

FileCloud Server

Version 23.262

FileCloud Site Maintenance

10 July, 2026

Table of Contents

Admin Portal Dashboard	2
Setup Checklist	2
Quick Actions	4
Dashboard Widgets	4
Release Notifications	19
By Subscribing to the Mailing List	19
By seeing the version update in the FileCloud Admin Portal	19
Managing Users	20
Listing FileCloud Users.....	20
Viewing User Properties.....	21
Disable a FileCloud User Account	31
Deleting a FileCloud User	32
Resetting a User Password.....	35
Manage A User's Policies.....	37
Manage a User's Profile Picture	40
Change a User's Email Address	41
Setting a User Account to Expire	42
Send Email from User Details	43
Managing Groups	45
Change a User Group Name	45
Delete a User Group.....	45
View and Change Group Members.....	46
Exporting a list of users in a group	47
View and Change Group Admins	48
View and Change a Group's Policy	49
View and Change an SSO-imported Group's Sync Options.....	50
Managing Admin Users.....	52
Check an admin user's permissions.....	52
Remove an admin role.....	54

Managing User Folders and Files	56
Add Folder-Level Permissions to User Folders.....	58
Copy and Move User Files.....	61
Download User Files and Folders	62
Cancel User Uploads in Progress	65
Delete User Folders and Files	66
Clear a Recycle Bin	67
Remove a User's Old File Versions	71
Remove Incomplete User Uploads	72
Restore a Previous File Version	73
Critical Section Cleanup Tool.....	76
Change the Name of the Zip File for Multiple File Downloads	79
Managing Team Folders	81
To view the breakdown of data in Team Folders:	83
To edit the Team Folders account fields:	83
To lock the Team Folder account:.....	84
To manage Team Folder shares:.....	85
To reset the Team Folder account password:	86
To manage Team Folder notifications	87
To delete the Team Folder account:.....	88
Search for a Team Folder.....	90
Recover Deleted Files	90
View and Restore Previous Versions in Team Folders	92
Managing User Shares	95
To manage user shares for an individual user:.....	95
To manage user shares for all users:.....	97
To export a list of all shares:.....	98
Transfer Ownership of a Reshare from a Team Folder or Network Share.....	99
Creating direct file download link from a public file share	101
Creating direct file download links from a public folder share.....	101
Managing Storage Space Usage	105
In this section.....	105

Related topics	105
Storage Scanner Tool for Missing Files	105
Storage Usage Tool	107
Thumbs Tool for Removing Excessive Thumb Files	108
Managing User Locks	111
Managing User-Defined Notifications	115
Editing individual user's file and folder notifications.....	115
Editing all users file and folder path notifications.....	118
Adding notifications for actions on user's files and folders	120
Managing Client Devices.....	122
FAQ's	123
How Do You Want to Manage a Device?.....	125
Centralized Device Management.....	129
iOS Device Management.....	186
Mass Deployment - Default Configuration Support.....	187
Search in the Admin Portal	201
FileCloud's Federated Search	201
All search.....	203
Audit Logs	212
What do you want to do?.....	212
View Audit Logs	212
Filter Audit Log Views.....	214
Compact the Audit Database.....	218
Configure What is Logged.....	218
Export Audit Logs	220
Delete Audit Log Entries.....	221
Change the Audit Log Warning Limit.....	229
Backing Up and Restoring FileCloud Server.....	231
What do you want to do?.....	231
The FileCloud Server Backup Tool.....	231
Backing Up and Restoring Linux.....	260
FileCloud Backup and Restore - Linux Manual	260

FileCloud Backup and Restore - Windows Manual	264
Migrating FileCloud Server to Another Server.....	266
Migrating a FileCloud Server Site	270
Enabling the Backup Server URL	270
Monitoring FileCloud	271
What do you want to do?.....	271
FileCloud Alerts.....	273
File Content Heuristic Engine.....	274
Identifying a FileCloud Specific Path.....	279
Custom Reports	281
Add Reports	281
Download Reports	284
Available Reports.....	284
Specifying Y-M-d H:i:s values.....	290
Manage Folder Level Permissions	292
To Edit Folder-Level Permissions	292
Read Only Sync	294
Managing Metadata	295
Metadata for governance and other system processes	295
Metadata for users	297
Metadata Components and Types	298
Create a New Metadata Set	301
Edit an Existing Metadata Set.....	304
Managing Metadata Attributes.....	306
Managing Metadata Permissions	307
Working with Built-In Metadata.....	311
Working with Custom Metadata	342
Working with Default Metadata	343
Troubleshooting Metadata	345
Finding files without metadata	346
Metadata Limitations/Recommendations.....	350
Managing FileCloud Licenses.....	352

FileCloud - License Purchase And Renewal	352
Install FileCloud License	370
Workflows - IFTTT	377
The Workflow Dashboard.....	377
Add a New Workflow	378
Define an IF Condition	379
Define a THEN Action.....	413
Edit a Workflow.....	429
Run a Workflow.....	430
Set Advanced Workflow Options	431
Workflow Recipes for FileCloud.....	437
Troubleshooting Workflows.....	486
Automated Workflow Management	489
Disabling Automated Workflows	489
Enable Sharing of Automated Workflows	490
Requiring a Share Approval Workflow.....	491
Reset Settings and Customizations	493
To return to default settings for options in Settings	493
To return to default settings for all options on the Settings pages:.....	493

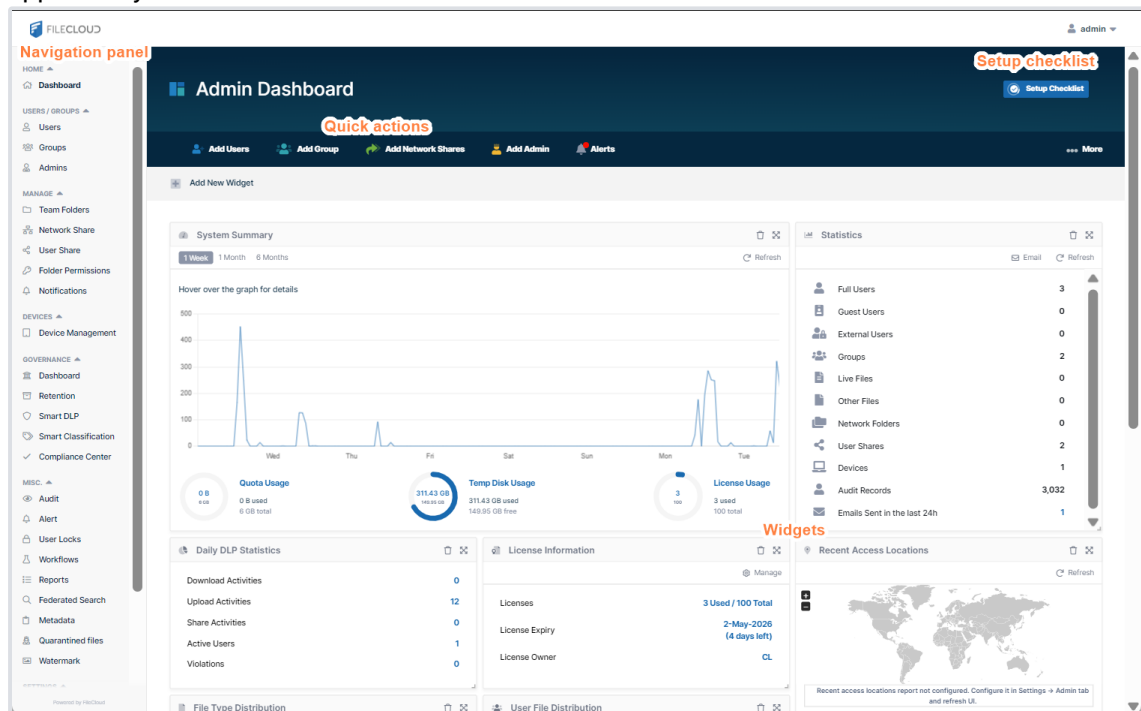
This section shows you how to monitor and maintain your FileCloud site, as well as how to edit and update its features and options.

Admin Portal Dashboard

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

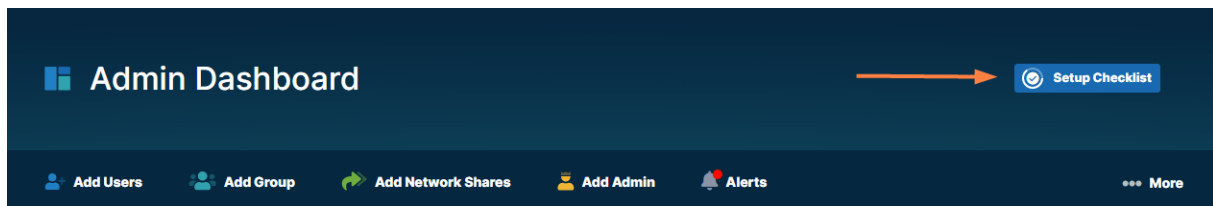
💡 The Admin dashboard displays several areas to help you manage your site.

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



Setup Checklist

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



The **Setup Checklist** includes various tasks generally necessary for setting up FileCloud, although some tasks may not apply to you.

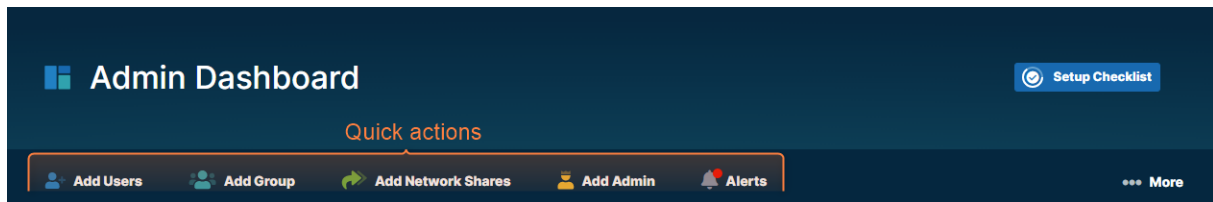
The tasks **Basic Installation Completed** and **Setup Cron Job** are automatically checked/unchecked for you, and you cannot modify them. All of the other tasks are not checked automatically, and you may check them manually to keep track of what you have completed.

The image shows a 'Setup Checklist' modal window. The title bar says 'Setup Checklist' with a close button (X). The content is organized into sections with blue headers: 'Basic', 'Authentication', 'Network Shares', and 'Sync and Backup'. Each section contains a list of tasks with checkboxes. Under 'Basic', 'Basic Installation Completed' is checked, while 'Setup 'My Files' Storage (Local or S3 or OpenStack)' and 'Setup Email Configuration' are unchecked. Under 'Authentication', 'Configure How Users are Authenticated (Local or AD or LDAP)' is checked, while 'Configure New Account Signup Policy' and 'Configure New Account Approval Policies' are unchecked. Under 'Network Shares', 'Enable or Disable Network Folder Access' is checked, 'Enable or Disable offline Sync of Network Folders' is unchecked, and 'Setup NTFS Helper Service (for NTFS file permissions)' is checked. The 'Sync and Backup' section is partially visible at the bottom. At the bottom of the modal are two buttons: 'Save' and '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

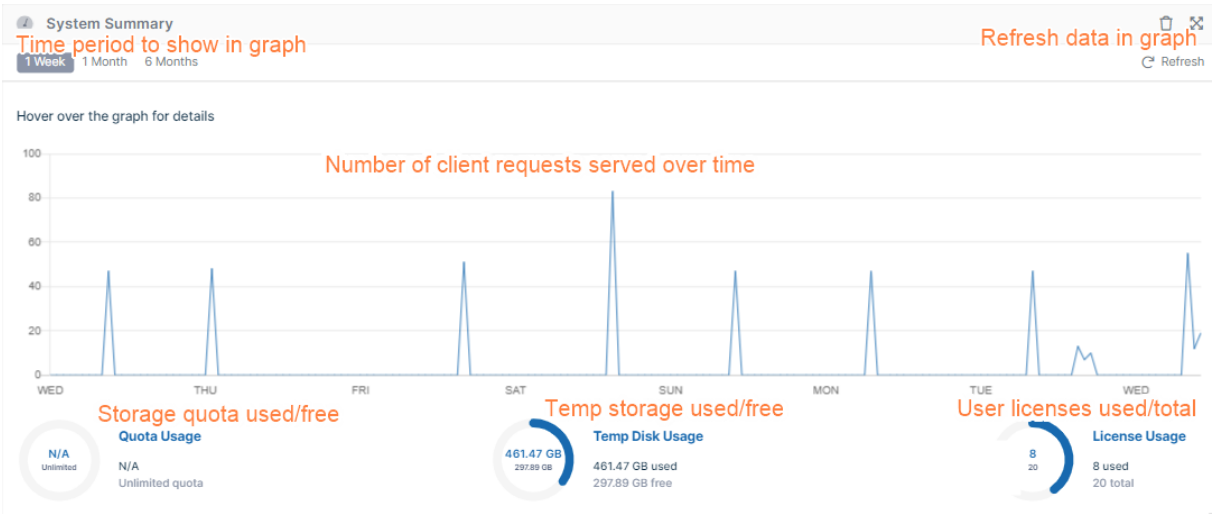
The FileCloud dashboard has widgets that display real-time information. If you are an Admin user, only those widgets involving actions you have access to are listed.

- 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.
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

Daily DLP Statistics

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

Daily DLP Statistics	
Download Activities	0
Upload Activities	12
Share Activities	0
Active Users	1
Violations	0

License Information

This widget shows you basic information about your license.

License Information

Manage

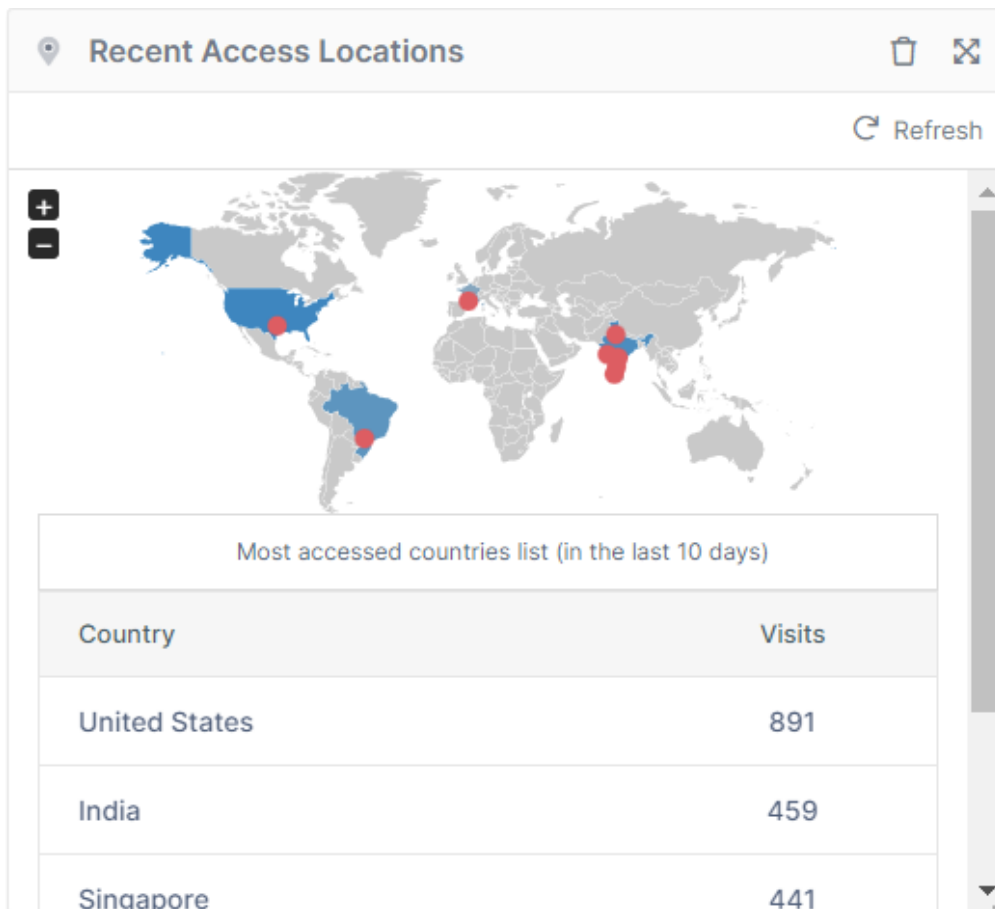
Licenses	15 Used / 500 Total
License Expiry	30-Aug-2022 (236 days left)
License Owner	CodeLathe Technologies Inc

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

Recent Access Locations

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

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



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

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

To enable the Recent Access Location report:

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

Show recent access locations in dashboard
Display the recent access locations chart in the admin dashboard. Default equals false.

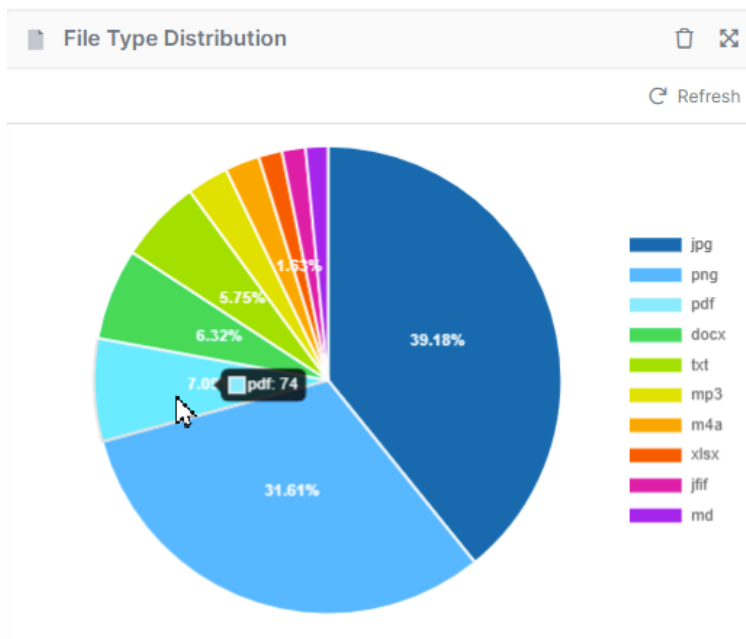
True ▼

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

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

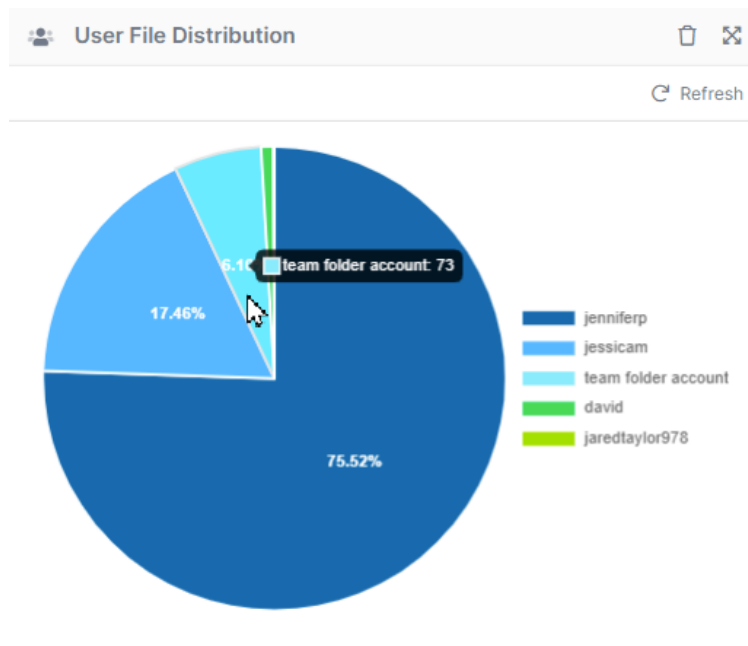
File Type Distribution

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



User File Distribution

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



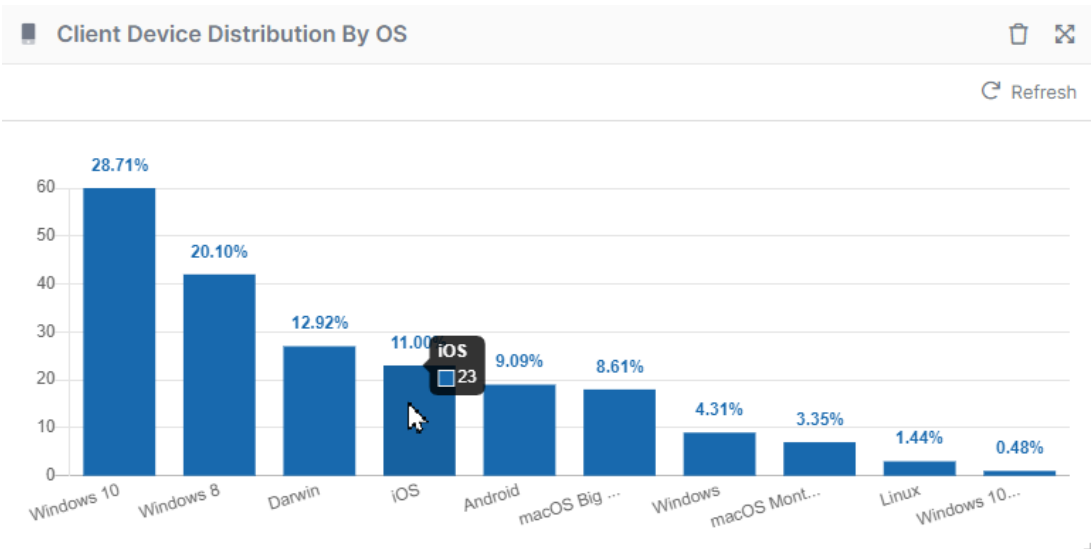
Version Information

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

Client Device Distribution by OS

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



Users with Lowest Quota Remaining

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

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

Users with Lowest Quota Remaining

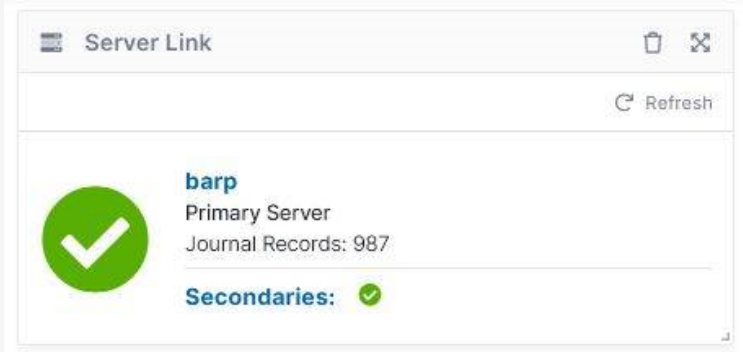
% Used	User name	File Count	Quota Used	Quota Assigned
	jenniferp	905	1.13 GB	2 GB
	jessicam	209	495.97 MB	2 GB
	team folder account	73	101.53 MB	0 B
	edwardtaylor978	1	523 KB	2 GB
	david	10	516 KB	2 GB

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.



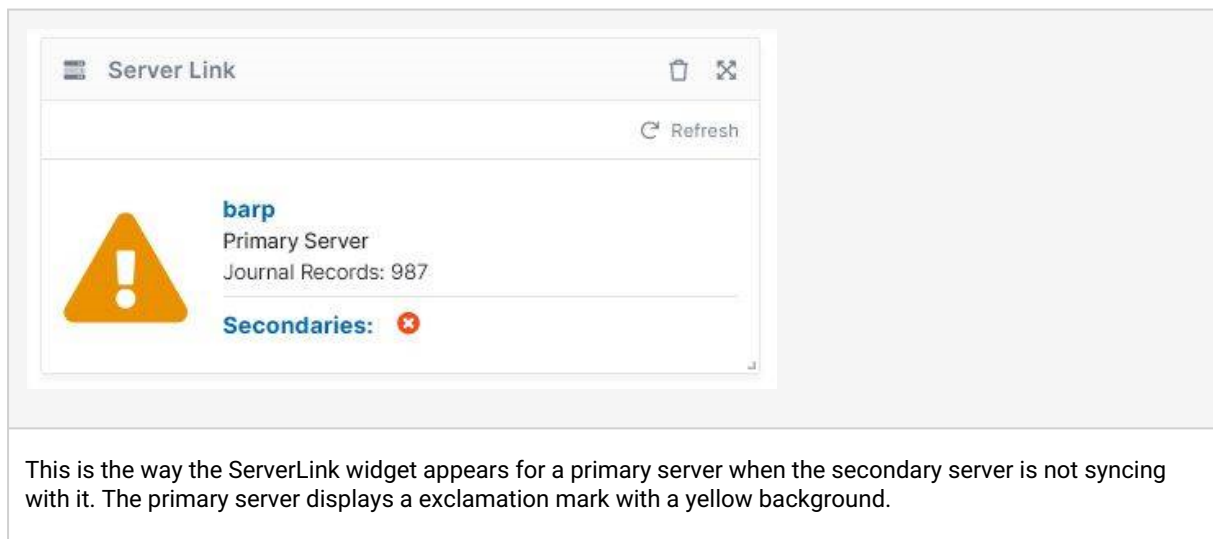
This is the way the ServerLink widget appears for a primary server with one secondary server. The check mark with a green background indicates that the server is running.

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 background indicates that the server is not running.

User signed into a primary server.

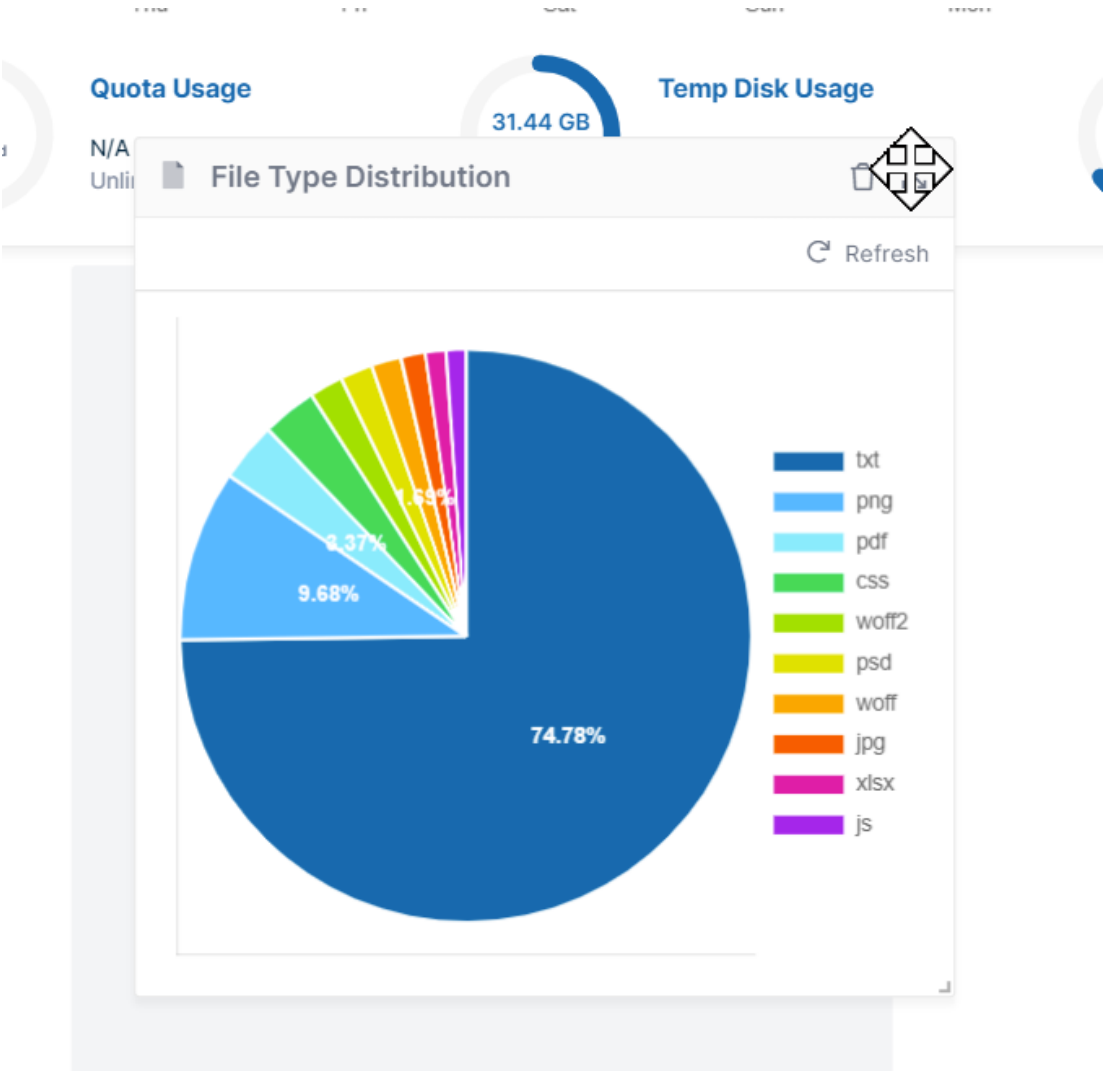


Journal Records indicates the number of log entries for ServerLink syncing actions.

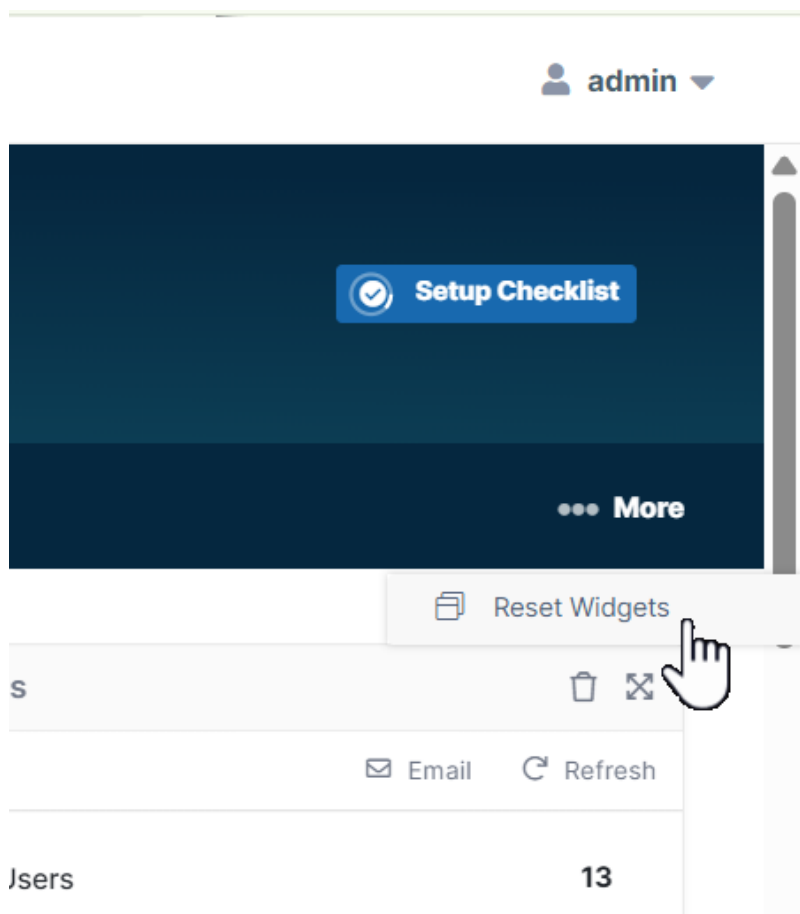
For more information, see [Viewing ServerLink Information](#).

Rearranging and resetting widgets

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

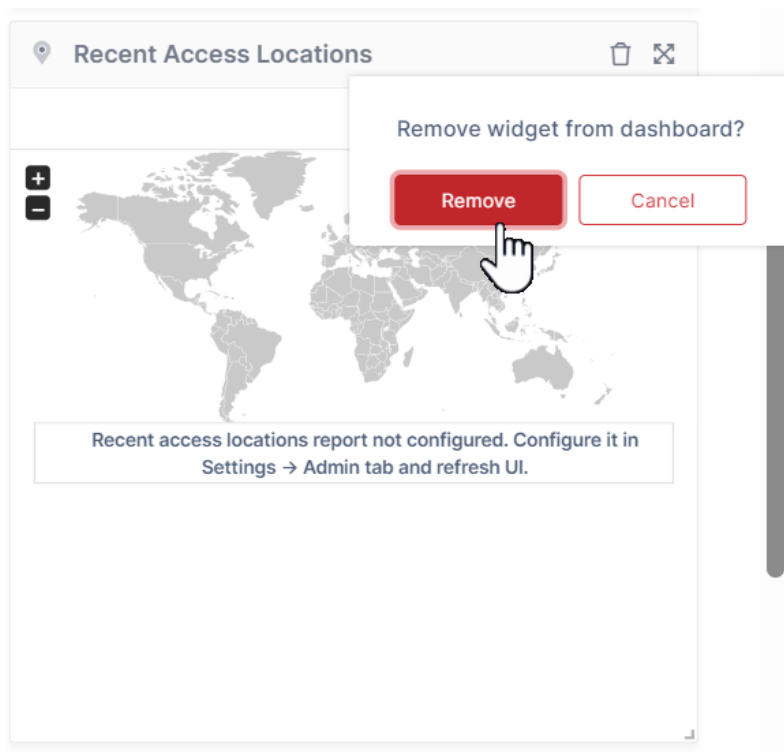


To move all widgets back to their original configuration, click **More** in the header ribbon and choose **Reset Widgets**.

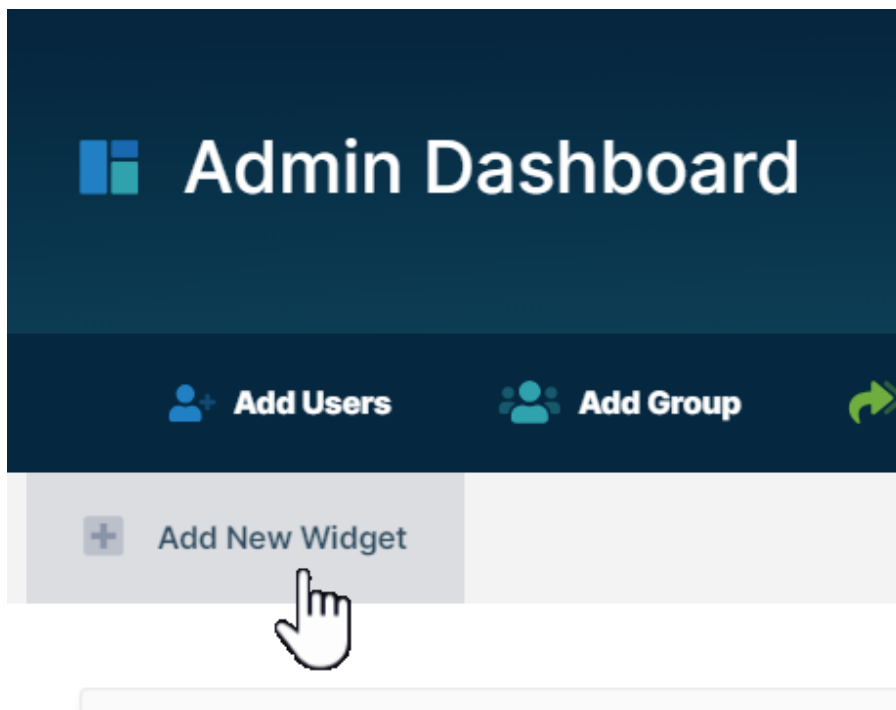


Removing and Restoring Widgets

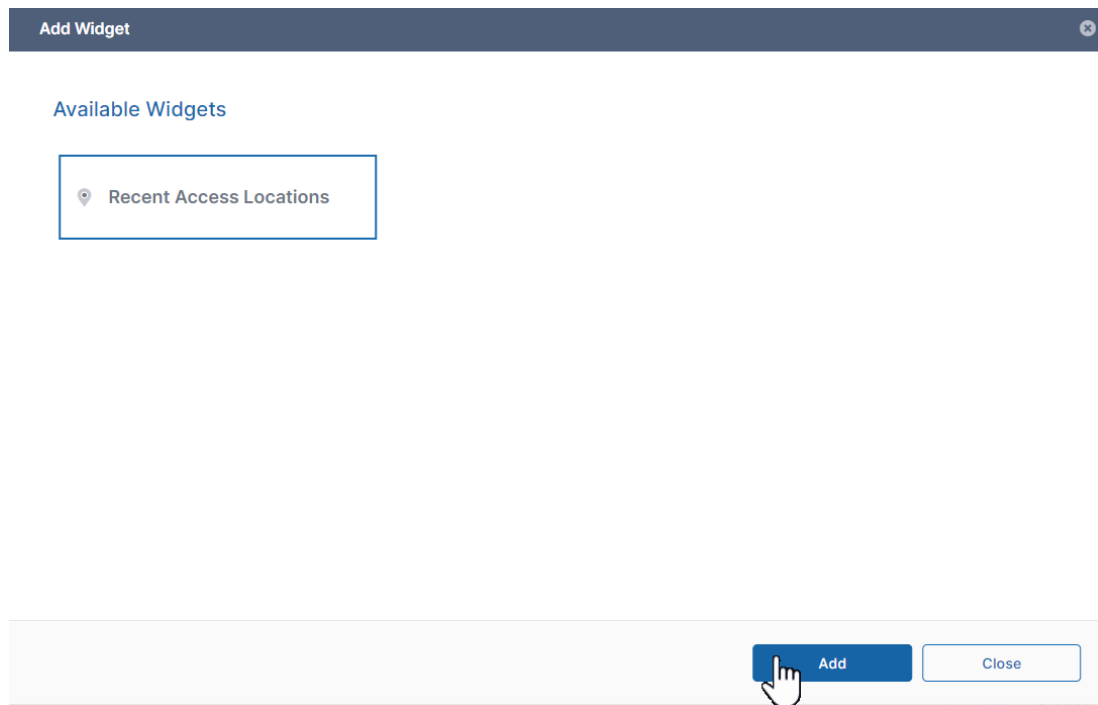
To remove a widget from the dashboard, click the delete icon in the upper-right corner of the widget, and then click **Remove**.



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



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



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

Release Notifications

You can learn about new FileCloud releases:

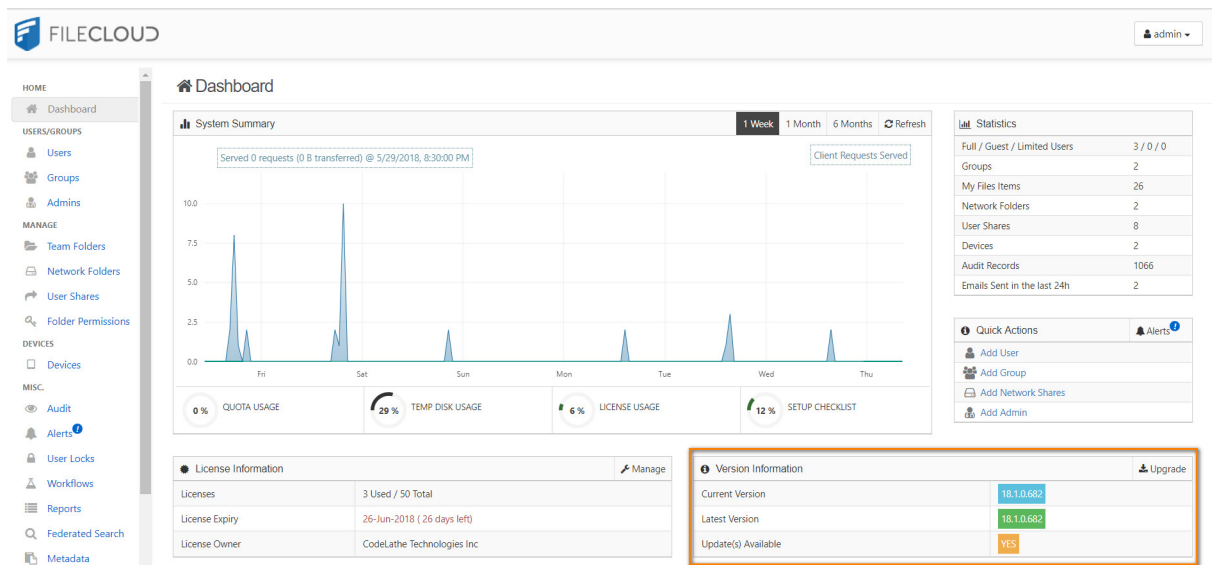
By Subscribing to the Mailing List

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

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

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 below.



Managing Users



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

In this section:

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

Listing FileCloud Users

Listing Users

To list all users in FileCloud:

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

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

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 ASCII Sort order for Listings of Users, Files and Folders](#).

Manage Users

Filter Status Filter Source Filter Show 10 Items

	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	

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.

Manage Users

Filter Status Filter: All Source Filter: All Show 10 Items

	User name	Display Name	Email	Last Login	Status	Actions
	aliah	Aliah	aliahp@example.com	--	Full Access	
	brianna	Brianna	brianna@example.com	10 Feb 2022 12:03	Guest Access	
	david	david	dm898002@gmail.com	04 Oct 2021 15:16	Full Access	
	gaby	Gaby	gabriele_95@example.com	14 Oct 2021 11:28	Full Access	
	hr manager	HR Manager	hrmanager@example.com	--	Full Access	

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotifications	LastLogin	Authentication Type	MobilePhone	Effective Policy	
2	david	dm898002@example.com		david	FULL		EVERYONE	YES	NO	10/4/2021 15:16	Default	15559992323	Group Management	
3	aliah	aliahp@example.com		Aliah	FULL		EVERYONE	YES	NO		Default	15556667777	Global Default Policy	
4	hr manager	hrmanager@example.com		HR Manager	FULL		EVERYONE	YES	NO		Default		Global Default Policy	
5	gaby	gabriele_95@example.com		Gaby	FULL		EVERYONE	YES	NO	10/14/2021 11:28	Default		Global Default Policy	

Viewing User Properties

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

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

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

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

4. Click the **edit icon**.

Show me

HOME

Dashboard

USERS/GROUPS

Users

Groups

Admins

MANAGE

Team Folders

Network Folders

User Shares

Folder Permissions

Manage Users

Add UserImportExport

Filter

gmail.com

Status Filter

Source Filter

Show 10 Items

	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	

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.

User Details

Name

jessicam

Email

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

Manage Files

Manage Policy

Manage Shares

Mobile Devices

Reset Password

Send Email

Manage Notifications

Manage Backups

Delete Account

Profile Image



Update

Remove

Access Level

Full

Authentication

Default

Save

Close

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("TONIDOCLOUD_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 Details

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

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

Profile Image

Update Remove

User Properties - Advanced Options

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

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

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

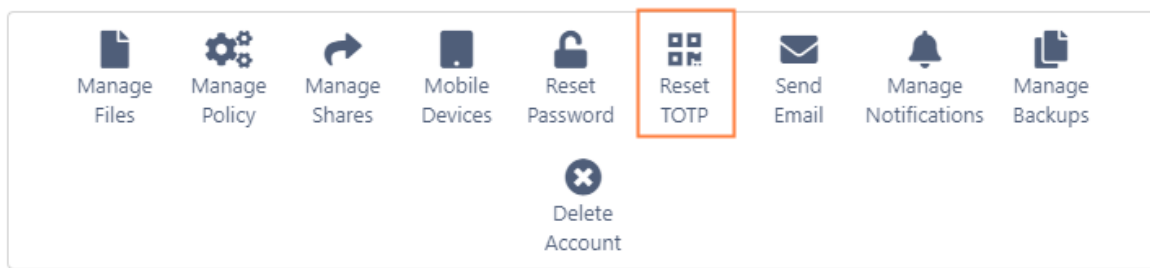
Manage Files, Manage Policy, Manage Shares, Mobile Devices, Reset Password, Send Email, Manage Notifications, Manage Backups, Delete Account

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

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

The Reset TOTP button

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



User Properties - Editable



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

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

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

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

Profile Image



 Update
  Remove

Access Level

Full ▼

Authentication

Default ▼

Email

amitbose@example.com

Save

Close

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

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

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

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

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

User Details ✕

Name	jessicam		Total Quota	2 GB
Email			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 ▾	

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



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

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

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

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

**Storage Details**

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

Disable a FileCloud User Account

Disabled User Account Status

Any user account can be disabled by the Administrator.

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

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

Disabling a User Account

Disable a user account by following the steps listed below

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

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

UNKNOWN ATTACHMENT

- 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:

- Open a browser and log on to the admin portal.
- In the navigation panel, click **Groups**.
- Select the **group** that you want to add users to, and then click the Edit icon.
- On the **Members** tab, click **Import Users from AD Group**.
- In **AD Group Name**, enter the AD group to import.
- 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 exists 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 .

HOME Dashboard USERS/GROUPS Users Groups Admins MANAGE User Shares	Manage Users Add User Import Export						
	Filter	Filter by name, email or notes	Status Filter	Source Filter	Show 10 Items		
	User name	Display Name	Email	Last Login	Status	Actions	
	Jared Taylor	Jared Taylor	JaredTaylor978@gmail.com	--	Full Access		
	Noah	Noah	noah@example.com	--	Full Access		
	abose	Amit Bose	amitbose@example.com	08 Oct 2020 15:52	Full Access		

Delete Jared Taylor



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

☐ Confirm and continue with deletion?

Delete

Cancel

Resetting a User Password

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



For user accounts with "Authentication Type" set to "AD or LDAP", password management must be done in AD or LDAP admin portal.

Sending the Account Welcome email option is available beginning with FileCloud 20.1.

To reset password for user account:

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

User Details
×

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

Manage Files

Manage Policy

Manage Shares

Mobile Devices

Reset Password

Send Email

Manage Notifications

Manage Backups

Delete Account

Profile Image

Update
Remove

Access Level

Full ▾

Authentication

Default ▾

Email

dm898002@gmail.com

Save

Close

5. Click **Reset Password**.



A dialog box titled "Set New Password" with a close button (X) in the top right corner. It contains two input fields: "Password" and "Confirm Password". The "Password" field has a blue border and a cursor. Below the input fields are two buttons: "Save" (blue) and "CANCEL" (white with a grey border).

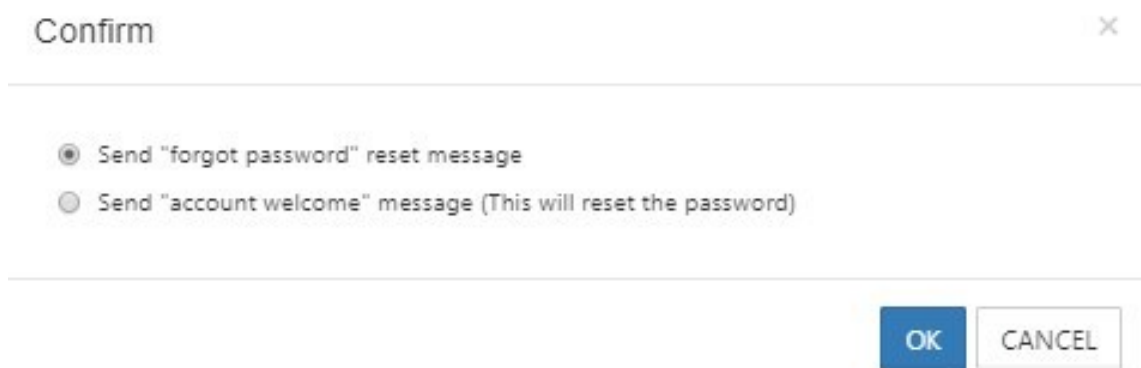
6. Enter the new password in **Password** and **Confirm Password**.

7. Click **Save**.

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

OR

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



A dialog box titled "Confirm" with a close button (X) in the top right corner. It contains two radio button options: "Send 'forgot password' reset message" (selected) and "Send 'account welcome' message (This will reset the password)". Below the options are two buttons: "OK" (blue) and "CANCEL" (white with a grey border).

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

Manage A User's Policies

Administrators can manage users easily using policies.

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

- The policy record can be associated with a user

[Learn more about Policies](#)

What do you want to do?

Select a Policy for a User

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

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

- Enable or Disable Printing in Mobile Apps
- Enable or Disable Configuration Changes in Clients
- Enable or Disable Two-Factor Authentication (2FA)
- Enable or Disable Notifications
- Enforce Session Timeout for Clients
- Set a Default Storage Quota
- Enable Privacy Settings

To select a policy for a user:

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

Change or Remove a User's Policy

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

To remove a policy for a user:

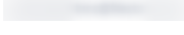
1. Open a browser and log on to the admin portal.
2. In the navigation panel, click **Users**.
3. In the **Manage Users** window, select a user, and then click the Edit icon.
4. In the **User Details** window, click **Manage Policy**.
5. Next to the **Selected Policy** box, click **Clear**.

Modifying a policy while managing a user

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

To edit a policy from a user account:

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

	▶ jason	Jason		16 Dec 2024 22:53	Full Access	  
	▶ jennifer	Jennifer		24 Jan 2025 09:02	Full Access	  

The **Policy Settings** dialog box opens.

3. Change the settings on any of the tabs.

Policy Settings - Admin Users - jennifer

Note: Custom Policy assigned to this User

General

2FA

User Policy

Client Application Policy

Device Configuration

Notifications

Share mode
Allow All Shares

Set Share Mode

Default Share Expiry in Days
0

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed

Save Reset All Close

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

Save Policy Changes

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

OK Cancel

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

Calculate the Effectiveness of a User's Policy

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

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

Learn more about Effective Policy Best Practices

To calculate the effectiveness of a policy for a user:

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

Manage a User's Profile Picture

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

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

User Details

Name	me	Total Quota	1 GB
Email	me@codeclathe.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
Full

Authentication
Default

Email
me@codeclathe.com

[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.
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

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

jess

Account Expires On

2022-08-31

←

August 2022

→

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

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.
4. Click the **edit icon** (.
5. Scroll down to see the **Account Expires On** field.
6. To see a calendar and select a date, click the text box.
7. To save your changes, click **Save**.

Send Email from User Details

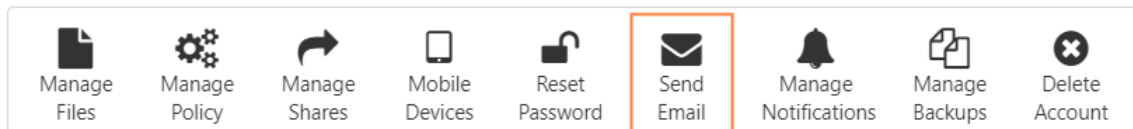
 This option is available beginning in FileCloud 20.1

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

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

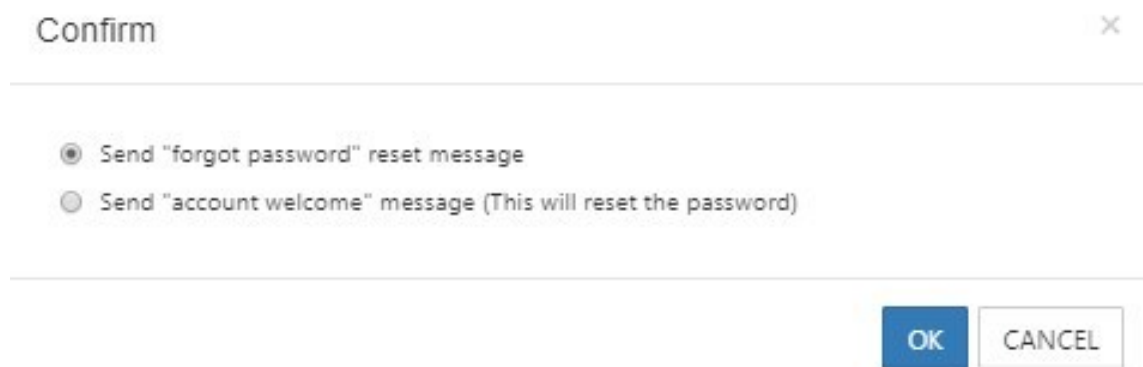
To send an email from User Details:

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



A dialog box for choosing the type of email opens.

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



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

Managing Groups

A FileCloud Admin can manage User Groups.

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

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

To add a group, see Group Settings.

Change a User Group Name

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

To change a group's name:

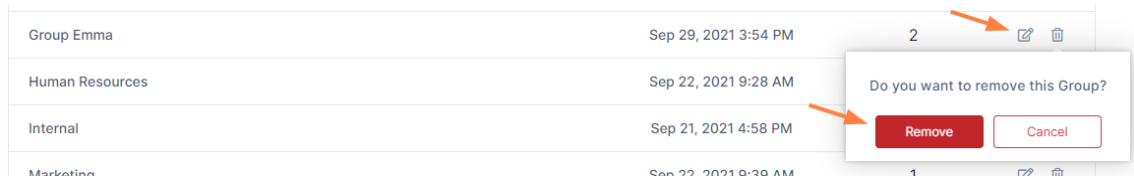
1. Log on to admin portal.
2. In the navigation panel, click **Groups**.
3. Click the Edit icon for the desired group from the list of groups.
4. In the **Manage Group** dialog box, change the group name.
5. Click **Save** once the change is complete.

Delete a User Group

To delete a group:

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

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



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

View and Change Group Members

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

To change a group's members:

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

Manage Group

Group Name:

Save

Members

Admins

Policies

Members Management

Add Users to Group

Import Users from AD Group

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

1

of 1 >

Close

Exporting a list of users in a group

To export a list of users in a group:

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

Manage Group

Group Name: Save

Members

Admins

Policies

Members Management

Add Users to Group Import Users from AD Group

Q

Users in Group ((count) members in this group) Export

Users

Jared
jaredtaylor978@gmail.com

Remove

Jessica
jm2344311@gmail.com

Remove

<< < Page 1 of 1 > >>

Close

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 Resourc	YES	NO	2/10/2022 14:08	Default		Global Default Policy

View and Change Group Admins

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

To modify group admin settings:

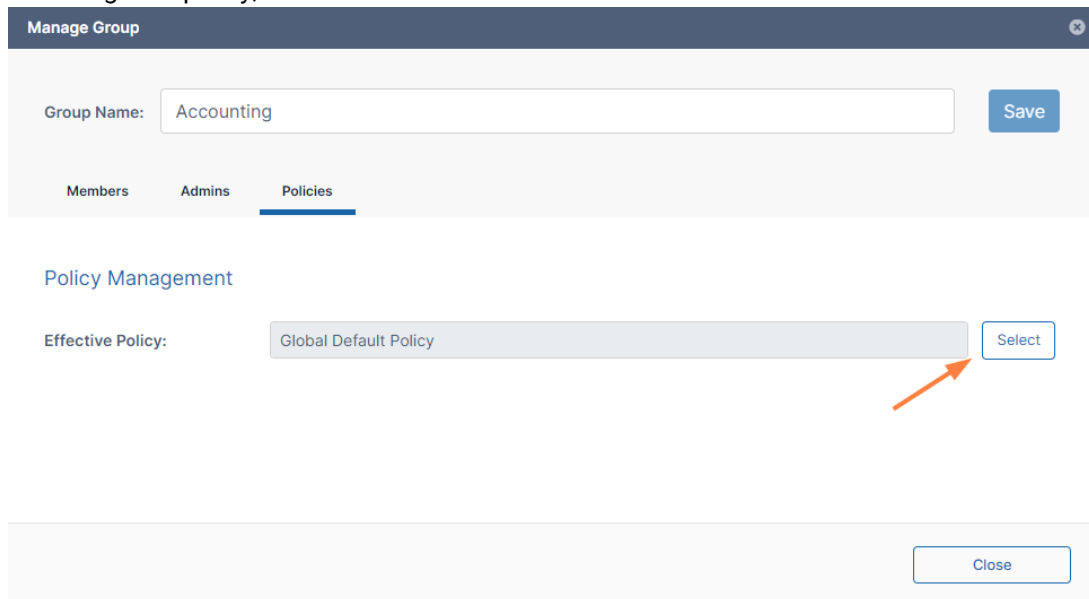
1. In the navigation panel, click **Groups**.
2. Click the Edit icon for the group.
3. In the **Admins** tab, view the admins of the group.
4. To add an admin, enter an existing FileCloud user's name or email address in the search bar, and click **Add**.
5. To remove an admin, click **Remove** next to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

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

View and Change a Group's Policy

To change a group's policy:

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



Manage Group

Group Name: Save

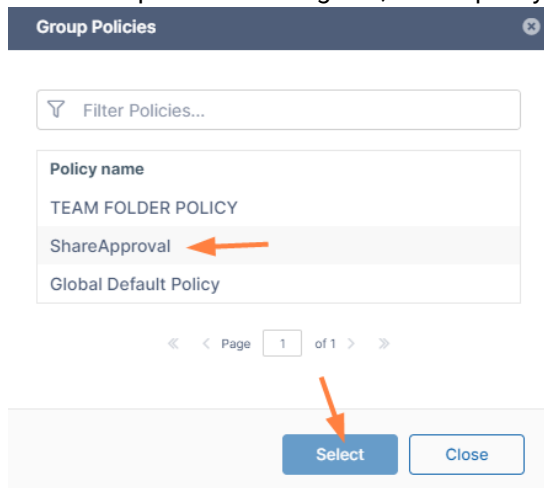
Members Admins **Policies**

Policy Management

Effective Policy: Select

Close

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



Group Policies

Filter Policies...

