# FileCloud Server
# 23.253
# FileCloud Site Maintenance

2 January, 2026

# Table of Contents

Admin Portal Dashboard ..... 2
Setup Checklist ..... 2
Quick Actions ..... 3
Dashboard Widgets ..... 4
Release Notifications ..... 16
By Subscribing to the Mailing List ..... 16
By seeing the version update in the FileCloud Admin Portal ..... 16
Managing Users ..... 17
Listing FileCloud Users ..... 17
Viewing User Properties ..... 18
Disable a FileCloud User Account ..... 28
Deleting a FileCloud User ..... 29
Resetting a User Password ..... 32
Manage A User's Policies ..... 34
Manage a User's Profile Picture ..... 37
Change a User's Email Address ..... 38
Setting a User Account to Expire ..... 38
Send Email from User Details ..... 39
Managing Groups ..... 41
Change a User Group Name ..... 41
Delete a User Group ..... 41
View and Change Group Members ..... 42
Exporting a list of users in a group ..... 43
View and Change Group Admins ..... 44
View and Change a Group's Policy ..... 45
View and Change an SSO-imported Group's Sync Options ..... 46
Managing Admin Users ..... 48
Check an admin user's permissions ..... 48
Remove an admin role ..... 50

Managing User Folders and Files ..... 52
Add Folder-Level Permissions to User Folders ..... 54
Copy and Move User Files ..... 57
Download User Files and Folders ..... 60
Cancel User Uploads in Progress ..... 63
Delete User Folders and Files ..... 64
Clear a Recycle Bin ..... 65
Remove a User's Old File Versions ..... 69
Remove Incomplete User Uploads ..... 70
Restore a Previous File Version ..... 71
Critical Section Cleanup Tool ..... 74
Change the Name of the Zip File for Multiple File Downloads ..... 77
Managing Team Folders ..... 79
To view the breakdown of data in Team Folders: ..... 81
To edit the Team Folders account fields: ..... 81
To lock the Team Folder account: ..... 82
To manage Team Folder shares: ..... 83
To reset the Team Folder account password: ..... 84
To manage Team Folder notifications ..... 85
To delete the Team Folder account: ..... 86
Search for a Team Folder ..... 88
Recover Deleted Files ..... 88
View and Restore Previous Versions in Team Folders ..... 90
Managing User Shares ..... 93
To manage user shares for an individual user: ..... 93
To manage user shares for all users: ..... 95
To export a list of all shares: ..... 96
Transfer Ownership of a Reshare from a Team Folder or Network Share ..... 97
Creating direct file download link from a public file share ..... 99
Creating direct file download links from a public folder share ..... 99
Managing Storage Space Usage ..... 103
In this section ..... 103

Related topics ..... 103
Storage Scanner Tool for Missing Files ..... 104
Storage Usage Tool ..... 105
Thumbs Tool for Removing Excessive Thumb Files ..... 106
Managing User Locks ..... 109
Managing User-Defined Notifications ..... 113
Editing individual user's file and folder notifications ..... 113
Editing all users file and folder path notifications ..... 116
Adding notifications for actions on user's files and folders ..... 118
Managing Client Devices ..... 120
FAQ's ..... 121
How Do You Want to Manage a Device? ..... 123
Centralized Device Management ..... 127
iOS Device Management ..... 184
Mass Deployment - Default Configuration Support ..... 185
Search in the Admin Portal ..... 199
FileCloud's Federated Search ..... 199
All search ..... 201
Audit Logs ..... 208
What do you want to do? ..... 208
View Audit Logs ..... 208
Filter Audit Log Views ..... 210
Compact the Audit Database ..... 213
Configure What is Logged ..... 213
Export Audit Logs ..... 215
Delete Audit Log Entries ..... 216
Change the Audit Log Warning Limit ..... 225
Backing Up and Restoring FileCloud Server ..... 226
What do you want to do? ..... 226
The FileCloud Server Backup Tool ..... 226
Backing Up and Restoring Linux ..... 255
FileCloud Backup and Restore - Linux Manual ..... 255

FileCloud Backup and Restore - Windows Manual ..... 259
Migrating FileCloud Server to Another Server ..... 261
Migrating a FileCloud Server Site ..... 265
Enabling the Backup Server URL ..... 265
Monitoring FileCloud ..... 266
What do you want to do? ..... 266
FileCloud Alerts ..... 269
File Content Heuristic Engine ..... 270
Identifying a FileCloud Specific Path ..... 275
Custom Reports ..... 277
Add Reports ..... 277
Download Reports ..... 279
Available Reports ..... 280
Specifying Y-M-d H:i:s values ..... 287
Manage Folder Level Permissions ..... 288
To Edit Folder-Level Permissions ..... 288
Read Only Sync ..... 290
Managing Metadata ..... 291
Metadata for governance and other system processes ..... 291
Metadata for users ..... 293
Metadata Components and Types ..... 294
Create a New Metadata Set ..... 299
Edit an Existing Metadata Set ..... 303
Managing Metadata Attributes ..... 305
Managing Metadata Permissions ..... 306
Working with Built-In Metadata ..... 310
Working with Custom Metadata ..... 335
Working with Default Metadata ..... 336
Troubleshooting Metadata ..... 338
Finding files without metadata ..... 339
Metadata Limitations/Recommendations ..... 343
Managing FileCloud Licenses ..... 345

FileCloud - License Purchase And Renewal ..... 345
Install FileCloud License ..... 362
Workflows - IFTTT ..... 369
The Workflow Dashboard ..... 369
Add a New Workflow ..... 370
Define an IF Condition ..... 371
Define a THEN Action ..... 405
Edit a Workflow ..... 421
Run a Workflow ..... 422
Set Advanced Workflow Options ..... 423
Workflow Recipes for FileCloud ..... 428
Troubleshooting Workflows ..... 477
Automated Workflow Management ..... 480
Disabling Automated Workflows ..... 480
Enable Sharing of Automated Workflows ..... 481
Requiring a Share Approval Workflow ..... 482
Reset Settings and Customizations ..... 484
To return to default settings for options in Settings ..... 484
To return to default settings for all options on the Settings pages: ..... 484

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

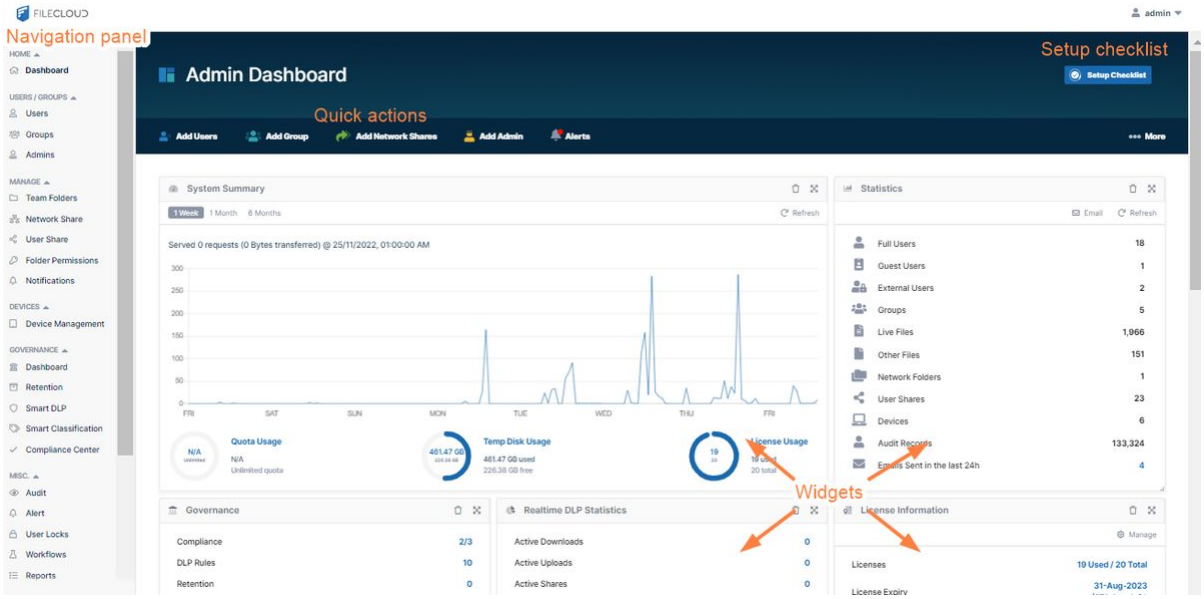

- Admin Portal Dashboard (see page 2)
- Release Notifications (see page 16)
- Managing Users (see page 17)
- Managing Groups (see page 41)
- Managing Admin Users (see page 48)
- Managing User Folders and Files (see page 52)
- Managing Team Folders (see page 79)
- Managing User Shares (see page 93)
- Managing Storage Space Usage (see page 103)
- Managing User Locks (see page 109)
- Managing User-Defined Notifications (see page 113)
- Managing Client Devices (see page 120)
- Search in the Admin Portal (see page 199)
- Audit Logs (see page 208)
- Backing Up and Restoring FileCloud Server (see page 226)
- Monitoring FileCloud (see page 266)
- FileCloud Alerts (see page 269)
- File Content Heuristic Engine (see page 270)
- Identifying a FileCloud Specific Path (see page 275)
- Custom Reports (see page 277)
- Manage Folder Level Permissions (see page 288)
- Read Only Sync (see page 290)
- Managing Metadata (see page 291)
- Managing FileCloud Licenses (see page 345)
- Workflows - IFTTT (see page 369)
- Automated Workflow Management (see page 480)
- Reset Settings and Customizations (see page 484)

# Admin Portal Dashboard

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

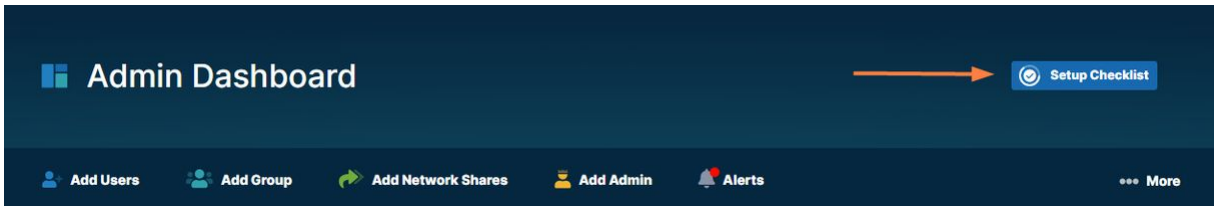
💡 The Admin dashboard displays several areas to help you manage your site.

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

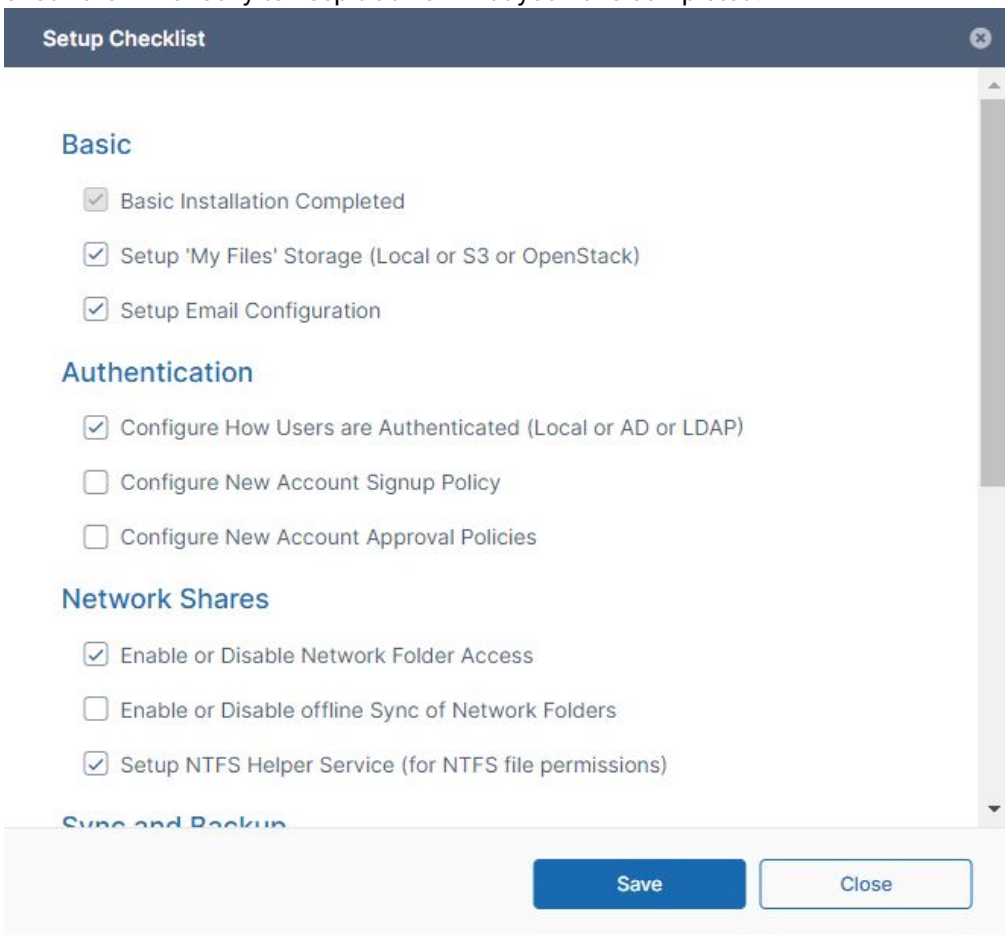



## Setup Checklist

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

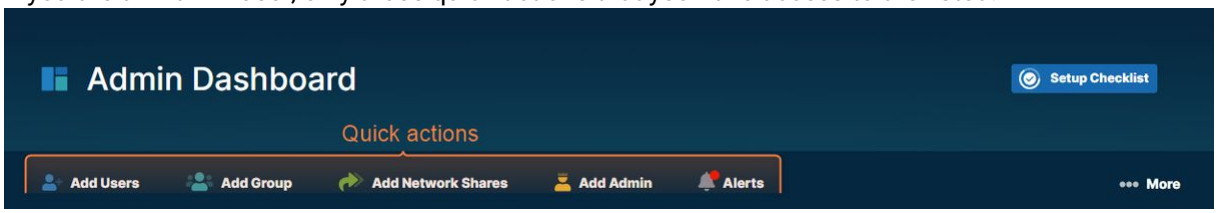


The **Setup Checklist** includes various tasks generally necessary for setting up FileCloud, although some tasks may not apply to you.
The tasks **Basic Installation Completed** and **Setup Cron Job** are automatically checked/unchecked for you, and you cannot modify them. All of the other tasks are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




## Quick Actions

Links for quick actions are listed in a ribbon near the top of the page. They take you to the screen in the Admin portal for the action, for example, the **Add Users** link takes you to the **Manage Users** screen. The **Alerts** link takes you to the **Manage Alerts** screen. It displays a red dot if there are alerts listed on the **Manage Alerts** screen. You must clear all alerts from this screen to remove the red dot from the **Alerts** link.
If you are an Admin user, only those quick actions that you have access to are listed.



For help performing the quick actions, see:
Add a user
Add a group
Add Network Shares
Add Admin (see page 48)
Alerts (see page 269)

# Dashboard Widgets

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

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

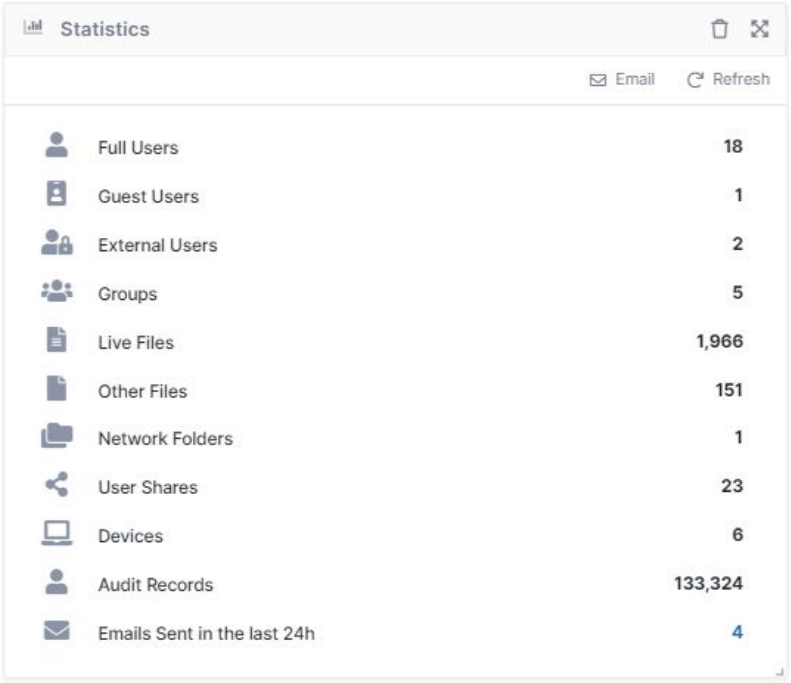
## Widget descriptions

### System Summary

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

### Statistics

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



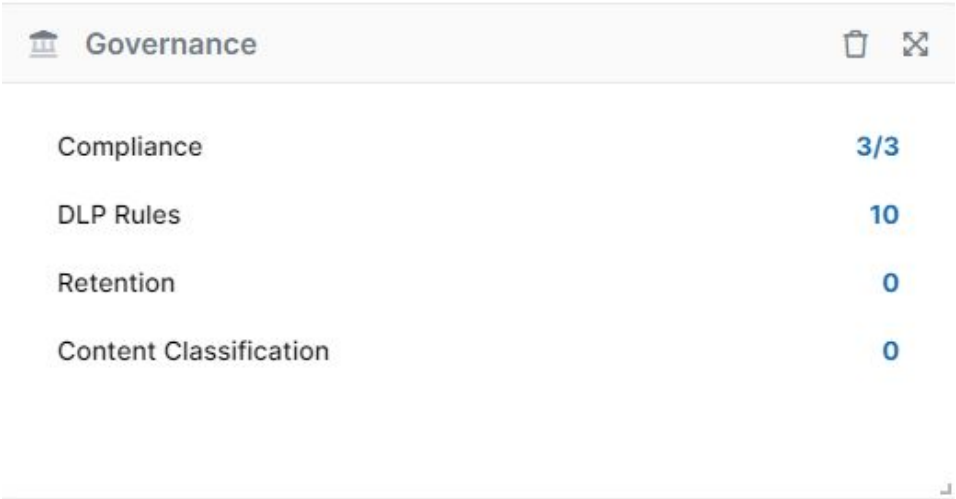

| Icon | Function |
|---|---|
| | Sends an Admin Summary email to the admin. By default, an Admin Summary email is sent to the admin every 24 hours. Click number to view report. |
| | Refreshes the statistics. |

| Statistic | Description |
|---|---|
| Full / Guest / External Users | Number of full users, guest users, and external users. |
| Groups | Number of groups. |
| Live Files | Number of files stored locally by all users combined that users can access directly from FileCloud folders. |
| Other Files | Other files are additional versions of Live files that users access from the Previous Version option for a file. |
| Network Folders | Number of Network folders. |

| Statistic | Description |
|---|---|
| User Shares | Number of shares by each user. A share is counted each time a different user shares it, but only once per time shared, even if it is shared with multiple users. |
| Devices | Number of clients (other than the Web server) that use your system, such as FileCloud Drive, FileCloud Sync, MS Office plugin, MS Outlook plugin, mobile applications, ServerSync, and ServerLink. |
| Audit Records | Number of audit records in the entire system. |
| Emails Sent in the last 24h | Number of emails sent in your system in the last 24 hours. Click the number to view a report. |

**Governance**

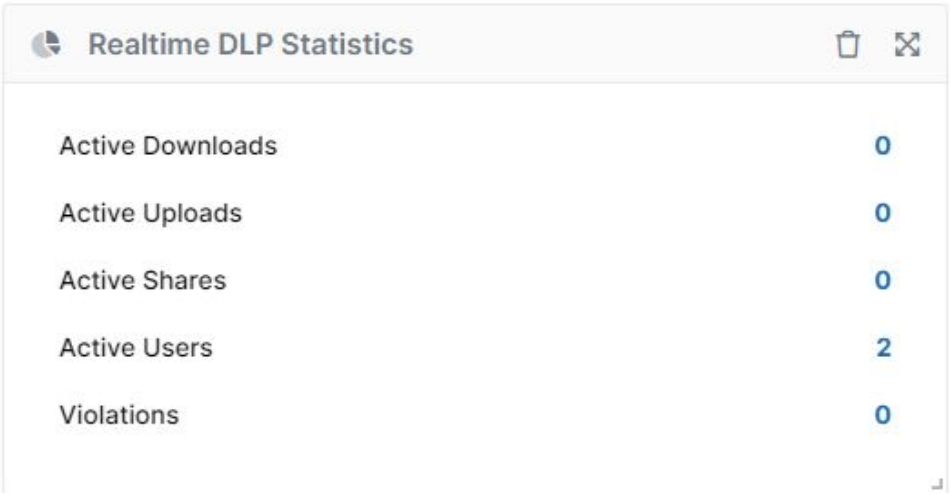
The Governance widget displays counts of your compliance configurations, DLP rules, retention policies and content classification rules. Each count is a link to the screen for configuring the feature.




**Realtime DLP Statistics**

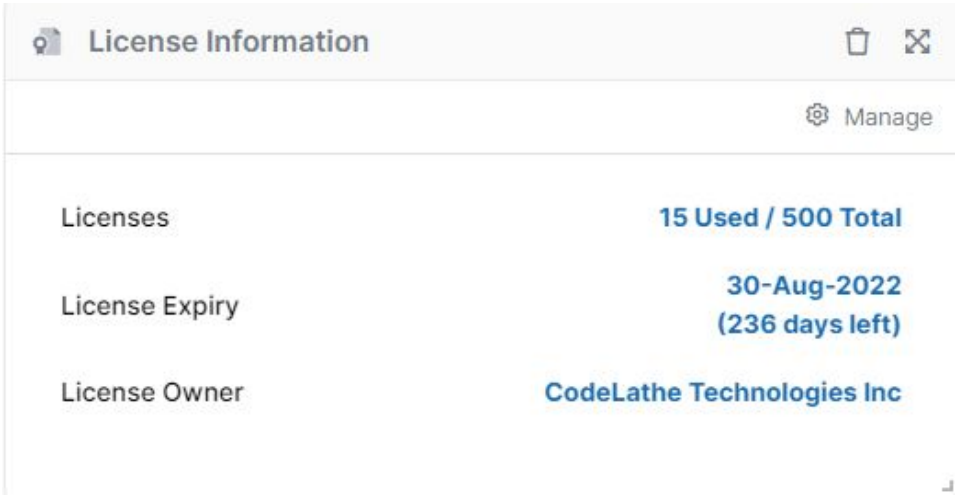
This widget displays DLP statistics from the last 7 days, and displays reports of Active Downloads, Active Uploads, Active Shares, and Active Users when you click the number on the right. When you click the number to the right of Violations, the Manage DLP Rules page opens.

⚠ Please note the following known issue:




**License Information**

This widget shows you basic information about your license.




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

**Recent Access Locations**

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

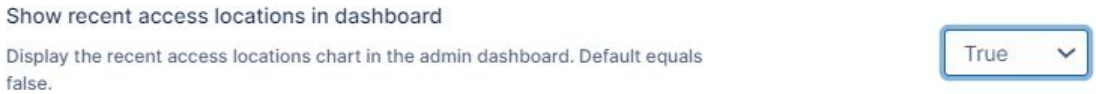
displays the total number of visits from that particular location in the last 10 days.

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

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

**To enable the Recent Access Location report:**

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

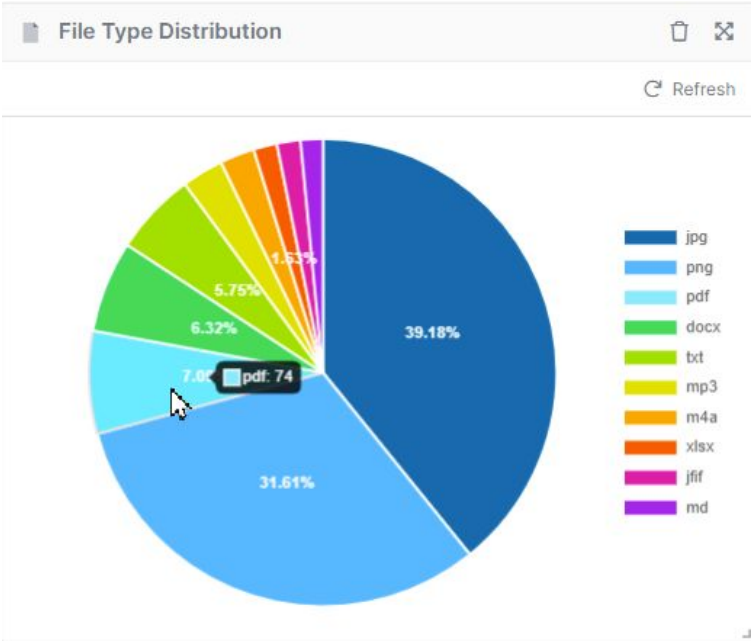


| Settings | Value |
|---|---|
| Show recent access location in dashboard | TRUE - Show the Geo IP Map with data<br>FALSE - Hide the Geo IP Map from the dashboard<br>DEFAULT - Show the Geo IP Map with no data. |
| Access locations Server URL | Server URL that converts the IP address to Geo Location Data.<br>Default URL: http://geoiplookup.codelathe.com/geoip.php<br>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.<br>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.

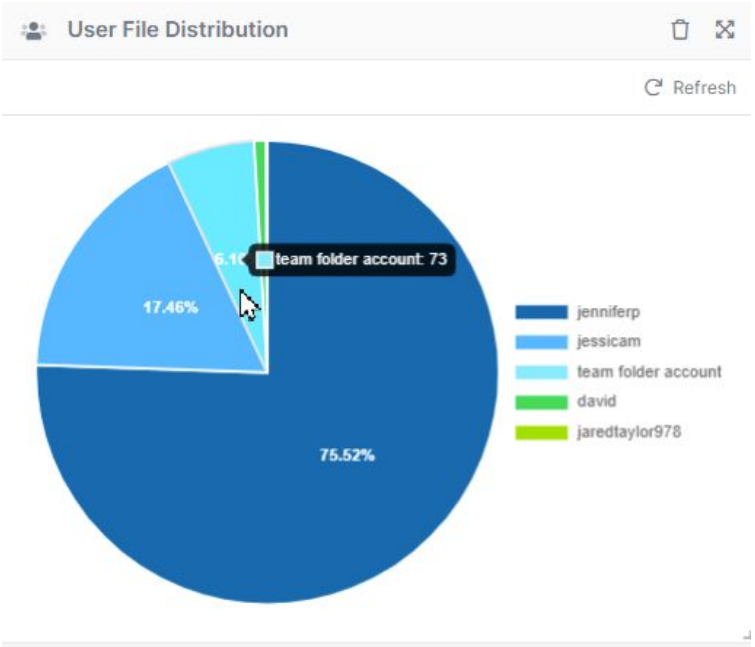
### File Type Distribution

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.



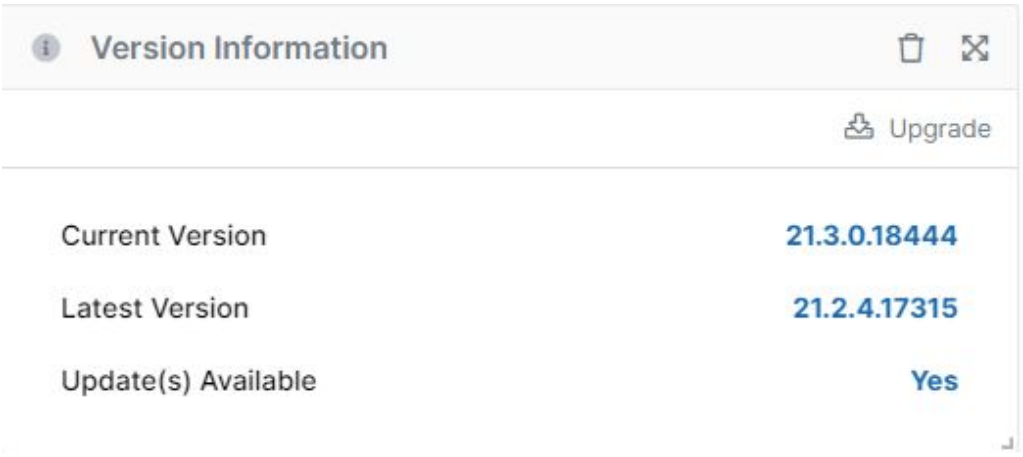

### User File Distribution

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.



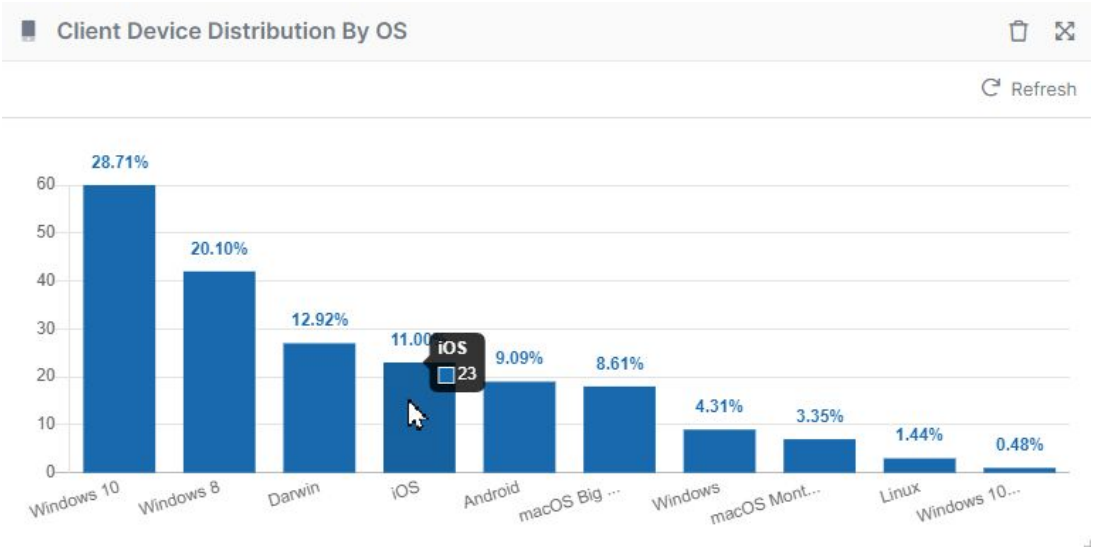

**Version Information**

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**.



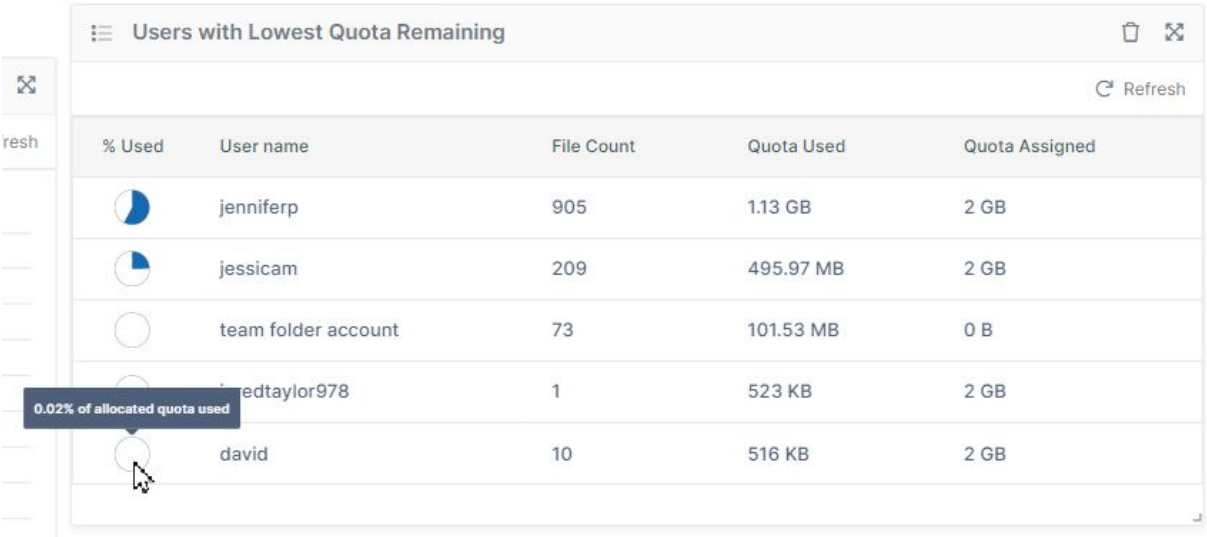

**Client Device Distribution by OS**

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.




### ServerLink

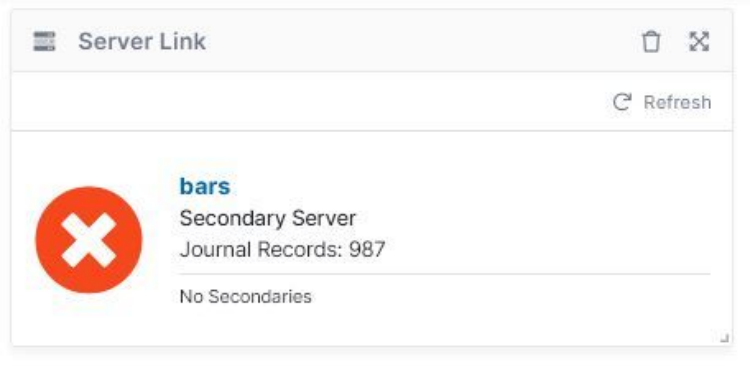
The **ServerLink** widget is available to customers who have ServerLink running. It gives you a quick view of the status of your ServerLink servers and is similar to the Status tab in the ServerLink settings screen.

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 a background indicates that the server is not running.

User signed into a primary server.

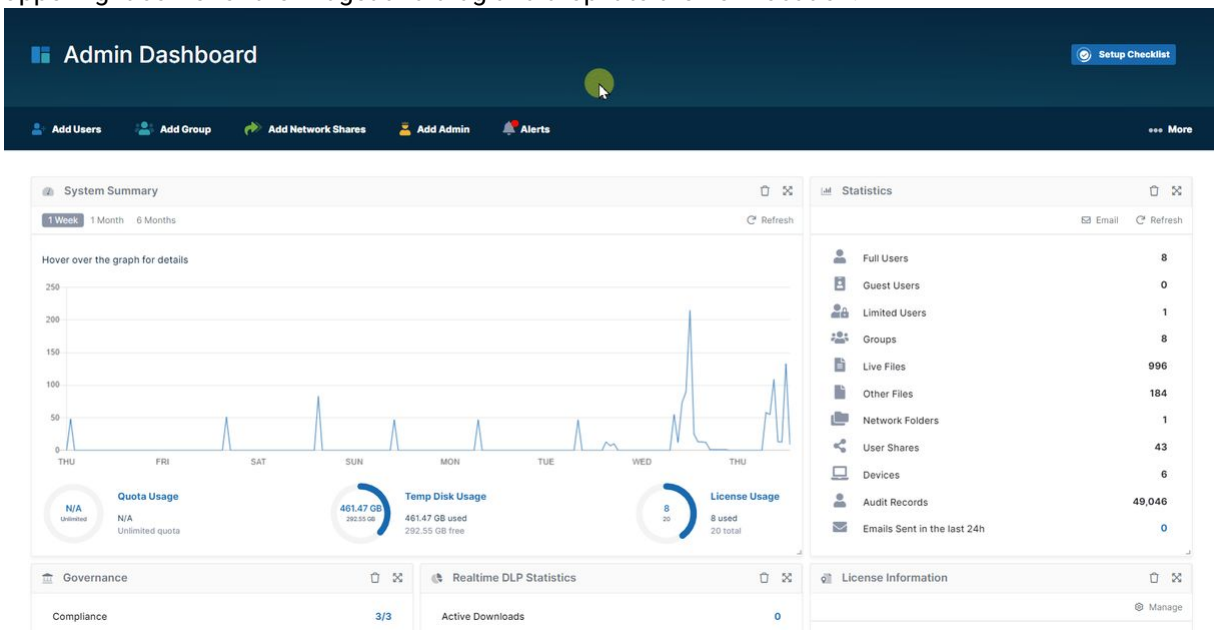
This is the way the ServerLink widget appears for a primary server when the secondary server is not syncing with it. The primary server displays a exclamation mark with a yellow background.

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

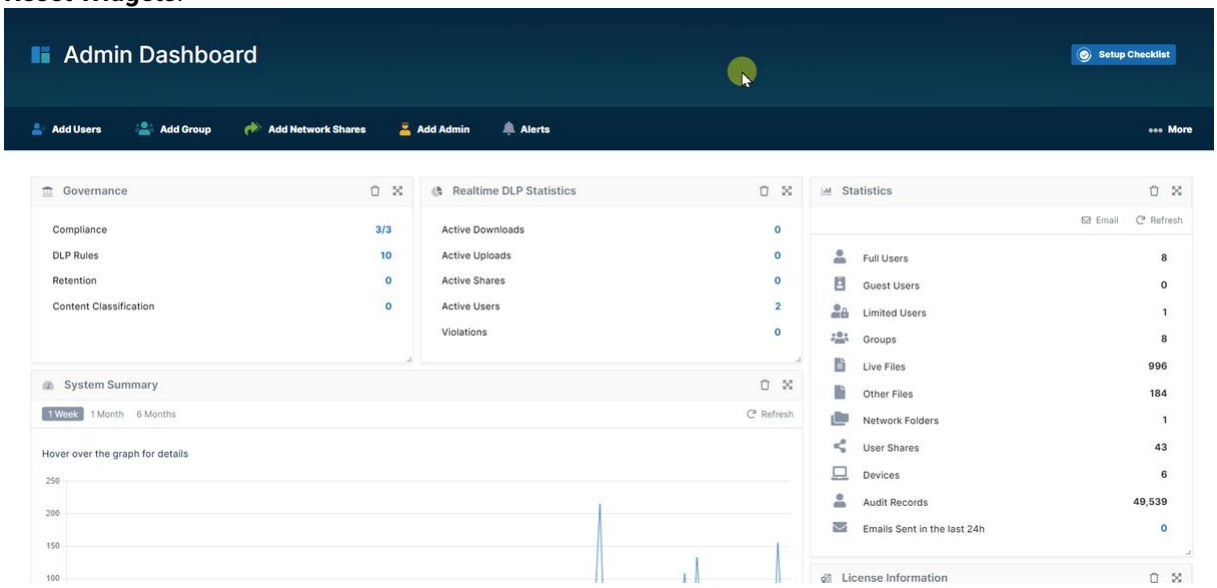
For more information, see Viewing ServerLink Information.

## 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.

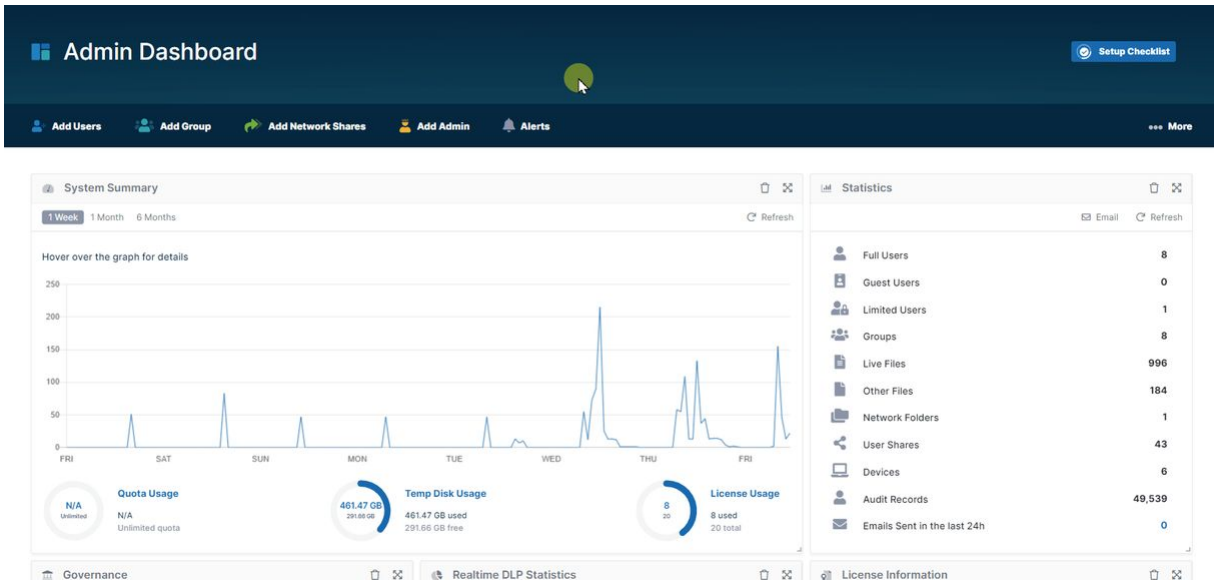


To move all widgets back to their original configuration, click **More** in the header ribbon and choose **Reset Widgets**.



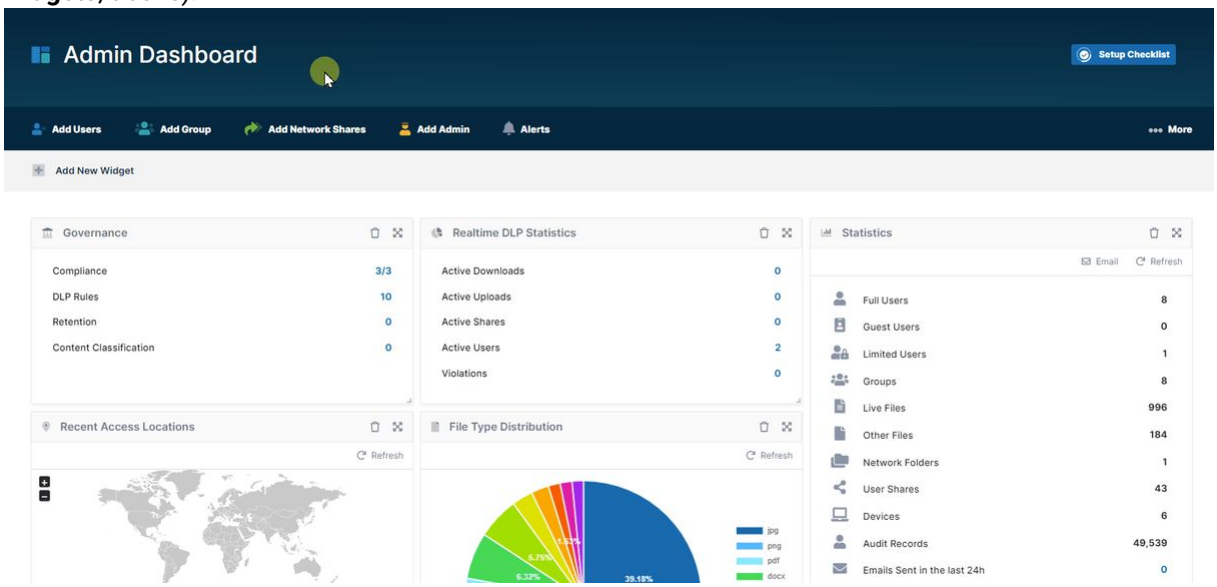

## Removing and Restoring Widgets

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:

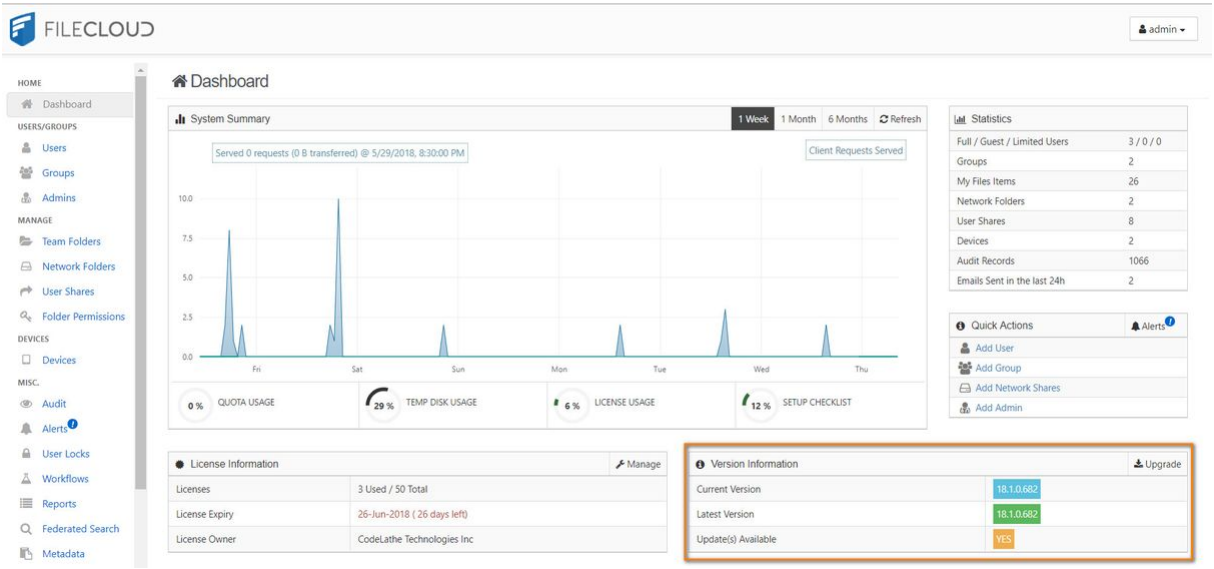
## By Subscribing to the Mailing List

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[1].

## 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.




1. https://www.filecloud.com/email-signup/

# Managing Users

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

**In this section:**


- Listing FileCloud Users (see page 17)
- Viewing User Properties (see page 18)
- Disable a FileCloud User Account (see page 28)
- Deleting a FileCloud User (see page 29)
- Resetting a User Password (see page 32)
- Manage A User's Policies (see page 34)
- Manage a User's Profile Picture (see page 37)
- Change a User's Email Address (see page 38)
- Setting a User Account to Expire (see page 38)
- Send Email from User Details (see page 39)

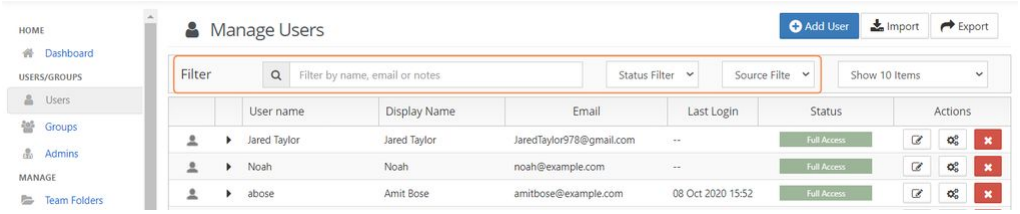

To add FileCloud users, see Create FileCloud Users.

## Listing FileCloud Users

### Listing Users

To list all users in FileCloud:

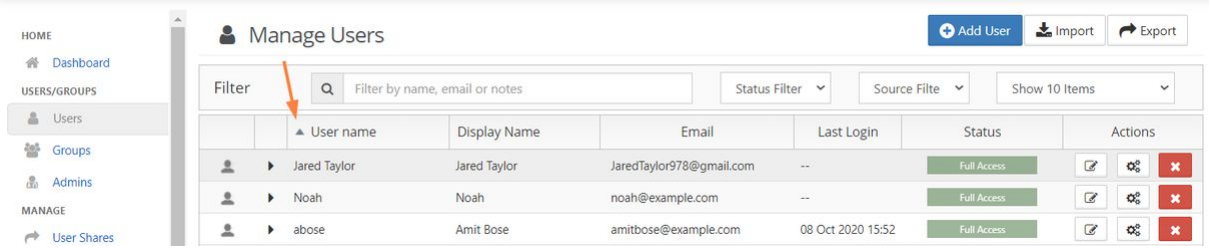
1. Log on to Administration Portal.
2. Click on **User** on the left navigation panel to list all users.
3. To find users:
   - by name or email,, use the **Filter by name, email or notes** box.
   - by status, use the **Status Filter** box.
   - by source, use the **Source Filter** box. Options are: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



## Sorting the User List

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

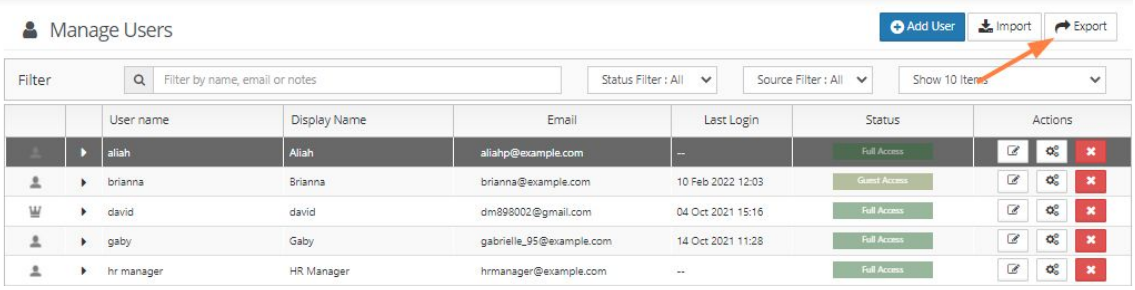
Notice that by default, all upper-case letters precede lower-case letters in alphabetical order.To change to a case-insensitive sort order, see Enabling ASCII Sort order for Listings of Users, Files and Folders.



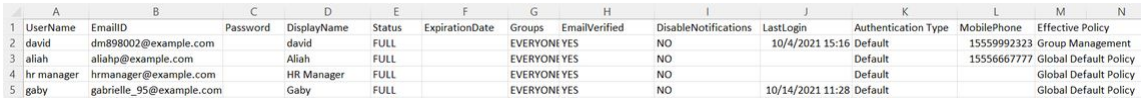

## Exporting a list of users

To export a list of FileCloud users:

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




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



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

# Viewing User Properties

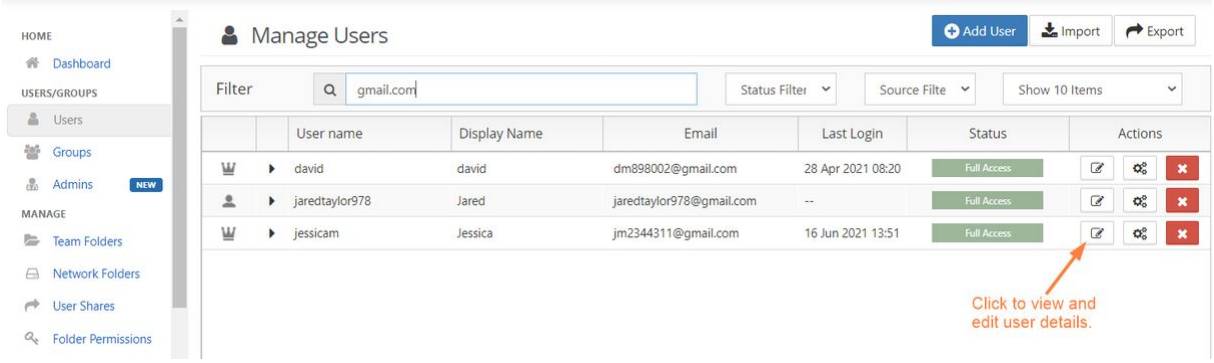
The ability to update and remove a user's profile picture is available in FileCloud Server version 18.2 and later.

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

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

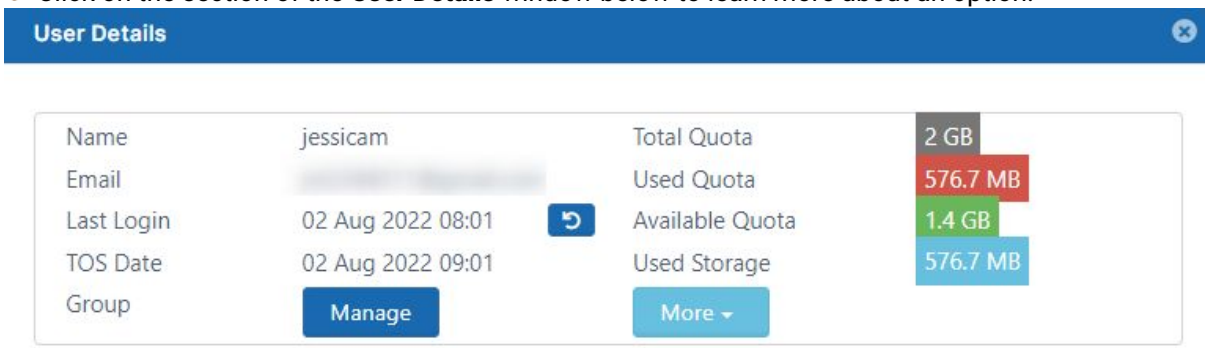
1. Open a browser and log on to the admin portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click on the row of the user you want whose details you want to view.
4. Click the **edit icon**.

**Show me**

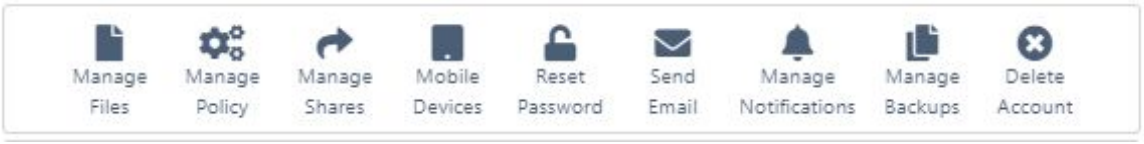



The **User Details** window opens showing you which user attributes you can set.

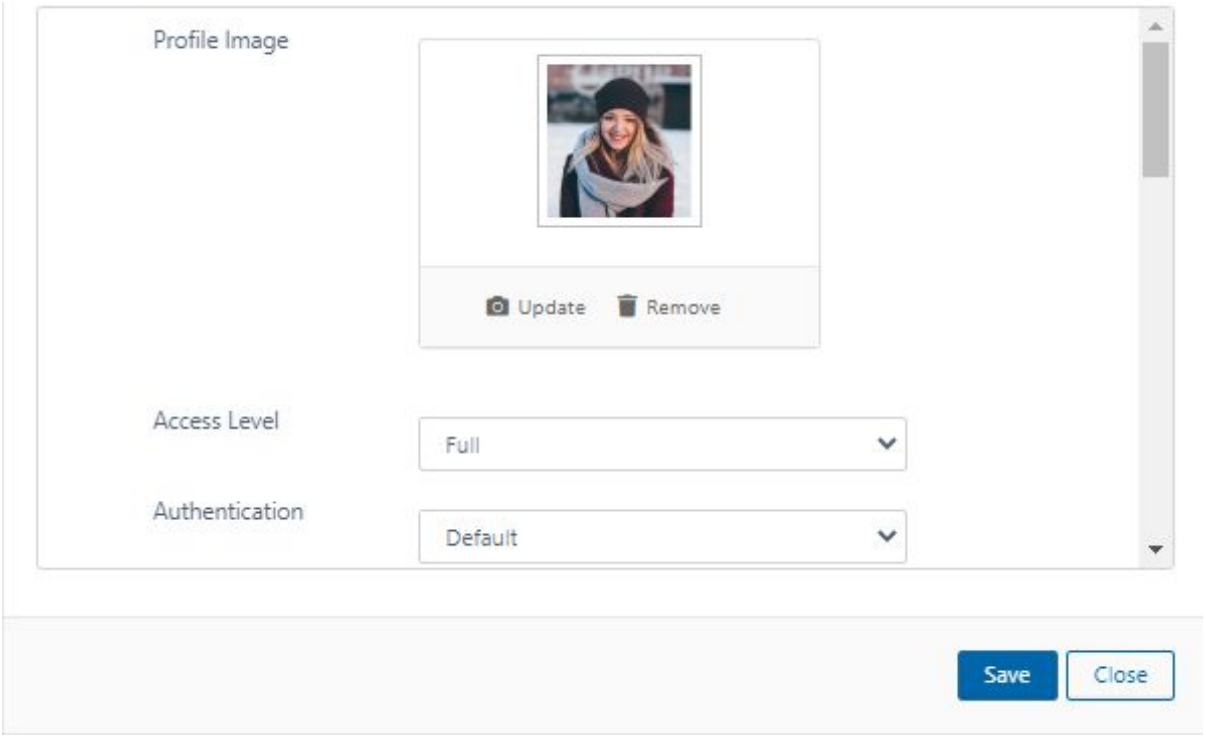
Click on the section of the **User Details** window below to learn more about an option.




(see page 26)




(see page 21)




(see page 23)

## Limit Admin Access to User Data

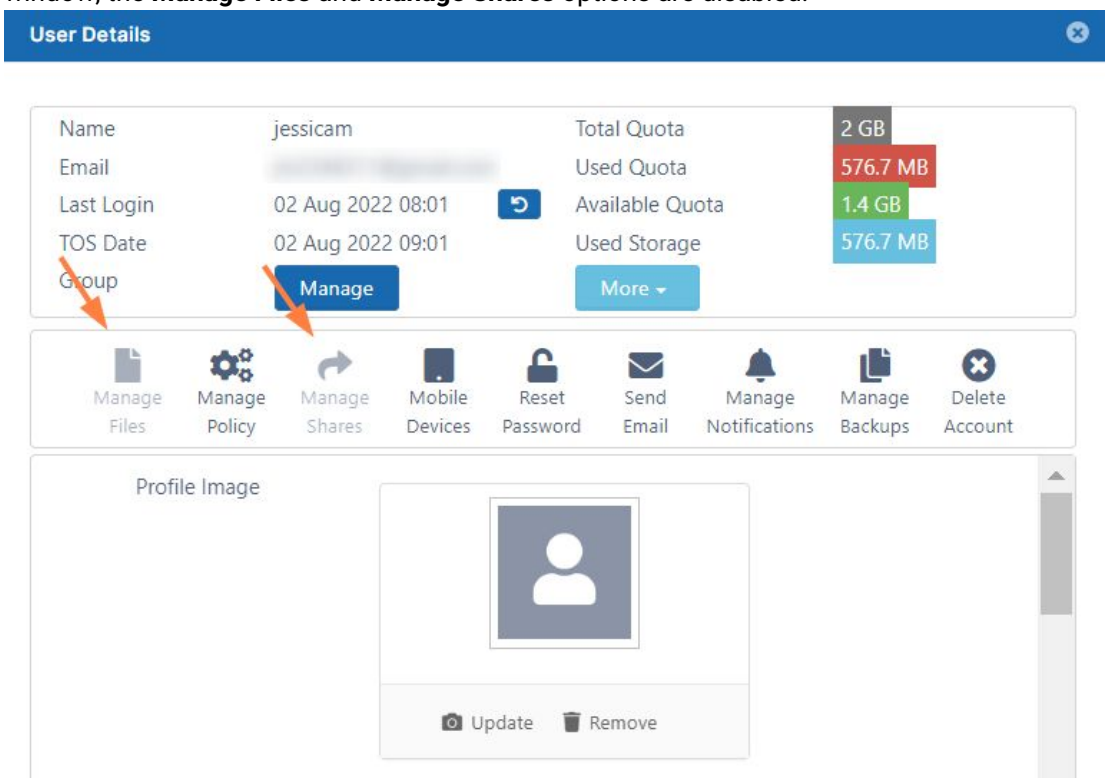
By default, the system's main admin and admin users with the proper access have the ability to manage user files and shares (see page 21), which includes the ability to download user content and view it.

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:

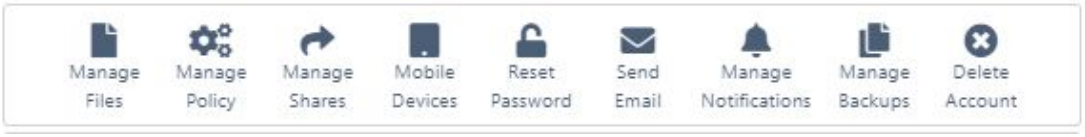



## User Properties - Advanced Options

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

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

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

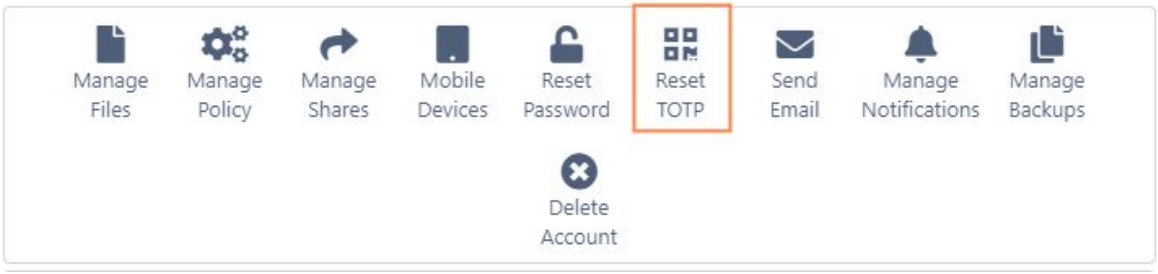


| Options | Description | For more information |
|---|---|---|
| **Manage Files** | Manage the files that are stored on your FileCloud Server site.<br>This allows you to protect and maintain your system in the following ways:<br>• Remove user files infected with a virus<br>• Remove files belonging to a user that no longer has an account<br>• Move folders for teams<br>• Download, copy and move files at a user's request<br>• Manage your storage space limits by moving or deleting files<br>• Copy and move files and folders between two FileCloud users | Managing User Files and Folders (see page 52) |
| **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 (see page 93) |
| **Mobile Devices** | Manage clients connecting to your FileCloud instance.<br>This feature is called Remote Client Management (RCM) or Data Leak Prevention Control (DLPC) | Managing Client Devices (see page 120) |
| **Reset Password** | Reset the password for user accounts with Authentication Type set to Default.<br>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 (see page 32) |
| **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.<br>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.<br>The option to send an account welcome message for accounts other than AD users is available beginning in FileCloud 20.1<br>The option to send an account welcome message to AD users is available beginning in FileCloud 20.3 | Send Email (see page 39) |
| **Manage Notifications** | Edit notifications configured on the user's file and folder paths. | Editing individual user's file and folder notifications (see page 113) |
| **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 (see page 29) |

### The Reset TOTP button

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



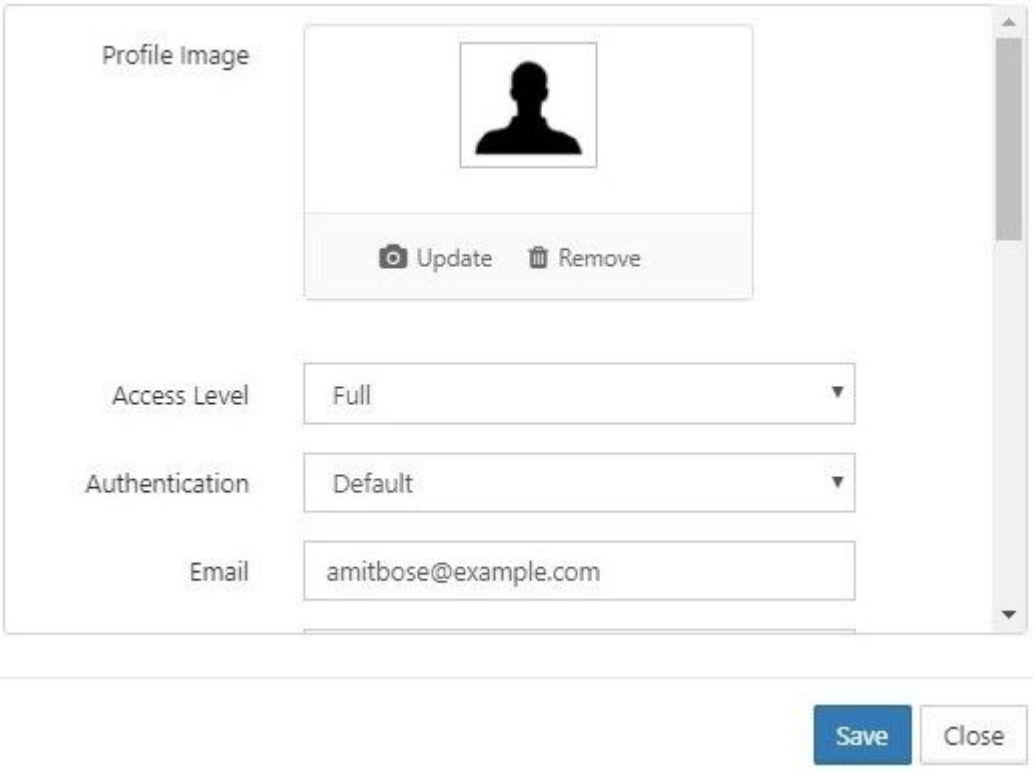

## User Properties - Editable

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

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

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

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




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

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

| Editable Property | Description |
|---|---|
| **Profile Image** | You can choose a new picture or remove the current one.<br>• This is useful for IT Managers who also manage user images in Active Directory.<br>• If no profile image is chosen, the default shown in the User Details panel is used by default. |
| **Access Level** | This is the access level set for this user. The possible values are:<br>• **Full Access**<br>• **Guest Access**<br>• **External Access**<br>• **Enabled**<br>• **Disabled**<br>Only accounts with enabled status can login into their account irrespective of their access level.<br>Disabled accounts do not count towards the License Limit.<br>For more information:<br>User Access Levels |

| Editable Property | Description |
|---|---|
| **Authentication** | This is the type of authentication used to verify the user's account.<br>The possible values are:<br>**Default**<br>**External (AD/LDAP)**<br>For more information:<br>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.<br>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. |
| **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 |

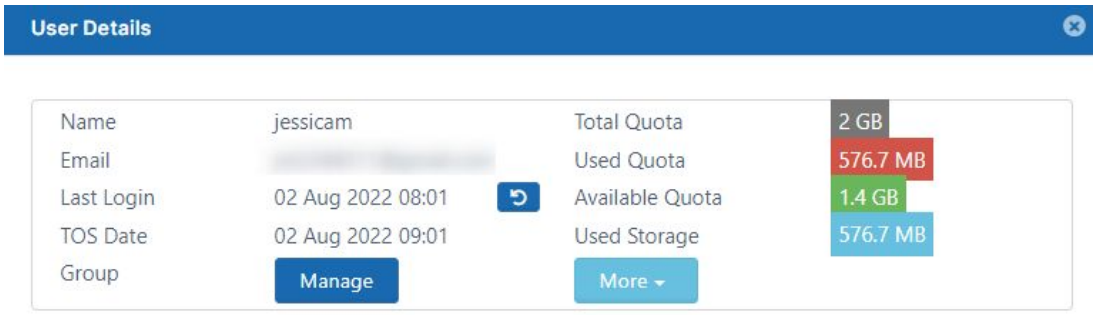
| Editable Property | Description |
|---|---|
| **Change Password on Login** | Forces the user to change the login password on first login to the user portal.<br> <br>Note: This does not appear when the following setting, **Creation Source**, is set to **SSO**. |
| **Creation Source** | Where user was created. Options are:<br>• Default (Admin user interface or import)<br>• 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** (added in FileCloud 20.1) | The user's phone number. |
| **Notes** | This filed allows the user to enter notes for the user and also search the user based on notes. |

## User Properties - Read Only

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

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

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




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

In this section of the User Details, you can manage the groups that a User belongs to by clicking the Manage button.
See Managing Groups (see page 41)

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.<br>**Note**: When a disabled user is re-enabled, Last Login is set to null. |
| **TOS Date** | Date that terms of service was approved on login. If not approved, **Not Accepted** appears. |
| **Group** | Click **Manage** to view, add, and remove the user's groups. |
| **Total Quota** | Quota allocated for this account (This can be changed using "**Total Quota (GB)**" text box) |
| **Used Quota** | This is the size of data this user has currently used. This includes all "Committed" Space by this user including file versions, files in recycle bin, partial files uploaded.<br>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 |

| Read only Property | Description |
|---|---|
| **Used Storage** | Space taken by all this user content. This includes space used for **multiple file versions**, **files in Recycle bin** contents and **Partial files in progress.** |

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

# Disable a FileCloud User Account

## Disabled User Account Status

Any user account can be disabled by the Administrator.

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

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

## Disabling a User Account

Disable a user account by following the steps listed below

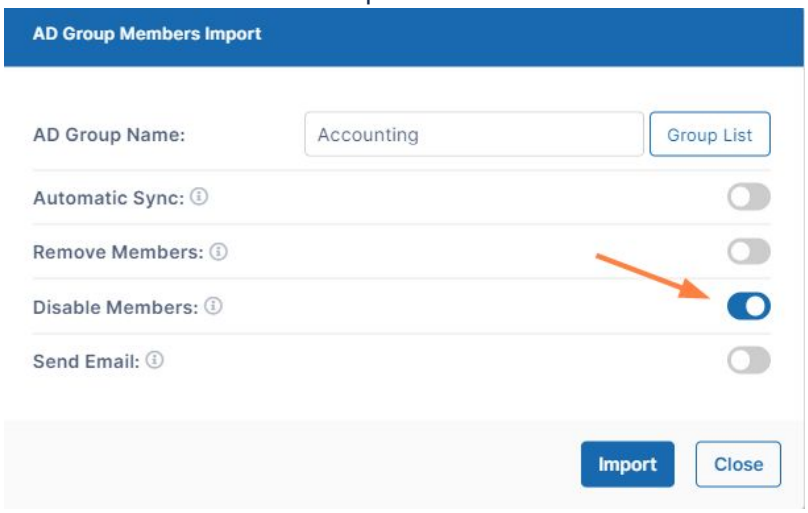
1. Log on to Administration Portal.
2. Click **Users** in the left navigation panel.
3. Click **Edit** in the user row.
4. Using the **Status** drop-down list, change the status to **Disabled**.
   UNKNOWN ATTACHMENT
5. Click **Save**.

### Import Disabled Users from Active Directory as Disabled

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

**To use this option:**

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




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

## Deleting a FileCloud User

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

When a user account is deleted

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

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

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

Use the admin portal to copy and move user files (see page 57)

**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 (see page 31)
- Use the admin portal (see page 32)

## 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

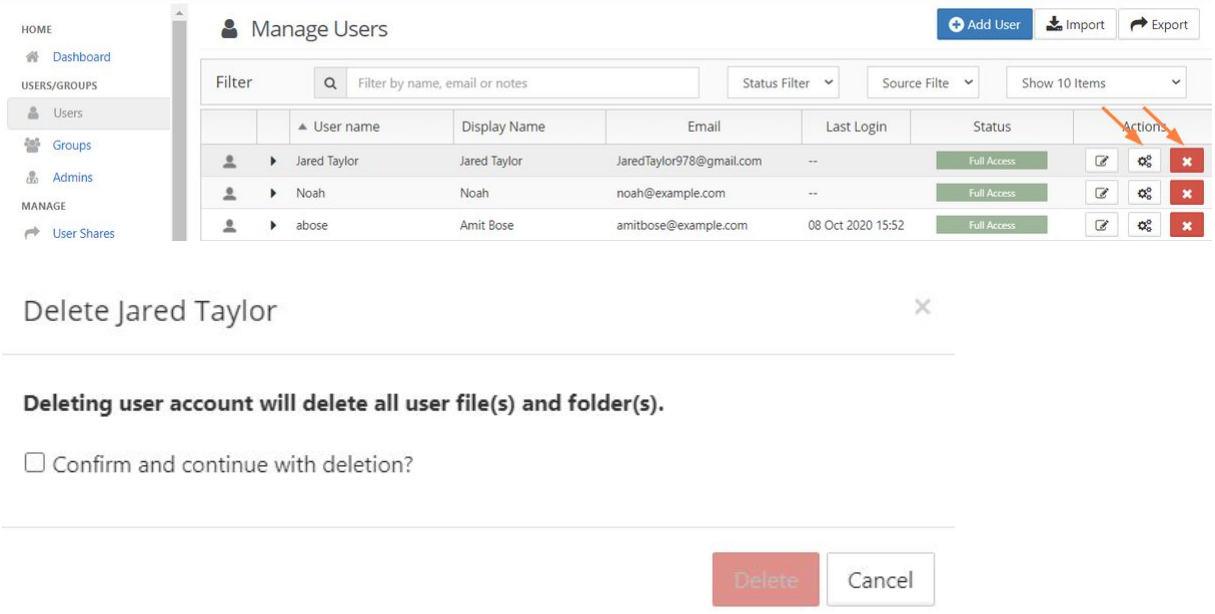
`php deleteuser.php -u <user_name> -h site2.xyz.com`

## 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 (see page 17) panel by clicking on the settings icon .







# Resetting a User Password

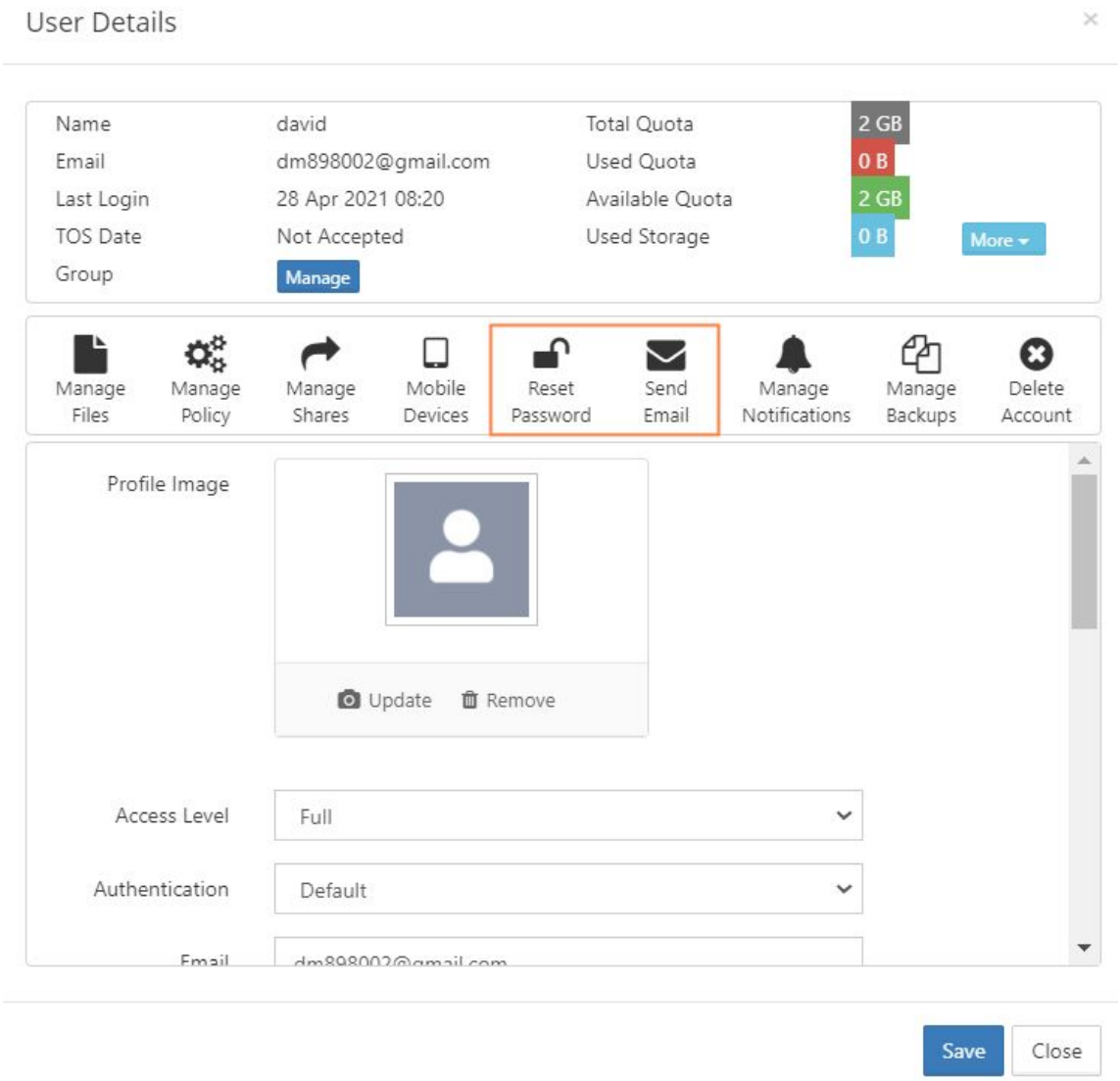
As a FileCloud Administrator, you can reset password for accounts with Authentication Type set to Default.

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

To reset password for user account:

1. Log on to Administration Portal.
2. Click on "**Users**" on left navigation panel.

3. Locate the user to reset the password using "**Filter Users**" or from the user list.
4. Click on "**Edit**" for the user row under the "**Actions**" column to launch the User Details window.

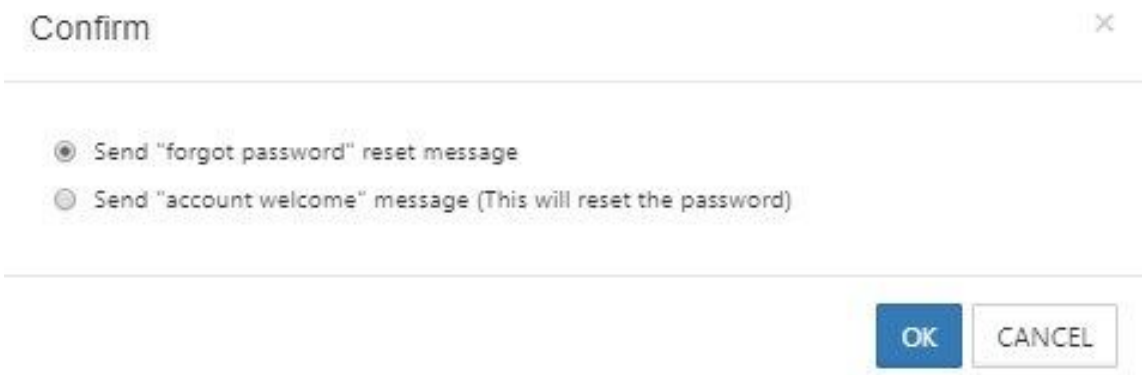



5. Click **Reset Password.**

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

OR

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




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

## Manage A User's Policies

Administrators can manage users easily using policies.

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

- The policy record can be associated with a user

Learn more about Policies

## What do you want to do?

**Select a Policy for a User**

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

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

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

**To select a policy for a user:**

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

**Change or Remove a User's Policy**

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

**To remove a policy for a user:**

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

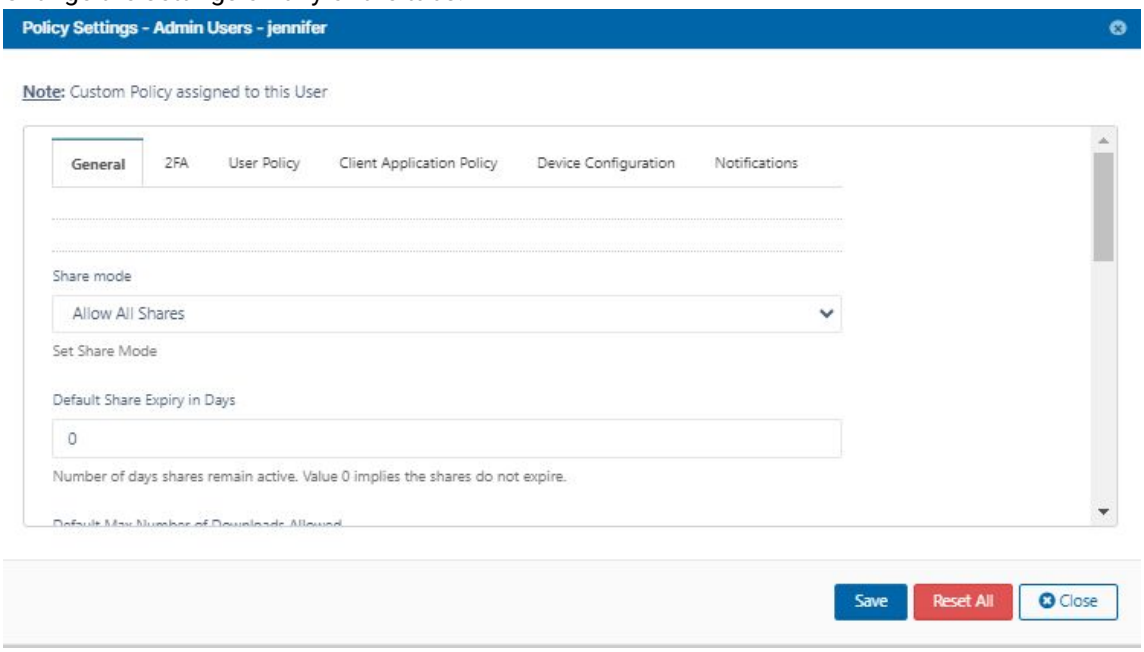
**Modifying a policy while managing a user**

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

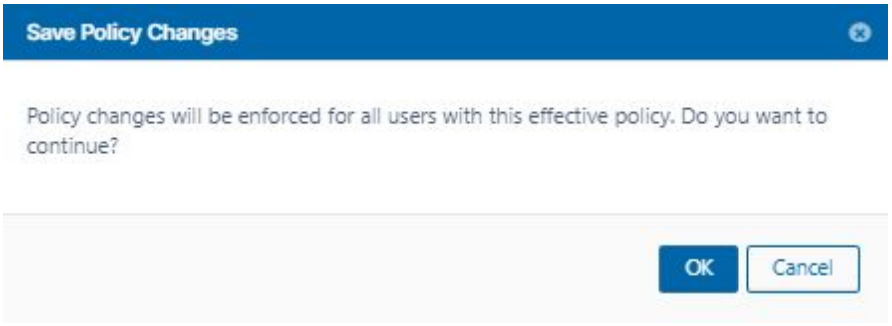
**To edit a policy from a user account:**

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

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




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




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

### Calculate the Effectiveness of a User's Policy

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

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

Learn more about Effective Policy Best Practices

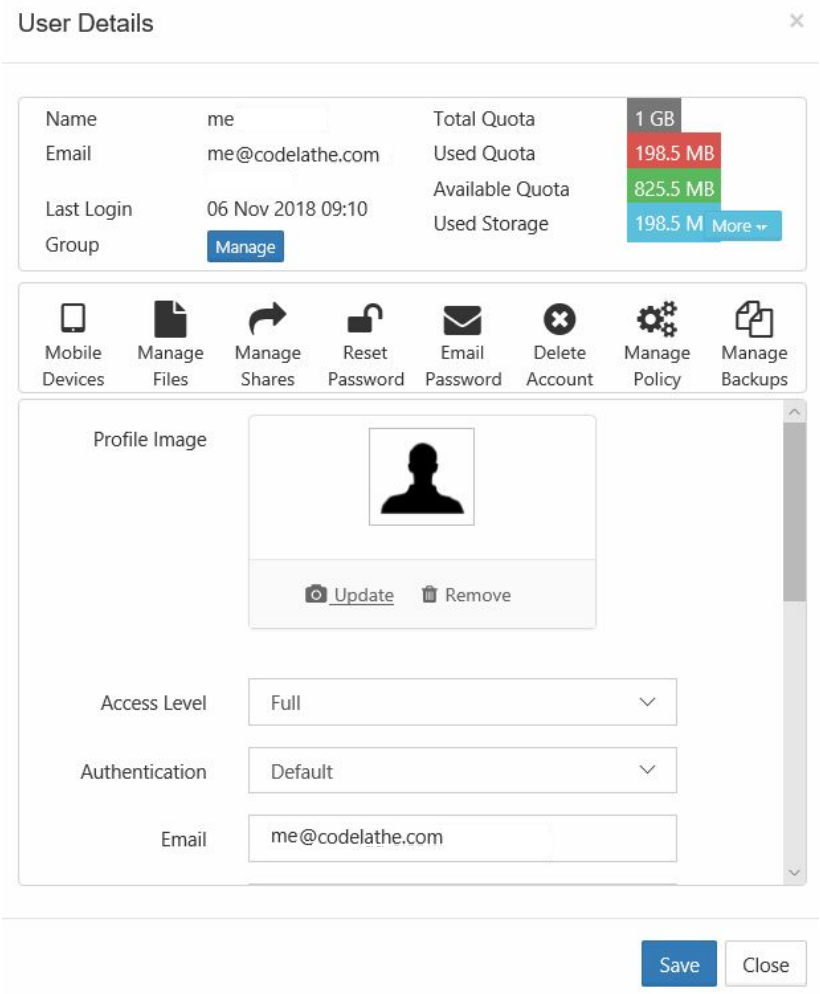
**To calculate the effectiveness of a policy for a user:**

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

## Manage a User's Profile Picture

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

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



To update a user's profile image:

1. Open a browser and log on to Admin Portal.
2. From the left navigation panel, click **Users**.
3. In the users list, click the row containing the user whose picture you want to change.
4. Click the **edit icon.**
5. Next to **Profile Image**, to add an image, click **Update**.
6. Next to **Profile Image**, to remove an image, click **Remove**.

## Change a User's Email Address

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

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

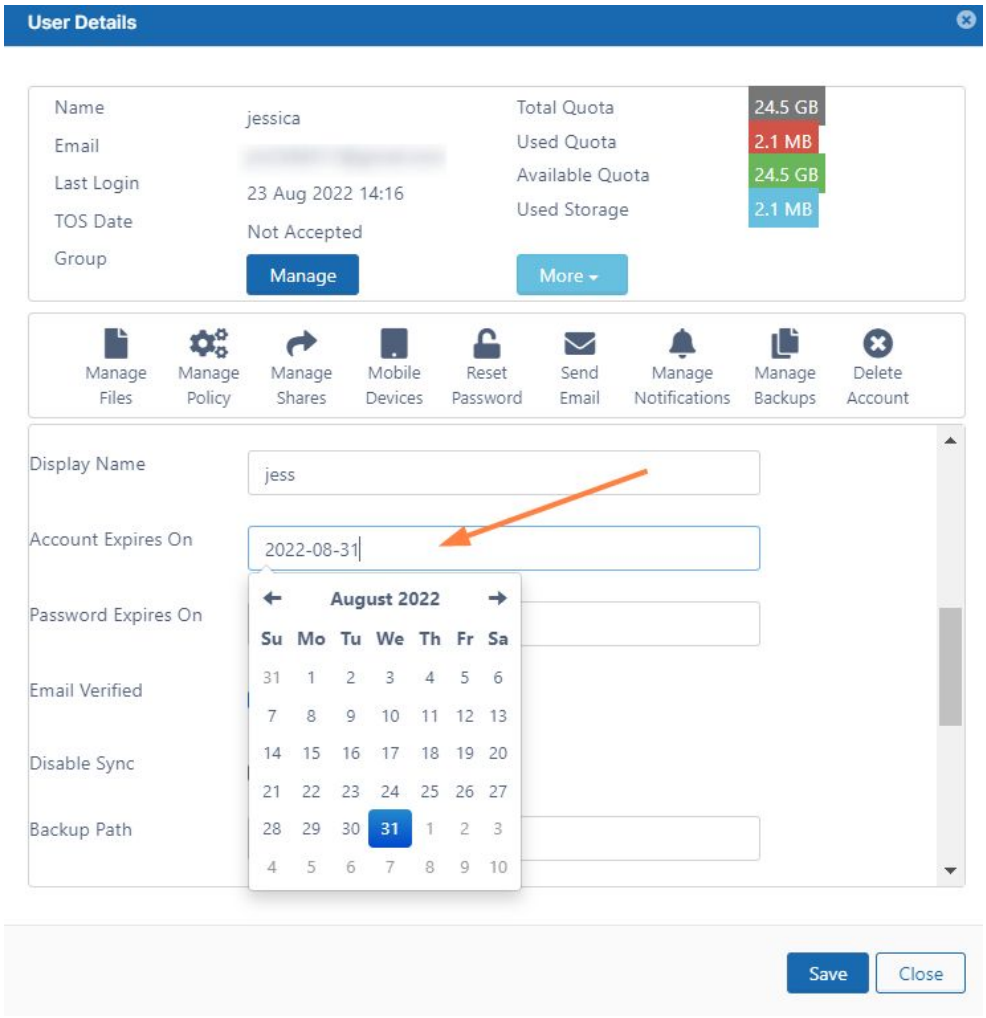
To change a user's email address:

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

## Setting a User Account to Expire

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

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




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

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

## Send Email from User Details

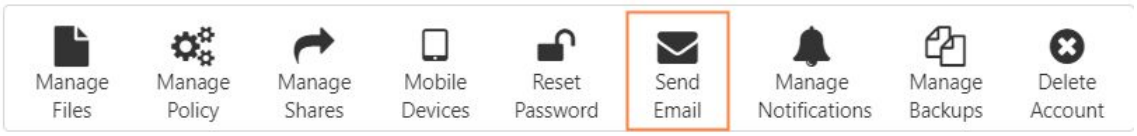
This option is available beginning in FileCloud 20.1

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

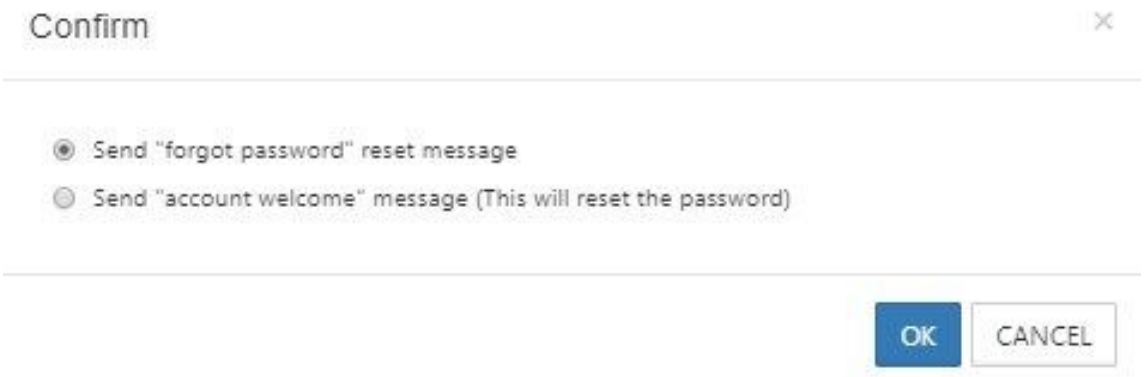
- A forgot password email that sends the user a password newly generated using the Reset Password option in User Details.
- An account welcome email that welcomes a new user to FileCloud. If the new user is not an AD user, the message includes a new password. If the new user is an AD user, the message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

To send an email from User Details:

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




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




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

# Managing Groups

A FileCloud Admin can manage User Groups.

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

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

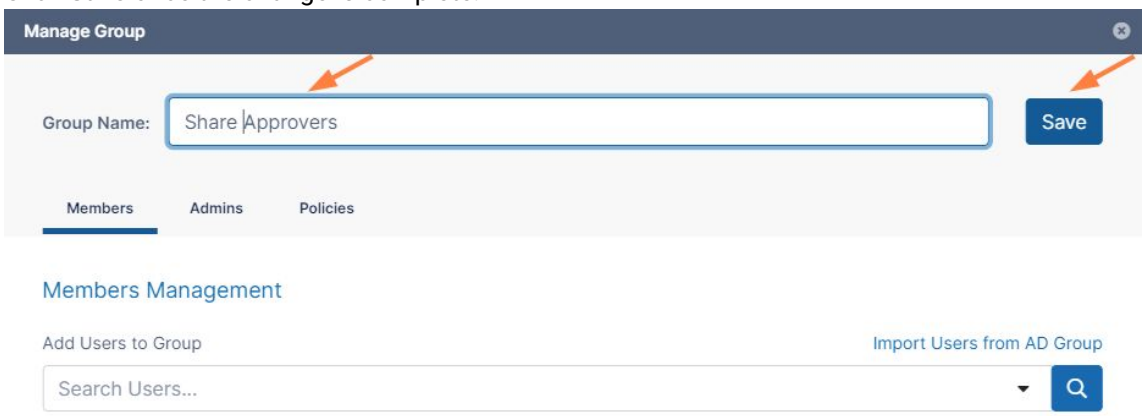
To add a group, see Group Settings.

## Change a User Group Name

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

**To change a group's name:**

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




## Delete a User Group

**To delete a group:**

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

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

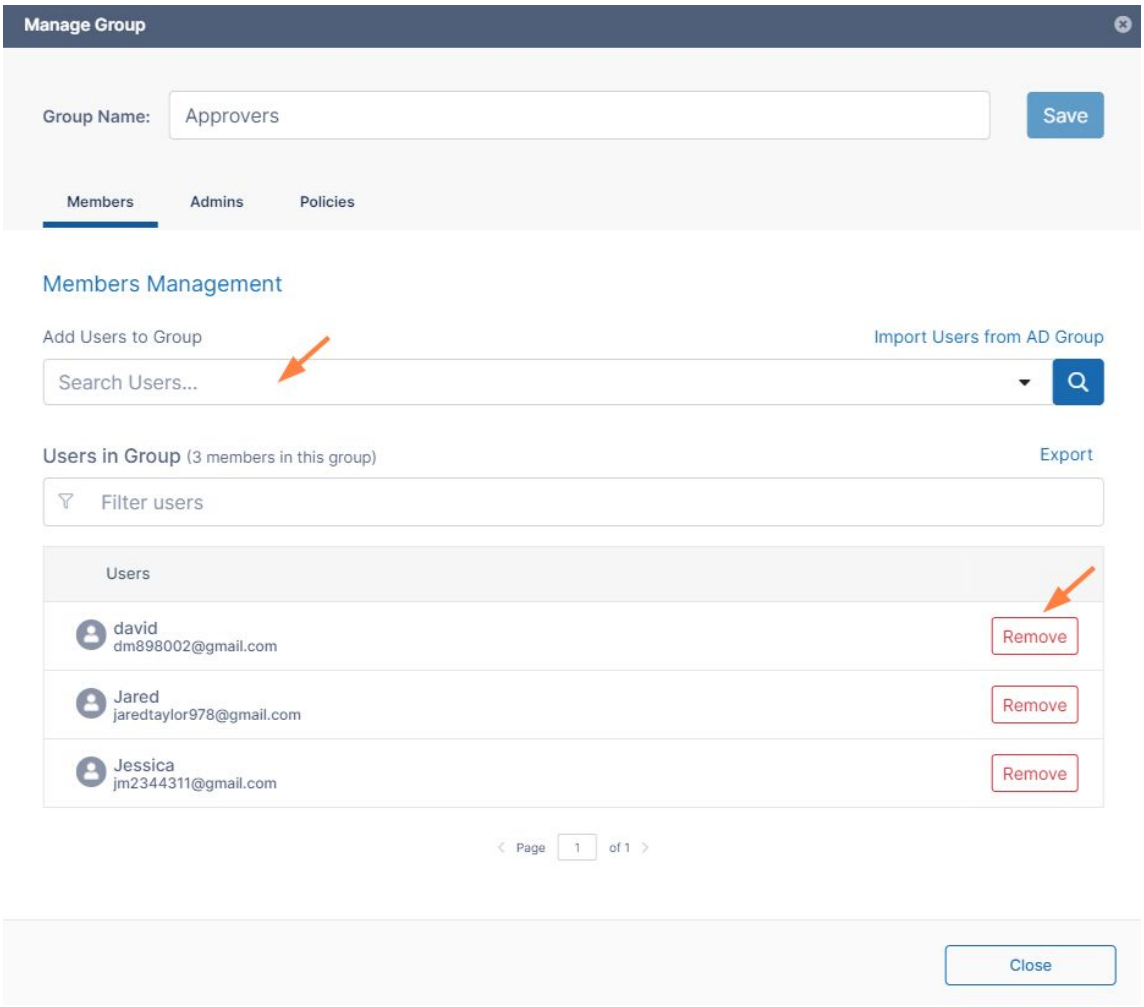
Once a group is removed, network shares shared with that removed group will no longer be available to the former members of the group

## View and Change Group Members

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

**To change a group's members:**

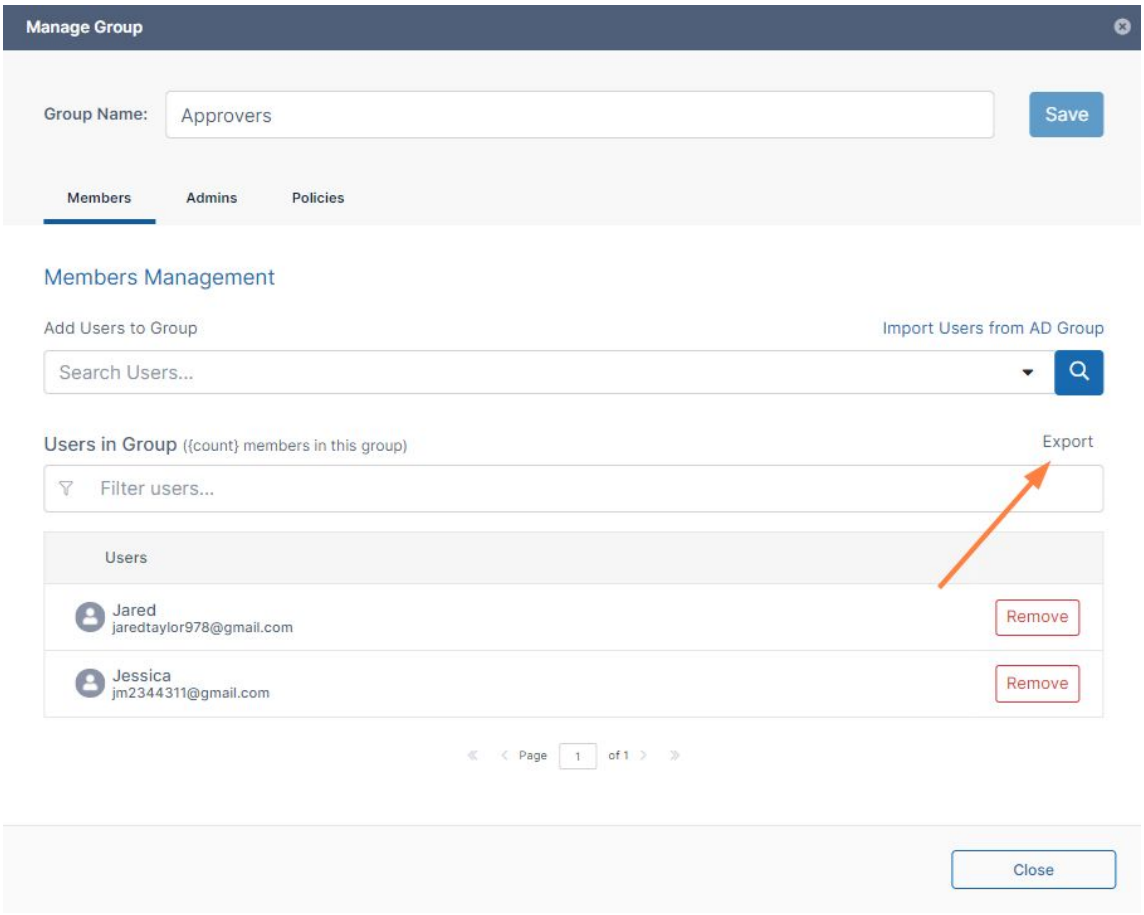
1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. In the **Members** tab, view the members of the group.
4. To add a member, enter an existing FileCloud user's name or email address in the search bar, and click **Add**.
5. To remove a user, click **Remove** next to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




## Exporting a list of users in a group

To export a list of users in a group:

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




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

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

## View and Change Group Admins

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

**To modify group admin settings:**

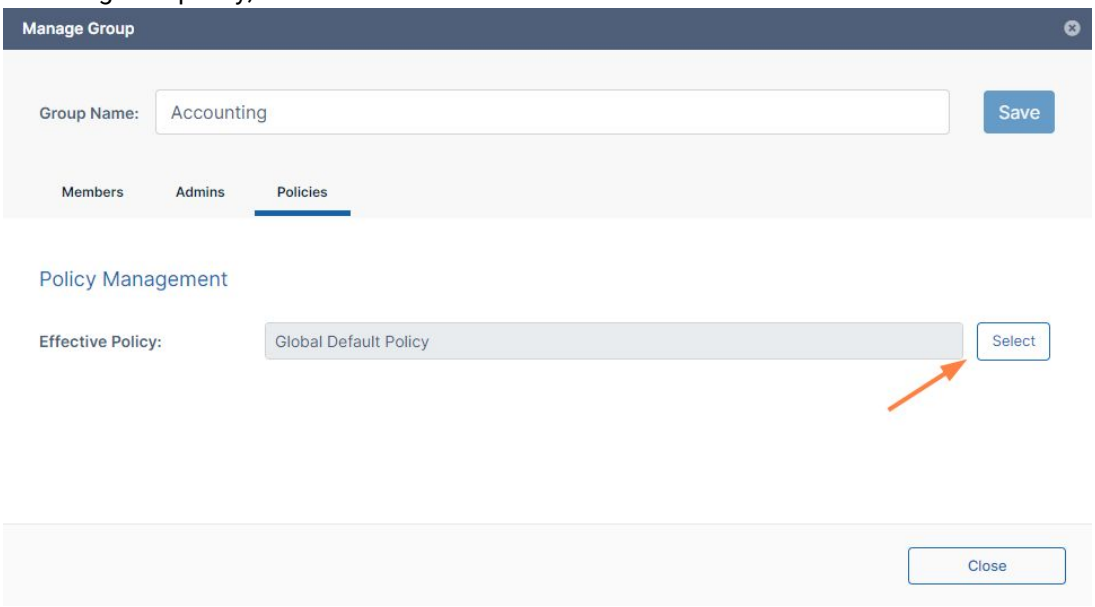
1. In the navigation panel, click **Groups.**
2. Click the Edit icon for the group.
3. In the **Admins** tab, view the admins of the group.
4. To add an admin, enter an existing FileCloud user's name or email address in the search bar, and click **Add**.
5. To remove an admin, click **Remove** next to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

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

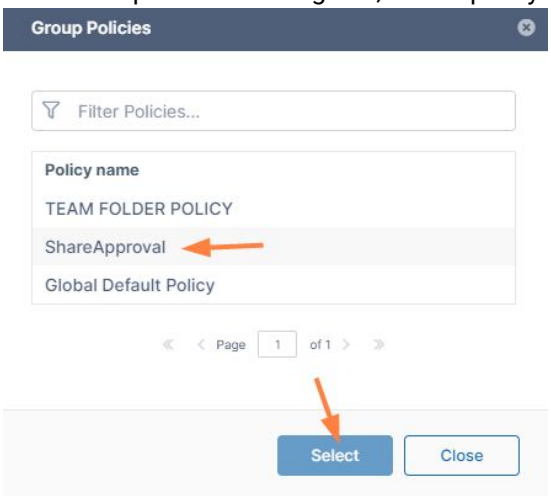
## View and Change a Group's Policy

**To change a group's policy**:

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




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




The policy is changed.

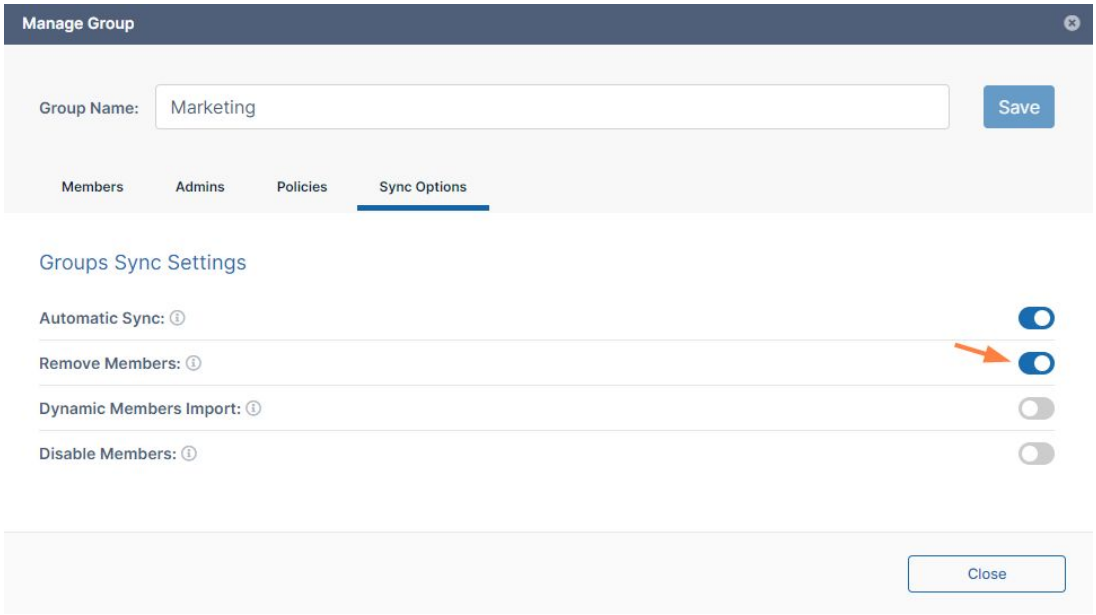
6. Click **Close**.

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

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

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

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




Their functions are as follows:

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

5. Click **Close**.

# Managing Admin Users

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

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

## Check an admin user's permissions

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

**To check all of a user's permissions:**

1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Check user permissions.**
   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.<br>**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, dreate, 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. *Note: The corresponding Folder Permission must be enabled to be able to perform a Team Folder operation.* |
| 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

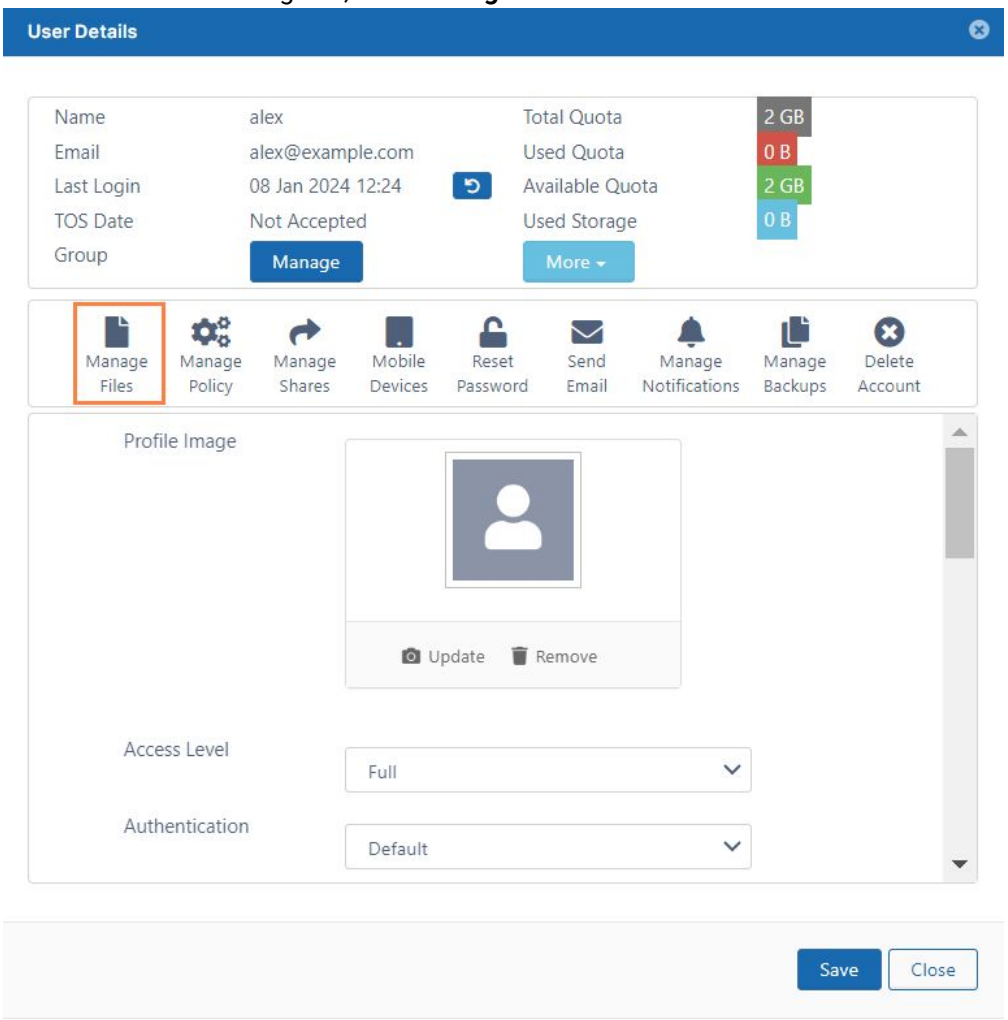
**How do I access user storage management settings?**

**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.**




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

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

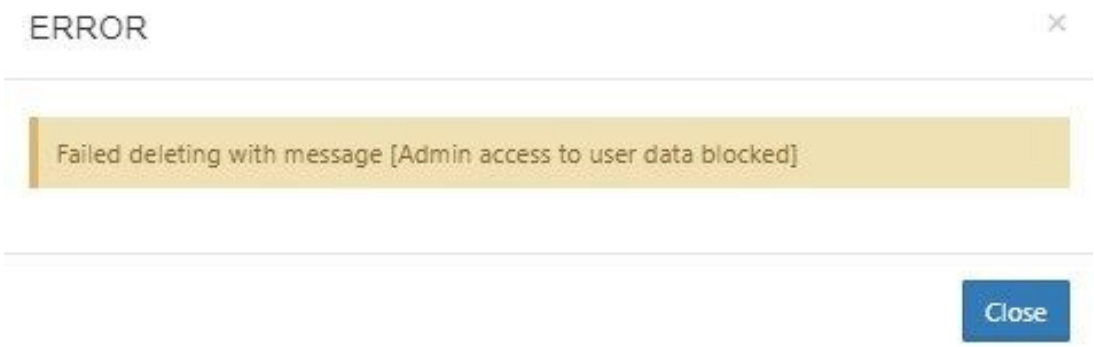
If you do not want the main administrator or admin users to have unlimited access to user files and folders, you can configure your system to prevent them from performing all of the following actions:

- 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 (see page 54)
- Copy and Move User Files (see page 57)
- Download User Files and Folders (see page 60)
- Cancel User Uploads in Progress (see page 63)
- Delete User Folders and Files (see page 64)
- Clear a Recycle Bin (see page 65)
- Remove a User's Old File Versions (see page 69)
- Remove Incomplete User Uploads (see page 70)
- Restore a Previous File Version (see page 71)
- Critical Section Cleanup Tool (see page 74)
- Change the Name of the Zip File for Multiple File Downloads (see page 77)


## Add Folder-Level Permissions to User Folders

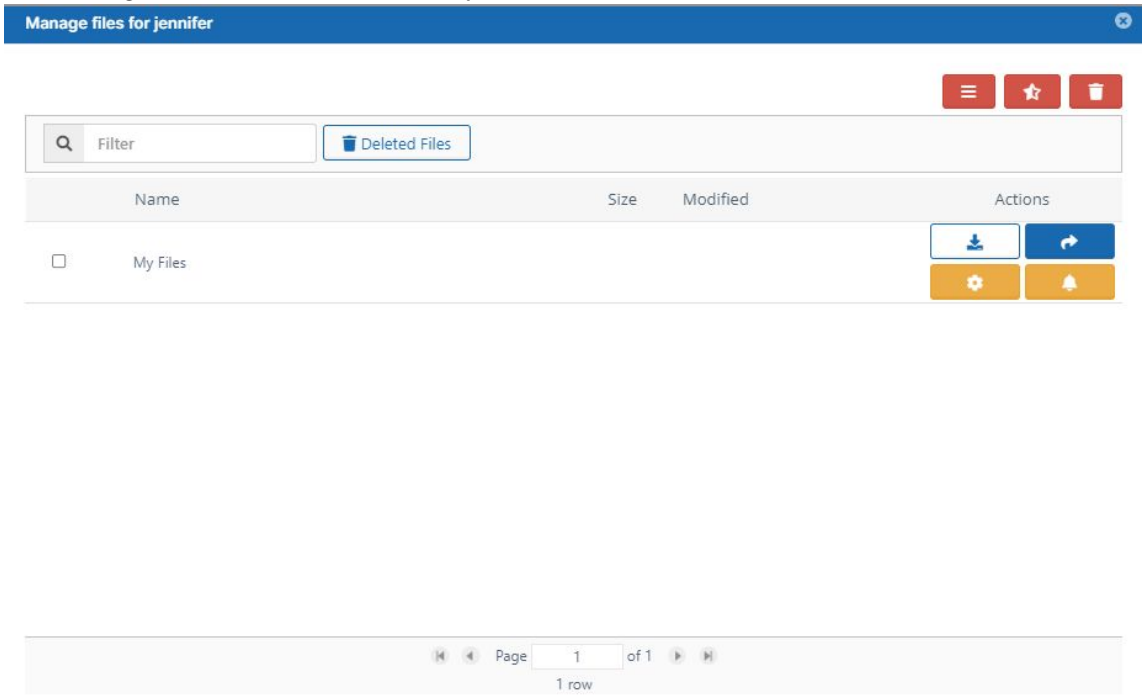
Folder-level permissions are permissions that are applied directly to a folder. They add additional restrictions to the share permissions when the folder is shared. Note that whatever is more restrictive, folder-level or share permissions, apply. For more information, see Folder-Level Permissions.

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

**To assign folder-level permissions to users' folders:**

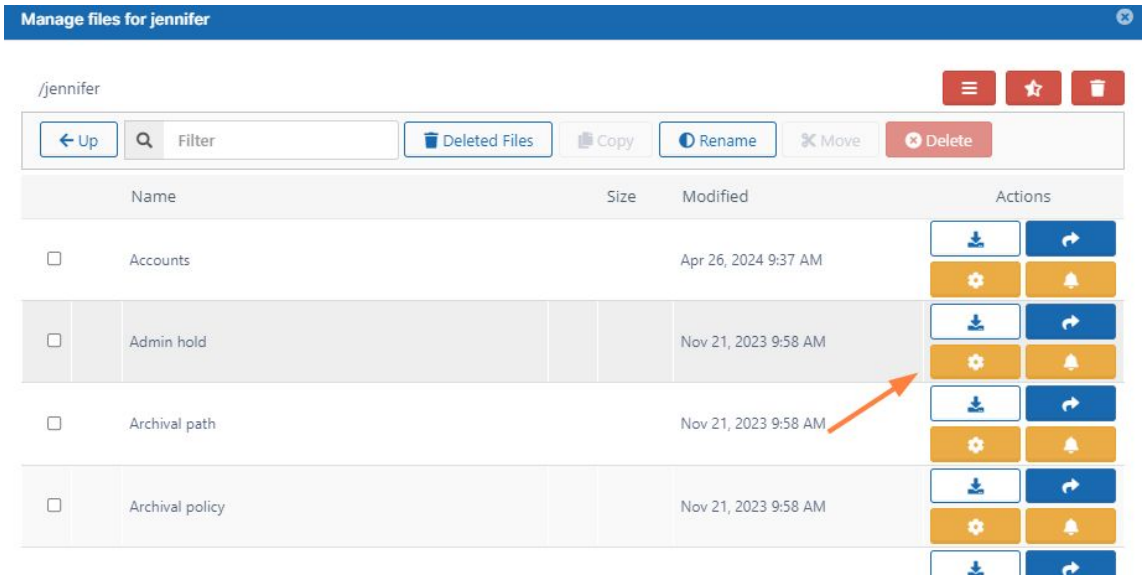
1. In the admin portal's left navigation panel, click **Users**.

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



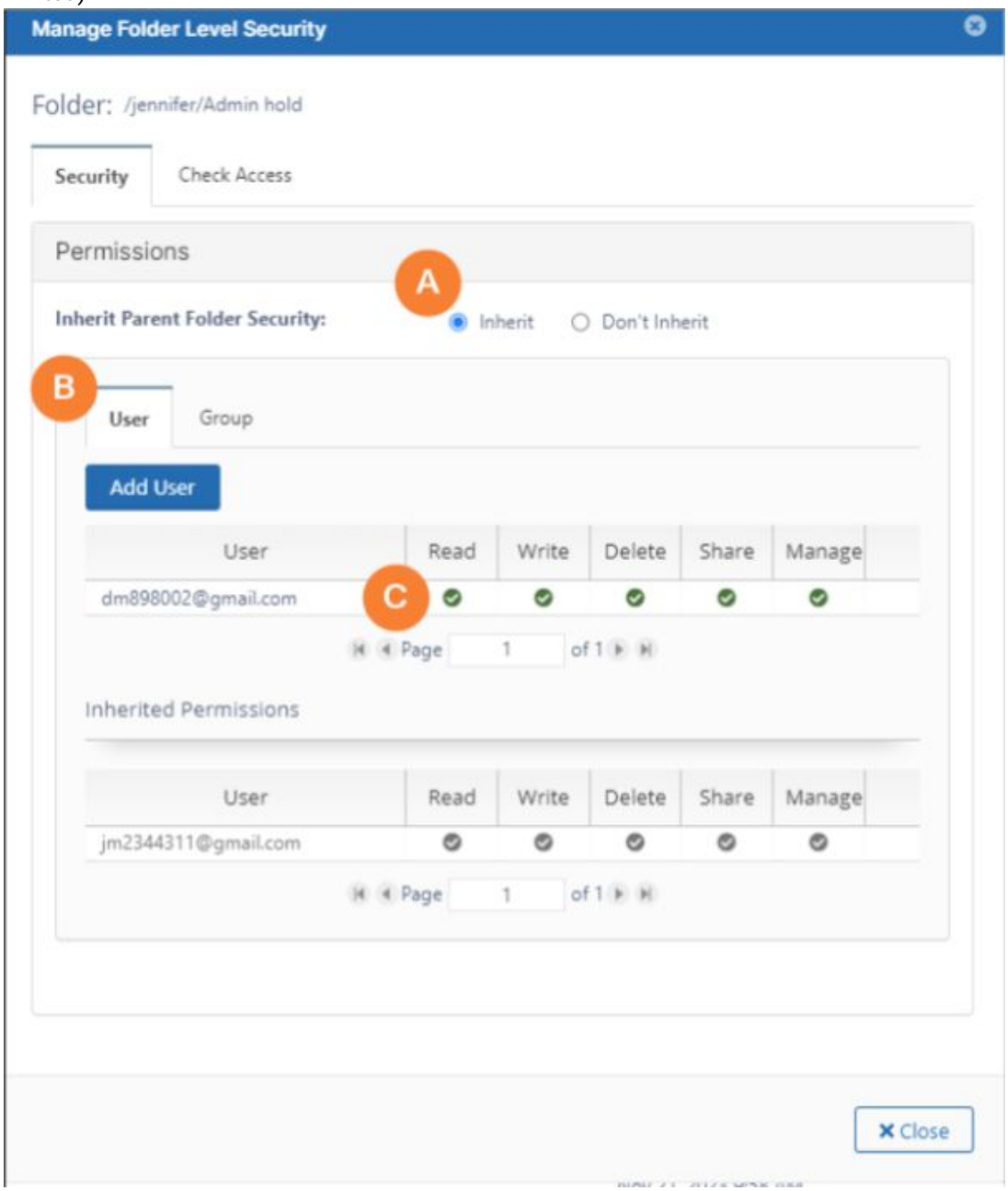

4. Expand **My Files** and locate the folder that you want to set folder-level permissions for.
5. Click the **Manage Access**

   button in the folder's row.




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

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




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

# Copy and Move User Files

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

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

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

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

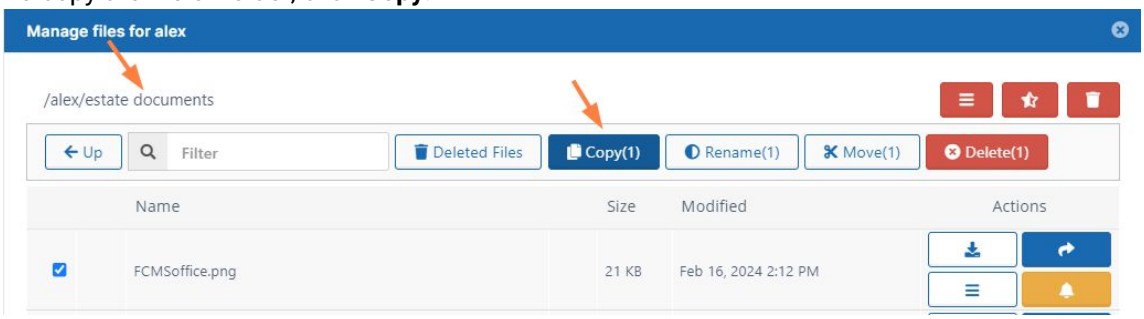
**What is the difference between copy and move?**

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

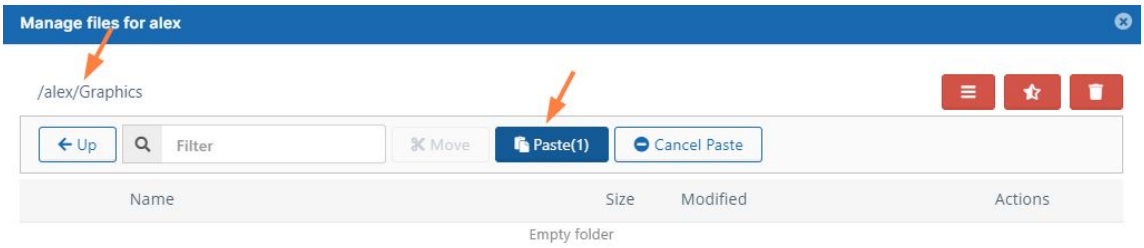
Moving a file will allow you to put the file in a new location so it can be removed from the original location.

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

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

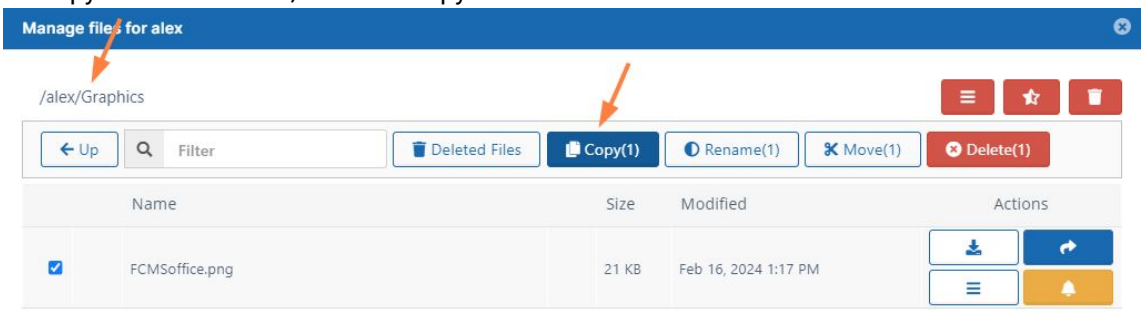



8. Navigate to the folder where you want to paste the copy.
9. Click **Paste**.

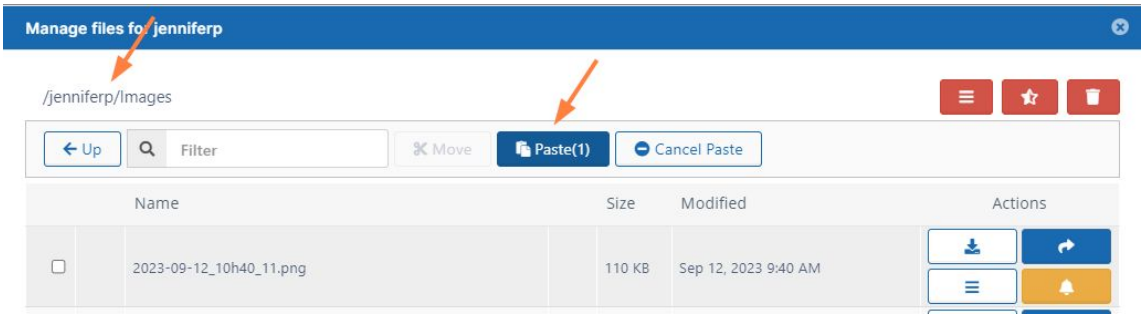



**To copy and paste files and folders between folder locations for two different user accounts:**

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files.**
   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 the Copy button.

