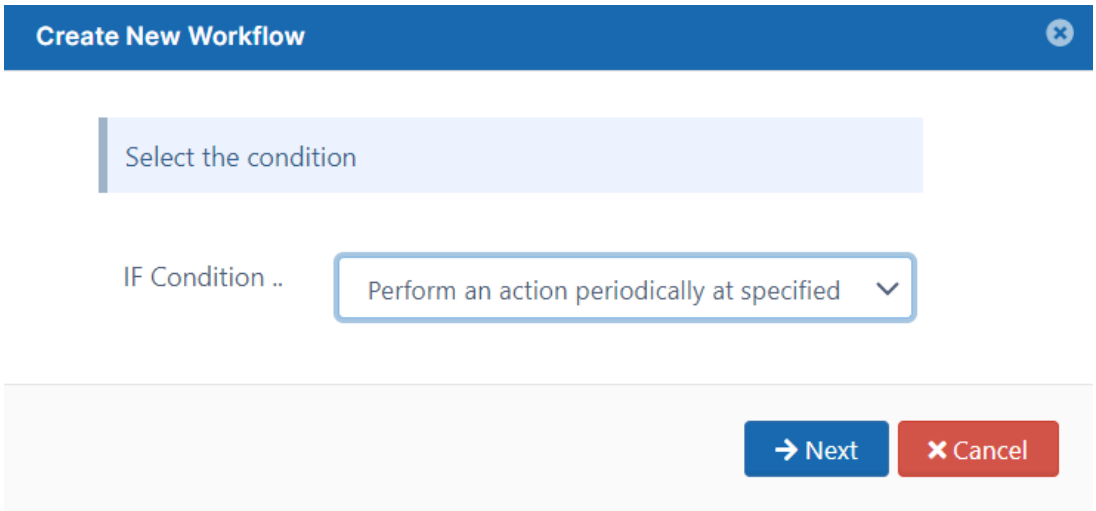
Periodically Send Custom Email Workflow

This workflow recipe sends a custom email to selected users at specified intervals.

In the example, an email is sent to users in the **Employees** group every 30 days from January to June to remind them to submit their receipts to a **Reimbursements** folder.

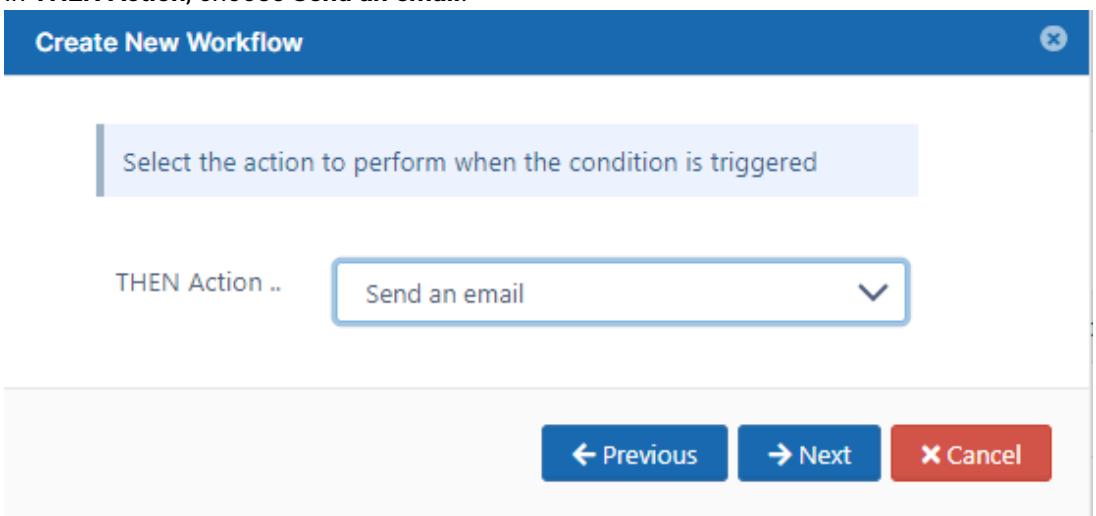
To create a workflow that sends a custom email periodically:

1. In the admin portal's navigation panel, click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
3. In **IF Condition**, choose **Perform an action periodically at specified time and interval**.



