FileCloud Server
Version 23.263
FileCloud Site Setup

13 October, 2026

Table of Contents

Navigating and Searching for Settings 4
Going to the Settings landing page 4
Go to a settings page 4
Reset settings 8
Server Settings 10
Setting Up a Cron Job or Scheduled Task 13
Storage Settings 21
FileCloud Managed Storage 21
Setting Up Network Folders 155
Administrator Settings 265
Resetting Admin Password 265
Changing the Default Login Name 271
Account Locked Alerts 271
FileCloud High Availability 274
FileCloud High Availability Architecture 274
Installation and Configuration of 3 server MongoDB cluster 276
Configure Memcache for HA Environments 284
Configure Solr for HA Environments 286
Install and Configure FileCloud Web Servers for HA 287
Configure Storage for HA 294
Set Up Load Balancing 297
Installation and Configuration of Standalone Backup Server 300
HA System Tests and License Installation 301
Configure Cluster Authentication with SSL 302
Multi-Tenancy Settings 310
Multi-Tenancy Requirements 310
Enable Multi-Tenancy Support 311
Password encryption and logging in to a multi-tenant admin portal 311
Manage Different Sites 313

Enable Email Notifications if Cluster is Down 316
Enable Automatic License Renewal and Reporting 319
Folder-Level Permissions 322
Setting Folder-Level Permissions from the Admin Portal 322
Enabling Users to Set Folder-Level Permissions 331
Setting Folder-Level Permissions on Team Folders 336
How Folder-Level Permissions and Share Permissions Work Together 347
More Examples 354
Team Folders 360
Configure the Team Folders Account 361
Seed and Organize Team Folder Data 370
Share the Team Folder and Set Permissions 375
User Settings 382
Create FileCloud Users 382
New Account Creation 395
Preload data for new accounts 437
Password Settings 439
Restrict Commonly Used Passwords 443
User Session Expiration 444
Changing the Storage Quota for Users 447
Customize the User Login Screen 453
Limiting File Upload Size for Users 459
Remove the Export Secure Doc Option 461
Disabling Send for Approval 462
Group Settings 465
What do you want to do? 466
Giving Users Group Management Permissions 478
Assign the Externals Group the Same File Access as the Everyone Group 481
Admin User and Role Settings 482
User Authentication Settings 489
Comparison of Default authentication, AD, and LDAP 489
Enabling Default Authentication 490

Active Directory Authentication 490
LDAP Based Authentication 520
Multi-Factor Authentication 527
Single sign-on (SSO) 553
Oracle Identity Manager LDAP integration with FileCloud 692
Desktop Apps Code-Based Authentication 697
Enabling Basic Authentication 703
Allowing Duplicate Usernames 704
Share Settings 706
Configure Sharing Defaults 706
Set the Share Mode 722
Specify Sharing Expiration 723
Secure Shares 729
Document Settings 742
Setting up Content Search for Documents 742
Setting Up Document Preview 791
Import Files : Pre-seeding 824
Enabling ASCII Sort order for Listings of Users, Files and Folders 829
Enabling PDF Merge 830
Optimize PDF Preview 832
Managing File Extensions 835
Restricting File Names 839
Manage File Versioning 840
Configuring Zip Files and Zero Trust File Sharing 843
Watermark Settings 850
Adding a watermark rule 852
Customizing preview IDs 863
Watermark Parameters for Code Editor 864
Email Settings 870
SMTP Configuration 873
Do Not Email Settings 879
To limit the number of emails sent to a user 880

Configuring System Generated Emails 880
Endpoint Backup Settings 883
What Do You Want To Do? 883
Automatic Database Backup 889
Setting Up Persona Backup Using Sync 891
Disabling Deletion of Backup Files 894
Client Security Settings 896
Preventing an attacker from bypassing 2fa 896
Setting Client Application Policies 897
Using a Proxy Server 901
Improving Cookie Security 902
Configuring OAuth for SCIM Integration 905
Dynamic CSP in FileCloud 909
Identify Company Devices in FileCloud Desktop for Windows Logins 913
Online Web Editing 914
Microsoft Office Online Web Editing 914
Web Editing With Collabora Code 939
Web Editing with OnlyOffice 944
Web Editing with Google Apps 945
New Document Creation via Web Browser 956
Web Editing Text Files 958
Web Editing Markdown and Readme Files 959
Coauthoring Office Documents Using Web Edit 959
Disable Online Web Editing 960
Changing the locale in online Office documents 962
Policies 963
Working with Policy Records 967
Creating a New Policy Video 977
Managing Policy Users and Groups Video 977
Notifications for File Changes 978
FAQ's 978
Why is the user not getting a notification? 978

How to access notification settings in the admin portal 979
Changing notification settings 981
Example Setup: Fixed Notifications for Uploads and Deletions 990
Example Setup: User-enabled Notifications on Folders 995
Anonymizing User Data 1003
Misc Settings 1007
General settings 1007
User settings 1010
Notifications settings 1011
Other Misc. tab settings 1012
Terms of Service 1013
Enabling privacy settings and the Terms of Use checkbox 1014
Showing TOS when users access public and password-protected shares 1016
Terms of service settings 1017
See if a user has accepted terms of service 1019
Change the content of the Terms of Service 1020
Set Search Location 1022
Migrating your data from Varonis DatAnywhere to FileCloud 1024
Download your files and folder from DatAnywhere 1024
Integrate your Network shares with FileCloud! 1027
Migrating your files and folder to FileCloud 1028
Migrating your DatAnywhere files and folders using FileCloud's Sync Client 1029
Migrating Content with the Seeding Tool 1031
How To Seed Data 1031
Seeding Scenarios 1033
Related help: 1036
FileCloud Best Practices 1037
Deployment 1037
Performance 1039
Restricting Access To Admin UI Based On IP Addresses 1040
Restricting Access To User UI Based On IP Addresses 1041
Manage IP Checks 1042

Changing default config and log directory for FileCloud 1043
Disable CONNECT Method in HTTP 1044
Enforcing TLS 1.2 and TLS 1.3 and Strong Ciphers 1045
Security: Changing a Default Port or Web Server Setting 1045
Security: HTTPS Best Practices for FileCloud 1048
Security: Managing File Extensions 1053
Security: Bind MongoDB to 127.0.0.1 Only 1055

You must perform certain administrative tasks before FileCloud users can log in and use FileCloud efficiently. Some of the system settings and custom settings that you can configure are listed in the table below by priority and function.



Some of the pages linked to in the following table may suggest making changes to the file cloudconfig.php (this initially appears in your FileCloud installation as cloudconfig-sample.php). After making changes to `cloudconfig.php`, restart the message queue.

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Required	Access the Admin Portal Change the Admin Password Admin Portal Dashboard Manage Account Approvals	Admin Settings Server Settings Run Cron Jobs and Scheduled Tasks Configure Backup Settings Manage Client Security Settings Configure Share Settings	Choose how to deploy FileCloud Storage then, set up as applicable: Set Up Managed Storage If not using, Disable My Files Set Up Network Folders If using, Set Up Network Folders with NTFS permissions Configure Team Folders	Create FileCloud Users Check User Access Level Create User Policies Create Groups Manage User Storage Quotas

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Recommended	Configure Email Settings Restrict Access to the Admin Portal FileCloud Best Practices	Enable MongoDB Bind IP and Authentication Set Client Application Policies Configure Security Options		Manage User Authentication • Configure Single Sign-On • Use LDAP Based Authentication • Active Directory Authentication Set Up MFA Configure Microsoft Office Integration Options Configure Online Web Editing • Installing Office Online Server • Collabora Code • Google Docs Editing • OnlyOffice Editing Set Up Document Preview Set Up Content Search
Provides a Better Experience	Add Customization and Branding Enable Antivirus Scanning	Configure High Availability		Manage Document Settings Enable MS Teams Integration Set Up Notifications for File Changes Automate Business Workflows Enable Users to Set Folder-Level Permissions Enable reCaptcha

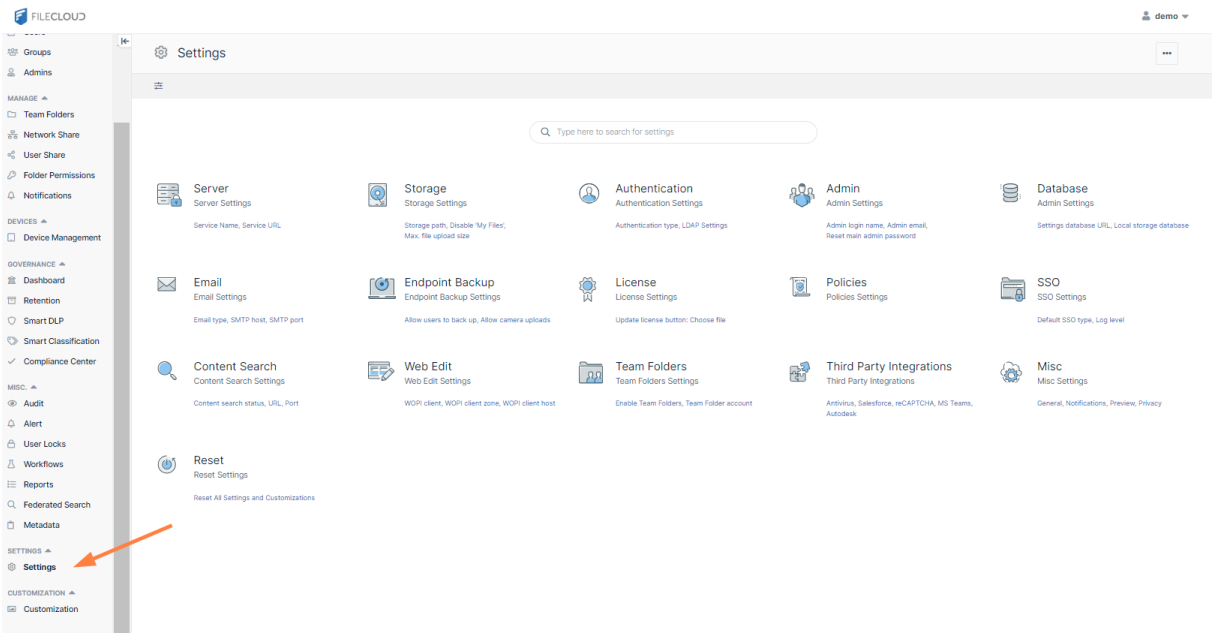
Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Advanced Features	Set Up Compliance Checking • HIPAA • ITAR • GDPR • PDPL • NIST	Set Up Data Governance		

Navigating and Searching for Settings

The Settings landing page, which includes a setting search, is available in FileCloud 23.242 and later.

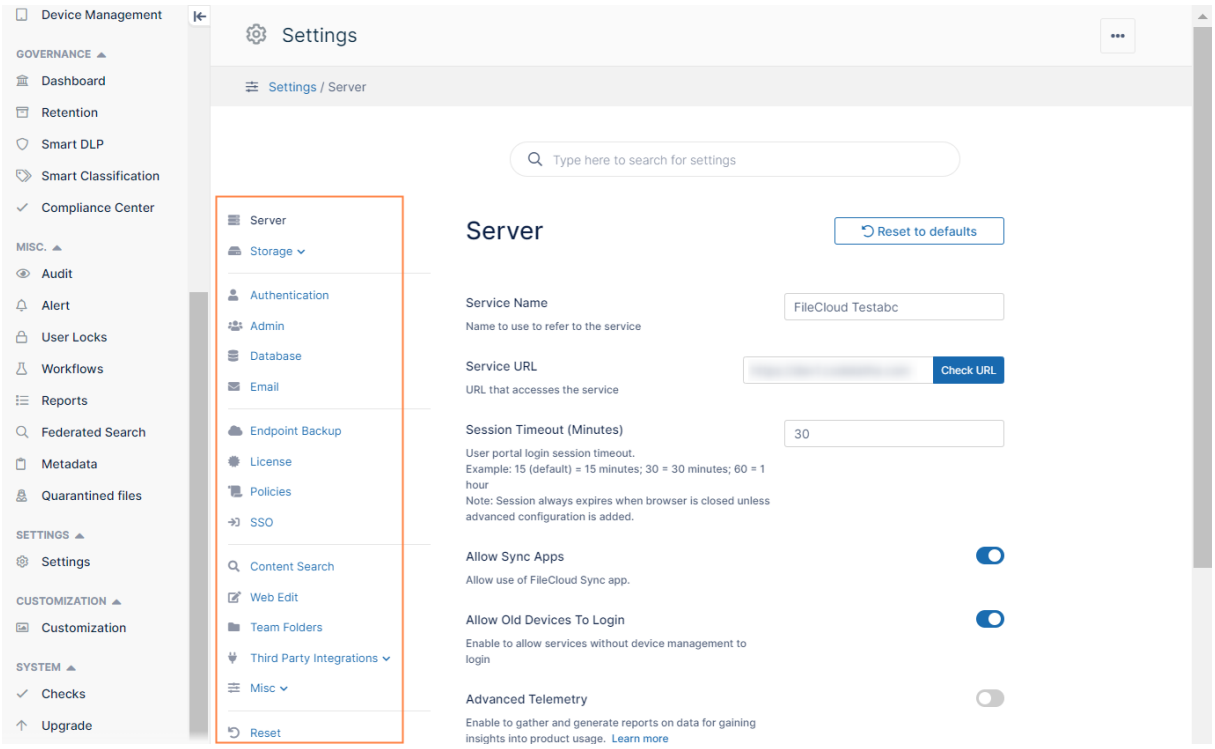
Going to the Settings landing page

To go to the **Settings** landing page in the admin portal, in the navigation panel, click **Settings**.
The **Settings** page opens as a grid of clickable icons that link to their respective settings screens.

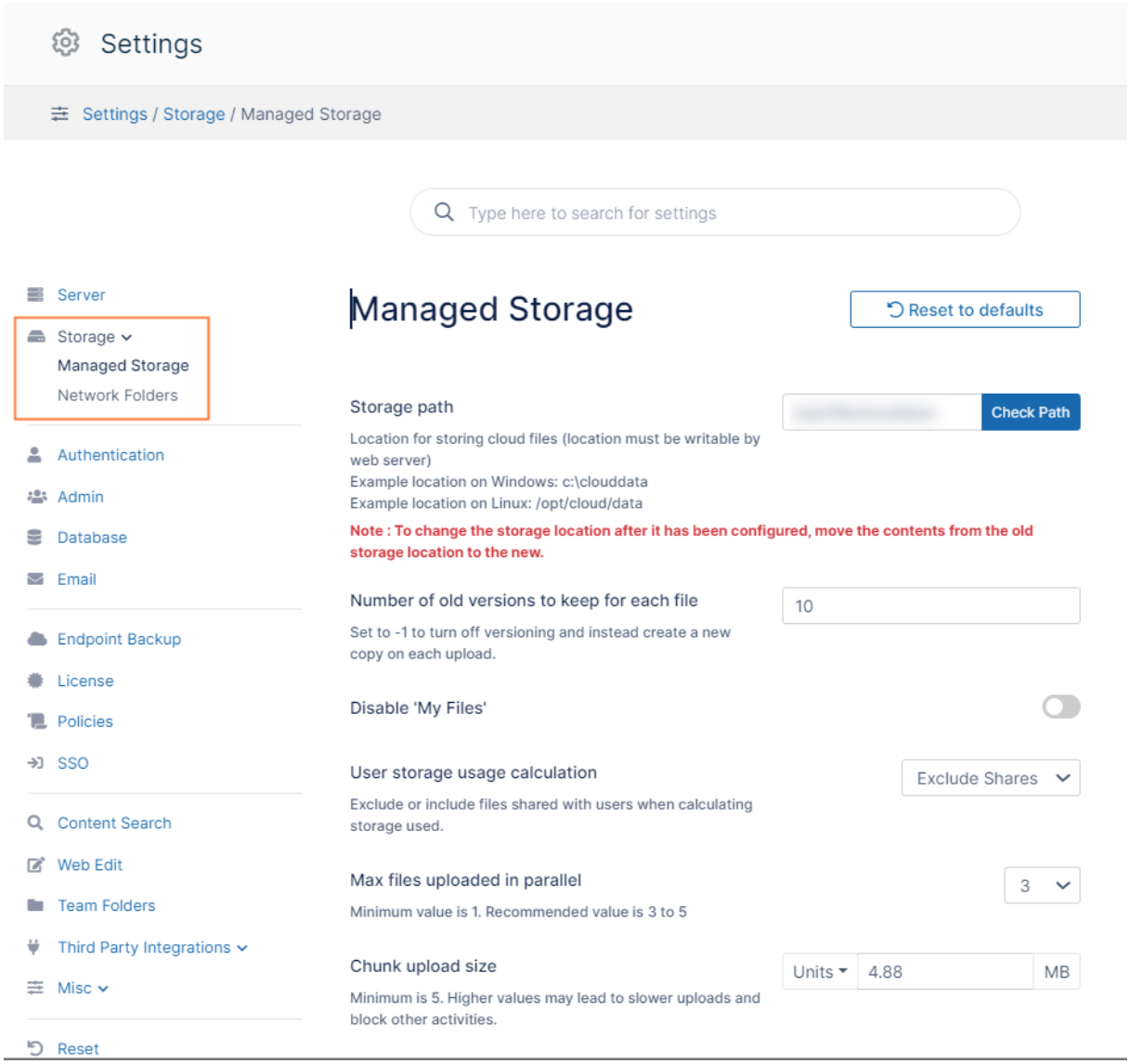


Go to a settings page

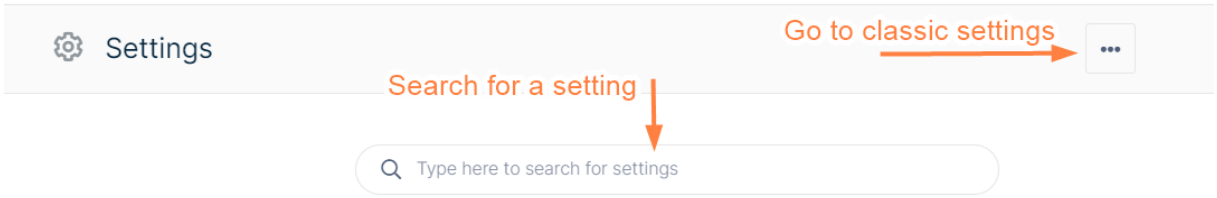
When you click a settings icon, its settings page opens. In the following image, the Server icon has been clicked and the Server settings appear. The navigation panel on the left appears on every settings page and lets you navigate to other settings pages.



If a setting has multiple pages, they appear in the navigation panel under the main setting name. When you click on the setting icon, the first setting page opens, but you can click the other sub-links to go to the setting's other pages.
For example, in the following image, the admin clicked the Storage setting icon and the first storage setting page, Managed Storage, opened. To go to the Network Folders page, the admin would click it in the left panel.



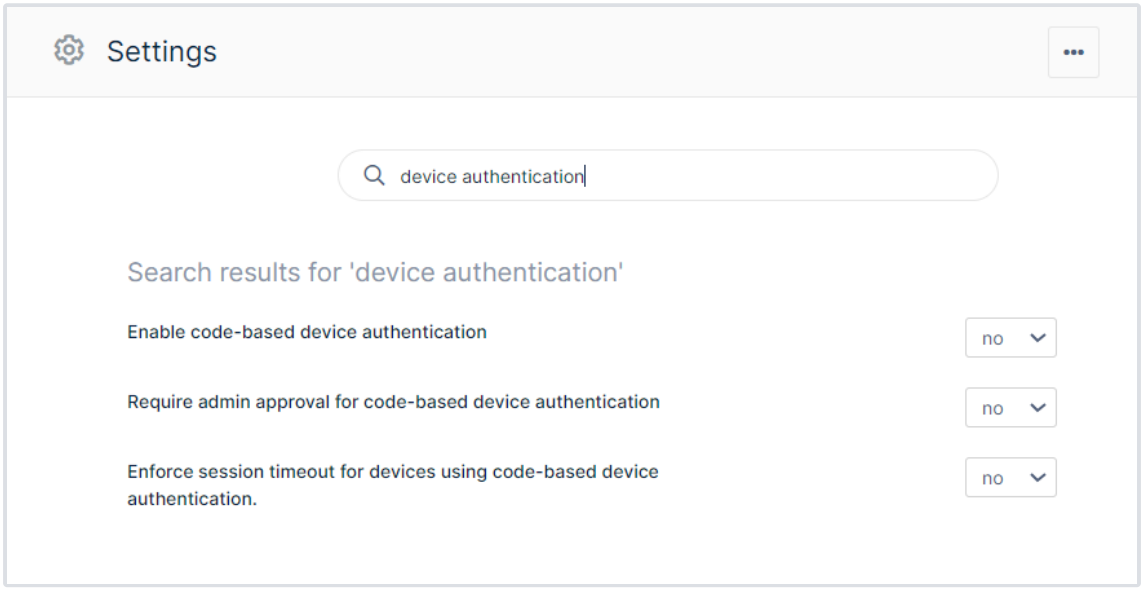
Above the settings icons, a search bar and a link to the classic settings interface appear.



Searching for settings

To search for a setting:

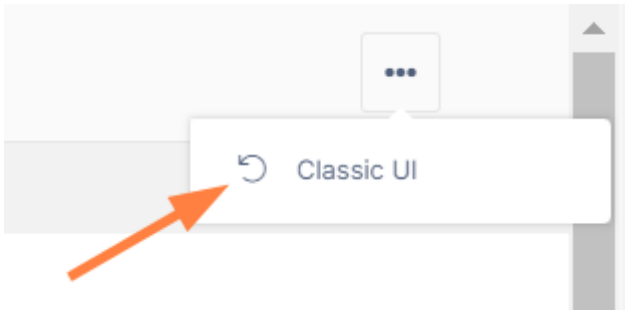
1. Enter a search term in the search bar.
   Settings with a matching name or description are returned.
   You can set the value of the setting directly from the search listing.



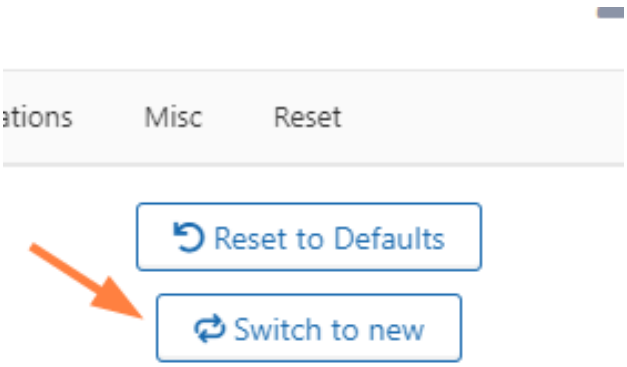
2. To return to the Settings landing page, clear the search box.

Going to classic settings

To return to the settings user interface used in versions prior to FileCloud 23.242, click the more icon in the upper-right corner of the screen and choose **Classic UI**.

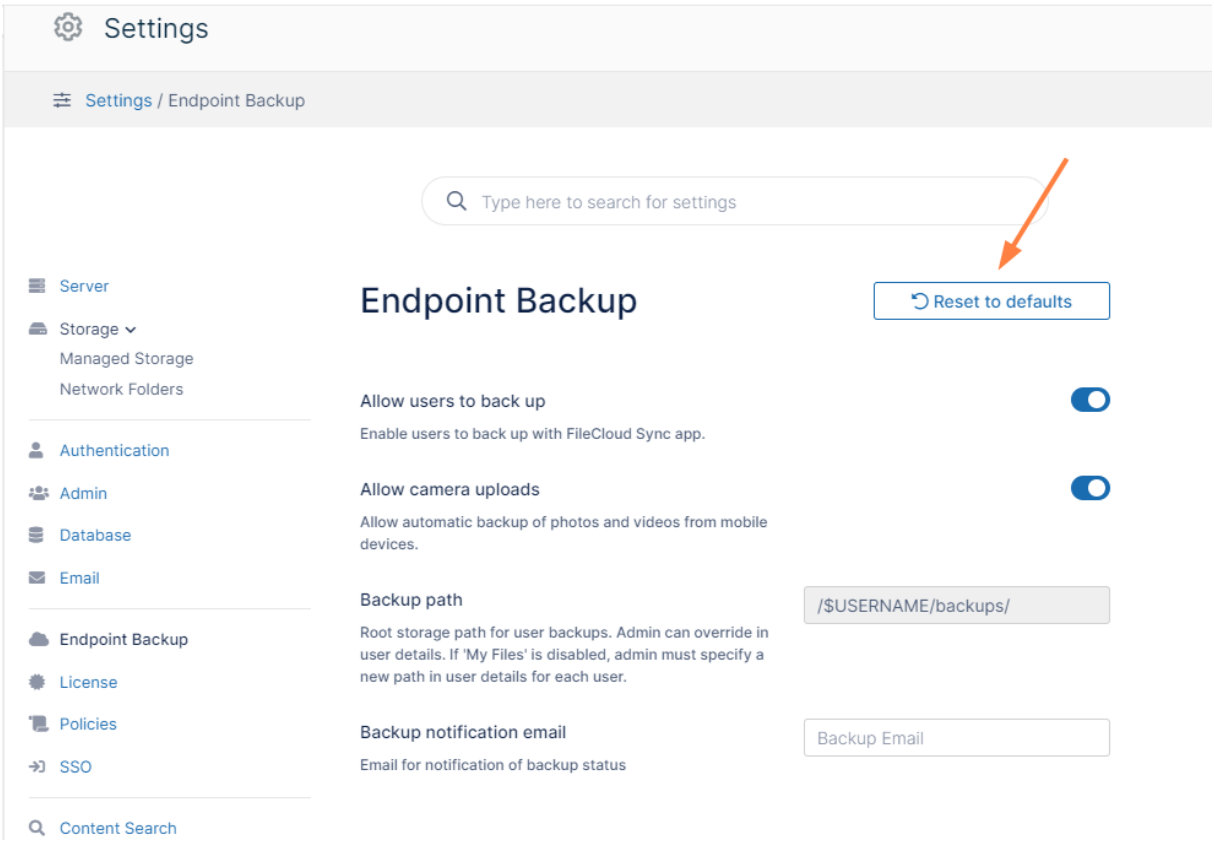


Once you are in the classic settings interface, return to the current UI by clicking **Switch to new**.

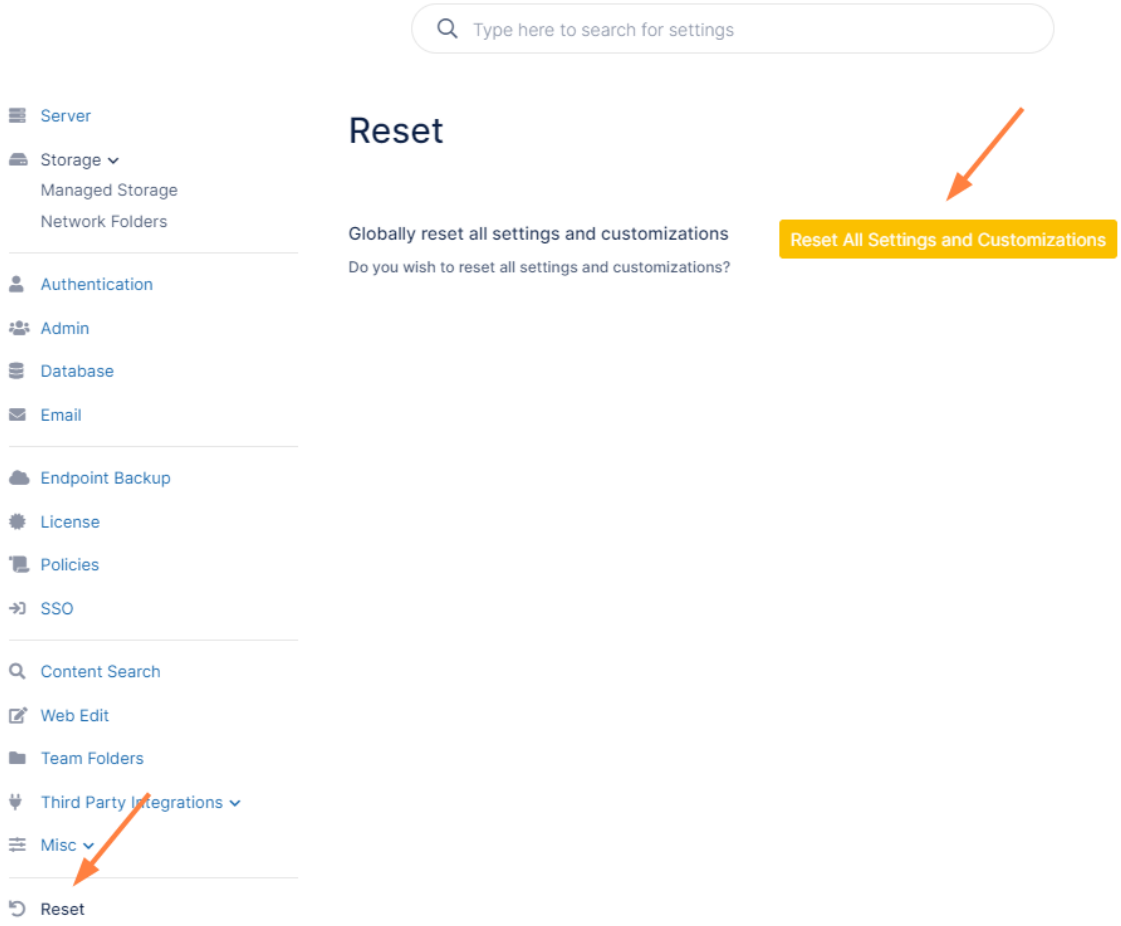


Reset settings

Some settings pages have a **Reset to defaults** button. Click **Reset to defaults** to reset the settings on that page only.



To reset all settings and customizations, click **Reset** at the bottom of the navigation panel. Then, in the Reset page, click **Reset All Settings and Customizations**.

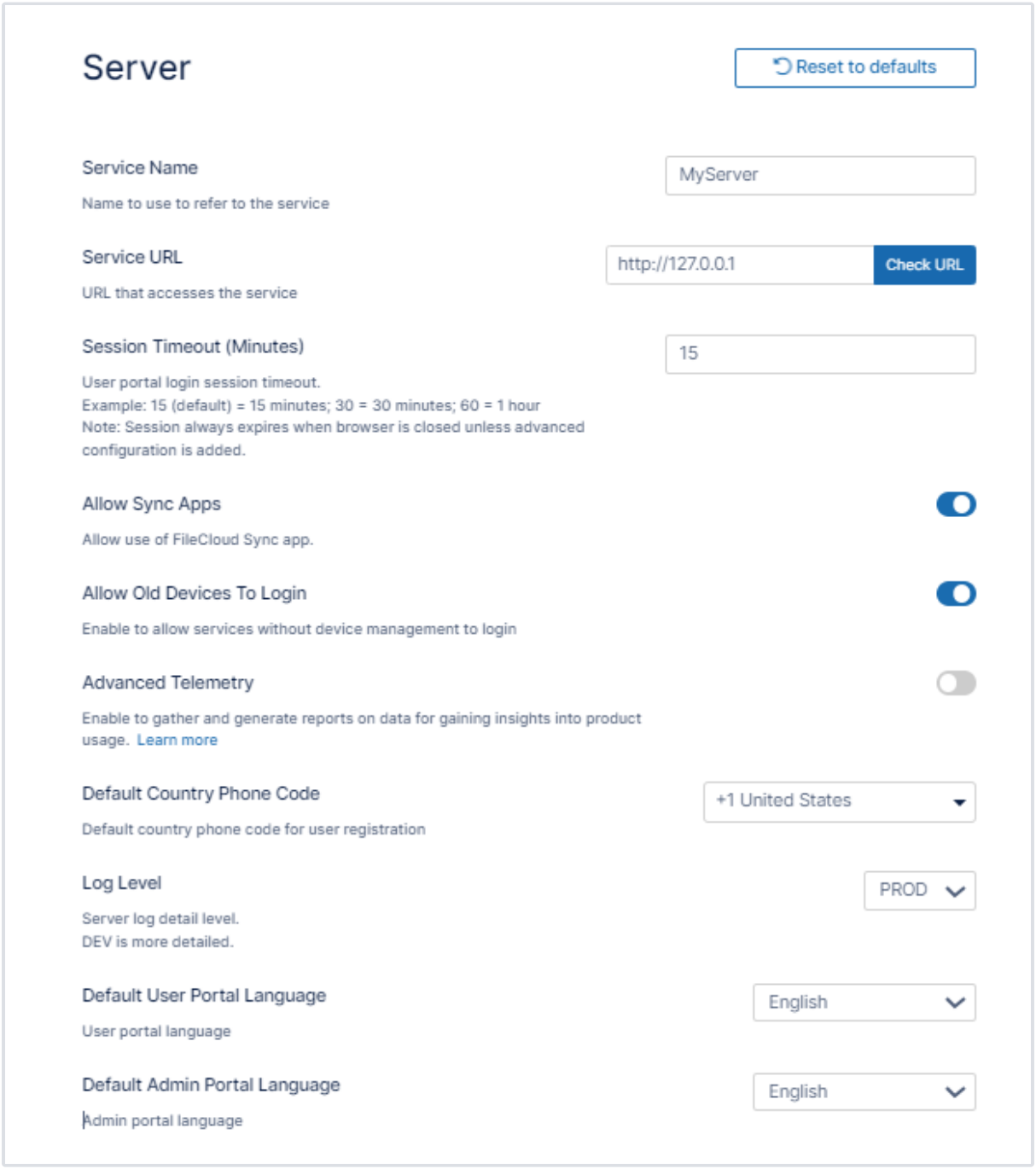


Server Settings

Server settings include the **Service Name** and **Service URL**, which you must set before using FileCloud, as well as other server-related settings such as the session timeout period and the languages of the user portal and admin portal.

To set the Server settings:

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.
2. Fill in the settings as shown in the following screenshot, using the table below as a guide.



Settings Name	Description
Service Name	The name used when referring to your FileCloud service. This is used in email messages, in the zip filename for multiple downloads, and anywhere else your service is referred to by its name.

<table>
<tr><th>Settings Name</th><th>Description</th></tr>
<tr><td>Service URL</td><td>The URL used to access your FileCloud site. Enter the protocol and domain name, for example, https://xyz.company.com, and click Check URL to confirm that it is accessible.
If you are using a custom port, also include the port number, for example, https://myfilecloud.com:3000.
Notes:
Confirm that your domain name is externally accessible via any firewall you have.
Since this URL is used for background cron job processing, if you are running a multitenant setup, make sure it is accessible from the server running FileCloud.
Use the appropriate protocol prefix (<code>https://</code> or <code>http://</code>). For production environments, use <code>https://</code> only.</td></tr>
<tr><td>Session Timeout</td><td>The number of minutes of inactivity that the browser session times out.<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>15 (default value)</td><td>Session expires after 15 minutes of inactivity (minimum session timeout)</td></tr><tr><td>60</td><td>Session expires after 1 hour of inactivity</td></tr></table>By default:
Session Timeout value is only applicable to the user portal and not to other FileCloud clients such as Sync, Drive, and FileCloud Desktop.
If the browser is closed, the session is logged out.
To apply Session Timeout to other clients or to disable session logout when the browser is closed, see User Session Expiration</td></tr>
<tr><td>Allow Sync Apps</td><td>Toggled on by default. Toggle off to block all Sync apps from connecting to this server and performing sync operations.</td></tr>
<tr><td>Allow Old Devices to Login</td><td>FileCloud supports clients that are Remote Client Management (RMC) compliant.
However, you can allow access using older FileCloud (non RMC compliant) clients by toggling on this setting.
For more information about using RMC in FileCloud, see Remote Client Management.</td></tr>
<tr><td>Advanced Telemetry</td><td>Toggle on to allow FileCloud to gather diagnostic and usage data.</td></tr>
<tr><td>Default Country Phone Code</td><td>The default country code that appears in the user portal when share creators invite users to a share and when users add/modify their phone numbers in settings.</td></tr>
</table>

Settings Name	Description
Log Level	How many activities are recorded in the system log. The default is **PROD** (production), a regular level of logging. Changing **Log Level** to **DEV** (development) generates more log entries and can have performance impact and consume additional storage. Technical Support may ask you to change this value to help troubleshoot issues.
Default User Portal Language	The language that is used when a user logs in to the user portal.
Default Admin Portal Language	The language that is used when an administrator logs in to the admin portal.

FileCloud needs a cron job to perform certain ongoing maintenance tasks.
These tasks include:

- Sending email notifications
- Sending admin summary emails
- Performing recycle bin cleanup
- Deleting expired shares
- Archiving old audit records

Set Up a Cron Job

Configure System-Generated Emails

To reset server settings:

- Click **Reset to defaults** to reset the settings on this page only.

Setting Up a Cron Job or Scheduled Task

If you are running a multitenant system with FileCloud, make sure all site URLs for each site are accessible from the local site. These are used by the task scheduler/Cron to run automated tasks for each site.
On multitenant environments with large numbers of sites, you may need to change the default timeout setting to give FileCloud time to execute the task for all of the sites. See below for information about changing the timeout setting in cron.ini.

Introduction

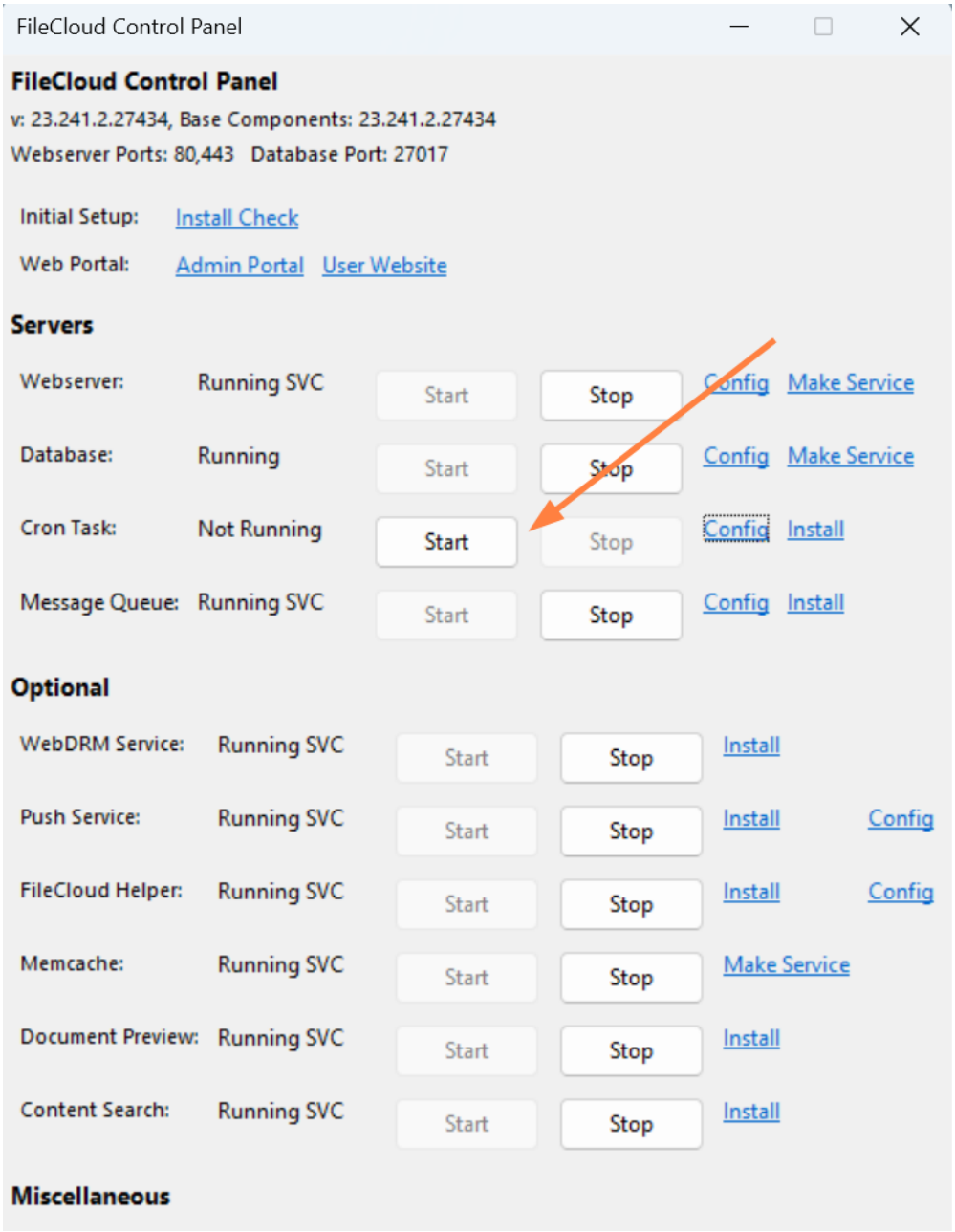
FileCloud needs a Cron job to perform certain ongoing maintenance tasks.
These tasks include:

- Sending email notifications such as file change notifications, share notifications etc.,
- Sending admin summary emails
- Performing recycle bin cleanup
- Deleting expired shares
- Archiving old audit records
- Performing periodic workflow tasks (if configured)
- Sending SPLA reports (only if there is SPLA licensing)
- Performing backup jobs (only if there is a backup server)
- Sending password expiry emails (7 days and 1 day before the expiry date)
- Sending storage quota notifications (when a specified threshold is met)

Setup Cron Job in Windows

Open the FileCloud Control Panel and click **Install** for the Cron Task.

Then click **Start** to start the Cron Task.



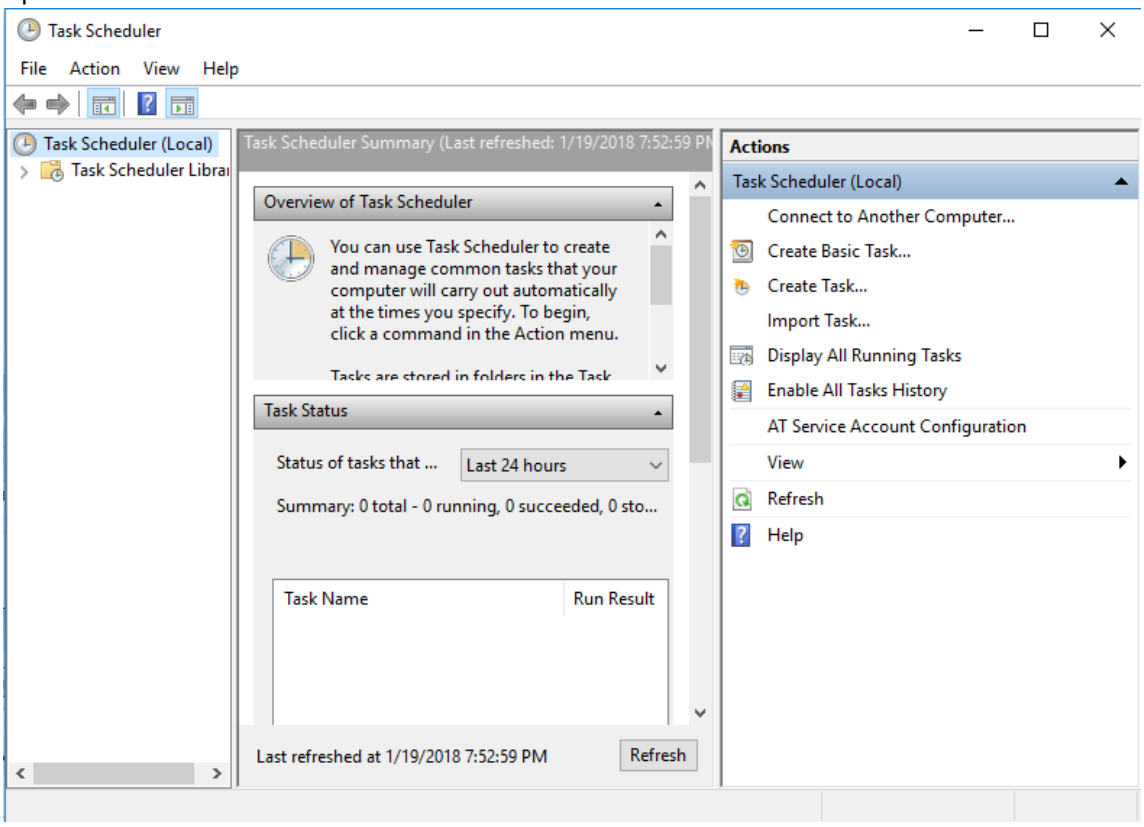
Additional Settings for the Cron Task are available by editing the xampp\cron.ini file
[settings]
frequency=300 ---> Frequency of Cron in seconds (Default is every 5 mins)
timeout=600 ---> Time to wait for Cron to complete in seconds (Default is 10 mins)

Set up a Scheduled Task in Windows (alternative to Cron Service)

1. Use Notepad or a similar program to create a new file named **fccron.vbs** in a location like c:\xampp\htdocs\resources\backup folder.
   Enter the following contents from the code block below and save the file. Additionally, in the code block below ensure that paths to php.exe and cron.php files are correct.

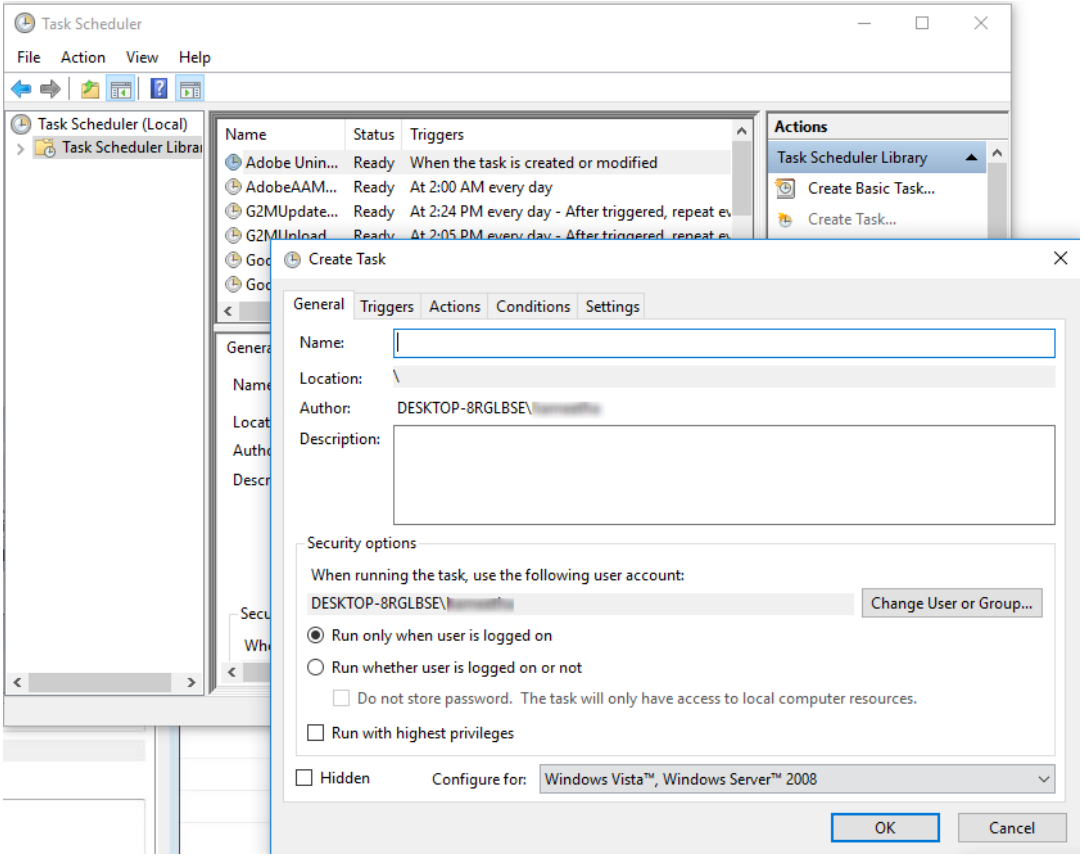
```
CreateObject("Wscript.Shell").Run "C:\xampp\php\php.exe -f ""c:
\xampp\htdocs\core\framework\cron.php"" ", 0, False
```

2. Open Task Scheduler:



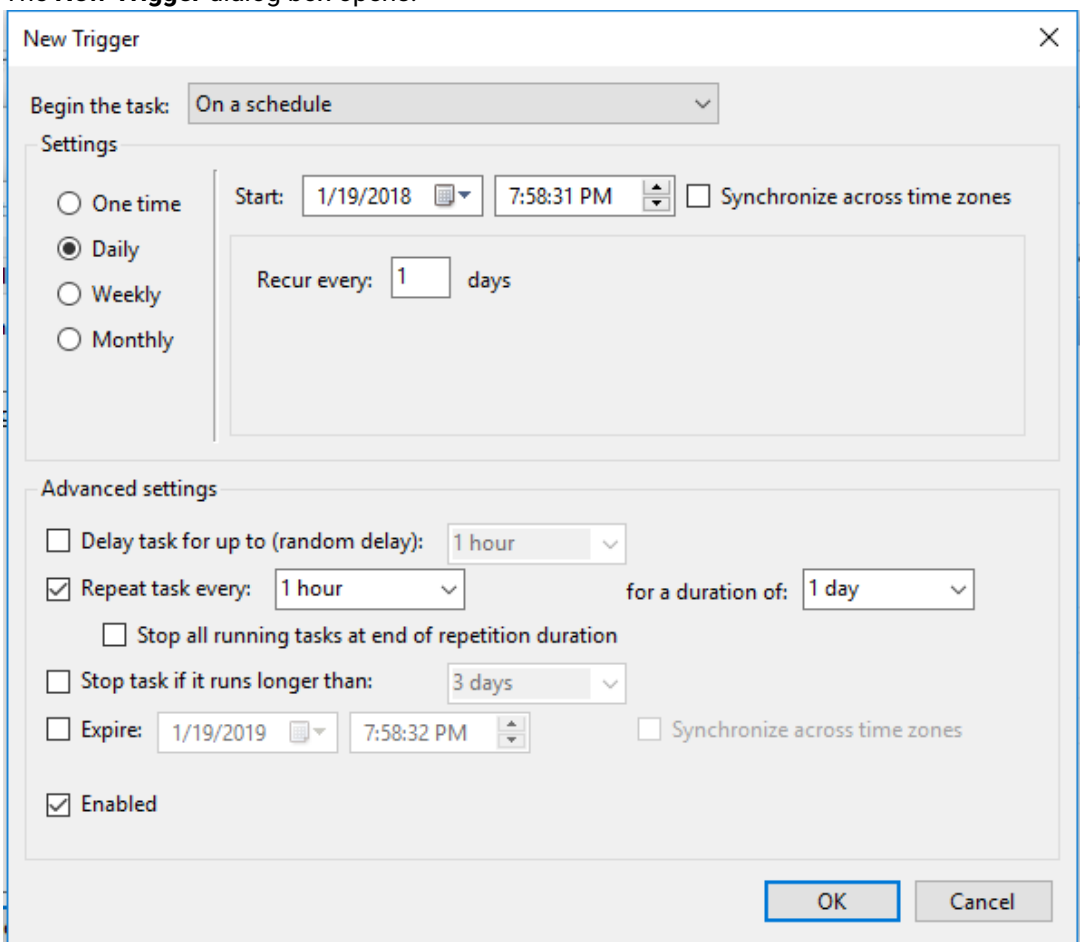
3. Click **Create Task** in the right menu under **Actions**
4. On the **General Tab**
   a. Set the **Name** to **FileCloud Notifications**.

b. Under **Security options**, select **Run whether user is logged on or not**.



5. On the **Triggers Tab:**

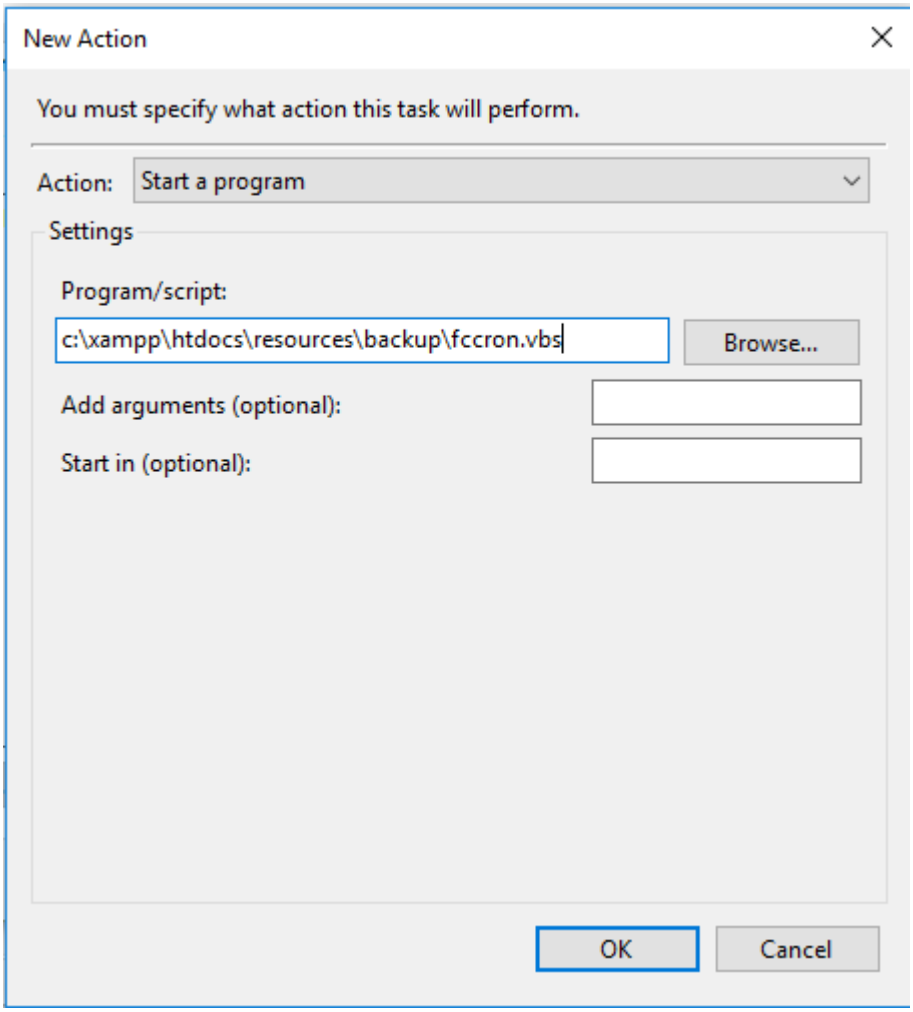
a. Click **New.**
The **New Trigger** dialog box opens.



b. Select **On a Schedule** from the **Begin the task** drop-down list.
c. In **Settings**, select **Daily**, select a **Start** time and then select **Recur every: 1 days**.
d. Under **Advanced settings**, in **Repeat task every 5 minutes** adjust the value if you want a different frequency of notifications.
e. Check **Enabled**.
f. Click **OK**.

6. On the **Actions Tab:**

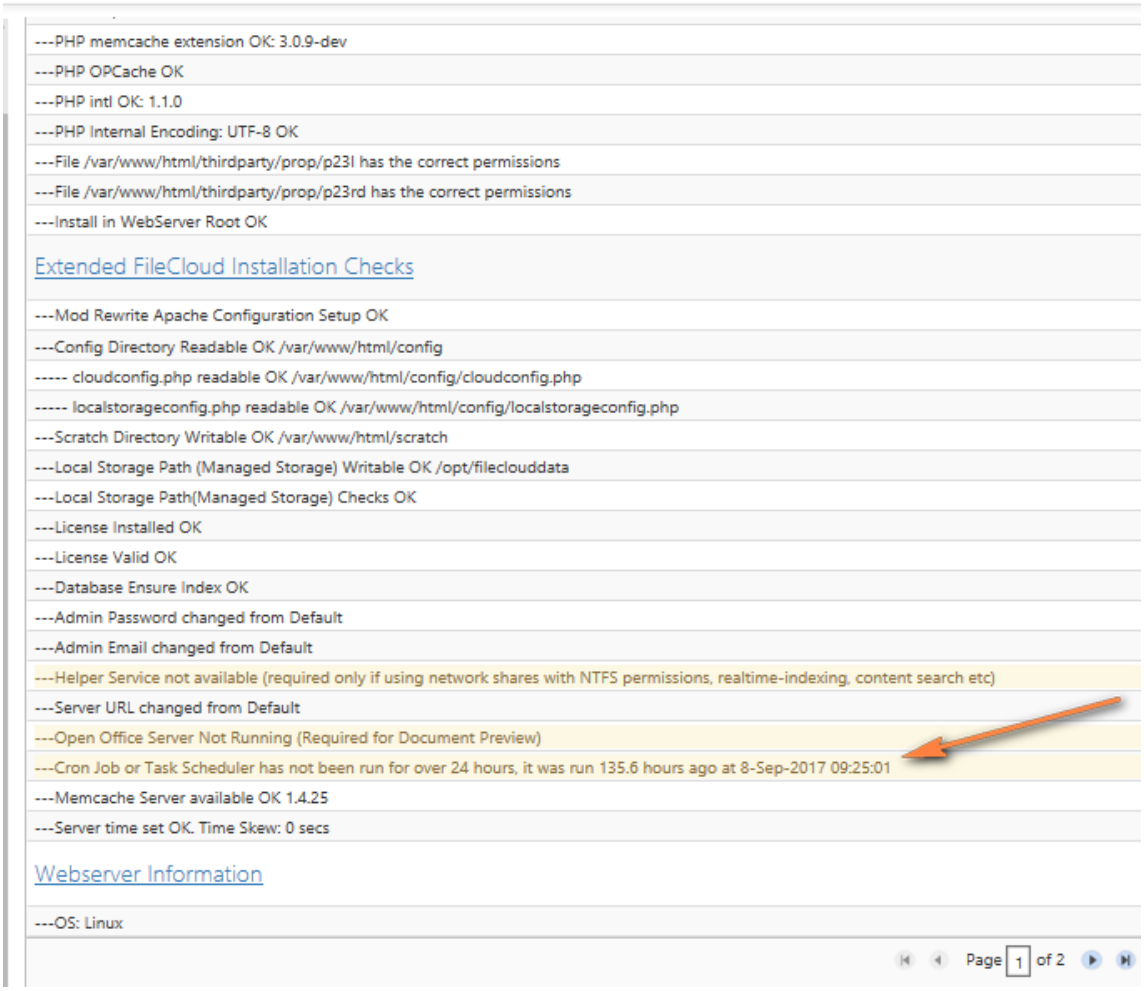
a. Click **New**.
The **New Action** dialog box opens:



b. In **Action**, choose **Start a program**.
c. In the **Program/script** text box, enter the path to the **fccron.vbs** file, (for example, c:\xampp\htdocs\resources\backup\fccron.vbs).
d. You may need to set **Start In** to **c:\xampp\htdocs\resources\backup** to resolve a problem.
e. Click **OK**.
f. All other settings can be default, unless there is a specific reason you need to change them.

Verify the Cron Job is Running

1. Go to admin portal.
2. In the navigation pane, click **Checks**.
Under **Extended FileCloud Installation Checks**, check the Cron status in the lines highlighted below.


---PHP memcache extension OK: 3.0.9-dev
---PHP OPCache OK
---PHP intl OK: 1.1.0
---PHP Internal Encoding: UTF-8 OK
---File /var/www/html/thirdparty/prop/p23l has the correct permissions
---File /var/www/html/thirdparty/prop/p23rd has the correct permissions
---Install in WebServer Root OK
Extended FileCloud Installation Checks
---Mod Rewrite Apache Configuration Setup OK
---Config Directory Readable OK /var/www/html/config
----- cloudconfig.php readable OK /var/www/html/config/cloudconfig.php
----- localstorageconfig.php readable OK /var/www/html/config/localstorageconfig.php
---Scratch Directory Writable OK /var/www/html/scratch
---Local Storage Path (Managed Storage) Writable OK /opt/fileclouddata
---Local Storage Path(Managed Storage) Checks OK
---License Installed OK
---License Valid OK
---Database Ensure Index OK
---Admin Password changed from Default
---Admin Email changed from Default
---Helper Service not available (required only if using network shares with NTFS permissions, realtime-indexing, content search etc)
---Server URL changed from Default
---Open Office Server Not Running (Required for Document Preview)
---Cron Job or Task Scheduler has not been run for over 24 hours, it was run 135.6 hours ago at 8-Sep-2017 09:25:01
---Memcache Server available OK 1.4.25
---Server time set OK. Time Skew: 0 secs
Webserver Information
---OS: Linux
Page 1 of 2

Storage Settings

FileCloud can access and manage content stored locally on your system as well as content stored on network-accessible locations.

Managed Storage is local storage that can be directly accessed and managed by FileCloud.

Network Folders are storage locations on your existing network that are not local to FileCloud but can be accessed and managed by FileCloud.

Managed Storage	Set Up Managed Storage
Network Folders	Set Up Network Folders
Protecting Your Storage	Enable Antivirus Scanning Set Up Encryption for Managed Storage Create an IAM User Policy for S3 Access

FileCloud Managed Storage

Data that is stored locally in FileCloud is called **Managed Storage.**

- Managed Storage is the location where the user files are stored locally and can be accessed directly by FileCloud.
- When you specify the path to managed storage, you give FileCloud control over the management of the user content located there.
- Managed Storage can be a file system, a local hard disk, a Storage Area Network (SAN), or a Network Attached Storage (NAS) disk.

Can I also configure network storage?

Administrators can also configure how users store data on your existing Network infrastructure.

Setting Up Network Folders

Managed storage setup must be done BEFORE users are created.
If users are already created and Managed Storage type or location is changed, then the existing users will no longer be able to access or store data, and their accounts will have to be deleted and recreated.

Setting up Managed Storage

Administrators can configure how users store data on the FileCloud Server site in Managed Storage.

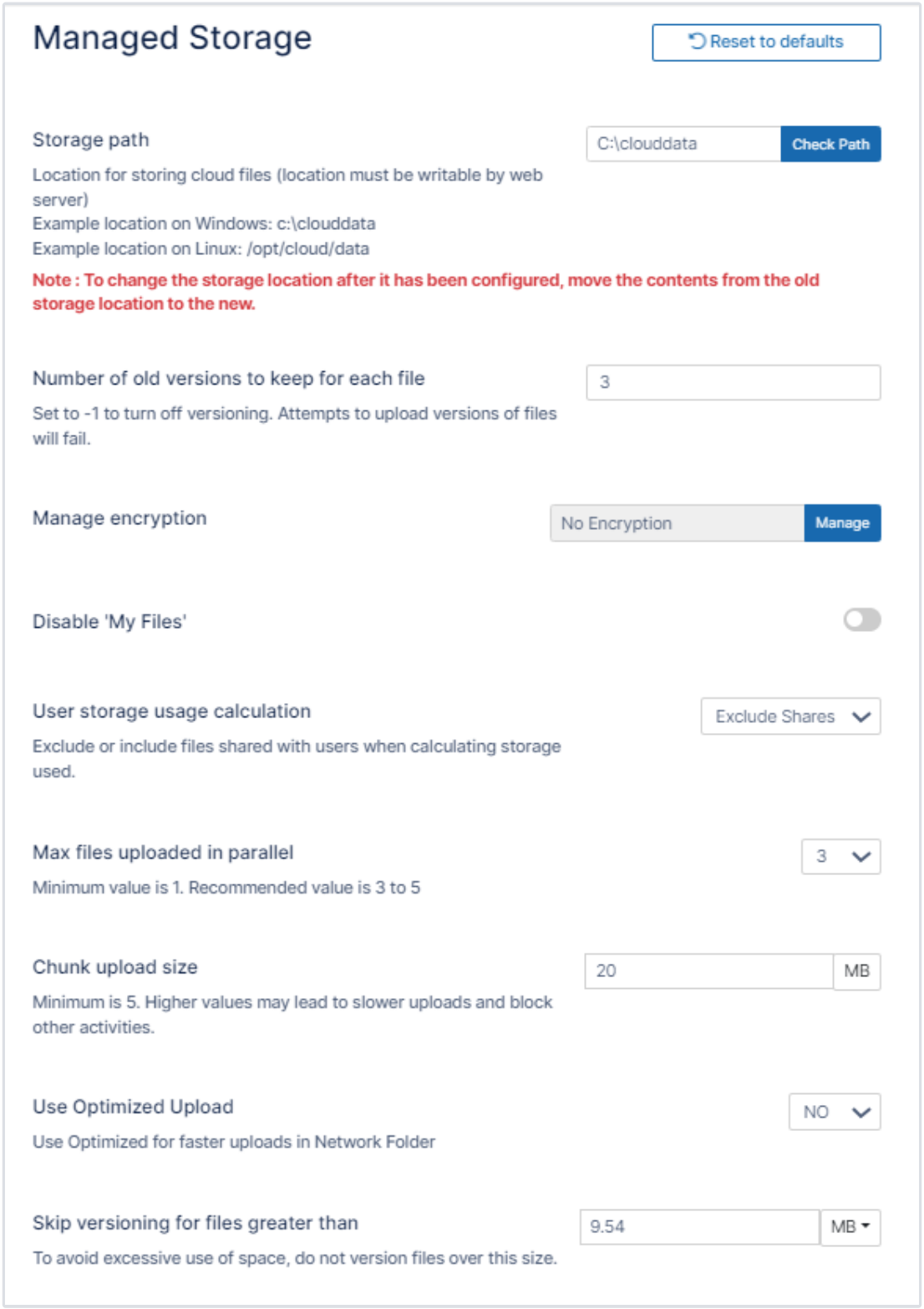
This is the default cloud storage, where the FileCloud server has direct access to the user files stored on the filesystem.

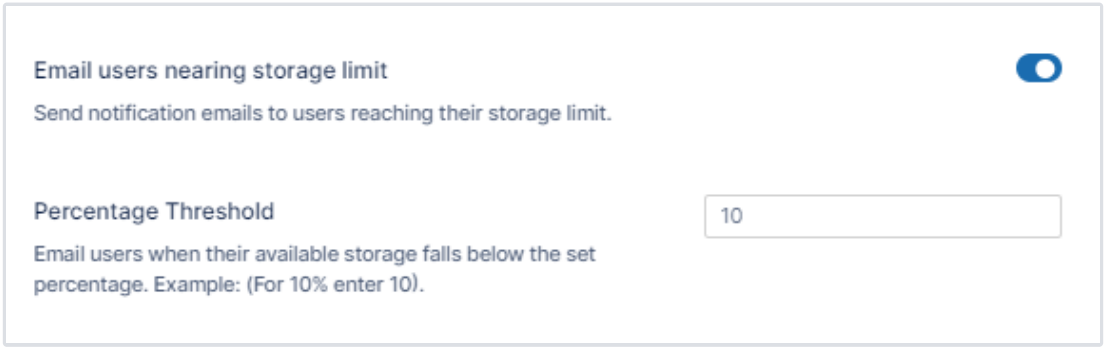
- Managed Storage provides FileCloud control over the management of user content.
- The storage can be on filesystems on a local hard disk, SAN, or NAS disks.

You can configure general storage settings in **Settings > Storage > Managed Storage** and more specific storage settings in **Settings > Policies. Policies** settings include user storage quota and rules for deleted files. You can assign different storage values in multiple policies and assign them to different users.

To set up Managed Storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage settings** page opens by default.
2. Type the information into the fields as described below.

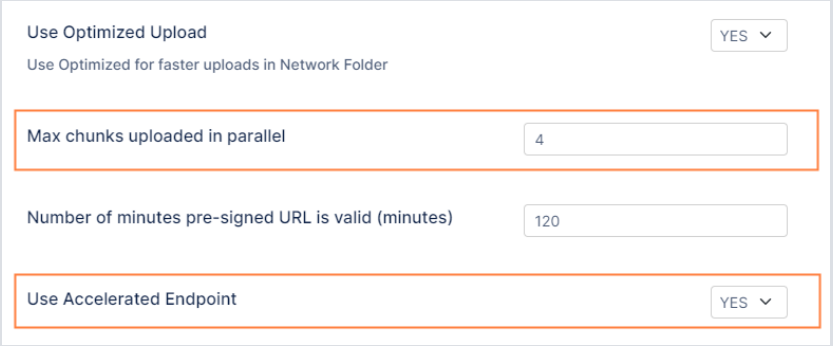

Managed Storage
Reset to defaults
Storage path
C:\clouddata
Check Path
Location for storing cloud files (location must be writable by web server)
Example location on Windows: c:\clouddata
Example location on Linux: /opt/cloud/data
Note : To change the storage location after it has been configured, move the contents from the old storage location to the new.
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
Manage encryption
No Encryption
Manage
Disable 'My Files'
User storage usage calculation
Exclude Shares
Exclude or include files shared with users when calculating storage used.
Max files uploaded in parallel
3
Minimum value is 1. Recommended value is 3 to 5
Chunk upload size
20
MB
Minimum is 5. Higher values may lead to slower uploads and block other activities.
Use Optimized Upload
NO
Use Optimized for faster uploads in Network Folder
Skip versioning for files greater than
9.54
MB
To avoid excessive use of space, do not version files over this size.



Setting	Description
Storage path	This is the location where all FileCloud user files are stored. Be sure to allow enough capacity for future storage expansion. **Note: Changing this Storage Path after installation and after users have uploaded files has to be done carefully. If it is not done properly, it could result in data loss.**
Number of old versions to keep for each file	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines the number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to -1. **NOTE**: Versioned files count towards the user's storage quota.
Manage Encryption	Appears when encryption is enabled in your system, and allows you to manage encryption. See Enabling Storage Encryption.
Disable 'My Files'	If you are only using the "Network Folders" features of FileCloud and don't want to show "My Files", you can enable this checkbox. If there are existing data in the "My Files" section, the data will no longer be accessible. Certain functions that depend on My Files will no longer be available.
User storage usage calculation	When the user storage usage is reported, the shares used by the user can also be counted towards the quota. This can be changed by selecting the appropriate drop-down option.
Max files uploaded in parallel	Number of files that can be uploaded at the same time when multiple files are uploaded. Default is 3. The recommended number is 3 to 5. Higher values may slow down the upload process and lower system efficiency.
Chunk upload size	The maximum size in MB for chunks uploaded. Default is 20. If size is set too high, the upload process may slow down and other operations may be blocked.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Use Optimized Upload</td><td>
Optimized upload uses a faster method for uploading.
Choose YES to use optimized upload for S3 Network Folders only. If you don't use Network Folders or your Network Folders do not use S3 storage, this setting does not have any effect.

If you choose YES, the additional fields Max chunks uploaded in parallel and Use Accelerated Endpoint appear:



Use the following information to determine the values you want to give these fields:

<table>
<tr><td>Max chunks uploaded in parallel</td><td>The number of file chunks that can be sent simultaneously to the server. Choose the highest number of chunks you can send without having a detrimental effect on efficiency. The default value is 10, and the minimum value is 1. Mid-range values are 4 - 20. Values above 20 may decrease efficiency by blocking other activities and slowing down uploads.</td></tr>
<tr><td>Use Accelerated Endpoint</td><td>If you have the accelerated feature in the S3 bucket enabled, set to YES to use the feature to complete downloads and uploads more quickly.</td></tr>
</table>

If you enter YES to use optimized storage, you must also configure a Cross Origin Resource Sharing (CORS) policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings. To configure the CORS policy, see Setting up FileCloud Managed S3 Storage, Integrate Amazon S3 Storage, Step 2.

Note: If you are using Network Folders with S3 storage, if you use server-side encryption with a customer key (SSE-C), optimized upload will fail due to security reasons.
</td></tr>
</table>

Setting	Description
Number of minutes pre-signed URL is valid (minutes)	How long the pre-signed URL can be used. Choose a value that is high enough to enable uploads and downloads on large files, and low enough to close the url in a timely manner so it is not a security risk. The recommended value is 30 to 60.
Skip versioning for files greater than	Any file larger than the specified value will not be versioned.
Email users nearing storage limit	If this option is enabled then automatic emails with notifications will be sent to users reaching their storage limit.
Percentage Threshold	Defines at what point the percentage of unused managed storage space is considered low. For example, if the value is set to 20, then storage is considered low if more than 80% of managed storage space is used. When unused storage is less than this value, an automatic email notification is sent to the admin. If the above option, **Email Users Nearing Storage Limit** is enabled, an automatic email notification is also sent to the user if their available storage falls below the set percentage.

3. Click **Save**.
4. Click the **Policies** tab.
5. For each policy that you want to change the default storage settings in:
   a. Click the edit button.
   b. Remain on the **General** tab.
   c. Type the information into the fields as described below:
   d. Click **Save**.
   e. Assign the policy containing the appropriate storage settings to each user.

Setting	Description
User storage quota	This is the storage quota that is provided for every user of FileCloud. Note that this is only a quota and does not require physical storage until the user actually consumes the space. Setting this to 0 means each user has no storage quota limit. Changing this setting does not affect the existing user quota. *For example, if a user has 2 GB quota and if this setting is changed to 10 GB, it only affects newly created users after this point. To update the quota for an existing user, use the User Details panel in Users section.*
Store deleted files in the recycle bin	Enable this setting if you wish to provide a way to keep deleted files in a Recycle Bin. When this option is enabled and a user deletes a file/folder, the deleted item gets moved into their personal deleted files area. Then the user can restore files from their recycle bin or empty the recycle bin completely. **Note: Files in the recycle bin count towards a user's storage quota.**

Setting	Description
Automatically delete files from recycle bin after set number days	Number of days after which Deleted Files is emptied automatically. Note that this recycle bin clearing happens at periodic intervals specified here and any files in any recycle bin are cleared. The default is 0 which means that the deleted files are not cleared automatically. Requires a Cron Job to be set up.
Do not store deleted files greater than	Any file larger than this setting is permanently deleted instead of getting moved into Deleted Files area.

Warning
Do not change the *Storage Path* once the installation is set up and data is stored.
This should only be set for fresh installs.
Be very careful when changing the storage path. If done improperly, it could lead to data loss.

The new S3 optimization feature introduced in FileCloud 23.241 is more efficient than the legacy method, below. The legacy method applies to both local and S3 uploads, but does not work for S3 uploads when **Use Optimized Upload** is set to **YES** (to enable the new feature).

Legacy method of upload optimization
If you upload large numbers of small files from the Web browser interface, to improve upload performance:

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

```
define("TONIDOCLOUD_UPLOAD_OPTIMIZATION", 0);
```

Setting up FileCloud Managed S3 Storage

Optimized file upload is available for managed S3 storage beginning in FileCloud 23.241. The settings added for optimized uploads are noted in the table in Step 3, below.

As an administrator, you can configure FileCloud Server to store user data in Amazon S3.

- **Amazon Simple Storage Service (Amazon S3) is a scalable object storage service.**
- **You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.**
- **You can manage Amazon S3 by using the AWS Management Console.**

Getting Started with Amazon Simple Storage Service

WARNINGS:

- Only change the FileCloud storage type to S3 for new installations.
- Do not change the FileCloud storage type to S3 if FileCloud has been in use and data is already stored.
- **Be careful when changing the storage path. If you change it incorrectly, it can result in data loss.**
- When changing the storage type from local to Amazon S3, the files and folders that have already been saved to local storage are not moved automatically to S3 storage.
  - For existing files and folders, the administrator must manually export them from local storage before changing the storage type.
  - After changing the storage type to S3, the administrator must manually import pre-existing files and folders.
- If the **S3 Bucket Name**, **S3 Secret** or **S3 Key** is changed after initial S3 configuration, restart the Cron service and the fcorchestrator (message queue) service.
- Never modify the S3 bucket outside the FileCloud subsystem.
- Do not add, edit, or modify files directly by using S3 tools. Doing so will destabilize your FileCloud installation.

Integrate Amazon S3 Storage

1. Change the Storage Type to S3

In this step you will need to access **WWWROOT. It is typically located at:**

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To use Amazon S3 as the backend storage:

1. Ensure that the server time is synchronized.

a. Configure an authoritative time server in Windows Server
b. Synchronize Time with NTP in Linux

2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to this line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

```
WWWROOT/config/amazons3storageconfig.php
```

Nothing needs to be added or edited in amazons3storageconfig.php

2. (Optional) Configure System to Use Optimized Upload

When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud includes an Optimized Upload feature. You can enable Optimized Upload by configuring a CORS policy with the required settings and confirming that your service address is in the .**htaccess** file.

Note: Although Use Optimized Upload and its associated settings appear in the Managed Storage settings page, they also apply to S3 Network Folders.

Required CORS policy for Optimized Upload

To use the Optimized Upload feature, configure a CORS policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings.

For more information about CORS, see:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/enabling-cors-examples.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/ManageCorsUsing.html

To configure the CORS policy:

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Bucket name list, choose the name of the bucket that you want to create a bucket policy for.
3. Choose Permissions, and then choose CORS configuration.
4. In the CORS configuration editor text box, type or copy and paste the following CORS configuration:

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "https://my-fc-instance.com"
        ],
        "ExposeHeaders": [
            "ETag"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

5. Click **Save**.

To confirm that the service address is configured in the .htaccess file:

1. Open the .**htaccess** file.
   Windows: C:\xampp\htdocs\.htaccess
   Linux: /var/www/.htaccess
2. Check if the following line exists, and if it does not, add it:
   If you use an external compatible S3 service, add the address to the service instead.

```
connect-src 'self' *.amazonaws.com
```

3. Restart the FileCloud server.

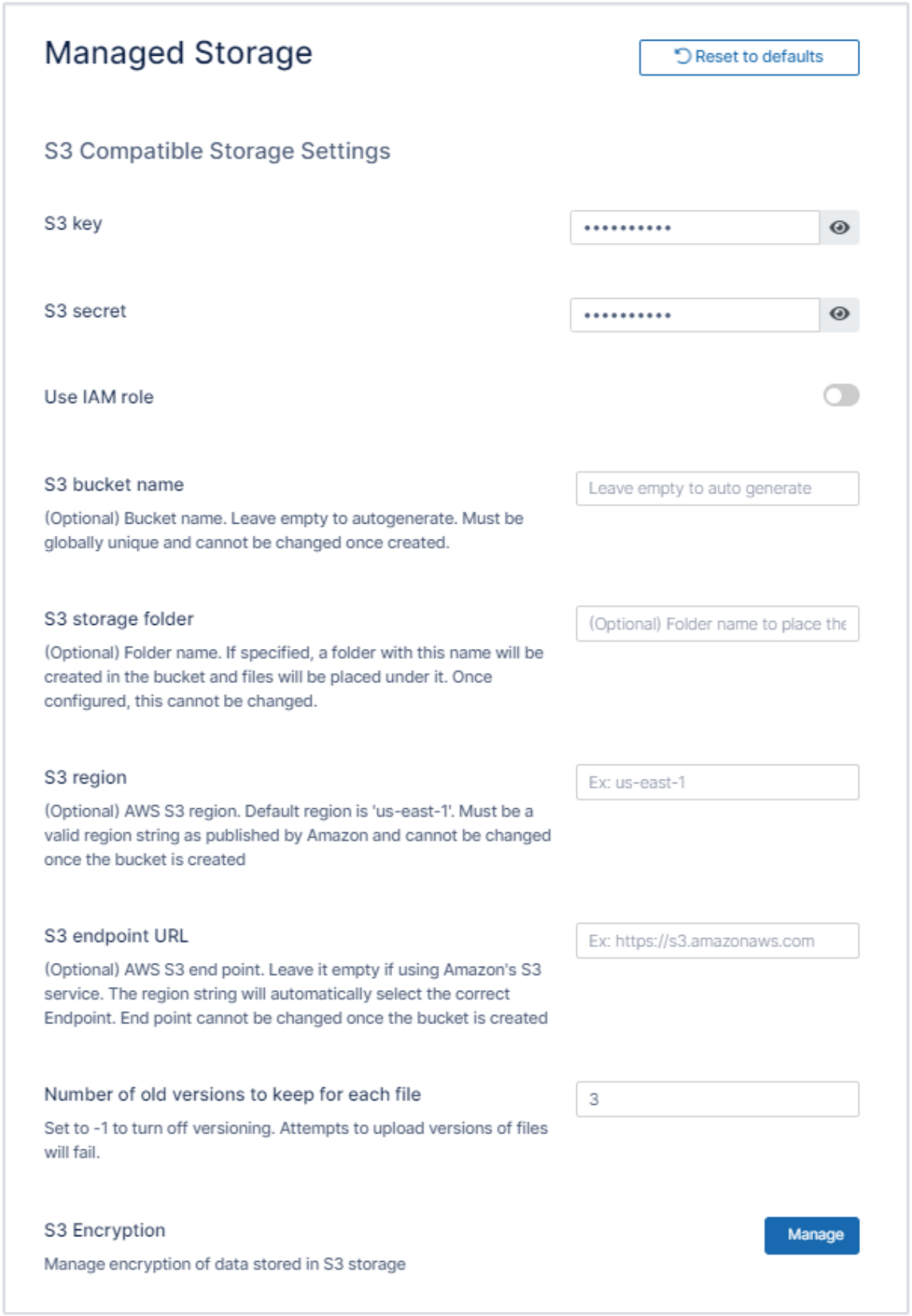
In Step 3, below, set **Use Optimized Upload** to **Yes,** and customize any of the settings that affect upload efficiency.

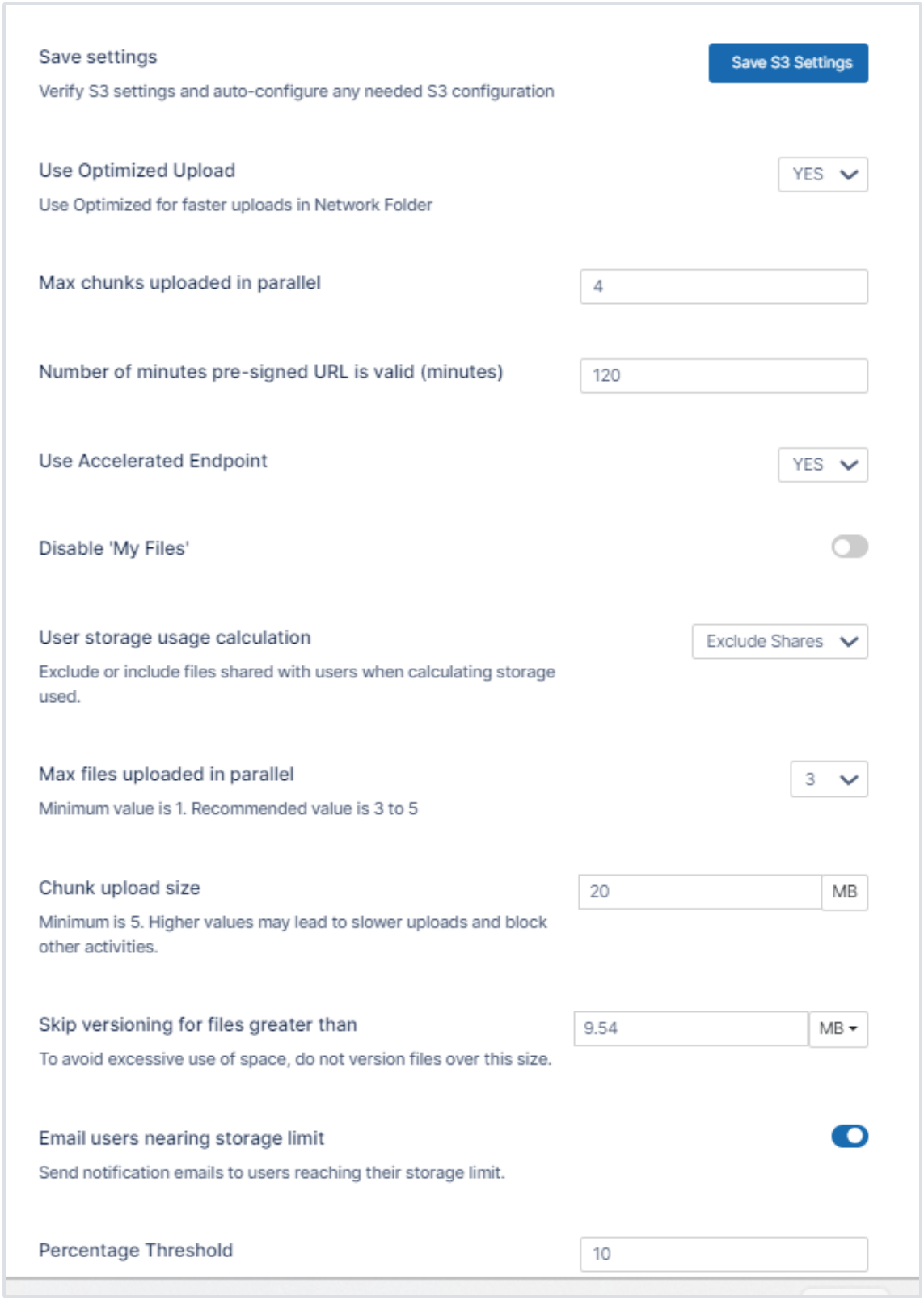
3. Configure Credentials and Settings

Now configure your S3 credentials and storage settings.

To configure S3 storage credentials and settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the S3 settings for your environment (the settings that appear above the **Save S3 Settings** button).
   Definitions of the settings appear in the table below.
3. Click **Save S3 Settings**.
4. Enter values for the settings below it or leave the default settings.
   Definitions of the settings appear in the table below.
5. Click **Save.**


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
Leave empty to auto generate
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
(Optional) Folder name to place the
S3 region
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
Ex: us-east-1
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Ex: https://s3.amazonaws.com
Number of old versions to keep for each file
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
3
S3 Encryption
Manage encryption of data stored in S3 storage
Manage


Save settings
Verify S3 settings and auto-configure any needed S3 configuration
Save S3 Settings
Use Optimized Upload
Use Optimized for faster uploads in Network Folder
YES
Max chunks uploaded in parallel
4
Number of minutes pre-signed URL is valid (minutes)
120
Use Accelerated Endpoint
YES
Disable 'My Files'
User storage usage calculation
Exclude or include files shared with users when calculating storage used.
Exclude Shares
Max files uploaded in parallel
Minimum value is 1. Recommended value is 3 to 5
3
Chunk upload size
Minimum is 5. Higher values may lead to slower uploads and block other activities.
20
MB
Skip versioning for files greater than
To avoid excessive use of space, do not version files over this size.
9.54
MB
Email users nearing storage limit
Send notification emails to users reaching their storage limit.
Percentage Threshold
10

Field	Description	FileCloud Version
S3 key	This is your Amazon access key ID (To get this value, visit Amazon security portal) . For an IAM user, it requires at least the following permissions.	
S3 secret	This is your Amazon secret access key (To get this value, visit Amazon security portal). For an IAM user, it requires at least the following permissions .	
Use IAM role	Either check **Use IAM role** or type in authentication credentials in **S3 Key** and **S3 Secret**. **Note**: To use an IAM role, you must attach it to your EC2 instance. See the page Attach an IAM role to an instance in the AWS documentation for instructions.	
S3 bucket name	Enter the bucket name. Use a new bucket whenever possible. Previously used buckets may be used in certain circumstances. It is very important that the S3 bucket is never modified outside of the FileCloud subsystem.	
S3 storage folder	Optional: All files will be stored inside this root storage folder. • FileCloud creates this folder automatically.	
S3 region	Optional: Provide the region string. If you leave this field blank, FileCloud uses the US Standard region. • If your bucket is in a different region, (Europe, Asia) provide the correct region string. The strings should match the region string published by Amazon. • **Note: For govcloud installs, you must use region string: us-gov-west-1**	
S3 endpoint URL	Optional: Specify the S3 endpoint. Use this option: • to specify your own S3 endpoint (typically S3 compatible storage) • if the region is not yet published. To use an AWS end point, it must be one of the values published AWS S3 endpoints	
Number of old versions to keep for each file	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines the number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to -1. **NOTE**: Versioned files count towards the user's storage quota.	
S3 Encryption	Allows you to manage encryption.	

Field	Description	FileCloud Version
Save settings	Click this button after you have entered the S3 settings above it to validate them and configure any automated values.	
Use Optimized Upload	Optimized upload uses a faster method for uploading files to S3 storage. Default is **No**. If you choose **Yes**, the **Max chunks uploaded in parallel** and **Use Accelerated Endpoint** fields appear. If you enter **Yes** to use optimized storage, you must also configure a Cross Origin Resource Sharing (CORS) policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings. To configure the CORS policy, see Step 2, above. **Note**: If you use server-side encryption with a customer key (SSE-C), optimized upload will fail due to security reasons.	23.241
Max chunks uploaded in parallel	Only appears if **Use Optimized Upload** is set to **Yes**. The number of file chunks that can be sent simultaneously to the server. Choose the highest number of chunks you can send without having a detrimental effect on efficiency. The default value is 10, and the minimum value is 1. Mid-range values are 4 - 20. Values above 20 may decrease efficiency by blocking other activities and slowing down uploads.	23.241
Number of minutes pre-signed URL is valid (minutes)	How long the pre-signed URL can be used. Choose a value that is high enough to enable uploads and downloads on large files, and low enough to close the url in a timely manner so it is not a security risk. The recommended value is 30 to 60.	23.241
Use Accelerated Endpoint	Only appears if **Use Optimized Upload** is set to **Yes**. If you have the accelerated feature in the S3 bucket enabled, check this setting to use the feature to complete downloads and uploads more quickly.	23.241
Disable 'My Files'	If you are only using the "Network Folders" features of FileCloud and don't want to show "My Files", you can enable this checkbox. If there are existing data in "My Files" section, the data will no longer be accessible. Certain functions that depend on My Files will no longer be available.	
User storage usage calculation	When the user storage usage is reported, the shares used by the user can also be counted towards the quota. This can be changed by selecting the appropriate drop-down option.	
Max files uploaded in parallel	Number of files that can be uploaded at the same time when multiple files are uploaded. Default is 3. The recommended number is 3 to 5. Higher values may slow down the upload process and lower system efficiency.	23.241

Field	Description	FileCloud Version
Chunk upload size	The maximum size in MB for chunks uploaded. Default is 40. If size is set too high, the upload process may slow down and other operations may be blocked.	23.241
Skip versioning for files greater than	Any file larger than the specified value will not be versioned.	
Email users nearing storage limit	If this option is enabled then automatic emails with notifications are sent to users reaching their storage limit.	
Percentage Threshold	Defines at what point the percentage of unused managed storage space is considered low. For example, if the value is set to 20, then storage is considered low if more than 80% of managed storage space is used. When unused storage is less than this value, an automatic email notification is sent to the admin. If the above option, **Email Users Nearing Storage Limit** is enabled, an automatic email notification is also sent to the user if their available storage falls below the set percentage.	

4. Enable Encryption

To protect data at rest in FileCloud Server, you can use S3 Managed Storage Encryption.

- The communication from FileCloud to AWS will use SSL encryption resulting in complete protection for data in transit.
- Once encryption is set up correctly, the field **S3 Encryption** appears.

FileCloud supports the following server side encryption types:

Encryption Type	Notes
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)	All data is encrypted at rest using AES256 bit encryption. The data can only be accessed using the supplied key/secret credentials. The data will be accessible via S3 Console (which should NOT done for FileCloud Managed storage data)
Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)	Similar to SSE-S3 but the key itself is managed using Amazon's KMS service. This allows management of specific keys and their permissions for encrypting the data. The data is still encrypted at rest and is accessible via S3 Console with appropriate credentials.

Encryption Type	Notes
Server-Side Encryption with Customer-Provided Keys (SSE-C)	The data is encrypted using the customer supplied 32 bit encryption key. This option has SLOWER performance due to restrictions on how this data can be decrypted (Amazon server is NOT be able to decrypt the data; the data has be first downloaded to FileCloud server and then decrypted). The data is NOT accessible via S3 console as well. **Notes**: • • When you choose **SSE-C**, any backups created before it was chosen will become invalid, and therefore that data will not be recoverable. • When SSE-C encryption is enabled, optimized upload is not available for S3 storage and S3 networks.

WARNINGS:

- Enabling encryption will start a process that attempts to encrypt all available data in the bucket as well as all new data.
- This process can take some time depending on the amount of existing data in the bucket.
- It is recommended that you modify the encryption setting when there is minimal activity on the FileCloud Server.

Although changing the Encryption setting can be done at any time, we recommend using off-peak hours to avoid any unexpected access issues.

To enable S3 encryption:

If you are not running the current version of FileCloud Server:
You must enable an additional extension in the php.ini file
	1. On the FileCloud server, open the following file for editing:
	`WEBROOT\php\php.ini`
	2. Add the following line to the file:
	`extension=php_com_dotnet.dll`
	3. Save your changes and close the file.
	4. Restart the Apache server.

If you are running FielCloud Server on Windows
AND
Your xampp folder is installed in a location other than c:\xampp
You must add a key to the cloudconfig.php file
• For example, if your xampp folder is in D:\xampp\htdocs\config\cloudconfig.php
• Then you would add the following line: define("PHPBIN_PATH","D:\\xampp\\php\\php.exe");
	1. On the FileCloud Server, open the following file for editing:
	`<your xampp folder>\htdocs\config\cloudconfig.php`
	2. Add the following line anywhere:
	Replacing *<location>* with your path to the xampp folder
	`define("PHPBIN_PATH","<location>:\\xampp\\php\\php.exe");`
	3. Save your changes and close the file.

Then go to Enabling S3 Storage Encryption	

Upload large files on an Amazon S3 storage server



Beginning with FileCloud 23.241, this process is only effective when you choose **Legacy** for **Upload Method**. When you choose **Optimized** for **Upload Method**, the value in **Chunk Upload Size** is used.

The maximum number of parts per upload accepted by AWS is 1000; to successfully upload files and images in excess of 500 GB, set up an appropriate chunk size. You may set the size as high as 5000 MB.

To set a custom chunk size:

1. Open the file **amazons3storageconfig.php** located in:
   Windows: **c:\xampp\htdocs\config**
   Linux: **/var/www/html/config/**
2. Uncomment the following line, and set the value to the necessary chunk size in MB, up to 5000.

```
define("TONIDOCLOUD_S3_MULTIPART_CHUNKSIZE_IN_MB", 5);
```

Troubleshoot

Using Override Configuration Keys

The following keys are not typically used, however they may be needed in specific circumstances.

KEY	VALUE	Description
TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER	"/somepath/location"	In HA installs, temp folder must be a commonly accessible location. This key must be set in each of the HA nodes
TONIDOCLOUD_S3_PROXY	"http://proxyaddress" or "http://ip"	If a proxy is set in the env, then this key must be set to allow FileCloud service to use the proxy to access S3 servers
TONIDOCLOUD_S3_REDUCED_REDUNDANCY	"1"	This will store the objects with "reduced redundancy"
TONIDOCLOUD_DISABLE_S3_REDIRECT	"1"	(NOT RECOMMENDED) This will force filecloud server to download the file from S3 to the filecloud server system and then send it to client on file downloads (Can be slow)

How to Correct Issues with Image Previews

If you are having problems in previewing images, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.amazonaws.com *.live.com  data: *.duosecurity.com"
```

How to Correct Issues with Text Editors

If you encounter issues where documents stored in Amazon S3 share object storage cannot be edited using a text editor, you can use a workaround to correct this.

Workaround:

1. Change the Header set in the Content-Security-Policy
2. Use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket.

Change the Content-Security-Policy

Content Security Policy (CSP) is an HTTP header that allows site operators control over where resources can be loaded from on their site.

- The use of this header is the best method to prevent cross-site scripting (XSS) vulnerabilities.

To change the Header set in CSP:

1. Open a command-line prompt.
2. Type in the following code (or copy and paste):

```
Content-Security-Policy: "default-src 'self' *.live.com *.amazonaws.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' data
```

Add a CORS Policy

To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket. A CORS configuration is an XML document that defines rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information.For more information about CORS, see Cross-Origin Resource Sharing (CORS) in the Amazon Simple Storage Service Developer Guide.

To allow the use of a text editor:

The CORS configuration is an XML file. The text that you type in the editor must be valid XML.

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Bucket name list, choose the name of the bucket that you want to create a bucket policy for.
3. Choose Permissions, and then choose CORS configuration.
4. In the CORS configuration editor text box, type or copy and paste the following CORS configuration:

```
<CORSConfiguration>
    <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
    <MaxAgeSeconds>3000</MaxAgeSeconds>
    </CORSRule>
</CORSConfiguration>
```

5. Click Save.

How to Correct Issues with playing mp4 videos

If you are having problems in playing mp4 videos, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com
*.amazonaws.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline'
'unsafe-eval' 'self';font-src 'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.amazonaws.com"
```

Add a CORS Policy

To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket. A CORS configuration is an XML document that defines rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information.

For more information about CORS, see Cross-Origin Resource Sharing (CORS) in the Amazon Simple Storage Service Developer Guide.

To allow the use of a text editor:

The CORS configuration is an XML file. The text that you type in the editor must be valid XML.

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Bucket name list, choose the name of the bucket that you want to create a bucket policy for.
3. Choose Permissions, and then choose CORS configuration.
4. In the CORS configuration editor text box, type or copy and paste the following CORS configuration:

```
<CORSConfiguration>
    <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
    <MaxAgeSeconds>3000</MaxAgeSeconds>
    </CORSRule>
</CORSConfiguration>
```

5. Click Save.

Setting up S3 Compatible Services



FileCloud officially supports only Amazon S3 storage.

- Other Amazon S3-compatible storage systems are supported through our Amazon S3 drivers, including:
  - Alibaba Cloud object-based storage
  - Digital Ocean S3 object storage
  - Scality
  - Wasabi
  - Google Cloud object storage
  - Backblaze B2
  - Cloudian S3-Compatible Object Storage
  - Oracle Cloud Infrastructure
  - Storj
- The reliability of these S3-compatible storage systems depends on their compatibility with Amazon S3 API.

Administrators can change the local FileCloud storage type to leverage an S3-compatible storage service you may already be using.

- The local FileCloud storage type should only be changed after FileCloud has been installed but BEFORE any data has been stored.
- Although FileCloud doesn't actively test all S3-compatible services, FileCloud should be able to leverage the storage services similar to Amazon S3.

Integrate with any of the available S3-compatible storage services:

How to Integrate FileCloud with Alibaba Cloud Object Based Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but BEFORE any data has been stored.

- When changing the storage type from local to Alibaba Cloud object storage, the files and folders that have been already stored in the local storage will not be automatically moved to S3 storage.
- In this case, the administrator has to manually export files and folders from local storage before changing the storage type, and manually import them after changing the storage type.

WARNINGS:

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- **Be very careful when changing the storage path, If done improperly it could lead to data loss.**
- The Alibaba cloud Bucket should NEVER be modified outside of FileCloud subsystem
- Do not add, edit, or modify files directly using Alibaba cloud tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to Alibaba Cloud object storage:

1. Enable Alibaba cloud object storage

NOTES:

Although FileCloud does not have an explicit connector for Alibaba cloud object storage, the Amazon S3 connector can be used.

In this step you will need to access **WWWROOT.** It is typically located at:

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To enable Alibaba cloud object storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server.
   b. Synchronize Time with NTP in Linux.
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to this line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

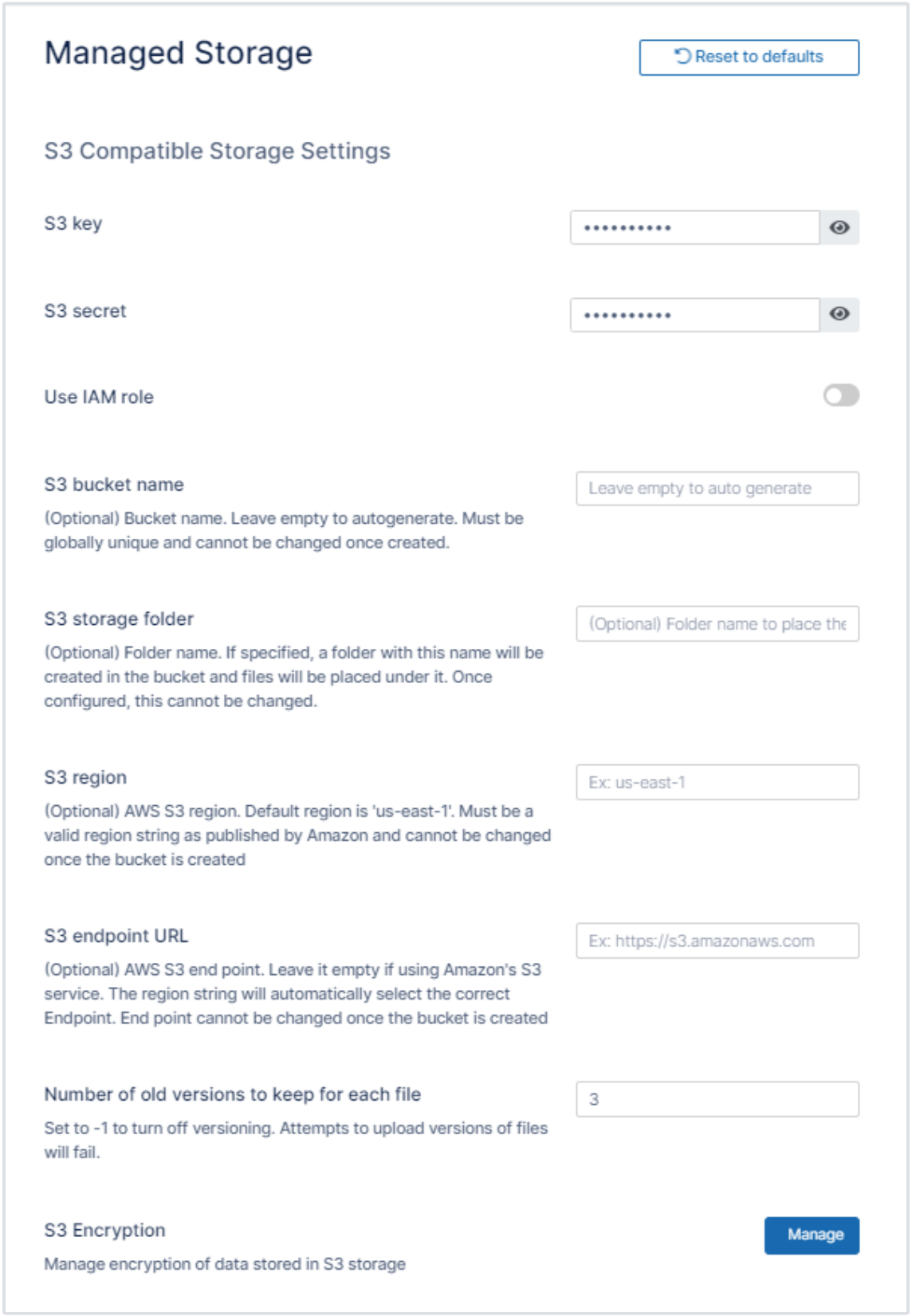
```
WWWROOT/config/amazons3storageconfig.php
```

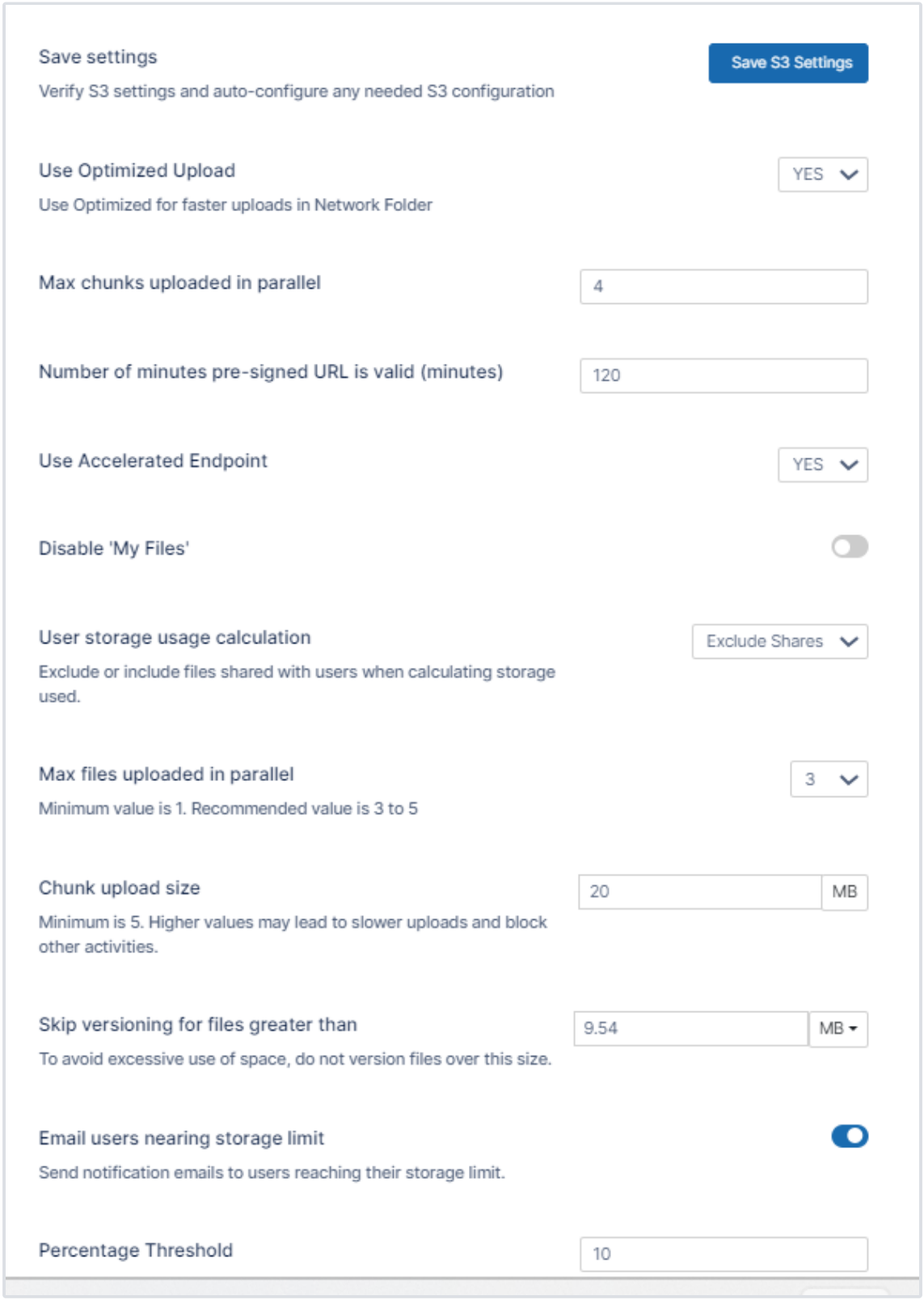
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Alibaba cloud-based object storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the settings for your environment. See the table below for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
Leave empty to auto generate
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
(Optional) Folder name to place the
S3 region
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
Ex: us-east-1
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Ex: https://s3.amazonaws.com
Number of old versions to keep for each file
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
3
S3 Encryption
Manage encryption of data stored in S3 storage
Manage



3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Alibaba cloud authentication key.
S3 Secret	Your Alibaba cloud authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is very important that the S3 bucket is never modified outside of the FileCloud subsystem, The bucket name is case sensitive. Make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: Root storage folder that stores all files. (Will be created automatically).
S3 Region	Optional: The region string.
S3 End Point URL	The S3 endpoint. Note that for each region there is a specific Endpoint URL.

4. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems previewing images, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.aliyuncs.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems playing mp4 videos, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.aliyuncs.com;
style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval'
'self';font-src 'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.aliyuncs.com"
```

How to Integrate Filecloud with Backblaze (B2) Cloud Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but before any data has been stored.

- When changing the storage type from local to B2 object storage, the files and folders that have been already stored in local storage will not be automatically moved to S3 storage.
- In this case, the administrator must manually export files and folders from local storage before changing the storage type, and then manually import them after changing the storage type.

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- Be careful when changing the storage path; If done improperly it could lead to data loss.
- The Backblaze B2 storage should NEVER be modified outside of the FileCloud subsystem.
- Do not add, edit, or modify files directly using Backblaze tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to Backblaze(B2) object storage:

1. Enable B2 object storage

NOTES:

Although FileCloud does not have an explicit connector for B2 object-based storage, the Amazon S3 connector can be used.

In this step you will need to access WWWROOT. It is typically located at:

Windows	Linux
c:\xampp\htdocs	/var/www/html

To enable B2 object storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

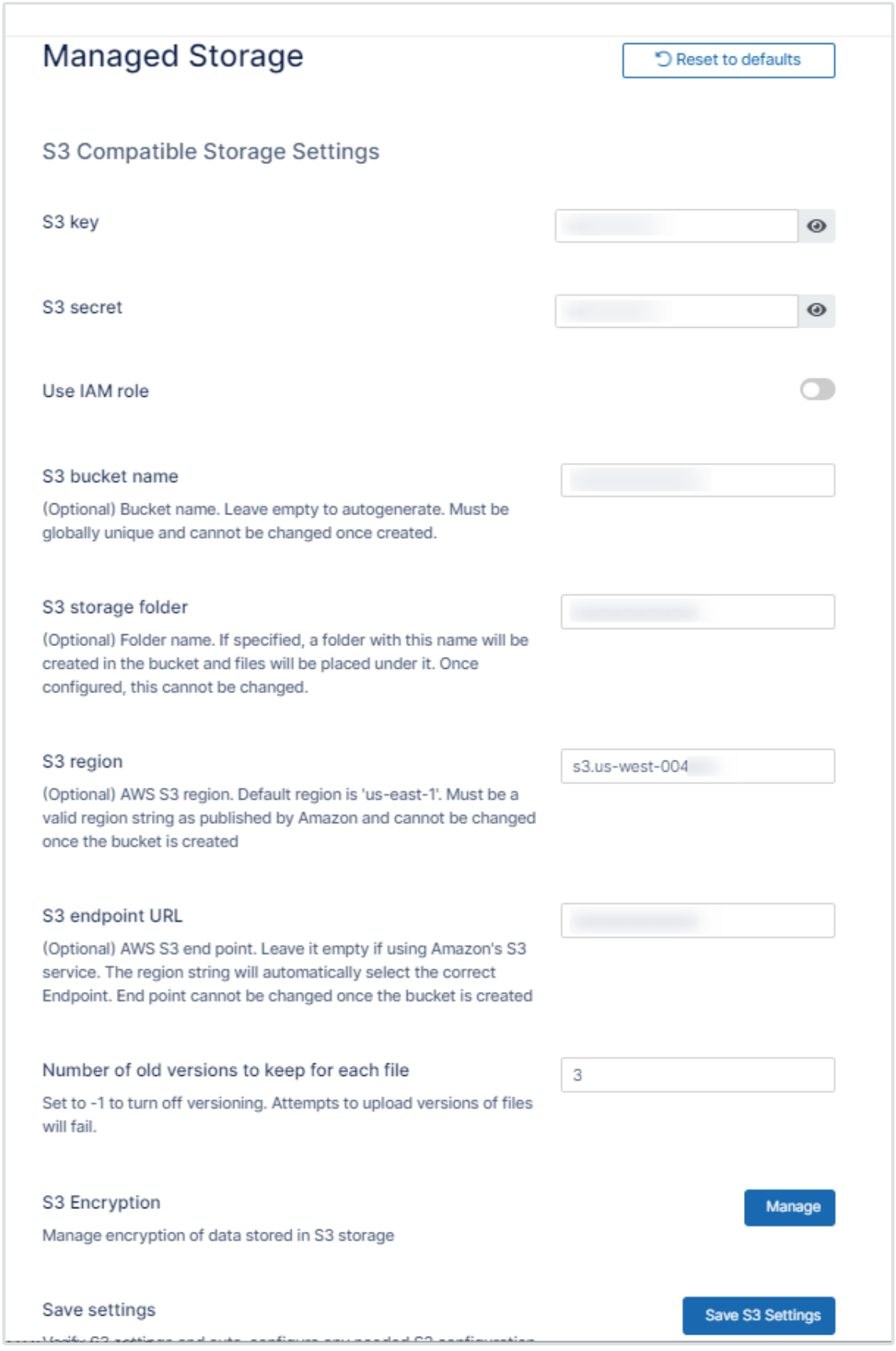
```
WWWROOT/config/amazons3storageconfig.php
```

💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

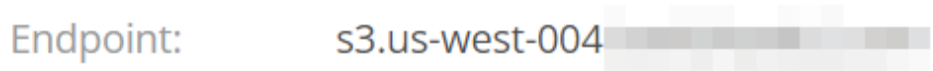
2. Configure Credentials

To configure Backblaze (B2) Credentials

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Enter the settings for your environment. See the table below for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
S3 region
s3.us-west-004
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
S3 Encryption
Manage
Manage encryption of data stored in S3 storage
Save settings
Save S3 Settings

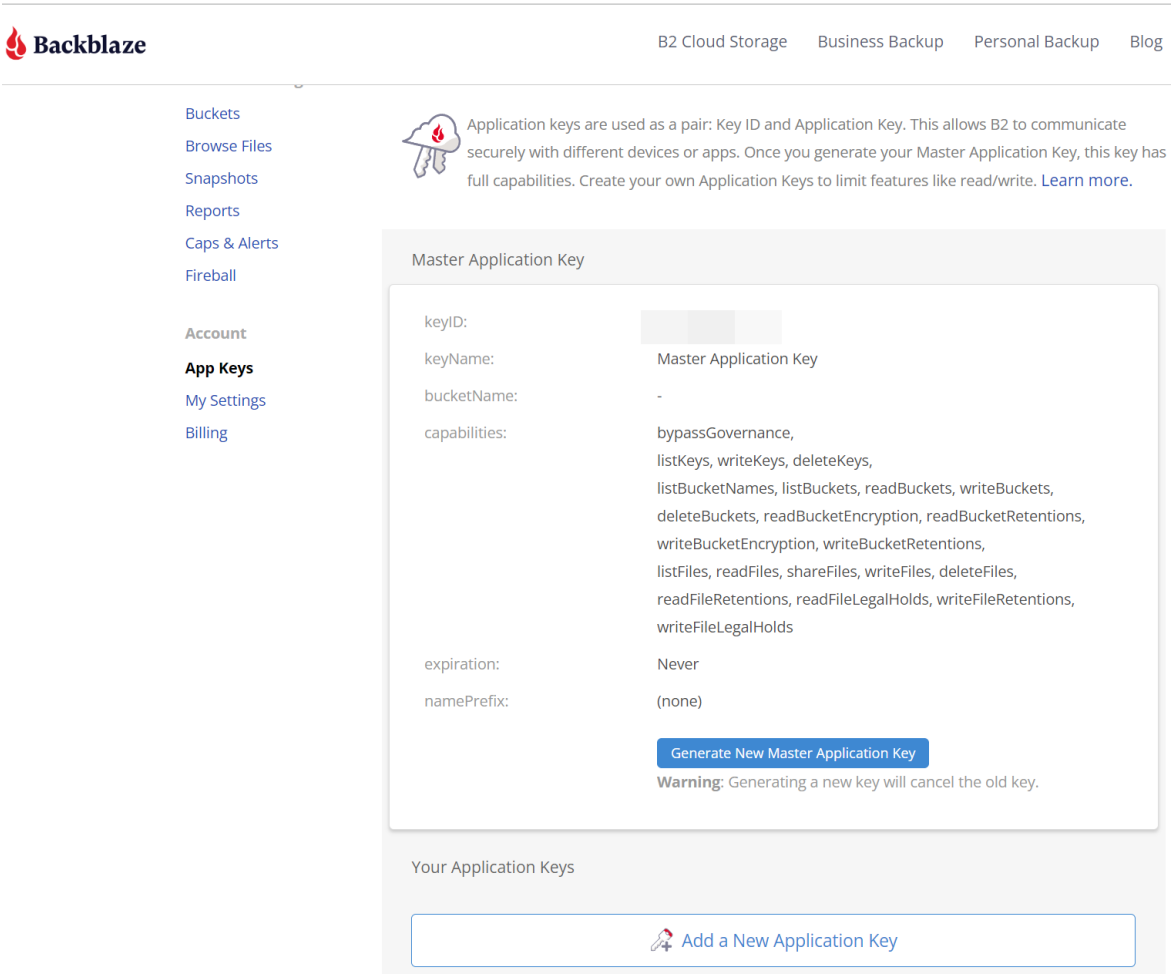
3. Click **Save S3 Settings**.
4. Enter values for **Number of old versions to keep for each file**, and, if you are using encryption, click **Manage** for **S3 Encryption** to set the encryption type.
5. Click **Save**.

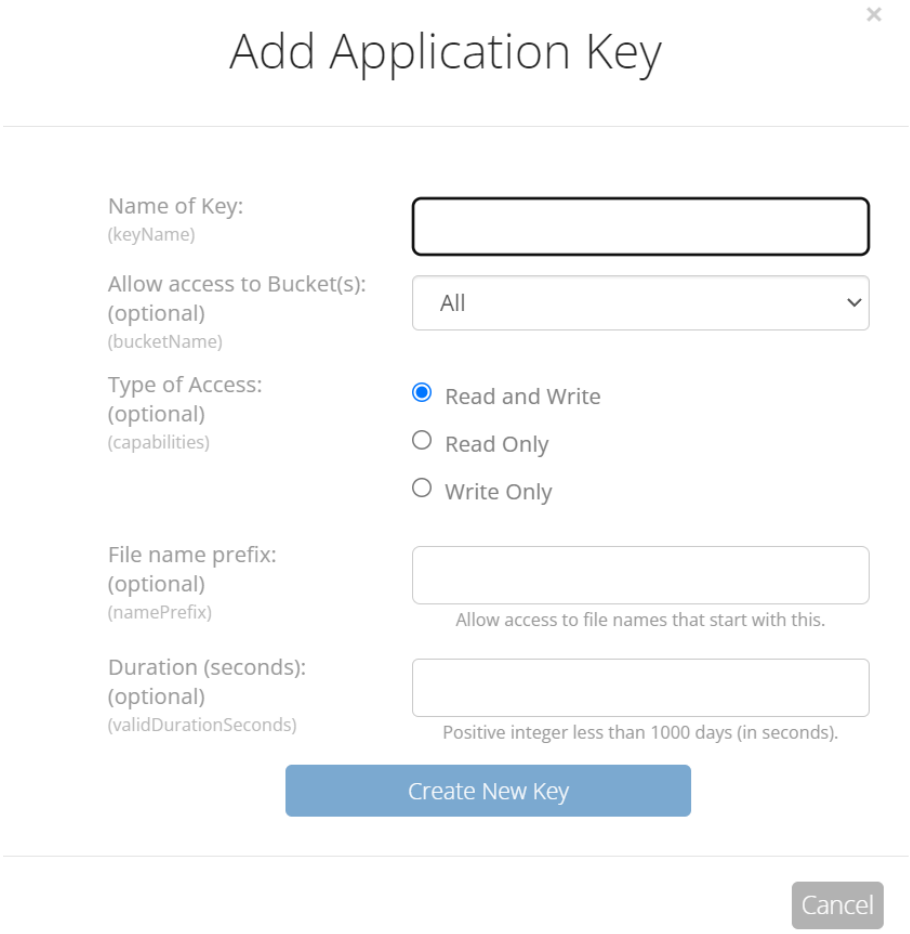
Field	Description
S3 Key	Your B2 authentication key.
S3 Secret	Your B2 authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem, The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string. 
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL.
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, attempts to upload versions of a file fail.
S3 Encryption	By default encryption type is: **Backblaze B2 key (SSE-B2)**, an encryption key that Backblaze creates, manages and uses for you. For this integration, only Google-managed key encryption is supported. No additional actions are need in FileCloud.

6. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

To enable HMAC access key for a bucket, go to **Account > App Keys**, and select the **Add a New Application Key** button under "Your Application Keys".

*Selecting "All" under "Allow access to Bucket(s): (optional) is a requirement for this integration. Otherwise it will throw out a missing capability error.


Backblaze
B2 Cloud Storage
Business Backup
Personal Backup
Blog
Buckets
Browse Files
Snapshots
Reports
Caps & Alerts
Fireball
Account
App Keys
My Settings
Billing
Application keys are used as a pair: Key ID and Application Key. This allows B2 to communicate securely with different devices or apps. Once you generate your Master Application Key, this key has full capabilities. Create your own Application Keys to limit features like read/write. Learn more.
Master Application Key
keyID:
keyName:
Master Application Key
bucketName:
-
capabilities:
bypassGovernance,
listKeys, writeKeys, deleteKeys,
listBucketNames, listBuckets, readBuckets, writeBuckets,
deleteBuckets, readBucketEncryption, readBucketRetentions,
writeBucketEncryption, writeBucketRetentions,
listFiles, readFiles, shareFiles, writeFiles, deleteFiles,
readFileRetentions, readFileLegalHolds, writeFileRetentions,
writeFileLegalHolds
expiration:
Never
namePrefix:
(none)
Generate New Master Application Key
Warning: Generating a new key will cancel the old key.
Your Application Keys
Add a New Application Key



Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems previewing images, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.wasabisys.com
*.googleapis.com *.backblazeb2.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems playing mp4 videos, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.wasabisys.com
*.googleapis.com *.backblazeb2.com; style-src 'unsafe-inline' 'self';script-src
'unsafe-inline' 'unsafe-eval' 'self';font-src 'self' data:;img-src 'self'
*.live.com  data: *.duosecurity.com *.wasabisys.com *.googleapis.com
*.backblazeb2.com"
```

How to Integrate FileCloud with Digital Ocean Spaces

Administrators can change the FileCloud storage type after FileCloud has been installed but BEFORE any data has been stored.

- When changing the storage type from local to Digital Ocean S3, files and folders that have been already stored in the local storage will not be automatically moved to S3 storage.
- In this case, the administrator must manually export files and folders from local storage before changing the storage type, and then manually import them after changing the storage type.

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- Be careful when changing the storage path; if done improperly it could lead to data loss.
- The Digital Ocean S3 Bucket should never be modified outside of FileCloud.
- Do not add/edit/modify files directly using Digital Ocean tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to DIGITAL OCEAN S3:

1. Enable Digital Ocean S3 object storage

Notes:

Although FileCloud does not have an explicit connector for Digital Ocean, the Amazon S3 connector can be used.

In this step you will need to access **WWWROOT**. It is typically located at:

Windows	Linux
c:\xampp\htdocs	/var/www/html

To enable Digital Ocean s3 storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

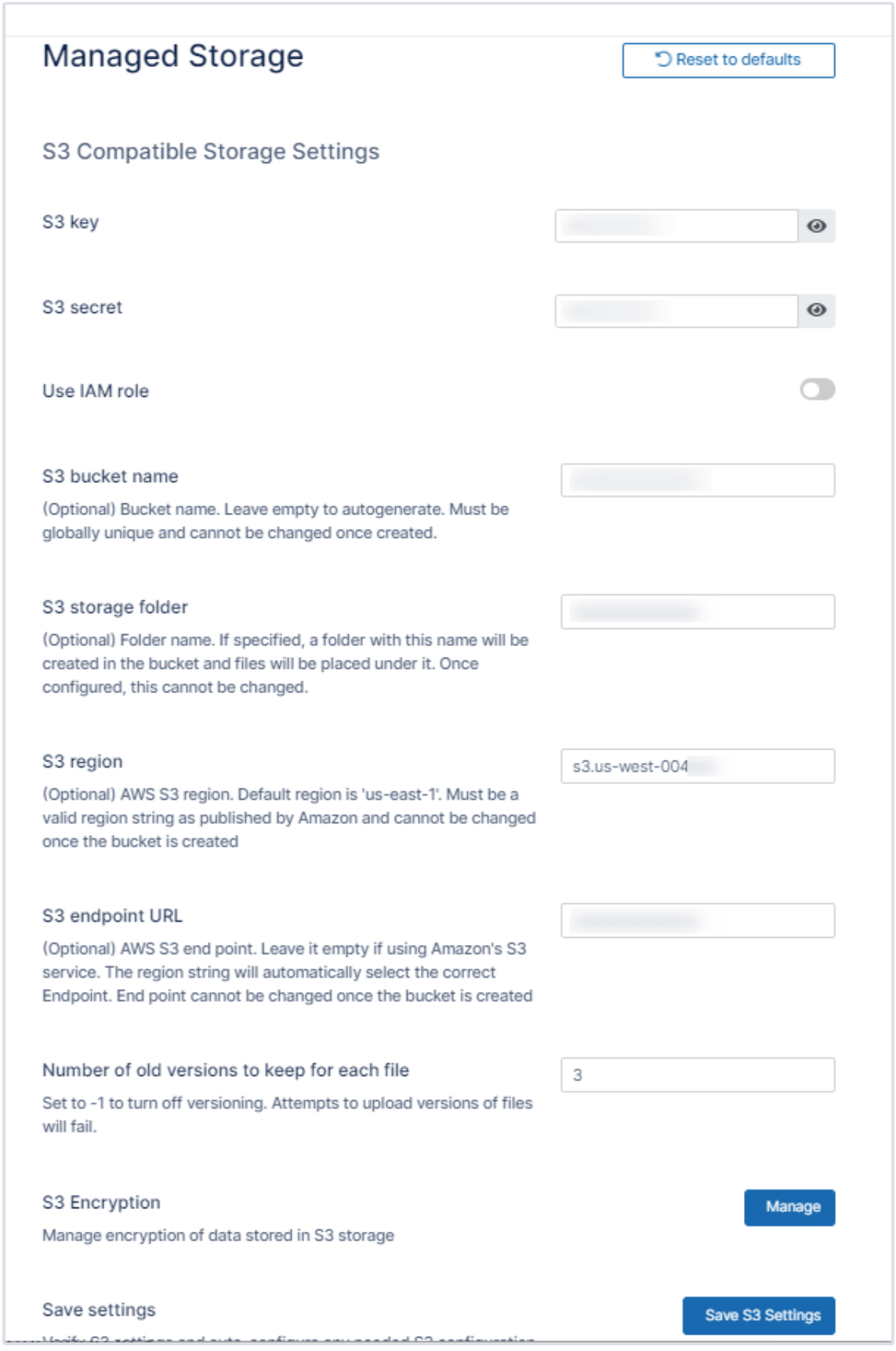
```
WWWROOT/config/amazons3storageconfig.php
```

💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Digital Ocean S3 Credentials

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Enter the settings for your environment.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
S3 region
s3.us-west-004
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
S3 Encryption
Manage
Manage encryption of data stored in S3 storage
Save settings
Save S3 Settings

3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Digital Ocean authentication key.
S3 Secret	Your Digital Ocean authentication secret.
Use IAM Role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstance, a previously used bucket in FileCloud may be used). It is important that the S3 bucket is never modified outside of FileCloud. The bucket name is case sensitive; confirm that you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string.
S3 End Point URL	The S3 endpoint. Note that for each region there is a specific Endpoint URL.

4. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Troubleshooting:

How to correct issues with image previews

If you are having problems previewing images, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
```

```
'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.digitaloceanspaces.com"
```

How to correct Issues with mp4 videos

If you are having problems playing mp4 videos, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com
*.digitaloceanspaces.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-
inline' 'unsafe-eval' 'self';font-src 'self' data:;img-src 'self' *.live.com
data: *.duosecurity.com *.digitaloceanspaces.com"
```

How to Integrate FileCloud with Google Cloud Object Based Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but before any data has been stored.

- When changing the storage type from local to GCP object storage, the files and folders that have been already stored in local storage will not be automatically moved to S3 storage.
- In this case, the administrator must manually export files and folders from local storage before changing the storage type, and then manually import them after changing the storage type.

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- Be careful when changing the storage path; If done improperly it could lead to data loss.
- The GCP Bucket should NEVER be modified outside of the FileCloud subsystem.
- Do not add, edit, or modify files directly using GCP tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to GCP object storage:

1. Enable GCP object storage

NOTES:

Although FileCloud does not have an explicit connector for GCP object-based storage, the Amazon S3 connector can be used.

In this step you will need to access WWWROOT. It is typically located at:

Windows	Linux
c:\xampp\htdocs	/var/www/html

To enable GCP object storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

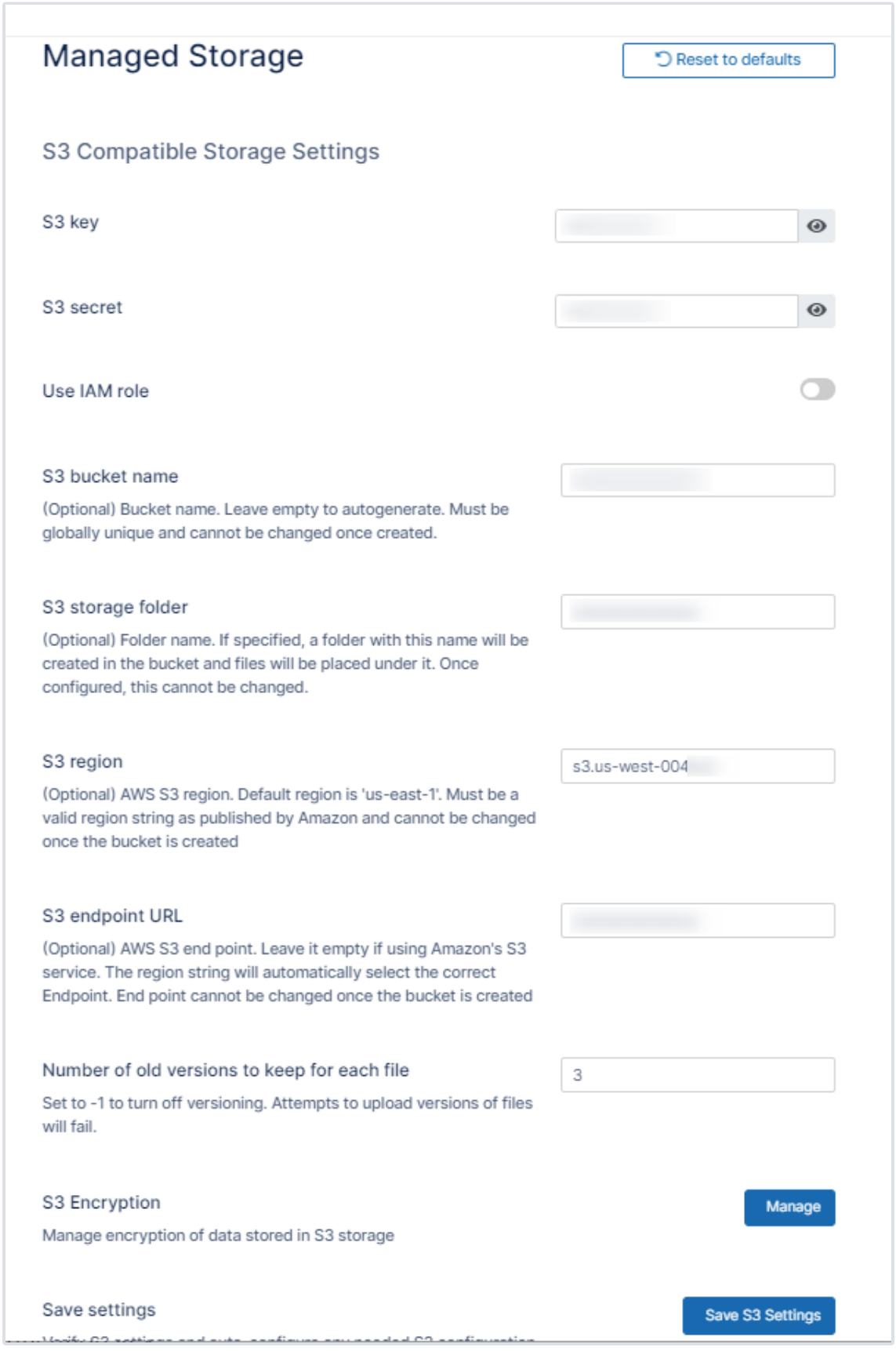
```
WWWROOT/config/amazons3storageconfig.php
```

💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Digital Ocean S3 Credentials

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the settings for your environment. See the table below for information about each setting.

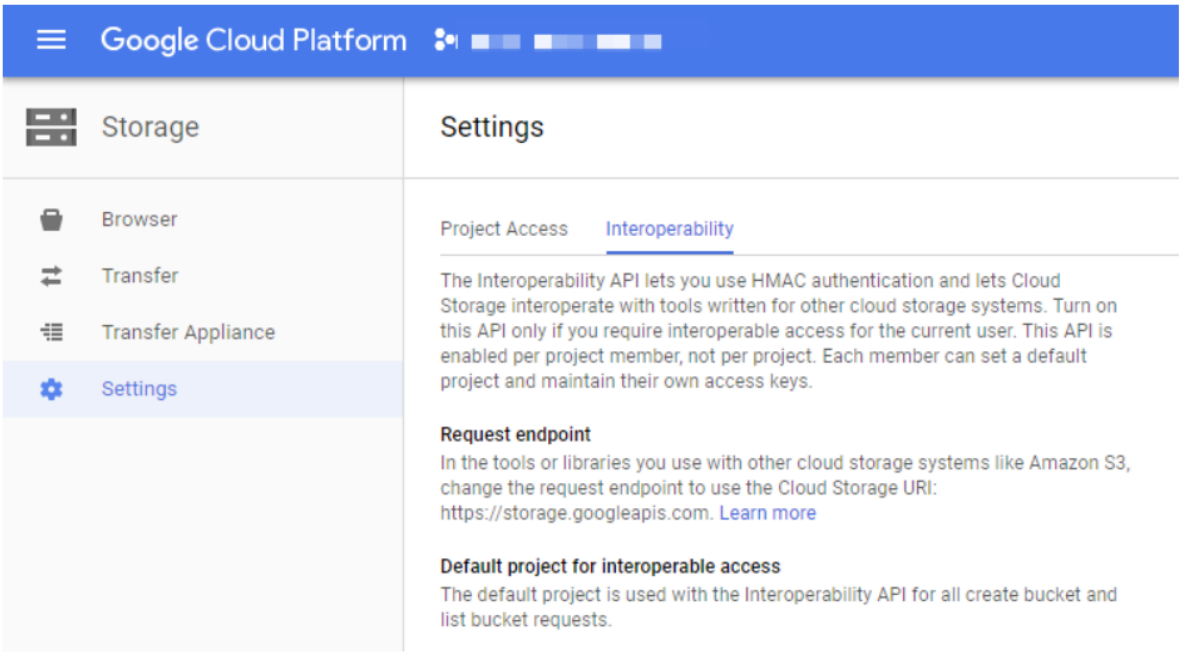

Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
S3 region
s3.us-west-004
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
S3 Encryption
Manage
Manage encryption of data stored in S3 storage
Save settings
Save S3 Settings

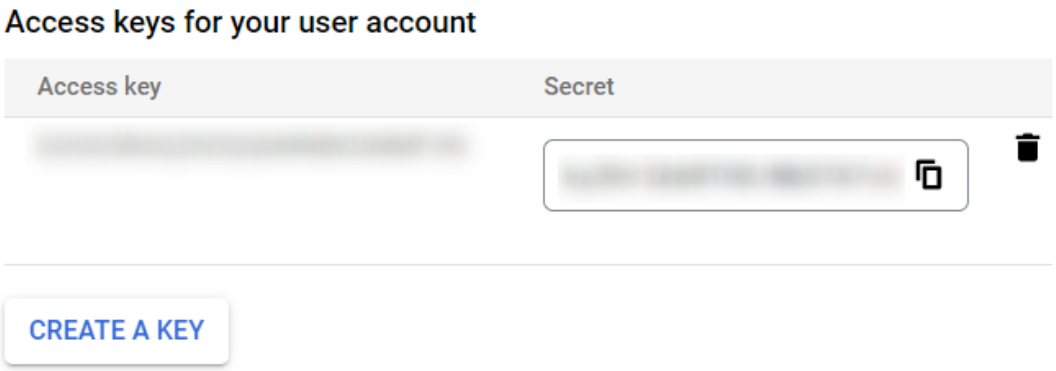
3. Click **Save S3 Settings**.
4. Enter values for **Number of old versions to keep for each file**, and, if you are using encryption, click **Manage** for **S3 Encryption** to set the encryption type.
5. Click **Save**.

Field	Description
S3 Key	Your GCP HMAC authentication key.
S3 Secret	Your GCP HMAC authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem, The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string. Generally use: **auto**
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL. Generally, it is: **https://storage.googleapis.com**
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, versioning is disabled and attempts to upload versions of a file fail.
S3 Encryption	By default encryption type is: **Google-managed keys**. For this integration, only Google-managed key encryption is supported. No additional actions are needed in FileCloud.

6. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

To enable HMAC access key for a bucket, go to **Google cloud storage > Settings**, and select the **Interoperability** tab. You should see an empty list and a **CREATE A KEY** button.





Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems previewing images, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.wasabisys.com
*.googleapis.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems playing mp4 videos, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.wasabisys.com
*.googleapis.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline'
'unsafe-eval' 'self';font-src 'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.wasabisys.com *.googleapis.com"
```

How to integrate FileCloud with Scality Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but BEFORE any data has been stored.

- When changing the storage type from local to Scality, the files and folders that have been already stored in the local storage will not be automatically moved to S3 storage.
- In this case, the administrator has to manually export files and folders from local storage before changing storage type and manually import them after changing the storage type.

WARNINGS:

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- **Be very careful when changing the storage path, If done improperly it could lead to data loss.**
- The Scality Bucket should NEVER be modified outside of FileCloud subsystem
- Do not add, edit, or modify files directly using Scality tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to SCALITY:

1. Enable Scality object storage

NOTES:

Although FileCloud does not have an explicit connector for Scality, the Amazon S3 connector can be used.

In this step you will need to access **WWWROOT. It is typically located at:**

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To enable Scality storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to this line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

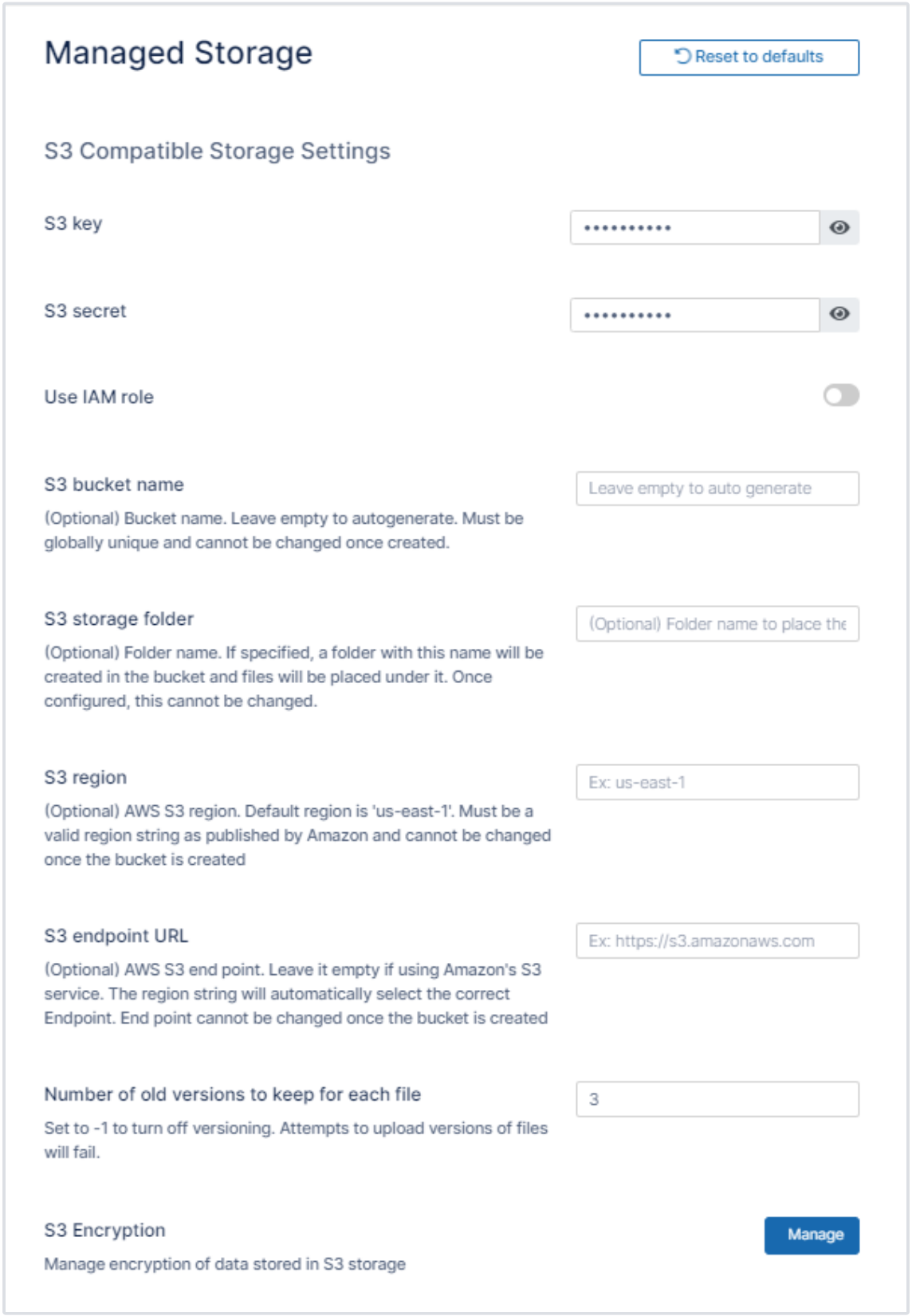
```
WWWROOT/config/amazons3storageconfig.php
```

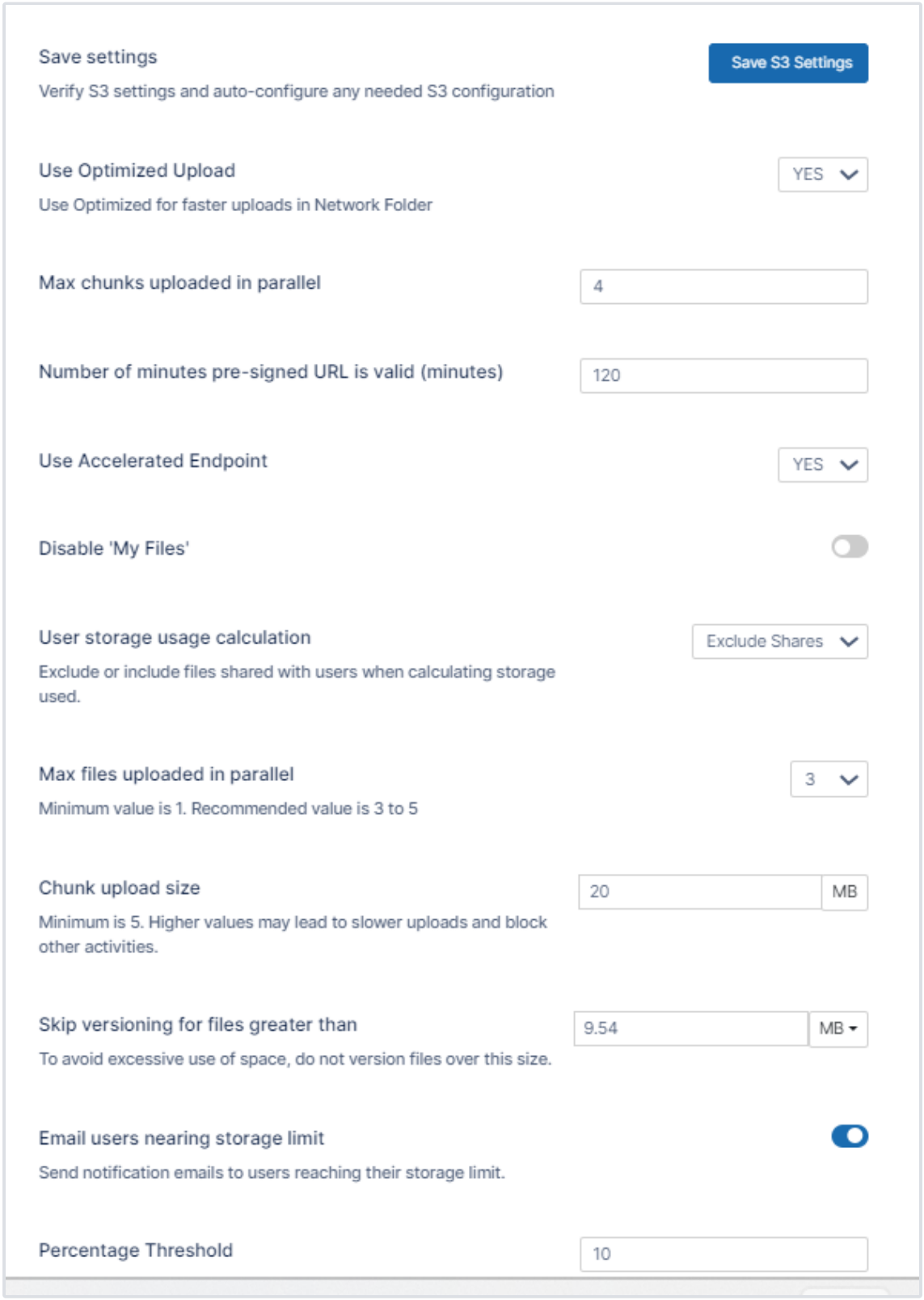
Nothing needs to be added or edited in amazons3storageconfig.php

2. Configure Credentials

To configure Digital Ocean S3 Credentials:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the settings for your environment. See the table below for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
Leave empty to auto generate
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
(Optional) Folder name to place the
S3 region
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
Ex: us-east-1
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Ex: https://s3.amazonaws.com
Number of old versions to keep for each file
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
3
S3 Encryption
Manage encryption of data stored in S3 storage
Manage



3. Click **Save S3 Settings**.

Field	Description
S3 Key	This is your Scality authentication key.
S3 Secret	This is your Scality authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstance, previously used bucket in FileCloud could be used). It is very important that the S3 bucket is never modified outside of the FileCloud subsystem, the bucket name is case sensitive make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files will be stored inside this root storage folder (Will be created automatically).
S3 Region	Optional: Provide the region string.
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific Endpoint URL.

4. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems in previewing images, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.scality.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems in playing mp4 videos, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.scality.com;
style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval'
'self';font-src 'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.scality.com"
```

How to Integrate FileCloud with Wasabi Object Based Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but BEFORE any data has been stored.

- When changing the storage type from local to Wasabi, the files and folders that have been already stored in the local storage will not be automatically moved to S3 storage.
- In this case, the administrator has to manually export files and folders from local storage before changing storage type and manually import them after changing the storage type.

WARNINGS:

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- **Be very careful when changing the storage path, If done improperly it could lead to data loss.**
- The Wasabi Bucket should NEVER be modified outside of FileCloud subsystem
- Do not add, edit, or modify files directly using Wasabi tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to WASABI:

1. Enable Wasabi object storage

NOTES:

Although FileCloud does not have an explicit connector for Wasabi Object based storage, the Amazon S3 connector can be used.

In this step you will need to access **WWWROOT. It is typically located at:**

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To enable Wasabi storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to this line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

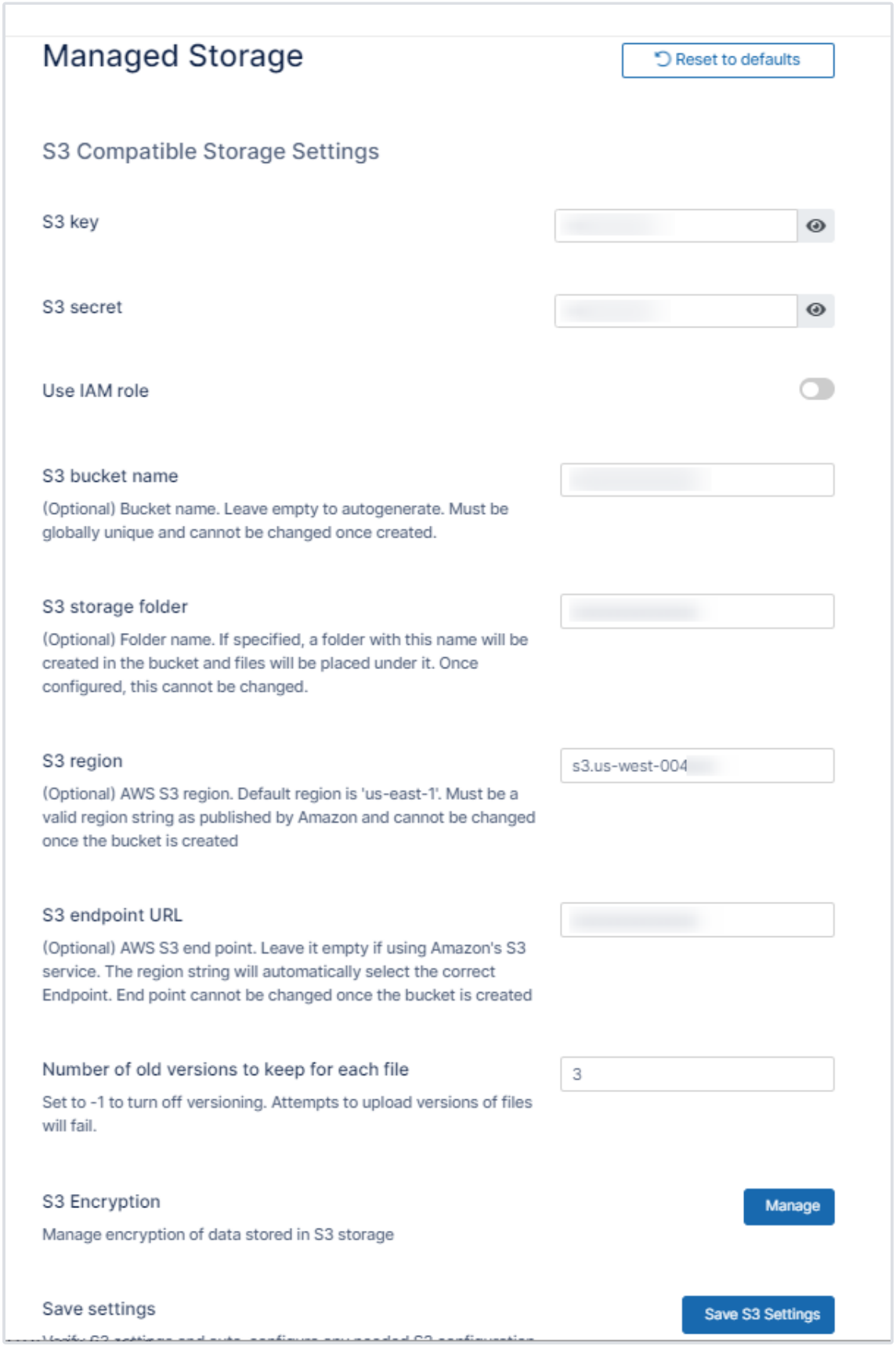
```
WWWROOT/config/amazons3storageconfig.php
```

Nothing needs to be added or edited in amazons3storageconfig.php

2. Configure Credentials

To configure Wasabi object-based storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the settings for your environment. See the table below for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
S3 region
s3.us-west-004
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
S3 Encryption
Manage
Manage encryption of data stored in S3 storage
Save settings
Save S3 Settings

Field	Description
S3 Key	This is your Wasabi authentication key.
S3 Secret	This is your Wasabi authentication secret.
Use IAM role	When checked, the S3 Key and S3 Secret fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstance, previously used bucket in FileCloud could be used). It is very important that the S3 bucket is never modified outside of the FileCloud subsystem, the bucket name is case sensitive make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files will be stored inside this root storage folder (Will be created automatically).
S3 Region	Optional: Provide the region string.
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific Endpoint URL.
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, versioning is disabled, and attempts to upload a version of a file fail.
S3 Encryption	Select **No encryption** because Wasabi does not support managed key encryption.

3. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems in previewing images, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`

b. `Linux: /var/www/html/.htaccess`

2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.wasabisys.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems in playing mp4 videos, you should add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com
*.wasabisys.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline'
'unsafe-eval' 'self';font-src 'self' data:;img-src 'self' *.live.com  data:
*.duosecurity.com *.wasabisys.com"
```

FileCloud Blogs

- Migrating Storage Between Regions

How to Integrate Filecloud with Cloudian S3-Compatible Object Storage

Administrators can change the FileCloud storage type after FileCloud has been installed but before any data has been stored.

- When changing the storage type from local to Cloudian S3-Compatible Object Storage, the files and folders that have been already stored in local storage will not be automatically moved to S3 storage.
- In this case, the administrator must manually export files and folders from local storage before changing the storage type, and then manually import them after changing the storage type.

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- Be careful when changing the storage path; If done improperly it could lead to data loss.
- The Cloudian S3-Compatible Object Storage should NEVER be modified outside of the FileCloud subsystem.
- Do not add, edit, or modify files directly using Cloudian tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to Cloudian S3-Compatible Object Storage:

1. Enable Cloudian S3-Compatible Object Storage

NOTES:

Although FileCloud does not have an explicit connector for Cloudian S3-Compatible Object Storage, the Amazon S3 connector can be used.

In this step you will need to access WWWROOT. It is typically located at:

Windows	Linux
c:\xampp\htdocs	/var/www/html

To enable Cloudian S3-Compatible Object Storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

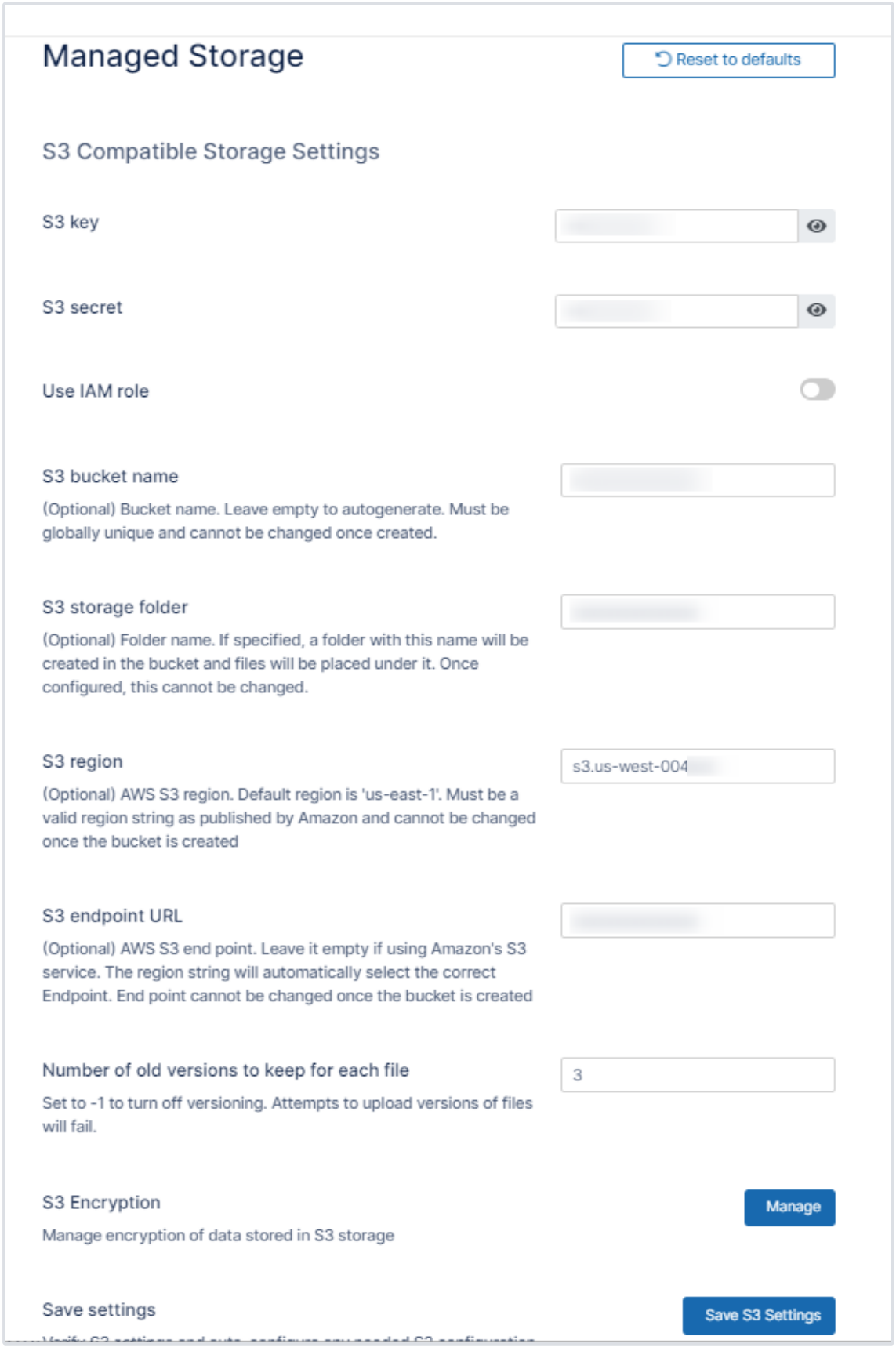
```
WWWROOT/config/amazons3storageconfig.php
```

💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Cloudian S3-compatible object storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Enter the settings for your environment. See the following table for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
S3 region
s3.us-west-004
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
S3 Encryption
Manage
Manage encryption of data stored in S3 storage
Save settings
Save S3 Settings

3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Cloudian S3 authentication key.
S3 Secret	Your Cloudian S3 authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem. The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string.
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL.
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, versioning is disabled and attempts to upload a version of a file fail.
S3 Encryption	Select **No encryption** because Cloudian does not support managed key encryption.

4. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Troubleshooting:

How to Correct Issues with Image Previews

If you are having problems previewing images, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`

b. `Linux: /var/www/html/.htaccess`

2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com; style-src
'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src
'self' data:;img-src 'self' *.live.com  data: *.duosecurity.com *.wasabisys.com
*.googleapis.com *.cloudian.com"
```

How to Correct Issues with playing mp4 videos

If you are having problems playing mp4 videos, add a line to the .htaccess file.

To add a line to the .htaccess file:

1. Open the following file:
   a. `Windows:  C:\xampp\htdocs\.htaccess`
   b. `Linux: /var/www/html/.htaccess`
2. Add the following line:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.wasabisys.com
*.googleapis.com *.cloudian.com.com; style-src 'unsafe-inline' 'self';script-src
'unsafe-inline' 'unsafe-eval' 'self';font-src 'self' data:;img-src 'self'
*.live.com  data: *.duosecurity.com *.wasabisys.com *.googleapis.com
*.cloudian.com"
```

How to Integrate FileCloud with Oracle Cloud Infrastructure

Administrators can change the FileCloud storage type to Oracle Cloud Infrastructure (OCI) after FileCloud has been installed but before any data has been stored.

- When changing the storage type from local to OCI, the files and folders that have been already stored in the local storage will not be automatically moved to S3 storage.
- In this case, the administrator has to manually export files and folders from local storage before changing the storage type, and manually import them after changing the storage type.

WARNINGS:

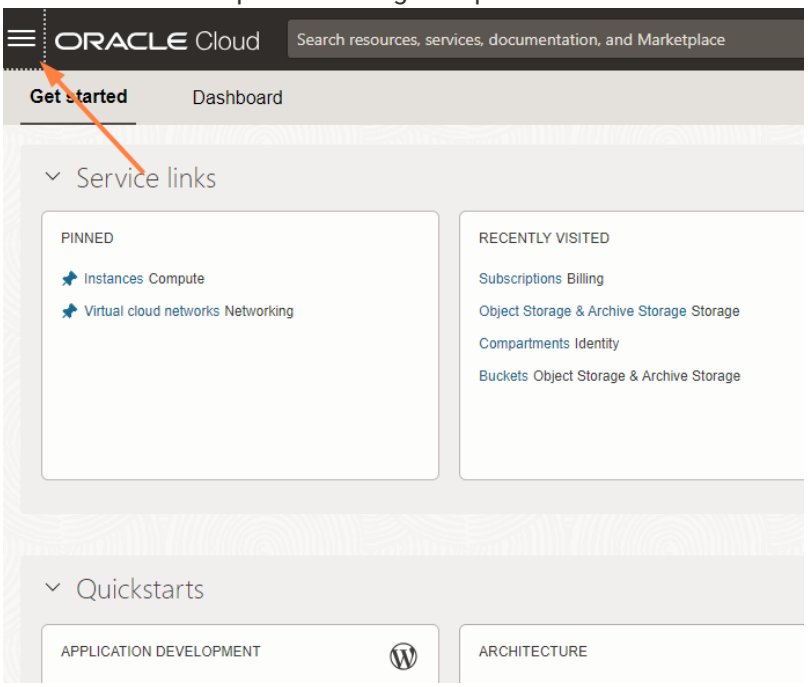
- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- **Be very careful when changing the storage path, If done improperly it could lead to data loss.**

- The OCI bucket should never be modified outside of FileCloud subsystem.
- Do not add, edit, or modify files directly using OCI cloud tools. Doing so will destabilize your FileCloud installation.

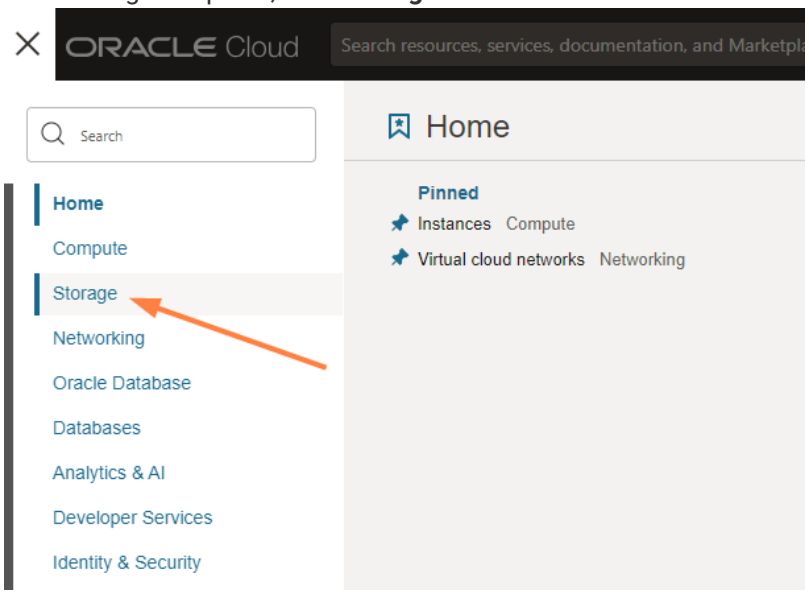
To create the S3 storage bucket and get your S3 key values in Oracle Cloud Infrastructure

Create the S3 storage bucket and generate your S3 keys. In addition, save the values you will need to enter when you are configuring the OCI/FileCloud integration in the next procedure on this page.

1. Log in to **https://cloud.oracle.com**.
2. Click the icon that opens the navigation panel:

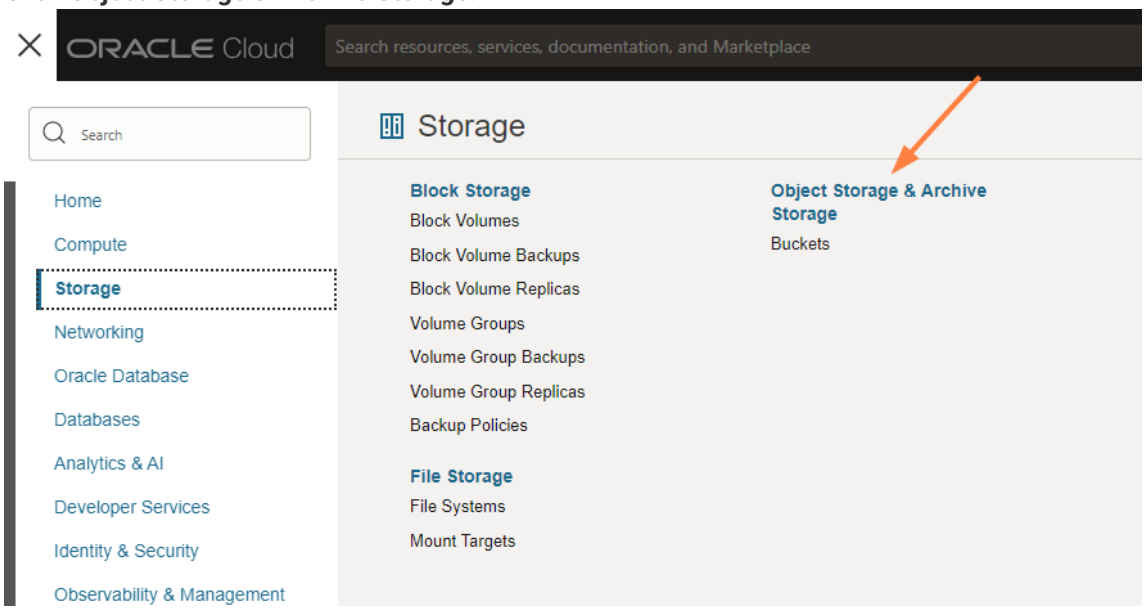


3. In the navigation panel, click **Storage**.



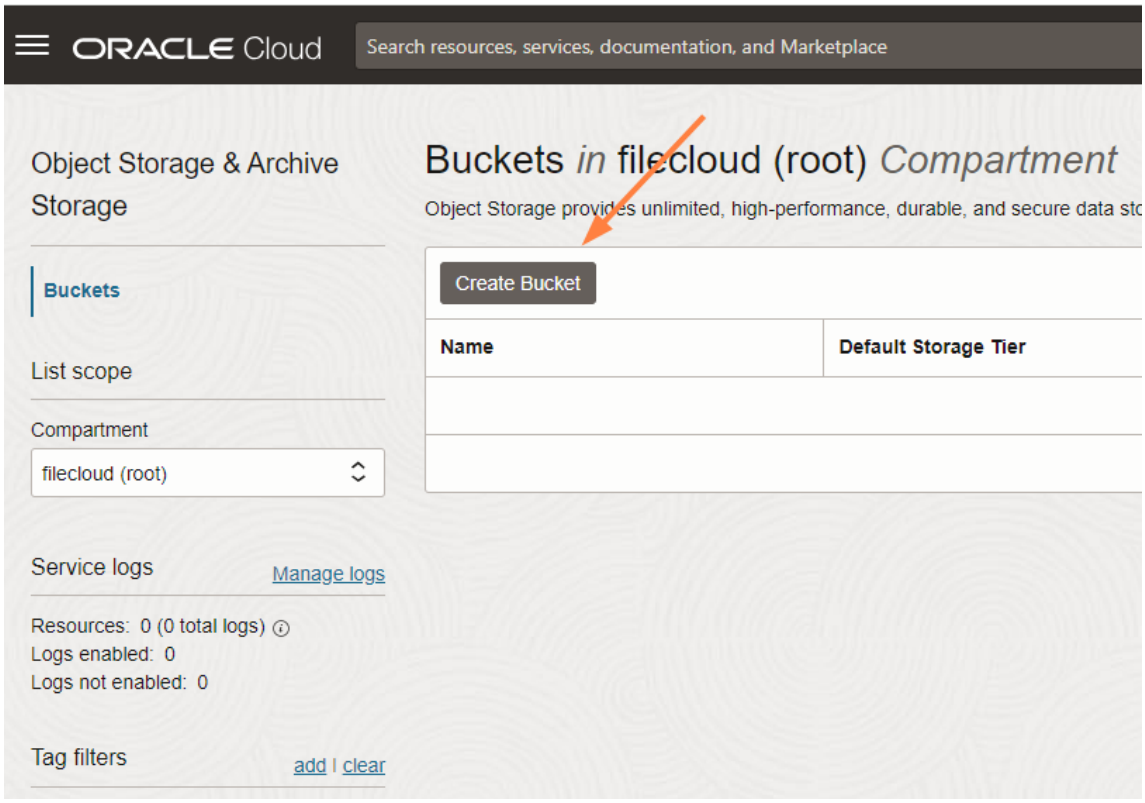
A list of storage-related pages opens.

4. Click **Object Storage & Archive Storage**.



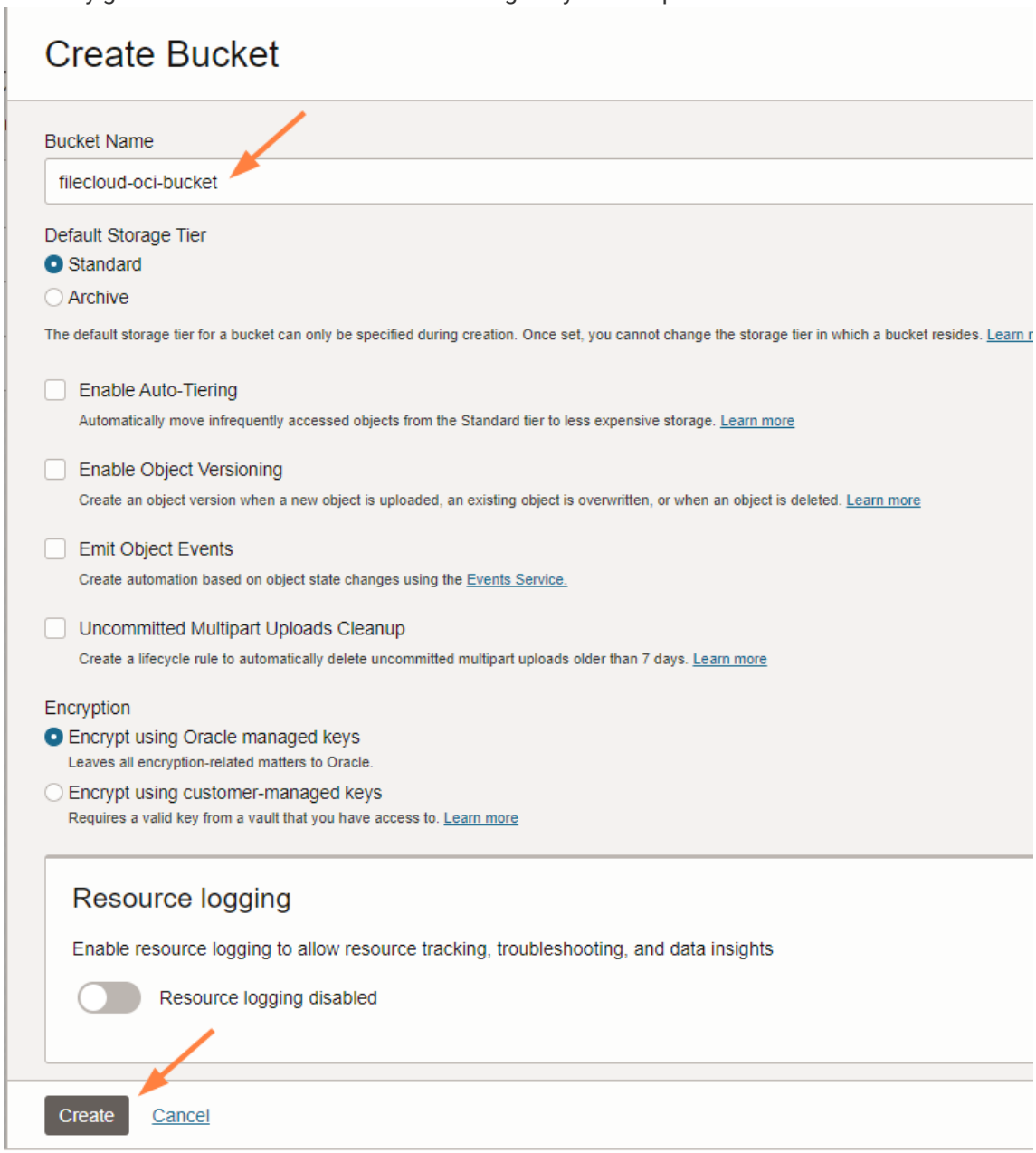
The **Object Storage & Archive Storage** page opens.

5. Click **Create Bucket**.



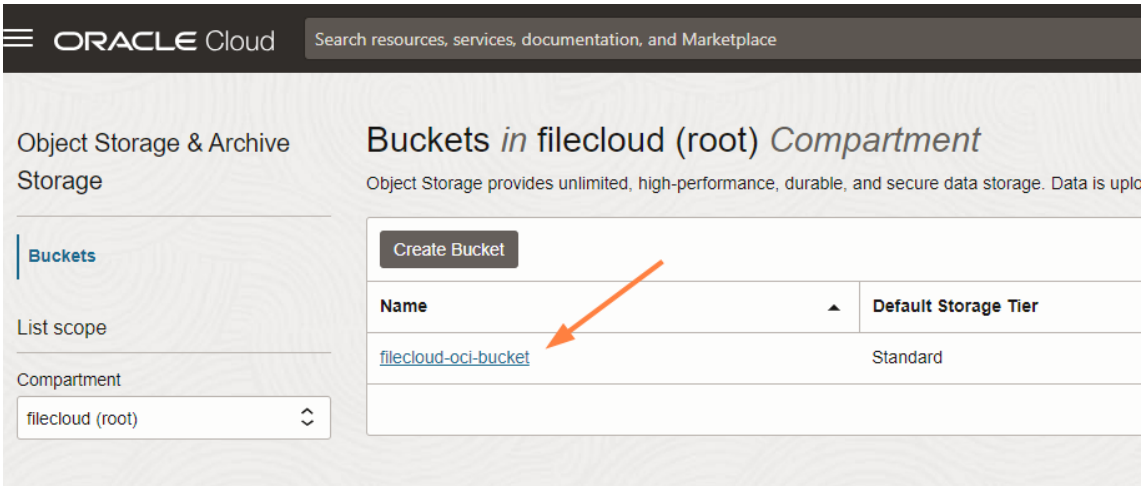
A **Create Bucket** dialog box opens.

6. You may give the bucket a new name and change any of the options. Then click **Create**.



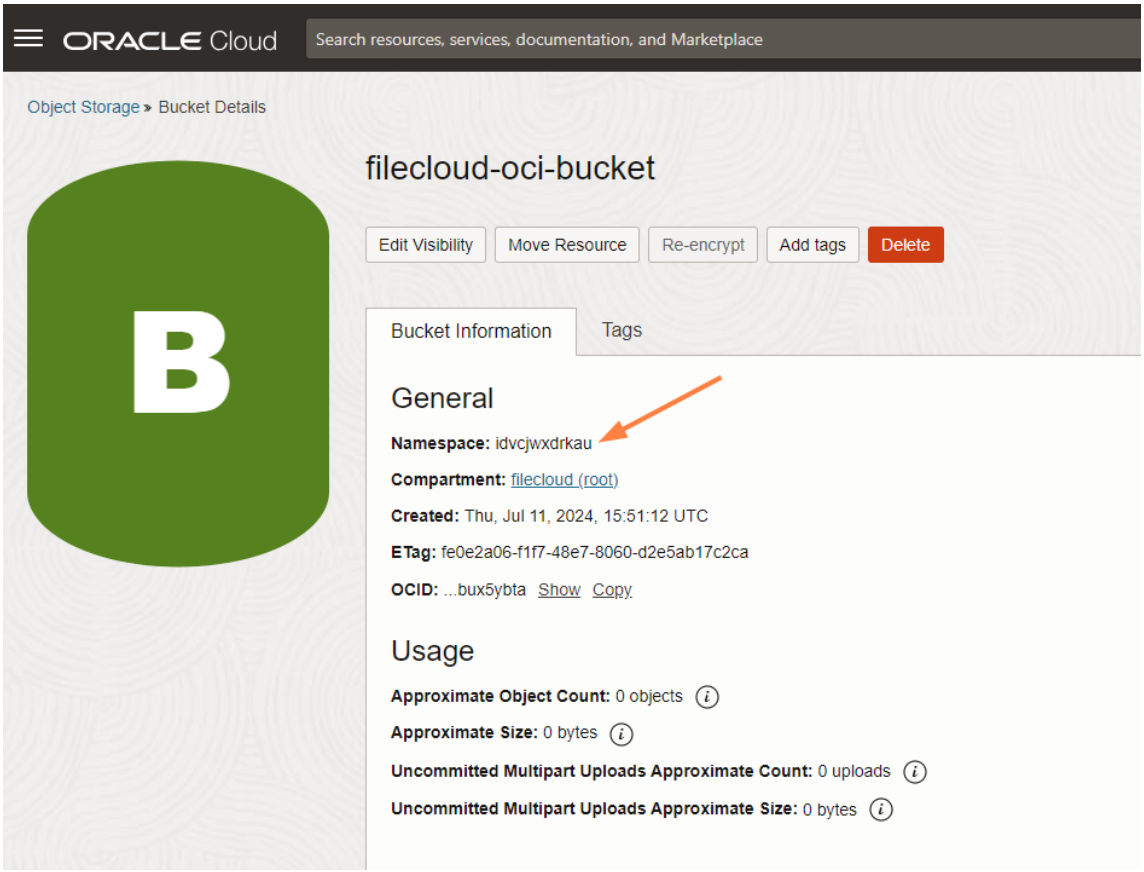
The bucket appears in the list of buckets.

7. Click the bucket name.



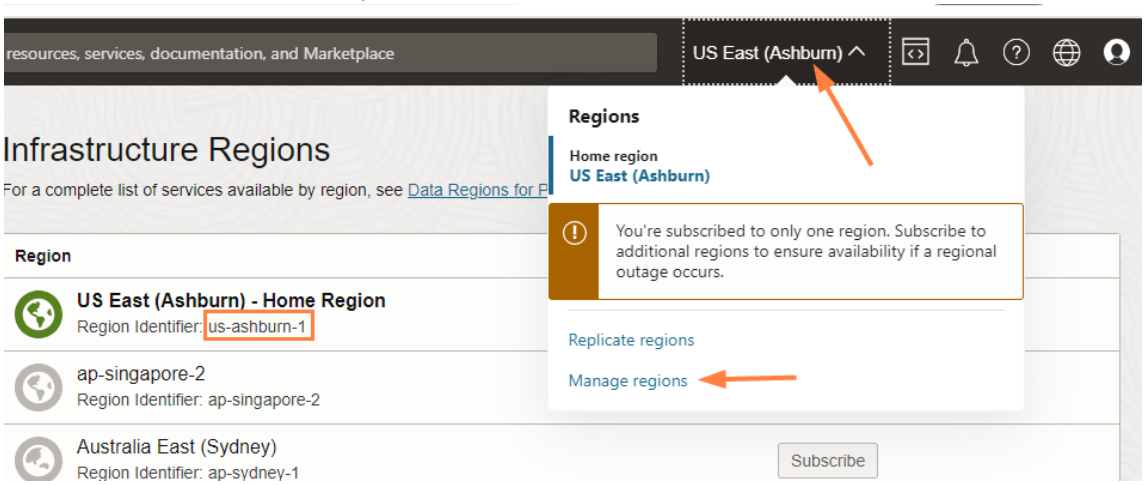
A tab with bucket information opens.

8. Copy and save the value of **Namespace** to use when you enter the S3 end point URL into FileCloud.

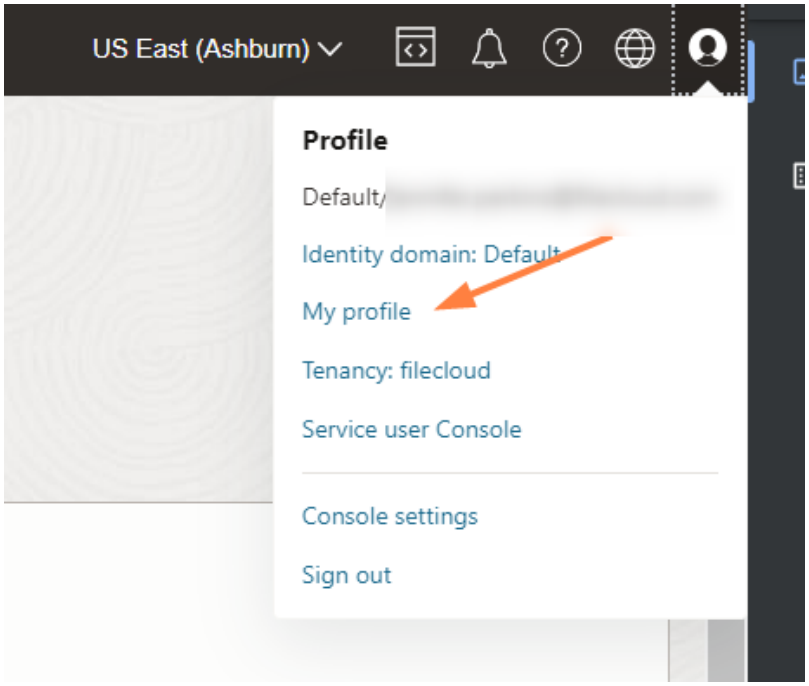


9. Get your region by clicking the name of your region at the top of the OCI screen, and choosing **Manage regions** in the drop-down list.
Copy the **Region Identifier** from the top region shown (the region with the green globe icon) and

save it to enter later in S3 end point URL in FileCloud.

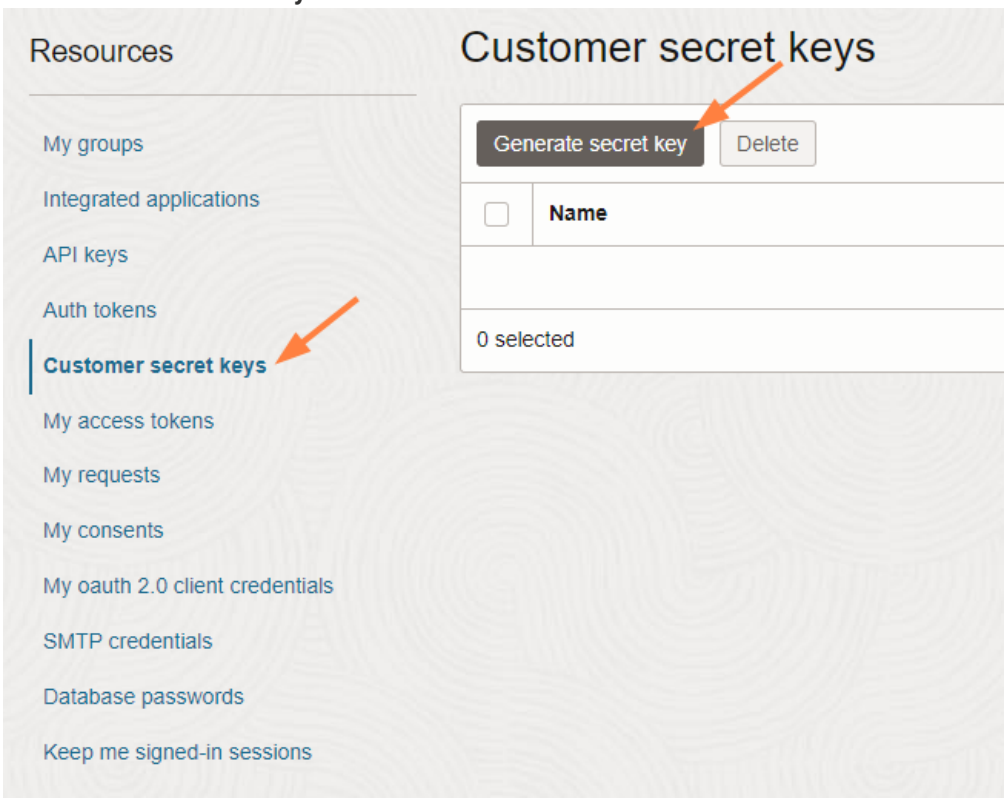


10. In the upper-right of the OCI screen, click the profile icon and choose **My profile**.



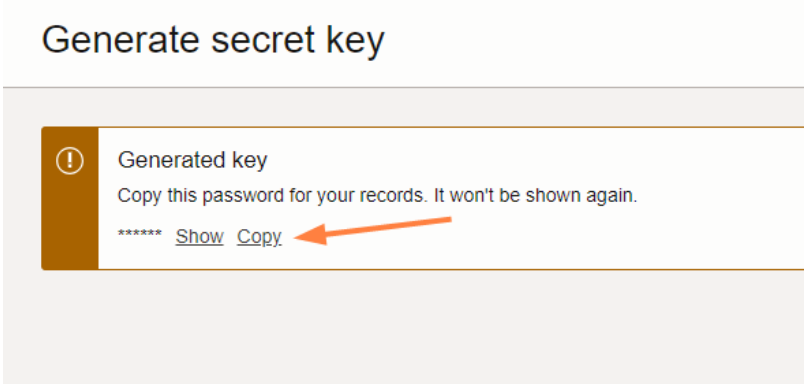
11. In the **My profile** screen navigation panel, scroll down to **Resources**, and click **Customer secret keys**.
    The **Customer secret keys** section opens.

12. Click **Generate secret key**.



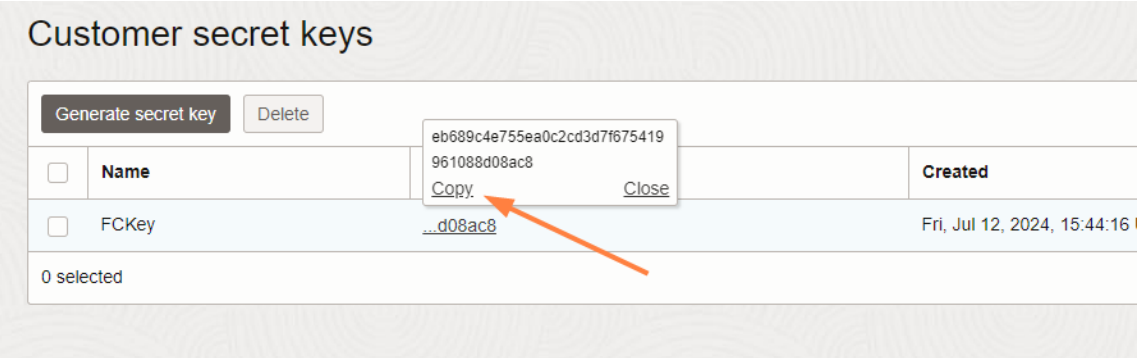
The screen confirms that the secret key was generated and prompts you to copy and save it.

13. Copy and save the secret key. You will use it for the value of **S3 Secret** in the next procedure.



It is now listed in the list of secret keys.

14. Hover over the value in the **Access key** column and copy and save the key. You will use it for the value of **S3 Key** in the next procedure.



To integrate FileCloud and OCI

1. Enable OCI cloud object storage

NOTES:

Although FileCloud does not have an explicit connector for OCI object storage, the Amazon S3 connector can be used.

In this step you will need to access **WWWROOT.** It is typically located at:

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To enable OCI cloud object storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server.
   b. Synchronize Time with NTP in Linux.
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

```
WWWROOT/config/amazons3storageconfig.php
```

8. Open **amazons3storageconfig.php** and find the line:

```
//define("TONIDOCLOUD_S3_USE_PATH_STYLE_ENDPOINT", 0 );
```

9. Uncomment it, and change the value to 1:

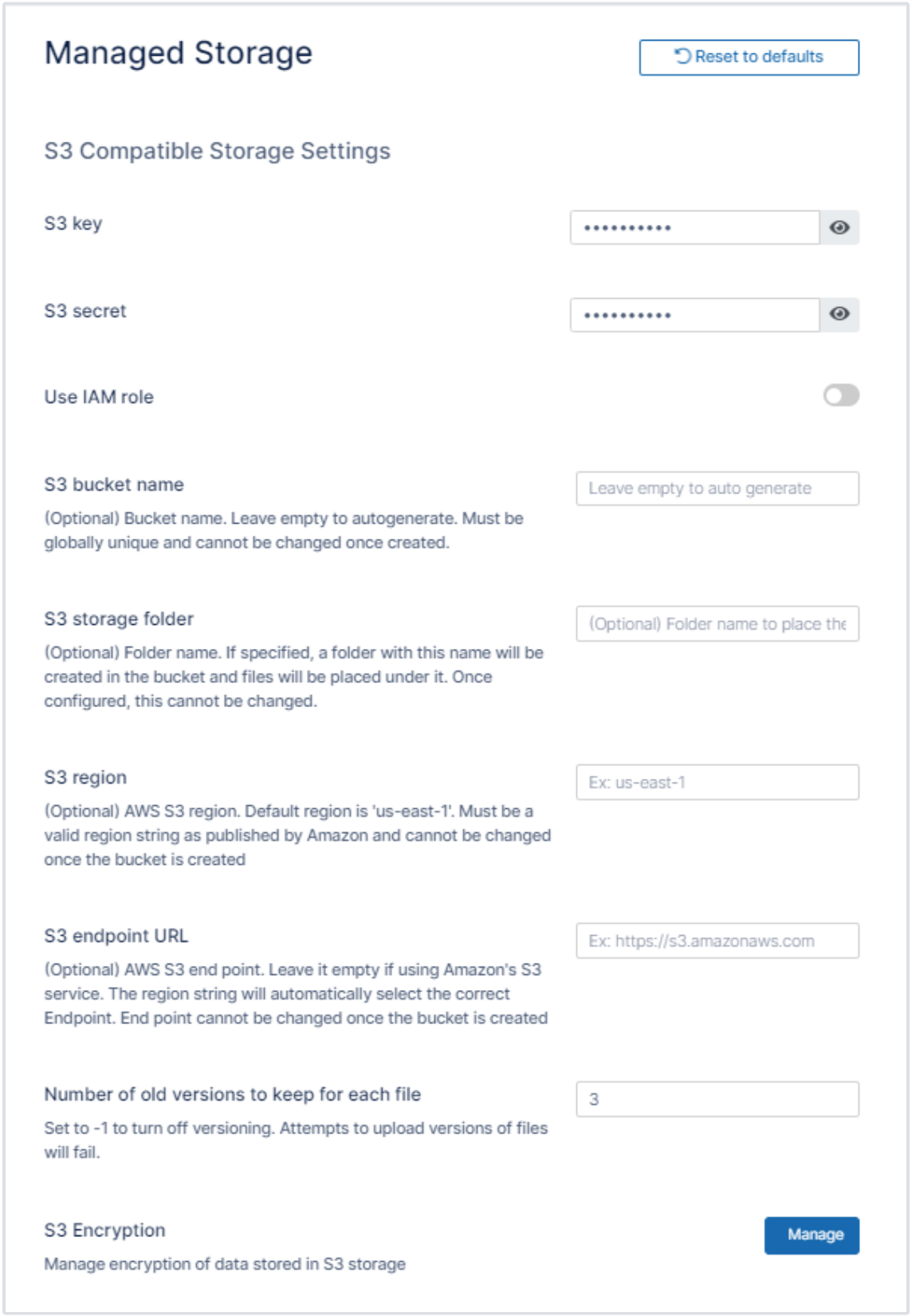
```
define("TONIDOCLOUD_S3_USE_PATH_STYLE_ENDPOINT", 1 );
```

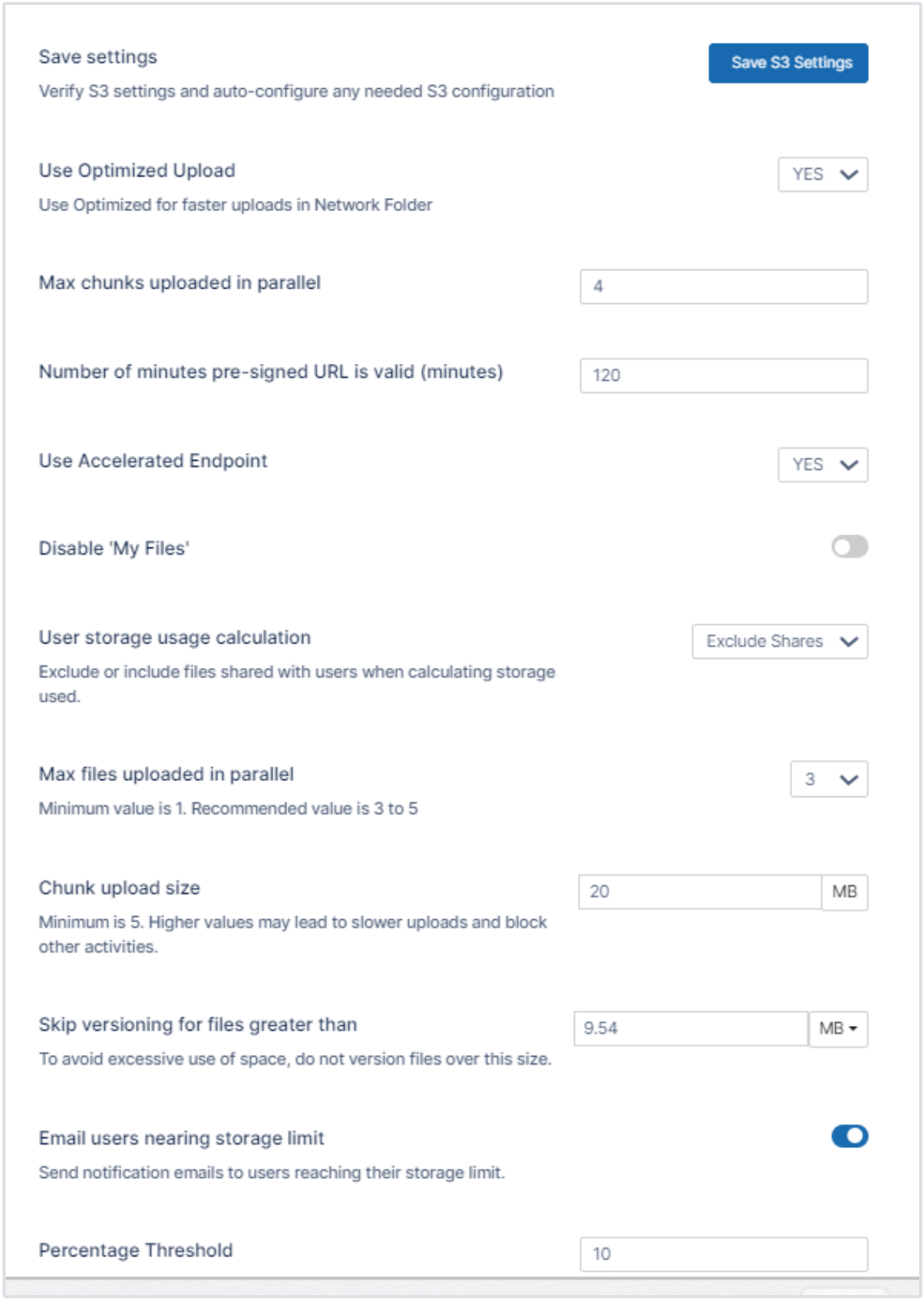
10. Save and close the file.

2. Configure Credentials in FileCloud for Managed Storage

To configure OCI object storage:

1. Open a browser and log into admin portal.
2. In the left navigation panel, click **Settings**.
3. On the **Manage Settings** screen, go to **Storage > My Files**.
4. Type in or select the settings for your environment. See the table below for information about each setting.


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
Leave empty to auto generate
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
(Optional) Folder name to place the
S3 region
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
Ex: us-east-1
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Ex: https://s3.amazonaws.com
Number of old versions to keep for each file
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
3
S3 Encryption
Manage encryption of data stored in S3 storage
Manage



5. Click **Save S3 Settings**.

Field	Description
S3 Key	Your OCI authentication key. Enter the **Access key** value generated in the OCI user interface.
S3 Secret	Your OCI cloud authentication secret. Enter the **Secret key** value generated in the OCI user interface.
Use IAM role	Leave unchecked.
S3 Bucket Name	Leave empty to autogenerate.
S3 Storage Folder	Leave empty.
S3 Region	Leave empty.
S3 End Point URL	Enter https://[namespace].compat.objectstorage.[region].oraclecloud.com For [namespace], use the **Namespace** value from the **Bucket** tab the in the OCI user interface. For [region], use the **Region Identifier** you located in the OCI user interface.

To fill in the other settings, see Setting up FileCloud Managed S3 Storage.

How to Integrate Filecloud with Storj

Administrators can change the FileCloud storage type after FileCloud has been installed but before any data has been stored.

- When changing the storage type from local to Storj S3-Compatible Object Storage, the files and folders that have been already stored in local storage will not be automatically moved to S3 storage.
- In this case, the administrator must manually export files and folders from local storage before changing the storage type, and then manually import them after changing the storage type.

- Only change the FileCloud storage type for new installations.
- Do not change the FileCloud storage type if FileCloud has been in use and data is already stored.
- Be careful when changing the storage path; If done improperly it could lead to data loss.
- Storj S3-Compatible Object Storage should NEVER be modified outside of FileCloud.

- Do not add, edit, or modify files directly using Storj tools. Doing so will destabilize your FileCloud installation.

To change the FileCloud storage path from LOCAL to Storj:

1. Enable Storj S3-Compatible Object Storage

NOTES:

Although FileCloud does not have an explicit connector for Storj, the Amazon S3 connector can be used.

In this step you will need to access WWWROOT. It is typically located at:

Windows	Linux
c:\xampp\htdocs	/var/www/html

To enable Storj as backend storage:

1. To ensure that your server's time does not vary, set it up to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:

```
WWWROOT/config/cloudconfig.php
```

3. Find the following line:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
```

4. Change it to:

```
define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
```

5. Save and close the file.
6. Find the following file:

```
WWWROOT/config/amazons3storageconfig-sample.php
```

7. Rename it to:

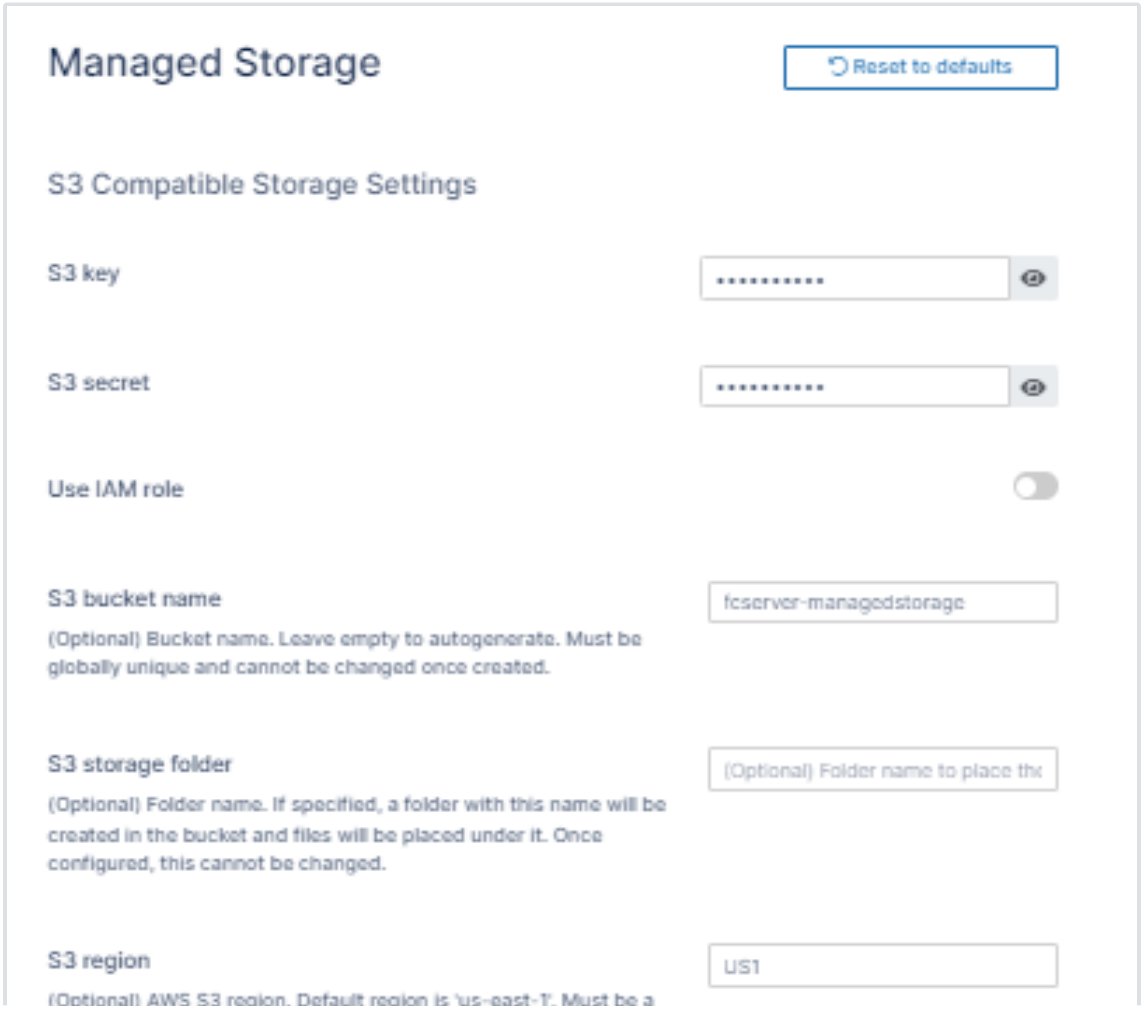
```
WWWROOT/config/amazons3storageconfig.php
```

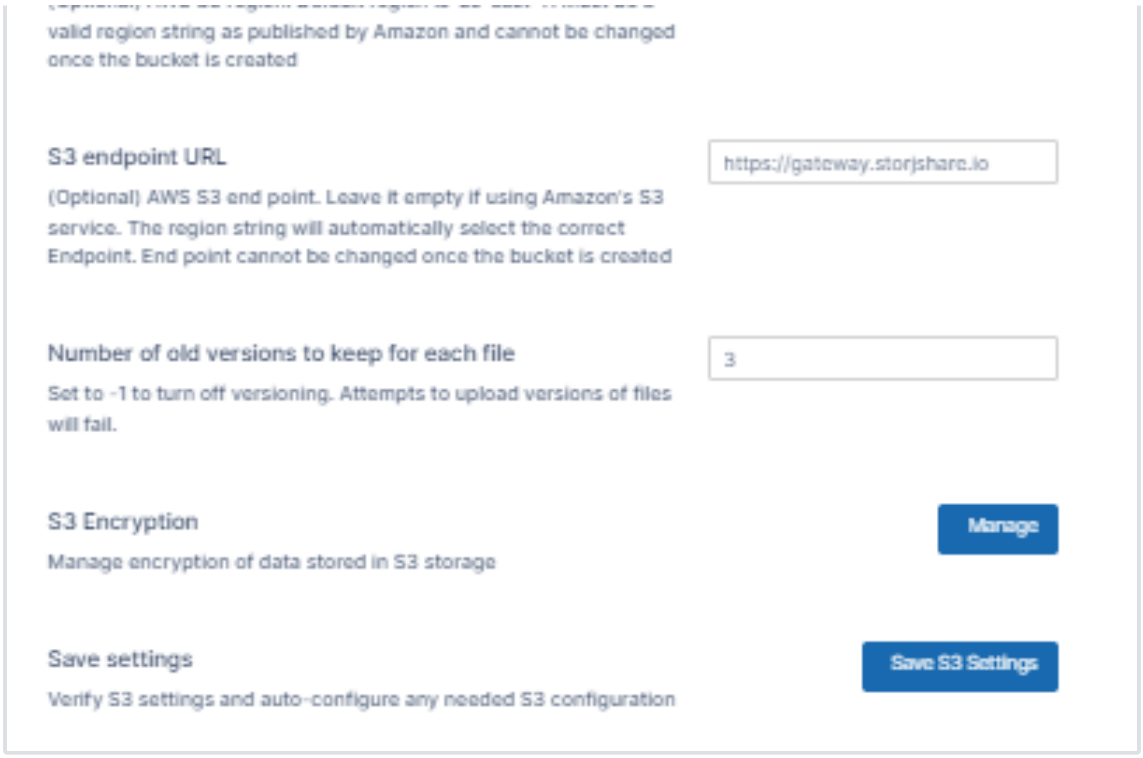
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure FileCloud to access the Storj S3 bucket:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   The **Managed Storage** settings page opens by default.
2. Enter the settings for your environment. See the following table for information about each setting.





3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Storj authentication key.
S3 Secret	Your Storj authentication secret.
Use IAM role	Do not check; this option is not supported in Storj.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem. The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Leave blank. Not supported in Storj.
S3 Region	US1, EU1, or AP1
S3 End Point URL	https://gateway.storjshare.io

Field	Description
Number of old versions to keep for each file	Storj has a beta feature supporting versioning. See https://docs.storj.io/dcs/buckets/object-versioning for more information. In FileCloud, when a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** are kept. When set to **-1**, versioning is disabled and attempts to upload a version of a file fail.
S3 Encryption	Select **No Encryption** or **Amazon S3-Managed Key Encryption**. See https://docs.storj.io/learn/concepts/encryption-key for more information.

4. To fill in the remainder of the settings, see Setting up FileCloud Managed S3 Storage.

Setting up Managed Storage Encryption

Administrators can enable storage-level encryption supported by FileCloud.

Currently, encryption is supported only for:

- Managed Storage (local)
- Amazon S3 storage

Storage encryption for **OpenStack** is not supported yet.

FileCloud Server supports FIPS licenses.
Enterprises who are subject to FIPS regulations must install and run a FIPS-enabled operating system.
When using a FIPS-enabled license, FileCloud Admins will see in the Admin Portal:

- A running in FIPS mode banner is displayed
- SSO features are hidden
- The storage encryption option is always available

What do you want to do?

Read more about Storage Encryption Technical Details

Enable Storage Encryption

Disable Storage Encryption

Activate Password-Protected Storage Encryption

Activate Encrypted-Protected Storage from the Command Line

Storage Encryption Technical Details

When you enable FileCloud storage encryption properly, all existing files in FileCloud managed storage will be encrypted before the system will be ready for use.

This topic describes:

- How a Plain File Key is Created
- Technical Details about Encryption Keys
- When are Files Encrypted?
- When are files Decrypted?

How a Plain File Key is Created

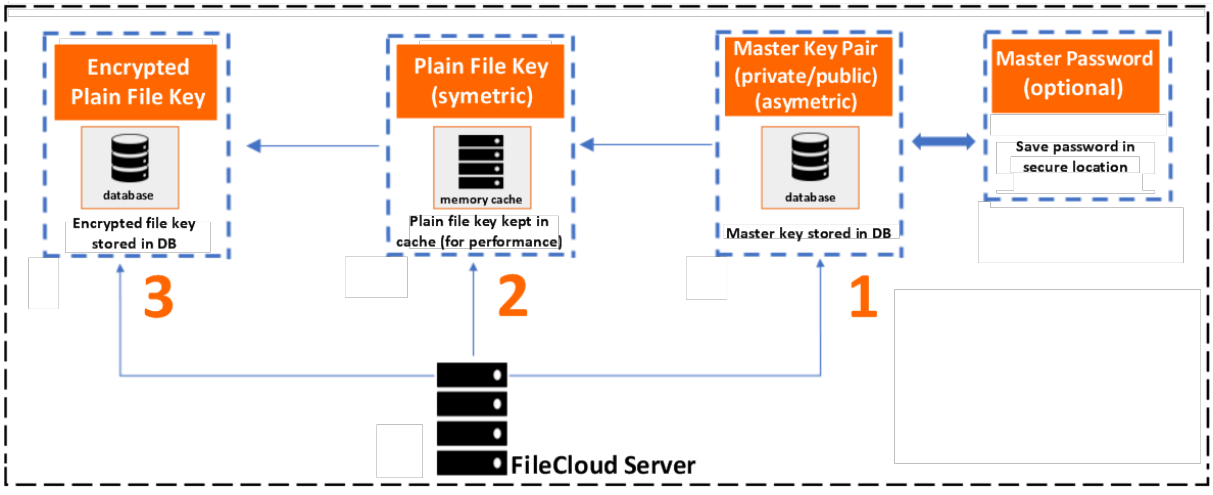
After you enable encryption, the initialization process begins so that a plain file key can be created.

- A plain file key will be used to encrypt and decrypt all files using symmetric encryption
- If you set a password when you enable encryption, you will need to supply the master password before the initialization process can start

Warning On Master Password
If an optional master password was specified, then you need to retain the password for future use. Without this password the encryption module cannot encrypt or decrypt files in the FileCloud storage.

Once FileCloud starts the initialization process, the plain file key is created as described in Figure 1.

Figure 1. How a Plain File Key is Created



1. An asymmetric key pair (private/public) known as the ***Master*** *key* is generated. (If the optional master password is specified it is also used.)
2. A symmetric key known as the ***Plain File*** *key* is generated.
3. The *Plain* ***File*** *key* (created in step 2) is encrypted using the **Master private** key. This step creates an ***Encrypted Plain File*** *key*.

Any existing unencrypted files in the FileCloud storage will be encrypted before the system will be ready for use.

After restarting the server, you must type in the master password for encryption to work properly.

Technical Details about Encryption Keys

Additional details on the keys:

Key	Key Details	User Input	Persistence	Remarks
Master public/ private key pair	• Asymetric • 4096 bits • RSA • sha512 digest	Password (optional)	Both private and public keys are persisted	• It is important to save the password (if one was provided)
Plain File Key	• Symetric • AES • 256 bits	None	Not persisted	• The plain file key will be used to encrypt decrypt all files using symmetric encryption • This key will not be persisted but will be cached for performance • The cache will be valid for the lifetime of the FileCloud server process

Key	Key Details	User Input	Persistence	Remarks
Encrypted File Key	• Encrypted using master public key	None	Encrypted file key is persisted	• Decryption of the encrypted file key results in plain file key • Decryption of the encrypted file key will be done using the master private key and optional master password • The plain key that is a result of decryption process is cached for the lifetime of the FileCloud server process 💡 Whenever you restart the server, the encrypted file key is decrypted again.

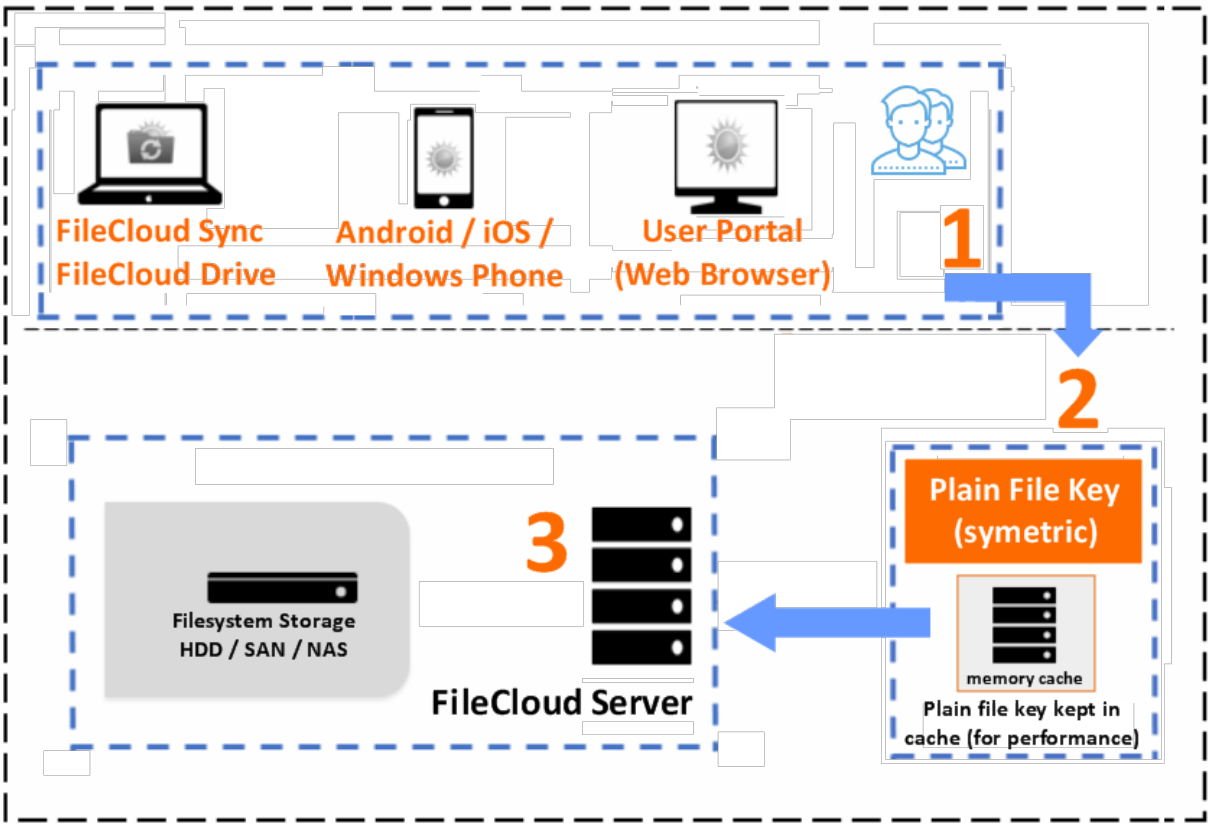
When are Files Encrypted?

Once the storage encryption is enabled and the plain file key is generated, it will be automatically used to encrypt all files stored in the FileCloud.

- Since this encryption process is a symmetric operation, the impact on your system to encrypt files is insignificant.

The file encryption process is described in Figure 2.

Figure 2. How Files Are Encrypted



1. A FileCloud user uploads a new file to the server.
2. The plain file key is looked for in the local key cache.
    a. If the key is not found, a decryption process will be started to decrypt the plain file key from the encrypted file key (which is stored in the database).
    b. For this decryption process the master private key and the optional master password will be used.
    c. At the end of decryption, the plain file key will be cached.
3. If the key is found, the plain file key will be used to symmetrically encrypt all incoming files.

When storage encryption is enabled, it will run when any of the following events occur:

- When a new file is uploaded completely
- When a thumb is created
- When a slide image is created
- When a slide image is rotated
- When a request to encrypt all existing plain files is initiated

When are Files Decrypted?

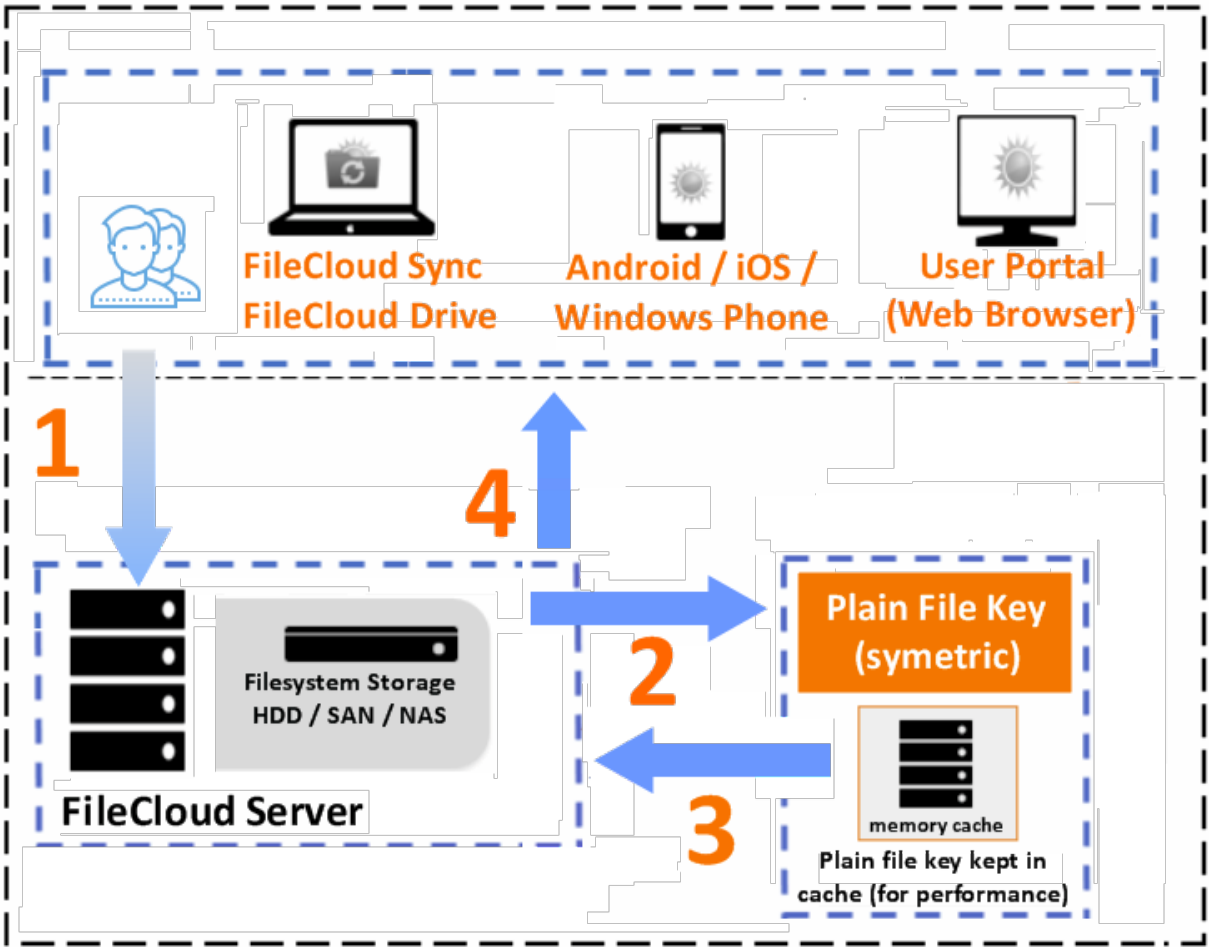
Storage decryption will occur without notifying the end user.

This means that:

- Decryption will automatically happen every time a file is accessed
- Decryption will occur without any additional steps to perform

The file decryption process is described in Figure 3.

Figure 3. How Files Are Decrypted



1. A FileCloud user requests to download a file from the server.
2. The plain file key is looked for in the local key cache.
    a. If the key is not found, a decryption process will be started to decrypt the plain file key from the encrypted file key (which is stored in the database).
    b. For this decryption process the master private key and the optional master password will be used.
    c. At the end of decryption, the plain file key will be cached.
3. If the key is found, the plain file key will be used to symmetrically decrypt an encrypted file.

4. The file is downloaded to the user's client computer or device.

When storage encryption is enabled, decryption will run when any of the following events occur:

- When a file is downloaded.
- When a thumb nail is downloaded.
- When a slide image is downloaded.
- When a document preview is requested.

Enabling Storage Encryption



If a FIPS-enabled FileCloud license is installed, there is an option in the Admin Portal to enable FileCloud to run in FIPS mode.

As an administrator, you can encrypt managed disk storage for compliance and security reasons.

To enable storage encryption:

1. Encryption Prerequisites

Before you can enable encryption, you must meet the following requirements:

Requirements	
Required	Memcached installation
Only required if the default path for openssl.cnf has been changed.	Set a custom path to the SSL configuration file by overriding the config value of **SSL_CONF_FILE** in cloudconfig.php. By default, **SSL_CONF_FILE** is set to **Windows: XAMPP_HOME\php\extras\ssl\openssl.cnf** **Linux: /etc/ssl/openssl.cnf** In Windows, for example, if XAMPP is installed in D:\xampp, add the following line to cloudconfig.php. **define("SSL_CONF_FILE","D:\\xampp\\php\\extras\\ssl\\openssl.cnf");**

2. Enable the Encryption Module

By default, the encryption module is not enabled.

You can enable the encryption module in two ways:

- If FIPS mode is active:
  In order to ensure FIPS mode is on, enable the FIPS Admin Banner by accessing (**WEBROOT/config/localstorageconfig.php** file) and adding the following:
  define("TONIDOCLOUD_FIPS140_ENABLED", 1);

Note: When enabling FIPS mode, you must also enable managed storage encryption. See Step 3 that follows.

- If you don't use FIPS mode:
  Edit the **WEBROOT/config/localstorageconfig.php** file.
  Add the following line:

  Additional Parameter To Enable Encryption

```
define("TONIDO_LOCALSTORAGE_INCLUDEENCRYPTION", 1 );
```

  where:

Parameter	Expected Value	Additional Notes
TONIDO_LOCALSTORAGE_INCLUDEENCRYPTION	1	1 - enable encryption for local managed storage 0 - disable encryption

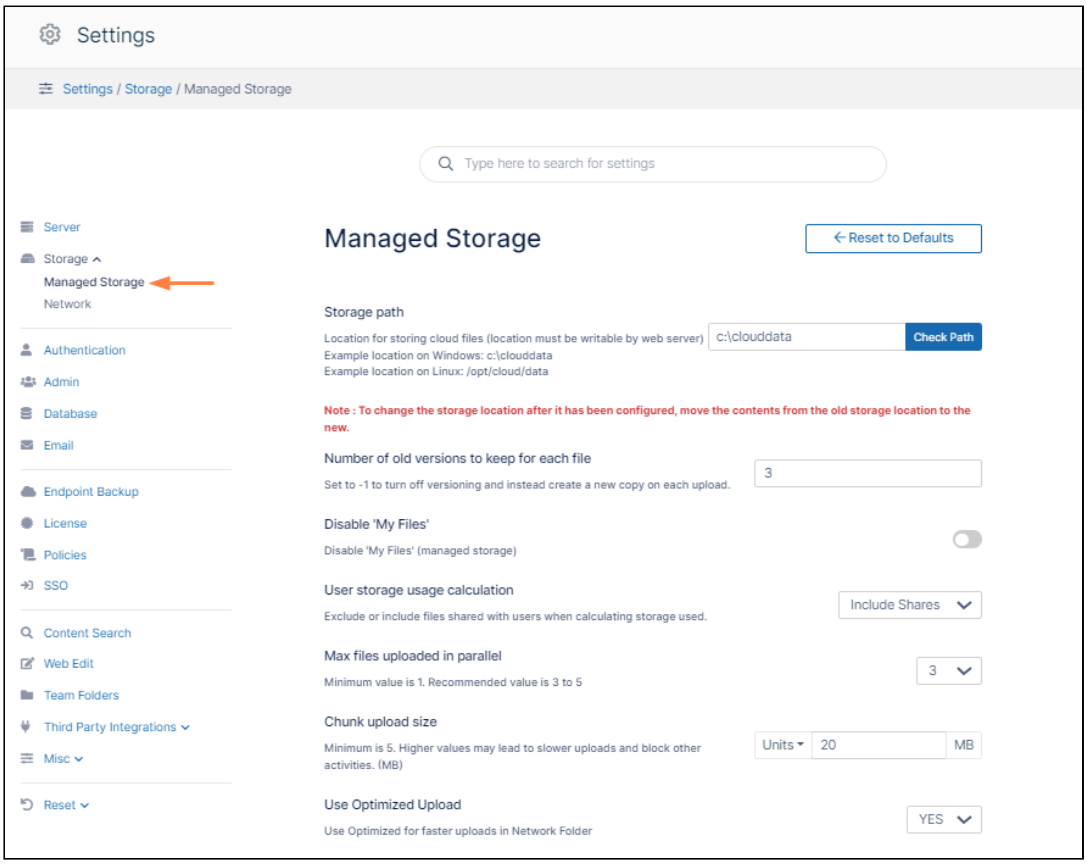
3. Manage Storage Encryption

After you enable the encryption module, the admin portal displays the encryption option.

Encryption Password
If an optional encryption password is specified, store it securely for future use.
Without this password, the encryption module cannot encrypt or decrypt files in FileCloud storage.

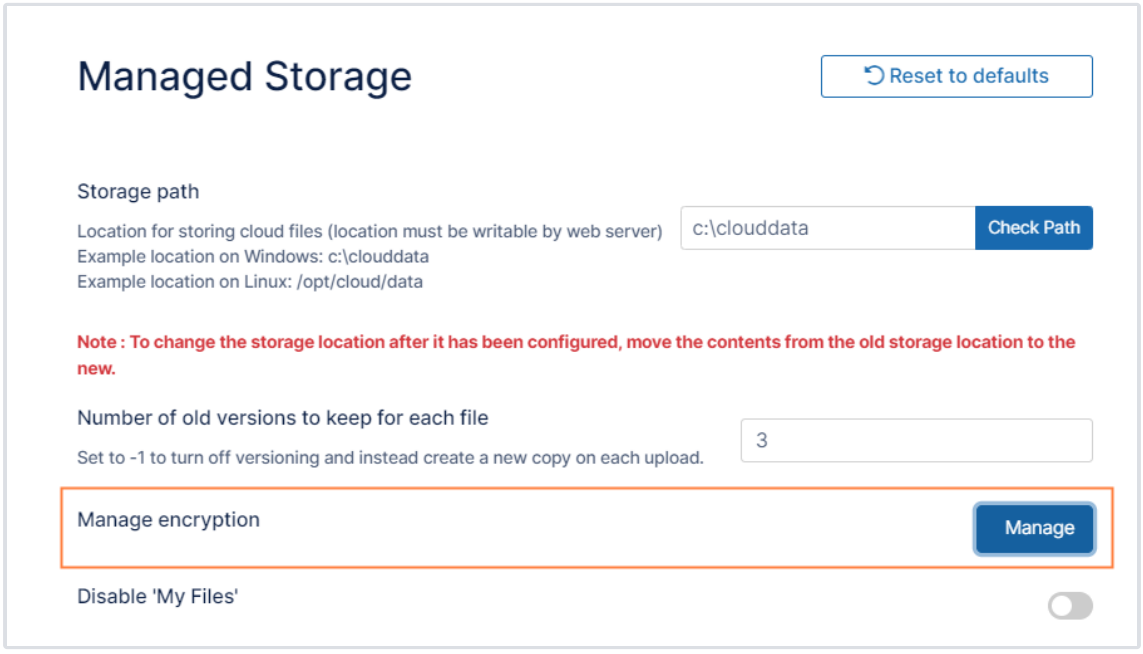
To manage encryption:

1. Open the **Managed Storage** settings page.
   To go to the Managed Storage settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   b. In the inner navigation bar on the left of the **Storage** settings page, expand the **Storage** menu, and click **Managed Storage**, as shown below.



The **Managed Storage** settings page opens.

The **Managed Storage** settings now include a **Manage Encryption** option.



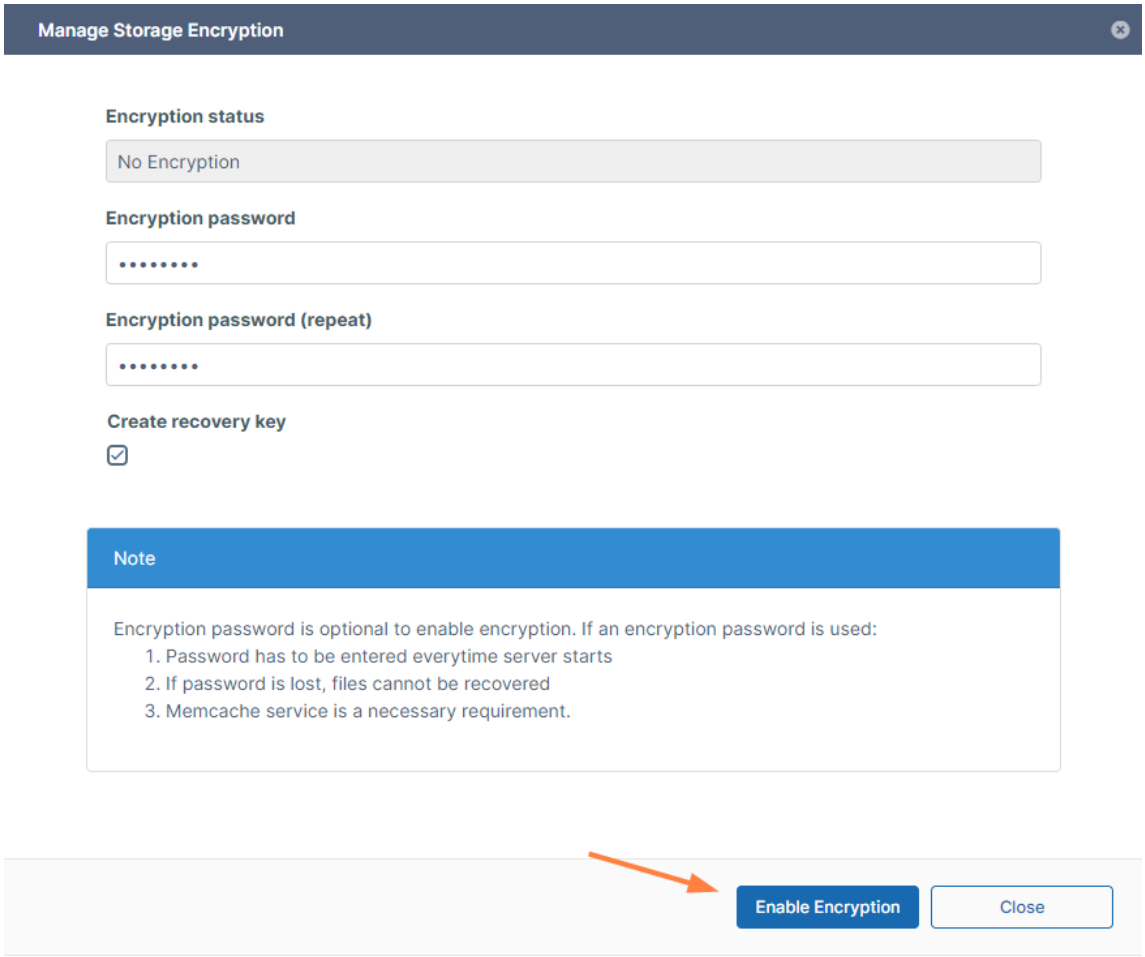
2. To open the **Manage Storage Encryption** dialog box, click **Manage**.
3. To set an optional password, in **Encryption password**, enter a strong password.

4. To create a recovery key, check **Create recovery key**.

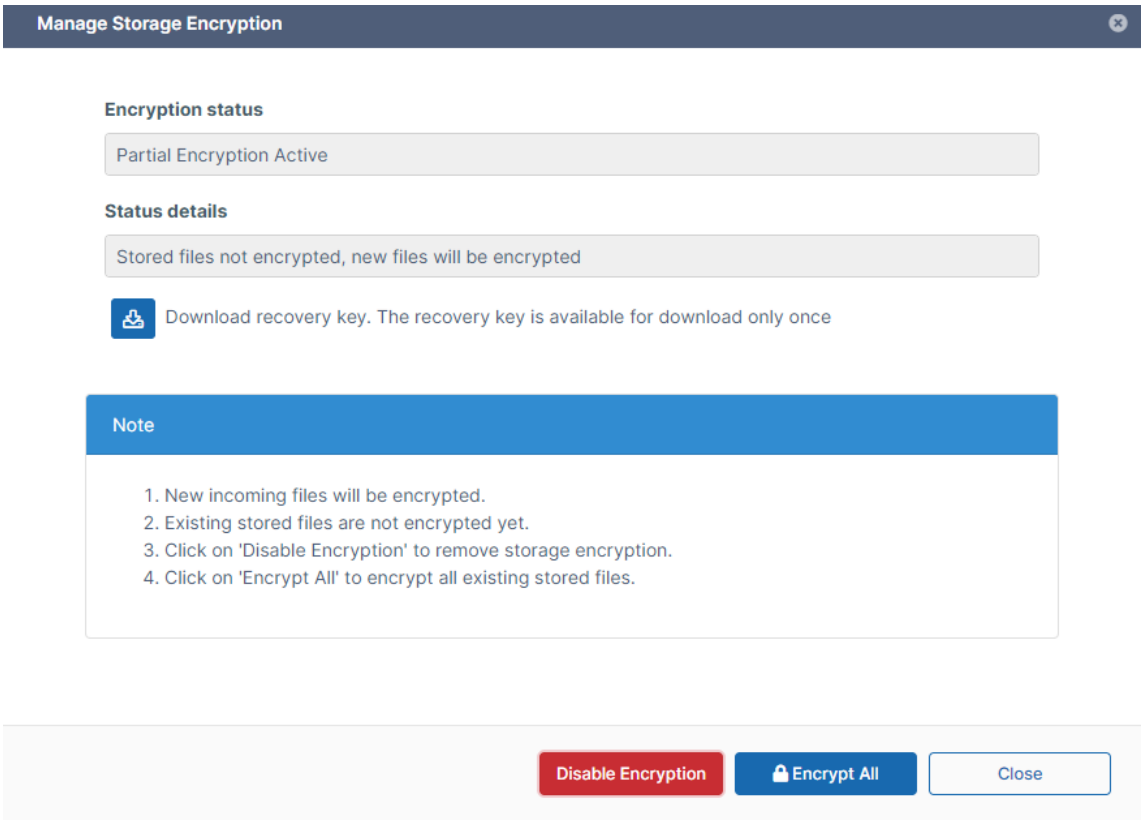
   The recovery key is a private key file that can be used to reactivate the encrypted filesystem in the case of a lost password.

   If the recovery key option is selected, **the recovery key file becomes available for download only once**.

5. To perform the necessary initialization of the encryption module, click **Enable Encryption**.



Now the **Encryption status** indicates that partial encryption is active. **Status details** indicates that files already stored in the system are not encrypted, but new files will be encrypted.



6. To save the recovery key, click the **Download recovery key** button and save it to your file system.

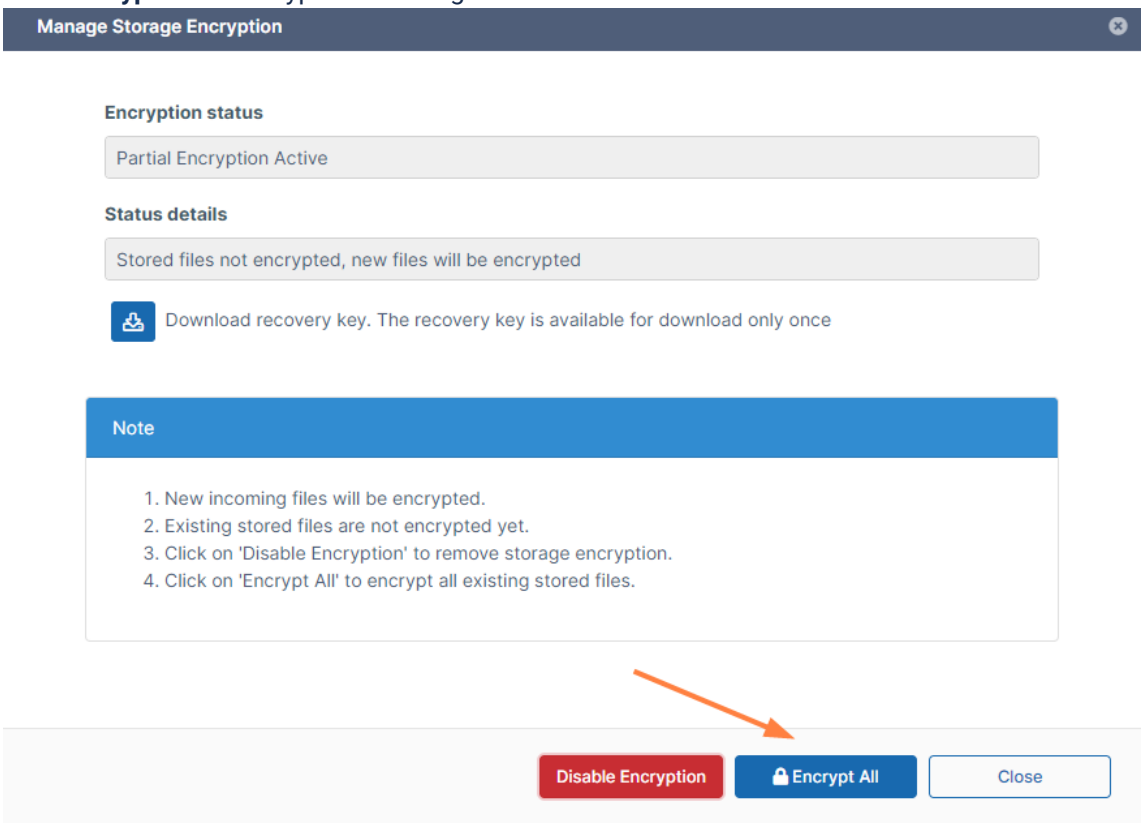
4. Encrypt any existing files

Once encryption is successfully initialized, another step is necessary if your FileCloud server had existing files in local storage.

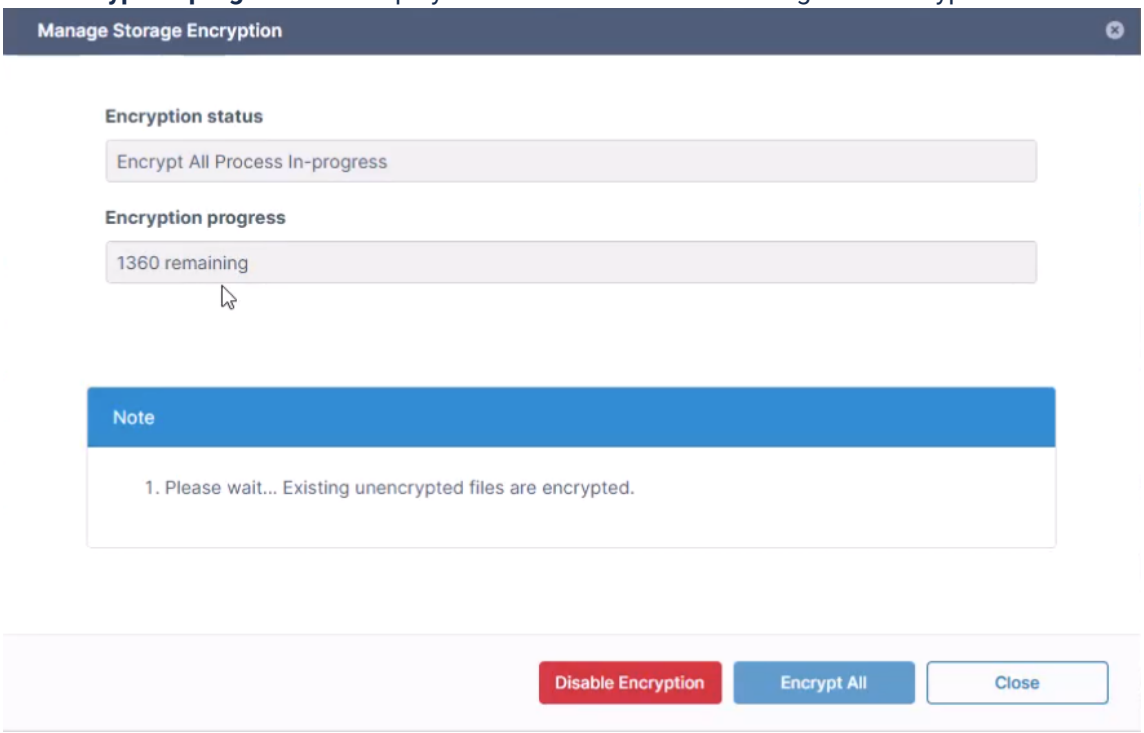
If your local storage already contains files:

If there are unencrypted files in the existing storage system, another screen is shown.

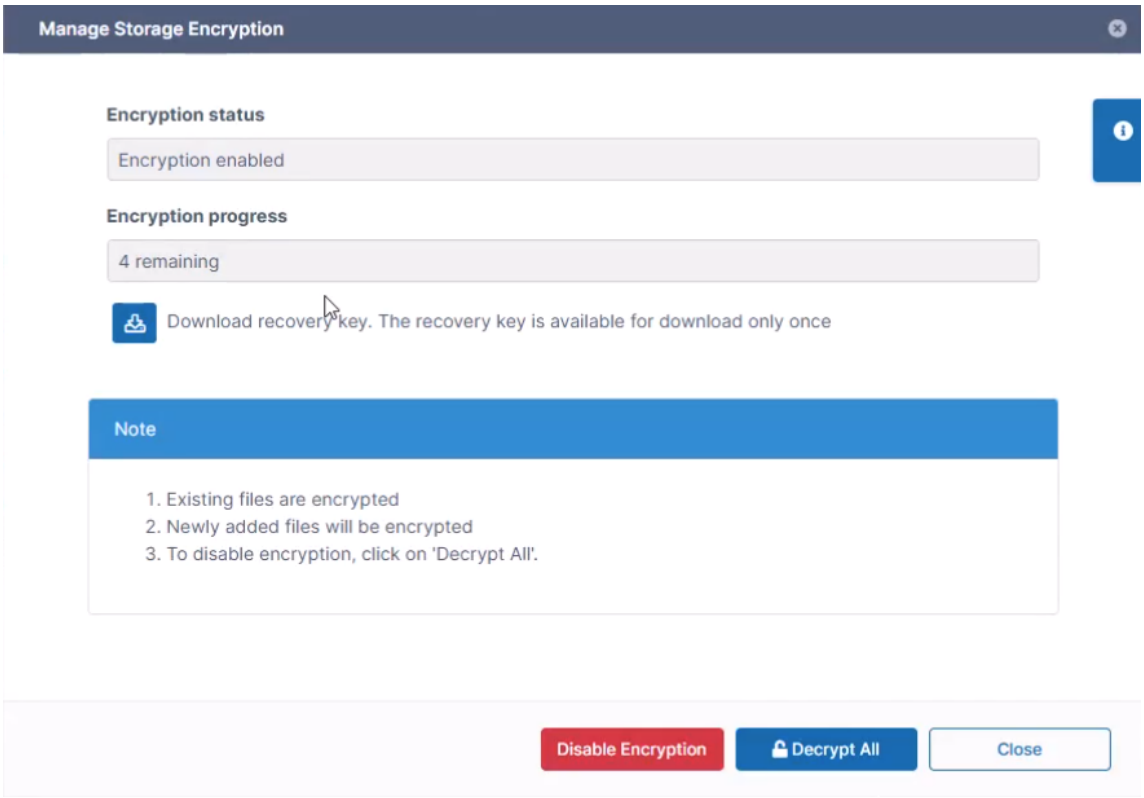
1. Click **Encrypt All** to encrypt the existing files.



The **Encryption progress** field displays the number of files remaining to be encrypted:



When all the existing files are encrypted, the Encryption status is **Encryption enabled**.



If your local storage doesn't contain pre-existing files:

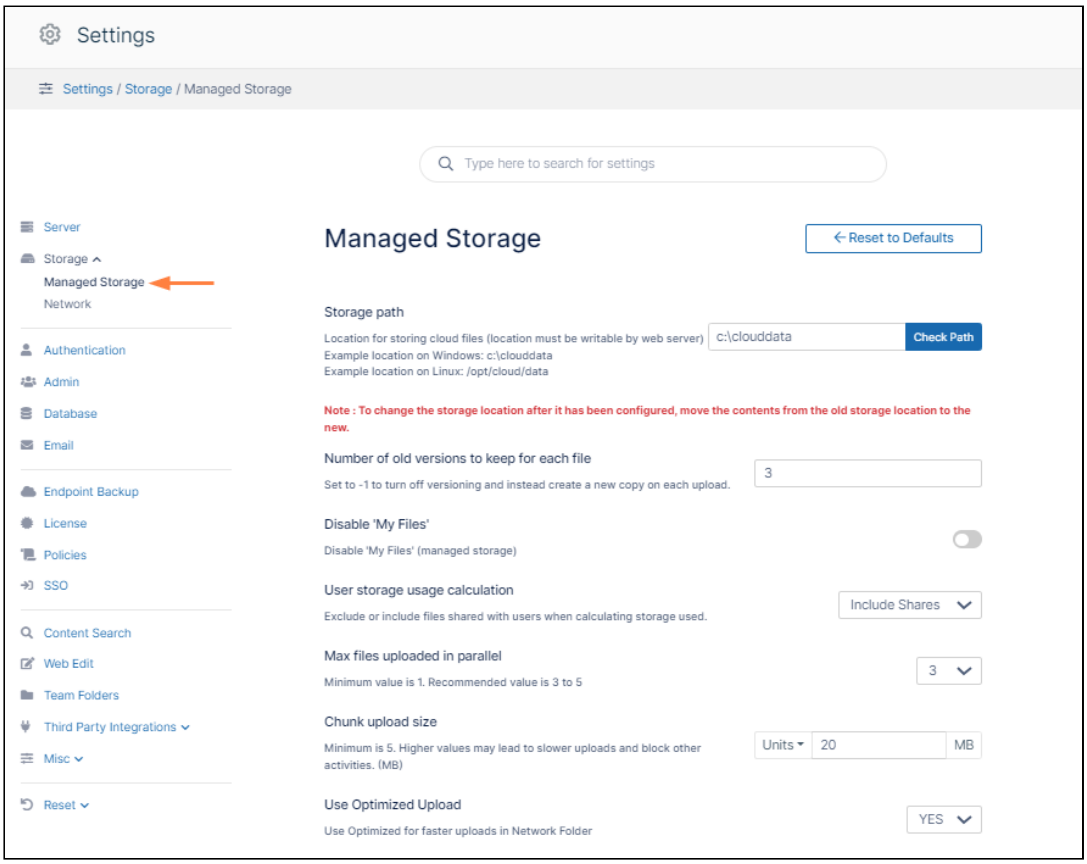
- You will not see an **Encrypt All** button.
- Your system is already in a fully-encrypted state.

Disabling Storage Encryption

Administrators can decrypt files and disable storage encryption following the steps here.

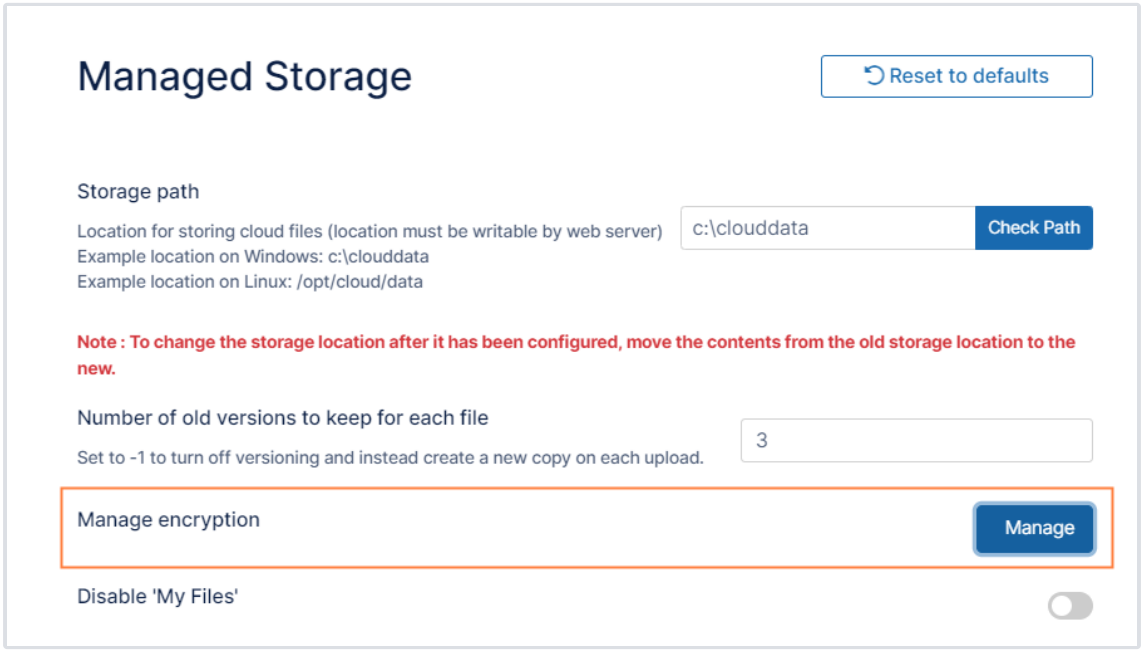
To decrypt files:

1. Open the **Managed Storage** settings page.
   To go to the Managed Storage settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   b. In the inner navigation bar on the left of the **Storage** settings page, expand the **Storage** menu, and click **Managed Storage**, as shown below.

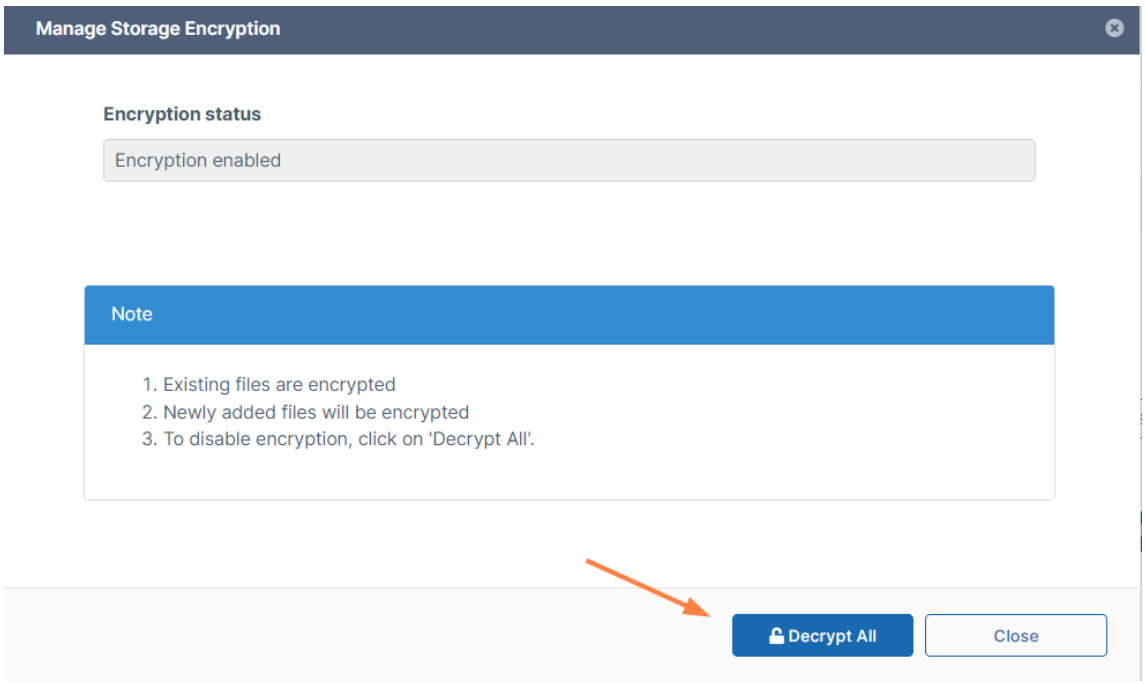


The **Managed Storage** settings page opens.

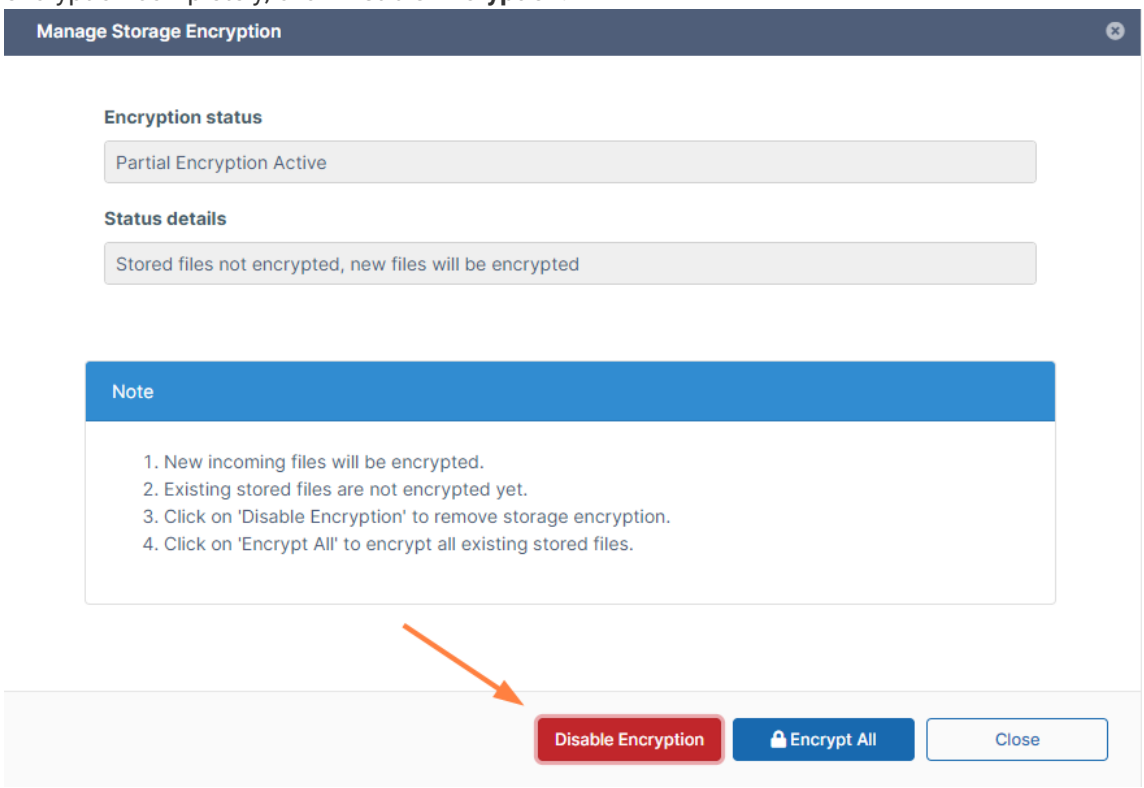
2. Next to **Manage encryption**, click **Manage**.



