



FileCloud Server 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	9
Setup Checklist	9
Quick Actions.....	10
Dashboard Widgets.....	11
Release Notifications	23
By Subscribing to the Mailing List	23
By seeing the version update in the FileCloud Admin Portal.....	23
Upgrade FileCloud	24
Upgrade using Admin Portal	30
Upgrade using Update Tool (Windows Only)	35
Backup FileCloud Before Upgrading.....	47
Upgrade FileCloud on Linux	47
Managing Users	49
Listing FileCloud Users	49
Viewing User Properties.....	50
Disable a FileCloud User Account.....	60
Deleting a FileCloud User	63
Resetting a User Password	66
Manage A User's Policies	68
Manage a User's Profile Picture.....	71
Change a User's Email Address	72
Setting a User Account to Expire.....	72
Send Email from User Details	73
Managing Groups	75
Change a User Group Name	75
Delete a User Group	75

View and Change Group Members	76
Exporting a list of users in a group	77
Managing Admin Users	79
Check an admin user's permissions.....	79
Remove an admin role.....	83
Managing User Folders and Files.....	86
What do you want to do?	87
Copy and Move User Files.....	87
Download User Files and Folders.....	90
Cancel User Uploads in Progress.....	92
Delete User Folders and Files	93
Clear a Recycle Bin	94
Remove a User's Old File Versions	97
Remove Incomplete User Uploads.....	98
Restore a Previous File Version	100
Critical Section Cleanup Tool	102
Change the Name of the Zip File for Multiple File Downloads.....	105
Managing User Shares	107
To manage user shares for an individual user:.....	107
To manage user shares for all users:.....	109
To export a list of all shares:	110
Transfer Ownership of a Reshare from a Team Folder or Network Share	111
Creating direct file download link from a public file share.....	114
Creating direct file download links from a public folder share	114
Managing Storage Space Usage	117
In this section	117
Related topics.....	117
Storage Scanner Tool for Missing Files	118
Storage Usage Tool.....	119
Managing User Locks	120

Managing User-Defined Notifications	124
Editing individual user's file and folder notifications	124
Editing all users file and folder path notifications	127
Adding notifications for actions on user's files and folders	129
Managing Client Devices.....	132
FAQ's	133
How Do You Want to Manage a Device?	134
Centralized Device Management	138
iOS Device Management	195
Mass Deployment - Default Configuration Support	196
Search in the Admin Portal.....	209
FileCloud's Federated Search.....	209
All search	211
Audit Logs.....	220
What do you want to do?	220
View Audit Logs	220
Filter Audit Log Views.....	222
Compact the Audit Database.....	224
Configure What is Logged	225
Export Audit Logs	227
Delete Audit Log Entries	227
Change the Audit Log Warning Limit.....	235
Backing Up and Restoring FileCloud Server	237
What do you want to do?	237
The FileCloud Server Backup Tool	237
Backing Up and Restoring Linux	267
FileCloud Backup and Restore - Linux Tool	267
FileCloud Backup and Restore - Linux Manual	274
FileCloud Backup and Restore - Windows Manual	277
Migrating FileCloud Server to Another Server	279

Migrating a FileCloud Server Site	282
Enabling the Backup Server URL.....	283
Monitoring FileCloud	284
What do you want to do?	284
FileCloud Alerts	286
File Content Heuristic Engine	287
Identifying a FileCloud Specific Path	292
Custom Reports.....	294
Add Reports	294
Download Reports	297
Available Reports	297
Specifying Y-M-d H:i:s values	304
Manage Folder Level Permissions	306
To Edit Folder Level Security	306
Read Only Sync.....	308
Managing Metadata	309
Metadata for governance and other system processes	309
Metadata for users	311
Metadata Components and Types	312
Create a New Metadata Set	316
Edit an Existing Metadata Set.....	319
Managing Metadata Attributes	322
Managing Metadata Permissions	325
Video of Managing Metadata	329
Working with Built-In Metadata	330
Working with Custom Metadata	347
Working with Default Metadata.....	348
Troubleshooting Metadata	351
Finding files without metadata	352

Metadata Limitations/Recommendations.....	356
Managing FileCloud Licenses	358
FileCloud - License Purchase And Renewal	358
Install FileCloud License	377
Workflows - IFTTT	383
The Workflow Dashboard	383
Add a New Workflow	384
Define an IF Condition	385
Define a THEN Action	410
Edit a Workflow	426
Run a Workflow	427
Set Advanced Workflow Options.....	428
Workflow Recipes for FileCloud	434
Troubleshooting Workflows	475
Automated Workflow Management	478
Disabling Automated Workflows.....	478
Requiring a Share Approval Workflow	478
Reset Settings and Customizations	480
To return to default settings for options on a Settings or Customization tab.....	480
To return to default settings for all options on the Settings and Customization pages:	480

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](#)
- [Upgrade FileCloud](#)
- [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](#)
- [Backing Up and Restoring FileCloud Server](#)
- [Monitoring FileCloud](#)
- [FileCloud Alerts](#)
- [File Content Heuristic Engine](#)
- [Identifying a FileCloud Specific Path](#)
- [Custom Reports](#)
- [Manage Folder Level Permissions](#)
- [Read Only Sync](#)
- [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.

The screenshot displays the FileCloud Admin Dashboard. On the left is a 'Navigation panel' with categories like HOME, DASHBOARD, USERS / GROUPS, MANAGE, DEVICES, GOVERNANCE, and MISC. The main area is titled 'Admin Dashboard' and features a 'Quick actions' ribbon with buttons for 'Add Users', 'Add Group', 'Add Network Shares', 'Add Admin', and 'Alerts'. A 'Setup checklist' button is in the top right. The dashboard contains several widgets: 'System Summary' with a line graph showing served requests; 'Quota Usage' (N/A); 'Temp Disk Usage' (481.47 GB used, 226.38 GB free); 'License Usage' (19 of 20 total); 'Statistics' table; 'Governance' table; 'Realtime DLP Statistics' table; and 'License Information' table. Red arrows labeled 'Widgets' point to the License Usage and License Information widgets.

Category	Count
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

Category	Count
Compliance	2/3
DLP Rules	10
Retention	0

Category	Count
Active Downloads	0
Active Uploads	0
Active Shares	0

Category	Count
Licenses	19 Used / 20 Total
License Expiry	31-Aug-2023

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.

This close-up shows the top header of the Admin Dashboard. It features the 'Admin Dashboard' title on the left and a 'Setup Checklist' button on the right, indicated by a red arrow. Below the header is a 'Quick actions' ribbon with buttons for 'Add Users', 'Add Group', 'Add Network Shares', 'Add Admin', and 'Alerts', along with a 'More' button.

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.

Setup Checklist

Basic

- Basic Installation Completed
- Setup 'My Files' Storage (Local or S3 or OpenStack)
- Setup Email Configuration

Authentication

- Configure How Users are Authenticated (Local or AD or LDAP)
- Configure New Account Signup Policy
- Configure New Account Approval Policies

Network Shares

- Enable or Disable Network Folder Access
- Enable or Disable offline Sync of Network Folders
- Setup NTFS Helper Service (for NTFS file permissions)

Sync and Backup

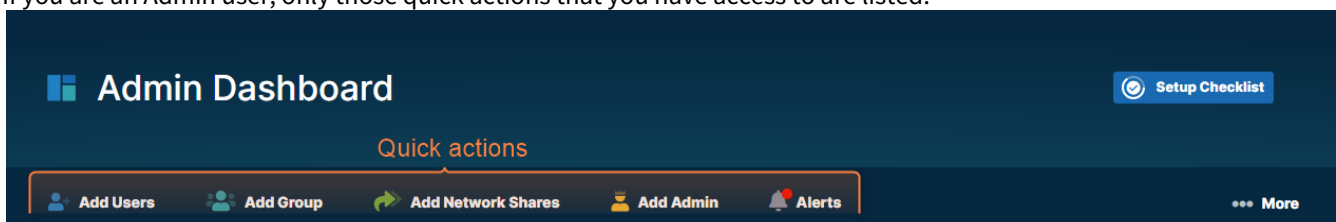
Save Close

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

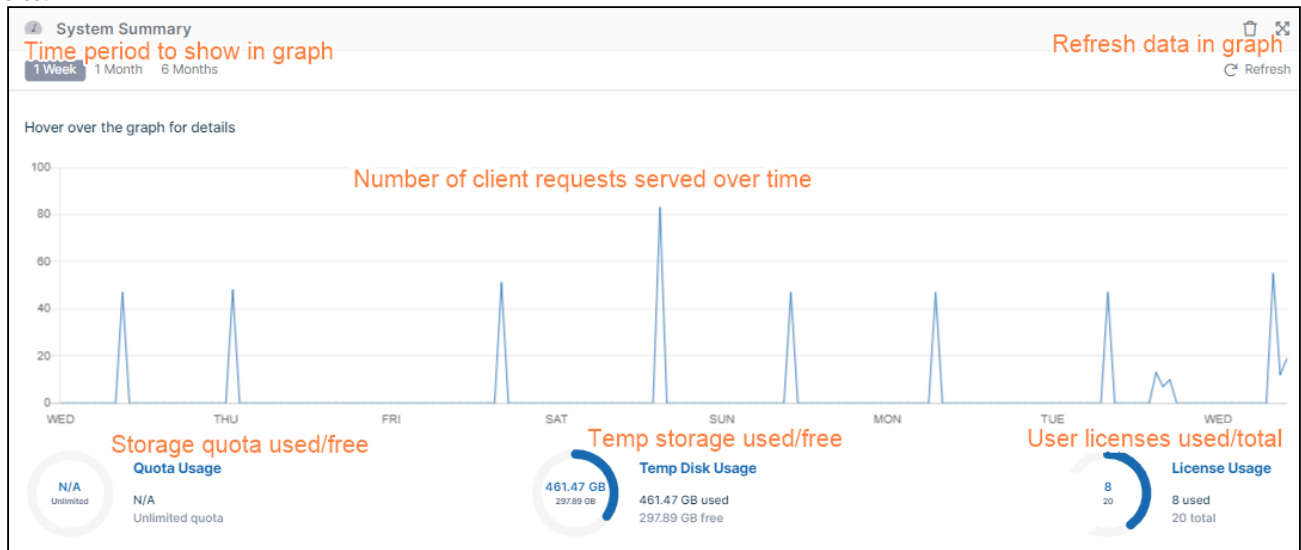
The FileCloud dashboard has widgets that display real-time information. If you are an Admin user, only those widgets involving actions you have access to are listed.

- 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

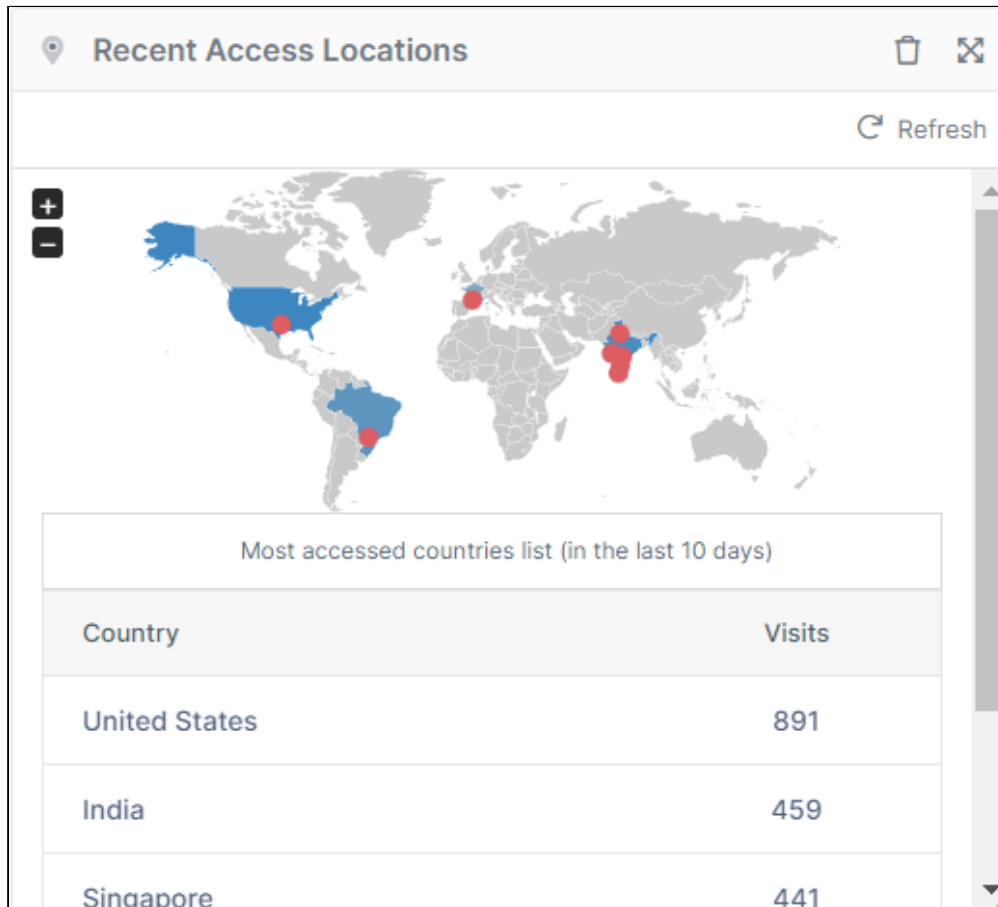
This widget shows you basic information about your license.

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.

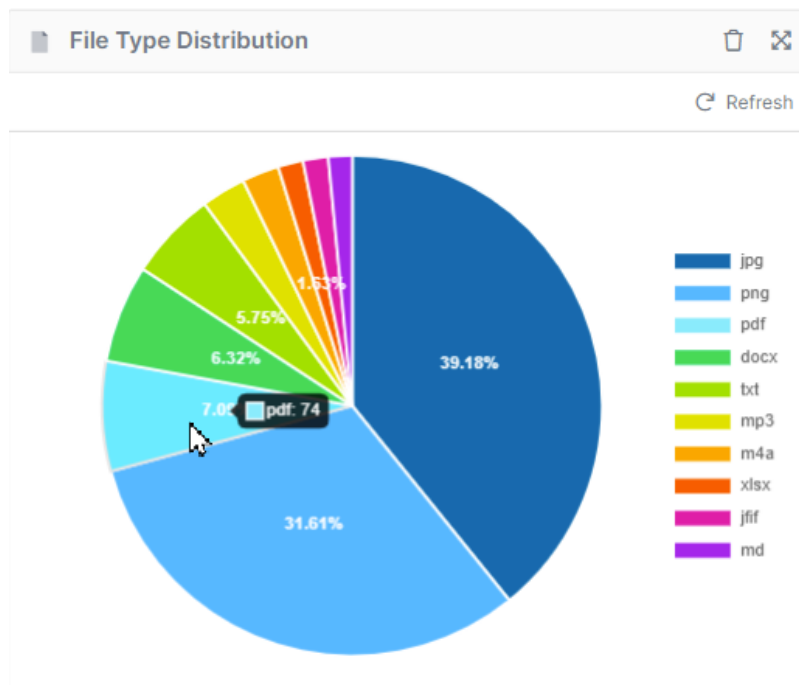
Settings	Value
Show Geo IP Report	TRUE - Show the Geo IP Map with data FALSE - Hide the Geo IP Map from the dashboard DEFAULT - Show the Geo IP Map with no data.
Geo IP Server URL	Server URL that converts the IP address to Geo Location Data. Default URL: http://geoiplookup.codelathe.com/geoip.php To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

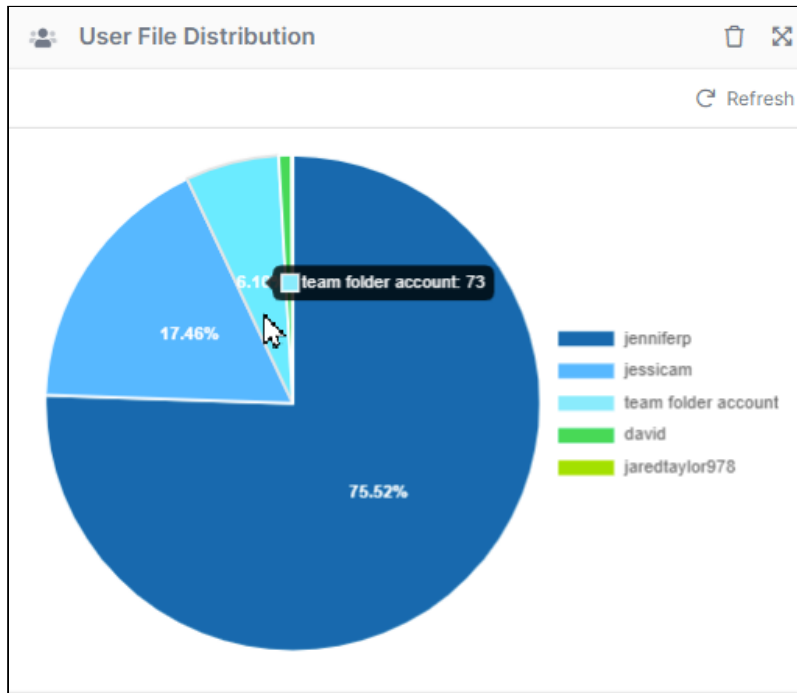
File Type Distribution

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**.

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

ServerLink

The **ServerLink** widget is available to customers who have ServerLink running. It gives you a quick view of the status of your ServerLink servers and is similar to the Status tab in the [ServerLink settings screen](#).

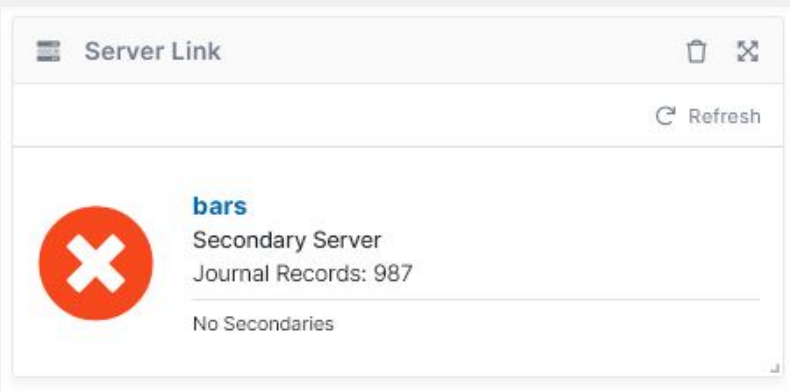
ServerLink enables your primary servers and one or more secondary servers that you have in other locations to sync with each other. The widget appears differently depending on whether you are using the primary server or a secondary server.

User signed into a primary server.



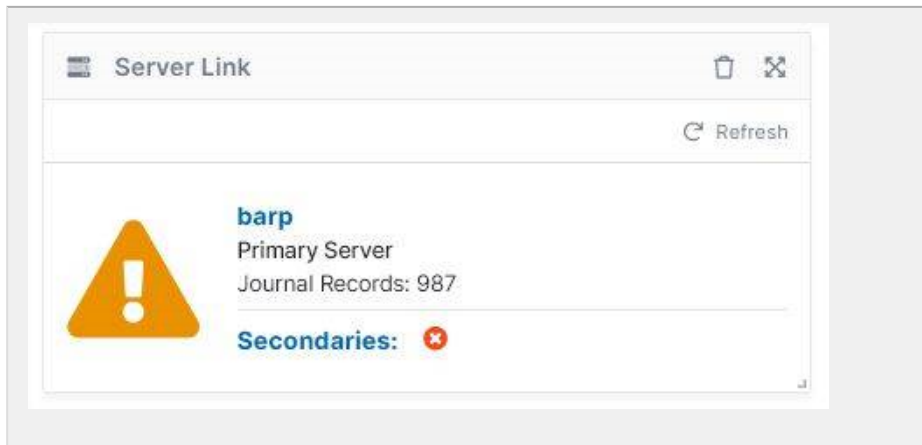
This is the way the ServerLink widget appears for a primary server with one secondary server. The check mark with a green background indicates that the server is running.

User signed into a secondary server.



This is the way the ServerLink widget appears for a secondary server with an additional secondary server running. The x with a red background indicates that the server is not running.

User signed into a primary server.



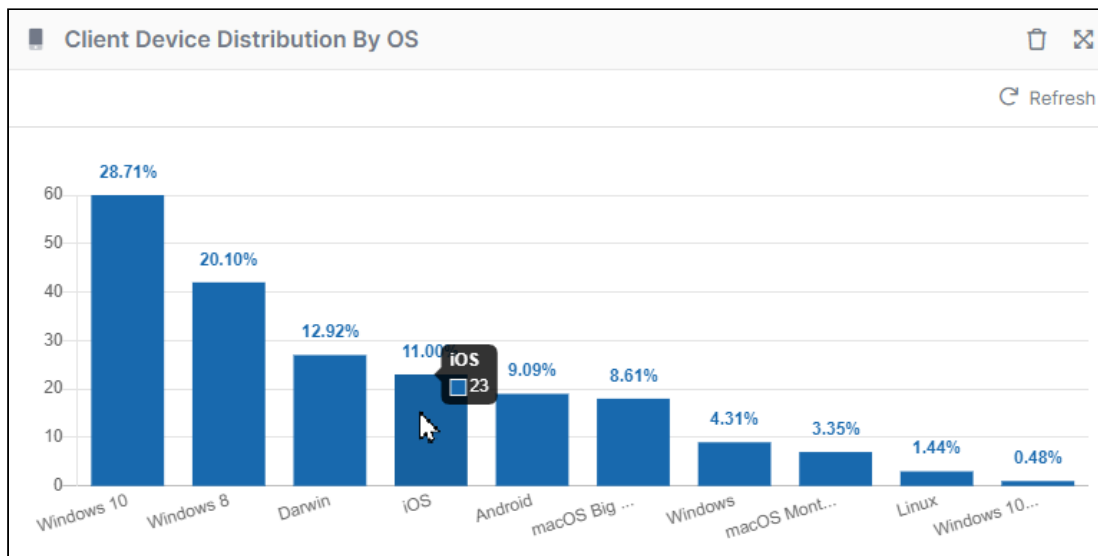
This is the way the ServerLink widget appears for a primary server when the secondary server is not syncing with it. The primary server displays a exclamation mark with a yellow background.

Journal Records indicates the number of log entries for ServerLink syncing actions.

For more information, see [Viewing ServerLink Information](#).

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.

Users with Lowest Quota Remaining					
Refresh					
	% 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
		edttaylor978	1	523 KB	2 GB
	0.02% of allocated quota used	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.

The Admin Dashboard features several widgets for system monitoring and management:

- System Summary:** Includes a line graph showing activity over time (THU, FRI, SAT, SUN, MON, TUE, WED, THU) and three circular gauges for Quota Usage (N/A), Temp Disk Usage (461.47 GB used, 292.55 GB free), and License Usage (8 used, 20 total).
- Statistics:** A list of system metrics including 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), and Emails Sent in the last 24h (0).
- Governance:** Shows Compliance status (3/3) and Realtime DLP Statistics (Active Downloads: 0).
- License Information:** A section for managing licenses.

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		Realtime DLP Statistics		Statistics	
Compliance	3/3	Active Downloads	0	Full Users	8
DLP Rules	10	Active Uploads	0	Guest Users	0
Retention	0	Active Shares	0	Limited Users	1
Content Classification	0	Active Users	2	Groups	8
		Violations	0	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

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**.

Admin Dashboard Setup Checklist

[Add Users](#) [Add Group](#) [Add Network Shares](#) [Add Admin](#) [Alerts](#) More

System Summary		Statistics	
Quota Usage	N/A	Full Users	8
Temp Disk Usage	461.47 GB	Guest Users	0
License Usage	8	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

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).

The screenshot displays the Admin Dashboard interface. At the top, there is a dark blue header with the title "Admin Dashboard" and a "Setup Checklist" button. Below the header is a navigation bar with buttons for "Add Users", "Add Group", "Add Network Shares", "Add Admin", and "Alerts". The main content area is titled "Add New Widget" and contains several widgets:

- Governance:** A table showing compliance metrics: Compliance (3/3), DLP Rules (10), Retention (0), and Content Classification (0).
- Realtime DLP Statistics:** A table showing active metrics: Active Downloads (0), Active Uploads (0), Active Shares (0), Active Users (2), and Violations (0).
- Statistics:** A table listing various system metrics: 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), and Emails Sent in the last 24h (0).
- Recent Access Locations:** A world map widget with a "Refresh" button.
- File Type Distribution:** A pie chart showing the distribution of file types: jpg (39.18%), png (13.33%), pdf (6.32%), docx (5.75%), and other types (35.42%).

Release Notifications

You can learn about new FileCloud releases:

By Subscribing to the Mailing List

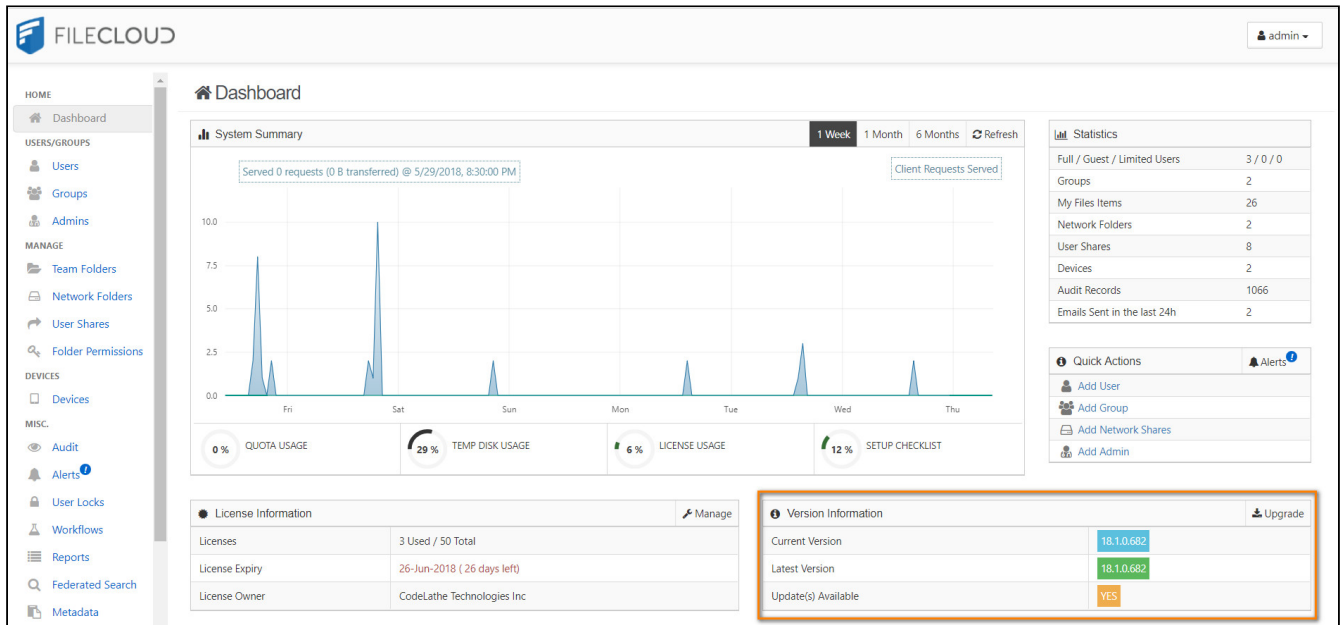
When you register with CodeLathe, you will automatically be added to the FileCloud Mailing List.

➔ If you are not receiving FileCloud emails, you can [Subscribe to the FileCloud Mailing List](#).

By seeing the version update in the FileCloud Admin Portal

When you log in to the Admin Portal, the default view on the dashboard includes update information, as shown in Figure 1.

Figure 1. Sample Admin Dashboard



Upgrade FileCloud

Administrators must keep FileCloud Server up-to-date with the latest version to take advantage of the new features, enhancements, and fixes for issues found in previous versions.

How do I know if an upgrade is available?

- FileCloud will always inform customers when a new upgrade is available.
- When you log on to the Admin Portal, the Admin Dashboard will also alert you to the fact that you can install an update.

Where is the notification on the Admin Dashboard?

The Version section is right next to the License section on the Dashboard.

The screenshot shows the FileCloud Admin Dashboard. The left sidebar contains navigation menus for HOME, USERS/GROUPS, MANAGE, DEVICES, MISC., SETTINGS, and CUSTOMIZATION. The main content area includes a top navigation bar, a dashboard overview with four circular progress indicators (QUOTA USAGE at 23%, TEMP DISK USAGE at 82%, LICENSE USAGE at 52%, and SETUP CHECKLIST at 100%), a License Information table, a Version Information table (highlighted with an orange box), a Recent Access Locations map, a File Type Distribution pie chart, and a User File Distribution section.

License Information		Version Information	
Licenses	52 Used / 100 Total	Current Version	18.2.0.1473
License Expiry	5-Oct-2019 (323 days left)	Latest Version	18.2.0.1473
License Owner	CodeLathe Technologies Inc	Update(s) Available	YES

How do I enable the weekly email?

To check for updates on a weekly basis:

This setting is available in FileCloud Version 18.2 and later.

1. Open a browser and log in to the **Admin Portal**.
2. From the left navigation panel, click **Settings**.
3. On the **Manage Settings** screen, select the **Admin** tab.
4. Scroll down to the **Check For Updates** checkbox.
5. Select the checkbox and then click **Save**.

Check For Updates

Enable to check for new versions

💡 To stop receiving the weekly email, just clear this checkbox.

Remember to [back up FileCloud](#) before upgrading.

For releases that DO NOT require a full system upgrade: [➔ Upgrade using Admin Portal](#)

For releases that DO require a full system upgrade: [➔ WINDOWS: Update Tool](#) [➔ Upgrade FileCloud on Linux](#)



⚠ Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.





Check if the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:







C:\xampp\apache\conf\httpd.conf







C:\xampp\apache\conf\extra\httpd-filecloud.conf

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
23.232	<p>Upgrading from ANY VERSION to 23.232</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. • If your installation of FileCloud uses admin portal user access restrictions, please see Restricting Access To Admin UI Based On IP Addresses for updated instructions. <p>Note: You can no longer use the Linux upgrade script to upgrade, see Upgrade FileCloud on Linux.</p>	<p>➔ Upgrade Notes for FileCloud 23.232 or Later</p>	<p>➔ FileCloud Version 23.232 Release Notes</p>

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
23.1	<p>Upgrading from ANY VERSION to 23.1</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. • If your installation of FileCloud uses admin portal user access restrictions, please see Restricting Access To Admin UI Based On IP Addresses for updated instructions. <p>Note: You can no longer use the Linux upgrade script to upgrade, see Upgrade FileCloud on Linux.</p>	<p> Upgrade Notes for FileCloud 23.1 or Later</p>	<p> FileCloud Version 23.1 Release Notes</p>

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
22.1	<p>Upgrading from ANY VERSION to 22.1</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. • If your installation of FileCloud uses admin portal user access restrictions, please see Restricting Access To Admin UI Based On IP Addresses for updated instructions. <p>Note: You can no longer use the Linux upgrade script to upgrade, see Upgrade FileCloud on Linux.</p>	<p> Upgrade Notes for FileCloud 22.1 or Later</p>	<p> FileCloud Version 22.1 Release Notes</p>
21.3	<p>Upgrading from ANY VERSION to 21.3</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 21.1 or Later</p>	<p> 21.3 Release Notes</p>

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
21.2	<p>Upgrading from ANY VERSION to 21.2</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 21.1 or Later</p>	<p> 21.2 Release Notes</p>
21.1	<p>Upgrading from ANY VERSION to 21.1</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 21.1 or Later</p>	<p> 21.1 Release Notes</p>
20.3	<p>Upgrading from ANY VERSION to 20.3</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 19.2 to 20.3</p>	<p> 20.3 Release Notes</p>

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
20.2	<p>Upgrading from ANY VERSION to 20.2</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 19.2 to 20.3</p>	<p> 20.2 Release Notes</p>
20.1	<p>Upgrading from ANY VERSION to 20.1</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 19.2 to 20.3</p>	<p> 20.1 Release Notes</p>
19.3	<p>Upgrading from ANY VERSION to 19.3</p> <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	<p> Upgrade Notes for FileCloud 19.2 to 20.3</p>	<p> 19.3 Release Notes</p>

Release	Upgrade Scenarios	Upgrade Notes	Release Notes
19.1	Upgrading from ANY VERSION to 19.1 <ul style="list-style-type: none"> • New Message Queue System is a REQUIRED service that needs to be running for FileCloud to be functional from 19.1 onwards • Please ensure the Message Queue Service is running after upgrade before opening up for live access • You CANNOT upgrade Windows and Linux using the Admin Portal. 	➔ 19.1 Upgrade Notes	➔ 19.1 Release Notes
18.2	Upgrading from 18.1 to 18.2 <ul style="list-style-type: none"> • There are no operating system or software update requirements • You can upgrade Windows and Linux FileCloud instances using the Admin Portal Upgrading from 17.3 or older to 18.2 <ul style="list-style-type: none"> • A full system upgrade is required for all existing installations 	➔ 18.2 Upgrade Notes	➔ 18.2 Release Notes
18.1	For all versions before 18.1: <ul style="list-style-type: none"> • A full system upgrade is required for all existing installations 	➔ 18.1 Upgrade Notes	➔ 18.1 Release Notes

Upgrade using Admin Portal

Minor updates can be performed directly in the FileCloud Admin Portal by clicking the **Start Upgrade** button, as shown in the steps below. Check the [release notes](#) to see the minimum version for an update in the Admin portal.

⚠ Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.

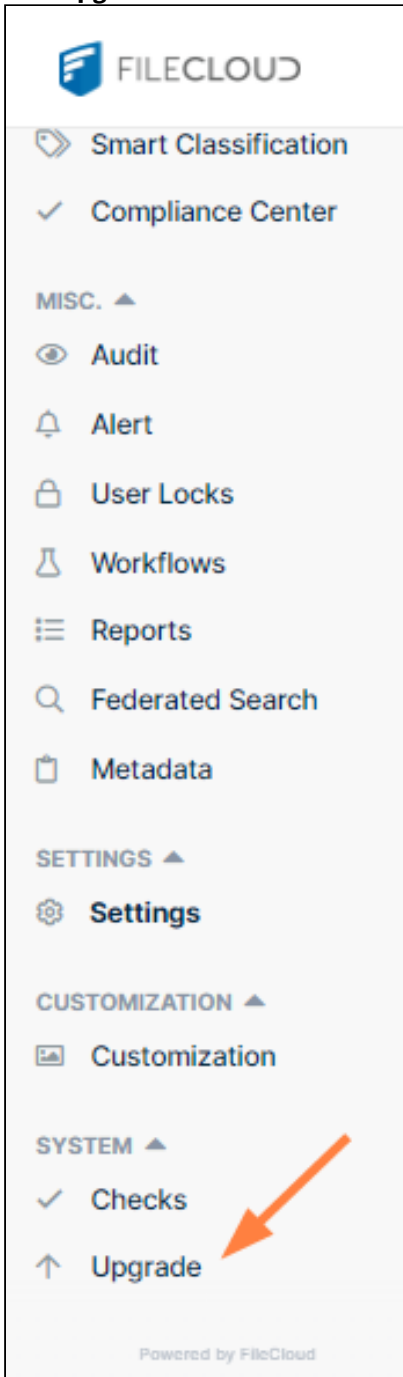
Check if the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:

C:\xampp\apache\conf\httpd.conf

C:\xampp\apache\conf\extra\httpd-filecloud.conf

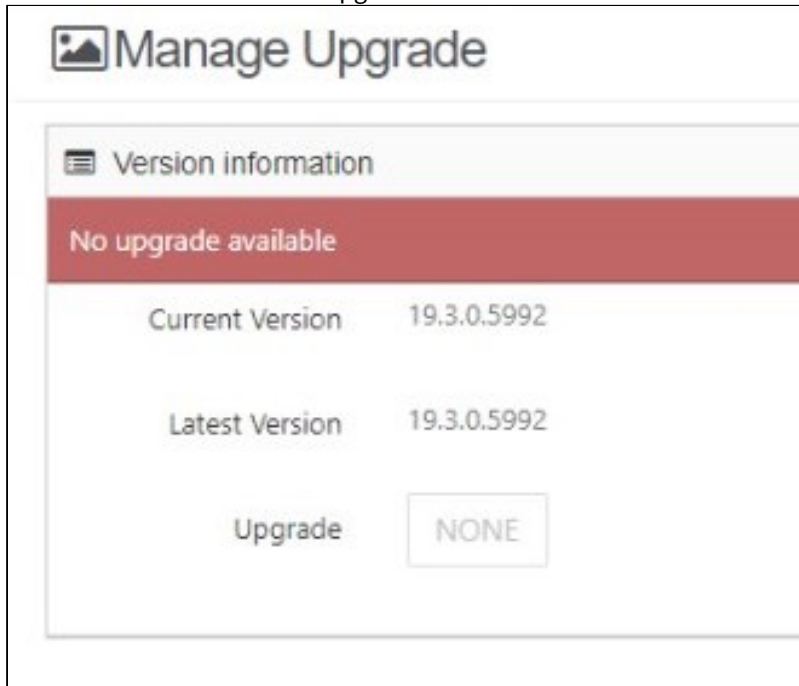
Upgrade Steps

1. Make a full backup or take a snapshot of the FileCloud server.
2. Login into the admin UI.
3. Click **Upgrade** at the bottom of the navigation panel.

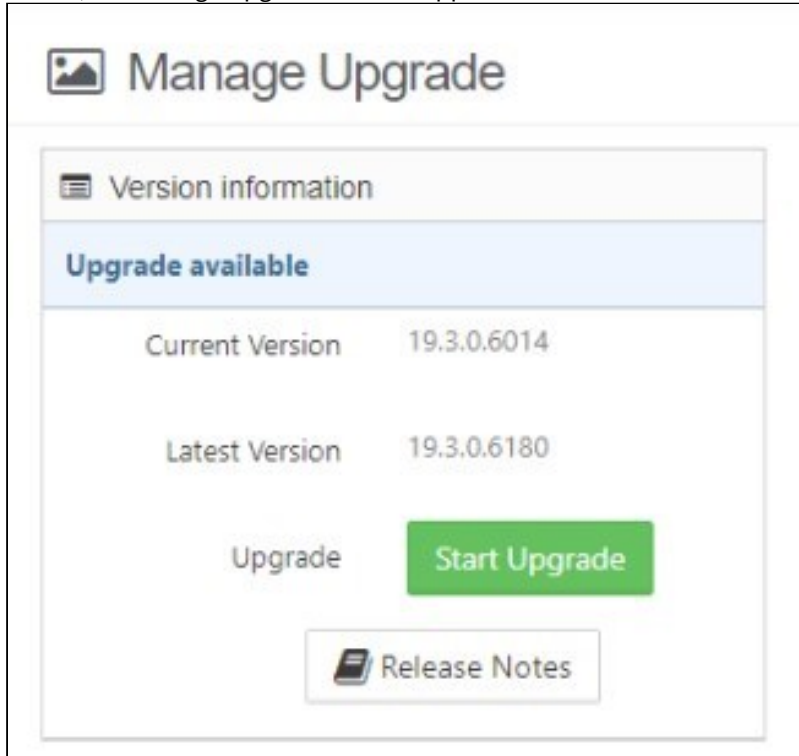


The Manage Upgrade window appears as follows if:

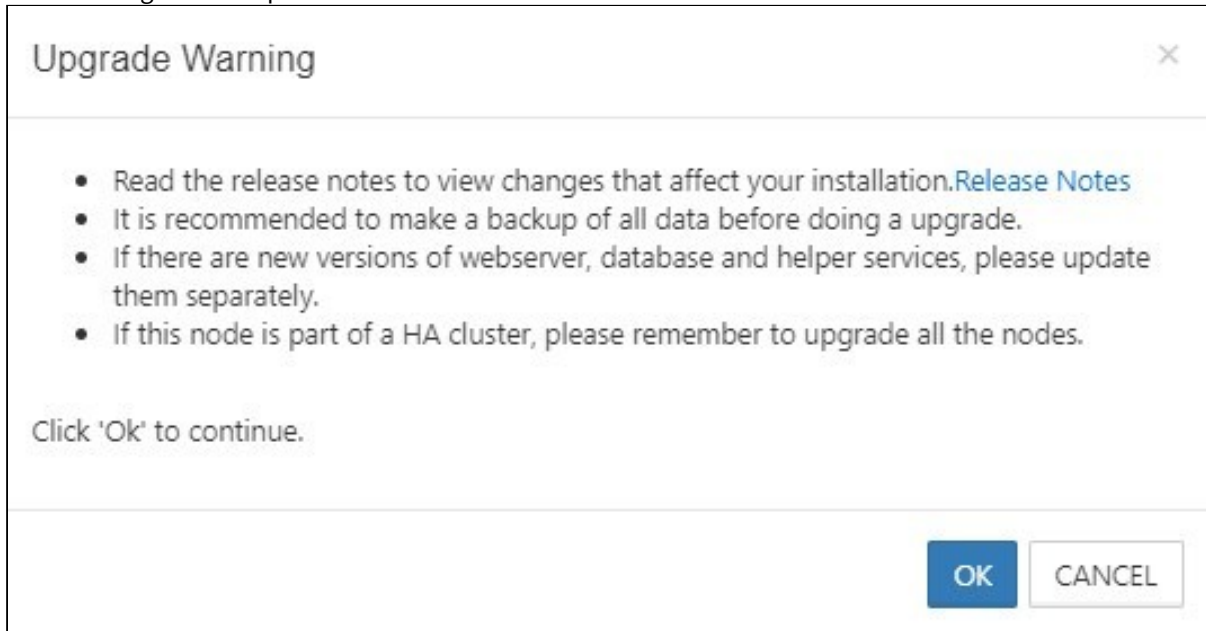
- No new upgrades are available
- Upgrades are not possible from the admin portal
- A license that does not allow upgrade to the latest version is installed



If there is an upgrade that can be installed from the admin portal and is permitted by the FileCloud license, the Manage Upgrade window appears as:



4. If the Manage Upgrade window indicates that an upgrade is available, click **Start Upgrade**.
The following window opens:



5. **Click OK.**
The upgrade process begins. When it is complete, messages similar to the following appear on the Manage Upgrade page.

Update completed without errors. Make sure to open the install check page and verify all the checks are OK before proceeding.

Filter Message : Message Type : All ▼

Message
===== Downloading update =====
Using override url for update : http://patch.codelathe.com/tonidocloud/qa1/installer/file_cloud.zip
===== Unpacking update =====
===== Cleaning update =====
===== Checking permissions =====
===== Loading file signatures =====
=====Applying update=====
Copying file C:/xampp/htdocs/resources/backup/activatesite.php
Copying file C:/xampp/htdocs/resources/backup/backup.class.php
Copying file C:/xampp/htdocs/resources/backup/backup.sh
Copying file C:/xampp/htdocs/resources/backup/backuphelper.php
Copying file C:/xampp/htdocs/resources/backup/checkfc.php
Copying file C:/xampp/htdocs/resources/backup/deleteuser.php
Copying file C:/xampp/htdocs/resources/backup/fcpostupgrade.php
Copying file C:/xampp/htdocs/resources/backup/fcpusite.php
Copying file C:/xampp/htdocs/resources/backup/licenseinstaller.php
Copying file C:/xampp/htdocs/resources/backup/licenses.txt
Copying file C:/xampp/htdocs/resources/backup/preparenaturalsort.php
Copying file C:/xampp/htdocs/resources/backup/preversionexporter.php
Copying file C:/xampp/htdocs/resources/backup/repairfc.php

Page of 588
11752 rows

Your database is up-to-date

6. In the navigation bar, click Installation Checks directly above the Upgrade link and make sure that the installation is free of errors.
7. Refresh the browser UI (Ctrl + F5) to get the latest updated User Interface.

Updating Systems That Cannot Connect Outside

If your FileCloud server cannot connect to our update server to download the packages directly, you can download file_cloud.zip and file_cloud.xml to a local folder and update your installation using the local path.

1. Open the WWWROOT\config\cloudconfig.php file and edit the following entry:

For Windows:

If the files are located in c:\users\administrator\Downloads folder, then modify the url as follows:

```
define("TONIDO_CLOUD_UPDATE_URL_OVERRIDE","file://C:\\Users\\Administrator\\Downloads\\file_cloud.zip");
```


For Linux:


If the the files are located in /home/filecloudupdate/ (Apache should have permission for this folder), then modify the url as follows:


```
define("TONIDOCLOUD_UPDATE_URL_OVERRIDE","/home/filecloudupdate/file_cloud.zip");
```


- Download the following packages and place them in the local folder specified in the TONIDOCLOUD_UPDATE_URL_OVERRIDE config:
https://patch.codelathe.com/tonidocloud/live/installer/file_cloud.zip
https://patch.codelathe.com/tonidocloud/live/installer/file_cloud.xml

Upgrade using Update Tool (Windows Only)

 If you have folder-level security (granular folder permissions) enabled in **Settings > Misc > General**, changes in functionality will significantly impact the way existing share behavior works when you upgrade from versions below 23.1 to FileCloud 23.x and higher. If you have granular folder permissions set, please [contact FileCloud Support](#) before upgrading to FileCloud 23.x and higher to avoid share and file access issues.

 If your system uses MongoDB authentication or custom IP binding, follow the steps at [Disable MongoDB Authentication and IP Binding](#) before performing the steps on this page.

 For FileCloud upgrade on cluster, see: [FileCloud Update for HA on Windows](#)


 FileCloud support is ending for Windows Server 2012 R2 with 22.1 release. If you are using Cloud Enterprise Server and Windows 2012, please migrate your FileCloud site to Windows 2016, Windows 2019, or Windows 2022.

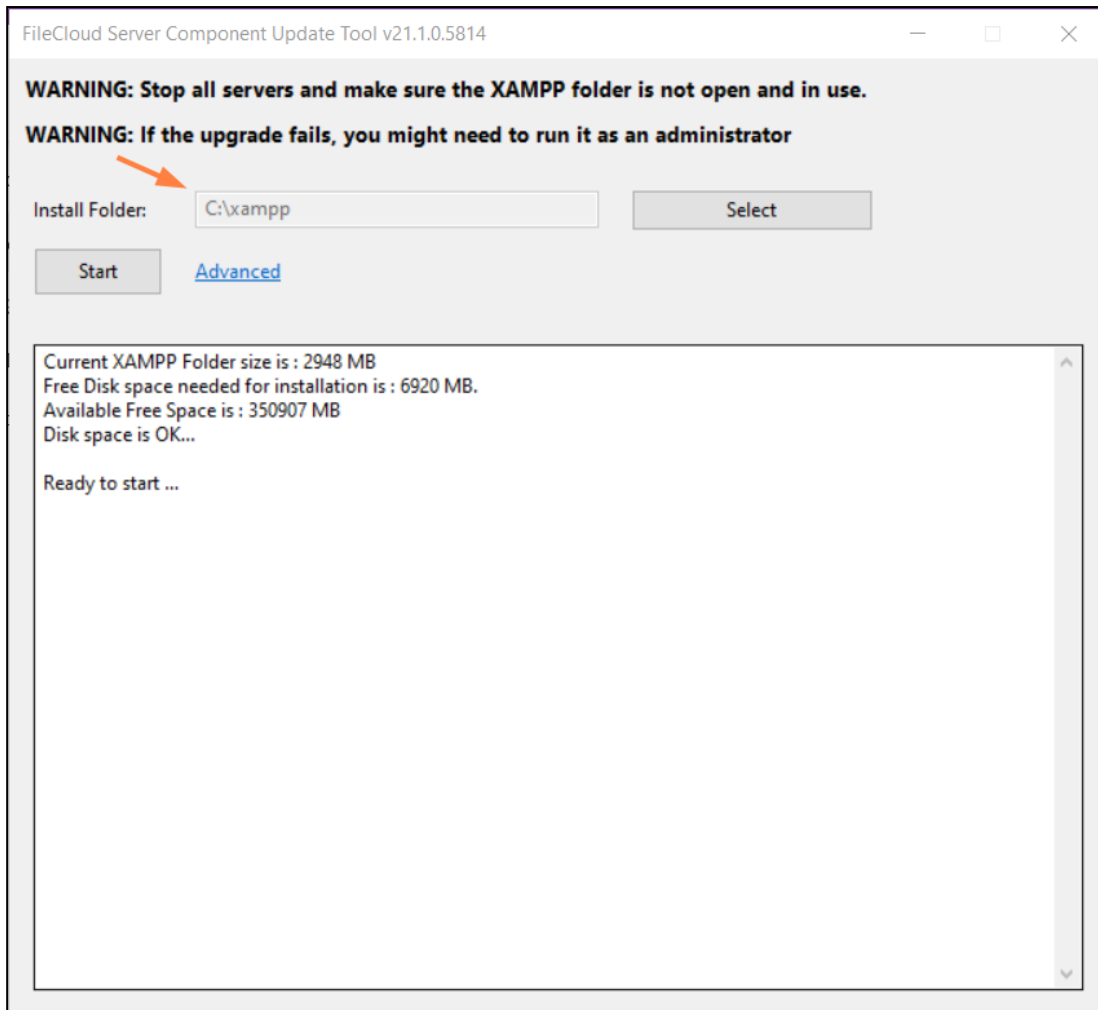
STEP 1: Backup existing installation

FileCloud installation environment	Backup steps
Windows OS and installation without backup tool	Windows manual backup

STEP 2: Preparing for update

- Download the latest FileCloud Windows Update Tool from <https://patch.codelathe.com/tonidocloud/live/installer/cloudupdatetool.zip>
Note: It is essential that you download the latest version of the update tool; If you run an old version of the tool, you will re-install an old version of FileCloud.
- Extract all files from [cloudupdatetool.zip](#) into a folder.
- If your system allows downloading of files from internet, go to step 5. Otherwise, complete step 4 first.

- Download the following files and copy them to the extracted folder (the cloudupdatetool folder)
 - FileCloud Windows Preupgrade Package from <https://patch.codelathe.com/tonidocloud/live/installer/filecloudpreupgrade.zip>
 - FileCloud Windows Preupgrade XML - Right-click and save the file <https://patch.codelathe.com/tonidocloud/live/installer/filecloudpreupgrade.xml>
 - FileCloud Windows Update Package from <https://patch.codelathe.com/tonidocloud/live/installer/filecloudupdate.zip>
 - FileCloud Windows Update XML - Right-click and save the file <https://patch.codelathe.com/tonidocloud/live/installer/filecloudupdate.xml>
- Now, navigate to the cloudupdatetool folder and double click on  cloudupdate (cloudupdate.exe). The following window opens:



STEP 3: Update

- Open the FileCloud Control Panel and click **Stop** for each running service. (If you are upgrading an HA system, stop all the nodes (All DB servers of the replica set as well as the Apache web servers on each of the nodes).) If running Memcache, make sure it is stopped too.

FileCloud Control Panel

FileCloud Control Panel
v: 21.1.0.14883, Base Components: 21.1.0.14883
Webserver Ports: 80,443 Database Port: 27017

Initial Setup: [Install Check](#)

Web Portal: [Admin Portal](#) [User Website](#)

Servers

Webserver:	Running SVC	Start	Stop	Config	Make Service
Database:	Running SVC	Start	Stop	Config	Make Service
Cron Task:	Running SVC	Start	Stop	Config	Install
Message Queue:	Running SVC	Start	Stop	Config	Install

Optional

FileCloud Helper:	Running SVC	Start	Stop	Install	Config
Memcache:	Running SVC	Start	Stop	Make Service	
Document Preview:	Running SVC	Start	Stop	Install	
Content Search:	Running SVC	Start	Stop	Install	

Miscellaneous

Configuration: [Application Folder](#) [Reset Admin Password](#)

SSL: [Create SSL CSR](#) [Install SSL Cert](#)

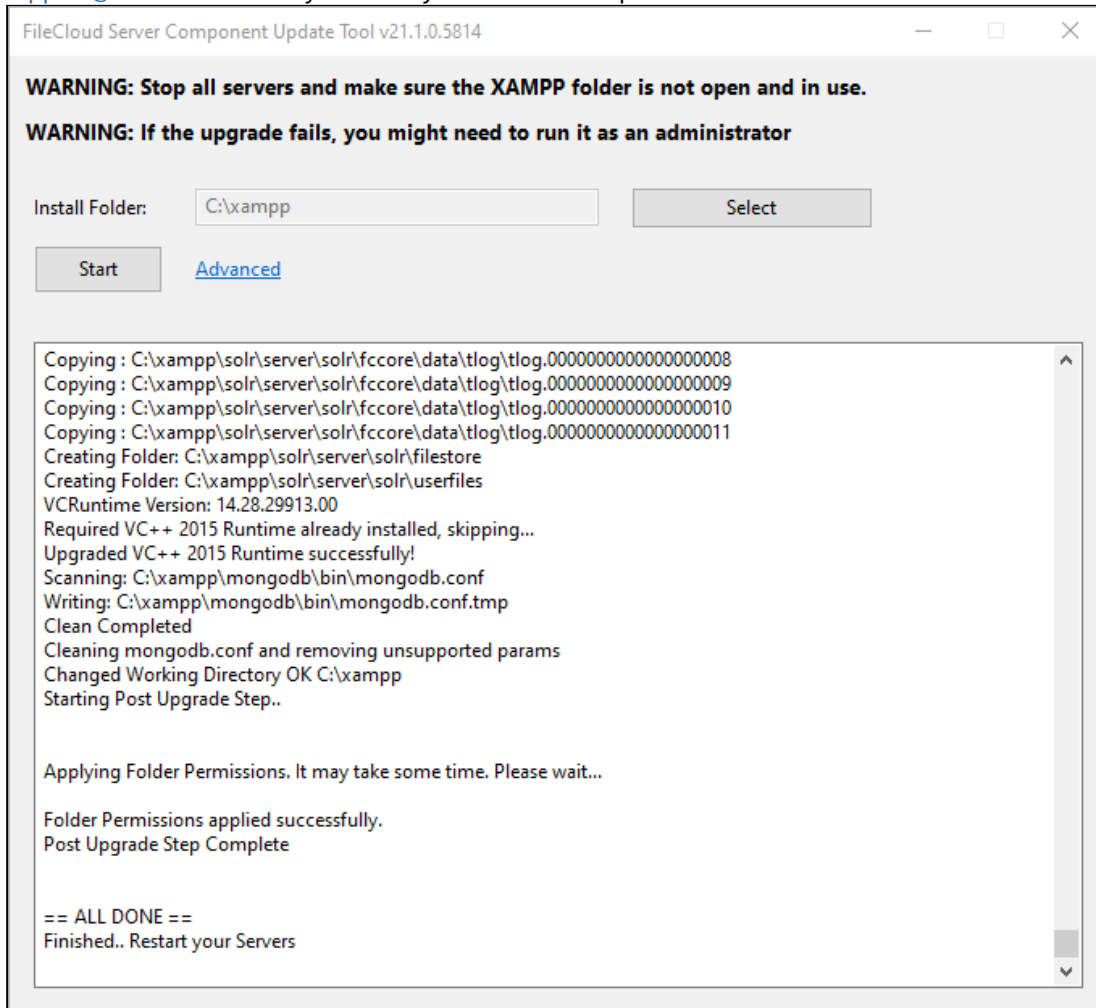
Technical Support

Need Help? [Documentation](#) [Contact Support](#) [Demo and Training](#)

2. Ensure that **Install Folder** shows the location of your XAMPP folder. This location is auto-detected, but it may not be able to determine it correctly if there are multiple XAMPP folders. If it is not correct, select the correct XAMPP install folder.

- Click **Start** on the Update Tool dialog box to begin the upgrade. (Repeat steps 1-3 for each of the nodes for HA system).

The tool must be able to connect to the internet in order to download the update package. Please contact support@codelathe.com if you see any errors in this step.



If you receive an error message, see [Troubleshooting the Upgrade Tool](#).

- If you are running multi-tenant FileCloud, make sure the database post upgrade script is run correctly.

```

cd c:\xampp\htdocs\resources\backup
c:\xampp\php\php.exe fcpostupgrade.php

```

- Once the nodes are updated, start each of the nodes using the cloud control panel.

The screenshot shows the FileCloud Control Panel interface. At the top, it displays the version 'v: 21.1.0.14984' and 'Base Components: 21.1.0.14984'. Below this, it lists 'Webserver Ports: 80,443' and 'Database Port: 27017'. There are links for 'Initial Setup: Install Check' and 'Web Portal: Admin Portal User Website'. An orange arrow points from the 'User Website' link down to the 'Start' button for the 'Webserver' service.

Service	Status	Start	Stop	Config	Install	Make Service
Webserver:	Not Running	Start	Stop	Config		Make Service
Database:	Running SVC	Start	Stop	Config		Make Service
Cron Task:	Not Running	Start	Stop	Config	Install	
Message Queue:	Not Running	Start	Stop	Config	Install	

Optional

FileCloud Helper:	Not Running	Start	Stop	Install	Config	
Memcache:	Not Running	Start	Stop	Make Service		
Document Preview:	Not Running	Start	Stop	Install		
Content Search:	Not Running	Start	Stop	Install		

Miscellaneous

Configuration: [Application Folder](#) [Reset Admin Password](#)

SSL: [Create SSL CSR](#) [Install SSL Cert](#)

Technical Support

Need Help? [Documentation](#) [Contact Support](#) [Demo and Training](#)

6. Message Queue is an important service and must be started after the upgrade.

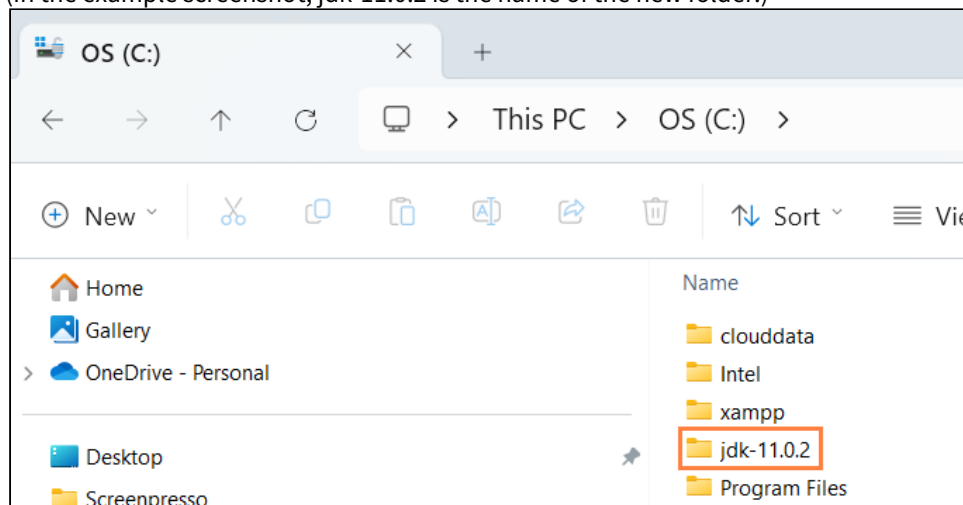
⚠ Message Queue must be installed. If you cannot click the **Start** button for **Message Queue**, it is not installed. Click **Install**, and once installation is complete, click **Start**.

7. Open the install URL <http://<your domain>/install/index.php>
8. Make sure [basic checks](#) are all OK.
9. Click on [Extended Checks](#).
In section 3 of **Extended Checks**, your new updates are shown with status and available actions.
10. If Apache is running as the Windows Logon account, then give the logon account write permission on the XAMPP folder.
11. When you initially log in to the admin portal after upgrade, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.
12. Beginning in FileCloud 20.1, to sign into the admin portal for multi-tenancy, you must sign in as the superadmin user and enter your password in encrypted format in the multi.php file. See [Password encryption and logging in to a multi-tenant admin portal](#) for instructions on encrypting your password.

Upgrade environments using Solr and Solr+OCR

Windows

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 11.
Upgrade OpenJDK to version 11.
 - a. Download **Open JDK 11.02+9** from <https://jdk.java.net/archive/>.
 - b. Create a new folder in the C: drive.
(In the example screenshot, jdk-11.0.2 is the name of the new folder.)



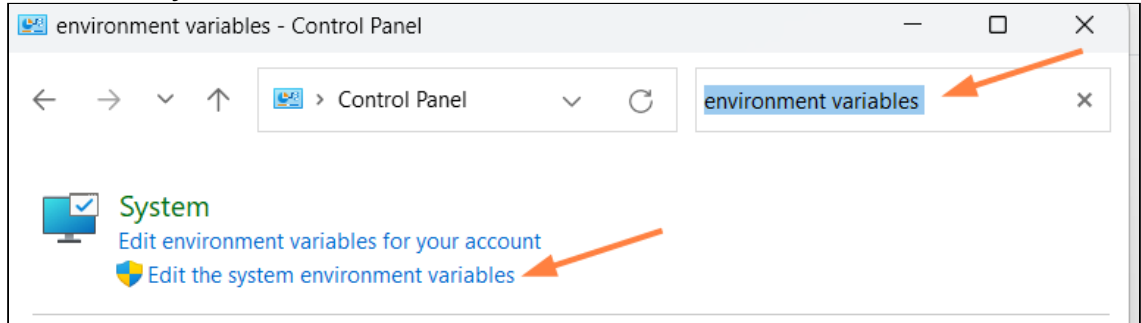
- c. Extract the Open JDK file you downloaded into the new folder.
3. Set JAVA_HOME to the new version's path.
Set the JAVA_HOME path

Setting the path and environment variables will differ depending on the version of Windows you have on your computer. These instructions were designed for Windows 11.

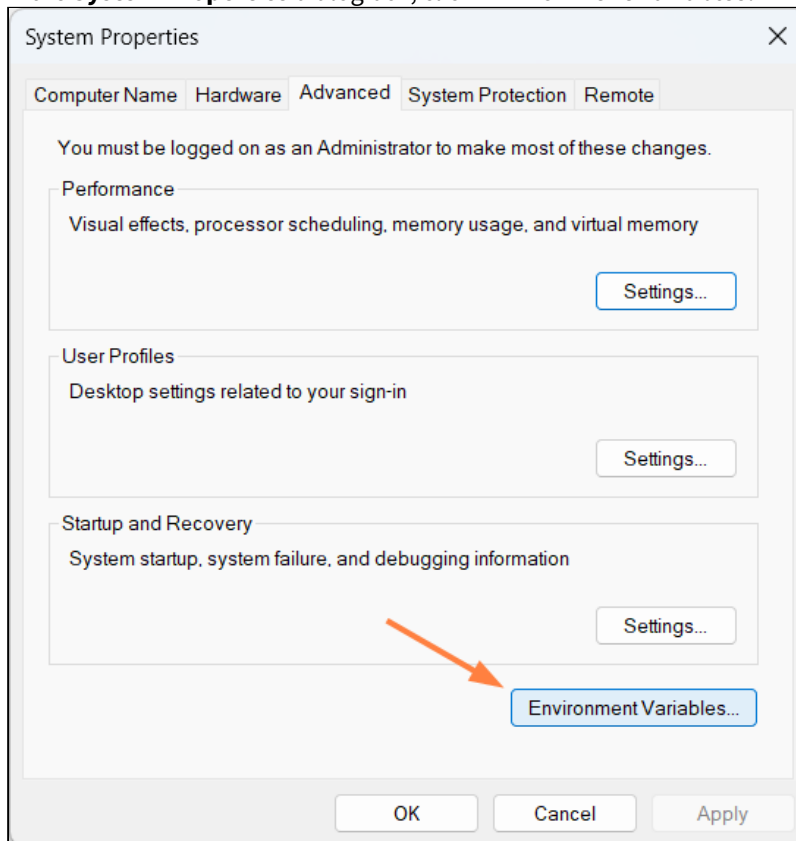
⚠ Administrator privileges are required to modify the path and environment variables.

To set the JAVA_Home path:

- a. Open the Windows Control Panel.
- b. Enter **environment variables** in the search bar.
- c. Click **Edit the system environment variables**.



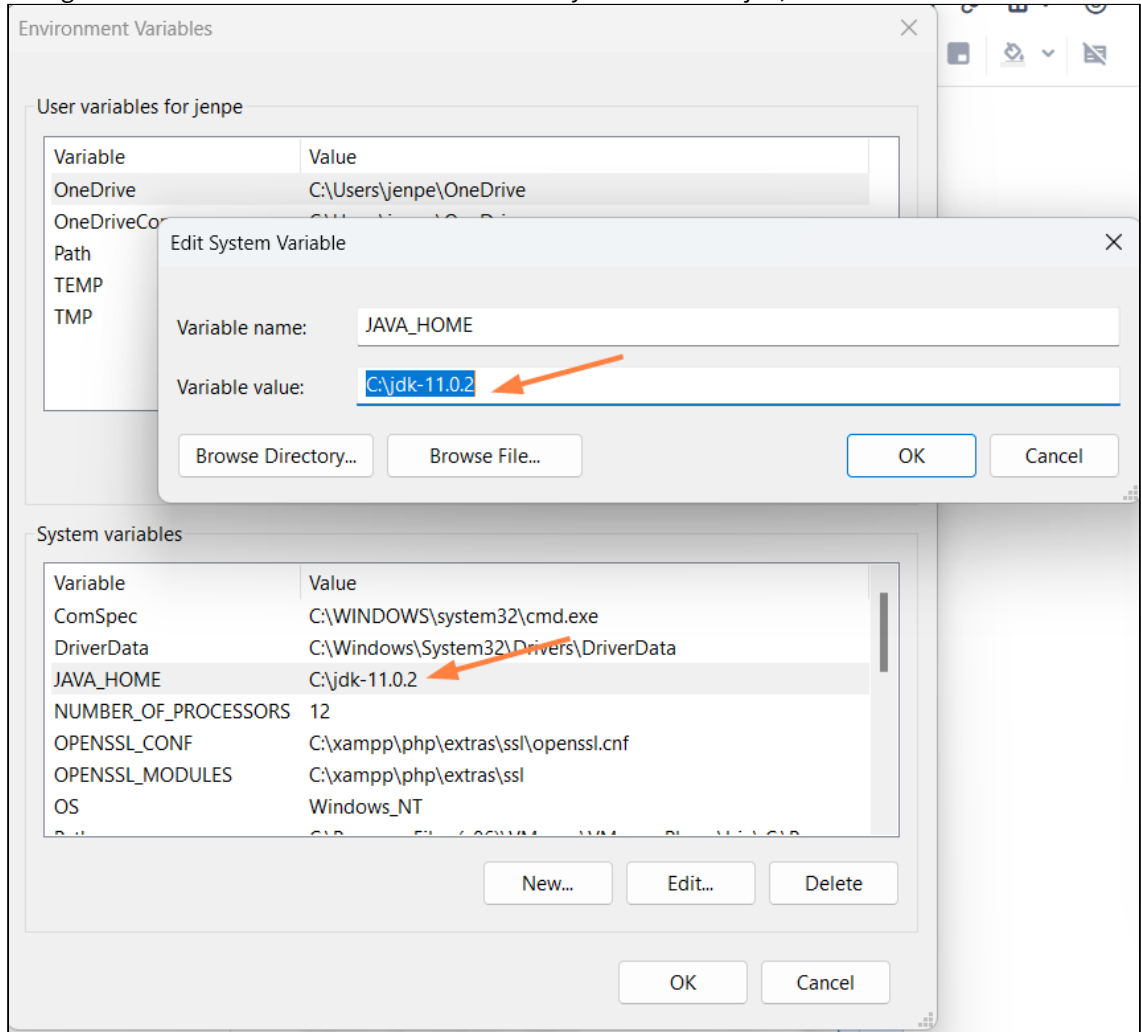
- d. In the **System Properties** dialog box, click **Environment Variables**.