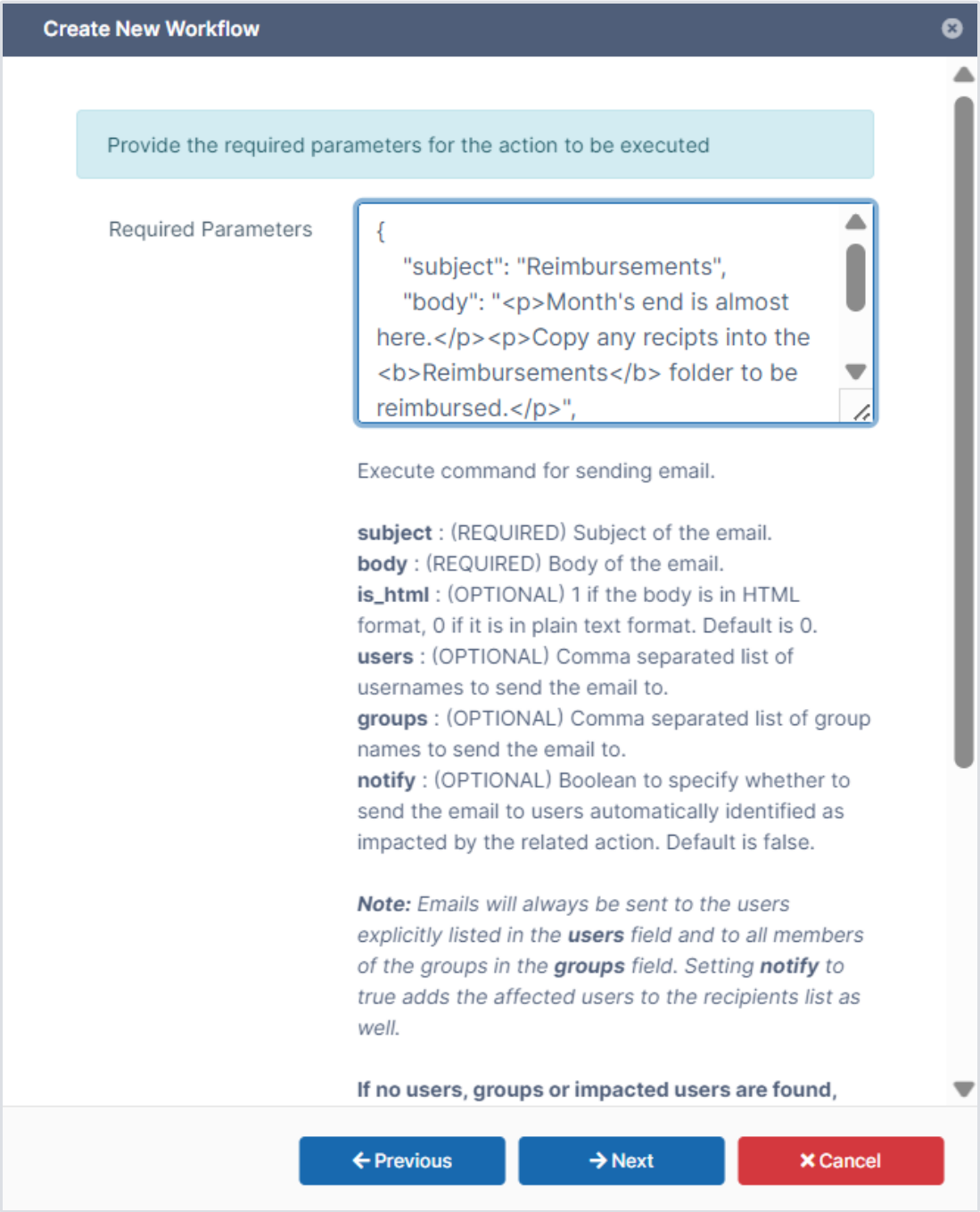
4. Click **Next**.
5. Set the parameters according to your requirements for the interval.
   In the image below, the message is scheduled to be sent approximately monthly for the first half of 2024 (every 30 days from January 1, 2024 to June 30, 2024).

