



FileCloud Online Version 23.232

Site Maintenance

Copyright Notice

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

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

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

Copyright Notice	2
Admin Portal Dashboard	8
Setup Checklist	8
Quick Actions.....	9
Dashboard Widgets.....	10
Release Notifications	20
By Subscribing to the Mailing List	20
Managing Users.....	21
Listing FileCloud Users	21
Viewing User Properties.....	22
Disable a FileCloud User Account.....	31
Deleting a FileCloud User	34
Resetting a User Password	35
Manage A User's Policies	37
Manage a User's Profile Picture.....	40
Change a User's Email Address	41
Setting a User Account to Expire	41
Send Email from User Details	42
Managing Groups	44
Change a User Group Name	44
Delete a User Group	44
View and Change Group Members	45
Exporting a list of users in a group	46
Managing Admin Users	48
Check an admin user's permissions.....	48
Remove an admin role.....	53
Managing User Folders and Files.....	55

What do you want to do?	55
Copy and Move User Files	56
Download User Files and Folders	58
Cancel User Uploads in Progress.....	60
Delete User Folders and Files	60
Clear a Recycle Bin	61
Remove a User's Old File Versions	63
Remove Incomplete User Uploads.....	64
Restore a Previous File Version	66
Change the Name of the Zip File for Multiple File Downloads.....	68
Managing User Shares	71
To manage user shares for an individual user:.....	71
To manage user shares for all users:.....	73
To export a list of all shares:	74
Transfer Ownership of a Reshare from a Team Folder or Network Share	75
Creating direct file download link from a public file share.....	78
Creating direct file download links from a public folder share	78
Managing Storage Space Usage	81
Related topics.....	81
Managing User Locks	82
Managing User-Defined Notifications	86
Editing individual user's file and folder notifications	86
Editing all users file and folder path notifications	89
Adding notifications for actions on user's files and folders.....	91
Managing Client Devices.....	94
FAQ's	95
How Do You Want to Manage a Device?	96
Centralized Device Management	100
iOS Device Management.....	140
Search in the Admin Portal.....	143

FileCloud's Federated Search.....	143
All search	145
Audit Logs	150
What do you want to do?	150
View Audit Logs	150
Filter Audit Log Views.....	152
Configure What is Logged	154
Export Audit Logs	156
Delete Audit Log Entries	156
FileCloud Alerts	158
File Content Heuristic Engine	159
Identifying a FileCloud Specific Path	164
Custom Reports.....	166
Add Reports	166
Download Reports	169
Available Reports	169
Specifying Y-M-d H:i:s values	176
Manage Folder Level Permissions.....	178
To Edit Folder Level Security	178
Managing Metadata	180
Metadata for governance and other system processes	180
Metadata for users	182
Metadata Components and Types	183
Create a New Metadata Set	187
Edit an Existing Metadata Set.....	190
Managing Metadata Attributes.....	193
Managing Metadata Permissions	196
Video of Managing Metadata	200
Working with Built-In Metadata	201
Working with Custom Metadata	217

Working with Default Metadata.....	218
Metadata Limitations/Recommendations.....	221
Managing FileCloud Licenses	223
FileCloud - License Purchase And Renewal	223
Workflows - IFTTT	242
The Workflow Dashboard	242
Add a New Workflow	243
Define an IF Condition	244
Define a THEN Action	269
Edit a Workflow	283
Run a Workflow	284
Set Advanced Workflow Options.....	285
Workflow Recipes for FileCloud	291
Automated Workflow Management	332
Disabling Automated Workflows.....	332
Requiring a Share Approval Workflow	332
Reset Settings and Customizations	334
To return to default settings for options on a Settings or Customization tab.....	334
To return to default settings for all options on the Settings and Customization pages:	334

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

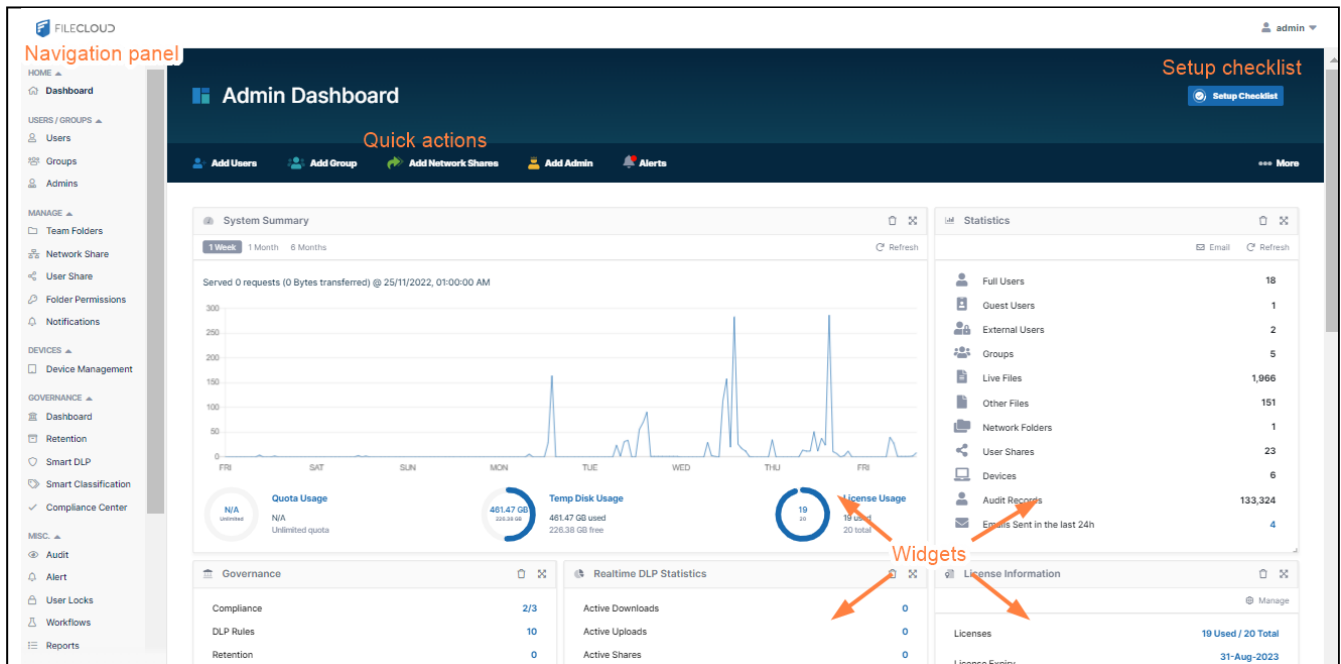
- [Admin Portal Dashboard](#)
- [Release Notifications](#)
- [Managing Users](#)
- [Managing Groups](#)
- [Managing Admin Users](#)
- [Managing User Folders and Files](#)
- [Managing User Shares](#)
- [Managing Storage Space Usage](#)
- [Managing User Locks](#)
- [Managing User-Defined Notifications](#)
- [Managing Client Devices](#)
- [Search in the Admin Portal](#)
- [Audit Logs](#)
- [FileCloud Alerts](#)
- [File Content Heuristic Engine](#)
- [Identifying a FileCloud Specific Path](#)
- [Custom Reports](#)
- [Manage Folder Level Permissions](#)
- [Managing Metadata](#)
- [Managing FileCloud Licenses](#)
- [Workflows - IFTTT](#)
- [Automated Workflow Management](#)
- [Reset Settings and Customizations](#)

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.

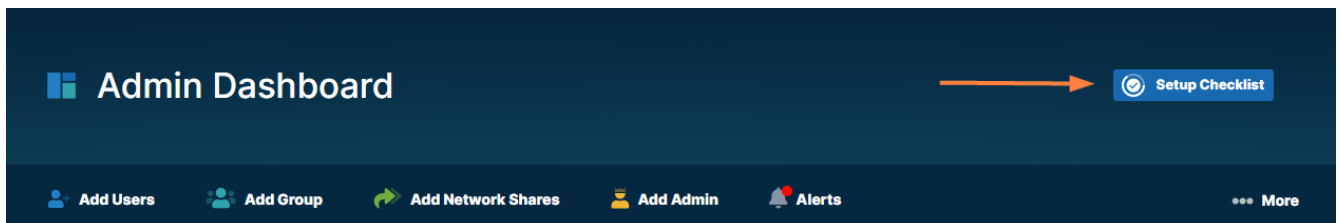
💡 The Admin dashboard displays several areas to help you manage your site.

- **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.



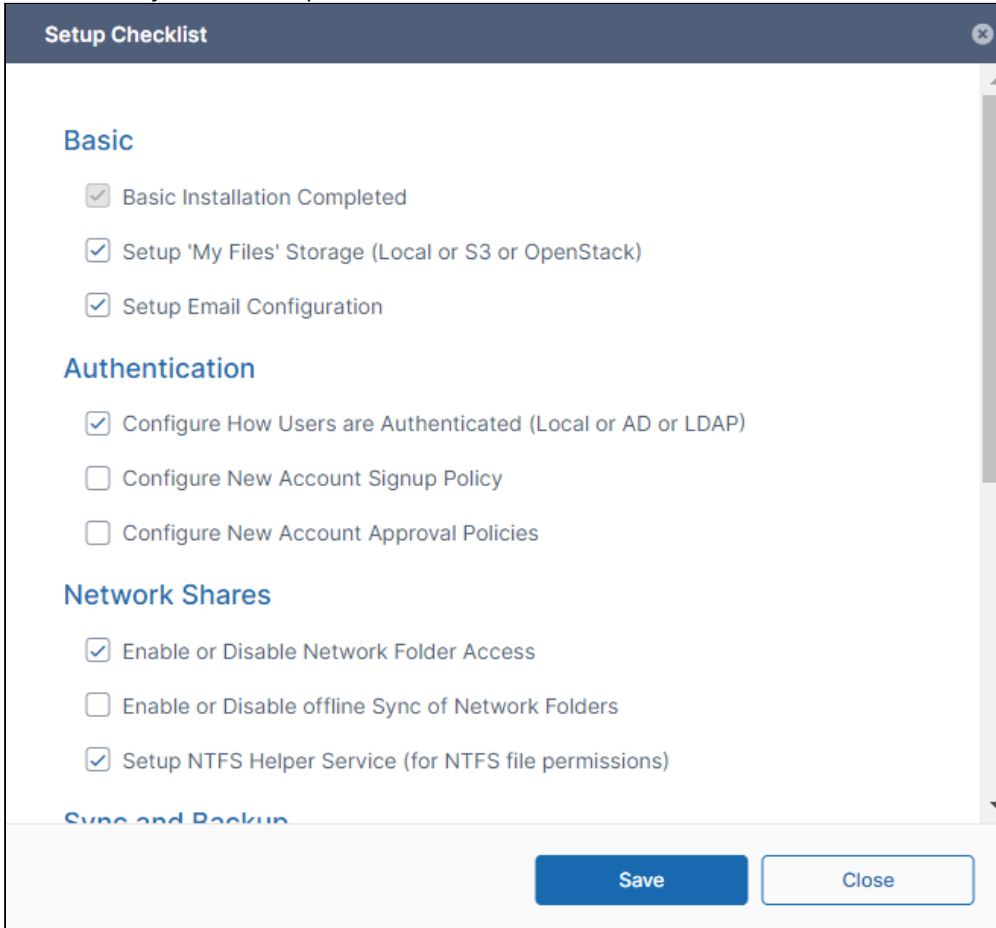
Setup Checklist

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.

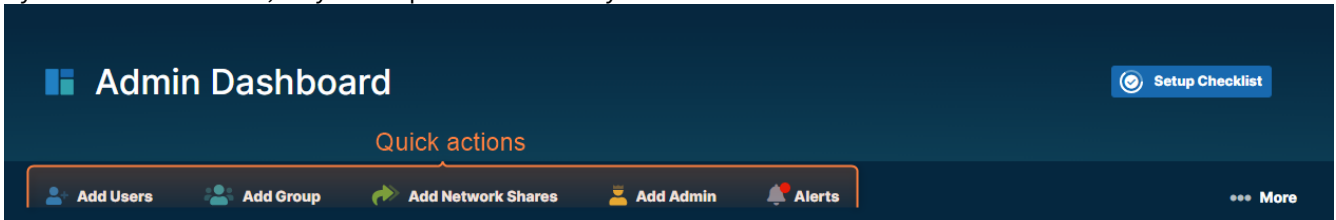


Quick Actions

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](#)

Dashboard Widgets

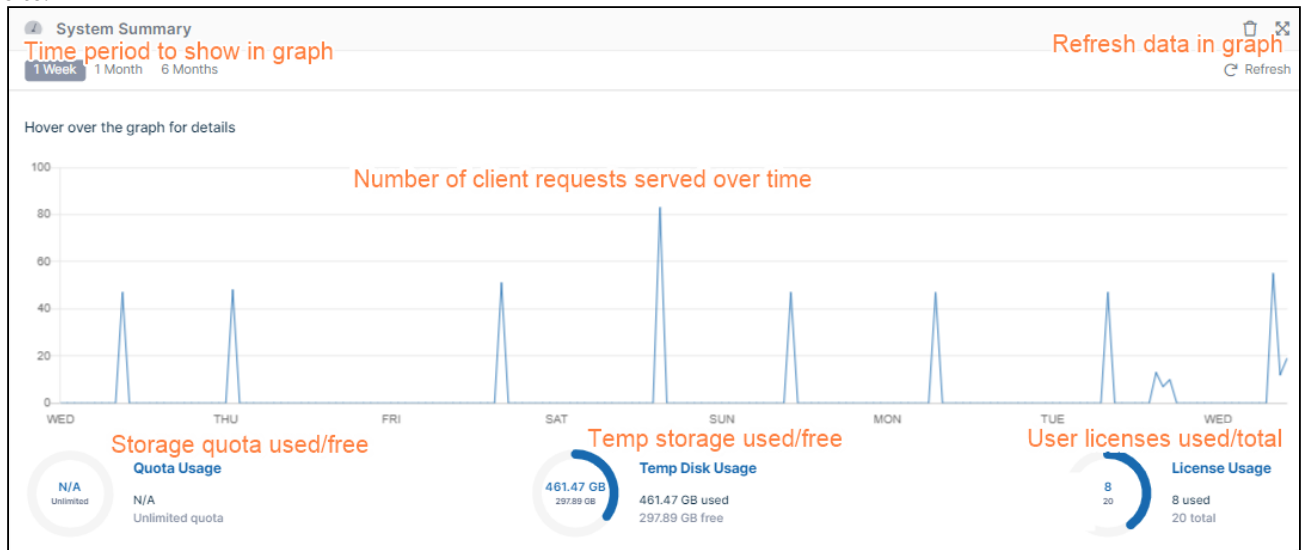
The FileCloud dashboard has widgets that display real-time information. If you are an Admin user, only those widgets involving actions you have access to are listed.

- 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:

Statistics	
Email Refresh	
Full Users	18
Guest Users	1
External Users	2
Groups	5
Live Files	1,966
Other Files	151
Network Folders	1
User Shares	23
Devices	6
Audit Records	133,324
Emails Sent in the last 24h	4

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.

Statistic	Description
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.

Governance	
Compliance	3/3
DLP Rules	10
Retention	0
Content Classification	0

Realtime DLP Statistics

This widget displays DLP statistics in real-time, and displays reports of Active Downloads, Active Uploads, Active Shares, and Active Users when you click the number on the right. When you click the number to the right of Violations, the [Manage DLP Rules](#) page opens.

Realtime DLP Statistics	
Active Downloads	0
Active Uploads	0
Active Shares	0
Active Users	2
Violations	0

License Information

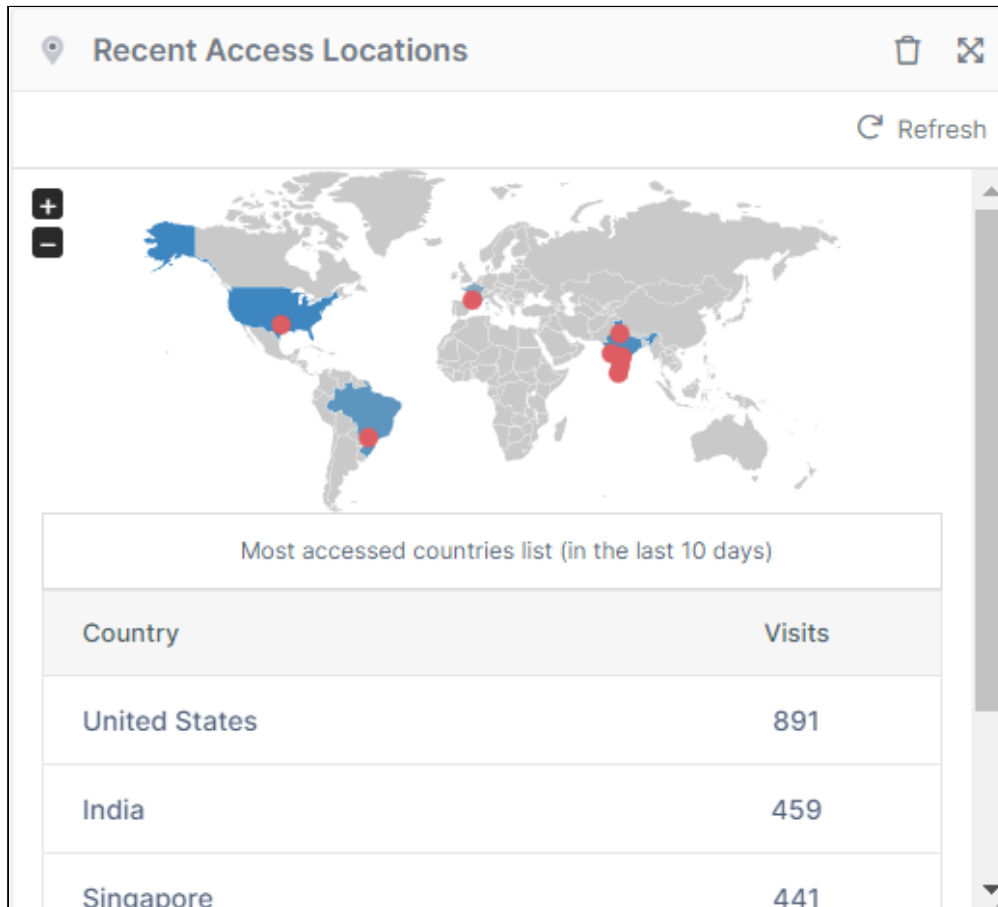
This widget shows you basic information about your license.

License Information	
Manage	
Licenses	15 Used / 500 Total
License Expiry	30-Aug-2022 (236 days left)
License Owner	CodeLathe Technologies Inc

In the upper-right corner of the widget, click **Manage** to go to the Settings page, License tab. To update your license, see [Viewing Your License Details](#).

Recent Access Locations

The Recent Access Locations report (also referred to as the Geo IP 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 Location report is not enabled by default. To enable the Recent Access Location report go to Admin UI > Settings > Admin tab, where it is referred to as the Geo IP report.

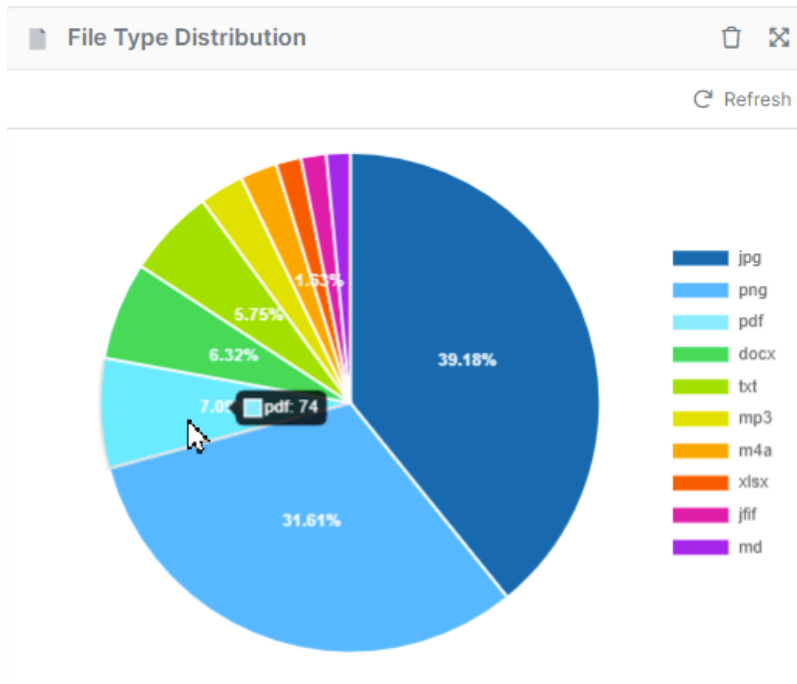
Settings	Value
Show Geo IP Report	TRUE - Show the Geo IP Map with data FALSE - Hide the Geo IP Map from the dashboard DEFAULT - Show the Geo IP Map with no data.
Geo IP Server URL	Server URL that converts the IP address to Geo Location Data. Default URL: http://geoiplookup.codelathe.com/geoip.php To point this URL to a different location contact FileCloud support.

Settings	Value
Geo IP Update frequency in Hours	The Frequency with which the GeoIP data is retrieved from the server. Default : 24.

NOTE: The Recent Access Location (GeoIP) map and report displays with proper data only when CRON job is set up and running and the access IP address recorded in audit are external IP.

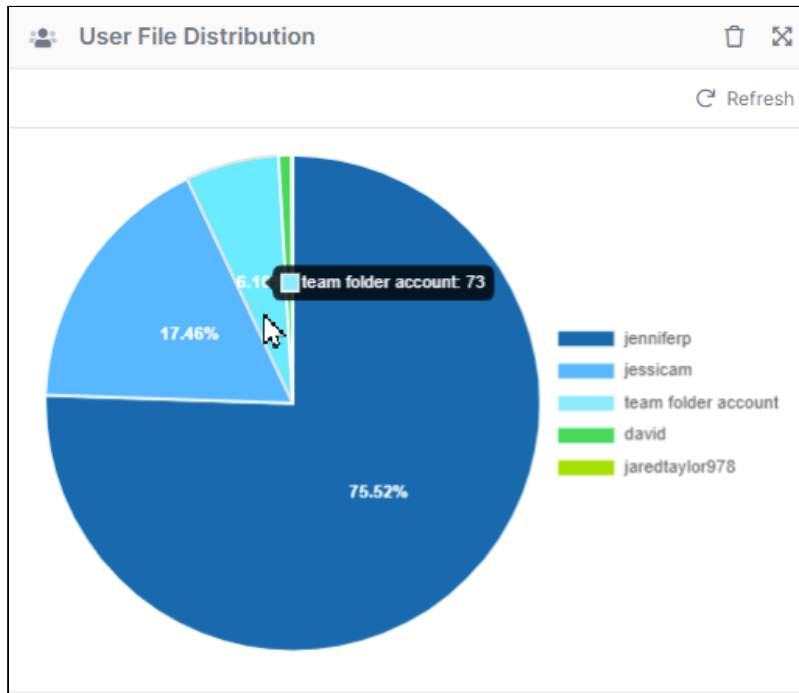
File Type Distribution

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

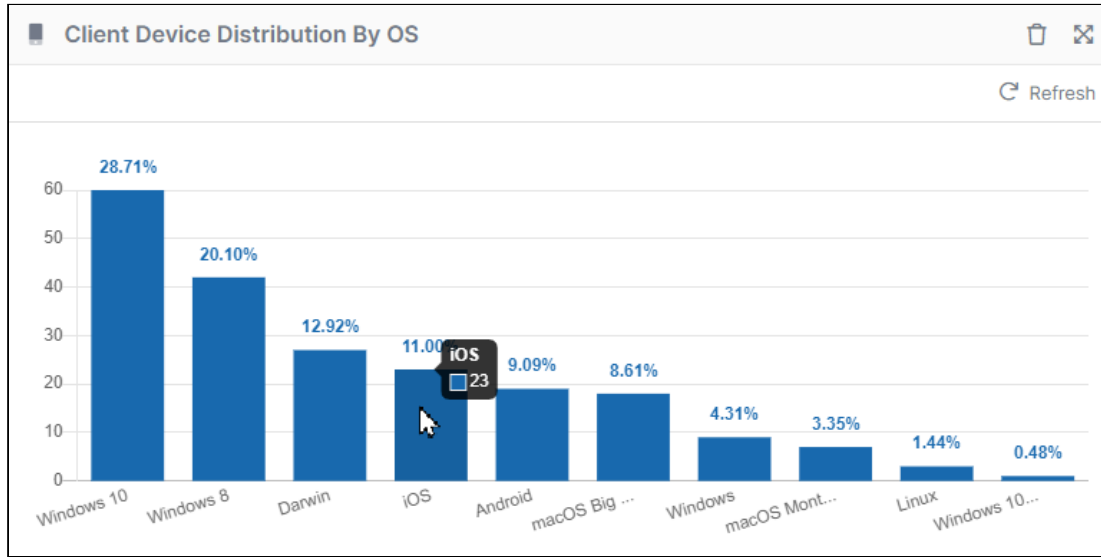
The Version Information widget displays your currently installed version and the latest available version of the system. If there is a new version available, the **Update(s) Available** button displays **Yes**.

The Version Information widget provides a clear comparison between the installed and latest versions. It includes an 'Upgrade' button and a status indicator for updates.

Current Version	21.3.0.18444
Latest Version	21.2.4.17315
Update(s) Available	Yes

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.

% Used	User name	File Count	Quota Used	Quota Assigned
	jenniferp	905	1.13 GB	2 GB
	jessicam	209	495.97 MB	2 GB
	team folder account	73	101.53 MB	0 B
	redtaylor978	1	523 KB	2 GB
	david	10	516 KB	2 GB

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.

Admin Dashboard Setup Checklist

Add Users Add Group Add Network Shares Add Admin Alerts More

System Summary Refresh

1 Week 1 Month 6 Months

Hover over the graph for details

250
200
150
100
50
0

THU FRI SAT SUN MON TUE WED THU

Quota Usage
N/A Unlimited
N/A Unlimited quota

Temp Disk Usage
461.47 GB
292.55 GB
461.47 GB used
292.55 GB free

License Usage
8 used
20 total

Statistics Email Refresh

Full Users	8
Guest Users	0
Limited Users	1
Groups	8
Live Files	996
Other Files	184
Network Folders	1
User Shares	43
Devices	6
Audit Records	49,046
Emails Sent in the last 24h	0

Governance Manage

Compliance 3/3

Realtime DLP Statistics Manage

Active Downloads 0

License Information Manage

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

Admin Dashboard Setup Checklist

Add Users Add Group Add Network Shares Add Admin Alerts More

Governance Manage

Compliance	3/3
DLP Rules	10
Retention	0
Content Classification	0

Realtime DLP Statistics Manage

Active Downloads	0
Active Uploads	0
Active Shares	0
Active Users	2
Violations	0

Statistics Email Refresh

Full Users	8
Guest Users	0
Limited Users	1
Groups	8
Live Files	996
Other Files	184
Network Folders	1
User Shares	43
Devices	6
Audit Records	49,539
Emails Sent in the last 24h	0

System Summary Refresh

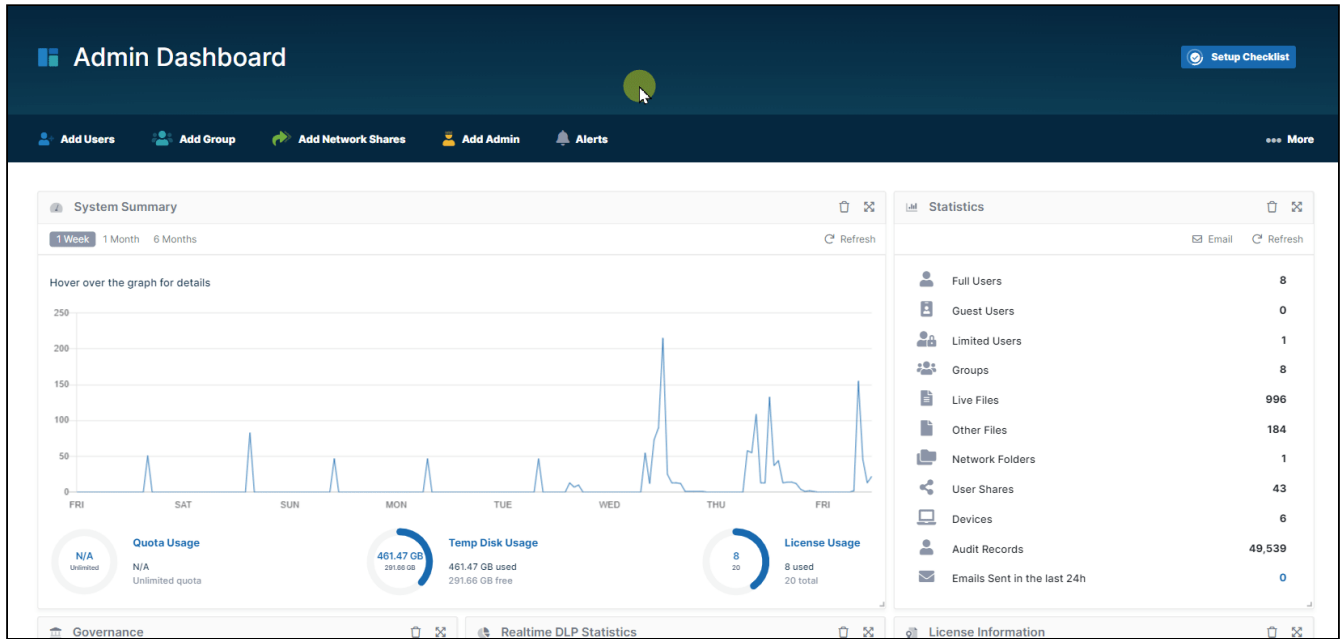
1 Week 1 Month 6 Months

Hover over the graph for details

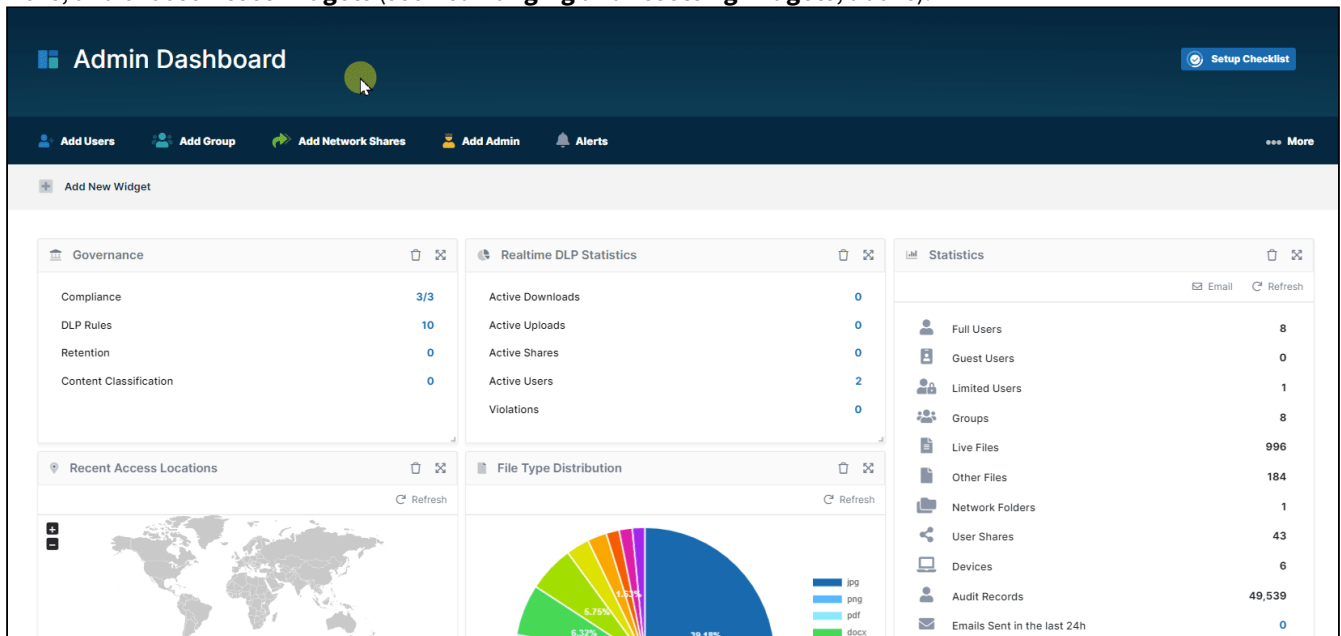
250
200
150
100

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:

- [Listing FileCloud Users](#)
- [Viewing User Properties](#)
- [Disable a FileCloud User Account](#)
- [Deleting a FileCloud User](#)
- [Resetting a User Password](#)
- [Manage A User's Policies](#)
- [Manage a User's Profile Picture](#)
- [Change a User's Email Address](#)
- [Setting a User Account to Expire](#)
- [Send Email from User Details](#)

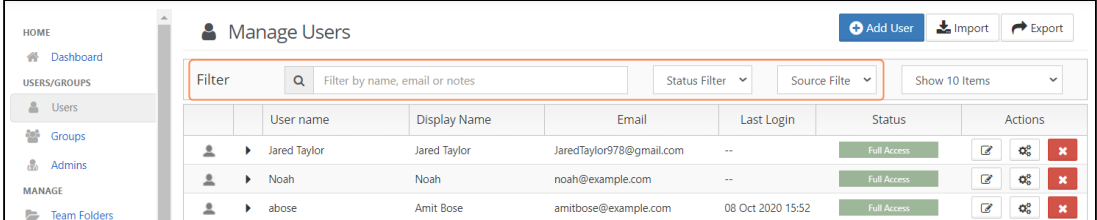
To add FileCloud users, see [Create FileCloud Users](#).













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.



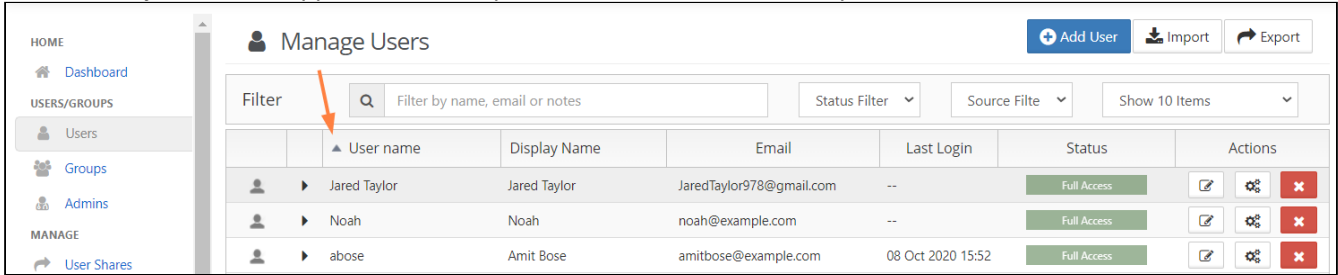
	User name	Display Name	Email	Last Login	Status	Actions
	Jared Taylor	Jared Taylor	JaredTaylor978@gmail.com	--	Full Access	  
	Noah	Noah	noah@example.com	--	Full Access	  
	abose	Amit Bose	amitbose@example.com	08 Oct 2020 15:52	Full Access	  

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.

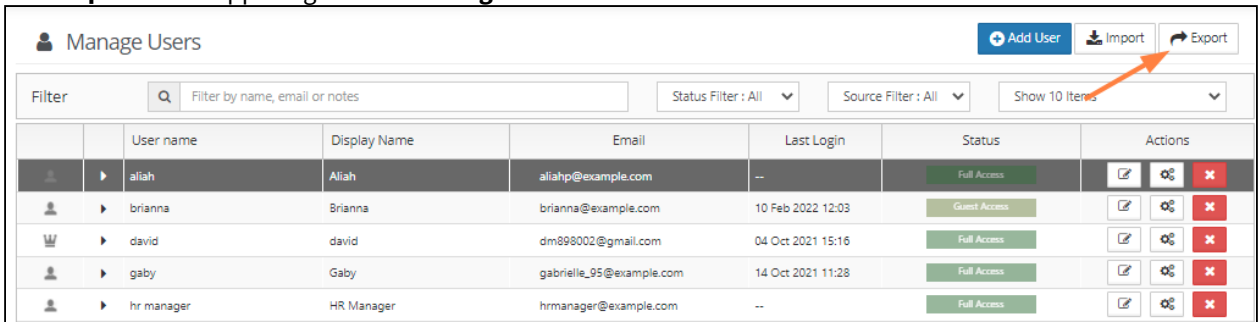
Notice that by default, all upper-case letters precede lower-case letters in alphabetical order.



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	gabriele_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 screenshot shows the 'Manage Users' interface. On the left is a navigation sidebar with sections: HOME (Dashboard), USERS/GROUPS (Users, Groups, Admins), and MANAGE (Team Folders, Network Folders, User Shares, Folder Permissions). The main area has a title 'Manage Users' and buttons for '+ Add User', 'Import', and 'Export'. Below is a filter bar with a search box containing 'gmail.com', 'Status Filter', 'Source Filter', and 'Show 10 Items'. A table lists three users:

	User name	Display Name	Email	Last Login	Status	Actions
👑 ▶	david	david	david@gmail.com	28 Apr 2021 08:20	Full Access	📄 ⚙️ ✖️
👤 ▶	jaredtaylor978	Jared	jaredtaylor978@gmail.com	--	Full Access	📄 ⚙️ ✖️
👑 ▶	jessicam	Jessica	jessicam@gmail.com	16 Jun 2021 13:51	Full Access	📄 ⚙️ ✖️

An orange arrow points to the edit icon (📄) in the Actions column for the user 'jessicam', with the text 'Click to view and edit user details.'

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.

The 'User Details' window for user 'jessicam' displays the following information:

Name	jessicam	Total Quota	2 GB
Email	[Redacted]	Used Quota	576.7 MB
Last Login	02 Aug 2022 08:01	Available Quota	1.4 GB
TOS Date	02 Aug 2022 09:01	Used Storage	576.7 MB
Group	Manage		More ▾

Manage Files Manage Policy Manage Shares Mobile Devices Reset Password Send Email Manage Notifications Manage Backups Delete Account

Profile Image

Update Remove

Access Level: Full


Authentication: Default

Save Close

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** ().

Manage Files Manage Policy Manage Shares Mobile Devices Reset Password Send Email Manage Notifications Manage Backups Delete Account

Options	Description	For more information
Manage Files	<p>Manage the files that are stored on your FileCloud Server site.</p> <p>This allows you to protect and maintain your system in the following ways:</p> <ul style="list-style-type: none"> • 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	<p>Manage clients connecting to your FileCloud instance.</p> <p>This feature is called Remote Client Management (RCM) or Data Leak Prevention Control (DLPC)</p>	Managing Client Devices
Reset Password	<p>Reset the password for user accounts with Authentication Type set to Default.</p> <p>For user accounts with an Authentication Type set to AD or LDAP, the password management must be done in AD or LDAP admin portal.</p>	Reset a User Password


Options	Description	For more information
Send Email	<p>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.</p> <p>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.</p> <p>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.</p>	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.	
Delete Account	Delete this user account from the command line or the admin portal.	Deleting a FileCloud User

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** ().


The screenshot displays a user profile configuration window. At the top, there is a 'Profile Image' section containing a silhouette icon and two buttons: 'Update' (with a camera icon) and 'Remove' (with a trash icon). Below this are three form fields: 'Access Level' is a dropdown menu currently showing 'Full'; 'Authentication' is a dropdown menu currently showing 'Default'; and 'Email' is a text input field containing 'amitbose@example.com'. At the bottom right of the window are two buttons: a blue 'Save' button and a white 'Close' button.

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
<p>Profile Image</p>	<p>You can choose a new picture or remove the current one.</p> <ul style="list-style-type: none"> • 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	<p>This is the access level set for this user. The possible values are:</p> <ul style="list-style-type: none"> • Full Access • Guest Access • External Access • Enabled • Disabled <p>Only accounts with enabled status can login into their account irrespective of their access level.</p> <p>Disabled accounts do not count towards the License Limit.</p> <p>For more information:</p> <p> User Access Levels</p>
Authentication	<p>This is the type of authentication used to verify the user's account.</p> <p>The possible values are:</p> <p>Default</p> <p>External (AD/LDAP)</p> <p>For more information:</p> <p> Authentication</p>
Total Quota (GB)	<p>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.</p>
Email	<p>Field to set the email ID for the user account. This value has to be unique for the FileCloud installation.</p>
Secondary Email	<p>Additional email account.</p>
Display Name	<p>Field to set an user readable name that will be used in various places such as email notifications etc.</p>
Account Expires On	<p>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</p>


Editable Property	Description
Password Expires On	<p>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.</p> <p>NOTE: An automatic email notification is sent to the user 7 days and 1 day before the actual password expiry date.</p>
Email Verified	<p>Indicates if the entered email has been verified. If email is not verified, then account cannot be logged in until the verification is completed.</p>
Disable Sync (Automatic Sync of My Files and Network Folders)	<p>Allow or disable Automatic sync of "My Files" location and Network Folders Location</p>
Disable Sync (Offline Network Share Sync)	<p>Allow or disable offline access of network folders in FileCloud Sync</p>
Backup Path	<p>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</p>
Change Password on Login	<p>This feature forces the user to change the login password on first login. When enabled user will be forced to change the password on login in user portal.</p> 
Creation Source	<p>Where user was created. Options are:</p> <ul style="list-style-type: none"> • Default (Admin user interface or import) • SSO (During SSO signin)

Editable Property	Description
Phone Number (added in FileCloud 20.1)	The user's phone number.
Notes	This field 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 *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.

→ [Managing Groups](#)

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


Readonly 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).

Readonly Property	Description
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)
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

 The ability to disable user account during import if the account is also disabled in Active Directory is available in FileCloud Server version 19.1 and later.

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**.


The screenshot shows the 'User Details' interface for a user named 'aliah'. The user's email is 'aliahp@example.com', last login was on 02 Dec 2022 at 08:50, and the TOS date is 16 Sep 2022 at 09:53. The user's total quota is 2 GB, with 251 KB used and 2 GB available. The user's storage usage is 251 KB. The interface includes a navigation bar with options like 'Manage Files', 'Manage Policy', 'Manage Shares', 'Mobile Devices', 'Reset Password', 'Send Email', 'Manage Notifications', 'Manage Backups', and 'Delete Account'. Below the navigation bar is a 'Profile Image' section with 'Update' and 'Remove' buttons. The 'Access Level' dropdown menu is open, showing options: Full, Disabled (selected), Guest, Full, and External. The 'Authentication' section is also visible. At the bottom right, there are 'Save' and 'Close' buttons.

5. Click **Save**.

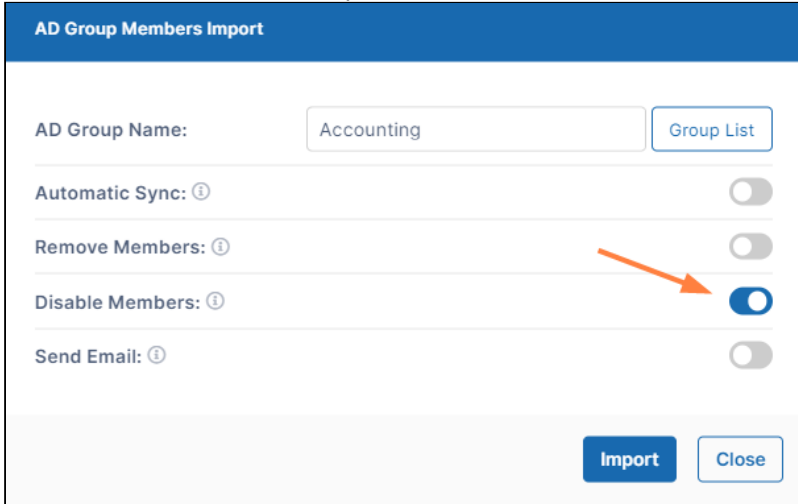
Import Disabled Users from Active Directory as Disabled

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 the navigation panel, click **Groups**.
3. Select the **group** that you want to add users to, and then click the Edit Group () 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

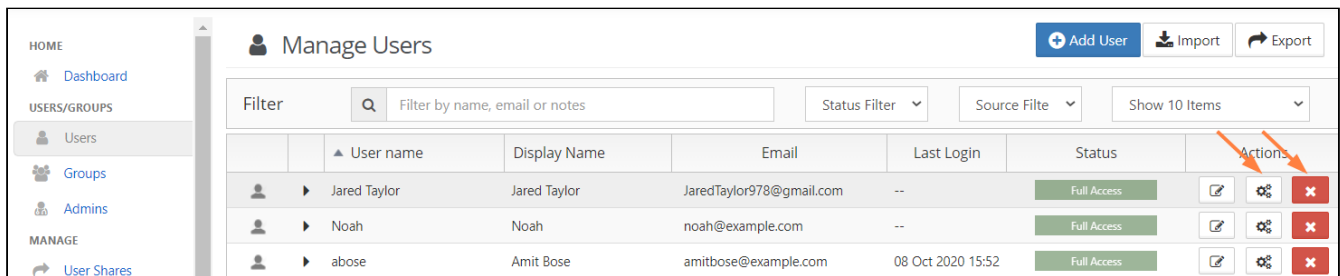
[Delete the account](#)










Deleting a FileCloud User From Admin Portal

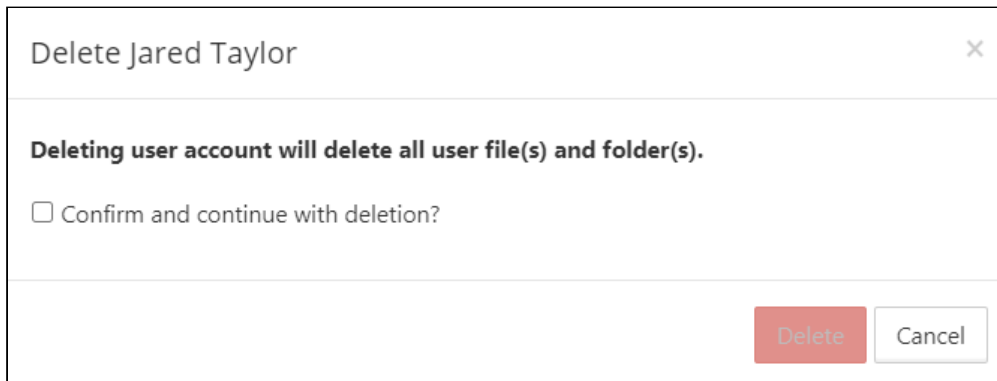
To delete a user:

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 ().



	User name	Display Name	Email	Last Login	Status	Actions
	Jared Taylor	Jared Taylor	JaredTaylor978@gmail.com	--	Full Access	  
	Noah	Noah	noah@example.com	--	Full Access	  
	abose	Amit Bose	amitbose@example.com	08 Oct 2020 15:52	Full Access	  



Delete Jared Taylor ✕

Deleting user account will delete all user file(s) and folder(s).

Confirm and continue with deletion?

Delete Cancel

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.


User Details ✕


Name	david	Total Quota	2 GB
Email	dm898002@gmail.com	Used Quota	0 B
Last Login	28 Apr 2021 08:20	Available Quota	2 GB
TOS Date	Not Accepted	Used Storage	0 B
Group	Manage		More ▾



Manage Files



Manage Policy



Manage Shares



Mobile Devices


Reset Password



Send Email




Manage Notifications


Manage Backups


Delete Account

Profile Image



 Update
  Remove

Access Level

Full
▾

Authentication

Default
▾

Email

dm898002@gmail.com

[Save](#)
[Close](#)

- Click **Reset Password**.

The screenshot shows a dialog box titled "Set New Password". It contains two text input fields: "Password" and "Confirm Password". The "Password" field has a vertical line indicating the cursor. At the bottom right of the dialog, there are two buttons: "Save" (highlighted in blue) and "CANCEL".

- Enter the new password in **Password** and **Confirm Password**.
 - 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

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

The screenshot shows a dialog box titled "Confirm". It contains two radio button options: "Send 'forgot password' reset message" (which is selected) and "Send 'account welcome' message (This will reset the password)". At the bottom right of the dialog, there are two buttons: "OK" (highlighted in blue) and "CANCEL".


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

Manage A User's Policies

 Policies are available in FileCloud 17.3 and later.

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 Devices
- 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.

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.

	▶ david	david	dm898002@gmail.com	28 Apr 2021 08:20	Full Access			
	▶ jaredtaylor978	Jared	jaredtaylor978@gmail.com	--	Full Access			

The **Policy Settings** dialog box opens.

3. Change the settings on any of the tabs.

Policy Settings - Global Default Policy - diaz

Note: Applied from Default

[General](#)
[2FA](#)
[User Policy](#)
[Client Application Policy](#)
[Device Configuration](#)
[Notifications](#)

Default Web UI Version to show:
Select the default UI Version to show on the web browser.

Allow User to Change Web UI Version:
Allow Users to change web UI version selected above.

Share mode:
Set Share Mode

4. **Click Save.**

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

Save Policy Changes

Policy changes will be enforced for all users with this effective policy. Do you want to continue?