The **Environment Variables** dialog box opens.

- e. In the **System variables** box, Click **JAVA_HOME**, and then click **Edit**.
The **Edit System Variable** dialog box opens.

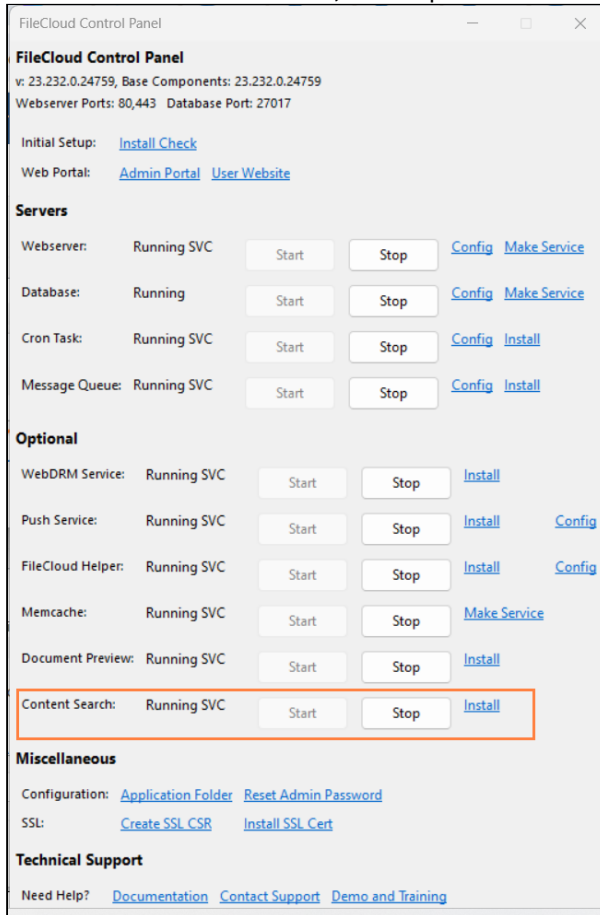
- f. Change **Variable value** to the address of the folder you created for jdk, and click **OK**.



- g. In the **Environment Variables** dialog box, click **OK**.

4. Log in to the FileCloud admin portal.

5. In the FileCloud Control Panel, and stop and restart Content Search.



⚠ Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.

Check if the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:

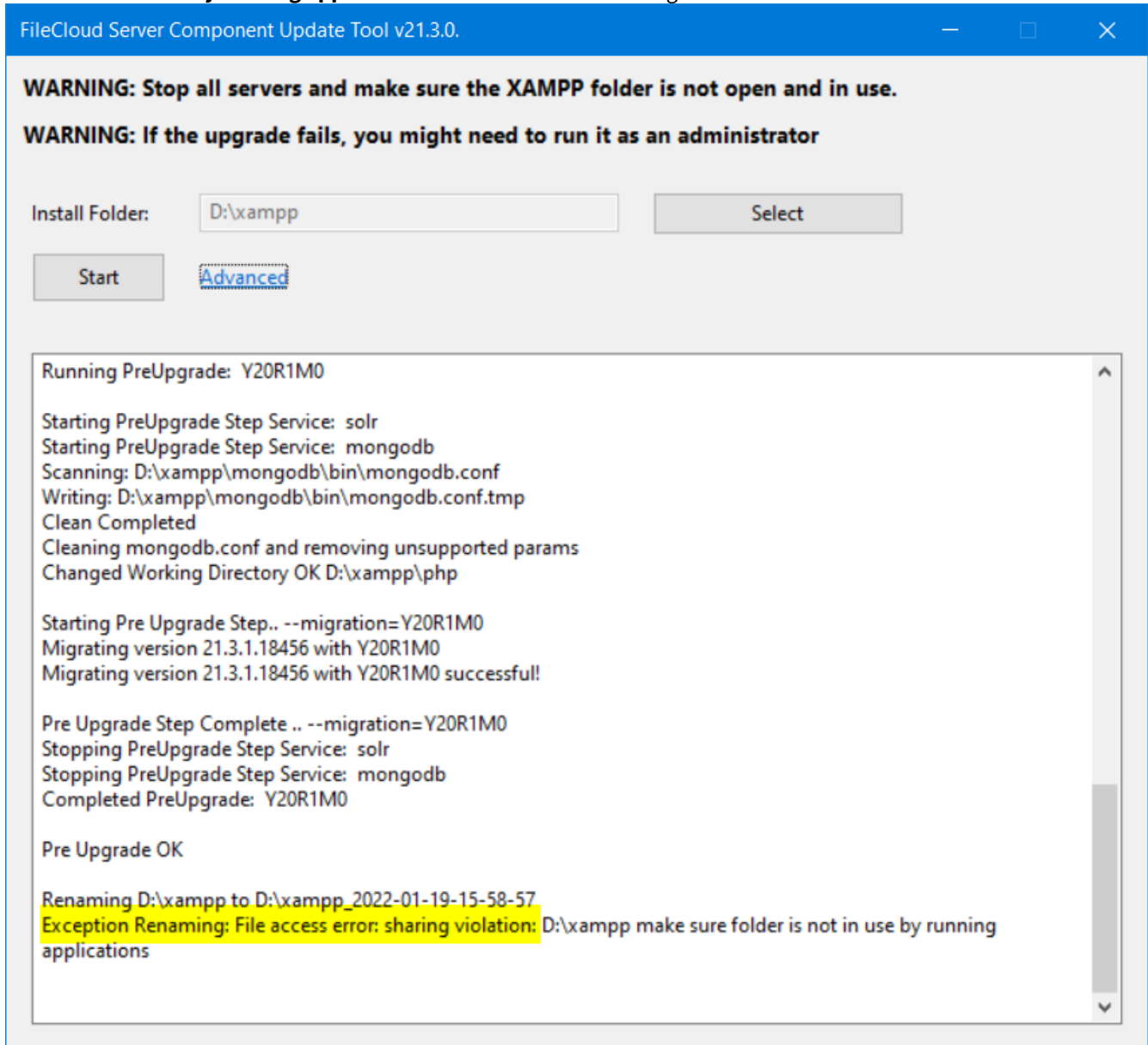
- C:\xampp\apache\conf\httpd.conf
- C:\xampp\apache\conf\extra\httpd-filecloud.conf
- C:\xampp\htdocs\htaccess
- C:\xampp\php\php.ini
- C:\xampp\apache\conf\extra\httpd-ssl.conf
- C:\xampp\htdocs\src\Scripts\config\default.json

Troubleshooting the Upgrade Tool

Exception Renaming

Problem:

The upgrade tool returns the error **Exception Renaming: File access error: sharing violation D:\xampp make sure folder is not in use by running applications** as shown in the following screenshot:

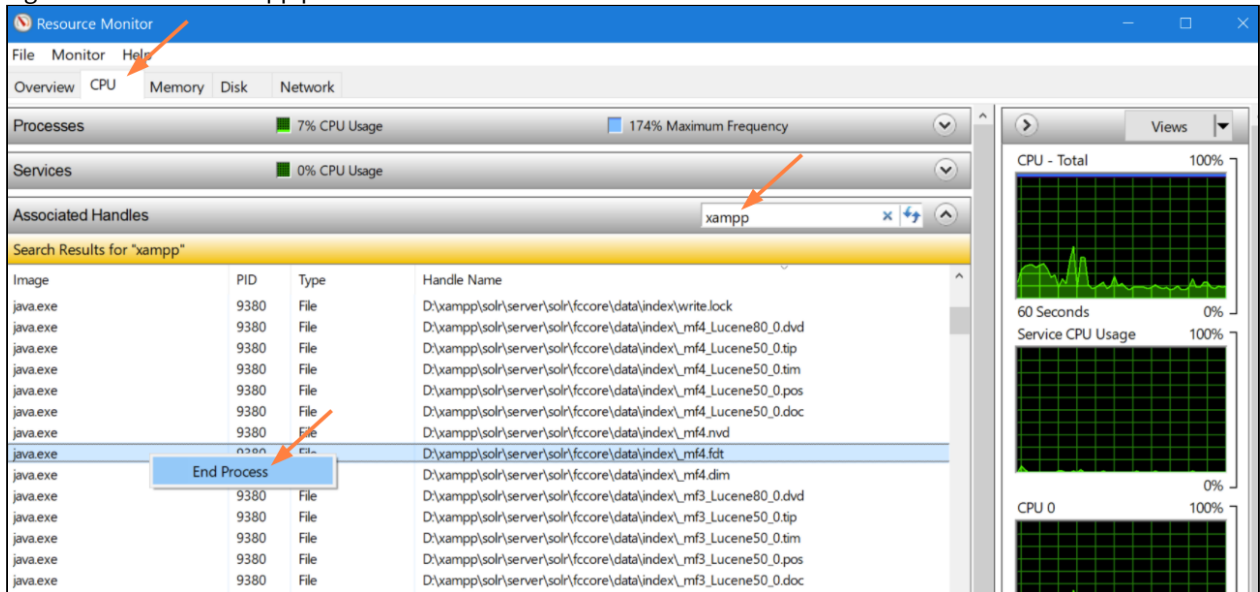


Solution:

Use the Windows Resource Monitor to end the processes that are blocking the move:

1. Start the Resource Monitor by clicking **Win-R**, and then entering **resmon**.

2. Click the **CPU** tab.
3. Search for **xampp** in **Associated Handles**.
4. Right-click on each xampp process and choose **End Process**.



5. Click **Start** in the **Update Tool** interface again.

FileCloud Update for HA on Windows

To upgrade to the latest version, please [Contact FileCloud Support](#).

FileCloud Upgrade for HA on Linux

To upgrade to the latest version, please [Contact FileCloud Support](#).

HA Update when MongoDB Version is Lower Than 4.2

When you are updating a Windows high availability system, if your version of MongoDB is lower than 4.2, create a new replica set, and use mongoDump/mongoRestore.

To create the new replica set:

1. Back up servers.
 - a. Create a backup or snapshot for all servers.
 - b. Perform a complete [database dump](#).
2. Remove all replica sets.
 - a. Stop all FileCloud services.
 - b. Remove all replica sets, TLS, and authentication parameters in mongod.conf for all db nodes. Details about the configuration can be found at [FileCloud High Availability](#).

- c. Delete DB data folder content for all DB nodes:
Linux: /var/lib/mongo/
Windows: C:\xampp\mongodb\bin\data\
- d. Start MongoDB on all nodes.
- e. Confirm that you can connect to all DB nodes with the [mongo shell](#) without authentication and TLS and if the replica set is disabled:

```
> rs.status()
{
  "ok" : 0,
  "errmsg" : "not running with --replSet",
  "code" : 76,
  "codeName" : "NoReplicationEnabled"
}

C/C++ detected
```

- f. Stop MongoDB on all nodes and remove the data folder content again.
3. Perform a standard FileCloud update.
4. Create a cluster and restore data.
 - a. [Create a new cluster](#).
 - b. Restore DB dump using [mongorestore](#).

Disable MongoDB Authentication and IP Binding

If your system uses MongoDB authentication or custom IP binding, prior to using the [FileCloud Update tool for Windows](#), MongoDB authentication and IP binding must be disabled.

To disable MongoDB authentication and IP binding:

1. Backup the MongoDB config file by running the command:

```
copy C:\xampp\mongodb\bin\mongodb.conf %TEMP%
```

2. In C:\xampp\mongodb\bin\mongodb.conf, disable authentication by adding # (a comment character) at the beginning of the line **auth = true**:

```
#auth = true
```

3. Also in C:\xampp\mongodb\bin\mnogodb.conf, disable IP binding by uncommenting **bind_ip_all** and commenting **bind_ip**:

```
#ip address
bind_ip_all = true
#bind_ip = 10.2.3.44
```

4. Restart MongoDB to activate the changes.

5. Test access using mongo shell.
(If you are updating from a version of FileCloud prior to version 23.1, use **mongo** instead of **mongosh** in the following command:

```
cd C:\xampp\mongodb\bin
mongosh --quiet --eval "show dbs"
# you should see output similar to this:
admin                148.00 KiB
config               108.00 KiB
fcbbackup            20.00 KiB
fcbbackup_duo        20.00 KiB
```

6. [Update FileCloud using the Update Tool.](#)
7. Re-enable IP binding and authentication and restart MongoDB.

Backup FileCloud Before Upgrading

Before any updating current FileCloud installation, it is important to backup your data!

Based on your installation environment, choose one of the following links to perform backup:



[Linux tool backup](#)



[Linux manual backup](#)



[Windows manual backup](#)

Upgrade FileCloud on Linux

! If you have folder-level security (granular folder permissions) enabled in **Settings > Misc > General**, changes in functionality will significantly impact the way existing share behavior works when you upgrade from versions below 23.1 to FileCloud 23.x and higher. If you have granular folder permissions set, please [contact FileCloud Support](#) before upgrading to FileCloud 23.x and higher to avoid share and file access issues.

! Beginning with version 23.1, Linux installation and upgrades have switched to a new repository-based system, and FileCloud no longer supports Ubuntu 18.04/20.04, CentOS 7/RHEL 7 and RHEL 8. In addition, FileCloud no longer supports Debian. If you are using any of those OS versions, please migrate to Ubuntu 22.04 LTS or RHEL 9.
Since support for [OpenSSL 1.1.1 ends on September 11, 2023](#), FileCloud 23.1 uses OpenSSL 3.0. which is not available for previous Linux versions, and therefore FileCloud requires installation or update to the Linux versions listed above.

! MongoDB 6 requires use of the AVX instruction set, which is available on [select Intel and AMD processors](#). If your CPU doesn't have the AVX instruction set, MongoDB 6 will not run.
To check whether your CPU has the instruction set, run:

```
#lscpu | grep -i avx"
```

Note: FIPS 140-3 modules are still in review for Ubuntu 22.04 and RHEL 9.

If you want to install FileCloud with FIPS, please wait until the OS vendors officially announce they are supporting FIPS.

[Ubuntu information](#)

[RHEL information](#)

Upgrade instructions for Linux

Upgrading FileCloud from 23.1.x to the latest version

To upgrade FileCloud from 23.1.x to the latest version in Linux see [Upgrade FileCloud on Linux from Version 23.1 to the Latest FileCloud Version](#).

Upgrading FileCloud from 22.1 in Ubuntu 20.04 and RHEL 8

You can either re-install FileCloud or upgrade both FileCloud and your operating system.

Option 1: Install one of the supported operating systems, then [Install the latest version of FileCloud](#) on the newly installed operating system, and then [migrate FileCloud to the newly installed operating system](#). This is the recommended option.


Option 2: Perform a FileCloud upgrade which requires OS upgrades to Ubuntu 22.04 or RHEL 9.x, For this procedure, please [Contact FileCloud Support](#).

Please note that FileCloud Support cannot resolve OS upgrade problems.

Upgrading FileCloud from versions lower than 22.1

If you are upgrading from a version of FileCloud lower than 22.1 or from an operating system below Ubuntu 22.04 LTS or RHEL 9, please install one of the supported operating systems, then [Install the latest version of FileCloud](#) on the newly installed operating system, and then [migrate FileCloud to the newly installed operating system](#).

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](#)

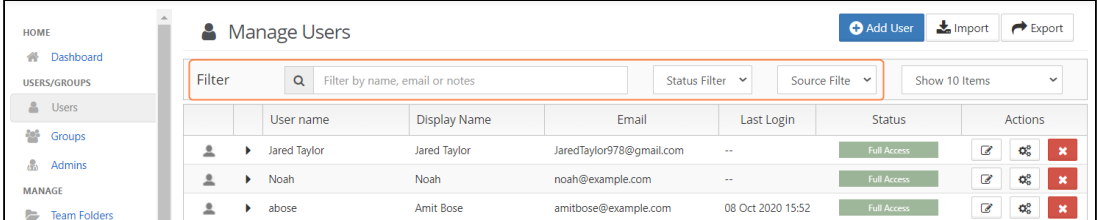
To add FileCloud users, see [Create FileCloud Users](#).













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.



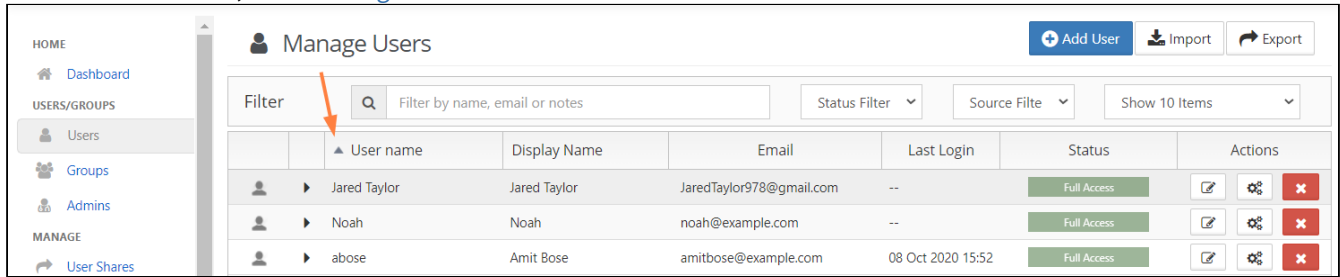
	User name	Display Name	Email	Last Login	Status	Actions
	Jared Taylor	Jared Taylor	JaredTaylor978@gmail.com	--	Full Access	  
	Noah	Noah	noah@example.com	--	Full Access	  
	abose	Amit Bose	amitbose@example.com	08 Oct 2020 15:52	Full Access	  

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.

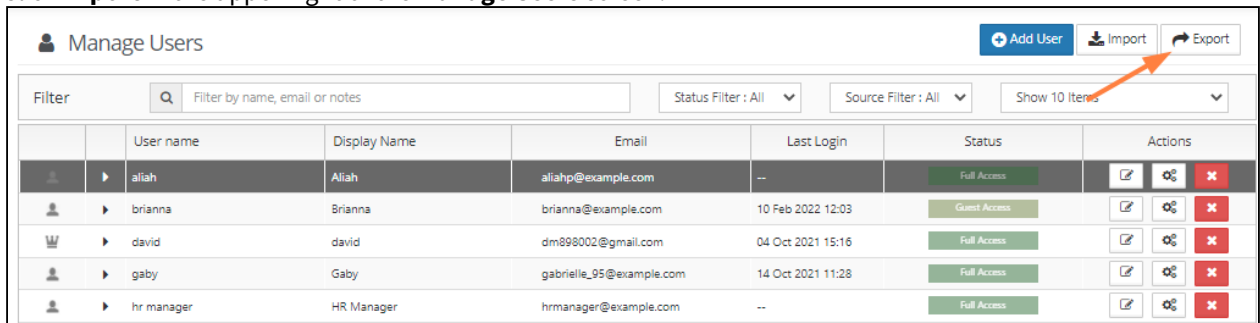
Notice that by default, all upper-case letters precede lower-case letters in alphabetical order. To change to a case-insensitive sort order, see [Enabling Natural Sort Order Of User List](#).



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		EVERYONEYES	NO		10/4/2021 15:16	Default	15559992323	Group Management
3	aliah	aliahp@example.com		Aliah	FULL		EVERYONEYES	NO			Default	15556667777	Global Default Policy
4	hr manager	hrmanager@example.com		HR Manager	FULL		EVERYONEYES	NO			Default		Global Default Policy
5	gaby	gabriele_95@example.com		Gaby	FULL		EVERYONEYES	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 categories: 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 the title is a search filter for 'gmail.com', a 'Status Filter' dropdown, a 'Source Filter' dropdown, and a 'Show 10 Items' dropdown. A table lists three users:

	User name	Display Name	Email	Last Login	Status	Actions
👑 ▶	david	david	dm898002@gmail.com	28 Apr 2021 08:20	Full Access	📄 ⚙️ ✖️
👤 ▶	jaredtaylor978	Jared	jaredtaylor978@gmail.com	--	Full Access	📄 ⚙️ ✖️
👑 ▶	jessicam	Jessica	jm2344311@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 displays the following information for user 'jessicam':


Name	jessicam	Total Quota	2 GB
Email	[blurred]	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

Authentication

Save

Close

Limit Admin Access to User Data

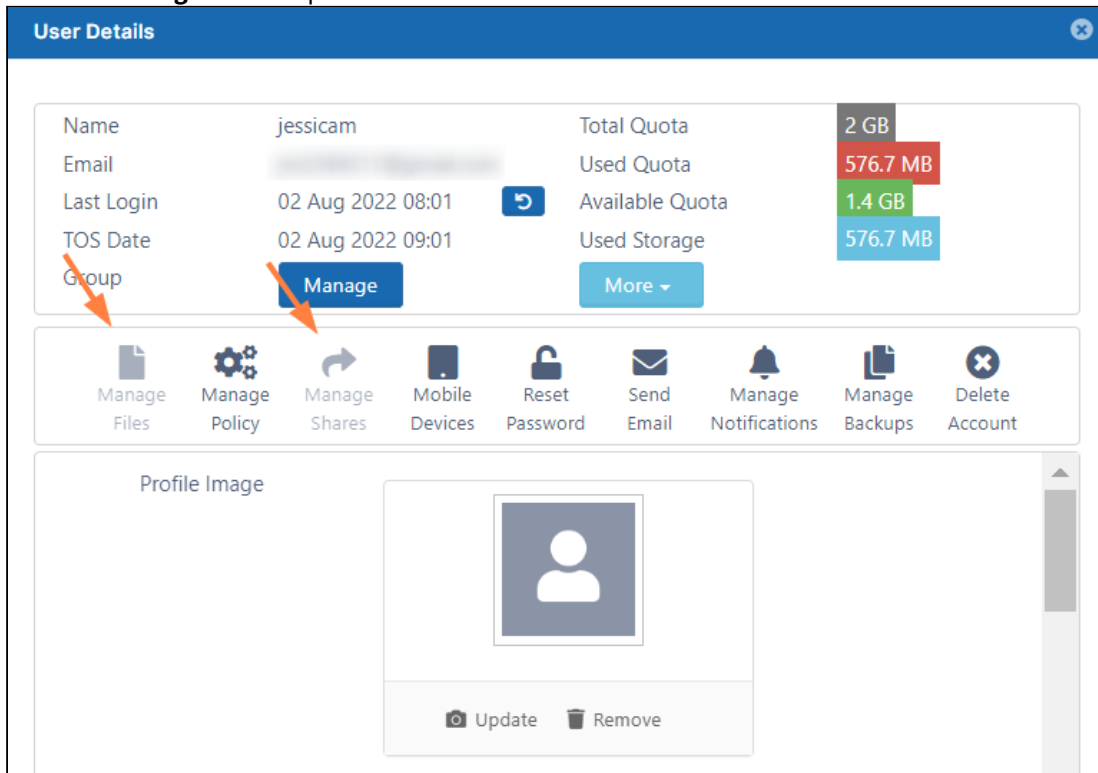
By default, the system's main admin and admin users with the proper access have the ability to [manage user files and shares](#), which includes the ability to download user content and view it.

Beginning with FileCloud Version 20.1, you can remove this access from the system admin and admin users:

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

```
define("TONIDOCLLOUD_DISABLE_ADMIN_USER_DATA_ACCESS_UI", true);
```


Now when an admin goes to the **Manage Users** screen and edits a user, in the **User Details** window, the **Manage Files** and **Manage Shares** options are disabled:

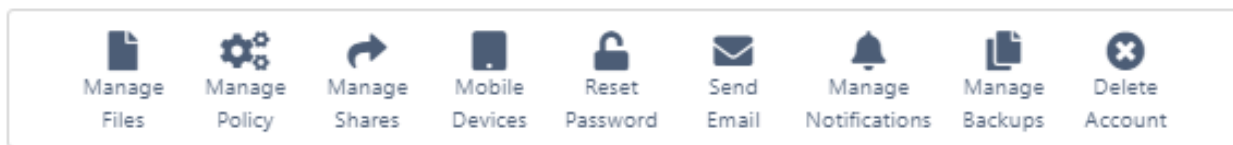


User Properties - Advanced Options

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

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


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



Options	Description	For more information
Manage Files	<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)

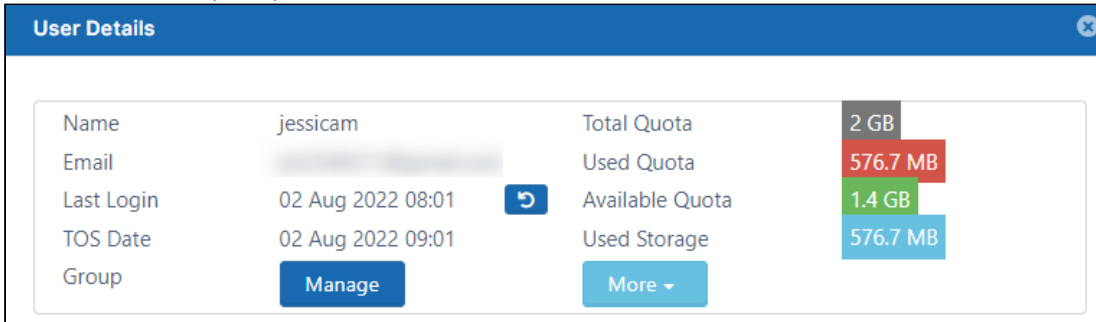
Editable Property	Description
Phone Number (added in FileCloud 20.1)	The user's phone number.
Notes	This field allows the user to enter notes for the user and also search the user based on notes.


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** ().



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

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', 'Guest', 'Full', and 'External'. An orange arrow points to the 'Disabled' option. 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](#)

Or:

[Use the command line to move the files to a different user.](#)

When a user account needs to be deleted, administrators can move the files to a different user instead of allowing the files to be deleted with the user account.

1. In a command line enter:

For Windows:

```
cd c:\xampp\htdocs\resources\tools\fileutils  
PATH=%PATH%;C:\xampp\php
```

For Linux:

```
cd /var/www/html/resources/tools/fileutils/
```

2. Then, for both Windows and Linux, enter:

```
php txfilesanddeleteaccount.php -h <host> -u <user> -p /destination/path -o
```

Parameters:

[Required] -h <host> Site host name or 'default' for default site

[Required] -u user account whose files are to be transferred before account delete

[Required] -p path to which the user files are to be moved before deleting account

[Optional] -o set this flag to overwrite and merge transferred file with destination

Examples:

- a) Command to transfer files of user "richard" to path /tgtuser/holding of default site:

```
php txfilesanddeleteaccount.php -h default -u richard -p /tgtuser/holding
```

- b) Command to transfer files of user "richard" to path /tgtuser/holding of default site, overwriting files/folders that may exist in the destination:

```
php txfilesanddeleteaccount.php -h default -u richard -p /tgtuser/holding -o
```

How do you want to delete a user account?

- ➔ [Use the command line](#)
- ➔ [Use the admin portal](#)

Deleting FileCloud User From Command Line

1. In a command line enter:

For Windows:

```
cd c:\xampp\htdocs\resources\backup
PATH=%PATH%;C:\xampp\php
```

For Linux:

```
cd /var/www/html/resources/backup
```

2. Then, for both Windows and Linux, enter:

```
php deleteuser.php -u <user_name>
```


Deleting User in Multi-Site Setups

To delete user for another site in case for multitenant setup, pass in the hostname using -h parameter

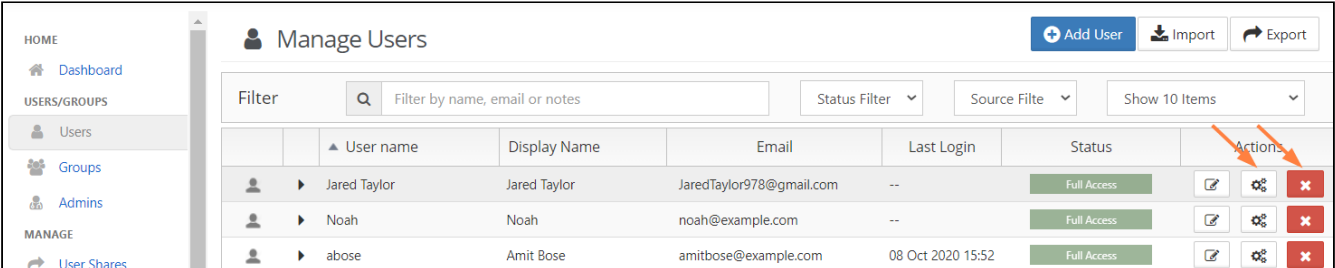
```
php deleteuser.php -u <user_name> -h site2.xyz.com
```










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:

Authentication:

Email:

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

- Click **Reset Password**.



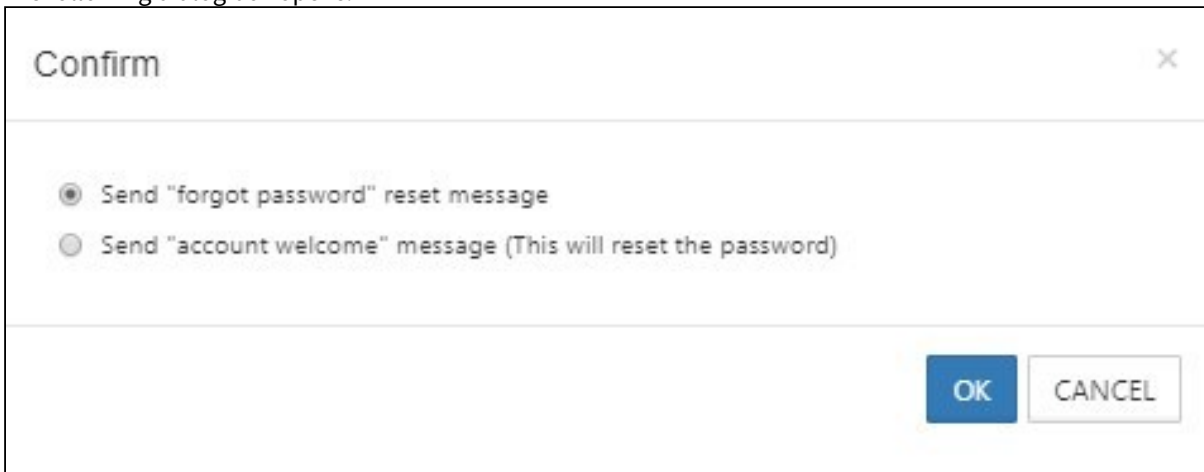
The dialog box titled "Set New Password" has a close button (X) in the top right corner. It contains two input fields: "Password" and "Confirm Password". At the bottom right, there are two buttons: "Save" (highlighted in blue) and "CANCEL".

- 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 dialog box titled "Confirm" has a close button (X) in the top right corner. 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, 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**.

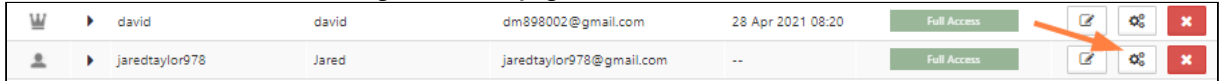
Modifying a policy while managing a user

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:

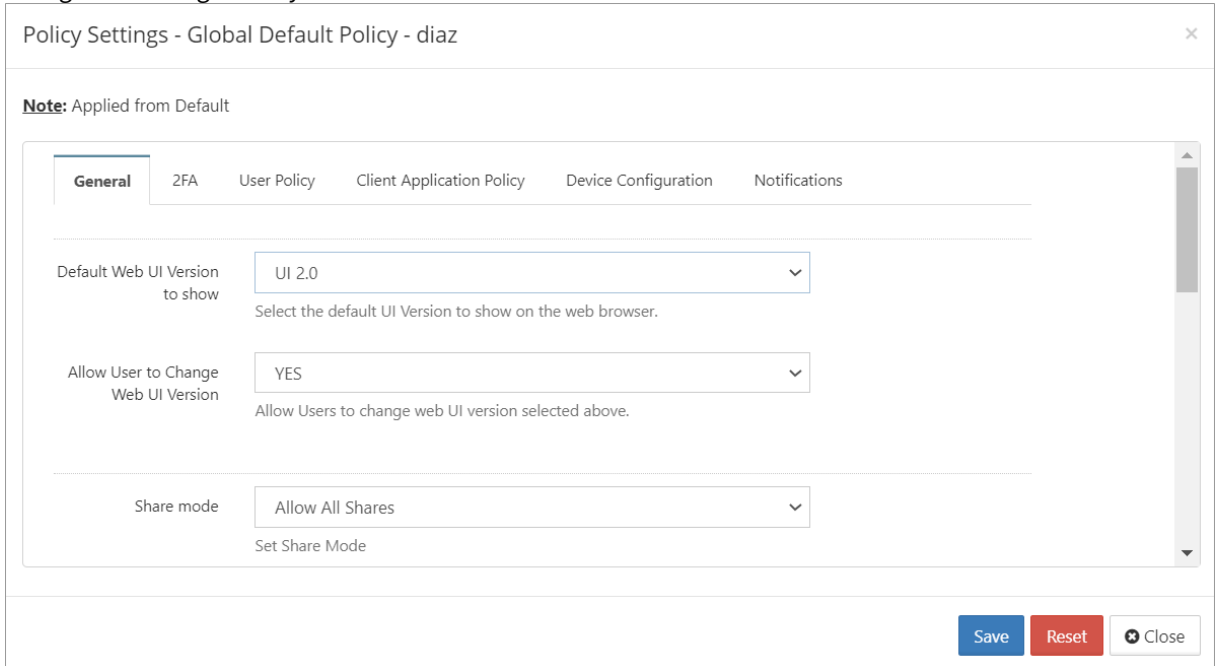
1. In the admin portal navigation panel, click **Users**.
The **Manage Users** page opens.

2. Across from a user, click the Manage User Policy (gears) icon.



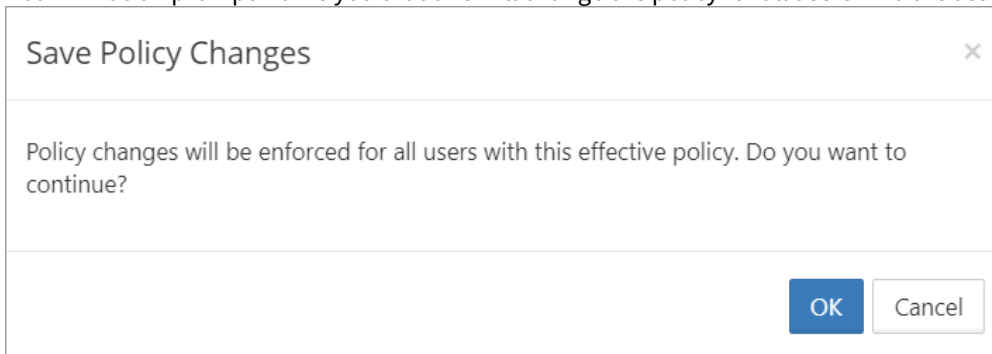
The **Policy Settings** dialog box opens.

3. Change the settings on any of the tabs.



4. **Click Save.**

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



5. Click **OK**.

The policy is changed.


Calculate the Effectiveness of a User's Policy

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


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

➔ Learn more about [Effective Policy Best Practices](#)

To calculate the effectiveness of a policy for a user:

1. Open a browser and log on to the admin portal.
2. From the navigation panel, click **Users**.
3. In the **Manage Users** window, select a user, and then click the Edit icon .
4. In the **User Details** window, click **Manage Policy**.
5. Next to the **Effective Policy** box, click **Calculate**.
6. The most effective policy for this user is shown in the box next to the **Calculate** button.
7. To see the details of a policy, click **Open**.

Manage a User's Profile Picture


 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

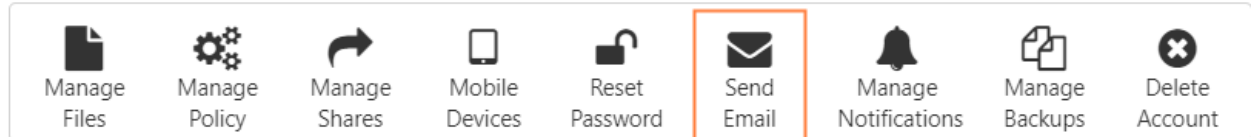
 This option is available beginning in FileCloud 20.1

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.

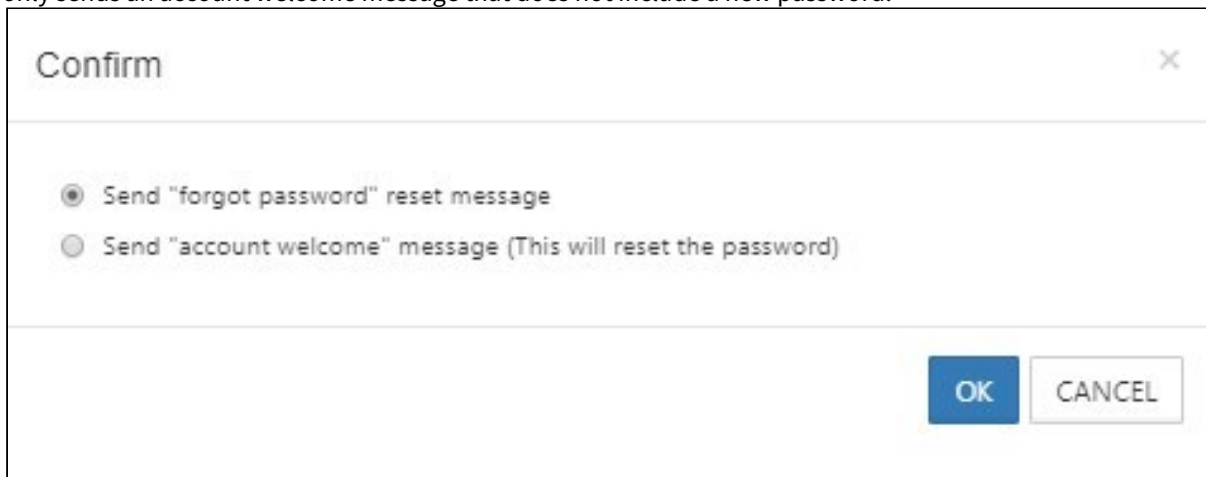
To send an email from User Details:

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

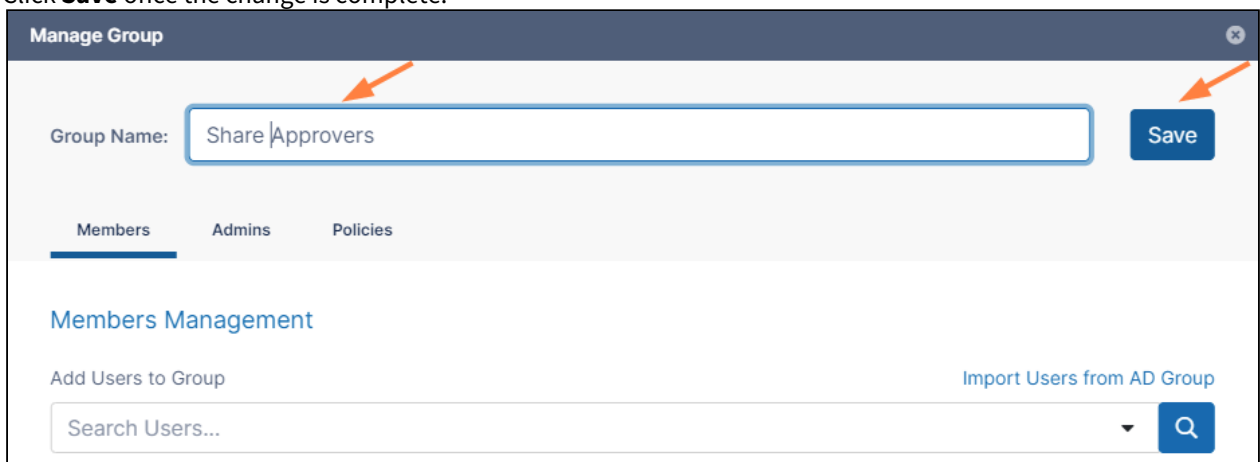
To add a group, see [Group Settings](#).

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**.

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

Manage Group

Group Name: Save

Members Admins Policies

Members Management

Add Users to Group Import Users from AD Group

Q

Users in Group (3 members in this group) Export

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

< Page of 1 >

Close

Exporting a list of users in a group

To export a list of users in a group:

- In the navigation pane, click **Groups**.
- 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, there are tabs for 'Members', 'Admins', and 'Policies'. The 'Members' tab is selected. The 'Members Management' section includes a search bar for users and an 'Import Users from AD Group' button. Below this, the 'Users in Group' section shows a list of two users: Jared and Jessica. Each user has a 'Remove' button next to their name. 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

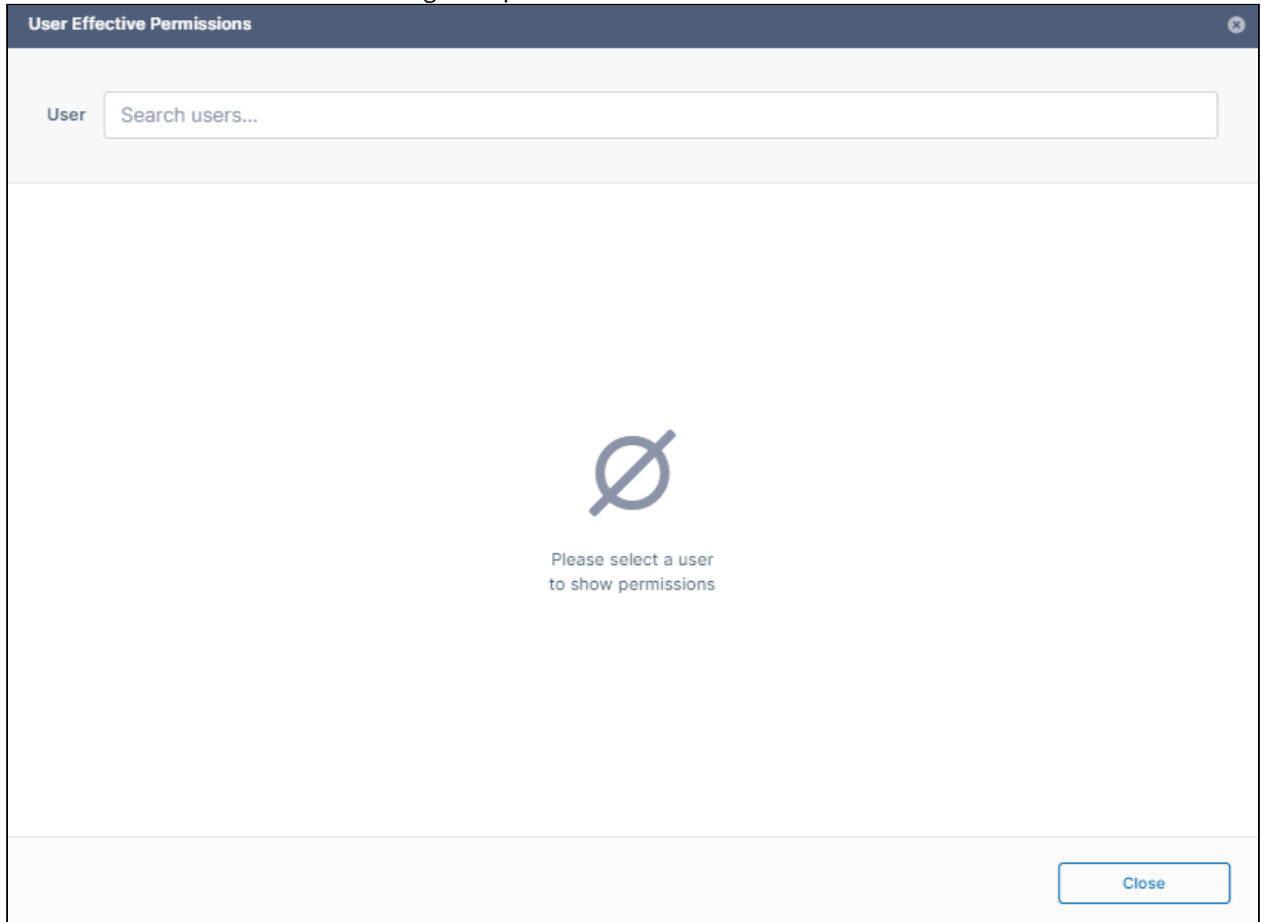
If an admin user has one role, the user has the permissions assigned to that role, but if an admin user has multiple roles, the user has the combined permissions of all of its roles.

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**.

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

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.
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.
Reports	Reports menu item on the admin interface is available. Add, execute, edit and delete reports.

Operation	Description
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

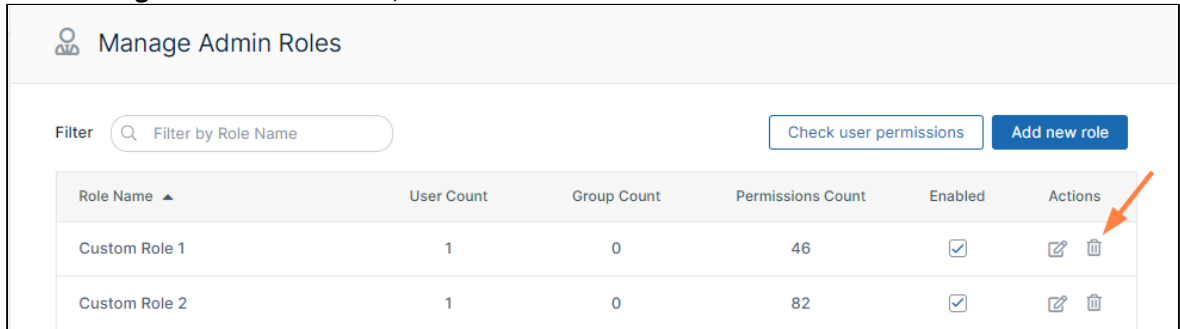
When you remove an admin role, you permanently delete it. To recreate it, you must create it, assign all permissions, and add users and groups again.

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.



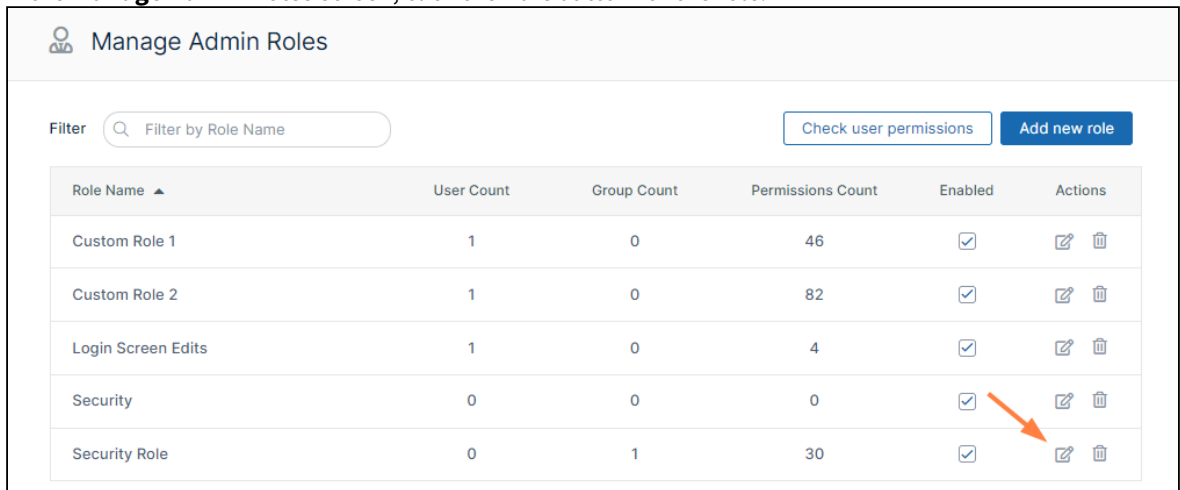
The screenshot shows the 'Manage Admin Roles' interface. At the top, there is a search filter 'Filter by Role Name', a 'Check user permissions' button, and an 'Add new role' button. Below is a table with the following data:

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"/>	

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

Or:

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

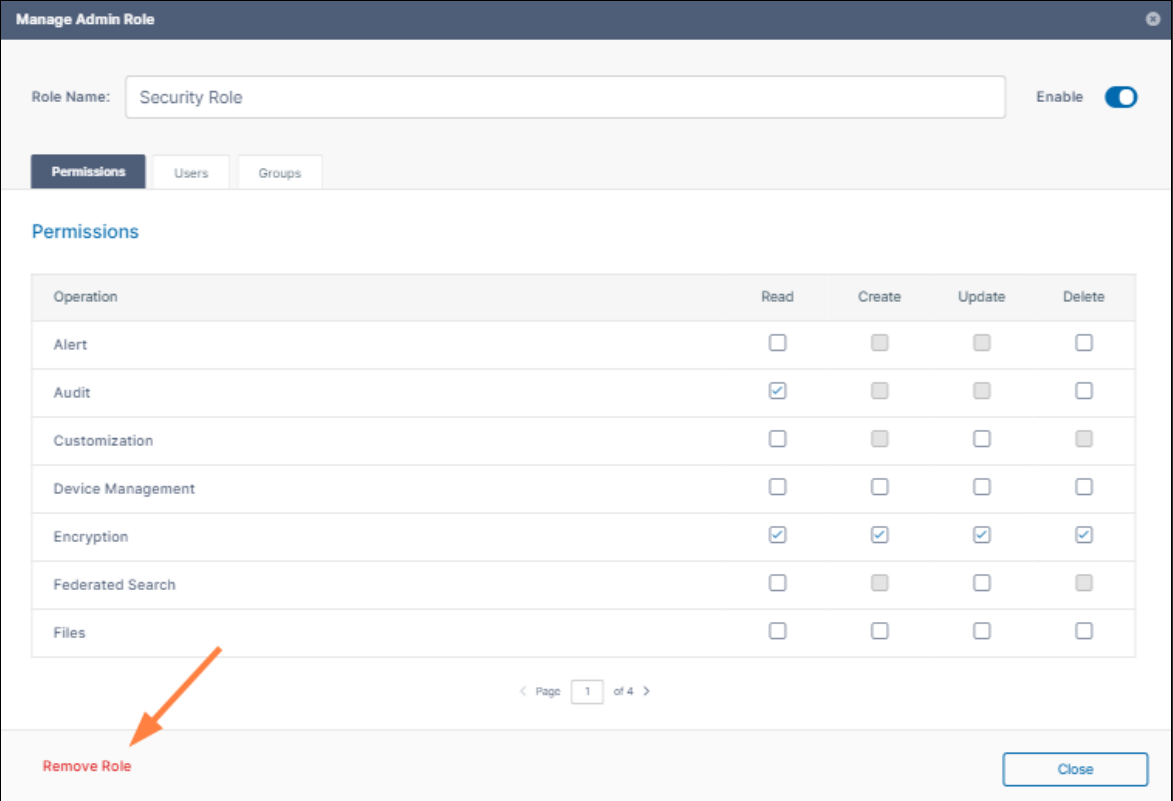


The screenshot shows the 'Manage Admin Roles' interface with a different set of roles. The table contains the following data:

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"/>	
Login Screen Edits	1	0	4	<input checked="" type="checkbox"/>	
Security	0	0	0	<input checked="" type="checkbox"/>	
Security Role	0	1	30	<input checked="" type="checkbox"/>	

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 it is enabled. Below this are tabs for 'Permissions', 'Users', and 'Groups'. The 'Permissions' tab is active, displaying a table of operations and their permissions. An orange arrow points to the 'Remove Role' button at the bottom left.

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 >

Remove Role Close

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

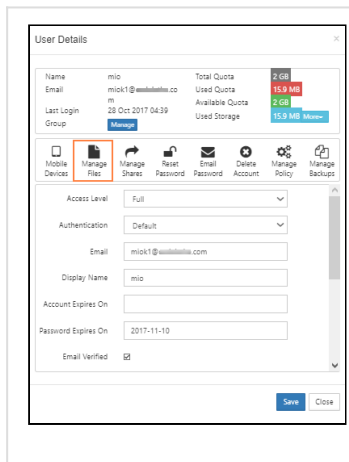
Managing User Folders and Files

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.

How do I limit admin access to users' files and folders?

If you do not want the main administrator or admin users to have unlimited access to user files and folders, you can configure your system to prevent them from performing all of the following actions:

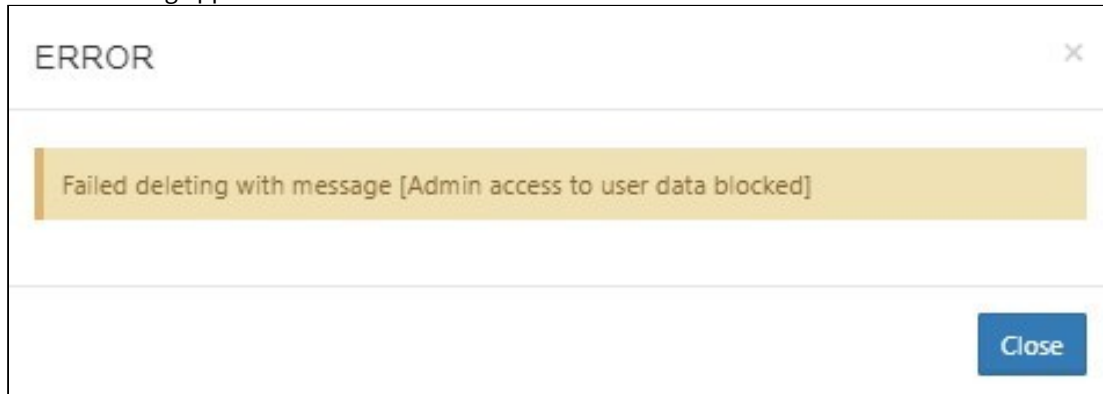
- download a file
- delete a file or folder
- rename a file or folder
- move a file or folder
- copy a file or folder

To limit admin access to user files and folders:



1. Open the configuration file:
Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux: /var/www/config/cloudconfig.php
2. Add the line:
`define("TONIDOCLOUD_DISABLE_ADMIN_USER_DATA_ACCESS", true);`

3. Save and close cloudconfig.php.


Now when an admin attempts to perform one of the above actions to a user file or folder, a message similar to the following appears:



What do you want to do?

 <p>Manage Files</p>	<ul style="list-style-type: none"> ➔ Download User Files and Folders ➔ Restore a Previous File Version ➔ Copy and Move User Files
 <p>Remove Files</p>	<ul style="list-style-type: none"> ➔ 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:

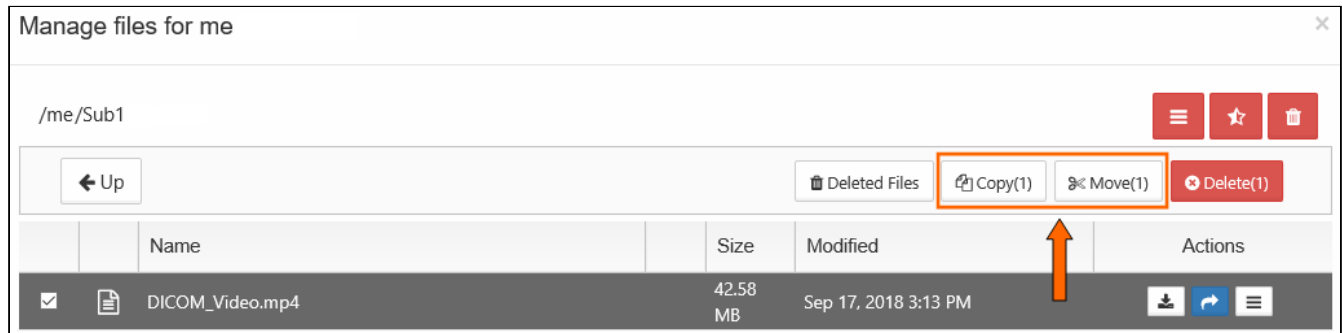
- Move folders for teams

- 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 .

Downloading Large Numbers of Files Using the Command Line Tool

 The file download tool is available in FileCloud 21.2 and later.

The most efficient way to download large numbers of files at once is through FileCloud's file download tool.

The tool is `filedownloader.php` and is located in `C:\xampp\htdocs\resources\tools\fileutils`

PHP should be installed on the system on which the tool is run.

To download files using the tool:

1. Create an ini file for the tool, for example, `C:\tool\downloadfiles.ini`, with the parameters in the following example and your own values replacing the values on the right.
The path that contains the files to be downloaded is **cloudpath**, and the path where the files will be downloaded is **destpath**.
Set **disablefilelogging** to **true** to avoid creating an overly large log file.


```
username=tester
password=qwerty123
serverurl=https://myserver.com
cloudpath=/tester/downloads
destpath=C:\samplefiledownloads
disablefilelogging=true
```

2. Enter the following commands to run the tool:

```
cd C:\xampp\htdocs\resources\tools\fileutils
C:\xampp\php\php.exe filedownloader.php --ini C:\tool\downloadfiles.ini
```

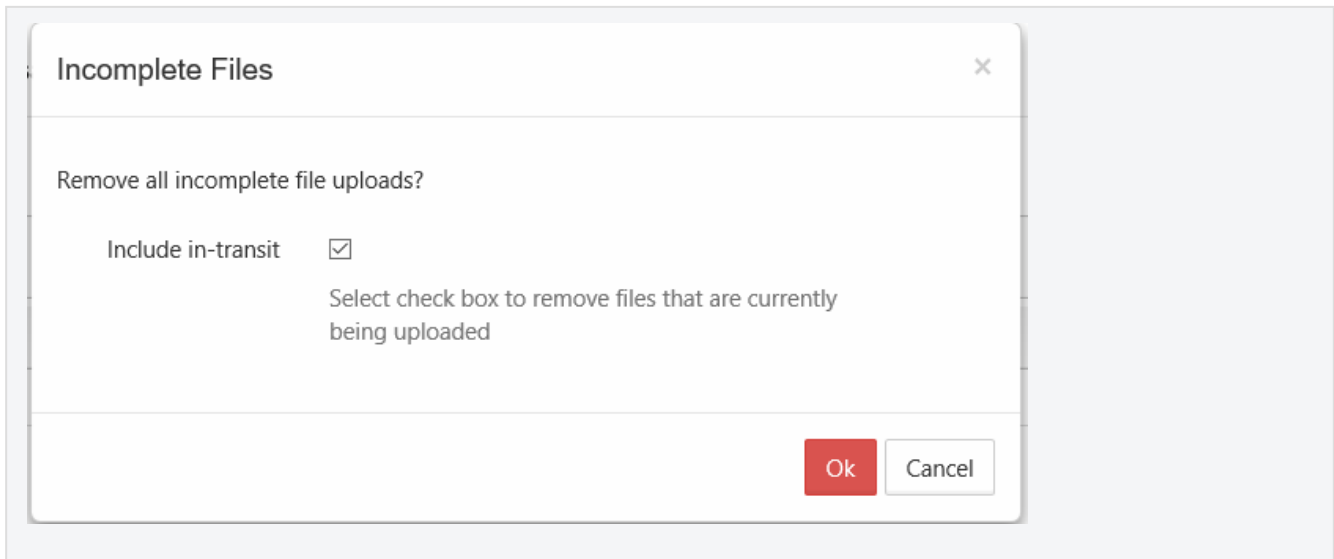
Note that this tool can be copied to any remote location and run. It does not require FileCloud to be present on the same system that the tool is run on.

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.

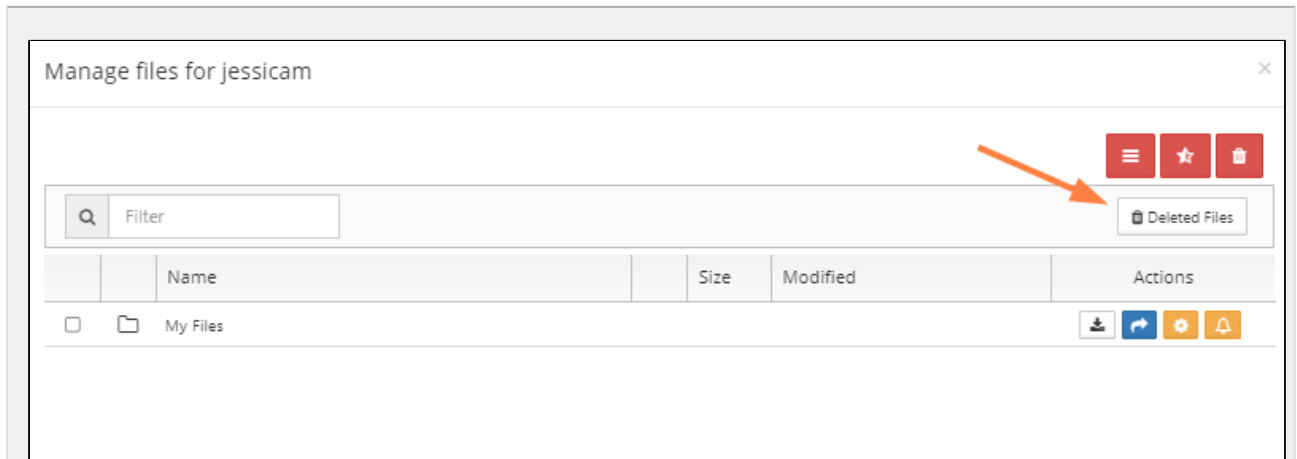
- If you have a policy that stores deleted files, they are saved in the Recycle Bin
- This means that they can be recovered if deleted by mistake or are needed again at a later time
- You can also set the Recycle Bin to automatically delete through a policy

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

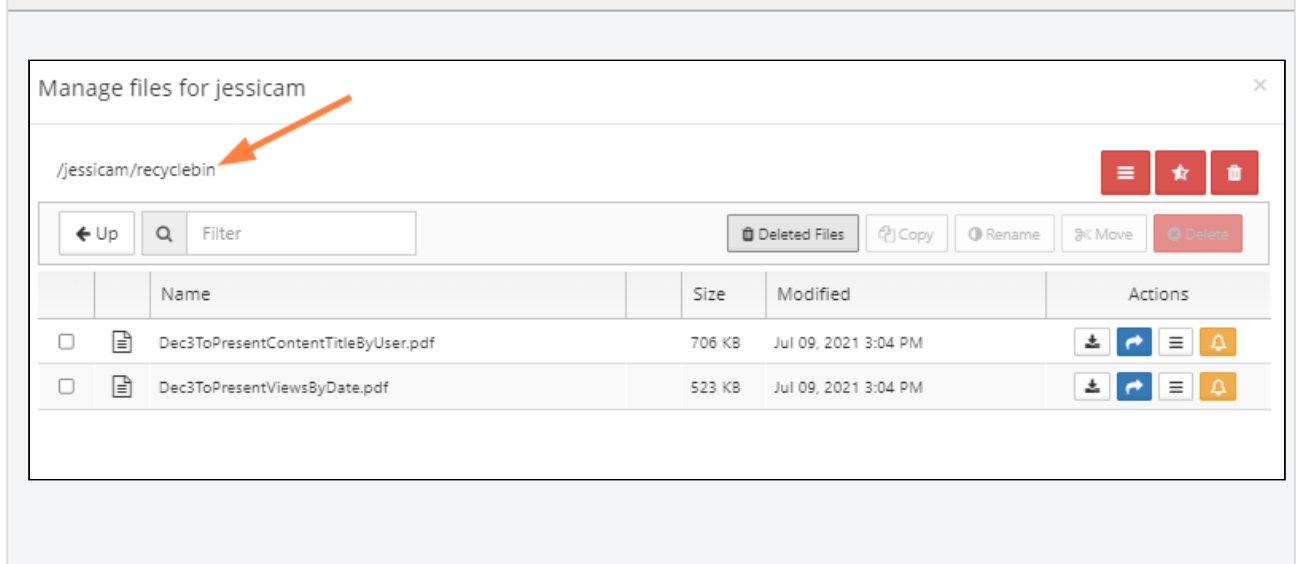
Go to the recycle bin

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:

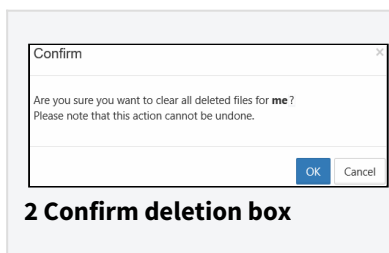


1 Manage Files dialog box, Deleted Files button



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

Run a tool to clear a recycle bin larger than 16 MB

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.

- The utility is at WWWROOT/fileutils/rmutil.php
-  This tool can be used not only for emptying recycle bin, but also any folder path. Please use it with caution.
- Usage:
 - [Optional] -h <host> Site host name or 'default' for default site. If not specified, command uses default site.
 - [Required] -u user account whose files are being removed from the recycle bin
 - [Required] -p path to the user's recycle bin which you want to delete
 - [Optional] -r 1 remove files in the destination (For a test run, do not specify this option.)
 - [Optional] --useaggregation Use this to prevent orphaned files from remaining if delete operation only partially finishes. Instead of relying on parent/child relationships, this causes the command to reconstruct the path of each file and folder after the initial delete operation, enabling it to identify and delete orphans.

To run the utility:

1. **Open a command line prompt.**
2. **Use the following code to navigate to the directory containing the utility**

```
cd C:\xampp\htdocs\resources\tools\fileutils
```

3. **Use the following command to delete files and folders under the path /user1/recyclebin/ (replace the sample parameters with your own data)**

```
C:\xampp\php\php.exe rmutil.php -h default -u jdoe -p /jdoe/recyclebin/ -r 1
```

To run the utility with the option to delete orphaned files:

```
C:\xampp\php\php.exe rmutil.php -u jdoe -p /jdoe/recyclebin -r 1 --useaggregation
```


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    

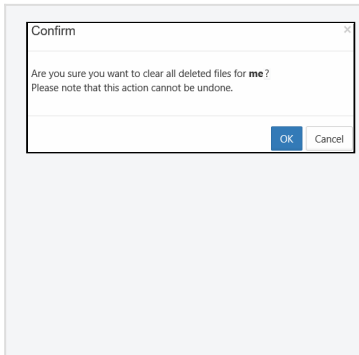
		Name	Size	Modified	Actions
<input type="checkbox"/>		Sub1 		Sep 18, 2018 10:13 AM	  
<input type="checkbox"/>		backups		Oct 26, 2018 11:13 AM	  
<input type="checkbox"/>		059c1770e5e39c50d5efa5ced3b913d2--writing-process-writing-tips.jpg	107 KB	Jul 25, 2018 2:39 PM	  

Manage files for me ✕



  




		Name	Size	Modified	Actions
<input type="checkbox"/>		My Files			  



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.