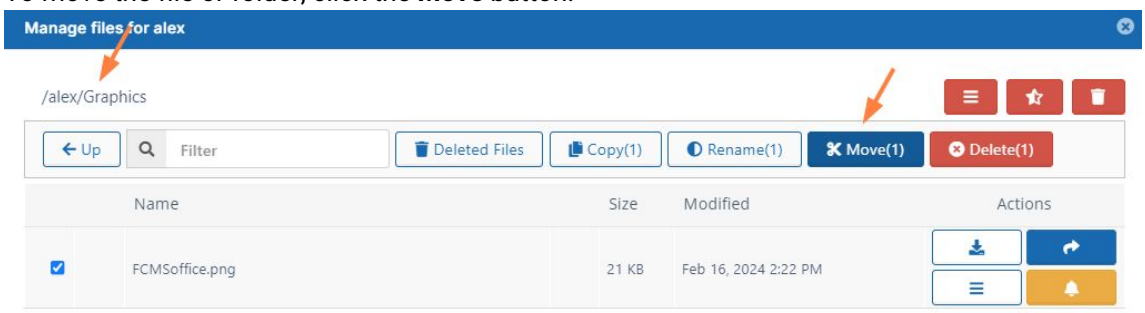



8. To close the window, in the top right corner, click the x button.
9. On the Manage Users page, select the user who wants a copy of the file or folder, and then click the Edit icon.
10. On the User Detail dialog box, click **Manage Files.**
    The Manage Files for <User> window opens.
11. Navigate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

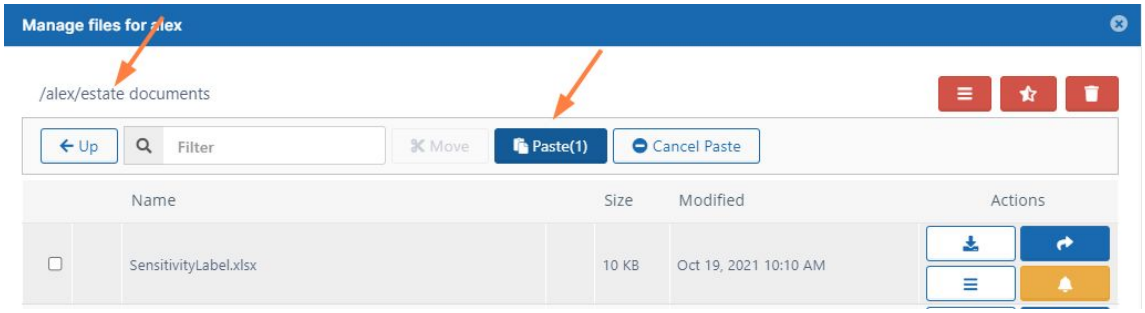


### To move and paste files and folders between folder locations for the same user account:

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

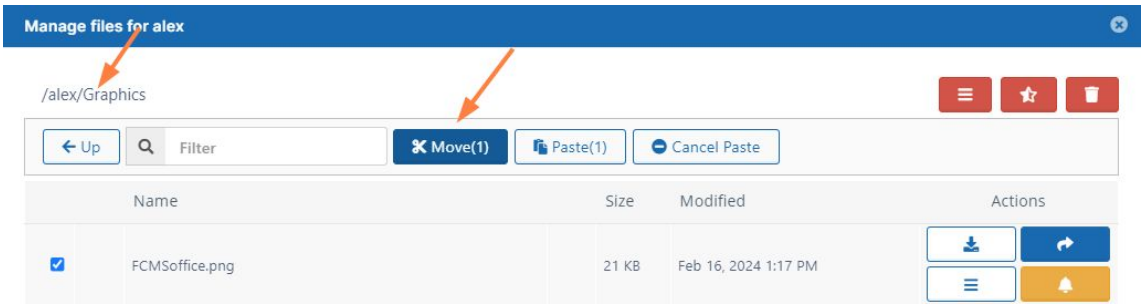



8. Navigate to the folder where you want to paste the original file or folder.
9. Click **Paste**.

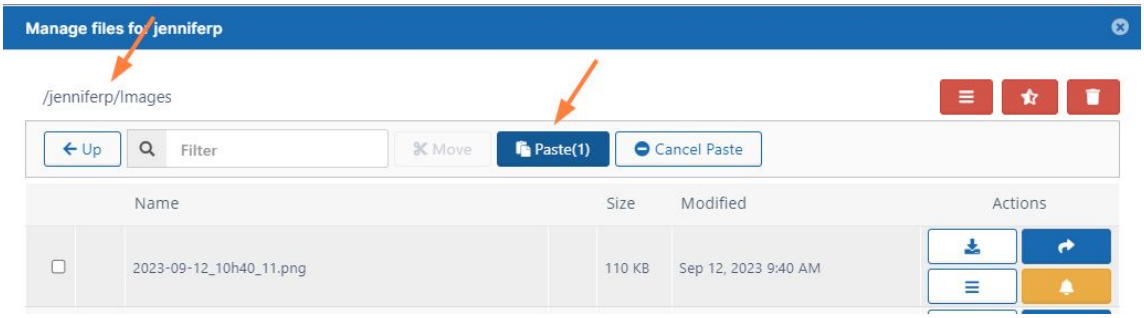



### To move and paste files and folders between folder locations for two different user accounts:

1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon.
4. On the User Detail dialog box, click **Manage Files**.
   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. To close the window, in the top right corner, click the x button.
9. On the Manage Users page, select the user who wants the file or folder, and then click the Edit icon.
10. On the User Detail dialog box, click **Manage Files.**
    The Manage Files for <User> window opens.
11. Navigate to the folder or file where you want to paste the original.
12. Click **Paste**.




# Download User Files and Folders

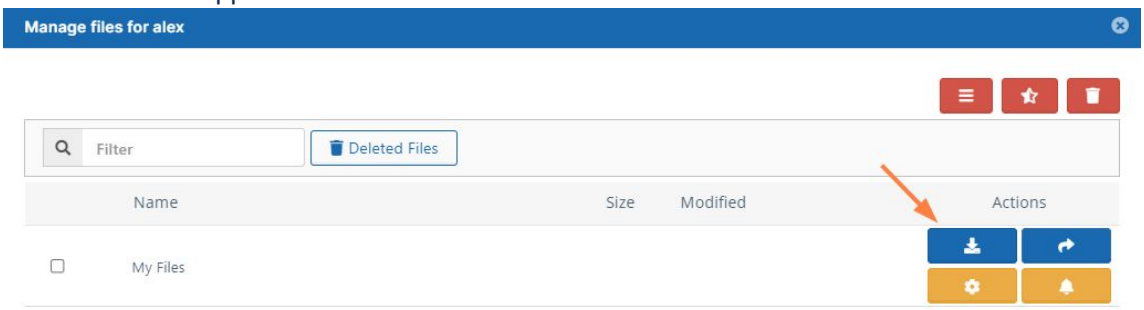
To disable users' ability to download folders from the user portal, see the setting **Disable Folder Download** at General Customization.

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.

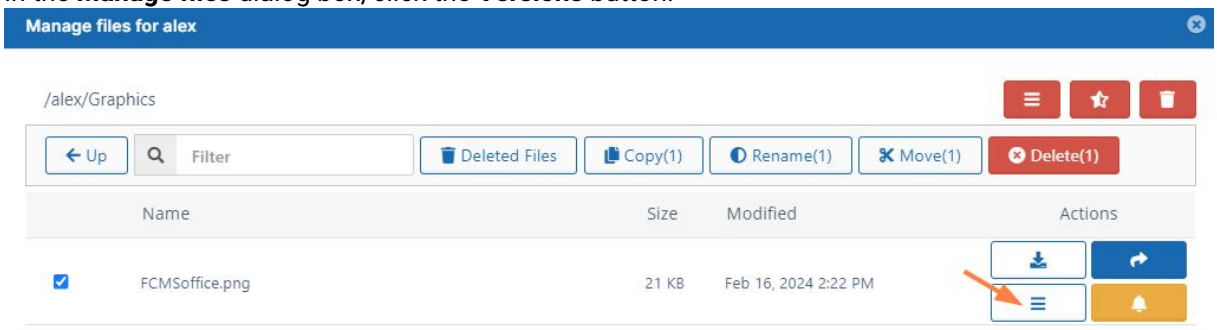



**Can I download an older version of a file?**

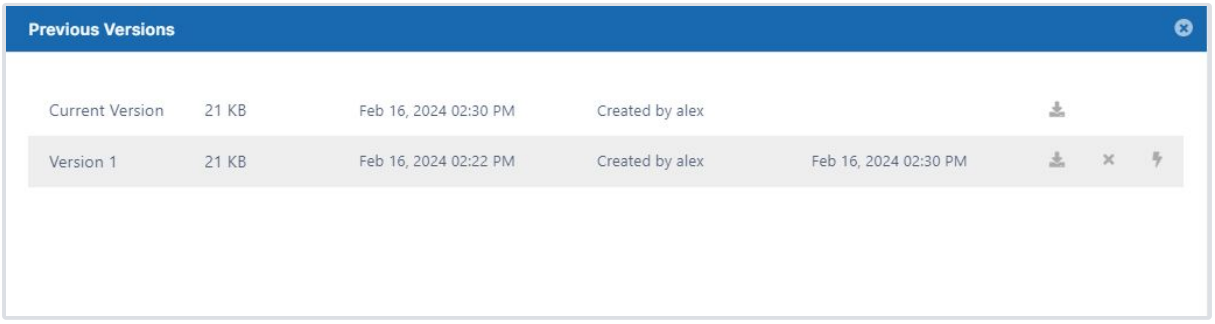
If the user has uploaded changes to a file, you can:

- 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.



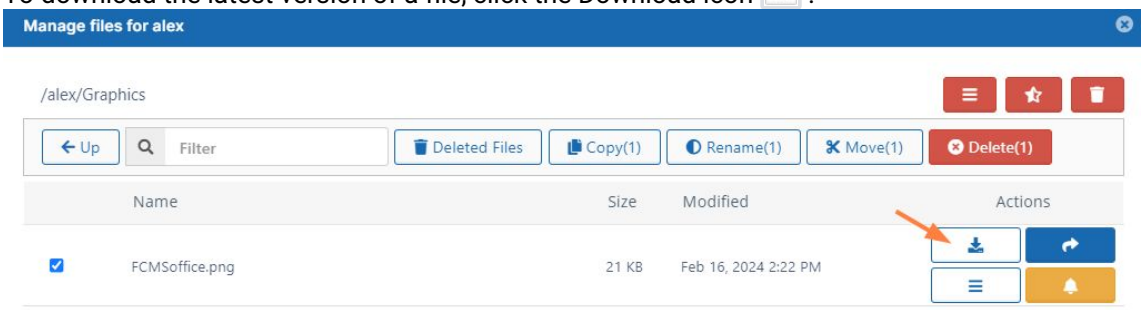

If you have older versions on your site, you may:

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

**To download user folder and files:**

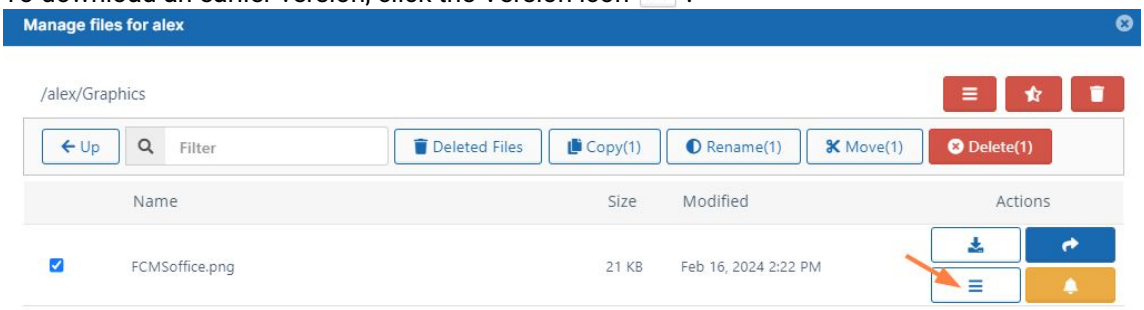
1. Open a browser and log on to the Admin Portal.
2. From the left navigation menu, select Users.
3. On the Manage Users page, select a user, and then click the Edit icon .

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 .

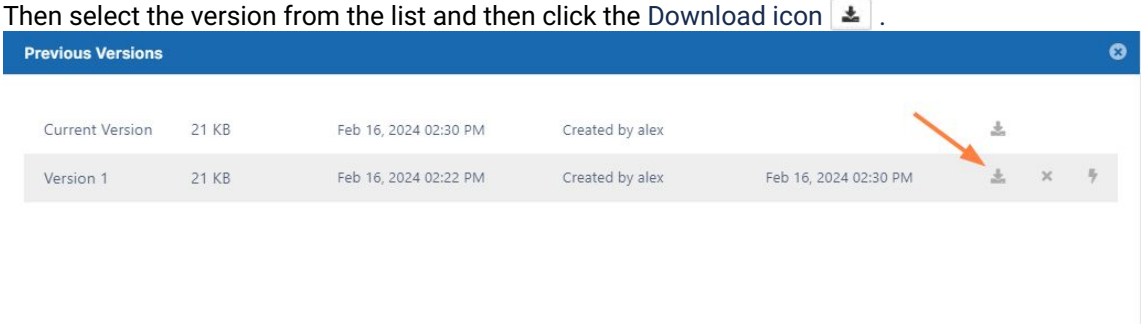



**OR**

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"

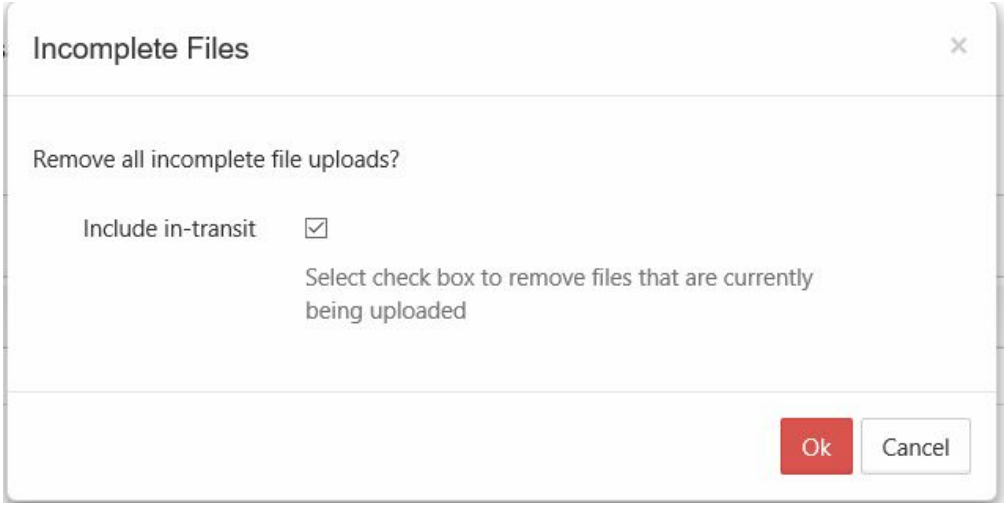
- Cannot be undone

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.

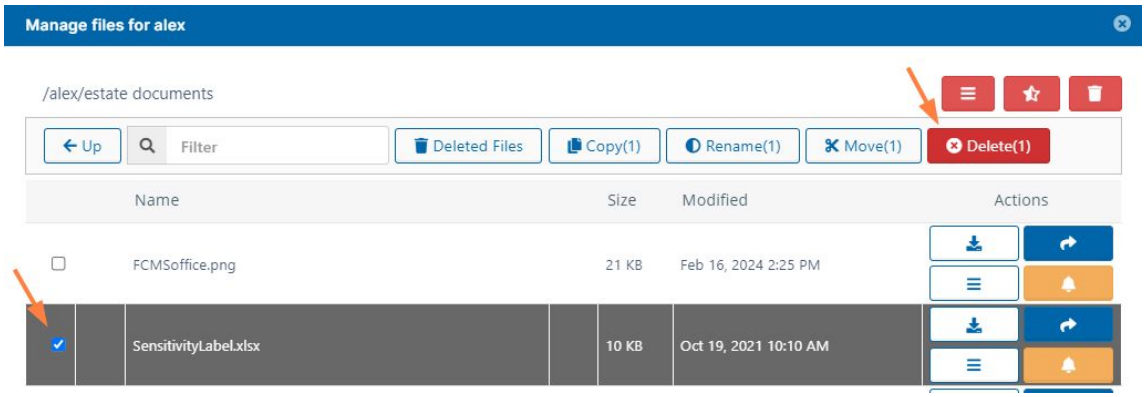
This allows you to protect and maintain your system in the following ways:

- 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 if from the recycle bin.

### To delete files and folders:

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




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

## Clear a Recycle Bin

⚠ This action:

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

As an administrator, you can delete a user's files and folders (see page 64).

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

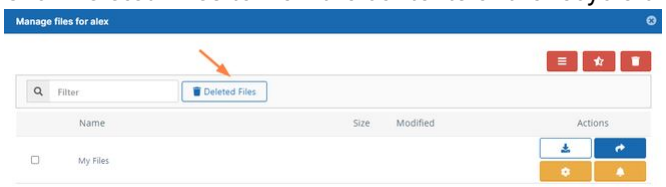
- If you have a policy that stores deleted files, they are saved in the Recycle Bin
- This means that they can be recovered if deleted by mistake or are needed again at a later time
- You can also set the Recycle Bin to automatically delete through a policy

Manage the Recycle Bin Using a Policy

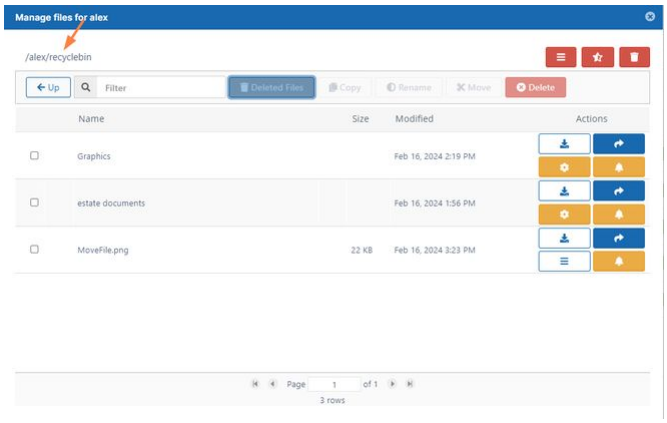
**Go the the recycle bin**

**To go to a user's recycle bin:**

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



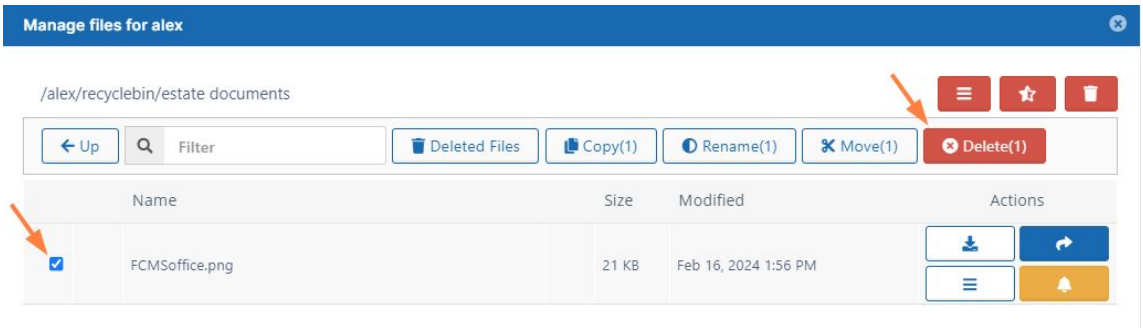

The recycle bin opens and displays deleted files. If the deleted files are in subfolders, navigate into the subfolders to locate them.




**Clear a deleted file or folder**

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

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



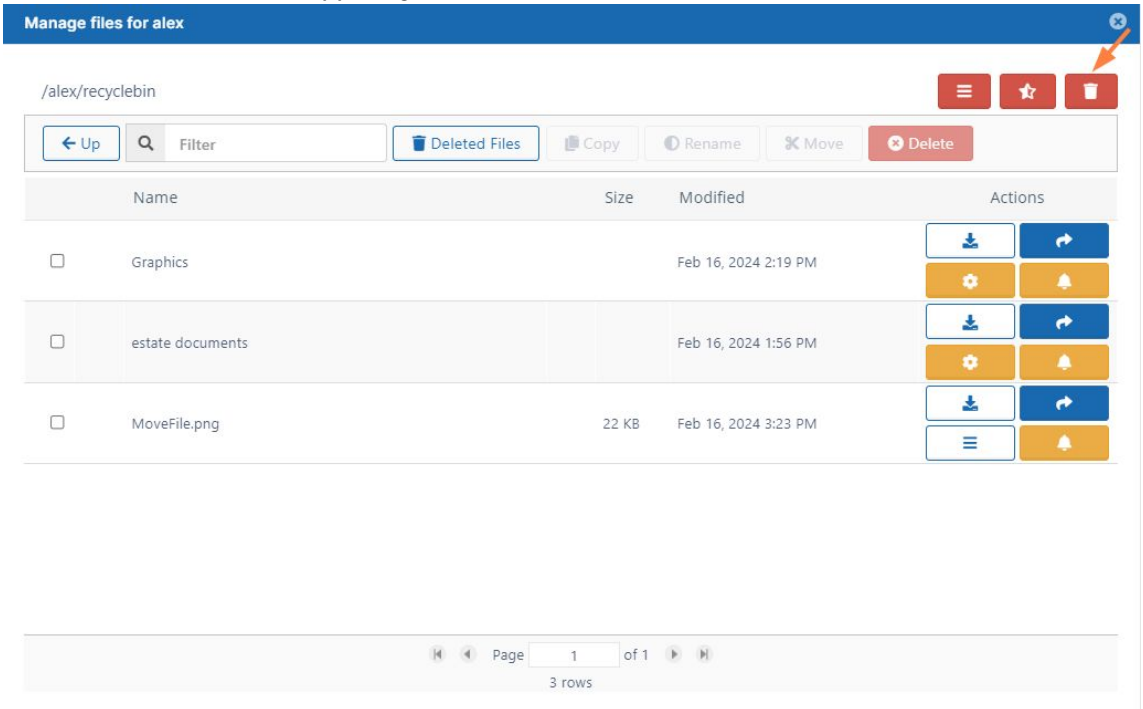

4. Click **Delete**.
5. In the **Confirm** dialog box, click **Yes**.
   The file or folder is deleted from the recycle bin (permanently removed from FileCloud).

### Clear all deleted files

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

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

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




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

### 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

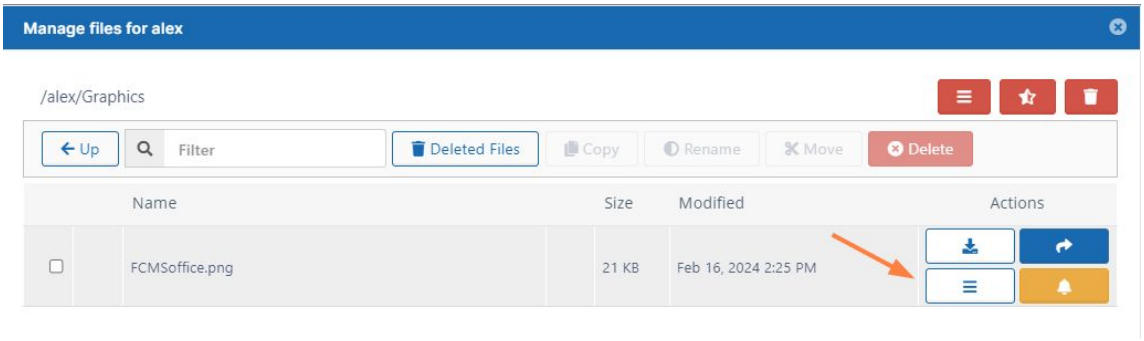
As an administrator, you can delete older versions of files that are stored on your FileCloud Server site.

- 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.

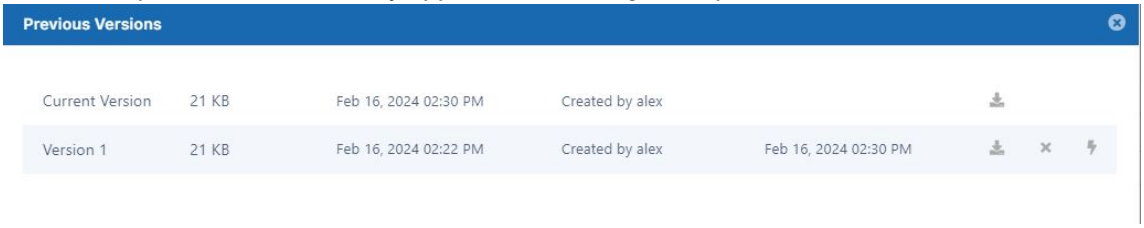
💡 This action does not remove the current version of a file, only all older versions saved on the FileCloud Server.

**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.

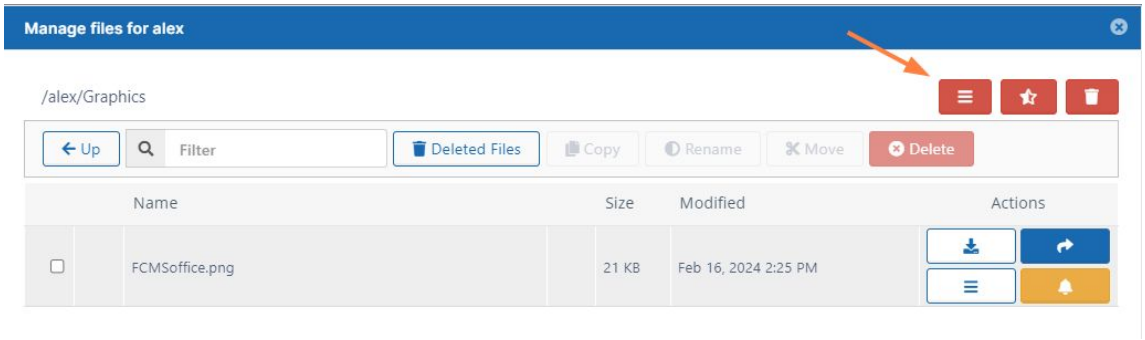



If there are previous versions they appear in the listing that opens:



**To remove all old versions of a file:**

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




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

## Remove Incomplete User Uploads

⚠ This action:

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

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

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

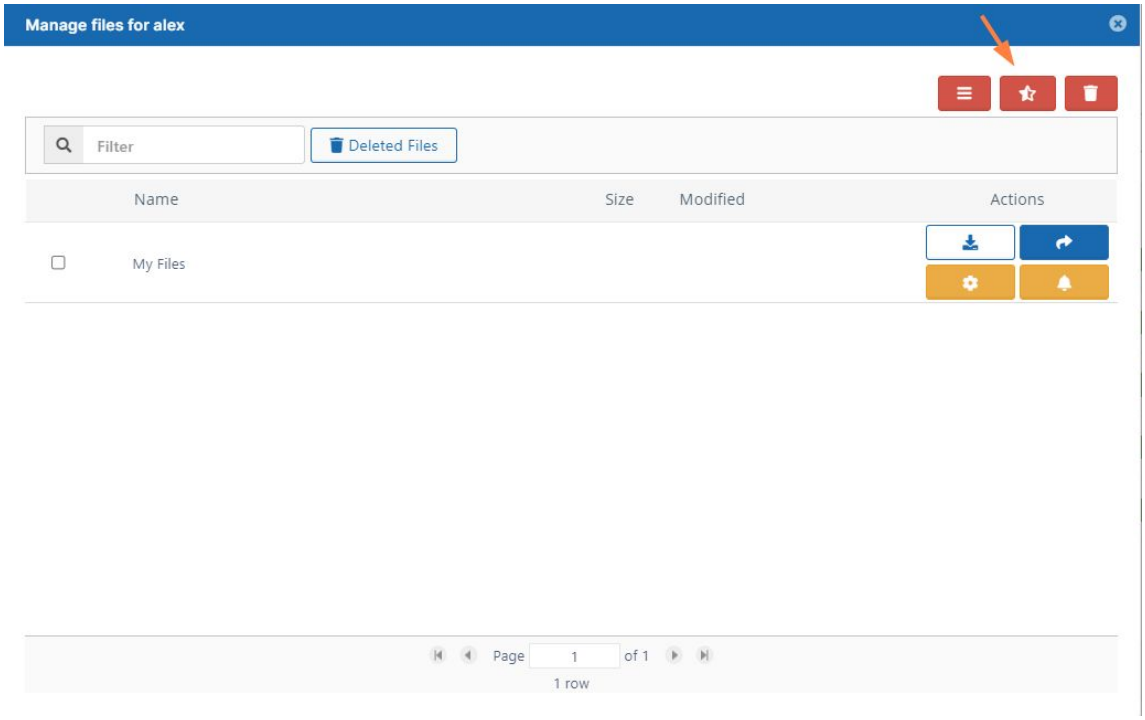
- Partial uploads are saved in case a network connection is lost and the user wants to continue the upload when connectivity is restored.
- Incomplete user uploads are never shown in the Manage Files listing.
- Over a period of time, these partial uploads can occupy lots of space.
- Admins can easily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

💡 If a file upload is in progress:

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

Cancel a Partial Upload (see page 63)

**To remove all incomplete user uploads:**

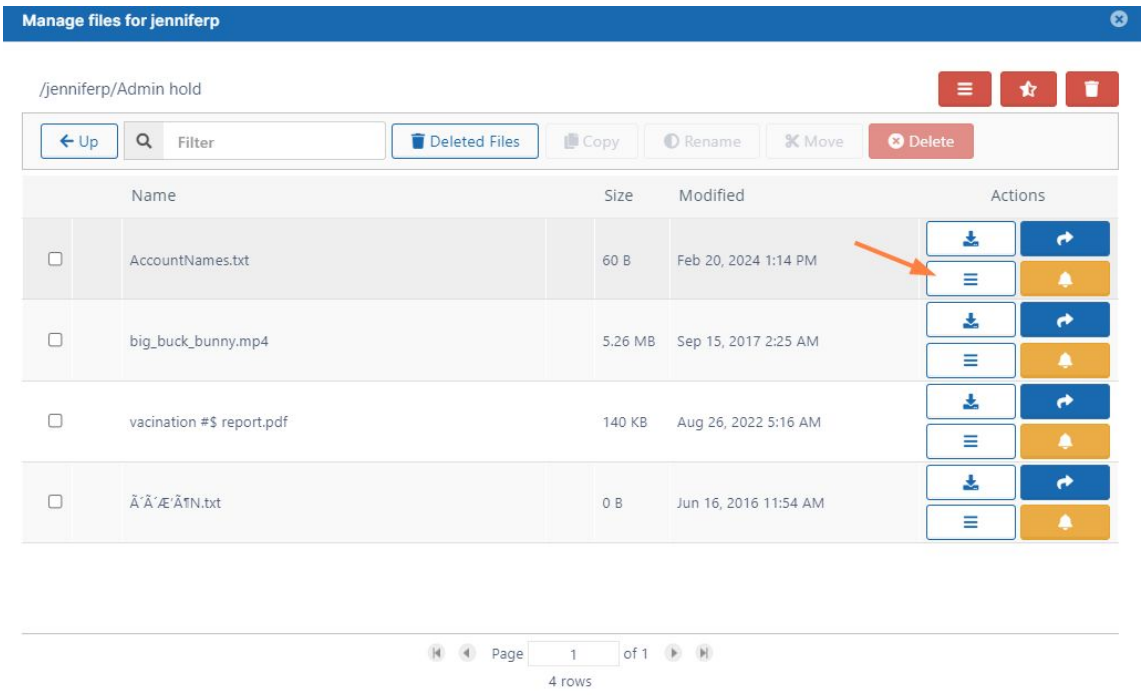
1. Open a browser and log in to the admin portal.
2. From the left navigation menu, select **Users**.
3. On the **Manage Users** page, select a user, and then click the Edit icon.
4. In the **User Detail** dialog box, click **Manage Files.**
   The **Manage Files for <User> window opens.**
5. Click the Remove All Incomplete Uploads icon
   
   .
   
   
6. On the **Incomplete Files** dialog box, to also remove incomplete uploads in progress, select Include in-transit.
7. Click **OK**.
   Incomplete downloads are removed.

## Restore a Previous File Version

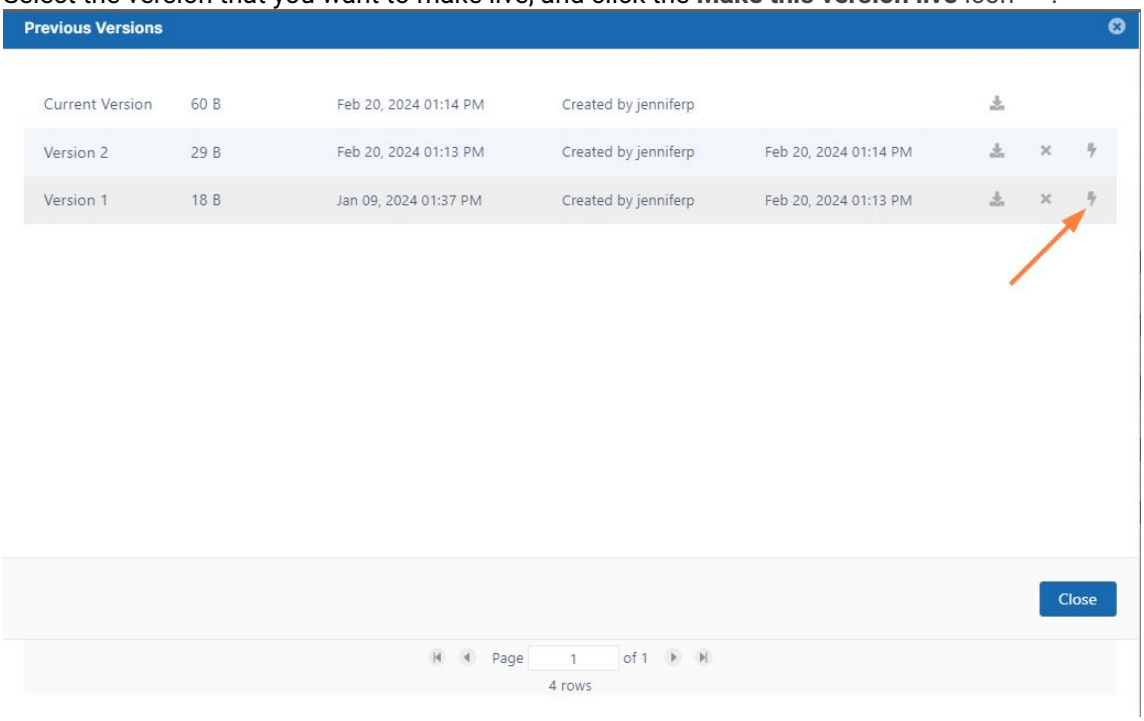
If a user has uploaded changes to a file, you can restore the previous version of a file and make it live.

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

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



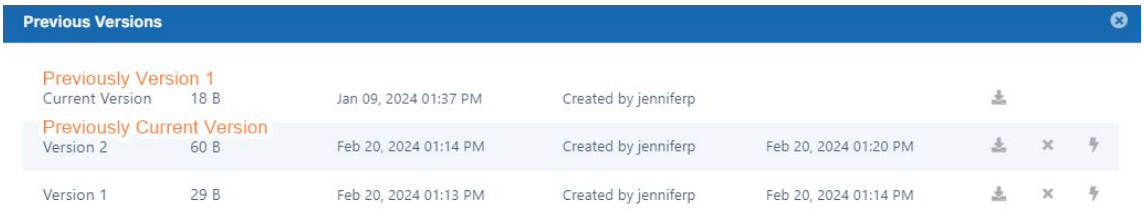
7. Select the version that you want to make live, and click the **Make this version live** icon .




The following confirmation box appears.

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

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




# 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[2] is optional and indicates the hostname if you want to look at a host other then 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**:

2. http://multitenant.site2-name.com

-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)
>>> -9999999999999999999
```

## 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');
```

:

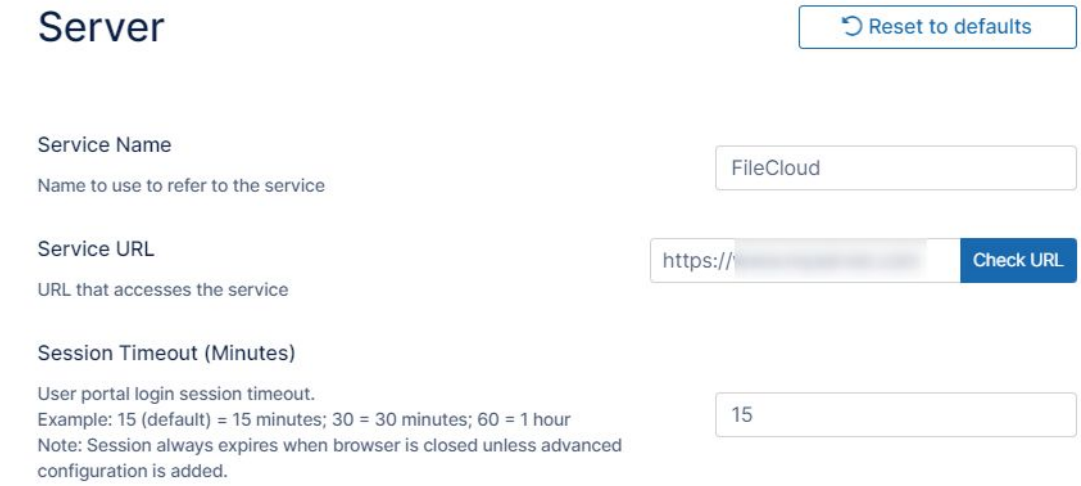
## Change the Name of the Zip File for Multiple File Downloads

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>**.

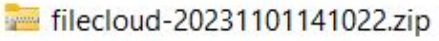
**Service Name** is used to refer to your FileCloud server throughout your system, on the user interface and in email messages and other notifications as well as in the download zip file name. By default, its value is FileCloud.

**To change the Service Name**:

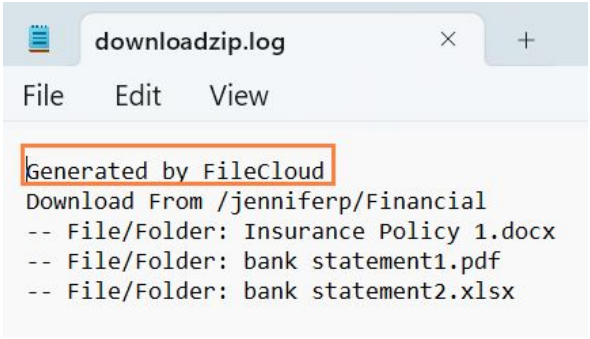
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server** .
   The **Server** settings page opens.




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

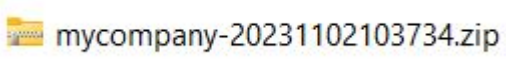



   and **downloadzip.log** has the line **Generated by FileCloud**:

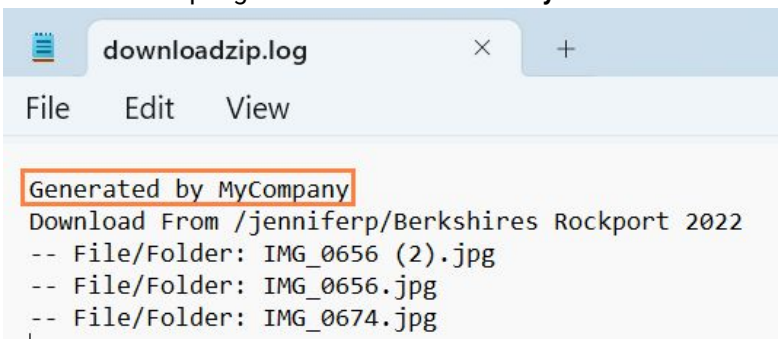



2. Change the value in **Service Name** to your own name for your server:

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




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



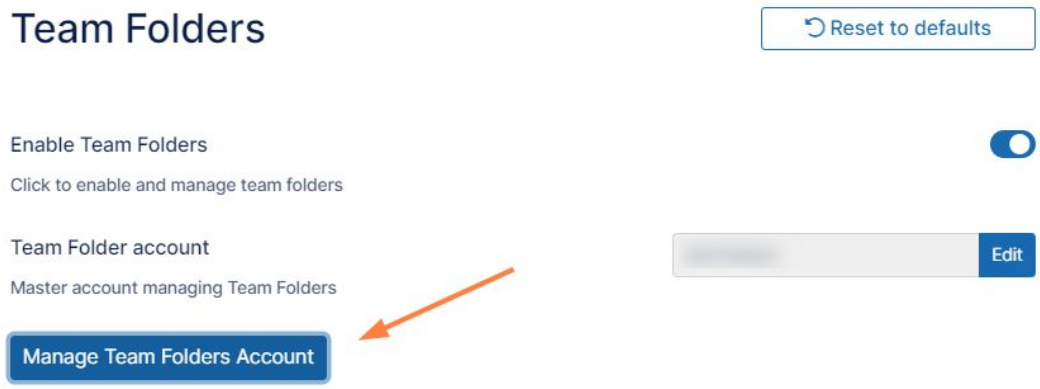
# Managing Team Folders

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

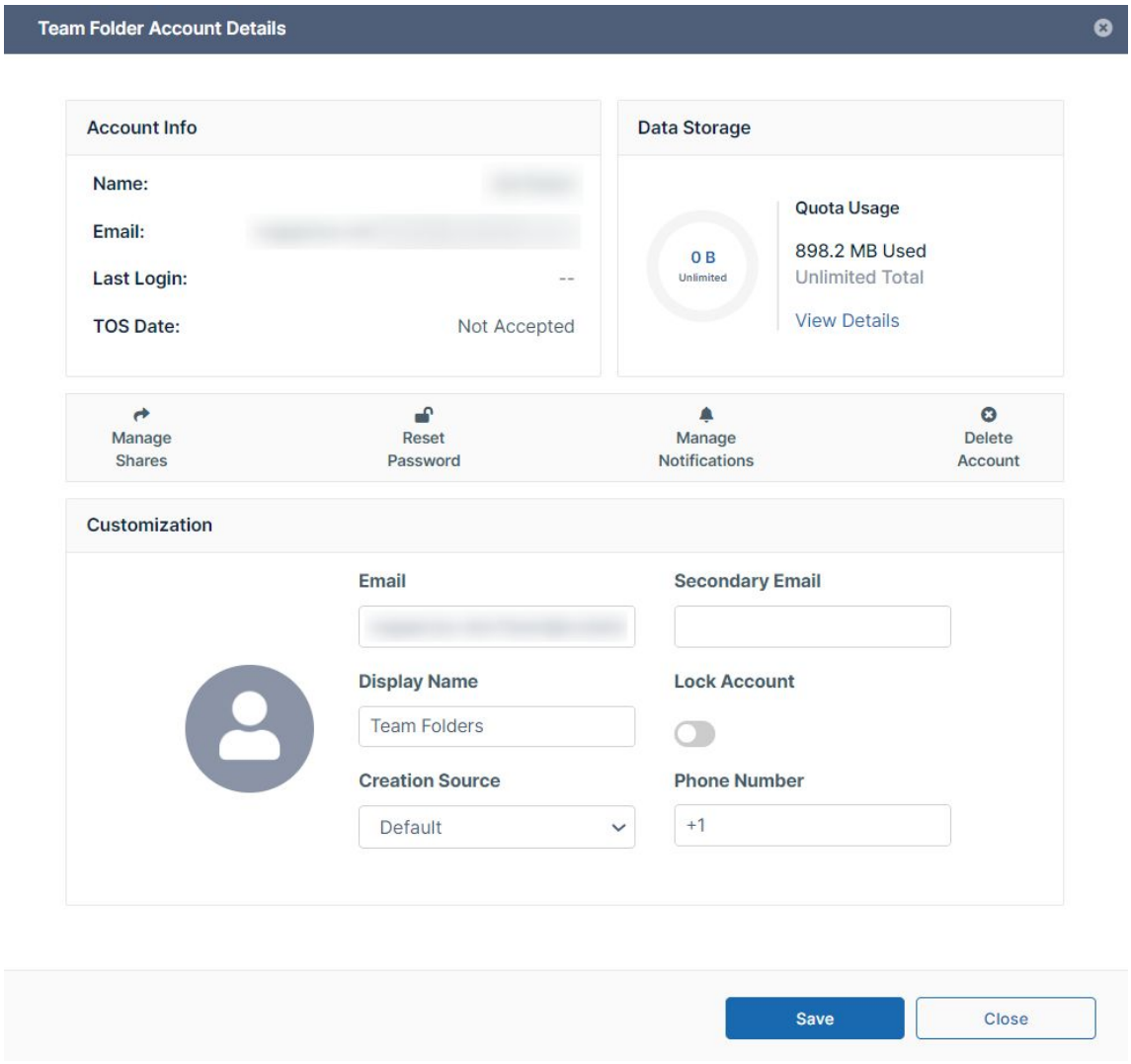
To access the **Team Folder Account Details**, you must have already set up your Team Folders account. If you have not set it up yet, see Configure the Team Folders Account.

**To manage and view details of Team Folders**:

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

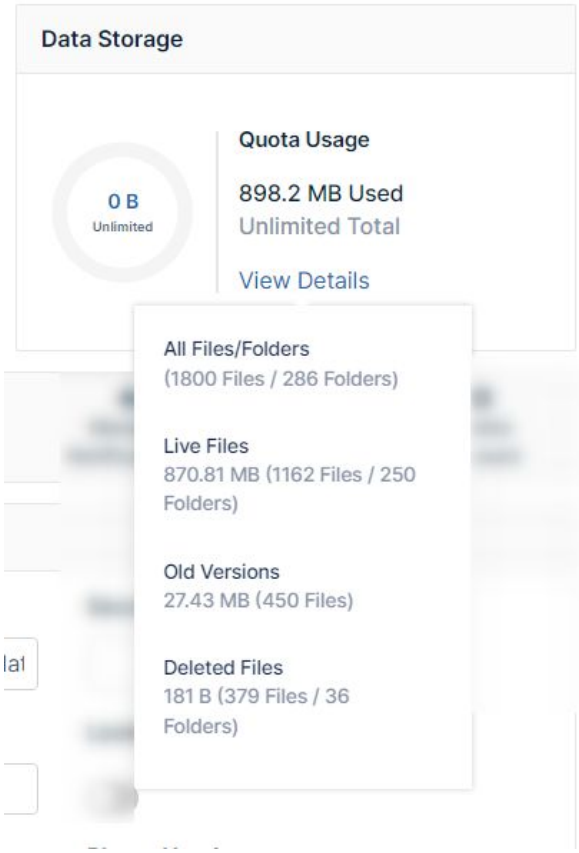



2. To see details of the Team Folders account, click **Manage Team Folders Account**.
   The Team Folder Account Details dialog box opens.
   The dialog box gives you account and data information, and enables you to manage Team Folder shares and notifications, reset the Team Folder account password,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


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

## To view the breakdown of data in Team Folders:

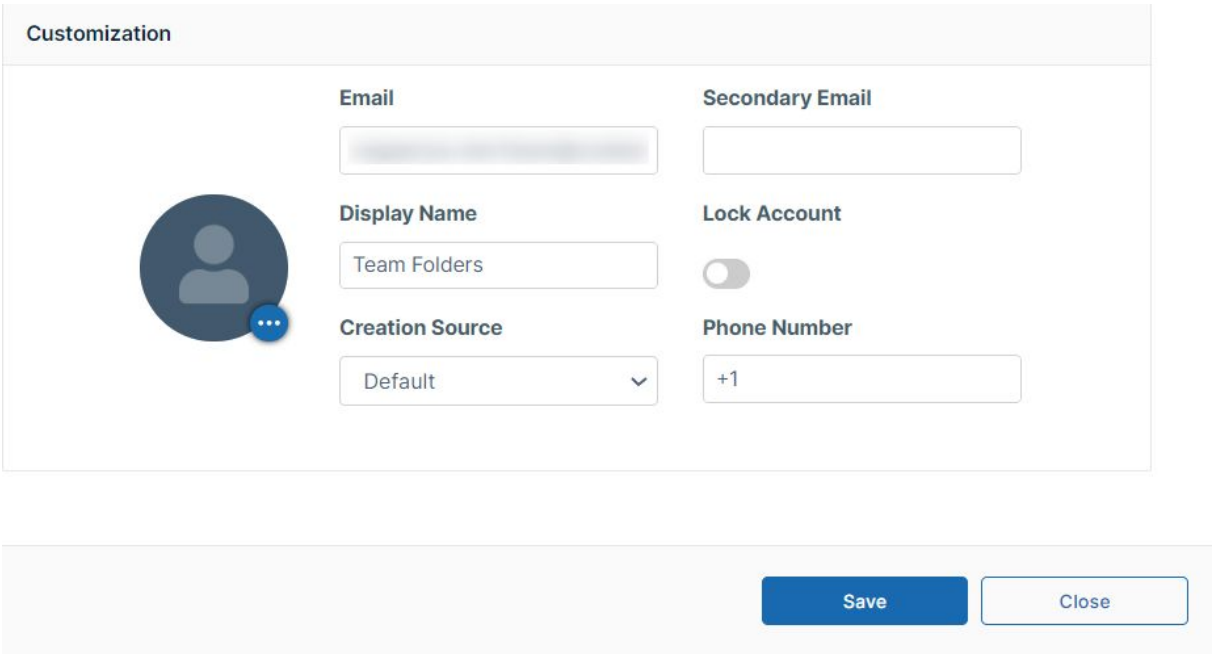
In the Data Storage section, click **View Details**.
You are shown a breakdown of the files and folders by live versions, old versions, and deleted files.




## To edit the Team Folders account fields:

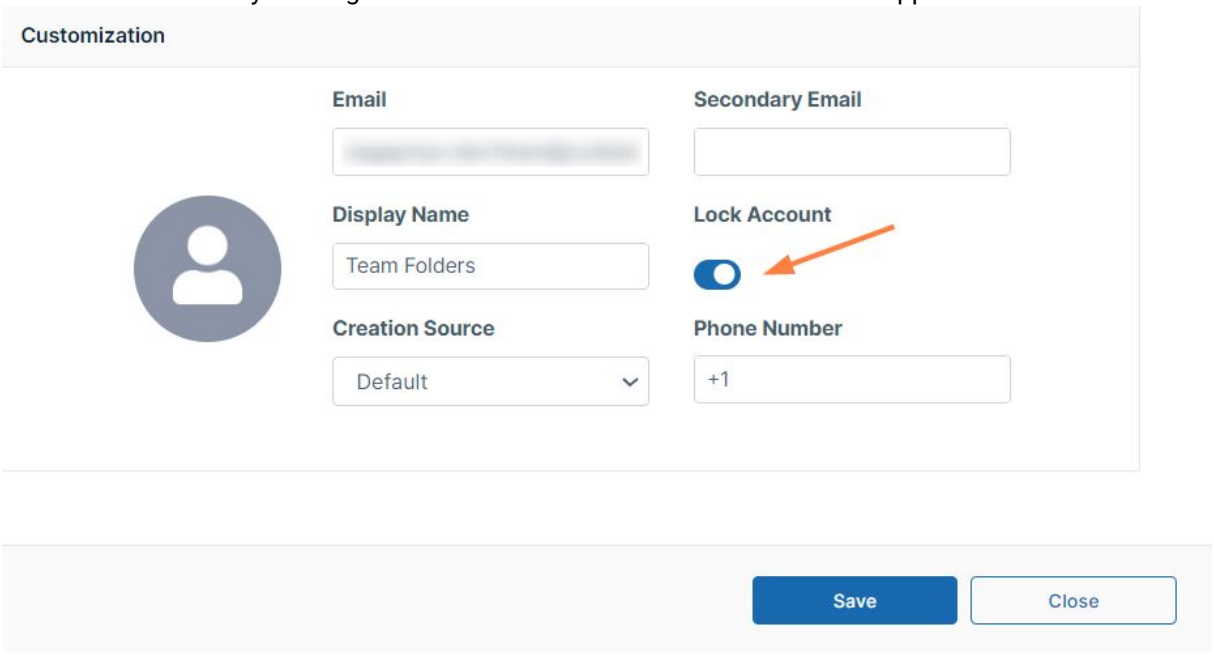
In the customization section, click the image, to upload a photo or graphic, or modify the **Email**, **Secondary Email**, **Display Name**, **Creation Source**, or **Phone Number** fields and click **Save** to save your changes.
**Lock Account** is automatically checked when too many login errors occur.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

and unlock the account.



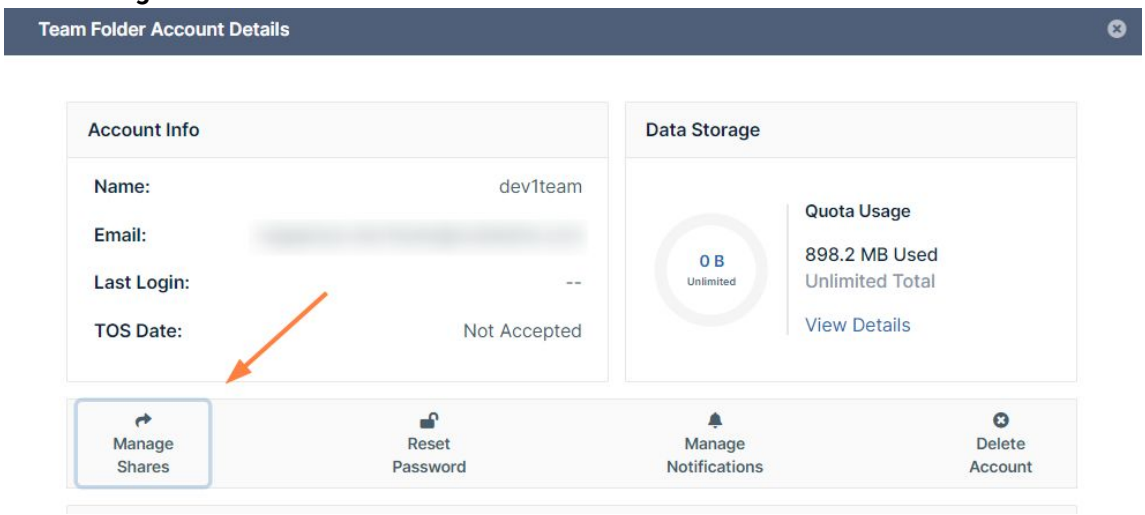

## To lock the Team Folder account:

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

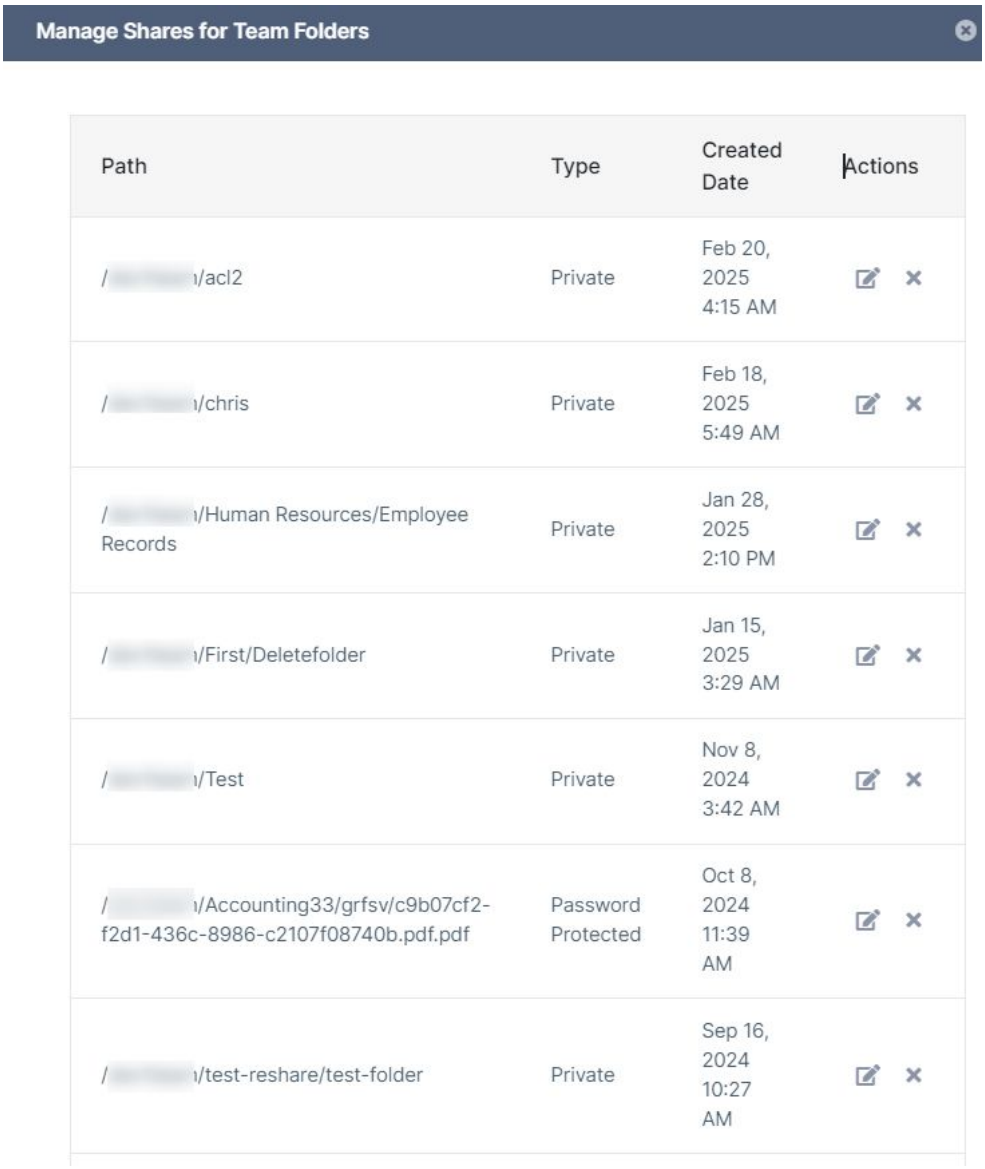


## To manage Team Folder shares:

1. Click **Manage Shares**.

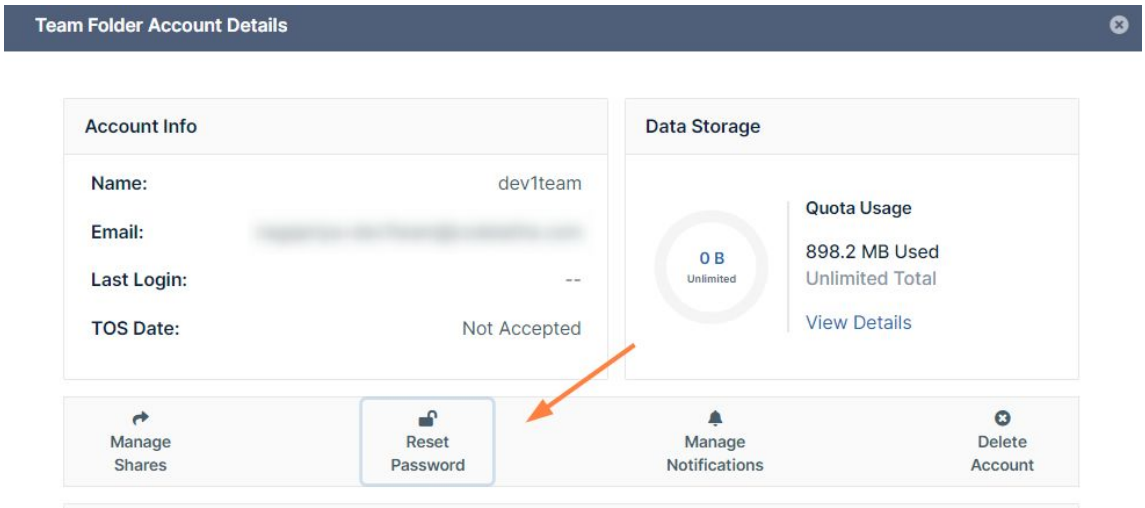



   A list of your Team Folder shares opens.
2. Click the edit icon to modify the options or permissions of a share.
3. Click the x icon to remove a share.

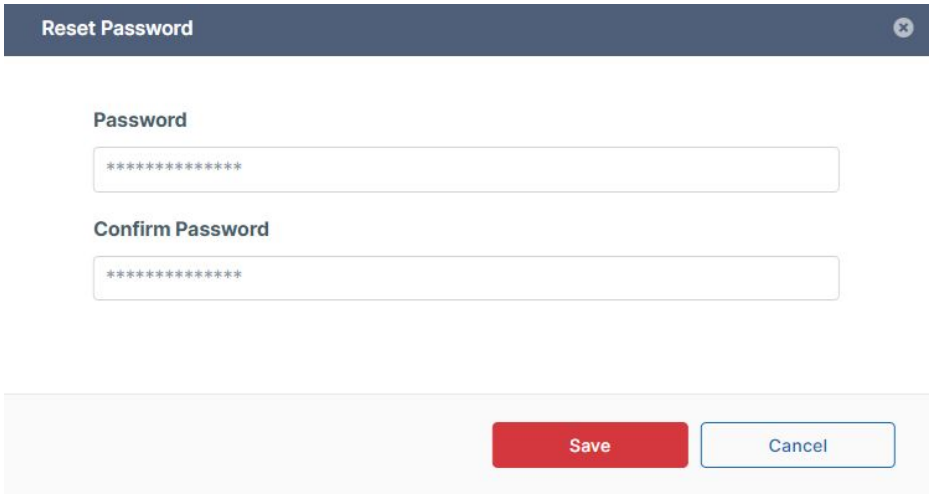



## To reset the Team Folder account password:

1. Click **Reset Password**.

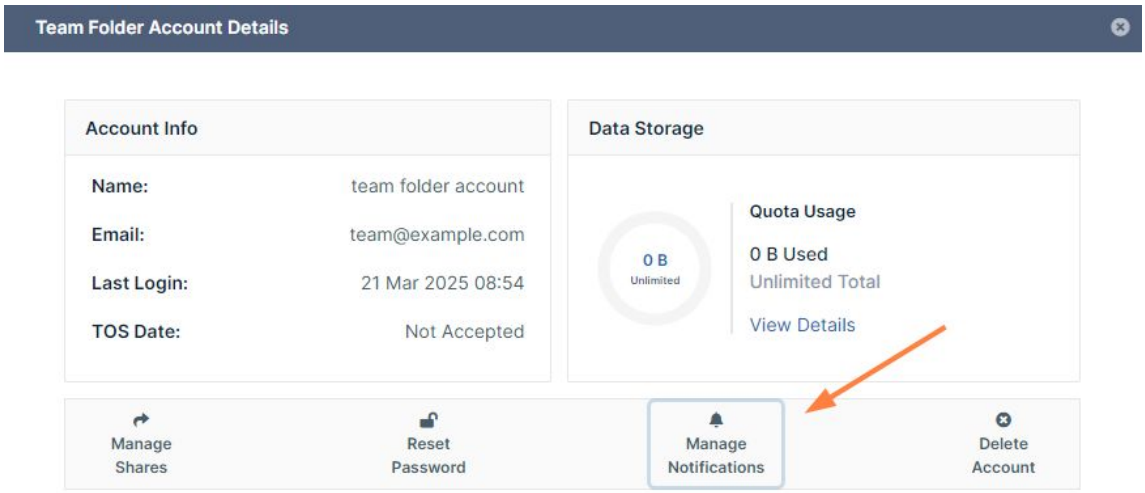



2. Enter and re-enter a new password, and click **Save**.

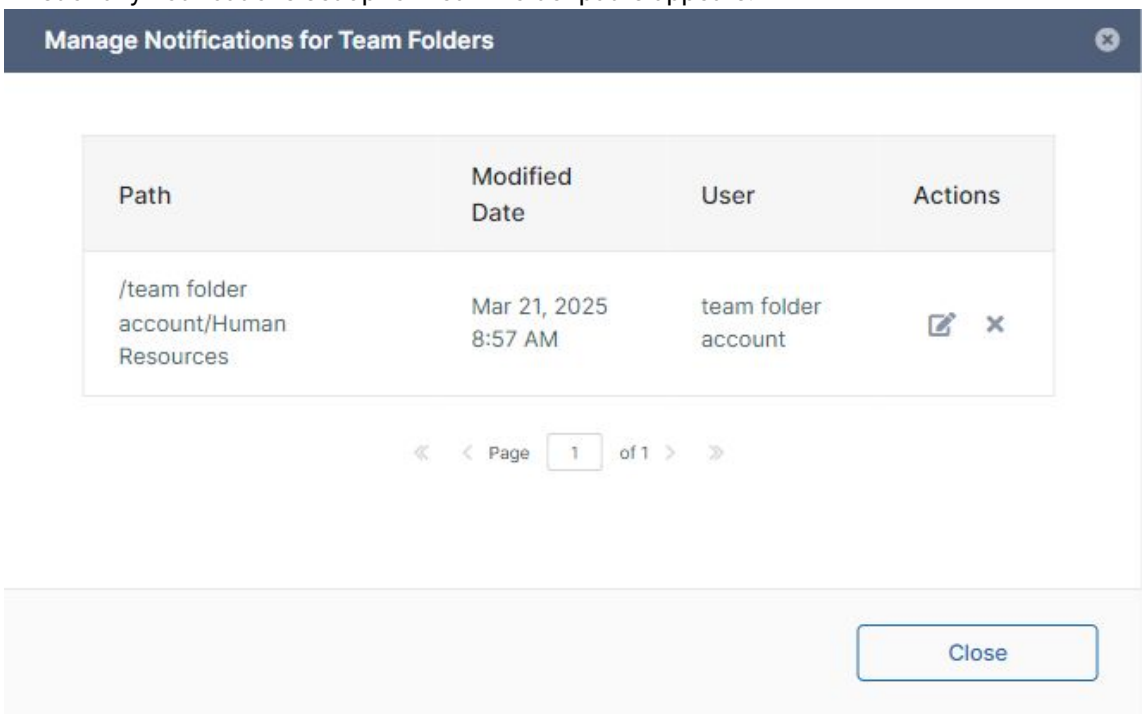



## To manage Team Folder notifications

1. Click **Manage Notifications**.




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



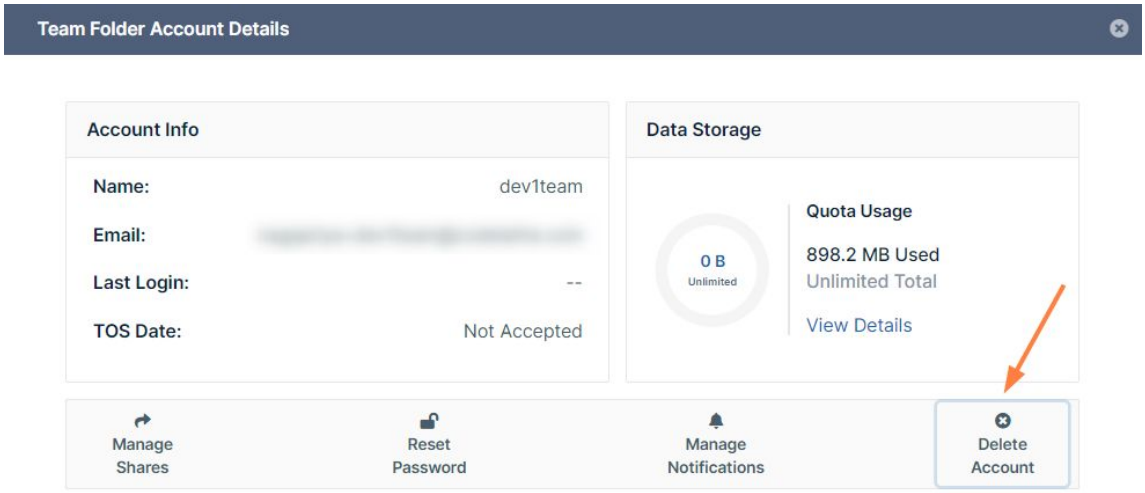

2. Click the Edit icon to change a notification's settings, or click the delete icon to delete the notification.

## To delete the Team Folder account:

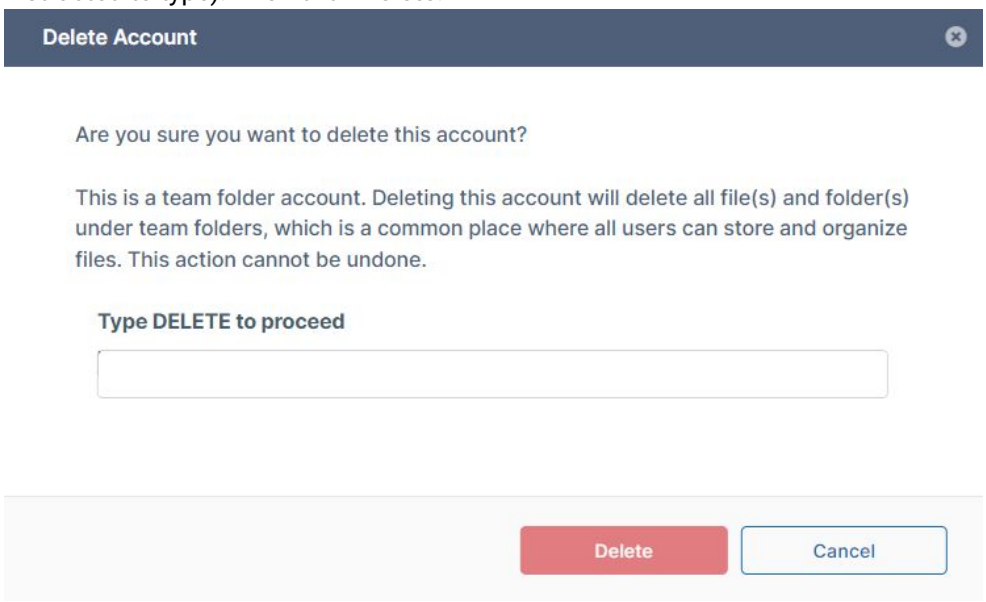
Check which files and folders will be deleted before you delete your Team Folder account. Deleting the account causes the following to be permanently deleted:

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

1. Click **Delete Account**.




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



# Search for a Team Folder

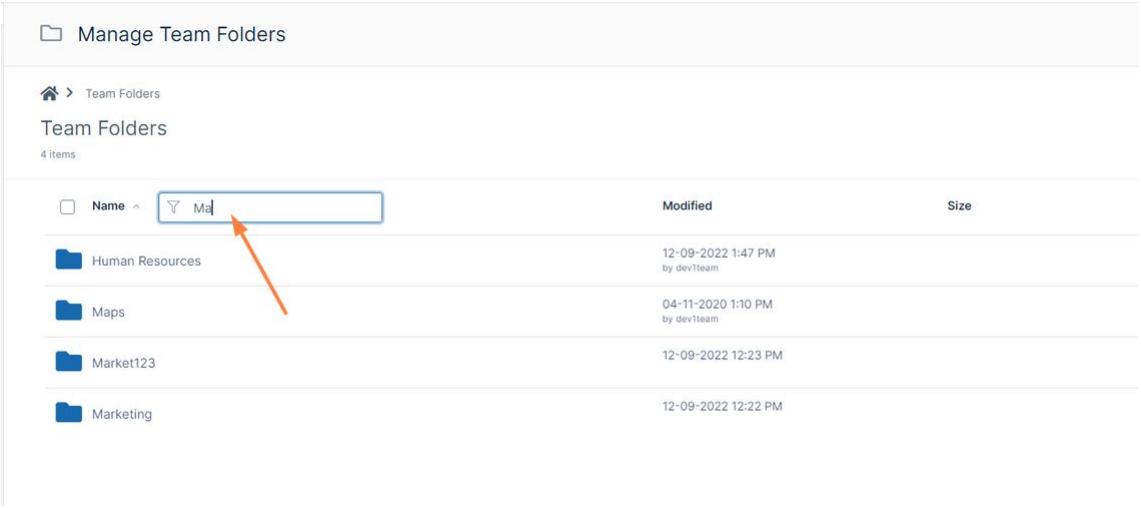
The ability to search for a specific Team Folder is available in FileCloud Server version 19.1 and later.

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

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

### To search for a Team Folder:

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



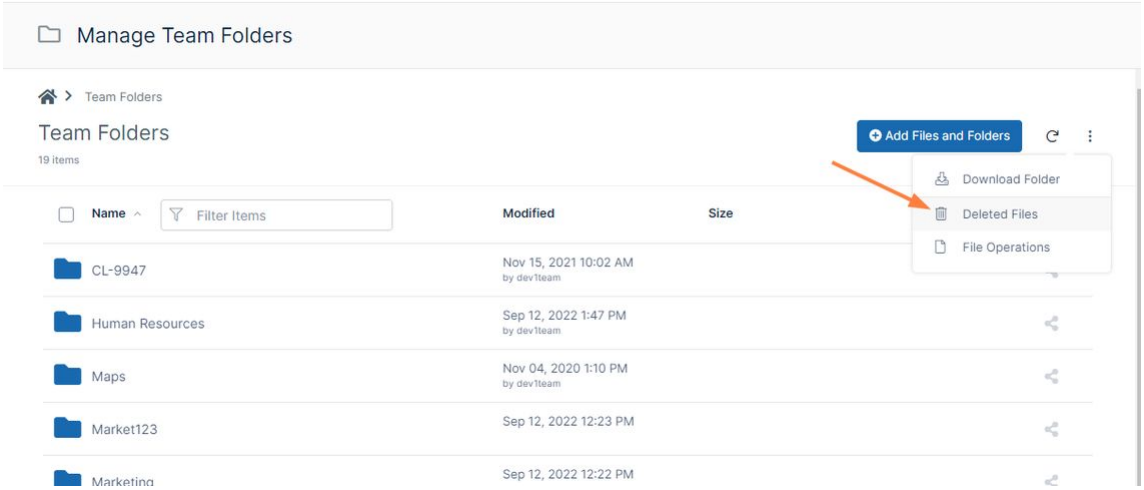

# Recover Deleted Files

The **Restore** button for deleted files and folders in Team Folders is available in FileCloud version 22.1 and later.
The ability to recover deleted files and folders in a Team Folder is available in FileCloud version 17.3 and later.

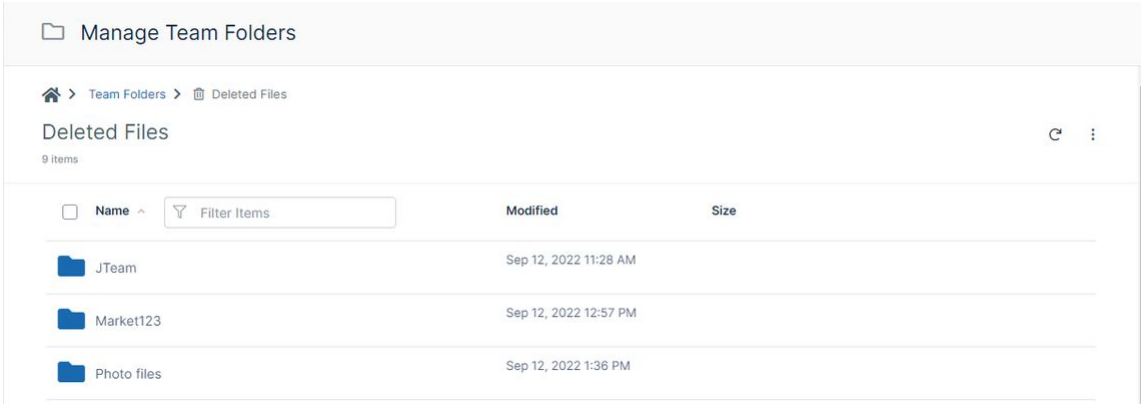
After you delete files and folders, they are placed in the Team Folder's recycle bin so that they can be recovered if deleted by mistake or are needed again at a later time.

**To recover a deleted folder or file:**

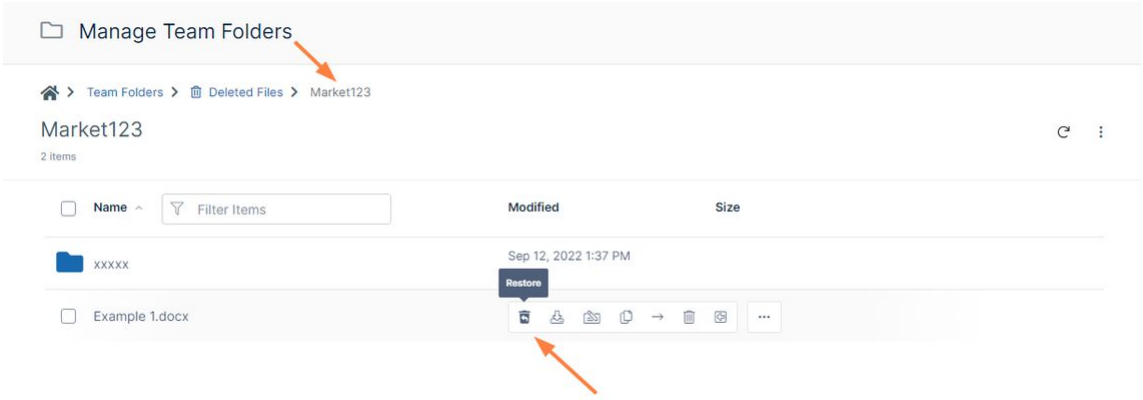
1. Open a browser and log in to the admin portal.
2. In the navigation panel, click **Team Folders**.
3. To open the **Deleted Files** page, in the upper-right corner, click the more icon and choose **Deleted Files**.



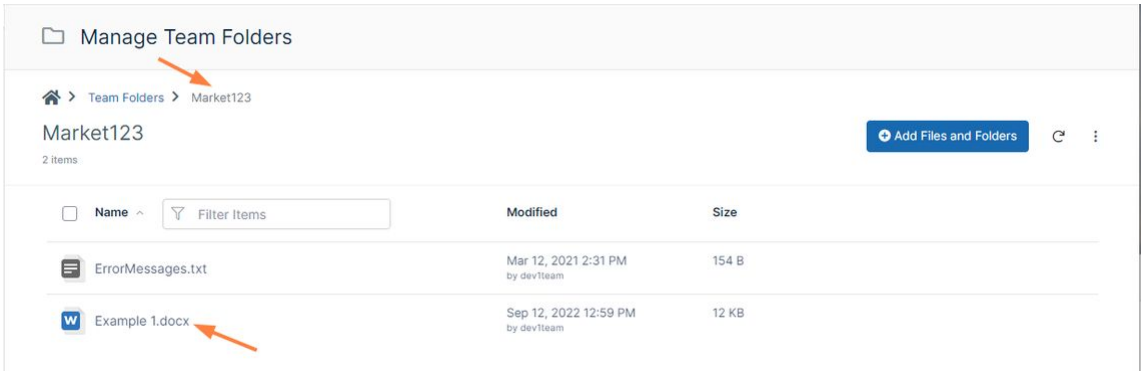

The **Deleted Files** screen opens. The top level of folders includes deleted team folders as well as non-deleted parent team folders of deleted files. For example, in the following screenshot, the **JTeam** and **Photo files** team folders are deleted team folders, but the **Market123** team folder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




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




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




## View and Restore Previous Versions in Team Folders

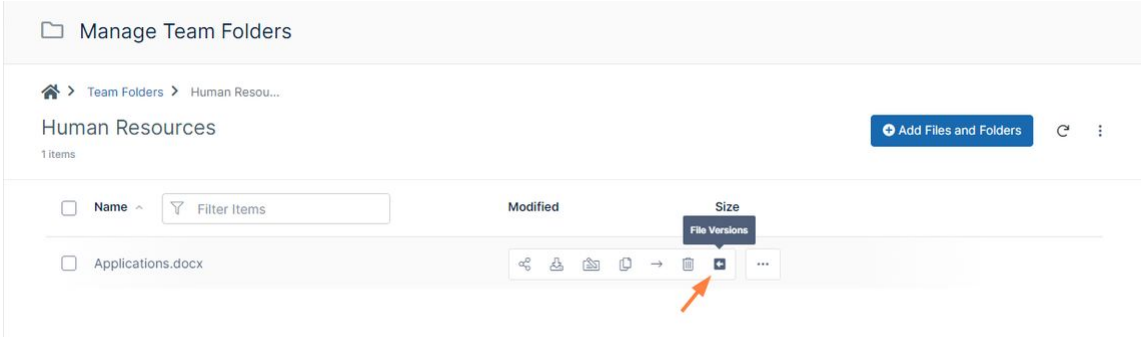
> The ability to restore a previous version of a file in Team Folders is available in FileCloud Server version 18.2 and later.

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

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

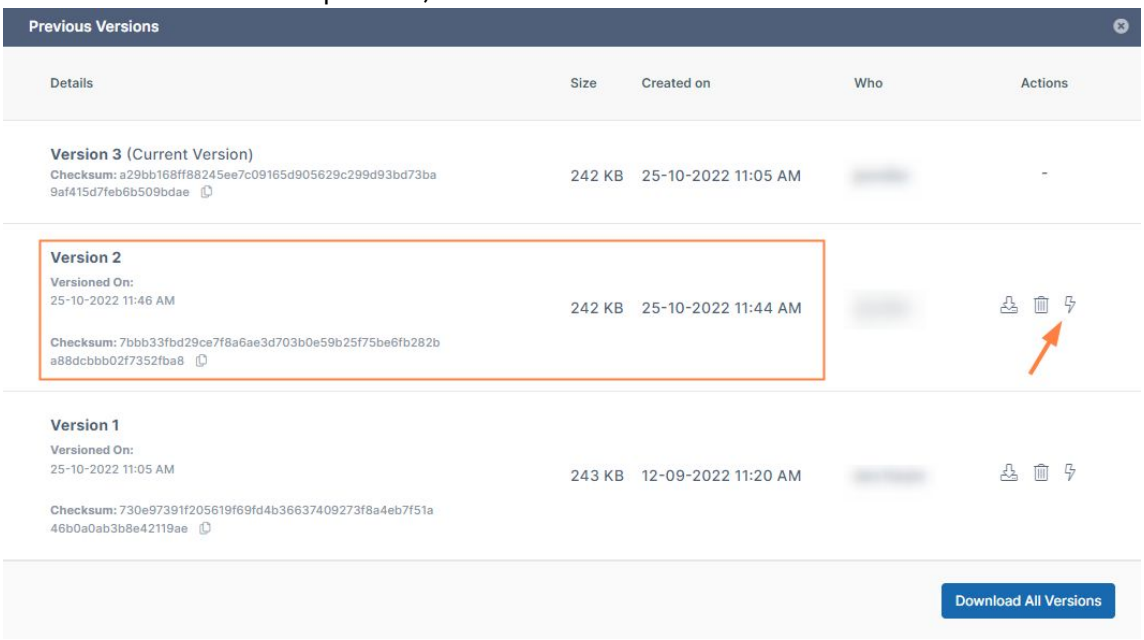
1. Open a browser and log in to the admin portal.
2. In the navigation pane, select **Team Folders.**
3. On the **Manage Team Folders** page, navigate to the file you want to revert to a previous version.

4. Click the version icon.

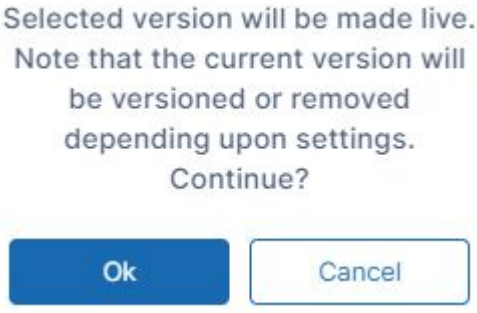



A list of the previous versions opens.

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

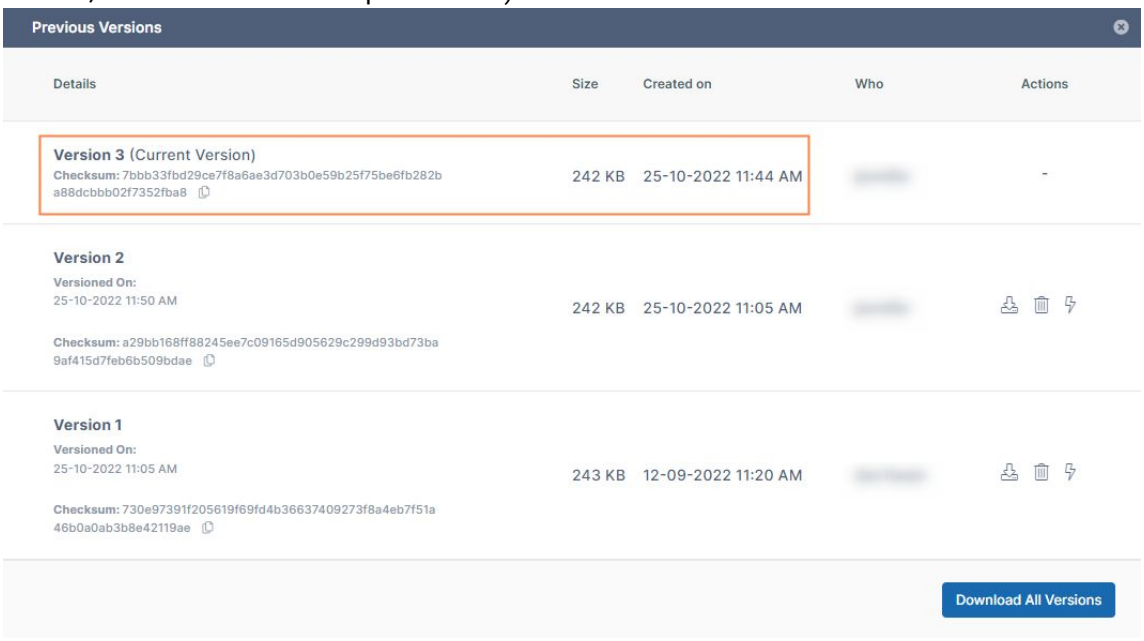



The following confirmation box appears:




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

version, it is Version 3 at the top of the list.)




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

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

# Managing User Shares

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

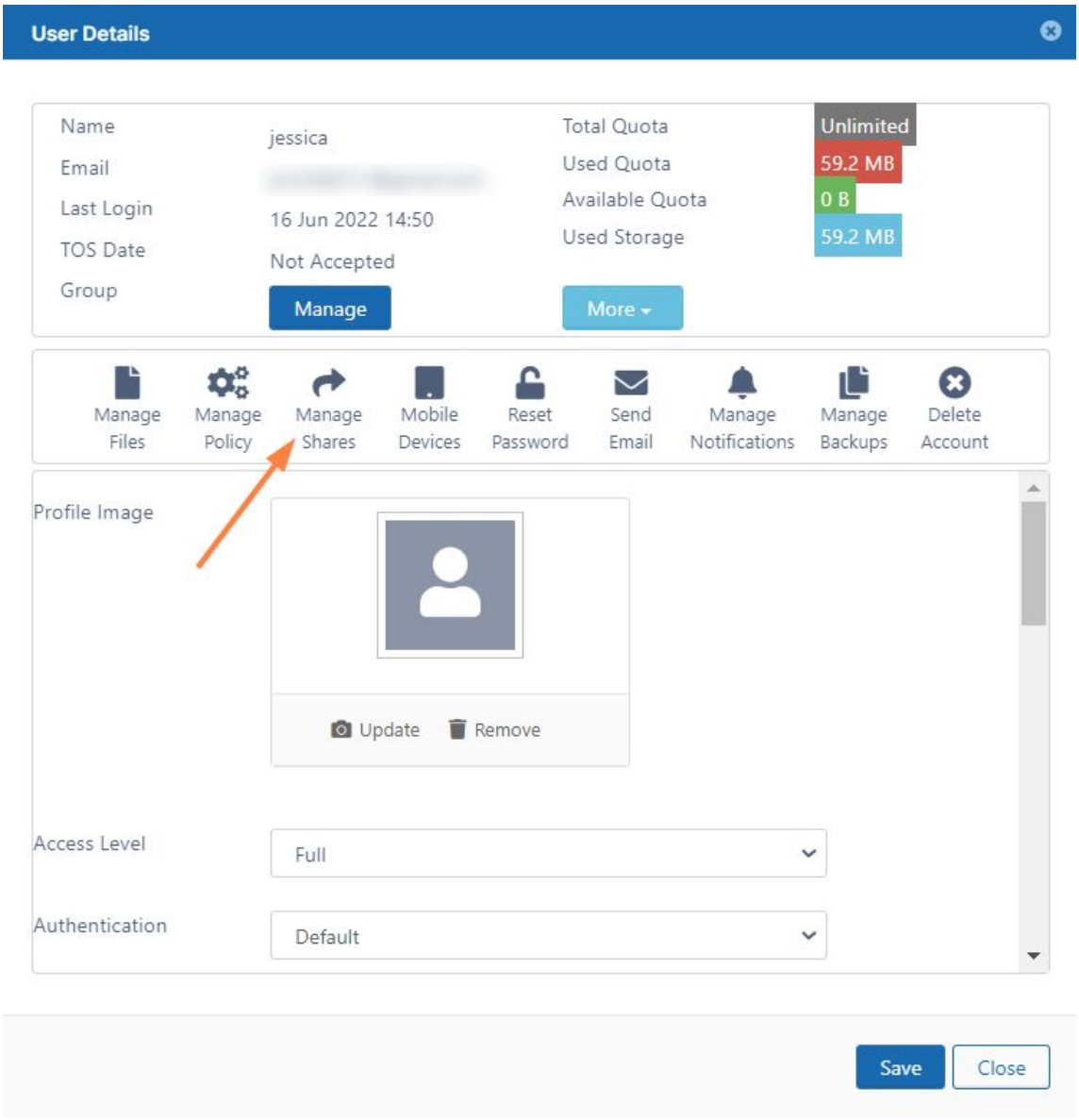
The Administrator is able to view, modify or remove shares done by users of the system.

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

To set up file sharing, see Share Settings.

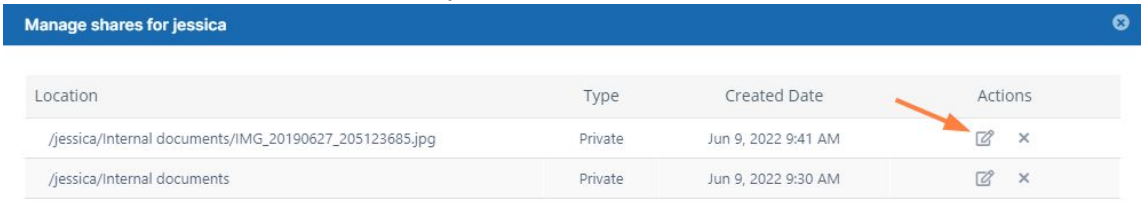
## To manage user shares for an individual user:

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



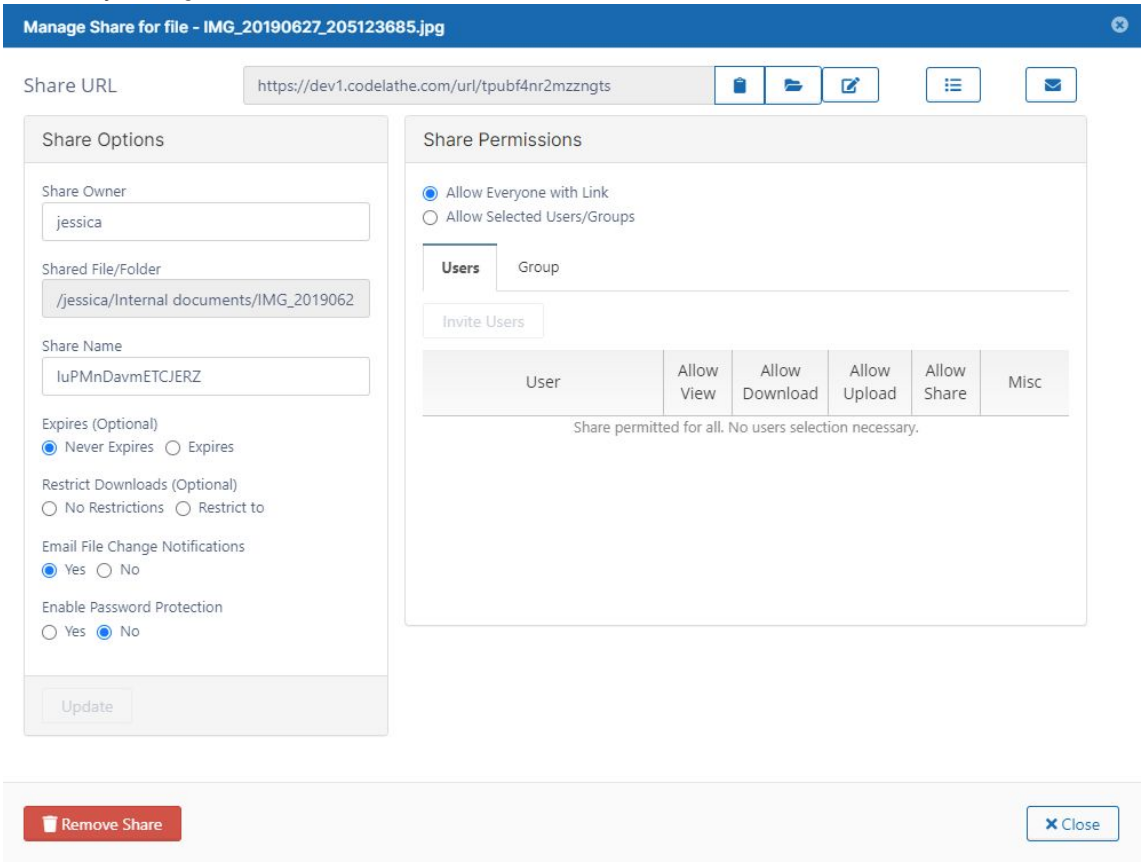

A **Manage shares for [user]** dialog box opens.

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



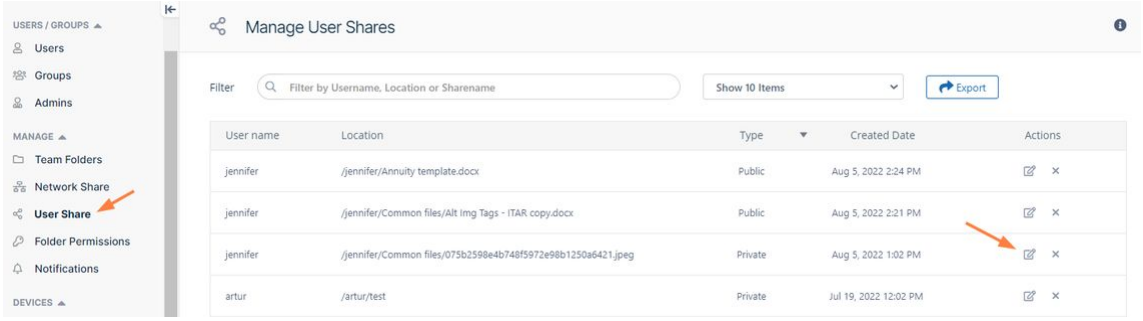
The **Manage Share** dialog box opens.

4. Make any changes to the share.

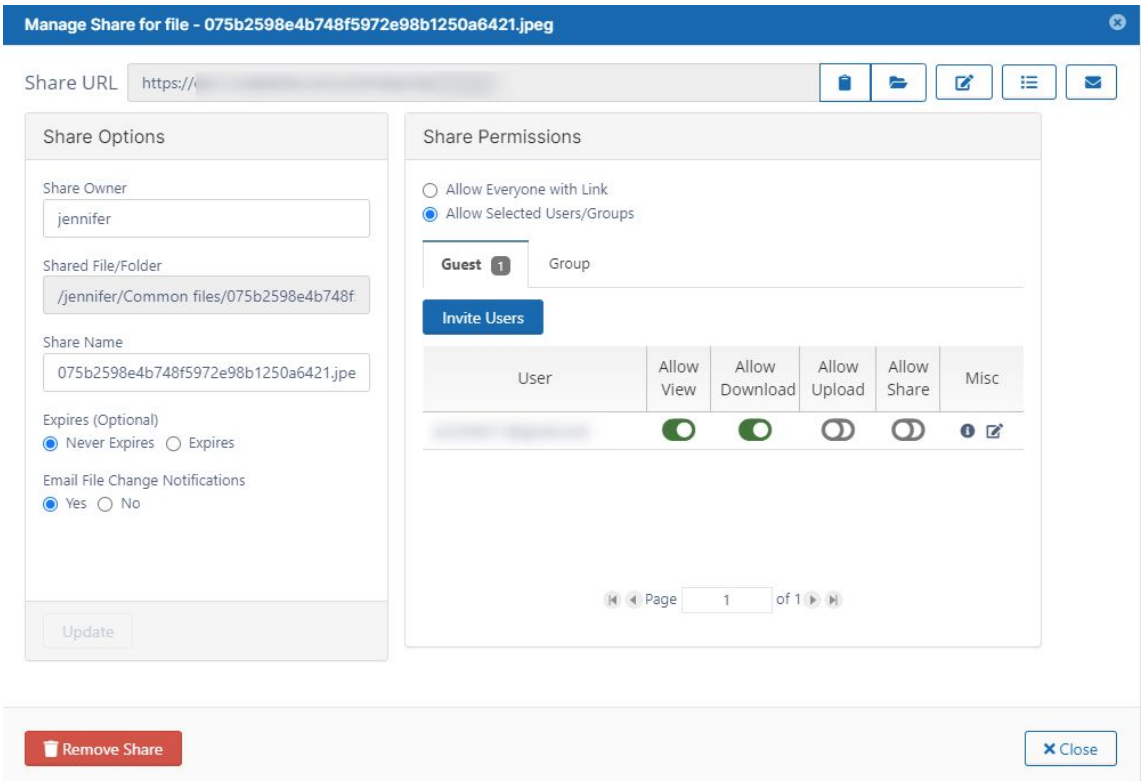



## To manage user shares for all users:

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

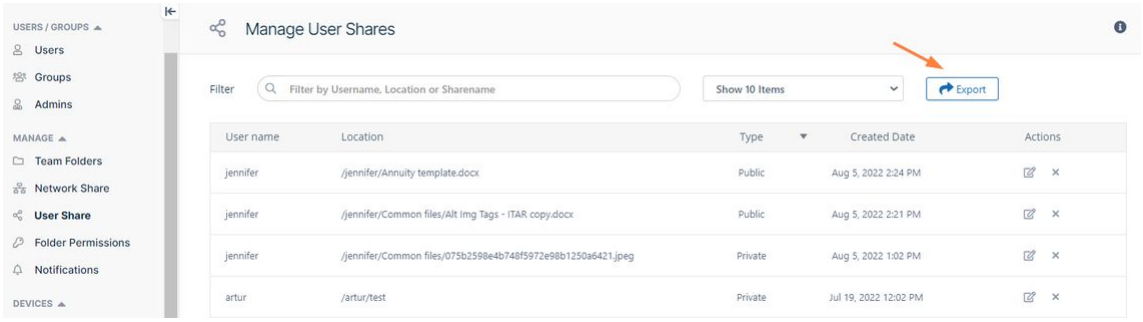



4. The **Manage Share** dialog box opens.
5. Make any changes to the share.




# To export a list of all shares:

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




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

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

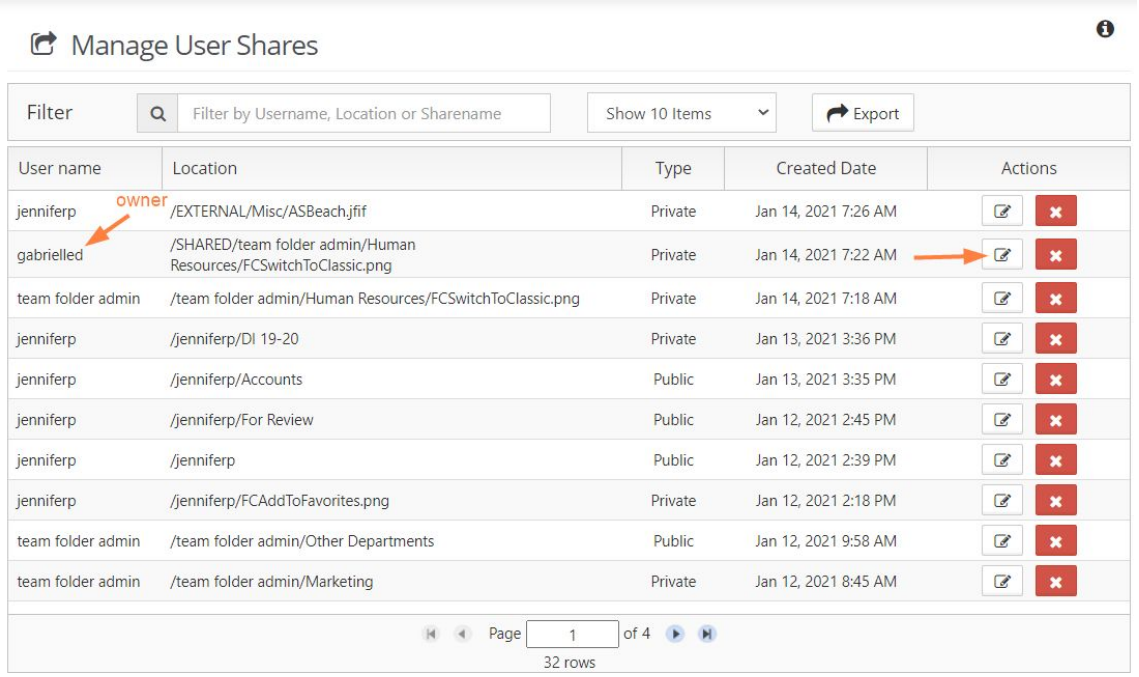
# Transfer Ownership of a Reshare from a Team Folder or Network Share

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

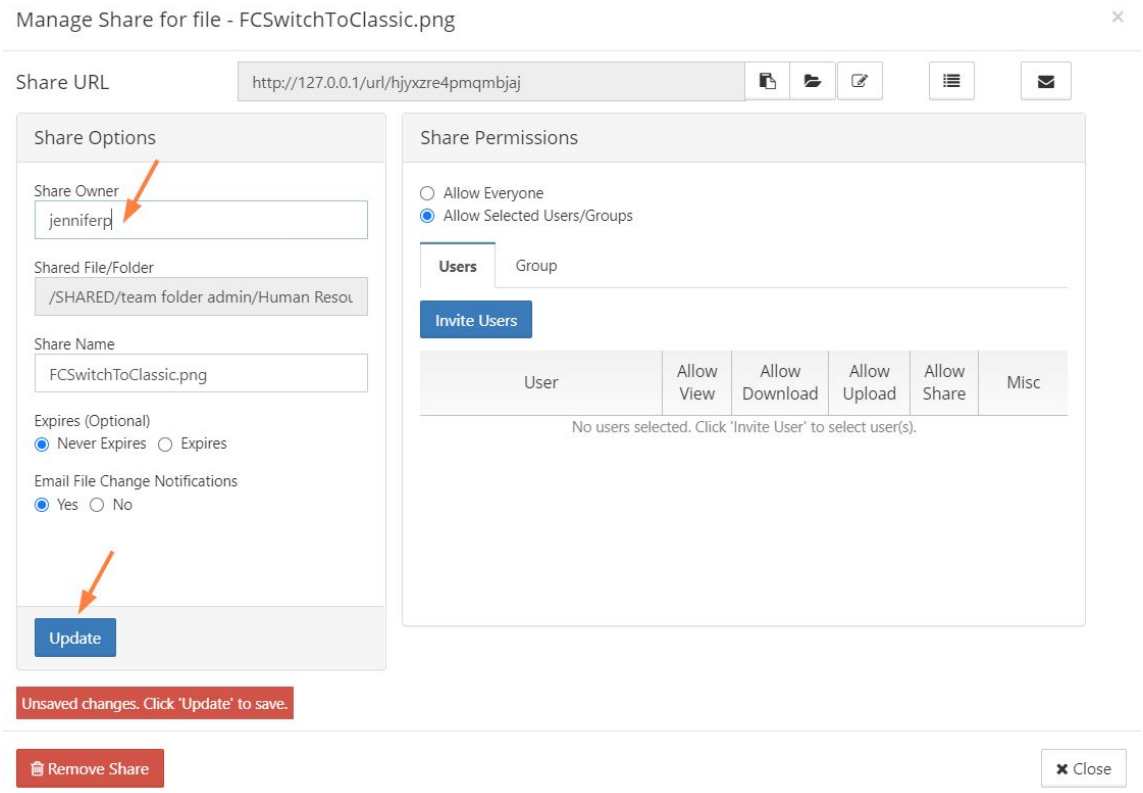
Reshared content from Team Folders and Network Shares is content that a user already has access to and has shared with another user.
In the **Manage User Shares** dialog box, its root is **/EXTERNAL** or **/SHARED**.

To change the owner of a reshare

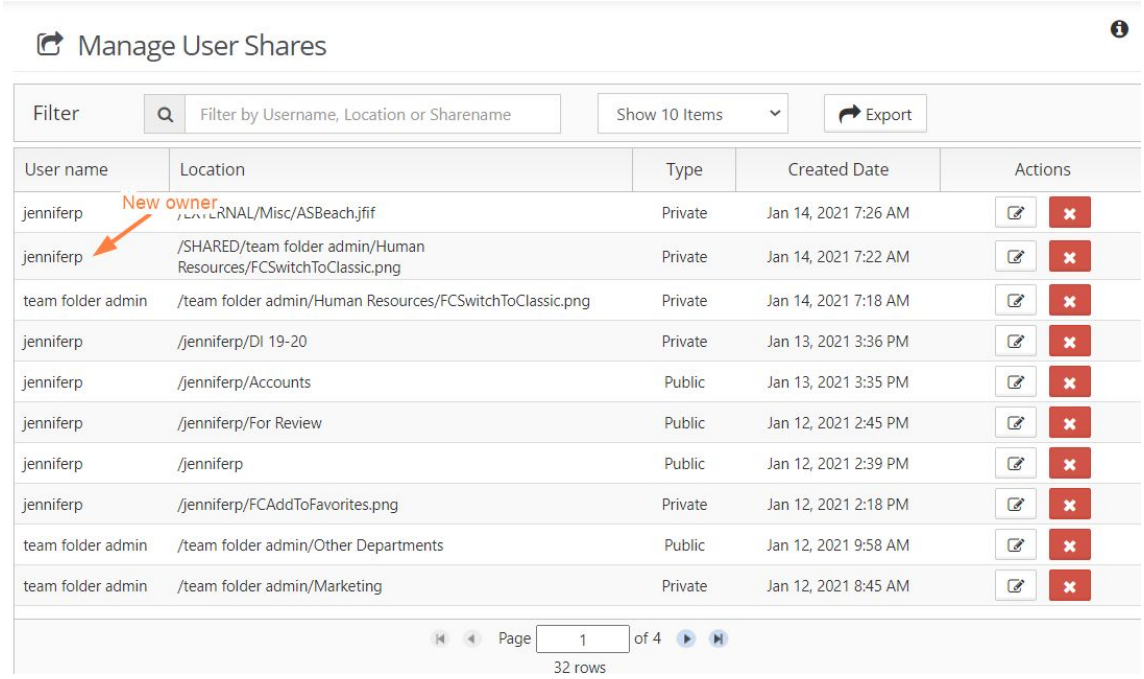
1. Follow the steps in Managing User Shares (see page 93) to open the list of shares.
2. To open the **Manage Share for File** dialog box, click the Edit button for a Team Folder share or a Network Share.




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




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



# Creating direct file download link from a public file share

## Creating direct download link for public shares

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

By default the public share link looks like this:

> https://abc.company.com/ui/core/index.html?mode=single&path=/SHARED/tester/MMQj5gqRymicnDib[3]

In the above link, replace the string "**ui/core/index.html?mode=single[4]&**" 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[5]?path=/SHARED/tester/MMQj5gqRymicnDib[6]"

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

# Creating direct file download links from a public folder share

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

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

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

---

3. https://dev1.codelathe.com/ui/core/index.html?mode=single&path=/SHARED/apptester/MMQj5gqRymicnDib
4. https://dev1.codelathe.com/ui/core/index.html?mode=single&path=/SHARED/apptester/MMQj5gqRymicnDib
5. https://dev1.codelathe.com/ui/core/index.html?mode=single&path=/SHARED/apptester/MMQj5gqRymicnDib
6. https://dev1.codelathe.com/ui/core/index.html?mode=single&path=/SHARED/apptester/MMQj5gqRymicnDib

## To copy the share link:

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

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

In our example, the link to the shared folder is:
http://127.0.0.1/ui/core/index.html?mode=public&shareto=#expl-tabl./SHARED/!bli3S5COtIoHQD49yINBKMSe5/XOOclSQ2AAdiOWP1
We would like the link to open a download page for the file customers.docx, which is located in the folder.

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

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

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

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

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

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

## Sample links before and after

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

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

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

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

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

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

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

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

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

# Managing Storage Space Usage

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

## In this section


- Storage Scanner Tool for Missing Files (see page 104)
- Storage Usage Tool (see page 105)
- Thumbs Tool for Removing Excessive Thumb Files (see page 106)


## Related topics

**A User's Storage**

Change the Storage Quota for a User or Group

Delete User Files and Folders (see page 64)

Clear a User's Recycle Bin (see page 65)

Remove a User's Incomplete Uploads (see page 70)

Remove Old File Versions (see page 69)

**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.

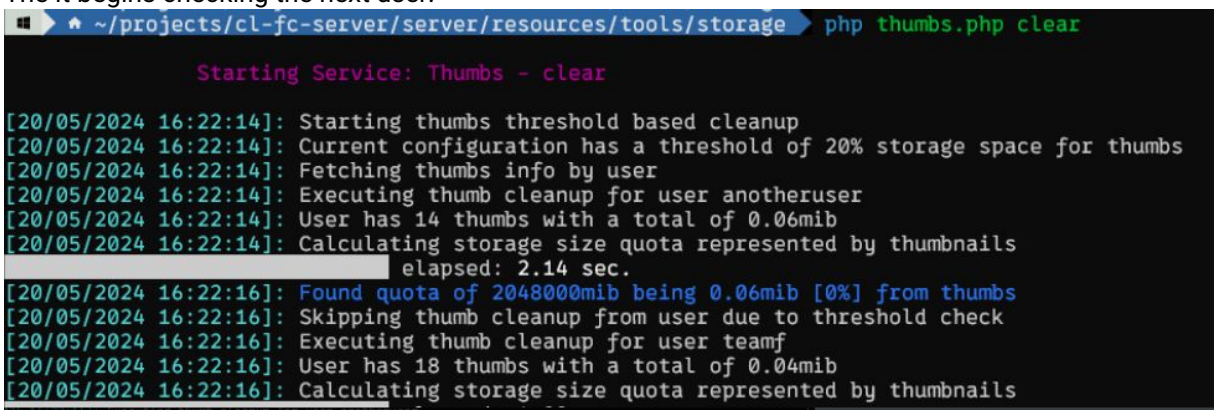
```
php thumbs.php clear-network -d 5 -p /EXTERNAL/Accounts -u all
```

**help** Displays help notes for the thumbs.php command.

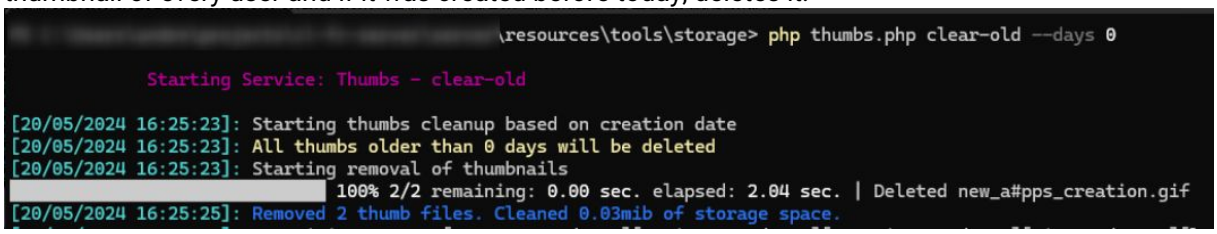
```
php thumbs.php help
```

## Example input and output

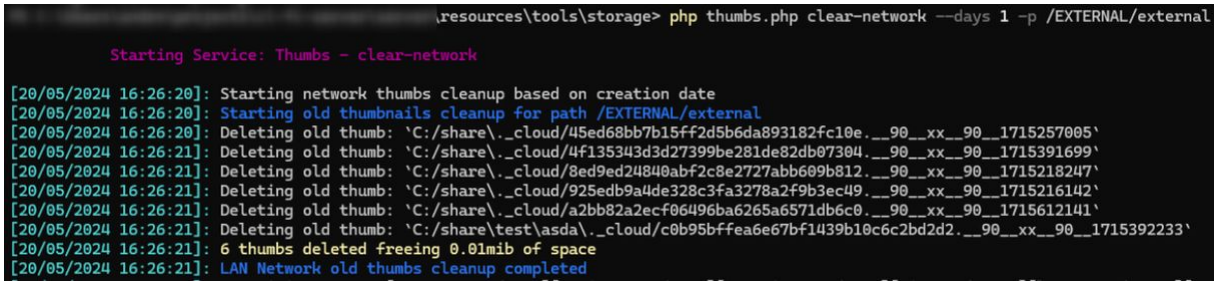
In the first example, the admin enters: **php thumbs.php clear**. The tool checks the first user and finds that the user's thumbs do not take up 20% or more of storage space, so it does not do thumb cleanup. The it begins checking the next user:



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.




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.




## 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

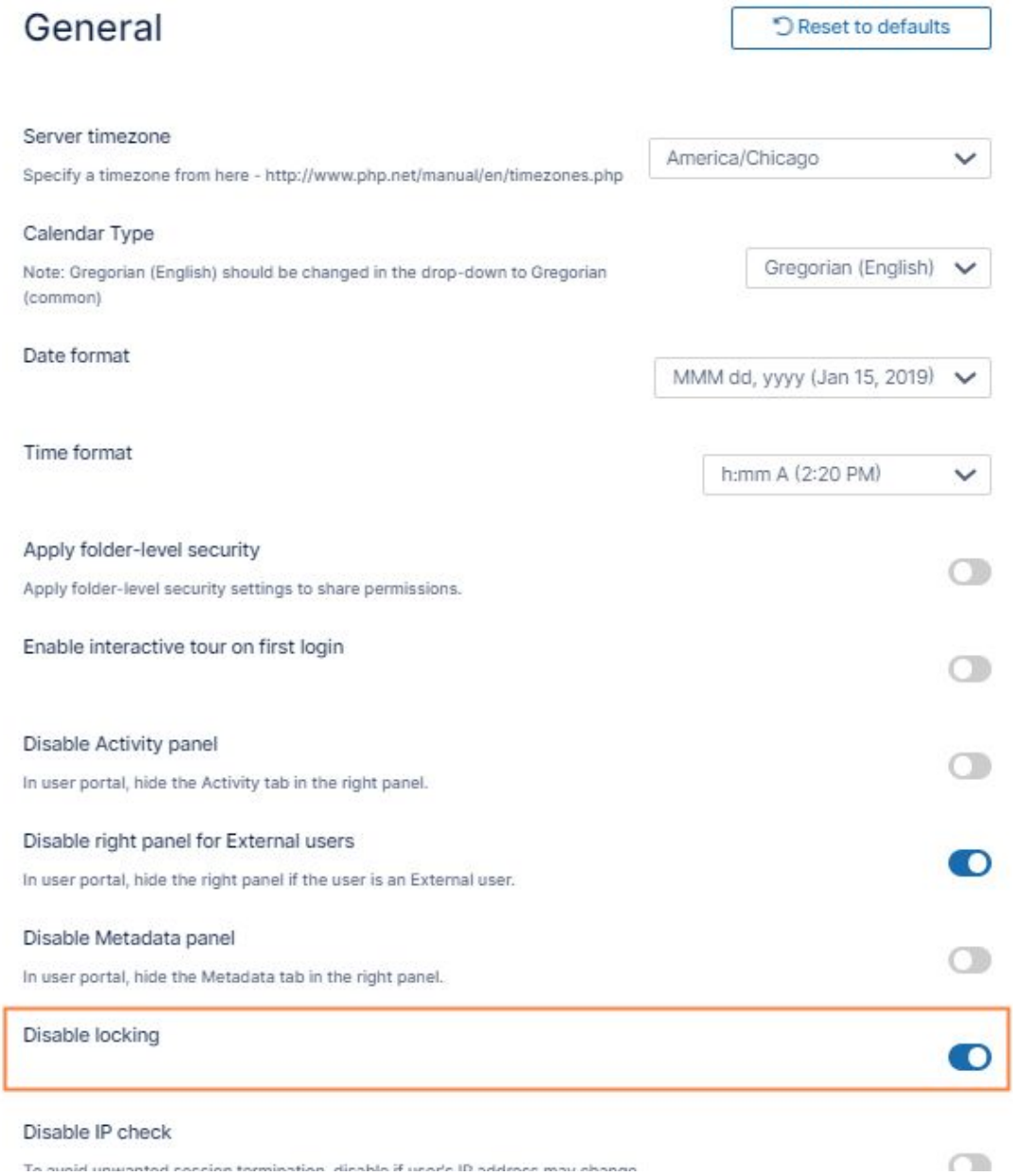
You can disable locking so that users are never given this option in the User Portal.

- 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.




3. Click **Save**.

**How to View Which Files or Folders are Locked**

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

**To view a list of locked files and folders**:

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

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

For example:

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

### Release a Single Lock

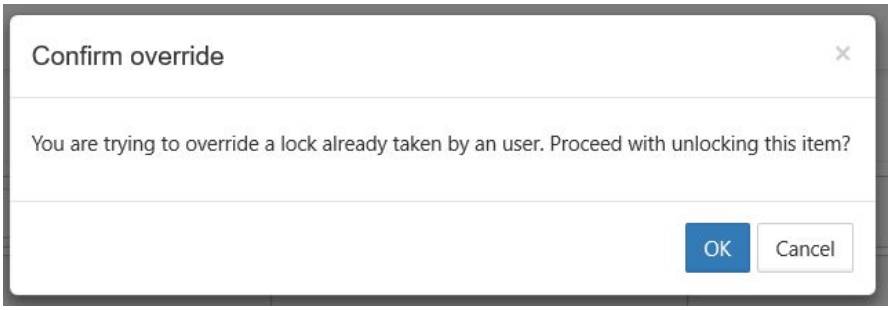
There are times when you may need to unlock a file for a user.

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

**To release the lock on a single file or folder**:

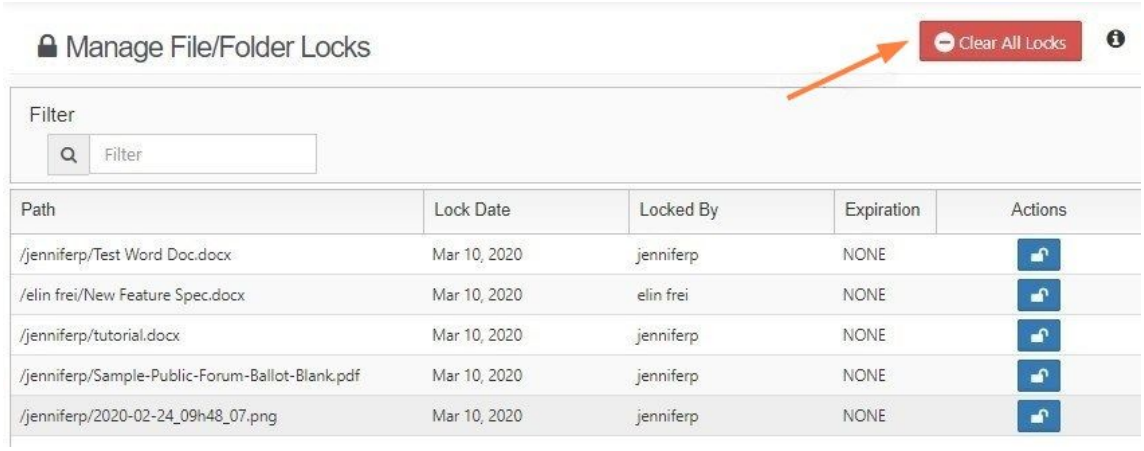
1. Log on to admin portal.
2. From the left navigation pane, click **User Locks**.
3. On the **Manage File/Folder Locks** screen, find the file or folder whose lock you want to remove.
4. In the row containing that file or folder name, under the **Actions** column, click the unlock button ( ).

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




**To release the lock on all locked files and folders**:

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




A confirmation dialog box opens.

4. Click **OK**.

# Managing User-Defined Notifications

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

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

**In this section:**

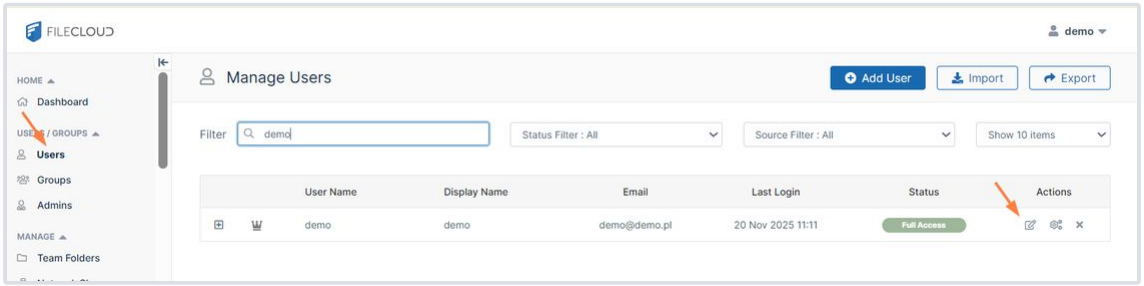

- Editing individual user's file and folder notifications (see page 113)
- Editing all users file and folder path notifications (see page 116)
- Adding notifications for actions on user's files and folders (see page 118)


## Editing individual user's file and folder notifications

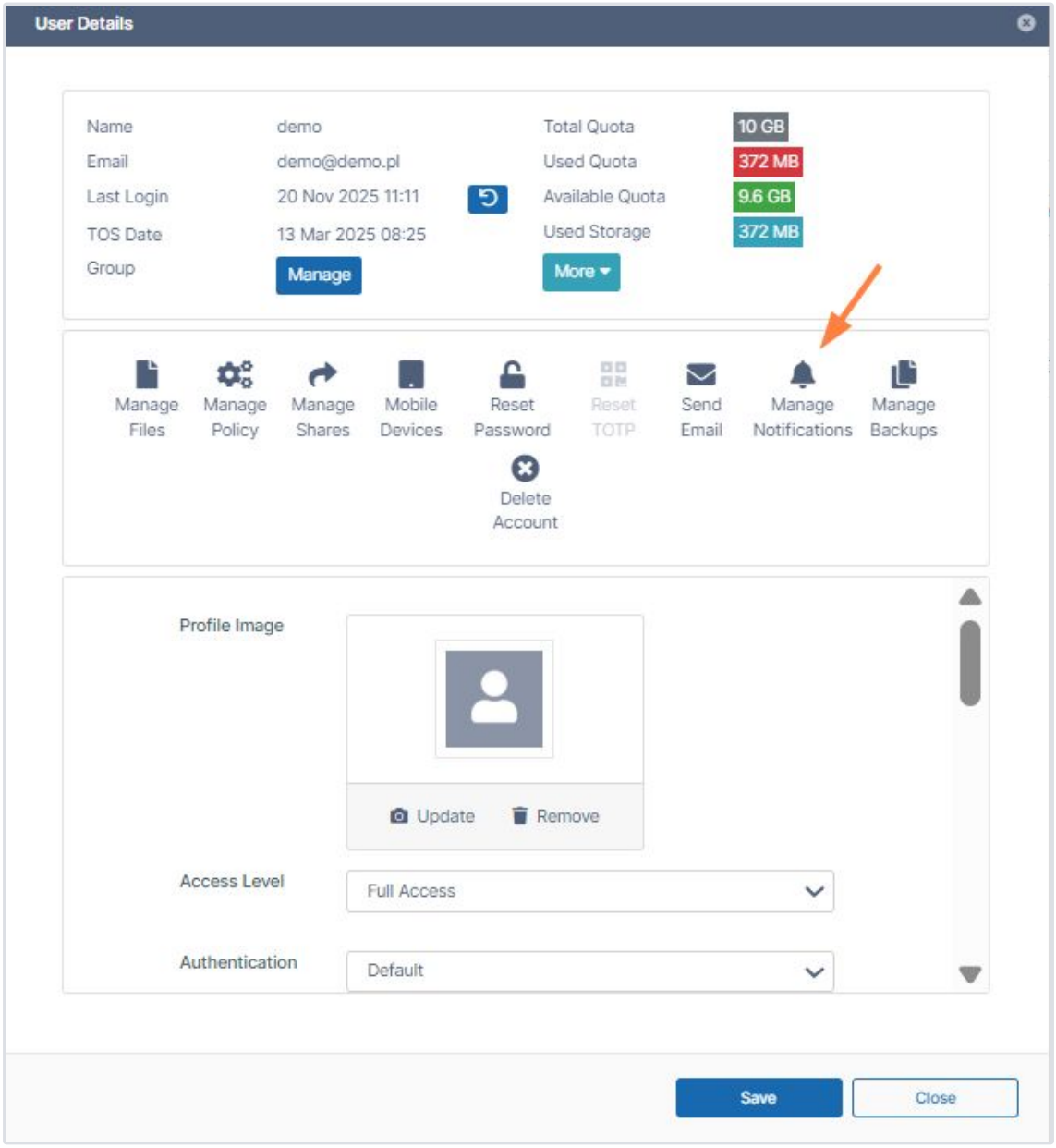
As an admin, you can edit notifications on a specific user's file and folder paths by clicking the **Manage Notifications** icon in the user's details.