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


 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 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:


User Details
✕


Name	me	Total Quota	1 GB
Email	me@codelathe.com	Used Quota	198.5 MB
Last Login	06 Nov 2018 09:10	Available Quota	825.5 MB
Group	Manage	Used Storage	198.5 M More ▾



Mobile Devices



Manage Files



Manage Shares


Reset Password



Email Password




Delete Account


Manage Policy


Manage Backups

Profile Image



 Update
 Remove


Access Level

Authentication

Email

[Save](#)
[Close](#)

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 you want whose details you want to view.
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.

User Details ✕

Name	jessica	Total Quota	24.5 GB
Email	[Redacted]	Used Quota	2.1 MB
Last Login	23 Aug 2022 14:16	Available Quota	24.5 GB
TOS Date	Not Accepted	Used Storage	2.1 MB
Group	Manage More ▾		

 Manage Files
 Manage Policy
 Manage Shares
 Mobile Devices
 Reset Password
 Send Email
 Manage Notifications
 Manage Backups
 Delete Account

Display Name

Account Expires On 

Password Expires On


Email Verified

Disable Sync


Backup Path

Save
Close

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** ().
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

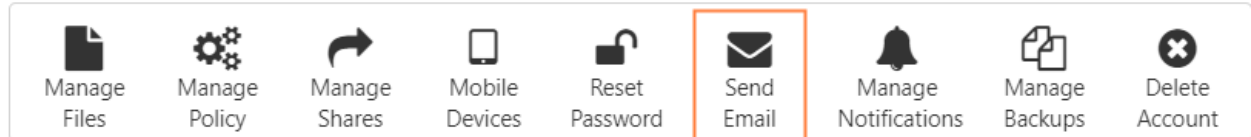
 This option is available beginning in FileCloud 20.1

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.

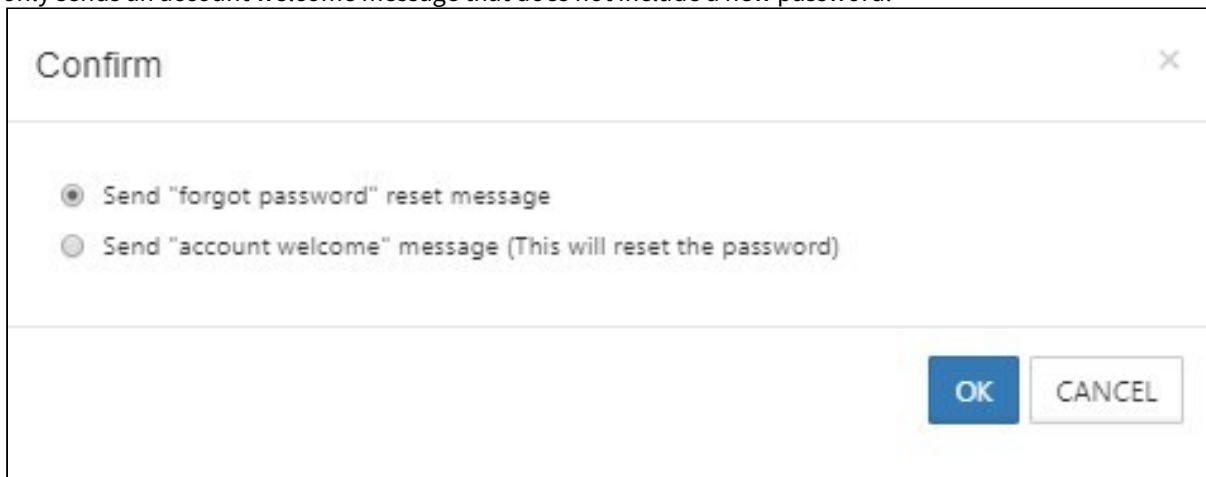
To send an email from User Details:

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 **Set "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** group.

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** group.

To change a group's members:

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

6. To remove a user, click **Remove** next to the user's name.

The screenshot shows the 'Manage Group' interface for the 'Approvers' group. At the top, there is a 'Group Name' field containing 'Approvers' and a 'Save' button. Below this are tabs for 'Members', 'Admins', and 'Policies', with 'Members' selected. The main section is titled 'Members Management' and includes an 'Add Users to Group' search bar (highlighted with an orange arrow) and an 'Import Users from AD Group' link. Below the search bar, it shows 'Users in Group (3 members in this group)' and an 'Export' button. A 'Filter users' input field is present. The user list table contains three entries:

Users	
david dm898002@gmail.com	Remove
Jared jaredtaylor978@gmail.com	Remove
Jessica jm2344311@gmail.com	Remove

At the bottom, there is a pagination control showing '< Page 1 of 1 >' and a 'Close' button.

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.

- In the **Members** tab of the **Manage Group** dialog box, click **Export**.

The screenshot shows the 'Manage Group' dialog box with the 'Members' tab active. The group name is 'Approvers'. Below the group name are tabs for 'Members', 'Admins', and 'Policies'. The 'Members Management' section includes a search bar and an 'Import Users from AD Group' link. The 'Users in Group' section shows two users: Jared and Jessica, each with a 'Remove' button. An orange arrow points to the 'Export' button in the top right corner of the 'Users in Group' section.

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			Jared	FULL		EVERYONE, Human Resources Group	YES	NO	10/18/2021 12:36	Default		Global Default Policy
jessicam			Jessica	FULL		EVERYONE, Internal, Human Resources	YES	NO	2/10/2022 14:08	Default		Global Default Policy

To import an AD group into a FileCloud group, see [Group Settings](#)

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.

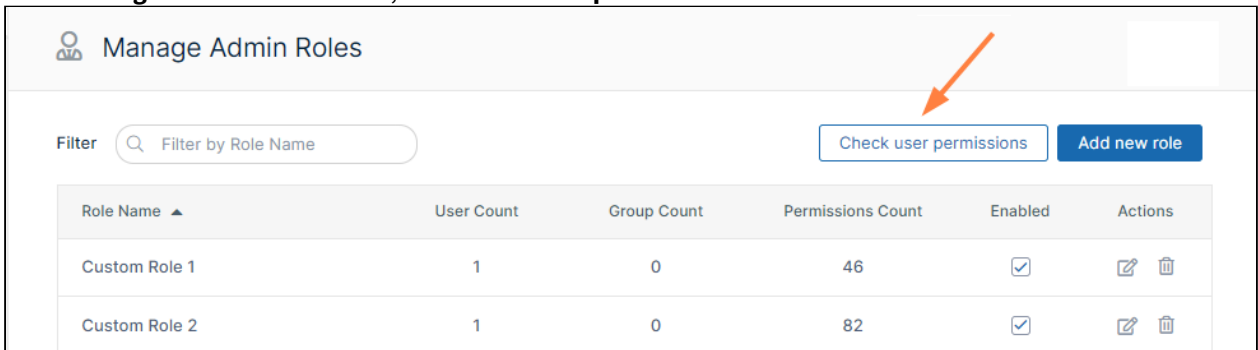
For information on about admin roles and admin users and instructions for setting them up, see [Admin User and Role Settings](#).

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:

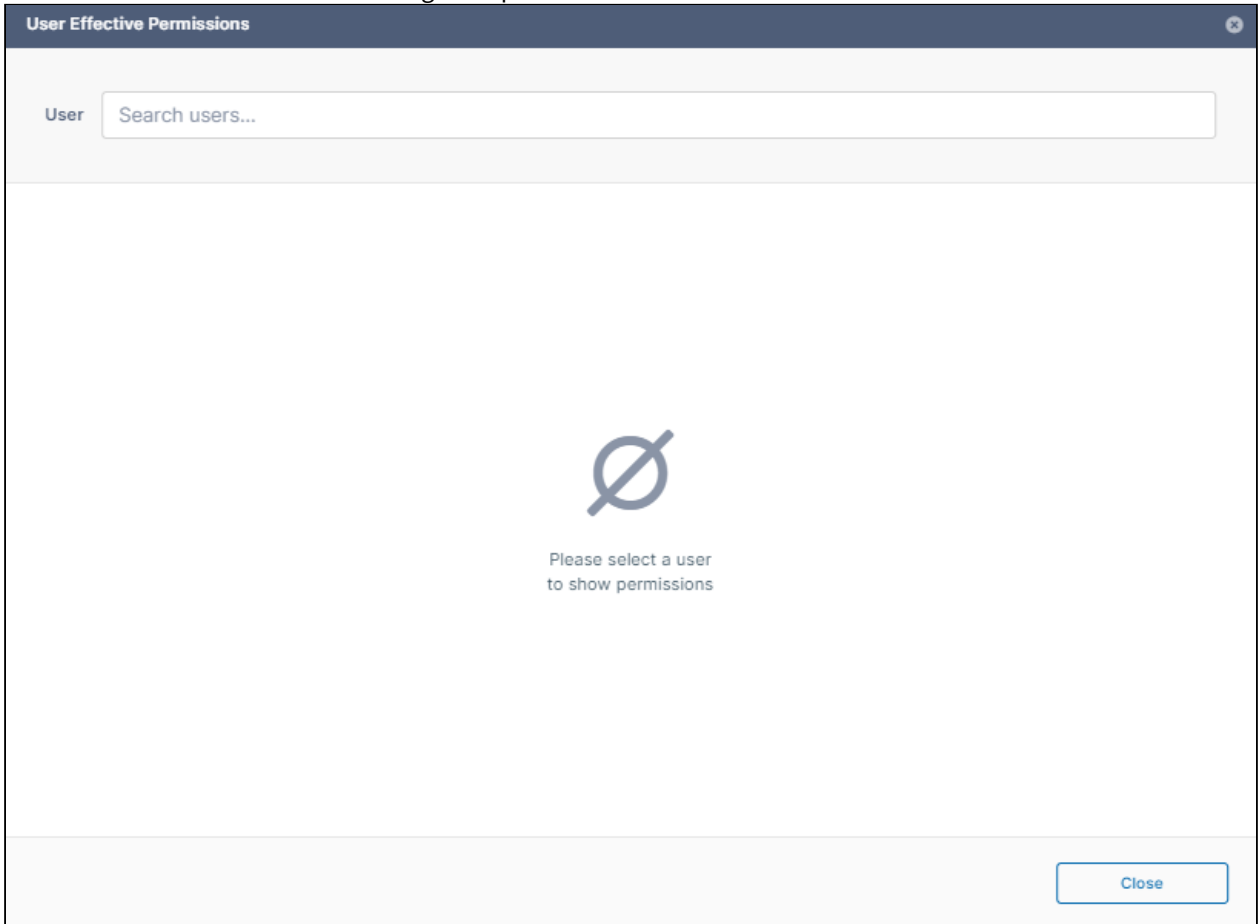
1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Check user permissions**.



The screenshot shows the 'Manage Admin Roles' interface. At the top, there is a search filter labeled 'Filter' with the text 'Filter by Role Name'. To the right of the filter are two buttons: 'Check user permissions' and 'Add new role'. Below the filter and buttons is a table with the following columns: Role Name, User Count, Group Count, Permissions Count, Enabled, and Actions. The table contains two rows of data:

Role Name ▲	User Count	Group Count	Permissions Count	Enabled	Actions
Custom Role 1	1	0	46	<input checked="" type="checkbox"/>	 
Custom Role 2	1	0	82	<input checked="" type="checkbox"/>	 

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.

User Effective Permissions

User

Permissions

Operation	Read	Create	Update	Delete
Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Federated Search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

< Page 1 of 4 >

> Definitions of Permissions

The following permissions represent functions that admin users may be permitted to perform.

Operation	Description
Alert	Alert item on the admin interface is visible. Authorization to view and clear alerts in admin interface.
Audit	Audit item on the admin interface is visible. Authorization to view, delete and export Audit Records.
Compliance	Compliance Dashboard on the admin interface is visible. Authorization to view and update compliance settings.

Operation	Description
Customization	Customization item on the admin interface is visible. Authorization to customize the FileCloud interface. Note: Admin users must have Customization > Update enabled to be able to change the user login background .
Device Management	Devices item on the admin interface is visible. Authorization to view, create, delete and update Devices.
Encryption	Authorization to manage all Encryption at Rest settings.
Federated Search	Support to perform federated search through the admin interface.
Files	Manage Files. Authorization to view, create, modify, download, and delete user files.
Folder Permissions	Manage Folder Level Permissions. Authorization to view and manage Folder Permissions.
Groups	Groups menu item on the admin interface is visible. Authorization to view, create, modify and delete Groups. Manage group members. Import group members from Active Directory.
Locks	View , create, and delete Locks on Files and Folders in FileCloud.
Manage Administrators	Allows promoted admin users to manage the permissions of other promoted admin users.
Metadata	View, create, update and delete metadata set definitions, attributes and permissions.
Mini Admin	View allows promoted users to open mini admin and perform all permitted actions except adding users. Create allows promoted users to open mini admin and perform all permitted actions including adding users.
Network Share	Network Folders item on the admin interface is visible. Authorization to view, create, modify and delete Network Folders. Manage User and Group Access to Network Folders.
Notifications	Notifications menu item on the admin interface is available. Add, edit, update, and delete notification rules.

Operation	Description
Reports	Reports menu item on the admin interface is available. Add, execute, edit and delete reports.
Retention	Retention menu item on the admin interface is available. Add, edit, and delete retention policies.
Rich Dashboard	View rich dashboard view including tables and graphs on the admin UI dashboard.
Settings	Settings item on the admin interface is visible. Authorization to view and modify FileCloud Settings.
Smart Classification	Smart Classification menu item on the admin interface is available. Add, update, run, and delete content classification rules.
Smart DLP	Smart DLP menu item on the admin interface is available. Add, edit, and delete DLP rules.
System	System item on the admin interface is visible. Authorization to run system checks, install check, generate logs and UPGRADE FileCloud to new version.
Team Folders	Set up Team Folders, add, edit, delete and manage team folder and corresponding permissions. <i>Note: The corresponding Folder Permission must be enabled to be able to perform a Team Folder operation.</i>
User Share	User Shares item on the admin interface is visible. Authorization to view, create, modify and delete User Shares.
Users	Users menu item on the admin interface is visible. Authorization to view, create, modify and delete Users. Import New Users. Reset Password for Users.
Workflow	Workflow menu item on the admin interface is visible. Add, edit and delete workflows on FileCloud.

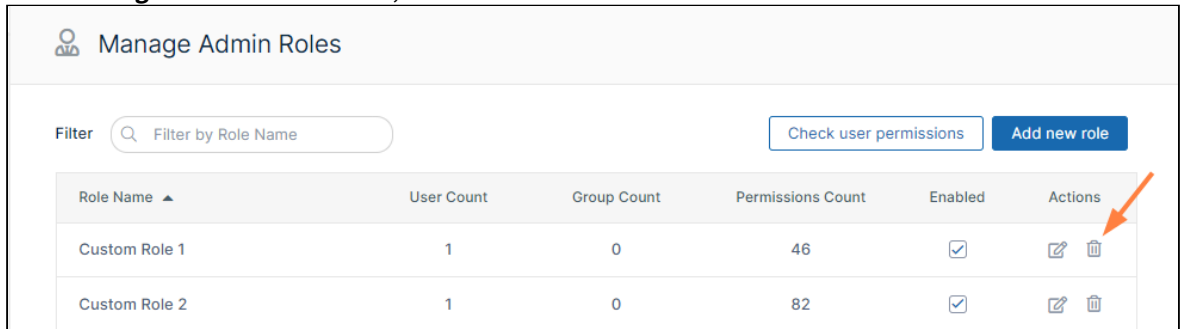
Admin users can log in to the admin portal using either their username or email id.

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:

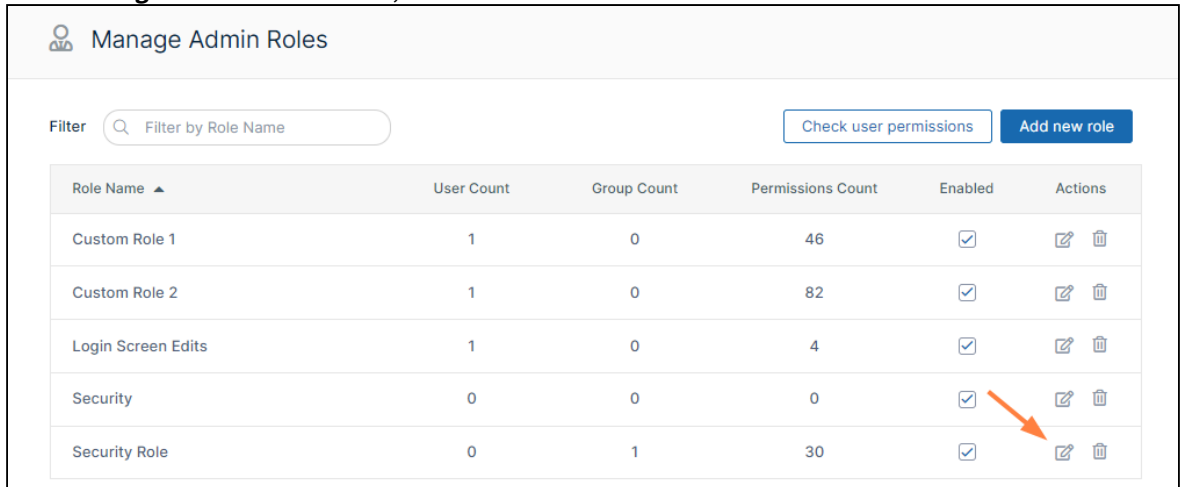
1. Click **Admins** in the navigation panel.
2. Either
 - In the **Manage Admin Roles** screen, click the **Delete** button for the role.



- Click **Remove** when you are prompted to confirm removal.

Or:

- In the **Manage Admin Roles** screen, click the **Edit** button for the role.



The **Manage Admin Role** dialog box opens.

- Click **Remove Role** at the bottom of the dialog box.

The screenshot shows the 'Manage Admin Role' dialog box. At the top, the role name is 'Security Role' and the 'Enable' toggle is turned on. Below this are three tabs: 'Permissions', 'Users', and 'Groups'. The 'Permissions' tab is selected, displaying a table of operations with checkboxes for Read, Create, Update, and Delete. An orange arrow points to the 'Remove Role' button at the bottom left of the dialog box.

Operation	Read	Create	Update	Delete
Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Federated Search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Click **Remove** when you are prompted to confirm removal.

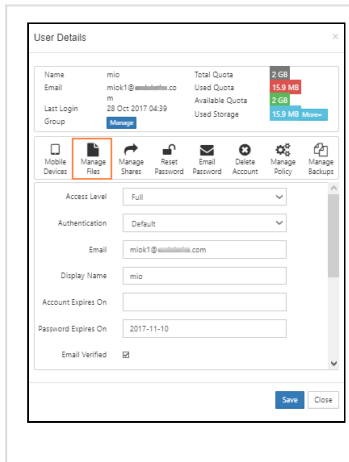
Managing User Folders and Files

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

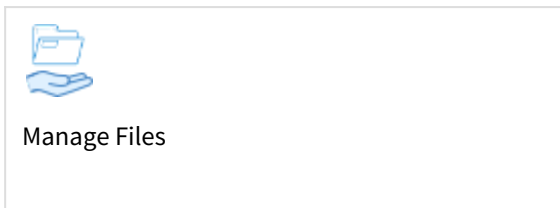
How do I access user storage management settings?



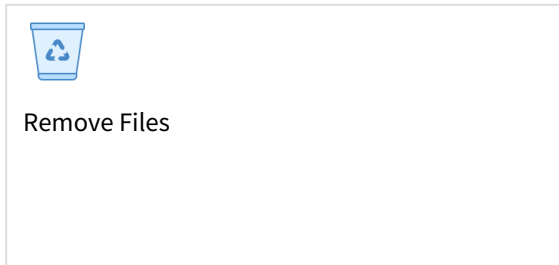
To access user folder and files settings:

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.

What do you want to do?



- ➔ Download User Files and Folders
- ➔ Restore a Previous File Version
- ➔ Copy and Move User Files



- ➔ Delete User Files and Folders
- ➔ Clear a Recycle Bin
- ➔ Remove a User's Incomplete Uploads
- ➔ Remove Old File Versions

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.

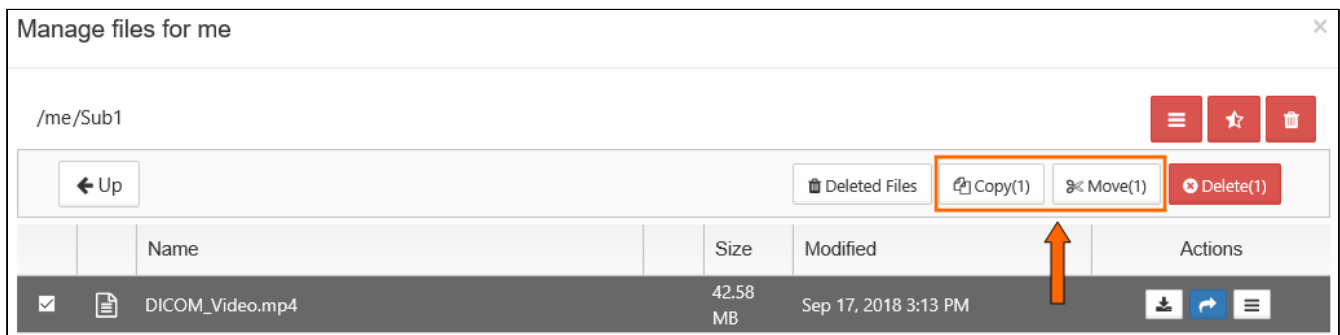
This allows you to protect and maintain your system in the following ways:

- 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 two different user accounts
- 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 folder locations for the same user account:


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.
6. Navigate to the folder or file you want to copy.
7. To select the file or folder, click the checkbox next to the name.
8. To copy the file or folder, click the Copy button.

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



To copy and paste files and folders between folder locations for two different user accounts:

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.
6. Navigate to the folder or file you want to copy.
7. To select the file or folder, click the checkbox next to the name.
8. To copy the file or folder, click the Copy button.
9. To close the window, in the top right corner, click the x button.
10. On the Manage Users page, select the user who wants a copy of the file or folder, and then click the Edit icon .
11. On the User Detail dialog box, click **Manage Files**.
12. The Manage Files for <User> window opens.
13. Navigate to the folder or file where you want to paste the copy.
14. Click Paste.


To move and paste files and folders between folder locations for the same user account:

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.
6. Navigate to the folder or file you want to move.
7. To select the file or folder, click the checkbox next to the name.
8. To move the file or folder, click the Move button.
9. Navigate to the folder where you want to paste the original file or folder.
10. Click Paste.

To move and paste files and folders between folder locations for two different user accounts:

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.
6. Navigate to the folder or file you want to move.
7. To select the file or folder, click the checkbox next to the name.
8. To copy the file or folder, click the Move button.
9. To close the window, in the top right corner, click the x button.
10. On the Manage Users page, select the user who wants the file or folder, and then click the Edit icon .
11. On the User Detail dialog box, click **Manage Files**.
12. The Manage Files for <User> window opens.
13. Navigate to the folder or file where you want to paste the original.
14. 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 will be zipped first 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



Look for the Versions button icon



Previous Versions						
Current Version	17.44 MB	Oct 15, 2018 11:56 AM	Created by me			
Version 3	9.43 MB	Oct 11, 2018 10:24 AM	Created by me	Oct 11, 2018 11:25 AM		
Version 2	9.2 MB	Oct 11, 2018 10:18 AM	Created by me	Oct 11, 2018 10:24 AM		
Version 1	8.36 MB	Oct 11, 2018 10:15 AM	Created by me	Oct 11, 2018 10:18 AM		

[Close](#)


Having older versions on the site also allows you to:
 Restore the previous version of a file and make it live
 Remove previous versions to save space

Manage files for me						
/me 						
← Up Deleted Files Copy Move Delete						
	Name	Size	Modified	Actions		
<input type="checkbox"/>	Sub1		Sep 18, 2018 10:13 AM			
<input type="checkbox"/>	backups		Oct 26, 2018 11:13 AM			
<input type="checkbox"/>	059c1770e5e39c50d5efa5ced3b913d2--writing-process-writing-tips.jpg	107 KB	Jul 25, 2018 2:39 PM			

To download user folder and files:

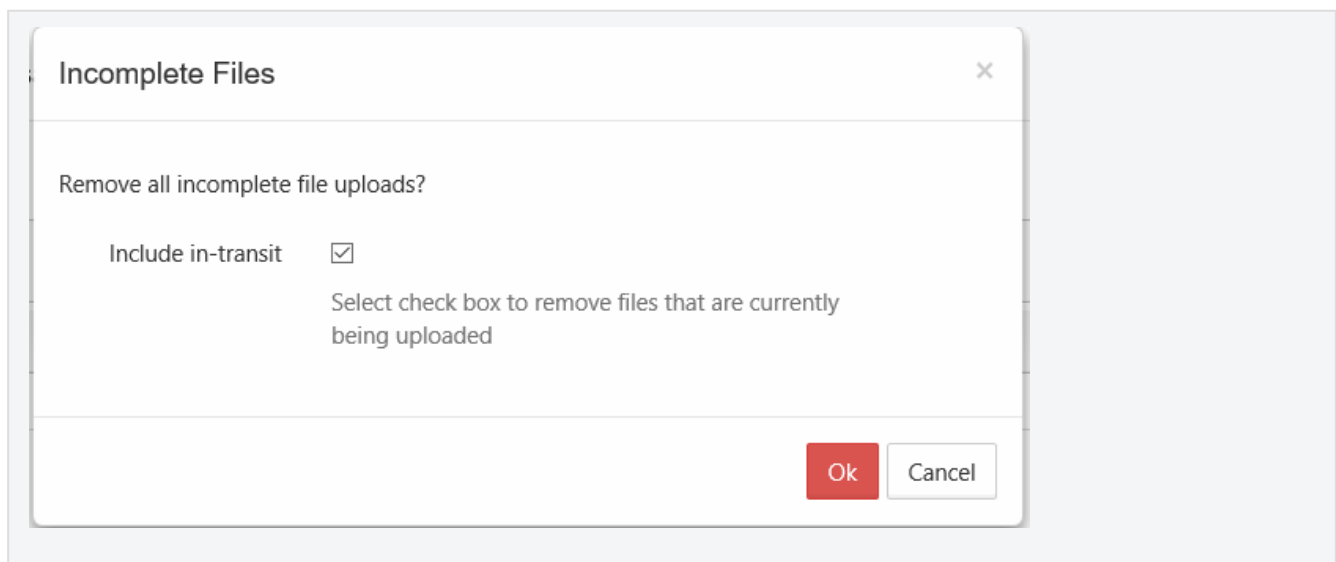
1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon
4. On the User Detail dialog box, click **Manage Files**.
5. The Manage Files for <User> window opens.
6. Navigate to the folder or file you want to download.
7. Select the file or folder.
8. To download the latest version of a file, click the Download icon .
9. To download an earlier version, click the Version icon .
10. 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**.
5. The Manage Files for <User> window opens.
6. Click the Remove all incomplete uploads icon .
7. On the Incomplete Files dialog box, select the Include in-transit checkbox.
8. Click OK.


Delete User Folders and Files

-  This action will be 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 it 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**.
5. The Manage Files for <User> window opens.
6. Navigate to the folder or file you want to delete.
7. To select the file or folder, click the checkbox next to the name.
8. Click the Delete button.
9. On the Confirm dialog box, click Yes.

Clear a Recycle Bin

 The ability to have FileCloud place files deleted on S3 Storage into a recycle bin and use the recycle bin functionality is available on FileCloud Server version 18.2 and later.

 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.

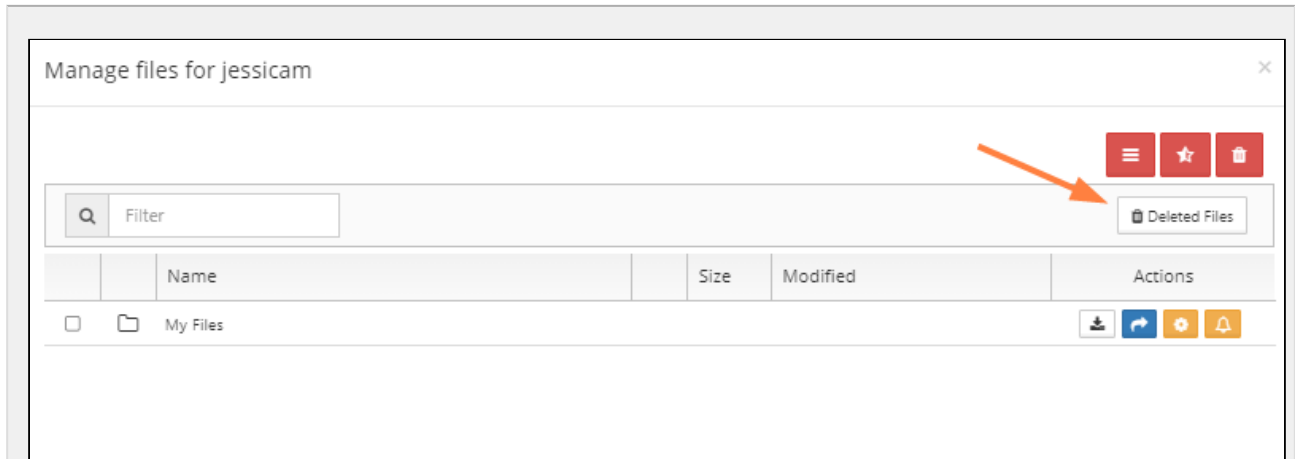
- If you have a policy that stores deleted files, they are saved in the Recycle Bin
- This means that they can be recovered if deleted by mistake or are needed again at a later time
- You can also set the Recycle Bin to automatically delete through a policy

 [Manage the Recycle Bin Using a Policy](#)

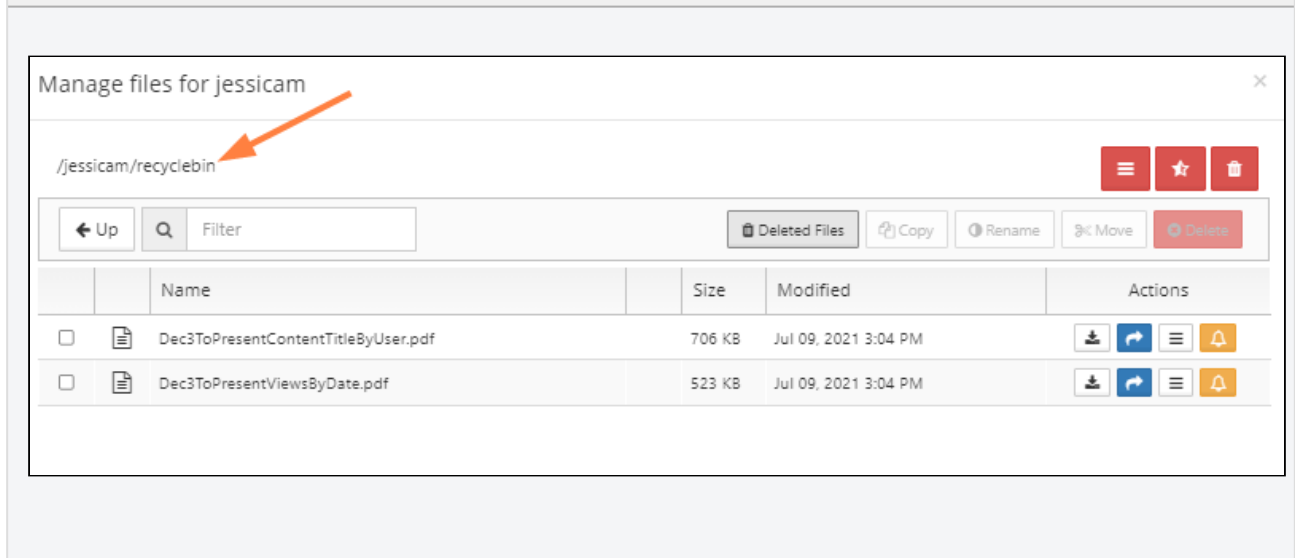
Go to the recycle bin

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**.

Click **Deleted Files** to view the contents of the recycle bin:

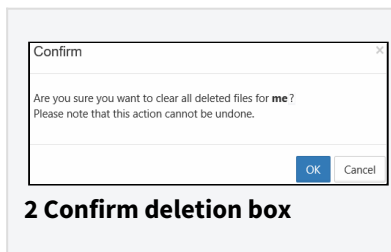


1 Manage Files dialog box, Deleted Files button




Clear a recycle bin smaller than 16 MB


If you are sure the user no longer needs the files in the recycle bin, they can be cleared.



2 Confirm deletion box

To clear a user's recycle bin:


1. Follow the steps above in **Go to the recycle bin** to open the recycle bin.
2. Click the Clear all Deleted Files icon .
3. On the Confirm dialog box, click **OK**.

 If you have a folder with a large number of files, more than 16 MB, and you delete this folder, it is moved to recycle bin.

- When you try to delete the folder or empty recycle bin, the request will fail

- A new utility has been added to help an administrator empty the recycle bin when it contains a large folder that won't delete
- See the next topic, Run a tool to clear a recycle bin larger than 16 MB for more information

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?

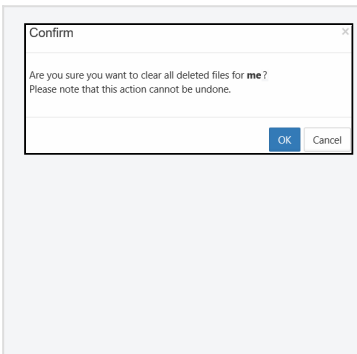
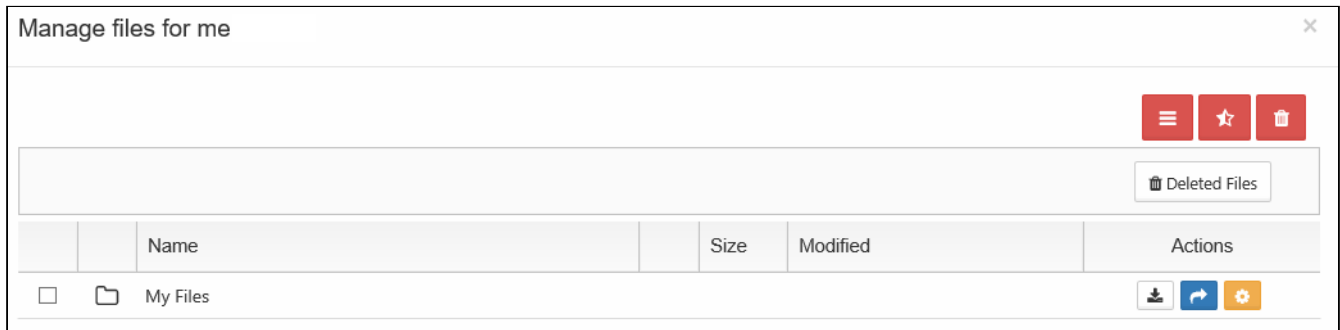
 Look for the Versions icon 

Manage files for me ✕



/me   

← Up    


	Name	Size	Modified	Actions
<input type="checkbox"/>	 Sub1 		Sep 18, 2018 10:13 AM	  
<input type="checkbox"/>	 backups		Oct 26, 2018 11:13 AM	  
<input type="checkbox"/>	 059c1770e5e39c50d5efa5ced3b913d2--writing-process-writing-tips.jpg	107 KB	Jul 25, 2018 2:39 PM	  



To remove a user's old 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**.
5. The Manage Files for <User> window opens.
6. Click the Remove all Old Versions icon .
7. On the Confirm dialog box, click OK.

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.

Manage files for jenniferp

Filter Deleted Files

Name	Size	Modified	Actions
My Files			   



Page 1 of 1
1 row

 If a file upload is in progress:

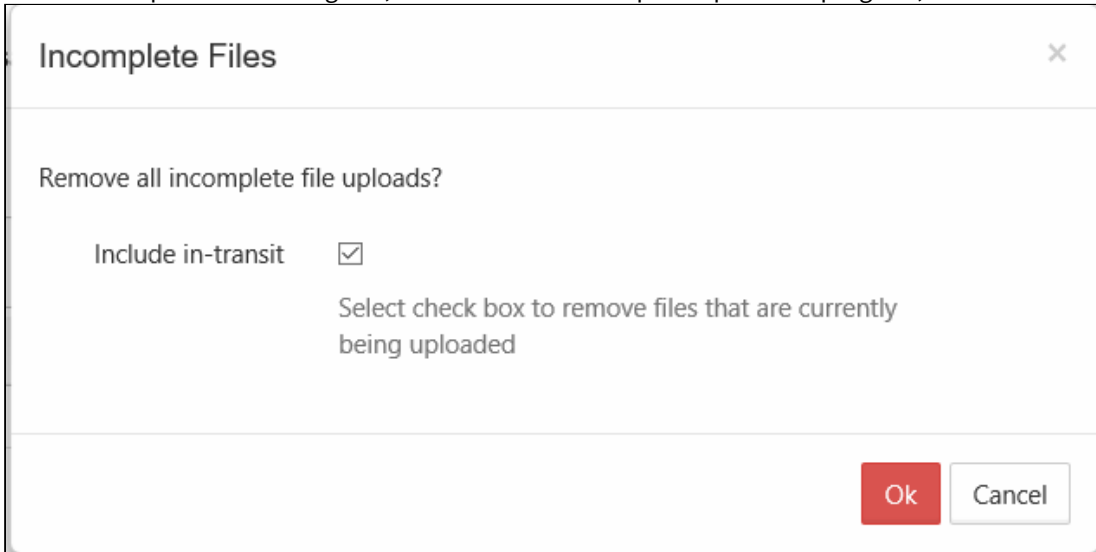
- It will not be removed, even if it only partially uploads, unless you use the In-transit option when removing partial uploads
- You can use the In-transit option to cancel a partial upload in progress

 [Cancel a Partial Upload](#)

To remove all incomplete user uploads:

1. Open a browser and log 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.
6. Click the Remove all incomplete uploads icon .

7. On the Incomplete Files dialog box, to also remove incomplete uploads in progress, select Include in-transit.




8. Click OK.

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**.
5. The **Manage Files for <User>** window opens.
6. Navigate to the file.

7. To see a list of earlier versions, click the Version icon  .


Manage files for jenniferp

/jenniferp/CustomerAccounts

← Up Deleted Files Copy Rename Move Delete

	Name	Size	Modified	Actions
<input type="checkbox"/>	Account Names Folder		May 14, 2021 9:47 AM	
<input type="checkbox"/>	FCInactiveUsers.png	74 KB	Jun 09, 2021 10:45 AM	
<input type="checkbox"/>	FCShareExpiry.png	68 KB	Nov 06, 2020 8:55 AM	
<input type="checkbox"/>	MenuOutline.docx	210 KB	Jul 31, 2020 10:29 AM	
<input type="checkbox"/>	Registration Form.docx	12 KB	Mar 10, 2021 11:16 AM	
<input type="checkbox"/>	accountnames.txt	55 B	Jun 16, 2021 3:17 PM	
<input type="checkbox"/>	announcements.md	81 B	Oct 23, 2020 12:28 PM	
<input type="checkbox"/>	social sec #.pdf	347 KB	Nov 17, 2020 1:57 PM	

Page 1 of 1 8 rows

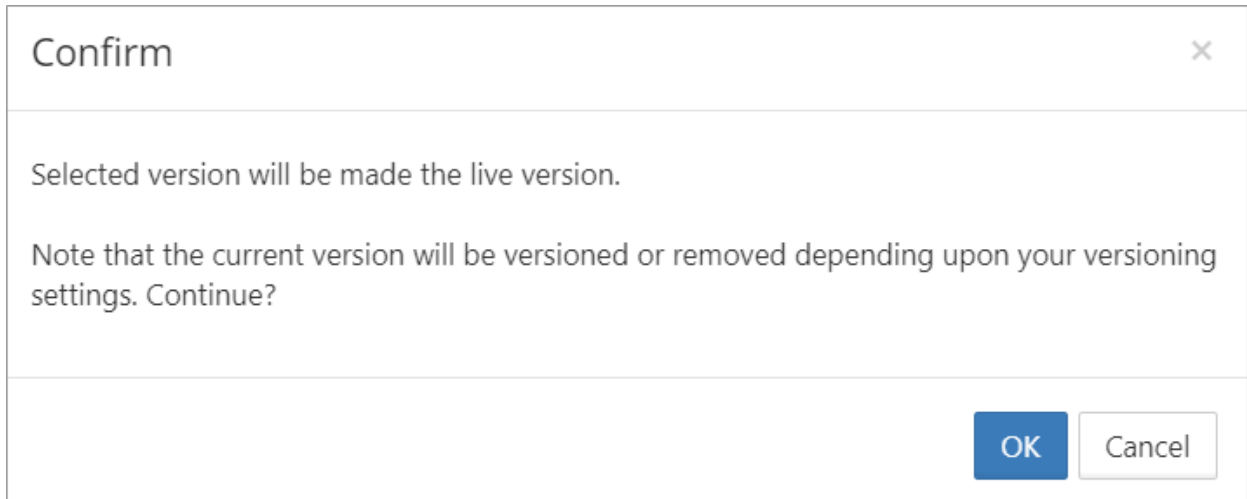
8. Select the version that you want to make live, and click the **Make it Live** icon  .

Previous Versions

Version	Size	Created	Created by	Modified	Actions
Current Version	55 B	Jun 16, 2021 03:17 PM	Created by jenniferp		
Version 3	28 B	Jun 16, 2021 01:01 PM	Created by jenniferp	Jun 16, 2021 03:17 PM	
Version 2	87 B	Jun 16, 2021 12:44 PM	Created by jenniferp	Jun 16, 2021 01:01 PM	
Version 1	40 B	May 28, 2021 01:01 PM	Created by jenniferp	Jun 16, 2021 12:44 PM	

3 Previous Versions dialog box, Make it Live icon

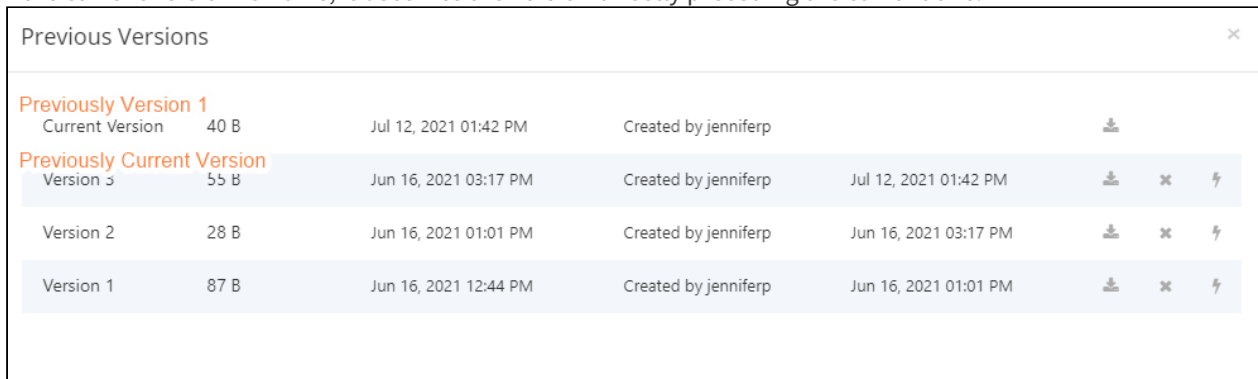
The following confirmation box appears.



4 Confirmation box for making the version live

i 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.

9. 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.



5 Previous Versions dialog box, showing new current version

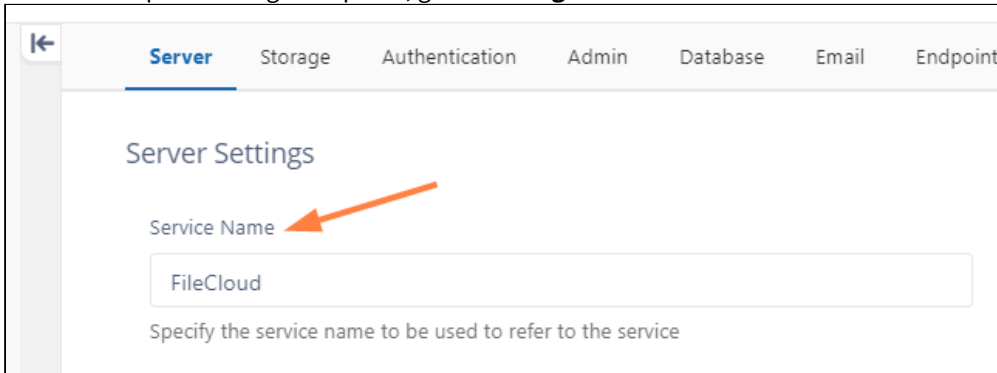
Change the Name of the Zip File for Multiple File Downloads

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:

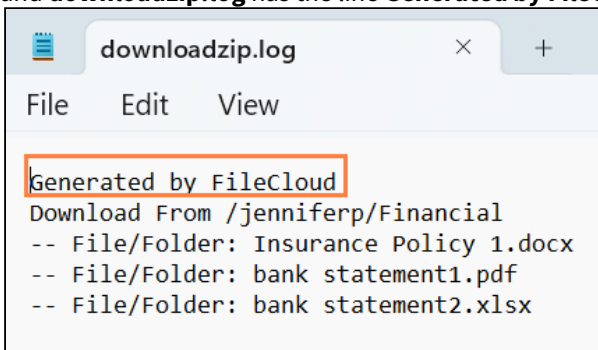
1. In the admin portal navigation panel, go to **Settings > Server**.



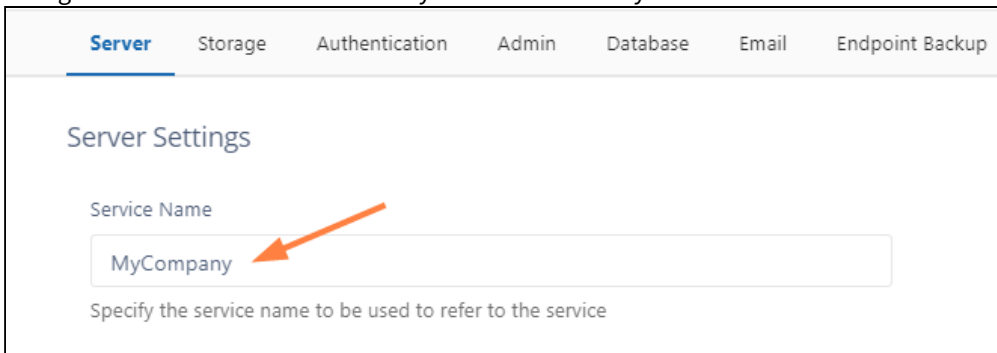
At this point, if a user downloads multiple files at the same time, the zip file has a name similar to:

 filecloud-20231101141022.zip


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



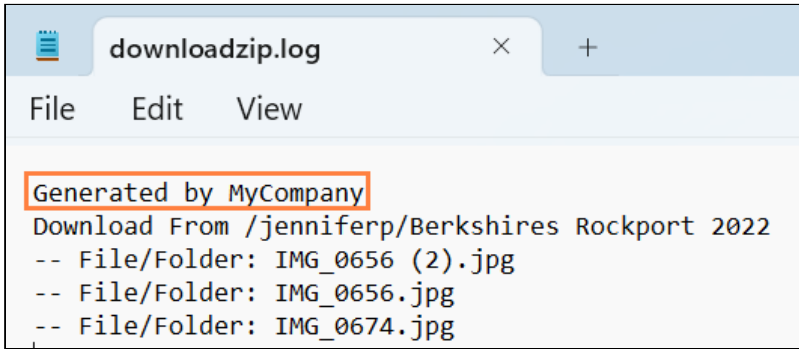
2. Change the value in **Service Name** to your own name for your server:



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

 mycompany-20231102103734.zip

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



```
downloadzip.log
File Edit View
Generated by MyCompany
Download From /jenniferp/Berkshires Rockport 2022
-- File/Folder: IMG_0656 (2).jpg
-- File/Folder: IMG_0656.jpg
-- File/Folder: IMG_0674.jpg
```

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.

The screenshot shows a 'User Details' dialog box with a blue header and a close button. The main content area is divided into several sections:

- User Information:** Name (jessica), Email (blurred), Last Login (16 Jun 2022 14:50), TOS Date (Not Accepted), and Group (Manage button).
- Quota and Storage:** Total Quota (Unlimited), Used Quota (59.2 MB), Available Quota (0 B), and Used Storage (59.2 MB).
- Management Options:** A horizontal bar with icons and labels for Manage Files, Manage Policy, Manage Shares (highlighted with an orange arrow), Mobile Devices, Reset Password, Send Email, Manage Notifications, Manage Backups, and Delete Account.
- Profile Image:** A placeholder image with 'Update' and 'Remove' buttons.
- Access Level:** A dropdown menu set to 'Full'.
- Authentication:** A dropdown menu set to 'Default'.
- Footer:** 'Save' and 'Close' buttons.