6. Click **Next**.
7. In **THEN Action**, choose **Send an email**.

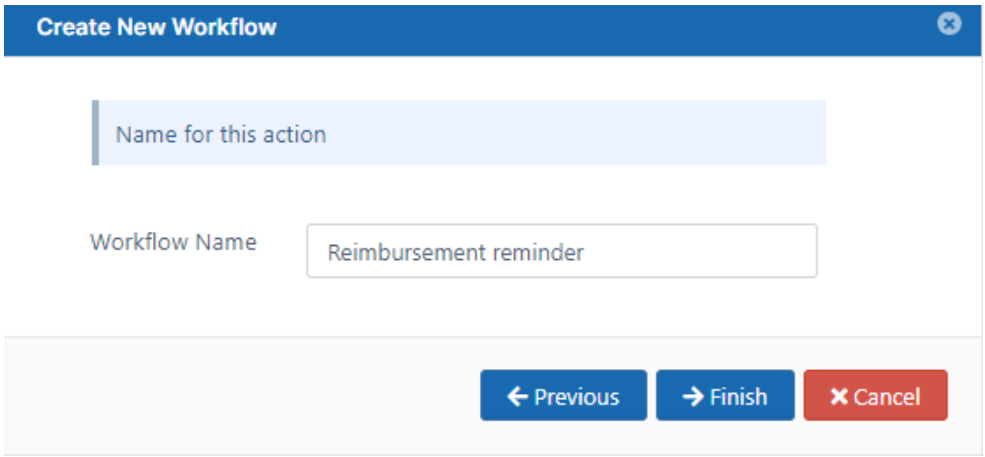


8. Click **Next**.
9. Use the parameters to enter the details of the custom email.
   In the parameters below, an email with the subject **Reimbursements** reminds users in the group **Employees** to copy their receipts into the Reimbursements folder.
   Since **is_html** is set to **1**, tags in the body are recognized as HTML tags and formatted.

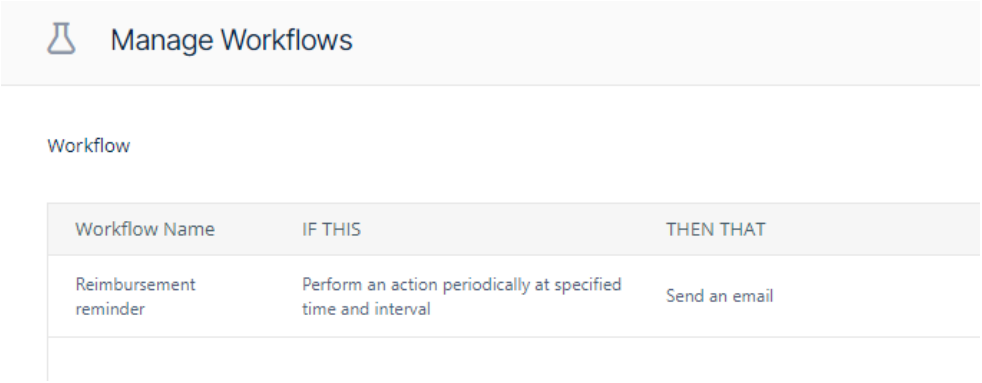
```
{
    "subject": "Reimbursements",
    "body": "<p>Month's end is almost here.</p><p>Copy any recipts into the
<b>Reimbursements</b> folder to be reimbursed.</p>",
    "is_html": 1,
    "groups": "Employees",
}
```



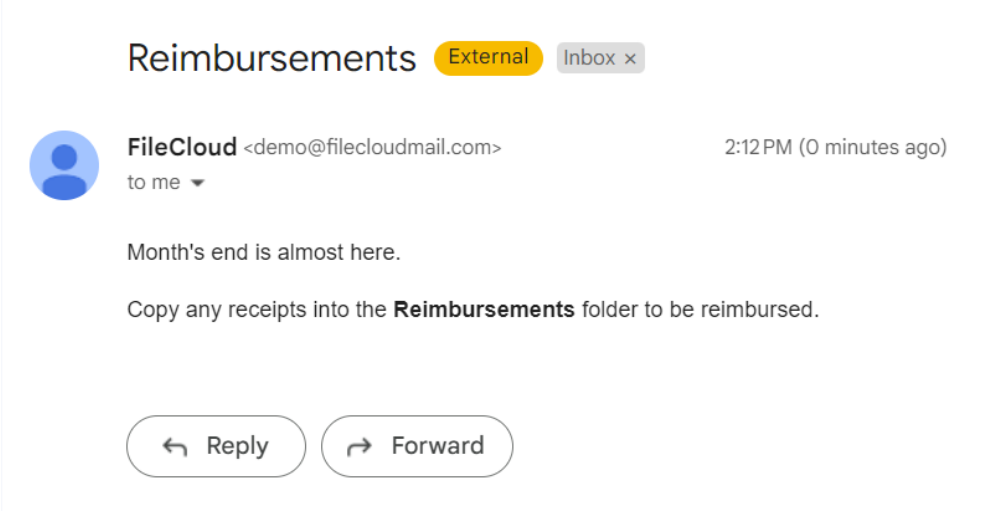
10. Click **Next**.
11. Give the workflow a name, and click **Finish**.