Policy name

TEAM FOLDER POLICY

ShareApproval ←

Global Default Policy

Page 1 of 1

Select Close

The policy is changed.

6. Click **Close**.

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

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

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

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

The screenshot shows the 'Manage Group' dialog box with the 'Sync Options' tab selected. The group name is 'Marketing'. The 'Automatic Sync' and 'Remove Members' options are enabled, while 'Dynamic Members Import' and 'Disable Members' are disabled. An orange arrow points to the 'Remove Members' toggle switch.

Their functions are as follows:

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

5. Click **Close**.

Managing Admin Users

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

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

Check an admin user's permissions

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

To check all of a user's permissions:

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

UNKNOWN ATTACHMENT

The **User Effective Permissions** dialog box opens.

UNKNOWN ATTACHMENT

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

UNKNOWN ATTACHMENT

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.
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.

Operation	Description
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.
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.

Operation	Description
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.

UNKNOWN ATTACHMENT

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

Or:

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

UNKNOWN ATTACHMENT

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

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

UNKNOWN ATTACHMENT

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**.

User Details

Name	alex	Total Quota	2 GB
Email	alex@example.com	Used Quota	0 B
Last Login	08 Jan 2024 12:24	Available Quota	2 GB
TOS Date	Not Accepted	Used Storage	0 B
Group	Manage	More	

Manage Files

Manage Policy

Manage Shares

Mobile Devices

Reset Password

Send Email

Manage Notifications

Manage Backups

Delete Account

Profile Image

Update

Remove

Access Level

Full

Authentication

Default

Save

Close

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

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

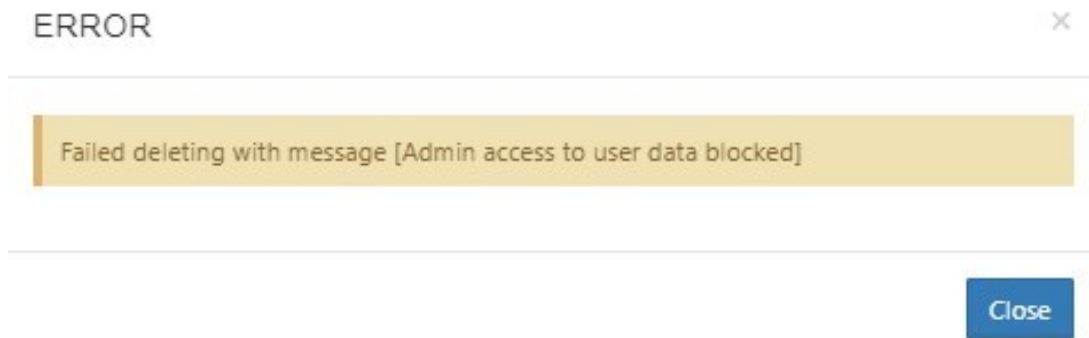
If you do not want the main administrator or admin users to have unlimited access to user files and folders, you can configure your system to prevent them from performing all of the following actions:

- 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:



In this section:

Add Folder-Level Permissions to User Folders

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

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

To assign folder-level permissions to users' folders:

1. In the admin portal's left navigation panel, click **Users**.
2. On the **Manage Users** page, select a user, and then click the Edit icon.
3. On the **User Details** dialog box, click **Manage Files**.
The **Manage Files for <User>** window opens.

Manage files for jennifer

Filter Deleted Files

Name	Size	Modified	Actions
☐ My Files			   

Page 1 of 1
1 row

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



button in the folder's row.

Manage files for jennifer

/jennifer

Up Filter Deleted Files Copy Rename Move Delete

Name	Size	Modified	Actions
☐ Accounts		Apr 26, 2024 9:37 AM	   
☐ Admin hold		Nov 21, 2023 9:58 AM	   
☐ Archival path		Nov 21, 2023 9:58 AM	   
☐ Archival policy		Nov 21, 2023 9:58 AM	   

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

6. Follow the steps below to assign and change user and group folder-level permissions. Users who do not appear

on the list have all folder-level permissions to the folder (unless their group permissions are limited)

Folder: /jennifer/Admin hold

Security Check Access

Permissions

Inherit Parent Folder Security: ☒ Inherit ☐ Don't Inherit

User Group

Add User

User	Read	Write	Delete	Share	Manage
dm898002@gmail.com	☒	☒	☒	☒	☒

Page 1 of 1

Inherited Permissions

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

Page 1 of 1

Close

A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.

B Click **Add User** to add a user and limit their access to the folder, or click the Group tab and add a group.

C In the top list of users, check or uncheck levels of permissions.

Copy and Move User Files



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

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

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

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

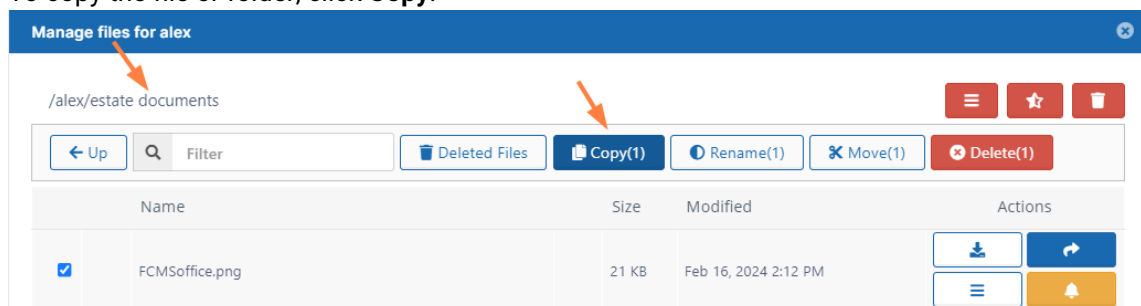
What is the difference between copy and move?

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

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

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

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

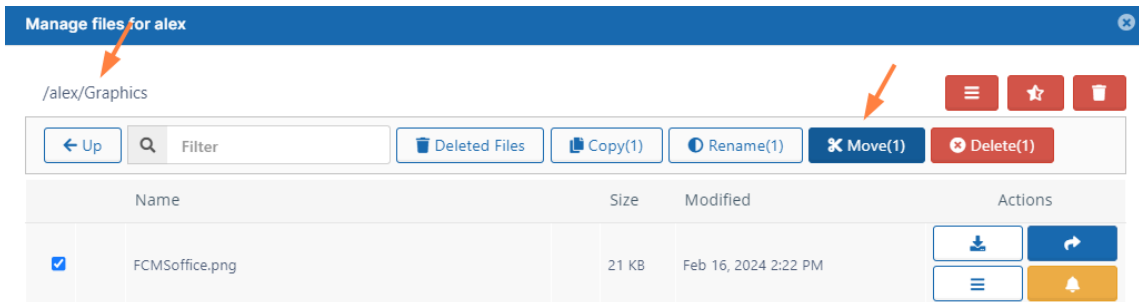


8. Navigate to the folder where you want to paste the copy.
9. Click **Paste**.

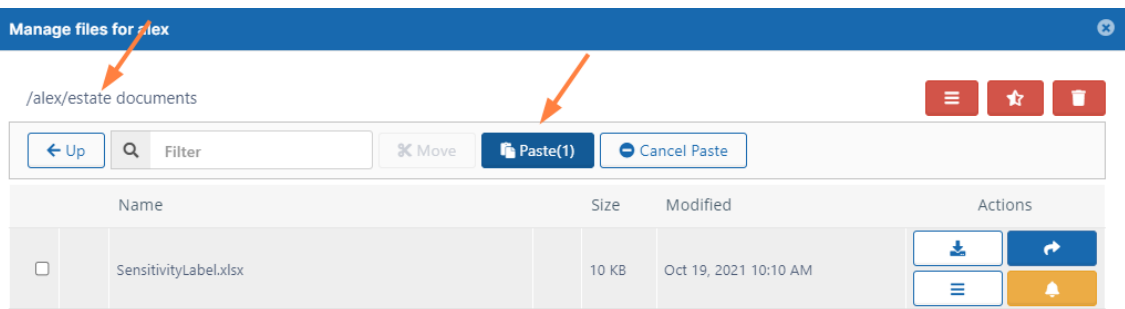
To move and paste files and folders between a user's folder locations:

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

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



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



Download User Files and Folders



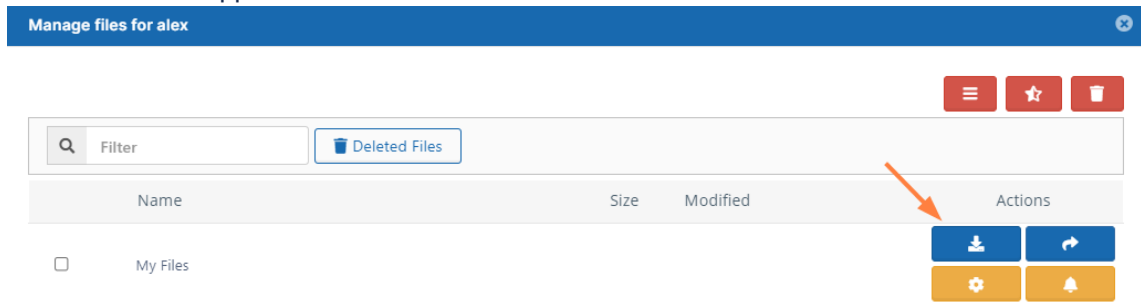
To disable users' ability to download folders from the user portal, see the setting **Disable Folder Download** at General Customization.

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

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

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

- Folders are first zipped and then downloaded.

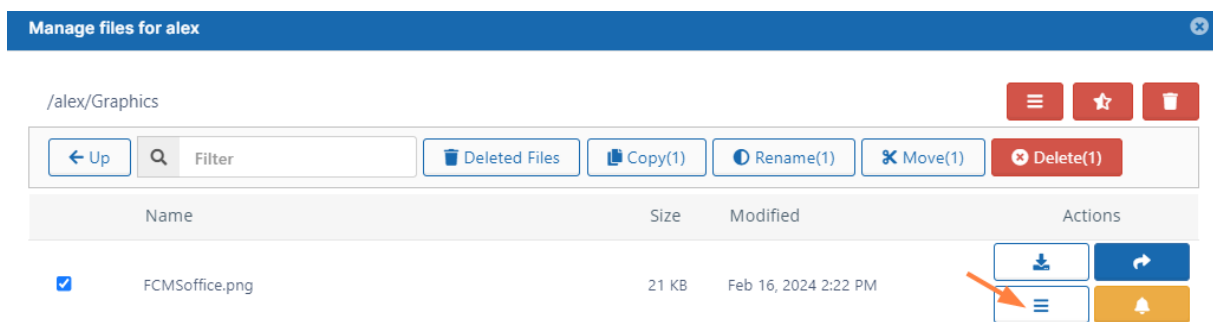


Can I download an older version of a file?

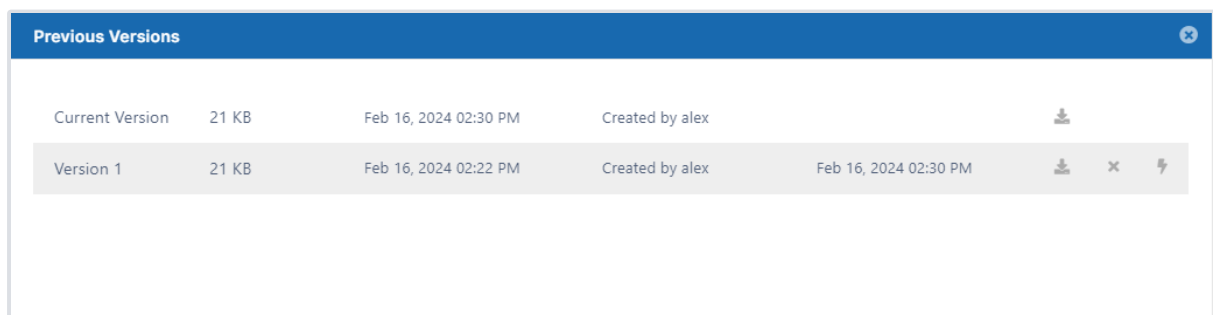
If the user has uploaded changes to a file, you can:

- download the latest version
- download a previous version

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



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

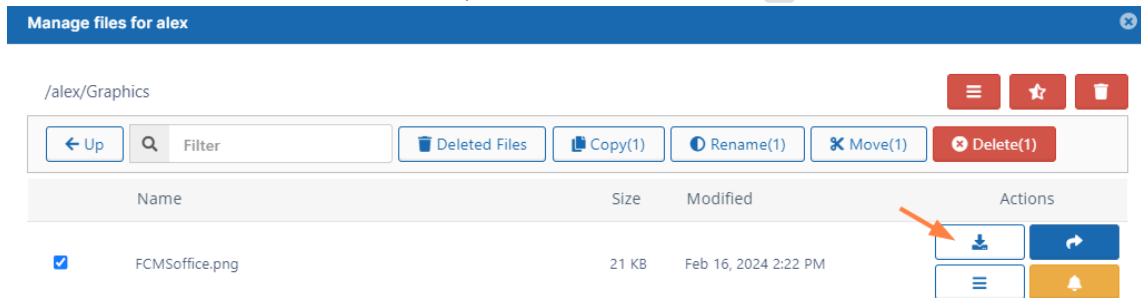


If you have older versions on your site, you may:

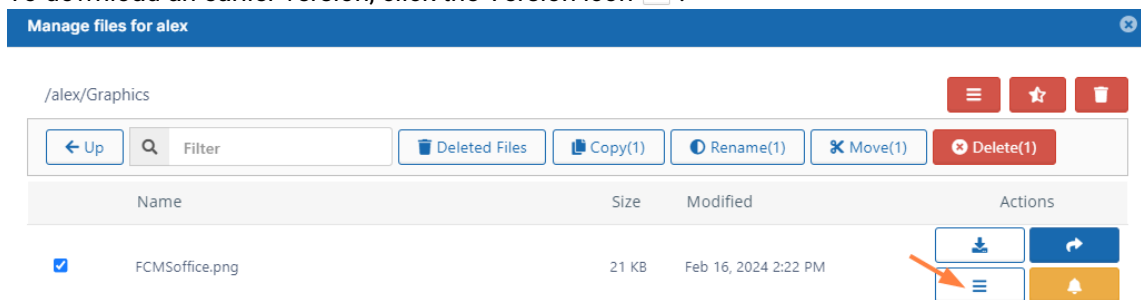
- Restore the previous version of a file and make it live
- Remove previous versions to save space

To download user folder and files:

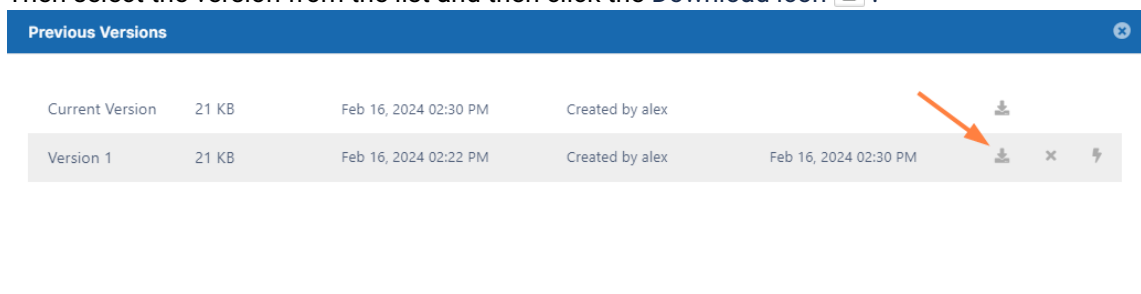
1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon .
4. On the User Detail dialog box, click **Manage Files**.
The Manage Files for <User> window opens.
5. Navigate to the folder or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

**OR**

To download an earlier version, click the Version icon .



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



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"

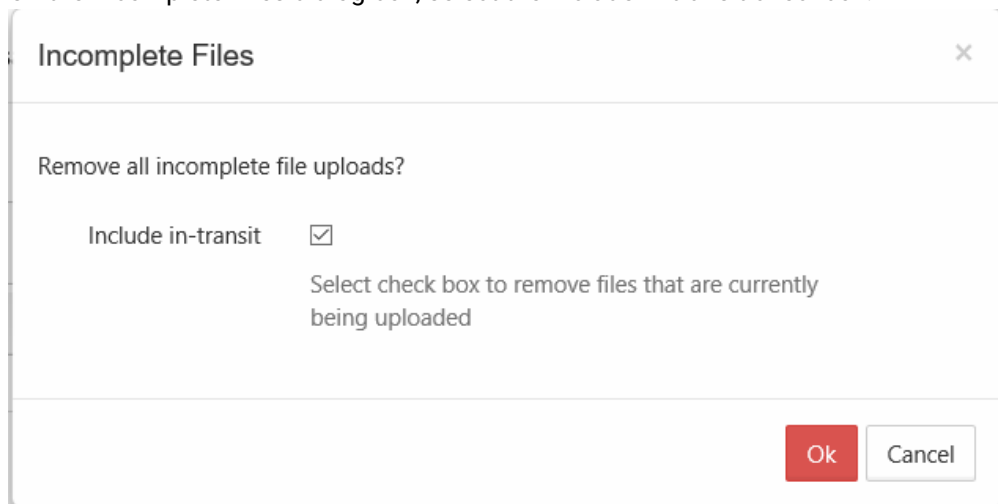
- Cannot be undone

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**.
The Manage Files for <User> window opens.
5. Click the Remove all incomplete uploads icon .
6. On the Incomplete Files dialog box, select the Include in-transit checkbox.



7. Click OK.

Delete User Folders and Files



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

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

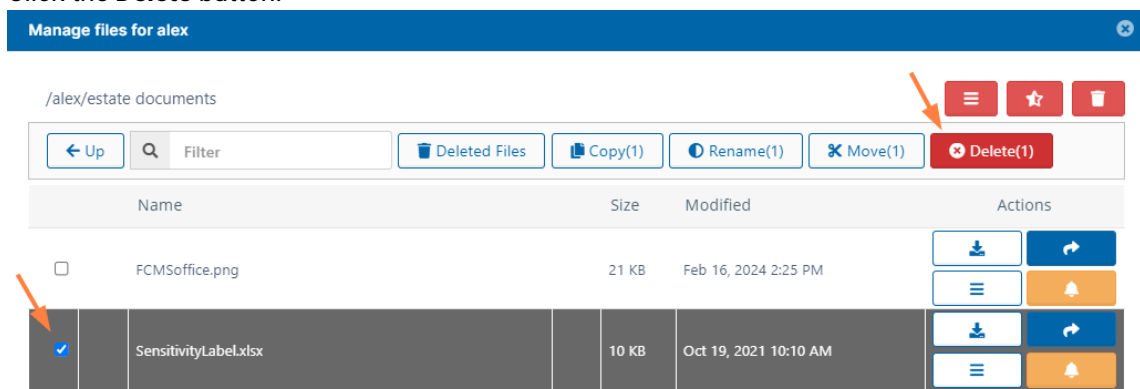
This allows you to protect and maintain your system in the following ways:

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

💡 Deleting a file or folder moves it to the Deleted Files recycle bin. To permanently remove a file, you must clear 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**.
The Manage Files for <User> window opens.
5. Navigate to the folder or file you want to delete.
6. To select the file or folder, click the checkbox next to the name.
7. Click the **Delete** button.



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

Clear a Recycle Bin



This action:

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

As an administrator, you can [delete a user's files and folders](#).

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

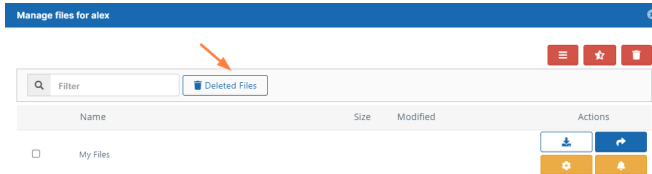
- If you have a policy that stores deleted files, they are saved in the Recycle Bin
- This means that they can be recovered if deleted by mistake or are needed again at a later time
- You can also set the Recycle Bin to automatically delete through a policy

Manage the Recycle Bin Using a Policy

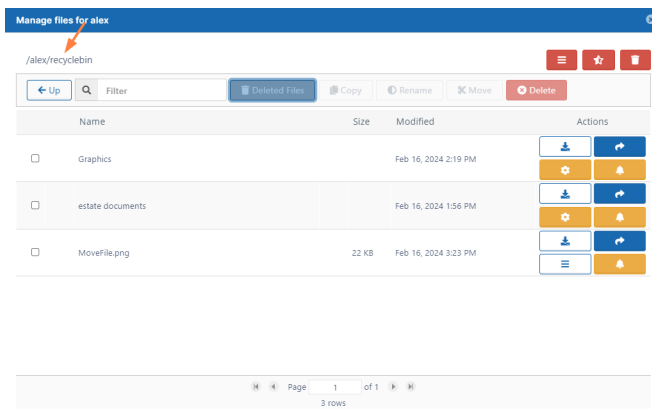
Go to the recycle bin

To go to a user's recycle bin:

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



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



Clear a deleted file or folder

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

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

Manage files for alex

/alex/recyclebin/estate documents

← Up Filter Deleted Files Copy(1) Rename(1) Move(1) Delete(1)

	Name	Size	Modified	Actions
☒	FCMSoffice.png	21 KB	Feb 16, 2024 1:56 PM	Download Share More Alert

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

Clear all deleted files



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

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

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

Manage files for alex

/alex/recyclebin

← Up Filter Deleted Files Copy Rename Move Delete

	Name	Size	Modified	Actions
☐	Graphics		Feb 16, 2024 2:19 PM	Download Share More Alert
☐	estate documents		Feb 16, 2024 1:56 PM	Download Share More Alert
☐	MoveFile.png	22 KB	Feb 16, 2024 3:23 PM	Download Share More Alert

Page 1 of 1
3 rows

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

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?

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

Manage files for alex

/alex/Graphics

← Up Filter Deleted Files Copy Rename Move Delete

	Name	Size	Modified	Actions
☐	FCMSoffice.png	21 KB	Feb 16, 2024 2:25 PM	

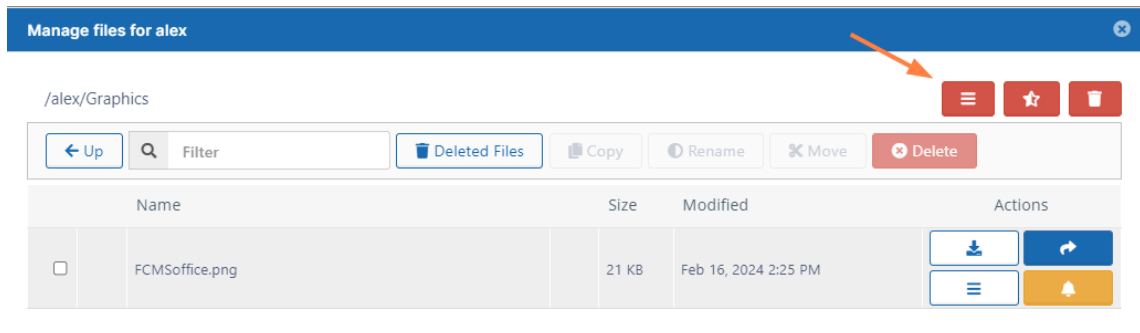
If there are previous versions they appear in the listing that opens:

Previous Versions

Version	Size	Modified	Created by	Actions
Current Version	21 KB	Feb 16, 2024 02:30 PM	Created by alex	
Version 1	21 KB	Feb 16, 2024 02:22 PM	Created by alex	

To remove all old versions of a file:

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



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

Remove Incomplete User Uploads



This action:

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

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

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

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

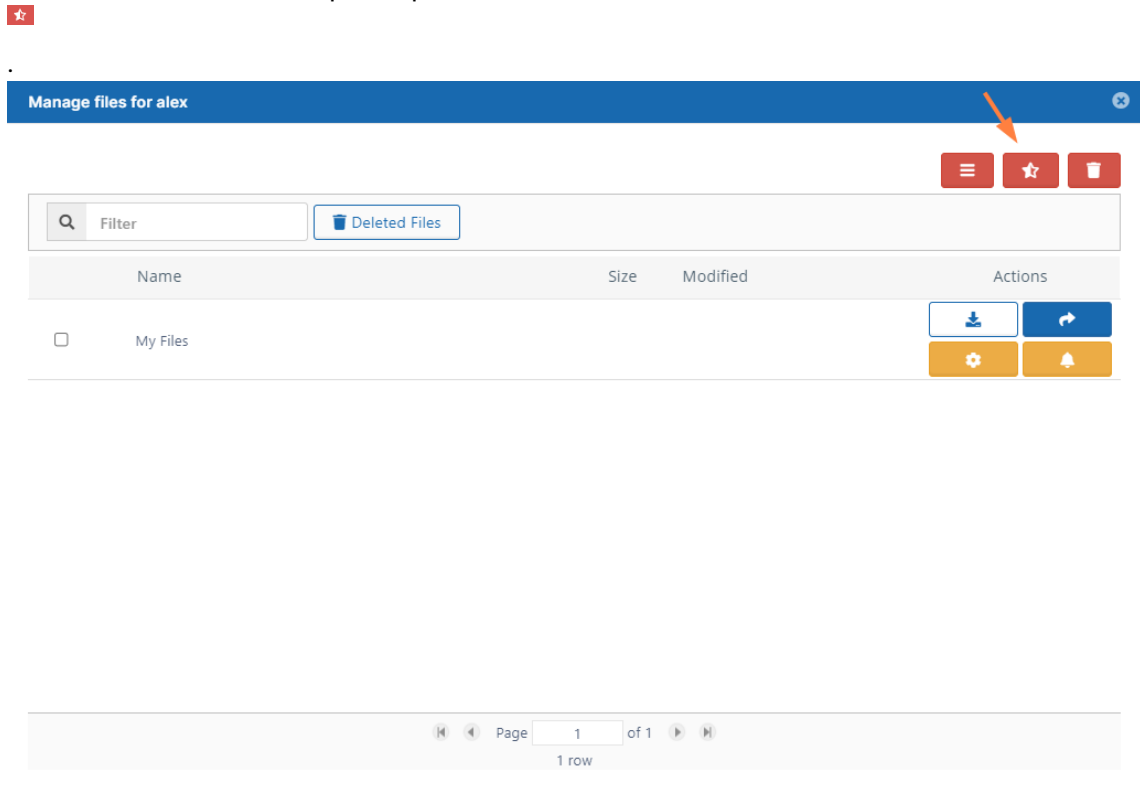
💡 If a file upload is in progress:

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

Cancel a Partial Upload

To remove all incomplete user uploads:

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



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

Restore a Previous File Version

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

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

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

Manage files for jenniferp ✕

/jenniferp/Admin hold ☰ ☆ 🗑

← Up
🔍 Filter
🗑 Deleted Files
📄 Copy
🔄 Rename
📁 Move
✕ Delete

	Name	Size	Modified	Actions
☐	AccountNames.txt	60 B	Feb 20, 2024 1:14 PM	📄 🔄 ☰ 🔔
☐	big_buck_bunny.mp4	5.26 MB	Sep 15, 2017 2:25 AM	📄 🔄 ☰ 🔔
☐	vacination #5 report.pdf	140 KB	Aug 26, 2022 5:16 AM	📄 🔄 ☰ 🔔
☐	Ã'Ã'Æ'ÃTN.txt	0 B	Jun 16, 2016 11:54 AM	📄 🔄 ☰ 🔔

⏮
⏪
Page 1 of 1
⏩
⏭

4 rows

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

Previous Versions

Current Version	60 B	Feb 20, 2024 01:14 PM	Created by jenniferp			
Version 2	29 B	Feb 20, 2024 01:13 PM	Created by jenniferp	Feb 20, 2024 01:14 PM	⬇️	⚡
Version 1	18 B	Jan 09, 2024 01:37 PM	Created by jenniferp	Feb 20, 2024 01:13 PM	⬇️	⚡

Close

Page 1 of 1

4 rows

The following confirmation box appears.

Confirm

Selected version will be made the live version.

Note that the current version will be versioned or removed depending upon your versioning settings. Continue?

OK

Cancel



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

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

Previous Versions							
Previously Version 1							
Current Version	18 B	Jan 09, 2024 01:37 PM	Created by jenniferp				
Previously Current Version							
Version 2	60 B	Feb 20, 2024 01:14 PM	Created by jenniferp	Feb 20, 2024 01:20 PM			
Version 1	29 B	Feb 20, 2024 01:13 PM	Created by jenniferp	Feb 20, 2024 01:14 PM			

Critical Section Cleanup Tool



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/fixedtree_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 FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on

the **Settings** navigation page, click **Server** .
The **Server** settings page opens.

Server

[Reset to defaults](#)

Service Name

Name to use to refer to the service

Service URL

URL that accesses the service

Session Timeout (Minutes)

User portal login session timeout.

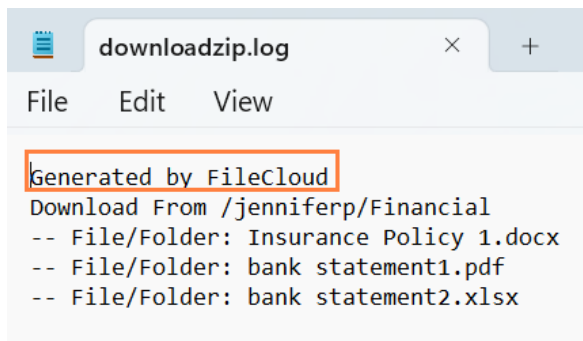
Example: 15 (default) = 15 minutes; 30 = 30 minutes; 60 = 1 hour

Note: Session always expires when browser is closed unless advanced configuration is added.

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

[Reset to defaults](#)

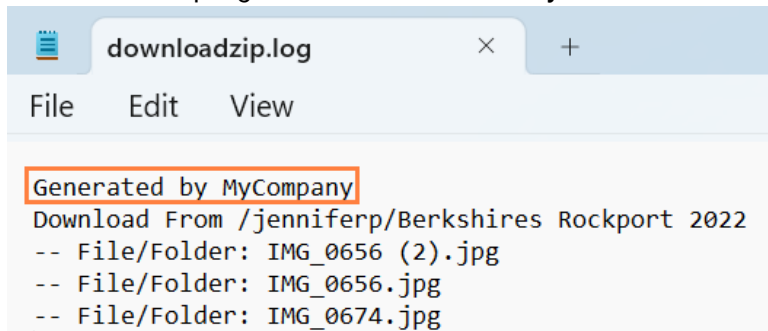
Service Name

Name to use 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 Team Folders



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

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

To manage and view details of Team Folders:

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

Team Folders

[Reset to defaults](#)

Enable Team Folders

Click to enable and manage team folders



Team Folder account

Master account managing Team Folders

 [Edit](#)

[Manage Team Folders Account](#)

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

Team Folder Account Details

Account Info

Name:

Email:

Last Login: --

TOS Date: Not Accepted

Data Storage

0 B

Unlimited

Quota Usage

898.2 MB Used

Unlimited Total

View Details

Manage Shares

Reset Password

Manage Notifications

Delete Account

Customization

Email

Secondary Email

Display Name

Creation Source

Team Folders

Default

Lock Account

Phone Number

+1

Save

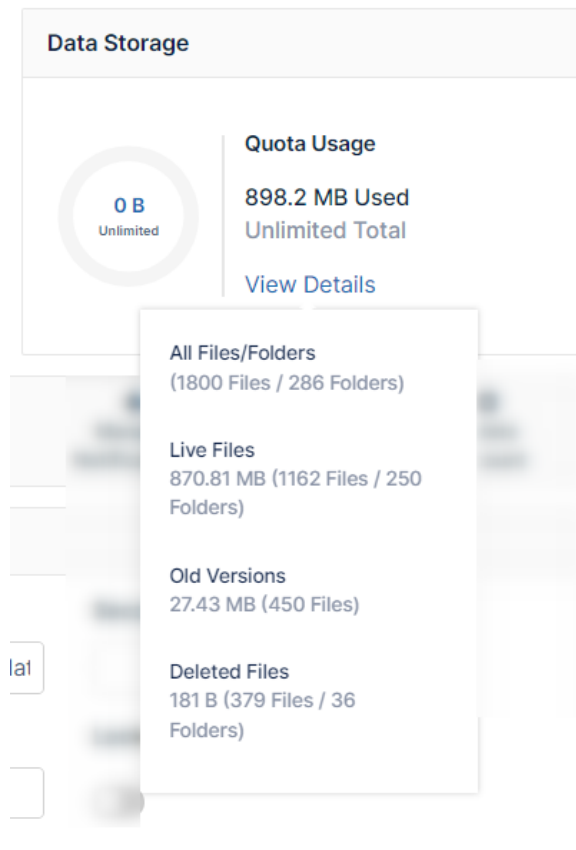
Close

Managing Team Folders – 82

To view the breakdown of data in Team Folders:

In the Data Storage section, click **View Details**.

You are shown a breakdown of the files and folders by live versions, old versions, and deleted files.



To edit the Team Folders account fields:

In the customization section, click the image, to upload a photo or graphic, or modify the **Email**, **Secondary Email**, **Display Name**, **Creation Source**, or **Phone Number** fields and click **Save** to save your changes.

Lock Account is automatically checked when too many login errors occur. Click to remove the check

and unlock the account.

Customization



Email

Secondary Email

Display Name

Team Folders

Lock Account

☐

Creation Source

Default

Phone Number

+1

Save

Close

To lock the Team Folder account:

The **Lock Account** field is automatically enabled when the account is locked.

Unlock the account by clicking the enabled **Lock Account** control so that it appears disabled.

Customization



Email

Secondary Email

Display Name

Team Folders

Lock Account

☒

Creation Source

Default

Phone Number

+1

Save

Close

To manage Team Folder shares:

1. Click **Manage Shares**.

Team Folder Account Details

Account Info

Name:

dev1team

Email:

Last Login:

--

TOS Date:

Not Accepted

Data Storage

0 B

Unlimited

Quota Usage

898.2 MB Used

Unlimited Total

[View Details](#)

Manage Shares

Reset Password

Manage Notifications

Delete Account

A list of your Team Folder shares opens.

2. Click the edit icon to modify the options or permissions of a share.
3. Click the x icon to remove a share.

Manage Shares for Team Folders

Path	Type	Created Date	Actions
/ /acl2	Private	Feb 20, 2025 4:15 AM	 
/ /chris	Private	Feb 18, 2025 5:49 AM	 
/ /Human Resources/Employee Records	Private	Jan 28, 2025 2:10 PM	 
/ /First/Deletefolder	Private	Jan 15, 2025 3:29 AM	 
/ /Test	Private	Nov 8, 2024 3:42 AM	 
/ /Accounting33/grfsv/c9b07cf2-f2d1-436c-8986-c2107f08740b.pdf.pdf	Password Protected	Oct 8, 2024 11:39 AM	 
/ /test-reshare/test-folder	Private	Sep 16, 2024 10:27 AM	 

To reset the Team Folder account password:

1. Click **Reset Password**.

Team Folder Account Details

Account Info
Name: dev1team
Email:
Last Login: --
TOS Date: Not Accepted

Data Storage

0 B
Unlimited

Quota Usage
898.2 MB Used
Unlimited Total
[View Details](#)

Manage Shares

Reset Password

Manage Notifications

Delete Account

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

Reset Password

Password

Confirm Password

Save

Cancel

To manage Team Folder notifications

1. Click **Manage Notifications**.

Team Folder Account Details

Account Info

Name:

team folder account

Email:

team@example.com

Last Login:

21 Mar 2025 08:54

TOS Date:

Not Accepted

Data Storage

0 B

Unlimited

Quota Usage

0 B Used

Unlimited Total

View Details

Manage Shares

Reset Password

Manage Notifications

Delete Account

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

Manage Notifications for Team Folders

Path	Modified Date	User	Actions
/team folder account/Human Resources	Mar 21, 2025 8:57 AM	team folder account	 

<<

<

Page

1

>

>>

Close

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

To delete the Team Folder account:



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

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

1. Click **Delete Account**.

Team Folder Account Details ✕

Account Info	Data Storage
Name: dev1team Email: [REDACTED] Last Login: -- TOS Date: Not Accepted	0 B Unlimited Quota Usage 898.2 MB Used Unlimited Total View Details
Manage Shares	Delete Account

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

Delete Account ✕

Are you sure you want to delete this account?

This is a team folder account. Deleting this account will delete all file(s) and folder(s) under team folders, which is a common place where all users can store and organize files. This action cannot be undone.

Type **DELETE** to proceed

Delete

Cancel

Search for a Team Folder

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

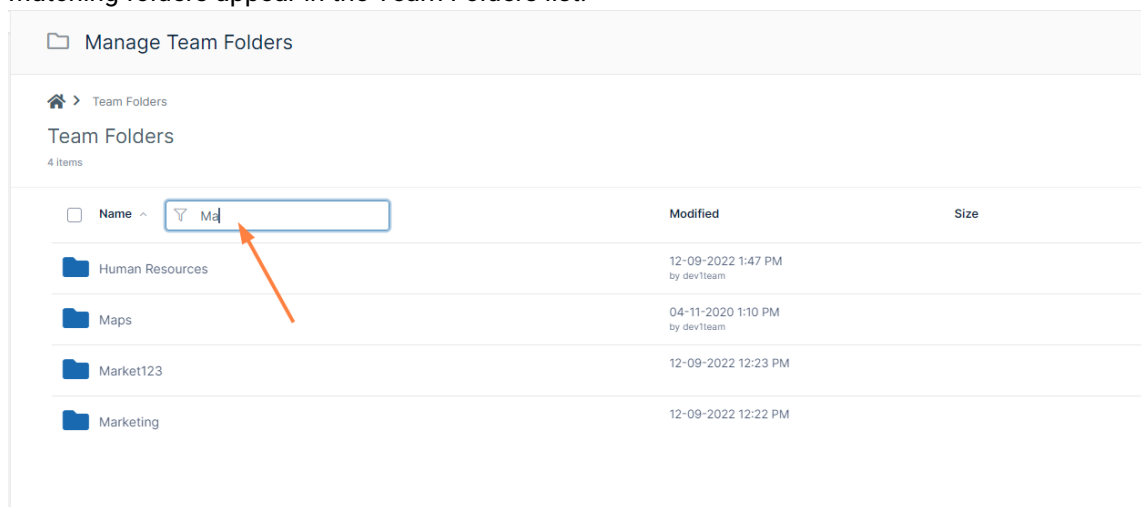
If you manage so many Team Folders that you have to look through multiple pages of folder listings to find a Team Folder, you can use the search box to find the folder you need quickly.

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

To search for a Team Folder:

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

Matching folders appear in the Team Folders list.



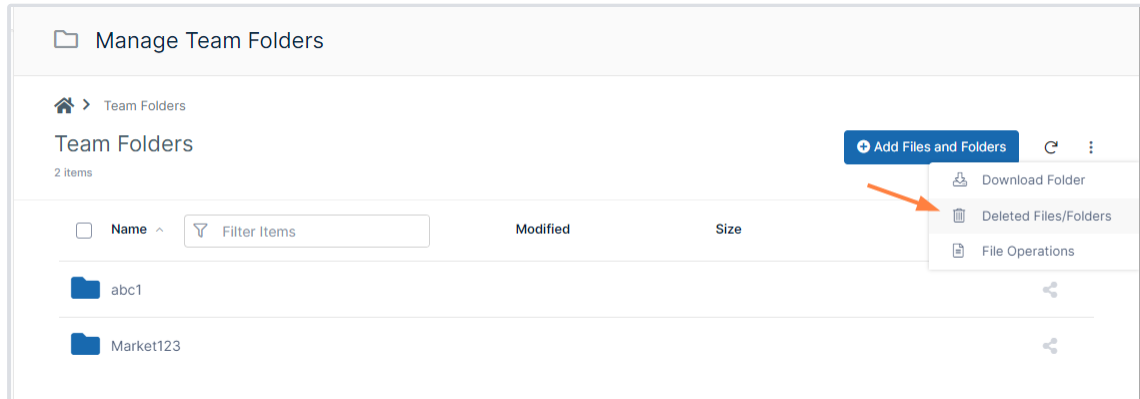
Recover Deleted Files

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

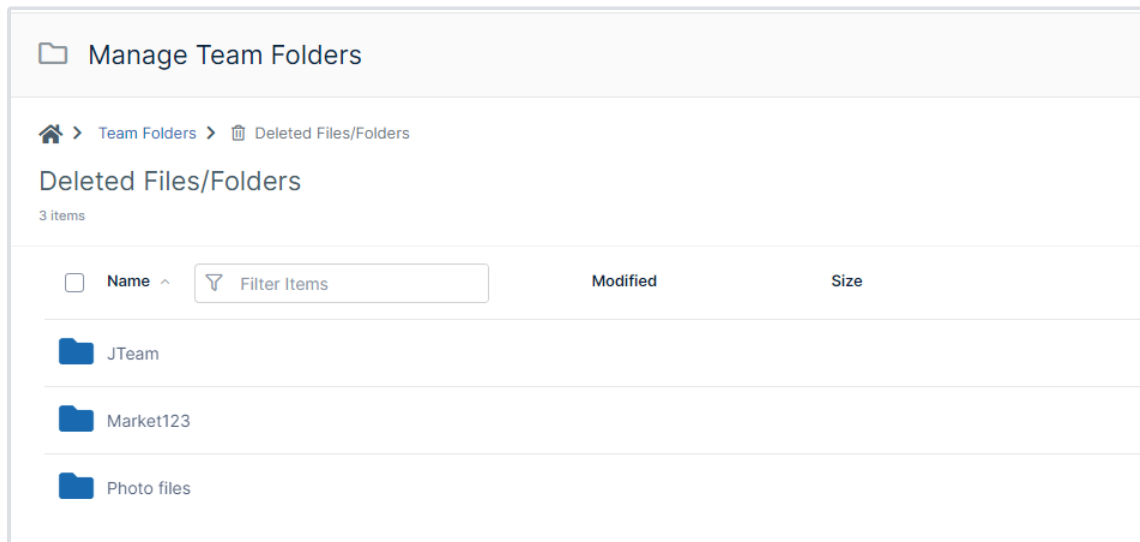
After you delete files and folders, they are placed in the Team Folder's recycle bin so that they can be recovered if deleted by mistake or are needed again at a later time.

To recover a deleted folder or file:

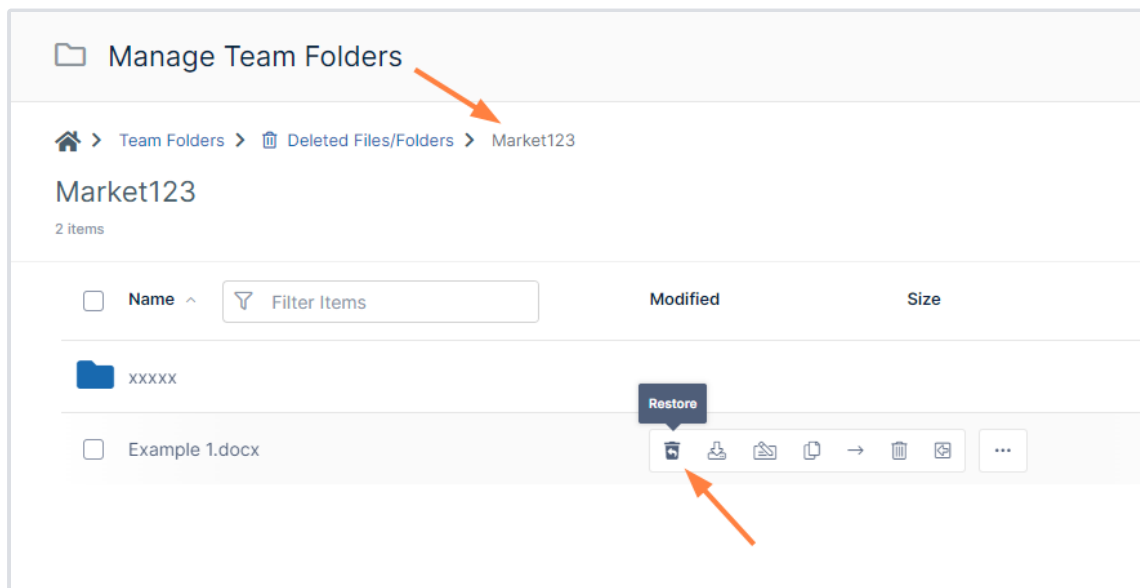
1. Open a browser and log in to the admin portal.
2. In the navigation panel, click **Team Folders**.
3. To open the **Deleted Files/Folders** page, in the upper-right corner, click the more icon and choose **Deleted Files/Folders**.



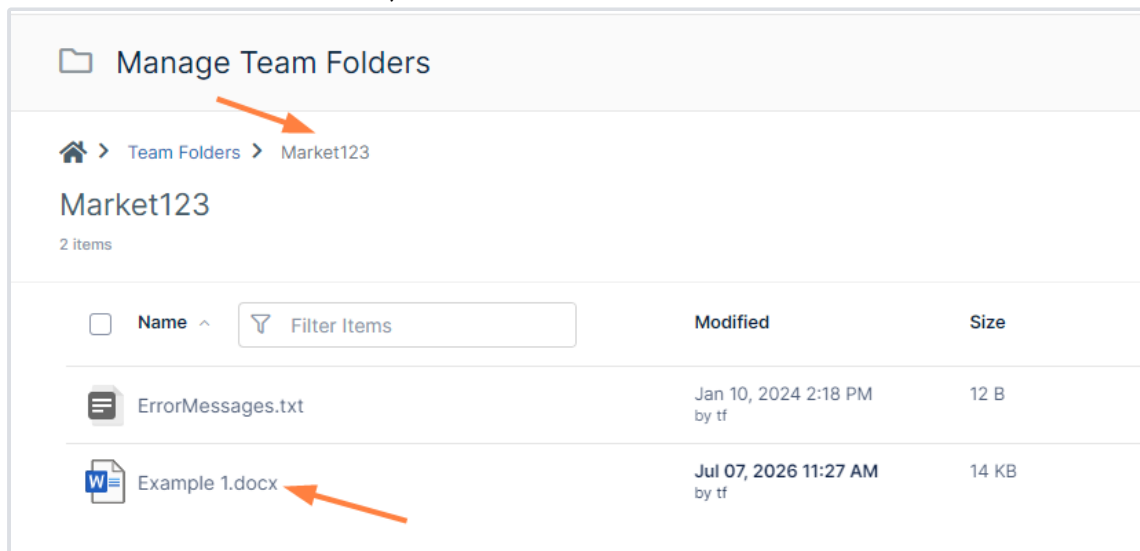
The **Deleted Files/Folders** page opens. The top level of folders includes deleted team folders as well as non-deleted parent team folders of deleted files. For example, in the following screenshot, the **JTeam** and **Photo files** team folders are deleted team folders, but the **Market123** team folder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



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



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



View and Restore Previous Versions in Team Folders



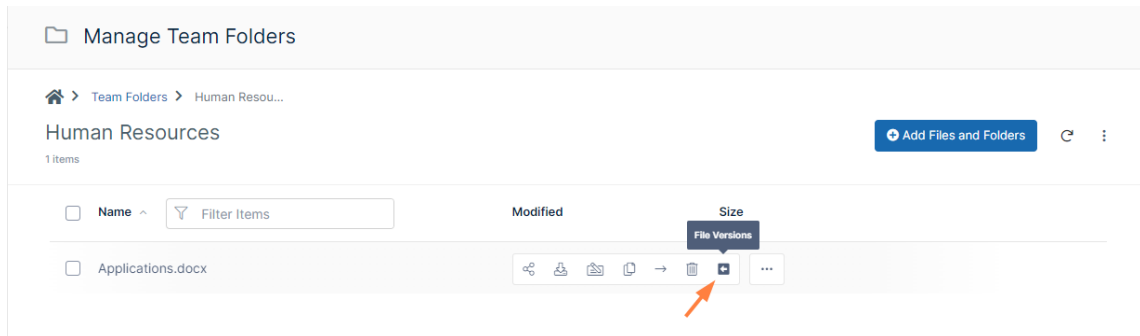
The ability to restore a previous version of a file in Team Folders is available in FileCloud Server version 18.2 and later.

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

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

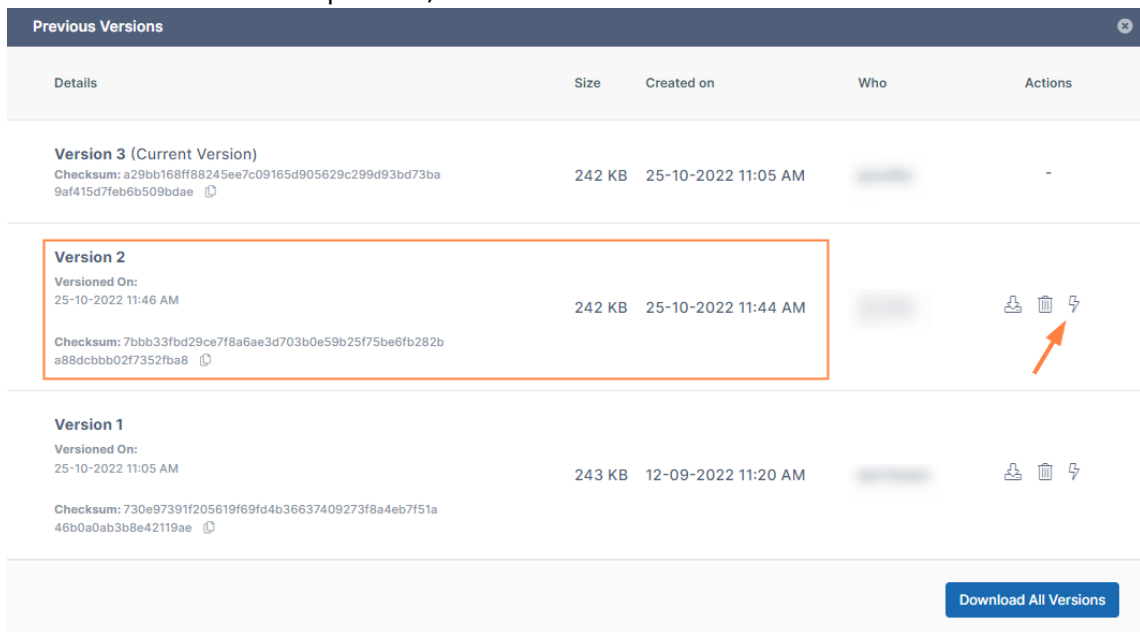
1. Open a browser and log in to the admin portal.

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

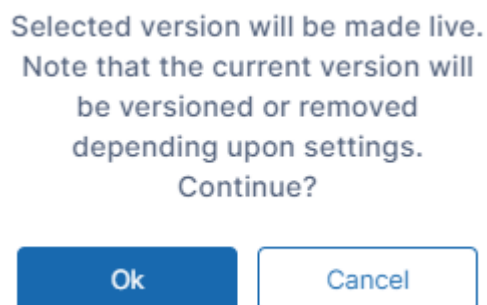


A list of the previous versions opens.

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



The following confirmation box appears:



6. Click **OK**.

The version that was made the current version now appears at the top, and the previous current version appears under it.

(Note that above, the 11:44 AM version was Version 2, but below, after it was made the current version, it is Version 3 at the top of the list.)

Previous Versions				
Details	Size	Created on	Who	Actions
Version 3 (Current Version) Checksum: 7bbb33fbd29ce7f8a6ae3d703b0e59b25f75be6fb282ba88dcbb02f7352fba8	242 KB	25-10-2022 11:44 AM		-
Version 2 Versioned On: 25-10-2022 11:50 AM Checksum: a29bb168ff88245ee7c09165d905629c299d93bd73ba9af415d7feb6b509bdae	242 KB	25-10-2022 11:05 AM		
Version 1 Versioned On: 25-10-2022 11:05 AM Checksum: 730e97391f205619f69fd4b36637409273f8a4eb7f51a46b0a0ab3b8e42119ae	243 KB	12-09-2022 11:20 AM		
				Download All Versions



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

To view and restore previous versions of files in the user portal, see [View Previous Versions Of Files](#)

Managing User Shares

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

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

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

The admin can also export a file listing all shares and their details from the **User Shares** screen.

To set up file sharing, see Share Settings.

To manage user shares for an individual user:

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

User Details

Name

jessica

Total Quota

Unlimited

Email

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

Full

Authentication

Default

Save

Close

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

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

Manage shares for jessica			
Location	Type	Created Date	Actions
/jessica/Internal documents/IMG_20190627_205123685.jpg	Private	Jun 9, 2022 9:41 AM	
/jessica/Internal documents	Private	Jun 9, 2022 9:30 AM	

The **Manage Share** dialog box opens.

4. Make any changes to the share.

Manage Share for file - IMG_20190627_205123685.jpg

Share URL: <https://dev1.codelathe.com/url/tpubf4nr2mzngts>

Share Options

Share Owner:

Shared File/Folder:

Share Name:

Expires (Optional): ☒ Never Expires ☐ Expires

Restrict Downloads (Optional): ☐ No Restrictions ☐ Restrict to

Email File Change Notifications: ☒ Yes ☐ No

Enable Password Protection: ☐ Yes ☒ No

[Update](#)

Share Permissions

☒ Allow Everyone with Link
☐ Allow Selected Users/Groups

Users Group

[Invite Users](#)

User	Allow View	Allow Download	Allow Upload	Allow Share	Misc
Share permitted for all. No users selection necessary.					