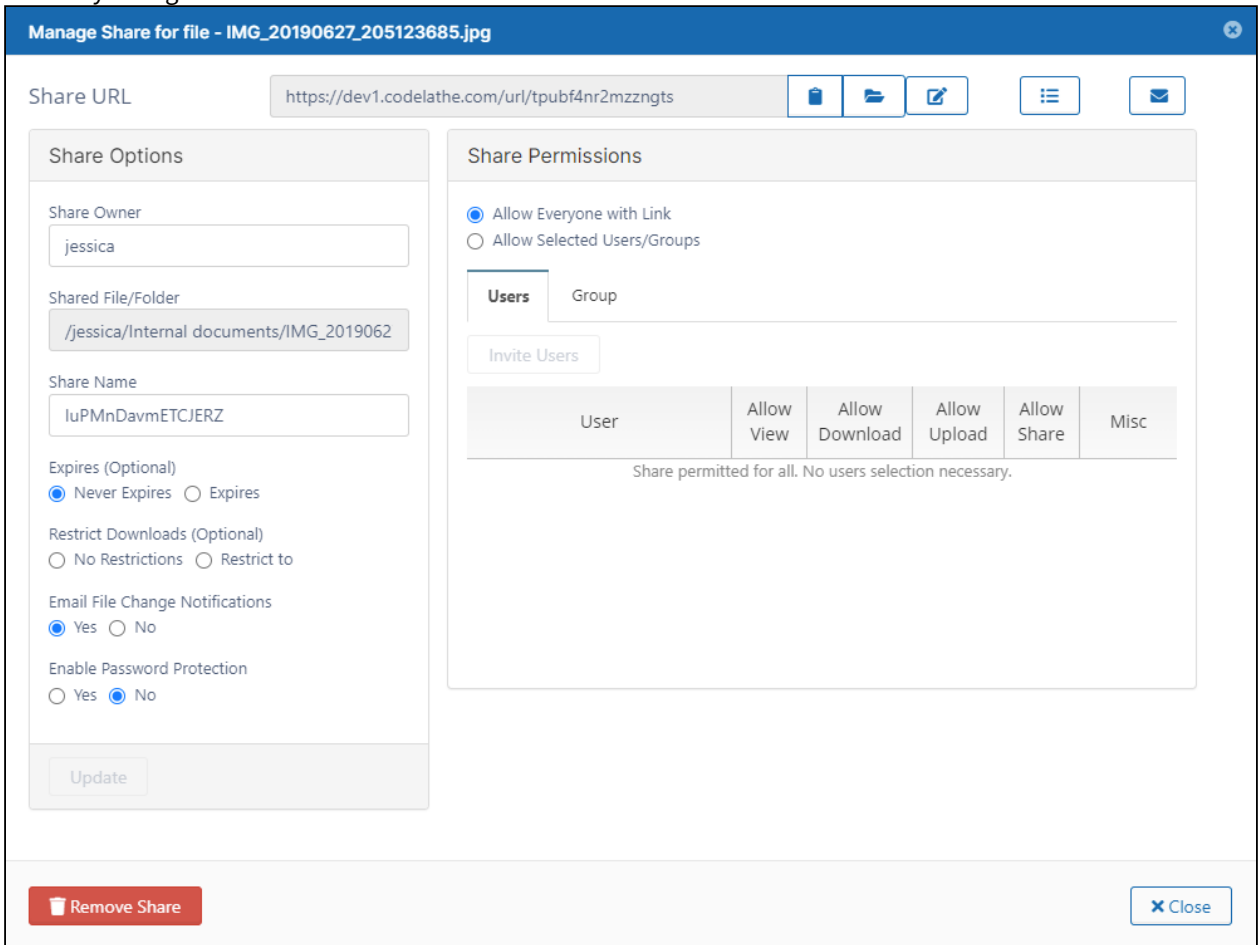
A **Manage shares for [user]** dialog box opens.

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.

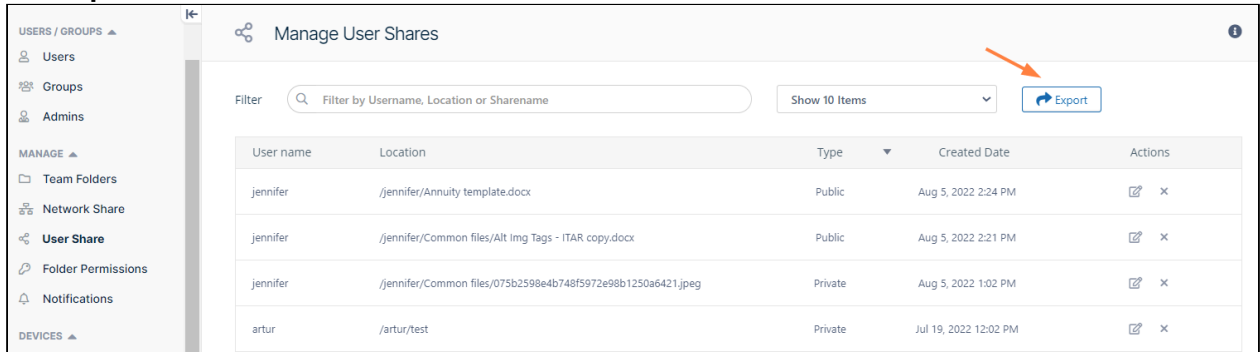
User name	Location	Type	Created Date	Actions
jennifer	/jennifer/Annuity template.docx	Public	Aug 5, 2022 2:24 PM	[Edit] [X]
jennifer	/jennifer/Common files/Alt Img Tags - ITAR copy.docx	Public	Aug 5, 2022 2:21 PM	[Edit] [X]
jennifer	/jennifer/Common files/075b2598e4b748f5972e98b1250a6421.jpeg	Private	Aug 5, 2022 1:02 PM	[Edit] [X]
artur	/artur/test	Private	Jul 19, 2022 12:02 PM	[Edit] [X]

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	User Name	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.

Manage User Shares i				
Filter		Filter by Username, Location or Sharename	Show 10 Items	Export
User name	Location	Type	Created Date	Actions
jenniferp ^{owner}	/EXTERNAL/Misc/ASBeachjfif	Private	Jan 14, 2021 7:26 AM	
gabrielled	/SHARED/team folder admin/Human Resources/FCSwitchToClassic.png	Private	Jan 14, 2021 7:22 AM	
team folder admin	/team folder admin/Human Resources/FCSwitchToClassic.png	Private	Jan 14, 2021 7:18 AM	
jenniferp	/jenniferp/DI 19-20	Private	Jan 13, 2021 3:36 PM	
jenniferp	/jenniferp/Accounts	Public	Jan 13, 2021 3:35 PM	
jenniferp	/jenniferp/For Review	Public	Jan 12, 2021 2:45 PM	
jenniferp	/jenniferp	Public	Jan 12, 2021 2:39 PM	
jenniferp	/jenniferp/FCAddToFavorites.png	Private	Jan 12, 2021 2:18 PM	
team folder admin	/team folder admin/Other Departments	Public	Jan 12, 2021 9:58 AM	
team folder admin	/team folder admin/Marketing	Private	Jan 12, 2021 8:45 AM	

Page 1 of 4 32 rows

- 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**.

Manage Share for file - FCSwitchToClassic.png

Share URL: [Icons]

Share Options

Share Owner: (arrow)

Shared File/Folder: /SHARED/team folder admin/Human Resol

Share Name:

Expires (Optional): Never Expires Expires

Email File Change Notifications: Yes No

(arrow)

Share Permissions

Allow Everyone
 Allow Selected Users/Groups

Users | Group

User	Allow View	Allow Download	Allow Upload	Allow Share	Misc
No users selected. Click 'Invite User' to select user(s).					

Unsaved changes. Click 'Update' to save.

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

Manage User Shares i				
Filter <input type="text" value="Filter by Username, Location or Sharename"/>		Show 10 Items ▼	Export	
User name	Location	Type	Created Date	Actions
jenniferp	/INTERNAL/Misc/ASBeachjfif	Private	Jan 14, 2021 7:26 AM	
jenniferp	/SHARED/team folder admin/Human Resources/FCSwitchToClassic.png	Private	Jan 14, 2021 7:22 AM	
team folder admin	/team folder admin/Human Resources/FCSwitchToClassic.png	Private	Jan 14, 2021 7:18 AM	
jenniferp	/jenniferp/DI 19-20	Private	Jan 13, 2021 3:36 PM	
jenniferp	/jenniferp/Accounts	Public	Jan 13, 2021 3:35 PM	
jenniferp	/jenniferp/For Review	Public	Jan 12, 2021 2:45 PM	
jenniferp	/jenniferp	Public	Jan 12, 2021 2:39 PM	
jenniferp	/jenniferp/FCAddToFavorites.png	Private	Jan 12, 2021 2:18 PM	
team folder admin	/team folder admin/Other Departments	Public	Jan 12, 2021 9:58 AM	
team folder admin	/team folder admin/Marketing	Private	Jan 12, 2021 8:45 AM	

Page 1 of 4 ▶▶
32 rows

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 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

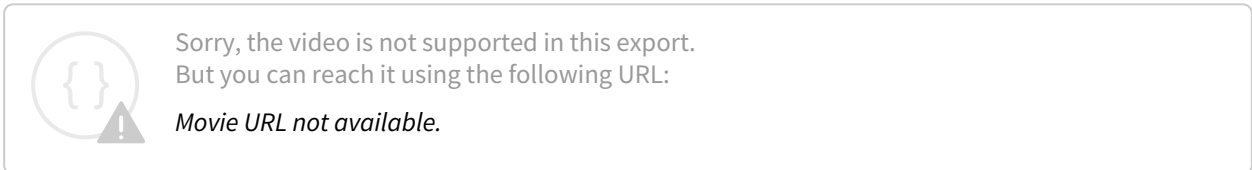
Public folder shares provide a share link that opens a page listing the contents of the folder. By making minor changes to the share link, a direct downloadable link for any file in the folder can be created.

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.



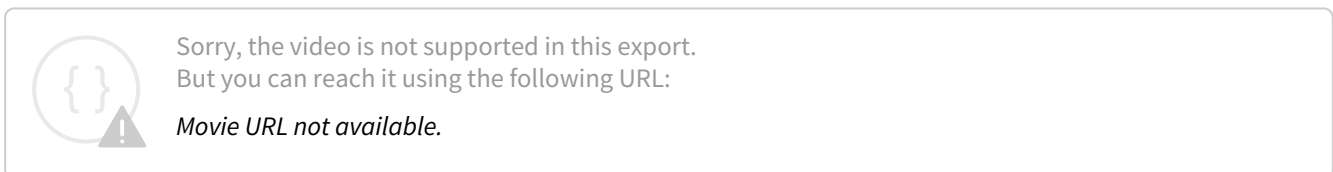
To create a direct link to a file in the shared folder:

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!/bli3S5COtloHQD49yINBKMS5/XOOcISQ2AAdiOWP1>

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.



1. Copy the link to a text editor in order to modify it.
2. 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](#).)
3. 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!/bli3S5COtloHQD49yINBKMS5/XOOcISQ2AAdiOWP1/customers.docx>)
4. 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!/bli3S5COtloHQD49yINBKMS5/XOOcISQ2AAdiOWP1/customers.docx&filename=customers.docx>)
5. 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!/bli3S5COtloHQD49yINBKMS5/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!/bli3S5COtloHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

Modified link

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5COtloHQD49yINBKMS5/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!/bli3S5COtloHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

Modified link

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5COtloHQD49yINBKMS5/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](#)
- [Clear Partial Uploads Automatically](#)
- [All Managed Storage Options](#)

Protecting Your Storage


- [Set Up Encryption for Managed Storage](#)

Managing User Locks

 Lock support is available in FileCloud v9.0 and later

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

⚙️ Manage Settings

Server
Storage
Authentication
Admin
Database
Email
Endpoint Backup

General
User
Password
Notifications
Share
Preview
Support Services

DUO Security
Privacy

General System Settings

Server Timezone ▼

America/Chicago

Specify a timezone from here - <http://www.php.net/manual/en/timezones.php>

Date Format ▼

MMM dd, yyyy (Jan 15, 2019)

Time Format ▼

h:mm A (2:20 PM)

Apply Folder Level Security

Allow folder level security settings to apply to share permissions

Disable Action Panel

Hide action panel that contains activity, comments, and permission detail panels in user UI.

Disable Metadata Panel

Hide Metadata panel in user UI.

Disable Locking

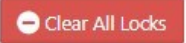






Disable ability for users from being able to lock files or folders

To disable locking:

1. Log on to *Admin Portal*.
2. From the left navigation pane, click *Settings*.
3. On the *Settings* screen, click the *Misc.* tab.
4. On the *Misc.* screen, select the *General* sub-tab.
5. Under *General System Settings*, next to *Disable Locking*, select the checkbox.
6. 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.

Manage File/Folder Locks					 
Filter					
<input type="text" value="Filter"/>					
Path	Lock Date	Locked By	Expiration	Actions	
/jenniferp/Test Word Doc.docx	Mar 10, 2020	jenniferp	NONE		
/elin frei/New Feature Spec.docx	Mar 10, 2020	elin frei	NONE		
/jenniferp/tutorial.docx	Mar 10, 2020	jenniferp	NONE		
/jenniferp/Sample-Public-Forum-Ballot-Blank.pdf	Mar 10, 2020	jenniferp	NONE		
/jenniferp/2020-02-24_09h48_07.png	Mar 10, 2020	jenniferp	NONE		

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, you can see a 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

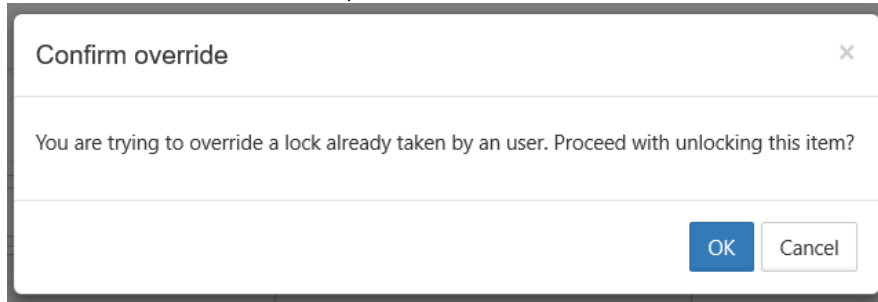
There are times when you may need to unlock a file for a user.

- 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 ().

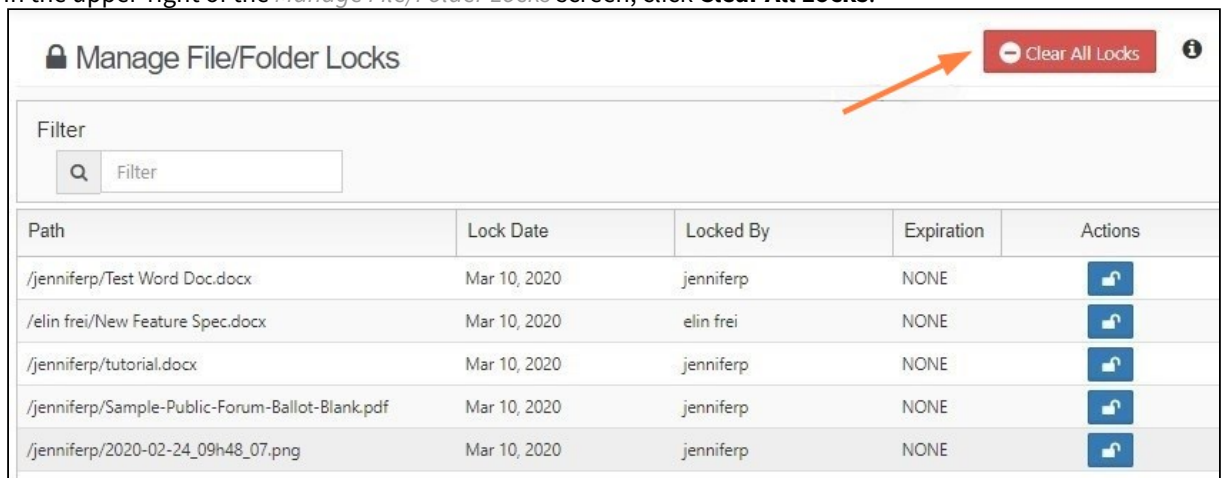
5. On the *Confirm Override* screen, click *OK*.



To release the lock on all locked files and folders:

Beginning with Version 19.3, FileCloud supports clearing all user locks simultaneously.

1. Log on to *Admin Portal*.
2. From the left navigation pane, click **User Locks**.
3. In the upper-right of 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](#)
- [Editing all users file and folder path notifications](#)
- [Adding notifications for actions on user's files and folders](#)

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 screenshot shows the 'Manage Users' interface. On the left is a navigation panel with 'Users' selected. The main area displays a table of users with columns for User name, Display Name, Email, Last Login, Status, and Actions. The user 'jessicam' is highlighted in grey, and an orange arrow points to the edit icon in the Actions column for that user.

	User name	Display Name	Email	Last Login	Status	Actions
	aliah	Aliah	aliahp@example.com	--	Full Access	[Edit] [Settings] [Delete]
	david	david	dm898002@gmail.com	28 Apr 2021 08:20	Full Access	[Edit] [Settings] [Delete]
	hr manager	HR Manager	hrmanager@example.com	--	Full Access	[Edit] [Settings] [Delete]
	jaredtaylor978	Jared	jaredtaylor978@gmail.com	09 Jul 2021 13:14	Full Access	[Edit] [Settings] [Delete]
	jenniferp	Emma	jennifer.perkins@codelathe.com	09 Jul 2021 08:23	Full Access	[Edit] [Settings] [Delete]
	jessicam	Jessica	jm2344311@gmail.com	15 Jul 2021 09:23	Full Access	[Edit] [Settings] [Delete]

The User Details dialog box opens.

3. Click the **Manage Notifications** icon.

User Details

Name	jessicam	Total Quota	2 GB
Email	jm2344311@gmail.com	Used Quota	2.2 MB
Last Login	15 Jul 2021 09:23	Available Quota	2 GB
TOS Date	Not Accepted	Used Storage	2.2 MB
Group	Manage		More

Manage Files Manage Policy Manage Shares Mobile Devices Reset Password Send Email **Manage Notifications** Manage Backups Delete Account

Profile Image

Update Remove

Access Level: Full

Authentication: Default

Email: jm2344311@gmail.com

Save Close

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.

Manage Notifications for jessicam

Path	Modified Date	User	Actions
/jessicam/Customer Info	Jul 15, 2021 9:24 AM	jessicam	

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

Notification Settings for Customer Info

Path: /jessicam/Customer Info

Use default notification settings
 Use my own notification settings

Send Notifications

Send Notifications on

- Upload
When file or folder is added
- Download
When file or folder is downloaded
- Share
When a file or folder is shared with someone
- Delete
When a file or folder is deleted
- Rename
When a file or folder is renamed
- Update
When a file is modified
- Preview
When a file is viewed in the browser or in the mobile app
- Lock/Unlock
When a file or folder is locked or unlocked
- Self Notifications
Send notifications for actions done by me

Save Cancel

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 turn off notifications temporarily, uncheck **Send Notifications**; otherwise, leave it checked.

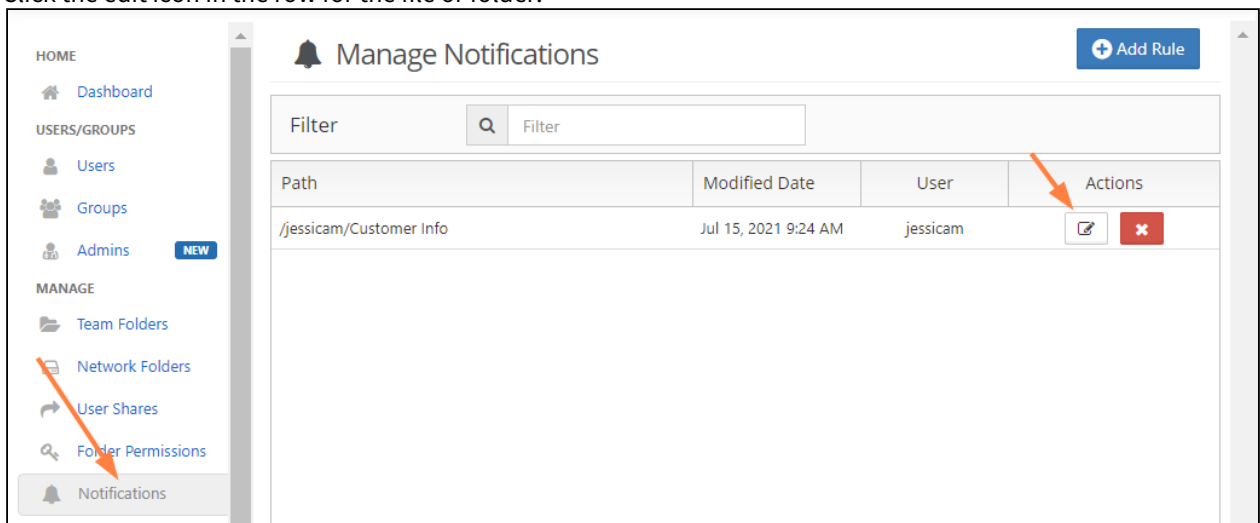
- If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
- If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications** box.
- If the user has **Use default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

Notification Settings for Customer Info
✕

Path: /jessicam/Customer Info

Use default notification settings
 Use my own notification settings

Send Notifications

Send Notifications on

- Upload
When file or folder is added
- Download
When file or folder is downloaded
- Share
When a file or folder is shared with someone
- Delete
When a file or folder is deleted
- Rename
When a file or folder is renamed
- Update
When a file is modified
- Preview
When a file is viewed in the browser or in the mobile app
- Lock/Unlock
When a file or folder is locked or unlocked
- Self Notifications
Send notifications for actions done by me

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 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 screenshot shows the 'Manage Notifications' interface. On the left, a navigation panel lists 'Groups', 'Admins', 'MANAGE' (with sub-items: 'Team Folders', 'Network Folders', 'User Shares', 'Folder Permissions', 'Notifications'), and 'DEVICES' (with sub-item: 'Devices'). The 'Notifications' item is highlighted. The main content area has a title 'Manage Notifications' and a '+ Add Rule' button in the top right corner, indicated by an orange arrow. Below the title is a search filter box. A table below the filter shows a single notification rule:

Path	Modified Date	User	Actions
/jessicam/Customer Info	Jul 15, 2021 9:24 AM	jessicam	

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

Add Custom User Notifications Rule
✕

Account or Email

jessicam

Q Search

Path

jessicam/Customer Info/LimaM

Use default notification settings

Use my own notification settings

Send Notifications

Send Notifications on

- Upload
When file or folder is added
- Download
When file or folder is downloaded
- Share
When a file or folder is shared with someone
- Delete
When a file or folder is deleted
- Rename
When a file or folder is renamed
- Update
When a file is modified
- Preview
When a file is viewed in the browser or in the mobile app
- Lock/Unlock
When a file or folder is locked or unlocked
- Self Notifications
Send notifications for actions done by me

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**.

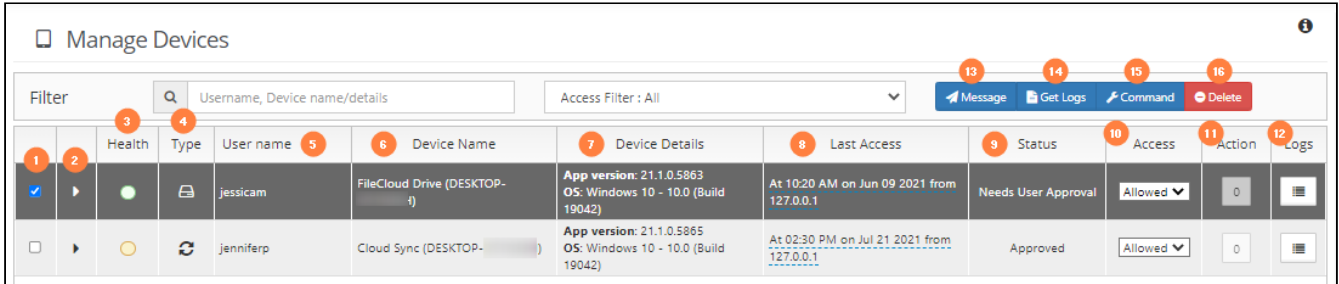
Managing Client Devices

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	<input type="checkbox"/>	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. <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 [Basic 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**
- **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.

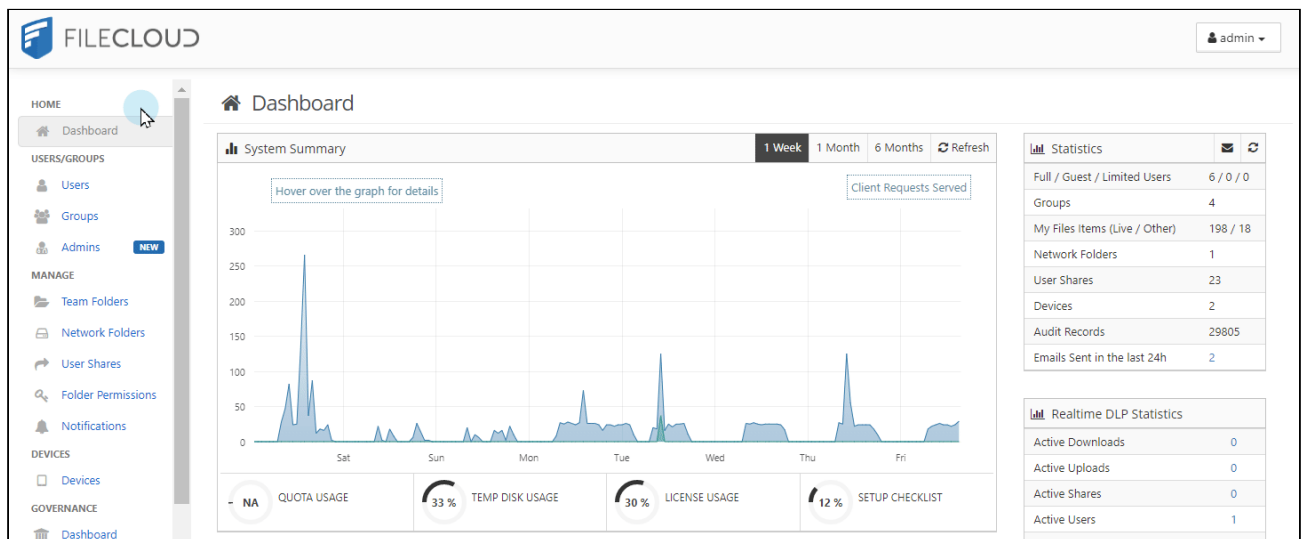
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

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

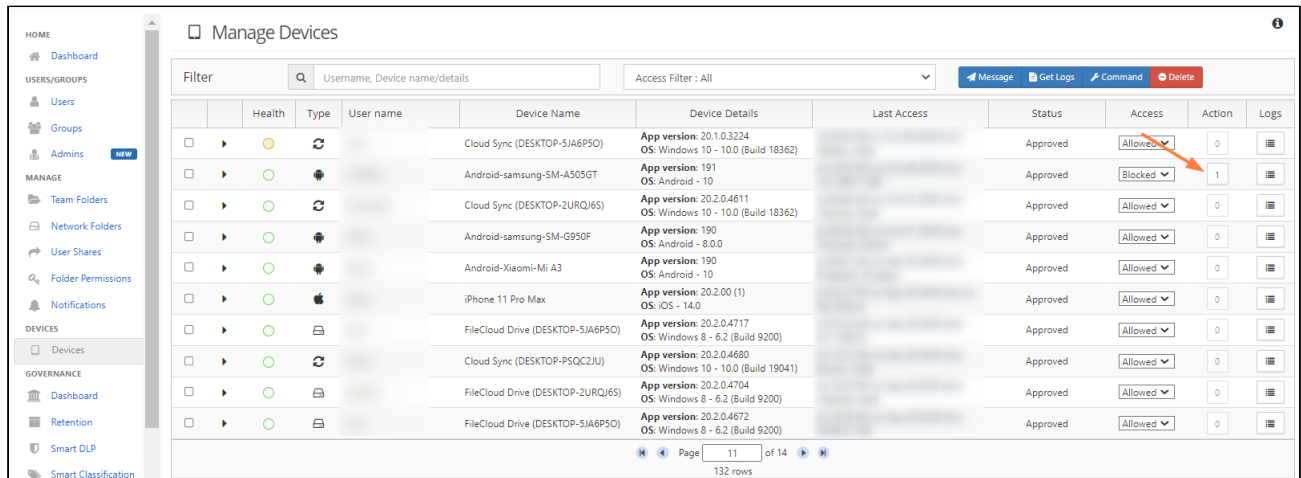


To see the details of a connected device:

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.



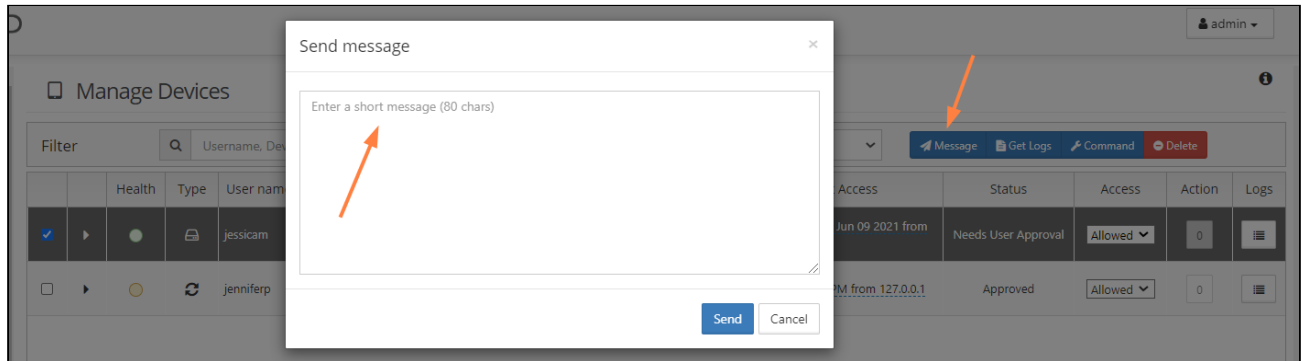
To view Actions:

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.

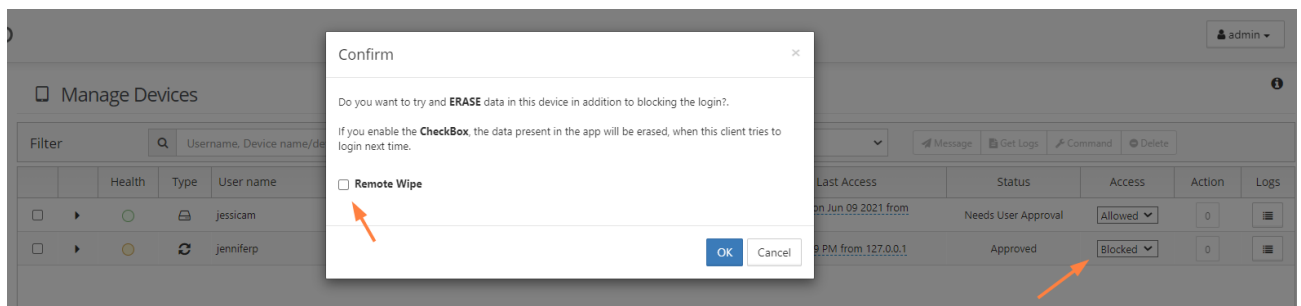
When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

- 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

- 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*.

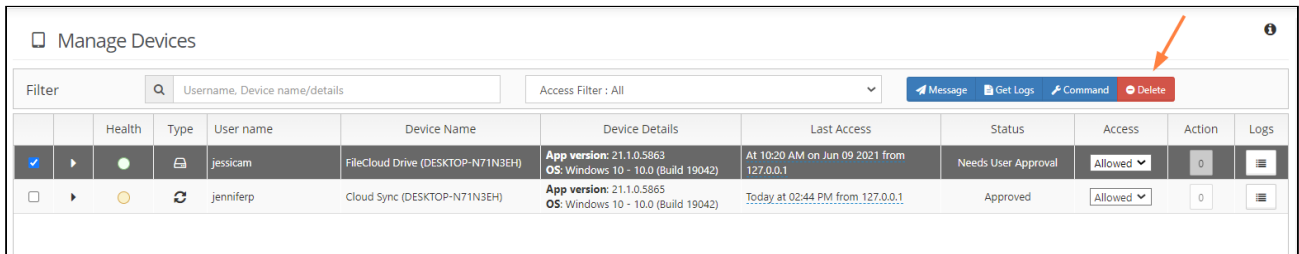
Delete a Client Device Record

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.




The screenshot shows the 'Manage Devices' interface. At the top, there is a search filter for 'Username, Device name/details' and an 'Access Filter' set to 'All'. Action buttons include 'Message', 'Get Logs', 'Command', and 'Delete' (highlighted with an orange arrow). Below is a table with columns: Health, Type, User name, Device Name, Device Details, Last Access, Status, Access, Action, and Logs.

Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
		jessicam	FileCloud Drive (DESKTOP-N71N3EH)	App version: 21.1.0.5863 OS: Windows 10 - 10.0 (Build 19042)	At 10:20 AM on Jun 09 2021 from 127.0.0.1	Needs User Approval	Allowed	0	
		jenniferp	Cloud Sync (DESKTOP-N71N3EH)	App version: 21.1.0.5865 OS: Windows 10 - 10.0 (Build 19042)	Today at 02:44 PM from 127.0.0.1	Approved	Allowed	0	

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

 Centralized Device Management is available in FileCloud Server version 17.3 and later.


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](#)
- [Viewing Client Information](#)
- [Requesting Client Log Files](#)
- [Blocking and Remotely Wiping a Client Device](#)
- [Sending a Message to a Client's Display](#)

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."

Policy Settings
✕

Note: Some policy settings will not be applicable for Guest and Limited users.

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications


Manage Device Configuration

Client Configuration

Specify default configuration for all client applications. This has to be a valid XML value.

Save
Reset
✕ Close

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the policy that you want to configure, and then click the edit icon ().
5. Click on the *Device Configuration* tab.
6. Paste or type in the remote device configuration XML in *Client Configuration*.

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

```

<xml>

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

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

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

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

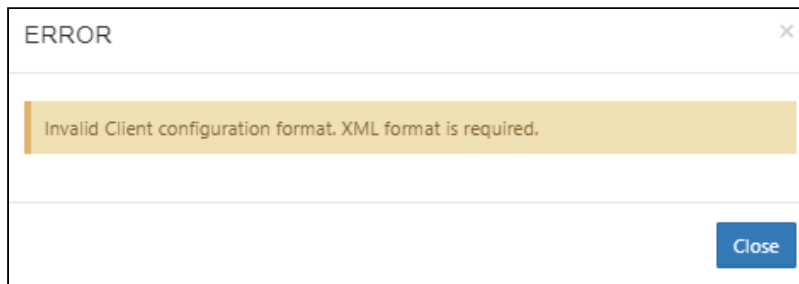
<outlookaddin>
  <settings>
    <!-- XML for outlookaddin App -->
  </settings>
</outlookaddin>

</xml>
```

What if the XML code for my policy is not working?

Incorrect XML Code

If your XML code cannot be validated then you will see the following warning:




Please correct the XML error and try again to Save your device configuration.

What do you want to configure?

- [Device Configuration XML For Drive for Mac](#)
- [Device Configuration XML For Outlook Add-in](#)
- [Device Configuration XML For Server Sync](#)
- [Device Configuration XML For Sync](#)
- [Device Configuration XML For Windows Drive](#)
- [Device Configuration XML for Desktop Edit](#)
- [Device Configuration XML for FileCloud Desktop for macOS](#)
- [Device Configuration XML for FileCloud Desktop for Windows](#)

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.

Policy Settings ✕

Note: Some policy settings will not be applicable for Guest and Limited users.

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications


Manage Device Configuration

Client Configuration

Specify default configuration for all client applications. This has to be a valid XML value.

Save
Reset
✕ Close

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the policy that you want to configure, and then click the edit icon ().
5. Click on the *Device Configuration* tab.
6. In *Client Configuration*, paste or type in the following remote device configuration XML.

```
<xml>
  <macclouddrive>
```

```


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

```

7. Replace the <!-- XML for Mac Drive --> line with the parameters that you need using the descriptions in Table 1.

Table 1. The following XML tags are supported for Drive for Mac device configuration.


Supported keys for **FileCloud Drive for Mac**. All keys are optional. One or more of these keys can be supplied to drive's section of XML command.

XML Tag	Value	Example
maxdownloadsizeinmb	<p>Assigns the maximum single file download limit to the supplied value.</p> <div data-bbox="506 709 1036 882" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> The download limit does not apply to the following file types: .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .indd.</p> </div>	<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>
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 finder when drive starts up and 0 will disable it.	<driveopenexploreronstartup>1</driveopenexploreronstartup>
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>

XML Tag	Value	Example
disableprecaching	<p>Setting this value to 1 disables precaching.</p> <p>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.</p>	<code><disableprecaching>1</disableprecaching></code>
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.	<code><disableautologin>1</disableautologin></code>
currentlanguage	See Translations for currently available languages.	<code><currentlanguage>english</currentlanguage></code>

Device Configuration XML For Outlook Add-in

[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.

Policy Settings ✕

Note: Some policy settings will not be applicable for Guest and Limited users.

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications


Manage Device Configuration

Client Configuration

Specify default configuration for all client applications. This has to be a valid XML value.