### To edit a user's file and folder notifications:

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

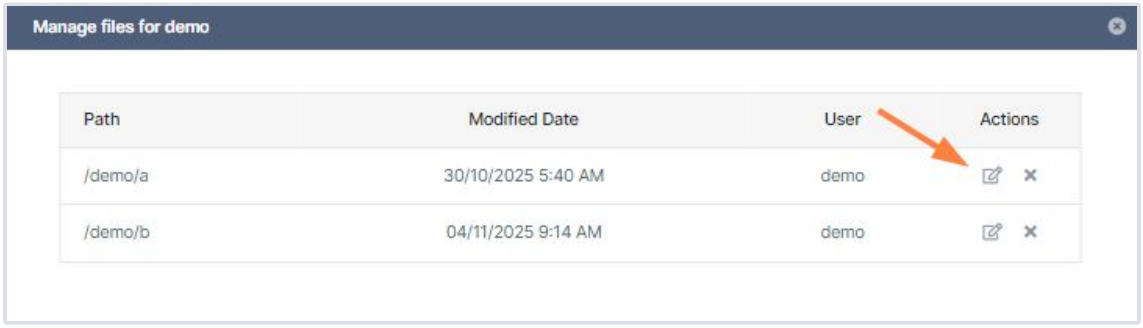



   The User Details dialog box opens.
3. Click the **Manage Notifications** icon.

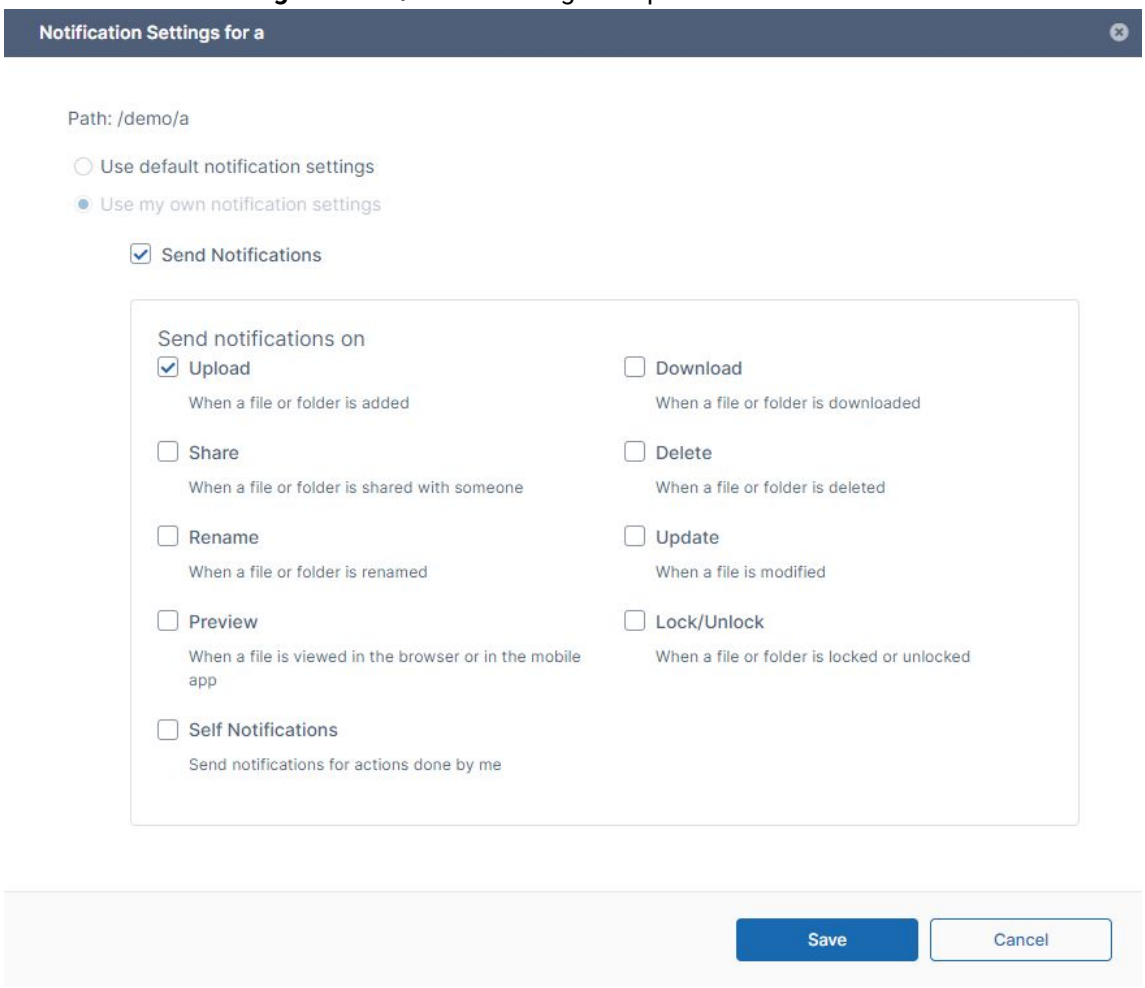



The **Manage Notifications for <user>** dialog box opens. All of the paths to files or folders with notifications defined on them are listed.

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




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




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

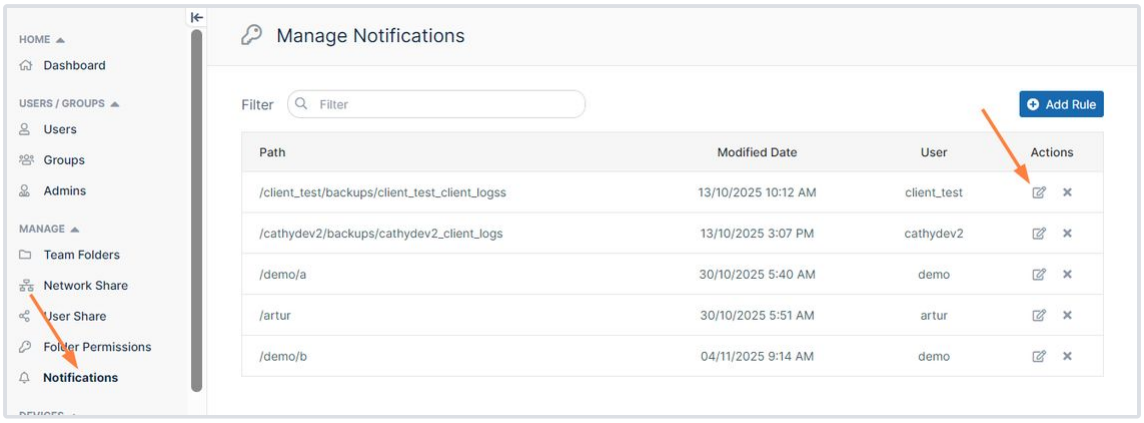
- If you want to edit which types of actions users are notified about, check and uncheck the boxes under **Send notifications on**.
- If you want the user to receive notifications when they have performed an action on the file or folder, check the **Self Notifications** box**.**
- If the user has **Use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

## Editing all users file and folder path notifications

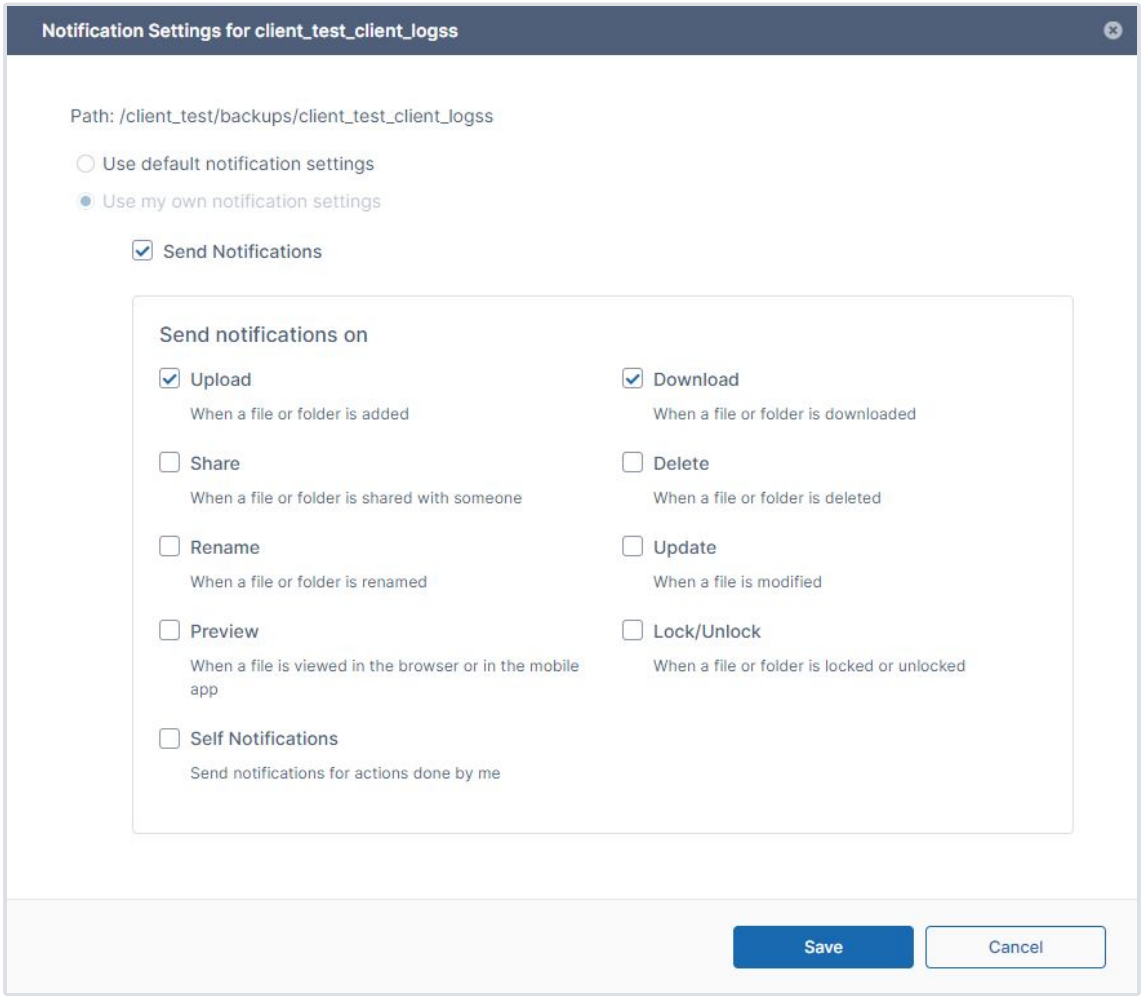
You can edit the notifications that users have defined for file and folder paths on the **Manage Notifications** screen. The screen shows all notifications assigned to paths for all users in your system.

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

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




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



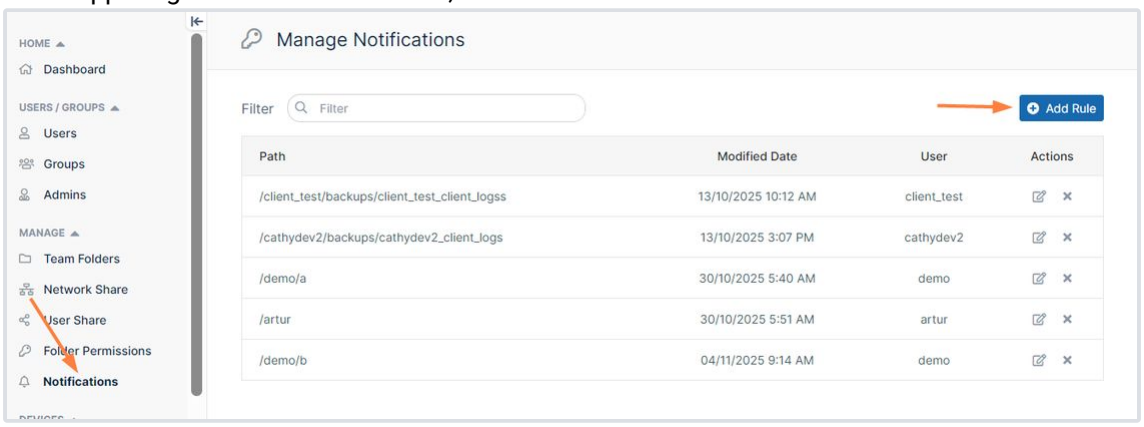

3. Edit the notification settings:
   - If you want to reset the user's settings to the defaults, check **Use default notification settings. Use my own notification settings** and all of the settings below it become unselected. If the user is permitted to override your settings, they may turn back on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

# Adding notifications for actions on user's files and folders

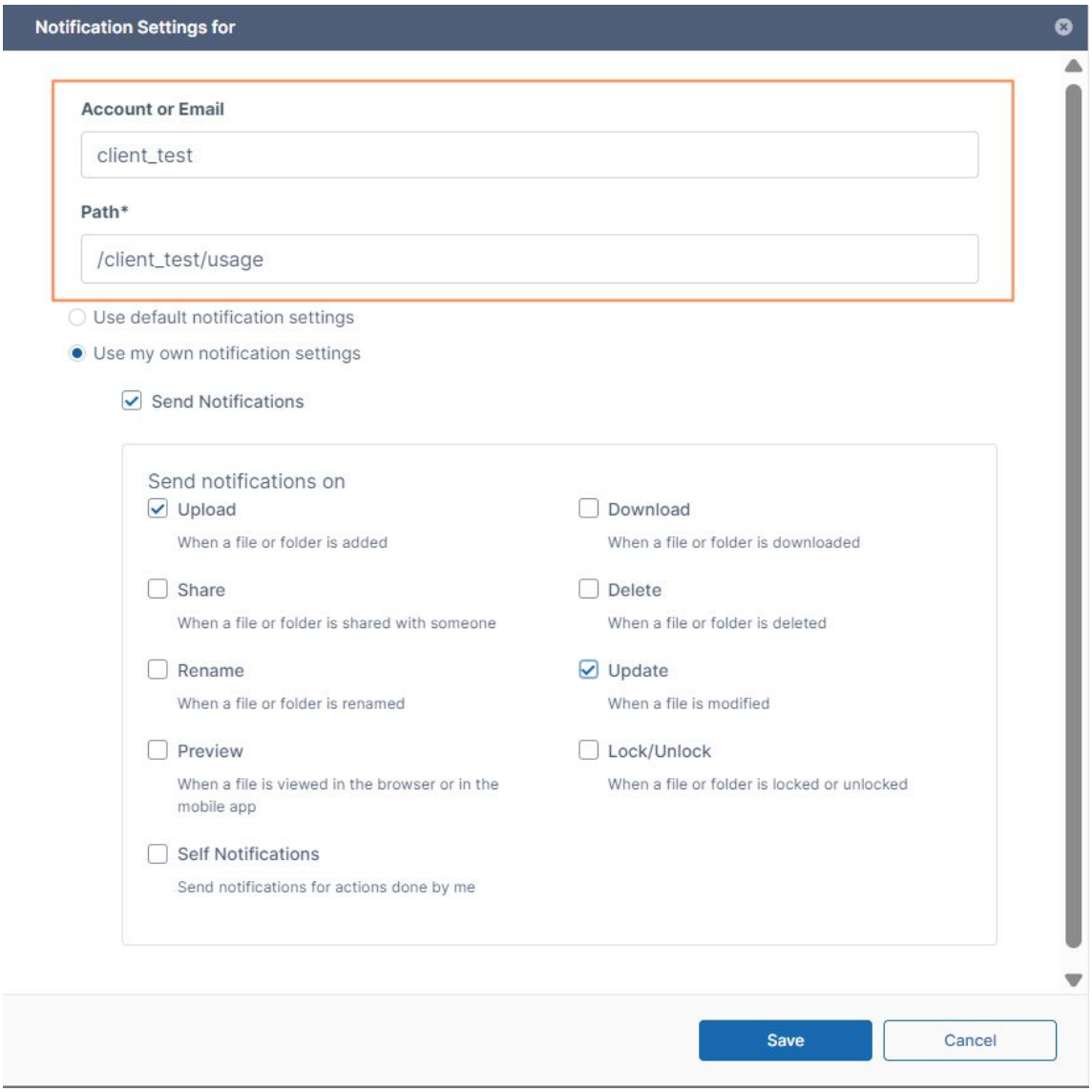
You can add notifications for actions performed on users' file and folder paths.

## To add notifications to users files or folder

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




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



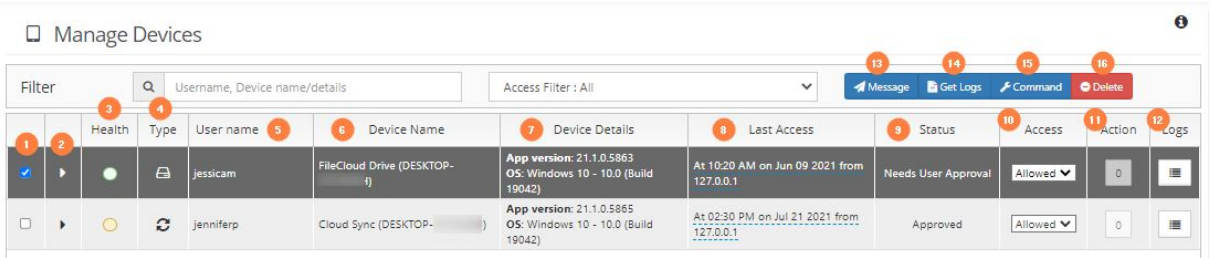

3. In **Account** or **Email**, enter the username or email address of the user.
4. In **Path**, enter the path to the file or folder in the user's storage.
5. Select **Use my notification settings**.
6. Check **Send Notifications**.
7. Below **Send Notifications on** check the actions for which you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

# Managing Client Devices

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

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

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




### What Do All These Columns Mean?

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

| | | |
|---|---|---|
| **8** | **Last Access** | Displays the last time this device connected to the FileCloud server<br>• 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.<br>• Allow<br>• Block<br>• 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<br>• Logs the user out of their account<br>• Closes the connection<br>• Removes data associated with the device<br>• 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.

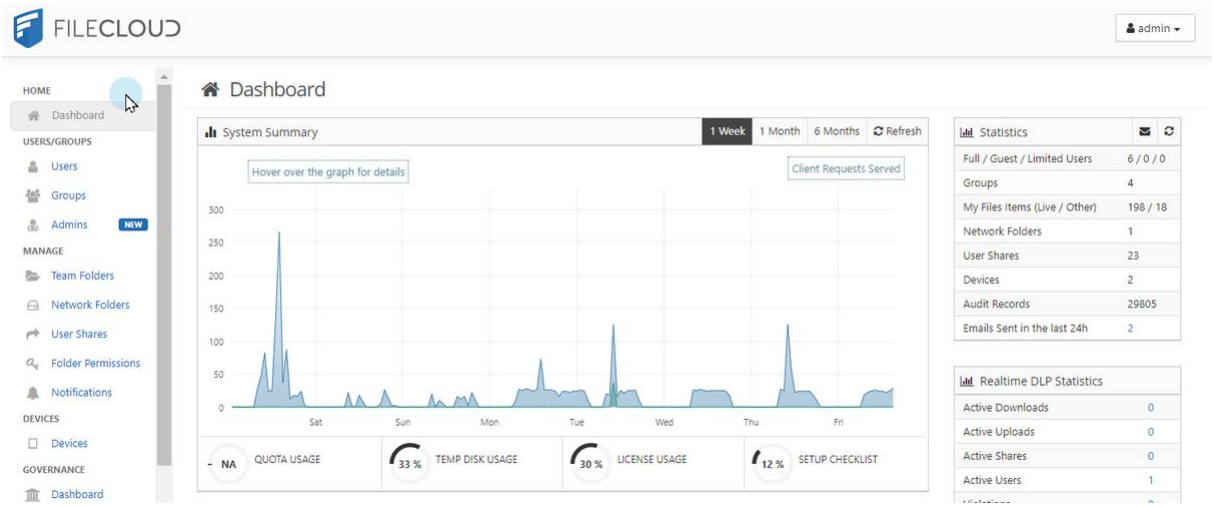
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

**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 (see page 18), click **Manage Mobile Devices**

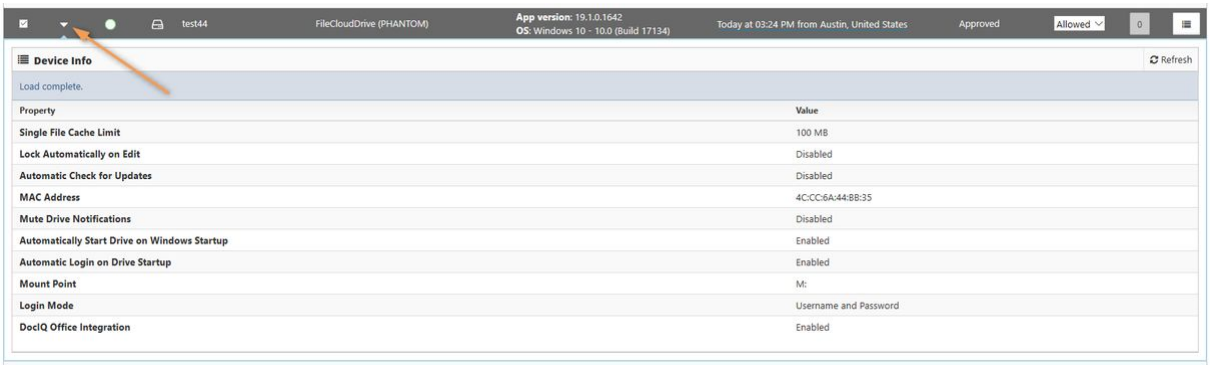
💡 Sometimes a list may start out empty. However, as users connect devices to the FileCloud Server by logging in, the devices will appear.



# How Do You Want to Manage a Device?

The following operations are available from the Device Management panel:

### View Details of a Client Device

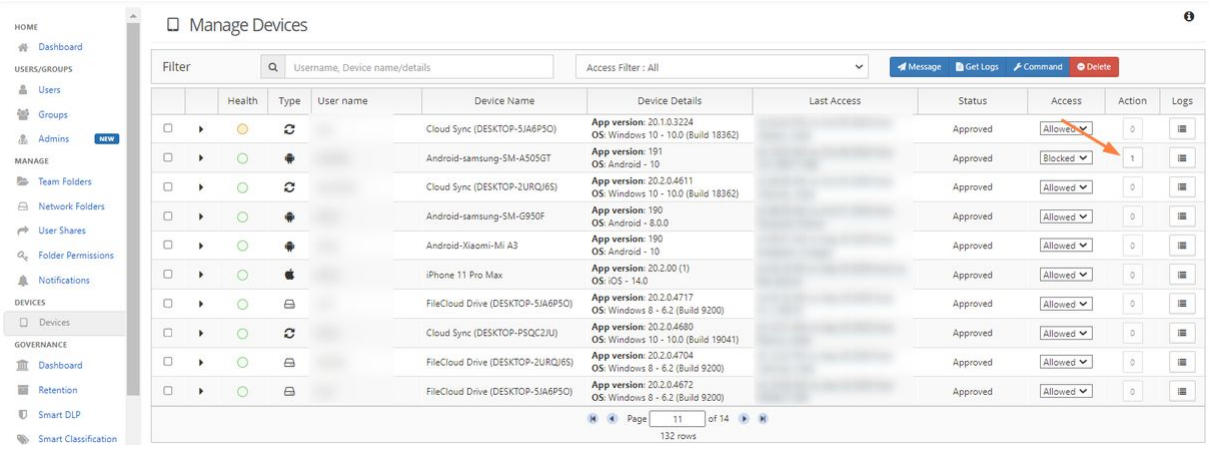



To see the details of a connected device:

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

### View and Manage Actions Queued

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



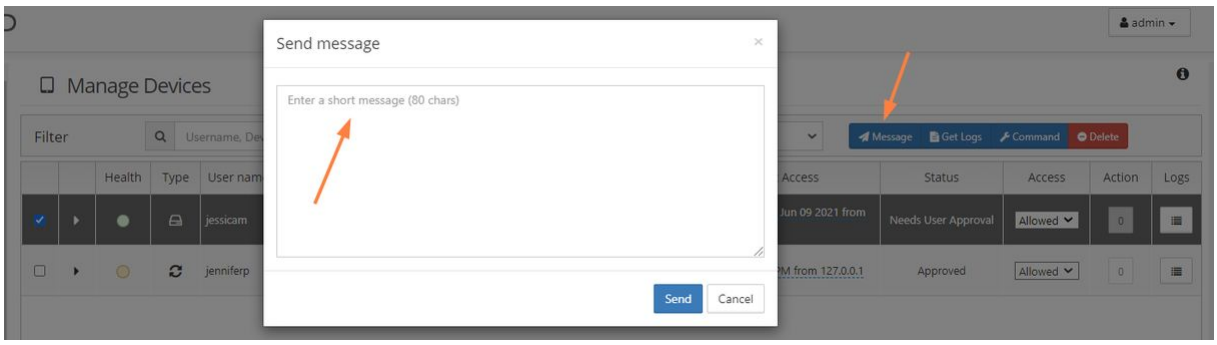

To view Actions:

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

### Add a Message to the Client's Display

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

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




To send a message:

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

### Blocking and Remote Wiping

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

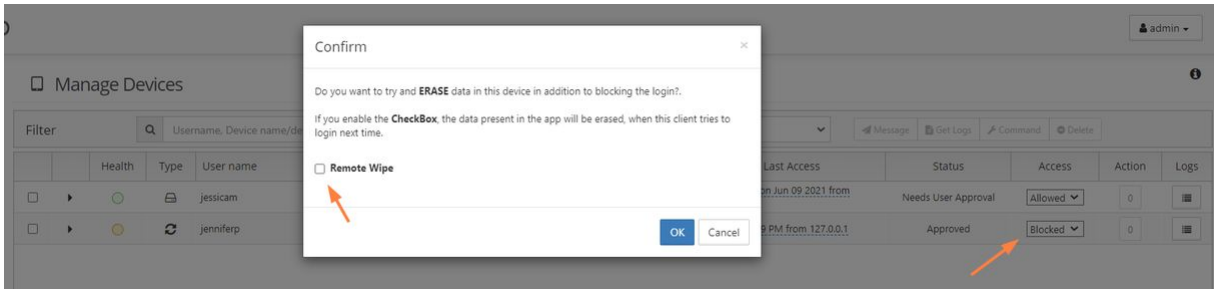
When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

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

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

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

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




**To block (but not wipe remote data):**

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

**To block and wipe remote data in a client device:**

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

### Delete a Client Device Record

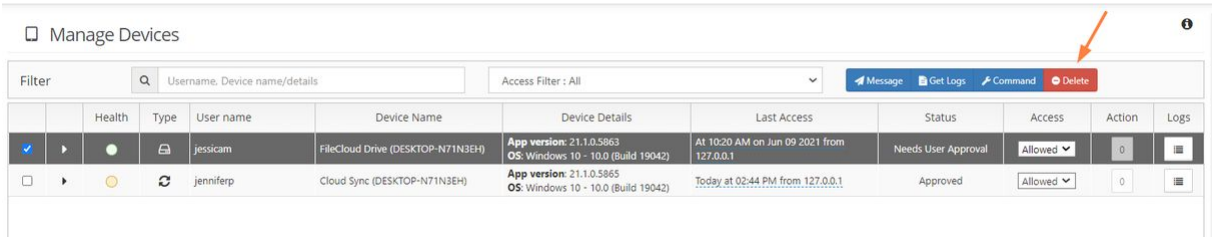
It is possible to delete a client record from the FileCloud system.

You might want to use this feature when:

- The userid is no longer valid

- The associated client record no longer needs to be managed

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




**To delete a client device record:**

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

### 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 (see page 127)
- Automating FileCloud Sync/Drive/OutLook-Addin Installation and Mass Deployment configuration (see page 167)
- Viewing Client Information (see page 181)
- Requesting Client Log Files (see page 182)
- Blocking and Remotely Wiping a Client Device (see page 183)
- Sending a Message to a Client's Display (see page 183)


## Configure Centralized Device Management

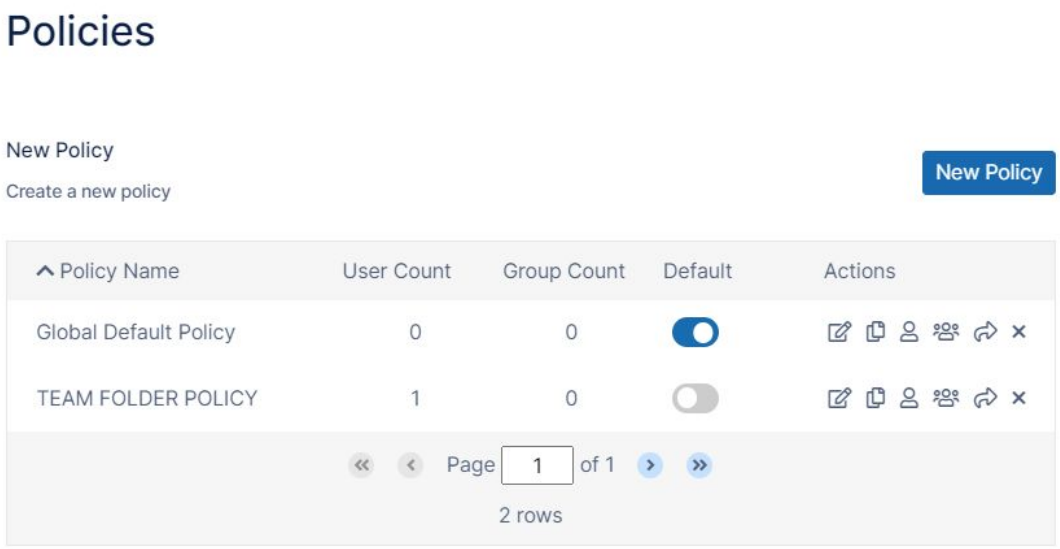
Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

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

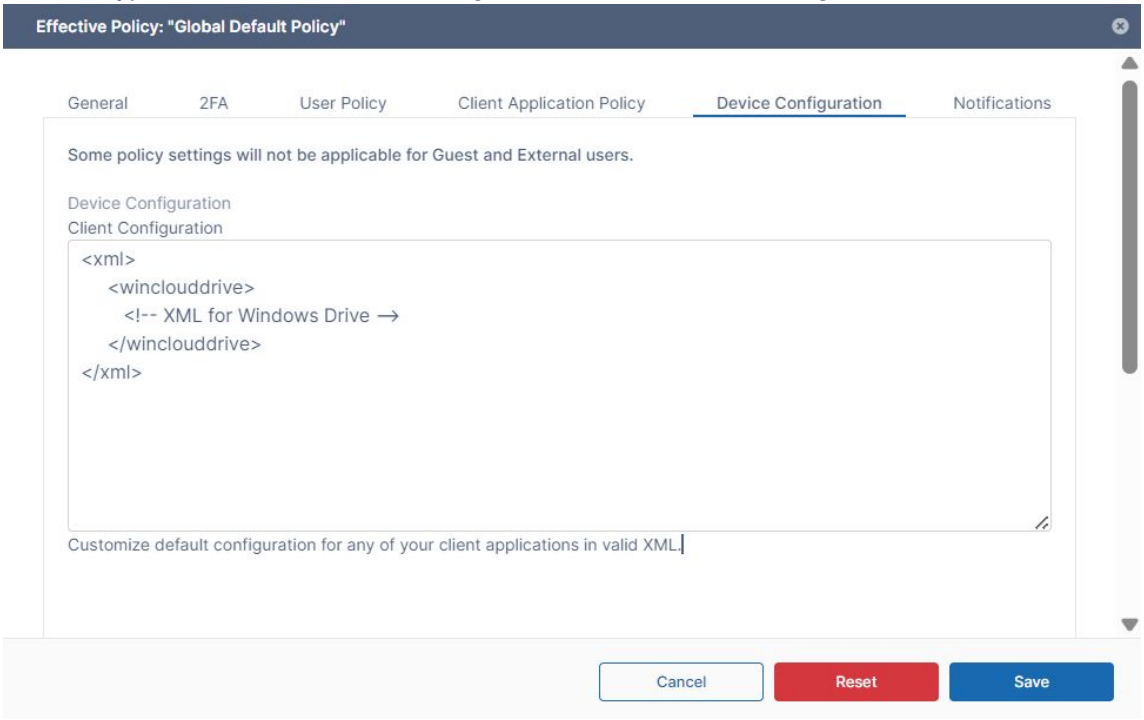
**To set a device configuration for a policy**:

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

The **Policies** settings page opens.




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




5. Click **Save**.

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

```
<xml>


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


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


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


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


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


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



</xml>
```

## What do you want to configure?

- Device Configuration XML For Drive for Mac (see page 130)
- Device Configuration XML For Outlook Add-in (see page 132)
- Device Configuration XML For Server Sync (see page 137)
- Device Configuration XML For Sync (see page 140)
- Device Configuration XML For Windows Drive (see page 154)

- Device Configuration XML for Desktop Edit (see page 157)
- Device Configuration XML for FileCloud Desktop for macOS (see page 159)
- Device Configuration XML for FileCloud Desktop for Windows (see page 163)

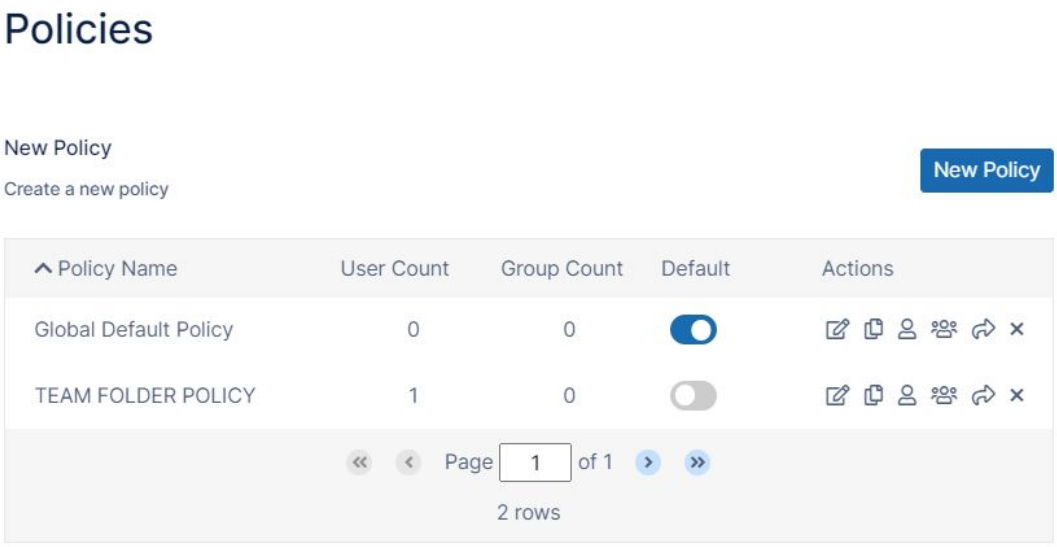
## Device Configuration XML For Drive for Mac

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

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

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

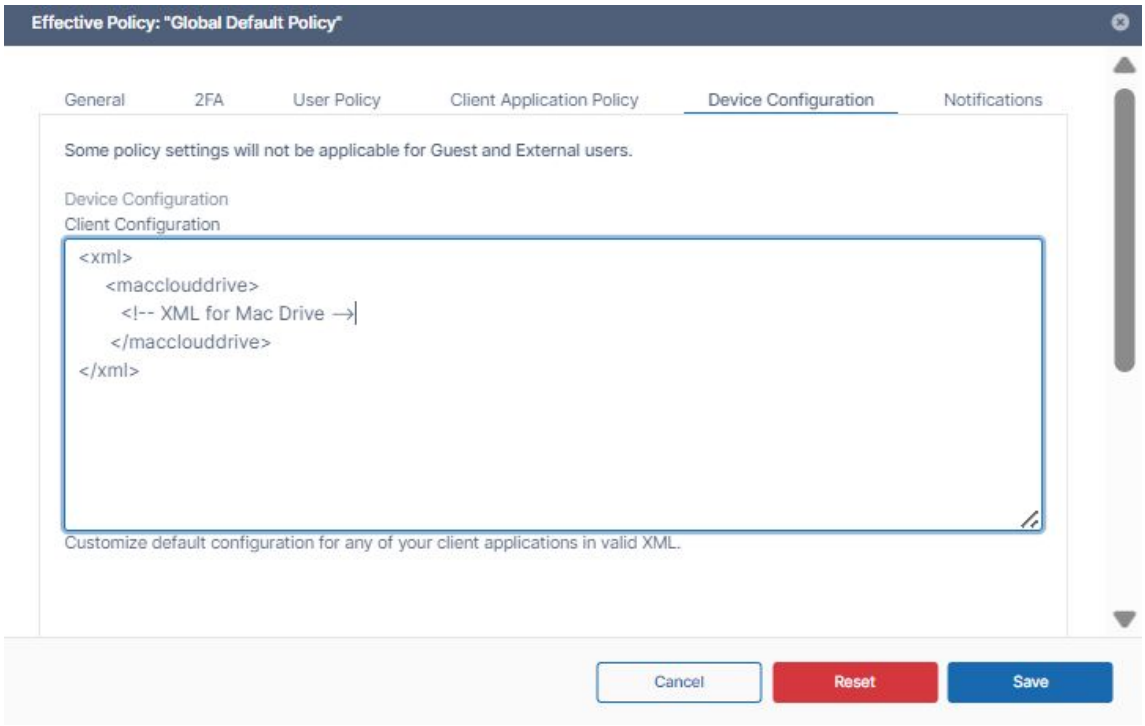
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.




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

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

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




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

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| maxdownloadsizeinmb | Assigns the maximum single file download limit to the supplied value.<br>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> |

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| drivelockonupdate | Setting this value to 1 will enable automatic lock on edit function in FileCloud Drive. Setting this to 0 will disable the drive's lock on edit function | <drivelockonupdate>1</drivelockonupdate> |
| drivemutemessages | Setting this value to 1 will disable system tray notifications being shown to the user. | <drivemutemessages>1</drivemutemessages> |
| driveopenexploreronstartup | Setting this value to 1 will automatically open finder when drive starts up and 0 will disable it. | <driveopenexploreronstartup>1</driveopenexploreronstartup> |
| checkupdates | Setting this value to 1 will enable automatic checking for new versions of FileCloud Drive for Mac and setting this value to 0 will disable it. | <checkupdates>1</checkupdates> |
| disableprecaching | Setting this value to 1 disables precaching.<br><br>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> |

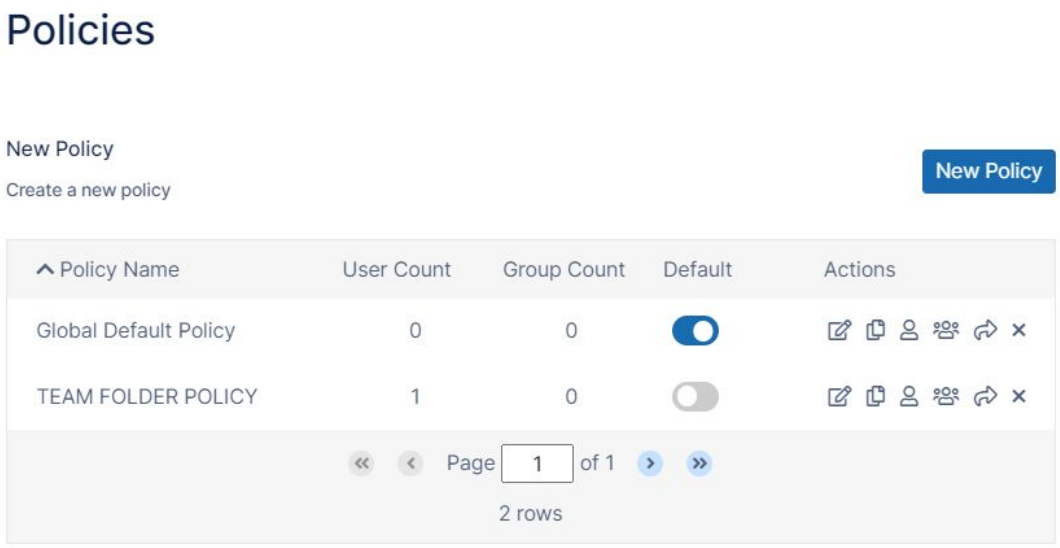
## Device Configuration XML For Outlook Add-in

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

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

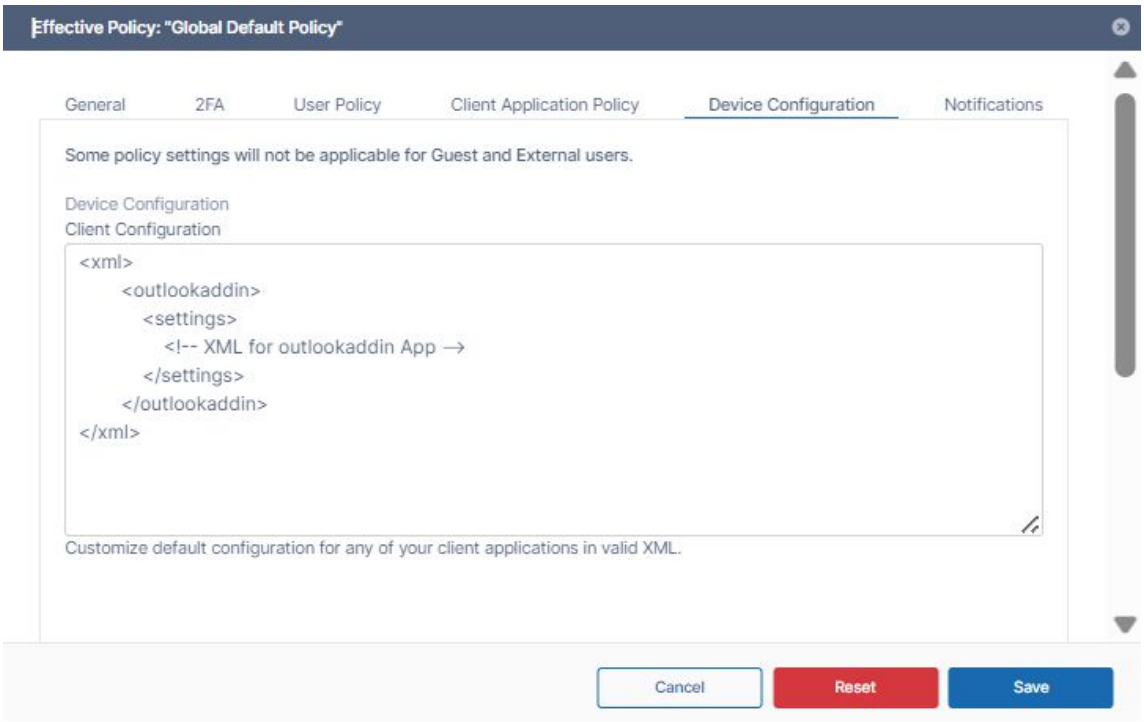
**To set FileCloud's Outlook add-in device configuration for a policy:**

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




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

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




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

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| autouploa d | Whether autoupload is on or off. 0 = off, 1= on | <autoupload>1</autoupload> |
| autouploa dsize | 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 (see page 132)> |
| 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#<br/>Download link: <a href='#url_link#'>#filename#</a><br/ >#password#]]></sharetext> |

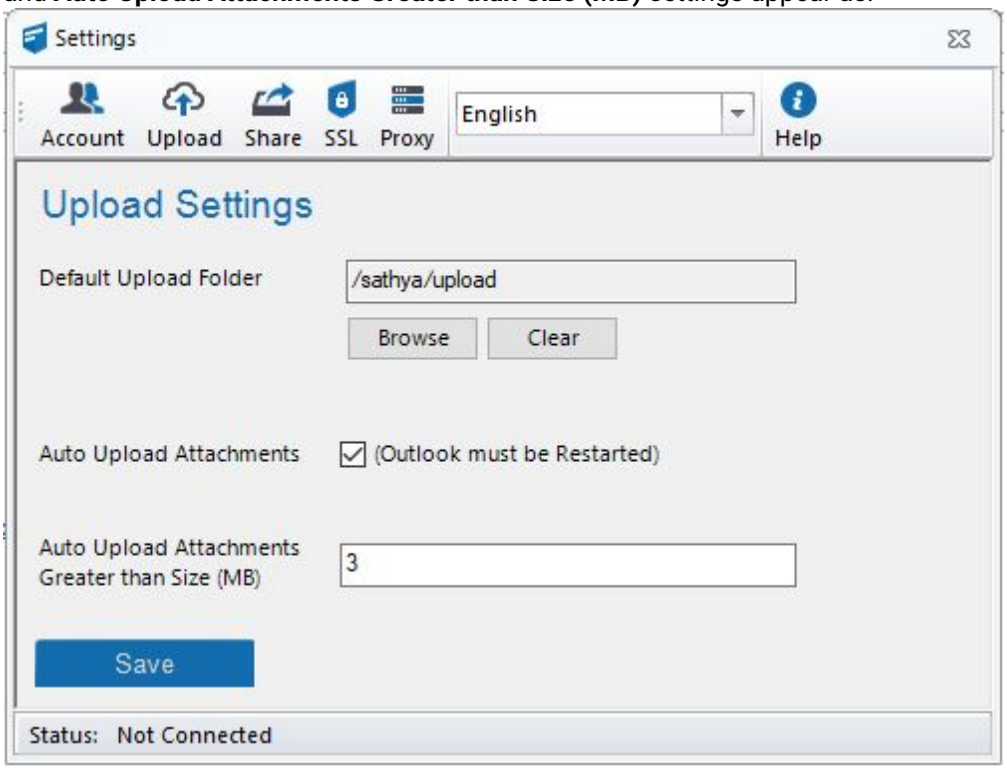
| Parameter (XML Tag) | Value | Example |
|---|---|---|
| proxyserver | Proxy Server URL | <proxyserver>http://proxyserverurl.com</proxyserver (see page 132)> |
| proxyusername | Proxy Server Username | <proxyusername>proxyserverusername</proxyusername> |
| proxypassword | Proxy Server Password | <proxypassword>proxyserverpassword</proxypassword> |
| proxyport | Proxy Server Port | <proxyport>9000</proxyport> |
| ssllevel | Require strict SSL verification of VERIFY_STRICT or VERIFY_NONE | <ssllevel>VERIFY_STRICT</ssllevel> |
| sslverify | Connect only TLS 1.2 server. Empty string or TLSV1_2_CLIENT_USE | <sslverify><sslverify> |

### To set default values for auto upload:

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

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

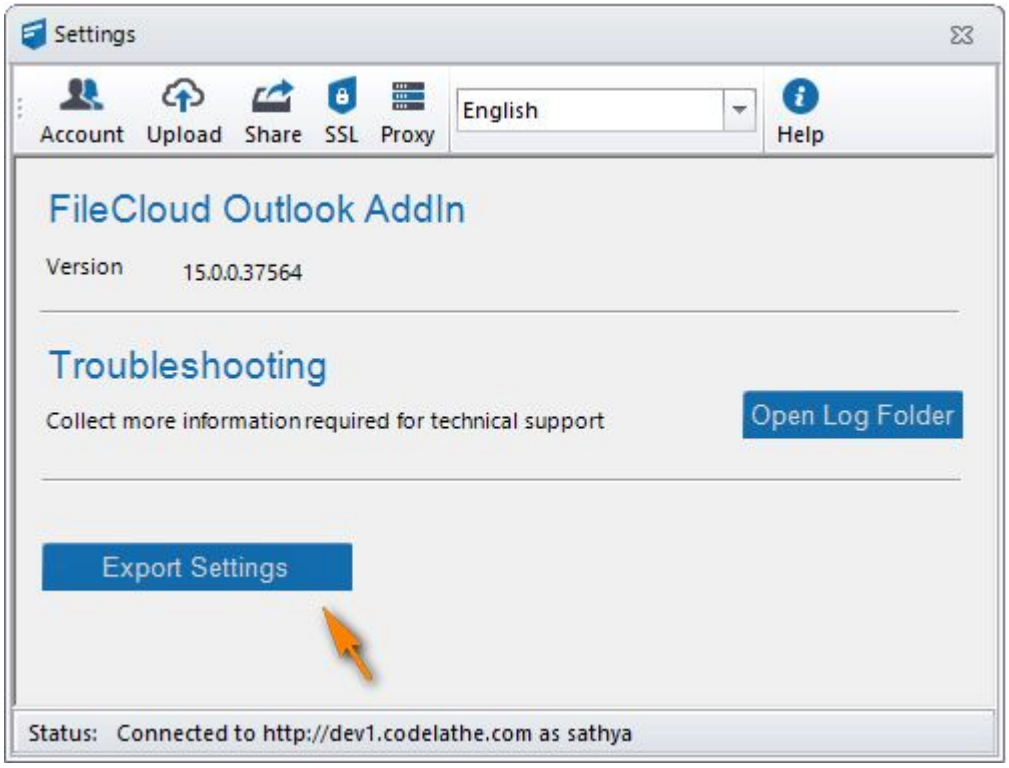
When the Outlook Add-in is opened, and **Settings > Upload** is accessed, the **Auto Upload Attachments** and **Auto Upload Attachments Greater than Size (MB)** settings appear as:




### Tips and Tricks

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

**Show me how...**




## Device Configuration XML For Server Sync

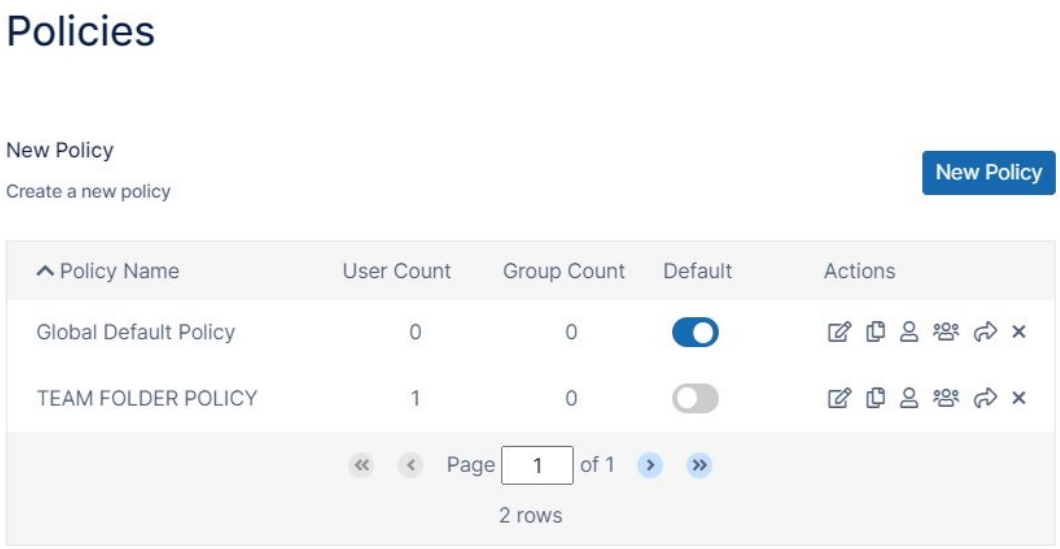
Client Device configuration settings can be configured remotely using policies.

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

**To set a ServerSync device configuration in a policy**:

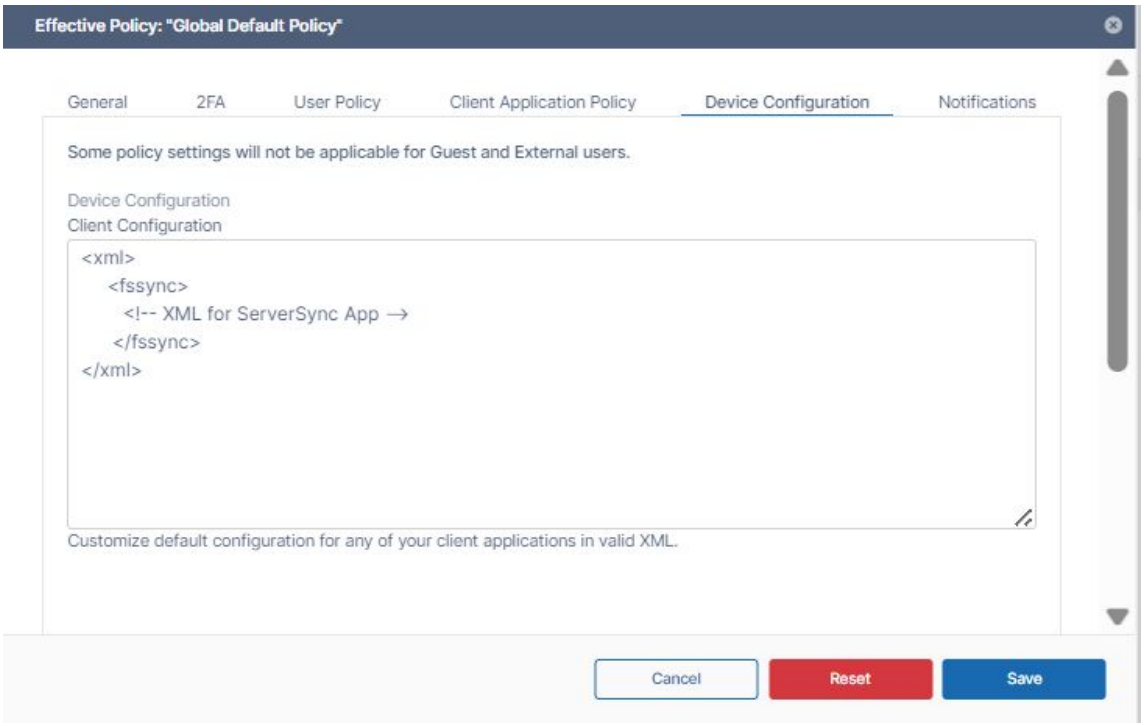
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.




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

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




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

| XML Tag | Value | Example |
|---|---|---|
| limit_folder_count | Number of folders to sync. If key is not specified, then there are no folders to sync. | <limit_folder_count>0</limit_folder_count> |
| limit_folder_1<br>limit_folder_2<br>limit_folder_3<br>... | Depending upon the number of folders specified in the limit_folder_count, you will need to have the appropriate number of entries.<br>The folder value is specified using 5 parameters using the following format<br>***<REMOTE FOLDER>\|<LOCAL FOLDER>\|<PERMISSIONS>\|<SYNC TYPE>\|<SYNC DISABLED>***<br>***<REMOTE FOLDER>*** = E.g.: /john/folder1<br>***<LOCAL FOLDER>*** = E.g: C:\data\localfolder<br>***<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<br>***<SYNC TYPE>*** = 0 (2-way sync) or 1 (remote to local sync).<br>***<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.<br>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.<br>When set to 1, approval is required if > 50 files are deleted AND percent of files being deleted is > **deleteapprovalpct**.<br>This applies only to file deletions in the local sync folder. | <skipdeleteapproval>1</skipdeleteapproval> |
| currentlanguage | Allows changing the current language of the Server sync app | <currentlanguage>dutch</currentlanguage> |

## Device Configuration XML For Sync

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

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

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

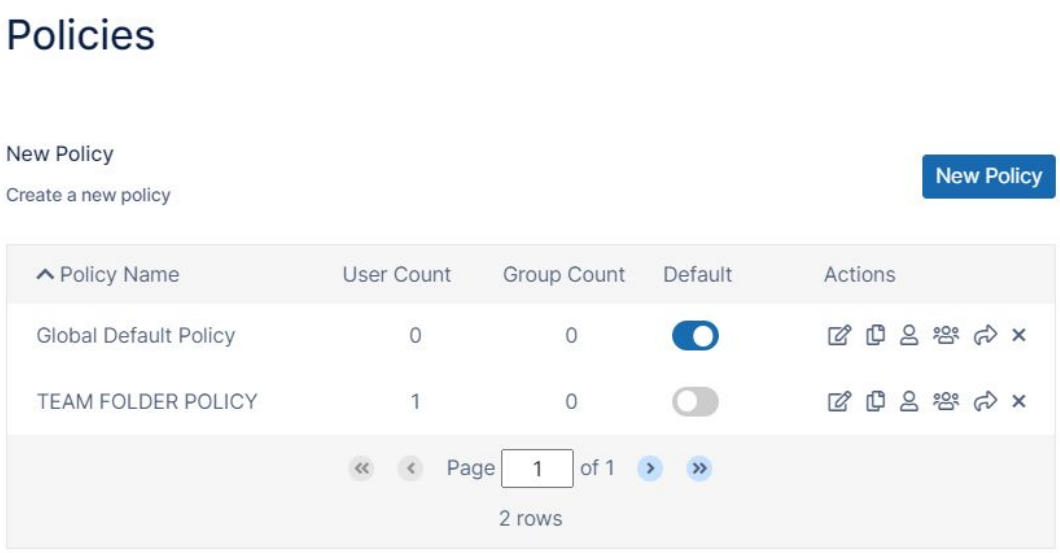
See What XML settings allow users to modify folders? below.

## FAQs

**How do I enter device configuration XML for Sync?**

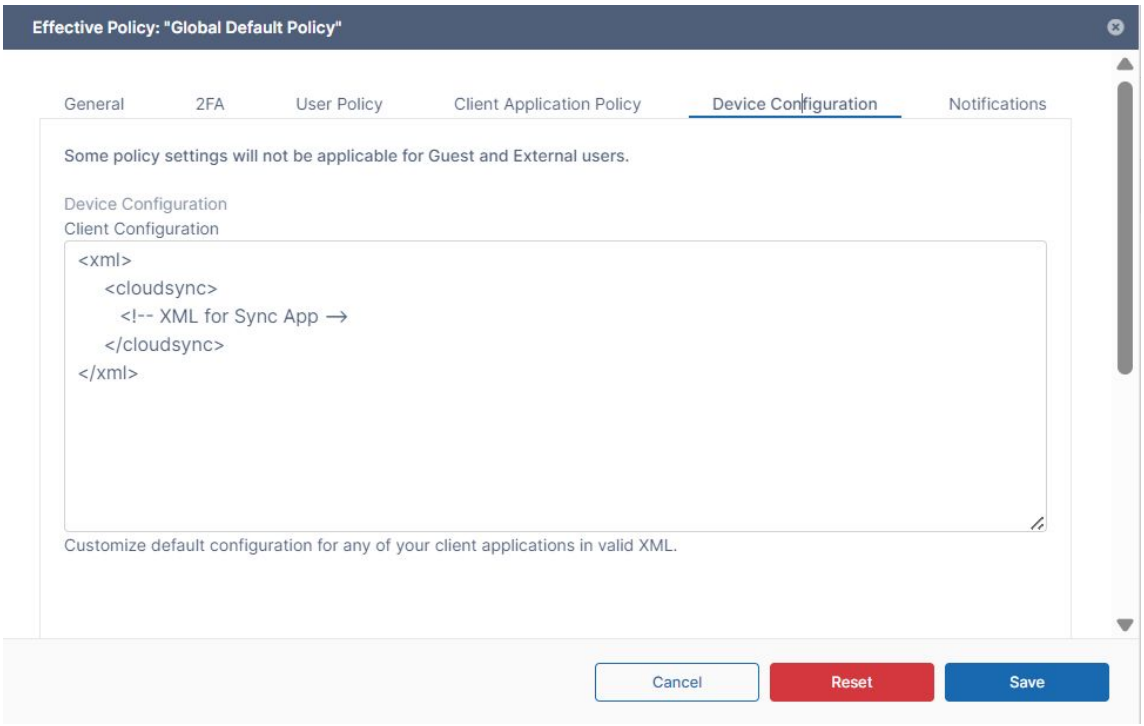
**To set a FileCloud Sync device configuration in a policy**:

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




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

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




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

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

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

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| skipdeleteapproval | 0/1 - Whether approvals are needed for bulk sync changes. Default is disabled.<br>When set to 1, approval is required if > 50 files are deleted AND percent of files being deleted is > **deleteapprovalpct**.<br>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.<br>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.<br>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.<br>⚠ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set. | <altbwforupload></altbwforupload> |
| altbwfordownload | Specifies that alternative settings should be used instead of the global bandwidth limit when downloading files from the server to the client in terms of KB only.<br>⚠ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set. | <altbwfordownload></altbwfordownload> |
| altbwfromtime | Specifies the starting time when the alternative settings should be used instead of the global bandwidth limit.<br>Time must be expressed in the format HH:MM:SS<br>⚠ If *altbwforupload* or *altbwfordownload* is specified but *altbwfromtime* and *altbwtotime* are missing, then the bandwidth values will not be set. | <altbwfromtime>16:45:00</altbwfromtime> |

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

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

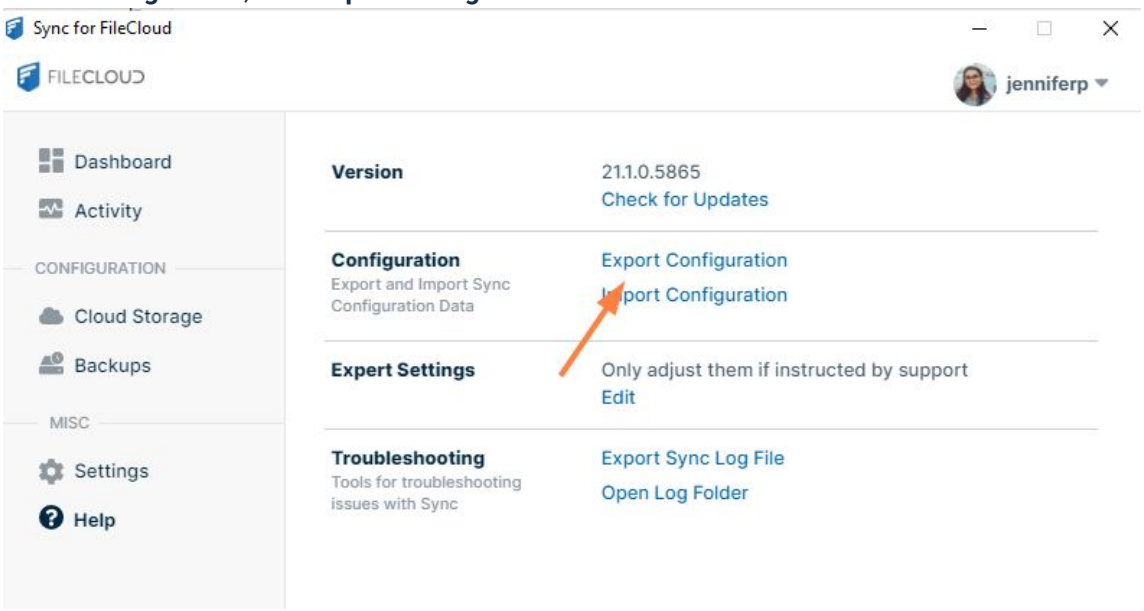
**How do I get the configuration XML for Sync?**

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.<br>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.<br>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.<br>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.<br>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.<br>This value can be any number such as: {-1, 0, 1, 2, 3, 4, 5, 6} where:<br>• -1 means every day<br>• 0 means Sunday<br>• 1 means Monday<br>• and so on.. | <altbwschedule_dayofweek>3</altbwschedule_dayofweek> |

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

**What is the XML code for Active Sync Hours?**

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

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

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

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

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

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

**What XML settings allows users to modify folders?**

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

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

- Selective Sync folders
- Network folders
- Backup folders

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

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

## Scenarios

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

### Controlling modifications to selective sync folders

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

### Controlling modifications to selective network folders

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

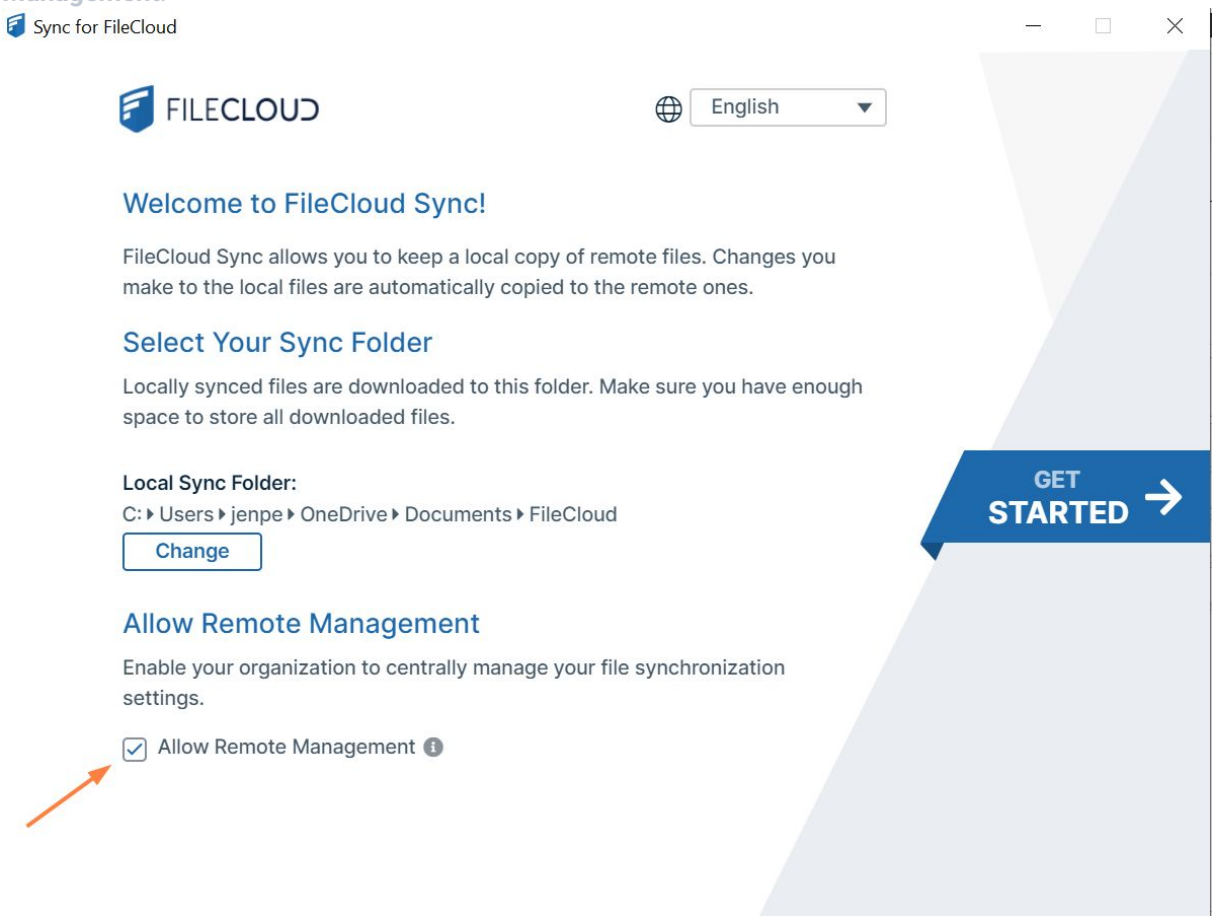
| | | |
|---|---|---|
| *None set but other settings are present* | 1 | Because *allowuserconfigfornwfolders* is set to enable modifications:<br>• Sync users CAN modify Network Folders, irrespective of any other settings in the config. |
| *None set but other settings are present* | 0 | Because *allowuserconfigfornwfolders*is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

### Controlling modifications to selective backup folders

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

### How do I prevent users from overriding remote management?

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




This setting is also available in the Settings window.

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

**To add the registry key**:

1. Add a registry key under:

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

2. Name the registry key:

```
allowcentralmgmtusermodify
```

3. Restart the computer.

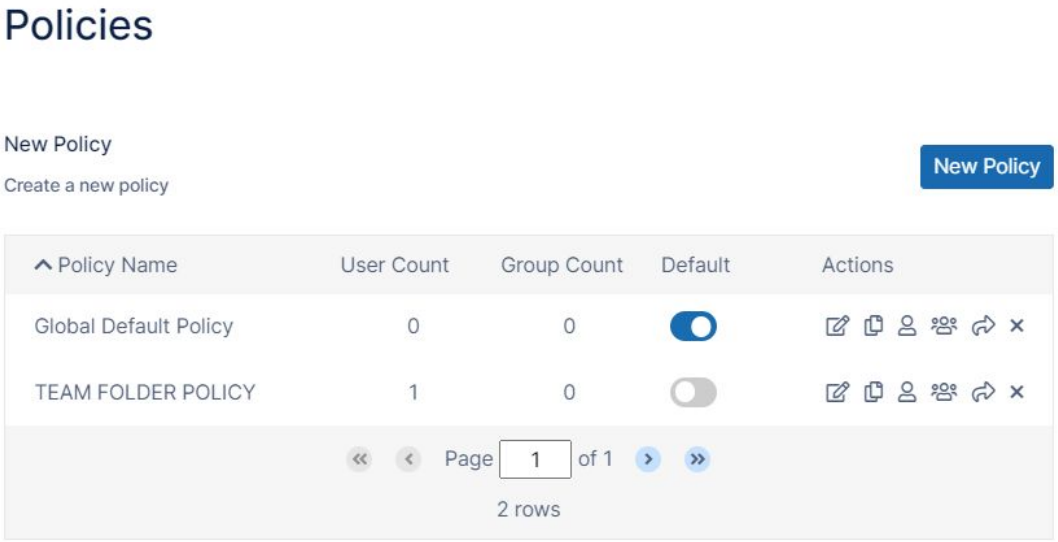
## Device Configuration XML For Windows Drive

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

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

### To set a FileCloud Drive device configuration in a policy:

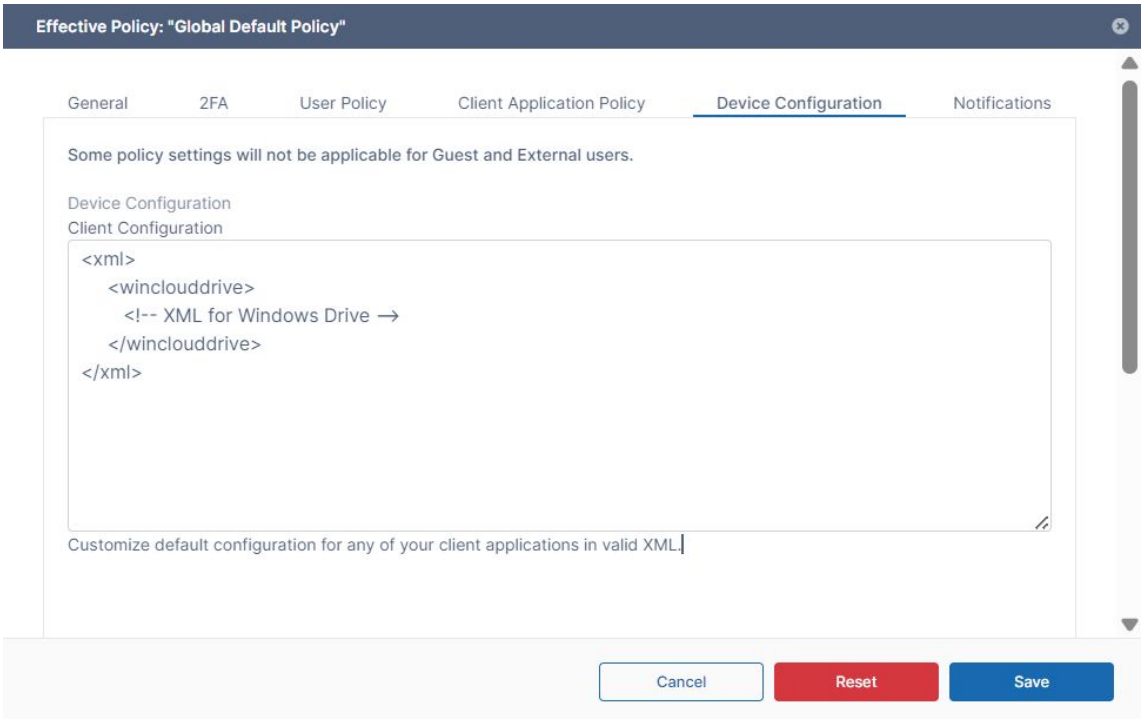
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.




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

```
<xml>
```

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




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

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| maxdownloadsizeinmb | Assigns the maximum single file download limit to the supplied value.<br>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.<br>**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><br>or<br><cachelocation>${HOME}\DriveCache<cachelocation><br>or<br><cachelocation>C:\somepath\${USERID}\DriveCache</cachelocation> |

| Parameter (XML Tag) | Value | Example |
|---|---|---|
| disableprecaching | Setting this value to 1 disables precaching.<br>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<br>english, dutch, french | <currentlanguage>french</currentlanguage> |

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

## Device Configuration XML for Desktop Edit

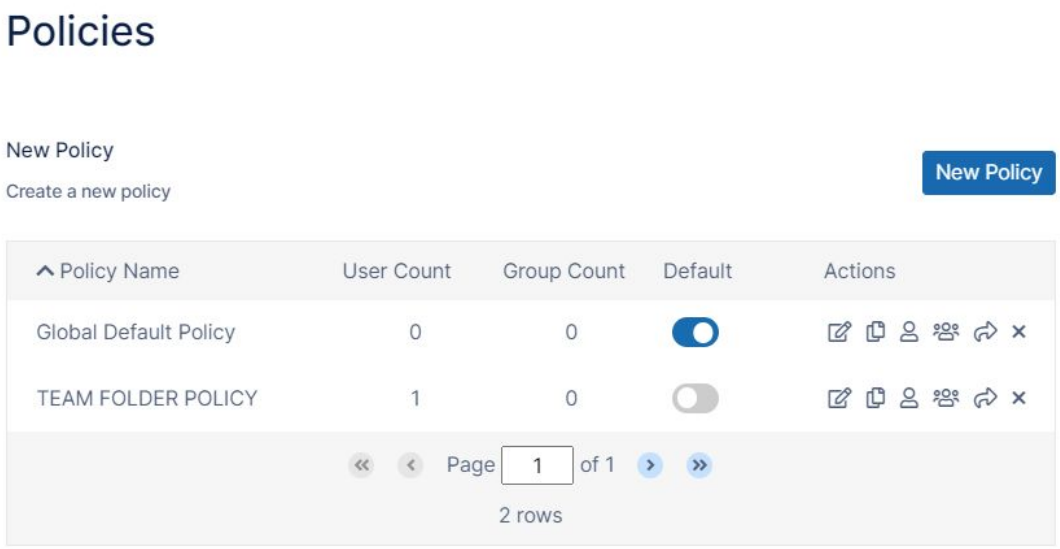
Client Device configuration settings can be configured remotely by specifying the configuration XML using policies.

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

**To set FileCloud Desktop Edit device configuration in a policy:**

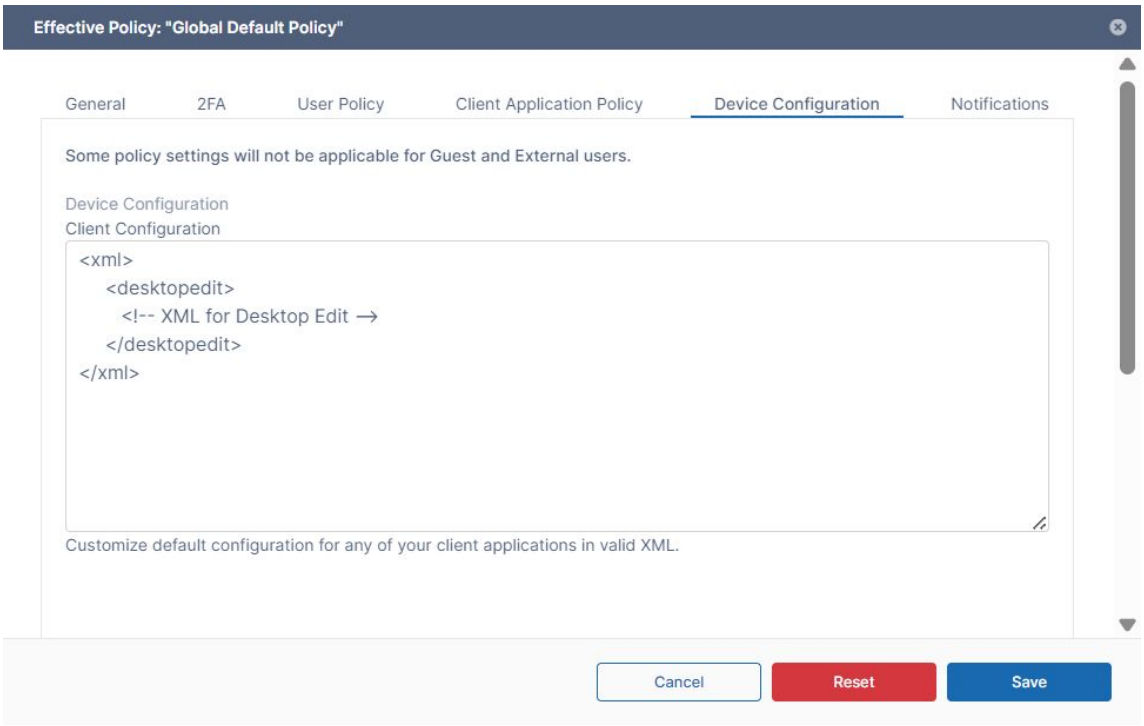
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** settings page opens.




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

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




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

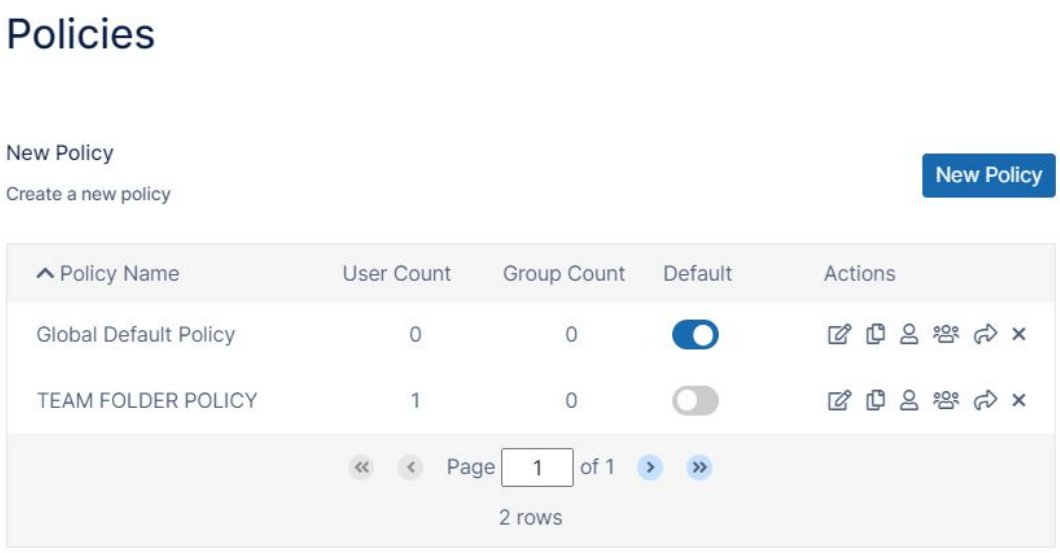
| Parameter (XML Tag) | Value | Example |
|---|---|---|
| lockfiles | 0/1 - Enable or Disable autolocking of files | <lockfiles>1</lockfiles> |
| runatstartup | 0/1 - Enable or Disable running application at OS startup | <runatstartup>1</runatstartup> |
| mutenotifications | 0/1 - Enable or Disable notifications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

## Device Configuration XML for FileCloud Desktop for macOS

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

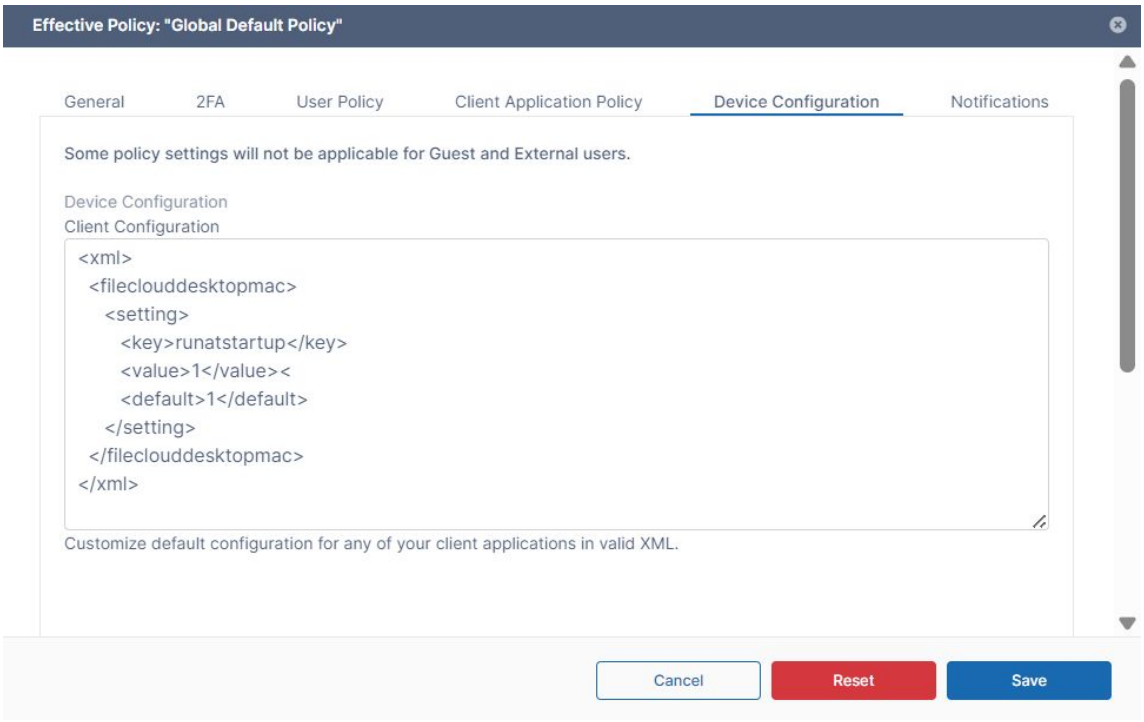
For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

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




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

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




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

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

| Parameter (Key) | Description | Values |
|---|---|---|
| lockonopen | Automatically lock files when they are opened. | 0 (disabled)<br>1 (enabled) default |
| runatstartup | Run FileCloud Desktop for macOS on system startup. | 0 (disabled)<br>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<br>"debug"<br>"trace" |

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

### Example:

The code below shows example settings:

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

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

In this example:

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

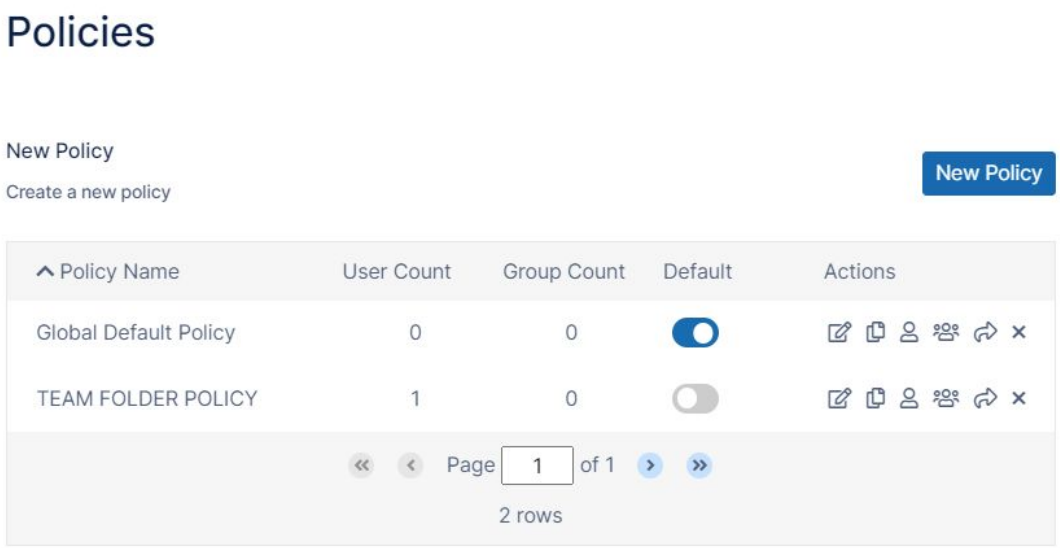
If a key is not supported or a value is incorrect, the application skips it and logs a warning message.

## Device Configuration XML for FileCloud Desktop for Windows

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

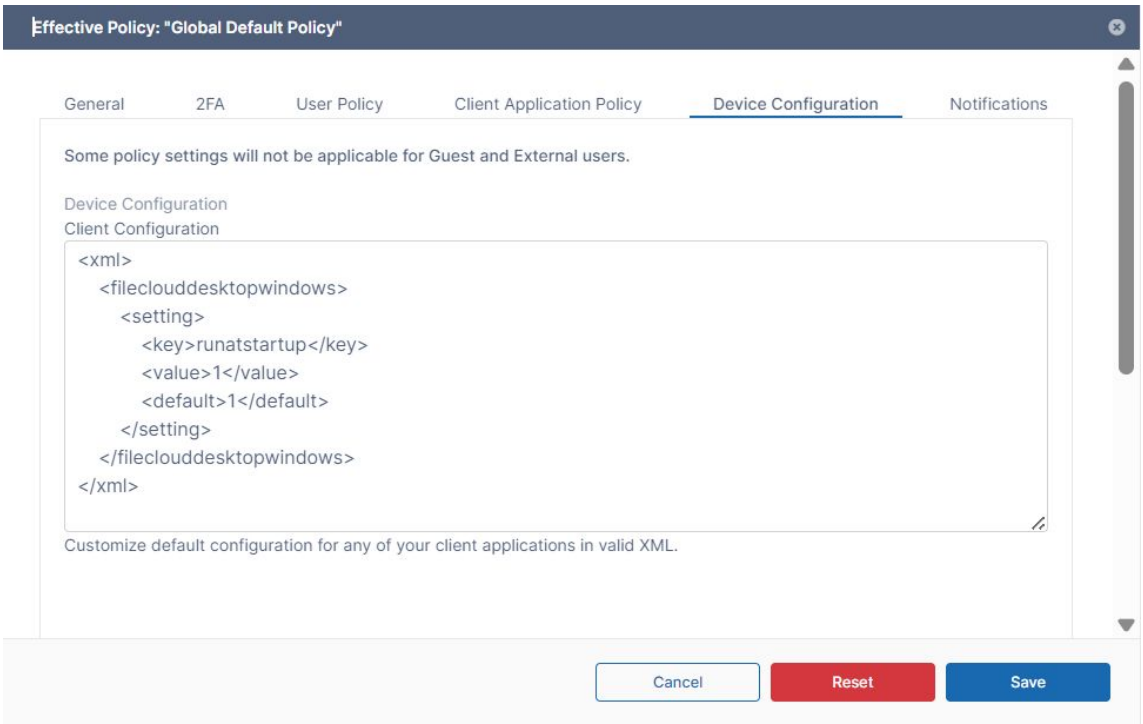
For most clients, if the user changes the configuration locally, then the remote settings configured by the Administrator will override those settings the next time the client refreshes its settings.

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




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

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




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

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

| Key | Description | Values |
|---|---|---|
| runatstartup | Run FileCloud Desktop for Windows on system startup. | 0 (disabled)<br>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<br>"debug"<br>"trace" |

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

### Example:

The code below shows example settings:

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

```
  <setting>
    <key>mutenotifications</key>
    <value>0</value>
  </setting>
</filecloudesktopwindows>
</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

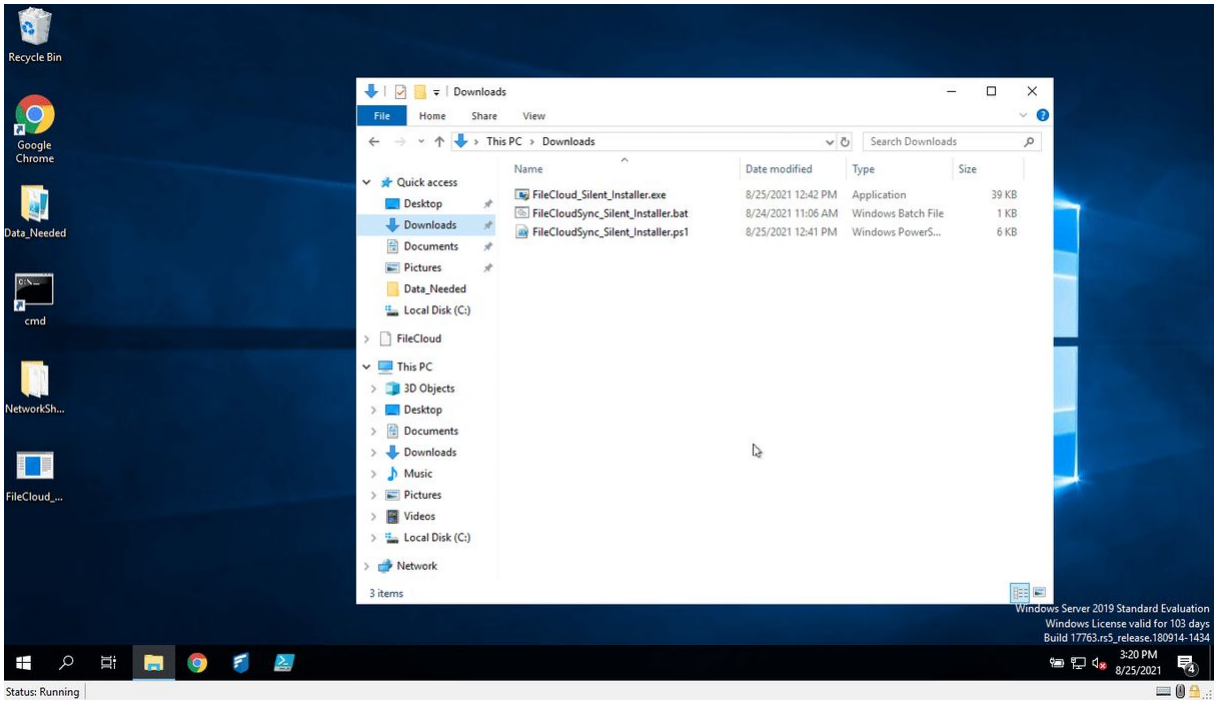
#### What does the Script do?

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 (see page 185)
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

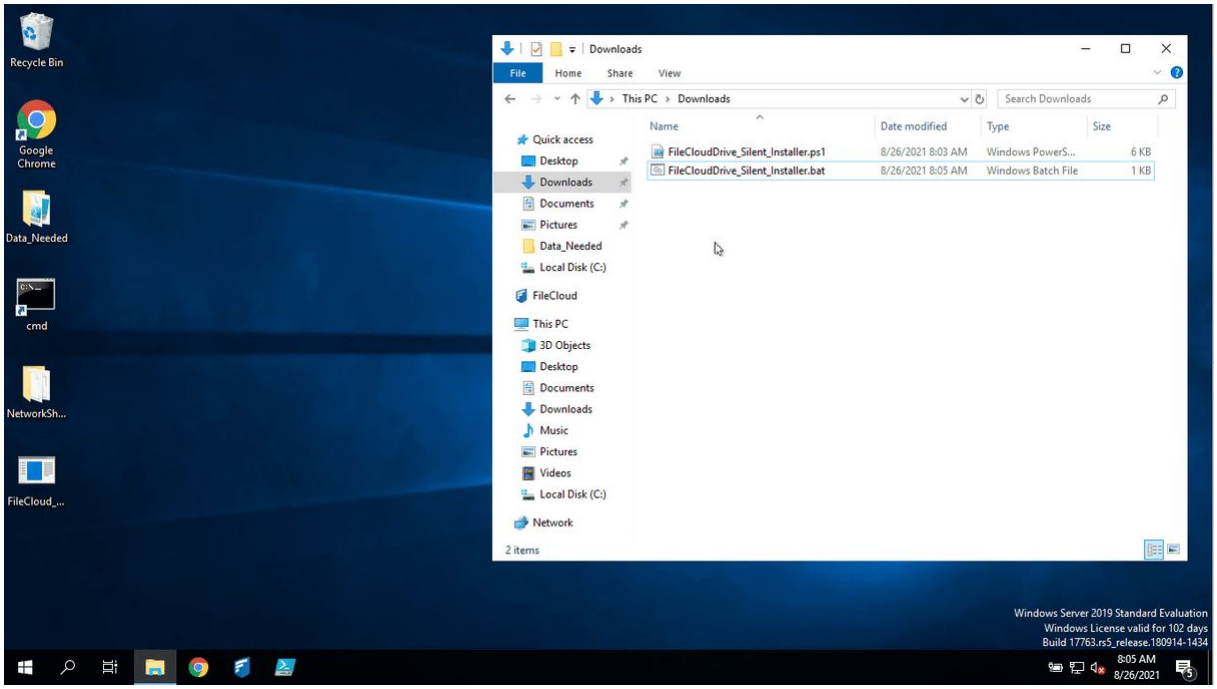
```
####Silent FileCloud Sync Installation & Mass Deployment Configuration####

##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 loggin##########" | 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 loggin##########" | 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.codelathe.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 loggin##########" | 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 loggin##########" | 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.codelathe.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 loggin#########" | 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 loggin#########" | 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
```

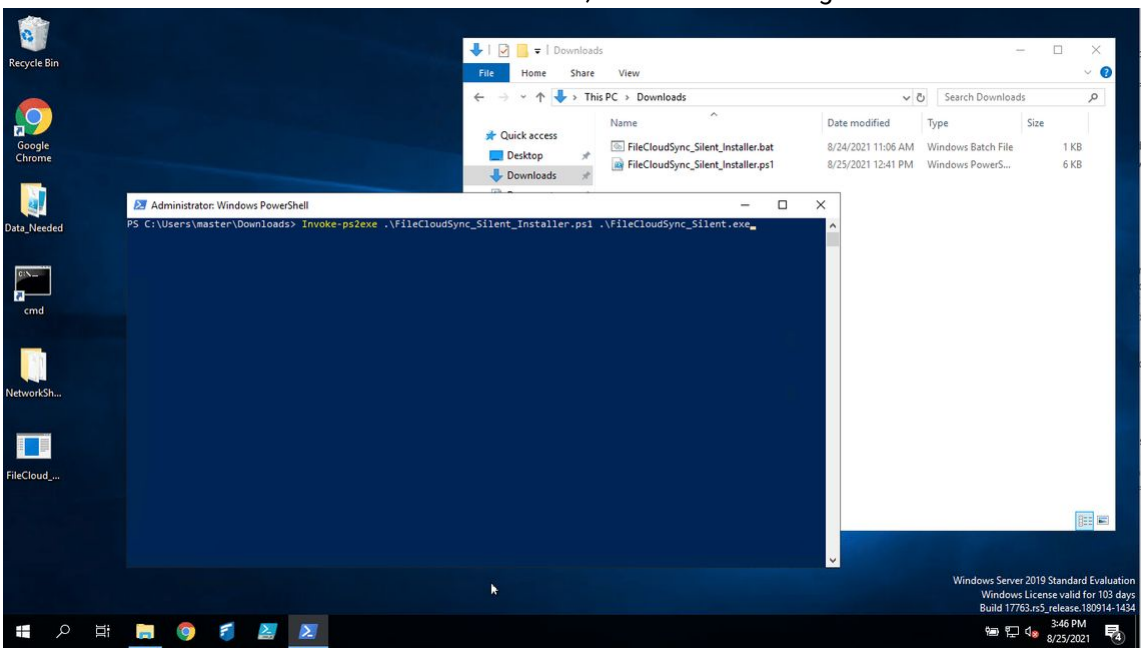
2. Once the above is completed enter "Y" to install the Module

```
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:

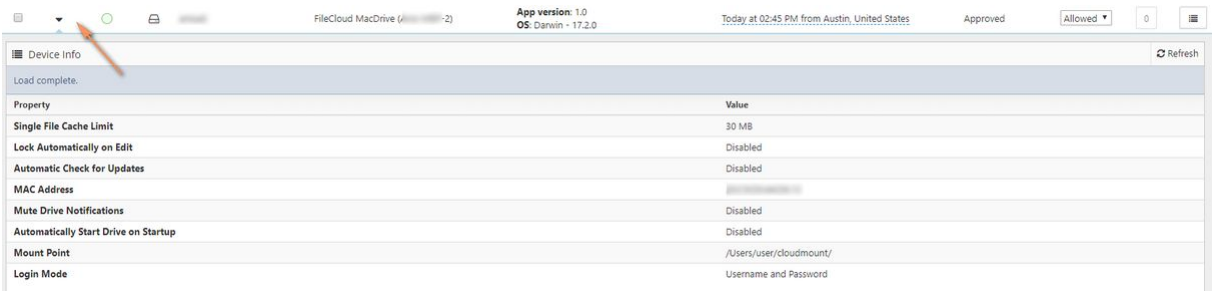



## Viewing Client Information

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

- Health
- State

Figure 1. Device Information




## What do you want to view?

### Client Health Information

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

To show information related to a device:

1. In the Devices table, click the device.

### Client State Information

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

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

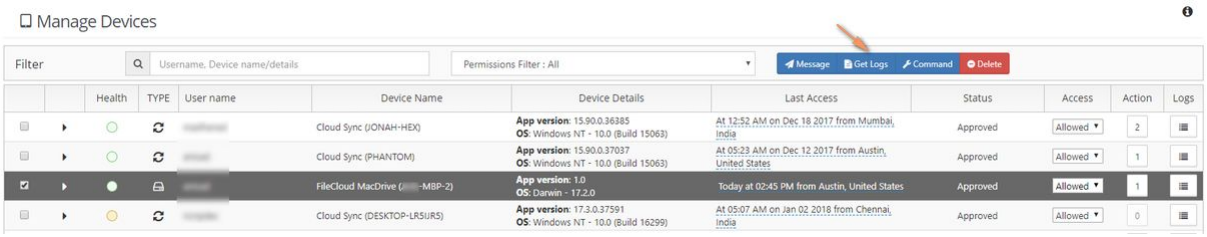
## Requesting Client Log Files

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

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

The logs are uploaded by the client

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




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

## Blocking and Remotely Wiping a Client Device

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

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

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

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

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

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

**Steps to block and wipe remote data in a client device**

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

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

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

## Sending a Message to a Client's Display

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

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

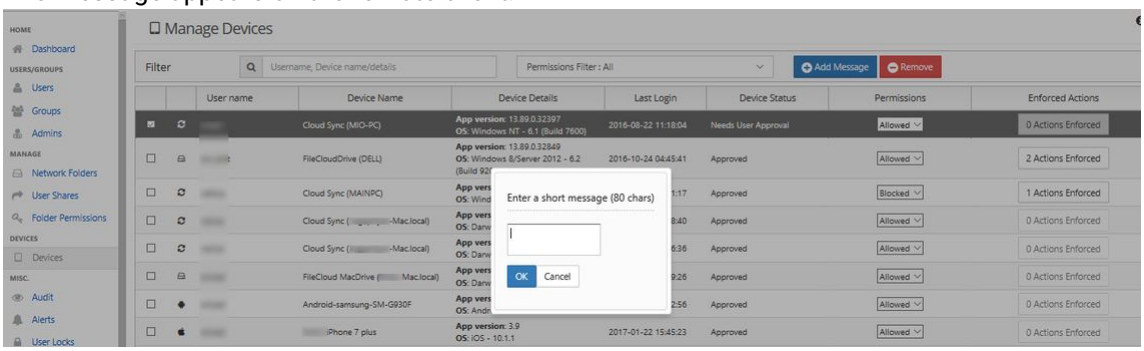
displayed in the order it was entered. The messages will be shown only once per client and during

Message will be shown

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

Steps to add message

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




# iOS Device Management

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

## Configuring Automatic Camera Uploads

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

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

**Why would I enable this feature?**

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

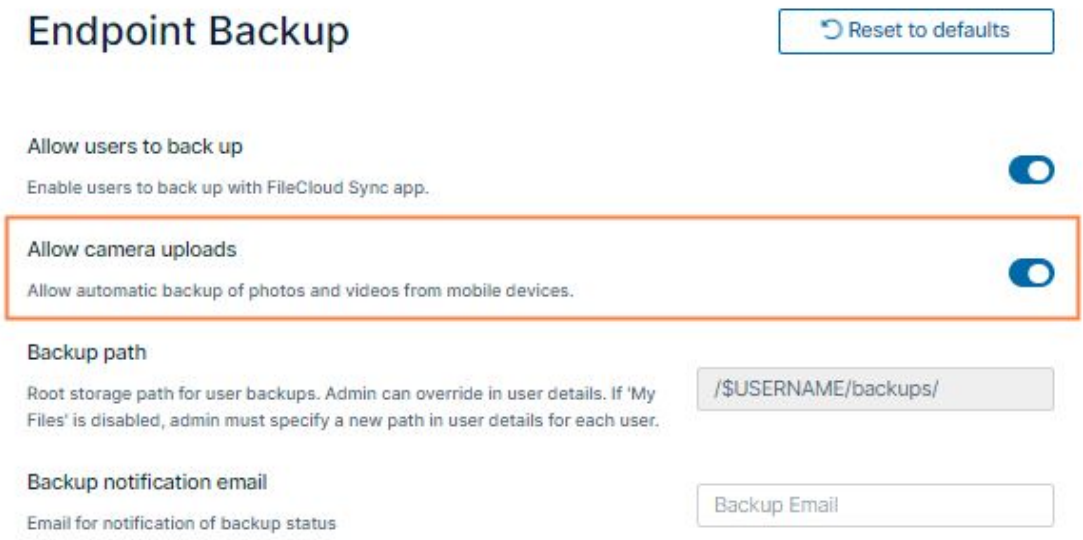
- Instead users saving all of their work files on their mobile device, they can save them to the FileCloud.
- Mobile users can spend time constantly managing their images/videos to free up more space unless they are able to save them to FileCloud.
- If you are concerned about privacy and security, work-related files and photos are stored securely in FileCloud.

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

**To enable automatic camera uploads:**

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

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




## 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.<br>example: https://files.xyz.com[7] | YES | YES | YES | YES | YES |
| profile | String | User name to use to login.<br>example: john or john@company.com[8]<br>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 |

7. https://files.xyz.com/
8. mailto:john@company.com

| 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.<br>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 |
| officehelperlockonedit | String | Automatic locking in FileCloud for Office (FFO/DocIQ) | YES | NO | NO | NO | NO |
| syncfolderlocation | String | Path to use for the sync folder location.<br>DEFAULT - use the default location<br>Absolute Full Paths - e.g. c:\filecloudsync<br>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.<br>DEFAULT - use the default location<br>Absolute Full Paths - e.g. c:\filecloudsyncdata<br>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 synching<br>"0" - Default, does not remove unshared folders<br>"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.<br>"password" - Password authentication<br>"sso" - SSO authentication<br>"devauth" - Device code authentication | YES | NO | NO | NO | NO |
| drivecachelocation | String | Path to use for drive cache<br>DEFAULT - use the default location<br>Absolute Full Paths - e.g. c:\filecloudrive<br>Expanded Paths - e.g. %APPDATA%\FileCloud Drive\data (Windows Only) or ${HOME}\FileCloud Drive (Windows and Mac OSX) | NO | YES | NO | NO | NO |
| enableshortcachepath | String | Whether to use a short path made up of random digits or to use "DOMAIN@USERNAME" for the folder in the cache. Use this option to avoid exceeding the maximum path length.<br>"0" - Default, use DOMAIN@USERNAME<br>"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<br>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 cerificates. If this key is not provied, the default is strict verification<br>VERIFY_NONE: disable SSL Verification checking<br>VERIFY_STRICT: enables strict SSL Verification checking | YES | YES | YES | YES | YES |
| driveloginmode | String | Directive to use password authentication or device code authentication<br>"0" - Password authentication<br>"1" - Device Code authentication<br>"2" - SSO authentication | NO | YES | YES | NO | NO |
| drivelockonupdate | String | Directive to lock file when opened for modification<br>"0" - No lock while editing<br>"1" - Auto Lock while editing | NO | YES | YES | NO | NO |
| drivemutemessages | String | Show or hide automatic information messages from drive<br>"0" - Do not mute messages<br>"1" - Mute messages | NO | YES | YES | NO | NO |
| officehelperdisabled | String | Whether to disable FileCloud for Office (FFO/DocIQ)<br>"0" - Do not disable FileCloud for Office (FFO/DocIQ)<br>"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<br>"0" - Do not display dashboard on startup<br>"1" (default) Display dashboard on startup | NO | YES | YES | NO | NO |
| driveopenexploreronstartup | String | Automatically launch explorer on startup of drive<br>"0" - Do not start explorer on startup<br>"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).<br>"0" - (default) Do not set mount label to unique value.<br>"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.<br>"0" - (default) Do not upload of thumbs.db files.<br>"1" = Upload thumbs.db files | NO | YES | NO | NO | NO |
| disableautologin | String | Whether to prevent Drive from remembering the password and automatically logging in.<br>"0" - (default) Allow auto-login<br>"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.<br>Note: When this is enabled, log-in information is not saved, and must be re-entered each time Drive is started.<br><br>"0" - (default) Do not allow multiple instances to run<br>"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.<br><br>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.<br><br>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.<br>Default types are:<br>txt,rtf,doc,docx,xls,xlsx,ppt,pptx,indd | NO | YES | YES | NO | NO |

| Parameter | Type | Notes | Sync | Windows Drive | Mac Drive | Office Add-On | Outlook Add-On |
|---|---|---|---|---|---|---|---|
| disablerecovering | String | 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.<br>"0" - (default) Files are copied to recovered folder before upload occurs.<br>"1" - Files are copied to recovered folder after upload is attempted if upload fails. | NO | YES | YES | NO | NO |
| disableprecaching | 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.<br>"0" – (default) File/folder directory is retrieved when Drive starts up.<br>"1" - File/folder directory is retrieved when a user starts navigating the folders. | NO | YES | YES | NO | NO |
| lockexpirationinmin | 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 | Sync | Windows Drive | Mac Drive | Office Add-On | Outlook Add-On |
|---|---|---|---|---|---|---|---|
| disablelockexpiration | String | Whether or not to enable expiring of locks. By default, locks on files expire after 10 minutes or the time set in **lockexpirationinmin**.<br>"0" - (default) Use expiration times set for file locks.<br>"1" - Do not use expiration times on locks. Locks expire on files when users close them. | NO | YES | YES | NO | NO |
| enablethumbnailpreview | String | Whether or not to display thumbnails and previews of listed files.<br>"0" - (default) Do not display thumbnails and previews (this reduces network traffic since files are downloaded when thumbnails and previews are generated)<br>"1" - Display thumbnails and previews. | NO | NO | YES | NO | NO |
| maxdownloadsizeinmb | String | Default single file download limit in MB.<br>0 - No limit<br>Other options can be 10,30,50, 100 | NO | YES | YES | NO | NO |
| allowcentralmgmt | String | Allow central management<br>0 - No Central Management<br>1- Allow Central Management | YES | NO | NO | NO | NO |
| globalbwforupload | String | Specifies the bandwidth limit when uploading files from the client to the server in terms of KB only. | YES | NO | NO | NO | NO |
| globalbwfordownload | 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 | Sync | Windows Drive | Mac Drive | Office Add-On | Outlook 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.<br>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.<br>This value can be any number such as: {-1, 0, 1, 2, 3, 4, 5, 6} where:<br>• -1 means every day<br>• 0 means Sunday<br>• 1 means Monday<br>• 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<br>1 = enabled<br>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<br>Any number {-1, 0, 1, 2, 3, 4, 5, 6} where:<br>• -1 = Every day<br>• 0 = Sunday<br>• 1 = Monday<br>• 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<br>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

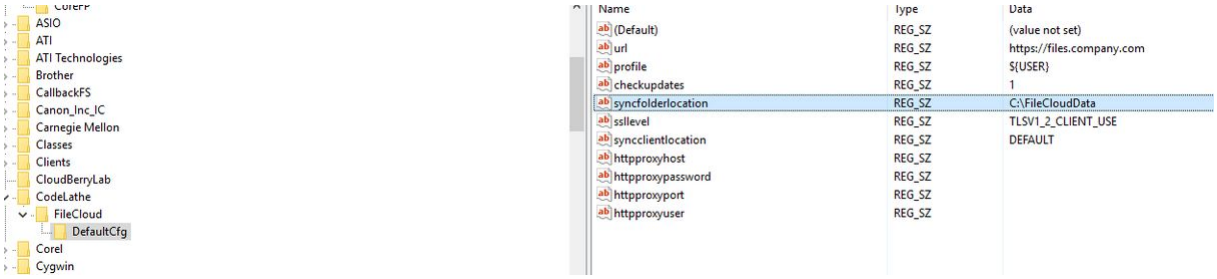
**In Windows, where is the default configuration located?**

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

An example configuration is shown below.

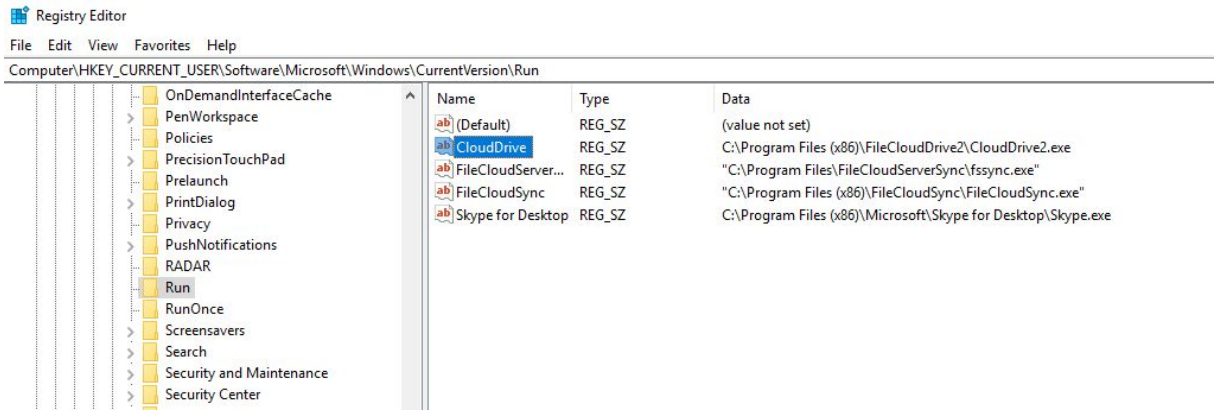
**Note:** The registry key (***HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg***) must be created manually, including the default values.

HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg




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

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run




**In Mac OSX, where is the default configuration located?**

The location of the default configuration is a plist file in

~/Library/Preferences/com.codelathe.filecloud.defaultcfg.plist

Example plist

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

```
  <string>1</string>
  <key>driveloginmode</key>
  <string>1</string>
  <key>checkupdates</key>
  <string>0</string>
</dict>
</plist>
```

# Search in the Admin Portal

## FileCloud's Federated Search

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

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

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

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

**Note:** For full content search or PII search, configure content search for documents.

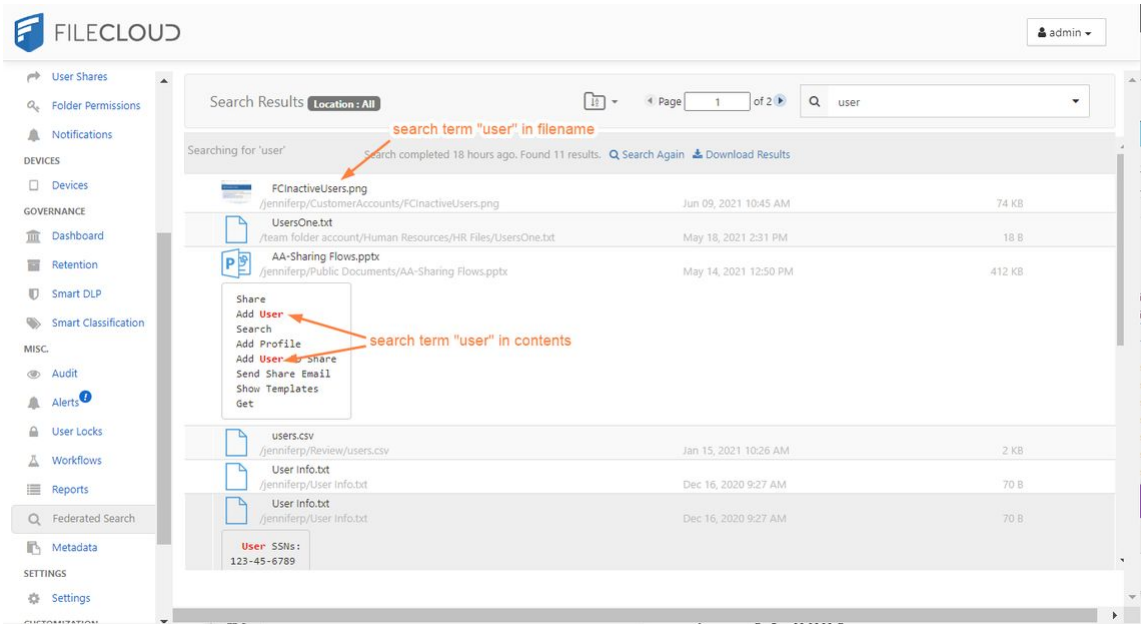
**Basic Search**

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

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

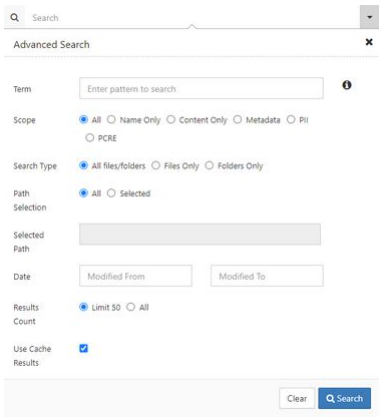
**To perform a basic search on the entire site:**

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




**Advanced Searches**

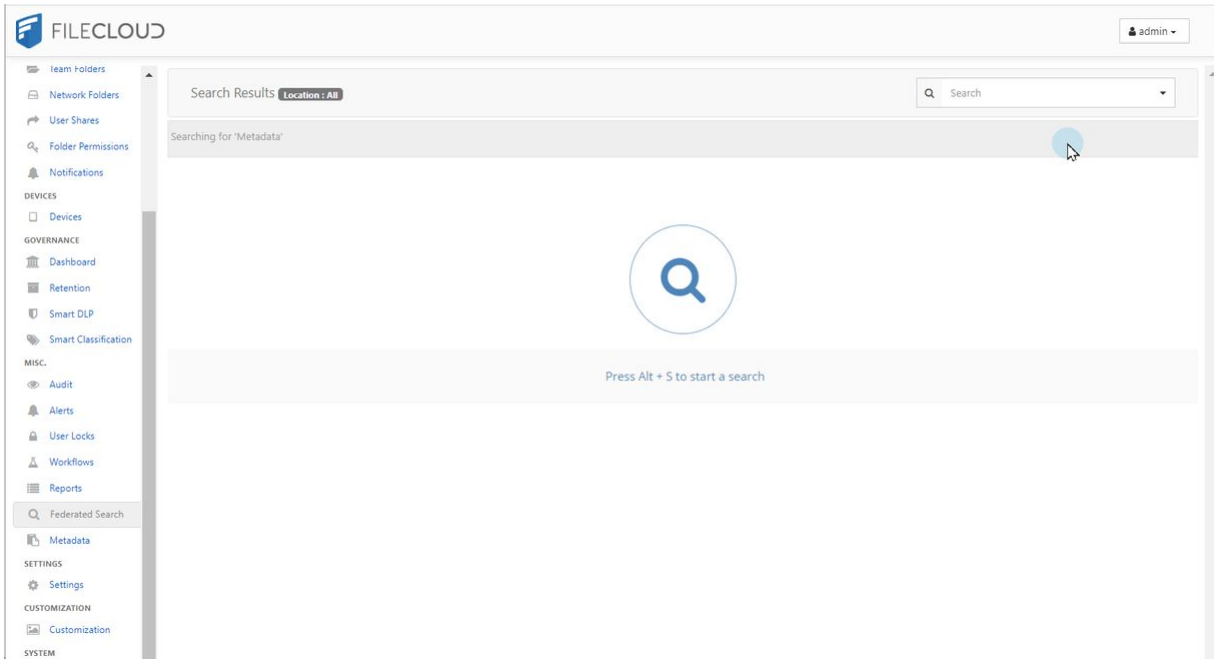
An advanced search lets you search on the search term and any of the options shown and listed below:

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

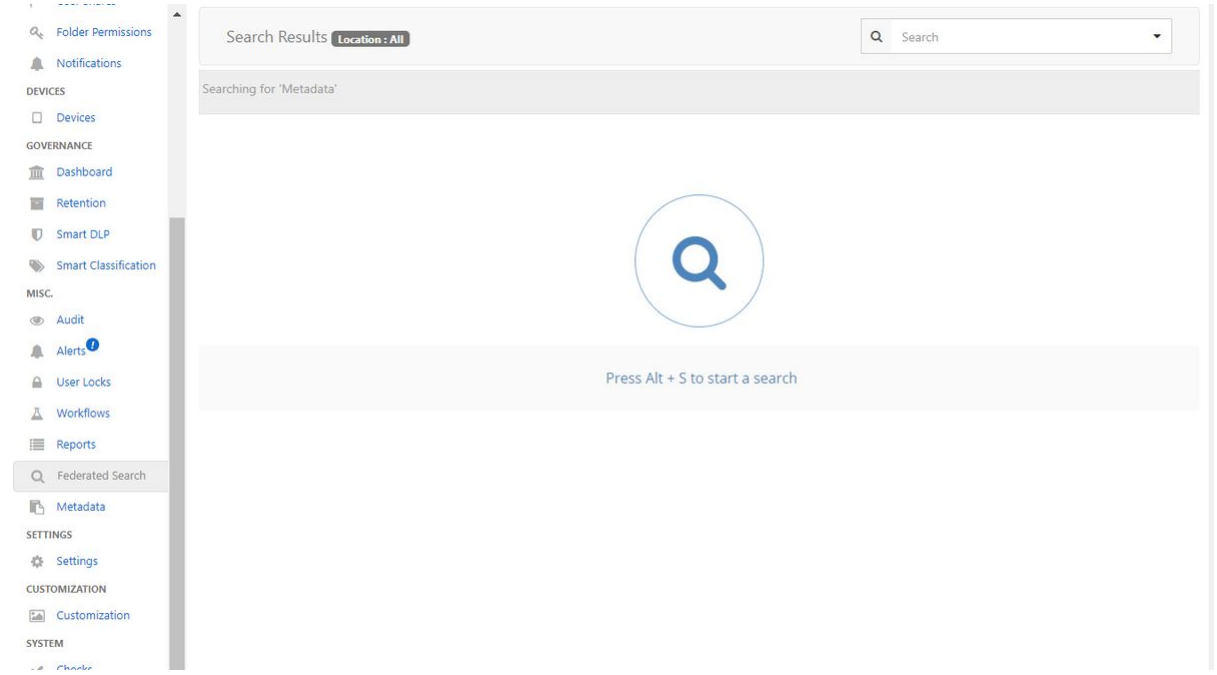
**All** is selected by default. This search looks for matches in file and folder names when content search is not enabled. It looks for matches in file and folder names and in the content of files when content search is enabled.




**Name only search**

## Name Only search

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



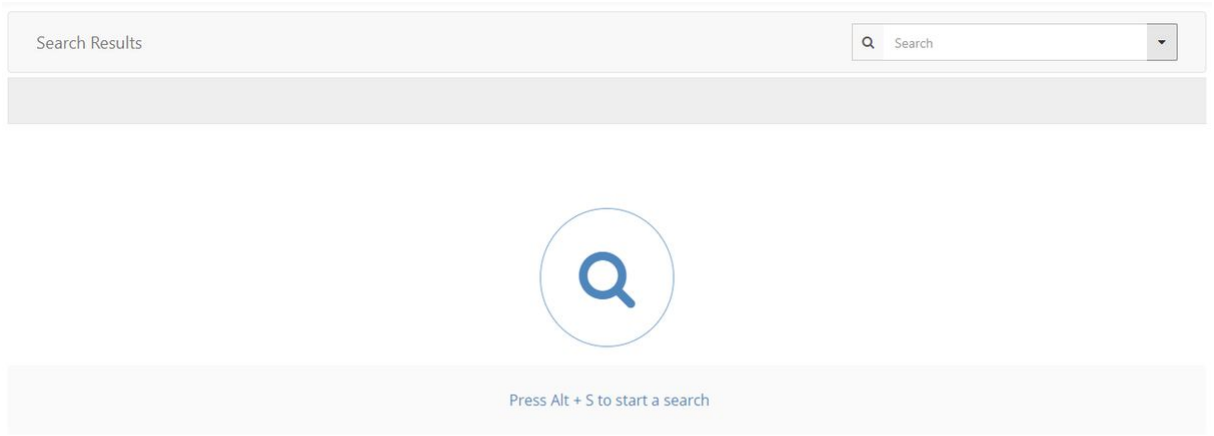

**Content only search**

## 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.

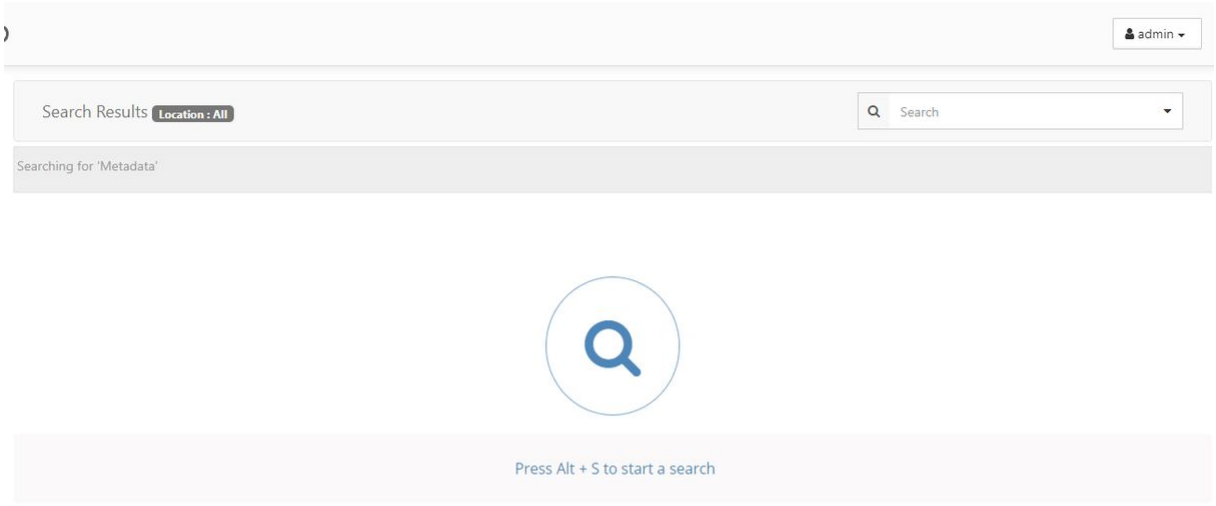



**Metadata search**

## Metadata search

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

with the image orientation field set to horizontal.




---

**PII and PCRE Searches**

## PII and PCRE searches

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

- **PII search** - The PII search is faster and more efficient than the PCRE search, and it displays the content it matches; however, it cannot match text that includes spaces or special characters. Therefore, you must use a PCRE search to find defined PII patterns that include spaces or special characters (such as US social security numbers with dashes).

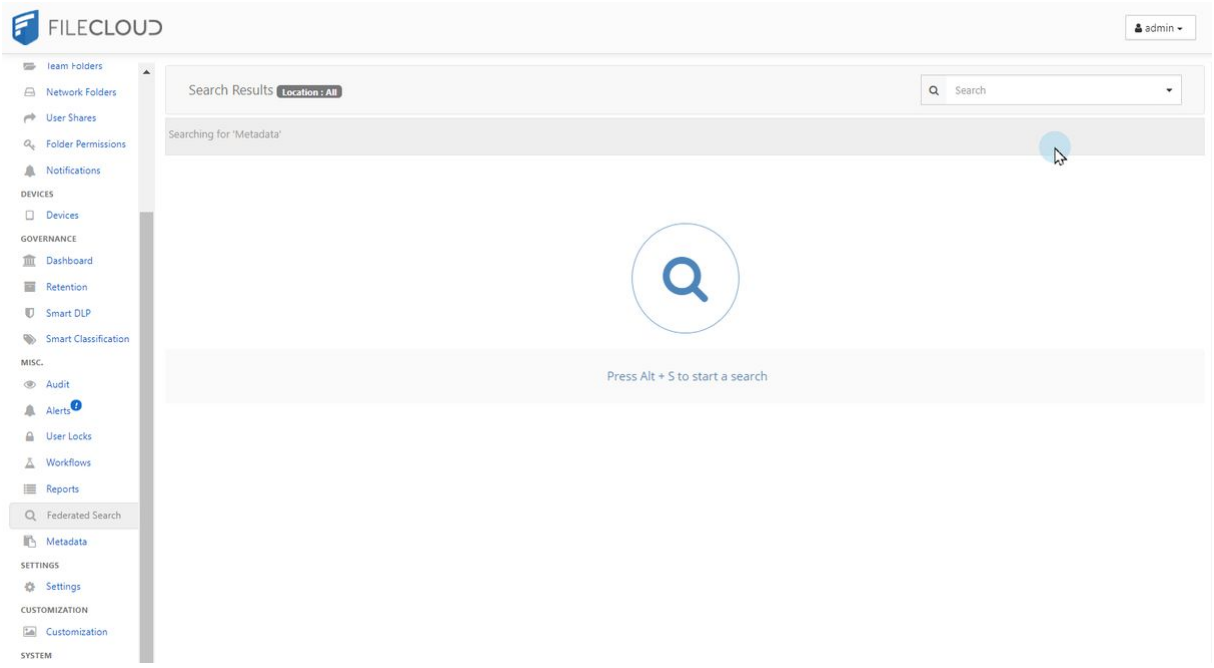
- **PCRE search** - The PCRE search is much more powerful than the PII search and can match patterns with spaces and special characters. However it is slower and less efficient, and it displays the file names of matches but it does not display the matched text. When you perform a PCRE search you must enter the entire pattern into the search field; you cannot choose it from a list of predefined patterns.