[Remove Share](#) [Close](#)

To manage user shares for all users:

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

Manage User Shares

Filter: Show 10 Items [Export](#)

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.

Manage Share for file - 075b2598e4b748f5972e98b1250a6421.jpeg

Share URLhttps://

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

Update

Share Permissions

Allow Everyone with Link

Allow Selected Users/Groups

Guest1

Group

Invite Users

User	Allow View	Allow Download	Allow Upload	Allow Share	Misc

Page1of1

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**.

USERS / GROUPS

Users

Groups

Admins

MANAGE

Team Folders

Network Share

User Share

Folder Permissions

Notifications

DEVICES

Manage User Shares

Filter by Username, Location or Sharename

Show 10 Items

Export

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

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

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

Managing User Shares – 98

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 ?				
Filter	Filter by Username, Location or Sharename	Show 10 Items	Export	
User name	Location	Type	Created Date	Actions
jenniferp	/EXTERNAL/Misc/ASBeach.jfif	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				

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

Manage Share for file - FCSSwitchToClassic.png

Share URL

Share Options

Share Owner

Shared File/Folder

Share Name

Expires (Optional)
☒ Never Expires ☐ Expires

Email File Change Notifications
☒ Yes ☐ No

Update

Share Permissions

☐ Allow Everyone
☒ Allow Selected Users/Groups

Users Group

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

Filter Show 10 Items **Export**

User name	Location	Type	Created Date	Actions
jenniferp	/LOCAL/LOCAL/Misc/ASBeach.jfif	Private	Jan 14, 2021 7:26 AM	
jenniferp	/SHARED/team folder admin/Human Resources/FCSSwitchToClassic.png	Private	Jan 14, 2021 7:22 AM	
team folder admin	/team folder admin/Human Resources/FCSSwitchToClassic.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/MMQj5ggRymicnDib
```

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/MMQj5ggRymicnDib"
```

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.

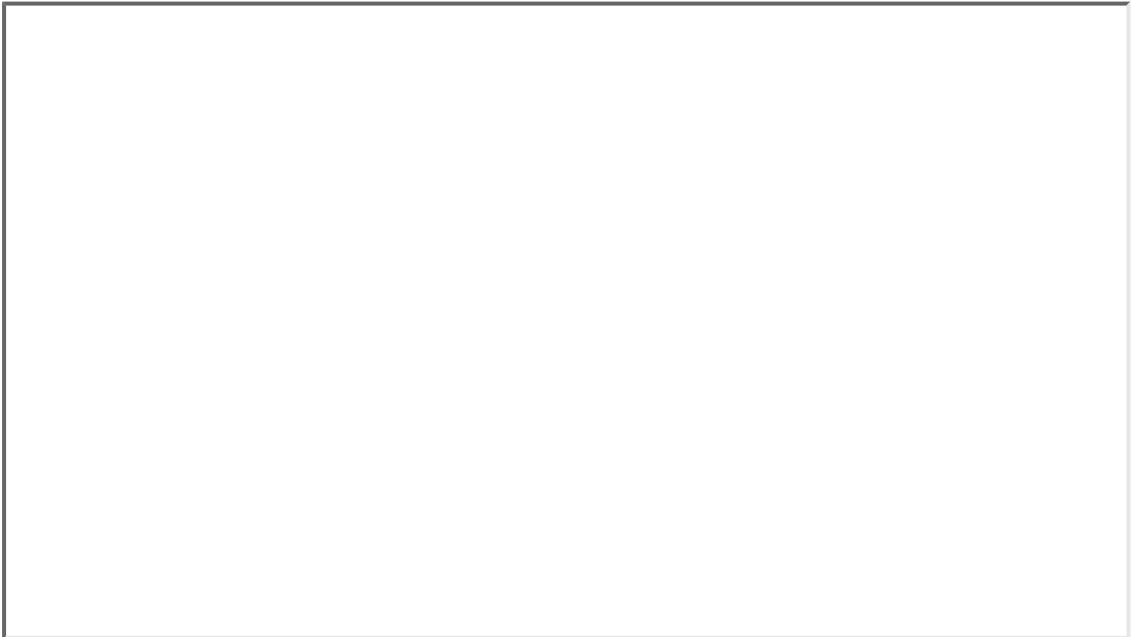
After you create the share, copy the share link and modify it to link to a download page for a file in the folder. Then send the new link to share users.

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:

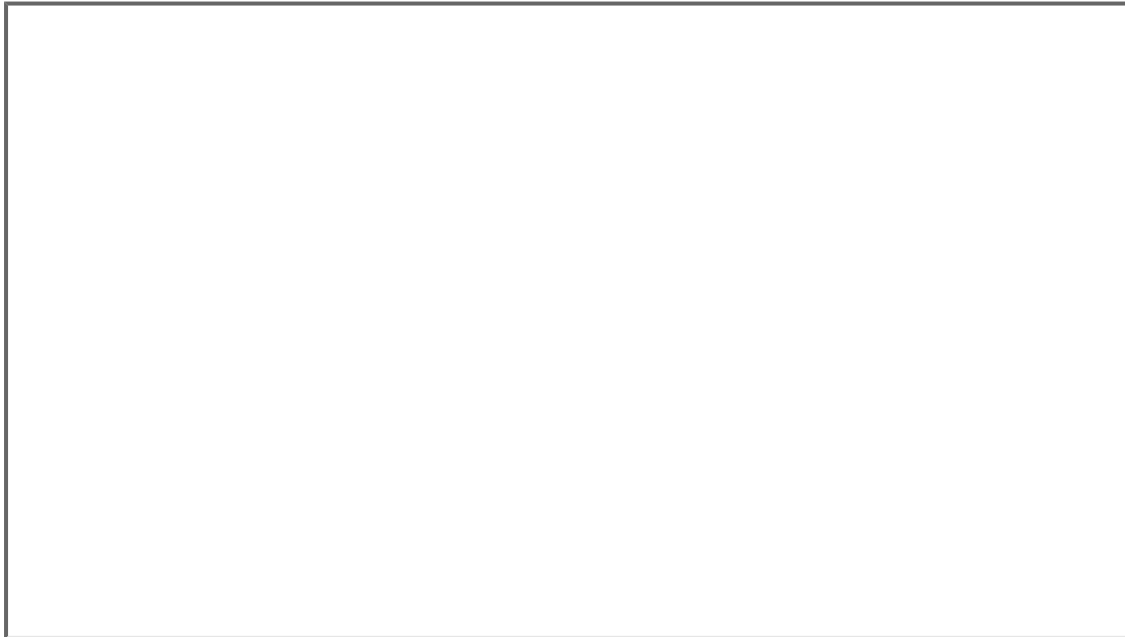
In our example, the link to the shared folder is:

<http://127.0.0.1/ui/core/index.html?mode=public&shareto=#expl-tab1./SHARED/!bli3S5C0tloHQD49yINBKMS5/X00clSQ2AAdiOWP1>

We would like the link to open a download page for the file customers.docx, which is located in the folder.

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

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



1. Remove the portion of the URL that takes you to the FileCloud page, and replace it with a path to a download page.
(Remove [/ui/core/index.html?mode=public&shareto=#expl-tabl](#) and replace it with [core/downloadfile](#).)
2. Add a **filepath** parameter after [core/downloadfile](#) and set it equal to the [/SHARED/](#) portion of the path. Then add the filename, [customers.docx](#), to the end of the path.
(At this point, the path is [http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bli3S5C0tloHQD49yINBKMS5/XOOclSQ2AAdiOWP1/customers.docx](#))
3. After the **filepath** parameter, add a **filename** parameter, and set it equal to [customers.docx](#).
(The final link in the example looks like [http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bli3S5C0tloHQD49yINBKMS5/XOOclSQ2AAdiOWP1/customers.docx&filename=customers.docx](#))
4. Send the link to share users. When clicked, it opens a download page for the customers.docx file.

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

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

[http://127.0.0.1/core/downloadfile?filepath=/SHARED/!bli3S5C0tloHQD49yINBKMS5/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!/bli3S5C0tloHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

**Modified link**

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5C0tloHQD49yINBKMS5/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!/bli3S5C0tloHQD49yINBKMS5/XOOclSQ2AAdiOWP1>

**Modified link**

<https://www.mycompany.com/core/downloadfile?filepath=/SHARED!/bli3S5C0tloHQD49yINBKMS5/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

Related topics

A User's Storage

Change the Storage Quota for a User or Group

[Delete User Files and Folders](#)

[Clear a User's Recycle Bin](#)

[Remove a User's Incomplete Uploads](#)

[Remove Old File Versions](#)

All Managed Storage

Clear Deleted Files Automatically

All Managed Storage Options

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
-----

```

Thumbs Tool for Removing Excessive Thumb Files



The Thumbs tool is available in FileCloud 23.241 and later.

The Thumbs tool removes excessive files in each user's storage space by regularly checking if thumbnails exceed a storage threshold (a certain percent of storage space), and deleting the oldest ones until the space they use is reduced by half. By default, when thumbnails exceed 20% of storage space they are removed until they take up half that amount of space (10%), but you may change the default.

The Thumbs tool runs automatically at regular intervals. However, you can also run it manually by accessing **thumbs.php**.

Windows location: **C:\xampp\htdocs\resources\tools\storage**

Linux location: **/var/www/html/resources/tools/storage**

This tool gives you additional options, such as deleting thumbnails for specific users and thumbnails that are more than a certain number of days old.

Running the Thumbs tool

To run the Thumbs tool, enter:

```
php thumbs.php clear -u user -p path -h hostname
```

Parameters:

--user or **-u** (optional) - The user account (use *all* or omit the parameter for all user accounts)
--path or **-p** (optional) - The path of the storage to be calculated
--host or **-h** (optional) - The fully qualified name of the site in a multisite installation. Omit the option for standalone or default site.

Command options:

clear -f - Clears all thumbs until half the storage threshold (by default half of the threshold is 10%) is reached.

The force parameter **--force** or **-f** (optional) causes the **clear** command to skip the threshold check but still proceed to delete thumbnails until half the storage threshold (10%) is reached.

The following example checks if each user's thumbs take up over 20% of their storage, and if they do, deletes them until they only take up 10% of the user's storage.

```
php thumbs.php clear
```

clear-old -d - Clears all thumbs older than days specified in **--days** or **-d** (required)

The following example clears thumbs more than 8 days old in storage for users monicam, jasonp, and aliyag.

```
php thumbs.php clear-old -d 8 -u monicam,jasonp,aliyag
```

clear-network -d -p - Clears all thumbs older than days specified in **--days** or **-d** (required) under the network path specified in **--path** or **-p** (required)

The following example clears thumbs in the network folder Accounts that are more than 5 days old for all users.

```
php thumbs.php clear-network -d 5 -p /EXTERNAL/Accounts -u all
```

help Displays help notes for the thumbs.php command.

```
php thumbs.php help
```

Example input and output

In the first example, the admin enters: **php thumbs.php clear**. The tool checks the first user and finds that the user's thumbs do not take up 20% or more of storage space, so it does not do thumb cleanup. Then it begins checking the next user:

```
~ /projects/cl-fc-server/server/resources/tools/storage php thumbs.php clear

Starting Service: Thumbs - clear
[20/05/2024 16:22:14]: Starting thumbs threshold based cleanup
[20/05/2024 16:22:14]: Current configuration has a threshold of 20% storage space for thumbs
[20/05/2024 16:22:14]: Fetching thumbs info by user
[20/05/2024 16:22:14]: Executing thumb cleanup for user anotheruser
[20/05/2024 16:22:14]: User has 14 thumbs with a total of 0.06mib
[20/05/2024 16:22:14]: Calculating storage size quota represented by thumbnails
elapsed: 2.14 sec.
[20/05/2024 16:22:16]: Found quota of 2048000mib being 0.06mib [0%] from thumbs
[20/05/2024 16:22:16]: Skipping thumb cleanup from user due to threshold check
[20/05/2024 16:22:16]: Executing thumb cleanup for user teamf
[20/05/2024 16:22:16]: User has 18 thumbs with a total of 0.04mib
[20/05/2024 16:22:16]: Calculating storage size quota represented by thumbnails
```

In the next example, the admin enters: **php thumbs.php clear-old --days 0**. The tool goes through each thumbnail of every user and if it was created before today, deletes it.

```

resources\tools\storage> php thumbs.php clear-old --days 0

Starting Service: Thumbs - clear-old
[20/05/2024 16:25:23]: Starting thumbs cleanup based on creation date
[20/05/2024 16:25:23]: All thumbs older than 0 days will be deleted
[20/05/2024 16:25:23]: Starting removal of thumbnails
[20/05/2024 16:25:25]: 100% 2/2 remaining: 0.00 sec. elapsed: 2.04 sec. | Deleted new_a#pps_creation.gif
[20/05/2024 16:25:25]: Removed 2 thumb files. Cleaned 0.03mib of storage space.

```

In the next example, the admin enters: **php thumbs.php clear-network --days 1 -p /EXTERNAL/external**. The tool checks each thumbnail on the network path **/external** and deletes it if it is over 1 day old.

```

resources\tools\storage> php thumbs.php clear-network --days 1 -p /EXTERNAL/external

Starting Service: Thumbs - clear-network
[20/05/2024 16:26:20]: Starting network thumbs cleanup based on creation date
[20/05/2024 16:26:20]: Starting old thumbnails cleanup for path /EXTERNAL/external
[20/05/2024 16:26:20]: Deleting old thumb: 'C:/share/.cloud/45ed68bb7b15ff2d5b6da893182fc10e.90xx90_1715257005'
[20/05/2024 16:26:21]: Deleting old thumb: 'C:/share/.cloud/4f135343d3d27399be281de82db07304.90xx90_1715391699'
[20/05/2024 16:26:21]: Deleting old thumb: 'C:/share/.cloud/8ed9ed24840abf2c8e2727abb609b812.90xx90_1715218247'
[20/05/2024 16:26:21]: Deleting old thumb: 'C:/share/.cloud/925edb9a4de328c3fa3278a2f9b3ec49.90xx90_1715216142'
[20/05/2024 16:26:21]: Deleting old thumb: 'C:/share/.cloud/a2bb82a2ecf06496ba6265a6571db6c0.90xx90_1715612141'
[20/05/2024 16:26:21]: Deleting old thumb: 'C:/share/test/asda.cloud/c0b95bffa6e67bf1439b10c6c2bd2d2.90xx90_1715392233'
[20/05/2024 16:26:21]: 6 thumbs deleted freeing 0.01mib of space
[20/05/2024 16:26:21]: LAN Network old thumbs cleanup completed

```

Changing the 20% threshold value

You may use the following setting to change the percent of storage space used by thumbnails that triggers Thumbs.php to delete excessive files. When the Thumb tool runs, it will delete thumbnails until they take up half of that percent in storage.

To change the threshold:

1. Open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add the following (16 is an example amount, you may enter any number).

```
define('TONIDOCLOUD_THUMBS_STORAGE_QUOTA_PERCENTAGE_THRESHOLD', 16);
```

The Thumb tool will run for users with 16% of their storage taken up by thumbnails, and it will delete half of them, leaving only 8% of storage filled with thumbnails.

Managing User Locks

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

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

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

How Locking Works

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

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

When a file or folder is locked:

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

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

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

Turn Off All File Locking

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

- This is a system-wide setting

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

To disable locking:

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

General

Reset to defaults

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

America/Chicago

Calendar Type
Note: Gregorian (English) should be changed in the drop-down to Gregorian (common)

Gregorian (English)

Date format

MMM dd, yyyy (Jan 15, 2019)

Time format

h:mm A (2:20 PM)

Apply folder-level security
Apply folder-level security settings to share permissions.

Enable interactive tour on first login

Disable Activity panel
In user portal, hide the Activity tab in the right panel.

Disable right panel for External users
In user portal, hide the right panel if the user is an External user.

Disable Metadata panel
In user portal, hide the Metadata tab in the right panel.

Disable locking

Disable IP check
To avoid unwanted session termination, disable if user's IP address may change.

3. Click **Save**.

How to View Which Files or Folders are Locked

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

Manage File/Folder Locks Clear All Locks i				
Filter 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, view the list of all files and folders currently locked.

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

For example:

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

Release a Single Lock

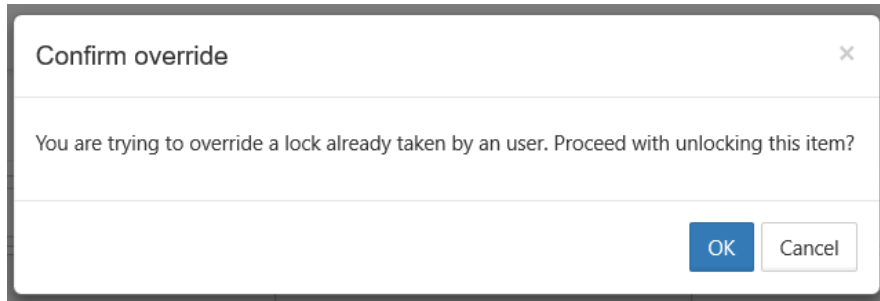
There are times when you may need to unlock a file for a user.

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

To release the lock on a single file or folder:

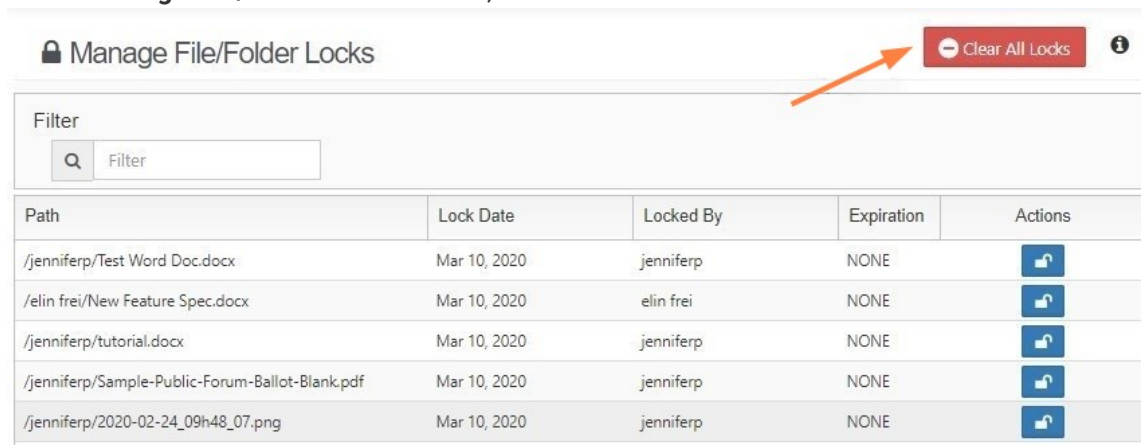
1. Log on to admin portal.
2. From the left navigation pane, click **User Locks**.
3. On the **Manage File/Folder Locks** screen, find the file or folder whose lock you want to remove.

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



To release the lock on all locked files and folders:

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



A confirmation dialog box opens.

- Click **OK**.

Managing User-Defined Notifications

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

Unless you check the **Disable User Override** setting in the policy assigned to a user, they can override your changes to their notification settings in the user interface.

See the page Notifications for file changes for information on disabling user overrides.

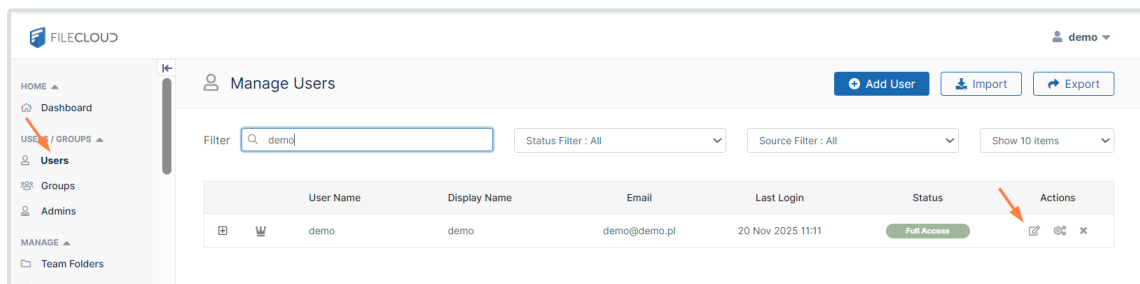
In this section:

Editing individual user's file and folder notifications

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

To edit a user's file and folder notifications:

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



The User Details dialog box opens.

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

User Details

Name

demo

Email

demo@demo.pl

Last Login

20 Nov 2025 11:11

TOS Date

13 Mar 2025 08:25

Group

Manage

Total Quota

10 GB

Used Quota

372 MB

Available Quota

9.6 GB

Used Storage

372 MB

More

Manage Files

Manage Policy

Manage Shares

Mobile Devices

Reset Password

Reset TOTP

Send Email

Manage Notifications

Manage Backups

Delete Account

Profile Image

Update

Remove

Access Level

Full Access

Authentication

Default

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 files for demo			
Path	Modified Date	User	Actions
/demo/a	30/10/2025 5:40 AM	demo	 
/demo/b	04/11/2025 9:14 AM	demo	 

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

Notification Settings for a

Path: /demo/a

☐ Use default notification settings
 ☒ Use my own notification settings

☒ Send Notifications

Send notifications on

☒ Upload
When a file or folder is added

☐ Share
When a file or folder is shared with someone

☐ Rename
When a file or folder is renamed

☐ Preview
When a file is viewed in the browser or in the mobile app

☐ Self Notifications
Send notifications for actions done by me

☐ Download
When a file or folder is downloaded

☐ Delete
When a file or folder is deleted

☐ Update
When a file is modified

☐ Lock/Unlock
When a file or folder is locked or unlocked

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.

Managing User-Defined Notifications – 117

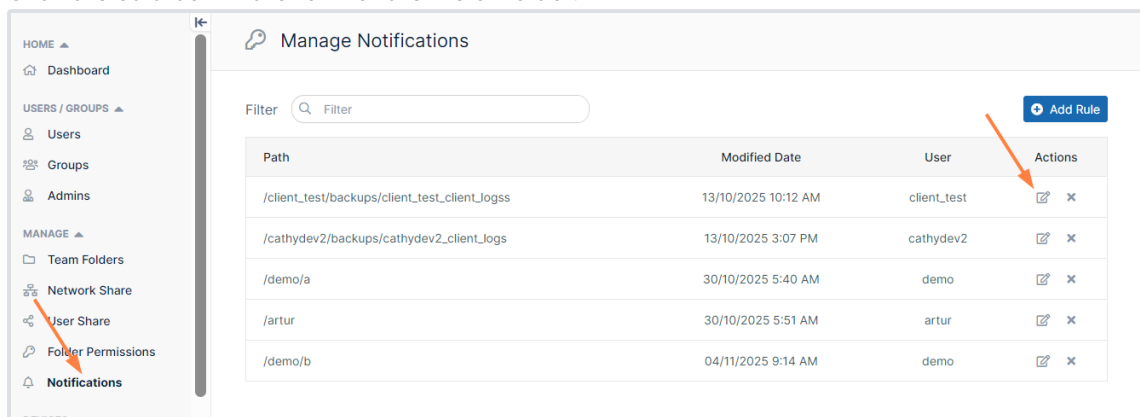
- If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
- If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications** box.
- If the user has **Use default 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 screenshot shows the 'Manage Notifications' interface. On the left, a navigation sidebar lists 'HOME', 'Dashboard', 'USERS / GROUPS' (Users, Groups, Admins), and 'MANAGE' (Team Folders, Network Share, User Share, Folder Permissions, and Notifications). The 'Notifications' item is selected. The main content area has a title 'Manage Notifications' and a search filter. Below is a table with the following data:

Path	Modified Date	User	Actions
/client_test/backups/client_test_client_logss	13/10/2025 10:12 AM	client_test	[Edit] [X]
/cathydev2/backups/cathydev2_client_logs	13/10/2025 3:07 PM	cathydev2	[Edit] [X]
/demo/a	30/10/2025 5:40 AM	demo	[Edit] [X]
/artur	30/10/2025 5:51 AM	artur	[Edit] [X]
/demo/b	04/11/2025 9:14 AM	demo	[Edit] [X]

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

Notification Settings for client_test_client_logss

Path: /client_test/backups/client_test_client_logss

☐ Use default notification settings
☒ Use my own notification settings

☒ Send Notifications

Send notifications on

☒ Upload
When a file or folder is added

☒ Download
When a 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

3. Edit the notification settings:

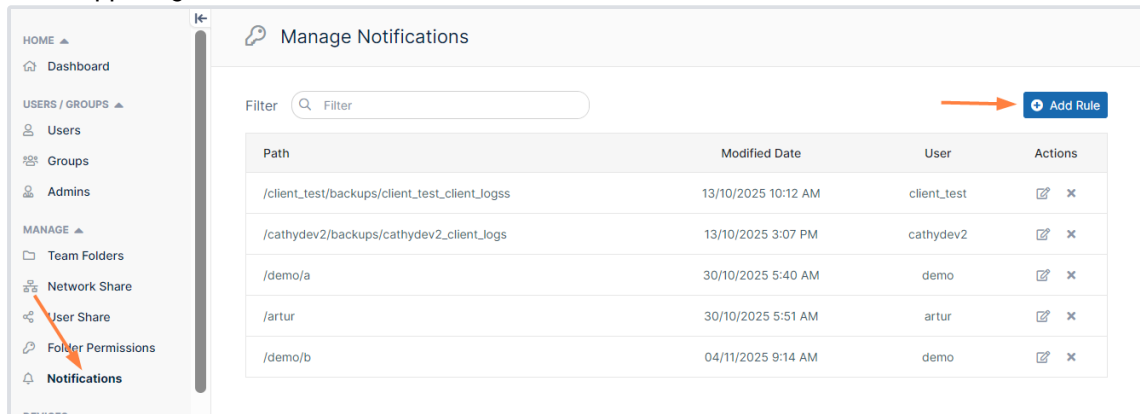
- If you want to reset the user's settings to the defaults, check **Use default notification settings**. **Use my own notification settings** and all of the settings below it become unselected. If the user is permitted to override your settings, they may turn back on **Use my own notification settings**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

Adding notifications for actions on user's files and folders

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

To add notifications to users files or folder

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



The screenshot shows the 'Manage Notifications' interface. On the left, the navigation menu has 'Notifications' highlighted. The main content area has a title 'Manage Notifications' and a search filter. Below the filter is a table with the following data:

Path	Modified Date	User	Actions
/client_test/backups/client_test_client_logss	13/10/2025 10:12 AM	client_test	
/cathydev2/backups/cathydev2_client_logs	13/10/2025 3:07 PM	cathydev2	
/demo/a	30/10/2025 5:40 AM	demo	
/artur	30/10/2025 5:51 AM	artur	
/demo/b	04/11/2025 9:14 AM	demo	

An orange arrow points to the 'Add Rule' button in the top right corner of the main area.

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

Notification Settings for

Account or Email

Path*

☐ Use default notification settings
☒ Use my own notification settings

☒ Send Notifications

Send notifications on

☒ Upload
When a file or folder is added

☐ Download
When a 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

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**.

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

FAQ's

What Devices Can Connect?



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

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

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

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

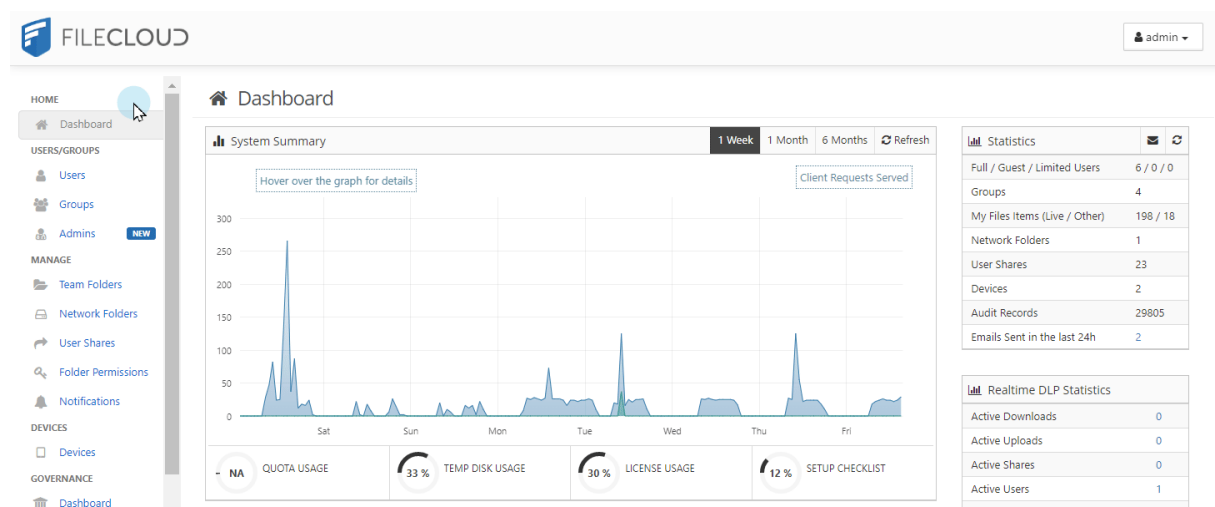
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

Where Can I See a List of Connected Devices?

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

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

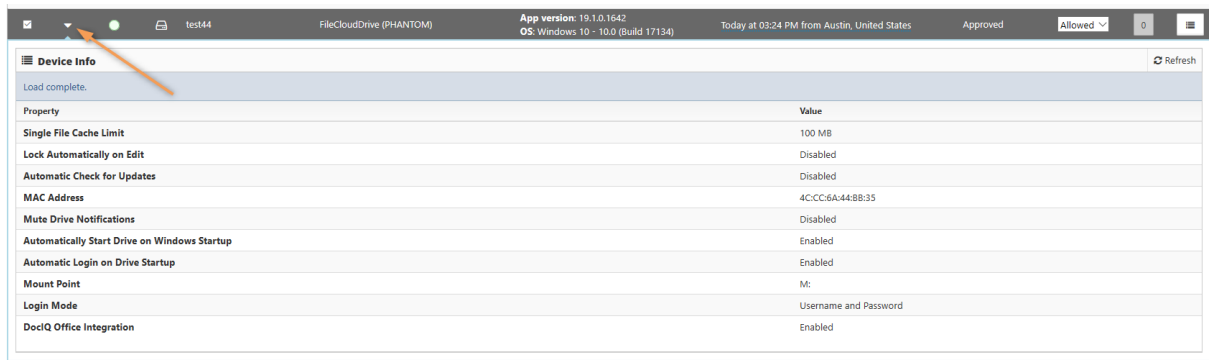
💡 Sometimes a list may start out empty. However, as users connect devices to the FileCloud Server by logging in, the devices will appear.



How Do You Want to Manage a Device?

The following operations are available from the Device Management panel:

View Details of a Client Device



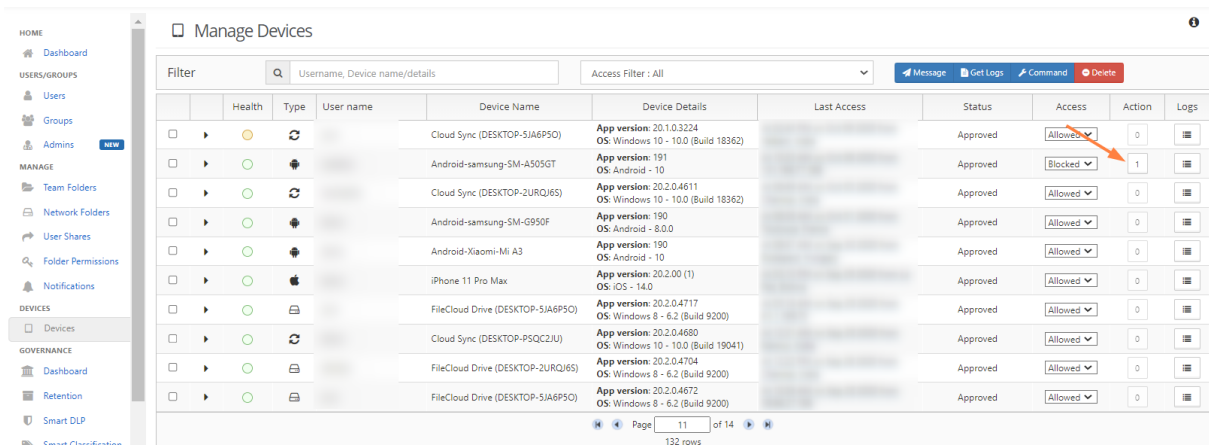
Property	Value
Single File Cache Limit	100 MB
Lock Automatically on Edit	Disabled
Automatic Check for Updates	Disabled
MAC Address	4C:CC:6A:44:8B:35
Mute Drive Notifications	Disabled
Automatically Start Drive on Windows Startup	Enabled
Automatic Login on Drive Startup	Enabled
Mount Point	M:
Login Mode	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
☐				Cloud Sync (DESKTOP-5JA6P5O)	App version: 20.1.0.3224 OS: Windows 10 - 10.0 (Build 18362)		Approved	Allowed	0	
☐				Android-samsung-SM-A505GT	App version: 191 OS: Android - 10		Approved	Blocked	1	
☐				Cloud Sync (DESKTOP-2URQJ6S)	App version: 20.2.0.4611 OS: Windows 10 - 10.0 (Build 18362)		Approved	Allowed	0	
☐				Android-samsung-SM-G950F	App version: 190 OS: Android - 8.0.0		Approved	Allowed	0	
☐				Android-Xiaomi-Mi A3	App version: 190 OS: Android - 10		Approved	Allowed	0	
☐				iPhone 11 Pro Max	App version: 20.2.0.0 (1) OS: iOS - 14.0		Approved	Allowed	0	
☐				FileCloud Drive (DESKTOP-5JA6P5O)	App version: 20.2.0.4717 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	
☐				Cloud Sync (DESKTOP-PSQC2JU)	App version: 20.2.0.4680 OS: Windows 10 - 10.0 (Build 19041)		Approved	Allowed	0	
☐				FileCloud Drive (DESKTOP-2URQJ6S)	App version: 20.2.0.4704 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	
☐				FileCloud Drive (DESKTOP-5JA6P5O)	App version: 20.2.0.4672 OS: Windows 8 - 6.2 (Build 9200)		Approved	Allowed	0	

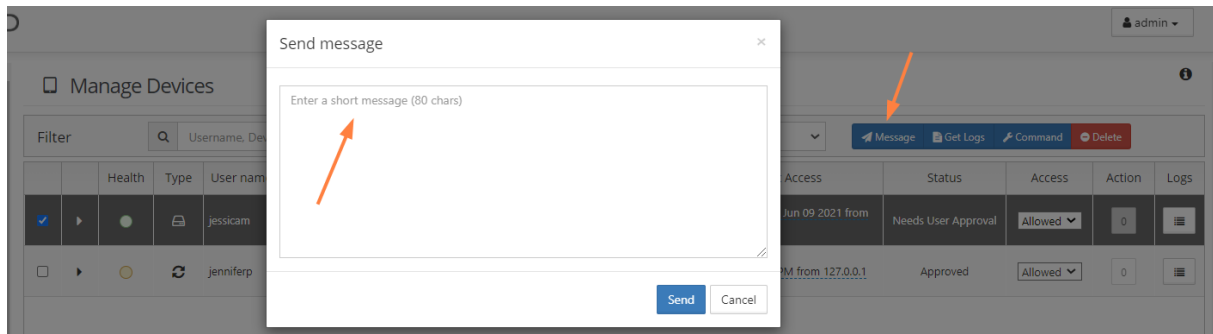
To view Actions:

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.

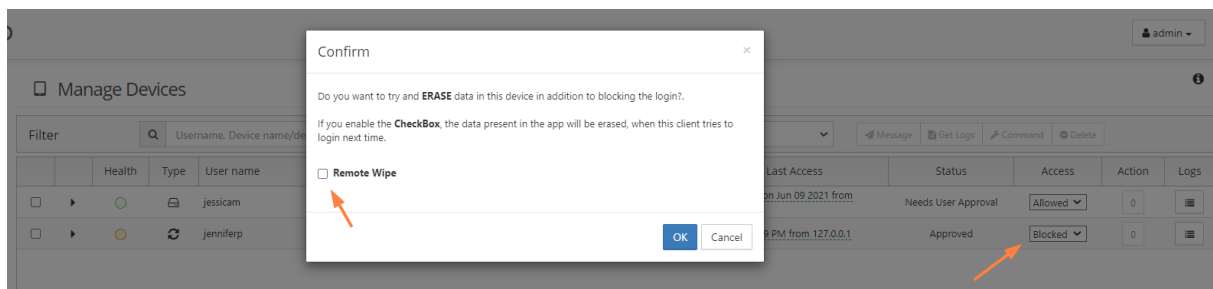
When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

- 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

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



To block (but not wipe remote data):

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

To block and wipe remote data in a client device:

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

6. Click *OK*.

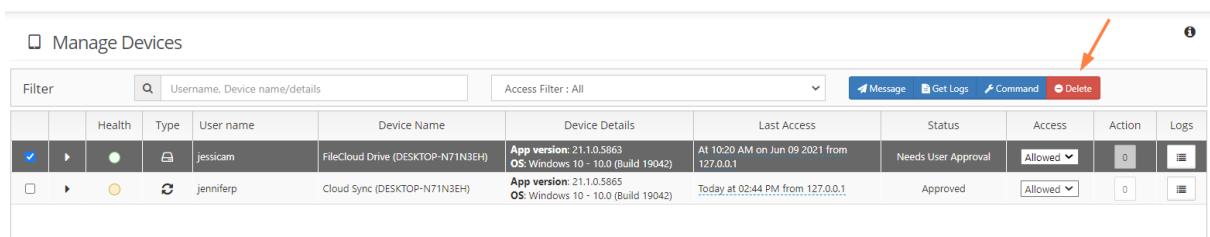
Delete a Client Device Record

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

You might want to use this feature when:

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

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



To delete a client device record:

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

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

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

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

Configure Centralized Device Management

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



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

To set a device configuration for a policy:

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

The **Policies** settings page opens.

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	
TEAM FOLDER POLICY	1	0	☐	

<<

<

Page 1 of 1

>

>>

2 rows

- 2. Edit the policy of the users whose client device settings you want to modify.
- 3. Click the **Device Configuration** tab.
- 4. Paste or type in the remote device configuration XML in **Device Configuration**.

Effective Policy: "Global Default Policy"

General

2FA

User Policy

Client Application Policy

Device Configuration

Notifications

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

Device Configuration

Client Configuration

<xml>

<winclouddrive>

<!-- XML for Windows Drive -->

</winclouddrive>

</xml>

Customize default configuration for any of your client applications in valid XML

Cancel

Reset

Save

- 5. Click **Save**.

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>

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

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

</xml>

```

What do you want to configure?

Device Configuration XML For Drive for Mac

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



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

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

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<< < Page 1 of 1 > >>

2 rows

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

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

Effective Policy: "Global Default Policy"

General2FAUser PolicyClient Application PolicyDevice ConfigurationNotifications

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

Device Configuration

Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

Cancel

Reset

Save

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

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

Managing Client Devices – 133

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

Device Configuration XML For Outlook Add-in

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



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

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

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

The **Policies** settings page opens.

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	
TEAM FOLDER POLICY	1	0	☐	

<<

<

Page 1 of 1

>

>>

2 rows

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

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

Effective Policy: "Global Default Policy"

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

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

Device Configuration
Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

Cancel Reset Save

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

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

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

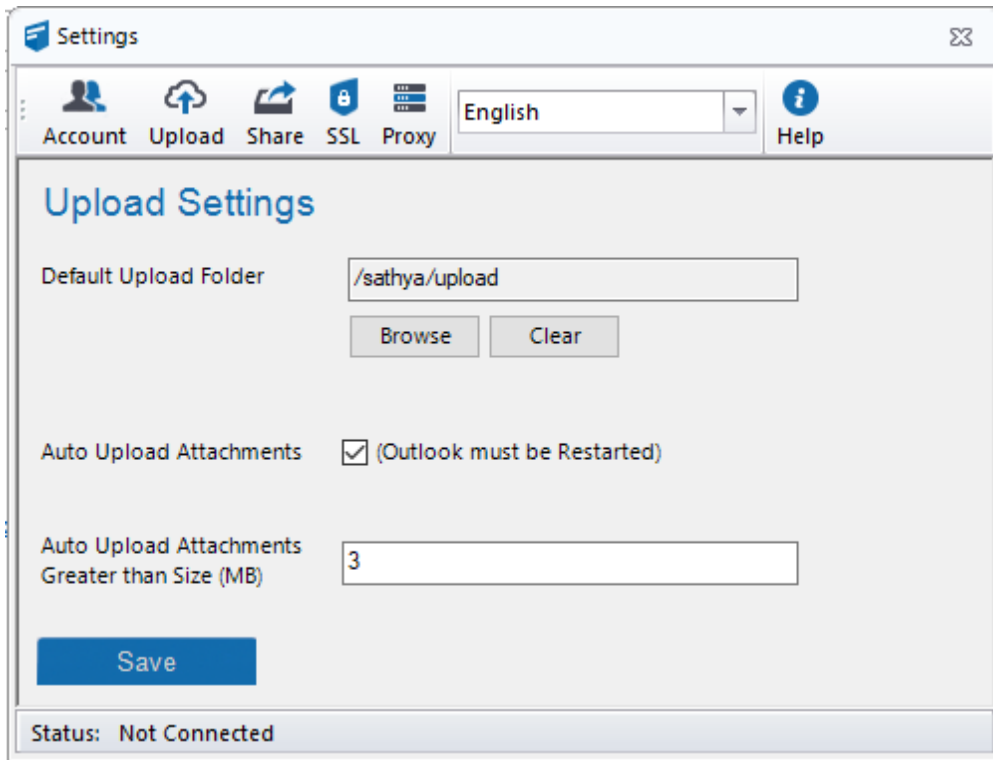
To set default values for auto upload:

In the Outlook add-in device configuration, you can set the default values for **Auto Upload Attachments** and **Auto Upload Attachments Greater than Size (MB)**.

Follow the instructions above for setting the device configuration, and enter values: for <autoupload> and <autouploadsize>, for example:

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

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



The screenshot shows the 'Settings' window with the 'Upload' tab selected. The 'Upload Settings' section contains the following fields and controls:

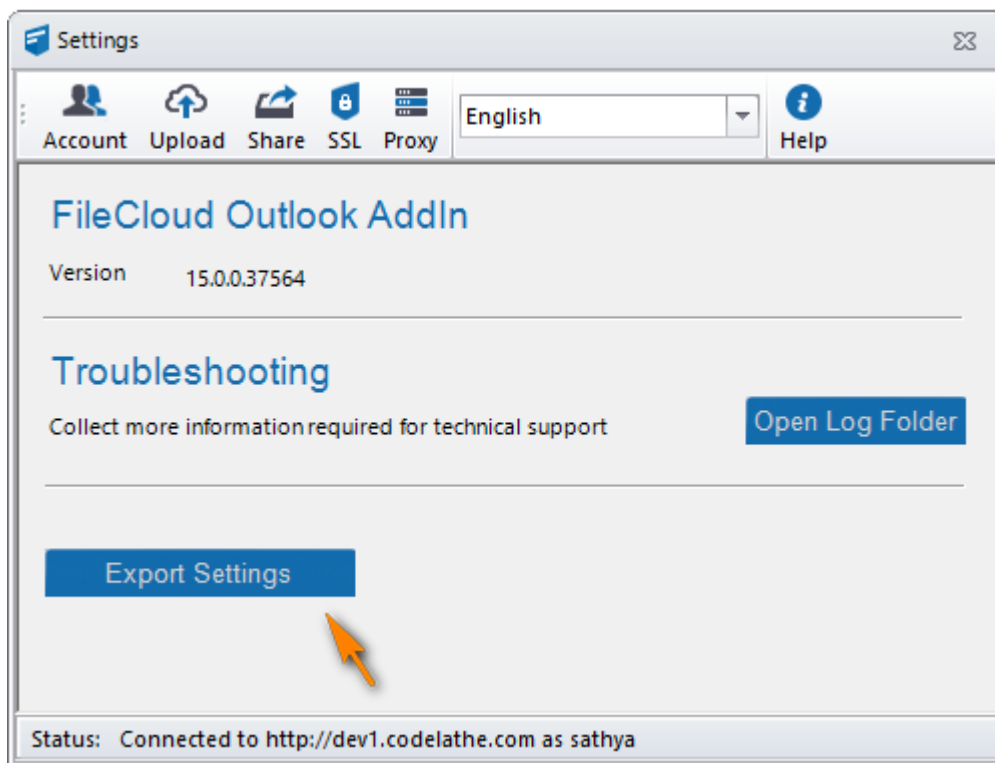
- Default Upload Folder:** A text box containing '/sathya/upload' with 'Browse' and 'Clear' buttons below it.
- Auto Upload Attachments:** A checkbox that is checked, with the text '(Outlook must be Restarted)' next to it.
- Auto Upload Attachments Greater than Size (MB):** A text box containing the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

The top of the window features a navigation bar with icons for Account, Upload, Share, SSL, and Proxy, a language dropdown set to 'English', and a Help icon.

💡 Tips and Tricks

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

Show me how...



Device Configuration XML For Server Sync

Client Device configuration settings can be configured remotely using policies.



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

To set a ServerSync device configuration in a policy:

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

The **Policies** settings page opens.

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	
TEAM FOLDER POLICY	1	0	☐	

<<

<

Page 1 of 1

>

>>

2 rows

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

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

Effective Policy: "Global Default Policy"

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications

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

Device Configuration
Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

Cancel
Reset
Save

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

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

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

Device Configuration XML For Sync

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



For the Sync client, when an Admin sets a remote client policy, a user working in the Sync app cannot modify the settings. Sync will display a message saying "Centralized Configuration is being applied. Settings cannot be changed."

Any Sync settings in the config xml block the user's ability to configure selective sync, network folder, and backup folder settings. If you want users to be able to continue to change these settings, set the `allowuserconfigforlimitsync`, `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 FileCloud Sync device configuration in a policy:

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<< < Page 1 of 1 > >>

2 rows

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

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

Effective Policy: "Global Default Policy"

General2FAUser PolicyClient Application PolicyDevice ConfigurationNotifications

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

Device ConfigurationClient Configuration

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

Customize default configuration for any of your client applications in valid XML.

CancelResetSave

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

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

Managing Client Devices – 144

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

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

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

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

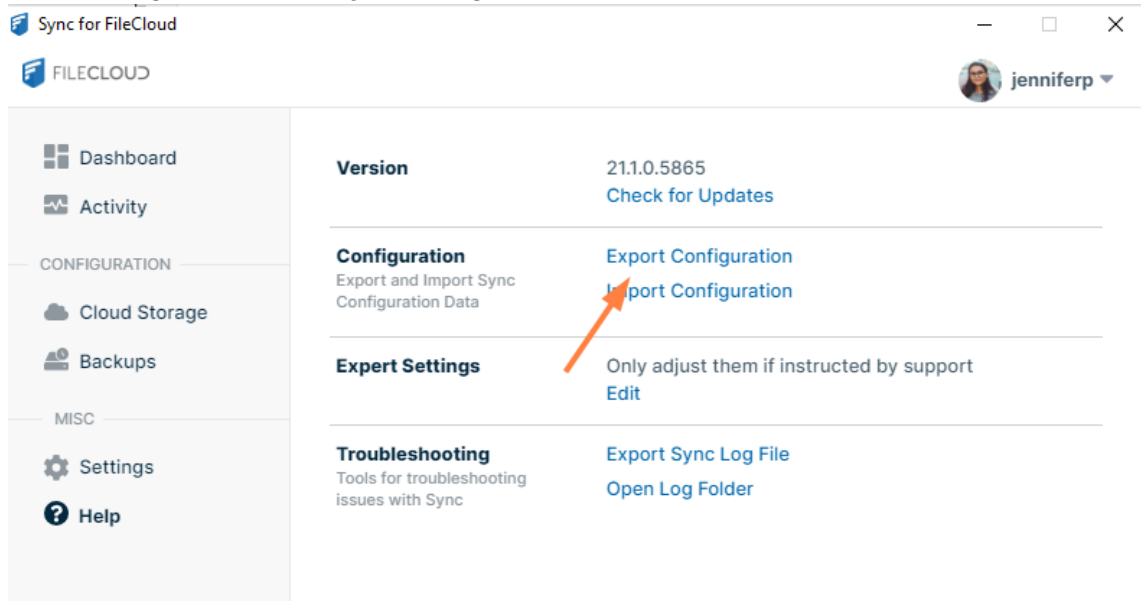
How do I get the configuration XML for Sync?

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

To export Sync configuration settings:

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

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



What variables are supported?

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

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

What is the XML code for limiting bandwidth rates?

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

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



Set Bandwidth Rate Limits for Sync

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

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

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

The XML code will include the following lines:

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

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

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



If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwto time* 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	<pre><timeactivecontrolsset>1</timeactivecontrolsset></pre>

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 overrides any <i>limitfolder</i> settings.	<allowuserconfigforlimitsync>1</allowuserconfigforlimitsync>
allowuserconfigfornewfolders	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 overrides any <i>offlinefolder</i> setting configured for Network folders.	<allowuserconfigfornewfolders>1</allowuserconfigfornewfolders>
allowuserconfigforbackup	0 = user cannot modify the Backup folder and any <i>offlinefolder</i> setting configured for Backup folders, if present, is applied. 1 = user can modify the folder and this overrides any <i>offlinefolder</i> setting configured for Backup folders	<allowuserconfigforbackup>1</allowuserconfigforbackup>

Scenarios

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

Controlling modifications to selective sync folders

limitfolders	allowuserconfig orlimitsync	Sync User's Access
/john/folder1 /john/ folder2	1	Although limit folders are present, because <i>allowuserconfigforlimitsync</i> is set to allow modifications: <i>limitfolder</i> settings will NOT be applied - Users CAN modify their selective sync folders
/john/folder1 /john/ folder2	0	Because limit folders are present, AND <i>allowuserconfigforlimitsync</i> is set to disable modifications: <i>limitfolder</i> settings will BE applied - Users CANNOT modify their selective sync folders
<i>None set but other settings are present</i>	1	Because <i>allowuserconfigforlimitsync</i> is set to allow modifications: 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	Because <i>allowuserconfigforlimitsync</i> is set to disable modifications: Users CANNOT modify their selective sync folders

Controlling modifications to selective network folders

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

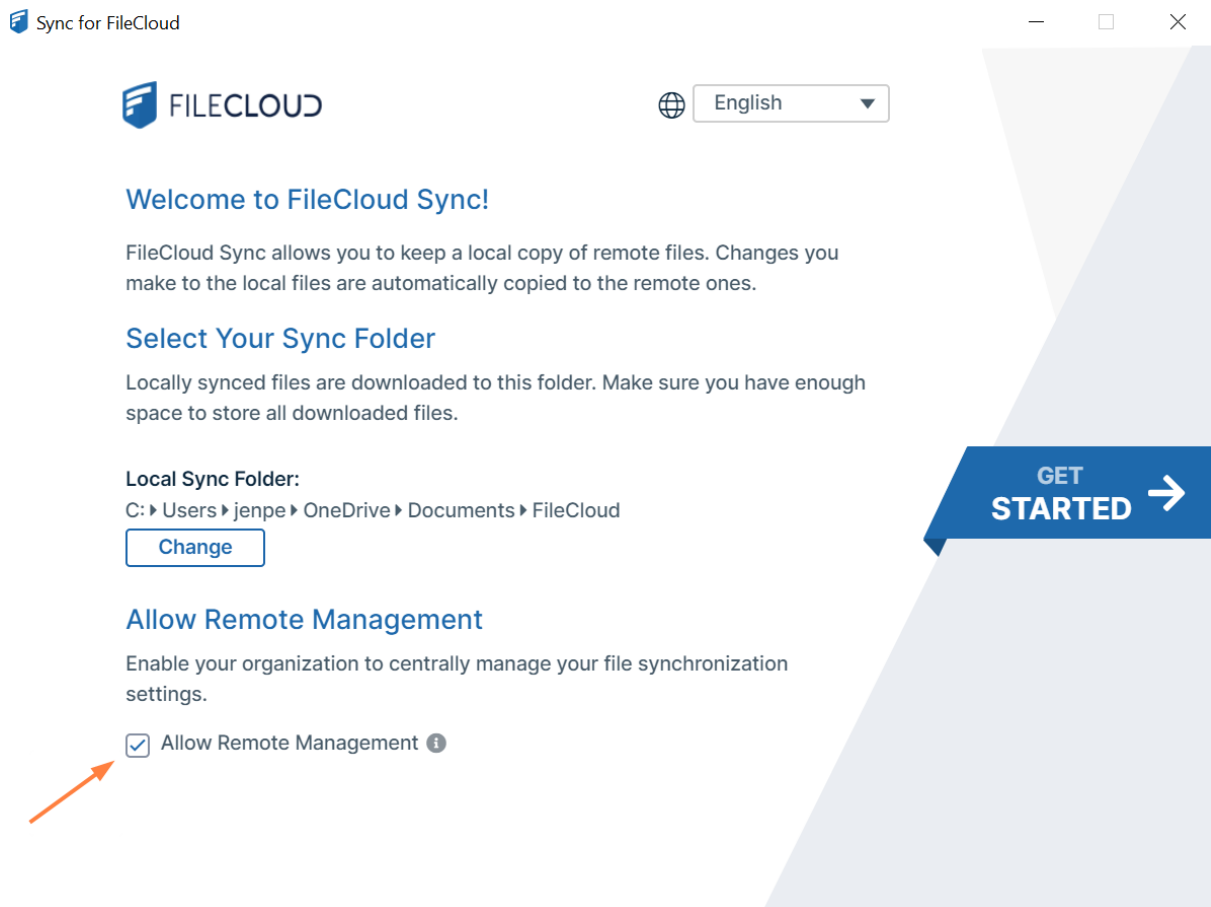
<i>None set but other settings are present</i>	1	Because <i>allowuserconfigfornewfolders</i> is set to enable modifications : • Sync users CAN modify Network Folders, irrespective of any other settings in the config.
<i>None set but other settings are present</i>	0	Because <i>allowuserconfigfornewfolders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

Controlling modifications to selective backup folders

offline folders	allowuserconfigforbackup	Sync User's Access
C:\data\local	1	Because offline folders (configured for backup) are present, AND <i>allowuserconfigforbackup</i> is set to enable modifications : • <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 : • <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 : • 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 : • Sync users CANNOT modify backup folders

How do I prevent users from overriding remote management?

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



This setting is also available in the Settings window.

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

To add the registry key:

1. Add a registry key under:

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

2. Name the registry key:

```
allowcentralmgmtusermodify
```

3. Restart the computer.

Device Configuration XML For Windows Drive

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



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

To set a FileCloud Drive device configuration in a policy:

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<<

<

Page 1 of 1

>

>>

2 rows

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

```
<xml>
```

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

Effective Policy: "Global Default Policy" ✕

General2FAUser PolicyClient Application PolicyDevice ConfigurationNotifications

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

Device Configuration

Client Configuration

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

Customize default configuration for any of your client applications in valid XML

Cancel

Reset

Save

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

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

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

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

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

Device Configuration XML for Desktop Edit

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



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

To set FileCloud Desktop Edit device configuration in a policy:

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

The **Policies** settings page opens.