Save
Reset
✕ Close

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the policy that you want to configure, and then click the edit icon (.
5. Click on the *Device Configuration* tab.
6. In *Client Configuration*, paste or type in the following remote device configuration XML.

```

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

7. Replace the `<!-- XML for outlookaddin App -->` line with the parameters that you need using the descriptions in Table 1.

To set default values for auto upload:

In the Outlook addin Client Configuration, you can set the default values for **Auto Upload Attachments** and **Auto Upload Attachments Greater than Size (MB)** in the Upload Settings.

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:

The screenshot shows the 'Settings' dialog box with the 'Upload' tab selected. The 'Upload Settings' section includes:

- Default Upload Folder:** A text box containing '/sathya/upload' with 'Browse' and 'Clear' buttons below it.
- Auto Upload Attachments:** A checked checkbox with the text '(Outlook must be Restarted)' next to it.
- Auto Upload Attachments Greater than Size (MB):** A text box containing the number '3'.
- Save:** A blue button at the bottom left.
- Status:** A bar at the bottom right indicating 'Not Connected'.

Table 1. The following XML tags are supported for Microsoft Outlook Addin device configuration.

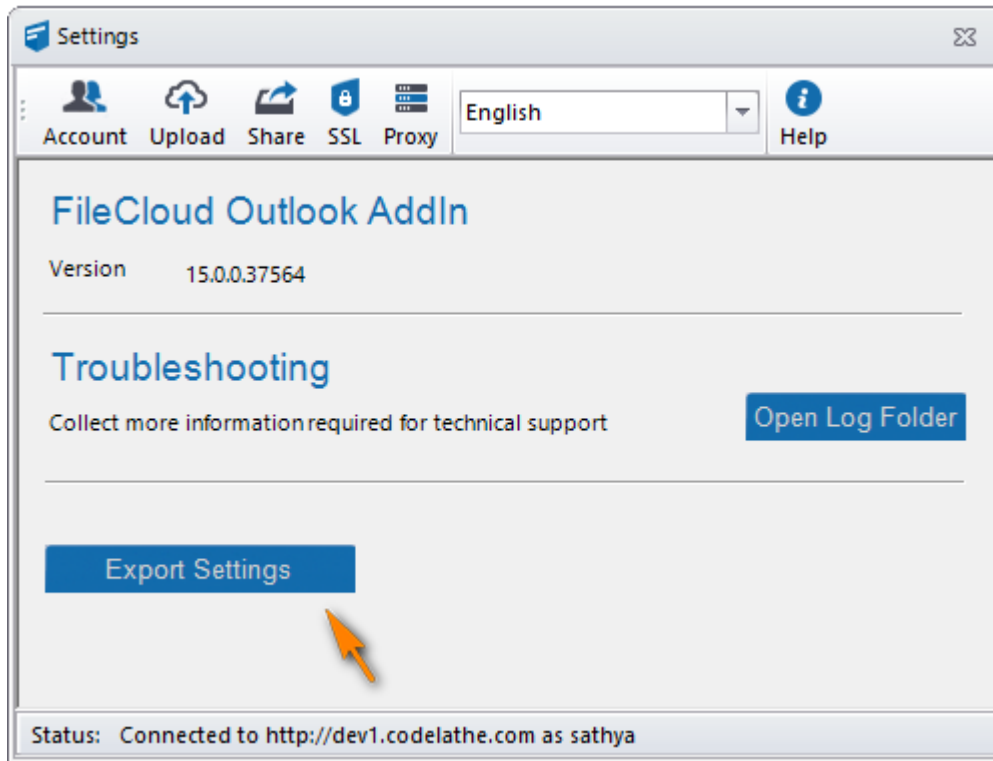
The following XML tags are supported for the Outlook Add-in

autoupload	Sets default for auto upload to on or off. 0 => auto upload is off; 1=> auto upload is on.	<autoupload>1</autoupload>
autouploadsize	Specifies the default minimum size in MB of an attachment that is automatically uploaded.	<autouploadsize>3</autouploadsize>
XML Tag	Value	Example
serverurl	FileCloud server URL	<serverurl> http://www.yourdomain.com/serverurl </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>
proxyserver	Proxy Server URL	<proxyserver> http://proxyserverurl.com/proxyserver </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>

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...](#)



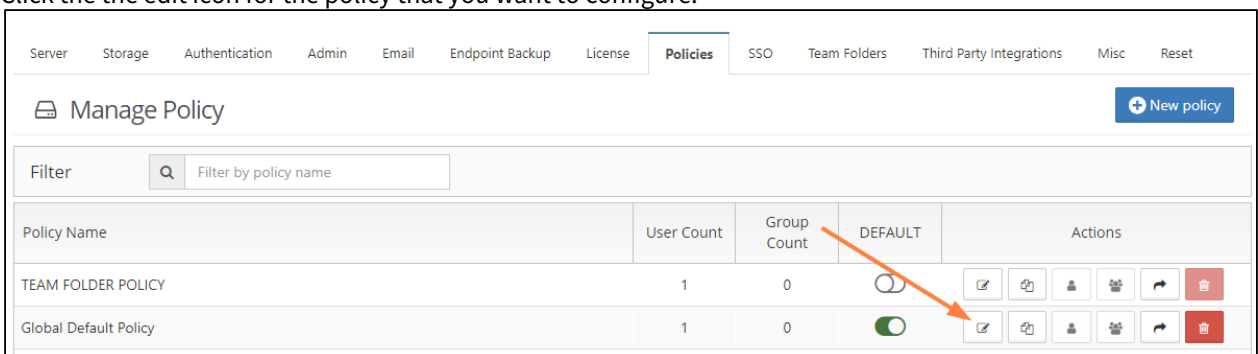
Device Configuration XML For Server Sync

Client Device configuration settings can be configured remotely using policies.

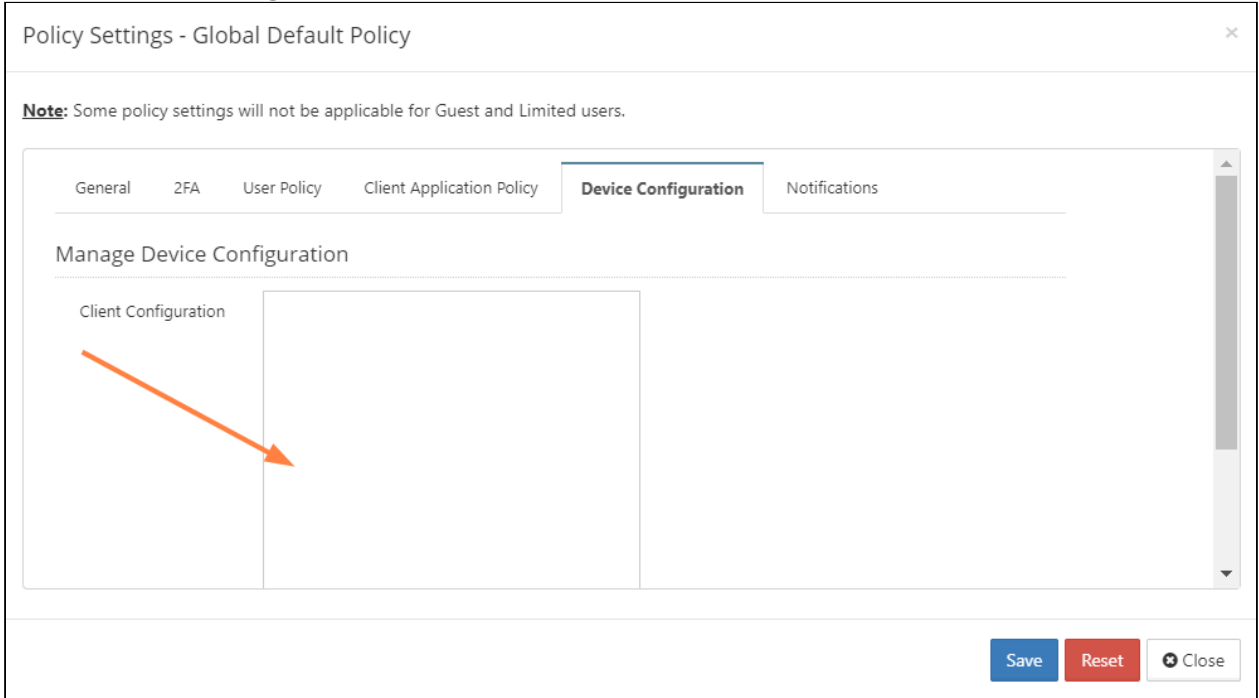
⚠ For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the the edit icon for the policy that you want to configure.



- Click on the *Device Configuration* tab.



- In *Client Configuration*, paste or type in the following remote device configuration XML.

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

- Replace the `<!-- XML for ServerSync App -->` line with the parameters that you need using the descriptions in Table 1.

Table 1. The following XML tags are supported for the ServerSync device configuration.


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>

XML Tag	Value	Example
limit_folder_1 limit_folder_2 limit_folder_3 ...	<p>Depending upon the number of folders specified in the limit_folder_count, you will need to have the appropriate number of entries.</p> <p>The folder value is specified using 5 parameters using the following format <REMOTE FOLDER> <LOCAL FOLDER> <PERMISSIONS> <SYNC TYPE> <SYNC DISABLED></p> <p><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).</p>	<limit_folder_1>/john/folder1 C:\data\local 0 1 0</limit_folder_1>
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	<p>Number from 0 to 100, which indicates what % of files being deleted requires approval. Default is 10.</p> <p>This applies only to file deletions in the local sync folder.</p>	<deleteapprovalpct>20</deleteapprovalpct>

XML Tag	Value	Example
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, allowuserconfigfornewfolders, and allowuserconfigforbackup tags to 1 in the policy.

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

See [What XML settings allow users to modify folders?](#) below.

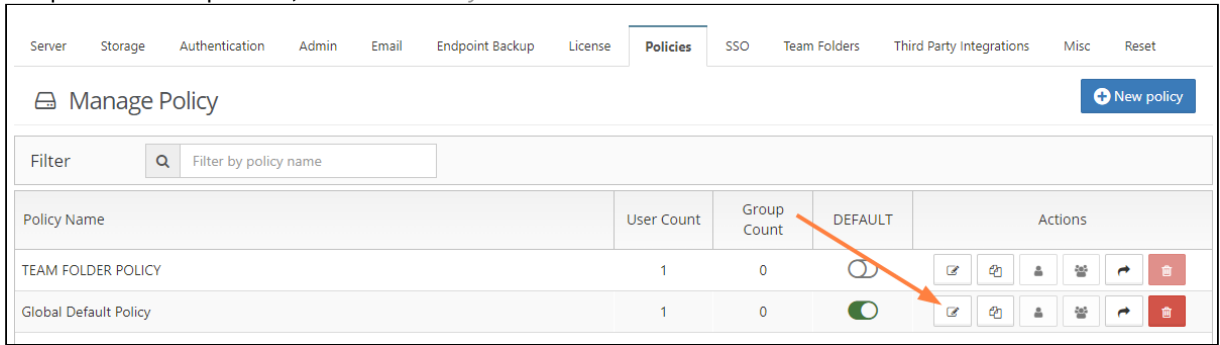
FAQs

How do I enter device configuration XML for Sync?

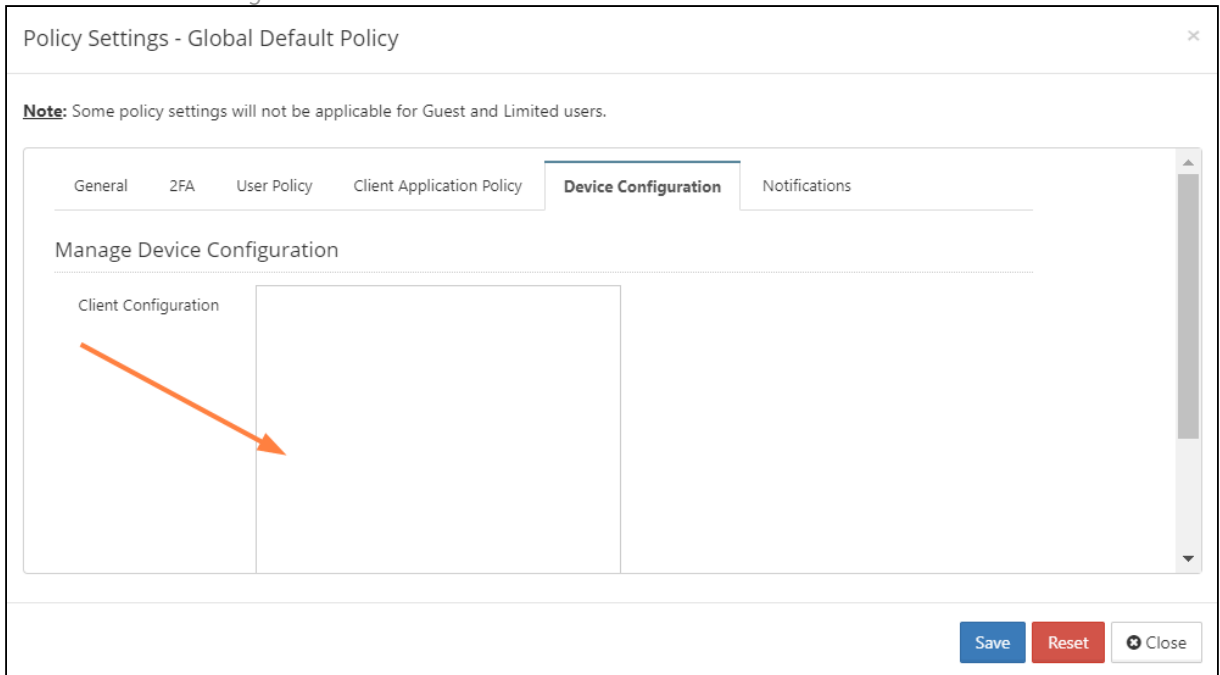
To set a device configuration for a policy:

1. Open the FileCloud Admin portal and then select *Settings*.

2. To open the list of policies, select the *Policy* tab.



- 3. Open the Policy that you want to edit
- 4. Select the *Device Configuration* tab.



5. In *Client Configuration*, paste or type in the following remote device configuration XML.

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

6. Replace **<!-- XML for Sync App -->** with any of the configuration parameters from the following table:.

Supported XML Tags for Sync

XML Tag	Value	Example
---------	-------	---------

<p>limitfolders</p>	<p>' ' separated list of folders for selective sync. If Limitfolders is not specified, then there are no folders for selective sync.</p>	<p><limitfolders>/john/folder1 /john/folder2</limitfolders></p>
<p>offline_folder_count</p>	<p>Number of offline folders to sync. If key is not specified, then there are no offline folders.</p>	<p><offline_folder_count>0</offline_folder_count></p>
<p>offline_folder_1 offline_folder_2 offline_folder_3 ...</p>	<p>Depending upon the number of offline folders specified in the offline_folder_count, you will need to have the appropriate number of entries.</p> <p>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></p> <p><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</p>	<p><offline_folder_1>C:\data\local\john/folder1 0 30m 1 0 0</offline_folder_1></p>
<p>disablenotifications</p>	<p>0/1 - Enable or Disable sync notifications.</p>	<p><disablenotifications>1</disablenotifications></p>
<p>showlocks</p>	<p>0/1 - Enable or Disable if lock information is shown in icon overlay</p>	<p><showlocks>1</showlocks></p>

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>
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>

albtwforupload	<p>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.</p> <p>⚠ If <i>albtwforupload</i> or <i>albtwfordownload</i> is specified but <i>albtwfromtime</i> and <i>albtwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albtwforupload></albtwforupload></pre>
albtwfordownload	<p>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.</p> <p>⚠ If <i>albtwforupload</i> or <i>albtwfordownload</i> is specified but <i>albtwfromtime</i> and <i>albtwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albtwfordownload></albtwfordownload></pre>
albtwfromtime	<p>Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit.</p> <p>Time must be expressed in the format HH:MM:SS</p> <p>⚠ If <i>albtwforupload</i> or <i>albtwfordownload</i> is specified but <i>albtwfromtime</i> and <i>albtwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albtwfromtime>16:45:00</albtwfromtime></pre>
albtwtotime	<p>Specifies the ending time when the alternative settings should be used instead of the global bandwidth limit.</p> <p>Time must be expressed in the format HH:MM:SS</p> <p>⚠ If <i>albtwforupload</i> or <i>albtwfordownload</i> is specified but <i>albtwfromtime</i> and <i>albtwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albtwtotime>24:00:00</albtwtotime></pre>

altbwschedule_dayofweek	<p>Specifies the days of the week when the alternative settings should be used instead of the global bandwidth limit.</p> <p>This value can be any number such as: {-1, 0, 1, 2, 3, 4, 5, 6} where:</p> <ul style="list-style-type: none"> -1 means every day 0 means Sunday 1 means Monday and so on... 	<altbwschedule_dayofweek>3</altbwschedule_dayofweek>
timeactivecontrolsset	<p>Enables/Disables the Active Sync Hours settings</p> <p>1 = enabled</p> <p>0 = disabled</p>	<timeactivecontrolsset>1</timeactivecontrolsset>
activesync_daysofweek	<p>Specifies the days of the week when a client can run the Sync app</p> <p>Any number {-1, 0, 1, 2, 3, 4, 5, 6} where:</p> <ul style="list-style-type: none"> -1 = Everyday 0 = Sunday 1 = Monday and so on... 	<activesync_daysofweek>5</activesync_daysofweek>
activesync_timeofday	<p>Specifies the times during the days of the week when a client can run the Sync app</p> <p>Use the format HH:MM:SS-HH:MM:SS</p>	<activesync_timeofday>8:00:00-20:00:00</activesync_timeofday>
allowuserconfigforlimitsync	<p>0 = cannot modify the folder and any <i>limitfolder</i> setting is applied</p> <p>1 = can modify the folder and overrules any <i>limitfolder</i> setting</p> <p>This value works in combination with:</p> <ul style="list-style-type: none"> <i>limitfolders</i> 	<allowuserconfigforlimitsync>1</allowuserconfigforlimitsync>

allowuserconfigfornewfolders	<p>Allows user to configure network folders</p> <p>0 = cannot modify the folder and any <i>offlinefolder</i> setting is applied</p> <p>1 = can modify the folder and overrules any <i>offlinefolder</i> setting</p> <p>This value works in combination with:</p> <ul style="list-style-type: none"> • <i>offlinefolders</i> 	<allowuserconfigfornewfolders>1</allowuserconfigfornewfolders>
allowuserconfigforbackup	<p>0 = cannot modify the folder and any <i>offlinefolder</i> setting is applied</p> <p>1 = can modify the folder and overrules any <i>offlinefolder</i> setting</p> <p>This value works in combination with:</p> <ul style="list-style-type: none"> • <i>offlinefolders</i> 	<allowuserconfigforbackup>1</allowuserconfigforbackup>
checkupdates (available in FileCloud 22.1)	<p>0 = Sync does not check for updates on startup</p> <p>1 = (default) Sync checks for updates on startup, and notifies user if there is an update</p>	<checkupdates>1</checkupdates>

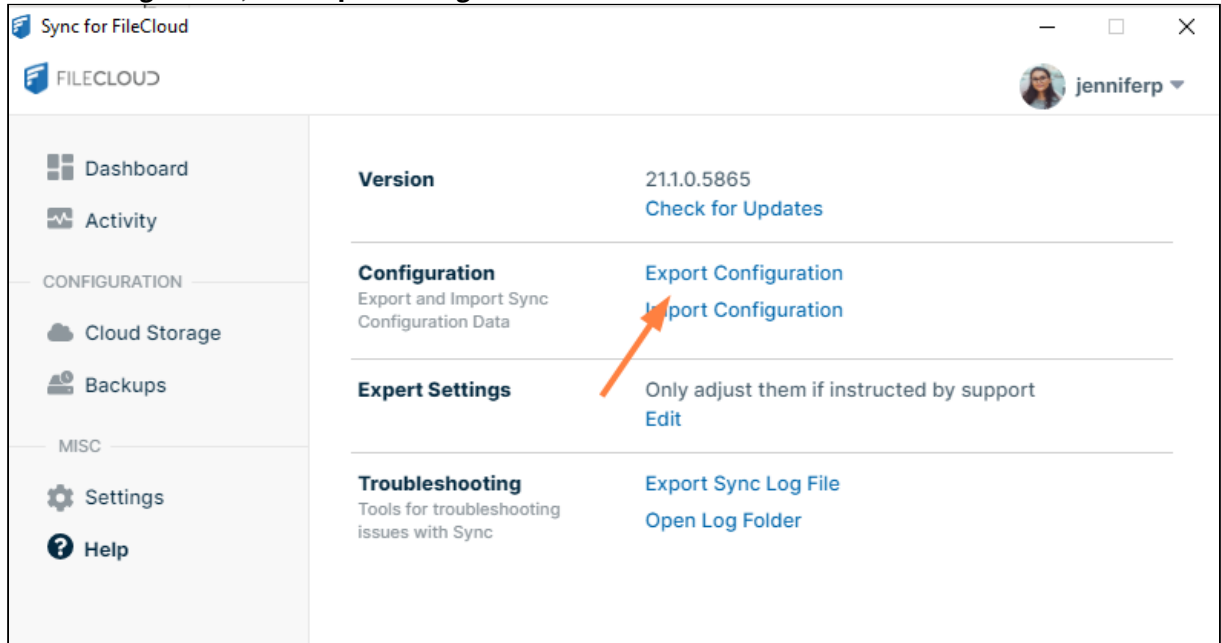
How do I get the configuration XML for Sync?

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>

XML Tag	Value	Example
albtwtotime	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	<albtwtotime>24:00:00</albtwtotime>
albtwschedule_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: <ul style="list-style-type: none"> • -1 means every day • 0 means Sunday • 1 means Monday • and so on.. 	<albtwschedule_dayofweek>3</albtwschedule_dayofweek>

 If *albtwforupload* or *albtwfordownload* is specified but *albtwfromtime* and *albtwtotime* 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 <i>limitfolder</i> setting, if present in xml, is applied. 1 = user can modify Selective Sync folders and this overrules any <i>limitfolder</i> settings.	<allowuserconfigforlimitsync>1<allowuserconfigforlimitsync>
allowuserconfigfornwfolders	0 = user cannot modify Network folders and any <i>offlinefolder</i> setting configured for Network folders, if present, is applied. 1 = user can modify Network folders and this overrules any <i>offlinefolder</i> setting configured for Network folders.	<allowuserconfigfornwfolders>1<allowuserconfigfornwfolders>

XML Tag	Value	Example
allowuserconfigforbackup	<p>0 = user cannot modify the Backup folder and any <i>offlinefolder</i> setting configured for Backup folders, if present, is applied.</p> <p>1 = user can modify the folder and this overrides any <i>offlinefolder</i> setting configured for Backup folders</p>	<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	<p>Although limit folders are present, because <i>allowuserconfigforlimitsync</i> is set to allow modifications:</p> <ul style="list-style-type: none"> • <i>limitfolder</i> settings will NOT be applied • Users CAN modify their selective sync folders
/john/folder1 /john/folder2	0	<p>Because limit folders are present, AND <i>allowuserconfigforlimitsync</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • <i>limitfolder</i> settings will BE applied • Users CANNOT modify their selective sync folders
<i>None set but other settings are present</i>	1	<p>Because <i>allowuserconfigforlimitsync</i> is set to allow modifications:</p> <ul style="list-style-type: none"> • Users CAN modify their selective sync folders, irrespective of any other settings in the config
<i>None set but other settings are present</i>	0	<p>Because <i>allowuserconfigforlimitsync</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • Users CANNOT modify their selective sync folders

Controlling modifications to selective network folders

offline folders	allowuserconfigfornwfolders	Sync User's Access
-----------------	-----------------------------	--------------------

/EXTERNAL/folderA	1	<p>Because offline folders (configured as Network Folders) are present, AND <i>allowuserconfigfornewfolders</i> is set to enable modifications:</p> <ul style="list-style-type: none"> • <i>offlinefolder</i> setting configured for Network Folders, will NOT be applied • Sync users CAN modify Network Folders
/EXTERNAL/folderA	0	<p>Because offline folders (configured as Network Folders) are present AND <i>allowuserconfigfornewfolders</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • <i>offlinefolder</i> setting configured for Network folders, will BE applied • Sync users CANNOT modify Network Folders
None set but other settings are present	1	<p>Because <i>allowuserconfigfornewfolders</i> is set to enable modifications:</p> <ul style="list-style-type: none"> • Sync users CAN modify Network Folders, irrespective of any other settings in the config.
None set but other settings are present	0	<p>Because <i>allowuserconfigfornewfolders</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • Sync users CANNOT modify Network Folders

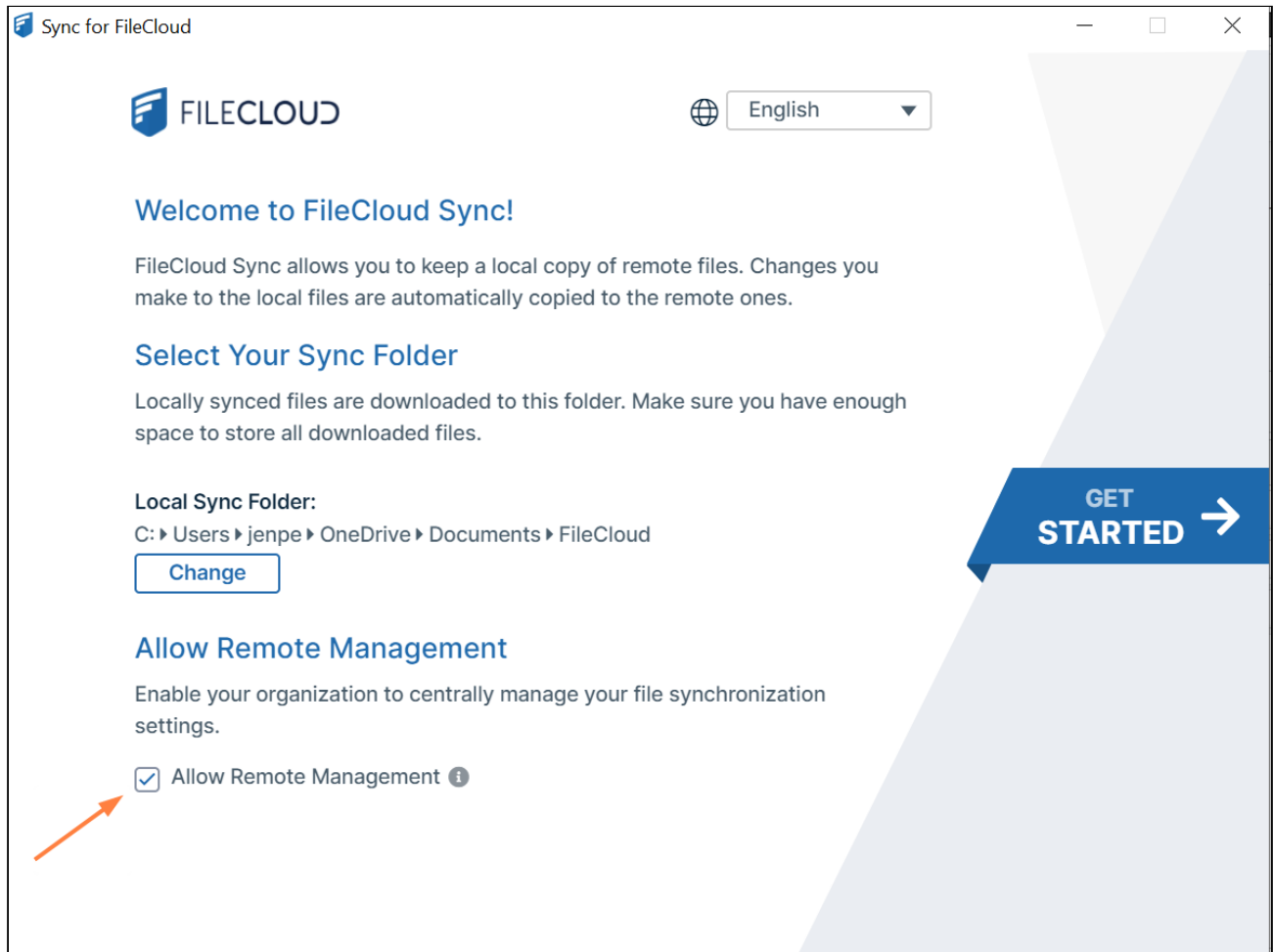
Controlling modifications to selective backup folders

offline folders	allowuserconfigforbackup	Sync User's Access
C:\data\local	1	<p>Because offline folders (configured for backup) are present, AND <i>allowuserconfigforbackup</i> is set to enable modifications:</p> <ul style="list-style-type: none"> • <i>offlinefolder</i> setting configured for Backup folders, will NOT be applied • Sync users CAN modify backup folders

C:\data\local	0	<p>Because offline folders (configured for backup) are present AND <i>allowuserconfigforbackup</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • <i>offlinefolder</i> setting configured for Backup folders, will BE applied • Sync users CANNOT modify backup folders
<i>None set but other settings are present</i>	1	<p>Because <i>allowuserconfigforbackup</i> is set to enable modifications:</p> <ul style="list-style-type: none"> • Sync users CAN modify backup folders, irrespective of any other settings in the config.
<i>None set but other settings are present</i>	0	<p>Because <i>allowuserconfigforbackup</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • 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.

Policy Settings
✕

Note: Some policy settings will not be applicable for Guest and Limited users.

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications


Manage Device Configuration

Client Configuration

Specify default configuration for all client applications. This has to be a valid XML value.

Save
Reset
✕ Close

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the policy that you want to configure, and then click the edit icon ().
5. Click on the *Device Configuration* tab.
6. In *Client Configuration*, paste or type in the following remote device configuration XML.

<xml>

```


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

```

7. Replace the <!-- XML for Windows Drive --> line with the parameters that you need using the descriptions in Table 1.

Table 1. The following XML tags are supported for the Windows Drive device configuration.

Supported keys for **Windows FileCloud Drive**. All keys are optional. One or more of these keys can be supplied to drive's section of XML command.

XML Tag	Value	Example
maxdownloadsizeinmb	<p>Assigns the maximum single file download limit to the supplied value.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> The download limit does not apply to the following file types: .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .indd.</p> </div>	<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>
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>
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>
driveopenexploreronstartu p	Setting this value to 1 will automatically open explorer window when drive starts up and 0 will disable it.	<driveopenexploreronstartup>1</driveopenexploreronstartup>


XML Tag	Value	Example
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>
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}	Replaces with current logged in user name from the Operating System
\${HOME}	Replaces with the location of the current user's Home Path

Variable	Notes
\${USERID}	Replaces 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.

Policy Settings ✕

Note: Some policy settings will not be applicable for Guest and Limited users.

General 2FA User Policy Client Application Policy **Device Configuration** Notifications


Manage Device Configuration

Client Configuration

Specify default configuration for all client applications. This has to be a valid XML value.

Save
Reset
✕ Close

To set a device configuration for a policy:

1. Open a browser and log in the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. To open the list of policies, select the *Policies* tab.
4. Click the policy that you want to configure, and then click the edit icon ().
5. Click on the *Device Configuration* tab.
6. In *Client Configuration*, paste or type in the following remote device configuration XML.

```

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

```


7. Replace the <!-- XML for Desktop Edit --> line with the parameters that you need using the descriptions in Table 1.

Table 1. The following XML tags are supported for Desktop Edit device configuration.

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.

Policy Settings - Global Default Policy

Note: Some policy settings will not be applicable for Guest and External users.

General 2FA User Policy Client Application Policy **Device Configuration** Notifications

Manage Device Configuration

Client Configuration

Save Reset All Close

To set a device configuration for a policy:

1. Open a browser and log in the **Admin Portal**.
2. From the left navigation pane, select **Settings**.
3. To open the list of policies, select the **Policies** tab.
4. Click the policy that you want to configure, and then click the edit icon (🔧).
5. Click on the **Device Configuration** tab.
6. In **Client Configuration**, paste or type in the remote device configuration XML for FileCloud Desktop for macOS. Please note that it uses the xml format:

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

<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.

Example:

The code below shows example settings:

```
<xml>
```



```

<fileclouddesktopmac>
  <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.

Keys and values

Table 1. The following XML tags are supported for FileCloud Desktop for macOS device configuration.


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"

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

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.

Policy Settings - Global Default Policy

Note: Some policy settings will not be applicable for Guest and External users.

General 2FA User Policy Client Application Policy **Device Configuration** Notifications

Manage Device Configuration

Client Configuration

Save Reset All Close

To set a device configuration for a policy:

1. Open a browser and log in to the **Admin Portal**.
2. From the left navigation pane, select **Settings**.
3. To open the list of policies, select the **Policies** tab.
4. Click the policy that you want to configure, and then click the edit icon.
5. Click the **Device Configuration** tab.
6. In **Client Configuration**, paste or type in the remote device configuration XML for FileCloud Desktop for Windows. Please note that it uses the xml format:

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

<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.

Example:

The code below shows example settings:

```
<xml>
<fileclouddesktopwindows>
```

```

<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>
</fileclouddesktopwindows>
</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.

Keys and values

The following XML tags are supported for FileCloud Desktop for Windows device configuration.

Key	Description	Values
lockonopen	Automatically lock files when they are opened.	0 (disabled) 1 (enabled) default
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"

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

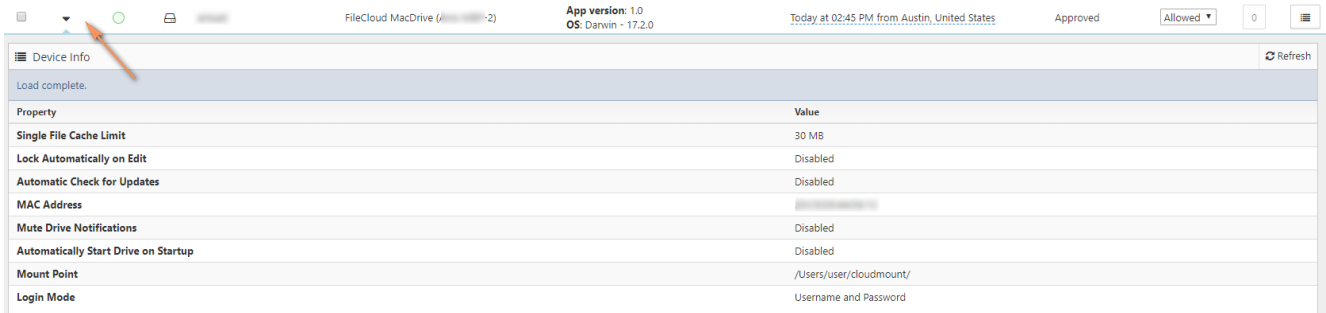
If a key is not supported or a value is incorrect, the application skips it and logs a warning message.

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.

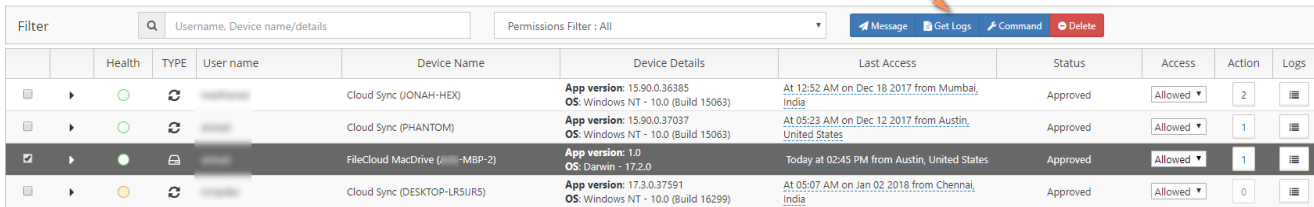
To get logs, select the device in the list and click on "Get Logs" button.

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.

Manage Devices



Filter	Health	TYPE	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
	●			Cloud Sync (JONAH-HEX)	App version: 15.90.0.36385 OS: Windows NT - 10.0 (Build 15063)	At 12:52 AM on Dec 18, 2017 from Mumbai, India	Approved	Allowed	2	
	●			Cloud Sync (PHANTOM)	App version: 15.90.0.37037 OS: Windows NT - 10.0 (Build 15063)	At 09:23 AM on Dec 12, 2017 from Austin, United States	Approved	Allowed	1	
<input checked="" type="checkbox"/>	●			FileCloud MacDrive (J...-MBP-2)	App version: 1.0 OS: Darwin - 17.2.0	Today at 02:45 PM from Austin, United States	Approved	Allowed	1	
	●			Cloud Sync (DESKTOP-LRSURS)	App version: 17.3.0.37591 OS: Windows NT - 10.0 (Build 16299)	At 05:07 AM on Jan 02, 2018 from Chennai, India	Approved	Allowed	0	

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 its 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

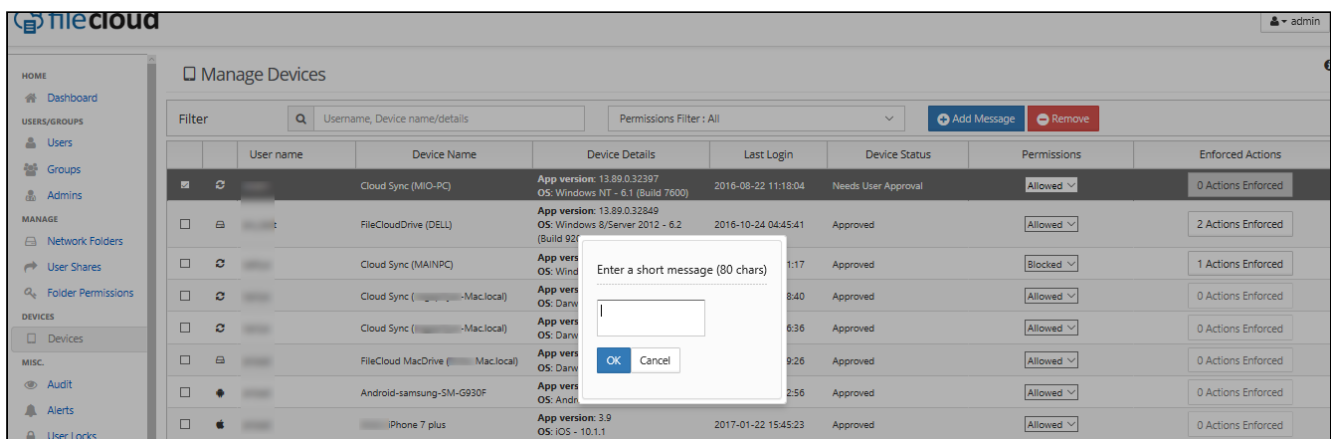
displayed in the order it was entered. The messages will be shown only once per client and during

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 device using the checkbox on the left most column of a device record
3. Click on "**Add Message**" button



iOS Device Management


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

Allow Sync Apps

This switch can be disabled to block all Desktop Sync Apps from connecting to FileCloud. **Default value is "Enabled"**


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.

Pre-Requisites

	Software	Version	Notes
Mobile User	FileCloud iOS app	version 7.0 or later	You can get this from the Apple app store
Administrator	A FileCloud account	18.2 and later	Check with your administrator to make sure they are running the latest version

To enable automatic camera uploads:

1. Open a browser window and log in to the admin portal.
2. From the left navigation menu, select **Settings**.
3. Click the **Endpoint Backup** tab.

4. Select the **Allow Camera Uploads** checkbox.


The screenshot shows the 'Endpoint Backup' settings page. At the top, there is a navigation bar with tabs for 'Server', 'Storage', 'Authentication', 'Admin', 'Email', 'Endpoint Backup' (selected), 'License', 'Policies', 'SSO', and 'Team Folders'. Below the navigation bar, the page title is 'Endpoint Backup Settings'. There are four main settings sections:

- Allow Users To Backup**: A checked checkbox with a blue checkmark. Below it, the text reads: 'Click to enable user to backup files using CloudSync client application.'
- Allow Camera Uploads**: A checked checkbox with a blue checkmark, highlighted by an orange arrow pointing to it from the right. Below it, the text reads: 'Allow automatic backup of photos and videos of mobile devices.'
- Backup Path**: A text input field containing the value '/\$USERNAME/backups/'. Below the field, the text reads: 'Root store path for backups. Can be overridden per user in user details panel. If 'My Files' is disabled, a new path must be specified in user details panel for each of the user'
- Backup Notification Email**: A text input field containing the value 'Backup Email'. Below the field, the text reads: 'Set a valid email address to receive the back up notifications'

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

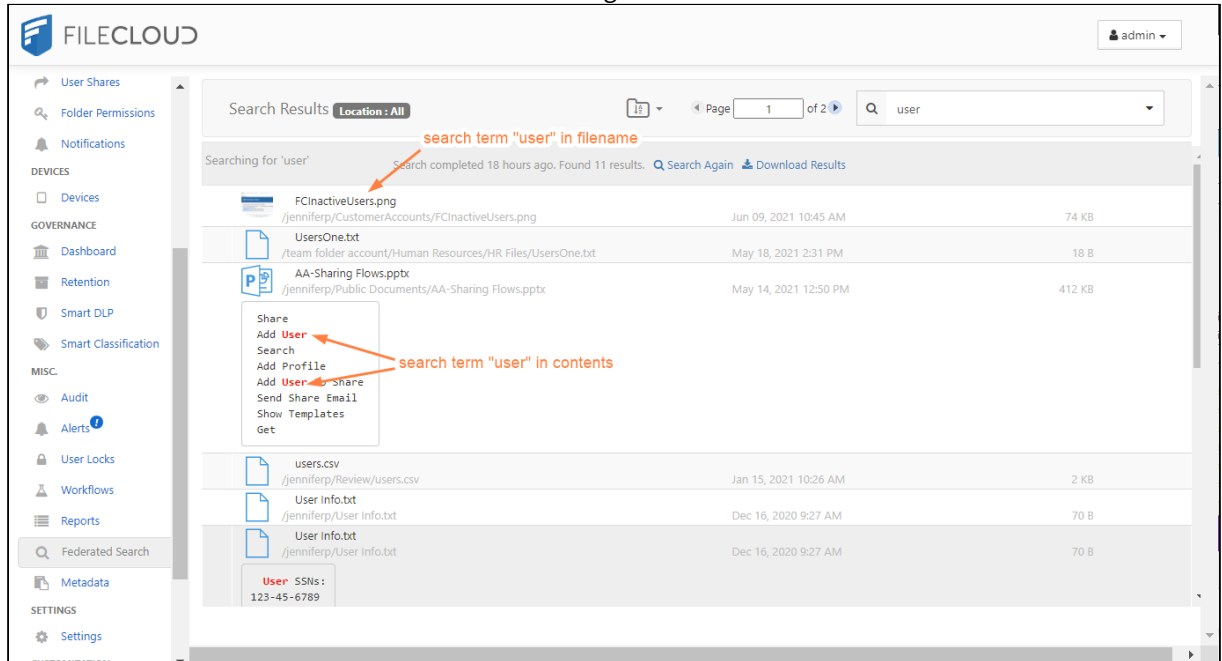
A basic search searches for the search term in file and folder names, and if content search is enabled, in the content of files.

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

To perform a basic search on the entire site:

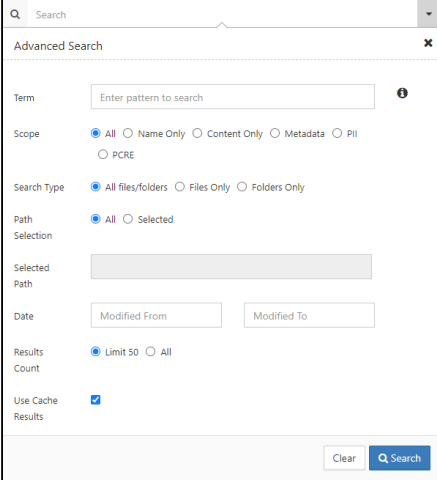
1. From the left navigation panel of the Admin Portal, under **Misc.**, click **Federated Search**.
2. On the search screen, in the search box, type the search term and press enter.
Files and folders with the search term in their names as well as files containing text that contains the search

term are listed as search results. Text in files containing the search terms is shown.



Advanced Searches

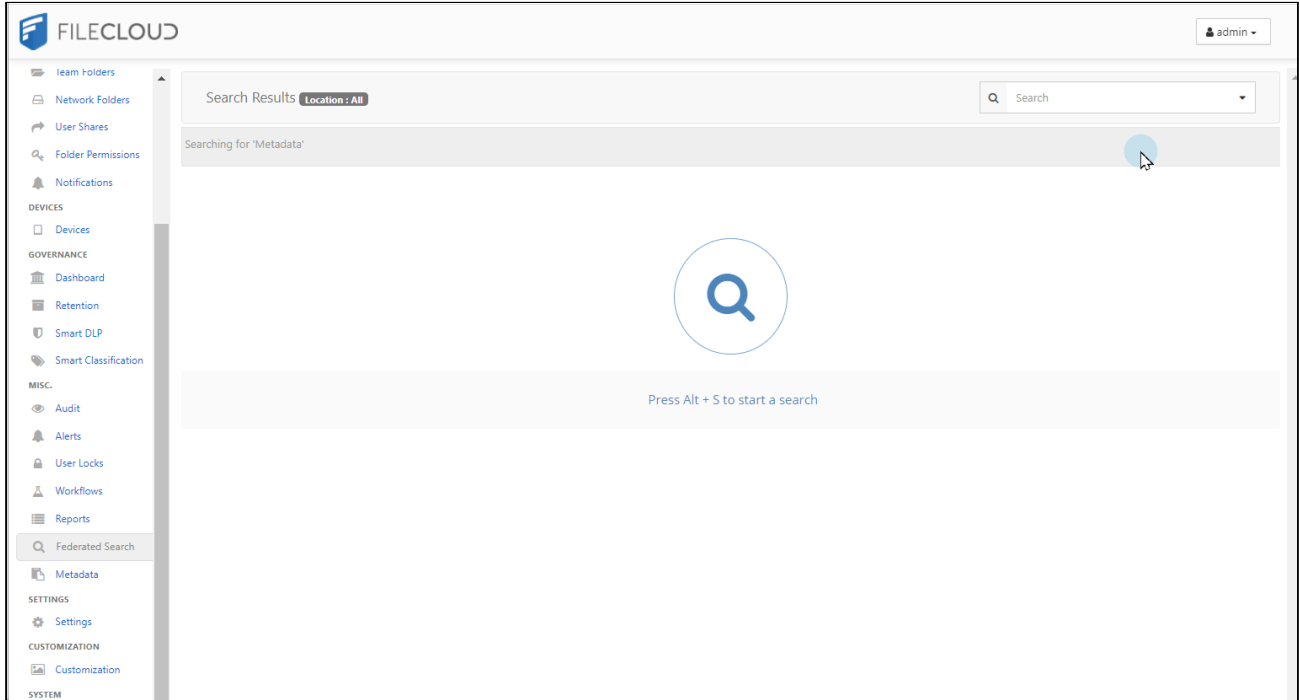
An advanced search lets you search on the search term and any of the options shown and listed below:

Advanced search box	Search options
	<p>Term - (required) The string to search for.</p> <p>Scope - Which content to search.</p> <p>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.</p> <p>Name Only - File and folder names only. See Name only search, below.</p> <p>Content Only - Content in files only. See Content only search, below.</p> <p>Metadata - Content stored in metadata fields only. You must define conditions to search for instead of entering a search term. See Metadata search, below.</p> <p>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.</p> <p>PCRE - Only appears when the PCRE mode setting is enabled. Searches on regular expressions. See PII and PCRE searches, below.</p> <p>Search Type - Options are All files/folders, Files Only, and Folders Only. Not applicable for Metadata search.</p> <p>Path Selection - Either All or Selected. If Selected is chosen, Selected Path is enabled for you to enter a path.</p> <p>Selected Path - When Selected is chosen for Path Selection, this is enabled. Enter the path to search on.</p> <p>Date - Range of Last Modified dates to search on.</p> <p>Results Count - Number of results to return. Choose Limit 50 or All. Use Limit 50 to reduce lengthy search times.</p> <p>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.</p>

All search

All search

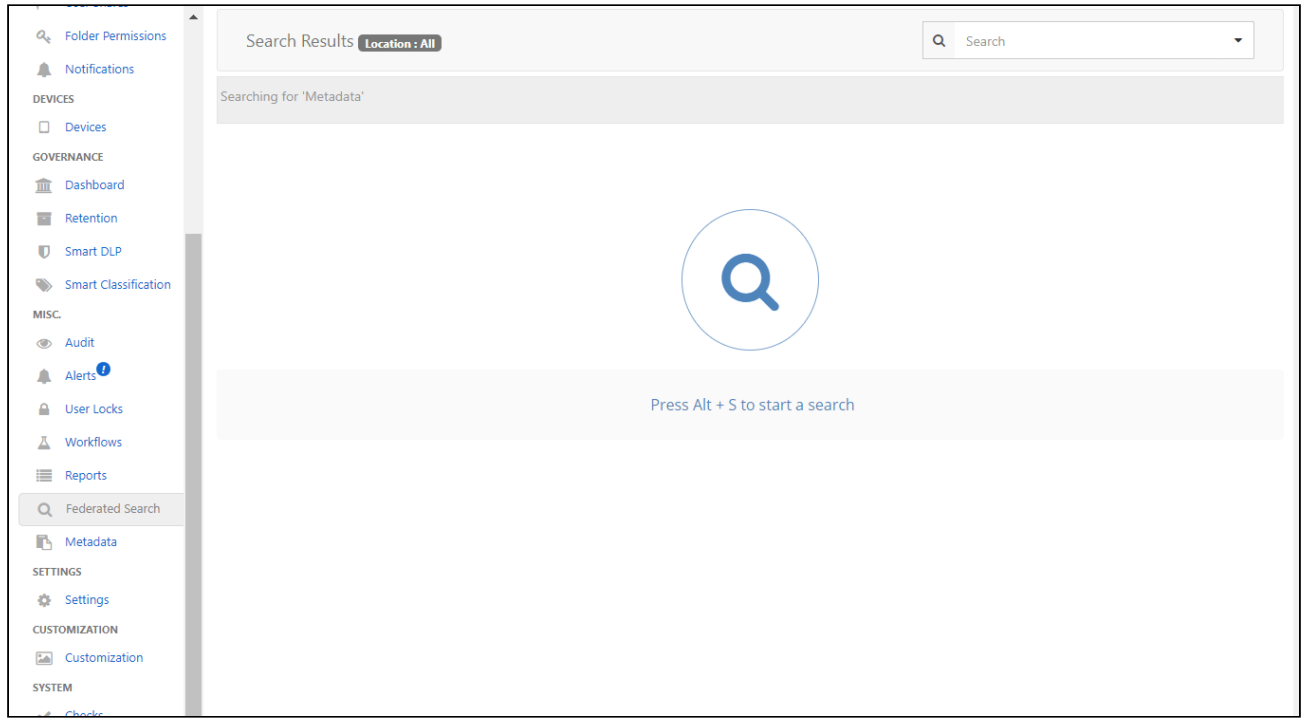
All is selected by default. This search looks for matches in file and folder names when content search is not enabled. It looks for matches in file and folder names and in the content of files when content search is enabled.



Name only search

Name Only search

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



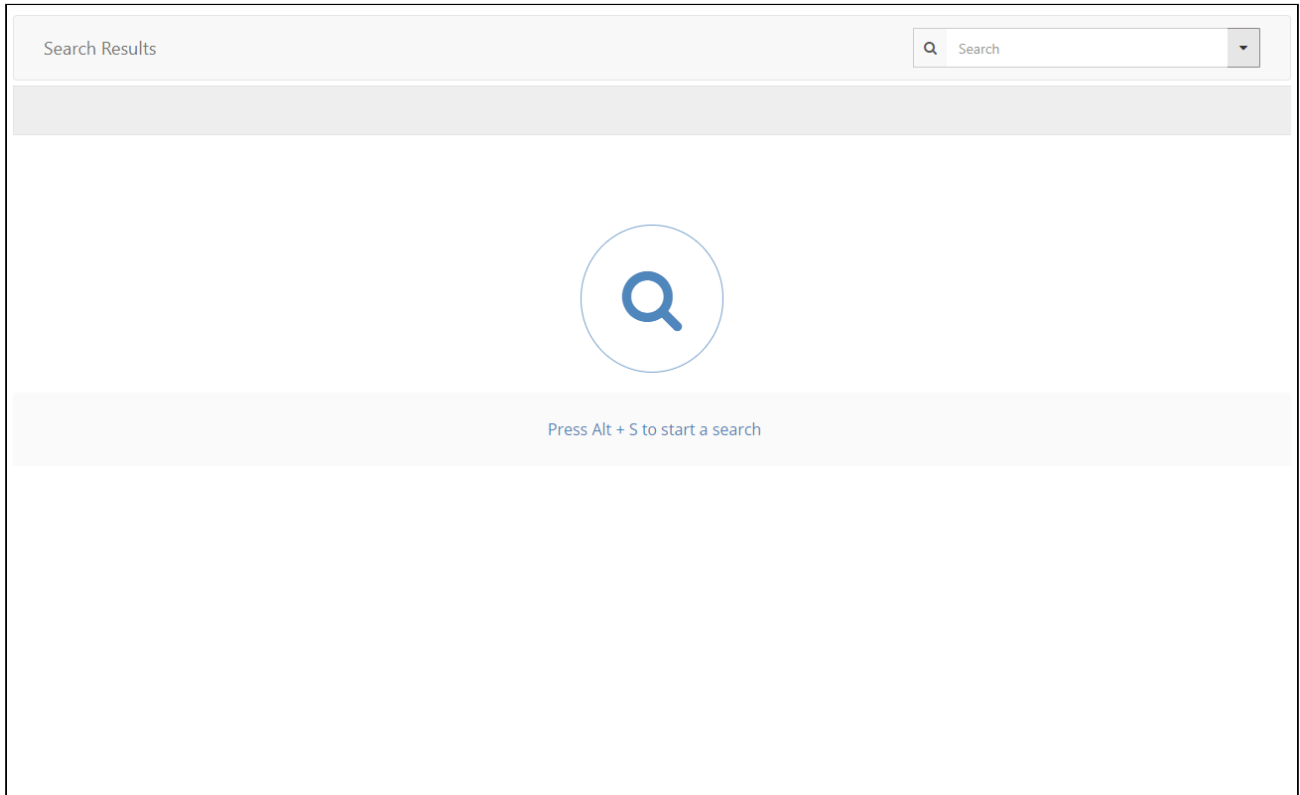
Content only search

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.

i 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.

admin

Search Results **Location: All**

Searching for 'Metadata'



Press Alt + S to start a search

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?

 <p>View Logs</p>	<p>View Audit Logs</p> <p>Filter Audit Log Views</p>
 <p>Manage Logs</p>	<p>Delete Audit Log Entries</p> <p>Configure What is Logged</p> <p>Export Audit Logs</p>

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**.

Filter-options

Search Term: [] 2020-04-01 2020-04-15

Operation Filter : Down User Agent : Drive Show 10 Items

Manage ← Export the log

← Rerun with current filter options → **Refresh**

Log-messages


User name	Message	IP	Agent	Created On
jenniferp	jenniferp downloaded file /jenniferp/New-Community-Edition-Boxes.docx	127.0.0.1	FileCloud Drive	2020-Apr-14 06:12 PM
jenniferp	jenniferp downloaded file /jenniferp/External/Lorem Ipsum.docx	127.0.0.1	FileCloud Drive	2020-Apr-14 06:12 PM
jenniferp	jenniferp downloaded file /jenniferp/PGT Order Form.doc	127.0.0.1	FileCloud Drive	2020-Apr-14 06:12 PM
jenniferp	jenniferp downloaded file /jenniferp/IconEmailLink.jpg	127.0.0.1	FileCloud Drive	2020-Apr-14 01:37 PM
jenniferp	jenniferp downloaded file /jenniferp/DriveSSOLogin.jpg	127.0.0.1	FileCloud Drive	2020-Apr-14 01:37 PM
jenniferp	jenniferp downloaded file /jenniferp/Thumbs.db	127.0.0.1	FileCloud Drive	2020-Apr-14 01:37 PM

At the top of the Audit Log 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.

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, <i>USER1 logged in FAIL</i>
IP address	The IP from which the event occurred
Agent	Indicates how FileCloud was accessed. For example: <ul style="list-style-type: none"> • Web browser • Sync • Drive • Mobile device
Created On	The date and time when the event was logged


Filter Audit Log Views


 The ability to filter the Audit Log list for Metadata and User Agent operations is available in FileCloud version 18.2 and later.




Since every operation is logged and displayed in the Audit screen, the display will show a lot of information and there may be times when you only want to see a specific event.

For example, if you want to see if a specific user was able to login but hundreds of operations are occurring on the server, finding your user may be difficult.

Therefore, you can search or filter your views to find the information you need.

 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?

Searching

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.

Specify 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.

Select 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
common	<p>Displays 6 of the most commonly logged operations:</p> <ul style="list-style-type: none"> • create new account • login • create file or folder • upload file • download file or folder • share file or folder <p>This is the default filter if no other is selected.</p>
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.


 A screenshot of a web interface showing a dropdown menu labeled 'Operation Filter : Common'. The dropdown is currently set to 'Common' and has a downward arrow on the right. To the right of the dropdown is a small grey button with an information icon (i).

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 the action or group of actions for which you want to view the log entries.

Select 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


 A screenshot of a web interface showing a dropdown menu labeled 'User Agent : All'. The dropdown is currently set to 'All' and has a downward arrow on the right. To the right of the dropdown is a small grey button with an information icon (i).

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 which client or device for which you want to see log entries.

Configure What is Logged

There might be some operations that you do not want logged in your Audit logs.

- For example, if a specific WebDAV client sends in hundreds of information requests or login requests it can cause your Audit logs to grow quite large quickly.

Audit Settings

Audit Logging Level REQUEST ▼

Level of Audit Logging

OFF - No Audit Log Recorded

REQUEST - Log all requests and results of request but not the full response

FULL - Log complete request and response.

Auto Archive Audit Database

Enable automatic export and delete of audit records.

NOTE: Cron Job must be set up and running

Auto Archive Audit Records After (in days) 7

Export and delete audit records that are older than (Number of Days)
(Required to auto archive audit db)

NOTE: Files will be exported daily and stored in CSV format. Exported records will be deleted from audit database.

Storage Path For Archived Audit Records Check Path

Specify the location to store exported audit files. This location must be writable by the webserver

To configure what is logged, you can:

Set a logging level

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

- **OFF** - Nothing will be recorded in the Audit log files
- **REQUEST** - This limits the logging to requests from agents or clients and the results of a request. The full response to the agent or client is not recorded.
- **FULL** - This 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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, click *Settings*.
3. On the *Admin* tab, scroll down to the bottom of the page.
4. Under *Audit Settings*, in *Audit Logging Level*, select *OFF*, *REQUEST*, or *FULL*.

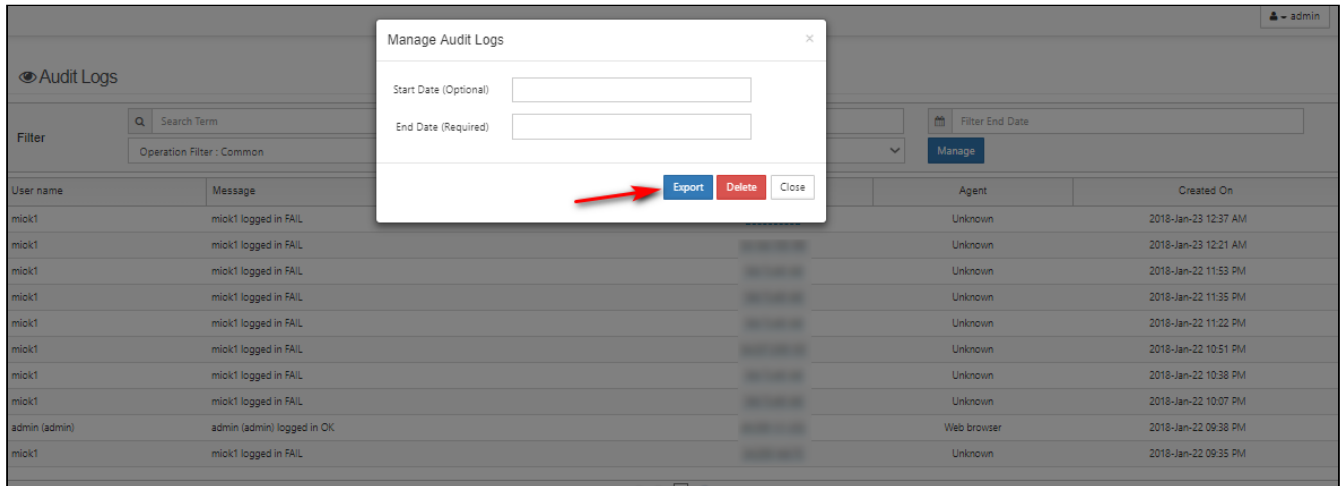
⚠ Remember that the information in audit logs can be extremely important for troubleshooting. Be careful not to exclude too much information from your log files.

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* and *End* date, select a date or type in a date in following format, YYYY-MM-DD.
5. Click **Export**.



Delete Audit Log Entries

i The ability to configure an automatic archival and deletion of audit records in the database is available in FileCloud Server version 11.0 and later.

i Admin Audit Log Deletion

Beginning with version 19.3, admins can now prohibit other admins from deleting audit logs.

If you need to you can remove entries from the log file manually or configure an automatic archival and deletion of log entries.

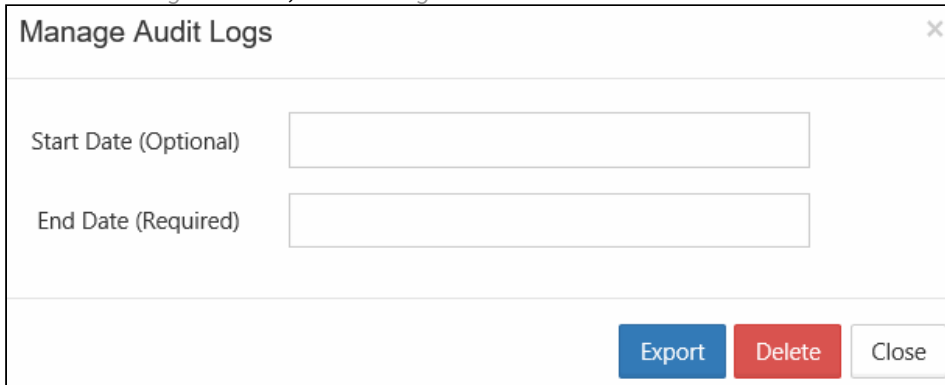
! It is important to keep in mind that removing log entries from the Admin dashboard also removes them from the database. However, MongoDB does not release the space but keeps it for new entries to be added in the future. Some reports, such as reports on file actions and failed logins, get their data 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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation panel, click *Audit*.
3. On the *Audit Logs* window, click *Manage*.



The screenshot shows a dialog box titled "Manage Audit Logs" with a close button (X) in the top right corner. The dialog contains two input fields: "Start Date (Optional)" and "End Date (Required)". At the bottom right, there are three buttons: "Export" (blue), "Delete" (red), and "Close" (white with grey border).

4. 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.
5. In *End Date*, select a date or type in a date in the following format: YYYY-MM-DD.
6. Click *Delete*.
7. 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 number of alerts are shown in the Dashboard and the Alerts page will show detailed information about the various errors encountered.

Depending on the error, you might 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.

To view alerts:

1. Log into the [Administration portal](#).
2. On the left navigation panel, click *Alerts*.

The following view shows errors detected by FileCloud File Content Heuristic Engine.

Date	Severity	Description	ACTIONS
2018-Jan-16 01:02 PM	Warning	Failed Upload for My Files: Disk Usage Size Limit Exceeded for anisad Usage: 2939030675 Limit: 1073741824	i
2018-Jan-16 12:36 PM	Warning	Failed Upload for My Files: Disk Usage Size Limit Exceeded for anisad Usage: 2939030675 Limit: 1073741824	i
2018-Jan-16 12:32 PM	Warning	Failed Upload for My Files: Disk Usage Size Limit Exceeded for anisad Usage: 2935884947 Limit: 1073741824	i
2018-Jan-16 07:32 AM	Warning	Failed Upload for My Files: Disk Usage Size Limit Exceeded for corentin Usage: 56234732 Limit: 2097152	i
2018-Jan-16 07:26 AM	Warning	Failed Upload for My Files: Disk Usage Size Limit Exceeded for corentin Usage: 53089004 Limit: 2097152	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed SMTP Error: The following recipients failed: sat25@s.com: unroutable domain: s.com	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed SMTP Error: The following recipients failed: test@gmail.cz: unroutable domain: gmail.cz	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed SMTP Error: The following recipients failed: trsrts@hdt.ln: <trsrts@hdt.ln>: previously hard-bounced	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed SMTP Error: The following recipients failed: tester@test2.com: unroutable domain: test2.com	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed You must provide at least one recipient email address.	i

Page 1 of 3
21 rows

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.

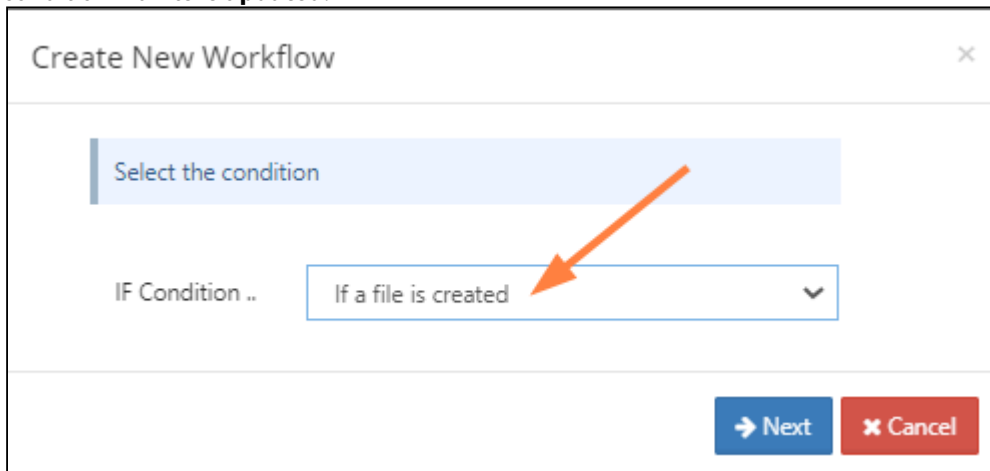
A heuristic engine can help prevent ransomware from entering your system by scanning files for characteristics that are often present in malicious files. FileCloud includes a heuristic engine that looks for files that identify their content inaccurately, a method sometimes used to trick users into opening 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.

Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parent_folder_path_string": "/"
}
```