💡 If a file upload is in progress:

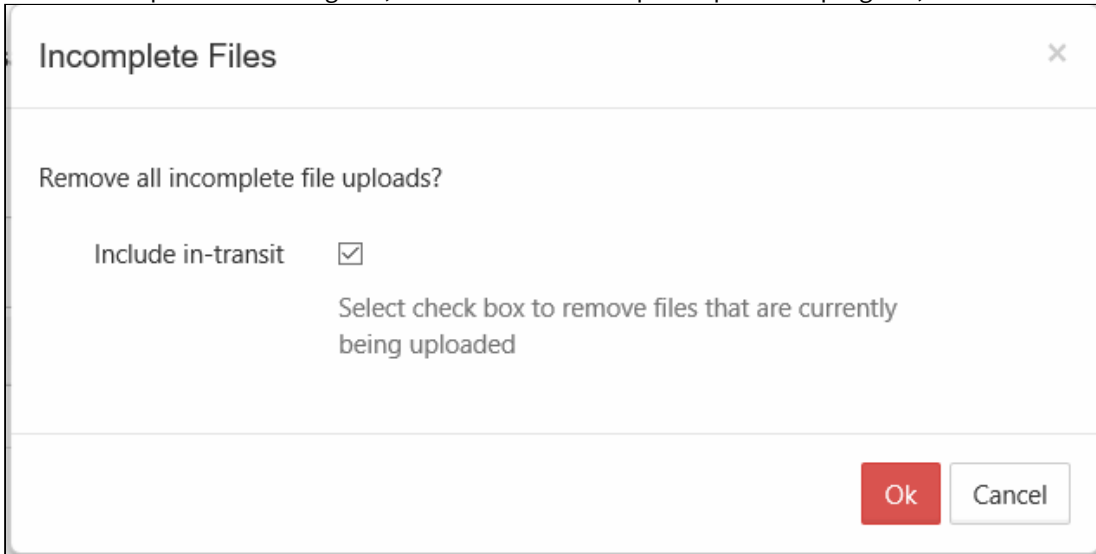
- It will not be removed, even if it only partially uploads, unless you use the In-transit option when removing partial uploads
- You can use the In-transit option to cancel a partial upload in progress

➔ [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

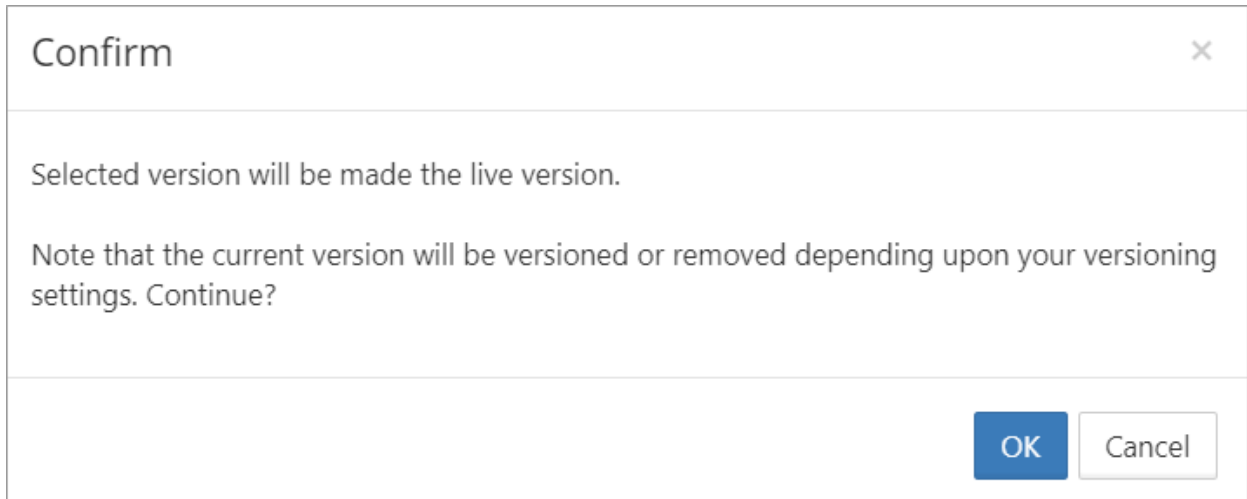
8. Select the version that you want to make live, and click the **Make it Live** icon  .

Previous Versions

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	
Version 2	87 B	Jun 16, 2021 12:44 PM	Created by jenniferp	
Version 1	40 B	May 28, 2021 01:01 PM	Created by jenniferp	

3 Previous Versions dialog box, Make it Live icon

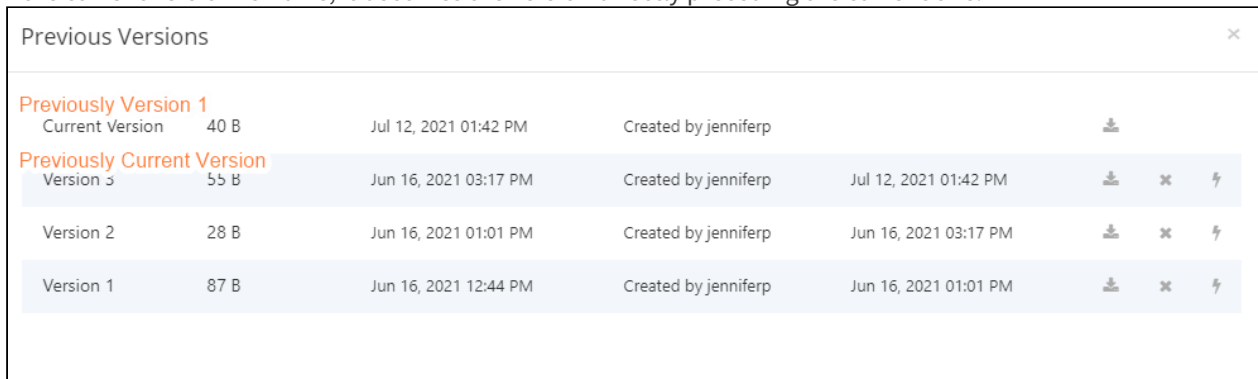
The following confirmation box appears.



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

Critical Section Cleanup Tool

i The FileCloud Critical Section Cleanup tool is available in FileCloud version 21.1 and later

After a move or copy operation for a large folder, the critical section is automatically released. However, if there is a server exception that interrupts regular FileCloud processing, a critical section record may remain and block other operations in the folder.

Manual Cleanup

The Critical Section Cleanup tool is a CLI tool that guides you in manually searching for and deleting critical section records. You may indicate how old the records must be to be included in the search.

The tool is `criticalsectioncleanup.php` and is located in `C:\xampp\htdocs\resources\tools\criticalsection`.

To run the tool, in a command line, enter the following. Note that `-h multitenant.site2-name.com` is optional and indicates the hostname if you want to look at a host other than the default.

for Windows:

```
C:\xampp\php\php.exe C:
\xampp\htdocs\resources\tools\criticalsection\criticalsectioncleanup.php -h
multitenant.site2-name.com -d 0
```

for Linux:

```
php /var/www/html/resources/tools/criticalsection/criticalsectioncleanup.php -h
multitenant.site2-name.com -d 0
```

Parameters:

`-h [host]` - (optional) - The hostname. Use this if you want to look at a host other than the default.

`-d [#days]` - (optional) Delete all records older than # days, for example, `-d 0` means delete all records older than today; `-d 10` means delete all records older than 10 days ago.

If you do not specify a value for `-d`, the response will appear similar to the following. Respond to the questions asked in the prompts, and specify the number in brackets when indicating which record you want to delete.

```
=====
=====

Looking at default host. Use option -h [HOST_NAME] to target other non default host.

>>> Please enter number of days to filter records. (e.g. 1 will fetch records older than
1 day. Leave empty to not filter by days)
>>>
>>> Please enter a partial or full FileCloud path to search critical section records.
(Leave empty to not filter by path)
>>>
>>> Found 3 record(s)
>>> ---- [1] /user0/folder1 ... 2021-03-31
>>> ---- [2] /user0/folder2 ... 2021-03-31
>>> ---- [3] /user0/folder3 ... 2021-03-31
>>> Do you want to select a record for removal? (Y/N):
>>> Y
```

```

>>> Please enter the number of record you want to delete:
>>> 1
>>> Deleted /user0/folder1
>>> Do you want to select a record for removal? (Y/N):
>>> Y
>>> Please enter the number of record you want to delete:
>>> 3
>>> Deleted /user0/folder3
>>> Do you want to select a record for removal? (Y/N):
>>> Y
>>> Please enter the number of record you want to delete:
>>> 2
>>> Deleted /user0/folder2
>>> Do you want to select a record for removal? (Y/N):
>>> N
>>> Exit command

```

If you specify a value for -d, the response will appear similar to the following. Respond **Y** to **Do you want to delete all records?** to confirm deletion of the records.

```

C:\xampp\htdocs\resources\tools\criticalsection> php criticalsectioncleanup.php -d 10
=====
### Critical Section Cleanup

**criticalsectioncleanup.php** allows searching for critical section records filtering
by path
and remove records selecting from the result list.
The command prompts the user before any action, so can be safely run and then follow the
prompt
messages.

#### Usage

php ./criticalsectioncleanup.php -h <site_url>'

[optional] site_url: full qualified site url of the site to be exported or to be import
target (multitenant).
If not specified, default site is assumed.
=====

Looking at default host. Use option -h [HOST_NAME] to target other non default host.

>>> Found 2 record(s)
>>> ---- [1] /user0/load/file2 ... 2022-11-18
>>> ---- [2] /user0/load/fixedtreen_local/file ... 2022-11-18
>>> Do you want to delete all records? (Y/N):

```

Note: If some critical section records have an expiry time which was set using a maximum PHP integer value, the tool may not delete the records because it does not evaluate them as older than the specified number of days.

A workaround is to enter a very large negative number of days so the tool selects and deletes those records, for example:

```
Looking at default host. Use option -h [HOST_NAME] to target other non default host.

>>> Please enter number of days to filter records. (e.g. 1 will fetch records older than 1 day. Leave empty to not filter by days)
>>> -999999999999999999
```

Automatic removal of critical section entries

To configure FileCloud to automatically remove critical section entries older than 3 days:

1. Open cloudconfig.php.
 - Windows Location : C:\xampp\htdocs\config\cloudconfig.php
 - Linux Location : /var/www/html/config/cloudconfig.php
2. Add the following:

```
define("TONIDOCLOUD_CRITICAL_SECTION_CLEANUP_DAYS", '3')
```

:

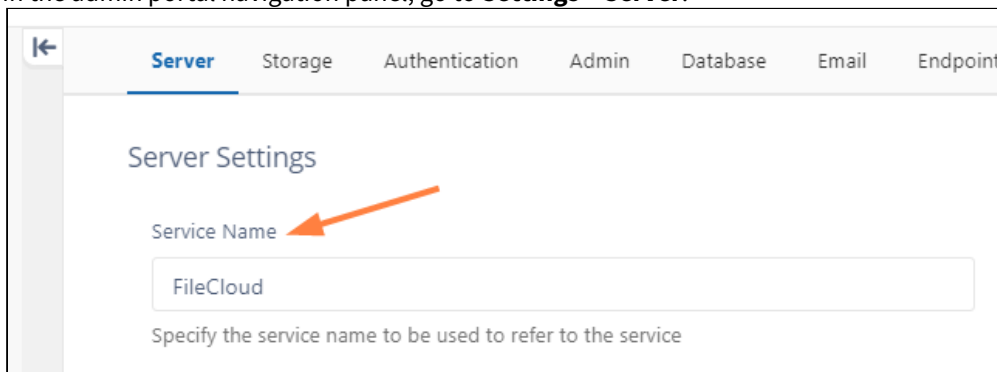
Change the Name of the Zip File for Multiple File Downloads

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:

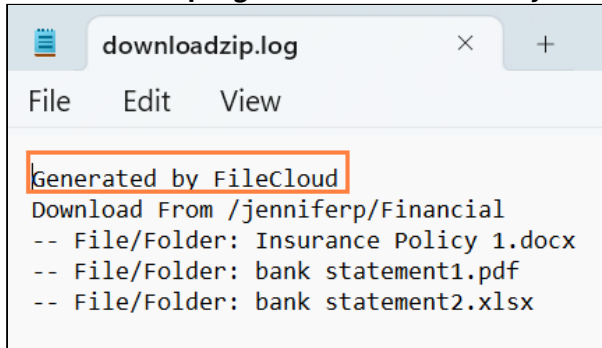
1. In the admin portal navigation panel, go to **Settings > Server**.



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**:

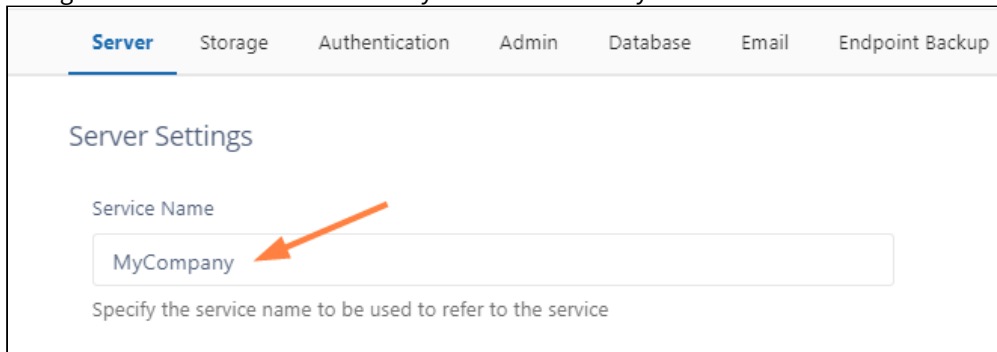


```

downloadzip.log
File Edit View
Generated by FileCloud
Download From /jenniferp/Financial
-- File/Folder: Insurance Policy 1.docx
-- File/Folder: bank statement1.pdf
-- File/Folder: bank statement2.xlsx

```

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




Server Settings

Service Name

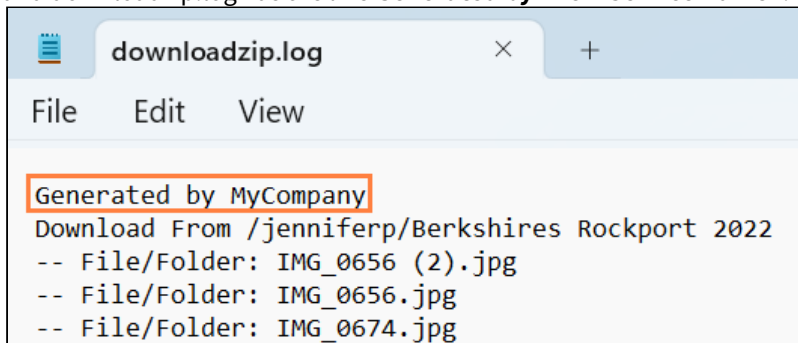
MyCompany

Specify the service name to be used to refer to the service

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.

User Details

Name	jessica	Total Quota	Unlimited
Email	[Redacted]	Used Quota	59.2 MB
Last Login	16 Jun 2022 14:50	Available Quota	0 B
TOS Date	Not Accepted	Used Storage	59.2 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:

Authentication:

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

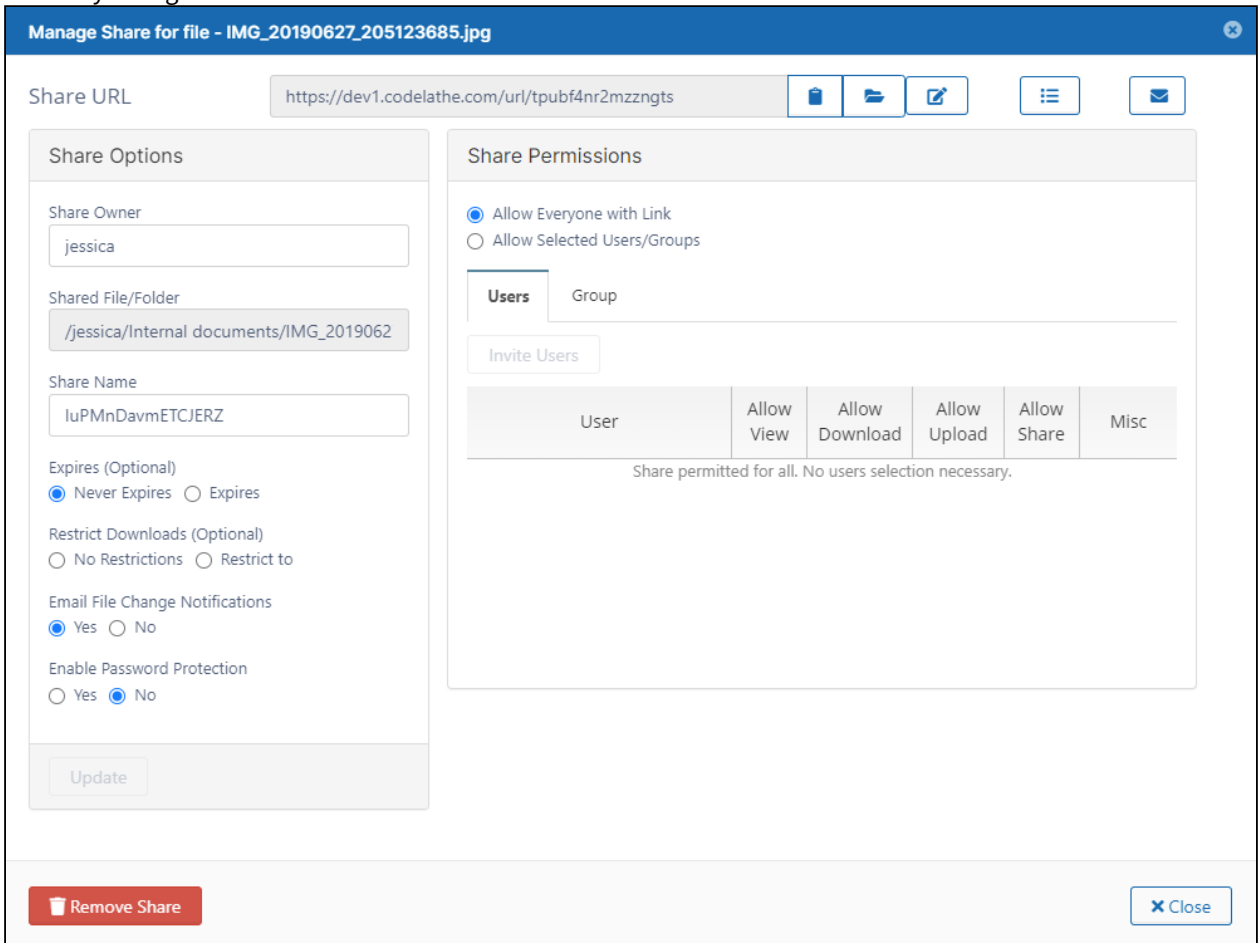
A **Manage shares for [user]** dialog box opens.

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



The **Manage Share** dialog box opens.

- Make any changes to the share.



To manage user shares for all users:

- Log on to [Administration Panel](#).
- 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.

Share URL: https://...

Share Options

Share Owner: jennifer

Shared File/Folder: /jennifer/Common files/075b2598e4b748f

Share Name: 075b2598e4b748f5972e98b1250a6421.jpe

Expires (Optional): Never Expires Expires

Email File Change Notifications: Yes No

Share Permissions

Allow Everyone with Link

Allow Selected Users/Groups

Guest 1 Group

Invite Users

User	Allow View	Allow Download	Allow Upload	Allow Share	Misc
Guest 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	[Info] [Edit]

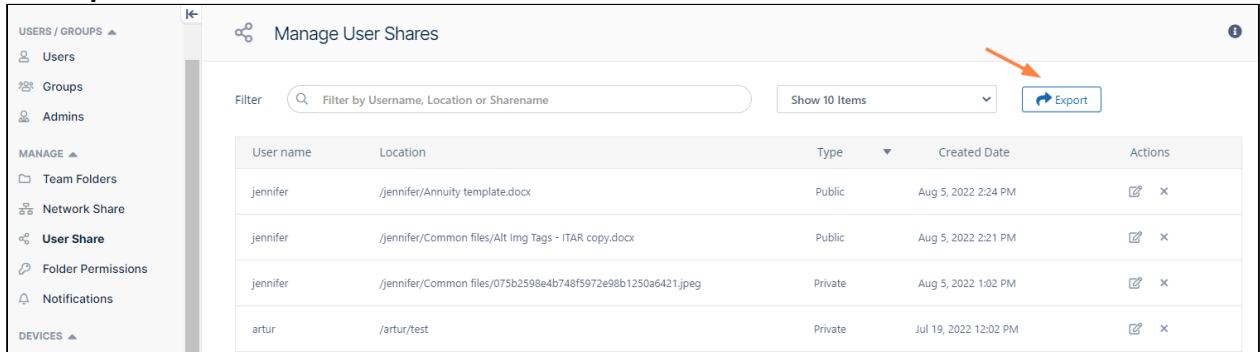
Page 1 of 1

Remove Share Close

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 http://127.0.0.1/url/hjyxze4pmqmbjaj

Share Options

Share Owner
jenniferp

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

Share Name
FCSwitchToClassic.png

Expires (Optional)
 Never Expires Expires

Email File Change Notifications
 Yes No

Update

Share Permissions

Allow Everyone
 Allow Selected Users/Groups

Invite Users

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.

Remove Share
✕ Close

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/ASBeachj.tif	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

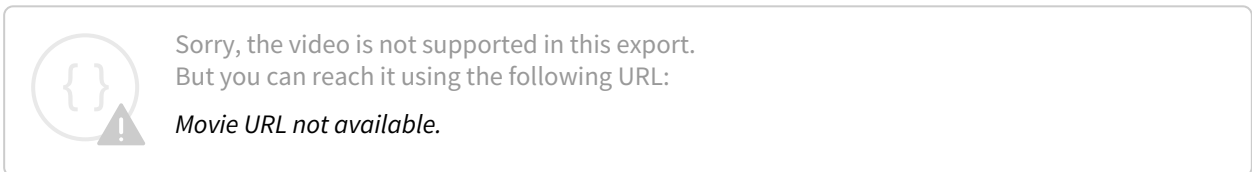
Public folder shares provide a share link that opens a page listing the contents of the folder. By making minor changes to the share link, a direct downloadable link for any file in the folder can be created.

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.



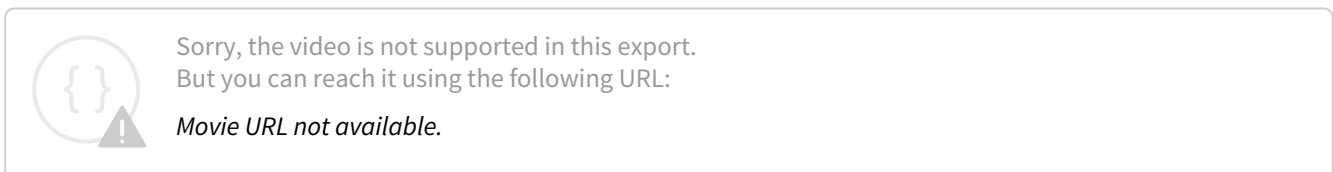
To create a direct link to a file in the shared folder:

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!/bli3S5COtIoHQD49yINBKMS5/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!/bli3S5COtIoHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

Modified link

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5COtIoHQD49yINBKMS5/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!/bli3S5COtIoHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

Modified link

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5COtIoHQD49yINBKMS5/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.

In this section

- [Storage Scanner Tool for Missing Files](#)
- [Storage Usage Tool](#)

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](#)


Network Shares

- ➔ [Clear All Deleted Files from a Network Folder](#)
- ➔ [Clear All Deleted Files from an S3-Based Network Folder](#)
- ➔ [All Network Folder Options](#)

Protecting Your Storage

- ➔ [Set Up Encryption for Managed Storage](#)
- ➔ [Enable Antivirus Scanning](#)
- ➔ [Create an IAM User Policy for S3 Access](#)

Storage Scanner Tool for Missing Files

 The Storage Scanner tool is available in FileCloud version 21.1 and later.

The storage scanner tool checks if each file entered into the FileCloud database has a corresponding physical file in storage. If a physical file is missing, the storage scanner prints its database entry details. An admin can remove the invalid files listed from the database.

The tool is `storagescanner.php`, and is located in `C:\xampp\htdocs\resources\tools\fileutils`

To run the Storage Scanner tool:

1. In a command line enter:

For Windows:

```
cd c:\xampp\htdocs\resources\tools\fileutils
PATH=%PATH%;C:\xampp\php
```

For Linux:

```
cd /var/www/html/resources/tools/fileutils/
```

2. Then, for both Windows and Linux, enter:

```
php storagescanner.php [-h hostname]
```

Parameters

`-h hostname` - (optional) fully qualified name of the site in a multisite installation. Do not include this parameter for a default site or a standalone site.


Sample output

```
Looking at default host
-----
Scanning storage for missing files
-----
Processed count : 100
Processed count : 200
Processed count : 300
Missing file in storage: /tester/3/vHGK.docx ->
0/5ecbc9bfa5e39606437822/5ecbc9bfa9a8a133028276/602ef8f0e35bb575222337.dat
Missing file in storage: /tester/3/Lsp.doc ->
0/5ecbc9bfa5e39606437822/5ecbc9bfa9a8a133028276/602ef90638ae0643407781.dat
```

```
-----
-----
Scanning complete
-----
```

```
Folders Scanned           : 43
Files Scanned            : 351
-----
```

Storage Usage Tool

 The Storage Usage tool is available in FileCloud version 21.1 and later.

The storage usage tool lists the storage used by the users on your FileCloud system.

The tool is **storageusageutil.php** and is located in **C:\xampp\htdocs\resources\tools\fileutils**

To run the storage usage tool:

```
php storageusageutil.php -u user -p path -h hostname
```

Parameters:

-u *user* - (required) - The user account (*all* for all user accounts)

-p *path* - (required) The path of the storage to be calculated


-h *hostname* - (*optional*) The fully qualified name of the site in a multisite installation. Omit the option for standalone or default site

Sample output

```
Looking at default host
Found 100 file(s)
Found 200 file(s)
Found 300 file(s)


-----
-----
Storage Usage
-----
Folder count           : 19
File count             : 349
File(s) size in bytes   : 974902531
File(s) size in GB : 0.91
-----
```

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				Clear All Locks	i
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

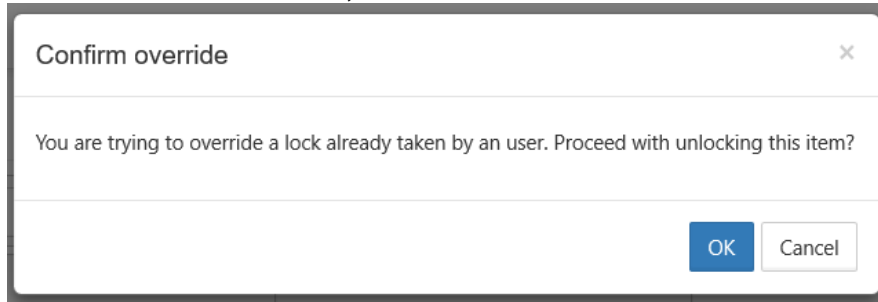
There are times when you may need to unlock a file for a user.

- 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 ().

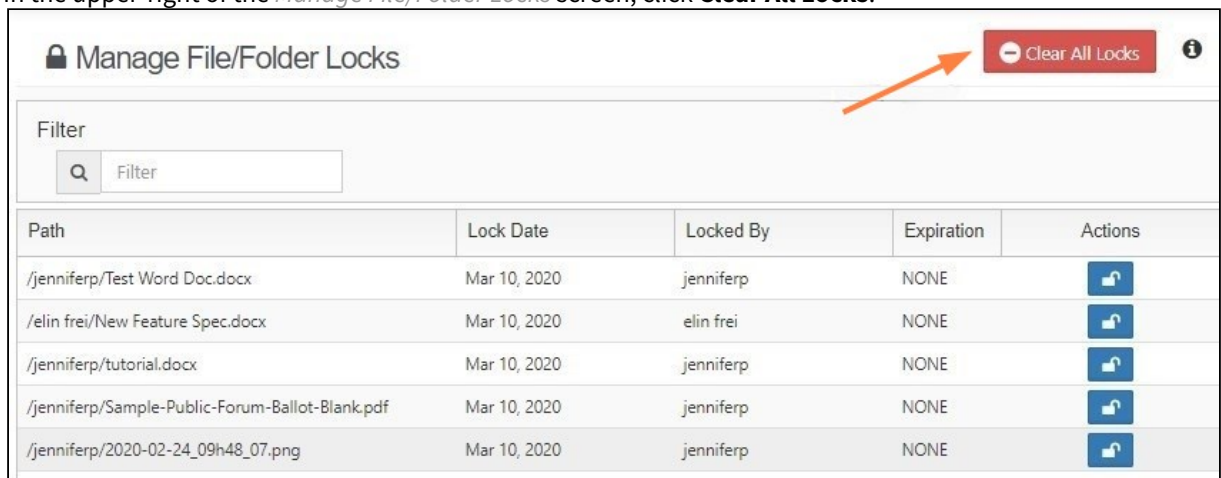
5. On the *Confirm Override* screen, click *OK*.



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 a dark row, 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:

Authentication:

Email:

[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	Edit Delete

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.

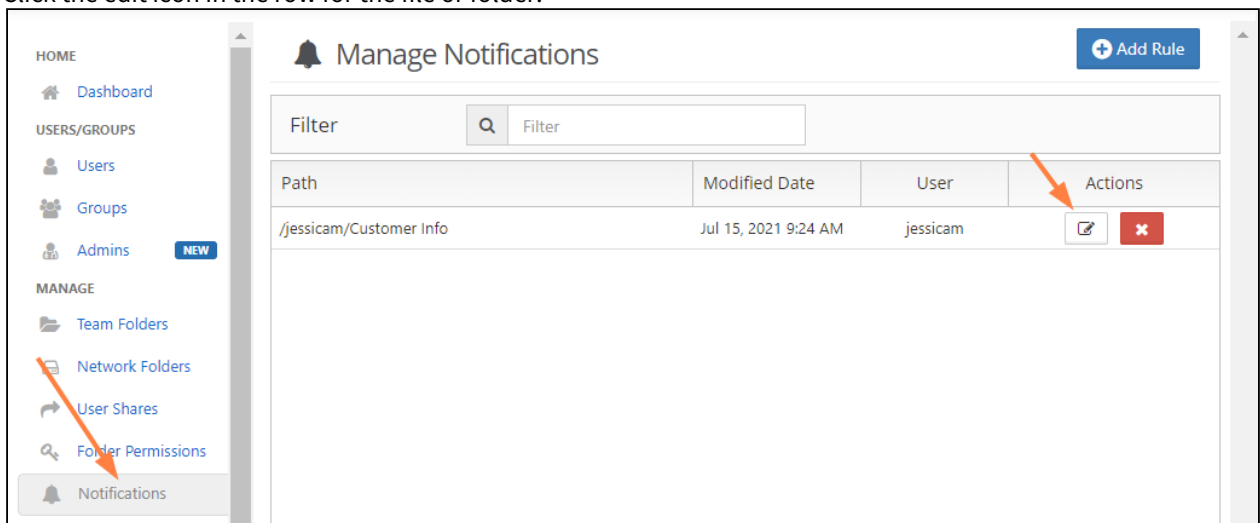
- If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
- If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications** box.
- If the user has **Use default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

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)

1	2	3	4	5	6	7	8	9	10	11	12
Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs		
<input checked="" type="checkbox"/>		Green	FileCloud Drive (DESKTOP-...)	jessicam	FileCloud Drive (DESKTOP-...)	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	
<input type="checkbox"/>		Yellow	Cloud Sync (DESKTOP-...)	jenniferp	Cloud Sync (DESKTOP-...)	App version: 21.1.0.5865 OS: Windows 10 - 10.0 (Build 19042)	At 02:30 PM on Jul 21 2021 from 127.0.0.1	Approved	Allowed	0	


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.

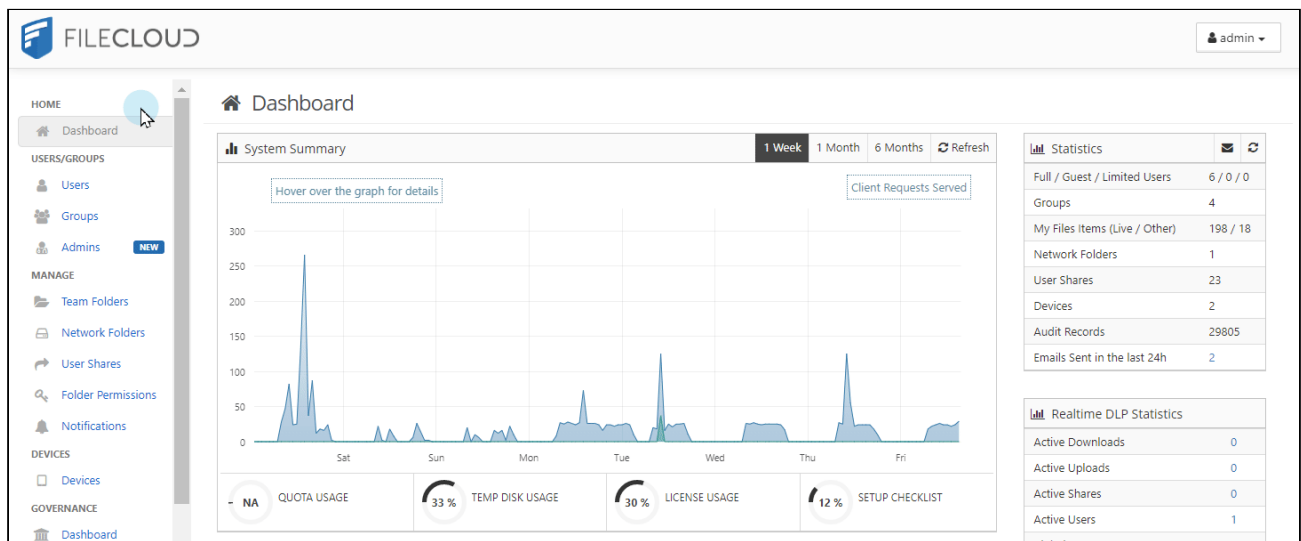
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

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

Property	Value
Single File Cache Limit	100 MB
Lock Automatically on Edit	Disabled
Automatic Check for Updates	Disabled
MAC Address	4CCC6A448B835
Mute Drive Notifications	Disabled
Automatically Start Drive on Windows Startup	Enabled
Automatic Login on Drive Startup	Enabled
Mount Point	M:
Login Mode	Username and Password
DocIQ Office Integration	Enabled

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.

	Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
<input type="checkbox"/>				Cloud Sync (DESKTOP-SJA6P50)	App version: 20.1.0.3224 OS: Windows 10 - 10.0 (Build 18362)		Approved	Allowed	0	
<input type="checkbox"/>				Android-samsung-SM-A505GT	App version: 191 OS: Android - 10		Approved	Blocked	1	
<input type="checkbox"/>				Cloud Sync (DESKTOP-2URQJ6S)	App version: 20.2.0.4611 OS: Windows 10 - 10.0 (Build 18362)		Approved	Allowed	0	
<input type="checkbox"/>				Android-samsung-SM-G950F	App version: 190 OS: Android - 8.0.0		Approved	Allowed	0	
<input type="checkbox"/>				Android-Xiaomi-Mi A3	App version: 190 OS: Android - 10		Approved	Allowed	0	
<input type="checkbox"/>				iPhone 11 Pro Max	App version: 20.2.0.0 (1) OS: iOS - 14.0		Approved	Allowed	0	
<input type="checkbox"/>				FileCloud Drive (DESKTOP-SJA6P50)	App version: 20.2.0.4717 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	
<input type="checkbox"/>				Cloud Sync (DESKTOP-PSQC2JU)	App version: 20.2.0.4680 OS: Windows 10 - 10.0 (Build 19041)		Approved	Allowed	0	
<input type="checkbox"/>				FileCloud Drive (DESKTOP-2URQJ6S)	App version: 20.2.0.4704 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	
<input type="checkbox"/>				FileCloud Drive (DESKTOP-SJA6P50)	App version: 20.2.0.4672 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	

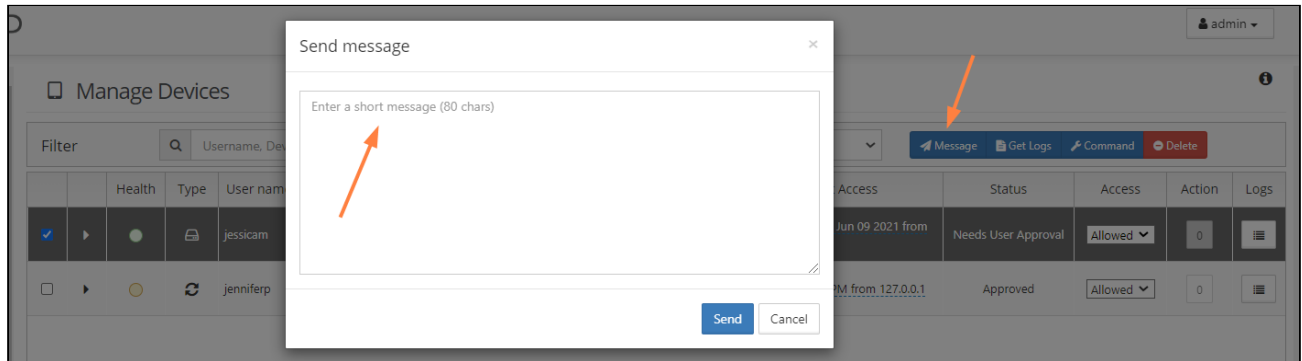
To view Actions:

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.

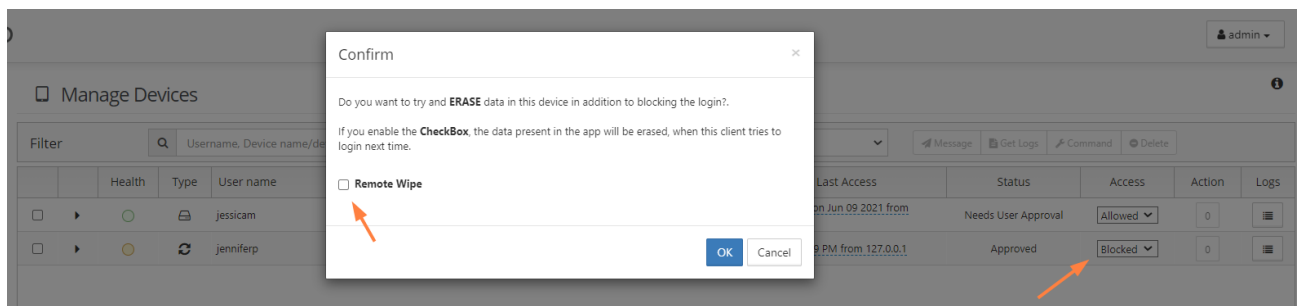
When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

- 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*.

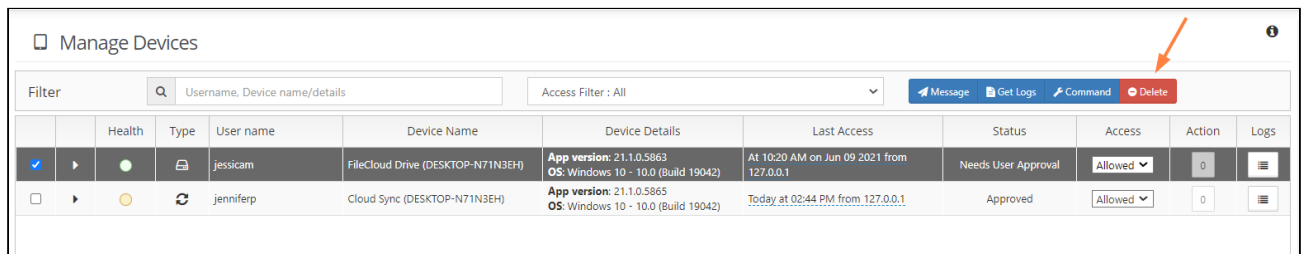
Delete a Client Device Record

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 and an 'Access Filter' dropdown set to 'All'. A toolbar contains buttons for 'Message', 'Get Logs', 'Command', and 'Delete'. The 'Delete' button is highlighted with an orange arrow. Below the toolbar is a table with columns: Health, Type, User name, Device Name, Device Details, Last Access, Status, Access, Action, and Logs. Two devices are listed:

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.

Disable Remote Management in Sync Clients

In the Sync client, by default users can see a setting called: *Allow Remote Management*

- This setting allows Sync users to manage their Sync application by overriding an Administrator's settings
- In some cases, administrators want to disable this toggling
- In FileCloud Server version 19.1 and later, an administrator can disable this option 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.

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](#)
- [Automating FileCloud Sync/Drive/OutLook-Addin Installation and Mass Deployment configuration](#)
- [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?

There can be a few reasons why the XML code in your policy isn't working:

- You are running FileCloud Server version 18.1 or older
- Your XML code is not correct

Older Versions of FileCloud

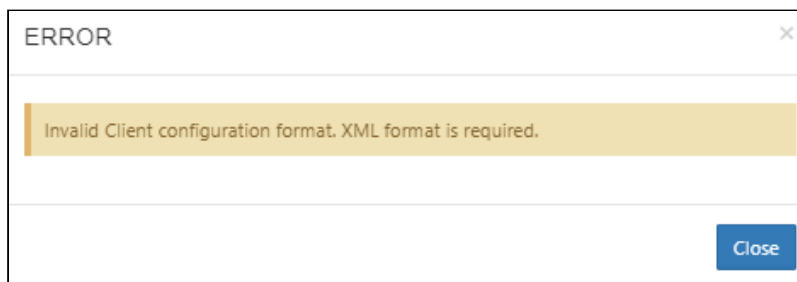
If you are not running FileCloud Server version 18.2 or later, you are missing the following bug fix:

! ISSUE: Device configuration in the Policies is not being applied by the desktop clients. The xml configuration needed to be corrected.
RESOLUTION: FileCloud Server now validates XML code before a device configuration can be saved.

[➔ Upgrade FileCloud](#)

Incorrect XML Code

After you upgrade to FileCloud Server 18.2, 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.

The screenshot shows a 'Policy Settings' window with a close button (X) in the top right corner. Below the title bar, there is a note: 'Note: Some policy settings will not be applicable for Guest and Limited users.' The interface features a horizontal tabbed menu with the following tabs: 'General', '2FA', 'User Policy', 'Client Application Policy', 'Device Configuration' (which is currently selected and highlighted), and 'Notifications'. Under the 'Device Configuration' tab, the section is titled 'Manage Device Configuration'. It contains a sub-section 'Client Configuration' with a large, empty rectangular text area. Below this area, a note reads: 'Specify default configuration for all client applications. This has to be a valid XML value.' At the bottom right of the window, there are three buttons: 'Save' (blue), 'Reset' (red), and 'Close' (white with a grey border).

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	Assigns the maximum single file download limit to the supplied value. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  The download limit does not apply to the following file types: .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, and .indd. </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>

XML Tag	Value	Example
driveopenexploreronstartu p	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>
disableprecaching	Setting this value to 1 disables precaching. If many Drive users have access to a large data structure, the FileCloud server may experience a high load. This can be avoided by deactivating precaching. However, folder contents will no longer be cached in Drive which can lead to longer response times.	<disableprecaching>1</disableprecaching>
disableautologin	By default, once a drive is mounted, the authentication will be reused on every FileCloud Drive for Mac start ups. Setting this key to 1 will require authentication from user on every start up.	<disableautologin>1</disableautologin>
currentlanguage	See Translations for currently available languages.	<currentlanguage>english</currentlanguage>

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 value '3'.
- Save:** A blue button at the bottom left of the settings area.
- Status:** A bar at the bottom of the dialog indicating 'Not Connected'.

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

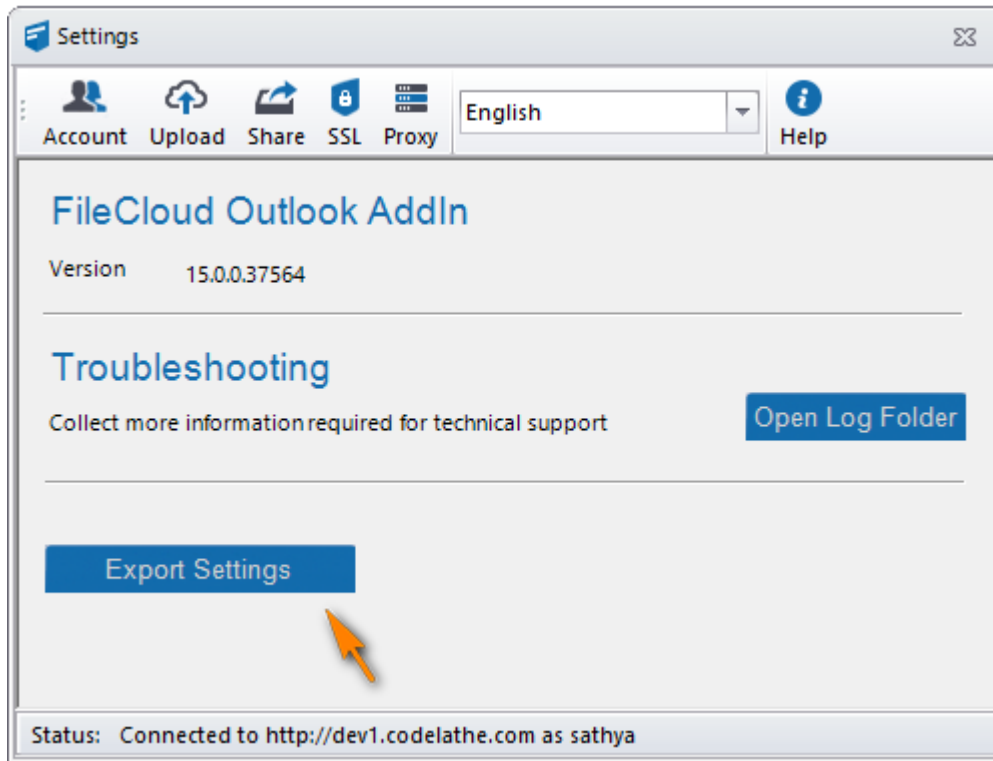
The following XML tags are supported for the Outlook Add-in

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...](#)



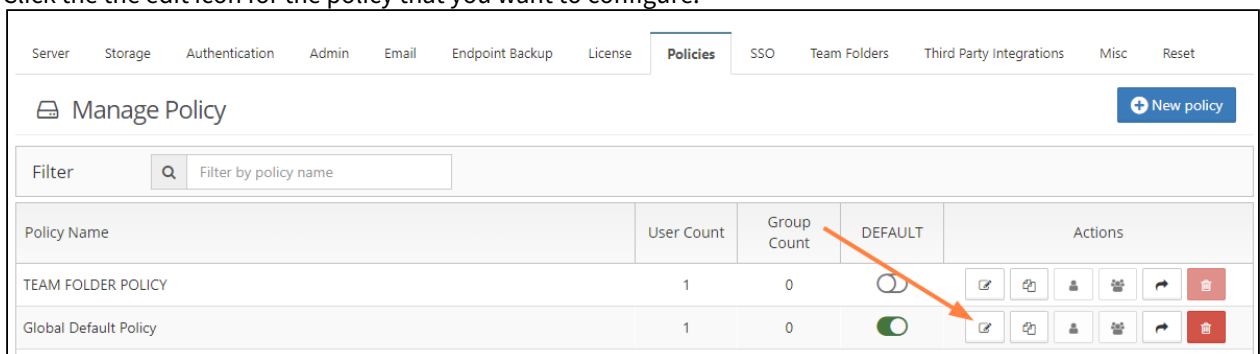
Device Configuration XML For Server Sync

Client Device configuration settings can be configured remotely using policies.

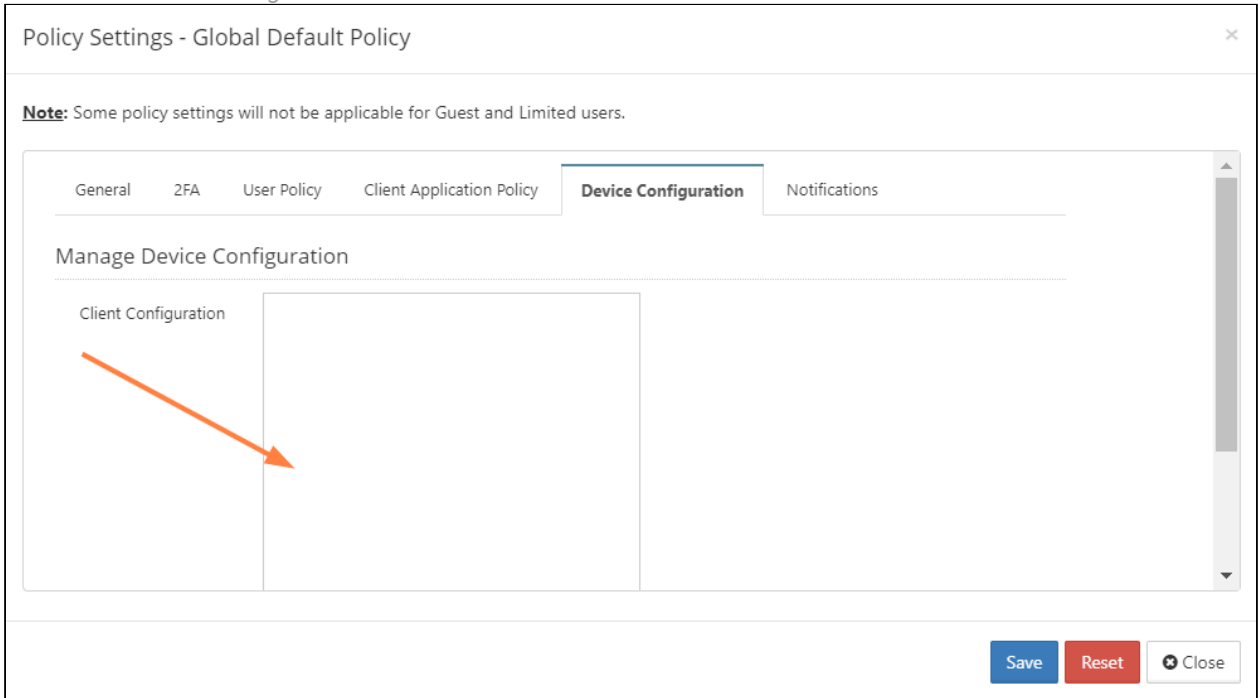
⚠ For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

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.	<code><limit_folder_count>0</limit_folder_count></code>

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.

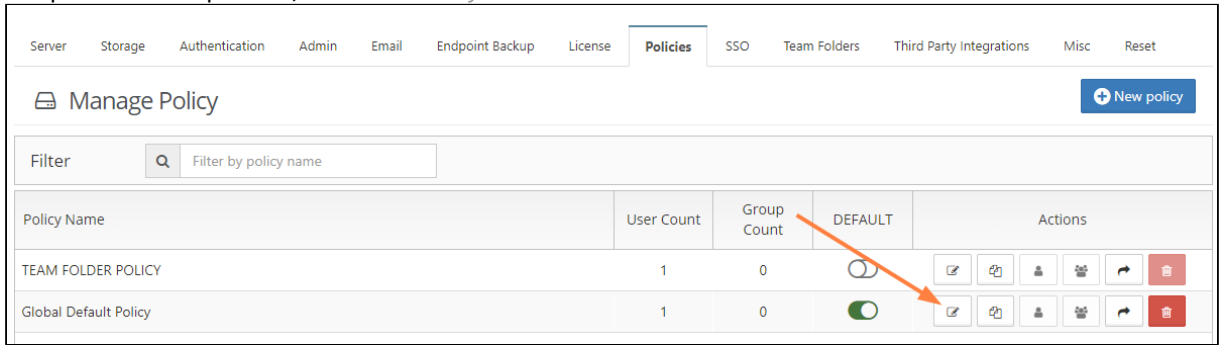
FAQs

How do I enter device configuration XML for Sync?

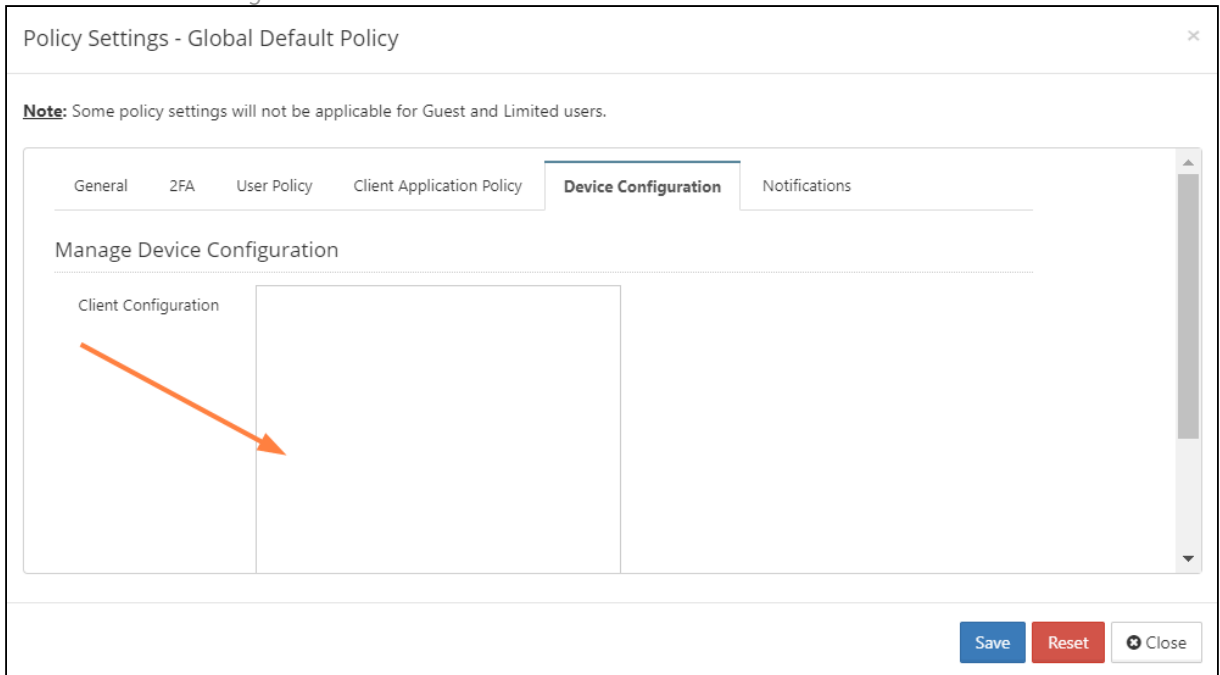
To set a device configuration for a policy:

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
---------	-------	---------

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

syncfrequency	number - Number in seconds to sync to the server (default is 120 seconds)	<syncfrequency>100</syncfrequency>
checkmodtime	0/1 - Advanced: check modification time in addition to size when checking for changes. Default is disabled.	<checkmodtime>1</checkmodtime>
checkcrc	0/1 - Advanced: check CRC in addition to size when checking for changes. Default is disabled.	<checkcrc>1</checkcrc>
removeunshared	0/1 - Delete locally synced folders that are unshared. Default is disabled	<removeunshared>1</removeunshared>
deleteapprovalpct	Number from 0 to 100, which indicates what % of files requires deletion approval. Default is 10. This applies only to file deletions in the local sync folder.	<deleteapprovalpct>20</deleteapprovalpct>
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>

albwforupload	<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>albwforupload</i> or <i>albwfordownload</i> is specified but <i>albwfromtime</i> and <i>albwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albwforupload></albwforupload></pre>
albwfordownload	<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>albwforupload</i> or <i>albwfordownload</i> is specified but <i>albwfromtime</i> and <i>albwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albwfordownload></albwfordownload></pre>
albwfromtime	<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>albwforupload</i> or <i>albwfordownload</i> is specified but <i>albwfromtime</i> and <i>albwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albwfromtime>16:45:00</albwfromtime></pre>
albwtotime	<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>albwforupload</i> or <i>albwfordownload</i> is specified but <i>albwfromtime</i> and <i>albwtotime</i> are missing, then the bandwidth values will not be set.</p>	<pre><albwtotime>24:00:00</albwtotime></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... 	<pre><altbwschedule_dayofweek>3</altbwschedule_dayofweek></pre>
timeactivecontrolsset	<p>Enables/Disables the Active Sync Hours settings</p> <p>1 = enabled</p> <p>0 = disabled</p>	<pre><timeactivecontrolsset>1</timeactivecontrolsset></pre>
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... 	<pre><activesync_daysofweek>5</activesync_daysofweek></pre>
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>	<pre><activesync_timeofday>8:00:00-20:00:00</activesync_timeofday></pre>
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> 	<pre><allowuserconfigforlimitsync>1</allowuserconfigforlimitsync></pre>

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>

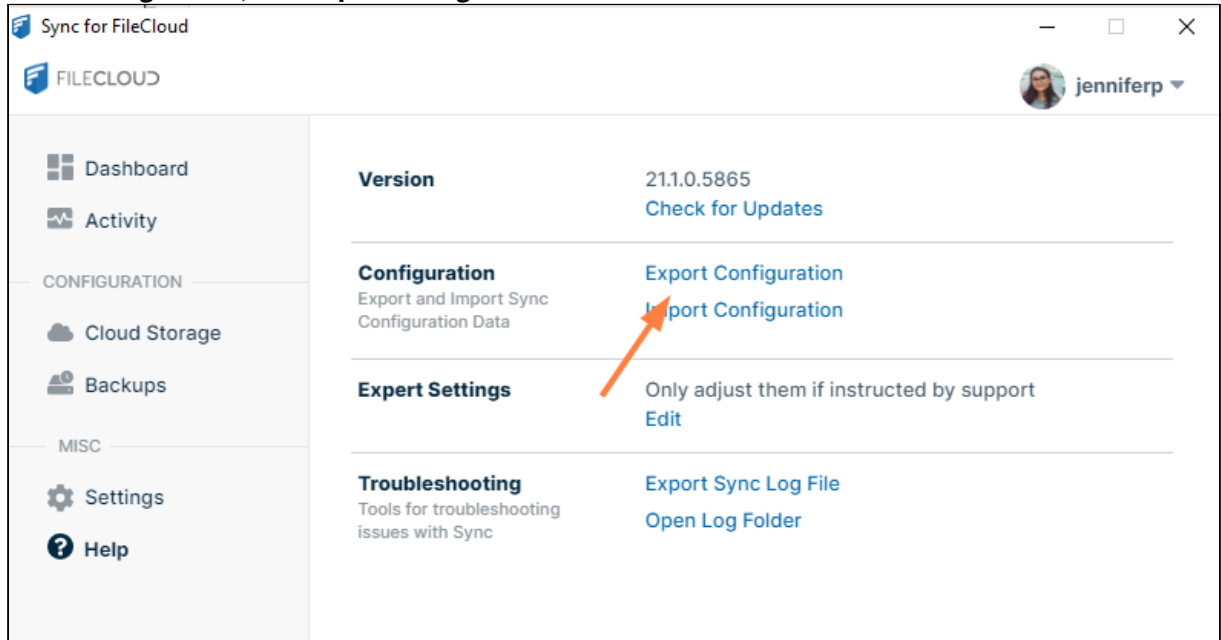
How do I get the configuration XML for Sync?

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
<i>None set but other settings are present</i>	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.
<i>None set but other settings are present</i>	0	<p>Because <i>allowuserconfigfornewfolders</i> is set to disable modifications:</p> <ul style="list-style-type: none"> • Sync users CANNOT modify Network Folders

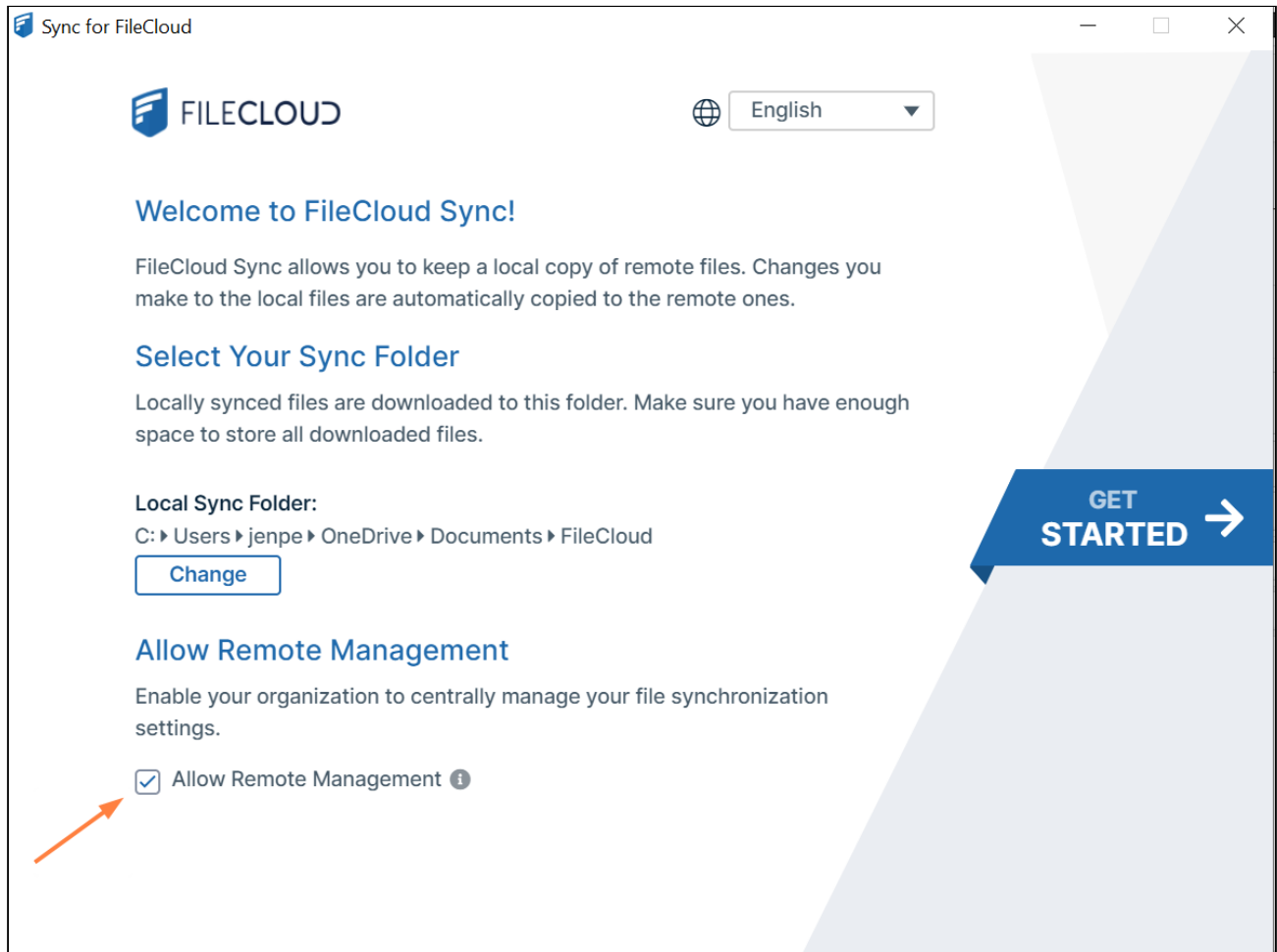
Controlling modifications to selective backup folders

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	Because offline folders (configured for backup) are present AND <i>allowuserconfigforbackup</i> is set to disable modifications: <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	Because <i>allowuserconfigforbackup</i> is set to enable modifications: <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	Because <i>allowuserconfigforbackup</i> is set to disable modifications: <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	<code><lockfiles>1</lockfiles></code>
runatstartup	0/1 - Enable or Disable running application at OS startup	<code><runatstartup>1</runatstartup></code>
mutenotifications	0/1 - Enable or Disable notifications	<code><mutenotifications>1</mutenotifications></code>

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																					
mutenotifications	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.

Automating FileCloud Sync/Drive/OutLook-Addin Installation and Mass Deployment configuration

Disclaimer

The following script has been created with the purpose of providing you with an example of how to install/mass deploy FileCloud Sync without user interaction and at the same time to automate the FileCloud's mass deployment configuration for the end user.

Requirements

- The PowerShell script, Bat file or Executable depending on your preference must be ran with elevated admin privileges.
- In case there is any download restriction created by your Firewall you will need to add <https://patch.codelathe.com> to your allow list.

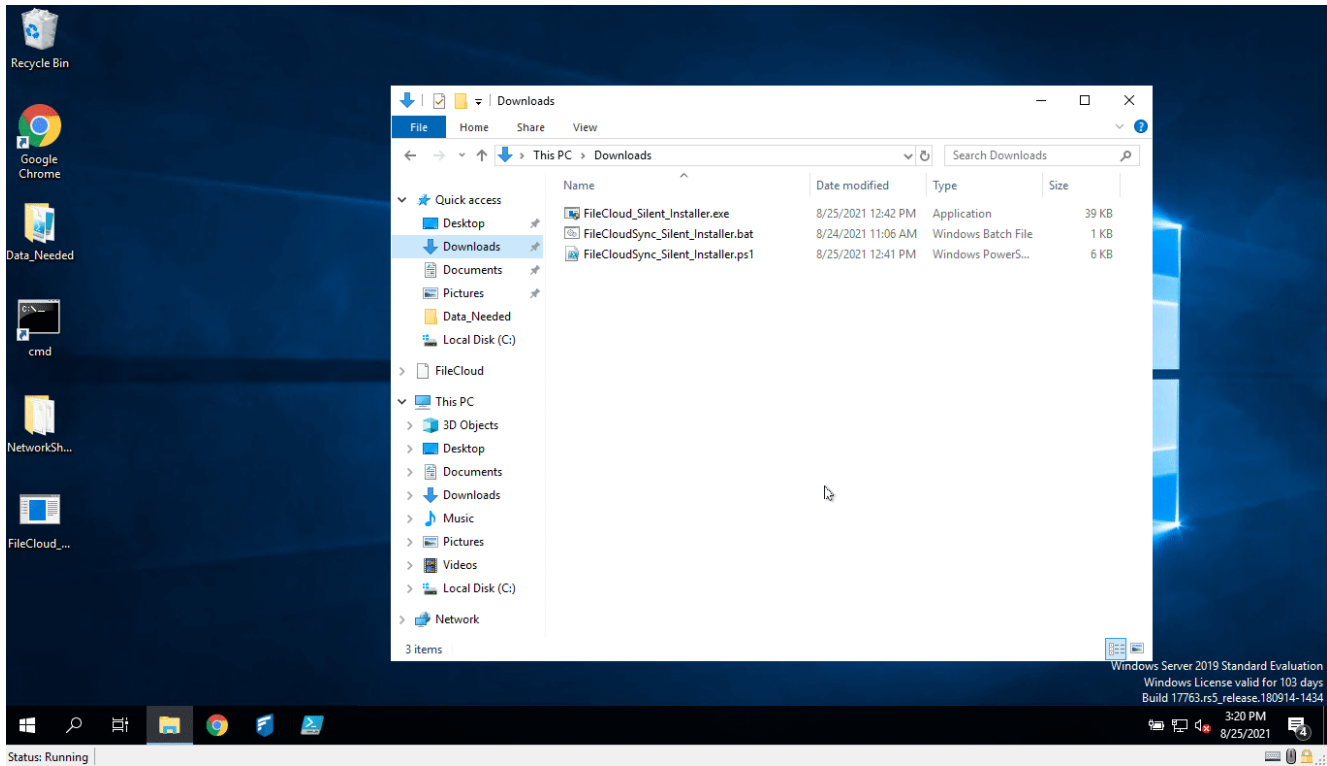
- FileCloud Sync must not be installed, If so proceed on uninstalling it and delete the folder under C:\Users\
%username%\AppData\Roaming\FileCloudSyncData\client
- You will need to update the script to customize and or add any mass deployment configuration needed, the ones provided are used for demonstration purposes. For example to update the URL you will need to modify line 134 to reflect your own URL rather than <https://your-filecloud-url.com>

What does the Script do?