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	
TEAM FOLDER POLICY	1	0	☐	

<<

<

Page 1 of 1

>

>>

2 rows

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

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

Effective Policy: "Global Default Policy"

General2FAUser PolicyClient Application PolicyDevice ConfigurationNotifications

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

Device Configuration

Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

CancelResetSave

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

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

Device Configuration XML for FileCloud Desktop for macOS

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

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

Managing Client Devices – 161

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<< < Page 1 of 1 > >>

2 rows

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

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

Effective Policy: "Global Default Policy" ✕

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications

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

Device Configuration

Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

Cancel
Reset
Save

<default> is an optional tag that indicates if the setting can be changed through the user interface.

A value of 1 indicates the setting is a default and can be changed by the user through the user interface.

A value of 0 (or omission of <default>) indicates that the setting is overridden and cannot be changed by the user through the user interface.

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

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

Parameter (Key)	Description	Values																				
language	Language of the FileCloud Desktop for macOS user interface.	<table><tr><th>Value</th><th>Language</th></tr><tr><td>nl</td><td>Dutch</td></tr><tr><td>en (default)</td><td>English</td></tr><tr><td>de</td><td>German</td></tr><tr><td>es</td><td>Spanish</td></tr><tr><td>pt</td><td>Portuguese</td></tr><tr><td>fr</td><td>French</td></tr><tr><td>ar</td><td>Arabic</td></tr><tr><td>it</td><td>Italian</td></tr><tr><td>ru</td><td>Russian</td></tr></table>	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)																				

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.

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

Device Configuration XML for FileCloud Desktop for Windows

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



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

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	0	0	☒	
TEAM FOLDER POLICY	1	0	☐	

<< < Page 1 of 1 > >>

2 rows

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

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


Effective Policy: "Global Default Policy"

General2FAUser PolicyClient Application PolicyDevice ConfigurationNotifications

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

Device Configuration

Client Configuration

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

Customize default configuration for any of your client applications in valid XML.

Cancel

Reset

Save

<default> is an optional tag that indicates if the setting can be changed through the user interface.

A value of 1 indicates the setting is a default and can be changed by the user through the user interface.

A value of 0 (or omission of <default>) indicates that the setting is overridden and cannot be changed by the user through the user interface.

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

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

Managing Client Devices – 167

language	Language of the FileCloud Desktop for Windows user interface.	<table><tr><th>Value</th><th>Language</th></tr><tr><td>nl</td><td>Dutch</td></tr><tr><td>en (default)</td><td>English</td></tr><tr><td>de</td><td>German</td></tr><tr><td>es</td><td>Spanish</td></tr><tr><td>pt</td><td>Portuguese</td></tr><tr><td>fr</td><td>French</td></tr><tr><td>ar</td><td>Arabic</td></tr><tr><td>it</td><td>Italian</td></tr><tr><td>ru</td><td>Russian</td></tr></table>	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)																				

Example:

The code below shows example settings:

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

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

In this example:

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

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

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>

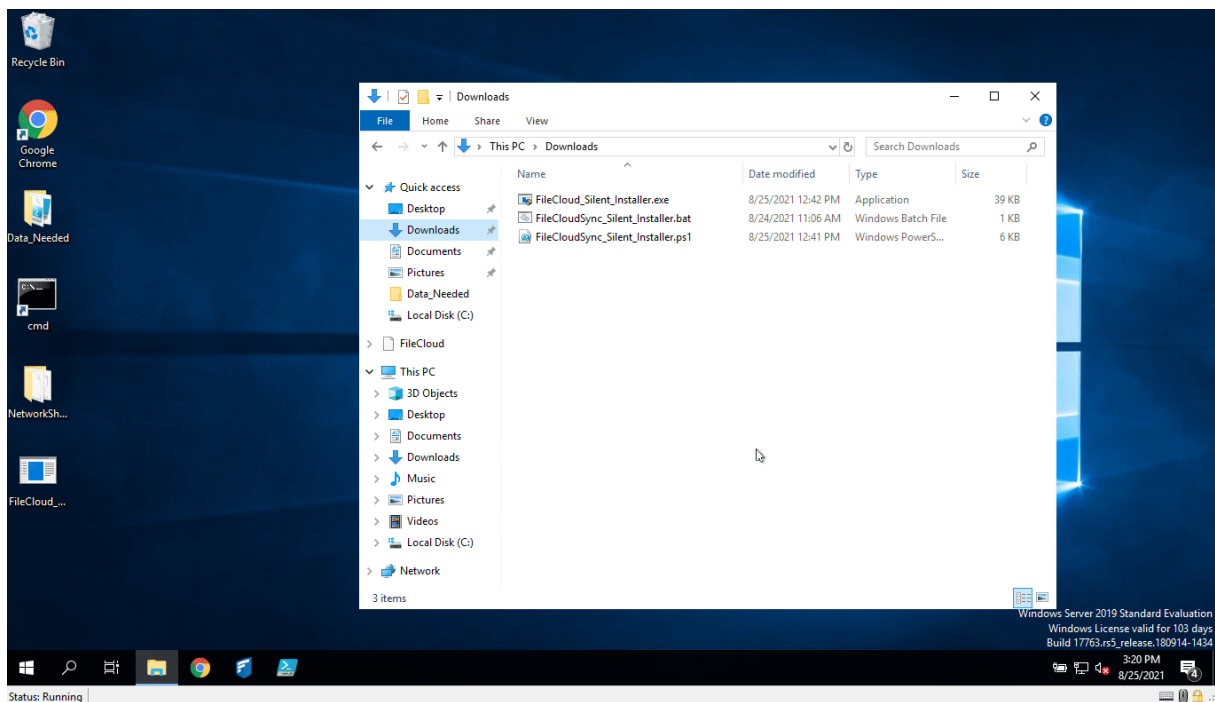
What does the Script do?

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

```
####Silent FileCloud Sync Installation & Mass Deployment Configuration####

##Allows the script to be executed without user consent##
set-ExecutionPolicy RemoteSigned -Force

### Sets the absolute path for the log file##
$Logfile = 'C:\FileCloudSync_SilentInstaller.log'

##Validates if the log file already exists if so it deletes it and creates a new log
file##
if (Test-Path -Path "C:\FileCloudSync_SilentInstaller.log") {
    Remove-Item 'C:\FileCloudSync_SilentInstaller.log' -Recurse
    New-Item -Path "c:\" -Name "FileCloudSync_SilentInstaller.log" -ItemType "file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}
else {
    New-Item -Path "c:\" -Name "FileCloudSync_SilentInstaller.log" -ItemType "file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}

##Check if FileCloud Sync is already installed if its installed cancel the installation
else continue##
if (Test-Path -Path "C:\Users\$env:USERNAME\AppData\Roaming\FileCloudSyncData\client")
{
    "FileCloud Sync is already installed, Unable to proceed with the installation" |
    Out-File $Logfile -Append
    clear
    Write-Warning "FileCloud Sync is already installed, Please uninstall FileCloud Sync
in order to proceed"
    $Input = Read-Host -Prompt "Press any key to Exit"
    Exit
}
Else {

    ##Create the directory where FileCloud Sync will be downloaded##
    Try {
        if (Test-Path -Path "C:\FileCloudSync") {
            Remove-Item 'C:\FileCloudSync' -Recurse
            "Folder already exists, Deleted Folder under C:\FileCloudSync " | Out-File
$Logfile -Append
            New-Item -Path "c:\" -Name "FileCloudSync" -ItemType "directory"
            -ErrorAction Stop
            "Created folder under C:\FileCloudSync " | Out-File $Logfile -Append
        }
    }
}
```

```

    }
    else {
        New-Item -Path "c:\\" -Name "FileCloudSync" -ItemType "directory"
    -ErrorAction Stop
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Downloads the FileCloud Sync Installer into the directory created##
Try {
    "Downloading FileCloud Sync.msi installer" | Out-File $Logfile -Append
    $url1 = "https://patch.codeatthe.com/tonido/live/installer/x86-win32/
FileCloudSync2.msi"
    $output1 = "C:\FileCloudSync\FileCloudSync2.msi"
    $start_time = Get-Date
    Import-Module BitsTransfer
    Start-BitsTransfer -Source $url1 -Destination $output1
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Validates if FileCloud has downloaded completely based on the file hash##

$hashSrc = "9B0F053DF45605E1CA819396D66B046310FE386BCF1B00A3F1B3B685B6FF29CA"
$fileToCheck = "C:\FileCloudSync\FileCloudSync2.msi"
$hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"

Try {
    if ($hashSrc.Hash -ne $hashDest.Hash) {
        "FileCloud Sync Installer downloaded successfully" | Out-File $Logfile
    -Append
    }
    else {
        "FileCloud Sync Installer was NOT downloaded or it has not been download
completely" | Out-File $Logfile -Append
        Exit
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Installs FileCloud Sync silently without needing any end-user interaction##
Try {

```

```

        Start-Process -Wait -FilePath "C:\FileCloudSync\FileCloudSync2.msi"
-ArgumentList '/quiet', '/passive', '/n' -passthru -ErrorAction Stop
        "FileCloud Installation Started" | Out-File $Logfile -Append
    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }

##Adds the needed registry keys to configure Mass Deployment##
cd HKLM:\

Try {
    set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the path within the registry
Try {
    Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name
'CodeLathe\FileCloud\DefaultCfg\' -Force -ErrorAction Stop
    "Creating registry entry" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the needed keys to assign the predefined settings
Try {
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'url' -Value "https://your-filecloud-url.com" -PropertyType String -Force
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'allowcentralmgmt' -Value "1" -PropertyType String -Force
    "Creating predefined parameters" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Exits the registry
Pop-Location

#Start FileCloud Sync#
Try {
    Start-Process -FilePath "C:\Program Files\FileCloud Sync\cloudsync.exe"
    "Starting FileCloud Sync" | Out-File $Logfile -Append
}

```

```

}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

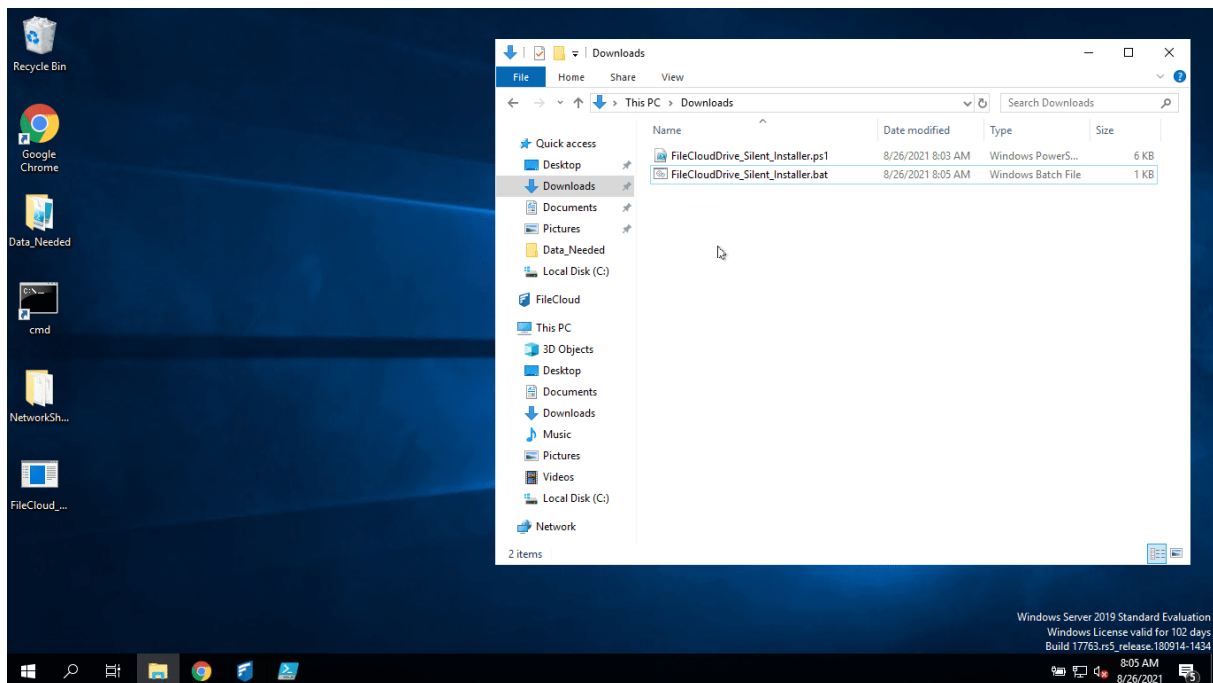
##Cleanup- Deletes the folder created and the installer within#
Try {
    Remove-Item 'C:\FileCloudSync' -Recurse
    "Deleting FileCloudSync download folder under C:\FileCloudSync " | Out-File
$Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Installation Completed - Closes PowerShell##
"Installation Completed" | Out-File $Logfile -Append

stop-process -Id $PID
exit
}

```

FileCloud Drive Installation & Mass Deployment automation - Video



FileCloud Drive Installation & Mass Deployment automation - Script

FileCloud Drive Installation & Mass Deployment automation

```
####Silent FileCloud Drive Installation & Mass Deployment Configuration####

##Allows the script to be executed without user consent##
set-ExecutionPolicy RemoteSigned -Force

### Sets the absolute path for the log file##
$Logfile = 'C:\FileCloudDrive_SilentInstaller.log'

##Validates if the log file already exists if so it deletes it and creates a new log
file##
if (Test-Path -Path "C:\FileCloudDrive_SilentInstaller.log") {
    Remove-Item 'C:\FileCloudDrive_SilentInstaller.log' -Recurse
    New-Item -Path "c:\" -Name "FileCloudDrive_SilentInstaller.log" -ItemType "file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}
else {
    New-Item -Path "c:\" -Name "FileCloudDrive_SilentInstaller.log" -ItemType "file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}

##Check if FileCloud Drive is already installed if its installed cancel the
installation else continue##
if (Test-Path -Path "C:\Users\%env:USERNAME%\AppData\Roaming\FileCloudDriveData\client")
{
    "FileCloud Drive is already installed, Unable to proceed with the installation" |
    Out-File $Logfile -Append
    clear
    Write-Warning "FileCloud Drive is already installed, Please uninstall FileCloud
Drive in order to proceed"
    $Input = Read-Host -Prompt "Press any key to Exit"
    Exit
}
Else {

    ##Create the directory where FileCloud Drive will be downloaded##
    Try {
        if (Test-Path -Path "C:\FileCloudDrive") {
            Remove-Item 'C:\FileCloudDrive' -Recurse
            "Folder already exists, Deleted Folder under C:\FileCloudDrive " | Out-File
$Logfile -Append
            New-Item -Path "c:\" -Name "FileCloudDrive" -ItemType "directory"
            -ErrorAction Stop
            "Created folder under C:\FileCloudDrive " | Out-File $Logfile -Append
        }
    }
}
```

```

    }
    else {
        New-Item -Path "c:\" -Name "FileCloudDrive" -ItemType "directory"
    -ErrorAction Stop
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Downloads the FileCloud Drive Installer into the directory created###
Try {
    "Downloading FileCloud Drive.msi installer" | Out-File $Logfile -Append
    $url1 = "https://patch.codebathe.com/tonido/live/installer/x86-win32/
FileCloudDrive2eSetup.msi"
    $output1 = "C:\FileCloudDrive\FileCloudDrive2eSetup.msi"
    $start_time = Get-Date
    Import-Module BitsTransfer
    Start-BitsTransfer -Source $url1 -Destination $output1
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Validates if FileCloud has downloaded completely based on the file hash##

$hashSrc = "1FCD2F88DD7615E68A2AD935AECCE4D04DD61ED769E52008002B1F7CA3CB7A17"
$fileToCheck = "C:\FileCloudDrive\FileCloudDrive2eSetup.msi"
$hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"

Try {
    if ($hashSrc.Hash -ne $hashDest.Hash) {
        "FileCloud Drive Installer downloaded successfully" | Out-File $Logfile
    -Append
    }
    else {
        "FileCloud Drive Installer was NOT downloaded or it has not been download
completely" | Out-File $Logfile -Append
        Exit
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Installs FileCloud Drive silently without needing any end-user interaction##
Try {

```

```

        Start-Process -Wait -FilePath "C:\FileCloudDrive\FileCloudDrive2eSetup.msi"
-ArgumentList '/quiet', '/passive', '/n' -passthru -ErrorAction Stop
        "FileCloud Installation Started" | Out-File $Logfile -Append
    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }

##Adds the needed registry keys to configure Mass Deployment##
cd HKLM:\

Try {
    set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the path within the registry
Try {
    Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name
'CodeLathe\FileCloud\DefaultCfg\' -Force -ErrorAction Stop
    "Creating registry entry" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the needed keys to assign the predefined settings
Try {
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'url' -Value "https://your-filecloud-url.com" -PropertyType String -Force
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'allowcentralmgmt' -Value "1" -PropertyType String -Force
    "Creating predefined parameters" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Exits the registry
Pop-Location

#Start FileCloud Drive#
Try {
    Start-Process -FilePath "C:\Program Files\FileCloud Drive\clouddrive.exe"
    "Starting FileCloud Drive" | Out-File $Logfile -Append
}

```

```

    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }

    ##Cleanup- Deletes the folder created and the installer within#
    Try {
        Remove-Item 'C:\FileCloudDrive' -Recurse
        "Deleting FileCloudDrive download folder under C:\FileCloudDrive " | Out-File
$Logfile -Append
    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }

    ##Installation Completed - Closes PowerShell##
    "Installation Completed" | Out-File $Logfile -Append

    stop-process -Id $PID
    exit
}

```

FileCloud Outlook Addin Installation & Mass Deployment automation - Script

FileCloud Outlook Addin

```

####Silent FileCloud Outlook_Plugin Installation & Mass Deployment Configuration####

##Allows the script to be executed without user consent##
set-ExecutionPolicy RemoteSigned -Force

### Sets the absolute path for the log file##
$Logfile = 'C:\FileCloudOutlookplugin_SilentInstaller.log'

##Validates if the log file already exists if so it deletes it and creates a new log
file##
if (Test-Path -Path "C:\FileCloudOutlook_Plugin_SilentInstaller.log") {
    Remove-Item 'C:\FileCloudOutlook_Plugin_SilentInstaller.log' -Recurse
    New-Item -Path "c:\" -Name "FileCloudOutlook_Plugin_SilentInstaller.log" -ItemType
"file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}
else {
    New-Item -Path "c:\" -Name "FileCloudOutlook_Plugin_SilentInstaller.log" -ItemType
"file"
    "#####Created log file and started login#####" | Out-File $Logfile -Append
    "Set-Execution Policy Successful" | Out-File $Logfile -Append
}

```

```

}

##Check if FileCloud Outlook_Plugin is already installed if its installed cancel the
installation else continue##
if (Test-Path -Path "C:\Users\$env:USERNAME\AppData\Roaming\FileCloudOutlookAddIn") {
    "FileCloud Outlook_Addin is already installed, Unable to proceed with the
    installation" | Out-File $Logfile -Append
    clear
    Write-Warning "FileCloud Outlook_Plugin is already installed, Please uninstall
    FileCloud Outlook_Plugin in order to proceed"
    $Input = Read-Host -Prompt "Press any key to Exit"
    Exit
}
Else {

    ##Create the directory where FileCloud Outlook_Plugin will be downloaded##
    Try {
        if (Test-Path -Path "C:\FileCloudOutlook_Plugin") {
            Remove-Item 'C:\FileCloudOutlook_Plugin' -Recurse
            "Folder already exists, Deleted Folder under C:\FileCloudOutlook_Plugin " |
            Out-File $Logfile -Append
            New-Item -Path "c:\" -Name "FileCloudOutlook_Plugin" -ItemType "directory"
            -ErrorAction Stop
            "Created folder under C:\FileCloudOutlook_Plugin " | Out-File $Logfile
            -Append
        }
        else {
            New-Item -Path "c:\" -Name "FileCloudOutlook_Plugin" -ItemType "directory"
            -ErrorAction Stop
        }
    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }

    ##Downloads the FileCloud Outlook_Plugin Installer into the directory created###
    Try {
        "Downloading FileCloud Outlook_Addin.exe installer" | Out-File $Logfile -Append
        $url1 = "https://patch.codelathe.com/tonidocloud/live/installer/
        FileCloudOutlookAddIn.exe"
        $output1 = "C:\FileCloudOutlook_Plugin\FileCloudOutlookAddin.exe"
        $start_time = Get-Date
        Import-Module BitsTransfer
        Start-BitsTransfer -Source $url1 -Destination $output1
    }
    Catch {
        $message = $_
        "ERROR $_ " | Out-File $Logfile -Append
    }
}

```

```

##Validates if FileCloud has downloaded completely based on the file hash##

$hashSrc = "0789F44D02453BEF3A7E9B533325CD90584BF37C5FC0F8F09611A5B7D417F505"
$fileToCheck = "C:\FileCloudOutLook_Plugin\FileCloudOutLookAddin.exe"
$hashDest = Get-FileHash $fileToCheck -Algorithm "SHA256"

Try {
    if ($hashSrc.Hash -ne $hashDest.Hash) {
        "FileCloud OutLook_Plugin Installer downloaded successfully" | Out-File
$Logfile -Append
    }
    else {
        "FileCloud OutLook_Plugin Installer was NOT downloaded or it has not been
download completely" | Out-File $Logfile -Append
        Exit
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##check if outlook is running if so kills it before proceeding.

Try {
    $app = 'OUTLOOK'

    $process = Get-Process $app -ErrorAction SilentlyContinue
    if ($process) {
        Stop-Process $process -Force
        Write-Output "$app has been stopped."
    }
    else {
        Write-Output "$app is not running."
    }
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Installs FileCloud OutLook_Plugin silently without needing any end-user
interaction##
Try {
    Start-Process -Wait -FilePath "C:
\FileCloudOutLook_Plugin\FileCloudOutlookAddin.exe" -ArgumentList '/VERYSILENT', '/
SUPPRESSMSGBOXES' -passthru -ErrorAction Stop
    "FileCloud Installation Started" | Out-File $Logfile -Append
}

```

```

Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

##Adds the needed registry keys to configure Mass Deployment##
cd HKLM:\

Try {
    set-location -path HKLM:\SOFTWARE\ -ErrorAction Stop
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the path within the registry
Try {
    Get-Item -Path 'HKLM:\SOFTWARE\' | New-Item -Name
'CodeLathe\FileCloud\DefaultCfg\' -Force -ErrorAction Stop
    "Creating registry entry" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Create the needed keys to assign the predefined settings
Try {
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'url' -Value "https://your-filecloud-url.com" -PropertyType String -Force
    New-ItemProperty -Path 'HKLM:\SOFTWARE\CodeLathe\FileCloud\DefaultCfg' -Name
'allowcentralmgmt' -Value "1" -PropertyType String -Force
    "Creating predefined parameters" | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

# Exits the registry
Pop-Location

##Cleanup- Deletes the folder created and the installer within#
Try {
    Remove-Item 'C:\FileCloudOutLook_Plugin' -Recurse
    "Deleting FileCloudOutLook_Plugin download folder under C:
\FileCloudOutLook_Plugin " | Out-File $Logfile -Append
}
Catch {
    $message = $_
    "ERROR $_ " | Out-File $Logfile -Append
}

```

```
##Installation Completed - Closes PowerShell##
"Installation Completed" | Out-File $Logfile -Append

stop-process -Id $PID
exit
}
```

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
```

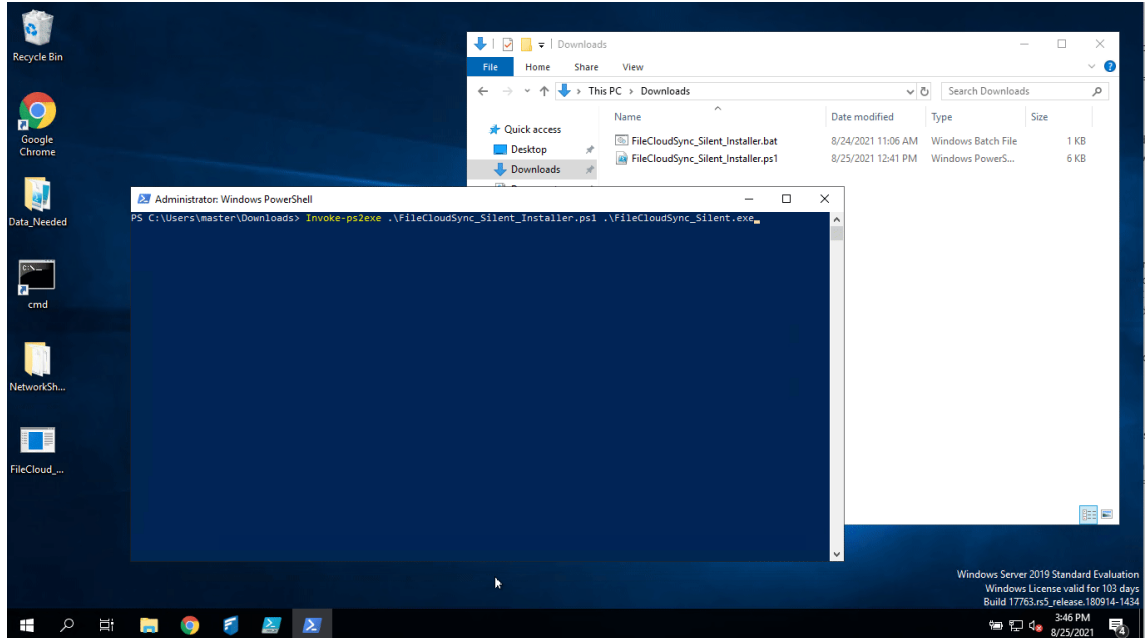
2. Once the above is completed enter "Y" to install the Module

```
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

FileCloud MacDrive (v1.0.0 - 2)

App version: 1.0
OS: Darwin - 17.2.0

Today at 02:45 PM from Austin, United States

Approved

Allowed

0

Device Info

Refresh

Load complete.

Property	Value
Single File Cache Limit	30 MB
Lock Automatically on Edit	Disabled
Automatic Check for Updates	Disabled
MAC Address	
Mute Drive Notifications	Disabled
Automatically Start Drive on Startup	Disabled
Mount Point	/Users/user/cloudmount/
Login Mode	Username and Password

What do you want to view?

Blocking and Remotely Wiping a Client Device

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

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

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

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

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

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

Steps to block and wipe remote data in a client device

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

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

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

Sending a Message to a Client's Display

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

The entered message(s) will be displayed when the remote client is connected to the FileCloud instance. If more than one message is queued to a device, they will be displayed in the order it was entered. The messages will be shown only once per client and during

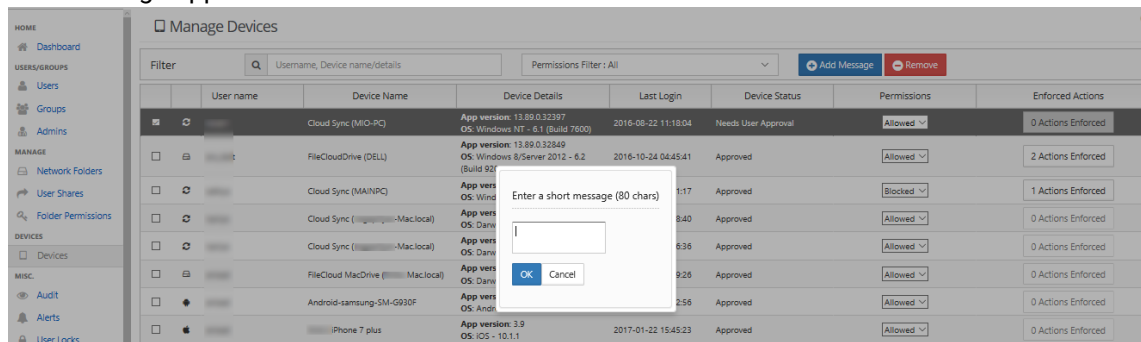
Message will be shown

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

Steps to add message

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

The message appears on the remote client.



iOS Device Management

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

Configuring Automatic Camera Uploads

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

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

Why would I enable this feature?

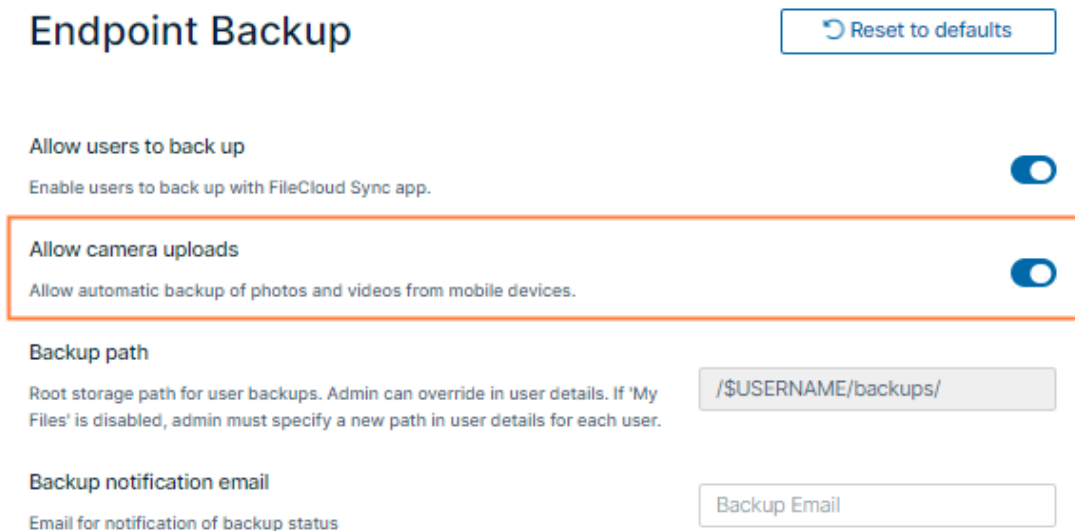
- This is a very convenient feature and it mobile users to know that your photos and videos are always saved in a safe location.

- Instead users saving all of their work files on their mobile device, they can save them to the FileCloud.
 - Mobile users can spend time constantly managing their images/videos to free up more space unless they are able to save them to FileCloud.
 - If you are concerned about privacy and security, work-related files and photos are stored securely in FileCloud.
- 💡 Keep in mind that with the amount of photos and videos generated by the mobile devices, the storage size can run out quickly.

To enable automatic camera uploads:

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

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



Endpoint Backup Reset to defaults

Allow users to back up Enable users to back up with FileCloud Sync app. ☒

Allow camera uploads Allow automatic backup of photos and videos from mobile devices. ☒

Backup path Root storage path for user backups. Admin can override in user details. If 'My Files' is disabled, admin must specify a new path in user details for each user.

Backup notification email Email for notification of backup status

Mass Deployment - Default Configuration Support

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
httpproxypassword	String	Proxy User Authentication password to use	YES	YES	YES	YES	YES

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
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) 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	Pas NO	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:\filecloud\drive Expanded Paths - e.g. %APPDATA%\FileCloud Drive\data (Windows Only) or \${HOME}\FileCloud Drive (Windows and Mac OSX)	NO	YES	NO	NO	NO
enablesortcachepath	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
drivedefaultstorageingb	String	The value in GB of the default user quota setting	NO	YES	YES	NO	NO

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
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
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

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
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
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

Parameter	Type	Notes	Sync	Windows Drive	Mac Drive	Office Add-On	Outlook Add-On
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	Syn c	Win dow s Drive	Mac Drive	Office Add-On	Out look Add-On
disablerecoveri ng	String	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. "0" - (default) Files are copied to recovered folder before upload occurs. "1" - Files are copied to recovered folder after upload is attempted if upload fails.	NO	YES	YES	NO	NO
disableprecachi ng	String	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. "0" – (default) File/folder directory is retrieved when Drive starts up. "1" - File/folder directory is retrieved when a user starts navigating the folders.	NO	YES	YES	NO	NO
lockexpirationin min	String	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.	NO	YES	YES	NO	NO

Parameter	Type	Notes	Syn c	Win dow s Dri ve	Ma c Dri ve	Offic e Add- On	Out loo k Ad d- On
disablelockexpir ation	String	Whether or not to enable expiring of locks. By default, locks on files expire after 10 minutes or the time set in lockexpirationinmin . "0" - (default) Use expiration times set for file locks. "1" - Do not use expiration times on locks. Locks expire on files when users close them.	NO	YES	YES	NO	NO
enablethumbna ilpreview	String	Whether or not to display thumbnails and previews of listed files. "0" - (default) Do not display thumbnails and previews (this reduces network traffic since files are downloaded when thumbnails and previews are generated) "1" - Display thumbnails and previews.	NO	NO	YES	NO	NO
maxdownloadsi zeinmb	String	Default single file download limit in MB. 0 - No limit Other options can be 10,30,50, 100	NO	YES	YES	NO	NO
allowcentralmg mt	String	Allow central management 0 - No Central Management 1- Allow Central Management	YES	NO	NO	NO	NO
globalbwforupl oad	String	Specifies the bandwidth limit when uploading files from the client to the server in terms of KB only.	YES	NO	NO	NO	NO
globalbwfordo wnload	String	Specifies the bandwidth limit when downloading files from the server to the client in terms of KB only.	YES	NO	NO	NO	NO

Parameter	Type	Notes	Syn c	Win dow s Drive	Mac Drive	Office Add-On	Out look Add-On
altbwforupload	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
altbwfordownload	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
altbwfromtime	String	Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit.	YES	NO	NO	NO	NO
altbwtotime	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
altbwschedule_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: -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: -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

Corel

ASIO

ATI

ATI Technologies

Brother

CallbackFS

Canon_Inc_IC

Carnegie Mellon

Classes

Clients

CloudBerryLab

CodeLathe

FileCloud

DefaultCfg

Corel

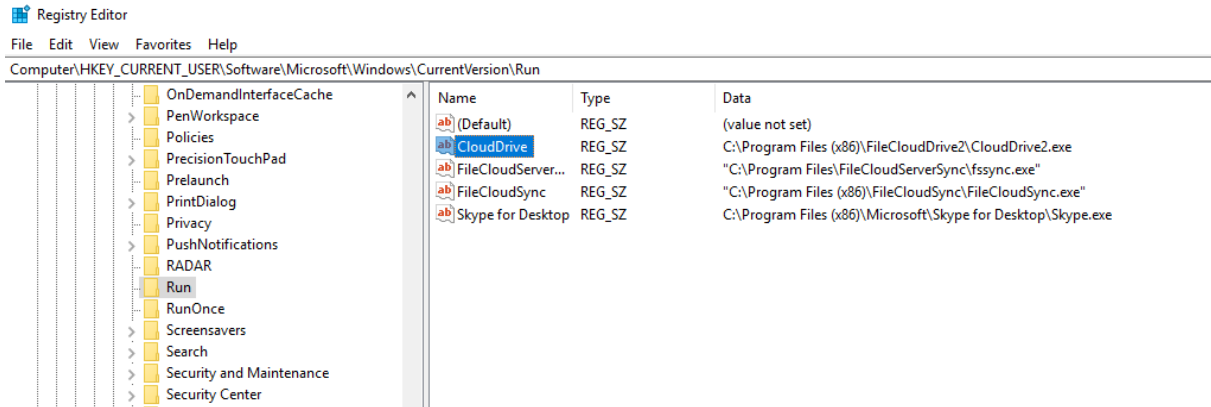
Cygwin

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>driveunlockonupdate</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.

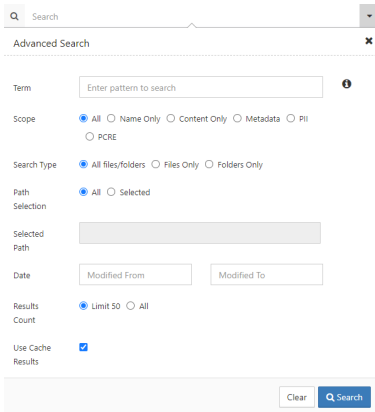
To perform a basic search on the entire site:

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.

The screenshot displays the FileCloud Admin Portal interface. On the left is a sidebar with navigation links: User Shares, Folder Permissions, Notifications, DEVICES (Devices), GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification), MISC. (Audit, Alerts, User Locks, Workflows, Reports), Federated Search, Metadata, and SETTINGS (Settings). The main content area shows search results for the term 'user'. At the top, it says 'Search Results Location: All' and 'Page 1 of 2'. Below this, a message states 'Searching for 'user'' and 'Search completed 18 hours ago. Found 11 results.' with links for 'Search Again' and 'Download Results'. The search results table lists files such as 'FCInactiveUsers.png', 'UsersOne.txt', and 'AA-Sharing Flows.pptx'. A context menu is open over the 'AA-Sharing Flows.pptx' file, showing options like 'Share', 'Add User', 'Search', 'Add Profile', 'Add User', 'Share', 'Send Share Email', 'Show Templates', and 'Get'. Red arrows point to the 'user' in the filename of the first result and the 'Add User' option in the context menu, with labels 'search term "user" in filename' and 'search term "user" in contents' respectively.

Advanced Searches

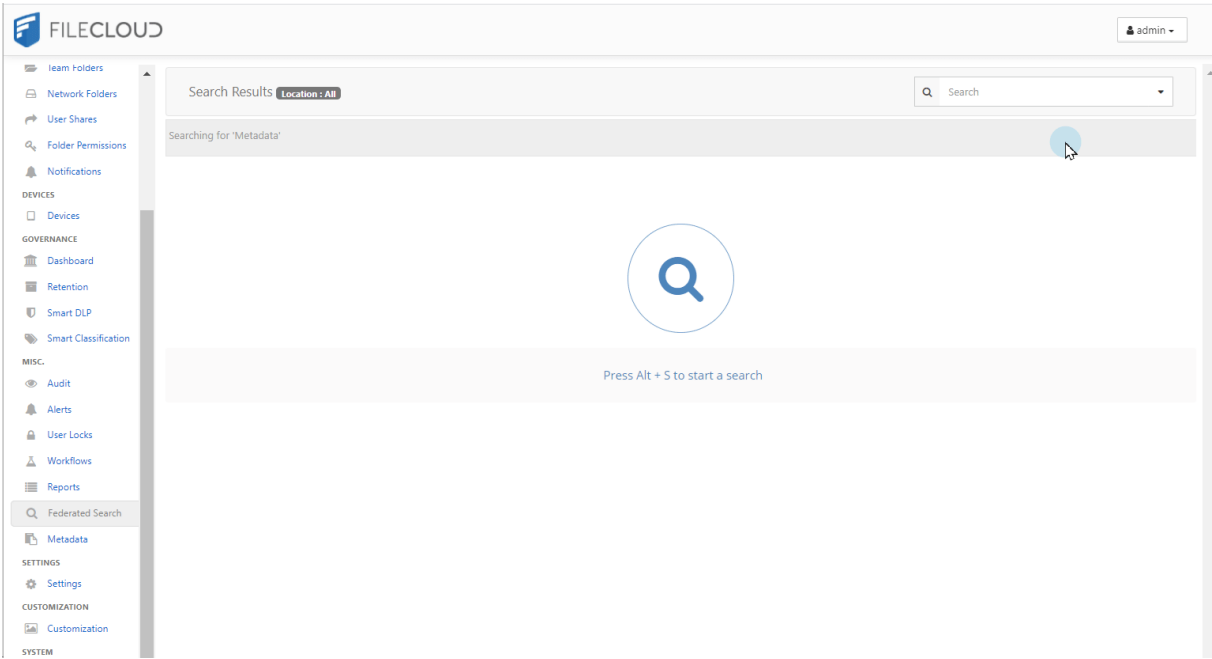
An advanced search lets you search on the search term and any of the options shown and listed below:

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

All search

All search

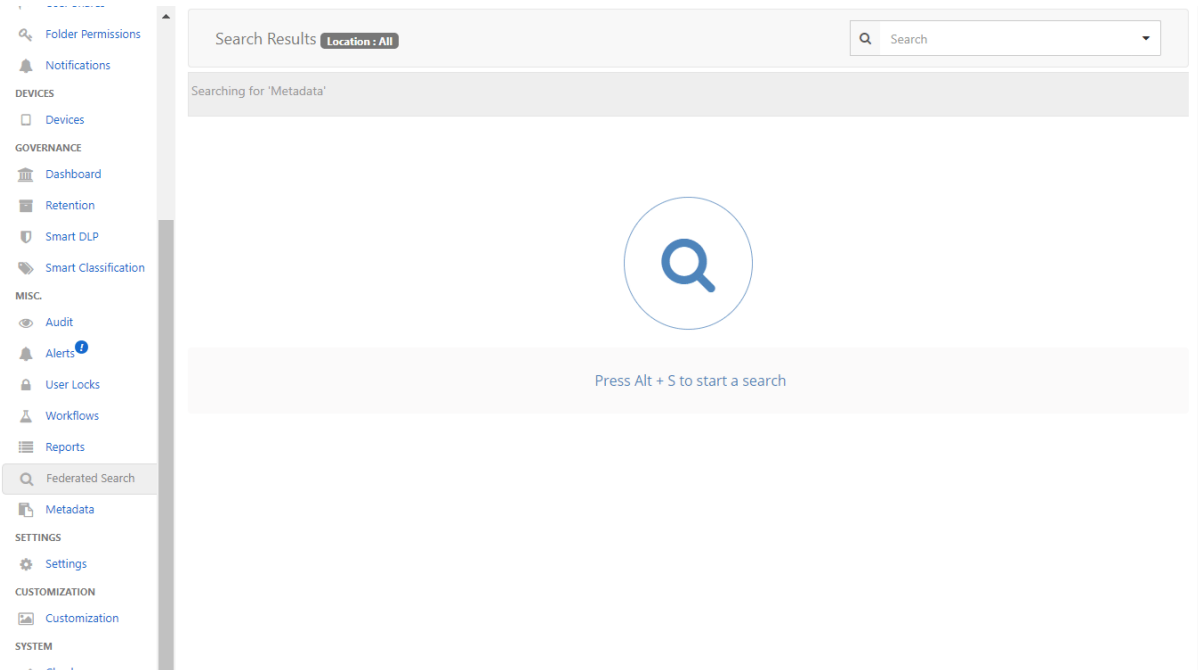
All is selected by default. This search looks for matches in file and folder names when content search is not enabled. It looks for matches in file and folder names and in the content of files when content search is enabled.



Name only search

Name Only search

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



Content only search

Content Only search

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

To perform a content search, your system must have full content search enabled.



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.

Search Results

Search



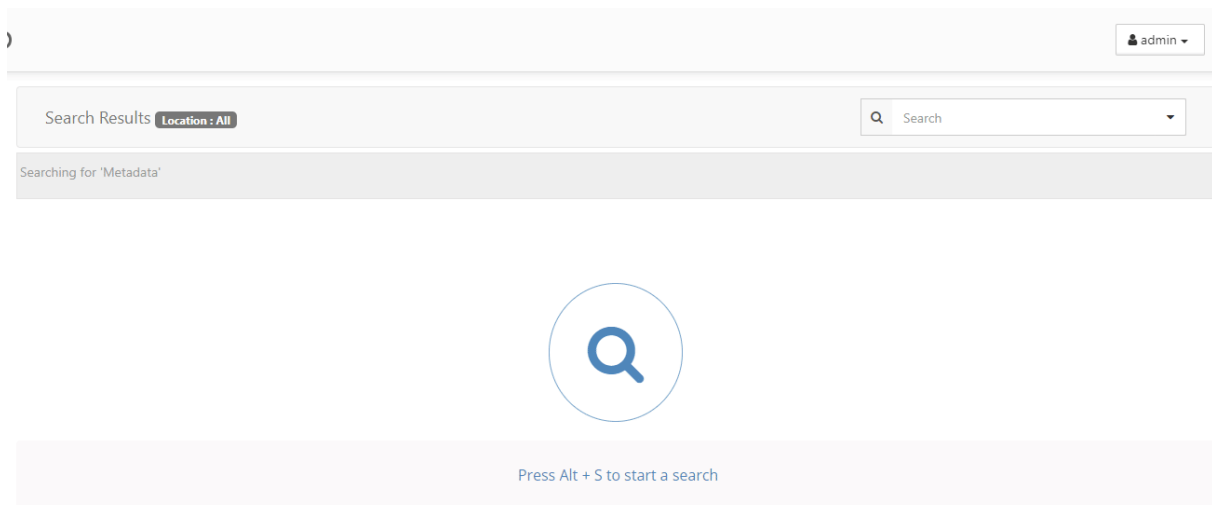
Press Alt + S to start a search

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.



Search Results Location : All

Searching for 'Metadata'

Press Alt + S to start a search

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.

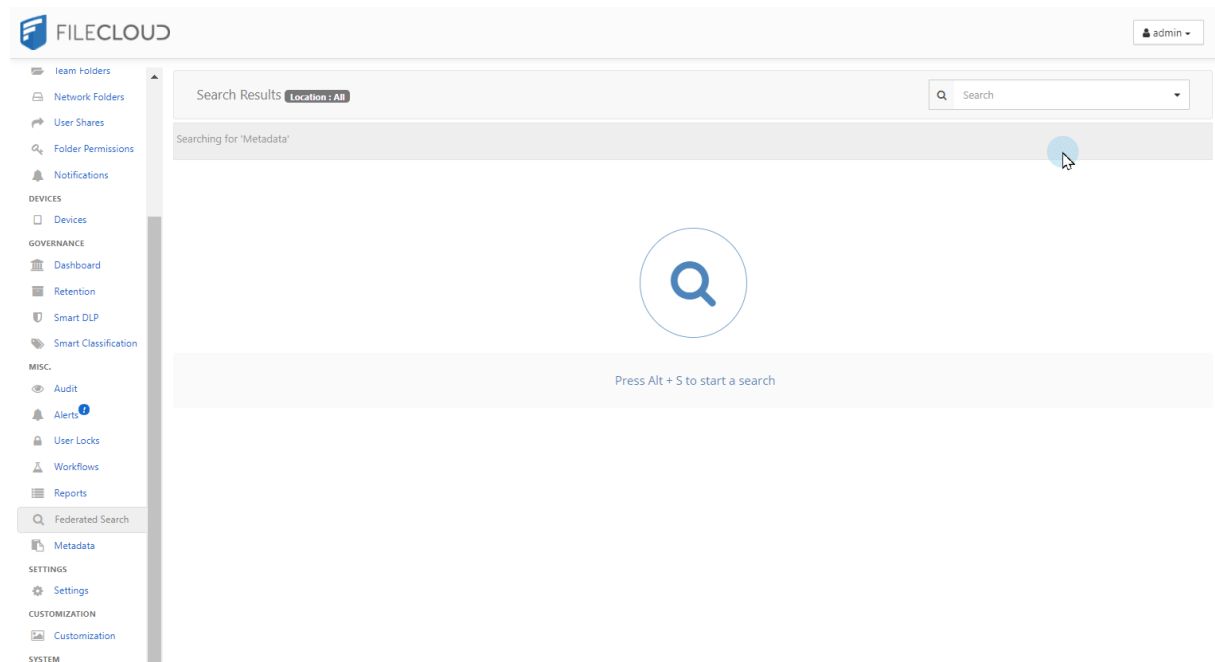
- **PII search** - The PII search is faster and more efficient than the PCRE search, and it displays the content it matches; however, it cannot match text that includes spaces or special characters. Therefore, you must use a PCRE search to find defined PII patterns that include spaces or special characters (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 **Content Search** settings page (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.

Advanced Search

✕

Term

?

Scope

☐ All
☐ Name Only
☐ Content Only
☐ Metadata
☐ PII
☒ PCRE

Search Type

☒ All files/folders
☐ Files Only
☐ Folders Only

Path Selection

☒ All
☐ Selected

Selected Path

File Type

Date

Results Count

☒ Limit 50
☐ All

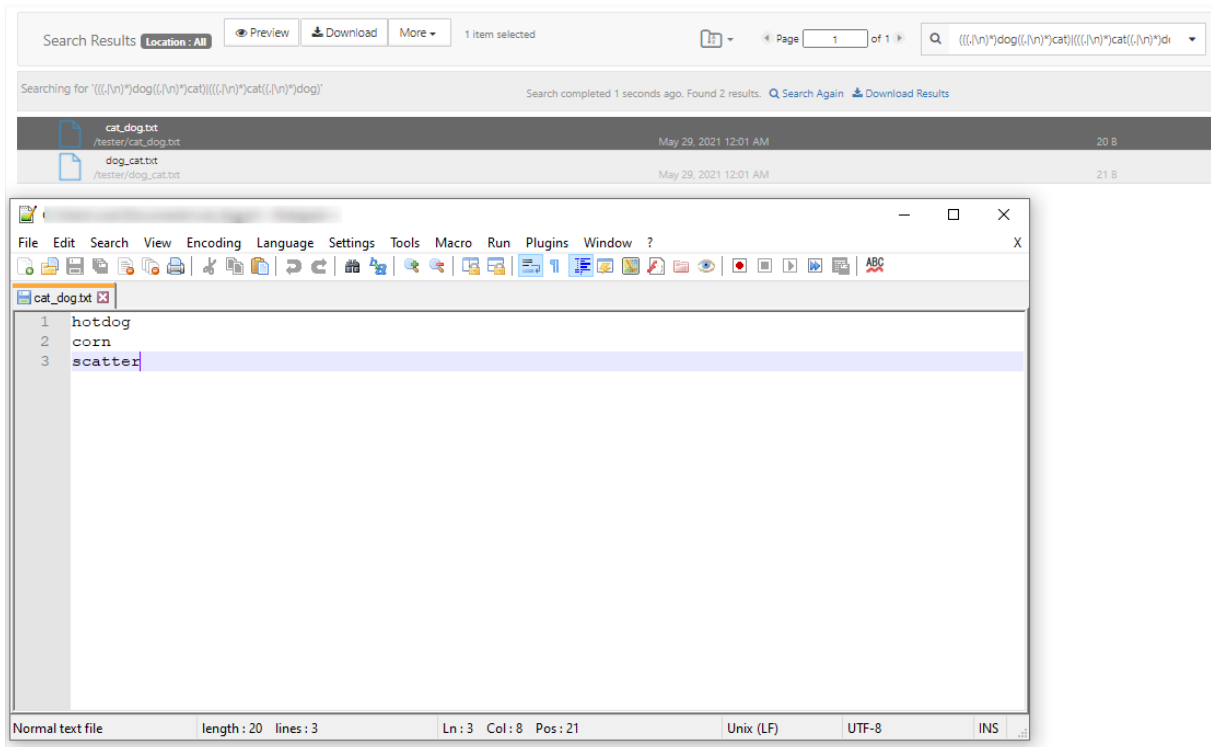
Use Cache Results

☐

Clear

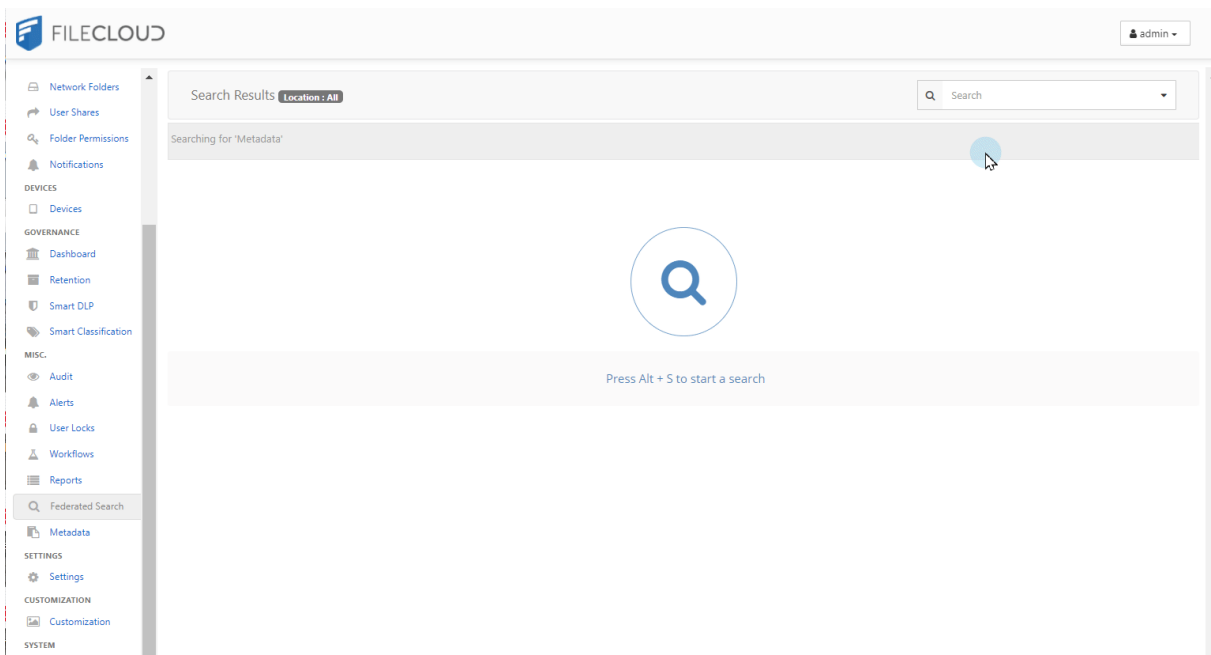
Search

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?

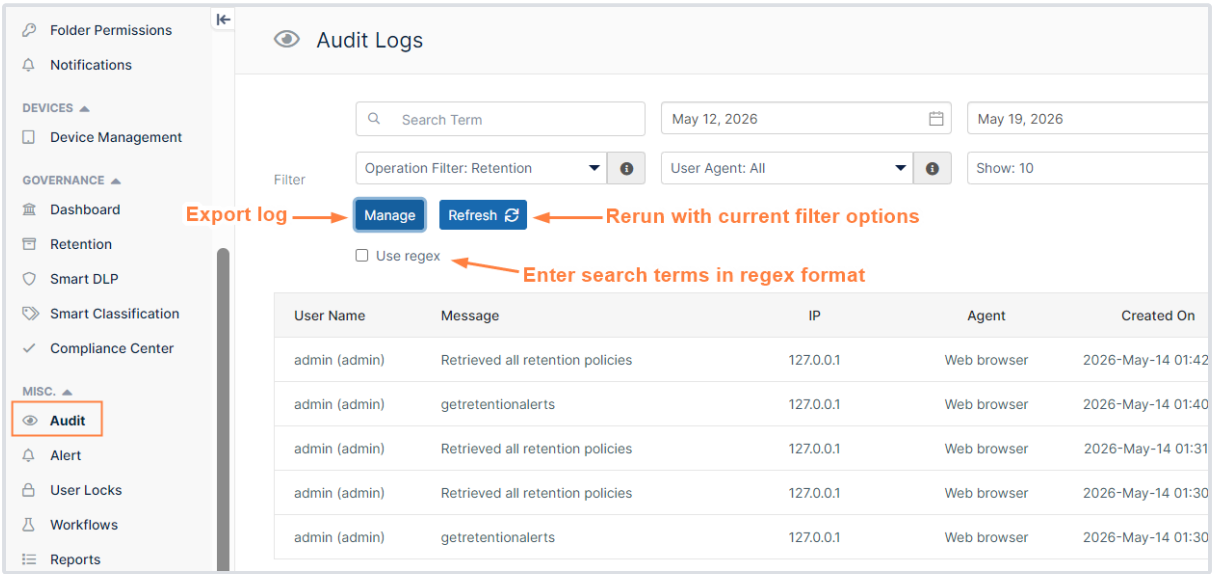
View Logs	View Audit Logs Filter Audit Log Views
Manage Logs	Delete Audit Log Entries Configure What is Logged Export Audit Logs Compact the Audit Database

View Audit Logs

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

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

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



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

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

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

Filter Audit Log Views

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

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



Filtering your view of log entries does not trim or decrease the size of your log database.