This condition will be triggered when a file is created.

parent_folder_path_string: path of the folder as shown below

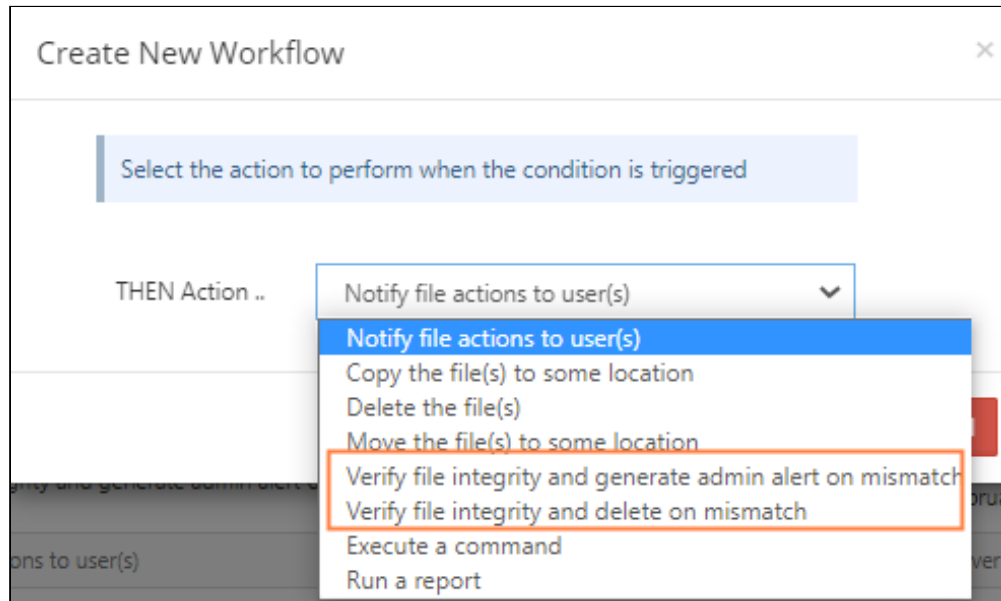
use_regex (optional): specifies whether path has a regex format

exclude (optional): specifying this parameter will result in excluding the supplied path matches

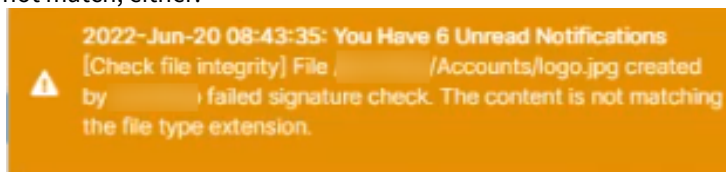
```
{
  "parent_folder_path_string": "/userid/somepath",
  "use_regex": "1",
  "exclude": "1"
}
```

← Previous
→ Next
✕ Cancel

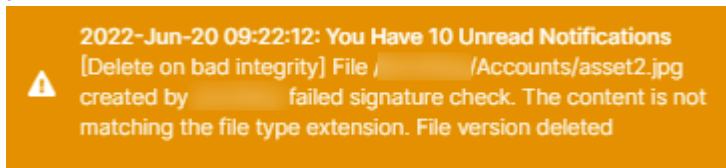
6. Click **Next**.
You are prompted to choose an action.
7. Choose one of the **Verify file integrity** actions depending on what you want the system to do when a mismatch is detected. The possible actions are:
- **Verify file integrity and generate admin alert on mismatch:** Detects the mismatch and 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**.

Create New Workflow ✕

Provide the required parameters for the action to be executed

Required Parameters

```
{  
  "ignore_file_size_in_mb": "10"  
}
```

This action will attempt to identify file type based on its content and check if it matches its extension.

If the file type does not match, generate admin portal alert.

File sizes larger than the specified size will not be scanned.

ignore_file_size_in_mb: Do not scan files larger than this limit specified in MegaBytes

```
{  
  "ignore_file_size_in_mb": "10"  
}
```

← Previous → Next ✕ Cancel

10. Click **Next**.

11. Enter a name for the workflow.

Create New Workflow
✕

Name for this action

Workflow Name

← Previous
→ Finish
✕ Cancel

12. Click **Finish**.

The workflow appears in the list on the Manage Workflows screen.

🔗
Manage Workflows

Workflow
+ Add Workflow

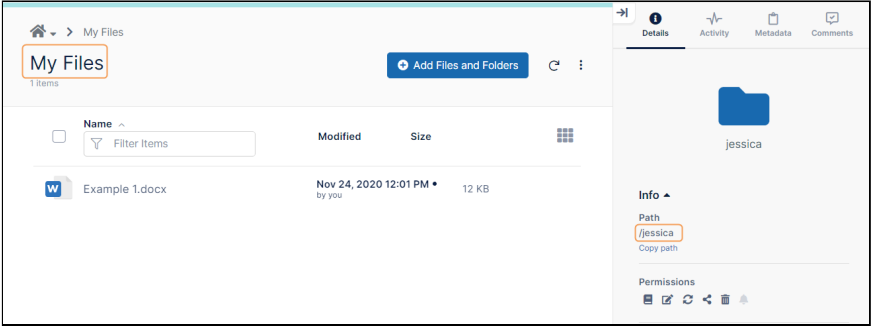
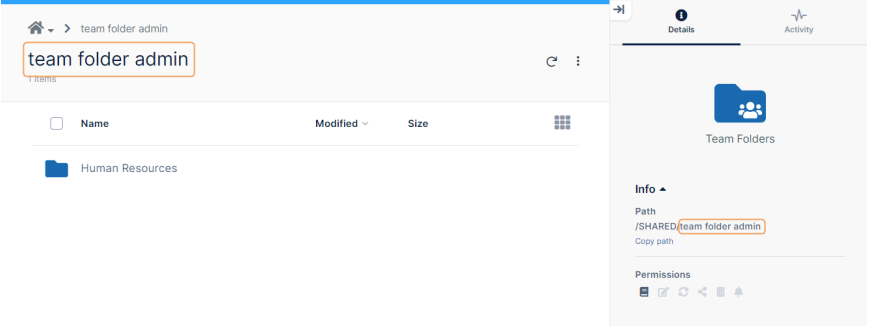
Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
Check file integrity	If a file is created	Verify file integrity and generate admin alert on mismatch	Never	Never	<input checked="" type="checkbox"/>	▶ ⏸ ✎ ↺ ✕
Inactive Files	If file was not modified for specified days	Notify file actions to user(s)	April 25, 2022, 7:21 am	April 25, 2022, 6:50 am	<input type="checkbox"/>	▶ ⏸ ✎ ↺ ✕
Notify on file upload	If a file is added or updated	Notify file actions to user(s)	August 2, 2021, 1:40 pm	July 12, 2021, 1:43 pm	<input type="checkbox"/>	▶ ⏸ ✎ ↺ ✕

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.

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**.

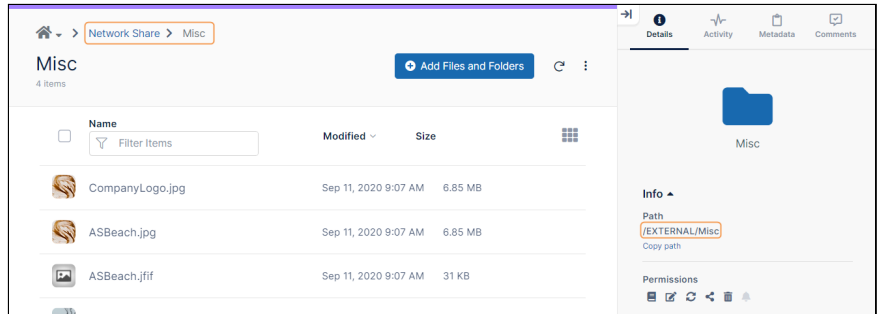
Folder	How to specify path	Example
My Files	/username	<p>In this example, to specify the My Files folder of the user with username jessica, use:</p> <p>/jessica</p> <p>If jessica were logged in, and she selected My Files, she would see the exact path in the Details tab in the right panel.</p> 
Team Folders	/teamfolderaccount	<p>In this example, to specify the Team Folders folder use the name of the account that manages Team Folders:</p> <p>/team folder admin</p> <p>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</p> 

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

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.

The screenshot shows the 'Manage Reports' interface. On the left is a navigation menu with categories: DEVICES (Devices), GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification, Compliance - NEW), MISC. (Audit, Alerts, User Locks, Workflows, Reports - highlighted), Federated Search, Metadata, and SETTINGS (Settings). The main content area is titled 'Manage Reports' and features a search bar with a 'Filter' label and a dropdown menu set to 'ALL'. An 'Add Report' button is in the top right. Below is a table with 9 rows, each representing a report. The table has three columns: Report Name, Query, and Actions. The reports listed are: dlp-2, dlp, OS Report, get effective permission for team folders, Metadata, Creation Date, Login report, File activities, and clients. Each row has three action icons: a blue play button, a blue document icon, and a red 'X' icon. At the bottom, there is a pagination control showing 'Page 1 of 1' and '9 rows'.

Report Name	Query	Actions
dlp-2	Get statistics about DLP violations	[Play] [Document] [X]
dlp	Get statistics about DLP violations	[Play] [Document] [X]
OS Report	Get client applications grouped by OS	[Play] [Document] [X]
get effective permission for team folders	Get the effective permissions for the team folders	[Play] [Document] [X]
Metadata	Get files tagged with metadata report	[Play] [Document] [X]
Creation Date	Get files tagged with metadata report	[Play] [Document] [X]
Login report	Get user login report	[Play] [Document] [X]
File activities	Get all file activities by users	[Play] [Document] [X]
clients	Retrieve client application information	[Play] [Document] [X]

⚠ 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.

Create New Report ✕

Select the report from the list

Select Report to Create

➔ Next ✕ Cancel

The next step is to 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.

Create New Report ✕

Provide the required parameters for the report query in JSON format

Required Parameters

```
{  
  "keyword": "jaredt"  
}
```

Get report of all shares
keyword : (OPTIONAL) Keyword to search in sharename, sharelocation, shareowner, shorturlstring
folderpath : (OPTIONAL) Enter the path to list the shares from path
permissions : (OPTIONAL) If set to '1' a list of effective permissions for each user assigned to the share will be displayed

```
{  
  "keyword": "keywordstring",  
  "folderpath" : "/pathname",  
  "permissions" : "1"  
}
```

← Previous → Next ✕ Cancel

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.

Report Results
✕

☰ user quota report

🔄 Refresh
📄 Download

2 rows.

username	email	file_count	quota_usage_bytes	quota_usage_readable	quota_assigned	quota_usage_percent
john baxter	██████████@██████████.com	186	106862964	101.91 MB	2 GB	4.98
mary higgins	██████████@██████████.com	20	970335	948 KB	2 GB	0.05

Close

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

Report Name	Description
Get client application grouped by OS	<p>Report of total client devices that are connected to FileCloud grouped by client OS.</p> <p>Data Retrieved: client OS type(Windows, Android etc), total devices connected.</p> <p>Parameters: None</p>
Get client apps grouped by TYPE	<p>Report of total client devices that are connected to FileCloud grouped by TYPE.</p> <p>Data Retrieved: Client Type(Sync, Drive etc), total devices connected.</p> <p>Parameters: None</p>
Get all file activities by users	<p>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.</p> <p>Data Retrieved: Timestamp of action, username, file name, action.</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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 <p>This report is available beginning in FileCloud 20.1.</p>
Get file type distribution in managed storage	<p>Report of File types stored in FileCloud along with the total count of each type</p> <p>Data Retrieved: File Type, total files stored.</p> <p>Parameters: None</p>
Get storage usage by file type	<p>Report of amount of storage space used by each file type.</p> <p>Data Retrieved: File type, sizeraw (file size in bytes), size (formatted file size)</p> <p>Parameters: None</p>
Get users who have most files in managed storage	<p>Report of users who have the most files stored under FileCloud in managed storage</p> <p>Data Retrieved: username, total files stored.</p> <p>Parameters: None</p>

Report Name	Description
Get user quota usage report	<p>Report of users who use the maximum quote in FileCloud managed storage</p> <p>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.</p> <p>Parameters: None</p>
Get number of active files in managed storage	<p>Report of total number of files that were changed in the last 1 day, 1 week, 1 month and 6 months</p> <p>Data Retrieved: days, total files changed, percent of files changed.</p> <p>Parameters: None</p>
Get uploaded files report	<p>Report on what files were uploaded during a given period, or files uploaded by a user or group of users during a particular period.</p> <p>Data Retrieved: Timestamp of upload, user name, user agent, IP address, file path, bytes of file uploaded</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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 <i>from_date</i> and <i>to_date</i> 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	<p>Report on what files were downloaded during a given period, or files downloaded by a user or group of users during a particular period.</p> <p>Data Retrieved: Timestamp of download, user name, user agent, IP address, file path, bytes of file downloaded</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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 <i>from_date</i> and <i>to_date</i> 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)

Report Name	Description
Get files tagged with metadata report	<p>Report listing files/folders and their value for a specified metadata field.</p> <p>Data Retrieved: path of folder or file, username, metadata field, value of metadata field</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Report listing shares created.</p> <p>Data Retrieved: Timestamp of download, user name, user agent, IP address, file path, password</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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 <i>from_date</i> and <i>to_date</i> are specified
File query report	<p>Report listing files or folders filtered by specified parameters if included.</p> <p>Data Retrieved: file or folder name, path, type (file or folder), size, last modification date, create date</p> <p>Note: Prior to FileCloud version 21.3, the year for the modification and create dates is returned in 2 digits (for example</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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.

Report Name	Description
File count report	<p>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.</p> <p>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.</p>
Get deleted files report	<p>Report of deleted files.</p> <p>Data Retrieved: Timestamp of delete, user name, user agent, IP address, file path</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Report of the total bandwidth (upload and download) as tracked by this instance of the file cloud server.</p> <p>Data Retrieved: upload bandwidth and download bandwidth</p> <p>Parameters:</p> <ul style="list-style-type: none"> • 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	<p>Report of all folders and sub folders within a given path, showing each file count and total size of the folder</p> <p>Data Retrieved: folder and sub folder path, file count and size</p> <p>Parameters:</p> <ul style="list-style-type: none"> • path: (REQUIRED) Location path. For help specifying the path correctly, see Identifying a FileCloud Specific Path. <p>This report is available in FileCloud version 20.3 and later.</p>
Get all exported secure docs report	<p>Report of all files exported securely.</p> <p>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</p> <p>Parameters: None</p>

Report Name	Description
Get user shares report	<p>Report of all the shares created in FileCloud and their details.</p> <p>Data Retrieved: share name, share owner, share URL, share type, share location, created on, last access, expiry date</p> <p>Parameters:</p> <ul style="list-style-type: none"> 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. <p>The CSV file that is downloaded contains additional information about users and groups that have access to each share.</p> <p>This update is available in FileCloud Server version 18.2 and later.</p>
Get the advanced share activity of users	<p>Report showing extensive details about the activity on a share. If no parameters are entered, the period reported is the last 7 days.</p> <p>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</p> <div data-bbox="721 982 1455 1213" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> 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.</p> </div> <p>Parameters:</p> <p>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</p> <p>This report is available beginning in FileCloud 20.1.</p>
Get files/folders shared with user	<p>Report listing the files and folders shared with a specific user</p> <p>Data Retrieved: share name, share owner, share url, share location, type (private or public), expiry date, creation date</p> <p>Parameter:email of share recipient</p> <p>This report is available beginning in FileCloud 21.1.</p>

Report Name	Description
Get effective permissions for team folders	<p>Report on the permission level of each user who has access to a team folder.</p> <p>Data Retrieved: folder, type (private or public), share location, user, permission</p> <p>Parameters:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>Data Retrieved: IP address, operation, username, user agent, geo area, city, country, create date</p> <p>Parameters:</p> <ul style="list-style-type: none"> 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	<p>Report of all logins to FileCloud and their details. If no parameters are entered, the period reported on is the last 7 days.</p> <p>Data Retrieved: login time, username, useragent, IP</p> <p>Parameters:</p> <ul style="list-style-type: none"> 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. <p>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.</p>
Get number of emails sent, grouped by sender	<p>Report of the number of emails sent in the last X hours</p> <p>Data Retrieved: sender, number of emails sent</p> <p>Parameters:</p> <ul style="list-style-type: none"> hours: number of hours ago to begin retrieving sent email records.

Report Name	Description
Get statistics about DLP violations	<p>Report of DLP violations by rule.</p> <p>Data Retrieved: user, time of violation, user action, rule violated</p> <p>Parameters:</p> <ul style="list-style-type: none"> • rule_name : (OPTIONAL) Name of the rule • minutes : (OPTIONAL) How many minutes ago to begin looking at violations <p>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.</p>
Get a report of active users	<p>Report of active users in the last 15 minutes or for the time defined in minutes</p> <p>Data Retrieved: user name</p> <p>Parameters:</p> <ul style="list-style-type: none"> • minutes : (OPTIONAL) How many minutes ago to consider users as active
Get file movement statistics	<p>Report of last file uploads, downloads, and shares (or share changes)</p> <p>Data Retrieved: number of files downloaded, number of files uploaded, number of files shared and share changes</p> <p>Parameters: None</p>

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

Format	Description	Example/Possible values
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.

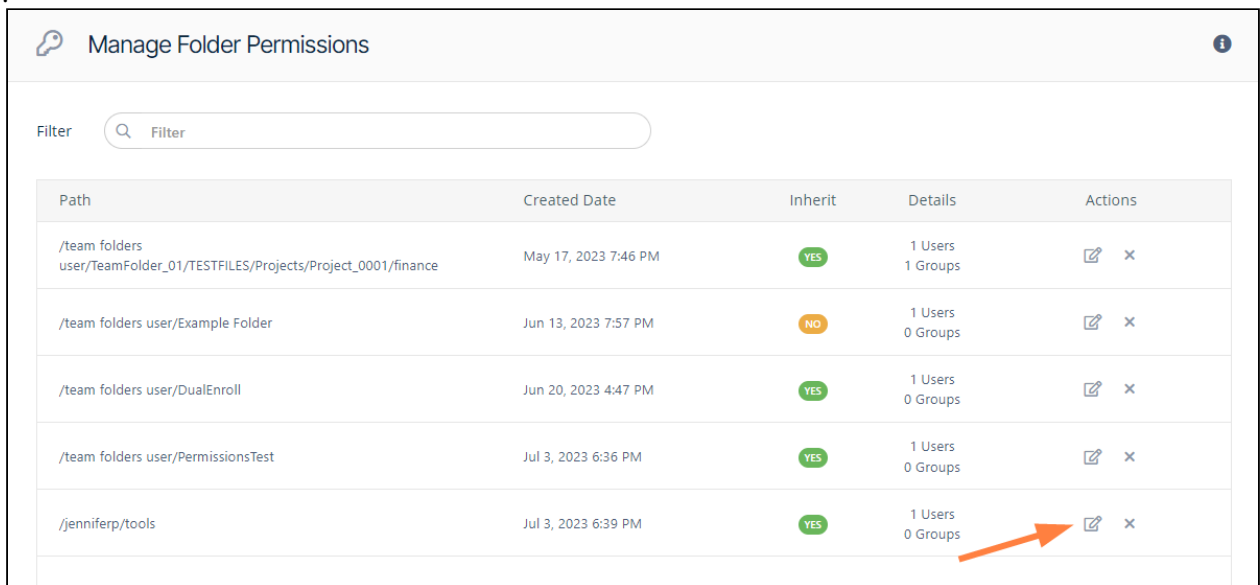
Manage Folder Level Permissions

Starting with FileCloud 14.0, administrators can manage all configured [folder-level permissions](#). In order to view folder-level permissions, the admin must be the master 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 permissions set in the system. Use the **Filter** box to filter folder permissions on the folder path. Individual permissions can then be viewed, edited and deleted.

To Edit Folder Level Security

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



The screenshot shows the 'Manage Folder Permissions' interface. At the top, there is a search bar labeled 'Filter'. Below it is a table with the following columns: Path, Created Date, Inherit, Details, and Actions. The table contains five rows of folder permissions. An orange arrow points to the edit icon (a pencil) in the Actions column of the last row, which corresponds to the path '/jenniferp/tools'.

Path	Created Date	Inherit	Details	Actions
/team folders user/TeamFolder_01/TESTFILES/Projects/Project_0001/finance	May 17, 2023 7:46 PM	YES	1 Users 1 Groups	
/team folders user/Example Folder	Jun 13, 2023 7:57 PM	NO	1 Users 0 Groups	
/team folders user/DualEnroll	Jun 20, 2023 4:47 PM	YES	1 Users 0 Groups	
/team folders user/PermissionsTest	Jul 3, 2023 6:36 PM	YES	1 Users 0 Groups	
/jenniferp/tools	Jul 3, 2023 6:39 PM	YES	1 Users 0 Groups	

2. To open the **Manage Folder Level Security** dialog box, click the edit button.

Manage Folder Level Security ✕

Folder: /jenniferp/tools

Security
Check Access

Permissions

Inherit Parent Folder Security: Inherit Don't Inherit

User

Group

Add User

User	Read	Write	Delete	Share	Manage
jm2344311@gmail.com	✓	✓	✓	✓	✓

⏪ ⏩ Page of 1 ⏪ ⏩

Inherited Permissions

User	Read	Write	Delete	Share	Manage
No entries					

✕ Close

1 By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from a parent folder that they have access to, and the lower **Inherited Permissions** section no longer appears. For more information about inherited permissions, see [Enable Folder Level Permissions](#).

2 Click **Add User** to add a user who has permission to access the file.

3 In the top list of users, check or uncheck levels of permissions. Click the delete button to completely remove the user's permissions to the folder. You cannot change the permissions or delete users with inherited 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.

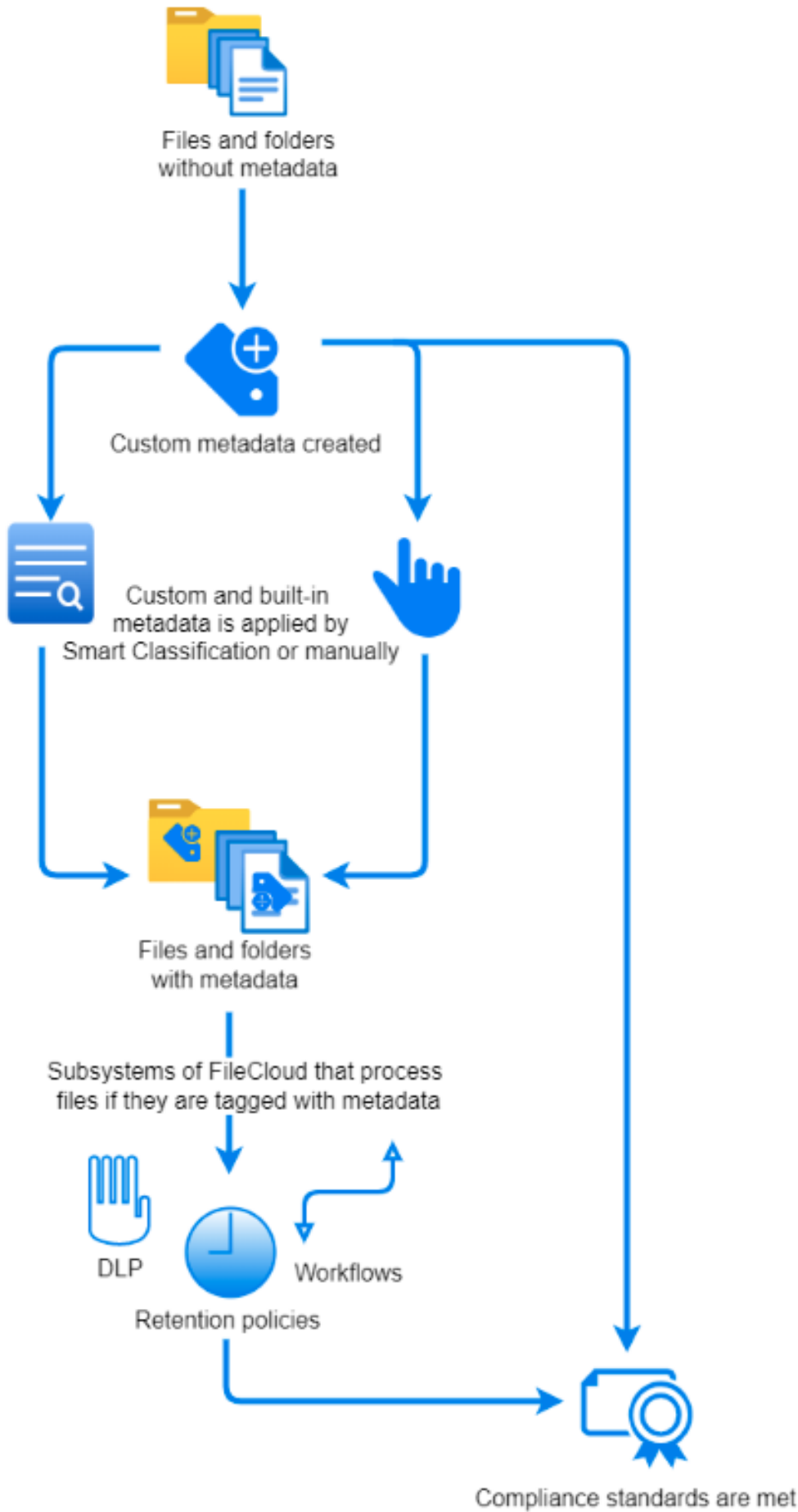
Metadata for governance and other system processes

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.



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**.

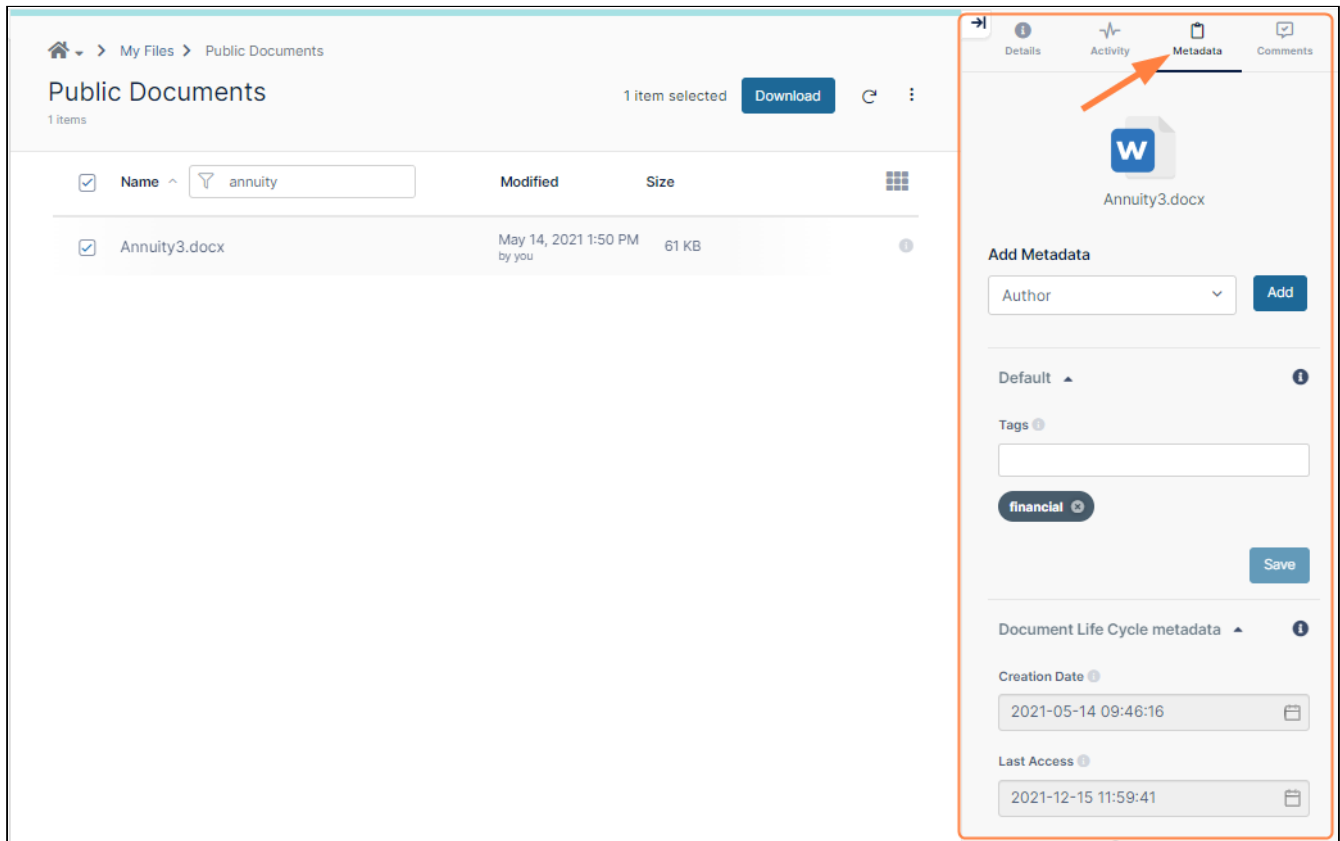
Here are some examples of the way compliance rules are met by metadata:

- 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](#)
- [Create a New Metadata Set](#)
- [Edit an Existing Metadata Set](#)
- [Managing Metadata Attributes](#)
- [Managing Metadata Permissions](#)
- [Video of Managing Metadata](#)
- [Working with Built-In Metadata](#)
- [Working with Custom Metadata](#)
- [Working with Default Metadata](#)
- [Metadata Limitations/Recommendations](#)






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

 <p>File Object</p>	 <p>Metadata</p>	 <p>Attribute</p>	 <p>Metadata Set</p>	 <p>Tag</p>
<p>Every file and folder that exists in FileCloud.</p>	<p>Information about the file data. Describes files and folders available in the system.</p>	<p>A single piece of information that describes the File Object. In FileCloud attributes are defined as a part of the metadata set.</p>	<p>A set of metadata attributes that might be logically grouped and can be attached as a single entity to File Objects.</p>	<p>a special type of attribute (referred to as the Array attribute type) that allows users to provide multiple custom values for each File Object.</p>
<p>For example:</p> <ul style="list-style-type: none"> • a resume 	<p>For example:</p> <ul style="list-style-type: none"> • Lives in the Human Resources Folder • Has a created date • Has a modified date 	<p>For example:</p> <ul style="list-style-type: none"> • the candidate's photo in their resume 	<p>For example, resumes will always have:</p> <ul style="list-style-type: none"> • Photo • Name • Address • Experience • Education 	<p>For example:</p> <p>HR wants to tag a resume status as:</p> <ul style="list-style-type: none"> • Candidate • New Hire • OnBoarding

Metadata Set Types

FileCloud supports the following types of Metadata Sets:

TYPE	DESCRIPTION	SETS AVAILABLE
Default	<p>This a special type of metadata set that is automatically associated with every single File Object when it is created, copied, uploaded, etc.</p> <ul style="list-style-type: none">• 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.	Defaults

TYPE	DESCRIPTION	SETS AVAILABLE														
<p>Built-In</p>	<p>These are metadata sets that have been created for you.</p> <ul style="list-style-type: none"> Administrators can edit the attributes Administrators can choose to disable the use of this metadata <p>When did each built-in metadata set become available?</p> <p>The versions of FileCloud in which each built-in metadata set and its attributes became available are listed in the following table:</p> <table border="1" data-bbox="555 781 1068 1415"> <thead> <tr> <th>Built-in Metadata Set</th> <th>FileCloud Version</th> </tr> </thead> <tbody> <tr> <td>Image</td> <td>18.1</td> </tr> <tr> <td>Document Life Cycles</td> <td>18.1</td> </tr> <tr> <td>Microsoft Office Tag</td> <td>20.1</td> </tr> <tr> <td>Color Tagging</td> <td>20.3</td> </tr> <tr> <td>PDF Tag</td> <td>21.2</td> </tr> <tr> <td>AIP Sensitivity Label</td> <td>21.2</td> </tr> </tbody> </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	<ul style="list-style-type: none"> Image metadata Document Life Cycle metadata Microsoft Office Tag metadata Color Tag metadata PDF Tag metadata AIP Sensitivity Label metadata
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															
<p>Custom Metadata Set</p>	<p>This is a fully customizable set of metadata, defined by the administrator.</p>	<p>As many as you want to create</p>														

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 Videos	FileCloud Blogs
	<ul style="list-style-type: none"><li data-bbox="1029 472 1333 541">• 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**.

The screenshot displays the 'Manage Metadata Sets' page in FileCloud. The left-hand navigation menu is expanded to show 'Metadata' as the selected option. The main content area features a search filter and a table listing various metadata sets. Each set includes a description, its status (all are 'Enabled'), its type (either 'Default' or 'Built-in'), and the number of users and groups associated with it. Action icons for editing and deleting are provided for each set. A blue button labeled 'Add Metadata Set' is located in the top right corner of the main area, and a user profile dropdown for 'jenniferperkins' is visible in the top right corner of the page header.

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	0	0	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	0	1	
AIP Sensitivity Label metadata	AIP Sensitivity Label metadata set	Enabled	Built-in	0	1	
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	0	1	

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

Add Metadata Set Definition
✕

Metadata Set

Name*

Description*

Disabled

Permissions

Users **Groups** Paths

Add Group

Name	Read Permission	Write Permission
HR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Page 1 of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	text	User's job title	Enabled	<input type="checkbox"/> <input style="background-color: #dc3545; color: white; padding: 2px 5px;" type="button" value="✕"/>
Type	text	Full time or part time job	Enabled	<input type="checkbox"/> <input style="background-color: #dc3545; color: white; padding: 2px 5px;" type="button" value="✕"/>

- Enter **Name** and **Description** and check **Disabled** if you don't want the metadata set to be enabled when you save it.
- 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](#).
- Click **Add Attribute** and add at least one metadata attribute definition. For more details, see [Create a New Metadata Set](#).

Metadata permissions

Although user / group permission widgets look very similar to share widgets, their behavior is different. Read / write permission changes for each user / group are not saved when the change happens (this is the process for shares). All changes are saved at the same time when **Create** is clicked.

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.
- Although user/group permission widgets look very similar to share widgets their behavior is different. Read/write permission change for each user/group is not saved when the change happens (this is the process for shares). All changes are saved at the same time - when the "Save" button is clicked.
- 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. On the Manage Metadata Sets screen, find the set you want to edit.
4. In the row of the set you want to edit, under ACTIONS, click the edit button ().

Manage Metadata Sets

[+ Add Metadata Set](#)

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	ACTIONS
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	0	1	 
Invoicing	Additional information about invoices	Enabled	Custom	0	2	 
Assets	Metadata set with media campaign information	Enabled	Custom	0	2	 

Page 1 of 1
3 rows



The Edit Metadata Set Widget will appear where set definition can be edited.

Edit Metadata Set Definition ✕

Metadata Set

Name

Description

Disabled

Permissions

Users **Groups** Paths

[Add Group](#)

Name	Read Permission	Write Permission
EVERYONE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>	<input type="checkbox"/>

⏪ ⏩ Page 1 of 1 ⏪ ⏩

Attributes

[+ Add Attribute](#)

Name	Attribute Type	Description	Status	ACTIONS
Category	Array	Asset category	Enabled	<input type="text"/> ✕
Banner Resolution	Enumeration	Resolution of the banner	Enabled	<input type="text"/> ✕
Active	Boolean	Specifies whether asset is active	Enabled	<input type="text"/> ✕
Image type	Enumeration	Type of the image	Enabled	<input type="text"/> ✕
Subsystem	Enumeration		Enabled	<input type="text"/> ✕

Save
Close

Administrator can edit set properties, [permissions](#) and [attributes](#). Once edited click "Save" button to store changes. When there are some pending changes and admin is about to close the edit dialog following confirm prompt will appear.

Edit Metadata Set Definition
✕

Metadata Set

Name

Description

Disabled

Permissions

Users
Groups
Paths

Add User

Name	Read Permission	Write Permission
assets_manager	<input checked="" type="checkbox"/>	<input type="checkbox"/>

⏪ ⏩ Page 1 of 1 ⏪ ⏩

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	ACTIONS
Category	Array	Asset category	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Banner Resolution	Enumeration	Resolution of the banner	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Active	Boolean	Specifies whether asset is active	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Image type	Enumeration	Type of the image	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Subsystem	Enumeration		Enabled	<input type="text"/> <input style="color: red;" type="text"/>

Save

Close

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



Administrators can manage metadata tags in FileCloud Server.

Edit Metadata Set Definition
✕

Metadata Set

Name

Description

Disabled

Permissions

Users
Groups
Paths

Add User

Name	Read Permission	Write Permission

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	ACTIONS
Status	Enumeration	Current invoice status	Enabled	✎ ✖
Net Value	Decimal	Net value of the invoice	Enabled	✎ ✖
Sales Tax	Enumeration	Local sales tax applicable	Enabled	✎ ✖
Total	Decimal	Total amount on the invoice	Enabled	✎ ✖
Payment method	Enumeration		Enabled	✎ ✖
Payment Due By	Date	Payment date of the invoice	Enabled	✎ ✖
Paid	Boolean	Marks whether invoice was paid	Enabled	✎ ✖
Test	Decimal		Enabled	✎ ✖

Save

Close

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.

i 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 Metadata permissions allowed paths. This affects File Objects based on their location.

Edit Metadata Set Definition ✕

Metadata Set	Permissions		
<p>Name</p> <input type="text" value="Assets"/>	<p>Users Groups Paths</p> <p><input type="radio"/> Allow All <input checked="" type="radio"/> Allow Selected Paths</p> <p>Add Allowed Path</p> <table border="1"><thead><tr><th>Path</th><th>Actions</th></tr></thead><tbody></tbody></table>	Path	Actions
Path	Actions		

Video of Granting a User Metadata Permissions



Administrators can grant user permission to access metadata fields for tagging their files.

Edit Metadata Set Definition
✕

Metadata Set

Name

Description

Disabled

Permissions

Users
Groups
Paths

Add User

Name	Read Permission	Write Permission

Attributes

+ Add Attribute

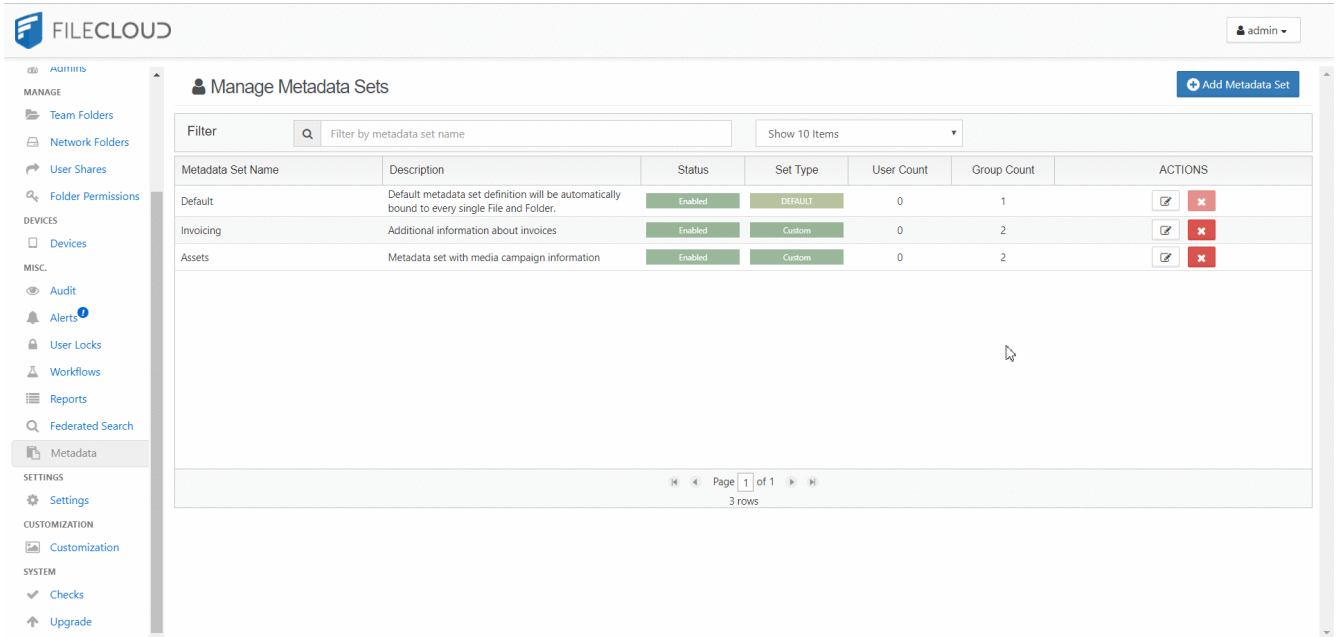
Name	Attribute Type	Description	Status	ACTIONS
Category	Array	Asset category	Enabled	<input type="text" value="edit"/> <input style="background-color: #d9534f; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>
Banner Resolution	Enumeration	Resolution of the banner	Enabled	<input type="text" value="edit"/> <input style="background-color: #d9534f; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>
Active	Boolean	Specifies whether asset is active	Enabled	<input type="text" value="edit"/> <input style="background-color: #d9534f; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>
Image type	Enumeration	Type of the image	Enabled	<input type="text" value="edit"/> <input style="background-color: #d9534f; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>
Subsystem	Enumeration		Enabled	<input type="text" value="edit"/> <input style="background-color: #d9534f; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>

Save
Close

Video of Managing Metadata

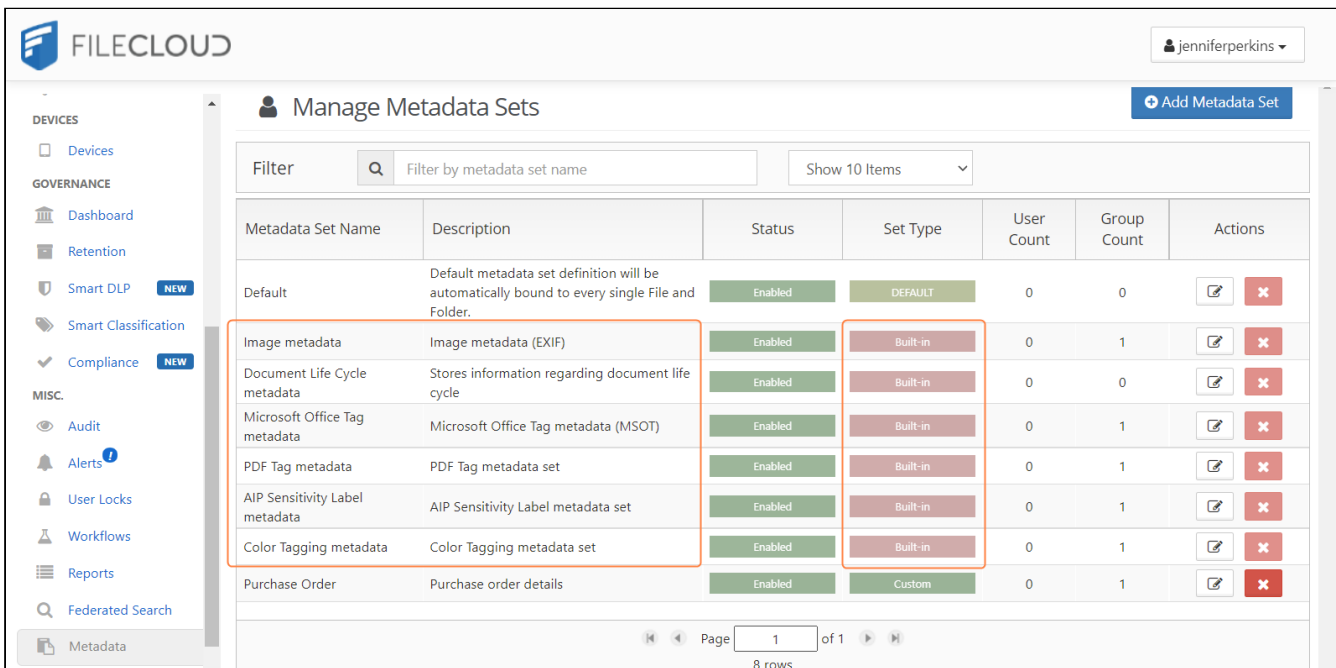


Administrators can manage data that provides additional information about files and folders available in FileCloud using **Metadata**.