The script below will accomplish the following actions when executed.

1. Change the Execution Policy on PowerShell to allow the scripts execution without any user intervention.
2. Validate if there is any log file under the name FileCloudSync_SilentInstaller.log within the C drive if so it will delete it and recreate it.
3. Validate if FileCloud Sync is already installed, If so the script will exit.
4. Create a directory under the C drive called FileCloudSync in which it will be used to download the FileCloud installer.
5. Download FileCloudSync.msi directly from FileCloud's server.
6. Validate if the installer has completely download and ensure that the installer was not altered during transit, this is done by validating the installers AES 256 hash. If the hash is not the same the installer will exit.
7. Proceed on silently installing FileCloud Sync without the need of any user input or interaction.
8. Create the registry entry for FileCloud's Mass Deployment configuration
9. Create the needed keys to assign the predefined settings based on [FileCloud's Mass Deployment documentation](#)
10. Once completed it will start FileCloud Sync, Delete the folder created, Delete the FileCloud Sync installer and Exit.

FileCloud Sync Installation & Mass Deployment automation - Video



FileCloud Sync Installation & Mass Deployment automation - Script

FileCloud's Sync and Mass Deployment PowerShell script

```

1  #####Silent FileCloud Sync Installation & Mass Deployment Configuration####
2
3  ##Allows the script to be executed without user consent##
4  set-ExecutionPolicy RemoteSigned -Force
5
6
7  ### Sets the absolute path for the log file##
8  $Logfile = 'C:\FileCloudSync_SilentInstaller.log'
9
10
11 ##Validates if the log file already exists if so it deletes it and creates a
12 new log file##
13 if (Test-Path -Path "C:\FileCloudSync_SilentInstaller.log") {
14     Remove-Item 'C:\FileCloudSync_SilentInstaller.log' -Recurse
15     New-Item -Path "c:\" -Name "FileCloudSync_SilentInstaller.log" -ItemType
"file"
16     "#####Created log file and started loggin#####" | Out-File
$Logfile -Append

```

```

16     "Set-Execution Policy Successful" | Out-File $Logfile -Append
17 }
18 else {
19     New-Item -Path "c:\" -Name "FileCloudSync_SilentInstaller.log" -ItemType
20     "file"
21     "#####Created log file and started loggin#####" | Out-File
22     $Logfile -Append
23     "Set-Execution Policy Successful" | Out-File $Logfile -Append
24 }
25 ##Check if FileCloud Sync is already installed if its installed cancel the
26 installation else continue##
27 if (Test-Path -Path "C:\Users\
28 $env:USERNAME\AppData\Roaming\FileCloudSyncData\client") {
29     "FileCloud Sync is already installed, Unable to proceed with the
30 installation" | Out-File $Logfile -Append
31     clear
32     Write-Warning "FileCloud Sync is already installed, Please uninstall
33 FileCloud Sync in order to proceed"
34     $Input = Read-Host -Prompt "Press any key to Exit"
35     Exit
36 }
37 Else {
38     ##Create the directory where FileCloud Sync will be downloaded##
39     Try {
40         if (Test-Path -Path "C:\FileCloudSync") {
41             Remove-Item 'C:\FileCloudSync' -Recurse
42             "Folder already exists, Deleted Folder under C:\FileCloudSync " |
43 Out-File $Logfile -Append
44             New-Item -Path "c:\" -Name "FileCloudSync" -ItemType "directory"
45 -ErrorAction Stop
46             "Created folder under C:\FileCloudSync " | Out-File $Logfile
47 -Append
48         }
49         else {
50             New-Item -Path "c:\" -Name "FileCloudSync" -ItemType "directory"
51 -ErrorAction Stop
52         }
53     }
54     Catch {
55         $message = $_
56         "ERROR $_ " | Out-File $Logfile -Append
57     }
58     ##Downloads the FileCloud Sync Installer into the directory created##

```

```

58     Try {
59         "Downloading FileCloud Sync.msi installer" | Out-File $Logfile
-Append
60         $url1 = "https://patch.codelathe.com/tonido/live/installer/x86-win32/
FileCloudSync2.msi"
61         $output1 = "C:\FileCloudSync\FileCloudSync2.msi"
62         $start_time = Get-Date
63         Import-Module BitsTransfer
64         Start-BitsTransfer -Source $url1 -Destination $output1
65     }
66     Catch {
67         $message = $_
68         "ERROR $_ " | Out-File $Logfile -Append
69     }
70
71
72
73     ##Validates if FileCloud has downloaded completely based on the file
hash##
74
75     $hashSrc =
"9B0F053DF45605E1CA819396D66B046310FE386BCF1B00A3F1B3B685B6FF29CA"
76     $fileToCheck = "C:\FileCloudSync\FileCloudSync2.msi"
77     $hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"
78
79     Try {
80         if ($hashSrc.Hash -ne $hashDest.Hash) {
81             "FileCloud Sync Installer downloaded successfully" | Out-File
$Logfile -Append
82         }
83         else {
84             "FileCloud Sync Installer was NOT downloaded or it has not been
download completely" | Out-File $Logfile -Append
85             Exit
86         }
87     }
88     Catch {
89         $message = $_
90         "ERROR $_ " | Out-File $Logfile -Append
91     }
92
93
94
95
96     ##Installs FileCloud Sync silently without needing any end-user
interaction##
97     Try {
98         Start-Process -Wait -FilePath "C:\FileCloudSync\FileCloudSync2.msi"
-ArgumentList '/quiet', '/passive', '/n' -passthru -ErrorAction Stop
99         "FileCloud Installation Started" | Out-File $Logfile -Append
100    }
101    Catch {

```

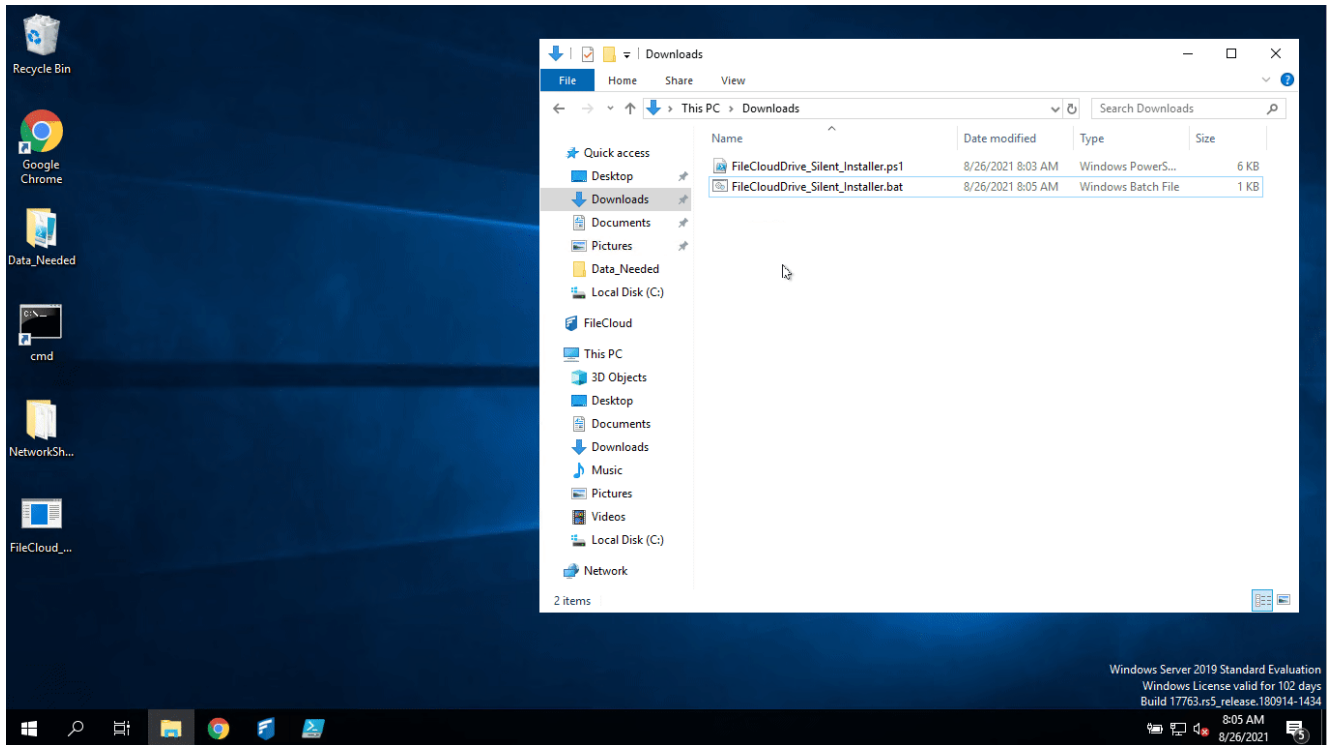
```

102     $message = $_
103     "ERROR $_ " | Out-File $Logfile -Append
104 }
105
106
107
108
109 ##Adds the needed registry keys to configure Mass Deployment##
110 cd HKLM:\
111
112 Try {
113     set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
114 }
115 Catch {
116     $message = $_
117     "ERROR $_ " | Out-File $Logfile -Append
118 }
119
120
121
122 # Create the path within the registry
123 Try {
124     Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name 'CodeLathe\FileCloud\DefaultCfg\' -Force -ErrorAction Stop
125     "Creating registry entry" | Out-File $Logfile -Append
126 }
127 Catch {
128     $message = $_
129     "ERROR $_ " | Out-File $Logfile -Append
130 }
131
132 # Create the needed keys to assign the predefined settings
133 Try {
134     New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'url' -Value "https://your-filecloud-url.com" -PropertyType String -Force
135     New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'allowcentralmgmt' -Value "1" -PropertyType String -Force
136     "Creating predefined parameters" | Out-File $Logfile -Append
137 }
138 Catch {
139     $message = $_
140     "ERROR $_ " | Out-File $Logfile -Append
141 }
142
143
144 # Exits the registry
145 Pop-Location
146
147 #Start FileCloud Sync#
148 Try {

```

```
149         Start-Process -FilePath "C:\Program Files\FileCloud
Sync\cloudsync.exe"
150         "Starting FileCloud Sync" | Out-File $Logfile -Append
151     }
152     Catch {
153         $message = $_
154         "ERROR $_ " | Out-File $Logfile -Append
155     }
156
157     ##CleanUp- Deletes the folder created and the installer within#
158     Try {
159         Remove-Item 'C:\FileCloudSync' -Recurse
160         "Deleting FileCloudSync download folder under C:\FileCloudSync " |
161     Out-File $Logfile -Append
162     }
163     Catch {
164         $message = $_
165         "ERROR $_ " | Out-File $Logfile -Append
166     }
167
168     ##Installation Completed - Closes PowerShell##
169     "Installation Completed" | Out-File $Logfile -Append
170
171     stop-process -Id $PID
172     exit
173 }
```

FileCloud Drive Installation & Mass Deployment automation - Video



FileCloud Drive Installation & Mass Deployment automation - Script

FileCloud Drive Installation & Mass Deployment automation

```

1  ####Silent FileCloud Drive Installation & Mass Deployment Configuration####
2
3  ##Allows the script to be executed without user consent##
4  set-ExecutionPolicy RemoteSigned -Force
5
6
7  ### Sets the absolute path for the log file##
8  $Logfile = 'C:\FileCloudDrive_SilentInstaller.log'
9
10
11 ##Validates if the log file already exists if so it deletes it and creates a
12 new log file##
13 if (Test-Path -Path "C:\FileCloudDrive_SilentInstaller.log") {
14     Remove-Item 'C:\FileCloudDrive_SilentInstaller.log' -Recurse
15     New-Item -Path "c:\" -Name "FileCloudDrive_SilentInstaller.log" -ItemType
16     "file"

```

```

15     "#####Created log file and started login#####" | Out-File
$Logfile -Append
16     "Set-Execution Policy Successful" | Out-File $Logfile -Append
17 }
18 else {
19     New-Item -Path "c:\" -Name "FileCloudDrive_SilentInstaller.log" -ItemType
"file"
20     "#####Created log file and started login#####" | Out-File
$Logfile -Append
21     "Set-Execution Policy Successful" | Out-File $Logfile -Append
22 }
23
24
25 ##Check if FileCloud Drive is already installed if its installed cancel the
installation else continue##
26 if (Test-Path -Path "C:\Users\
$env:USERNAME\AppData\Roaming\FileCloudDriveData\client") {
27     "FileCloud Drive is already installed, Unable to proceed with the
installation" | Out-File $Logfile -Append
28     clear
29     Write-Warning "FileCloud Drive is already installed, Please uninstall
FileCloud Drive in order to proceed"
30     $Input = Read-Host -Prompt "Press any key to Exit"
31     Exit
32 }
33 Else {
34
35
36
37
38     ##Create the directory where FileCloud Drive will be downloaded##
39     Try {
40         if (Test-Path -Path "C:\FileCloudDrive") {
41             Remove-Item 'C:\FileCloudDrive' -Recurse
42             "Folder already exists, Deleted Folder under C:\FileCloudDrive "
| Out-File $Logfile -Append
43             New-Item -Path "c:\" -Name "FileCloudDrive" -ItemType "directory"
-ErrorAction Stop
44             "Created folder under C:\FileCloudDrive " | Out-File $Logfile
-Append
45         }
46         else {
47             New-Item -Path "c:\" -Name "FileCloudDrive" -ItemType "directory"
-ErrorAction Stop
48         }
49     }
50 }
51 Catch {
52     $message = $_
53     "ERROR $_ " | Out-File $Logfile -Append
54 }
55

```

```

56
57     ##Downloads the FileCloud Drive Installer into the directory created###
58     Try {
59         "Downloading FileCloud Drive.msi installer" | Out-File $Logfile
60     -Append
61         $url1 = "https://patch.codelathe.com/tonido/live/installer/x86-win32/
FileCloudDrive2eSetup.msi"
62         $output1 = "C:\FileCloudDrive\FileCloudDrive2eSetup.msi"
63         $start_time = Get-Date
64         Import-Module BitsTransfer
65         Start-BitsTransfer -Source $url1 -Destination $output1
66     }
67     Catch {
68         $message = $_
69         "ERROR $_ " | Out-File $Logfile -Append
70     }
71
72
73     ##Validates if FileCloud has downloaded completely based on the file
hash##
74
75     $hashSrc =
76     "1FCD2F88DD7615E68A2AD935AECCE4D04DD61ED769E52008002B1F7CA3CB7A17"
77     $fileToCheck = "C:\FileCloudDrive\FileCloudDrive2eSetup.msi"
78     $hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"
79
80     Try {
81         if ($hashSrc.Hash -ne $hashDest.Hash) {
82             "FileCloud Drive Installer downloaded successfully" | Out-File
$Logfile -Append
83         }
84         else {
85             "FileCloud Drive Installer was NOT downloaded or it has not been
download completely" | Out-File $Logfile -Append
86             Exit
87         }
88     }
89     Catch {
90         $message = $_
91         "ERROR $_ " | Out-File $Logfile -Append
92     }
93
94
95
96     ##Installs FileCloud Drive silently without needing any end-user
interaction##
97     Try {
98         Start-Process -Wait -FilePath "C:
\FileCloudDrive\FileCloudDrive2eSetup.msi" -ArgumentList '/quiet', '/passive',
'/n' -passthru -ErrorAction Stop

```



```

99         "FileCloud Installation Started" | Out-File $Logfile -Append
100     }
101     Catch {
102         $message = $_
103         "ERROR $_ " | Out-File $Logfile -Append
104     }
105
106
107
108
109     ##Adds the needed registry keys to configure Mass Deployment##
110     cd HKLM:\
111
112     Try {
113         set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
114     }
115     Catch {
116         $message = $_
117         "ERROR $_ " | Out-File $Logfile -Append
118     }
119
120
121
122     # Create the path within the registry
123     Try {
124         Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name 'CodeLathe\FileCloud\DefaultCfg\' -Force -ErrorAction Stop
125         "Creating registry entry" | Out-File $Logfile -Append
126     }
127     Catch {
128         $message = $_
129         "ERROR $_ " | Out-File $Logfile -Append
130     }
131
132     # Create the needed keys to assign the predefined settings
133     Try {
134         New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'url' -Value "https://your-filecloud-url.com" -PropertyType String -Force
135         New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'allowcentralmgmt' -Value "1" -PropertyType String -Force
136         "Creating predefined parameters" | Out-File $Logfile -Append
137     }
138     Catch {
139         $message = $_
140         "ERROR $_ " | Out-File $Logfile -Append
141     }
142
143
144     # Exits the registry
145     Pop-Location

```

```

146
147     #Start FileCloud Drive#
148     Try {
149         Start-Process -FilePath "C:\Program Files\FileCloud
Drive\clouddrive.exe"
150         "Starting FileCloud Drive" | Out-File $Logfile -Append
151     }
152     Catch {
153         $message = $_
154         "ERROR $_ " | Out-File $Logfile -Append
155     }
156
157     ##CleanUp- Deletes the folder created and the installer within#
158     Try {
159         Remove-Item 'C:\FileCloudDrive' -Recurse
160         "Deleting FileCloudDrive download folder under C:\FileCloudDrive " |
161         Out-File $Logfile -Append
162     }
163     Catch {
164         $message = $_
165         "ERROR $_ " | Out-File $Logfile -Append
166     }
167
168     ##Installation Completed - Closes PowerShell##
169     "Installation Completed" | Out-File $Logfile -Append
170
171     stop-process -Id $PID
172     exit
173 }

```

FileCloud Outlook Addin Installation & Mass Deployment automation - Script

FileCloud Outlook Addin

```

1     #####Silent FileCloud Outlook_Plugin Installation & Mass Deployment
Configuration####
2
3     ##Allows the script to be executed without user consent##
4     set-ExecutionPolicy RemoteSigned -Force
5
6
7     ### Sets the absolute path for the log file##
8     $Logfile = 'C:\FileCloudOutlookplugin_SilentInstaller.log'
9
10
11    ##Validates if the log file already exists if so it deletes it and creates a
new log file##
12    if (Test-Path -Path "C:\FileCloudOutLook_Plugin_SilentInstaller.log") {

```

```

13     Remove-Item 'C:\FileCloudOutLook_Plugin_SilentInstaller.log' -Recurse
14     New-Item -Path "c:\" -Name "FileCloudOutLook_Plugin_SilentInstaller.log"
-ItemType "file"
15     "#####Created log file and started login#####" | Out-File
$Logfile -Append
16     "Set-Execution Policy Successful" | Out-File $Logfile -Append
17 }
18 else {
19     New-Item -Path "c:\" -Name "FileCloudOutLook_Plugin_SilentInstaller.log"
-ItemType "file"
20     "#####Created log file and started login#####" | Out-File
$Logfile -Append
21     "Set-Execution Policy Successful" | Out-File $Logfile -Append
22 }
23
24
25 ##Check if FileCloud Outlook_Plugin is already installed if its installed
cancel the installation else continue##
26 if (Test-Path -Path "C:\Users\
$env:USERNAME\AppData\Roaming\FileCloudOutlookAddIn") {
27     "FileCloud Outlook_Addin is already installed, Unable to proceed with the
installation" | Out-File $Logfile -Append
28     clear
29     Write-Warning "FileCloud Outlook_Plugin is already installed, Please
uninstall FileCloud Outlook_Plugin in order to proceed"
30     $Input = Read-Host -Prompt "Press any key to Exit"
31     Exit
32 }
33 Else {
34
35
36
37
38     ##Create the directory where FileCloud Outlook_Plugin will be
downloaded##
39     Try {
40         if (Test-Path -Path "C:\FileCloudOutLook_Plugin") {
41             Remove-Item 'C:\FileCloudOutLook_Plugin' -Recurse
42             "Folder already exists, Deleted Folder under C:
\FileCloudOutLook_Plugin " | Out-File $Logfile -Append
43             New-Item -Path "c:\" -Name "FileCloudOutLook_Plugin" -ItemType "d
irectory" -ErrorAction Stop
44             "Created folder under C:\FileCloudOutLook_Plugin " | Out-File
$Logfile -Append
45         }
46         else {
47             New-Item -Path "c:\" -Name "FileCloudOutLook_Plugin" -ItemType "d
irectory" -ErrorAction Stop
48         }
49     }
50 }
51 Catch {

```

```

52     $message = $_
53     "ERROR $_ " | Out-File $Logfile -Append
54 }
55
56
57     ##Downloads the FileCloud Outlook_Plugin Installer into the directory
created###
58     Try {
59         "Downloading FileCloud Outlook_Addin.exe installer" | Out-File
$Logfile -Append
60         $url1 = "https://patch.codelathe.com/tonidocloud/live/installer/
FileCloudOutlookAddIn.exe"
61         $output1 = "C:\FileCloudOutlook_Plugin\FileCloudOutlookAddin.exe"
62         $start_time = Get-Date
63         Import-Module BitsTransfer
64         Start-BitsTransfer -Source $url1 -Destination $output1
65     }
66     Catch {
67         $message = $_
68         "ERROR $_ " | Out-File $Logfile -Append
69     }
70
71
72
73     ##Validates if FileCloud has downloaded completely based on the file
hash##
74
75     $hashSrc =
"0789F44D02453BEF3A7E9B53325CD90584BF37C5FC0F8F09611A5B7D417F505"
76     $fileToCheck = "C:\FileCloudOutlook_Plugin\FileCloudOutlookAddin.exe"
77     $hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"
78
79     Try {
80         if ($hashSrc.Hash -ne $hashDest.Hash) {
81             "FileCloud Outlook_Plugin Installer downloaded successfully" |
Out-File $Logfile -Append
82         }
83         else {
84             "FileCloud Outlook_Plugin Installer was NOT downloaded or it has
not been download completely" | Out-File $Logfile -Append
85             Exit
86         }
87     }
88     Catch {
89         $message = $_
90         "ERROR $_ " | Out-File $Logfile -Append
91     }
92
93
94
95
96     ##check if outlook is running if so kills it before proceeding.

```

```

97
98     Try {
99         $app = 'OUTLOOK'
100
101         $process = Get-Process $app -ErrorAction SilentlyContinue
102         if ($process) {
103             Stop-Process $process -Force
104             Write-Output "$app has been stopped."
105         }
106         else {
107             Write-Output "$app is not running."
108         }
109     }
110     Catch {
111         $message = $_
112         "ERROR $_ " | Out-File $Logfile -Append
113     }
114
115
116
117
118     ##Installs FileCloud Outlook_Plugin silently without needing any end-user
119     interaction##
120     Try {
121         Start-Process -Wait -FilePath "C:
122         \FileCloudOutlook_Plugin\FileCloudOutlookAddIn.exe" -ArgumentList '/
123         VERYSILENT', '/SUPPRESSMSGBOXES' -passthru -ErrorAction Stop
124         "FileCloud Installation Started" | Out-File $Logfile -Append
125     }
126     Catch {
127         $message = $_
128         "ERROR $_ " | Out-File $Logfile -Append
129     }
130
131     ##Adds the needed registry keys to configure Mass Deployment##
132     cd HKLM:\
133
134     Try {
135         set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
136     }
137     Catch {
138         $message = $_
139         "ERROR $_ " | Out-File $Logfile -Append
140     }
141
142     # Create the path within the registry
143     Try {
144         Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name 'CodeLathe\FileClou
145         d\DefaultCfg\' -Force -ErrorAction Stop
146         "Creating registry entry" | Out-File $Logfile -Append

```

```

145     }
146     Catch {
147         $message = $_
148         "ERROR $_ " | Out-File $Logfile -Append
149     }
150
151     # Create the needed keys to assign the predefined settings
152     Try {
153         New-ItemProperty -Path 'HKLM:
\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'url' -Value "https://your-
filecloud-url.com" -PropertyType String -Force
154         New-ItemProperty -Path 'HKLM:
\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name 'allowcentralmgmt' -Value "1"
-PropertyType String -Force
155         "Creating predefined parameters" | Out-File $Logfile -Append
156     }
157     Catch {
158         $message = $_
159         "ERROR $_ " | Out-File $Logfile -Append
160     }
161
162
163     # Exits the registry
164     Pop-Location
165
166     ##CleanUp- Deletes the folder created and the installer within#
167     Try {
168         Remove-Item 'C:\FileCloudOutLook_Plugin' -Recurse
169         "Deleting FileCloudOutLook_Plugin download folder under C:
\FileCloudOutLook_Plugin " | Out-File $Logfile -Append
170     }
171     Catch {
172         $message = $_
173         "ERROR $_ " | Out-File $Logfile -Append
174     }
175
176     ##Installation Completed - Closes PowerShell##
177     "Installation Completed" | Out-File $Logfile -Append
178
179     stop-process -Id $PID
180     exit
181 }

```

Creating a .bat file to execute the script

Once created your PowerShell script based on the example above you can automate its execution by creating a .bat file, for details view the example below.

1. Using a notepad or a text editor create a new file with the following content

```
echo on FileCloud Silent Installer and Mass Deployment Configuration
cd C:\Users\%username%\Downloads
Powershell.exe -File "FileCloudSync_Silent_Installer.ps1"
```

2. Once done save the file as a .bat
3. Before executing it you will need to have both, the .bat file and the .ps1 file on the same location as per this example it should be under Downloads.
4. Right-click run as administrator.

Converting the PowerShell script to an executable

Once created your PowerShell script based on the example above you can automate its execution by creating an executable file, for details view the example below.

1. Run PowerShell as an administrator and run the following to install and import the ps2exe module

```
Install-Module ps2exe
```

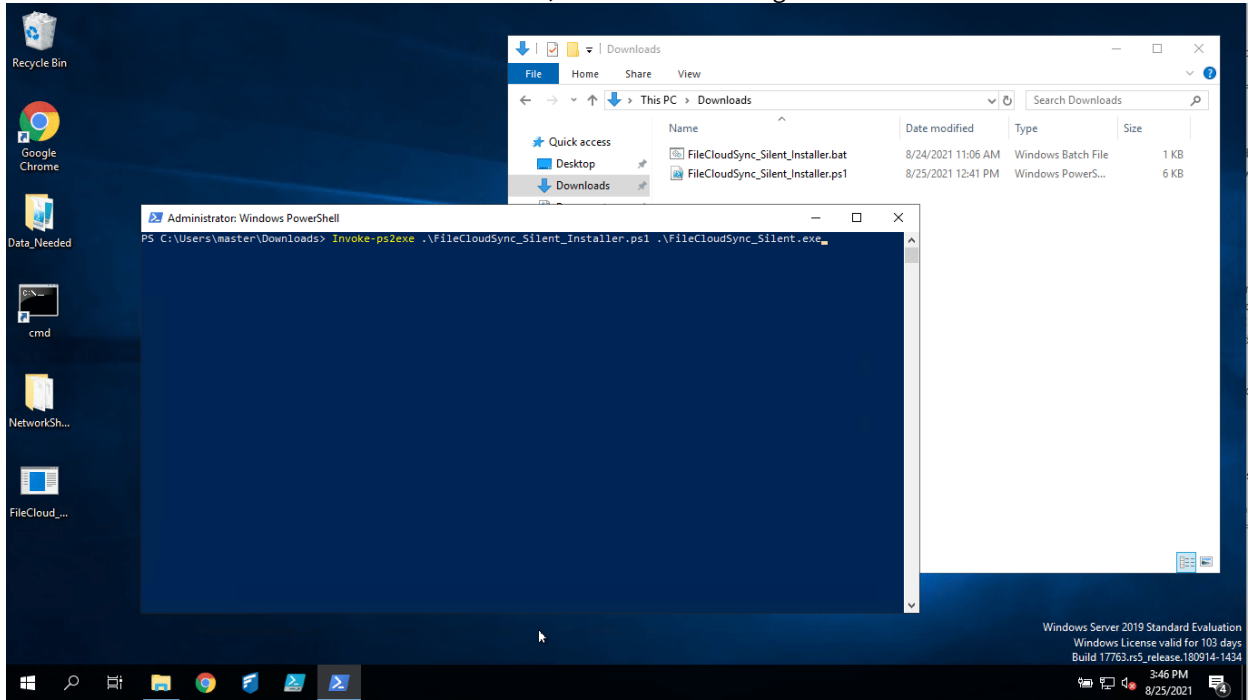
2. Once the above is completed enter "Y" to install the Module

```
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change
its InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to
install the modules from 'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
```

3. Once the module has been installed you can convert the .ps1 to .exe by running the following command

```
Invoke-ps2exe .\NAME-OF-YOUR-SCRIPT.ps1 .
\FileCloud_Silent_Installer_and_Mass_Deployment.exe
```

4. Your end result should be a executable for details, review the following:

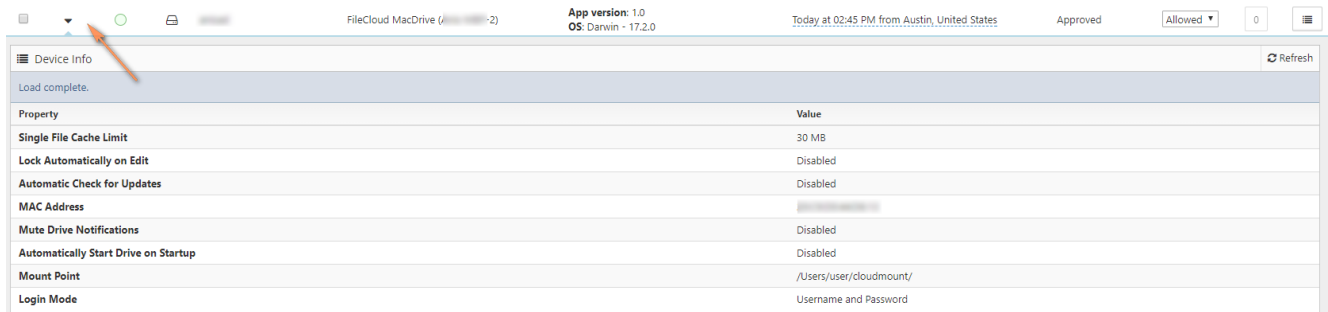


Viewing Client Information

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
Username, Device name/details				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 05:23 AM on Dec 12, 2017 from Austin, United States	Approved	Allowed	1	
				FileCloud MacDrive (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 no 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

- 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

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

The screenshot shows the 'Manage Devices' interface in the FileCloud Administration Panel. A table lists various devices, including Cloud Sync (MIO-PC), FileCloud Drive (DELL), Cloud Sync (MAINPC), Cloud Sync (Mac.local), FileCloud MacDrive (Mac.local), Android-samsung-SM-G930F, and iPhone 7 plus. A modal dialog box is overlaid on the table, asking for a short message (80 characters) with an input field and 'OK' and 'Cancel' buttons.

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 in the FileCloud Server Admin Portal. The navigation tabs at the top are: Server, Storage, Authentication, Admin, Email, **Endpoint Backup**, License, Policies, SSO, and Team Folders. The settings are as follows:

- Allow Users To Backup**: Click to enable user to backup files using CloudSync client application.
- Allow Camera Uploads**: Allow automatic backup of photos and videos of mobile devices. (An orange arrow points to this checkbox.)
- Backup Path**: 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**: Set a valid email address to receive the back up notifications

Mass Deployment - Default Configuration Support

i The ability to provide defaults for the FileCloud Client Apps like Sync, Drive and Office Add-ins is available in FileCloud Server version 15.0 and later.

The ability to provide defaults for bandwidth limits and **time active controls** in FileCloud Sync is available in FileCloud Server version 18.2 and later.

As an administrator you can roll out a mass deployment of settings for all the client apps across the enterprise.

⚠ Notes:

- Mass deployment requires that default configurations be added to the Windows registry.
- These defaults are used by the apps when initially starting up and don't have any effect if they are changed after the apps are initialized.
- Please ensure before adding a value that it is not already present in the "syncclientconfig.xml" before testing. Otherwise, the mass deployment configuration values will not be used.

The following table lists the supported default configuration parameters.

Table 1. Supported Parameters

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
url	String	The server URL. example: https://files.xyz.com	YES	YES	YES	YES	YES
profile	String	User name to use to login. example: john or john@company.com You can use the current OS user as the username by specifying \${USER}	YES	YES	YES	YES	YES
checkupdates	String	'0' to disable, '1' to enable	YES	YES	YES	NO	NO
httpproxyenabled	String	'0' to disable, '1' to enable	NO	YES	YES	NO	NO
httpproxyhost	String	Proxy Hostname to use for connection	YES	YES	YES	YES	YES
httpproxyport	String	Proxy Port to use for connection	YES	YES	YES	YES	YES
httpproxyuser	String	Proxy User Authentication name to use	YES	YES	YES	YES	YES

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
httpproxypassword	String	Proxy User Authentication password to use	YES	YES	YES	YES	YES
ssllevel	String	Special directive to allow apps to connect to TLS-only servers. Possible usages are CLIENT_USE, TLSV1_1_CLIENT_USE, TLSV1_2_CLIENT_USE, TLSV1_3_CLIENT_USE	YES	YES	YES	NO	NO
officehelperdisabled	String	FileCloud for Office (FFO)/DocIQ Office Integration	YES	NO	NO	NO	NO
officehelperlocked	String	Automatic locking in FileCloud for Office (FFO)/DocIQ	YES	NO	NO	NO	NO
syncfolderlocation	String	Path to use for the sync folder location. DEFAULT - use the default location Absolute Full Paths - e.g. c:\filecloudsync Expanded Paths - e.g. %APPDATA%\FileCloudSync (Windows Only) or \${HOME}\FileCloudSync (Windows and Mac OSX)	YES	NO	NO	NO	NO
syncclientlocation	String	Path to use for the sync folder data and cache location. DEFAULT - use the default location Absolute Full Paths - e.g. c:\filecloudsyncdata Expanded Paths - e.g. %APPDATA%\FileCloudSyncData (Windows Only) or \${HOME}\FileCloudSyncData (Windows and Mac OSX)	YES	PasNO	NO	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
removeunshared	String	Directive to require sync to delete shared folders from local device if they are no longer shared for syncing "0" - Default, does not remove unshared folders "1" - Removes shared folders from local when they are no longer shared from the server	YES	NO	NO	NO	NO
authmode	String	Directive to use password authentication, SSO, or device code authentication for log in to Sync. "password" - Password authentication "sso" - SSO authentication "devauth" - Device code authentication	YES	NO	NO	NO	NO
drivecachelocation	String	Path to use for drive cache DEFAULT - use the default location Absolute Full Paths - e.g. c:\fileclouddrive Expanded Paths - e.g. %APPDATA%\FileCloud Drive\data (Windows Only) or \${HOME}\FileCloud Drive (Windows and Mac OSX)	NO	YES	NO	NO	NO
enableshortcachepath	String	Whether to use a short path made up of random digits or to use "DOMAIN@USERNAME" for the folder in the cache. Use this option to avoid exceeding the maximum path length. "0" - Default, use DOMAIN@USERNAME "1" - Use short path made up of random digits	NO	YES	YES	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
drivedefaultstorageingb	String	The value in GB of the default user quota setting	NO	YES	YES	NO	NO
drivemountpoint	String	Mount point to override Can be empty or it must be a drive letter with ":" like "F:"	NO	YES	NO	NO	NO
sslverify	String	Directive to disable strict checking of SSL certificates. If this key is not provided, the default is strict verification VERIFY_NONE: disable SSL Verification checking VERIFY_STRICT: enables strict SSL Verification checking	YES	YES	YES	YES	YES
driveloginmode	String	Directive to use password authentication or device code authentication "0" - Password authentication "1" - Device Code authentication "2" - SSO authentication	NO	YES	YES	NO	NO
drivelockonupdate	String	Directive to lock file when opened for modification "0" - No lock while editing "1" - Auto Lock while editing	NO	YES	YES	NO	NO
drivemutemessages	String	Show or hide automatic information messages from drive "0" - Do not mute messages "1" - Mute messages	NO	YES	YES	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
officehelperdisabled	String	Whether to disable FileCloud for Office (FFO)/DocIQ "0" - Do not disable FileCloud for Office (FFO)/DocIQ "1" - Disable FileCloud for Office (FFO)/DocIQ	NO	YES	YES	NO	NO
showdashboardonstartup	String	Whether to show the dashboard on startup "0" - Do not display dashboard on startup "1" (default) Display dashboard on startup	NO	YES	YES	NO	NO
driveopenexploreronstartup	String	Automatically launch explorer on startup of drive "0" - Do not start explorer on startup "1" - Launch explorer on startup	NO	YES	YES	NO	NO
useuniquemountlabel	String	When enabled, sets mount label to a unique value (by adding the user name to the label). "0" - (default) Do not set mount label to unique value. "1" - Set mount label to unique value (add user name to the label)	NO	YES	NO	NO	NO
allowthumbsdbupload	String	Whether to upload of thumbs.db files. "0" - (default) Do not upload of thumbs.db files. "1" = Upload thumbs.db files	NO	YES	NO	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
disableautologin	String	Whether to prevent Drive from remembering the password and automatically logging in. "0" - (default) Allow auto-login "1" - disable auto-login	NO	YES	YES	NO	NO
multimount	String	Allow multiple FileCloud Drive sessions to run on the same computer (and allow mounting of different cloud locations simultaneously. Note: When this is enabled, log-in information is not saved, and must be re-entered each time Drive is started. "0" - (default) Do not allow multiple instances to run "1" - Allow multiple instances to run.	NO	YES	NO	NO	NO
currentlanguage	String	The default language of FileCloud Drive. The value is English by default. Supported values are English, Dutch, French, Spanish, Portuguese, German, Italian, Arabic, and Russian.	NO	YES	YES	NO	NO
language	String	The default language of FileCloud Sync. The value is English by default. Supported values are English, Dutch, French, Spanish, Portuguese, German, Italian, Arabic, and Russian.	YES	NO	NO	NO	NO
cachevalidationseconds	String	Interval in seconds between checks for changes in values stored in cache. Default, recommended value is 60.	NO	YES	YES	NO	NO
autolocktypes	String	Lists file types that are exempt from download limits. Default types are: txt,rtf,doc,docx,xls,xlsx,ppt,pptx,indd	NO	YES	YES	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
disablerecovering	String	<p>By default, files are copied to the recovered folder before they are uploaded to Drive and deleted after upload succeeds. You may change the setting to copy the files to the recovered folder only after upload to Drive is attempted and fails.</p> <p>"0" - (default) Files are copied to recovered folder before upload occurs.</p> <p>"1" - Files are copied to recovered folder after upload is attempted if upload fails.</p>	NO	YES	YES	NO	NO
disableprecaching	String	<p>By default, when Drive starts up, the file/folder directory is retrieved from the server so that it is immediately available to Drive users. You may change the setting so that the file/folder directory is retrieved when the user begins navigating the folders to reduce the load on the server after startup; in this case, initially navigating the folders may be slower.</p> <p>"0" - (default) File/folder directory is retrieved when Drive starts up.</p> <p>"1" - File/folder directory is retrieved when a user starts navigating the folders.</p>	NO	YES	YES	NO	NO
lockexpirationinmin	String	<p>Value, in minutes, that a lock on a file is maintained before it expires. Default and minimum is 10; if value is set below 10, expiration time still occurs in 10 minutes.</p>	NO	YES	YES	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
disablelockexpiration	String	<p>Whether or not to enable expiring of locks. By default, locks on files expire after 10 minutes or the time set in lockexpirationinmin.</p> <p>"0" - (default) Use expiration times set for file locks.</p> <p>"1" - Do not use expiration times on locks. Locks expire on files when users close them.</p>	NO	YES	YES	NO	NO
enablethumbnailpreview	String	<p>Whether or not to display thumbnails and previews of listed files.</p> <p>"0" - (default) Do not display thumbnails and previews (this reduces network traffic since files are downloaded when thumbnails and previews are generated)</p> <p>"1" - Display thumbnails and previews.</p>	NO	NO	YES	NO	NO
maxdownloadsizeinmb	String	<p>Default single file download limit in MB.</p> <p>0 - No limit</p> <p>Other options can be 10,30,50, 100</p>	NO	YES	YES	NO	NO
allowcentralmgmt	String	<p>Allow central management</p> <p>0 - No Central Management</p> <p>1- Allow Central Management</p>	YES	NO	NO	NO	NO
globalbwforupload	String	<p>Specifies the bandwidth limit when uploading files from the client to the server in terms of KB only.</p>	YES	NO	NO	NO	NO
globalbwfordownload	String	<p>Specifies the bandwidth limit when downloading files from the server to the client in terms of KB only.</p>	YES	NO	NO	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
albtwforupload	String	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.	YES	NO	NO	NO	NO
albtwfordownload	String	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.	YES	NO	NO	NO	NO
albtwfromtime	String	Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit.	YES	NO	NO	NO	NO
albtwtotime	String	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	YES	NO	NO	NO	NO
albtwschedule_dayofweek	String	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.. 	YES	NO	NO	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
timeactivecontrolsset	Enables/Disables the Active Sync Hours settings 1 = enabled 0 = disabled	<timeactivecontrolsset>1</timeactivecontrolsset>	YES	NO	NO	NO	NO
activesync_daysofweek	Specifies the days of the week when a client can run the Sync app Any number {-1, 0, 1, 2, 3, 4, 5, 6} where: <ul style="list-style-type: none"> • -1 = Every day • 0 = Sunday • 1 = Monday • and so on... 	<activesync_daysofweek>5</activesync_daysofweek>	YES	NO	NO	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
activesync_timeofday	Specifies the times during the days of the week when a client can run the Sync app Use the format HH:MM:SS- HH:MM:SS	<activesync_timeofday>8:00:00-20:00:00</activesync_timeofday>	YES	NO	NO	NO	NO


FAQs

In Windows, where is the default configuration located?

The location of the default configuration is in the Windows Registry.

An example configuration is shown below.

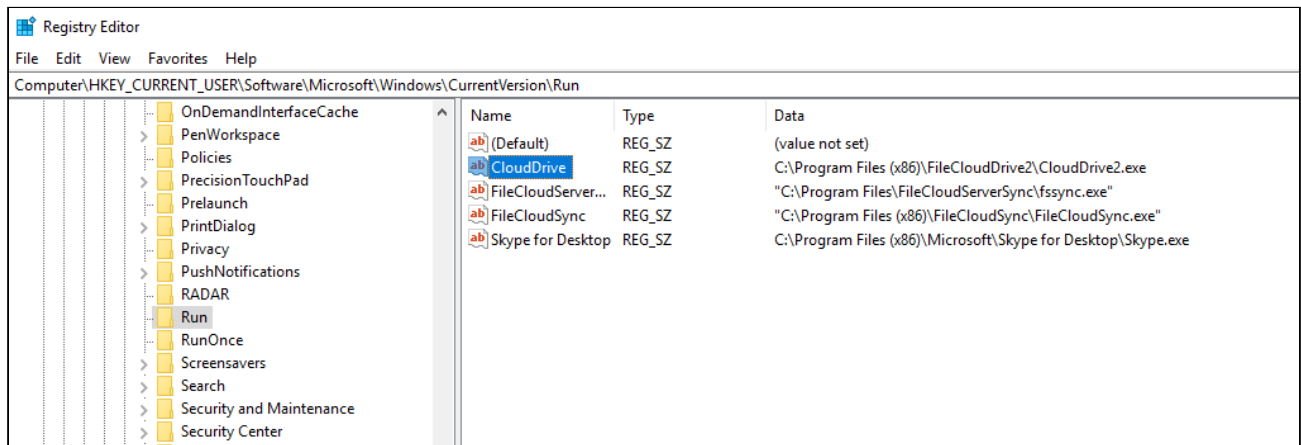
Note: The registry key (**HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg**) must be created manually, including the default values.

 HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg

Name	Type	Data
(Default)	REG_SZ	(value not set)
url	REG_SZ	https://files.company.com
profile	REG_SZ	{USER}
checkupdates	REG_SZ	1
syncfolderlocation	REG_SZ	C:\FileCloudData
ssllevel	REG_SZ	TLSV1_2_CLIENT_USE
syncclientlocation	REG_SZ	DEFAULT
httpproxyhost	REG_SZ	
httpproxypassword	REG_SZ	
httpproxyport	REG_SZ	
httpproxyuser	REG_SZ	

How to setup Run on Windows Startup for MSI installation for Drive?

 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



In Mac OSX, where is the default configuration located?

The location of the default configuration is a plist file in
~/Library/Preferences/com.codelathe.filecloud.defaultcfg.plist


Example plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>url</key>
  <string>https://mysite.company.com</string>
  <key>profile</key>
  <string>jsmith</string>
  <key>maxdownloadsizeinmb</key>
  <string>0</string>
  <key>drivelockonupdate</key>
  <string>1</string>
  <key>drivemutemessages</key>
  <string>1</string>
  <key>driveopenexploreronstartup</key>
  <string>1</string>
  <key>driveloginmode</key>
  <string>1</string>
  <key>checkupdates</key>
  <string>0</string>
</dict>
</plist>
```


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.

Note: For full content search or PII search, configure [content search for documents](#).

Basic Search

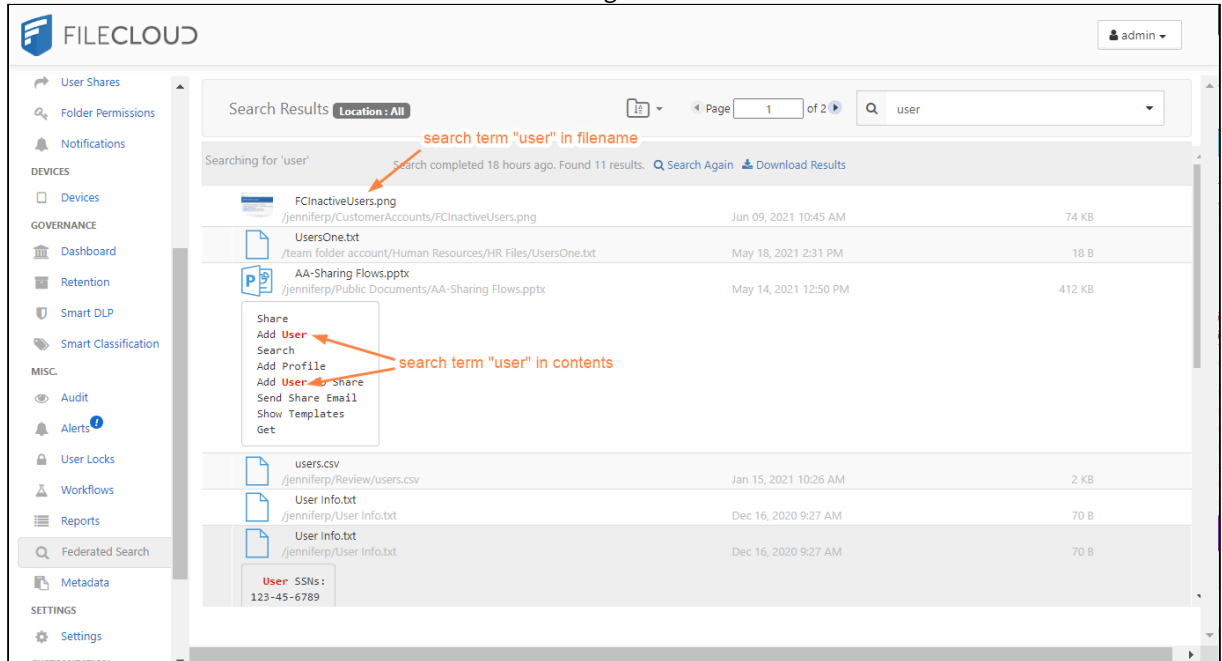
A basic search searches for the search term in file and folder names, and if content search is enabled, in the content of files.

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

To perform a basic search on the entire site:

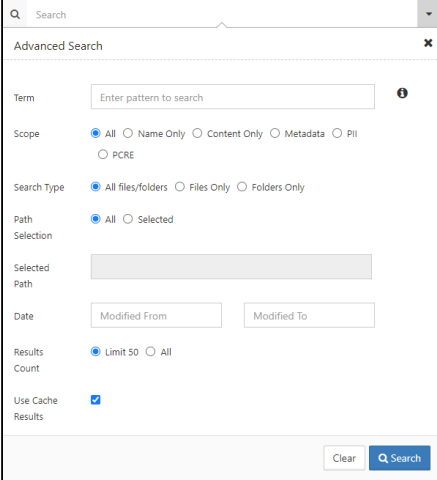
1. From the left navigation panel of the Admin Portal, under **Misc.**, click **Federated Search**.
2. On the search screen, in the search box, type the search term and press enter.
Files and folders with the search term in their names as well as files containing text that contains the search

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



Advanced Searches

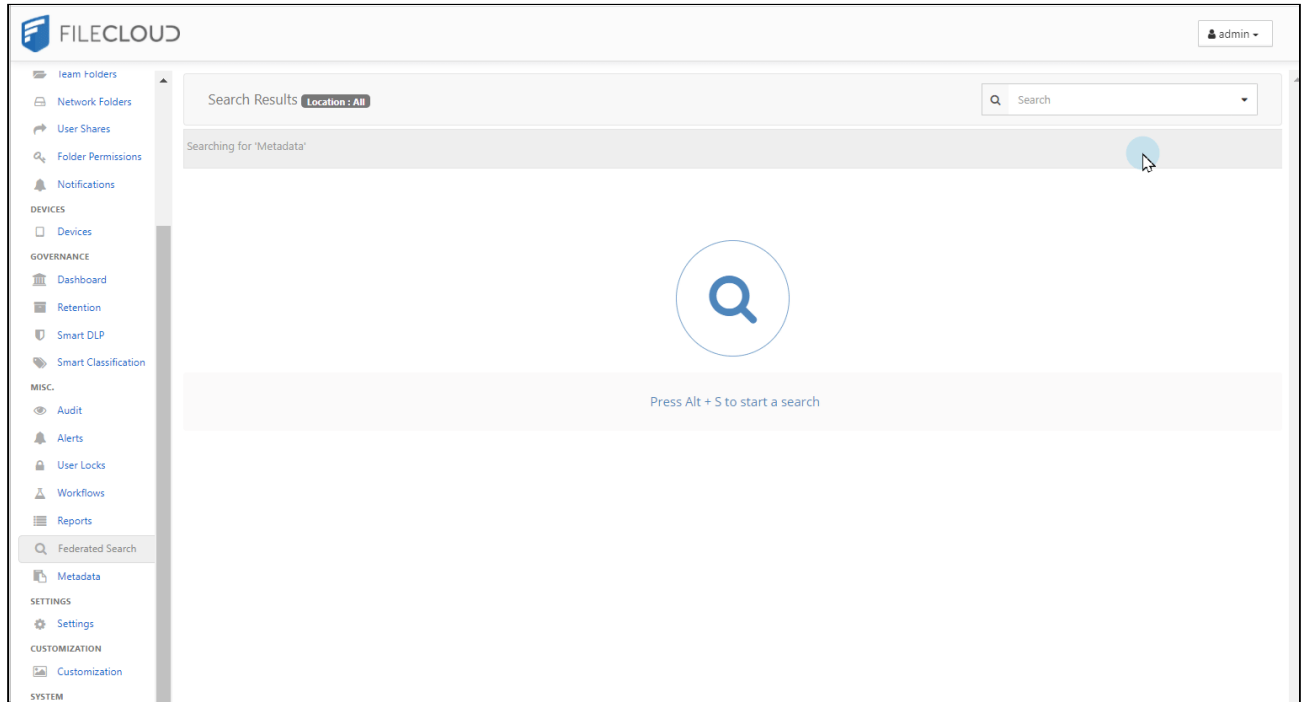
An advanced search lets you search on the search term and any of the options shown and listed below:

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

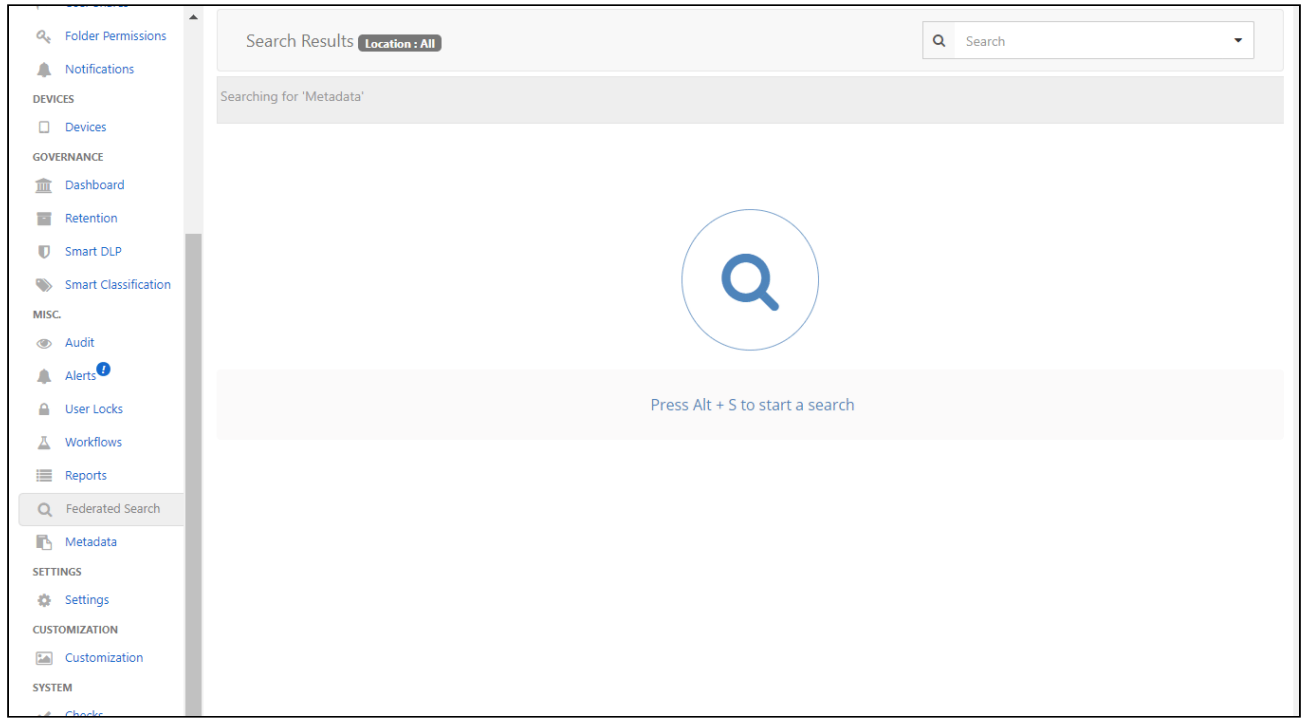
All is selected by default. This search looks for matches in file and folder names when content search is not enabled. It looks for matches in file and folder names and in the content of files when content search is enabled.



Name only search

Name Only search

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

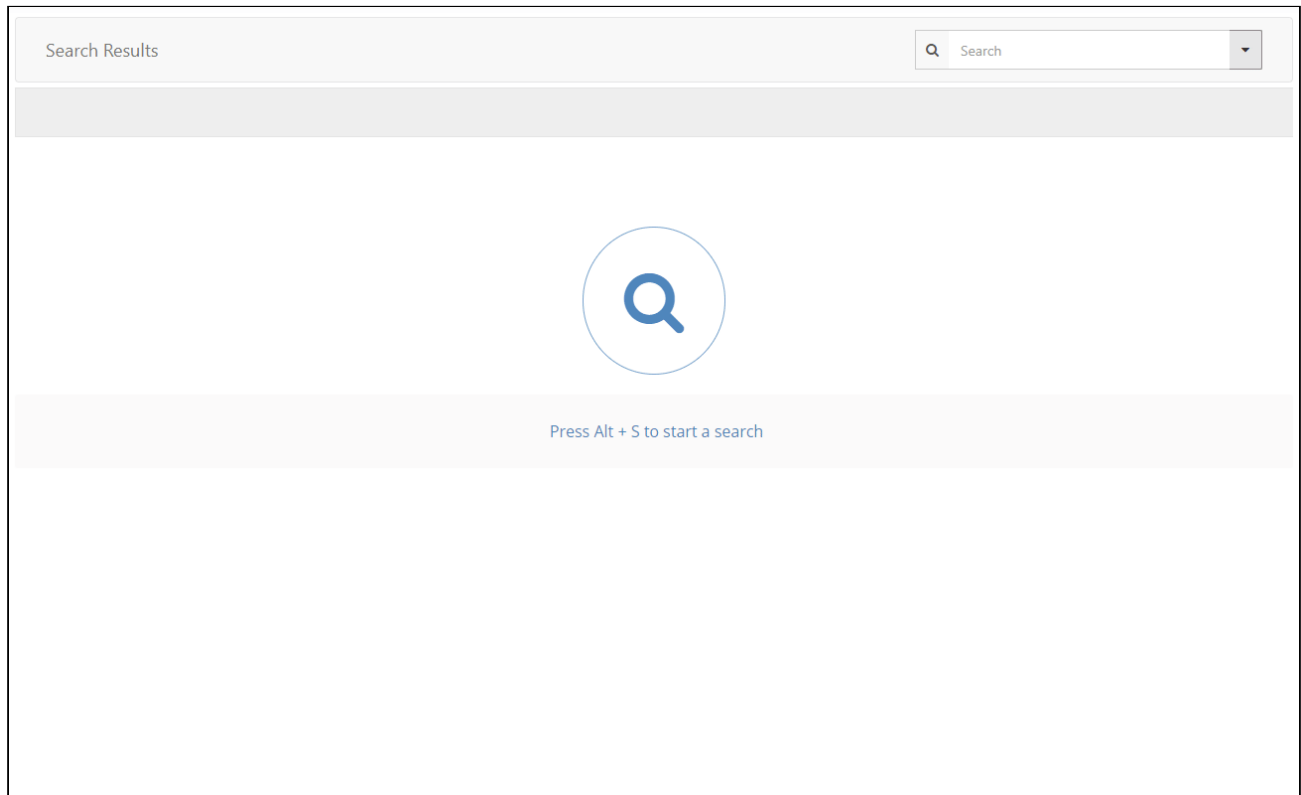


Content only search

Content Only search

When **Content Only** is selected, the search only looks for matches in the text of files. To perform a content search, your system must have [full content search](#) enabled.

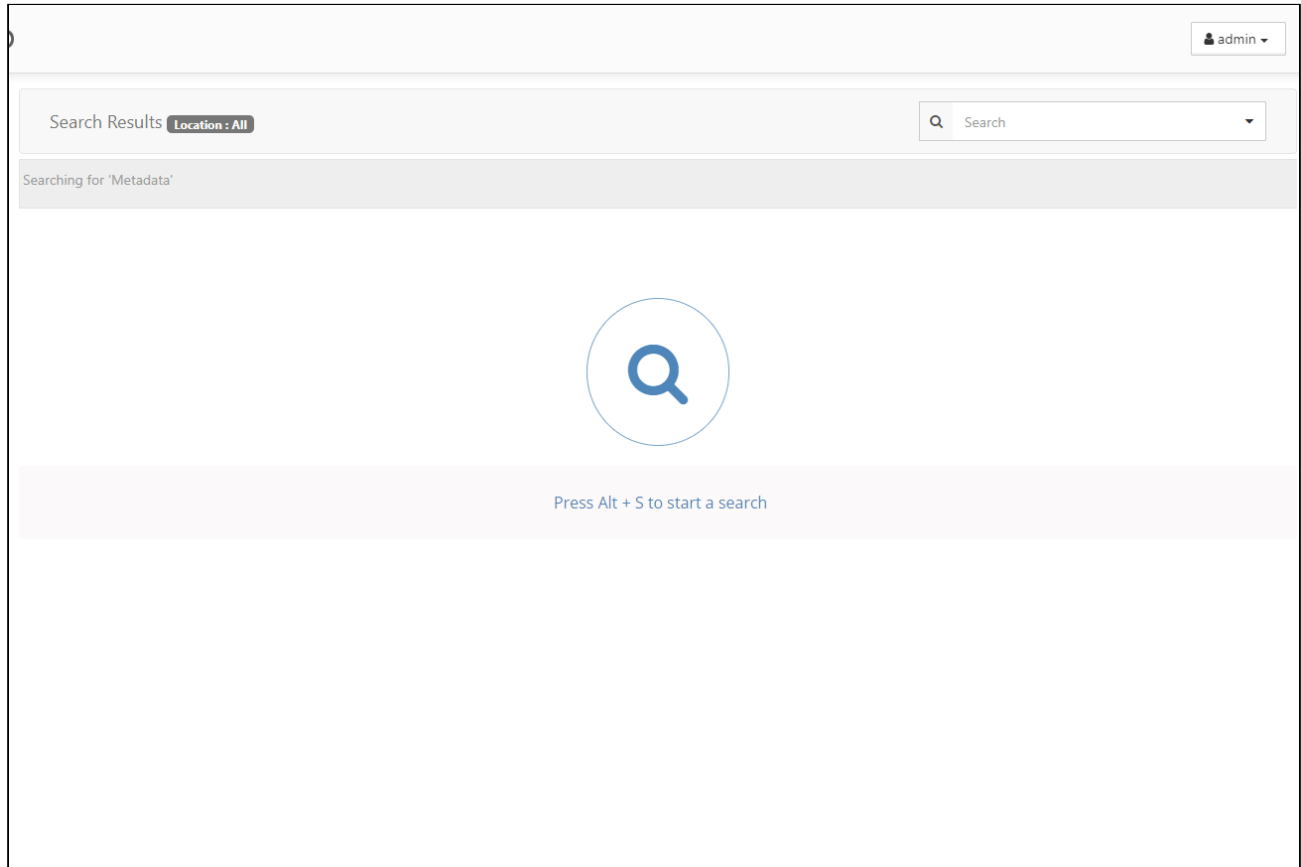
i Content search hits are returned with the matching string highlighted except in the case of lengthy search results, where omitting highlighting achieves quicker response time.



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.



PII and PCRE Searches

PII and PCRE searches

The PII search and the PCRE search both search for regex patterns, but each has its own advantages.

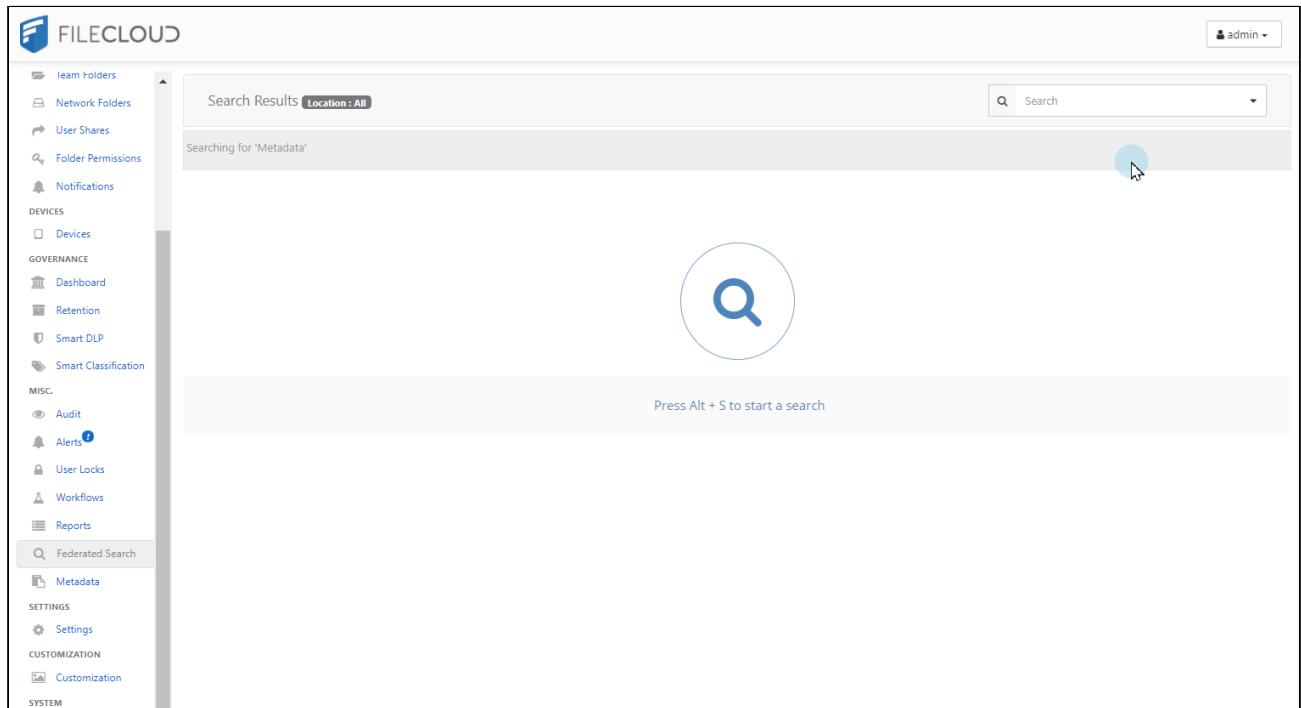
- **PII search** - The PII search is faster and more efficient than the PCRE search, and it displays the content it matches; however, it cannot match text that includes spaces or special characters. Therefore, you must use a PCRE search to find defined PII patterns that include spaces or special characters (such as US social security numbers with dashes).
- **PCRE search** - The PCRE search is much more powerful than the PII search and can match patterns with spaces and special characters. However it is slower and less efficient, and it displays the file names of matches but it does not display the matched text. When you perform a PCRE search you must enter the entire pattern into the search field; you cannot choose it from a list of predefined patterns.

PII search

The PII search searches for patterns that are set up in the [Manage PII Search](#) box in your **Settings > Content Search** tab (but cannot match PII patterns with spaces or special characters in them).

It is simpler than PCRE search and highlights content it matches. It also supports management and groupings of PII patterns which is convenient when needing to re-use a particular regex often.

Note: In the case of lengthy search results, highlighting may be omitted to achieve quicker response time.



PCRE search

The PCRE search is a content search that uses the regex engine of Perl Compatible Regular Expressions (PCRE). It is meant to be used by regex experts, search power users, and users who want to cross check patterns used in [Smart Classification](#) (CCE).

The PCRE search enables you to search directly on patterns typically used in CCE, for example, Amex CC numbers with the following patterns:

- `3[47]{1}[0-9]{13}`
- `3[47]{1}[0-9]{2}-[0-9]{6}-[0-9]{5}`
- `3[47]{1}[0-9]{2} [0-9]{4} [0-9]{4} [0-9]{3}`

The **PCRE** search option only appears when you enable PCRE mode in your system configuration.

To enable PCRE mode:

Note: Enabling PCRE mode has a performance impact on searches.

1. Open `cloudconfig.php`.
 - Windows Location : `C:\xampp\htdocs\config\cloudconfig.php`
 - Linux Location : `/var/www/html/config/cloudconfig.php`

2. Add the following:

```
define("TONIDOCLOUD_PII_PATTERN_SEARCH_PCRE_MODE_ENABLED", 1)
```

3. Save your edits.
4. Re-index your content; otherwise, existing files are not searchable by PCRE.

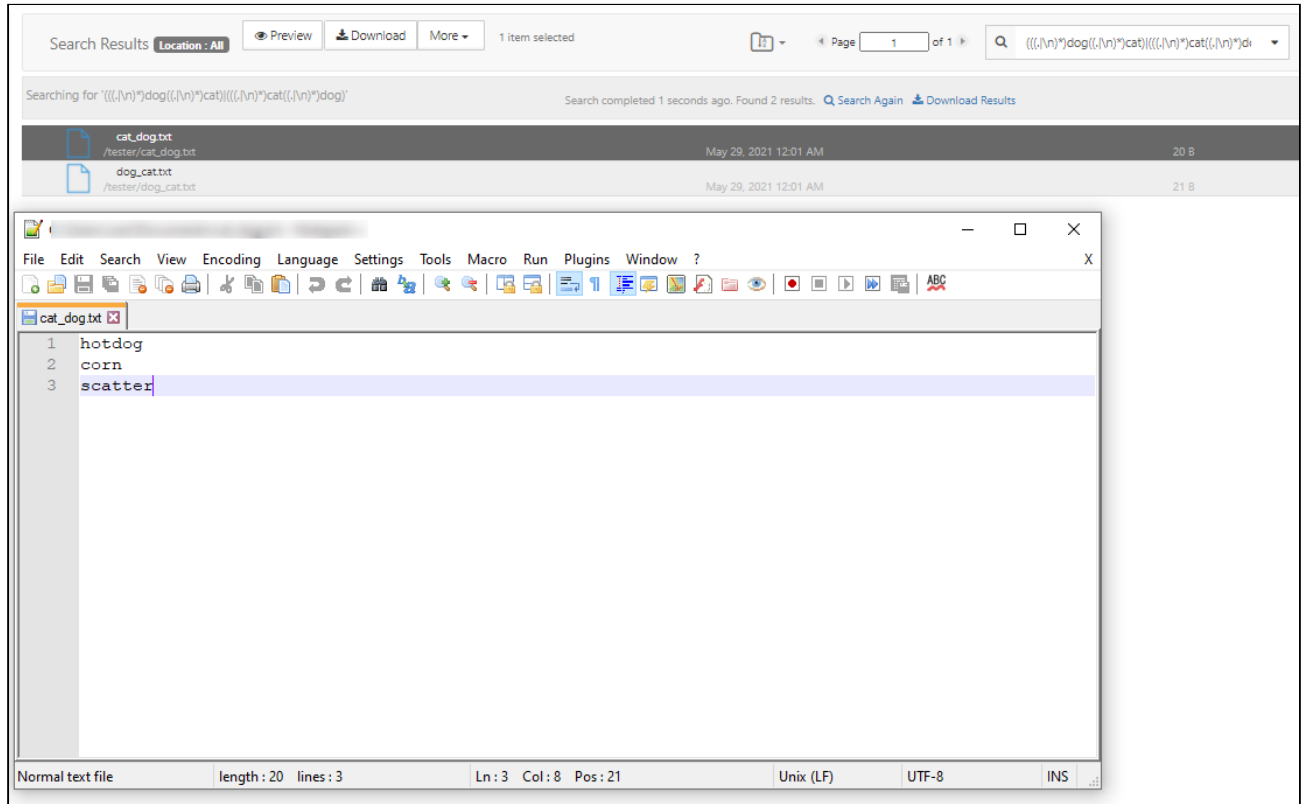
After PCRE search is enabled, newly uploaded files are automatically searchable by PCRE.

Complex searching with PCRE mode

The PCRE search is capable of using complex patterns to match strings. In the following example, the PCRE term matches with file contents that contain both **dog** and **cat** in any order.

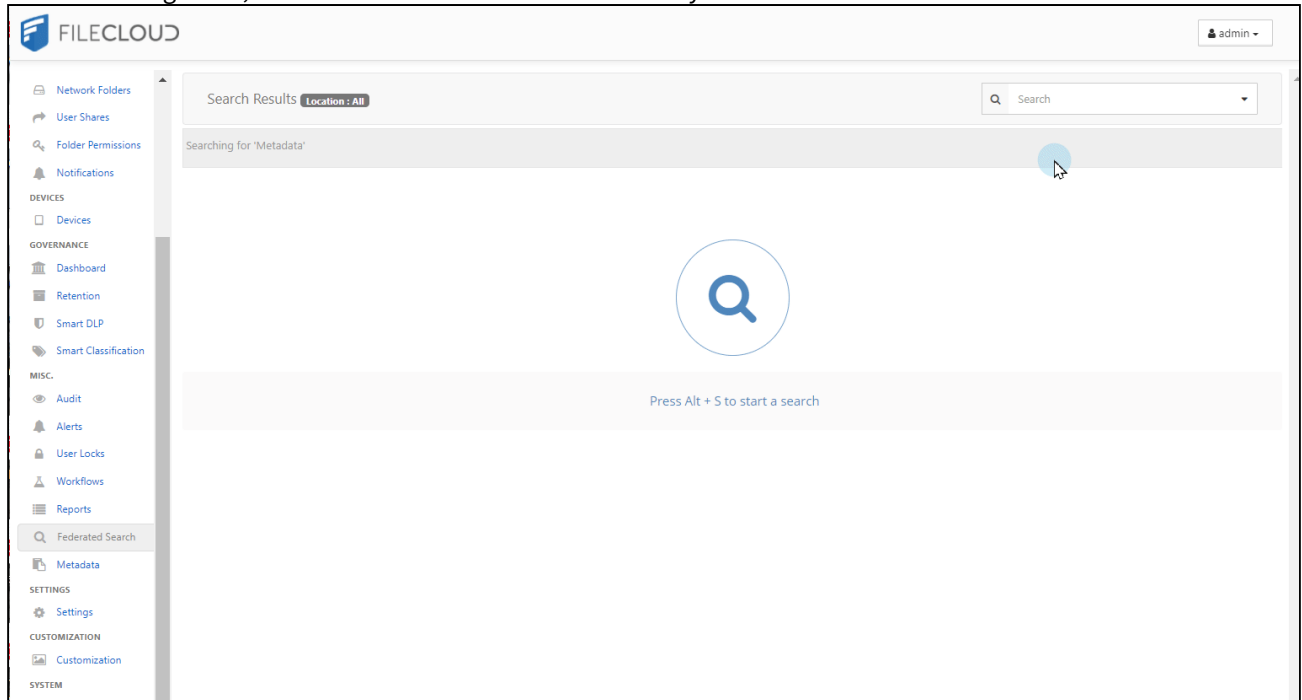
The screenshot shows the 'Advanced Search' dialog box. At the top, a search bar contains the PCRE pattern: `((.\\n)*dog(.\\n)*cat)((.\\n)*cat(.\\n)*dog)`. Below the search bar, the 'Term' field also contains this pattern. The 'Scope' section has radio buttons for 'All', 'Name Only', 'Content Only', 'Metadata', and 'PII', with 'PCRE' selected. The 'Search Type' section has radio buttons for 'All files/folders', 'Files Only', and 'Folders Only', with 'All files/folders' selected. The 'Path Selection' section has radio buttons for 'All' and 'Selected', with 'All' selected. The 'Selected Path' field is empty. The 'File Type' dropdown is set to 'All Types'. The 'Date' section has two input fields for 'Modified From' and 'Modified To'. The 'Results Count' section has radio buttons for 'Limit 50' and 'All', with 'Limit 50' selected. The 'Use Cache Results' checkbox is unchecked. At the bottom right, there are 'Clear' and 'Search' buttons.

The following files are returned. The first is opened to show the matching content.



Performing a PCRE Search

In the following video, the PCRE search looks for social security numbers.



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> <p>Compact the Audit Database</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](#)
-  [Compact the Audit Database](#)

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.



Operation Filter : Common

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



User Agent : All

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.

Compact the Audit Database

Although deleting entries from the audit logs on the Audit screen removes the entries from the database, MongoDB doesn't free up that space.

- MongoDB retains the space to use for new entries that will be added in the future.

If for some reason, you need to reclaim the space, you can compact or repair the database.

To compact a MongoDB database:

1. Open MongoDB client command interface, which is typically located in:

Windows	C:\xampp\mongodb\bin\mongosh.exe
Linux	/usr/bin/mongosh

2. Run the following command in the MongoDB client.