3. In the Manage Storage Encryption dialog box, click **Decrypt All**.

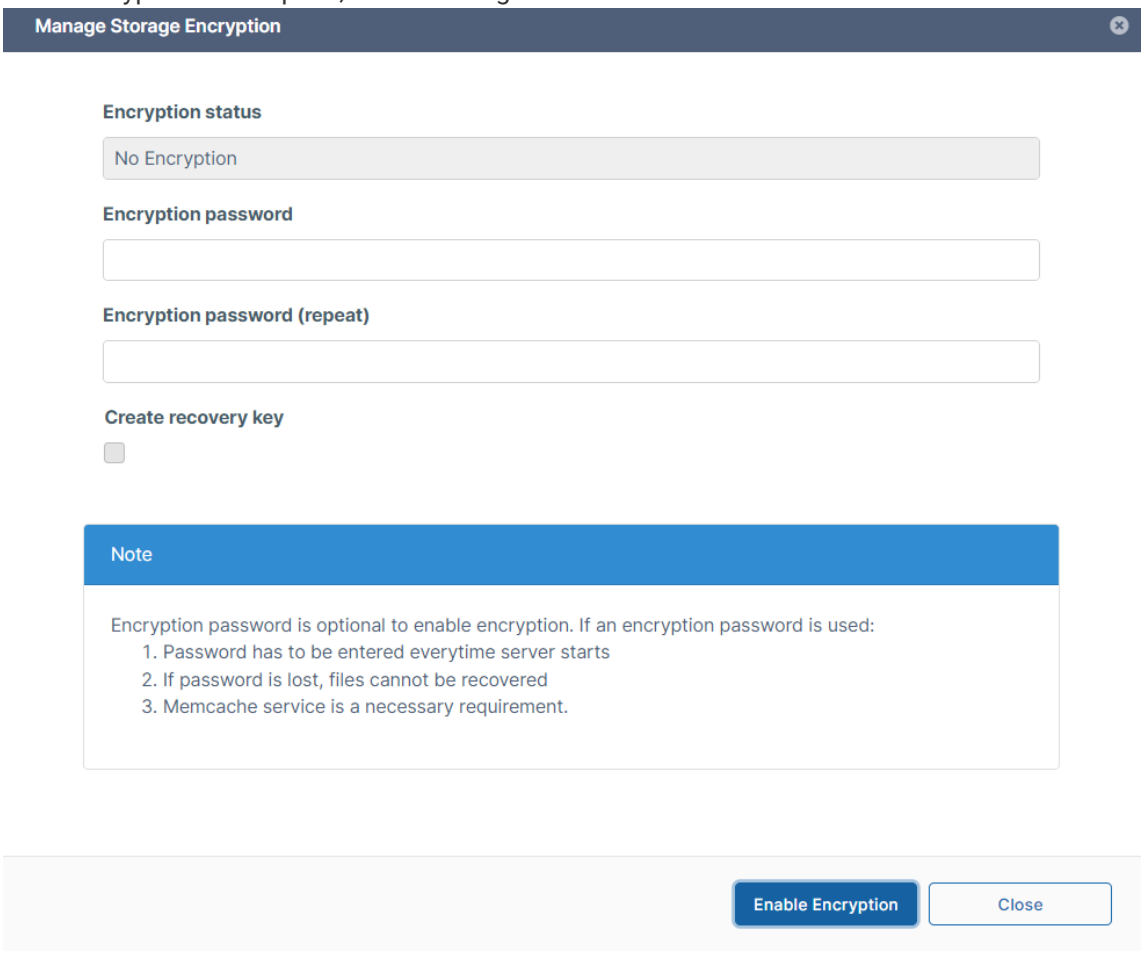


4. Now all the stored files are decrypted, but new files will continue to be encrypted. To disable encryption completely, click **Disable Encryption**.



The dialog box shows notifications that decryption is in progress.

Once decryption is complete, the following screen is shown.

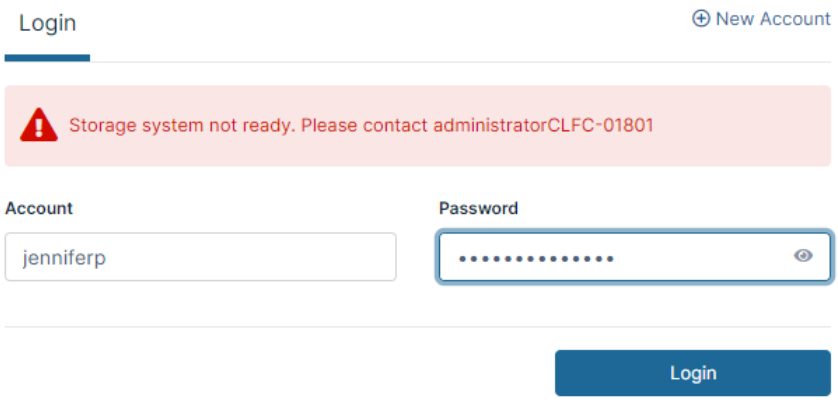


Activating Password Protected Storage Encryption

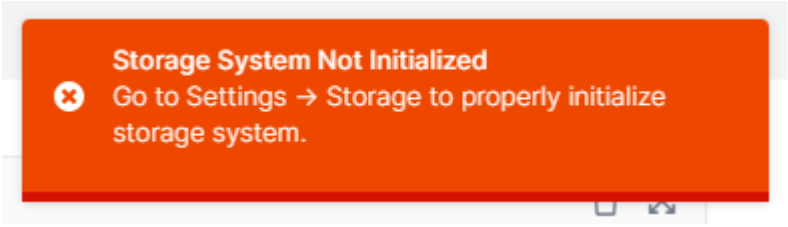
When FileCloud server is restarted, a password-protected encrypted storage system is not activated automatically. This design is for additional security, such that the encryption password is not stored on the same physical server.

If a user tries to log in to the user portal and the storage system is not activated, the user sees the

message:



When an admin logs into the admin portal and the storage system is not activated, the admin sees the pop-up notification:

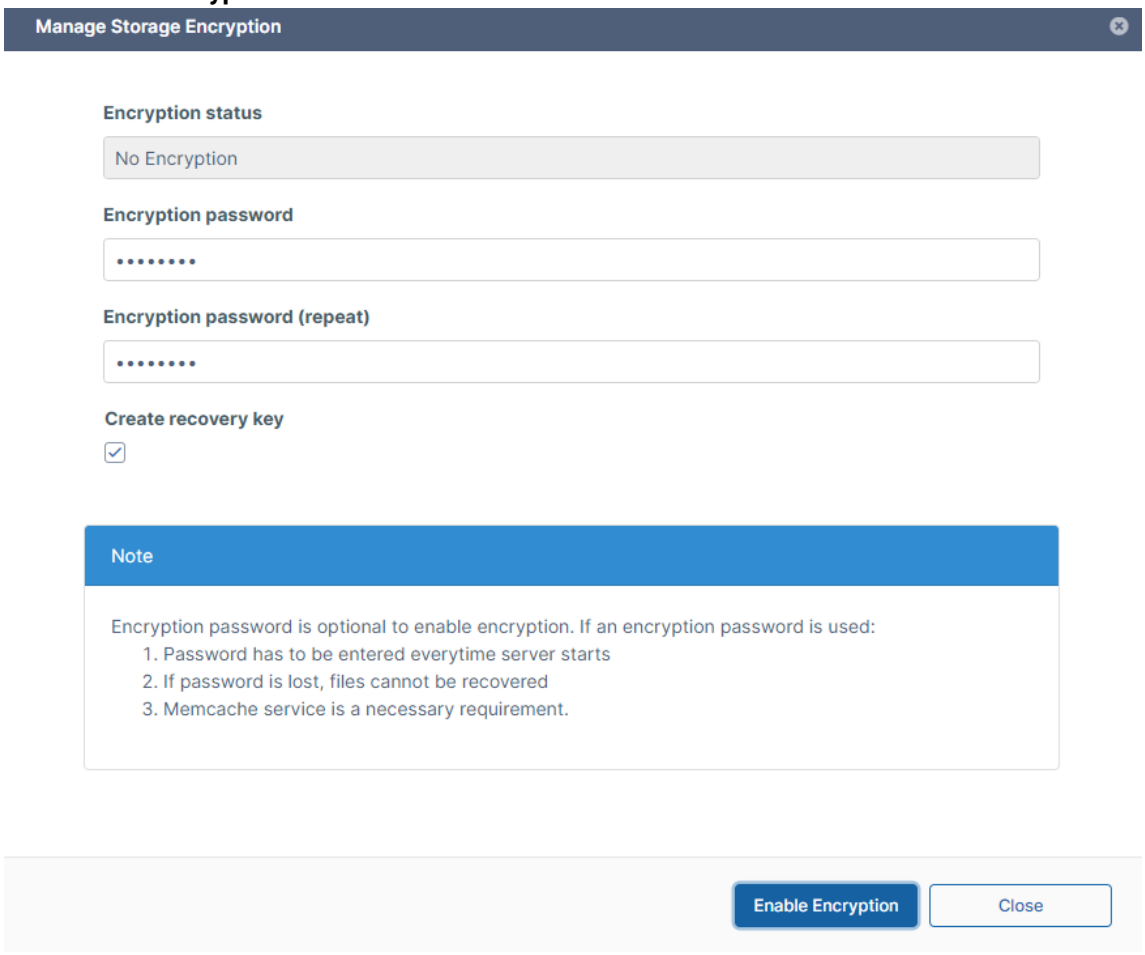


You can reactivate the storage system using the encryption password or the recovery key.

Activating with password and recovery key

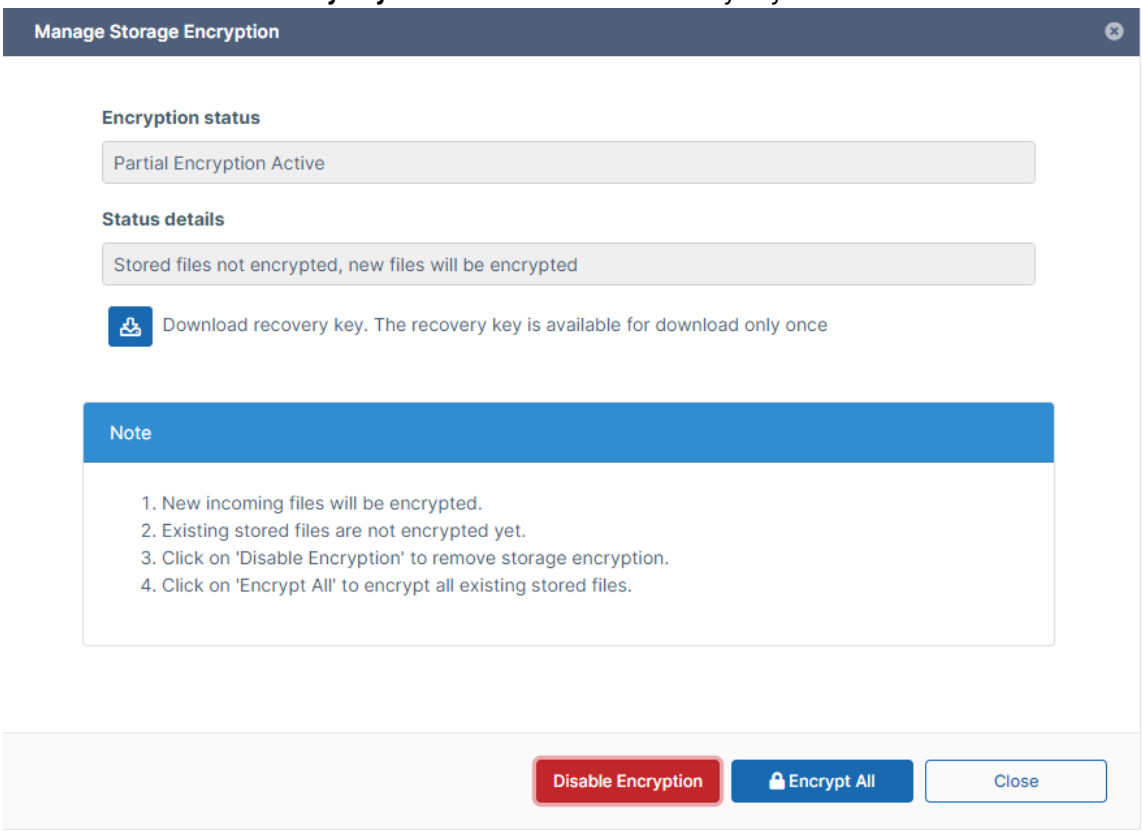
1. Enter the encryption password, in **Encryption password** and **Encryption password (repeat)**.
2. Check **Create recovery key**.

3. Click **Enable Encryption**.



The following screen appears.

4. Click the **Download recovery key** button and save the recovery key file.



5. Click **Encrypt All**.

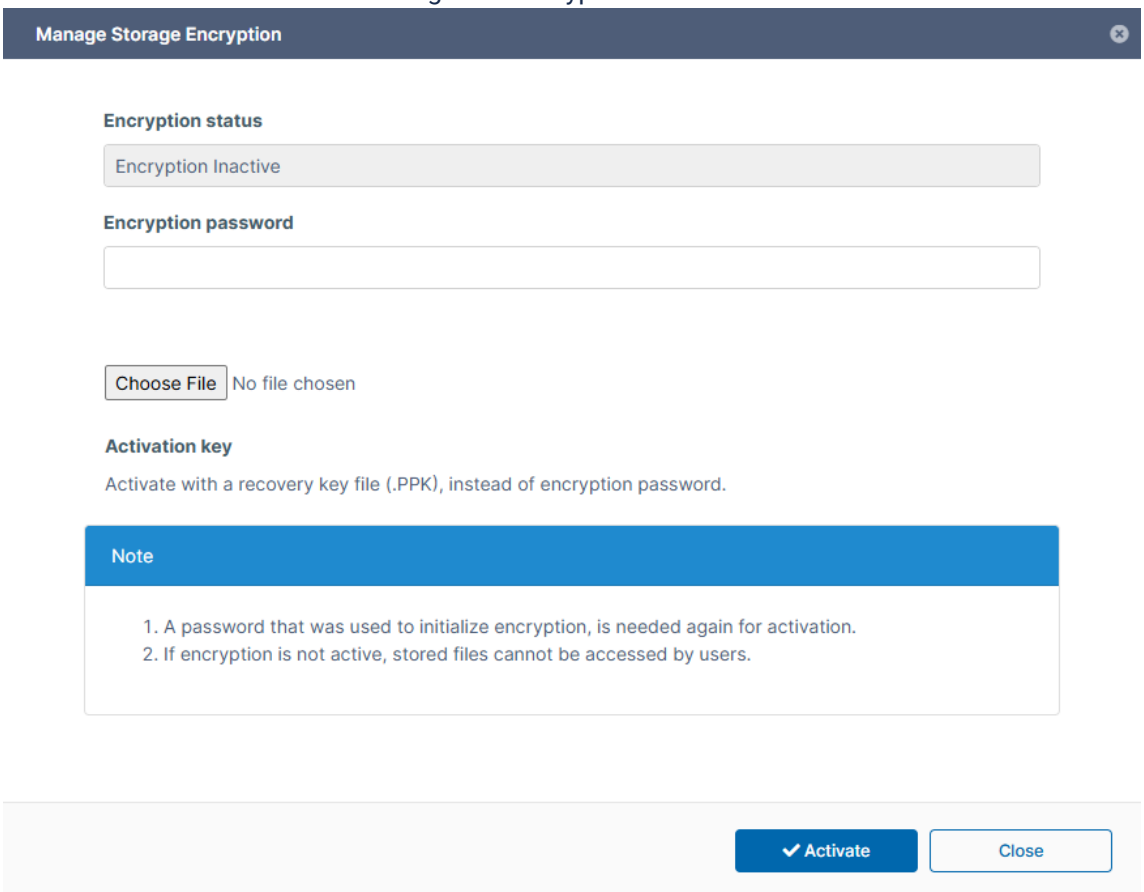
Activating With Recovery Key

> **Note**
> This option is available only when a recovery key was created during initialization.

After the full upgrade, if memcache service is down or stopped or any time you you restart memcache services, storage becomes inactive and encryption becomes inactive as well.
Use your password or recovery key to re-activate storage and encryption.

1. From the Manage Storage Encryption dialog box, either enter your encryption password or click **Choose File** and select your recovery key.

2. Then click **Activate** to activate storage and encryption.



Activating Encrypted Protected Storage From Command Line

When the FileCloud server restarts, password-protected storage encryption is not activated automatically. This design provides additional security by ensuring that the encryption password is not stored on the same physical server.

You can also activate FileCloud storage from the command line.

Prerequisites

Enable PHP CLI Mode
To run the following commands, PHP CLI mode must be enabled.
On Linux, edit the file /etc/php5/cli/php.ini and make sure the module mongo.so is enabled. Without this the reset password command will fail.
To enable mongo.so, add the following line at the end of file /etc/php5/cli/php.ini (if this line doesn't exist in the file)
extension=mongo.so
On Windows, the PHP CLI mode is already enabled in FileCloud installer.

Activating Storage

1. At the 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. To **activate storage with a password**, for both Windows and Linux, enter:
   In the following example, the command activates **site1.filecloud.com** using password **root01**.

   ```
   php activatesite.php -h site1.filecloud.com -p=root01
   ```

   To **activate storage on Linux using a recovery key**:
   In the following example, **for Linux only**, the command activates **site1.filecloud.com** using a recovery key.

   Activating Site From Command Line

   ```
   php ./activatesite.php -h site1.filecloud.com -r "/tmp/recovery.ppk"
   ```

Note
To activate default site, use -h default

Setting up Managed S3 Storage Encryption

FileCloud supports S3 storage-level encryption that administrators can enable.

FileCloud Server now supports FIPS licenses.
Organizations that must comply with FIPS regulations must install FileCloud server on a FIPS-enabled operating system.
When using a FIPS-enabled license, the Admin Portal:

- displays a banner indicating that the server is running in FIPS mode

- hides SSO features
- shows the Storage Encryption option

What do you want to do?

Enabling S3 Storage Encryption

Disabling S3 Storage Encryption

Read more about Choosing S3 Encryption Type

Enabling S3 Storage Encryption

In FileCloud, if a FIPS-enabled FileCloud license is installed, there is an option in the Admin Portal to enable FileCloud to run in FIPS mode.

As an administrator, you can encrypt Managed S3 Storage for compliance and security reasons

To enable storage encryption:

1. Encryption Pre-Requisites

Before you can enable encryption, you must meet the following requirements:

Order	Requirements
1	FileCloud Installation
2	Memcached installation
3	Path to SSL configuration file. This can be set to custom path by overriding the config value **SSL_CONF_FILE** in cloudconfig.php. By default, SSL_CONF_FILE is set to Windows: XAMPP_HOME\php\extras\ssl\openssl.cnf Linux: /etc/ssl/openssl.cnf In Windows, for example if you have XAMPP installed in D:\xampp, then you will be adding the following line to cloudconfig.php. **define("SSL_CONF_FILE","D:\\xampp\\php\\extras\\ssl\\openssl.cnf");**

Order	Requirements
5	For Windows, if your xampp is installed in location other than C:\xampp, then add the following key in <WWWROOT>\config\cloudconfig.php For example, if your xampp is in D:\xampp, then in file D:\xampp\htdocs\config\cloudconfig.php, add the following string (any location before the bottom "?>" line) **define("PHPBIN_PATH","D:\\xampp\\php\\php.exe");**

2. Manage Storage Encryption

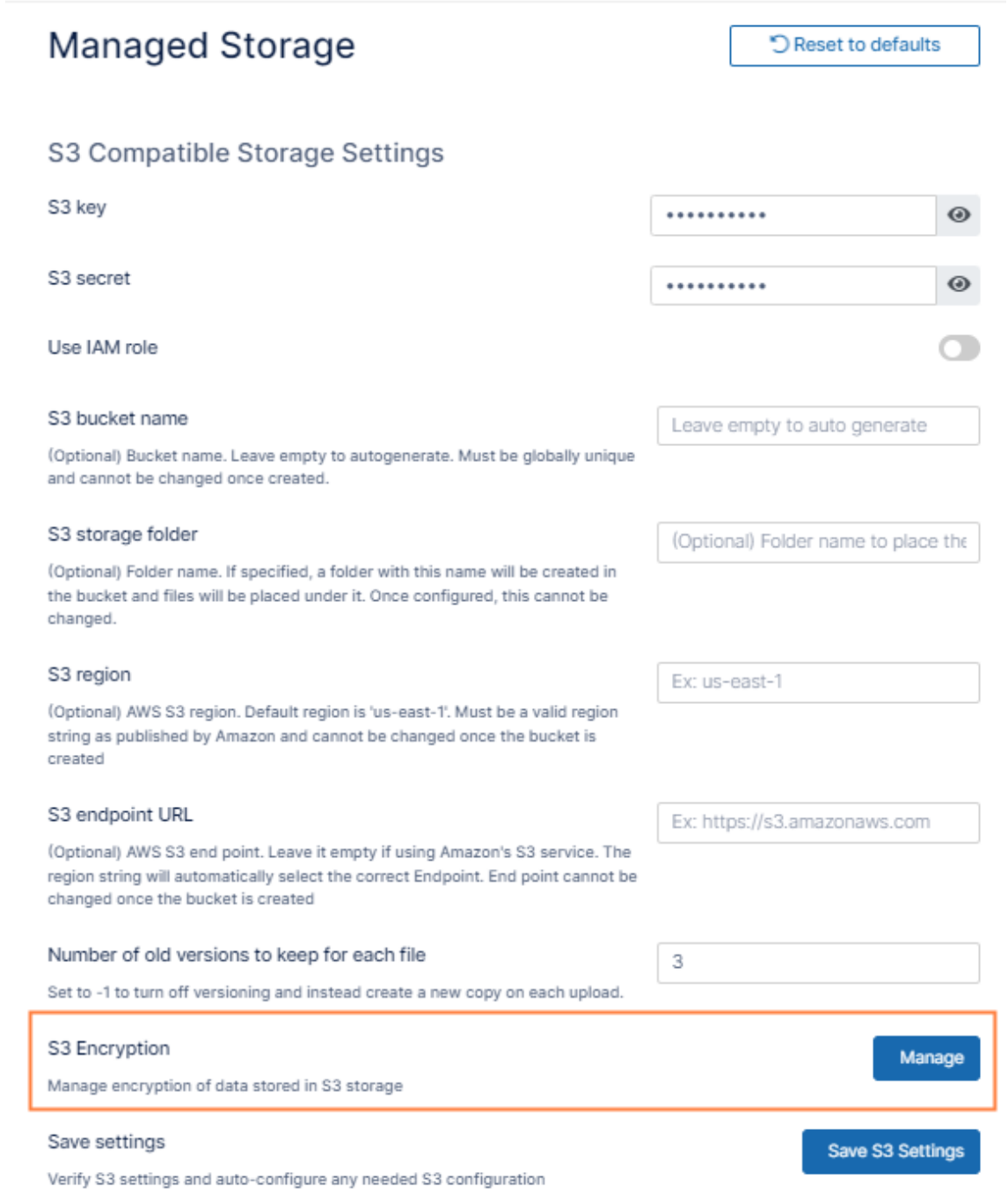
After S3 encryption is enabled, the Admin Portal will display new options for managing it.

Warning On Master Password
If an optional master password was specified, retain the password for future use.
Without this password the encryption module cannot encrypt or decrypt files in FileCloud storage.

To manage S3 encryption:

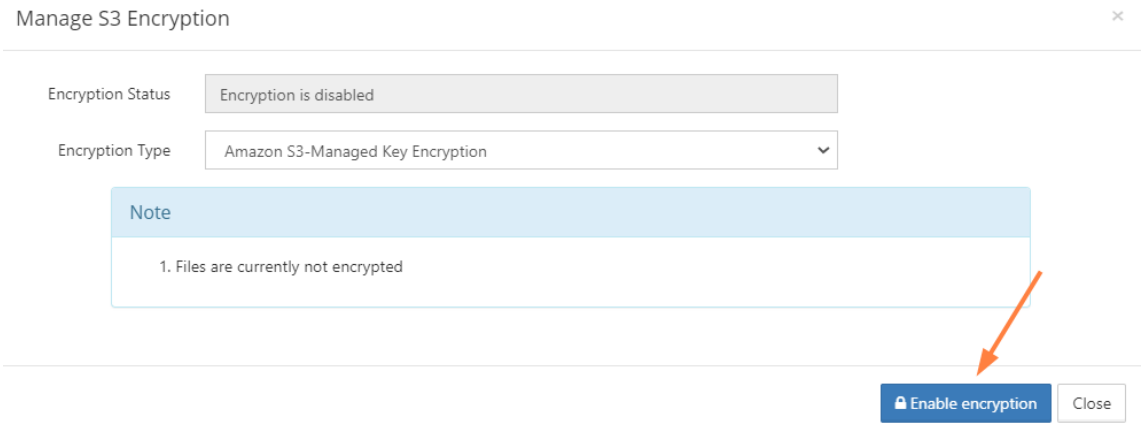
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The Managed Storage settings page opens. An **S3 Encryption** field with a **Manage** button appears.

2. To open the **Manage S3 Encryption** screen, click **Manage**.



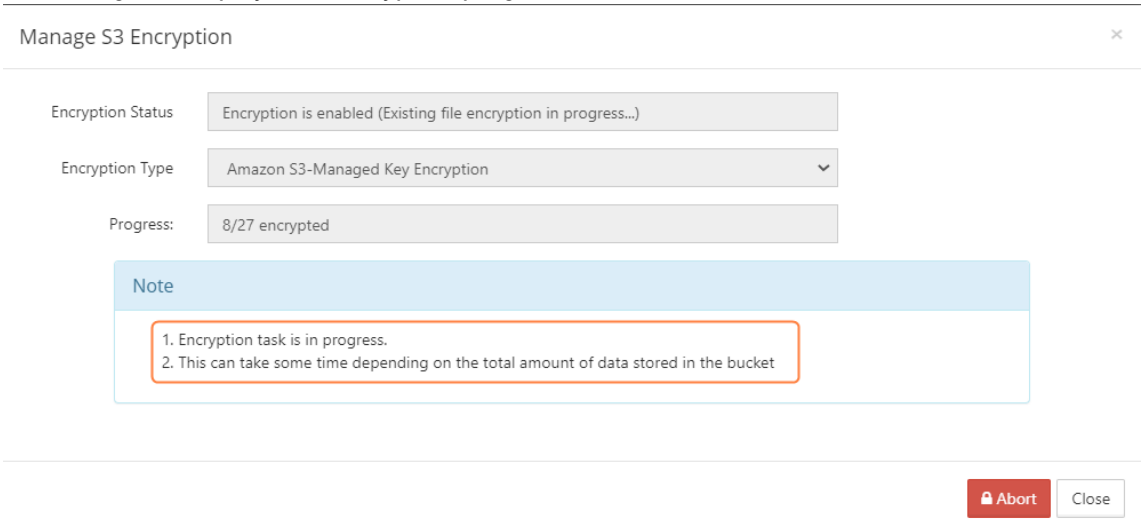
The **Manage S3 Encryption** dialog box opens:

3. To perform the necessary initialization of the encryption module, click **Enable Encryption.**

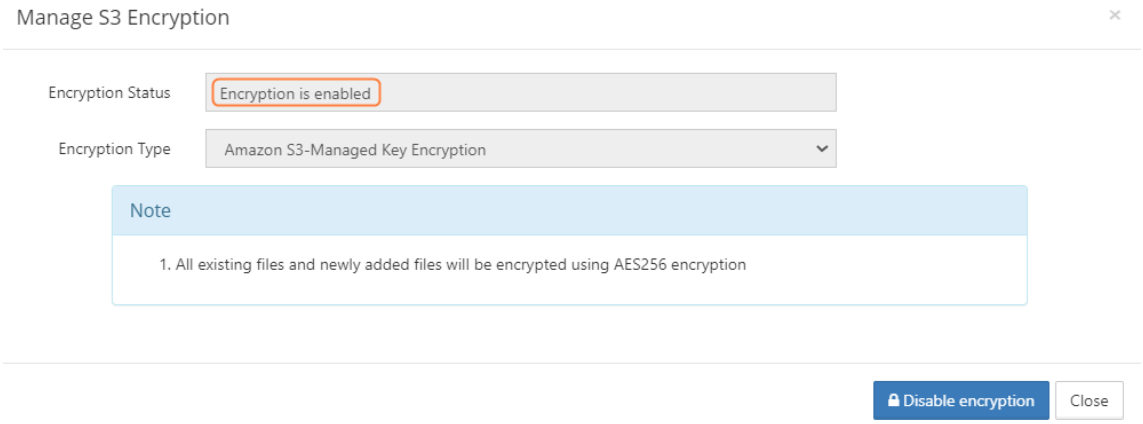


You are prompted to confirm encryption.

4. Click **OK**.
The dialog box displays the encryption progress.



When it is complete, it displays **Encryption is enabled**.



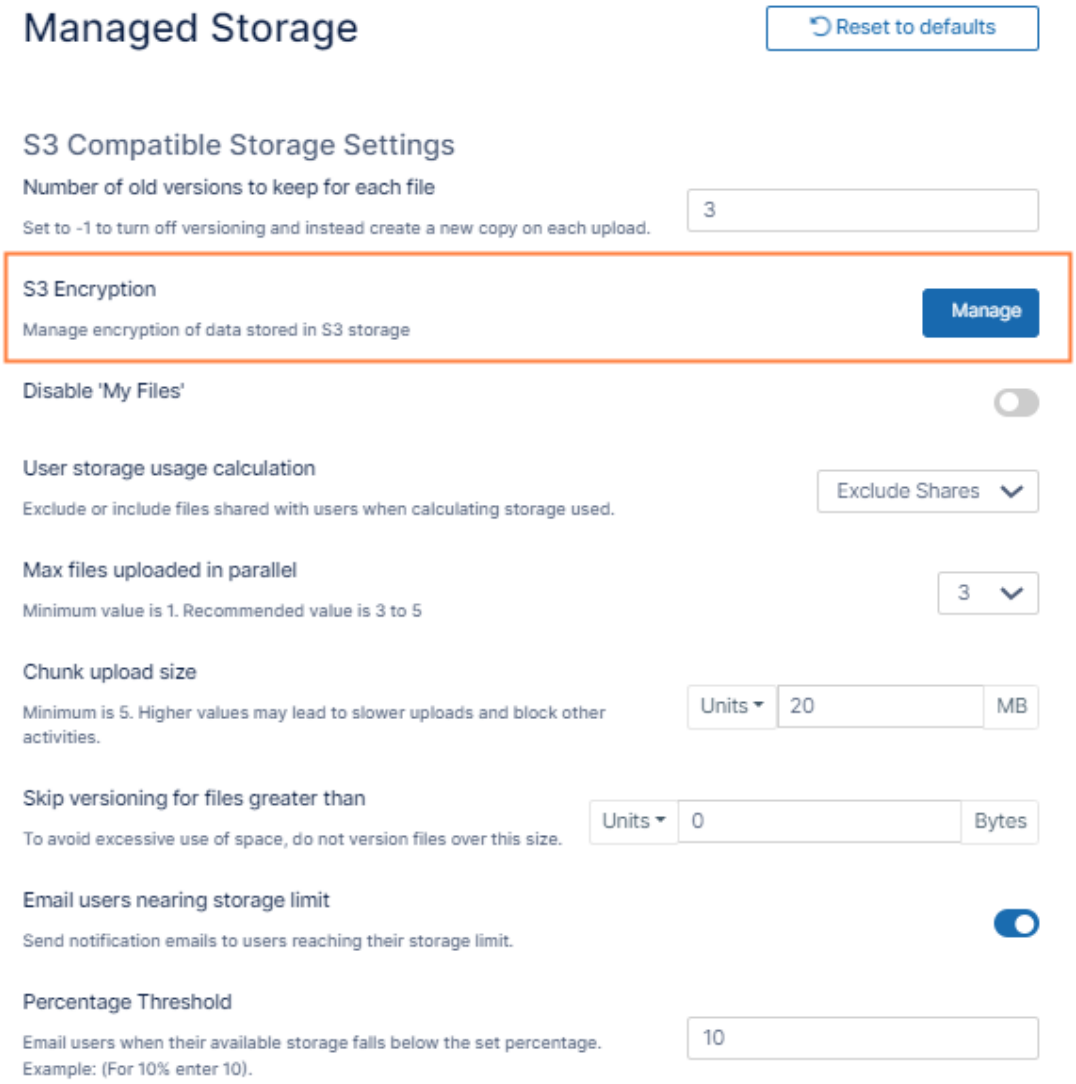
Disabling S3 Storage Encryption

Administrators can disable S3 storage encryption following the steps here.

To disable S3 encryption:

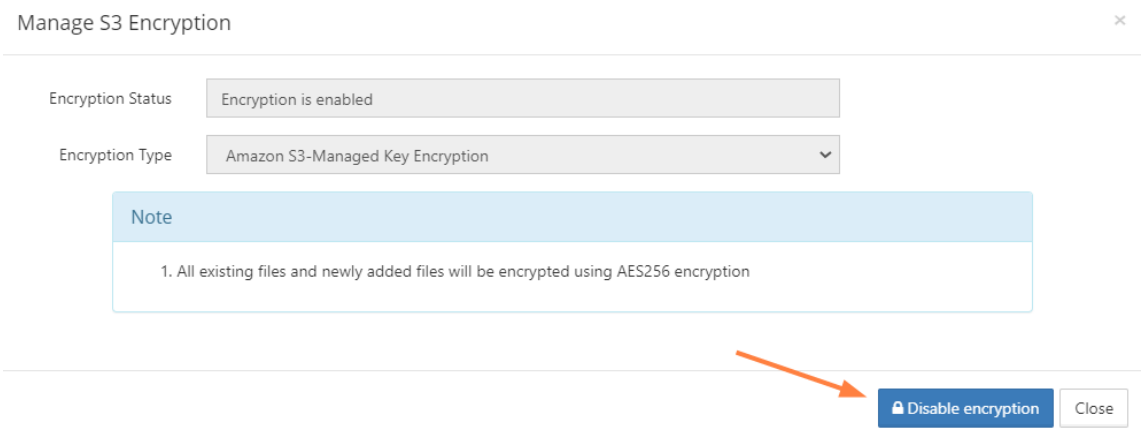
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The Managed Storage settings page opens. An **S3 Encryption** field with a **Manage** button

appears.



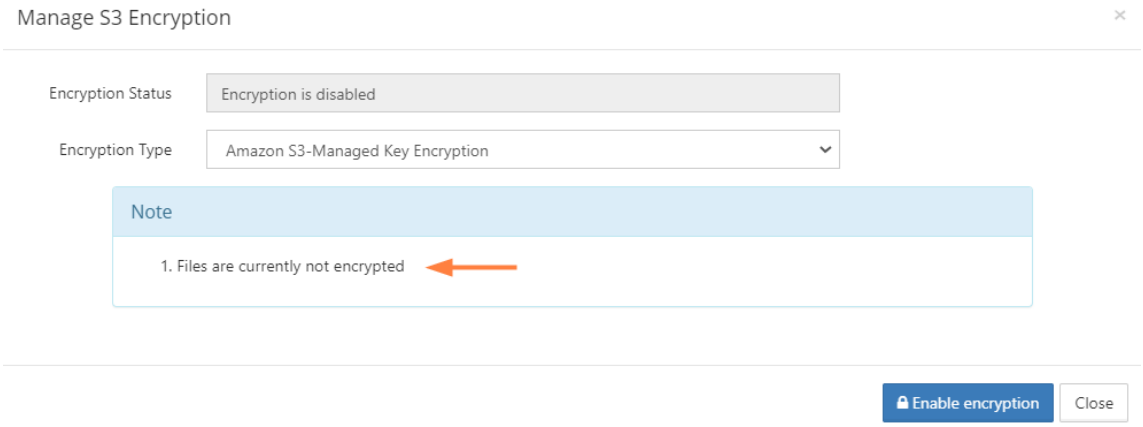
2. Click **Manage**.
   The **Manage S3 Encryption** dialog box opens

3. Click **Decrypt All**.



You are prompted to confirm disabling encryption.

4. Click **OK**.
Once the decryption is complete, the dialog box confirms that files are not encrypted.



Choosing S3 Encryption Type

When you enable S3 Storage Encryption:

- Communication between FileCloud and AWS uses SSL encryption to protect data in transit.
- Once S3 is set up correctly, the **S3 Encryption** field becomes available under **Amazon S3 Storage Settings**.

FileCloud supports the following Server Side Encryption types:

- **Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)**
All data is encrypted at rest using AES-256 encryption. The data can only be accessed using the AWS access key and secret key credentials. The data is accessible through the Amazon S3 console.
Note: Although encrypted data is accessible through the Amazon S3 console, do not modify

data created by FileCloud Managed Storage, as doing so can corrupt the FileCloud repository. In this case, the data should only be modified by FileCloud.

- **Server-Side Encryption with Customer-Provided Keys (SSE-C)**
  The data is encrypted using the customer-supplied 32-byte encryption key. This option has slower performance due to restrictions on how this data can be decrypted (Amazon S3 cannot decrypt the data. The data must first be downloaded to FileCloud server and then decrypted). The data is also inaccessible through the Amazon S3 console.
  Notes:
  - When you choose **SSE-C**, any backups created before SSE-C was enabled will become invalid, and therefore that data will not be recoverable.
  - When SSE-C encryption is enabled, optimized upload is not available for S3 storage and S3 network shares.
- **Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)**
  Similar to SSE-S3 but the key itself is managed using Amazon's KMS service. This allows management of specific keys and their permissions for encrypting the data. The data is still encrypted at rest and is accessible via S3 Console with appropriate credentials.

WARNINGS:

- Enabling encryption starts a process that encrypts all available data in the bucket as well as all new data.
- This process may take some time depending on the amount of existing data in the bucket.
- It is recommended that you modify the encryption setting during periods of low server activity.

Although you can change the Encryption setting can be done at any time, we recommend doing so during off-peak hours to minimize the risk of disrupting user access.

IAM User Policy for S3 Access

If you use Amazon S3 for file storage, FileCloud requires S3 access to create and manage the bucket.

The IAM user that manages the bucket must have the following permissions. The following policy grants access to all S3 buckets in your AWS account. You can restrict access to a specific bucket using the appropriate resource arn. For example, **arn:aws:s3:::bucket_name**

```
{
    "Version": "2012-10-17",
    "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                  "s3:CreateBucket",
```

```
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject"
            ],
             "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```

or

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Allow",
          "Action": [
                "s3:CreateBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject"
            ],
             "Resource": [
                "arn:aws:s3:::bucketname/*"
            ]
        }
    ]
}
```

S3 Storage Encryption with AWS cross-account KMS key

Prerequisites for S3 Storage Encryption with AWS cross-account KMS key

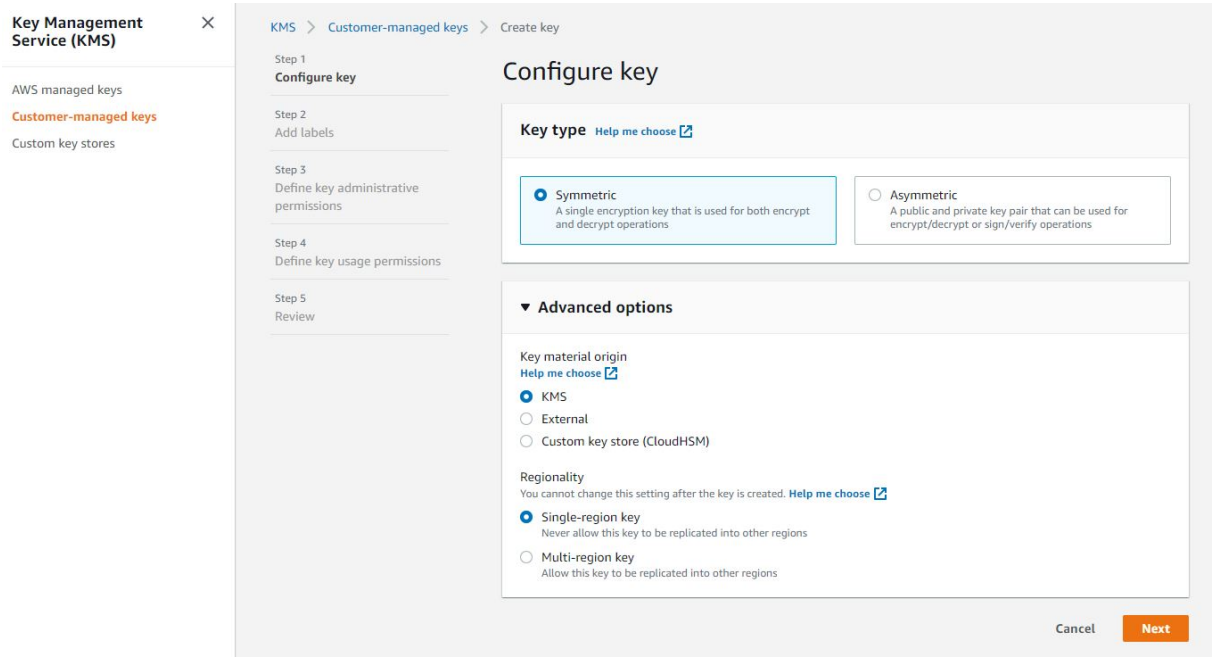
- A Symmetric Customer Managed Key created on an AWS account which will hold the key for encryption. Let's say for example, this account is called, **KMS Account**.
- Key Policy added to the above created key on KMS Account, which gives access to the other AWS account, let's say for example, this account is called, **S3 Hosted Account**.
- IAM Policy added to the IAM user on S3 Hosted Account, which delegates access to the key from KMS Account.

Customer Managed Keys should NOT be deleted. If they are deleted, files that were encrypted using that key, will not be accessible and also cannot be recovered.

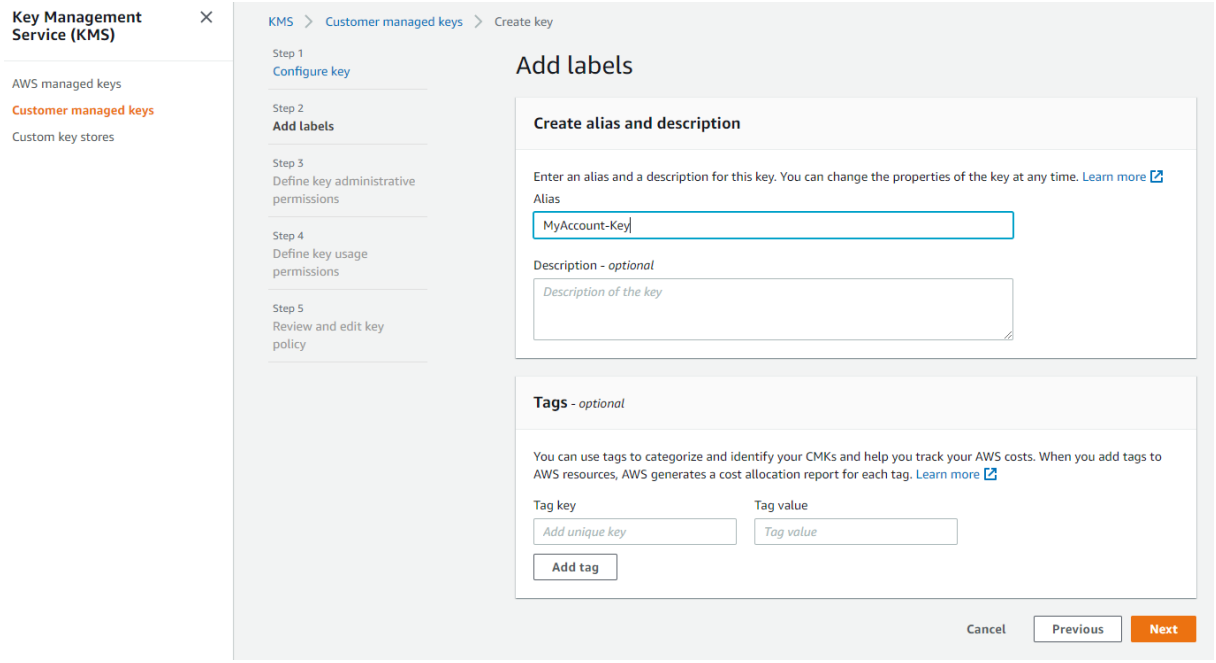
Configuring S3 Storage Encryption with AWS cross-account KMS key

A) The following steps can be used as reference in creating a key on KMS Account:

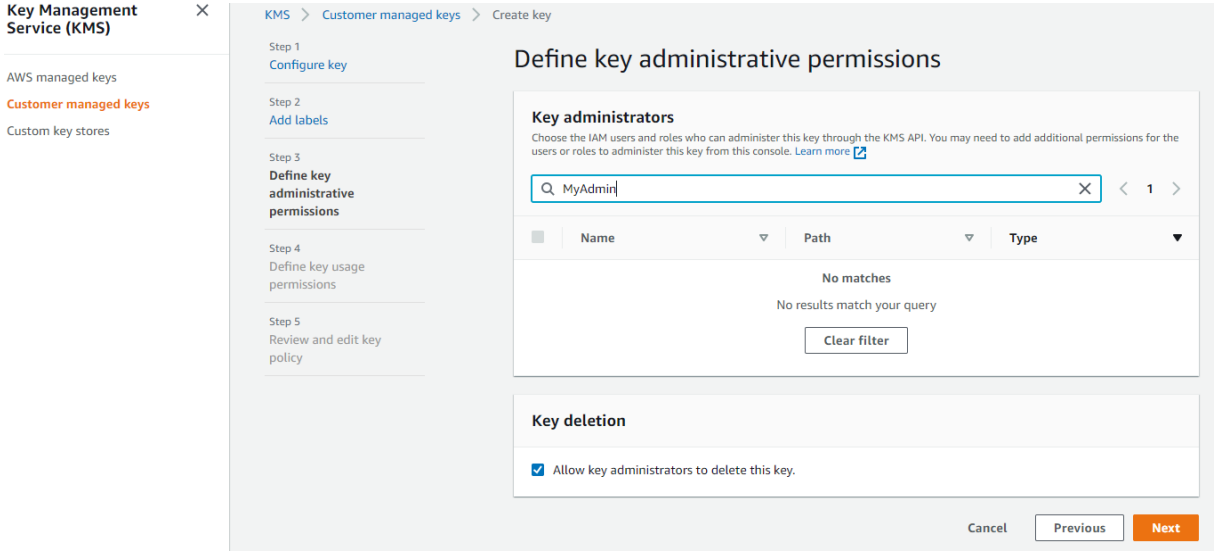
1) From AWS Console, navigate to KMS > Customer Managed Keys and click on "Create Key". Choose the default options as in below screenshot and click on 'Next'.



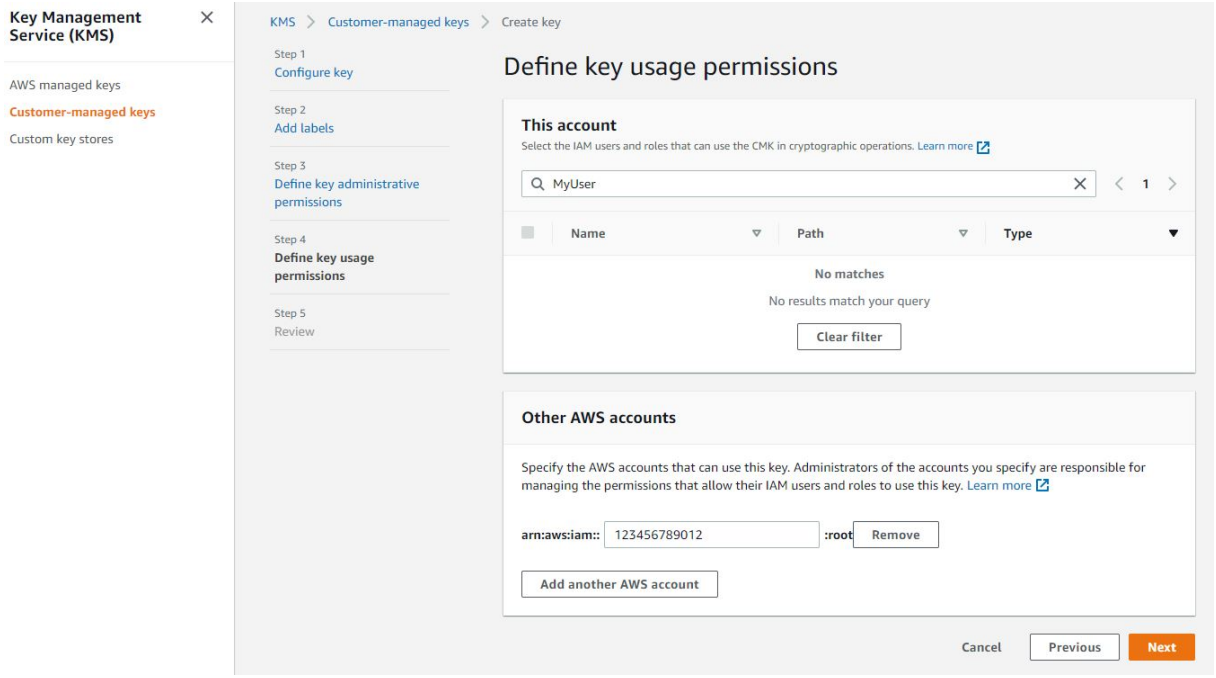
2) Provide an Alias or Name for the key and click on 'Next'.



3) Provide access to admin IAM users if needed or proceed with the defaults and click on 'Next'.



4) Provide access to IAM users if needed and **under "Other AWS accounts", provide the Account ID of S3 Hosted Account** and click on 'Next' and in the next page, click on 'Finish'. **NOTE: This gives access to root user of the S3 Hosted Account.**



NOTE: Make sure the key policy includes the following permissions.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<KMS Account ID>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<S3 Hosted Account ID>:root"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
```

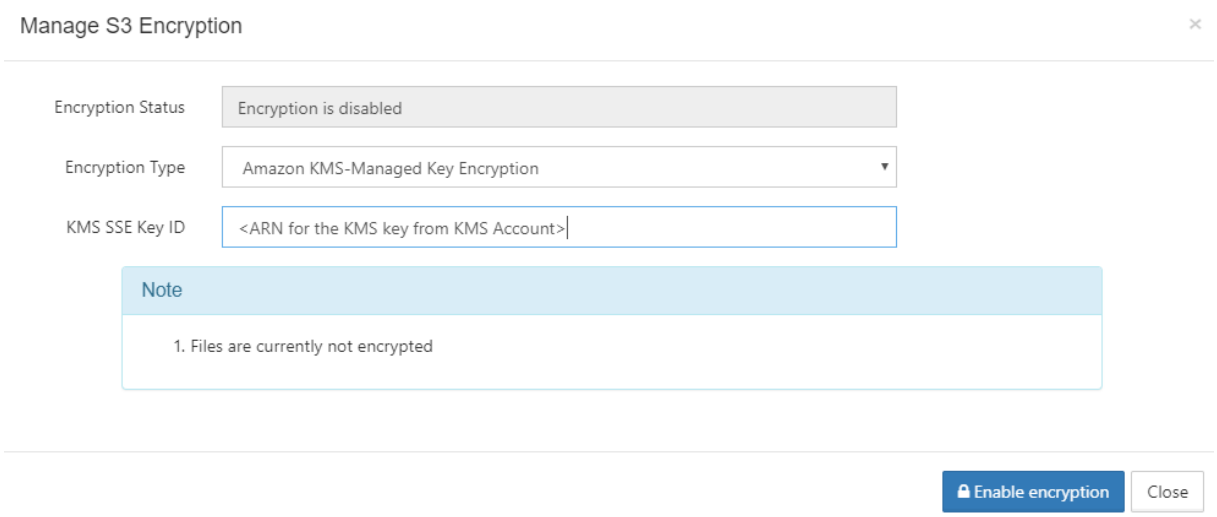
```
}
```

B) The following step is to be done on the S3 Hosted Account for delegating access to an IAM user for the key from KMS Account:

Add the following IAM policy **to the IAM user that has access to the S3 bucket** on S3 Hosted Account.

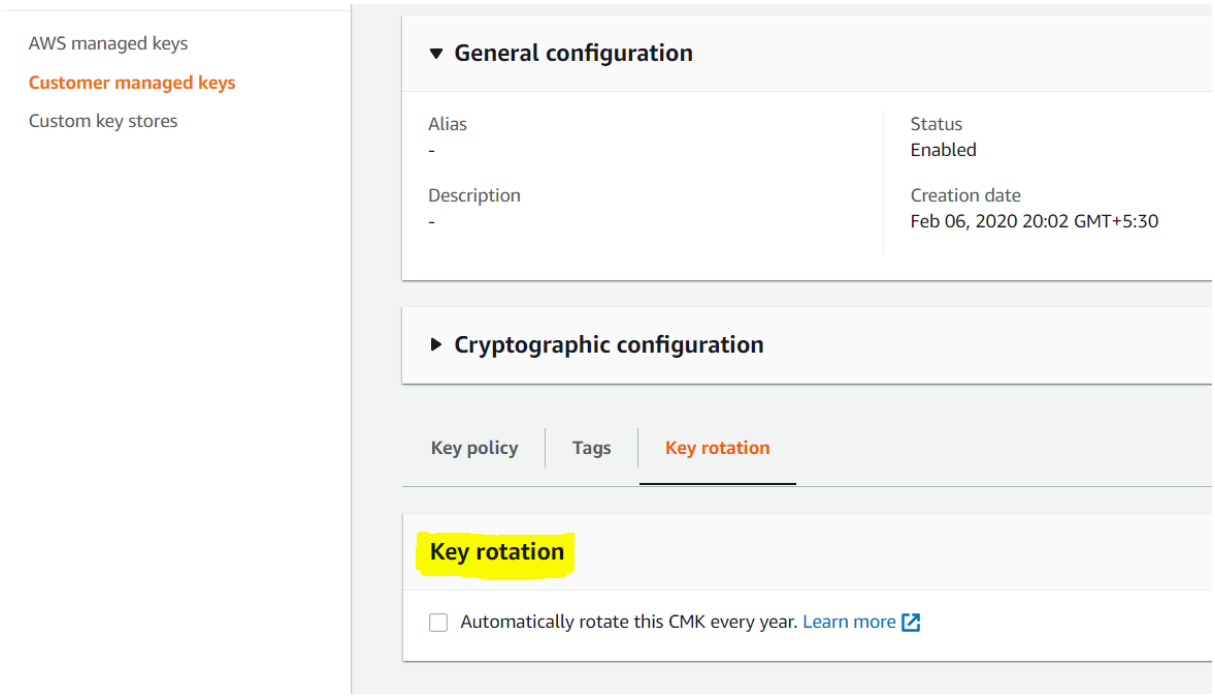
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CMK",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "<ARN for the KMS key from KMS Account>"
        }
    ]
}
```

C) Finally, Navigate to the FileCloud admin page, Settings > Storage > My Files > S3 Encryption, and click on "Manage". Choose the "Amazon KMS-Managed Key Encryption" option and provide the ARN for the KMS key from KMS Account, as in below screenshot. Then click on "Enable encryption".



Rotating AWS Customer Managed Keys

1. In the navigation pane, choose **Customer managed keys**.
2. Choose the alias or key ID of a CMK.
3. Choose the **Key rotation** tab.
4. Select the **Automatically rotate this CMK every year** check box. If a CMK is disabled or pending deletion, the **Automatically rotate this CMK every year** check box is cleared, and you cannot change it. The key rotation status is restored when you enable the CMK or cancel deletion.
5. Choose **Save**.



When you enable ***automatic key rotation*** for a CMK, **AWS KMS generates new cryptographic material for the CMK every year**. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. Key rotation changes only the CMK's *backing key*, which is the cryptographic material that is used in encryption operations.

However, automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key.

NOTE : Manual key rotation is not supported by FileCloud.

Enabling access logging for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

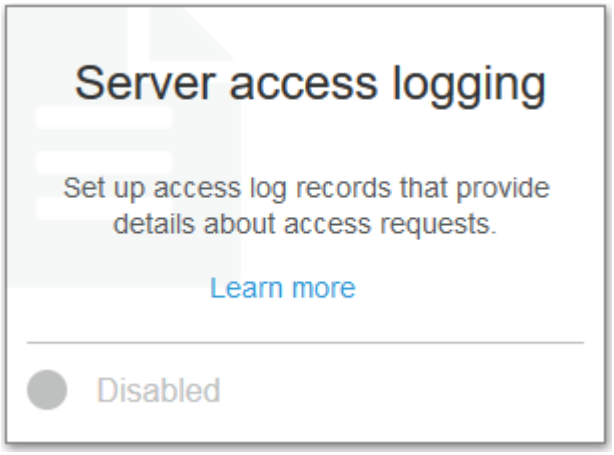
2. In the **Bucket name** list, choose the name of the bucket that you want to enable server access logging for.



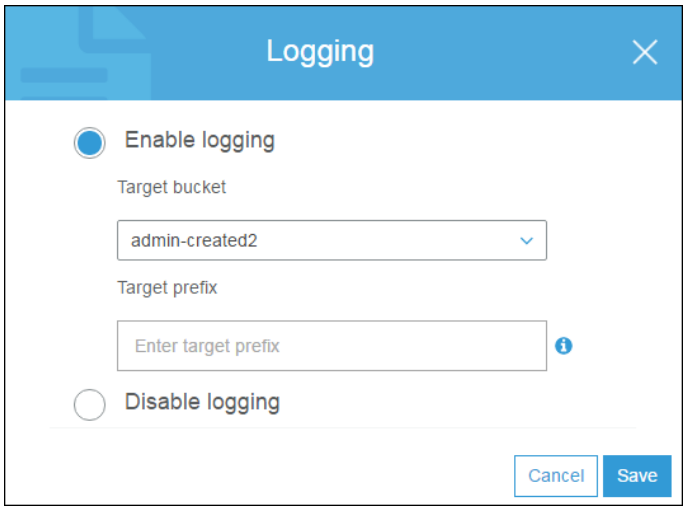
3. Choose **Properties**.



4. Choose **Server access logging**.



5. Choose **Enable Logging**. For **Target**, choose the name of the bucket that you want to receive the log record objects. The target bucket must be in the same Region as the source bucket. Also, it must be owned by the same AWS account and must not have a default retention period configuration.



6. (Optional) For **Target prefix**, type a key name prefix for log objects, so that all of the log object names begin with the same string.
7. Choose **Save**.

   You can view the logs in the target bucket. If you specified a prefix, the prefix shows as a folder in the target bucket in the console. After you enable server access logging, it might take a few hours before the logs are delivered to the target bucket.

Setting Up MongoDB Enterprise Advanced Server

Full support for MongoDB Enterprise Advanced Server has been added in FileCloud 23.241.

By default, FileCloud includes MongoDB Community Edition, a versatile, efficient database that meets most customers needs. However, if your system requires database encryption or compliance with the MongoDB STIG, you may choose to deploy MongoDB Enterprise Advanced, which meets those requirements. For more information about MongoDB Enterprise Advanced, see https://www.mongodb.com/products/self-managed/enterprise-advanced.

Install MongoDB Enterprise Advanced

Installing on Ubuntu

1. If **gnupg** and **curl** are not already installed, install them.
   In a command line enter:

```
sudo apt-get install gnupg curl

curl -fsSL https://pgp.mongodb.com/server-6.0.asc | \
```

```
sudo gpg -o /usr/share/keyrings/mongodb-server-6.0.gpg \

--dearmor
```

2. Go to **/etc/apt/sources.list.d/**
3. Create the list file **mongodb-enterprise-6.0.list**:

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
server-6.0.gpg ] https://repo.mongodb.com/apt/ubuntu jammy/mongodb-enterprise/6.0
multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-enterprise-6.0.list
```

4. Reload the local package database:

```
sudo apt-get update
```

5. Install MongoDB Enterprise Advanced:

```
sudo apt-get install -y mongodb-enterprise
```

Installing on RHEL

1. Go to **/etc/yum.repos.d/** and create the file **mongodb-enterprise-6.0.repo** file with the following contents.

```
[mongodb-enterprise-6.0]

name=MongoDB Enterprise Repository

baseurl=https://repo.mongodb.com/yum/redhat/9/mongodb-enterprise/6.0/$basearch/

gpgcheck=1

enabled=1

gpgkey=https://pgp.mongodb.com/server-6.0.asc
```

2. The **mongodb-enterprise-6.0.repo** enables you to install MongoDB Enterprise Advanced directly using yum.
   Enter the following to perform the installation.

```
sudo yum install -y mongodb-enterprise
```

Configure the connection to FileCloud for Ubuntu or RHEL

1. Make the bind IP of MongoDB in the Enterprise Advanced server private:

```
vi /etc/mongod.conf
change bindip: 127.0.0.1 to bindip: [private ip of Enterprise Advanced server]
```

2. Create a new db user in the Enterprise Advanced server.
   First, connect to the mongo shell:

```
mongosh private_ip
```

   Then create the user:

```
db.createUser({user: 'fcdbuser', pwd: 'passw0rd1', roles:['root']})
```

   Finally, verify the connection from the FileCloud server:

```
mongosh private_ip -u fcdbuser  --authenticationDatabase "admin"
```

3. Open **/var/www/html/config/cloudconfig.php** and update the IP address of the db server to point to the MongoDB Enterprise Advanced server:

```
// ... Cloud Database

define("TONIDOCLOUD_DBSERVER", "mongodb://[private ip of Enterprise Advanced
server]");

// ... Audit Database

define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://[private ip of Enterprise Advanced
server]");

// … Settings Database
```

```
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://[private ip of Enterprise
Advanced server]");
```

4. Open **/var/www/html/config/localstorageconfig.php,** and update the IP address of the db server to point to the MongoDB Enterprise Advanced server:

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://[private ip of Enterprise
Advanced server]");
```

Installing on Windows

1. Download MongoDB Enterprise 6.0 Windows msi from https://www.mongodb.com/try/download/enterprise.
2. Launch the msi file, and install MongoDB Enterprise 6.0.
   When the installer prompts you to specify where you want to install the file, enter:
   C:\Program Files\MongoDB\Server\6.0\bin

Configure the connection to FileCloud for Windows

1. In the server containing the MongoDB Enterprise installation, set the bind IP of **C:\Program Files\MongoDB\Server\6.0\bin\mongodb.cfg** to the server's private IP.
   Open mongodb.cfg and change the setting:

```
bindip: 127.0.0.1
```

   to

```
bindip: [private_ip of Enterprise Advanced server]
```

2. Restart the mongodb service.
3. In the server containing the MongoDB Enterprise installation, open a command prompt and switch to the /bin directory:

```
cd C:\Program Files\MongoDB\Server\6.0\bin\
```

   Connect to the mongo shell.

```
mongosh private_ip
```

4. Switch to the admin user:

```
use admin
```

5. Create a new db user:

```
db.createUser({user: 'fcdbuser', pwd: 'passw0rd1', roles:['root']})
```

6. If necessary, open port 27017 to the IP of the other machine on both servers to allow connection between the servers.
   Run the following command in both servers and set the value of the remote ip to the private ip address of the other server.

```
netsh advfirewall firewall add rule name="Opening port to allow MongoDB" dir=in
action=allow protocol=TCP localport=27017 remoteip=[remote ip of other server]
```

7. From the FileCloud server, verify the connection:

```
mongosh [private ip of Enterprise Advanced server] -u fcdbuser  --
authenticationDatabase "admin”
```

8. Open **C:/xampp/htdocs/config/cloudconfig.php** and update the IP address of the db server to point to the MongoDB Enterprise Advanced server:

```
// ... Cloud Database

define("TONIDOCLOUD_DBSERVER", "mongodb://[private ip of Enterprise Advanced
server]");

// ... Audit Database
```

```
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://[private ip of Enterprise Advanced
server]");

// … Settings Database

define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://[private ip of Enterprise
Advanced server]");
```

9. Open **C:/xampp/htdocs/config/localstorageconfig.php** and replace the DB server IP with the private IP of the Enterprise Advanced server:

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://[private ip of Enterprise
Advanced server]");
```

Manage the Recycle Bin Using Policies

Administrators can configure FileCloud to deal with specific users' and groups' recycle bins through policies.

Why?

- Files deleted by users are moved to recycle bin (if enabled).
- The files in recycle bin will take up space over time.

To manage the recycle bin, you can decide what to do with files in the following cases:

Do you want to store deleted files for recovery purposes?

If you enable this setting, whenever a user deletes a file, it will automatically be placed in the Recycle Bin.

This allows the user to recover an old file if it is deleted by accident.

💡 If this option is not enabled, then when a user deletes a file it is removed from FileCloud permanently.

Do you want to empty the recycle bin after a specific number of days?

You can automatically clear the files deleted by users and partial uploads.

This is configured by the setting called:

- **Automatically delete File from the recycle bin After Set Number of Days**

You set this to the number of days you want a deleted file to be kept before being permanently removed.

- For example, if the value is set to 7, then files older than 7 days will be deleted automatically.

If you do not want FileCloud to automatically empty the recycle bin at any time, use a value of 0.

Do you want to set a size limit for the deleted files that are stored?

If you do not want deleted files to take up too much space, you can decide to only store deleted files of a certain size.

This is configured in the following setting:

- **Do Not Store Deleted Files Greater Than**

Files less than this size are stored

Files greater than this size are permanently deleted

You can specify the file size in the following ways:

- GB
- MB
- KB
- B

You can also restrict users' ability to empty their own recycle bins.
Restrict User's Recycle Bin Options

Administrators configure options related to Recycle Bin behavior for a user or group in policies.

- This allows administrators to use different settings for different users and groups.
- The recycle bin configuration settings for Network folders are global and managed in the Admin Portal under the MANAGE section by selecting Network Folders.

For example: In the Cherry Road Real Estate company, every user working in the Accounting office must retain their recycled items for 60 days, but everyone else can have their bins cleared in 30 days.
The following three Recycle Bin settings exist in Policies:

Setting	Option	Description
Store deleted files in the recycle bin	yes or no	Move the file from it's location in My Files to the recycle bin when the user deletes it

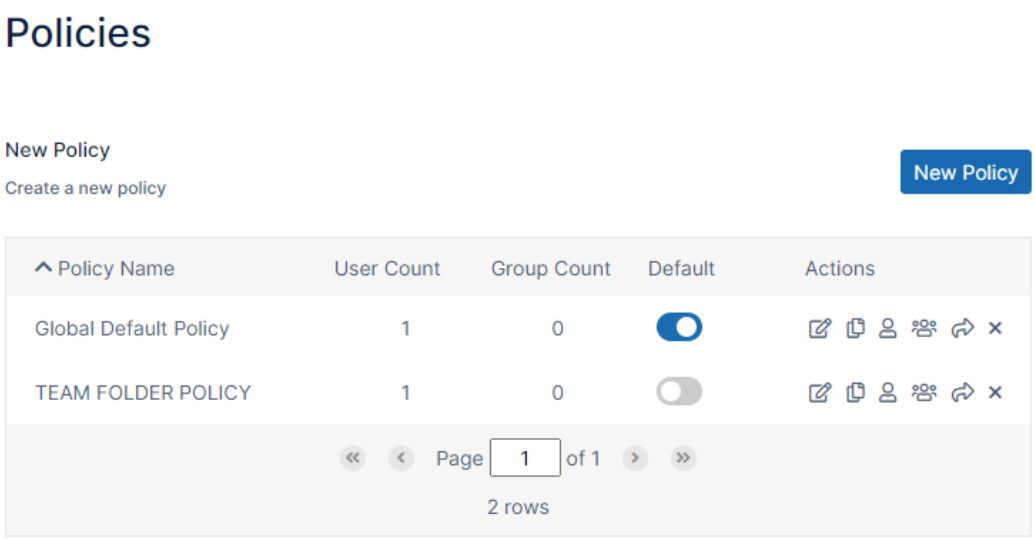
Setting	Option	Description
Automatically delete files from recycle bin after set number of days	Whole number	Number of days after a file was deleted that it will be automatically cleared from the recycle bin (and therefore, no longer be present in FileCloud). A value of 0 indicates that deleted files will not be cleared automatically. If they are not manually cleared from the recycle bin, they will remain available to be restored in FileCloud but will also use up available storage.
Do not store deleted files greater than	Any positive number of Units: • GB • MB • KB • B	Files greater than the specified size are permanently deleted. The number can contain decimals. For example: • 0.09765625 GB

You must ensure that the Cron service is running. This is a prerequisite for any automatic functionality in FileCloud Server.

To configure a recycle bin policy for users or groups:

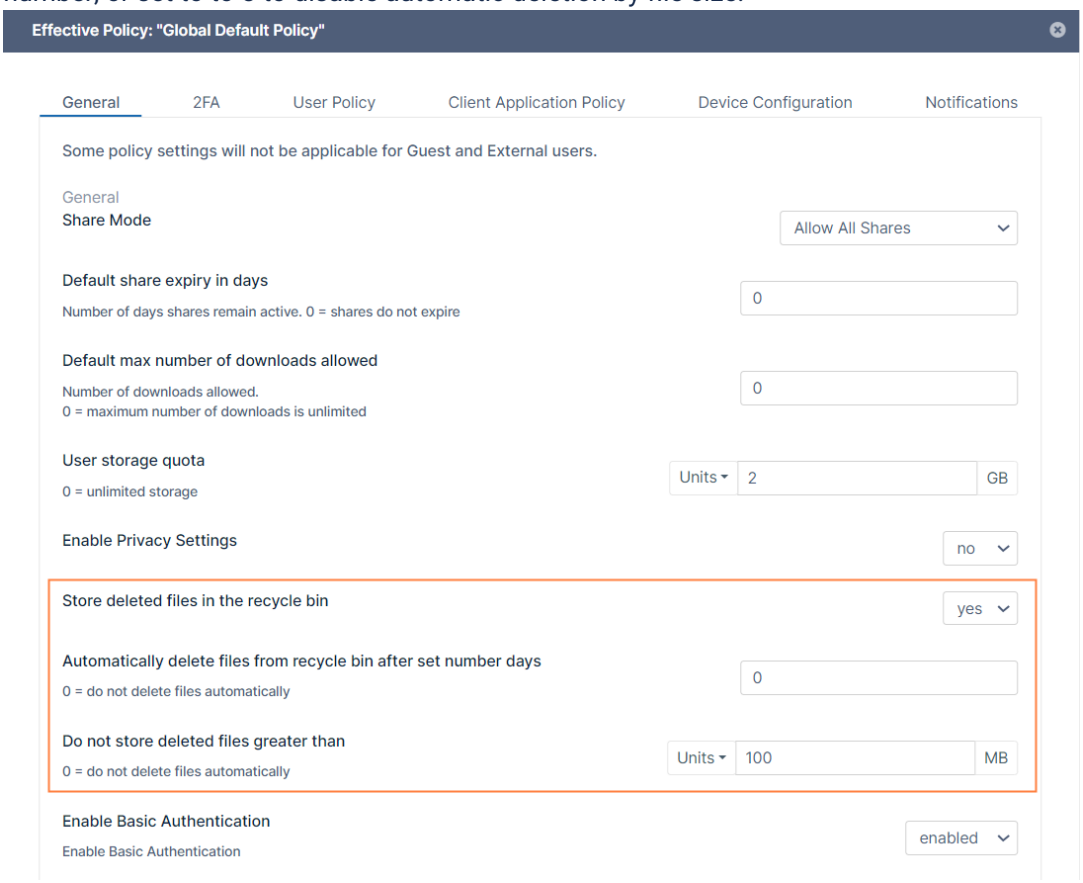
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .

The **Policies** page opens.



2. Edit the policy of the users or groups.
3. In the **General** tab, scroll down and set **Store deleted files in the recycle bin** to **yes** or **no**.
4. If you selected **no**, to save your changes, click **Save**.
5. If you selected **yes:**
    a. In **Automatically delete File from the recycle bin after set number of days**, enter a number, or set to **0** to disable automatic deletion by number of days.

b. In **Do not store deleted files greater than**, select the type of unit in **Units**, and then type in a number, or set to to **0** to disable automatic deletion by file size.



6. To save your changes, click **Save**.

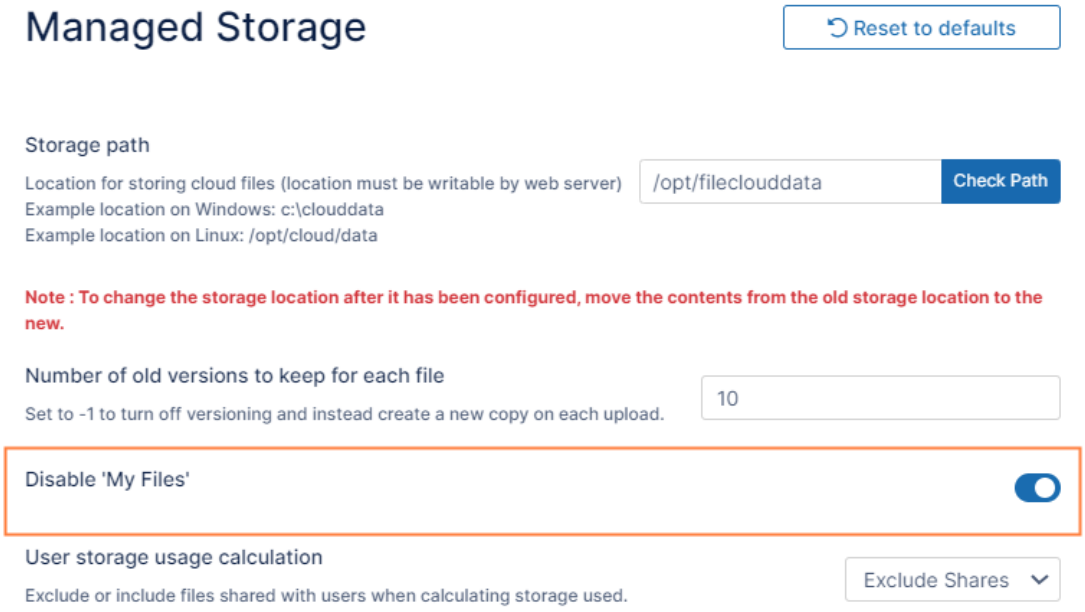
Disable My Files

My Files can be disabled completely if users need to access only Network Folders, Team Folders or shared data.

This should be done during initial server setup. If My Files is disabled after users are created, data previously stored in My Files will no longer be accessible, and if users have camera backup set up, their photos and videos will no longer be backed up.

To disable My Files:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   The **Managed Storage settings** page opens by default.
2. Scroll down to the setting **Disable 'My Files'**, and enable it.



3. Click **Save.**

Manually Clearing Large Recycle Bins

> The tool to manually empty a recycle bin is available in FileCloud version 18.2 and later.

Administrators may need to use a tool to manually clear overfilled recycle bins that contain more than:

- 100K of files
- 1000 folders

Why?

- When a user tries to empty their overfilled recycle bin, you may see errors in the Admin Portal.

To manually clear an overfilled recycle bin:

1. On the FileCloud Server, open the Command Prompt application.
2. To calculate the recycle bin size, type the following command:

```
C:\xampp\htdocs\resources\tools\fileutils> c:\xampp\php\php.exe emptyrecyclebin.php -h default
-u tester -s
```

3. To simulate emptying of the recycle bin, type the following command:

```
C:\xampp\htdocs\resources\tools\fileutils> c:\xampp\php\php.exe emptyrecyclebin.php -h default
-u tester
```

4. To empty the recycle bin, type the following command:

```
C:\xampp\htdocs\resources\tools\fileutils> c:\xampp\php\php.exe emptyrecyclebin.php -h default
-u tester –r
```

Embedded File Upload Website Form

It is possible to create a file upload form that can be integrated with your existing website so that when users upload files they get uploaded to a specific file cloud folder without the need for a user name or password. This is similar to having a simple "File Drop box" allowing your customers / clients / vendors to send files to you quickly and easily.

Step 1:

To allow cross domain requests, in the WWWROOT/.htaccess file disable the setting:

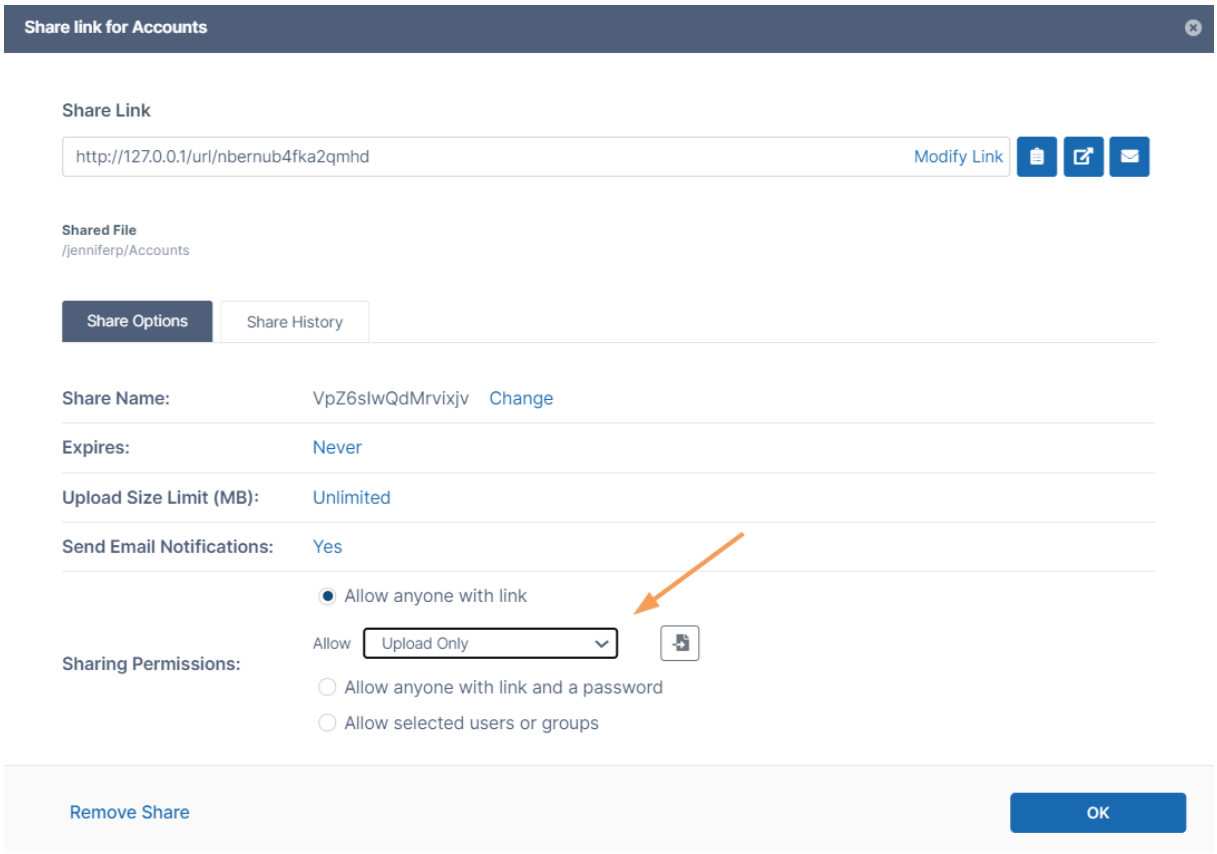
```
<IfModule mod_headers.c>
Header set X-Frame-Options "SAMEORIGIN"
</IfModule>
```

by putting a hashtag (#) in front of it.

```
<IfModule mod_headers.c>
#Header set X-Frame-Options "SAMEORIGIN"
</IfModule>
```

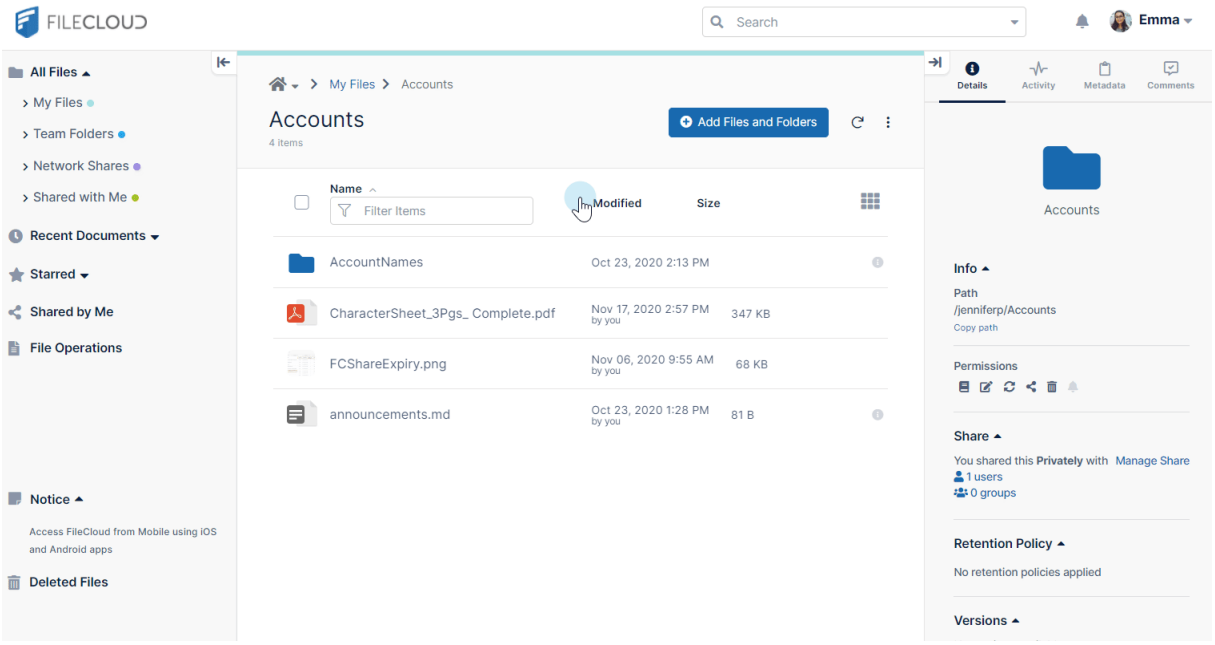
Step 2:

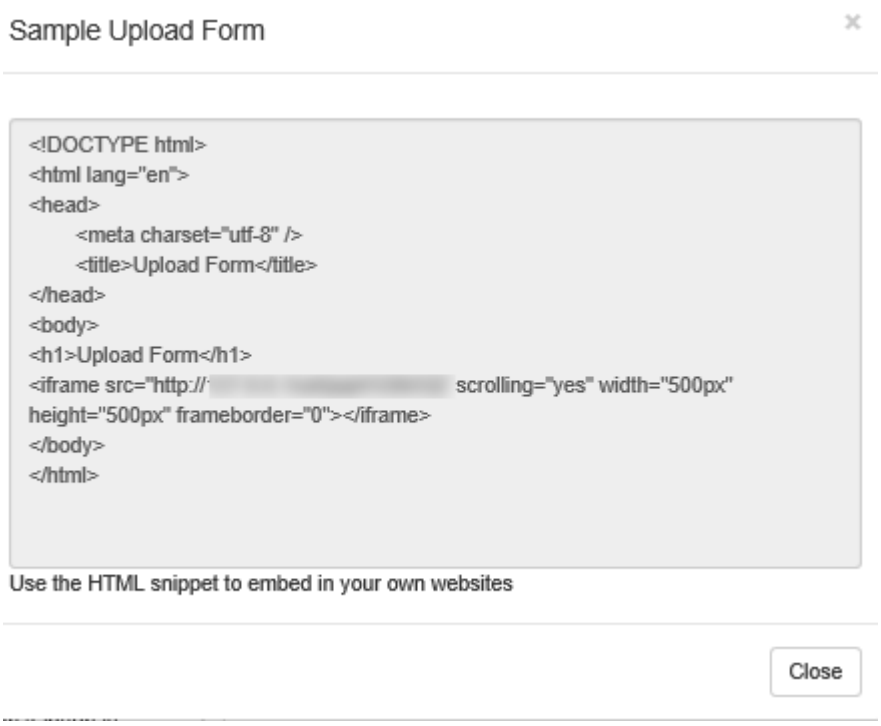
Create a public share for a folder and set Share Permissions to Allow Everyone with **Upload Only**.



Step 3:

Click on the Sample Form to open a sample HTML web form that should be integrated in your website.

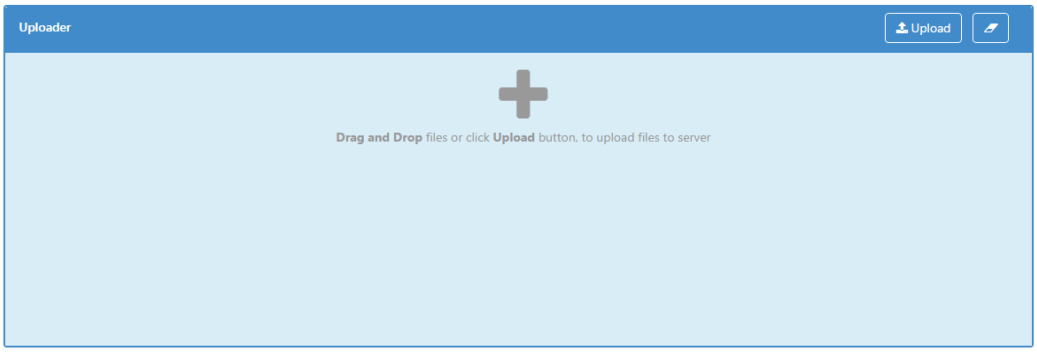




Step 4:

Embed the form in your existing web page or website.

If you open the webpage, you should see a form appear like this. You should now be able to upload files either by dragging or dropping or selecting the files using the upload button.



Restrict a User's Recycle Bin Options

Administrators can allow users to clear all files at once from their recycle bins by enabling **Enable recycle bin clearing** in the users' policy**.**

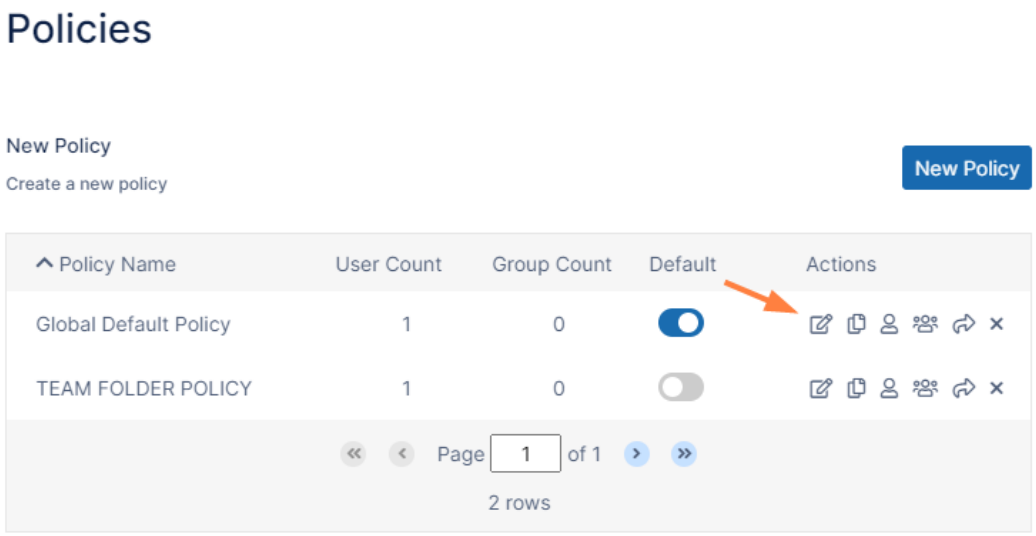
By default, **Enable recycle bin clearing** is enabled**,** allowing users to click **Clear Deleted Files** in the recycle bin.

If **Enable recycle bin clearing** is disabled in a policy, users belonging to the policy do not see a **Clear Deleted Files** button in the recycle bin.

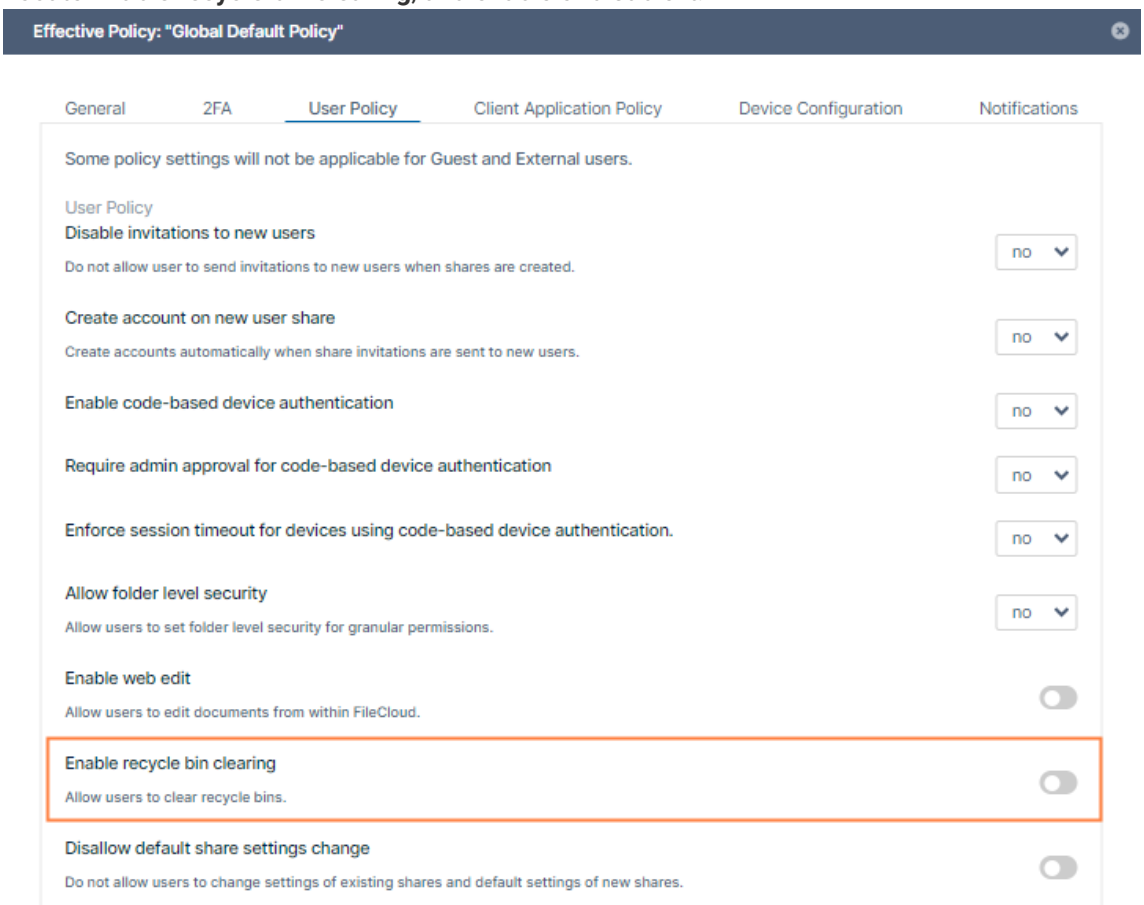
> ⚠ Disabling **Enable recycle bin clearing** doesn't block the delete operation. Users can still remove files from the recycle bin on a file-by-file basis.

To enable or disable recycle bin clearing:

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. Click the Edit icon in the row for the users' policy.



3. The **Policy Settings** dialog box opens.
4. Click the **User Policy** tab.
5. Locate **Enable recycle bin clearing**, and enable or disable it.



6. Click **Save**.

Setting up FileCloud Managed Azure Blob Storage

As an administrator, you can integrate FileCloud Server to store user data in Azure Blob Storage.

- Azure Blob Storage is a massively scalable object storage service for unstructured data.
- You can use Blob Storage to store and retrieve any amount of data at any time, from anywhere on the web.
- You can perform these tasks using the Azure portal.

Getting Started with Azure Blob Storage

WARNINGS:

- Only change the FileCloud storage type to Blob for new installations.
- Do not change the FileCloud storage type to Blob if FileCloud has been in use and data is already stored.
- **Be very careful when changing the storage path. If done improperly, it could lead to data loss.**
- When changing the storage type from local to Azure Blob, the files and folders that have already been saved to local storage **will not** be moved automatically to Blob storage.
  - For existing files and folders, the administrator must manually export them from local storage before changing the storage type.
  - After changing the storage type to Blob, the administrator must manually import pre-existing files and folders.
- The Azure Storage Container should NEVER be modified outside of the FileCloud subsystem.
- Do not add/edit/modify files directly using Azure Storage tools. Doing so will destabilize your FileCloud installation.

Integrate Azure Blob Storage

1. Change the Storage Type to Azure Blob Storage

NOTE:

For this step you will need to access **WWWROOT. It is typically located at:**

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

To enable Azure Blob storage as the backend:

1. To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
   a. Configure an authoritative time server in Windows Server
   b. Synchronize Time with NTP in Linux
2. Open the following file for editing:
   WWWROOT/config/cloudconfig.php
3. Find the following line:
   define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
4. Change it to:
   define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "azureblob");
5. Save and close the file.
6. Find the following file:
   WWWROOT/config/azureblobstorageconfig-sample.php
7. Rename it to:
   WWWROOT/config/azureblobstorageconfig.php

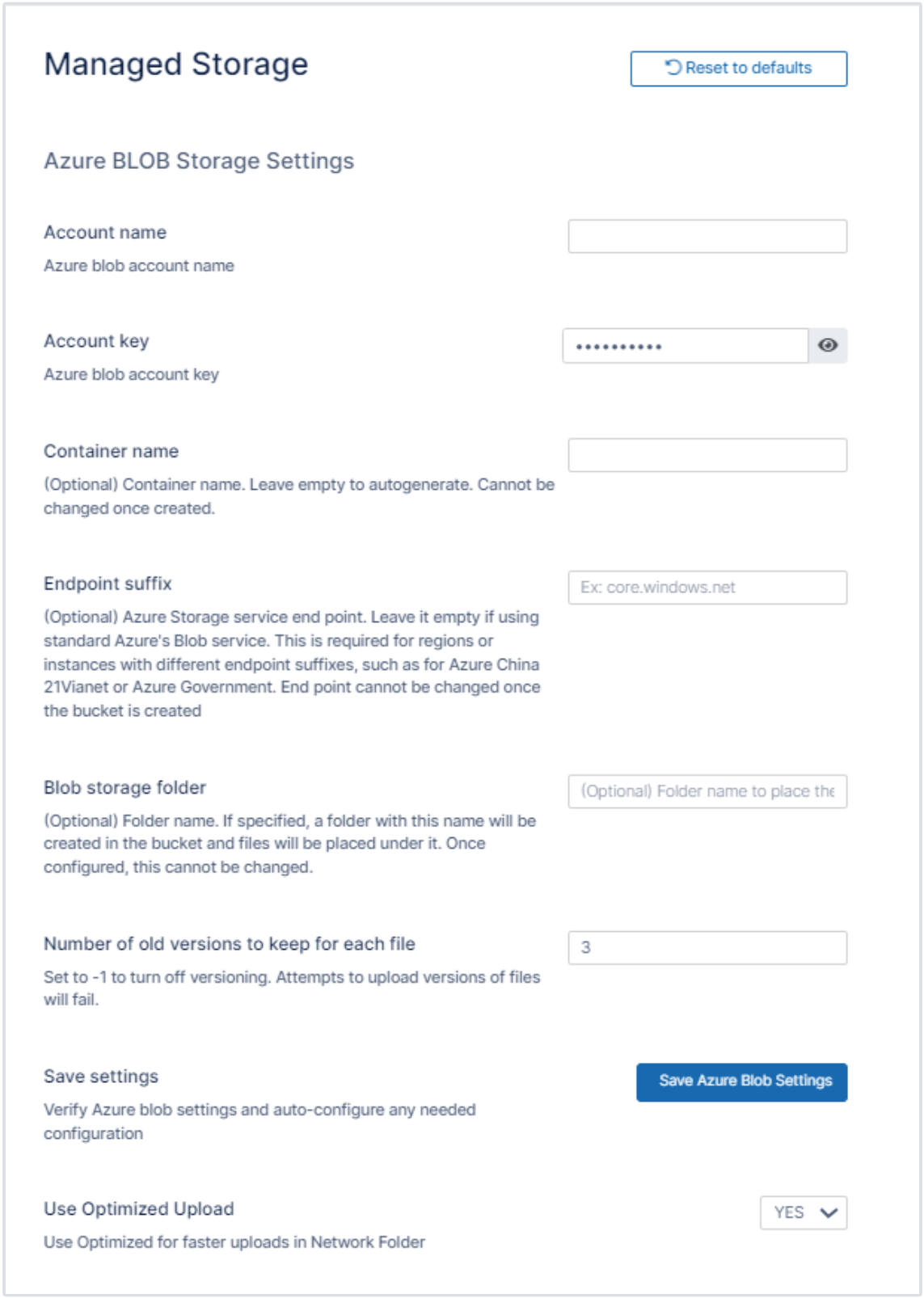
You do not need to modify **azureblobstorageconfig.php**

2. Configure Credentials

After you have set up the storage implementation key in step 1, you can configure the credentials:

To configure Azure Blob Storage credentials:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage** settings page opens by default.
2. Type in or select the Azure Blob settings for your environment (the settings that appear above the **Save Settings** button).
   Definitions of the settings appear in the table below.



3. Click **Save Settings**.

4. Enter values for the settings below it or leave the default settings.
   Definitions of the settings appear in the table on the page Setting up FileCloud Managed S3 Storage.
5. Click **Save.**

Field	Description
Account Name	This is your Azure storage account name. For an RBAC user, it requires at least the following permissions.
Account Key	This is your Azure storage account key (visit the https://azure.microsoft.com/en-us/get-started/azure-portal to obtain your account key). For an RBAC user, it requires at least the following permissions.
Container Name	Provide a storage container name. Use a new storage container whenever possible. (in some circumstances, containers previously used in FileCloud could be used). It is very important that the Azure storage container is never modified outside of the FileCloud subsystem. **Container name rules** • The name of the container has to be unique and follow the naming rules. • If you leave the **Container Name** field blank, FileCloud automatically generates the container name when setting up the storage. • Container name **cannot** be changed once storage is set up.
Endpoint Suffix	Optional: This is the Azure Blob storage endpoint. • Use this option to specify a custom Azure storage endpoint (typically Azure-compatible storage) • Use this if it is an unpublished region. To use an Azure endpoint, it must be one of the values published here. • **Note: For govcloud installs, you must use the following endpoint suffix: blob.core.usgovcloudapi.net**
Blob Storage Folder	Optional: All files will be stored inside this root storage folder. • This folder will be created automatically.
Number of old versions to keep for each file	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to -1; attempts to upload versions of a file will fail.

3. Data Encryption

Encryption at rest
Azure Storage automatically encrypts your data when persisting it to the cloud. Encryption protects your data and helps you meet your organizational security and compliance commitments. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.
Azure Storage encryption is enabled for all new and existing storage accounts and cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications to take advantage of Azure Storage encryption.
Storage accounts are encrypted regardless of their performance tier (standard or premium) or deployment model (Azure Resource Manager or classic). All Azure Storage redundancy options support encryption, and all copies of a storage account are encrypted. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. Encryption does not affect Azure Storage performance. There is no additional cost for Azure Storage encryption.

This means that all configuration can be done in Azure Portal and no additional steps are required in FileCloud

Troubleshooting

Using Override Configuration Keys

The following keys are not typically used. However, they may be needed in specific circumstances.

KEY	VALUE	Description
TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER	"/somepath/location"	In HA installs, temp folder must be a commonly accessible location. This key must be set in each of the HA nodes
TONIDOCLOUD_AZURE_BLOB_DOWNLOAD_SIZE_LIMIT	10485760	Specifies the file size limit for which file will be downloaded
TONIDOCLOUD_DISABLE_AZURE_BLOB_REDIRECT	"1"	(NOT RECOMMENDED) This will force FileCloud server to download the file from Azure Blob storage to the filecloud server system and then send it to client on file downloads (Can be slow)

How to Correct Issues with Image Previews

If you are having problems previewing images, add the following domain to the .htaccess file.

To add the domain to the .htaccess file:

1. Open the following file:
   Windows: **C:\xampp\htdocs\.htaccess**
   Linux: **/var/www/html/.htaccess**
2. Locate the following line and add the domain ***.core.windows.net** to the locations shown in the example below. The first instance may already be included.

```
Header set Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com
```

Setting Up Network Folders

Network Folders store data managed by FileCloud but saved in the existing infrastructure through various access points.

Currently, FileCloud supports legacy infrastructures like files stored on LAN and Amazon S3.

Can I also configure the FileCloud Server site storage?

💡 Administrators can also configure how users store data on the FileCloud Server site (My Files).

FileCloud Managed Storage

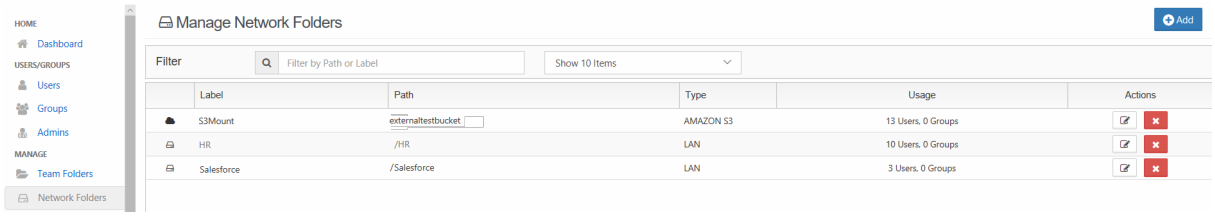
In this section:

FileCloud Blogs
• **Connect Your SFTP to FileCloud**

LAN Based Network Folders

Administrators can integrate local storage or existing files on Windows and Linux servers into FileCloud.

- This gives FileCloud users access to files on your corporate servers
- Network folders can be mounted in FileCloud
- Network Shares appears as a location on the user portal.



In this section:

Create a LAN-Based Network Folder

To configure Network Folders, first block any paths that should not be mounted, then add the remaining folder paths as Network Folders and grant users and groups access.

Beginning with FileCloud 23.241, **TONIDOCLOUD_ENABLE_NETWORK_SHARE_MOUNTS** is enabled by default.
The **TONIDOCLOUD_ENABLE_NETWORK_SHARE_MOUNTS** setting was added in FileCloud 22.1, and was disabled by default.
Prior to FileCloud 22.1, no configuration file setting was required for enabling or disabling Network Folders.

Block locations from mounting as share paths

The **TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST** setting has been added in FileCloud 22.1. In FileCloud versions prior to this, C:/xampp was not permitted to be mounted as a Network Folder, but no configuration file setting existed for manually blocking specific paths.

By default, the xampp path in Windows and the /var/www/html path in Linux are not permitted to be mounted as Network Folders. You may add any other paths that you do not want mounted as Network Folders.

1. Open cloudconfig.php.
   - Windows Location : C:\xampp\htdocs\config\cloudconfig.php
   - Linux Location : /var/www/html/config/cloudconfig.php
2. Find the setting for blocking locations. If it does not exist, create it.
   In Windows it should appear as:

   ```
   define("TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST", 'C:/xampp|c$/xampp');
   ```

   In Linux it should appear as:

```
define("TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST", '/var/www/html');
```

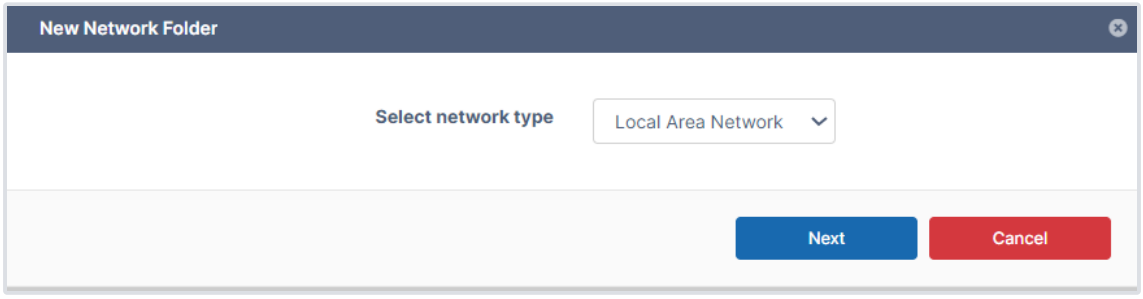
3. Add any locations that you do not want to be shared, for example:

```
define("TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST", 'C:/xampp|c$/xampp,C:/
PatientRecords');
```

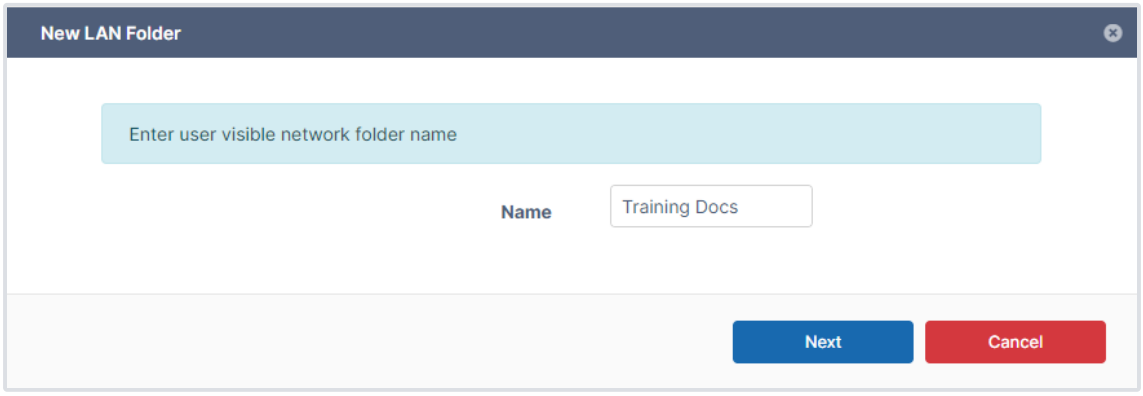
Create a Network Folder

To create a Network Folder:

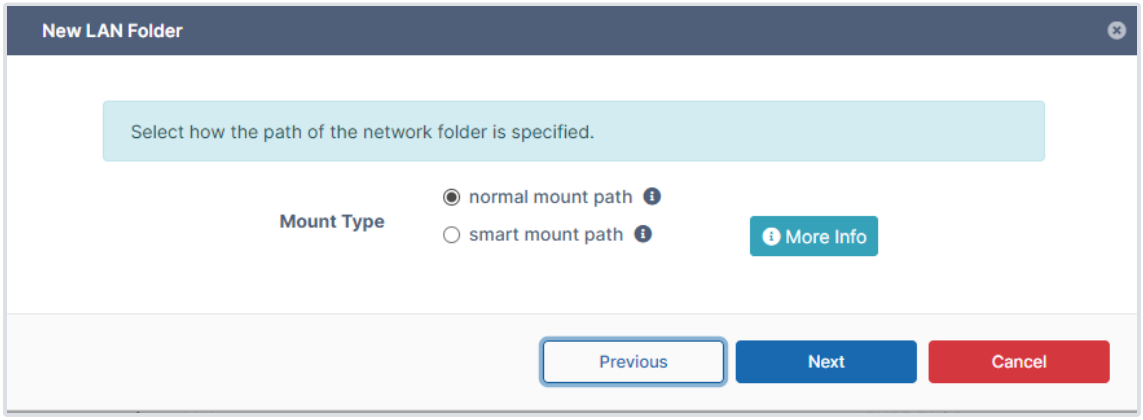
1. Log in to the FileCloud admin portal.
2. Navigate to **Network Folders** in the left navigation panel.
3. Click **Add** to launch the **New Network Folder** dialog box.
4. Select **Local Area Network** from the dropdown.



5. Enter the name of the network share. This will be the name shown to the user to access this network share resource. For example, "Training Docs". This name can only contain alphanumeric characters.



6. Select whether you want to use a normal mount path or a smart mount path. Read more about smart mounts.



7. For normal mount paths select the remote folder to use as the network share

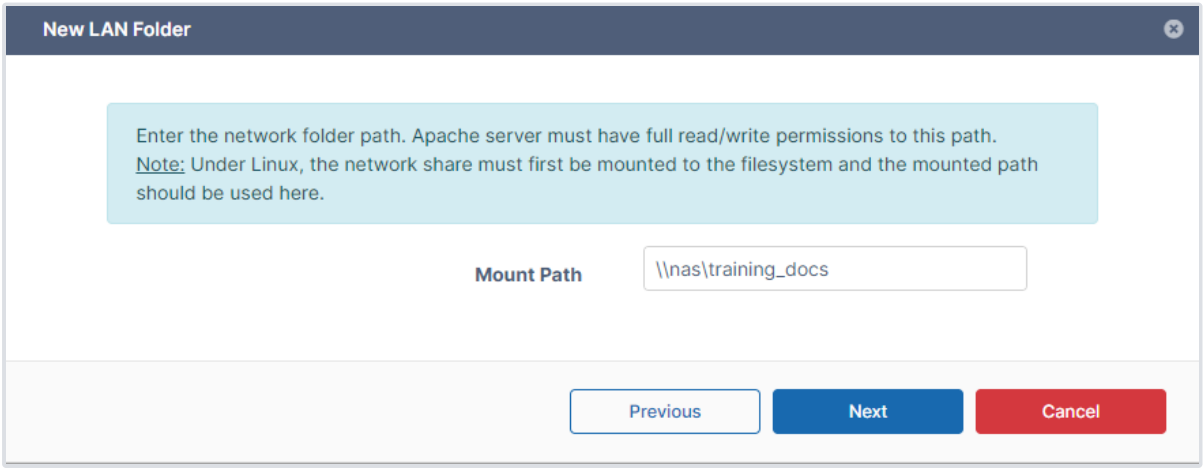
The FileCloud Web Server, fcorchestrator, cron, and Document Preview services must run as accounts with full permissions on that folder. See Web Server Permissions for Network Shares

Note: When using UNC paths (Paths like \\computername\sharename) set FileCloud to run as a service and set the log-on account for the service to the admin user that has access to that UNC share path.
Otherwise the network share cannot be added.

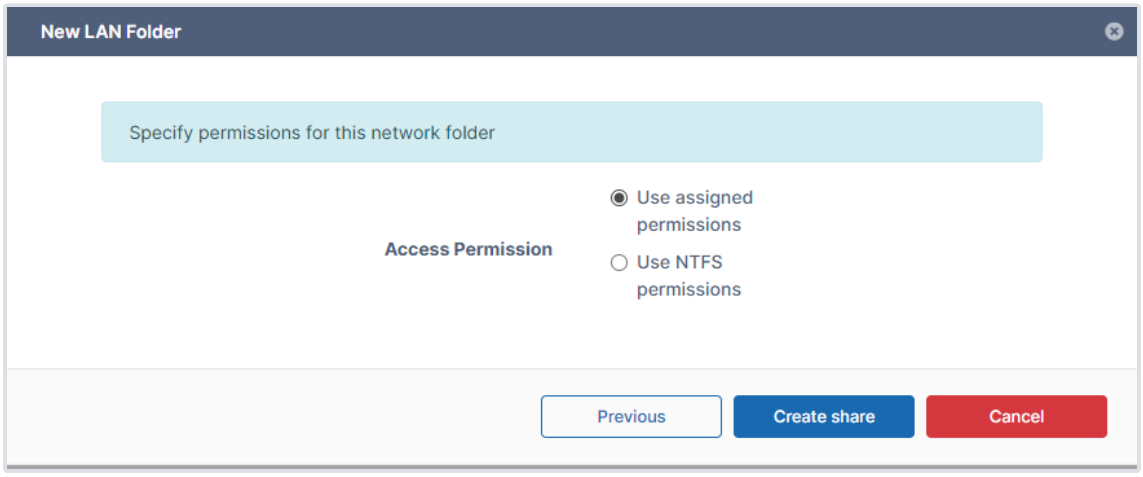
When adding Network Shares to FileCloud Server in a Windows Environment please note that file paths cannot exceed 260 characters, due to a PHP limitation. If you want to find out if you have files with a path greater than 260 you can use a 3rd party tool like Path Length Checker, which will read all the files from a specific location and show you which files are passing this restriction, you can visit the following link and download the tool:
https://pathlengthchecker.codeplex.com/

Network Folders function to give FileCloud users who are assigned to them access to their content; when you enter the **Mount Path**, please be careful to avoid entering:

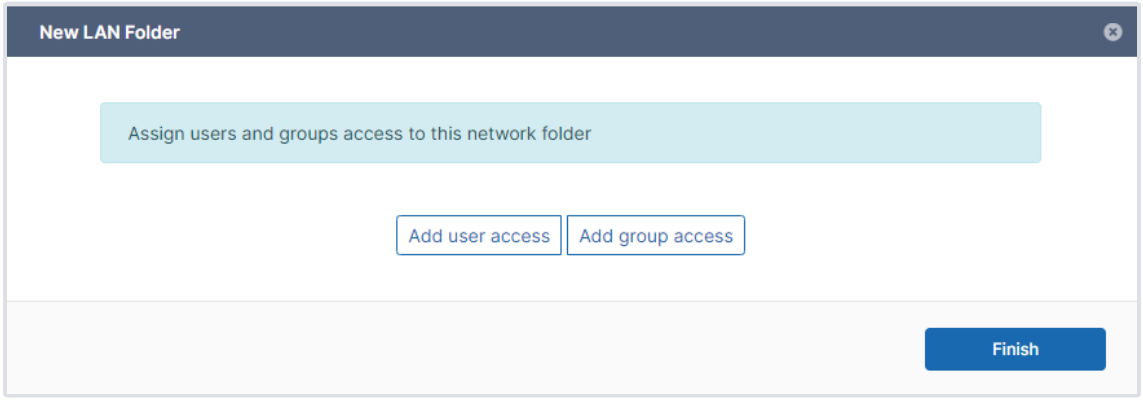
- an internal mount path that exposes internal secure documents related to servers and configurations.
- an internal mount path that contains documents required to remain inaccessible to users given Network Folder permissions through FileCloud.



8. Choose the access permission option.
   Assigned permissions specifies that FileCloud's permissions are applied to restrict user access. NTFS permissions specifies that the existing NTFS permissions are used to restrict user access. See more information about setting Network Folders with NTFS Permissions.



9. Once the Network Folder is created, you can assign users and groups to this folder.
   Click **Add User Access** to include users; click **Add Group Access** to add groups.



10. Click **Finish** to create the folder.

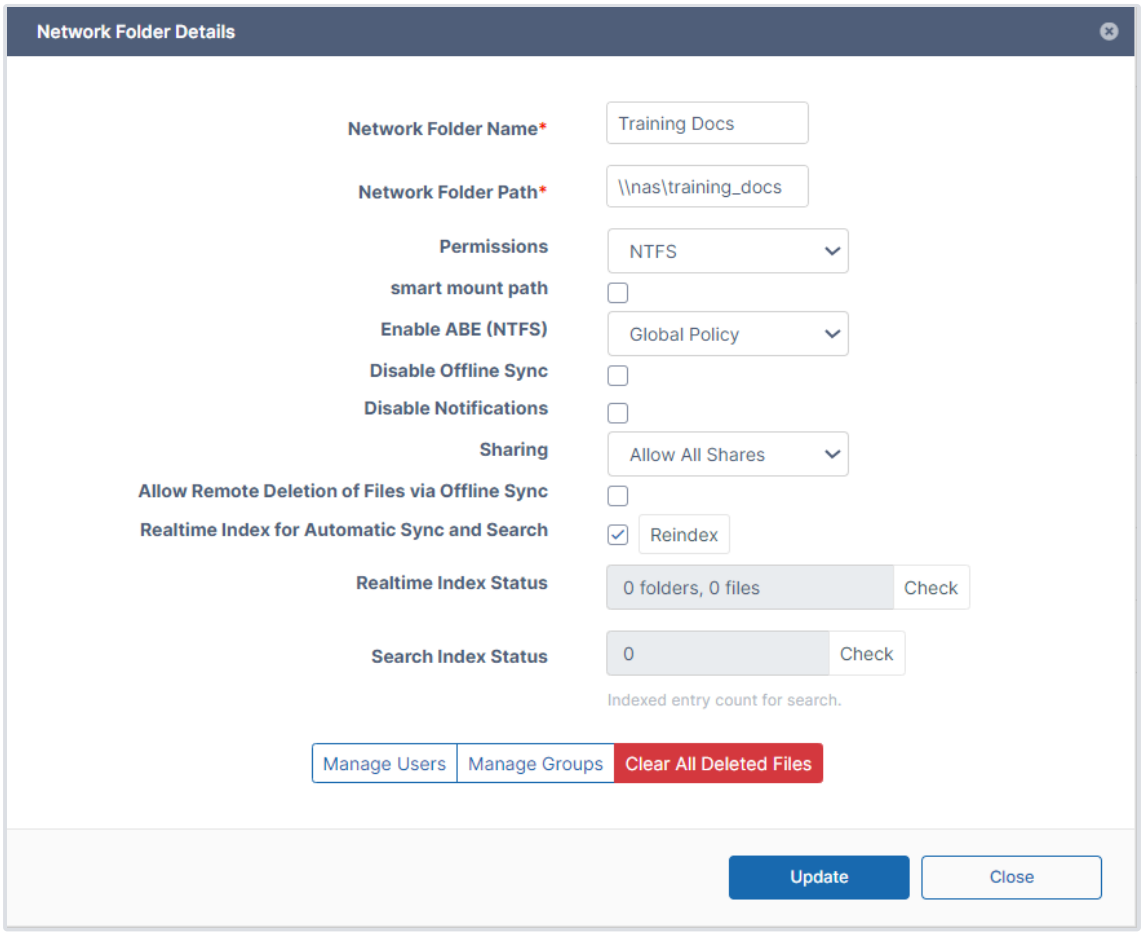
Granting access to Network Folder

After the network share is created, you may add and remove user access to it.
The network share access can be granted to Full users, Guest users or User Groups.

FileCloud licensing doesn't allow adding External users to network shares. To add External users to a network share, the folder has to be shared by another user directly to the External user and not by the admin.

To grant access to a network share:

1. Click **Network Folders** in the left navigation menu to display the list of available network shares
2. Click the Edit button for a network share entry to add user or group access
3. Click **Manage Users** or **Manage Groups** at the bottom of the **Network Folder Details** panel.



4. Set the appropriate Access level
   Available access levels:
   - Full Access - The user can read, write and share the contents of the share. Note that for a user to be able to sync a network folder, the user must have Full access.
   - Read Access - The user can only read (no write and share) the contents
   - NTFS Access - The permissions are extracted from the actual Windows NTFS permissions and user actions are restricted based on those permissions. See more information.

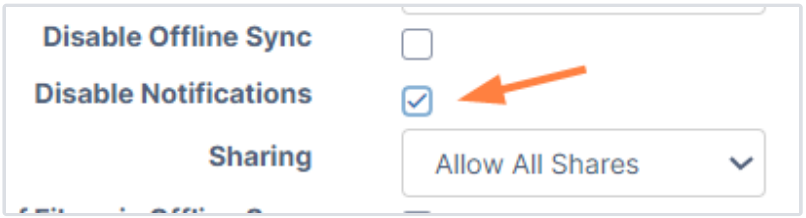
Notifications for Network Folders

By default, notifications are enabled for network folders. This means that all users who have access to a network folder and have notifications enabled receive notifications about all actions on the folder.

However, since multiple users may have access to the same network folder, users may receive notifications about actions that aren't relevant to them.

There are various ways you can limit their access to these notifications. First disable notifications for the folder, and then override the setting only for notifications that you want to permit.

1. Disable notifications for the folder:
   a. Click **Network Folders** in the left navigation menu to display the list of network folders
   b. Click the **Edit** button for the network folder.
   The **Network Folder Details** dialog box opens.
   c. Check the **Disable Notifications** box.



2. Click **Update**.
3. Do one of the following:

- **Leave all notifications about actions in the folder disabled.**
  By default, admins and users can override this setting. An admin can enable notifications about the folder for specific users, or users can enable their own notifications for the folder.
  If you do not want users to be able to override this setting, you must disable file change notifications in **Settings > Misc > Notifications**. See Notifications for File Changes for help.

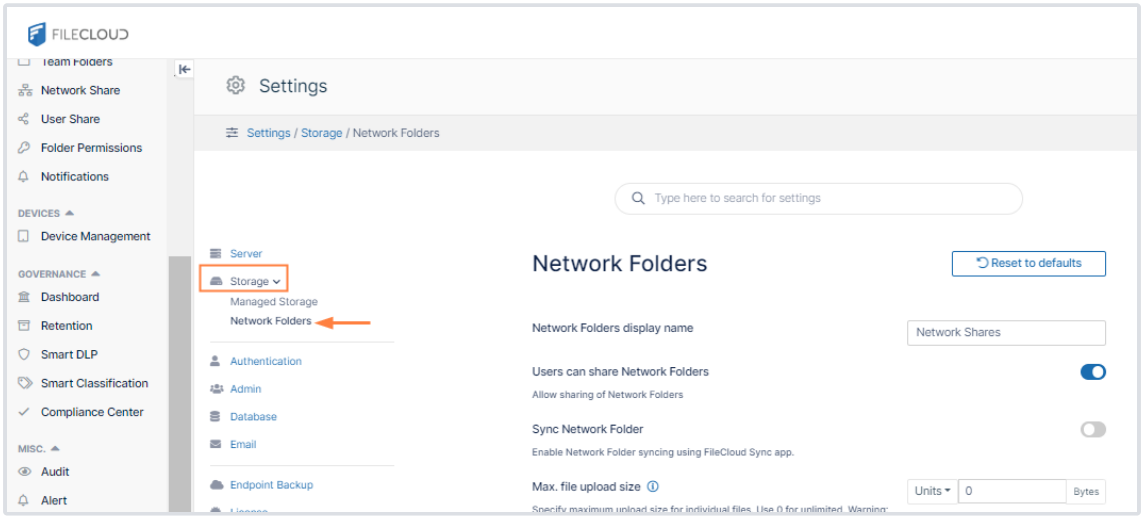
- **Enable notifications about the folder for specific users.**
  This is useful if you want to limit the users who receive notifications about a network folder to those you have shared it with.
  See the various options for setting users' notifications in the section Managing User-Defined Notifications.

- **Allow users to enable their own notifications about the folder.**
  See the options users have for setting their own notifications in the section Notifications.

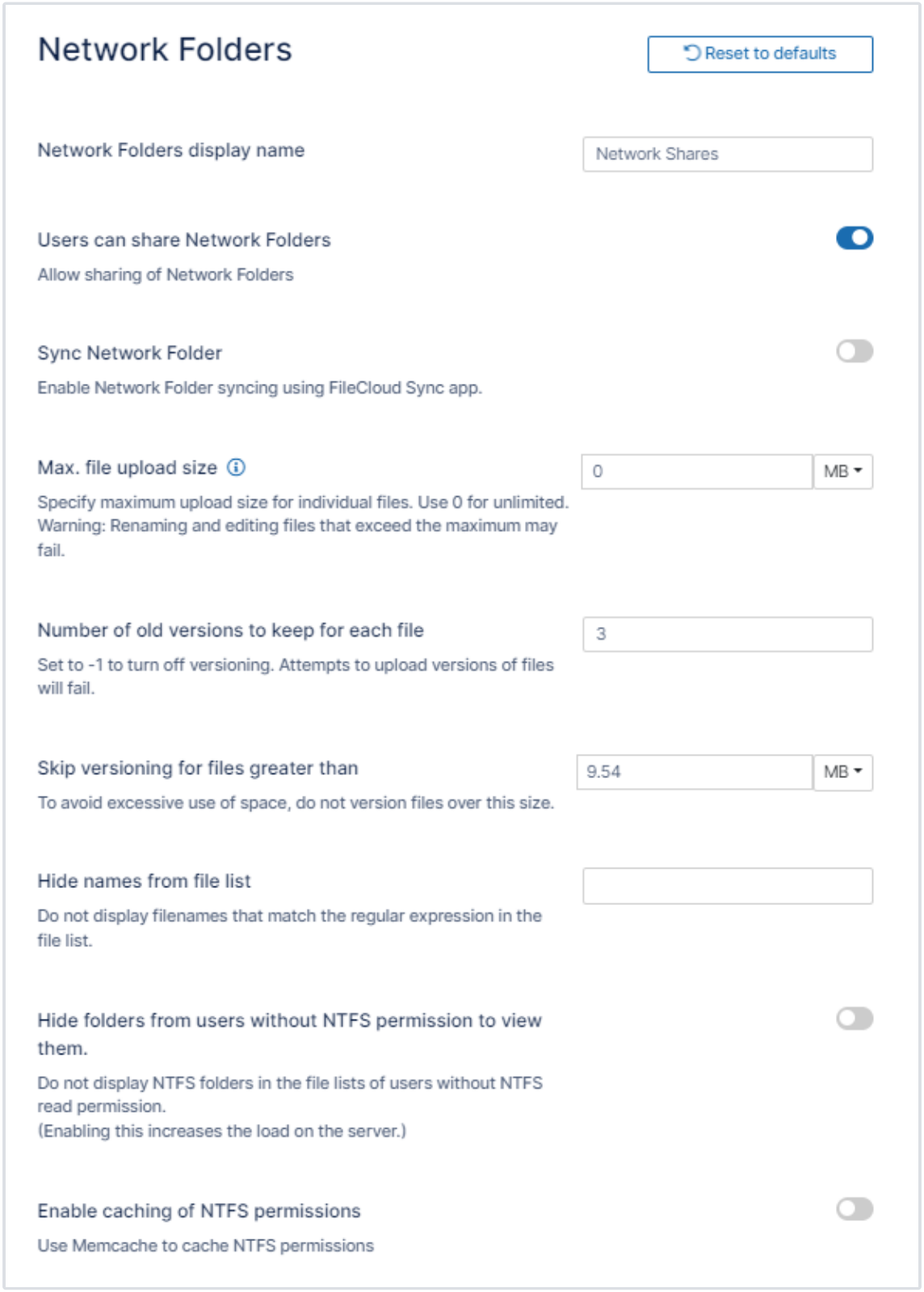
Configuring Network Folder Behavior

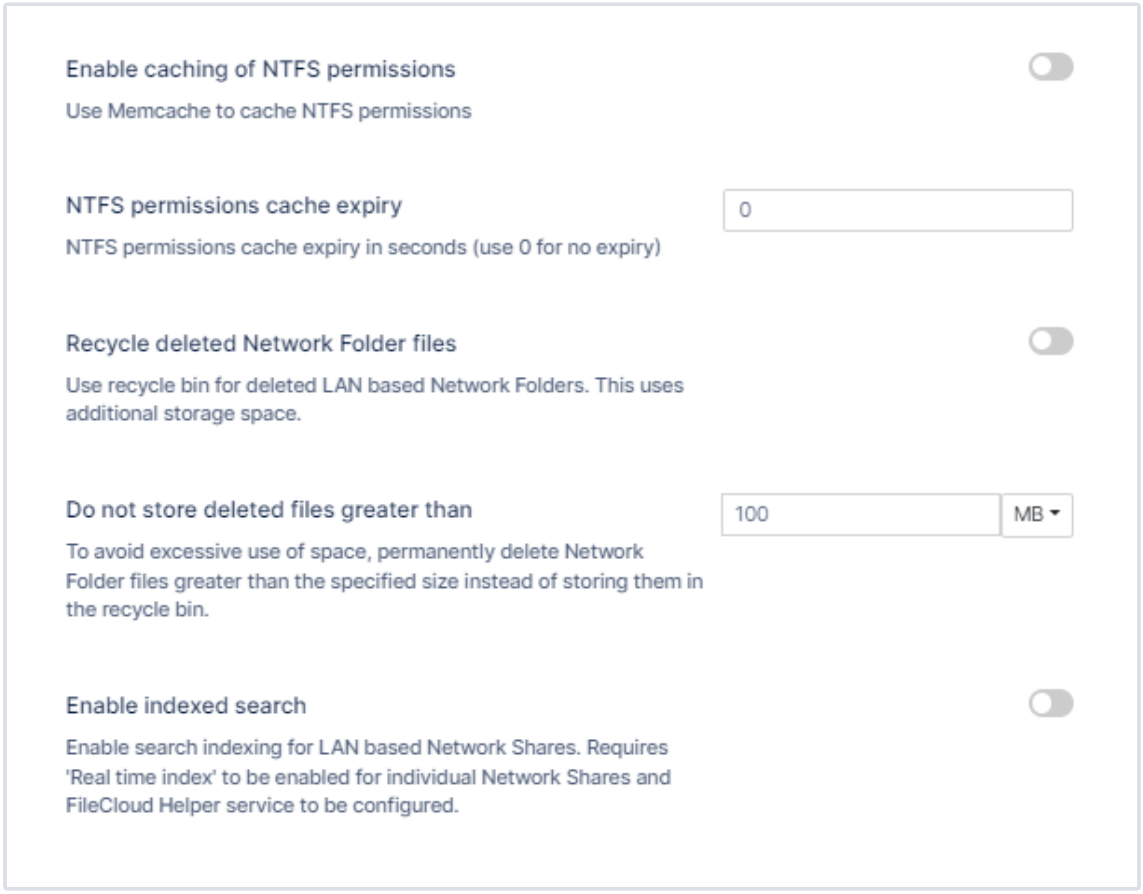
You can configure some of the behaviors of Network Folders in the storage settings for Network Folders.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
2. In the inner navigation bar on the the left of the Settings page, expand the **Storage** menu, and click **Network Folders**, as shown below.



The Network Folders settings appear as:


Network Folders
Reset to defaults
Network Folders display name
Network Shares
Users can share Network Folders
Allow sharing of Network Folders
Sync Network Folder
Enable Network Folder syncing using FileCloud Sync app.
Max. file upload size
0
MB
Specify maximum upload size for individual files. Use 0 for unlimited.
Warning: Renaming and editing files that exceed the maximum may fail.
Number of old versions to keep for each file
3
Set to -1 to turn off versioning. Attempts to upload versions of files will fail.
Skip versioning for files greater than
9.54
MB
To avoid excessive use of space, do not version files over this size.
Hide names from file list
Do not display filenames that match the regular expression in the file list.
Hide folders from users without NTFS permission to view them.
Do not display NTFS folders in the file lists of users without NTFS read permission.
(Enabling this increases the load on the server.)
Enable caching of NTFS permissions
Use Memcache to cache NTFS permissions



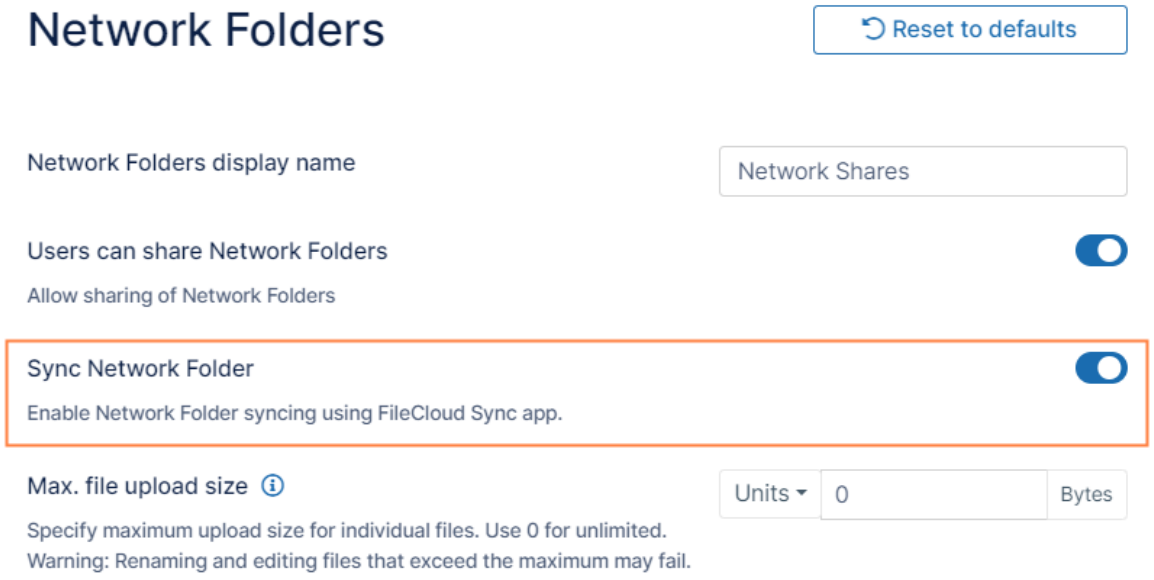
3. Fill in the settings as described in the following table.

Function	Description
Network Folders display name	This label appears in the User portal when the user logs into their account. Please Note: Once set up, don't change it as this will affect existing sync apps that have started syncing. Existing sync apps will continue to sync to the older name and only new network shares configured via Sync will use the new name.
Users can share Network Folders	This setting controls whether a network share location can be shared by a user
Sync Network Folder	This setting controls whether or not a network share location can be synced by a user using Sync client for offline access. You can disable offline sync for individual network folders as well. See Sync Network Folders for Offline Access for more information about syncing network folders.
Max. file upload size	Limits file size when uploading in Web clients. By default, this setting is not honored in Sync and Drive. It could affect folders that are renamed in Sync, since they are deleted and reuploaded during rename operations. Use 0 to allow files of any size.

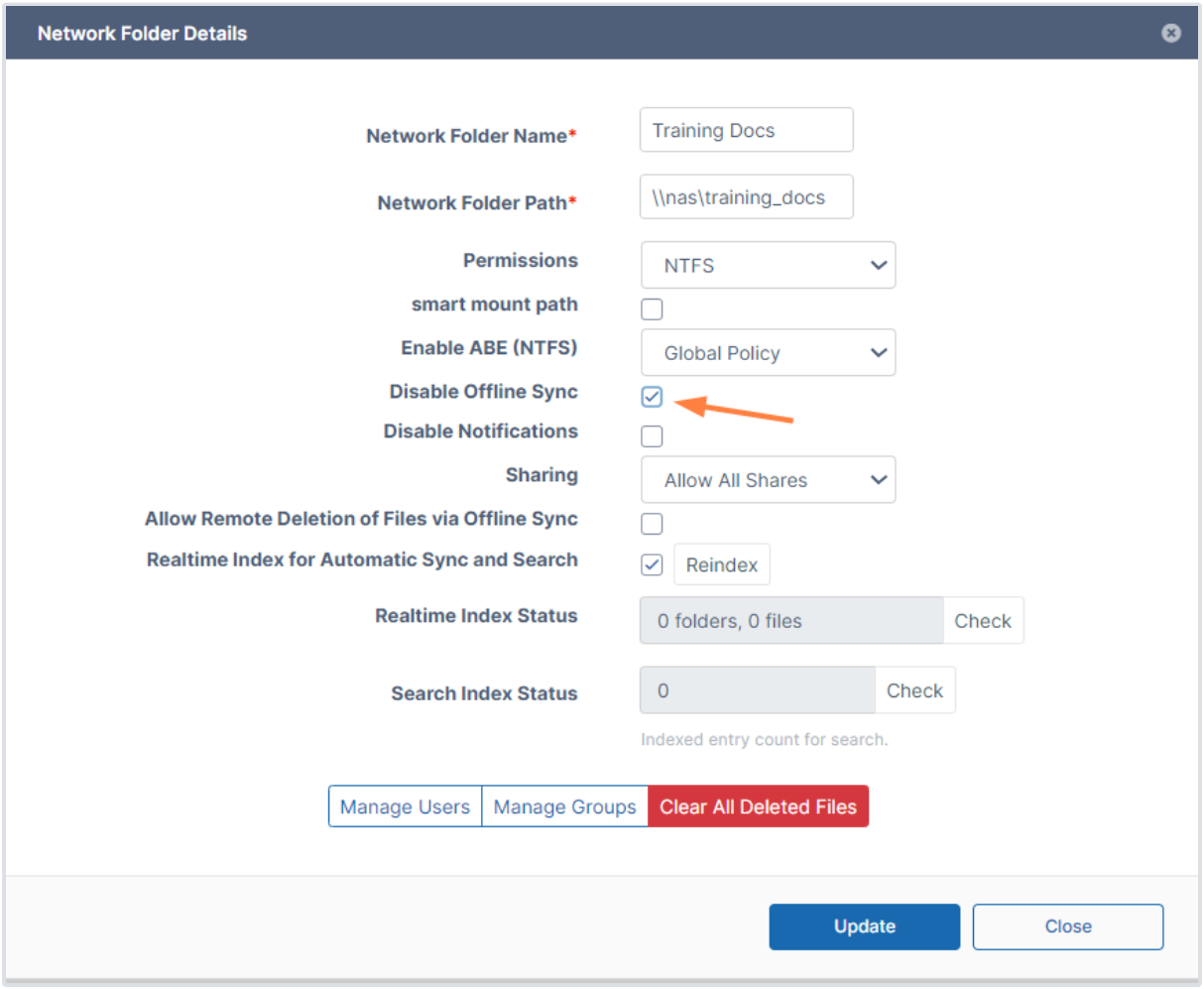
Function	Description
Number of old versions to keep for each file	Enables versioning and specifies the maximum number of versions of files in network location. To disable versioning, set to -1; attempts to upload versions of files will fail.
Skip versioning for files greater than	The file size limit in bytes beyond which the versioning will not be applied
Hide names from file list	This regular expression (regex) filters matching files from the file listing. For example, the regular expression /(sub.*|copy.*)/ filters out all files that start with "sub" or "copy"
Hide folders from users without NTFS permission to view them	When browsing network folders with NTFS permissions, folders that users don't have read access to are hidden from view. Enabling this increases the load on the server.
Enable caching of NTFS permissions	Enable this to use Memcache to cache NTFS permissions.
NTFS permissions cache expiry	Number of seconds after which NTFS permissions are no longer cached in the system.
Recycle deleted Network Folder files	Enable this to store deleted files from Network Folders in the recycle bin.
Do not store deleted files greater than	Do not store files greater than this size in the recycle bin.
Enabled indexed search	Enable indexing of Network Folders for fast searching. See Searching in Network Folders for more information.

Offline Access to Network Folders

The FileCloud Sync app can provide offline access to Network Folders by allowing users to download files from Network Folders automatically.
To enable Offline Access, you need to enable the **Sync Network Folder** option.



See how to configure Offline Access to Network Shares in the FileCloud Sync app.
You can disable offline sync of certain Network Folders. Edit a network folder and enable the checkbox to Disable Offline sync.



Sharing Restrictions on Network Folders

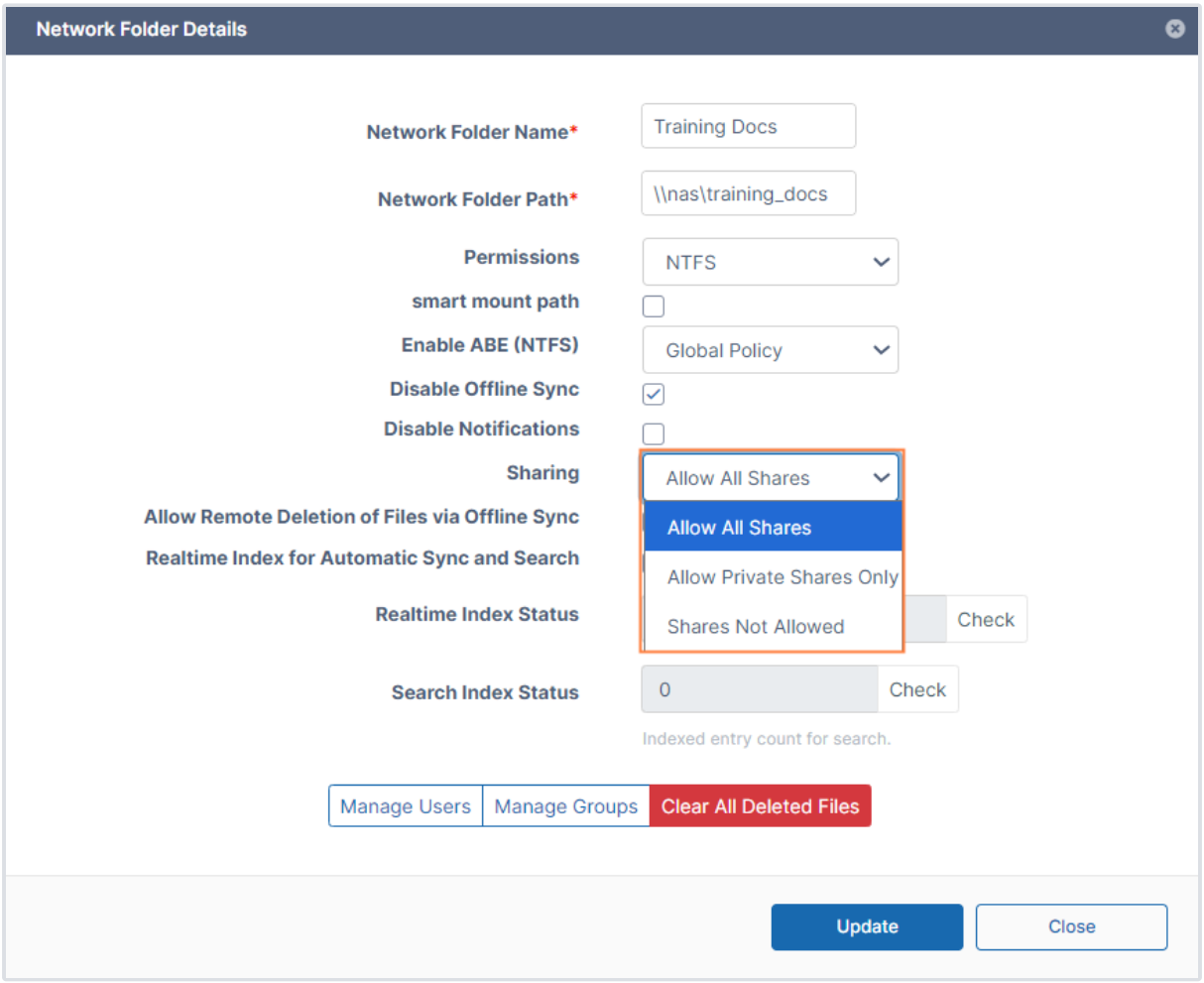
To restrict sharing for a Network Folder:

1. Navigate to **Network Folders** in the admin portal, and click **Edit** for the respective Network Folder.
2. In the **Network Folder Details** dialog box, set **Sharing** to **Shares not allowed**.
3. Click **Update**, now the Network Folder cannot be shared.

The following sharing options are available:

Sharing Options	Notes
Allow All Shares	Allow public and private sharing of the Network Folder

Sharing Options	Notes
Allow Private Shares Only	Allow only private sharing of the Network Folder
Shares Not Allowed	Restrict both public and private sharing for Network Folder



Disabling Network Folders

To disable Network Folders:

1. Open cloudconfig.php.
   - Windows Location : C:\xampp\htdocs\config\cloudconfig.php
   - Linux Location : /var/www/html/config/cloudconfig.php
2. Find the following setting, or if it does not exist, create it:

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

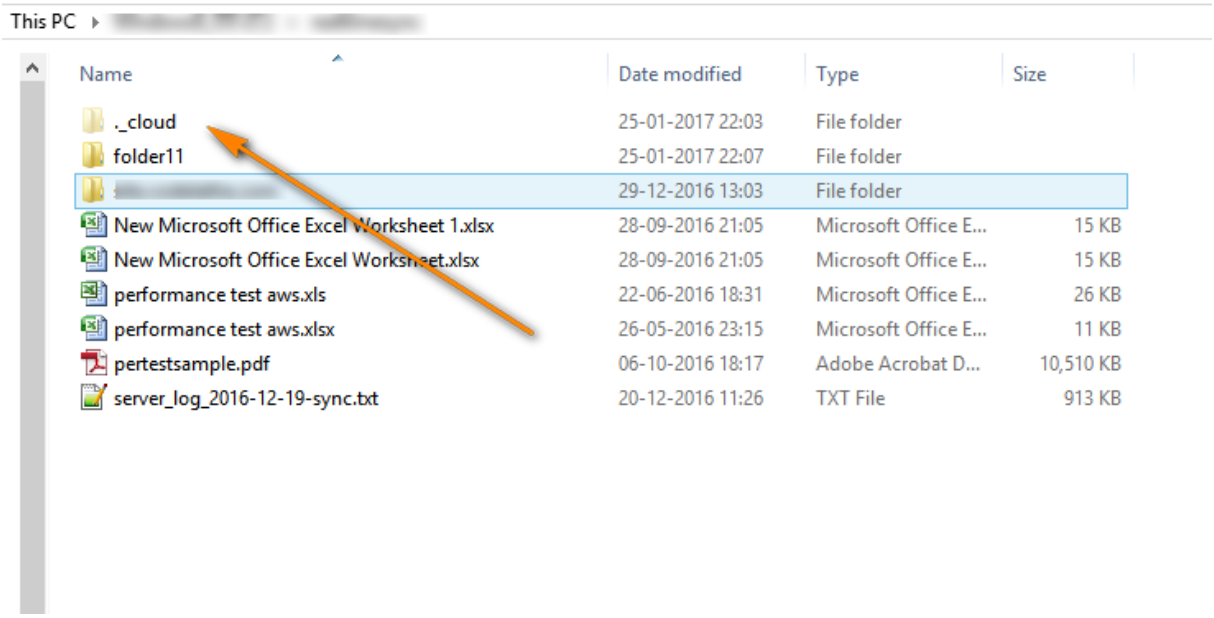
3. Change the value **true** to **false**.
4. To re-enable Network Folders, change the setting back to **true**.

Miscellaneous: ._cloud Folder

Network folders at times will create a **._cloud** subfolder for the following reasons:

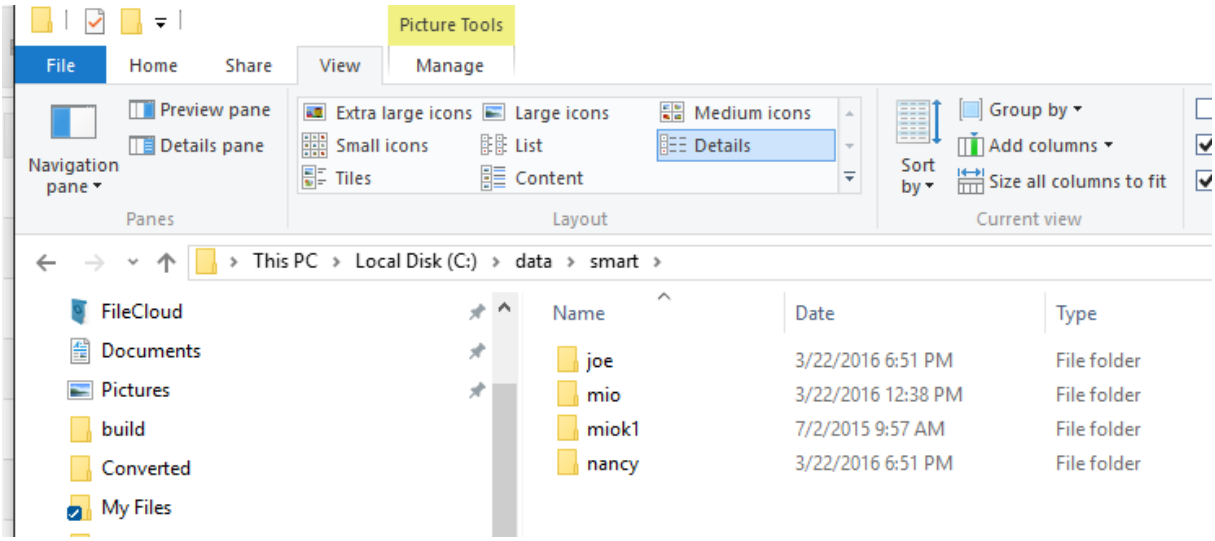
- To store previous versions of files
- To store the deleted files under that Network Folder
- To store image thumbnails.

There is no option to automatically delete the ._cloud folder. However, the previous versions of the files can be deleted by the user, and an administrator can permanently remove deleted files by using **Clear All Deleted Files**, shown above. Even if thumbnails are deleted, FileCloud recreates them automatically the next time an image is accessed.



Smart Mounted Network Folders

Smart mounts are a special type of network share whose file system paths contain variables. The variables are resolved to the actual file system path. This will greatly simplify access to network shares as long as certain criteria is met.
For example, take a look at the following image showing a folder structure in the File System.



In the folder structure shown in the image above, the Administrator can configure the Network share in such a way that:

- When user **joe** logs in, he will be able to see **c:\data\smart\joe** and no other folder
- When user **alexis** logs into FileCloud, she will only be able to see and access **C:\data\smart\alexis**.

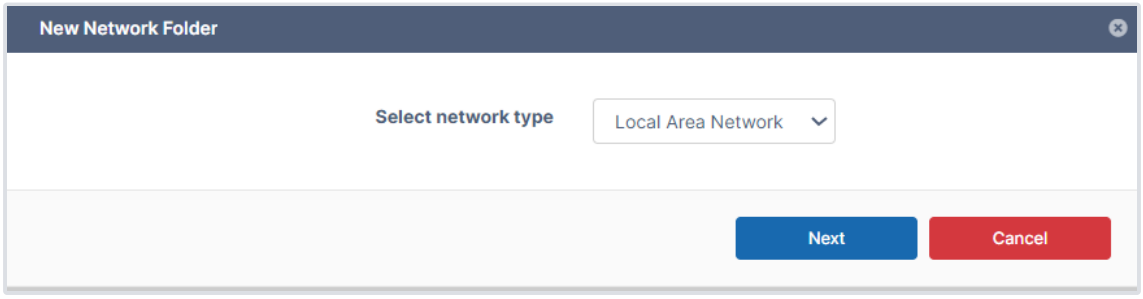
To achieve this, create a network share with smart mount path such as **C:\data\smart\%USERID%**. The system will automatically replace the **%USERID%** variable with the actual user name and mount it to the network share for the user to access.
The following special tokens can be inserted in the smart mount parameter

PATH PATTERN SPECIAL VARIABLES	NOTES
%USERID%	User id as a variable in path
%EMAILID%	Email id as a variable in path
%DISPLAYNAME%	User display name as a variable in path

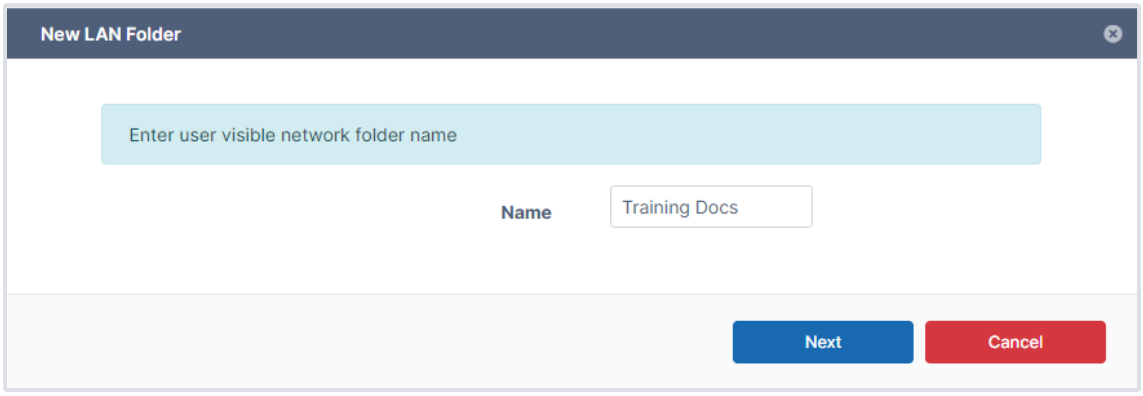
Creating a smart LAN-based network folder

To create a smart mount network share:

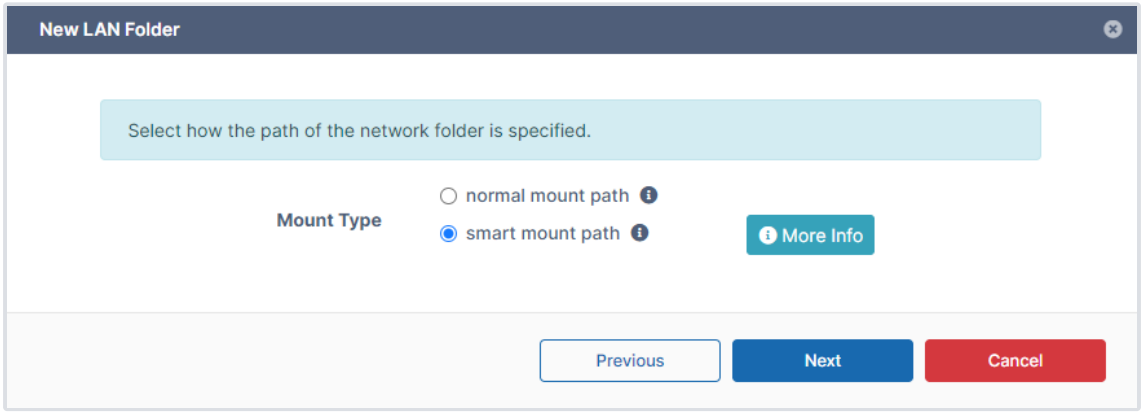
1. Log in to the FileCloud admin portal.
2. Navigate to **Network Folders** in the left navigation panel.
3. Click **Add** to launch the **New Network Folder** dialog box.
4. Select **Local Area Network** from the dropdown.



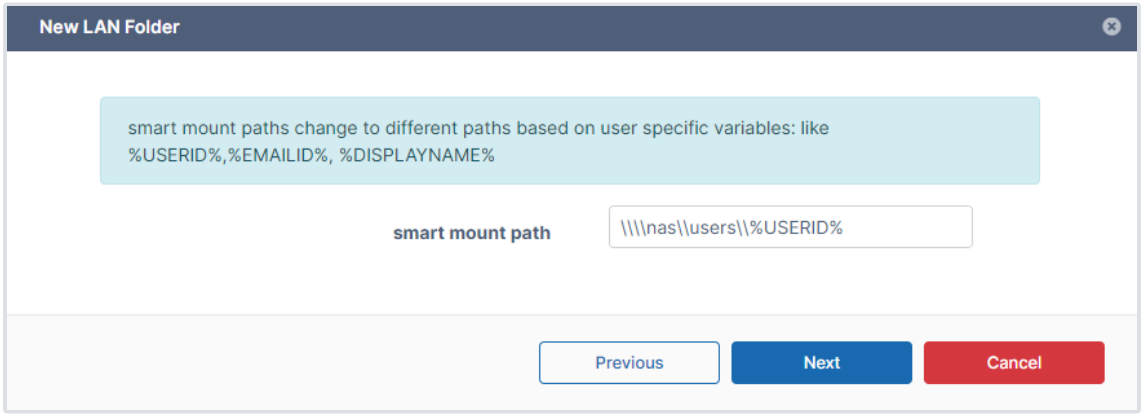
5. Enter the name of the network share. This will be the name shown to the user to access this network share resource. For example, "Training Docs". This name can only contain alphanumeric characters.



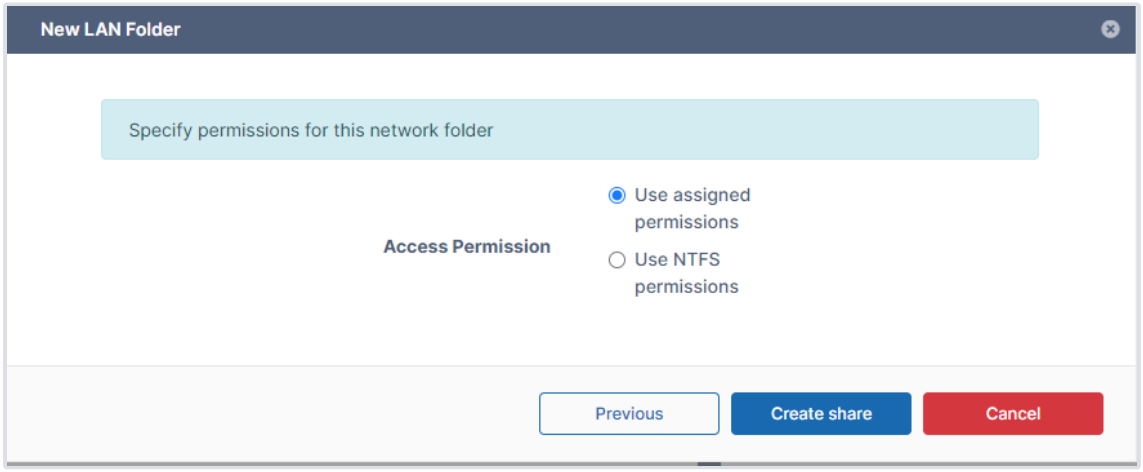
6. Select smart mount path.



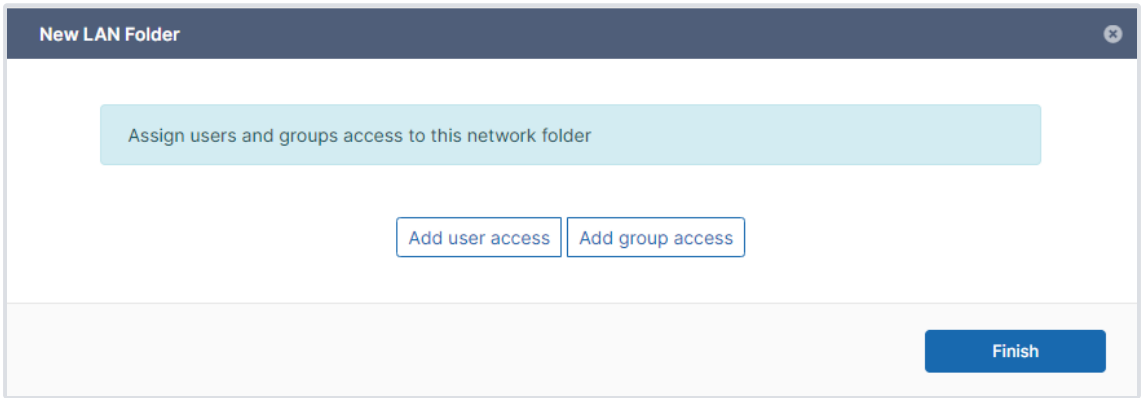
7. Click **Next**.
8. Enter the **smart mount path**.
   The path should have a variable, such as %USERID% that matches the path name.



9. Click **Next**.
10. Choose the **Access Permission** option.
    See Create a LAN-Based Network Folder for more information about this field.



11. Click **Create share**.
12. Once the Network Folder is created, you can assign users and groups to this folder.
    Click **Add user access** to include users; click **Add group access** to add groups.



13. Click **Finish** to create the folder.
14. To further configure the folder, see Create a LAN-Based Network Folder .

Network Folders with NTFS permissions

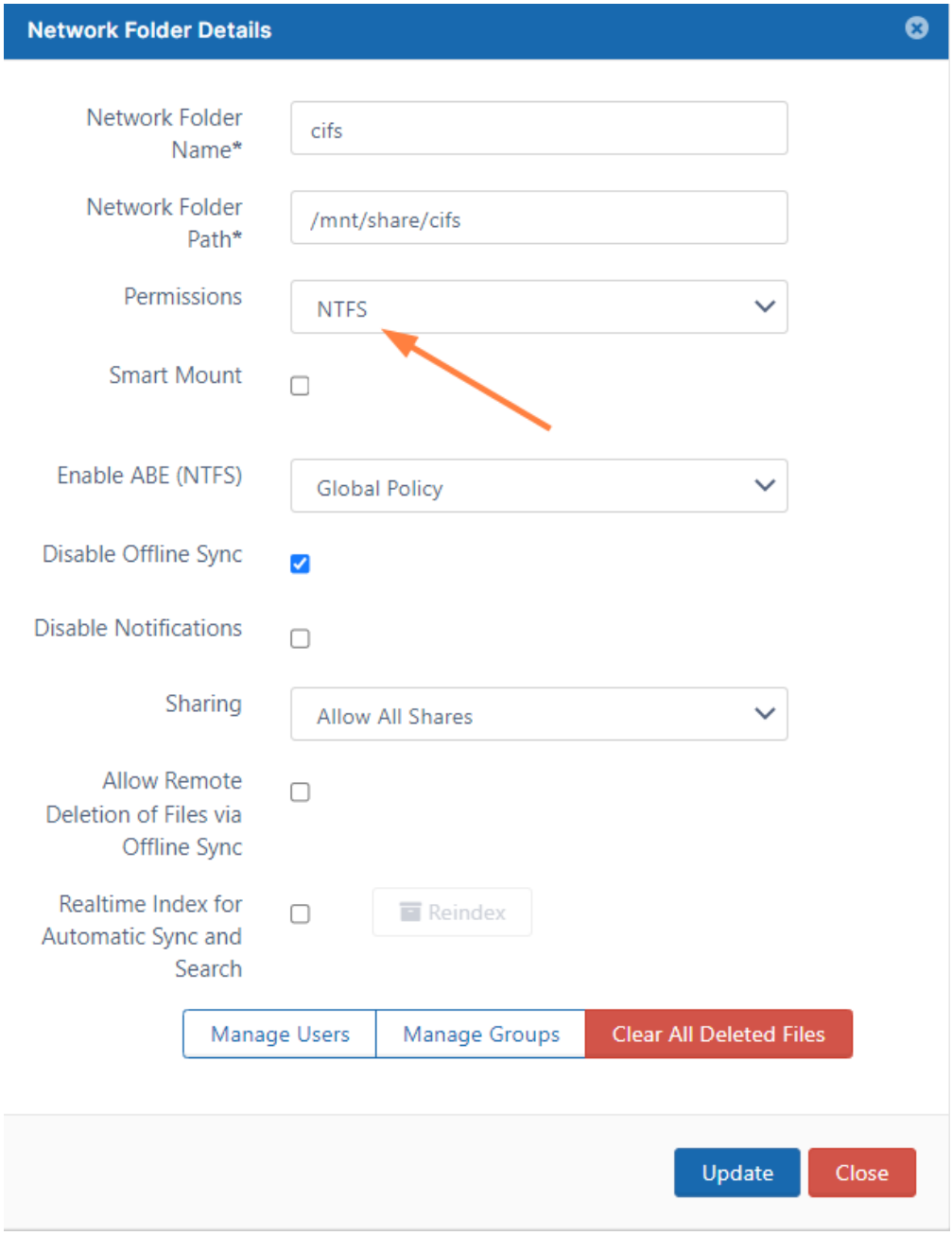
If you are using Network Folders with NTFS permissions:

- It is recommended that you run FileCloud on Windows Servers instead of Linux.
- Authenticate user accounts with Active Directory. Users with default authentication can't leverage NTFS permissions due to security issues.
- If you are running FileCloud on Linux, a Windows Server running the FileCloud Helper Service is required.
- Install and use memcache to improve performance.

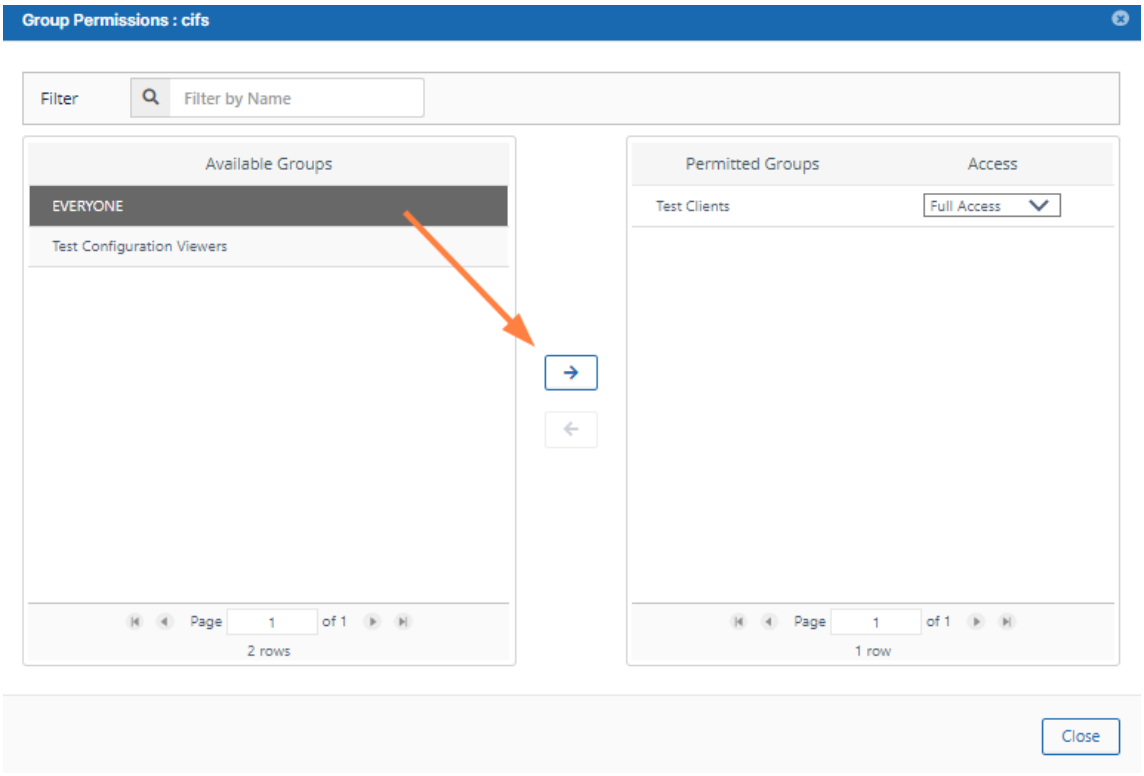
Many organizations have Windows based Network Folders that are shared with employees. The permissions on these Network Folders are managed using NTFS rights setup for various users and groups (usually from Active Directory). FileCloud can use the same NTFS permissions on the Network Folders for user authorization and access to these resources.

To setup a network Folder with NTFS permissions:

1. Set **Permissions** to **NTFS**.



2. Click **Manage Users** or **Manage Groups** and add users to the share as needed. For example, you might want to give the EVERYONE group access to the Network Folder. In this case even if the user has been given access to the share, they will only be able to view the share if they have NTFS permissions enabled.



3. If you are running FileCloud on Linux, you may need to **configure and install the FIleCloud helper service**.

Additional Information and Troubleshooting

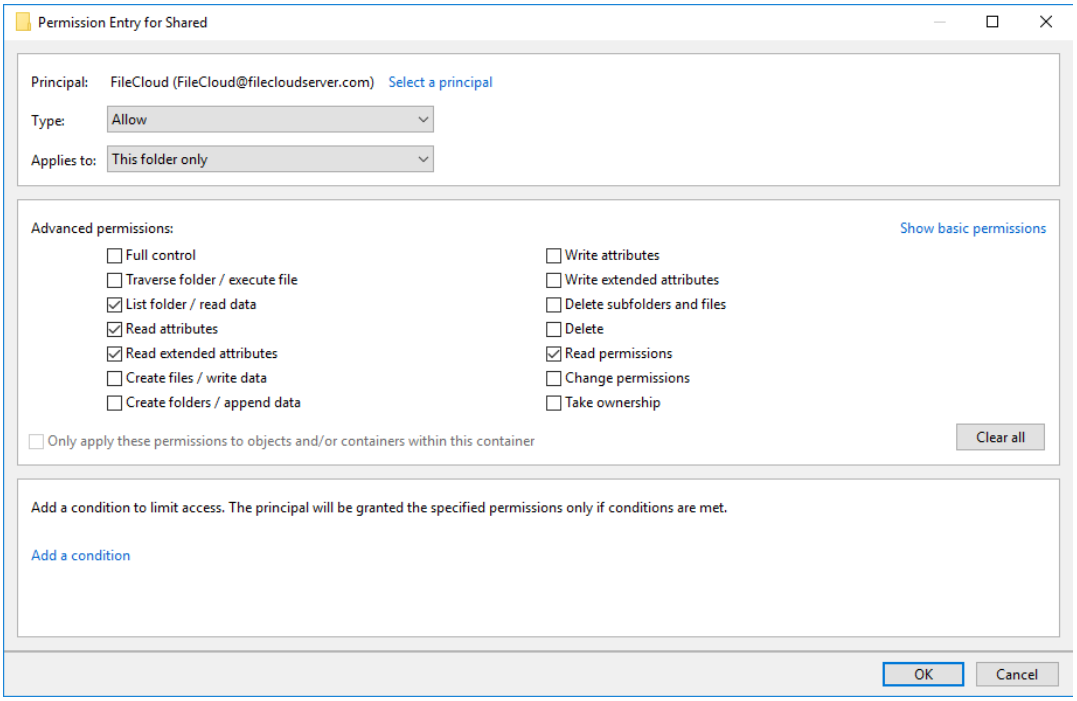
- When user membership in a AD group is modified, that change is not propagated immediately and is cached by Windows. As a result, if you change a user group membership, it might not be picked up NTFS helper immediately. It might take some time ranging from 10 minutes to several hours before the change is picked up. If you need the changes to be picked up immediately, you can restart the helper service.
- Make sure that don't have a local machine account name as the domain user account. This will cause problems.
- If you get **authzinitializecontextfromsid** errors, make sure the account running the Helper service has full permissions to look up user accounts, Also make sure the user account name is not the same as the computer name, use a different name.

FileCloud evaluates special permissions as well as standard permissions on Network Folders.

NTFS special permissions

When sharing a network folder with special permissions ensure that the options below are enabled. By enabling the options below the user will still be limited to have access
only to the folders or sub-folders the administrator allows however this grants the ability to FileCloud to read and display the needed information for that specific user.

NTFS permissions include both standard and special permissions. Standard permissions on a folder are Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Standard file permissions are the same, with the exception of List Folder Contents. Special permissions are considerably more granula.

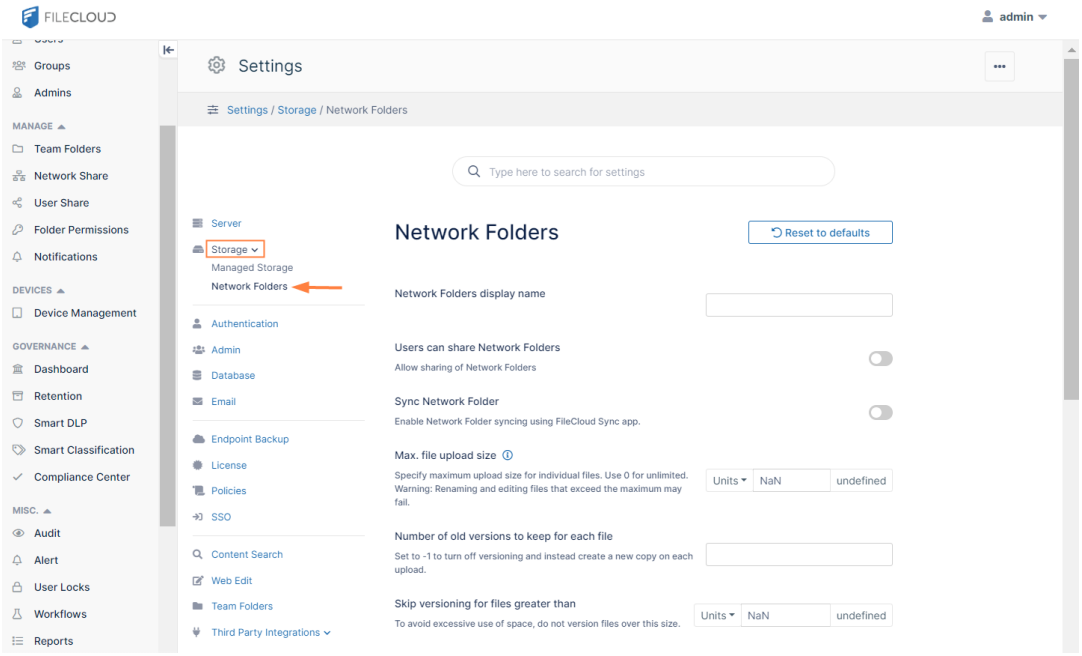


For Microsoft Documentation (https://technet.microsoft.com/en-us/library/2006.01.howitworksntfs.aspx)

NTFS Network Folders with Access Based Enumeration

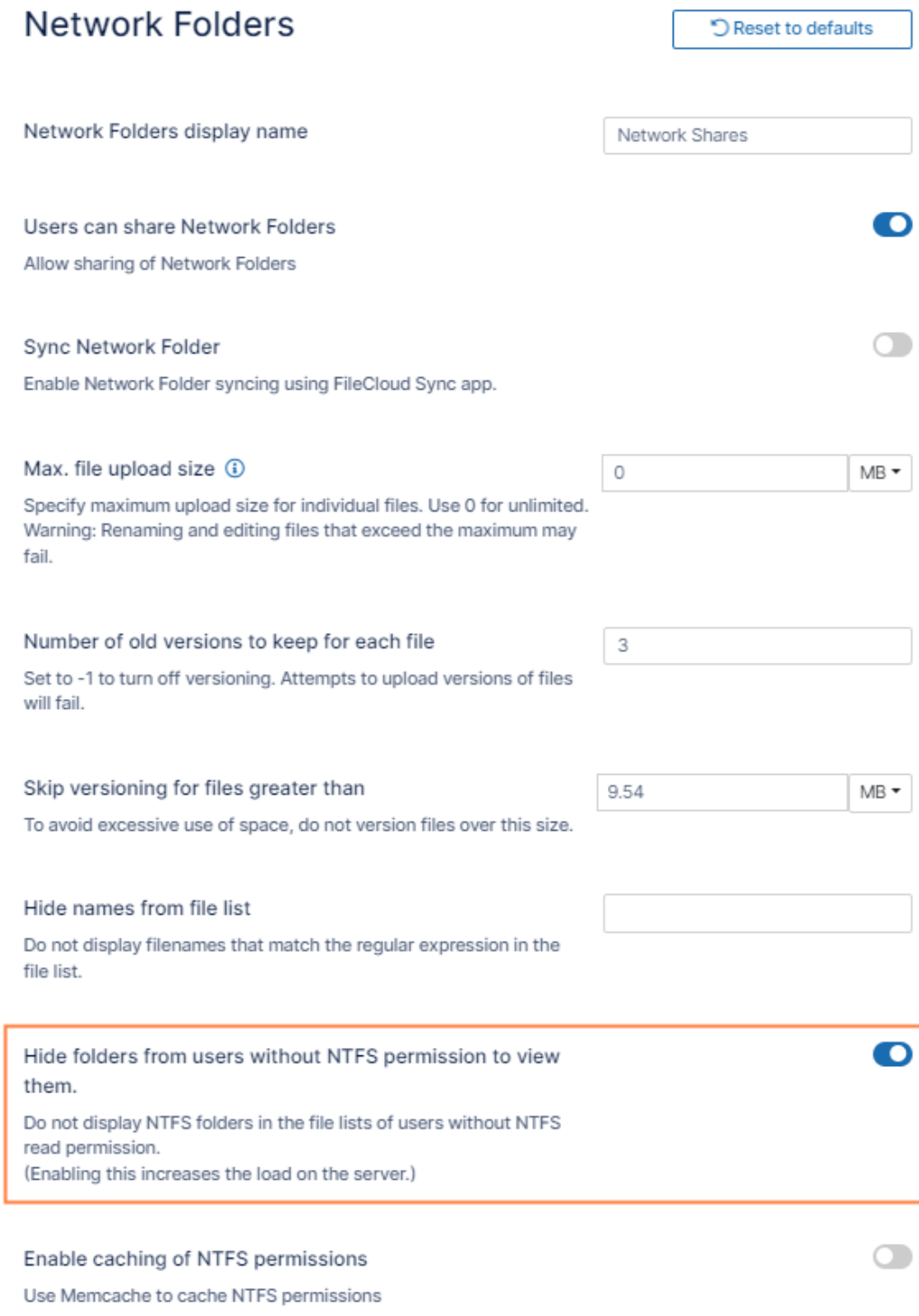
When using Network Folders with NTFS permissions, it is possible to automatically hide folders that users who don't have permission to view them.

1. Go to the **Network Folders** settings page.
   To go to the Network settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   b. In the inner navigation bar on the left of the **Storage** settings page, expand the **Storage** menu, and click **Network Folders**, as shown below.



The **Network Folders** settings page opens.

2. Enable **Hide folders from users without NTFS permissions to view them**, and click **Save.**

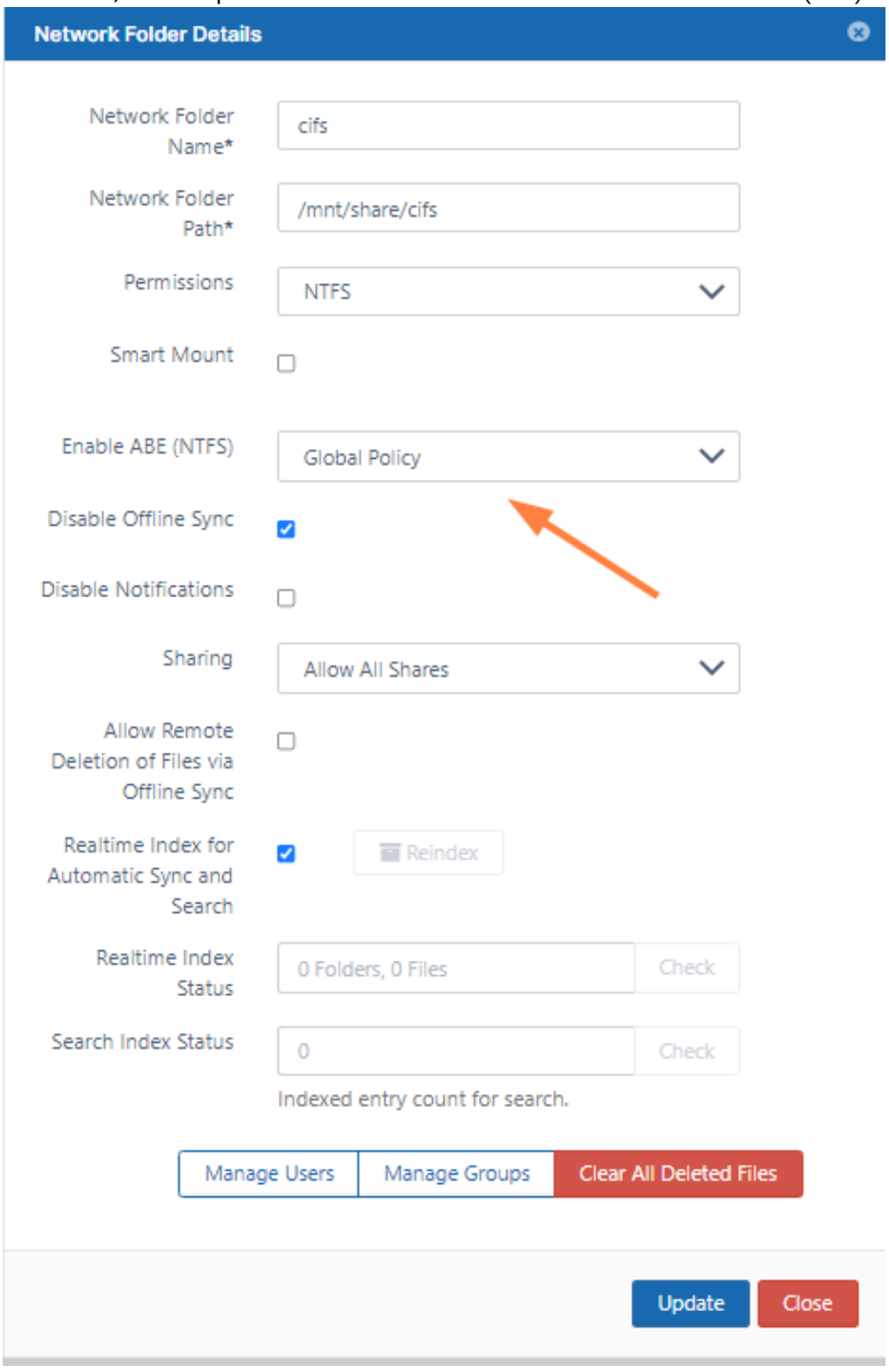


To disable or enable hiding specific folders from users without NTFS permissions to view them:

1. In the FileCloud navigation panel, click **Network Share**.

2. Edit the specific network folder.
3. In **Enable ABE (NTFS)** Select **Global Policy** to use the global setting, or choose **NO** or **YES** options to disable or enable hiding of this network share only from users without NTFS permissions to view it.

Note: Here, the view permission is referred to as **Access Based Enumeration** (**ABE**).



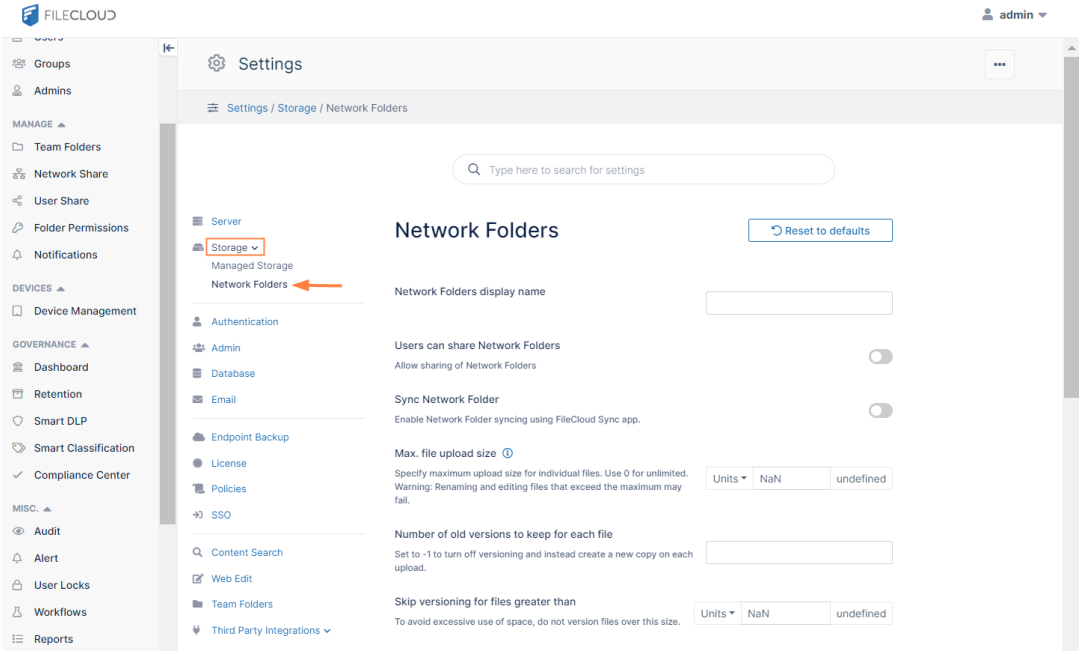
NTFS permission checks read the **tokenGroupsGlobalAndUniversal** attribute of the SID specified in the call to determine the current user's group memberships. To simplify granting accounts permission to query a user's group information, add accounts that need the ability to look up group information to the **Windows Authorization Access Group**. Please make sure to add the **Windows Authorization Access Group** to the **FileCloud Account Group** that you have created.

Improving performance of NTFS Network Folders

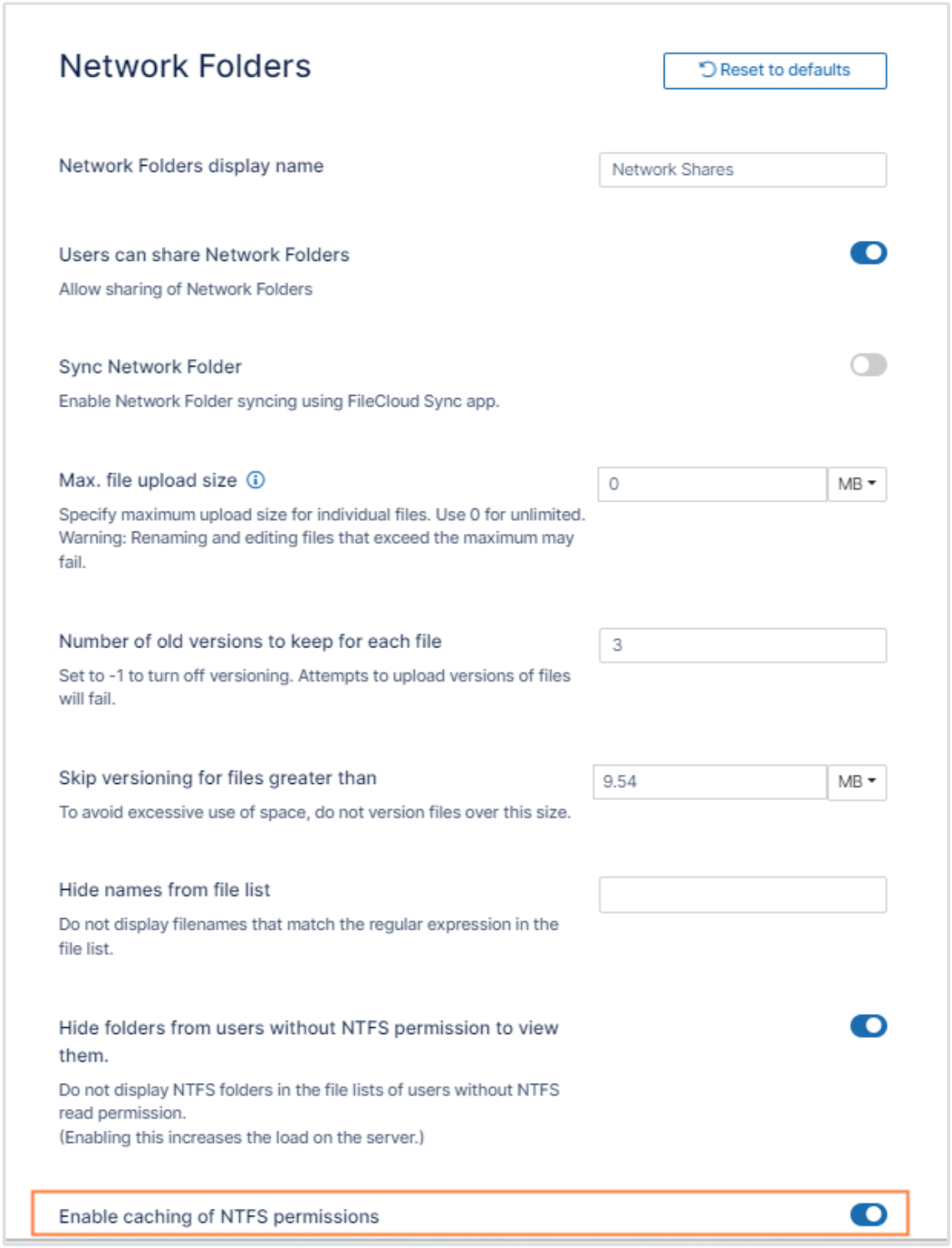
In general, extracting NTFS permissions for folders and files can add additional processing latency. To improve performance, you can enable caching of NTFS permissions.
This speeds up lookup of NTFS permissions by caching the permissions once accessed in the memcache server. For this caching to work, the memcache server needs to be installed and running. By default, once permissions are cached, they are stored until the memcache is restarted. If you are changing any NTFS Permissions and want FileCloud to pick up the new permissions, make sure to restart the memcache service.

To enable caching of NTFS permissions:

1. Go to the **Network Folders** settings page.
   To go to the Network settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   b. In the inner navigation bar on the left of the **Storage** settings page, expand the **Storage** menu, and click **Network**, as shown below.



   The **Network Folders** settings page opens.
2. Enable **Enable Caching of NTFS Permissions**, and click **Save**.



Guide to FileCloud Network folders with NTFS Permissions

Quick help on setting up NTFS network shares
This guide explains prerequisites and basic steps for setting up NTFS on your network files.

Common questions regarding NTFS FileCloud integration are also addressed in this page.

FileCloud Network Folders

Windows based Network Folders that are shared with the team are managed effectively by setting permissions on them. Network Folders are further managed using NTFS rights set up for various AD users and groups.

To set up Network Folders, see Setting Up Network Folders.

FileCloud can inherit the NTFS permissions on Network Folders for user authorization and access to these resources.

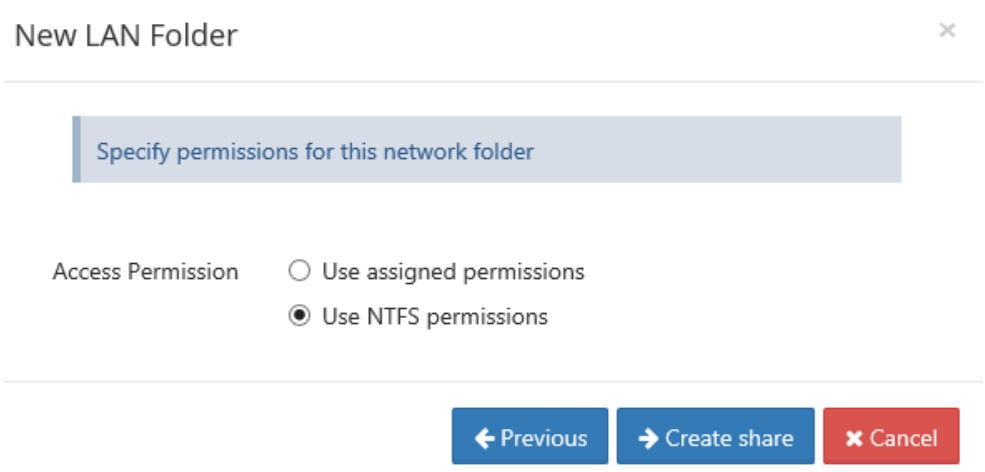
Pre-Requisites for NTFS setup

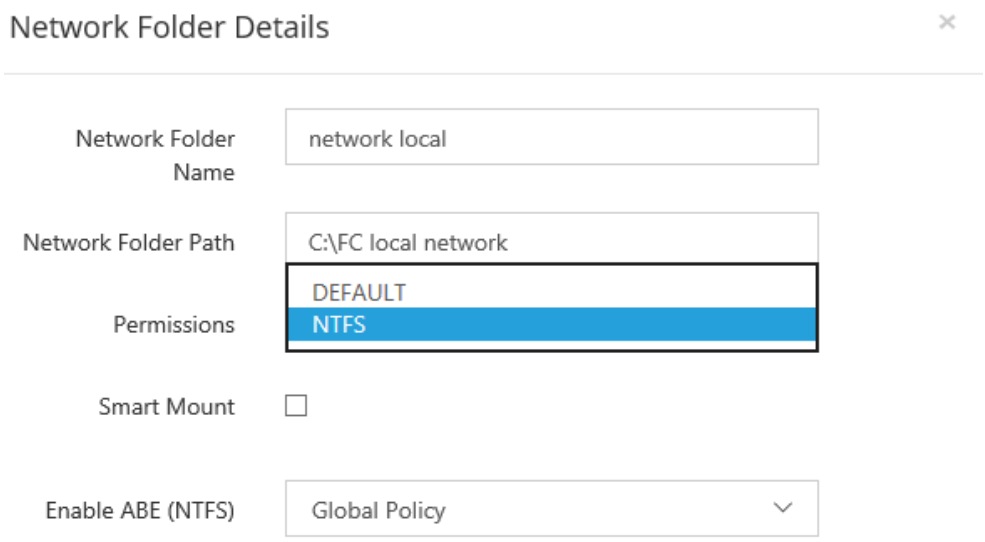
When Network Folders are added to FileCloud, permission needs to be set as NTFS. This uses all the NTFS permissions already set on the Network Share.

To set up Network Folders, see Setting Up Network Folders.

If your Web Server is running as a service, please make sure to it is running with a user account that has all permissions over the Network Share in NTFS.

Prerequisite 1: NTFS is applicable on Network Folders only if NTFS is selected for Permissions is during Network Folder creation.



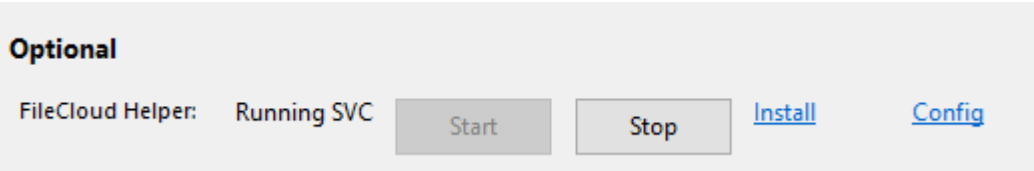


Prerequisite 2: FileCloud Helper service (optional)

> **Helper Optional**
> If you are running FileCloud on a Windows Server, you **do not need** the Helper Service for NTFS permission checks as the Web Server can perform access checks.
> If you are running FileCloud on a Linux Server, you **do need** the Helper Service to perform NTFS permission checks

The FileCloud Helper service performs:

- NTFS Permission checks for Network Folders configured with NTFS permissions on a Linux Server
- Indexed search of Network Folders in Windows and Linux Server
- Content search of documents in Network Folders in Windows and Linux Server



- For more information on FileCloud Helper service refer to: FileCloud Helper Service

Prerequisite 3: Assign users (AD Users)

The permissions on these Network Folders are managed using NTFS rights setup for various users and groups (usually from Active Directory).

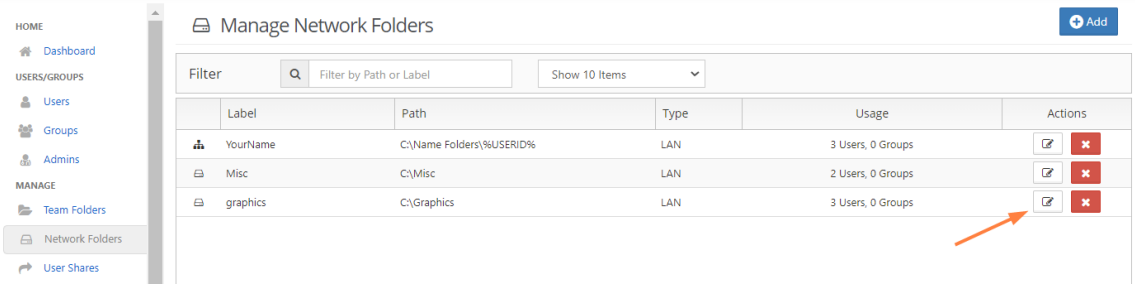
To set up AD users, see Active Directory Authentication

To give permissions:

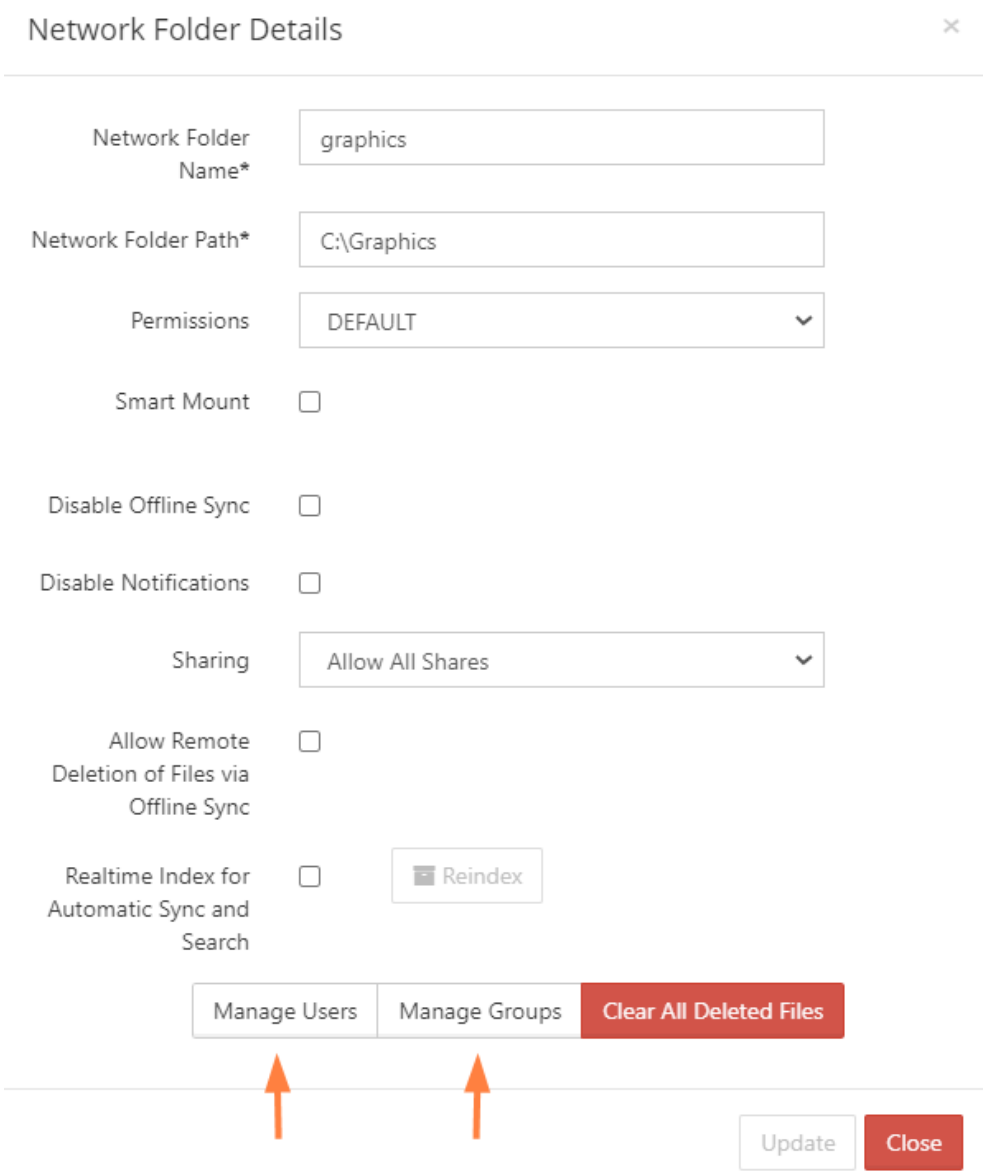
1. On the **Manage Network Folders** screen, click the

   icon of the network folder with NTFS permission.



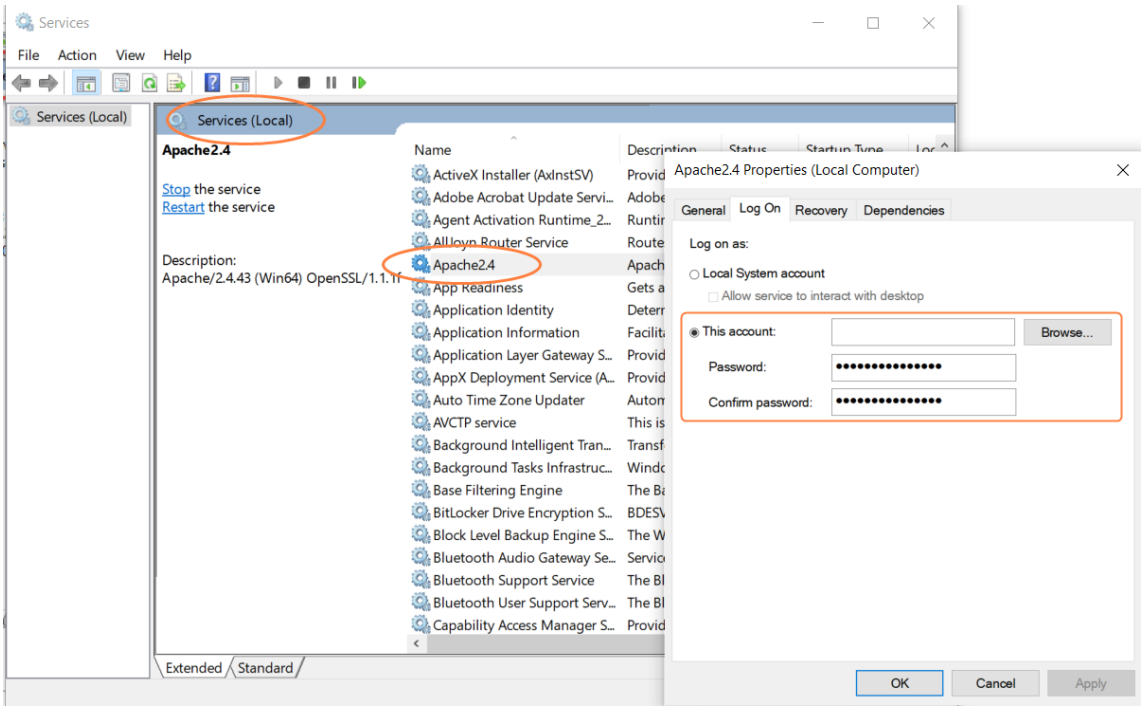
2. In the **Network Folder Details** dialog box, click **Manage Users** or **Manage Groups**.



3. Select users or groups that require permission for this network folder.
   Only the AD users in the group have access to contents.

Helpful information

1. **Does the Server where FileCloud runs have to be part of the domain?**
   If you run the FileCloud Web Server as a service, yes, the server has to be part of the machine, and the Web Server service has to be running as an AD user with all permissions on the Network Share.



2. **Are there any restrictions or limitations on Network Folders?**
   Yes, the path and file names together cannot be longer than 255 characters. This is a Windows restriction that the Server cannot override. Please refer to Limits in File System Functionality Comparison

> **Note:**
>
> Full path includes the name of the file to, for example: "C:\Users\Default\Downloads\sample.docx"
> If you want to find out if you have files with a path greater than 255 you can use a 3rd party path length checker, which will read all the files from a specific location and show you which files do not comply with this restriction.

3. **Can a regular user be given access to NTFS Network folder?**
   Yes, regular users can be given access, but they will not be able to see the subfolders of the network share.
   ONLY, AD users will be able to use the network folder information.

4. **When using Network Folders with NTFS permissions, is it possible to automatically hide folders that users don't have access to?**
   Yes, by enabling **Access Based Enumeration (ABE)** settings on the Network folders.
   For more information see Network Folders with NTFS permissions.

5. **What happens when a user permission is changed in AD?**
   When user membership in an AD group is modified, that change is not propagated immediately and is cached by Windows. For more information, see Microsoft help
   As a result, if you change a user group membership, it might take some time ranging (10 minutes to several hours) before the change is picked up by NTFS. If the changes must be picked up immediately, restart the Helper service.

6. **Is FileCloud Helper service compulsory**?
   If you are running FileCloud on a Windows server, you **do not need** the Helper service for NTFS permission checks as the Web Server itself can perform access checks.
   If you are running FileCloud on a Linux server, you **do need** the Helper service to perform NTFS permission checks.

For your reference
The FileCloud Helper service performs:

-
  - NTFS permission checks for Network Folders configured with NTFS permissions on a Linux server
  - Indexed search of Network Folders in Windows and Linux servers
  - Content search of documents for Network Folders in Windows and Linux servers

For more information on FileCloud Helper service refer to: FileCloud Helper Service

Advanced: Set Owner of Uploaded File to be the User Account

In some cases, it might be desirable to make the owner of the file the same as the user who uploads the file.

To enable this option, add this setting to cloudconfig.php

```
define("TONIDO_NETWORKSHARE_ASSIGN_UPLOAD_OWNER", 1);
```

If set owner doesn't work, make sure to add the service account that runs the web server to the local administrators group in your Windows file share servers or run it as a domain admin.

Indexing of Network Folders

Introduction

Unlike files in managed storage, files in Network Folders exist outside of FileCloud and therefore changes occurring in Network Folders might not be propagated into the FileCloud index. Monitoring such changes are important in the following scenarios:

- Faster searching
- Content search for files in Network Folders
- Automatic Realtime Syncing of Network Folders

For these scenarios, you must index network folders and keep them indexed as files and folders change.

- To index network folders, the FileCloud Helper service is required
- See instructions below on how to set up the Helper service for indexing

Setting up Indexing of Network Folders

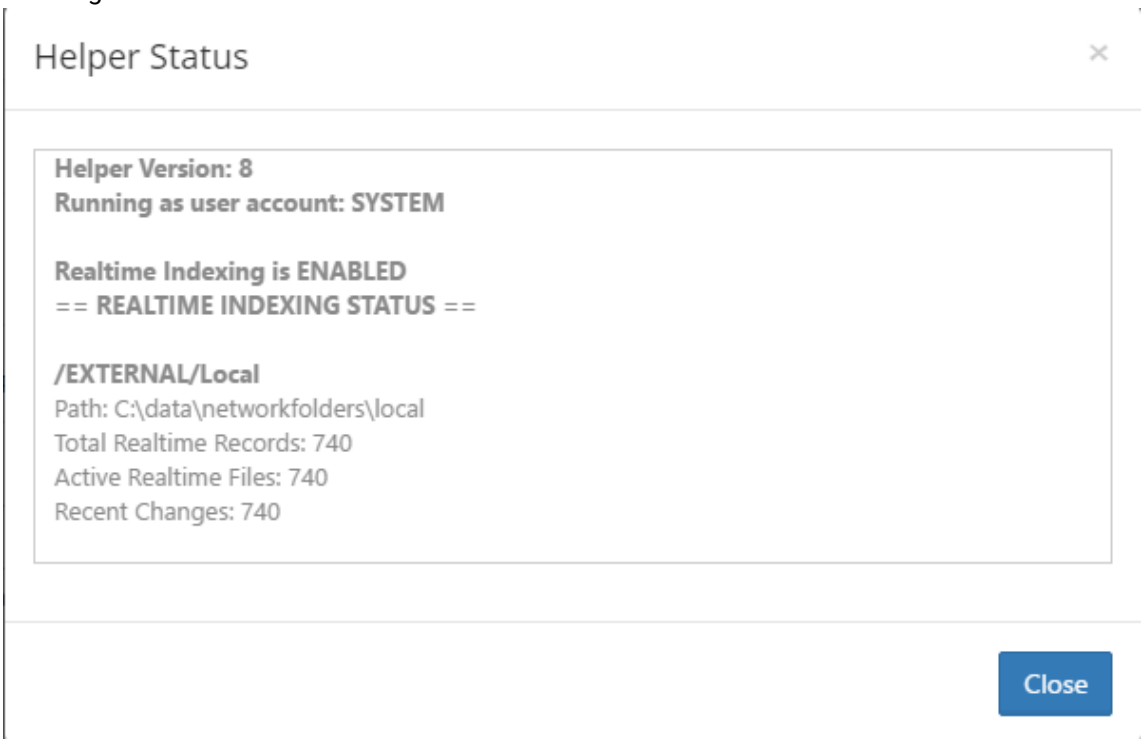
1. Install the latest FileCloud Helper service and set it up to run automatically. Ensure the **Logon as** user is set to a user account with permissions to Network Shares.
2. Open **realtimeconfig.ini** file in the FileCloud Helper install folder (%APPDATA%\FileCloudHelper) or (c:\xampp\FileCloudHelper)

```
[databases]
settingsdb=mongodb://127.0.0.1:27017
clouddb=mongodb://127.0.0.1:27017
syncdb=mongodb://127.0.0.1:27017


[misc]
enable=1
sleep=10
securitykey=nosoup4u
```

   a. Change the database settings if not using the default.
   b. Change the **enable** setting to **enable=1**
   c. change the **securitykey** value from the default to any other password value.
   d. Restart the Helper.

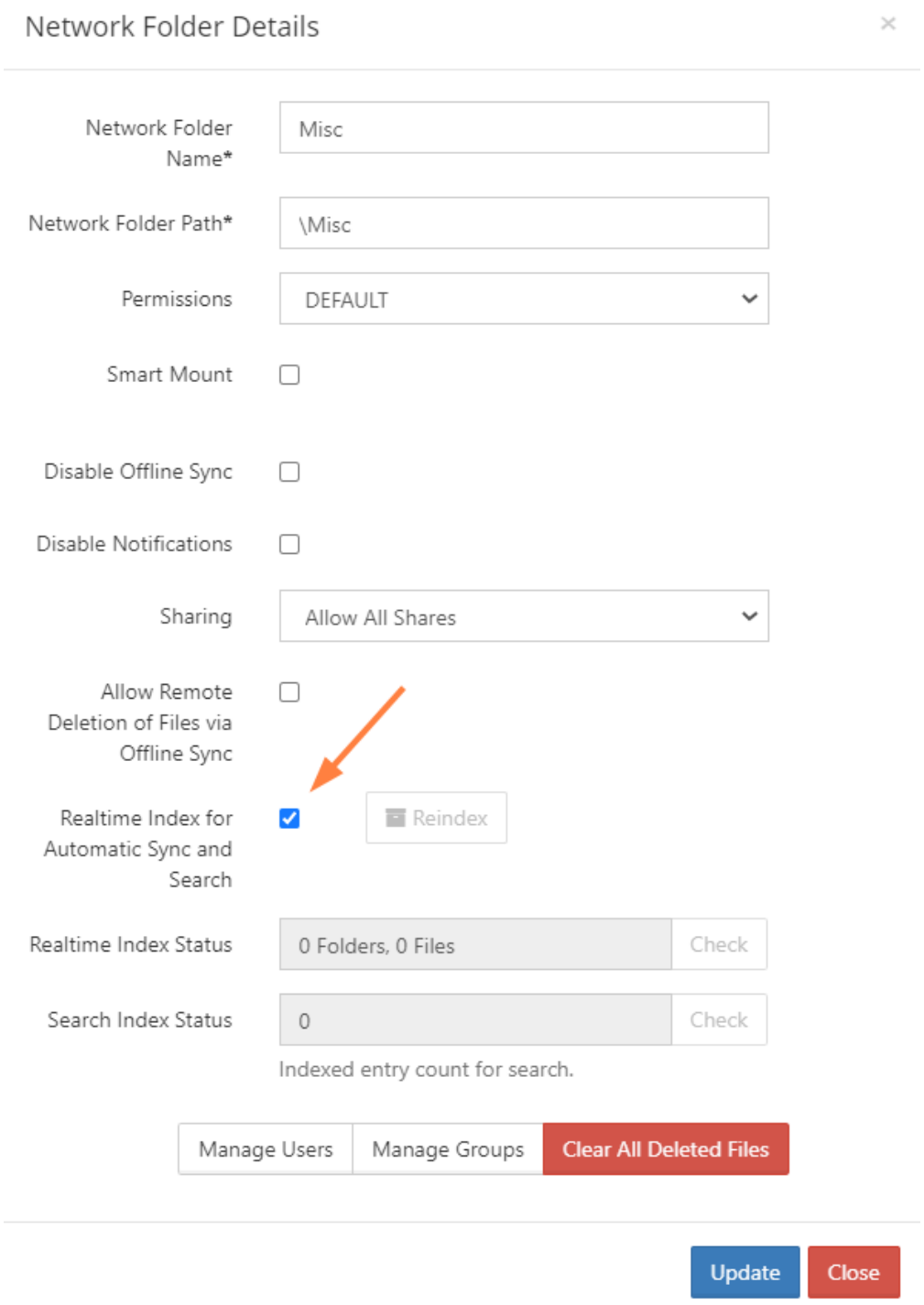
3. Verify that the Helper is configured correctly by opening **Settings > Misc > Support Services** in the admin portal. Click the **Helper Status** button and ensure the status shows that realtime indexing is enabled.



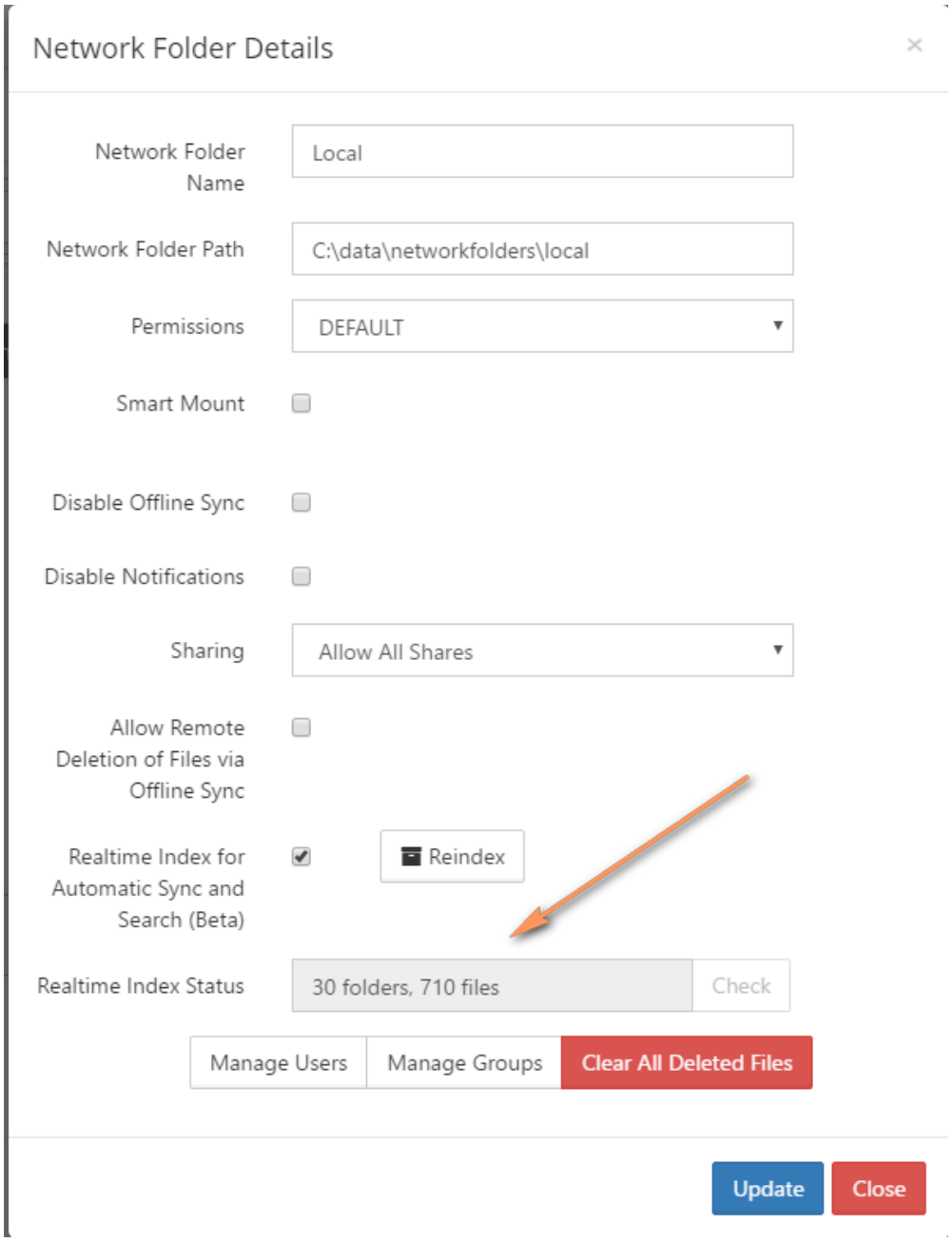
4. Edit **cloudconfig.php** file found on the WWWROOT config folder (**c:\xampp\htdocs\config** or **\var\www\config**) and add the following, making sure the security key default is changed to the same password value set in the **realtimeconfig.ini** file

```
define("TONIDOCLOUD_PUSH_KEY", "nosoup4u");
```

5. Now add a network folder and edit the settings to enable realtime scanning.



6. Always, restart the NTFS helper after enabling realtime index options for Network Folders or after adding or removing Network Folders
7. If indexing is happening correctly, **Realtime Index Status** will soon display stats of the indexed files and folders.



Searching in Network Folders

FileCloud normally searches Network Folders by searching files and folders directly on the operating system recursively, which can take considerable time if there are large folders with many files.

For faster searching, you can

- enable indexed search of Network Folders
- enable content search of the files in the Network Folders

Both options require that you have enabled indexing of Network Folders.

Enable indexed search of Network Folders

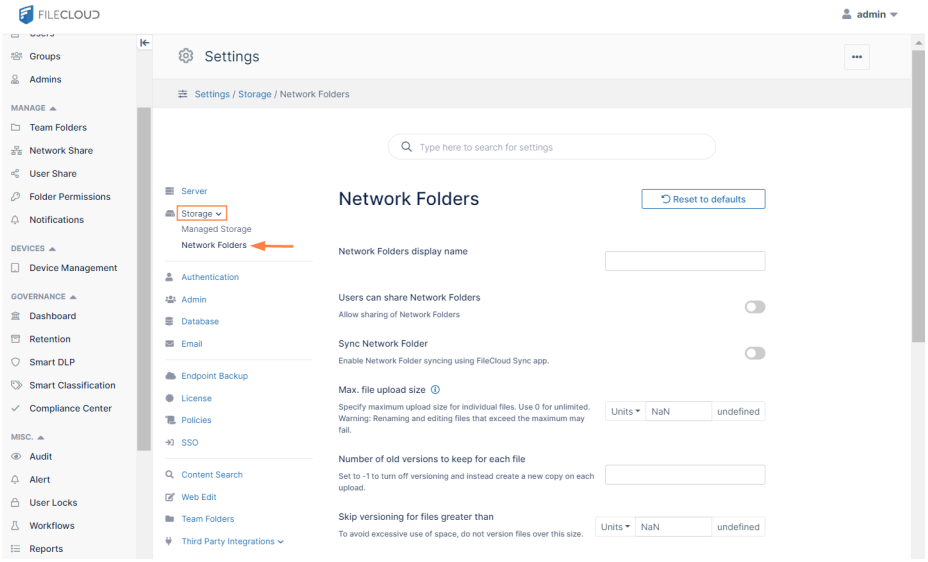
Realtime Index
NOTE: Real time network Indexing must be enabled on the server before indexed search can be activated. See Indexing of Network Folders.

To enable Indexed Search in Network Folders:

1. Go to the **Network Folders** settings page.
   To go to the Network settings page

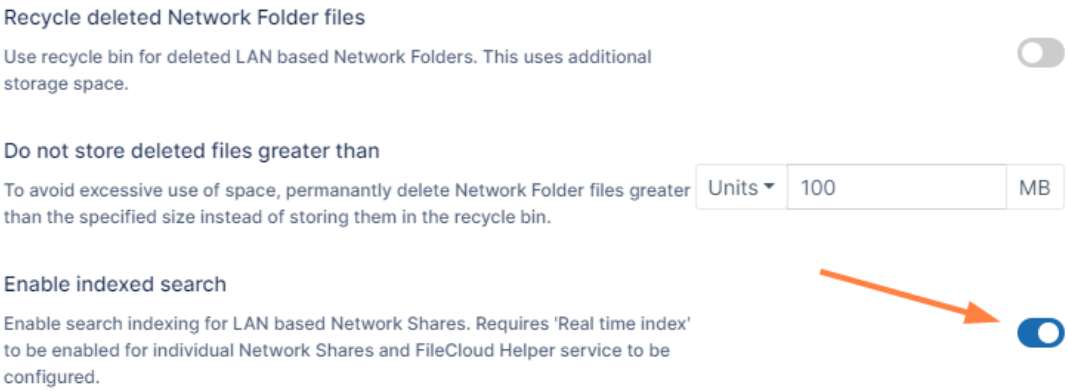
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .

   b. In the inner navigation bar on the left of the **Storage** settings page, expand the **Storage** menu, and click **Network Folders**, as shown below.



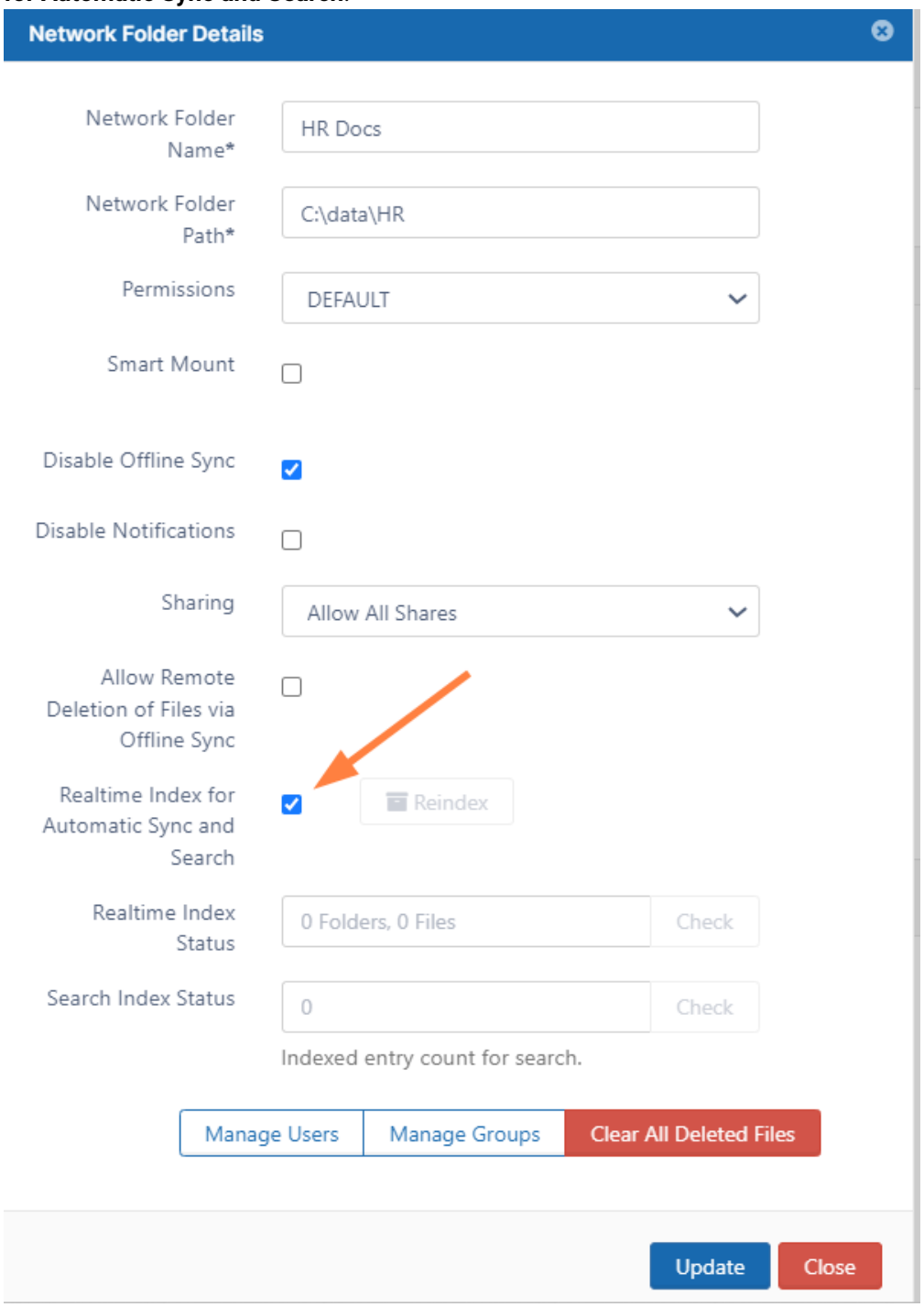
The **Network Folders** settings page opens.

2. Scroll to the bottom of the page, and enable **Enable Indexed Search**.



3. In the FileCloud navigation panel, go to **Network Share**.

4. Edit each Network Folder that you want to apply indexed searching to, and check **Realtime Index for Automatic Sync and Search**.



Web Server Permissions for Network Shares

FileCloud Control Panel names and corresponding Windows Services names

The same services have different names in the FileCloud Control Panel and the Windows Services screen.

The following table lists the corresponding names:

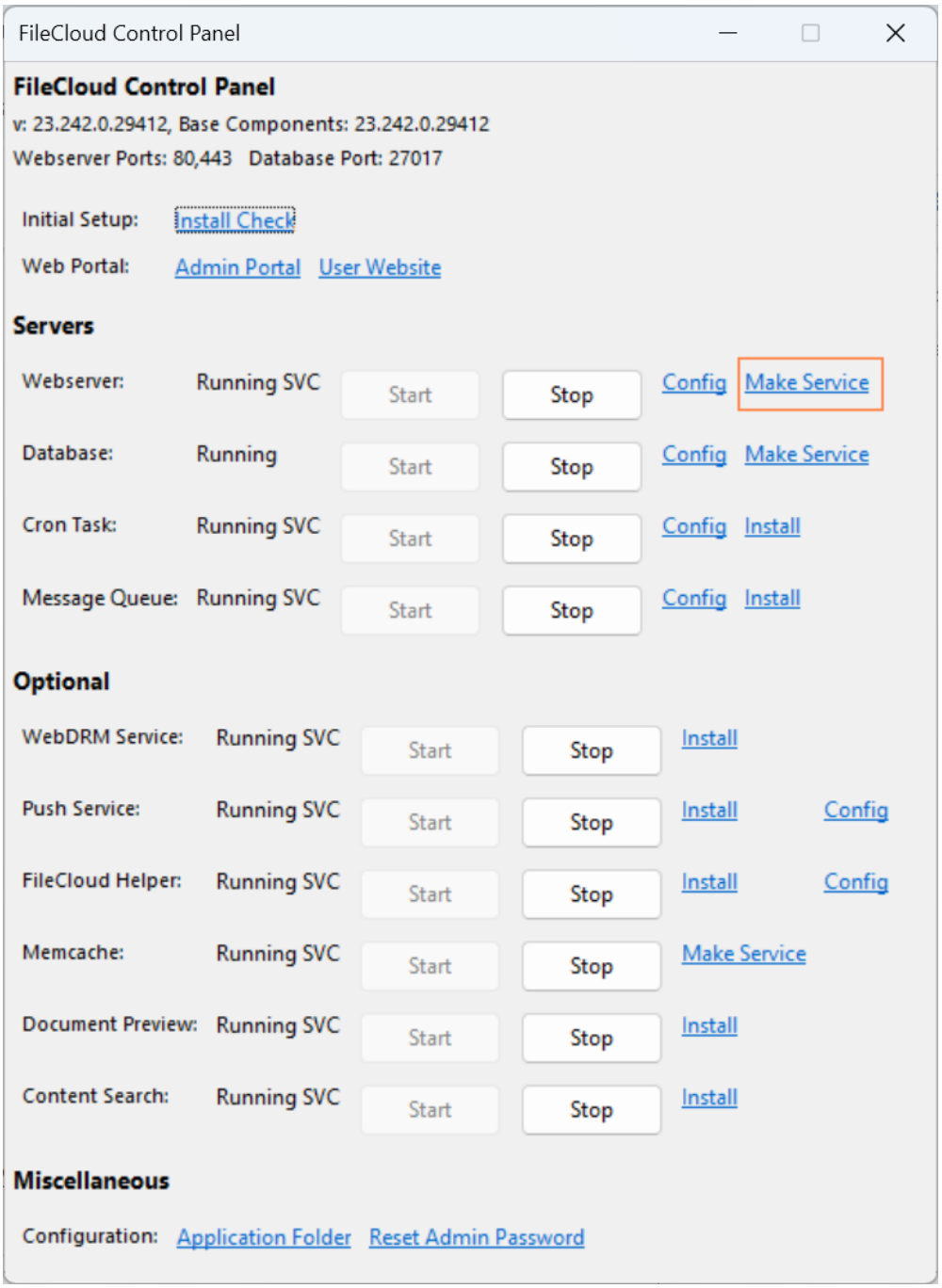
FileCloud Control Panel name	Windows Services name
Webserver	Apache or Apache#.# (for example, Apache2.4)
Message Queue	fcorchestrator
Cron Task	FileCloud Cron Service
Document Preview	FileCloud Docconverter

FileCloud Webserver (Apache), Message Queue (fcorchestrator), Cron Task (FileCloud Cron Service) and Document Preview (FileCloud Docconverter) permissions on Windows

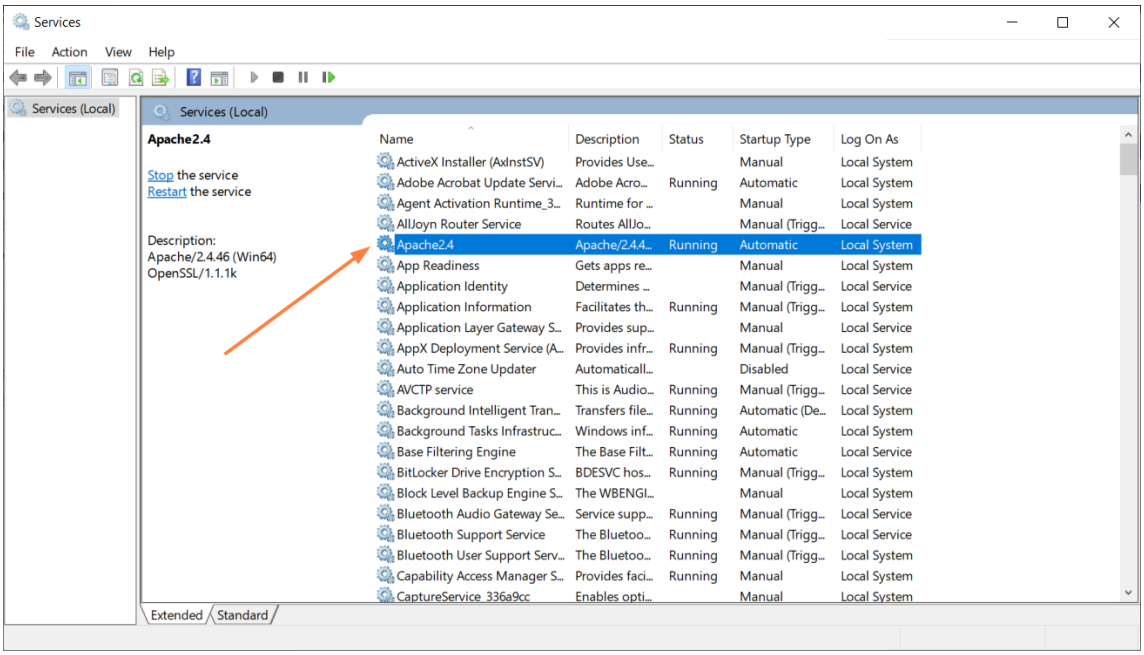
To make Network Folders accessible via FileCloud, the Webserver (Apache), Message Queue (fcorchestrator), Cron Task (FileCloud Cron Service), and Document Preview (FileCloud Docconverter) services must run as accounts with full permissions on Network Folders, otherwise there may be problems accessing network shares.

To configure this, run the Webserver (Apache) and Message Queue (fcorchestrator) as Windows services.

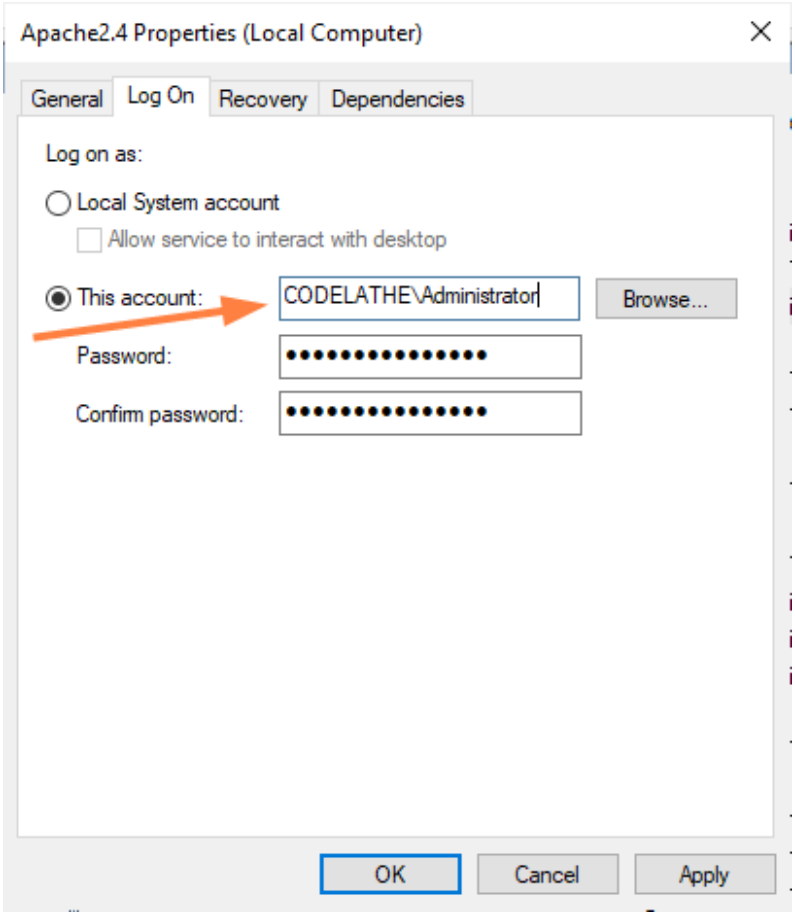
1. In the **FileCloud Control Panel**, click on the **Make Service** link.



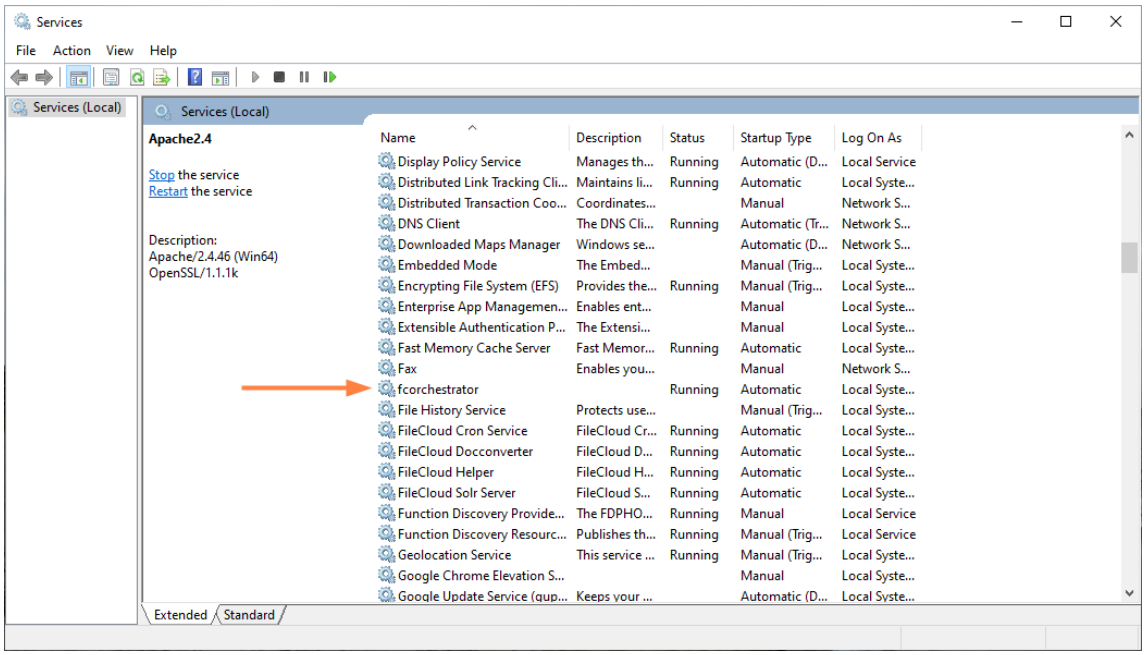
2. Open the Windows **Services** panel, then access the **Apache** service (the name may include the version of Apache installed).



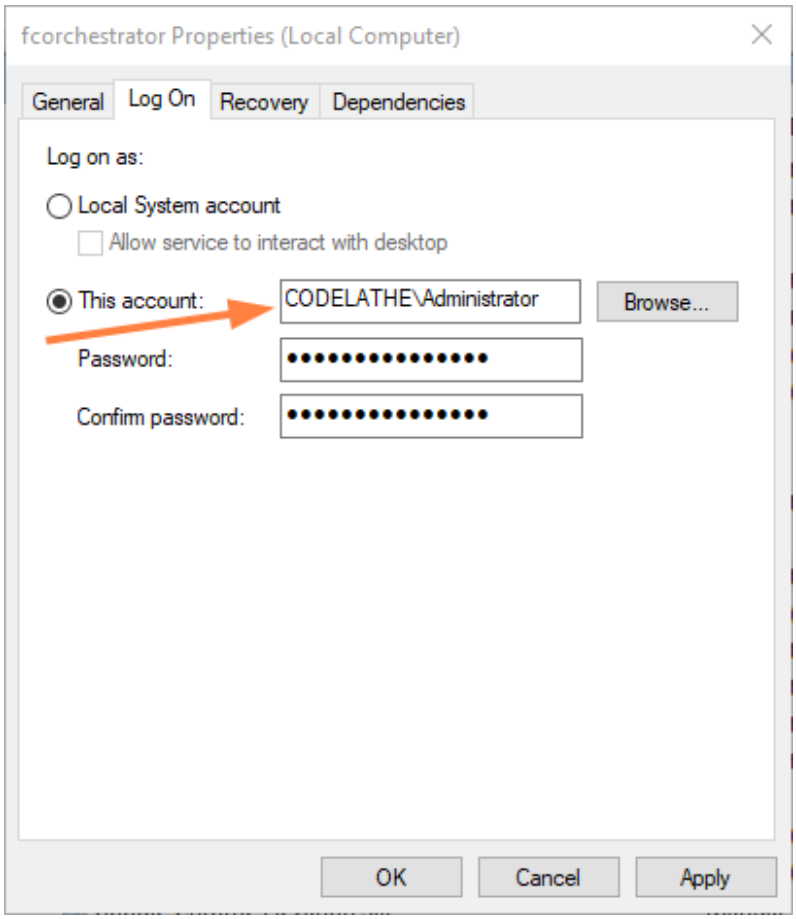
3. Right-click on the service and choose **Properties**.
4. In the **Properties** dialog box, click the **Log On** tab.
5. Set **This account** to an AD user that has full access to the network share.



6. Restart the service. Now the web server is running as a user account with full access to the network share.
7. Open the Windows **Services** panel again, and access the **fcorchestrator** service.



8. Repeat the process completed with the **Apache** service.
   Right-click on the service and choose **Properties**, then click the **Log On** tab and set **This account** to an AD user that has full access to the network share.



9. Restart the service. Now **fcorchestrator** is running as a user account with full access to the network share.

Running the Network Share Scanner (Beta)

> The beta version of the Network Share Scanner with services for Windows accessible from the FileCloud Control Panel is available in FileCloud 23.261 and later.

The new FileCloud Network Share Scanner, a more efficient indexer service than FileCloud Helper, monitors file system events on LAN-based Network Folders, enabling use of advanced FileCloud features with files in Network Folders including:

- Content search
- User workflows
- Content Disarm and Reconstruction (CDR)
- Antivirus integration
- Metadata rules
- Data Loss Prevention (DLP)

- Content Classification Engine (CCE)

Once you are running the Network Share Scanner, these features will function successfully when you specify network share paths using the root **external**.

The Network Share Scanner is available on both Linux and Windows systems.

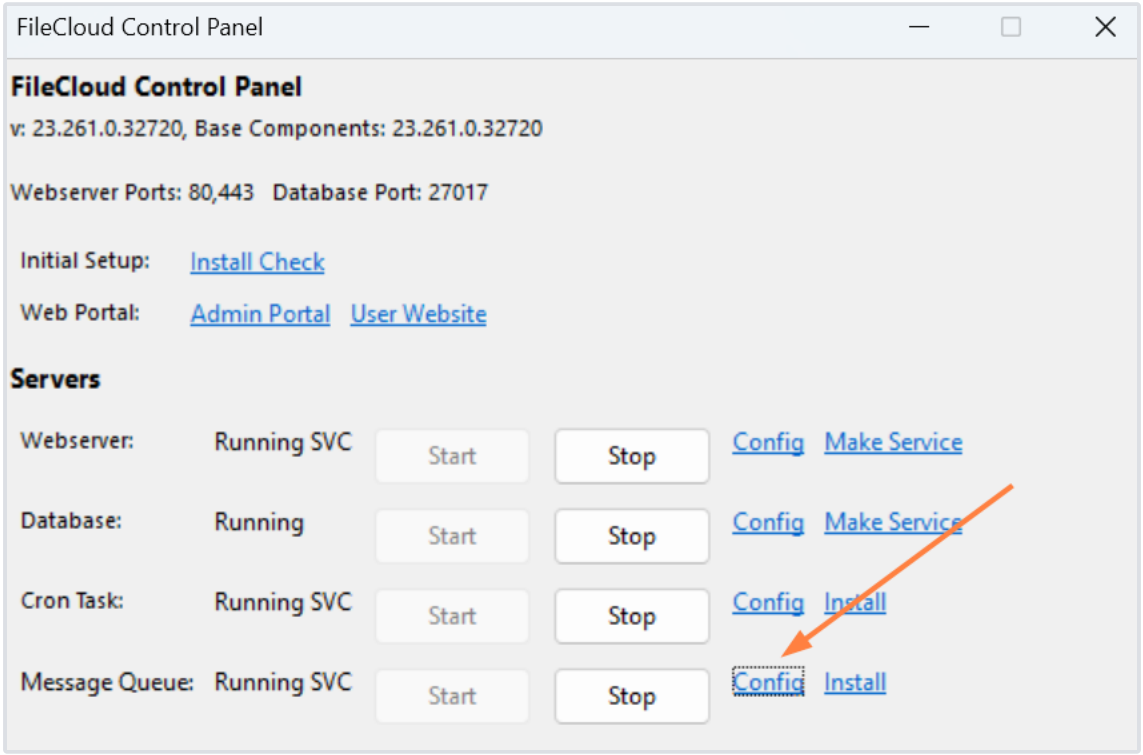
Start/Manage Network Share Scanner

Note that on Linux, you must install the Network Share Scanner, but it Windows it is already installed.

Windows

To start the Network Share Scanner in Windows:

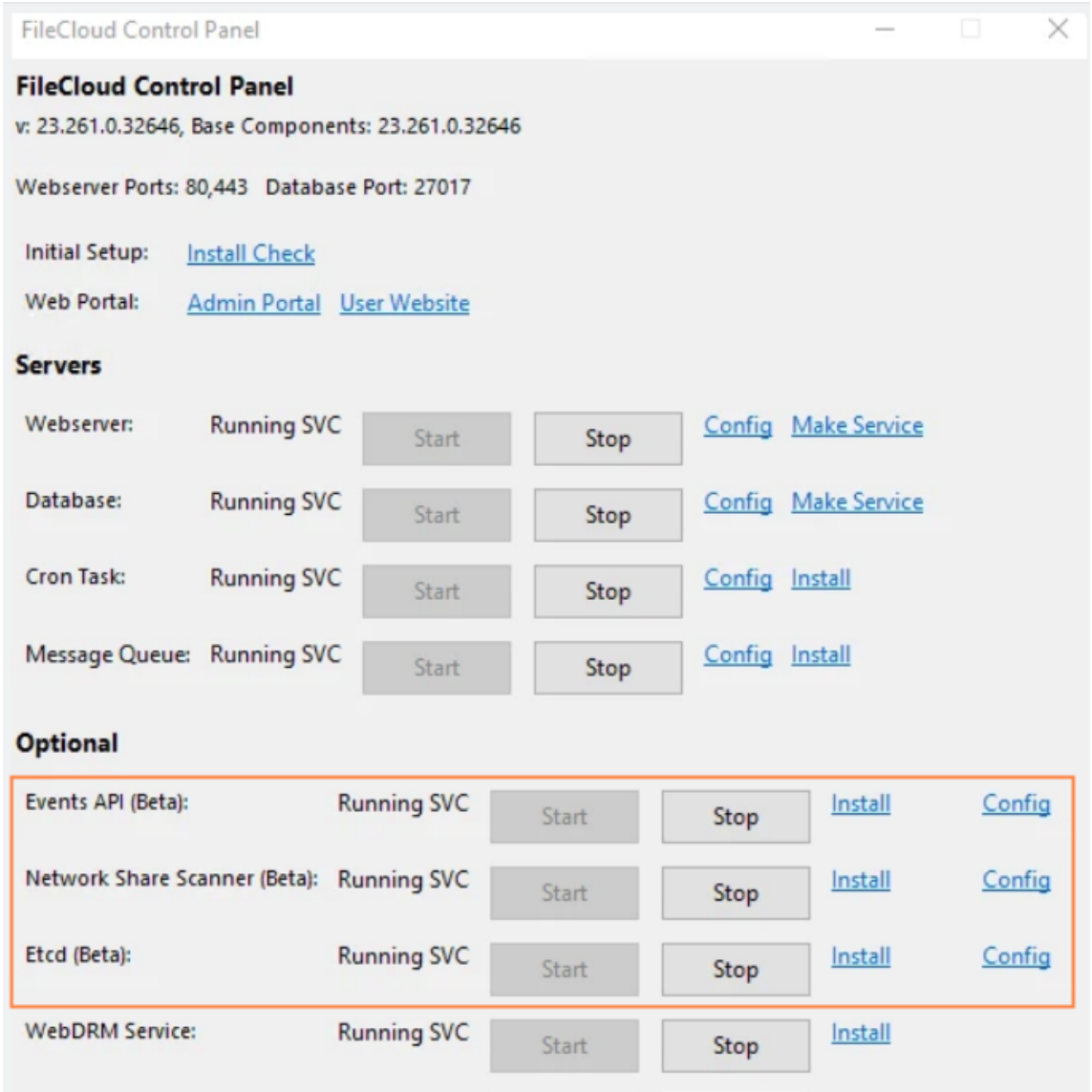
1. Open the FileCloud Control Panel.
2. Click **Config** next to **Message Queue**:



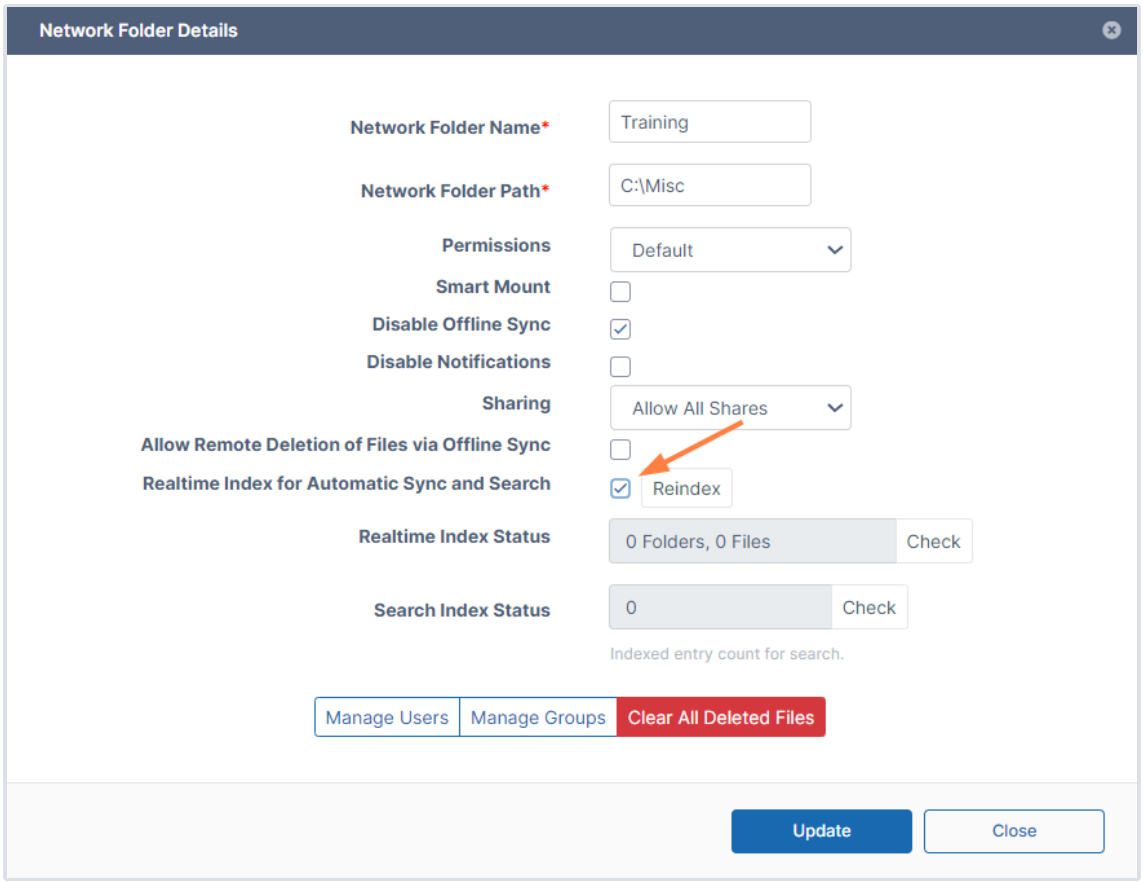
   The **default.json** file opens. By default, the field **"event_api_workers_count"** is set to 0. To process the eventapi queue, increase it. The number you increase it to depends on the size of your network shares; increasing it to 2 to 4 is typical, but you may go as high as 10.
3. Enable the Network Share Scanner:
   a. Open the cloudconfig file at: C:\xampp\htdocs\config\cloudconfig.php
   b. Add the setting:

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

4. Restart **Message Queue**.
5. In the FileCloud Control Panel, click **Install** for the services:
   Events API (Beta)
   Network Share Scanner (Beta)
   Etcd (Beta)
6. In the FileCloud Control Panel start the following services:
   Memcache
   Etcd (Beta)
7. After **Memcache** and **Etcd (Beta)** have started, start:
   Events API (Beta)
   Network Share Scanner (Beta)



8. For each network share that you want to be monitored by the Network Share Scanner, in the Network Folder Details for the folder, check **Realtime Index for Automatic Sync and Search**.
Note: After changing this flag, it can take up to 1 minute for this feature to detect the new network and start monitoring it.



Linux

1. Open the file **/var/www/html/src/Scripts/default.json**
By default, the field "**event_api_workers_count**" is set to 0. To process the eventapi queue, increase it. The number you increase it to depends on the size of your network shares; increasing it to 2 to 4 is typical, but you may go as high as 10.
2. Enable the Network Share Scanner:
   a. Open the cloudconfig file at:
   /var/www/html/config/cloudconfig.php
   b. Add the setting:

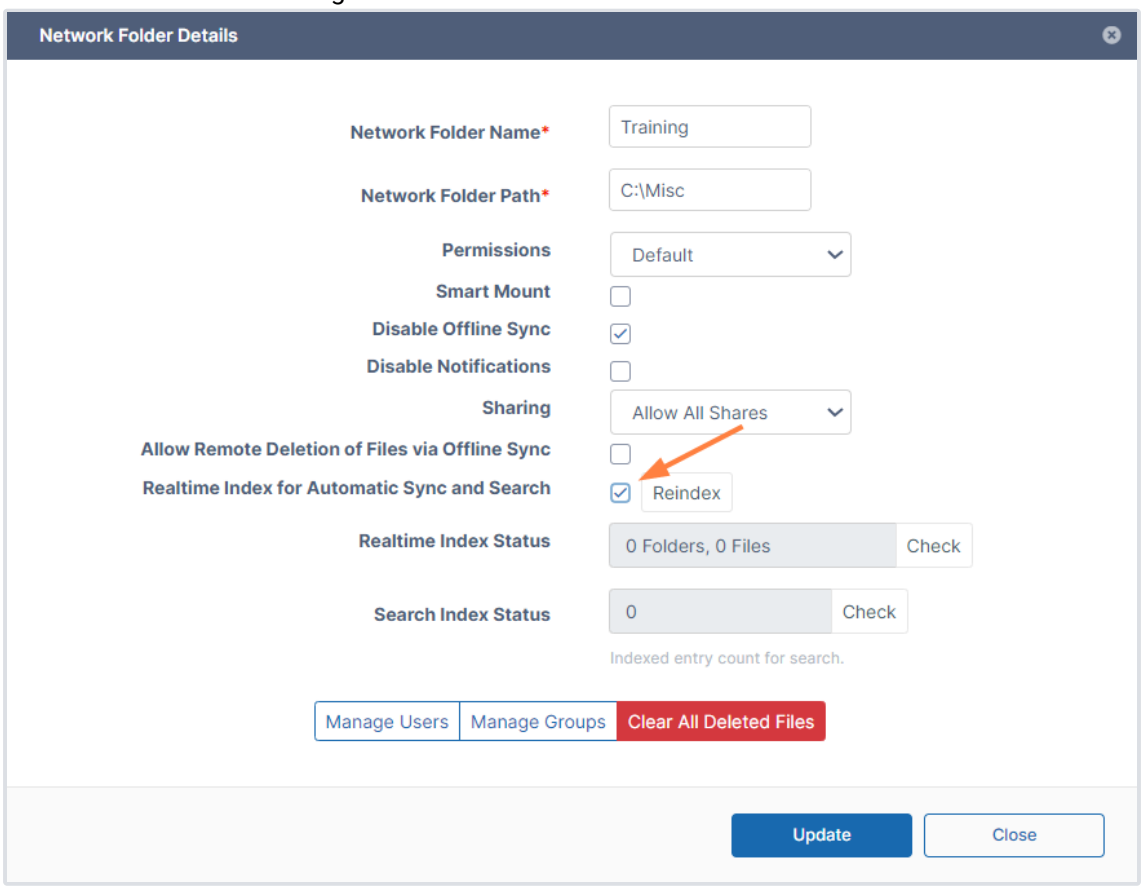
```
define("TONIDOCLOUD_EVAPI_ENABLED", true);
```

3. Restart the message queue service.
4. Install the Network Share Scanner in Linux:

```
filecloudcp -e → install EventAPI
filecloud -n → installs network share scanner
```

The services start automatically after you install them.

5. For each network share that you want to be monitored by the Network Share Scanner, in the Network Folder Details for the folder, check **Realtime Index for Automatic Sync and Search**. **Note**: After changing this flag, it can take up to 1 minute for this feature to detect the new network and start monitoring it.



To manage the Network Share Scanner in Linux:

Use a regular service manager to manage the services. For example, to stop the service, enter:

```
systemctl stop fceventapisystemctl
systemctl stop fcnetworksharescanner
```

Log management

The Network Share Scanner includes several settings for managing your log output.

To manage your logs:

1. In C:\xampp\eventsapi, open **networker-config.yaml**.
   You can change your log settings in the section that appears as:

```
log:
    stdout: false
    level: info
    path: logs
    filename: log.json
```

   The settings options are shown in the following table:

Setting	Options
stdout	**false** (default) - do not print logs to command line interface **true** - print logs to command line interface
level	**info** (default) Enter an option to indicate how granular the logs should be. The options, from most granular to least granular are: **debug** **info** **warn** **error** **fatal** **panic**
path	**logs** (default) The path to the log directory. Change to use a different path.
filename	**log.json** (default) The log file name. Change to use a different name.

2. Restart **FCC-NSS_Maestro.exe** for any changes to take effect.

Network Share Scanner: Steps after FileCloud Upgrade

Any changes to the files **maestro-config.yaml** and **networker-config.yaml** appear in the files **maestro-config.dist.yaml** and **networker-config.dist.yaml** after FileCloud upgrade. After upgrade, you must take the following steps to add the new content to your files while preserving any customizations you have made.

Windows

- In **C:\xampp\eventsapi\maestro-config.yaml**
  - If you did not make changes to **maestro-config.yaml** previously:
    Replace the content of **maestro-config.yaml** with the content of **maestro-config.dist.yaml**.
  - If you made changes to **maestro-config.yaml** previously:
    Add the changes to **maestro-config.dist.yaml**, then remove **maestro-config.yaml**.
    Rename **maestro-config.dist.yaml** to **maestro-config.yaml**.
- In **C:\xampp\eventsapi\networker-config.yaml**
  - If you did not make changes to **networker-config.yaml** previously:
    Replace the content of **networker-config.yaml** with the content of **networker-config.dist.yaml**.
  - If you made changes to **networker-config.yaml** previously:
    Add the changes to **networker-config.dist.yaml**, then remove **networker-config.yaml**.
    Rename **networker-config.dist.yaml** to **networker-config.yaml**.

Linux

- In **/opt/fcnetworksharescanner/maestro-config.yaml**
  - If you did not make changes to **maestro-config.yaml** previously:
    Replace the content of **maestro-config.yaml** with the content of **maestro-config.dist.yaml**.
  - If you made changes to **maestro-config.yaml** previously:
    Add the changes to **maestro-config.dist.yaml**, then remove **maestro-config.yaml**.
    Rename **maestro-config.dist.yaml** to **maestro-config.yaml**.
- In **/opt/fcnetworker/networker-config.yaml**
  - If you did not make changes to **networker-config.yaml** previously:
    Replace the content of **networker-config.yaml** with the content of **networker-config.dist.yaml**.
  - If you made changes to **networker-config.yaml** previously:
    Add the changes to **networker-config.dist.yaml**, then remove **networker-config.yaml**.
    Rename **networker-config.dist.yaml** to **networker-config.yaml**.

Amazon S3 Bucket Based Network Folders

Administrators can integrate Amazon's AWS S3 buckets with FileCloud Server to give users access to this data inside FileCloud Server portals and clients.

What is an AWS bucket?

Amazon S3 is cloud storage for the internet.

To upload your data (photos, videos, documents etc.), first create a bucket in one of the AWS Regions. Then upload any number of objects to the bucket.

Working with Amazon S3 Buckets

⚠ There are a few limitations you should know about using Amazon S3 bucket network folders

1. There is no versioning support (version key is ignored and file will be overwritten).

2. No real time network sync or indexed search is allowed (regular file search works).

What do you want to do?

Attach an AWS S3 Bucket to a Network Folder	Create a Network Folder for an Amazon S3 Bucket
Configure the bucket-based Network Folder	Configure the AWS S3 bucket-based Network Folder Clear All Deleted Files

Create a Network Folder Based on an Amazon S3 Bucket

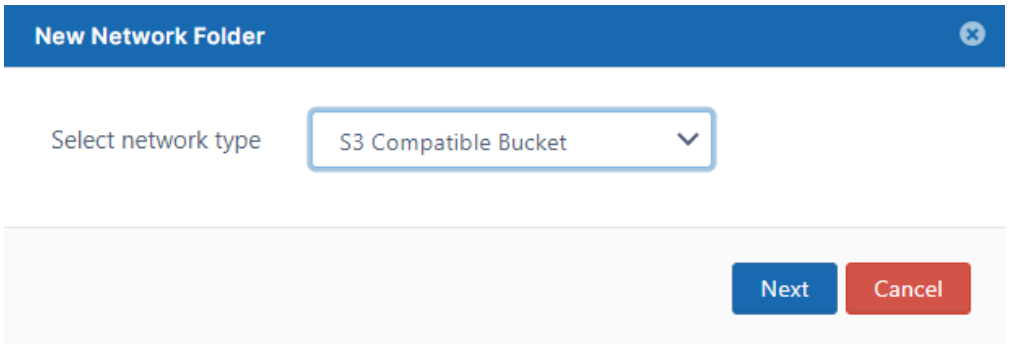
Administrators can integrate Amazon's AWS S3 buckets with FileCloud Server to give users access to this data inside FileCloud Server portals and clients.

⚠ There are a few limitations you should know about using Amazon S3 bucket network folders

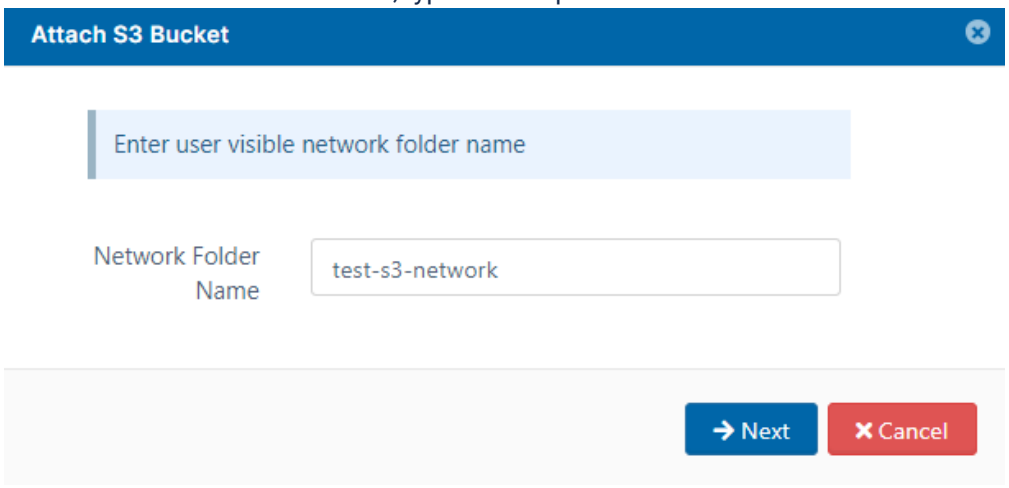
1. There is no versioning support (version key is ignored and file is overwritten).
2. No real time network sync or indexed search is allowed (regular file search works).

To create a network share from an S3 bucket:

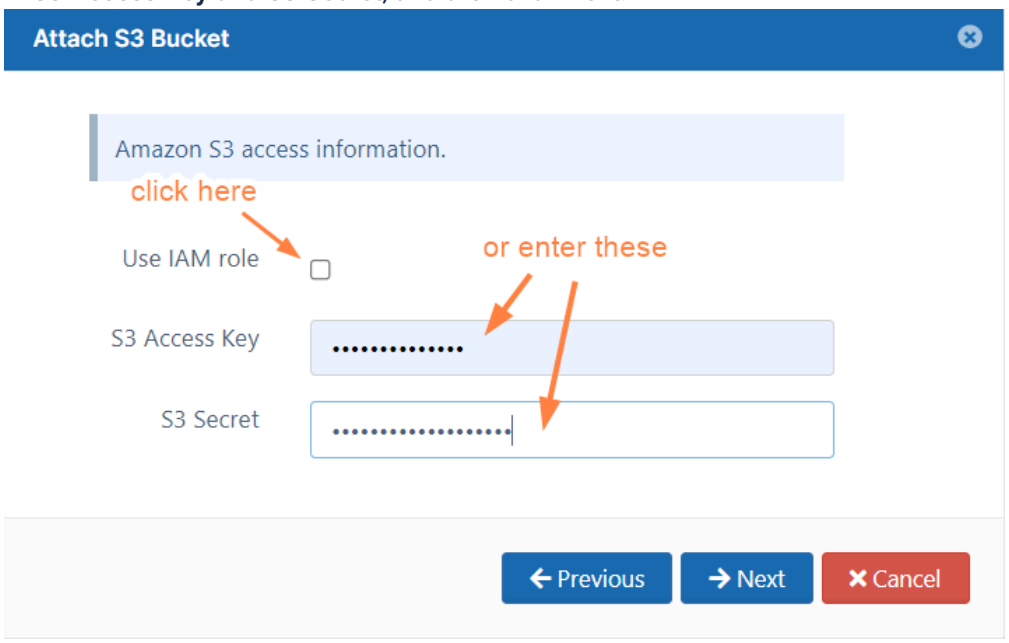
1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



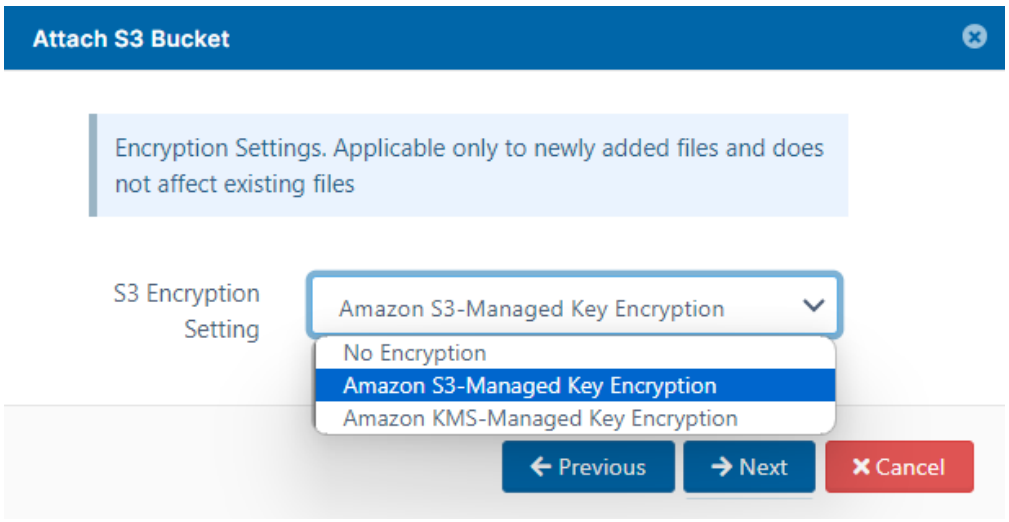
5. On the **Attach S3 Bucket** window, type in a unique **Network Folder Name** and then click **Next**.



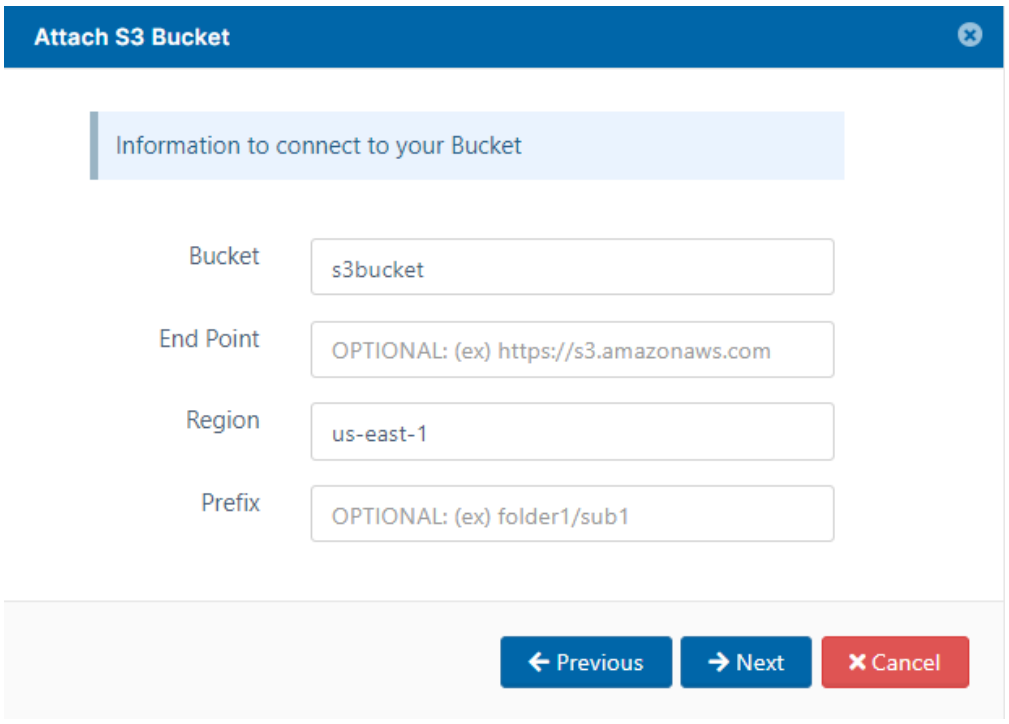
6. On the **Attach S3 Bucket** window, either check **Use IAM role** or type in authentication credentials in **S3 Access Key** and **S3 Secret**, and then click **Next**.



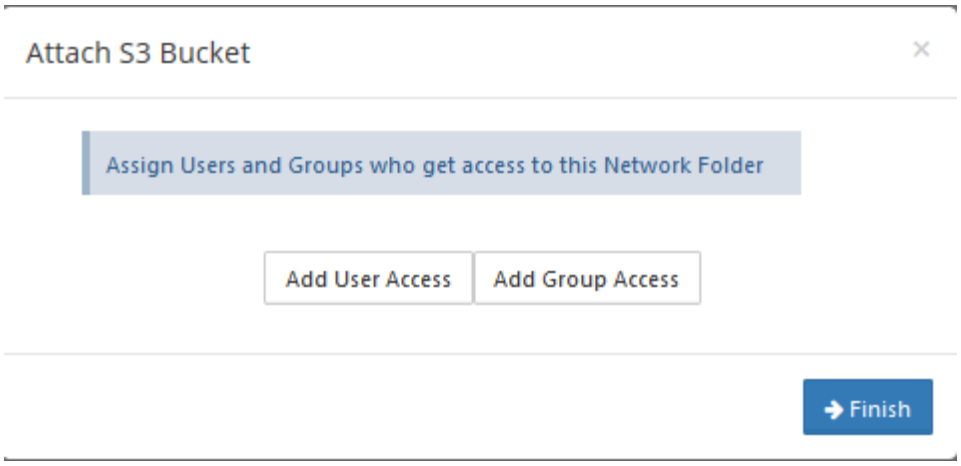
7. On the **Attach S3 Bucket** window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:



8. On the **Attach S3 Bucket** window, type in the **Bucket** name, **Region**, and optionally the **End Point** and **Prefix**.
9. Click **Next**.

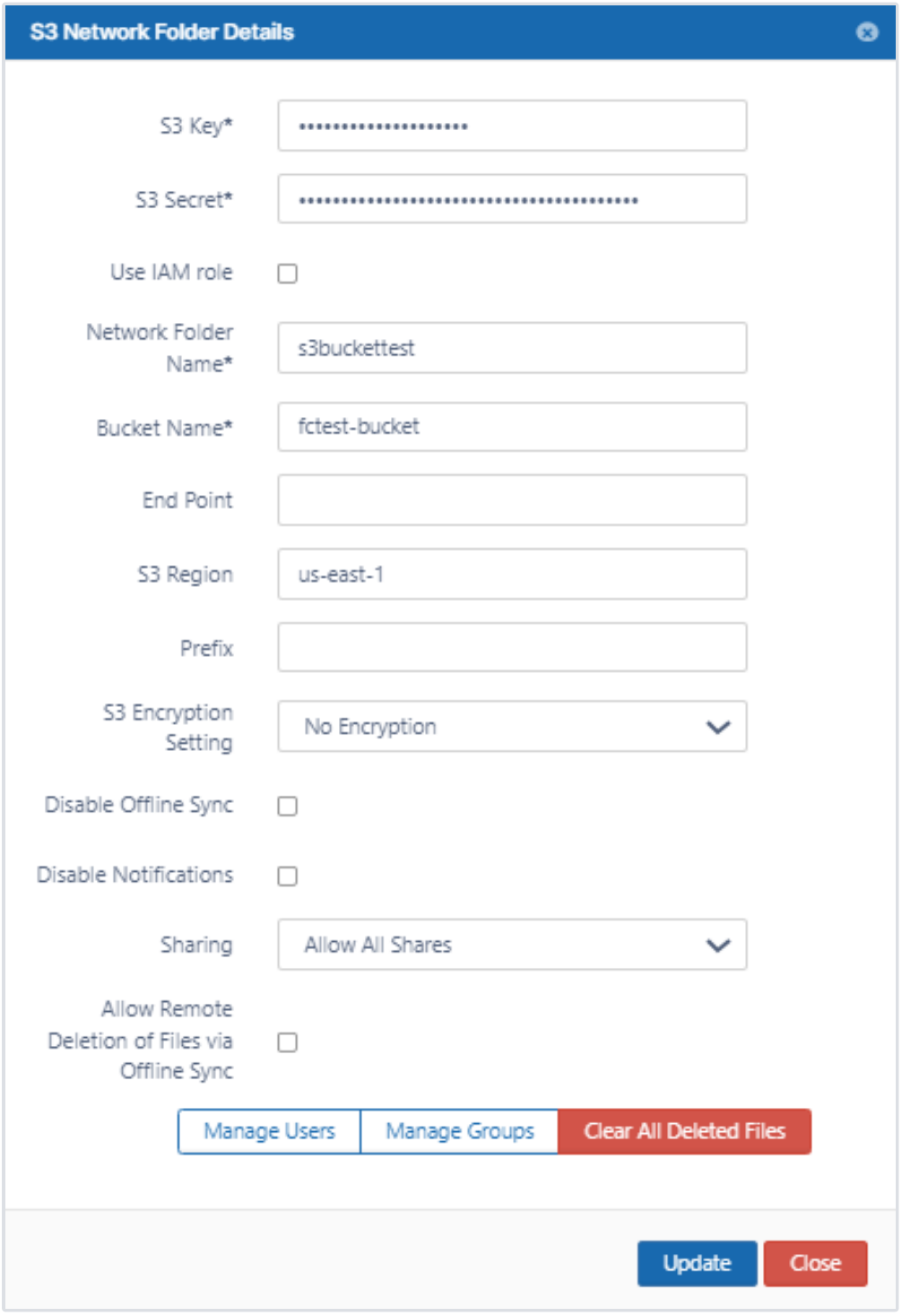


10. When the S3 bucket is mounted as a network share, permissions need to be assigned to users or groups to allow access.
The network share access can be granted to:
    - Guest User
    - Full User
    - User Group



Configure AWS S3 Bucket-Based Network Folders

After you attach an AWS S3 bucket to a FileCloud Network Folder, you can update any of the original settings.

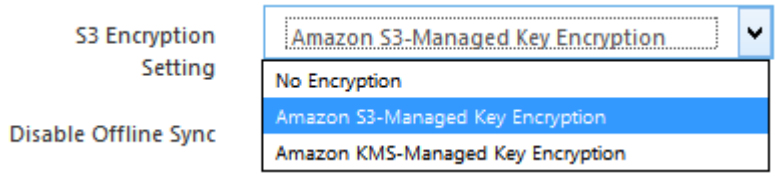
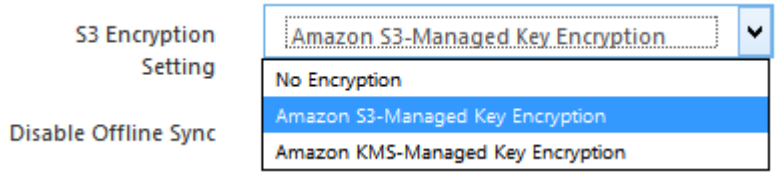


To edit an AWS S3 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the AWS S3 bucket-based network folder, and then click the edit icon.

4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	S3 access key
S3 Secret	S3 secret access key
Use IAM role	Either check **Use IAM role** or type in authentication credentials in **S3 Key** and **S3 Secret**. **Note**: To use an IAM role, you must attach it to your E2 instance. See the page Attach an IAM role to an instance in the AWS documentation for instructions.
Network Folder Name	Display name of network folder
Bucket Name	Name of bucket attached to network folder After September 2020, new AWS bucket names with a "." in them are invalid. However, bucket names with a "." in them created in September 2020 or earlier are still supported. To allow S3 buckets created after September 2020 to have a "." in the bucket name, include the flag **TONIDOCLOUD_S3_USE_PATH_STYLE_ENDPOINT** in the file amazons3storageconfig.php and set it to **1**.
End Point	(Optional) AWS S3 endpoint URL. Leave empty if using Amazon's S3 service; the region string automatically selects the correct endpoint. This value cannot be changed once the bucket is created.
S3 Region	The geographical AWS region where the bucket is created.
Prefix	A prefix to add to the network share paths to create different paths within buckets

Option	Description
S3 Encryption Setting	**No Encryption** When this option is set the files in the S3 network share are not encrypted. **Amazon S3-Managed Key encryption** When this option is set the files are encrypted. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.  **Amazon KMS-Managed Key Encryption** When this option is set the files are encrypted using AWS KMS key. AWS KMS uses customer master keys (CMKs) to encrypt your Amazon S3 network share. You use AWS KMS via the Encryption Keys section in the IAM console or via AWS KMS APIs to centrally create encryption keys, define the policies that control how keys can be used, and audit key usage to prove they are being used correctly.  **Note**: Unlike S3 managed storage encryption, enabling encryption in Network Shares encrypts only newly added files and does not encrypt existing files.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Disable Notifications	Disable some or all S3 Network Folder notifications for users with access to the folders. See Disable notifications for Amazon S3 bucket-based Network Folders, below.

Option	Description
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to S3 bucket when deleted via Sync client.

Configure optimized upload for Amazon S3 Network Folders

When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud 23.241 includes an Optimized Upload feature.

- If you are using Amazon S3 storage for your managed storage in FileCloud, follow the instructions in Setting up FileCloud Managed S3 Storage under **Integrate Amazon S3 Storage**. Make sure you follow **Step 2 (Optional) Configure System to Use Optimized Upload** and **Step 3 Configure Credentials and Settings.** This sets up optimized upload for both S3 managed storage and S3 Network Folders.

- If you are not using Amazon S3 storage for managed storage in FileCloud:

Click to expand

1. Create a CORS file and confirm that your service address is configured in the .htaccess file.

   When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud 23.241 includes an Optimized Upload feature which can be enabled in your system by following the instructions below to configure a CORS policy with the required settings, and to confirm that your service address is in the .**htaccess** file.

   Note: Although Use Optimized Upload and its associated settings appear in the Managed Storage settings page, they also apply to S3 Network Folders.

   Required CORS policy for Optimized Upload

To use the Optimized Upload feature, configure a CORS policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings.
For more information about CORS, see:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/enabling-cors-examples.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/ManageCorsUsing.html

To configure the CORS policy:

a. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
b. In the Bucket name list, choose the name of the bucket that you want to create a bucket policy for.
c. Choose Permissions, and then choose CORS configuration.
d. In the CORS configuration editor text box, type or copy and paste the following CORS configuration:

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "https://my-fc-instance.com"
        ],
        "ExposeHeaders": [
            "ETag"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

e. Click **Save**.

To confirm that the service address is configured in the .htaccess file:

a. Open the .**htaccess** file.
Windows: C:\xampp\htdocs\.htaccess
Linux: /var/www/.htaccess
b. Check if the following line exists, and if it does not, add it:
If you use an external compatible S3 service, add the address to the service instead.

```
connect-src 'self' *.amazonaws.com
```

c. Restart the FileCloud server.

2. Set up Optimized Upload in your managed storage settings. On page Setting up Managed Storage, read the instructions for the **Use Optimized Upload** setting in the table to configure your S3 Network Folders to use optimized upload.

Note: If you are using Network Folders with S3 storage, if you use server-side encryption with a customer key (SSE-C), optimized upload will fail due to security reasons.

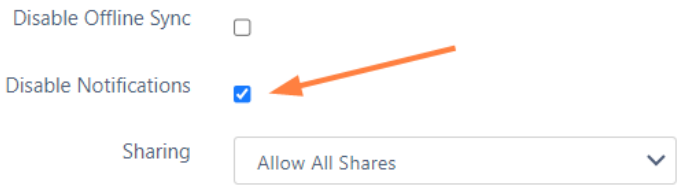
Disable notifications for Amazon S3 Network Folders

By default, notifications are enabled for network folders. This means that all users who have access to a network folder and have notifications enabled receive notifications about all actions on the folder.

However, since multiple users may have access to the same network folder, users may receive notifications about actions that are not relevant to them.

There are various ways you can limit their access to these notifications. First, disable notifications for the folder, and then, override the setting only for notifications that you want to permit.

1. Disable notifications for the folder:
   a. In the left navigation panel, click **Network Folders**.
   b. Click the **Edit** button for the network folder.
   The **Network Folder Details** dialog box opens.
   c. Check the **Disable Notifications** box.



2. Click **Update**.
3. Do one of the following:
   - **Leave all notifications about actions in the folder disabled.**
   By default, admins and users can override this setting. An admin can enable notifications about the folder for specific users, or users can enable their own notifications for the folder.
   If you do not want users to be able to override this setting, you must disable file change notifications in **Settings > Misc > Notifications**. See Notifications for File Changes for help.
   - **Enable notifications about the folder for specific users.**
   This is useful if you want to limit the users who receive notifications about a network folder to those it has been shared with.

See the various options for setting users' notifications in the section Managing User-Defined Notifications.

- **Allow users to enable their own notifications about the folder.**
  See the options users have for setting their own notifications in the section Notifications.

Clearing Deleted Files from S3 Network Folders

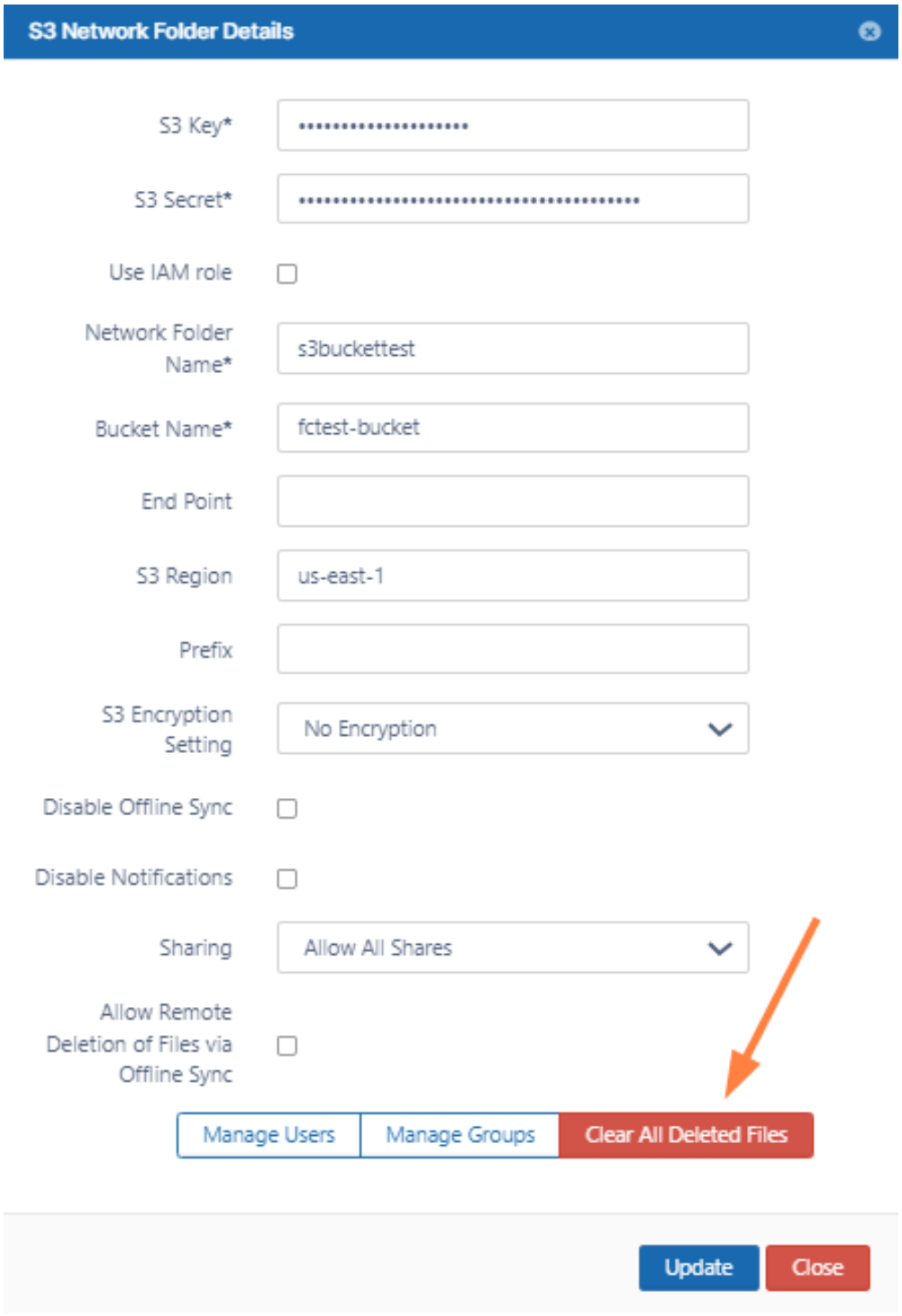
Administrators can clear the files deleted by users in Network Folders.

Why?

- Files deleted by users are moved to the recycle bin (if enabled).
- The files in the recycle bin take up space over time.

To clear deleted files in an S3 Network Folder:

1. Open a browser and log on to the admin portal.
2. In the left navigation panel, click **Network Folders**.
3. In the **Manage Network Folders** window, click the row containing the folder you want to clear of deleted files.
4. Click the edit icon (
   
).
5. On the **S3 Network Folder Details** window, click **Clear All Deleted Files**.



6. To save your changes, click **Update**.

Azure Blob Storage Based Network Folders

Administrators can integrate an Azure Blob Storage container with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

What is Azure Blob Storage?

Azure Blob Storage is cloud storage for the internet.

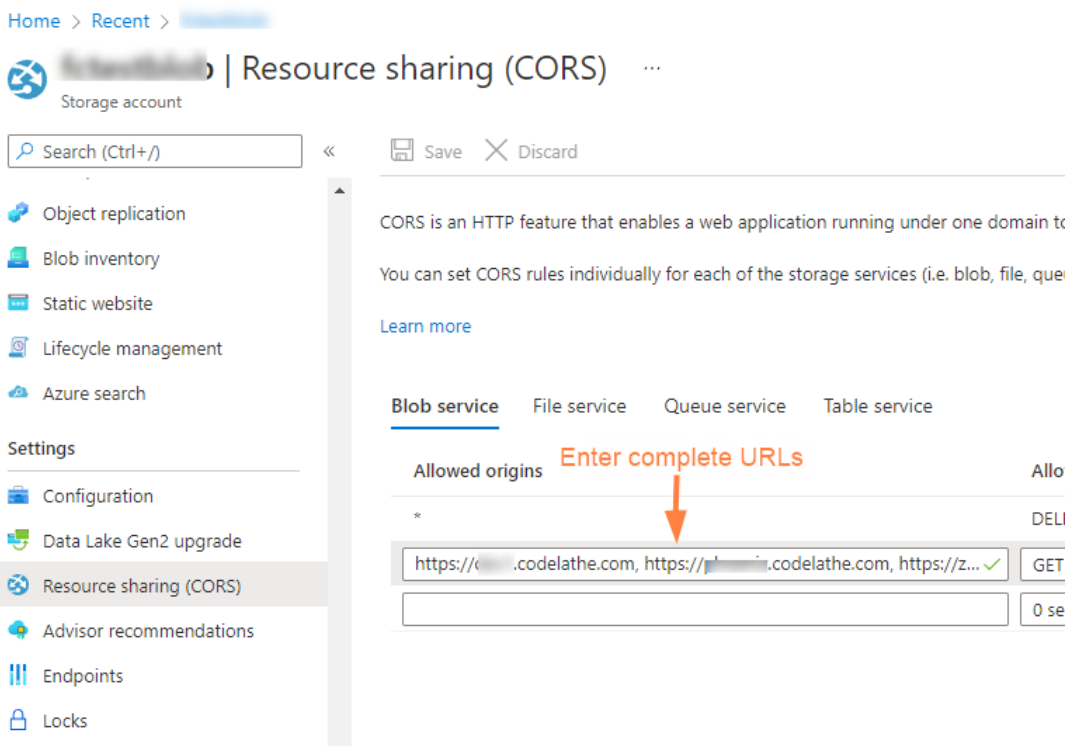
To upload your data (photos, videos, documents etc.), first create a Blob Storage container in an Azure Region, then upload any number of objects to the bucket.

Working with Azure Blob Storage

⚠ There are a few limitations you should know about using Azure Blob Storage network folders

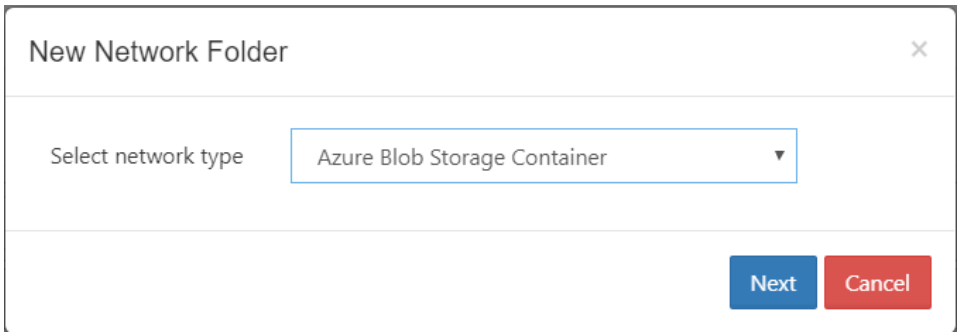
1. No versioning support (Version key will be ignored and file will be overwritten)
2. Real-time network sync and indexed search are not supported (regular file search will work)

⚠ For preview and edit to work correctly when you use Azure Blob Storage for Network Folders, in the Azure CORS settings, for the value of **Allowed origins**, enter the exact URLs that will be accessing the objects. (Do not enter *.)
For example:



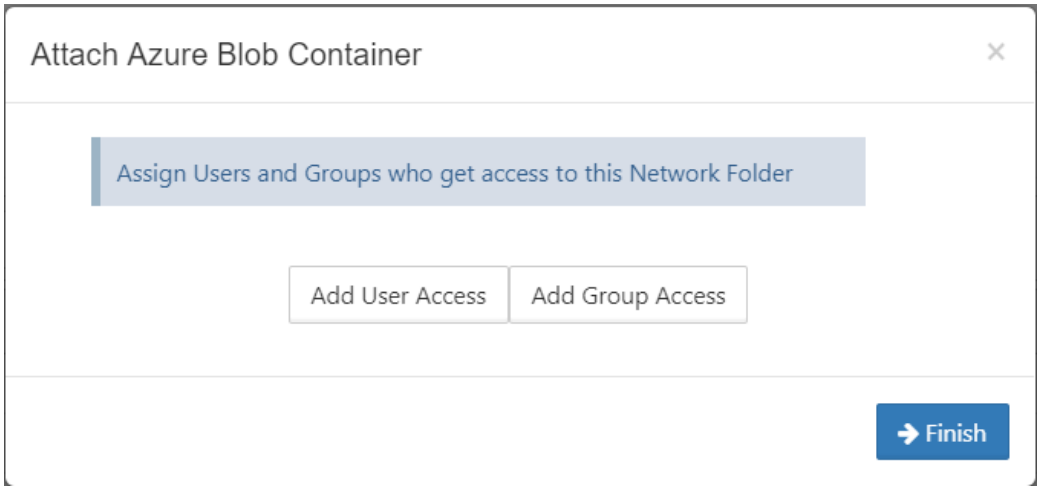
Create a Network Folder Based on an Azure Blob Storage

Administrators can integrate an Azure Blob Storage container with FileCloud to give users access to this data inside FileCloud Server portals and clients.



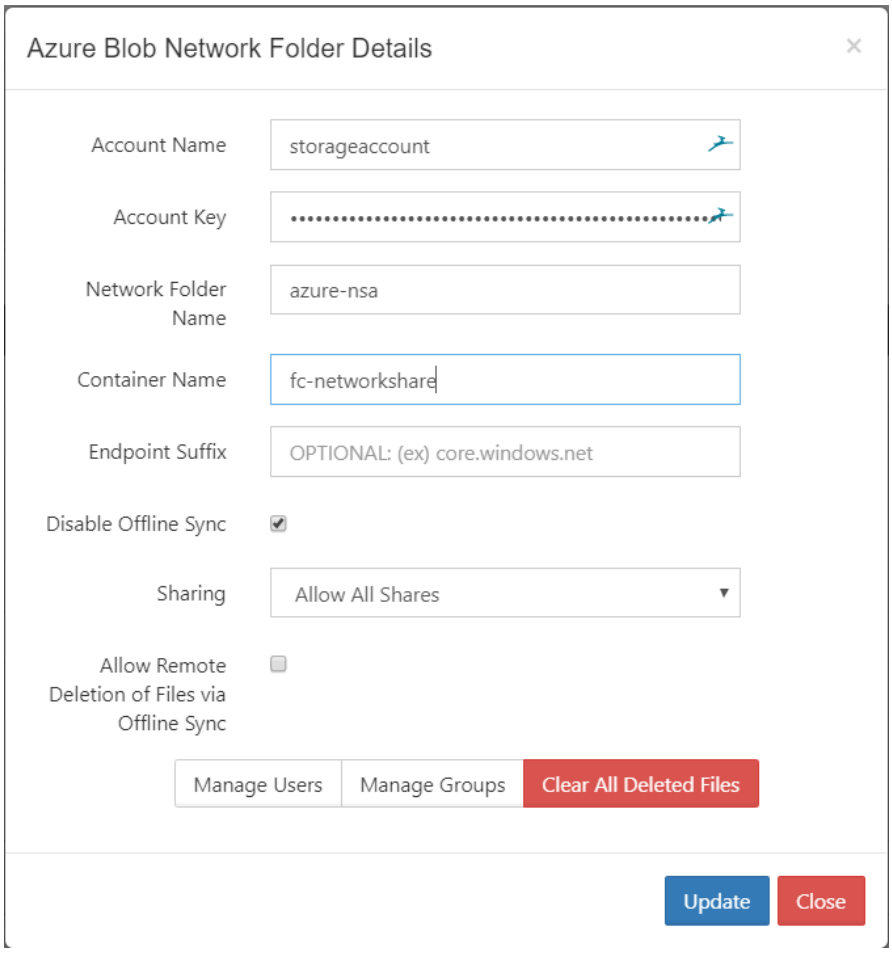
To create a network share from the Azure Blob Storage Container:

1. Open a browser and log in to the Admin Portal.
2. In the left navigation panel, select **Network Folders**.
3. On the Manage Network Folders window, click **Add.**
4. On the New Network Folder dialog box, in Select network type, select **Azure Blob Storage Container**, and then click **Next**.
5. In **Network Folder Name,** enter a unique name for the Network Folder and then click **Next**.
6. Enter an **Account Name** and **Account Key**, and then click **Next**.
7. Enter the **Container Name** and optionally, the **Endpoint Suffix**, and then click **Next**.
8. When the Azure Blob Storage container is mounted as a network share, assign permissions to users or group to allow access. The network share access can be granted to:
   - Guest User
   - Full Access User
   - User Group



Configure Azure Blob Storage Container-Based Network Folders

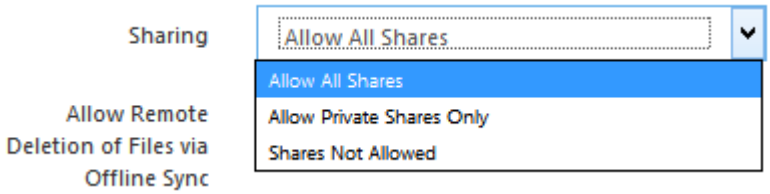
After you attach an Azure Blob Storage container to a FileCloud Server Network Folder, you can update any of the original settings.



To edit an an Azure Blob Storage container-based Network Folder:

1. Open a browser and log in to the Admin Portal.
2. In the left navigation panel, select **Network Folders**.
3. On the Manage Network Folders window, click the Azure Blob Storage container-based network folder, and then click the edit icon.
4. On the Azure Blob Network Folder Details window, set any of the following options:

Option	Description
Account Name	Name of the Azure storage account

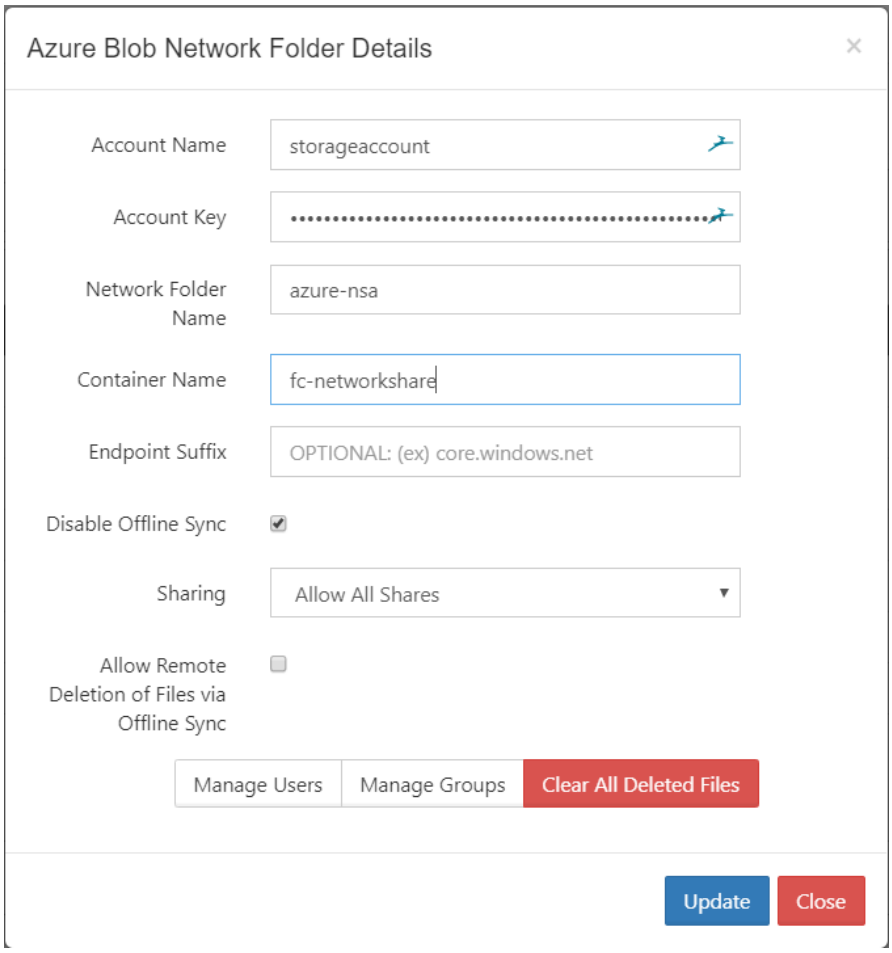
Option	Description
Account Key	Azure's Storage account key
Network Folder Name	Name of the network share
Container Name	Name of the container - it has to exist in Azure when creating a share
Endpoint Suffix	Endpoint suffix. To use an Azure end point, it must be one of the values published here.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the Azure Blob Storage container if the files are deleted in the synced client. By default deletes are not propagated to Azure Blob Storage container when deleted via Sync client.

Clearing Deleted Files from Azure Blob Storage Network Folders

Administrators can clear the files deleted by users in Network Folders.

Why?

The files deleted by users that are moved to the recycle bin (if enabled) take up space over time.



To clear deleted files in an an Azure Blob Storage Network Folder:

1. Open a browser, and log on to the admin portal.
2. On the left navigation pane, under **Manage**, click **Network Folders**.
3. On the **Manage Network Folders** window, click the row containing the folder you want to clear of deleted files.
4. Click the edit icon ( ).
5. On the **Azure Blob Storage Network Folder Details** window, click **Clear All Deleted Files**.
6. To save your changes, click **Update**.

Network Folder Limitations

- **Offline Syncing of Network Folders:** Since Network Folders are stored outside of FileCloud, offline syncing of files using the Sync app can be slower and can cause more server CPU load. If offline syncing is needed for folders with more than 5,000 subfolders, it is recommended to use Managed Storage.
- **Folder and File Listings can be Slower:** Depending upon network connectivity to the Network Share, it can take more time to access and list Network Folders than Managed Storage. To

improve response time in the user portal, FileCloud includes a feature that caches the Network Folder listing and maintains the cache for thirty minutes. By default, this feature is enabled, but you can disable it.

To disable caching of Network Folders:

a. Open the configuration file:
Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux: /var/www/config/cloudconfig.php

b. Add the line:

```
define("TONIDO_CACHE_NETWORK_FILELIST", 0);
```

- **Paths that exceed 255 characters:** When using network folders on Windows, file paths that exceed 255 characters cannot be processed.

  To fix this problem, use the prefix \\?\ in front of your Network Folder path. Using this prefix allows paths of up to 1024 characters.
  With the prefix, the path is formatted as:
  \\?\C:\[Network Folder name]

  Note: FileCloud Drive and FileCloud Sync can handle paths of up to 32,000 characters in Windows. However, in some cases, this may be limited by the application or the server.
- Folders containing very large amounts of content may time out when displayed in the user portal. The maximum size is determined by your environment's OS and resource limitations.

Enabling Directory Scraping

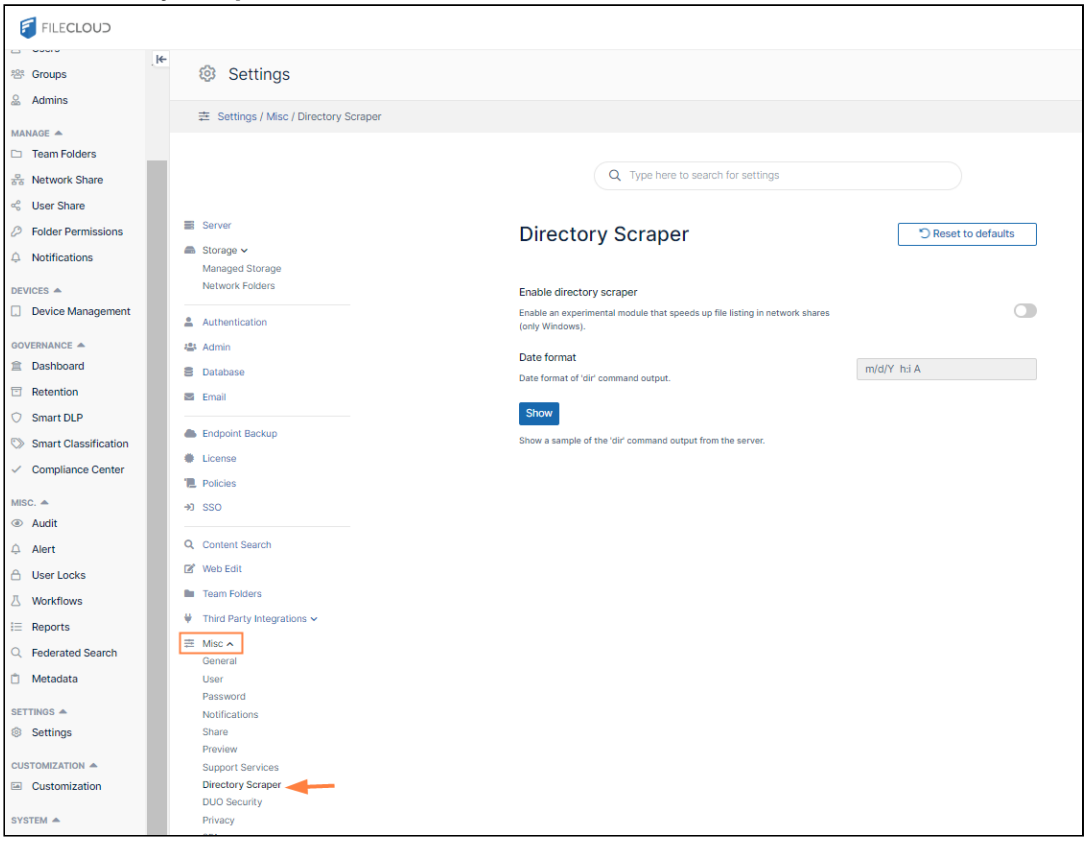
If FileCloud is running on Windows OS but Network Folders are on a slower network, then listing of files/folders in network shares will be very slow.
To list network files and folders more quickly, enable directory scraping.

Enabling Directory Scraping

1. Open the Directory Scraper settings page.
   To open the Directory Scraper settings page

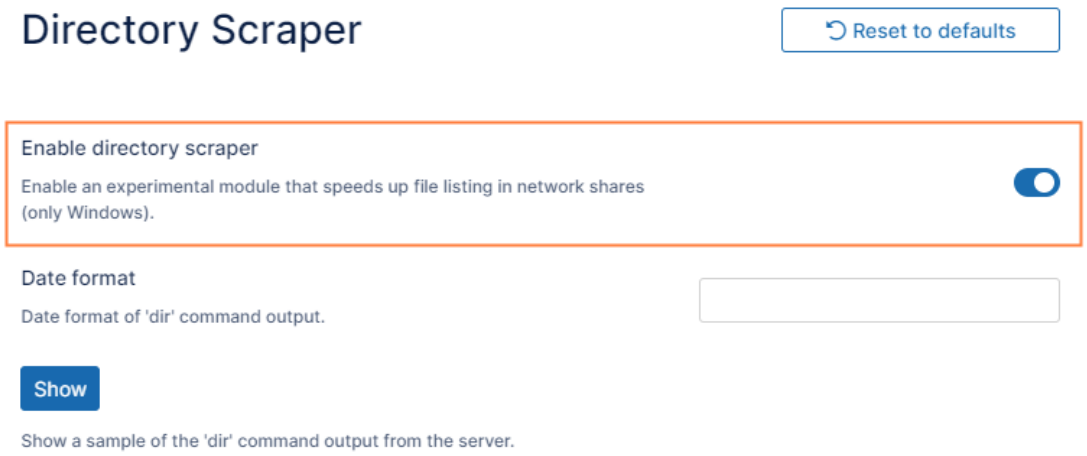
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Directory Scraper**, as shown below.



The **Directory Scraper** settings page opens.

2. Select the check box **Enable Directory Scraper**.



3. Correct the system date format, if needed. See To find the date format, below, for help finding your system date format.
4. Click **Save**.
   Now network shares will use directory scraping to get file listings.

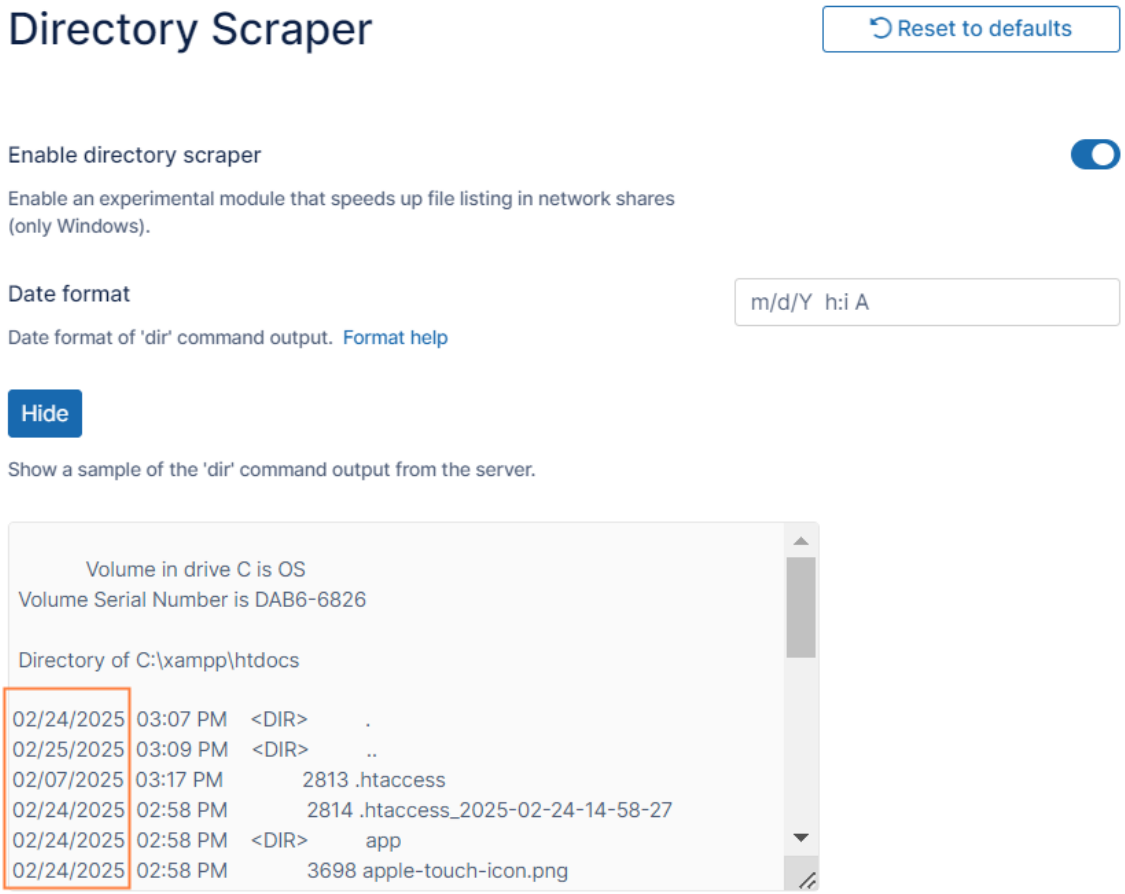
To find the date format:

Since directory scraping relies on the exact location and format of the output, any difference in the date format from FileCloud's default can cause issues.

To see the correct date format, click **Show**.



You are shown a sample of server output from the dir command, which includes the formatted date for you to reference.



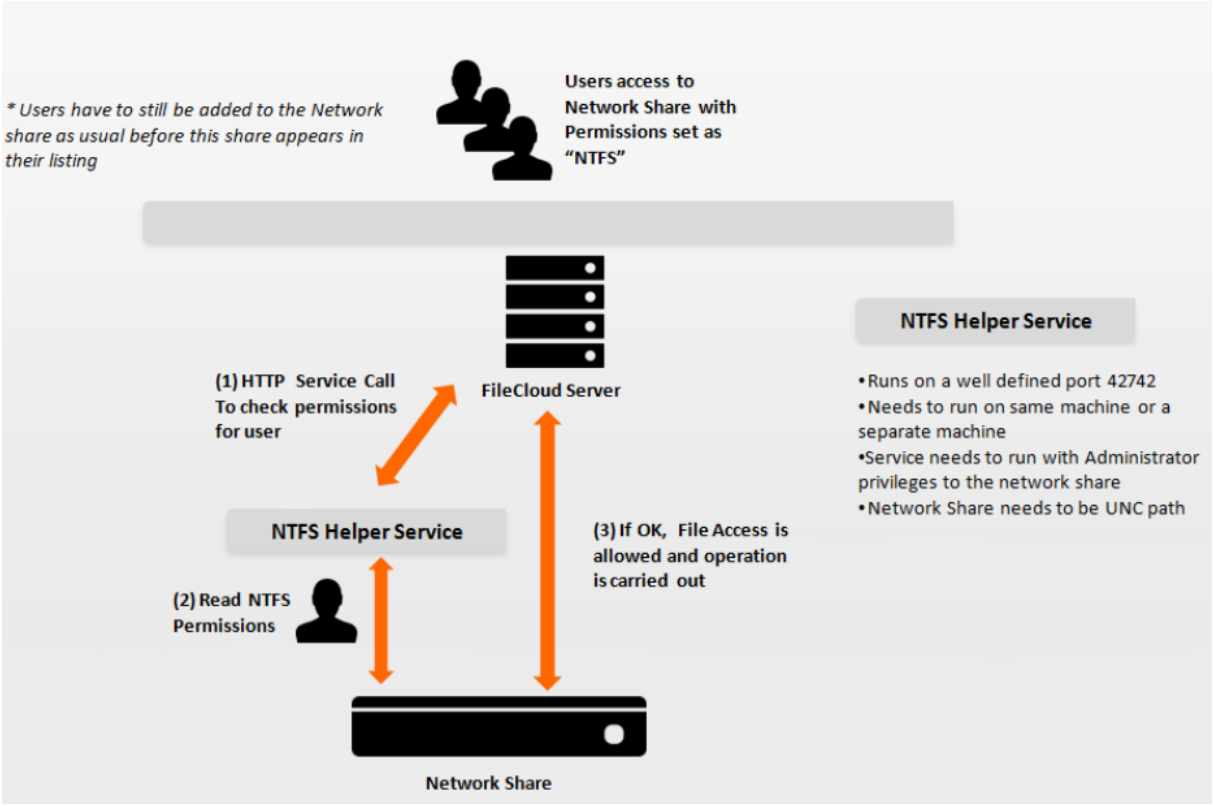
FileCloud Helper Service

You can use the FileCloud Helper service to perform these important functions on Network folders:

- Handle NTFS Permission checks for Network Folders configured with NTFS permissions
- Provide an indexed search of Network Folders
- Allow content search of documents for Network Folders

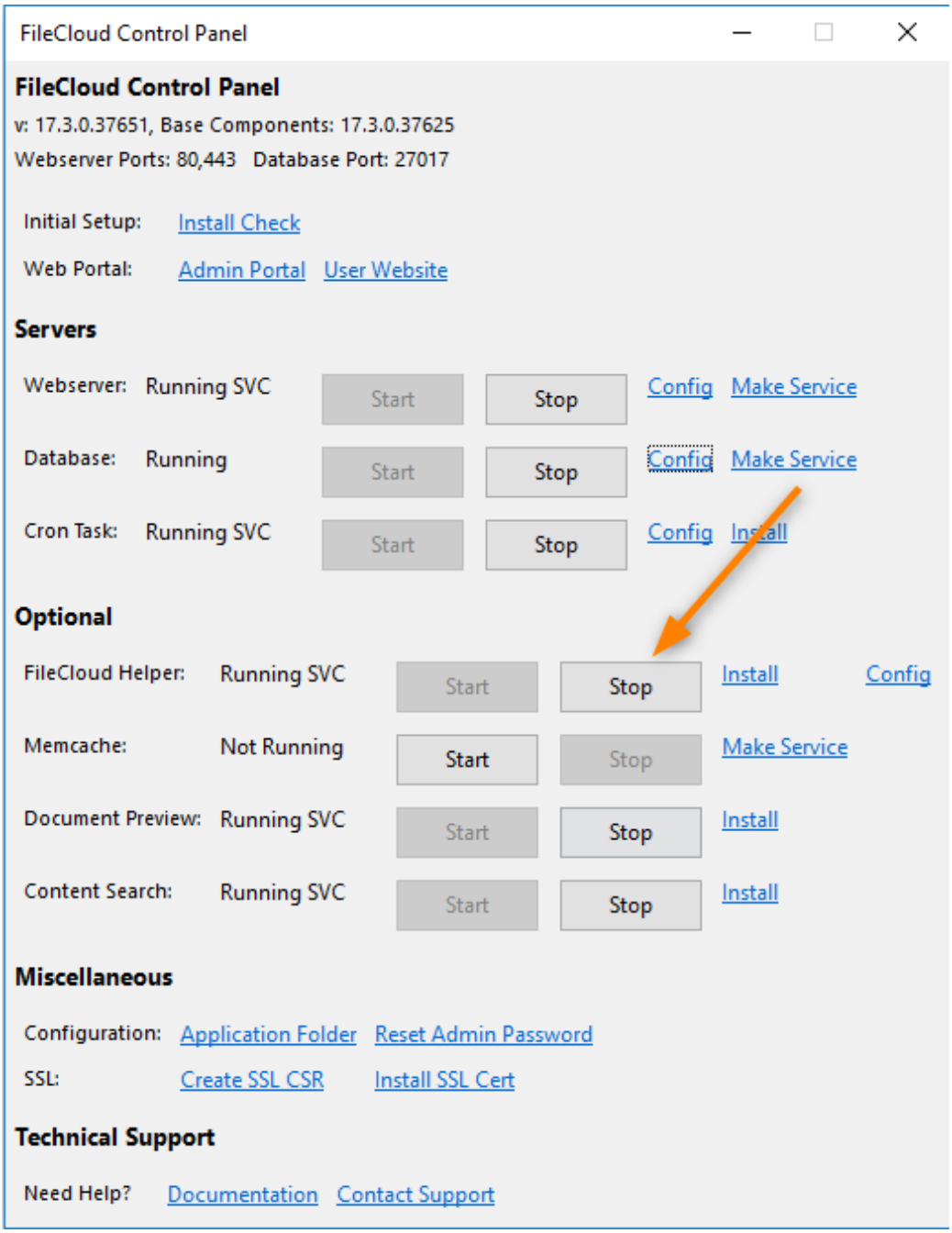
If you are running FileCloud on a Windows server, you **do not need** the Helper Service to perform NTFS permission checks as the Web Server itself can perform access checks.
If you are running FileCloud on a Linux server, you **do need** the Helper Service to perform NTFS permission checks.

Helper Service Architecture



Install Helper Service

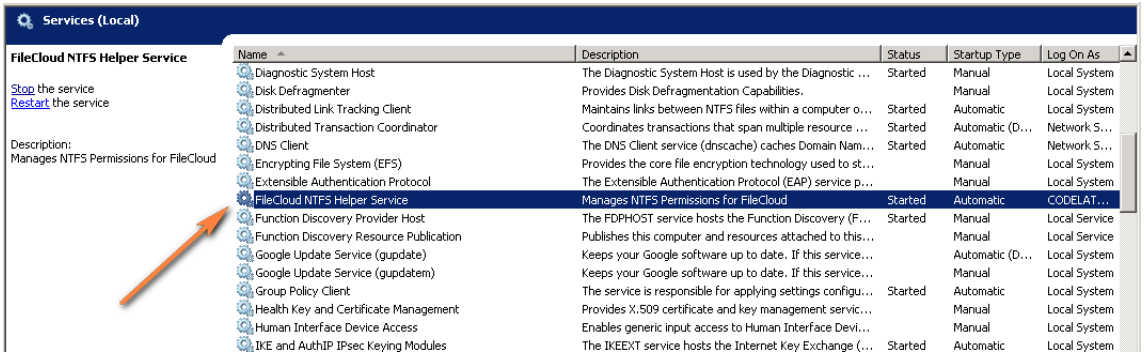
For FileCloud Server instances running on Windows, Helper service is a separate installation.



To install the FileCloud Helper service:

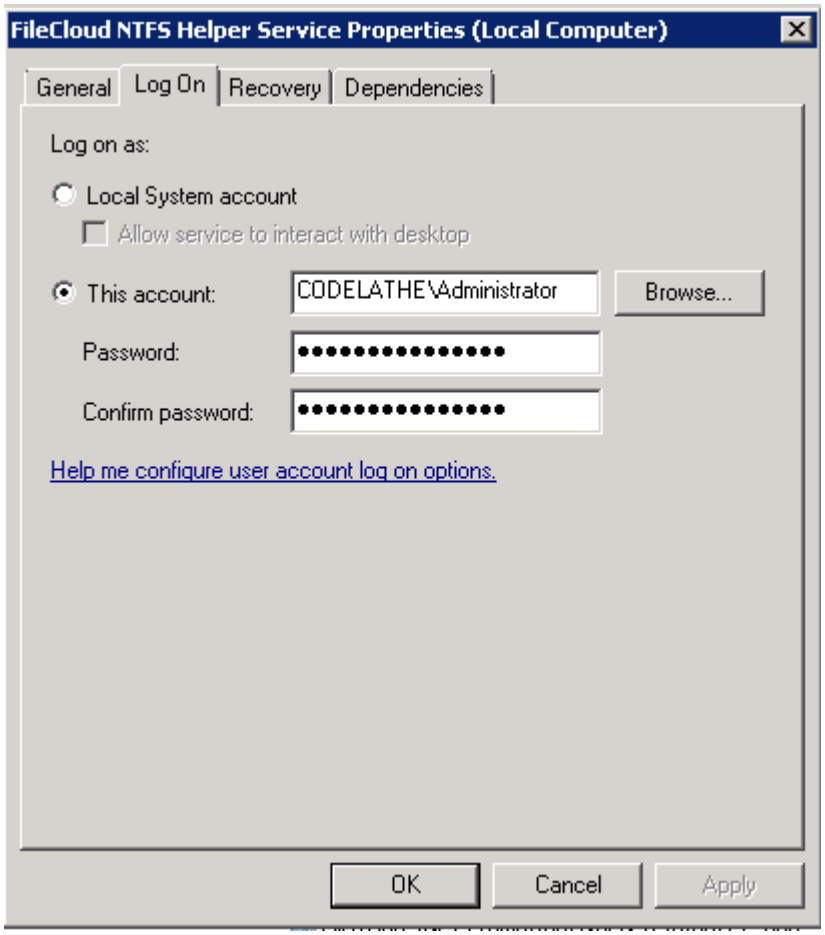
1. The download link for this service can be found in the customer portal. FileCloud helper service can also be installed from the FileCloud control panel using the install link.

> FileCloud Helper can only be installed on a local hard drive, so if your APPDATA folder points to a network location, installation will fail.



2. After installation, change the logon information for the FileCloud Helper service to the user account that has full access to all the network shares.

> Important: Note that this service cannot work properly when operating as a local system account. It has to run as a specific user account with permissions to the network share folder that is being shared via FileCloud.



Exclude Folder Paths from Indexing

As an administrator, you may see errors when FileCloud Helper service indexes Network Folders.

- FileCloud Server may return exceptions instead of skipping folders during real-time indexing of Network Folders for the specific paths.
- The best way to tell Helper service that you want to ignore some folders when indexing is to add regexes (regular expressions) paths to the folders.

To exclude files or folders from indexing:

1. Open the following file for editing

```
realtimeconfig.ini
```

2. Add the following line, replacing REGEX with a path to the files or folders that you want to skip during indexing of Network Folders.

```
skipregex=REGEX
```

For example:

The following line tells the Helper service to ignore all files in the Network Folders sub-folder called **archived**.

```
skipregex=mynetwork/ntfs/archived
```

Run Server and Helper on Different Machines

Normally FileCloud and Helper are run on the same machine.

- If you are running FileCloud on Linux, then it is impossible to run Helper on Linux as well.
- In this case install the Helper on a Windows machine.

You can use these steps to configure the FileCloud Server with the right location and map path information required.

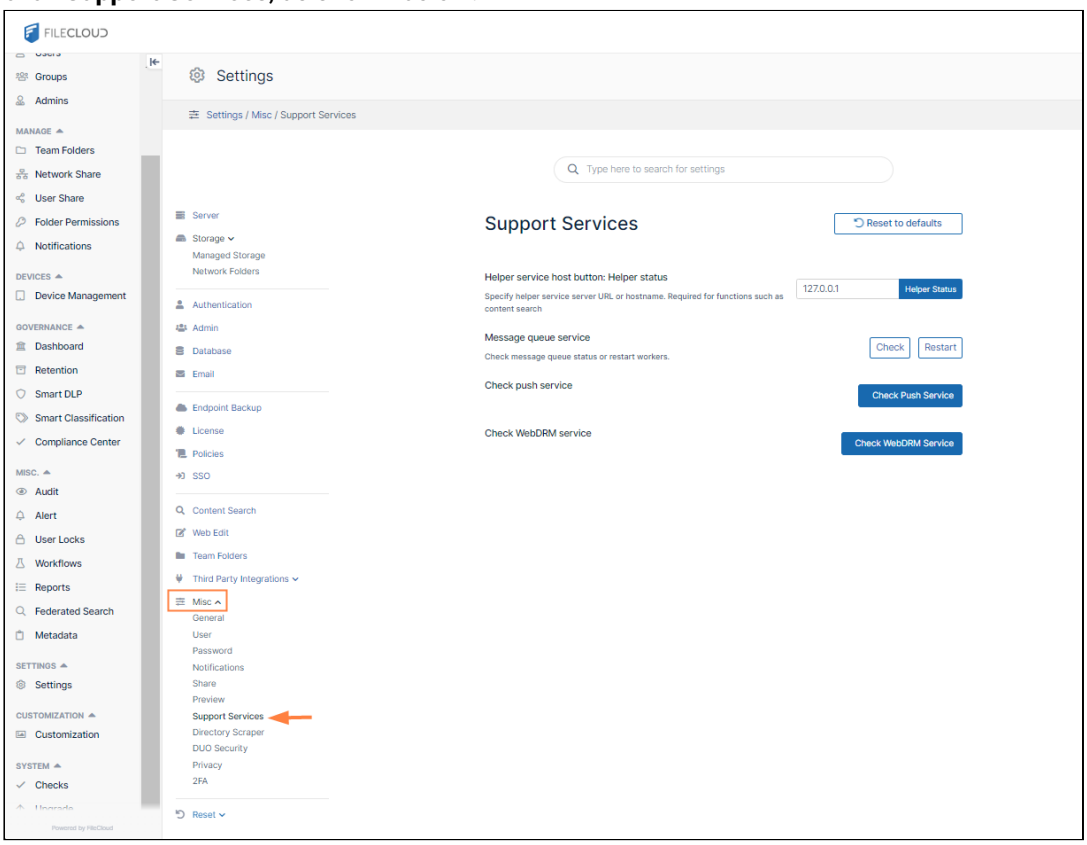
💡 It is recommended that, if possible, you run both Helper and FileCloud on Windows.

To configure FileCloud Server to Find Helper on Another Machine:

1. Open the Support Services settings page.
   To open the Support Services settings page

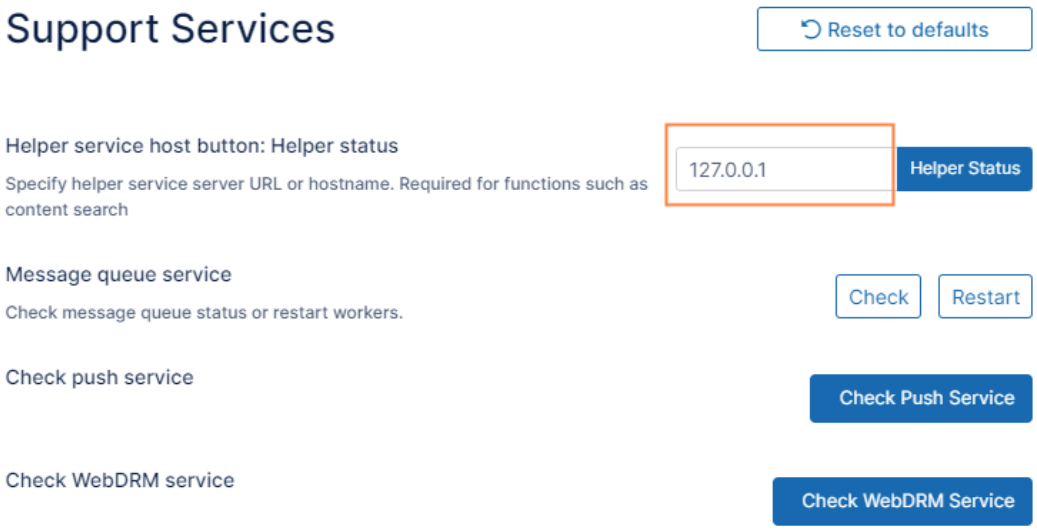
a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Support Services**, as shown below.



The Support Services settings page opens.

2. In **Helper service host button**, enter the host name or host address of the computer running the Helper service.



3. Click **Save**.
4. On the Helper server, open the following location:

```
%appdata%\FileCloudHelper
```

5. Edit or create (if not available) config.ini in the install folder and change the following lines:

```
; Settings for FileCloud Helper
[settings]
address=0.0.0.0
```

6. Edit the pathmap.ini file and add the network path to the same path used by Linux but accessed by Windows:

```
; Path maps for FileCloud Helper
; Example format is <remote path> = <local path>
; e.g. /network/share1=\\share1comp\sharedfolder\share1
[pathmaps]
/mnt/share1=\\share1comp\sharedfolder\share1
```

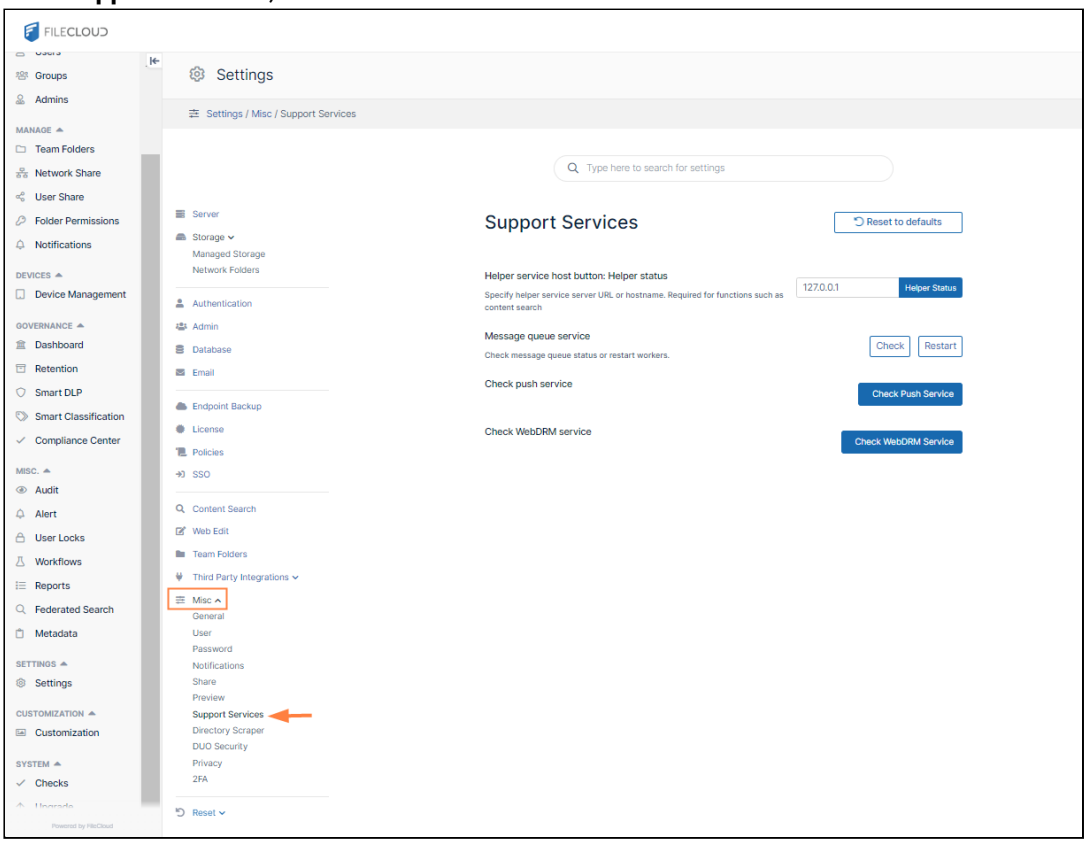
7. Restart the FileCloud Helper service.

Improve Helper Performance

As an administrator, you can use built-in tools to check the status of the service and you can also increase the expiry time of the cached results so that existing results can be returned faster.

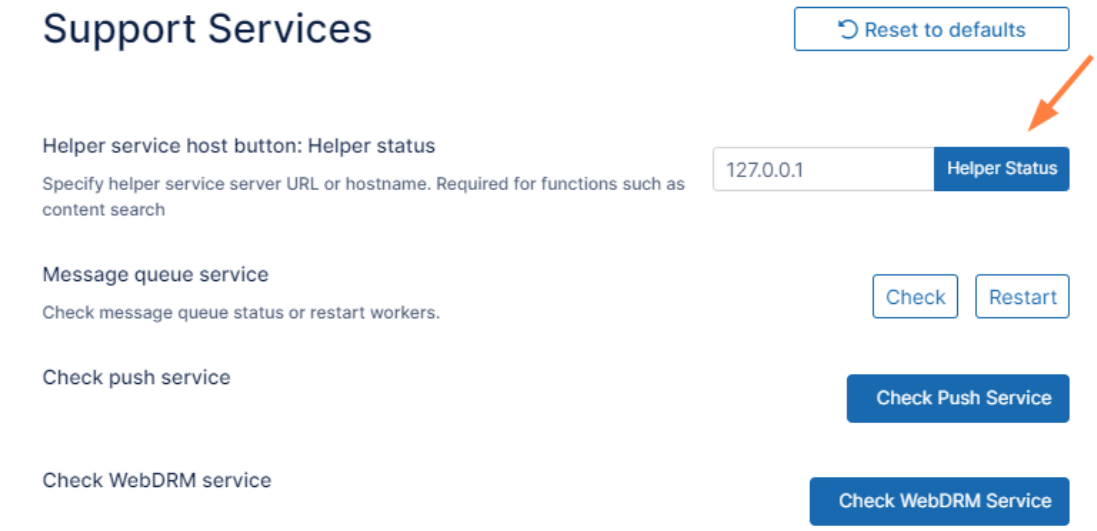
To check the status of Helper Service:

1. Open the Support Services settings page.
   To open the Support Services settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Support Services**, as shown below.

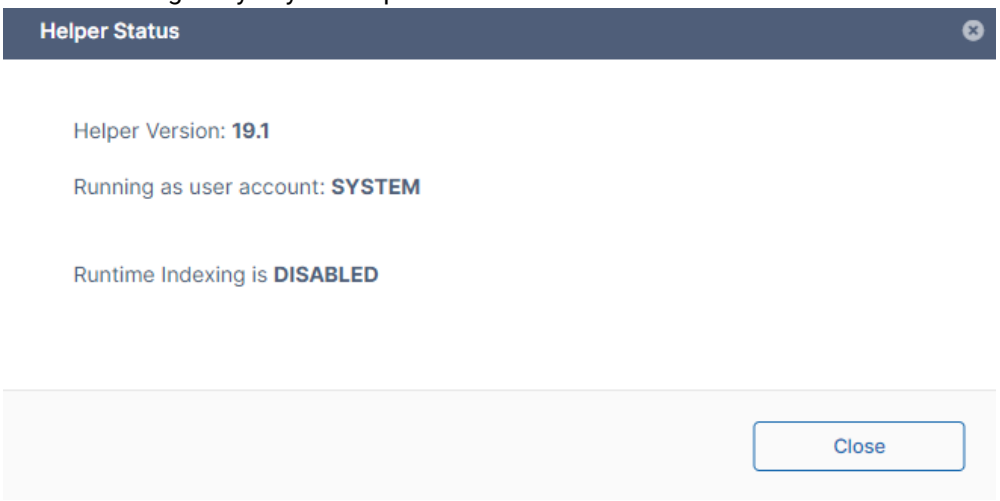


The Support Services settings page opens.

2. Click **Helper Status**.



A notification gives you your Helper status:



Return Permission Results Faster

By default, Permissions check results are cached for 30 seconds.

- For systems where the permissions are not changing dynamically, you can increase the expiry time of the cached results.
- Reducing the cache expiry time can improve responsiveness for systems with frequently changing permissions.

To modify the cache expiry settings:

1. Open the following file for editing.

```
config.ini
```

2. Find the following code

```
; Settings for FileCloud NTFS Helper
[settings]
address=0.0.0.0
cacheexpiry=30000
```

3. Set **cacheexpiry** to a value that is less than you are using now. Use Table 1 options to understand how to set this value.

Table 1. Settings for FileCloud NTFS Helper

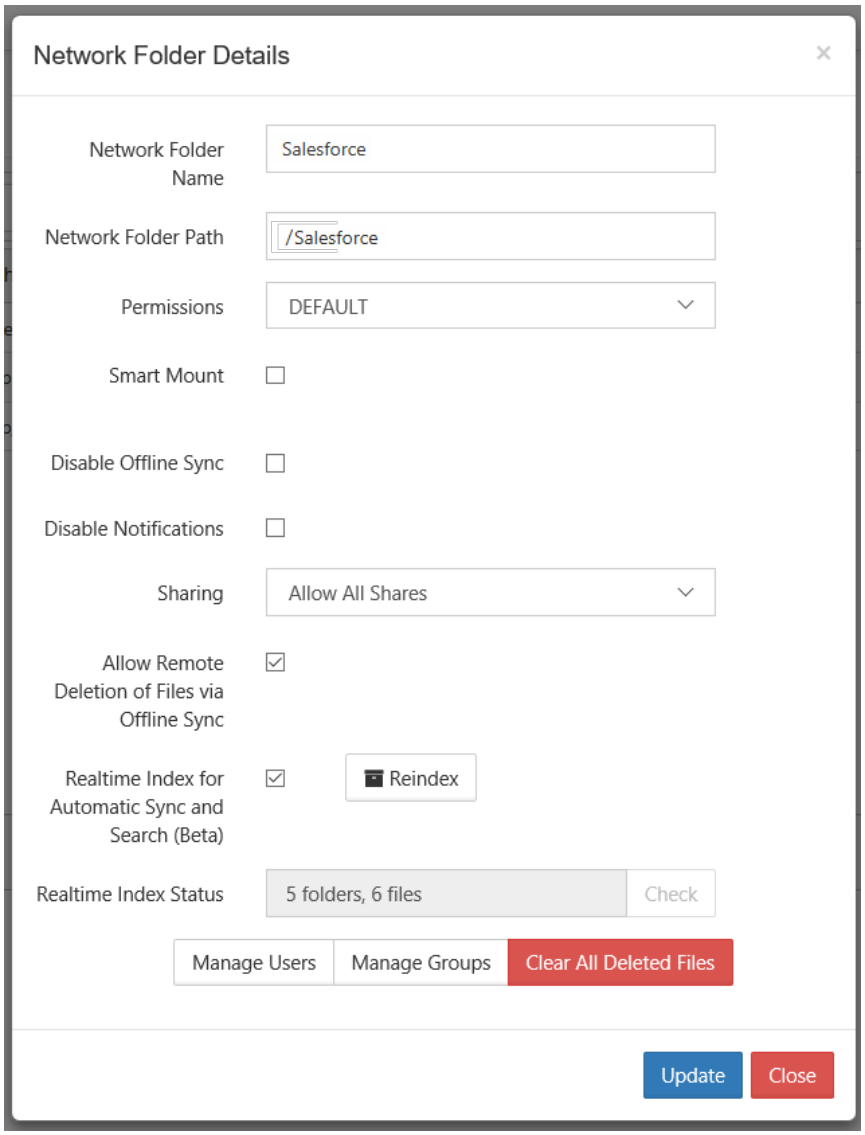
Parameter	Notes	Default Value
cacheexpiry	specifies how long cached results are stored in memory for faster performance. Specified in microseconds	30000 us (30 secs)
threadpoolsize	specifies the number of threads pre-created in the threadpool for fast spin up	40
threadmaxqueued	sets the maximum number of queued connections If there are already more than the maximum number of connections new connections are discarded.	64
threadmaxthreads	sets the maximum number of simultaneous threads	30
threadidletime	sets the maximum idle time for a thread before it is terminated, specified in seconds	600 (10 mins)

Clearing Deleted Files from Network Folders

Administrators can clear the files deleted by users in Network Folders.

Why?

- Files deleted by users are moved to recycle bin (if enabled).
- The files in recycle bin will take up space over time.



To clear deleted files in Network Folders:

1. Open a browser and log on to the **Admin Portal**.
2. On the left navigation pane, under **Manage**, click **Network Folders**.
3. On the **Manage Network Folders** window, click the row containing the folder you want to clear of deleted files.
4. Click the edit icon.
5. On the **Network Folder Details** window, click **Clear All Deleted Files**.
6. To save your changes, click **Update**.

Display Names that Start with a Dot

As an administrator you have the option to display files and folders that have a name starting with a (.) dot.

- This option can be set for network shares.

By default, if you:

- Create a network share from a folder that has a name starting with a dot (.), for example, .SystemTest
- Share it with another user
- When the user browses to the share the folder will not be displayed and it will appear empty

Similarly, if you:

- Create a network share from a folder with a name that does not start with a dot (.), for example, AdminTest
- Create files inside this folder that have a filename that starts with a dot (.), for example .Atest1, .ATest2
- Share it with another user
- When the user browses to the share the folder will be displayed but the files inside will not and it will appear empty

To display folders and files that start with a dot (.) :

1. Open the following file for editing:

```
cloudconfig.php
```

2. Add the following line:

```
define("TONIDOCLOUD_SHOW_FILES_STARTWITH_DOT", 1);
```

3. Refresh User Portal web page and the folders and files are now visible.

Wasabi S3 Bucket Based Network Folders



FileCloud officially supports only Amazon S3 storage to be configured as Network Folders.

- Other Amazon S3 compatible storage systems are supported through our Amazon S3 drivers, including:
  - Wasabi

- Backblaze B2
- Cloudian
- The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

Administrators can integrate Wasabi's S3 buckets with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

What is a Wasabi bucket?

Wasabi S3 is cloud storage for the internet.

To upload your data (photos, videos, documents etc.), you first create a bucket in one of the Wasabi Regions.

You can then upload any number of objects to the bucket.

⚠ There are a few limitations you should know about using Wasabi S3 bucket network folders.

1. No versioning support (Version key will be ignored and the file will be overwritten)
2. No real-time network sync or indexed search is allowed (Regular file search will work)

What do you want to do?

Attach an AWS S3 Bucket to a Network Folder	Create a Network Folder for Wasabi S3 Bucket
Configure the bucket-based Network Folder	Configure the AWS S3 bucket-based Network Folder Clear All Deleted Files

Create a Network Folder Based on an Wasabi S3 Bucket

Administrators can integrate Wasabi S3 buckets with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

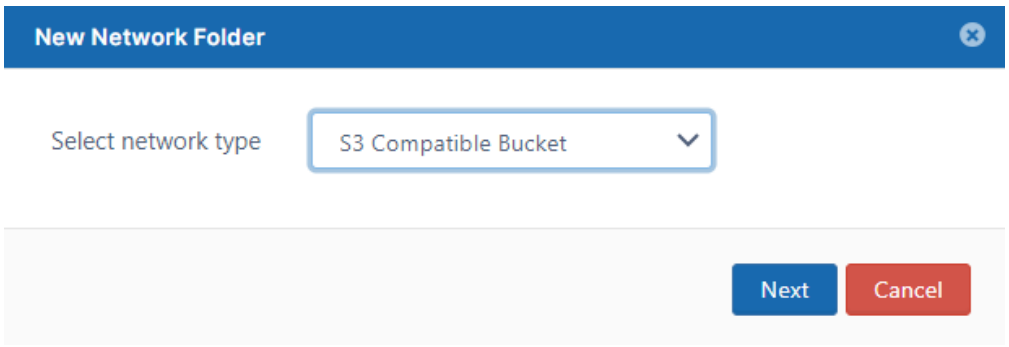
⚠ There are few limitations you should know about using Wasabi S3 bucket network folders

1. No versioning support (Version key will be ignored and the file will be overwritten)
2. No real-time network sync or indexed search is allowed (Regular file search will work)

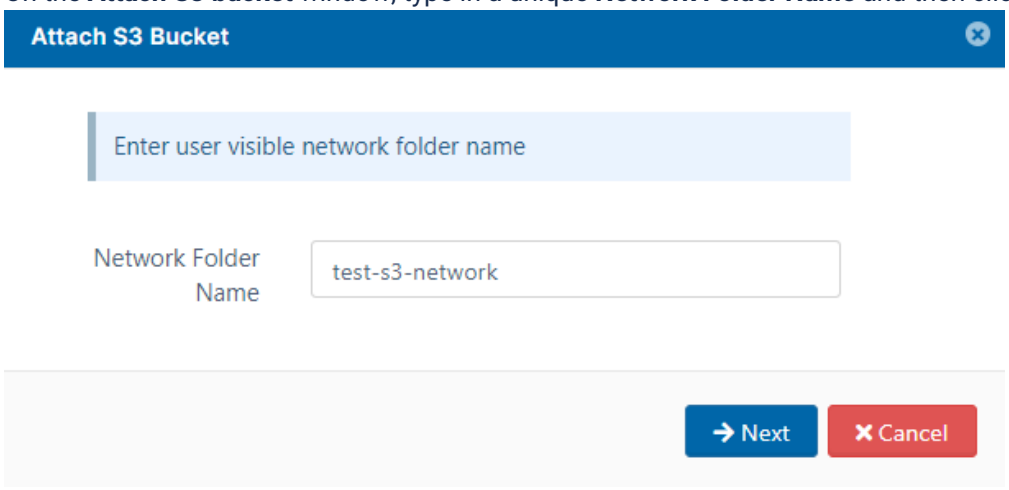
To create a Network Folder from an S3 bucket:

1. Open a browser and log in to the Admin Portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.

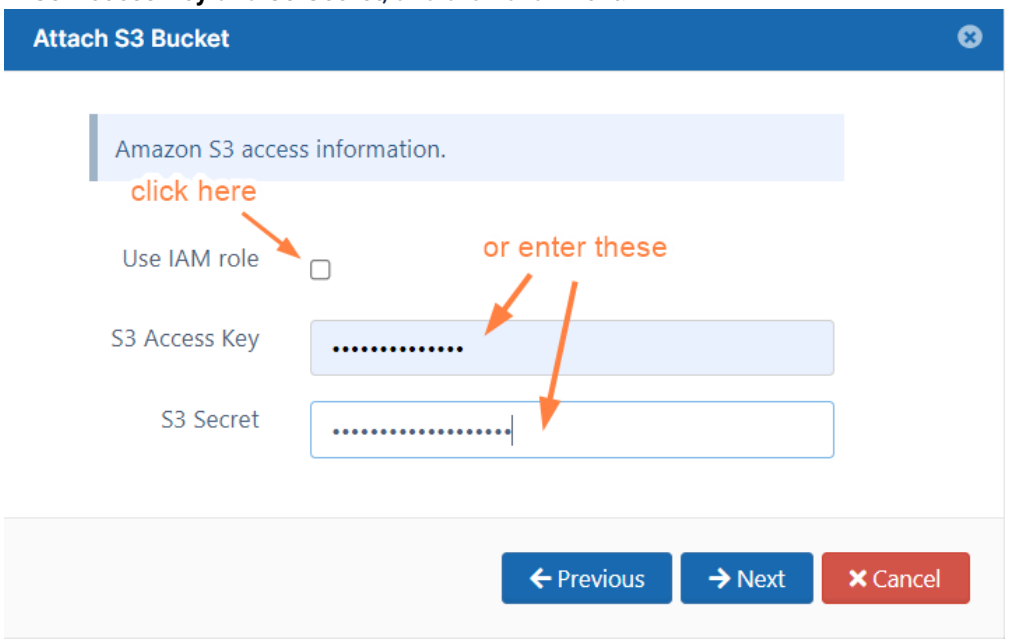
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



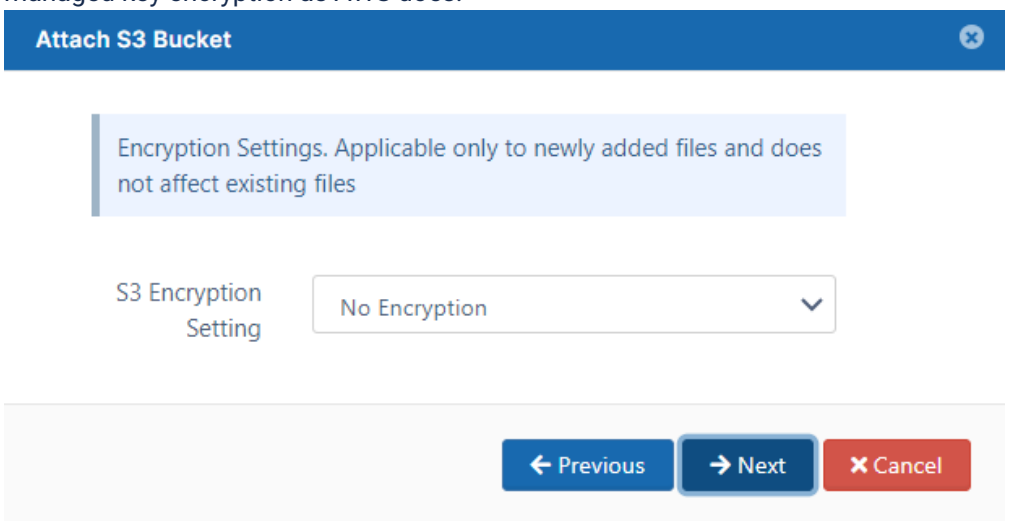
5. On the **Attach S3 bucket** window, type in a unique **Network Folder Name** and then click **Next**.



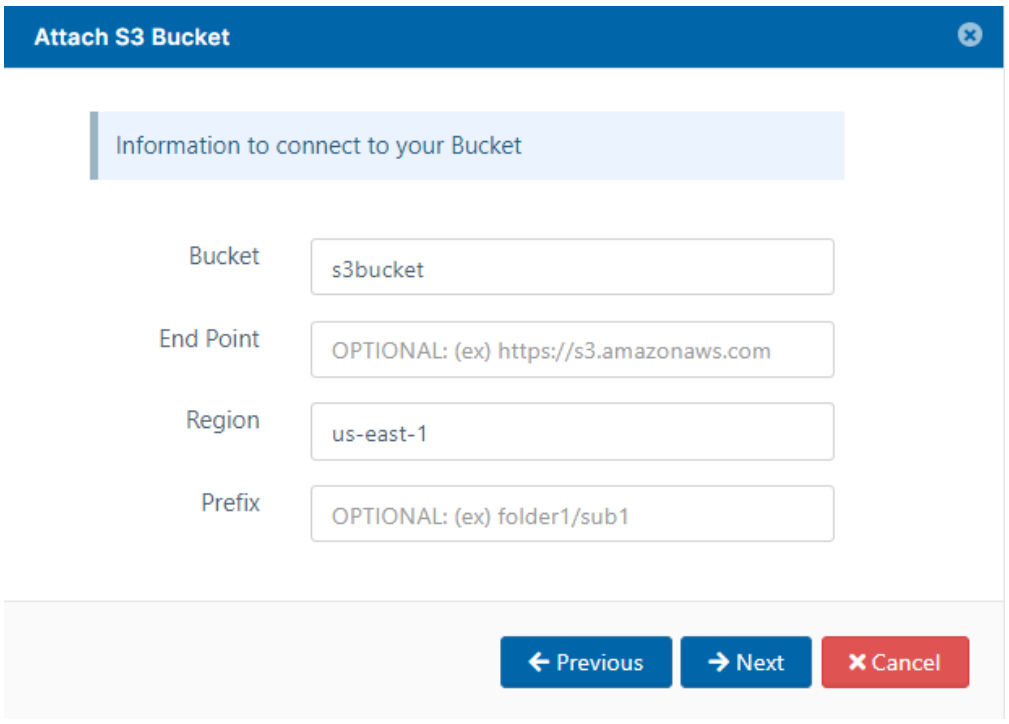
6. On the **Attach S3 Bucket** window, either check **Use IAM role** or type in authentication credentials in **S3 Access Key** and **S3 Secret**, and then click **Next**.



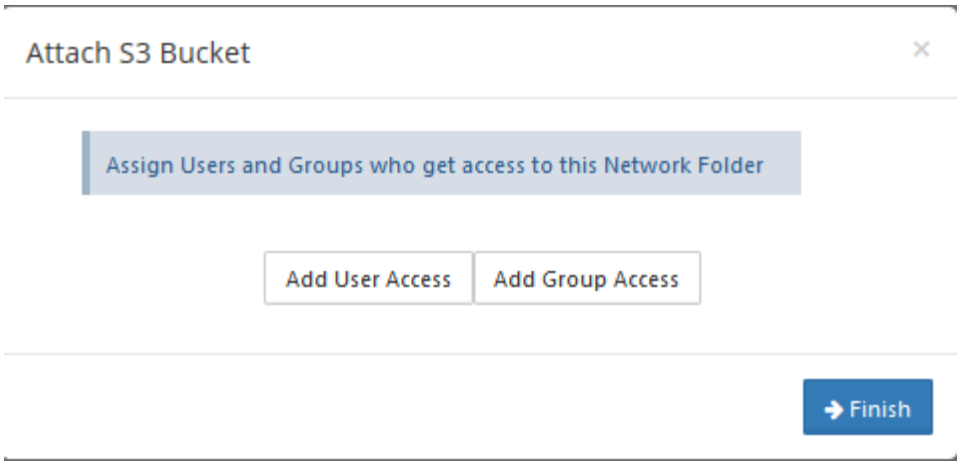
7. On the **Attach S3 bucket** window, select **No Encryption** because Wasabi does not provide managed key encryption as AWS does.



8. On the **Attach S3 bucket** window, type in the bucket name and **Region**, and optionally the **End Point** and **Prefix.**.
9. Click **Next**.

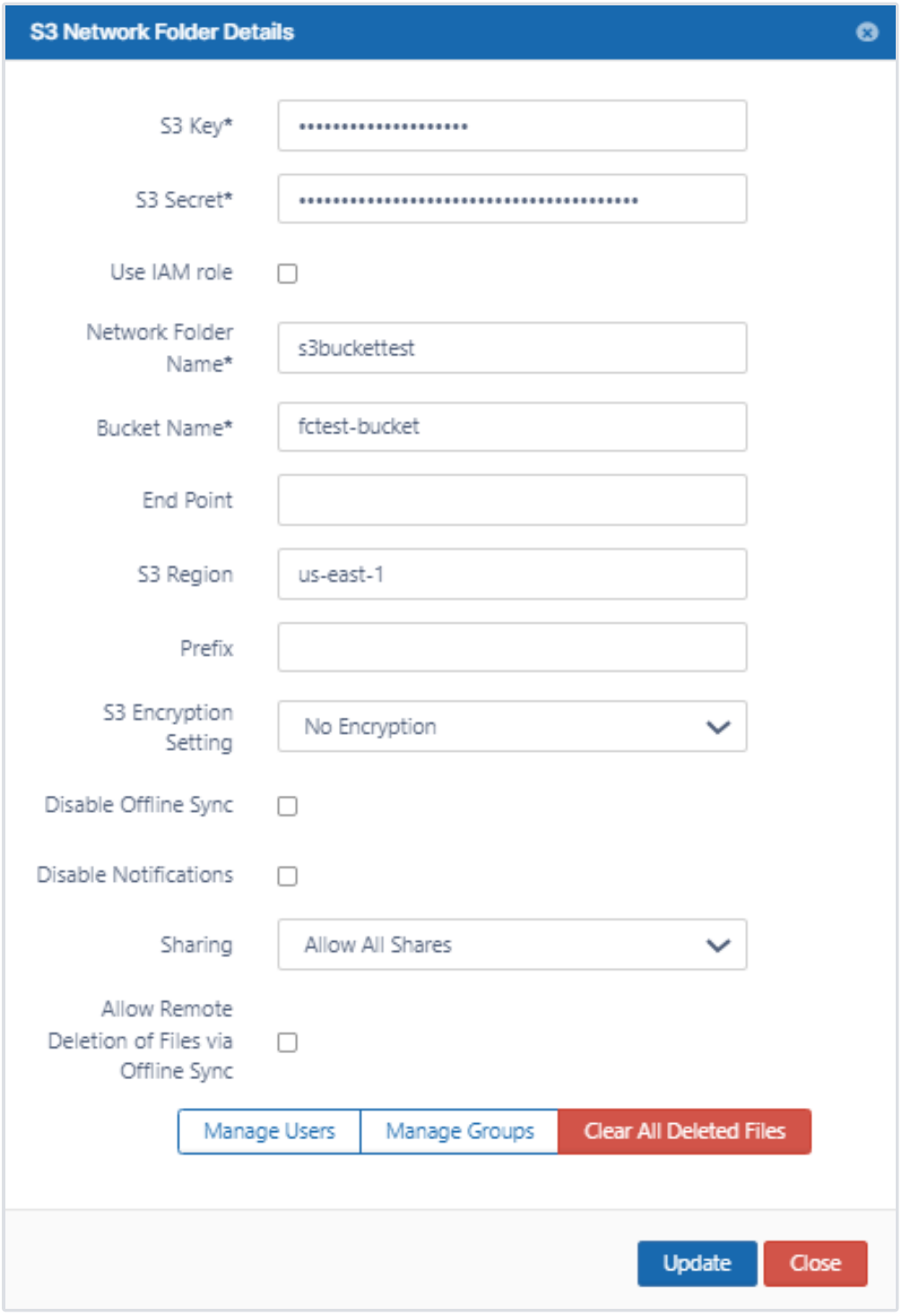


10. When the S3 bucket is mounted as a network share, permissions need to be assigned to users or group to allow access.
    The network share access can be granted to
    a. Guest User
    b. Full User
    c. User Group



Configure Wasabi S3 Bucket-Based Network Folders

After you attach a Wasabi S3 bucket to a FileCloud Server Network Folder, you can update any of the original settings.



To edit a Wasabi S3 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Wasabi S3 bucket-based network folder, and then click the edit icon.

4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
S3 Region	Physical region where buckets are created.
End Point	URL where API requests are sent.
S3 Encryption Setting	On the **Attach S3 bucket** window, select the type as **No encryption** because Wasabi does not support managed key encryption.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud Sync client
Disable Notifications	Disable some or all S3 Network Folder notifications for users with access to the folders. See **Disable notifications for Amazon S3 bucket-based Network Folders**, below.
Sharing	Sharing the content of the network share can be disabled or enabled using this option 

Option	Description
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to S3 bucket when deleted via Sync client.

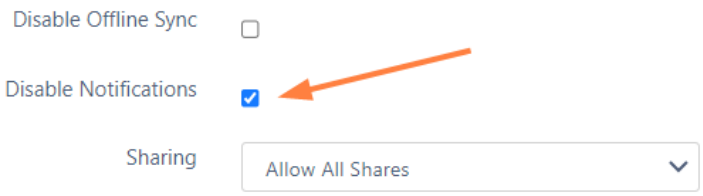
Disable notifications for Amazon S3 Network Folders

By default, notifications are enabled for network folders. This means that all users who have access to a network folder and have notifications enabled receive notifications about all actions on the folder.

However, since multiple users may have access to the same network folder, users may receive notifications about actions that don't interest or don't apply to them.

There are various ways you can limit their access to these notifications. First disable notifications for the folder, and then override the setting only for notifications that you want to permit.

1. Disable notifications for the folder:
   a. Click **Network Folders** in the left navigation menu to display the list of network folders
   b. Click the **Edit** button for the network folder.
   The **Network Folder Details** dialog box opens.
   c. Check the **Disable Notifications** box.



2. Click **Update**.
3. Do one of the following:

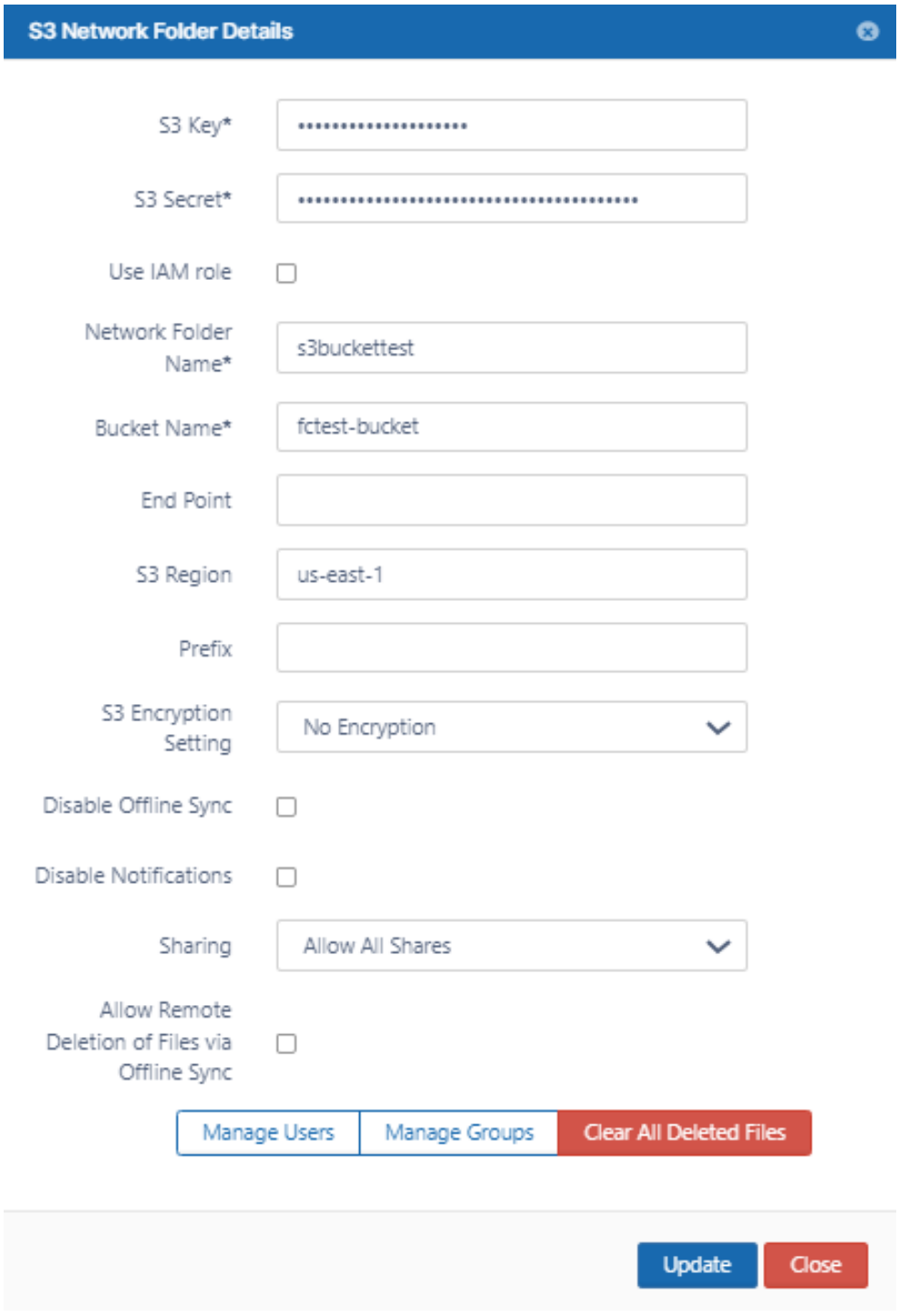
   - **Leave all notifications about actions in the folder disabled.**
   By default, admins and users can override this setting. An admin can enable notifications about the folder for specific users, or users can enable their own notifications for the folder.
   If you do not want users to be able to override this setting, you must disable file change notifications in **Settings > Misc > Notifications**. See Notifications for File Changes for help.

- **Enable notifications about the folder for specific users.**
  This is useful if you want to limit the users who receive notifications about a network folder to those you have shared it with.
  See the various options for setting users' notifications in the section Managing User-Defined Notifications.

- **Allow users to enable their own notifications about the folder.**
  See the options users have for setting their own notifications in the section Notifications.

Backblaze B2 Bucket Based Network Folders

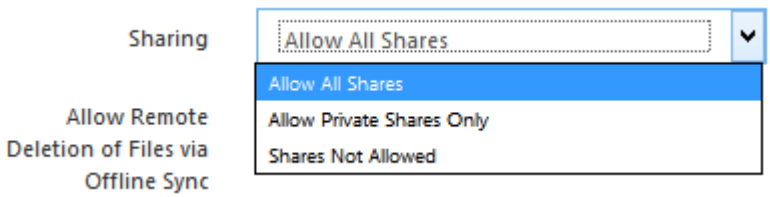
After you attach a Backblaze B2 bucket to a FileCloud Server Network Folder, you can update any of the original settings.



To edit a Backblaze B2 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Backblaze B2 bucket-based network folder, and then click the edit icon.

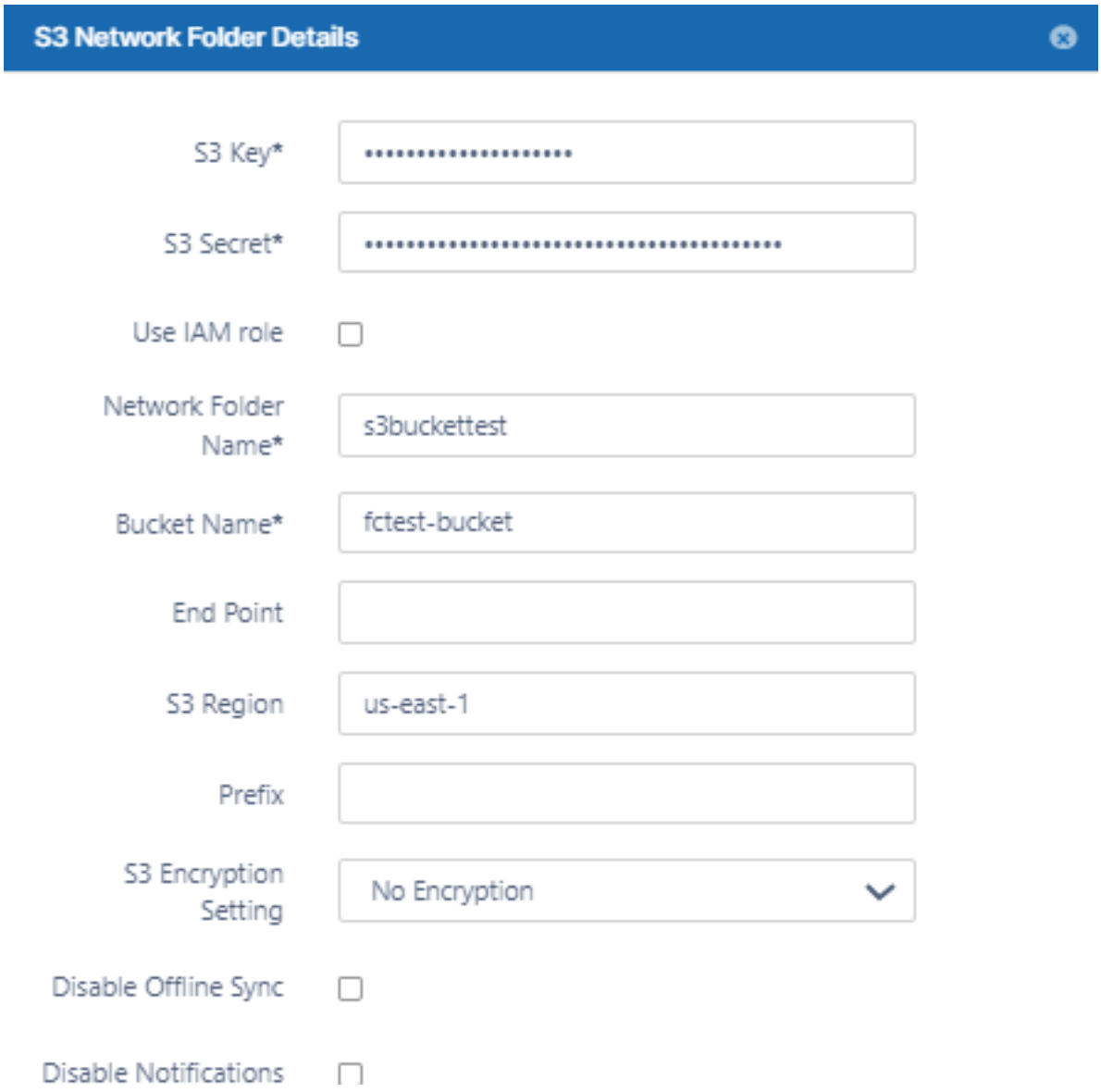
4. On the **S3 Network Folder Details** window, set any of the following options:

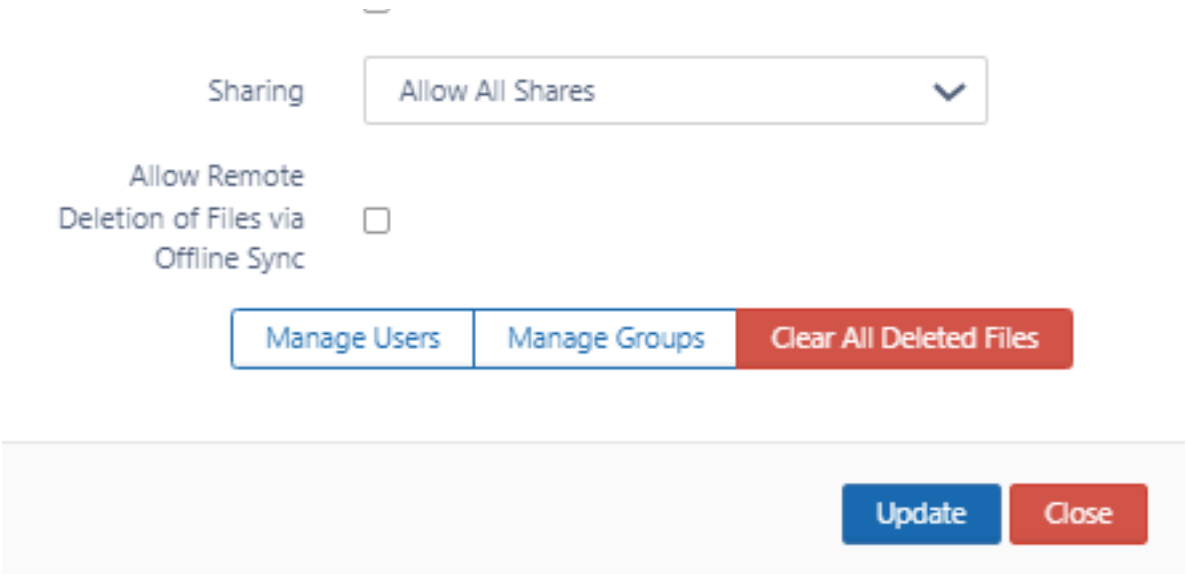
Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
S3 Region	Physical region where buckets are created.
End Point	URL where API requests are sent.
S3 Encryption Setting	**No Encryption** On the **Attach S3 bucket** window, select the type as **No encryption** because Backblaze does not support managed key encryption.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Sharing	Sharing the content of the network share can be disabled or enabled using this option 

Option	Description
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the B2 Bucket if the files are deleted in the synced client. By default deletes are not propagated to B2 bucket when deleted via Sync client.

Cloudian S3-Compatible Object Storage Network Folders

After you attach a Cloudian S3-Compatible Object Storage bucket to a FileCloud Server Network Folder, you can update any of the original settings.

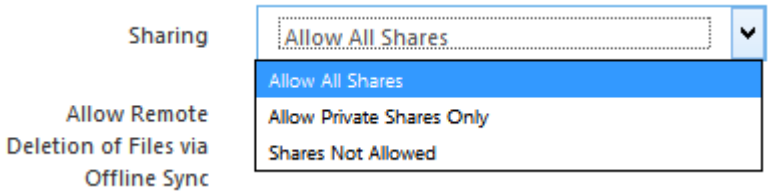




To edit a Cloudian S3-Compatible Object Storage bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Cloudian S3-Compatible Object Storage bucket-based network folder, and then click the edit icon.
4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear, and the IAM role is used to connect to the S3 bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
End Point	URL where API requests are sent.

Option	Description
S3 Region	Physical region where buckets are created.
Prefix	Optional. A prefix to add to the network share paths to create sub-paths within the bucket.
S3 Encryption Setting	**No Encryption** - On the **Attach S3 bucket** window, select the type as **No encryption** because Cloudian does not support managed key encryption.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud Sync client
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the Cloudian S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to Cloudian S3 bucket when deleted via Sync client.

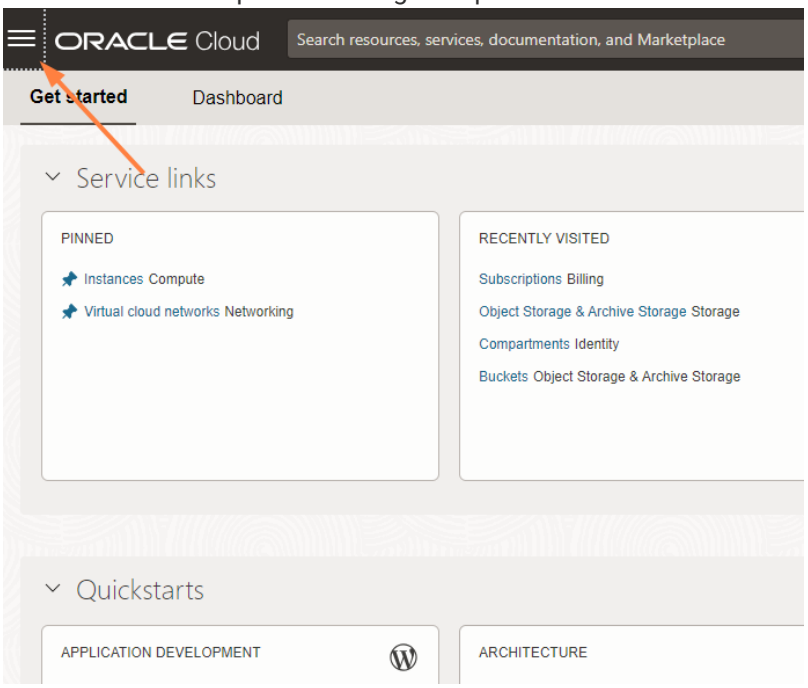
Oracle Cloud Infrastructure S3 Bucket Based Network Folders

To create the S3 storage bucket and get your S3 key values in Oracle Cloud Infrastructure

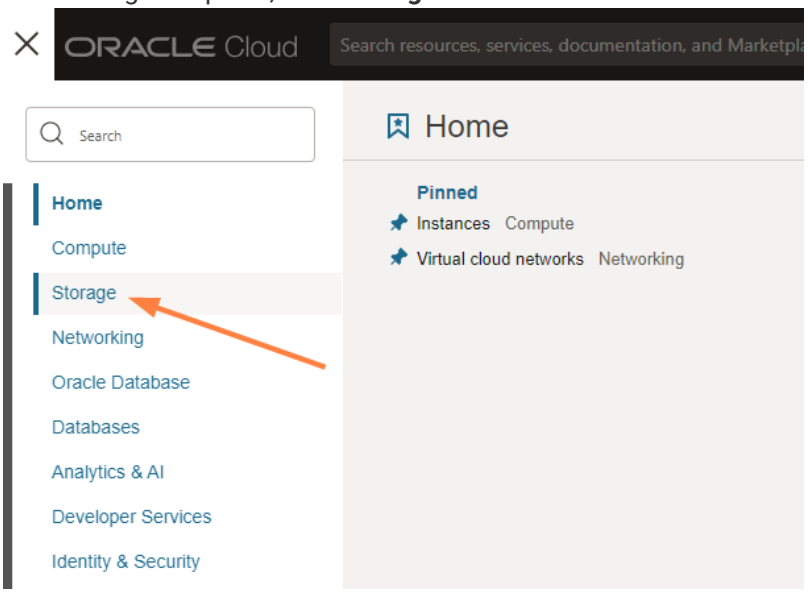
Create the S3 storage bucket and generate your S3 keys. In addition, save the values you will need to enter when you are configuring the OCI/FileCloud integration in the next procedure on this page.

1. Log in to **https://cloud.oracle.com**.

2. Click the icon that opens the navigation panel:

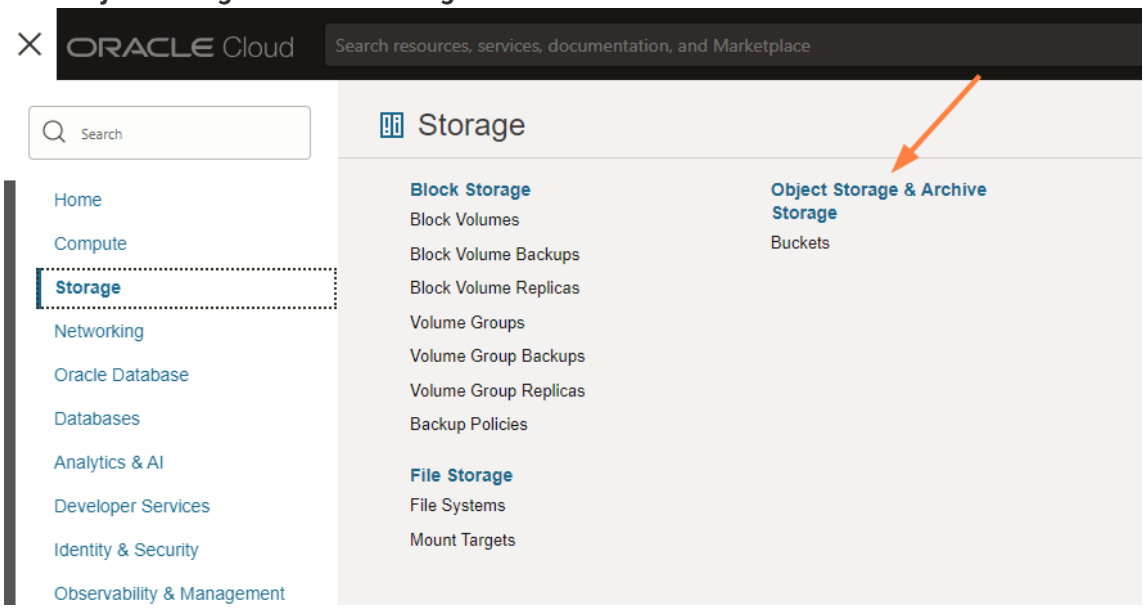


3. In the navigation panel, click **Storage**.



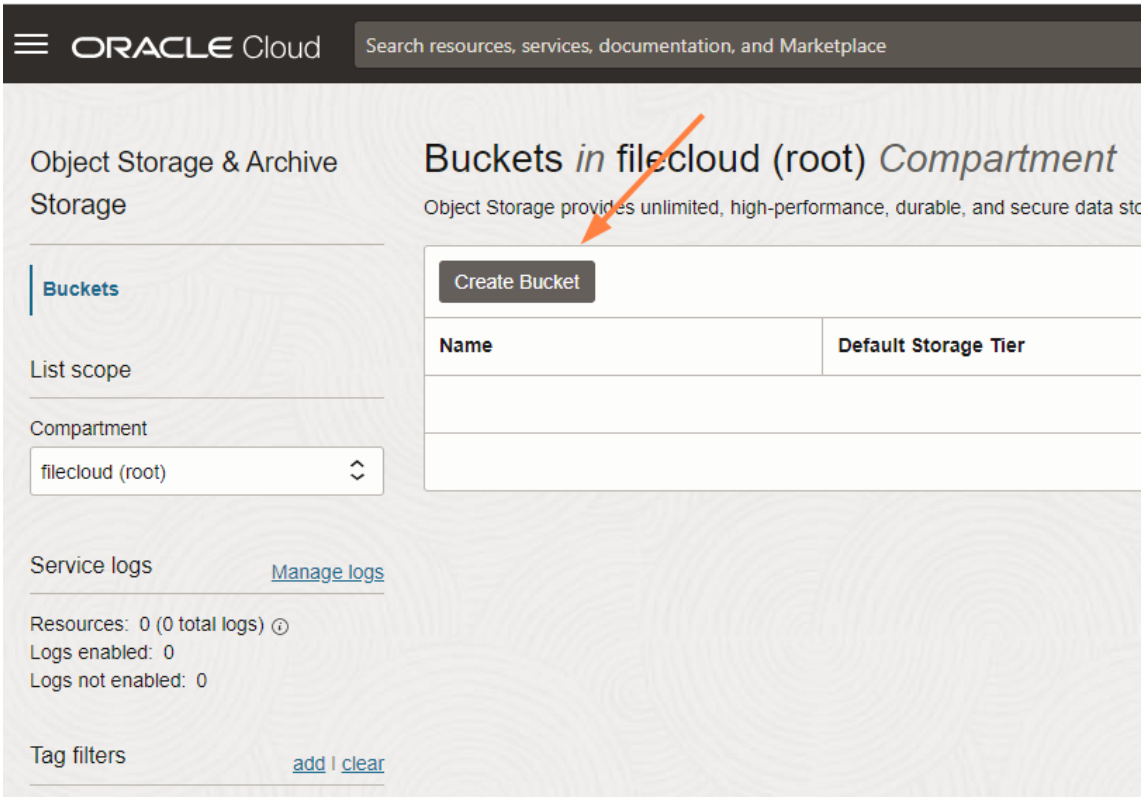
A list of storage-related pages opens.

4. Click **Object Storage & Archive Storage**.



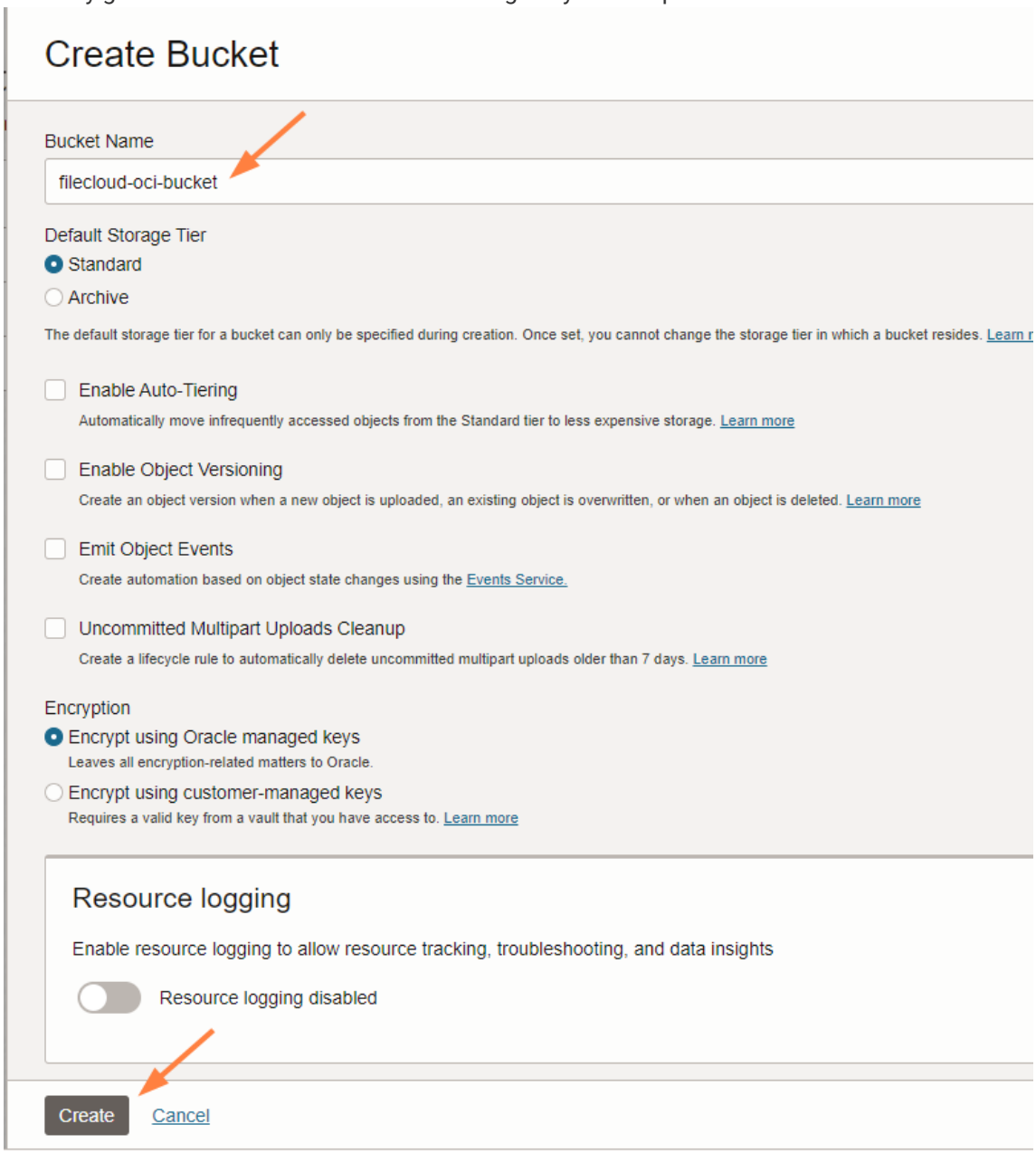
The **Object Storage & Archive Storage** page opens.

5. Click **Create Bucket**.



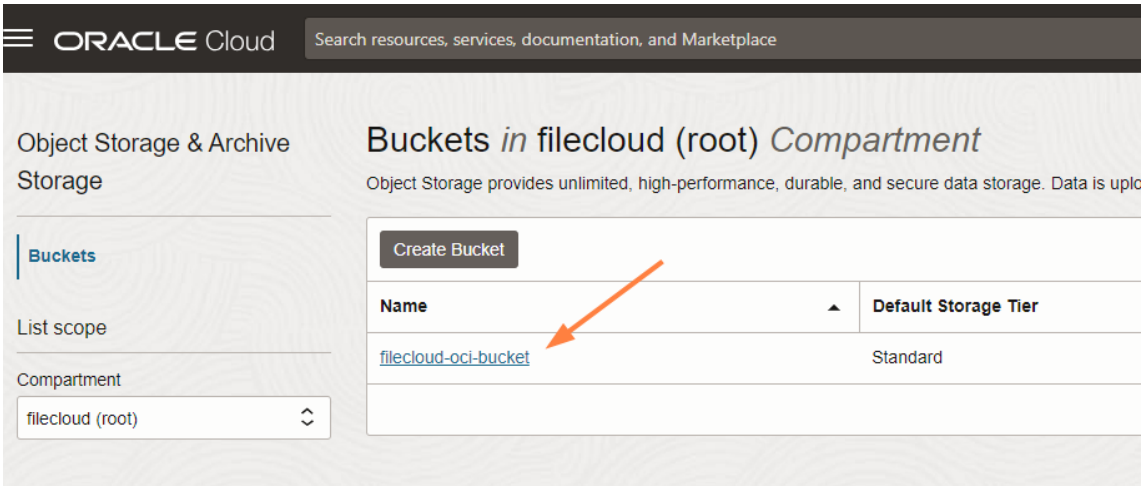
A **Create Bucket** dialog box opens.

6. You may give the bucket a new name and change any of the options. Then click **Create**.



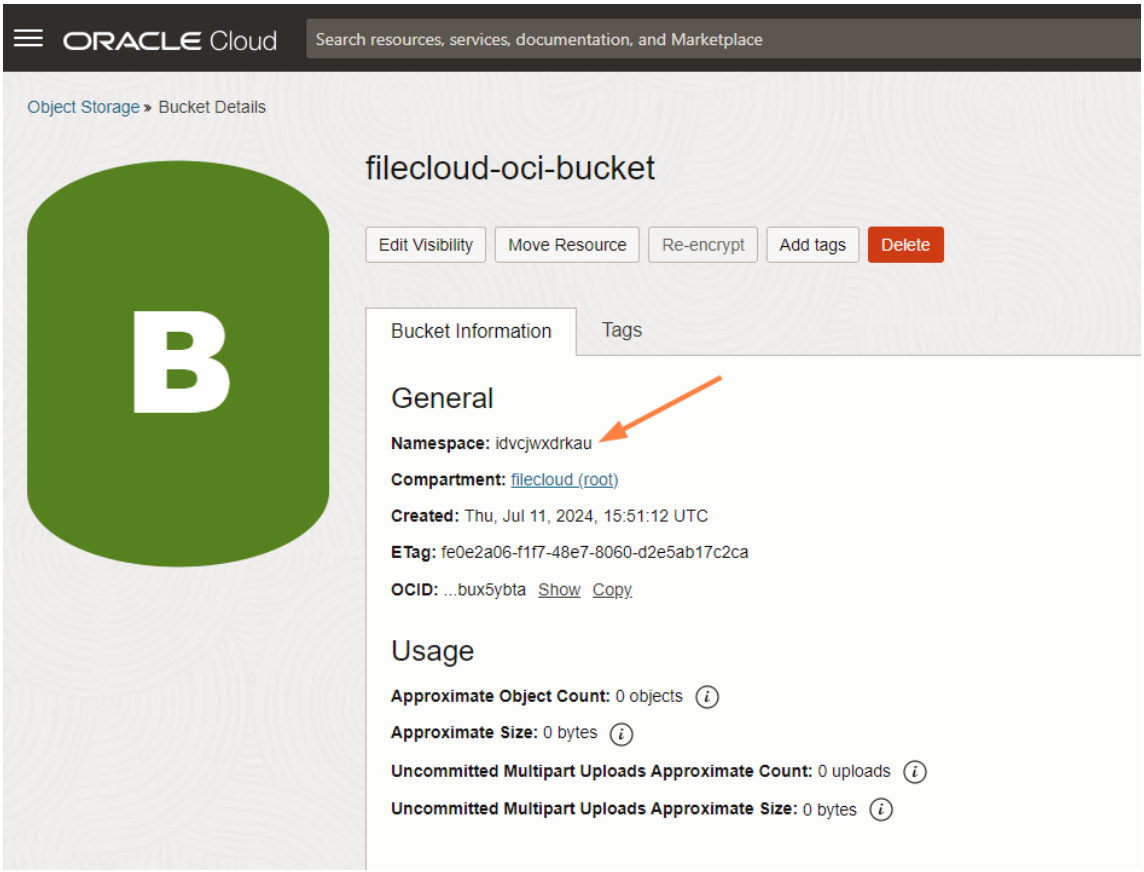
The bucket appears in the list of buckets.

7. Click the bucket name.



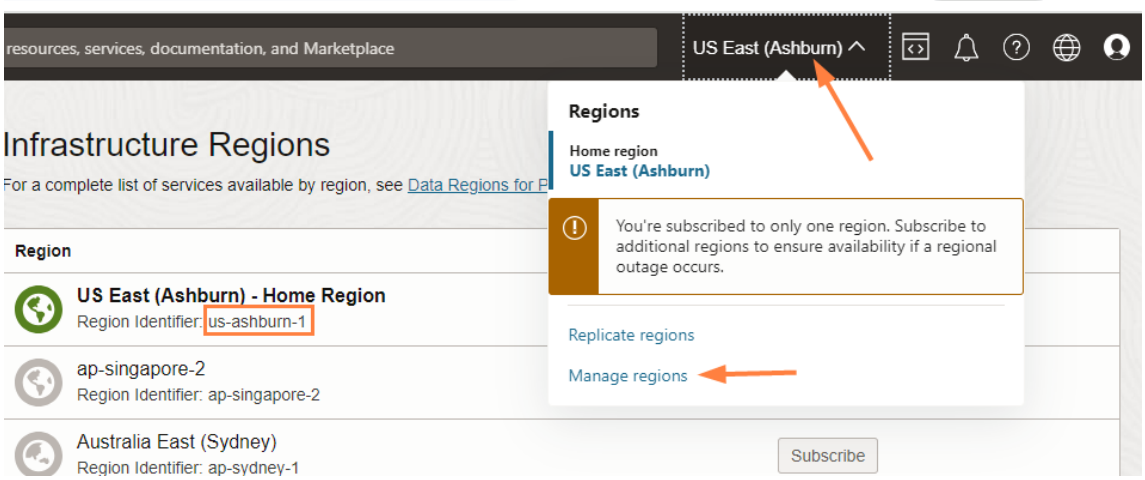
A tab with bucket information opens.

8. Copy and save the value of **Namespace** to use when you enter the S3 end point URL into FileCloud.

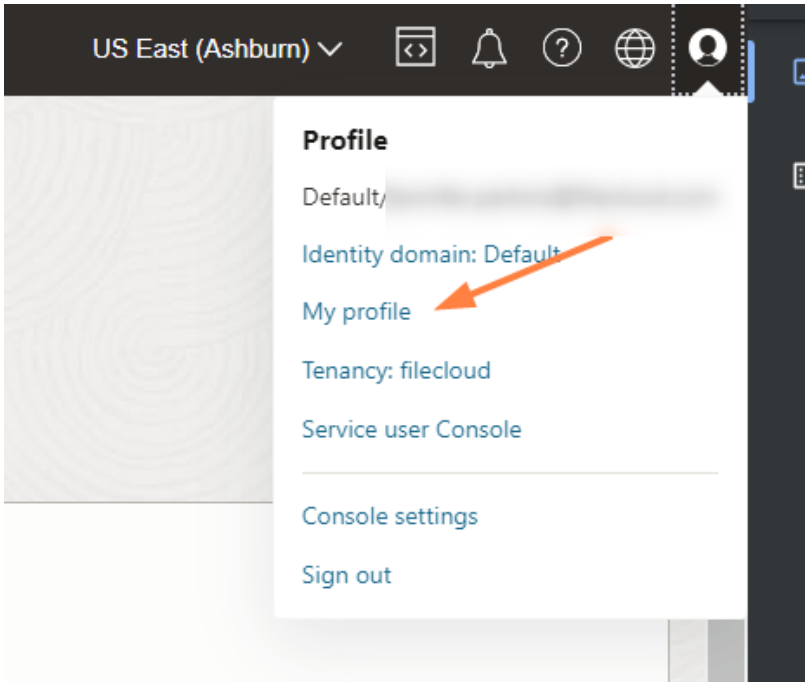


9. Get your region by clicking the name of your region at the top of the OCI screen, and choosing **Manage regions** in the drop-down list.
Copy the **Region Identifier** from the top region shown (the region with the green globe icon) and

save it to enter later in S3 end point URL in FileCloud.

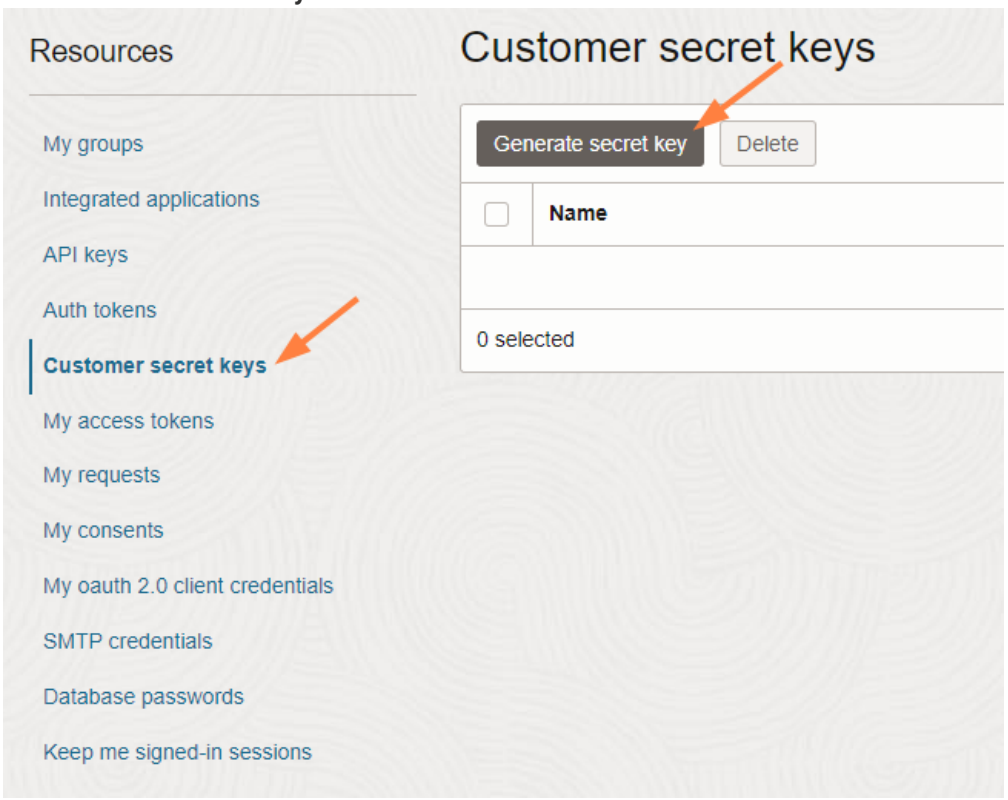


10. In the upper-right of the OCI screen, click the profile icon and choose **My profile**.



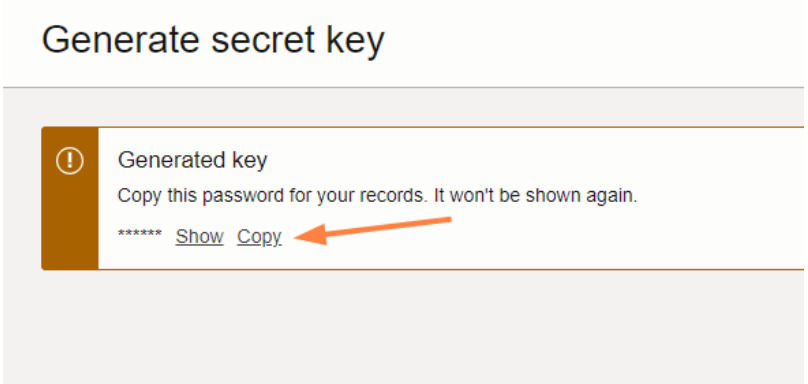
11. In the **My profile** screen navigation panel, scroll down to **Resources**, and click **Customer secret keys**.
    The **Customer secret keys** section opens.

12. Click **Generate secret key**.



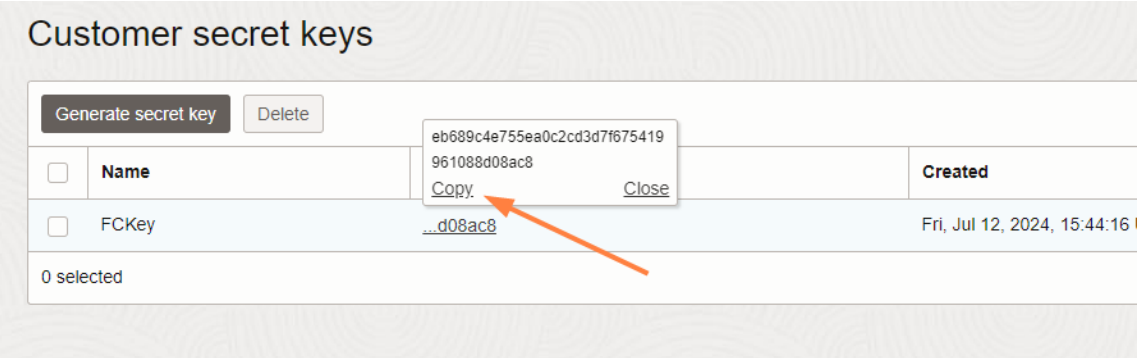
The screen confirms that the secret key was generated and prompts you to copy and save it.

13. Copy and save the secret key. You will use it for the value of **S3 Secret** in the next procedure.



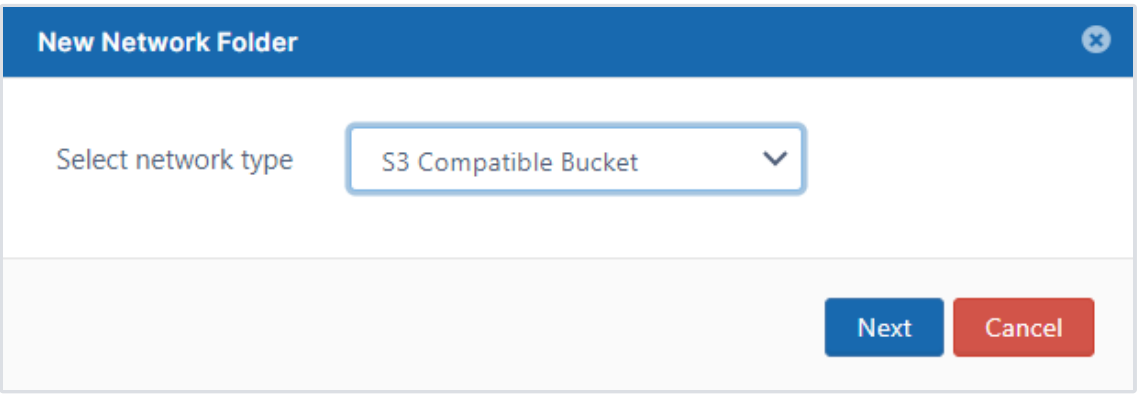
It is now listed in the list of secret keys.

14. Hover over the value in the **Access key** column and copy and save the key. You will use it for the value of **S3 Key** in the next procedure.

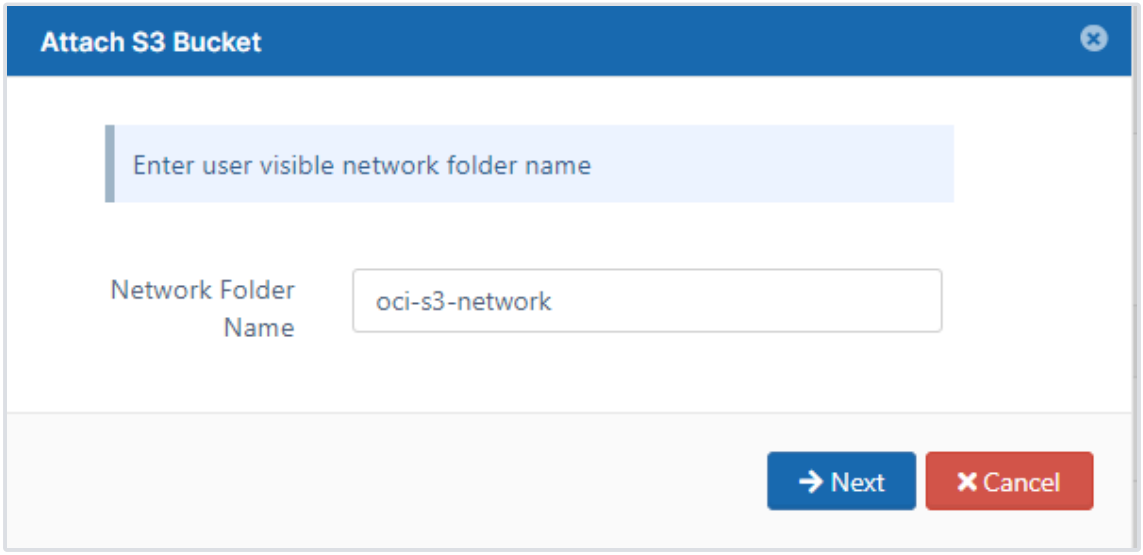


Connect the OCI bucket as a Network Share:

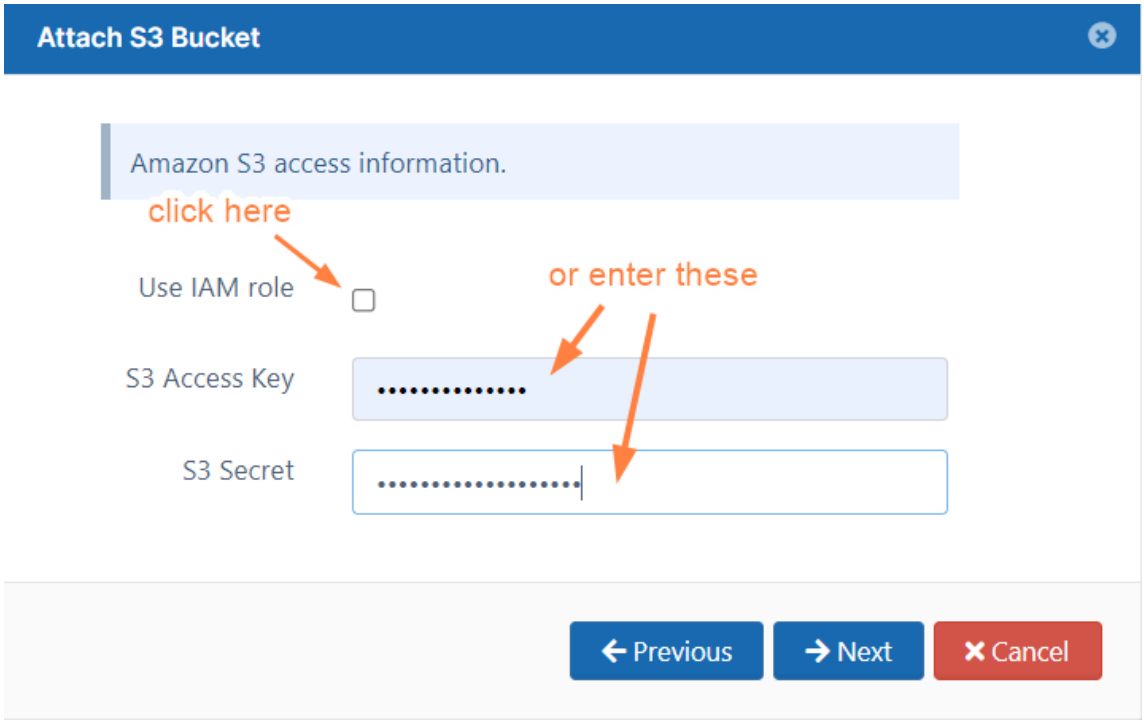
1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



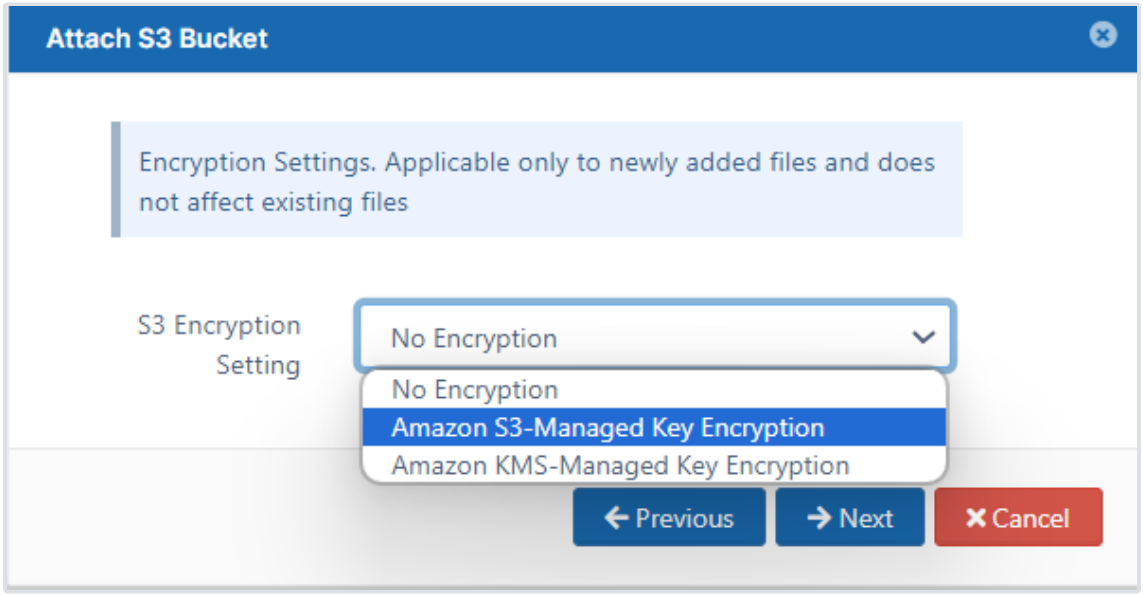
5. On the next window, type in a unique **Network Folder Name** and then click **Next**.



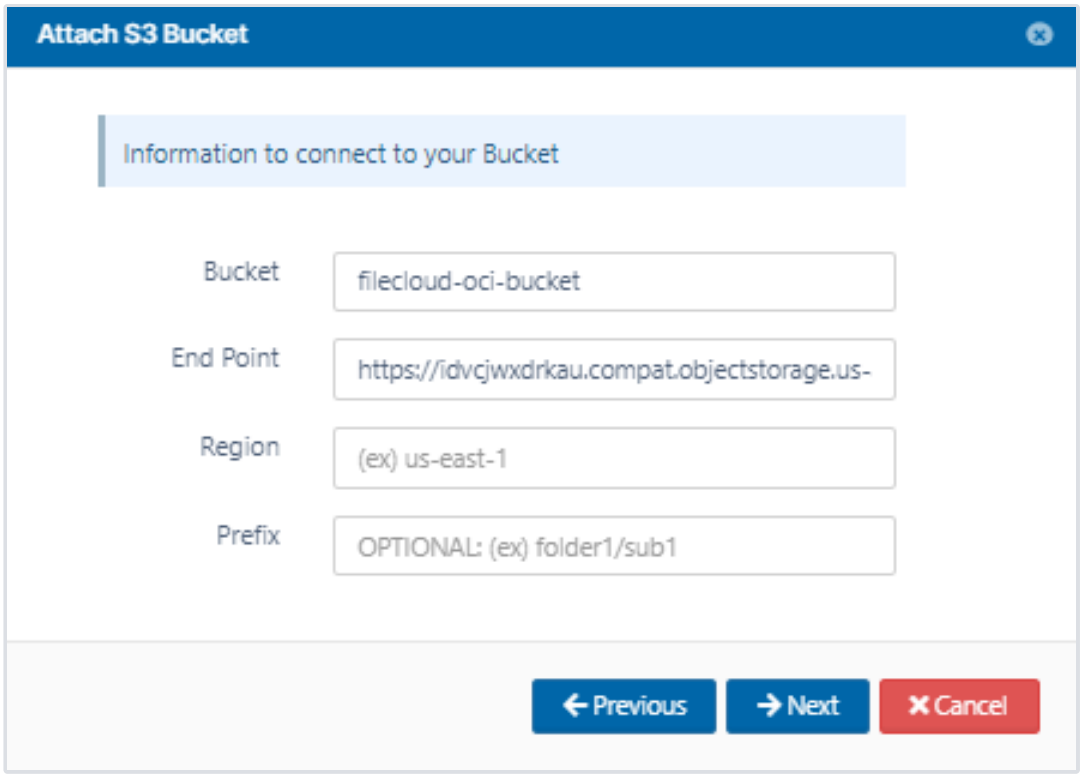
6. In the next window:
   In **S3 Access Key** enter the **Access key** value generated in the OCI user interface.
   In **S3 Secret**, enter the **Secret key** value generated in the OCI user interface.



7. On the next window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:



8. In the next window, fill in the fields as shown. You may leave **Region** and **Prefix** blank.
   - **Bucket** - Enter the name of the bucket you created in Oracle.
   - **End Point** - Use the format: https://[namespace].compat.objectstorage.[region].oraclecloud.com
     where **namespace** and **region** are the values you copied from Oracle as shown in the previous procedure. In the example shown, **End Point** is: https://idvcjwxdrkau.compat.objectstorage.us-ashburn-1.oraclecloud.com



9. Click **Next**.
   The bucket is connected to FileCloud as a Network Share. You may assign users and groups access before finishing.

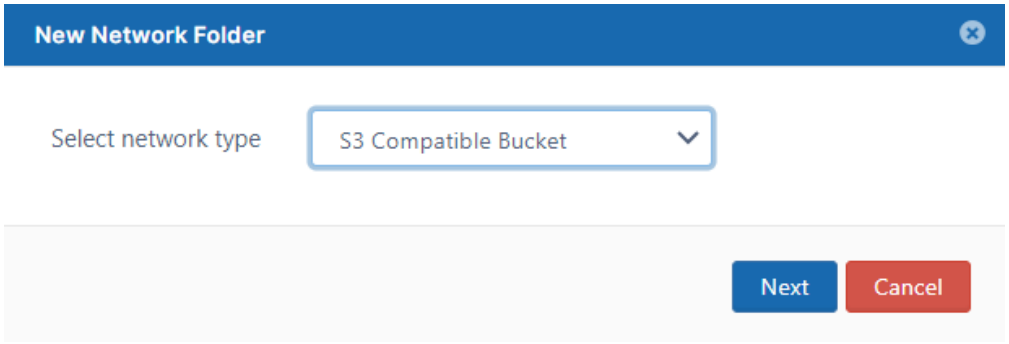
Storj S3 Bucket Based Network Folders

To create the S3 storage bucket and get your S3 key values in Storj

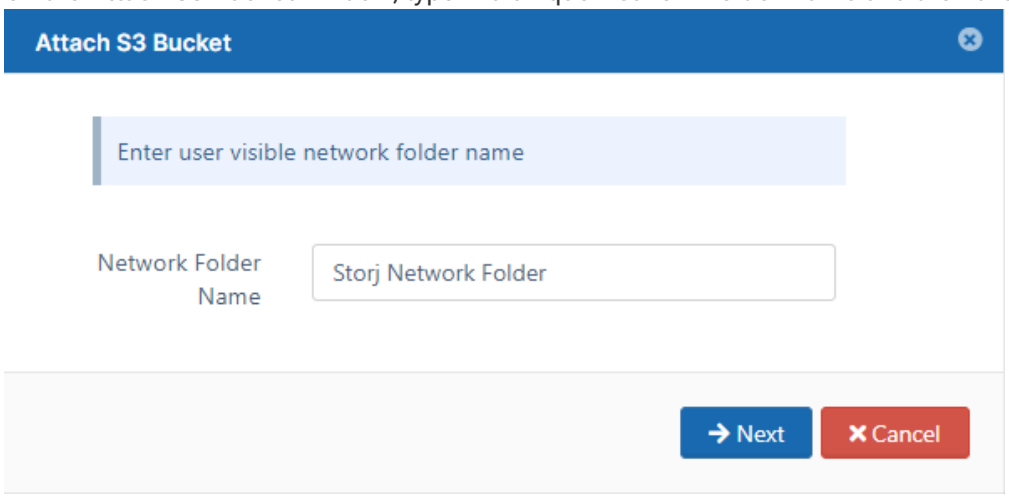
1. Log in to www.storj.io.
2. Create a bucket.
3. Create an access key and a secret key with full access to the bucket.

Connect the Storj bucket to FileCloud as a Network Share:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.

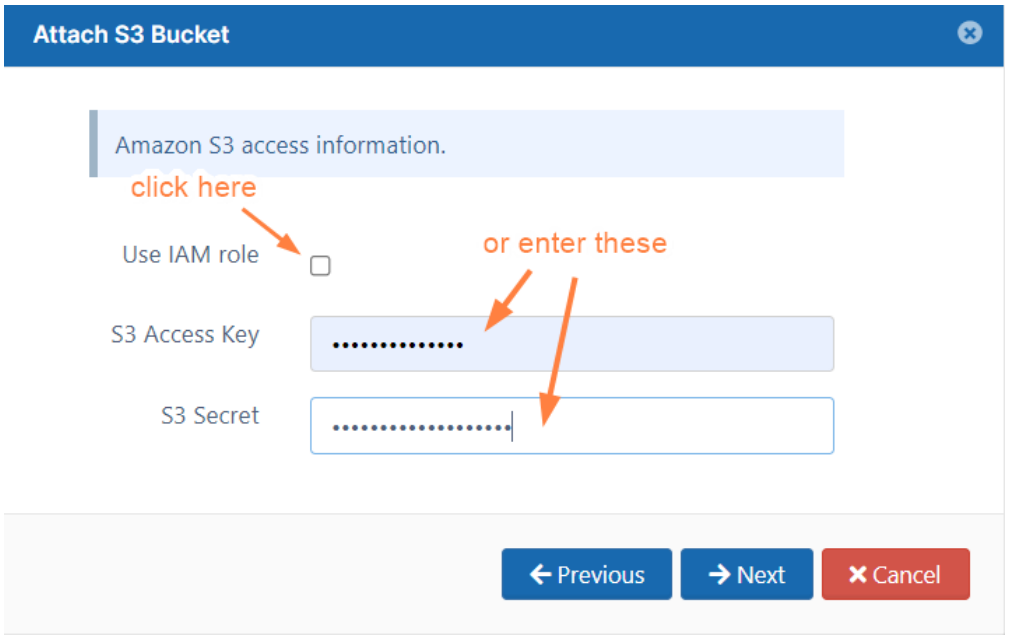


5. On the **Attach S3 Bucket** window, type in a unique **Network Folder Name** and then click **Next**.

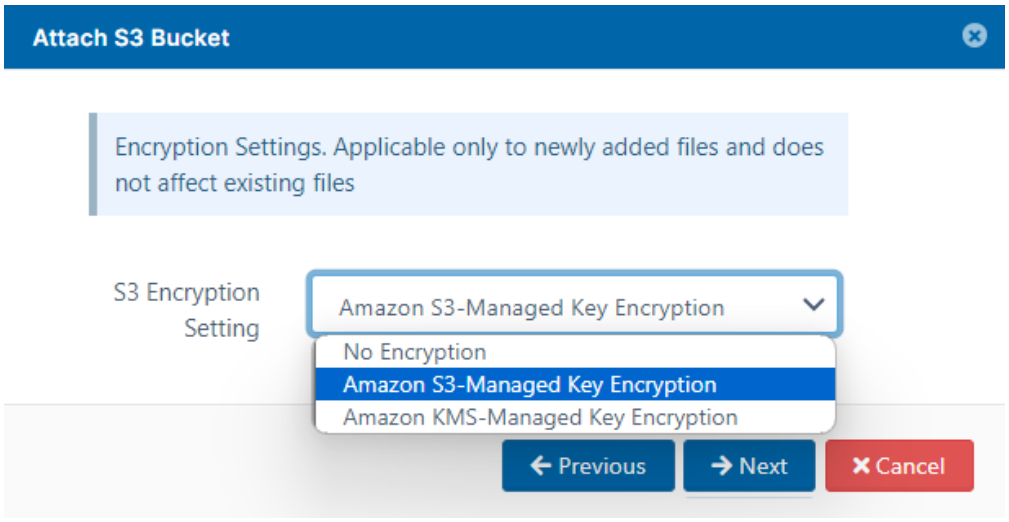


6. In the fields shown:

   Leave **Use IAM role** unchecked. It is not supported in Storj.
   Insert the access key and secret key values you created in Storj into **S3 Access Key** and **S3 Secret**.

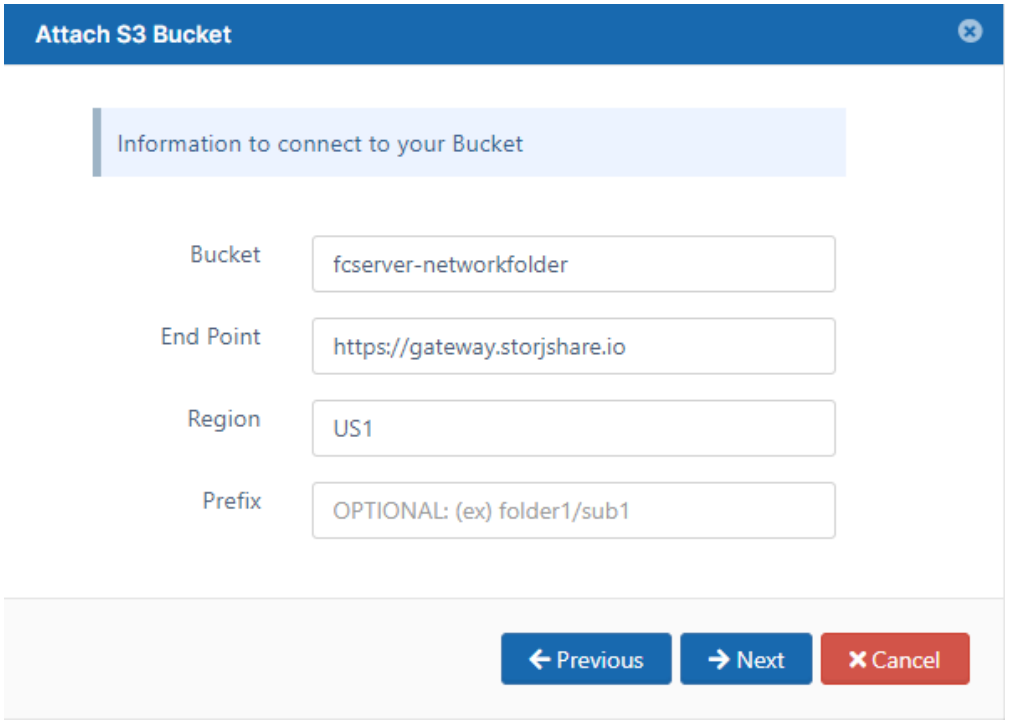


7. On the **Attach S3 Bucket** window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:

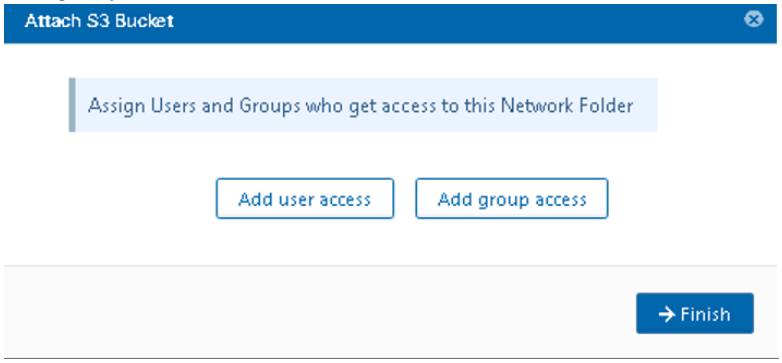


8. Enter the next set of values as follows:

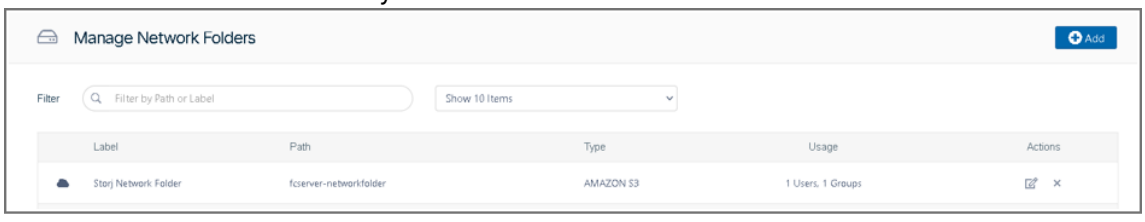
   Bucket: The bucket name (case-sensitive)
   End Point: https://gateway.storjshare.io
   Region: **US1**, **EU1** or **AP1**
   Prefix: Leave blank



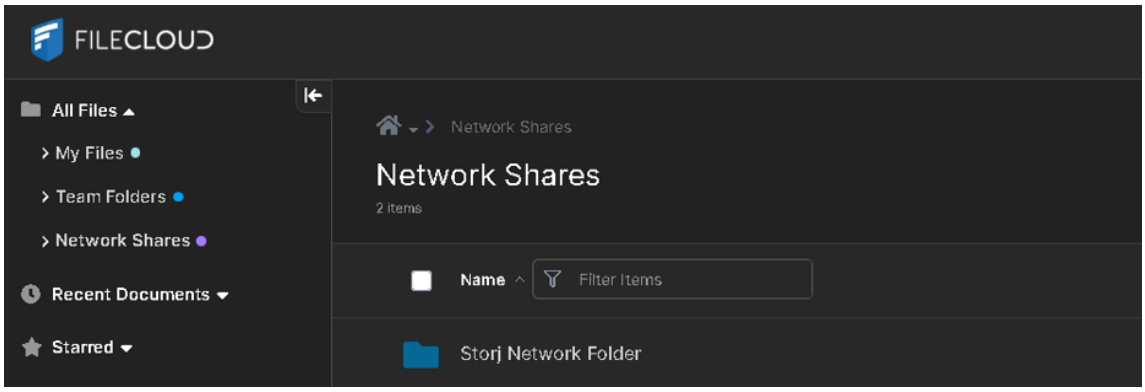
9. Click **Next**.
   The bucket is connected to FileCloud as a Network Share, and you are prompted to give users and groups access.



10. Give users and/or groups access and click **Finish**.
    The Network Folder is added to your list of Network Folders in FileCloud.



The users you have given access see it in their Network Shares folder in the FileCloud user portal:


FILECLOUD
All Files
My Files
Team Folders
Network Shares
Recent Documents
Starred
Network Shares
Network Shares
2 items
Name
Filter Items
Storj Network Folder

Administrator Settings

Resetting Admin Password

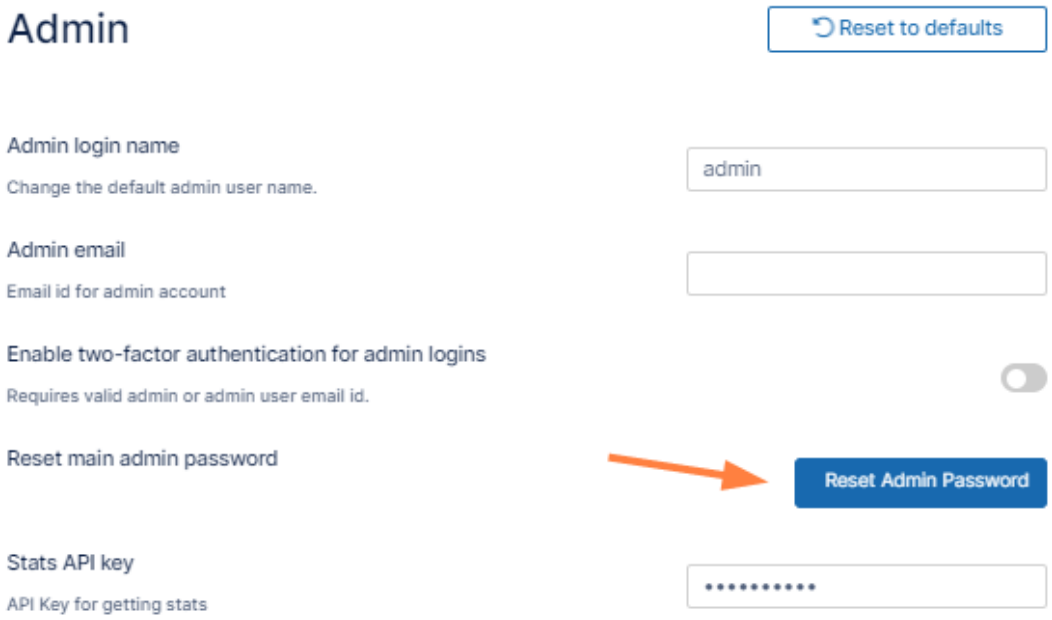
> When Auth Type is set to AD or LDAP, the admin password cannot be changed using the procedure on this page, but must be changed in the AD or LDAP server by the AD or LDAP admin. See User Authentication Settings.

Reset the main admin password in the Admin settings screen

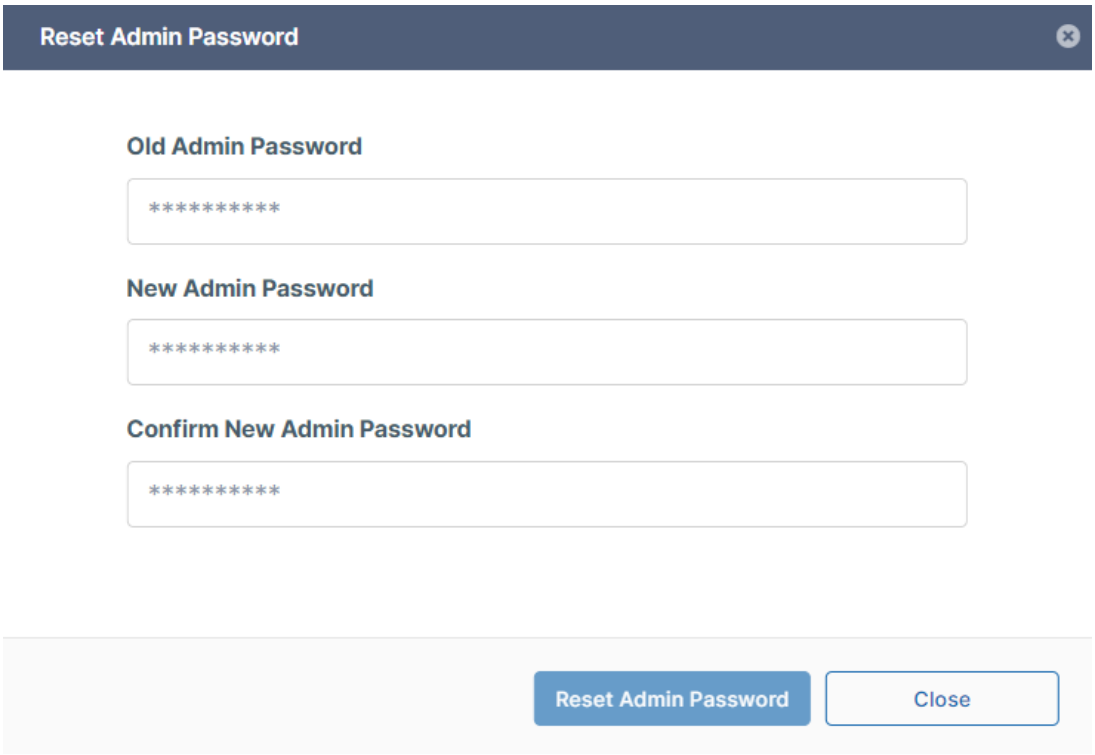
Reset in admin settings...

This setting can only be used to reset the main admin password. It cannot be used to change promoted admin passwords.

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. Click **Reset Admin Password**.



A **Reset Admin Password** dialog box opens.



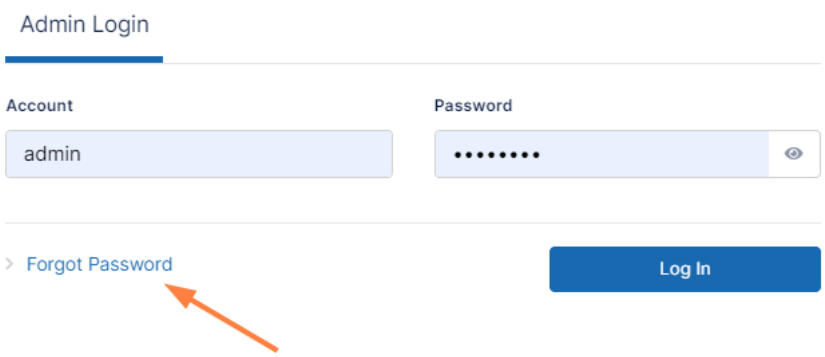
3. Enter the old and new password values, and click **Reset Admin Password**.

Reset a forgotten admin password from the login screen

Reset from login screen...

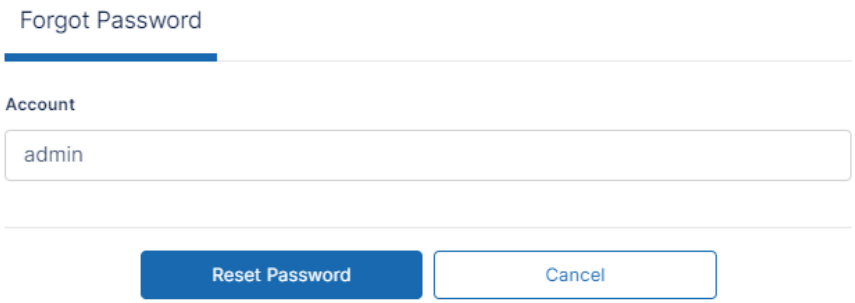
This method can be used to reset the main admin password as well as user admin passwords.

1. On the admin portal login screen click **Forgot Password**.

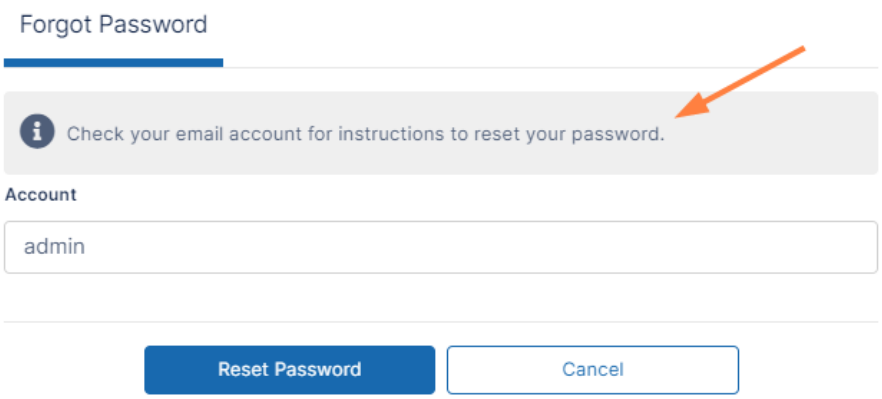


A dialog box prompts you to enter your user account.

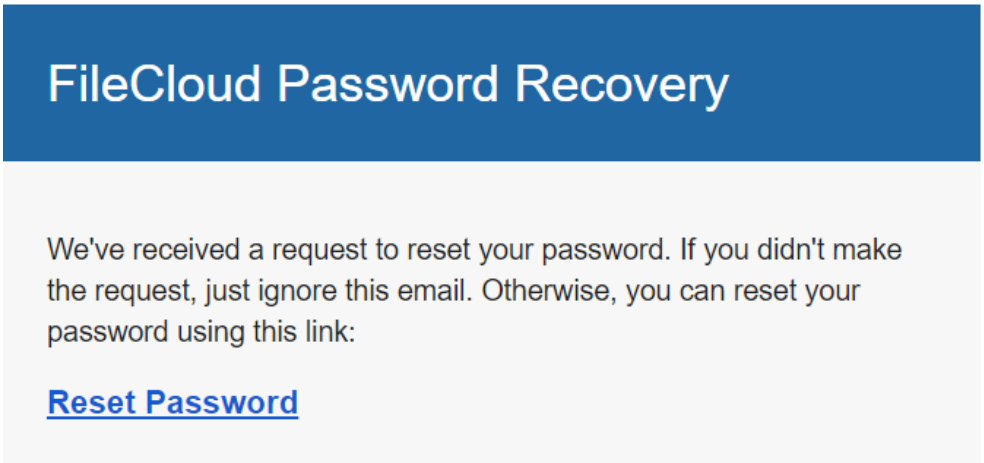
2. Enter your admin account name, and click **Reset Password**.
   Note: To reset their passwords, promoted admin users must use the user portal.



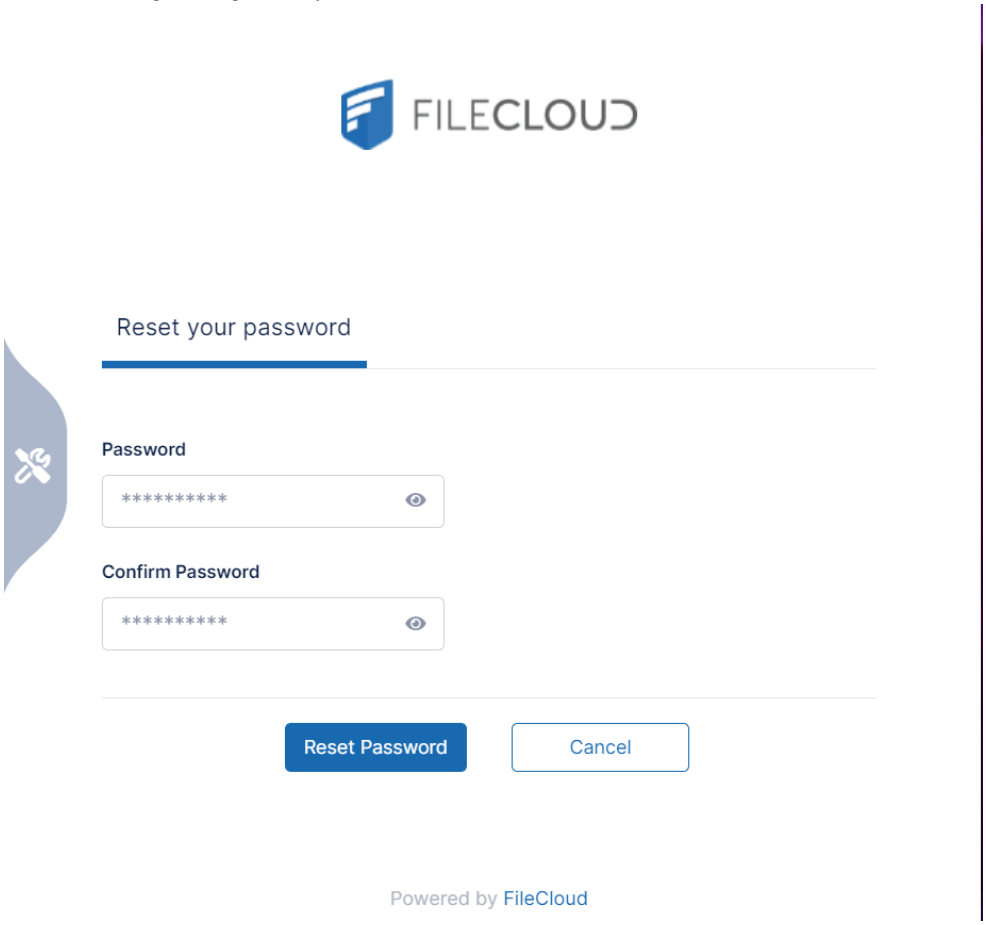
A message appears, telling you to check your email for a message.



3. Find and open the message in your email.
   The message appears as:



4. Click **Reset Password**.
   The following dialog box opens:



5. In **Password**, enter your new password. In **Confirm Password** enter it again.
6. Click **Reset Password**.
   Your password is reset.

Reset the main admin password in the command line interface

The reset password script clears any admin login locks and disables multi-factor authentication, if enabled.

Reset in command line...

This setting can only be used to reset the main admin password. It cannot be used to change promoted admin passwords.

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:
   - To reset the Admin password to **password**, enter:

     ```
     php resetadminpw.php
     ```

   - You can also reset the Admin password to a custom value. To reset the admin password to **he!@#%$%^)*el$AAo**, enter:

     ```
     php resetadminpw.php -p "he!@#%$%^)*el$AAo"
     ```

Displaying the new password in the system log

When the admin password is reset, by default, the new password is not shown in the system logs. However, you may display the new password in the system logs by using the **-d** settings.

To display the new password in the system logs:

1. Follow Step 1, above, to navigate to the correct path for Windows or Linux.
2. Then, for both Windows and Linux, enter:

```
php resetadminpw.php -d
```

Resetting the admin password in multi-site setups

To reset password for another site, pass in the hostname using -h parameter in the command line interface.

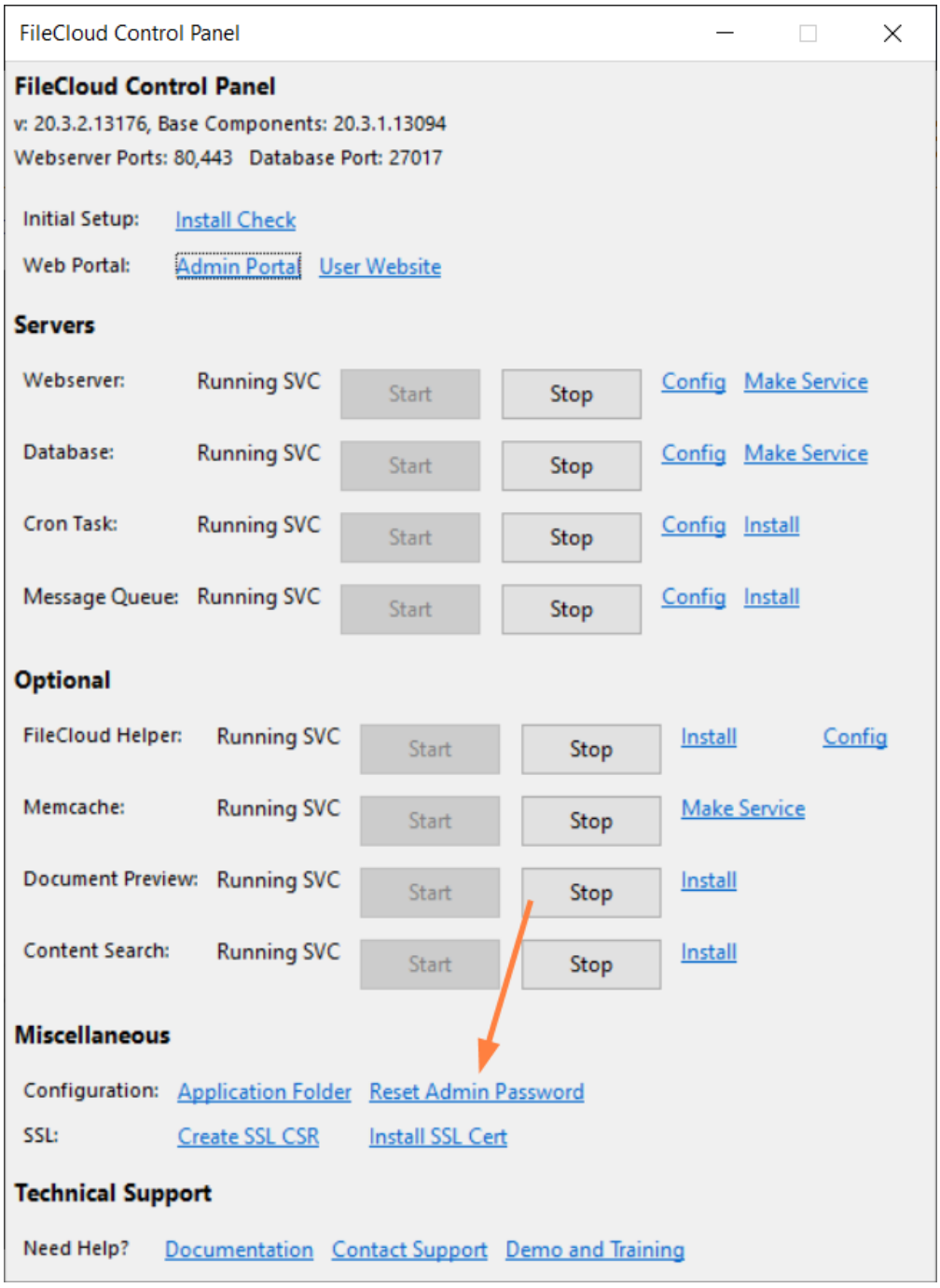
```
php resetadminpw.php -h site2.xyz.com
```

Reset the main admin password using the FileCloud control panel

Reset from control panel...

This method can only be used to reset the main admin password. It cannot be used to change promoted admin passwords.

The main admin password can also be reset to **password** using the FileCloud control panel.

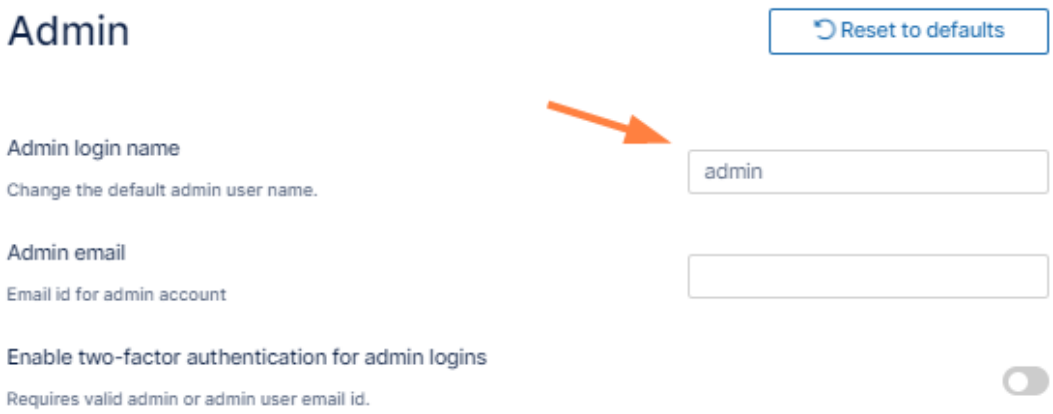


Changing the Default Login Name

FileCloud has a built-in admin account to log in to the admin portal and manage the site.

The name of the account is **admin**. This name can be changed in the **Admin login name** setting.

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. Enter the new name in **Admin login name**.
   The name can only contain letters, numbers, spaces, hyphens, underscores and periods. It cannot be the same as the superadmin name.

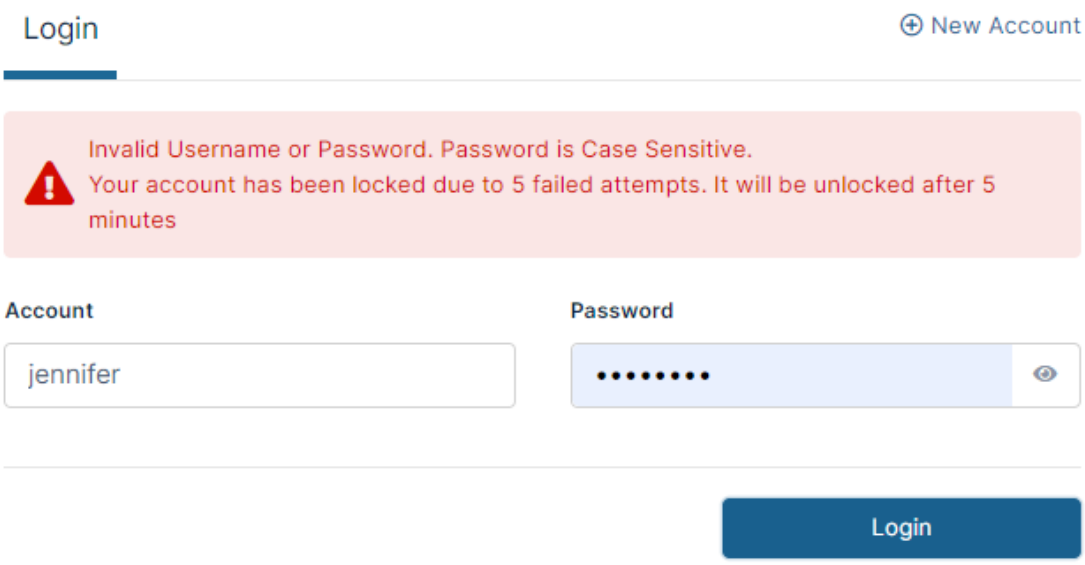


3. Click **Save.**

Account Locked Alerts

By default, FileCloud locks a FileCloud user's account for 5 minutes after 5 incorrect log in attempts. (You may change the default values in Password settings.)

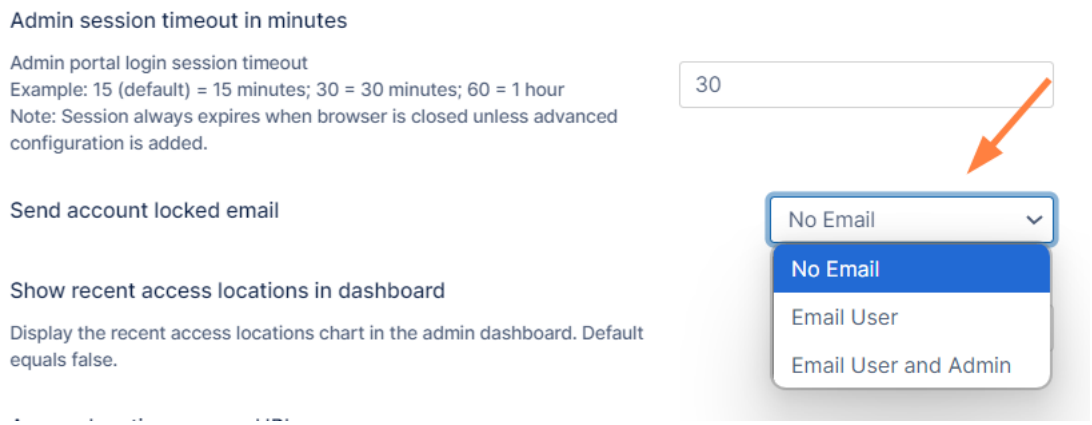
After each failed login attempt, the system displays remaining attempts allowed before account lockout.
If the user's account is locked due to too many failed login attempts, the following notification appears:



By default, FileCloud is set to not send an email message to the user or admin to notify them that the account has been locked due to incorrect login attempts. However, you may change this setting.

To change the **Account Locked Alert** setting:

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 the **Send account locked email** setting.



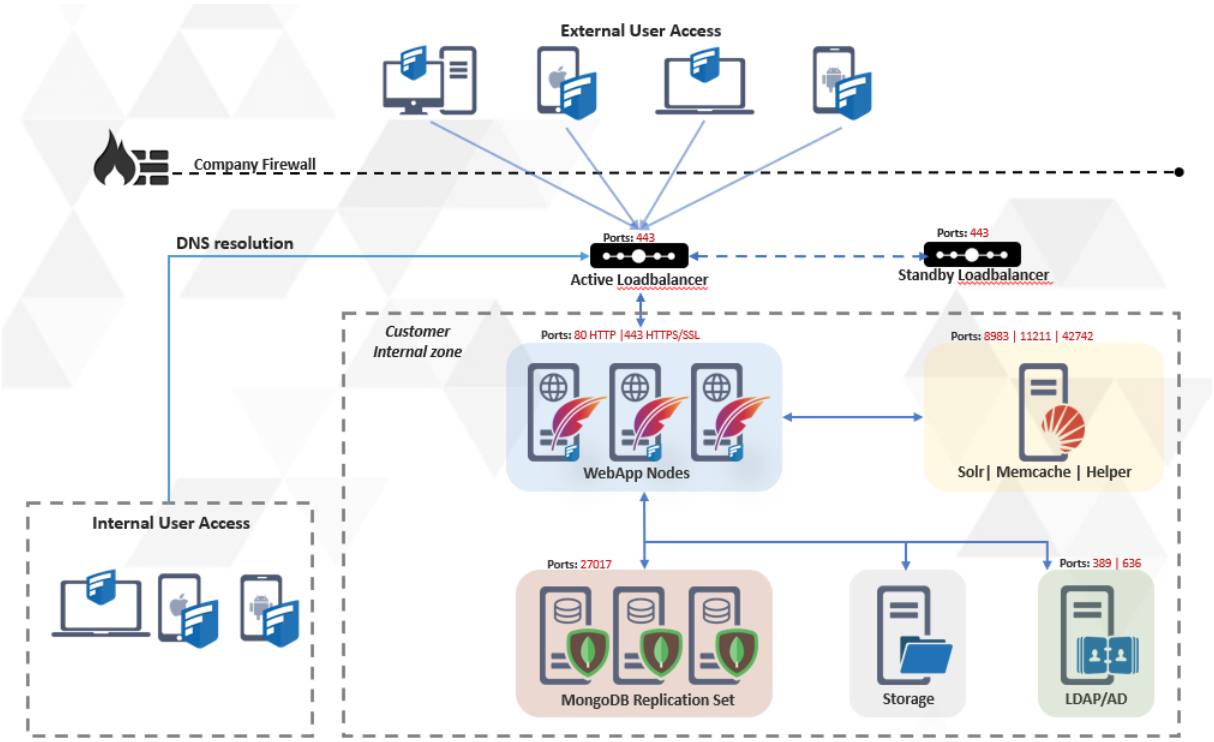
3. In the drop-down list, choose one of the following settings:
   No Email - Neither the user nor the admin receives an email notification about the user account

lockout.
Email User - The user receives an email notification about their account lockout but the admin does not.
Email User and Admin - Both the user and the admin receive an email about the user account lockout.

FileCloud High Availability

FileCloud High Availability Architecture

FileCloud servers can be configured for an HA environment to improve service reliability and reduce downtime in your IT environment. FileCloud supports HA in Linux and Windows environments.



Load Balancers

The Load balancer routes traffic to the FileCloud Application nodes. Load balancers route requests efficiently and provide failover capabilities, ensuring optimal performance and reliability. If one or more App server nodes fail, the load balancer will automatically reroute traffic to other App server nodes.

Typically there is no need to scale the number of load balancers because these servers can handle a very large amount of traffic. However, more than one load balancer can be used to provide additional reliability in the event that a load balancer fails.

In order to protect against load balancer hardware failure, multiple records for the load balancer host name in the DNS service can be used.

The idea here is that different clients will get different ordered lists of IP addresses corresponding to your domain name. This has the effect of distributing requests across the group of IPs in a specific manner. If an IP address does not respond in an appropriate amount of time, the client times out on

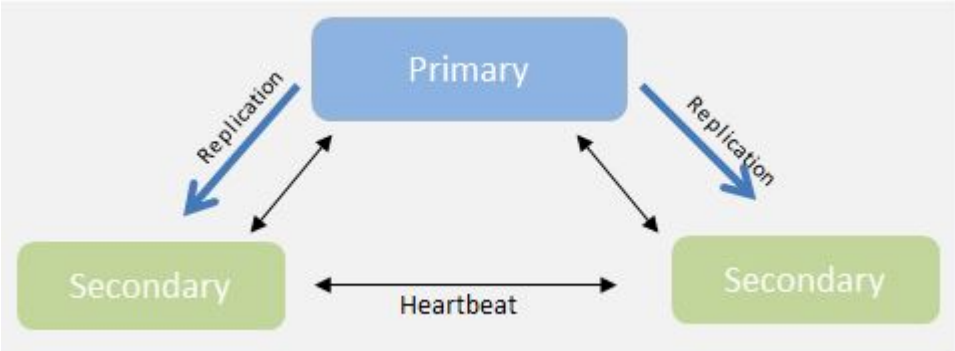
that request and moves on to the next IP address until the list is exhausted or it finds a connection that's valid.

FileCloud Component: App server node

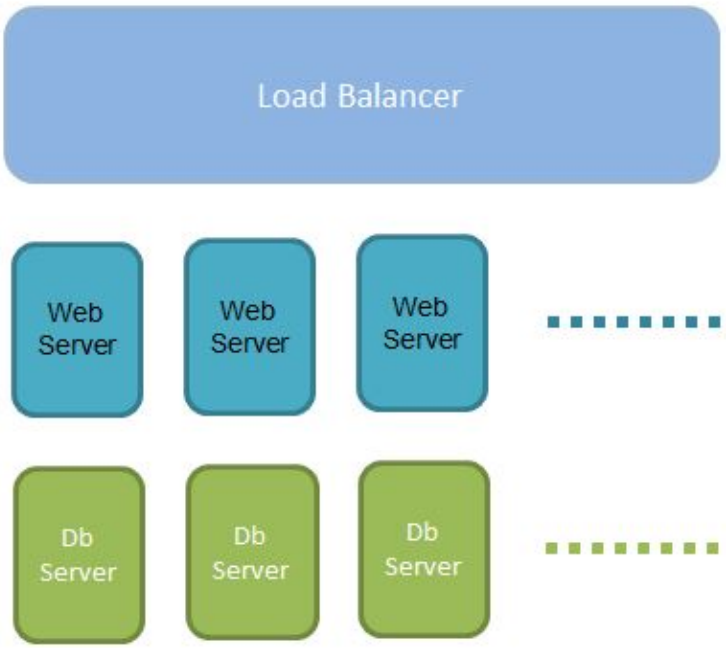
The FileCloud app server node consists of the Apache webserver as well as the FileCloud Application code to serve the client requests. The FileCloud app server nodes do not contain any application-specific data. The data is retrieved from the MondoDB replica sets. Because of this, the FileCloud app server nodes can be added or removed without disrupting the service.

FileCloud Component: MongoDB Replica set

MongoDB database replica sets provide high availability with automatic failover support. Failover allows a secondary member to become primary in the event of failure to the primary database server. The minimum number of database servers needed for MongoDB is three. All app server nodes connect to the primary node, and in the event of primary node failure, a new primary is elected and all the app server nodes will switch to the new primary.



This document describes the classic 3-tier approach with the load balancer handling the client traffic, application server nodes serving requests, and redundant database servers storing application data.



To set up a High Availability FileCloud system, use the instructions on the following pages in order:

Installation and Configuration of 3 server MongoDB cluster

Use the following steps to install and configure MongoDB on three servers.

1. Install MongoDB on three servers.

   Windows:
   Use the FileCloud Installer package to install MongoDB. On the FileCloud control panel, start only the **Database** service. If Web and MongoDB are hosted on the same server, start all services except for **Solr**, **Helper** and **Memcache**.

   Ubuntu:
   Use the following code to install using the MongoDB repository.

   ```
   curl -fsSL https://pgp.mongodb.com/server-8.0.asc | sudo gpg -o /usr/share/
   keyrings/mongodb-server-8.0.gpg --dearmor
   echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-
   server-8.0.gpg ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/8.0
   multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-8.0.list
   ```

   ```
   sudo apt-get update
   ```

```
sudo apt-get install -y mongodb-org
sudo systemctl enable --now mongod
```

RHEL:
Use the following code to install using the MongoDB repository.

```
cat <<EOF > /etc/yum.repos.d/mongodb-org-8.0.repo
[mongodb-org-8.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/8/mongodb-org/8.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-8.0.asc
EOF
```

```
sudo dnf install -y mongodb-org
sudo systemctl enable --now mongod
```

2. Set up the hostname binding and replication.
   It is recommended that you use hostnames for the MongoDB IP bindings in the MongoDB config file, for example:
   db1.filecloudlabs.com
   db2.filecloudlabs.com
   db3.filecloudlabs.com

   Change or add the values of the replica set and bind IP configuration parameters in the MongoDB configuration file as follows:

   Windows:
   In the configuration file: xampp\mongodb\bin\mongodb.conf

   For IP or Host binding, add:

```
bind_ip = db1.filecloudlabs.com
```

   For replication, add:

```
replSet = rs0
```

For example:

```
#ip address
bind_ip = db1.filecloudlabs.com
port = 27017

#replication
replSet = rs0
```

Ubuntu/RHEL:
In the configuration file: /etc/mongod.conf
For IP or Host binding, add:
net:
port: 27017
bindIp: db1.filecloudlabs.com

For replication, add:
replication:
replSetName: rs0

for example:

```
# network interfaces
net:
  port: 27017
  bindIp: db1.filecloudlabs.com

#security:

#operationProfiling:

replication:
 replSetName: rs0
```

After making the above changes, restart the MongoDB service.
On Windows, restart **mongoDB** from Windows Services or **Database** on the FileCloud Control Panel.
On Ubuntu and RHEL, use the command **systemctl restart mongod** or **service mongod restart**

3. Initiate Replica Set configuration
   Before proceeding with this step, verify that all 3 DB servers can connect to port 27017 using the bind IP value.

This applies to only one node. Select a node, db1.filecloudlabs.com, for example, and run the following command. If you run this in more than one DB server, the configuration will become invalid. It's also important to use the bind_ip value used in one of the DB servers to connect to the Mongo Shell.

To connect to the mongo shell on **db1.filecloudlabs.com** run the below command:
On Ubuntu/RHEL:

```
mongosh --host db1.filecloudlabs.com
```

On Windows:

```
xampp\mongodb\bin\mongosh --host db1.filecloudlabs.com
```

Initiate with an explicit configuration document so the exact FQDNs are stored:

```
rs.initiate({
 _id: "rs0",
 members: [
 { _id: 0, host: "db1.filecloudlabs.com:27017" },
 { _id: 1, host: "db2.filecloudlabs.com:27017" },
 { _id: 2, host: "db3.filecloudlabs.com:27017" }
  ]
})
```

4. Check the status of the Cluster

   After the replica set initiation, connect to the replica set using Mongo Shell. Enter the below command from any one of the DB servers:

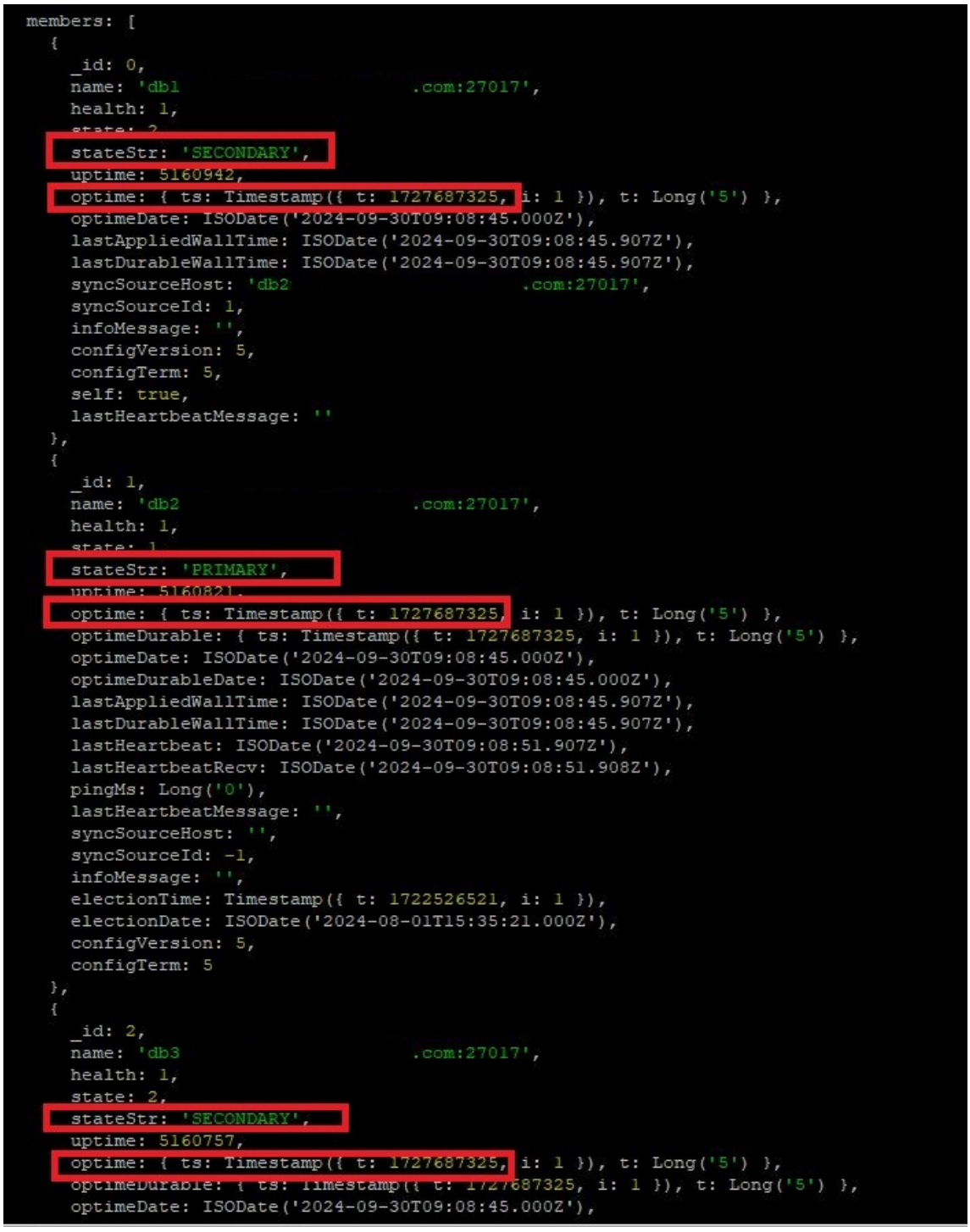
   Ubuntu/RHEL:

```
mongosh --host “rs0/
db1.filecloudlabs.com,db2.filecloudlabs.com,db3.filecloudlabs.com”
```

   Windows:

```
xampp\mongodb\bin\mongosh --host “rs0/
db1.filecloudlabs.com,db2.filecloudlabs.com,db3.filecloudlabs.com”
```

Run rs.status() inside the Mongo Shell to see the replica set status. One of the nodes should show as Primary, and the other two nodes should show as Secondary. The same optime on all the servers indicates that the servers are in sync.



5. Create the MongoDB user to use for DB authentication from FileCloud web nodes.
   On the Primary, before authentication is enabled:

```
use admin
db.createUser({
 user: "fcadmin",
 pwd: 'aSecretPassword',
 roles: [ { role: "root", db: "admin" } ]
})
```

Upon executing the above commands, 'dbuser' is added as a valid database user. (You may use a different username and password.)

6. Enable MongoDB cluster authentication in the MongoDB configuration file
   To enable replica cluster authentication, use either MongoDB Keyfile Authentication or x.509 certificate. The following steps cover MongoDB Keyfile cluster authentication.

   Generate MongoDB Key File:
   In a Linux environment, you can perform this step in a FileCloud web node, and then copy the key to the MongoDB server, or install OpenSSL in the MongoDB server to run the commands.

   To install OpenSSL in MongoDB nodes:
   Ubuntu:

```
apt-get install openssl
```

   RHEL:

```
yum -y install openssl
```

   Perform the following steps to generate a key file on any one of the servers. Once the key file is generated, copy it to the other MongoDB servers.

   Ubuntu/RHEL:

```
sudo -s /bin/bash -c 'openssl rand -base64 741 > /etc/mongodb-keyfile'
sudo -s /bin/bash -c 'chmod 600 /etc/mongodb-keyfile'
```

   Ubuntu:

```
sudo -s /bin/bash -c 'chown mongodb.mongodb /etc/mongodb-keyfile'
```

RHEL:

```
sudo -s /bin/bash -c 'chown mongod.mongod /etc/mongodb-keyfile'
```

Windows:

```
cd C:\xampp\apache\bin
openssl rand -base64 741 >"C:\MongoAuthFiles\mongodb-keyfile"
```

Change the MongoDB configuration file to enable Cluster Authentication.

Linux

a. Open the file /etc/mongod.conf.

b. Add the lines:

```
security:
 authorization: enabled
 keyFile: /etc/mongodb-keyfile
```

Windows

1.

a. Open the file xampp\mongodb\bin\mongodb.conf

b. Add the line:

```
keyFile = C:\MongoAuthFiles\mongodb-keyfile
```

Once the changes are made to the config file, restart the MongoDB services one by one and verify the cluster status.

After authentication is enabled, the connection string for accessing the Mongo Shell is:

Ubuntu/RHEL:

```
mongosh --host “rs0/db1.filecloudlabs.com,db2.filecloudlabs.com,db3.filecloudlabs.com”
--authenticationDatabase admin --username dbuser --password aSecretPassword
```

Windows:

```
xampp\mongodb\bin\mongosh -host “rs0/
db1.filecloudlabs.com,db2.filecloudlabs.com,db3.filecloudlabs.com” --
authenticationDatabase admin --username dbuser --password aSecretPassword
```

To configure x.509 certificate authentication, see Configure Cluster Authentication with SSL.

Note: Following the same process, additional servers can be added to a replica cluster. FileCloud does not recommend setting up a three server DB replica cluster with one primary, one secondary, and one arbiter.

Configure Memcache for HA Environments

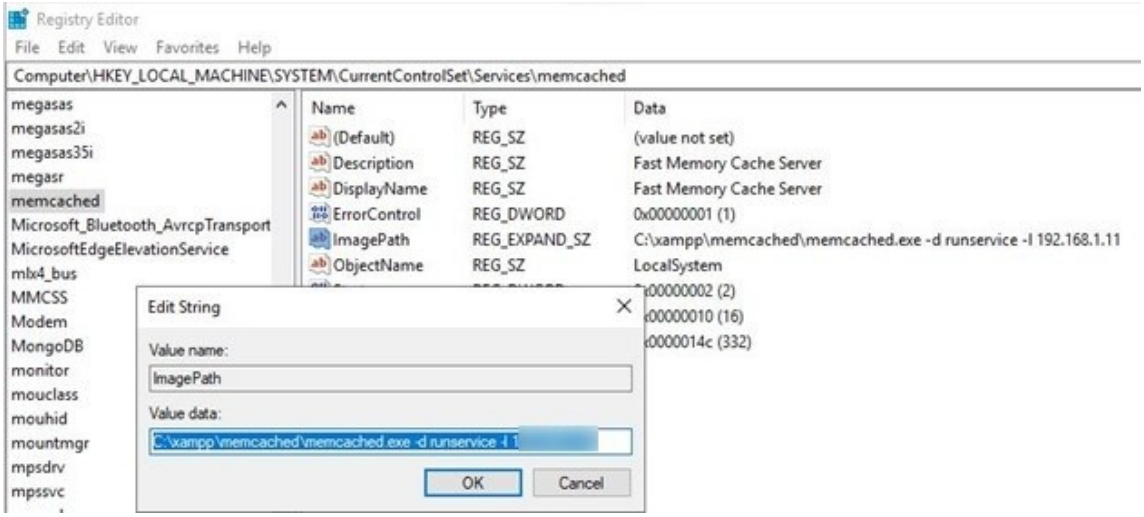
In FileCloud, Memcache is used as a storage cache for NTFS permissions, storage encryption, and SSO session handling.

In HA configurations, bind the Memcache service to the private IP address of the Memcache server so it's accessible to the application servers.

To change the Memcache IP binding:

Windows:

1. Edit the Registry entry **ImagePath** under:
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\memcached
2. To change the localhost binding to the private IP of the servers where Memcache is running, in **Value data**, enter the following, replacing 192.0.2.0 with your server's IP address:
   C:\xampp\memcached\memcached.exe -d runservice -l 192.0.2.0



3. Click **OK**.
4. Restart the Memcache service from FileCloud control panel or Windows Services.

Ubuntu:

1. Edit the file **/etc/memcached.conf**.
2. Locate the line **-l 127.0.0.1** and change it to the private IP of your server.
   For example, if the private server is 192.0.2.0, enter:
   -l 192.0.2.0
3. Once the changes are made, restart the Memcache service by entering:
   service memcached restart
   or
   systemctl restart memcached

RHEL:

1. Edit the file **/etc/sysconfig/memcached**.
2. Locate the line **OPTIONS="-l 127.0.0.1 -U 0"** and change it to the private IP of your server.
   For example, if the private server is 192.0.2.0, enter:
   OPTIONS="-l 192.0.2.0 -U 0"

```
PORT="11211"
USER="memcached"
MAXCONN="1024"
CACHESIZE="64"
#OPTIONS="-l 127.0.0.1,::1"
#OPTIONS="-l 127.0.0.1 -U 0"
#OPTIONS="-l 127.0.0.1 -U 0"
#OPTIONS="-l 127.0.0.1 -U 0"
#OPTIONS="-l 127.0.0.1 -U 0"
OPTIONS="-l 192.168.1.11 -U 0"
```

3. Once the changes are made restart the Memcache service by entering:
   service memcached restart

or
systemctl restart memcached



In HA environments with SSO, either point all FileCloud server nodes to the same memcache server or to the same memcache cluster.
Any of the following will break SSO:

- Pointing each FileCloud server node to the local memcache server, IP 127.0.0.1
- Point each FileCloud server node to a different memcache server.

To configure Memcached in FileCloud, see Install and Configure FileCloud Web Servers for HA.

Configure Solr for HA Environments

Solr, which is used for content search and automatic content classification in FileCloud, can be configured only as a standalone system for HA environments. Solr service can be run on an application server or on a separate server. When deploying FileCloud with multiple web application servers, Solr service should only run on one server whether it's in the same application node or a separate server.

See Install Content Search for Windows to install Solr on Windows Server or Install Content Search for Linux to install Solr on Linux. Solr service should be binded to an IP/hostname that is accessible from the web node in this setup.

1. **Change the Solr IP binding.**

   In Windows:

1.
   a. Open the file **xampp\solr\bin\solr.in.cmd**
   b. Locate the line:
   REM set SOLR_JETTY_HOST=127.0.0.1
   and replace it with the following, using the IP or hostname of the Solr server in place of 192.0.2.1.
   set SOLR_JETTY_HOST=192.0.2.1
   c. Restart the **Content Search** service from FileCloud control panel. (The service is located at xampp\cloudcp.exe).

In RHEL/Ubuntu:

1.
   a. Open the file **/opt/solr/server/etc/jetty-http.xml**
   b. Locate the line:
   <Set name="host"><Property name="solr.jetty.host" default="127.0.0.1"/></Set>
   and replace it with the following, using the IP address of the Solr server in place of 192.0.2.0.
   <Set name="host"><Property name="solr.jetty.host" default="192.0.2.0"/></Set>
   c. Restart the Solr Service by entering:
   service solr restart
   or
   systemctl restart solr
2. **Configure Solr in FileCloud.**
   For help, see Setting up Content Search for Documents.

Install and Configure FileCloud Web Servers for HA

Installing FileCloud web servers for high availability

1. To install the FileCloud web servers, see Direct Installation.
2. After installation, make sure that each web server node has the following services running on it:
   Apache
   Cron
   Message queue
   Web DRM
   Push service
   Memcache (If multiple memcache server are needed for SSO session caching)
   Document preview
3. In Linux environments:
   - Add the MongoDB repository to install MongoDB tools.
   - When you are hosting MongoDB on separate servers, disable the instance of MongoDB running on the web application server, by running:

```
systemctl stop mongodb
systemctl disable mongodb
```

Configuring FileCloud Web Application nodes with MongoDB Cluster and Memcache

Connect a MongoDB Replica Set with an encrypted DB Password

The following steps explain how to connect to a MongoDB replica set with an encrypted MongDB user password so that it does not appear as plain text in cloudconfig.php.

To encrypt the password:

1. Generate a secure key for encryption.
   First run the tool **genkey.php** to create a random password.
   a. In a command line enter:
      In Windows:

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

      In Linux:

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

   b. Then, for both Windows and Linux, enter the genkey.php script to generate the secure key for encrypting the plain text password. Since genkey.php outputs to the screen by default, direct the output to the file securekey.key. Generate the key to a folder outside of the root document directory, such as /home/mongoauth in Linux and C:\MongoAuth in Windows as shown in the following examples.

      Use the following commands:

      For Linux:

```
php genkey.php > /home/mongoauth/securekey.key
```

      Confirm that the **mongoauth** folder is created.

      For Windows:

```
php genkey.php > C:\MongoAuth\securekey.key
```

2. Use the **fcencrypt.php** script with the key generated in the previous step (securekey.key) to encrypt the plain text password ("aSecretPassword" in the example below).
   a. At the command prompt, enter:

```
php fcencrypt.php --message "aSecretPassword" --key "securekey.key"
```

   The encrypted message is returned:

```
Encrypted message:
PgxQKdMU+k5756194hlIcUcp5Qod7oXe2XgaQNO+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/vQ==
```

   b. Copy and save the encrypted message, which you will use as your encrypted password.

Connect Web Server nodes to MongoDB Cluster:

After the MongoDB user password is encrypted, follow the steps below to configure all FileCloud web nodes to connect to the Mongo replica cluster as its database.

1. Open the configuration file and change the following configurations to match the replica set details. Repeat this step for each web node.
   Windows Location: **xampp/htdocs/config/cloudconfig.php**
   Linux Location: **/var/www/html/config/cloudconfig.php**

```
// ... Cloud Database
define("TONIDOCLOUD_DBSERVER", "mongodb://hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3/?replicaSet=rs0&connectTimeoutMS=1000");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3/?replicaSet=rs0&connectTimeoutMS=1000");
// … Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3/?replicaSet=rs0&connectTimeoutMS=1000");
define('TONIDOCLOUD_PUSH_SERVICE_DB_SERVER', 'mongodb://hostname of
Mongo1,hostname of Mongo2,hostname of Mongo3/?
replicaSet=rs0&connectTimeoutMS=1000');
```

2. Add the key file and the encrypted password in cloudconfig.php. Repeat this step for each web node.

```
define('TONIDOCLOUD_ENCRYPTION_KEYFILE', 'c:
\xampp\htdocs\resources\tools\security\securekey.key');
```

```
define('TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD',
'PgxQKdMU+k5756194hlIcUcp5Qod7oXe2XgaQNO+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/vQ==');
```

Set the value of TONIDOCLOUD_ENCRYPTION_KEYFILE to the location of your securekey.key tool (for example, the path /home/mongoauth/securekey.key or C:\MongoAuth\securekey.key) and confirm that Apache users are permitted to access this path. Set the value of TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD to your encrypted password.

3. Add the MongoDB user and encrypted password string using MongoDB URI function. Repeat this step for each web node.

```
function
FC_MONGODB_URI_OPTIONS(){
    return [
            "username" => "dbuser",
            "password" => "%tonidocloud_mongodb_password%"
    ];
}
```

4. Edit the configuration file at:
   Windows location: **xampp/htdocs/config/localstorageconfig.php**
   Linux location: **/var/www/html/config/localstorageconfig.php**

   Add/replace the following keys in the file. Repeat this step for each web node.

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3/?replicaSet=rs0&connectTimeoutMS=1000");
```

5. Add the auto backup mongodump parameter. Repeat this step for each web node.

```
define("AUTOBACKUP_MONGODUMP_PARAMS", '--host "rs0/ hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3" --username dbuser --password
%tonidocloud_mongodb_password% --authenticationDatabase admin');
```

Memcache Configuration:

Beginning in FileCloud 23.242, HA availability for memcache is supported. Encryption remains active as long as at least one server or memcache service, without being restarted since activation, stays up. Storage reactivation is required when the final active server or memcache service is restarted.

1. Configure memcache for NTFS caching and storage encryption. Repeat this step for each web node.
   a. Edit cloudconfig.php:

      Windows Location: **xampp/htdocs/config/cloudconfig.php**
      Linux Location: **/var/www/html/config/cloudconfig.php**

   b. Comment out the lines:

```
//define("TONIDOCLOUD_MEMCACHED_SERVER", "127.0.0.1");
//define("TONIDOCLOUD_MEMCACHED_PORT", 11211);
```

   c. Add the line:

```
define("TONIDOCLOUD_MEMCACHED_SERVERS",
"192.168.1.149:11211;192.168.1.150:11211;192.168.1.195:11211;192.168.1.196:11
211");
```

      IP values in this configuration can be replaced by the IP or hostname of servers running memcache (in the above example, the memcache service is running on 3 Web servers and 1 Solr server).

      Servers can be also grouped for load balancing using “,” and “;”. This is recommended only for NTFS permission caching.

```
define("TONIDOCLOUD_MEMCACHED_SERVERS",
"192.168.1.149:11211,192.168.1.150:11211;192.168.1.195:11211,192.168.1.196:11
211");
```

2. SSO in the FileCloud HA setup requires Memcache to handle the login session. Repeat this step for each web node.
   Edit the configuration file:
   Windows: **xampp/htdocs/thirdparty/simplesaml/config/config.php**
   Linux: **/var/www/html/thirdparty/simplesaml/config/config.php**
   a. Locate the line **'store.type' => 'phpsession'** and change the reference to **‘store.type’ => ‘memcache’**

b. Multiple Memcache servers are recommended to handle SSO sessions in HA setup. To configure this the Memcache server hostname or IP must be specified in FileCloud configuration file.

   Edit the configuration file:
   Windows Location: **xampp/htdocs/config/cloudconfig.php**
   Linux Location: **/var/www/html/config/cloudconfig.php**

   Set the Memache hostnames to each Memcache server IP or hostname.

```
function SSO_MEMCACHED_SERVERS() {
return [
    [
        ['hostname' => ' memcachehostname/ip1']
    ],
    [
        ['hostname' => ' memcachehostname/ip2']
    ],
];
}
```

For more details, see SAML Single Sign-On Support.

> In HA environments with SSO, either point all FileCloud server nodes to the same memcache server or to the same memcache cluster.
> Any of the following will break SSO:
> - Pointing each FileCloud server node to the local memcache server, IP 127.0.0.1
> - Point each FileCloud server node to a different memcache server.

FC Push Service Configuration:

Note: Push service configuration currently doesn't support using an encrypted MongoDB password.

Push service is essential to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload and share notifications).

To configure Push service:

RHEL/Ubuntu:

1. Open and edit the .env file:
   Linux: **/opt/fcpushservice/.env**
   Windows: **xampp\pushservice\.env**
2. Update the MongoDB connection string:

```
FCPS_DB_DSN=mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
```

3. Restart the **fcpushservice**.

   In **Linux**, enter:

   ```
   systemctl restart fcpushservice
   ```

   In **Windows**, restart the Push service from the FileCloud Control Panel.

FileCloud Helper Configuration

Note: FileCloud Helper configuration currently doesn't support using an encrypted password.

FileCloud Helper service can be deployed only in a Windows Server environment, and is used for network share solr indexing and realtime syncing of network shares.

1. To configure the IP binding for FileCloud Helper, edit the file **C:\xampp\FileCloudHelper\config.ini** and change the address binding to the IP of the FileCloud Helper server.

   ```
   ; Settings for FileCloud NTFS Helper
   [settings]
   address=helper.filecloudlabs.com
   ```

2. To configure FileCloud Helper to connect to the MongoDB replica set edit the file **C:\xampp\FileCloudHelper\realtime.ini** and change the db connection string to match the replica set value.

   ```
   settingsdb= mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
   clouddb= mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
   syncdb= mongodb://dbusToer:passw0rd1@dbserver01,dbserver02,dbserver03:27017
   ```

To enable the Helper service, see Indexing of Network Folders.

The Helper service should be running with a logon account. For help, see Install Helper Service.

Additional Configurations and considerations:

For S3 storage:

1. If you are using Amazon S3 for backend storage, then edit the **amazons3storageconfig.php** file.
   Linux location: **/var/www/html/config/amazons3storageconfig.php**
   Windows location: **c:\xampp\htdocs\config\amazons3storageconfig.php**

If the file is not found, copy **amazons3storageconfig-sample.php** and rename it **amazons3storageconfig.php** on each of the nodes.

A temp space must be mounted to the same mount point on each of the nodes (For example /mount/fctemp in linux or F:\fctemp or //hostname/tempfolder in windows).

2. Add/replace the following key:

```
define("TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER", "/mount/fctemp");
```

Document Preview

If you have enabled Document Converter service, it must be started in each node.

The local webserver will use the local service to handle document preview.

See Document Preview for help setting up Document Converter on the web nodes.

Apache Logon Account

For Windows systems connected to a domain, it is recommended that you run the below services using a logon account.

Apache Service or Web Server
Message Queue or fcorchestrator
FileCloud Cron Service
FileCloud Docconverter
FileCloud Helper (Only on one server)
FileCloud Solr(Only on one server)

Configure Storage for HA

The storage setup covered here is intended to help you set up your HA environment, but is outside the scope of FileCloud Support.

We use SAMBA Share on RHEL in our example, but you may use the file sharing software that best serves your needs.

In a Windows environment, the Apache service must run under a user account with full read/write permissions to the storage path; to modify the Apache service log-on permissions to run as a user account with full privileges to the storage path, do the following.

The storage path created to store FileCloud data should be accessible across all the web nodes in the setup and readable/writable for Apache.

1. To install Samba in RHEL, run:

```
yum update -y
yum install samba -y
```

2. Then, enable and check Samba status:

```
systemctl enable --now smb
systemctl status smb
```

3. Create a directory for Samba to share and add a dedicated user account:
   The command below:
   - creates the folder **/data/filecloud**
   - adds a new user account named **filecloud** with no login shell
   - sets proper Samba permissions so the user can access the share.

```
mkdir -p /data/filecloud
adduser --home /data/filecloud --no-create-home --shell /usr/sbin/nologin --group
sambashare filecloud
chmod 2770 /data/filecloud
chown filecloud:sambashare /data/filecloud
```

4. Samba keeps its own database of users and passwords, which it uses to authenticate logins. In order to log in, all users must be added to the Samba server and enabled.
   Execute the following `smbpasswd` commands:

```
smbpasswd -a filecloud    # Add the user to Samba's password database
smbpasswd -e filecloud    # Enable the user for Samba access
```

5. The configuration file for Samba is located at `/etc/samba/smb.conf`. To add the new directory as a share, edit the file by running:

```
vi /etc/samba/smb.conf
```

   Below is the samba conf sample used in this setup:

```
[global]
 server string = samba_server
 server role = standalone server
 interfaces = 192.0.2.0
 bind interfaces only = yes
 disable netbios = yes
```

```
 smb ports = 445
 log file = /var/log/samba/smb.log
 max log size = 10000

[filecloud]
 path = /data/filecloud
 browseable = yes
 read only = no
 force create mode = 0660
 force directory mode = 2770
 valid users = filecloud
```

To mount the Samba share in your FileCloud web server nodes, see How to properly mount a CIFS share on RHEL for FileCloud.

Set up the managed storage path in FileCloud

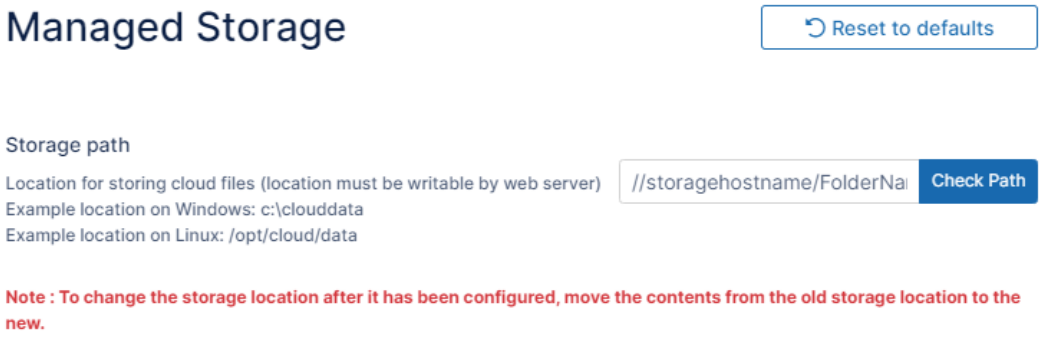
Since the FileCloud app server nodes do not store any of the application data, managed storage must reside in an external location (NAS, ISCSI, SAN, Amazon S3, or OpenStack)

In this example, the storage path is **/data/filecloud** which is already available and mounted on each of the Linux webserver nodes.

1. Open the FileCloud admin portal using one of these URL formats, and then log in:
   - **http://<load balancer IP>/ui/admin/index.html**
   - **http://<Private IP of Web Server>/ui/admin/index.html**
2. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   The **Managed Storage settings** page opens by default.
3. Enter the mounted path in **Storage Path**, and click **Save**.



In Windows, the path must be a UNC path that is accessible from all web nodes. Here the example path is **//storagehostname/FolderName**.



To enable encryption for FileCloud managed storage, see Enabling Storage Encryption.

If you are using S3 object storage see Setting up FileCloud Managed S3 Storage.

If you are using Azure blob storage, see Setting up FileCloud Managed Azure Blob Storage.

Set Up Load Balancing

The core component of an HA setup is its load balancer.

The load balancer installation and configuration processes covered here are intended to help you set up your HA environment, but they are outside the scope of FileCloud Support.

We use HAProxy in an Ubuntu 22.04 environment in our example, but you may adapt our instructions to the load balancing software and environment that best serves your needs. This example uses HTTP but can be expanded to use HTTPS as well.

Load Balancer

The load balancer is the component that distributes incoming requests among a group of servers. In this example, the load balancer is HAProxy (http://www.haproxy.org/). HAProxy is a high performance load balancer that allows you to scale your FileCloud deployment quickly.

NOTE: Before starting the installation, ensure the servers are already available and their IP addresses are known.

Setting up HAProxy

1. Use the apt-get command to install HAProxy.

```
apt-get install haproxy
```

2. Enable HAProxy to be started by the init script.

```
vi /etc/default/haproxy
```

Set the ENABLED option to 1.

```
ENABLED=1
```

3. Move the default config file to create a new default configuration file.

```
mv /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.save
vi /etc/haproxy/haproxy.cfg
```

4. Add the following in the empty haproxy.cfg file.

   The log directive mentions a syslog server to which log messages are sent. On Ubuntu, rsyslog is already installed and running but it doesn't listen on an IP address. We'll modify the config files of rsyslog later.

   The maxconn directive specifies the number of concurrent connections on the frontend. The default value is 2000 and should be tuned according to your VPS' configuration.

   The user and group directives change the HAProxy process to the specified user/group. These shouldn't be changed.

```
global
    log 127.0.0.1 local0 notice
    maxconn 2000
    user haproxy
    group haproxy
```

Defaults

This section demonstrates how to specify default values. The values to be modified are the various timeout directives. The connect option specifies the maximum time to wait for a connection attempt to a VPS to succeed.

The client and server timeouts apply when the client or server is expected to acknowledge or send data during the TCP process. HAProxy recommends setting the client and server timeouts to the same value.

The retries directive sets the number of retries to perform on a VPS after a connection failure.

The option redispatch enables session redistribution in case of connection failures. So session stickiness is overridden if a VPS goes down.

```
defaults
    log global              # Use log settings from global section
    mode http               # Operate in HTTP mode
    option httplog          # Log HTTP-specific information
    option dontlognull      # Don't log empty connections
    retries 3               # Retry 3 times on connection failure
    option redispatch       # Redistribute traffic if backend fails
    timeout connect 5000    # Max 5s to connect to backend
    timeout client 10000    # Max 10s for client inactivity
    timeout server 10000    # Max 10s for server inactivity
```

Host Configuration

This contains the configuration for both the frontend and backend and shows how to configure HAProxy to listen on port 80 for filecloud (which is just a name for identifying the application).

The stats directives enable the connection statistics page and protect it with HTTP Basic authentication using the credentials specified by the stats auth directive.

This page can be viewed with the URL mentioned in stats uri, so in this case, it is http://<loadbalancerip>/haproxy?stats;

The balance directive specifies the load balancing algorithm to use. Options available are Round Robin (roundrobin), Static Round Robin (static-rr), Least Connections (leastconn), Source (source), URI (uri) and URL parameter (url_param).

For information about each algorithm, see https://www.haproxy.com/documentation/haproxy-configuration-manual/latest/#balance .

The server directive declares a backend server with the syntax:

server <name> <address>[:port] [param*]

The names used for the three webservers in these instructions are Ha-WS1, Ha-WS2, Ha-WS3.

In the directive server Ha-WS1 xx.xx.xx.xx:80, replace xx.xx.xx.xx with the actual IP address of the app server nodes.

```
listen filecloud
    bind 0.0.0.0:80
    mode http
    stats enable
    stats uri /haproxy?stats
    stats realm Strictly\ Private
    stats auth  proxyuser:proxypassword
    balance roundrobin
    option http-server-close
    timeout http-keep-alive 3000
```

```
    option forwardfor
    server Ha-WS1 xx.xx.xx.xx:80 check
    server Ha-WS2 xx.xx.xx.xx:80 check
    server Ha-WS3 xx.xx.xx.xx:80 check
```

Starting HAProxy

From a command line, start HAProxy, using the following command:

```
service haproxy start
```

Installation and Configuration of Standalone Backup Server

Backup server limitations

- The backup server cannot back up files if you are using S3 backend storage.
- The backup server cannot back up or restore files if storage is encrypted.
- When the backup server uses the HTTP protocol for downloads, it cannot scale for larger installations. We recommend using the Rsync method for larger installations.
- If backup is performed during peak production time, system performance may be affected.

Recommendations for best performance

- Configure FileCloud target backup only in one web node in the HA setup.
- Route traffic via private network.

Installation

Follow the installation procedures at FileCloud Backup Server Installation.