### PII search

The PII search searches for patterns that are set up in the **Manage PII Search** box in your **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:

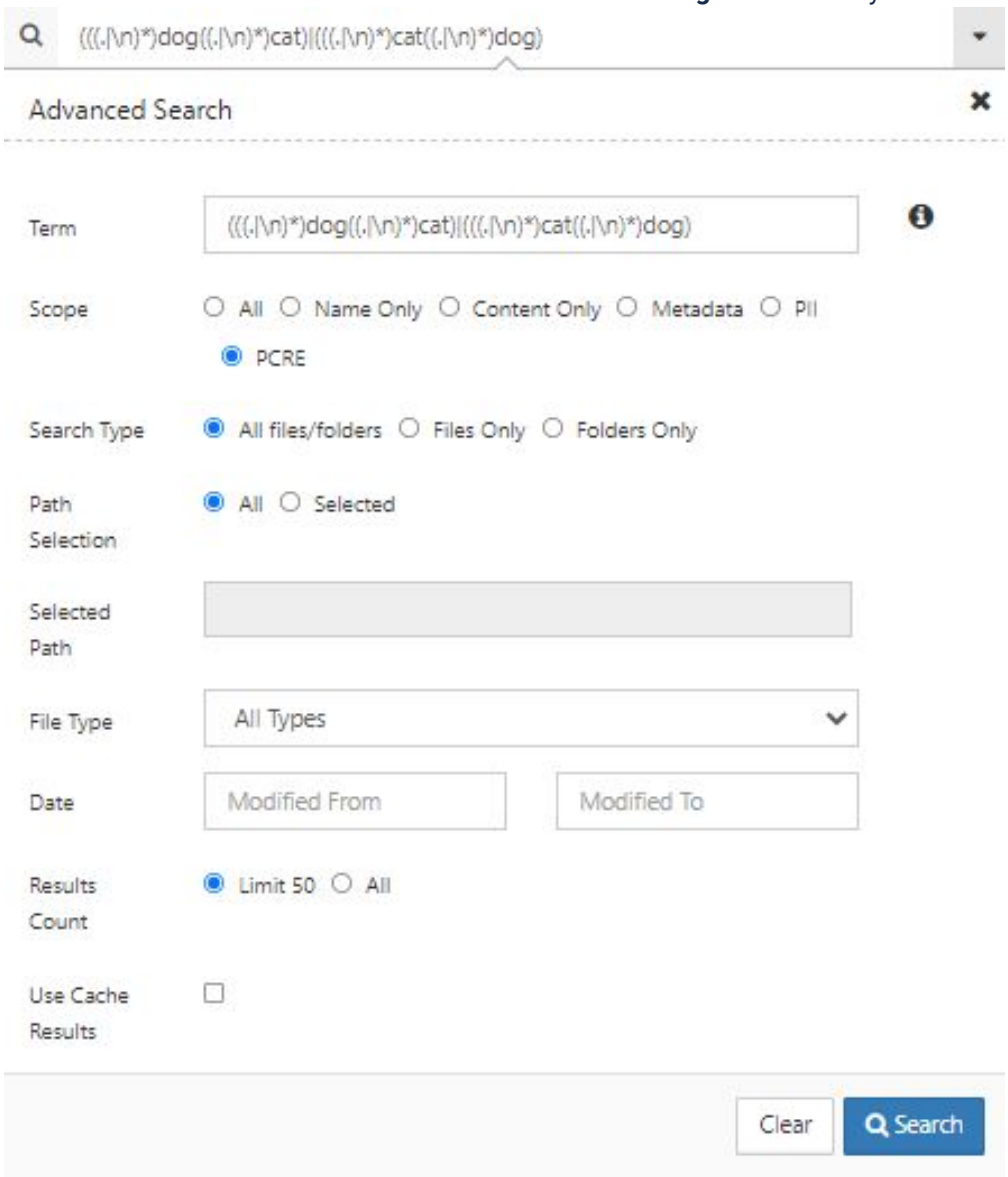
```
define("TONIDOCLOUD_PII_PATTERN_SEARCH_PCRE_MODE_ENABLED",1)
```

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

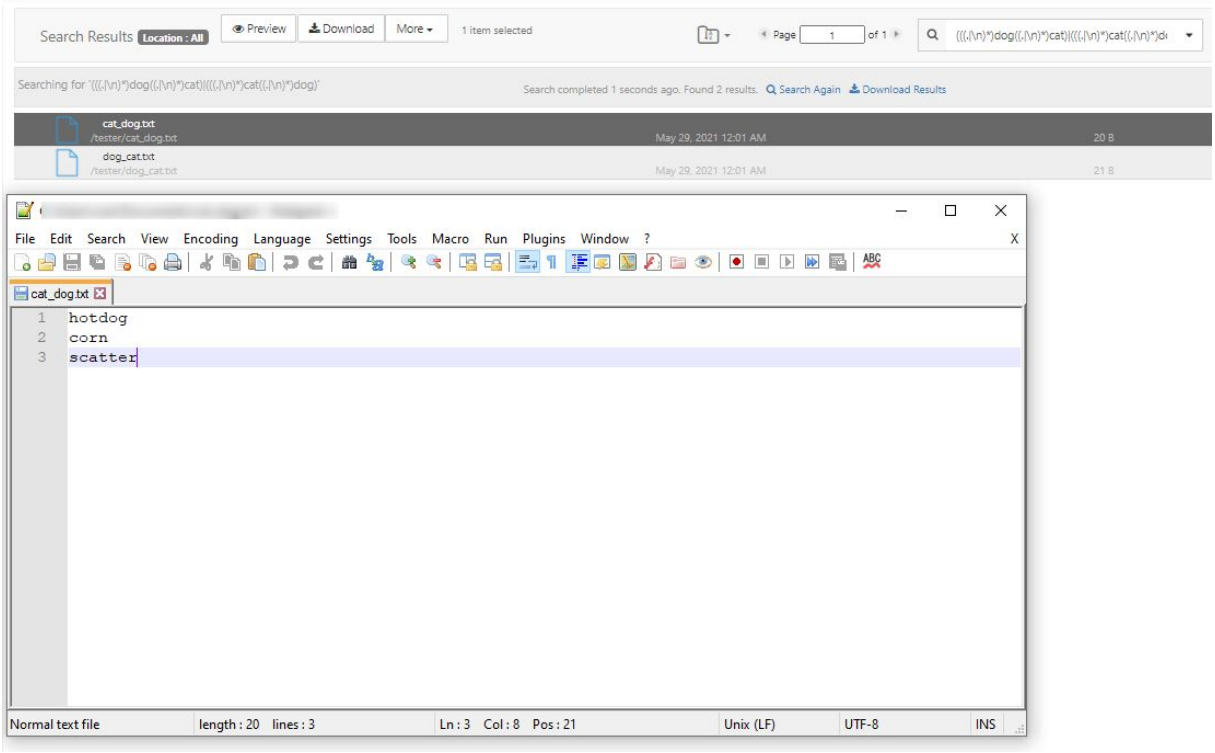
After PCRE search is enabled, newly uploaded files are automatically searchable by PCRE.

**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.

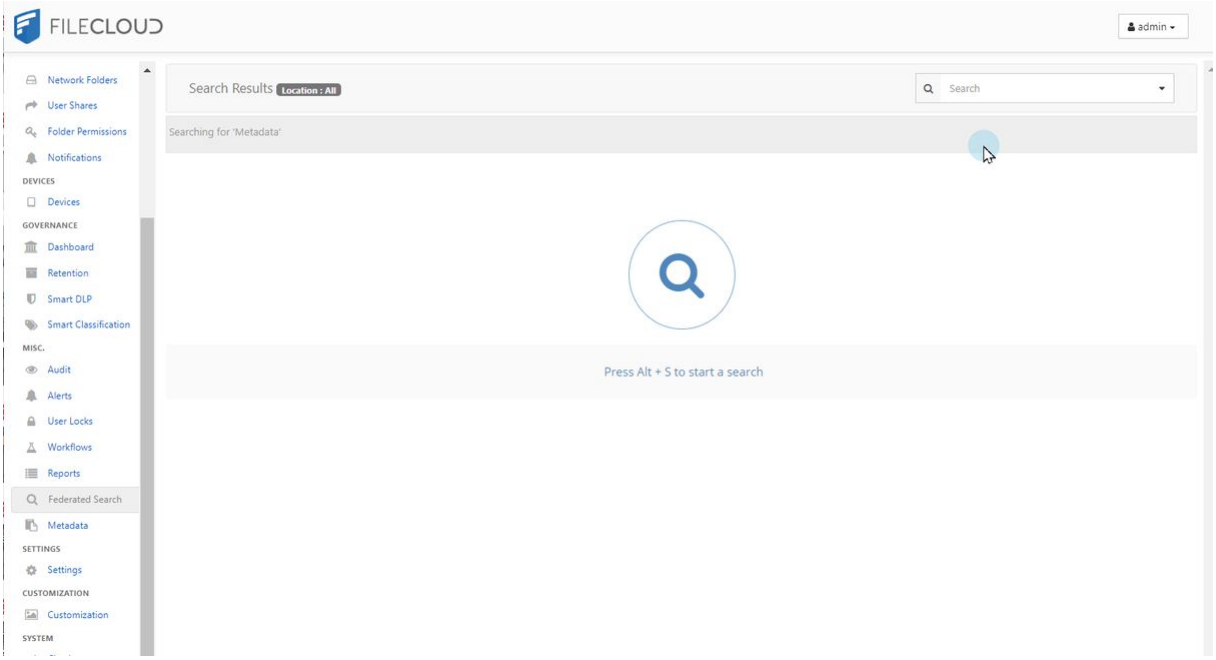



The following files are returned. The first is opened to show the matching content.




**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?

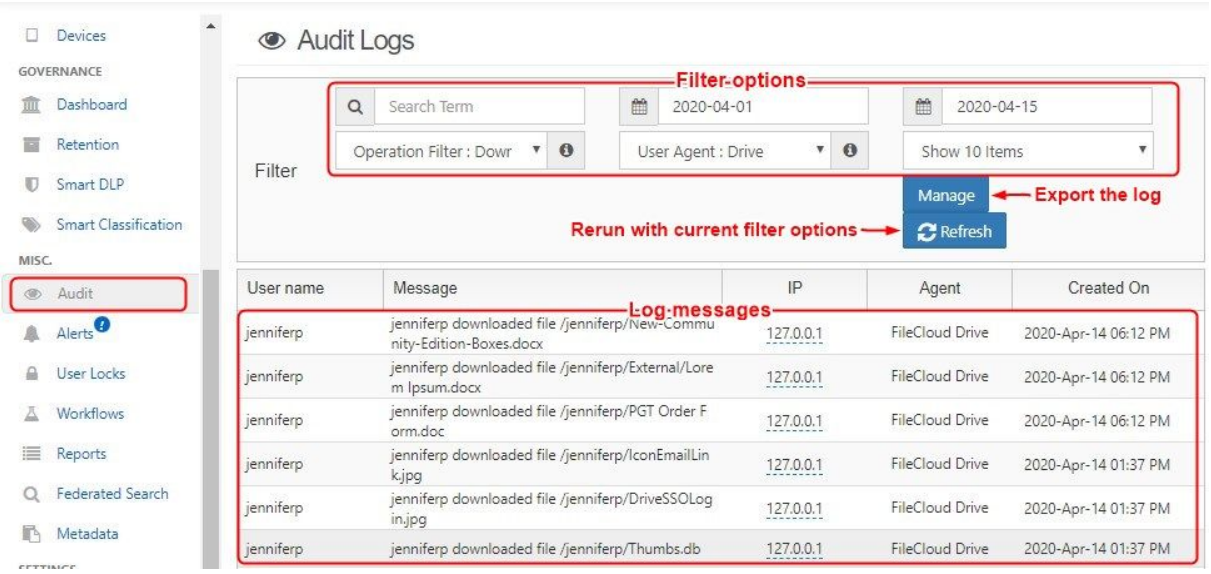
| | |
|---|---|
| View Logs | View Audit Logs (see page 208)<br>Filter Audit Log Views (see page 210) |
| Manage Logs | Delete Audit Log Entries (see page 216)<br>Configure What is Logged (see page 213)<br>Export Audit Logs (see page 215)<br>Compact the Audit Database (see page 213) |

## 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 Log screen are fields that enable you to filter log results. Below them, a **Manage** button opens a dialog box for exporting the log to a csv file and downloading it. A **Refresh** button regenerates the log with the current filter settings.

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

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

# Filter Audit Log Views

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

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

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

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

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

Filtering your view of log entries does not trim or decrease the size of your log database.
If your log database is growing too large, you can:
Export Audit Logs (see page 215)
Configure What is Logged (see page 213)
Delete Audit Log Entries (see page 216)Compact the Audit Database (see page 213)

## How do you want to filter the Audit log?

### 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 start and end dates

**To filter the audit log by date**:

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

2. From the left navigation panel, click Audit.
3. In the Filter Start Date box, select a date or type in a date in the following format: YYYY-MM-DD.
4. In the Filter End Date box, select a date or type in a date in the following format: YYYY-MM-DD.

**By an operation**

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

| Operation | Description |
|---|---|
| All | Displays all operations logged by FileCloud Server<br>This is the default filter. |
| Common | Displays 6 of the most commonly logged operations:<br>• create new account<br>• login<br>• create file or folder<br>• upload file<br>• download file or folder<br>• 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. |

| Operation | Description |
|---|---|
| No virus found | Displays logs created when antivirus scanned an upload and found no virus. |
| SSO | Displays logs related to SSO activities. |

**To filter the audit log by operation**:

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

**By an agent**

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

You can select from the following user agents:

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

**To filter the audit log by agent**:

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

## 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**:

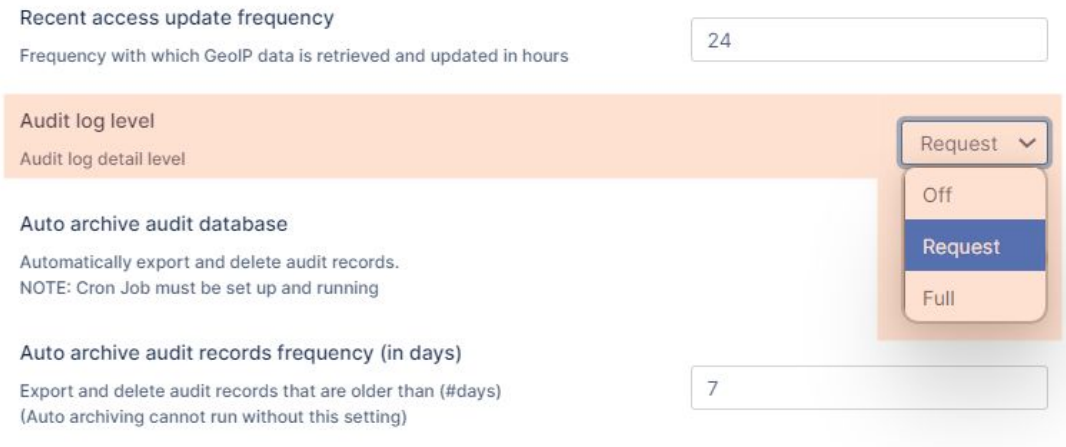
**Set a logging level**

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**.




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

⚠ 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|loginguest|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.

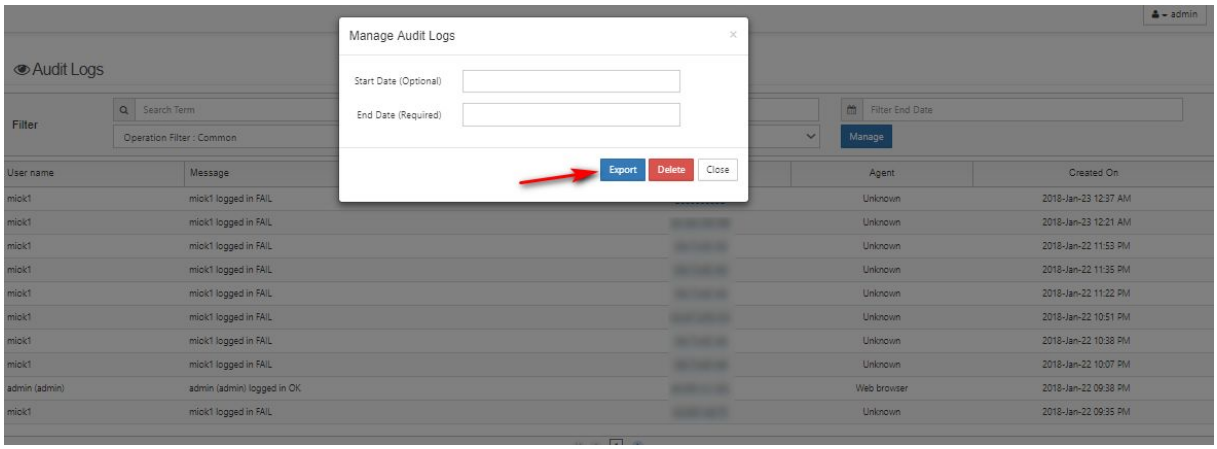
## Export Audit Logs

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 (see page 277) for information about specific reports

If you need to reclaim the space, you should compact the database (see page 213).

## How do you want to remove Audit log entries?

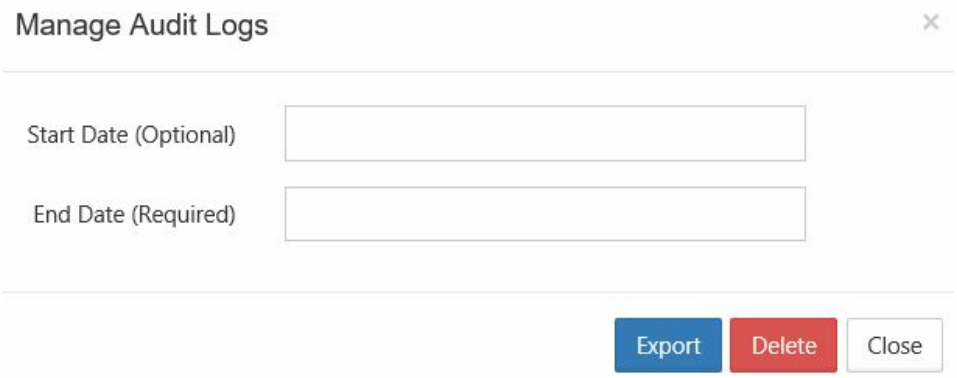
Manually Trim the Audit Database (see page 219)

**Manually delete entries**

To manually remove audit log entries:

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

2. On the **Audit Logs** window, click **Manage**.




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

**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.

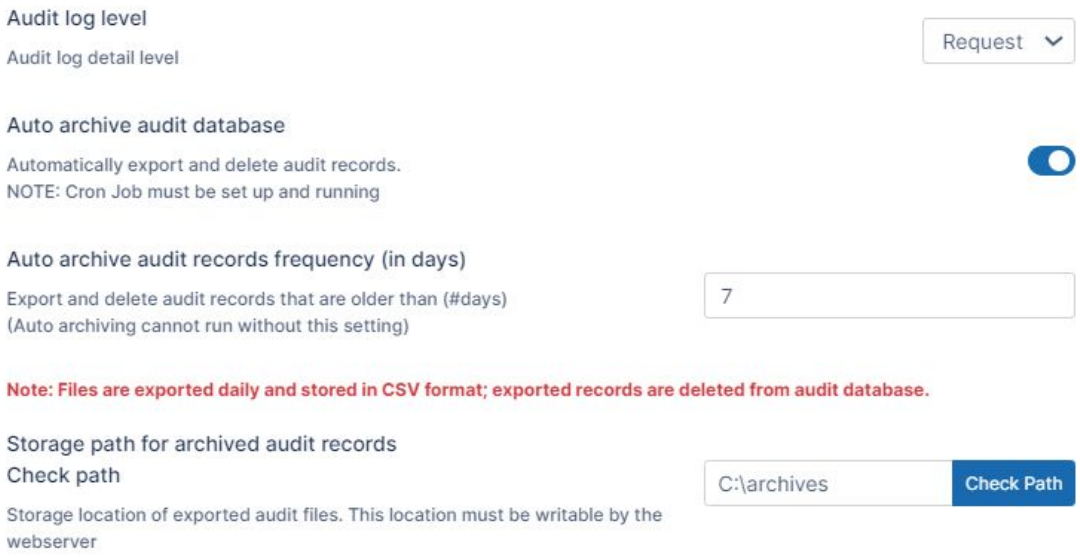
When you are deciding whether or not to automatically archive and remove audit records (or how often to archive and remove them), please note that some reports use the audit log (see page 277) and can only show events if they are still contained in the audit log.

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.




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 |

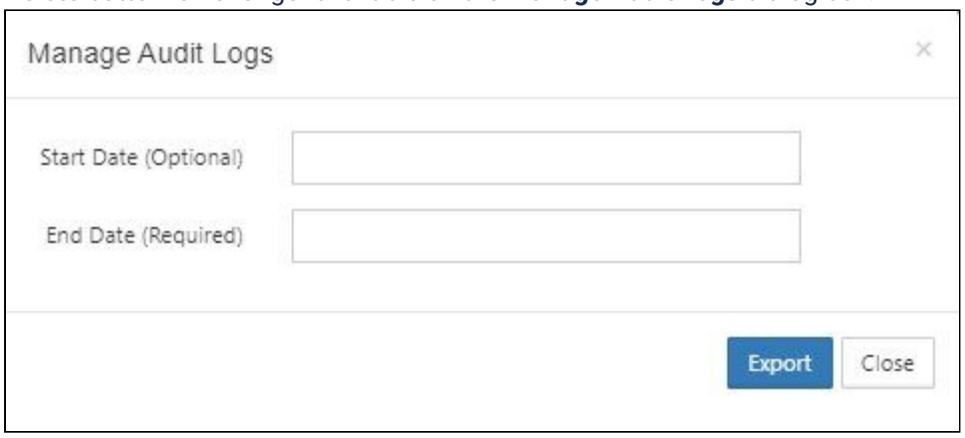
If you want to automatically remove records but not archive them, you can configure FileCloud to remove audit records but not export them to a csv file.
To auto remove records without exporting them:

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<br>**Always replace the sample values in the examples with the values used in your deployment.** |
|---|---|---|
| --port `<port>` | Specifies the port where the mongod[9] or mongos[10] instance is listening.<br>If --port[11] is not specified, **mongo** attempts to connect to port `27017`. | --port 27017 |

| Option | Description | Example<br>💡 **Always replace the sample values in the examples with the values used in your deployment.** |
|---|---|---|
| --username `<username>`, `-u <username>` | Specifies a username with which to authenticate to a MongoDB database that uses authentication.<br>Use in conjunction with the `--password` and `--authenticationDatabase` options. | -u "myUserAdmin" |
| --password `<password>`, `-p <password>` | Specifies a password with which to authenticate to a MongoDB database that uses authentication.<br>Use in conjunction with the --username[12]and --authenticationDatabase[13]options.<br>To force **mongo** to prompt for a password, enter the --password[14]option as the last option and leave out the argument. | -p "abc123" |
| --authenticationDatabase `<dbname>` | Specifies the database in which the user is created. See Authentication Database[15].<br>If you do not specify a value for --authenticationDatabase[16], **mongo** uses the database specified in the connection string. | --authenticationDatabase "admin" |

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

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

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

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

9. https://docs.mongodb.com/manual/reference/program/mongod/#bin.mongod
10. https://docs.mongodb.com/manual/reference/program/mongos/#bin.mongos
11. https://docs.mongodb.com/manual/reference/program/mongo/#cmdoption-mongo-port
12. https://docs.mongodb.com/manual/reference/program/mongo/#cmdoption-mongo-username
13. https://docs.mongodb.com/manual/reference/program/mongo/#cmdoption-mongo-authenticationdatabase
14. https://docs.mongodb.com/manual/reference/program/mongo/#cmdoption-mongo-password
15. https://docs.mongodb.com/manual/core/security-users/#user-authentication-database
16. https://docs.mongodb.com/manual/reference/program/mongo/#cmdoption-mongo-authenticationdatabase

Table 1. MongoExport Options

| Option | Description | Example |
|---|---|---|
| --db `<database>`, `-d <database>` | Specifies the name of the database on which to run the **mongoexport**. | `--db tonidoauditdb` |
| --collection `<collection>`, `-c <collection>` | Specifies the collection to export. | `--collection audit` |
| --type `<string>` | *Default*: json<br>New in version 3.0.<br>Specifies the file type to export. Specify `csv` for CSV[17]format or `json` for JSON[18]format.<br>If you specify `csv`, then you must also use either the --fields[19]or the --fieldFile[20]option to declare the fields to export from the collection. | `--type=csv` |
| --fields `<field1[,field2]>`, `-f <field1[,field2]>` | Specifies a field or fields to *include* in the export. Use a comma separated list of fields to specify multiple fields.<br>If any of your field names include white space, use quotation marks to enclose the field list.<br>For example, to export two fields, `phone` and `user number`, you would specify `--fields "phone,user number"`.<br>For csv[21]output formats, mongoexport[22]includes only the specified field(s), and the specified field(s) can be a field within a sub-document. | `--fields createdon,username,how,ip,useragent,operation,request,deviceinfo` |
| --out `<file>`, `-o <file>` | The output directory where you need to export data as a csv.<br>You must change this location to match the directory in your deployment. | `--out c:\xampp\test.csv` |

17. https://docs.mongodb.com/manual/reference/glossary/#term-csv
18. https://docs.mongodb.com/manual/reference/glossary/#term-json
19. https://docs.mongodb.com/manual/reference/program/mongoexport/index.html#cmdoption-mongoexport-fields
20. https://docs.mongodb.com/manual/reference/program/mongoexport/index.html#cmdoption-mongoexport-fieldfile
21. https://docs.mongodb.com/manual/reference/program/mongoexport/index.html#cmdoption-mongoexport-type
22. https://docs.mongodb.com/manual/reference/program/mongoexport/index.html#bin.mongoexport

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[23].

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[24]from the database.

The drop method also removes any indexes associated with the dropped collection.

- The method provides a wrapper around the drop[25]command.
- This method obtains a write lock on the affected database and will block other operations until it has completed.

23. https://docs.mongodb.com/manual/reference/program/mongoexport/index.html
24. https://docs.mongodb.com/manual/core/views/
25. https://docs.mongodb.com/manual/reference/command/drop/#dbcmd.drop

- The db.collection.drop()[26]method and drop[27]command create an invalidate Event[28]for any Change Streams[29]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:

26. https://docs.mongodb.com/manual/reference/method/db.collection.drop/#db.collection.drop
27. https://docs.mongodb.com/manual/reference/command/drop/#dbcmd.drop
28. https://docs.mongodb.com/manual/reference/change-events/#change-event-invalidate
29. https://docs.mongodb.com/manual/changeStreams/

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

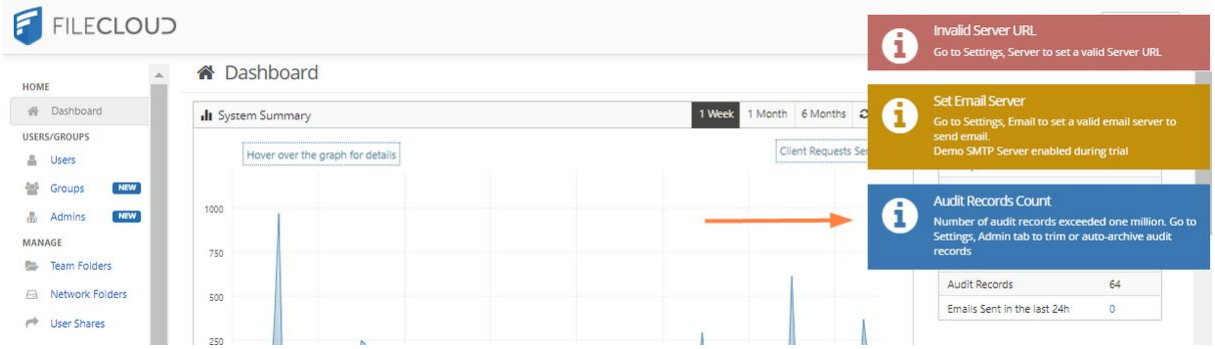
8. To list all the databases available for use on the connected MongoDB instance, run the following command:

```
show collections
```

You should see responses similar to the following example:

# 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 (see page 227) for Linux or Windows

Back up and Restore Linux Deployments (see page 255)

Manually Back up and Restore Windows Deployments (see page 259)

Migrate or transfer Files to a FileCloud Site (see page 265)

## 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 (see page 227)
- FileCloud Backup Server Installation (see page 227)
- FileCloud Backup Server Configuration (see page 230)
- Backup Server Configuration Using RSync (see page 236)
- FileCloud Backup Server Operations (see page 242)
- FileCloud Backup Server Troubleshooting (see page 254)

## 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 (see page 265).

### 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

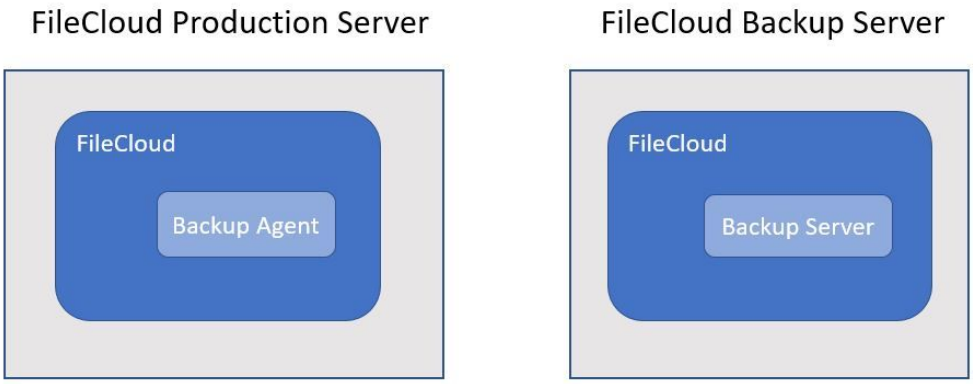
### Introduction

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[30]. 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

30. https://portal.getfilecloud.com/ui/user/index.html

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:

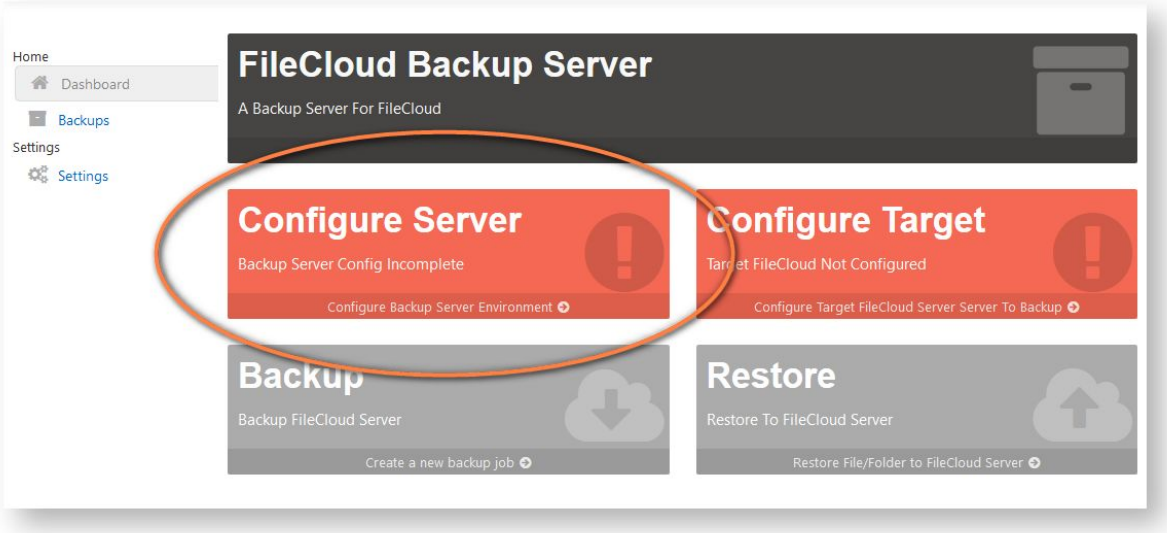
# FileCloud Backup Server Configuration

## Introduction

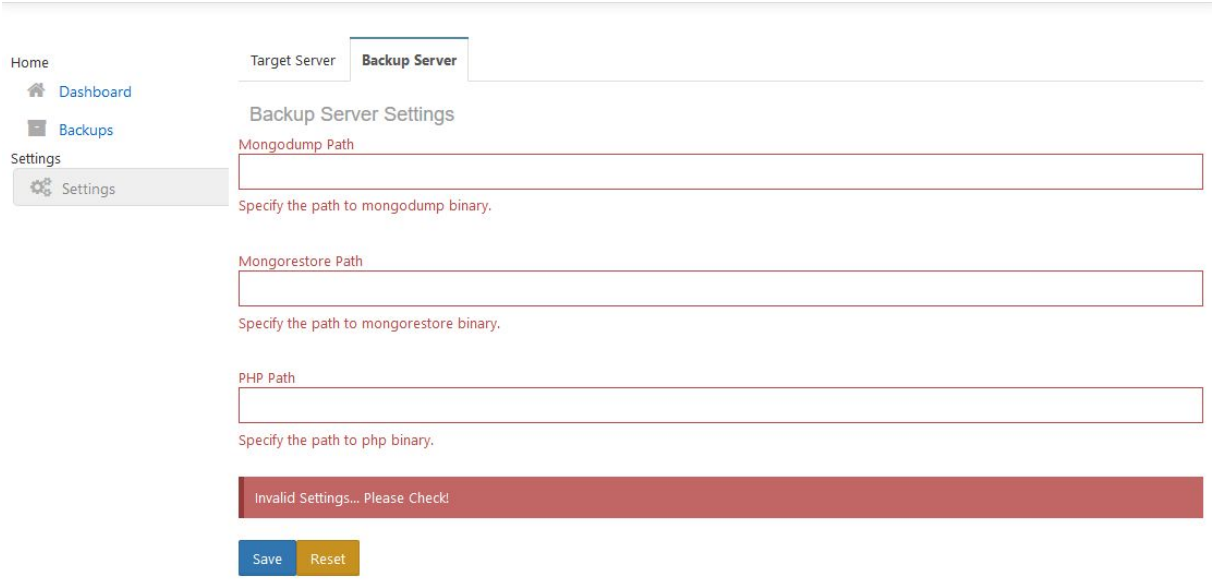
A new FileCloud installation needs to be configured before it can be used for backup purposes.

## 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.

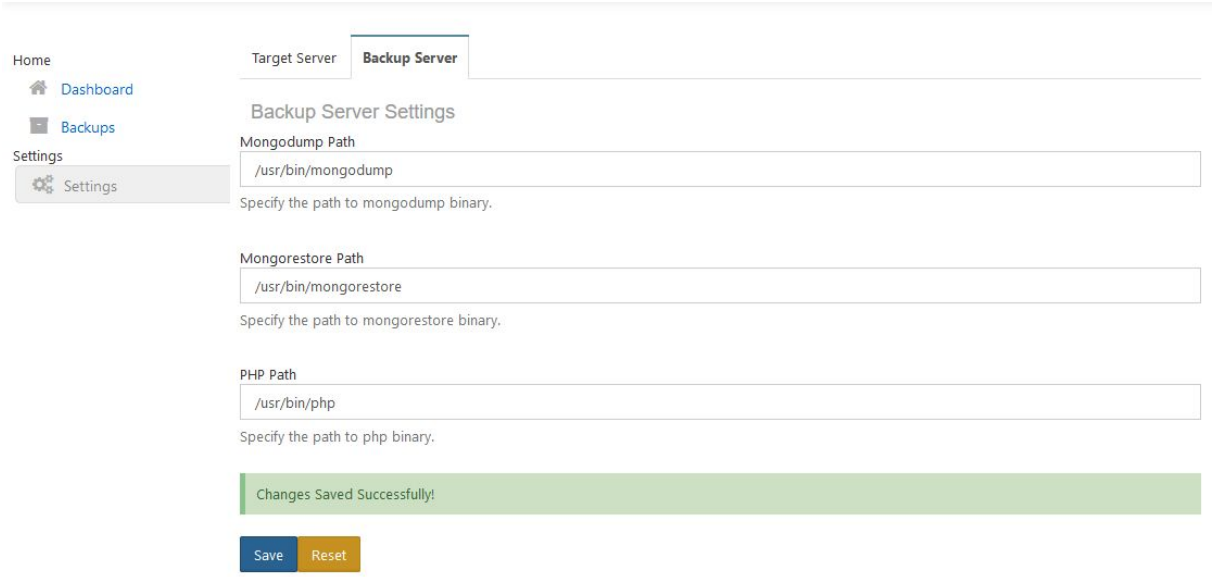



By default the backup server parameters will be empty and update them using the table below.




| Parameter Label | Value | Remarks |
|---|---|---|
| Mongodump Path | Linux: /usr/bin/mongodump<br>Win: C:\xampp\mongodb\bin\mongodump.exe | Path to the mongodump command. |
| Mongorestore Path | Linux: /usr/bin/mongorestore<br>Win: C:<br>\xampp\mongodb\bin\mongorestore.exe | Path to the mongorestore command. |
| PHP Path | Linux: /usr/bin/php<br>Win: C:\xampp\php\php.exe | Path to the php executable. |

A properly configured backup server settings should like this:




## 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 a access key. This access key serves as a security mechanism, allowing only backup requests made along with this key.

To enable this access key, follow these steps:

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

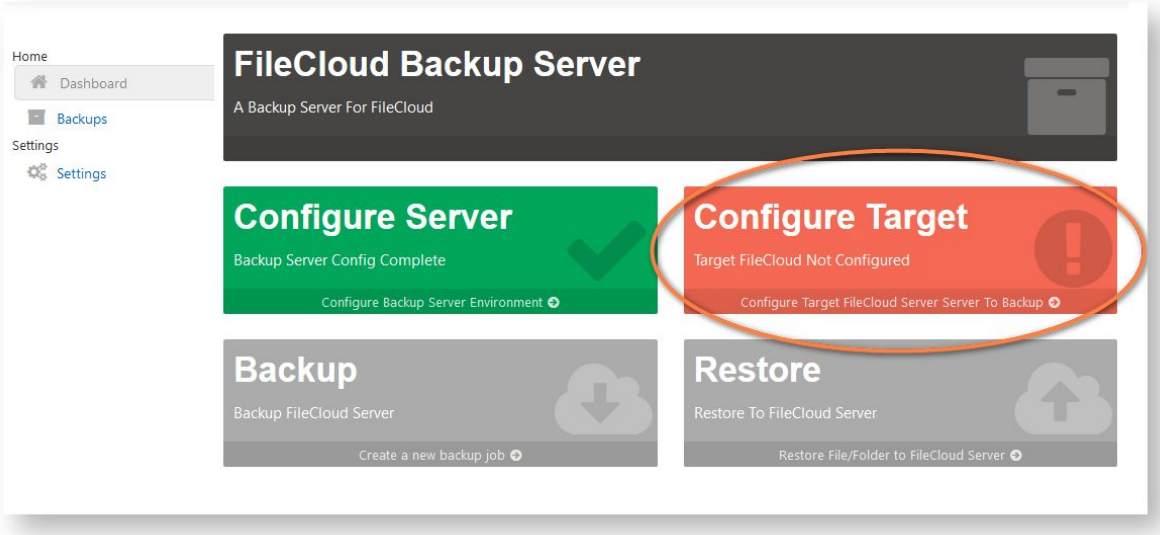
```
<?php
/* Configuration values for FileCloud */
// ... Server URL
define("BACKUPAGENT_ACCESS_KEY", "test908acc" );
?>
```

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

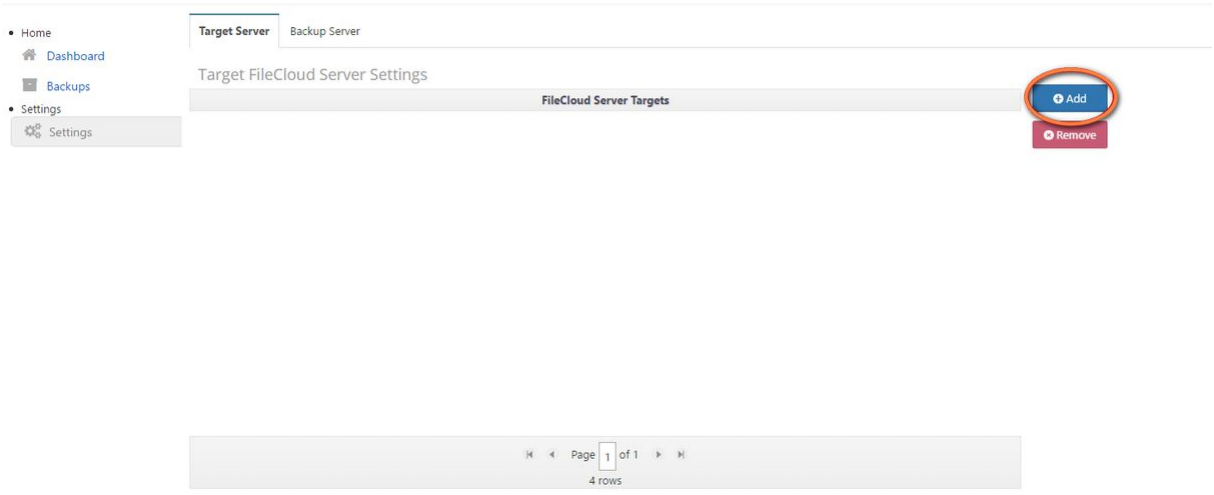
```
define("BACKUPAGENT_DBDATA_PATH", "D:\\xampp\\mongodb\\bin\\data" );
define("BACKUPSERVER_MONGODUMP_PATH", "D:\\xampp\\mongodb\\bin\
\mongodump.exe" );
```

## Step 3: Adding Target FileCloud Server

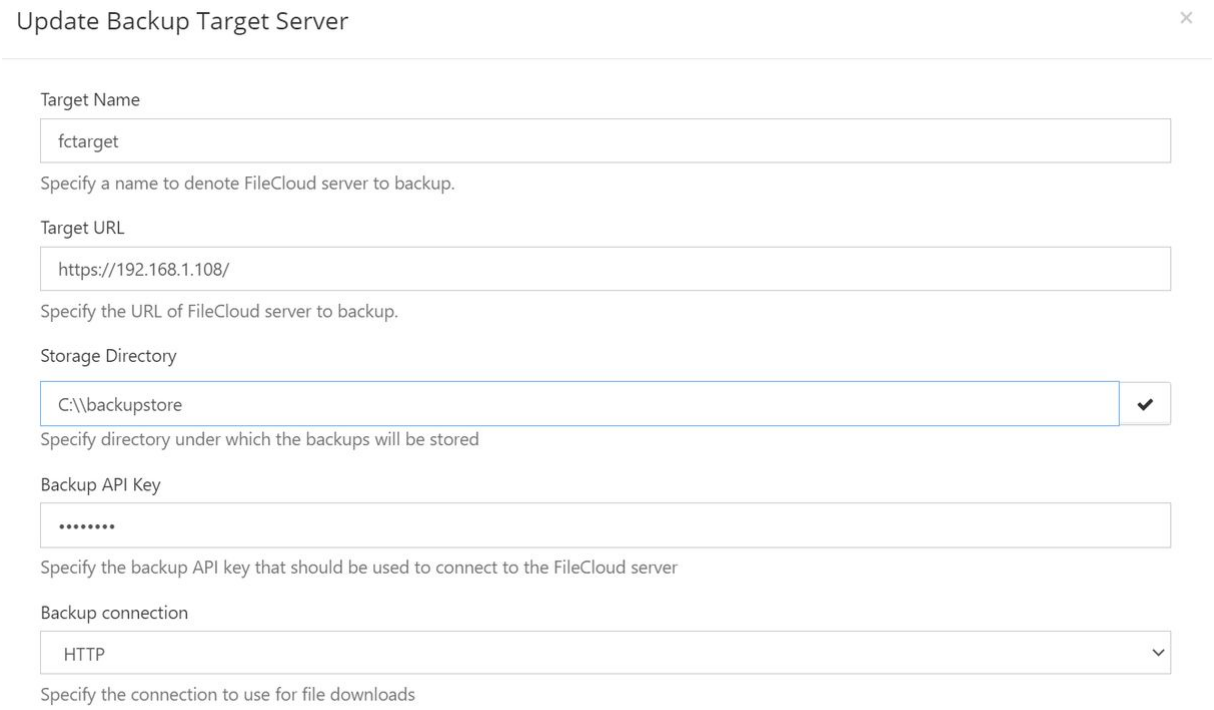
After setting the access key, the prepped FileCloud server can be added as a backup target. To add a new FileCloud server target, open the backup server UI and click on Settings -> "Target Server" tab. The backup server settings can also be opened by clicking on the "Configure Button" button on the dashboard.




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




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




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.

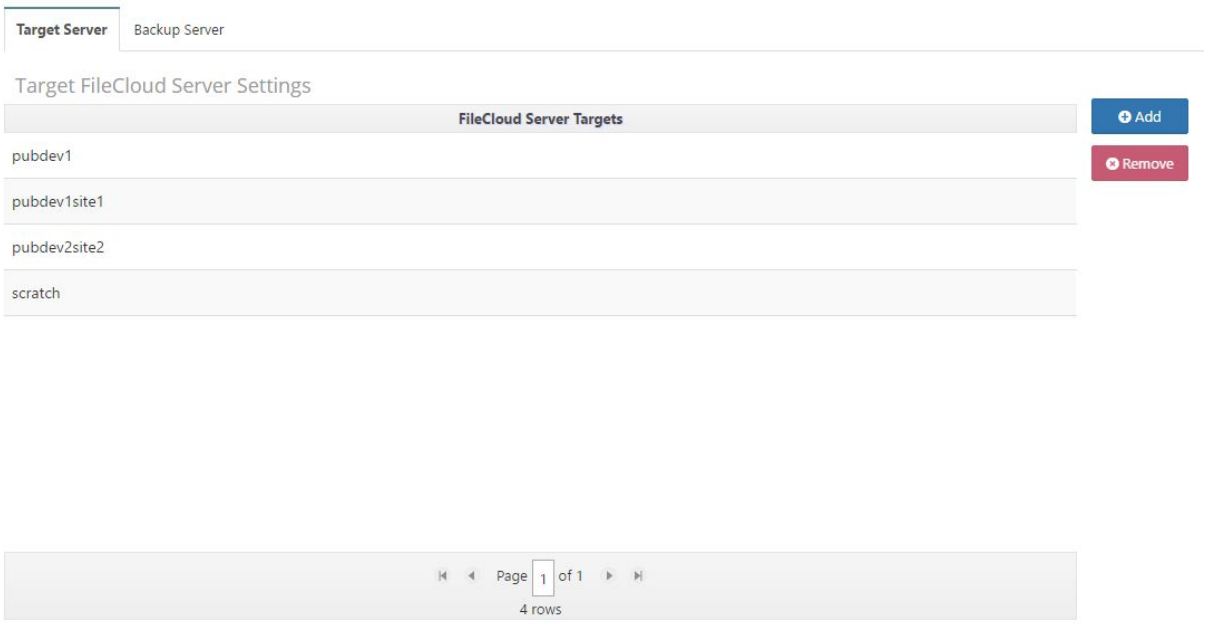
| Parameter Label | Sample Value | Remarks |
|---|---|---|
| Target Name | fctarget | A string to represent the target. |
| Target URL | http:// 192.168.1.108/ | Base URL to the target FileCloud server. |
| Storage Directory | Linux: / backupstore/ Win: C:\ \backupstore | A folder in the backup server where the backups from this target will be stored.<br>Admins can use the "Check Path" button to check if the folder is valid and writable for the backup server.<br><br>***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 (see page 236). |

Note:

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

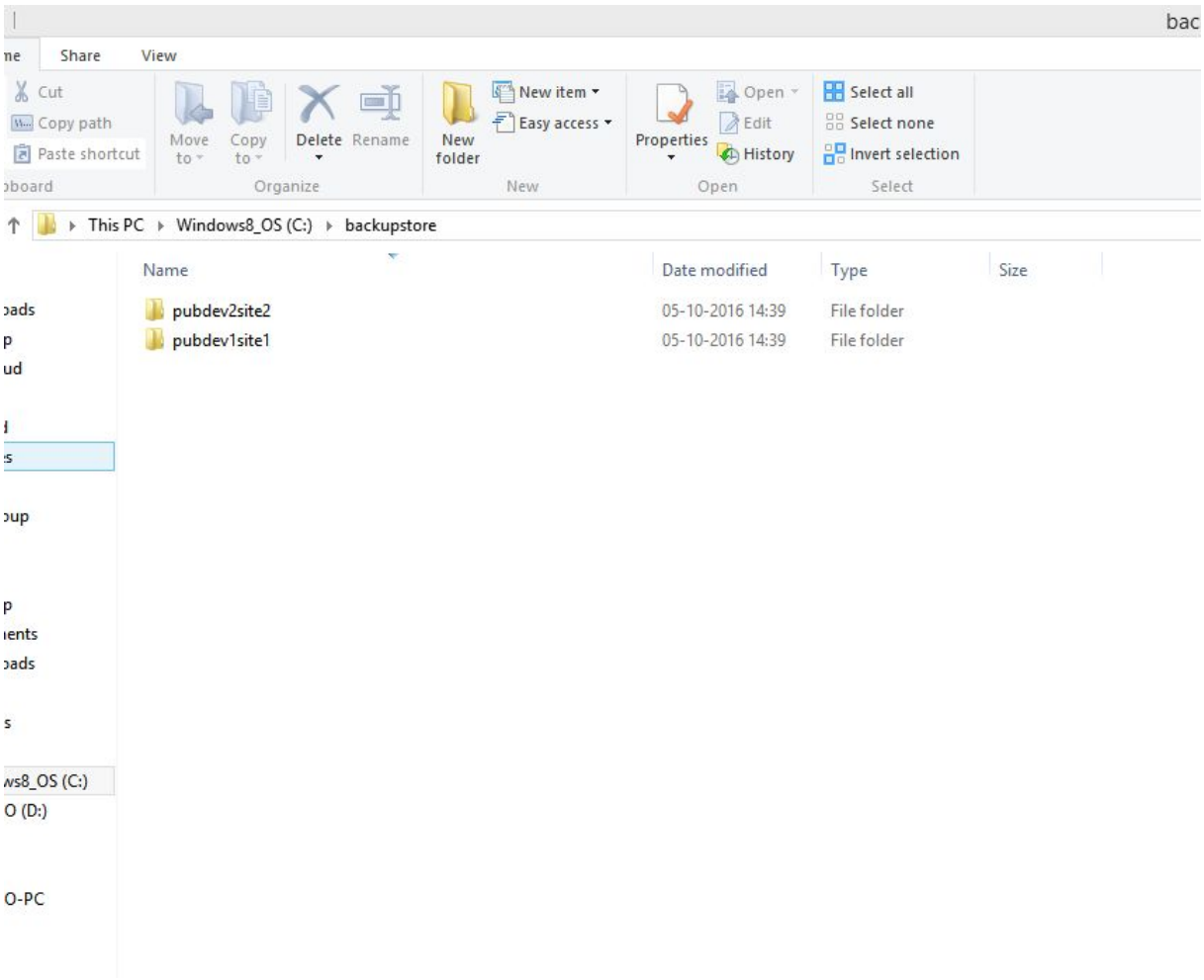
## Step 4: Adding Multiple Target FileCloud Servers

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




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

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




## Backup Server Configuration Using RSync

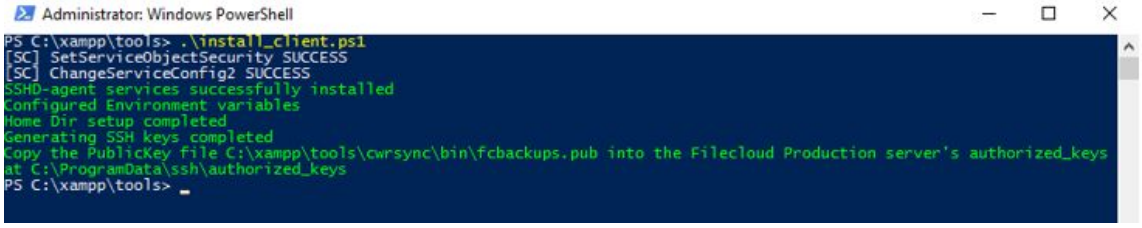
Please make sure the Filecloud Production server and the backup server are the same version.

### Configure the backup server using Rsync:

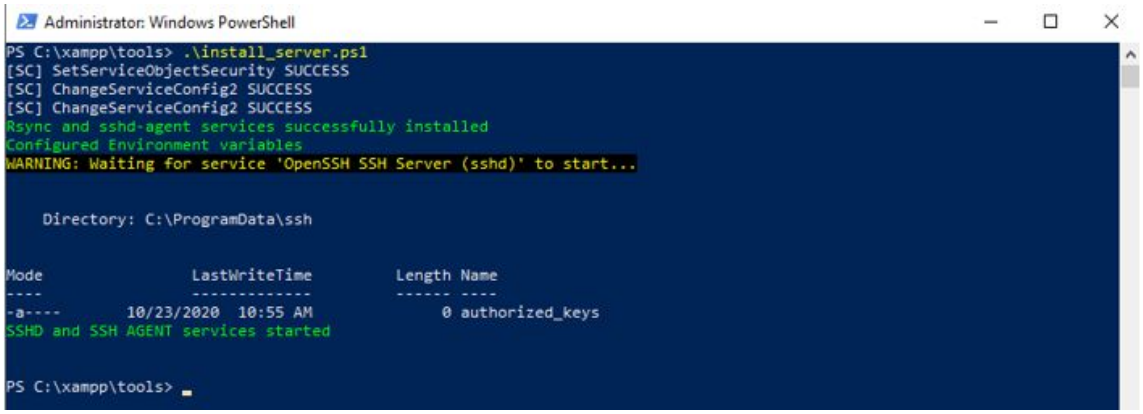
1. Download the Rsync tool from: https://patch.codelathe.com/tonidocloud/live/installer/backupserver-rsync-tool-win.zip
2. Unzip it and place it under **xampp\tools.**
3. To run the PowerShell scripts, first run the following command in PowerShell:
   **Set-ExecutionPolicy -Scope Process -ExecutionPolicy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

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:

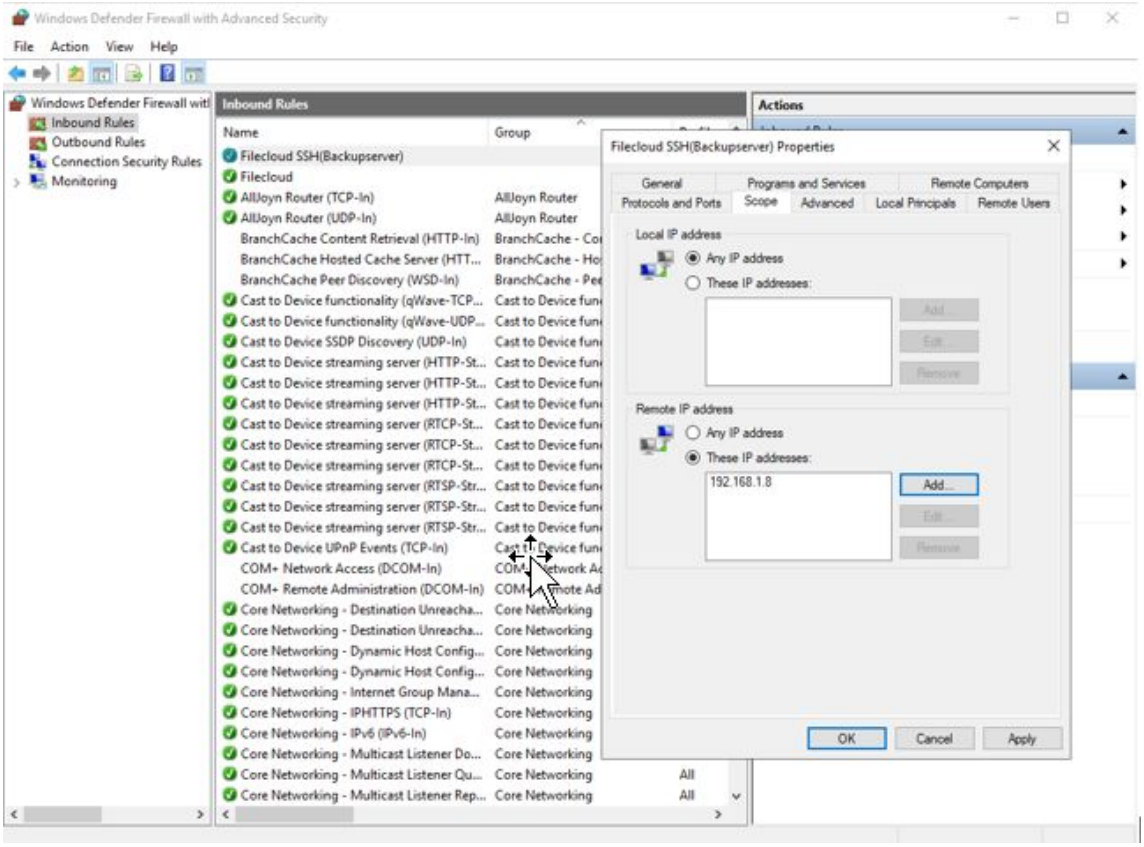
   **Backup server:**



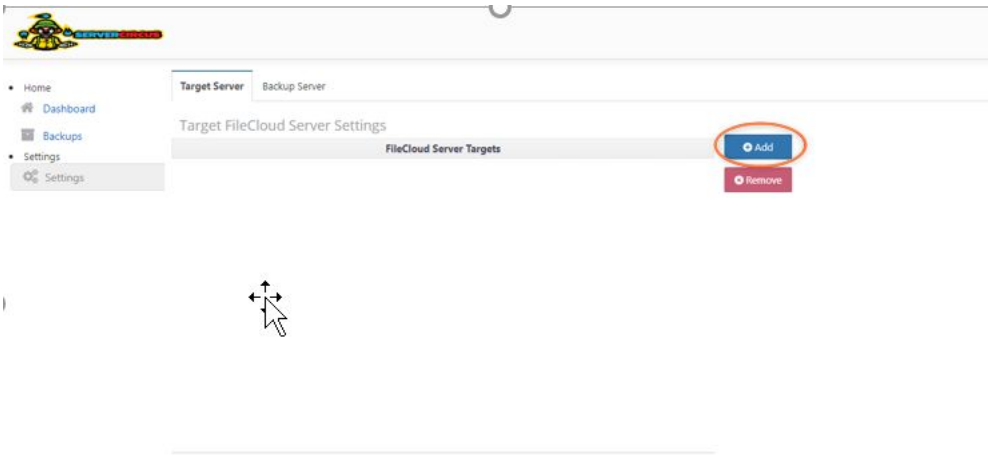

   **Production server:**



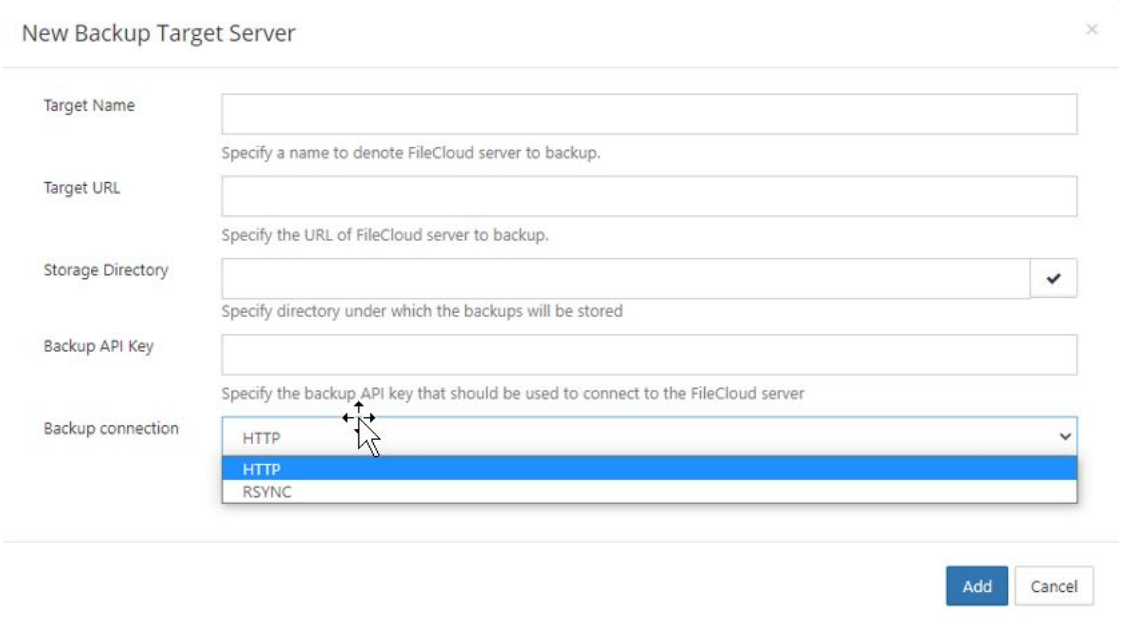

5. Open firewall access to the backup server on port 2233 (the default SSH port for the production server).




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 (see page 230) for help navigating to the **Settings > Target Server** tab in the Backup Server user interface.

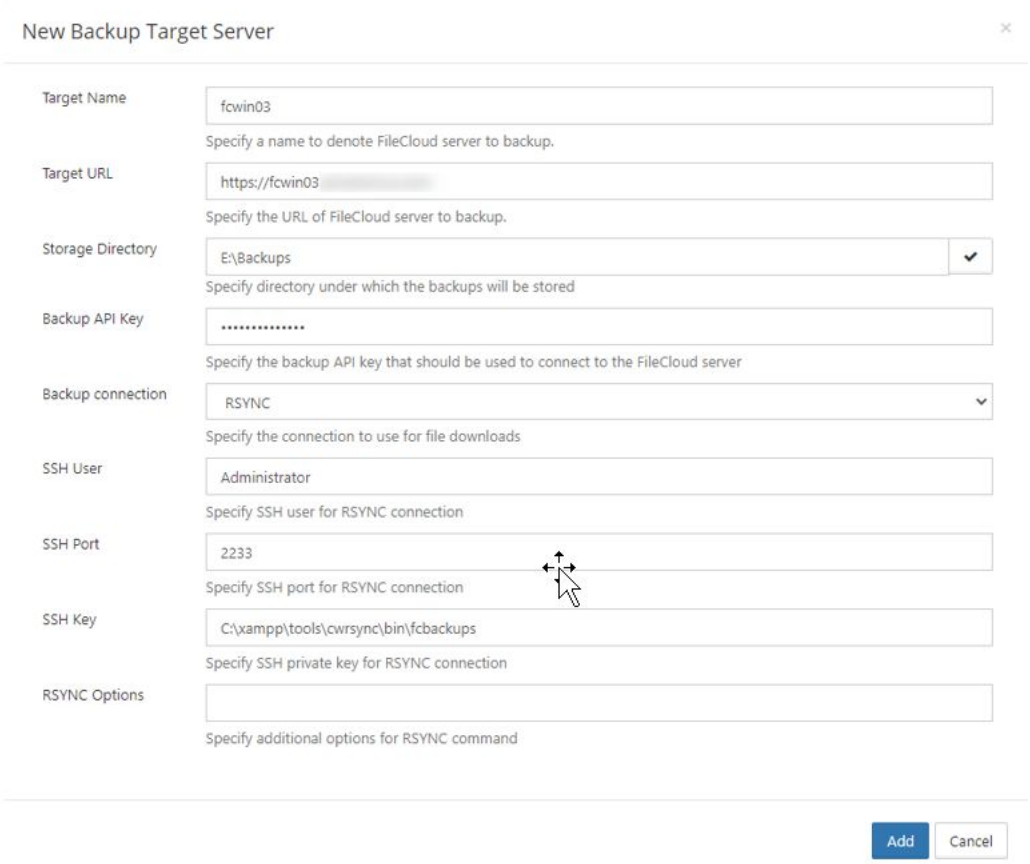



9. In the **New Backup Target Server** form, choose **RSYNC** as the backup connection:




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

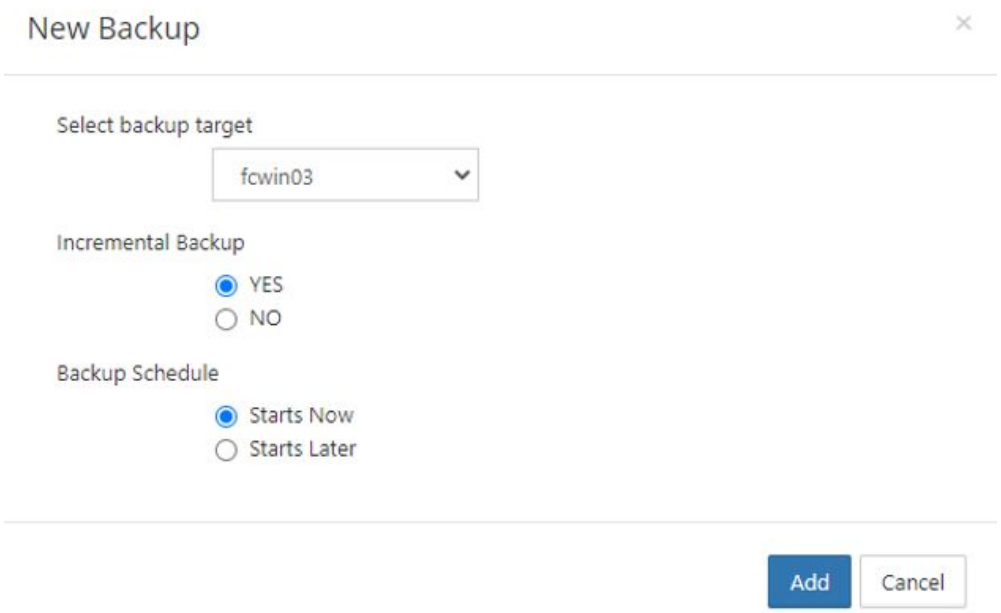
10. Enter the other settings.
If the Admin is an AD user, enter **DOMAIN\Administrator** for **SSH User**.



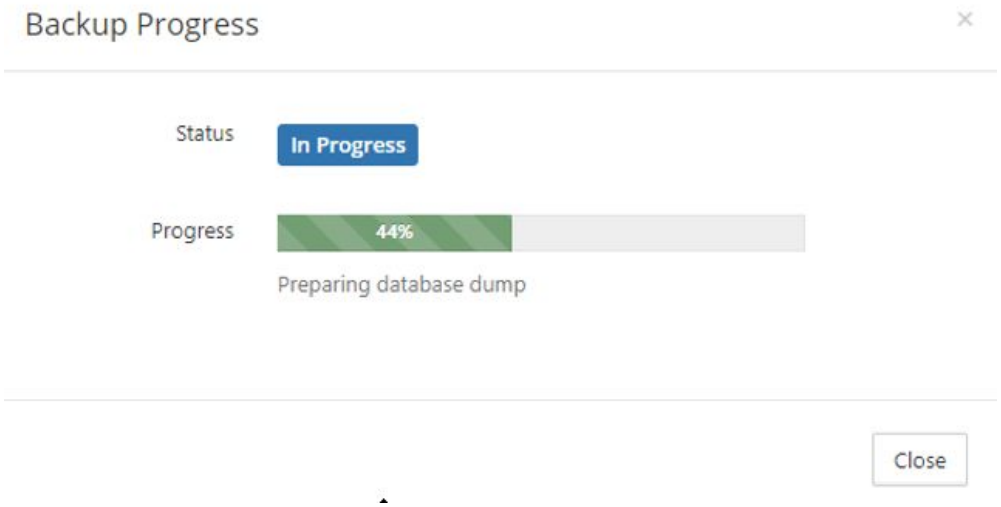

11. Click **Add**.

## Run the backup for the target server

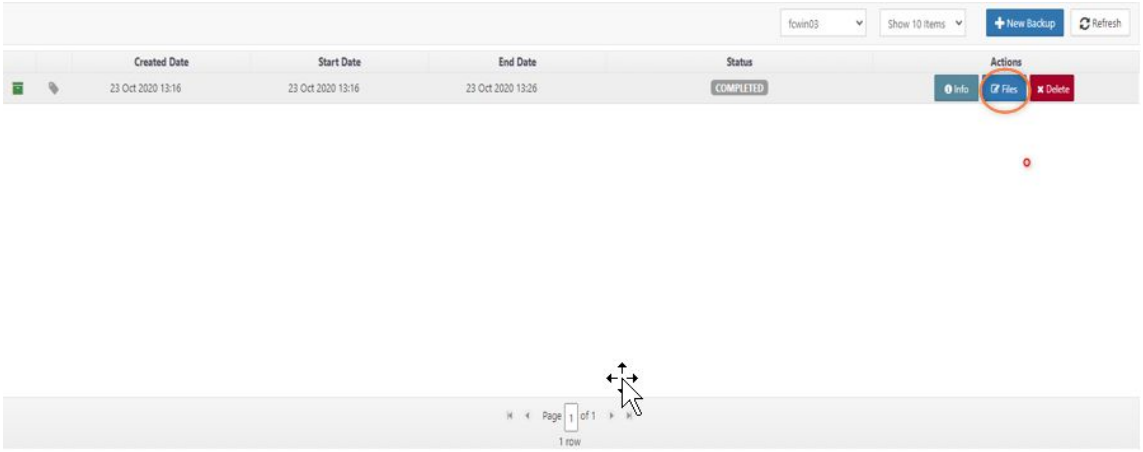
1. Open the **New Backup** screen.




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




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




## 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 (see page 242)
- Backup Server - Restore Files and Folders (see page 246)
- Backup Server - Export (see page 248)
- Backup Server - Download (see page 251)
- Backup Server - Cron Command (see page 252)

## 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.<br>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

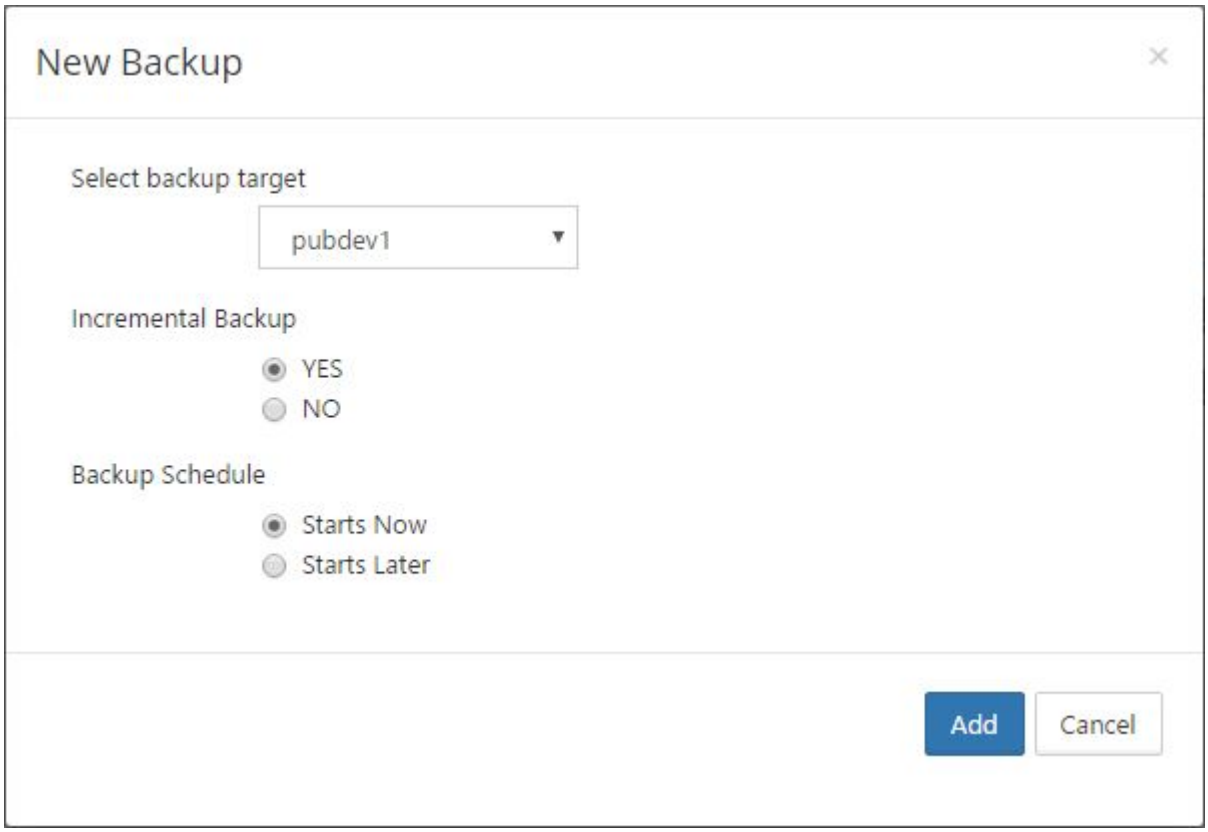
Backup server supports scheduling of backup operations. There are two types of schedules:

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

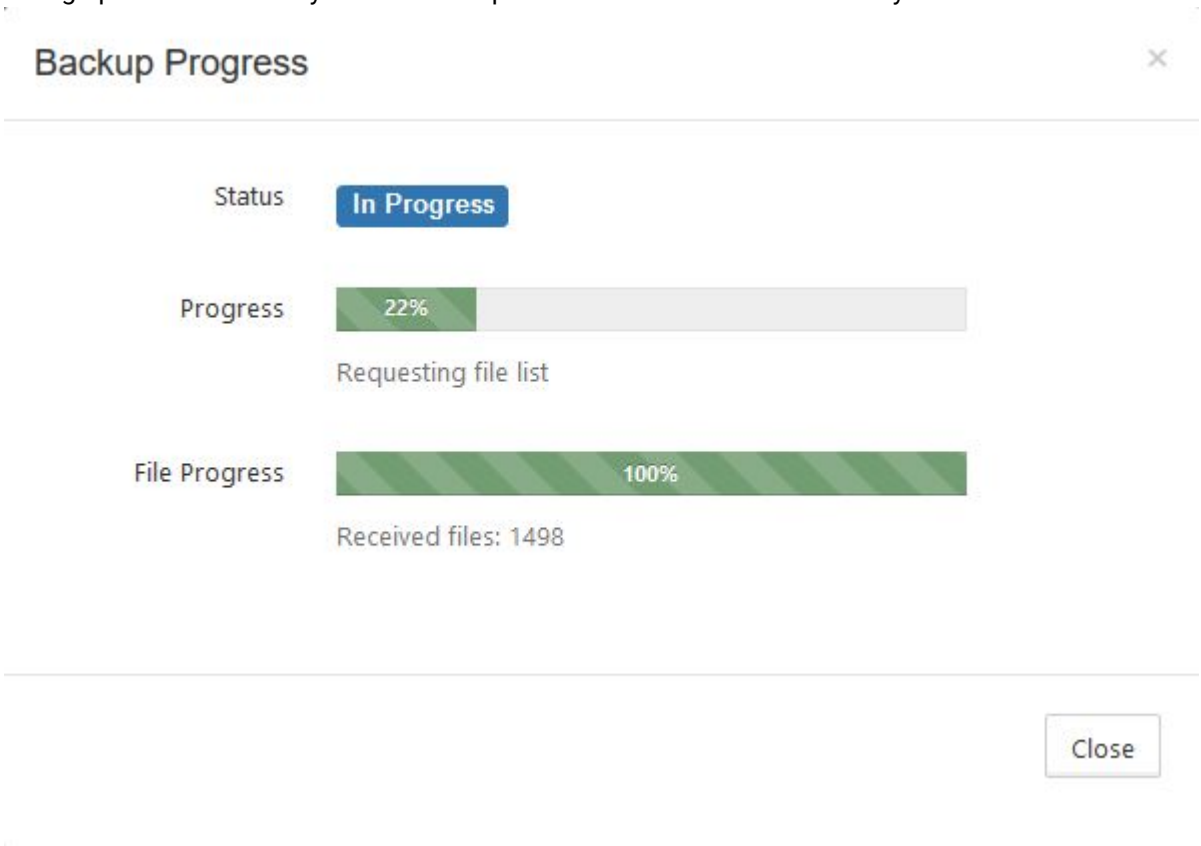
A new backup can be scheduled by going to the "Backups" tab of backup server UI and clicking on the "New Backup" button. This brings up the "New Backup" popup, which requires the following information.

- 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.

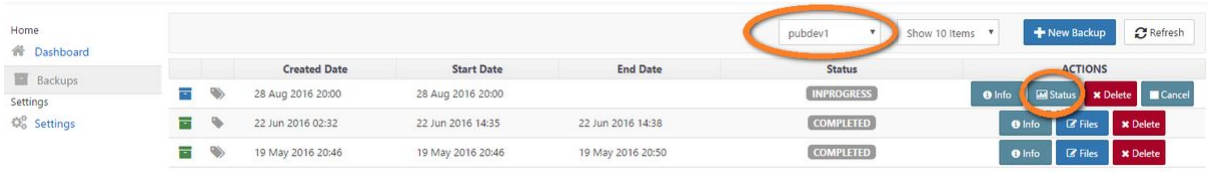

New Backup
Select backup target
pubdev1
Incremental Backup
YES
NO
Backup Schedule
Starts Now
Starts Later
Add
Cancel

### 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.




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.




### 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. |

| State | Meaning |
|---|---|
| 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

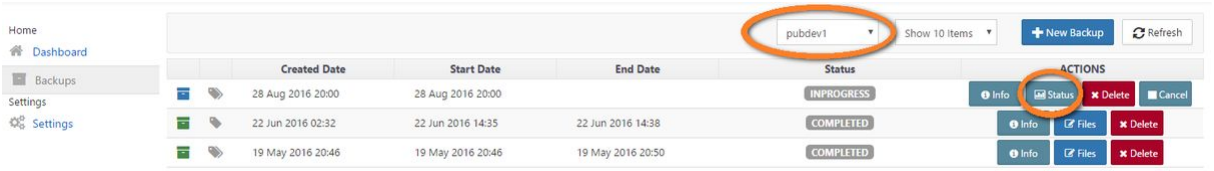
FileCloud backup server supports restoring of files/folders from the backups.

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

**Note**

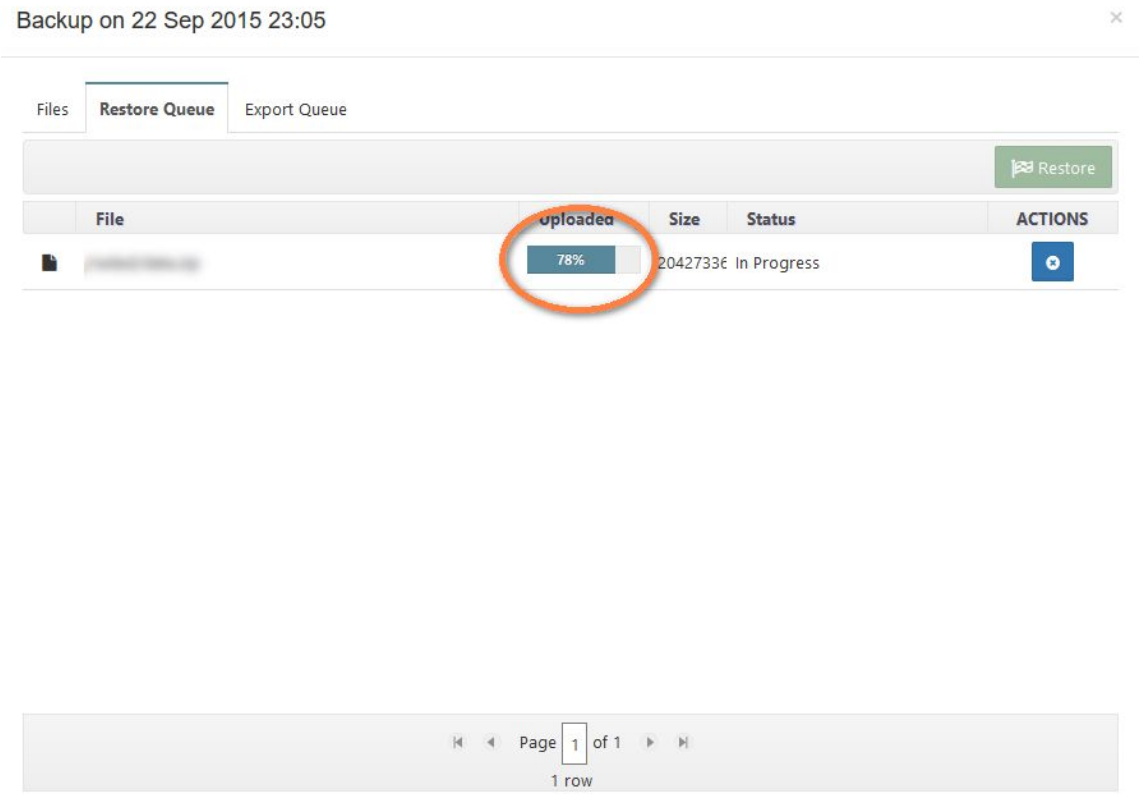
- You can restore user files and folders using Backup Server.
- You can restore databases and the entire cloud storage path manually, using the back ups you have created.

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 Server - Export

## Introduction

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

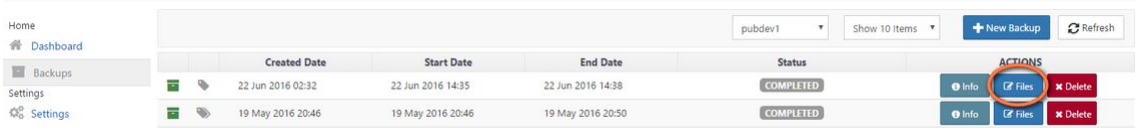
**Note**

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

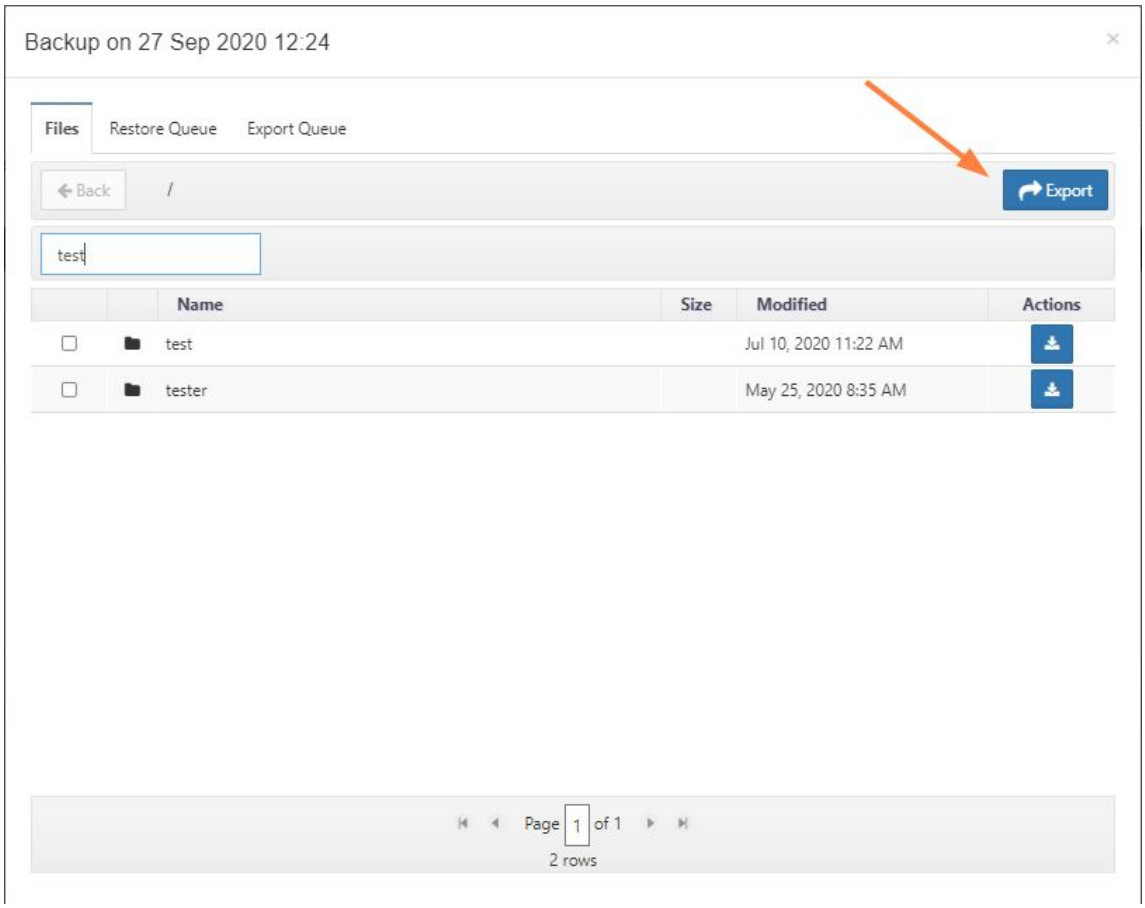
## Exporting File/Folder

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

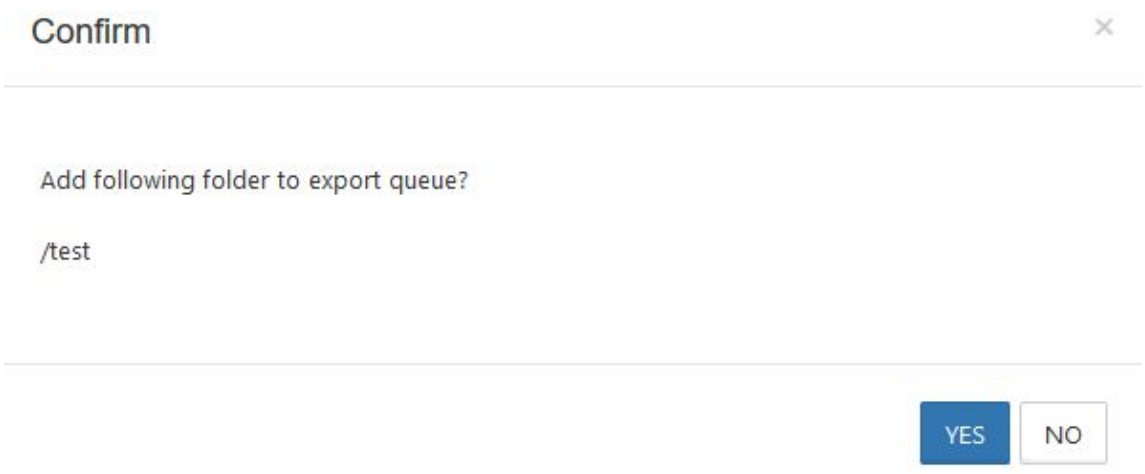
1. Select the backup from which the file/folder has to be exported.
2. Select the target from the drop-down and click on the 'Files' button for the backup that needs to be restored.



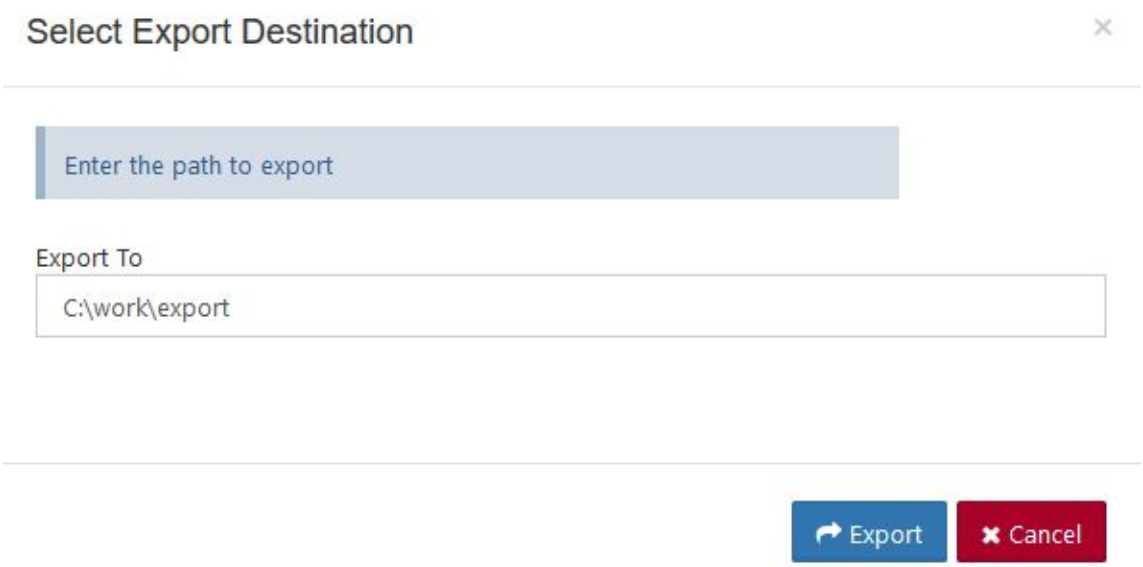

3. In the files dialog, navigate to the path containing the file/folder to be exported.
4. Select one or more file/folders and click on the 'Export' button. The selected file/folders will be sent to the export queue.



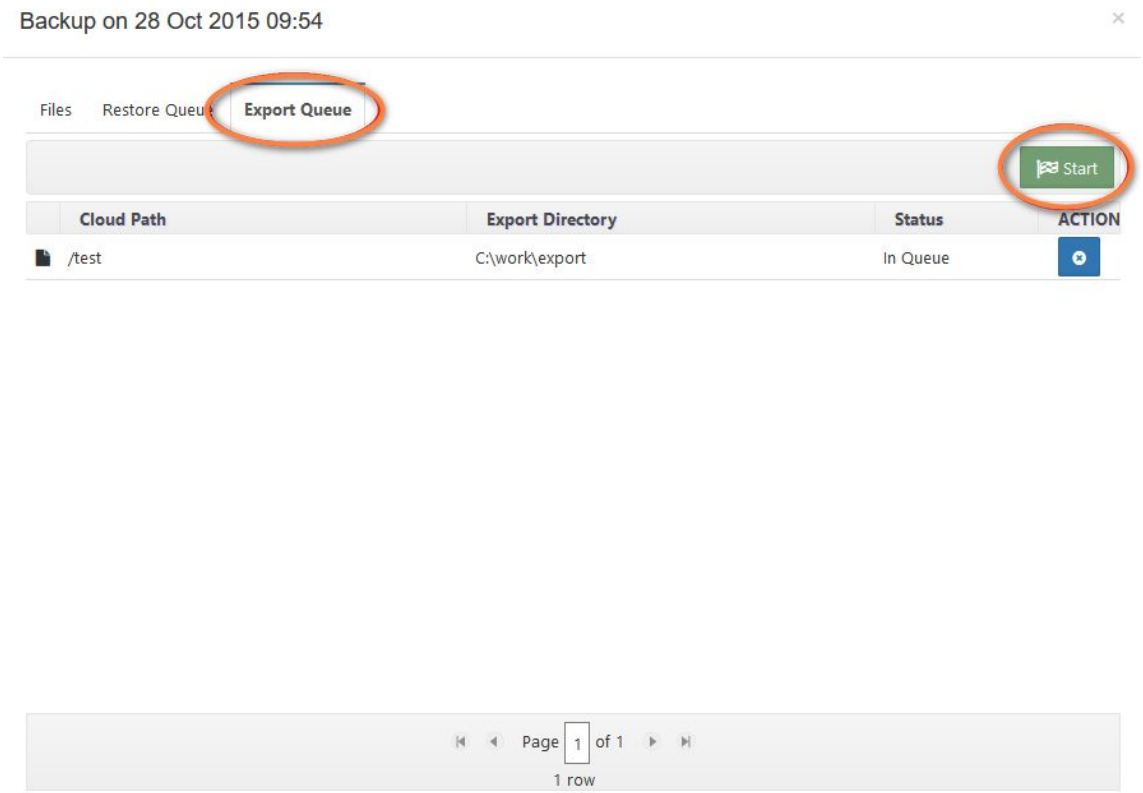

5. A prompt will appear to confirm the export path, select 'Yes' to continue.




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.




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.




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

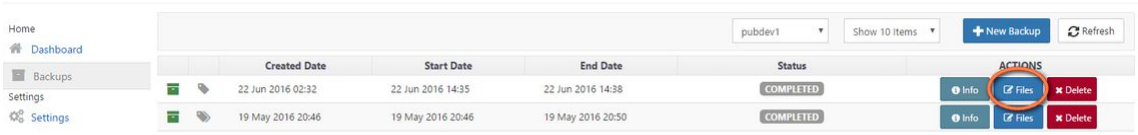
FileCloud backup server also supports downloading of files/folders from the backups directly from the web UI. When a folder is selected for download, it will be downloaded as a zip.

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

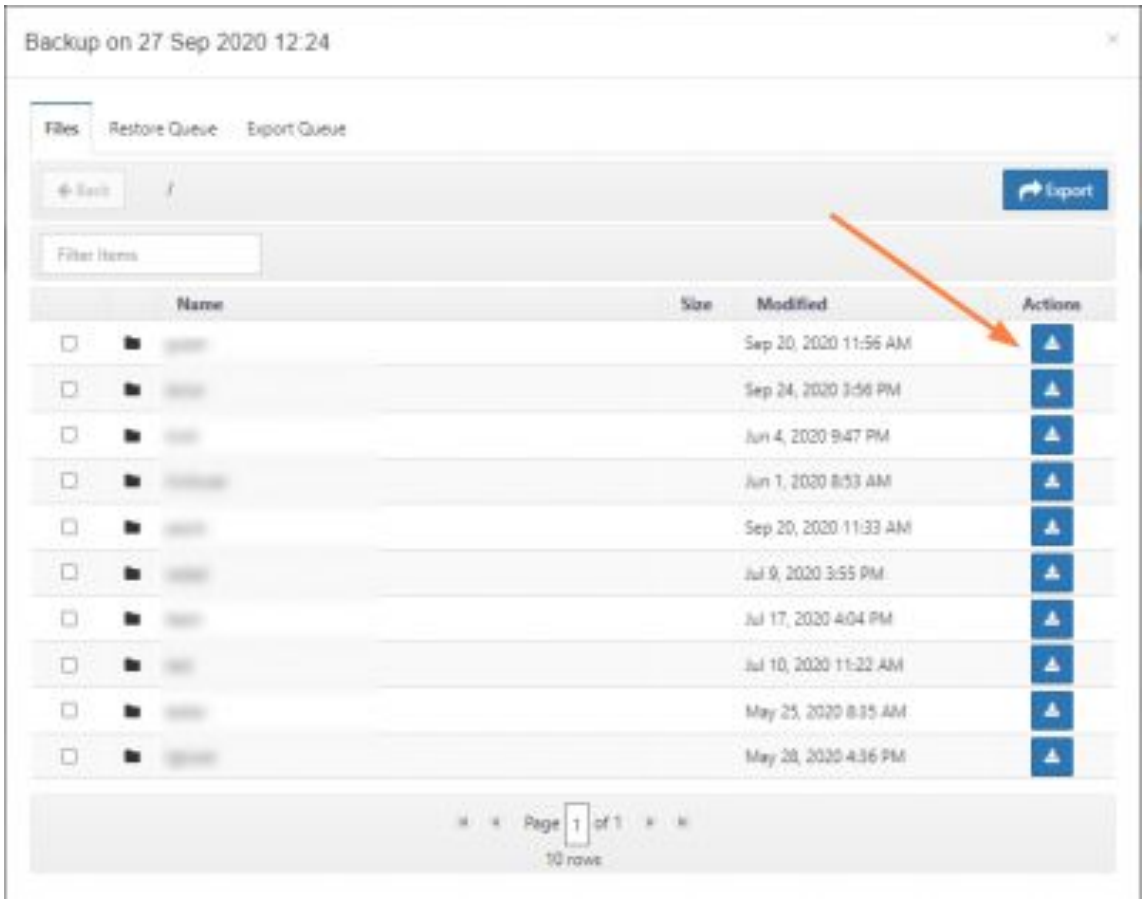
### Downloading File/Folder

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/<br>$ 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><br>--targetid specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional><br>--targetname specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional><br>--incremental specifies whether the backup job is full or incremental. Use 0 for full or 1 for incremental. Default is 0. <optional><br>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><br>--targetid specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional><br>--targetname specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional><br>--incremental specifies whether the backup job is full or incremental. Use 0 for full or 1 for incremental. Default is 0. <optional><br>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** | backupcron.php --command=listold <--targetid=target_db_id \| --targetname=target_name> --daysold=x |

| | |
|---|---|
| **Parameters** | --command=listold specifies that a list of all the backup jobs completed x days and earlier should be returned<mandatory><br>--targetid specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional><br>--targetname specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional><br>--daysold specifies the number of days or earlier for which the list should be generated. Default is 14. <optional><br>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** | backupcron.php --command=deleteold<--targetid=target_db_id \| --targetname=target_name> --daysold=x |
| **Parameters** | --command=listold specifies that a list of all the backup jobs completed x days and earlier should be returned<mandatory><br>--targetid specifies the id of the target for which the backup job is to be created. This is the database id of target. <optional><br>--targetname specifies the name of the target. This is the name assigned for the target during its creation in the UI <optional><br>--daysold specifies the number of days or earlier for which the list should be generated. Default is 14. <optional><br>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, tonidoclouddb, tonidosyncdb,
tonidostoragedb")
```

So the AuditDB will be skipped during backups.

## Backing Up and Restoring Linux

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

### What do you want to do?

- Use the FileCloud Server Backup Tool (see page 226)
- Manually Create a Linux Backup to Restore (see page 255)

## 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 mongodb. This prevents any client from adding/removing files while the backup is in progress.

## Stopping services

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

Please use equivalent commands applicable for your OS distro.

## Restore FileCloud installation

Restore the FileCloud installation files using the following command.

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

## Restoring FileCloud installation

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

## Restore database

Restore the database using the following command.

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

## Restoring FileCloud installation

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

## Restore user files

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

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

Use the following commands, to restore user files.

## Backing up user data files

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

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

## Start Webserver and MongoDB

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

### Starting services

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

Please use equivalent commands applicable for your OS distro.

## FileCloud Backup and Restore - Windows Manual

An easy to use FileCloud Server Backup and Restore option is available for administrators.
See The FileCloud Server Backup Tool (see page 226) for more details

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

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

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

**Backup**

High level steps to backup FileCloud in windows:

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

### Stop Webserver and MongoDB

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

### Backup cloud files

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

## Backup database

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

Backup user files

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

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

## Start Webserver and MongoDB

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

**Restore**

High level steps to restore FileCloud in windows:

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

## Stop Webserver and MongoDB

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

## Restore cloud files

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

## Restore database

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

Restore user files

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

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

### Start Webserver and MongoDB

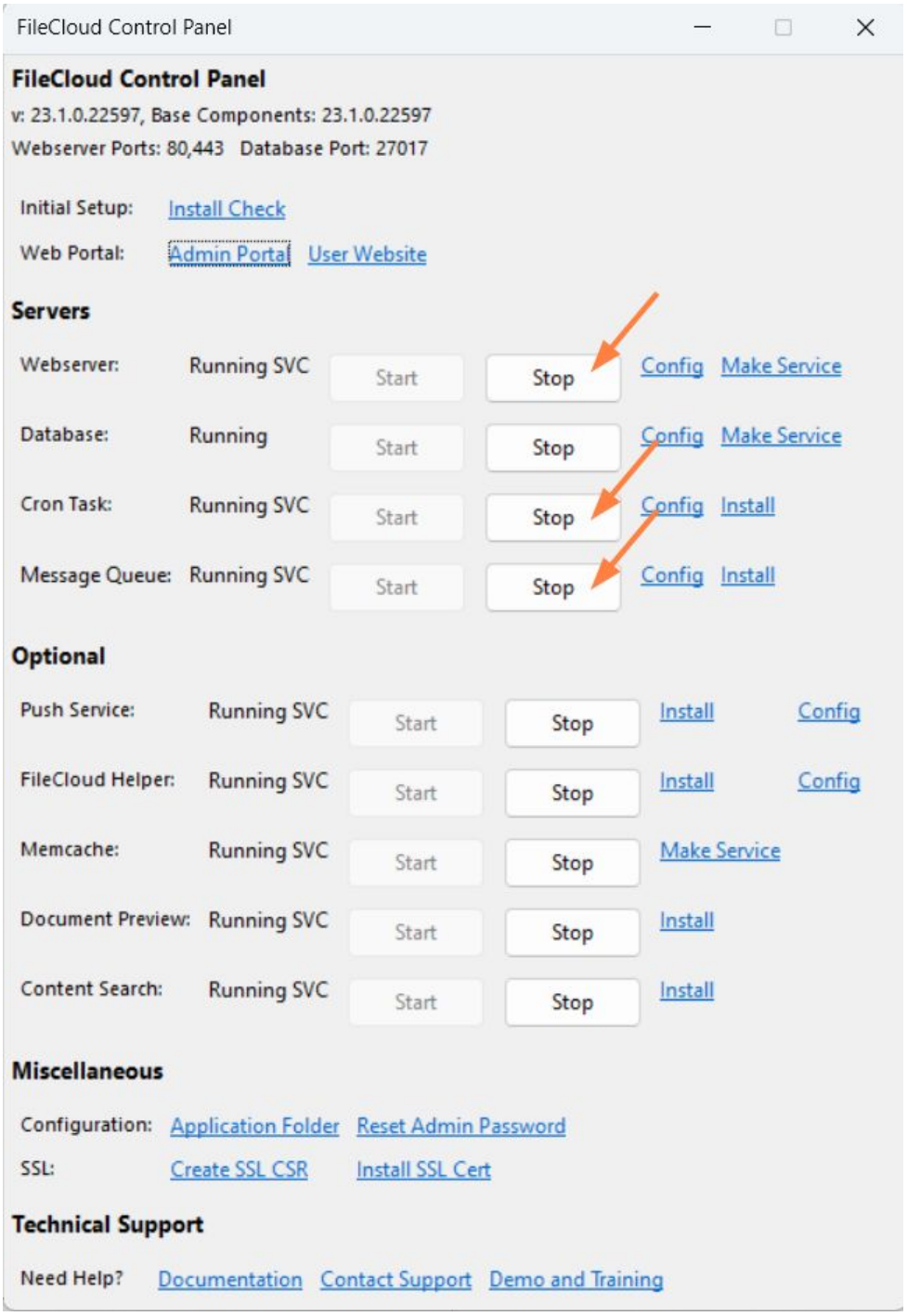
After the above restore steps are performed, start the apache webserver and mongodb process.

## Migrating FileCloud Server to Another Server

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

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

| OS | |
|---|---|
| **Linux** | **Ubuntu:**<br>systemctl stop apache2<br>systemctl stop cron<br>systemctl stop fcorchestrator<br><br>**RedHat:**<br>service stop httpd<br>service stop crond<br>service stop fcorchestrator |

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



3. Create a database dump on the source system.

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

4. If the database has "TONIDO" in its name, copy the database dump to the new system and restore it.

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

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<br>**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[31]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[32]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[33].

To disable SELinux, enter:

31. https://www.filecloud.com/supportdocs/fcdoc/latest/server/filecloud-administrator-guide/filecloud-site-maintenance/audit-logs/delete-audit-log-entries
32. https://www.filecloud.com/supportdocs/fcdoc/latest/server/filecloud-administrator-guide/installing-filecloud-server/post-installation/ssl-configuration
33. https://www.filecloud.com/supportdocs/fcdoc/latest/server/filecloud-administrator-guide/installing-filecloud-server/post-installation/selinux-policies-for-filecloud-installation

**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 (see page 261)

## 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[34]

#### RETURNED XML DATA

```
<stats>
 <stat>
<totalusers>55</totalusers>
<fullaccessusers>25</fullaccessusers>
<guestaccessusers>27</guestaccessusers>
<totalsize>87.5 GB</totalsize>
<totalsizeused>2.45 GB</totalsizeused>
```

34. https://itonido.com/admin/?op=getstats&password=apipassword

```
<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.

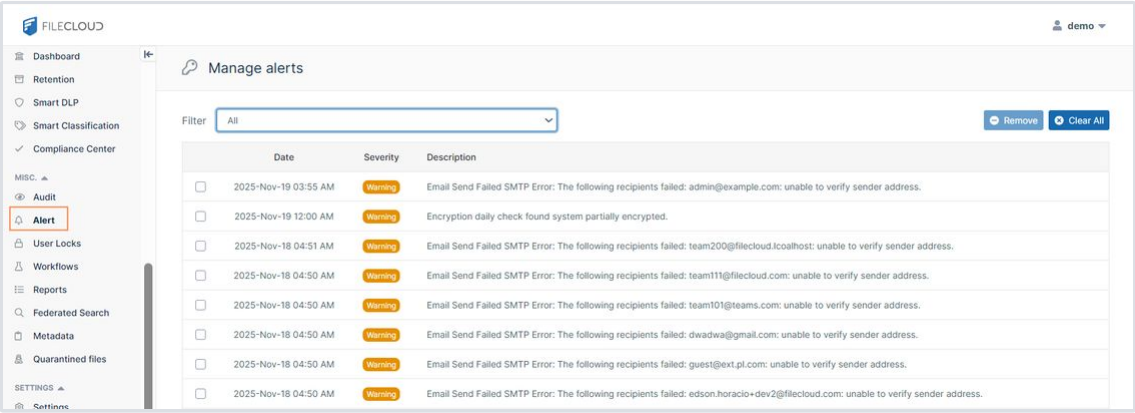
Depending on the error, you may need to take steps to correct the problem. For example, if alerts indicate that system is frequently running out of memory, then system memory may need to be increased.

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

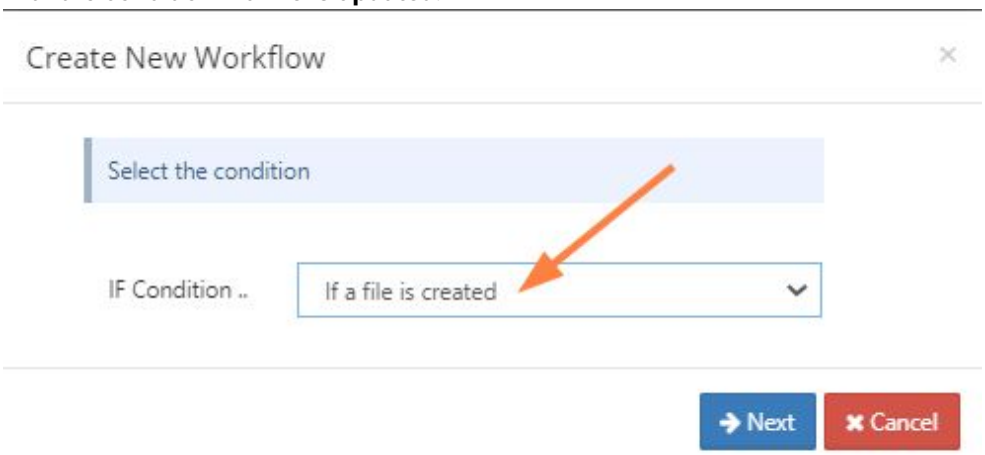
Ransomware is a type of malware that an attacker uses to infiltrate your system and make your files inaccessible, usually by encrypting them. The attacker then demands that you pay a ransom to decrypt your files.

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.

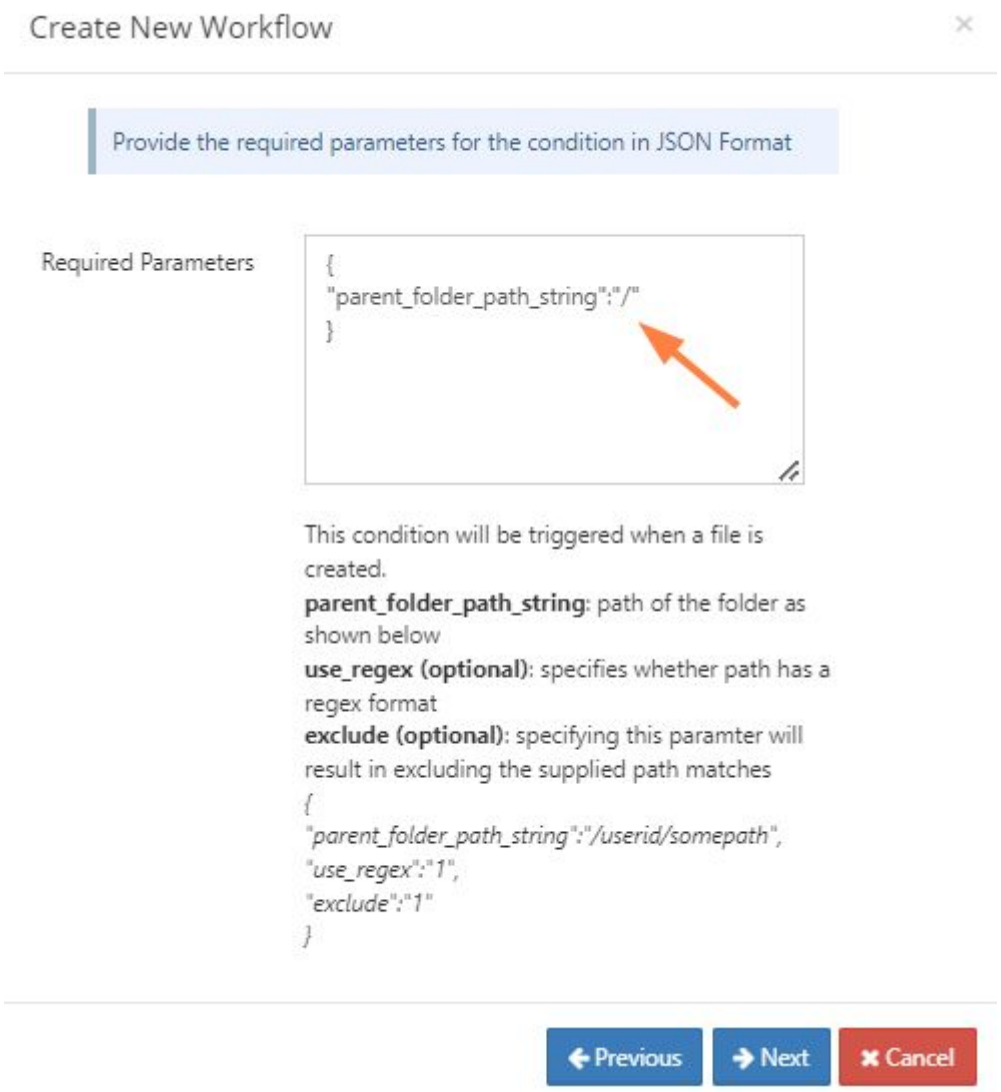
The FileCloud heuristic engine is available to you, but to use it, you must add it to a workflow (see page 369) in your system by choosing a **Verify file integrity** action. When a file fails the integrity check, the workflow can either delete the file or send a notification.

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

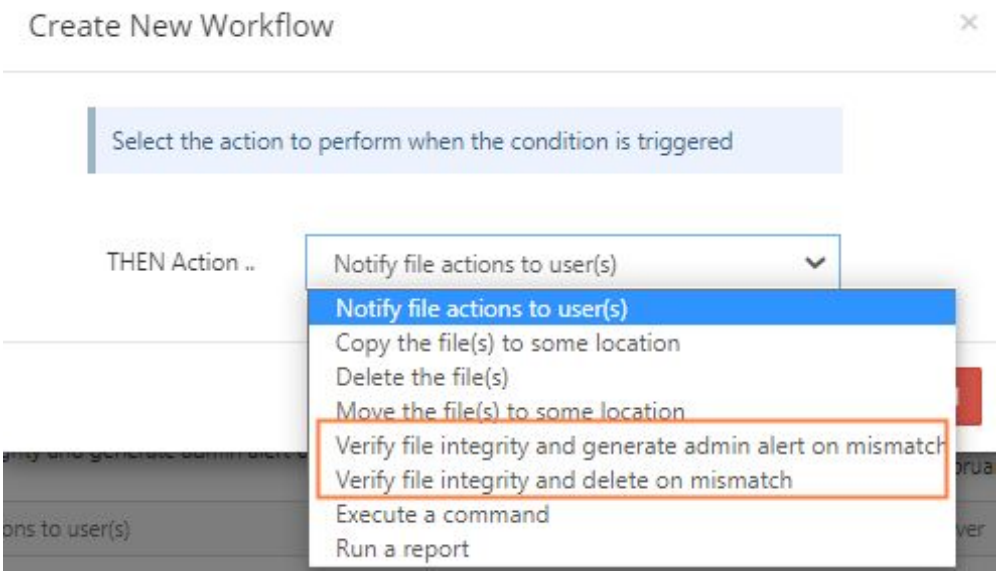
1. In the admin portal, in the navigation panel, click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
   The **Create New Workflow** dialog box opens.
3. To perform the check on every file that is uploaded for the first time, in the **IF Condition** drop-down list, choose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




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

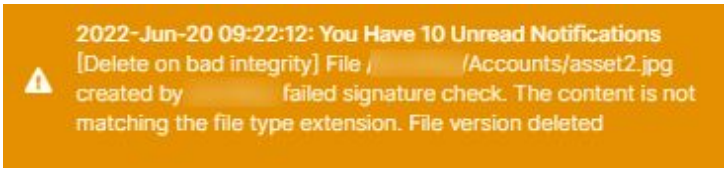



6. Click **Next**.
   You are prompted to choose an action.
7. Choose one of the **Verify file integrity** actions depending on what you want the system to do when a mismatch is detected. The possible actions are:
   - **Verify file integrity and generate admin alert on mismatch**: Detects the mismatch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



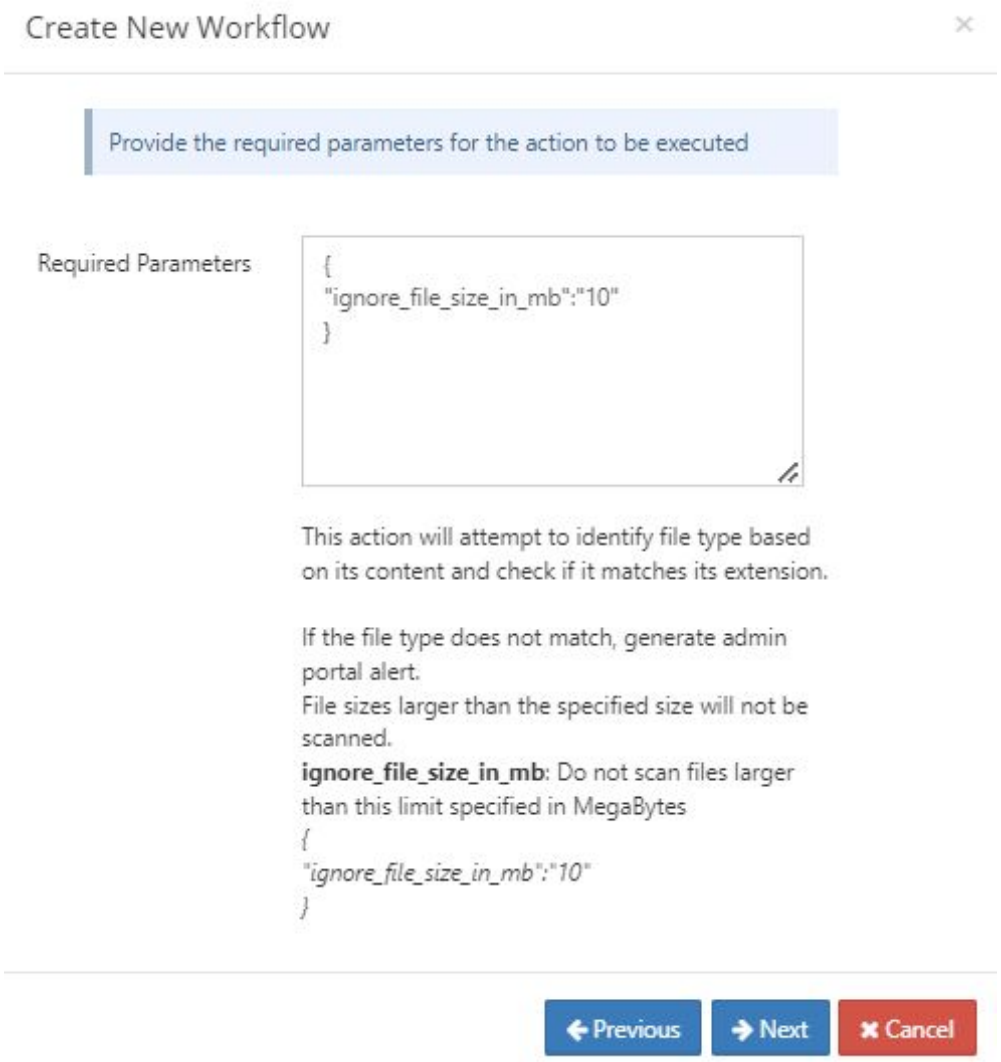

In both cases, a pop-up in the user interface notifies the user that the content and file type extension do not match, either:

or

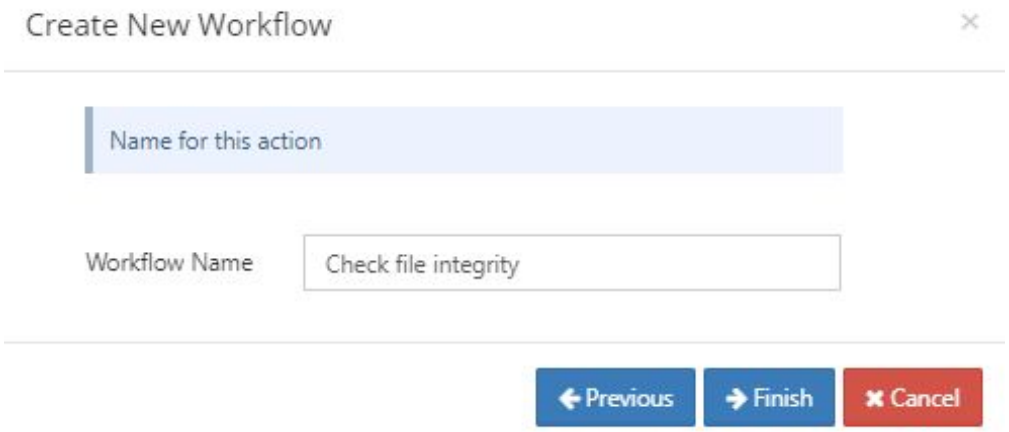



In both cases, alerts also appear in the **Manage Alerts** screen of the admin portal.

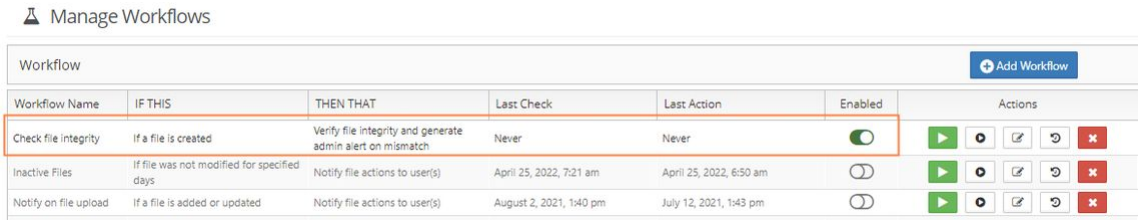
8. After you choose one of the actions, click **Next**.
9. Add the **ignore_file_size_in_mb** parameter. The purpose of this parameter is to prevent the system from slowing down by scanning the content of large files.
   In the following example, the parameter is set to **10**.




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



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




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

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

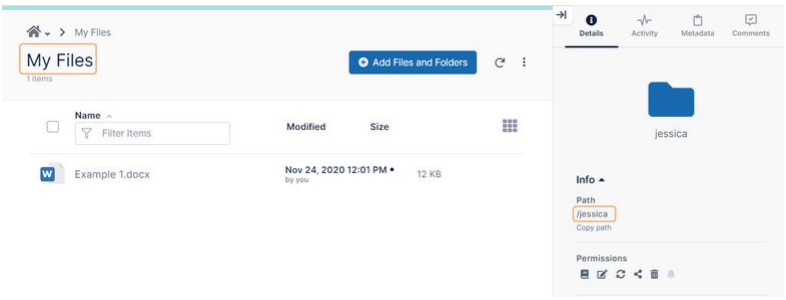
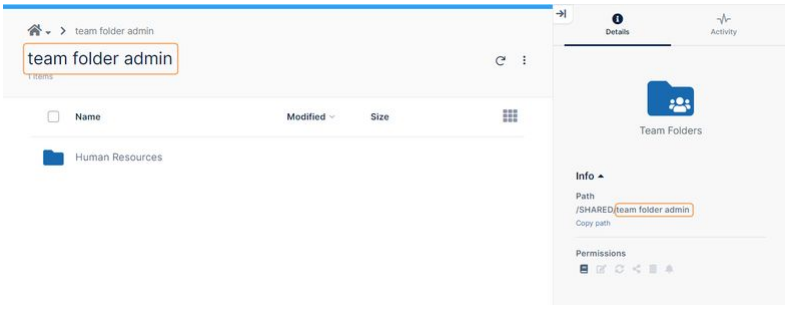
2. Include the following setting, and add additional extensions. You may also remove extensions. In the following example, the extensions pem, cfg, and cfg2 are added:

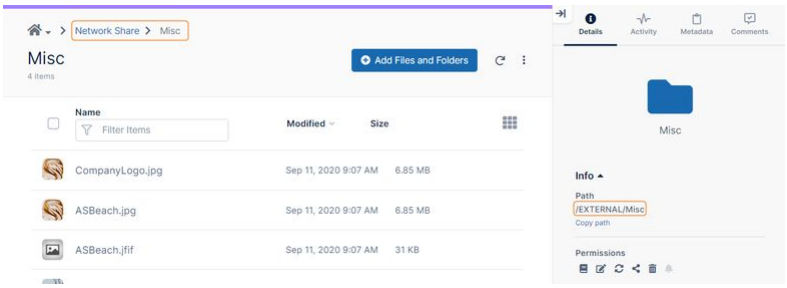
```
define('TONIDO_TEXT_FILE_EXTENSIONS', 'TXT|DAT|LOG|CSV|PEM|CFG|CFG2');
```

# 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 (see page 277) or a workflow (see page 369), 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:<br><br>**/jessica**<br><br>If **jessica** were logged in, and she selected **My Files**, she would see the exact path in the **Details** tab in the right panel.<br>  |
| Team Folders | /teamfolderaccount | In this example, to specify the **Team Folders** folder use the name of the account that manages Team Folders:<br>**/team folder admin**<br><br>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<br>  |

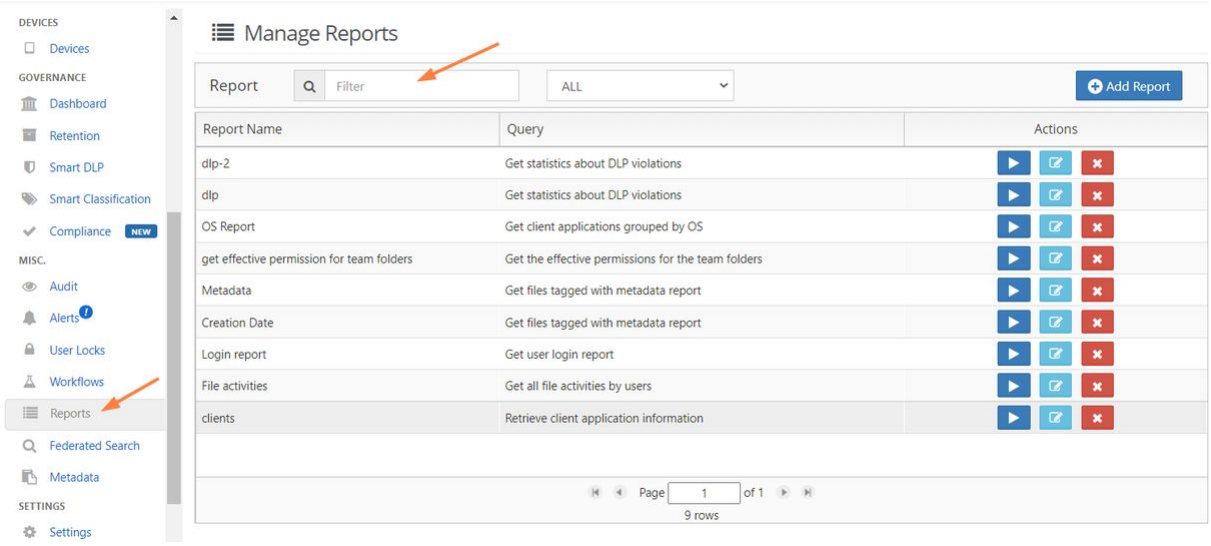
| | | |
|---|---|---|
| Network Shares | /EXTERNAL/foldername | In this example, to specify the **Network Shares** folder **Misc**, use: /EXTERNAL/Misc<br>An end user who selected **Network Shares/Misc** could look in the **Details** tab in the right panel and copy the exact path.<br>  |
| Shared with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

# Custom Reports

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

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

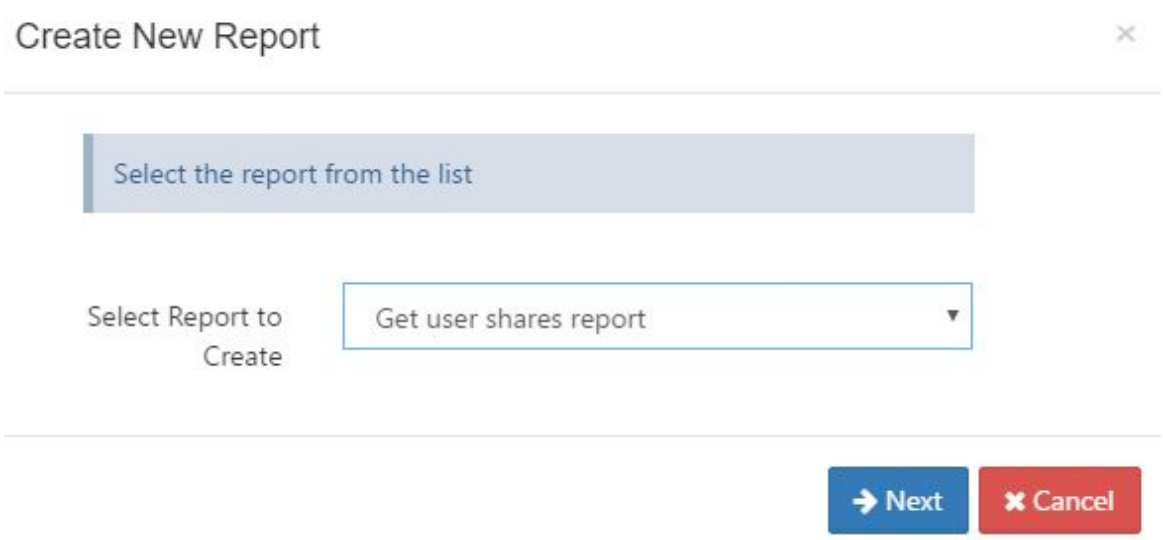
The reports screen displays the list of existing reports. The filter text box can be used to filter reports by name. The individual reports on the report list can be viewed, downloaded, edited and deleted. New reports can be added by clicking the Add Report button.