The workflow is listed in the **Manage Workflows** page. It will run automatically in 30 days.



12. In 30 days, the workflow automatically runs, and sends the following email to users of the group **Employees**.



Automated Workflow Management

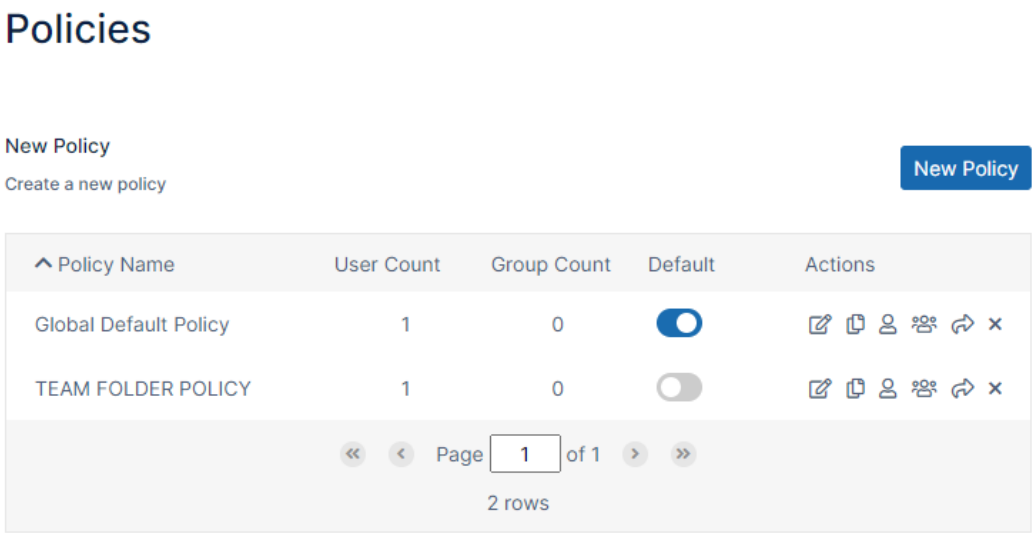
> Automated Workflows are available in FileCloud 21.2 and later.
> Prior to FileCloud 23.251, by default, all users could share automated workflows. Beginning in 23.251, the setting **Allow Automation Workflow Sharing** must be enabled to permit all users to share automated workflows.

Disabling Automated Workflows

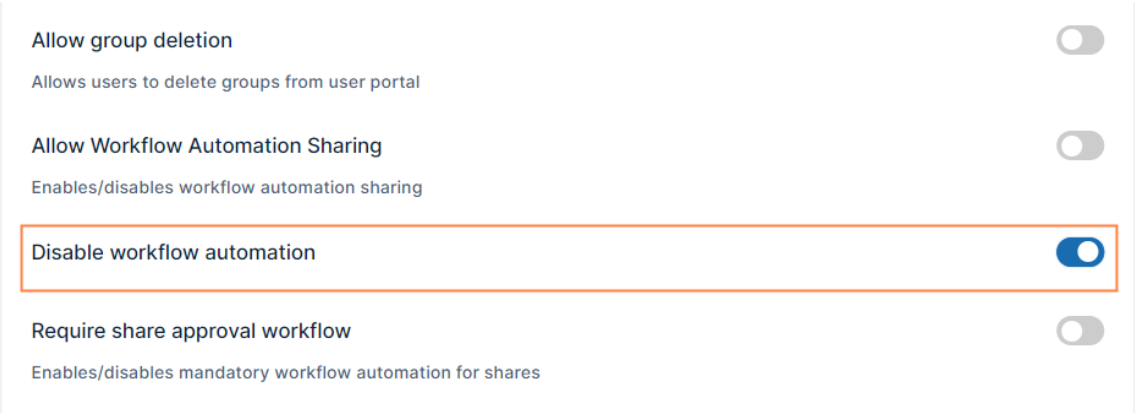
Automated Workflows enable users in the user portal to create automated processes, such as file approvals and file storage. By default the Automated Workflow function is enabled, but you can disable it.