Working 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

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.

Edit Metadata Set Definition ✕

Metadata Set

Name
Image metadata

Description
Image metadata (EXIF)

Disabled

Permissions

Users Groups Paths

[Add User](#)

Name	Read Permission
	<input checked="" type="checkbox"/>

Page 1 of 1

Attributes

[Add Attribute](#)

Name	Attribute Type	Description	Status	Actions
Width	Integer	Image Width in Pixels	Enabled	✎ ✖
Height	Integer	Image Height in Pixels	Enabled	✎ ✖
Image Orientation	Enumeration	Image orientation	Enabled	✎ ✖
Image Orientation - Numeric	Integer	Image orientation as a number (8 different orientations)	Enabled	✎ ✖
Image XResolution	Text	Image Resolution in width direction	Enabled	✎ ✖
Image YResolution	Text	Image Resolution in height direction	Enabled	✎ ✖
Unit of Resolution	Enumeration	Unit of resolution	Enabled	✎ ✖

The following attributes exist in the Image BUILT-IN metadata set:

	Description	Options
Name	Title for the metadata set: Image metadata	<ul style="list-style-type: none"> • Required • This cannot be changed
Description	By default, says: Image metadata (Exif)	<ul style="list-style-type: none"> • Required • This cannot be changed

	Description	Options
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	<ul style="list-style-type: none"> • Not selected • This cannot be changed
User Permissions	Grant access to specific users to: <ul style="list-style-type: none"> • Read: this permission displays the metadata to the user in the User Portal <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> • Not Required • Read
Group Permissions	Grant access to specific groups to: <ul style="list-style-type: none"> • Read: this permission displays the metadata to the user in the User Portal <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> • Not Required • Read
Path Permissions	File Objects in this location will have the metadata set applied	<ul style="list-style-type: none"> • Not available • This cannot be changed
Attributes	A number of tags that are built-in for image files	<ul style="list-style-type: none"> • 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.

Edit Metadata Set Definition ✕

Metadata Set

Name
Document Life Cycle metadata

Description
Stores information regarding document life cycle

Disabled

Permissions

Users | Groups | Paths

[Add User](#)

Name	Read Permission
...	<input checked="" type="checkbox"/>

Page 1 of 1

Attributes

[Add Attribute](#)

Name	Attribute Type	Description	Status	Actions
Creation Date	Date	File/Folder creation date	Enabled	✎ ✖
Last Access	Date	Last access date	Enabled	✎ ✖
Last Modification	Date	Last modification date	Enabled	✎ ✖
Check Sum	Text	File SHA256 fingerprint	Enabled	✎ ✖


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

	Description	Options
Name	Title for the metadata set: Document Life Cycle Metadata	<ul style="list-style-type: none"> • Required • This cannot be changed
Description	By default, says: Stores information regarding document life cycle	<ul style="list-style-type: none"> • Required • This cannot be changed

	Description	Options
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	<ul style="list-style-type: none"> • Not selected • This cannot be changed
User Permissions	Grant access to specific users to: <ul style="list-style-type: none"> • Read: this permission displays the metadata to the user in the User Portal <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> • Not Required • Read
Group Permissions	Grant access to specific groups to: <ul style="list-style-type: none"> • Read: this permission displays the metadata to the user in the User Portal <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> • Not Required • Read
Path Permissions	File Objects in this location will have the metadata set applied	<ul style="list-style-type: none"> • 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). <ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Creation Date • Last Access • Last Modification • Check Sum: File SHA256 Fingerprint

Microsoft Office 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.

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

Edit Metadata Set Definition ✕

Metadata Set

Name*
Microsoft Office Tag metadata

Description*
Microsoft Office Tag metadata (MSOT)

Disabled

Permissions

Users Groups Paths

Add User

Name	Read Permission
jenniferp	<input checked="" type="checkbox"/>

Page 1 of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	A name given to the resource	Enabled	✎ ✖
Subject	Text	The topic of the resource	Enabled	✎ ✖
Creator	Text	A person, company, or other entity responsible for making the resource	Enabled	✎ ✖
Keywords	Array	Important words or phrases related to the resource	Enabled	✎ ✖
Description	Text	A textual representation or account of the resource	Enabled	✎ ✖
Last Modified By	Text	The person, company, or other entity responsible for making the most recent change to the resource	Enabled	✎ ✖
Created	Date	Date of creation of the resource	Enabled	✎ ✖

Save Close

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

	Description	Options
Title	Name of file.	<ul style="list-style-type: none"> Not required Read (can only be changed in Microsoft Office file before uploading)

	Description	Options
Subject	Topic of file.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Creator	User who created file.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Keywords	Keyword tags assigned to file.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Description	Description of file.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Last Modified By	Last user who modified file.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Created	Date file was created.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Modified	Date file was last modified.	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading)
Category	Category of file.	<ul style="list-style-type: none"> • 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 .	<ul style="list-style-type: none"> • Not required • Read (can only be changed in Microsoft Office file before uploading) <p>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.</p>



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:

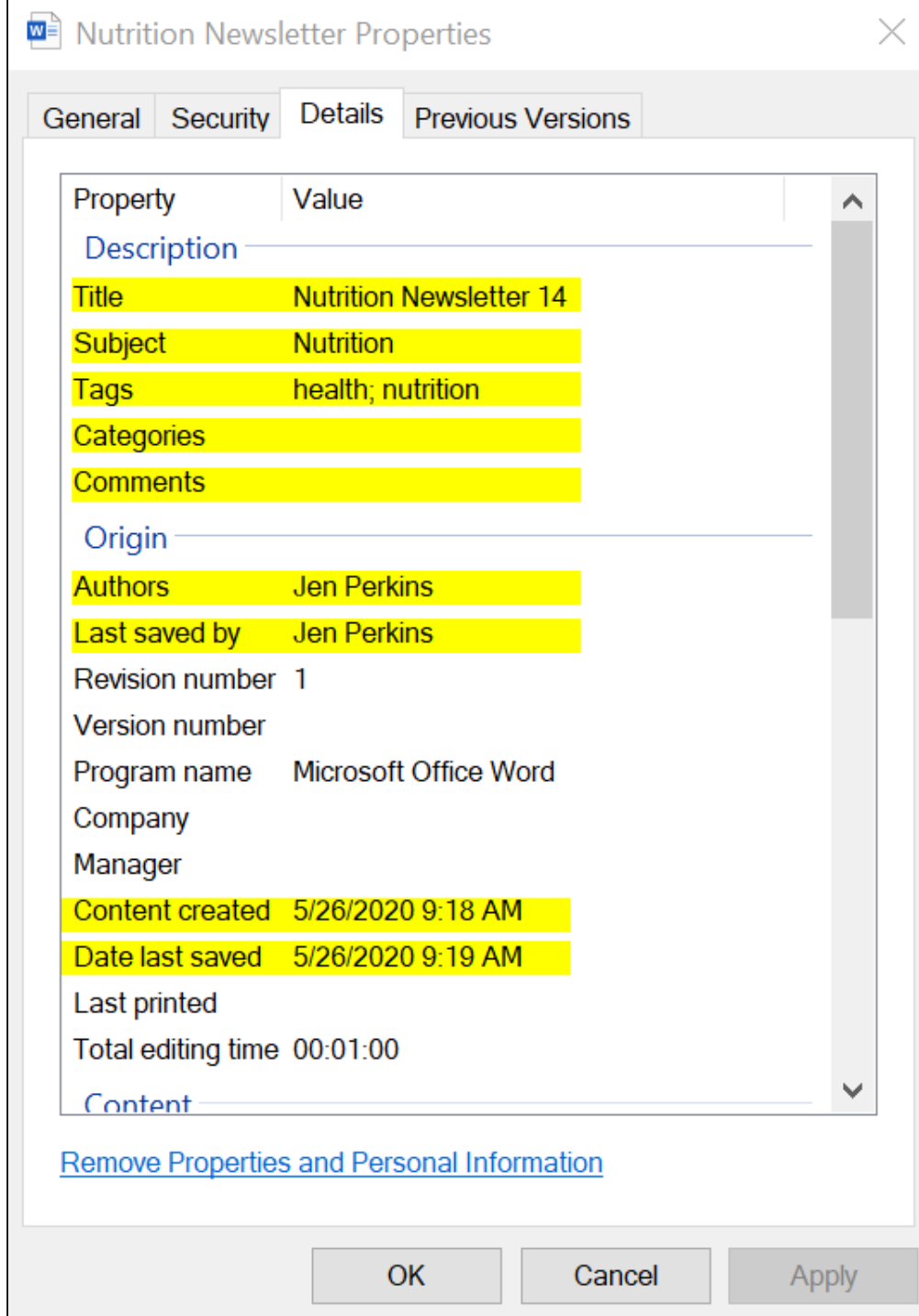
The screenshot shows the Microsoft Word ribbon with several document management options on the left and a Properties pane on the right.

- Protect Document:** Control what types of changes people can make to this document.
- Inspect Document:** Before publishing this file, be aware that it contains:
 - Document properties and author's name
- Version History:** View and restore previous versions.
- Manage Document:** There are no unsaved changes.
- Slow and Disabled COM Add-ins:** Manage COM add-ins that are affecting your Word experience.

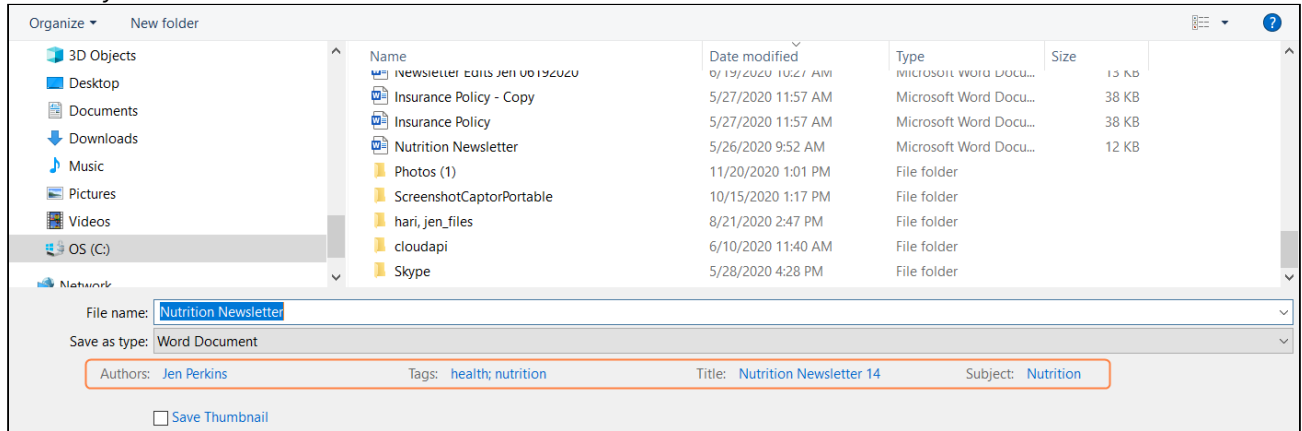
The **Properties** pane on the right displays the following information:

- Size:** 11.5KB
- Pages:** 1
- Words:** 7
- Total Editing Time:** 2 Minutes
- Title:** Nutrition Newsletter 14
- Tags:** health; nutrition
- Comments:** Newsletter sent to all members
- Related Dates:**
 - Last Modified:** Today, 9:19 AM
 - Created:** Today, 9:18 AM
 - Last Printed
- Related People:**
 - Author:** JP Jen Perkins
 - Add an author
 - Last Modified By:** JP Jen Perkins

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.

Edit Metadata Set Definition
✕

Metadata Set

Name*

Description*

Disabled

Permissions

Users
Groups
Paths

Add User

Name	Read Permission	Write Permission

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	Actions
Color	Key Value Pair	Color	Enabled	✎ ✕

Save
Close

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	<ul style="list-style-type: none"> 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.

The screenshot shows the 'Edit Attribute' dialog box for the 'Color' attribute. The 'Name' field is 'Color', and the 'Description' field is also 'Color'. The 'Attribute Type' is set to 'Key Value Pair'. The 'Predefined Values' field contains a list of color entries: Red:#FF0000, Yellow:#FF9900, Green:#18C600, Aqua:#00B4C9, Blue:#0054C9, Purple:#7E00C9, and Orange:#FE9A2E. An orange arrow points to the 'Orange:#FE9A2E' entry. The 'Disabled' and 'Required' checkboxes are unchecked. The 'Default Value' field is 'Tag input'. The dialog has 'Save' and 'Close' buttons at the bottom right.

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.

i 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.

Edit Metadata Set Definition
✕

Metadata Set

Name*

Description*

Disabled

Permissions

Users
Groups
Paths

Add User

Name	Read Permission
jenniferp	<input checked="" type="checkbox"/>

⏪ Page of 1 ⏩

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	Title of document	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Author	Text	Person who created the document	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Subject	Text	Subject of the document	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Keywords	Array	Keywords associated with the document	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Creator	Text	If the document was converted to PDF from another format, the application that created the original document	Enabled	<input type="text"/> <input style="color: red;" type="text"/>
Producer	Text	If the document was converted to PDF from another format, the application that converted it to PDF	Enabled	<input type="text"/> <input style="color: red;" type="text"/>

Save
Close

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.

Edit Metadata Set Definition ✕

Metadata Set

Name*

Description*

Disabled

Permissions

Users Groups Paths

[Add User](#)

Name	Read Permission
jenniferp	<input checked="" type="checkbox"/>

Page of 1

Attributes

[Add Attribute](#)

Name	Attribute Type	Description	Status	Actions
Enabled	Boolean	This attribute indicates whether the classification represented by this set of key-value pairs is enabled for the data item.	Enabled	✎ ✕
Siteld	Text	Azure Active Directory Tenant ID	Enabled	✎ ✕
Method	Text	Standard implies that the label is applied by default or automatically. Privileged implies that the label was manually selected.	Enabled	✎ ✕
SetDate	Date	The timestamp when the label was set.	Enabled	✎ ✕
Name	Text	Label unique name within the tenant. It doesn't necessarily correspond to display name.	Enabled	✎ ✕
ContentBits	Integer	Bitmask that describes the types of content marking	Enabled	✎ ✕


[Save](#) [Close](#)

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

	Description	Options
SitelD	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




Working with Custom Metadata

 Metadata functionality is available in FileCloud 18.1 and later.

Administrators can manage data that provides additional information about files and folders available in FileCloud using **Metadata**.

FileCloud allows you to create a fully customizable set 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

⚠ Default Metadata Set cannot be removed.

⚠ You cannot undo or revert this deletion.

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.

The screenshot shows the 'Manage Metadata Sets' interface. The table contains the following data:

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	ACTIONS
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	0	1	[Edit] [Delete]
Invoicing	Additional information about invoices	Enabled	Custom	0	1	[Edit] [Delete]
Assets	Metadata set with media campaign information	Enabled	Custom	0	2	[Edit] [Delete]

The left sidebar menu includes: HOME (Dashboard), USERS/GROUPS (Users, Groups, Admins), MANAGE (Team Folders, Network Folders, User Shares, Folder Permissions), DEVICES (Devices), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, **Metadata**), and SETTINGS.

Working with Default Metadata



DEFAULT is 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 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.

Manage Metadata Sets + Add Metadata Set						
Filter		Show 10 Items				
Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
Defaults	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	0	0	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	1	1	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	1	1	
Date	dfsdfs	Enabled	Custom	3	0	

The DEFAULT metadata set can be disabled but it cannot be deleted.

The following attributes can be edited in the DEFAULT metadata set:

Edit Metadata Set Definition ✕

Metadata Set

Name

Description

Disabled

Permissions

Users
Groups
Paths

[Add User](#)

Name	Read Permission	Write Permission

Attributes

[+ Add Attribute](#)

Name	Attribute Type	Description	Status	Actions
Tags	Array	Tags	Enabled	✎ ✕

	Description	Options
Name	Title for the metadata set.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Required This can be changed Validated on Creation

	Description	Options
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	<ul style="list-style-type: none"> By default this is not selected You can choose to disable this set
User Permissions	Grant access to specific users to: <ul style="list-style-type: none"> 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 <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> Not Required Read Write
Group Permissions	Grant access to specific groups to: <ul style="list-style-type: none"> 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 <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> Not Required Read Write
Path Permissions	File Objects in this location will have the metadata set applied <p>➔ For more information, read Managing Metadata Permissions</p>	<ul style="list-style-type: none"> Not Required
Array	A number of custom values (tags) provided by the administrator	<ul style="list-style-type: none"> Name Description Disabled Required Tag Input

➔ [How To Edit a Metadata Set](#)

Metadata Limitations/Recommendations

Metadata feature	Recommended maximum
Metadata set name	128 characters

Metadata feature	Recommended maximum
Metadata set description	128 characters
Attributes per metadata set	99
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](#)

FileCloud - License Purchase And Renewal

Purchase a new license

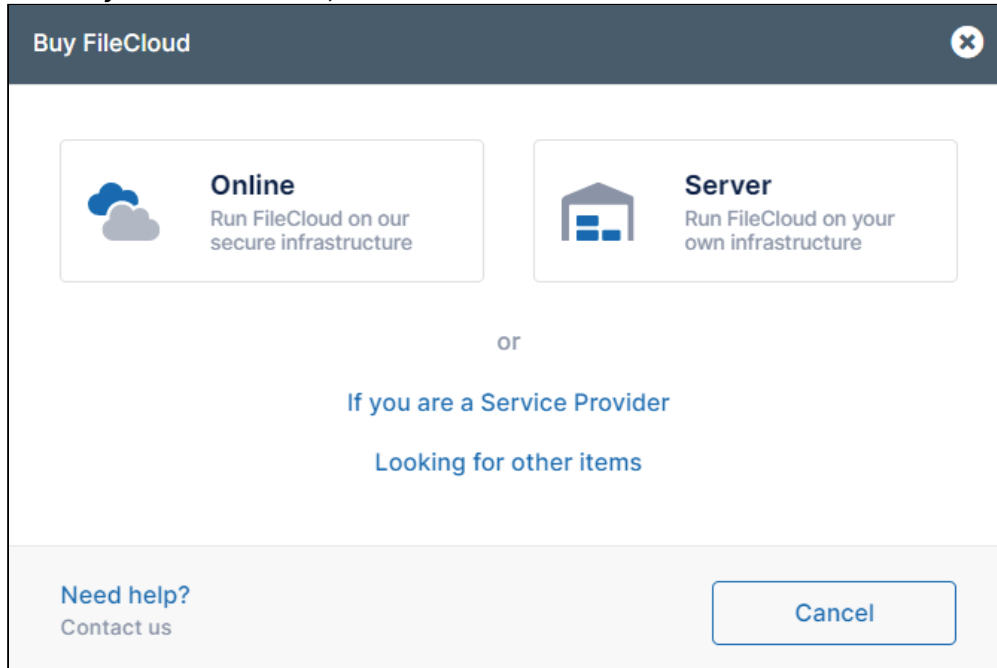
First

Choose a server or online license

1. Log into <https://portal.getfilecloud.com>
2. Click the **New license** icon.

The screenshot displays the FileCloud user interface. On the left is a navigation sidebar with options: Dashboard, Sites, Downloads, SPLA Reports, and Billing. The main content area is titled 'Sites & Licenses' and includes a search bar and filters. A prominent 'New license' button with a plus sign and the text 'Click here to buy a new license' is highlighted with a red dashed box and an orange arrow. To its right, there are two license cards: one for 'www' with 5 seats in a 'pending' state, and another for 'citest1.filecloudonline.com' with 20 seats in an 'expired' state. Below this is a 'Useful Resources' section with three columns: 'Get started' (Need guidance?, Schedule a free demo), 'Learn More' (Case Studies, Data Sheet / FAQ, Documentation, Release Notes, Suggest an idea, Developers), and 'Downloads' (Server, Sync, Drive, Secure Document Viewer, Mobile Apps, Other Downloads). A 'Need help? Contact us' button is located in the bottom left corner.

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**.

Buy FileCloud ✕

FileCloud Server

Run FileCloud on your own infrastructure

Essentials

\$6 user/mo
minimum 20 users, billed annually ⓘ

[BUY](#)

RECOMMENDED

Advanced

Custom pricing available

[GET QUOTE](#)

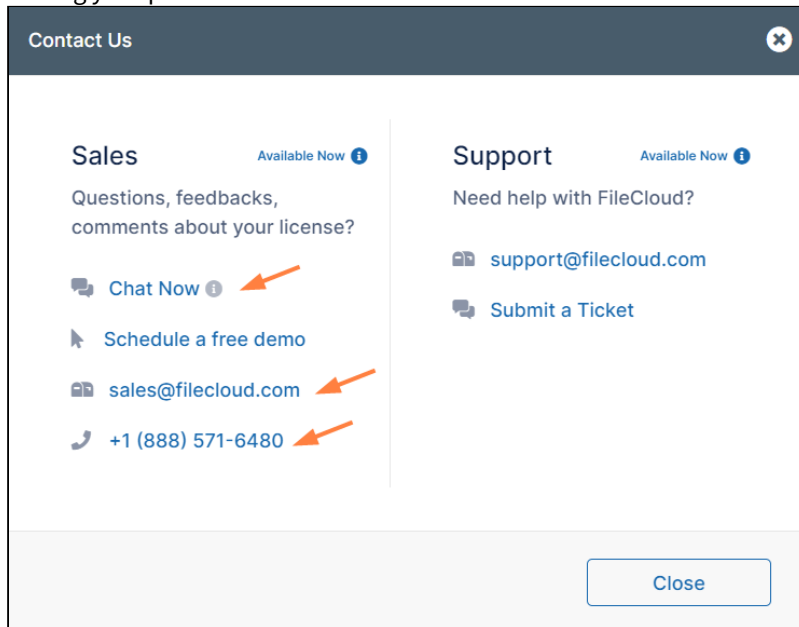
Service Provider

Custom pricing available

[GET QUOTE](#)

✓ Unlimited Storage	✓ Unlimited Storage	✓ Unlimited Storage
✓ Unlimited Licensed External Users	✓ Unlimited Licensed External Users	✓ Unlimited Licensed External Users
✓ Support for Network Shares with NTFS Integration for VPN-less secure access.	✓ Support for Network Shares with NTFS Integration for VPN-less secure access.	✓ Support for Network Shares with NTFS Integration for VPN-less secure access.
✗ Content Classification & Search	✓ Content Classification & Search	✓ Content Classification & Search
✗ Content Lifecycle Management - Legal Hold, Retention, & Archival	✓ Content Lifecycle Management - Legal Hold, Retention, & Archival	✓ Content Lifecycle Management - Legal Hold, Retention, & Archival
✗ Unlimited Workflows	✓ Unlimited Workflows	✓ Unlimited Workflows
✗ Digital Rights Management	✓ Digital Rights Management	✓ Digital Rights Management
✗ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM	✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM	✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM
✗ Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments)	✓ Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments)	✓ Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments)

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.

Order details
✕

FileCloud Server - Enterprise Essentials

Starting at \$6.00 per user, per month, minimum 20 users

Number of Users Drag the slider below to change

20

seats

1

Recommended Support Optional

FileCloud Premium Live Support
Premium Live Technical Support for FileCloud Server Enterprise Essentials - M - F Business Hours, Response SLA - \$1.00 per user, per month.

FileCloud Extended Live Support
Extended Live Technical Support for FileCloud Server Enterprise Essentials - 24/7 Support, Response SLA - \$2.00 per user, per month.

FileCloud Self Service Email Technical Support
Free

Licensed Site URL ⓘ

files.yoursite.com 3

Need professional assistance?
Professional services option available to assist with deployment, configuration, and customization. Please get in touch with us at sales@filecloud.com.

Total
Billed annually ⓘ

[Need help?](#)

Contact us

Back

4

Checkout

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**.

Buy FileCloud
✕

FileCloud Online

Run FileCloud on our secure infrastructure

Essentials

\$12^{.50} user/mo

minimum 10 users, billed annually ⓘ

BUY

RECOMMENDED

Advanced

\$18^{.75} user/mo

minimum 50 users, billed annually ⓘ

BUY

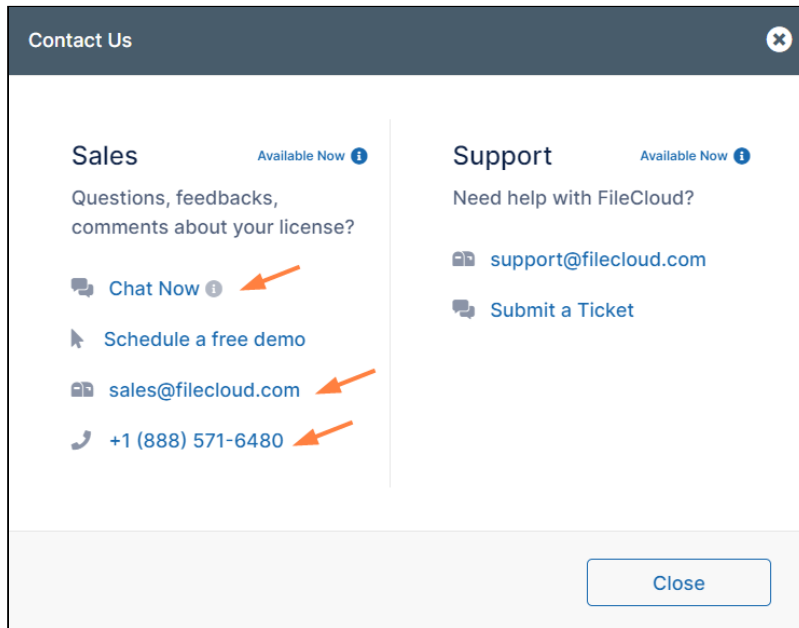
GovCloud

Custom pricing available

GET QUOTE

<ul style="list-style-type: none"> ✓ 1 TB, 100 GB per User ✓ Unlimited Licensed External Users ✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection ✗ Sync/Backup Local File Server to Cloud ✗ Content Classification & Search ✗ Content Lifecycle Management - Legal Hold, Retention, & Archival ✗ Unlimited Workflows ✗ Digital Rights Management ✗ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM ✗ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations <p style="font-size: 8px; color: #2c3e50;">More...</p>	<ul style="list-style-type: none"> ✓ 1 TB, 200 GB per User ✓ Unlimited Licensed External Users ✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection ✓ Sync/Backup Local File Server to Cloud ✓ Content Classification & Search ✓ Content Lifecycle Management - Legal Hold, Retention, & Archival ✓ Unlimited Workflows ✓ Digital Rights Management ✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM ✗ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations <p style="font-size: 8px; color: #2c3e50;">More...</p>	<ul style="list-style-type: none"> ✓ 1 TB, 200 GB per User ✓ Unlimited Licensed External Users ✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection ✓ Sync/Backup Local File Server to Cloud ✓ Content Classification & Search ✓ Content Lifecycle Management - Legal Hold, Retention, & Archival ✓ Unlimited Workflows ✓ Digital Rights Management ✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM ✓ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations <p style="font-size: 8px; color: #2c3e50;">More...</p>
---	---	---

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.

Order details
✕

FileCloud Online - Enterprise Advanced

Starting at \$18.75 per user, per month, minimum 50 users

Number of Users

50 seats **1**

Drag the slider below to change

Recommended Support Optional

FileCloud Premium Live Support
Premium Live Technical Support for FileCloud Online Enterprise Advanced - M - F Business Hours, Response SLA - \$2.00 per user, per month.

FileCloud Extended Premium Live Support
Extended Premium Live Technical Support for FileCloud Online Enterprise Advanced - 24/7 Support, Response SLA - \$3.30 per user, per month.

FileCloud Self Service Email Technical Support
Free

Licensed Site URL ⓘ

 3

Preferred Region

 4 ▼

Need professional assistance?

Professional services option available to assist with deployment, configuration, and customization. Please get in touch with us at sales@filecloud.com.

Included Storage

1 TB

Total

Billed annually ⓘ

[Need help?](#)

Contact us

Back

5 Checkout

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.

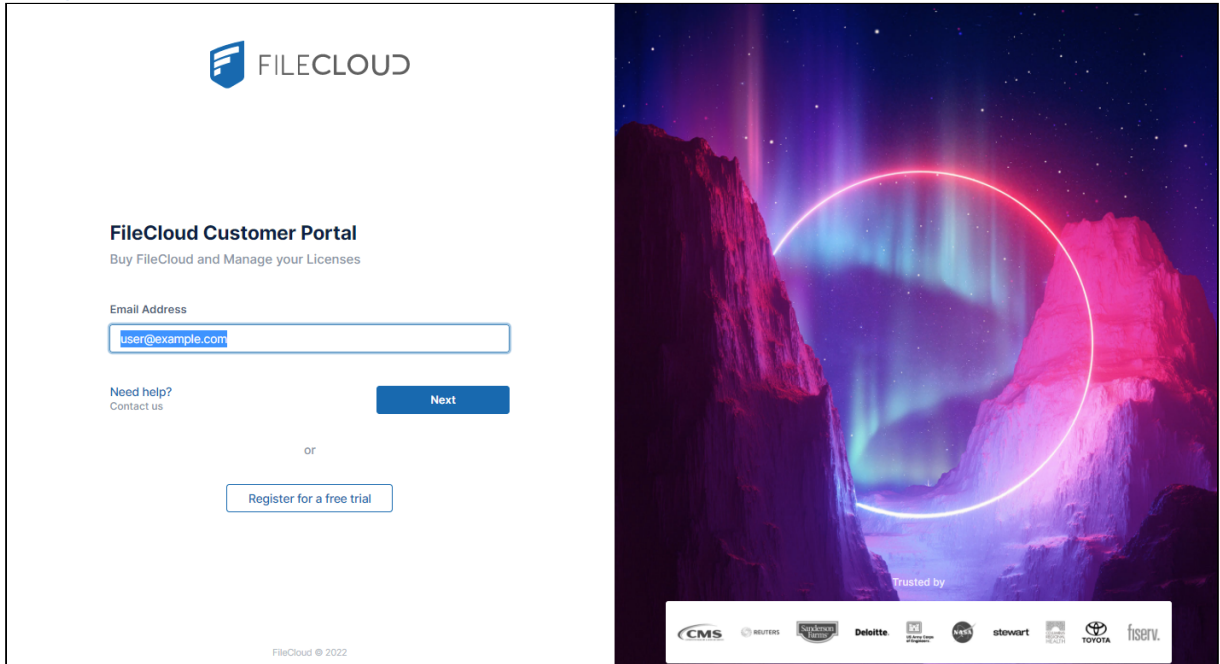
Renew an existing license

Renew a license

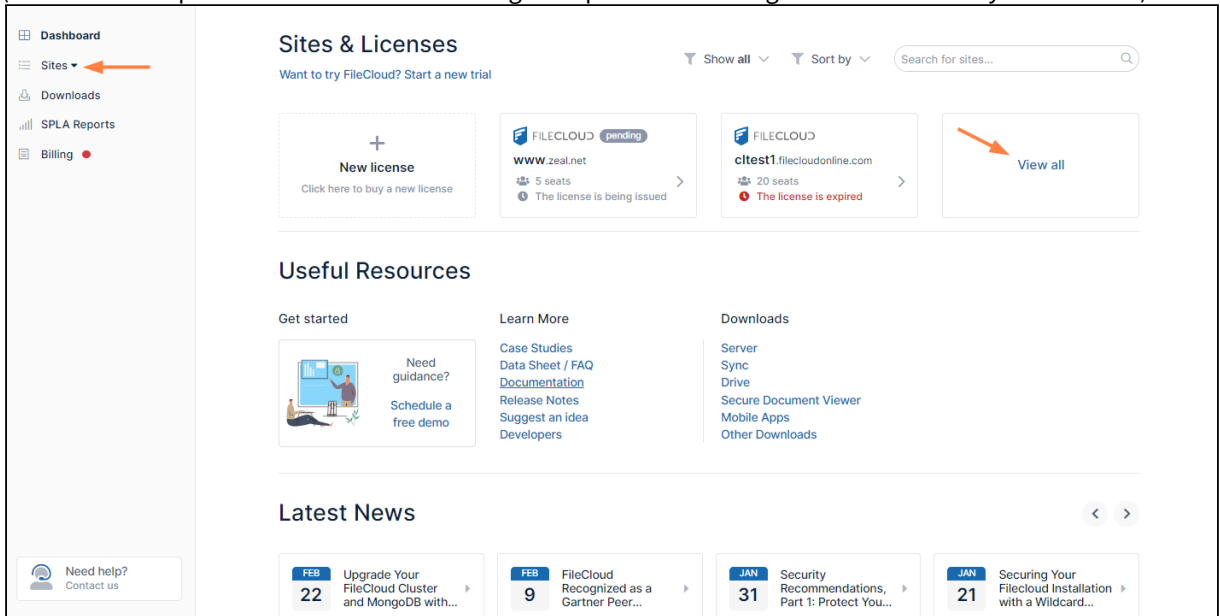
Note: If you are an MSP and want to renew an SPLA License, please follow the [purchase a new license instructions, above.](#)

1. Log into <https://portal.getfilecloud.com>

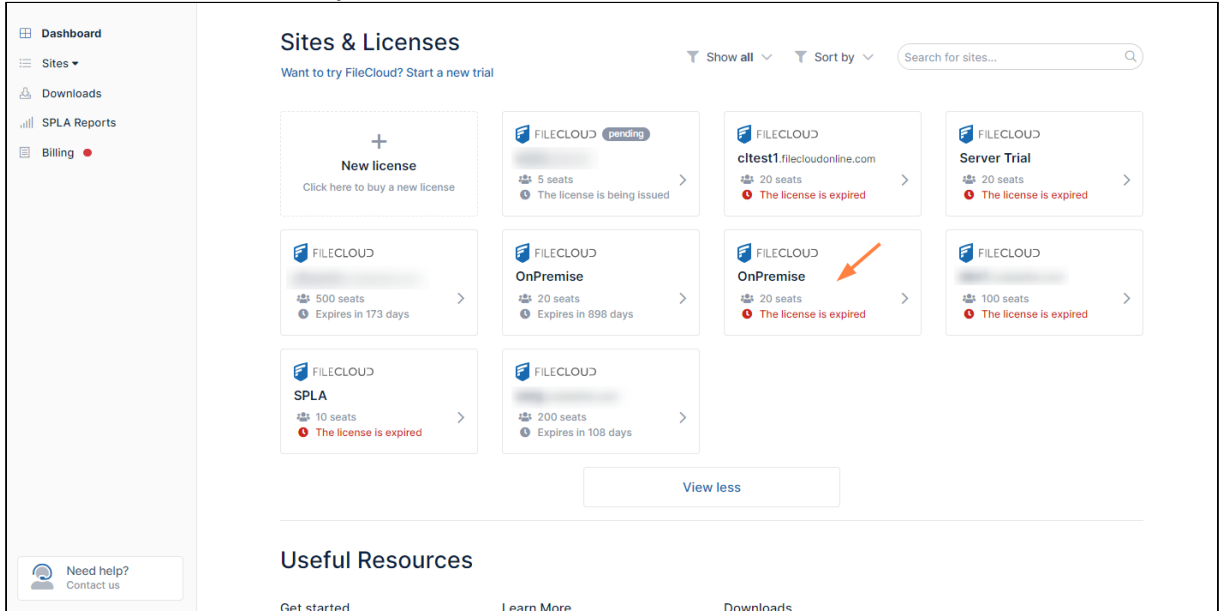
Note: Enter the email of the license holder. To change the license holder email, please contact sales@codelathe.com.



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.)

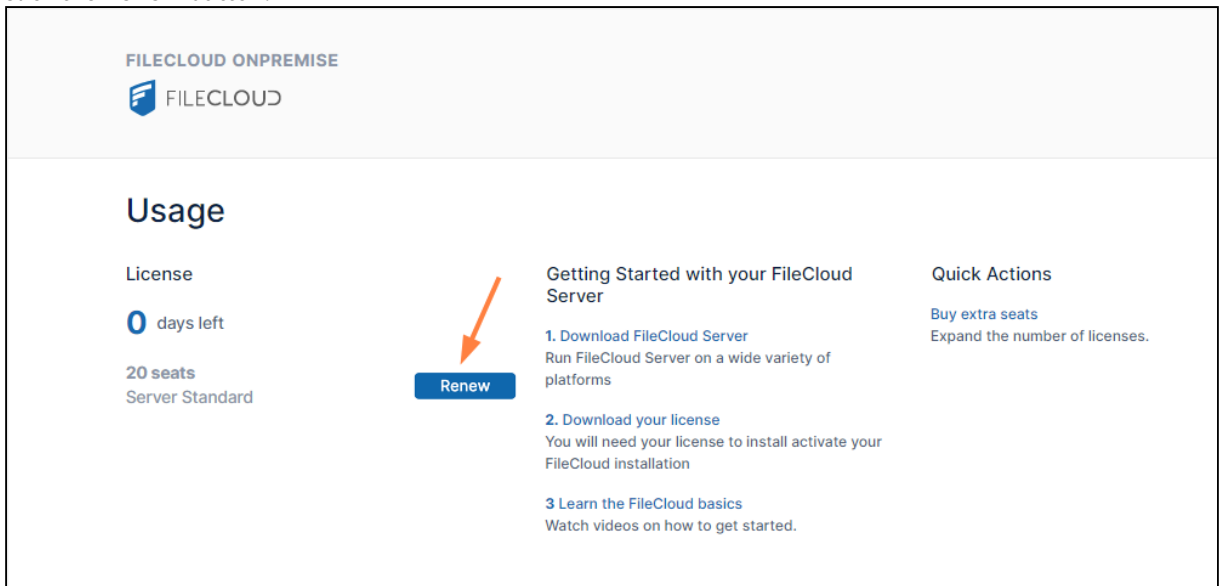


3. Find and click the license that you want to renew.



A screen that displays the license details opens.

4. Click the **Renew** button.



An **Order Summary** opens.

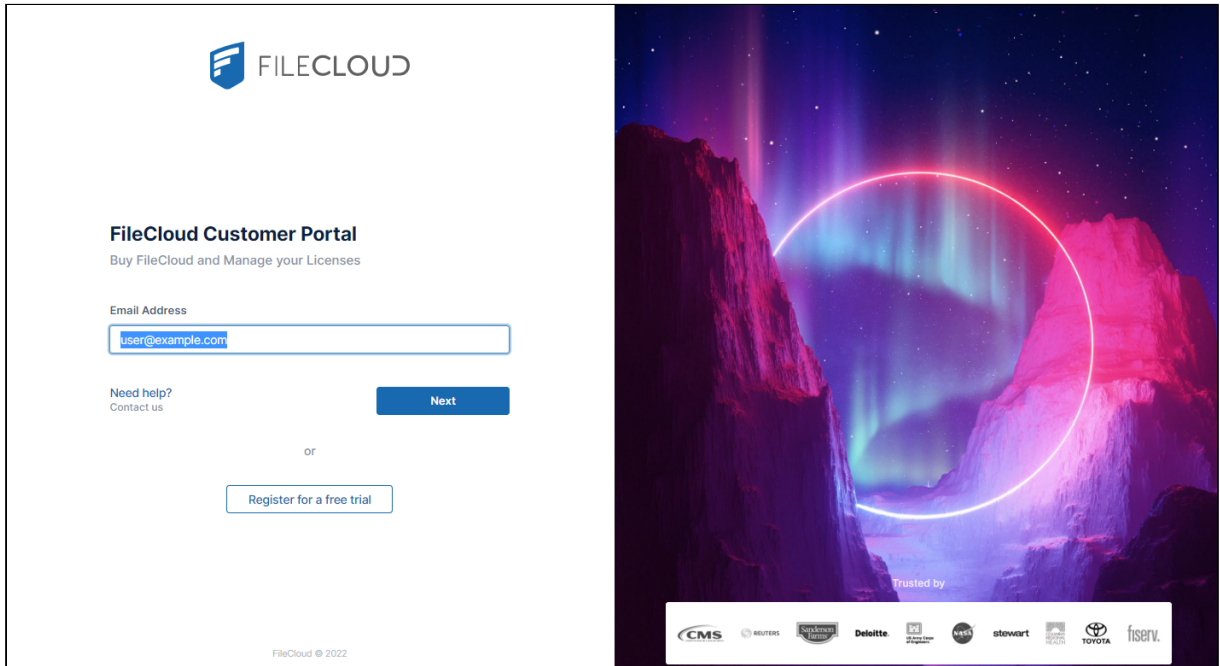
5. Follow the [checkout process](#), below.

Add additional users to an existing license

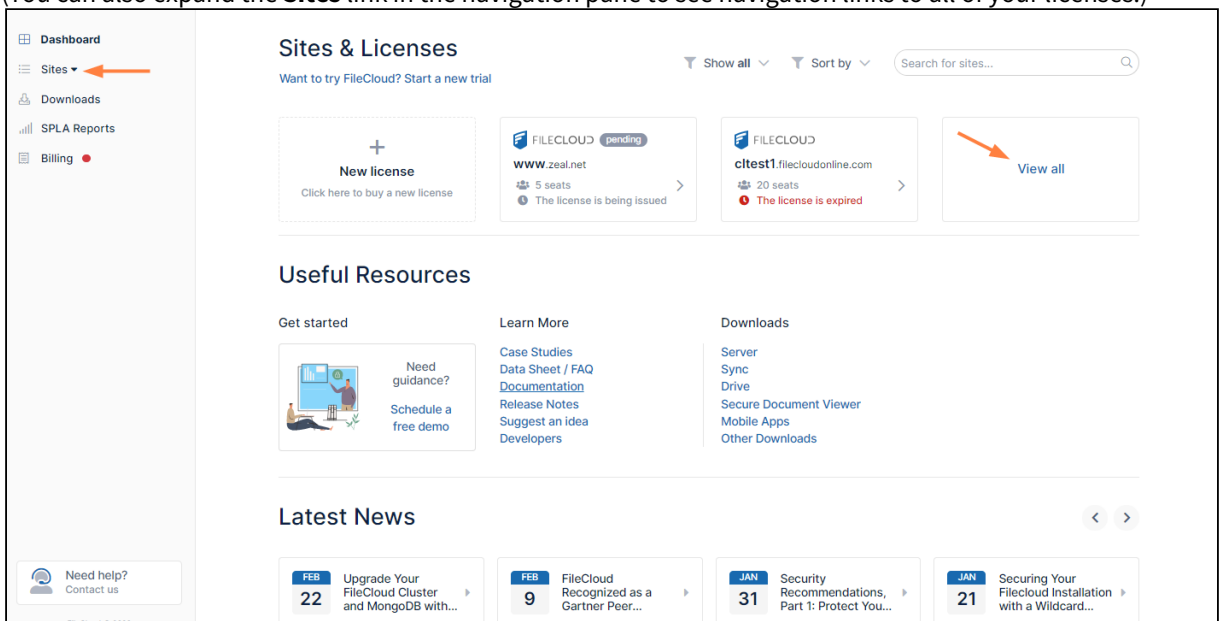
Add additional users to a license

1. Log into <https://portal.getfilecloud.com>

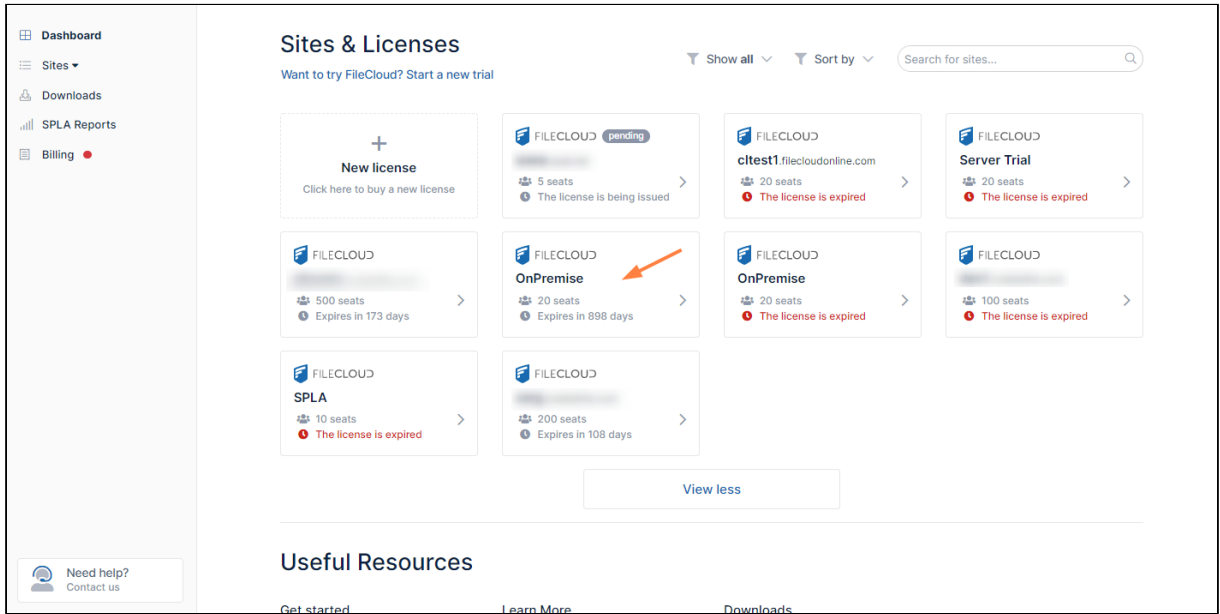
Notes: Enter the email of the license holder. To change the license holder email, please email sales@codelathe.com.



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.)

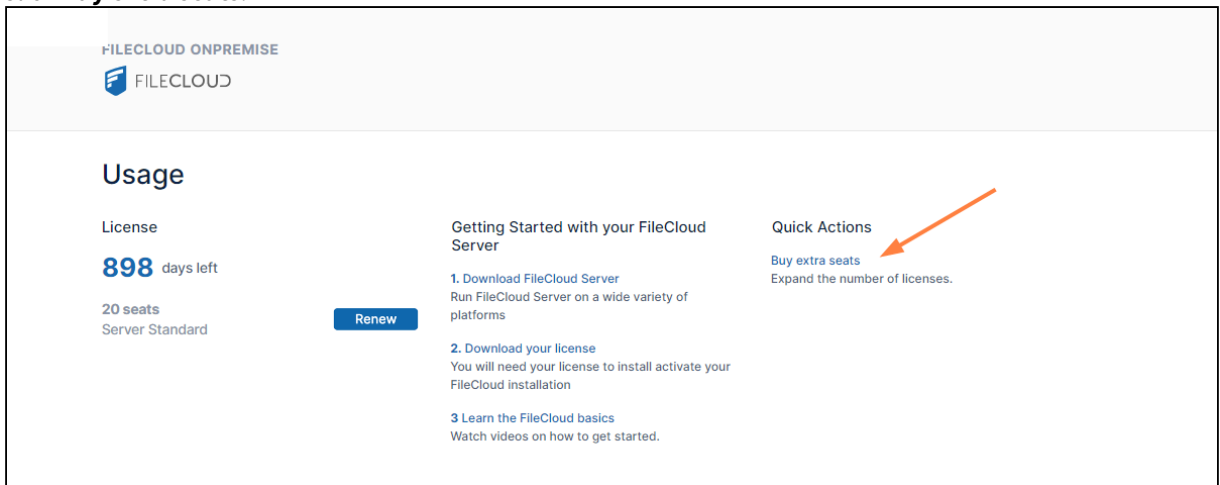


3. Find and click the license that you want to add additional users to.



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.

The screenshot shows a checkout window titled "Checkout" with a close button (X) in the top right corner. The main heading is "FileCloud Server - Enterprise Advanced" with a subtitle "Additional licenses for jenperkins.com". Below this, a message states "Your license expires in 361 days, you will be charged proportionately". A section for "Additional licenses" includes a slider set to "1 seats" and the instruction "Drag the slider below to change". Below the slider, it shows "Additional Seats" as "1 Seats" and "Total Billed annually" with a dollar sign icon. At the bottom, there is a "Need help? Contact us" link, a "Cancel" button, and a blue "Checkout" button.


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:

Order summary

Billing Details  [Edit Billing Details](#)

filecloud
5 Main Street
Newtown / MA / 55555
United States

Additional Info

P.O. Number	Optional	Notes	Optional
<input type="text"/>		<input type="text"/>	

Items

50x FileCloud Server - Enterprise Advanced Renewal
On-premise, Private Cloud-based Enterprise Advanced File Sharing and Collaboration Software Platform. Base Support Only. 50 User Lic. Minimum Req. Renewal. Renew License for jenperkins.com

Invoice Number FC-30574

Order Sub Total

Sales Tax

Total Due
All prices are in U.S. Dollars

[Need help? Contact us](#)

2. Click **Checkout**.

Checkout

Card Payment

Card number MM / YY CVC

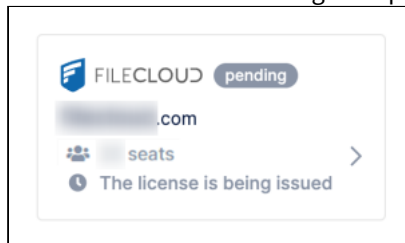
Invoice Number	FC-30574
Order Sub Total	
Sales Tax	
Total Due	

All prices are in U.S. Dollars

By proceeding you accept FileCloud's [Terms of Service](#)
The credit card data is secured, encrypted, and processed by **stripe**

[Need help? Contact us](#)

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:

Order summary
✕

Billing Details → Edit Billing Details

filecloud
5 Main Street
Newtown / MA / 55555
United States

Additional Info

P.O. Number	Optional	Notes	Optional
<input style="width: 90%;" type="text" value="44444"/>		<input style="width: 90%;" type="text"/>	

Items

50x FileCloud Online - Enterprise Advanced (files.site.com)
Fully managed, Cloud-based Enterprise Advanced File Sharing and Collaboration Platform. Base Support Only. 50 User Lic. Minimum Req.