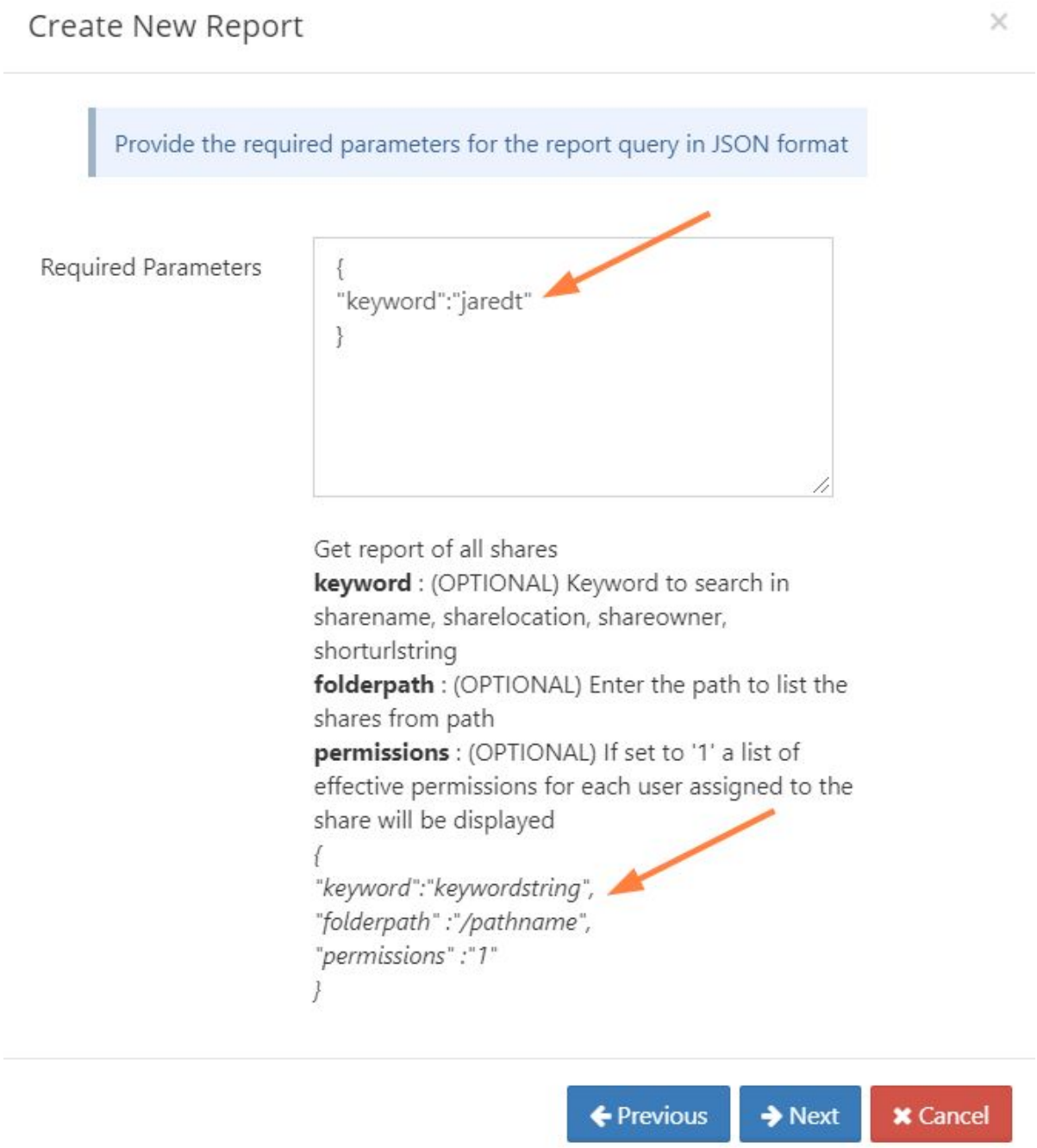

Some reports, such as reports on file actions and failed logins, get their data from the audit log. These reports only include events that are in the audit logs when you run the report.

## Add Reports

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



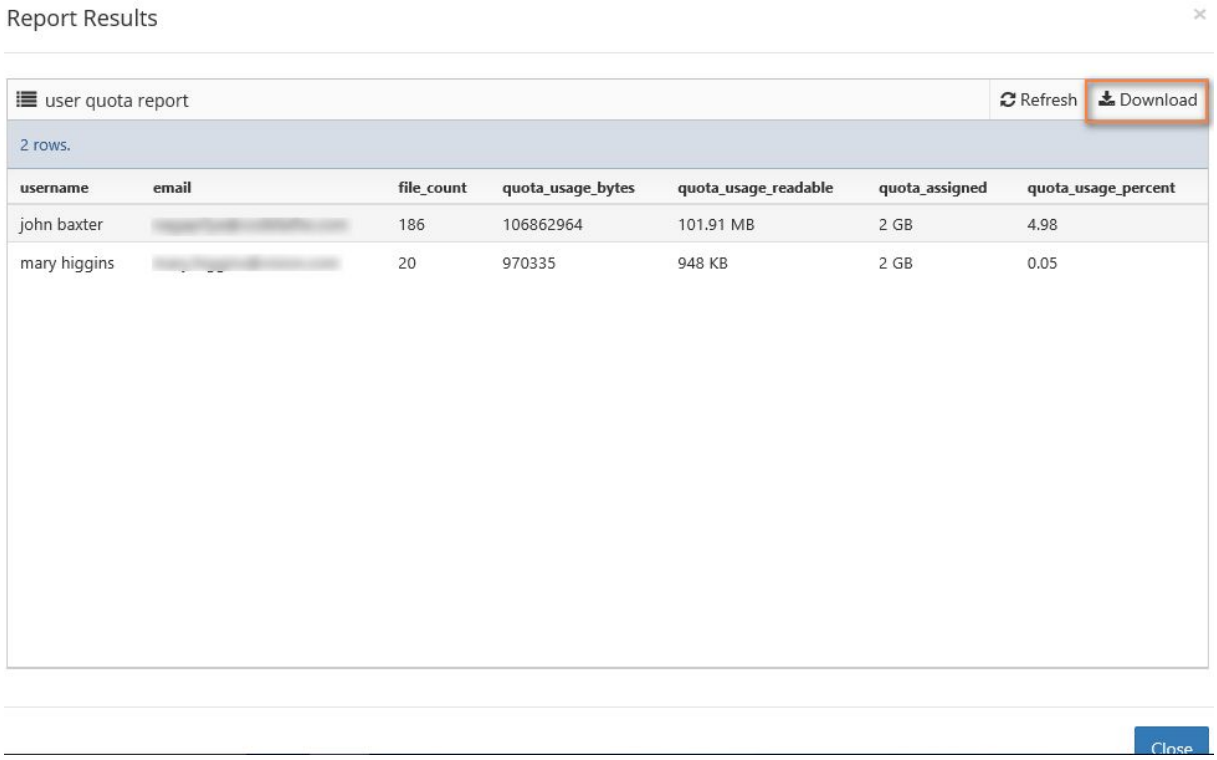

The next step is the set the parameters. The parameters can be entered in the text box. The format for the parameters are given on the bottom of the screen. The screen also indicates whether the parameters are optional or required.




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

## Download Reports

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




## Available Reports

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

| Report Name | Description |
|---|---|
| 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.<br>**Data Retrieved**: Timestamp of action, username, file name, action.<br>**Parameters**:<br>• user: (OPTIONAL) Enter the username to list the file activities of the user<br>• from_date: (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date: (OPTIONAL) To date in Y-M-d H:i:s<br>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<br>**Data Retrieved**: File Type, total files stored.<br>**Parameters**: None |
| Get storage usage by file type | Report of amount of storage space used by each file type.<br>**Data Retrieved**: File type, sizeraw (file size in bytes), size (formatted file size)<br>**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<br>**Data Retrieved**: username, total files stored.<br>**Parameters**: None |
| Get user quota usage report | Report of users who use the maximum quote in FileCloud managed storage<br><br>**Data Retrieved**: username, email, file count, quote usage, quote assigned, quote usage percentage.<br>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.<br><br>**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<br>**Data Retrieved**: days, total files changed, percent of files changed.<br>**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.<br>**Data Retrieved:** Timestamp of upload, user name, user agent, IP address, file path, bytes of file uploaded<br>**Parameters:**<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date : (OPTIONAL) To date in Y-M-d H:i:s<br>• username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified<br>• 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.<br>**Data Retrieved:** Timestamp of download, user name, user agent, IP address, file path, bytes of file downloaded<br>**Parameters:**<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date : (OPTIONAL) To date in Y-M-d H:i:s<br>• folder_path : (OPTIONAL) Restrict report to files inside specified path.<br>• username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified<br>• 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.<br>**Data Retrieved:** path of folder or file, username, metadata field, value of metadata field<br>**Parameters:**<br>• metadata_name : (REQUIRED) Name of the metadata set<br>• attribute_name : (REQUIRED) Name of the metadata attribute<br>• attribute_value: (OPTIONAL) Metadata attribute value |
| Get shares report | Report listing shares created.<br>**Data Retrieved:** Timestamp of download, user name, user agent, IP address, file path, password<br>**Parameters:**<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date : (OPTIONAL) To date in Y-M-d H:i:s<br>• username : (OPTIONAL) User account name - can be set only when *from_date* and *to_date* are specified |

| Report Name | Description |
|---|---|
| File query report | Report listing files or folders filtered by specified parameters if included.<br>**Data Retrieved:** file or folder name, path, type (file or folder), size, last modification date, create date<br>Note: Prior to FileCloud version 21.3, the year for the modification and create dates is returned in 2 digits (for example<br>**Parameters**:<br>• userid : (OPTIONAL) User id to retrieve listing. If not supplied, all user listings are generated<br>• sort : (OPTIONAL) Sort criteria can be "SIZE" or "MODDATE" or "CREATEDDATE"<br>• limit : (OPTIONAL) the total number of results<br>• searchterm : (OPTIONAL) Match keyword in file or folder name<br>• type : (OPTIONAL) Type can be "file" or "folder", default is "file"<br>• path : (OPTIONAL) Restrict report to files inside specified path. For help specifying the path correctly, see Identifying a FileCloud Specific Path (see page 275). |
| File count report | Report of file count in paths specified in parameters.<br>**Data Retrieved**: number of files in each specified path.<br>**Parameters**: List of paths. For help specifying the path correctly, see Identifying a FileCloud Specific Path (see page 275).<br><br>**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.<br>**Data Retrieved:** Timestamp of delete, user name, user agent, IP address, file path<br>**Parameters:**<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• 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.<br>**Data Retrieved:** upload bandwidth and download bandwidth<br>**Parameters:**<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date : (OPTIONAL) To date in Y-M-d H:i:s |

| Report Name | Description |
|---|---|
| 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<br>**Data Retrieved**: folder and sub folder path, file count and size<br>**Parameters**:<br>• path: (REQUIRED) Location path. For help specifying the path correctly, see Identifying a FileCloud Specific Path (see page 275).<br>This report is available in FileCloud version 20.3 and later. |
| Get all exported secure docs report | Report of all files exported securely.<br>**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<br>**Parameters**: None |
| Get user shares report | Report of all the shares created in FileCloud and their details.<br>**Data Retrieved**: share name, share owner, share URL, share type, share location, created on, last access, expiry date<br>**Parameters**:<br>• keyword - search keyword in share name, share owner, share url string (string following /url/)<br>• folderpath - location path. For help specifying the path correctly, see Identifying a FileCloud Specific Path (see page 275).<br>The CSV file that is downloaded contains additional information about users and groups that have access to each share.<br>This update is available in FileCloud Server version 18.2 and later. |

| Report Name | Description |
|---|---|
| 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.<br>**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<br>For multiple entries of the same share, the Action Details column on the report shows the most recent share's permissions.<br>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.<br>**Parameters**:<br>from_date: (OPTIONAL) From date in Y-M-d H:i:s<br>to_date: (OPTIONAL) To date in Y-M-d H:i:s<br>owner: (OPTIONAL) Owner name<br>This report is available beginning in FileCloud 20.1. |
| Get files/folders shared with user | Report listing the files and folders shared with a specific user<br>**Data Retrieved**: share name, share owner, share url, share location, type (private or public), expiry date, creation date<br>**Parameter**:email of share recipient<br>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.<br>**Data Retrieved**: folder, type (private or public), share location, user, permission<br>**Parameters**:<br>• 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 (see page 275).<br>• users : (OPTIONAL) List of users to be included in the report. |

| Report Name | Description |
|---|---|
| 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** (see page 2) in **Settings > Admin** must be set to **TRUE**.<br>**Data Retrieved**: IP address, operation, username, user agent, geo area, city, country, create date<br>**Parameters**:<br>• from_date : (OPTIONAL) From date in Y-M-d H:i:s<br>• to_date : (OPTIONAL) To date in Y-M-d H:i:s<br>• 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.<br>**Data Retrieved**: login time, username, useragent, IP<br>**Parameters**:<br>• from_date: (OPTIONAL) login from date<br>• to_date: (OPTIONAL) login to date<br>OR<br>• last_number_of_hours : (OPTIONAL) number of hours before the present time to begin retrieving login records.<br>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<br>**Data Retrieved:** sender, number of emails sent<br>**Parameters:**<br>• hours: number of hours ago to begin retrieving sent email records. |
| Get statistics about DLP violations | Report of DLP violations by rule.<br>**Data Retrieved:** user, time of violation, user action, rule violated<br>**Parameters:**<br>• **rule_name** : (OPTIONAL) Name of the rule<br>• **minutes** : (OPTIONAL) How many minutes ago to begin looking at violations<br>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<br>**Data Retrieved:** user name<br>**Parameters:**<br>• **minutes** : (OPTIONAL) How many minutes ago to consider users as active |

| Report Name | Description |
|---|---|
| Get file movement statistics | Report of last file uploads, downloads, and shares (or share changes)<br>**Data Retrieved:** number of files downloaded, number of files uploaded, number of files shared and share changes<br>**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

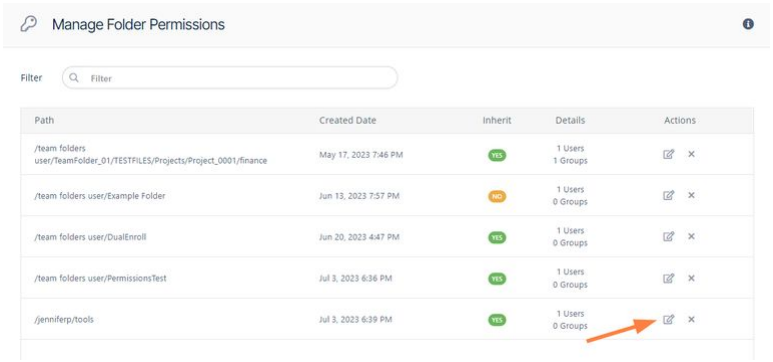
Administrators can manage folder-level permissions assigned to folders. In order to view these folder-level permissions, the admin must be the master admin or an admin user with access to the folder permissions enabled. An admin user can be granted access to the Folder permissions system through the Admins menu item on the left navigation panel (see Managing Admin Users (see page 48)).

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

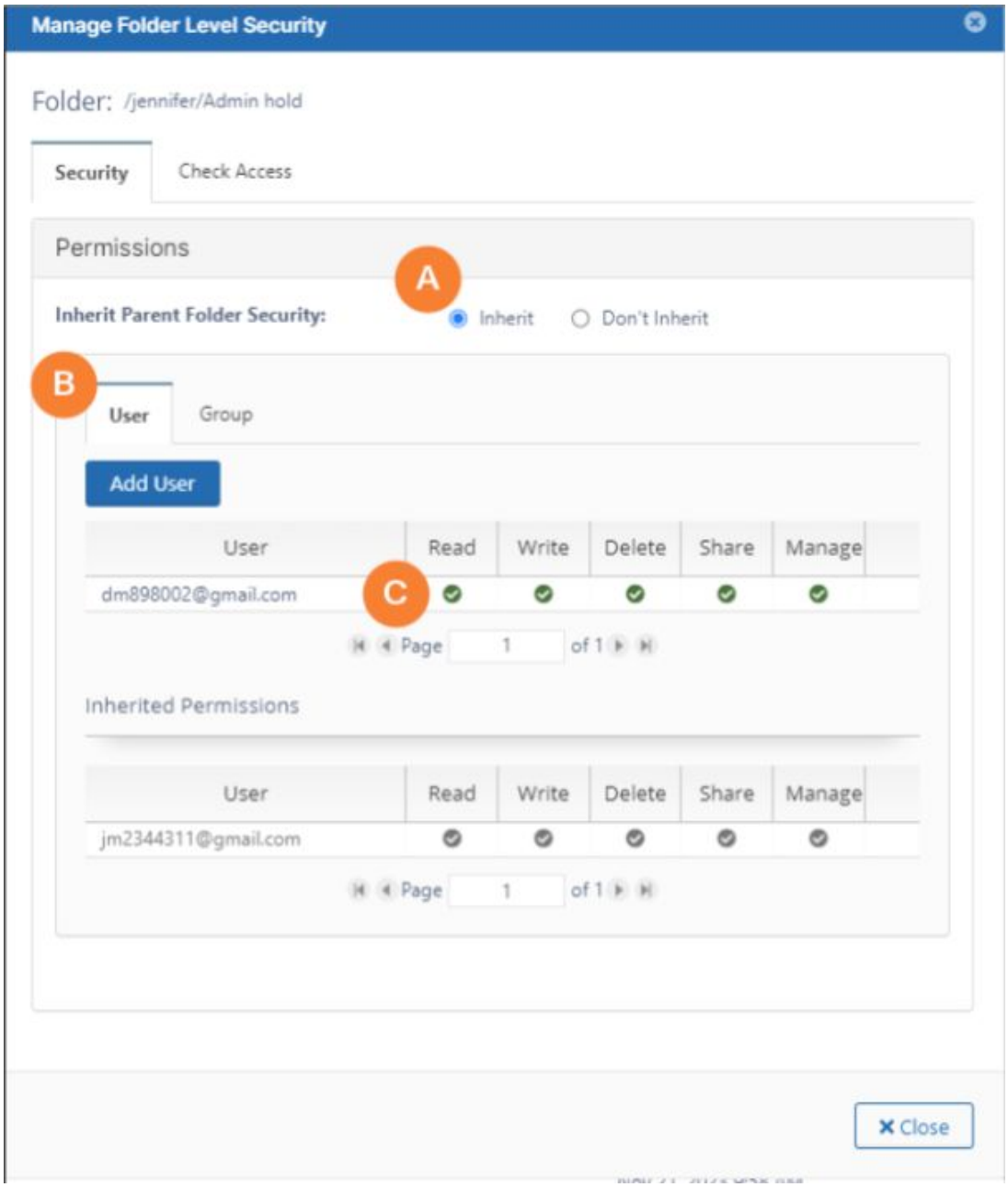
For more information about folder-level permissions, see Folder-Level Permissions.

## To Edit Folder-Level Permissions

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




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




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

# Read Only Sync

Read only sync is supported starting from FileCloud 17.3

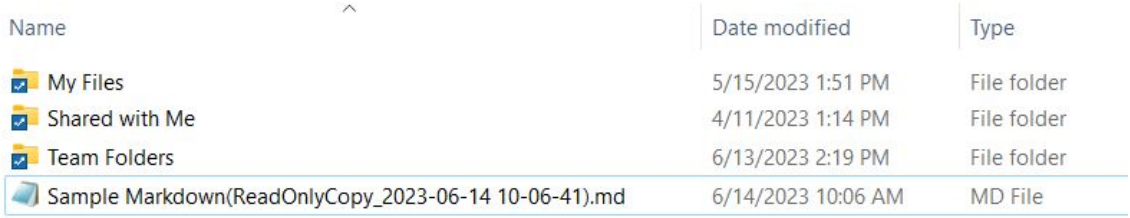
One way read-only syncing of shared folders is supported in FileCloud for Shared Folders with Folder Permissions.

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:




- 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.

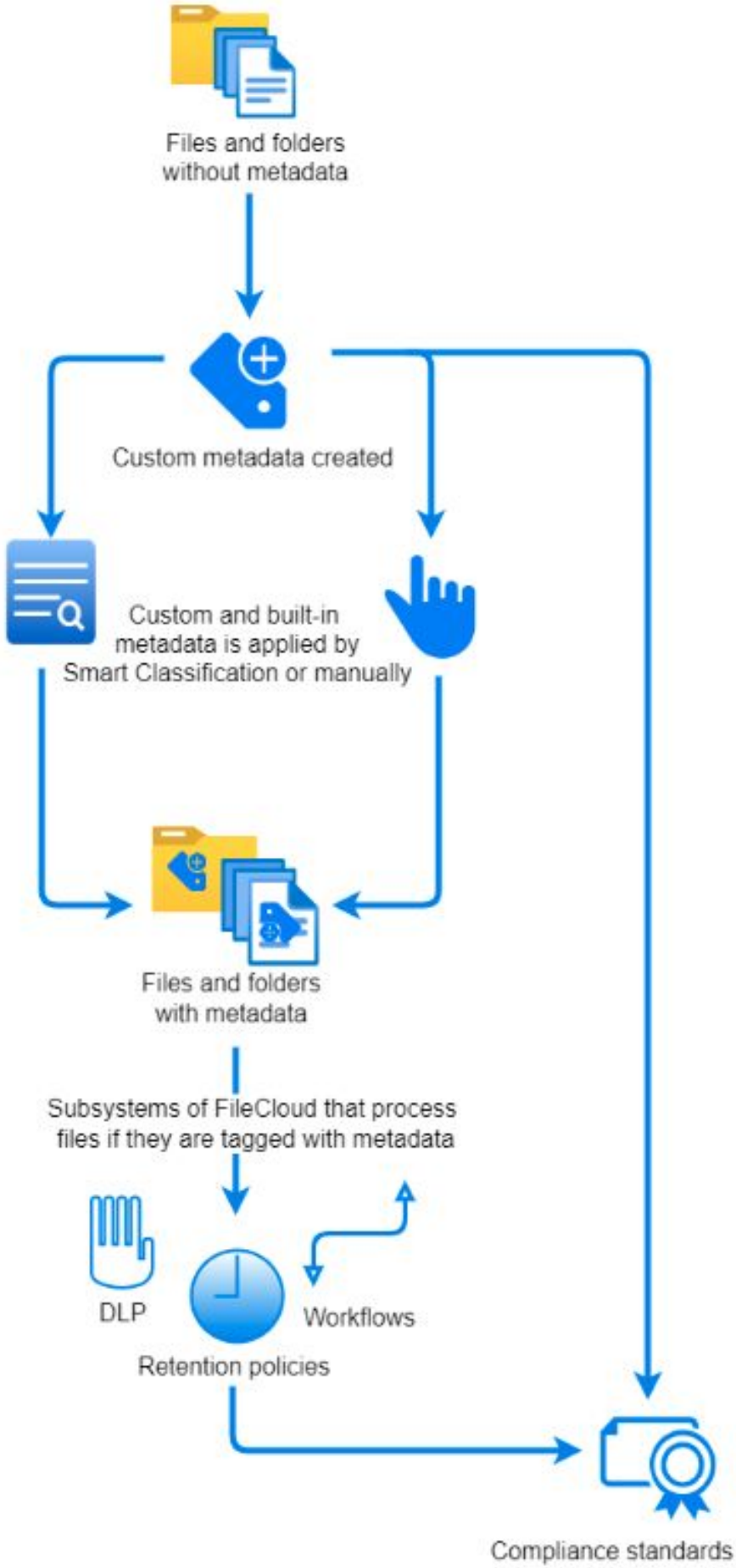
## Metadata for governance and other system processes

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.


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

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

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

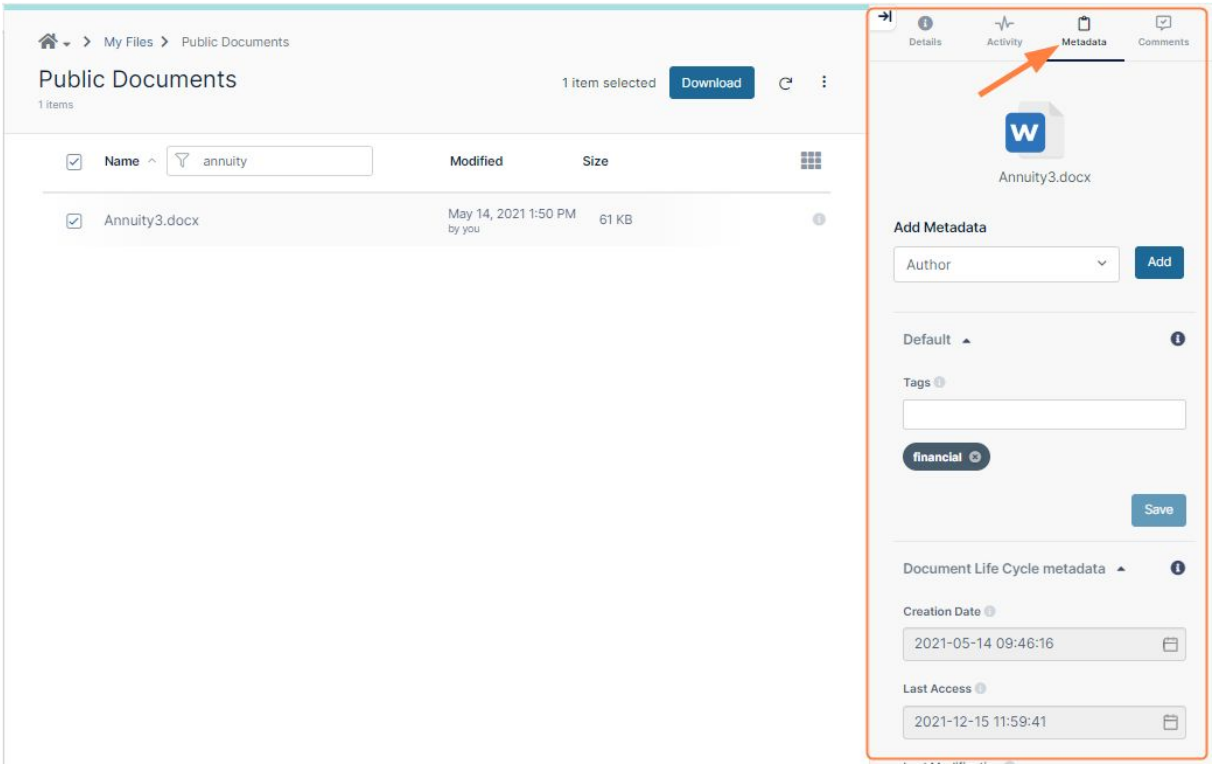
Here are some examples of the way compliance rules are met by metadata:

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

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

## Metadata for users

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




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

In this section


- Metadata Components and Types (see page 294)
- Create a New Metadata Set (see page 299)
- Edit an Existing Metadata Set (see page 303)
- Managing Metadata Attributes (see page 305)
- Managing Metadata Permissions (see page 306)
- Working with Built-In Metadata (see page 310)
- Working with Custom Metadata (see page 335)
- Working with Default Metadata (see page 336)
- Troubleshooting Metadata (see page 338)
- Finding files without metadata (see page 339)
- Metadata Limitations/Recommendations (see page 343)


## 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.<br>Describes files and folders available in the system. | A single piece of information that describes the File Object.<br>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:<br>• a resume | For example:<br>• Lives in the Human Resources Folder<br>• Has a created date<br>• Has a modified date | For example:<br>• the candidate's photo in their resume | For example, resumes will always have:<br>• <br>• Photo<br>• Name<br>• Address<br>• Experience<br>• Education | For example:<br>HR wants to tag a resume status as:<br>• Candidate<br>• New Hire<br>• OnBoarding |

## Metadata Set Types

FileCloud supports the following types of Metadata Sets:

| TYPE | DESCRIPTION | SETS AVAILABLE |
| --- | --- | --- |
| Default (see page 336) | This a special type of metadata set that is automatically associated with every single File Object when it is created, copied, uploaded, etc.<br>• For already existing File Objects it will be associated when the file / folder is accessed for the first time.<br>• Exactly one Default Set exists in FileCloud - it cannot be deleted, renamed or disabled, but administrators can customize attributes and permissions.<br>• Out of the box it is shipped with a single predefined attribute of Array type - Tags. | Defaults |

<table>
<tr><th>TYPE</th><th>DESCRIPTION</th><th>SETS AVAILABLE</th></tr>
<tr>
<td>Built-In (see page 310)</td>
<td>These are metadata sets that have been created for you.<ul><li>Administrators can edit the attributes</li><li>Administrators can choose to disable the use of this metadata</li></ul>The versions of FileCloud in which each built-in metadata set and its attributes became available are listed in the following table:
<table>
<tr><th>Built-in Metadata Set</th><th>FileCloud Version</th></tr>
<tr><td>Image</td><td>18.1</td></tr>
<tr><td>Document Life Cycles</td><td>18.1</td></tr>
<tr><td>Microsoft Office Tag</td><td>20.1</td></tr>
<tr><td>Color Tagging</td><td>20.3</td></tr>
</table>
</td>
<td><ul><li>Image metadata</li><li>Document Life Cycle metadata</li><li>Microsoft Office Tag metadata</li><li>Color Tag metadata</li><li>PDF Tag metadata</li><li>AIP Sensitivity Label metadata</li><li>Everfox CDR metadata</li><li>Signority eSignature metadata</li><li>ITAR metadata</li><li>CUI metadata</li></ul></td>
</tr>
</table>

| TYPE | DESCRIPTION | SETS AVAILABLE |
|---|---|---|
| | **Built-in Metadata Set** / **FileCloud Version**<br>PDF Tag / 21.2<br>AIP Sensitivity Label / 21.2<br>CDR / 23.241.4<br>Signority eSignature / 23.241.4<br>ITAR / 23.252<br>CUI / 23.252 | |

| TYPE | DESCRIPTION | SETS AVAILABLE |
|---|---|---|
| Custom Metatdata Set (see page 335) | 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 (see page 306)

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 (see page 338) page.

## More Information:

| FileCloud Blogs |
|---|
| • How to Best Utilize FileCloud's Metadata[35] |

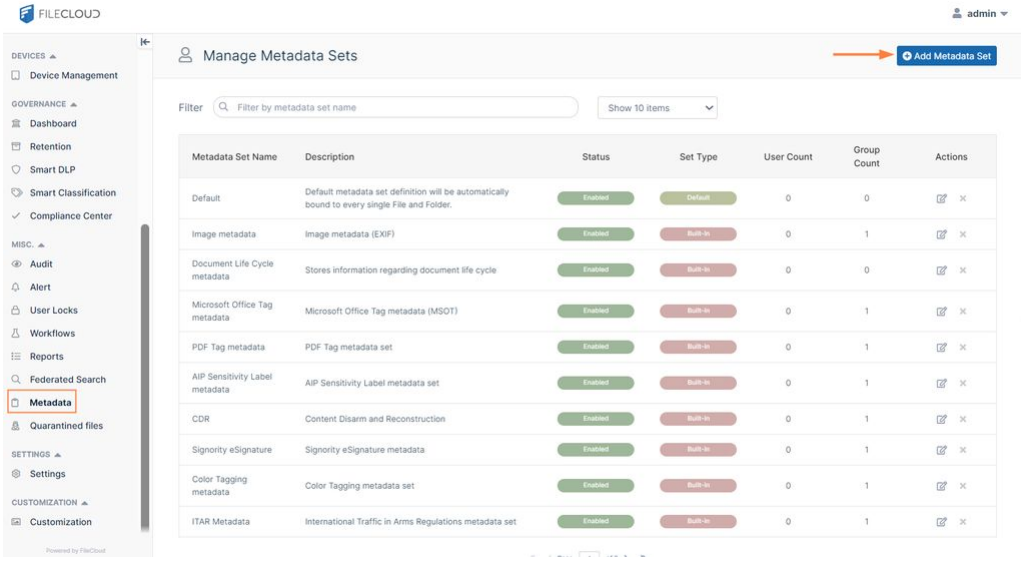
# Create a New Metadata Set

## Add a new metadata set definition

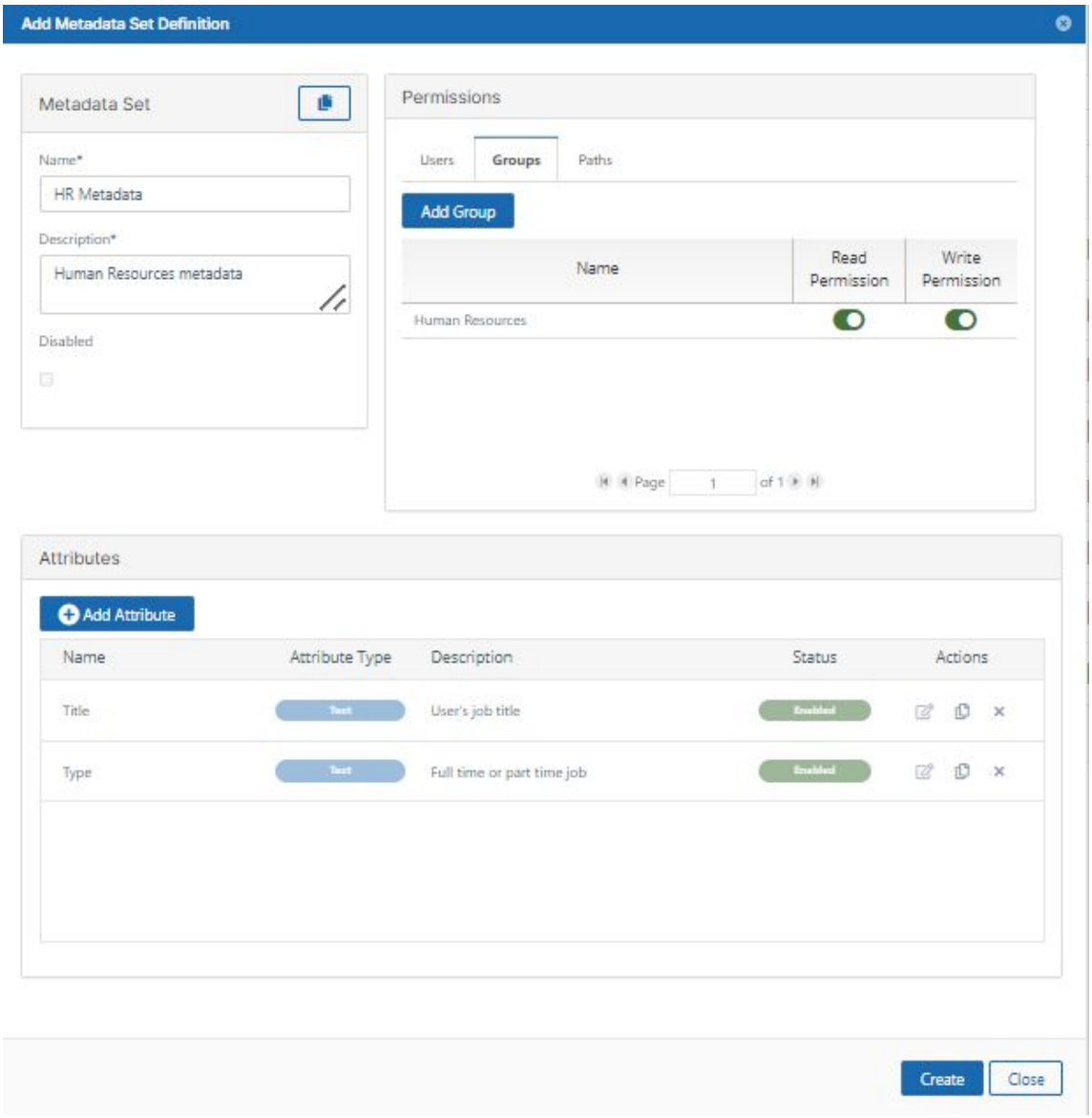
To add new metadata:

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

35. https://www.filecloud.com/blog/2021/03/how-to-best-utilize-fileclouds-metadata/#.YMzknWhKhIA

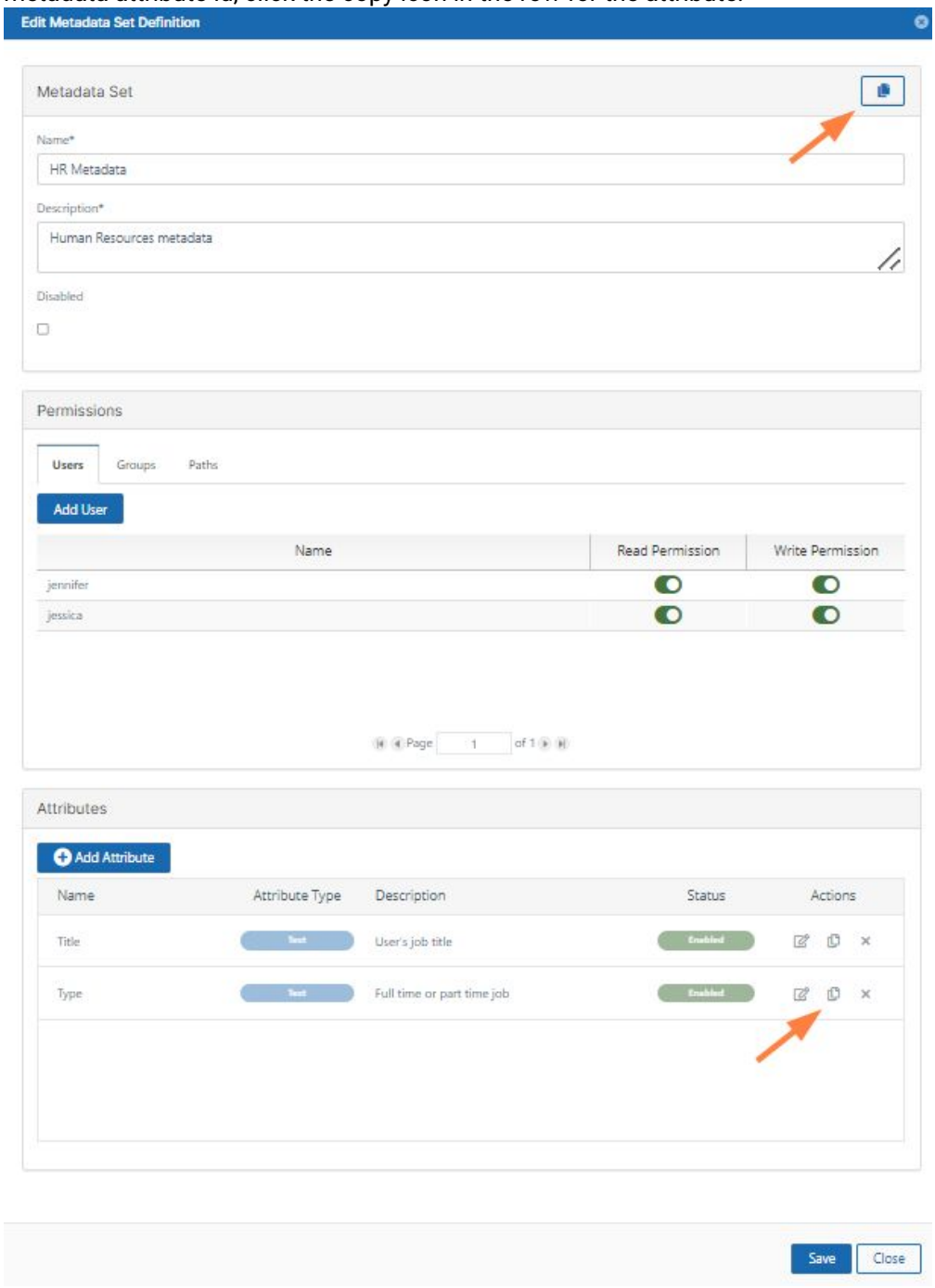



2. To open the **Add Metadata Set Definition** dialog box, click **Add Metadata Set**.




3. Enter **Name** and **Description** and check **Disabled** if you don't want the metadata set to be enabled when you save. it.
4. Add users or groups and specify permissions for them. Define FileCloud paths (locations) that have access to the metadata set. For more details, see Managing Metadata Permissions (see page 306).
5. Click **Add Attribute** and add at least one metadata attribute definition. For more details, see Managing Metadata Attributes (see page 305).
6. Click **Create**.

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



# Edit an Existing Metadata Set

### Propagating changes

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

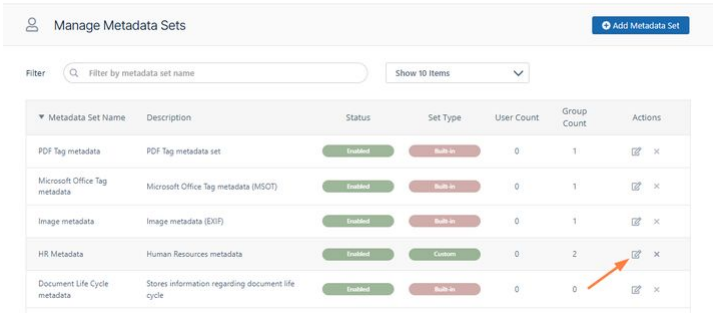
1. **New attribute is added** - attribute definition is added to each associated metadata_values document. Default value provided for this attribute is used.
2. **Existing attribute is changed** - attribute definitions is updated for each associated metadata_values document. **Existing values remain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

Notes:

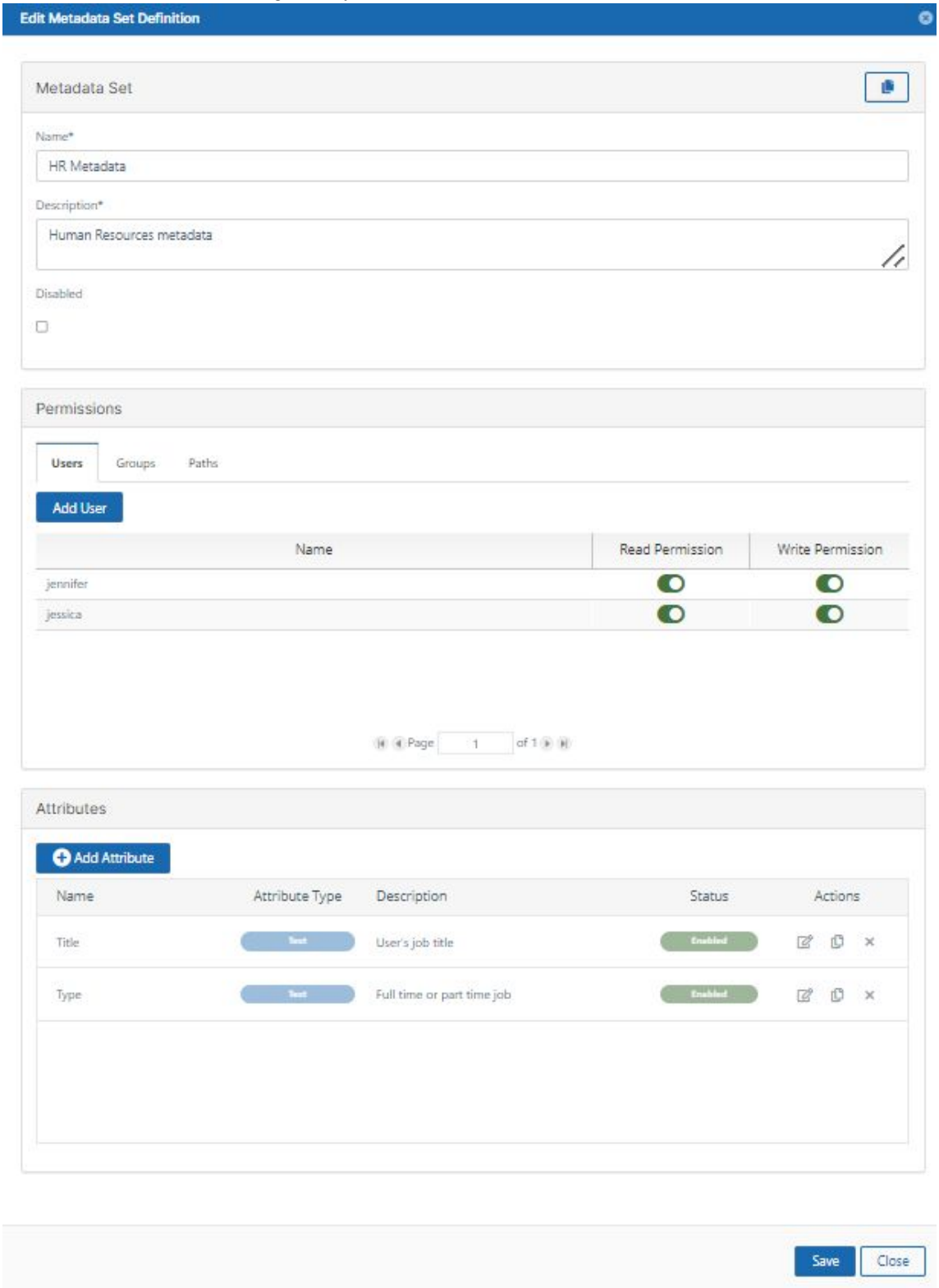
- The Default Metadata set is a special type and cannot be renamed.
- When an existing attribute is removed **all** associated values will be removed. This operation cannot be reverted.

**To edit an existing metadata set:**

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



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




4. Edit properties, permissions (see page 306) and attributes (see page 305).

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 (see page 306).

⚠ 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 (see page 309).

**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.

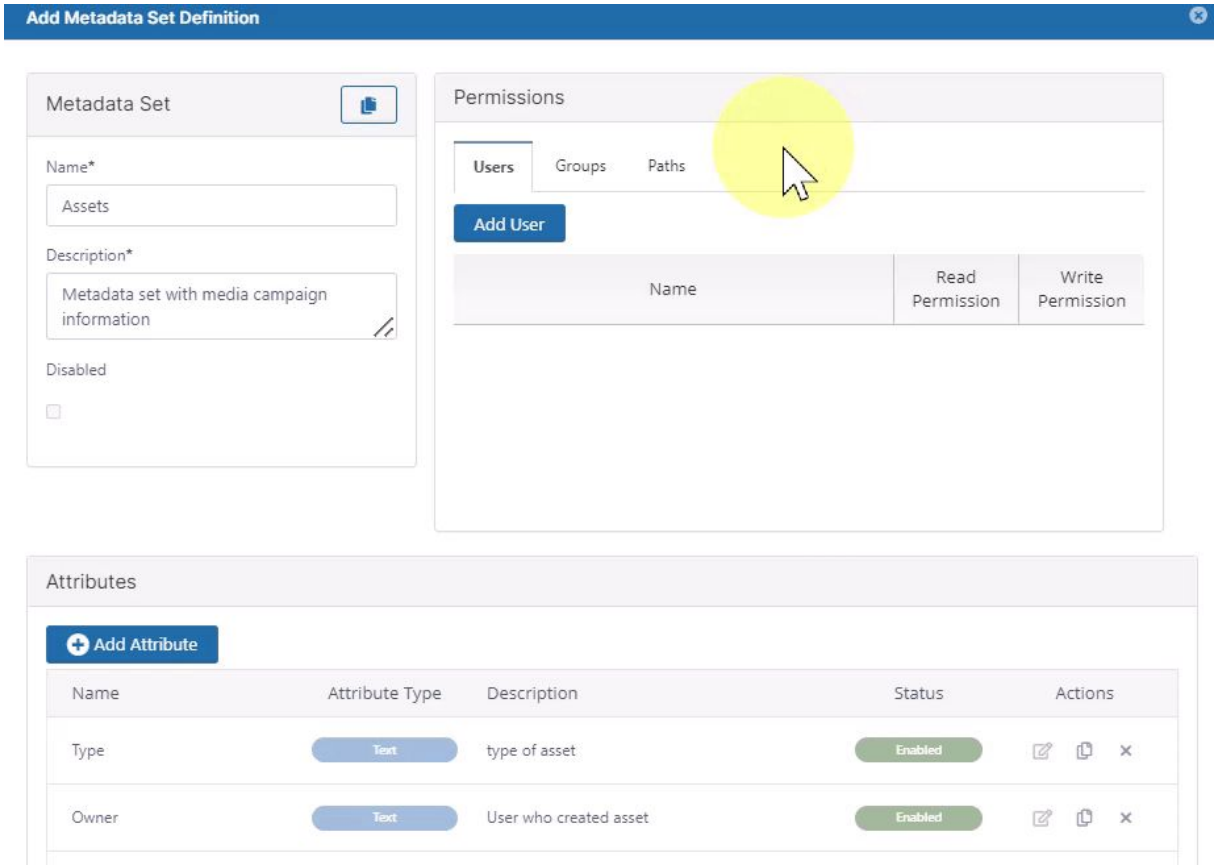
- By default all paths are allowed.
- When an administrator wants to provide a specific set of allowed paths:
  - the "Allow Selected Paths" option has to be selected and
  - all allowed paths have to be specified via the Add Allowed Path dialog.
- When the path is added it will be displayed on the list.
- 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 (see page 309).

## Video of Allowing Paths for Metadata Permissions

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



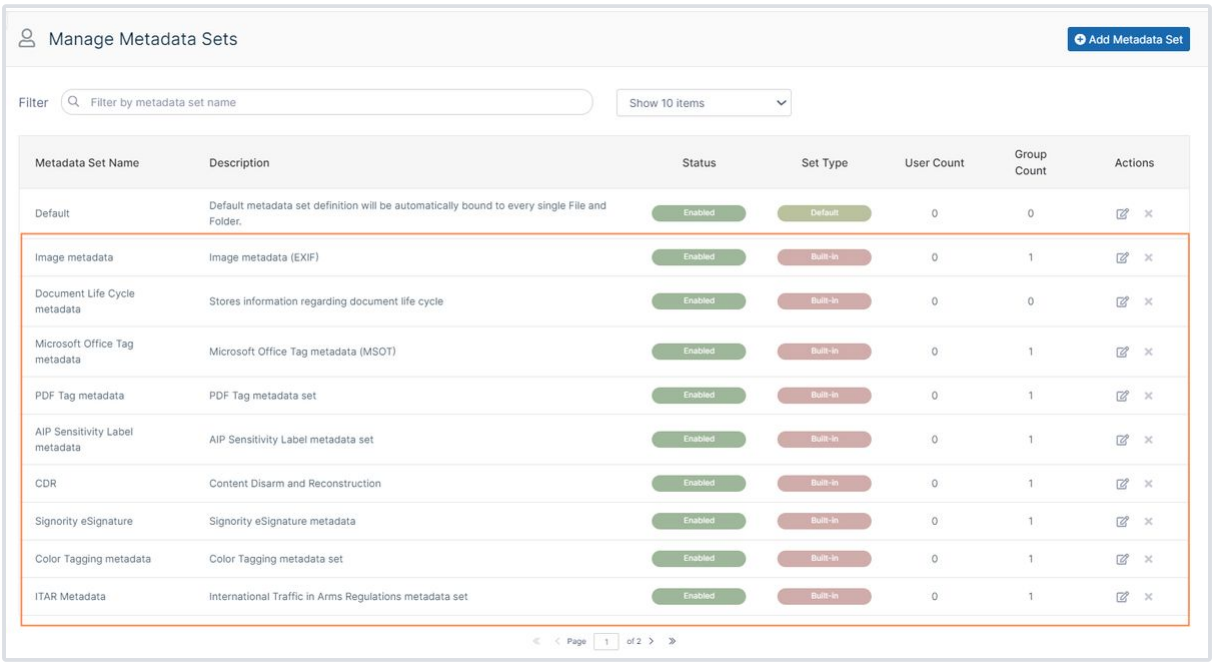

## Video of Granting a User Metadata Permissions

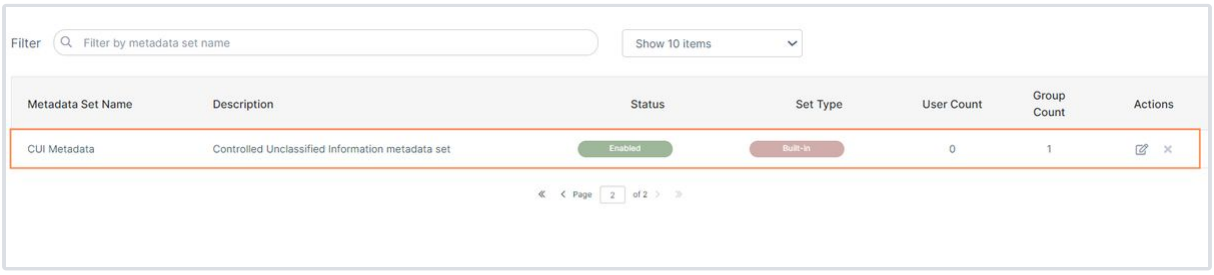
When you add a user to a metadata set, you can choose whether the user has write permission. If you remove read permission, the user is removed from the list.

Wor
king
with

## Built-In Metadata

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



⚠ Unlike the **Default** metadata set:

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

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

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

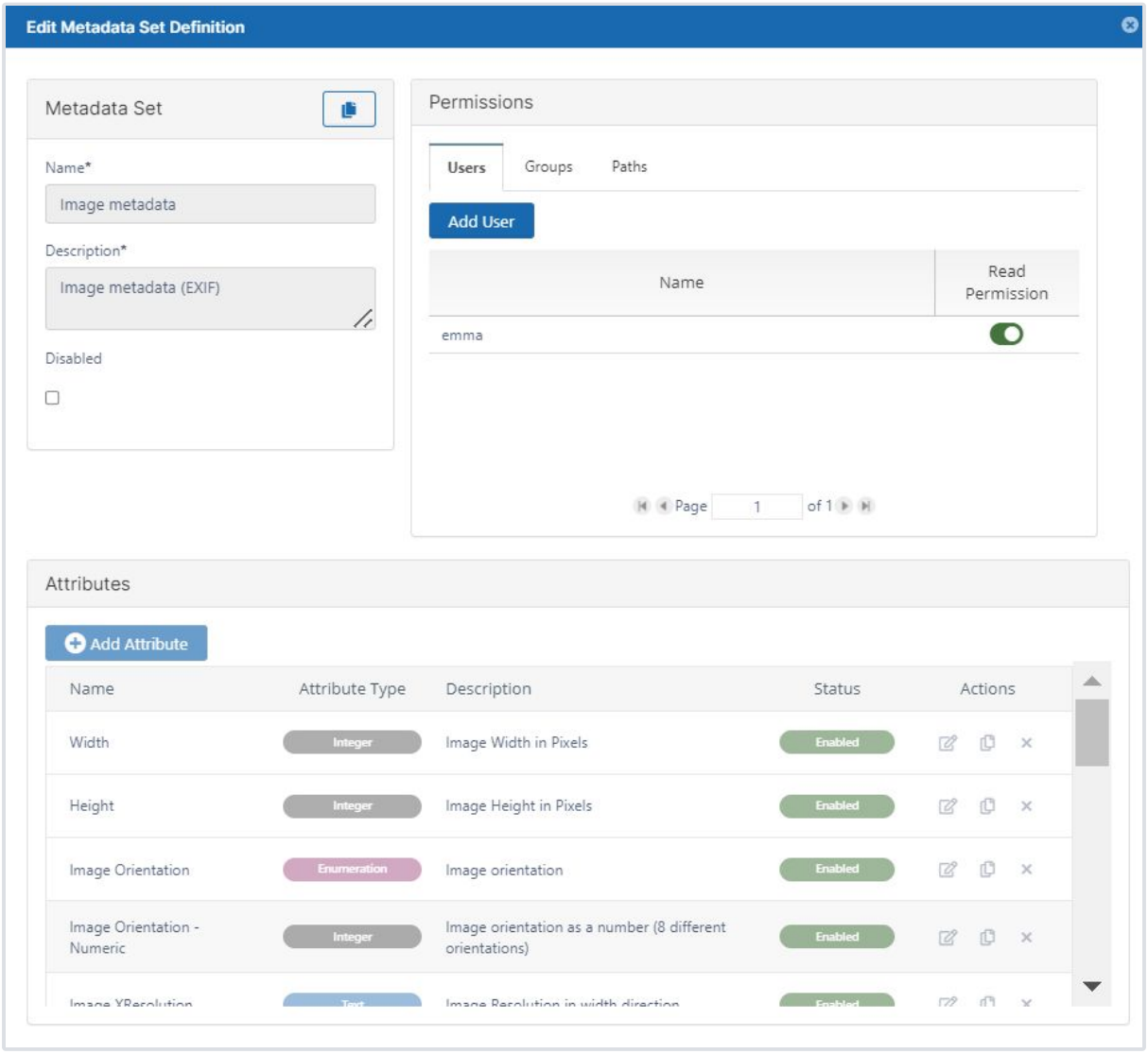
⚠ The **Color Tagging** metadata set differs from the other built-in metadata sets because its Tag attribute can be edited (but not deleted).
The attributes of all other built-in metadata sets cannot be edited or deleted.

The sets that have been created for you include:

**Image Metadata**

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

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



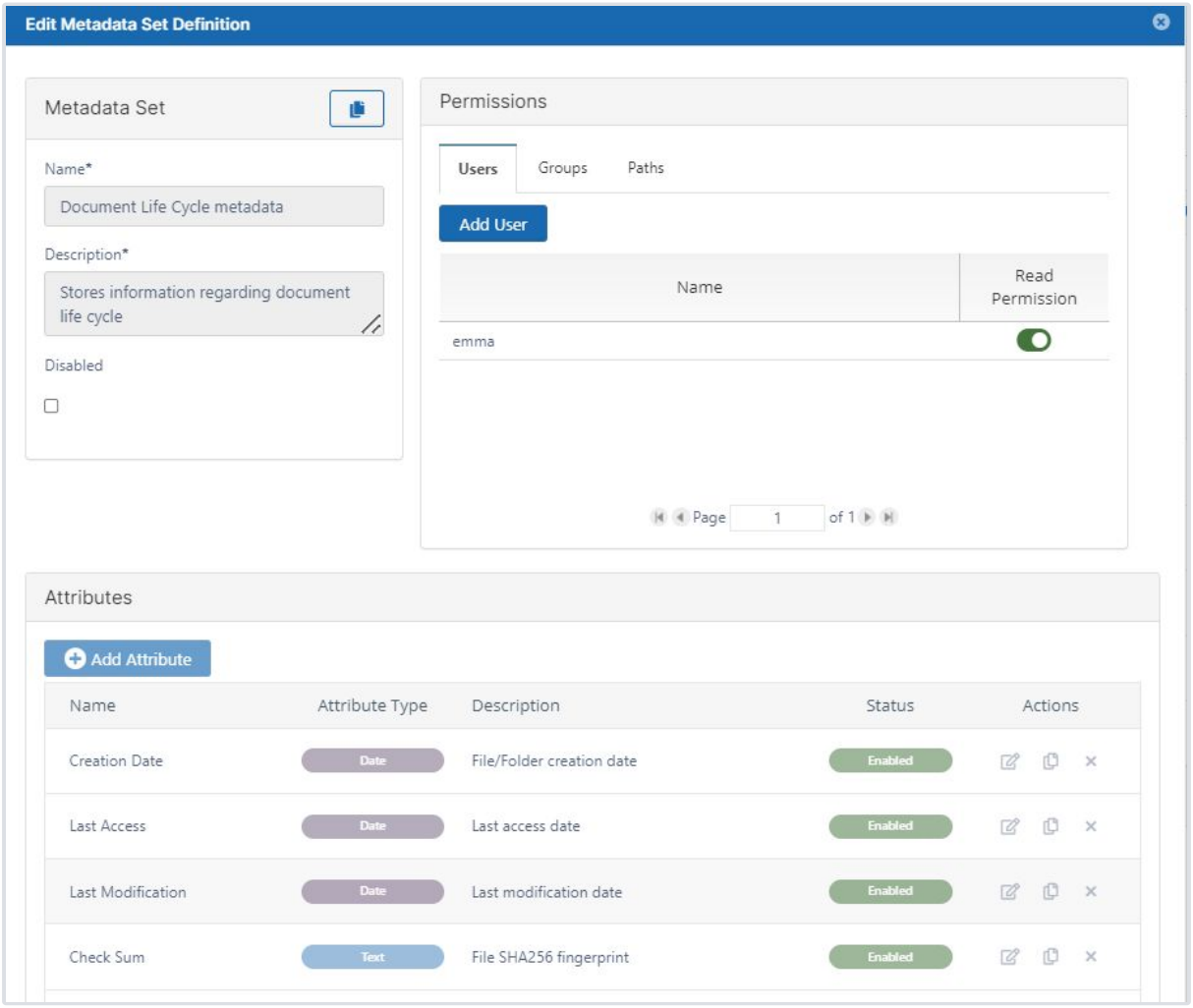

The following attributes exist in the **Image** built-in metadata set:

| | **Description** | **Options** |
|---|---|---|
| Name | Title for the metadata set: Image metadata | • Required<br>• This cannot be changed |

| | Description | Options |
|---|---|---|
| Description | By default, says: Image metadata (Exif) | • Required<br>• This cannot be changed |
| Disabled | Stops the metadata set from being automatically bound to every new file and folder. | • Not selected<br>• This cannot be changed |
| User Permissions | Grant access to specific users to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read |
| Group Permissions | Grant access to specific groups to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read |
| Path Permissions | File Objects in this location will have the metadata set applied | • Not available<br>• This cannot be changed |
| Attributes | A number of tags that are built-in for image files | • Width: Image width in pixels<br>• Height: Image Height in pixels<br>• Image Orientation<br>• Image Orientation - Numeric: orientation as a number<br>• Image XResolution: width direction<br>• Image YResolution: height direction<br>• Unit of Resolution |

### Document Life Cycle Metadata

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




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

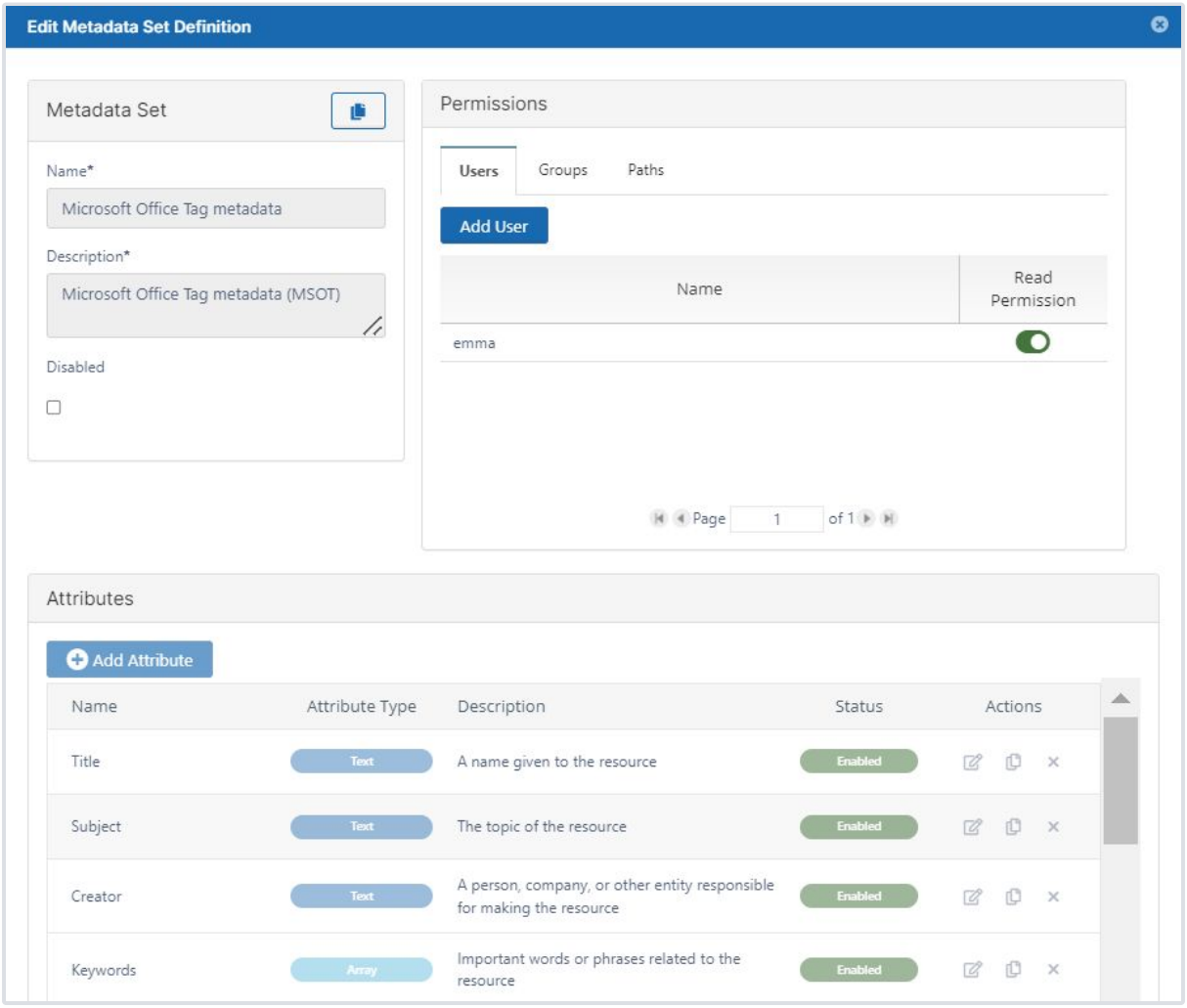
| | **Description** | **Options** |
|---|---|---|
| Name | Title for the metadata set: Document Life Cycle Metadata | • Required<br>• This cannot be changed |
| Description | By default, says:<br>Stores information regarding document life cycle | • Required<br>• This cannot be changed |
| Disabled |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

| | Description | Options |
|---|---|---|
| User Permissions | Grant access to specific users to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read |
| Group Permissions | Grant access to specific groups to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read |
| Path Permissions | File Objects in this location will have the metadata set applied | • Not available<br>• This cannot be changed |
| Attributes | A number of custom values (tags) extracted from the file.<br>One of these attributes is a SHA256 Fingerprint (file checksum).<br>• This is a unique text string generated by the SHA-1 hash algorithm.<br>• It is a standard for the implementation of a secure hash algorithm.<br>• It is a one-way cryptographic function that can be used to act as a 'signature' of a sequence of bytes.<br>• It is very unlikely that 2 different byte sequences would produce the same value (though not impossible) | • Creation Date<br>• Last Access<br>• Last Modification<br>• Check Sum: File SHA256 Fingerprint |

### Microsoft Ofiice Tag metadata

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

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

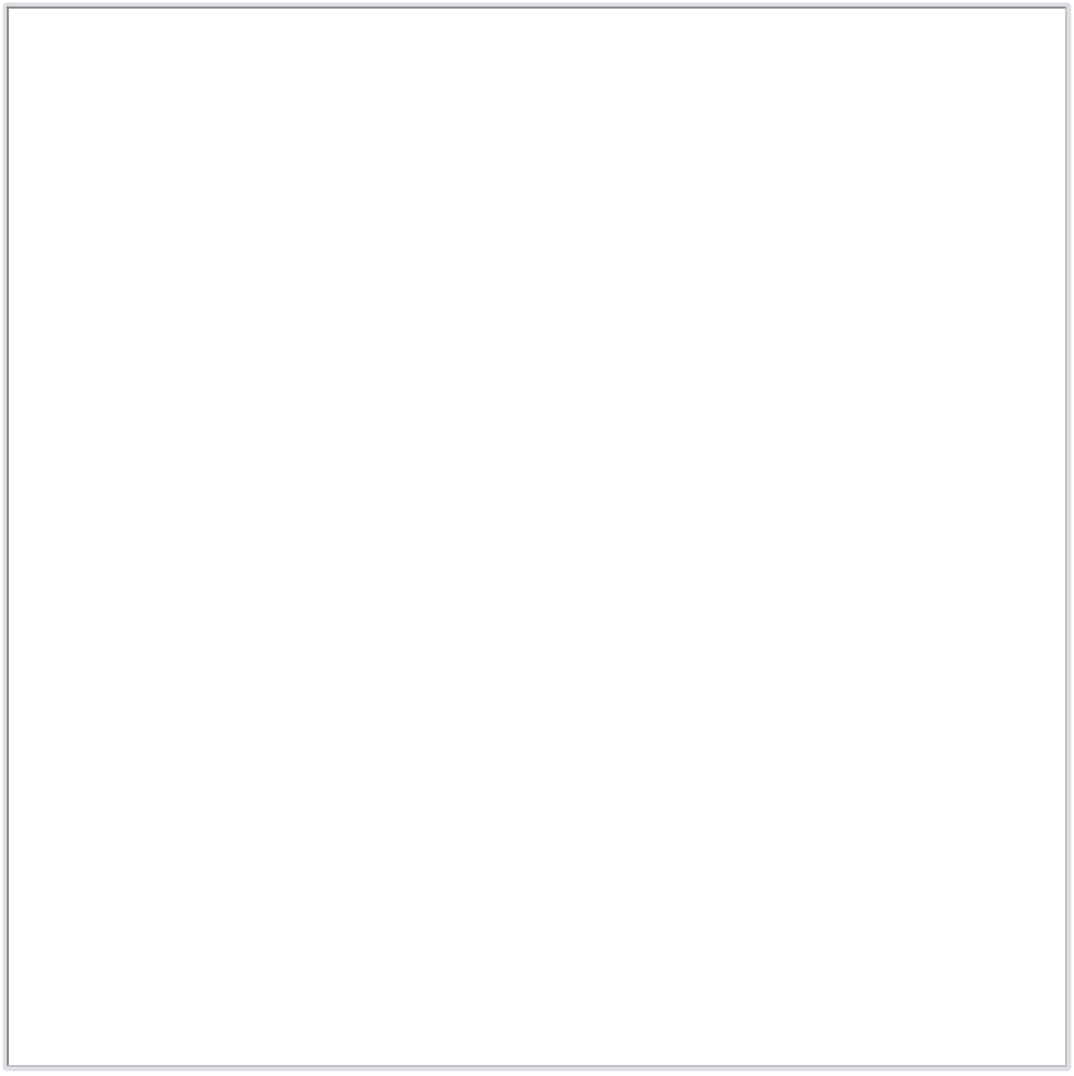



The following attributes are included in FileCloud's **Microsoft Office Tag** metadata set:

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

| | Description | Options |
|---|---|---|
| Keywords | Keyword tags assigned to file. | • Not required<br>• Read (can only be changed in Microsoft Office file before uploading) |
| Description | Description of file. | • Not required<br>• Read (can only be changed in Microsoft Office file before uploading) |
| Last Modified By | Last user who modified file. | • Not required<br>• Read (can only be changed in Microsoft Office file before uploading) |
| Created | Date file was created. | • Not required<br>• Read (can only be changed in Microsoft Office file before uploading) |
| Modified | Date file was last modified. | • Not required<br>• Read (can only be changed in Microsoft Office file before uploading) |
| Category | Category of file. | • Not required<br>• 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<br>• Read (can only be changed in Microsoft Office file before uploading)<br>***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.*** |

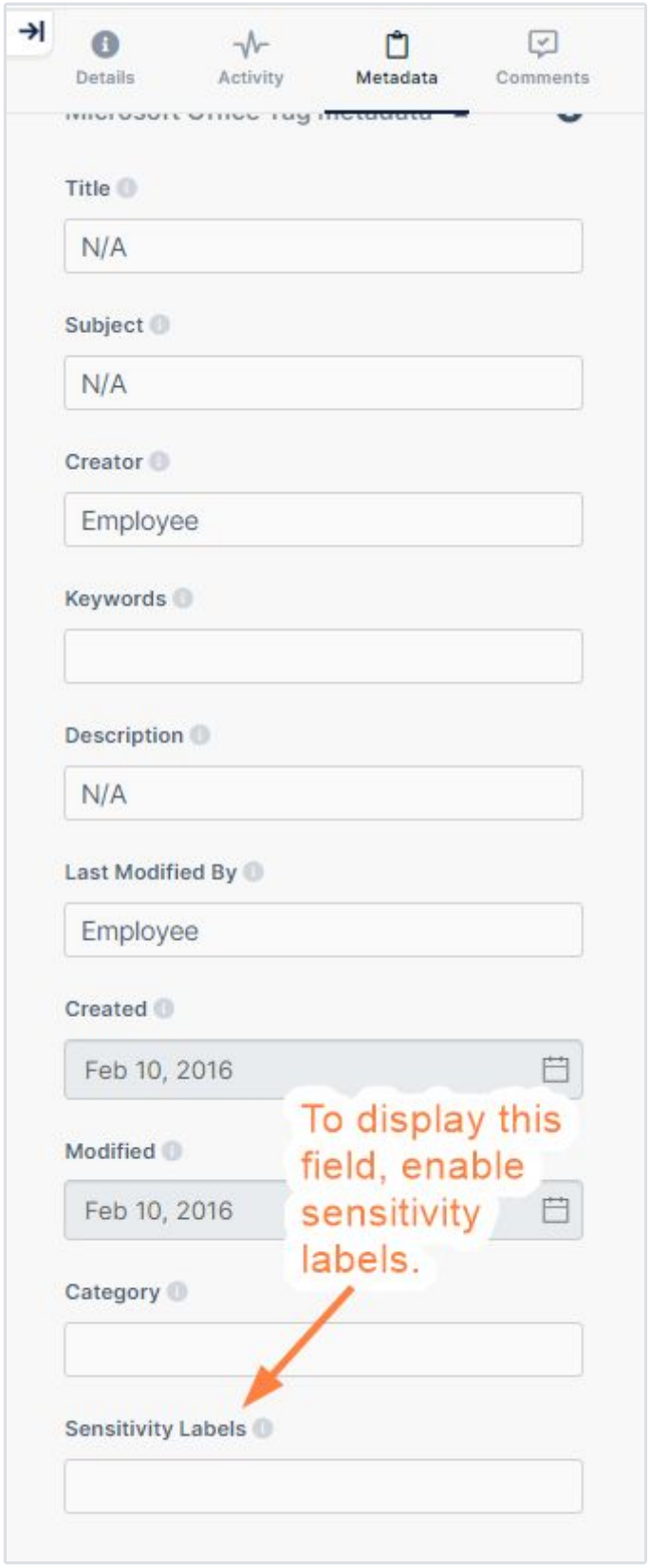
**MSOT Sensitivity Labels**
By default, FileCloud does not capture MSOT sensitivity label data even if sensitivity labels are enabled in Office.
Prior to FileCloud 21.2, enabling the Sensitivity Label field was the only way to extract sensitivity label data. In FileCloud 21.2, AIP Sensitivity Label metadata, 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.

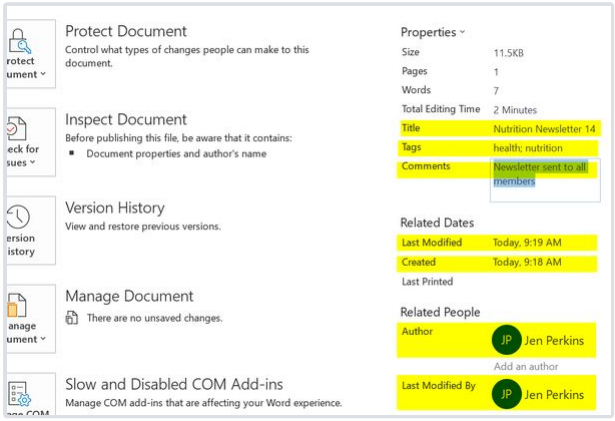
1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the following :

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

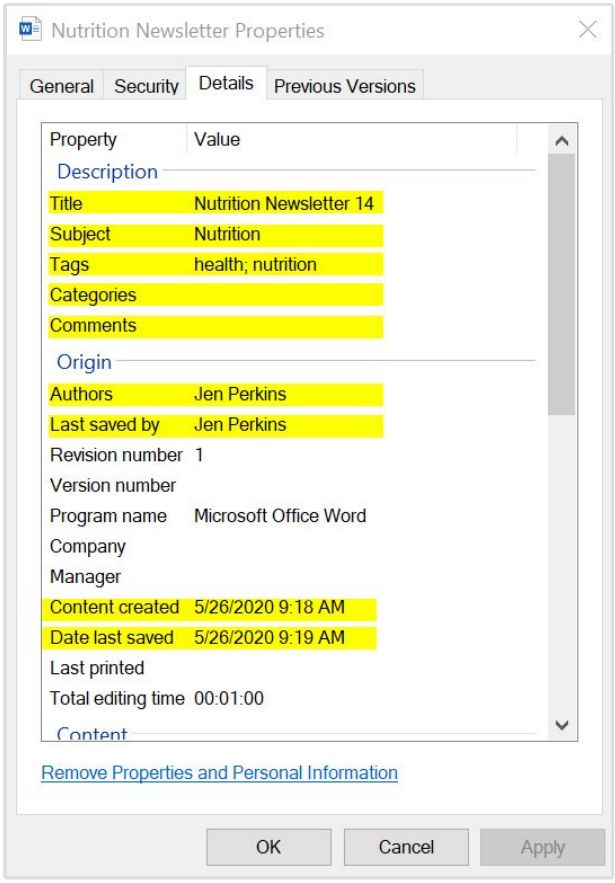

Details
Activity
Metadata
Comments
Title
N/A
Subject
N/A
Creator
Employee
Keywords
Description
N/A
Last Modified By
Employee
Created
Feb 10, 2016
Modified
Feb 10, 2016
To display this field, enable sensitivity labels.
Category
Sensitivity Labels

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:

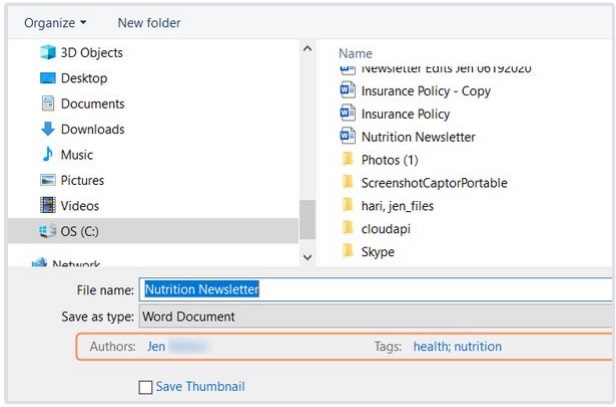



When you right-click an Office document in file explorer and select Properties > Details tab:



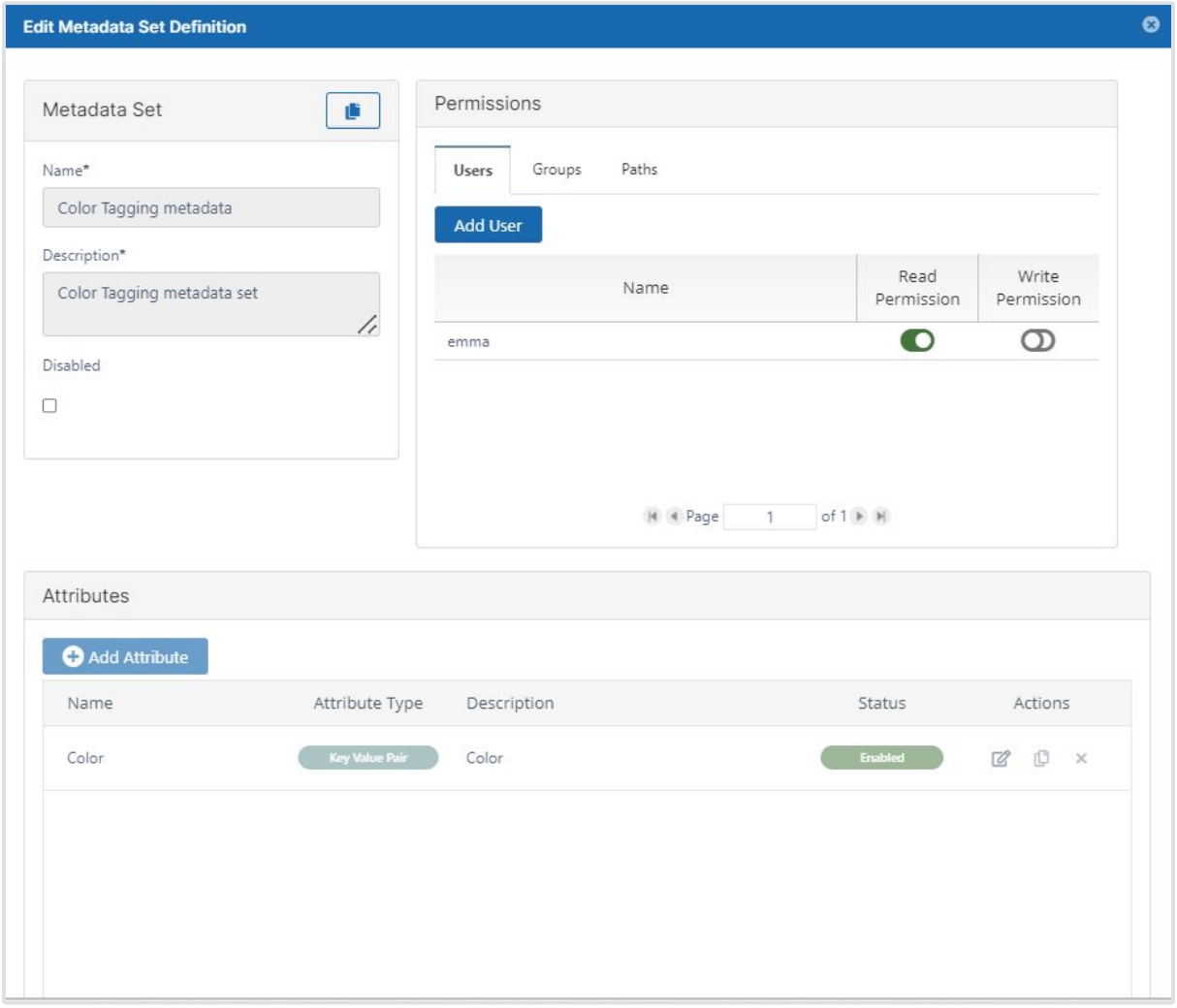

Or when you save an Office document:

| 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.



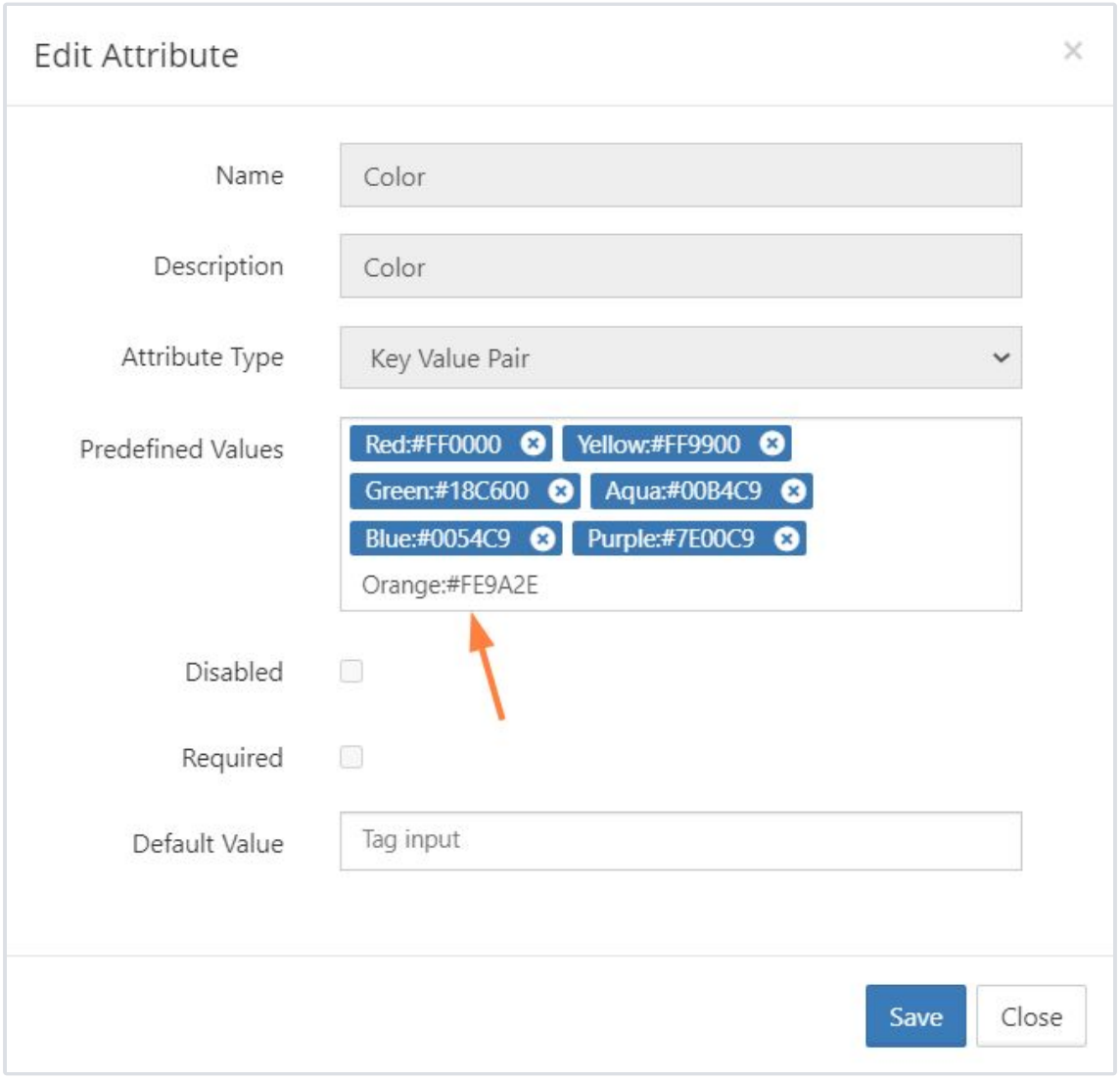
Color is the only attribute included in the **Color Tagging** metadata set.

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

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

To add values to the Color attribute:

1. To open the **Edit Metadata Set Definition** dialog box, click the Edit button for Color Tagging metadata.
2. Under **Attributes**, click the Edit button for **Color**.
   The **Edit Attribute** dialog box opens.
3. Click in the **Predefined Values** box, and type the name of a color followed by **:#** and then the hexadecimal color code.



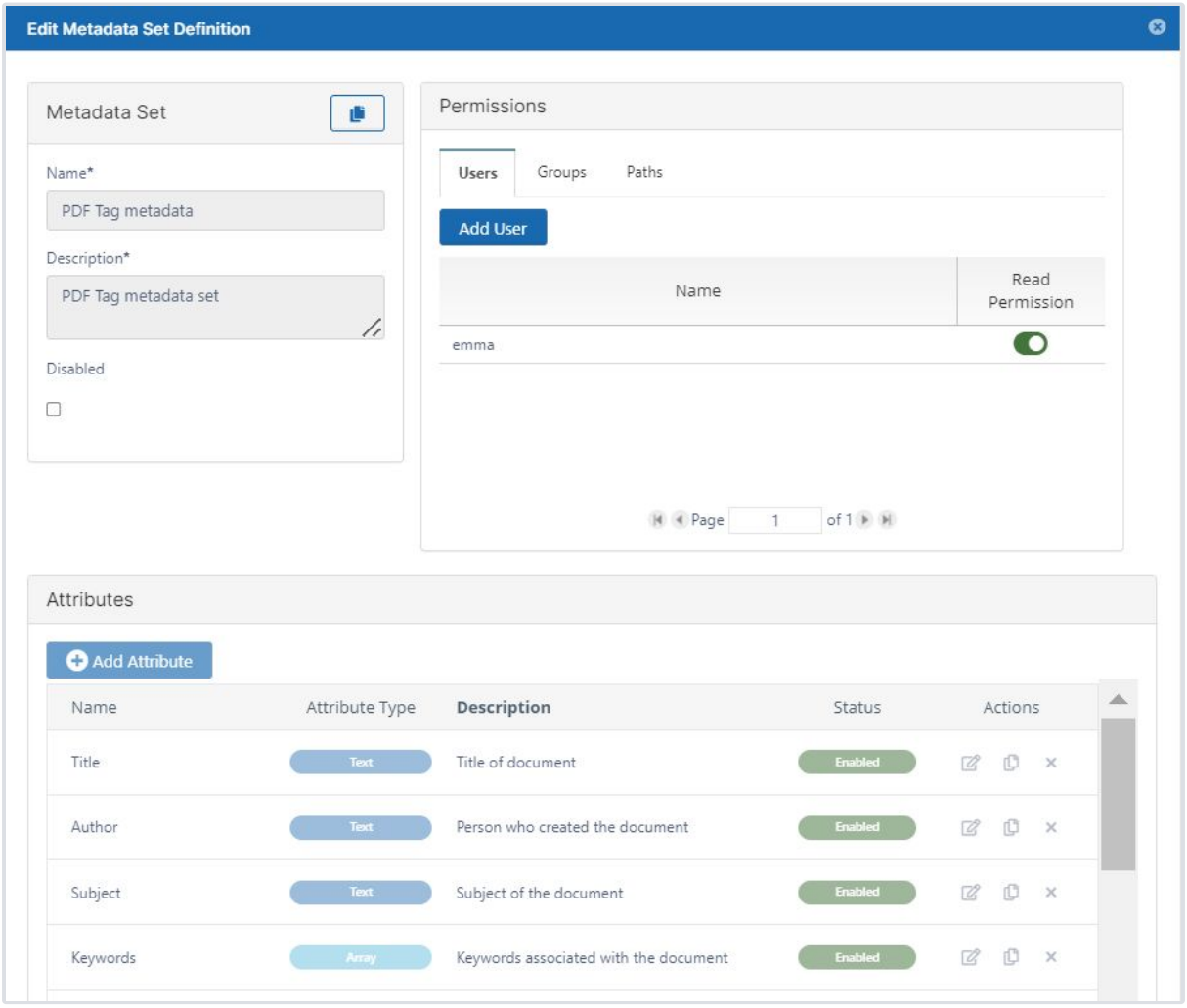

4. Click Enter.
   The color is saved and formatted with white letters on a blue background.
5. Add any number of custom colors and click **Save**.
   The colors now appear as options to users when they apply color tags to files or folders.

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

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

**PDF Tag metadata**

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




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

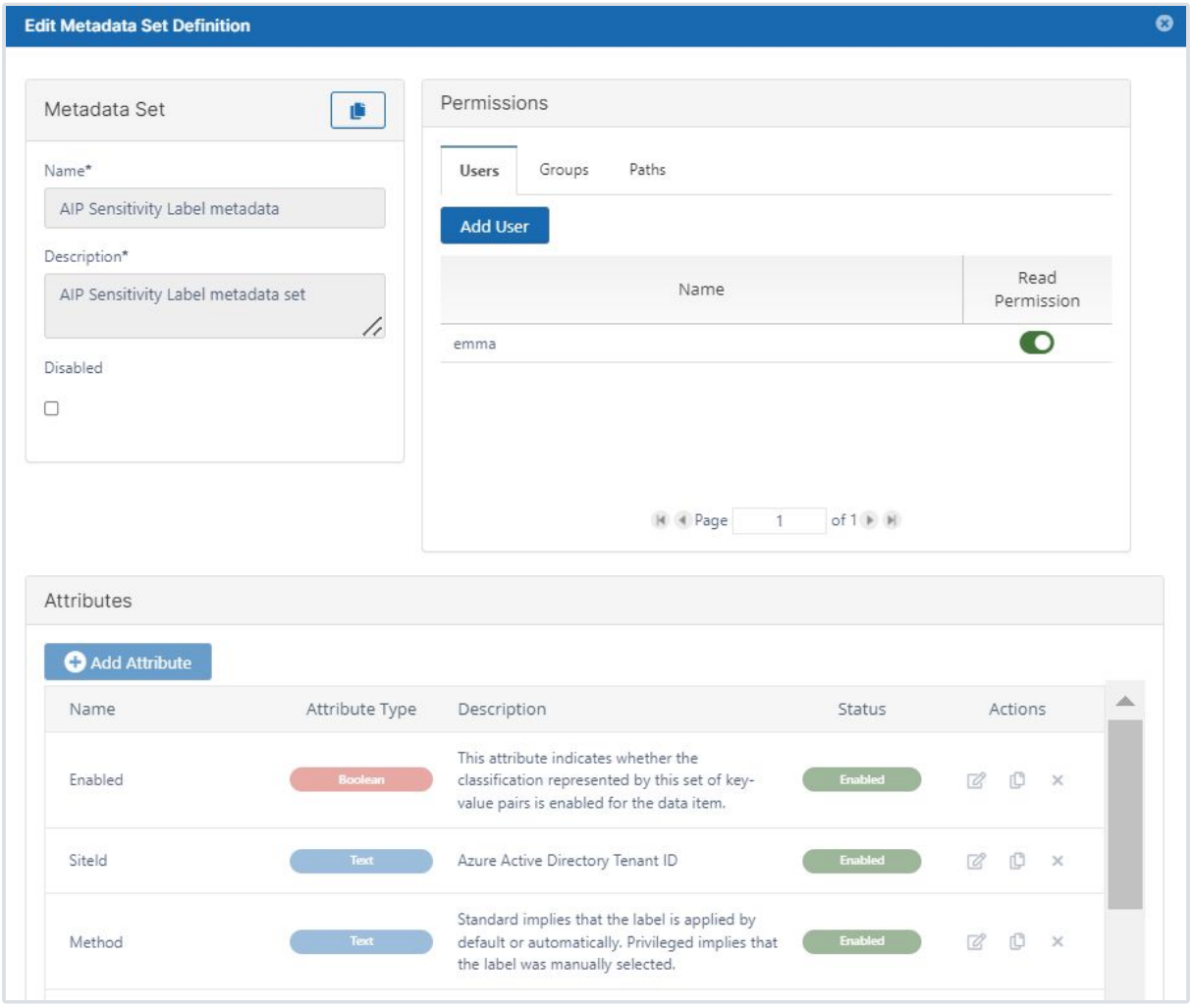
| | **Description** | **Options** |
|---|---|---|
| Title | Title of document. | Read only |
| Author | Author of document | Read only |
| Subject | Subject of document. | Read only |
| Keywords | Keywords associated with document. | Read only |
| Creator | Application used to create file before it was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

| | | |
|---|---|---|
| Created | Date created. | Read only |
| Modified | Date last modified. | Read only |

### AIP Sensitivity Label metadata

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

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



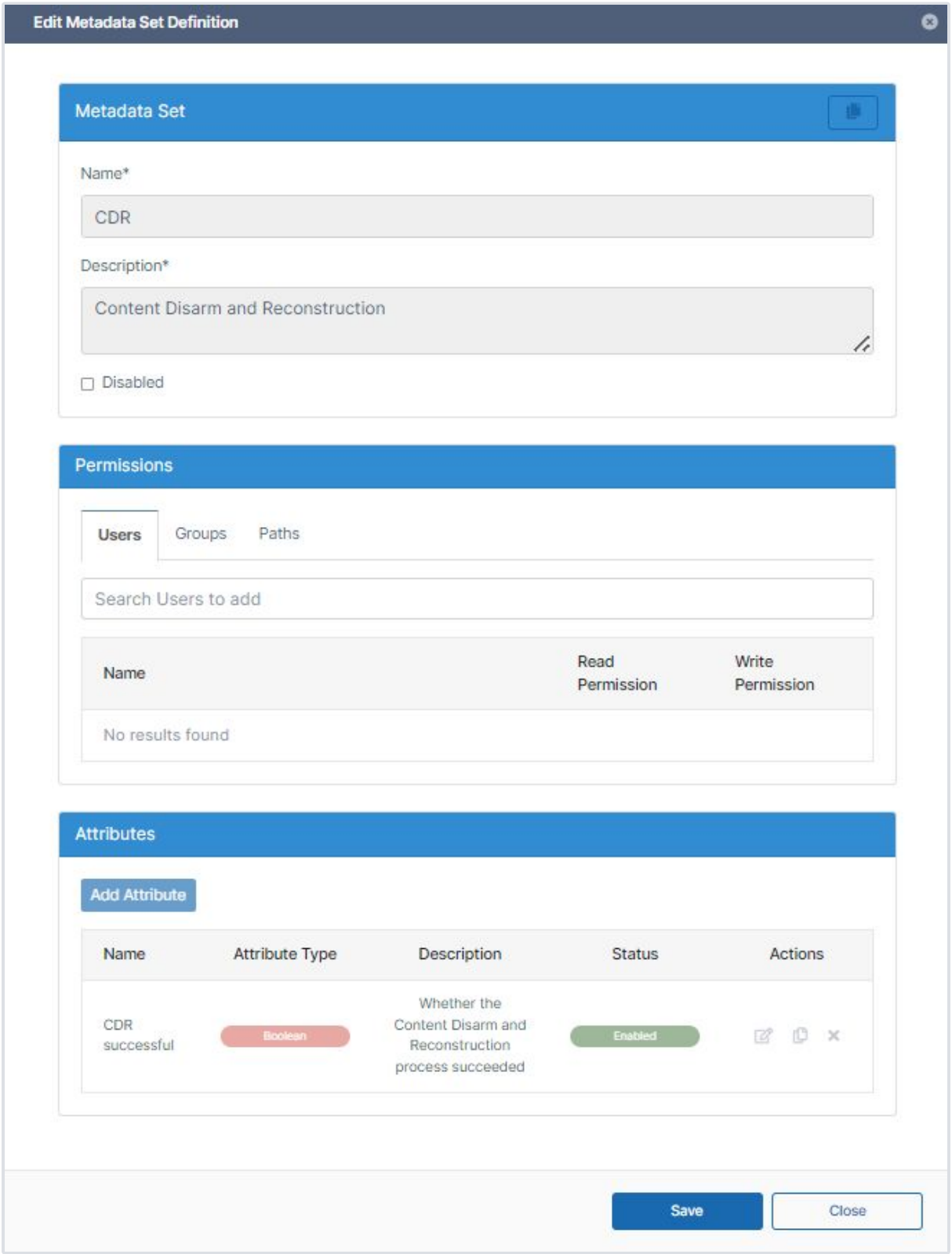

The following attributes are included in FileCloud's **AIP Sensitivity Label** metadata set:

| | Description | Options |
|---|---|---|
| Enabled | Whether the sensitivity label is enabled for this item. | Read only |
| SiteID | Azure Active Directory tenant ID. | Read only |
| Method | Indicates whether label was applied by default/automatically or if the label was applied manually.<br>Value may be:<br>**Standard** - Label was applied by default or automatically.<br>**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.<br>See https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-markings for more information. | Read only |

### CDR metadata

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

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



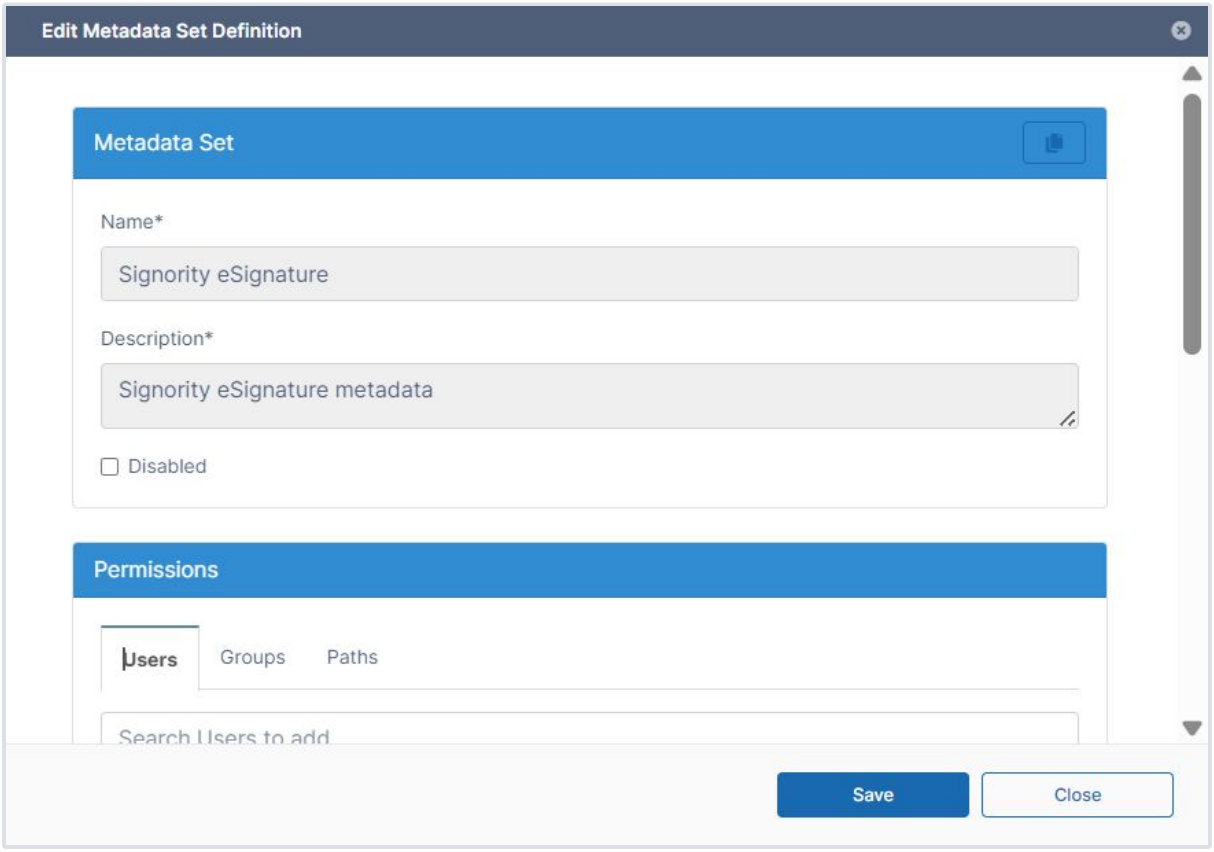

The following attribute is included in FileCloud's **CDR** metadata set:

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

### Signority eSignature metadata

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

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




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

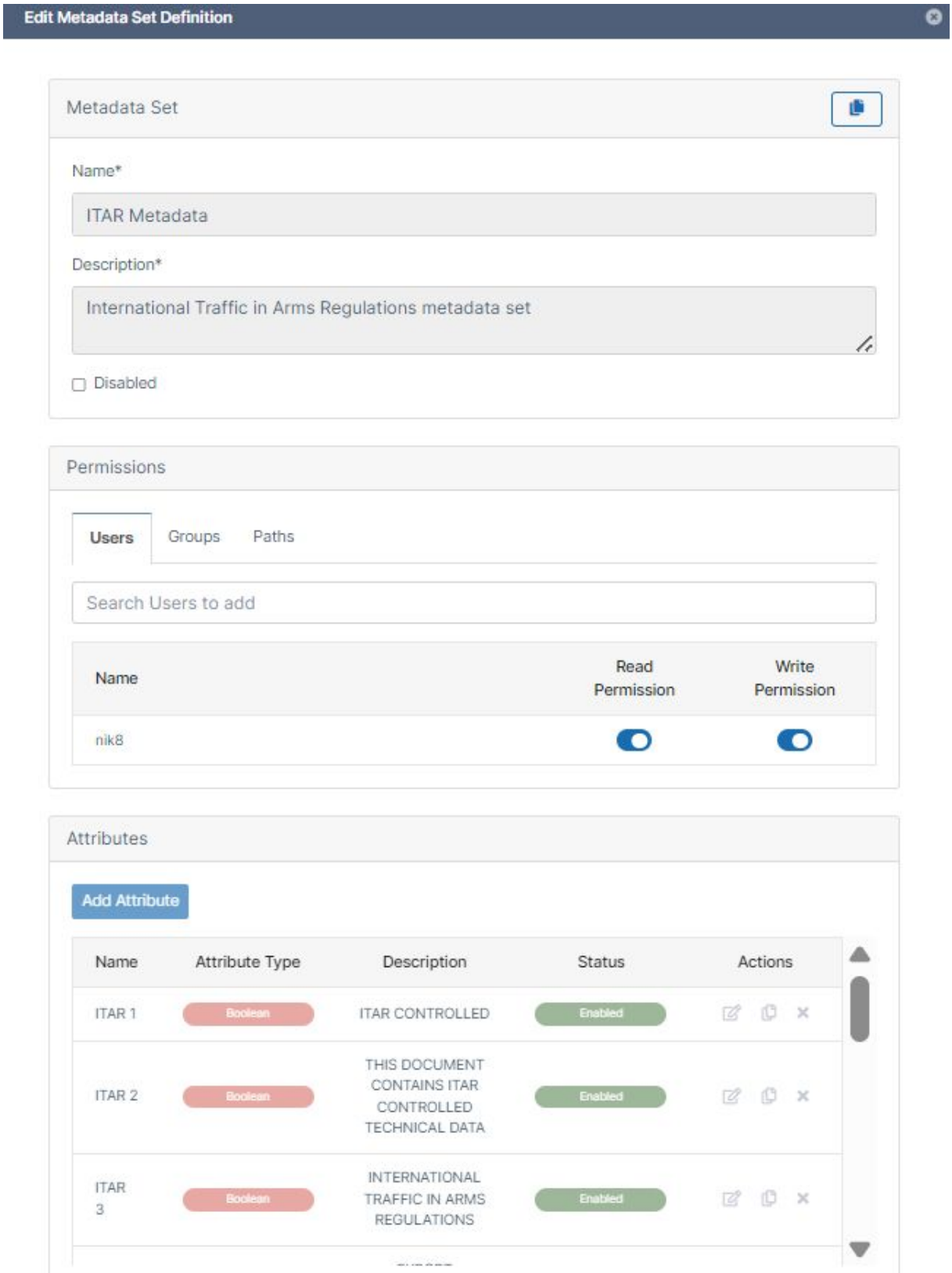
| | Description | Options |
|---|---|---|
| Completion Date | Date signing was completed. | Read only |
| Total Signers | Total number of people who received signing requests. | Read only |

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

### ITAR metadata

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

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




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

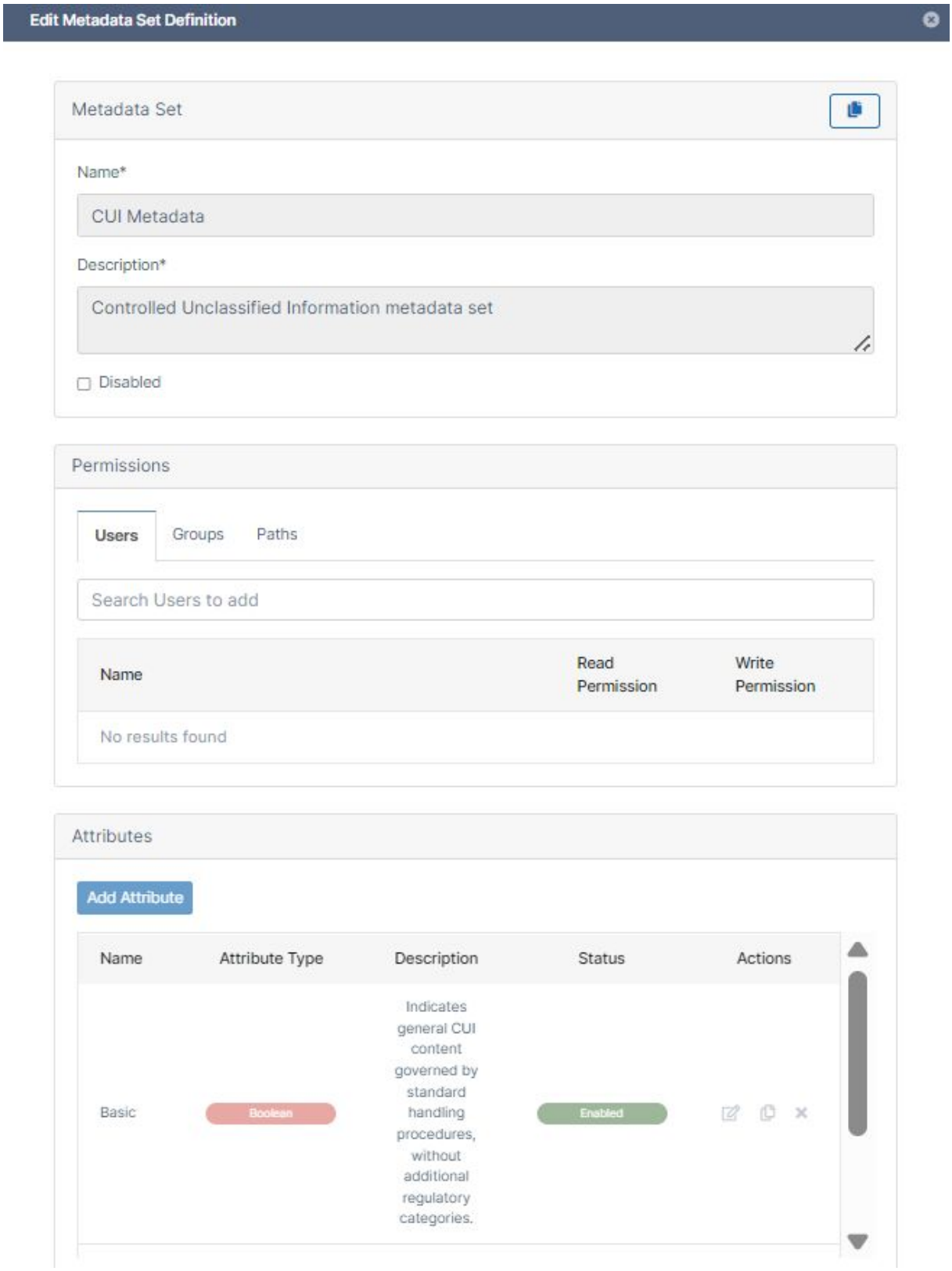
Note that the descriptions are phrases that commonly appear in ITAR documents. If other phrases are used in your ITAR documents, search for those phrases.

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

**CUI metadata**

Note: CUI metadata was added in FileCloud Version 23.252

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




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

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

# 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 (see page 299)

Manage Metadata Permissions (see page 306)

Edit an existing Set Definition (see page 303)

### Delete a Set Definition

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

⚠ You cannot undo or revert deletions.

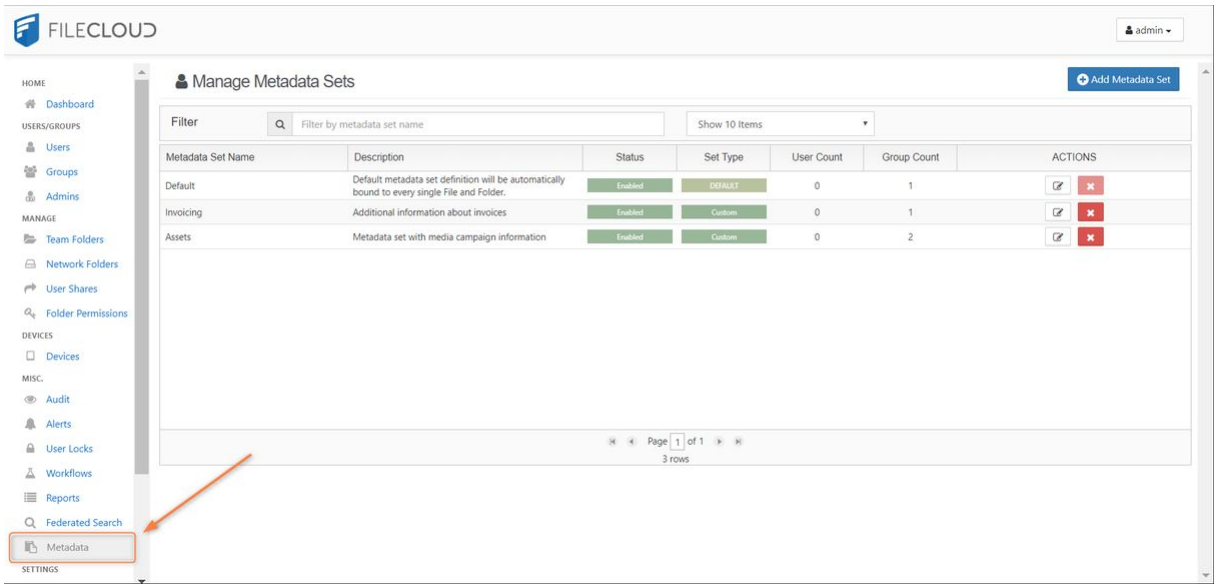
To delete an existing Custom metadata set definition:

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

### View the Set Definition List

The metadata set definitions screen displays the list of defined metadata sets.

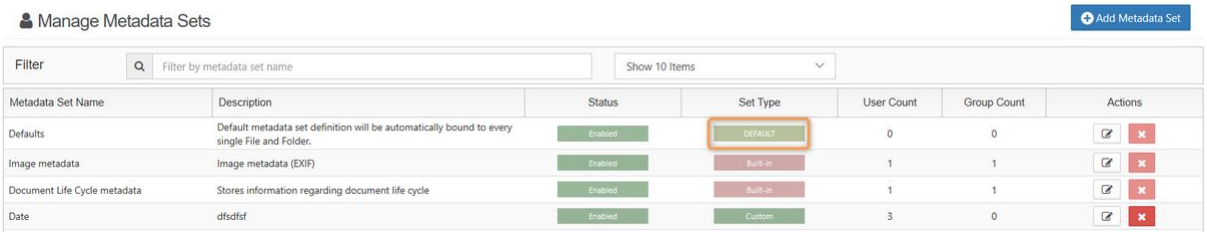
- The filter text box can be used to filter the metadata sets based on the metadata name.
- The individual metadata set on the metadata list can be viewed, edited and deleted.
- New metadata sets can be added by clicking the Add Metadata Set button and filling in the metadata set definition form.



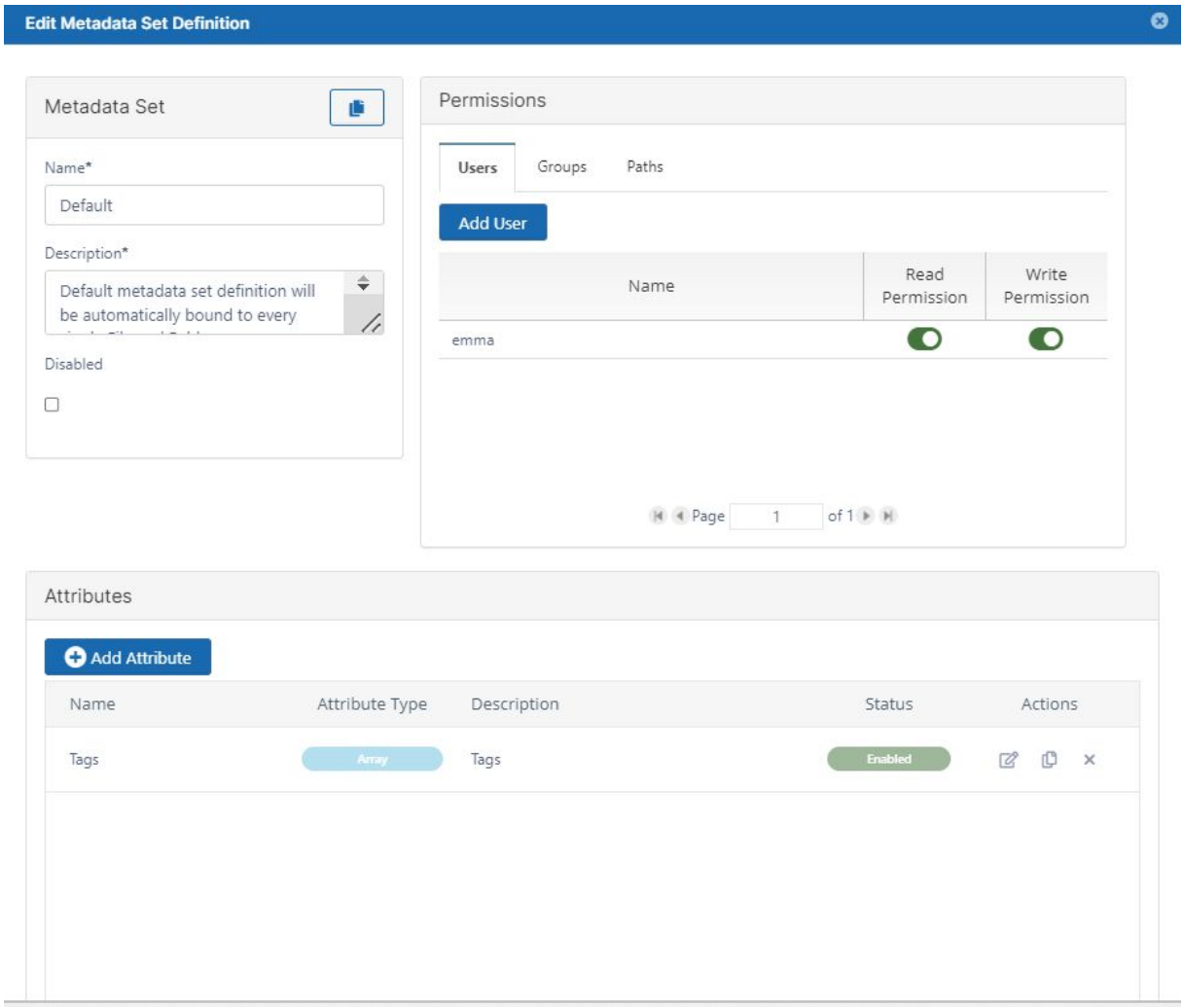

# Working with Default Metadata

**Default** is a special metadata set that is automatically associated with every File Object when it is created, copied, uploaded, etc.

- For already existing File Objects it will be associated when the file or folder is accessed for the first time.
- Exactly one Default Set exists in FileCloud - it cannot be deleted, but administrators can customize attributes and permissions or disable it.
- Out of the box it is shipped with a single predefined attribute of Array type - Tags.




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




| | Description | Options |
|---|---|---|
| Name | Title for the metadata set. | • Required<br>• This can be changed<br>• Validated on Creation |
| Description | By default, says:<br>Default metadata set definition will be automatically bound to every single File and Folder. | • Required<br>• This can be changed<br>• Validated on Creation |
| Disabled | Stops the metadata set from being automatically bound to every new file and folder. | • By default this is not selected<br>• You can choose to disable this set |

| | Description | Options |
|---|---|---|
| User Permissions | Grant access to specific users to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>• Write: this permission allows the user to add, edit, copy, or paste a value<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read<br>• Write |
| Group Permissions | Grant access to specific groups to:<br>• Read: this permission displays the metadata to the user in the User Portal<br>• Write: this permission allows the user to add, edit, copy, or paste a value<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required<br>• Read<br>• Write |
| Path Permissions | File Objects in this location will have the metadata set applied<br>For more information, read Managing Metadata Permissions (see page 306) | • Not Required |
| Array | A number of custom values (tags) provided by the administrator | • Name<br>• Description<br>• Disabled<br>• Required<br>• Tag Input |

How To Edit a Metadata Set (see page 303)

# Troubleshooting Metadata

## Allowed Memory Size Exhausted

An error message similar to the following indicates that while uploading a large file, the system could not extract metadata because it required more memory than the allowed PHP memory limit:

**019-04-05 5:27:29 - ERROR : CLFC-00004 ERROR | 2019-04-05 05:27:29 | 1 | Allowed memory size of 524288000 bytes exhausted (tried to allocate 316675836 bytes)**

Starting with FileCloud Version 20.1, the setting TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB in cloudconfig.php file enables you to override the maximum file size for automatic metadata extraction to take place.

By default, the value of the setting is:

- 500MB for local storage
- 100MB for Azure / S3

For example, if the value of the setting is 500, when files over 500 MB are uploaded, metadata extraction will not occur.

**Change the maximum file size for metadata extraction:**

1. Open cloudconfig.php at
   - Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Find the following:

```
define("TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB",500);
```

3. Change the value of the setting.
   For example:

```
define("TONIDOCLOUD_MAX_METADATA_EXTRACTION_FILE_SIZE_MB",128);
```

# Finding files without metadata

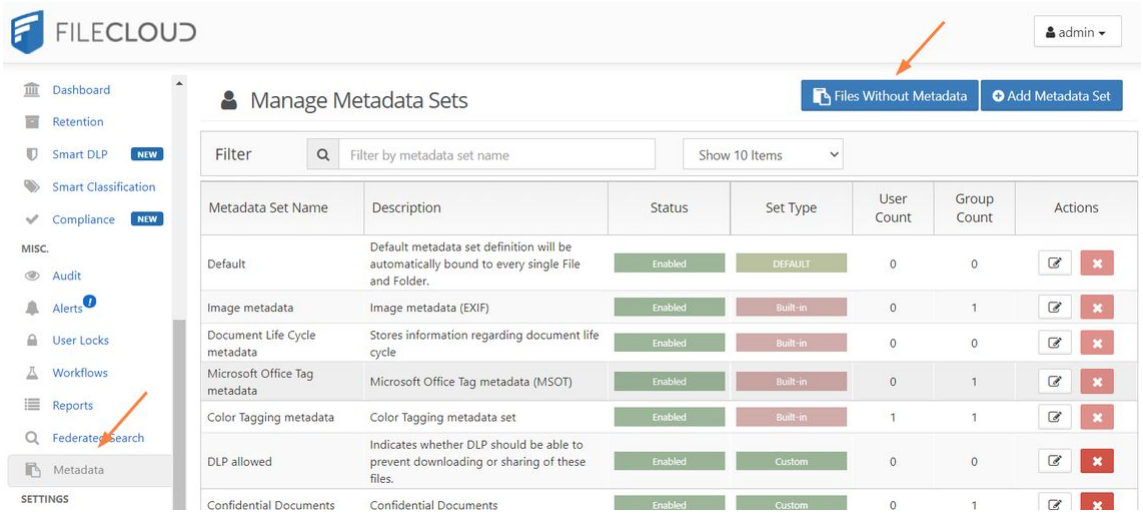
Smart Classification does not apply metadata to files over a specified size, but you can add metadata to those files manually. Beginning in FileCloud 20.1, you can configure your system to search for files without metadata.