To disable the Automated Workflows for certain users, disable them in the users' policies.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** page opens.



2. Open the policy assigned to the users who you do not want to access Automated Workflows.
3. Click the **Users** tab.
4. Scroll down and locate the **Disable workflow automation** setting. Enable the setting.



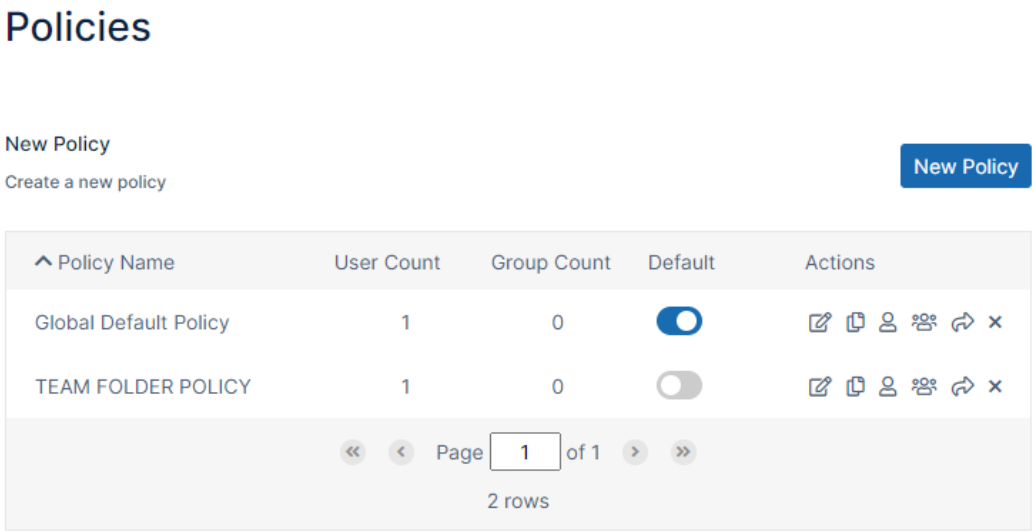
5. Click **Save**.
   The **Workflows** navigation link no longer appears in the user portal of users assigned to the policy.

Enable Sharing of Automated Workflows

By default, users other than promoted admins with all user share and file privileges, cannot share automated workflows with other users. Enabling this setting allows all users to share automated workflows.

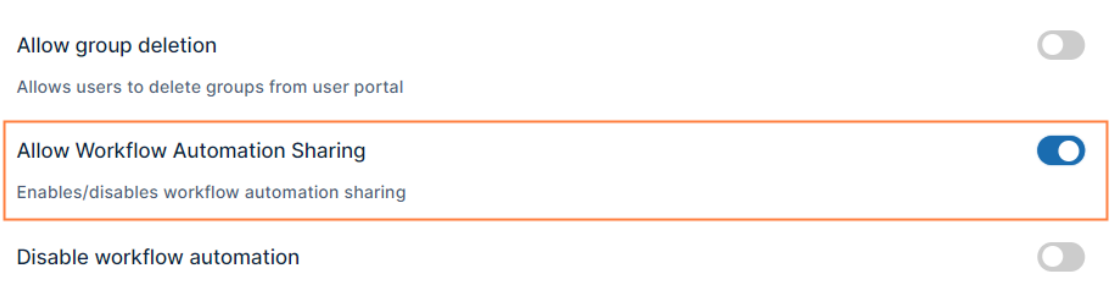
To enable sharing of Automated Workflows for certain users, enable the setting in the users' policies.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** page opens.



2. Open the policy assigned to the users who you want to be able to share automated workflows.
3. Click the **Users** tab.