```
> use tonidoauditdb;
> db.runCommand({ compact: 'audit' });
> show dbs;
> exit;
```

Now the unused space is available on your server.

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	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> REQUEST ▼ </div> <p style="font-size: small; margin-top: 5px;">Level of Audit Logging</p> <p style="font-size: x-small; margin-top: 5px;">OFF - No Audit Log Recorded</p> <p style="font-size: x-small; margin-top: 5px;">REQUEST - Log all requests and results of request but not the full response</p> <p style="font-size: x-small; margin-top: 5px;">FULL - Log complete request and response.</p>
Auto Archive Audit Database	<input type="checkbox"/> <p style="font-size: x-small; margin-top: 5px;">Enable automatic export and delete of audit records.</p> <p style="font-size: x-small; margin-top: 5px;">NOTE: Cron Job must be set up and running</p>
Auto Archive Audit Records After (in days)	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <input style="width: 100%; border: none;" type="text" value="7"/> </div> <p style="font-size: x-small; margin-top: 5px;">Export and delete audit records that are older than (Number of Days) (Required to auto archive audit db)</p> <p style="font-size: x-small; margin-top: 5px; color: red;">NOTE: Files will be exported daily and stored in CSV format. Exported records will be deleted from audit database.</p>
Storage Path For Archived Audit Records	<div style="display: flex; align-items: center;"> <input style="width: 80%; border: 1px solid #ccc;" type="text"/> <div style="border: 1px solid #ccc; background-color: #007bff; color: white; padding: 2px 5px; margin-left: 5px;">Check Path</div> </div> <p style="font-size: x-small; margin-top: 5px;">Specify the location to store exported audit files. This location must be writable by the webserver</p>

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*.

Specify which operations and from which agents don't get logged

To configure what information is logged:

1. On the FileCloud Server, navigate to the following folder:

```
WWWROOT\config
```

2. Open the following file for editing:

```
cloudconfig.php
```

3. Add the following lines:

Configuration Lines to add	Notes	Example
define("TONIDOCLOUD_AUDIT_IGNORE_OPS", "");	When specified, does not add audit logs for specific FileCloud requests. You can specify multiple requests by using a ' ' symbol as a delimiter. For example, if you add "deletefile loginguest", both these operations would not be added to the audit log.	<i>define("TONIDOCLOUD_AUDIT_IGNORE_OPS", "deletefile loginguest createfolder");</i>
define("TONIDOCLOUD_AUDIT_IGNORE_AGENT", "");	When specified, does not add audit logs for any requests coming in from specified FileCloud clients. You can specify multiple clients by using a ' ' symbol as a delimiter.	<i>define("TONIDOCLOUD_AUDIT_IGNORE_AGENT", "Cloud Sync Mozilla/5.0 (Windows NT 6.3; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0 FileCloudDrive");</i>

⚠ If both defines are specified, then only requests that match both conditions are excluded from the Audit Log.

For example:

```
define("TONIDOCLOUD_AUDIT_IGNORE_OPS", "deletefile|loginquest|createfolder");
define("TONIDOCLOUD_AUDIT_IGNORE_AGENT", "Cloud Sync");
```

The above configuration will skip adding audit logs when the Cloud Sync client requests to:

- Delete File
- Login Guest
- Create Folder

! 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**.

User name	Message	Agent	Created On
miok1	miok1 logged in FAIL	Unknown	2018-Jan-23 12:37 AM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-23 12:21 AM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 11:53 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 11:35 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 11:22 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 10:51 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 10:38 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 10:07 PM
admin (admin)	admin (admin) logged in OK	Web browser	2018-Jan-22 09:38 PM
miok1	miok1 logged in FAIL	Unknown	2018-Jan-22 09:35 PM

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.

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

➔ If you need to reclaim the space, you should [compact the database](#).

How do you want to remove Audit log entries?

➔ [Manually Trim the Audit Database](#)

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. Below the title bar, there are two text input fields. The first is labeled "Start Date (Optional)" and the second is labeled "End Date (Required)". At the bottom of the dialog, there are three buttons: "Export" (blue), "Delete" (red), and "Close" (grey).

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*.

Enable automatic archival and removal

To ensure that audit database does not grow too large for its allotted disk space, audit records should be archived and removed regularly.

⚠ Before you enable Automatic Archiving, you must ensure that Cron job or Task Scheduler is installed and running.

When you are deciding whether or not to automatically archive and remove audit records (or how often to archive and remove them), please note that [some reports use the audit log](#) and can only show events if they are still contained in the audit log.

As part of the daily [cron job](#) (scheduled task), you can configure FileCloud to export records to a .csv file and delete those records from the audit database.

This is configured in the Settings screen on the Admin tab.

To auto archive audit log entries:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation panel, click *Settings*.
3. Click the Admin tab.
4. Scroll down to Audit Settings.
5. Fill in all of the settings as indicated in the following table:

Setting	Description
Audit Logging Level	Options are <ul style="list-style-type: none"> • 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	Check the check box to enable auto archive. NOTE: Cron Job must be set up and running.
Auto Archive Audit Records after (in days)	Number of days to store the audit records in the database. After the number of days specified, audit records are exported to csv and deleted from the audit database
Storage Path for Archived Audit Records	Folder path to store the exported audit records in CSV format. For example, C:\archives

i If you want to automatically remove records but not archive them, you can configure FileCloud to remove audit records but not export them to a csv file.

To auto remove records without exporting them:

1. Open cloudconfig.php:
 Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
 Linux Location: /var/www/config/cloudconfig.php

2. Add the following :

```
Define("TONIDOCLOUD_AUDIT_AUTO_ARCHIVE_OMIT_BACKUP", true);
```

Disable manual deletion

To disable manual deletion by administrators.:

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

```
define("TONIDOCLOUD_DISALLOW_ADMIN_AUDIT_DELETE", true);
```
3. Save and close cloudconfig.php.
 Now, in the *Admin Portal* when you click *Audit* in the navigation pane, and then click *Manage*, the Delete button is no longer available on the Manage Audit Logs dialog box.



Manually Trim the Audit Database

Removing older data by archiving it in a CSV file can help reduce the size of your audit database as well as improve the performance of audit logging and the system where the audit logs are stored.

Trimming the audit database for FileCloud uses the following procedure:

1. Log In to the MongoDB Shell

You will need to log in to the MongoDB database to trim it. Use the following information when logging on.

Table 1. MongoDB Log In Options

Option	Description	Example  Always replace the sample values in the examples with the values used in your deployment.
--port <port>	Specifies the port where the <code>mongod</code> or <code>mongos</code> instance is listening. If <code>--port</code> is not specified, <code>mongo</code> attempts to connect to port 27017.	--port 27017
--username <username>, -u <username>	Specifies a username with which to authenticate to a MongoDB database that uses authentication. Use in conjunction with the <code>--password</code> and <code>--authenticationDatabase</code> options.	-u "myUserAdmin"
--password <password>, -p <password>	Specifies a password with which to authenticate to a MongoDB database that uses authentication. Use in conjunction with the <code>--username</code> and <code>--authenticationDatabase</code> options. To force <code>mongo</code> to prompt for a password, enter the <code>--password</code> option as the last option and leave out the argument.	-p "abc123"
--authenticationDatabase <dbname>	Specifies the database in which the user is created. See Authentication Database . If you do not specify a value for <code>--authenticationDatabase</code> , <code>mongo</code> uses the database specified in the connection string.	--authenticationDatabase "admin"

To log in to the mongo shell, use the following command: (replace the settings in this example with settings used in your deployment)

```
mongosh --port 27017 -u "myUserAdmin" -p "abc123" --authenticationDatabase "admin"
```

2. Export the Mongo database collection that contains the audit entries.

You can use `mongoexport` to produce a JSON or CSV export of data stored in a MongoDB instance.

Table 1. MongoExport Options

Option	Description	Example
<code>--db <database>, -d <database></code>	Specifies the name of the database on which to run the mongoexport .	<code>--db tonidoauditdb</code>
<code>--collection <collection>, -c <collection></code>	Specifies the collection to export.	<code>--collection audit</code>
<code>--type <string></code>	<p><i>Default:</i> json</p> <p>New in version 3.0.</p> <p>Specifies the file type to export. Specify <code>csv</code> for CSV format or <code>json</code> for JSON format.</p> <p>If you specify <code>csv</code>, then you must also use either the <code>--fields</code> or the <code>--fieldFile</code> option to declare the fields to export from the collection.</p>	<code>--type=csv</code>
<code>--fields <field1[,field2]>, -f <field1[,field2]></code>	<p>Specifies a field or fields to <i>include</i> in the export. Use a comma separated list of fields to specify multiple fields.</p> <p>If any of your field names include white space, use quotation marks to enclose the field list.</p> <p>For example, to export two fields, phone and user number, you would specify <code>--fields "phone,user number"</code>.</p> <p>For <code>csv</code> output formats, <code>mongoexport</code> includes only the specified field(s), and the specified field(s) can be a field within a sub-document.</p>	<code>--fields createdon,username,how,ip,useragent,operation,request,deviceinfo</code>
<code>--out <file>, -o <file></code>	<p>The output directory where you need to export data as a csv.</p> <p>You must change this location to match the directory in your deployment.</p>	<code>--out c:\xampp\test.csv</code>

Export considerations:

- You must run `mongoexport` against a running `mongod` or `mongos` instance as appropriate.
- Avoid using `mongoimport` and `mongoexport` for full instance production backups. These utilities do not reliably preserve all rich BSON data types, because JSON can only represent a subset of the types supported

by BSON. Use `mongodump` and `mongoexport` as described in [MongoDB Backup Methods](#) for this kind of functionality.

➔ To read more about this utility, read the MongoDB documentation for [MongoExport](#).

To export the Audit database:

1. Ensure that MongoDB is running before attempting to start the mongo shell.
2. Log into the primary database as the admin user through mongo shell.
3. Run the following command:

```
mongoexport.exe --db tonidoauditdb --collection audit --type=csv --fields
createdon,username,how,ip,useragent,operation,request,deviceinfo --out c:
\xampp\test.csv
```

3. Verify the CSV contains valid information.

It is important to check that the data has been successfully exported before removing it from the MongoDB database.

To verify the exported data:

1. Navigate to the output directory where you saved the csv file. For example: `c:\xampp\test.csv`
2. Open the csv file in Excel or another editor.
3. Verify the data looks correct.

4. Remove the exported audit data from the Mongo database.

After you have exported the data to a csv file, you can now drop the collections in the auditdb database.

The drop command removes a collection or [view](#) from the database.

- ❗ The drop method also removes any indexes associated with the dropped collection.
 - The method provides a wrapper around the `drop` command.
 - This method obtains a write lock on the affected database and will block other operations until it has completed.
 - The `db.collection.drop()` method and `drop` command create an `invalidate Event` for any `Change Streams` opened on dropped collection.
 - Starting in MongoDB 4.0.2, dropping a collection deletes its associated zone/tag ranges.

To drop the exported data from auditdb:

1. Ensure that MongoDB is running before attempting to start the mongo shell.
2. Log in to the mongo shell
3. To print a list of all databases on the server, run the following command:

```
show dbs;
```

4. To switch to the database provided as a parameter, run the following command:

```
use tonidoauditdb
```

5. To list all the databases available for use on the connected MongoDB instance, run the following command:

```
show collections
```

6. To remove an entire collection from a database, use the following command:

```
db.audit.drop()
```

7. You will see one of the following responses:

```
Returns:  
true when successfully drops a collection.  
false when collection to drop does not exist.
```

8. To list all the databases available for use on the connected MongoDB instance, run the following command:

```
show collections
```

You should see responses similar to the following example:

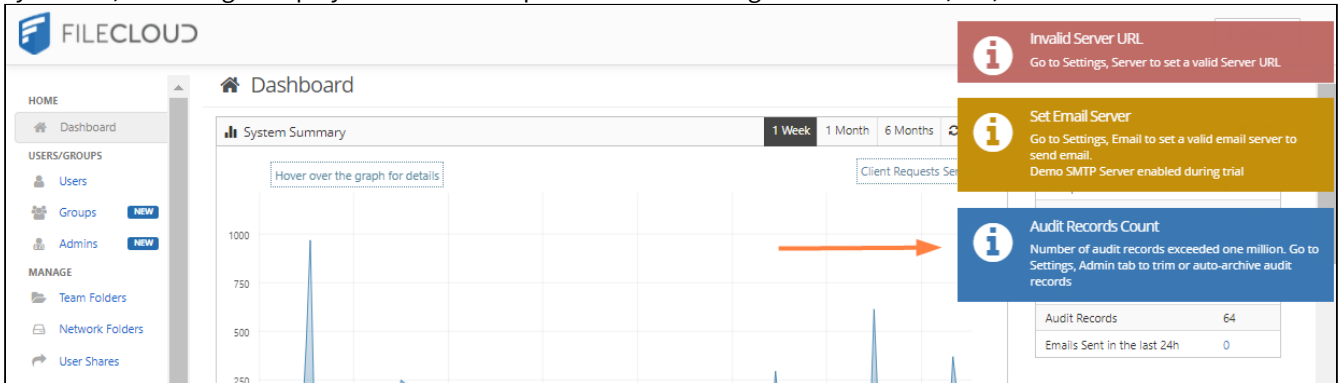
```

Administrator: Command Prompt - mongo.exe
C:\xampp\mongodb\bin>
C:\xampp\mongodb\bin>
C:\xampp\mongodb\bin>mongo.exe
MongoDB shell version: 3.4.3-80-gbc3d66e
connecting to: mongodb://127.0.0.1:27017
MongoDB server version: 3.4.3-80-gbc3d66e
Server has startup warnings:
2018-08-15T10:50:40.526-0700 I CONTROL [initandlisten]
2018-08-15T10:50:40.526-0700 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2018-08-15T10:50:40.526-0700 I CONTROL [initandlisten] **           Read and write access to data and configuration is unrestricted.
2018-08-15T10:50:40.526-0700 I CONTROL [initandlisten]
> show dbs;
admin                0.000000
local                0.000000
tonidoauditdb        0.000000
tonidoclouddb        0.001000
tonidosettings       0.000000
tonidostoredb        0.001000
tonidosyncdb         0.000000
> use tonidoauditdb
switched to db tonidoauditdb
> show collections
audit
audit
notificationstream
report_result
search_result
searchterms
shareactivity
> db.audit.drop()
true
> show collections
audit
notificationstream
report_result
search_result
searchterms
shareactivity

```

Change the Audit Log Warning Limit

By default, a warning is displayed in the Admin portal when audit log entries exceed 1,000,000:



You may customize the number of entries that triggers the warning.

To change the number of audit log entries that triggers a warning:

1. Open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add the following :

```
define("TONIDOCLOUD_AUDIT_ENTRIES_WARNING_THRESHOLD,1000000)
```

3. Replace 1000000 with the number of entries that will trigger the warning.
Any number is valid.

Backing Up and Restoring FileCloud Server



FileCloud Server provides many ways to back up data. Having a copy of the database and the FileCloud Server site allows you to restore the site if you encounter a catastrophic failure.

What do you want to do?



→ [Install and Use the Backup Server Tool](#) for Linux or Windows



→ [Backup and Restore Linux Deployments](#)



→ [Manually Backup and Restore Windows Deployments](#)



→ [Migrate or transfer Files to a FileCloud Site](#)

The FileCloud Server Backup Tool



FileCloud Server Backup and Restore option is available for administrators in version 11.0 and later.



You can use FileCloud Backup Server to create a copy of an entire server installation.

The backup includes:

- files
- folders
- users
- groups
- shares
- audit logs

- [FileCloud Backup Server Features](#)
- [FileCloud Backup Server Installation](#)

- [FileCloud Backup Server Configuration](#)
- [Backup Server Configuration Using RSync](#)
- [FileCloud Backup Server Operations](#)
- [FileCloud Backup Server Troubleshooting](#)

FileCloud Backup Server Features

Warning

FileCloud backup server is still a beta feature. Please test the capabilities and features before using in a production environment.

Introduction

FileCloud backup server feature is available with FileCloud server version starting from v11.0.

Features

FileCloud backup server is same as any FileCloud server except it will only backup other FileCloud installations. Following are some of the features of FileCloud backup server.

- Backup server can be installed on Windows or Linux. It is supported in the distros on which FileCloud server is supported.
- Backup server supports backing up of multiple sites.
- Backup server supports backing up of multiple FileCloud servers.
- Backups can be started immediately or scheduled for later.
- Backups can be started from command line.
- Backup schedules can be repeated daily, weekly or monthly.
- Backup server uses security key to connect to FileCloud servers for backup.
- By default, the backup server URL is not enabled. To enable the backup server URL see [Enabling the Backup Server URL](#).

Limitations

Current version of FileCloud backup server has some limitations:

- Backup server cannot backup files if the backend storage is S3.
- Backup server cannot backup or restore files if the storage is encrypted.
- When the backup server uses the HTTP protocol for downloads, it will not scale for larger installations. We recommend using the Rsync method for larger installations.
- Backup server might affect performance if backup is performed during peak production time.

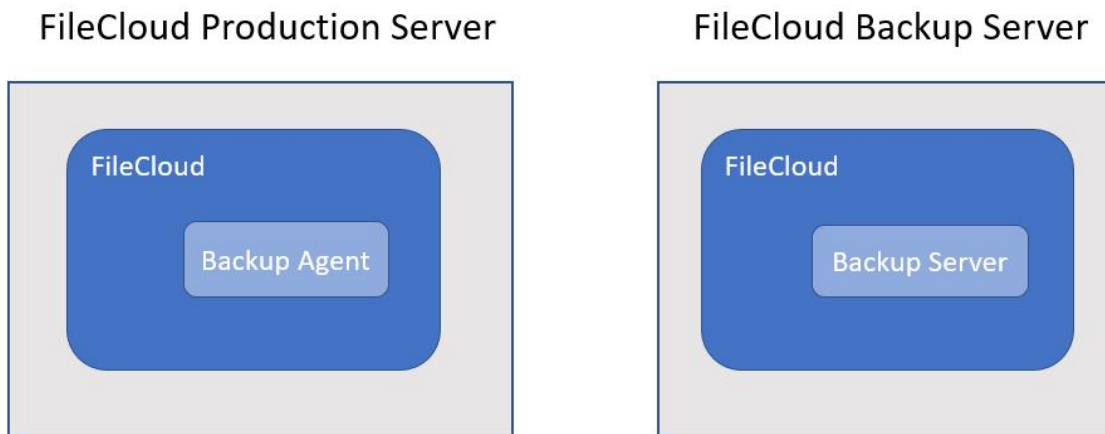
FileCloud Backup Server Installation

Introduction

Follow these steps to install FileCloud backup server.

Note

- **The FileCloud backup server has to be installed on a new server. Installing the backup server on the production server is not supported by the backup solution. Please refer to Figure 1 for the recommended setup.**
- **The FileCloud backup server is added to a fresh FileCloud installation** without the need for a FileCloud user license. For this installation, the administrator has to first install FileCloud on the new server and then add backup server capability to it.
- **The target/production FileCloud server must be running same FileCloud version as the FileCloud backup server.**

Figure 1: Backup Server Setup**Step 1: Install FileCloud Server**

Install latest FileCloud on the backup server. Note that this FileCloud installation is different from the production FileCloud installation. Backup server is same as any FileCloud server except it will only backup other FileCloud installations. The installation of FileCloud backup server starts with installing a FileCloud server using the OS specific installation packages, available in your trial [portal](#). Please find the installation instructions [here](#).

Step 2: Install Backup Server

In FileCloud version 19.1 and later, Backupserver is bundled as part of the main installer. If you are installing 19.1 or later, there is no need for a separate download.

By default, the backup server URL is disabled. You must add a setting to both the backup server config file and the production server config file to enable it and access it as a site.

To enable the backup server URL:

1. In your production server's FileCloud directory, open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add the following:

```
define("TONIDOCLOUD_ENABLE_BACKUPSERVER_APP", true);
```

- Repeat steps 1 and 2 in your backup server's FileCloud directory.

I am installing a version earlier than 19.1 (18.2 and earlier)

Now that the base FileCloud server is installed, download the backup server installation package(backupserver.zip) from [here](#). Assume the file is downloaded to a temporary location as follows:

OS	Temporary Location
Linux	/tmp/backupserver.zip
Win	C:\temp\backupserver.zip

Now to install backup server, unzip the contents of backup server zip onto the WWWROOT folder of FileCloud server.

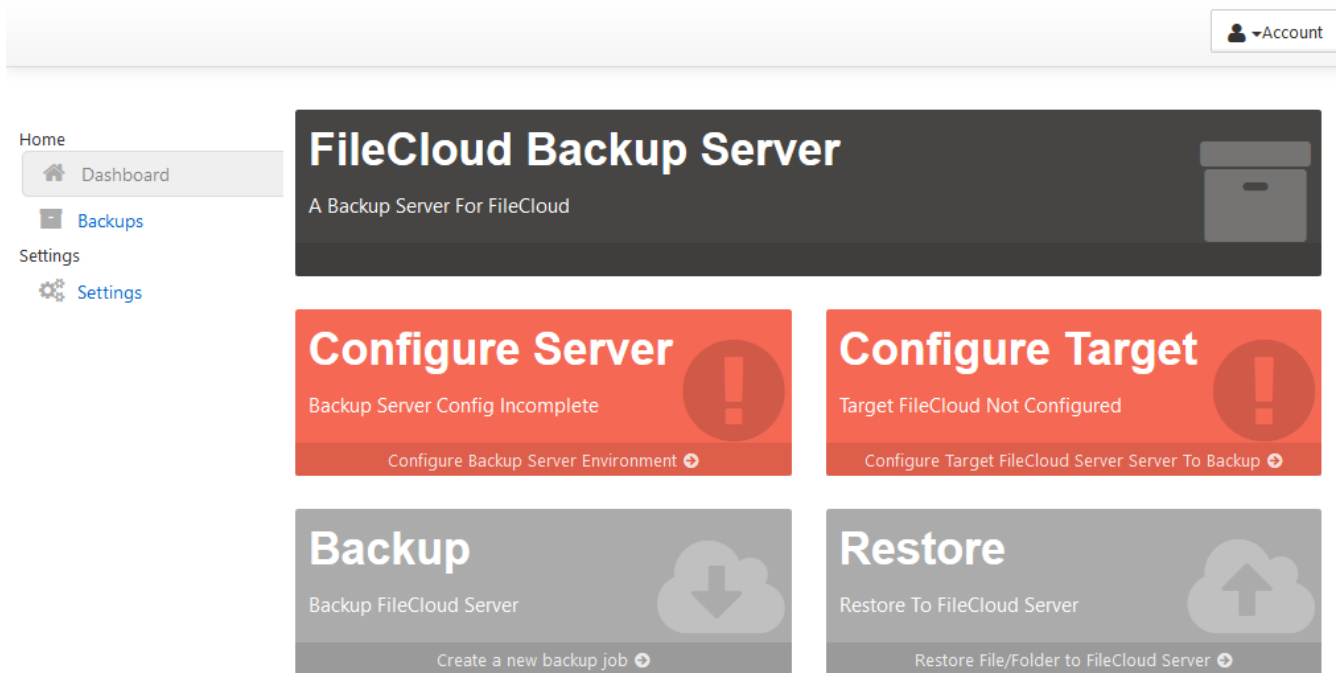
OS	Unzip command	Remarks
Linux	\$ sudo cd /var/www/app \$ sudo su - www-data -s /bin/bash -c "unzip /tmp/backupserver.zip"	If your WWWROOT is a different folder, adjust the command accordingly.
Win	Place the contents of backupserver.zip onto C:\xampp\htdocs\app	If your xampp WWWROOT is a different folder, adjust the command accordingly.

Step 3: Access Backup Server UI

Once the above steps are completed, access the backup server web UI by using the following information:

Parameter	Value	Remarks
URL	http://<SERVER_IP>/ui/backupserver/index.html	
User name	admin	
Password	Default value is 'password'	The default password can be changed by visiting the admin server (http://<SERVER_IP>/ui/admin/index.html).

An unconfigured backup server UI will look like this:



FileCloud Backup Server Configuration

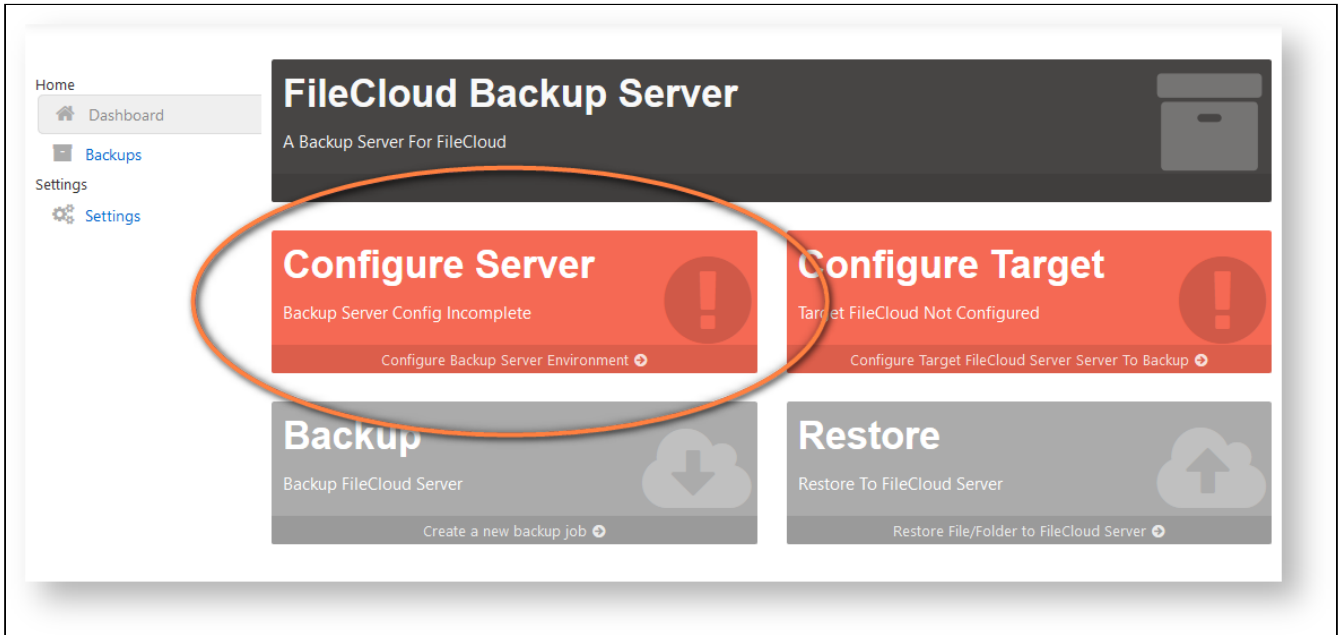
Introduction

A new FileCloud installation needs to be configured before it can be used for backup purposes.

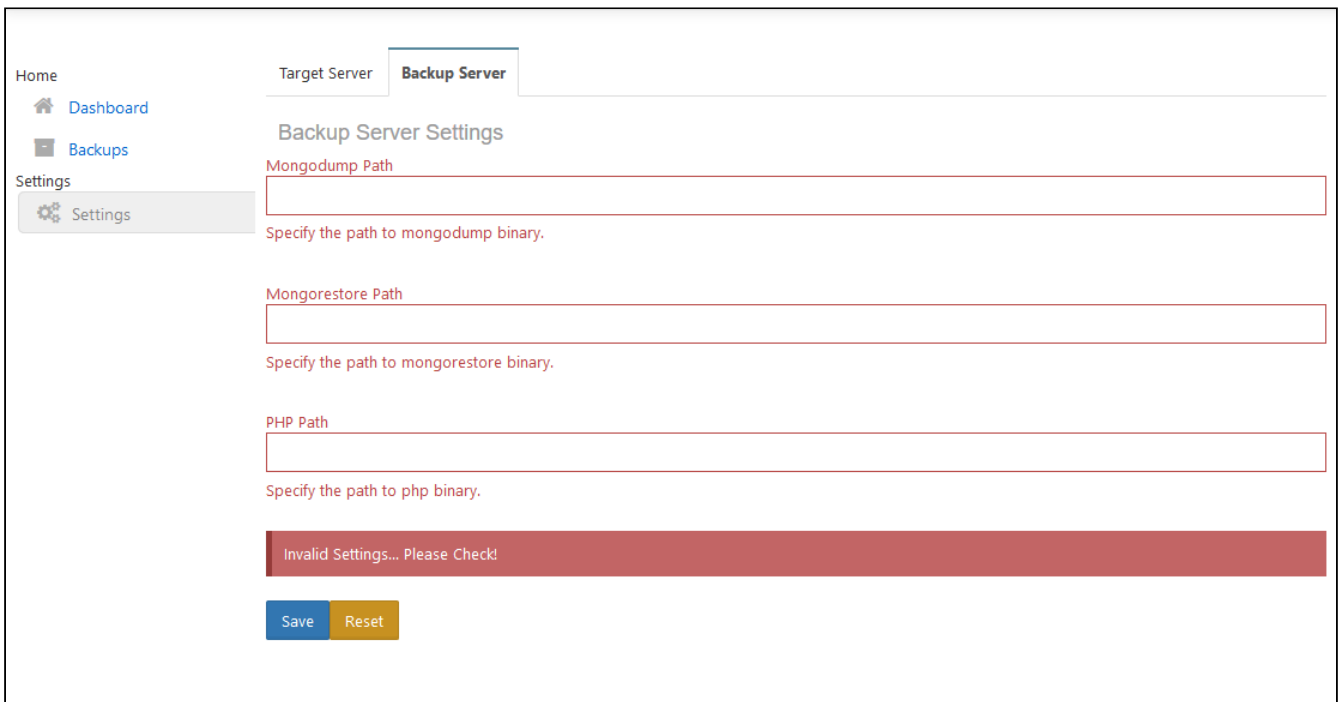
Step 1: Configuring Backup Server

This step is necessary to configure some basic parameters necessary for backup server. To configure the backup server, open the backup server UI and click on Settings -> "Backup Server" tab.

The backup server settings can also be opened by clicking on the "Configure Server" button on the dashboard.



By default the backup server parameters will be empty and update them using the table below.



Parameter Label	Value	Remarks
Mongodump Path	Linux: /usr/bin/mongodump Win: C: \xampp\mongodb\bin\mongodump.exe	Path to the mongodump command.

Parameter Label	Value	Remarks
Mongorestore Path	Linux: /usr/bin/mongorestore Win: C: \xampp\mongodb\bin\mongorestore.exe	Path to the mongorestore command.
PHP Path	Linux: /usr/bin/php Win: C:\xampp\php\php.exe	Path to the php executable.

A properly configured backup server settings should like this:

The screenshot shows the 'Backup Server' configuration page. On the left, there is a navigation menu with 'Home', 'Dashboard', 'Backups', and 'Settings'. The 'Settings' section is active. The main content area is titled 'Backup Server Settings' and contains three input fields: 'Mongodump Path' with the value '/usr/bin/mongodump', 'Mongorestore Path' with the value '/usr/bin/mongorestore', and 'PHP Path' with the value '/usr/bin/php'. Below each field is a small instruction: 'Specify the path to mongodump binary.', 'Specify the path to mongorestore binary.', and 'Specify the path to php binary.' respectively. At the bottom of the form, there is a green banner that says 'Changes Saved Successfully!' and two buttons: 'Save' and 'Reset'.

Step 2: Preparing Target FileCloud Server

Before a FileCloud server can be added to the backup server as a backup target, it needs to be prepared with an access key. This access key serves as a security mechanism, allowing only backup requests made along with this key.

To enable this access key, follow these steps:

1. Open the folder `WWWROOT/config/` on the target FileCloud server.
2. Copy the file `backupagentconfig-sample.php` as `backupagentconfig.php`
3. Edit the `backupagentconfig.php` file and set a backup security key.

```
<?php
/* Configuration values for FileCloud */

// ... Server URL
define("BACKUPAGENT_ACCESS_KEY", "test908acc" );

?>
```

4. **Optional:** If your installation is not the default location, then you can specify the installation paths using the following keys in backupagentconfig.php

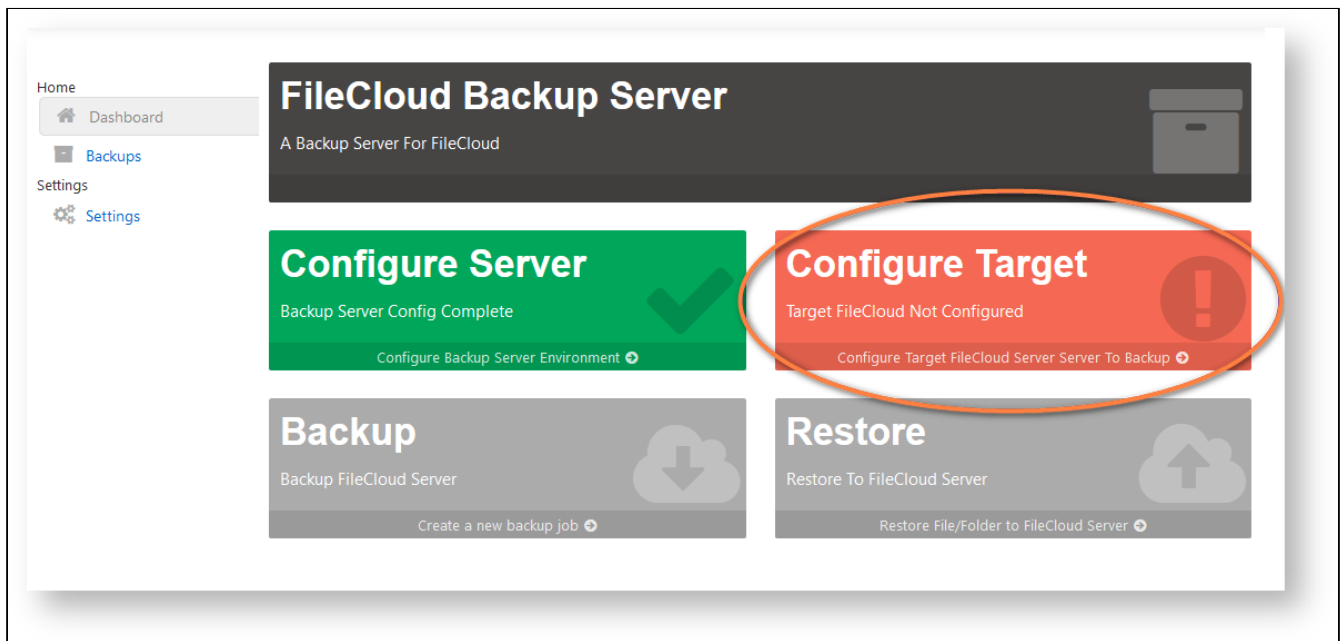
```
define("BACKUPAGENT_DBDATA_PATH", "D:\\xampp\\mongodb\\bin\\data" );

define("BACKUPSERVER_MONGODUMP_PATH", "D:\\xampp\\mongodb\\bin\\
\\mongodump.exe" );
```

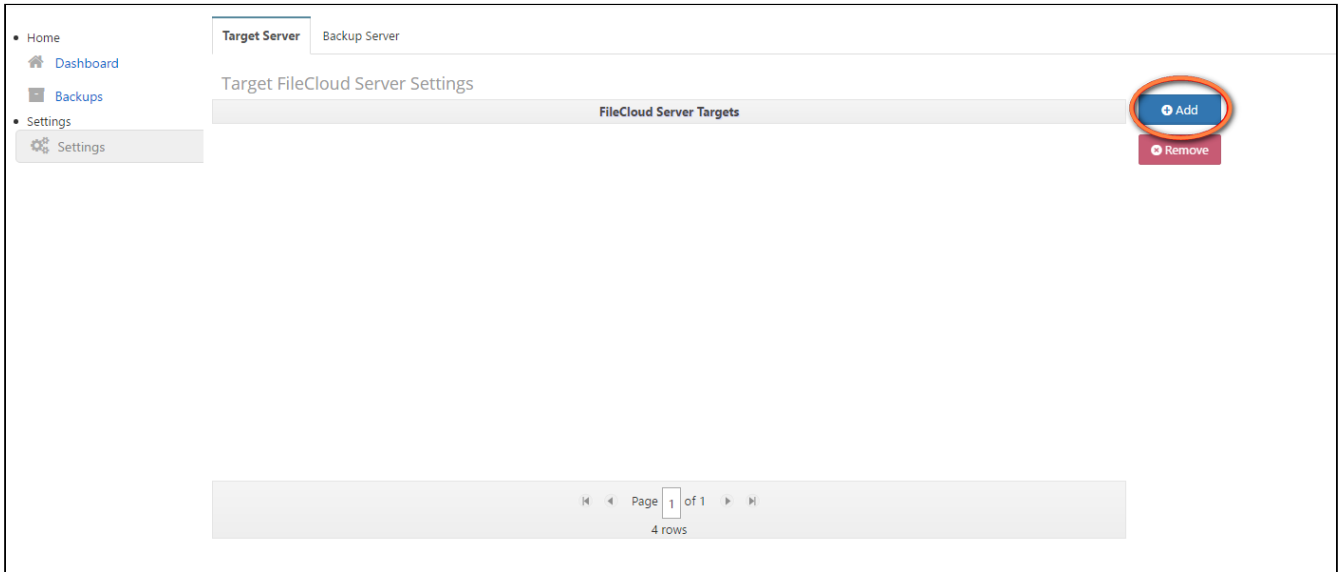
Step 3: Adding Target FileCloud Server

After setting the access key, the prepped FileCloud server can be added as a backup target. To add a new FileCloud server target, open the backup server UI and click on Settings -> "Target Server" tab.

The backup server settings can also be opened by clicking on the "Configure Button" button on the dashboard.



This will navigate to 'Settings' tab. Click on the 'Add' button, to add a new target site.



Clicking 'Add' button will bring up the backup target server dialog.

The screenshot shows the 'Update Backup Target Server' dialog box. It contains the following fields and instructions:

- Target Name:** A text input field containing 'fctarget'. Below it, the instruction reads: 'Specify a name to denote FileCloud server to backup.'
- Target URL:** A text input field containing 'https://192.168.1.108/'. Below it, the instruction reads: 'Specify the URL of FileCloud server to backup.'
- Storage Directory:** A text input field containing 'C:\\backupstore' with a checkmark icon on the right. Below it, the instruction reads: 'Specify directory under which the backups will be stored'
- Backup API Key:** A text input field containing seven dots. Below it, the instruction reads: 'Specify the backup API key that should be used to connect to the FileCloud server'
- Backup connection:** A dropdown menu with 'HTTP' selected. Below it, the instruction reads: 'Specify the connection to use for file downloads'

By default the target server parameters will be empty and update them using the table below. Click 'Add' once all the information has been added.

Parameter Label	Sample Value	Remarks
Target Name	fctarget	A string to represent the target.
Target URL	http://192.168.1.108/	Base URL to the target FileCloud server.
Storage Directory	Linux: /backupstore/ Win: C:\\backupstore	A folder in the backup server where the backups from this target will be stored. Admins can use the "Check Path" button to check if the folder is valid and writable for the backup server. Note: This directory must be mounted locally; it cannot be a remotely mounted network share.
Backup API Key	test908acc	The target access key set in the previous step (Step 2).
Backup Connection	HTTP	You can set the backup connection to HTTP or RSYNC. This example shows you the setup for using HTTP. To set up using RSYNC, see Backup Server Configuration Using RSync .

Note:

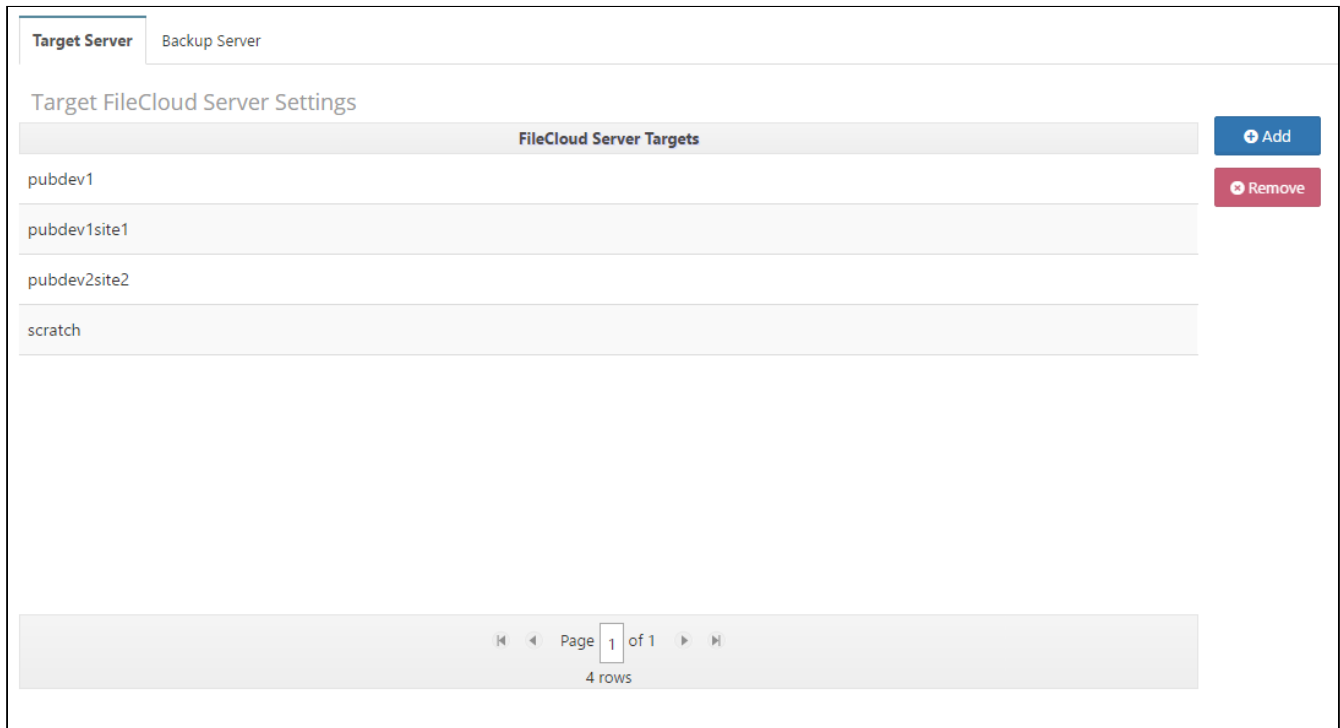
A dashboard with at least one fully configured backup target will look like this:

The screenshot displays the FileCloud Backup Server dashboard. On the left is a navigation menu with 'Home', 'Dashboard', 'Backups', 'Settings', and 'Settings'. The main content area features a header 'FileCloud Backup Server' with a subtitle 'A Backup Server For FileCloud' and a server icon. Below the header are four action cards:

- Configure Server**: 'Backup Server Config Complete' with a green checkmark and a 'Configure Backup Server Environment' button.
- Configure Target**: 'Target FileCloud Configured' with a green checkmark and a 'Configure Target FileCloud Server Server To Backup' button.
- Backup**: 'Backup FileCloud Server' with a blue download icon and a 'Create a new backup job' button.
- Restore**: 'Restore To FileCloud Server' with a blue upload icon and a 'Restore File/Folder to FileCloud Server' button.

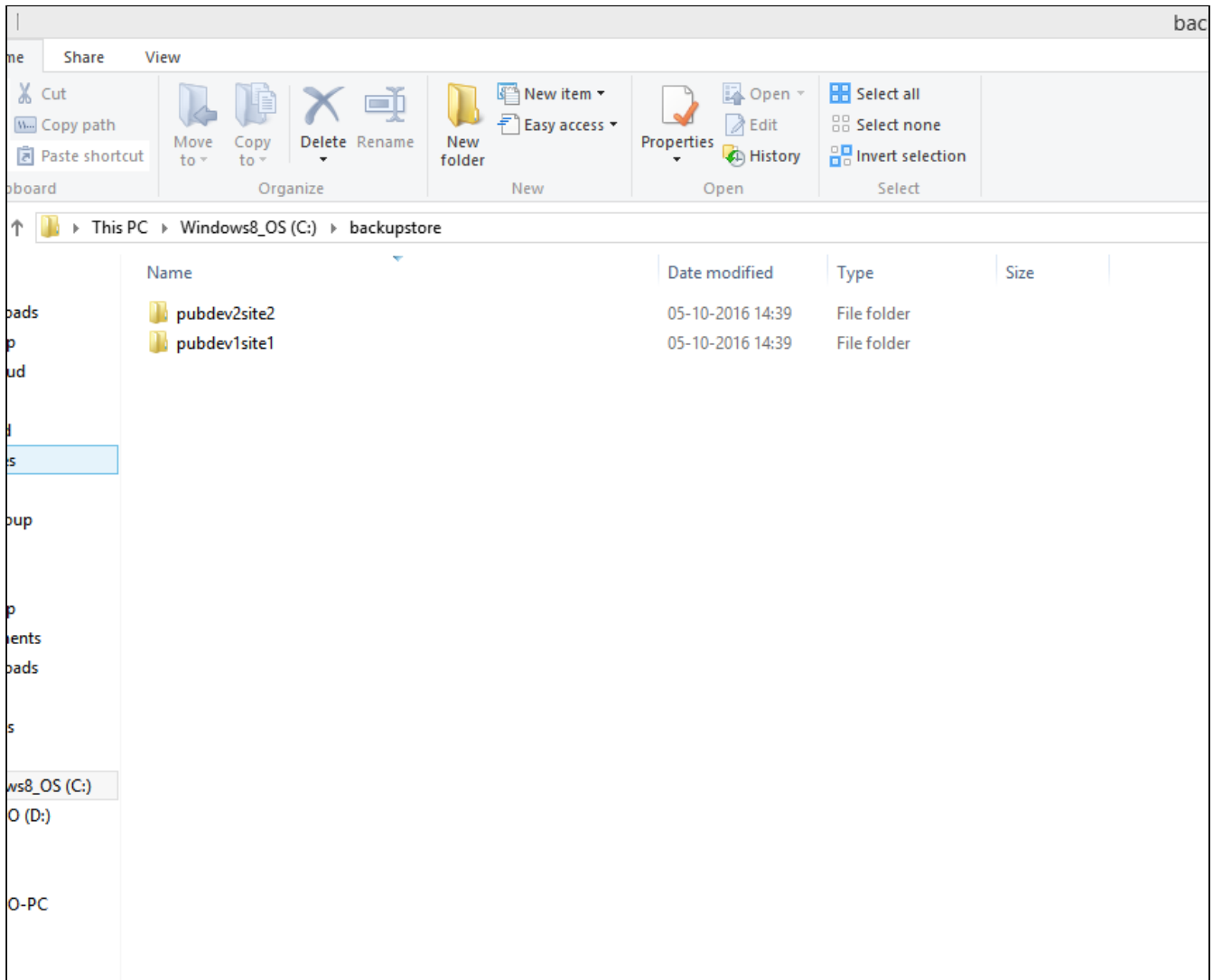
Step 4: Adding Multiple Target FileCloud Servers

Adding multiple target servers is same as adding a single server. From the 'Settings' tab, click on 'Add' button, to bring up the target server dialog. Enter all the information there and click 'Add' button. Following screenshot shows multiple target servers added to the backup server.




Multi-sites can also be added as multiple target servers which is same as adding single server.

Once the backup is done, the contents are stored separately for each multi-site backed up.



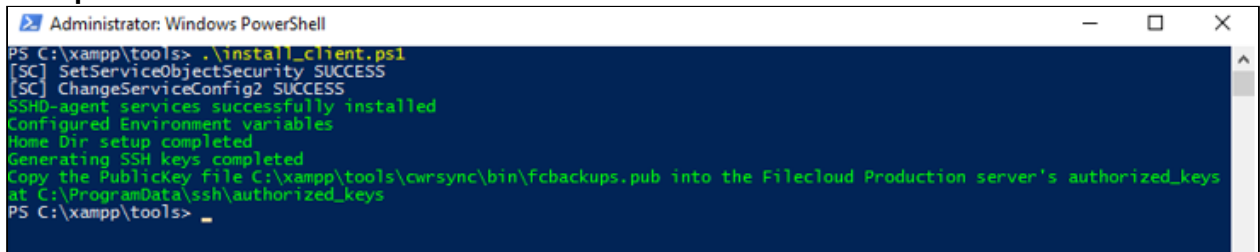
Backup Server Configuration Using RSync

 Please make sure the Filecloud Production server and the backup server are the same version.

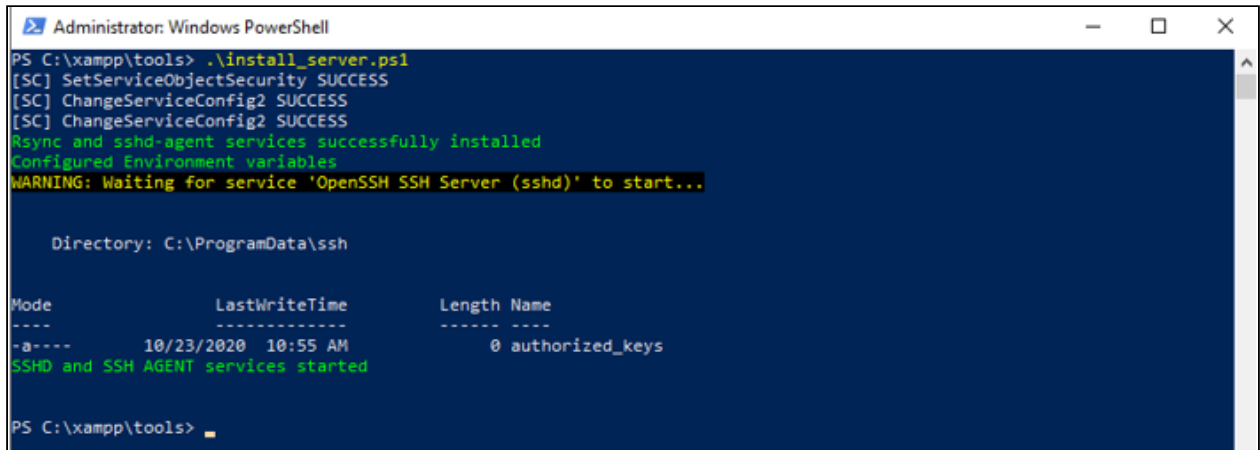
Configure the backup server using Rsync:

1. Download the Rsync tool from: <https://patch.codelathe.com/tonidocloud/live/installer/backupserver-rsync-tool-win.zip>
2. Unzip it and place it under **xampp\tools**.
3. To run the PowerShell scripts, first run the following command in PowerShell:
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass

- To install and configure the rsync and ssh binaries in the backup server and the production server, run **xampp\tools\install_client.ps1** on the backup server and **xampp\tools\install_server.ps1** on the production server:

Backup server:

```
Administrator: Windows PowerShell
PS C:\xampp\tools> .\install_client.ps1
[SC] SetServiceObjectSecurity SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
SSH-agent services successfully installed
Configured Environment variables
Home Dir setup completed
Generating SSH keys completed
Copy the PublicKey file C:\xampp\tools\cwrsync\bin\fcbackups.pub into the Filecloud Production server's authorized_keys
at C:\ProgramData\ssh\authorized_keys
PS C:\xampp\tools>
```

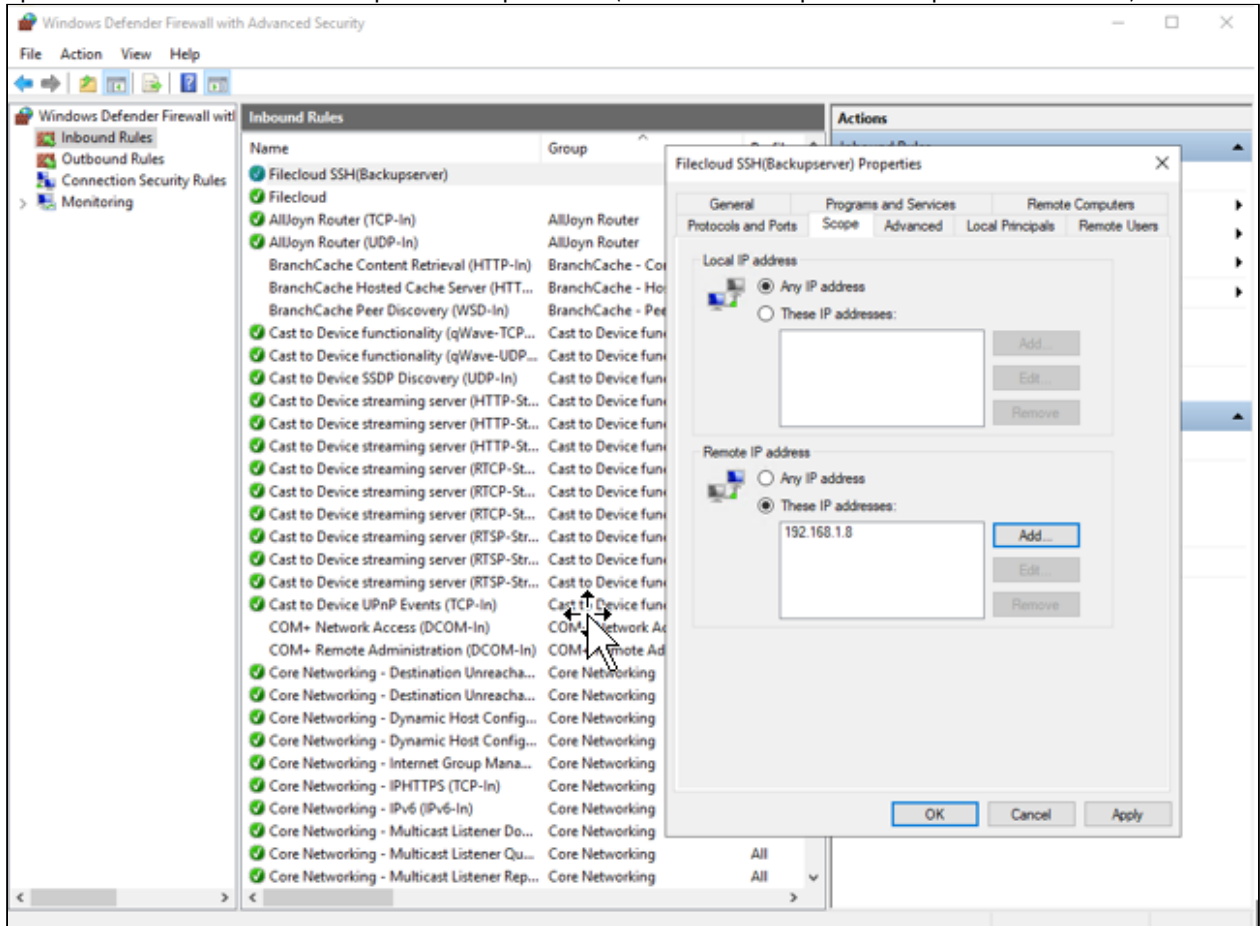
Production server:

```
Administrator: Windows PowerShell
PS C:\xampp\tools> .\install_server.ps1
[SC] SetServiceObjectSecurity SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
Rsync and sshd-agent services successfully installed
Configured Environment variables
WARNING: Waiting for service 'OpenSSH SSH Server (sshd)' to start...