Configuration of standalone backup server for HA

1. Follow the configuration steps at FileCloud Backup Server Configuration.
2. Add the following code to **backupagent.php**.

```
// ... Server URL
define("BACKUPAGENT_ACCESS_KEY", "filecloudbackups" );

//Additional mongodump params
//Use this if you have additional params to be passed to mongodump command
define("BACKUPAGENT_MONGODUMP_PARAMS", "--host "rs0/ hostname of Mongo1,hostname
of Mongo2,
```

```
hostname of Mongo3" --username dbuser --password password --authenticationDatabase
admin " );
```

3. If your installation is using a non-default MongoDB data path, add the following line:

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

RHEL:
define("BACKUPAGENT_DBDATA_PATH","/var/lib/mongo");
```

HA System Tests and License Installation

Install the FileCloud license
To install the FileCloud license, follow the instructions at Install the FileCloud License.

HA setup system health checks

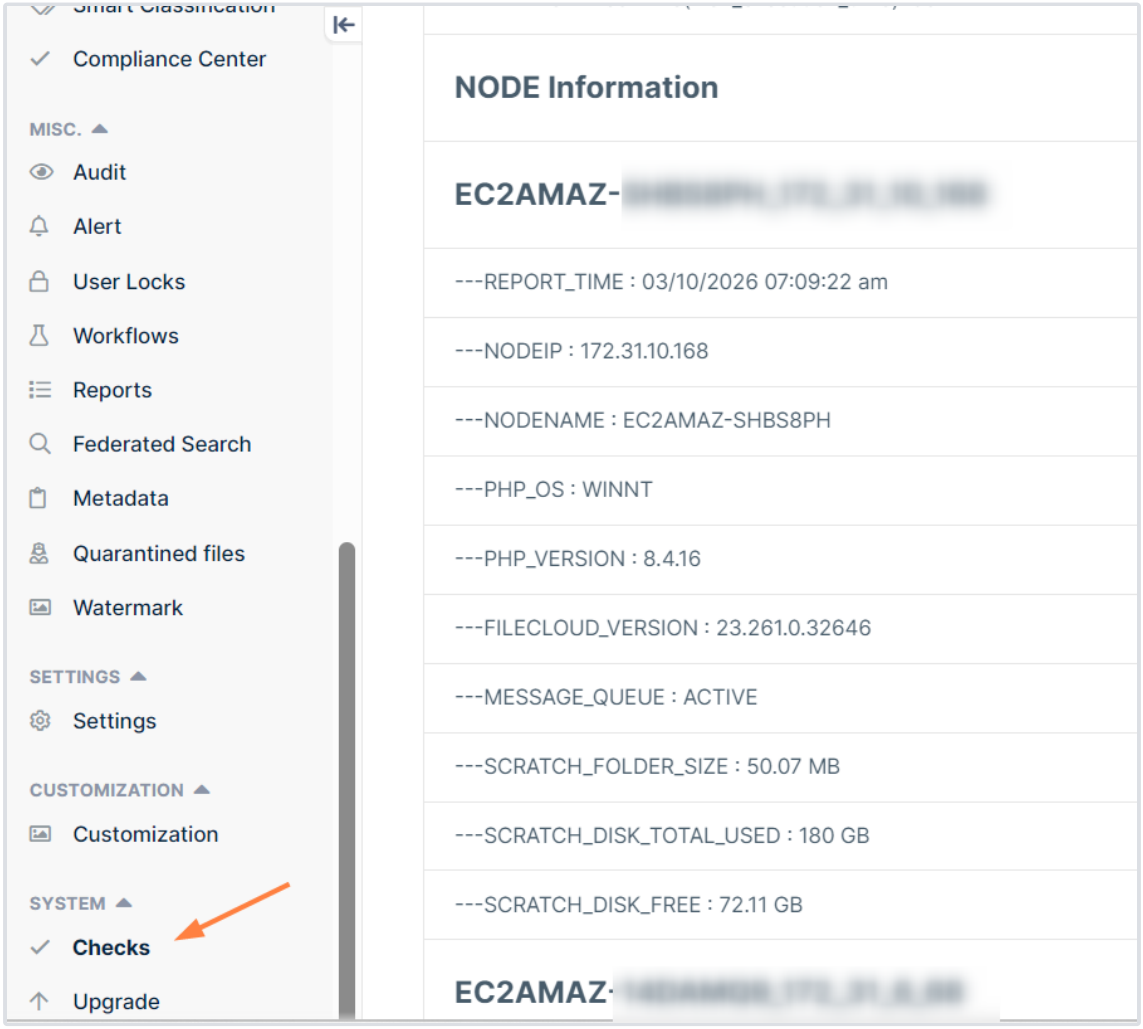
The Installation Checks page on the admin portal gives information about the health of each node.

- When you run a system check, the Installation Checks page shows one record with health information for each node of the HA system.
- Cron continues adding node information to the checks.
- This data helps you determine node information such as code level and MQ status.

Since Cron is providing the data for the system check, it can take a few minutes for Cron to run and collect the data.

To see the System Check:

1. Open a browser and log in to the admin portal.
2. From the left navigation pane, under **SYSTEM**, click **Checks**.



System Availability Tests:
Application Servers:
To test app server HA, turn off one of the app servers by logging into the app server (for example, Web Node1) and stopping the Apache service. The service should be accessible because the loadbalancer will reroute traffic to Web Node2 or Web Node3.

Database Servers:
To test database replica set redundancy, stop MongoDB service on one of the MongoDB nodes and service should be accessible with the two other database servers running.

Configure Cluster Authentication with SSL

A MongoDB HA cluster is configured to listen to external requests so that all nodes in the cluster are able to sync with one another. Hosting such a configuration in a private dedicated network is secure, but hosting it in an intranet or public network is not. It is necessary to enable authentication on these

clusters. Follow the steps outlined here to enable authentication on a MongoDB cluster and upgrade it to use SSL/TLS certificates.

As a prerequisite you are required to have a working HA cluster. It can either be a replica set cluster or a sharding cluster.

Enable Mongodb Authentication:

Enable Role-Based Access Control

For encryption to be used in your replica set, first activate Role-Based Access Control (RBAC). By default, a MongoDB installation permits anyone to connect and see the data. Having RBAC enabled is mandatory for encryption.

Create a DB user in MongoDB to use in FileCloud for secure database access.
In this example, the user has the following credentials:

User Name	Password
dbuser	passw0rd1

To create the user, enter:

OS	Command
Linux	$ use admin $ db.createUser({user: 'dbuser', pwd: 'passw0rd1', roles:['root']})

Now to connect to MongoDB in Linux, enter following command:

OS	Command
Linux	$ mongosh -u dbuser-p passw0rd1 --authenticationDatabase "admin"

Configuration of mongodb to use TLS/SSL:

In order to use encryption, create certificates on all nodes and have a certification authority (CA) that signs them.

For testing purposes (to ensure encryption is working) you can use self-signed certificates; for a production environment, it's better to use valid certificates.

To proceed with certificate generation make sure you have **OpenSSL** installed on your system and that your certificates satisfy these requirements:

- all certificates need to be signed by the same CA
- the common name (CN) required during certificate creation must correspond to the hostname of the host
- any other field requested in certificate creation should be a non-empty value and should reflect your organization details
- all fields, except CN, should match those from the certificates for the other cluster members

The following guide describes all the steps to configure internal X.509 certificate-based encryption.

1 – Connect to one of the hosts and generate a new private key using openssl:

OS	Command
Linux	$ openssl genrsa -out mongoCA.key -aes256 8192

This creates a new 8192-bit private key and saves it in the file mongoCA.key. Enter a strong passphrase when requested.

2 – Sign a new CA certificate

Now, create the “test” local certification authority that you’ll use later to sign each node certificate.

During certificate creation, values must be entered into some fields. You may choose these values randomly but it is better if they correspond to your organization’s details.

OS	Command
Linux	$ openssl req -x509 -new -extensions v3_ca -key mongoCA.key -days 365 -out mongoCA.crt

3 – Issue self-signed certificates for all nodes

For each node, generate a certificate request and sign it using the CA certificate created in the previous step.

Remember: Fill out all fields requested with the same values for each host, except fill out a different common name (CN) for each host - use a common name that corresponds to the particular hostname.

For the first node issue the following commands.

OS	Command

Linux	$ openssl req -new -nodes -newkey rsa:4096 -keyout mongossl1.key -out mongossl1.csr
	$ openssl x509 -CA mongoCA.crt -CAkey mongoCA.key -CAcreateserial -req -days 365 -in mongossl1.csr -out mongossl1.crt
	$ cat mongossl1.key mongossl1.crt > psmdb1.pem

Issue the same commands for the second and third nodes.

4 - Create certificate for FileCloud web nodes

OS	Command
Linux	$ cat psmdb1.pem psmdb2.pem psmdb3.pem > filecloud-mongo.pem

5 – Place the files

You could execute all of the commands in the previous step on the same host, but instead copy the generated files to the proper nodes:

- Copy to each node the CA certificate file: **mongoCA.crt**
- Copy each self-signed certificate **<hostname>.pem** into the relative member
- Create on each member a directory that only the MongoDB user can read, and copy both files there

OS	Command

Linux	$ sudo mkdir -p /etc/mongodb/ssl
	$ sudo chmod 700 /etc/mongodb/ssl
	$ sudo chown -R mongod:mongod /etc/mongodb
	$ sudo cp mongossl1.pem /etc/mongodb/ssl
	$ sudo cp mongoCA.crt /etc/mongodb/ssl

- Copy these files to all web nodes and make sure apache has access:

  /etc/ssl/filecloud-mongo.pem
  /etc/ssl/mongoCA.crt

6 – Configure mongod

Finally, inform mongod about the certificates to enable encryption.

Change the configuration file **/etc/mongod.conf** on each host adding the following rows:

OS	Command
Linux	net: ssl: mode: requireSSL PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem CAFile: /etc/mongodb/ssl/mongoCA.crt

Restart Mongod Daemon:

OS	Command
Linux	$ Systemctl restart mongod

Put the proper file names on other hosts (mongossl2.pem on mongossl2 hosts, and so on)

Now you should have a properly configured replica set that uses encrypted connections.

Issue the following command to connect on node mongossl1:

OS	Command
Linux	$ mongosh --authenticationDatabase "dbuser" --host mongossl1:27017 --ssl --sslCAFile /etc/ssl/mongoCA.crt --sslPEMKeyFile /etc/mongodb/ssl/mongossl1.pem -u dbuser -p passw0rd1

Certificate Notice :

For production use, your MongoDB deployment should use valid certificates generated and signed by a single certificate authority. You or your organization can generate and maintain an independent certificate authority, or use certificates generated by a third-party TLS/SSL vendor.
MongoDB can use any valid TLS/SSL certificate issued by a certificate authority or a self-signed certificate. If you use a self-signed certificate, although the communications channel is encrypted, there is no validation of server identity. Although such a situation prevents eavesdropping on the connection, it leaves you vulnerable to a man-in-the-middle attack. Using a certificate signed by a trusted certificate authority will permit MongoDB drivers to verify the server's identity. In general, avoid using self-signed certificates unless the network is trusted.

Enable Cluster Node Authentication

To enable the cluster nodes to communicate with each other in a secure mode, enable what is called "Internal Authentication". This is done by using an x509 certificate or secure keyfile and configuring each cluster node to use that key.

1-Using x509 certificate:

You can use the same Pem file created for each node in the previous step for the cluster authentication between nodes, or you can generate another Pem file used for this purpose only.

MongoDB configuration should appear as follows:

OS	Command

Linux	`net:`
	`  ssl:`
	`  mode: requireSSL`
	`  PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem`
	`  CAFile: /etc/mongodb/ssl/mongoCA.crt`
	`  clusterFile: /etc/mongodb/ssl/mongossl1.pem`
	`security:`
	`authorization: enabled`
	`clusterAuthMode: x509`

Each node has its own PEMKeyFile and clusterFile.

Restart MongoDB server nodes.
Save the configuration changes and restart the server. Make sure the cluster is back to normal operation.

2-Using Keyfile:

1- Create secure key

Create a secure key with the following command.

OS	Command
Linux	$ sudo openssl rand -base64 741 > /etc/mongodb-keyfile $ sudo chmod 600 /etc/mongodb-keyfile $ sudo chown mongodb.mongodb /etc/mongodb-keyfile

2- Copy secure key to all nodes
After the key is generated, copy the key file to all the cluster nodes.

3- Modify configuration file to use the key
Edit mongodb.conf file and make the following changes

OS	Command

Linux	`net:`
	`  ssl:`
	`  mode: requireSSL`
	`  PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem`
	`  CAFile: /etc/mongodb/ssl/mongoCA.crt`
	`security:keyFile:/etc/mongodb-keyfile`

4-Restart MongoDB server nodes.
Save the configuration changes and restart the server. Make sure the cluster is back to normal operation.

Configure Other DB URLs In Config File

Edit the configuration file WWWROOT/config/cloudconfig.php and update the following lines :

Update DB URLs in cloudconfig.php

```
// ... Cloud Database
define("TONIDOCLOUD_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// connection parameter for db backups:
define("AUTOBACKUP_MONGODUMP_PARAMS", "--host 'rs0/HOST1,HOST2,HOST3' --username dbuser
--password passw0rd1 --authenticationDatabase admin --ssl --sslCAFile=/etc/ssl/
mongoCA.crt --sslPEMKeyFile=/etc/ssl/filecloud-mongo.pem " );
```

Note: If the password you supply in AUTOBACKUP_MONGODUMP_PARAMS doesn't work or contains special characters, use the password parameter embedded in the characters \"password\"
For example:

```
define("AUTOBACKUP_MONGODUMP_PARAMS", "--host 'rs0/HOST1,HOST2,HOST3' --username dbuser
--password \"passw0rd1?]\" --authenticationDatabase admin --ssl --sslCAFile=/etc/ssl/
mongoCA.crt --sslPEMKeyFile=/etc/ssl/filecloud-mongo.pem " );
```

Add WWWROOT/config/cloudconfig.php at the bottom:

Update DB URLs in cloudconfig.php

```
function
FC_MONGODB_URI_OPTIONS(){
    return [
        "tlsCertificateKeyFile" => "/etc/ssl/filecloud-mongo.pem",
        "tlsCAFile" => "/etc/ssl/mongoCA.crt"
    ];
}
```

and update the following line in WWWROOT/config/localstorage.php:

Update DB URLs in localstorageconfig.php

```
// ... Cloud Database
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
```

Restart Services

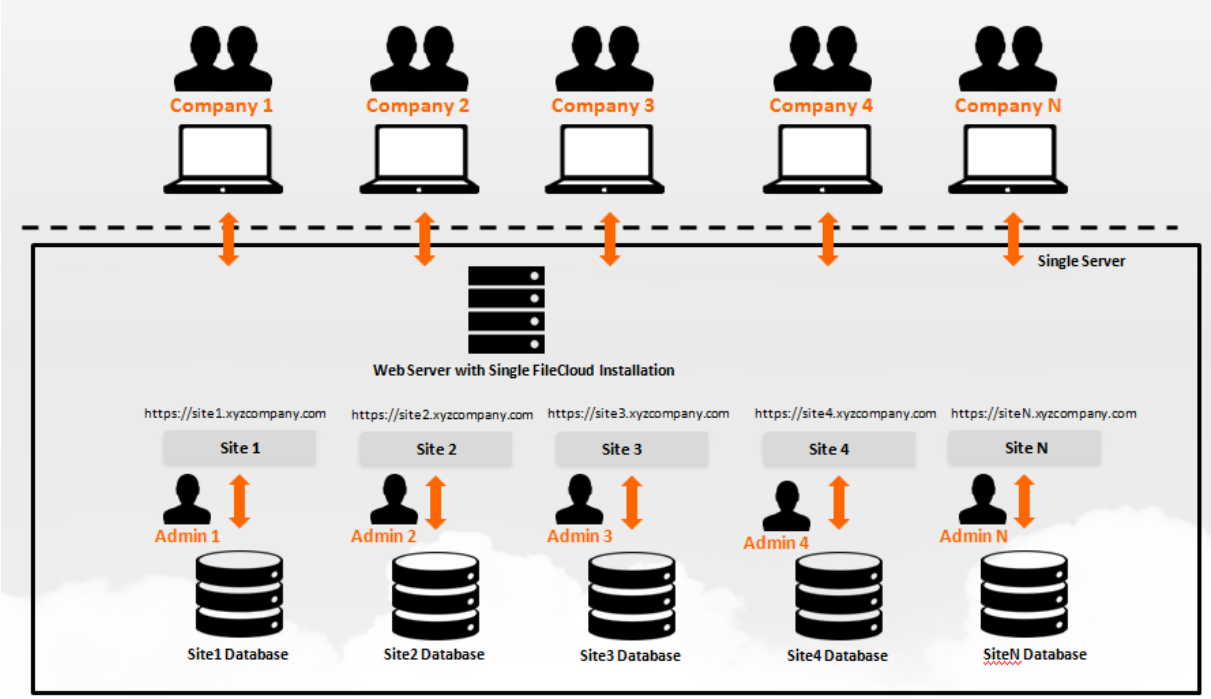
Finally, restart both MongoDB and Apache to get the security in-place.

Note

- In case of any issues, disable security in mongodb and fix the problems.
- To disable security, the mongodb security key has to be disabled and the database URLs have to be reverted back.

Multi-Tenancy Settings

It is possible with FileCloud to have a single install but still have many different independent FileCloud sites available.



In this section:

Multi-Tenancy Requirements

Administrators can install a single deployment of FileCloud Server but still have many independent FileCloud sites available.

General Requirements

1. You must have a fully working FileCloud installation before you proceed with multi-tenancy. Make sure all the install checks pass and all the checks in the admin portal are without errors.
2. Only a single SSL certificate can be installed for all the sites, so it is recommended that you use a wildcard SSL certificate for a main domain, such as: https://*.xyzcompany.com and then set up each site as a subdomain of the main site, for example, site1.xyzcompany.com and site2.xyzcompany.com
3. After adding a new site, you need to add an entry in your DNS configuration for the new site to point to the server on which FileCloud is installed.

4. When removing a site added previously, only the site is removed from the list; however, any data associated with that site or its database is not removed. We recommend you remove this separately to avoid data loss.
5. Each configured site needs its own license file. You cannot use a single license with different sites.

Enable Multi-Tenancy Support

Administrators can enable multi-tenancy support by editing the appropriate PHP file and setting the multisite option to 1.

💡 A sample **multi-sample.php** file is provided in your FileCloud installation. You can rename the sample file to **multi.php** if you need to.

To enable multi-tenancy support:

1. On the FileCloud Server, open the following file for editing:

```
WEBROOT/config/multi.php
```

2. Add the configuration as follows:

```
define("TONIDOCLOUD_MULTISITE_ENABLE",1);
```

Password encryption and logging in to a multi-tenant admin portal

To access multi-tenancy admin portal, log in to the admin portal as the superadmin user. The password for the superadmin must be specified in encrypted format in the multi.php file.

FileCloud includes a script that admins must use to generate an encrypted superadmin password and paste it into the multi-tenant configuration file.

Note: The default password in the multi-tenant configuration file cannot be used to sign in to the system.

To generate the password:

1. Locate the script file:
   Windows: C:/xampp/htdocs/resources/tools/security/passwordenc.php
   Linux: /var/www/html/resources/tools/security/passwordenc.php
2. Run the script. Your password should look similar to the password generated in the following code:

```
C:\xampp\htdocs\resources\tools\security>set path=C:\xampp\php

C:\xampp\htdocs\resources\tools\security>php passwordenc.php
This tool generates an encrypted password string
to paste into FileCloud configuration files

Enter your desired password: testpassword
Copy and paste the following string:
$pbkdf2-
sha512$50000$ENIGvUsu3T6rIbI5Bz9DXw$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtf
rVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw

Finished
```

3. Copy the string.
4. Find the sample multi-tenant config file:
   Windows: **C:/xampp/htdocs/config/multi-sample.php**
   Linux: **/var/www/config/multi-sample.php**
5. Copy **multi-sample.php**, and rename the copy **multi.php**.
6. Open **multi.php** and find the setting:

```
define("TONIDOCLOUD_MULTISITE_ADMIN_PASSWORD", 'Vrwfq7xNHV');
```

7. Paste the string generated by **passwordenc.php** over the password value:

```
define("TONIDOCLOUD_MULTISITE_ADMIN_PASSWORD", '$pbkdf2-
sha512$50000$ENIGvUsu3T6rIbI5Bz9DXw$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtf
rVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw');
```

   Note: The encrypted password must be surrounded by single quotes (not double-quotes) or it will be broken.
8. Save and close **multi.php**.
   The user superadmin can now sign in using the clear text password you entered as your desired password in **passwordenc.php**.

To login into the special multi-tenancy admin portal:

1. Open a browser and access the FileCloud admin portal.
2. In **User**, type in superadmin.
3. In **Password**, type in the clear text password you entered in **passwordenc.php**.
4. If Multi-Factor Authentication access is enabled, then provide the additional code to continue.

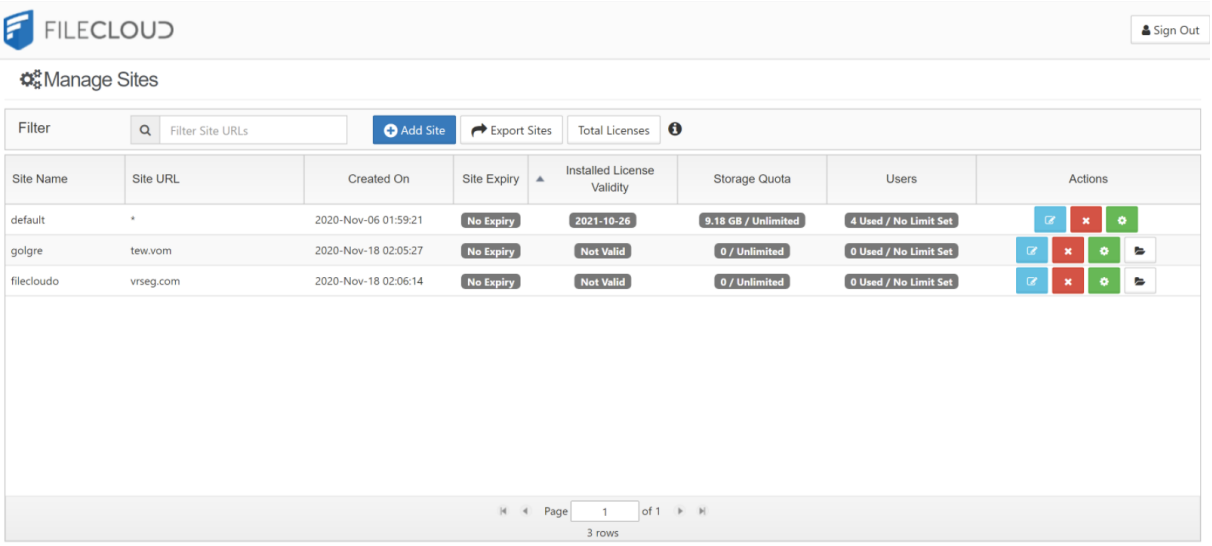
Manage Different Sites

When you log in as superadmin, the **Manage Sites** screen opens.

- **Storage Quota** column - the current storage quota and the maximum allowed storage quota limit in GB for that site.
- **Users** column- the current user count and maximum allowed limit for that site.

⚠ **Please note that in order for the current storage quota and current users to be calculated a Cron job must be set up by the admin.**

Figure 1. Admin portal for superadmin management of multi-tenant sites.



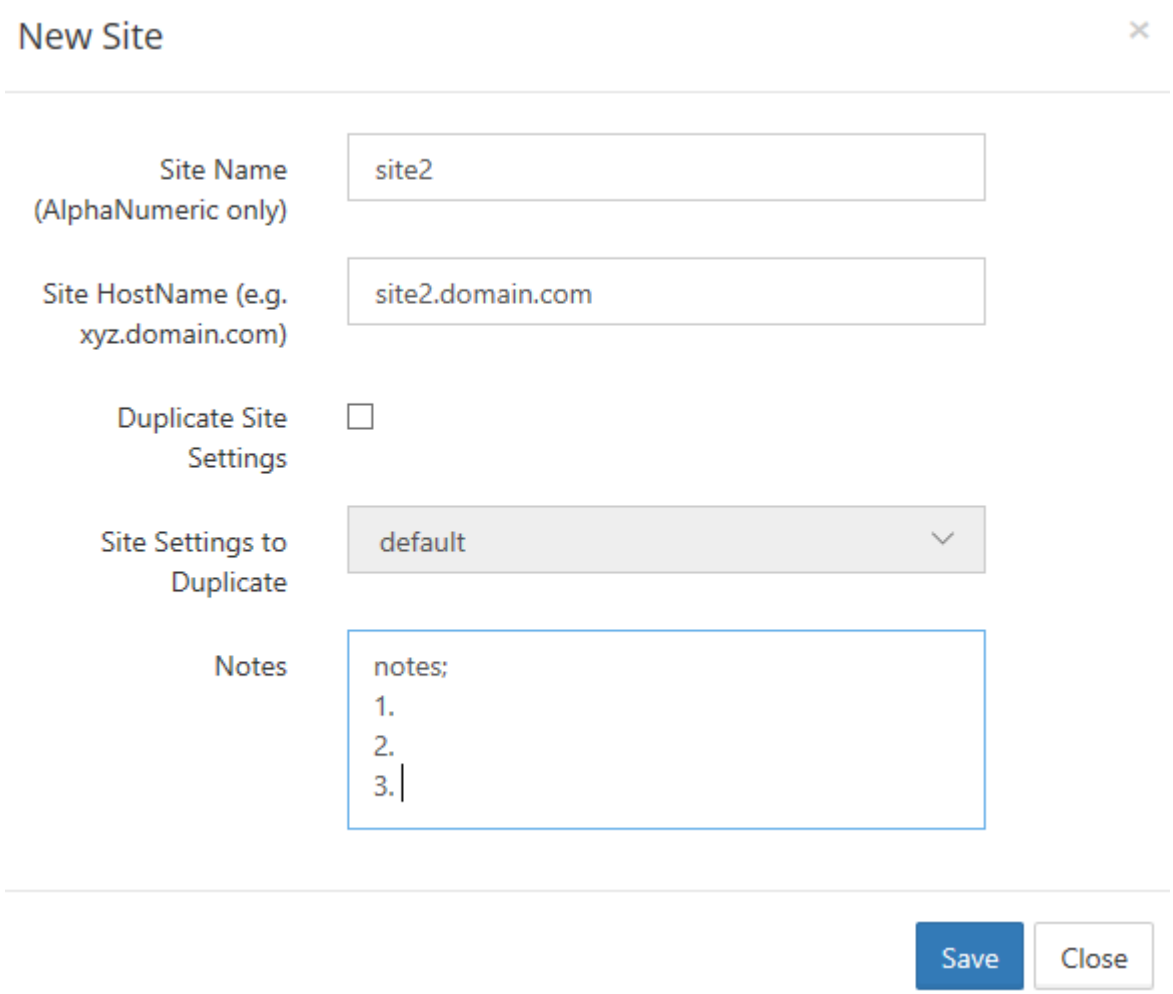
Since the report runs only once a month, updates to **Installed License Validity** may be delayed.

What do you want to do?

Add a new site

To add a new site, click on the **Add Site** button to open the **New Site** dialog box.

- Provide a **Site Name**, you cannot change the **Site Name** later. The **Site Name** must be alphanumeric and is used to prefix database names for this site.
- Provide the **Site HostName** (for example: site1.xyzcompany.com). Do not provide any http or https prefixes. The character @ is not permitted in site names.
- Make sure to add a DNS entry for the domain name to point to the server running FileCloud.
- You can duplicate the site settings by checking the **Duplicate Site Settings** check box and selecting a site in **Site Settings to Duplicate**. The new site is created with the settings from the selected site.
- **Notes** is optional.



|

View Site Settings

Site settings can be used to enforce limits on the total number of users and total storage quota in GB per site.

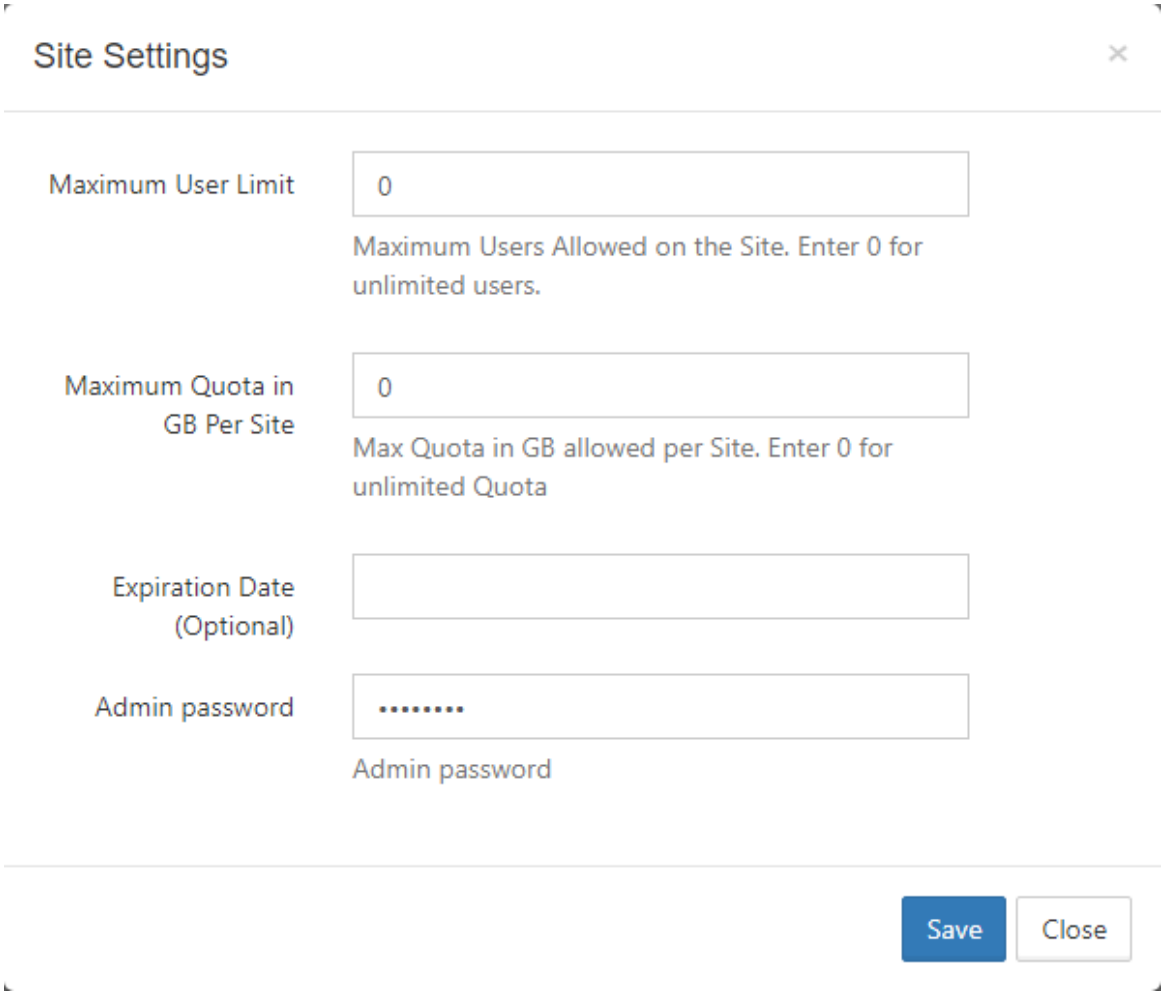
When **Maximum User Limit** is specified for a site, FileCloud does not allow additional users to be added when the limit is reached. 0 implies there is no limit to the number of users that can be added.

When **Maximum Quota in GB Per Site** is specified for a site, FileCloud limits the total GB of files added to ensure that total size of all files added will not be more than the quota specified. 0 implies unlimited quota.
Note: If the **User Storage Quota** (set in users' policies) for all users combined exceeds **Maximum Quota in GB Per Site** then new user creation is blocked. To enable admins to create additional users, the Superadmin must do one of the following:

- Increase **Maximum Quota in GB Per Site**.
- Set **Maximum Quota in GB Per Site** to 0 (unlimited).
- Set **User Storage Quota** (in all user policies) to 0 (unlimited).

When **Expiration Date** is specified, users cannot log in to the site after the expiration date is passed.

It is possible to set up an **Admin password** for a site directly in the **Site Settings** dialog box.



Access a newly added site

To access the newly added site, use the domain name setup for the site. For example, use https://site1.xyzcompany.com to access the user site and https://site1.xyzcompany.com/ui/admin/index.html to access the admin site.

Make sure to set up the site using the admin portal before opening up the site to new users.

> ⚠ All operations, including use s3 backend, add files, enable encryption, disable encryption, create reports, and create workflows can be performed in multi-tenants.

Remove a site

Select the site entry and click **Delete** to remove the site entry. Note that you have to manually remove the sites database and data. These are not removed automatically.

Note that the default site is the fallback site when a user tries to access FileCloud without using any of the domains specified and therefore cannot be edited or removed.

Enable Email Notifications if Cluster is Down

If you are running a multi-tenant system with FileCloud, make sure all site URLs for each site are accessible from the local site. They are used by the task scheduler/cron to run automated tasks for each site.

Email can be used to monitor not only clusters in a multi-tenancy but any MongoDB replica you have set up.

FileCloud uses a cron job (on Linux) or Windows Task Scheduler (on Windows) to perform certain ongoing maintenance tasks.
One of these tasks can be to send an email when one of the cluster instances or any MongoDB replica is down.

The email settings used for this notification are in **cloudconfig.php**.

- The email will be sent from: **TONIDOCLOUD_REPLY_TO_EMAIL**
- The email will be sent to the address configured in: **TONIDOCLOUD_DBSERVER**

These settings should already be configured in your **cloudconfig.php** file.

What do you want to do?

Add a PHP file to Cron

These instructions assume your FileCloud installation is in the **/var/www/** folder.

To add a PHP to a Cron Job in Linux:

1. Open the crontab (assuming apache is running under www-data account).

```
crontab -u www-data -e
```

2. At the end of the crontab file add the following line:

```
php ./tools/mongohealth/index.php
```

3. Save and exit.

Add a PHP file to Scheduler

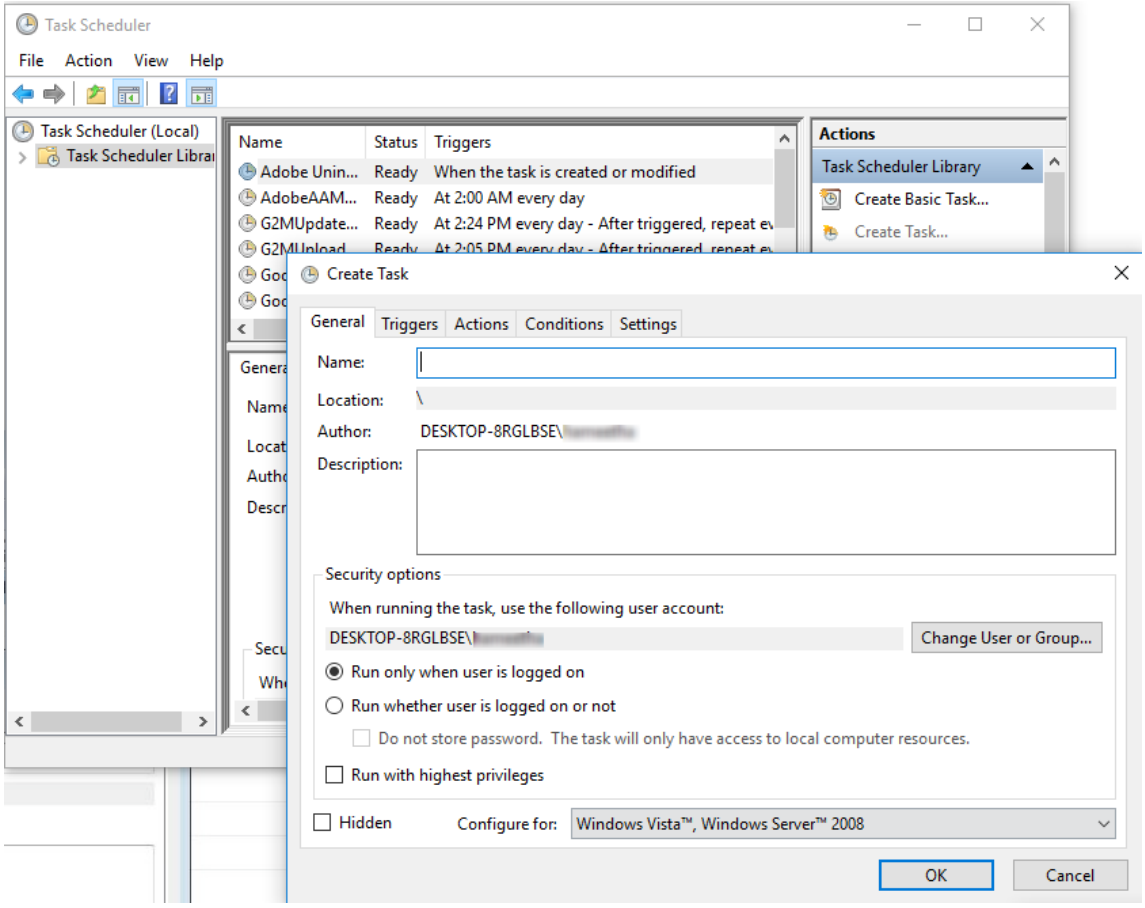
To configure a Scheduled Task in Windows:

1. Use Notepad or similar program to create a new file named "fccron.vbs" in a location like c:\xampp\htdocs\resources\backup folder.
2. Enter the following contents from the code block below and save the file. Additionally, in the code block below ensure that paths to php.exe and cron.php files are correct.

```
CreateObject("Wscript.Shell").Run "C:\xampp\php\php.exe -f ""c:
\xampp\htdocs\core\framework\cron.php"" ", 0, False
```

3. Open Task Scheduler.
4. In the right menu under **Actions**, click **Create Task.**

5. On the **General** tab, in **Name**, type in **MongoDB Cluster Notification**, or something similar.



6. On the **Triggers** tab, click **New Trigger**.
7. For **Begin the Task**, select **On a Schedule**.
8. In **Settings**, select **Daily**, select a time, and then select **Recur every 1 days**.
9. Under **Advanced Settings**, select **Repeat Task every 5 minutes**, to specify how often you want the trigger to run.
10. For **Duration**, select **Indefinitely**.
11. Check **Enabled**, and then click **OK**.
12. On the **Actions** tab, click **New Action**.
13. For **Action**, select **Start a program**.
14. Enter the following path:

```
php ./tools/mongohealth/index.php
```

15. Click **OK**.

Enable Automatic License Renewal and Reporting

An administrator can set up a Task Scheduler/cron job for a multi-tenancy site with a SPLA license, so that license renewal and reporting will occur automatically.

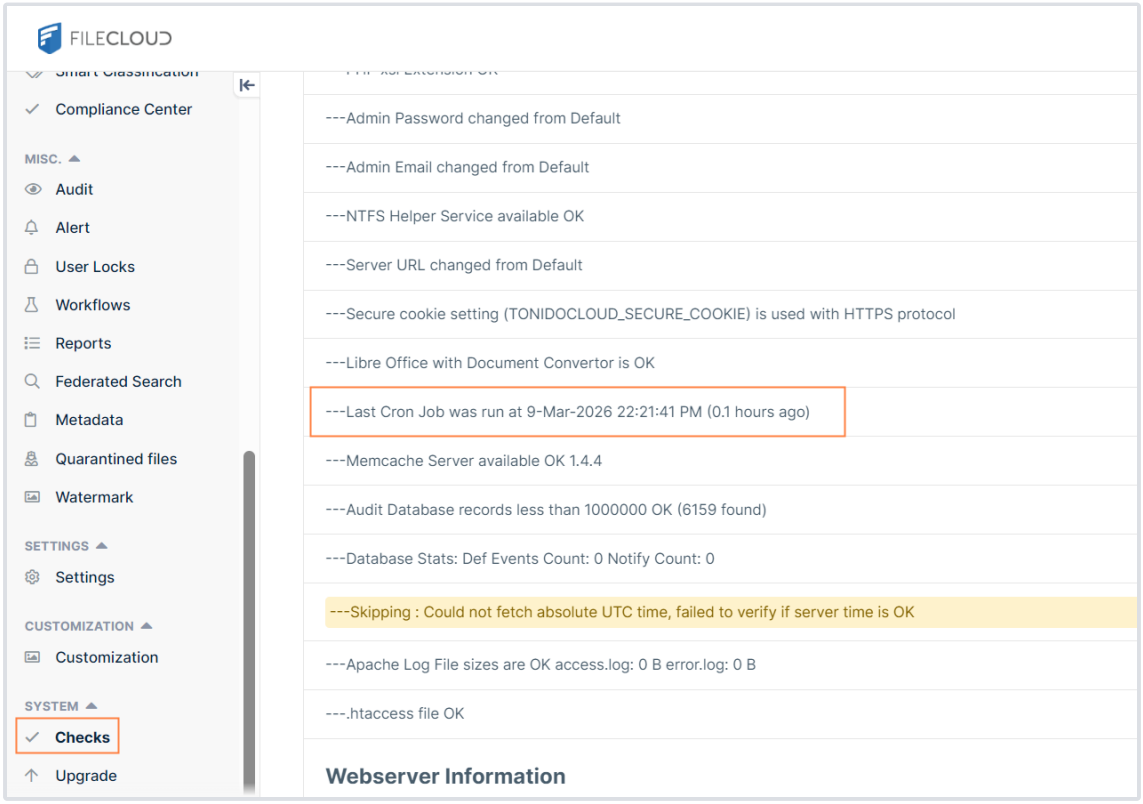
If a Task Scheduler (Windows) or cron job (Linux) is not set up for a multi-tenancy site with an SPLA license, then license renewal and reporting does not happen automatically.
The site won't automatically acquire a monthly license; only the admin can acquire it by logging in. If the monthly report is not completed, then users will get a license error when they log in.

Name resolution and HTTPS:

- The URLs of all tenants must be resolvable on the FileCloud server. A workaround is to enter the tenant URLs in the local hosts file.
- If HTTPS is used, the SSL certificates must be installed in Apache even if the SSL termination is done in an external load balancer.

If site licensing expires every month and is not renewed automatically when using the SPLA license, please follow the steps below to troubleshoot.

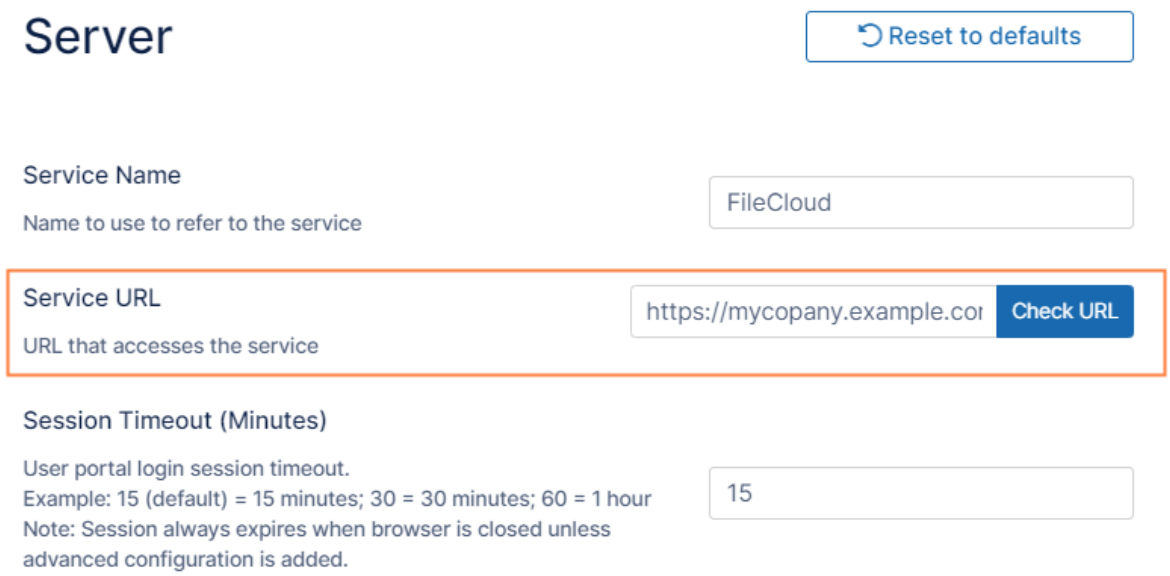
1. Open the admin portal for the specific site; click **Checks** and verify that the cron job was run recently.



2. If the cron job was not run recently, it is **critical** that a Task Scheduler or cron job be set up to run properly when running a multi-tenant system. See instructions on how to set this up. When running cron jobs in multi-tenant scenarios, ensure all site domain names are resolvable on the system running the cron job.

The cron job uses the **Server URL** setting specified in the Server settings page to access the site. Make sure the Server URL works on the local system correctly.
If you are using an HTTPS site, ensure that the Server URL has the correct prefix (https instead of http). After making the Server URL change, wait some time to see if the cron job is now reported as working correctly.

Note: If your DNS doesn't resolve the site URL inside the FileCloud server, you can work around it by adding an entry to the domain name to the local Windows HOSTS file in the server.


Server
Reset to defaults
Service Name
Name to use to refer to the service
FileCloud
Service URL
URL that accesses the service
https://mycopany.example.cor
Check URL
Session Timeout (Minutes)
User portal login session timeout.
Example: 15 (default) = 15 minutes; 30 = 30 minutes; 60 = 1 hour
Note: Session always expires when browser is closed unless advanced configuration is added.
15

Folder-Level Permissions

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 whichever is more restrictive, folder-level or share permissions, apply.

Folder-Level Permissions Support	Folder-Level Permissions Do Not Support
✅ Interaction with share permissions. ✅ Allowing or restricting access by specifying a user's email account ✅ Folders in Managed Storage ✅ Configuration by admins, and configuration by the owner of the folder, if permitted.	❌ Folders in Network Storage ❌ Permissions set by a user other than the owner

You can apply folder-level permissions to:

- a user's folders
- Team folders

You can also enable users to apply folder-level permissions to their folders.

It's important to understand what takes precedence when there are folder-level and share permissions on the same folder, and when sub-folders inherit the permissions of their parent folders. It's also necessary to know which permissions apply when a user and the user's group(s) have different permissions for the same folder.

To simplify complex permission interactions, FileCloud provides effective permissions calculators that show you which permissions apply in these situations. The different effective permissions calculators are explained in the topics in this section.

The topics in this section show you how to enable and apply folder-level permissions and explain which permissions take precedence when multiple permissions are applied.

Setting Folder-Level Permissions from the Admin Portal

Apply folder-level permissions for users or groups to certain folders if you want to limit their access to the folders when they are shared.

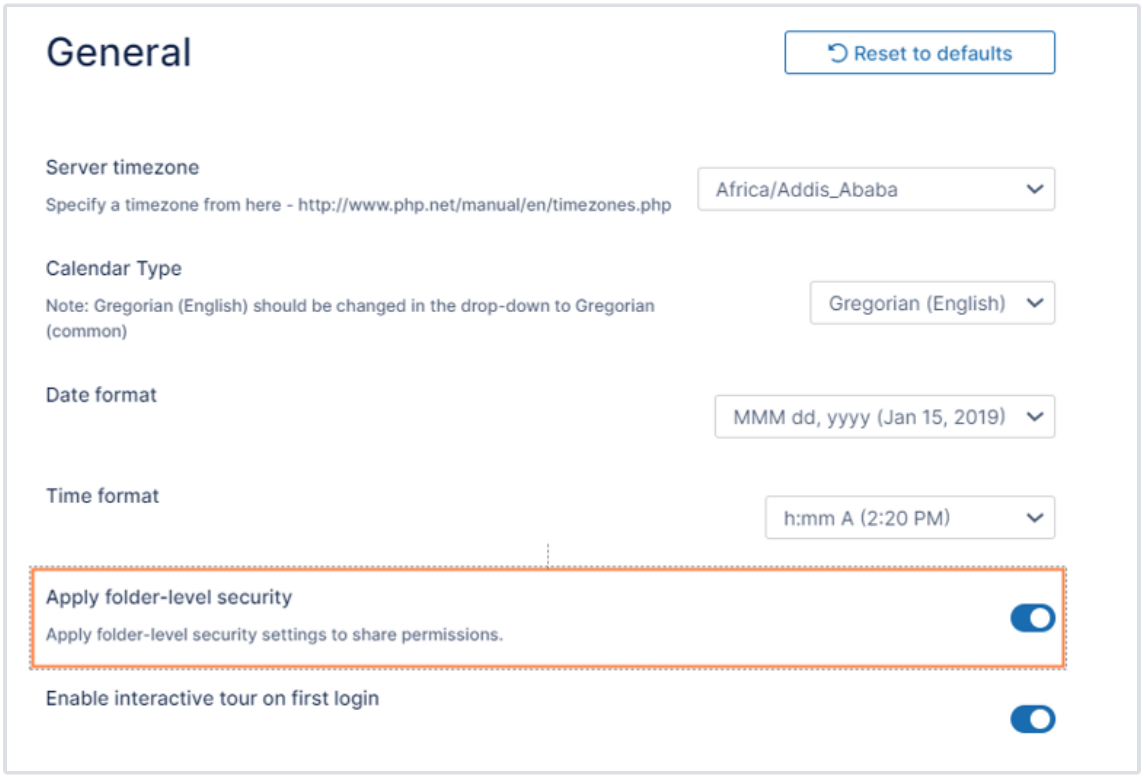
- You can apply folder-level permissions directly to user folders from the **Manage Users** page.
- You can apply folder-level permissions to Team Folders from the Manage Team Folders page. See instructions at Setting Folder-Level Permissions on Team Folders.
- You can edit folder-level permissions set by users and folder-permissions set on Team Folders from the **Folder Permissions** link in the navigation panel.

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
  - Subfolders inherit the folder-level permissions of their immediate parent folders.
  - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.
- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

To configure FileCloud to allow setting folder-level permissions

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. Enable **Apply folder-level security.**

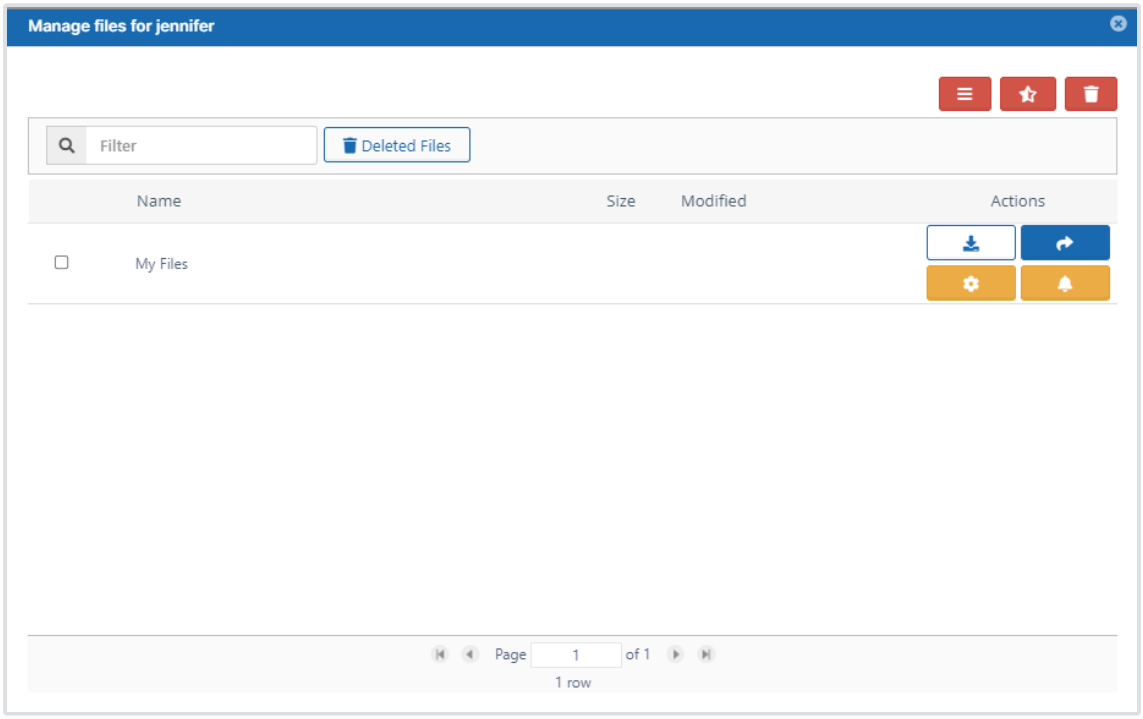


Now, folder-level permissions can be set.

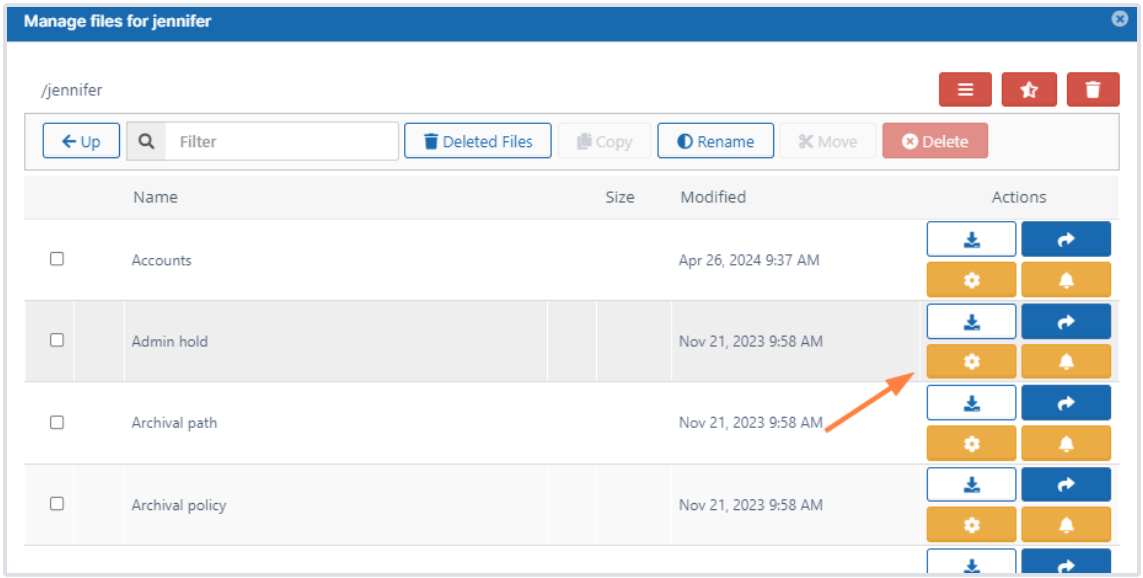
To apply folder-level permissions to user folders:

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.

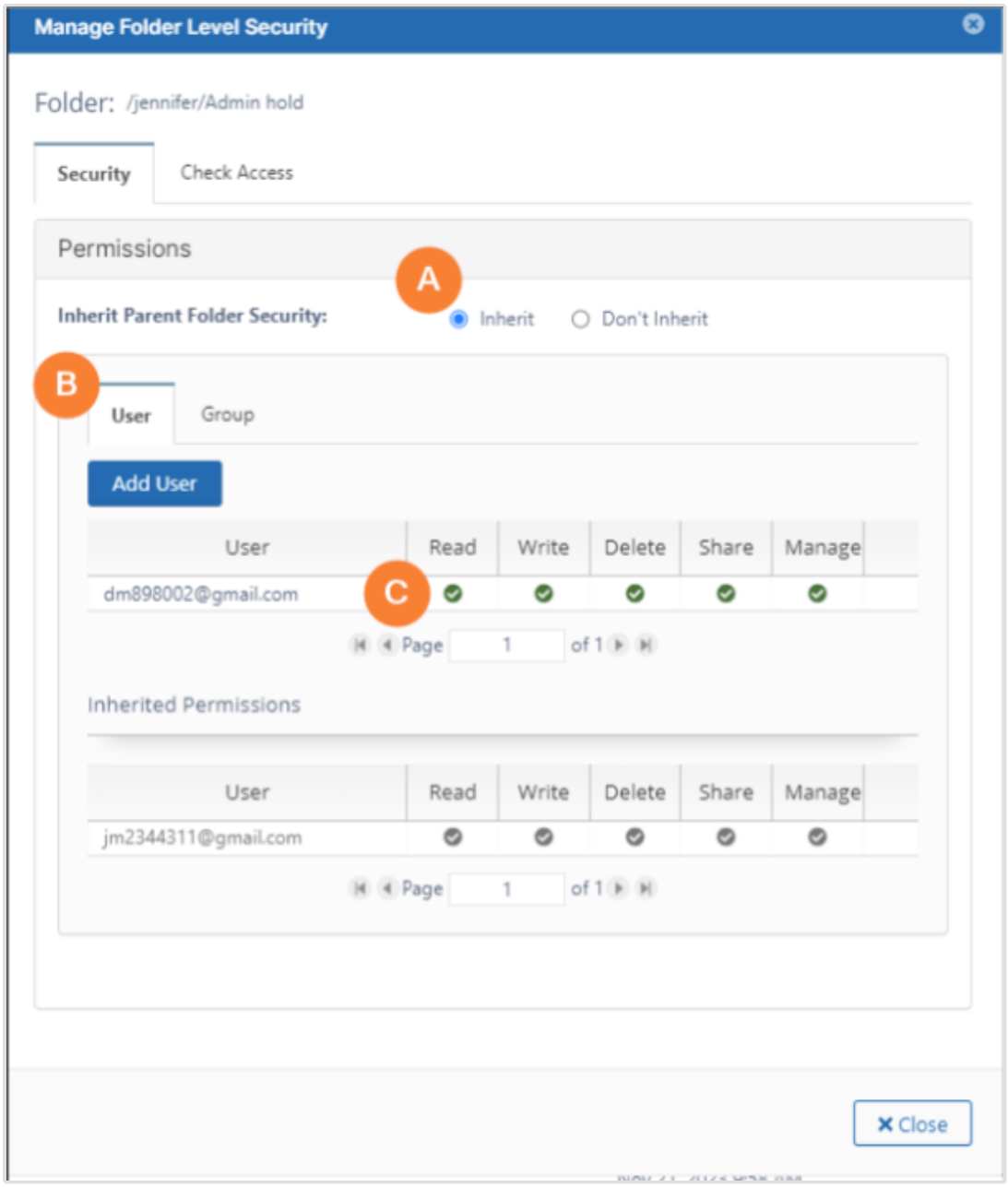


4. Expand **My Files** and locate the folder that you want to set folder-level permissions for.
5. Click the **Manage Access**
   
   button in the folder's row.



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

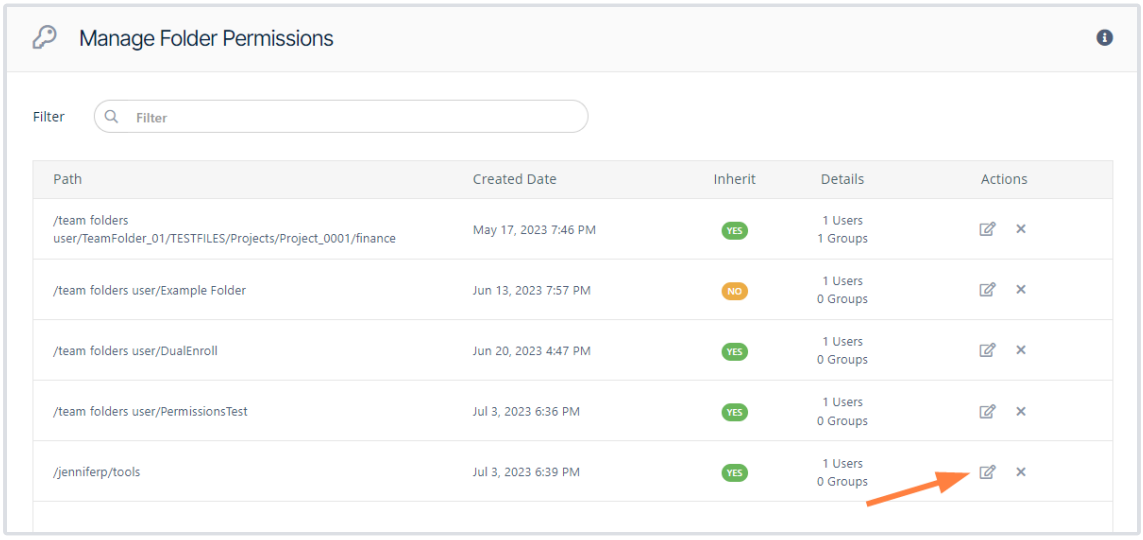
6. Follow the steps below to assign and change user and group folder-level permissions. Users who do not appear
on the list have all folder-level permissions to the folder (unless their group permissions are limited)



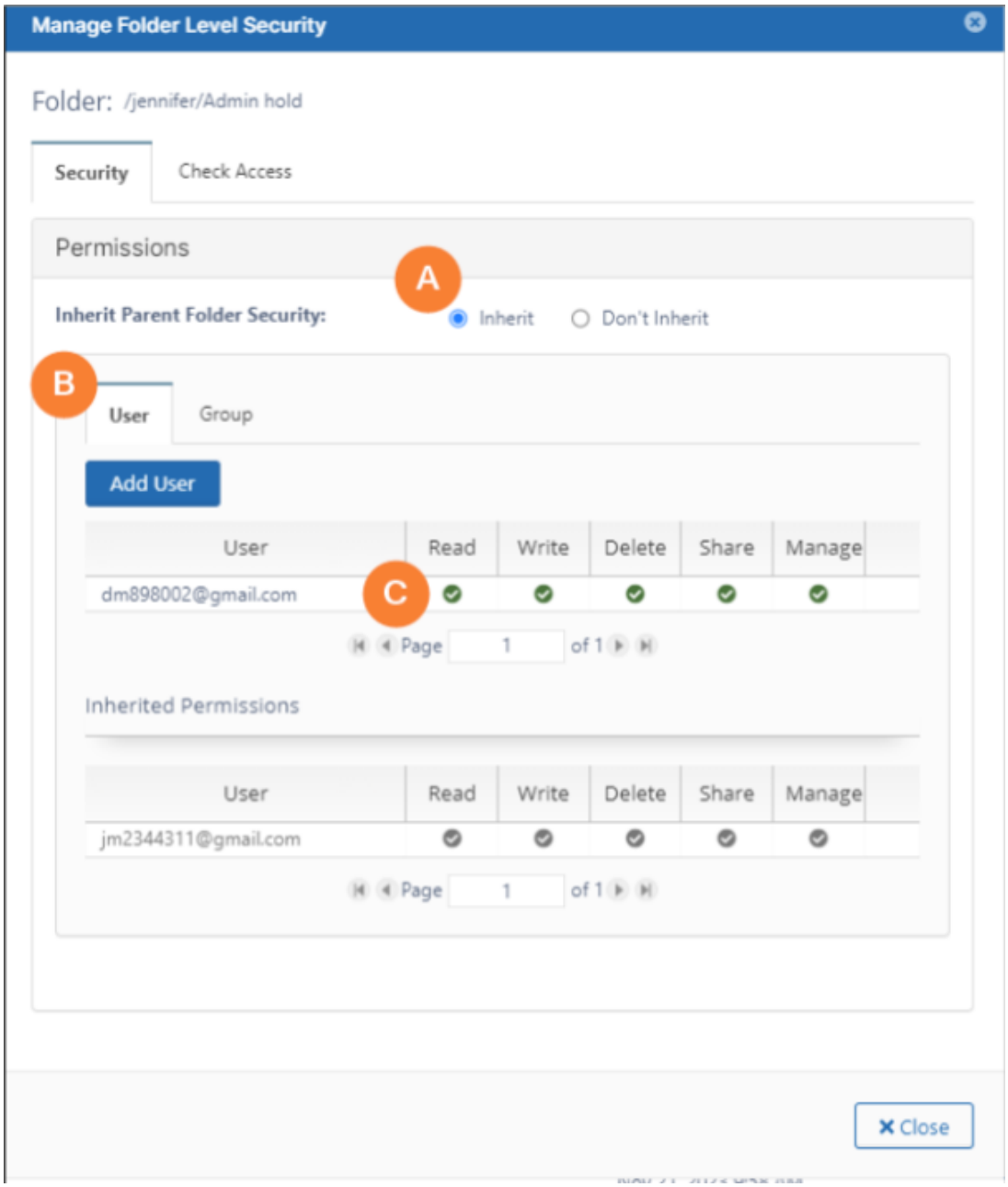
A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.
B Click **Add User** to add a user and limit their access to the folder, or click the Group tab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

To edit folder-level permissions set by admins on Team Folders and set by users on user folders:

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.

Checking Effective Permissions

Check Effective Permissions

Administrators can check to see which effective folder permissions a user has to a folder. Effective permissions are the actual permissions when various permissions assigned to a user for the same folder are combined (for example, effective permissions show which permissions apply when a user has both individual and group permissions).

However, when you are using the methods shown on this page, this does not take into account which share permissions may have been given to the user for the folder. So, when the folder is shared, the share permissions may change the actual access the user has to the folder.



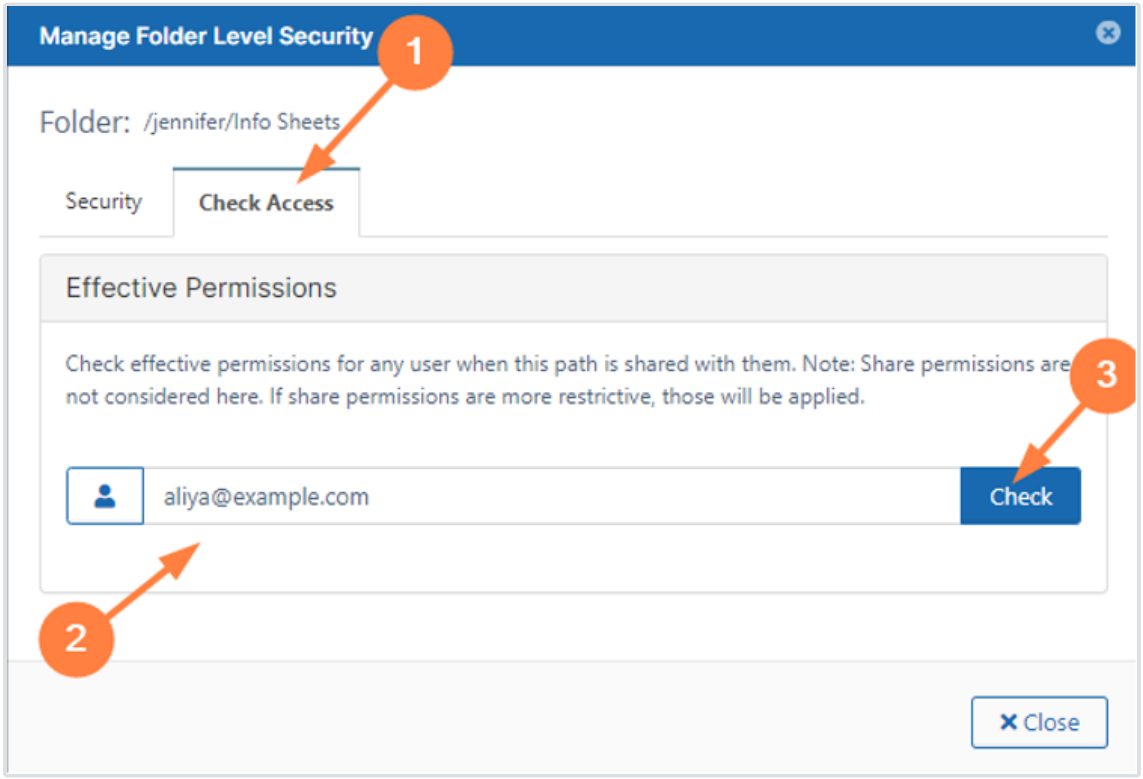
When a user checks effective permissions for Team Folders in the user portal, share permissions and folder-level permissions are taken into account.

The possible folder-level permissions are:

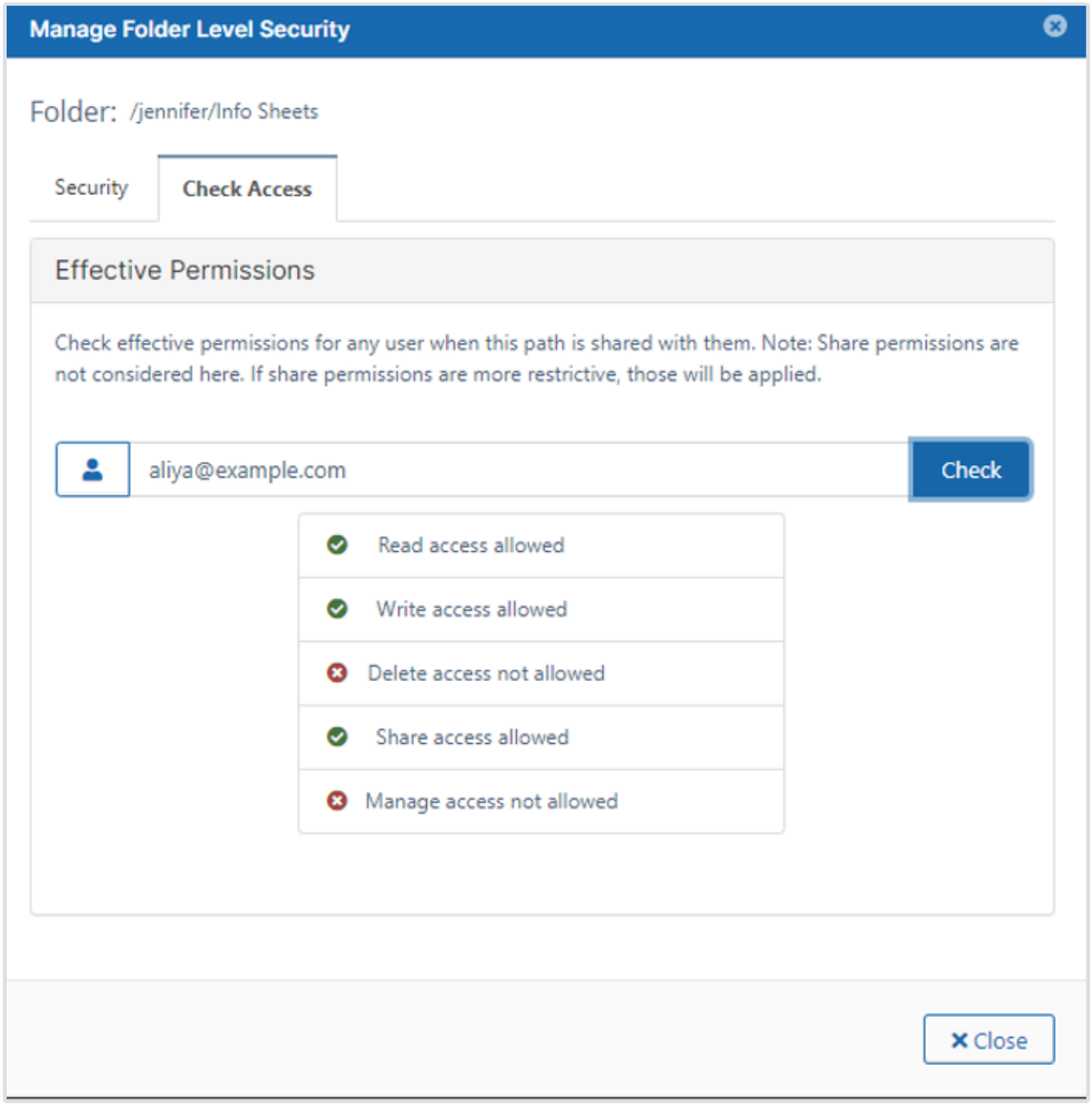
Permission	Description
Read	• Allows Downloading Files • Allows Previewing Files
Write	• Allows uploading and modifying existing files • Allows creating files and folders • Allows renaming files and folders
Delete	• Allows deleting files and folders
Share	• Allows sharing files and folders
Manage	• Allow managing folder-level permissions for this folder

To check a user's effective permissions on a folder from the Manage Folder Permissions or Manage Users screen:

1. Access the **Manage Folder Level Security** dialog box in one of the ways shown on this page.
2. Select the **Check Access** tab.
3. In the box next to the user icon, enter the user's email id for their FileCloud account.
4. Click **Check**.



The user's permissions to the folder are listed:



Permission inheritance

How Do Inherited Permissions Work?

In general, a **folder** can be in one of the following states:

- The sub-folder has all of the same permissions as its parent folder
- The sub-folder has all of the same permissions as its parent folder, plus additional permissions
- The sub-folder has all of the same permissions as its parent, minus additional permissions
- The sub-folder's permissions are not connected in any way to the parent folder and the sub-folder retains a separate set of permissions

When setting folder-level permissions in FileCloud, you have the following options:

Option	Description
Inherit Permissions	Permissions set by default in this folder are exactly the same as its parent folder's permissions.
Don't Inherit Permissions	Permissions set in this folder don't inherit from its parent folder's permissions and are specific to only this folder.

Enabling Users to Set Folder-Level Permissions

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
  - Subfolders inherit the folder-level permissions of their immediate parent folders.
  - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.
- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

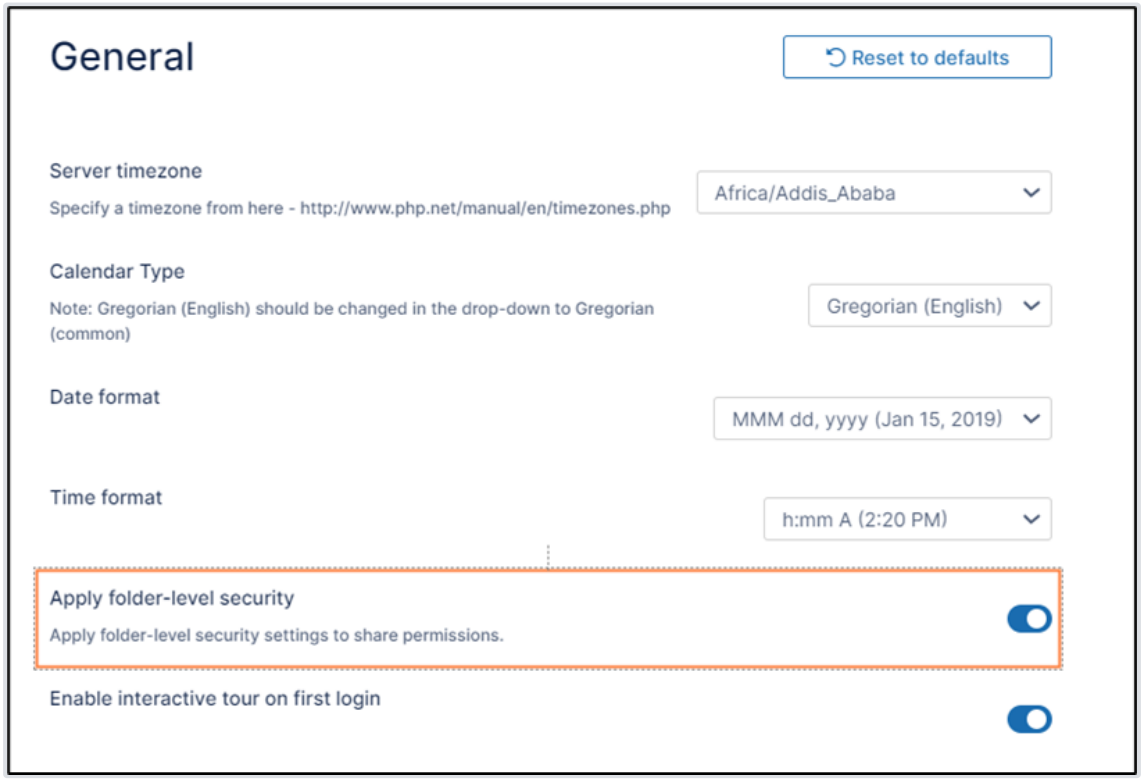
To enable users to set folder-level permissions:

First enable folder-level security settings, then enable setting folder-level permissions in the user policy.

1. Enable folder-level permissions in Misc > General settings

To enable folder-level permissions in your system:

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. Enable **Apply folder-level security.**

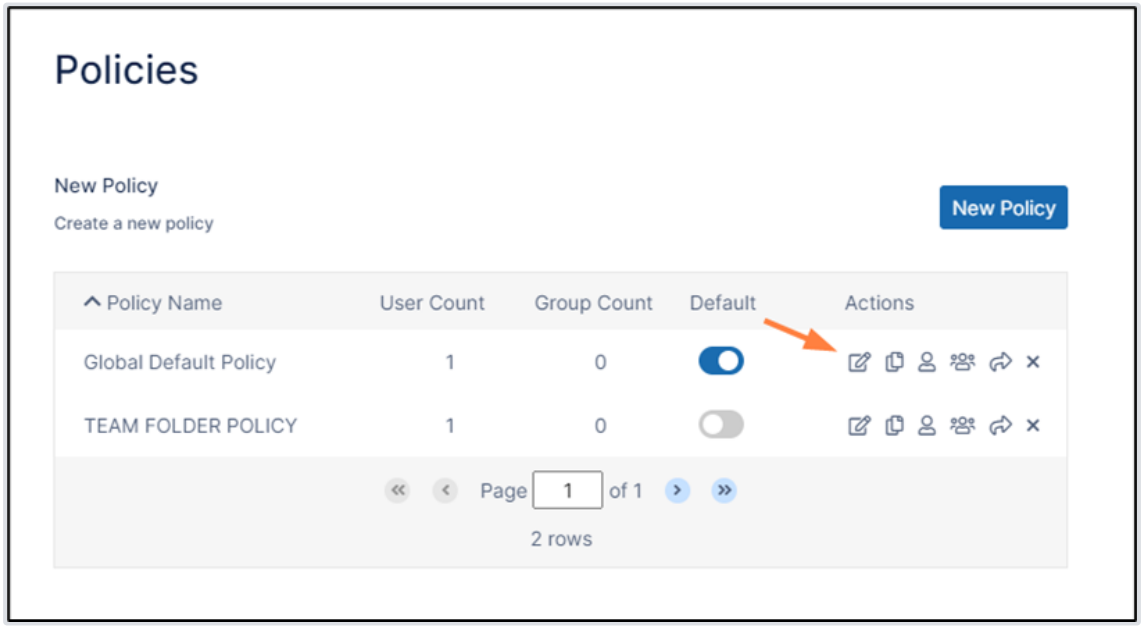


Now, folder-level permissions can be set.

2. Enable users to set folder permissions in their user policies

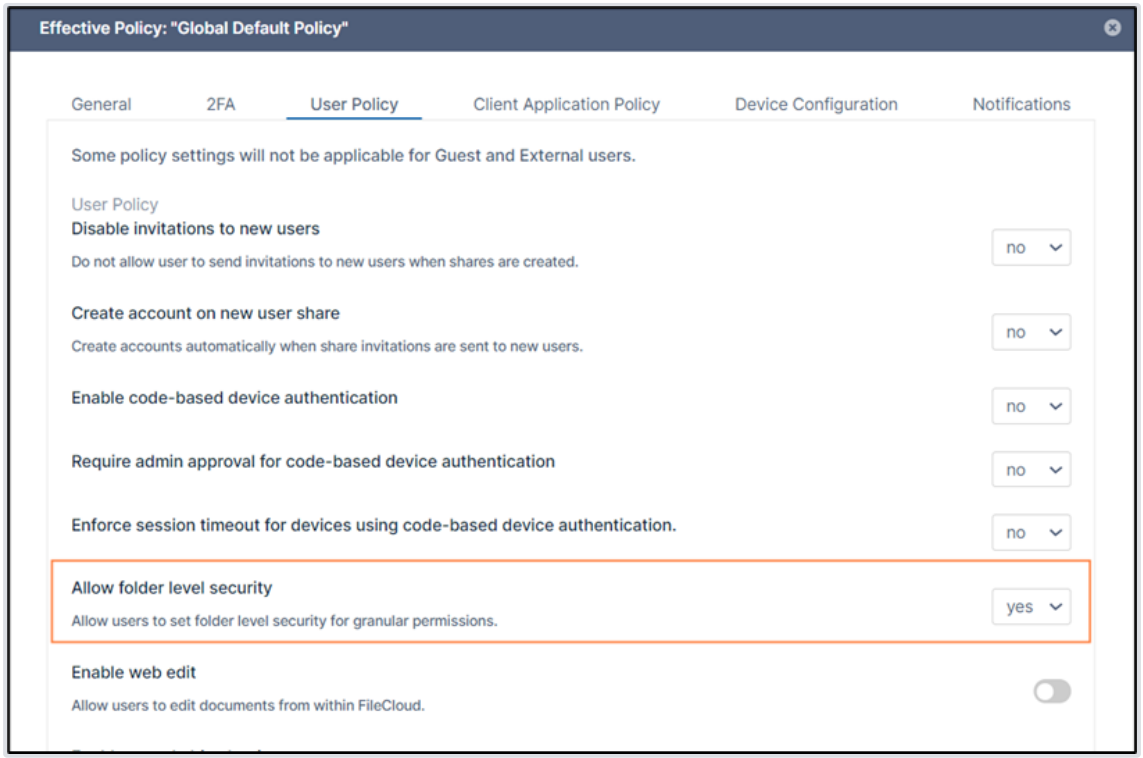
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**

   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



The **Policy Settings** dialog box opens.

3. Click the **User Policy** tab.
4. Scroll down to the setting **Allow Folder Level Security** and set it to **yes**.

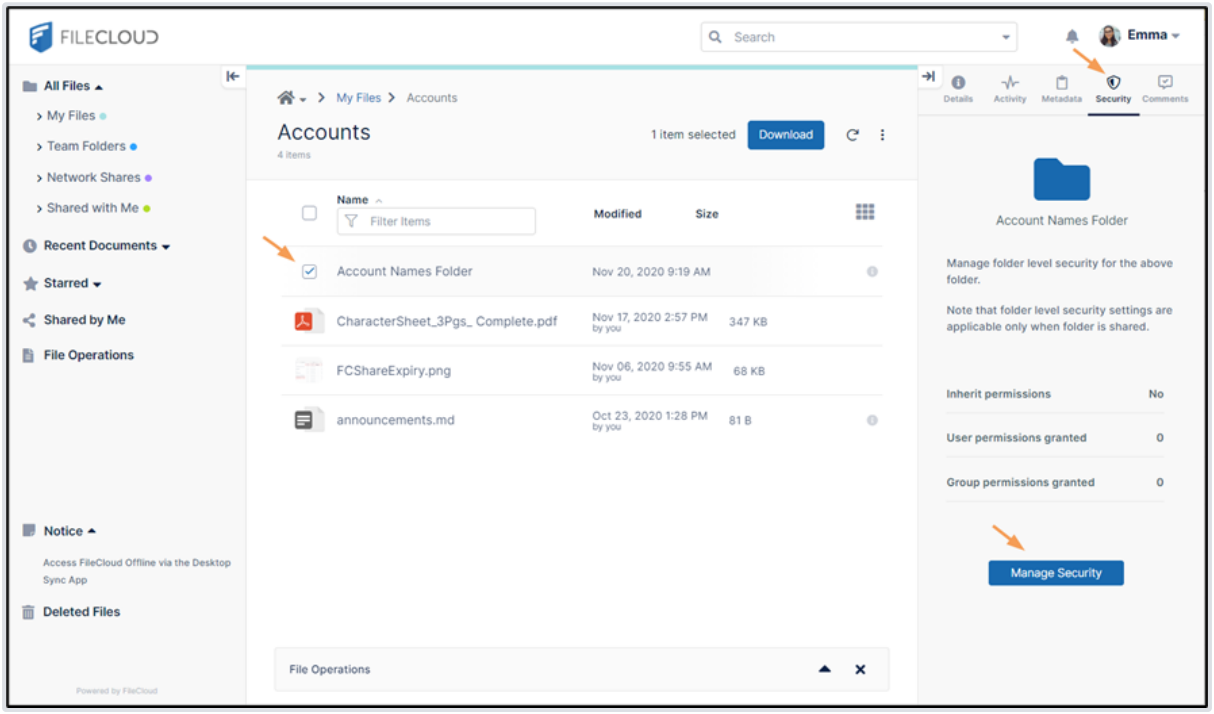


5. Click **Save**.

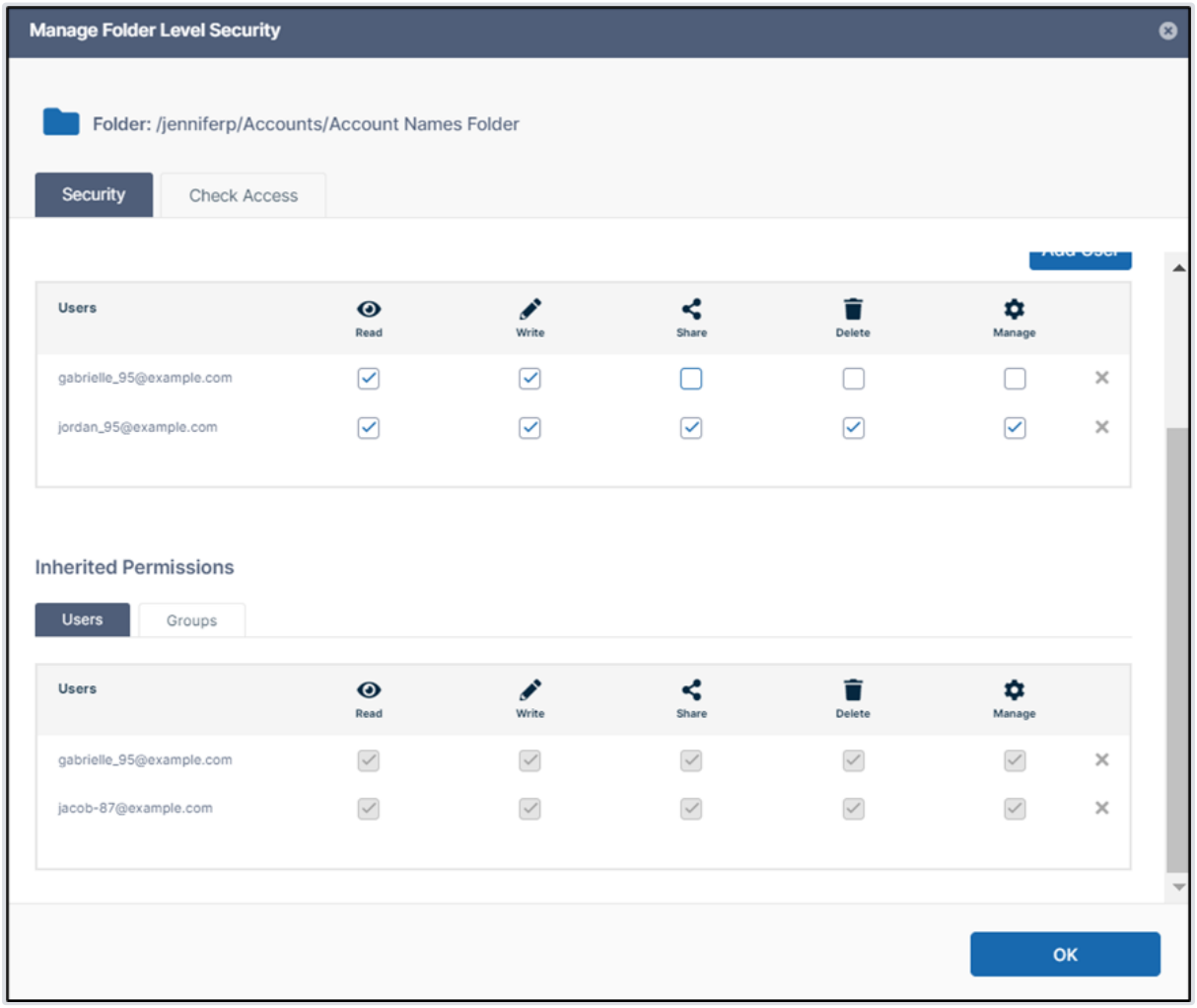
How a user sets folder permissions

How a user sets folder permissions

Once a user is permitted to set folder-level permissions, they can select a folder's checkbox and click the **Security** tab in the right panel. In the **Security** tab, the user clicks **Manage Security** to open the **Manage Folder Level Security** checkbox.



They can then add users and select one or more of the following folder-level permissions:



Permission	Description
Read	• Allows Downloading Files • Allows Previewing Files
Write	• Allows uploading and modifying existing files • Allows creating files and folders • Allows renaming files and folders
Delete	• Allows deleting files and folders
Share	• Allows sharing files and folders
Manage	• Allow managing folder-level permissions for this folder

See Set Permissions on Folders in the User Dashboard for more information.

Setting Folder-Level Permissions on Team Folders

Once a Team Folder is shared, all users with access to the share will see the folder in Team Folders in the navigation panel of the user portal and all FileCloud clients such as Sync, Drive, Outlook and the Office Add-In. A user's actions on a Team Folder are generally limited by the share permissions given to them on the Team Folder. However, additional limitations may be added to the share permissions for specific users and groups in the form of folder-level permissions.

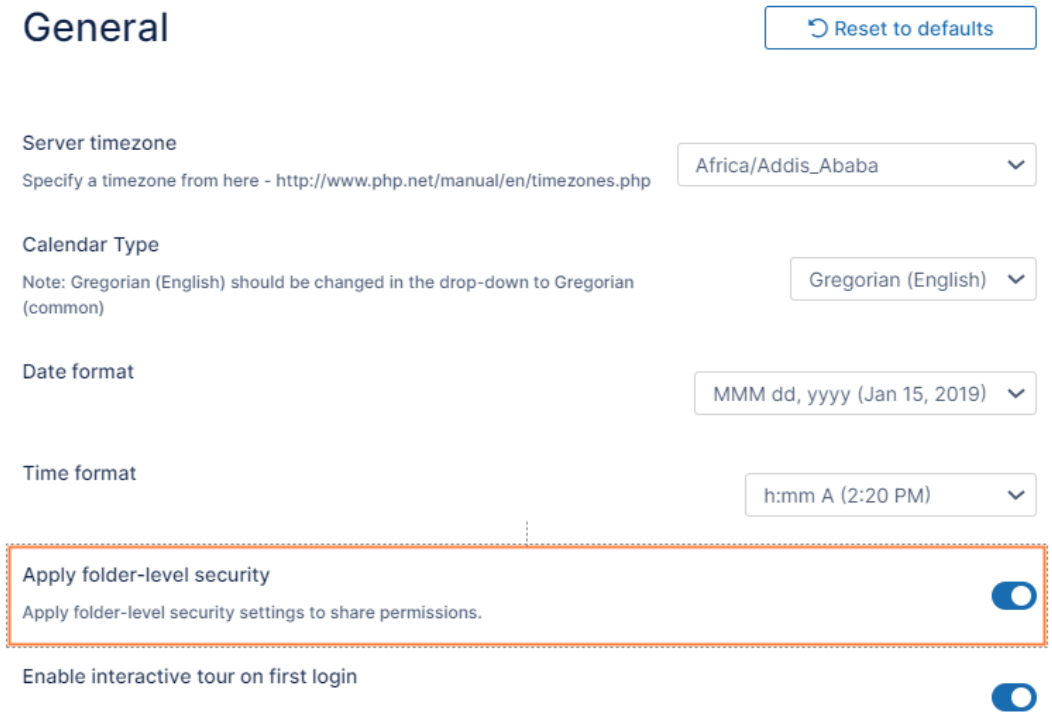
For more information on folder **share** permissions, read about the Private Share Permissions for Folders.

Enable folder-level permissions

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.

1. Enable **Apply folder-level security.**



Apply folder-level permissions to Team Folders:

You can apply folder-level permissions to the top-level Team Folder or to its subfolders.

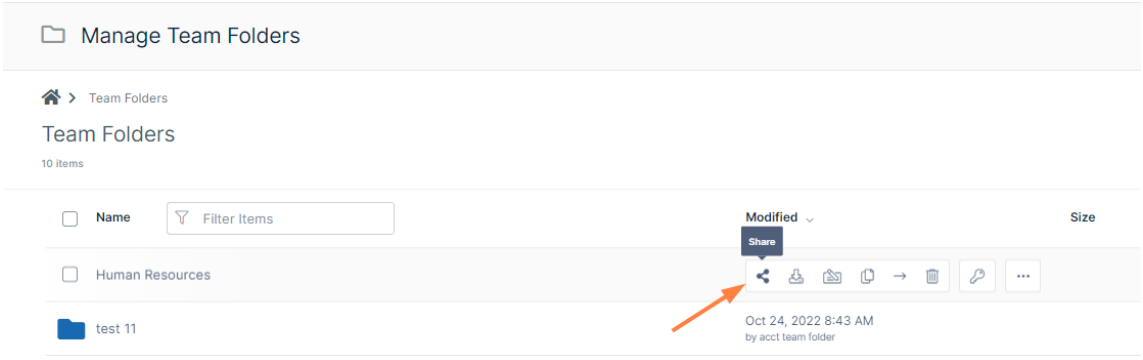
Here, we will demonstrate how folder-level permissions can be used to enhance share permissions on Team Folders through an example.

This example uses a common scenario, in which a top-level Team Folder stores various subfolders for the team. The entire team is given access to some of the subfolders, for example, those that contain general information. But only team members whose jobs require more secure information, such as employee ID numbers, are given access to the subfolders that contain that information.

In this example, we will give the entire **Human Resources** team access to the **HR Files** subfolder, but we will only give the users **HR Manager** and **Jessica** access to the **Employee Records** and **Forms** subfolders.

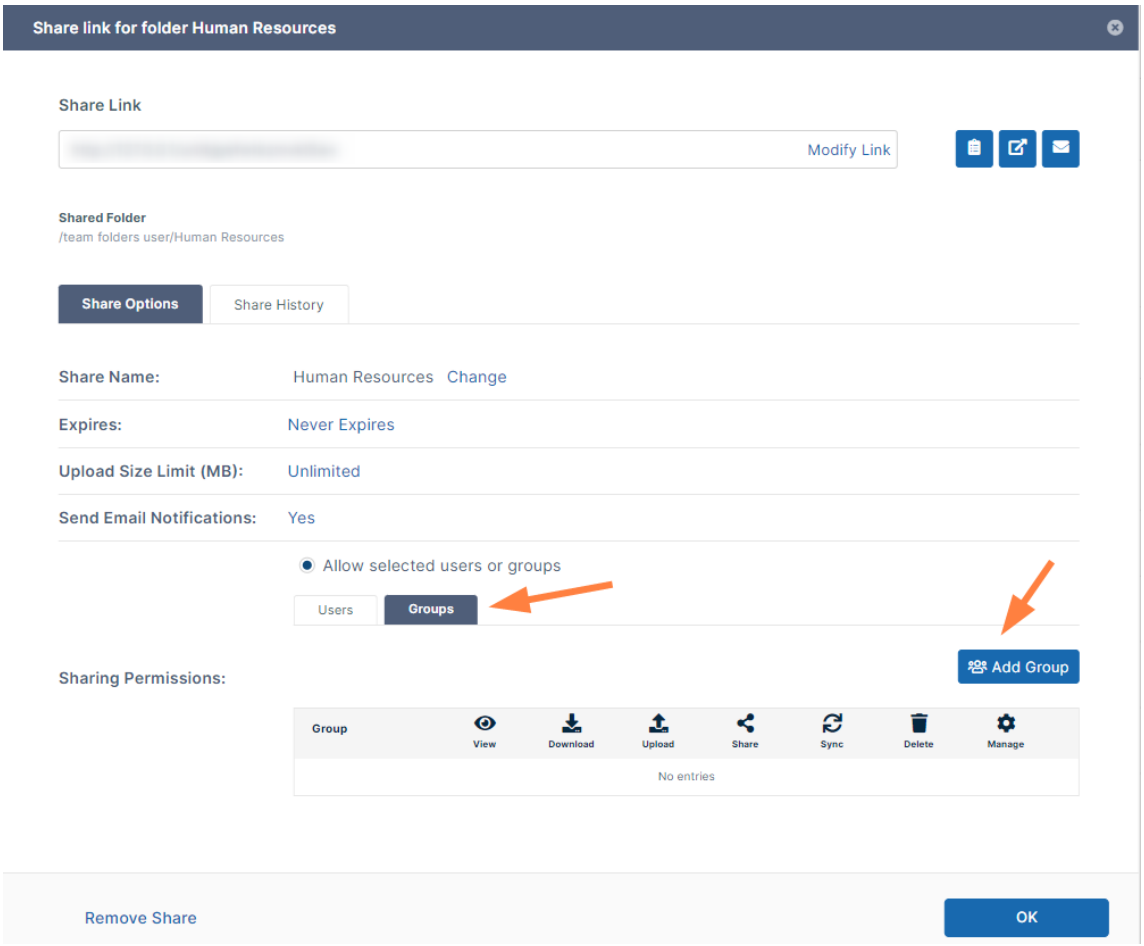
Share the top-level Team Folder with the entire group with all permissions

1. From the left navigation panel, click **Team Folders**.
2. Hover over the Team Folder (in this case **Human Resources**), and click the share icon.



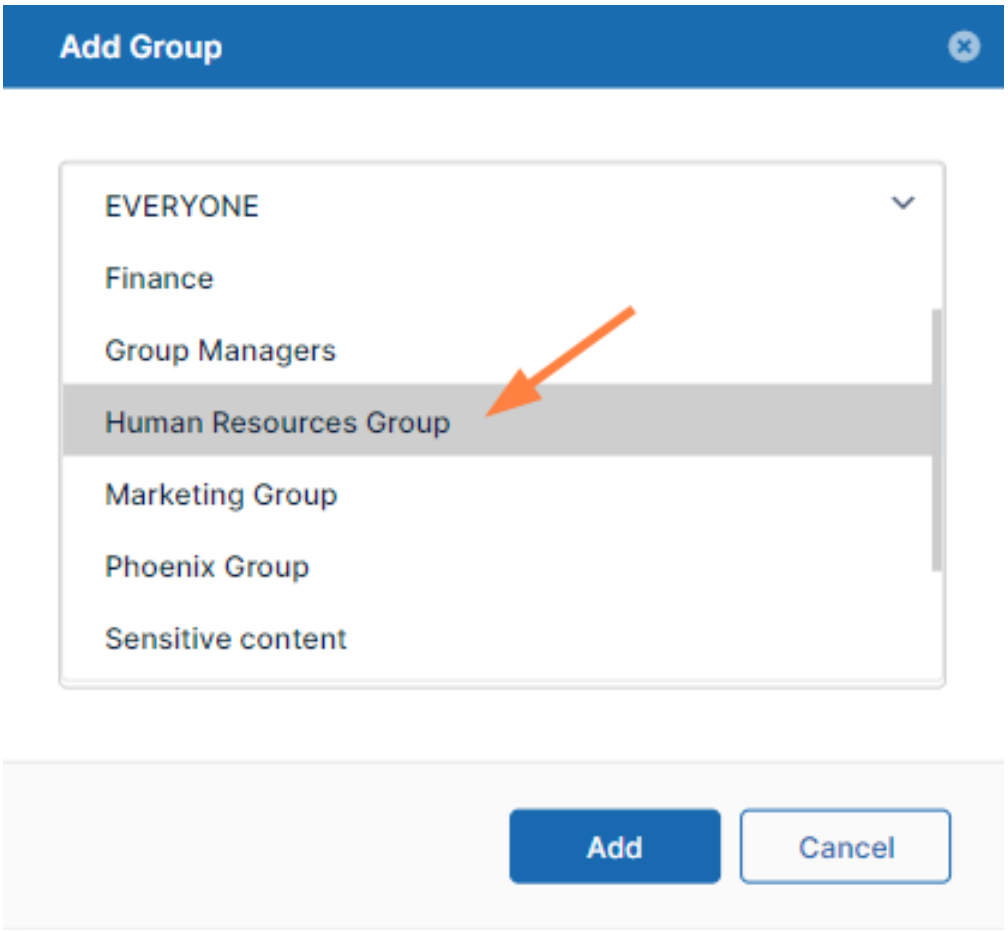
A **Share link for folder** dialog box opens.
First give the entire **Human Resources Group** access to the **Human Resources** folder.

3. Click **Allow selected users or groups,** and then click the **Groups** tab.
4. Click **Add Group**.

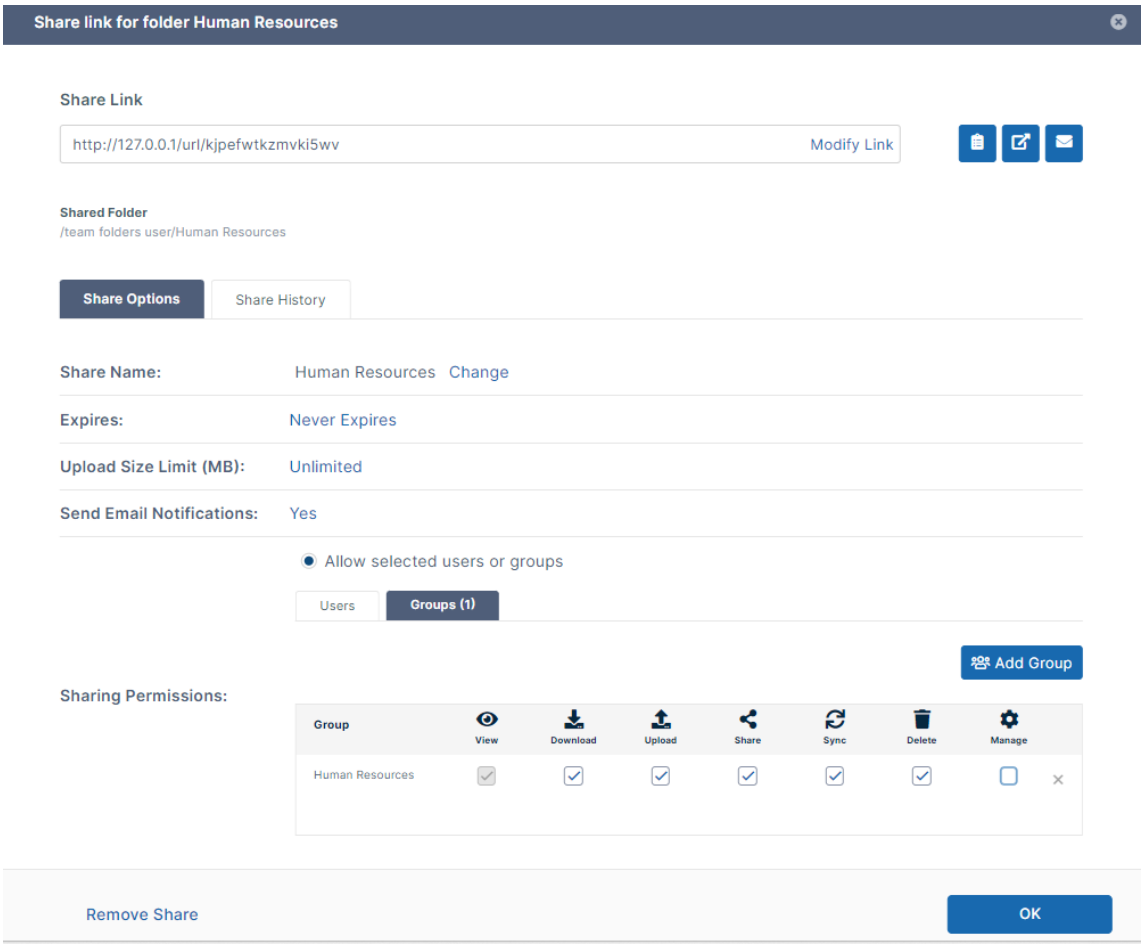


An **Add Group** dialog box listing your FileCloud groups opens.

5. Select the group (**Human Resources Group**) that you want to give access to the Team Folder and click **Add**.



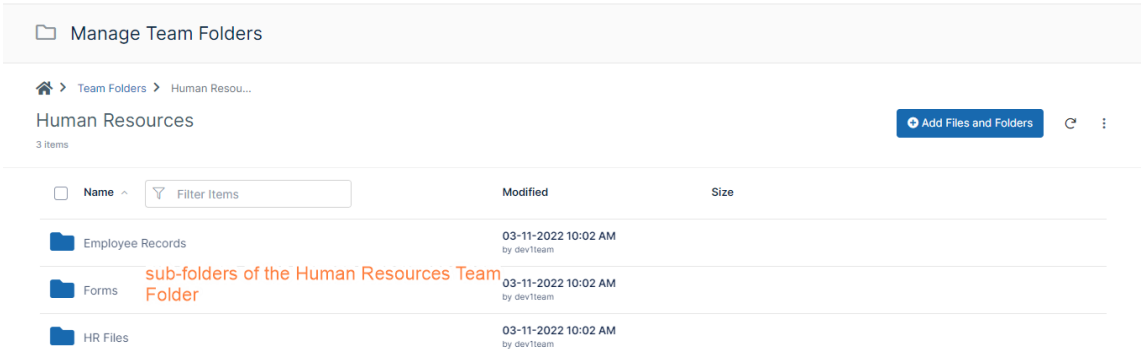
6. Enable all permissions to the folder for the group except **Manage** permission, which is not allowed for a group.



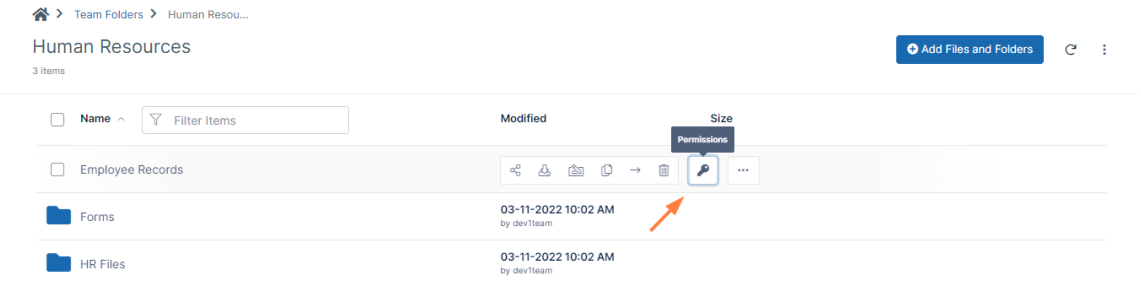
7. Click **OK** and close the dialog box.

Restrict permissions to specific users within the group

1. Open the Human Resources folder to view its subfolders.

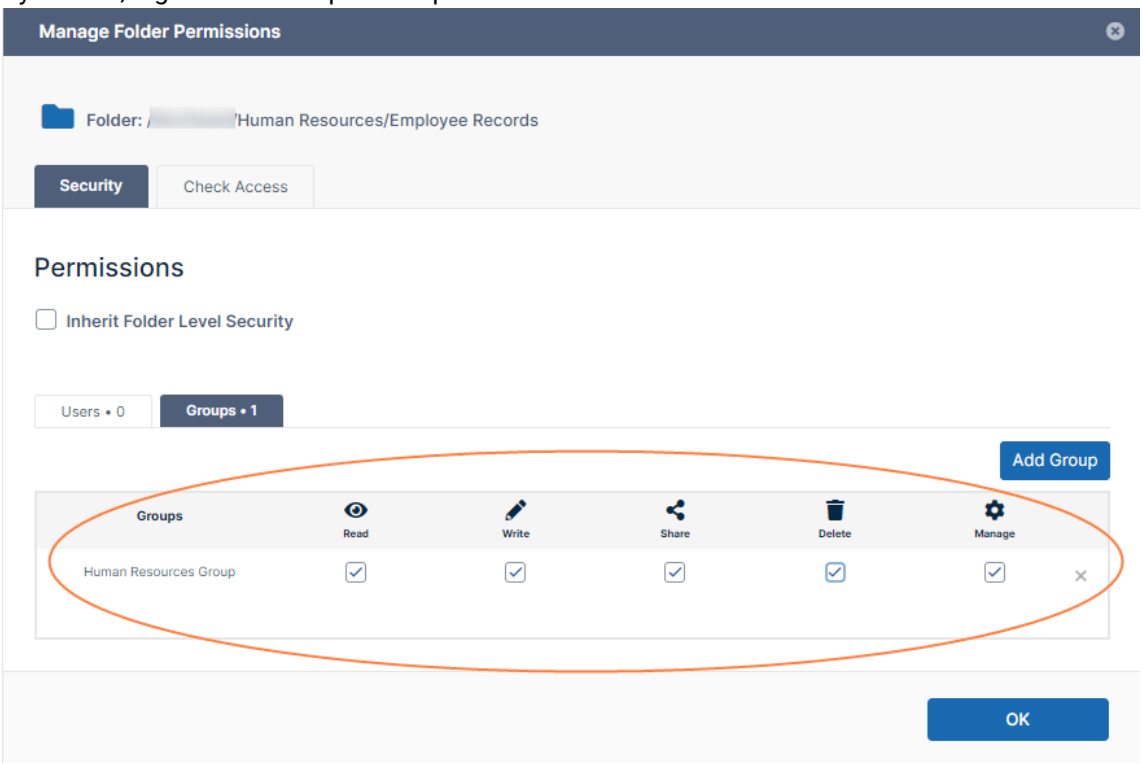


2. We want to give the users **HR Manager** and **Jessica** full access to the **Employee Records** and **Forms** subfolders. We don't want to give the other members of the team any access to these subfolders, but they will still have access to the **HR Files** folder.
3. Hover over the **Employee Records** folder and click the **Permissions** icon.

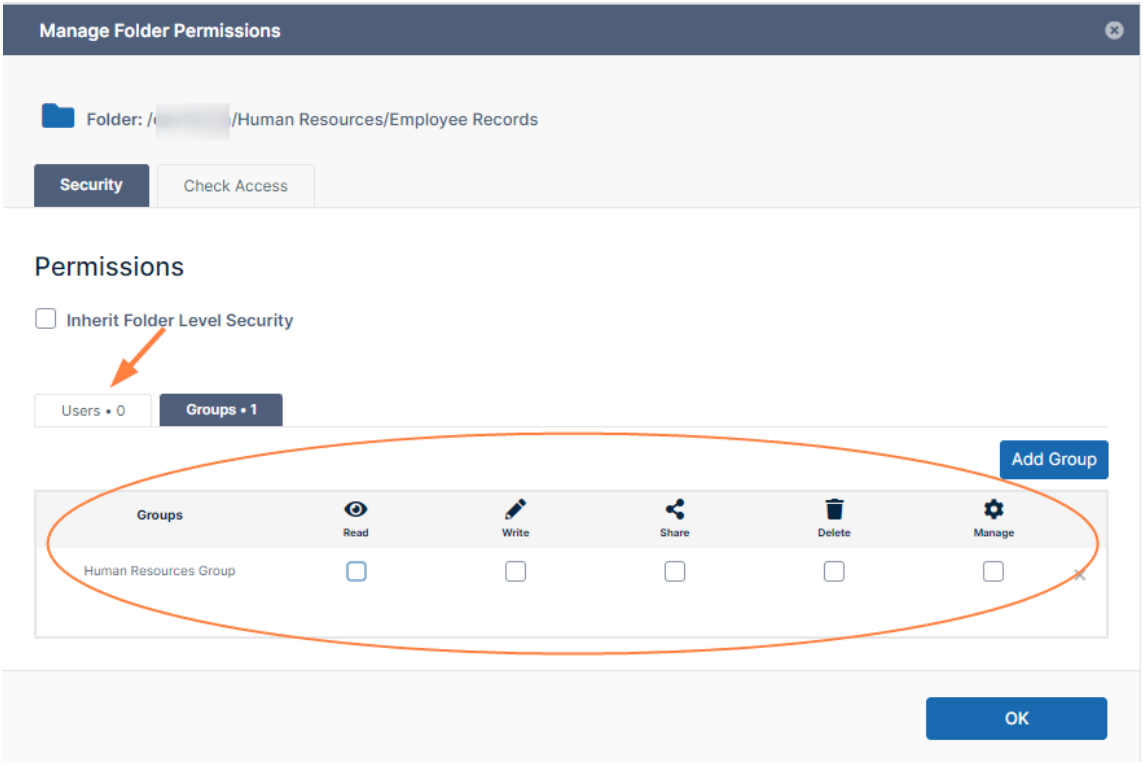


The **Manage Folder Level Security** dialog box opens for the **Employee Records** subfolder.

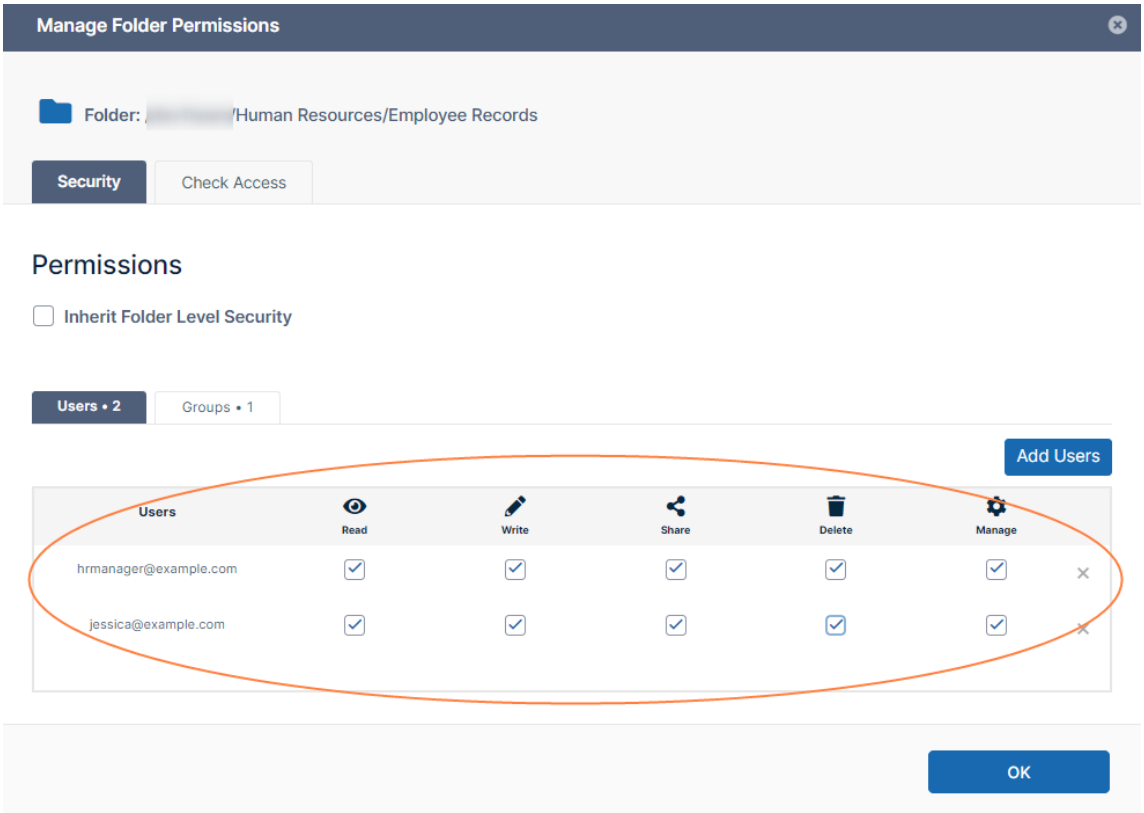
4. Uncheck **Inherit Folder Level Security**.
5. Click the **Groups** tab, then click the **Add Group** button and add **Human Resources Group**. By default, it grants all file operation permissions.



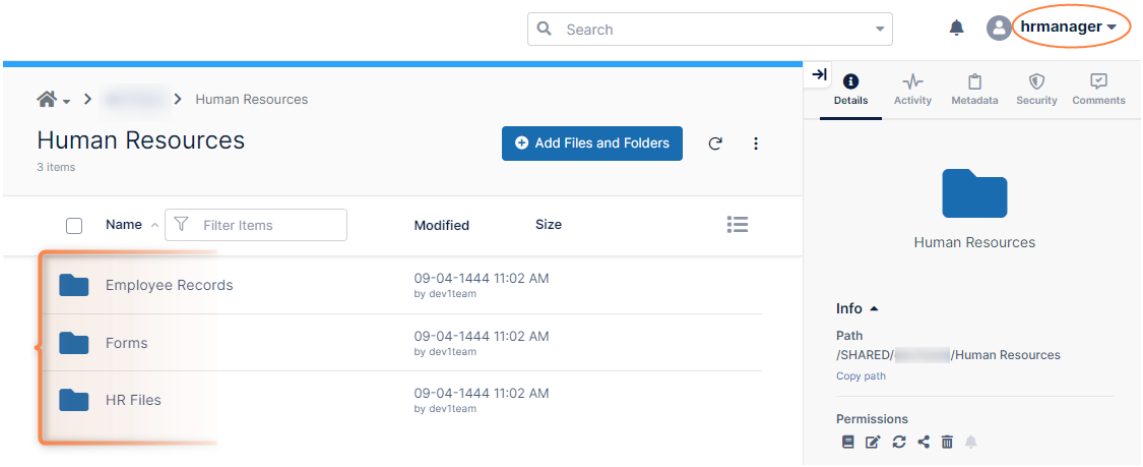
6. To disable the group's access to the **Employee Records** folder, uncheck the boxes under the operations.
7. Then click the **Users** tab.



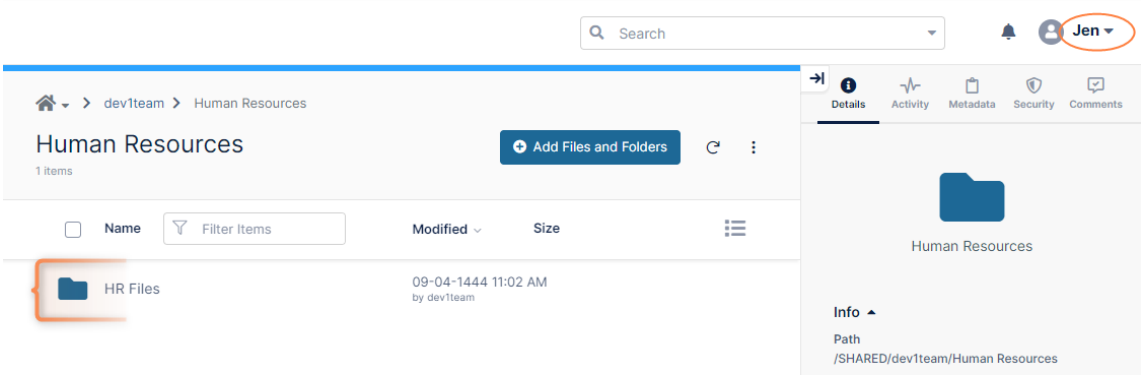
8. Click **Add Users** and add only the users who you want to give access to the **Employee Records** folder.



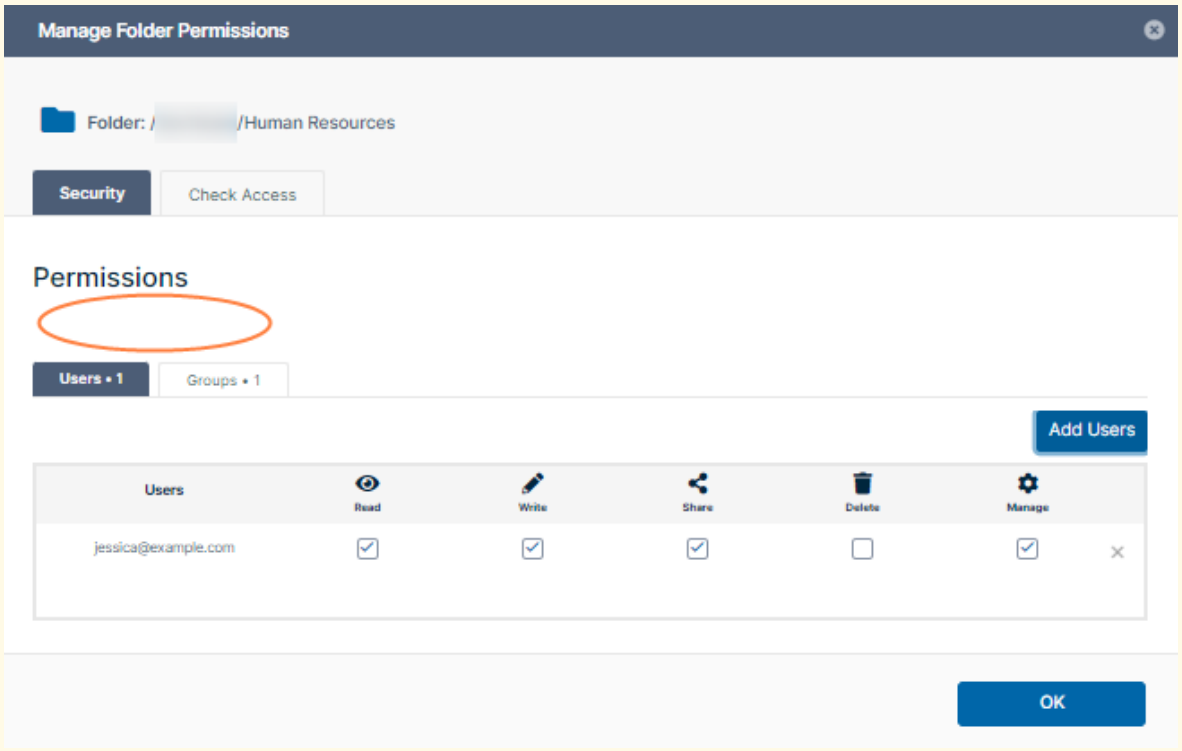
9. Repeat steps 3 through 8 for the **Forms** folder.
   Now, when either **HR Manager** or **Jessica** logs in to the user portal, they see the **Human Resources** Team Folder and all of its subfolders: **Employee Records**, **HR Files**, and **Forms**.



When another member of the **Human Resources** group logs in, they see the **Human Resources** Team Folder, but only the **HR Files** subfolder:



Note: Top-level Team Folder permissions cannot be inherited, and the **Inherit Folder Level Security** checkbox does not appear for top-level Team Folders on the **Manage Folder Level Security** dialog box.



Checking Effective Permissions

A user may have been assigned multiple types of permissions for a Team Folder. For example, the Team Folder shared with the user gave the user certain permissions but you may also have applied different folder-level permissions to the folder. In addition, the user may have permissions through a group it belongs to.

You can check the Team Folder's effective permissions to see the actual permissions the user has to the folder when all of these permissions are combined.

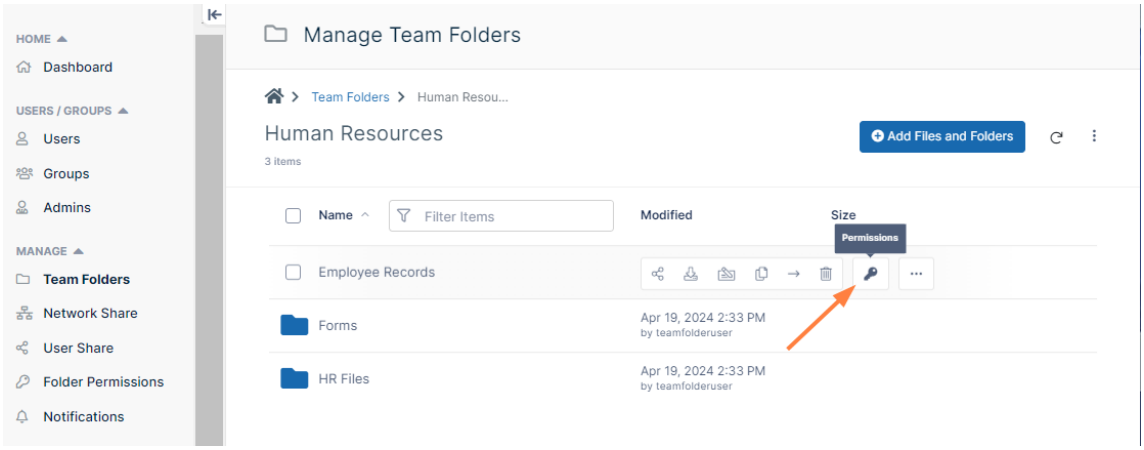
Effective permissions take into account that:

- If a user has both share and folder-level permissions to a folder, the more restrictive of the two apply.
- If a user has folder-level permissions assigned to them individually, and folder-level permissions assigned through a group they belong to, the user assigned permissions take precedence.

To check effective Team Folder permissions:

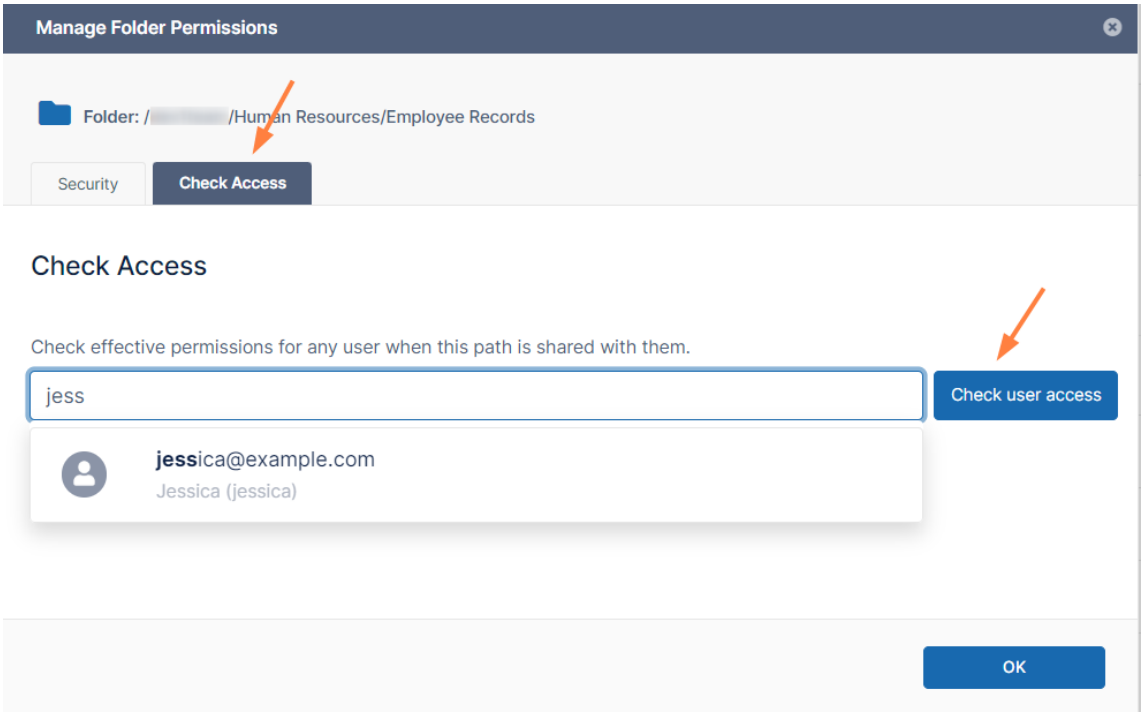
In this example, we'll check the effective permissions for the example above.

1. Navigate to the Human Resources/Employee Records Team Folder and click the permissions icon (the Key icon) in its row.



The **Manage Folder Level Security** dialog box opens with the **Security** tab selected.

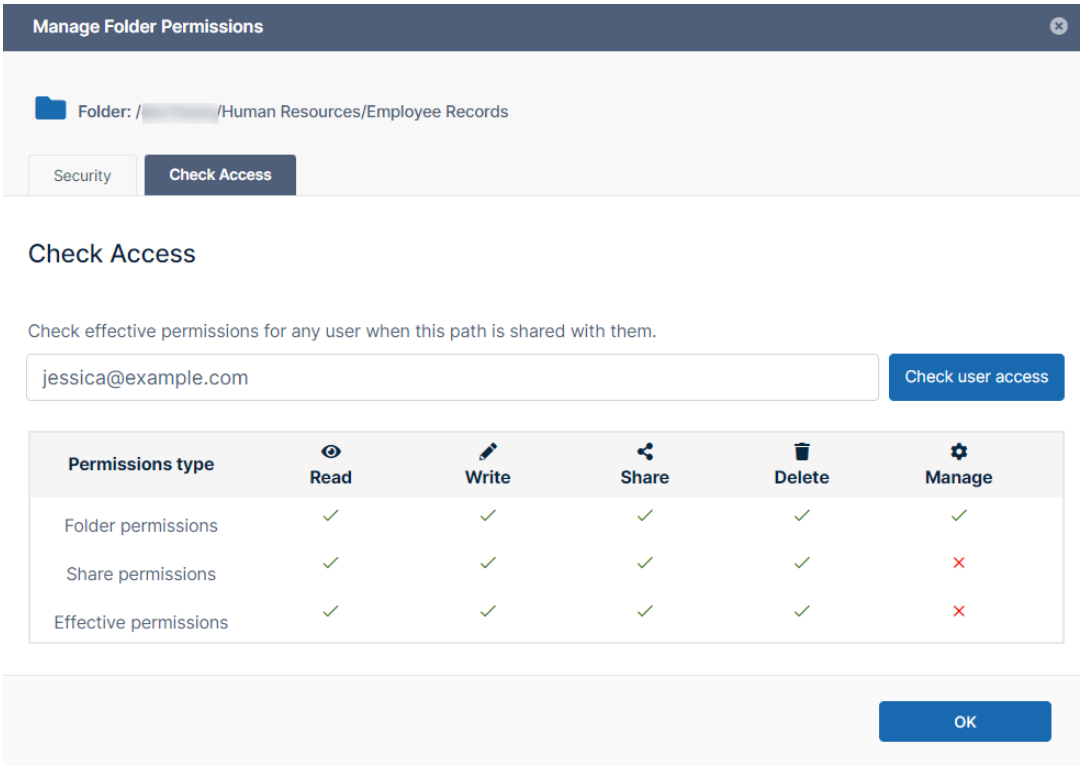
2. Click the **Check Access** tab.
3. Enter the email or username for Jessica, one of the users we gave folder-level permissions to this folder.
4. Click **Check user access**.



The dialog box lists Jessica's permissions.

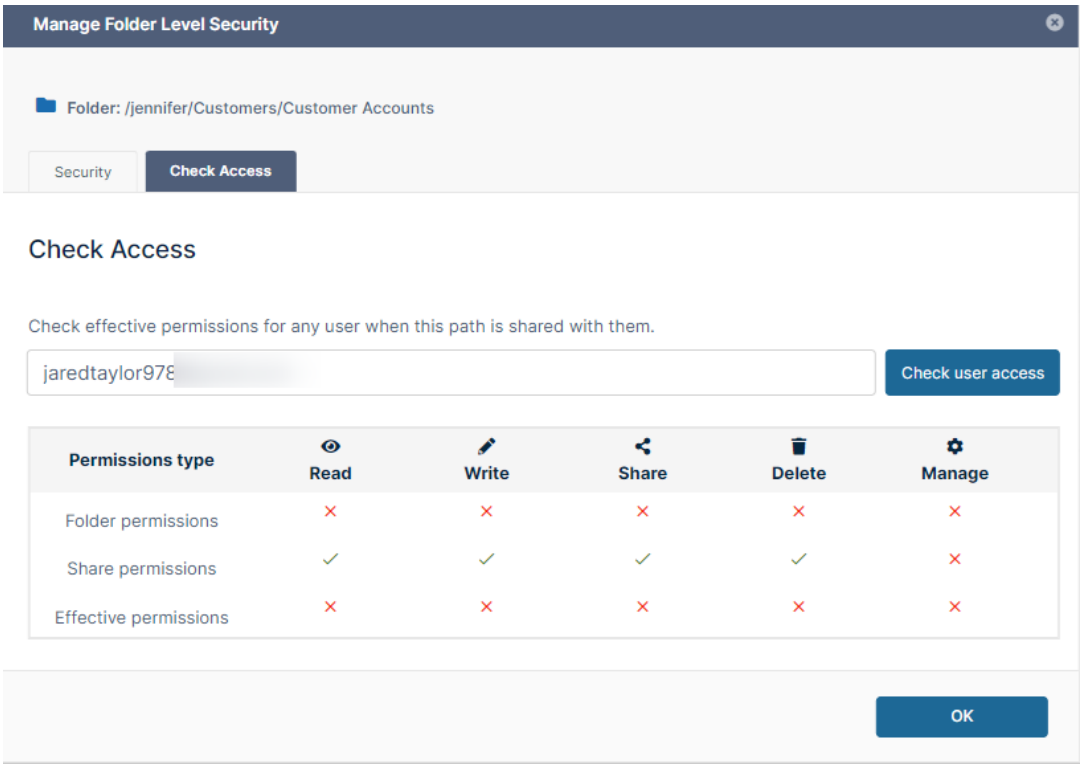
- The **Folder Permissions** row shows that she has all folder-level permissions to the Employee Records folder.
- In the share of the folder, Jessica's group, **Human Resources**, was given all but Manage permissions for the folder, which is shown in the **Share permissions** row.

- The more restrictive of folder-level or share permissions apply, so the **Effective permissions** row shows that ultimately, Jessica does not have Manage permission because she does not have it in the share.



Now let's look at the effective permissions for Aliya, another user in the **Human Resources** group who has not been given any user folder-level permissions to the **Employee Records** folder. Her group has had all folder-level permissions for the Human Resources folder removed.

- The **Folder permissions** row shows that she has no folder-level permissions for accessing the folder.
- On the share of the folder, her group is given read, write, share, and delete permissions, so the **Share permissions** row shows those permissions.
- The combined permissions, which appear in the **Effective permissions** row, show that Aliya has no access to the folder, because her group has both folder-level and share permissions assigned, and in this case the most restrictive apply.



More Information:

FileCloud Blogs
• Using "Allow Manage" on FileCloud Team Folders • User-Based Management of Team Folder Permissions

How Folder-Level Permissions and Share Permissions Work Together

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
  - Subfolders inherit the folder-level permissions of their immediate parent folders.
  - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.

- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

The following examples illustrate the above permission rules using these components:

Group: **Sales Group** **Members:** **SalesUser1** **SalesUser2**	**Folder:** **Accounts** **Subfolder:** **MillerAcct**

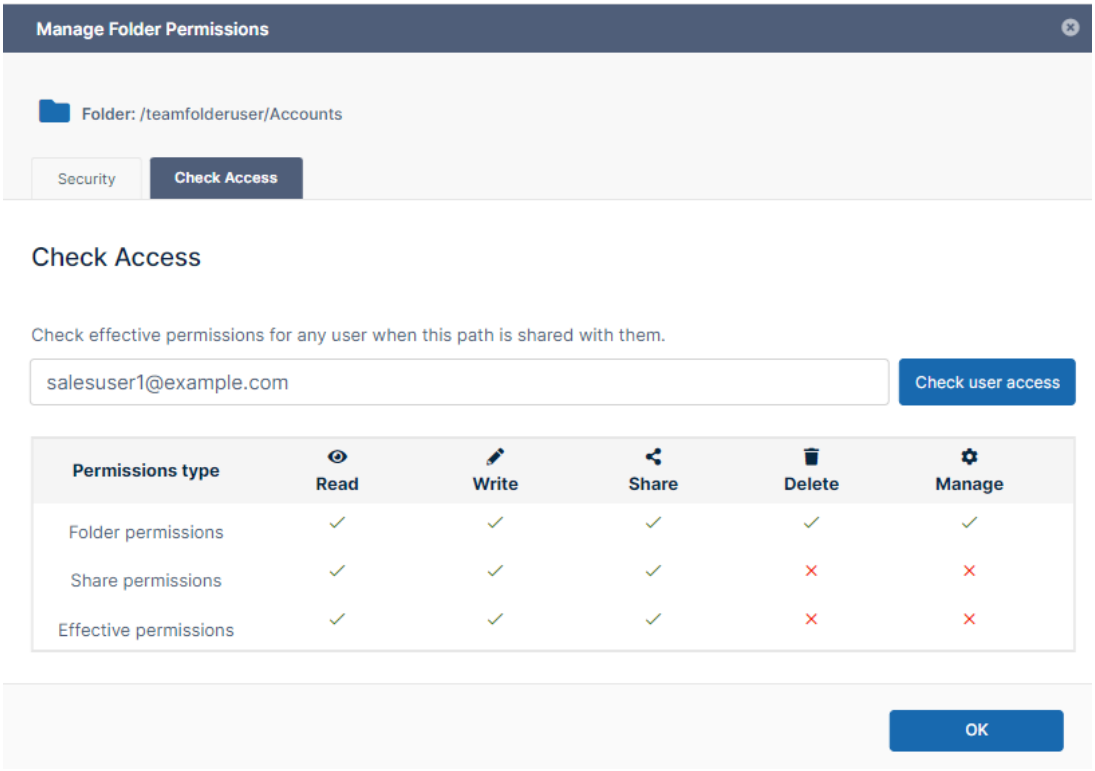
Example 1:
The more restrictive of folder-level and share permissions apply.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **Accounts** are **read**, **write**, and **share**.



	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
	EFFECTIVE	SalesUser1	Y	Y	Y		



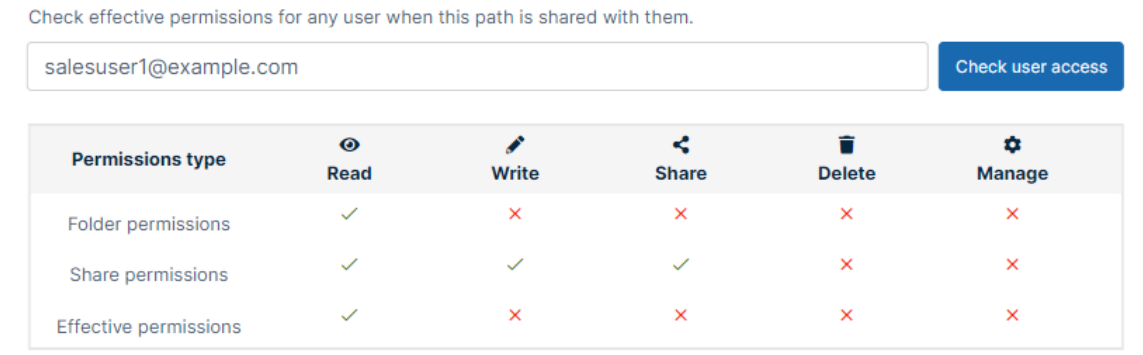
Example 2:

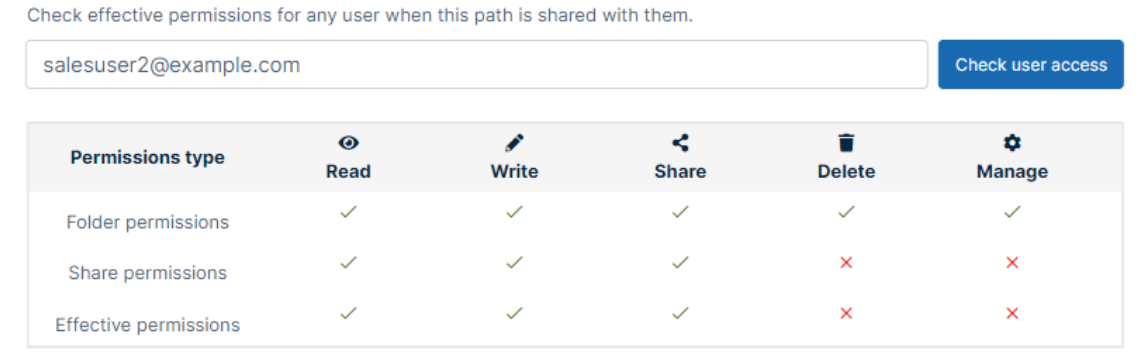
The more restrictive of folder-level and share permissions apply.
User folder-level permissions supersede group folder-level permissions.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1** is given **read** folder-level permission to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permission to the Team Folder **Accounts** is **read**.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **Accounts** are **read, write, and share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1	Y				
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE	SalesUser1	Y				
		SalesUser2	Y	Y	Y		





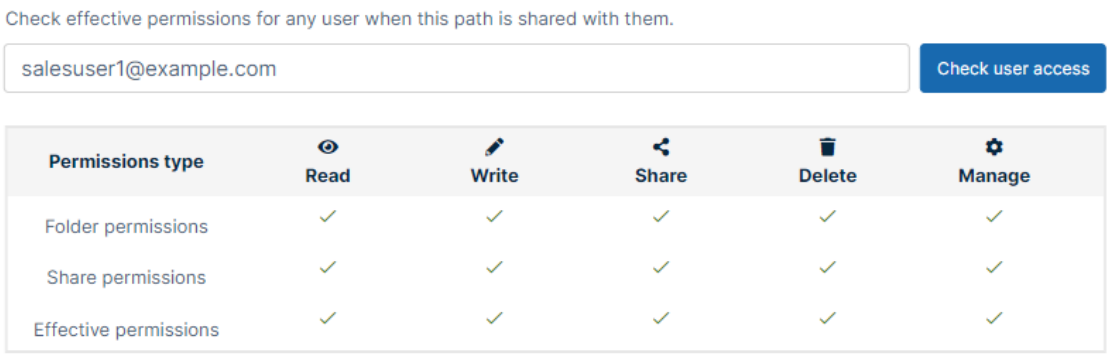
Example 3:

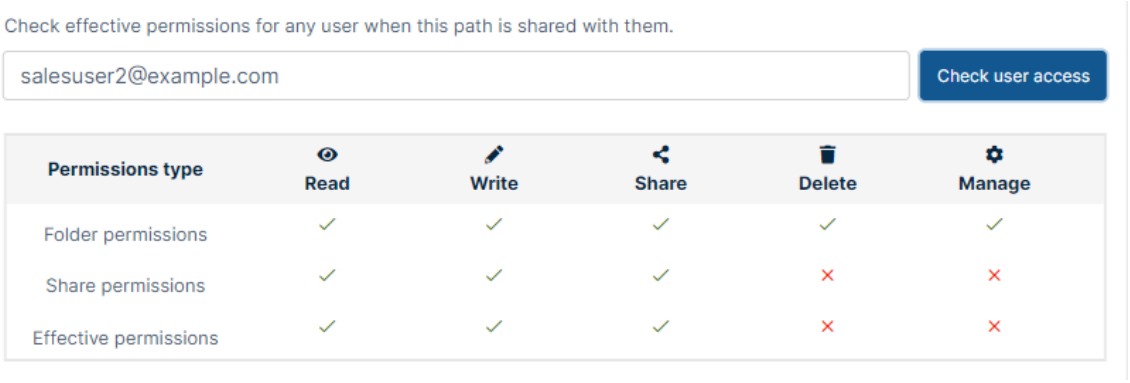
The more restrictive of folder-level and share permissions apply.
In a share, greatest share permissions given to a user or the user's group apply.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1** has **all** share permissions to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **Accounts** are **all** permissions.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **Accounts** are **read**, **write**, and **share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1	Y	Y	Y	Y	Y
		SalesUser2					
	EFFECTIVE	SalesUser1	Y	Y	Y	Y	Y
		SalesUser2	Y	Y	Y		





Example 4:

By default, subfolders inherit the permissions of their parent folders.
User folder-level permissions supersede group folder-level permissions.

View the example

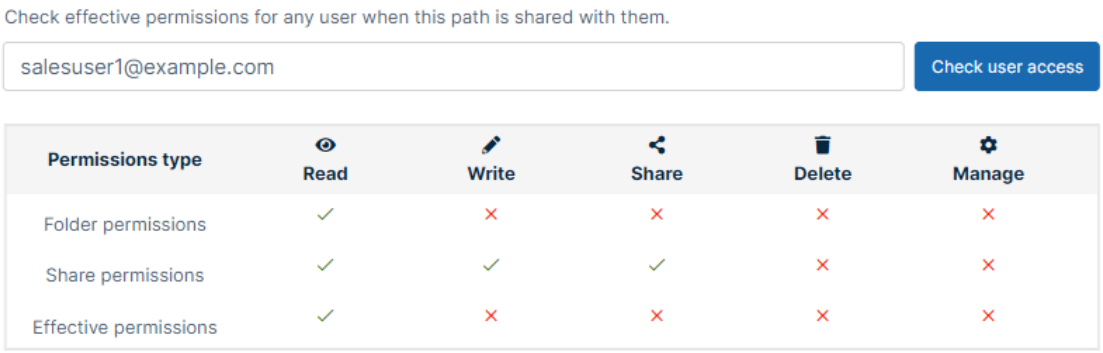
- The **Sales Group** is given the folder-level permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.

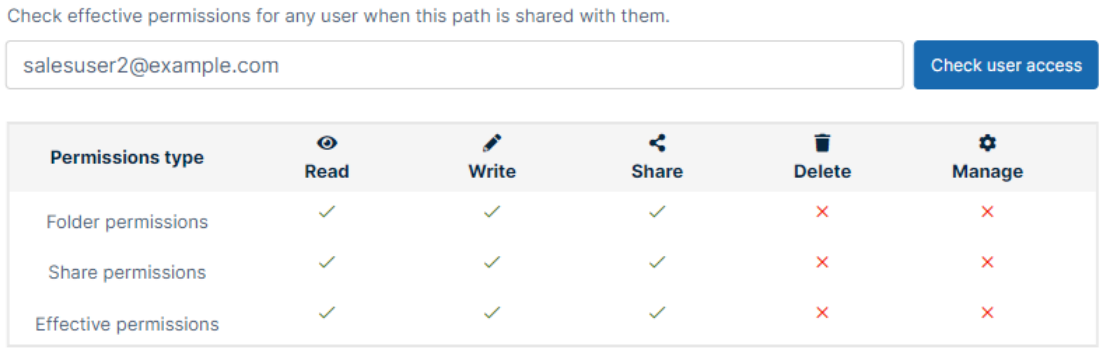
- The Team Folder **MillerAcct** inherits the permissions from the Team Folder **Accounts**.
- **SalesUser1** is given the folder-permission read to the Team Folder **MillerAcct**.
- **SalesUser1**'s effective (actual) permission to the Team Folder **MillerAcct** is **read** permission.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts Folder	ACL	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE	SalesUser1	Y	Y	Y		
		SalesUser2	Y	Y	Y		

Inherited by

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
MillerAcct	ACL	Sales Group	Y	Y	Y		
		SalesUser1	Y				
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE	SalesUser1	Y				
		SalesUser2	Y	Y	Y		



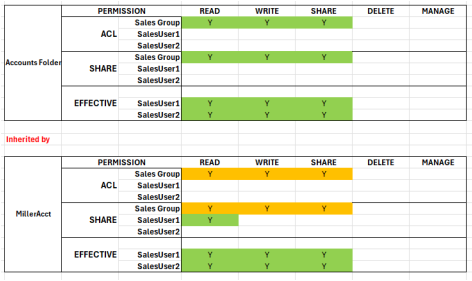


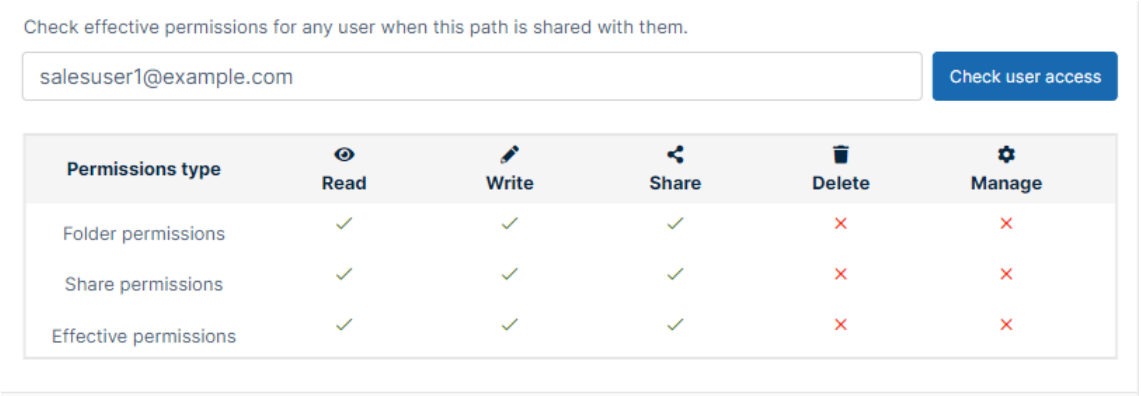
Example 5:
By default, subfolders inherit the permissions of their parent folders.
In a share, greatest share permissions given to a user or the user's group apply.

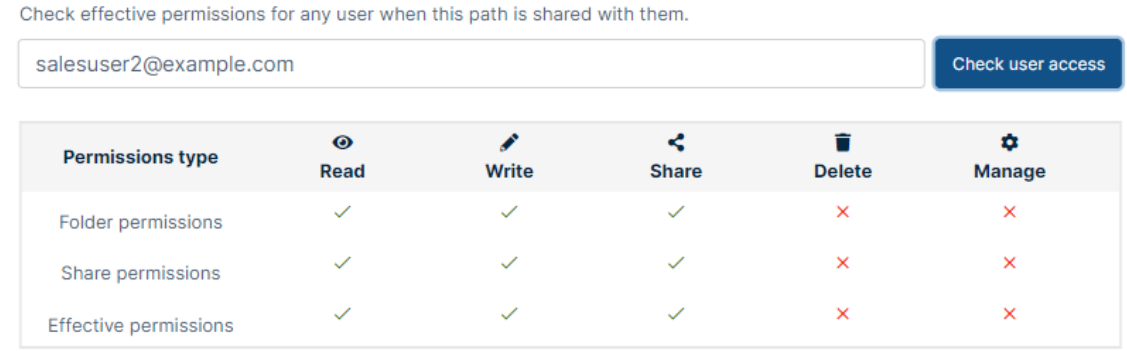
View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- The Team Folder **MillerAcct** inherits the permissions from the Team Folder **Accounts**.

- **SalesUser1** is given the share permission read to the Team Folder **MillerAcct**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share** permission.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share** permission.







How folder permissions affect copy and move actions

In some cases, combined share and folder-level permissions on folders limit whether **copy** and **move** for files or folders and **copy file or folder** and **move file or folder** in automated (user) workflows are permitted. In the scenarios in the following table, copy and move or move only is not allowed, and if you attempt to perform the action an error message is returned.

1	View	-	NOT allowed	NOT allowed
2	View+Download	-	allowed	NOT allowed
3	View	Read	NOT allowed	NOT allowed
4	View+Download	Read	allowed	NOT allowed

More Examples

Scenario 1: Give folder permissions only to specific users or groups

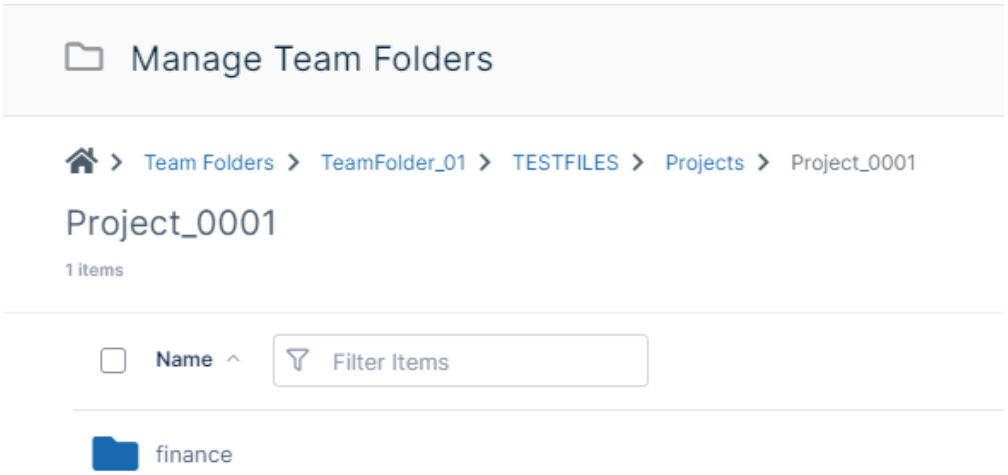
In this scenario, an administrator gives two groups access to a folder, but only gives one group access to one of its subfolders.

Example of giving permissions to only specific users or groups

In this example, the folder **TeamFolder_01** is only shared with the groups:

- **ProjectManagers**
- **ProjectTeam**

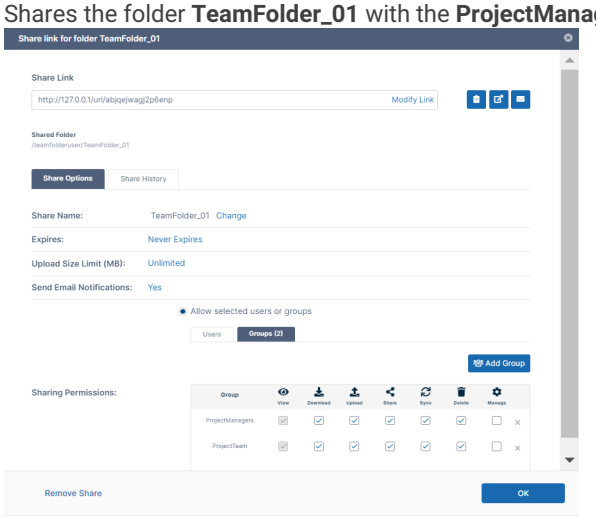
Only the group **ProjectManagers** is given access to the embedded subfolder **Project_0001/finance.**



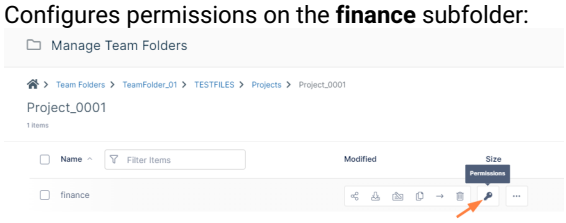
Example of giving permissions to only specific users or groups

To accomplish this, the administrator:

1. Shares the folder **TeamFolder_01** with the **ProjectManagers** and **ProjectTeam** groups only.

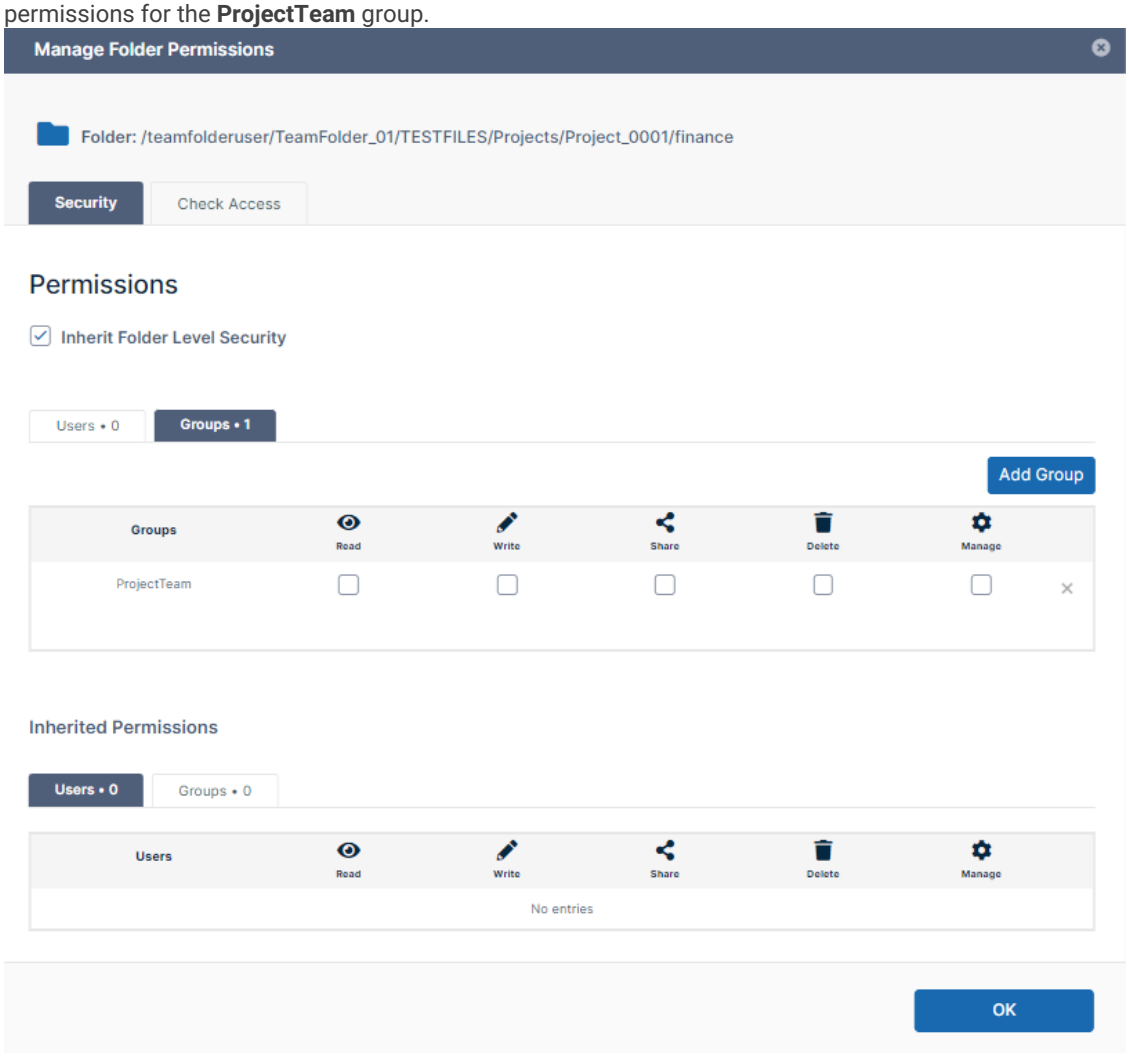


2. Configures permissions on the **finance** subfolder:



Example of giving permissions to only specific users or groups

3. Adds **ProjectTeam** group to the **finance** folder in **Manage Folder Permissions**. Then removes all permissions for the **ProjectTeam** group.

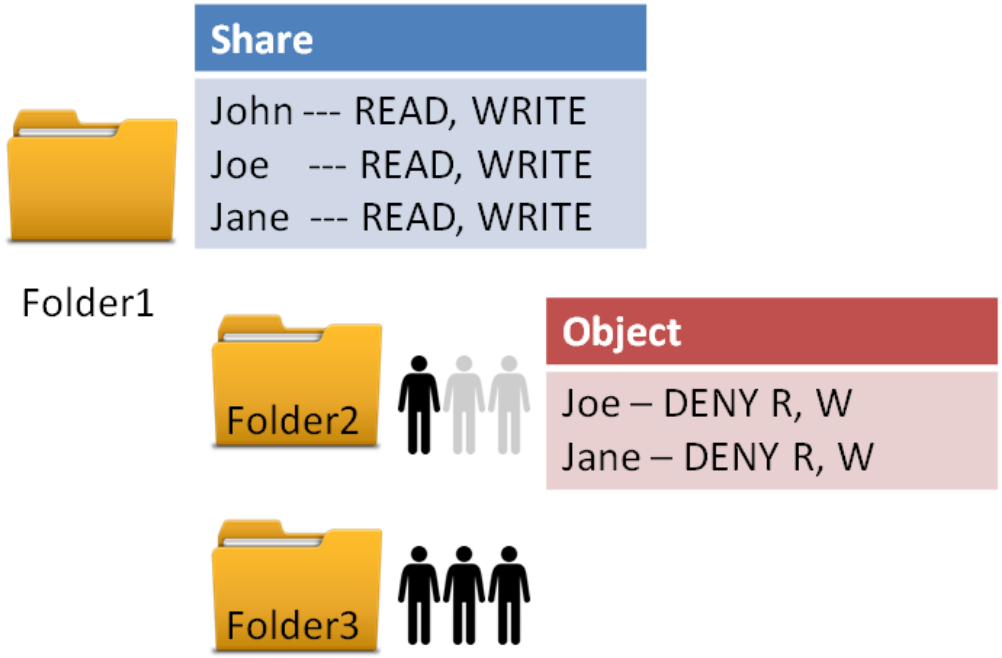


Now, members of the **ProjectManagers** group are able to access the finance folder, but members of the **ProjectTeam** group are not.

Scenario 2: Remove access to specific folders for certain users

In this scenario, an administrator sets different permissions on parent and child folders.

Example of a Sharing Scenario



In this example, Folder1 is shared with Read and Write permissions to the following users:

- John
- Joe
- Jane

This means all three users can:

- Read files in Folder1
- Write files in Folder1

In this example, the administrator wants to allow only John access to the subfolder, Folder2.

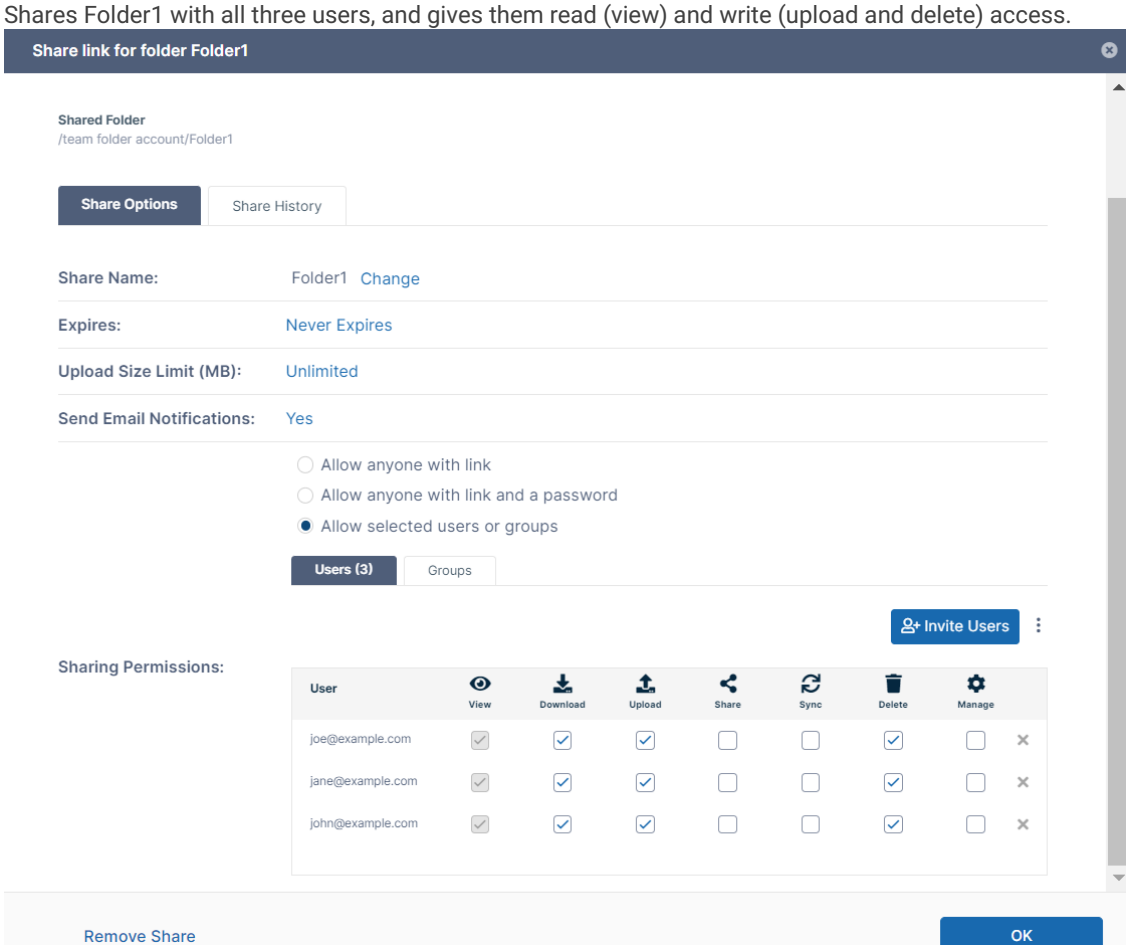
The administrator therefore wants the folder access to be the following:

- Folder1 - accessible to John, Joe, and Jane
- Folder2 - accessible to John
- Folder3 - accessible to John

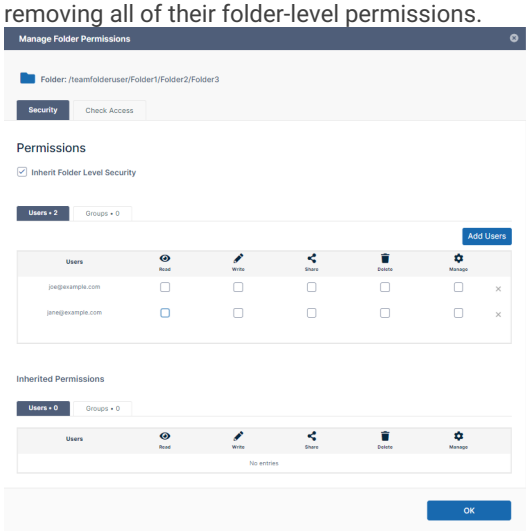
Example of a Sharing Scenario

To accomplish this, the administrator:

1. Shares Folder1 with all three users, and gives them read (view) and write (upload and delete) access.



2. Removes folder-level security permissions for the two users who will not have access to Folder2 removing all of their folder-level permissions.



When John, Joe, and Jane access the folders:

Example of a Sharing Scenario

User	Folder1	Folder2	Folder3
John	✅ See it listed ✅ Access its content	✅ See it listed ✅ Access its content	✅ See it listed ✅ Access its content
Joe	✅ See it listed ✅ Access its content	❌ See it listed ❌ Access its content	❌ See it listed ❌ Access its content
Jane	✅ See it listed ✅ Access its content	❌ See it listed ❌ Access its content	❌ See it listed ❌ Access its content

Team Folders

The ability to upload files by dragging and dropping them from file explorer or another application onto a Team Folder is available in FileCloud version 22.1 and later.

As an administrator, you may be asked to manage folders that are shared to allow for collaboration among certain users or groups in your company.

- In FileCloud, these folders are called Team Folders.
- Team folders provide a single place where teams in a company can store and organize files and folders.
- Team folders are normally created by admins or authorized users and instantly made available to all members of a team.

Team Folders use managed storage and are not available for network storage. Therefore, Team Folders are created on managed storage where all files and folders under Team Folders are stored.

How do Team Folders help administrators?

- **Centralized Content Management**: Team Folders facilitate organizing files and folders in a centralized place.
- **Easy Provisioning of Users, Files and Folders**: New users can be provisioned quickly with access to specific files and folders through Team Folders. Similarly, new files can be granted immediate access to all relevant users by uploading the file to the relevant Team Folder.
- **Granular Control of Folders:** Team Folders and their sub folders can give users granular permissions such as Read, Write, Share and Sync access.
- **Manage Selective Sync:** Admins can select specific Team Folders and enable or disable sync permissions on an easy to use user interface.

How can a size limit be placed on a Team Folder?

You can place a size limit on a Team Folder when you share it. You must share a Team Folder to give users and groups access to it. As with any shared folder, when you share a Team Folder, you can set an upload limit that applies to the total amount that can be uploaded to the folder. See Share the Team Folder and Set Permissions.

To Manage Team Folders

Set Up Team Folders	1. Configure the Team Folder Account. 2. Seed and Organize the Team Folder Data. 3. Share a Team Folder and Set Share Permissions for users and groups. 4. Set Granular Folder Permissions on Team Folders (Optional)
Manage Team Folders	Search for a Team Folder Recover Deleted Files View and Restore Previous Versions

Configure the Team Folders Account

As an administrator, you must enable Team Folders and set up a Team Folder account.

The Team Folder account is a system-designated FULL USER account.

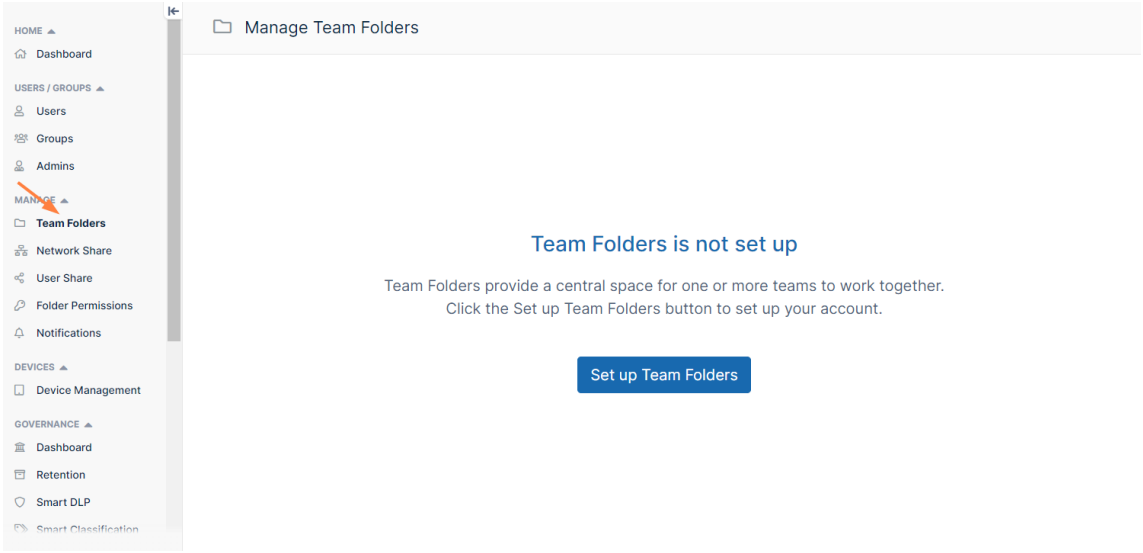
- FileCloud can create the account for you - you just need to choose the name you want to use.
- The Team Folder account is not counted towards your user license.
- FileCloud can also create an email account where it will send Team Folder notifications.
- The email address for Team Folder notifications should take the form of <newalias@mycompany.com>.
- Alternatively, you can promote a user account currently used for company-wide communication as the Team Folder account.

To allow FileCloud to create the Team Folders account

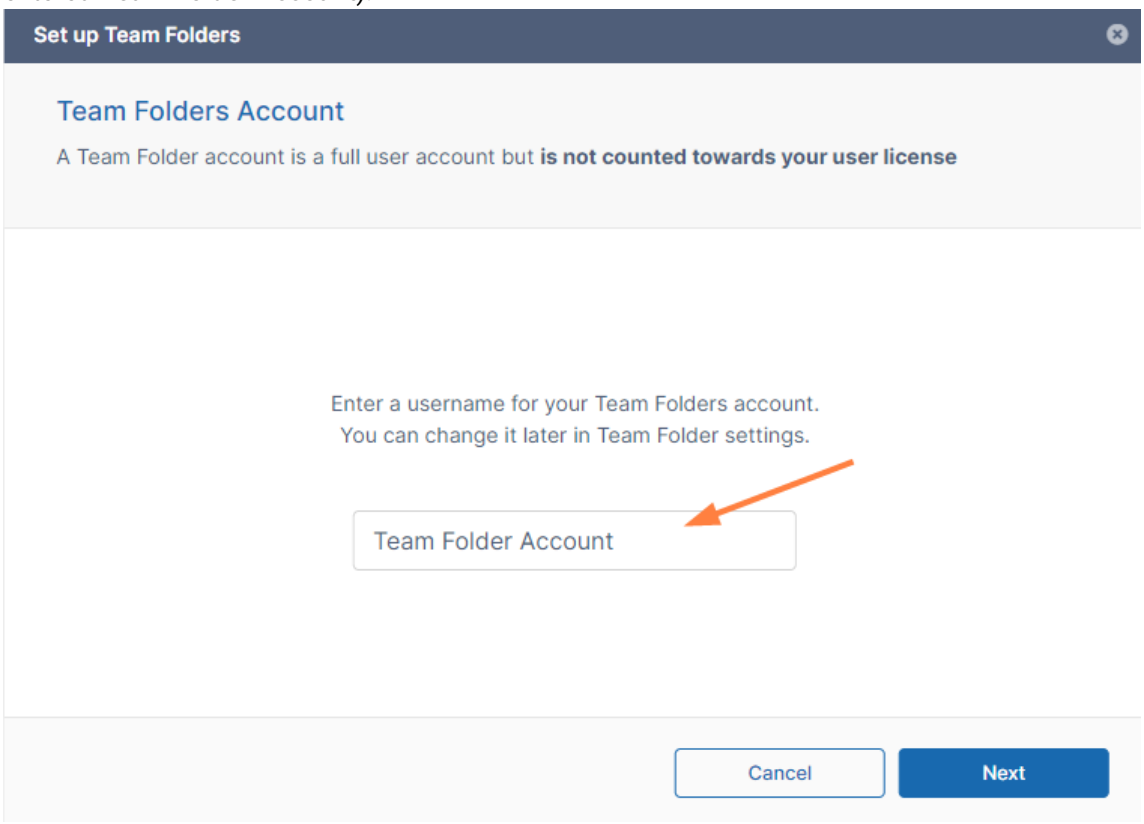
Choose one of the following options:

Create a new account through the Team Folders screen

1. In the admin portal's navigation pane, click **Team Folders**.
   The screen tells you Team Folders is not set up, and it provides you with a **Set up Team Folders** button.

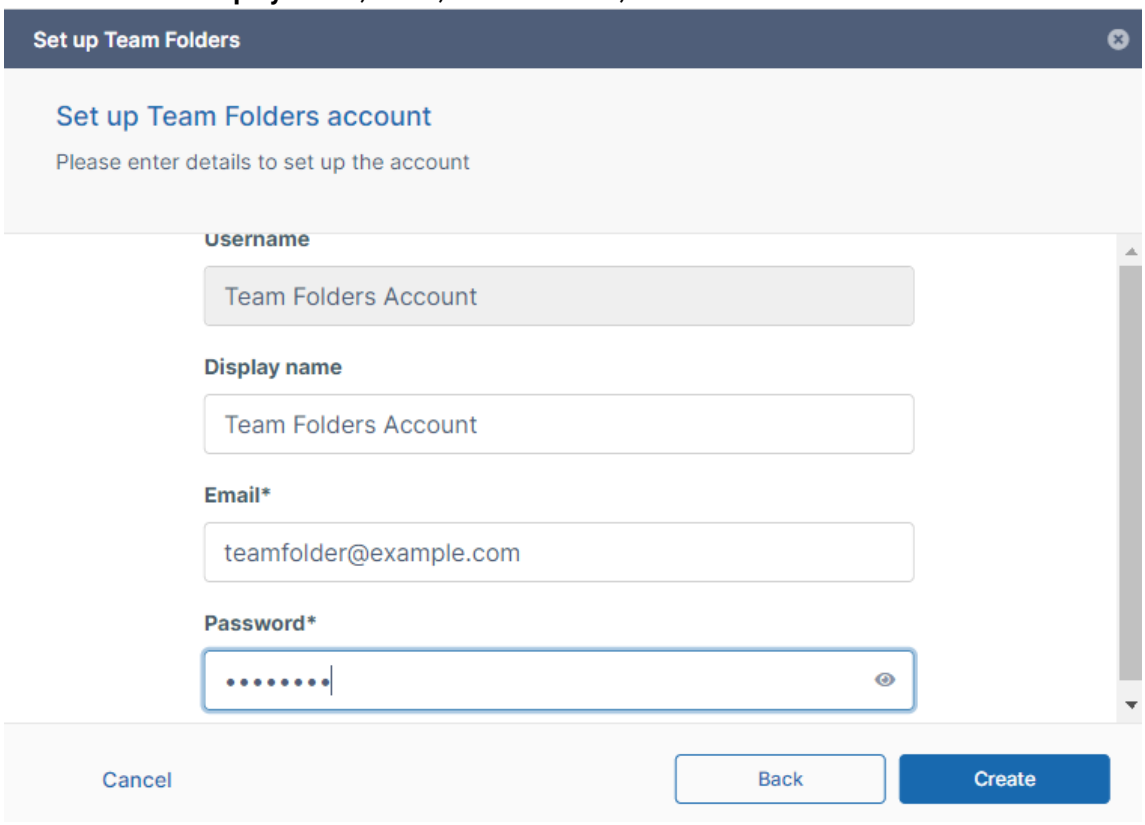


2. Click the **Set up Team Folders** button.
   A wizard for setting up Team Folders opens.
3. In the **Username** field, enter a name for your Team Folders account (in the example below, we've entered **Team Folder Account**).

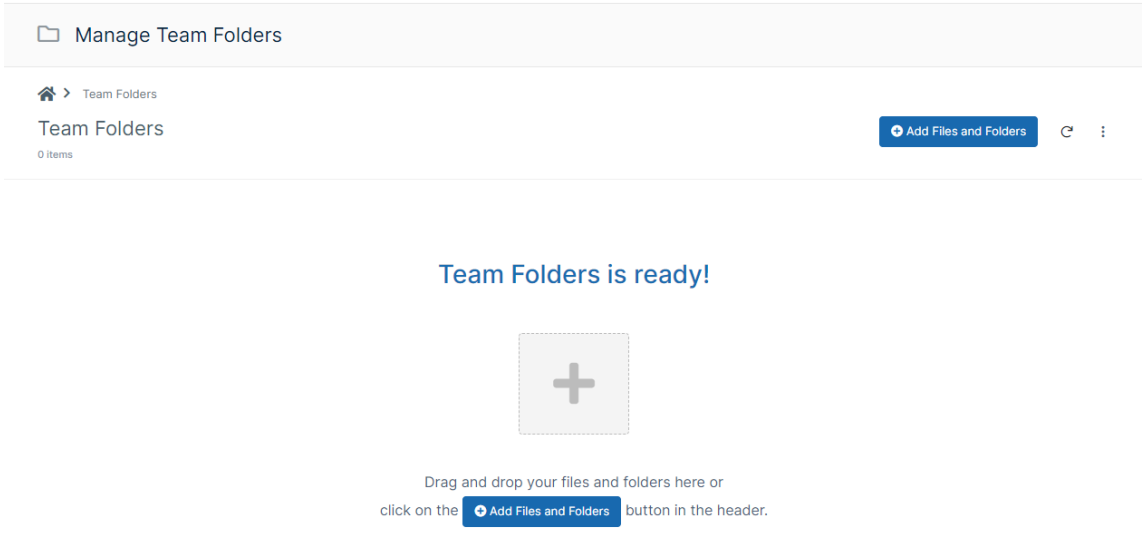


4. Click **Next**.
   The next window of the wizard displays additional fields.

5. Enter values for **Display Name**, **Email**, and **Password**, and click **Create**.



The following screen appears:

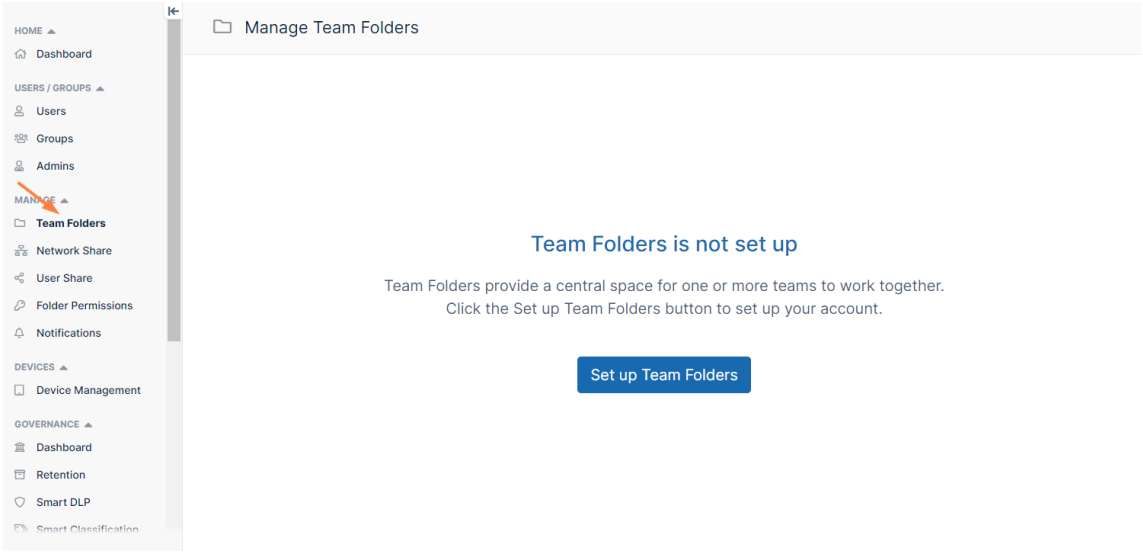


6. Now you are ready to create your Team Folders and fill them with contents. You can proceed from where you are by dragging and dropping folders onto the page or by clicking **Add Files and Folders**. This is a good option if you do not already have a folder structure set up that you want

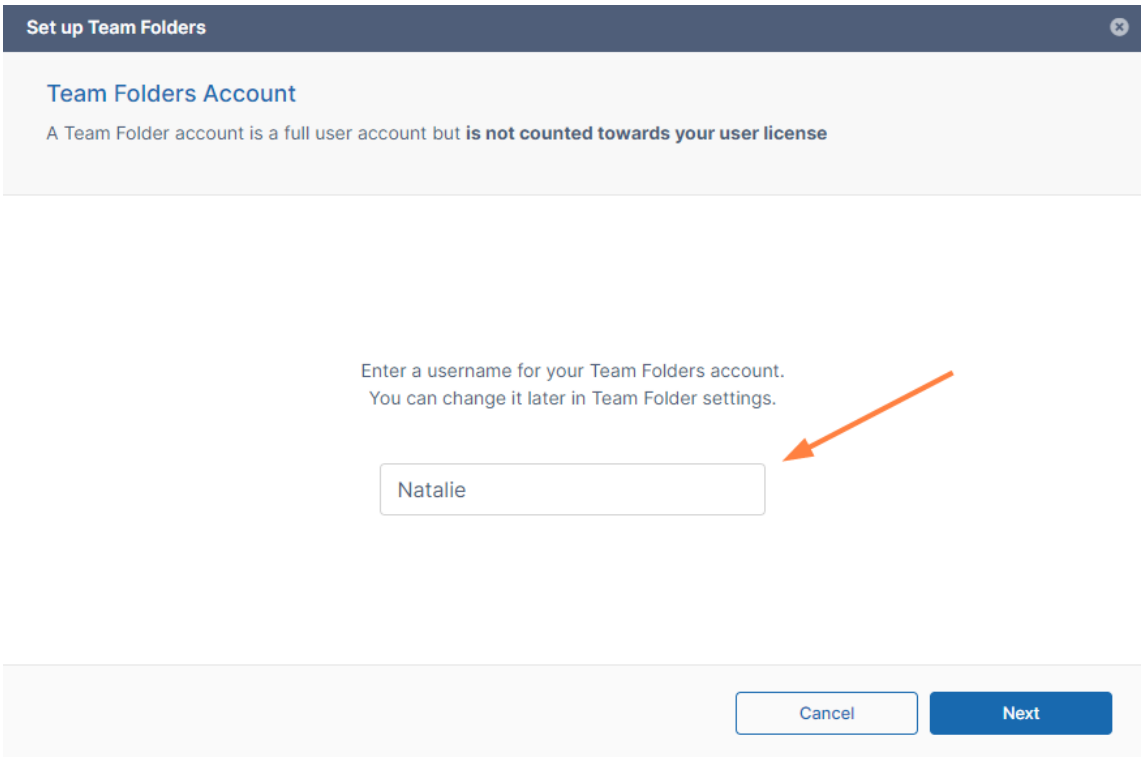
to bring into FileCloud as your Team Folders.
If you already have a folder structure that you want to use, FileCloud Sync is the preferred method.
For instructions on using these methods and others, see Seed and Organize Team Folder Data.

Convert an existing user account into the Team Folders account

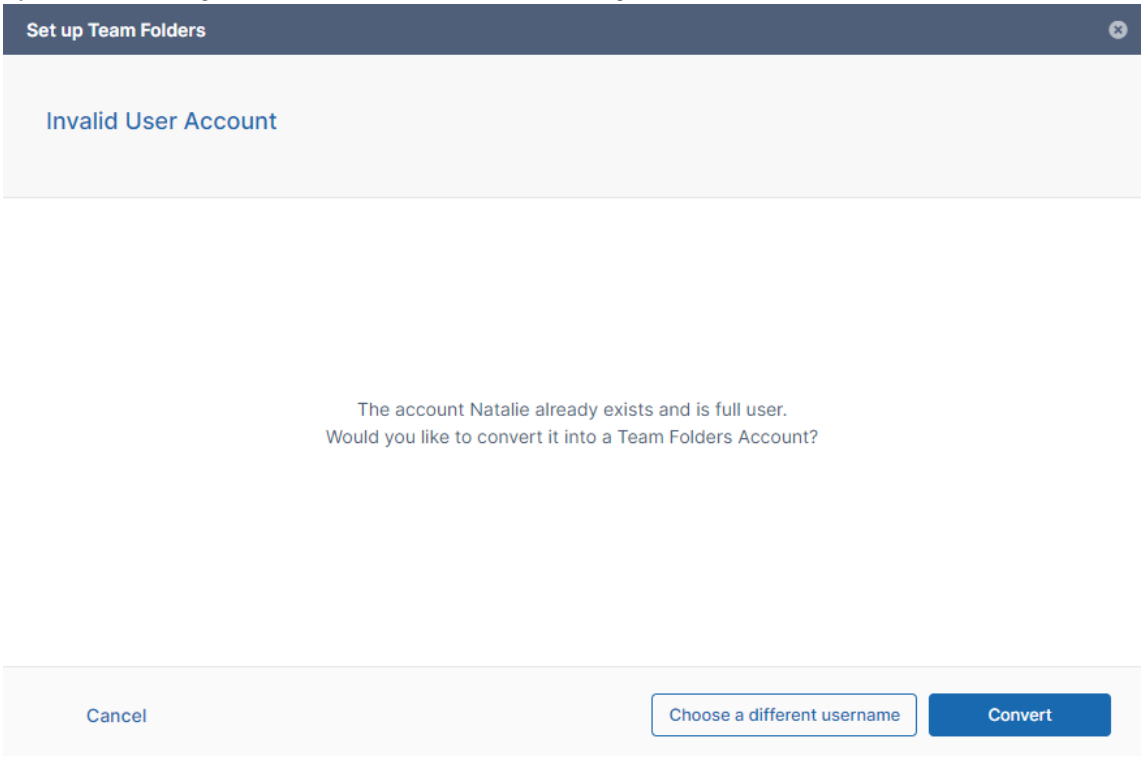
1. In the admin portal's navigation pane, click **Team Folders**.
   The screen tells you Team Folders is not set up, and it provides you with a **Set up Team Folders** button.



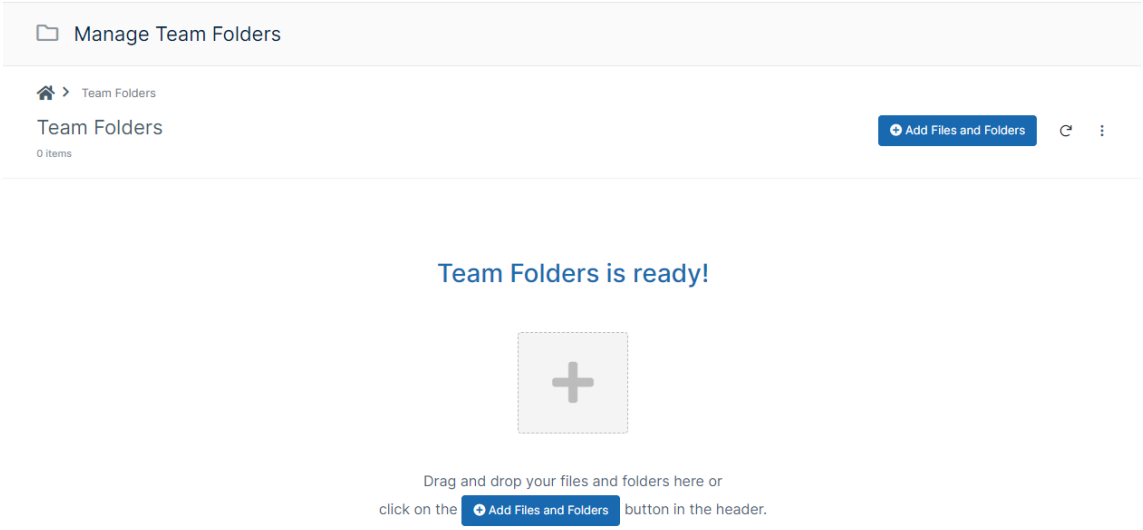
2. Click the **Set up Team Folders** button.
   A wizard for setting up Team Folders opens.
3. In the **Username** field, enter the username of the account that you want to convert into the Team Folder account.



4. Click **Next**.
   The next window of the wizard indicates that the username already exists, and gives you the option of entering a different username or converting this user:



5. Click **Convert**.
   The following screen appears:



   Now you are ready to create your Team Folders and fill them with contents. You can begin by dragging and dropping folders onto the page or clicking **Add Files and Folders**. These are good options if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.

If you already have a folder structure that you want to use, FileCloud Sync is the preferred method. For instructions on using these methods and others, see Seed and Organize Team Folder Data.

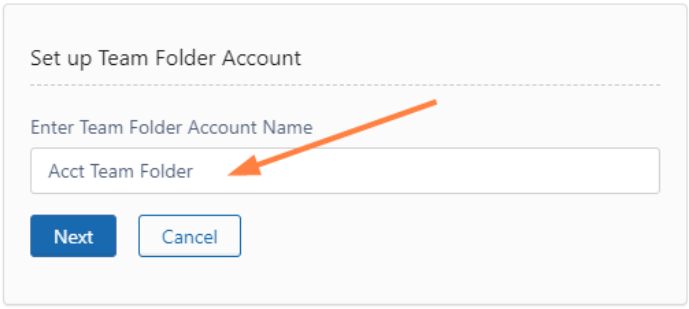
Create a new account through the Team Folders settings page

To enable team folders and create an account through Team Folders settings:

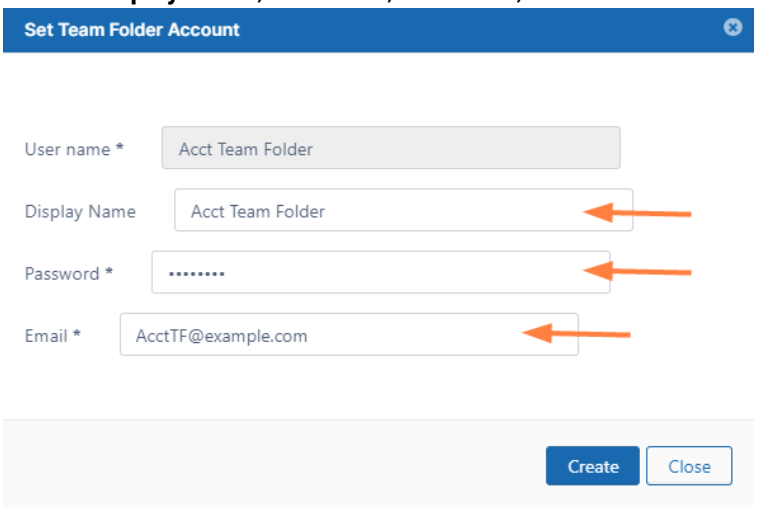
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Team Folders**  .
   The Team Folders settings page opens.
2. Click the **Enable Team Folders** toggle control.



3. Click **Save.**
   The **Set up Team Folder Account** dialog box **opens.**
4. in **Enter Team Folder Account Name**, type in a unique name.
   The **Team Folder Account Name** can contain alphanumeric characters and underscores, periods, dashes and spaces.

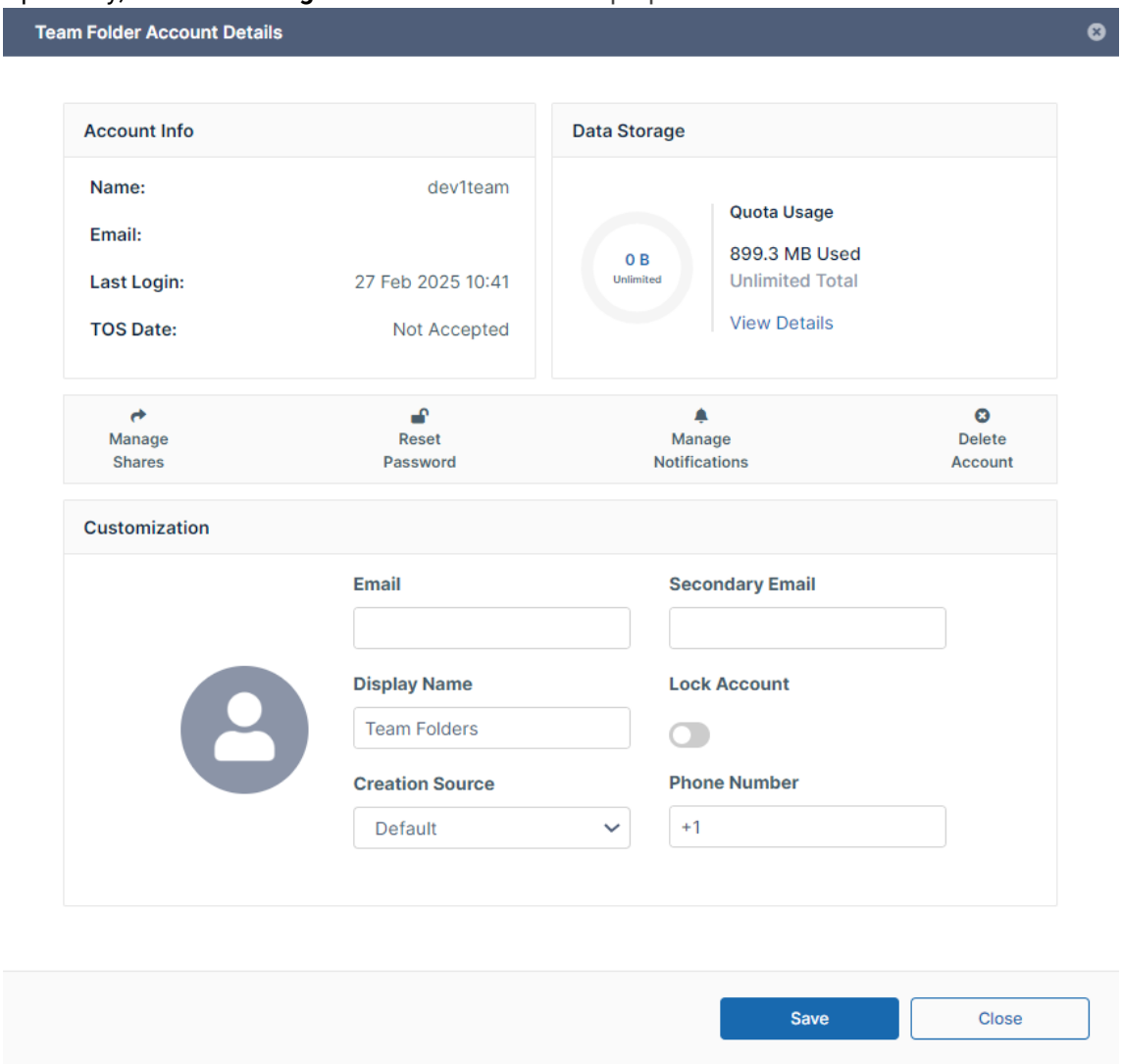


5. In the confirmation window, click **OK**.
   The **Set Team Folder Account** dialog box opens.
6. Enter a **Display Name**, **Password**, and **Email**, and click **Create**.



The Team Folder account is created and team folders are enabled.

Optionally, click the **Manage** button to set additional properties for the Team Folder account.



Action	Description
Manage Shares	View all the shares that are created under the Team Folder account.
Reset Password	Reset the password for the Team Folder account.
Manage Notifications	Edit notifications configured on the Team Folder account's file and folder paths.

Action	Description
Delete Account	Delete the Team Folder account. This will delete all the files and folders under the Team Folders.

Property Name	Property Description
Profile image	Image for the Team Folder account.
Email	Email address for the Team Folder account.
Secondary Email	Alternate email address.
Display Name	Display Name for Team Folders that appears in the user interface.
Lock Account	Automatically checked when too many login errors occur. Click to remove check and unlock account.
Creation Source	Where the Team Folder account was created. Options are: • Default (Admin user interface or import) • SSO (During SSO sign in)
Phone Number (added in FileCloud 20.1)	Used when logging in with 2FA.

Now you are ready to create your Team Folders and fill them with contents. You can go to the Team Folders screen and add the folders there. This is a good option if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.

If you already have a folder structure that you want to use, FileCloud Sync is the preferred method.

For instructions on using these methods and others, see Seed and Organize Team Folder Data.

Convert an existing account through the Team Folder settings

You can also create the Team Folder account by promoting a user account that is already in use for company-wide communication.

Promoting existing user accounts to team folders should be done only after understanding all the consequences of such an action.

- This can cause company-wide changes to Sync app users
- Promoting an existing account can potentially cause re-downloading of existing content

To move an existing user account to a Team Folder account:

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. Click the **Enable Team Folders** toggle control.



3. Click **Save.**
   The **Set up Team Folder Account** dialog box **opens.**
4. Click the **Enable Team Folders** checkbox.
5. On the **Set up Team Folder Account** window, in **Enter Team Folder Account Name**, type in the existing full user account name you want to use.
6. On the **Set Team Folder Account** window, type in the existing **Password** and **Email** for the existing full user.
7. Click **Create**.
8. Have each user connecting with the Sync app, log out of Sync and restart it.
   If any files in the user account that was converted to the Team Folder account were originally shared with any Sync users, the shared data was synced previously to **Shared With Me**, but is now synced to **Team Folders** → ***foldername***.
   After all the data has been downloaded, delete the old folders in **Shared with Me**.

Seed and Organize Team Folder Data

When you log into the FileCloud user portal with the Team Folder account, the files that appear in the My Files folder are the Team Folders for your FileCloud system. You can create and seed Team Folders by logging into Sync, Drive, or the user portal as the Team Folder account and moving the folders that you want to become Team Folders into the Team Folder account's My Files folder. The recommended method is to log into the Sync client and sync the folders.

Alternately, as an admin, you can log into the admin portal, and manually create Team Folders.

Sync Client (Recommended)

Seeding Team Folder data with FileCloud Sync Client is both simple and quick. Follow these steps:

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Download and install the FileCloud Sync Client.
3. Log in to the Sync Client using the Team Folder account credentials created during the Team Folder Account Setup.
4. Open the My Files folder.
5. In file explorer, copy the folders created in Step 1 into My Files.
6. Wait for Sync to run automatically or click Sync Now.
   The folders are synced to My Files in your Team Folder Account. The folders become Team Folders for all other users.

Once the sync is complete, you can log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Note: Alternately, use the ServerSync Client instead of the Sync Client.

Drive Client

Team Folder data can be seeded using the Drive Client. The following steps must be followed to seed data using Drive Client.

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Download and install the FileCloud Drive Client.
3. Log in to the Drive Client using the Team Folder account credentials created during the Team Folder Account Setup.
4. Locate Drive in your file explorer, and copy the folders created in Step 1 into My Files.
   Drive will automatically detect the new folders and add them to My Files in your Team Folder Account. The folders become Team Folders for all other users.

Once the files and folders are copied, you can log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Open a browser and log in to the User Portal

The FileCloud web user interface can be used to seed and organize Team Folder data. The following steps must be followed to set up Team Folder data using the user portal.

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Using a web browser, go to the FileCloud user portal.
3. Log in using the Team Folder account credentials created during the Team Folder account set up.
4. Browse to My Files
5. Copy the folders that you created in Step 1 into My Files.
   These folders become Team Folders for all other users.

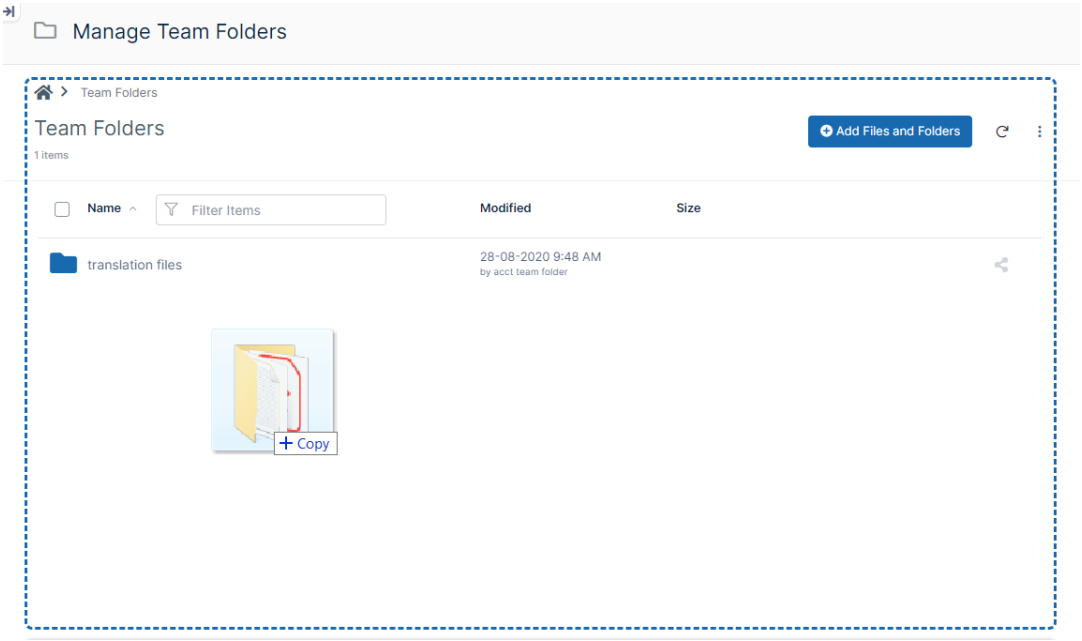
Now, log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Admin Portal

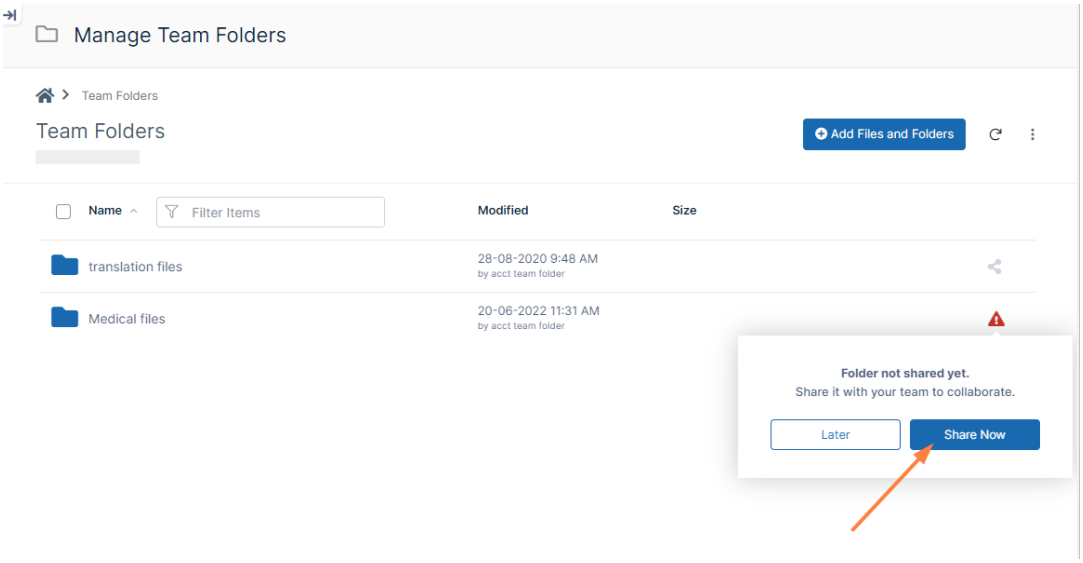
Go to the **Team Folders** page in the admin portal to create Team Folders and seed them with files.

1. Open a browser and log in to the admin portal.
2. Ensure the account that is used to log in has permissions to access Team Folders.
   The main admin account has automatic access to Team Folders. To set Team Folder access to additional admin accounts, see Managing Admin Users.
3. From the left navigation panel, click **Team Folders**.
4. Add Team Folders.
   Add Team Folders by dragging and dropping

   a. Drag and drop an existing folder (with or without contents) from your file system onto the Team folders screen.



   b. The folder becomes a Team Folder, and you are prompted to share it with users or groups.

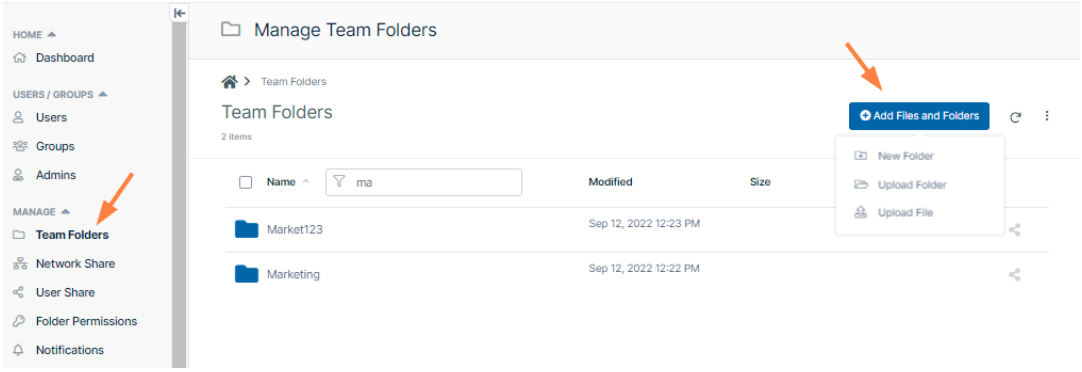


c. Click **Share Now** to share the Team Folder with users and/or groups.

d. To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

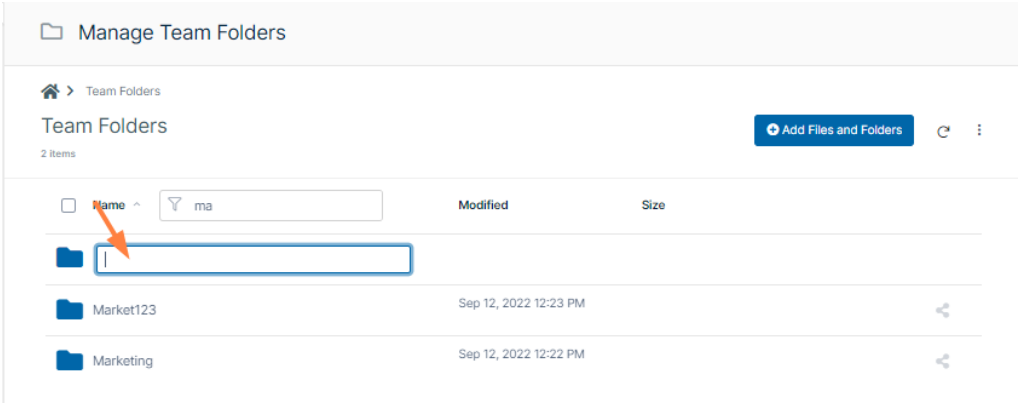
Add Team Folders by clicking the button

a. Click the **Add Files and Folders** button.
A drop-down menu opens.

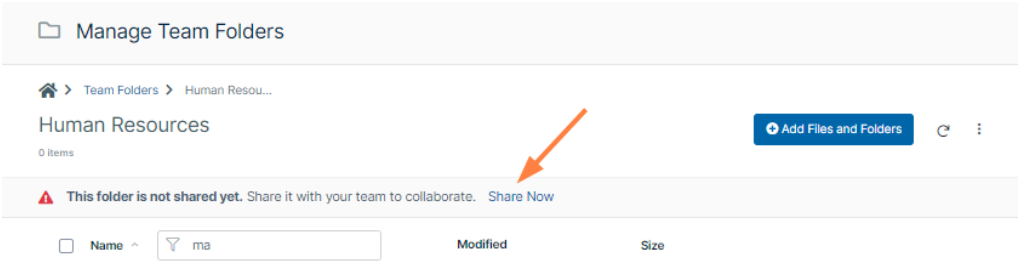


b. Either choose **New Folder** to create a new Team Folder, or click **Upload Folder** to upload an existing folder (with or without contents) and make it a Team Folder.
If you choose **New Folder:**

-
  - A new folder appears in the list. Your cursor is positioned so that you may give the folder a name.



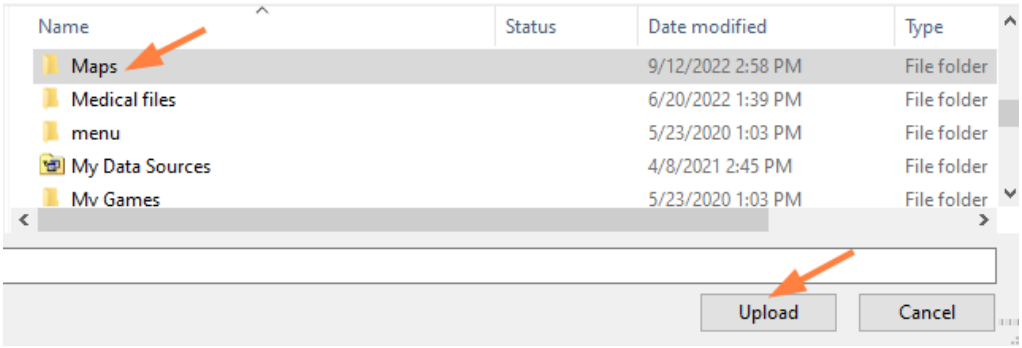
-
  - Add a name and click Enter.
    The folder opens and displays a reminder to share the file.
  - Click **Share Now**.



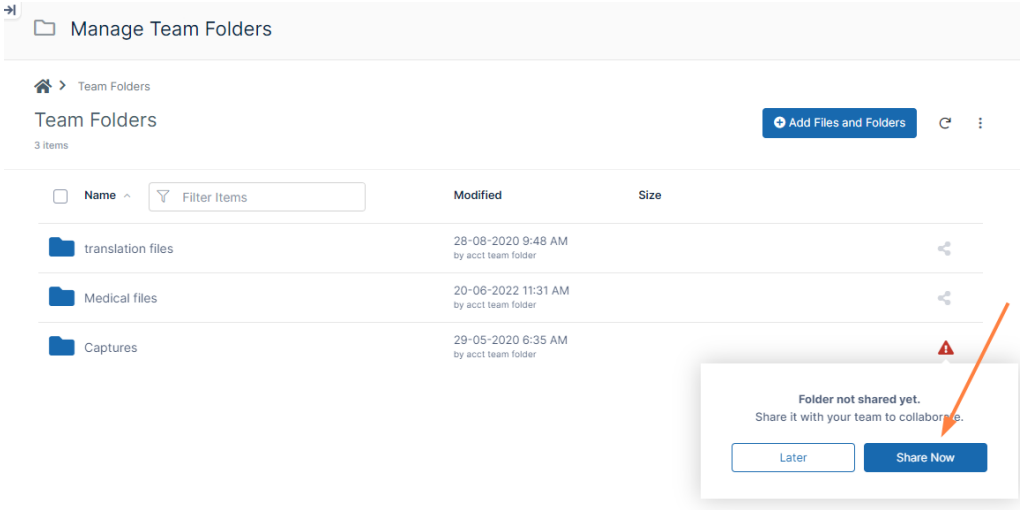
    A share dialog box opens.
  - To share the folder with users, see Share the Team Folder and Set Permissions.
  - To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

If you choose **Upload Folder**, your file explorer opens.

a.
  - Select the folder to use as a Team Folder and upload it. Agree to upload the its files if prompted.



The folder and its contents are uploaded. The folder becomes a Team Folder, and you are prompted to share it with users or groups.



- Click **Share Now** to share the Team Folder with users and/or groups.
- To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

Share the Team Folder and Set Permissions

Beginning with FileCloud 23.241, admins can share Team Folders with external users. Prior to FileCloud 23.232, they were unable to share Team Folders with external users.

Beginning with FileCloud 23.1, by default, you can no longer share a top-level Team Folder publicly. To change the default, see To enable public sharing of top-level Team Folders, below.

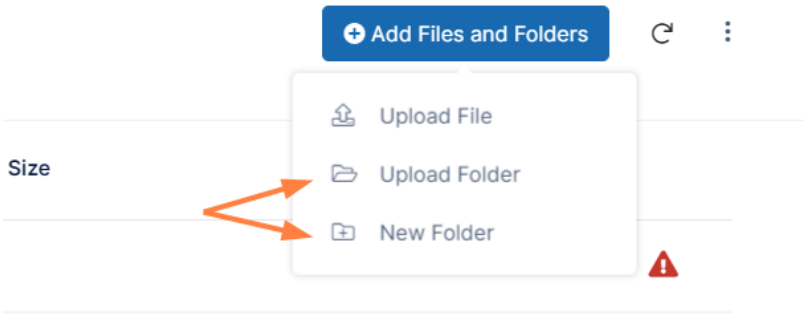
You must share Team Folders before users can access them.

- Team folders that are not shared do not appear under any user's account and are not accessible.
- Team Folders are shared from the admin portal, and may be shared privately with specific groups or users.

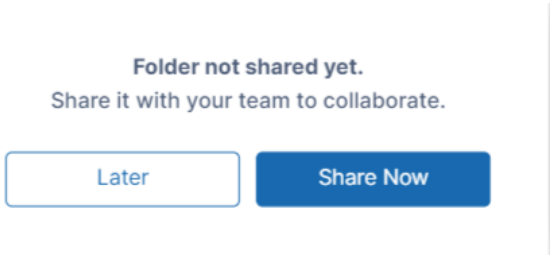
After setting up Team Folders, you can add and share them.

To share a new Team Folder when adding it:

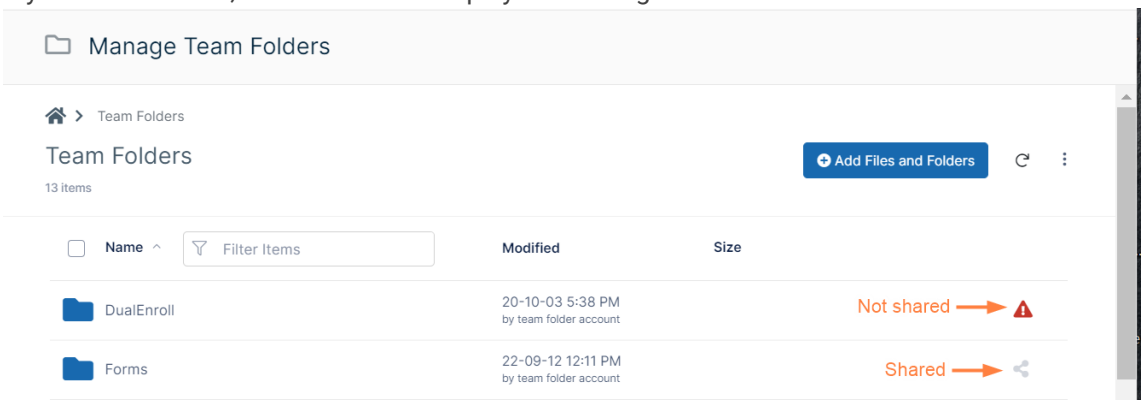
1. In the admin portal, click **Team Folders** in the navigation panel.
2. Drag and drop the folder onto the **Team Folders** screen or use the **Add Files and Folders** button and choose either **Upload Folder** or **New Folder**.



When the folder is added the following prompt appears:



3. Click **Share Now**, to configure the share and share it with users now, or click **Later** to configure and share it at a later time.
   If you choose **Later**, the folder's row displays a warning icon.

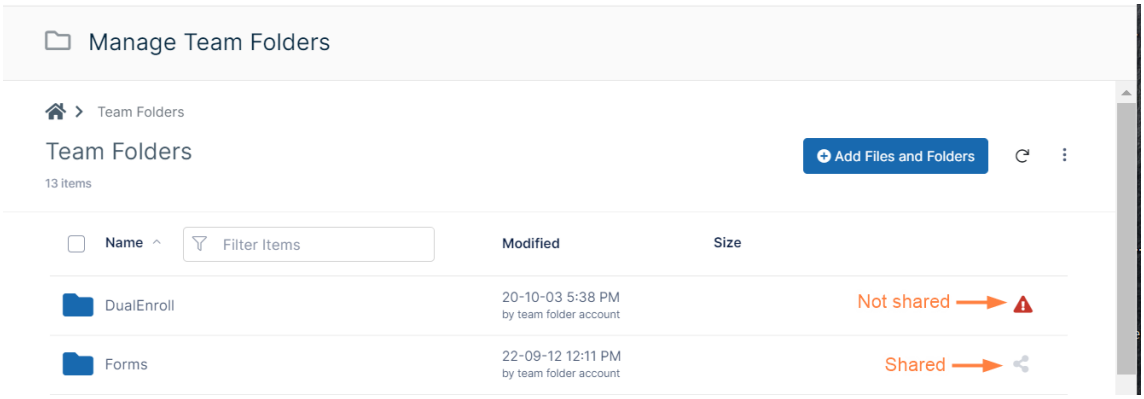


   If you choose **Share Now** a **Share link for folder** dialog box opens.
4. To configure the share, see To complete the Team Folder share, below.

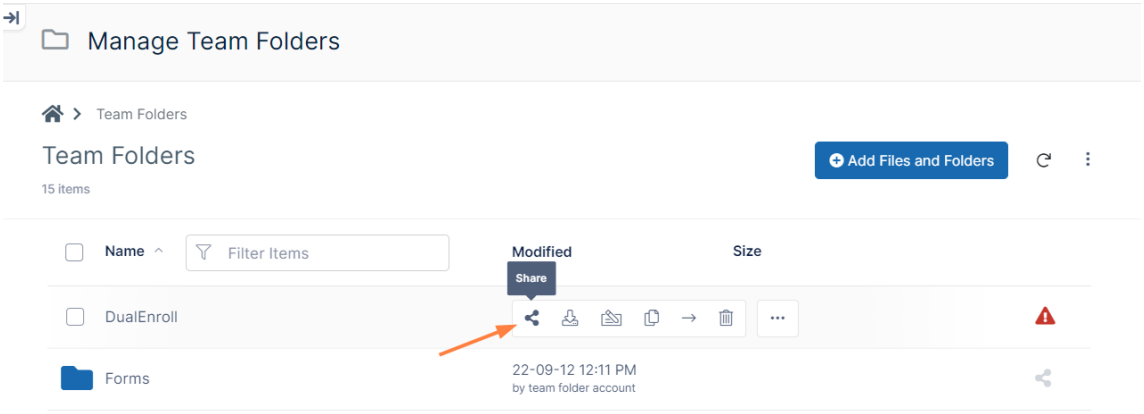
To share an existing Team Folder:

1. In the admin portal, click **Team Folders** in the navigation panel.

2. The row for a Team Folder displays a share icon if it has already been shared or a warning icon if it has not been shared.



3. Hover over a Team Folder with a warning icon, and click the share icon.

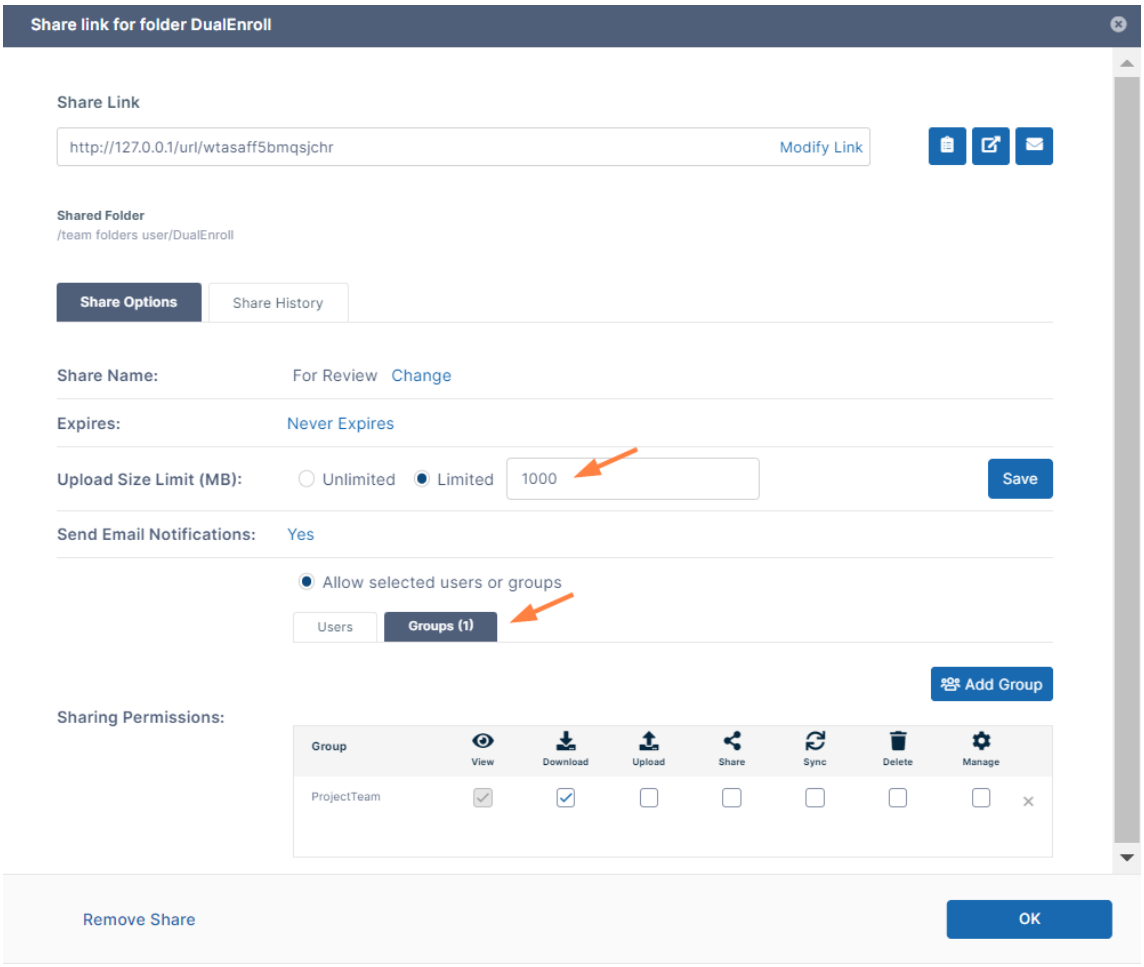


The **Share link for folder** dialog box opens.

4. To configure the share, see To complete the Team Folder share, below.

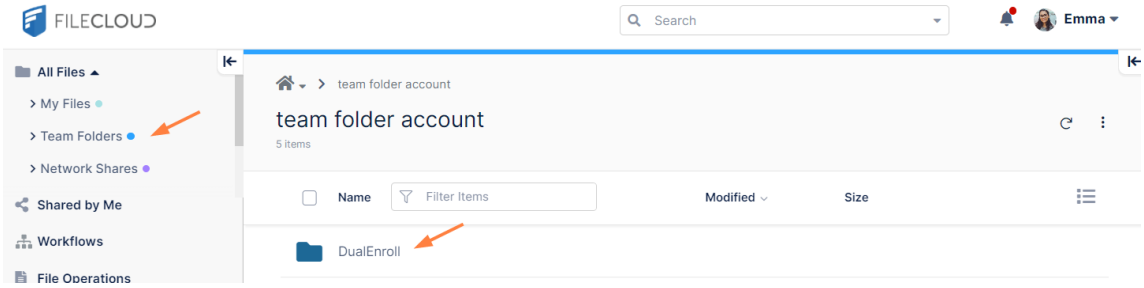
To complete the Team Folder share:

1. In the **Share link for folder** dialog box, configure the settings for the share.
For example, you may want to share the folder with a specific group only or limit the upload size.



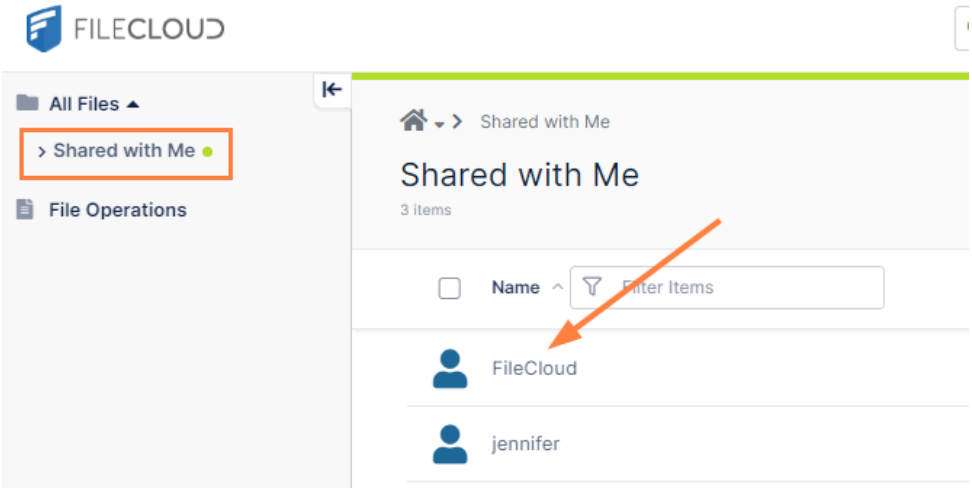
For information about share settings, see Share Options for Public and Private Folders.
For information about sharing permissions, see Public Share Permissions for Folders or Private Share Permissions for Folders.
Note: You cannot share a top-level Team Folder publicly,

Once the Team Folder is shared, it appears to all users that have access to it under Team Folders in their account in the FileCloud user portal and in FileCloud clients such as Sync, Drive, and Outlook Add-In.

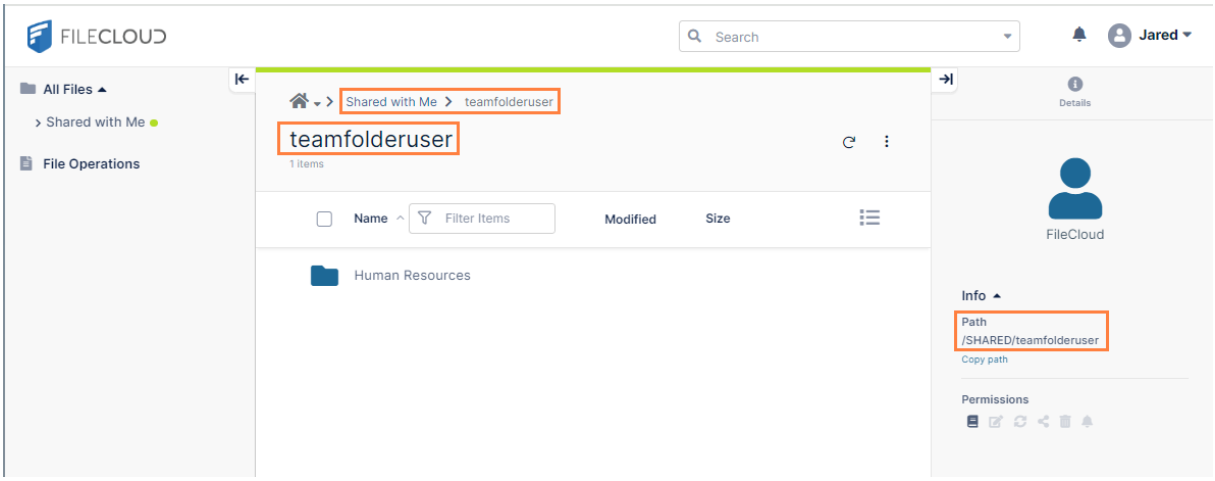


When you share a Team Folder with an external user

When you share a Team Folder with an external user, the folder appears under **Shared with Me**, and the name of the user who created the share is the **Service Name** (the value in **Settings > Server > Service Name**).



When the external user clicks the **Service Name** to access the share, the Team Folder username appears in path names and as the name over the list of folders.



If you rename a Team Folder

If you rename a folder, but do not change the name of the Team Folder share, users will continue to see the original Team Folder name. To help you remember to change the share name, FileCloud automatically asks you if you want to change the share name when you change a Team Folder name, as shown in the following video:

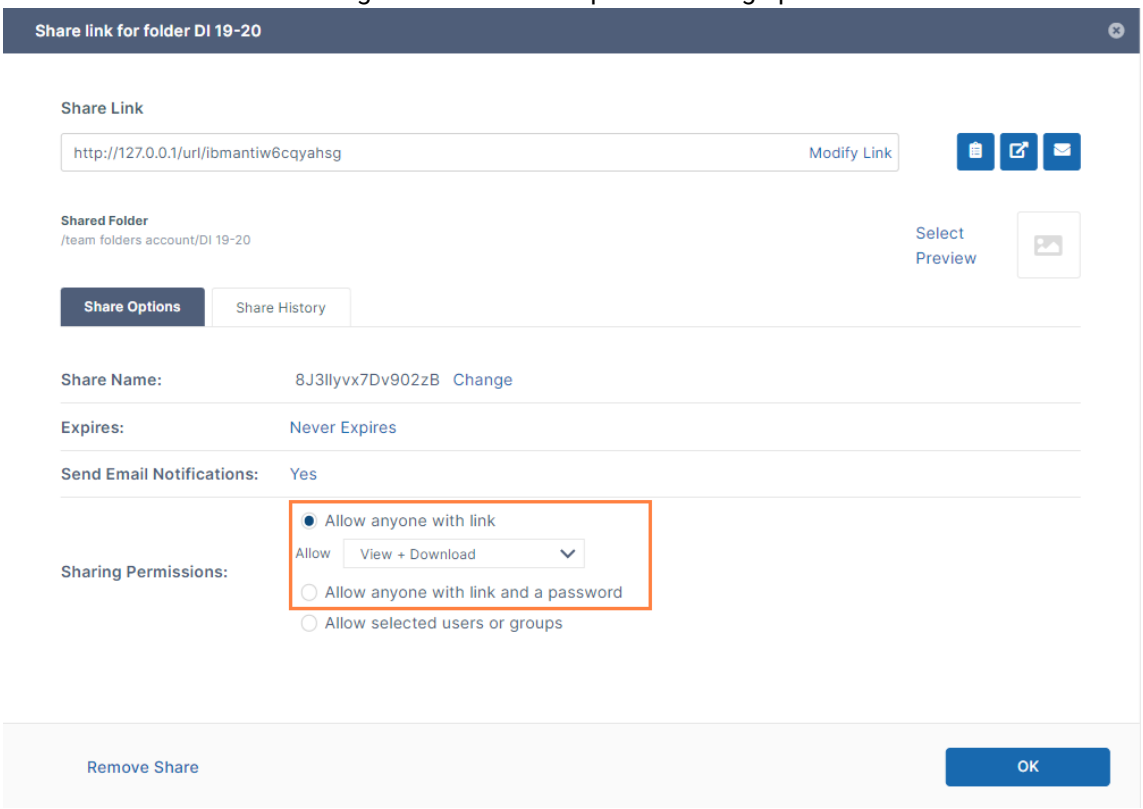


To enable public sharing of top-level Team Folders

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