If your log database is growing too large, you can:

[Export Audit Logs](#)

[Configure What is Logged](#)

[Delete Audit Log Entries](#)[Compact the Audit Database](#)

How do you want to filter the Audit log?



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

By a search term

To filter the audit log by searching:

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

By a regular expression search term

 **Audit Logs**

May 12, 2026

Operation Filter: All
User Agent: All

Filter

Manage
Refresh

☒ Use regex

Regex searches scan more data. Use a date range to limit results.

User Name	Message
jennifer	Successfully retrieved Signing Requests
jennifer	Successfully created Editor URL for Signing Request with id:

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

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

By start and end dates

 Filter Start Date

 Filter End Date

To filter the audit log by date:

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

By an operation

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

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

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

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 an action or group of actions.

By an agent

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

You can select from the following user agents:

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

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 a client or device.

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 that you do not want logged because they fill your audit log with unnecessary information.

To configure what is logged:

Set a logging level

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

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

To set a log level:

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

Recent access update frequency
Frequency with which GeoIP data is retrieved and updated in hours

24

Audit log level
Audit log detail level

Request ▼

Off

Request

Full

Auto archive audit database
Automatically export and delete audit records.
NOTE: Cron Job must be set up and running

Auto archive audit records frequency (in days)
Export and delete audit records that are older than (#days)
(Auto archiving cannot run without this setting)

7

3. Click **Save**.

Specify operations that 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
<code>define("TONIDOCLOUD_AUDIT_IGNORE_OPS", "");</code>	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 logginguest", both these operations would not be added to the audit log.	<code>define("TONIDOCLOUD_AUDIT_IGNORE_OPS", "deletefile logginguest createfolder");</code>
<code>define("TONIDOCLOUD_AUDIT_IGNORE_AGENT", "");</code>	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.	<code>define("TONIDOCLOUD_AUDIT_IGNORE_AGENT", "Cloud Sync Mozilla/5.0 (Windows NT 6.3; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0 FileCloudDrive");</code>

⚠ 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|logginguest|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.

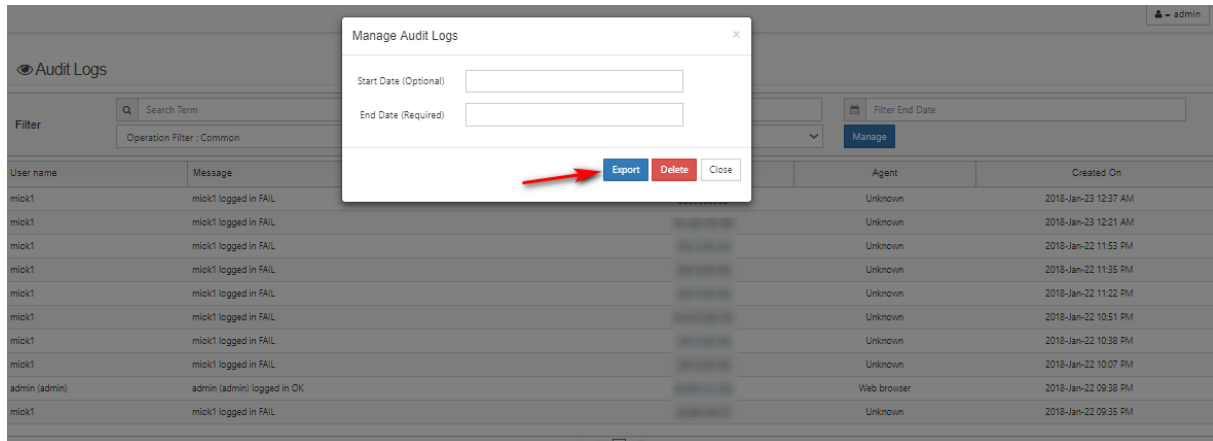
Export Audit Logs

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 Date** and **End Date**, select dates or type in dates in the format YYYY-MM-DD.
5. Click **Export**.



Delete Audit Log Entries



Admin Audit Log Deletion

Admins can prohibit other admins from deleting audit logs.

If you need to you can remove entries from the log file manually or 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. In the FileCloud admin portal's left navigation bar, scroll down and click **Misc > Audit**.
2. On the **Audit Logs** window, click **Manage**.

Manage Audit Logs
×

Start Date (Optional)

End Date (Required)

Export

Delete

Close

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

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. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin** . The **Admin** settings page opens.
2. Scroll down and locate the audit settings.

Audit log level

Audit log detail level

Request ▼

Auto archive audit database

Automatically export and delete audit records.

NOTE: Cron Job must be set up and running

**Auto archive audit records frequency (in days)**

Export and delete audit records that are older than (#days)

(Auto archiving cannot run without this setting)

7

Note: Files are exported daily and stored in CSV format; exported records are deleted from audit database.**Storage path for archived audit records**

Check path

C:\archives

Check Path

Storage location of exported audit files. This location must be writable by the webserver

3. Fill in the audit settings as indicated in the following table:

Setting	Description
Audit log level	To create an audit log, set to Request or Full .
Auto archive audit database	Enable this setting. Note: Cron Job must be set up and running.
Auto archive audit records frequency (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	Path of folder that stores the exported audit records in CSV format. For example, C:\archives



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.
<code>--port <port></code>	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 <code>27017</code> .	<code>--port 27017</code>

Option	Description	Example 💡 Always replace the sample values in the examples with the values used in your deployment.
<code>--username <username>, -u <username></code>	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.	<code>-u "myUserAdmin"</code>
<code>--password <password>, -p <password></code>	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 mongo to prompt for a password, enter the <code>--password</code> option as the last option and leave out the argument.	<code>-p "abc123"</code>
<code>--authenticationDatabase <dbname></code>	Specifies the database in which the user is created. See Authentication Database . If you do not specify a value for <code>--authenticationDatabase</code> , mongo uses the database specified in the connection string.	<code>--authenticationDatabase "admin"</code>

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>

Option	Description	Example
<code>--collection</code> <code><collection>, -c</code> <code><collection></code>	Specifies the collection to export.	<code>--collection audit</code>
<code>--type <string></code>	<i>Default:</i> json New in version 3.0. Specifies the file type to export. Specify <code>csv</code> for CSV format or <code>json</code> for JSON format. 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.	<code>--type=csv</code>
<code>--fields</code> <code><field1[,field2]>, -f</code> <code><field1[,field2]></code>	Specifies a field or fields to <i>include</i> in the export. Use a comma separated list of fields to specify multiple fields. If any of your field names include white space, use quotation marks to enclose the field list. For example, to export two fields, <code>phone</code> and <code>user number</code> , you would specify <code>--fields "phone,user number"</code> . 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.	<code>--fields</code> <code>createdon,username,</code> <code>how,ip,useragent,op</code> <code>eration,request,dev</code> <code>iceinfo</code>
<code>--out <file>, -o</code> <code><file></code>	The output directory where you need to export data as a csv. You must change this location to match the directory in your deployment.	<code>--out c:</code> <code>\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 `mongorestore` 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:

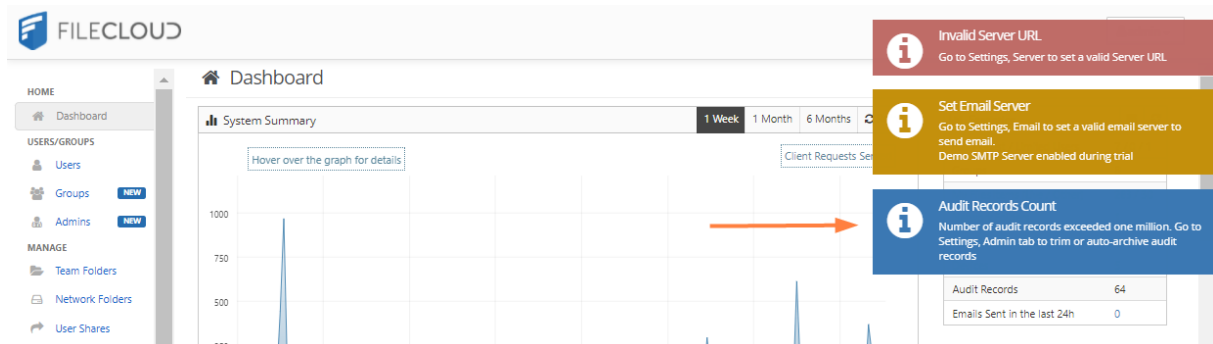
```

Administrator: Command Prompt - mongo.exe
c:\xampp\mongodb\bin>
c:\xampp\mongodb\bin>
c:\xampp\mongodb\bin>mongo.exe
MongoDB shell version v3.4.3-88-gbe3d66e
connecting to: mongodb://127.0.0.1:27017
MongoDB server version: 3.4.3-88-gbe3d66e
Server has startup warnings:
2018-08-15T18:58:48.528-0700 I CONTROL [initandlisten]
2018-08-15T18:58:48.528-0700 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2018-08-15T18:58:48.528-0700 I CONTROL [initandlisten] **           Read and write access to data and configuration is unrestricted.
2018-08-15T18:58:48.528-0700 I CONTROL [initandlisten]
> show dbs;
admin                0.000GB
local                0.000GB
tonidoauditdb        0.000GB
tonidoclouddb        0.001GB
tonidosettingsdb     0.000GB
tonidostoredb        0.001GB
tonidoanonymdb       0.000GB
> use tonidoauditdb
switched to db tonidoauditdb
> show collections
audit
geoup
notificationstream
report_result
search_result
searchterms
shareactivity
> db.audit.drop()
true
> show collections
geoup
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

[Back up and Restore Linux Deployments](#)

[Manually Back up 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



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

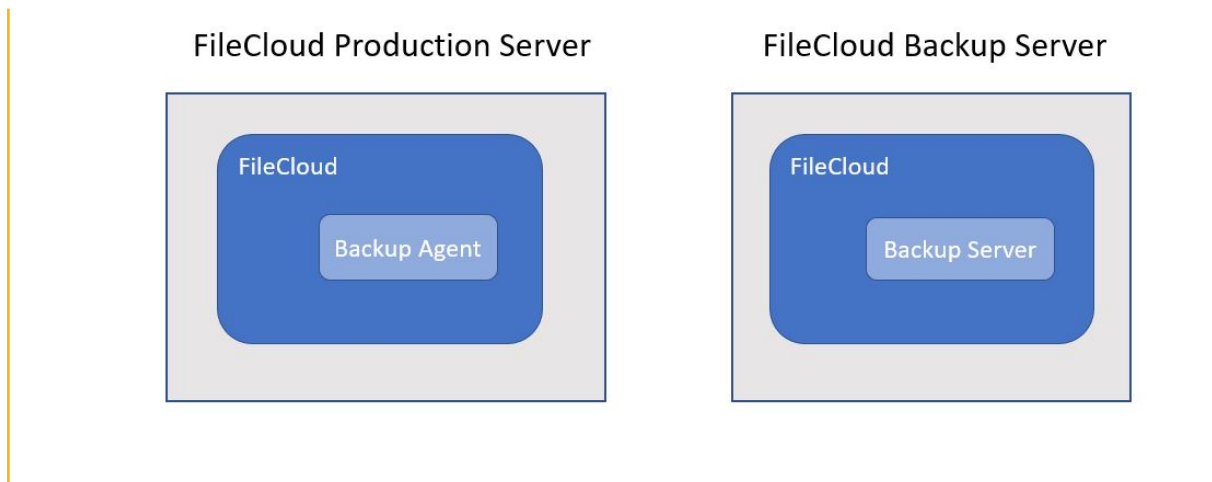
Follow these steps to install FileCloud backup server.



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

The backup server is bundled as part of the main installer.

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);
```

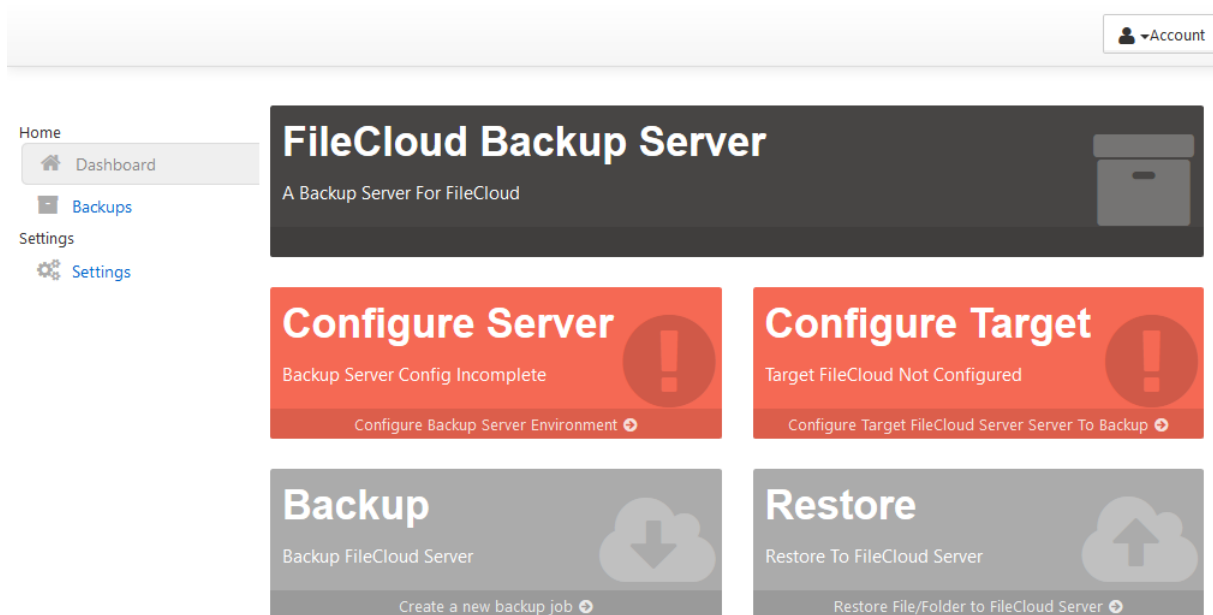
3. Repeat steps 1 and 2 in your backup server's FileCloud directory.

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

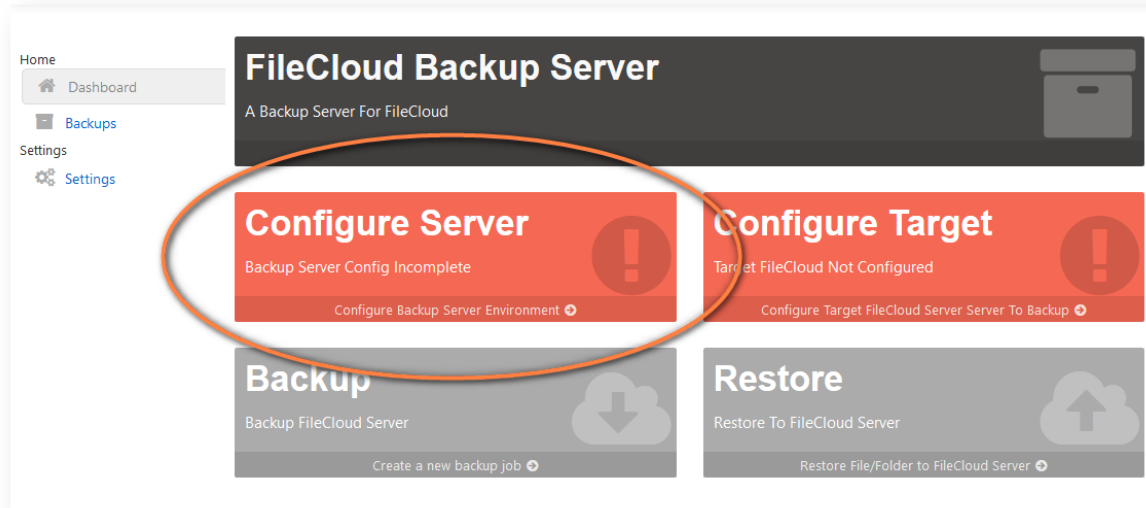
Introduction

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.

Home

Dashboard

Backups

Settings

Settings

Target Server

Backup Server

Backup Server Settings

Mongodump Path

Specify the path to mongodump binary.

Mongorestore Path

Specify the path to mongorestore binary.

PHP Path

Specify the path to php binary.

Invalid Settings... Please Check!

Save Reset

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 displays the 'Backup Server Settings' page in the FileCloud interface. The sidebar on the left contains links for 'Home', 'Dashboard', 'Backups', and 'Settings'. The 'Settings' section is expanded, showing the 'Backup Server' tab. 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'. Each field has a descriptive label below it: 'Specify the path to mongodump binary.', 'Specify the path to mongorestore binary.', and 'Specify the path to php binary.' respectively. A green success message 'Changes Saved Successfully!' is displayed at the bottom of the settings area. At the very bottom, there are 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" );

?>
```

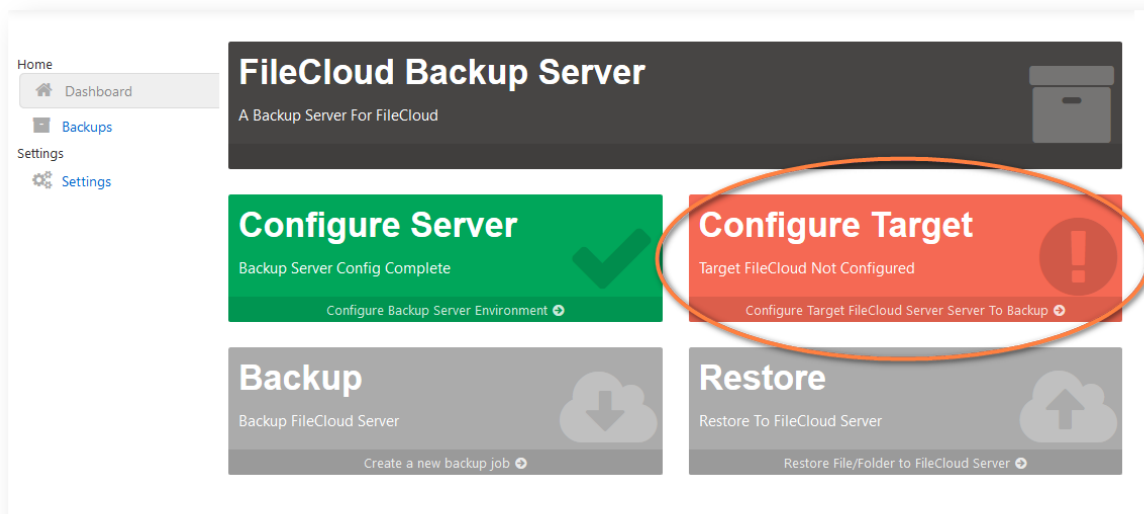
4. **Optional:** If your installation is not the default location, then you can specify the installation paths using the following keys in backupagentconfig.php

```
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.

Target FileCloud Server Settings

FileCloud Server Targets

Page 1 of 1
4 rows

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

Update Backup Target Server ×

Target Name

Specify a name to denote FileCloud server to backup.

Target URL

Specify the URL of FileCloud server to backup.

Storage Directory

 ✓

Specify directory under which the backups will be stored

Backup API Key

Specify the backup API key that should be used to connect to the FileCloud server

Backup connection

 ▼

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:

Home
Dashboard
Backups
Settings
Settings

FileCloud Backup Server

A Backup Server For FileCloud



Configure Server

Backup Server Config Complete



Configure Backup Server Environment

Configure Target

Target FileCloud Configured



Configure Target FileCloud Server Server To Backup

Backup

Backup FileCloud Server



Create a new backup job

Restore

Restore To FileCloud Server



Restore File/Folder to FileCloud Server

Step 4: Adding Multiple Target FileCloud Servers

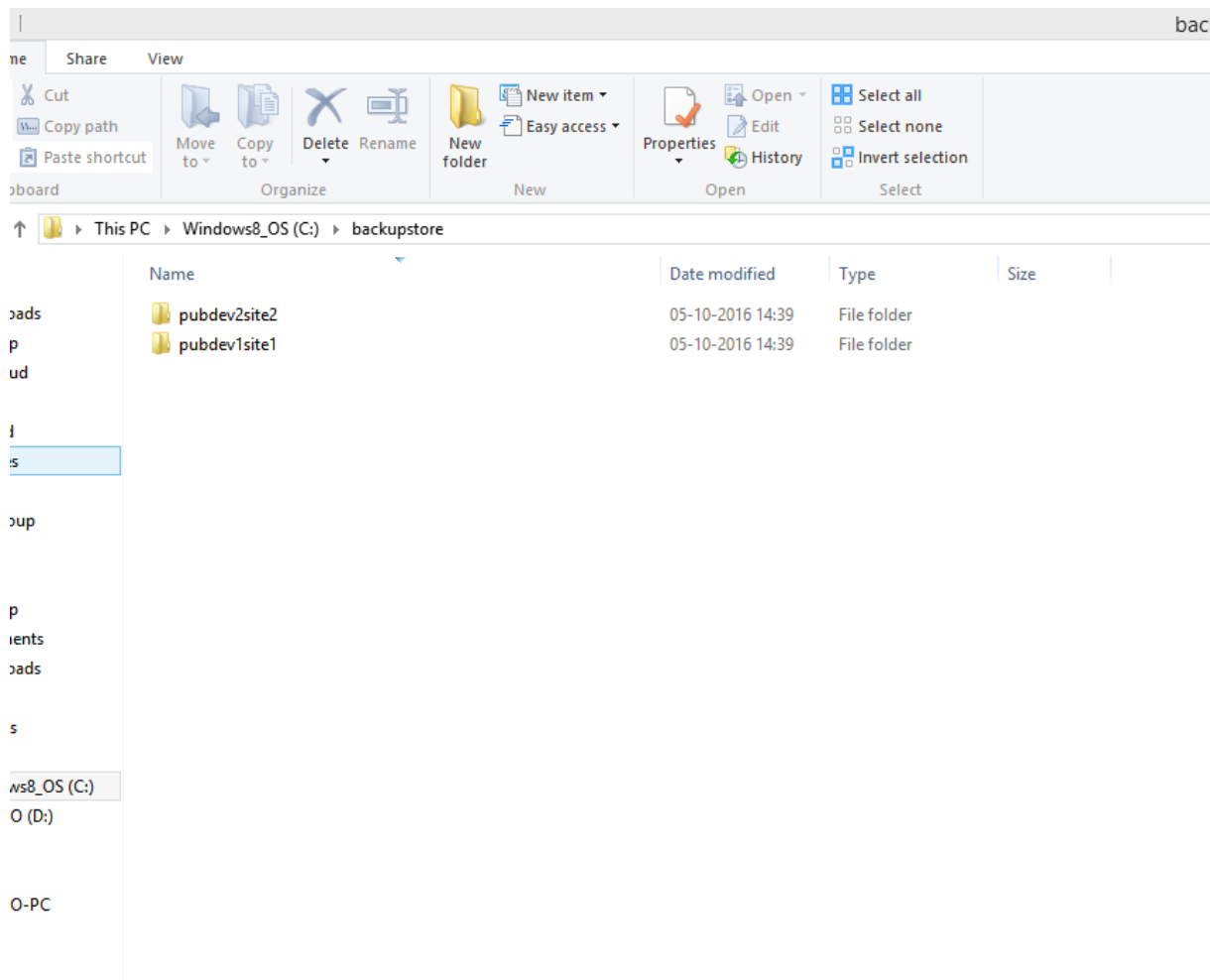
Adding multiple target servers is same as adding a single server. From the 'Settings' tab, click on 'Add' button, to bring up the target server dialog. Enter all the information there and click 'Add' button. Following screenshot shows multiple target servers added to the backup server.

The screenshot displays the 'Target FileCloud Server Settings' interface. At the top, there are two tabs: 'Target Server' (selected) and 'Backup Server'. Below the tabs, the title 'Target FileCloud Server Settings' is shown. The main area is titled 'FileCloud Server Targets' and contains a table with four rows of target servers. To the right of the table, there are two buttons: 'Add' (blue) and 'Remove' (red). At the bottom, there is a pagination bar showing 'Page 1 of 1' and '4 rows'.

FileCloud Server Targets
pubdev1
pubdev1site1
pubdev2site2
scratch

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
4. 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:

```

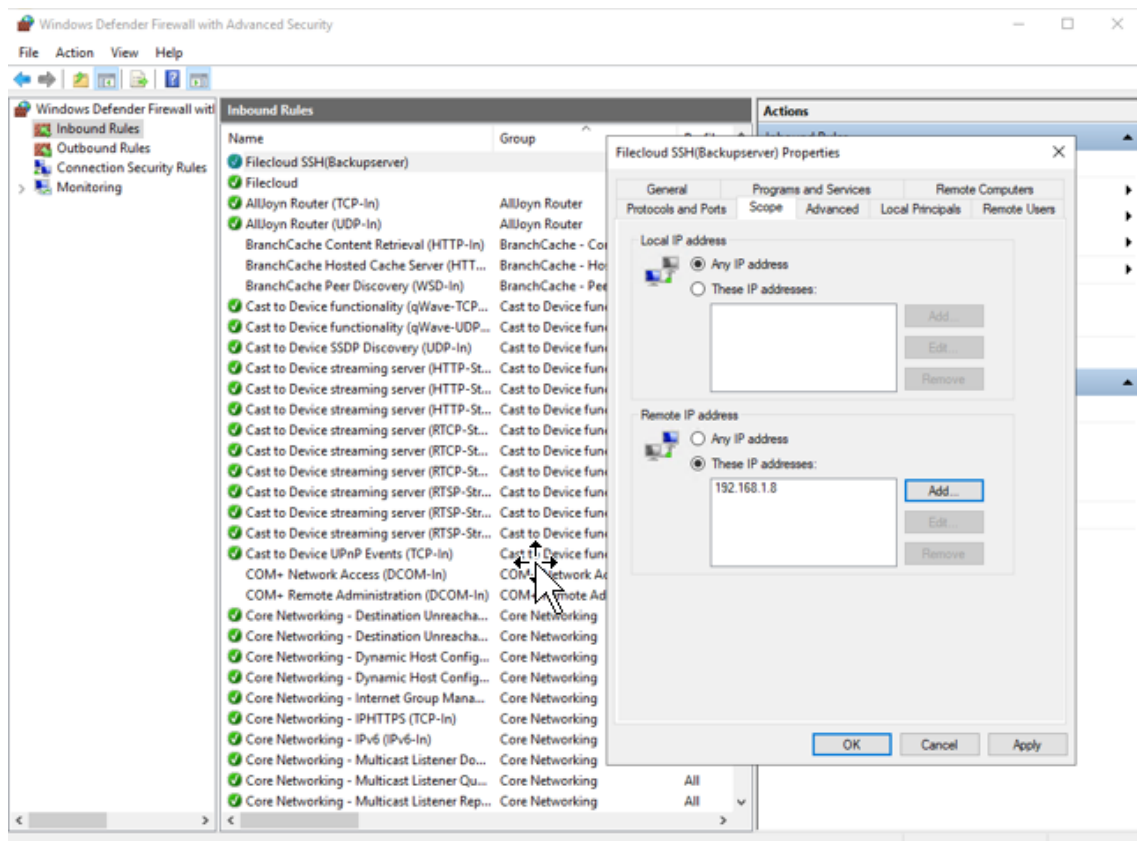
Administrator: Windows PowerShell
PS C:\xampp\tools> .\install_server.ps1
[SC] SetServiceObjectSecurity SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
Rsync and sshd-agent services successfully installed
Configured Environment variables
WARNING: Waiting for service 'OpenSSH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

Directory: C:\ProgramData\ssh

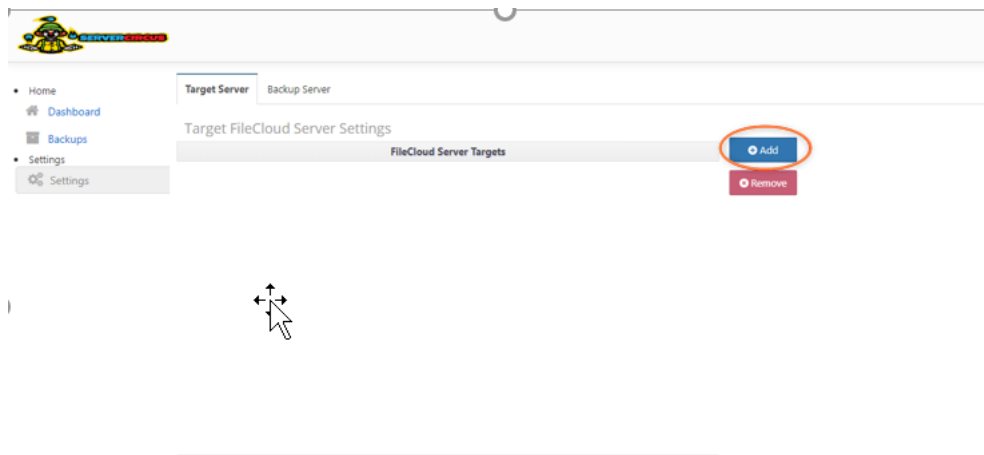
Mode                LastWriteTime         Length Name
----                -
-a-----      10/23/2020  10:55 AM              0 authorized_keys
SSH and SSH AGENT services started
PS C:\xampp\tools>

```

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



6. Copy the PUB key from the backup server at:
xampp\tools\cwrsync\bin\fcbackups.pub
 to:
C:\ProgramData\ssh\authorized_keys
7. On the production server, restart SSH services.
8. 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:

New Backup Target Server ×

Target Name
Specify a name to denote FileCloud server to backup.

Target URL
Specify the URL of FileCloud server to backup.

Storage Directory ✓
Specify directory under which the backups will be stored

Backup API Key
Specify the backup API key that should be used to connect to the FileCloud server

Backup connection

HTTP

HTTP

RSYNC

Add
Cancel

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

fcwin03

Specify a name to denote FileCloud server to backup.

Target URL

https://fcwin03

Specify the URL of FileCloud server to backup.

Storage Directory

E:\Backups

Specify directory under which the backups will be stored

Backup API Key

.....

Specify the backup API key that should be used to connect to the FileCloud server

Backup connection

RSYNC

Specify the connection to use for file downloads

SSH User

Administrator

Specify SSH user for RSYNC connection

SSH Port

2233

Specify SSH port for RSYNC connection

SSH Key

C:\xampp\tools\cwrsync\bin\fcbackups

Specify SSH private key for RSYNC connection

RSYNC Options

Specify additional options for RSYNC command

Add

Cancel

11. Click **Add**.

Run the backup for the target server

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

New Backup

×

Select backup target

fcwin03 ▼

Incremental Backup

☒ YES
☐ NO

Backup Schedule

☒ Starts Now
☐ Starts Later

Add

Cancel

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

Backup Progress

×

Status

In Progress

Progress

44%

Preparing database dump

Close

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

					fcwin03	Show 10 Items	New Backup	Refresh
	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	

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

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

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.

Home

Dashboard

Backups

Settings

Settings

			pubdev1	Show 10 Items	New Backup	Refresh
	Created Date	Start Date	End Date	Status	ACTIONS	
	28 Aug 2016 20:00	28 Aug 2016 20:00		INPROGRESS	Info	Status
	22 Jun 2016 02:32	22 Jun 2016 14:35	22 Jun 2016 14:38	COMPLETED	Info	Files
	19 May 2016 20:46	19 May 2016 20:46	19 May 2016 20:50	COMPLETED	Info	Files

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.
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.

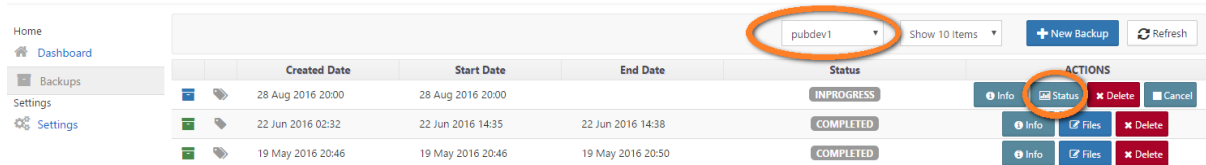


Note

- 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.

Backup on 22 Sep 2015 23:05

✕

Files				
Restore Queue		Export Queue		
				Restore
File	Uploaded	Size	Status	ACTIONS
 [blurred]	78%	20427336	In Progress	

Page 1 of 1
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

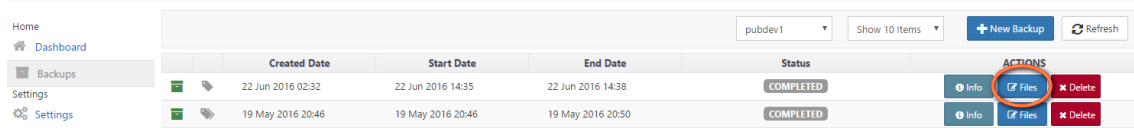
- Export from backup server UI supports files and folders.
- Main difference between export and restore is that export stores the file locally on the backup server, while restore stores file directly on the target FileCloud server.
- When export is selected, the current path will be chosen as path to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

Exporting File/Folder

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

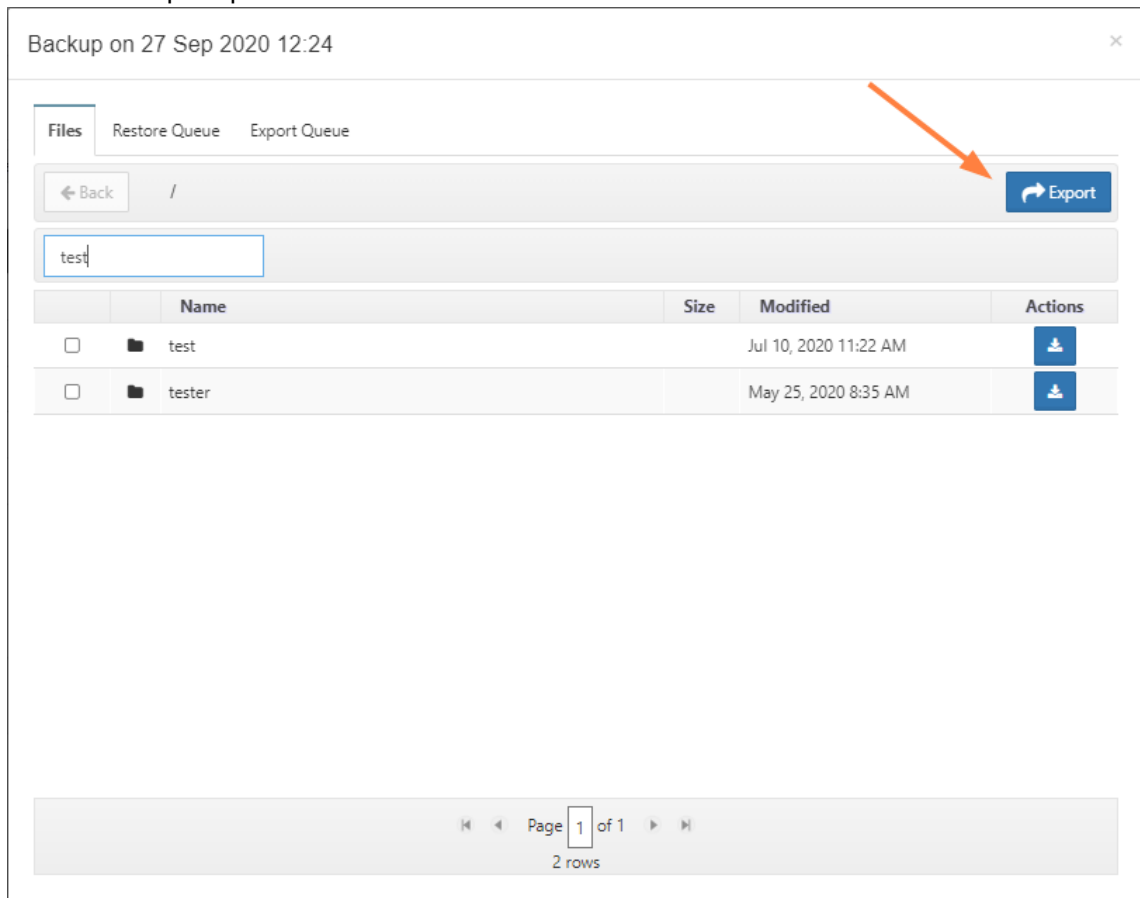
1. Select the backup from which the file/folder has to be exported.

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



	Created Date	Start Date	End Date	Status	Actions
	22 Jun 2016 02:32	22 Jun 2016 14:35	22 Jun 2016 14:38	COMPLETED	Info Files Delete
	19 May 2016 20:46	19 May 2016 20:46	19 May 2016 20:50	COMPLETED	Info Files Delete

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.



Backup on 27 Sep 2020 12:24

Files Restore Queue Export Queue

← Back /

test

	Name	Size	Modified	Actions
☐	test		Jul 10, 2020 11:22 AM	Download
☐	tester		May 25, 2020 8:35 AM	Download

Page 1 of 1
2 rows

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

Confirm



Add following folder to export queue?

/test

YES

NO

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

Export

Cancel

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	Start

⏪ ⏴ 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

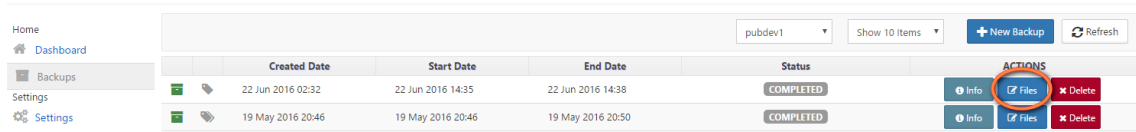
- Download of only one file or folder is supported at this time.

Downloading File/Folder

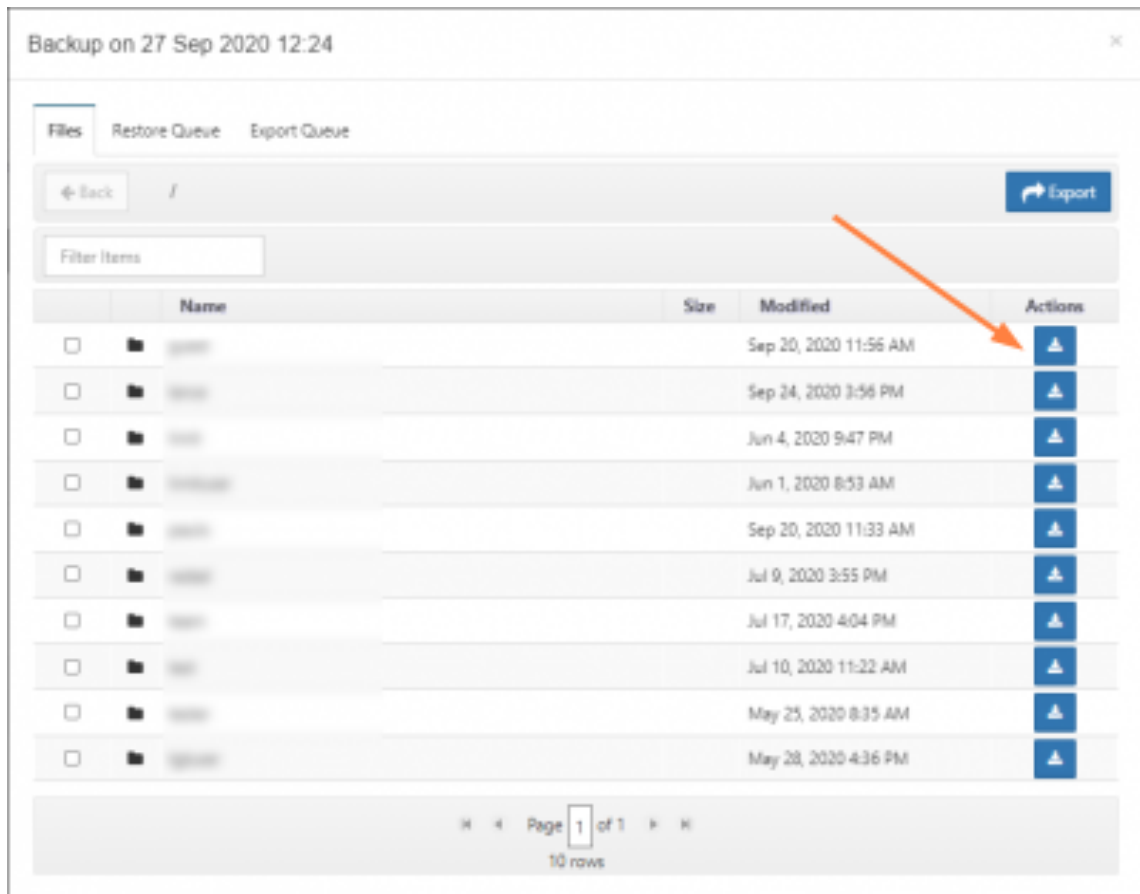
User file/folders can be downloaded using the following steps:

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

Create New Backup Job

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

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

Create And Start Backup Job

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

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

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

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

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, tonidocloud db, 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 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:

- FileCloud config files
- FileCloud database files
- [FileCloud user files](#)

Backup

High level steps to backup FileCloud in Linux:

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 -dprv /var/www/. /filecloudbackup/www
```

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

Backup database

Once the mongodb is stopped, backup the database files.

Backing up FileCloud database.

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

Check your mongodb 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 -dprv /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 Linux:

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 mongod. 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



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

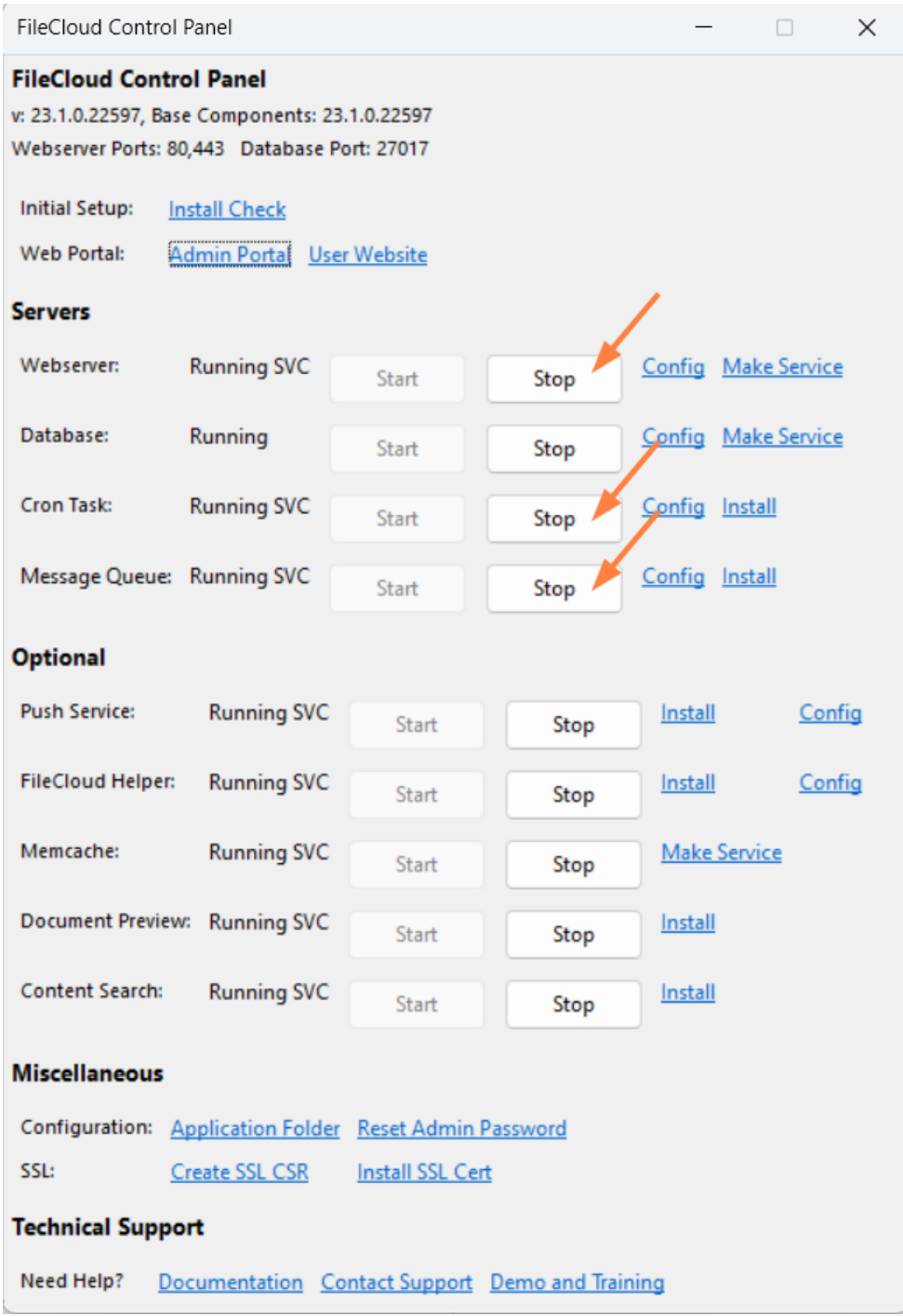
After the above restore steps are performed, start the apache webserver and mongod process.

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	Ubuntu: systemctl stop apache2 systemctl stop cron systemctl stop fcorchestrator RedHat: service stop httpd service stop crond service stop fcorchestrator

OS	
Windows	Use the FileCloud Control Panel to stop the above-mentioned services as indicated in the screenshot:  The screenshot shows the FileCloud Control Panel interface. At the top, it displays version information: 'v: 23.1.0.22597, Base Components: 23.1.0.22597' and port information: 'Webserver Ports: 80,443 Database Port: 27017'. Below this are links for 'Initial Setup' (Install Check), 'Web Portal' (Admin Portal, User Website), and a 'Servers' section. The 'Servers' section lists four services: Webserver, Database, Cron Task, and Message Queue, all with status 'Running SVC'. Each service has 'Start' and 'Stop' buttons. Three orange arrows point to the 'Stop' buttons for Webserver, Cron Task, and Message Queue. Below the 'Servers' section is an 'Optional' section with services like Push Service, FileCloud Helper, Memcache, Document Preview, and Content Search. At the bottom are 'Miscellaneous' links for configuration and SSL, and a 'Technical Support' section with links for help, documentation, 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. If the database has "TONIDO" in its name, 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

- 1.

- 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

1.

- 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:
 1.
 - 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.

[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



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:

```
TONIDOCLOUD_REPLY_TO_EMAIL
```

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

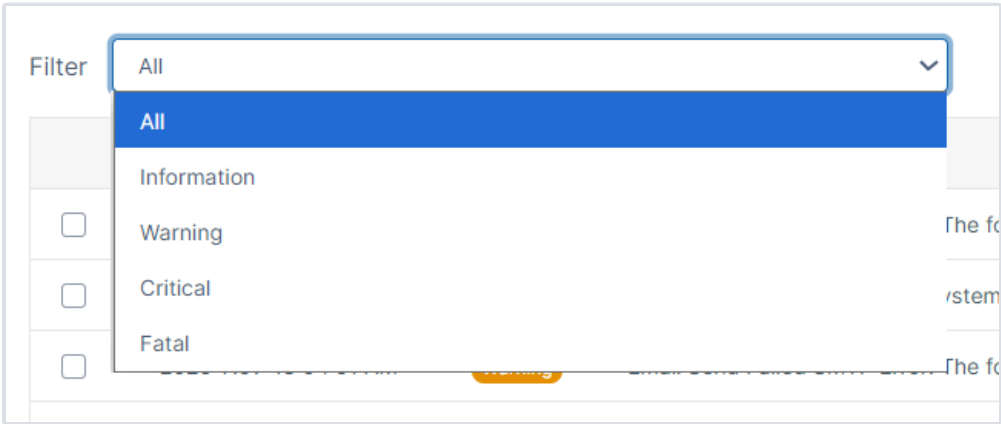
FileCloud Alerts

FileCloud Alerts are available in FileCloud's Admin portal.

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

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

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

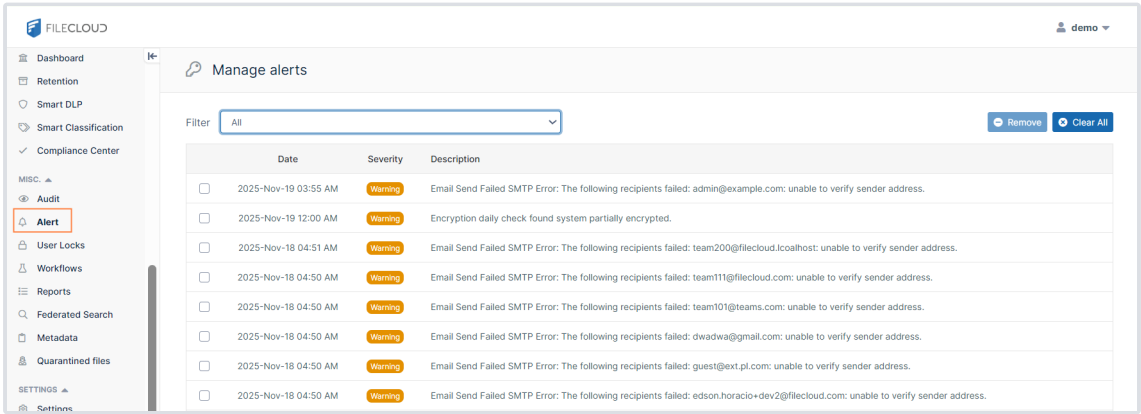


You can also remove individual or all alerts from the screen.

To view alerts:

- 1. Log into the Administration portal.
- 2. On the left navigation panel, click **Alerts**.

The Manage alerts page opens:



File Content Heuristic Engine

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

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

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

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

1. In the admin portal, in the navigation [panel](#), click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
The **Create New Workflow** dialog box opens.
3. To perform the check on every file that is uploaded for the first time, in the **IF Condition** drop-down list, choose **If a file is created**.

Note: To also apply the condition to files that are re-uploaded, add a verify file integrity action with the condition **If a file is updated**.

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

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

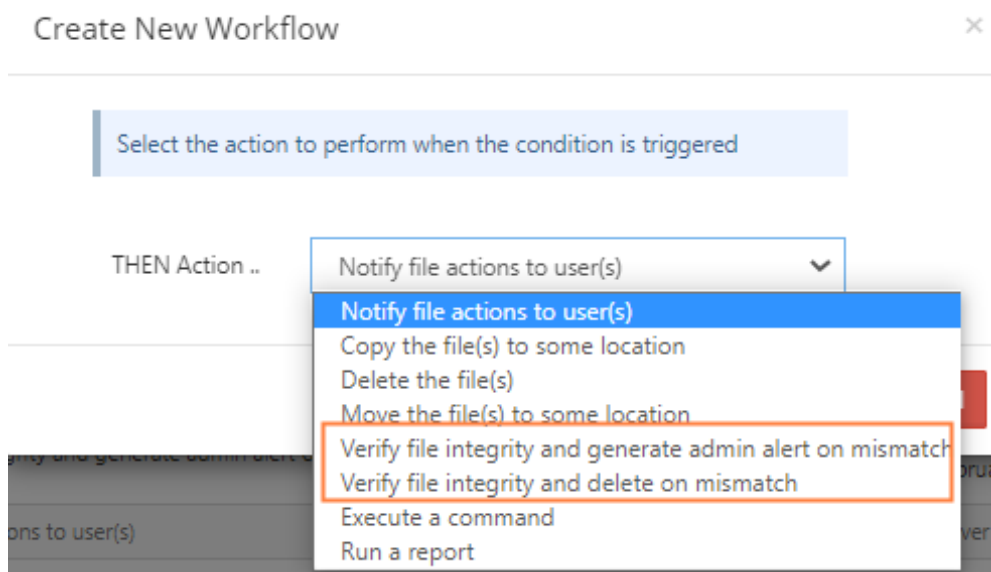
✕ Cancel

6. Click **Next**.

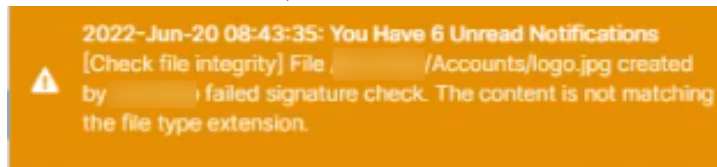
You are prompted to choose an action.

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:

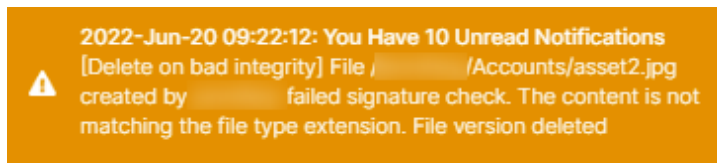
- **Verify file integrity and generate admin alert on mismatch:** Detects the mismatch and adds an entry to the **Alerts** screen of the admin portal. However, the file is uploaded into FileCloud, and if it is determined that it should be deleted, this must be done as a separate action.
- **Verify file 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"
}
```

10. Click **Next**.

11. Enter a name for the workflow.

Create New Workflow



Name for this action

Workflow Name

Check file integrity

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						
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						
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						

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



By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check. You may add additional allowable extensions for text files by adding the setting TONIDOLOUD_TEXT_FILE_EXTENSIONS to your cloudconfig file.