## Find files without metadata:

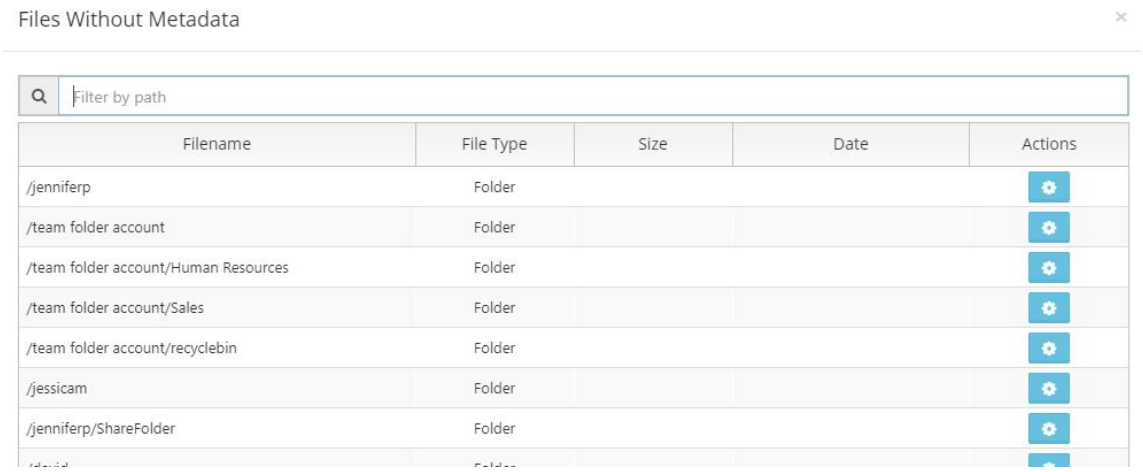
1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define('TONIDOCLOUD_SHOW_FILES_WITHOUT_METADATA', true);
```

3. In the navigation bar, click **Metadata**.
   Now the upper-right corner of the Manage Metadata Sets screen displays a **Files Without Metadata** button.

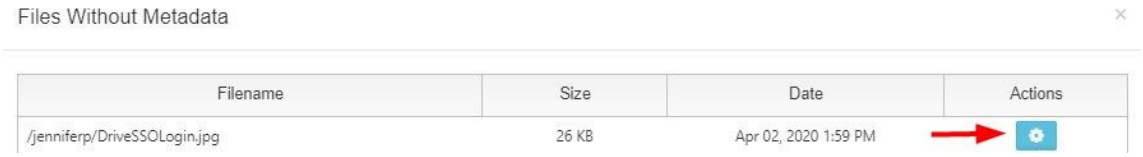



4. To display a list of files without metadata, click **Files Without Metadata**.

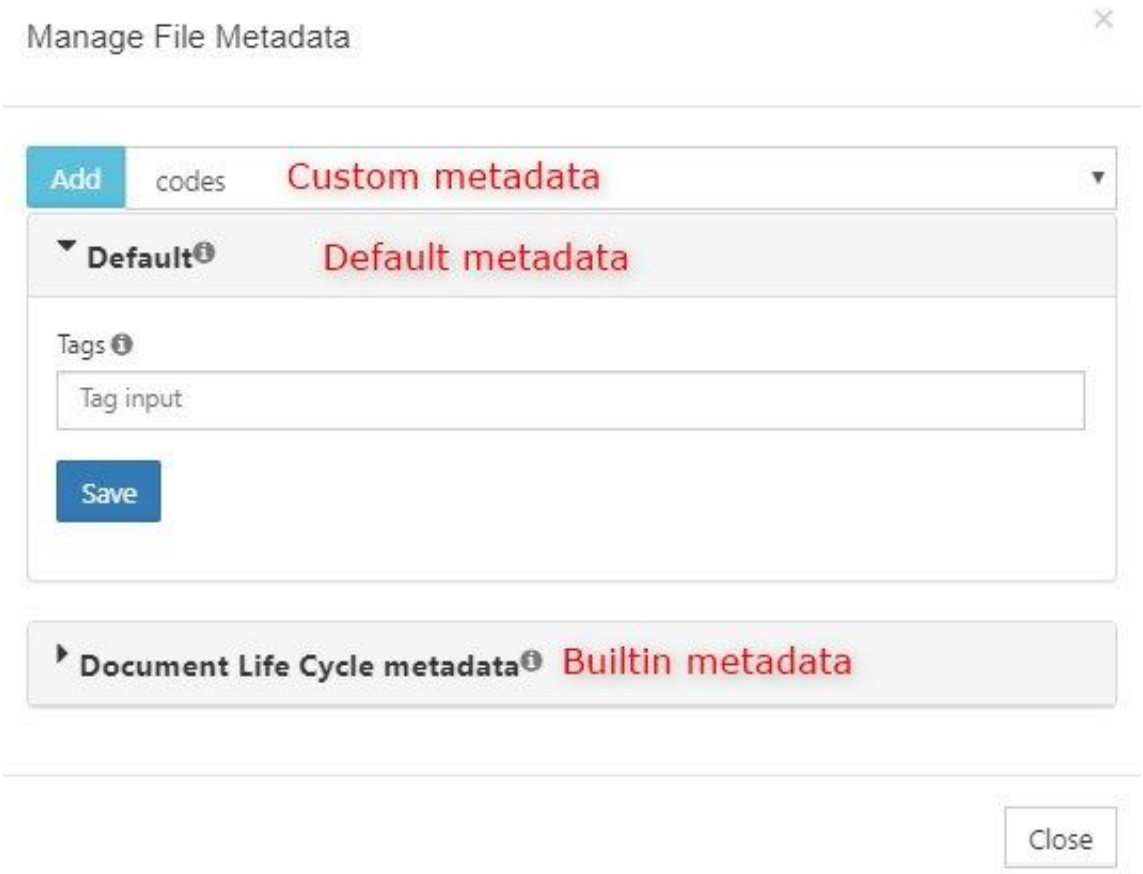



## Add metadata from the Files Without Metadata list

1. Follow the procedure above to access your **Files Without Metadata** list.
2. Across from a file, click the button under **Actions**.

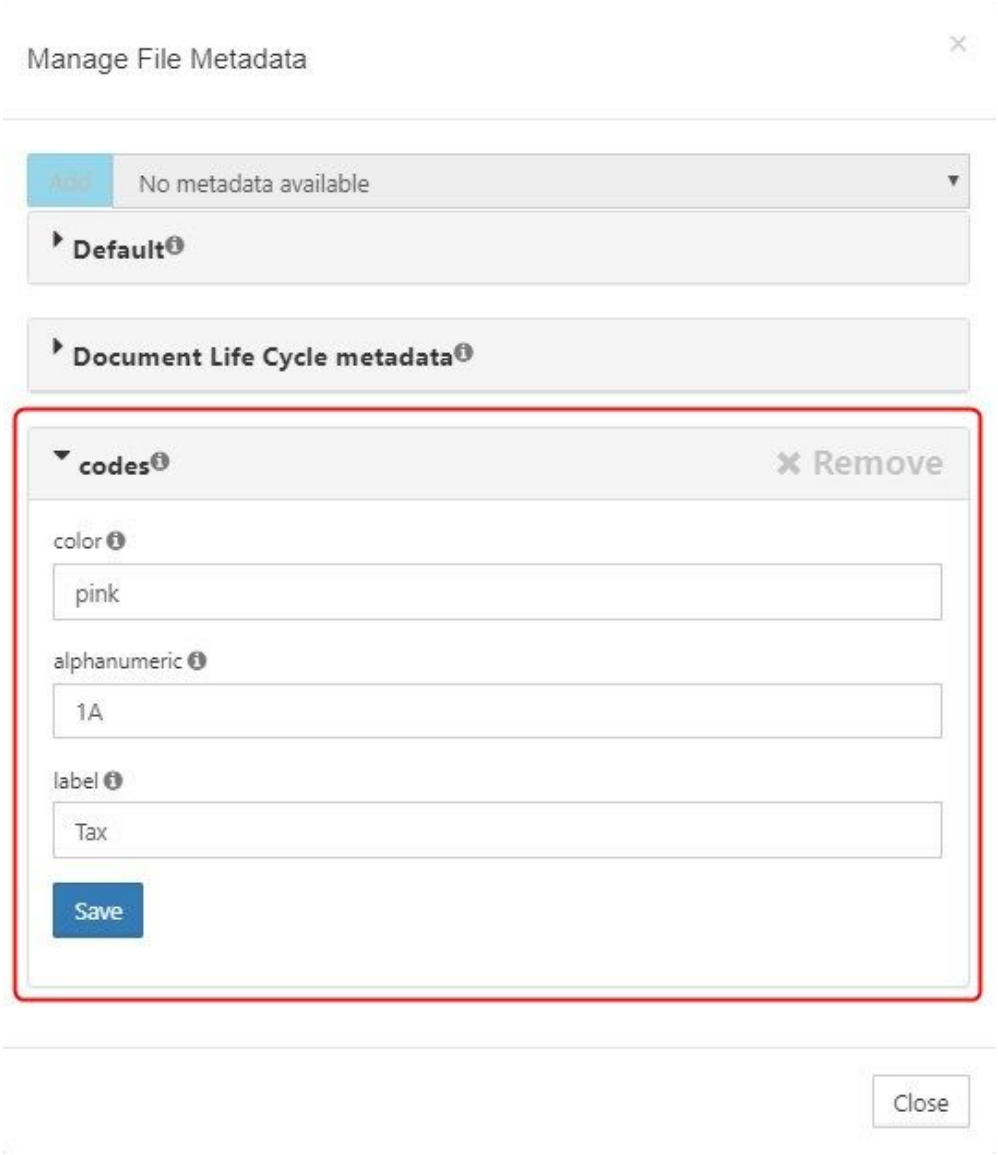



The Manage File Metadata window opens.

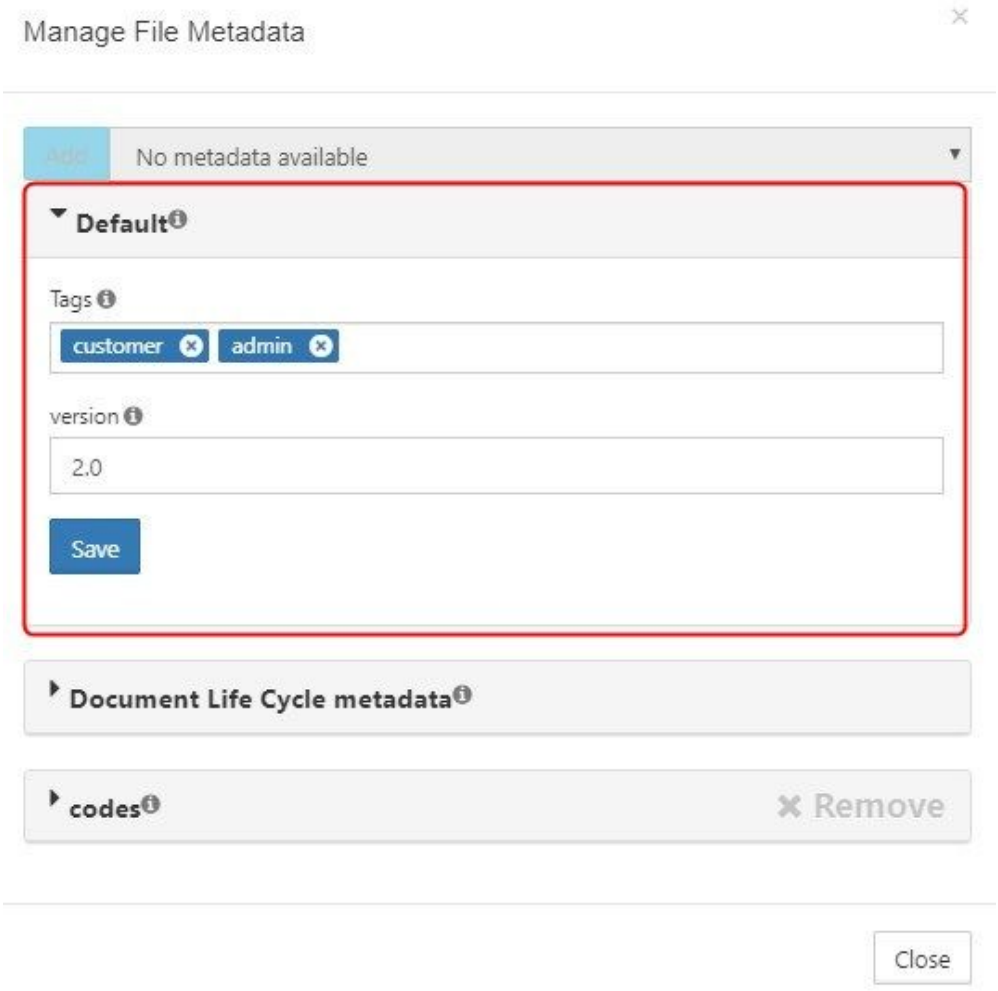



The top drop-down list holds custom metadata (see page 335), the drop-down list below that holds default metadata (see page 336), and any drop-down lists below that hold built-in metadata (see page 310).

3. To add a custom metadata set, choose it in the drop-down list and click **Add**.
   It is added below the other metadata sets.
4. Add or change values in any of the metadata fields.




5. You can update the value of fields that appear in **t**he **Default** metadata set**.**. Expand the section, and add or change the values in the metadata fields, and click **Save**.




6. You can view, but not update the values in built-in metadata sets. Expand the sections to view the metadata and any values they have.

## Metadata Limitations/Recommendations

| Metadata feature | Recommended maximum |
|---|---|
| Metadata set name | 128 characters |
| Metadata set description | 128 characters |
| Attributes per metadata set | 99 |

| Metadata feature | Recommended maximum |
|---|---|
| Attribute name | 128 characters |
| Attribute description | 128 characters |
| Values per enum/array | 99 |
| Predefined value (enum) | 128 characters |
| Default value | 128 characters |
| Actual value | 128 characters |

# Managing FileCloud Licenses

Your FileCloud license provides legally binding guidelines on your use and distribution of FileCloud.

**In this section:**


- FileCloud - License Purchase And Renewal (see page 345)
- Install FileCloud License (see page 362)

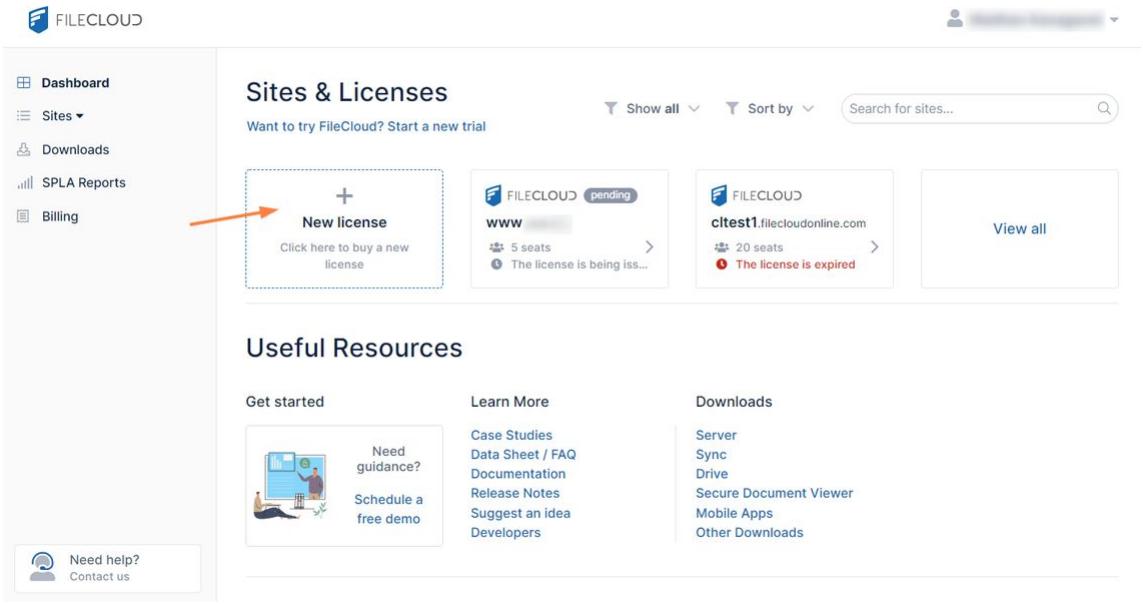

## FileCloud - License Purchase And Renewal

### Purchase a new license

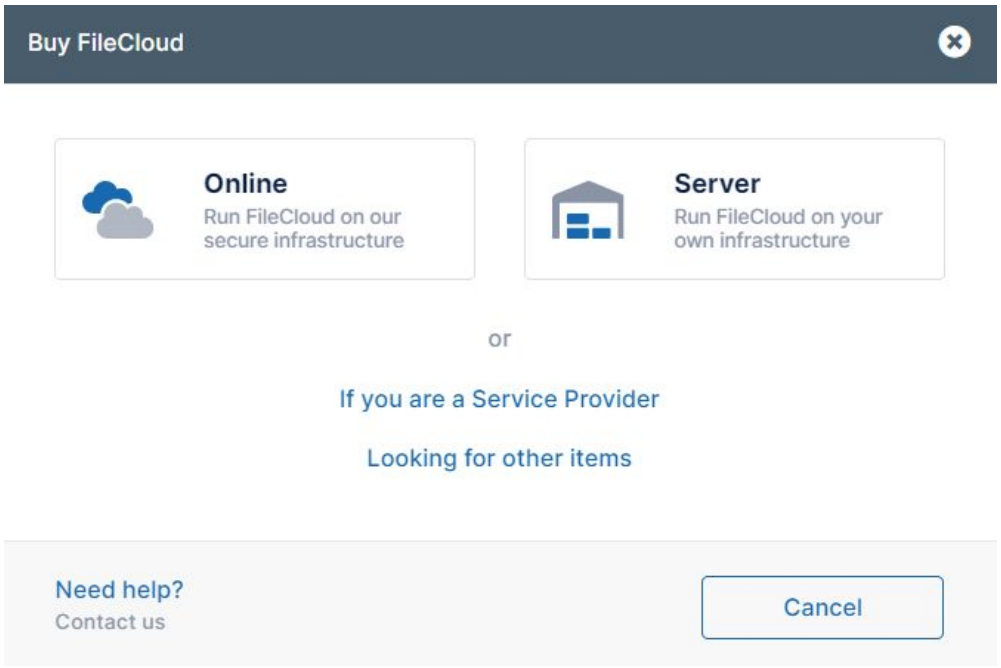
#### First

#### Choose a server or online license

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



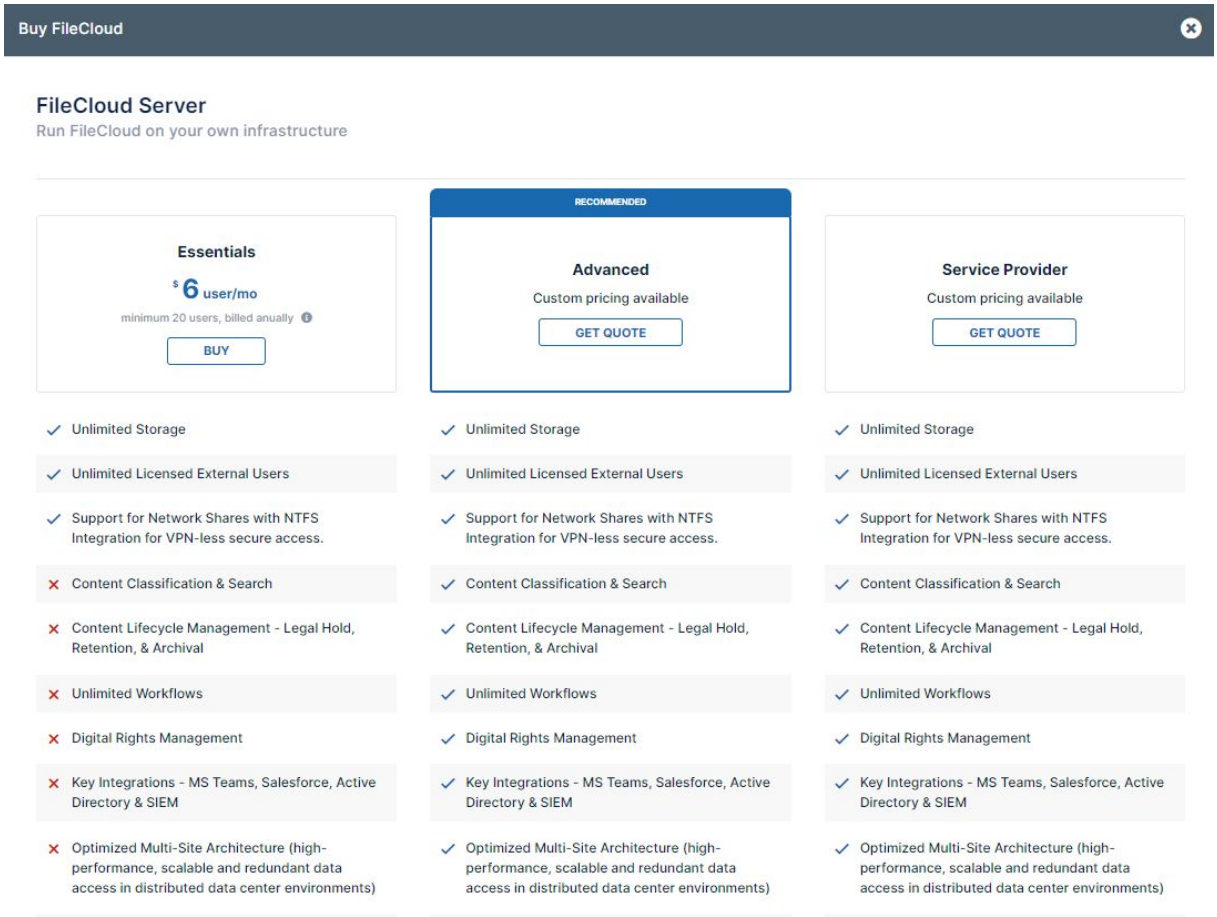

3. In the **Buy FileCloud** window, click **Online** or **Server**.



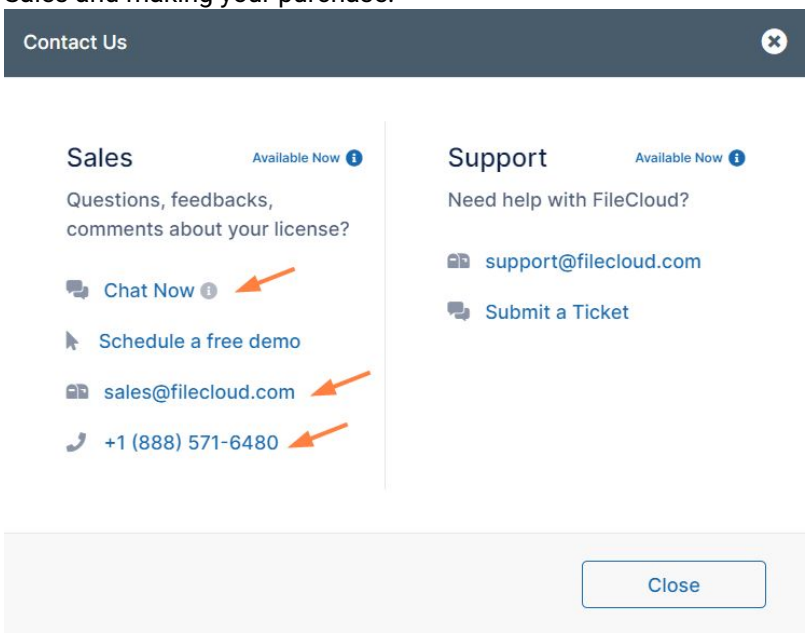

**Then**

**Purchase the server license**

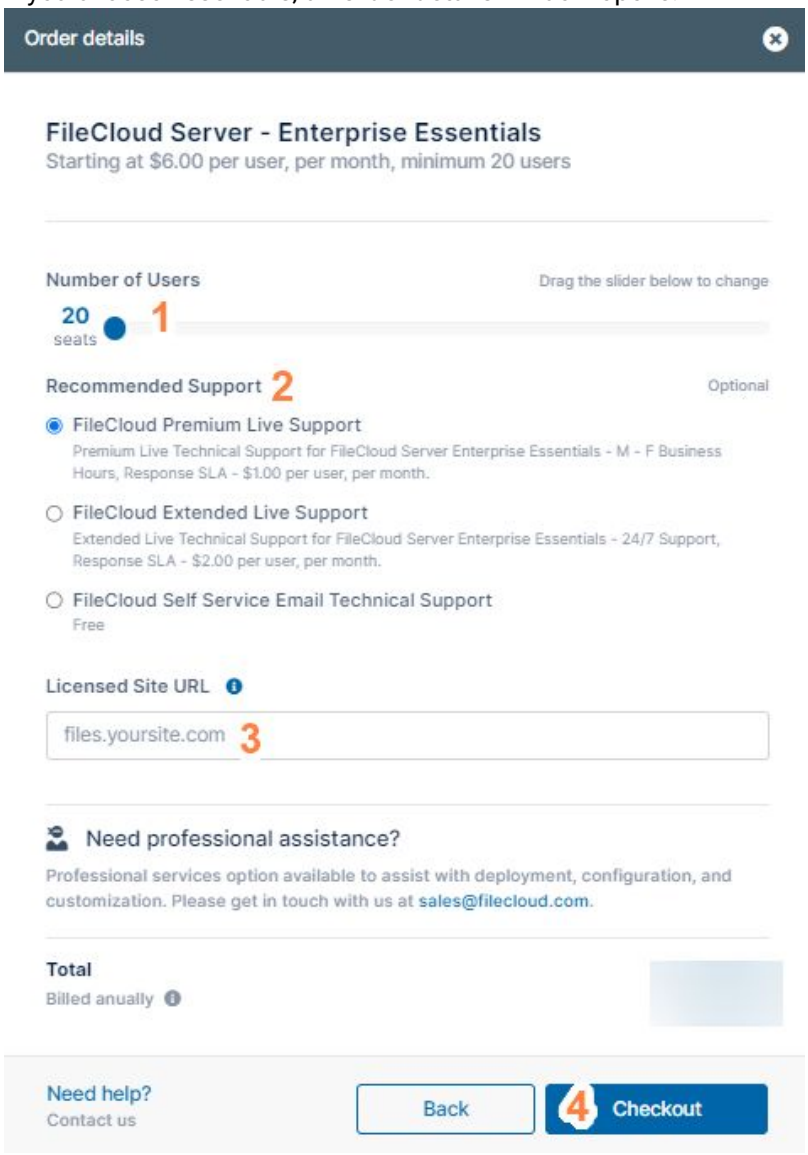
If you choose **Server**, the next window prompts you to choose **Essentials, Advanced,** or **Service Provider**.




If you click **Advanced** or **Service Provider,** in the window that opens, choose an option for contacting Sales and making your purchase.



If you choose **Essentials**, an **Order details** window opens.

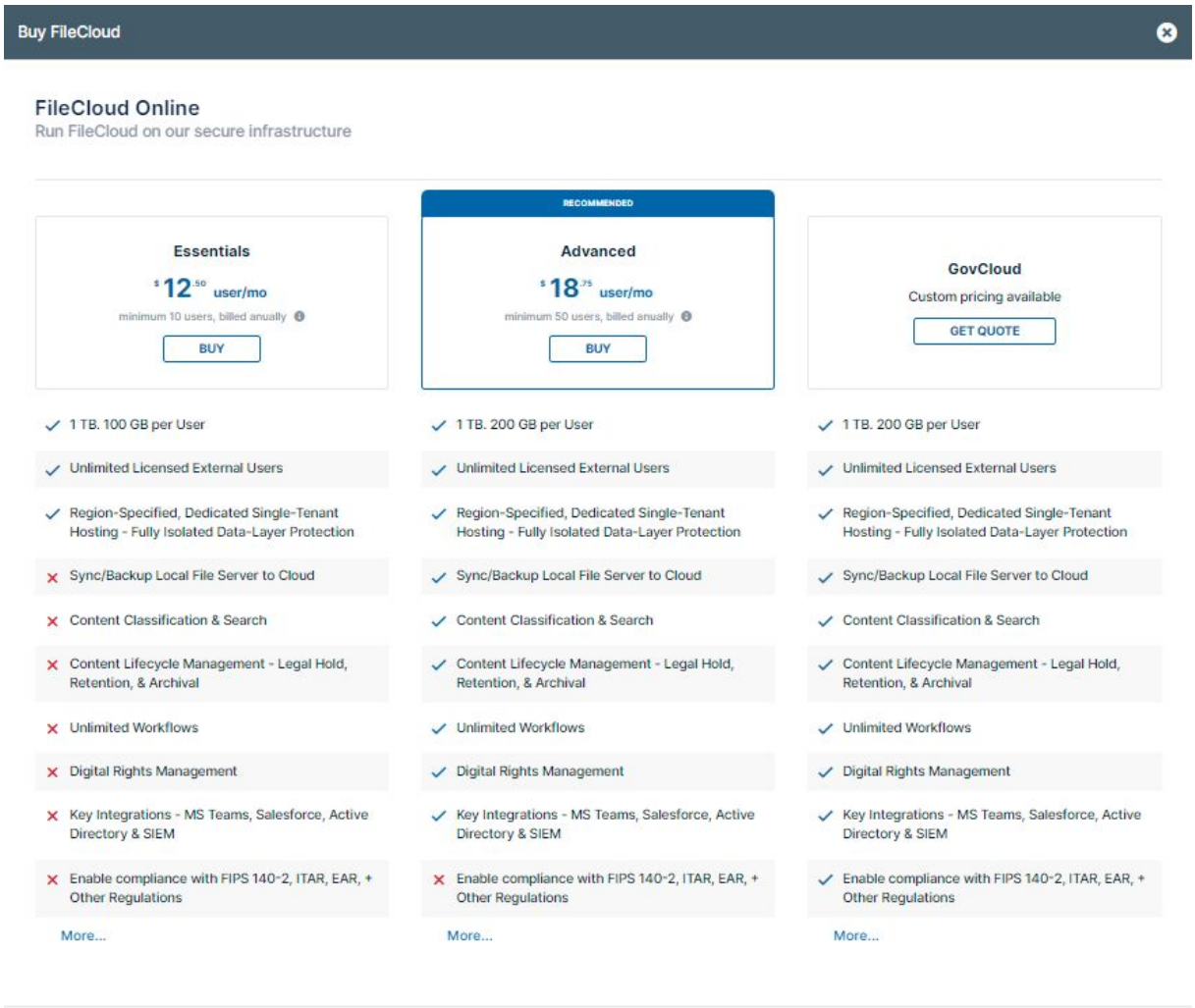



1. Move the **Number of Users** slider to indicate the number of users to include on the license.
2. Choose a support option.
3. In **Licensed Site URL**, enter your site address.
4. Click **Checkout**.
5. Perform the checkout process, below.

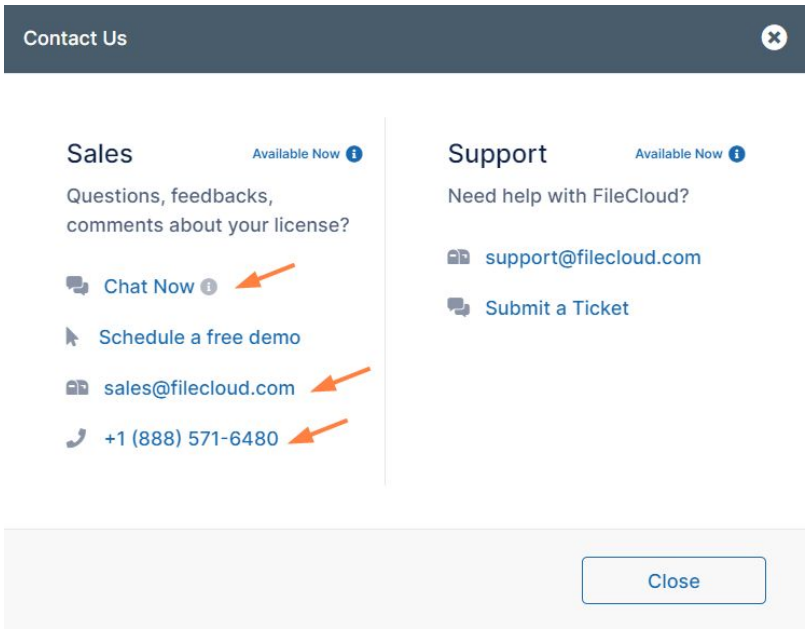
or

**Purchase the online license**

If you choose **Online**, the next window prompts you to choose **Essentials, Advanced, or GovCloud.**

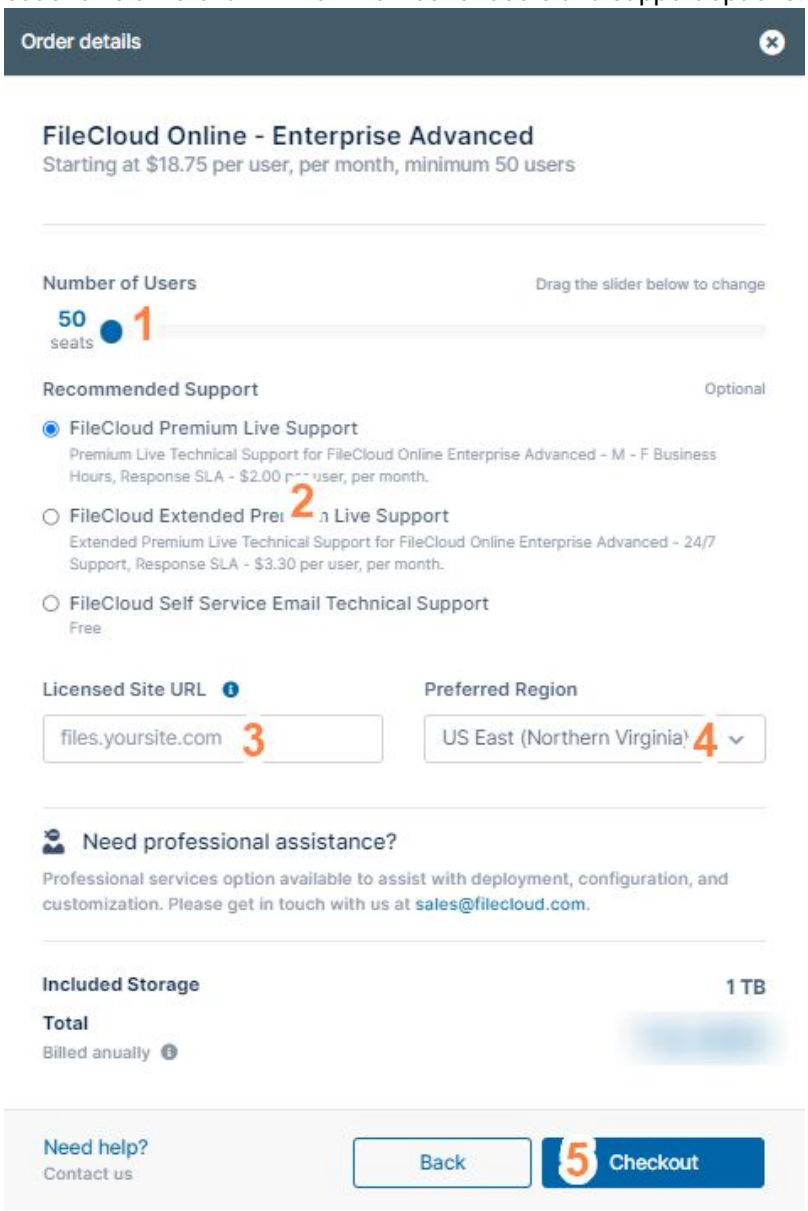



If you click the **GovCloud,** in the window that opens, choose an option for contacting Sales and making your purchase.




If you choose **Essentials** or **Advanced**, an **Order details** window opens. It is similar for both options,

but shows different minimum number of users and support options.



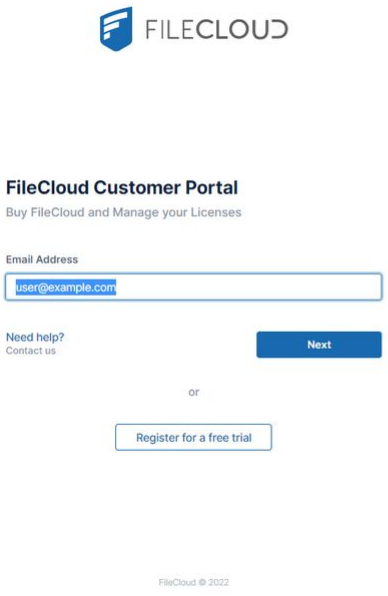

1. Move the **Number of Users** slider to indicate the number of users to include.
2. Choose a support option.
3. In **Licensed Site URL**, enter your site address.
4. In **Preferred Region**, choose the region where you want your server located.
5. Click **Checkout**.
6. Perform the checkout process, below.

## Renew an existing license

### Renew a license

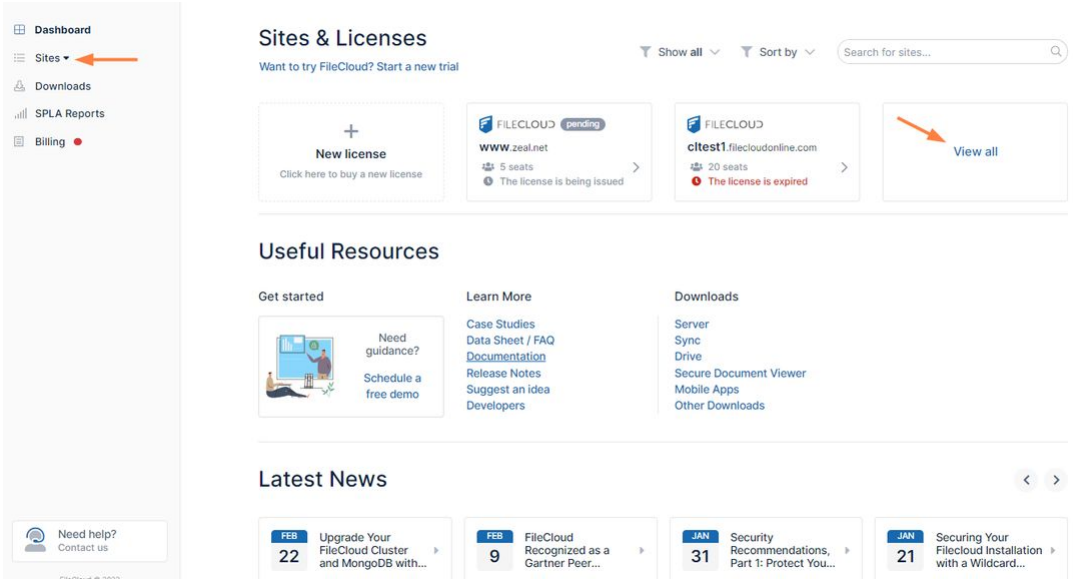
***Note: If you are an MSP and want to renew an SPLA License, please follow the purchase a new license instructions, above.***

1. Log into https://portal.getfilecloud.com[36]
   *Note: Enter the email of the license holder. To change the license holder email, please contact sales@codelathe.com*[37].

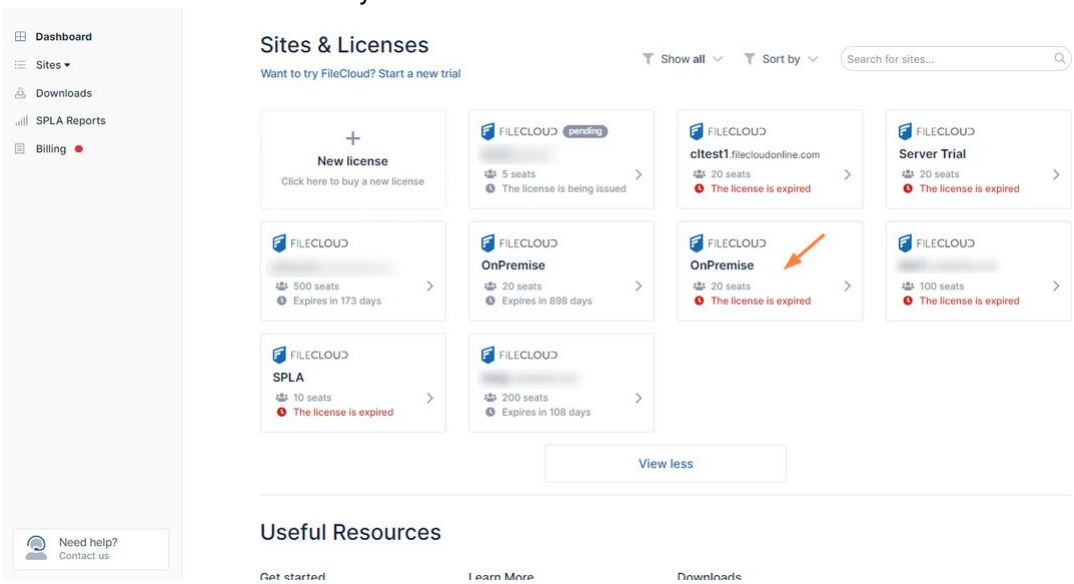


2. If you don't see the license you want to renew on the initial dashboard page, click **View all** to view all of your licenses.
   (You can also expand the **Sites** link in the navigation pane to see navigation links to all of your licenses.)

36. https://portal.getfilecloud.com/
37. mailto:sales@codelathe.com

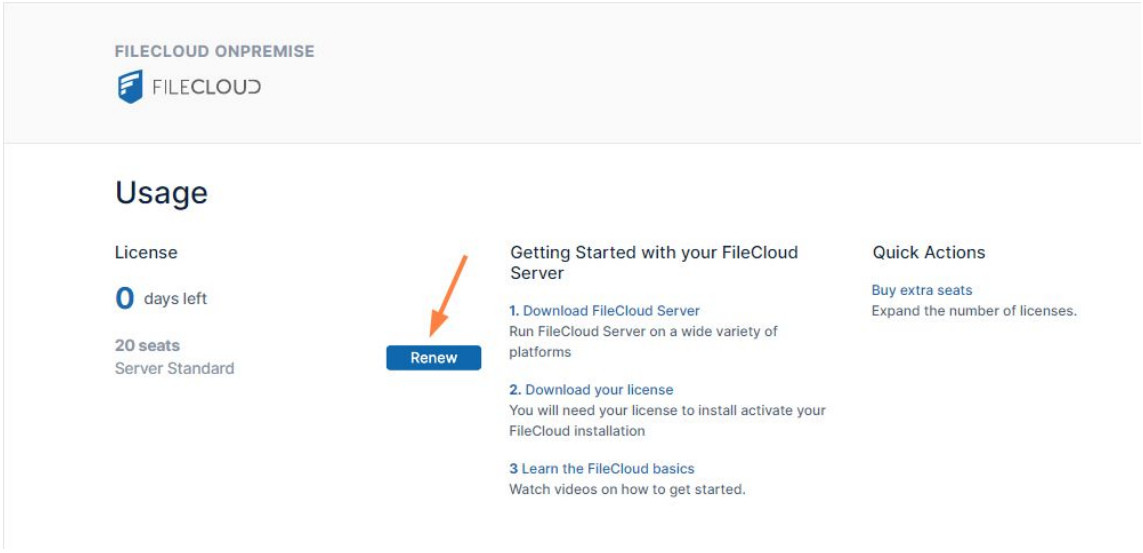



3. Find and click the license that you want to renew.




A screen that displays the license details opens.

4. Click the **Renew** button.



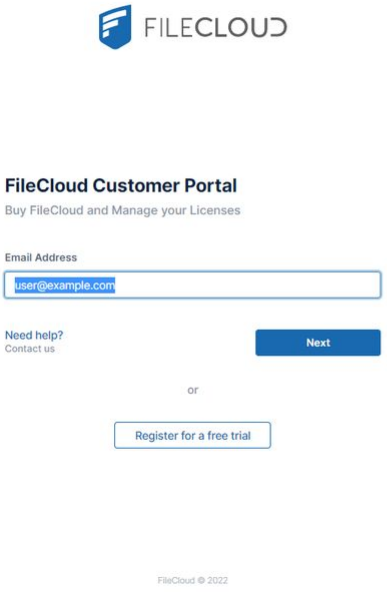

An **Order Summary** opens.

5. Follow the checkout process, below.

## Add additional users to an existing license

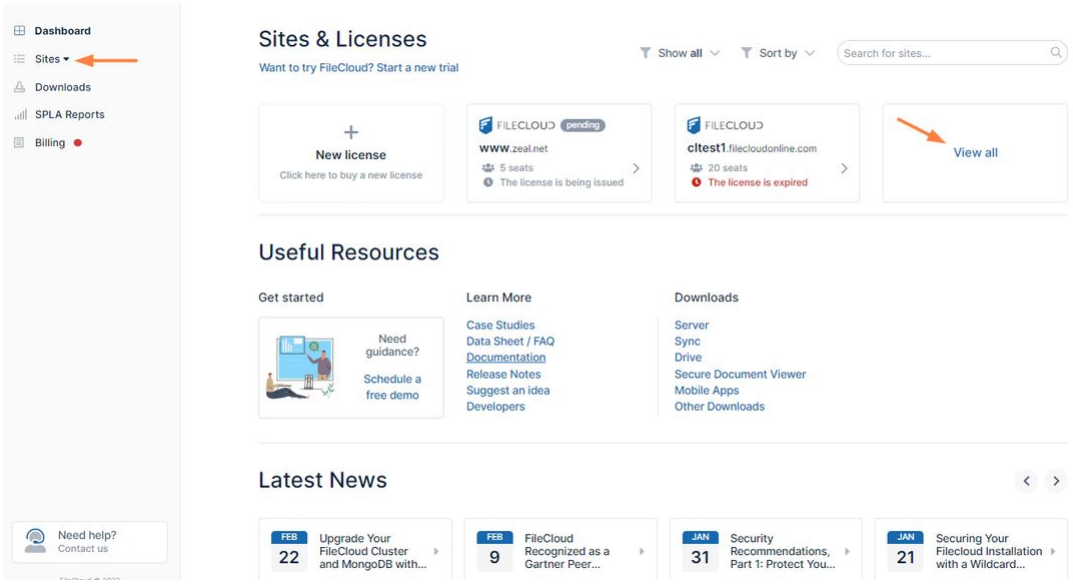
### Add additional users to a license

1. Log into https://portal.getfilecloud.com[38]
   *Notes: Enter the email of the license holder. To change the license holder email, please email sales@codelathe.com*[39].



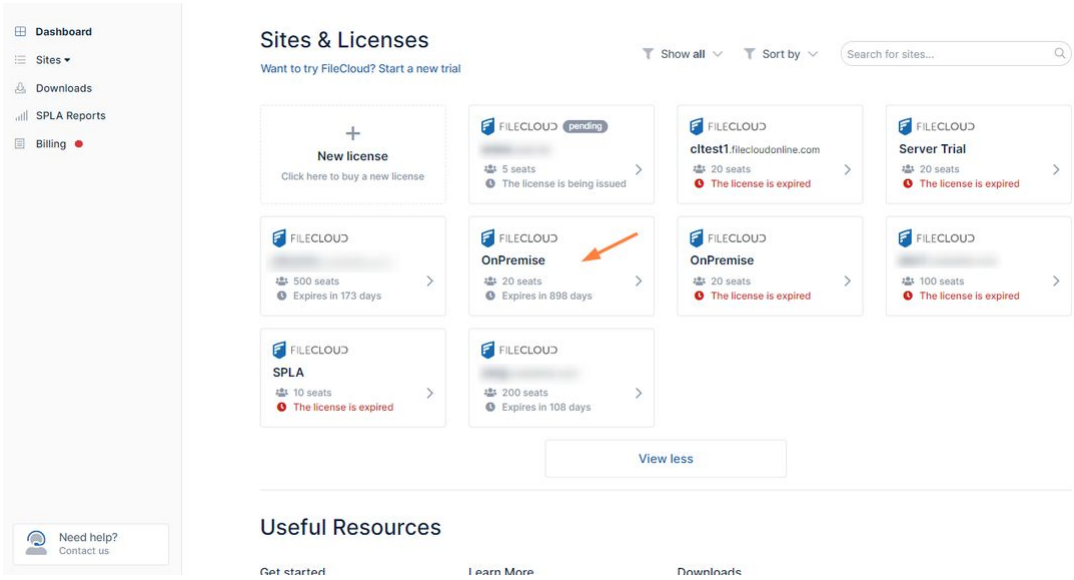
38. https://portal.getfilecloud.com/
39. mailto:sales@codelathe.com

2. If you don't see the license you want to add users to on the initial dashboard page, click **View all** to view all of your licenses.
   (You can also expand the **Sites** link in the navigation pane to see navigation links to all of your licenses.)



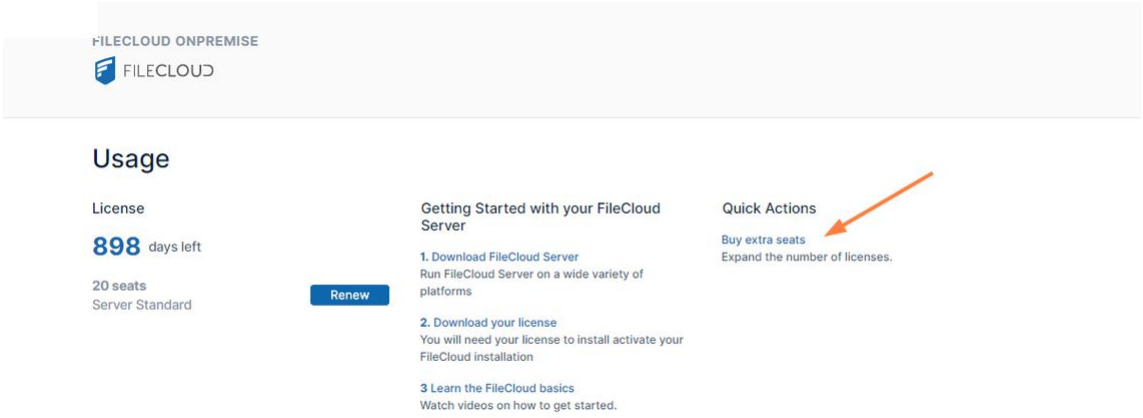

3. Find and click the license that you want to add additional users to.

.



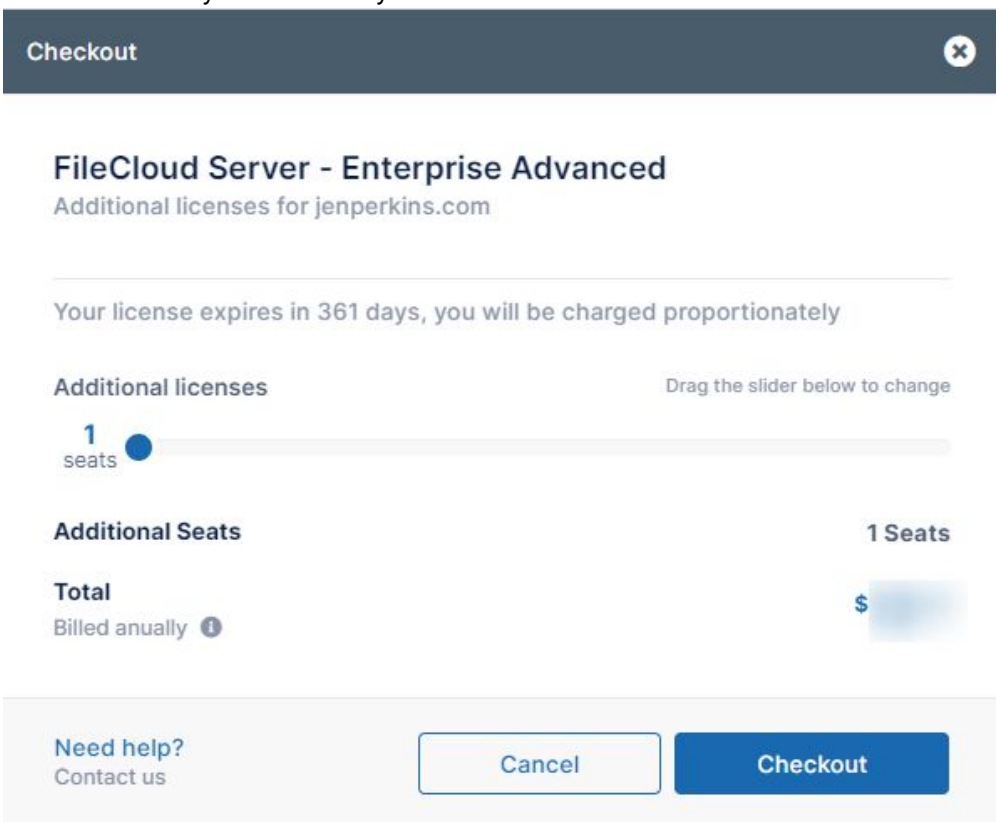

   A screen that displays the license details opens.

4. Click **Buy extra seats**.




A checkout window opens. The number of extra seats is set to 1 by default.

5. If you want to purchase more than 1 extra seat, move the **Number of Users** slider to indicate the number of seats you want to buy.

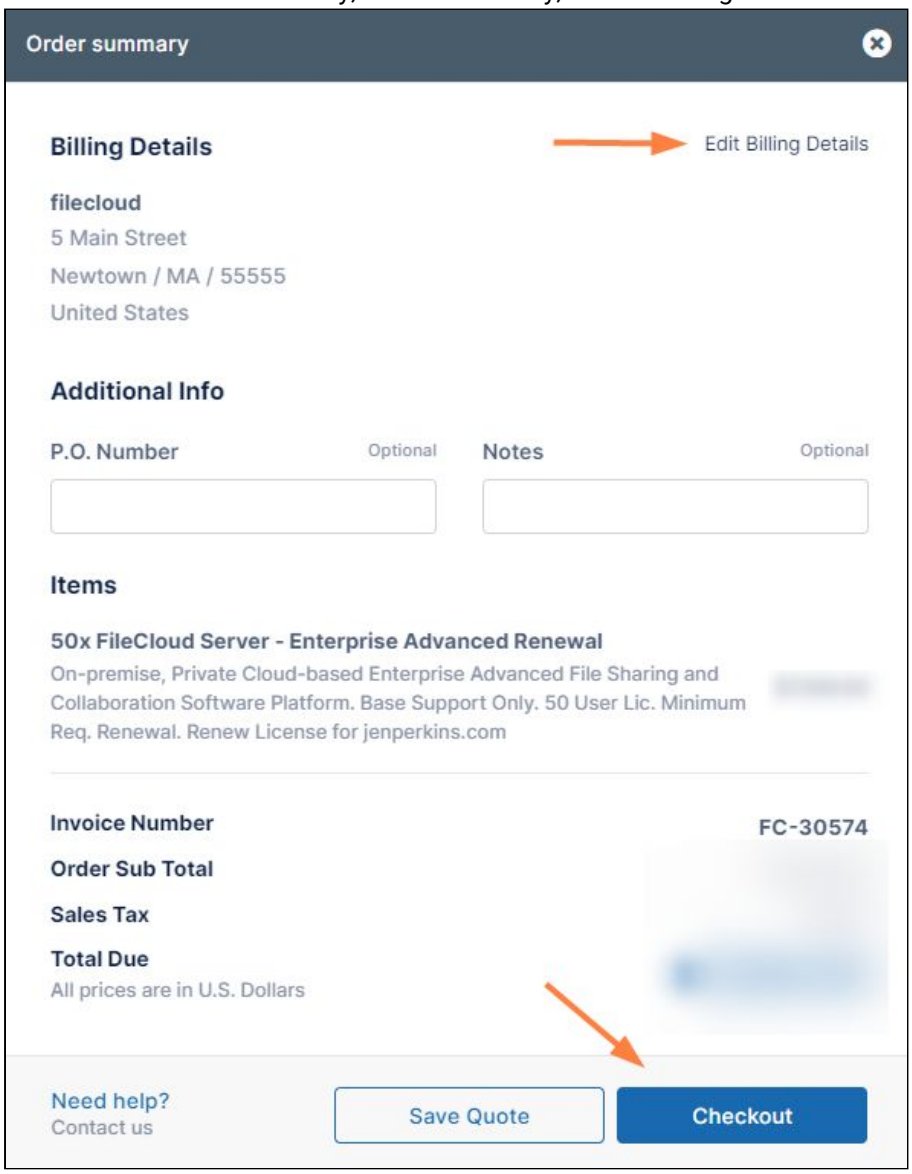



6. Click **Checkout**.
   An **Order Summary** opens.
7. Follow the checkout process.

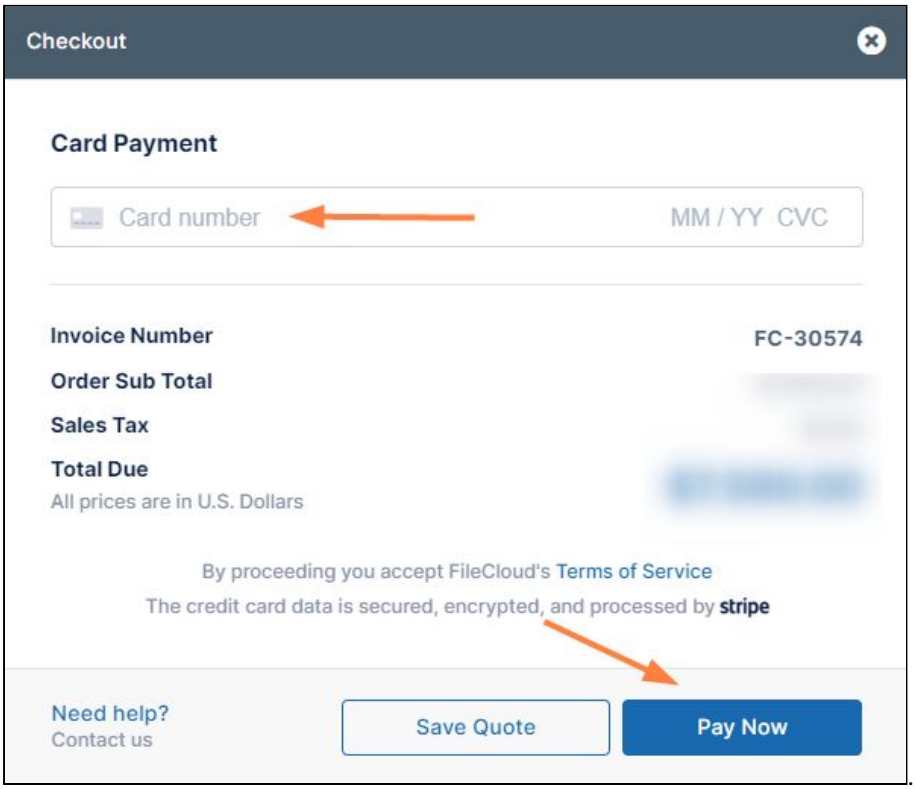
## Checkout process

### Pay now

1. Look over the order summary, and if necessary, edit the billing details:



2. Click **Checkout.**

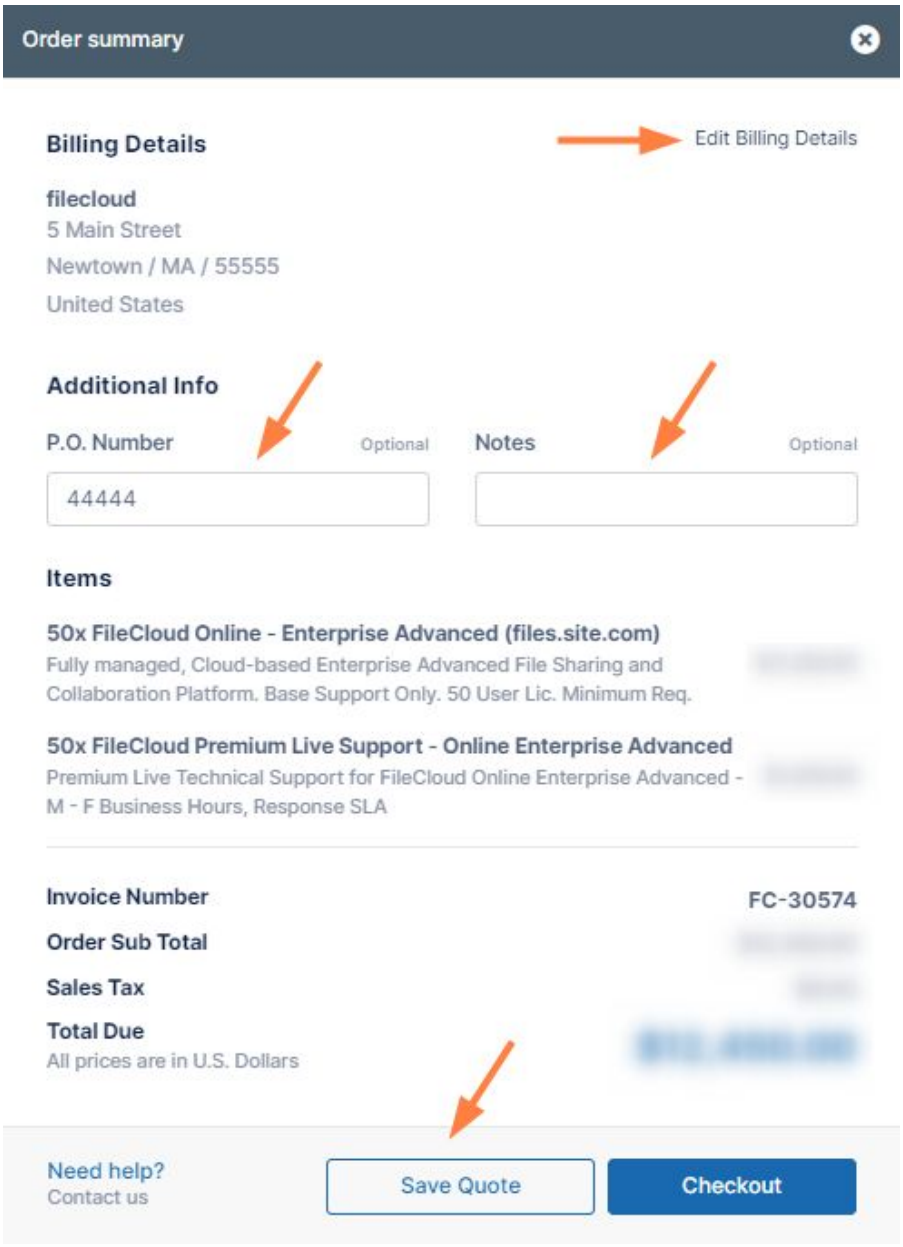



3. Enter your credit card number, and click **Pay Now**.
   A confirmation window appears.
4. Click **Dashboard** in the navigation pane to see an icon for your new pending license:

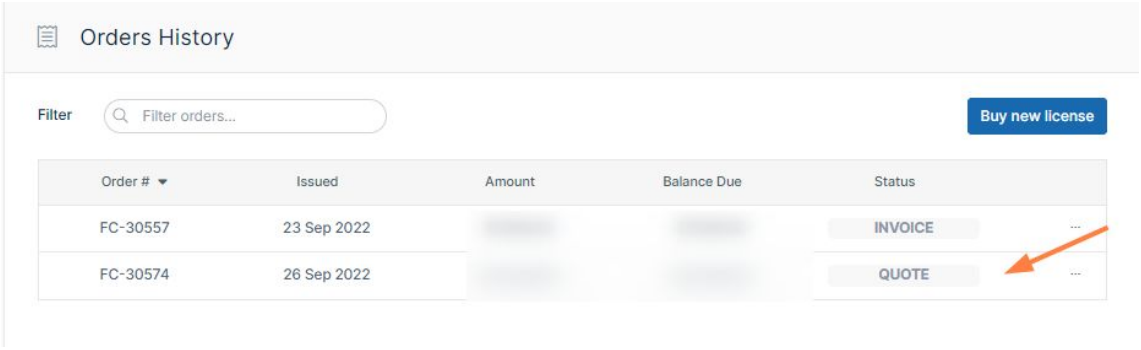
or

**Send a purchase order**

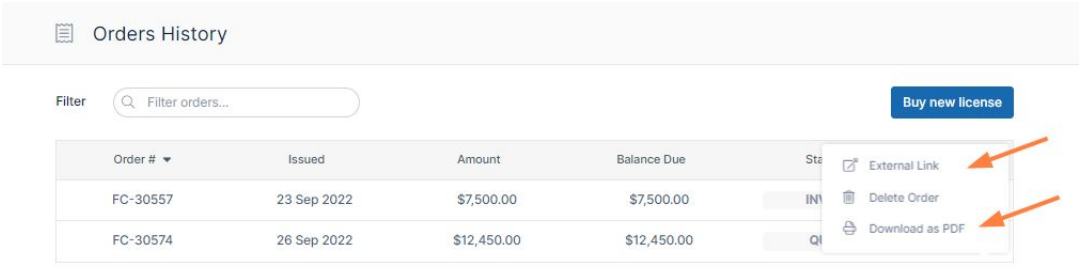
1. Look over the order summary, and if necessary, edit the billing details:



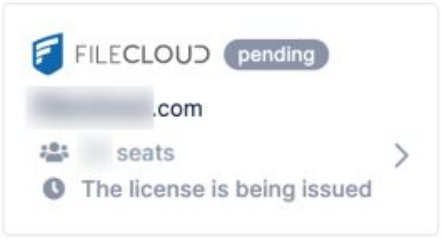

2. Optionally, enter a **P.O. Number** and any **Notes** for FileCloud Sales.
3. Click **Save Quote**.
   The **Billing** screen opens.
4. Your order appears under **Orders History** with the status **QUOTE**.




5. Click the **More** (triple-dot) icon in the row for the order, and either:
   - choose **External Link** and copy the link,
     or
   - choose **Download as PDF** and save the PDF.




6. Send a purchase email to sales@codelathe.com[40]with the quote link included or the PDF attached.
7. Once FileCloud begins to process the license, it is overlaid with a pending icon.



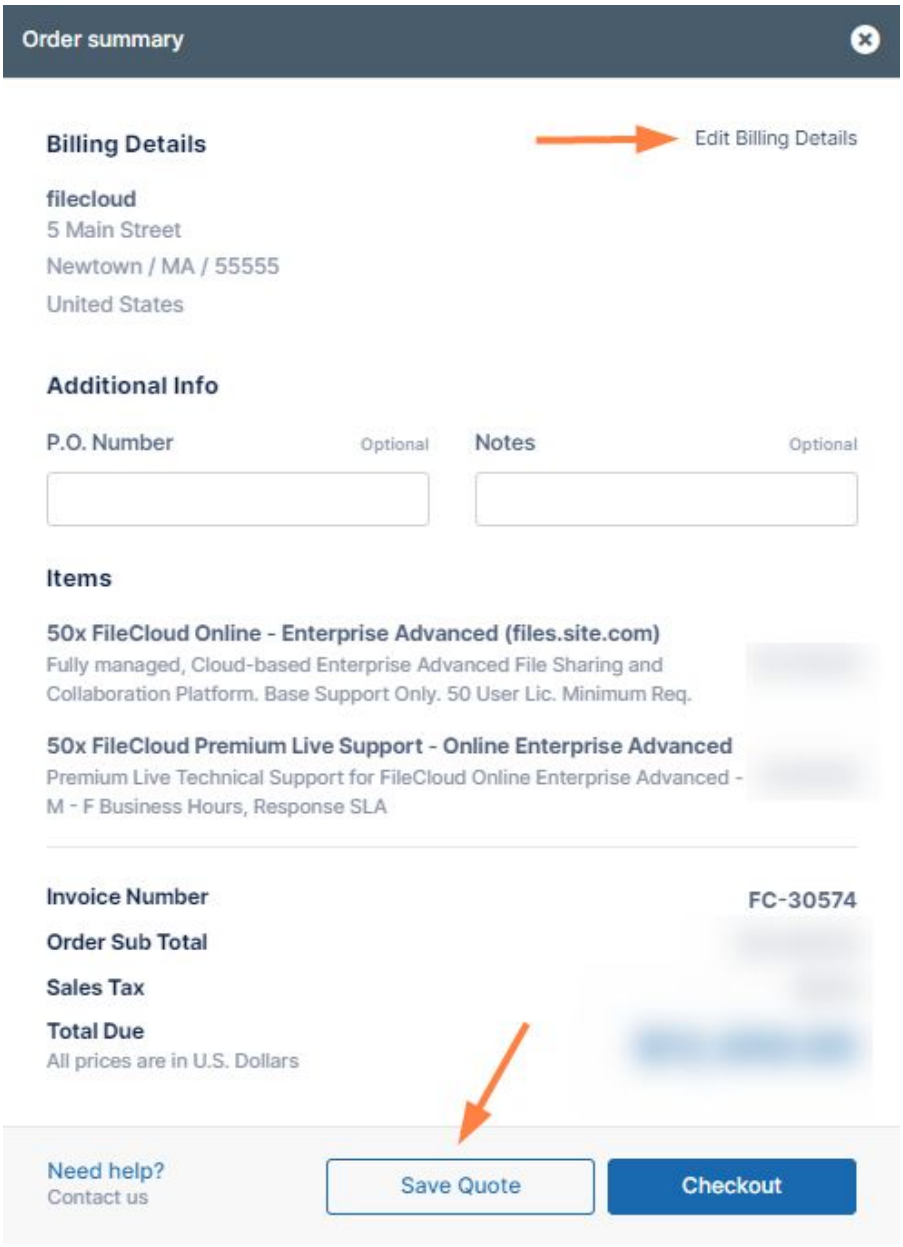

   When processing of the license is complete, the pending icon disappears. Now you can download and install the license.

or

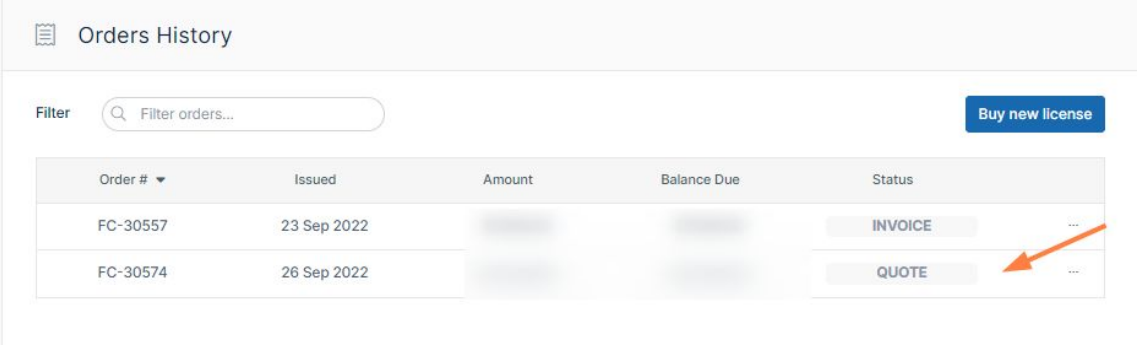
**Save quote and continue later**

1. Look over the order summary, and if necessary, edit the billing details:

40. mailto:sales@codelathe.com




2. Click **Save Quote**.
   The **Billing** screen opens. Your order appears under **Orders History** with the status **QUOTE**, and remains there unless you delete it.

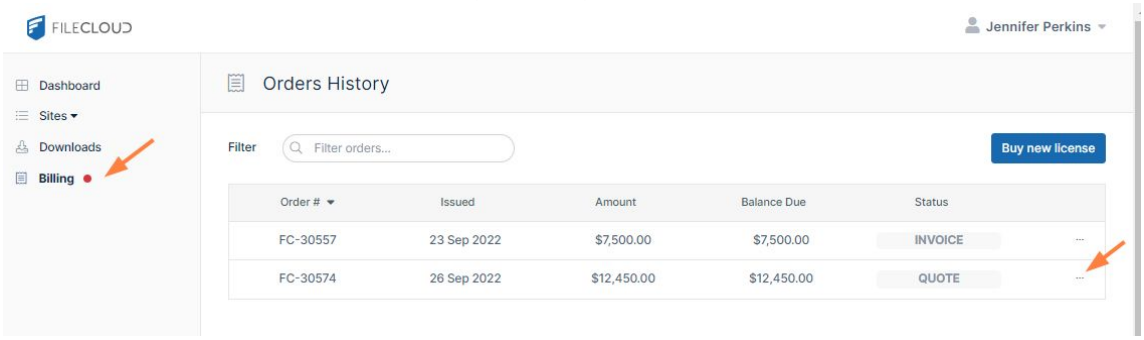


3. When you are ready to continue, return to the **Billing** screen and perform one of the actions in Manage orders, below.

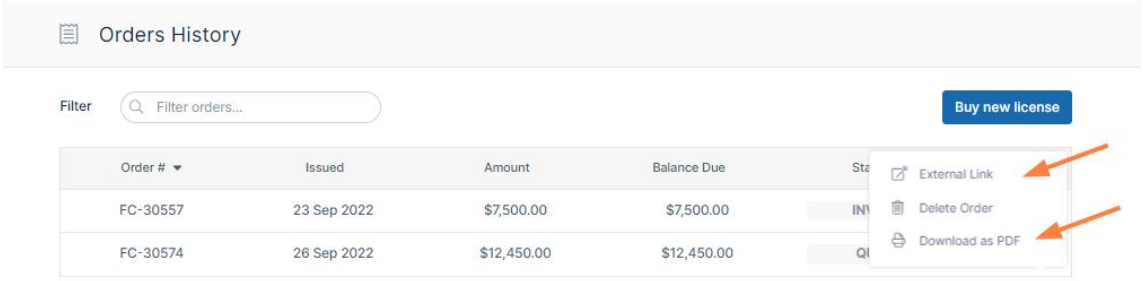
## Manage orders

**View order, save order link, save to pdf or delete order history**

1. Log into https://portal.getfilecloud.com[41]
2. In the navigation pane, click the **Billing** link.
3. To the right of the order, click the **More** (triple-dot) icon.




4. You are given options to view the order in another link, delete it, or download it as a PDF. If you click **External Link**, you can copy the link and send it to another user to view the order or you can send it to FileCloud to purchase it. You can also send a copy of the PDF to FileCloud to purchase the order.




# Install FileCloud License

Your FileCloud license is a document that provides legally binding guidelines on the use and distribution of your newly installed FileCloud software.

**Obtaining a FileCloud License**

## Obtaining a FileCloud License

The length of access and site configuration will vary depending on your license type.

41. https://portal.getfilecloud.com/

There are two basic forms of FileCloud licenses:

| License Type | Duration | Features | Availability |
|---|---|---|---|
| Trial (free) | Temporary<br>30 days for a server license<br>15 days for an online license | • All features<br>• Mobile and desktop apps<br>• Free support<br>Deployment URL will be set as "*" (accessible from any URL) | Server (Self-host)<br><br>Online (Hosted by us) |
| Production | Permanent based on length paid for<br>Usually 1 year | • All features<br>• Mobile and desktop apps<br>• Choose from 3 levels of support<br>Deployment URL can be set to use your specific domain<br>(URL accessibility from within your company and outside access managed by Administrators) | Server (Self-host)<br>• Essentials<br>• Advanced<br>• Service Provider<br><br>Online (Hosted by us)<br>• Essentials<br>• Advanced<br>• GovCloud |

For more information, read the license descriptions and Key Features on the FileCloud Pricing[42] page.

To purchase a license, see License Purchase and Renewal (see page 345)

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.

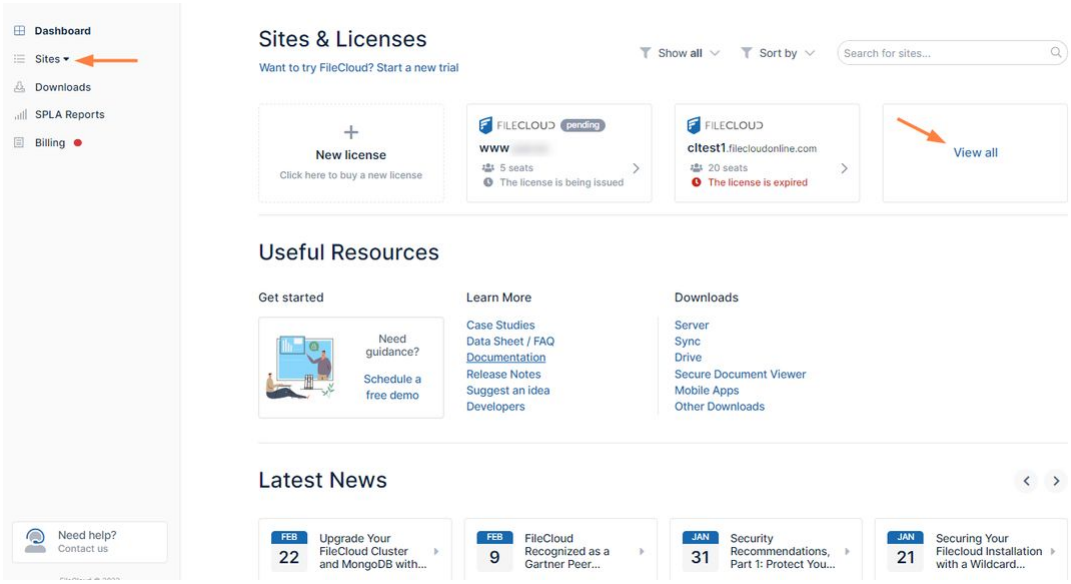
**Downloading your license**

## Downloading your License

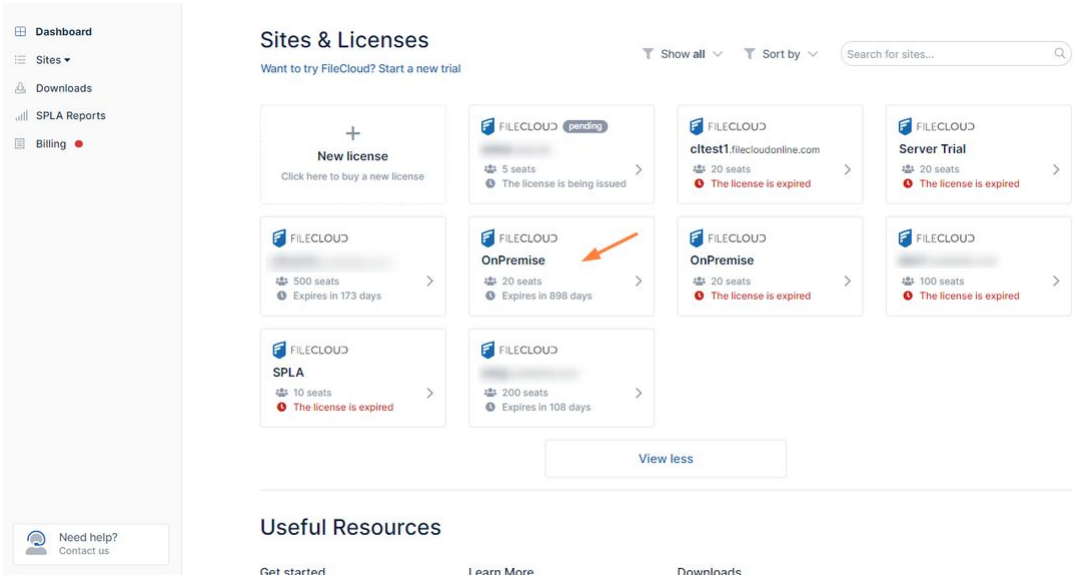
**To download your license**:

42. https://www.filecloud.com/pricing

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.




3. If you don't see the license you want to download listed, click **View all** to see all of your licenses. (You can also expand **Sites** in the navigation pane to access links to all of your licenses).
4. Click the license that you want to download.




5. The license is stored on your server as license.xml.

### Installing Your License

> The ability to install license components such as SALESFORCE is available in FileCloud Server version 18.2 and later.

## Installing Your License

You can operate FileCloud Server using any of the license types.

- If you do not need to use individual additional components, such as SALESFORCE, and Pattern Search, you can use an Essentials license.
- However, if you need to use individual additional components, such as SALESFORCE, and Pattern Search, then you must use an Advanced or Service Provider license.

There are multiple places where you can install your FileCloud license:

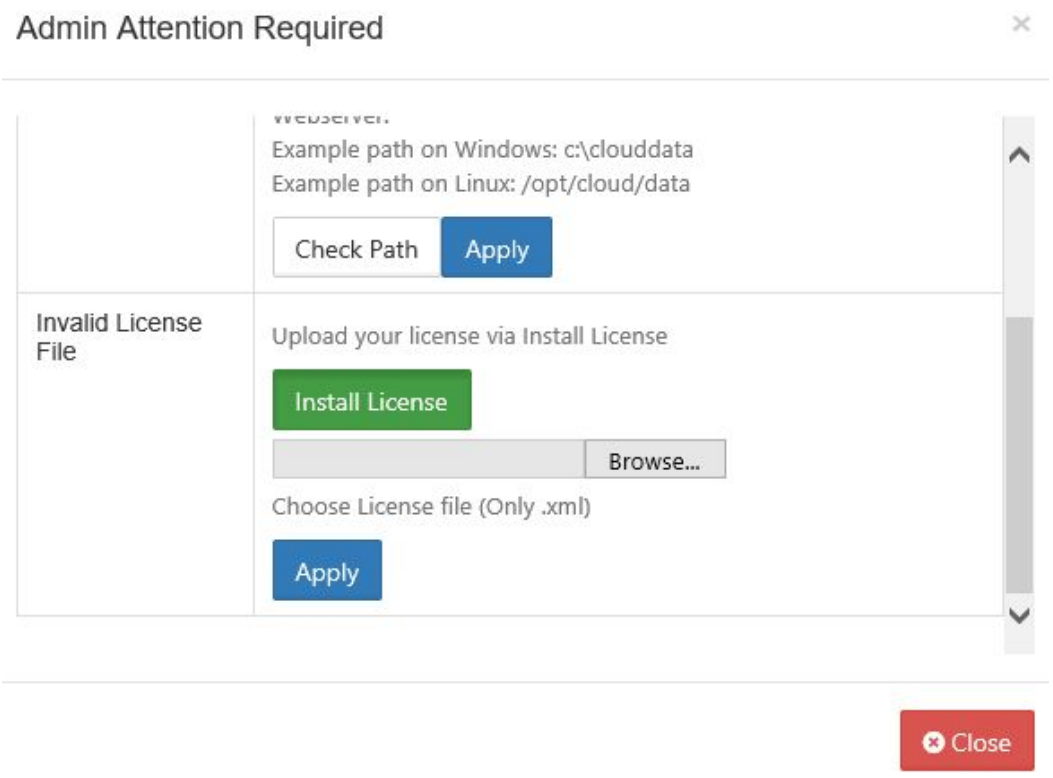
- Admin alert dialog box
- The dashboard's **License Information** widget
- The admin portal's License settings page.

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.



**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.

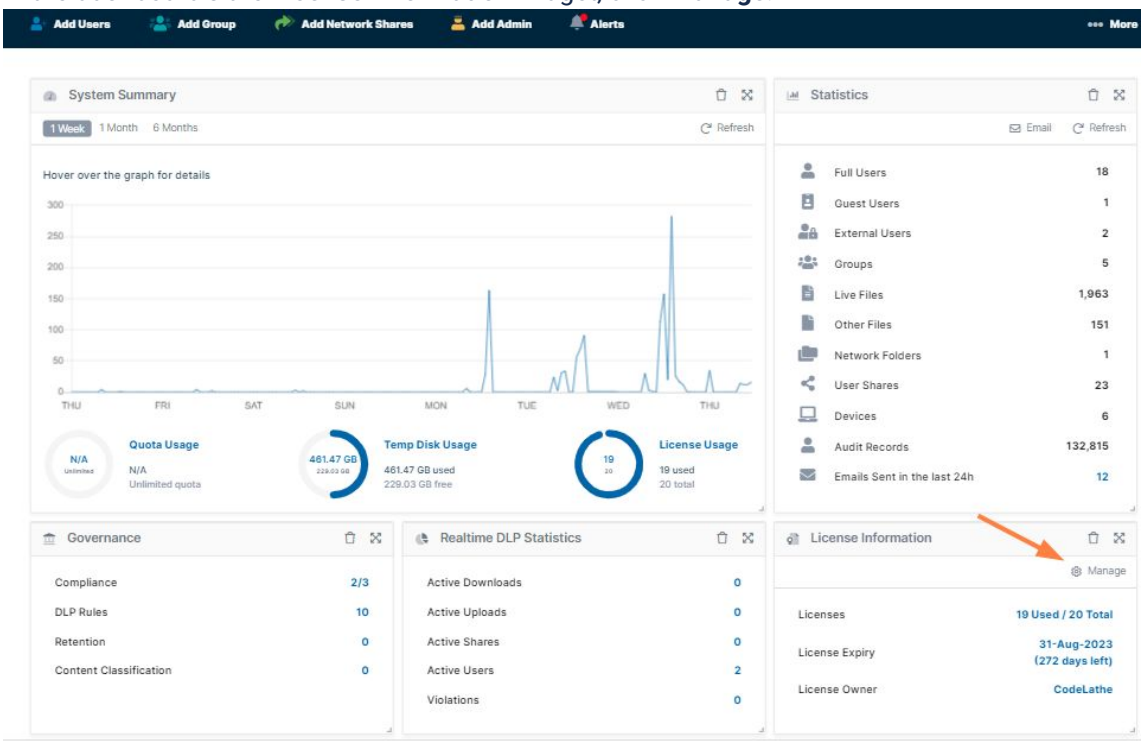
## Dashboard

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.

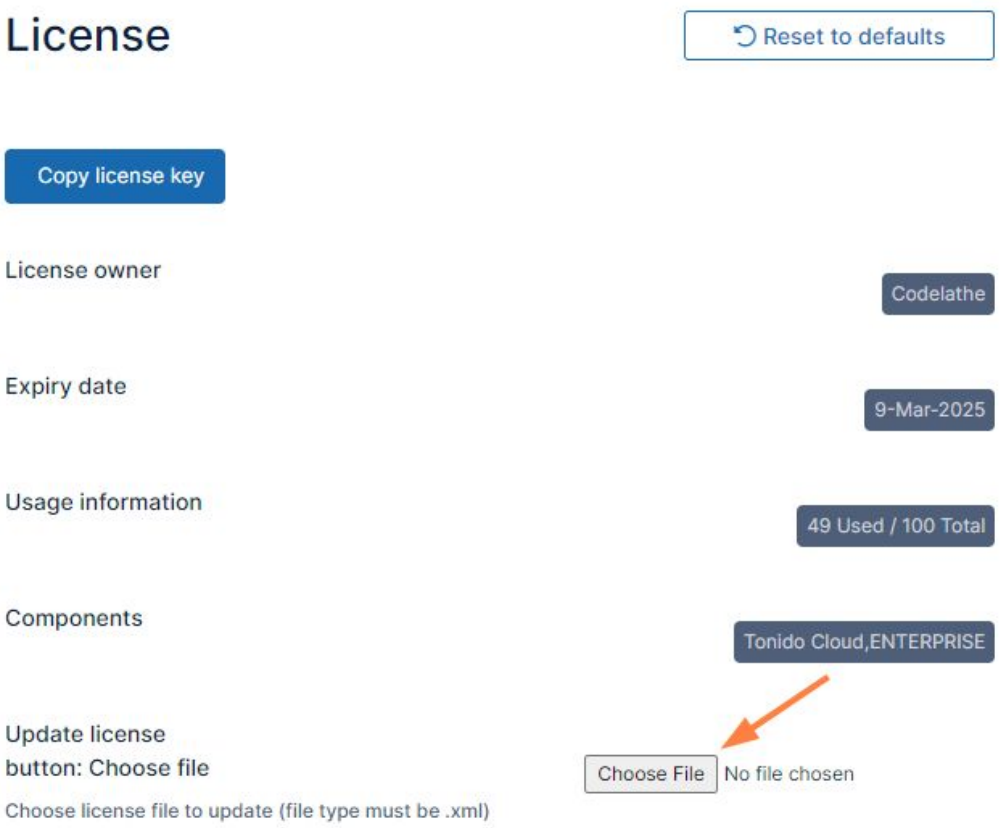
The dashboard opens the same window that opens when you click **Settings > License**.

**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.




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)
```

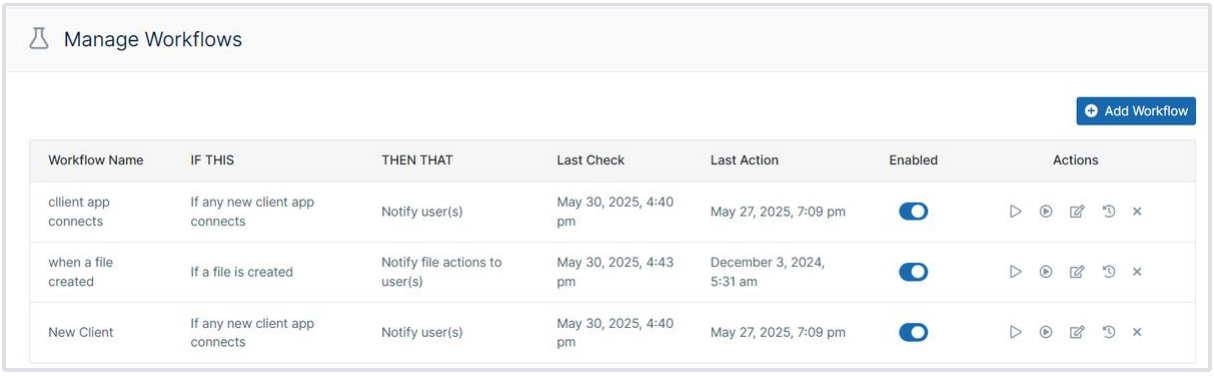
You can setup specific triggers to run when the following conditions occur:

- 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

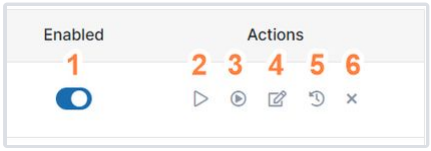
All workflows are created and managed on the Workflows dashboard.




**To access the Workflows dashboard:**

1. Open a browser and log into the admin portal.
2. On the left hand navigation panel, under **MISC.**, click **Workflows**.

The actions you can perform on a workflow you have created include:




1. Enable or Disable the workflow
2. Run the workflow (once, on-demand)
3. Simulate the workflow. Displays the list of users or files that a workflow will affect. The Simulate option is only available to workflows that are configured to run on demand and not to run automatically at scheduled times.
4. Edit the workflow
5. See activity. (Shows the date of an event, and a description of the event, such as file upload, move, and deletion.
6. Delete the workflow

In this section:


- Add a New Workflow (see page 370)
- Define an IF Condition (see page 371)
- Define a THEN Action (see page 405)
- Edit a Workflow (see page 421)
- Run a Workflow (see page 422)
- Set Advanced Workflow Options (see page 423)
- Workflow Recipes for FileCloud (see page 428)
- Troubleshooting Workflows (see page 477)


# 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 (see page 405) 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 (see page 371)
- Define a THEN Action (see page 405)

**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 (see page 371), 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 (see page 405), and then click Next.
7. If an Action requires you to specify a value for something, for example a date or time, type in the values in the Required Parameters, and then click Next. Information about what is required is described below this box.
8. In Workflow Name, type in a unique word or phrase that describes the workflow, and then click Finish.

## Define an IF Condition

Beginning in version 23.253, FileCloud supports expressions, special conditions based on user and path owner properties.

The workflow **If a user's account is near its expiration date** is available in FileCloud 23.251 and later.

Not all actions are compatible with all conditions.

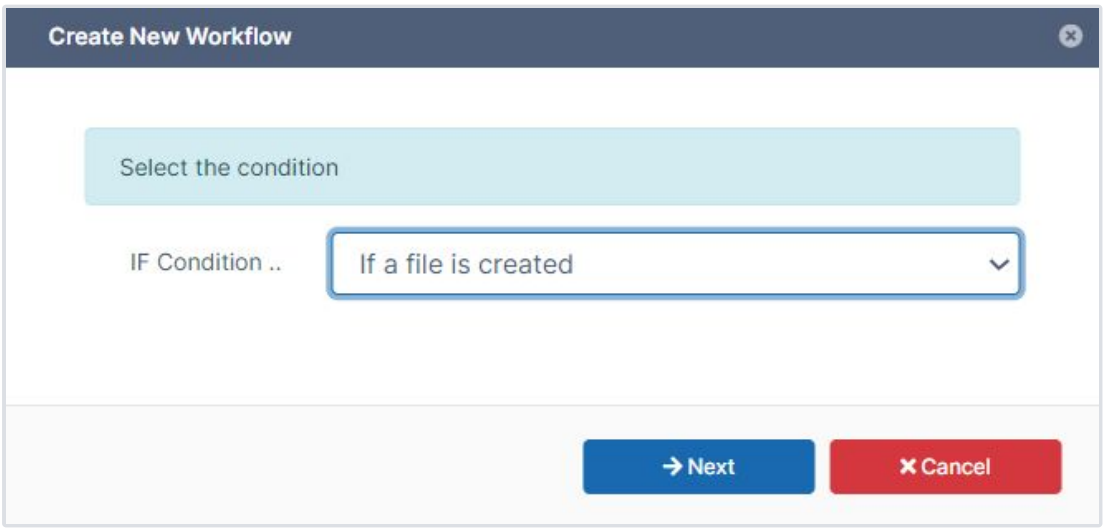
When you create a workflow, you must select a condition to act as a trigger.

- Depending on the trigger, additional parameters may be required.

- Once a Condition is selected, compatible Actions can be selected.

**Where do I set up the condition?**

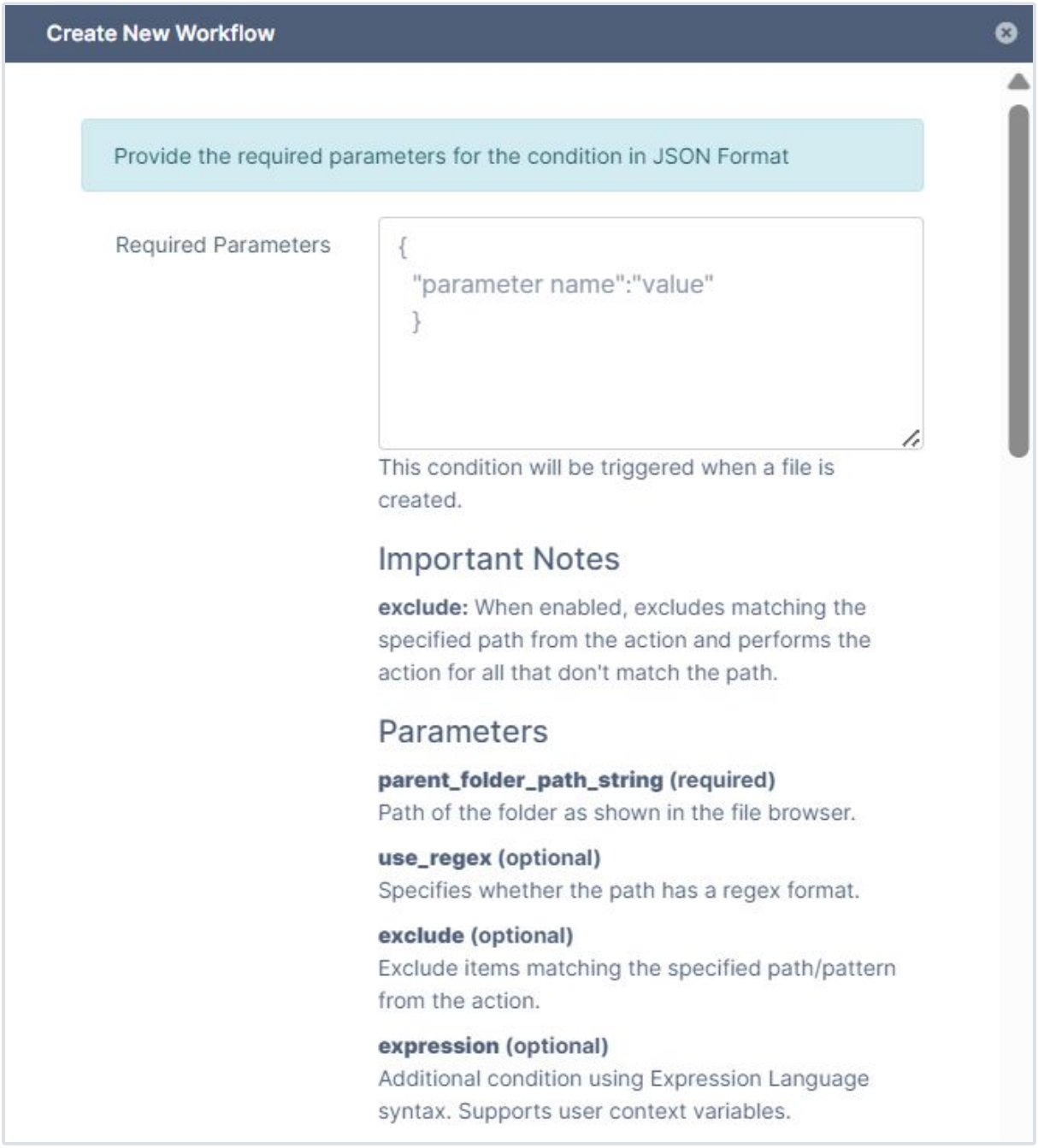
When you create a new Workflow, you will be able to select a condition.




**Where do I add my parameters?**

After you select a Condition, then you can enter any parameters, such as a date or time.

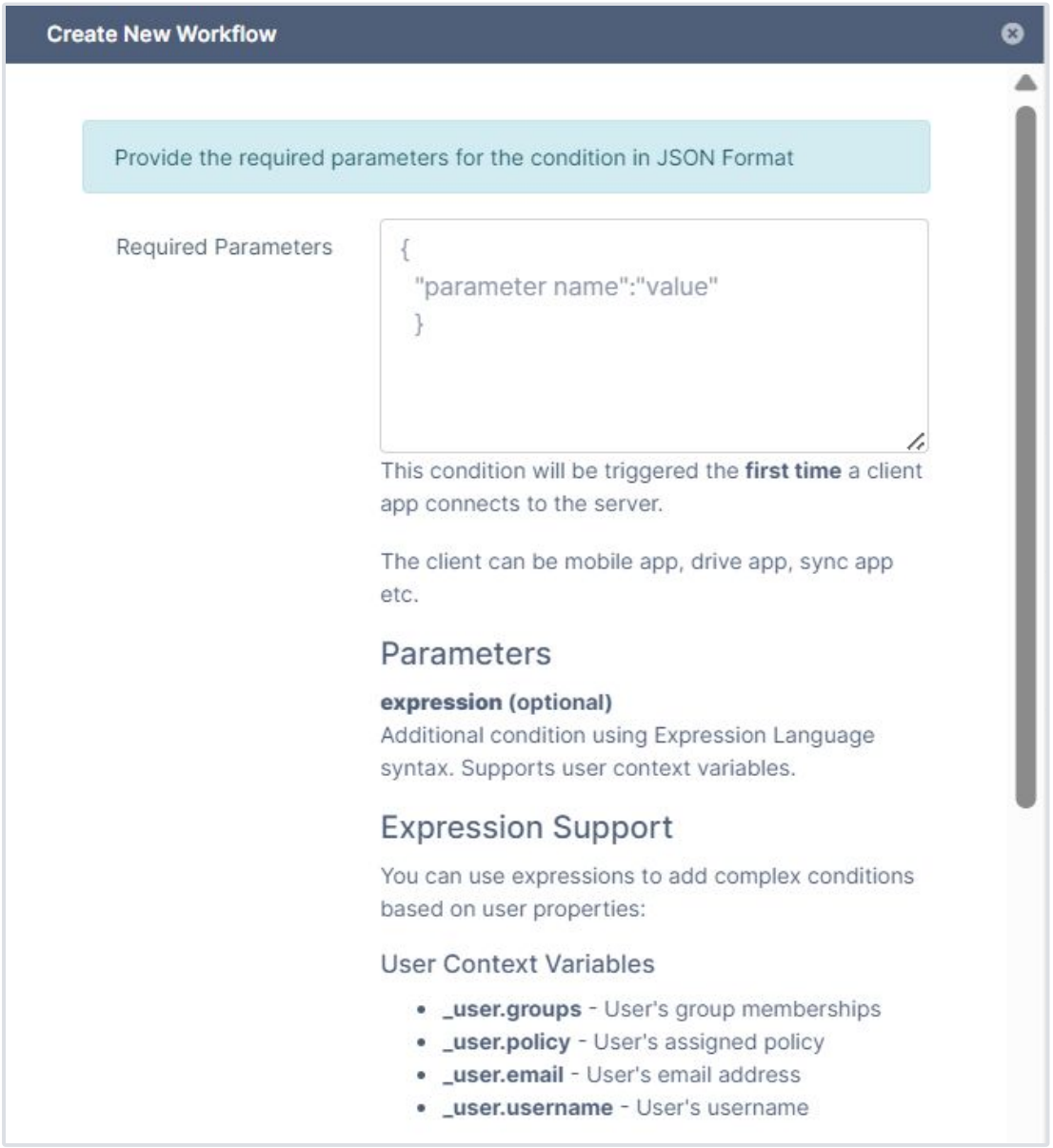
If you need more information about what parameters are required, look below the Required Parameters box.




## Available Conditions

### Client App Conditions

**If any new client app connects**

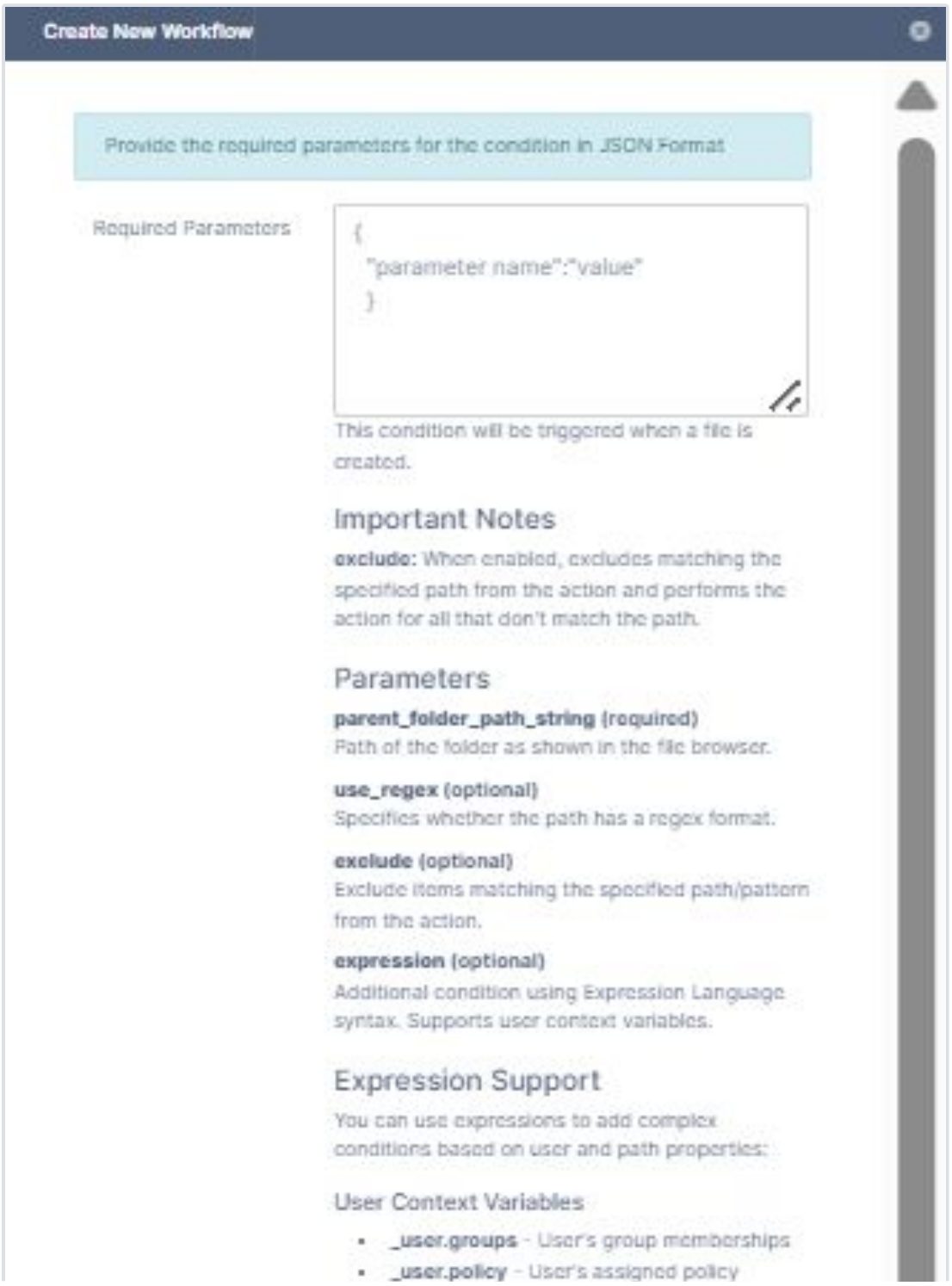


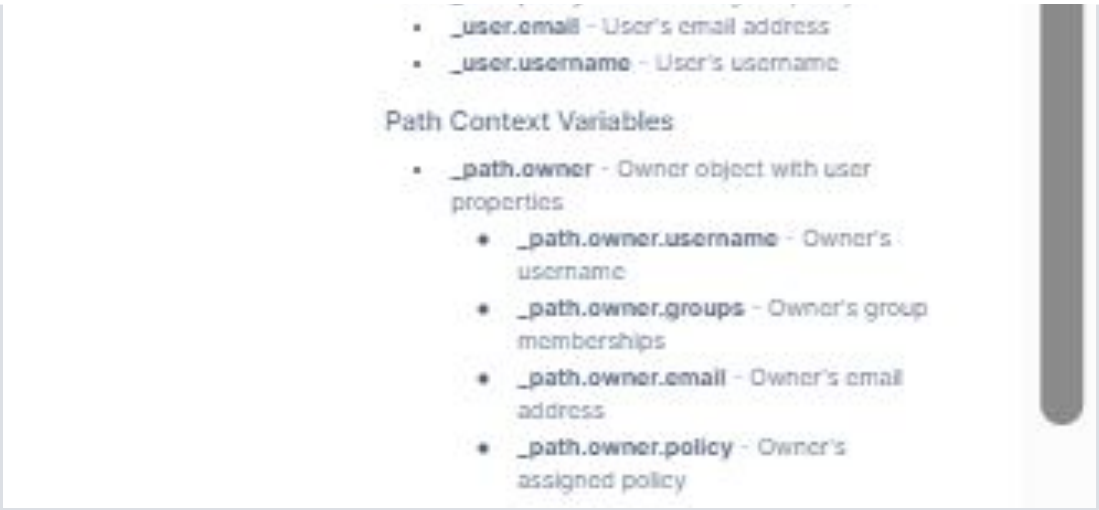

| Workflow Condition | Parameters | Description |
|---|---|---|
| If any new client app connects | **No parameters required** | This condition is triggered when an external (non-browser) client connects to FileCloud Server.<br>For example, this condition will trigger for clients such as:<br>• FileCloudSync<br>• FileCloudDrive<br>• iOS<br>• Android App |

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

## File Conditions

**If a file is created**






| Workflow Condition | Parameters | Description |
|---|---|---|
| If a file is created | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered if a file is created via any means (Browser, Clients, etc.)<br>**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 (see page 275).<br>**use_regex (optional)** - specifies how the folder path is validated.<br>• 0 or unspecified = use an exact match for the parent folder path string<br>• 1 = use a regular expression match for the parent folder path string<br>**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 (see page 397)

**If a file is updated**

| Workflow Condition | Parameters | Description |
|---|---|---|

| | | |
|---|---|---|
| If a file is updated. | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered if a file is updated.<br>**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 (see page 275).<br>**use_regex (optional)** - specifies how the folder path is validated.<br>• 0 or unspecified = use an exact match for the parent folder path string<br>• 1 = use a regular expression match for the parent folder path string<br>**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 (see page 397)

**If a file is deleted**

| Workflow Condition | Parameters | Description |
|---|---|---|
| If a file is deleted | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered if a file is deleted.<br>**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 (see page 275).<br>**use_regex (optional)** - specifies how the folder path is validated.<br>• 0 or unspecified = use an exact match for the parent folder path string<br>• 1 = use a regular expression match for the parent folder path string<br>**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 (see page 397)
Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

**If file is downloaded**

| Workflow Condition | Parameters | Description |
|---|---|---|

| | | |
|---|---|---|
| If a file is downloaded | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered if a file is downloaded<br>**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 (see page 275).<br>**use_regex (optional)** - specifies how the folder path is validated.<br>• 0 or unspecified = use an exact match for the parent folder path string<br>• 1 = use a regular expression match for the parent folder path string<br>**exclude (optional)** - specifies the system should only perform the action on non-matching paths (do not perform the action on matching paths). |

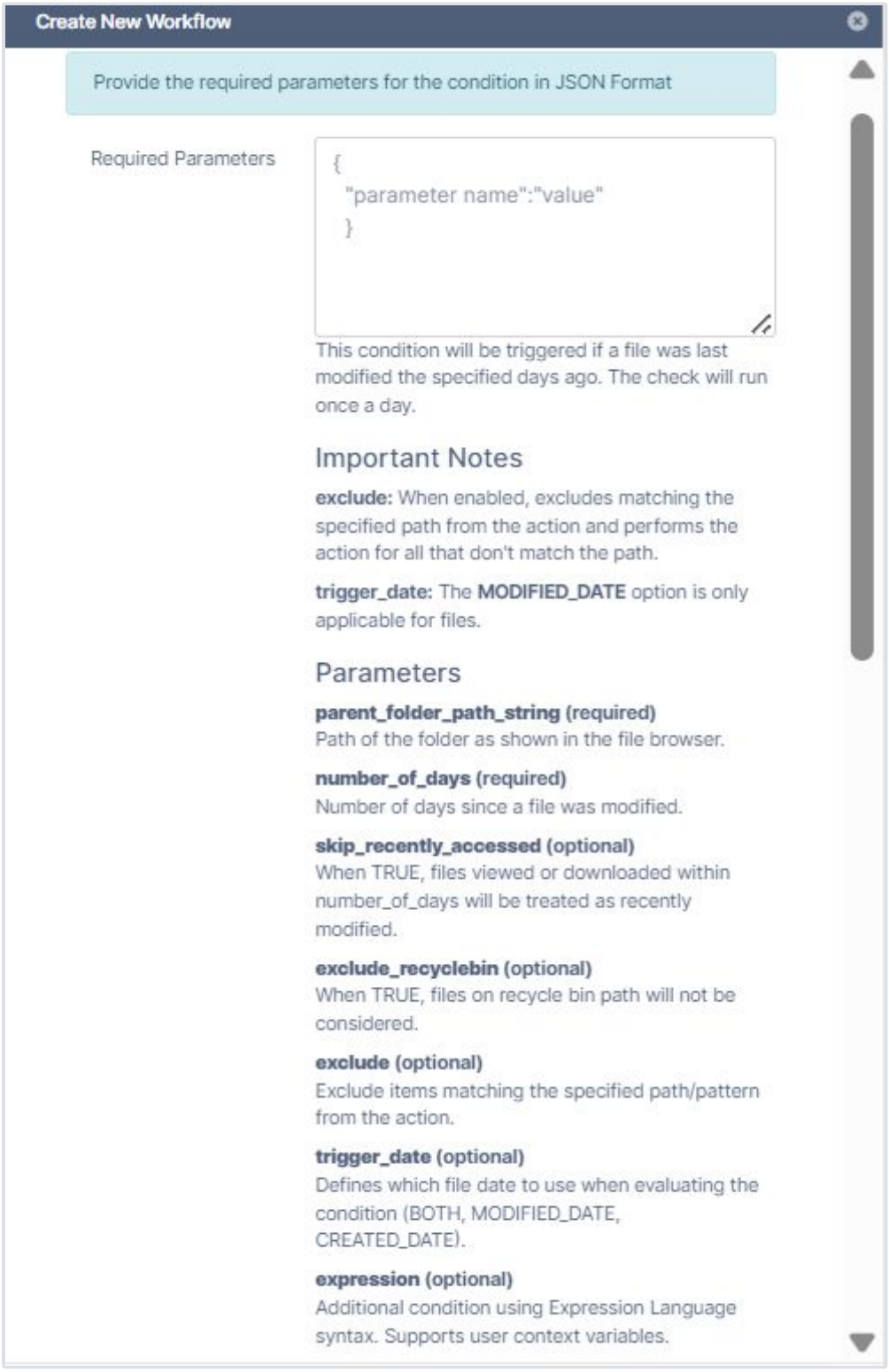
Available expression variables: **User Context variables**, **Path Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

**If a file is added or updated**

| Workflow Condition | Parameters | Description |
|---|---|---|
| If a file is added or updated | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered if a file is added or updated<br>**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 (see page 275).<br>**use_regex (optional)** - specifies how the folder path is validated.<br>• 0 or unspecified = use an exact match for the parent folder path string<br>• 1 = use a regular expression match for the parent folder path string<br>**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 (see page 397)

**If file was not modified/created in specified days**

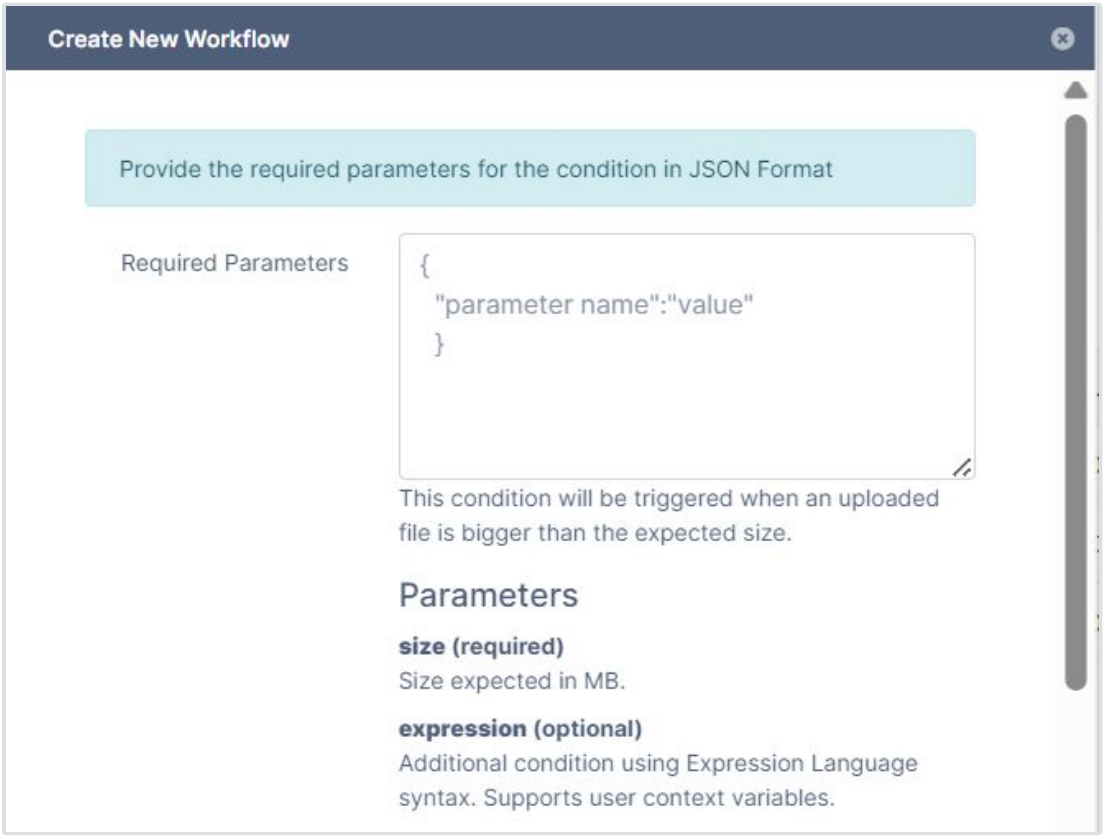



| Workflow Condition | Parameters | Description |
|---|---|---|

| | | |
|---|---|---|
| If a file was not modified/ created in specified days | `{ "parent_folder_path_string": "/johndoe", "number_of_days": 7, "skip_recently_accessed": 1, "exclude_recyclebin": 1, "exclude": ".*secret.*" }` | This condition will be triggered if a file was not created [specified days] ago or has not been updated for [specified days].<br>• This is useful for removing old files that are no longer being used<br>• This check will run once a day<br>**parent_folder_path_string** - required as a parameter for this condition to trigger.<br>• 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 (see page 275).<br>• NOTE: ONLY Managed storage paths are supported for this condition.<br>**number_of_days** - required to specify the number of days before the current date that a file was last modified.<br>• This will be checked once a day and all files that match this condition will be subject to the THEN action you choose.<br>• 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.<br>**skip_recently_accessed** - required to specify whether files that were viewed or downloaded during the number of days are considered modified. Default is *false*, viewed or downloaded files are not considered recently modified. When *true*, files viewed or downloaded within number_of_days are considered modified and will not be included in the *Then* action.<br>**exclude_recyclebin** - (added in FileCloud version 21.3) optional (default is false) When true, files in recycle bin are not considered.<br>**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).<br>**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:<br>BOTH - (default) Check if the CREATED_DATE and the MODIFIED_DATE are the specified number of days ago or more.<br>CREATED_DATE - Check if the CREATED_DATE is the specified number of days ago or more.<br>MODIFIED_DATE - Check if the CREATED_DATE is the specified number of days ago or more. |

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

**If the file uploaded is bigger than the expected size**




| Workflow Condition | Parameters | Description |
|---|---|---|
| If the file uploaded is bigger than expected size. | *{ "size":"4" }* | This condition will be triggered when an uploaded file is bigger than the size specified.<br>**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 (see page 397)

**If the file downloaded is bigger than the expected size**

| Workflow Condition | Parameters | Description |
|---|---|---|
| If the file downloaded is bigger than expected size. | *{ "size":"4" }* | This condition will be triggered when a downloaded file is bigger than the size specified.<br>**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 (see page 397)

## Folder Conditions

**If a folder is created**

| Workflow Condition | Parameters | Description |
|---|---|---|
| If a folder is created | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered when a folder is created in the system<br>**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 (see page 275).<br>**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")<br>**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 (see page 397)

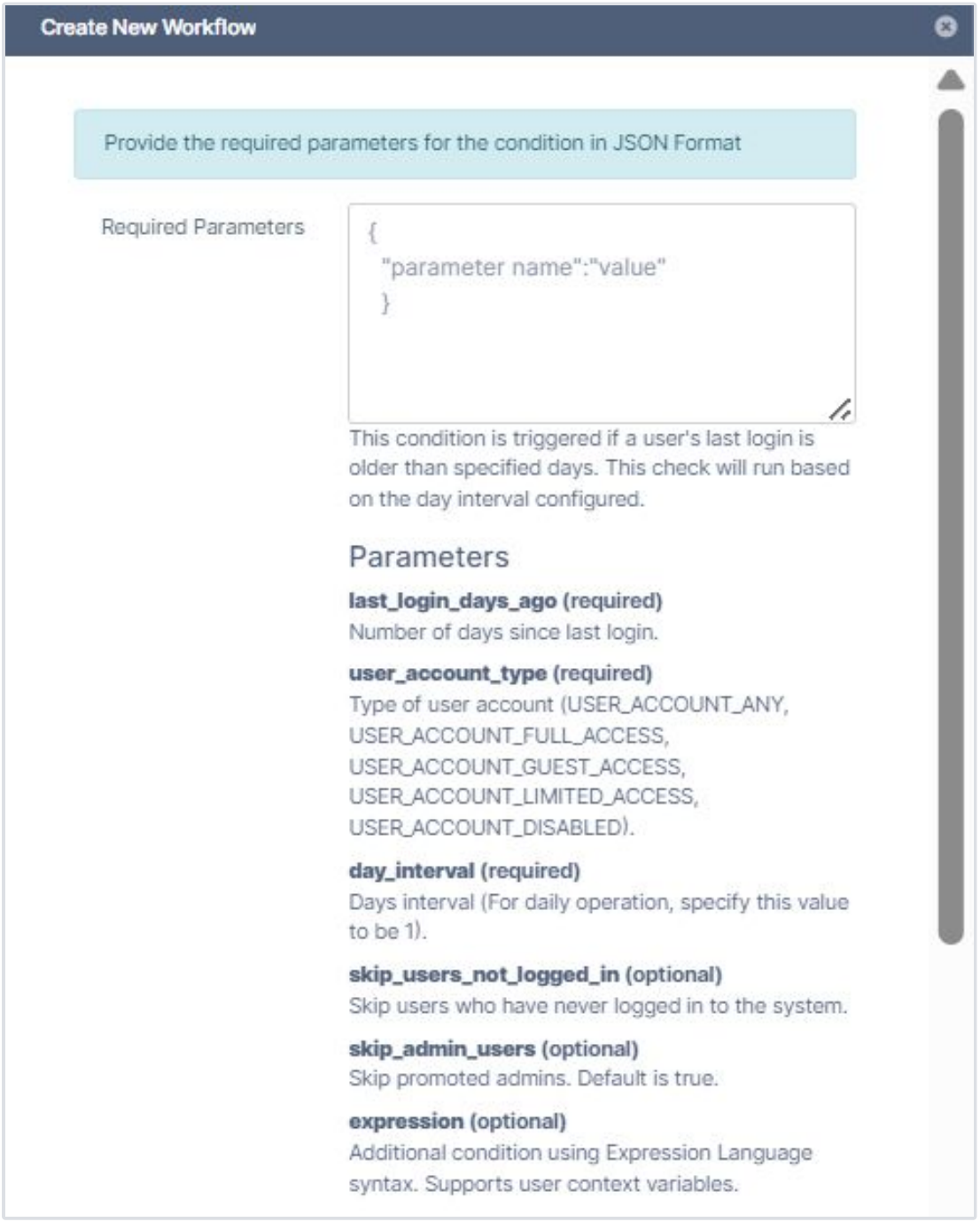
**If a folder is deleted**

| Workflow Condition | Parameters | Description |
|---|---|---|
| If a folder is deleted | *{ "parent_folder_path_string":"/userid/somepath", "use_regex":"1", "exclude":"1" }* | This condition will be triggered when a folder is deleted<br>**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 (see page 275).<br>**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")<br>**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 (see page 397)

## User Account Conditions

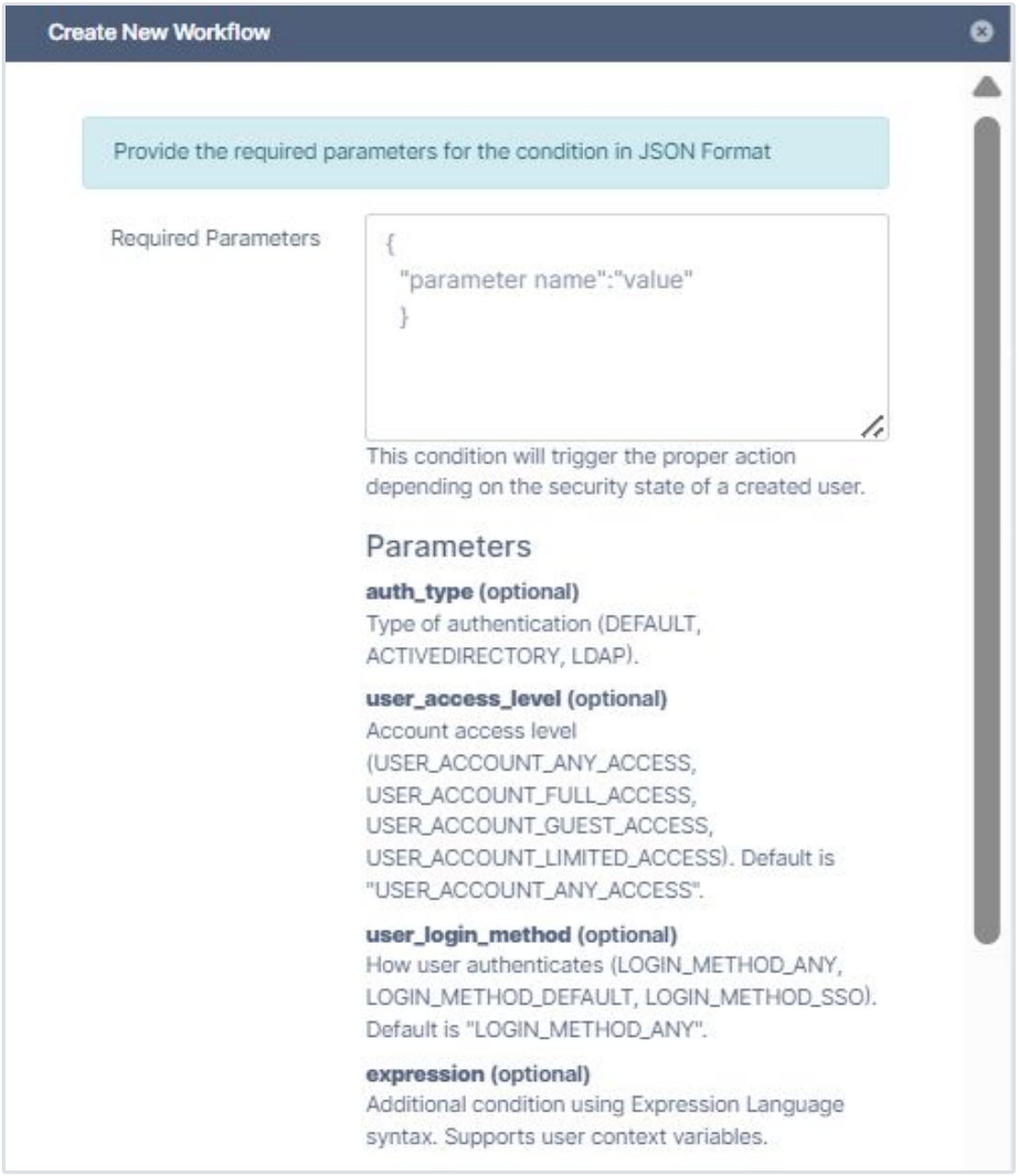
**If a user's last login is older than...**


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.