50x FileCloud Premium Live Support - Online Enterprise Advanced
Premium Live Technical Support for FileCloud Online Enterprise Advanced - M - F Business Hours, Response SLA

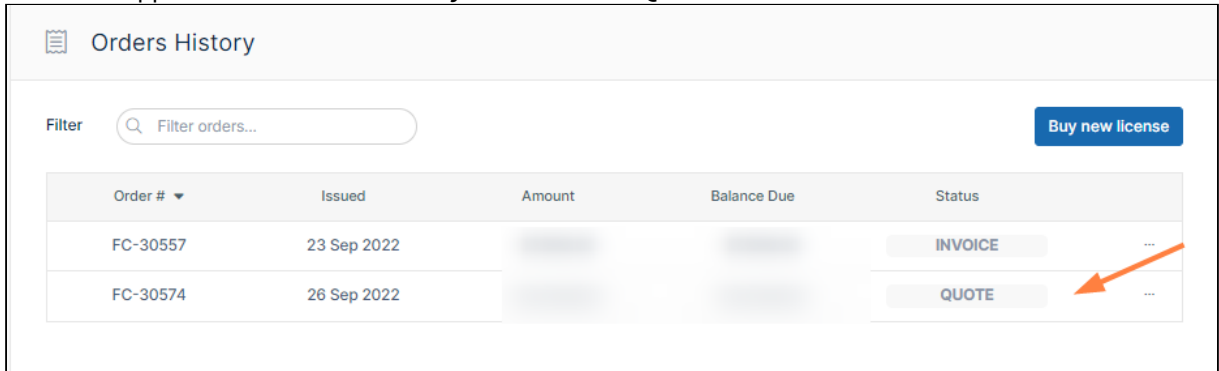
Invoice Number	FC-30574
Order Sub Total	\$11,999.00
Sales Tax	\$0.00
Total Due	\$11,999.00

All prices are in U.S. Dollars

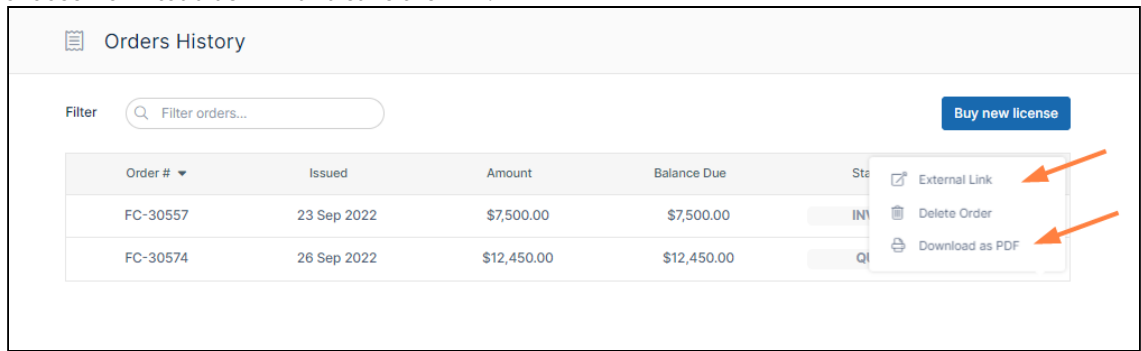
[Need help?](#)
Contact us

2. Optionally, enter a **P.O. Number** and any **Notes** for FileCloud Sales.
 3. Click **Save Quote**.
- The **Billing** screen opens.

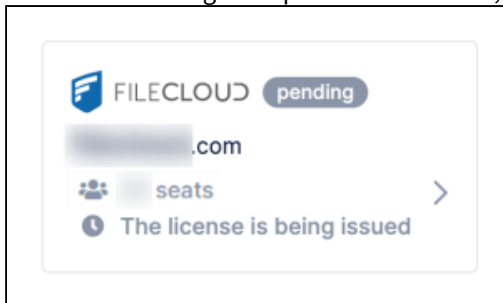
4. Your order appears under **Orders History** with the status **QUOTE**.



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:

Order summary ✕

Billing Details  [Edit Billing Details](#)

filecloud
5 Main Street
Newtown / MA / 55555
United States

Additional Info

P.O. Number	Optional	Notes	Optional
<input type="text"/>		<input type="text"/>	

Items

50x FileCloud Online - Enterprise Advanced (files.site.com)
Fully managed, Cloud-based Enterprise Advanced File Sharing and Collaboration Platform. Base Support Only. 50 User Lic. Minimum Req.

50x FileCloud Premium Live Support - Online Enterprise Advanced
Premium Live Technical Support for FileCloud Online Enterprise Advanced - M - F Business Hours, Response SLA

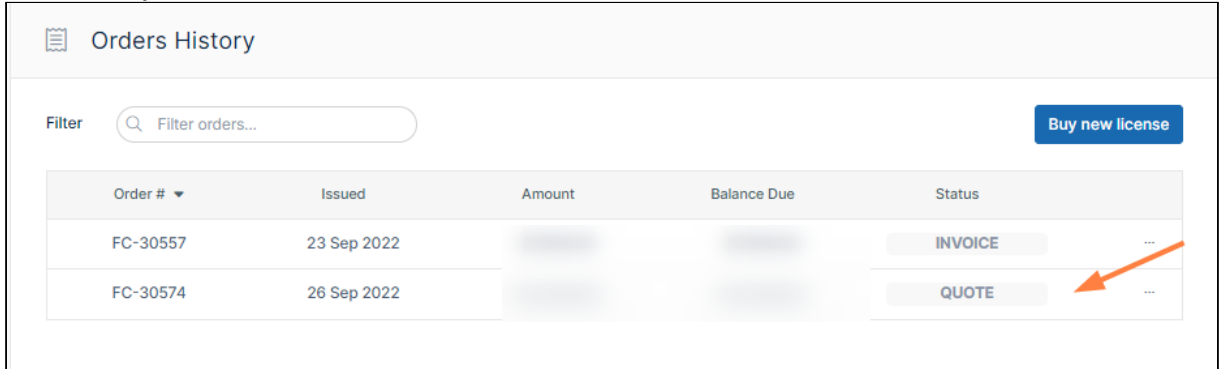
Invoice Number	FC-30574
Order Sub Total	
Sales Tax	
Total Due	

All prices are in U.S. Dollars

[Need help?
Contact us](#)

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.

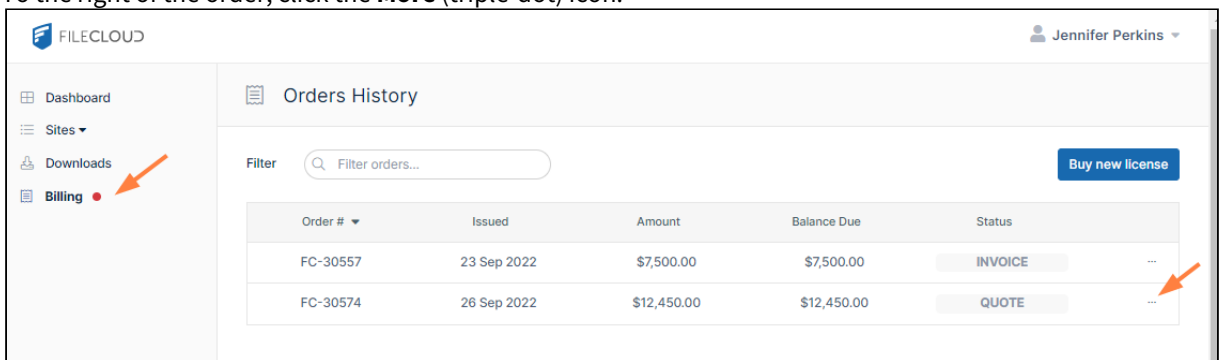


3. When you are ready to continue, return to the **Billing** screen and perform one of the actions in [Manage orders](#), below.

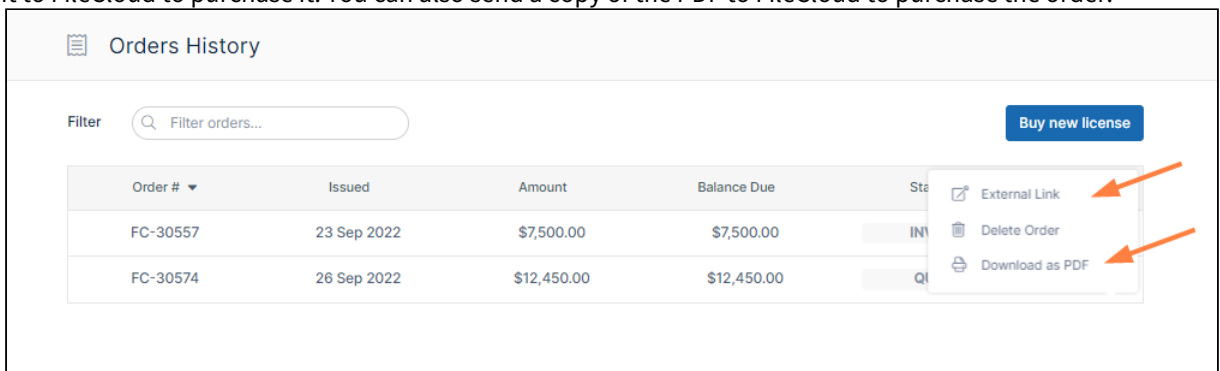
Manage orders

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

- i** Creating custom workflows to perform a variety of actions is available in FileCloud Server version 13 and later.
- A new Workflow *Generic Email Template* is available in FileCloud Server version 18.2.
 - In FileCloud version 19.1 and later, three new features have been added to the Manage Workflow screen to provide more details about how workflows are functioning and how they impact your FileCloud Server system.
 - *Activity* - All workflows now have the ability to show the Date of an event, and a Description of the event, such as file uploads, moves, and deletions.
 - *Suspension* - Suspending a workflow will prevent the workflow from automatically running at the next Cron job. This option retains the workflow if you want to manually run it.
 - *Simulation* - Use this option to display 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.

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.

Manage Workflows

Workflow [+ Add Workflow](#)


Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Actions
mv	If file is downloaded	Move the file(s) to some location	March 14, 2019, 11:30 am	March 7, 2019, 10:47 am	✎ ⏸ ↺ ✖
File Integrity Test	If file was not modified for specified days	Verify file integrity and generate admin alert on mismatch	March 14, 2019, 11:30 am	Never	▶ ⏸ ✎ ⏸ ↺ ✖
3374 a	If a new user is created	Change user status	February 26, 2019, 5:50 am	February 26, 2019, 5:49 am	✎ ⏸ ↺ ✖
3374	If a new user is created	Change user status	February 26, 2019, 5:50 am	February 8, 2019, 3:26 am	✎ ⏸ ↺ ✖
move	If a file is added or updated	Move the file(s) to some location	March 14, 2019, 11:30 am	Never	✎ ⏸ ↺ ✖
chk nags	If any new client app connects	Notify user(s)	February 5, 2019, 12:57 pm	February 5, 2019, 9:08 am	✎ ⏸ ↺ ✖

Page 1 of 1
6 rows

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. **Run the workflow (once, on-demand)**
2. **Simulate the workflow**
3. **Edit the workflow**
4. **Enable or Disable the workflow**
5. **See the activity**
6. **Delete the workflow**

In this section:

- [Add a New Workflow](#)
- [Define an IF Condition](#)
- [Define a THEN Action](#)
- [Edit a Workflow](#)
- [Run a Workflow](#)
- [Set Advanced Workflow Options](#)
- [Workflow Recipes for FileCloud](#)

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.

Create New Workflow
✕

Name for this action

Workflow Name

← Previous
→ Finish
✕ Cancel

Define an IF Condition

⚠ 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.

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.

Create New Workflow ✕

Select the condition

IF Condition .. ▼

→ Next ✕ Cancel

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.

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

This condition will be triggered the **first time** a client app connects to the server.
No additional parameter is required.
The client can be mobile app, drive app, sync app etc

← Previous → Next ✕ Cancel

Available Conditions



Client App Conditions

If any new client app connects

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{  
  "parameter name": "value"  
}
```

This condition will be triggered the **first time** a client app connects to the server.
No additional parameter is required.
The client can be mobile app, drive app, sync app etc

← Previous → Next ✕ Cancel

Workflow Condition	Parameters	Description
If any new client app connects	No parameters required	<p>This condition is triggered when an external (non-browser) client connects to FileCloud Server.</p> <p>For example, this condition will trigger for clients such as:</p> <ul style="list-style-type: none">• FileCloudSync• FileCloudDrive• iOS• Android App



File Conditions

If a file is created

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name": "value"
}
```

This condition will be triggered when a file is created.

parent_folder_path_string: path of the folder as shown below

use_regex (optional): specifies whether path has a regex format

exclude (optional): exclude files matching the specified path from the action, and perform the action for all files that don't match the path.

```
{
  "parent_folder_path_string": "/userid/
somepath",
  "use_regex": 1,
  "exclude": 1
}
```

← Previous → Next ✕ Cancel

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).

If a file is updated

Workflow Condition	Parameters	Description
If a file is updated.	<pre>{ "parent_folder_path_string":"/ userid/somepath", "use_regex":"1", "exclude":"1" }</pre>	<p>This condition will be triggered if a file is updated.</p> <p>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.</p> <p>use_regex (optional) - specifies how the folder path is validated.</p> <ul style="list-style-type: none"> • 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 <p>exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).</p>

If a file is deleted

Workflow Condition	Parameters	Description
If a file is deleted	<pre>{ "parent_folder_path_string":"/ userid/somepath", "use_regex":"1", "exclude":"1" }</pre>	<p>This condition will be triggered if a file is deleted.</p> <p>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.</p> <p>use_regex (optional) - specifies how the folder path is validated.</p> <ul style="list-style-type: none"> • 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 <p>exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).</p>

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).

If file was not modified for specified days

Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name": "value"
}
```

This condition will be triggered if a file was last modified the specified days ago. The check will run once a day.

parent_folder_path_string : Path of the folder containing the files as shown below.

number_of_days : Number of days since a file was modified.

skip_recently_accessed : (OPTIONAL) When TRUE, files viewed or downloaded within number_of_days will be treated as recently modified.

exclude_recyclebin : (OPTIONAL) When TRUE, files on recycle bin path will not be considered.

exclude : (OPTIONAL) Do not include files matching the regex in workflow, and do include files that don't match the regex in this workflow.

```
{
  "parent_folder_path_string": "/johndoe",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*"
}
```

In the example, any folder or file that has the string "secret" in its name will be excluded.

← Previous

→ Next

✕ Cancel

Workflow Condition	Parameters	Description
<p>If a file was not modified for specified days</p>	<pre data-bbox="591 275 927 947"> { "parent_folder_path_string": "/johndoe", "number_of_days": 7, "skip_recently_accessed": 1, "exclude_recyclebin": 1, "exclude": ".*secret.*" } </pre>	<p>This condition will be triggered if a file is not updated for specified number of days.</p> <ul data-bbox="976 352 1442 447" style="list-style-type: none"> • This is useful for removing old files that are no longer being used • This check will run once a day <p>parent_folder_path_string - required as a parameter for this condition to trigger.</p> <ul data-bbox="976 541 1455 762" style="list-style-type: none"> • 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. <p>number_of_days - required to specify the number of days before the current date that a file was last modified.</p> <ul data-bbox="976 894 1458 1146" style="list-style-type: none"> • 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. <p>skip_recently_accessed - required to specify whether files that were viewed or downloaded during the number of days are considered modified. Default is <i>false</i>, viewed or downloaded files are not considered recently modified. When <i>true</i>, files viewed or downloaded within number_of_days are considered modified and will not be included in the <i>Then</i> action.</p> <p>exclude_recyclebin - (added in FileCloud version 21.3) optional (default is false) When true, files in recycle bin are not considered.</p> <p>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).</p>

If a file is added or updated

Workflow Condition	Parameters	Description
If a file is added or updated	<pre>{ "parent_folder_path_string":"/ userid/somepath", "use_regex":"1", "exclude":"1" }</pre>	<p>This condition will be triggered if a file is added or updated</p> <p>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.</p> <p>use_regex (optional) - specifies how the folder path is validated.</p> <ul style="list-style-type: none"> • 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 <p>exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).</p>

If the file uploaded is bigger than the expected size

Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name": "value"
}
```

This condition will be triggered when an uploaded file is bigger than the expected size.
size: Size expected in MB

```
{
  "size": 4
}
```

← Previous
→ Next
✕ Cancel

Workflow Condition	Parameters	Description
If the file uploaded is bigger than expected size.	<pre>{ "size": "4" }</pre>	This condition will be triggered when an uploaded file is bigger than the size specified. size - specifies the maximum expected file size in MB.

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.



Folder Conditions

If a folder is created

Workflow Condition	Parameters	Description
If a folder is created	<pre> { "parent_folder_path_string": "/ userid/somepath", "use_regex": "1", "exclude": "1" } </pre>	<p>This condition will be triggered when a folder is created in the system</p> <p>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.</p> <p>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")</p> <p>exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).</p>

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).

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 once a day

last_login_days_ago: number of days ago.

user_account_type: Type of account. This can be
 USER_ACCOUNT_ANY
 USER_ACCOUNT_FULL_ACCESS
 USER_ACCOUNT_GUEST_ACCESS
 USER_ACCOUNT_LIMITED_ACCESS (external users)
 USER_ACCOUNT_DISABLED

day_interval: Days interval to perform the check (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

include_domain (optional): Email domain(s) to include separated by comma.

exclude_domain (optional): Email domain(s) to exclude separated by comma.

For example, to disable external access users who have not logged in for 30 days, set the following parameters:

```
{
  "last_login_days_ago": 30,
  "user_account_type": "USER_ACCOUNT_LIM
  "day_interval": 1,
  "skip_users_not_logged_in": 1,
  "include_domain": "domain.com",
  "exclude_domain": "subdomain.domain.co
}
```

Work

← Previous
→ Next
✕ Cancel

Workflow Condition	Parameters	Description
If a user's last login is older than ...	<pre>{ "last_login_days_ago": 30, "user_account_type": "USER_ACCOUNT_LIMITED_ACCESS" , "day_interval": 1, "skip_users_not_logged_in": 1, "include_domain": "domain.com", "exclude_domain": "subdomain.domain.com,@otherd omain.com" }</pre> <p><i>For example, every five days to check for external (limited) access users who have not logged in for the last 30 days:</i></p> <pre>{ "last_login_days_ago": 30, "user_account_type": "USER_ACCOUNT_LIMITED_ACCESS" , "day_interval": 1, "skip_users_not_logged_in": 1 }</pre>	<p>If a user's last login is older than the specified number of days, then the THEN condition you configure will be run.</p> <p>last_login_days_ago: last login of a user account in number of days ago.</p> <p>user_account_type - type of account. You must use one of the following values:</p> <ul style="list-style-type: none"> • USER_ACCOUNT_ANY • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (for external users) • USER_ACCOUNT_DISABLED <p>day_interval - the number of days between checks</p> <ul style="list-style-type: none"> • For daily operation, specify a value of 1 <p>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.</p> <p>include_domain - Optional. If the user's email domain matches one of the domains listed here, the condition applies.</p> <p>exclude_domain - Optional. If the user's email matches one of the domains listed here, the condition does not apply.</p>

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 chose the proper action depending on the security state of a created user.

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
- USER_ACCOUNT_FULL_ACCESS
- USER_ACCOUNT_GUEST_ACCESS
- USER_ACCOUNT_LIMITED_ACCESS

user_login_method: How user authenticates. This is **optional** and can be:

- LOGIN_METHOD_ANY
- LOGIN_METHOD_DEFAULT
- LOGIN_METHOD_SSO

excluded_email_domains: Email domain used to create the user. This is **optional**. Users created with these domains will be excluded from this workflow

```
{
  "auth_type": "ACTIVEDIRECTORY",
  "user_access_level": "USER_ACCOUNT_FULL_ACCESS",
  "user_login_method": "LOGIN_METHOD_ANY",
  "excluded_email_domains": "a.com,b.com"
}
```

← Previous
→ Next
✕ Cancel

This tells FileCloud that if a new user account is created to trigger the THEN action.

Workflow Condition	Parameters	Description
If a new user is created ...	None	<p>When a new user account is created, the THEN action you configure will be triggered.</p> <p>Optional Parameters</p> <p>auth-type - Type of authentication. This is optional and can be:</p> <ul style="list-style-type: none"> • DEFAULT • ACTIVEDIRECTORY • LDAP <p>user_access_level: Account access level. This is optional and can be:</p> <ul style="list-style-type: none"> • USER_ACCOUNT_ANY_ACCESS • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (for external users) <p>user_login_method: How user authenticates. This is optional and can be:</p> <ul style="list-style-type: none"> • LOGIN_METHOD_ANY • LOGIN_METHOD_DEFAULT • LOGIN_METHOD_SSO <p>excluded_email_domains: (Available in FileCloud 21.2 and later) Email domain used to create the user. This is optional. If the new user has any of these domains, the workflow is not triggered.</p>

If a user's create date 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 account creation is older than specified days. This check will run once a day

days: number of days after account creation.
include_domain (optional): Email domain(s) to include separated by comma.
exclude_domain (optional): Email domain(s) to exclude separated by comma.

To exactly match the domain use the @ character. Example: "@domain.com"

```
{
  "days": 30,
  "include_domain": "domain.com",
  "exclude_domain": "subdomain.domain.com"
}
```

← Previous → Next ✕ Cancel

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.

include_domain - Optional. If the user's email domain matches one of the domains listed here, the condition applies.

exclude_domain - Optional. If the user's email matches one of the domains listed here, the condition does not apply.

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"  
}
```

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).

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.
time_string : time in format H:i:s
day_interval : Days interval (For daily operation, specify this value to be 1)

```
{  
  "time_string": "16:45:05",  
  "day_interval": 7  
}
```

← Previous → Next ✕ Cancel

Workflow Condition	Parameters	Description
Perform an action periodically at specified time and interval	<pre>{ "time_string": "16:45:05", "day_interval": "7" }</pre>	<p>This condition will be triggered when the current time on the FileCloud Server matches the supplied time.</p> <p>time_string - the time when you want the THEN action triggered</p> <ul style="list-style-type: none"> The matching time includes the time zone The time is specified in a 24-hour format of Hours, minutes, seconds <p>days_interval - number of days between triggering the THEN action you configure</p> <ul style="list-style-type: none"> The THEN action you choose will be triggered every "day_interval" days. If the "day_interval" is 1, then it will be done daily

Perform an action on the specified date

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 date matches the supplied date and time.
date_string : date and time in format yyyy-mm-dd H:i:s

```
{
  "date_string": "2020-01-11 16:45:05"
}
```

← Previous
→ Next
✕ Cancel

Workflow Condition	Parameters	Description
Perform an action on the specified date	<pre>{ "date_string": "2020-01-11" }</pre>	<p>When the date matches the supplied date and time, the THEN action you configure will be run.</p> <p>date_string - date and time in a 24-hour format</p> <ul style="list-style-type: none"> yyyy-mm-dd H:i:s

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: <ul style="list-style-type: none"> • cron job • task scheduler

If share has not been accessed for specified days

Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name": "value"
}
```

This condition will be triggered if a share has not been accessed for the specified number of days. The check will run once a day

number_of_days: (REQUIRED) Number of days since share had an activity e.g. last 180 days

share_permission: (REQUIRED) Share permissions to target. Possible values: ["PUBLIC", "PRIVATE"]

```
{
  "number_of_days": 180,
  "share_permission": ["PUBLIC", "PRIVAT
}
```

← Previous
→ Next
✕ Cancel

Workflow Condition	Parameters	Description
If a share has not been accessed for specified days	<pre>{ "share_permission": ["PUBLIC", "PRIVATE"], "number_of_days": "180", }</pre>	<p>This condition will be triggered when a shared file or folder has not been accessed for the specified number of days.</p> <ul style="list-style-type: none"> • NOTE: The only supported action is <i>Delete share</i>. • This is useful for removing shared files that are no longer being used • This check will run once a day <p>share_permission - required as a parameter for this condition to trigger. An array that specifies the type of shares to monitor. Valid values are:</p> <ul style="list-style-type: none"> • PUBLIC • PRIVATE <p>Both PUBLIC and PRIVATE may be included in the array.</p> <p>number_of_days - required to specify the number of days before the current date that a shared file was accessed.</p> <ul style="list-style-type: none"> • 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.

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.

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action .. Notify user(s)

← Previous → Next × Cancel

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	Parameters	Details	Compatible IF conditions
Notify the file actions to user(s)	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" }</pre>	<p>Sends an email with information about the file and the action performed.</p> <p>comma_separated_email_id - email ids in comma separated format</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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
Notify the user that the account may be deactivated soon	None	<p>Notifies the user that the account may be disabled or deleted due to inactivity.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> If a user's last login is older than . . . If a new user is created If a user's create date is older than

Action	Parameters	Details	Compatible IF conditions
Notify user(s)	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" }</pre>	<p>Sends a notification to users matching the criteria and sends an email to the admin and the specified addresses with information about the users who were sent notifications.</p> <p>comma_separated_email_id - email ids in comma separated format</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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 new client app connects

File actions

Action	Parameters	Details	Compatible IF conditions
Copy the file(s) to some location	<pre>{ "target_path":"/usera/ folderb/", "allow_overwrite":"1", "keep_folder_structure ":"1" }</pre>	<p>Copies files.</p> <p>target_path - path to copy the file to.</p> <ul style="list-style-type: none"> This path must be in the same storage type Files cannot be copied from managed storage to network shares or vice versa. <p>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.</p> <p>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.</p> <p>The placeholders. %who, %when, %path, %how, %filename are available for this action.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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)	<pre>{ "excluded_users": "user 1,user2,user3", "delete_empty_folders ": true, "notify_owner": false, "comma_separated_e mail_id": "email1@ema il.com,email2@email.c om" }</pre>	<p>Deletes matching files.</p> <p>excluded_users (Optional): Users whose files will be excluded from deletion. Names must be provided in a comma separated format.</p> <p>delete_empty_folders (Optional): When files are deleted, delete the parent folder as well if it is empty.</p> <p>notify_owner (Optional): When the files are deleted, send an email to the owners.</p> <p>comma_separated_email_id (Optional): Email ids in comma separated format.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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	<pre>{ "target_path":"/usera/ folderb/", "allow_overwrite":"1", "keep_folder_structure ":"1" }</pre>	<p>Moves files.</p> <p>target_path - Path to the new file location (where it should be moved).</p> <ul style="list-style-type: none"> This path must be in the same storage type Files cannot be moved from managed storage to network shares or vice versa. <p>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.</p> <p>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.</p> <p>The placeholders. %who, %when, %path, %how, %filename are available for this action.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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)	<pre>{ "days": 7 }</pre>	<p>Releases locks on files and folders.</p> <p>days - Number of days after a lock was created on a file or folder to release it.</p>	<p>Click to see if conditions</p> <ul style="list-style-type: none"> 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	<pre>{ "ignore_file_size_in_mb": "10" }</pre>	<p>Attempts to identify the file type based on its content and checks if it matches the extension.</p> <ul style="list-style-type: none"> If the file type does not match, then generate admin portal alert. <p>Optional</p> <p>ignore_file_size_in_mb: - Do not scan files larger than this limit specified in megabytes.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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
Verify file integrity and delete on mismatch	<pre>{ "ignore_file_size_in_mb": "10" }</pre>	<p>Attempts to identify file type based on its content and checks if it matches its mime type.</p> <ul style="list-style-type: none"> A MIME type is a string identifier composed of two parts: a "type" and a "subtype". If the file type does not match, then <ul style="list-style-type: none"> the latest version is deleted users listed in the parameter are notified <p>Optional</p> <p>ignore_file_size_in_mb: - Do not scan files larger than this limit specified in megabytes.</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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	<pre>{ "report_name": "my_report", "comma_separated_email_id": "a@x.com, b@y.com" }</pre>	<p>Opens a saved report, runs it, and then sends the results in email.</p> <p> This action requires you to have already created the report from the Admin dashboard.</p> <p> Create a Custom Report</p> <p>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.</p> <p>comma_separated_email_id: Comma separated email ids to be notified after report is run</p>	<p>Click to see If conditions</p> <ul style="list-style-type: none"> 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 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	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" }</pre>	<p>Sends an email to the specified addresses with information about the users matching the criteria.</p> <p>comma_separated_email_id - email ids in comma separated format</p>	<p>Click to see If conditions</p> <p>If a user's last login is older than ...</p> <p>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)</p> <p>If a user's create date is older than</p>

Modifying users

Action	Parameters	Details	Compatible IF conditions
Disable user account	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" }</pre>	<p>Disables the user account and then sends an email with information about the action performed.</p> <p>comma_separated_email_id - email IDs in comma separated format</p> <p>donot_email_user (optional): Do not send email to the user affected (1 or 0). Default 0.</p>	<p>Click to see If conditions</p> <p>If a user's last login is older than ...</p> <p>If a new user is created</p> <p>If a user's create date is older than</p>
Delete user account	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" }</pre>	<p>Deletes the user account and then sends an email with information about the action performed.</p> <p>comma_separated_email_id - email IDs in comma separated format</p> <p>donot_email_user (optional): Do not send email to user affected (1 or 0). Default 0.</p>	<p>Click to see If conditions</p> <p>If a user's last login is older than ...</p> <p>If a new user is created</p> <p>If a user's create date is older than</p>

Action	Parameters	Details	Compatible IF conditions
Change user status	<pre>{ "user_status": "USER_ACCOUNT_LIMITED_ACCESS", "mark_as_verified": 0, "comma_separated_email_id": "xyz@a.com,abc@b.com" , "donot_email_user": 0 }</pre>	<p>user_account_type - type of account. You must use one of the following values:</p> <ul style="list-style-type: none"> • USER_ACCOUNT_DISABLED_ACCESS • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (external access) <p>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.</p> <p>comma_separated_email_id - email IDs in comma separated format</p> <p>donot_email_user (optional) - prevents an email from being sent to the user affected when the status is changed</p> <ul style="list-style-type: none"> • 1 = Does not send an email • 0 = Sends an email • If nothing is specified, the default is 0 	<p>Click to see IF conditions</p> <p>If a user's last login is older than . . .</p> <p>If a new user is created</p> <p>If a user's create date is older than</p>
Set user group	<pre>{ "group_name": "Group1,Group2" }</pre>	<p>Assigns user to groups.</p> <p>group_name - Comma separated list of groups to assign user to.</p>	<p>If a new user is created</p> <p>If a user's create date is older than</p>
Set user policy	<pre>{ "policy_name": "SamplePolicy Name", "comma_separated_email_id": "", "donot_email_user": 0 }</pre>	<p>Sends an email notification to the listed users that the user's policy was set as the specified policy</p> <p>policy_name - Name of policy to set</p> <p>comma_separated_email_id - email ids in comma separated format</p> <p>donot_email_user 0 (default) send the emails 1 do not send the emails</p>	<p>If a user's last login is older than . . .</p> <p>If a new user is created</p> <p>If a user's create date is older than</p>

Action	Parameters	Details	Compatible IF conditions
Set user properties	<pre>{ "policy_name":"SamplePolicy Name", "user_status":"USER_ACCOUNT_LIMITED_ACCESS", "comma_separated_email_id": "", "donot_email_user": 0 }</pre>	<p>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</p> <p>policy_name: Name of policy to set.</p> <p>user_status (optional): User status to set. (USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS (external access))</p> <p>comma_separated_email_id (optional): Comma separated emails to notify of workflow action.</p> <p>donot_email_user (optional): Set to 1 to prevent system from notifying user.</p>	<p>If a user's last login is older than . . .</p> <p>If a new user is created</p> <p>If a user's create date is older than</p>

Share actions

Action	Parameters	Details	Compatible IF conditions
Delete the share(s)	<i>None</i>	Delete the share.	<p>Click to see If conditions</p> <p>If a share has not been accessed for specified days</p>

Device actions

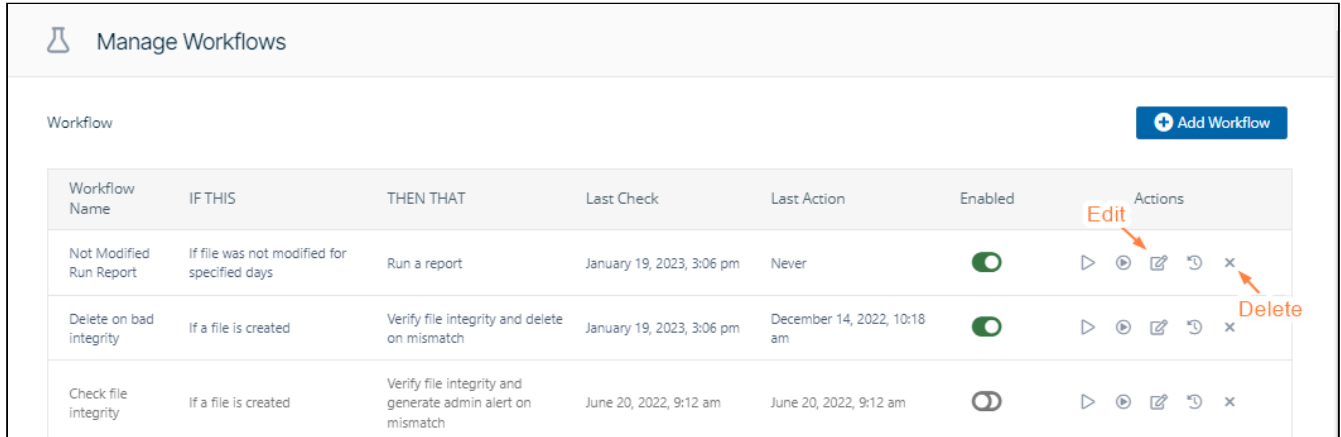
Action	Parameters	Details	Compatible IF conditions
Block the device for admin approval	<i>None</i>	Blocks the device and marks it with "Needs Approval" on the Manage Devices screen	<p>Click to see If conditions</p> <p>If a new client app connects</p>

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.



The screenshot shows the 'Manage Workflows' interface. At the top right, there is a blue 'Add Workflow' button. Below it is a table with the following columns: Workflow Name, IF THIS, THEN THAT, Last Check, Last Action, Enabled, and Actions. Three workflows are listed:

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
Not Modified Run Report	If file was not modified for specified days	Run a report	January 19, 2023, 3:06 pm	Never	<input checked="" type="checkbox"/>	▶ ⏸ 📄 🔄 ✖
Delete on bad integrity	If a file is created	Verify file integrity and delete on mismatch	January 19, 2023, 3:06 pm	December 14, 2022, 10:18 am	<input checked="" type="checkbox"/>	▶ ⏸ 📄 🔄 ✖
Check file integrity	If a file is created	Verify file integrity and generate admin alert on mismatch	June 20, 2022, 9:12 am	June 20, 2022, 9:12 am	<input type="checkbox"/>	▶ ⏸ 📄 🔄 ✖

Red arrows point to the edit (pencil) icon in the first row and the delete (X) icon in the second row.

Update Workflow ✕

Workflow Name

IF Condition ..

Required Parameters

```
{"parent_folder_path_string":"\\jennifer","number_of_days":7,"skip_recently_accessed":true,"exclude_recyclebin":true,"exclude":"*secret.*"}
```

THEN Action ..

Required Parameters

```
{"report_name":"my_report","comma_separated_email_id":"jennifer@example.com"}
```

▶ Execute
🔄 Update
✕ Cancel

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.

i The ability to run a workflow on demand, where the condition for trigger does not depend on a user action, is available in FileCloud Server version 18.1 and later.


Administrators can run a workflow on demand, where the condition for trigger does not depend on a user action. In previous versions, running a workflow on-demand is set up with condition "If a user's last login is older than.."

Update Workflow ✕

Workflow Name	<input type="text" value="Disable Not logged in users"/>
IF Condition ..	<input type="text" value="If a user's last login is older than .."/>
Required Parameters	<pre>{"last_login_days_ago": "30", "user_account_type": "USER_ACCOUNT_ANY", "day_interval": "5"}</pre>
THEN Action ..	<input type="text" value="Disable user account"/>
Required Parameters	<pre>{"comma_separated_email_id": "xyz@a.com,abc@b.com"}</pre>



Set Advanced Workflow Options

 The ability to create and run more advanced scenarios is available in FileCloud version 17.3 and later.

 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

By default FileCloud Workflow Conditions use *strict matching* in order to check the file/folder path. In 17.3 version a new feature was introduced to enable regular expressions utilisation. In order to enable regular expression match, administrator has to set the **use_regex** parameter to **"1"** in the condition definition. This is an optional parameter and by default will take the **"0"** value (don't use regular expressions - use strict match instead). If regular expressions are enabled administrator has to provide a valid regular expression pattern as the **parent_folder_path_string** value. This pattern will be used in the condition resolution process to find all matching paths (files / folders), for which the action should be run.

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 powerful 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 from 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 is a feature available in FileCloud from version 17.3. The idea behind the process is that conditions can 'publish' a set of additional parameters (or placeholders to be more precise) which can be later utilize in the action. It is not a default behavior and it has to be implicitly implemented by both: conditions and actions.

In the 17.3 version runtime resolved parameters are provided 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
- if the file updated is bigger than the expected size
- if the file downloaded is bigger than the expected size

and might be utilized in all compatible actions. The process works as follows:

1. Each condition may define a special set of placeholders that might be used as a part of the parameter definition in the compatible action.
2. After the condition is met FileCloud resolves values for each placeholder. It is done **at runtime** and might allow, i.e. dynamic path definitions.
3. Condition passes the resolved dictionary (placeholder - value pairs) to the action.
4. If any placeholder is used in the action parameter definition it is replaced with the resolved value.
5. Action executes normally with all parameters resolved at **runtime**.

Currently FileCloud supports placeholders only for the file/folder related conditions. The whole set contains:

- **%who** - user who performed the action that triggered the condition (i.e. file upload or download)
- **%when** - time of the action
- **%path** - path of the file / folder
- **%how** - user agent of the performed action (i.e. a browser type, etc.)
- **%filename** - name of the file

If selected condition implements runtime resolved parameters it will be reflected in the Action definition modal window:

Create New Workflow ✕

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "parameter name": "value"
}
```

Execute commandline. The must not be script is not long running or should perform operation in background.

command_line: Command line syntax to be executed.

Admin will be notified after running the command

```
{
  "command_line": "rm -rf /tmp/scratch"
}
```

Following placeholders are available for this action:
 %who, %when, %path, %how, %filename

← Previous
→ Next
✕ Cancel

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:

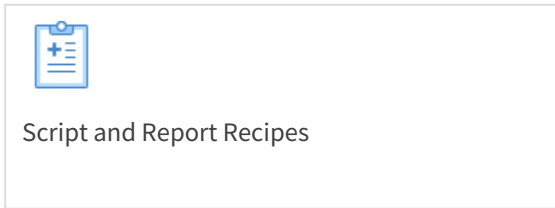
- IF CONDITION - THEN ACTION (IFTTT)

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

What do you want to do?

 File Management Recipes	<ul style="list-style-type: none"> ➔ Notify on Upload of a File ➔ Detect and Notify Files with Mismatched Signature ➔ Detect and Generate a List of Inactive Files ➔ Detect and Delete Inactive Files
 User Monitoring Recipes	<ul style="list-style-type: none"> ➔ Detect and Generate a List of Inactive Users ➔ Detect and Notify Inactive Users ➔ Detect and Disable Inactive Users
 Client Security Recipes	<ul style="list-style-type: none"> ➔ Require admin approval for all clients



- ➔ Perform periodic script
- ➔ Run a specific report and email the results
- ➔ Run workflows commands with /tmp paths in Linux systems

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.

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

This condition will be triggered the **first time** a client app connects to the server.
No additional parameter is required.
The client can be mobile app, drive app, sync app etc

[← Previous](#) [→ Next](#) [✕ Cancel](#)

6. click on Next, to give the THEN action

Create New Workflow ✕

Select the action to perform when the condition is triggered

THEN Action ..

[← Previous](#) [→ Next](#) [✕ Cancel](#)

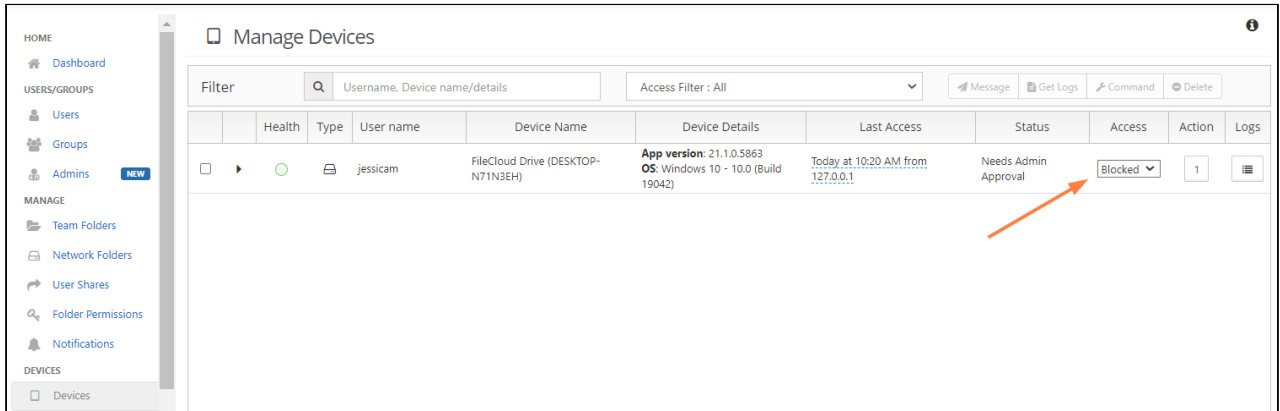
7. Click on Next, No workflow are required for this action

The screenshot shows a dialog box titled "Create New Workflow" with a close button (X) in the top right corner. A blue instruction bar at the top reads "Provide the required parameters for the action to be executed". Below this, the label "Required Parameters" is followed by a text area containing the JSON string `{ "parameter name": "value" }`. Underneath the text area, the text reads "Block the device and require admin to approve the device." and "No parameters are required for this action." At the bottom of the dialog, there are three buttons: "Previous" (with a left arrow), "Next" (with a right arrow), and "Cancel" (with an X icon).

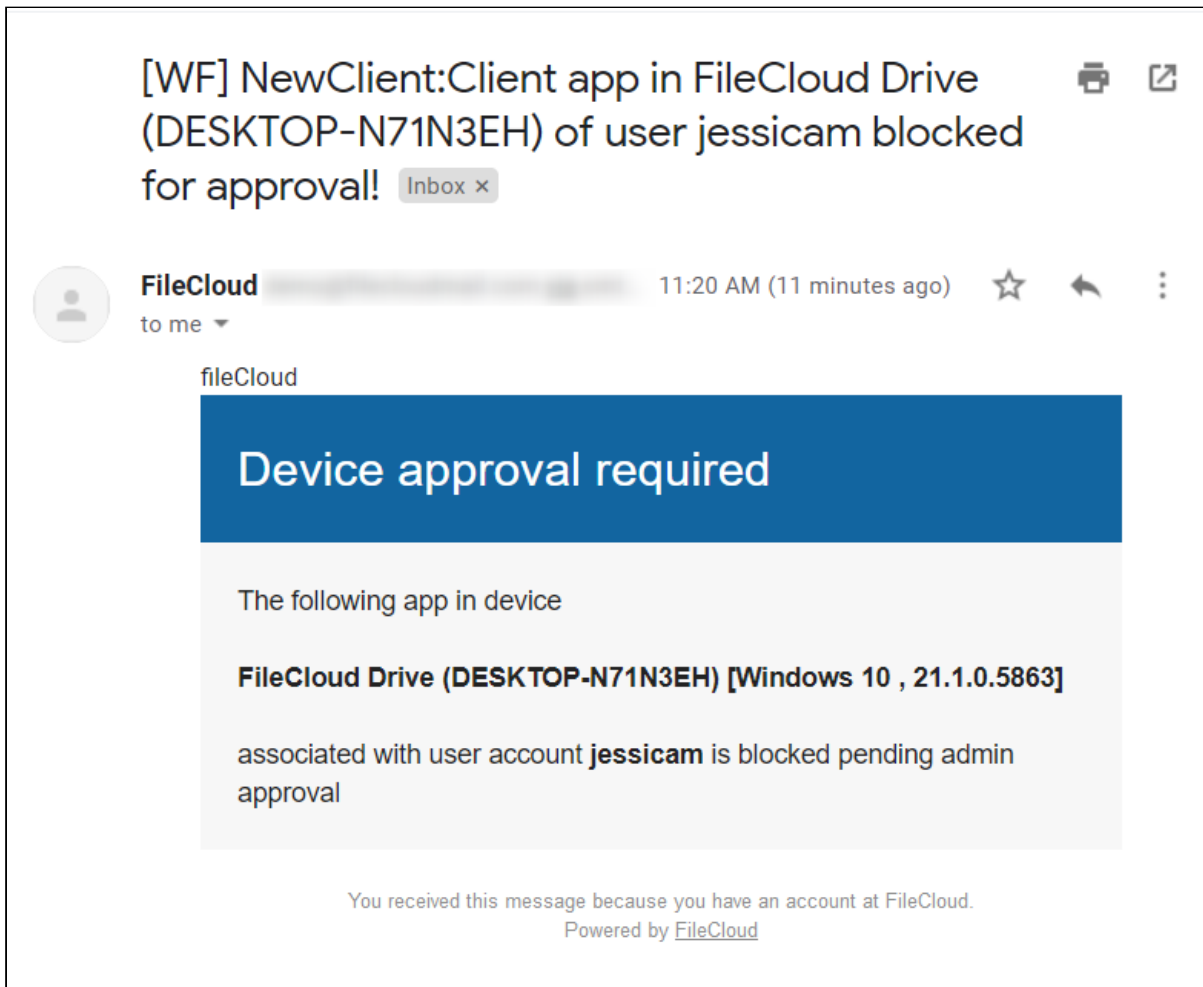
8. Click on Next, to give workflow name

The screenshot shows the same "Create New Workflow" dialog box. The blue instruction bar now reads "Name for this action". Below it, the label "Workflow Name" is followed by a text input field containing the text "Require admin approval for all clients". At the bottom of the dialog, the buttons are "Previous" (with a left arrow), "Finish" (with a right arrow), and "Cancel" (with an X icon).

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**.

The screenshot shows a 'Create New Report' dialog box. At the top, there is a blue header bar with the text 'Create New Report' and a close button (X). Below the header, there is a light blue box containing the text 'Select the report from the list'. Underneath this box, there is a label 'Select Report to Create' followed by a dropdown menu. The dropdown menu is open, showing the selected option 'Get user login report' with a downward arrow. At the bottom right of the dialog, there are two buttons: a blue button with a right arrow and the text 'Next', and a red button with an 'X' and the text 'Cancel'.

5. Enter the required time parameters to create the report.

Create New Report

Provide the required parameters for the report query in JSON format

Required Parameters

```
{  "from_date": "2023-01-01 00:00:00",  "to_date": "2023-01-21 23:59:59",}
```

Generate a report of login. If no parameters are supplied, last 7 days are retrieved by default.
from_date : (OPTIONAL) From date in Y-M-d H:i:s format.
to_date : (OPTIONAL) To date in Y-M-d H:i:s format.
last_number_of_hours : (OPTIONAL) Number of last hours from now.

If from_date is provided, then to_date is also required.
If last_number_of_hours is provided along with **from_date & to_date**, from_date & to_date will not be considered.

```
{  "from_date": "2020-01-01 00:00:00",  "to_date": "2020-01-01 23:59:59",  "last_number_of_hours": "24"}
```

[← Previous](#) [→ Next](#) [✕ Cancel](#)

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.

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{  
  "time_string": "16:45:05",  
  "day_interval": "1"  
}
```

This condition will be triggered when the current time matches the supplied time.
time_string : time in format H:i:s **day_interval** : Days interval (For daily operation, specify this value to be 1)

```
{  
  "time_string": "16:45:05",  
  "day_interval": "7"  
}
```

← Previous → Next × Cancel

10. Set the **THEN Action** as **Run a report**.

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action .. Run a report

← Previous → Next × Cancel

11. Specify the report name created previously and the emails of the users who will receive the report in the format given in the template.