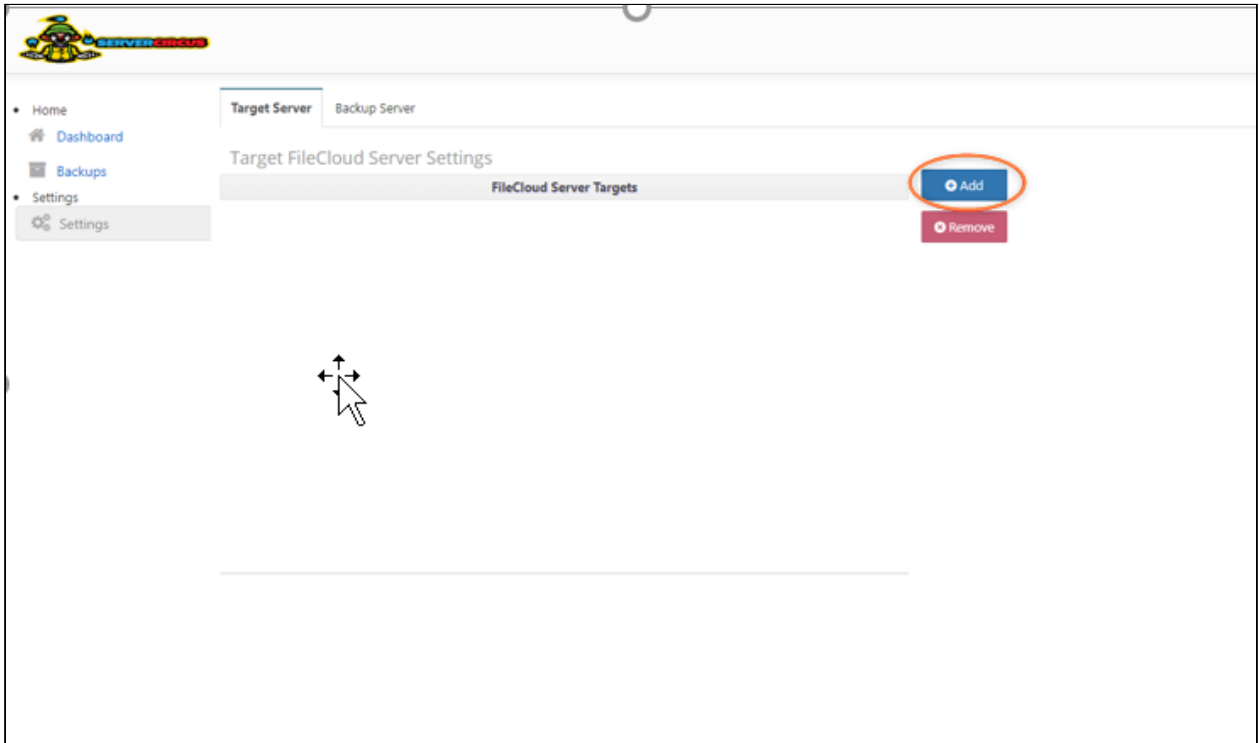
Directory: C:\ProgramData\ssh

Mode                LastWriteTime         Length Name
----                -
-a----             10/23/2020 10:55 AM              0 authorized_keys
SSH-agent and SSH AGENT services started
PS C:\xampp\tools>
```

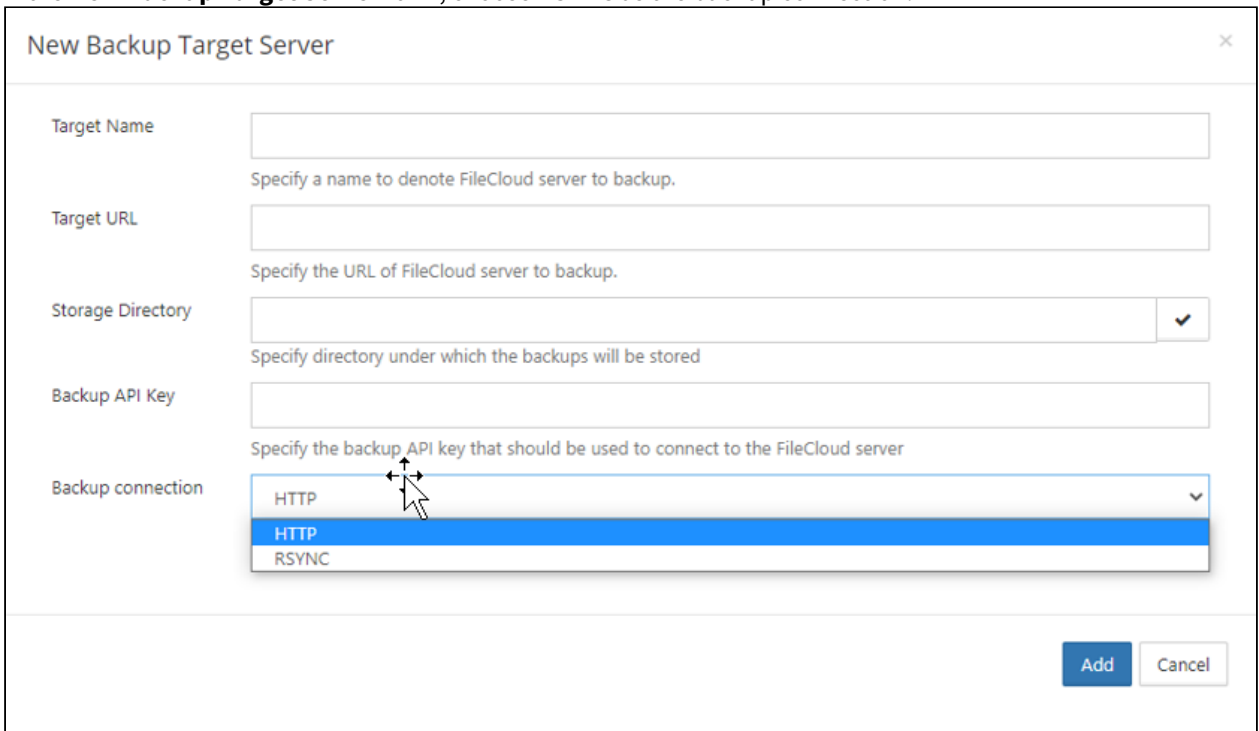
- Open firewall access to the backup server on port 2233 (the default SSH port for the production server).



- Copy the PUB key from the backup server at:
xampp\tools\cwrsync\bin\fbbackups.pub
to:
C:\ProgramData\ssh\authorized_keys
- On the production server, restart SSH services.
- Configure the target server on the backup server.
See Step 3 in [FileCloud Backup Server Configuration](#) for help navigating to the **Settings > Target Server** tab in the Backup Server user interface.



9. In the **New Backup Target Server** form, choose **RSYNC** as the backup connection:



After you choose **RSYNC**, the additional fields appear.

10. Enter the other settings.

If the Admin is an AD user, enter **DOMAIN\Administrator** for **SSH User**.

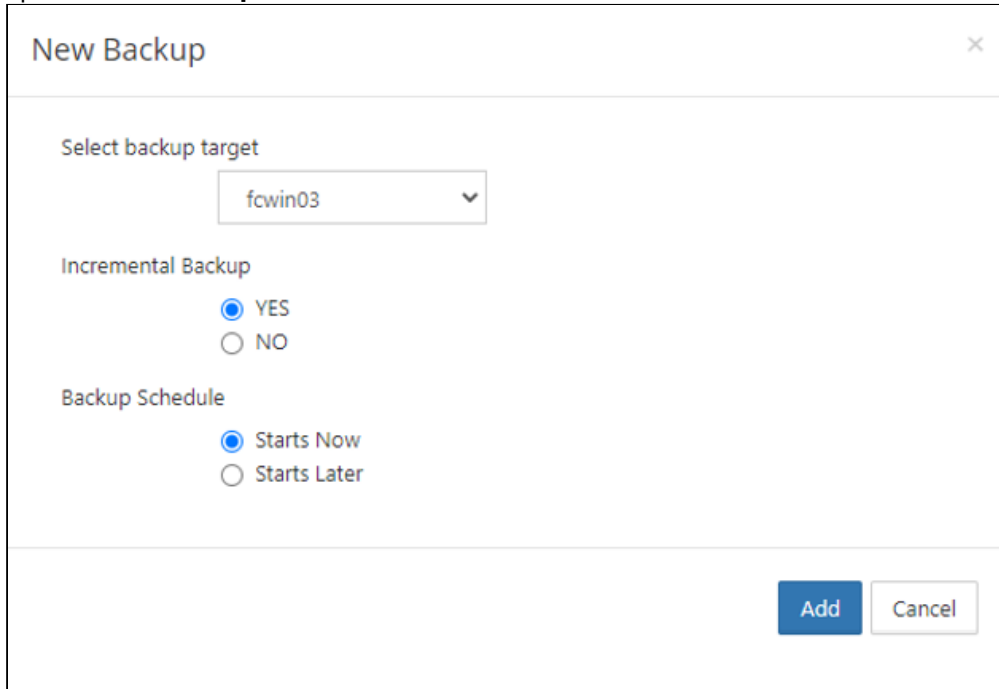
New Backup Target Server ✕

Target Name	<input type="text" value="fcwin03"/>
	<small>Specify a name to denote FileCloud server to backup.</small>
Target URL	<input type="text" value="https://fcwin03"/>
	<small>Specify the URL of FileCloud server to backup.</small>
Storage Directory	<input type="text" value="E:\Backups"/> <input checked="" type="checkbox"/>
	<small>Specify directory under which the backups will be stored</small>
Backup API Key	<input type="text" value="....."/>
	<small>Specify the backup API key that should be used to connect to the FileCloud server</small>
Backup connection	<input type="text" value="RSYNC"/> <input type="checkbox"/>
	<small>Specify the connection to use for file downloads</small>
SSH User	<input type="text" value="Administrator"/>
	<small>Specify SSH user for RSYNC connection</small>
SSH Port	<input type="text" value="2233"/>
	<small>Specify SSH port for RSYNC connection</small>
SSH Key	<input type="text" value="C:\xampp\tools\cwrsync\bin\fcbackups"/>
	<small>Specify SSH private key for RSYNC connection</small>
RSYNC Options	<input type="text"/>
	<small>Specify additional options for RSYNC command</small>

11. Click **Add**.

Run the backup for the target server

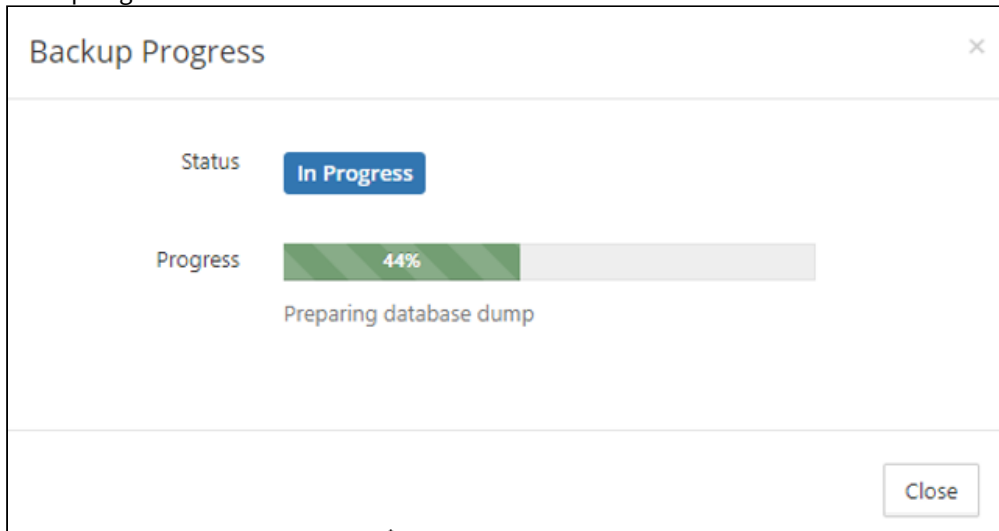
1. Open the **New Backup** screen.



The 'New Backup' dialog box contains the following elements:

- Select backup target:** A dropdown menu with 'fcwin03' selected.
- Incremental Backup:** Radio buttons for 'YES' (selected) and 'NO'.
- Backup Schedule:** Radio buttons for 'Starts Now' (selected) and 'Starts Later'.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

2. Configure the settings and click **Add**.
Backup begins:



The 'Backup Progress' dialog box displays the following information:

- Status:** A blue button labeled 'In Progress'.
- Progress:** A progress bar showing 44% completion.
- Task:** The text 'Preparing database dump' is displayed below the progress bar.
- Buttons:** A 'Close' button at the bottom right.

3. When backup is complete, review the backup details:

Created Date	Start Date	End Date	Status	Actions
23 Oct 2020 13:16	23 Oct 2020 13:16	23 Oct 2020 13:26	COMPLETED	Info Files Delete

Page 1 of 1
1 row

To install on Linux

Install the Rsync client and SSH service on the servers from the respective repositories.

In Ubuntu, enter:

```
apt-get install rsync openssh-server -y
```

In Centos enter:

```
yum -y install openssh-server openssh-clients rsync
```

Proceed from Step 5 under **Configure the backup server using RSync.**

FileCloud Backup Server Operations

Introduction

Various operations supported by the backup server is explained in the following sections.

- [Backup Server - Backup](#)
- [Backup Server - Restore Files and Folders](#)
- [Backup Server - Export](#)
- [Backup Server - Download](#)
- [Backup Server - Cron Command](#)

Backup Server - Backup



The main functionality of the backup server is to make backups of FileCloud server. Once the backup server is properly configured, it can perform manual and automatic backups.

Type Of Backups

Backup server supports two types of backup jobs:

1. Full backup
2. Incremental backup

Look below for detailed comparison of these backups.

	Full Backup	Incremental Backup
Description	Takes a complete backup of the target FileCloud server.	Backups only changed files, since the previous backup.
Space Usage	Takes the same size as the backed up FileCloud server. This includes both files and the database.	Takes only fractional space compared to full backups, as it captures only the delta changes.
Dependency	It is standalone and not dependent on any other backups.	It is not a standalone backup and dependent on the previous complete backup.
Time Taken	Takes more time, as it copies every single file from the target.	Takes less time, as it copies only changed files from the target.

Backup Schedule

Backup server supports scheduling of backup operations. There are two types of schedules:

1. Backup starting now: This schedule lets the backup operation to start immediately.
2. Backup starting later: This schedule lets the backup operation to start at a later time.

Schedule New Backup

A new backup can be scheduled by going to the "Backups" tab of backup server UI and clicking on the "New Backup" button. This brings up the "New Backup" popup, which requires the following information.

- Backup Target: The target of this backup. If there were multiple targets configured, select the target that needs to be backed up.
- Incremental Backup: Select 'Yes', if this backup has to be incremental. Note if the new backup is the first backup for the target, even selecting an incremental backup, will result in a full backup. The reason for this is that there are no existing backups available.
- Backup Schedule: Select 'Starts Now' or 'Starts Later', depending when the backup job has to be started.

New Backup ✕

Select backup target

pubdev1 ▼

Incremental Backup

YES
 NO

Backup Schedule

Starts Now
 Starts Later

Add Cancel

Monitoring Backup Progress

The progress of a backup job that is currently executing can be monitored from the web UI. If progress dialog opens automatically when a backup is scheduled to start immediately.

Backup Progress ✕

Status In Progress

Progress 22%

Requesting file list

File Progress 100%

Received files: 1498

Close

This dialog can also be opened again later by selecting the target from the drop-down and clicking on the 'Status' button of the backup job.

	Created Date	Start Date	End Date	Status	ACTIONS
	28 Aug 2016 20:00	28 Aug 2016 20:00		INPROGRESS	
	22 Jun 2016 02:32	22 Jun 2016 14:35	22 Jun 2016 14:38	COMPLETED	
	19 May 2016 20:46	19 May 2016 20:46	19 May 2016 20:50	COMPLETED	

Backup States

While monitoring backup progress, the following states may be encountered. The states of all jobs can be seen on the table under the 'Status' column.

State	Meaning
QUEUED	The backup job is scheduled to start during a later time.

State	Meaning
INPROGRESS	The backup job is currently in progress.
COMPLETED	The backup job has completed successfully.
FAILED	The backup job failed during execution. Check logs and email notifications for details in this case.
CANCELLING	A cancel request has been received for the job and it is in the process of stopping.
CANCELLED	The backup job is stopped because a cancel request.

Backup Actions

Each backup job in the 'Backup' table has a bunch of actions associated with it.

Action	Remarks
Info	The details of the backup job such as start/end dates, full/incremental backup, target, status.
Start	Starts the job. This action is available only for the jobs that are not in progress.
Status	Monitor the progress of the job. This action is available only for 'INPROGRESS' jobs.
Delete	Delete a backup job. While deleting a job, the files that are associated with this backup can be also be optionally deleted.
Cancel	Request a job cancel. This action is available only for 'INPROGRESS' jobs.

Backup Server - Restore Files and Folders



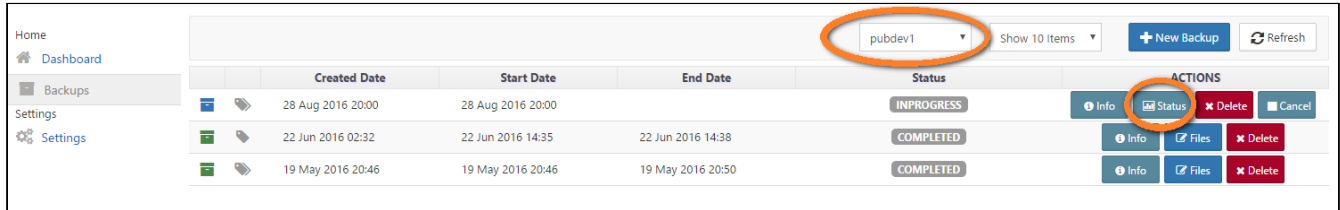
FileCloud backup server supports restoring of files/folders from the backups.

When a file/folder is selected for restore, it will be uploaded directly to its original location as found in the backup.

Note

- You can restore user files and folders using Backup Server.
- You can restore databases and the entire cloud storage path manually, using the back ups you have created.

Figure 1. Restoring a user's files.



To restore a User's files and folders:

1. Log in to the FileCloud Admin portal.
2. On the left Home panel, select Backups.
3. Select the backup you want to restore, and then click the Files button.
4. On the Files screen, select the path containing the files or folder to be restored, and then click the Restore button.
5. The selected files or folders will be sent to the restore queue. To see the queue, click the Restore Queue tab.
6. Continue adding more files or folders as necessary.
7. When all the files and folders you need to restore are added to the restore queue, click the Restore Queue tab.
8. To restore everything listed, click the Restore button.

9. You will see the progress of files and folders being restored to the FileCloud target server.

The screenshot shows a web interface titled "Backup on 22 Sep 2015 23:05". It has three tabs: "Files", "Restore Queue", and "Export Queue". The "Restore Queue" tab is active. At the top right of the queue area is a green "Restore" button. Below this is a table with the following columns: "File", "Uploaded", "Size", "Status", and "ACTIONS". A single row is visible in the table, showing a file icon, a redacted filename, a progress bar at 78% (circled in orange), a size of 20427336, a status of "In Progress", and a blue "Actions" button. At the bottom of the interface, there is a pagination control showing "Page 1 of 1" and "1 row".

Backup Server - Export

Introduction

FileCloud backup server also supports exporting of files/folders from the backups. When a file/folder is selected for export, it will be copied to a local path on the backup server.

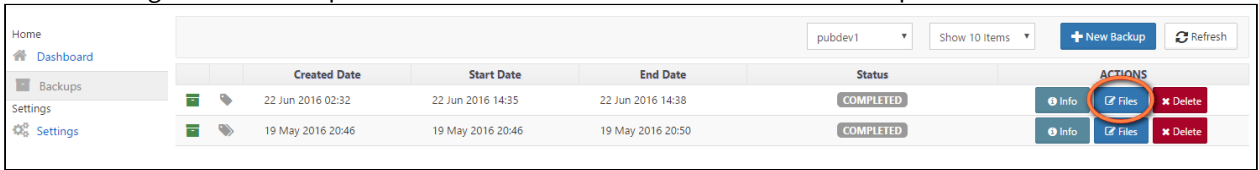
Note

- Export from backup server UI supports files and folders.
- Main difference between export and restore is that export stores the file locally on the backup server, while restore stores file directly on the target FileCloud server.
- When export is selected, the current path will be chosen as path to export.

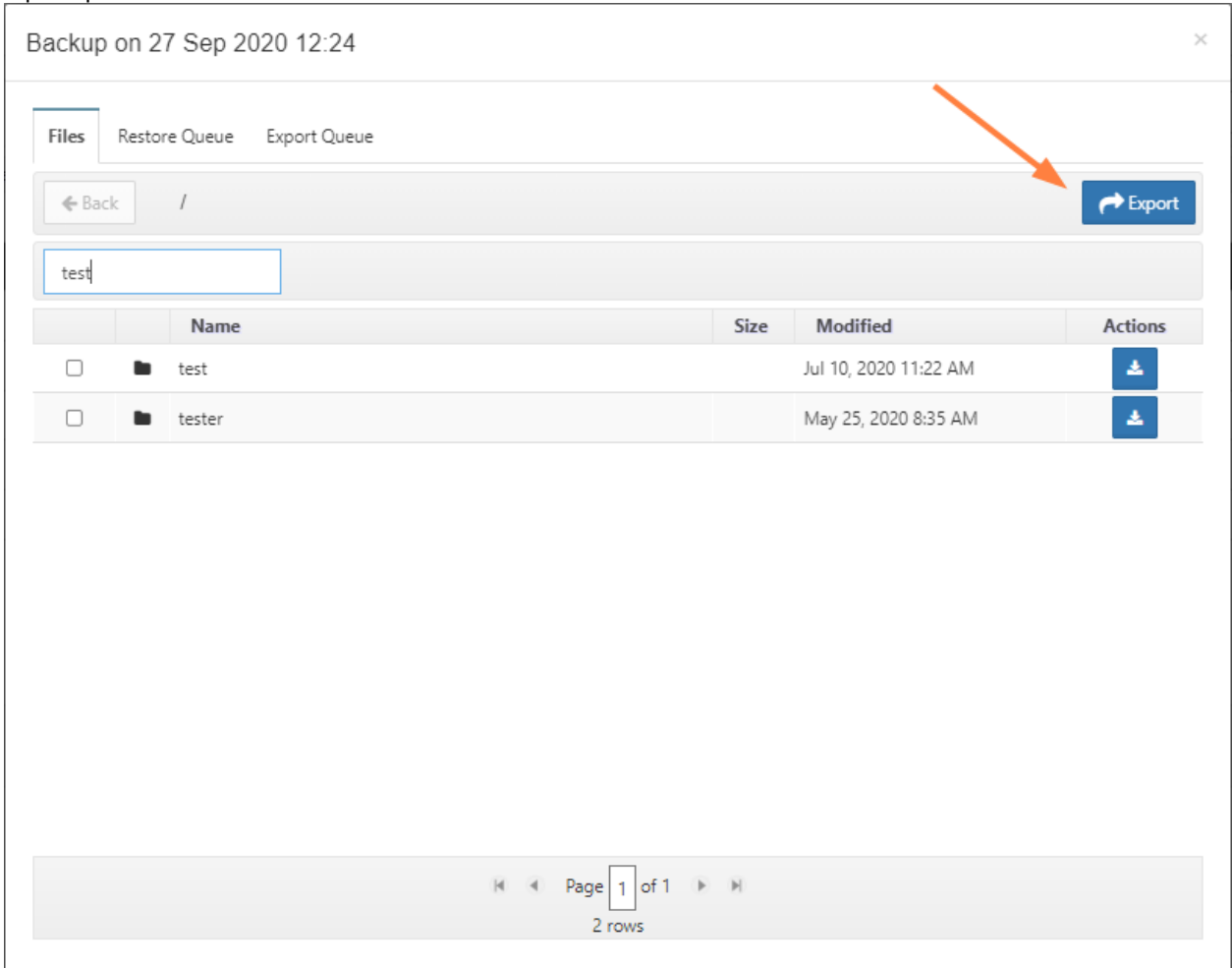
Exporting File/Folder

User file/folders can be exported with the following steps:

1. Select the backup from which the file/folder has to be exported.
2. Select the target from the drop-down and click on the 'Files' button for the backup that needs to be restored.



3. In the files dialog, navigate to the path containing the file/folder to be exported.
4. Select one or more file/folders and click on the 'Export' button. The selected file/folders will be sent to the export queue.



5. A prompt will appear to confirm the export path, select 'Yes' to continue.

Confirm ×

Add following folder to export queue?

/test

6. Next prompt will require the local path where the exported folder/file(s) are to be stored. Enter a path with write access and click on 'Export' button. This will add the export request to the queue.

Select Export Destination ×

Enter the path to export

Export To


C:\work\export

7. Continue adding more folders to export as necessary.
8. When all the folders to be restored are added to the export queue, switch to 'Export Queue' tab. Click on the 'Start' button.

Backup on 28 Oct 2015 09:54

Files Restore Queue **Export Queue**

Start

Cloud Path	Export Directory	Status	ACTION
/test	C:\work\export	In Queue	

Page 1 of 1
1 row

9. Once the export process completed, the folder will be removed from the queue.
10. Look at the local destination folder for the exported files.

Backup Server - Download

Introduction

FileCloud backup server also supports downloading of files/folders from the backups directly from the web UI. When a folder is selected for download, it will be downloaded as a zip.

Note

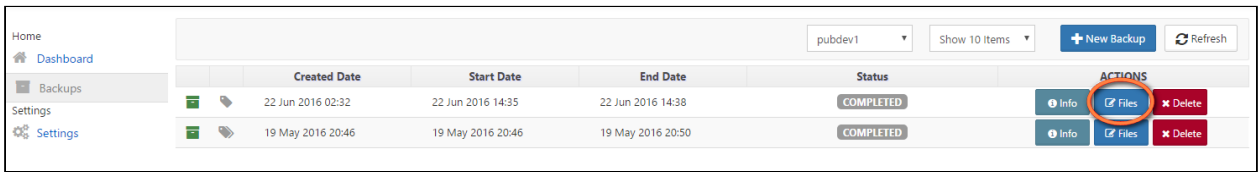
- Download of only one file or folder is supported at this time.

Downloading File/Folder

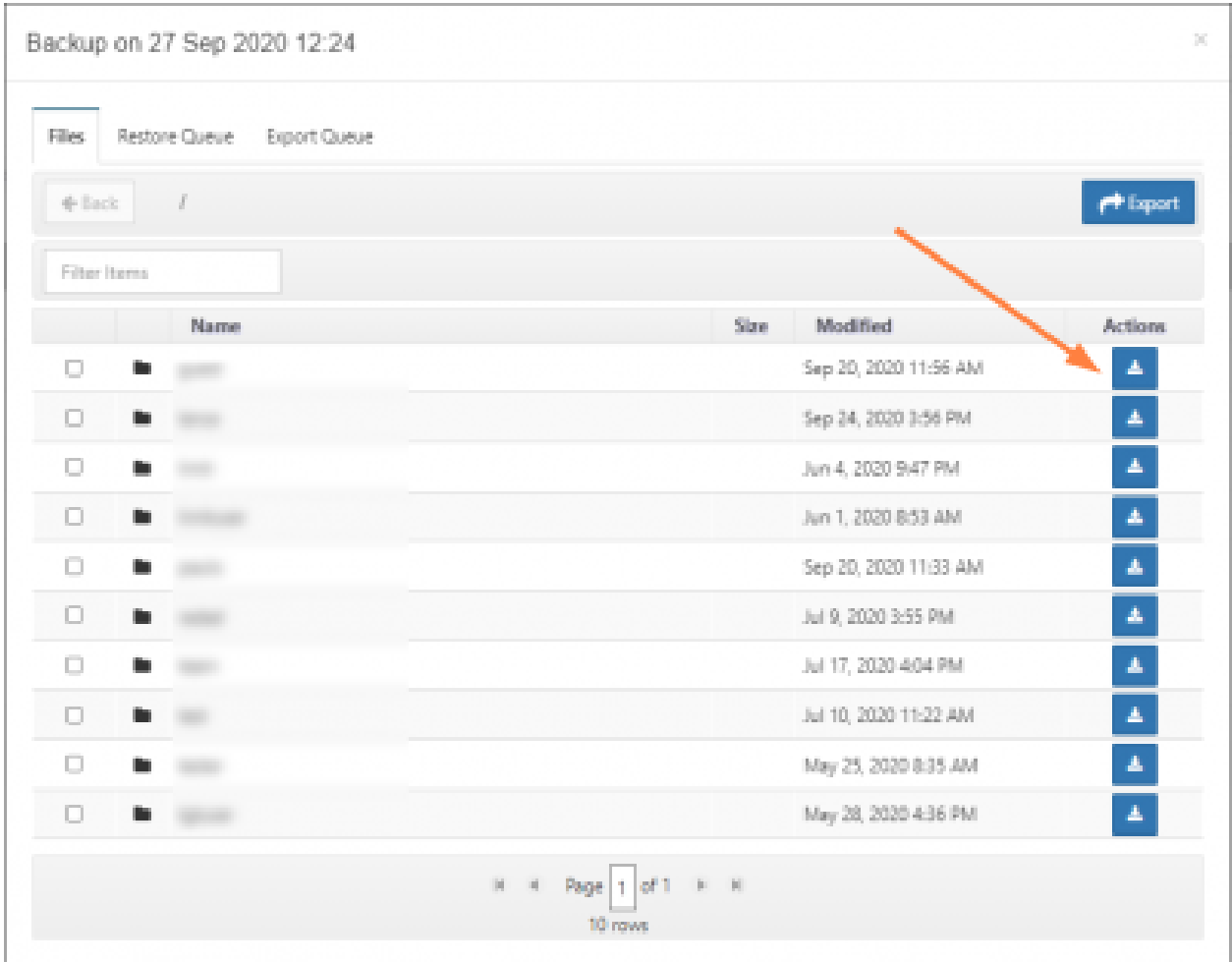
User file/folders can be downloaded using the following steps:

1. Select the backup from which the file/folder has to be restored.

2. Select the target from the drop-down and click on the 'Files' button for the backup that needs to be restored.



3. In the files dialog, navigate to the path containing the file/folder to be downloaded.
4. Select the download button for the file or folder to start the download.



Backup Server - Cron Command

Introduction

FileCloud backup server is bundled with a command line utility (starting v12.0) that can be used for automation or in OS specific cron jobs. This section shows the various options supported by the cron utility command.

Running Cron Command

Cron command can be invoked as follows:

Windows	<code>C:\xampp\htdocs\app\backupserver\> c:\xampp\php\php.exe backupcron.php</code>
Linux	<code>\$ cd /var/www/app/backupserver/ \$ php backupcron.php</code>

Create New Backup Job

To create a new backup job, but not start it, use the following command:

Command	<code>backupcron.php --command=backup <--targetid=target_db_id --targetname=target_name> --incremental=[0 1]</code>
Parameters	<p><code>--command=backup</code> specifies that a new backup job is to be created <mandatory></p> <p><code>--targetid</code> specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional></p> <p><code>--targetname</code> specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional></p> <p><code>--incremental</code> specifies whether the backup job is full or incremental. Use 0 for full or 1 for incremental. Default is 0. <optional></p> <p>Note: Though <code>--targetid</code> and <code>--targetname</code> is optional individually, one of these two should be present to uniquely identify the target.</p>

Create And Start Backup Job

To create a new backup job and start it immediately, use the following command:

Command	<code>backupcron.php --command=backupnow <--targetid=target_db_id --targetname=target_name> --incremental=[0 1]</code>
Parameters	<p><code>--command=backupnow</code> specifies that a new backup job is to be created and started <mandatory></p> <p><code>--targetid</code> specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional></p> <p><code>--targetname</code> specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional></p> <p><code>--incremental</code> specifies whether the backup job is full or incremental. Use 0 for full or 1 for incremental. Default is 0. <optional></p> <p>Note: Though <code>--targetid</code> and <code>--targetname</code> is optional individually, one of these two should be present to uniquely identify the target.</p>

List Old Backup Jobs

To get a list of backup jobs, which were completed `x` days or earlier, use the following command:

Command	<code>backupcron.php --command=listold <--targetid=target_db_id --targetname=target_name> --daysold=x</code>
Parameters	<p><code>--command=listold</code> specifies that a list of all the backup jobs completed <code>x</code> days and earlier should be returned <mandatory></p> <p><code>--targetid</code> specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional></p> <p><code>--targetname</code> specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional></p> <p><code>--daysold</code> specifies the number of days or earlier for which the list should be generated. Default is 14. <optional></p> <p>Note: Though <code>--targetid</code> and <code>--targetname</code> is optional individually, one of these two should be present to uniquely identify the target.</p>

Delete Old Backup Jobs

To delete a bunch of backup jobs, which were completed `x` days or earlier, use the following command:

Command	<code>backupcron.php --command=deleteold<--targetid=target_db_id --targetname=target_name> --daysold=x</code>
Parameters	<p><code>--command=listold</code> specifies that a list of all the backup jobs completed <code>x</code> days and earlier should be returned <mandatory></p> <p><code>--targetid</code> specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional></p> <p><code>--targetname</code> specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional></p> <p><code>--daysold</code> specifies the number of days or earlier for which the list should be generated. Default is 14. <optional></p> <p>Note: Though <code>--targetid</code> and <code>--targetname</code> is optional individually, one of these two should be present to uniquely identify the target.</p>

FileCloud Backup Server Troubleshooting

Sometimes the backup job stops before completion. The backup server logs can give more details on the reason for this failure. Following are few reasons for a backup job failure.

Unable to request a db dump. Already one in progress.

Everytime a backup job is started, the production FileCloud server creates a lock, so that it cannot be interfered by another backup job.

This error can be seen in the backup server logs if there was a backup job that failed or canceled previously and the lock is not removed.

To remove the lock, on the FileCloud server, which is to be backed up, look for the folder WWWROOT/scratch/dbdump* If there is no other backup job running currently, this directory can be removed safely and a new backup job can be started.

Skipping Large AuditDB for backup

You need to add this flag in the file backupagent.php of production server if the auditdb is too large to take backup.

```
define('BACKUPAGENT_DBS_TO_BACKUP',"tonidosettings, tonidoclouddb, tonidosyncdb, tonidostoragedb")
```

So the AuditDB will be skipped during backups.

Backing Up and Restoring Linux



You can back up and restore FileCloud Server deployments running on Linux. Having a copy of the database and the FileCloud Server site allows you to restore the site if you encounter a catastrophic failure.

What do you want to do?

- ➔ [Use the FileCloud Server Backup Tool](#)
- ➔ [Manually Create a Linux Backup to Restore](#)

FileCloud Backup and Restore - Linux Tool

Note: This utility is deprecated and will be removed in future releases. Starting with FileCloud 11.0, an easy to use FileCloud Server Backup and Restore option is available for administrators. See FileCloud Server Backup for more details

FileCloud is bundled with necessary tool to perform full backups of your cloud installation ie., both files and database.

Some of the features of these backup scripts:

- can be run at anytime manually from command line
- can be part of an automated system like cron job.
- can be run on a live cloud installation (though its safer to do backup of cloud in maintenance mode).
- can backup to local or remote linux targets.

In this section you can learn some basic tasks such as

1. Initializing backup system
2. Adding a new host to the backup system
3. Removing a target
4. Creating new backups
5. Removing existing backups
6. Listing existing backups
7. Restoring a backup

Terminologies

Here are some basic terminologies used to explain the backup tool.

Backup Target: Host where the backups are stored.

Backup Directory: Directory under which the backups are stored.

Initializing Backup Tool

Backup tool has to be initialized before it can be used to backup your cloud installation. This initialization needs to be done only once and tool will automatically initialize itself upon first use. During this initialization process, the tool performs an important routine that the user needs to be aware of.

SSH Key Generation : The tool generates a RSA ssh key pair during initialization. This key pair will be used to communicate between the tool and backup targets. This enables tool to communicate with the backup target without prompting for password every time. These are encrypted keys and are safer than entering passwords everytime for communication. Also the tool exchanges the key with the localhost and will be used to run even commands on the local host.

When the backup tool is run without any options, it initializes the tool on first run and then displays help. Further runs only displays help. Following section shows a session initializing the backup tool.

Initializing backup tool

```
madhan@li111-150:~$ cd /var/www/resources/backup
madhan@li111-150:/var/www/resources/backup$ sudo chmod +x backup.sh
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh
Feb 18 01:26:05 : Initializing backup system
Feb 18 01:26:05 : Generating ssh encryption keys
Generating public/private rsa key pair.
Your identification has been saved in ./keys/id_rsa.
```

```

Your public key has been saved in ./keys/id_rsa.pub.
The key fingerprint is:
f4:cd:e8:ff:1e:db:e6:b4:7f:f7:da:d4:02:16:dd:ba root@li111-150
The key's randomart image is:
+--[ RSA 2048]-----+
| |
| . . |
| . . . .|
| . . + . . |
| S o = . |
| . . . .|
| . E +|
| . 0=|
| .o==@|
+-----+
Feb 18 01:26:06 : Please enter local user to store backups :
madhan
Feb 18 01:26:22 : Exchanging ssh keys with host 127.0.0.1
madhan@127.0.0.1's password:
Feb 18 01:26:30 : Successfully initialized localhost to store backups
Script to backup tonidocloud data
Usage :
sudo /path/backup.sh <command>
where <command> could be on of the following:
    addtgt <user> <host> <tgtdir> - Adds the <tgtdir> in machine <user>@<host> as a
valid backup directory
    rmtgt <index> - Removes the backup target at specified index.
                    If index parameter is missing, a list of available targets will be
shown to choose one from.
    lstgts - Lists available backup directories
    crtbackup <index> - Create a new backup of tonidocloud at specified backup
target index.
                    If index parameter is missing, a list of available targets will be
shown to choose one from.
    lstbkups <index> - List all backups under the specified target index.
                    If index parameter is missing, a list of available targets will be
shown to choose one from.
    rmbkup <index1> <index2> - Removes index2 directory from index1 backup target.
                    If index parameters is missing, a lists of available targets and
directories will be shown to choose one from.
    resbkup <index1> <index2> - Restores index2 directory from index1 backup target.
                    If index parameters is missing, a lists of available targets and
directories will be shown to choose one from.

```

Add Backup Target

The backup tool has to have atleast one backup target before it can create and store backups. Even if you plan to store the backups on the local system, you still need to the local host as a backup target. When multiple backup target directories are added to the tool, the ssh keys are exchanged only the first time.

To add a backup target you need

- a user
- ip address of the remote host.
- a directory to store backups (and the above user should have write permissions)

Use the option `addtgt` to add a new backup target to the tool. The following snippet shows commands to add 2 backup targets.

Local host (madhan, 127.0.0.1, /backup)

Adding a localhost target

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh addtgt madhan 127.0.0.1 /
cloudbackup/
Feb 18 02:20:23 : Adding backup target : madhan@127.0.0.1:/cloudbackup/
Feb 18 02:20:25 : Added backup target : madhan@127.0.0.1:/cloudbackup
```

Remote host (cloud, 192.168.1.148, /backup)

Adding a remote host target

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh addtgt cloud
192.168.1.148 /cloudbackup/
Feb 17 18:31:47 : Adding backup target : cloud@192.168.1.148:/cloudbackup/
Feb 17 18:31:47 : Exchanging ssh keys with host 192.168.1.148
cloud@192.168.1.148's password:
Feb 17 18:31:51 : Added backup target : cloud@192.168.1.148:/cloudbackup
```

Remove Backup Target

To remove a backup target use the option `rmtgt`. This option lists the available backup targets and prompts for the target to be deleted. Upon entering the target number, the tool deletes the target. When a target is deleted, the tool just removes pointer to the target from its internal list. The physical directory is not deleted. This allows admins to add the same target at later point of time with all the backups intact.

Note: The target number can also be specified from the command line

Removing a target

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh rmtgt
No Targets
-----
0) madhan@127.0.0.1:/cloudbackup
1) cloud@192.168.1.148:/cloudbackup
-----
```

```
Feb 17 18:41:20 : Select a backup target to remove from the above list :
1
Feb 17 18:41:37 : Selected backup target cloud@192.168.1.148:/cloudbackup
Feb 17 18:41:37 : Backup target removed : cloud@192.168.1.148:/cloudbackup
```

List Backup Targets

To list the available backup targets in the tool use the option `lstgts`.

Listing targets

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh lstgts
No Targets
-----
0) madhan@127.0.0.1:/cloudbackup
-----
```

Create New Backup

To create a new backup use the option `crtbkup`.

Create Backup

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh crtbkup
Feb 18 03:22:19 : Creating backup
No Targets
-----
0) madhan@127.0.0.1:/cloudbackup
-----
Select a backup target from the above list : 0
Feb 18 03:22:21 : Selected backup target madhan@127.0.0.1:/cloudbackup
sending incremental file list
5108a8b6bff4d/
5108a8b6bff4d/5108a8b6c26d2/
5108a8b6bff4d/5108a8b6c26d2/510d2ecb07217.dat
 42.55K 100% 9.33MB/s 0:00:00 (xfer#1, to-check=54/57)
5108a8b6bff4d/5108a8b6c26d2/510d2ecb08d48.dat

.....

5108a8b6bff4d/5108a8b6c26d2/51132eeb6a45a.dat
 174.84K 100% 241.84kB/s 0:00:00 (xfer#55, to-check=0/57)

sent 60.89M bytes received 1.06K bytes 24.36M bytes/sec
total size is 60.88M speedup is 1.00
```

```
tonidobak.log 100% 20KB 19.8KB/s 00:00
```

Note: The target number can also be specified from the command line.

List Backups

To list backups available on a particular backup target directory use the option `lstbkups`.

Listing Backups

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh lstbkups
No Targets
-----
0) madhan@127.0.0.1:/cloudbackup
-----
Feb 18 03:26:39 : Select a target from above to list available backups :
0
Feb 18 03:27:03 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No      Date          Files      Size      Status
  Path
-----
0)      03:22:21 2013-02-18      59M      44
COMPLETE      /cloudbackup/1361157741
-----
```

Note: The target number can also be specified from the command line.

Delete Backup

To delete a backup target directory use the option `rmbkup`.

Deleting Backups

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh rmbkup
No Targets
-----
0) madhan@127.0.0.1:/cloudbackup
-----
Feb 18 03:31:25 : Select a target from above to list available backups
0
Feb 18 03:31:28 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No      Date          Files      Size      Status
  Path
-----
```



```

-----
0)          03:22:21 2013-02-18          59M          44
COMPLETE          /cloudbackup/1361157741
-----

Feb 18 03:31:30 : Select a backup directory
0
Feb 18 03:31:34 : Selected backup path /cloudbackup/1361157741
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh lstbkups 0
Feb 18 03:32:01 : Selected backup target madhan@127.0.0.1:/cloudbackup

  No          Date          Files          Size          Status
Path
-----
-----
-----

```

Note: The backup target number and backup target directory number can also be specified from the command line.

Restore Backup

To restore a backup from a particular backup target directory use the option resbkup.

Note: When a backup is restored, the cloud service will be stopped to restore the backup. Upon restoring the snapshot the service will be started again.

Restoring Backups

```

madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh resbkup
  No          Targets
-----

0)          madhan@127.0.0.1:/cloudbackup
-----

Feb 18 03:42:00 : Select a target from above to list available backups
0
Feb 18 03:42:05 : Selected backup target madhan@127.0.0.1:/cloudbackup

  No          Date          Files          Size          Status
Path
-----

0)          03:40:16 2013-02-18          59M          44
COMPLETE          /cloudbackup/1361158816
-----

Feb 18 03:42:07 : Select a backup directory
0
Feb 18 03:42:15 : Selected backup path /cloudbackup/1361158816
Rather than invoking init scripts through /etc/init.d, use the service(8)

```

utility, e.g. `service mongodb stop`

Since the script you are attempting to invoke has been converted to an Upstart job, you may also use the `stop(8)` utility, e.g. `stop mongodb mongodb stop/waiting`

Rather than invoking init scripts through `/etc/init.d`, use the `service(8)` utility, e.g. `service mongodb start`

Since the script you are attempting to invoke has been converted to an Upstart job, you may also use the `start(8)` utility, e.g. `start mongodb mongodb start/running, process 17363`

Note: The backup target number and backup target directory number can also be specified from the command line.

FileCloud Backup and Restore - Linux Manual

FileCloud can be backed up and restored on Linux following these manual steps.

While performing the backup/restore, these are the important file categories that should be backed up/restored:

- cloud cloud files.
- cloud database.
- cloud user files.

Backup

High level steps to backup FileCloud in windows:

1. Stop webserver
2. Backup configuration files
3. Backup database.
4. Backup user files.
5. Start webserver

Stop Webserver and MongoDB

Before backup is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress.

Stopping services

```
# sudo /etc/init.d/apache2 stop
# sudo /etc/init.d/mongodb stop
```

Please use equivalent commands applicable for your OS distro.

Backup FileCloud installation

Once the apache server is stopped, make a copy of entire cloud installation. The cloud installation is typically under `/var/www/` directory.

Backing up FileCloud installation

```
# mkdir -p /filecloudbackup/www
# sudo cp -prv /var/www/. /filecloudbackup/www
```

If your installation uses a different directory, update the above commands accordingly.

Backup database

Once the mongod is stopped, backup the database files.

Backing up FileCloud database.

```
# mkdir -p /filecloudbackup/db
# sudo cp -prv /var/lib/mongodb/. /filecloudbackup/db
```

Check your mongod installation to make sure /var/lib/mongodb is the correct database path.

Backup user files

To backup user files, make a copy of the entire directory specified for the managed storage settings, in the "Storage Path". This is found in Settings->Storage tab in the FileCloud Admin panel.

Note: In the following case, the entire "/opt/filecloud/data" directory has to be backed up.

Use the following commands, to backup user files.

Backing up user data files

```
# mkdir -p /filecloudbackup/userdata
# sudo cp -prv /opt/filecloud/data/. /filecloudbackup/userdata
```

Start Webserver and MongoDB

After the above backup steps are performed, start the apache webserver and mongo db processes.

Starting services

```
# sudo /etc/init.d/mongodb start
# sudo /etc/init.d/apache2 start
```

Please use equivalent commands applicable for your OS distro.

Restore

High level steps to restore FileCloud in windows:

1. Stop webserver
2. Restore configuration files
3. Restore database.
4. Restore user files.
5. Start webserver

Stop Webserver and MongoDB

Before restore is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress.

Stopping services

```
# sudo /etc/init.d/apache2 stop
# sudo /etc/init.d/mongodb stop
```

Please use equivalent commands applicable for your OS distro.

Restore FileCloud installation

Restore the FileCloud installation files using the following command.

Note: Check your apache installation to ensure `/var/www/` is the document root directory.

Restoring FileCloud installation

```
# sudo cp -dprv /filecloudbackup/www/. /var/www/
```

Restore database

Restore the database using the following command.

Note: Check your mongodb installation to ensure `/var/lib/mongodb` is the database path.

Restoring FileCloud installation

```
# sudo cp -dprv /filecloudbackup/db/. /var/lib/mongodb/
```

Restore user files

To restore user files, restore the user files to the directory specified and then make sure that path is set correctly in Managed Storage Settings in "Storage Path".

Note: In the following case, the entire "/opt/filecloud/data" directory has to be restored.

Use the following commands, to restore user files.

Backing up user data files

```
# sudo cp -dprv /filecloudbackup/userdata/. /opt/filecloud/data
```

Check your mongodb installation to make sure /var/lib/mongodb is the correct database path.

Start Webserver and MongoDB


After the above restore steps are performed, start the apache webserver and mongodb process.

Starting services

```
# sudo /etc/init.d/mongodb start
# sudo /etc/init.d/apache2 start
```

Please use equivalent commands applicable for your OS distro.

FileCloud Backup and Restore - Windows Manual

 Starting with FileCloud 11.0, an easy to use FileCloud Server Backup and Restore option is available for administrators. See [The FileCloud Server Backup Tool](#) for more details

FileCloud can be backed up and restored on windows following these manual steps.

While performing the backup/restore, these are the important file categories that should be backed up/restored:

- cloud cloud files.
- cloud database.
- cloud user files.

Backup

High level steps to backup FileCloud in windows:

1. Stop webserver
2. Backup configuration files
3. Backup database.

4. Backup user files.
5. Start webserver

Stop Webserver and MongoDB

Before backup is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress. To stop the apache webserver, open the FileCloud control panel and hit stop for Apache. Also stop the Mongo DB process.

Backup cloud files

Once the apache server is stopped, make a copy of entire cloud installation. The cloud installation can be found under the installation directory under htdocs. (e.g. c:\xampp\htdocs)

Backup database

To backup the database, copy the mongodb database files under c:\xampp\mongodb\bin\data

Backup user files

To backup user files, make a copy of the entire directory specified in the "Storage Path" in Managed Storage Settings (Admin Panel->Settings->Storage Tab)

Note: In the following case, the entire "c:\Filecloud\userdata\" directory has to be backed up..

Start Webserver and MongoDB

After the above backup steps are performed, start the apache webserver and mongo db processes.

Restore

High level steps to restore FileCloud in windows:

1. Stop webserver
2. Restore configuration files
3. Restore database.
4. Restore user files.
5. Start webserver

Stop Webserver and MongoDB

Before restore is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the restore is in progress.

Restore cloud files

Once the apache server is stopped, restore copy of entire cloud installation files to <cloud_install_dir>. (c:\xampp\htdocs)

Restore database

To restore the database, copy the mongodb files into the mongodb data directory. (c:\xampp\mongodb\data)

Restore user files

To restore user files, restore the user files to the directory specified in the Storage Path specified in the Managed Storage Settings. (Admin Panel->Settings->Storage Tab)

Note: In the following case, the user files had to be copied to "c:\FileCloud\userdata\".

Start Webserver and MongoDB

After the above restore steps are performed, start the apache webserver and mongodb process.

Migrating FileCloud Server to Another Server

Use the following instructions to migrate an existing FileCloud Server to another physical or virtual server.

1. [Install the latest FileCloud Server](#) on the new server.
Do not start any services after successful installation; only the database should be running.
2. Stop Apache, cron and the message queue (fcorchestrator) services in the source system to prevent user access and changes:

OS	
Linux	<p>Ubuntu:</p> <pre>systemctl stop apache2 systemctl stop cron systemctl stop fcorchestrator</pre> <p>RedHat:</p> <pre>service stop httpd service stop crond service stop fcorchestrator</pre>

OS

Windows

Use the FileCloud Control Panel to stop the above-mentioned services as indicated in the screenshot:

FileCloud Control Panel

FileCloud Control Panel
v: 23.1.0.22597, Base Components: 23.1.0.22597
Webserver Ports: 80,443 Database Port: 27017

Initial Setup: [Install Check](#)

Web Portal: [Admin Portal](#) [User Website](#)

Servers

Webserver:	Running SVC	Start	Stop	Config	Make Service
Database:	Running	Start	Stop	Config	Make Service
Cron Task:	Running SVC	Start	Stop	Config	Install
Message Queue:	Running SVC	Start	Stop	Config	Install

Optional

Push Service:	Running SVC	Start	Stop	Install	Config
FileCloud Helper:	Running SVC	Start	Stop	Install	Config
Memcache:	Running SVC	Start	Stop	Make Service	
Document Preview:	Running SVC	Start	Stop	Install	
Content Search:	Running SVC	Start	Stop	Install	

Miscellaneous

Configuration: [Application Folder](#) [Reset Admin Password](#)

SSL: [Create SSL CSR](#) [Install SSL Cert](#)

Technical Support

Need Help? [Documentation](#) [Contact Support](#) [Demo and Training](#)

3. Create a database dump on the source system.

OS	
Linux	<code>mongodump --out /tmp/mongodump</code>
Windows	<code>cd C:\xampp\mongodb\bin</code> <code>mongodump --out C:\mongodump</code>

4. Copy the database dump to the new system and restore it.

OS	
Linux	<code>mongorestore --noIndexRestore --drop /tmp/mongodump</code>
Windows	<code>cd C:\xampp\mongodb\bin</code> <code>mongorestore --noIndexRestore --drop C:\mongodump</code>

5. Copy the managed storage files to the new server.
Some common scenarios are shown below.

Info

Managed storage files : Files stored in the storage path specified in the Managed Storage settings. (Admin Panel->Settings->Storage Tab).

Scenario 1: When using an SMB/NFS/CIFS share as managed storage:

- If the SMB/NFS/CIFS share is accessible through the network from the new FileCloud Server, then no action is needed at FileCloud application level.
- If the SMB/NFS/CIFS share is not accessible from the new FileCloud Server, then either:
 - Allow this access.
 - or
 - Deploy a new SMB/NFS/CIFS share that is accessible from the new FileCloud Server to an Apache user with the correct permissions. Then copy the data from the existing SMB/NFS/CIFS share to the new one.

Scenario 2: When using local disk (HDD/SSD) as managed storage

- a. Create a new disk partition on the new FileCloud Server, and assign the same drive letter from the existing FileCloud Server.
- b. Copy the data from the existing HDD/SSD disk to the new FileCloud Server HDD/SSD.

Scenario 3: When using S3 storage as managed storage

- a. No action is needed since the S3 configuration/setting is available in the MongoDB dump.
- b. Copy all FileCloud configuration files from the below paths to the new server.

OS	
Linux	Ubuntu: /var/www/html/config RedHat: /var/www/html/config
Windows	C:\xampp\htdocs\config

- c. Start all services on the new FileCloud Server.
 - d. Log in to the admin portal, and update the managed storage path (**Settings > Storage > Storage Path**). Click **Check Path** to ensure that the path is accessible/writable.
Note: This step is only necessary if the directories are different in the old and the new system.
 - e. If [Auto Archive Audit Database](#) is enabled, in the admin portal, go to **Settings > Admin**, then enter a storage path in **Storage Path For Archived Audit Records**, and click **Check Path** to confirm that the path exists and is writable.
Note: This step is only necessary if the directories are different in the old and the new system.
Note: Steps 4 and 5 must be done for each tenant in a multi-tenant system.
 - f. [Install SSL certificates](#) on the new FileCloud Server.
6. If you are using RHEL OS, check if SELinux is in enforcing mode.
To know the current SELinux mode, enter:

```
getenforce
```

If SELinux is in enforcing mode, you may have issues accessing the FileCloud admin portal and user portal unless you disable SELinux, using the following command or follow the steps listed in [SELinux Policies For FileCloud Installation](#).

To disable SELinux, enter:

```
setenforce 0
```

Note: Changes made with **setenforce** are lost when you restart the system. To permanently change the SELinux mode, edit the **/etc/selinux/config** file and restart the system.

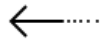
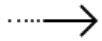
7. If you have added custom settings to any of the the configuration files under **c:/xampp/htdocs/config** or **/var/www/html/config**, copy those files to the new server.
8. If you use storage encryption, after migration:
 - a. Confirm that **Memcache** is running.
 - b. In the admin portal go to **Settings > Storage > My Files** and reactivate encryption in the new server using same password.
To set up encryption, see [Setting up Managed Storage Encryption](#) or [Setting up Managed S3 Storage Encryption](#).

Migrating a FileCloud Server Site



You can transfer files easily to a FileCloud Server site that is running.

What do you want to do?



Transfer a FileCloud Server site from one OS to another

Enabling the Backup Server URL

By default, the backup server URL is disabled. You must add a setting to both the backup server config file and the production server config file to enable it and access it as a site.

To enable the backup server URL:

1. In your production server's FileCloud directory, open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add the following:

```
define("TONIDOCLOUD_ENABLE_BACKUPSERVER_APP", true);
```

3. Repeat steps 1 and 2 in your backup server's FileCloud directory.

Monitoring FileCloud

i The ability to receive email notification when a MongoDB error occurs is available in FileCloud version 18.2 and later.

! For security purposes, to initially access the API, you must now change the default API key. If you do not change it, when you enter a command to call the API, an error is returned.
Note: You are only required to change the default API key initially; after that, you can continue to use the new key you entered.

Administrators can use tools provided by FileCloud Server to review current statistics and monitor MongoDB.

- [Get stats using an HTTP REST API](#). This is useful for integration with external monitoring systems like Nagios.
- [Review email notifications about MongoDB errors](#). This is useful for preventing loss of data. For example, if you have a High Availability (HA) deployment, and one day after a VMs in the cluster dies you discover that the master MongoDB node replication failed weeks ago, then you would not be able to recover all of your data.

What do you want to do?

Get Current Statistics

API URL

```
https://<SiteAddress>/admin/?op=getstats&apikey=yourpassword
```

RETURNED XML DATA

```
<stats>
<stat>
<totalusers>55</totalusers>
<fullaccessusers>25</fullaccessusers>
<guestaccessusers>27</guestaccessusers>
<totalsize>87.5 GB</totalsize>
<totalsizeused>2.45 GB</totalsizeused>
<totalsizefree>85.05 GB</totalsizefree>
<totalsizeusedraw>2632858720</totalsizeusedraw>
<groupscount>19</groupscount>
<externalscount>10</externalscount>
<scratchuseddisk>19.69 GB</scratchuseddisk>
<scratchfreedisk>9.52 GB</scratchfreedisk>
<scratchsize>375.25 MB</scratchsize>
<sharescount>73</sharescount>
<localstoragefreedisk>9.52 GB</localstoragefreedisk>
```

```


<totalmanagedfiles>1190</totalmanagedfiles>
<totaldevicescount>45</totaldevicescount>
<totalauditrecords>7260</totalauditrecords>
<totalvalidmanagedfiles>818</totalvalidmanagedfiles>
<totalsyncfiles>822</totalsyncfiles>
<totalvalidmanagedfolders>178</totalvalidmanagedfolders>
<totalsyncfolders>171</totalsyncfolders>
<totalalerts>0</totalalerts>
</stat>
</stats>

```

The XML can be parsed to graph various values and to trigger various actions.

Monitor MongoDB

In FileCloud Server version 18.2 and later, you will automatically receive an email notification on MongoDB cluster failure status.

 Please note that when MongoDB fails, then nothing will respond through FileCloud including the FileCloud cron jobs.

Therefore, the mongo health monitor must be running separately from and independent of FileCloud's cron jobs.

To run MongoHealth:

1. In FileCloud Server version 18.2 and later, FileCloud includes a `mongohealth` folder in the following location:

```
/server/resources/tools
```

2. The email address that is sent the notification (TO) is configured by the following variable:

```
TONIDO_CLOUD_REPLY_TO_EMAIL
```

3. Add the `/server/resources/tools/index.php` to the cron directly.

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: unrouteable domain: s.com	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed SMTP Error: The following recipients failed: test@gmail.cz: unrouteable 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: unrouteable domain: test2.com	i
2018-Jan-16 05:50 AM	Warning	Email Send Failed You must provide at least one recipient email address.	i

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

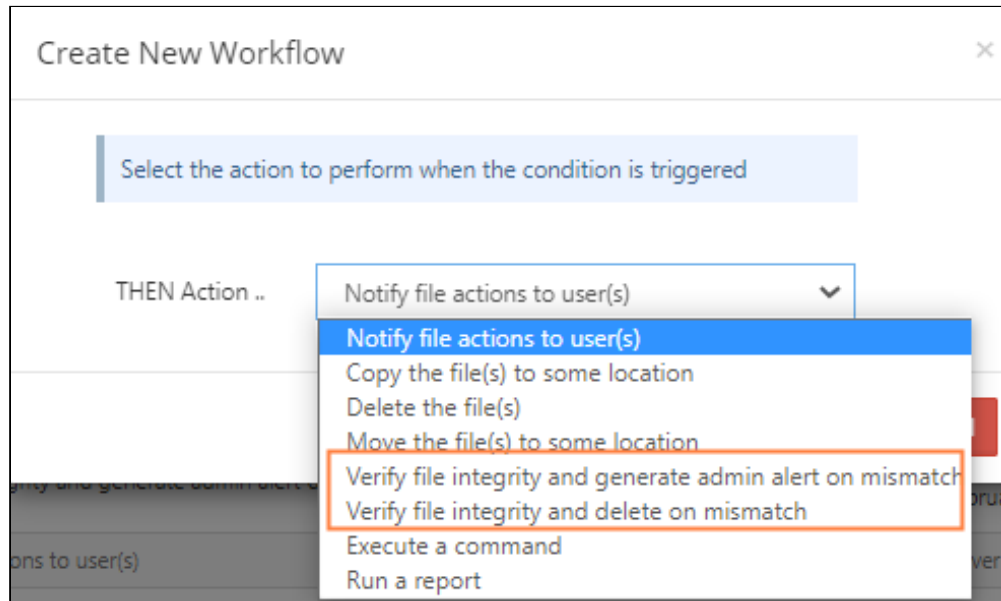
use_regex (optional): specifies whether path has a regex format

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

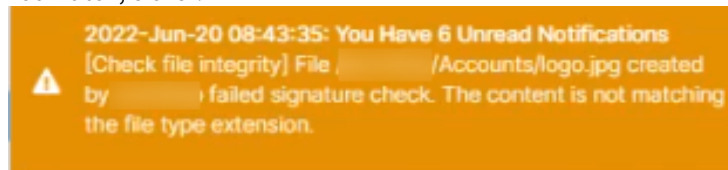
```
{
  "parent_folder_path_string": "/userid/somepath",
  "use_regex": "1",
  "exclude": "1"
}
```

← Previous
→ Next
✕ Cancel

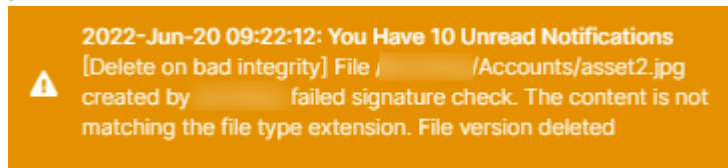
6. Click **Next**.
You are prompted to choose an action.
7. Choose one of the **Verify file integrity** actions depending on what you want the system to do when a mismatch is detected. The possible actions are:
- **Verify file integrity and generate admin alert on mismatch**: Detects the mismatch and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

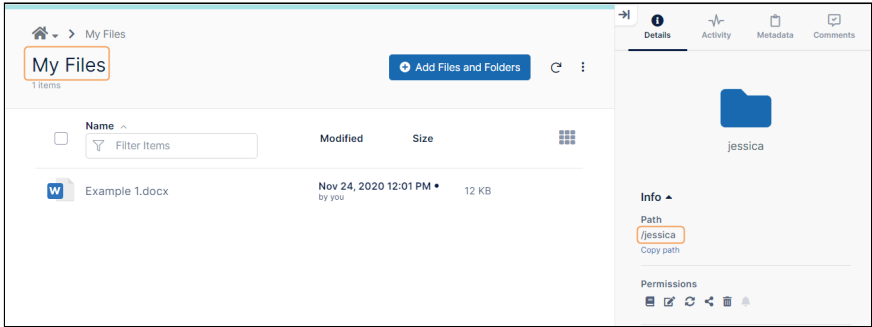
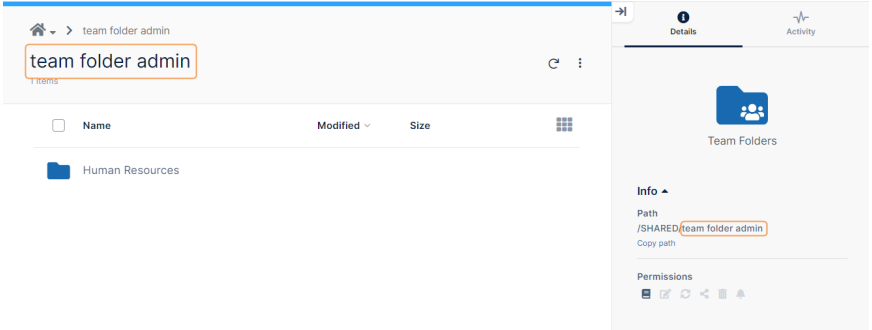
Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
Check file integrity	If a file is created	Verify file integrity and generate admin alert on mismatch	Never	Never	<input checked="" type="checkbox"/>	▶ ⏸ ✎ ↺ ✕
Inactive Files	If file was not modified for specified days	Notify file 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**.

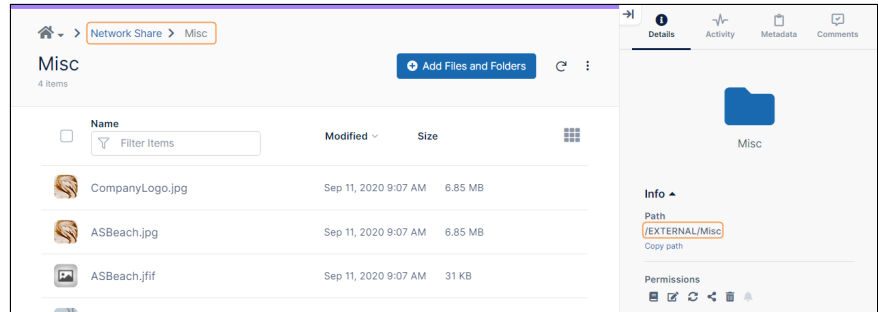
Folder	How to specify path	Example
My Files	/username	<p>In this example, to specify the My Files folder of the user with username jessica, use:</p> <p>/jessica</p> <p>If jessica were logged in, and she selected My Files, she would see the exact path in the Details tab in the right panel.</p> 
Team Folders	/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 sidebar with categories: DEVICES (Devices), GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification, Compliance - NEW), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), and SETTINGS (Settings). The 'Reports' item is highlighted with an orange arrow. 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 'Actions' column contains three icons: a play button (run), a document with a checkmark (download), and a red 'X' (delete).

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

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and '9 rows'.

⚠ 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.

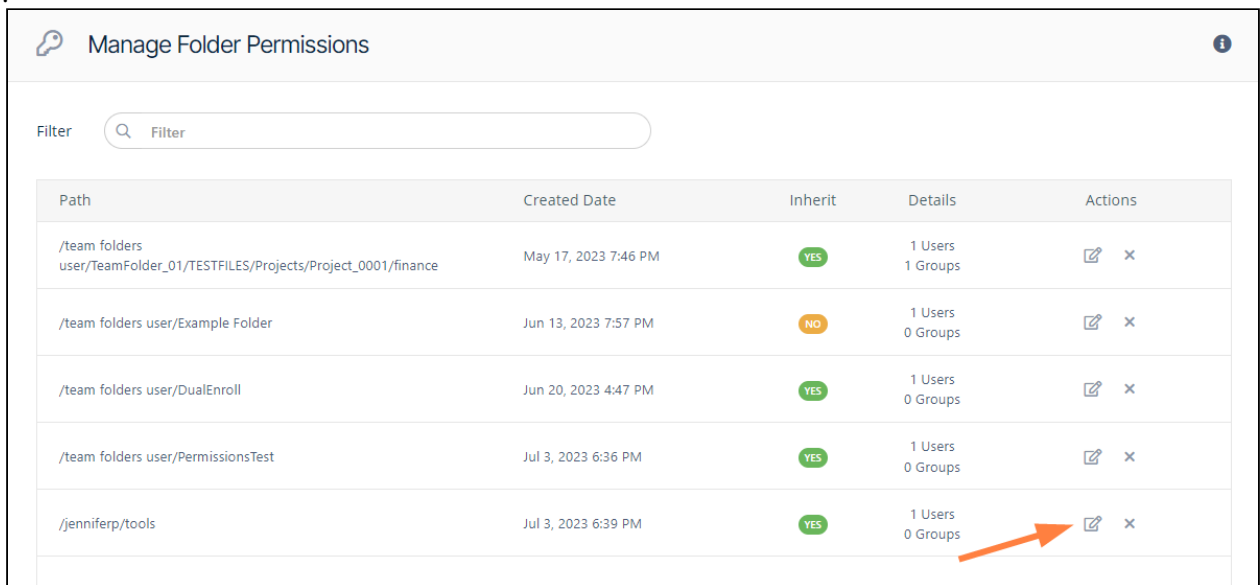
Manage Folder Level Permissions

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' with a magnifying glass icon. Below this is a table with the following columns: Path, Created Date, Inherit, Details, and Actions. The table contains five rows of folder permissions. The last row, for the path '/jenniferp/tools', has an orange arrow pointing to the edit icon (a pencil) in the Actions column.

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.

Read Only Sync

 Read only sync is supported starting from FileCloud 17.3





One way read-only syncing of shared folders is supported in FileCloud for Shared Folders with [Folder Permissions](#).

To allow read-only synchronization of shared folders.

1. Add this option to your cloudconfig.php file
define("TONIDOCLOUD_ENABLE_READONLYSYNC", 1);
2. Setup folder permissions for folders read only permissions.
3. Share this folder allowing read, write and sync permissions

Now when users sync this folder using their sync app, read only folders are synchronized down their local sync folders, but any changes that are made are discarded.

- If a new file or folder is added to a local read only sync folder it is ignored.
- If a file is modified, the modifications are discarded in the subsequent sync cycle and replaced with the file from the server.
- In FileCloud versions 23.1 and later, the modified file is saved in the top-level local Sync folder with **(ReadOnlyCopy_YYYY-MM-DD HH-MM-SS)** appended to its name:

Name	Date modified	Type
 My Files	5/15/2023 1:51 PM	File folder
 Shared with Me	4/11/2023 1:14 PM	File folder
 Team Folders	6/13/2023 2:19 PM	File folder
 Sample Markdown(ReadOnlyCopy_2023-06-14 10-06-41).md	6/14/2023 10:06 AM	MD File

- If a file is deleted, the file is re-downloaded from the server and reappears in the local sync folder in the subsequent sync cycle

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.