4. Scroll down and locate the **Allow Workflow Automation Sharing** setting. Enable the setting.



5. Click **Save**.
   Now, all users have the ability to share automation workflows.

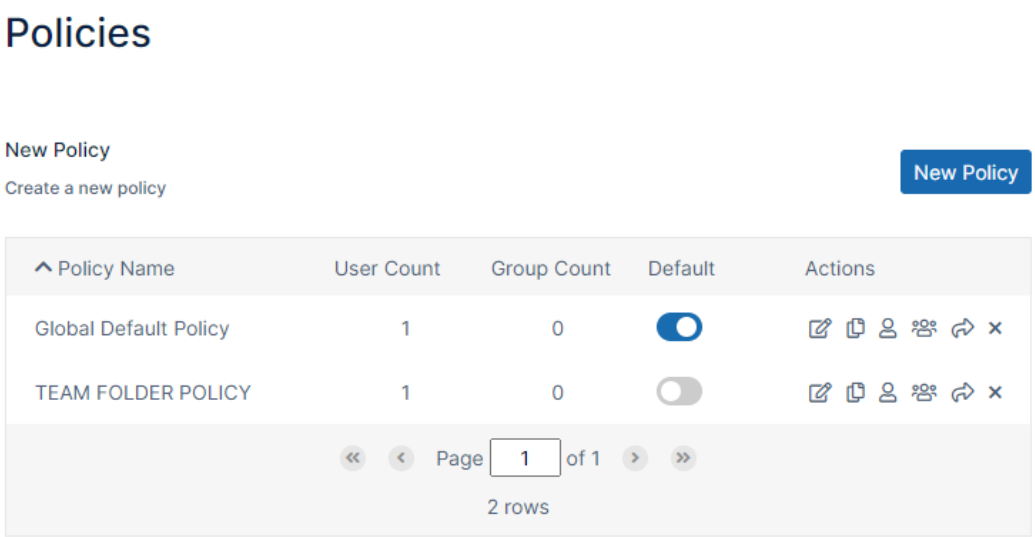
Requiring a Share Approval Workflow

A Share Approval workflow is a specialized type of workflow that requires a share to be approved before it is made available.
In order for a Share Approval workflow to become active for specific users, you must mark it required in their policies and choose the specific Share Approval workflow to use.

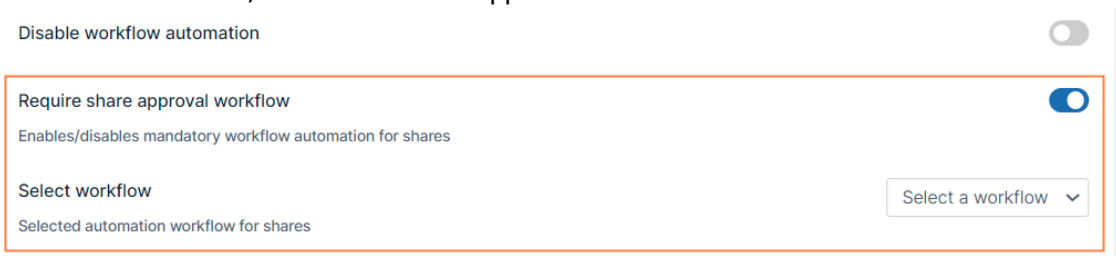
> For the Share Approval workflow to apply to all users' shares in FileCloud, it must be created by a promoted Admin with all User Share permissions enabled. Otherwise, the share approval workflow will only apply to shares initiated by the workflow creator on files and folders in their My Files folder.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** page opens.



2. Open the policy assigned to the users who you do not want to access Automated Workflows.
3. Click the **Users** tab.
4. Scroll down to **Require share approval** and enable it**.**
5. In **Selected Workflow**, choose the Share Approval workflow to make effective.