<table>
<tr><th></th><th>Workflow Condition</th><th>Parameters</th><th>Description</th></tr>
<tr><td>If a user's last login is older than ...</td><td>{</td><td>"last_login_days_ago": 30,<br>"user_account_type":<br>"USER_ACCOUNT_LIMITED_ACCESS",<br>"day_interval": 1,<br>"skip_users_not_logged_in": 1,<br>"skip_admin_users": 0,<br>"include_domain": "domain.com",<br>"exclude_domain":<br>"subdomain.domain.com,@otherdomain.com"<br>}<br><br>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.<br>{ "last_login_days_ago": 30,<br>"user_account_type":<br>"USER_ACCOUNT_FULL_ACCESS",<br>"day_interval": 1,<br>"skip_users_not_logged_in": 1,<br>"skip_admin_users": 1,<br><br>}</td><td>If a user's last login is older than the specified number of days, then the THEN condition you configure will be run.<br>last_login_days_ago: Number of days since last login.<br>user_account_type - type of account. You must use one of the following values:<ul><li>USER_ACCOUNT_ANY</li><li>USER_ACCOUNT_FULL_ACCESS</li><li>USER_ACCOUNT_GUEST_ACCESS</li><li>USER_ACCOUNT_LIMITED_ACCESS (for external users)</li><li>USER_ACCOUNT_DISABLED</li></ul>day_interval - the number of days between checks<ul><li>For daily operation, specify a value of 1</li></ul>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.<br>skip_admin_users (added in FileCloud 23.251) Optional. Do not include promoted admins.<br>0 (default) - Include promoted admins<br>1 - Do not included promoted admins</td></tr>
</table>

Available expression variables: **User Context variables**.
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

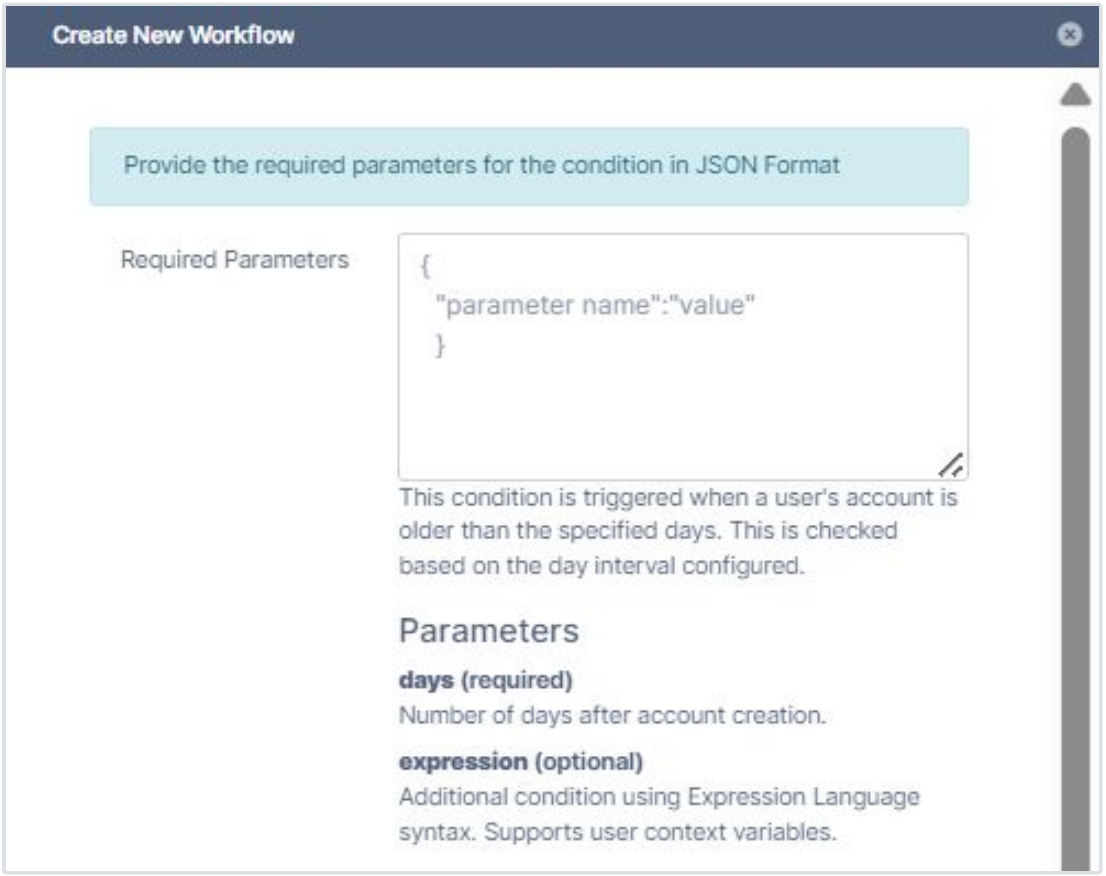
**If a new user is created**


Create New Workflow
Provide the required parameters for the condition in JSON Format
Required Parameters
{
"parameter name":"value"
}
This condition will trigger the proper action depending on the security state of a created user.
Parameters
auth_type (optional)
Type of authentication (DEFAULT, ACTIVEDIRECTORY, LDAP).
user_access_level (optional)
Account access level (USER_ACCOUNT_ANY_ACCESS, USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS). Default is "USER_ACCOUNT_ANY_ACCESS".
user_login_method (optional)
How user authenticates (LOGIN_METHOD_ANY, LOGIN_METHOD_DEFAULT, LOGIN_METHOD_SSO). Default is "LOGIN_METHOD_ANY".
expression (optional)
Additional condition using Expression Language syntax. Supports user context variables.

| Workflow Condition | Parameters | Description |
|---|---|---|
| If a new user is created ... | *None* | When a new user account is created, the THEN action you configure will be triggered.<br>Optional Parameters<br>**auth-type** - Type of authentication. This is **optional** and can be:<br>• DEFAULT<br>• ACTIVEDIRECTORY<br>• LDAP<br>**user_access_level:** Account access level. This is **optional** and can be:<br>• USER_ACCOUNT_ANY_ACCESS (default)<br>• USER_ACCOUNT_FULL_ACCESS<br>• USER_ACCOUNT_GUEST_ACCESS<br>• USER_ACCOUNT_LIMITED_ACCESS (for external users)<br>**user_login_method:** How user authenticates. This is **optional** and can be:<br>• LOGIN_METHOD_ANY (default)<br>• LOGIN_METHOD_DEFAULT<br>• LOGIN_METHOD_SSO |

Available expression variables: **User Context variables** (_user.email, _user.username)
For instructions on including expressions, see Using Expressions in IF Conditions (see page 397)

**If a user's account is older than**

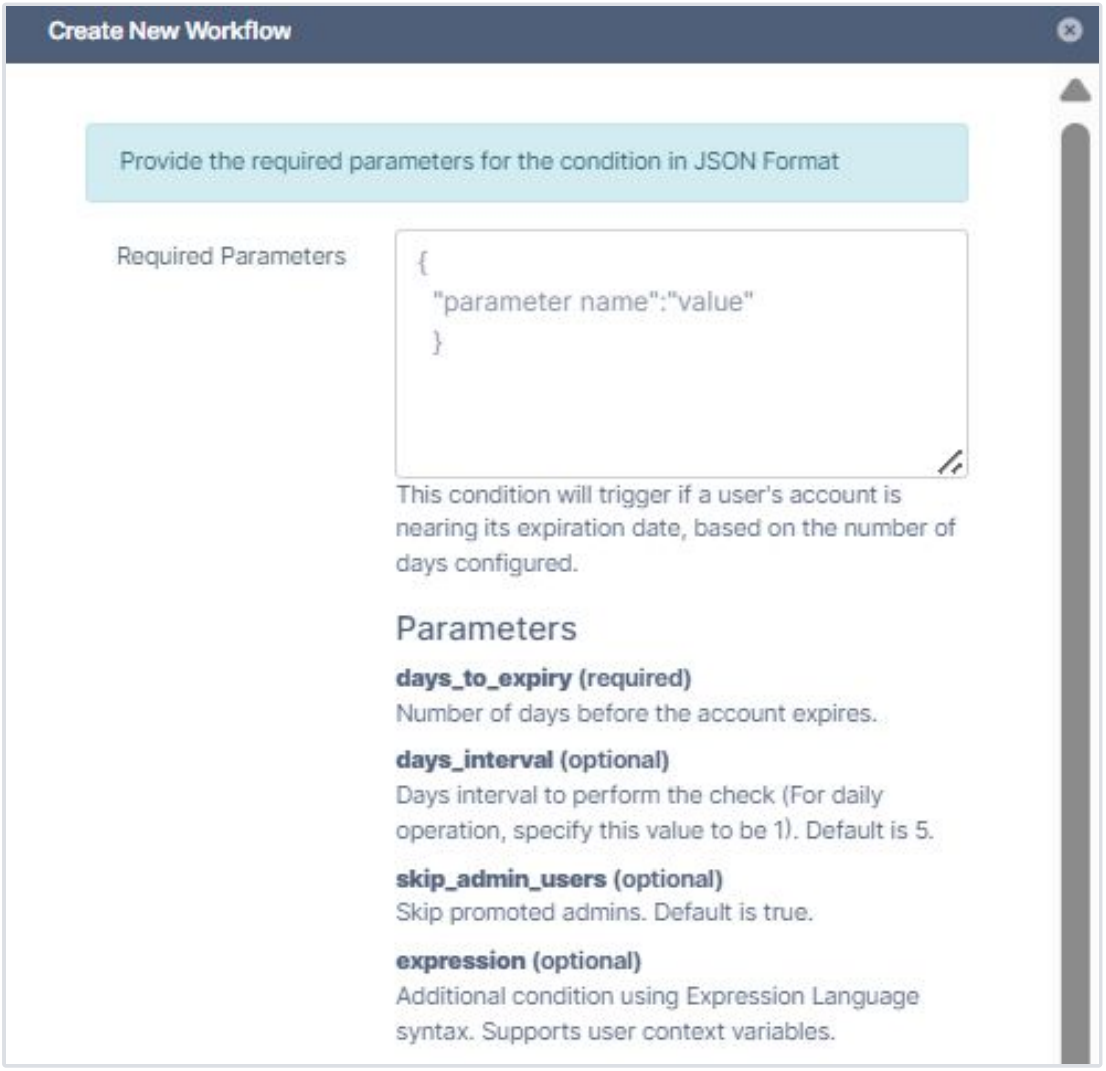



| Workflow Condition | Parameters | Description |
|---|---|---|

| | | |
|---|---|---|
| If a user's create date is older than<br><br>Available in FileCloud Version 23.232 | `{`<br>`"days": 30,`<br>`"include_domain": "contractor.com",`<br>`"exclude_domain": "subdomain.domain.com,@otherdomain.com"`<br>`}`<br><br>`For example, if a user's account was created more than 60 days ago and it is in the domain contractor.com`<br><br>`{`<br>`"days": 60,`<br>`"include_domain": "contractor.com",`<br>`}` | This condition is triggered when a user's create date is older than the number of days specified in **days**.<br>**Parameters**<br>**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 (see page 397)

**If a user's account is near its expiration date**

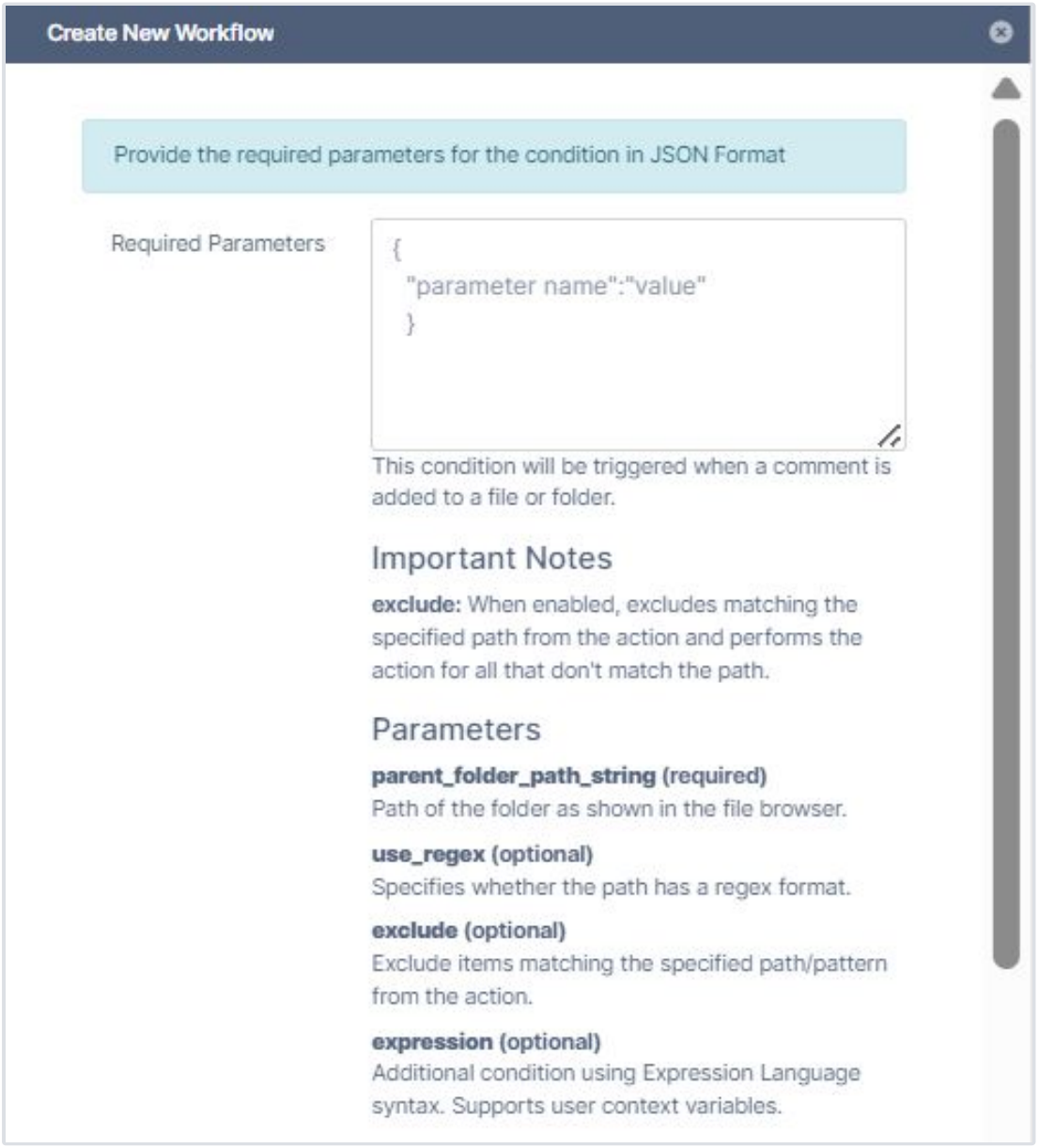

Create New Workflow
Provide the required parameters for the condition in JSON Format
Required Parameters
{
"parameter name":"value"
}
This condition will trigger if a user's account is nearing its expiration date, based on the number of days configured.
Parameters
days_to_expiry (required)
Number of 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>{<br>"days_to_expiry": 10,<br>"days_interval": 5,<br>"skip_admin_users": 1<br>}</pre><br>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.<br><pre>{<br>""days_to_expiry": 15,<br>"days_interval": 5,<br>"skip_admin_users": 1<br><br>}</pre> | **days_to_expiry** - Number of days before account expiration<br>**days_interval** - (optional)<br>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:<br>• Action is "Send an email"<br>• days_to_expiry = 15<br>• days_interval = 5<br>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.<br>**skip_admin_users** Optional. Do not include promoted admins.<br>0 (default) - Include promoted admins<br>1 - Do not included promoted admins<br>**Interval Logic**<br>During the last interval, the action is executed every day. For example:<br>• Action: "Send an email"<br>• days_to_expiry = 15<br>• days_interval = 5<br>An email is sent at 15 days before account expiration, 10 days before account expiration and 5, 4, 3, 2, and 1 days before account expiration. |

## Other Conditions

**If a comment is added**

**Comments can be added to files and folders.**




| Workflow Condition | Required Parameters | Description |
|---|---|---|

| | | |
|---|---|---|
| If a comment is added | *{*<br>*"parent_folder_path_string":"*<br>*/userid/somepath",*<br>*"use_regex":"1",*<br>*"exclude":"1"*<br>*}*<br>Available expression variables: **User Context variables**.<br>For instructions on including expressions, see Using Expressions in IF Conditions (see page 397) | This condition will be triggered when a comment is added<br>**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 (see page 275).<br>**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")<br>**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 (see page 397)

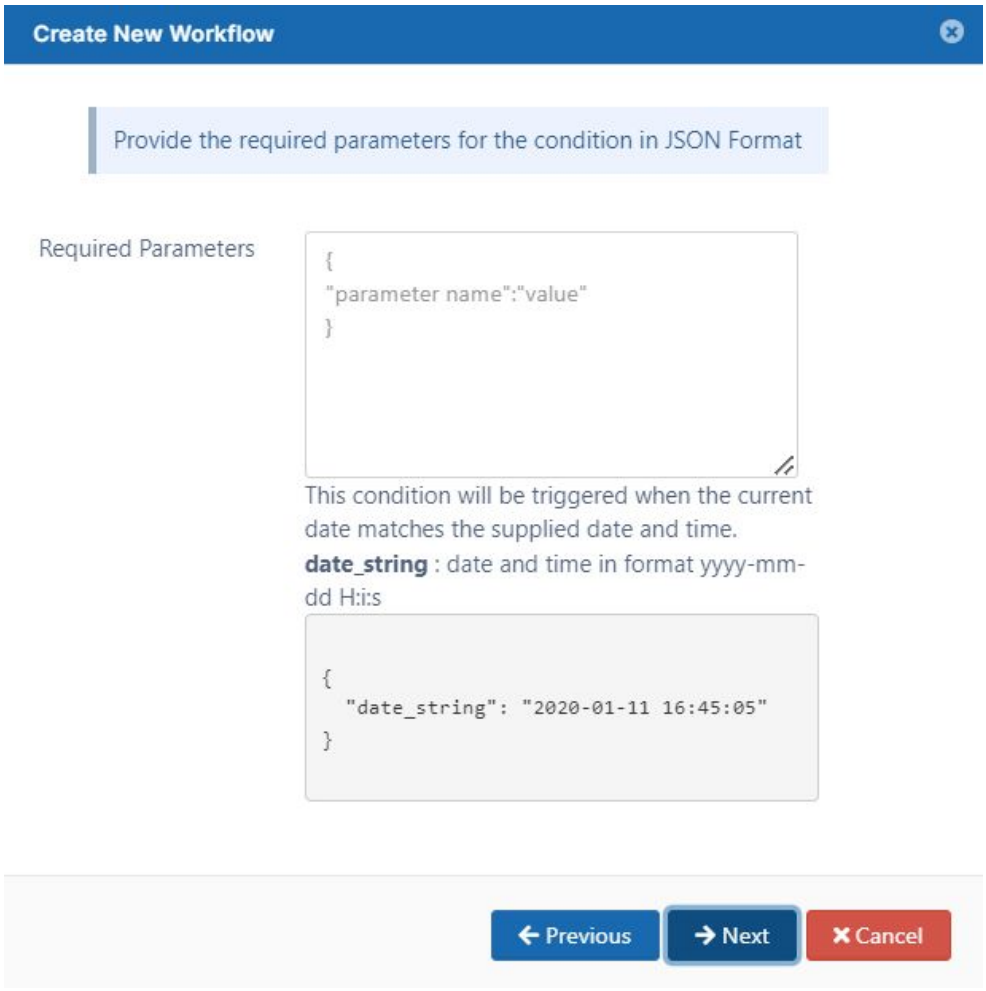
**Perform an action periodically at specified time and interval**

Create New Workflow
Provide the required parameters for the condition in JSON Format
Required Parameters
{
"parameter name":"value"
}
This condition will be triggered when the current time matches the supplied time.
day_interval : Days interval (For daily operation, specify this value to be 1)
time_string : (OPTIONAL) Time in format H:i:s (If not specified, it will run at 00:00:00)
start_date : (OPTIONAL) Start date in format yyyy-mm-dd (If not specified, it will start from today)
end_date : (OPTIONAL) End date in format yyyy-mm-dd (If not specified, it will run indefinitely)
{
"day_interval": 7,
"time_string": "08:00:00",
"start_date": "2020-01-01",
"end_date": "2020-01-31"
}
Previous
Next
Cancel

| Workflow Condition | Parameters | Description |
|---|---|---|
| Perform an action periodically at specified time and interval | *{ "time_string":"16:45:05", "day_interval":"7" }* | This condition will be triggered when the current time on the FileCloud Server matches the supplied time.<br>**day_interval** - number of days that passes after a THEN action before it is triggered again.<br>• The THEN action you choose will be triggered every "day_interval" days.<br>• If the "day_interval" is 1, it is done daily<br>**time_string** - the time of day when you want the THEN action triggered<br>• The matching time includes the time zone<br>• The time is specified in a 24-hour format of Hours, minutes, seconds<br>**start-date** - Date that FileCloud begins checking for the condition<br>**end-date** - Last date that FileCloud checks for the condition. |

Available expression variables: **None.**

**Perform an action on the specified date**




| Workflow Condition | Parameters | Description |
|---|---|---|
| Perform an action on the specified date | *{ "date_string":"2020-01-11" }* | When the date matches the supplied date and time, the THEN action you configure will be run.<br>**date_string** - date and time in a 24-hour format<br>• yyyy-mm-dd H:i:s |

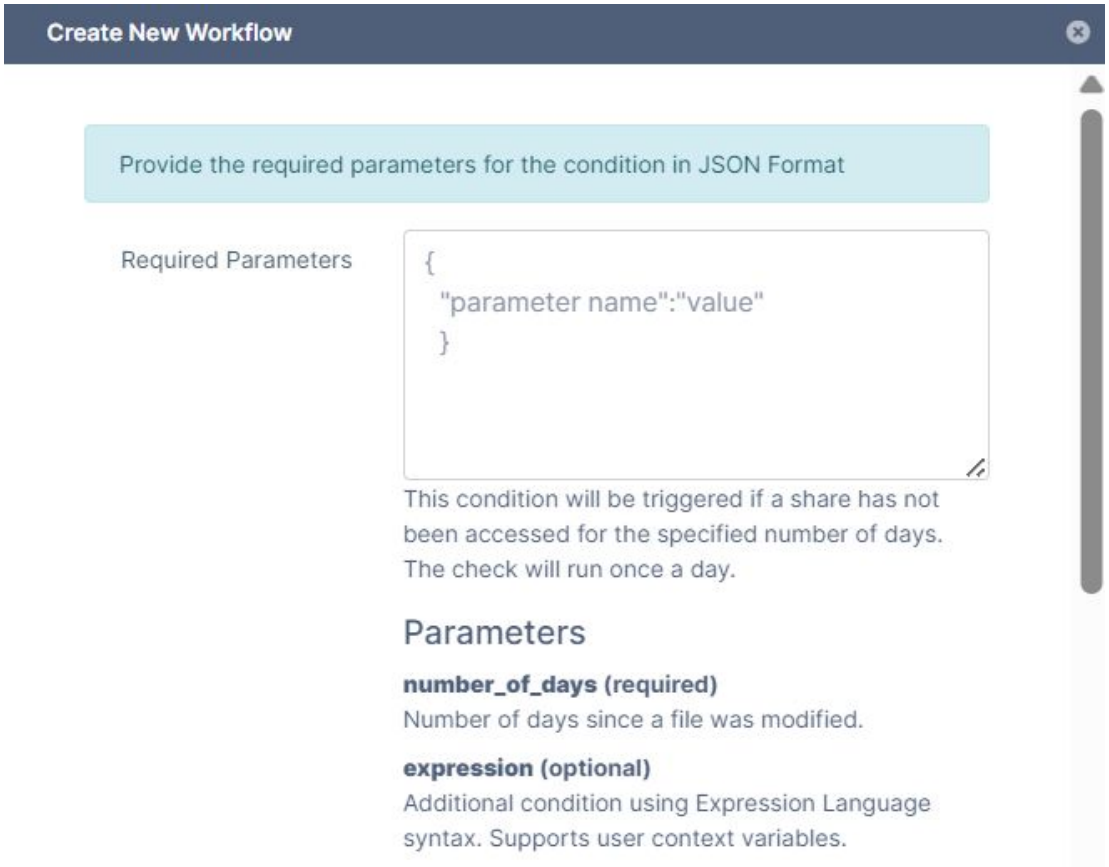
Available expression variables: **None.**

**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:<br>• cron job<br>• task scheduler |

Available expression variables: **None.**

**If share has not been accessed for specified days**




| Workflow Condition | Parameters | Description |
|---|---|---|
| If a share has not been accessed for specified days | *{ "share_permission": ["PUBLIC", "PRIVATE"], "number_of_days":"180", }* | This condition will be triggered when a shared file or folder has not been accessed for the specified number of days.<br>• NOTE: The only supported action is *Delete share*.<br>• This is useful for removing shared files that are no longer being used<br>• This check will run once a day<br>**number_of_days** - required to specify the number of days before the current date that a shared file was accessed.<br>• This will be checked once a day and all files that match this condition will be subject to the THEN action you choose.<br>• 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 (see page 397)

## Using Expressions in IF Conditions

Expressions are available in FileCloud beginning in version 23.253.

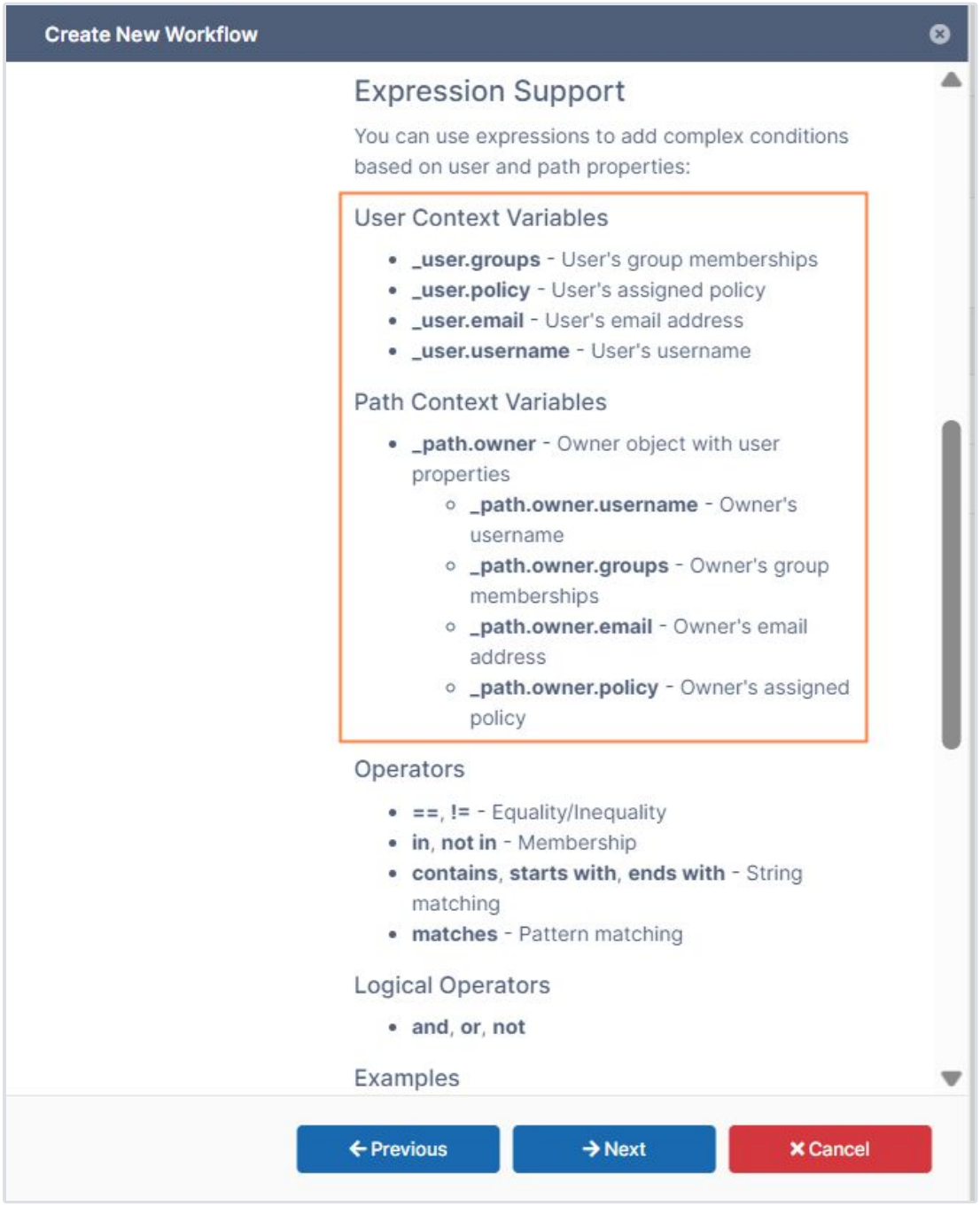
Many admin workflows allow you to set up custom conditions in workflows based on user, path owner, and share properties. These conditions (referred to as expressions) must be written in regular expression syntax. They greatly expand your ability to customize workflows.

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 (see page 403), below.
  As an example, in the following workflow, which uses the IF condition **If a file is added or updated**, the user and path context variables are supported, but not the share context variables. Below the variables, the available regular expression operators and examples are listed.



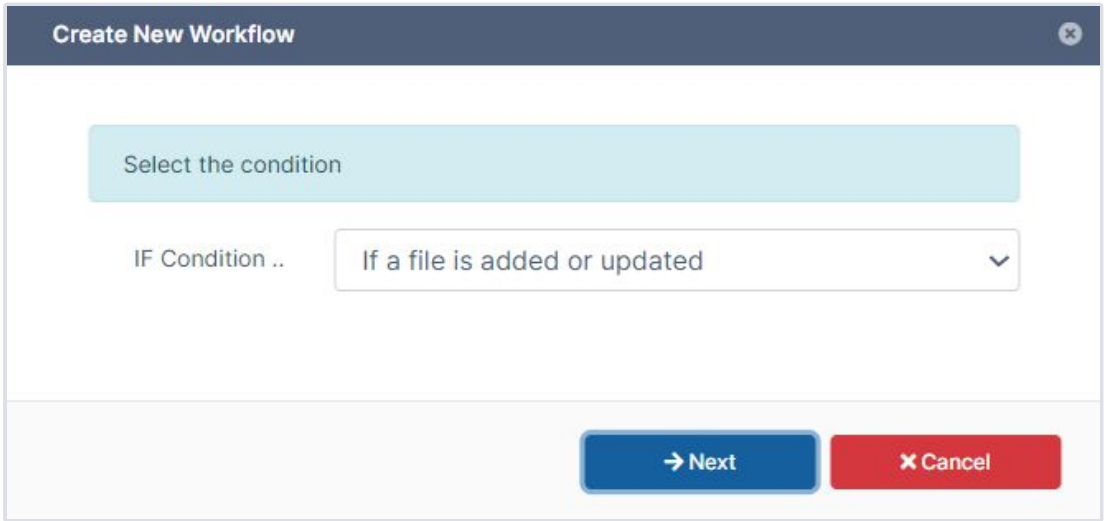

The examples help you use the proper syntax when adding conditions:

The variables available depend on the workflow, and not all workflows have variables available.

**To create an IF statement with an expression condition**

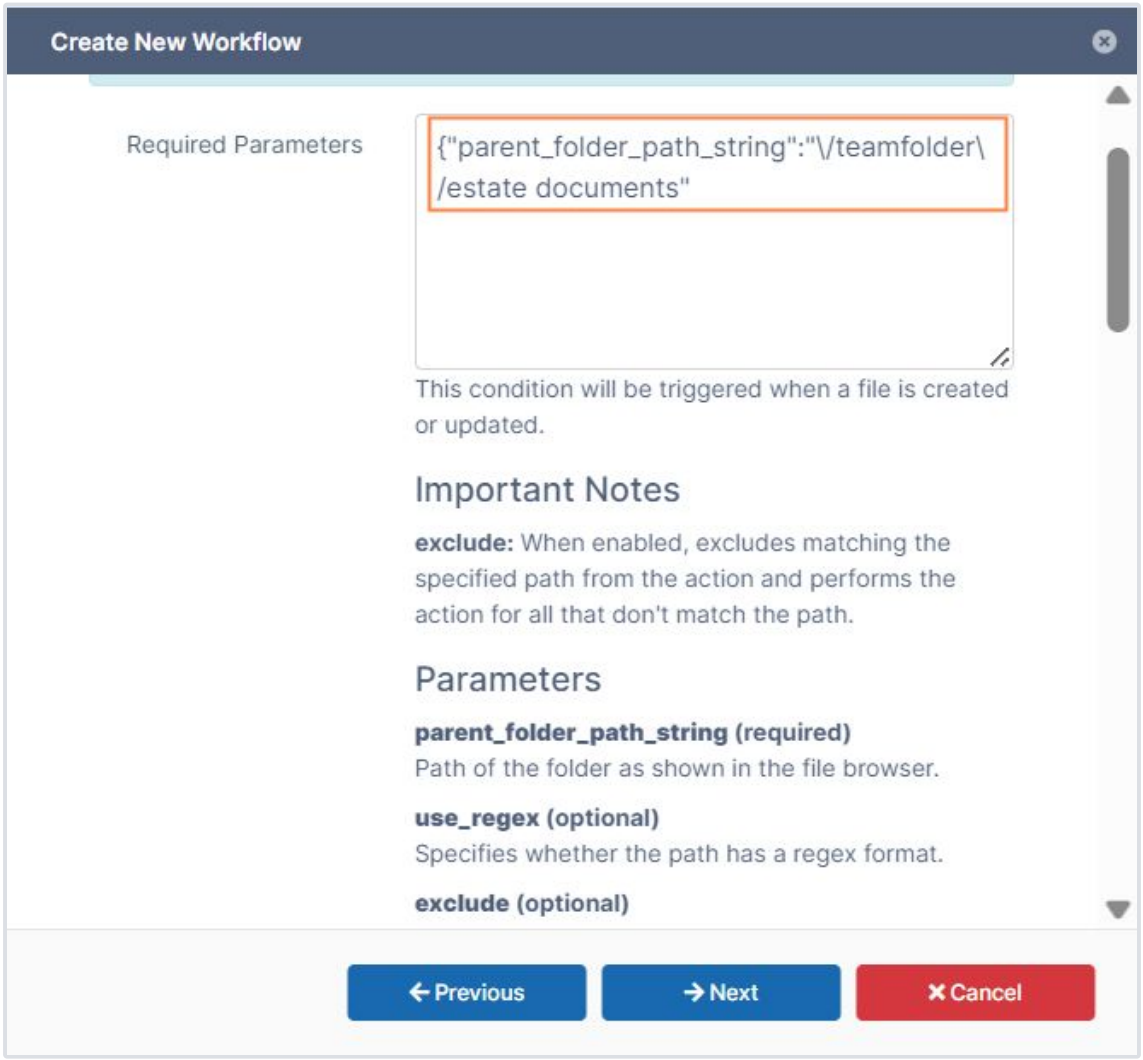
The IF statement we are setting up in this example uses an expression to specify a user's group and policy. The IF statement requires that the user who added or updated a file must also be in the group **TeamMember** and have the policy **Staff**.

1. In the admin portal, go to the Workflows page, and click **Add Workflow**.
2. In the Create New Workflow dialog box, choose an IF condition.
   This example uses the condition **If a file is added or updated**.

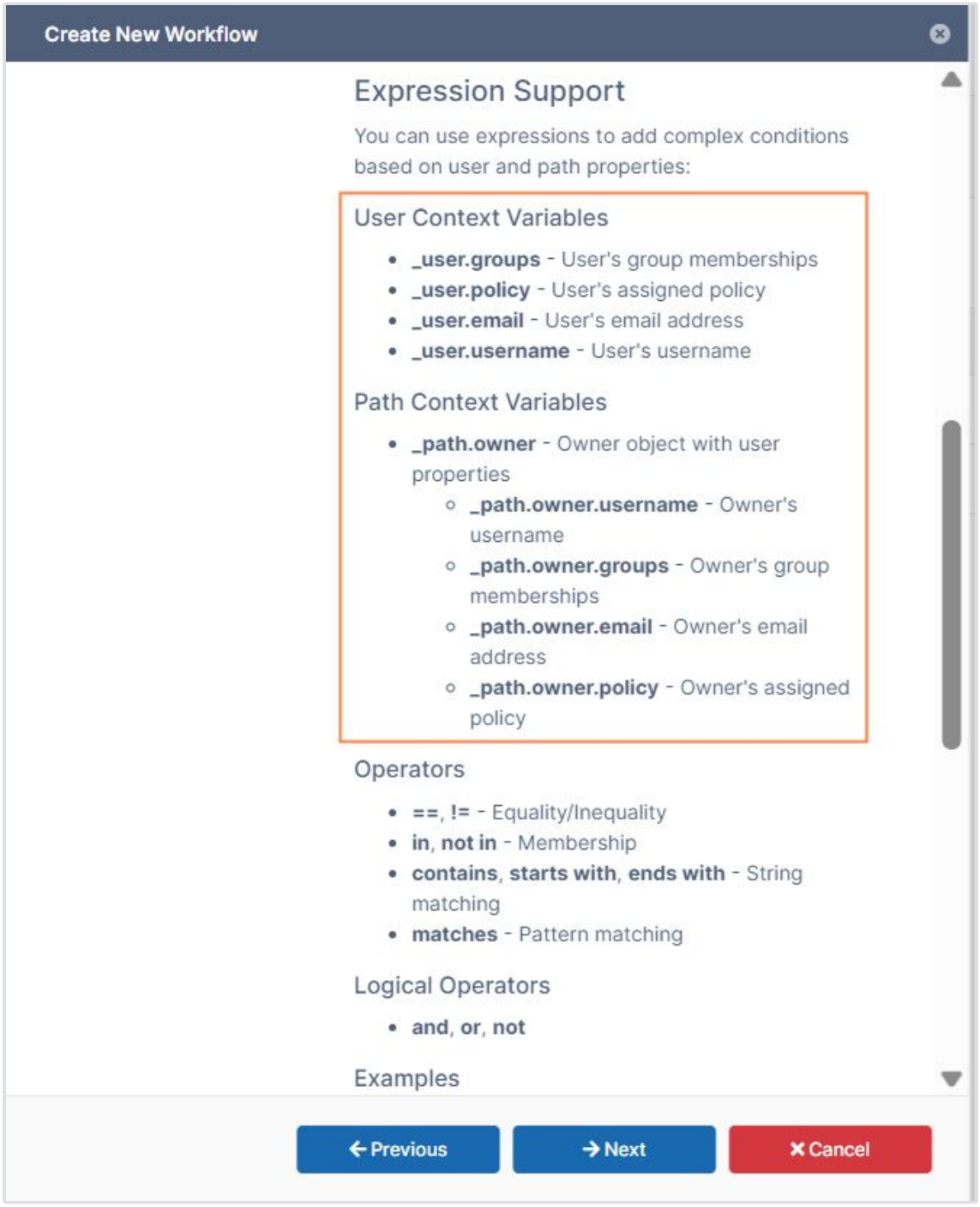



3. Click **Next**.

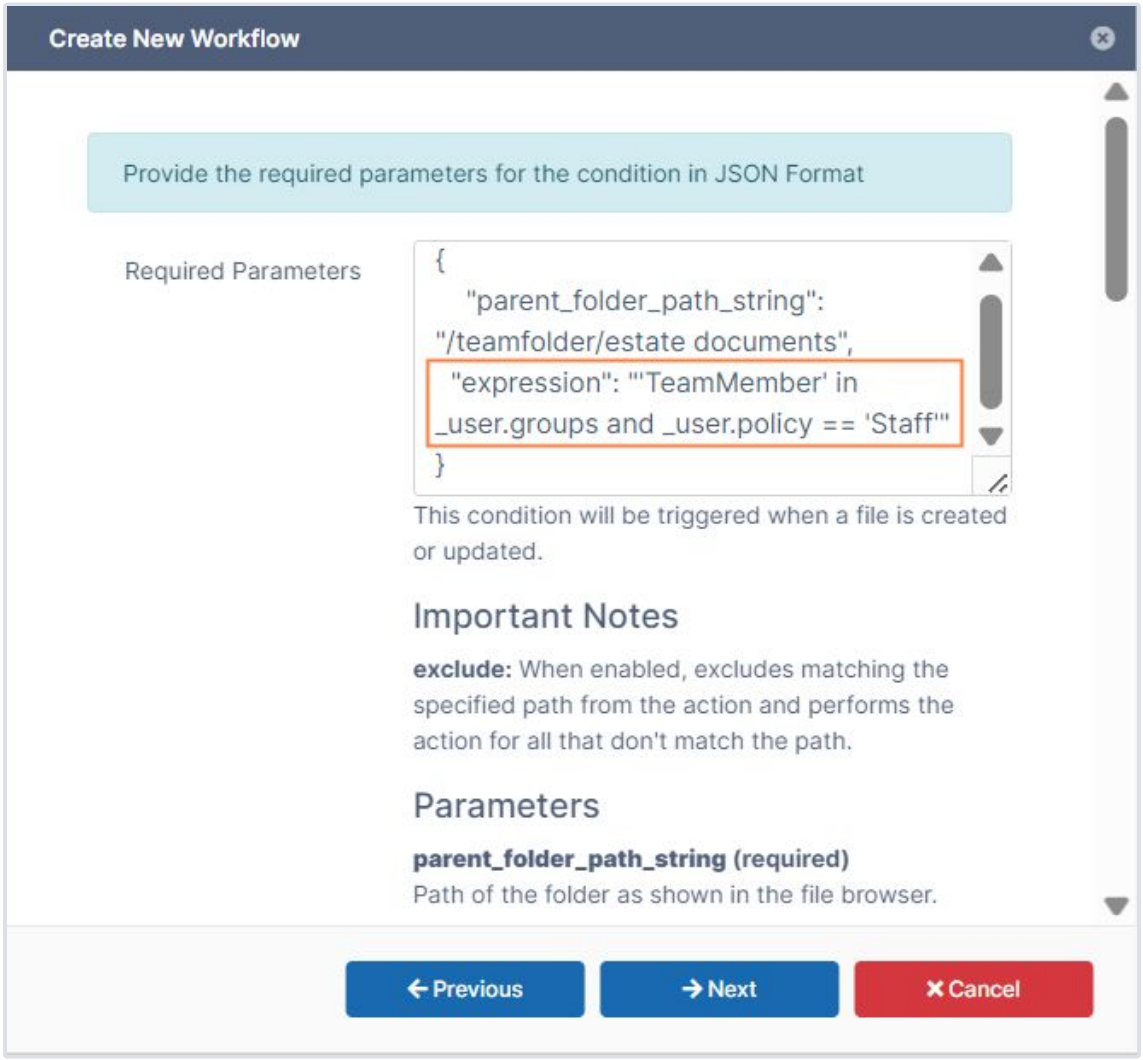
4. The only required parameter is **parent_folder_path_string**, so begin by entering it into the **Required Parameters** box.
   This example uses the Team Folder **estate documents**.



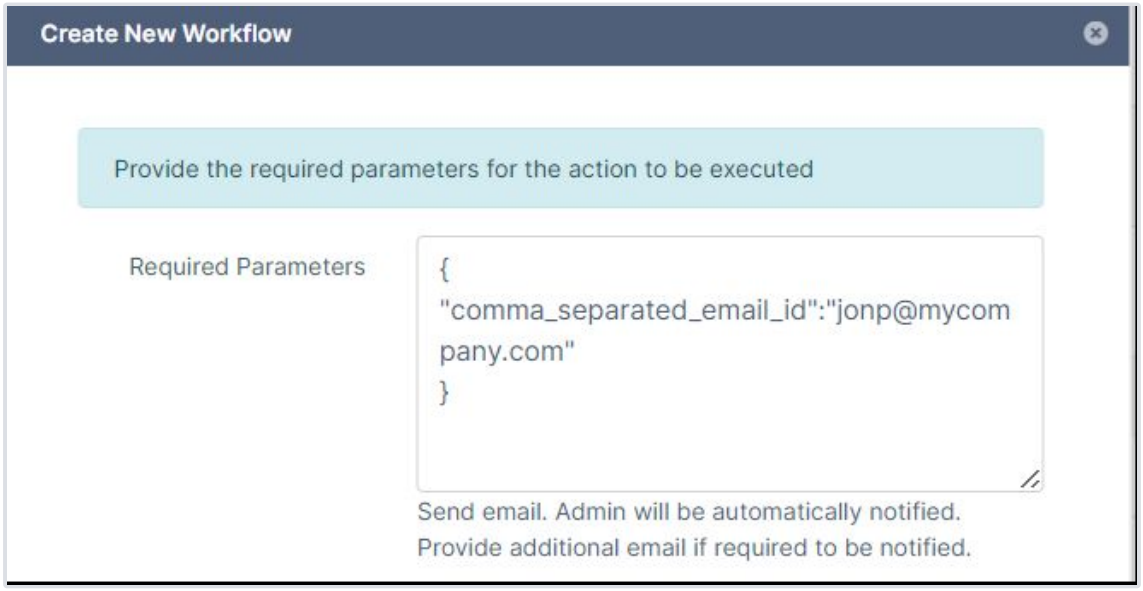

   Scroll down to **Expression Support** to see the supported context variables. In this case the user and path context variables are supported.
   To specify the user's group and policy, use the variables **_user.groups** and **user.policy**.



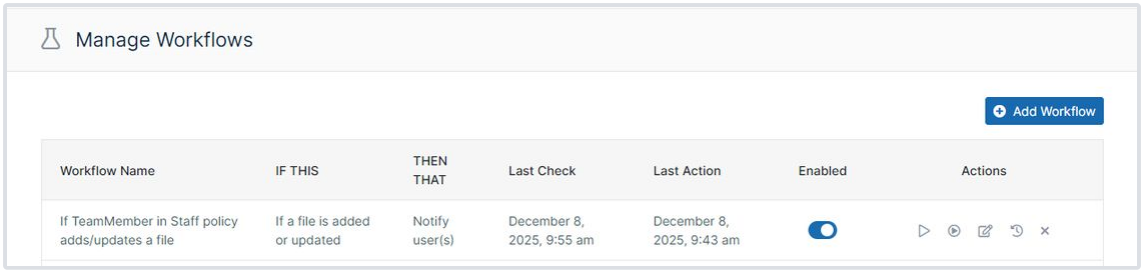

5. Add the variables and values.



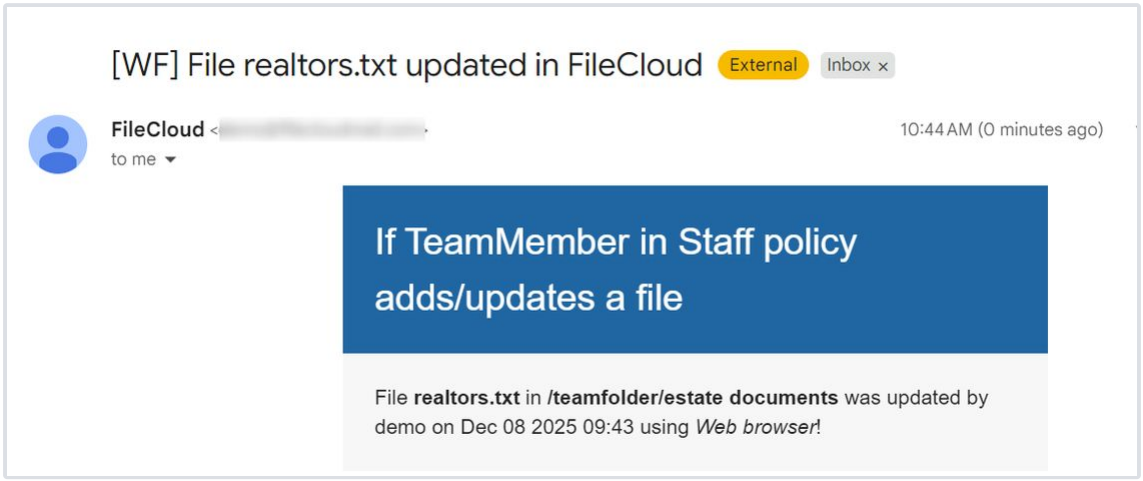

6. Click **Next**.
7. Choose the appropriate THEN action, and add the parameters.
   This example uses a THEN action that sends an email to a specific user, and specifies the user's email address.




8. Click **Next**, and enter a name for the workflow, then click **Finish**.
   The workflow is saved.




9. Test the workflow by having a user in the **TeamMember** group who has the policy **Staff** add or update a file in the Team Folder **estate documents**.
   The user specified will receive an email notification similar to the following one if the workflow is effective:




**Guide to expression variables and operators**

The tables below show the variables and operators supported in regular expressions when used with IF/THEN workflows in FileCloud. For examples using regular expression syntax with these variables and operators, see the wizard for adding each workflow.

| **User Context Variables** | |
|---|---|
| _user.groups | User's groups |
| _user.policy | User's policy |
| _user.email | User's email address |
| _user.username | User's username |
| **Path Owner Context Variables** | |
| _path.owner.username | Path owner's username |
| _path.owner.groups | Path owner's groups |
| _path.owner.email | Path owner's email |
| _path.owner.policy | Path owner's policy |
| **Share Context Variables** | |
| _share.owner.username | Share owner's username |
| _share.owner.groups | Share owner's groups |
| _share.owner.email | Share owner's email |
| _share.owner.policy | Share owner's policy |
| _share.public | If share is public, true; if share is not public, false. |
| _share.private | If share is private, true; if share is not private, false. |
| _share.is_dir | If this is a folder share, true; if this is a file share, false. |

| Operators | |
|---|---|
| ==, != | equal/not equal |
| in, not in | is a member of/is not a member of |
| contains, starts with, ends with | string contains, string starts with, string ends with |
| matches | pattern matches |

| Logical Operators |
|---|
| and |
| or |
| not |

## Define a THEN Action

Not all THEN actions are compatible with all IF conditions. Please see the table below for compatible settings.

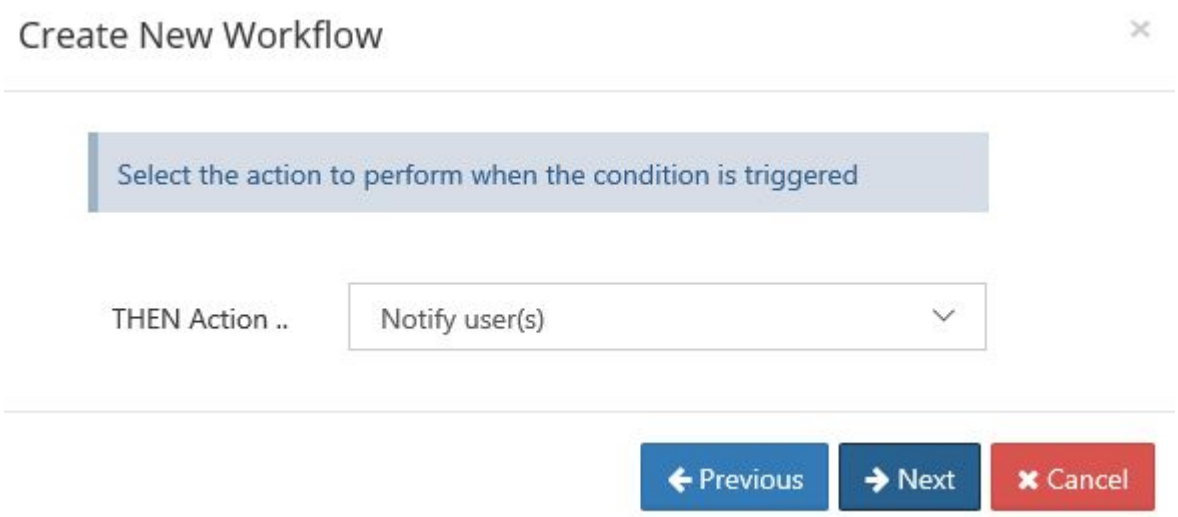
Once you select an IF Condition, compatible THEN Actions can be selected.

- Actions are performed if the associated Condition is triggered.

Some Actions may require you to specify parameters, such as a specific date or time.

**Where do I set up the Action?**

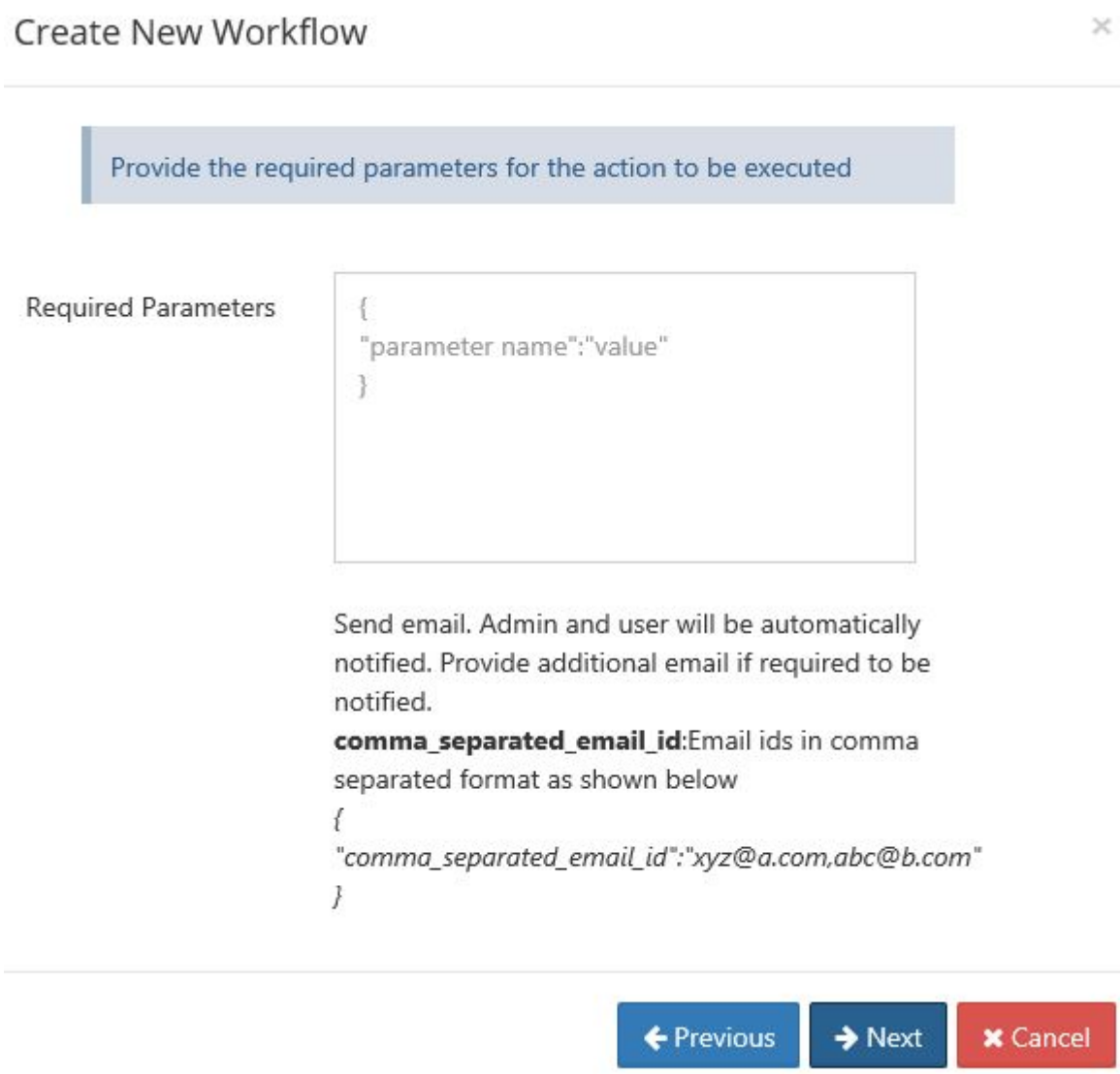
When you create a new Workflow, after you select a condition and specify parameters, then you can select an Action.




**Where do I add my parameters?**

After you select an Action, then you can enter any parameters, such as a date or time.

If you need more information about what parameters are required, look below the Required Parameters box.


Create New Workflow
Provide the required parameters for the action to be executed
Required Parameters
{
"parameter name":"value"
}
Send email. Admin and user will be automatically notified. Provide additional email if required to be notified.
comma_separated_email_id:Email ids in comma separated format as shown below
{
"comma_separated_email_id":"xyz@a.com,abc@b.com"
}
Previous
Next
Cancel

## THEN Actions

### Notifications

| Action and | | Details | Compatible IF conditions |
|---|---|---|---|
| Notify the user that the account may be deactivated soon | None | Notifies the user that the account may be disabled or deleted due to inactivity. | Click to see If conditions<br><br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |
| Notify user(s) | { "comma_separated_email_id":"xyz@a.com,abc@b.com", "comma_separated_group_name":"Group A,Group B" } | Sends a notification to users matching the criteria and sends an email to the admin and the specified addresses with information about the users who were sent notifications.<br>**comma_separated_email_id** - email ids in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format. | Click to see If conditions<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date<br>If a new client app connects<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created |

| Action and | | Details | Compatible IF conditions |
|---|---|---|---|
| Send an email | {<br>"subject": "Subject of the email",<br>"body": "Body of the email in HTML format.",<br>"is_html": 1,<br>"users": "user1,user2",<br>"groups": "group1,group2",<br>"notify": 0<br>} | Sends a customized email to the users and/or groups indicated<br>**subject** - Subject of the email<br>**body** - Body of the email<br>**is_html** (optional) - 1 if the body is in HTML format; 0 if the body is in plain text format. Default is 0.<br>**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.<br>**users** (optional) - Comma separated list of users to send the email to.<br>**groups** (optional) - Comma separated list of groups to send the email to.<br>**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.<br>If no users or groups are specified, the email is sent to the admin. | Click to see if conditions<br>If a file is created<br>If a folder is created<br>If a file is updated<br>If a file is deleted<br>If a folder is deleted<br>If a file is downloaded<br>If a comment is added<br>If a file was not modified for specified days<br>If a file is added or updated<br>If the file uploaded is bigger than the expected size<br>If the file uploaded is bigger than the expected size<br>Perform an action periodically at specified time and interval<br>Perform an action on the specified date<br>Perform an action periodically<br>If a new user is created<br>If a user's account is older than<br>If a user's last login is older than<br>If a user's account is near its expiration date |

## File actions

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Copy the file(s) to some location | { "target_path": "/usera/folderb/", "allow_overwrite": 1, "keep_folder_structure": 1 } | Copies files.<br>**target_path** - path to copy the file to.<br>• This path must be in the same storage type<br>• Files cannot be copied from managed storage to network shares or vice versa.<br>**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.<br>**keep_folder_structure** (Optional): Keep folder structure while copying files.<br>Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided.<br><br>The placeholders. %who, %when, %path, %how, %filename are available for this action. | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deleted<br>If a comment is added |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Delete the file(s) | { "delete_empty_folders":1, "notify_owner":0, "comma_separated_email_id":"email1@email.com,email2@email.com", "comma_separated_group_name":"Group A,Group B" } | Deletes matching files.<br>**delete_empty_folders (Optional)**: When files are deleted, delete the parent folder as well if it is empty.<br>**notify_owner (Optional)**: When the files are deleted, send an email to the owners.<br>**comma_separated_email_id (Optional)**: Email ids in comma separated format.<br>**comma_separated_group_name (Optional)**: Group names in comma separated format. | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deleted<br>If a comment is added |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Move the file(s) to some location | {<br>"target_path": "/usera/folderb/",<br>"allow_overwrite": 1,<br>"keep_folder_structure": 1<br>} | Moves files.<br>**target_path** - Path to the new file location (where it should be moved).<br>• This path must be in the same storage type<br>• Files cannot be moved from managed storage to network shares or vice versa.<br>**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.<br>**keep_folder_structure** (Optional): Keep folder structure while moving files.<br>Valid values are 0 (do not keep folder structure) or 1 (keep folder structure). Default is 0 if not provided.<br><br>The placeholders. %who, %when, %path, %how, %filename are available for this action. | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is deleted<br>If a comment is added |
| Release locks (added in FileCloud 22.1) | {<br>"days": 7<br>} | Releases locks on files and folders.<br>**days** - Number of days after a lock was created on a file or folder to release it. | Click to see if conditions<br>Perform an action periodically at specified time and interval<br>Perform an action on the specified date<br>Perform an action periodically<br>If a user's create date is older than |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Verify file integrity and generate admin alert on mismatch | { "ignore_file_size_in_mb": 10 } | Attempts to identify the file type based on its content and checks if it matches the extension.<br>• If the file type does not match, then generate admin portal alert.<br>Optional<br>**ignore_file_size_in_mb**: - Do not scan files larger than this limit specified in megabytes.<br><br>**Note:** By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check.<br>However, You may add additional allowable extensions for text files by adding the setting TONIDO_TEXT_FILE_EXTENSIONS to your cloudconfig file.<br>See File Content Heuristic Engine (see page 270). | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deletedIf a comment is added |

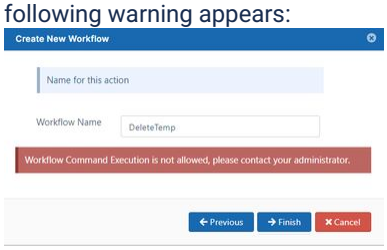
| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Verify file integrity and delete on mismatch | { "ignore_file_size_in_mb": 10 } | Attempts to identify file type based on its content and checks if it matches its mime type.<br>• A MIME type is a string identifier composed of two parts: a "type" and a "subtype".<br>• If the file type does not match, then<br>  • the latest version is deleted<br>  • users listed in the parameter are notified<br>Optional<br>**ignore_file_size_in_mb**: - Do not scan files larger than this limit specified in megabytes.<br><br>**Note:** By default, plain text files must have the extension txt, dat, log or csv to pass the integrity check.<br>However, You may add additional allowable extensions for text files by adding the setting TONIDO_TEXT_FILE_EXTENSIONS to your cloudconfig file.<br>See File Content Heuristic Engine (see page 270). | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deleted<br>If a comment is added |

## Reporting

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Run a report | { "report_name": "my_report", "comma_separated_email_id": "a@x.com,b@y.com", "comma_separated_group_name": "Group A,Group B" } | Opens a saved report, runs it, and then sends the results in email.<br>💡 This action requires you to have already created the report from the Admin dashboard.<br>Create a Custom Report (see page 277)<br>**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.<br>**comma_separated_email_id**: Comma separated email ids to be notified after report is run<br>**comma_separated_group_name (Optional)**: Group names in comma separated format. | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deleted<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date<br>If a comment is added<br>Perform an action periodically at specified time and interval<br>Perform an action on the specified date<br>Perform an action periodically |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Generate an email report | { "comma_separated_email_id":"xyz@a.com,abc@b.com", "comma_separated_group_name":"Group A,Group B" } | Sends an email to the specified addresses with information about the users matching the criteria. **comma_separated_email_id** - email ids in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format. | Click to see If conditions<br>If a user's last login is older than . . .<br>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)<br>If a user's create date is older than<br>If a user's account is near its expiration date |

## Running commands

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Execute a command | { "command_line":"rm -rf / tmp/scratch" } | Executes the command line.<br>**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 (see page 423).<br>The placeholders. %who, %when, %path, %how, %filename are available for this action.<br><br>Beginning in FileCloud 23.1, by default, the **Execute a command** action is not available for admin users.<br>If an admin user selects the action and tries to save the workflow, the following warning appears:<br>  <br>To enable admin users to choose the **Execute a command** option, add:<br>1. Open cloudconfig.php: Windows Location: XAMPP DIRECTORY/ htdocs/config/ cloudconfig.php Linux Location: / var/www/config/ cloudconfig.php<br>2. Add the following: | Click to see If conditions<br>If a file is created<br>If a file is updated<br>If a file is deleted<br>If a file is downloaded<br>If a file was not modified for specified days<br>If a file is added or updated<br>If a file uploaded is bigger than expected size<br>If a file downloaded is bigger than expected size<br>If a folder is created<br>If a folder is deleted<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a comment is added<br>Perform an action periodically at specified time and interval<br>Perform an action on the specified date<br>Perform an action periodically |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| | | define("TONIDOCLOUD_ALLOW_ADMIN_WORKFLOW_COMMAND_EXECUTION",1); | |

## Modifying users

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Disable user account | { "comma_separated_email_id":"xyz@a.com,abc@b.com", "comma_separated_group_name":"Group A,Group B", "donot_email_user": 0 } | Disables the user account and then sends an email with information about the action performed.<br>**comma_separated_email_id** - email IDs in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format.<br>**donot_email_user (optional)**: Do not send email to the user affected (1 or 0). Default 0.<br><br>**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<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Delete user account | { "comma_separated_email_id":"xyz@a.com,abc@b.com", "comma_separated_group_name":"Group A,Group B", "donot_email_user": 0 } | Deletes the user account and then sends an email with information about the action performed.<br>**comma_separated_email_id** - email IDs in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format.<br>**donot_email_user (optional)**: Do not send email to user affected (1 or 0). Default 0. | Click to see If conditions<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |
| Change user status | { "user_status": "USER_ACCOUNT_LIMITED_ACCESS", "mark_as_verified": 0, "comma_separated_email_id": "xyz@a.com,abc@b.com", "comma_separated_group_name": "Group A,Group B", "donot_email_user": 0 } | **user_account_type -** type of account. You must use one of the following values:<br>• USER_ACCOUNT_DISABLED_ACCESS<br>• USER_ACCOUNT_FULL_ACCESS<br>• USER_ACCOUNT_GUEST_ACCESS<br>• USER_ACCOUNT_LIMITED_ACCESS (external access)<br>**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.<br>**comma_separated_email_id** - email IDs in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format.<br>**donot_email_user** (optional) - prevents an email from being sent to the user affected when the status is changed<br>• 1 = Does not send an email<br>• 0 = Sends an email<br>• If nothing is specified, the default is 0 | Click to see If conditions<br>If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |

| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Set user group | {<br>"group_name":"Group1,Group2"<br>} | Assigns user to groups.<br>**group_name** - Comma separated list of groups to assign user to. | If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |
| Set user policy | {<br>"policy_name":"SamplePolicyName",<br>"comma_separated_email_id": "",<br>"comma_separated_group_name": "Group A,Group B",<br>"donot_email_user": 0<br>} | Sends an email notification to the listed users that the user's policy was set as the specified policy<br>**policy_name** - Name of policy to set<br>**comma_separated_email_id** - email ids in comma separated format<br>**comma_separated_group_name**: Group names in comma separated format.<br>**donot_email_user**<br>**0** (default) send the emails<br>**1** do not send the emails | If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>If a user's account is near its expiration date |
| Set user properties | {<br>"policy_name":"SamplePolicyName",<br>"user_status":"USER_ACCOUNT_LIMITED_ACCESS",<br>"comma_separated_email_id": "",<br>"comma_separated_group_name": "Group A,Group B",<br>"donot_email_user": 0<br>} | 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<br>**policy_name**: Name of policy to set.<br>**user_status (optional)**: User status to set. (USER_ACCOUNT_FULL_ACCESS, USER_ACCOUNT_GUEST_ACCESS, USER_ACCOUNT_LIMITED_ACCESS (external access))<br>**comma_separated_email_id (optional)**: Comma separated emails to notify of workflow action.<br>**comma_separated_group_name (Optional)**: Group names in comma separated format.<br>**donot_email_user (optional)**: Set to 1 to prevent system from notifying user. | If a user's last login is older than . . .<br>If a new user is created<br>If a user's create date is older than<br>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<br>If a share has not been accessed for specified days |

## Device actions

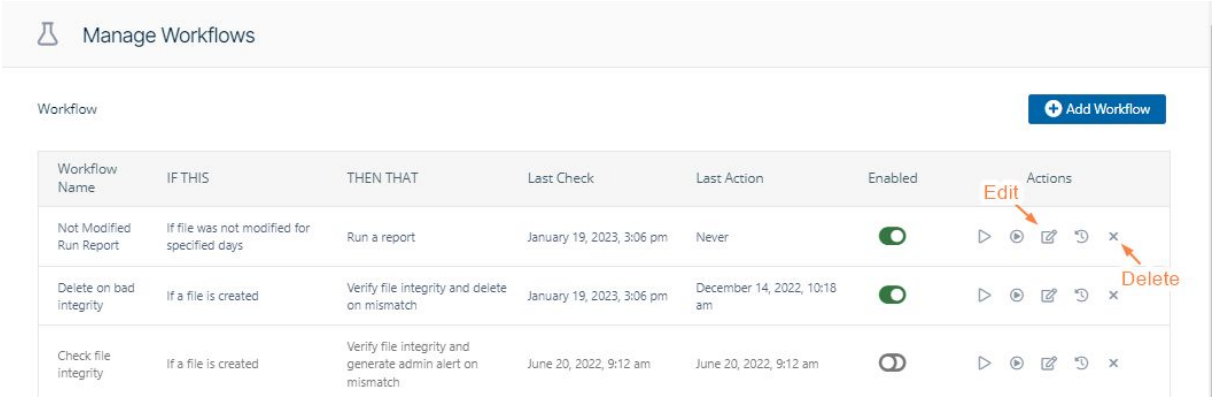
| Action | Parameters | Details | Compatible IF conditions |
|---|---|---|---|
| Block the device for admin approval | *None* | Blocks the device and marks it with "Needs Approval" on the Manage Devices screen | Click to see If conditions<br>If a new client app connects |

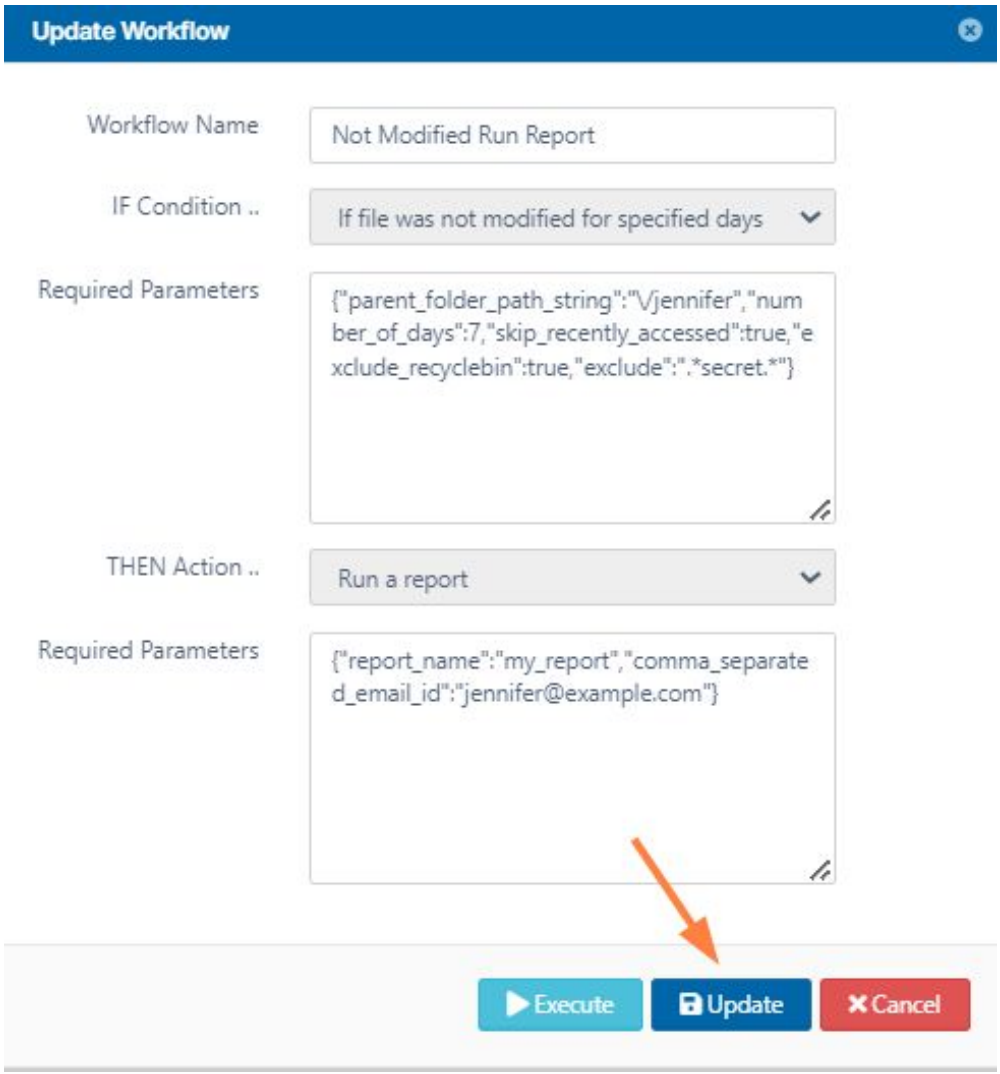
# Edit a Workflow

It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and set up correct workflows.

Administrators can edit workflows to change the name or parameters of the conditions and action.

To edit, click on the Edit button; to delete, click on the Delete button.





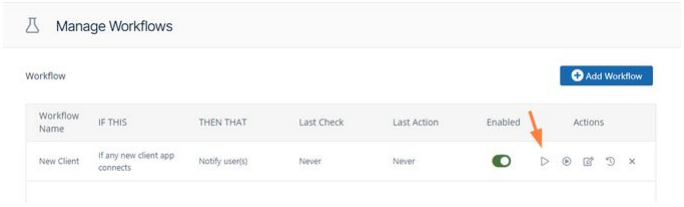

## Run a Workflow

It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

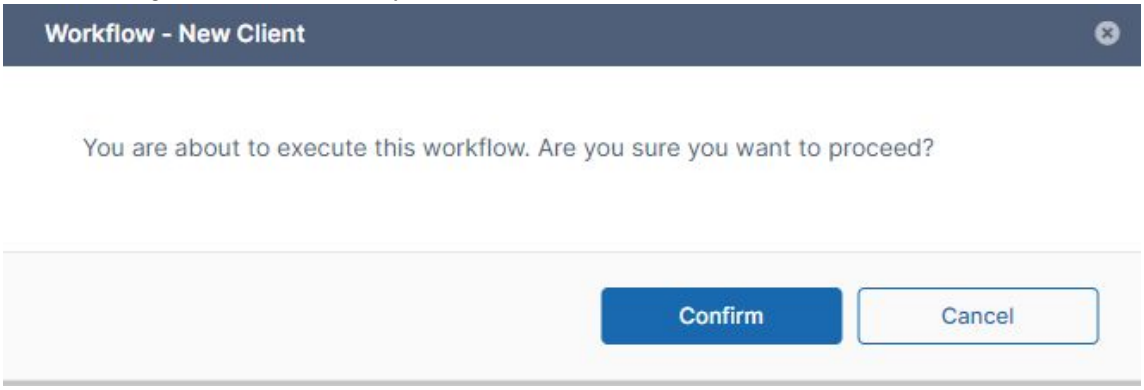
Administrators can run a workflow manually from the **Manage Workflows** screen.

**To run a workflow manually**:

1. In the FileCloud admin portal's navigation panel, click **Workflows**.
2. In the Manage Workflows screen, in the row for the workflow you want to run, click the first arrow under **Actions**.




The following confirmation box opens.




3. Click **Confirm**.
   A screen notification confirms that the workflow ran successfully.

# Set Advanced Workflow Options

It is important to note that not all actions are compatible with all conditions and it is up to the user to determine and setup correct workflows.

Administrators can create and run more advanced scenarios., such as:

- regular expression in path matching
- the ability to pass additional, runtime-resolved data between conditions and actions

## What scenario do you want to use?

### Regular Expressions and Path Matching

You can enable regular expression matching in workflows by setting the **use_regex** parameter to **"1"** in the condition definition. This is an optional parameter and by default is **"0"** (don't use regular expressions - use strict match instead). If regular expressions are enabled you must provide a valid regular expression pattern as the **parent_folder_path_string** value. This pattern is used in the condition resolution process to find all matching paths (files / folders).

Regular expressions are supported by the following workflow conditions:

- if a file is created

- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated

## Parameters definition - example

Strict match

*{*
*"parent_folder_path_string":"/userid/somepath",*
*}*

or

*{*
*"parent_folder_path_string":"/userid/somepath",*
*"use_regex":"0"*
*}*

Regular expression

*{*
*"parent_folder_path_string":"/userid/somepath",*
*"use_regex":"1"*
*}*

## Usage - Example

For simplicity sake assume that Administrator wants to send email notifications whenever someone downloads a file from a given location. The following example shows the difference between *strict match* and *regular expression match*

Strict match

Parameters are defined as follows:

*{*
*"parent_folder_path_string":"/userA/downloads",*
*}*

For such defined condition action will be triggered whenever a files is downloaded directly from the "/userA/downloads" directory and only from this one.

Regular expression

In this case the definition might look something like:

{
*"parent_folder_path_string":"**~/.*/downloads~**",*
***"use_regex":"1"***
}

For this condition action will be triggered for **all** directories that match the /user/download format, i.e. /userA/downloads, /userB/downloads, etc. This is a huge change that enables Administrators to define much more universal workflow scenarios.

**Important**
**Regular expression patterns aren't validated for correctness. Please double check them, especially when dealing with the data-changing actions (i.e. delete files / move files, etc.).**

**RegEx Patterns**
Regular expression definition has to start and end with one of the following characters:
'/', '~', '@', ';', '%', `'
We strongly advise against the / usage as it adds confusion to the pattern definition.

### Reversed Path Matching

The **Exclude** parameter enables the "reversed" path matching. That means that the specified action will be triggered for all files / folders whose path **doesn't match**. It's another huge change that allows administrators to define a new set of workflow. This is a very flexible and poweful feature, especially when combined with regular expressions.

Exclude parameter is supported by the following conditions:

- if a file is created

- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated

Example

Administrator wants to delete all files that were downloaded form the FileCloud, but wants to keep files in one particular location - /userA/prevented. Condition should be then defined as:

*{*
*"parent_folder_path_string":"/userA/prevented",*
*"exclude":"1"*
*}*

The match condition will be reversed, so action will be triggered for all files, except the ones located in this particular directory.

**Regular Expressions**
For a regular expression it is very important to understand that if it is invalid it will return a **NOT MATCH** result for all paths. Administrators have to be very careful when using exclude parameter with regular expressions, especially for a data sensitive operations.

**Runtime Resolved Parameters**

Runtime resolved parameters are available in Workflows.

The runtime resolved parameters can be specified in the following IF conditions:

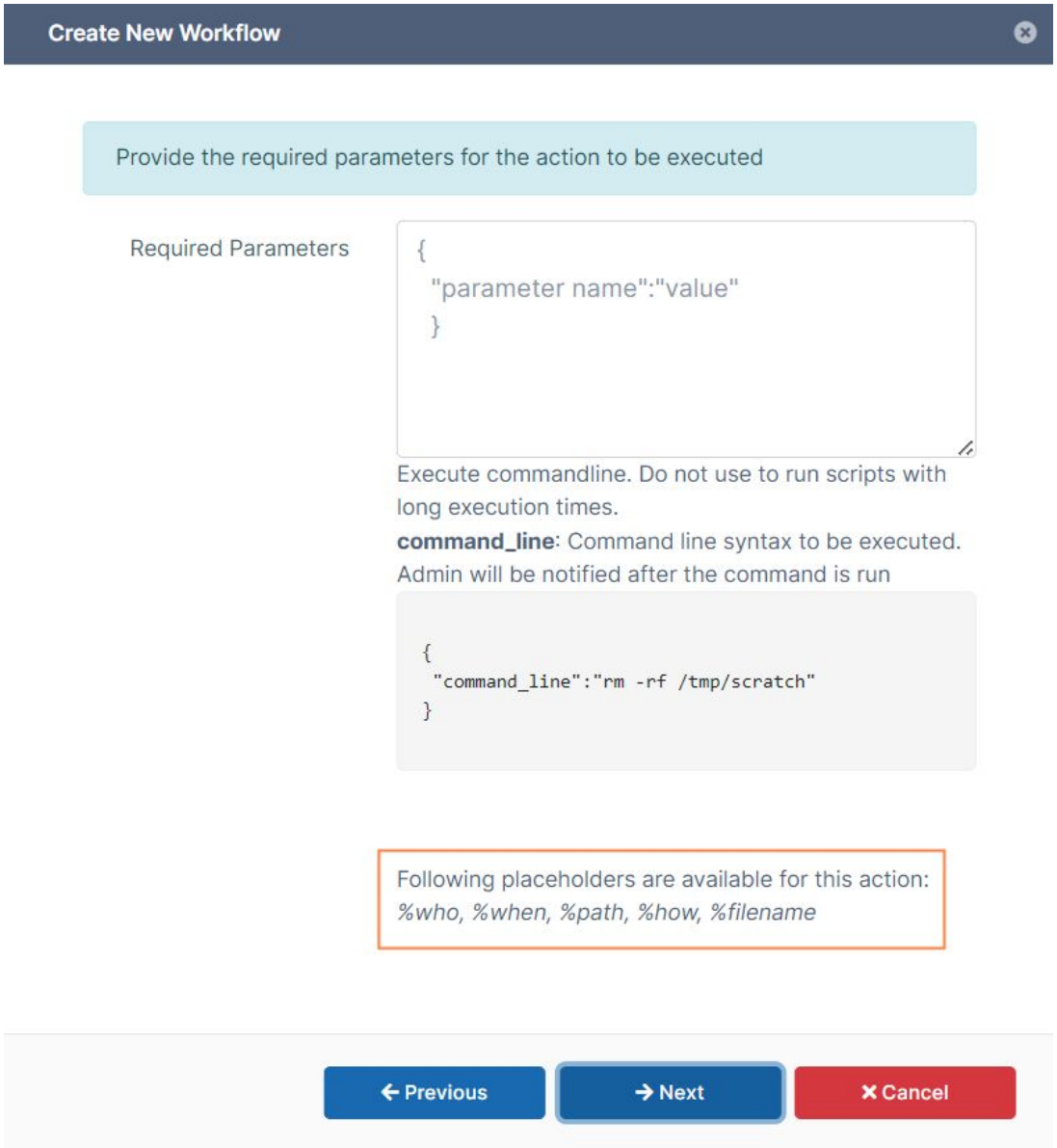
- if a file is created
- if a folder is created
- if a file is updated
- if a file is deleted
- if a folder is deleted
- if a file is downloaded
- if a comment is added
- if a file is added or updated
- if the file updated is bigger than the expected size
- if the file downloaded is bigger than the expected size

and then used in all compatible THEN actions.

Currently FileCloud supports the following placeholders only for file/folder related conditions.

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

If the selected IF condition is able to implement runtime resolved parameters they are listed in the THEN action dialog box.



**Example - how condition resolves parameters**
Assume that **user1** downloaded a file **file1.pdf** from the **/user1/test** folder through a **Firefox** browser on **4pm** on the **01.01.2018**.
Condition will resolve all the parameters and pass it to the action:

- **%who** - user1
- **%when** - 2018-01-01 16:00:00
- **%path** - /user1/test/file1.pdf
- **%how** - Web browser
- **%filename** - file1.pdf

**Recommended usage**
Although it is possible to use resolved parameters in all compatible actions, this feature was designed and implemented mainly for the **command execution** action.

# Workflow Recipes for FileCloud

You can create custom workflows to perform a variety of actions.

Workflows operate using the following model:

- IF CONDITION - THEN ACTION (IFTTT)

Since there are many different ways to create custom workflows, this page provides you with some simple recipes to create a specific workflow.

- Using some of these recipes will help you learn how a workflow functions
- After using some recipes you should be able to understand how to create your own workflows

## In this section:


- Admin Approval Required Workflow (see page 429)
- Create Report and Send Email Workflow (see page 432)
- Detect and Delete Inactive Files Workflow (see page 439)
- Detect and Disable Inactive Users Workflow (see page 444)
- Detect and Generate Inactive File List Workflow (see page 448)
- Detect and Notify Failed Signatures Workflow (see page 453)
- Detect and Notify Inactive Users Workflow (see page 458)
- Notify on File Upload Workflow (see page 462)
- Periodic Script Workflow (see page 467)
- Periodically Send Custom Email Workflow (see page 470)

- Run workflows commands with /tmp paths in Linux systems (see page 476)

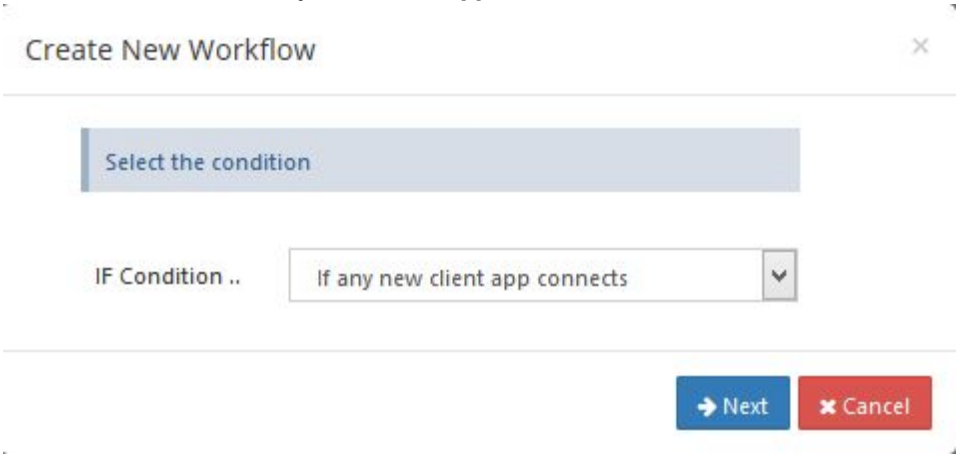
## Admin Approval Required Workflow

This workflow recipe blocks the connection of a new app or device until it is approved by an administrator.

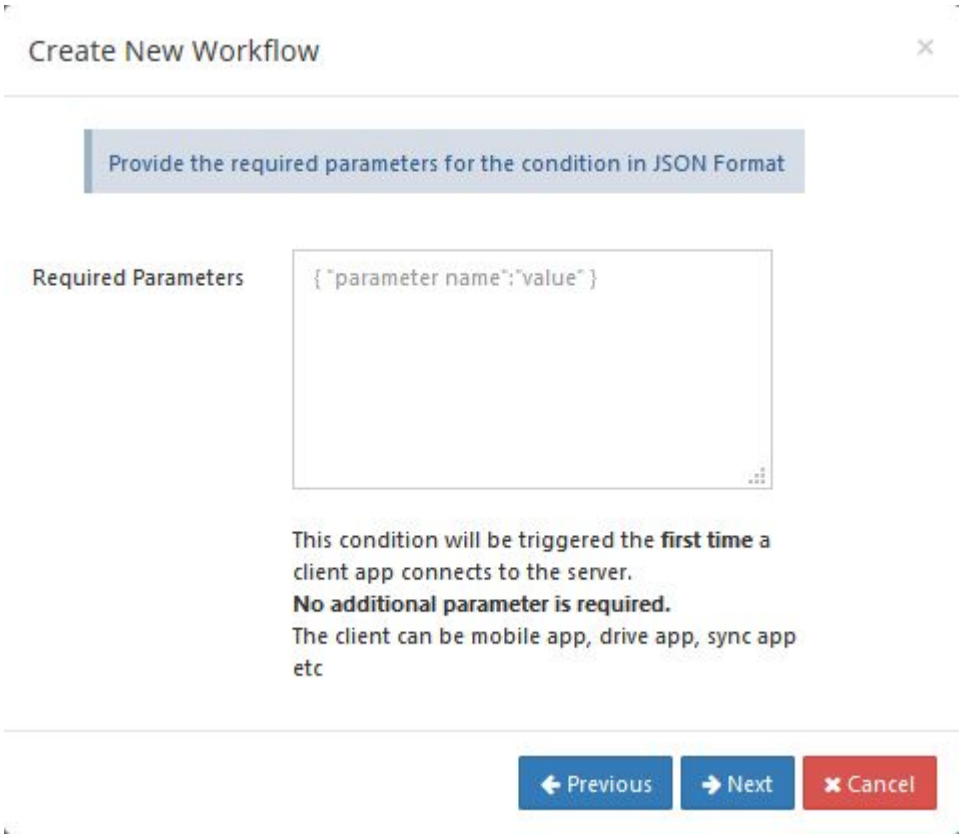
- When a new app or device tries to connect to FileCloud, the action is unblocked ONLY after admin approval.
- In the Admin Portal, you can see the devices in BLOCKED status, awaiting ADMIN approval.

**To create a workflow that requires admin approval for all clients**:

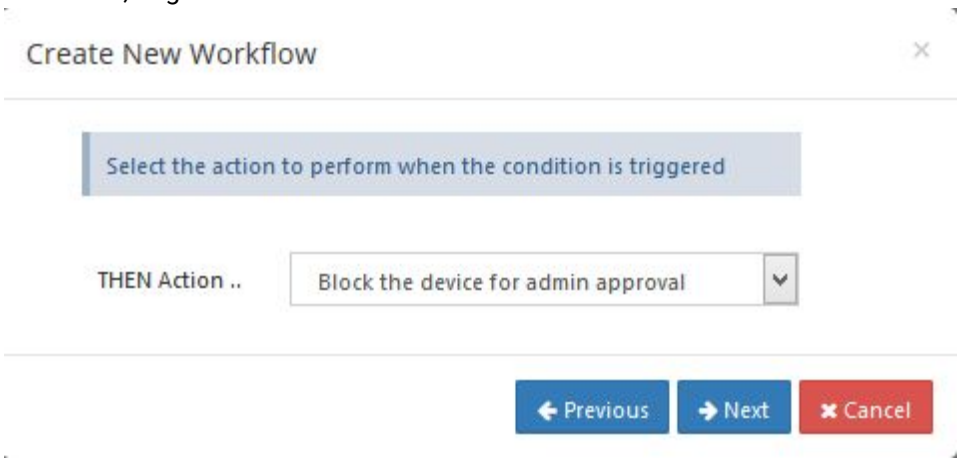
1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition "**If any new client app connects**"



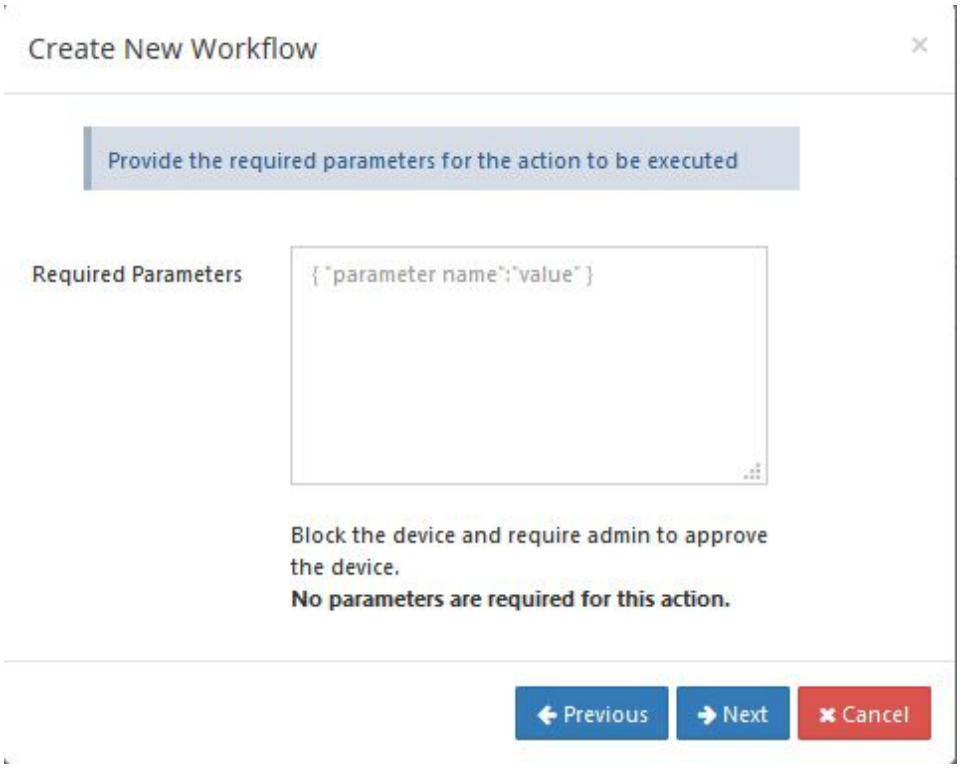

5. Click Next,  no required parameters are to be given as ,the condition triggers for any client app that connects to FileCloud.



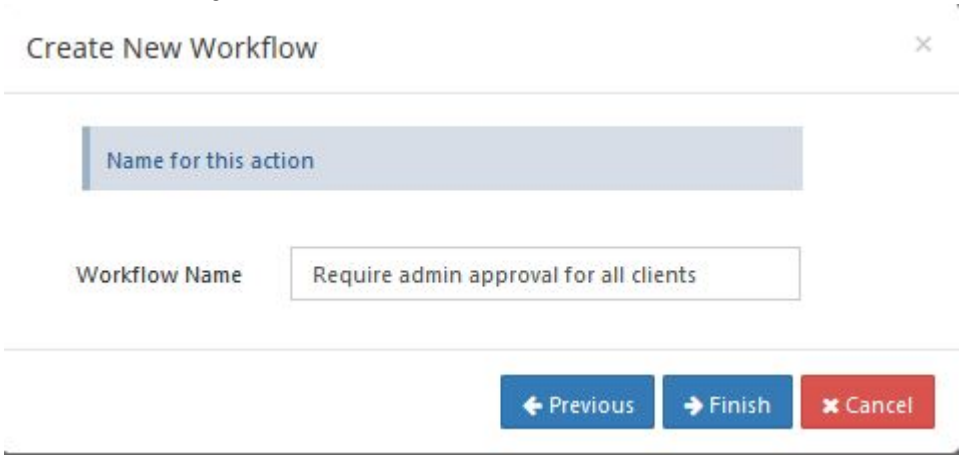

6. Click Next, to give the THEN action



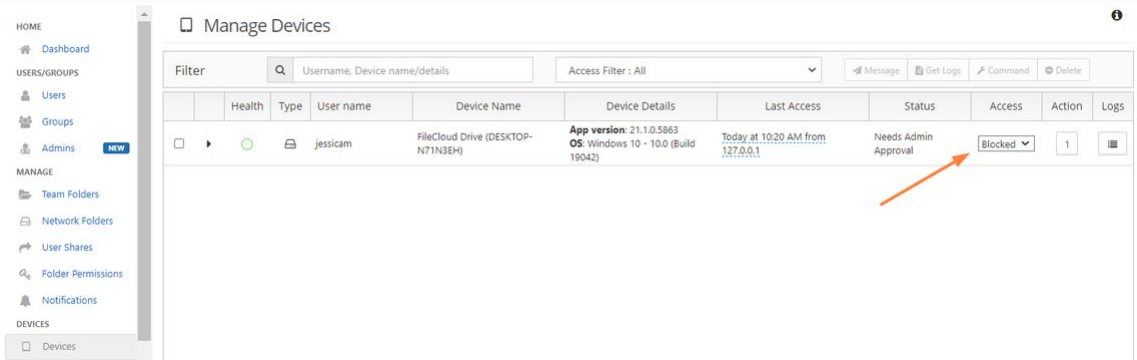

7. Click on Next, No parameters are required for this action



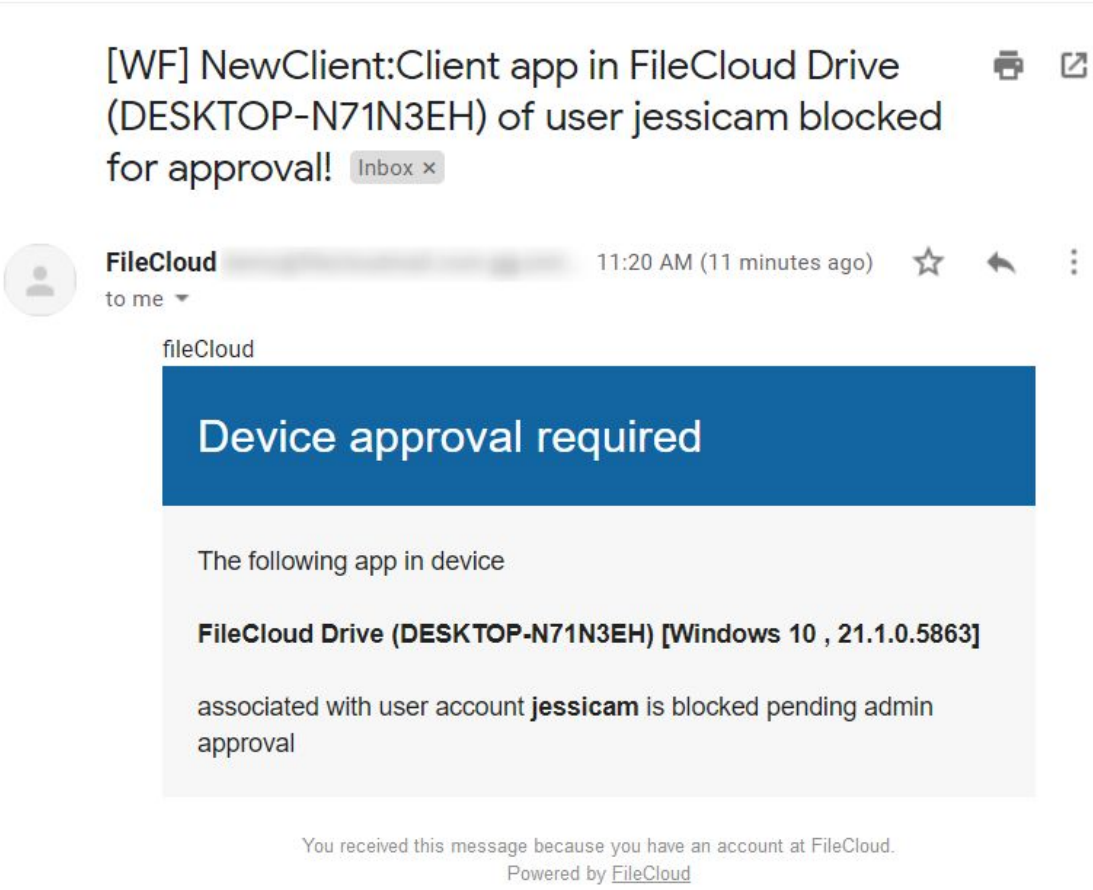

8. Click on Next, to give workflow name




9. In the admin dashboard, the Devices tab will show the status of the devices awaiting Admin approval. The Admin is also sent an email.



10. An email will be sent to the user trying to connect to FileCloud notifying the user that the device needs to be approved by the admin.



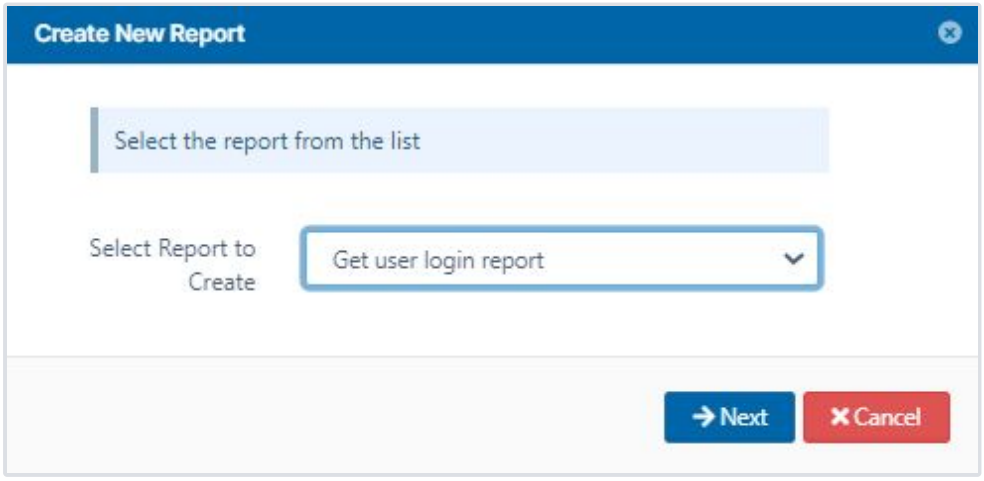

## Create Report and Send Email Workflow

This workflow recipe creates a specific report and sends the result to specified emails once a day.

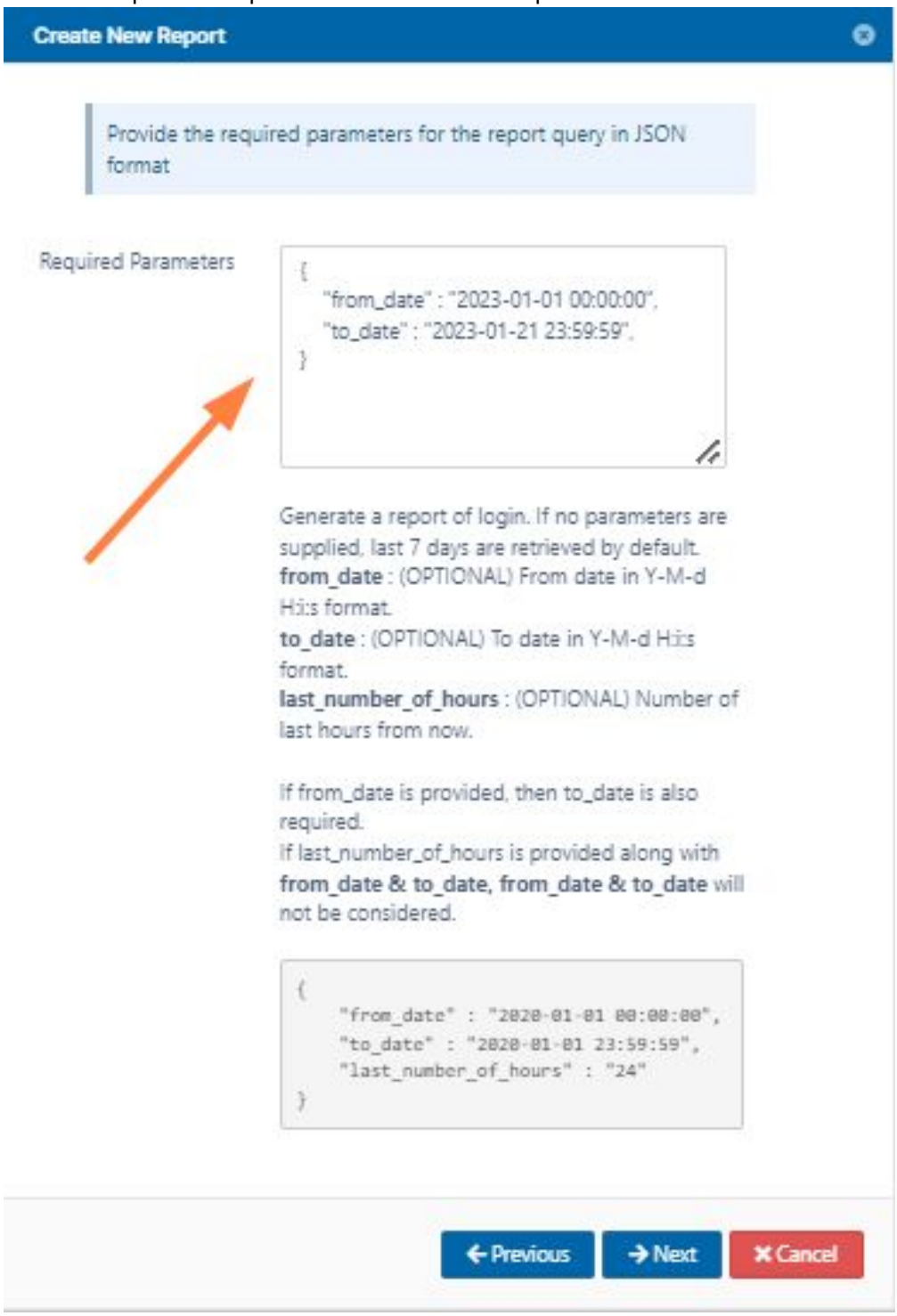
- The email can be configured to be sent at a specific time in the day, and the day interval can be set to daily.

**To create a workflow that generates a specific report and sends the result to specified emails:**

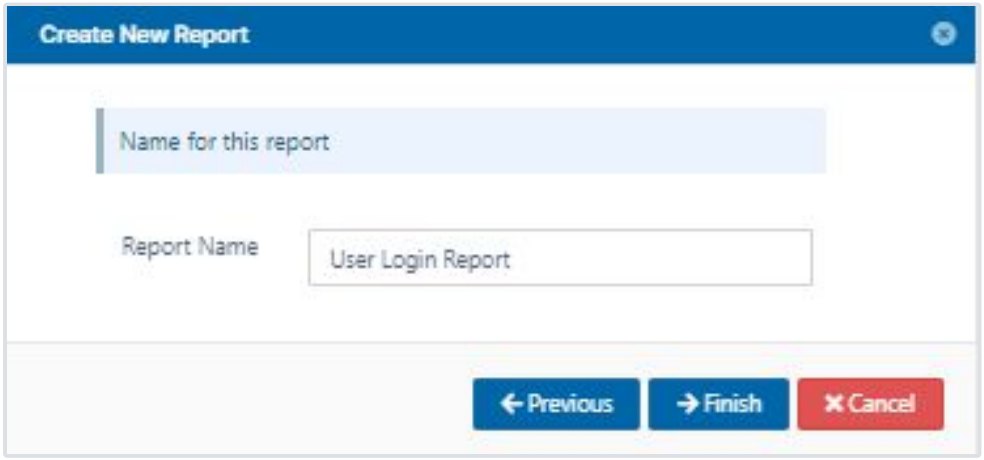
1. Log in to the admin portal
2. In the navigation panel, click **Reports**.
3. Click **Add Report**.
4. In **Select Report to Create**, choose **Get user login report**.


Create New Report
Select the report from the list
Select Report to Create
Get user login report
Next
Cancel

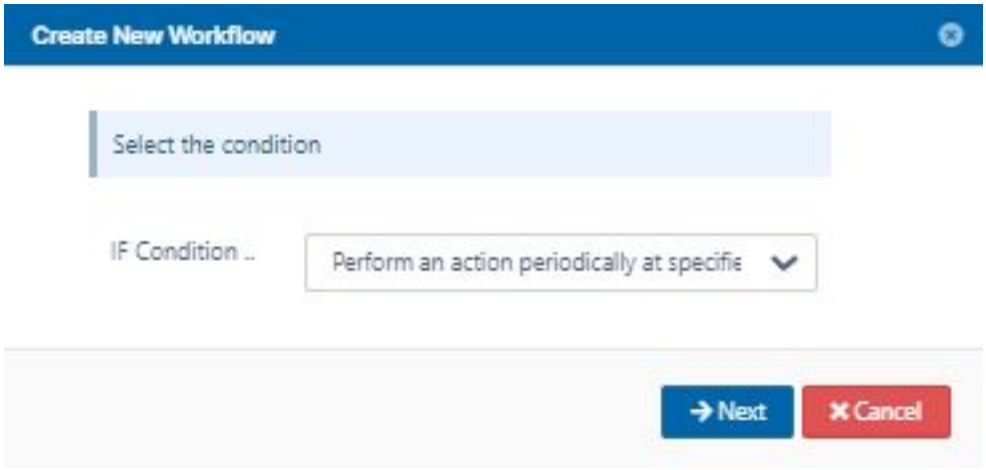
5. Enter the required time parameters to create the report.



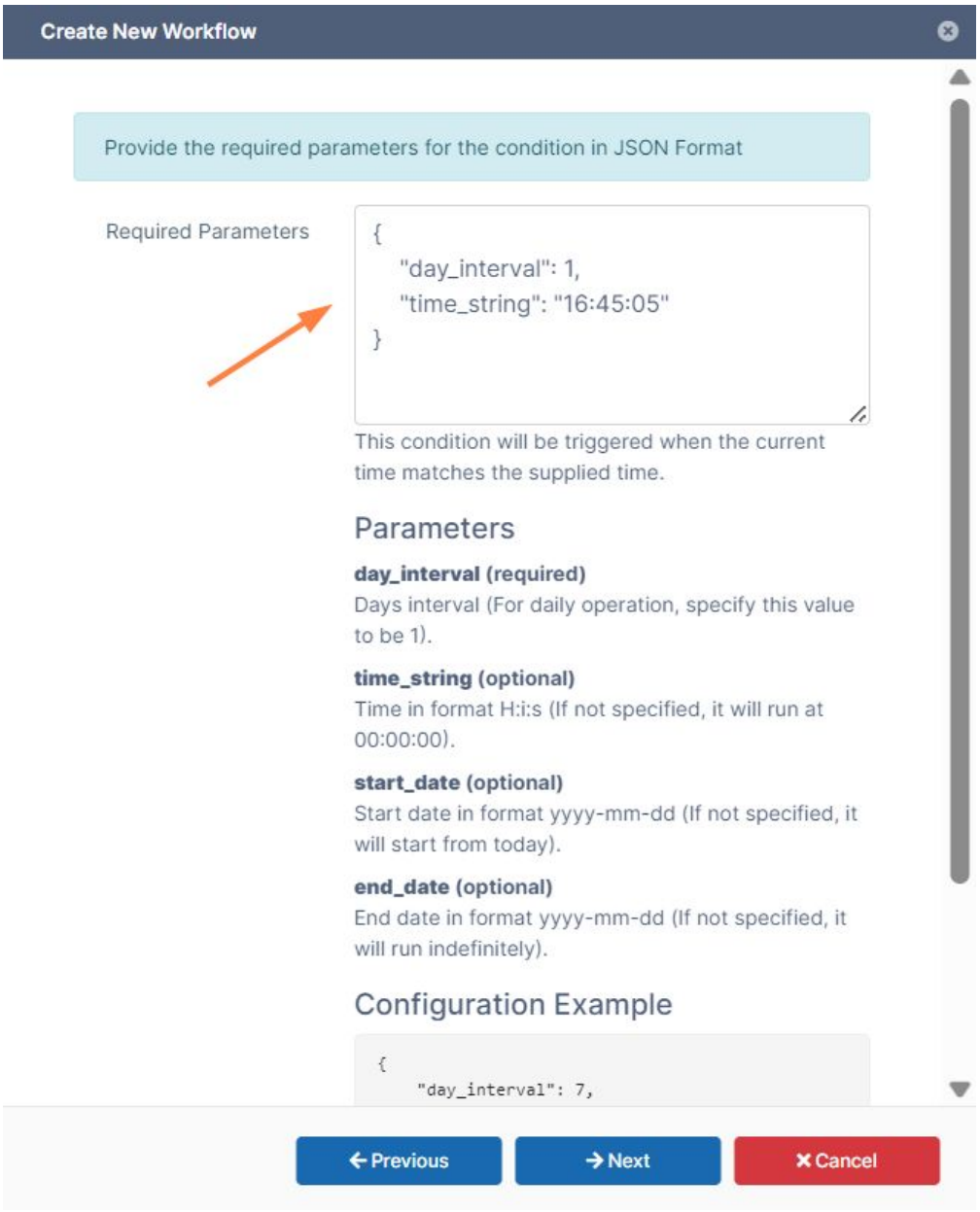

6. Save the report with an appropriate name, and click **Finish**.



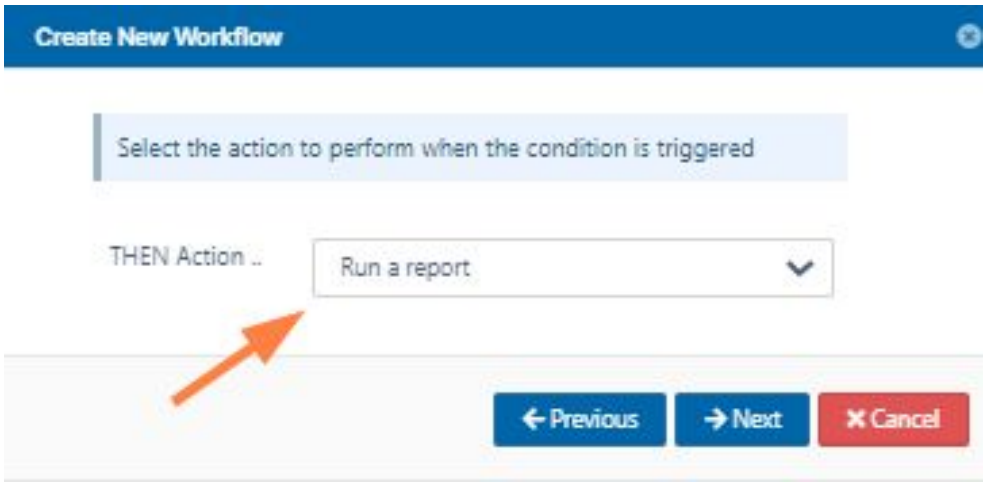

7. Click **Workflows** in the navigation panel.
8. Click **Add Workflow** and set the **If condition** as **Perform an action periodically at specified time and interval**.



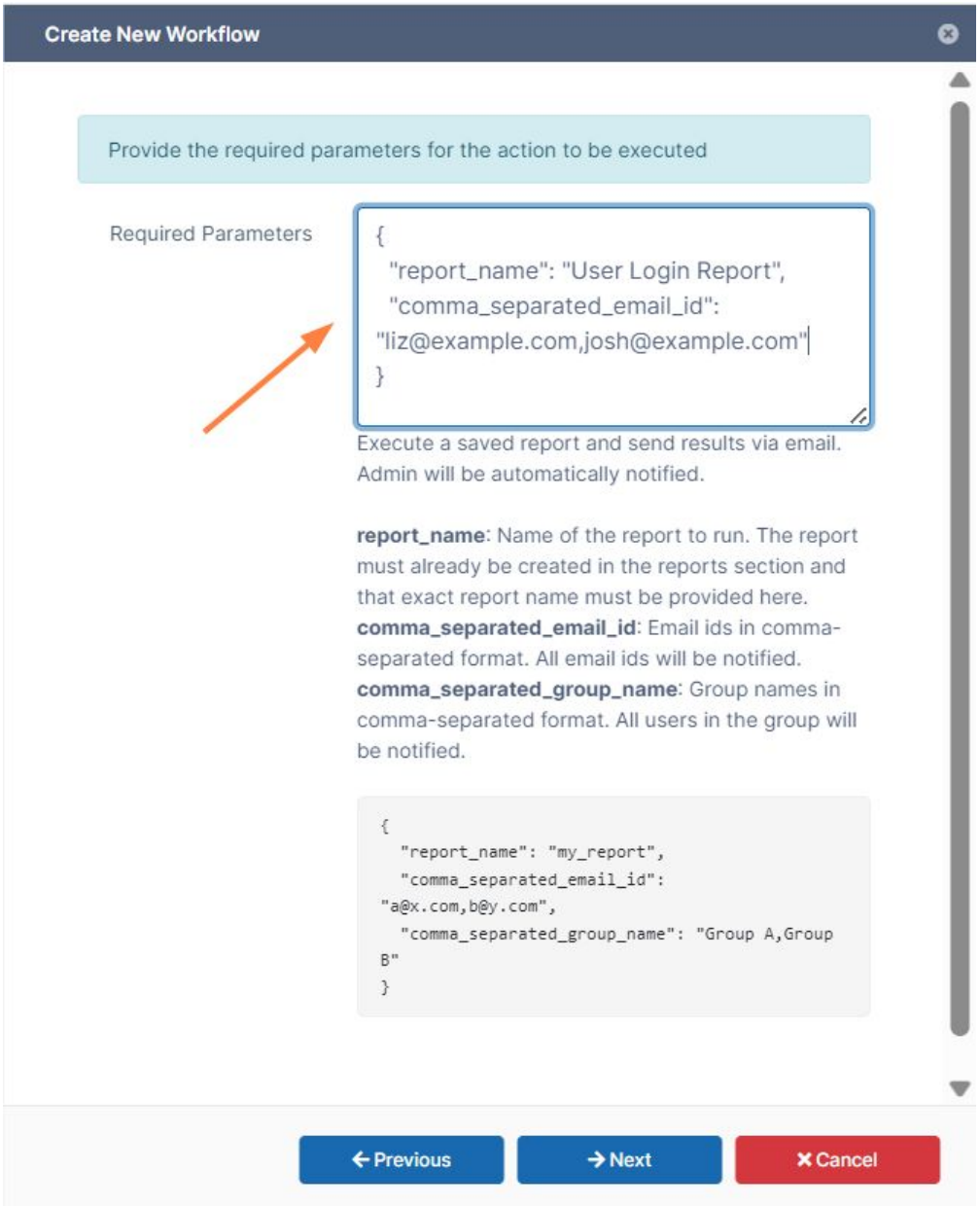

9. Specify the time in the format given in the template. Specify the day interval as 1 to indicate that the workflow should be triggered daily.



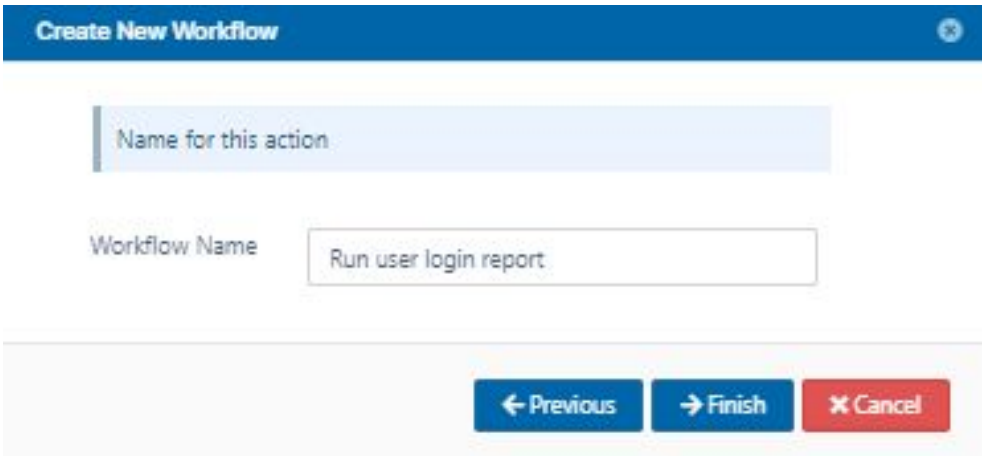

10. Set the **THEN Action** as **Run a report.**



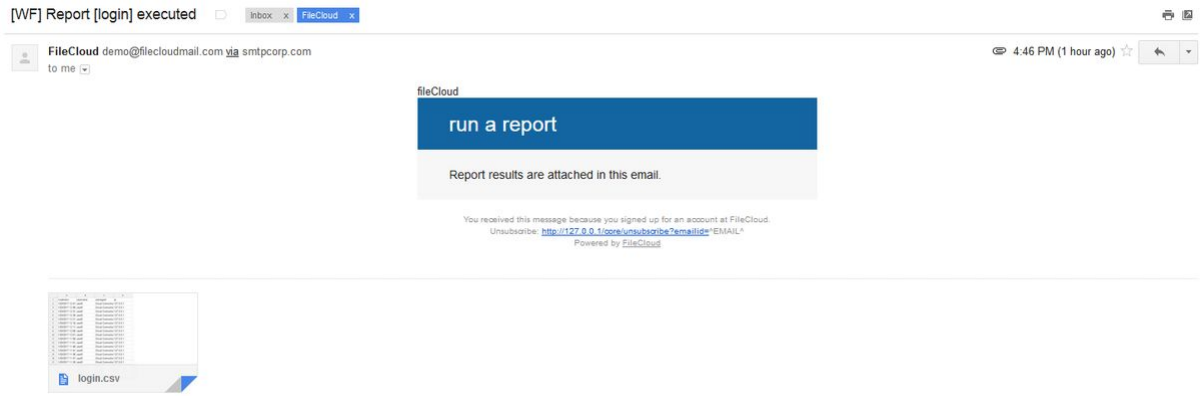

11. Specify the report name created previously and the emails or group of the users who will receive the report in the format given in the template.




12. Save the workflow with an appropriate name.




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



Similar workflows can be created to run reports with THEN conditions like:
- **Perform an action on the specified date**
- **Perform an action periodically**

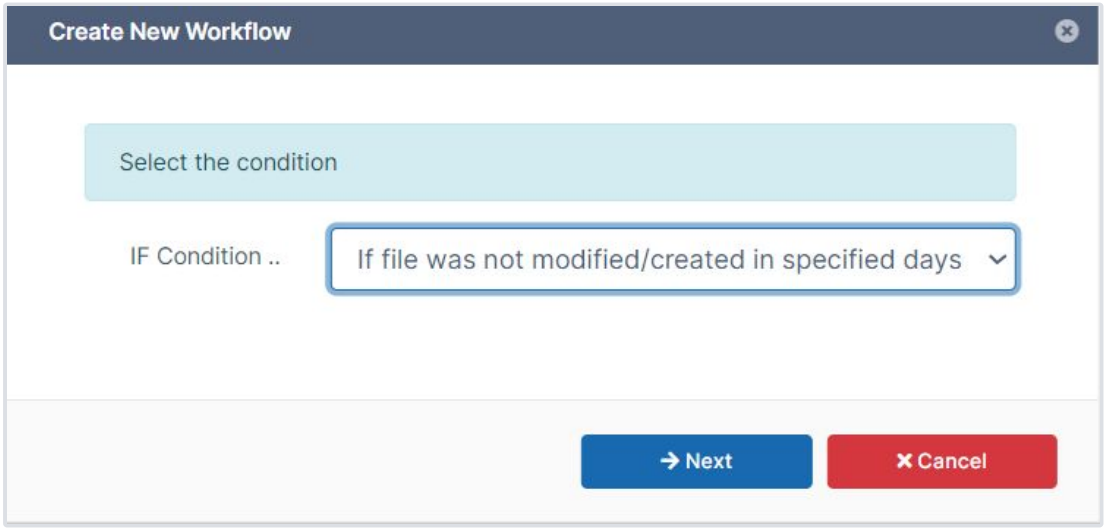
## Detect and Delete Inactive Files Workflow

This workflow recipe deletes all unused files.

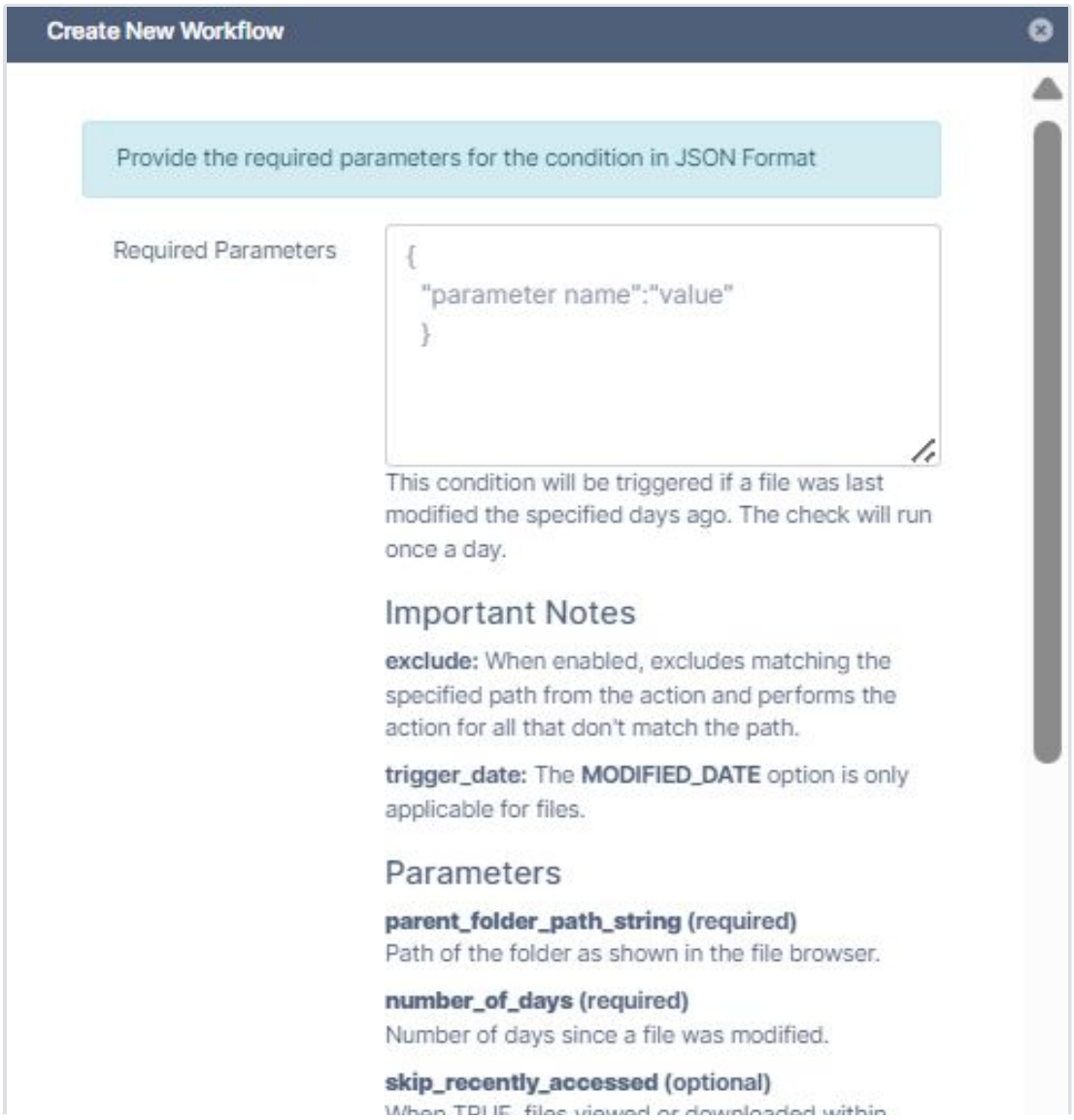
- The workflow checks the number of days a file was unused and deletes those files.
- You can provide a set of email ID's to send the generated report to.