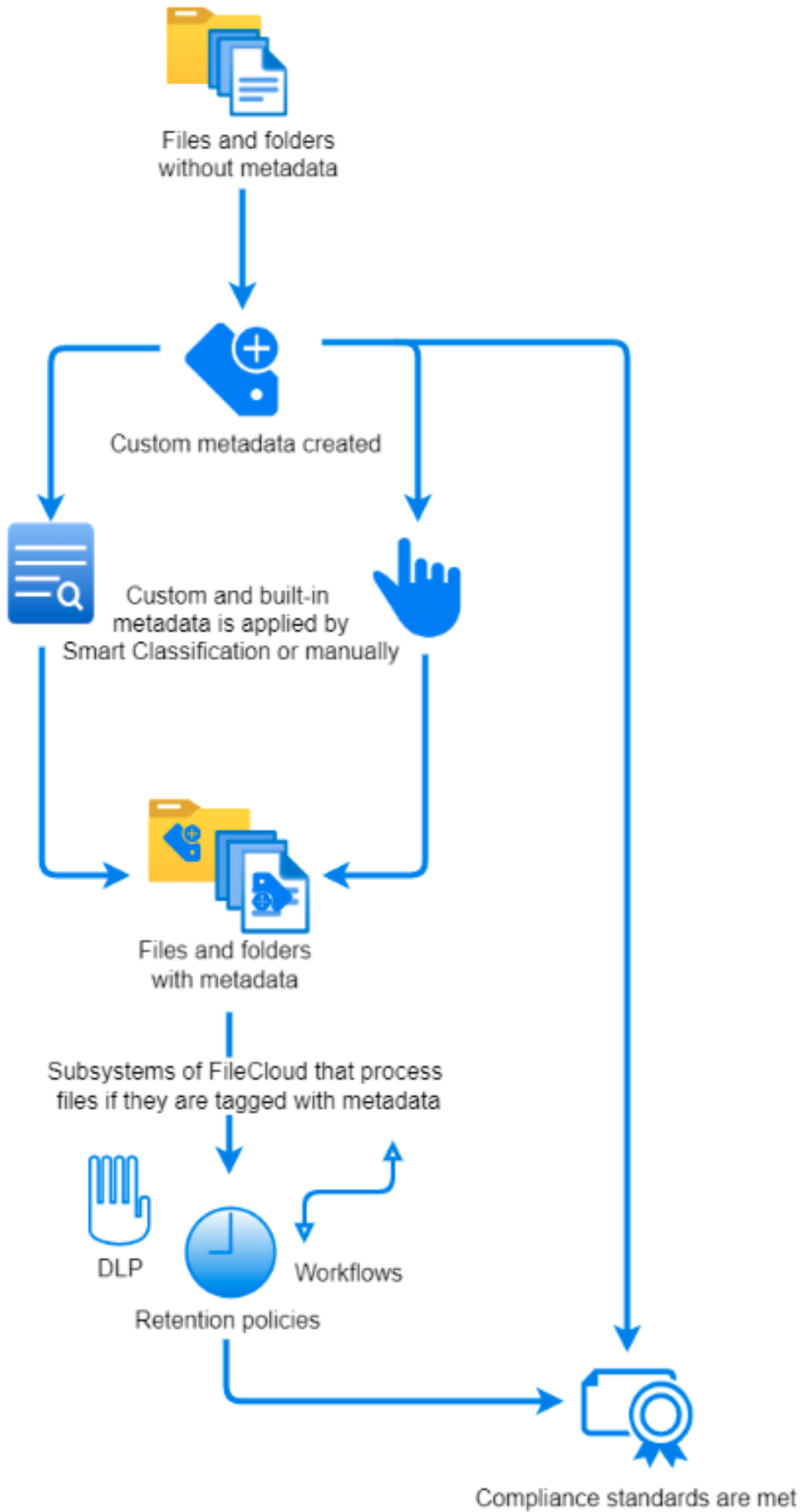
Metadata for governance and other system processes

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](#).

The screenshot displays the FileCloud interface for a document named 'Annuity3.docx'. The main view shows a list of files with columns for Name, Modified, and Size. The 'Annuity3.docx' file is selected. On the right, a metadata panel is open, showing the document's details and metadata options. The 'Metadata' tab is highlighted with an orange arrow. The panel includes an 'Add Metadata' section with an 'Author' dropdown and an 'Add' button. Below this, there is a 'Default' section and a 'Tags' section with a search bar and a 'financial' tag. At the bottom, the 'Document Life Cycle metadata' section shows 'Creation Date' as 2021-05-14 09:46:16 and 'Last Access' as 2021-12-15 11:59:41.

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](#)
- [Troubleshooting Metadata](#)
- [Finding files without 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														
Built-In	<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="557 783 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															
Custom Metadata Set	This is a fully customizable set of metadata, defined by the administrator.	As many as you want to create														

How do I allow users to tag their files?

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

 [Manage Metadata Permissions](#)

 Starting with FileCloud Version 20.1, by default, FileCloud files and folders stored on S3 and Azure cannot be downloaded for extraction if they are over 100MB. You may change the default size permitted for download using the procedure under **Allowed Memory Size Exhausted** on the [Troubleshooting Metadata](#) page.

More Information:

FileCloud Videos	FileCloud Blogs
	<ul style="list-style-type: none"><li data-bbox="1029 646 1333 716">• 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 FileCloud interface for managing metadata sets. On the left, the navigation panel includes sections for DEVICES, GOVERNANCE (with sub-items like Dashboard, Retention, Smart DLP, Smart Classification, and Compliance), and MISC. (with sub-items like Audit, Alerts, User Locks, Workflows, Reports, Federated Search, and Metadata). The 'Metadata' option is highlighted. The main content area is titled 'Manage Metadata Sets' and features a search filter, a 'Show 10 Items' dropdown, and a table of metadata sets. The table has columns for Metadata Set Name, Description, Status, Set Type, User Count, Group Count, and Actions. The 'Default' set is highlighted. A user dropdown 'jenniferperkins' and an 'Add Metadata Set' button are in the top right corner.

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	[Edit] [Delete]
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	[Edit] [Delete]
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	[Edit] [Delete]
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	[Edit] [Delete]
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	0	1	[Edit] [Delete]
AIP Sensitivity Label metadata	AIP Sensitivity Label metadata set	Enabled	Built-in	0	1	[Edit] [Delete]
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	0	1	[Edit] [Delete]

- 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"/> ✕
Type	text	Full time or part time job	Enabled	<input type="checkbox"/> ✕

Create

- 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](#)

Filter Show 10 Items

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	ACTIONS
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	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" value="edit"/> <input style="background-color: #f44336; 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: #f44336; 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: #f44336; 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: #f44336; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>
Subsystem	Enumeration		Enabled	<input type="text" value="edit"/> <input style="background-color: #f44336; color: white; padding: 2px 5px; border-radius: 3px;" type="button" value="✕"/>

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	R	W	Comment
Write	Readonly	All	/USERNAME/assets	-	x	x	Write permission is granted based on the user permissions
Write	-	All	/USERNAME/assets/image1.png	write lock	x	-	As lock is applied readonly access to metadata will only be granted
Readonly	Write	All	/SHARED/user1/assets	view only access for share	x	-	Share permissions will narrow metadata permissions to readonly
Readonly	Write	/USERNAME/assets	/USERNAME/assets/images	-	x	x	As file path is a subpath of one of the allowed paths user will be granted the write access for metadata
Write	-	/USERNAME/assets	/USERNAME/images	-	-	-	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

Name

Description

Disabled

Permissions

Users
Groups
Paths

Allow All
 Allow Selected Paths

Add Allowed Path

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="checkbox"/> <input style="background-color: #f44336; color: white;" type="checkbox"/>
Banner Resolution	Enumeration	Resolution of the banner	Enabled	<input type="checkbox"/> <input style="background-color: #f44336; color: white;" type="checkbox"/>
Active	Boolean	Specifies whether asset is active	Enabled	<input type="checkbox"/> <input style="background-color: #f44336; color: white;" type="checkbox"/>
Image type	Enumeration	Type of the image	Enabled	<input type="checkbox"/> <input style="background-color: #f44336; color: white;" type="checkbox"/>
Subsystem	Enumeration		Enabled	<input type="checkbox"/> <input style="background-color: #f44336; color: white;" type="checkbox"/>

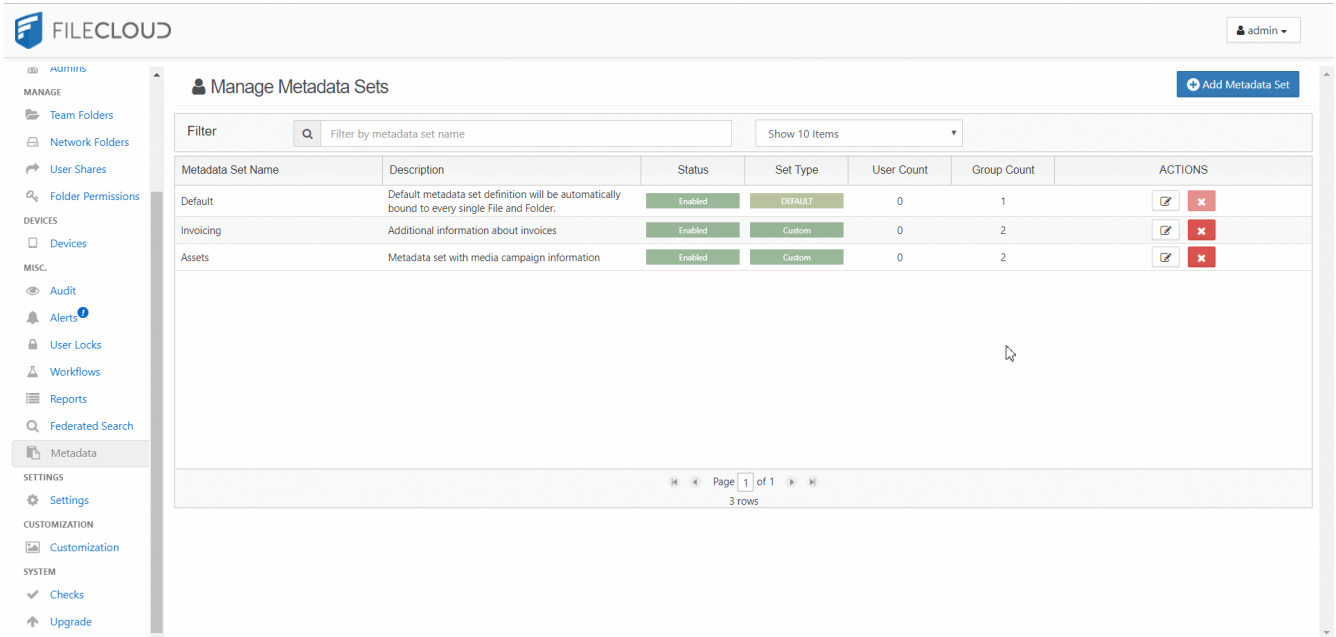
Save

Close

Video of Managing Metadata

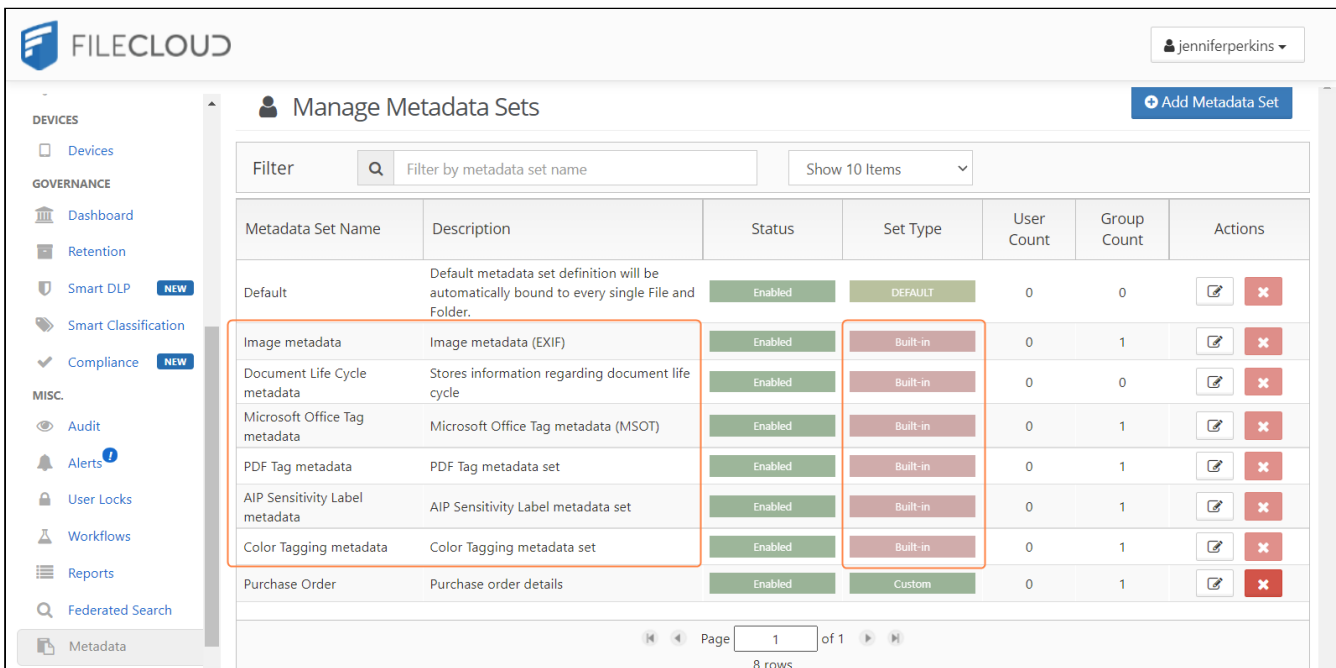


Administrators can manage data that provides additional information about files and folders available in FileCloud using **Metadata**.



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

Description

Disabled

Permissions

Users | Groups | Paths

[Add User](#)

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

Page 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*

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	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>

Use of MSOT Sensitivity Labels in FileCloud

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, add the following setting to the config file.

To enable MSOT sensitivity labels in FileCloud:

1. Open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add the following :

```
define('TONIDO_DISABLE_MSOT_SENSITIVITY_LABELS', 0);
```


The screenshot shows the 'Metadata' panel for a Microsoft Office file. The fields are as follows:

- Title: N/A
- Subject: N/A
- Creator: Employee
- Keywords: (empty)
- Description: N/A
- Last Modified By: Employee
- Created: Feb 10, 2016
- Modified: Feb 10, 2016
- Category: (empty)
- Sensitivity Labels: (empty)


An orange callout bubble with an arrow points to the 'Sensitivity Labels' field, containing the text: "To display this field, enable sensitivity labels."

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:




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.

Properties ▾



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

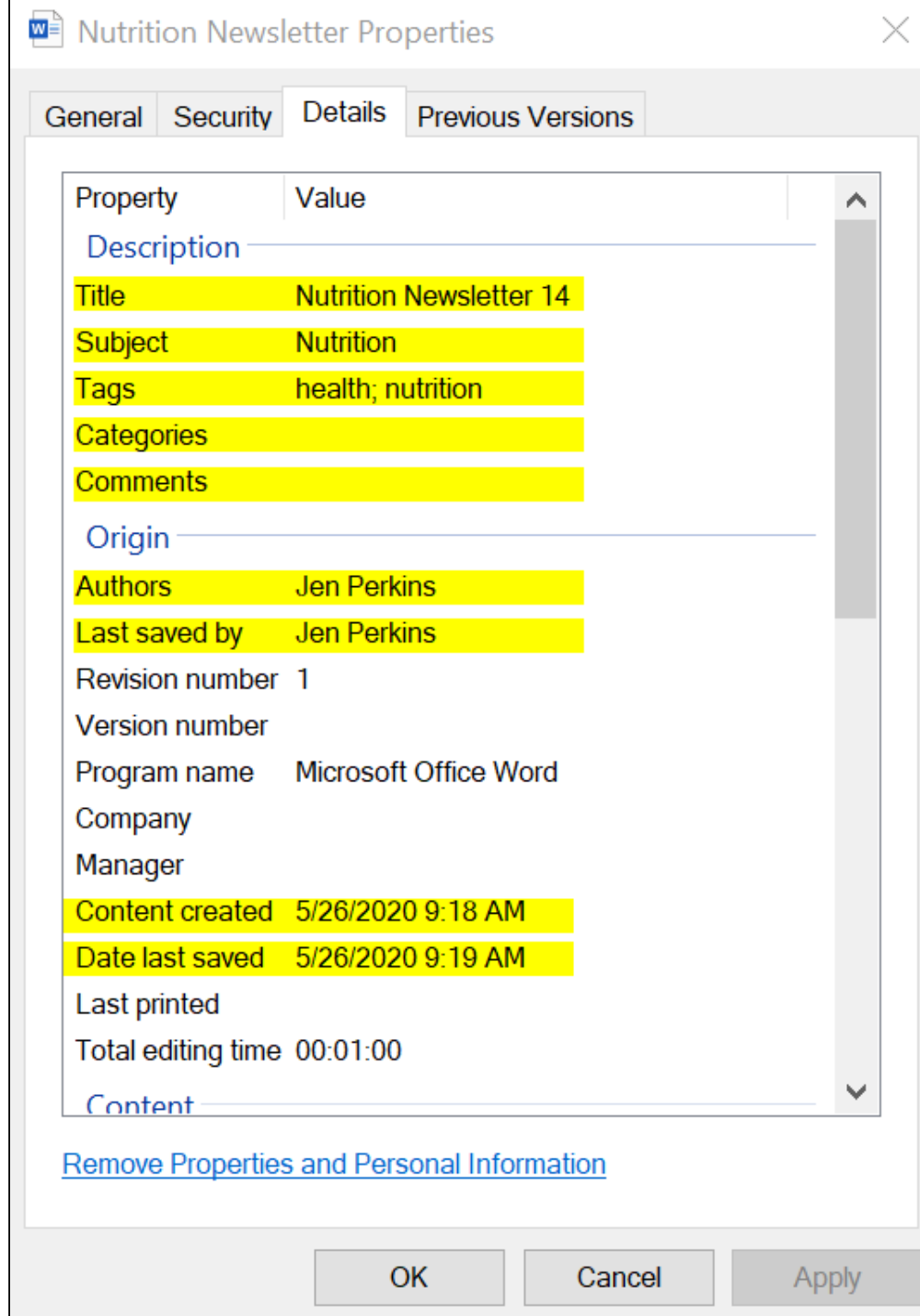
Last Modified	Today, 9:19 AM
Created	Today, 9:18 AM

Last Printed

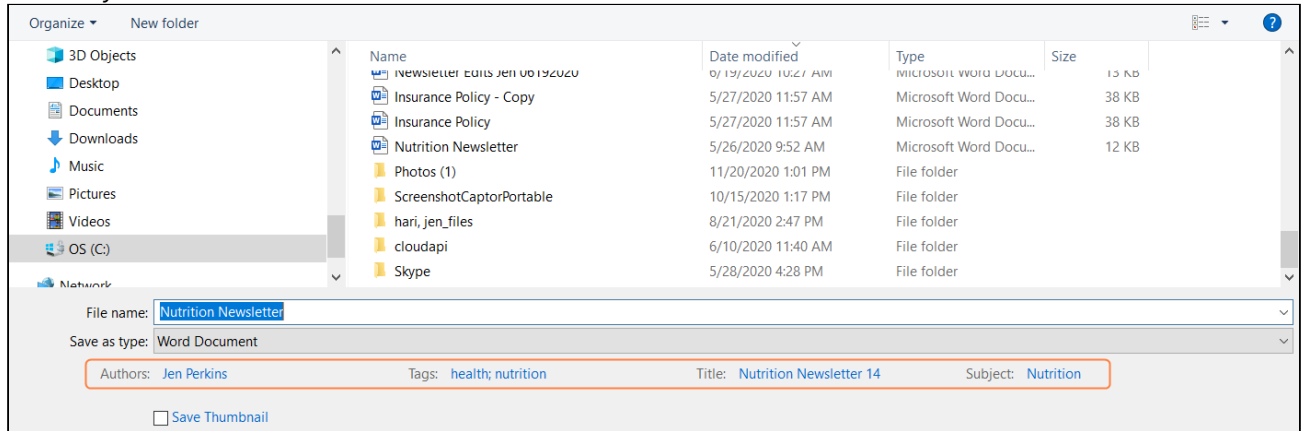
Related People

Author	 Jen Perkins
	Add an author
Last Modified By	 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	<div style="display: flex; justify-content: space-between; width: 20px;"> ✎ ✕ </div>

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 dialog has a title bar with a close button (X). The main area contains several fields:

- Name:** Color
- Description:** Color
- Attribute Type:** Key Value Pair (dropdown menu)
- Predefined Values:** A list of color entries, each with a name and a hexadecimal code, and a small 'X' icon to the right. The entries are: Red:#FF0000, Yellow:#FF9900, Green:#18C600, Aqua:#00B4C9, Blue:#0054C9, Purple:#7E00C9, and Orange:#FE9A2E. An orange arrow points to the 'Orange:#FE9A2E' entry.
- Disabled:**
- Required:**
- Default Value:** Tag input

At the bottom right, there are two buttons: 'Save' (blue) and 'Close' (white).

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"/> ✕
Author	Text	Person who created the document	Enabled	<input type="text"/> ✕
Subject	Text	Subject of the document	Enabled	<input type="text"/> ✕
Keywords	Array	Keywords associated with the document	Enabled	<input 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"/> ✕
Producer	Text	If the document was converted to PDF from another format, the application that converted it to PDF	Enabled	<input type="text"/> ✕

[Save](#)

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*
AIP Sensitivity Label metadata

Description*
AIP Sensitivity Label metadata set

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
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 displays the 'Manage Metadata Sets' interface. On the left, a navigation menu includes 'HOME', 'USERS/GROUPS', 'MANAGE', 'DEVICES', 'MISC.', and 'SETTINGS'. The 'Metadata' option under 'MISC.' is highlighted with a red box and a red arrow. The main content area shows a table with 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]

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and '3 rows'.

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](#)

Troubleshooting Metadata

Allowed Memory Size Exhausted

An error message similar to the following indicates that while uploading a large file, the system could not extract metadata because it required more memory than the allowed PHP memory limit:

019-04-05 5:27:29 - ERROR : CLFC-00004 ERROR | 2019-04-05 05:27:29 | 1 | Allowed memory size of 524288000 bytes exhausted (tried to allocate 316675836 bytes)

Starting with FileCloud Version 20.1, the setting `TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB` in `cloudconfig.php` file enables you to override the maximum file size for automatic metadata extraction to take place.

By default, the value of the setting is:

- 500MB for local storage
- 100MB for Azure / S3

For example, if the value of the setting is 500, when files over 500 MB are uploaded, metadata extraction will not occur.

Change the maximum file size for metadata extraction:

1. Open `cloudconfig.php` at
 - Windows: `XAMPP DIRECTORY/htdocs/config/cloudconfig.php`
 - Linux: `/var/www/config/cloudconfig.php`
2. Find the following:

```
define("TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB", 500);
```

3. Change the value of the setting.
For example:

```
define("TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB", 128);
```

Finding files without metadata

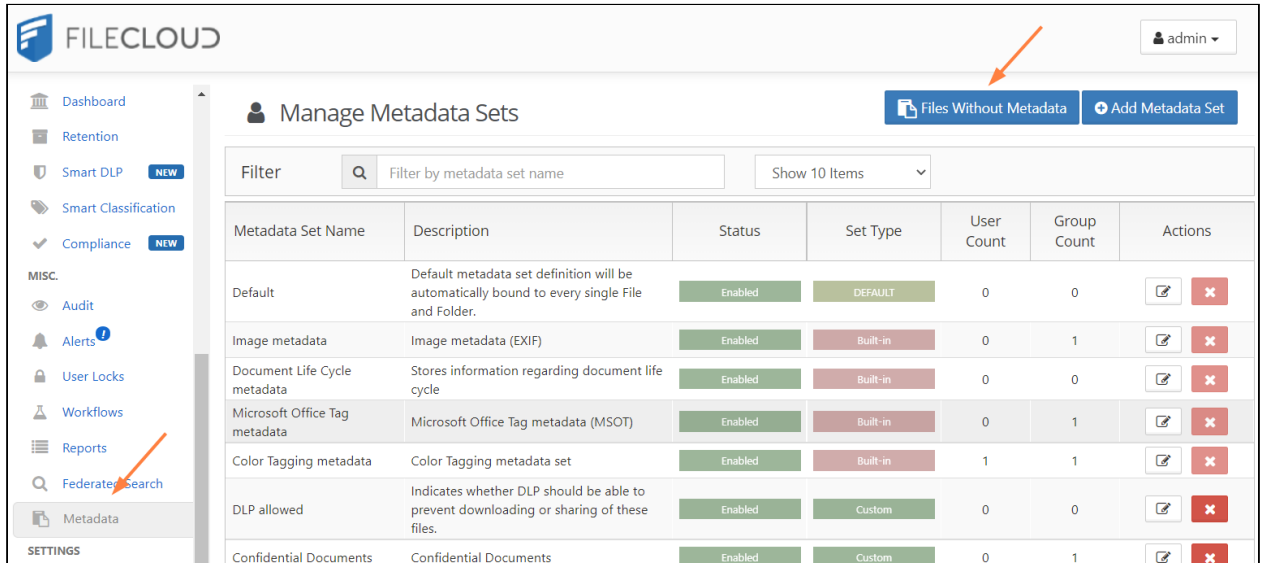
[Smart Classification](#) does not apply metadata to files over a specified size, but you can add metadata to those files manually. Beginning in FileCloud 20.1, you can configure your system to search for files without metadata.

Find files without metadata:

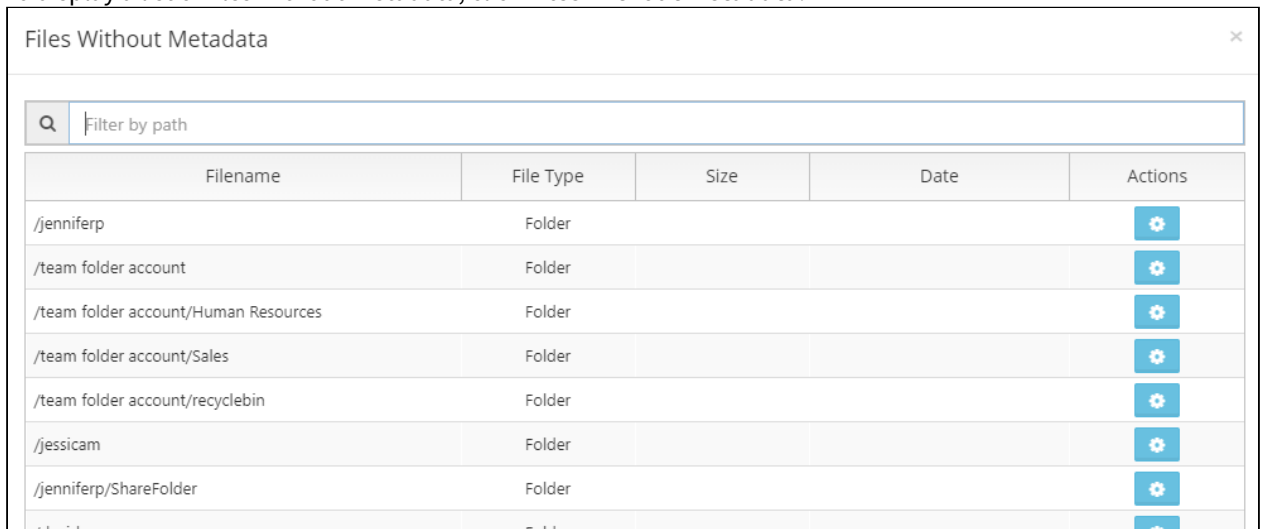
1. Open the configuration file:
Windows: `XAMPP DIRECTORY/htdocs/config/cloudconfig.php`
Linux: `/var/www/config/cloudconfig.php`
2. Add the line:

```
define('TONIDOCLOUD_SHOW_FILES_WITHOUT_METADATA', true);
```

3. In the navigation bar, click **Metadata**.
Now the upper-right corner of the Manage Metadata Sets screen displays a **Files Without Metadata** button.



4. To display a list of files without metadata, click **Files Without Metadata**.



Add metadata from the Files Without Metadata list

1. Follow the procedure above to access your **Files Without Metadata** list.
2. Across from a file, click the button under **Actions**.



The Manage File Metadata window opens.

Manage File Metadata ✕

Add codes **Custom metadata** ▼

▼ Default ⓘ **Default metadata**

Tags ⓘ

Save

▶ Document Life Cycle metadata ⓘ **Builtin metadata**

Close

The top drop-down list holds [custom metadata](#), the drop-down list below that holds [default metadata](#), and any drop-down lists below that hold [built-in metadata](#).

- To add a custom metadata set, choose it in the drop-down list and click **Add**. It is added below the other metadata sets.

4. Add or change values in any of the metadata fields.

The screenshot shows a 'Manage File Metadata' dialog box. At the top, there is a close button (X). Below it, a dropdown menu shows 'Add' and 'No metadata available'. There are three expandable sections: 'Default', 'Document Life Cycle metadata', and 'codes'. The 'codes' section is expanded and highlighted with a red border. It contains three input fields: 'color' with the value 'pink', 'alphanumeric' with the value '1A', and 'label' with the value 'Tax'. Below these fields is a blue 'Save' button. At the bottom right of the dialog is a 'Close' button.

5. You can update the value of fields that appear in the **Default** metadata set.. Expand the section, and add or change the values in the metadata fields, and click **Save**.

Manage File Metadata
✕

Add
No metadata available
▼

▼ **Default** ⓘ

Tags ⓘ

customer ✕
 admin ✕

version ⓘ

2.0

Save

▶ **Document Life Cycle metadata** ⓘ

▶ **codes** ⓘ ✕ Remove

Close

6. You can view, but not update the values in built-in metadata sets. Expand the sections to view the metadata and any values they have.

Metadata Limitations/Recommendations

Metadata feature	Recommended maximum
Metadata set name	128 characters
Metadata set description	128 characters
Attributes per metadata set	99

Metadata feature	Recommended maximum
Attribute name	128 characters
Attribute description	128 characters
Values per enum/array	99
Predefined value (enum)	128 characters
Default value	128 characters
Actual value	128 characters

Managing FileCloud Licenses

Your FileCloud license provides legally binding guidelines on your use and distribution of FileCloud.

In this section:

- [FileCloud - License Purchase And Renewal](#)
- [Install FileCloud License](#)

FileCloud - License Purchase And Renewal

Purchase a new license

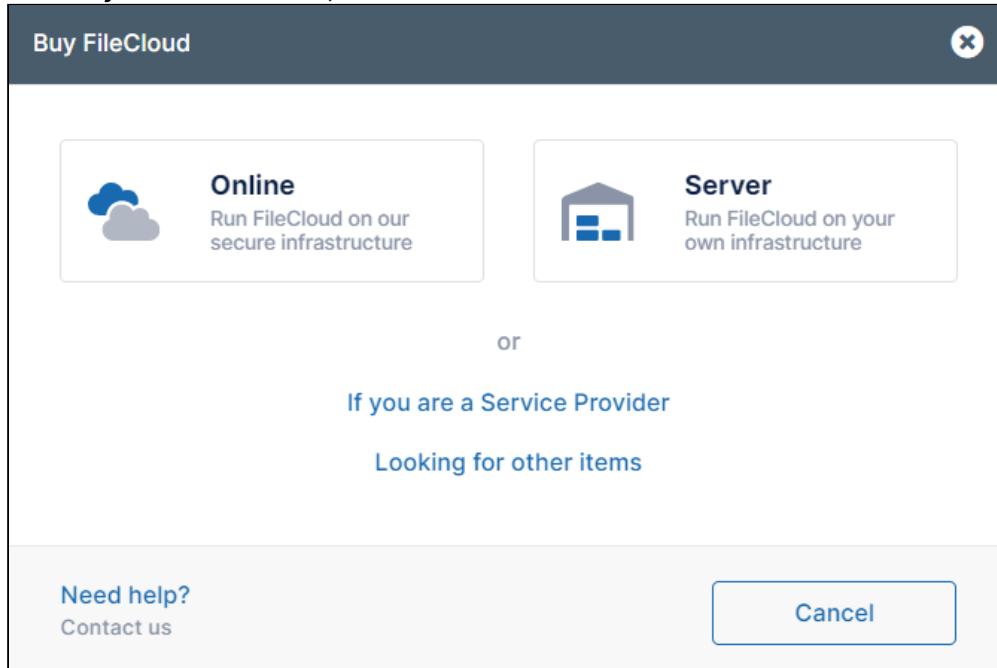
First

Choose a server or online license

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

The screenshot displays the FileCloud portal interface. On the left is a sidebar with navigation links: Dashboard, Sites, Downloads, SPLA Reports, and Billing. The main content area is titled "Sites & Licenses" and features a search bar and a "New license" button (highlighted with a red dashed box and an orange arrow). Below this are two license cards: one for "www" (pending) and one for "citest1.filecloudonline.com" (expired). A "View all" button is also present. The "Useful Resources" section includes links for "Get started", "Learn More", and "Downloads".

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

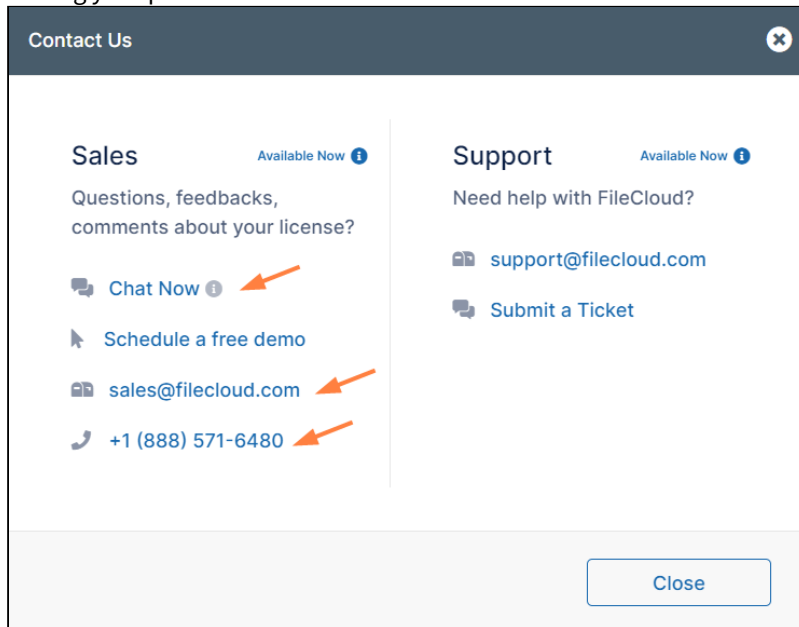
Service Provider

Custom pricing available

GET QUOTE

<ul style="list-style-type: none"> <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Storage <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Licensed External Users <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Support for Network Shares with NTFS Integration for VPN-less secure access. <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Content Classification & Search <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Content Lifecycle Management - Legal Hold, Retention, & Archival <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Unlimited Workflows <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Digital Rights Management <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM <li style="background-color: #ffe0b2; padding: 5px; margin-bottom: 5px;">✗ Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments) 	<ul style="list-style-type: none"> <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Storage <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Licensed External Users <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Support for Network Shares with NTFS Integration for VPN-less secure access. <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Content Classification & Search <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Content Lifecycle Management - Legal Hold, Retention, & Archival <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Workflows <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Digital Rights Management <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments) 	<ul style="list-style-type: none"> <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Storage <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Licensed External Users <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Support for Network Shares with NTFS Integration for VPN-less secure access. <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Content Classification & Search <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Content Lifecycle Management - Legal Hold, Retention, & Archival <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Unlimited Workflows <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Digital Rights Management <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM <li style="background-color: #e8f5e9; padding: 5px; margin-bottom: 5px;">✓ 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.

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](#)

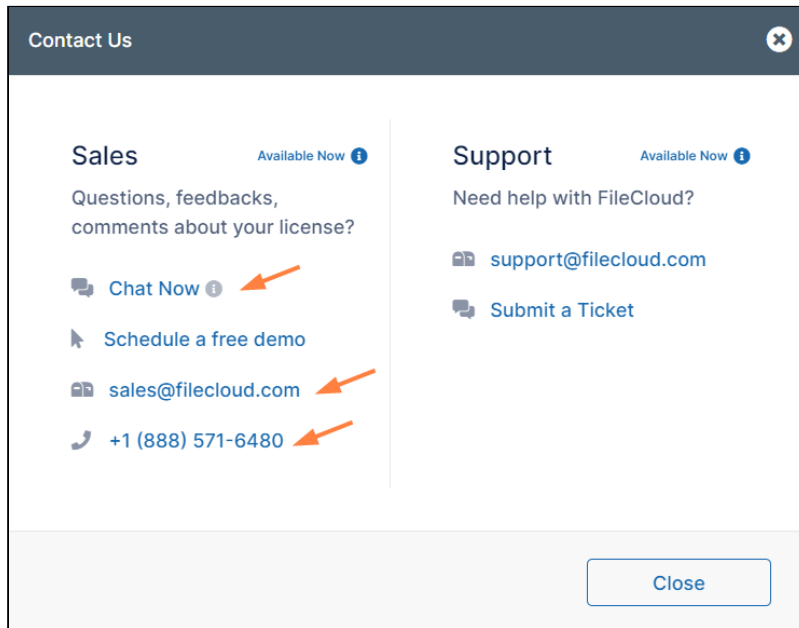
GovCloud

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>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>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>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.

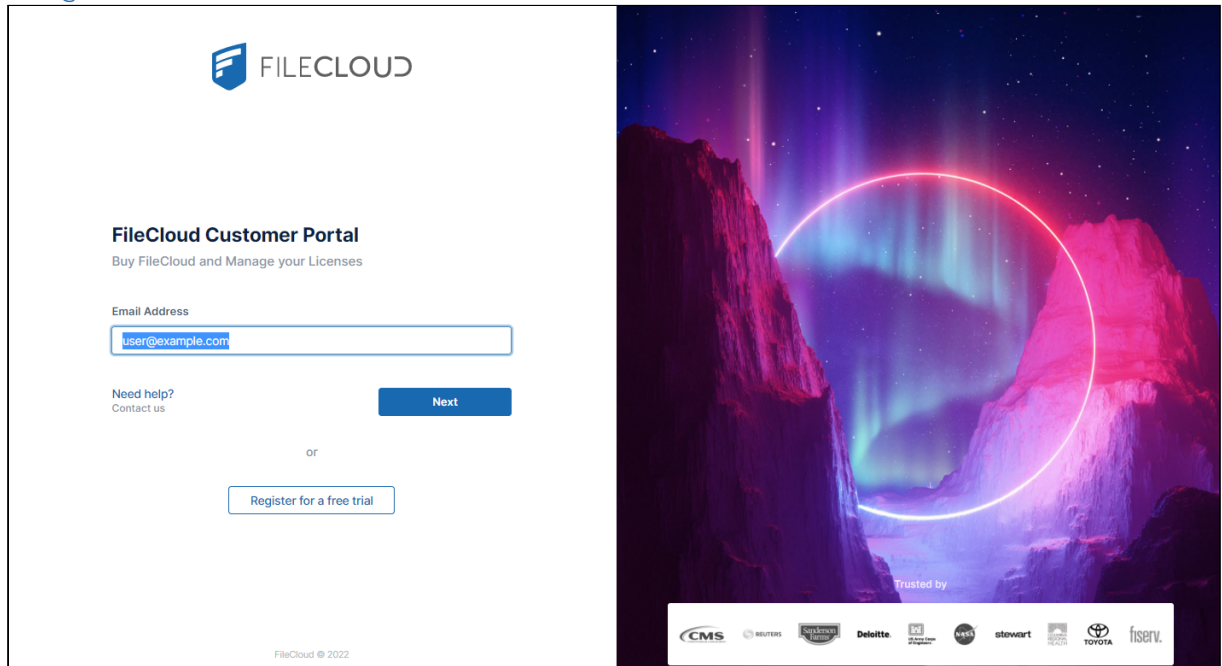
Renew an existing license

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.](#)

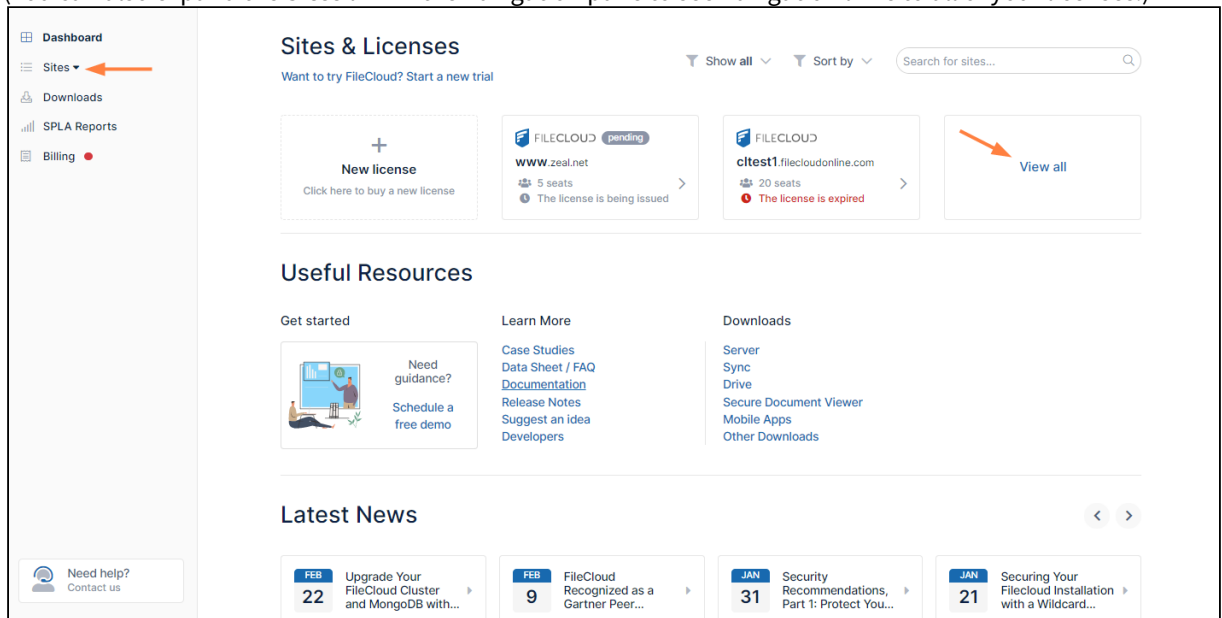
1. Log into <https://portal.getfilecloud.com>

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

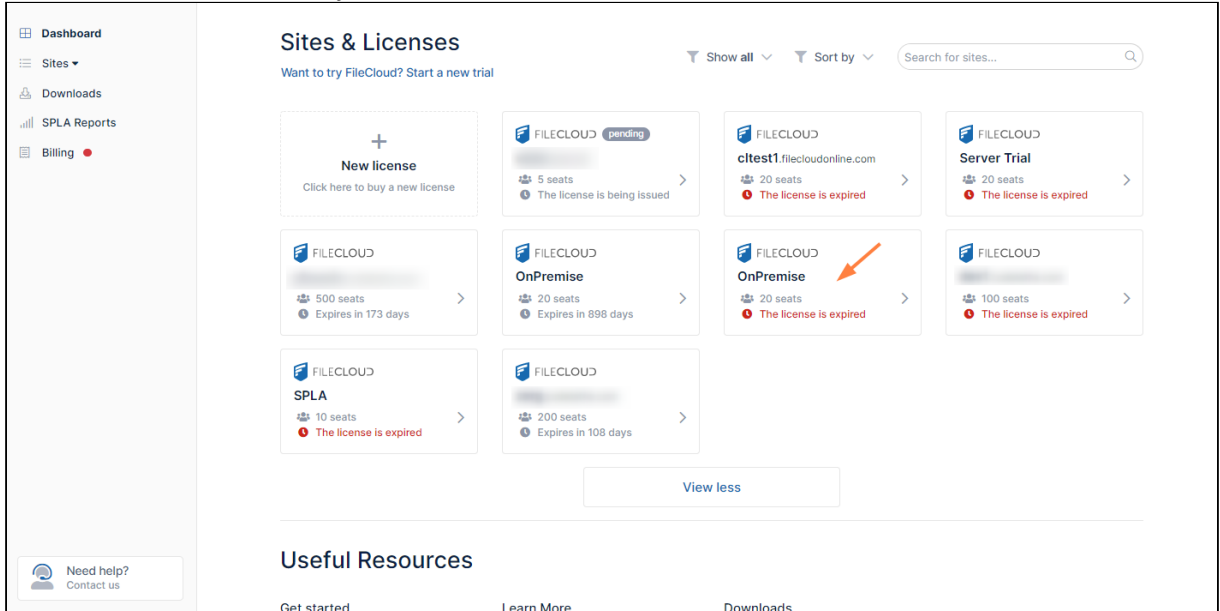


2. If you don't see the license you want to renew on the initial dashboard page, click **View all** to view all of your licenses.

(You can also expand the **Sites** link in the navigation pane to see navigation links to all of your licenses.)

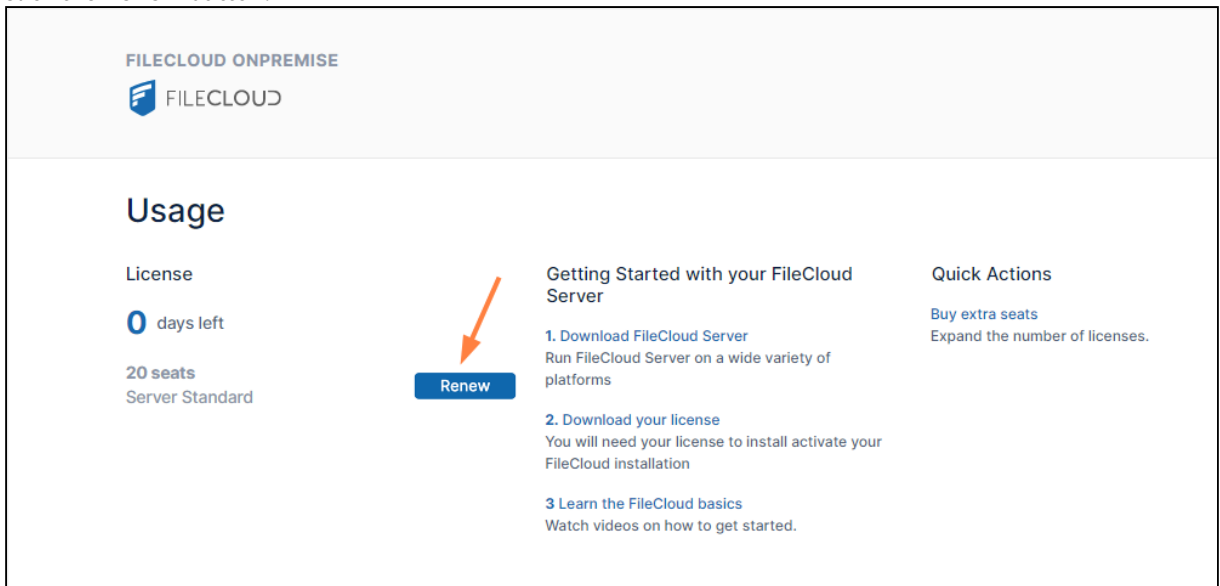


3. Find and click the license that you want to renew.



A screen that displays the license details opens.

4. Click the **Renew** button.



An **Order Summary** opens.

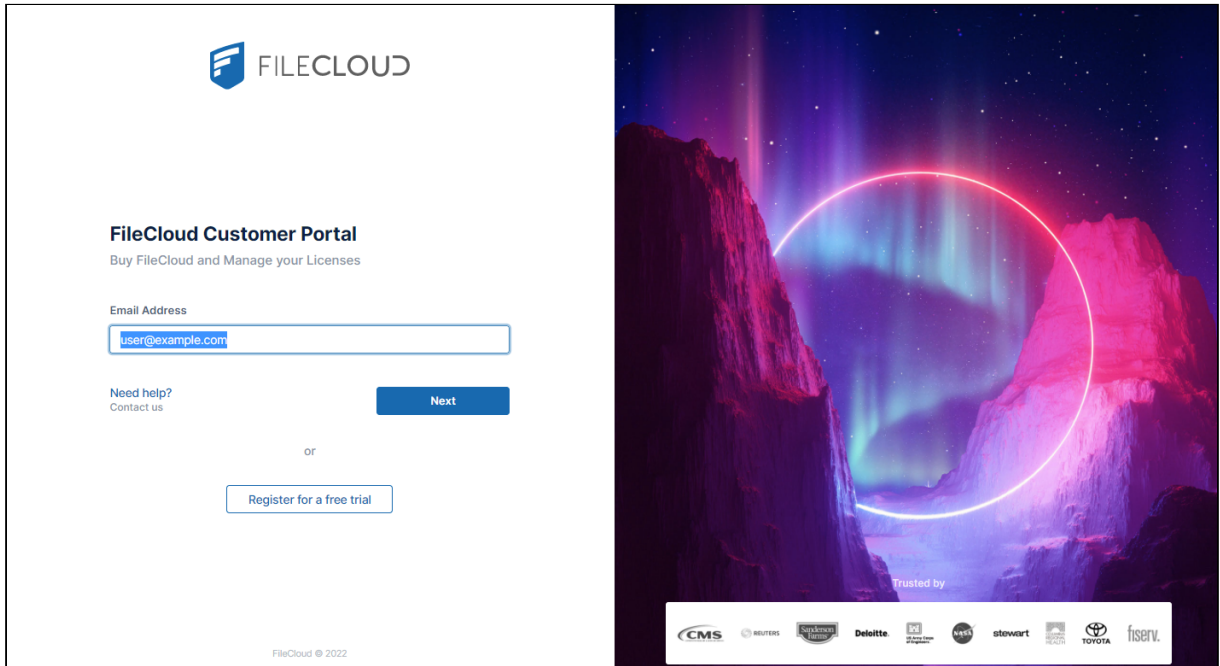
5. Follow the [checkout process](#), below.

Add additional users to an existing license

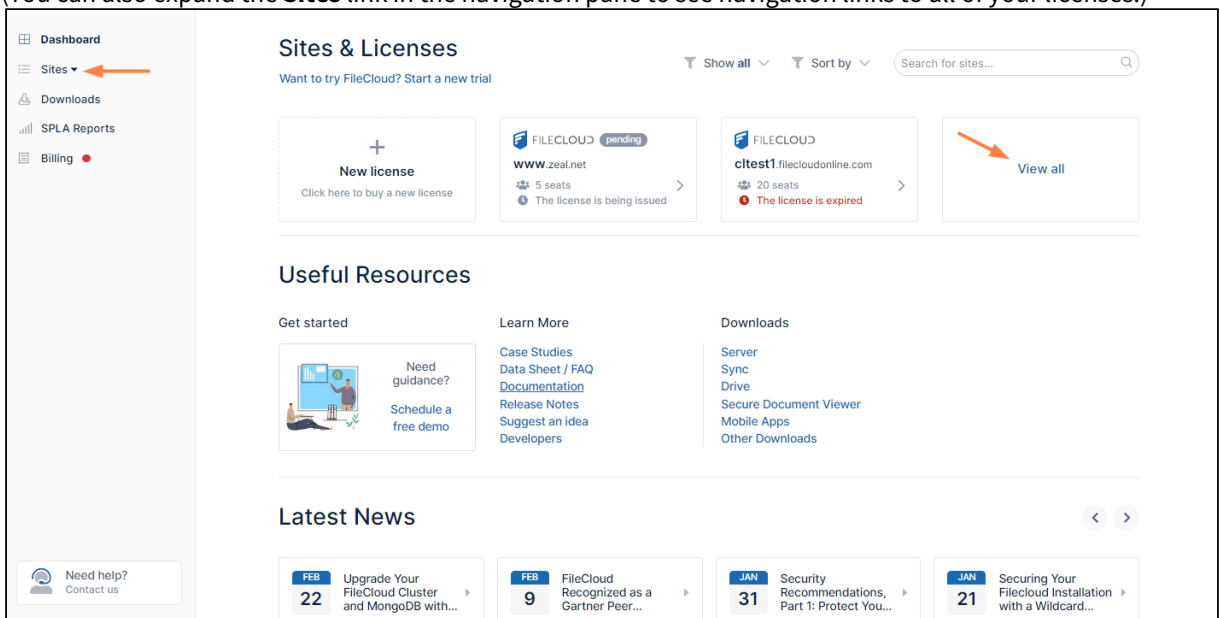
Add additional users to a license

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

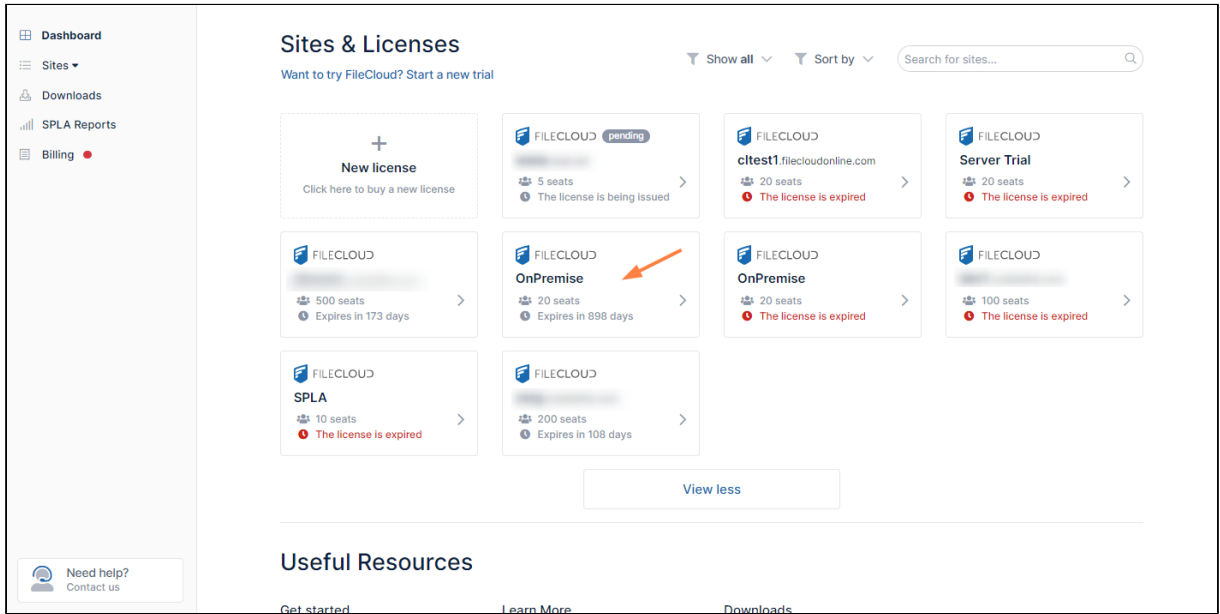
Notes: Enter the email of the license holder. To change the license holder email, please email sales@codelathe.com.



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.)

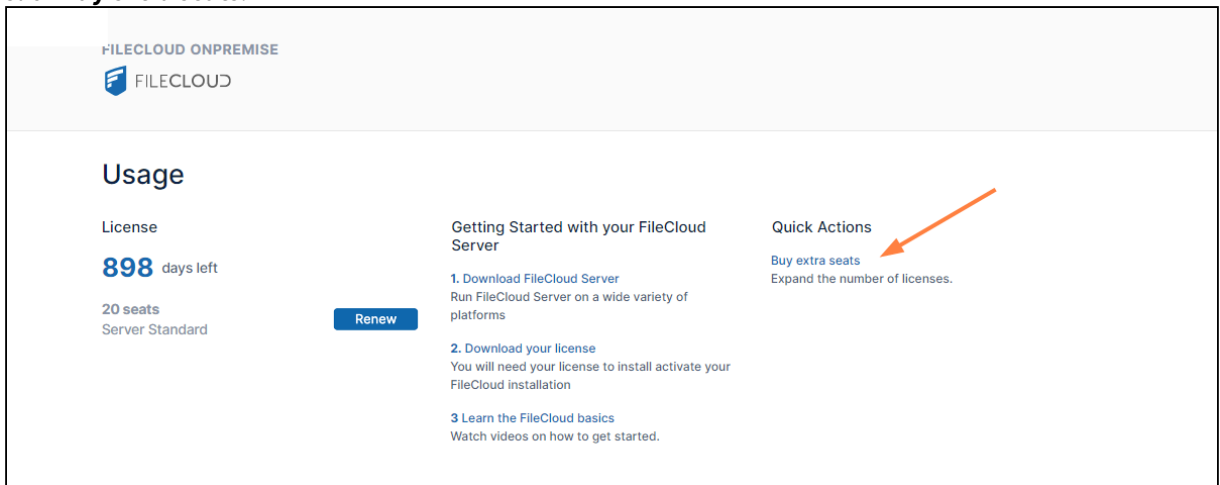


3. Find and click the license that you want to add additional users to.



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.

Checkout

FileCloud Server - Enterprise Advanced
Additional licenses for jenperkins.com

Your license expires in 361 days, you will be charged proportionately

Additional licenses Drag the slider below to change

1 seats

Additional Seats 1 Seats

Total \$

Billed annually ⓘ

[Need help?](#)
Contact us


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

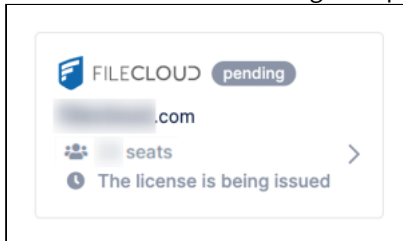
Total Due

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](#) [Save Quote](#) [Pay Now](#)

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, the pending icon disappears. Now you can [download and install](#) the license.

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 type="text" value="44444"/>		<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

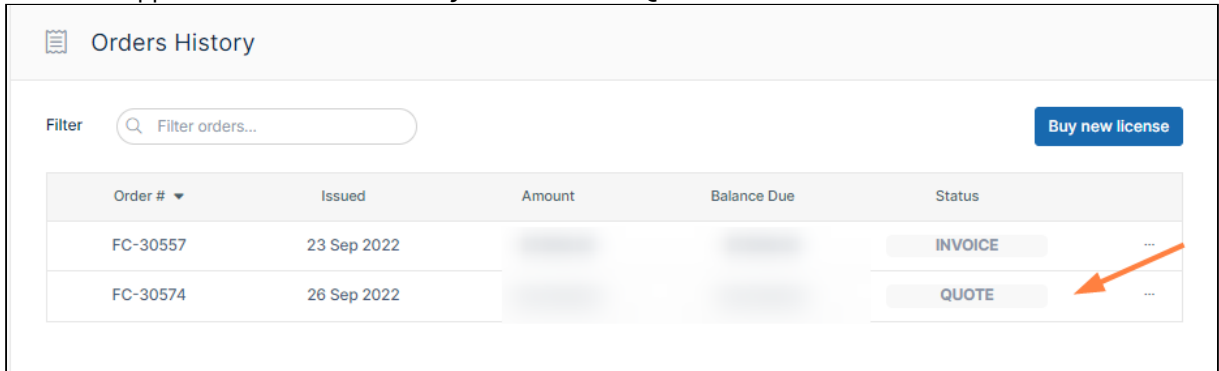
Invoice Number	FC-30574
Order Sub Total	
Sales Tax	
Total Due	

All prices are in U.S. Dollars

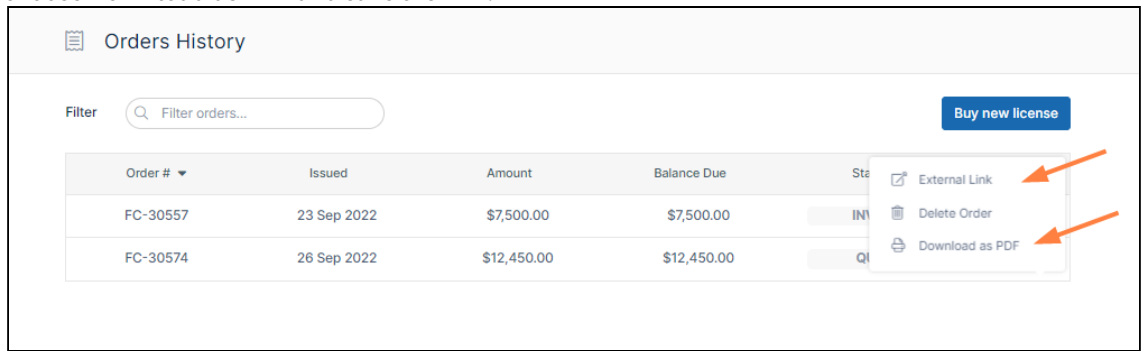
[Need help?](#)
Contact us

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

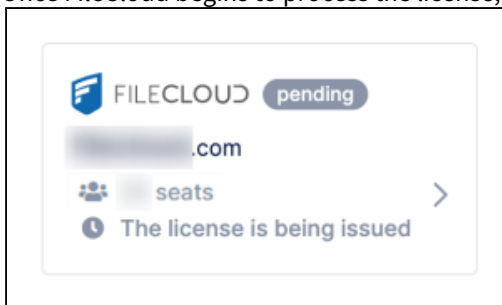
4. Your order appears under **Orders History** with the status **QUOTE**.



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, the pending icon disappears. Now you can [download and install](#) the license.

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	

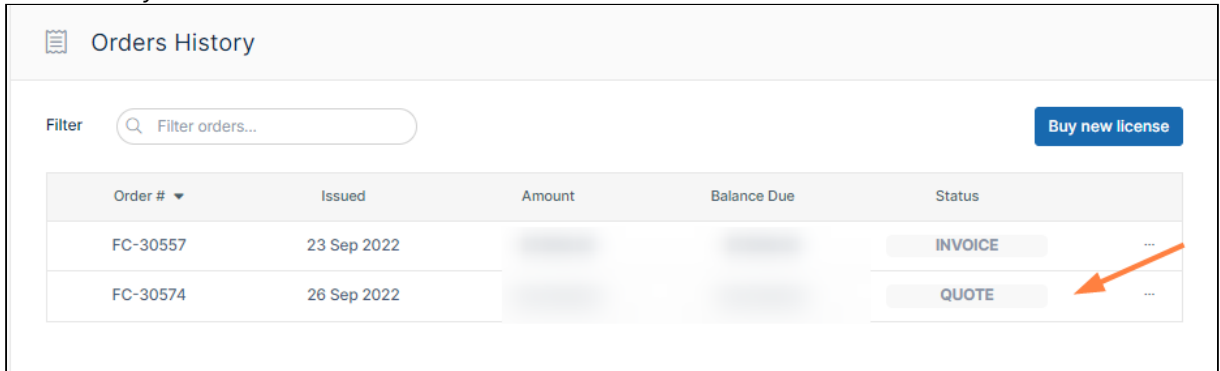
All prices are in U.S. Dollars

[Need help?](#)
Contact us

[Save Quote](#) [Checkout](#)

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.

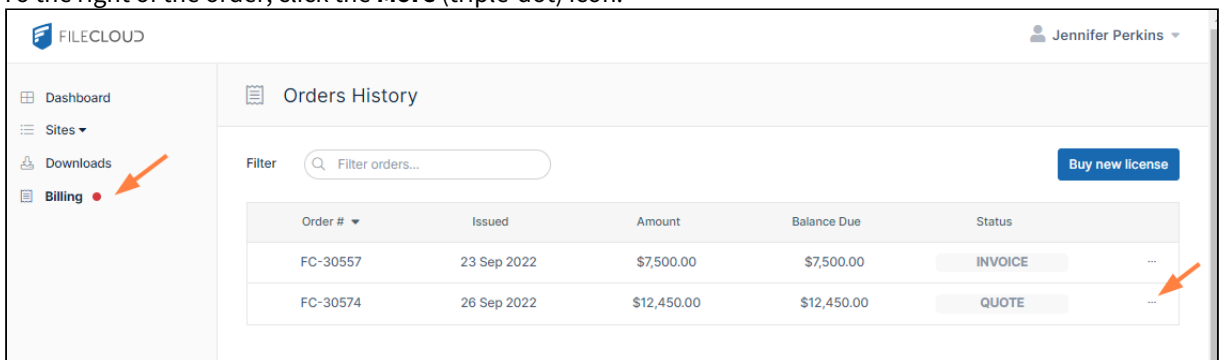


3. When you are ready to continue, return to the **Billing** screen and perform one of the actions in [Manage orders](#), below.

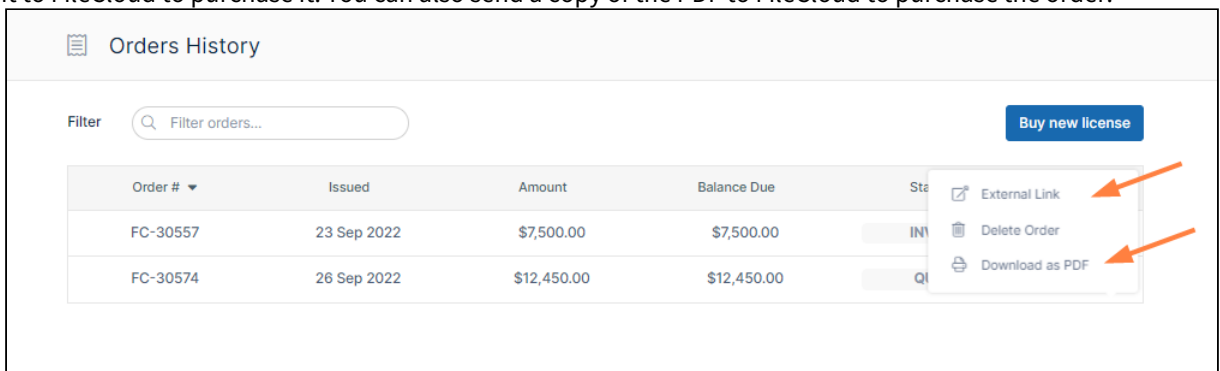
Manage orders

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.



Install FileCloud License

Your FileCloud license is a document that provides legally binding guidelines on the use and distribution of your newly installed FileCloud software.

Obtaining a FileCloud License

Obtaining a FileCloud License

The length of access and site configuration will vary depending on your license type.

There are two basic forms of FileCloud licenses:

License Type	Duration	Features	Availability
Trial (free)	Temporary 30 days for a server license 15 days for an online license	<ul style="list-style-type: none"> All features Mobile and desktop apps Free support <p>💡 Deployment URL will be set as "*" (accessible from any URL)</p>	Server (Self-host) Online (Hosted by us)
Production	Permanent based on length paid for Usually 1 year	<ul style="list-style-type: none"> All features Mobile and desktop apps Choose from 3 levels of support <p>💡 Deployment URL can be set to use your specific domain (URL accessibility from within your company and outside access managed by Administrators)</p>	Server (Self-host) <ul style="list-style-type: none"> Essentials Advanced Service Provider Online (Hosted by us) <ul style="list-style-type: none"> Essentials Advanced GovCloud

➔ For more information, read the license descriptions and Key Features on the [FileCloud Pricing](#) page.

➔ To purchase a license, see [License Purchase and Renewal](#)

➔ For a trial license, go to <https://www.filecloud.com/#hostedTrial> and follow the instructions in the wizard.

- ⚠ When you register on the FileCloud web site to access the installation software, you should receive your trial license, although it still needs to be installed.
- If you already downloaded your license, proceed to the steps for installing it.
 - If you did not download your license yet, use the next procedure to download it, and then proceed to the steps for installing your license.

Downloading your license

Downloading your License

To downloading your license:

1. Navigate to <https://portal.getfilecloud.com/ui/user/index.html>
2. Type in the registered email and the password provided to access the license portal.

The license portal opens to the dashboard, where it lists all of your licenses.


The screenshot shows the FileCloud 'Sites & Licenses' dashboard. On the left, a navigation menu has 'Sites' selected with an orange arrow. The main area features a 'New license' button, a grid of license cards, and a 'View all' button with an orange arrow pointing to it. The license cards include details like '5 seats' and 'The license is being issued' or 'The license is expired'. Below the licenses are sections for 'Useful Resources' (Get started, Learn More, Downloads) and 'Latest News' with several news items.

3. If you don't see the license you want to download listed, click **View all** to see all of your licenses. (You can also expand **Sites** in the navigation pane to access links to all of your licenses).
4. Click the license that you want to download.

This screenshot shows the same dashboard but with more license cards displayed in a grid. An orange arrow points to a specific 'OnPremise' license card with 20 seats and an expiration date of 898 days. The 'View all' button is now visible at the bottom of the license grid. The 'Useful Resources' section is partially visible at the bottom.