To change the default allowable text file extensions from txt, dat, log, and csv:

1. On the FileCloud Server, open the cloudconfig file:

In Windows:

C:\xampp\htdocs\config\cloudconfig.php

In Linux:

/var/www/html/config/cloudconfig.php

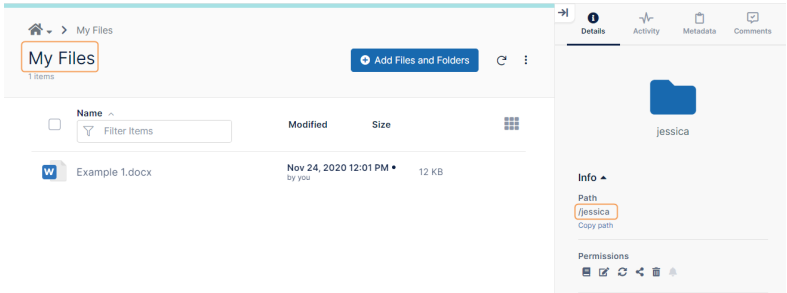
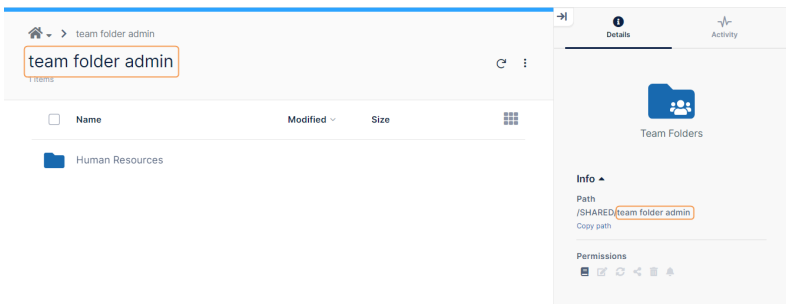
2. Include the following setting, and add additional extensions. You may also remove extensions. In the following example, the extensions pem, cfg, and cfg2 are added:

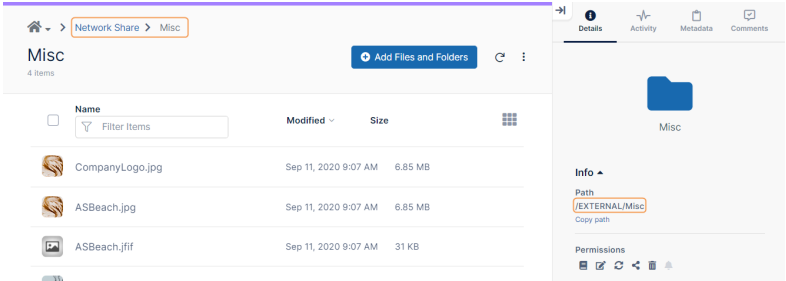
```
define('TONIDO_TEXT_FILE_EXTENSIONS', 'TXT|DAT|LOG|CSV|PEM|CFG|CFG2');
```


Identifying a FileCloud Specific Path

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

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

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

Netwo rk 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.  The screenshot shows the FileCloud web interface. On the left, the breadcrumb path is 'Network Share > Misc'. The main area displays a list of files: 'CompanyLogo.jpg' (6.85 MB), 'ASBeach.jpg' (6.85 MB), and 'ASBeach.jfif' (31 KB). On the right, the 'Details' tab is active, showing the folder icon and the path '/EXTERNAL/Misc' which is highlighted with an orange box. Below the path, there is a 'Copy path' link. The 'Permissions' section is also visible at the bottom of the details panel. <table><tr><td>Shared with Me</td><td>Can't be done. You must specify the path from the owner's My Files (use the owner's username)</td><td></td></tr></table>	Shared with Me	Can't be done. You must specify the path from the owner's My Files (use the owner's username)	
Shared with Me	Can't be done. You must specify the path from the owner's My Files (use the owner's username)				
Shared with Me	Can't be done. You must specify the path from the owner's My Files (use the owner's username)				

Custom Reports



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

FileCloud enables you to create custom reports and download them in an Excel format. To get started with the reporting system, go to the Reports menu item in the left navigation menu in admin interface.

In order to view the reports, the admin user must be the master admin or must have access to the reports system. An admin user can be granted access to the reports system through the Admins menu item on the left navigation menu.

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

Manage Reports

Report ALL + Add Report

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

Page 1 of 1
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

Get user shares report



→ 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		186	106862964	101.91 MB	2 GB	4.98	
mary higgins		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
Get client application grouped by OS	Report of total client devices that are connected to FileCloud grouped by client OS. Data Retrieved: client OS type(Windows, Android etc), total devices connected. Parameters: None

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

Report Name	Description
Get uploaded files report	Report on what files were uploaded during a given period, or files uploaded by a user or group of users during a particular period. Data Retrieved: Timestamp of upload, user name, user agent, IP address, file path, bytes of file uploaded Parameters: • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • username : (OPTIONAL) User account name - can be set only when <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	Report on what files were downloaded during a given period, or files downloaded by a user or group of users during a particular period. Data Retrieved: Timestamp of download, user name, user agent, IP address, file path, bytes of file downloaded Parameters: • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • folder_path : (OPTIONAL) Restrict report to files inside specified path. • username : (OPTIONAL) User account name - can be set only when <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)
Get files tagged with metadata report	Report listing files/folders and their value for a specified metadata field. Data Retrieved: path of folder or file, username, metadata field, value of metadata field Parameters: • metadata_name : (REQUIRED) Name of the metadata set • attribute_name : (REQUIRED) Name of the metadata attribute • attribute_value: (OPTIONAL) Metadata attribute value
Get shares report	Report listing shares created. Data Retrieved: Timestamp of download, user name, user agent, IP address, file path, password Parameters: • from_date : (OPTIONAL) From date in Y-M-d H:i:s • to_date : (OPTIONAL) To date in Y-M-d H:i:s • username : (OPTIONAL) User account name - can be set only when <i>from_date</i> and <i>to_date</i> are specified

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

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

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

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

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

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

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

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

Manage Folder Level Permissions

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

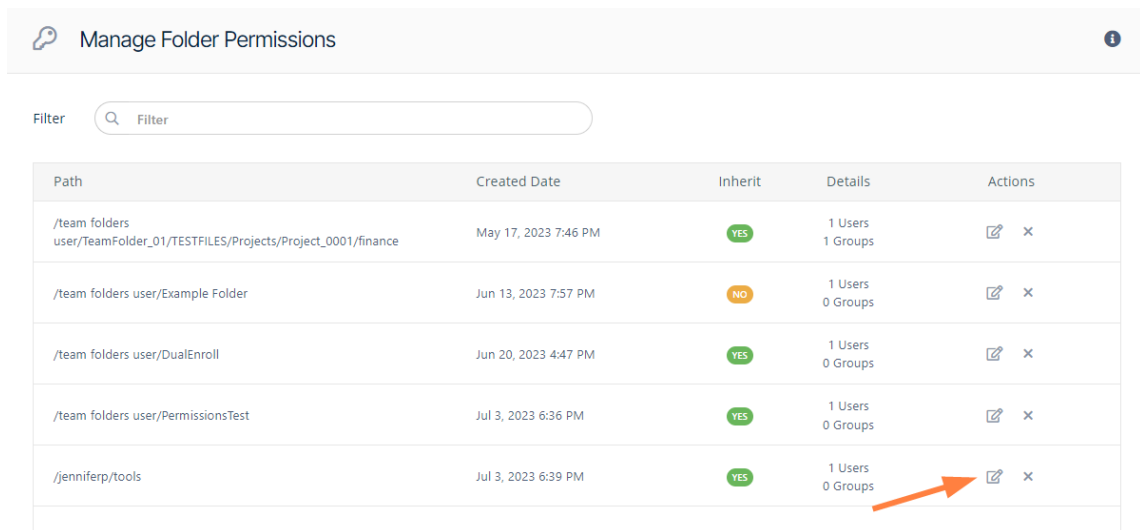
The screen displays the list of existing folder-level permissions set in the system. This includes folder-level permissions set on Team Folders in the admin portal and folder-level permissions set on user folders in the user portal.

Use the **Filter** box to filter folder permissions on the folder path. Individual permissions can then be viewed, edited and deleted.

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

To Edit Folder-Level Permissions

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



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

Manage Folder Level Security

Folder: /jennifer/Admin hold

Security

Check Access

Permissions

Inherit Parent Folder Security:

☒ Inherit
 ☐ Don't Inherit

User

Group

Add User

User	Read	Write	Delete	Share	Manage
dm898002@gmail.com	☒	☒	☒	☒	☒

Page 1 of 1

Inherited Permissions

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

Page 1 of 1

Close

A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.

B Click **Add User** to add a user and limit their access to the folder, or click the **Group** tab and add a group.

C In the top list of users, check or uncheck levels of permissions.

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.

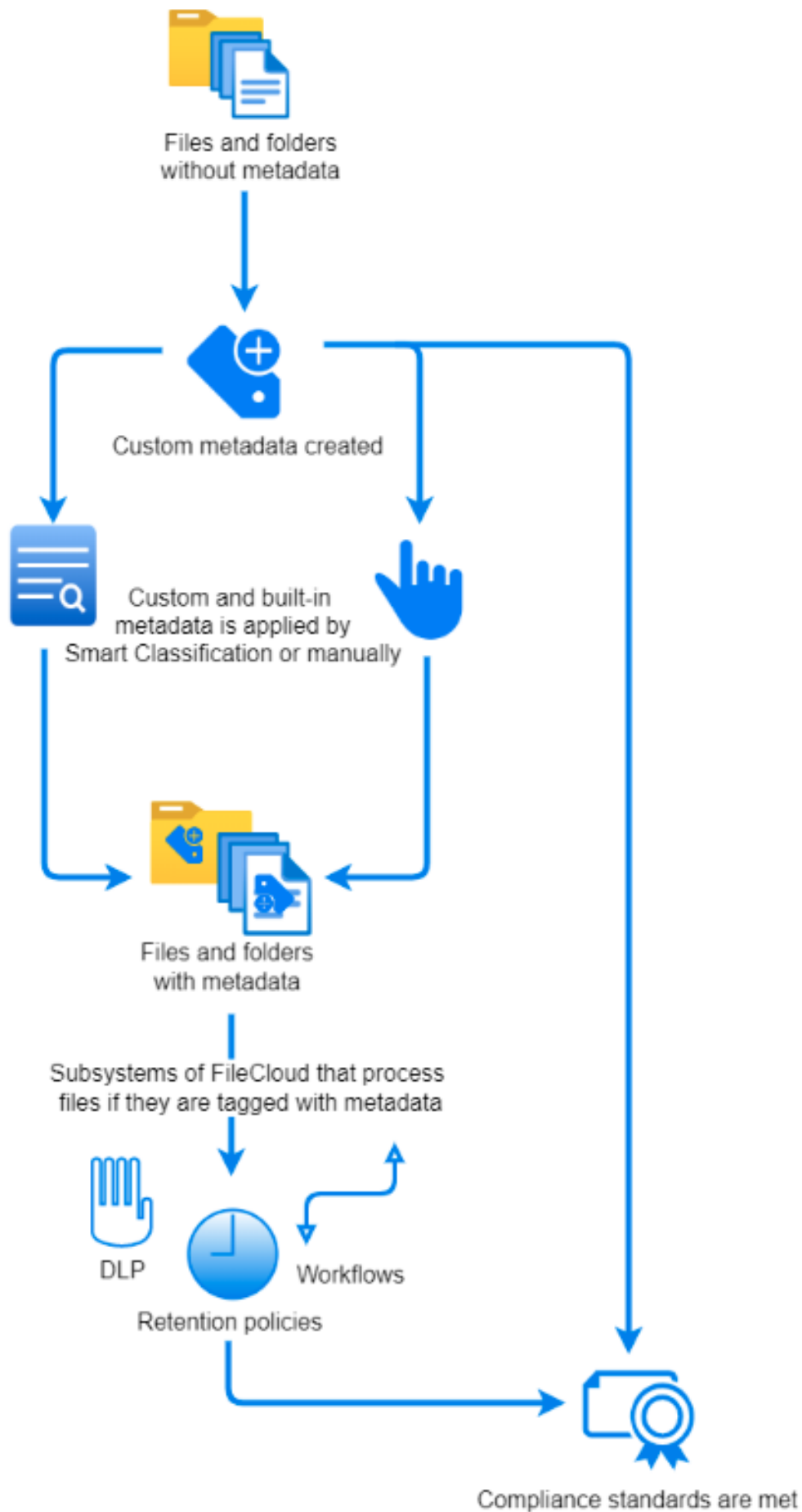
Metadata for governance and other system processes

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:

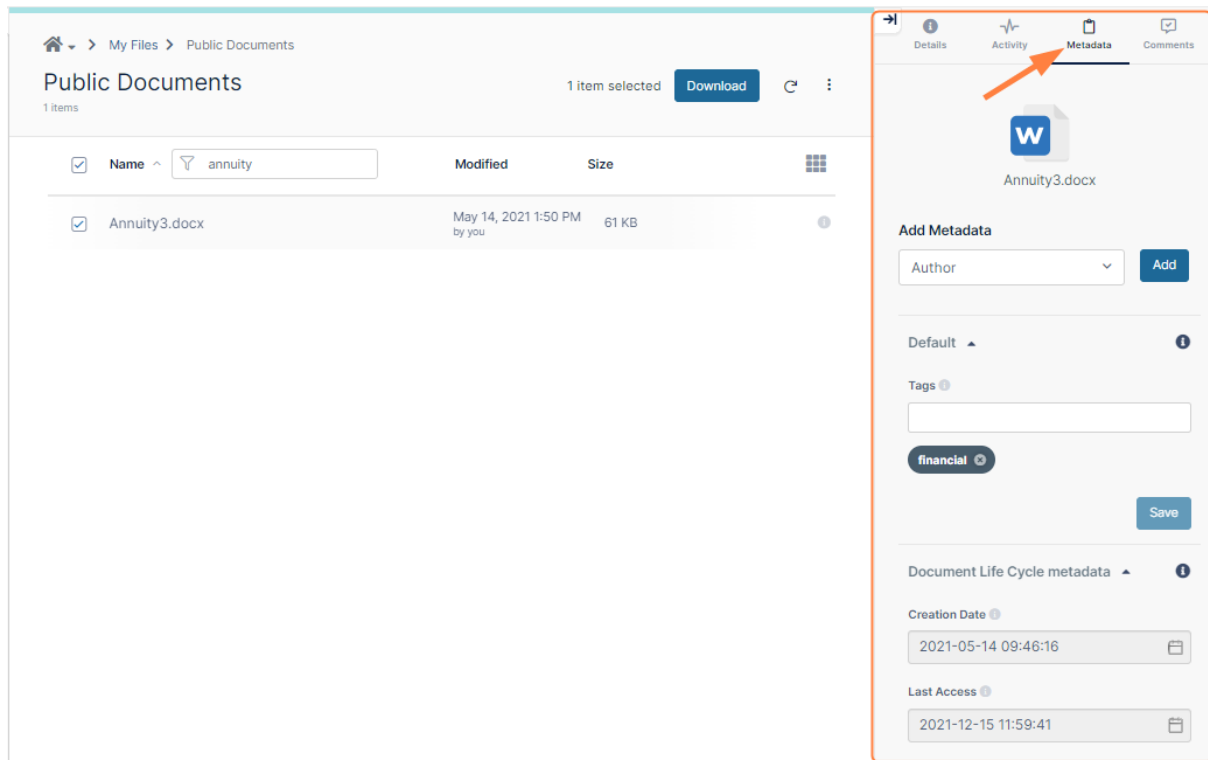
- The HIPAA section of the Compliance Center requires that your system include metadata that identifies PHI data.
- The ITAR section requires your system to use content classification to apply metadata tags to defense and technical articles, and then use DLP to block public sharing of the tagged articles.



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.



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

In this section

Metadata Components and Types

FileCloud defines two levels of metadata definition:

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

See a Description of Metadata Terms

Figure 1. Metadata Terms

 File Object	 Metadata	 Attribute	 Metadata Set	 Tag
Every file and folder that exists in FileCloud.	Information about the file data. Describes files and folders available in the system.	A single piece of information that describes the File Object. In FileCloud attributes are defined as a part of the metadata set.	A set of metadata attributes that might be logically grouped and can be attached as a single entity to File Objects.	a special type of attribute (referred to as the Array attribute type) that allows users to provide multiple custom values for each File Object.
For example: a resume	For example: - Lives in the Human Resources Folder - Has a created date - Has a modified date	For example: the candidate's photo in their resume	For example, resumes will always have: - Photo - Name - Address - Experience - Education	For example: HR wants to tag a resume status as: - Candidate - New Hire - OnBoarding

Metadata Set Types

FileCloud supports the following types of Metadata Sets:

TYPE	DESCRIPTION	SETS AVAILABLE
Default	This 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 / folder is accessed for the first time. - Exactly one Default Set exists in FileCloud - it cannot be deleted, renamed or disabled, but administrators can customize attributes and permissions. - Out of the box it is shipped with a single predefined attribute of Array type - Tags.	Default

TYPE	DESCRIPTION	SETS AVAILABLE
Built-In	These are metadata sets that have been created for you. - Administrators can edit the attributes - Administrators can choose to disable the use of this metadata	- Image metadata - Document Life Cycle metadata - Microsoft Office Tag metadata - Color Tag metadata - PDF Tag metadata - AIP Sensitivity Label metadata - CDR metadata (added in FileCloud 23.241.4) - Signority eSignature metadata (added in FileCloud 23.241.4) - ITAR metadata (added in FileCloud 23.252) - CUI metadata (added in FileCloud 23.252) - Extended metadata (added in FileCloud 23.262)
Custom 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 Blogs

- [How to Best Utilize FileCloud's Metadata](#)

Create a New Metadata Set

Add a new metadata set definition

To add new metadata:

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

The screenshot shows the FileCloud interface for managing metadata sets. The left sidebar contains a navigation menu with categories like DEVICES, GOVERNANCE, MISC, SETTINGS, and CUSTOMIZATION. The 'Metadata' option under MISC is highlighted. The main content area is titled 'Manage Metadata Sets' and includes a search filter, a 'Show 10 Items' dropdown, and a table of existing metadata sets. An orange arrow points to the 'Add Metadata Set' button in the top right corner of the main area.

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 X
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	Edit X
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	Edit X
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	Edit X
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	0	1	Edit X
AIP Sensitivity Label metadata	AIP Sensitivity Label metadata set	Enabled	Built-in	0	1	Edit X
CDR	Content Disarm and Reconstruction	Enabled	Built-in	0	1	Edit X
Signority eSignature	Signority eSignature metadata	Enabled	Built-in	0	1	Edit X
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	0	1	Edit X
ITAR Metadata	International Traffic in Arms Regulations metadata set	Enabled	Built-in	0	1	Edit X

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

Add Metadata Set Definition

Metadata Set

Name*

HR Metadata

Description*

Human Resources metadata

Disabled

☐

Permissions

Users

Groups

Paths

Add Group

Name	Read Permission	Write Permission
Human Resources	☒	☒

Page

1

of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	User's job title	Enabled	
Type	Text	Full time or part time job	Enabled	

Create

Close

- 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 [Managing Metadata Attributes](#).
- Click **Create**.

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

Edit Metadata Set Definition

Metadata Set

Name*

HR Metadata

Description*

Human Resources metadata

Disabled

☐

Permissions

Users
Groups
Paths

Add User

Name	Read Permission	Write Permission
jennifer	☒	☒
jessica	☒	☒

Page 1 of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	User's job title	Enabled	
Type	Text	Full time or part time job	Enabled	

Save
Close

Managing Metadata – 303

Edit an Existing Metadata Set



Propagating changes

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

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

⚠ Notes:

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

To edit an existing metadata set:

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

Manage Metadata Sets
Add Metadata Set

Filter
Show 10 Items

▼ Metadata Set Name	Description	Status	Set Type	User Count	Group Count	Actions
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	0	1	
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	
HR Metadata	Human Resources metadata	Enabled	Custom	0	2	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	

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

Edit Metadata Set Definition

Metadata Set

Name*

HR Metadata

Description*

Human Resources metadata

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name	Read Permission	Write Permission
jennifer	☒	☒
jessica	☒	☒

Page 1 of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	User's job title	Enabled	
Type	Text	Full time or part time job	Enabled	

Save

Close

4. Edit properties, [permissions](#) and [attributes](#).

5. Click **Save**.

Managing Metadata Attributes

Administrators can manage metadata tags in FileCloud.

Attribute Types

Each attribute can have one of the following types:

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

 Attribute type cannot change once the definition is saved.

How do I add or delete attributes?

You can use the following ways to manage attributes:

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

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

See a video on [Managing Attributes](#).

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

Video of Managing Metadata Attributes



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



Managing Metadata Permissions

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

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

What are effective permissions?

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

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

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

Table 1. Permissions Examples

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

How do I grant users permission to access Metadata?

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

To grant a user access to the Metadata field:

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

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

Watch a video on [granting users permission to access Metadata](#).

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

-  All paths have to have one of the following formats:

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

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

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

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



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

Watch a video on [creating allowed paths](#).

Video of Allowing Paths for Metadata Permissions

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

Add Metadata Set Definition

Metadata Set

Name*

Assets

Description*

Metadata set with media campaign information

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name	Read Permission	Write Permission

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	Actions
Type	Text	type of asset	Enabled	
Owner	Text	User who created asset	Enabled	

Video of Granting a User Metadata Permissions

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

Wor
king
with

Built-In Metadata

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

Manage Metadata Sets				
Filter Filter by metadata set name		Show 10 items ▼		
Metadata Set Name	Description	Status	Set Type	User Co
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	Default	0
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0
PDF Tag metadata	PDF Tag metadata set	Enabled	Built-in	0
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	0
Extended Metadata	Extended metadata extracted from files	Disabled	Built-in	0
AIP Sensitivity Label metadata	AIP Sensitivity Label metadata set	Enabled	Built-in	0
CDR	Content Disarm and Reconstruction	Enabled	Built-in	0
Signority eSignature	Signority eSignature metadata	Enabled	Built-in	0

Metadata Set Name	Description	Status	Set Type	User Co
CUI Metadata	Controlled Unclassified Information metadata set	Enabled	Built-in	0
ITAR Metadata	International Traffic in Arms Regulations metadata set	Enabled	Built-in	0

Unlike the **Default** metadata set:

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

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

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



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

The sets that have been created for you include:

Image Metadata

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

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

Edit Metadata Set Definition

Metadata Set

Name*

Image metadata

Description*

Image metadata (EXIF)

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name

emma

Read Permission

☒

Page 1 of 1

Attributes

Add Attribute

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

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

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

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

Document Life Cycle Metadata

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

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
emma	☒

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	- Required - This cannot be changed
Description	By default, says: Stores information regarding document life cycle	- Required - This cannot be changed
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	- Not selected - This cannot be changed

Managing Metadata – 316

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

Microsoft 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.

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

Edit Metadata Set Definition

Metadata Set

Name*

Microsoft Office Tag metadata

Description*

Microsoft Office Tag metadata (MSOT)

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name

emma

Read Permission

☒

Page 1 of 1

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	A name given to the resource	Enabled	
Subject	Text	The topic of the resource	Enabled	
Creator	Text	A person, company, or other entity responsible for making the resource	Enabled	
Keywords	Array	Important words or phrases related to the resource	Enabled	

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

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

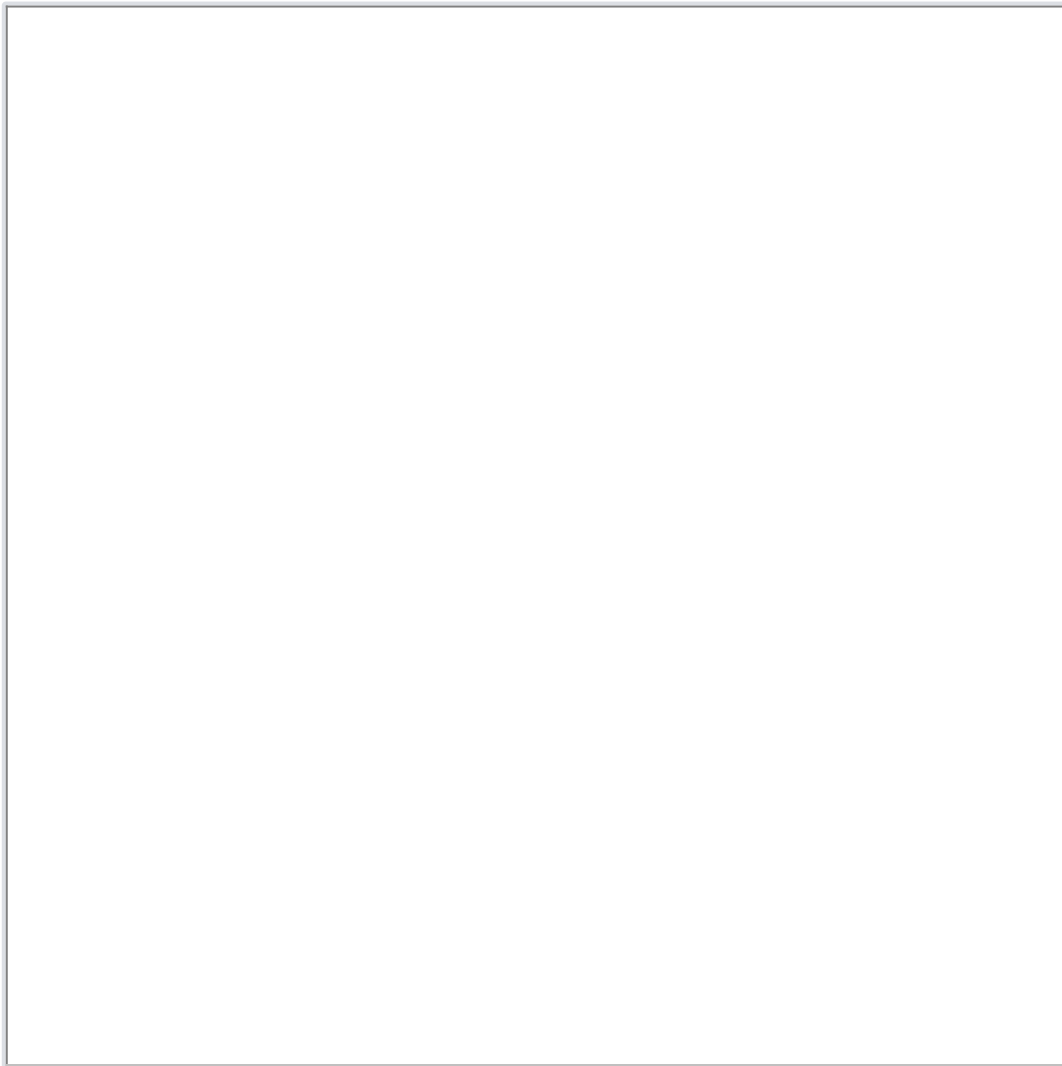
	Description	Options
Keywords	Keyword tags assigned to file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Description	Description of file.	• Not required • Read (can only be changed in Microsoft Office file before uploading)
Last Modified By	Last user who modified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



MSOT Sensitivity Labels

By default, FileCloud does not capture MSOT sensitivity label data even if sensitivity labels are enabled in Office.

Prior to FileCloud 21.2, enabling the Sensitivity Label field was the only way to extract sensitivity label data. In FileCloud 21.2, AIP Sensitivity Label metadata, which captures more details and applies to more file types was added to replace this method; however, the MSOT sensitivity label is still available for backwards compatibility.



To enable FileCloud to capture MSOT sensitivity label data and to display the **Sensitivity Label** field in the **Metadata** panel, add the following setting to the config file.

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);
```

→ | Details Activity Metadata Comments

Microsoft Office Tag Metadata

Title ⓘ
N/A

Subject ⓘ
N/A

Creator ⓘ
Employee

Keywords ⓘ

Description ⓘ
N/A

Last Modified By ⓘ
Employee

Created ⓘ
Feb 10, 2016

Modified ⓘ
Feb 10, 2016

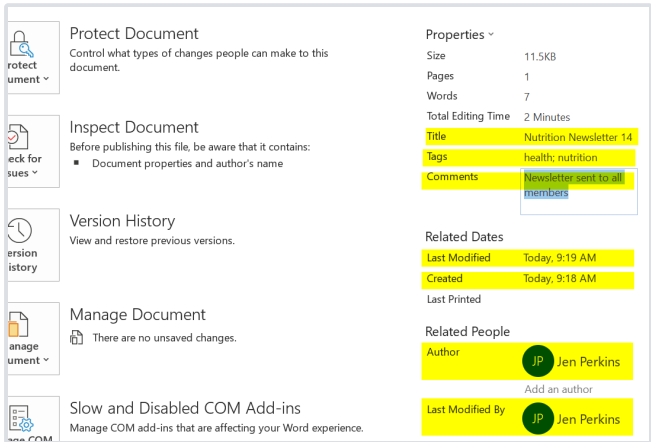
Category ⓘ

Sensitivity Labels ⓘ

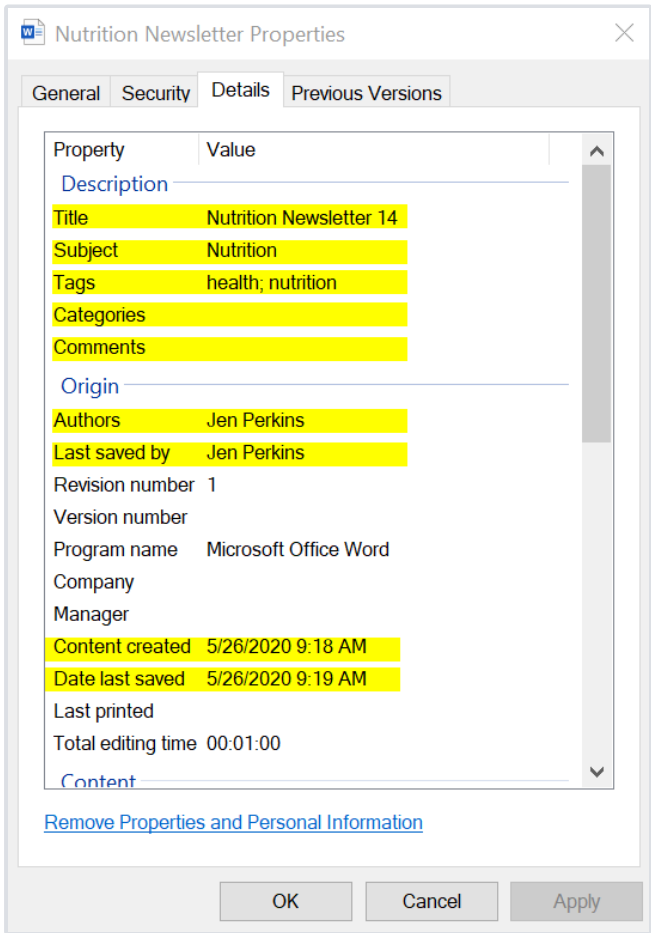
To display this field, enable sensitivity labels.

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:

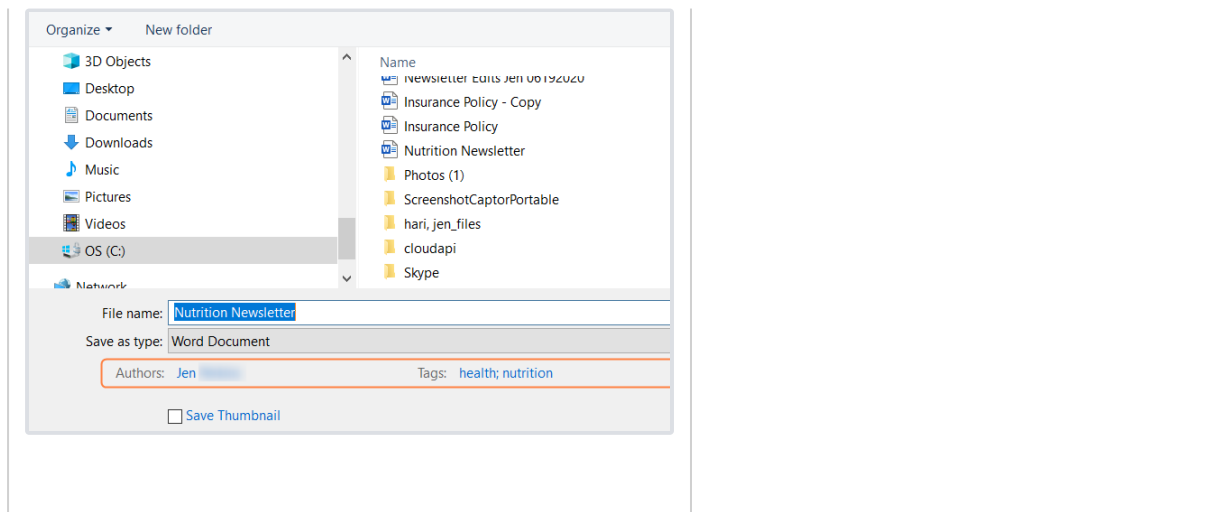


When you right-click an Office document in file explorer and select **Properties > Details** tab:



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*

Color Tagging metadata

Description*

Color Tagging metadata set

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name	Read Permission	Write Permission
emma	☒	☐

Page

1

of 1

Attributes

+ Add Attribute

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

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

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

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

To add values to the Color attribute:

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

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

Edit Attribute

Name: Color

Description: Color

Attribute Type: Key Value Pair

Predefined Values:

- Red:#FF0000
- Yellow:#FF9900
- Green:#18C600
- Aqua:#00B4C9
- Blue:#0054C9
- Purple:#7E00C9
- Orange:#FE9A2E

Disabled: ☐

Required: ☐

Default Value: Tag input

Save Close

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

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

Beginning with FileCloud 21.1, the Smart Classification can apply color tag values to files.

Note: Although users can search on color metadata in both the new and classic user interfaces, they can only apply color tags to files and folders in the new interface.

PDF Tag metadata

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

Edit Metadata Set Definition

Metadata Set

Name*

PDF Tag metadata

Description*

PDF Tag metadata set

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name

emma

Read Permission

☒

Page 1 of 1

Attributes

+ Add Attribute

Name	Attribute Type	Description	Status	Actions
Title	Text	Title of document	Enabled	
Author	Text	Person who created the document	Enabled	
Subject	Text	Subject of the document	Enabled	
Keywords	Array	Keywords associated with the document	Enabled	

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
emma	☒

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	

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

Managing Metadata – 328

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

CDR metadata

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

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

Edit Metadata Set Definition

Metadata Set

Name*

CDR

Description*

Content Disarm and Reconstruction

☐ Disabled

Permissions

Users

Groups

Paths

Search Users to add

Name	Read Permission	Write Permission
No results found		

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
CDR successful	Boolean	Whether the Content Disarm and Reconstruction process succeeded	Enabled	

Save

Close

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

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

Signority eSignature metadata

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

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

Edit Metadata Set Definition

Metadata Set

Name*

Signority eSignature

Description*

Signority eSignature metadata

☐ Disabled

Permissions

Users

Groups

Paths

Search Users to add

Save

Close

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

	Description	Options
Completion Date	Date signing was completed.	Read only

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

ITAR metadata

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

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

Edit Metadata Set Definition

Metadata Set

Name*

ITAR Metadata

Description*

International Traffic in Arms Regulations metadata set

☐ Disabled

Permissions

Users
Groups
Paths

Search Users to add

Name	Read Permission	Write Permission
nik8	☒	☒

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
ITAR 1	Boolean	ITAR CONTROLLED	Enabled	
ITAR 2	Boolean	THIS DOCUMENT CONTAINS ITAR CONTROLLED TECHNICAL DATA	Enabled	
ITAR 3	Boolean	INTERNATIONAL TRAFFIC IN ARMS REGULATIONS	Enabled	

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



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

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

CUI metadata

Note: CUI metadata was added in FileCloud Version 23.252

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

Edit Metadata Set Definition

Metadata Set

Name*

CUI Metadata

Description*

Controlled Unclassified Information metadata set

☐ Disabled

Permissions

Users

Groups

Paths

Search Users to add

Name	Read Permission	Write Permission
No results found		

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Basic	Boolean	Indicates general CUI content governed by standard handling procedures, without additional regulatory categories.	Enabled	  

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

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

Extended metadata



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

How metadata attributes are added

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

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

Metadata attributes are extracted and added to the Extended metadata set if they match regex filters that you have supplied.

Manually created attributes are always available in the Extended metadata set, and if a manually created attribute matches a tag in the file, it is applied to the uploaded file.

Setting an auto extraction limit

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

Why full set of attributes are not added to every file

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

Example

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

Edit Metadata Set Definition

Metadata Set

Name*

Extended Metadata

Description*

Extended metadata extracted from files

☐ Disabled

Permissions

Users

Groups

Paths

Search Users to add

Name	Read Permission	Write Permission
	☒	☐

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
DLPTAH	Text	SAD	Enabled	
DLPTagId01	Text	Extended metadata extracted automatically	Enabled	
DLPTagId02	Text	Extended metadata extracted automatically	Enabled	

Save

Close

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

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

To configure the Extended metadata set:

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

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

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

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

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

- c. To add the per file extraction limit for automatically extracted tags, set TONIDOCLOUD_METADATA_AUTO_TAG_LIMIT to the limit value.

About the limit:

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

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

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

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

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

Once the number of attributes in the limit is reached:

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

Working with Custom Metadata

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

Managing Metadata Sets

[Create a new Set Definition](#)

[Manage Metadata Permissions](#)

[Edit an existing Set Definition](#)

Delete a Set Definition

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

⚠ You cannot undo or revert deletions.

To delete an existing Custom metadata set definition:

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

View the Set Definition List

The metadata set definitions screen displays the list of defined metadata sets.

- The filter text box can be used to filter the metadata sets based on the metadata name.
- The individual metadata set on the metadata list can be viewed, edited and deleted.
- New metadata sets can be added by clicking the Add Metadata Set button and filling in the metadata set definition form.

Manage Metadata Sets

Filter: Filter by metadata set name Show 10 Items

Metadata Set Name	Description	Status	Set Type	User Count	Group Count	ACTIONS
Default	Default metadata set definition will be automatically bound to every single File and Folder.	Enabled	DEFAULT	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

Page 1 of 1 3 rows

Working with Default Metadata

Default is a special metadata set that is automatically associated with every File Object when it is created, copied, uploaded, etc.

- For already existing File Objects it will be associated when the file or folder is accessed for the first time.
- Exactly one Default Set exists in FileCloud - it cannot be deleted, but administrators can customize attributes and permissions or disable it.
- Out of the box it is shipped with a single predefined attribute of Array type - Tags.

Manage Metadata Sets

Filter: Filter by metadata set name 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	Edit Delete
Image metadata	Image metadata (EXIF)	Enabled	Built-in	1	1	Edit Delete
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	1	1	Edit Delete
Date	dfsdfs	Enabled	Custom	3	0	Edit Delete

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

Edit Metadata Set Definition

Metadata Set

Name*

Default

Description*

Default metadata set definition will be automatically bound to every

Disabled

☐

Permissions

Users

Groups

Paths

Add User

Name	Read Permission	Write Permission
emma	☒	☒

Page 1 of 1

Attributes

Add Attribute

Name	Attribute Type	Description	Status	Actions
Tags	Array	Tags	Enabled	

	Description	Options
Name	Title for the metadata set.	- Required - This can be changed - Validated on Creation
Description	By default, says: Default metadata set definition will be automatically bound to every single File and Folder.	- Required - This can be changed - Validated on Creation
Disabled	Stops the metadata set from being automatically bound to every new file and folder.	- By default this is not selected - You can choose to disable this set

	Description	Options
User Permissions	Grant access to specific users to: - Read: this permission displays the metadata to the user in the User Portal - Write: this permission allows the user to add, edit, copy, or paste a value For more information, read Managing Metadata Permissions	- Not Required - Read - Write
Group Permissions	Grant access to specific groups to: - Read: this permission displays the metadata to the user in the User Portal - Write: this permission allows the user to add, edit, copy, or paste a value For more information, read Managing Metadata Permissions	- Not Required - Read - Write
Path Permissions	File Objects in this location will have the metadata set applied For more information, read Managing Metadata Permissions	Not Required
Array	A number of custom values (tags) provided by the administrator	- Name - Description - Disabled - Required - Tag Input
How To Edit a Metadata Set		

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.

FILECLOUD

admin

Manage Metadata Sets

Files Without Metadata 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	0	
Image metadata	Image metadata (EXIF)	Enabled	Built-in	0	1	
Document Life Cycle metadata	Stores information regarding document life cycle	Enabled	Built-in	0	0	
Microsoft Office Tag metadata	Microsoft Office Tag metadata (MSOT)	Enabled	Built-in	0	1	
Color Tagging metadata	Color Tagging metadata set	Enabled	Built-in	1	1	
DLP allowed	Indicates whether DLP should be able to prevent downloading or sharing of these files.	Enabled	Custom	0	0	
Confidential Documents	Confidential Documents	Enabled	Custom	0	1	

4. To display a list of files without metadata, click **Files Without Metadata**.

Files Without Metadata

Q

Filter by path

Filename	File Type	Size	Date	Actions
/jenniferp	Folder			
/team folder account	Folder			
/team folder account/Human Resources	Folder			
/team folder account/Sales	Folder			
/team folder account/recyclebin	Folder			
/jessicam	Folder			
/jenniferp/ShareFolder	Folder			

Add metadata from the Files Without Metadata list

- Follow the procedure above to access your **Files Without Metadata** list.
- Across from a file, click the button under **Actions**.

Files Without Metadata

Filename	Size	Date	Actions
/jenniferp/DriveSSOLogin.jpg	26 KB	Apr 02, 2020 1:59 PM	

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](#).

3. To add a custom metadata set, choose it in the drop-down list and click **Add**. It is added below the other metadata sets.
4. Add or change values in any of the metadata fields.

Manage File Metadata

add

No metadata available

Default

Document Life Cycle metadata

codes

Remove

color

pink

alphanumeric

1A

label

Tax

Save

Close

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:

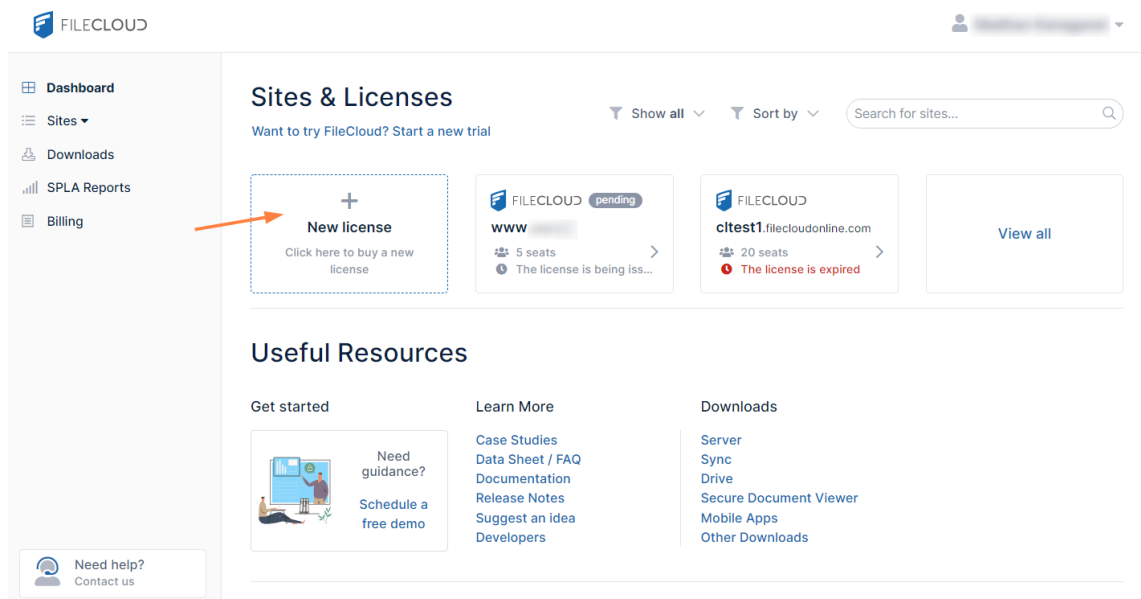
FileCloud - License Purchase And Renewal

Purchase a new license

First

Choose a server or online license

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



3. In the **Buy FileCloud** window, click **Online** or **Server**.

Buy FileCloud

**Online**
Run FileCloud on our
secure infrastructure

**Server**
Run FileCloud on your
own infrastructure

or

[If you are a Service Provider](#)

[Looking for other items](#)

[Need help?](#)
Contact us

[Cancel](#)

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

✓

Unlimited Storage

✓

Unlimited Licensed External Users

✓

Support for Network Shares with NTFS Integration for VPN-less secure access.

✗

Content Classification & Search

✗

Content Lifecycle Management - Legal Hold, Retention, & Archival

✗

Unlimited Workflows

✗

Digital Rights Management

✗

Key Integrations - MS Teams, Salesforce, Active Directory & SIEM

✗

Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments)

RECOMMENDED

Advanced

Custom pricing available

GET QUOTE

✓

Unlimited Storage

✓

Unlimited Licensed External Users

✓

Support for Network Shares with NTFS Integration for VPN-less secure access.

✓

Content Classification & Search

✓

Content Lifecycle Management - Legal Hold, Retention, & Archival

✓

Unlimited Workflows

✓

Digital Rights Management

✓

Key Integrations - MS Teams, Salesforce, Active Directory & SIEM

✓

Optimized Multi-Site Architecture (high-performance, scalable and redundant data access in distributed data center environments)

Service Provider

Custom pricing available

GET QUOTE

✓

Unlimited Storage

✓

Unlimited Licensed External Users

✓

Support for Network Shares with NTFS Integration for VPN-less secure access.

✓

Content Classification & Search

✓

Content Lifecycle Management - Legal Hold, Retention, & Archival

✓

Unlimited Workflows

✓

Digital Rights Management

✓

Key Integrations - MS Teams, Salesforce, Active Directory & SIEM

✓

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.

Contact Us

Sales

Available Now

Questions, feedbacks,
comments about your license?

Chat Now

Schedule a free demo

sales@filecloud.com

+1 (888) 571-6480

Support

Available Now

Need help with FileCloud?

support@filecloud.com

Submit a Ticket

Close

Managing FileCloud Licenses – 355

If you choose **Essentials**, an **Order details** window opens.

Order details

FileCloud Server - Enterprise Essentials

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

Number of Users

Drag the slider below to change

20 seats
1

Recommended Support
2

Optional

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

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

☐ FileCloud Self Service Email Technical Support
Free

Licensed Site URL ⓘ

files.yoursite.com
3

Need professional assistance?

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

Total

Billed annually ⓘ

Need help?
Contact us

Back

4 Checkout

1. Move the **Number of Users** slider to indicate the number of users to include on the license.
2. Choose a support option.
3. In **Licensed Site URL**, enter your site address.
4. Click **Checkout**.
5. Perform the [checkout process](#), below.

or

Purchase the online license

If you choose **Online**, the next window prompts you to choose **Essentials**, **Advanced**, or **GovCloud**.

Buy FileCloud



FileCloud Online

Run FileCloud on our secure infrastructure

Essentials	Advanced	GovCloud
\$12⁵⁰ user/mo minimum 10 users, billed annually ⓘ BUY	\$18⁷⁵ user/mo minimum 50 users, billed annually ⓘ BUY	GovCloud Custom pricing available GET QUOTE
✓ 1 TB. 100 GB per User	✓ 1 TB. 200 GB per User	✓ 1 TB. 200 GB per User
✓ Unlimited Licensed External Users	✓ Unlimited Licensed External Users	✓ Unlimited Licensed External Users
✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection	✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection	✓ Region-Specified, Dedicated Single-Tenant Hosting - Fully Isolated Data-Layer Protection
✗ Sync/Backup Local File Server to Cloud	✓ Sync/Backup Local File Server to Cloud	✓ Sync/Backup Local File Server to Cloud
✗ Content Classification & Search	✓ Content Classification & Search	✓ Content Classification & Search
✗ Content Lifecycle Management - Legal Hold, Retention, & Archival	✓ Content Lifecycle Management - Legal Hold, Retention, & Archival	✓ Content Lifecycle Management - Legal Hold, Retention, & Archival
✗ Unlimited Workflows	✓ Unlimited Workflows	✓ Unlimited Workflows
✗ Digital Rights Management	✓ Digital Rights Management	✓ Digital Rights Management
✗ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM	✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM	✓ Key Integrations - MS Teams, Salesforce, Active Directory & SIEM
✗ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations	✗ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations	✓ Enable compliance with FIPS 140-2, ITAR, EAR, + Other Regulations
More...	More...	More...

If you click the **GovCloud**, in the window that opens, choose an option for contacting Sales and making your purchase.

Contact Us

Sales

Available Now

Questions, feedbacks,
comments about your license?

Chat Now

Schedule a free demo

sales@filecloud.com

+1 (888) 571-6480

Support

Available Now

Need help with FileCloud?

support@filecloud.com

Submit a Ticket

Close

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

Drag the slider below to change

50 seats
1

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 ⓘ

Preferred Region

files.yoursite.com 3

US East (Northern Virginia) 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.

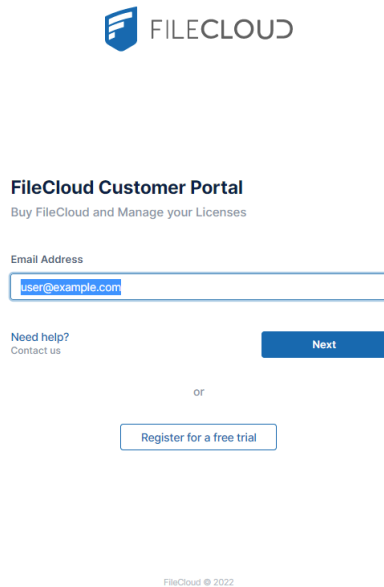
Renew an existing license

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@codeatthe.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.)

Sites & Licenses

Want to try FileCloud? Start a new trial

Show all Sort by Search for sites...

New license
Click here to buy a new license

FILECLOUD pending
www.zeal.net
5 seats
The license is being issued

FILECLOUD
cftest1.filecloudonline.com
20 seats
The license is expired

View all

Useful Resources

Get started
Need guidance?
Schedule a free demo

Learn More
Case Studies
Data Sheet / FAQ
Documentation
Release Notes
Suggest an idea
Developers

Downloads
Server
Sync
Drive
Secure Document Viewer
Mobile Apps
Other Downloads

Latest News

FEB 22 Upgrade Your FileCloud Cluster and MongoDB with...

FEB 9 FileCloud Recognized as a Gartner Peer...

JAN 31 Security Recommendations, Part 1: Protect You...

JAN 21 Securing Your FileCloud Installation with a Wildcard...

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

Sites & Licenses

Want to try FileCloud? Start a new trial

Show all Sort by Search for sites...

New license
Click here to buy a new license

FILECLOUD pending
5 seats
The license is being issued

FILECLOUD
cftest1.filecloudonline.com
20 seats
The license is expired

FILECLOUD
OnPremise
20 seats
Expires in 898 days

FILECLOUD
OnPremise
20 seats
The license is expired

FILECLOUD
SPLA
10 seats
The license is expired

FILECLOUD
200 seats
Expires in 108 days

View less

Useful Resources

Get started
Need help? Contact us

Learn More

Downloads

A screen that displays the license details opens.

4. Click the **Renew** button.

FILECLOUD ONPREMISE



FILECLOUD

Usage

License

0 days left

20 seats

Server Standard



Renew

Getting Started with your FileCloud Server

- 1. Download FileCloud Server**
Run FileCloud Server on a wide variety of platforms
- 2. Download your license**
You will need your license to install activate your FileCloud installation
- 3 Learn the FileCloud basics**
Watch videos on how to get started.

Quick Actions

Buy extra seats
Expand the number of licenses.

An **Order Summary** opens.

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

Add additional users to an existing license

Add additional users to a license

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

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



FILECLOUD

FileCloud Customer Portal

Buy FileCloud and Manage your Licenses

Email Address

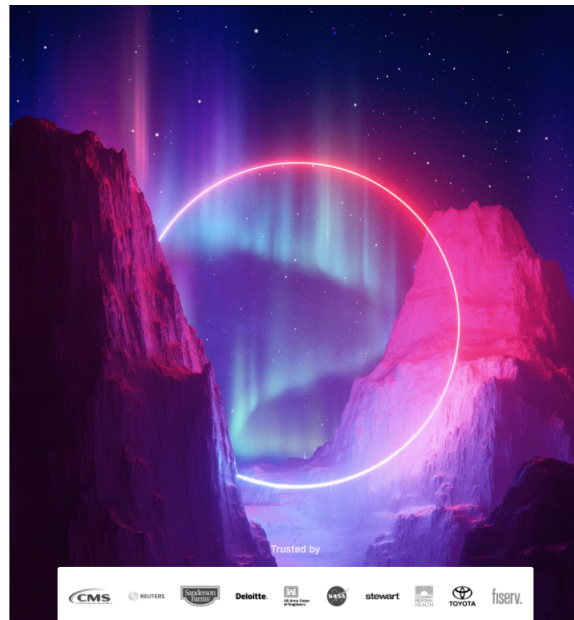
Need help?
Contact us

Next

or

Register for a free trial

FileCloud © 2022



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.)

Sites & Licenses

Want to try FileCloud? Start a new trial

[New license](#)
Click here to buy a new license

FILECLOUD pending
www.zeal.net
5 seats
The license is being issued

FILECLOUD
citest1.filecloudonline.com
20 seats
The license is expired

[View all](#)

Useful Resources

Get started
Need guidance?
Schedule a free demo

Learn More
Case Studies
Data Sheet / FAQ
Documentation
Release Notes
Suggest an idea
Developers

Downloads
Server
Sync
Drive
Secure Document Viewer
Mobile Apps
Other Downloads

Latest News

FEB 22 Upgrade Your FileCloud Cluster and MongoDB with...

FEB 9 FileCloud Recognized as a Gartner Peer...

JAN 31 Security Recommendations, Part 1: Protect You...

JAN 21 Securing Your Filecloud Installation with a Wildcard...

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

Sites & Licenses

Want to try FileCloud? Start a new trial

[New license](#)
Click here to buy a new license

FILECLOUD pending
5 seats
The license is being issued

FILECLOUD
citest1.filecloudonline.com
20 seats
The license is expired

FILECLOUD
Server Trial
20 seats
The license is expired

FILECLOUD
500 seats
Expires in 173 days

FILECLOUD
OnPremise
20 seats
Expires in 898 days

FILECLOUD
OnPremise
20 seats
The license is expired

FILECLOUD
SPLA
10 seats
The license is expired

FILECLOUD
200 seats
Expires in 108 days

[View less](#)

Useful Resources

Get started
Need help?
Contact us

Learn More

Downloads

A screen that displays the license details opens.

4. Click **Buy extra seats**.

FILECLOUD ONPREMISE
FILECLOUD

Usage

License

898 days left

20 seats
Server Standard

[Renew](#)

Getting Started with your FileCloud Server

1. Download FileCloud Server
Run FileCloud Server on a wide variety of platforms
2. Download your license
You will need your license to install activate your FileCloud installation
- 3 Learn the FileCloud basics
Watch videos on how to get started.

Quick Actions

[Buy extra seats](#)
Expand the number of licenses.

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

[Cancel](#)

[Checkout](#)

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

filecloud

5 Main Street

Newtown / MA / 55555

United States

Edit Billing Details

Additional Info

P.O. Number

Optional

Notes

Optional

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

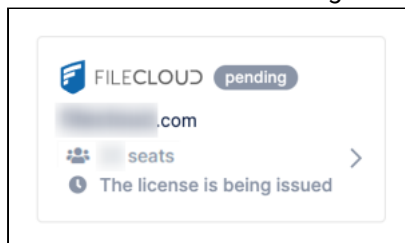
Need help?
Contact us

Save Quote

Checkout

2. Click **Checkout**.

3. Enter your credit card number, and click **Pay Now**.
A confirmation window appears.
4. Click **Dashboard** in the navigation pane to see an icon for your new pending license:



or

Send a purchase order

1. Look over the order summary, and if necessary, edit the billing details:

Order summary

Billing Details

filecloud
5 Main Street
Newtown / MA / 55555
United States

Edit Billing Details

Additional Info

P.O. Number
Optional

44444

Notes
Optional

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

- Optionally, enter a **P.O. Number** and any **Notes** for FileCloud Sales.
- Click **Save Quote**.
The **Billing** screen opens.
- Your order appears under **Orders History** with the status **QUOTE**.

Managing FileCloud Licenses – 367

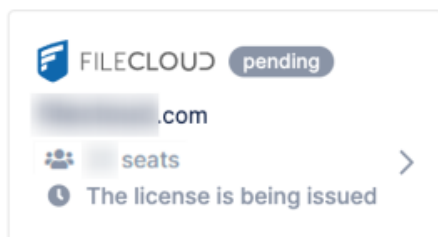
Orders History				
Filter Filter orders... Buy new license				
Order #	Issued	Amount	Balance Due	Status
FC-30557	23 Sep 2022			INVOICE
FC-30574	26 Sep 2022			QUOTE

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.

Orders History				
Filter Filter orders... Buy new license				
Order #	Issued	Amount	Balance Due	Status
FC-30557	23 Sep 2022	\$7,500.00	\$7,500.00	IN
FC-30574	26 Sep 2022	\$12,450.00	\$12,450.00	Q

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

filecloud
5 Main Street
Newtown / MA / 55555
United States

Edit Billing Details

Additional Info

P.O. Number
Optional

Notes
Optional

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.

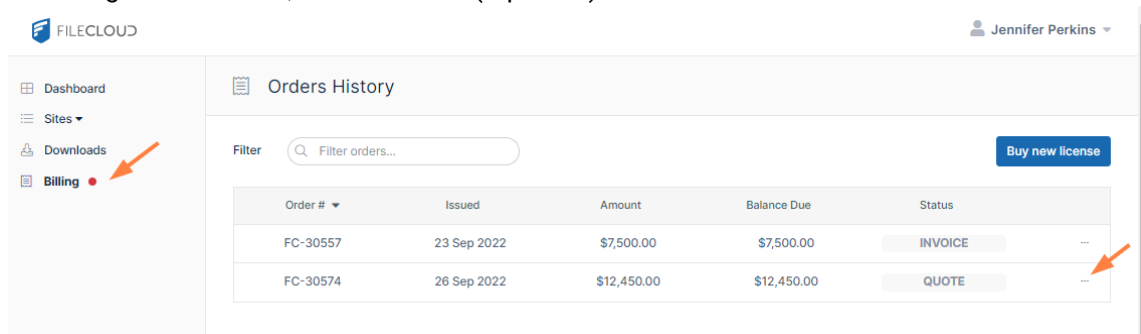
Orders History				
Filter Filter orders... Buy new license				
Order # ▼	Issued	Amount	Balance Due	Status
FC-30557	23 Sep 2022			INVOICE ...
FC-30574	26 Sep 2022			QUOTE ...

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

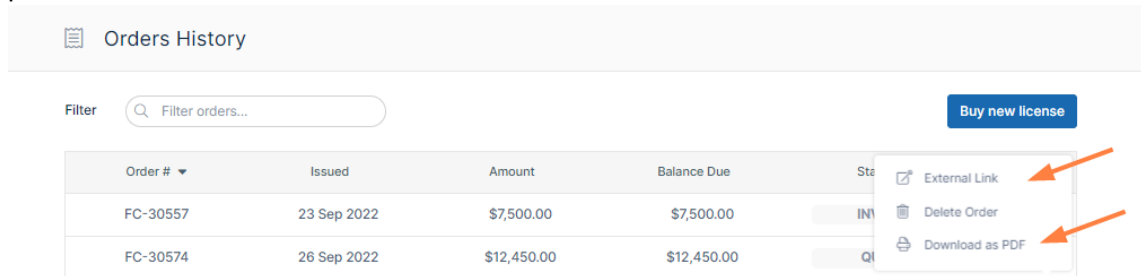
Manage orders

View order, save order link, save to pdf or delete order history

- Log into <https://portal.getfilecloud.com>
- In the navigation pane, click the **Billing** link.
- To the right of the order, click the **More** (triple-dot) icon.



- 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	• All features • Mobile and desktop apps • Free support Deployment URL will be set as "*" (accessible from any URL)	Server (Self-host) Online (Hosted by us)
Production	Permanent based on length paid for Usually 1 year	• All features • Mobile and desktop apps • Choose from 3 levels of support Deployment URL can be set to use your specific domain (URL accessibility from within your company and outside access managed by Administrators)	Server (Self-host) • Essentials • Advanced • Service Provider Online (Hosted by us) • 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 download 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.

Sites & Licenses

Want to try FileCloud? Start a new trial

[Show all](#) [Sort by](#)

[New license](#)
Click here to buy a new license

FILECLOUD pending
www...
5 seats
The license is being issued

FILECLOUD
cftest1.filecloudonline.com
20 seats
The license is expired

[View all](#)

Useful Resources

Get started
Need guidance?
Schedule a free demo

Learn More
Case Studies
Data Sheet / FAQ
Documentation
Release Notes
Suggest an idea
Developers

Downloads
Server
Sync
Drive
Secure Document Viewer
Mobile Apps
Other Downloads

Latest News

FEB 22 Upgrade Your FileCloud Cluster and MongoDB with...

FEB 9 FileCloud Recognized as a Gartner Peer...

JAN 31 Security Recommendations, Part 1: Protect You...

JAN 21 Securing Your FileCloud Installation with a Wildcard...

- 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).
- Click the license that you want to download.

Sites & Licenses

Want to try FileCloud? Start a new trial

[Show all](#) [Sort by](#)

[New license](#)
Click here to buy a new license

FILECLOUD pending
5 seats
The license is being issued

FILECLOUD
cftest1.filecloudonline.com
20 seats
The license is expired

FILECLOUD
Server Trial
20 seats
The license is expired

FILECLOUD
500 seats
Expires in 173 days

FILECLOUD OnPremise
20 seats
Expires in 898 days

FILECLOUD OnPremise
20 seats
The license is expired

FILECLOUD
100 seats
The license is expired

FILECLOUD
SPLA
10 seats
The license is expired

FILECLOUD
200 seats
Expires in 108 days

[View less](#)

Useful Resources

Get started **Learn More** **Downloads**

- 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 License settings page.](#)

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

Invalid License File

Example path on Windows: c:\clouddata
Example path on Linux: /opt/cloud/data

Check Path

Apply

Upload your license via Install License

Install License

Browse...

Choose License file (Only .xml)

Apply

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.

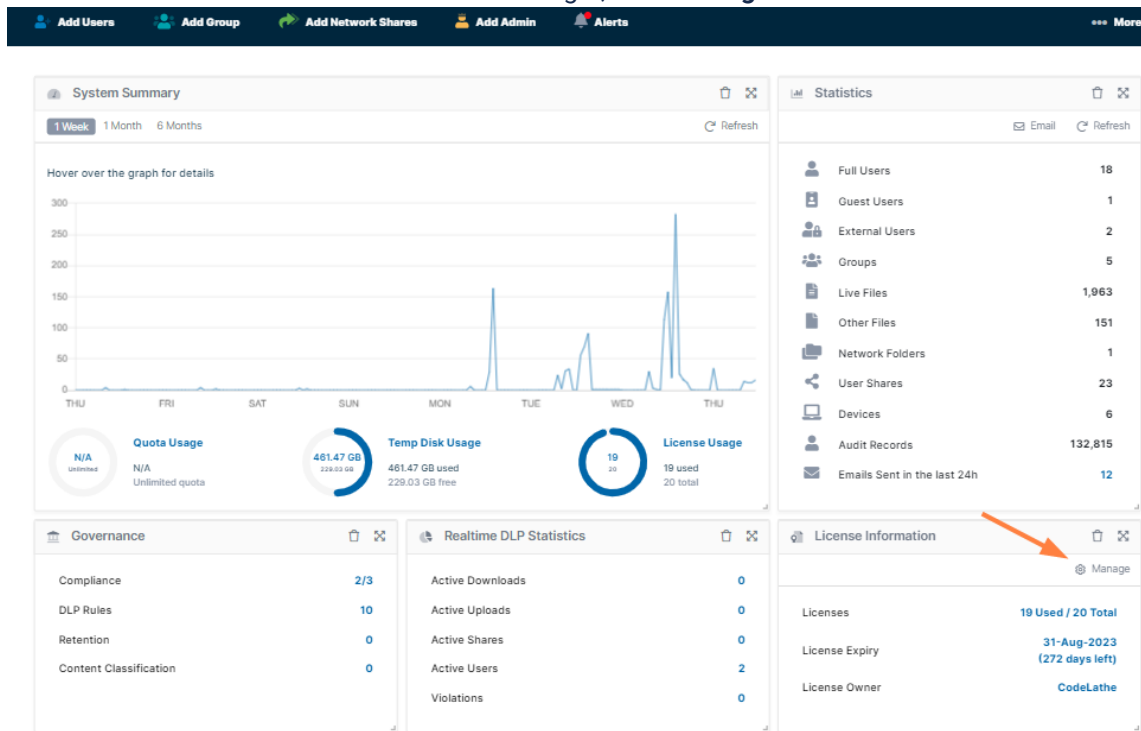
Dashboard

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 go to the License settings page.

License

[Reset to defaults](#)
[Copy license key](#)

License owner

Codelathe

Expiry date

9-Mar-2025

Usage information

49 Used / 100 Total

Components

Tonido Cloud,ENTERPRISE

Update license
button: Choose file

Choose license file to update (file type must be .xml)

No file chosen

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**.



If you have hosts available for accessing FileCloud in addition to the one listed in Server URL, your FileCloud installation log may display **Not allowed host** errors for those hosts.

To avoid getting Not allowed host errors:

1. Open cloudconfig.php at
 - Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
 - Linux: /var/www/config/cloudconfig.php
2. Add the following, replacing the Server URLs with your own.