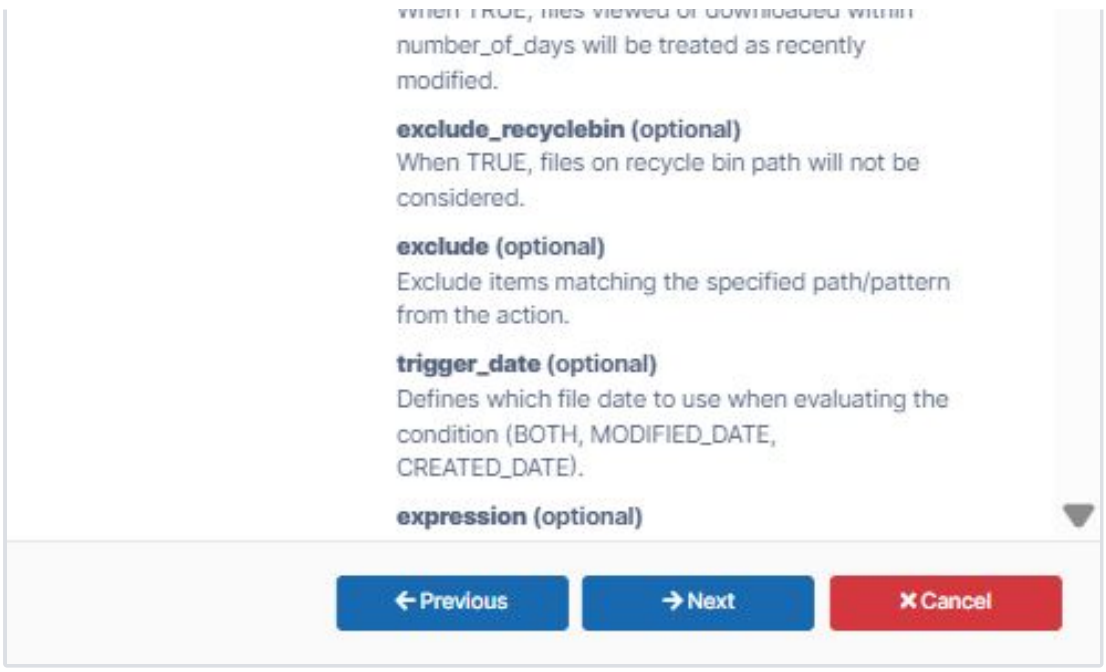
**To create a workflow that detects and deletes inactive files**:

1. Log in to the admin portal.
2. Click **Workflow** on the left navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified for specified days**, and click **Next.**




5. Enter the parameters in the given format.





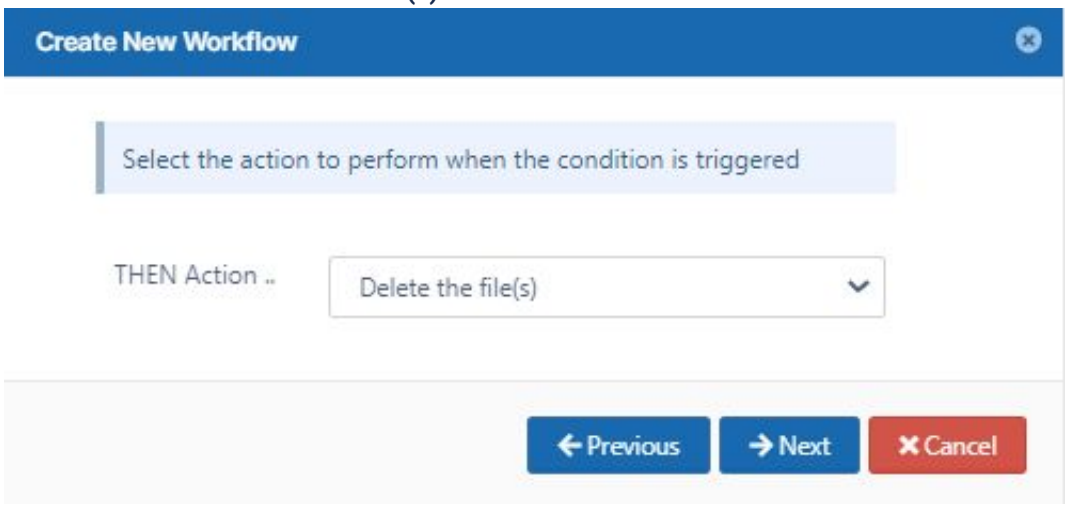

For example:

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

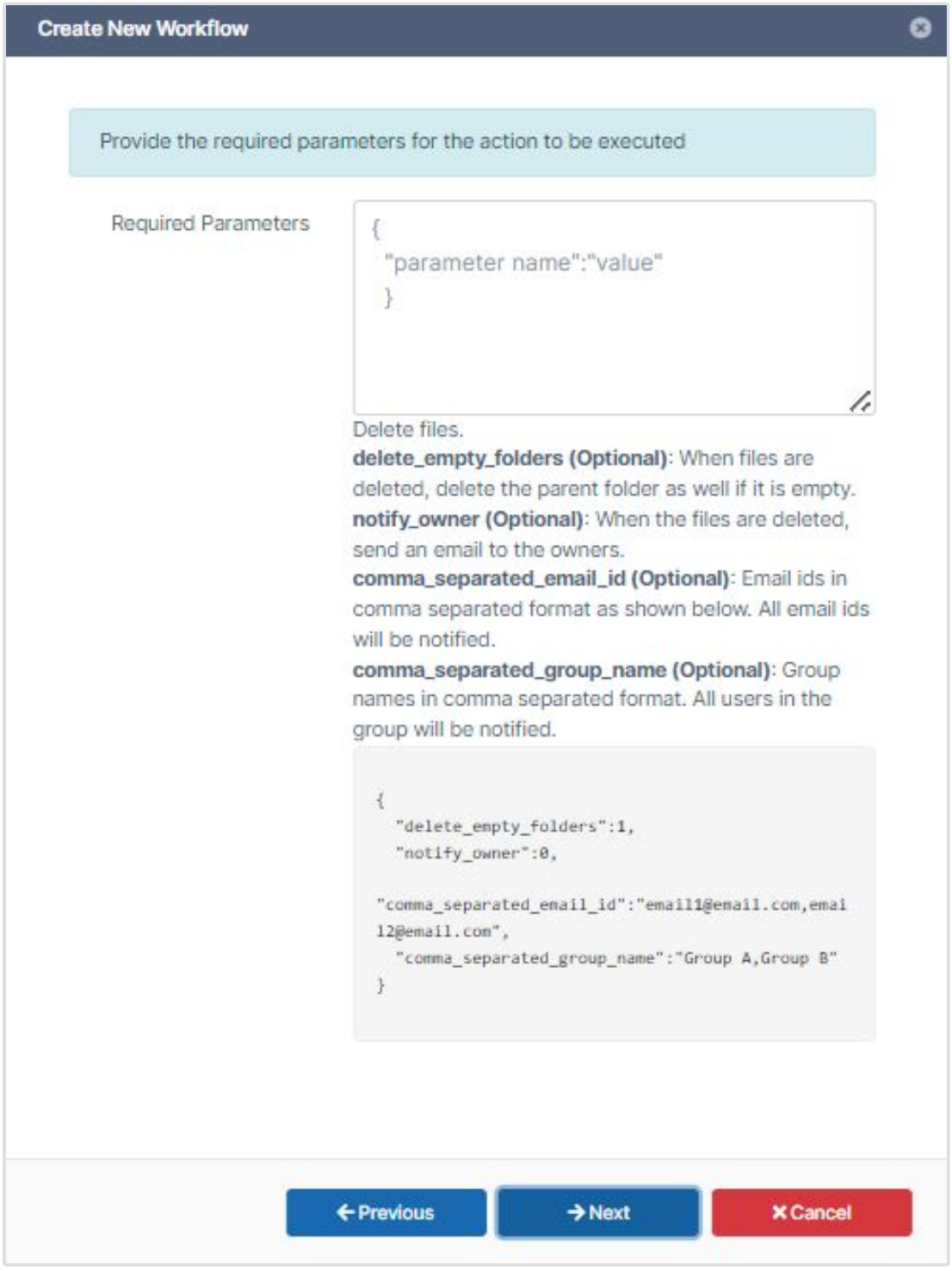
**Note** - This workflow only applies to Managed Storage and not to Network Folders.
To identify a FileCloud specific path for a folder, see Identifying a FileCloud Specific Path (see page 275).

6. Click **Next.**

7. Set **THEN Action** to **Delete the file(s)**.




8. Click **Next**.
   Set any of the parameters. They are all optional.

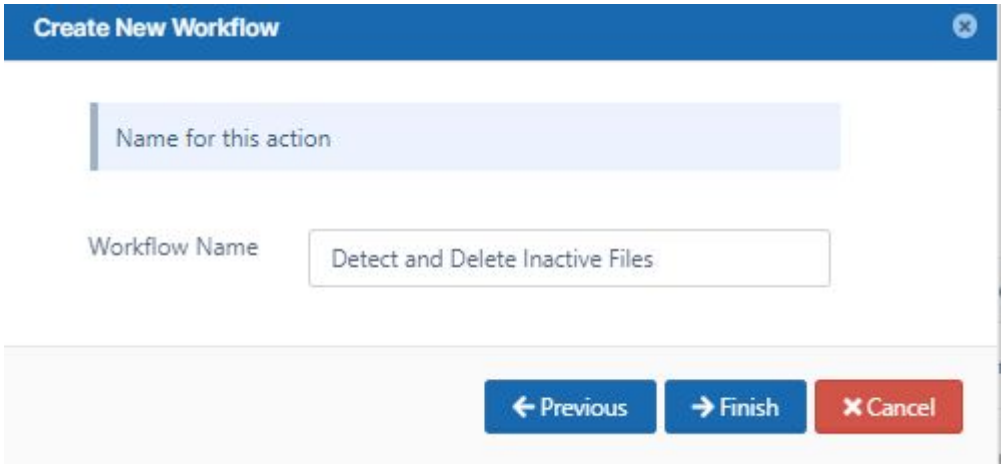



For example:

```
{
"delete_empty_folders":true
```

```
}
```

9. Click **Next**.
10. Enter a **Workflow Name** and click **Finish**.



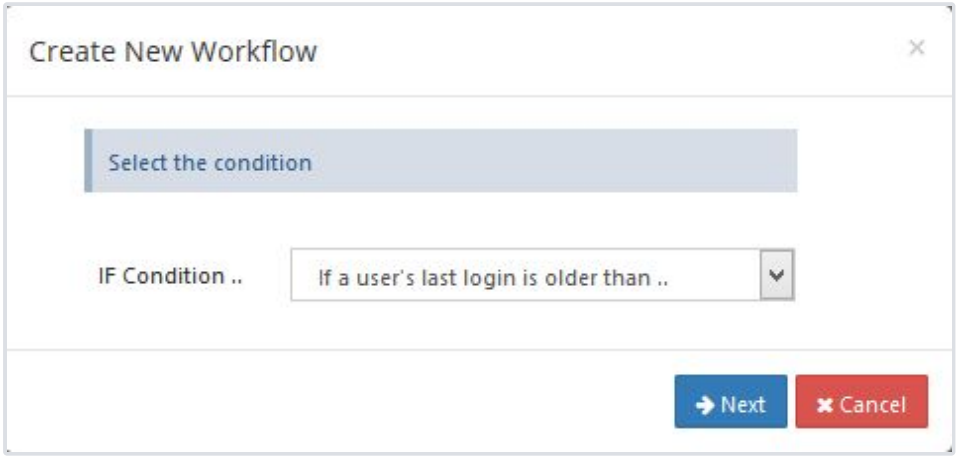

## Detect and Disable Inactive Users Workflow

This workflow recipe disables a user when the user is no longer active and notifies the user through email once the account is deactivated.

- The last login date of the user is used to know if the user is Active or Inactive.
- You can avoid looking at users who have not begun using FileCloud.
- You provide the email ID's to which a report of disabled users is sent.

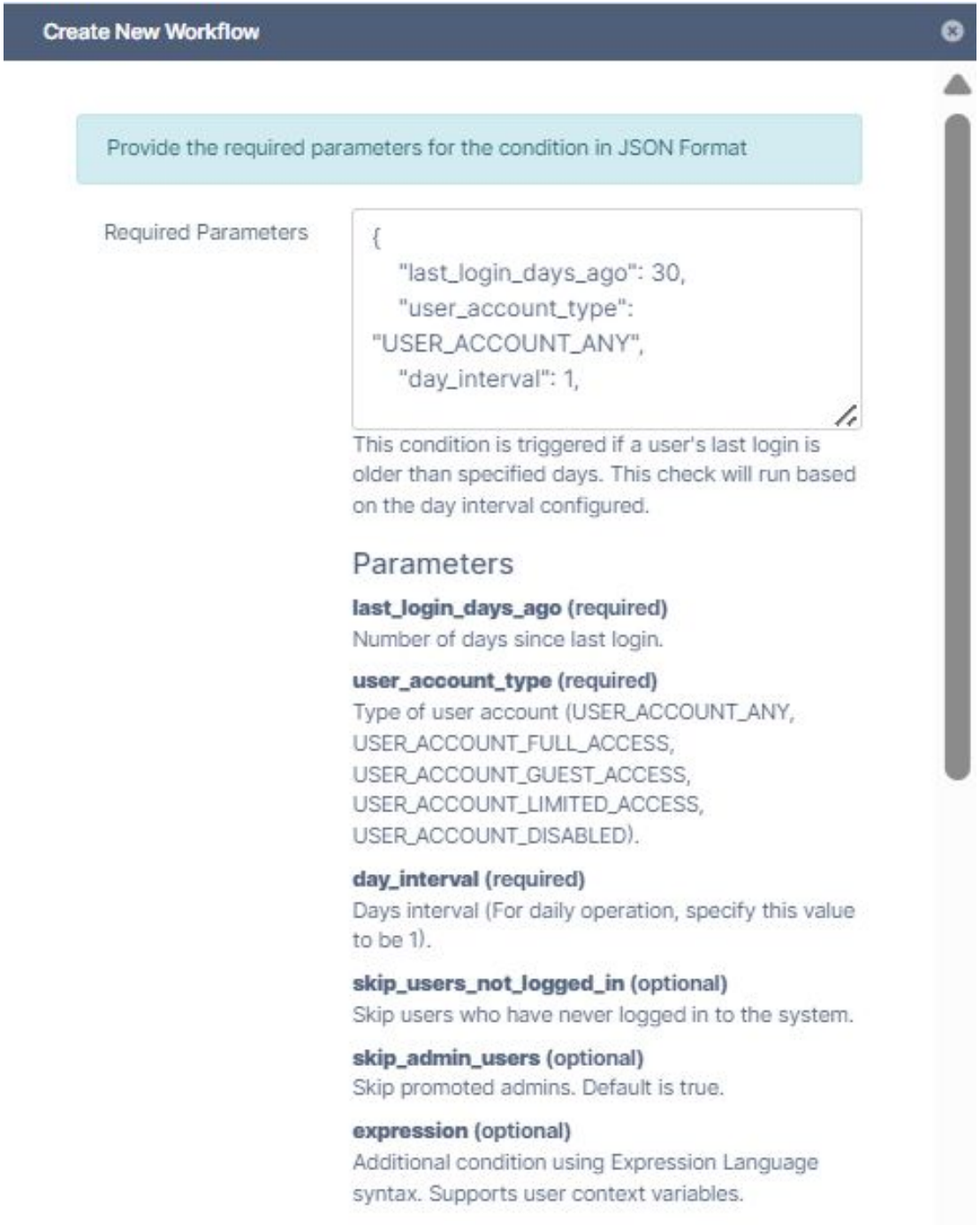
**To create a workflow that detects and disables inactive users**:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Click the **Add Workflow** button
4. Set the If Condition " **If a user's last login is older than..** "



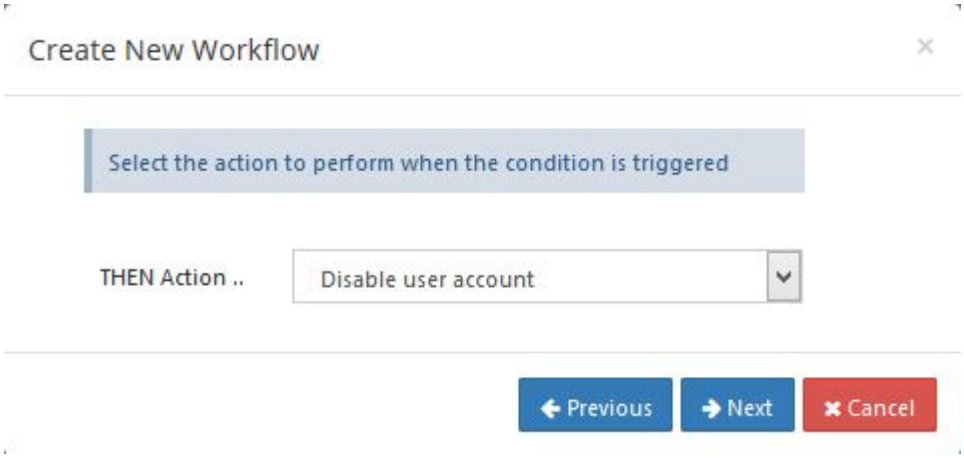
5. Enter the required parameters in the given format.

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



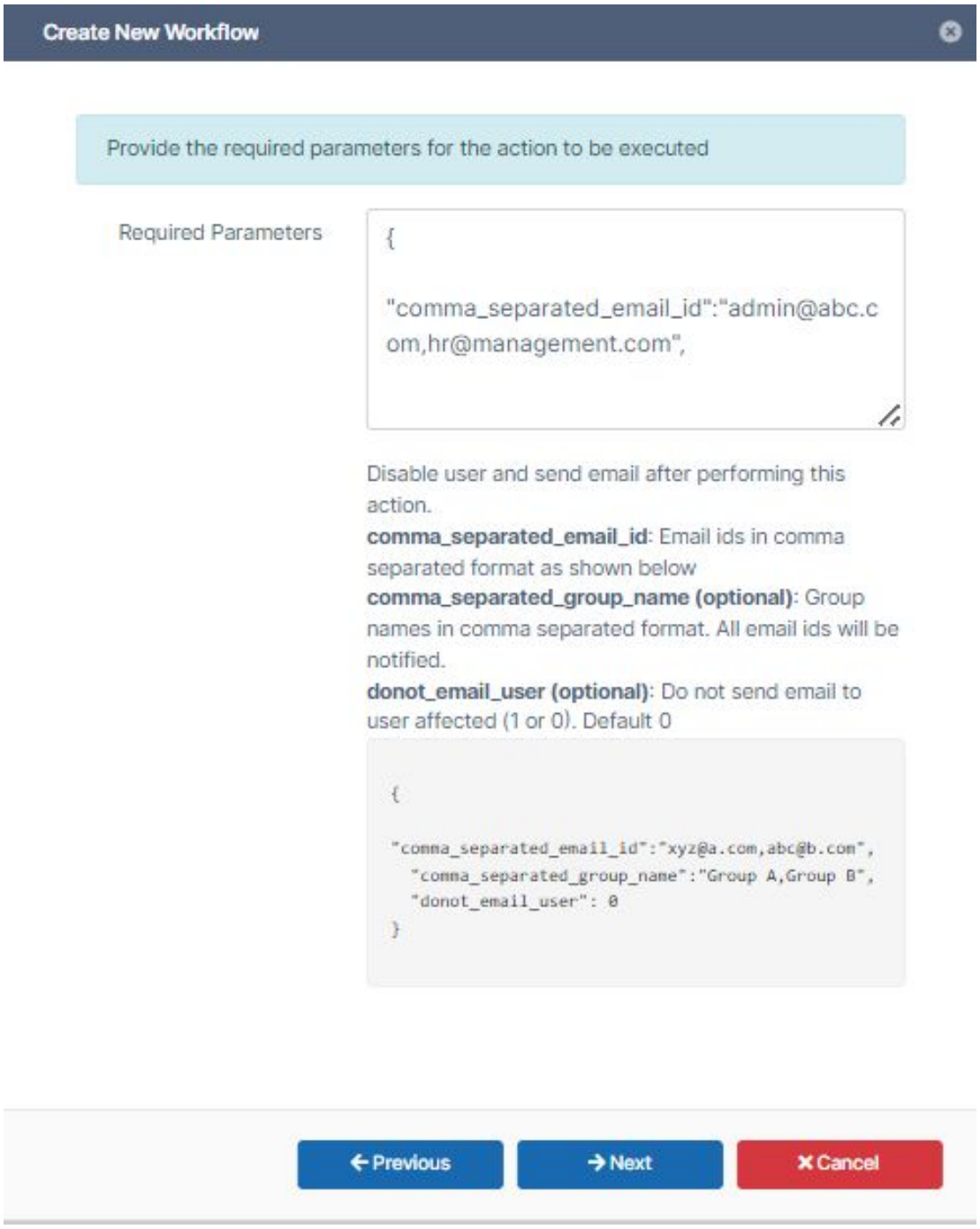

6.

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

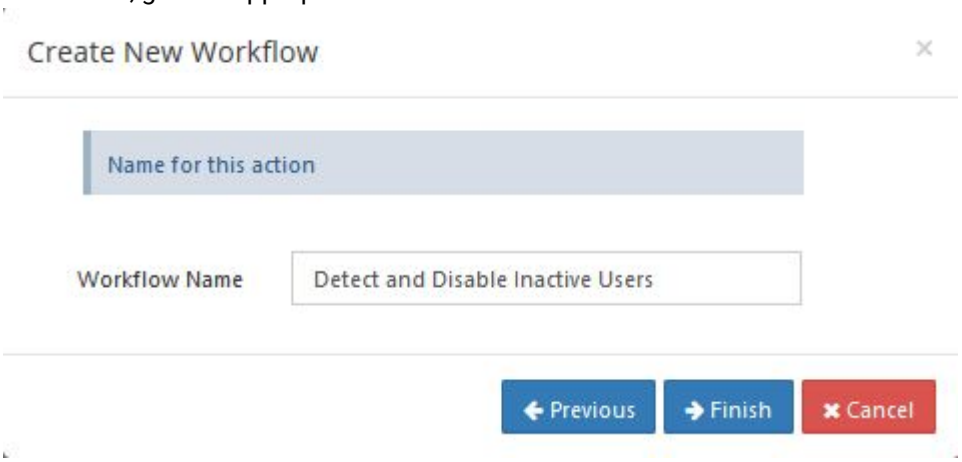



7. Enter the Required parameters in the given format.

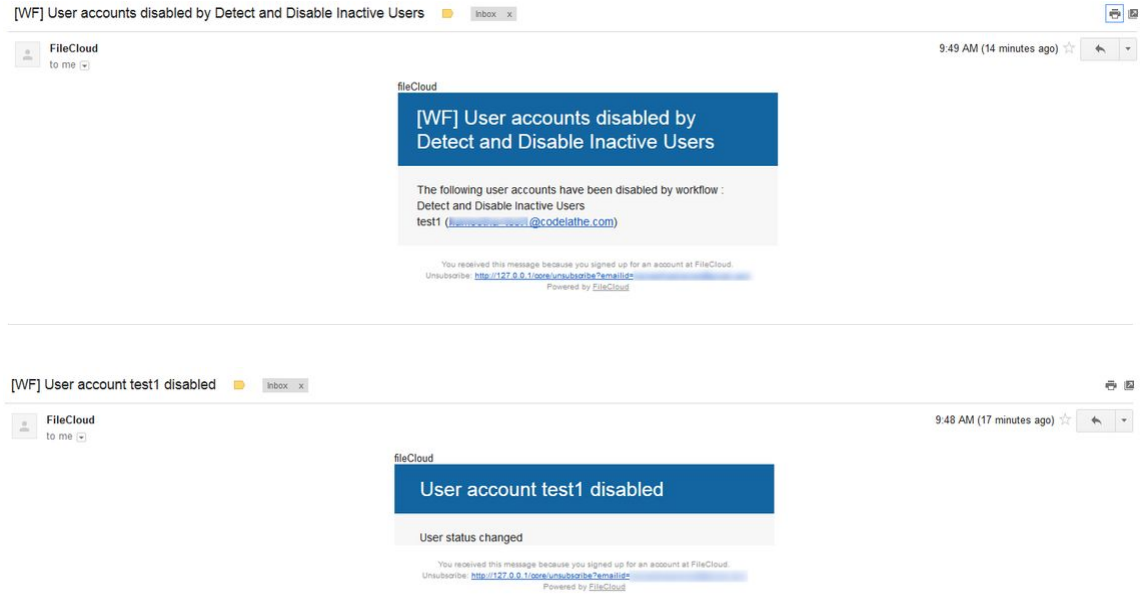
```
{
"comma_separated_email_id":"admin@abccompany.com,hr@management.com"
  }
```


Create New Workflow
Provide the required parameters for the action to be executed
Required Parameters
{
"comma_separated_email_id":"admin@abc.com,hr@management.com",
Disable user and send email after performing this action.
comma_separated_email_id: Email ids in comma separated format as shown below
comma_separated_group_name (optional): Group names in comma separated format. All email ids will be notified.
donot_email_user (optional): Do not send email to user affected (1 or 0). Default 0
{
"comma_separated_email_id":"xyz@a.com,abc@b.com",
"comma_separated_group_name":"Group A,Group B",
"donot_email_user": 0
}
Previous
Next
Cancel

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




9. The user accounts are disabled and the notifications are sent once the workflow is executed.




10. Go to the users list to confirm that the users are disabled.

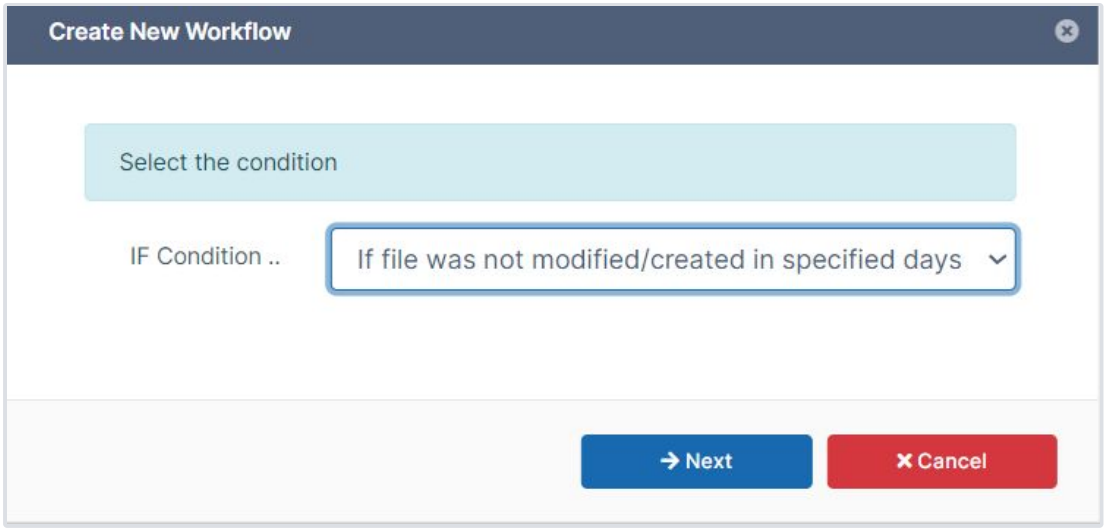
## Detect and Generate Inactive File List Workflow

This workflow recipe sends an email report with a list of inactive files.

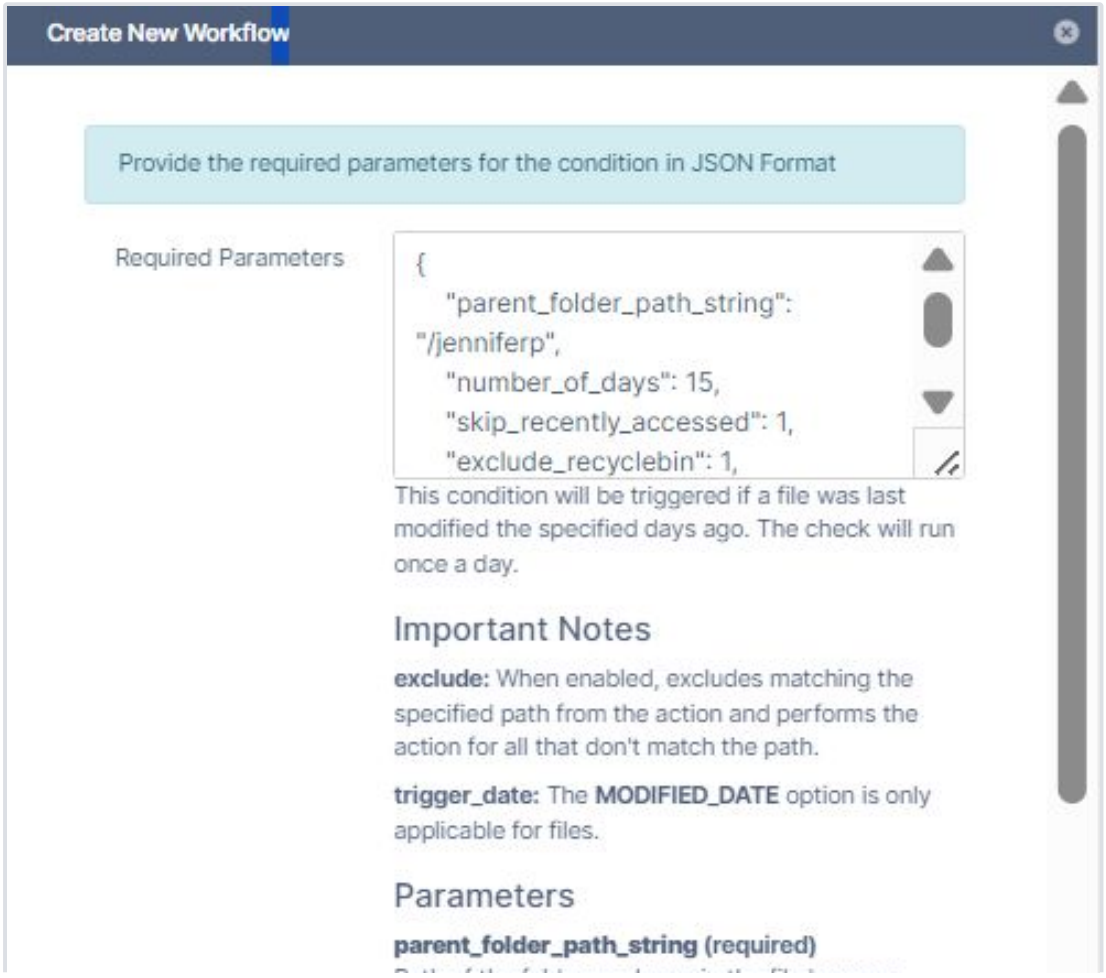
- The workflow checks the number of days a file was unused and generates a report.
- You can provide a set of email IDs the generated report will be emailed to.

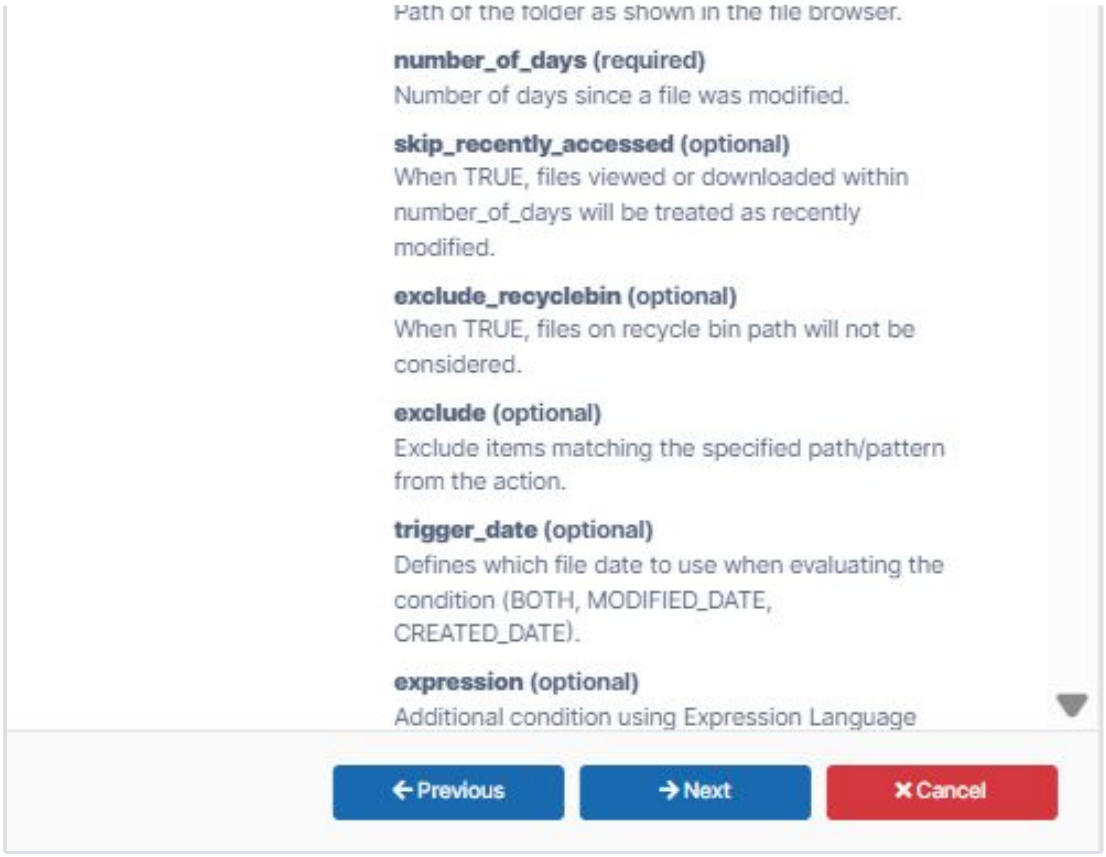
**To create a workflow that detects and generates a list of inactive files**:

1. Log in to the  admin portal.
2. Click **Workflow** in the navigation panel.
3. Click **Add Workflow**.
4. Set **IF Condition** to **If file was not modified/created for specified days**, and click **Next**.




5. Enter the parameters in the given format.



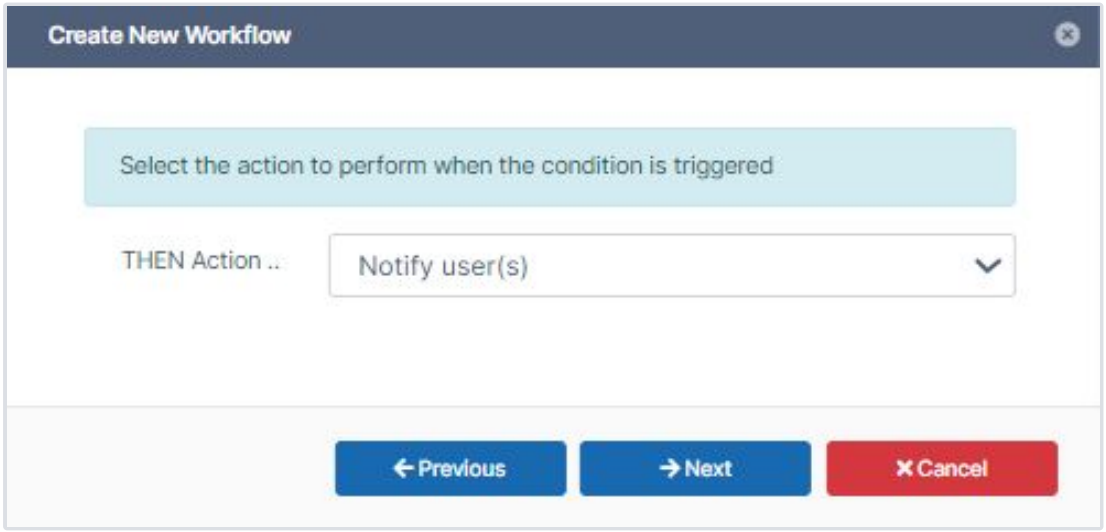



For example:

```
{
    "parent_folder_path_string": "/jenniferp",
    "number_of_days": 15,
    "skip_recently_accessed": 1,
    "exclude_recyclebin": 1,
    "exclude": ".*secret.*",
    "trigger_date": "BOTH",
}
```

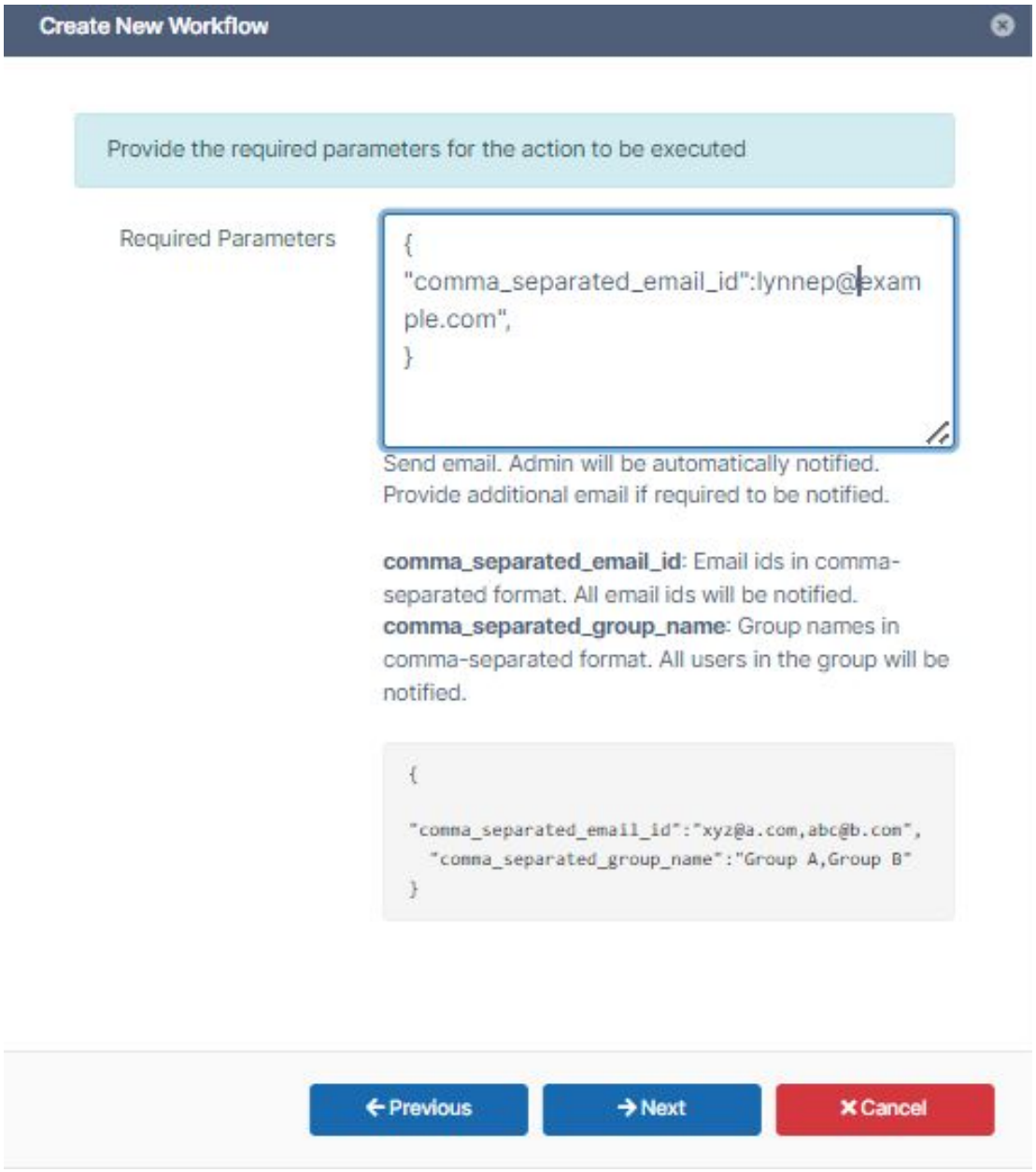
**Note**: This workflow applies only to Managed Storage and not to Network Folders.
To identify a FileCloud specific path for a folder please refer to Identifying a FileCloud Specific Path (see page 275).

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

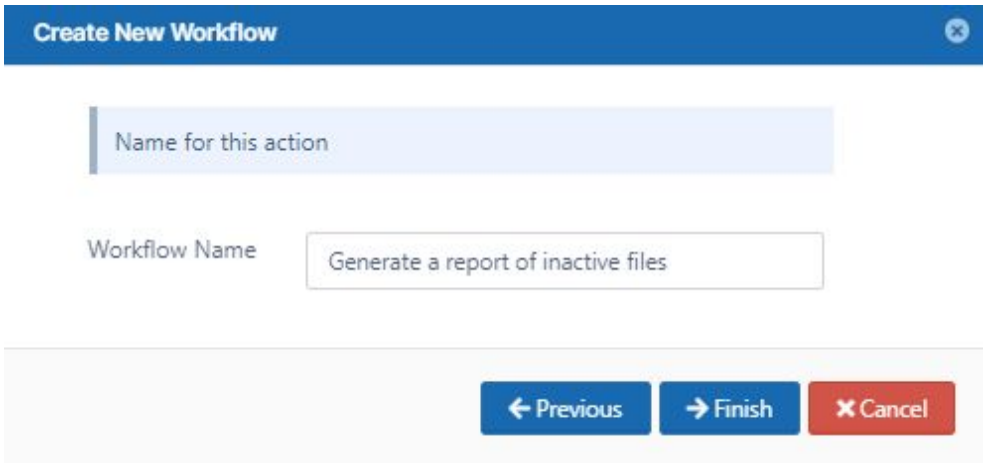



8. Click **Next**.
9. Enter the parameters in the given format.
   For example,

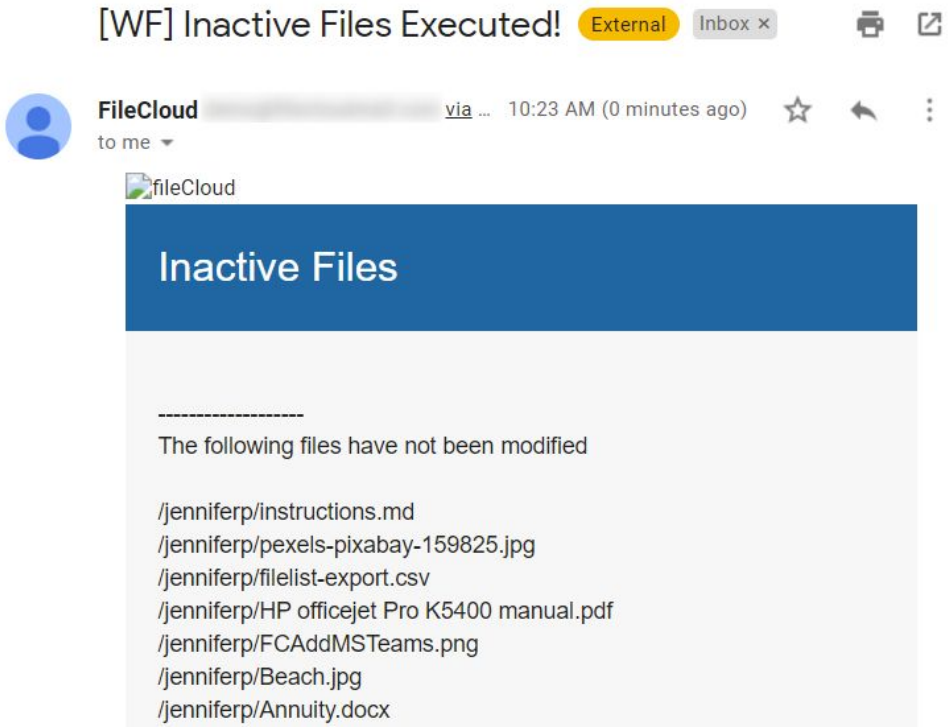
```
{
"comma_separated_email_id":"lynnep@example.com"
}
```




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




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




## Detect and Notify Failed Signatures Workflow

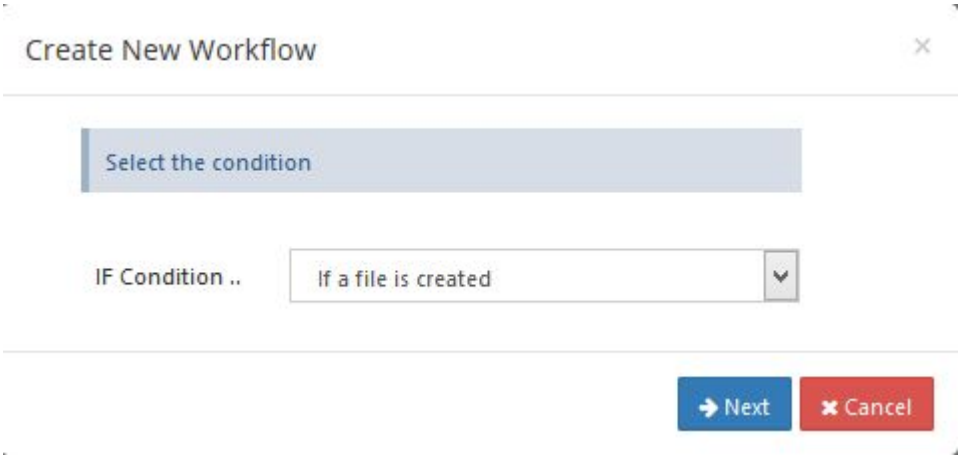
This workflow recipe creates an ALERT notification when a file is created or uploaded to FileCloud with a signature mismatch.

- This ALERT notification can be set for a specific folder location only.
- You can view the alerts on the Admin Portal in the alert panel.

**To create a workflow to detect and notify when a file with a signature mismatch is uploaded**:

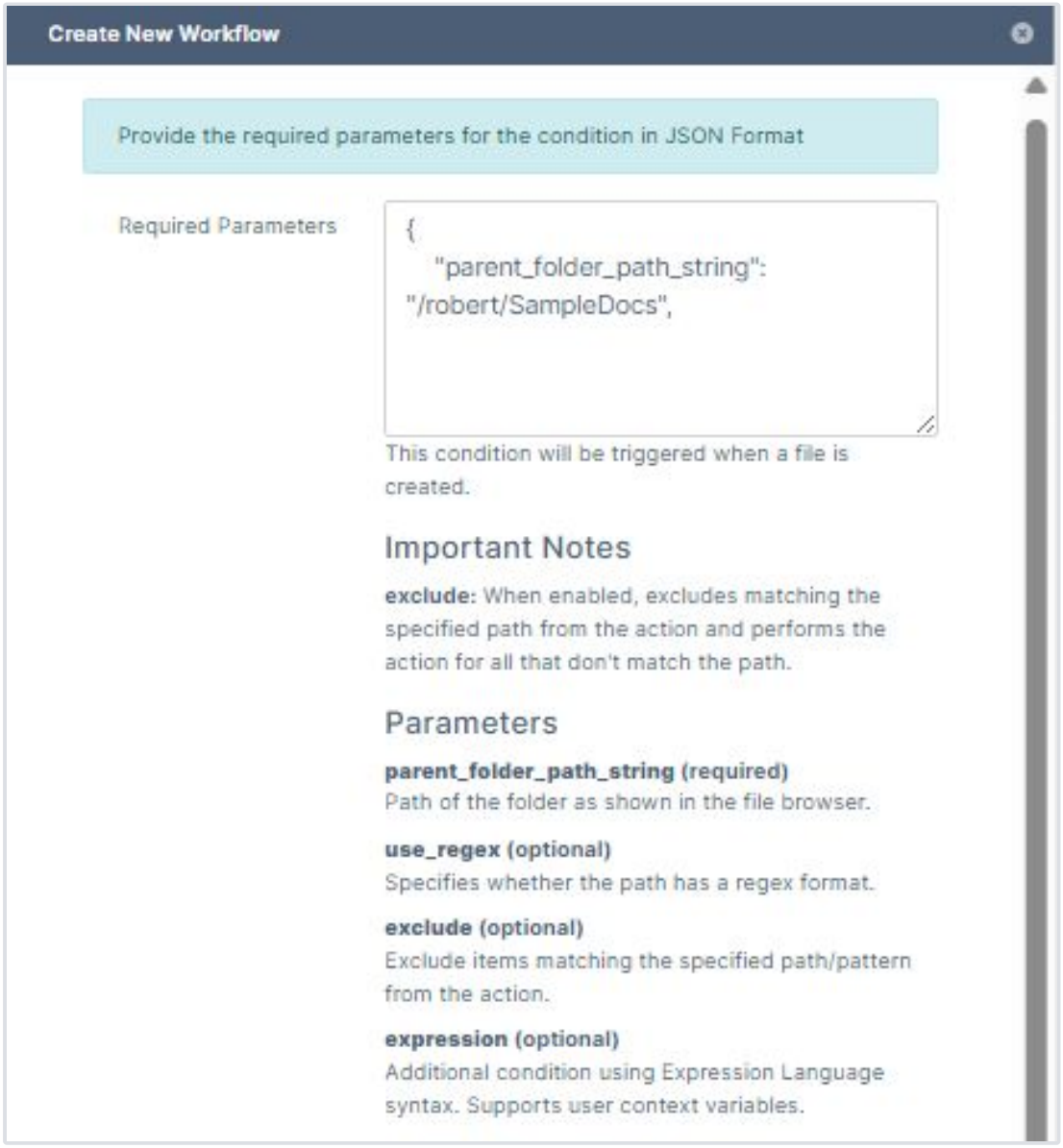
1. Login to Admin Portal

2. Navigate to **Workflow** on the left navigation panel.
3. Click the **Add Workflow** button.
4. Set the **If Condition** to **If a file is created.**

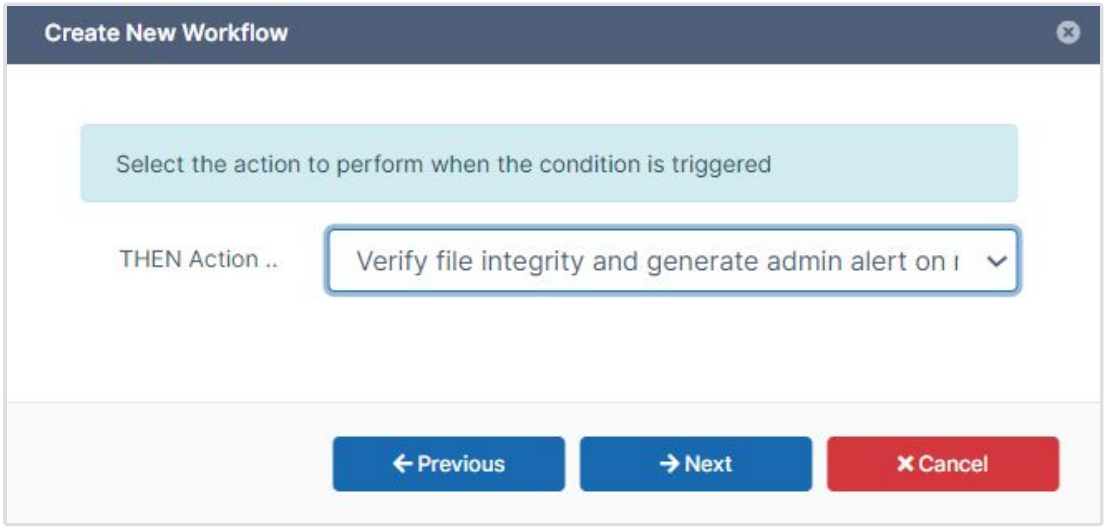



5. Click **Next.**
6. **Set the parameters as shown in the following screenshot.**
   To identify a FileCloud specific path for a folder please refer to Identifying a FileCloud Specific Path (see page 275).

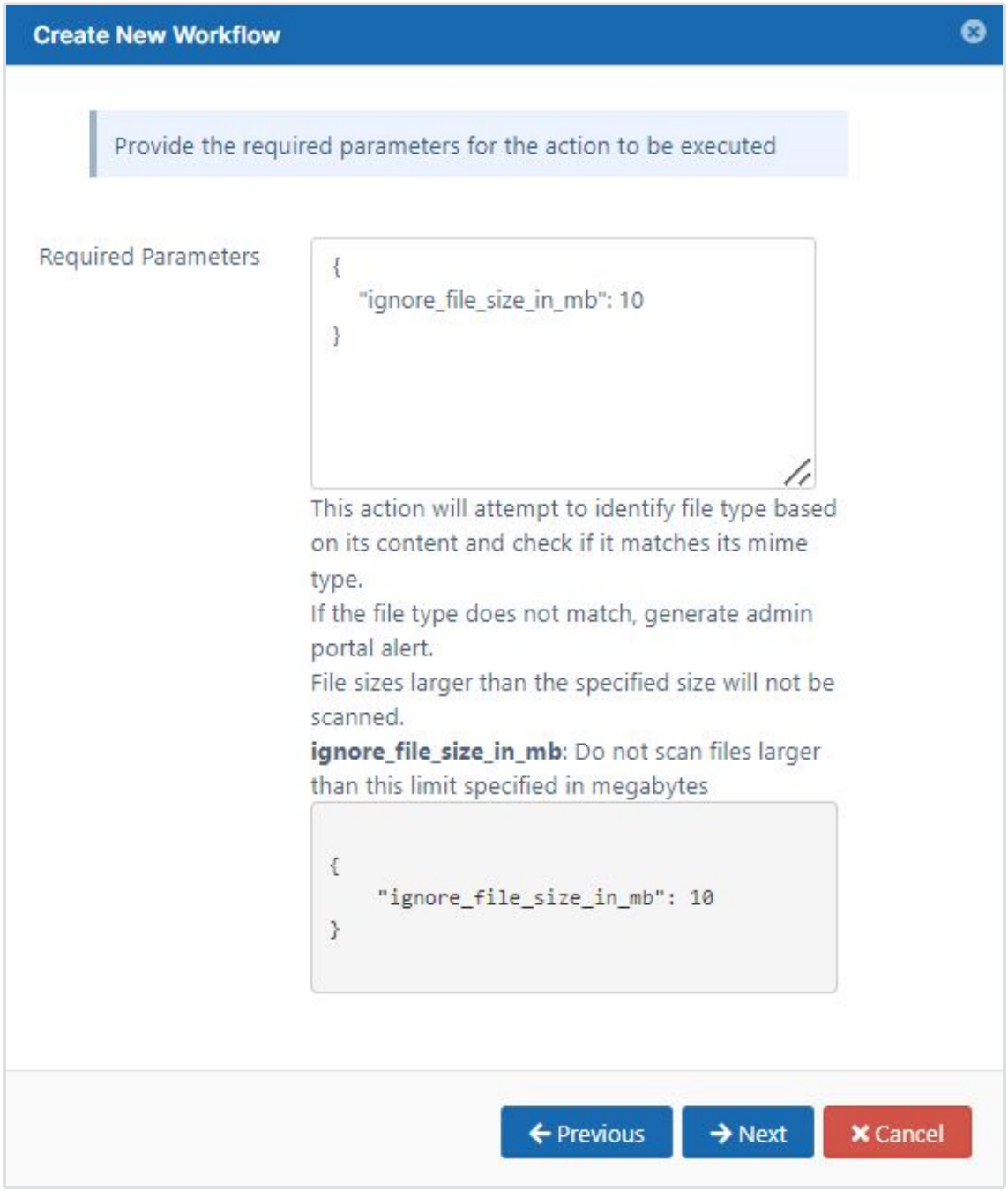
> Set the path to "/" if you want to monitor all the folders in the system.

7. 

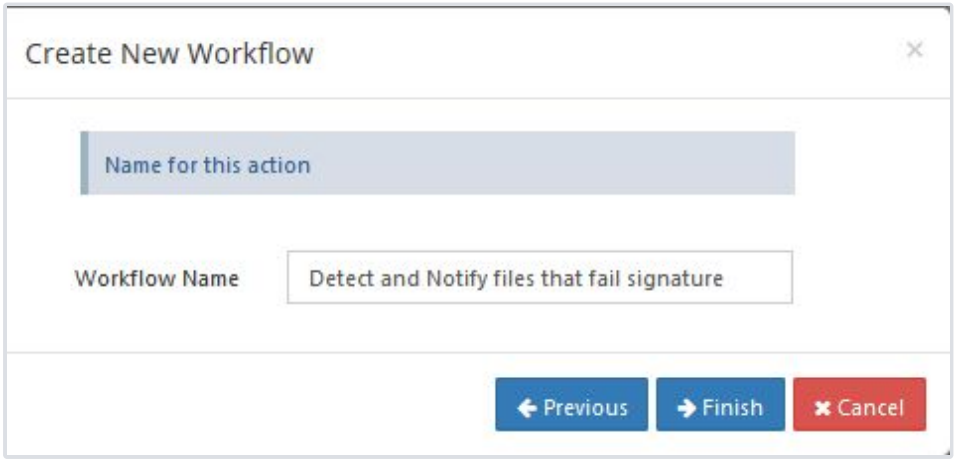

Click **Next**, and set **Then Action** to **Verify file integrity and generate admin alert on mismatch**



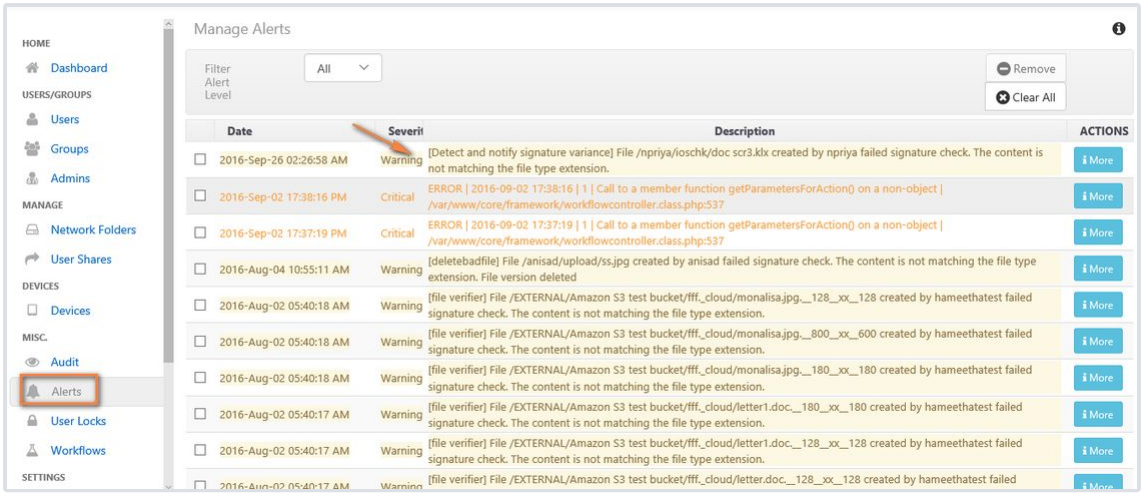

8. **Click Next**, and **enter the size limit of files to scan.**




9. **Click Next**, and give **a name to this workflow.**




Once this workflow is set, the Admin receives alert messages in the **Alerts** page.



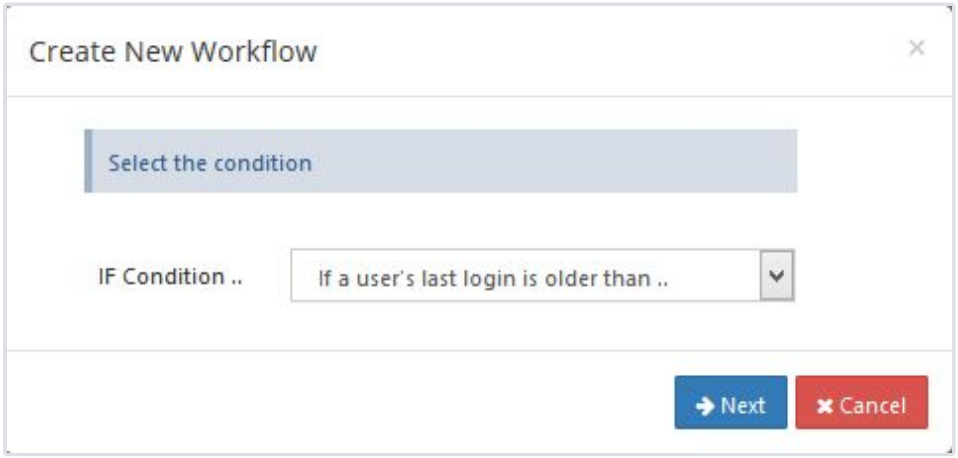

## Detect and Notify Inactive Users Workflow

This workflow recipe sends an email report with a list of all the inactive users.

- The last login date of the user is used to determine if the user is Active or Inactive
- You can avoid looking at users who have not begun using FileCloud
- You provide a set of email ID's to which the generated report will be mailed

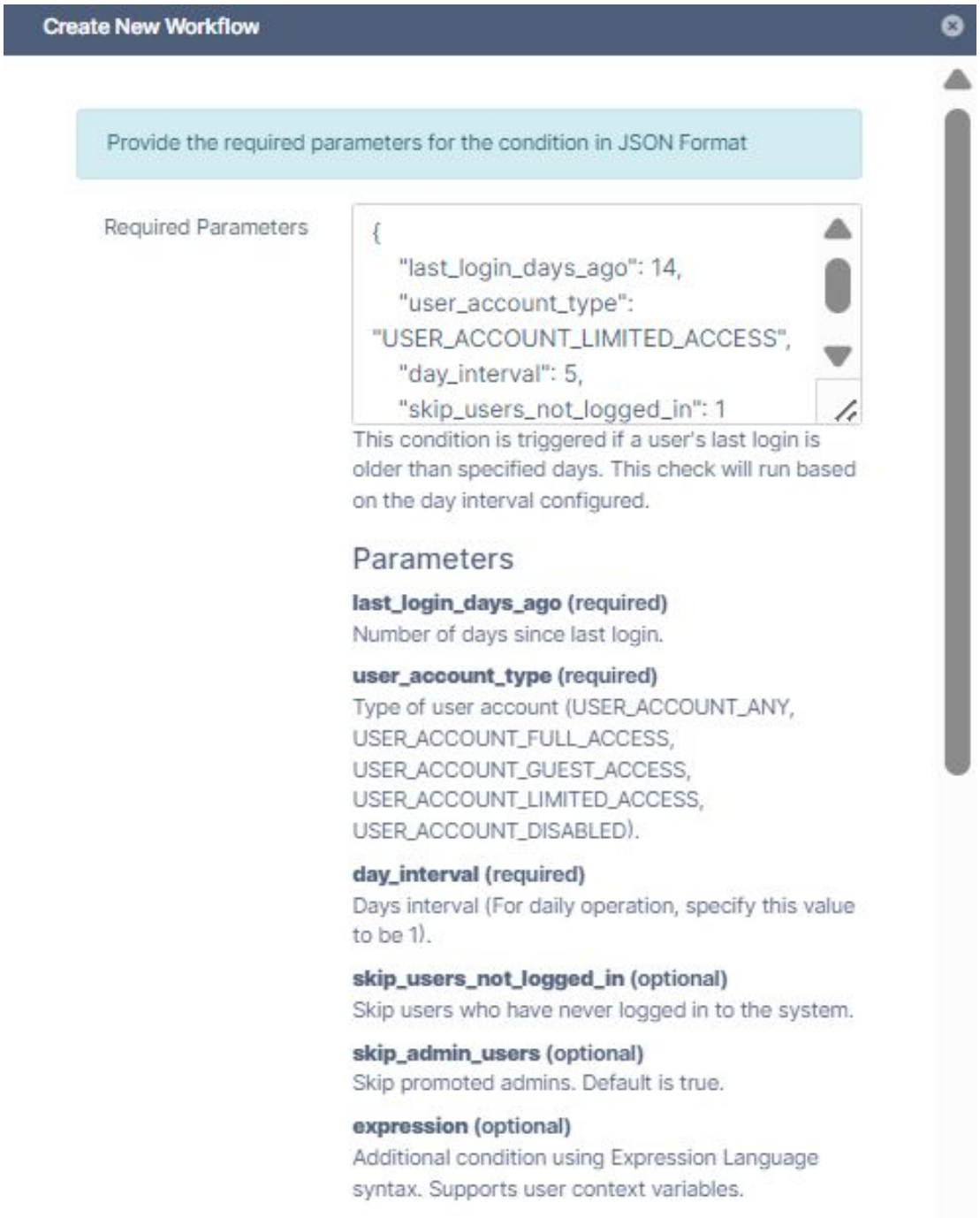
**To create a workflow that sends an email report with a list of all the inactive users**:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition **If a user's last login is older than..**, and click **Next**.

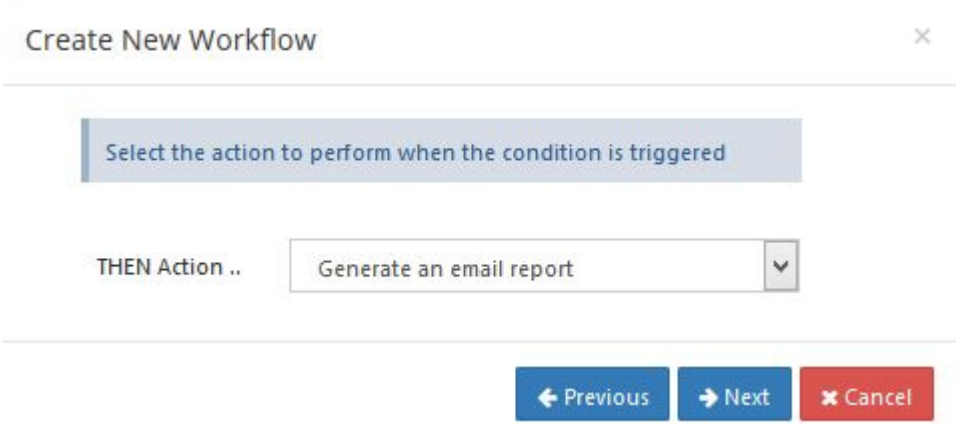



5. Enter the required parameters in the given format

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

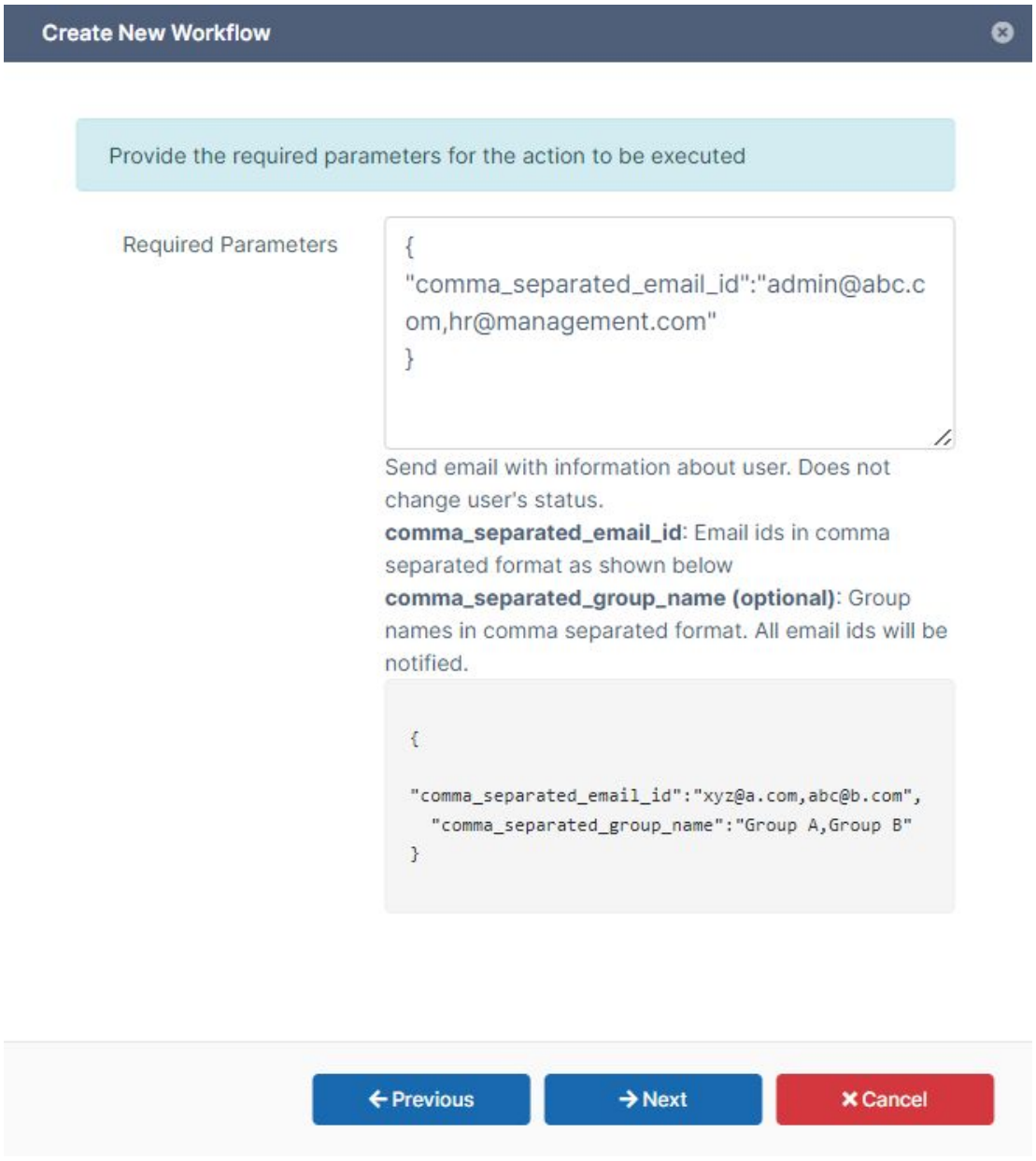



6. Click Next, set Then Action **Generate an email report**.




7. Enter the Required parameters in the given format

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




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

## Notify on File Upload Workflow

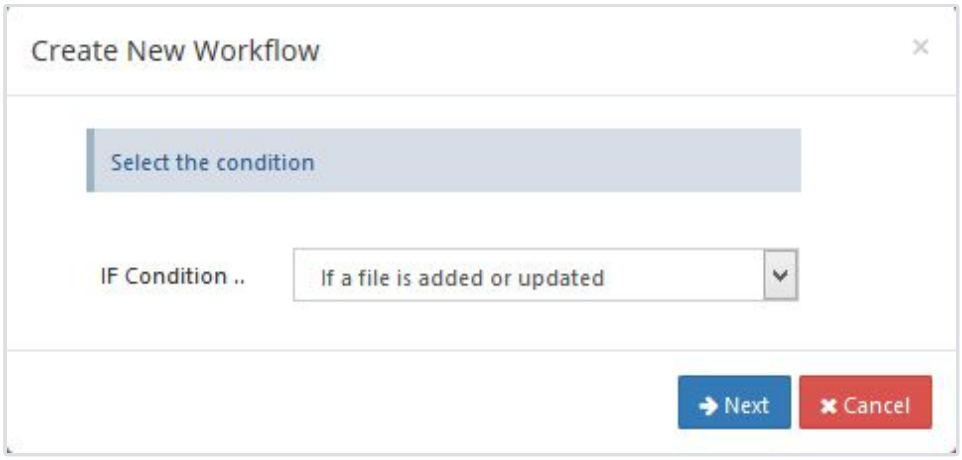
This workflow recipe sends an email notification when a file is created or uploaded to FileCloud.

- This notification can be set for a specific folder location only
- The admin can provide a set of email ids to which the notification email has to be sent

**To create a workflow to notify when a file is uploaded**:

1. Login to Admin Portal

2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition to **If a file is added or updated** and click **Next**

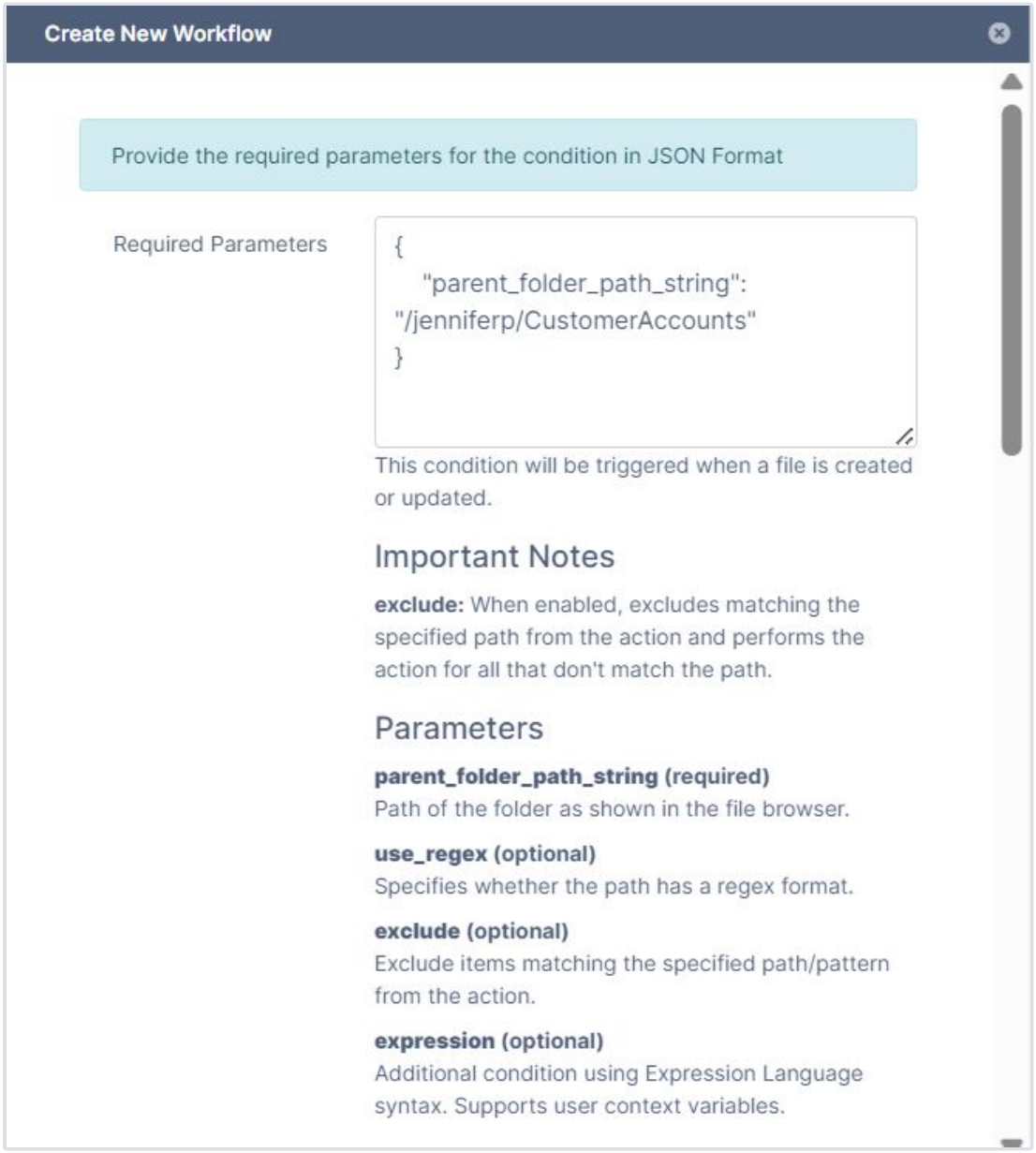



5. Enter the Required parameters in the given format, and click **Next**.

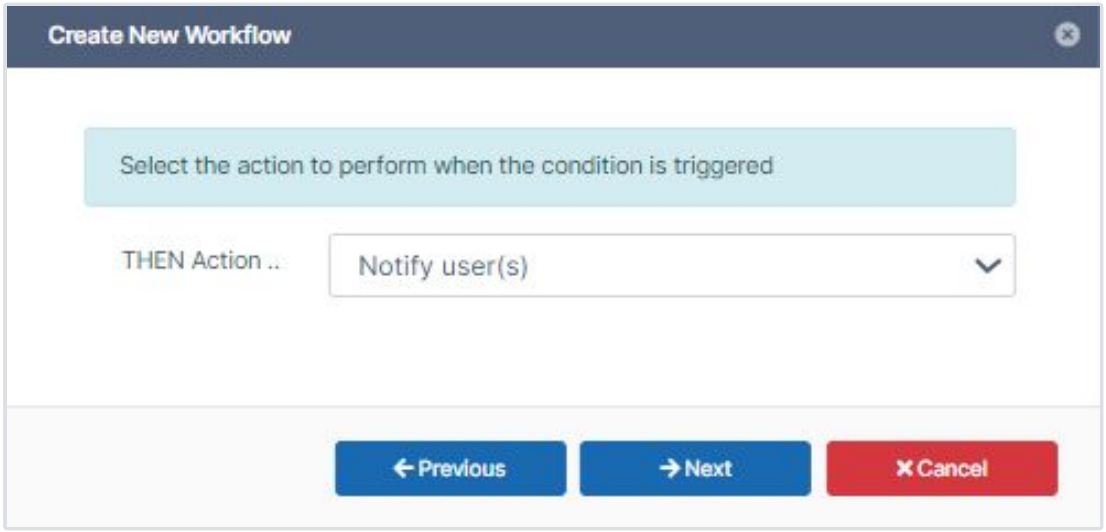
```
eg: Path : My Files Location (/jenniferp/CustomerAccounts)
{
"parent_folder_path_string":"/jenniferp/CustomerAccounts"
}
```

To identify FileCloud specific path for a folder please refer this Identifying a FileCloud Specific Path (see page 275).

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

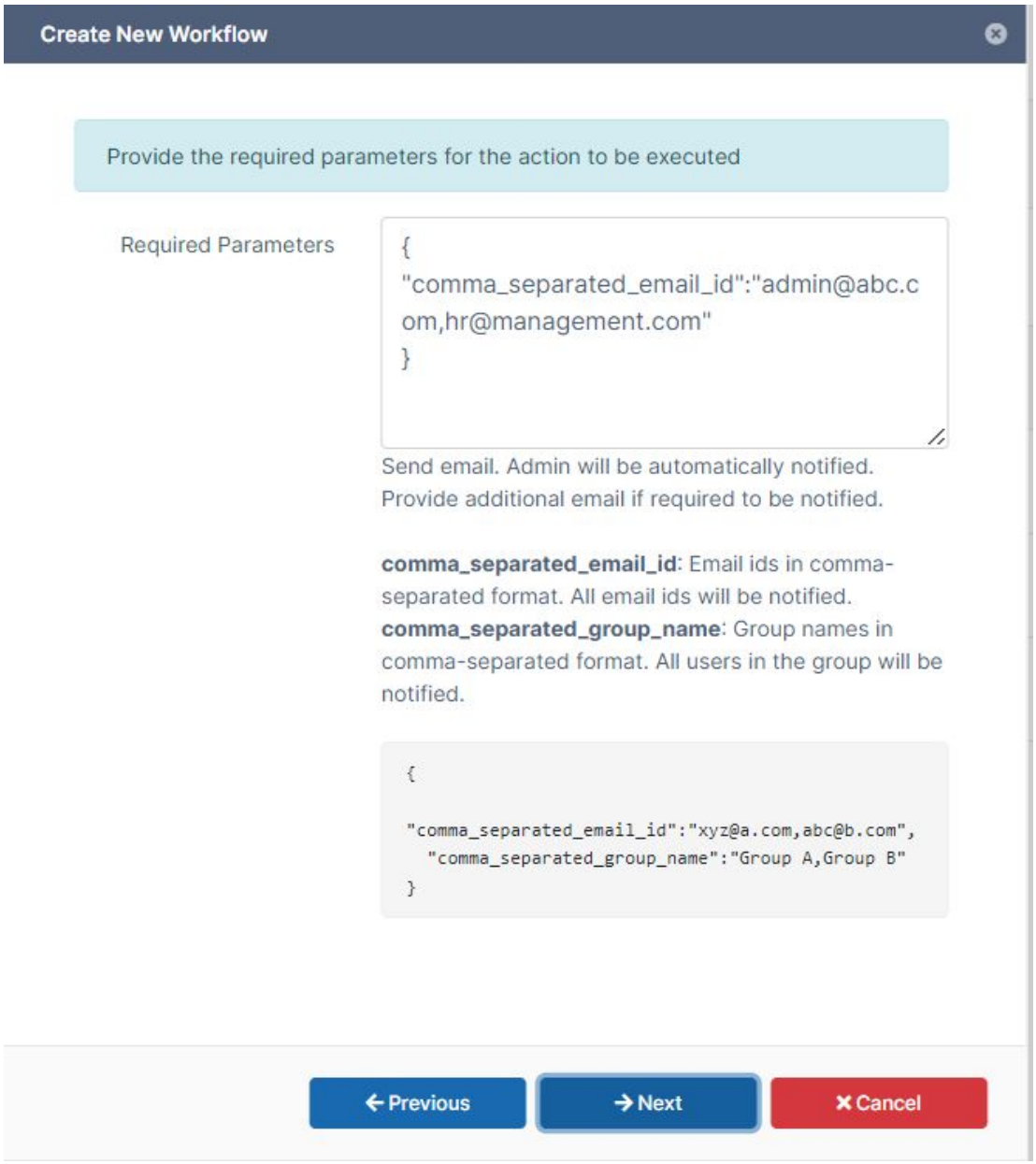



6. Set the then action to **Notify user(s)**, and click **Next.**

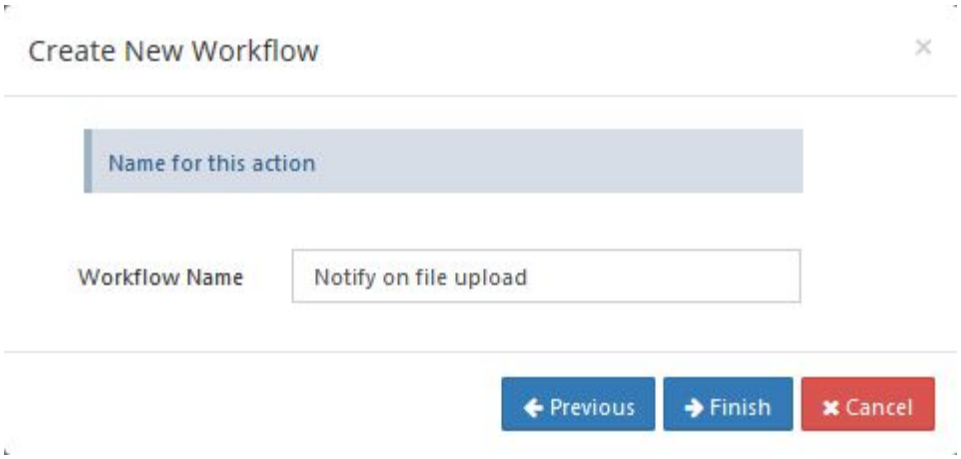



7. Enter the Required parameters in the given format

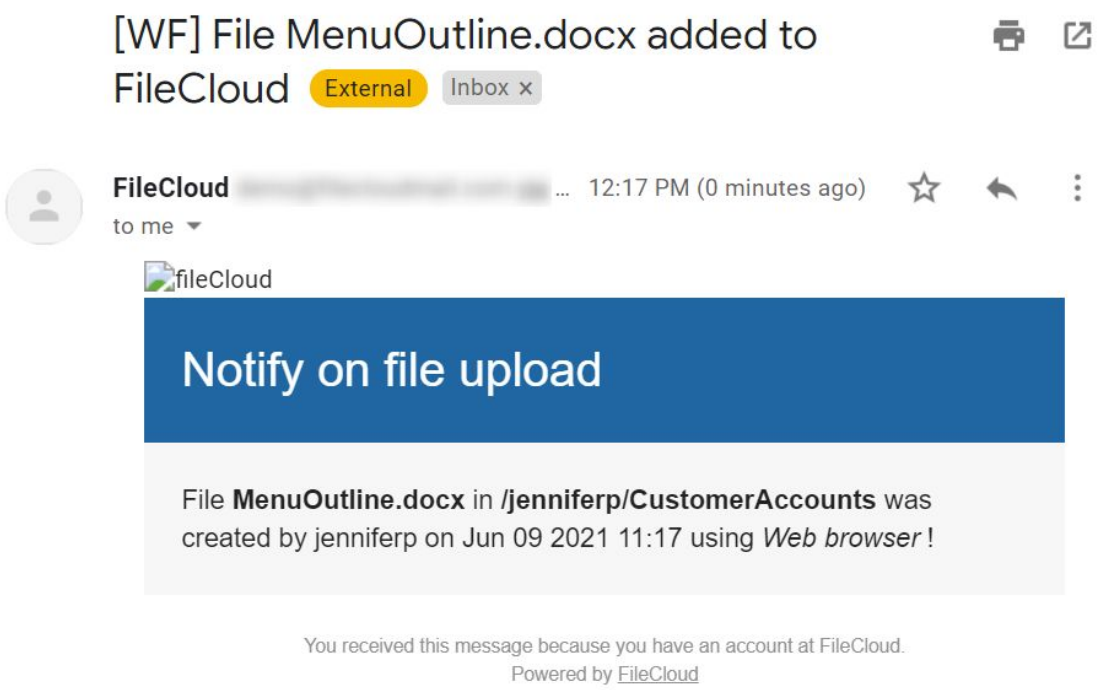
```
{
"comma_separated_email_id":"admin@abccompany.com,hr@management.com"
}
```




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




9. Sample notification email on a file upload.




## Periodic Script Workflow

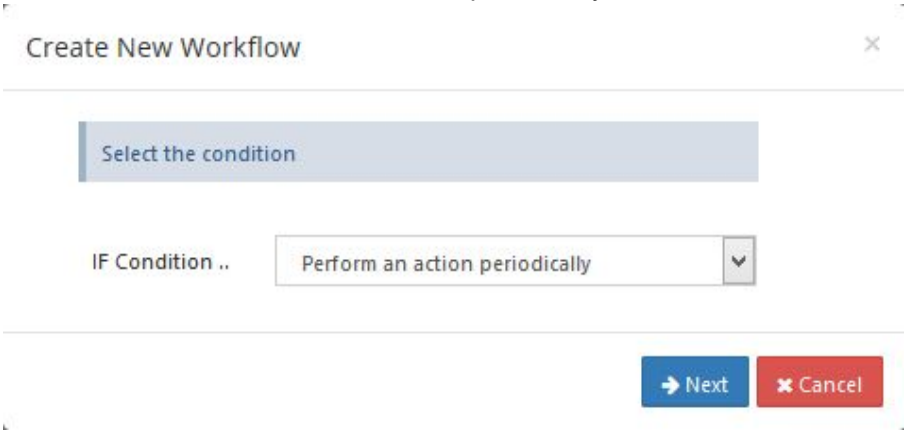
This workflow recipe runs a specified command at a periodic interval.

- This requires you to set up cron job or task scheduler to run the command.

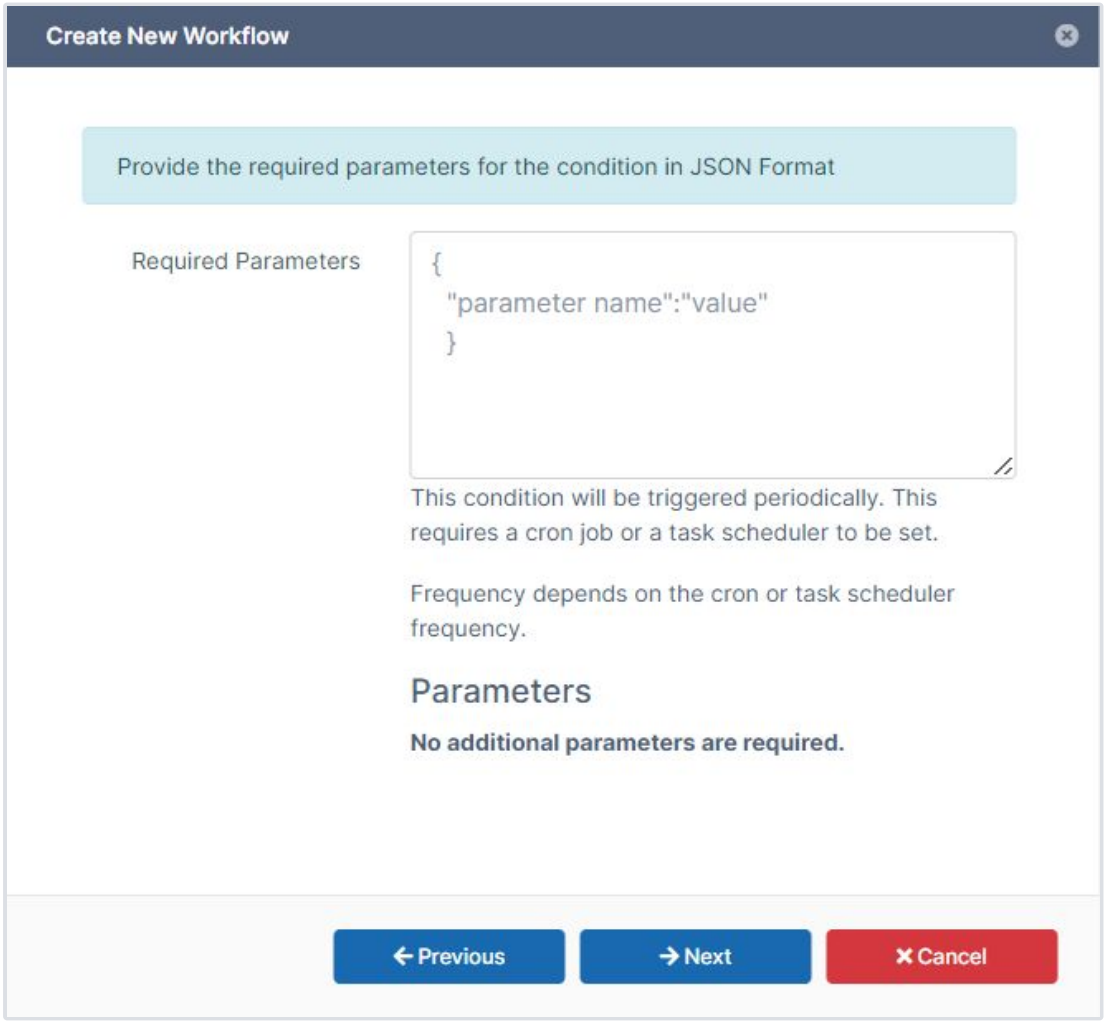
- The frequency depends on the cron or task scheduler frequency you set

**To create a workflow that performs a periodic script**:

1. Login to Admin Portal
2. Navigate to Workflow on the left navigation
3. Tap on the Add Workflow button
4. Set the If Condition " Perform an action periodically "




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



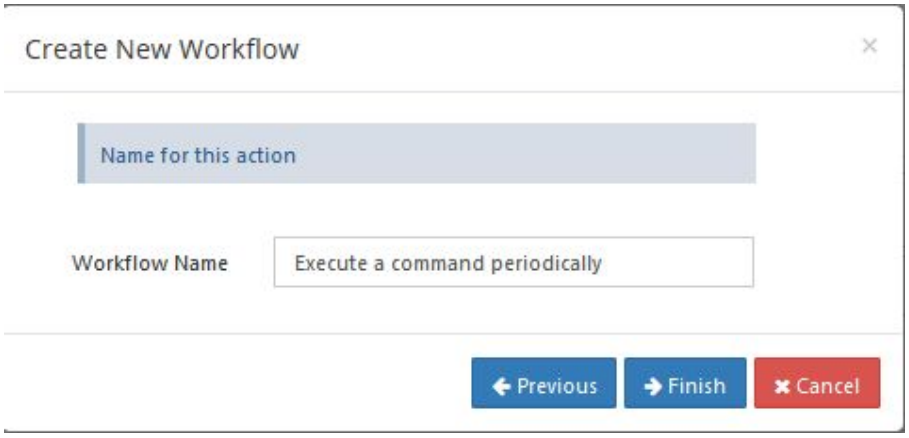

6. Set the Then Action "Execute a command"

7. Enter the required Command.
   In the following example, ls causes all files and folders to be listed.:

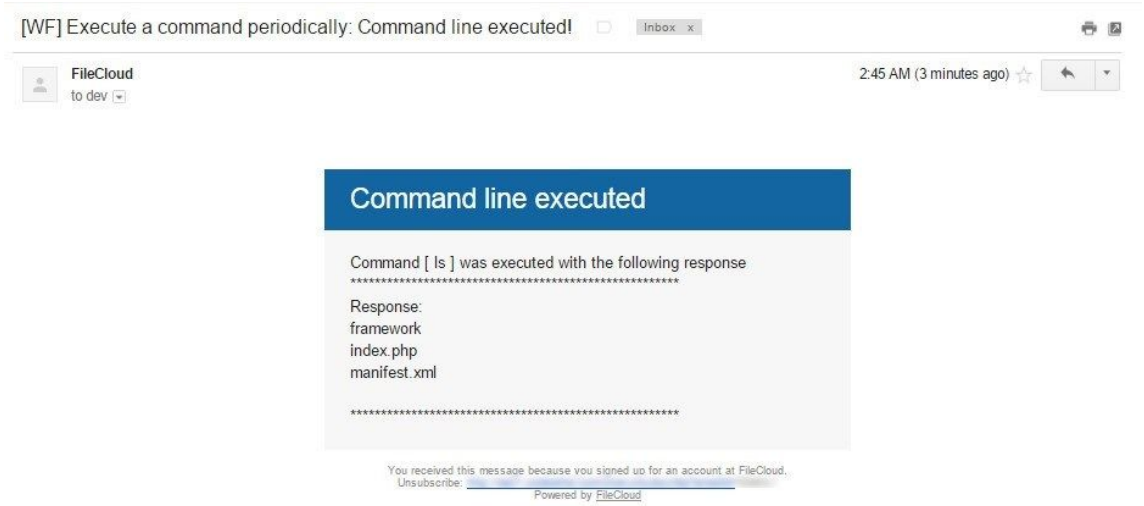
```
{
"command_line":"ls"
```

```
}
```

8. Enter the Workflow name and Finish.




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



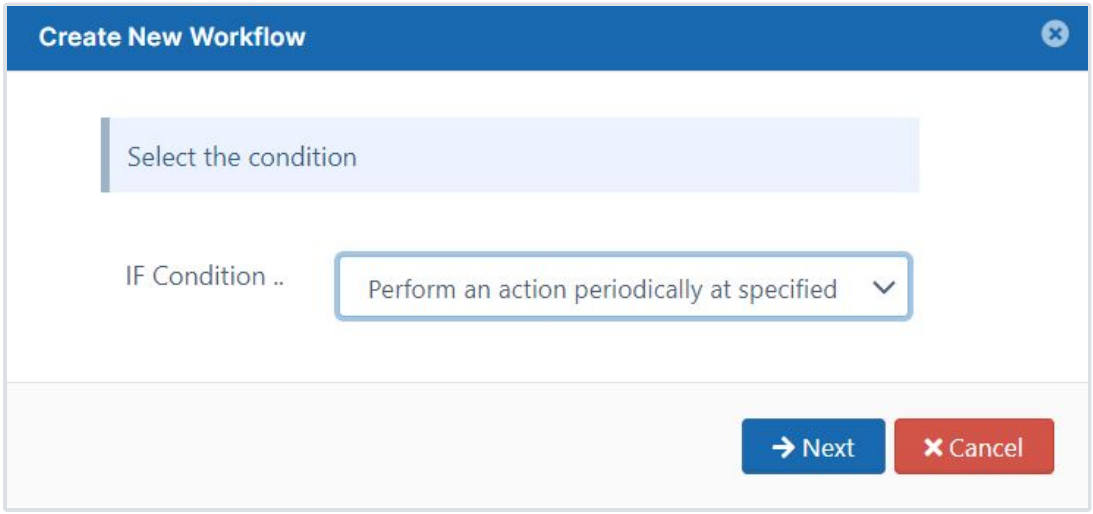

## Periodically Send Custom Email Workflow

This workflow recipe sends a custom email to selected users at specified intervals.

In the example, an email is sent to users in the **Employees** group every 30 days from January to June to remind them to submit their receipts to a **Reimbursements** folder.

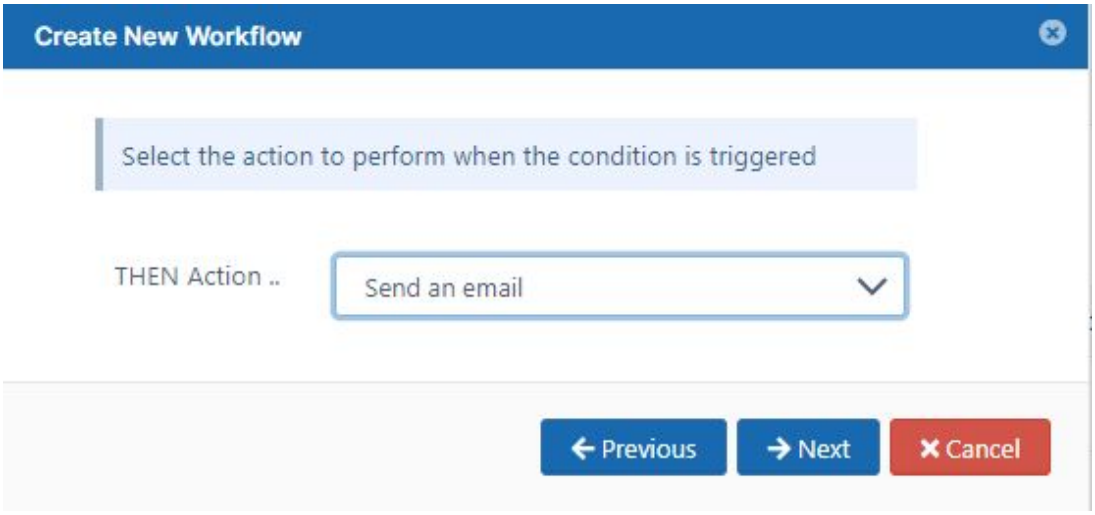
**To create a workflow that sends a custom email periodically**:

1. In the admin portal's navigation panel, click **Workflows**.
2. In the **Manage Workflows** screen, click **Add Workflow**.
3. In **IF Condition**, choose **Perform an action periodically at specified time and interval**.



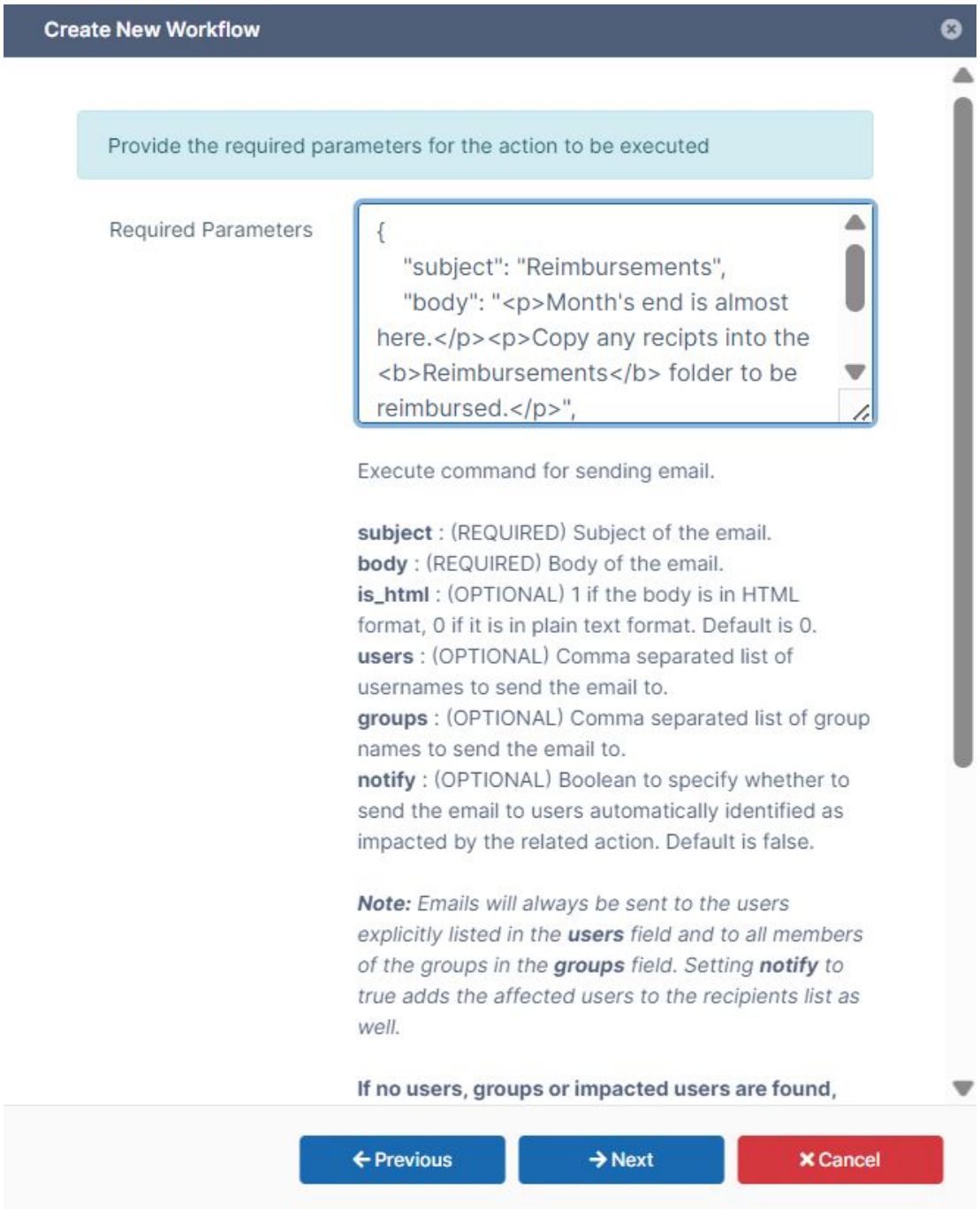

4. Click **Next**.
5. Set the parameters according to your requirements for the interval.
   In the image below, the message is scheduled to be sent approximately monthly for the first half of 2024 (every 30 days from January 1, 2024 to June 30, 2024).

6. Click **Next**.
7. In **THEN Action**, choose **Send an email**.

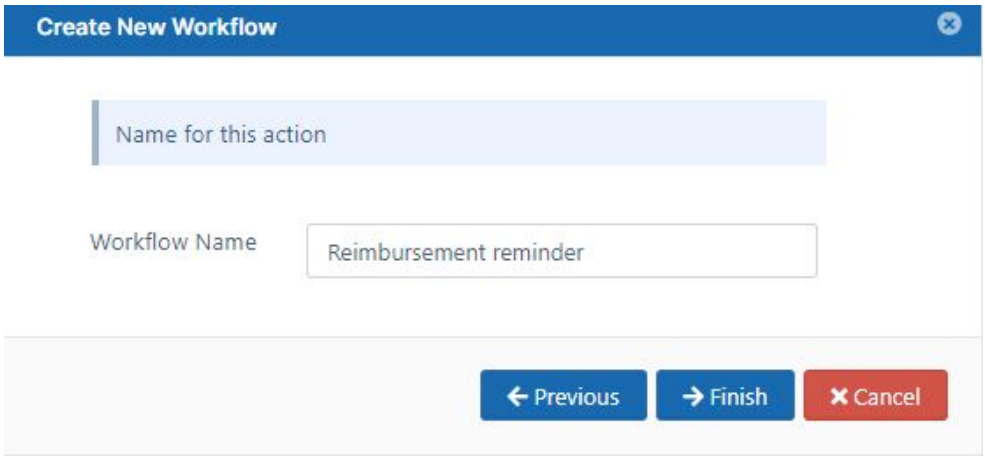


8. Click **Next**.
9. Use the parameters to enter the details of the custom email.
   In the parameters below, an email with the subject **Reimbursements** reminds users in the group **Employees** to copy their receipts into the Reimbursements folder.
   Since **is_html** is set to **1**, tags in the body are recognized as HTML tags and formatted.

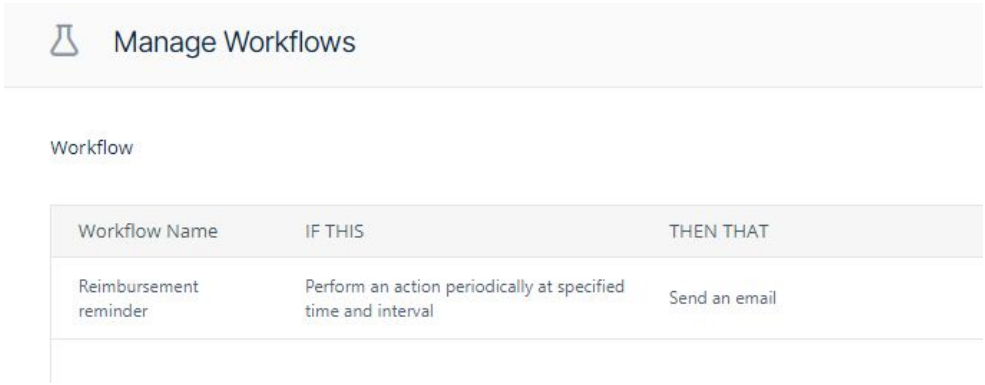
```
{
    "subject": "Reimbursements",
    "body": "<p>Month's end is almost here.</p><p>Copy any recipts into the
<b>Reimbursements</b> folder to be reimbursed.</p>",
    "is_html": 1,
    "groups": "Employees",
}
```



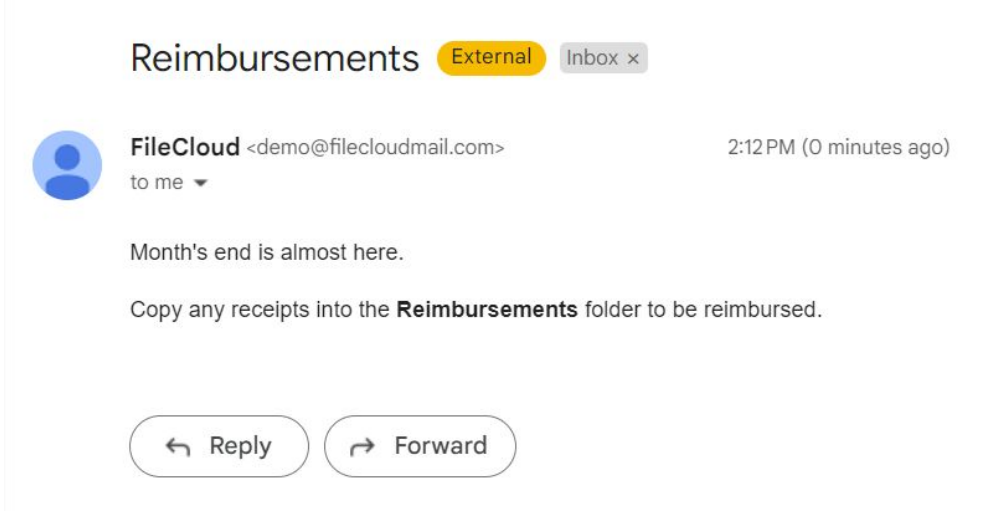

10. Click **Next**.
11. Give the workflow a name, and click **Finish**.




The workflow is listed in the **Manage Workflows** page. It will run automatically in 30 days.




12. In 30 days, the workflow automatically runs, and sends the following email to users of the group **Employees**.



## 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
```

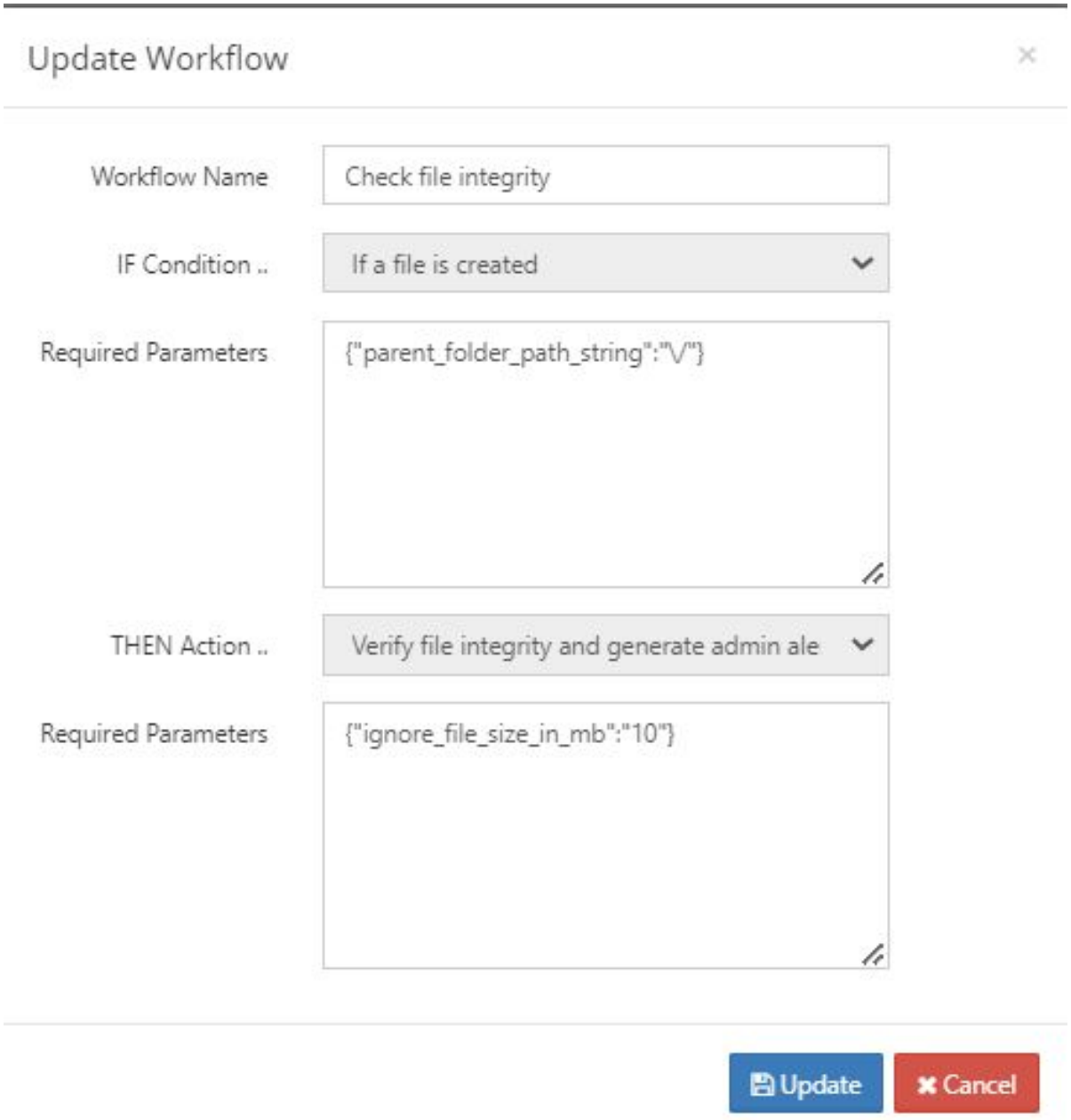
```
[Install]
WantedBy=multi-user.target

>> systemctl daemon-reload

>> service fcorchestrator restart
```

# Troubleshooting Workflows


- Integrity Check Not Working in Linux (see page 477)


## 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.




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

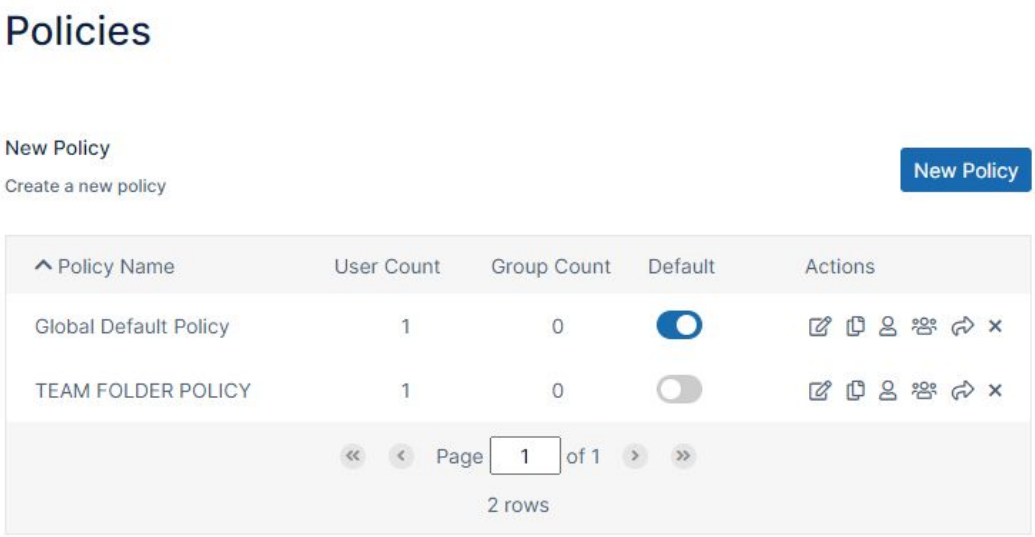
Automated Workflows are available in FileCloud 21.2 and later.
Prior to FileCloud 23.251, by default, all users could share automated workflows. Beginning in 23.251, the setting **Allow Automation Workflow Sharing** must be enabled to permit all users to share automated workflows.

## Disabling Automated Workflows

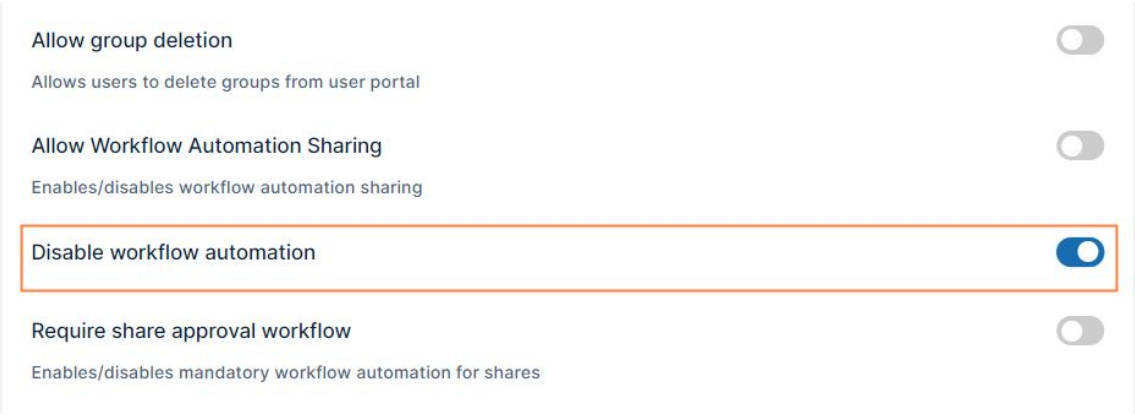
Automated Workflows enable users in the user portal to create automated processes, such as file approvals and file storage. By default the Automated Workflow function is enabled, but you can disable it.

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.




2. Open the policy assigned to the users who you do not want to access Automated Workflows.
3. Click the **Users** tab.
4. Scroll down and locate the **Disable workflow automation** setting. Enable the setting.



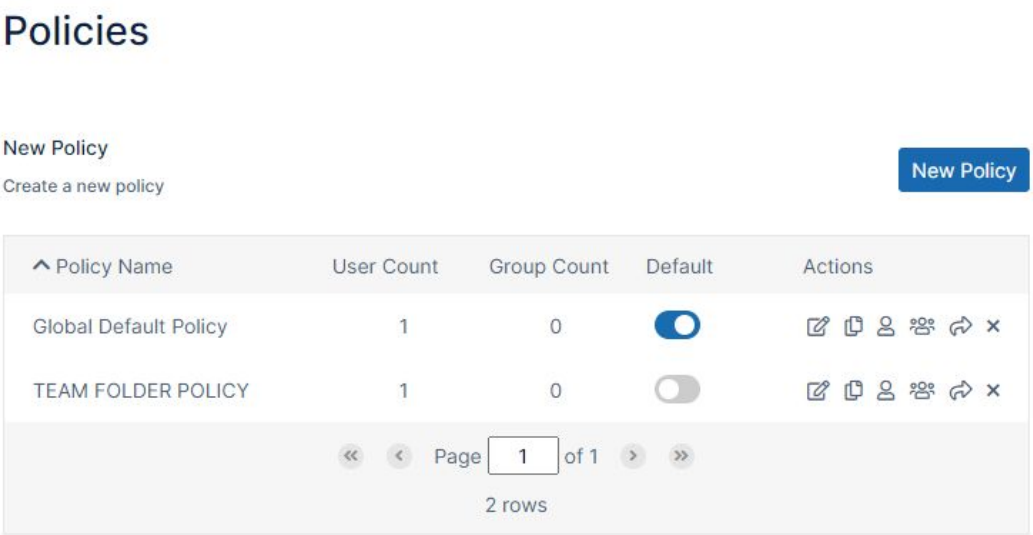

5. Click **Save**.
   The **Workflows** navigation link no longer appears in the user portal of users assigned to the policy.

## Enable Sharing of Automated Workflows

By default, users other than promoted admins with all user share and file privileges, cannot share automated workflows with other users. Enabling this setting allows all users to share automated workflows.

To enable sharing of Automated Workflows for certain users, enable the setting in the users' policies.

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




2. Open the policy assigned to the users who you want to be able to share automated workflows.
3. Click the **Users** tab.

4. Scroll down and locate the **Allow Workflow Automation Sharing** setting. Enable the setting.

5. Click **Save**.
   Now, all users have the ability to share automation workflows.

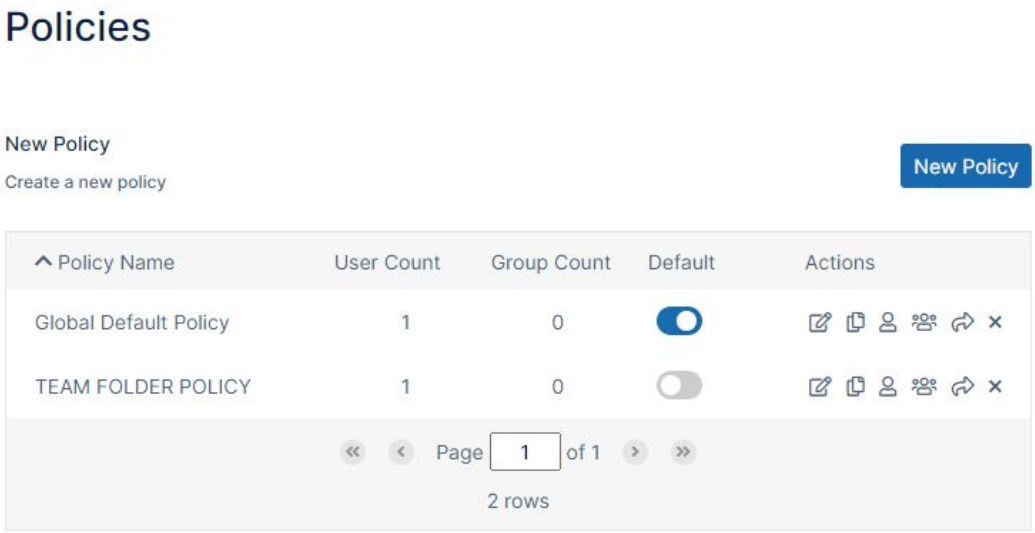
## Requiring a Share Approval Workflow

A Share Approval workflow is a specialized type of workflow that requires a share to be approved before it is made available.
In order for a Share Approval workflow to become active for specific users, you must mark it required in their policies and choose the specific Share Approval workflow to use.

For the Share Approval workflow to apply to all users' shares in FileCloud, it must be created by a promoted Admin (see page 48)with all User Share permissions enabled. Otherwise, the share approval workflow will only apply to shares initiated by the workflow creator on files and folders in their My Files folder.

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

The **Policies** page opens.




2. Open the policy assigned to the users who you do not want to access Automated Workflows.
3. Click the **Users** tab.
4. Scroll down to **Require share approval** and enable it**.**
5. In **Selected Workflow**, choose the Share Approval workflow to make effective.

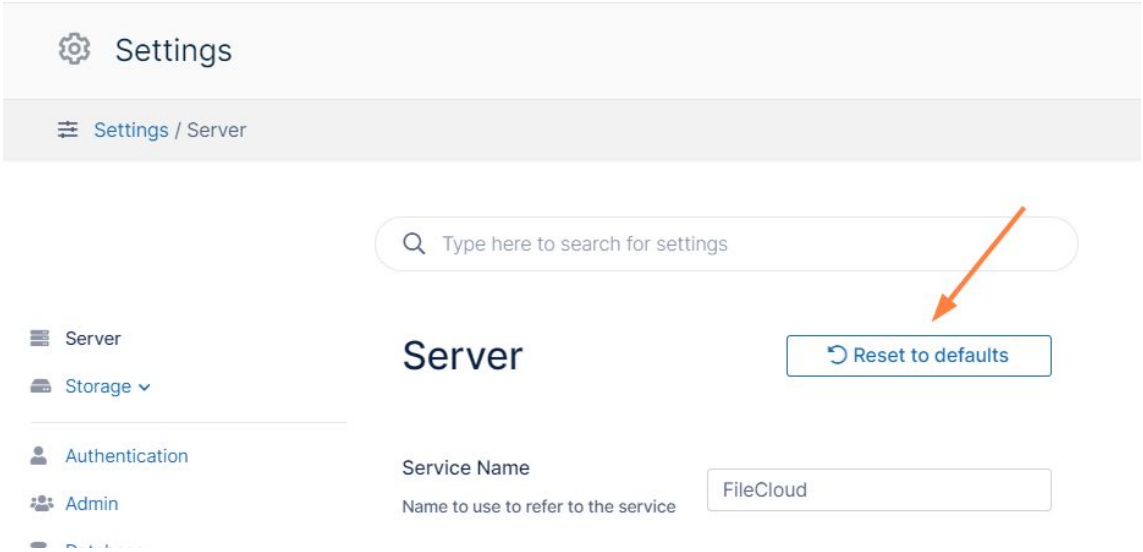
For end user information on creating Automated Workflows, see Workflow Automation.

# Reset Settings and Customizations

Beginning in FileCloud 20.1, the option for resetting all selections in the Settings and Customization pages is located in the Reset tab on the Settings page. In FileCloud versions earlier than 20.1, the **Reset All** button appears in the upper-right corner of the Settings and Customization pages and resets both settings and customizations regardless of which page you access it from.

## To return to default settings for options in Settings

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**, then navigate to the page whose settings you want to reset.
2. Click the **Reset to defaults** button in the upper right of the page.



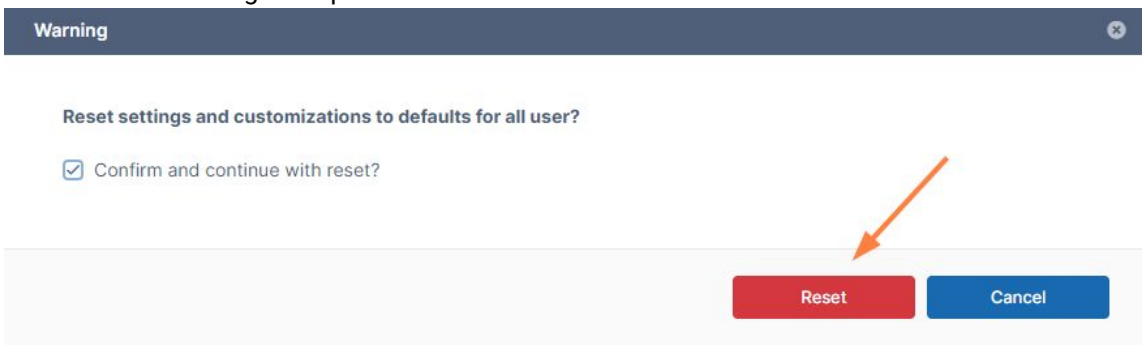

A confirmation dialog box opens.

3. Click **OK.**
The settings on the page are set back to their default settings.

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

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Reset** .
The Reset page opens.
2. Click **Reset All Settings and Customizations**.

A confirmation dialog box opens.




3. Check **Confirm and continue with the reset**, and click **Reset.**
   All of the options that appear on the Settings and Customization pages are reset to their defaults.