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{  
  "report_name": "User Login Report",  
  "comma_separated_email_id": "liz@example.com,josh@example.com"  
}
```

Execute a saved report and send results.
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 executed

```
{  
  "report_name": "my_report",  
  "comma_separated_email_id": "a@x.com,b@y.com"  
}
```

← Previous → Next × Cancel

12. Save the workflow with an appropriate name.

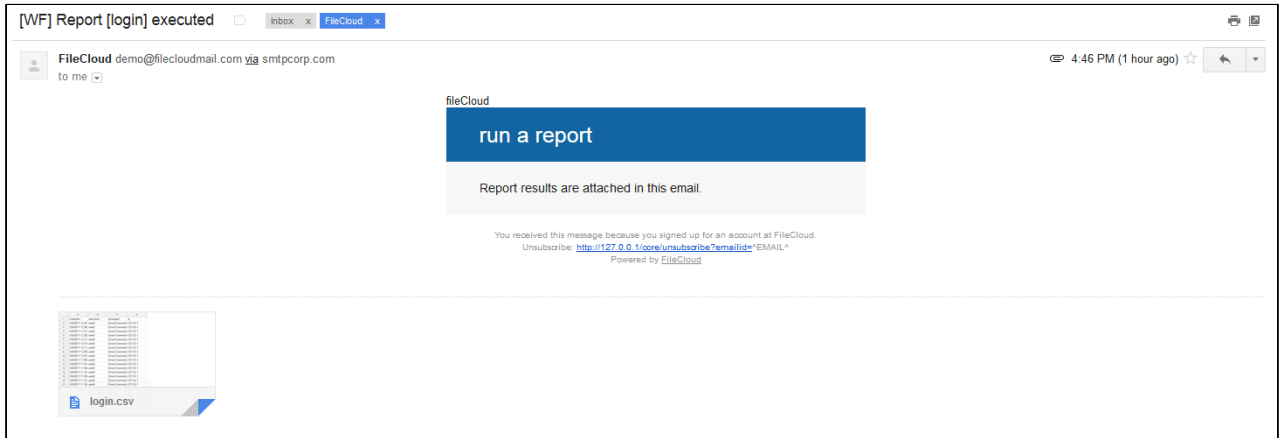
Create New Workflow

Name for this action

Workflow Name Run user login report

← Previous → Finish × Cancel

13. Once the workflow is run the report results are sent to the email ids specified.



- i** Similar workflows can be create 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.

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name":"value"
}
```

This condition will be triggered if a file was last modified the specified days ago. The check will run once a day.

parent_folder_path_string : Path of the folder containing the files as shown below.

number_of_days : Number of days since a file was modified.

skip_recently_accessed : (OPTIONAL) When TRUE, files viewed or downloaded within number_of_days will be treated as recently modified.

exclude_recyclebin : (OPTIONAL) When TRUE, files on recycle bin path will not be considered.

exclude : (OPTIONAL) Do not include files matching the regex in workflow, and do include files that don't match the regex in this workflow.

```
{
  "parent_folder_path_string": "/johndoe",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*"
}
```

For example:

```
{
  "parent_folder_path_string": "/johndoe",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*"
```

}

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.

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "parameter name":"value"
}
```

Delete files.

excluded_users (Optional): Users, whose files will be excluded from deletion. Names must be provided in a comma separated format as shown below

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 as shown below.

```
{
  "excluded_users":"user1,user2,user3",
  "delete_empty_folders":1,
  "notify_owner":0,
  "comma_separated_email_id":"email1@email.com,email2@email.com"
}
```

[← Previous](#) [→ Next](#) [✕ Cancel](#)

For example:

```
{
  "excluded_users":"abose",
  "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  
}
```


Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "last_login_days_ago": 30,
  "user_account_type":
"USER_ACCOUNT_ANY",
  "day_interval":1
}
```

This condition is triggered if a user's last login is older than specified days. This check will run once a day

last_login_days_ago: number of days ago.

user_account_type: Type of account. This can be
 USER_ACCOUNT_ANY
 USER_ACCOUNT_FULL_ACCESS
 USER_ACCOUNT_GUEST_ACCESS
 USER_ACCOUNT_LIMITED_ACCESS (external users)
 USER_ACCOUNT_DISABLED

day_interval: Days interval to perform the check (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

For example, to disable external access users who have not logged in for 30 days, set the following parameters:

```
{
  "last_login_days_ago": 30,
  "user_account_type": "USER_ACCOUNT_LIM
  "day_interval": 1,
  "skip_users_not_logged_in": true
}
```

← Previous

→ Next

✕ Cancel

- Click **Next**, and set the **Then Action** to "Disable user account".

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

← Previous → Next × Cancel

- 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.c  
om,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
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",  
  "donot_email_user": 0  
}
```

← Previous → Next × Cancel

8. Click **Next**, give an appropriate workflow name and click **Finish**.

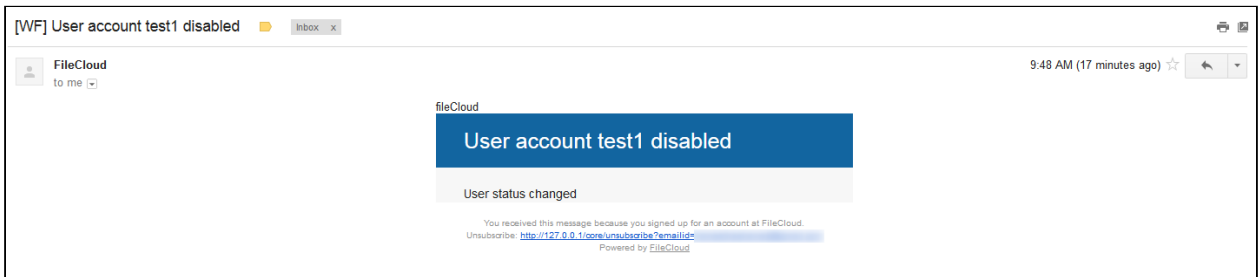
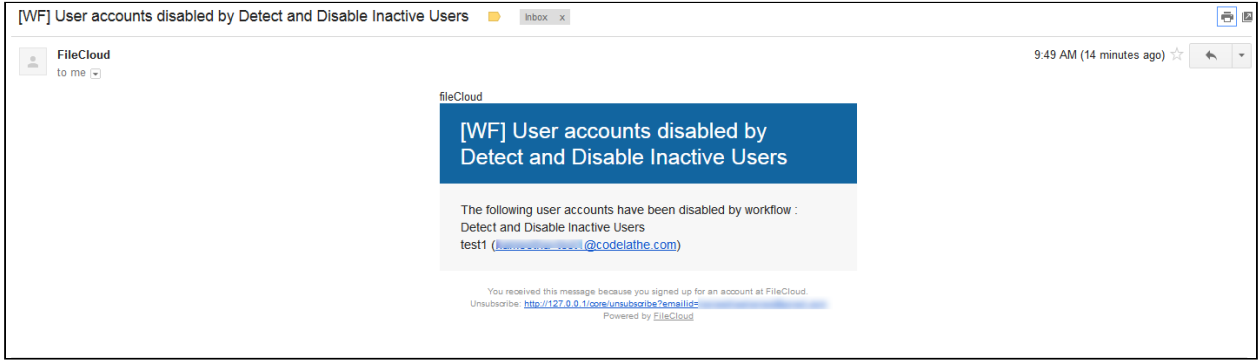
Create New Workflow

Name for this action

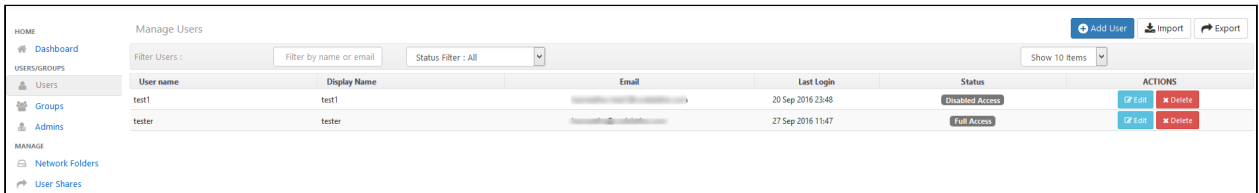
Workflow Name

← Previous → Finish × Cancel

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 for specified days**, and click **Next**.

Create New Workflow

Select the condition

IF Condition .. If file was not modified for specified days

→ Next × Cancel

5. Enter the parameters in the given format.

Create New Workflow
✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parameter name":"value"
}
```

This condition will be triggered if a file was last modified the specified days ago. The check will run once a day.

parent_folder_path_string : Path of the folder containing the files as shown below.

number_of_days : Number of days since a file was modified.

skip_recently_accessed : (OPTIONAL) When TRUE, files viewed or downloaded within number_of_days will be treated as recently modified.

exclude_recyclebin : (OPTIONAL) When TRUE, files on recycle bin path will not be considered.

exclude : (OPTIONAL) Do not include files matching the regex in workflow, and do include files that don't match the regex in this workflow.

```
{
  "parent_folder_path_string": "/johndoe",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*"
}
```

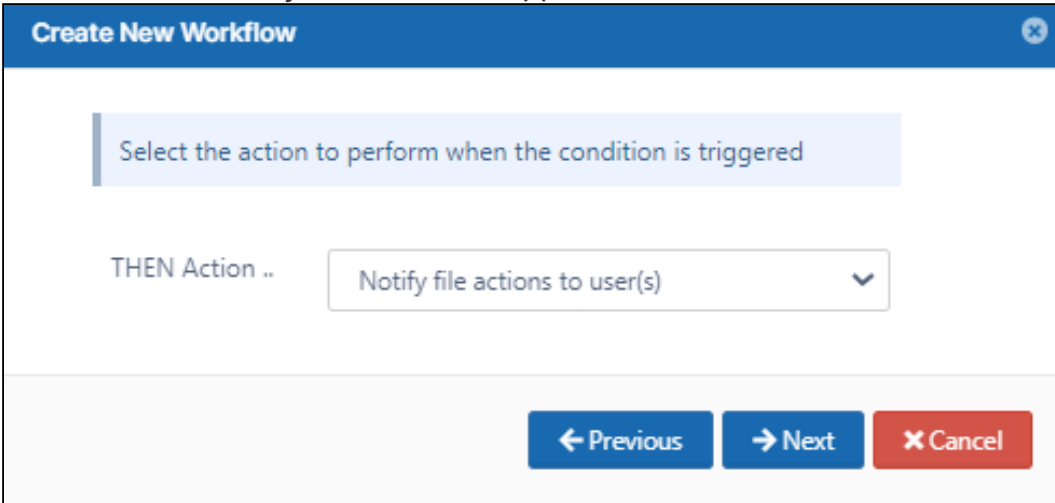
For example:

```
{
  "parent_folder_path_string": "/jenniferp",
  "number_of_days": 15,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
```

```
"exclude": ".*secret.*"
}
```

Note: This workflow applies only to Managed Storage and not to Network Folders.
To identify FileCloud specific path for a folder please refer to [Identifying a FileCloud Specific Path](#).

6. Click **Next**.
7. Set **THEN Action** to **Notify file actions to user(s)**.



8. Click **Next**.
9. Enter the parameters in the given format.
For example,

```
{
  "comma_separated_email_id": "lynnep@example.com"
}
```

Create New Workflow [Close]

Provide the required parameters for the action to be executed

Required Parameters

```
{  
  "lynnep@example.com"  
}
```

Send email.
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

- 10. Click **Next**.
- 11. Enter a **Workflow Name**, and click **Finish**.

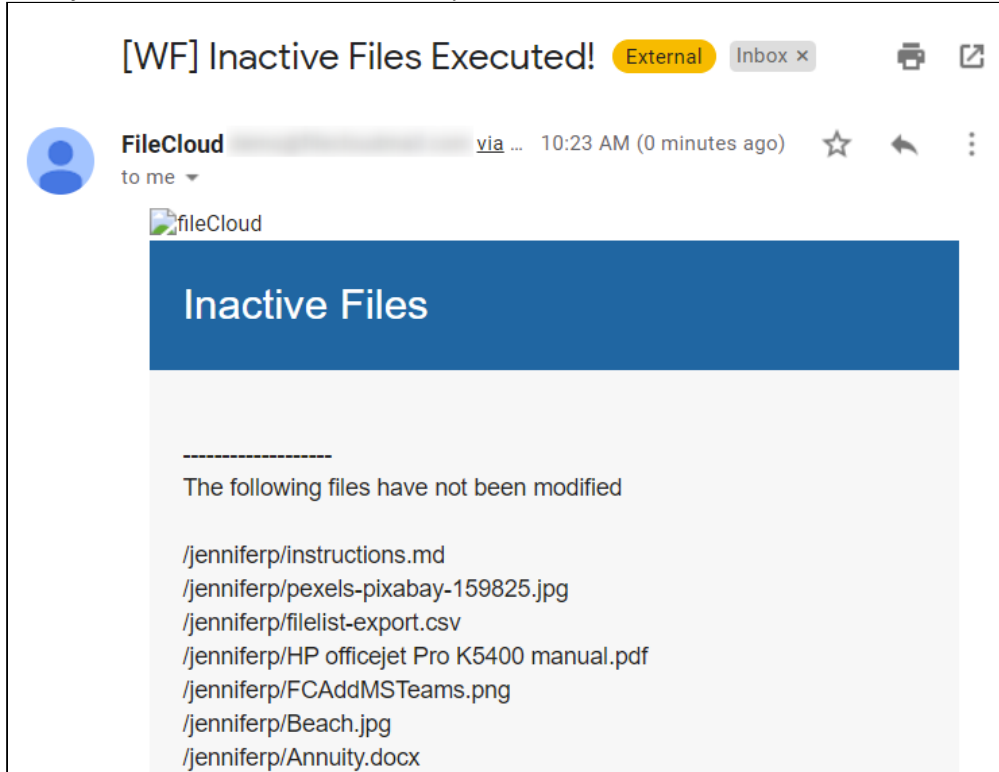
Create New Workflow [Close]

Name for this action

Workflow Name

← Previous → Finish × Cancel

When you run the workflow, the emails specified receive an email with a list of inactive files.



Detect and Notify Failed Signatures Workflow

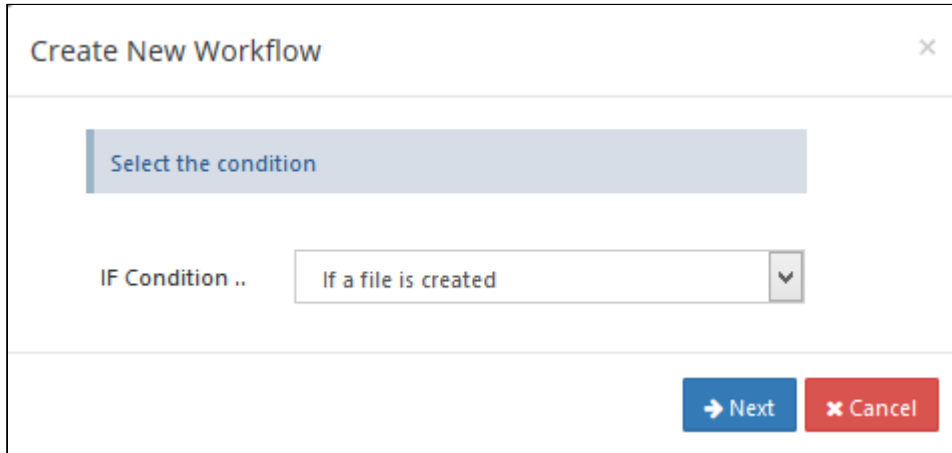
This workflow recipe creates an ALERT notification when a file is created or uploaded to FileCloud with a signature mismatch.

- 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**.




Create New Workflow

Select the condition

IF Condition .. If a file is created

Next Cancel

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.

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parent_folder_path_string":
  "/robert/SampleDocs"
}
```

This condition will be triggered when a file is created.

parent_folder_path_string: path of the folder as shown below

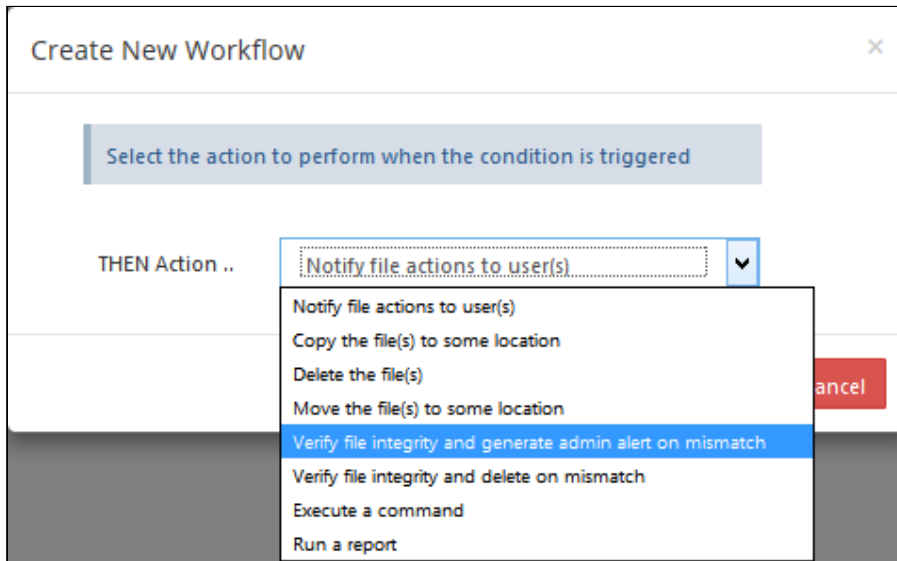
use_regex (optional): specifies whether path has a regex format

exclude (optional): exclude files matching the specified path from the action, and perform the action for all files that don't match the path.

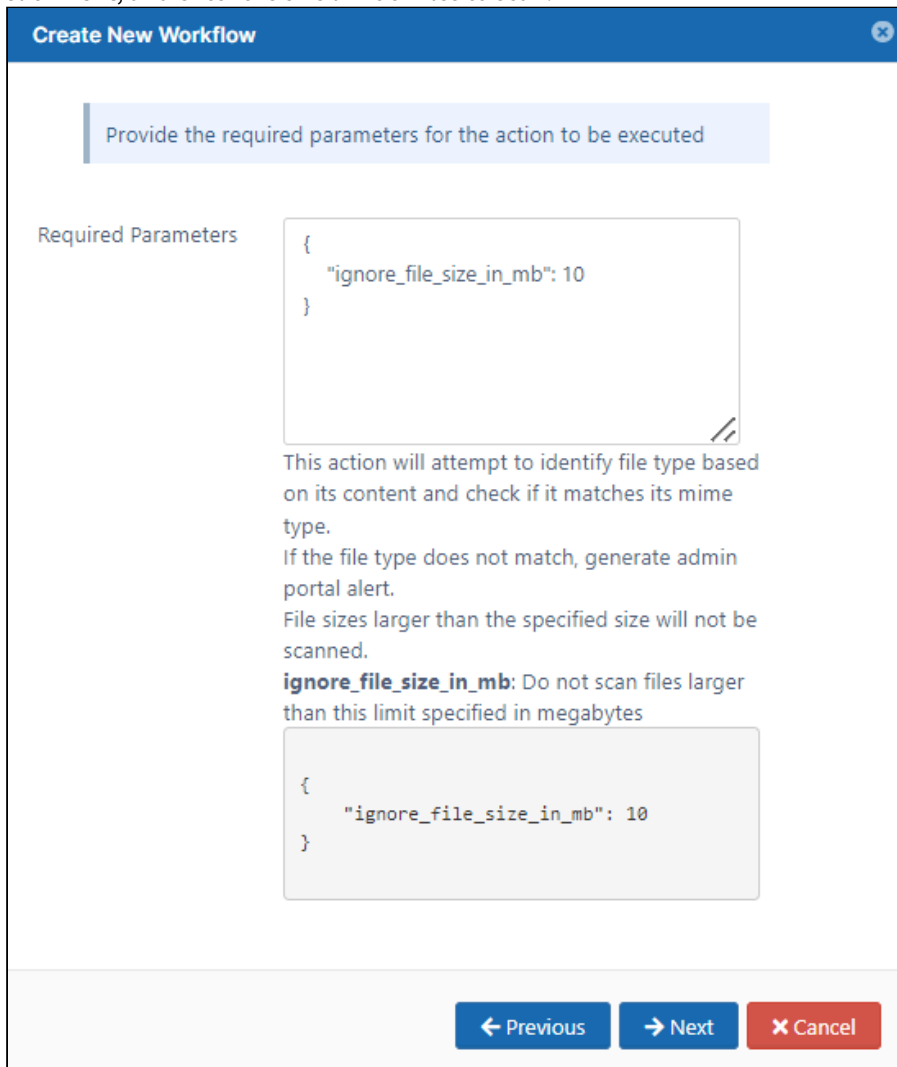
```
{
  "parent_folder_path_string": "/userid/
somepath",
  "use_regex": 1,
  "exclude": 1
}
```

← Previous → Next × Cancel

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.

Date	Severity	Description	ACTIONS
2016-Sep-26 02:26:58 AM	Warning	[Detect and notify signature variance] File /npriya/ioschk/doc scr3.klx created by npriya failed signature check. The content is not matching the file type extension.	More
2016-Sep-02 17:38:16 PM	Critical	ERROR 2016-09-02 17:38:16 1 Call to a member function getParametersForAction() on a non-object /var/www/core/framework/workflowcontroller.class.php:537	More
2016-Sep-02 17:37:19 PM	Critical	ERROR 2016-09-02 17:37:19 1 Call to a member function getParametersForAction() on a non-object /var/www/core/framework/workflowcontroller.class.php:537	More
2016-Aug-04 10:55:11 AM	Warning	[deletebadfile] File /anisad/upload/ss.jpg created by anisad failed signature check. The content is not matching the file type extension. File version deleted	More
2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg__128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More
2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg__800_xx_600 created by hameethatest failed signature check. The content is not matching the file type extension.	More
2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg__180_xx_180 created by hameethatest failed signature check. The content is not matching the file type extension.	More
2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter1.doc__180_xx_180 created by hameethatest failed signature check. The content is not matching the file type extension.	More
2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter1.doc__128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More
2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter.doc__128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More

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**.

Create New Workflow ✕

Select the condition

IF Condition .. ▼

➔ Next ✕ Cancel

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  
}
```

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "last_login_days_ago": 14,
  "user_account_type":
  "USER_ACCOUNT_LIMITED_ACCESS",
  "day_interval": 5,
  "skip_users_not_logged_in": 1
}
```

This condition is triggered if a user's last login is older than specified days. This check will run once a day

last_login_days_ago: number of days ago.

user_account_type: Type of account. This can be
 USER_ACCOUNT_ANY
 USER_ACCOUNT_FULL_ACCESS
 USER_ACCOUNT_GUEST_ACCESS
 USER_ACCOUNT_LIMITED_ACCESS (external users)
 USER_ACCOUNT_DISABLED

day_interval: Days interval to perform the check (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

For example, to disable external access users who have not logged in for 30 days, set the following parameters:

```
{
  "last_login_days_ago": 30,
  "user_account_type": "USER_ACCOUNT_LIMITED_ACCESS",
  "day_interval": 1,
  "skip_users_not_logged_in": 1
}
```

← Previous
→ Next
✕ Cancel

6. Click Next, set Then Action **Generate an email report**.

Create New Workflow ✕

Select the action to perform when the condition is triggered

THEN Action ..

← Previous → Next ✕ Cancel

7. Enter the Required parameters in the given format

```
{  
  "comma_separated_email_id":"admin@abc.com,hr@management.com"  
}
```

Create New Workflow
✕

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "comma_separated_email_id": "admn@abc.com,hr@management.com"
}
```

Send email with information about user. Does not change user's status.

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

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**

Create New Workflow ✕

Select the condition

IF Condition ..

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](#).

i Set the path to "/" if you want to monitor all the folders in the system.

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parent_folder_path_string":
  "/jenniferp/CustomerAccounts"
}
```

This condition will be triggered when a file is created or updated.

parent_folder_path_string: path of the folder as shown below

use_regex (optional): specifies whether path has a regex format

exclude (optional): exclude files matching the specified path from the action, and perform the action for all files that don't match the path.

```
{
  "parent_folder_path_string": "/userid/
somepath",
  "use_regex": 1,
  "exclude": 1
}
```

[← Previous](#) [→ Next](#) [✕ Cancel](#)

6. Set the then action to **Notify file actions to user(s)**, and click **Next**.

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

← Previous → Next × Cancel

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

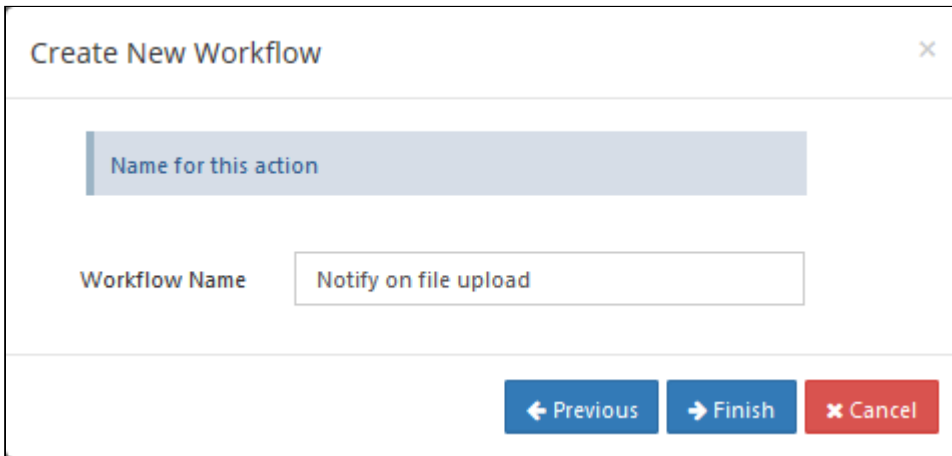
```
{  
  "comma_separated_email_id": "admin@abc  
company.com,hr@management.com"  
}
```

Send email.
comma_separated_email_id: Email ids in comma separated format as shown below

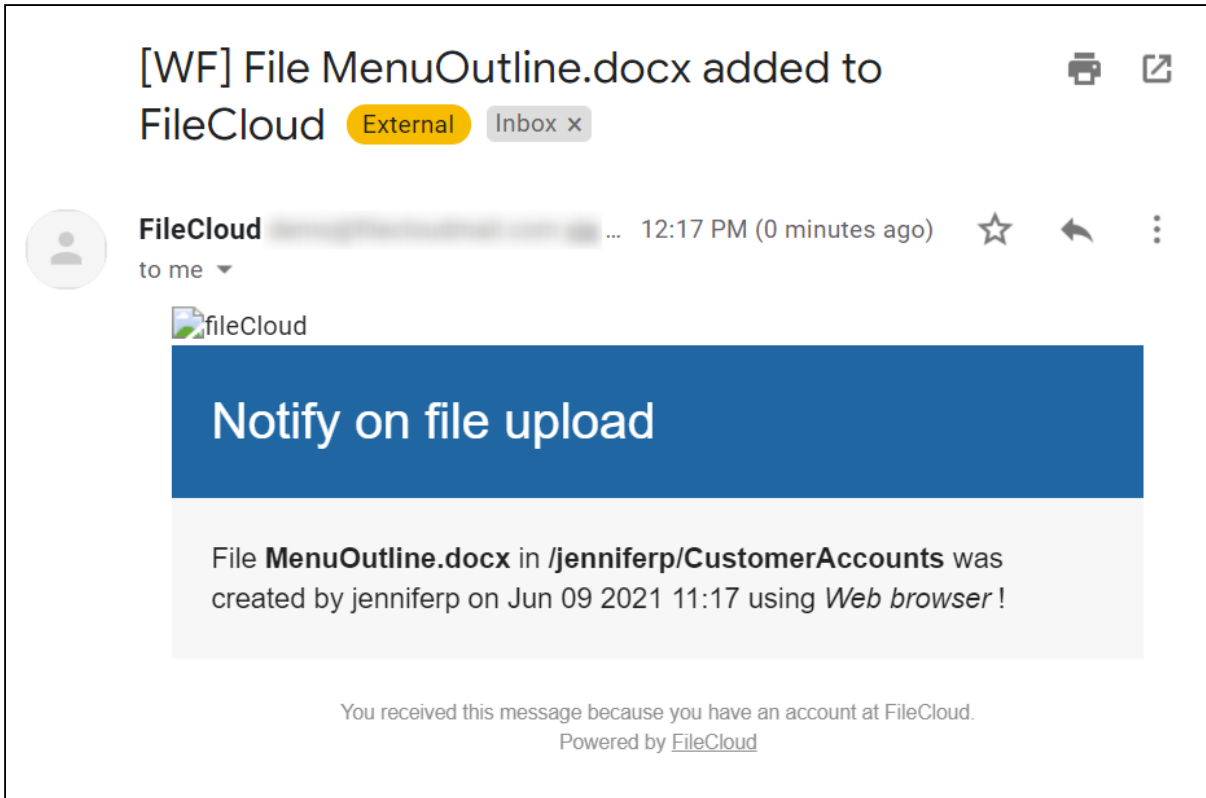
```
{  
  "comma_separated_email_id": "xyz@a.com,abc@b.com"  
}
```

← Previous → Next × Cancel

8. Click **Next**, then give an appropriate workflow name and click **Finish**.



9. Sample notification email on a file upload.



Periodic Script Workflow

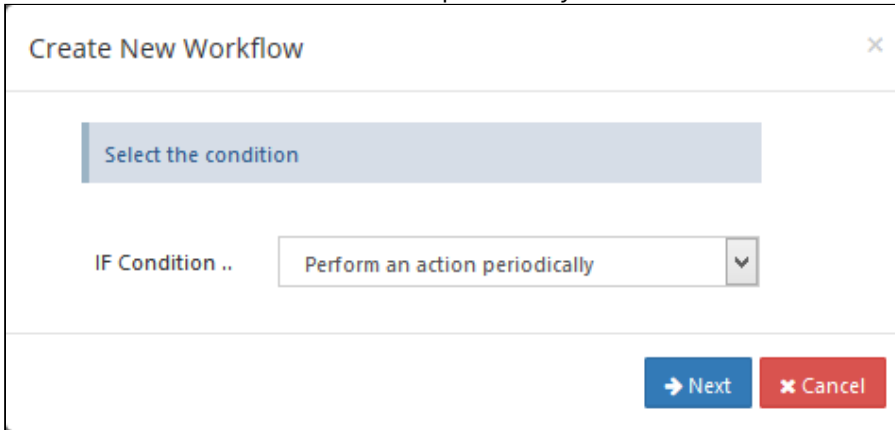
This workflow recipe runs a specified command at a periodic interval.

- 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

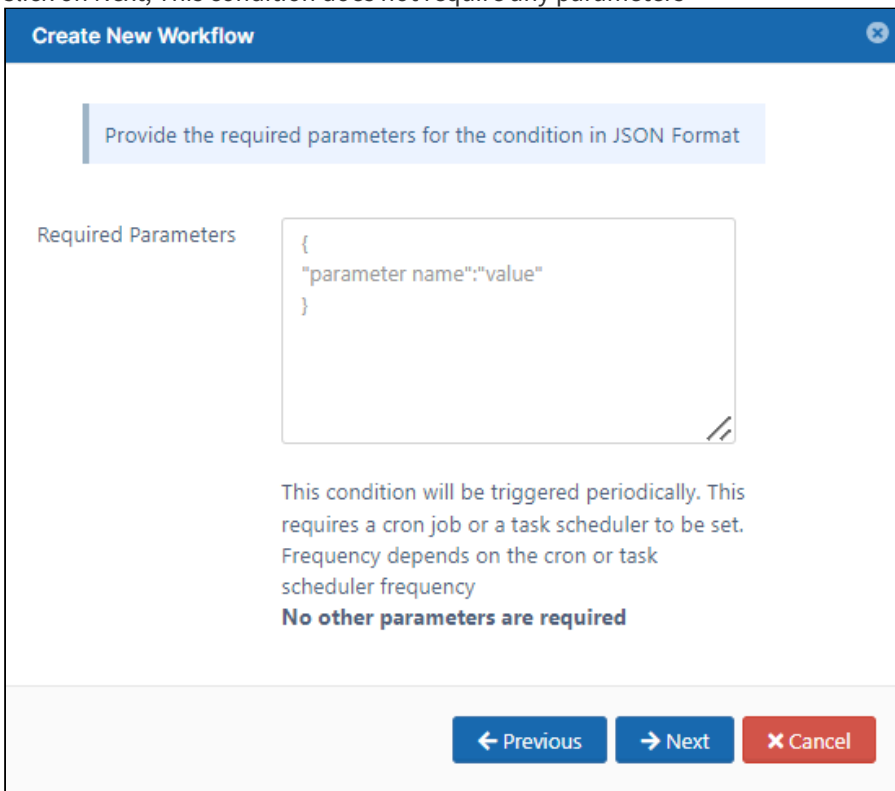
To create a workflow that performs a periodic script:

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 "



The screenshot shows a modal window titled "Create New Workflow" with a close button (X) in the top right corner. Below the title bar, there is a light blue instruction box that says "Select the condition". Underneath, the text "IF Condition .." is followed by a dropdown menu that has "Perform an action periodically" selected. At the bottom right of the modal, there are two buttons: a blue "Next" button with a right-pointing arrow and a red "Cancel" button with a white X.

5. Click on Next, This condition does not require any parameters

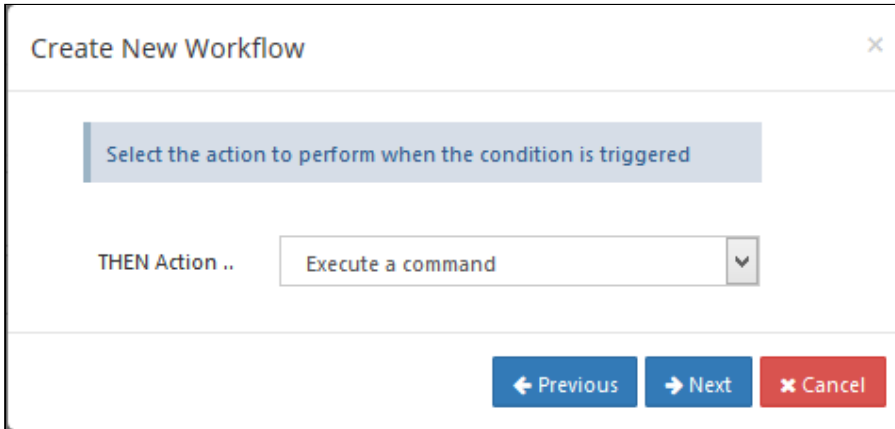


The screenshot shows the next step in the "Create New Workflow" modal. The title bar is blue with the text "Create New Workflow" and a close button (X). Below the title bar, there is a light blue instruction box that says "Provide the required parameters for the condition in JSON Format". Underneath, the text "Required Parameters" is followed by a text area containing the JSON code:

```
{  
  "parameter name": "value"  
}
```

. Below the text area, there is a note: "This condition will be triggered periodically. This requires a cron job or a task scheduler to be set. Frequency depends on the cron or task scheduler frequency". Below the note, there is a bolded text: "No other parameters are required". At the bottom of the modal, there are three buttons: a blue "Previous" button with a left-pointing arrow, a blue "Next" button with a right-pointing arrow, and a red "Cancel" button with a white X.

6. Set the Then Action "Execute a command"



The screenshot shows a dialog box titled "Create New Workflow" with a close button (X) in the top right corner. Below the title bar, there is a blue instruction bar that says "Select the action to perform when the condition is triggered". Underneath, the label "THEN Action .." is followed by a dropdown menu that currently displays "Execute a command". At the bottom of the dialog, there are three buttons: "Previous" (with a left arrow), "Next" (with a right arrow), and "Cancel" (with an X icon).

7. Enter the required Command

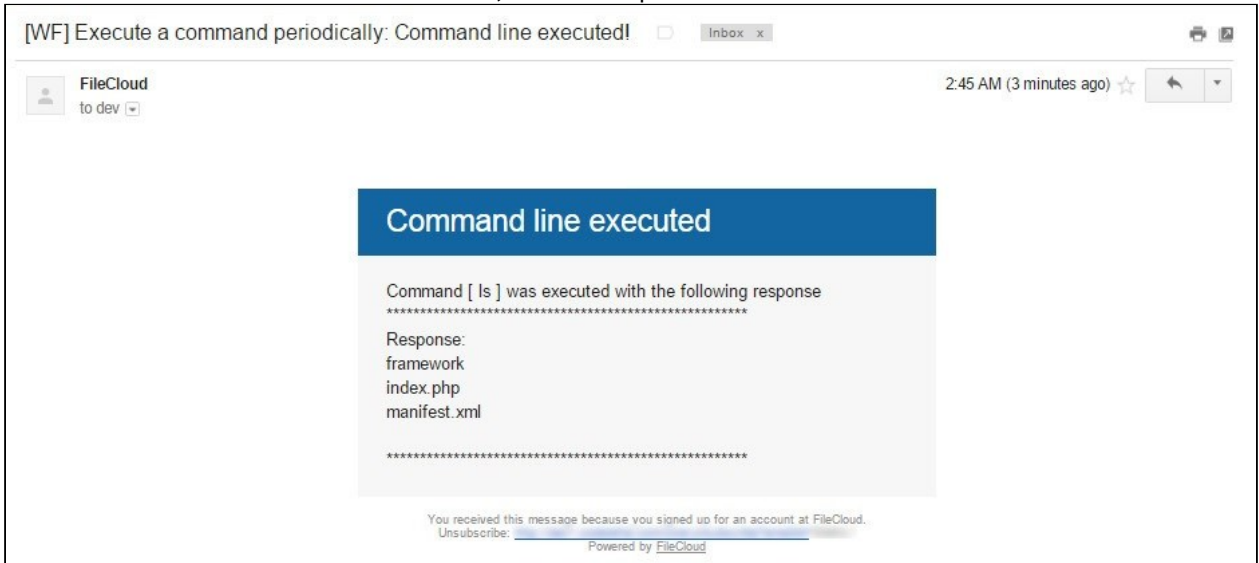
```
eg:-  
{  
  "command_line":"ls"  
}ls - will list all the folders and files.
```

8. Enter the Workflow name and Finish.




The screenshot shows the same "Create New Workflow" dialog box. The blue instruction bar now says "Name for this action". Below it, the label "Workflow Name" is followed by a text input field containing the text "Execute a command periodically". At the bottom, the buttons are "Previous" (with a left arrow), "Finish" (with a right arrow), and "Cancel" (with an X icon).

9. A notification email will be sent to the Admin, with the response information of command line execution.



Automated Workflow Management

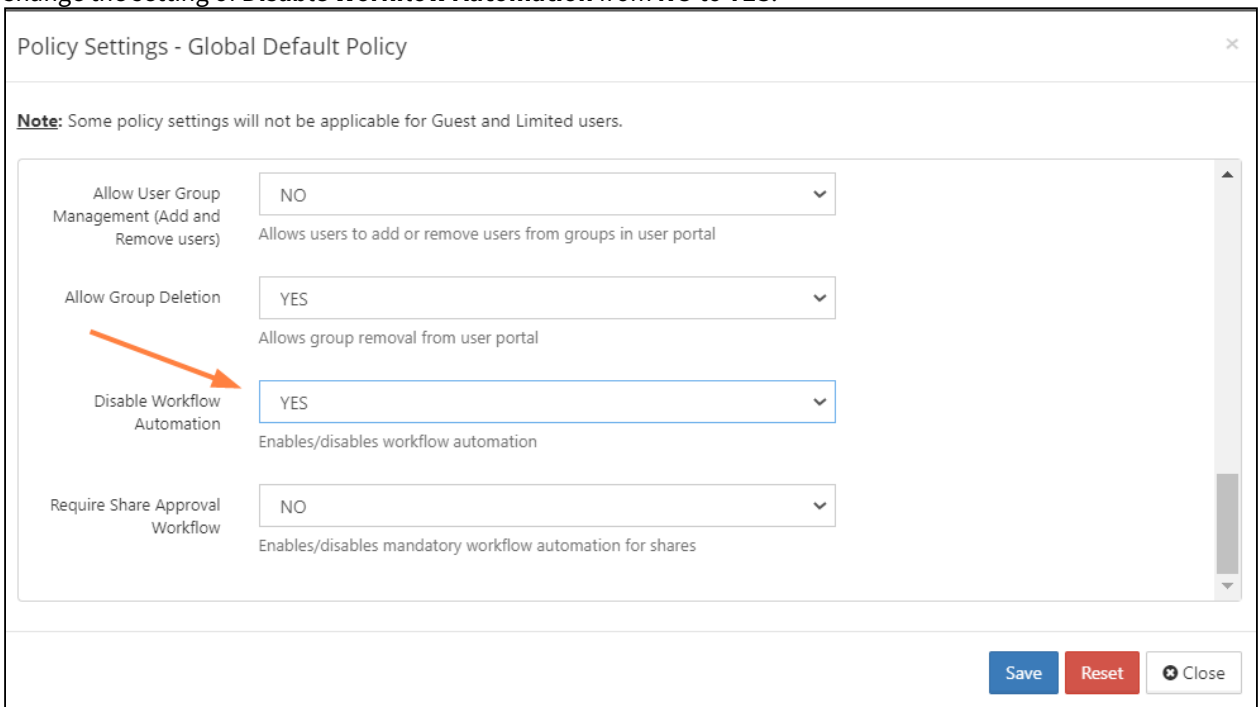
 Automated Workflows are available in FileCloud 21.2 and later.

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 Admin portal, go to **Settings > Policies**.
2. Open the policy assigned to the users, and click the **User Policy** tab.
3. Change the setting of **Disable Workflow Automation** from **NO** to **YES**.



Policy Settings - Global Default Policy

Note: Some policy settings will not be applicable for Guest and Limited users.

Allow User Group Management (Add and Remove users)	NO	Allows users to add or remove users from groups in user portal
Allow Group Deletion	YES	Allows group removal from user portal
Disable Workflow Automation	YES	Enables/disables workflow automation
Require Share Approval Workflow	NO	Enables/disables mandatory workflow automation for shares

Save Reset Close

4. Click **Save**.
The **Workflows** navigation link no longer appears in the user portal of users assigned to the policy.

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 require approval for all of the policy's users, the Share Approval workflow creator must be a [promoted Admin](#) with all User Share permissions enabled. If the Share Approval workflow creator is not a promoted Admin with all User Share Permissions enabled, only the creator's shares will require approval.

In addition, in order to approve the shares, the share approver(s) specified in a Share Approval workflow (in **Approver Emails**) must be promoted Admins with all User Share permissions enabled. Please confirm this before choosing the workflow as the **Selected Workflow**.

1. In the Admin portal, go to **Settings > Policies**.
2. Open the policy assigned to the users, and click the **User Policy** tab.
3. Change to setting of **Require Share Approval** from **NO** to **YES**.
4. In **Selected Workflow**, choose the Share Approval workflow to make effective.

Policy Settings - Global Default Policy ✕

Note: Some policy settings will not be applicable for Guest and Limited users.

Allow Group Deletion	<input type="text" value="YES"/> <div style="font-size: 0.8em; margin-top: 2px;">Allows group removal from user portal</div>
Disable Workflow Automation	<input type="text" value="NO"/> <div style="font-size: 0.8em; margin-top: 2px;">Enables/disables workflow automation</div>
Require Share Approval Workflow	<input type="text" value="YES"/> <div style="font-size: 0.8em; margin-top: 2px;">Enables/disables mandatory workflow automation for shares</div>
Selected Workflow	<input type="text" value="Share approval"/> <div style="font-size: 0.8em; margin-top: 2px;">Selected automation workflow for shares</div>

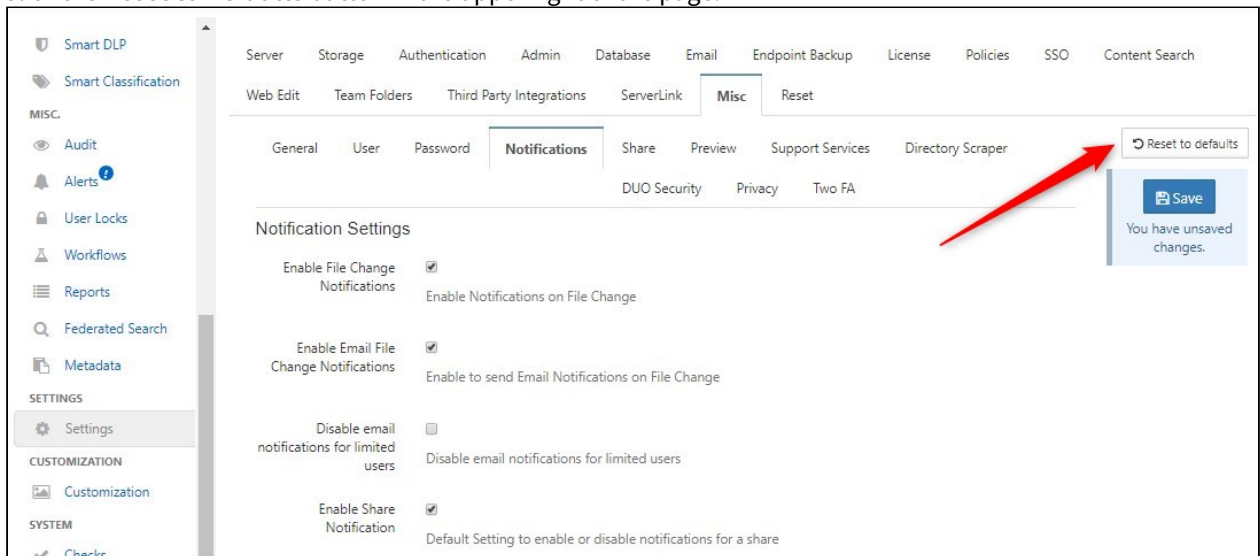
For end user information on creating Automated Workflows, see [Workflow Automation](#).

Reset Settings and Customizations

- i** 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 on a Settings or Customization tab

1. In the navigation pane, click Settings or Customization.
2. Click the setting or customization type tab.
If there are sub-tabs, click a sub-tab.
3. Click the **Reset to Defaults** button in the upper right of the page.



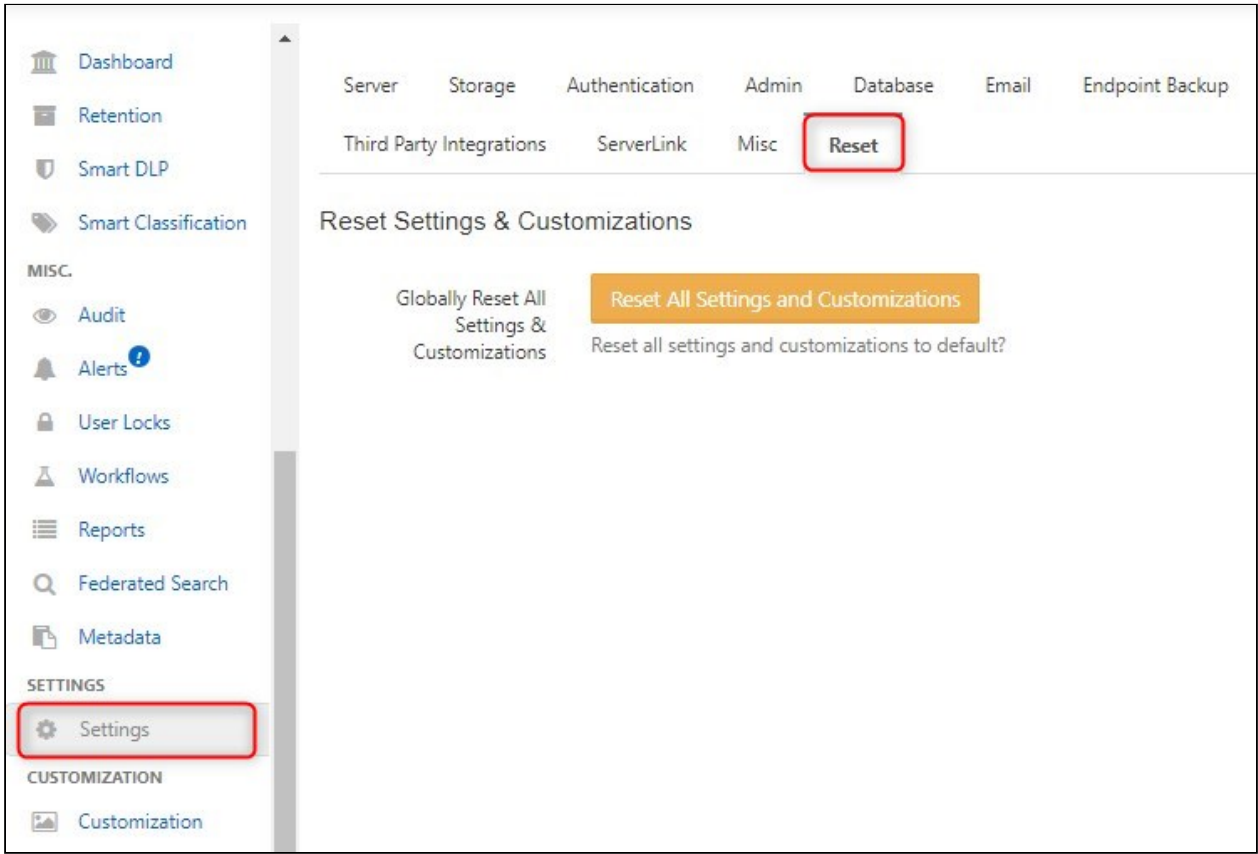
A confirmation dialog box opens.

4. Click **OK**.
The settings on the main tab and the settings on all its the sub-tabs are set back to their default settings. (This is true even if you have clicked **Reset to Defaults** from a sub-tab. The options on its parent tab and all of its sibling tabs are reset to their defaults.).

To return to default settings for all options on the Settings and Customization pages:

1. In the navigation pane, click **Settings**.

2. Click the Reset tab.



3. Click **Reset All Settings and Customizations**.
A confirmation dialog box opens.
4. Check **Confirm** and continue with the reset.
All of the options that appear on the Settings and Customization pages are reset to their defaults.