```
define("TONIDOCLOUD_ALLOWED_HOSTS",
"mycompany.store1.com,mycompany.store2.com,mycompany.store3.com");
```


Workflows - IFTTT

Administrators can use workflows to automate certain standard operations within FileCloud.

Workflows operate using the following model:

IF "CONDITION" - THEN "ACTION" (IFTTT)

You can setup specific triggers to run when the following conditions occur:

- A system event
- A specific date and time
- A variety of actions

💡 Each of the Conditions and Actions may require a parameter in JSON format.

The Workflow Dashboard

All workflows are created and managed on the Workflows dashboard.

Manage Workflows

Add Workflow

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
client app connects	If any new client app connects	Notify user(s)	May 30, 2025, 4:40 pm	May 27, 2025, 7:09 pm		
when a file created	If a file is created	Notify file actions to user(s)	May 30, 2025, 4:43 pm	December 3, 2024, 5:31 am		
New Client	If any new client app connects	Notify user(s)	May 30, 2025, 4:40 pm	May 27, 2025, 7:09 pm		

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:

Enabled	Actions					
1 	2 	3 	4 	5 	6 	

1. Enable or Disable the workflow
2. Run the workflow (once, on-demand)
3. Simulate the workflow. Displays the list of users or files that a workflow will affect. The Simulate option is only available to workflows that are configured to run on demand and not to run automatically at scheduled times.
4. Edit the workflow
5. See activity. (Shows the date of an event, and a description of the event, such as file upload, move, and deletion.
6. Delete the workflow

In this section:

Add a New Workflow



It is important to note that not all actions are compatible with all conditions. Please see the table on the page [Define a THEN Action](#) for compatible settings.

Administrators can add Workflows in the Admin Portal.

You will need to choose a condition, and specify what action should be taken when that condition occurs.

- [Define an IF Condition](#)
- [Define a THEN Action](#)

To add a new workflow:

1. Open a browser and log into the Admin Portal.
2. On the left hand navigation panel, click **Workflows**.
3. On the top right, click the Add Workflow button.
4. In the Create New Workflow window, select an [IF Condition](#), and then click Next.
5. If a condition requires you to specify a value for something, for example a date or time, type in the values in the Required Parameters, and then click Next. Information about what is required is described below this box.
6. In the Create New Workflow window, select a [THEN Action](#), and then click Next.
7. If an Action requires you to specify a value for something, for example a date or time, type in the values in the Required Parameters, and then click Next. Information about what is required is described below this box.

8. In Workflow Name, type in a unique word or phrase that describes the workflow, and then click Finish.

Create New Workflow ✕

Name for this action

Workflow Name

← Previous

→ Finish

✕ Cancel

Define an IF Condition



Beginning in version 23.253, FileCloud supports expressions, special conditions based on user and path owner properties.



The workflow **If a user's account is near its expiration date** is available in FileCloud 23.251 and later.



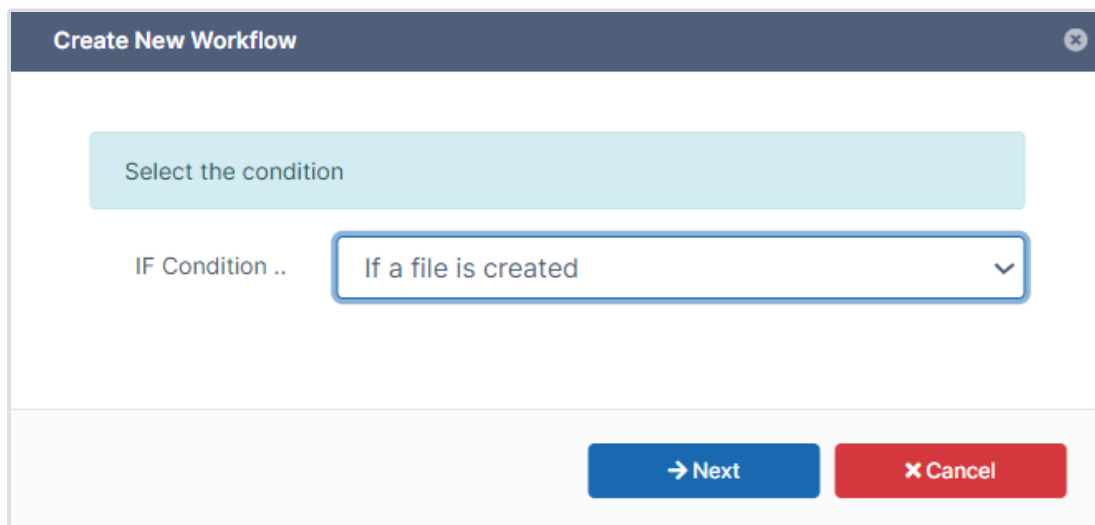
Not all actions are compatible with all conditions.

When you create a workflow, you must select a condition to act as a trigger.

- Depending on the trigger, additional parameters may be required.
- Once a Condition is selected, compatible Actions can be selected.

Where do I set up the condition?

When you create a new Workflow, you will be able to select a condition.



The image shows a 'Create New Workflow' dialog box. At the top, there is a dark blue header bar with the text 'Create New Workflow' and a close button (X) on the right. Below the header, there is a light blue rectangular box containing the text 'Select the condition'. Underneath this box, the text 'IF Condition ..' is followed by a dropdown menu. The dropdown menu is open, showing the selected option 'If a file is created' and a downward arrow. At the bottom of the dialog box, there are two buttons: a blue button with a right arrow and the text 'Next', and a red button with a close icon (X) and the text 'Cancel'.

Where do I add my parameters?

After you select a Condition, then you can enter any parameters, such as a date or time.

If you need more information about what parameters are required, look below the Required Parameters box.

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition will be triggered when a file is created.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

use_regex (optional)
Specifies whether the path has a regex format.

exclude (optional)
Exclude items matching the specified path/pattern from the action.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

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.

The client can be mobile app, drive app, sync app etc.

Parameters

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Expression Support

You can use expressions to add complex conditions based on user properties:

User Context Variables

- **_user.groups** - User's group memberships
- **_user.policy** - User's assigned policy
- **_user.email** - User's email address
- **_user.username** - User's username

Workflow Condition	Parameters	Description
If any new client app connects	No parameters required	This condition is triggered when an external (non-browser) client connects to FileCloud Server. For example, this condition will trigger for clients such as: • FileCloudSync • FileCloudDrive • iOS • Android App

Available expression variables: **User Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

File Conditions

If a file is created

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.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

use_regex (optional)
Specifies whether the path has a regex format.

exclude (optional)
Exclude items matching the specified path/pattern from the action.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Expression Support

You can use expressions to add complex conditions based on user and path properties:

User Context Variables

- _user.groups** - User's group memberships

- `_user.policy` - User's assigned policy
- `_user.email` - User's email address
- `_user.username` - User's username

Path Context Variables

- `_path.owner` - Owner object with user properties
 - `_path.owner.username` - Owner's username
 - `_path.owner.groups` - Owner's group memberships
 - `_path.owner.email` - Owner's email address
 - `_path.owner.policy` - Owner's assigned policy

Workflow Condition	Parameters	Description
If a file is created	<pre>{ "parent_folder_path_string":"/ userid/ somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered if a file is created via any means (Browser, Clients, etc.) parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies how the folder path is validated. • 0 or unspecified = use an exact match for the parent folder path string • 1 = use a regular expression match for the parent folder path string exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a file is updated

Workflow Condition	Parameters	Description

If a file is updated.	<pre>{ "parent_folder_path_string":"/ userid/ somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered if a file is updated. parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies how the folder path is validated. 0 or unspecified = use an exact match for the parent folder path string 1 = use a regular expression match for the parent folder path string exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables, Path Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a file is deleted

Workflow Condition	Parameters	Description
If a file is deleted	<pre>{ "parent_folder_path_string":"/ userid/ somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered if a file is deleted. parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies how the folder path is validated. 0 or unspecified = use an exact match for the parent folder path string 1 = use a regular expression match for the parent folder path string exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables, Path Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#) Available expression variables: **User Context variables, Path Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If file is downloaded

Workflow Condition	Parameters	Description

If a file is downloaded	<pre>{ "parent_folder_path_string":"/ userid/ somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered if a file is downloaded parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies how the folder path is validated. 0 or unspecified = use an exact match for the parent folder path string 1 = use a regular expression match for the parent folder path string exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a file is added or updated

Workflow Condition	Parameters	Description
If a file is added or updated	<pre>{ "parent_folder_path_string":"/ userid/ somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered if a file is added or updated parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies how the folder path is validated. 0 or unspecified = use an exact match for the parent folder path string 1 = use a regular expression match for the parent folder path string exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables**, **Path Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If file was not modified/created in specified days

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.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

trigger_date: The **MODIFIED_DATE** option is only applicable for files.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

number_of_days (required)
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)
Exclude items matching the specified path/pattern from the action.

trigger_date (optional)
Defines which file date to use when evaluating the condition (BOTH, MODIFIED_DATE, CREATED_DATE).

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Parameters	Description

If a file was not modified/created in specified days	<pre>{ "parent_folder_path_string": "/johndoe", "number_of_days": 7, "skip_recently_accessed": 1, "exclude_recyclebin": 1, "exclude": ".*secret.*" }</pre>	This condition will be triggered if a file was not created [specified days] ago or has not been updated for [specified days]. • This is useful for removing old files that are no longer being used • This check will run once a day parent_folder_path_string - required as a parameter for this condition to trigger. • If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. • NOTE: ONLY Managed storage paths are supported for this condition. number_of_days - required to specify the number of days before the current date that a file was last modified. • This will be checked once a day and all files that match this condition will be subject to the THEN action you choose. • For example, if you specify the number of days as 15, all files in the specified folder that have not been modified in the last 15 days will subject to the the THEN action you configure. skip_recently_accessed - required to specify whether files that were viewed or downloaded during the number of days are considered modified. Default is <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. exclude_recyclebin - (added in FileCloud version 21.3) optional (default is false) When true, files in recycle bin are not considered. exclude - (added in FileCloud version 22.1) optional - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths). trigger_date - (added in FileCloud version 23.253) optional (default is BOTH) - specifies which field to use as the date the file was last modified. Use one of the following values: BOTH - (default) Check if the CREATED_DATE and the MODIFIED_DATE are the specified number of days ago or more. CREATED_DATE - Check if the CREATED_DATE is the specified number of days ago or more. MODIFIED_DATE - Check if the MODIFIED_DATE is the specified number of days ago or more.

Available expression variables: **User Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If the file uploaded is bigger than the expected size

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.

Parameters

size (required)
Size expected in MB.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

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

Available expression variables: **User Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If the file downloaded is bigger than the expected size

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

Available expression variables: **User Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

Folder Conditions

If a folder is created

Workflow Condition	Parameters	Description
If a folder is created	<pre>{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered when a folder is created in the system parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables, Path Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a folder is deleted

Workflow Condition	Parameters	Description
If a folder is deleted	<pre>{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }</pre>	This condition will be triggered when a folder is deleted parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables, Path Context variables.**

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

User Account Conditions

If a user's last login is older than...

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition is triggered if a user's last login is older than specified days. This check will run based on the day interval configured.

Parameters

last_login_days_ago (required)
Number of days since last login.

user_account_type (required)
Type of user account (USER_ACCOUNT_ANY, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS, USER_ACCOUNT_DISABLED).

day_interval (required)
Days interval (For daily operation, specify this value to be 1).

skip_users_not_logged_in (optional)
Skip users who have never logged in to the system.

skip_admin_users (optional)
Skip promoted admins. Default is true.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

	Workflow Condition	Parameters	Description
If a user's last login is older than . ..	{	<pre> "last_login_days_ago": 30, "user_account_type": "USER_ACCOUNT_LIMITED_ACCESS", "day_interval": 1, "skip_users_not_logged_in": 1, "skip_admin_users": 0, "include_domain": "domain.com", "exclude_domain": "subdomain.domain.com,@otherdomain.com" } </pre> <i>For example, every five days to check for full access users who have not logged in for the last 30 days. Omit them from this check if they have never logged in or are promoted admins.</i> <pre> { "last_login_days_ago": 30, "user_account_type": "USER_ACCOUNT_FULL_ACCESS", "day_interval": 1, "skip_users_not_logged_in": 1, "skip_admin_users": 1, } </pre>	If a user's last login is older than the specified number of days, then the THEN condition you configure will be run. last_login_days_ago: Number of days since last login. user_account_type - type of account. You must use one of the following values: • USER_ACCOUNT_ANY • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (for external users) • USER_ACCOUNT_DISABLED day_interval - the number of days between checks • For daily operation, specify a value of 1 skip_users_not_logged_in (optional): Skip users who have never logged in to the system. This enables you to only apply the action to users who are already using the system. Values are true and false. skip_admin_users (added in FileCloud 23.251) Optional. Do not include promoted admins. 0 (default) - Include promoted admins 1 - Do not included promoted admins

Available expression variables: **User Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a new user is created

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition will trigger the proper action depending on the security state of a created user.

Parameters

auth_type (optional)
Type of authentication (DEFAULT, ACTIVEDIRECTORY, LDAP).

user_access_level (optional)
Account access level
(USER_ACCOUNT_ANY_ACCESS, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS). Default is "USER_ACCOUNT_ANY_ACCESS".

user_login_method (optional)
How user authenticates (LOGIN_METHOD_ANY, LOGIN_METHOD_DEFAULT, LOGIN_METHOD_SSO). Default is "LOGIN_METHOD_ANY".

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Parameters	Description
If a new user is created ...	<i>None</i>	When a new user account is created, the THEN action you configure will be triggered. Optional Parameters auth-type - Type of authentication. This is optional and can be: • DEFAULT • ACTIVEDIRECTORY • LDAP user_access_level: Account access level. This is optional and can be: • USER_ACCOUNT_ANY_ACCESS (default) • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (for external users) user_login_method: How user authenticates. This is optional and can be: • LOGIN_METHOD_ANY (default) • LOGIN_METHOD_DEFAULT • LOGIN_METHOD_SSO

Available expression variables: **User Context variables** (_user.email, _user.username)

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a user's account is older than

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition is triggered when a user's account is older than the specified days. This is checked based on the day interval configured.

Parameters

days (required)
Number of days after account creation.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workfl ow Condi on	Parameters	Description

If a user's create date is older than Available in FileCloud Version 23.232	<pre>{ "days": 30, "include_domain": "contractor.com", "exclude_domain": "subdomain.domain.com,@otherdomain.com" }</pre> For example, if a user's account was created more than 60 days ago and it is in the domain contractor.com <pre>{ "days": 60, "include_domain": "contractor.com", }</pre>	This condition is triggered when a user's create date is older than the number of days specified in days. Parameters days - Required. When a user's create date is older than this number of days, the condition is triggered.

Available expression variables: **User Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

If a user's account is near its expiration date

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition will trigger if a user's account is nearing its expiration date, based on the number of days configured.

Parameters

days_to_expiry (required)
Number of days before the account expires.

days_interval (optional)
Days interval to perform the check (For daily operation, specify this value to be 1). Default is 5.

skip_admin_users (optional)
Skip promoted admins. Default is true.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Parameters	Description
If a user's account is near its expiration date	<pre>{ "days_to_expiry": 10, "days_interval": 5, "skip_admin_users": 1 }</pre> For example, When a user's account is set to expire in 15 days, perform an action such as sending the user an email. Send the email again every 5 days, but the last 5 days, send the email every day. Do not perform the action on promoted admins. <pre>{ "days_to_expiry": 15, "days_interval": 5, "skip_admin_users": 1 }</pre>	days_to_expiry - Number of days before account expiration days_interval - (optional) At what interval to perform the action again after it is performed the first time. During the last interval, the action is performed every day. Default is 5 days. For example: - Action is "Send an email" - days_to_expiry = 15 - days_interval = 5 An email is sent at 15 days before account expiration, 10 days before account expiration and 5, 4, 3, 2, and 1 days before account expiration. skip_admin_users Optional. Do not include promoted admins. 0 (default) - Include promoted admins 1 - Do not included promoted admins Interval Logic During the last interval, the action is executed every day. For example: - Action: "Send an email" - days_to_expiry = 15 - days_interval = 5 An email is sent at 15 days before account expiration, 10 days before account expiration and 5, 4, 3, 2, and 1 days before account expiration.

Other Conditions

If a comment is added

💡 Comments can be added to files and folders.

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 comment is added to a file or folder.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

use_regex (optional)
Specifies whether the path has a regex format.

exclude (optional)
Exclude items matching the specified path/pattern from the action.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Required Parameters	Description

If a comment is added	<pre>{ "parent_folder_path_string": "/userid/somepath", "use_regex":"1", "exclude":"1" }</pre> Available expression variables: User Context variables. For instructions on including expressions, see Using Expressions in IF Conditions	This condition will be triggered when a comment is added parent_folder_path_string - required as a parameter for this condition to trigger. If the condition needs to be triggered for all folders, then you can set it to be "/". For help specifying the path correctly, see Identifying a FileCloud Specific Path. use_regex (optional) - specifies whether system uses an exact match for the parent folder path string ("use_regex": "0" or missing) or whether to use a regular expression match ("use_regex":"1") exclude (optional) - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths).

Available expression variables: **User Context variables, Path Context variables.**
For instructions on including expressions, see [Using Expressions in IF Conditions](#)

Perform an action periodically at specified time and interval

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

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

This condition will be triggered when the current time matches the supplied time.

day_interval : Days interval (For daily operation, specify this value to be 1)

time_string : (OPTIONAL) Time in format H:i:s (If not specified, it will run at 00:00:00)

start_date : (OPTIONAL) Start date in format yyyy-mm-dd (If not specified, it will start from today)

end_date : (OPTIONAL) End date in format yyyy-mm-dd (If not specified, it will run indefinitely)

```
{
  "day_interval": 7,
  "time_string": "08:00:00",
  "start_date": "2020-01-01",
  "end_date": "2020-01-31"
}
```

← Previous

→ Next

✕ Cancel

Workflow Condition	Parameters	Description
Perform an action periodically at specified time and interval	<pre>{ "time_string": "1 6:45:05", "day_interval": "7 "} </pre>	This condition will be triggered when the current time on the FileCloud Server matches the supplied time. day_interval - number of days that passes after a THEN action before it is triggered again. - The THEN action you choose will be triggered every "day_interval" days. - If the "day_interval" is 1, it is done daily time_string - the time of day when you want the THEN action triggered - The matching time includes the time zone - The time is specified in a 24-hour format of Hours, minutes, seconds start-date - Date that FileCloud begins checking for the condition end-date - Last date that FileCloud checks for the condition.

Available expression variables: **None.**

Perform an action on the specified date

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>	When the date matches the supplied date and time, the THEN action you configure will be run. date_string - date and time in a 24-hour format yyyy-mm-dd H:i:s

Available expression variables: **None.**

Perform an action periodically

Workflow Condition	Parameters	Description
Perform an action periodically	None. The frequency depends on how you configure the cron or task scheduler frequency.	This requires you to set up one of the following: - cron job - task scheduler

Available expression variables: **None**.

If share has not been accessed for specified days

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.

Parameters

number_of_days (required)
Number of days since a file was modified.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

Workflow Condition	Parameters	Description
If a share has not been accessed for specified days	<pre>{ "share_permission": ["PUBLIC", "PRIVATE"], "number_of_days": "180", }</pre>	This condition will be triggered when a shared file or folder has not been accessed for the specified number of days. NOTE: The only supported action is Delete share. - This is useful for removing shared files that are no longer being used - This check will run once a day number_of_days - required to specify the number of days before the current date that a shared file was accessed. - This will be checked once a day and all files that match this condition will be subject to the THEN action you choose. - For example, if you specify the number of days as 15, all shared files or folders that have not been accessed in the last 15 days will subject to the the THEN action you configure.

Available expression variables: **Share Context variables**.

For instructions on including expressions, see [Using Expressions in IF Conditions](#)

Using Expressions in IF Conditions



Expressions are available in FileCloud beginning in version 23.253.

Many admin workflows allow you to set up custom conditions in workflows based on user, path owner, and share properties. These conditions (referred to as expressions) must be written in regular expression syntax. They greatly expand your ability to customize workflows.

For example, you can expand the IF statement in a workflow to check if a user is a member of a certain group or has a certain policy, or to check if a share is a folder or file share.

Specifically, the additional conditions available for you to include can be based on:

- the user's or the path owner's **group, policy, email (or domain), or name**
- the share owner's **group, policy, email (or domain), or name**, the type of share (**public or private**), and the type of item shared (**folder vs. file**).

The list of available expression variables for each workflow is shown in its wizard. You can view a list of all available variables in the tables under [Guide to expression variables and operators](#), below.

As an example, in the following workflow, which uses the IF condition **If a file is added or updated**, the user and path context variables are supported, but not the share context variables. Below the variables, the available regular expression operators and examples are listed.

Create New Workflow

Expression Support

You can use expressions to add complex conditions based on user and path properties:

User Context Variables

- **_user.groups** - User's group memberships
- **_user.policy** - User's assigned policy
- **_user.email** - User's email address
- **_user.username** - User's username

Path Context Variables

- **_path.owner** - Owner object with user properties
 - **_path.owner.username** - Owner's username
 - **_path.owner.groups** - Owner's group memberships
 - **_path.owner.email** - Owner's email address
 - **_path.owner.policy** - Owner's assigned policy

Operators

- **==, !=** - Equality/Inequality
- **in, not in** - Membership
- **contains, starts with, ends with** - String matching
- **matches** - Pattern matching

Logical Operators

- **and, or, not**

Examples

← Previous

→ Next

✕ Cancel

The examples help you use the proper syntax when adding conditions:

Examples

- **'Admin Group' in _user.groups** - User must be in Admin Group
- **_user.policy == 'AdminPolicy'** - User must have Admin Policy
- **'Admin' in _path.owner.groups** - Path owner must be in Admin group
- **_path.owner.policy == 'AdminPolicy'** - Path owner must have Admin policy
- **_user.username == _path.owner.username** - Current user is the path owner
- **_path.owner.email ends with '@company.com'** - Owner must be from company domain
- **'Manager' in _user.groups and _path.owner.username != 'admin'** - Complex condition example

The variables available depend on the workflow, and not all workflows have variables available.

To create an IF statement with an expression condition

The IF statement we are setting up in this example uses an expression to specify a user's group and policy. The IF statement requires that the user who added or updated a file must also be in the group **TeamMember** and have the policy **Staff**.

1. In the admin portal, go to the Workflows page, and click **Add Workflow**.
2. In the Create New Workflow dialog box, choose an IF condition.

This example uses the condition **If a file is added or updated**.

3. Click **Next**.

4. The only required parameter is **parent_folder_path_string**, so begin by entering it into the **Required Parameters** box.

This example uses the Team Folder **estate documents**.

Create New Workflow

Required Parameters

```
{"parent_folder_path_string":"\\teamfolder\\estate documents"}
```

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

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

use_regex (optional)
Specifies whether the path has a regex format.

exclude (optional)

← Previous → Next × Cancel

Scroll down to **Expression Support** to see the supported context variables. In this case the user and path context variables are supported.

To specify the user's group and policy, use the variables **_user.groups** and **user.policy**.

Create New Workflow

Expression Support

You can use expressions to add complex conditions based on user and path properties:

User Context Variables

- **_user.groups** - User's group memberships
- **_user.policy** - User's assigned policy
- **_user.email** - User's email address
- **_user.username** - User's username

Path Context Variables

- **_path.owner** - Owner object with user properties
 - **_path.owner.username** - Owner's username
 - **_path.owner.groups** - Owner's group memberships
 - **_path.owner.email** - Owner's email address
 - **_path.owner.policy** - Owner's assigned policy

Operators

- **==, !=** - Equality/Inequality
- **in, not in** - Membership
- **contains, starts with, ends with** - String matching
- **matches** - Pattern matching

Logical Operators

- **and, or, not**

Examples

← Previous

→ Next

✕ Cancel

5. Add the variables and values.

Create New Workflow

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "parent_folder_path_string":
  "/teamfolder/estate documents",
  "expression": "'TeamMember' in
_user.groups and _user.policy == 'Staff'"
}
```

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

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

← Previous

→ Next

✕ Cancel

6. Click **Next**.
7. Choose the appropriate THEN action, and add the parameters.
This example uses a THEN action that sends an email to a specific user, and specifies the user's email address.

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "comma_separated_email_id": "jonp@mycompany.com"
}
```

Send email. Admin will be automatically notified.

Provide additional email if required to be notified.

8. Click **Next**, and enter a name for the workflow, then click **Finish**.
The workflow is saved.

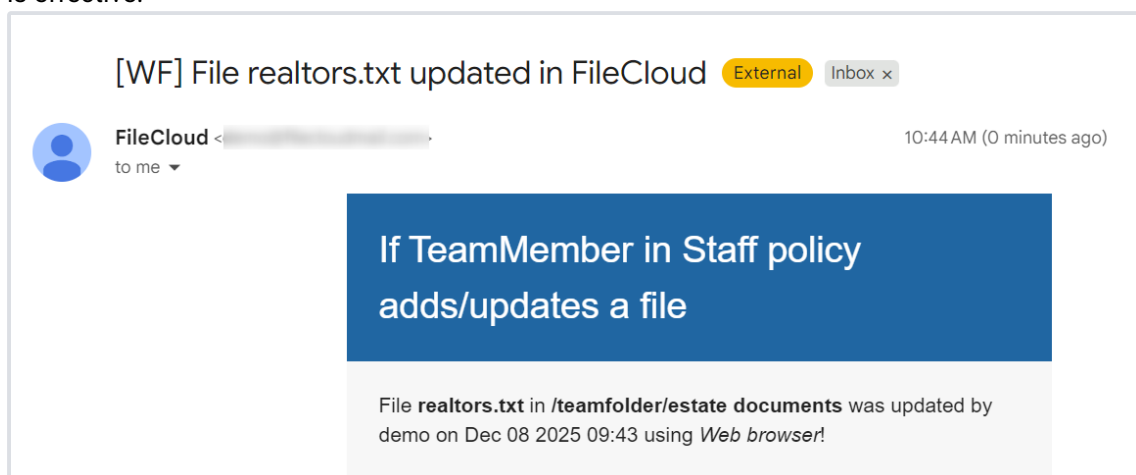
Manage Workflows

Add Workflow

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
If TeamMember in Staff policy adds/updates a file	If a file is added or updated	Notify user(s)	December 8, 2025, 9:55 am	December 8, 2025, 9:43 am	☒	▶ ⌂ ✎ ↺ ✕

9. Test the workflow by having a user in the **TeamMember** group who has the policy **Staff** add or update a file in the Team Folder **estate documents**.

The user specified will receive an email notification similar to the following one if the workflow is effective:



Guide to expression variables and operators

The tables below show the variables and operators supported in regular expressions when used with IF/THEN workflows in FileCloud. For examples using regular expression syntax with these variables and operators, see the wizard for adding each workflow.

User Context Variables	
_user.groups	User's groups
_user.policy	User's policy
_user.email	User's email address
_user.username	User's username
Path Owner Context Variables	
_path.owner.username	Path owner's username
_path.owner.groups	Path owner's groups
_path.owner.email	Path owner's email
_path.owner.policy	Path owner's policy
Share Context Variables	
_share.owner.username	Share owner's username
_share.owner.groups	Share owner's groups
_share.owner.email	Share owner's email
_share.owner.policy	Share owner's policy
_share.public	If share is public, true; if share is not public, false.
_share.private	If share is private, true; if share is not private, false.
_share.is_dir	If this is a folder share, true; if this is a file share, false.

Operators	
==, !=	equal/not equal
in, not in	is a member of/is not a member of
contains, starts with, ends with	string contains, string starts with, string ends with
matches	pattern matches

Logical Operators	
and	
or	
not	

Define a THEN Action



Not all THEN actions are compatible with all IF conditions. Please see the table below for compatible settings.

Once you select an IF Condition, compatible THEN Actions can be selected.

- Actions are performed if the associated Condition is triggered.

Some Actions may require you to specify parameters, such as a specific date or time.

Where do I set up the Action?

When you create a new Workflow, after you select a condition and specify parameters, then you can select an Action.

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 and		Details	Compatible IF conditions
Notify the user that the account may be deactivated soon	None	Notifies the user that the account may be disabled or deleted due to inactivity.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Notify user(s)	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" , "comma_separated_group_name": "Group A,Group B" }</pre>	Sends email notifications to the emails listed and to the users in the groups listed. comma_separated_email_id - email ids in comma separated format comma_separated_group_name: Group names in comma separated format.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date If a new client app connects If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created

Action and		Details	Compatible IF conditions
Send an email	<pre>{ "subject": "Subject of the email", "body": "Body of the email in HTML format.", "is_html": 1, "users": "user1,user2", "groups": "group1,group2", "notify": 0 }</pre>	Sends a customized email to the users and/or groups indicated subject - Subject of the email body - Body of the email is_html (optional) - 1 if the body is in HTML format; 0 if the body is in plain text format. Default is 0. Note: If is_html=1, HTML tags are interpreted and the body of the email is formatted. For example, you can insert tags to make text bold. users (optional) - Comma separated list of users to send the email to. groups (optional) - Comma separated list of groups to send the email to. notify (optional) - 1 to automatically send the email to users impacted by the related action; 0 to not automatically send them the email. Default is 0.	Click to see if conditions If a file is created If a folder is created If a file is updated If a file is deleted If a folder is deleted If a file is downloaded If a comment is added If a file was not modified for specified days If a file is added or updated If the file uploaded is bigger than the expected size If the file uploaded is bigger than the expected size Perform an action periodically at specified time and interval Perform an action on the specified date Perform an action periodically If a new user is created If a user's account is older than If a user's last login is older than If a user's account is near its expiration date

File actions

Action	Parameters	Details	Compatible IF conditions
Copy the file(s) to some location	<pre>{ "target_path": "/usera/ folderb/", "allow_overwrite": 1, "keep_folder_structure": 1 }</pre>	Copies files. target_path - path to copy the file to. - This path must be in the same storage type - Files cannot be copied from managed storage to network shares or vice versa. allow_overwrite - (Added in FileCloud 20.1) Optional. Allow file to overwrite existing files with the same name in the target path. If allow_overwrite is not included, overwrites are allowed. keep_folder_structure (Optional): Keep folder structure while copying files. Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided. The placeholders. %who, %when, %path, %how, %filename are available for this action.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a comment is added

Action	Parameters	Details	Compatible IF conditions
Delete the file(s)	<pre>{ "delete_empty_folders":1, "notify_owner":0, "comma_separated_email_id":"email1@email.com,email2@email.com", "comma_separated_group_name":"Group A,Group B" }</pre>	Deletes matching files. delete_empty_folders (Optional): When files are deleted, delete the parent folder as well if it is empty. notify_owner (Optional): When the files are deleted, send an email to the owners. comma_separated_email_id (Optional): Email ids in comma separated format. comma_separated_group_name (Optional): Group names in comma separated format.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a comment is added

Action	Parameters	Details	Compatible IF conditions
Move the file(s) to some location	<pre>{ "target_path": "/usera/ folderb/", "allow_overwrite": 1, "keep_folder_structure": 1 }</pre>	Moves files. target_path - Path to the new file location (where it should be moved). - This path must be in the same storage type - Files cannot be moved from managed storage to network shares or vice versa. allow_overwrite - (Added in FileCloud 20.1) Optional. Allow file to overwrite existing files with the same name in the target path. If allow_overwrite is not included, overwrites are allowed. keep_folder_structure (Optional): Keep folder structure while moving files. Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided. The placeholders. %who, %when, %path, %how, %filename are available for this action. ⚠ Currently, if creation/update of a file in FileCloud via WOPI triggers a move file workflow, the move fails.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is deleted If a comment is added
Release locks (added in FileCloud 22.1)	<pre>{ "days": 7 }</pre>	Releases locks on files and folders. days - Number of days after a lock was created on a file or folder to release it.	Click to see if conditions Perform an action periodically at specified time and interval Perform an action on the specified date Perform an action periodically If a user's create date is older than

Action	Parameters	Details	Compatible IF conditions
Verify file integrity and generate admin alert on mismatch	<pre>{ "ignore_file_size_in_mb": 10 }</pre>	Attempts to identify the file type based on its content and checks if it matches the extension. If the file type does not match, then generate admin portal alert. Optional ignore_file_size_in_mb: - Do not scan files larger than this limit specified in megabytes. Note: By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check. However, You may add additional allowable extensions for text files by adding the setting TONIDO_TEXT_FILE_EXTENSIONS to your cloudconfig file. See File Content Heuristic Engine.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deletedIf a comment is added

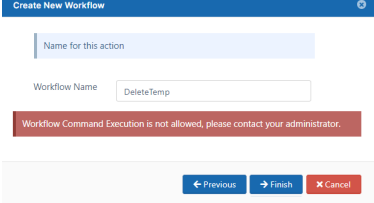
Action	Parameters	Details	Compatible IF conditions
Verify file integrity and delete on mismatch	<pre>{ "ignore_file_size_in_mb": 10 }</pre>	Attempts to identify file type based on its content and checks if it matches its mime type. - A MIME type is a string identifier composed of two parts: a "type" and a "subtype". - If the file type does not match, then - the latest version is deleted - users listed in the parameter are notified Optional ignore_file_size_in_mb: - Do not scan files larger than this limit specified in megabytes. Note: By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check. However, You may add additional allowable extensions for text files by adding the setting TONIDO_TEXT_FILE_EXTENSIONS to your cloudconfig file. See File Content Heuristic Engine.	Click to see If conditions - If a file is created - If a file is updated - If a file is deleted - If a file is downloaded - If a file was not modified for specified days - If a file is added or updated - If a file uploaded is bigger than expected size - If a file downloaded is bigger than expected size - If a folder is created - If a folder is deleted - If a comment is added

Reporting

Action	Parameters	Details	Compatible IF conditions
Run a report	<pre>{ "report_name": "my_report", "comma_separated_email_id": "a@x.com,b@y.com", "comma_separated_group_name": "Group A,Group B" }</pre>	Opens a saved report, runs it, and then sends the results in email. 💡 This action requires you to have already created the report from the Admin dashboard. Create a Custom Report report_name: Name of the report to run. The report must already be created in the reports section and that exact report name must be provided here. comma_separated_email_id: Comma separated email ids to be notified after report is run comma_separated_group_name (Optional): Group names in comma separated format.	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date If a comment is added Perform an action periodically at specified time and interval Perform an action on the specified date Perform an action periodically

Action	Parameters	Details	Compatible IF conditions
Generate an email report	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" , "comma_separated_group_name": "Group A,Group B" }</pre>	Sends an email to the specified addresses with information about the users matching the criteria. comma_separated_email_id - email ids in comma separated format comma_separated_group_name: Group names in comma separated format.	Click to see If conditions If a user's last login is older than . . . If a new user is created (if the user account was created by the user; not applicable if the user account was created by an admin) If a user's create date is older than If a user's account is near its expiration date

Running commands

Action	Parameters	Details	Compatible IF conditions
Execute a command	<pre>{ "command_line": "rm -rf / tmp/scratch" }</pre>	Executes the command line. command_line: - Command line syntax to be executed. Admin is notified after the command runs. The following placeholders are available: %who, %when, %path, %how, %filename. See Set Advanced Workflow Options. The placeholders. %who, %when, %path, %how, %filename are available for this action. Beginning in FileCloud 23.1, by default, the Execute a command action is not available for admin users. If an admin user selects the action and tries to save the workflow, the following warning appears:  To enable admin users to choose the Execute a command option, add: 1. Open cloudconfig.php : Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php Linux Location: /var/www/config/cloudconfig.php 2. Add the following:	Click to see If conditions If a file is created If a file is updated If a file is deleted If a file is downloaded If a file was not modified for specified days If a file is added or updated If a file uploaded is bigger than expected size If a file downloaded is bigger than expected size If a folder is created If a folder is deleted If a user's last login is older than . . . If a new user is created If a user's create date is older than If a 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
		<pre>define(" TONIDOCL OUD_ALLO W_ADMIN_ WORKFLOW _COMMAND _EXECUTI ON",1);</pre>	

Modifying users

Action	Parameters	Details	Compatible IF conditions
Disable user account	<pre>{ "comma_separated_email_id":"xyz@a.com,abc@b.com" , "comma_separated_group_name":"Group A,Group B", "donot_email_user": 0 }</pre>	Disables the user account and then sends an email with information about the action performed. comma_separated_email_id - email IDs in comma separated format comma_separated_group_name: Group names in comma separated format. donot_email_user (optional): Do not send email to the user affected (1 or 0). Default 0. Note: To customize the email sent to the user, go to Customization > Email Templates and edit the template Workflow Auto Disable Account Email Template.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Action	Parameters	Details	Compatible IF conditions
Delete user account	<pre>{ "comma_separated_email_id": "xyz@a.com,abc@b.com" , "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }</pre>	Deletes the user account and then sends an email with information about the action performed. comma_separated_email_id - email IDs in comma separated format comma_separated_group_name: Group names in comma separated format. donot_email_user (optional): Do not send email to user affected (1 or 0). Default 0.	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Change user status	<pre>{ "user_status": "USER_ACCOUNT_LIMITED_ACCESS", "mark_as_verified": 0, "comma_separated_email_id": "xyz@a.com,abc@b.com", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }</pre>	user_account_type - type of account. You must use one of the following values: • USER_ACCOUNT_DISABLED_ACCESS • USER_ACCOUNT_FULL_ACCESS • USER_ACCOUNT_GUEST_ACCESS • USER_ACCOUNT_LIMITED_ACCESS (external access) mark_as_verified (optional) - marks the account as verified, so that the user can log in immediately without waiting for the admin to send the verification email. comma_separated_email_id - email IDs in comma separated format comma_separated_group_name: Group names in comma separated format. donot_email_user (optional) - prevents an email from being sent to the user affected when the status is changed • 1 = Does not send an email • 0 = Sends an email • If nothing is specified, the default is 0	Click to see If conditions If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Action	Parameters	Details	Compatible IF conditions
Set user group	<pre>{ "group_name": "Group1,Group2" }</pre>	Assigns user to groups. group_name - Comma separated list of groups to assign user to.	If a new user is created If a user's create date is older than If a user's account is near its expiration date
Set user policy	<pre>{ "policy_name": "SamplePolicyName", "comma_separated_email_id": "", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }</pre>	Sends an email notification to the listed users that the user's policy was set as the specified policy policy_name - Name of policy to set comma_separated_email_id - email ids in comma separated format comma_separated_group_name: Group names in comma separated format. donot_email_user 0 (default) send the emails 1 do not send the emails	If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date
Set user properties	<pre>{ "policy_name": "SamplePolicyName", "user_status": "USER_ACCOUNT_LIMITED_ACCESS", "comma_separated_email_id": "", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 }</pre>	Sends an email notification to the listed users that the user's policy was set as specified and the user access was set as specified policy_name: Name of policy to set. user_status (optional): User status to set. (USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS (external access)) comma_separated_email_id (optional): Comma separated emails to notify of workflow action. comma_separated_group_name (Optional): Group names in comma separated format. donot_email_user (optional): Set to 1 to prevent system from notifying user.	If a user's last login is older than . . . If a new user is created If a user's create date is older than If a user's account is near its expiration date

Share actions

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

Device actions

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

Edit a Workflow



It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and set up correct workflows.

Administrators can edit workflows to change the name or parameters of the conditions and action.

To edit, click on the Edit button; to delete, click on the Delete button.

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		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		
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		

Update Workflow

Workflow Name

Not Modified Run Report

IF Condition ..

If file was not modified for specified days

Required Parameters

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

THEN Action ..

Run a report

Required Parameters

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

Execute

Update

Cancel

Run a Workflow



It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

Administrators can run a workflow manually from the **Manage Workflows** screen.

To run a workflow manually:

1. In the FileCloud admin portal's navigation panel, click **Workflows**.

2. In the Manage Workflows screen, in the row for the workflow you want to run, click the first arrow under **Actions**.

Manage Workflows

Workflow Add Workflow

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Enabled	Actions
New Client	If any new client app connects	Notify user(s)	Never	Never		

The following confirmation box opens.

Workflow - New Client

You are about to execute this workflow. Are you sure you want to proceed?

Confirm Cancel

3. Click **Confirm**.

A screen notification confirms that the workflow ran successfully.

Set Advanced Workflow Options



It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

Administrators can create and run more advanced scenarios., such as:

- regular expression in path matching
- the ability to pass additional, runtime-resolved data between conditions and actions

What scenario do you want to use?

Regular Expressions and Path Matching

You can enable regular expression matching in workflows by setting the **use_regex** parameter to "1" in the condition definition. This is an optional parameter and by default is "0" (don't use regular expressions - use strict match instead). If regular expressions are enabled you must provide a valid regular expression pattern as the **parent_folder_path_string** value. This pattern is used in the condition resolution process to find all matching paths (files / folders).

Regular expressions are supported by the following workflow conditions:

- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated

Parameters definition - example

Strict match

```
{
  "parent_folder_path_string":"/userid/somepath",
}
```

or

```
{
  "parent_folder_path_string":"/userid/somepath",
  "use_regex":"0"
}
```

Regular expression

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

Usage - Example

For simplicity sake assume that Administrator wants to send email notifications whenever someone downloads a file from a given location. The following example shows the difference between *strict match* and *regular expression match*

Strict match

Parameters are defined as follows:

```
{
  "parent_folder_path_string":"/userA/downloads",
}
```

For such defined condition action will be triggered whenever a files is downloaded directly from the "/userA/downloads" directory and only from this one.

Regular expression

In this case the definition might look something like:

```
{
  "parent_folder_path_string": "~/.*/downloads~",
  "use_regex": "1"
}
```

For this condition action will be triggered for **all** directories that match the /user/download format, i.e. /userA/downloads, /userB/downloads, etc. This is a huge change that enables Administrators to define much more universal workflow scenarios.



Important

Regular expression patterns aren't validated for correctness. Please double check them, especially when dealing with the data-changing actions (i.e. delete files / move files, etc.).



RegEx Patterns

Regular expression definition has to start and end with one of the following characters:

'/', '~', '@', ',', '%', ''

We strongly advise against the / usage as it adds confusion to the pattern definition.

Reversed Path Matching

The **Exclude** parameter enables the "reversed" path matching. That means that the specified action will be triggered for all files / folders whose path **doesn't match**. It's another huge change that allows administrators to define a new set of workflow. This is a very flexible and 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 are available in Workflows.

The runtime resolved parameters can be specified in the following IF conditions:

- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated
- if the file updated is bigger than the expected size
- if the file downloaded is bigger than the expected size

and then used in all compatible THEN actions.

Currently FileCloud supports the following placeholders only for file/folder related conditions.

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

If the selected IF condition is able to implement runtime resolved parameters they are listed in the THEN action dialog box.

Create New Workflow



Provide the required parameters for the action to be executed

Required Parameters

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

Execute commandline. Do not use to run scripts with long execution times.

command_line: Command line syntax to be executed. Admin will be notified after the command is run

```
{
  "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

In this section:

Admin Approval Required Workflow

This workflow recipe blocks the connection of a new app or device until it is approved by an administrator.

- When a new app or device tries to connect to FileCloud, the action is unblocked **ONLY** after admin approval.
- In the Admin Portal, you can see the devices in **BLOCKED** status, awaiting **ADMIN** approval.

To create a workflow that requires admin approval for all clients:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition "**If any new client app connects**"

Create New Workflow

×

Select the condition

IF Condition .. If any new client app connects

→ Next × Cancel

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 { "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

6. Click Next, to give the THEN action

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

Block the device for admin approval

← Previous

→ Next

✕ Cancel

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

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

{ "parameter name": "value" }

Block the device and require admin to approve the device.
No parameters are required for this action.

← Previous

→ Next

✕ Cancel

8. Click on Next, to give workflow name

Create New Workflow

×

Name for this action

Workflow Name

Require admin approval for all clients

← Previous

→ Finish

✕ Cancel

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.

HOME

Dashboard

USERS/GROUPS

Users

Groups

Admins NEW

MANAGE

Team Folders

Network Folders

User Shares

Folder Permissions

Notifications

DEVICES

Devices

Manage Devices

Filter

Username, Device name/details

Access Filter : All

Message

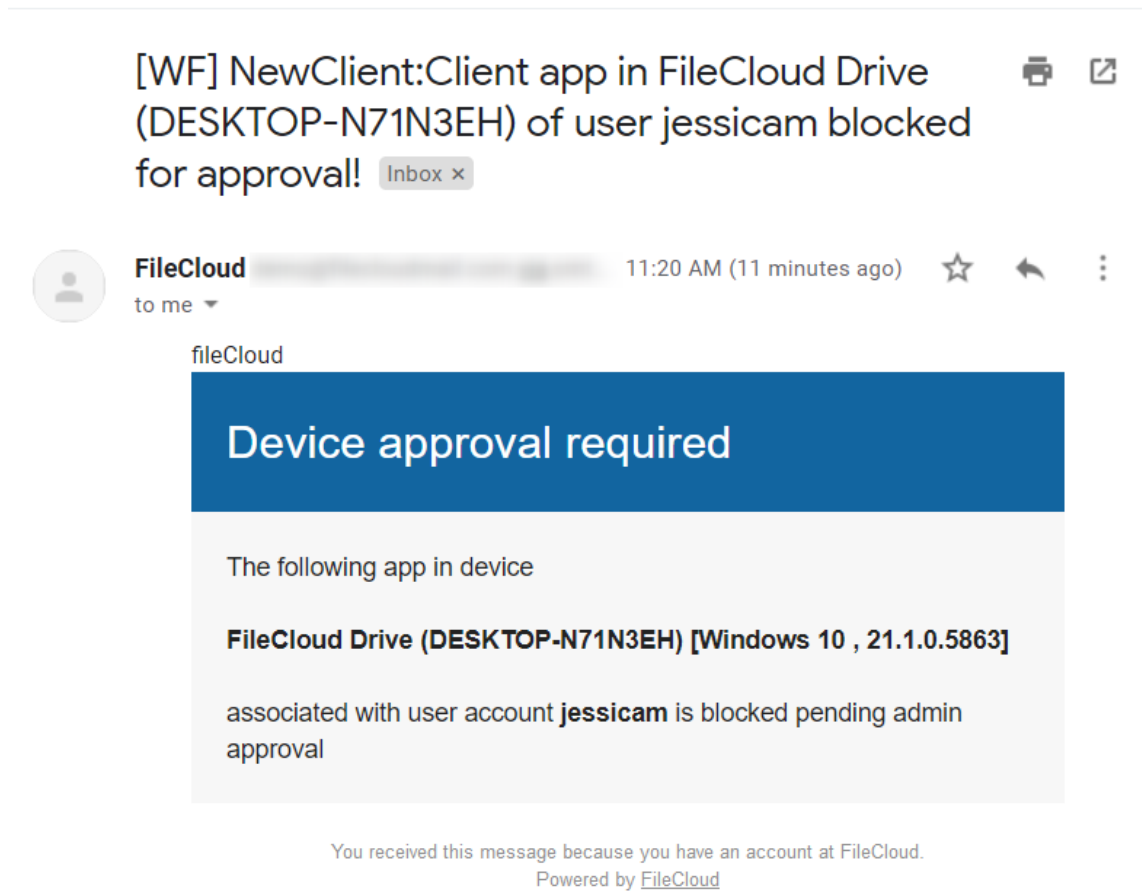
Get Logs

Command

Delete

	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)	Today at 10:20 AM from 127.0.0.1	Needs Admin Approval	Blocked	1	

10. An email will be sent to the user trying to connect to FileCloud notifying the user that the device needs to be approved by the admin.