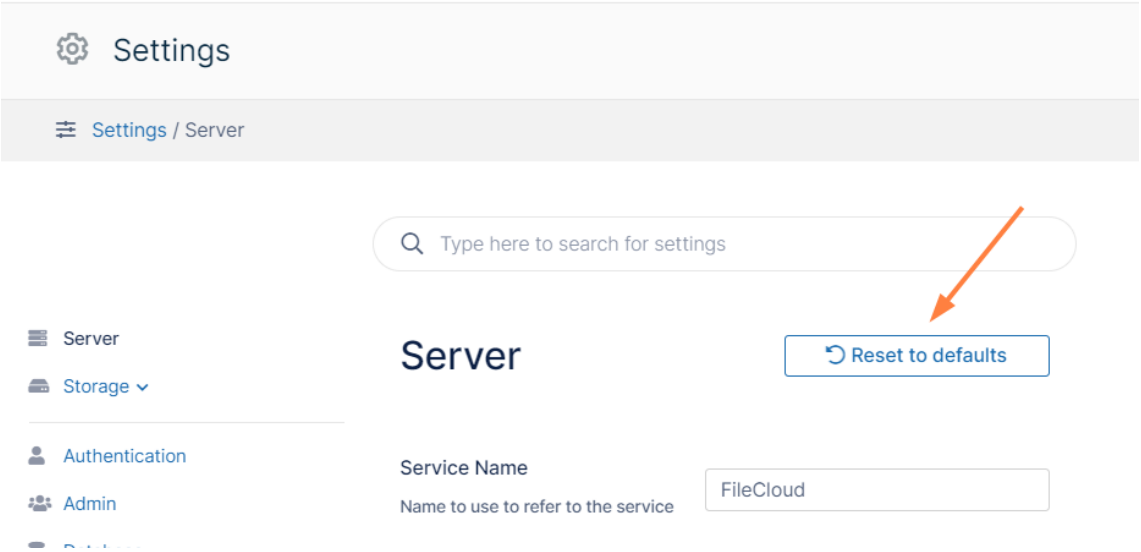
For end user information on creating Automated Workflows, see Workflow Automation.

Reset Settings and Customizations

> Beginning in FileCloud 20.1, the option for resetting all selections in the Settings and Customization pages is located in the Reset tab on the Settings page. In FileCloud versions earlier than 20.1, the **Reset All** button appears in the upper-right corner of the Settings and Customization pages and resets both settings and customizations regardless of which page you access it from.

To return to default settings for options in Settings

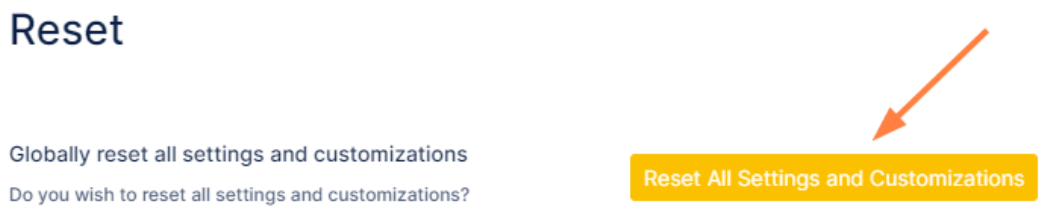
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**, then navigate to the page whose settings you want to reset.
2. Click the **Reset to defaults** button in the upper right of the page.



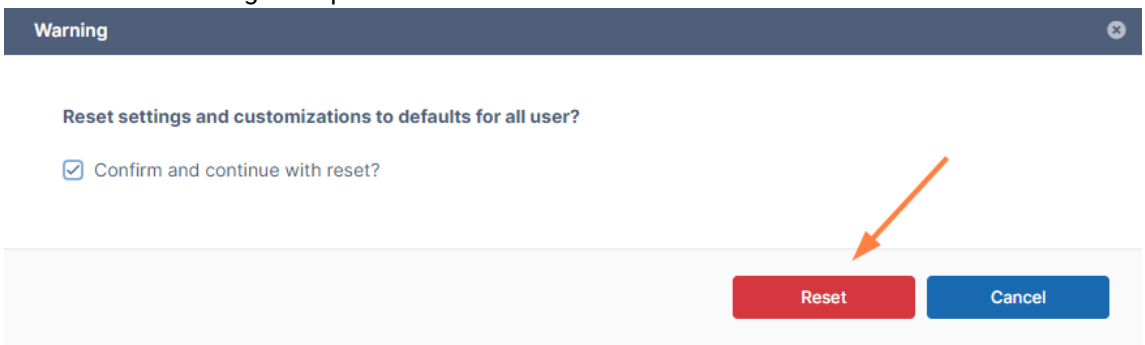
   A confirmation dialog box opens.
3. Click **OK.**
   The settings on the page are set back to their default settings.

To return to default settings for all options on the Settings pages:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Reset** .
   The Reset page opens.
2. Click **Reset All Settings and Customizations**.



A confirmation dialog box opens.



3. Check **Confirm and continue with the reset**, and click **Reset.**
   All of the options that appear on the Settings and Customization pages are reset to their defaults.