5. The license is stored on your server as license.xml.

Installing Your License

-  The ability to install license components such as SALESFORCE is available in FileCloud Server version 18.2 and later.

Installing Your License


You can operate FileCloud Server using any of the license types.

- If you do not need to use individual additional components, such as SALESFORCE, and Pattern Search, you can use an Essentials license.
- However, if you need to use individual additional components, such as SALESFORCE, and Pattern Search, then you must use an Advanced or Service Provider license.

There are multiple places where you can install your FileCloud license:

- Admin alert dialog box
- The dashboard's **License Information** widget
- The admin portal's **Settings > License** tab

It doesn't matter which one of these places you use; they all perform the same task.

-  After installation, to update or manage licenses, use the dashboard's **License Information** widget or the admin portal's **Settings > License** tab.

Admin Alert Dialog

During initial setup, when you log in to the admin portal, you see the **Admin Attention Required** dialog box, which allows you to upload your **license.xml** file and apply the license.

Admin Attention Required



	<p>WEBSERVER.</p> <p>Example path on Windows: c:\clouddata Example path on Linux: /opt/cloud/data</p> <p> <input type="button" value="Check Path"/> <input type="button" value="Apply"/> </p>
<p>Invalid License File</p>	<p>Upload your license via Install License</p> <p> <input type="button" value="Install License"/> </p> <p> <input type="text"/> <input type="button" value="Browse..."/> </p> <p>Choose License file (Only .xml)</p> <p> <input type="button" value="Apply"/> </p>

Close

To install your license from the Admin dialog:

1. In the **Invalid License File** row, click **Install License**.
2. In the new section that appears, click **Browse**.
3. Locate the license.xml file, and then click **Apply**.
4. The installed license appears in green under the textbox.

Dashboard

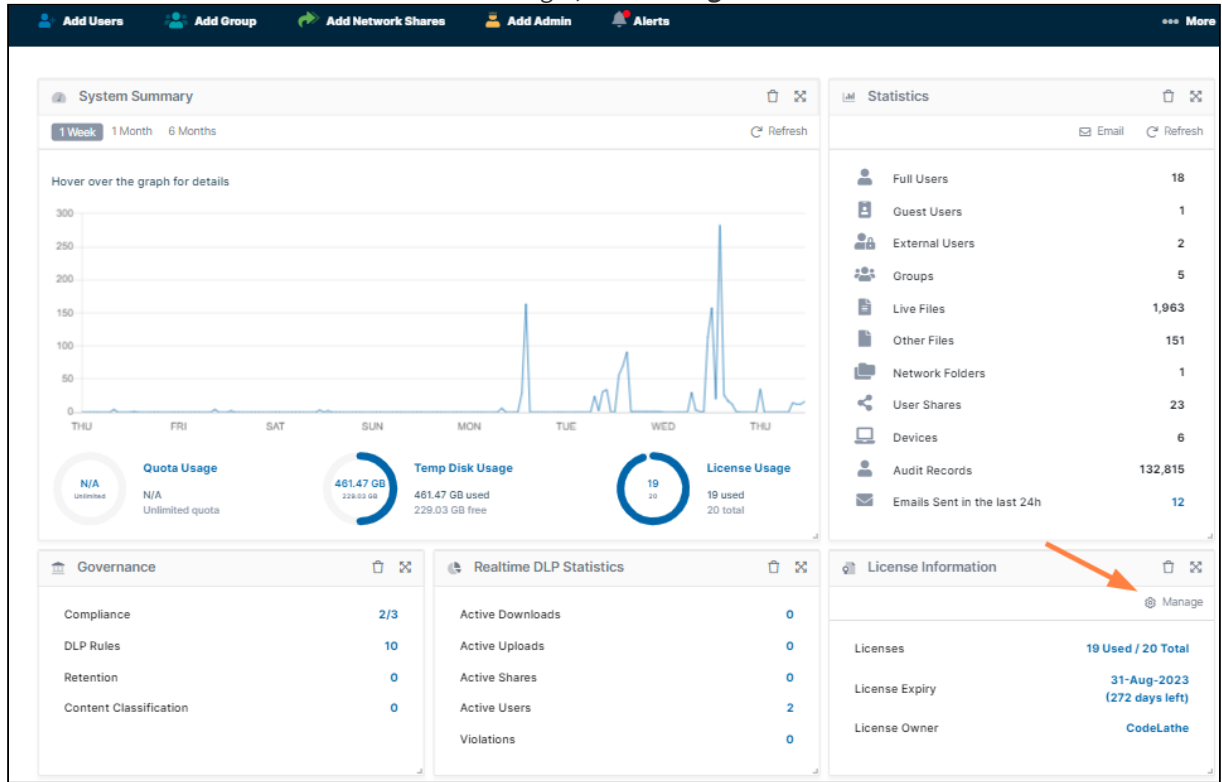
If you close the Admin dialog without installing a license, you can always use the FileCloud dashboard to manage your licenses. You can also use it to update a license.

The dashboard opens the same window that opens when you click **Settings > License**.

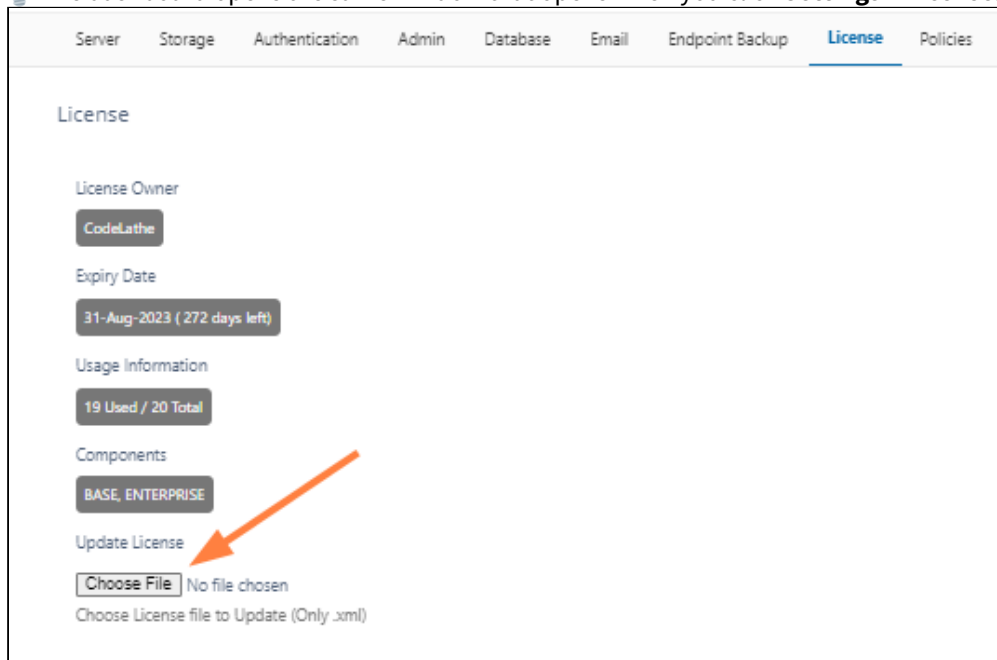
To install your license from the Dashboard:

1. Log in to the **Admin Portal**.

2. In the dashboard's the **License Information** widget, click **Manage**.



The dashboard opens the same window that opens when you click **Settings > License**.



3. On the **License** page, click the **Choose File** button.
4. Select the license.xml file and click **OK**.
5. On the License page, click **Save**.

Also see:

- [Installing FileCloud License On Multiple Sites](#)
- [Viewing Your License Details](#)

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](#)
- [Troubleshooting Workflows](#)

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 ..

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

```
{
  "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

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="591 279 927 947"> { "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>	<p>This condition will be triggered when an uploaded file is bigger than the size specified.</p> <p>size- specifies the maximum expected file size in MB.</p>

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 ...	<i>None</i>	<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

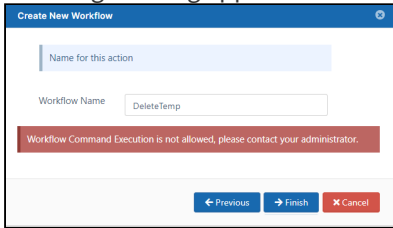
Action	Parameters	Details	Compatible IF conditions
Verify file integrity and delete on mismatch	<pre>{ "ignore_file_size_in_mb": "10" }</pre>	<p>Attempts to identify file type based on its content and checks if it matches its mime type.</p> <ul style="list-style-type: none"> A MIME type is a string identifier 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>

Running commands

Action	Parameters	Details	Compatible IF conditions
Execute a command	<pre>{ "command_line": "rm -rf /tmp/scratch" }</pre>	<p>Executes the command line.</p> <p>command_line: - Command line syntax to be executed. Admin is notified after the command runs. The following placeholders are available: <i>%who</i>, <i>%when</i>, <i>%path</i>, <i>%how</i>, <i>%filename</i>. See Set Advanced Workflow Options.</p> <p>The placeholders. <i>%who</i>, <i>%when</i>, <i>%path</i>, <i>%how</i>, <i>%filename</i> are available for this action.</p> <p>Beginning in FileCloud 23.1, by default, the Execute a command action is not available for admin users.</p> <p>If an admin user selects the action and tries to save the workflow, the following warning appears:</p>  <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>i To enable admin users to choose the Execute a command option, add:</p> <ol style="list-style-type: none"> Open cloudconfig.php: Windows Location: XAMPP DIRECTORY/ htdocs/config/ cloudconfig.php Linux Location: /var/ www/config/ cloudconfig.php Add the following: </div>	<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 <p>Perform an action periodically at specified time and interval</p> <p>Perform an action on the specified date</p> <p>Perform an action periodically</p>

Action	Parameters	Details	Compatible IF conditions
		<pre>define("TONI DOCLOUD_ALLO W_ADMIN_WORK FLOW_COMMAND _EXECUTION", 1);</pre>	

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.

Manage Workflows

Workflow + Add Workflow

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"/>	Edit ▶ ⏸ ✎ ↺ ✖
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"/>	Delete ▶ ⏸ ✎ ↺ ✖
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"/>	▶ ⏸ ✎ ↺ ✖

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" }
```

➔

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

IF Condition ..


Required Parameters

```
{ "last_login_days_ago": "30", "user_account_type": "USER_ACCOUNT_ANY", "day_interval": "5" }
```

THEN Action ..

Required Parameters

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



Set Advanced Workflow Options

i 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:

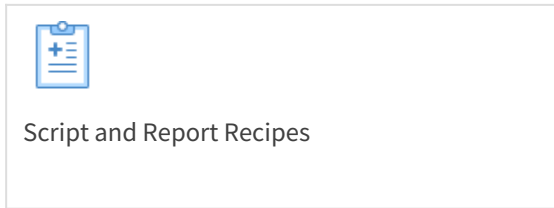
- IF CONDITION - THEN ACTION (IFTTT)

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?

 <p>File Management Recipes</p>	<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
 <p>User Monitoring Recipes</p>	<ul style="list-style-type: none"> ➔ Detect and Generate a List of Inactive Users ➔ Detect and Notify Inactive Users ➔ Detect and Disable Inactive Users
 <p>Client Security Recipes</p>	<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

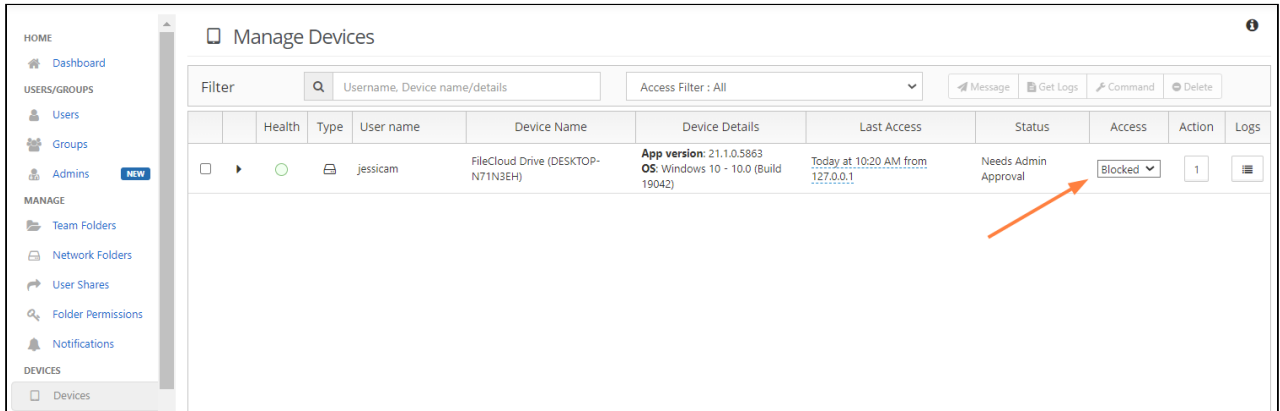
7. Click on Next, No workflow are required for this action

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" (blue with a left arrow), "Next" (blue with a right arrow), and "Cancel" (red with an X).

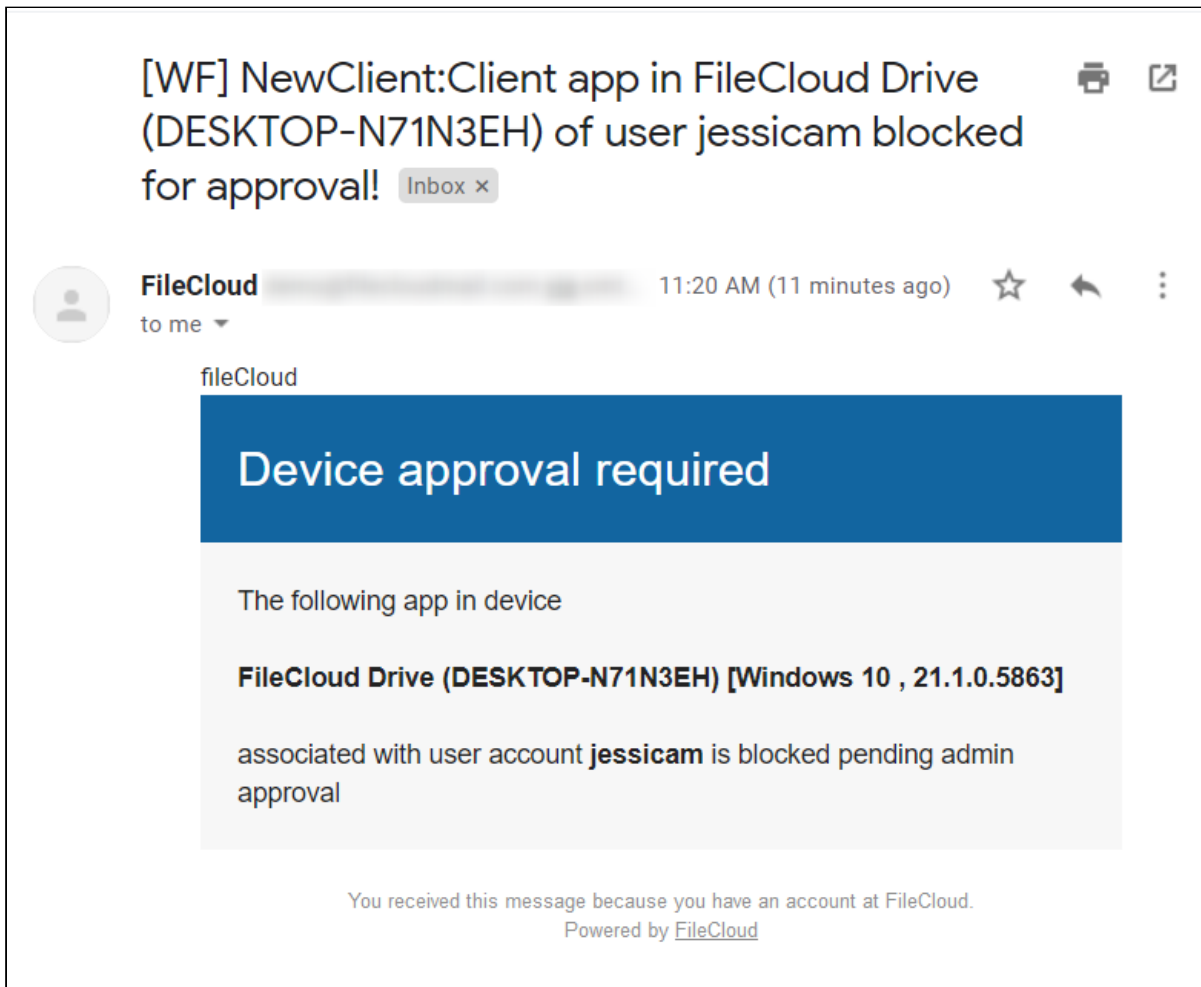
8. Click on Next, to give workflow name

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" (blue with a left arrow), "Finish" (blue with a right arrow), and "Cancel" (red with an X).

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. The title bar is blue with the text 'Create New Report' and a close button. Below the title bar is a light blue box with the text 'Select the report from the list'. Underneath is a label 'Select Report to Create' followed by a dropdown menu showing 'Get user login report' with a downward arrow. At the bottom right are two buttons: a blue 'Next' button with a right arrow and a red 'Cancel' button with an 'X'.

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",}
```

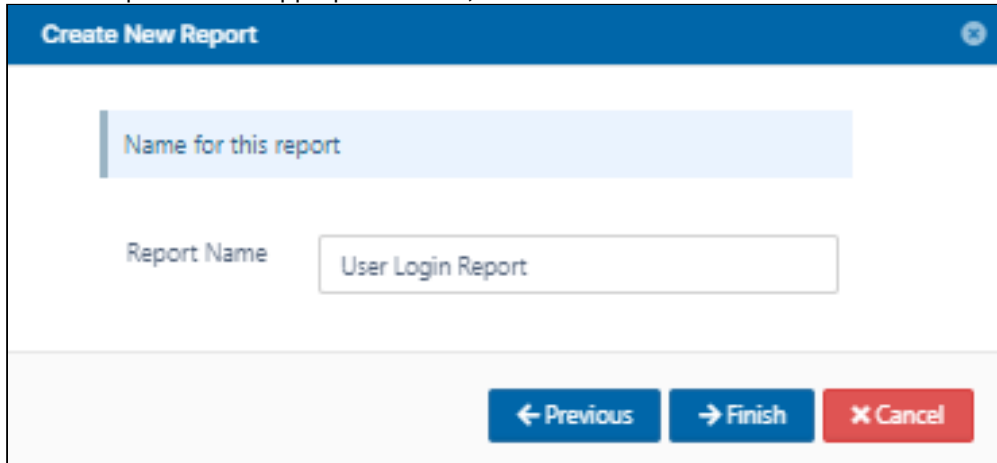
Generate a report of login. If no parameters are supplied, last 7 days are retrieved by default.
from_date : (OPTIONAL) From date in Y-M-d H:i:s format.
to_date : (OPTIONAL) To date in Y-M-d H:i:s format.
last_number_of_hours : (OPTIONAL) Number of last hours from now.

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"}
```

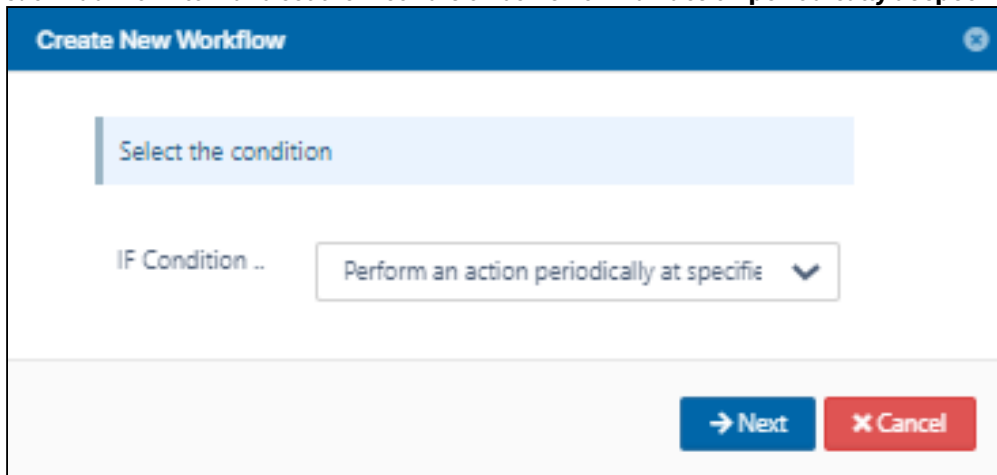
[← Previous](#) [→ Next](#) [✕ Cancel](#)

6. Save the report with an appropriate name, and click **Finish**.



The screenshot shows a dialog box titled "Create New Report" with a close button in the top right corner. Inside the dialog, there is a light blue input field with the placeholder text "Name for this report". Below this, there is a label "Report Name" followed by a text input field containing the text "User Login Report". At the bottom of the dialog, there are three buttons: a blue button with a left arrow and the text "Previous", a blue button with a right arrow and the text "Finish", and a red button with a white 'X' and the text "Cancel".

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**.



The screenshot shows a dialog box titled "Create New Workflow" with a close button in the top right corner. Inside the dialog, there is a light blue input field with the placeholder text "Select the condition". Below this, there is a label "IF Condition .." followed by a dropdown menu showing the selected option "Perform an action periodically at specific" with a downward arrow. At the bottom of the dialog, there are two buttons: a blue button with a right arrow and the text "Next", and a red button with a white 'X' and the text "Cancel".

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.

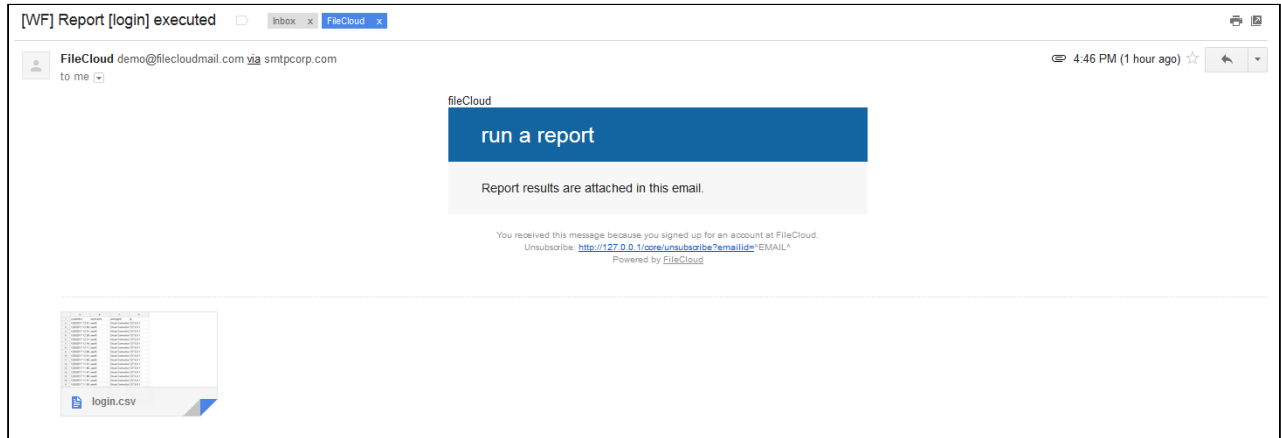
Create New Workflow ✕

Name for this action

Workflow Name

← 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](#).

- Click **Next**.
- Set **THEN Action** to **Delete the file(s)**.

- 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.com,hr@management.com"
}
```

Disable user and send email after performing this action.
comma_separated_email_id: Email ids in comma separated format as shown below
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**.

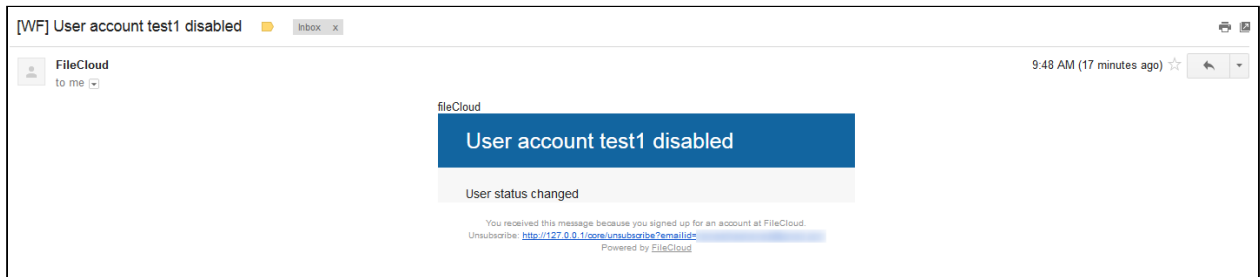
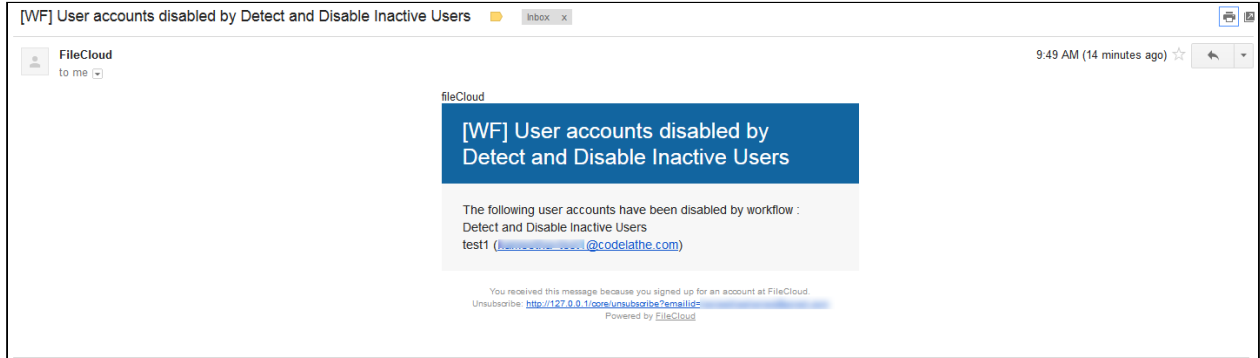
Create New Workflow

Name for this action

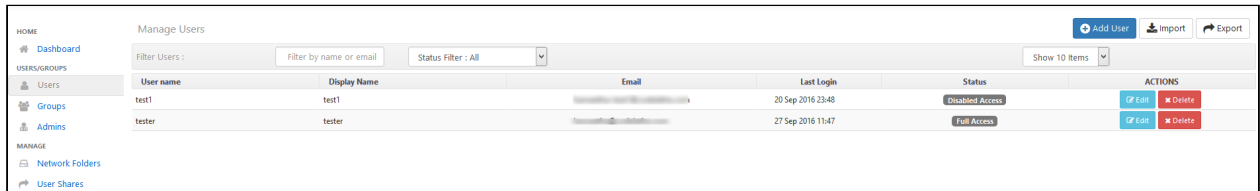
Workflow Name

← 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": "/johndo
e",
  "number_of_days": 7,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*"
}
```

For example:

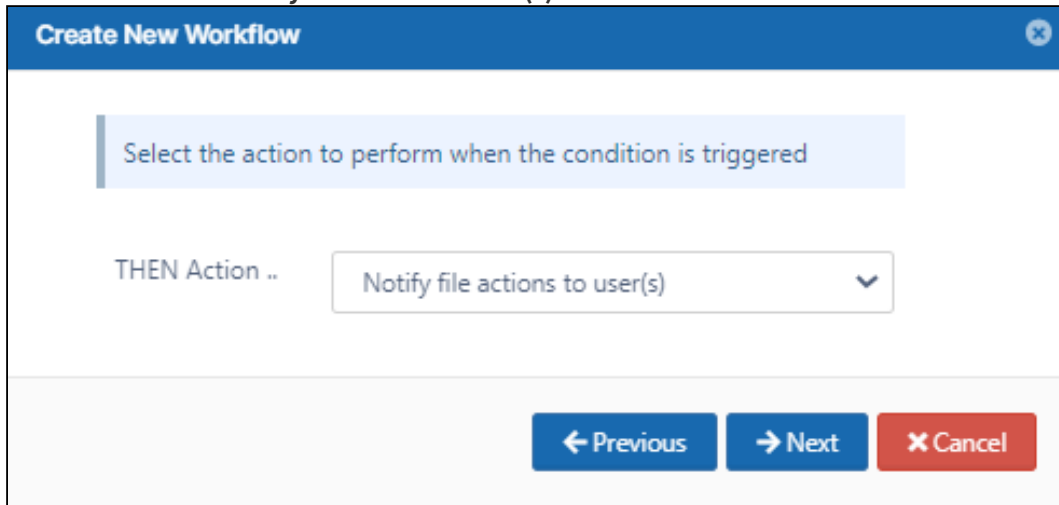
```
{
  "parent_folder_path_string": "/jenniferp",
  "number_of_days": 15,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
```



```
"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**.

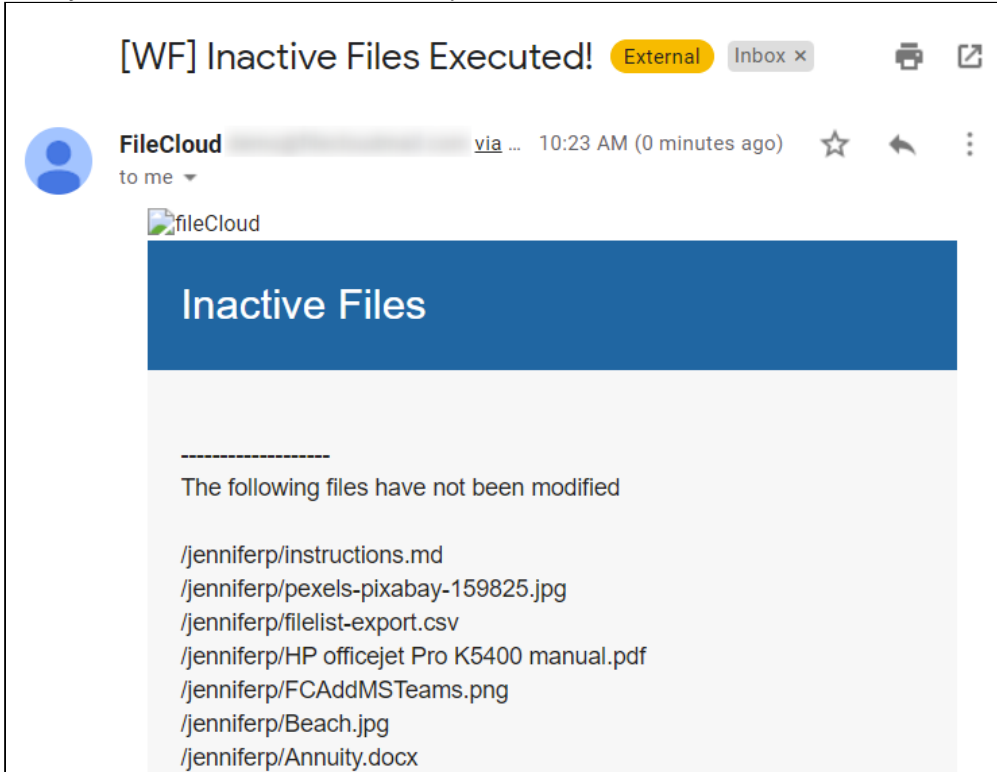
Create New Workflow [Close]

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

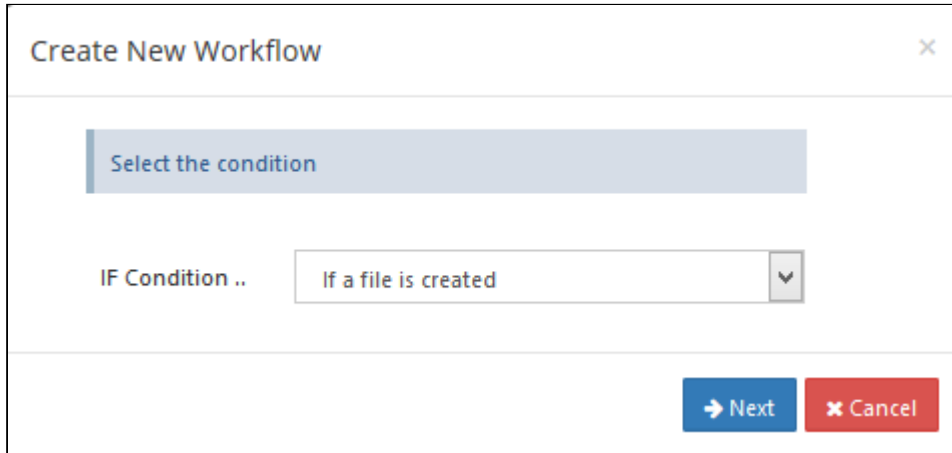
This workflow recipe creates an ALERT notification when a file is created or uploaded to FileCloud with a signature mismatch.

- 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

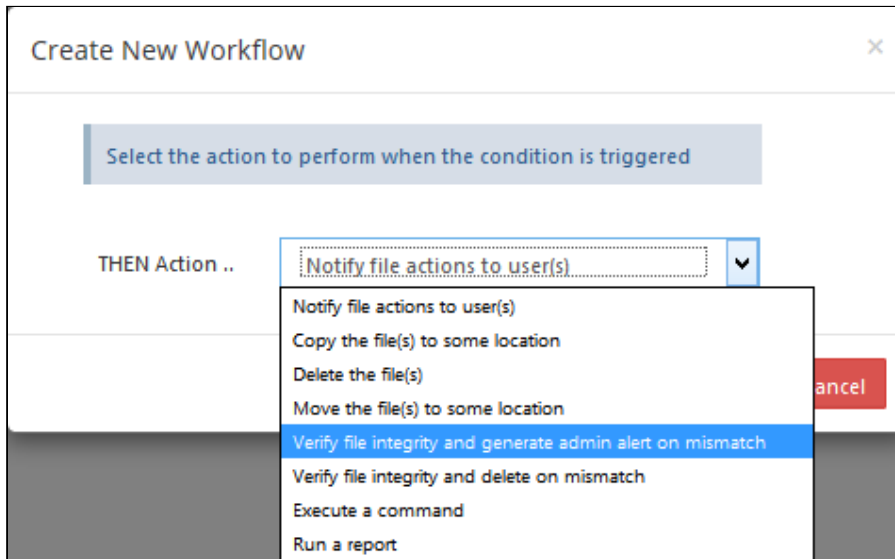
use_regex (optional): specifies whether path has a regex format

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

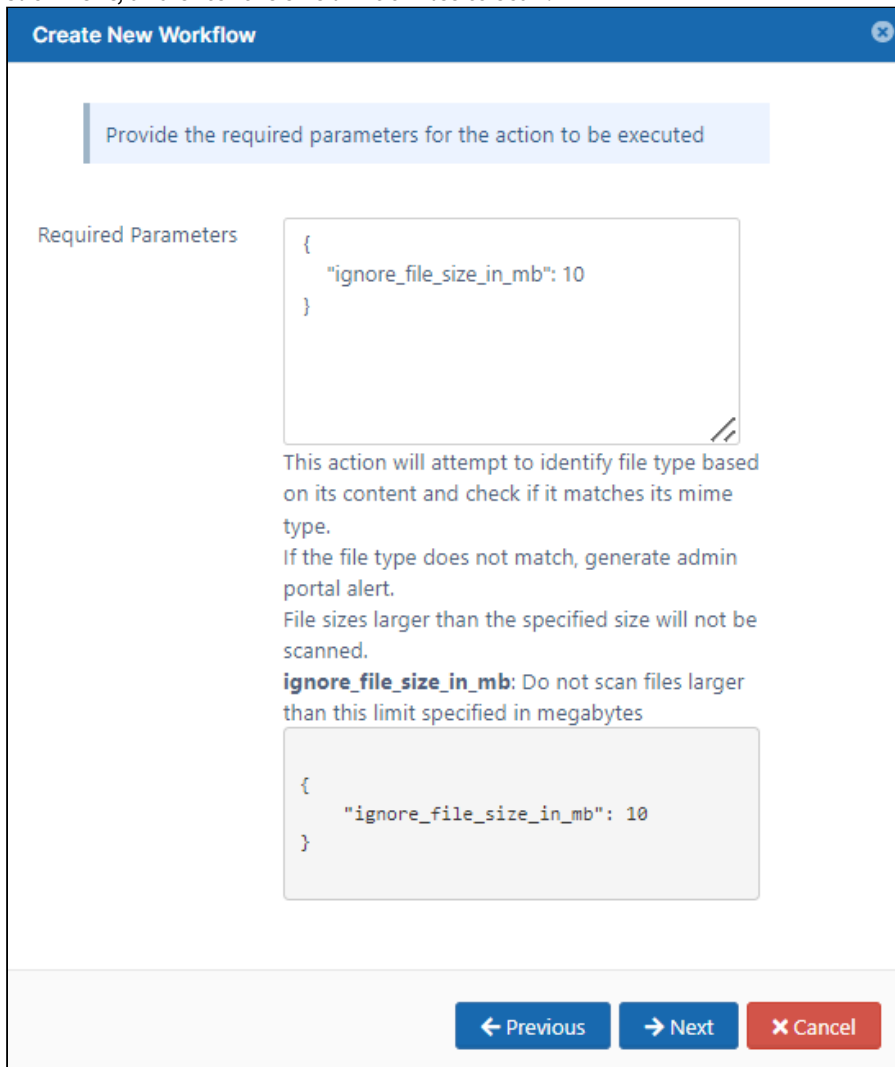
```
{
  "parent_folder_path_string": "/userid/
somepath",
  "use_regex": 1,
  "exclude": 1
}
```

← Previous → Next ✕ Cancel

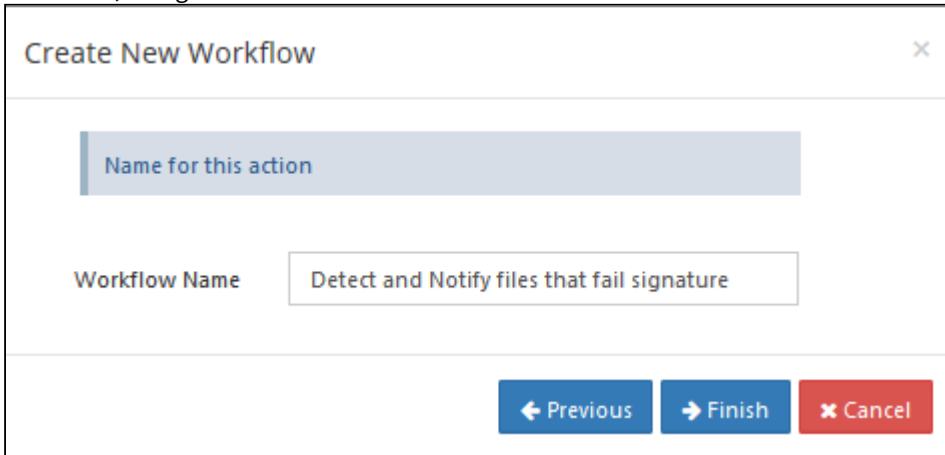
7. Click **Next**, and set **Then Action** to **Verify file integrity and generate admin alert on mismatch**



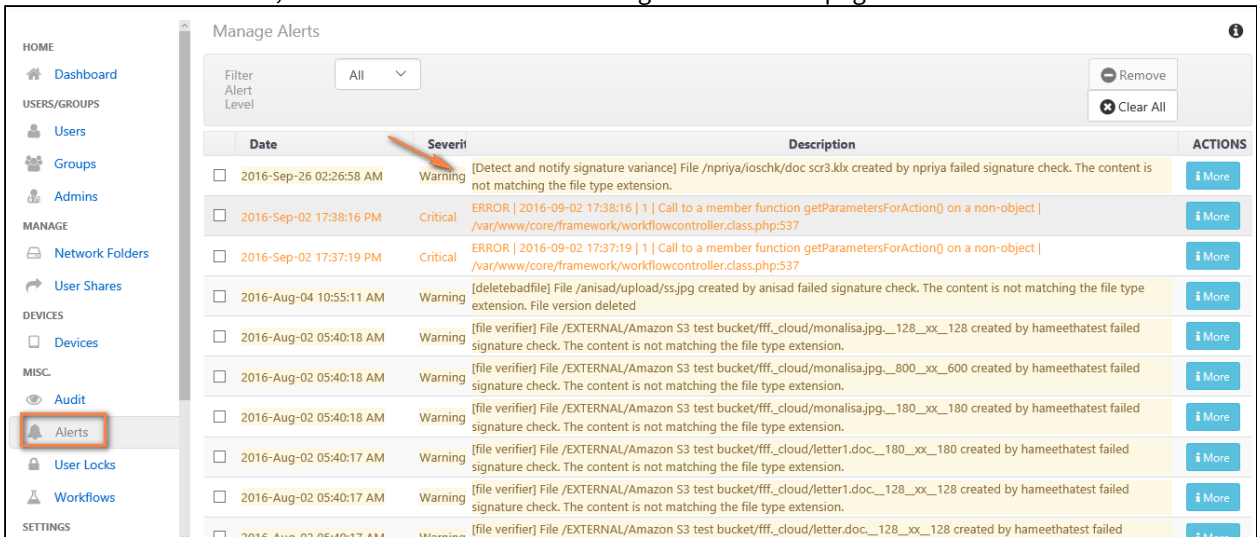
8. Click **Next**, and enter the size limit of files to scan.



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	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**.

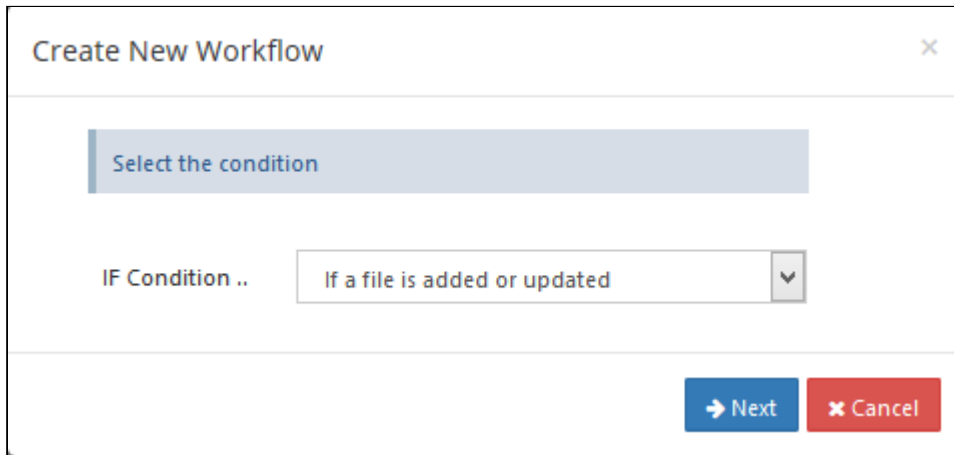
Notify on File Upload Workflow

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 .. If a file is added or updated

Next Cancel

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

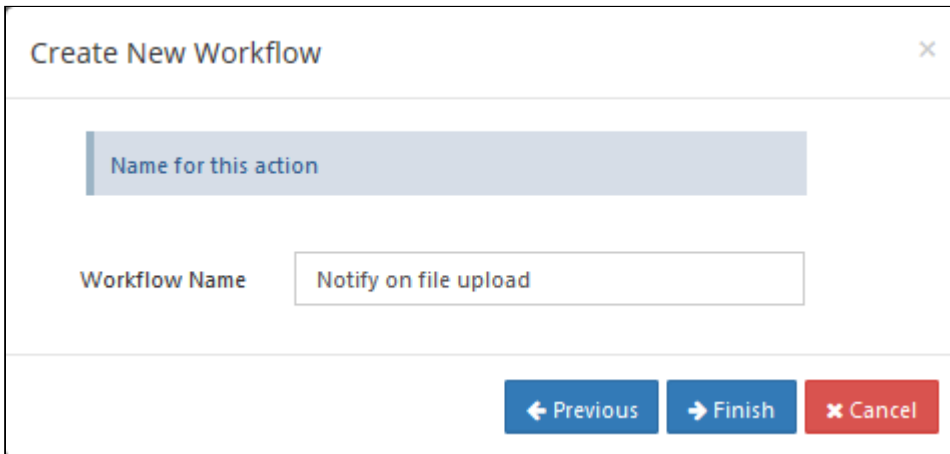

```
{
  "comma_separated_email_id":"admin@abc
  company.com,hr@management.com"
}
```

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

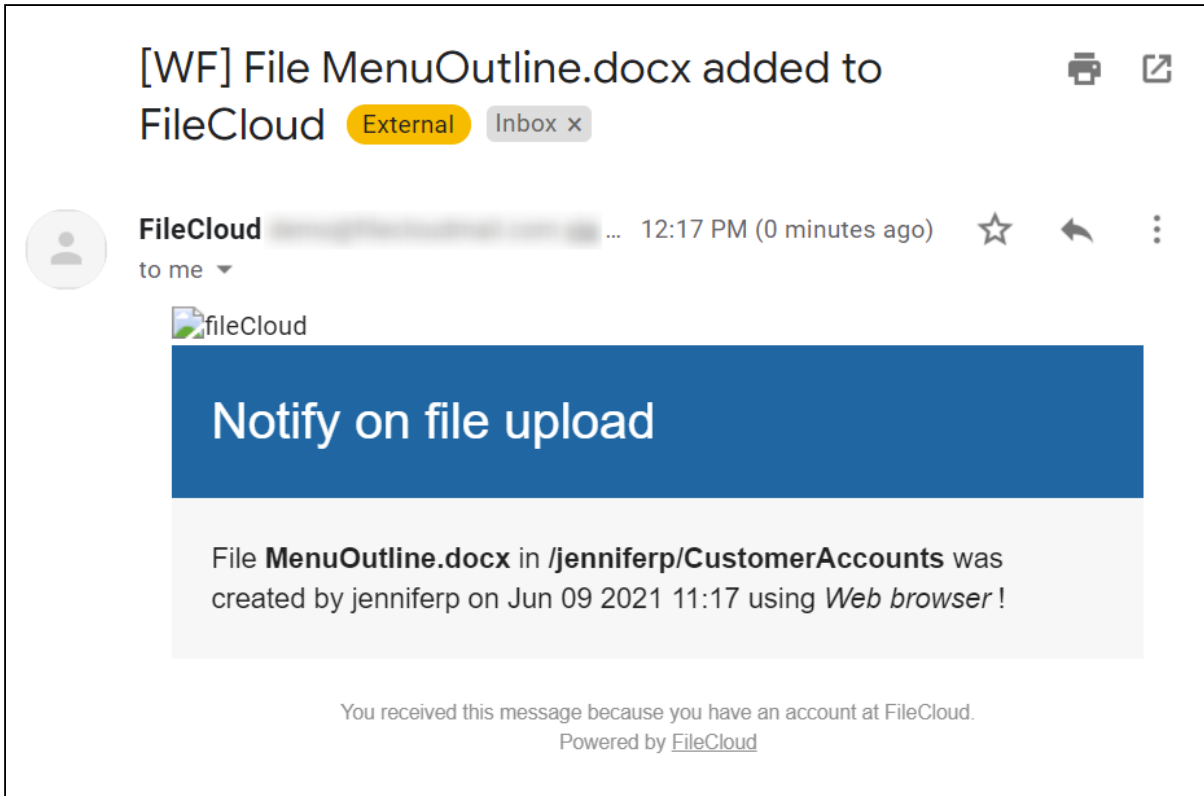

```
{
  "comma_separated_email_id":"xyz@a.com,abc@b.com"
}
```

← 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

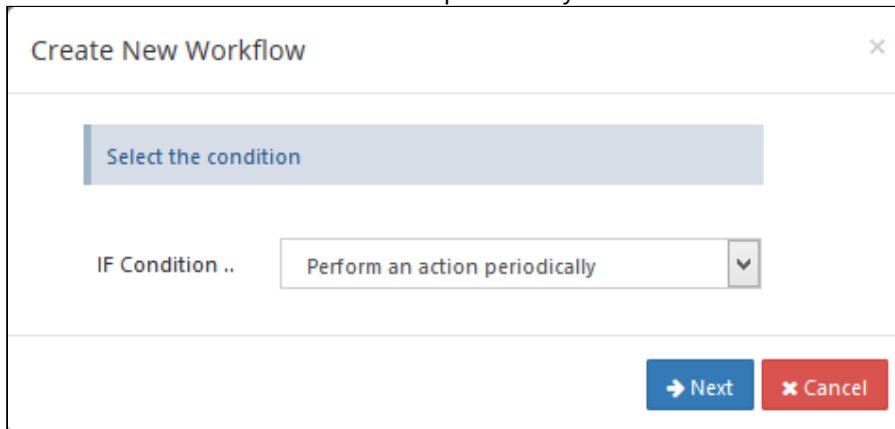
This workflow recipe runs a specified command at a periodic interval.

- 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 "



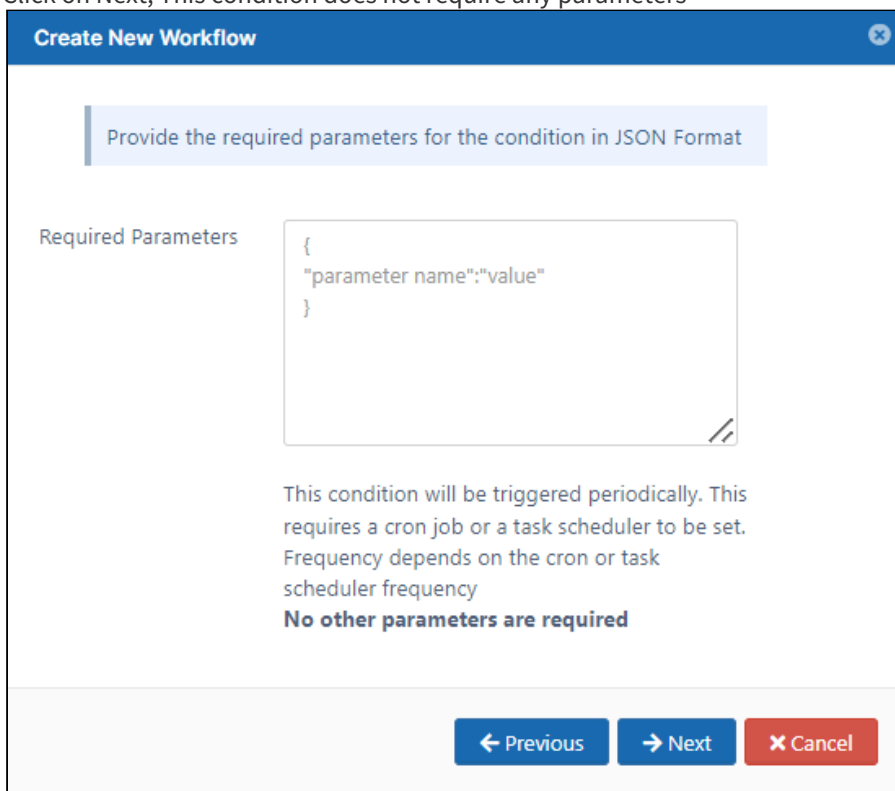
Create New Workflow

Select the condition

IF Condition .. Perform an action periodically

Next Cancel

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



Create New Workflow

Provide the required parameters for the condition in JSON Format

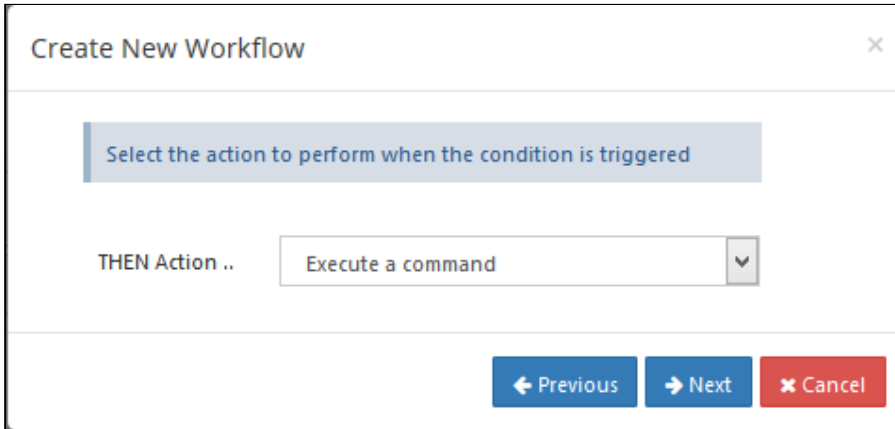
Required Parameters

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

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
No other parameters are required

Previous Next Cancel

- Set the Then Action "Execute a command"



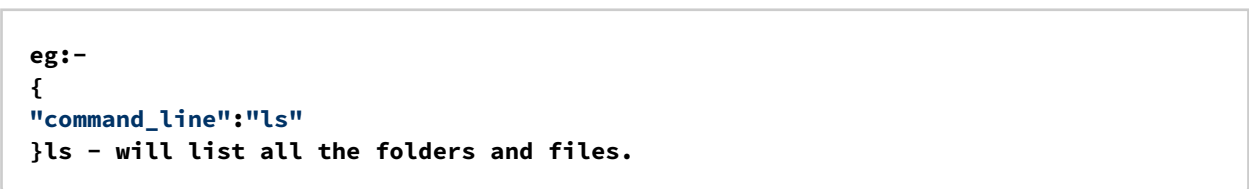
Create New Workflow

Select the action to perform when the condition is triggered

THEN Action .. Execute a command


Previous Next Cancel

- Enter the required Command



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

- Enter the Workflow name and Finish.



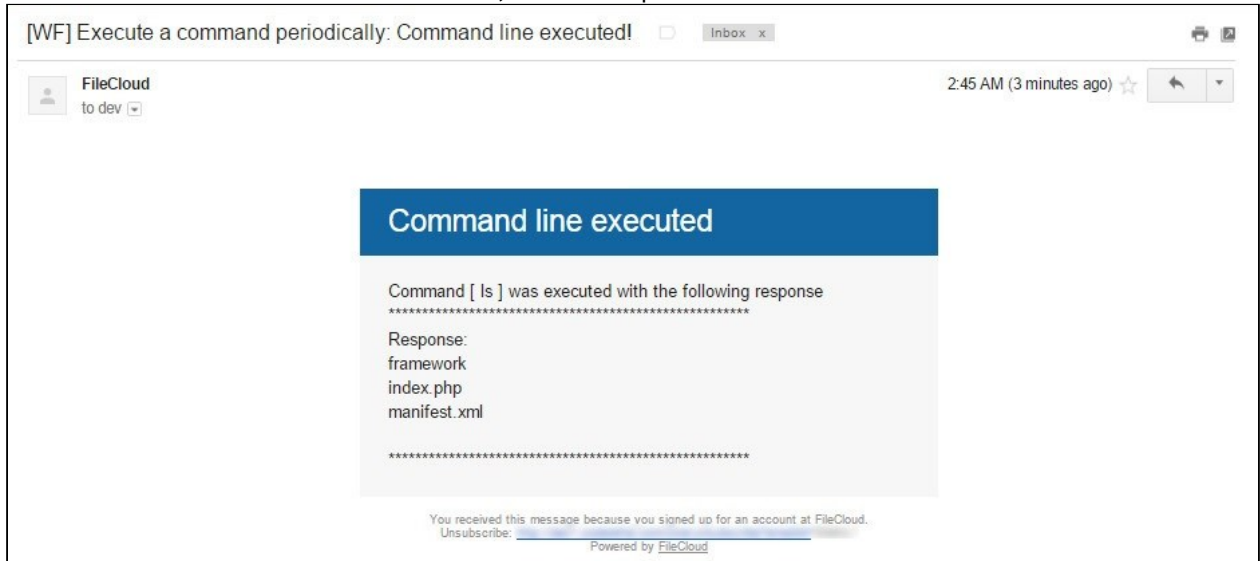
Create New Workflow

Name for this action

Workflow Name Execute a command periodically

Previous Finish Cancel

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



Run workflows commands with /tmp paths in Linux systems

When using Linux as OS for Filecloud systems, some workflows include the /tmp folder.

By default, using the /tmp folder with command workflows does not work as expected because the fcorchestrator services have a private /tmp folder

To change that behavior we need to disable the private tmp folder of fcorchestrator. To do that:

1. Edit the file `/etc/systemd/system/fcorchestrator.service`

```
>> vi /etc/systemd/system/fcorchestrator.service

[Unit]
Description= Filecloud Queue service
After=httpd.service

[Service]
Type=simple
PIDFile=/run/fcorchestrator.pid
ExecStart=/bin/sh -c '/usr/bin/node /var/www/html/src/Scripts/fcorchestrator.js'
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s QUIT $MAINPID
WorkingDirectory=/var/www/html/src/Scripts/
PrivateTmp=yes
User=www-data
Restart=always
SuccessExitStatus=143

[Install]
WantedBy=multi-user.target
```

2. Change **PrivateTmp** to **no** and execute the command "**systemctl daemon-reload**" and then restart **fc-orchestrator** with "**service fcorchestrator restart**"

```
>> vi /etc/systemd/system/fcorchestrator.service

[Unit]
Description= Filecloud Queue service
After=httpd.service

[Service]
Type=simple
PIDFile=/run/fcorchestrator.pid
ExecStart=/bin/sh -c '/usr/bin/node /var/www/html/src/Scripts/fcorchestrator.js'
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s QUIT $MAINPID
WorkingDirectory=/var/www/html/src/Scripts/
PrivateTmp=no
User=www-data
Restart=always
SuccessExitStatus=143

[Install]
WantedBy=multi-user.target

>> systemctl daemon-reload

>> service fcorchestrator restart
```

Troubleshooting Workflows

- [Integrity Check Not Working in Linux](#)

Integrity Check Not Working in Linux

An integrity check workflow attempts to determine if the content in a file is different from what is expected for the file's extension.

Update Workflow ✕

Workflow Name	<input type="text" value="Check file integrity"/>
IF Condition ..	<div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;">If a file is created</div> ▼
Required Parameters	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">{"parent_folder_path_string":"V"}</div>
THEN Action ..	<div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;">Verify file integrity and generate admin ale</div> ▼
Required Parameters	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">{"ignore_file_size_in_mb":"10"}</div>

Update
Cancel

If you are working in a Linux environment, and the logs for the workflow indicate that it cannot detect the file type, the workflow will not be able to perform its integrity check.

This may be due to problems with the locale settings.

To fix this, remove the existing locale and install a new one by entering the following into a command line.


Note: It is important that you include the `--no-archive` flag.

```
rm -f /usr/lib/locale/locale-archive  
locale-gen --no-archive  
locale-gen --no-archive en_US.utf8
```

If you are using any additional locale settings, for example, ru_RU.utf8, newly install them as well:

```
locale-gen --no-archive ru_RU.utf8
```

Automated Workflow Management

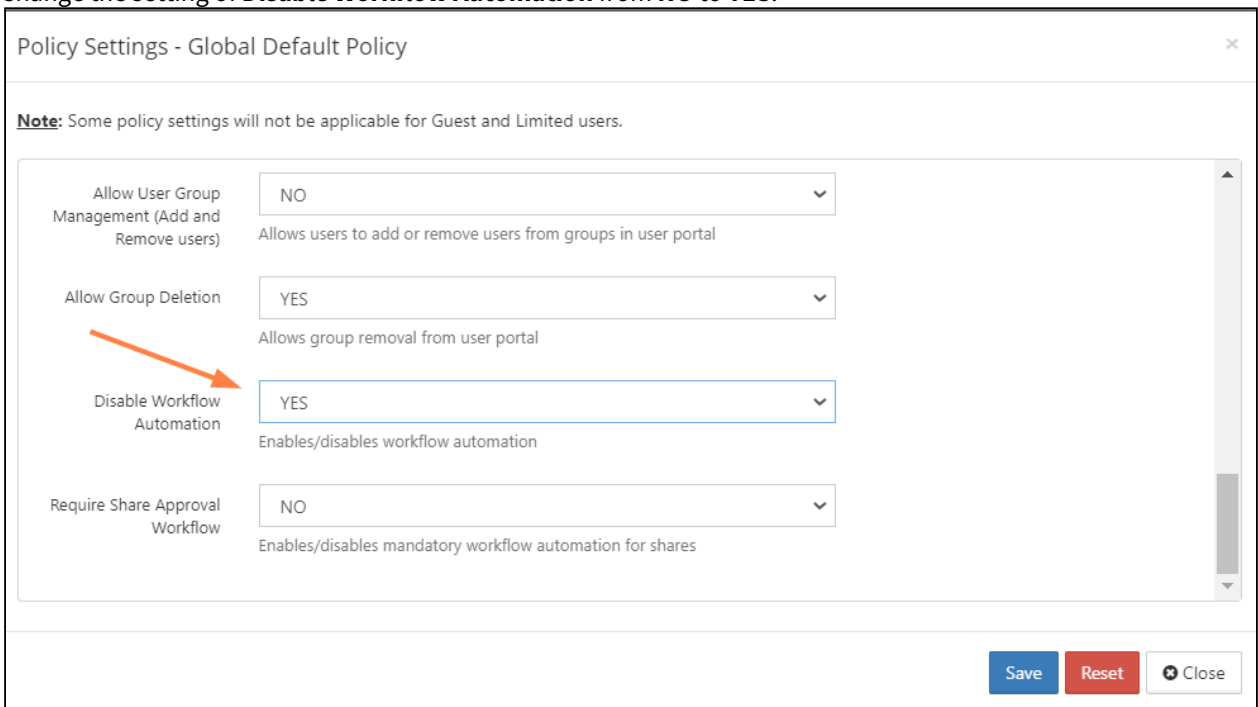
 Automated Workflows are available in FileCloud 21.2 and later.

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>

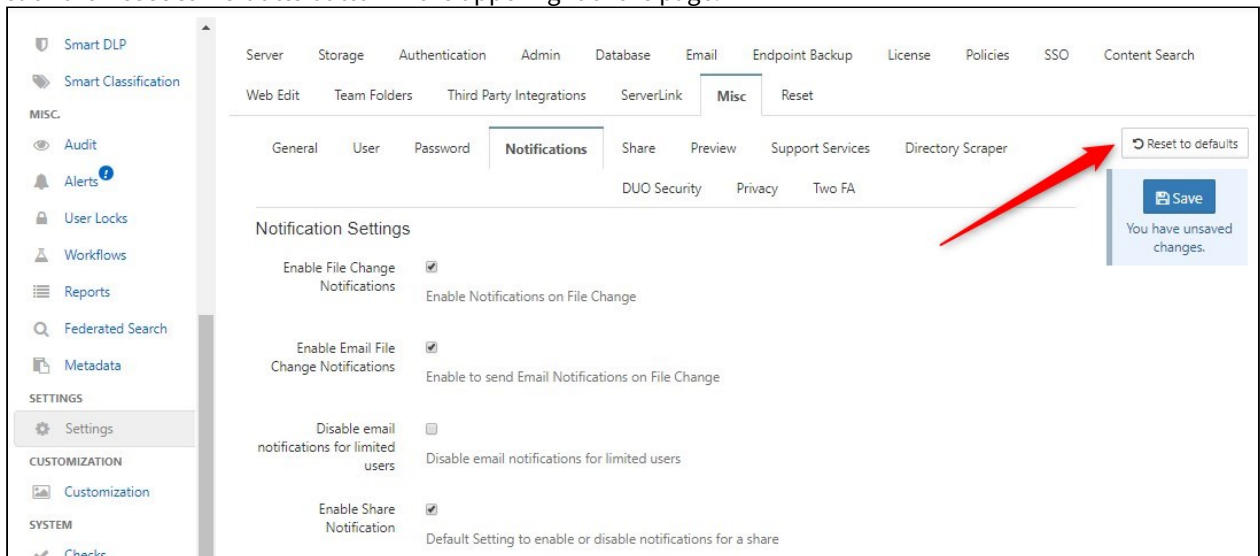
For end user information on creating Automated Workflows, see [Workflow Automation](#).

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.



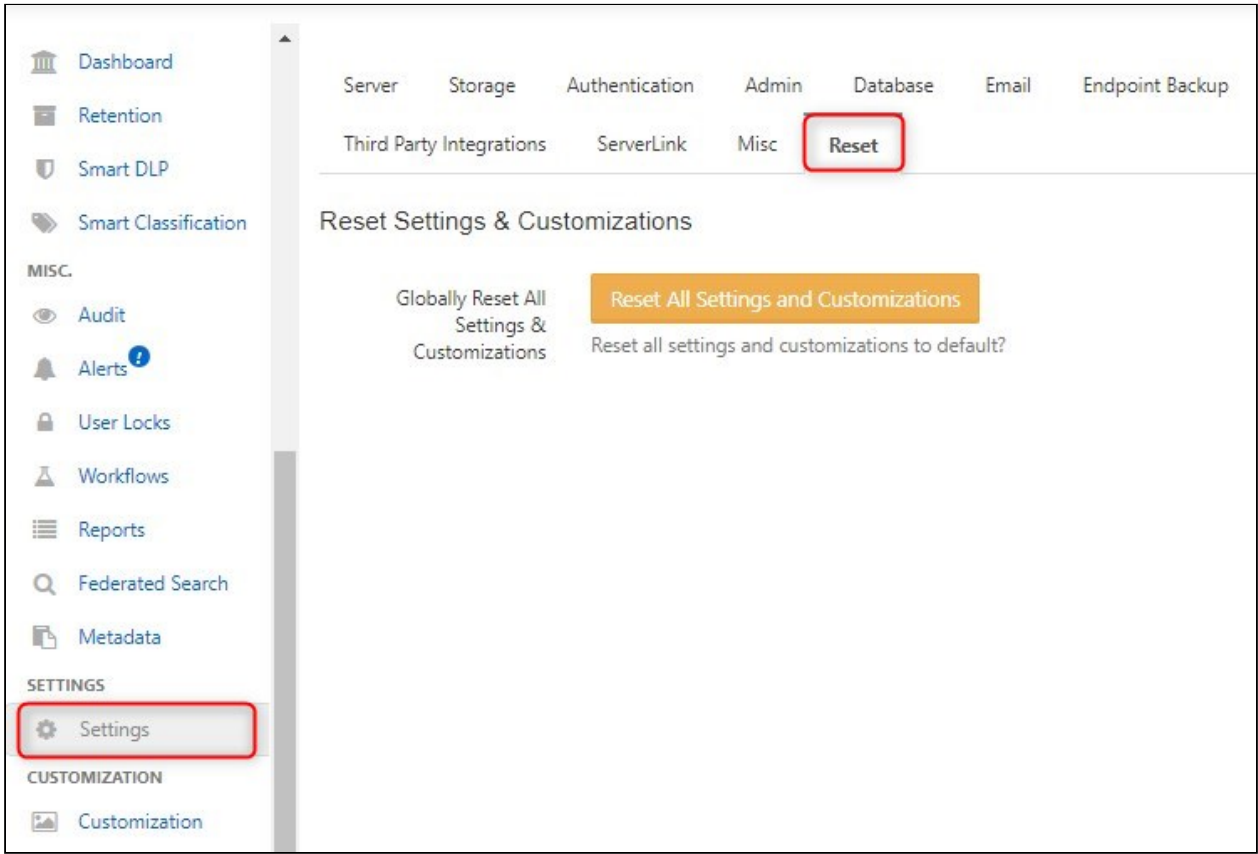
A confirmation dialog box opens.

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.