Create Report and Send Email Workflow

This workflow recipe creates a specific report and sends the result to specified emails once a day.

- The email can be configured to be sent at a specific time in the day, and the day interval can be set to daily.

To create a workflow that generates a specific report and sends the result to specified emails:

1. Log in to the admin portal
2. In the navigation panel, click **Reports**.
3. Click **Add Report**.
4. In **Select Report to Create**, choose **Get user login report**.

Create New Report

Select the report from the list

Select Report to Create

Get user login report

→ Next

✕ Cancel

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

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.

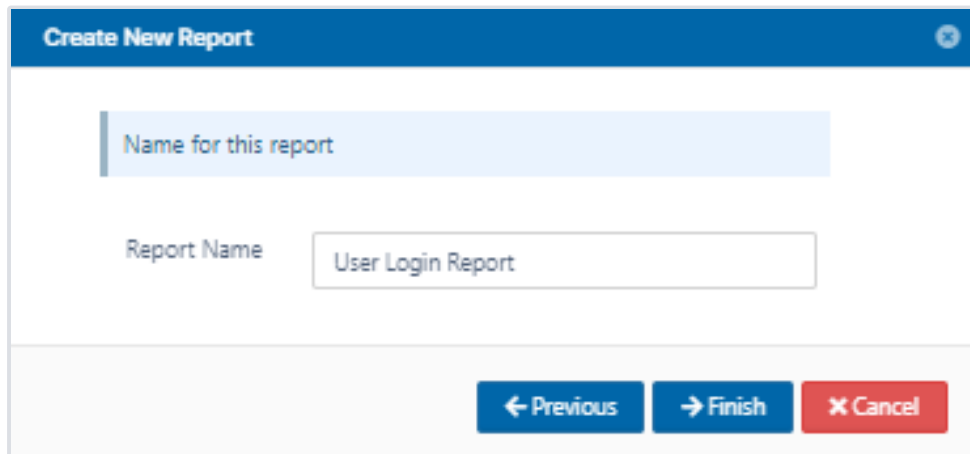
```
{  "from_date" : "2020-01-01 00:00:00",  "to_date" : "2020-01-01 23:59:59",  "last_number_of_hours" : "24",}
```

← Previous

→ Next

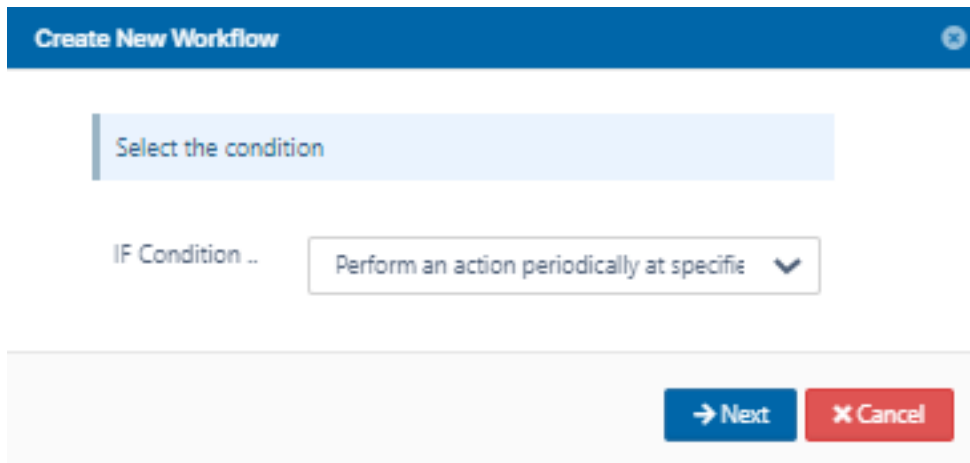
✕ Cancel

6. Save the report with an appropriate name, and click **Finish**.



The 'Create New Report' dialog box features a blue header with the title and a close button. Below the header, there is a light blue highlighted section labeled 'Name for this report'. Underneath, the 'Report Name' is set to 'User Login Report' in a text input field. At the bottom, there are three buttons: 'Previous' (blue with a left arrow), 'Finish' (blue with a right arrow), and 'Cancel' (red with an 'X').

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 'Create New Workflow' dialog box has a blue header with the title and a close button. Below the header, there is a light blue highlighted section labeled 'Select the condition'. Underneath, the 'IF Condition ..' is set to 'Perform an action periodically at specific' in a dropdown menu. At the bottom, there are two buttons: 'Next' (blue with a right arrow) and 'Cancel' (red with an 'X').

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

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

This condition will be triggered when the current time matches the supplied time.

Parameters

day_interval (required)

Days interval (For daily operation, specify this value to be 1).

time_string (optional)

Time in format H:i:s (If not specified, it will run at 00:00:00).

start_date (optional)

Start date in format yyyy-mm-dd (If not specified, it will start from today).

end_date (optional)

End date in format yyyy-mm-dd (If not specified, it will run indefinitely).

Configuration Example

```
{
  "day_interval": 7,
```

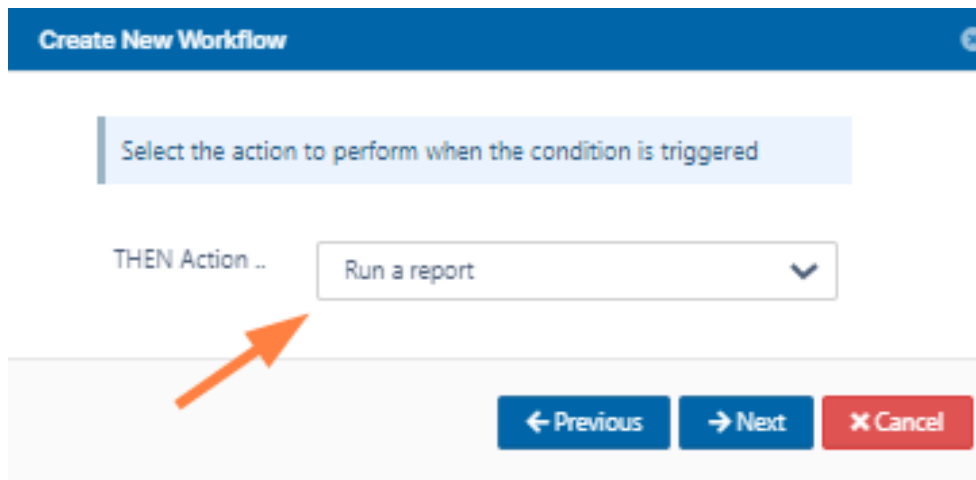
← Previous

→ Next

✕ Cancel

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

Workflows - IFTTT – 445



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 or group 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 via email.
Admin will be automatically notified.

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: Email ids in comma-separated format. All email ids will be notified.

comma_separated_group_name: Group names in comma-separated format. All users in the group will be notified.

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

← Previous

→ Next

✕ Cancel

12. Save the workflow with an appropriate name.

Create New Workflow
ⓘ

Name for this action

Workflow Name

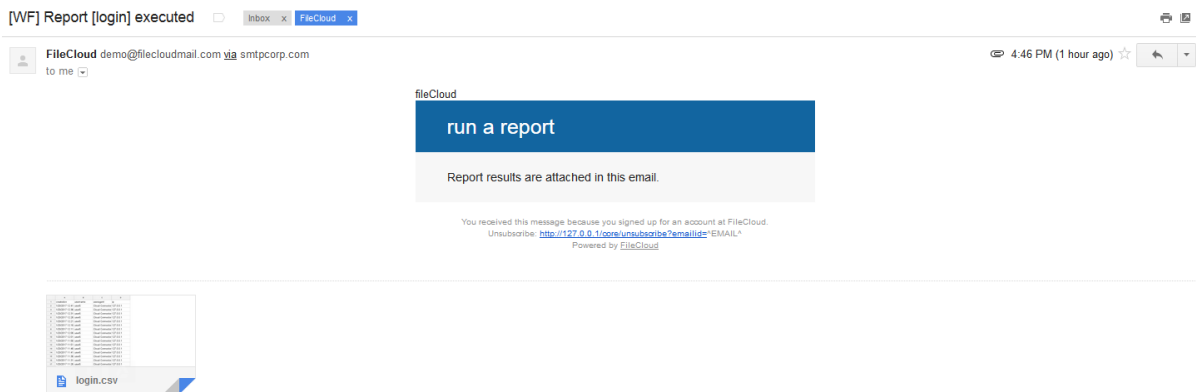
Run user login report

← Previous

→ Finish

✕ Cancel

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



Similar workflows can be created to run reports with THEN conditions like:

- **Perform an action on the specified date**
- **Perform an action periodically**

Detect and Delete Inactive Files Workflow

This workflow recipe deletes all unused files.

- The workflow checks the number of days a file was unused and deletes those files.
- You can provide a set of email ID's to send the generated report to.

To create a workflow that detects and deletes inactive files:

1. Log in to the admin portal.
2. Click **Workflow** on the left navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified for specified days**, and click **Next**.

Create New Workflow

Select the condition

IF Condition .. If file was not modified/created in 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.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

trigger_date: The **MODIFIED_DATE** option is only applicable for files.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

number_of_days (required)
Number of days since a file was modified.

skip_recently_accessed (optional)
When TRUE, files viewed or downloaded within

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)
Exclude items matching the specified path/pattern from the action.

trigger_date (optional)
Defines which file date to use when evaluating the condition (BOTH, MODIFIED_DATE, CREATED_DATE).

expression (optional)

← Previous → Next ✕ Cancel

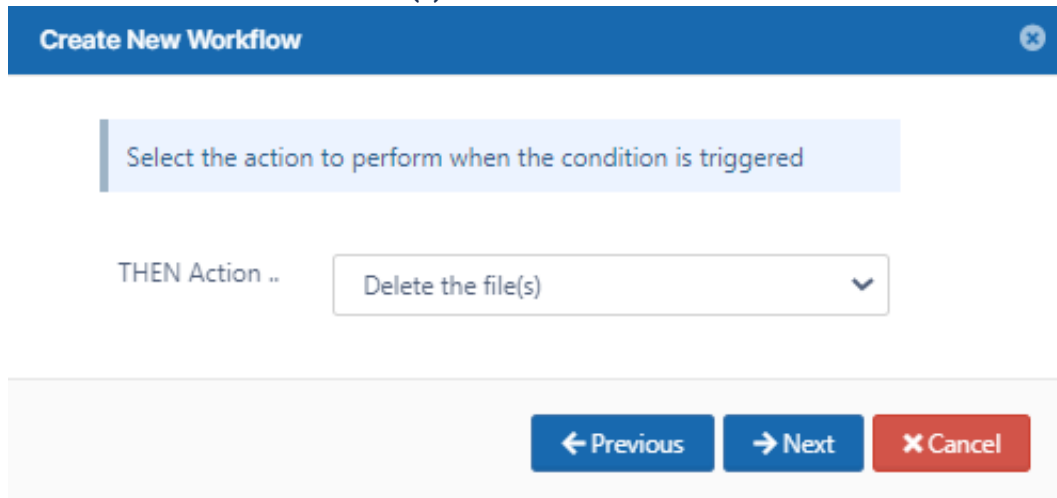
For example:

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

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

6. Click **Next**.

- Set **THEN Action** to **Delete the file(s)**.



Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

Delete the file(s)

← Previous → Next × Cancel

- 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.

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. All email ids will be notified.

comma_separated_group_name (Optional): Group names in comma separated format. All users in the group will be notified.

```
{
  "delete_empty_folders":1,
  "notify_owner":0,

  "comma_separated_email_id":"email1@email.com,email12@email.com",
  "comma_separated_group_name":"Group A,Group B"
}
```

← Previous

→ Next

✕ Cancel

For example:

```
{
  "delete_empty_folders":true
}
```

}

9. Click **Next**.
10. Enter a **Workflow Name** and click **Finish**.

Detect and Disable Inactive Users Workflow

This workflow recipe disables a user when the user is no longer active and notifies the user through email once the account is deactivated.

- The last login date of the user is used to know if the user is Active or Inactive.
- You can avoid looking at users who have not begun using FileCloud.
- You provide the email ID's to which a report of disabled users is sent.

To create a workflow that detects and disables inactive users:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Click the **Add Workflow** button
4. Set the If Condition " **If a user's last login is older than..** "

5. Enter the required parameters in the given format.

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

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 based on the day interval configured.

Parameters

last_login_days_ago (required)

Number of days since last login.

user_account_type (required)

Type of user account (USER_ACCOUNT_ANY, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS, USER_ACCOUNT_DISABLED).

day_interval (required)

Days interval (For daily operation, specify this value to be 1).

skip_users_not_logged_in (optional)

Skip users who have never logged in to the system.

skip_admin_users (optional)

Skip promoted admins. Default is true.

expression (optional)

Additional condition using Expression Language syntax. Supports user context variables.

- 6.

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 ..

Disable user account

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.c  
om,hr@management.com",
```



Disable user and send email after performing this action.

comma_separated_email_id: Email ids in comma separated format as shown below

comma_separated_group_name (optional): Group names in comma separated format. All email ids will be notified.

donot_email_user (optional): Do not send email to user affected (1 or 0). Default 0

```
{  
  
  "comma_separated_email_id": "xyz@a.com,abc@b.com",  
  "comma_separated_group_name": "Group A,Group B",  
  "donot_email_user": 0  
}
```

← Previous

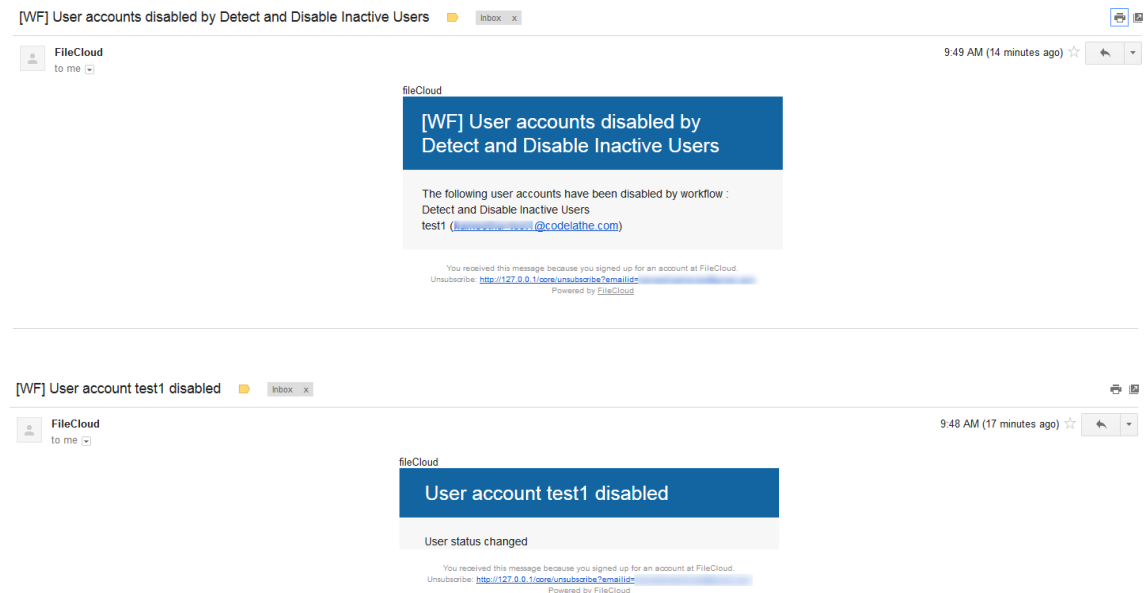
→ Next

× Cancel

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



9. The user accounts are disabled and the notifications are sent once the workflow is executed.



[WF] User accounts disabled by Detect and Disable Inactive Users

The following user accounts have been disabled by workflow :
Detect and Disable Inactive Users
test1 (test1@codeatthe.com)

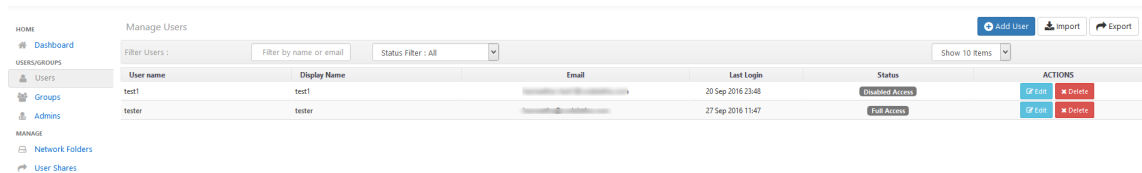
You received this message because you signed up for an account at FileCloud.
Unsubscribe: <http://127.0.0.1/core/unsubscribe?emailid=...>
Powered by FileCloud

[WF] User account test1 disabled

User status changed

You received this message because you signed up for an account at FileCloud.
Unsubscribe: <http://127.0.0.1/core/unsubscribe?emailid=...>
Powered by FileCloud

10. Go to the users list to confirm that the users are disabled.



User name	Display Name	Email	Last Login	Status	ACTIONS
test1	test1	test1@codeatthe.com	20 Sep 2016 23:48	Disabled Account	Edit Delete
tester	tester	tester@codeatthe.com	27 Sep 2016 11:47	Full Access	Edit Delete

Detect and Generate Inactive File List Workflow

This workflow recipe sends an email report with a list of inactive files.

- The workflow checks the number of days a file was unused and generates a report.
- You can provide a set of email IDs the generated report will be emailed to.

To create a workflow that detects and generates a list of inactive files:

1. Log in to the admin portal.
2. Click **Workflow** in the navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified/created for specified days**, and click **Next**.

5. Enter the parameters in the given format.

Path of the folder as shown in the file browser.

number_of_days (required)
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)
Exclude items matching the specified path/pattern from the action.

trigger_date (optional)
Defines which file date to use when evaluating the condition (BOTH, MODIFIED_DATE, CREATED_DATE).

expression (optional)
Additional condition using Expression Language

← Previous
→ Next
✕ Cancel

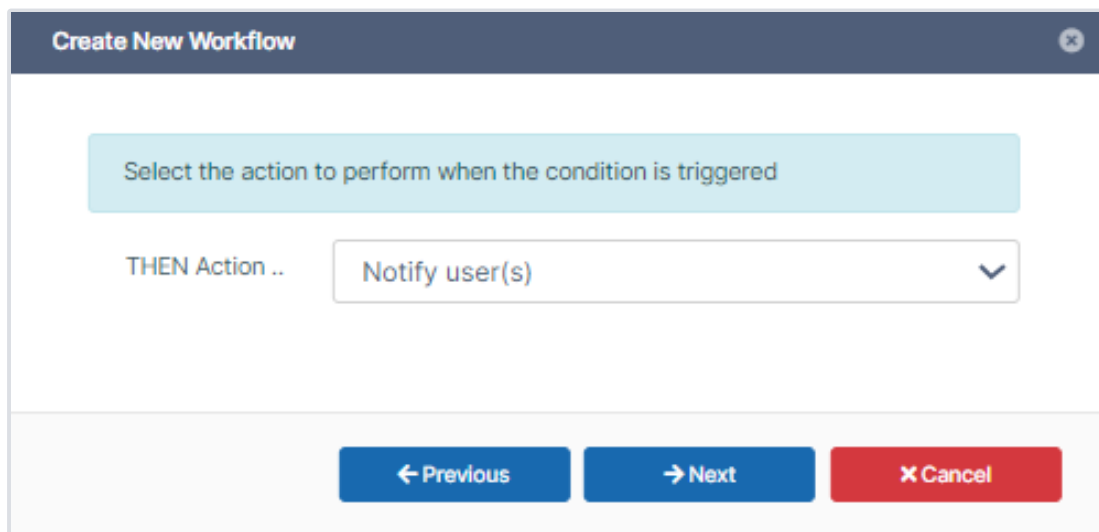
For example:

```
{
  "parent_folder_path_string": "/jenniferp",
  "number_of_days": 15,
  "skip_recently_accessed": 1,
  "exclude_recyclebin": 1,
  "exclude": ".*secret.*",
  "trigger_date": "BOTH",
}
```

Note: This workflow applies only to Managed Storage and not to Network Folders.

To identify a FileCloud specific path for a folder please refer to [Identifying a FileCloud Specific Path](#).

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



The image shows a 'Create New Workflow' dialog box. At the top is a dark blue header with the title 'Create New Workflow' and a close button. Below the header is a light blue instruction box that says 'Select the action to perform when the condition is triggered'. Underneath this is a label 'THEN Action ..' followed by a dropdown menu. The dropdown menu is open, showing 'Notify user(s)' as the selected option. At the bottom of the dialog are three buttons: '← Previous' (blue), '→ Next' (blue), and '✕ Cancel' (red).

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

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

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "comma_separated_email_id": "lynnep@exam
  ple.com",
}
```

Send email. Admin will be automatically notified.
Provide additional email if required to be notified.

comma_separated_email_id: Email ids in comma-separated format. All email ids will be notified.
comma_separated_group_name: Group names in comma-separated format. All users in the group will be notified.

```
{
  "comma_separated_email_id": "xyz@a.com, abc@b.com",
  "comma_separated_group_name": "Group A, Group B"
}
```

← Previous

→ Next

✕ Cancel

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

Create New Workflow
✕

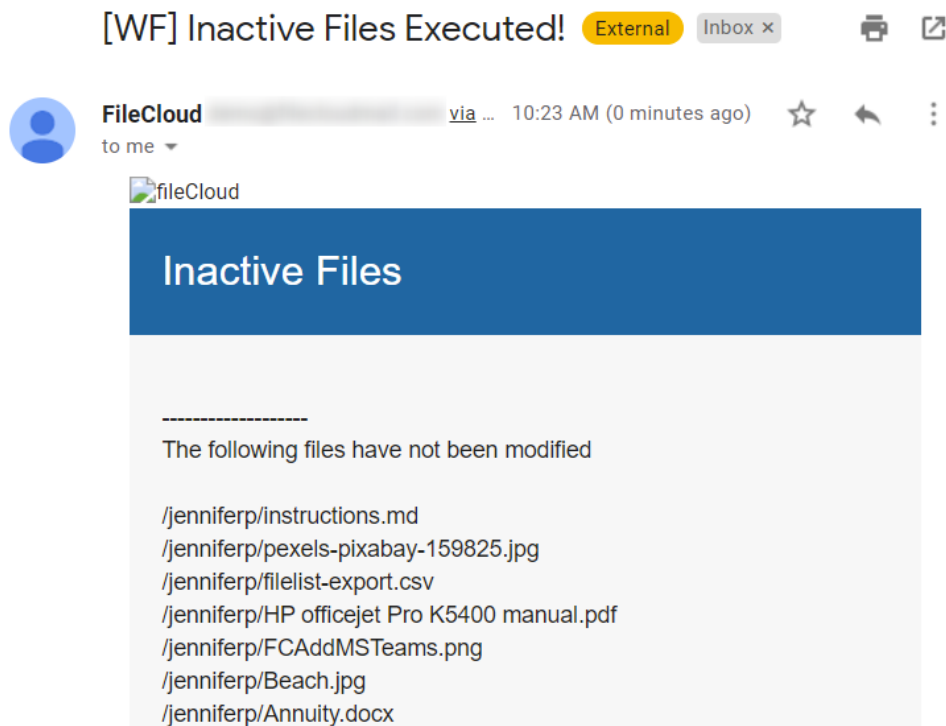
Name for this action

Workflow Name

Generate a report of inactive files

← 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

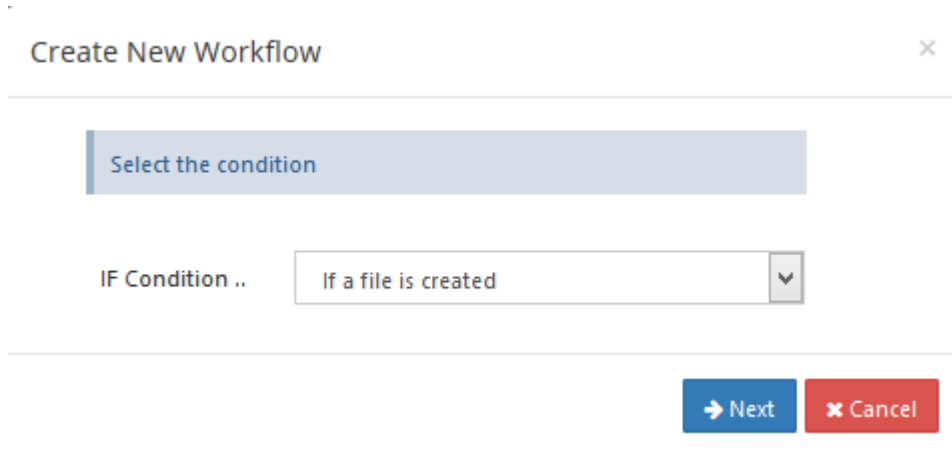
This workflow recipe creates an ALERT notification when a file is created or uploaded to FileCloud with a signature mismatch.

- 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**.



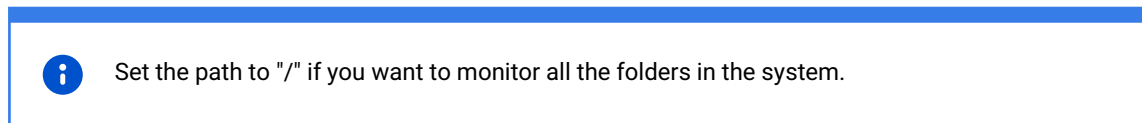
Create New Workflow

Select the condition

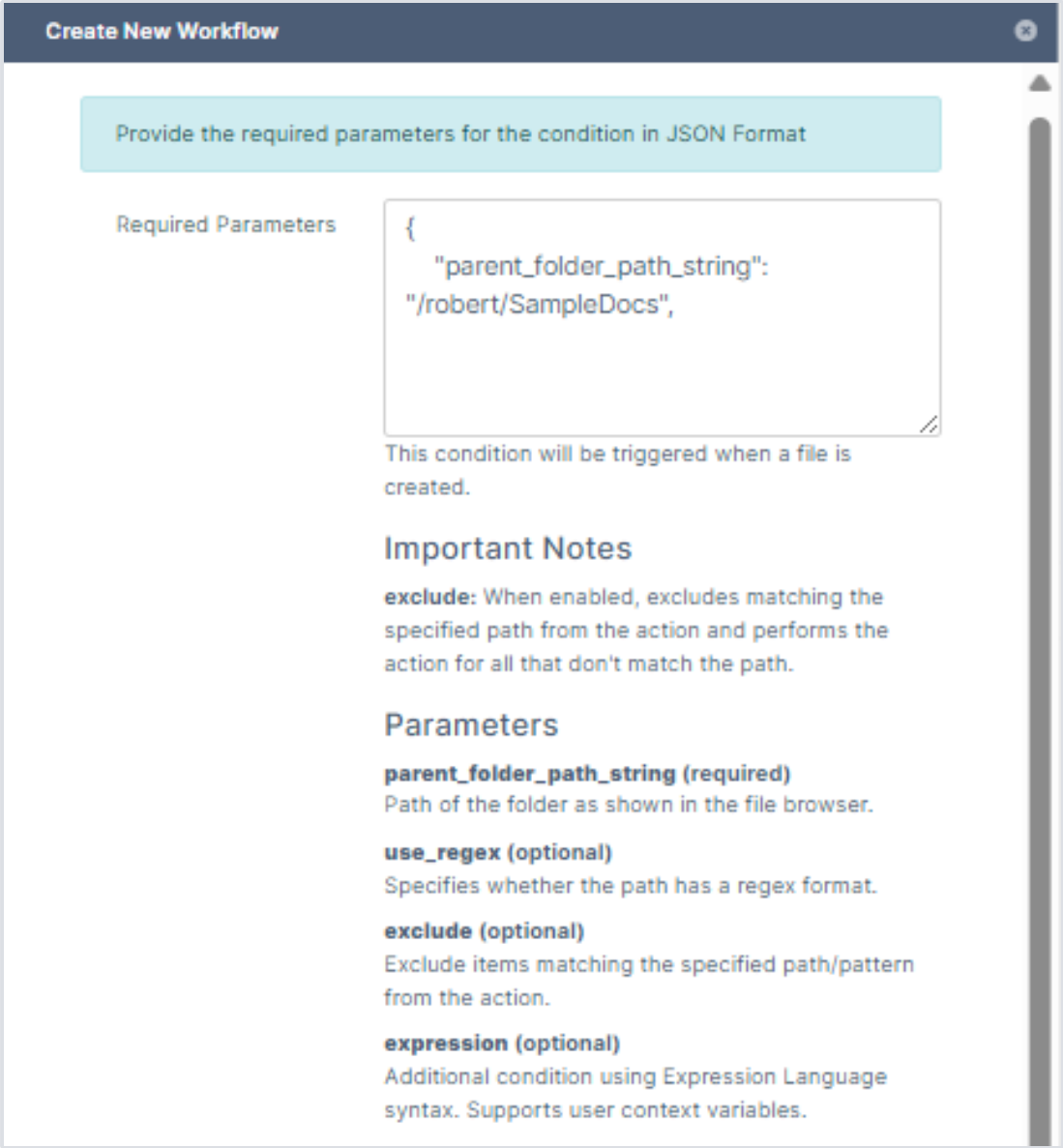
IF Condition .. If a file is created

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](#).



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

7. 

Click **Next**, and set **Then Action** to **Verify file integrity and generate admin alert on mismatch**

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

Verify file integrity and generate admin alert on I

← Previous

→ Next

✕ Cancel

8. Click **Next**, and **enter the size limit of files to scan**.

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 mime type.

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

9. Click **Next**, and give **a name to this workflow**.

Create New Workflow

Name for this action

Workflow Name

Detect and Notify files that fail signature

Previous

Finish

Cancel

Once this workflow is set, the Admin receives alert messages in the **Alerts** page.

Manage Alerts				
Filter Alert Level		All	Remove Clear All	
	Date	Severity	Description	ACTIONS
☐	2016-Sep-26 02:26:58 AM	Warning	[Detect and notify signature variance] File /npriya/fioschk/doc scr3.klx created by npriya failed signature check. The content is not matching the file type extension.	More
☐	2016-Sep-02 17:38:16 PM	Critical	ERROR 2016-09-02 17:38:16 1 Call to a member function getParametersForAction() on a non-object /var/www/core/framework/workflowcontroller.class.php:537	More
☐	2016-Sep-02 17:37:19 PM	Critical	ERROR 2016-09-02 17:37:19 1 Call to a member function getParametersForAction() on a non-object /var/www/core/framework/workflowcontroller.class.php:537	More
☐	2016-Aug-04 10:55:11 AM	Warning	[deletebadfile] File /anisad/upload/ss.jpg created by anisad failed signature check. The content is not matching the file type extension. File version deleted	More
☐	2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg_128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More
☐	2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg_800_xx_600 created by hameethatest failed signature check. The content is not matching the file type extension.	More
☐	2016-Aug-02 05:40:18 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/monalisa.jpg_180_xx_180 created by hameethatest failed signature check. The content is not matching the file type extension.	More
☐	2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter1.doc_180_xx_180 created by hameethatest failed signature check. The content is not matching the file type extension.	More
☐	2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter1.doc_128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More
☐	2016-Aug-02 05:40:17 AM	Warning	[file verifier] File /EXTERNAL/Amazon S3 test bucket/fff_cloud/letter.doc_128_xx_128 created by hameethatest failed signature check. The content is not matching the file type extension.	More

Detect and Notify Inactive Users Workflow

This workflow recipe sends an email report with a list of all the inactive users.

- The last login date of the user is used to determine if the user is Active or Inactive
- You can avoid looking at users who have not begun using FileCloud
- You provide a set of email ID's to which the generated report will be mailed

To create a workflow that sends an email report with a list of all the inactive users:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition **If a user's last login is older than..**, and click **Next**.

Create New Workflow

Select the condition

IF Condition ..

If a user's last login is older than ..

→ 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 based on the day interval configured.

Parameters

last_login_days_ago (required)
Number of days since last login.

user_account_type (required)
Type of user account (USER_ACCOUNT_ANY, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS, USER_ACCOUNT_DISABLED).

day_interval (required)
Days interval (For daily operation, specify this value to be 1).

skip_users_not_logged_in (optional)
Skip users who have never logged in to the system.

skip_admin_users (optional)
Skip promoted admins. Default is true.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

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 ..

Generate an email report

▼

← 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": "admin@abc.c
om,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_group_name (optional): Group names in comma separated format. All email ids will be notified.

```
{
  "comma_separated_email_id": "xyz@a.com,abc@b.com",
  "comma_separated_group_name": "Group A,Group B"
}
```

← Previous

→ Next

✕ Cancel

8.

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

Notify on File Upload Workflow

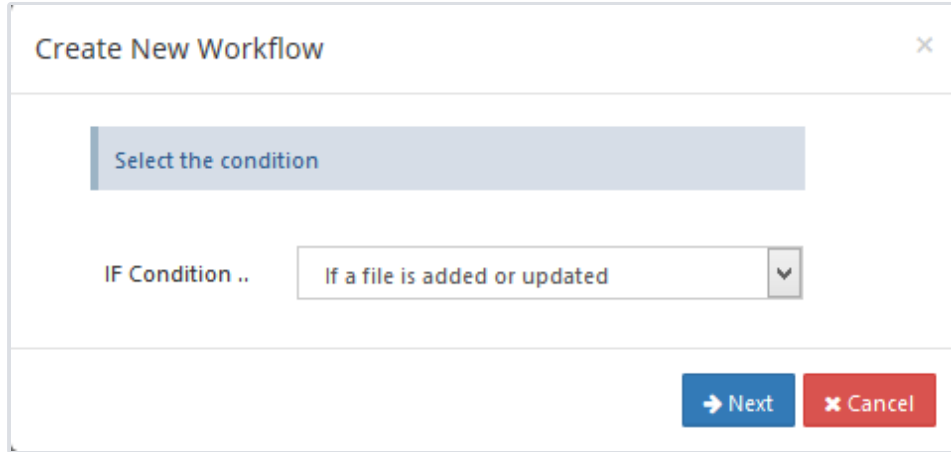
This workflow recipe sends an email notification when a file is created or uploaded to FileCloud.

- 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](#).



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.

Important Notes

exclude: When enabled, excludes matching the specified path from the action and performs the action for all that don't match the path.

Parameters

parent_folder_path_string (required)
Path of the folder as shown in the file browser.

use_regex (optional)
Specifies whether the path has a regex format.

exclude (optional)
Exclude items matching the specified path/pattern from the action.

expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

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

Create New Workflow

Select the action to perform when the condition is triggered

THEN Action ..

Notify user(s)

← Previous

→ Next

✕ Cancel

7. Enter the Required parameters in the given format

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"
}
```

Send email. Enter emails to be notified.

comma_separated_email_id: Email ids in comma-separated format. All email ids will be notified.

comma_separated_group_name: Group names in comma-separated format. All users in the group will be notified.

```
{
  "comma_separated_email_id": "xyz@a.com,abc@b.com",
  "comma_separated_group_name": "Group A,Group B"
}
```

← Previous

→ Next

✕ Cancel

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

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

Workflows - IFTTT – 475

Create New Workflow

Name for this action

Workflow Name

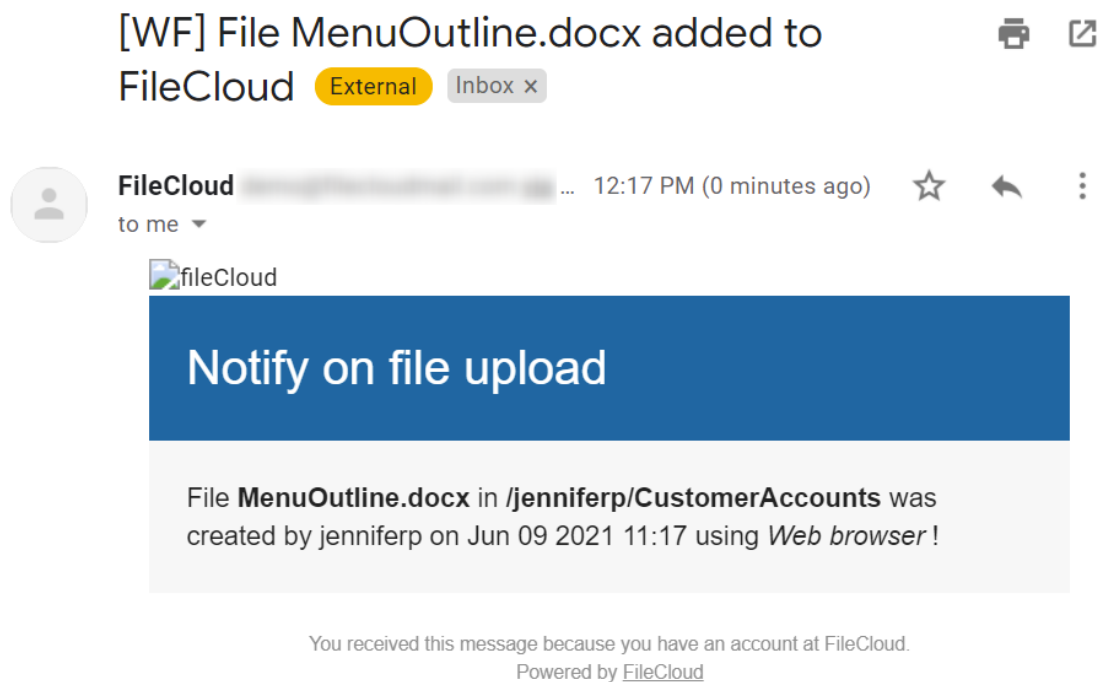
Notify on file upload

← Previous

→ Finish

✕ Cancel

9. Sample notification email on a file upload.



Periodic Script Workflow

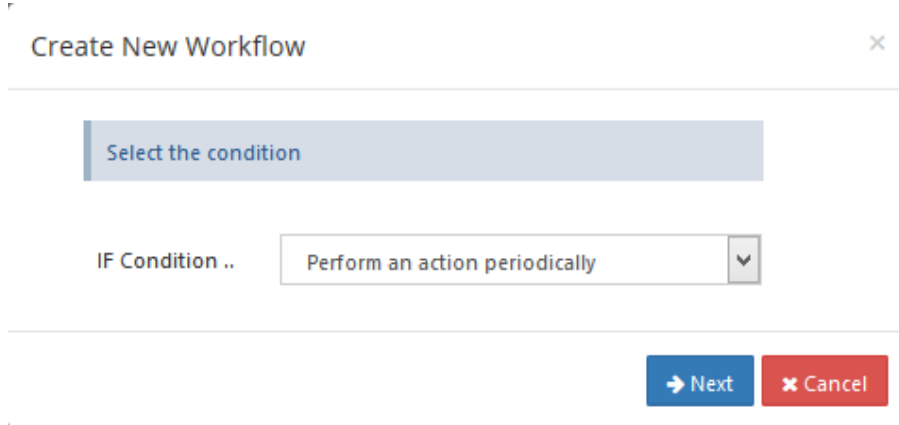
This workflow recipe runs a specified command at a periodic interval.

- 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.

Parameters

No additional parameters are required.

← Previous

→ Next

✕ Cancel

6. 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

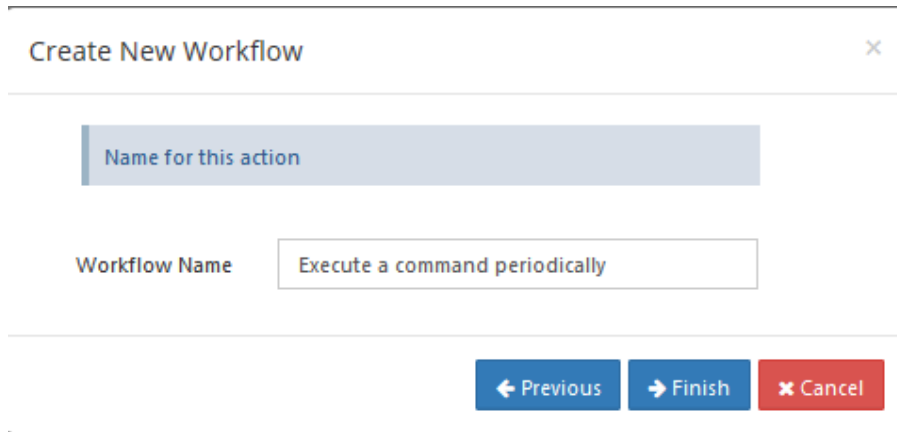
7. Enter the required Command.

In the following example, ls causes all files and folders to be listed.:

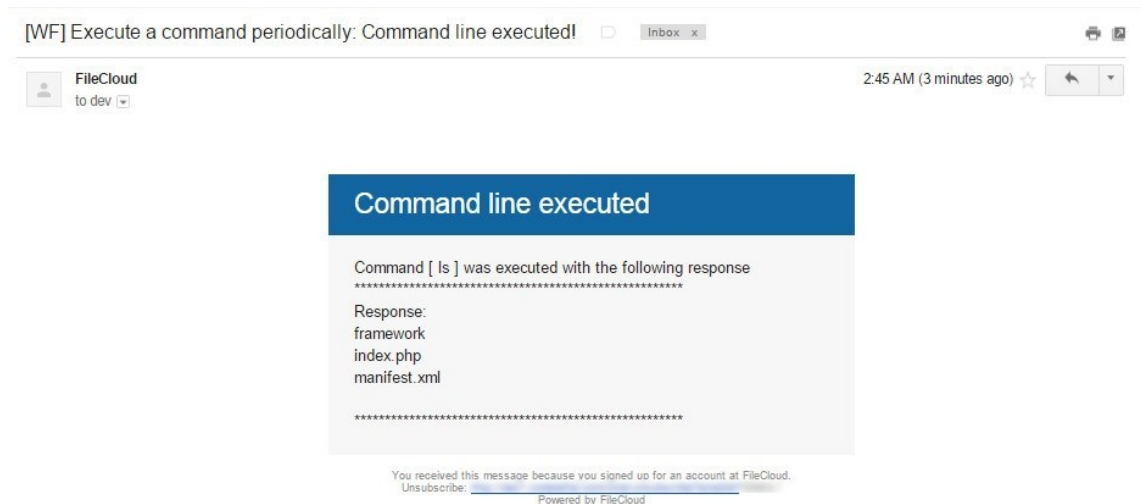
```
{
  "command_line": "ls"
```


}

8. Enter the Workflow name and Finish.



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



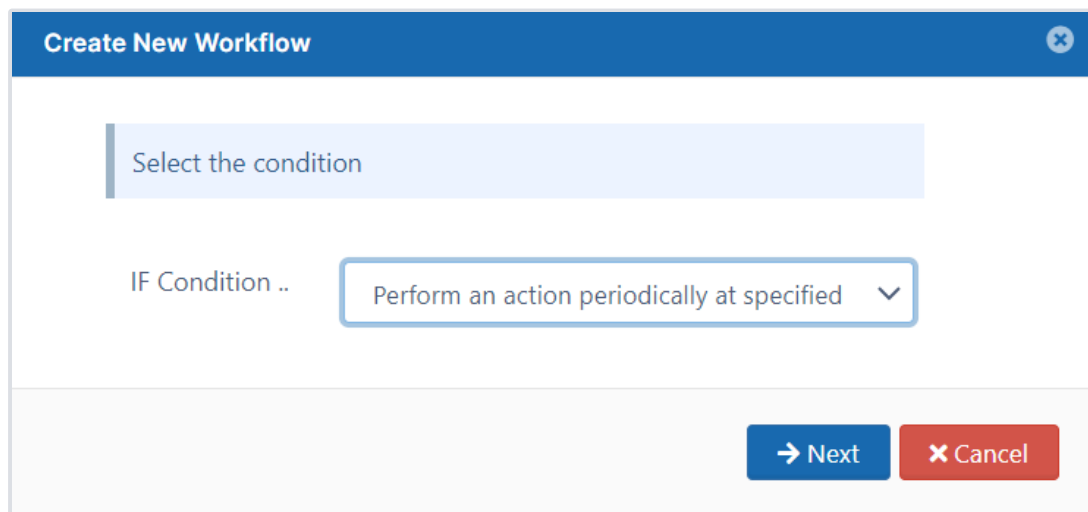
Periodically Send Custom Email Workflow

This workflow recipe sends a custom email to selected users at specified intervals.

In the example, an email is sent to users in the **Employees** group every 30 days from January to June to remind them to submit their receipts to a **Reimbursements** folder.

To create a workflow that sends a custom email periodically:

1. In the admin portal's navigation panel, click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
3. In **IF Condition**, choose **Perform an action periodically at specified time and interval**.



Create New Workflow

Select the condition

IF Condition .. Perform an action periodically at specified ▼

→ Next × Cancel

4. Click **Next**.
5. Set the parameters according to your requirements for the interval.
In the image below, the message is scheduled to be sent approximately monthly for the first half of 2024 (every 30 days from January 1, 2024 to June 30, 2024).

Create New Workflow ✕

Provide the required parameters for the condition in JSON Format

Required Parameters

```
{
  "day_interval": 30,
  "start_date": "2024-01-01",
  "end_date": "2024-06-30"
}
```

This condition will be triggered when the current time matches the supplied time.

day_interval : Days interval (For daily operation, specify this value to be 1)

time_string : (OPTIONAL) Time in format H:i:s (If not specified, it will run at 00:00:00)

start_date : (OPTIONAL) Start date in format yyyy-mm-dd (If not specified, it will start from today)

end_date : (OPTIONAL) End date in format yyyy-mm-dd (If not specified, it will run indefinitely)

```
{
  "day_interval": 7,
  "time_string": "08:00:00",
  "start_date": "2020-01-01",
  "end_date": "2020-01-31"
}
```

← Previous → Next ✕ Cancel

6. Click **Next**.
7. In **THEN Action**, choose **Send an email**.

Create New Workflow ✕

Select the action to perform when the condition is triggered

THEN Action ..

Send an email ▼

← Previous → Next ✕ Cancel

8. Click **Next**.

9. Use the parameters to enter the details of the custom email.

In the parameters below, an email with the subject **Reimbursements** reminds users in the group **Employees** to copy their receipts into the Reimbursements folder.

Since **is_html** is set to **1**, tags in the body are recognized as HTML tags and formatted.

```
{
  "subject": "Reimbursements",
  "body": "<p>Month's end is almost here.</p><p>Copy any receipts into the
<b>Reimbursements</b> folder to be reimbursed.</p>",
  "is_html": 1,
  "groups": "Employees",
}
```

Create New Workflow

Provide the required parameters for the action to be executed

Required Parameters

```
{
  "subject": "Reimbursements",
  "body": "<p>Month's end is almost here.</p><p>Copy any receipts into the <b>Reimbursements</b> folder to be reimbursed.</p>",
```

Execute command for sending email.

subject : (REQUIRED) Subject of the email.

body : (REQUIRED) Body of the email.

is_html : (OPTIONAL) 1 if the body is in HTML format, 0 if it is in plain text format. Default is 0.

users : (OPTIONAL) Comma separated list of usernames to send the email to.

groups : (OPTIONAL) Comma separated list of group names to send the email to.

notify : (OPTIONAL) Boolean to specify whether to send the email to users automatically identified as impacted by the related action. Default is false.

***Note:** Emails will always be sent to the users explicitly listed in the **users** field and to all members of the groups in the **groups** field. Setting **notify** to true adds the affected users to the recipients list as well.*

If no users, groups or impacted users are found,

← Previous

→ Next

✕ Cancel

10. Click **Next**.

11. Give the workflow a name, and click **Finish**.

Create New Workflow

Name for this action

Workflow Name

Reimbursement reminder

← Previous

→ Finish

✕ Cancel

The workflow is listed in the **Manage Workflows** page. It will run automatically in 30 days.

Manage Workflows

Workflow

Workflow Name	IF THIS	THEN THAT
Reimbursement reminder	Perform an action periodically at specified time and interval	Send an email

12. In 30 days, the workflow automatically runs, and sends the following email to users of the group **Employees**.

Reimbursements

External

Inbox x

FileCloud

<demo@filecloudmail.com>

2:12 PM (0 minutes ago)

to me ▾

Month's end is almost here.

Copy any receipts into the **Reimbursements** folder to be reimbursed.

↩ Reply

➦ Forward

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

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

Check file integrity

IF Condition ..

If a file is created

▼

Required Parameters

```
{"parent_folder_path_string":"\"V\"}"
```

THEN Action ..

Verify file integrity and generate admin ale

▼

Required Parameters

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

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. Prior to FileCloud 23.251, by default, all users could share automated workflows. Beginning in 23.251, the setting **Allow Automation Workflow Sharing** must be enabled to permit all users to share automated workflows.

Disabling Automated Workflows

Automated Workflows enable users in the user portal to create automated processes, such as file approvals and file storage. By default the Automated Workflow function is enabled, but you can disable it.

To disable the Automated Workflows for certain users, disable them in the users' policies.

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	1	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<< < Page 1 of 1 > >>

2 rows

2. Open the policy assigned to the users who you do not want to access Automated Workflows.
3. Click the **Users** tab.
4. Scroll down and locate the **Disable workflow automation** setting. Enable the setting.

Allow group deletion	☐
Allows users to delete groups from user portal	
Allow Workflow Automation Sharing	☐
Enables/disables workflow automation sharing	
Disable workflow automation	☒
Require share approval workflow	☐
Enables/disables mandatory workflow automation for shares	

5. Click **Save**.

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

Enable Sharing of Automated Workflows

By default, users other than promoted admins with all user share and file privileges, cannot share automated workflows with other users. Enabling this setting allows all users to share automated workflows.

To enable sharing of Automated Workflows for certain users, enable the setting in the users' policies.

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

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	1	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<< < Page 1 of 1 > >>

2 rows

2. Open the policy assigned to the users who you want to be able to share automated workflows.
3. Click the **Users** tab.

4. Scroll down and locate the **Allow Workflow Automation Sharing** setting. Enable the setting.

Allow group deletion	☐
Allows users to delete groups from user portal	
Allow Workflow Automation Sharing	☒
Enables/disables workflow automation sharing	
Disable workflow automation	☐

5. Click **Save**.

Now, all users have the ability to share automation workflows.

Requiring a Share Approval Workflow

A Share Approval workflow is a specialized type of workflow that requires a share to be approved before it is made available.

In order for a Share Approval workflow to become active for specific users, you must mark it required in their policies and choose the specific Share Approval workflow to use.



For the Share Approval workflow to apply to all users' shares in FileCloud, it must be created by a [promoted Admin](#) with all User Share permissions enabled. Otherwise, the share approval workflow will only apply to shares initiated by the workflow creator on files and folders in their My Files folder.

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

The **Policies** page opens.

Policies

New Policy

Create a new policy

New Policy

Policy Name	User Count	Group Count	Default	Actions
Global Default Policy	1	0	☒	     
TEAM FOLDER POLICY	1	0	☐	     

<<

<

Page 1 of 1

>

>>

2 rows

- 2. Open the policy assigned to the users who you do not want to access Automated Workflows.
- 3. Click the **Users** tab.
- 4. Scroll down to **Require share approval** and enable it.
- 5. In **Selected Workflow**, choose the Share Approval workflow to make effective.

Disable workflow automation

☐

Require share approval workflow

☒

Enables/disables mandatory workflow automation for shares

Select workflow

Select a workflow

Selected automation workflow for shares

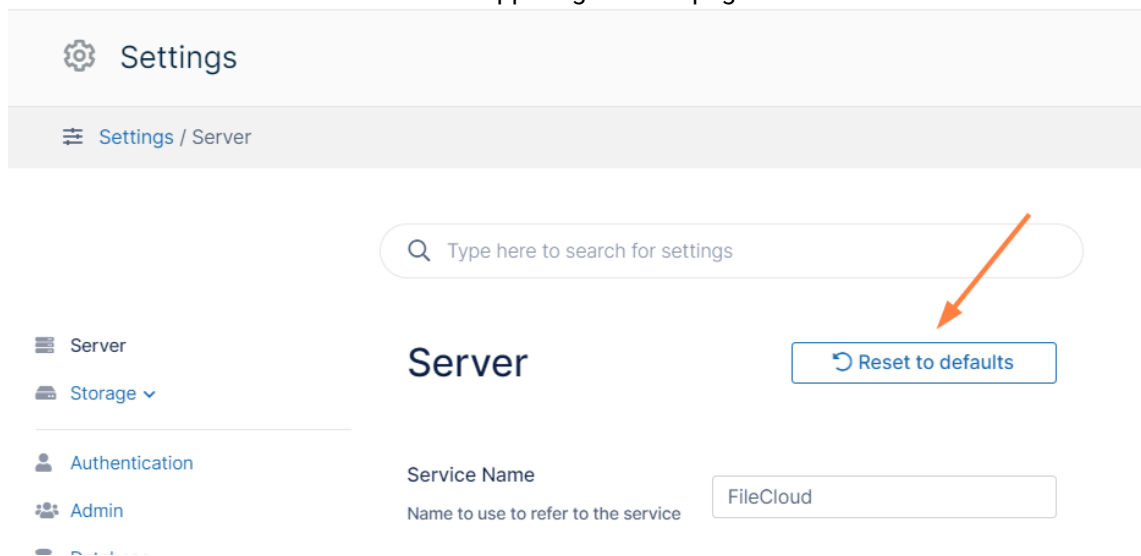
For end user information on creating Automated Workflows, see Workflow Automation.

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 in Settings

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**, then navigate to the page whose settings you want to reset.
2. Click the **Reset to defaults** button in the upper right of the page.



A confirmation dialog box opens.

3. Click **OK**.
The settings on the page are set back to their default settings.

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

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Reset** . The Reset page opens.
2. Click **Reset All Settings and Customizations**.

Reset

Globally reset all settings and customizations

Do you wish to reset all settings and customizations?

Reset All Settings and Customizations



A confirmation dialog box opens.

Warning ✕

Reset settings and customizations to defaults for all user?

☒ Confirm and continue with reset?

Reset

Cancel



3. Check **Confirm and continue with the reset**, and click **Reset**.
All of the options that appear on the Settings and Customization pages are reset to their defaults.