```
define('TONIDOCLOUD_ALLOW_PUBLIC_SHARE_TOP_LEVEL_TEAM_FOLDER', true);
```

The **Share link for folder** dialog box now includes public sharing options:



To return to disabling public sharing of top-level Team Folders:

- Change the value of the cloudconfig.php setting from **true** to **false**:

```
define('TONIDOCLOUD_ALLOW_PUBLIC_SHARE_TOP_LEVEL_TEAM_FOLDER', false);
```

User Settings

Your FileCloud site provides your users with a place to store and share files.

- Every user of FileCloud needs a user account before they can store and access files
- You can configure user accounts to authenticate with the system you already have in place



Administrators cannot create users with the account names **admin** or **superadmin**.

Add User Accounts	Create or Import New Accounts Allow Users to Create Accounts
Configure User Authentication	User Authentication Settings Enabling Default Authentication Active Directory Authentication Connecting to AD via SSL Using Single Sign-On
Manage User Accounts	Migrate data after an account name change Changing the Storage Quota for Users User Session Expiration Restrict Commonly Used Passwords Customize the User Login Screen

Create FileCloud Users

You can control access to files stored in FileCloud by configuring permissions for user accounts.

- Every user who has access to FileCloud storage must have an account.
- Once a user account is created, it can be assigned different access levels.



In FileCloud version 20.1 and later, special characters from the extended UTF8 alphabet are supported in display names.
Beginning in FileCloud version 23.251, you can also import users when you import their groups from certain SSO providers. For instructions, see Group Settings.

⚠ Administrators cannot create users with the account names **admin** or **superadmin**.

In this section

User Access Levels and User Types

When you create a user account, you assign it an access level.

There are four different access levels for users.

Level	Access	Notes
Admin Access	The default Admin has complete control over the FileCloud system. Other admin users have those admin permissions given to them.	The default Admin account is used to manage the FileCloud. The default admin user account is 'admin'. Other users can be marked as admins and given a limited set of permissions. Read more about Multiple Admins
Full Access	Control over its own private cloud storage space in My Files.	These user accounts can: • store files in their own private cloud storage space • view and download files stored in their storage space • view and download files shared with them by other users
Guest Access	Restricted access to the FileCloud system.	These user accounts: • Do not have private cloud storage • Can only view/upload/download files shared to them by other user accounts • Can re-share content if they have permissions

Level	Access	Notes
External Access	Access to FileCloud only through a Web browser.	These user accounts: • Can only view/upload/download content shared with them • Do not count towards the user license limit • Cannot be authenticated via AD and can only be local user accounts • Have external linked email accounts and cannot use the same domain as the FileCloud URL • Can't be added directly to network shares via the admin portal • Can access content from network folders if they are shared

- **Both Full and Guest users accounts are counted towards user accounts specified in the license.**
- **External Access accounts are NOT counted towards the license.**

User Types Comparison

User Access Feature	Full Access	Guest Access	External Access
User Portal (Web Browser) Access	Permitted Fully supported	Permitted Not all functions available	Permitted Not all Functions Available
View shared files	Permitted	Permitted	Permitted
Authentication	Local / ActiveDirectory	Local / ActiveDirectory	Local Only
Mobile App Access	Permitted Fully supported	Permitted Not all functions available	Not Available
Personal storage in FileCloud	Available	Not Available	Not Available

Share files with other users	Permitted	Permitted	Not Available
Install and use FileCloud Desktop, FileCloud Sync, and FileCloud Drive	Permitted	Permitted	Not Available
Sync storage using Cloud Sync	Permitted	Permitted	Not Available
SSO Login	Permitted	Permitted	Not Available
Group Membership	Can be member of any group	Can be member of any group	Can be member of any group except Everyone.
Admin Account	Can be Admin Account	Can be Admin Account	Cannot be an Admin Account
Team Folders	Permitted	Permitted	Permitted
Automation App	Permitted	Permitted	Not Available
File and Folder Comments	Permitted	Permitted	Not Available
MFA	Permitted	Permitted	Available by license beginning in Version 20.2 for Enterprise Advanced customers.

User Access Feature	Full Access	Guest Access	External Access
View Network Shares	Permitted	Permitted	Only via shares created by users

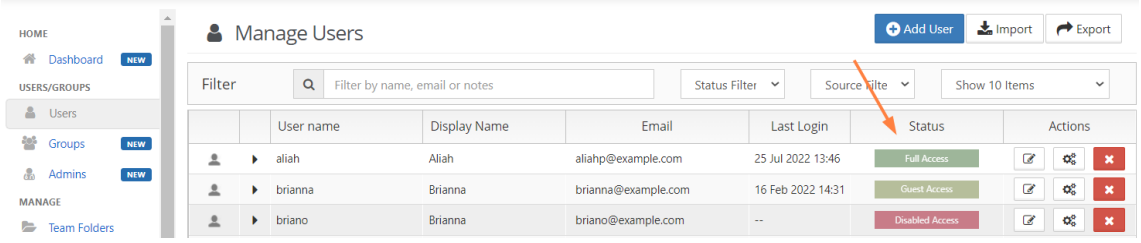
Checking User Access Level

The access level of any user account can be checked by the Administrator using the admin portal.

To check a user's access level:

1. Log on to Administration Portal.
2. Click **Manage Users** in the navigation panel.
3. In **Filter**, enter the name or email address of the user.

4. The **Access** for the user will be listed in the **Status** column.



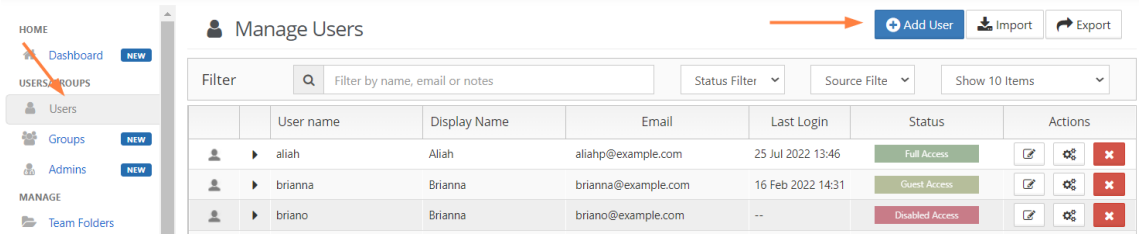
Manually Create a New User Account

> The default user storage quota for every new user is set in Managed Storage. See Setting up Managed Disk Storage

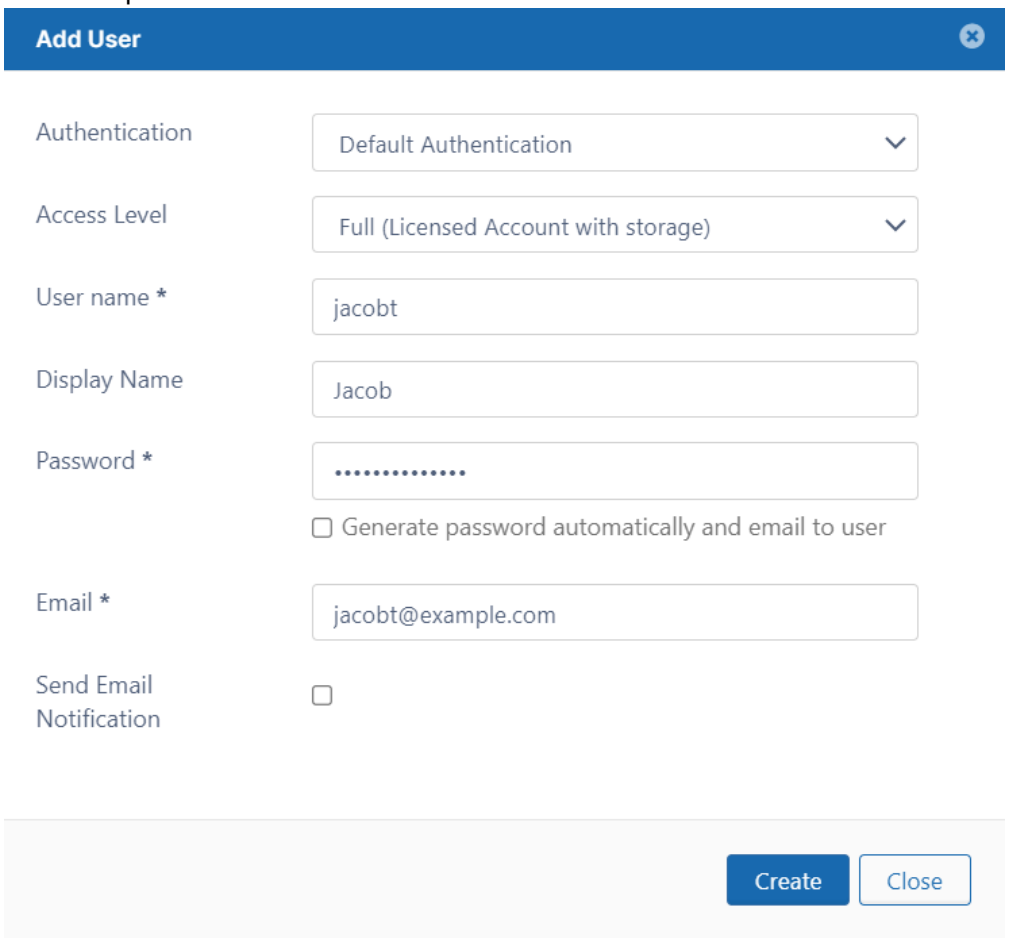
An optional sample set of files can be preloaded for every user on creation.

To create a FileCloud user with default authentication:

1. Log on to Admin Portal.
2. In the left navigation panel, click **Users.**
3. In the top right corner, click the **Add User**.



4. Set the required account information.

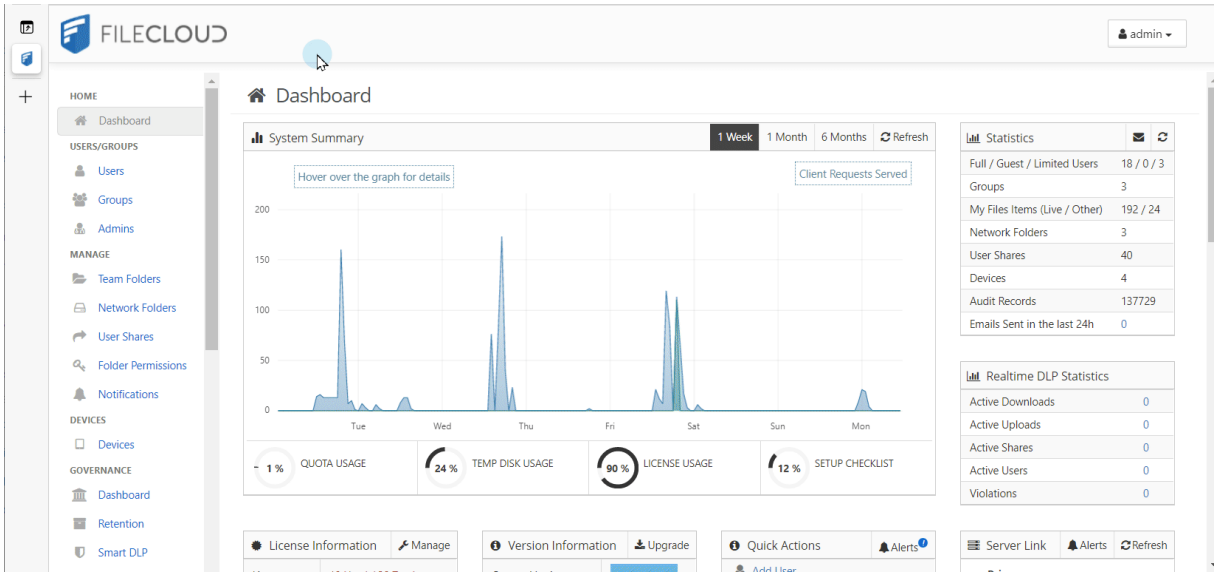


Settings	Description
Authentication	Allows you to select the authentication type for granting access into the system. • **Default Authentication** - creates a local user account. User credentials are stored and authenticated within FileCloud. • **LDAP or AD Authentication** - creates an external user account. User credentials are stored and authenticated from an external LDAP or AD server.
Access Level	Allows you to select the user tu[e. A user account with Full or Guest access counts as a license.
User name	Name to be used to log into the system. By default, **User name** can only contain numbers, spaces, hyphens, periods, underscores, and letters from the Latin alphabet (A-Z, uppercase and lowercase), and email addresses may not be used as usernames. **Note**: To also enable use of apostrophes in the **User name**, go to **Settings > Admin** and check **Allow Email as Username**.

Settings	Description
Display name	Name that appears on user interface
Password	Password for the user (Should adhere to password length and strength requirements for your organization). Either enter a password here, or check the following box.
Generate password automatically and email to user	FileCloud generates a password according to your settings for password limitations and emails it to the user. Anything entered into the **Password** field is ignored.
Email	An email id that is unique in the FileCloud system
Send Email Notification	When checked, a welcome email is sent to the new user. Unchecked by default. Beginning with FileCloud 20.1, if you uncheck this, you can send a welcome email with a newly generated password later. See Send Email from User Details.
Include Password in Email	When checked, the new user's password is included in the welcome email. Checked by default. Beginning with FileCloud 20.1, if you uncheck this, you can send a welcome email with a newly generated password later. See Send Email from User Details.

5. Click **Create**.

Video of Adding FileCloud Server User Account



Bulk creation of User Accounts from a CSV File

You can create multiple accounts at one time using a CSV file.

Format of CSV file for creating user

To import from a CSV, create a simple text file with the all the user account information. The format of the created file is explained below:

CSV import format

```
UserName, EmailID, Password, DisplayName, Status, ExpirationDate, Groups, EmailVerified
```

Field	Description
UserName	The user id.
EmailID	A unique email id to be associated with the user.
Password	Password for the user. Must follow password requirements (minimum length, etc.)
DisplayName (optional)	The name that appears in the user interface for the user. Default is same as UserName.
Status (optional)	The user's account type (access level). Options are Guest|Full|External. Default is Full.
ExpirationDate (optional)	The date the user account will expire. Default is none.
Groups (optional)	The group or groups the user belongs to. If there are multiple groups, separate them with the | character. Default is none. All users other than External users are automatically placed into the **Everyone** group. External users are automatically placed into the **Externals** group. **Note**: FileCloud can only recognize group names if you do not insert spaces between the group names and the | characters: • Valid: **GROUP 1|GROUP 2** • Invalid: **GROUP 1 | GROUP 2**

Field	Description
EmailVerified (optional)	Whether or not the user can initially log in without administrator approval after the account is created. YES - Email is verified, so user can log in without account approval. Default. NO - Email is not verified, so administrator must approve account before user can log in. Administrator approval is only required for the initial login.

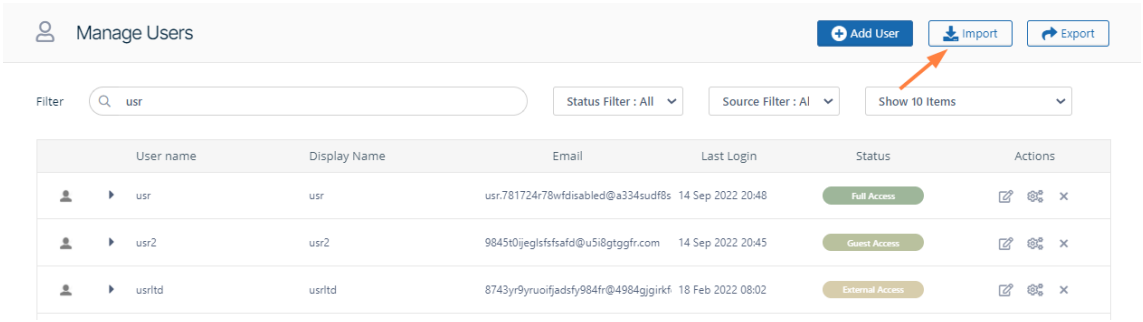
Below is a sample csv file for import.

	UserName	EmailID	Password	DisplayName	Status	ExpirationI	Groups	EmailVerified
2	nick	nick@mycompany.com		Nick	FULL			NO
3	joe	joe@mycompany.com		Joe	FULL		Accounting|Human Reso	YES
4	lisa	lisa@lisat.com		Lisa	EXTERNAL			YES
5	demozzz	demozzz@mycompany.c		demozzz	DISABLED		Accounting	YES
6								

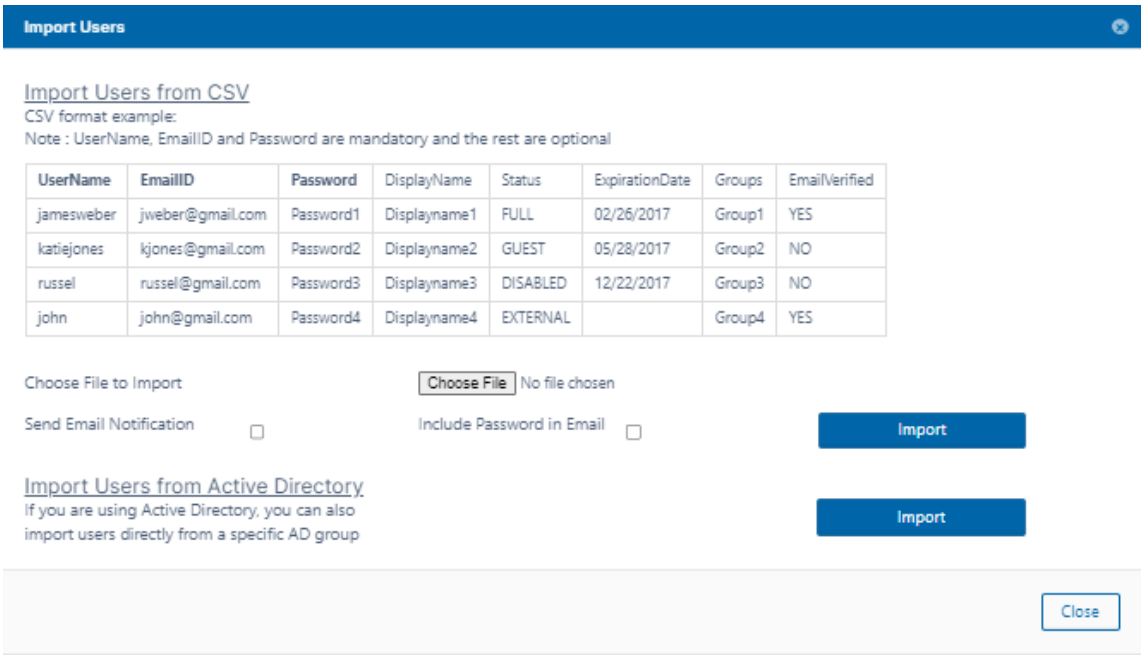
Importing a CSV File

To import a CSV File:

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



3. Click the **Import** button in the upper-right corner to open the import dialog box.



4. Click **Choose File**, and select the CSV file containing the entries of users to be created.
5. To send a notification to each user imported, check **Send Email Notification**. (*Added in FileCloud 20.1)*
   - To include each user's password in the email, check **Include Password in Email**.
6. Click **Import.**
   When the process is complete, a report is generated indicating the status of each user account creation.

Note: To export a CSV file of the users in your system, click the **Export** button.

The fields exported are the same as the imported fields with the addition of the fields **DisableNotifications**, **LastLogin**, **Authentication Type**, **MobilePhone,** and **Effective Policy**. Notice that the **Password** value is not exported.

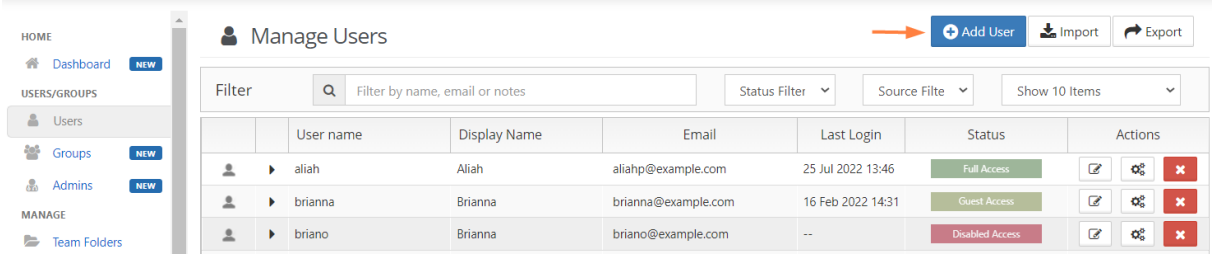
UserName	EmailID	Password	DisplayNa	Status	Expiration	Groups	EmailVerif	DisableNo	LastLogin	Authentica	MobilePhc	Effective Policy
gaby	gabrielle_95@exampl		Gaby	FULL		EVERYONE	YES	NO	11/28/2022 14:28	Default		Global Default Policy
keira	keira@example.com		Keira	FULL		EVERYONE	YES	NO		Default		Global Default Policy
brianna	brianna@example.co		Brianna	GUEST		EVERYONE	YES	NO	9/16/2022 9:54	Default	1.44E+10	Global Default Policy
laurel	laurel@example.com		Laurel	FULL		EVERYONE	YES	NO		Default		Global Default Policy
marion	marion@example.co		Marion	FULL		EVERYONE	YES	NO	3/11/2022 12:02	Default		Global Default Policy
briano	briano@example.con		Brianna	DISABLED		EVERYONE	YES	NO		Default		Global Default Policy

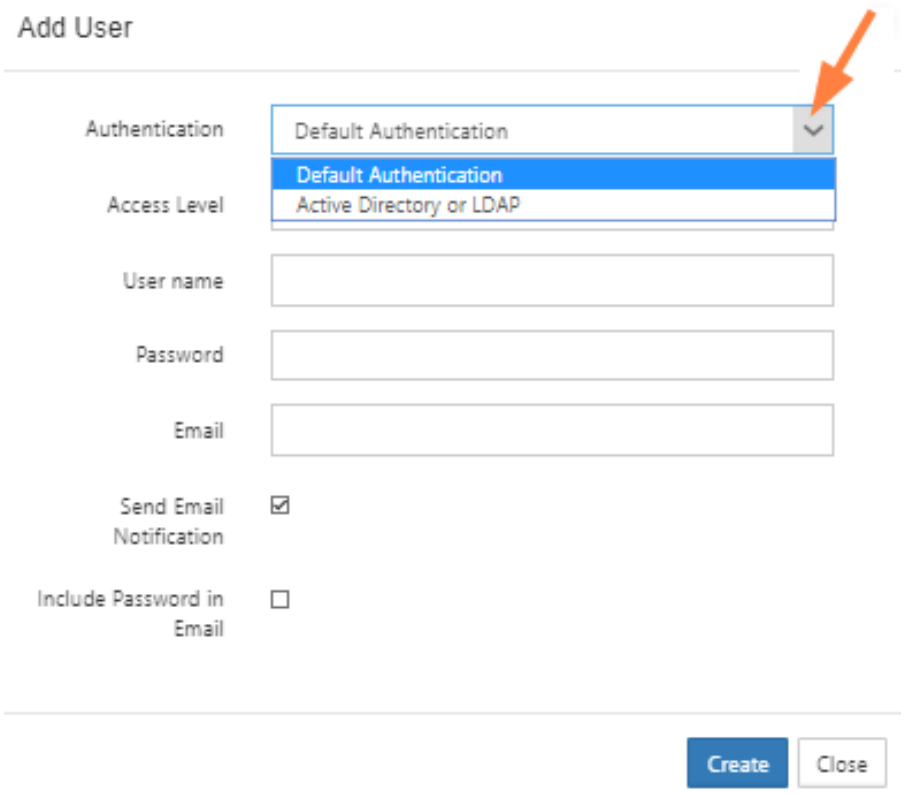
Import a user account from AD or LDAP Service

1. Log on to Administration Portal.

2. Set up AD configuration or LDAP configuration depending on your requirements.
3. Click **Users** on the left navigation panel.
4. Click **Add User** button.
5. Select **Active Directory or LDAP** as the authentication type.
6. Set the required account information as shown and click save.

Settings	Description
Authentication	Set to **Active Directory or LDAP**
AD/LDAP User name	AD/LDAP User name to import
AD/LDAP Password	AD/LDAP User name's Password
Email	Disabled: This will be imported from AD/LDAP service





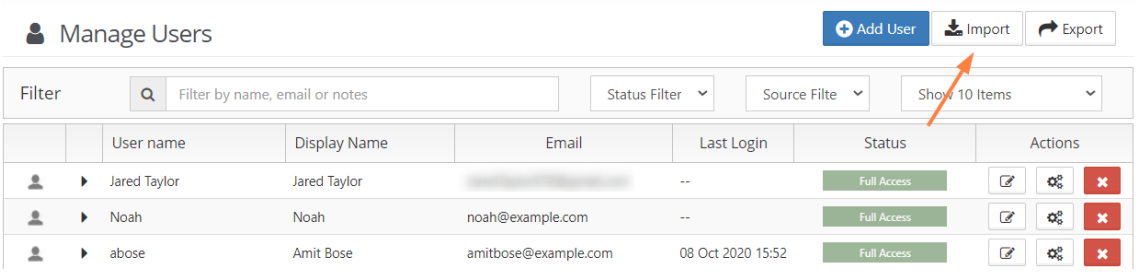
Bulk Import User Accounts from AD Server

As an administrator, you can create FileCloud user accounts by importing existing accounts from an AD group in your existing AD server.

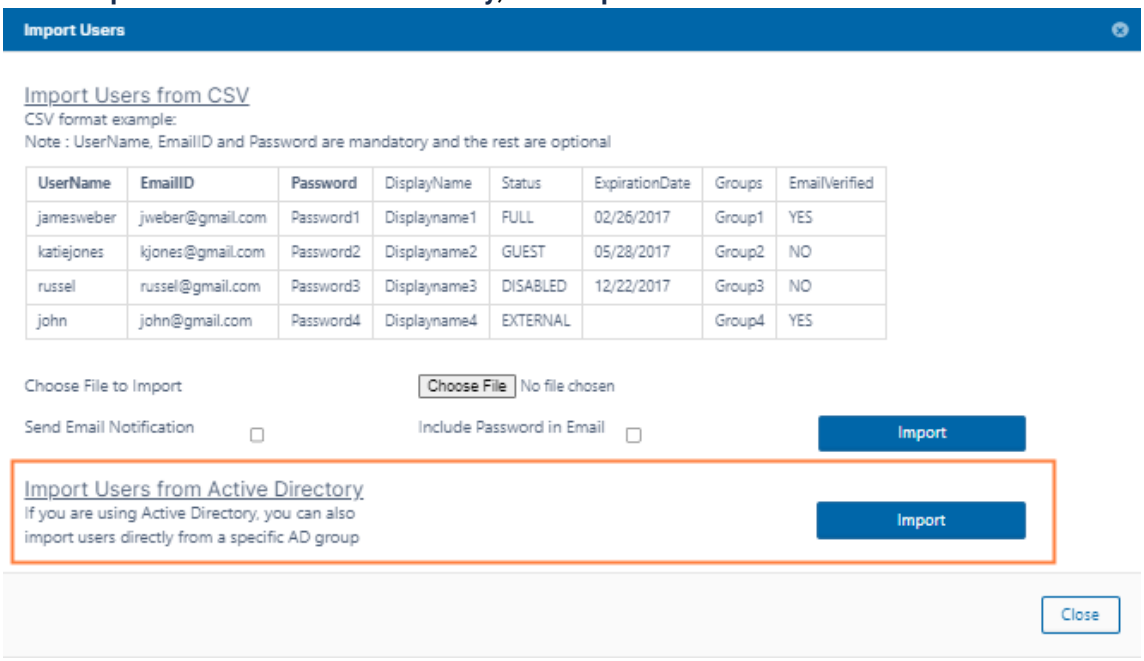
Import users from an AD Server

To import users from an AD server:

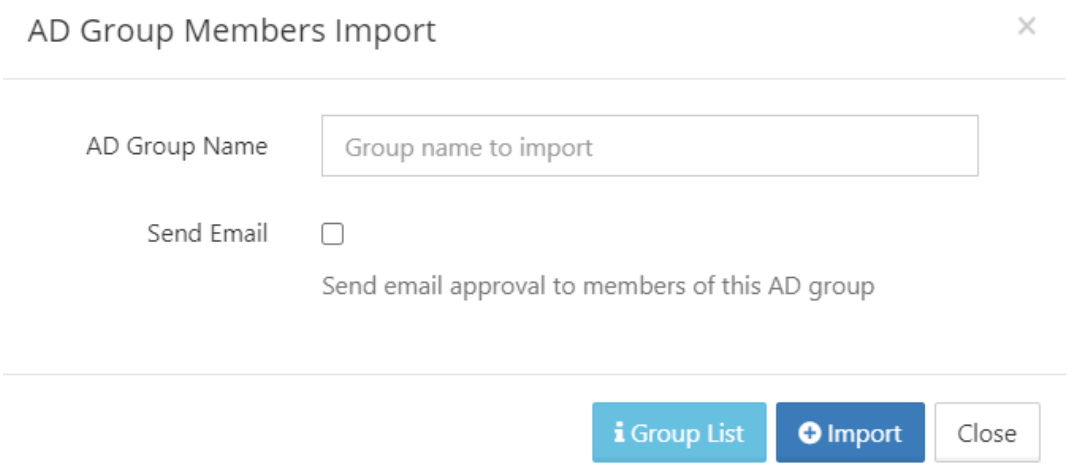
1. Open a browser and log on to Admin Portal.
2. Setup AD configuration or LDAP configuration depending on your requirements.
3. From the left navigation panel, under USERS/GROUPS, click **Users**.
4. To open the **Import** window, click **Import**.



5. Under **Import Users from Active Directory**, click **Import**.



An **AD Group Members Import** dialog box opens.



6. Type in the **AD Group Name**. A list of existing groups can also be viewed by clicking the **Group List** button.
7. To send an email to notify each user after their account is approve, check **Send Email**.
8. Click the **Import** button.

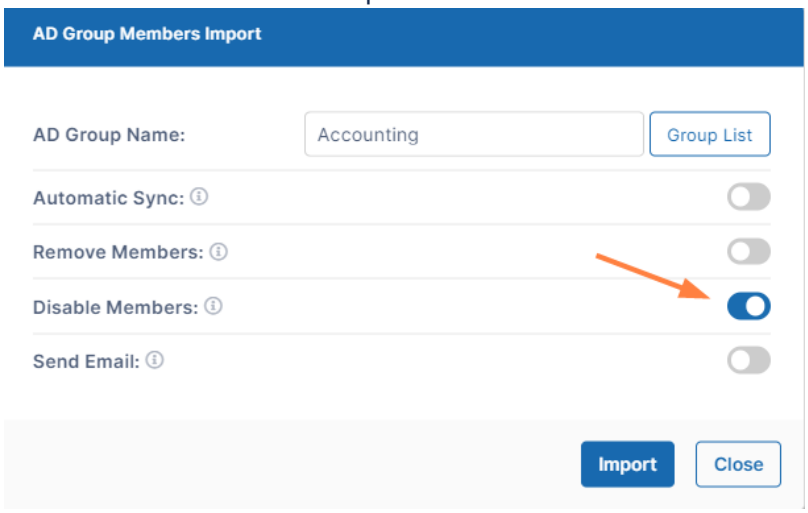
Import Disabled Users from Active Directory as Disabled

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.

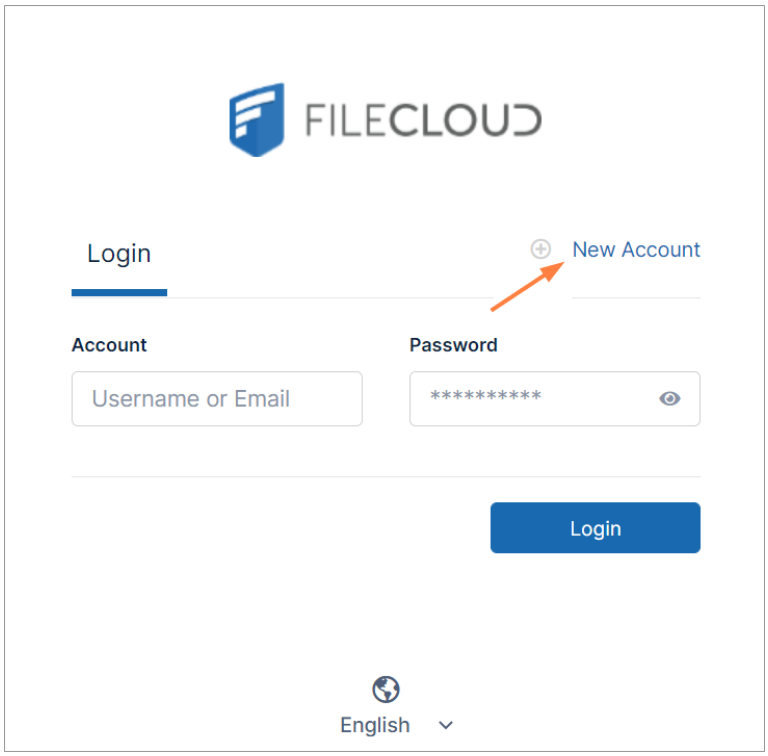
2. In then navigation panel, click **Groups**.
3. Select the **group** that you want to add users to, and then click the Edit icon.
4. On the **Members** tab, click **Import Users from AD Group**.
5. In **AD Group Name**, enter the AD group to import.
6. Enable the **Disable Members** option.



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**.

New Account Creation

By default, a **New Account** button appears on the log-in page that users can click to create or sign up for a new account.



Administrators can customize how new user accounts are created.

If you are enabling FileCloud users to create new accounts when sharing with external individuals, and SMS 2FA is enabled, you must add a setting that allows the user to enter the individual's phone number with the share. To add the setting, see the section **Enable Two Factor Authentication for User Portal (Global setting)** in Two-Factor Authentication.

Who can create and approve accounts

New account settings

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		• Local users (who are not using AD or LDAP authentication) cannot create their own accounts. **True** = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed	

Setting	Location	Options	Description
		• LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	💡 If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

Scenarios

FileCloud supports the ability to customize the creation of user accounts in the following ways:

- Only an Administrator can create new user accounts.
- Users can create their own account but it is disabled. An administrator approves it or denies approval by deleting it.
- Users can create and approve their own accounts.
  - With a default level of access set by an administrator.
  - When Share invitations are sent to new users.
- AD or LDAP users can create a new FileCloud account different from their AD or LDAP credentials.

Table 2. Only an Admin Creates New Accounts

Only an Admin can create (or deny) User accounts
1. The administrator enables the account in the Admin Portal on the Users page by changing the user's status from **Disabled Access** to one of the enabled access statuses. 2. The user receives a Welcome email with the account credentials and user portal URL. Note: An administrator denies approval by deleting a user account. In this case the user receives an email to inform them that the account has not been approved.
Customization settings, Login tab New Account button = DISABLED **Admin settings** Allow Account Signups = False Automatic Account Approval = No automatic approval. Admin has to approve account.

The scenarios where a user can create a new FileCloud account are described in Table 3.

Table 3. Users Can Create New Accounts

Users can create their own accounts

Users can create their own accounts **The Admin must approve the accounts** **💡 This scenario can also be used to allow new users to create an account when a Share invitation is sent.**	**Users can create their own accounts** **Users can approve their own accounts** **💡 This scenario can also be used to allow new users to create an account when a Share invitation is sent.**	**Active Directory or LDAP** **Users create a new FileCloud account different from their AD or LDAP credentials** **The Admin can configure the approval process**

⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users.

1. The Administrator configures the User Search Mode.
2. The Administrator configures New Account Creation settings.
3. The Administrator provides the user with the URL for the User Portal OR an invitation to create a new account is sent when a user shares a folder or file.
4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app.
5. On the user portal login window, the user clicks the New Account button.
6. The user enters details in the account creation fields.
7. The account is created but is disabled by default.
8. The Admin will be notified about the new account.
9. The Admin will approve the account.
10. The Admin will set the user account type to Full or Guest.
11. The user will receive an account creation email using the email address provided during account creation.
12. The user is required to verify the email account to complete the account creation process.

⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users.

1. The Administrator configures the User Search Mode.
2. The Administrator configures New Account Creation settings.
3. The Administrator provides the user with the URL for the User Portal OR an invitation to create a new account is sent when a user shares a folder or file.
4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app.
5. On the User Portal Login window, the user clicks the New Account button.
6. The user enters details in the account creation fields.
7. The account is created and is granted access of a Full, Guest, or External User as set by the Administrator in Settings > Admin.
8. The Admin is notified about the new account.
9. The user will receive an account creation email using the email address provided during account creation.
10. The user is required to verify the email account to complete the account creation process.

1. The Administrator configures the Authentication Type as Active Directory or LDAP.
2. The Administrator imports AD or LDAP user accounts into FileCloud.
3. The Administrator provides the user with the URL for the User Portal.
4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app.
5. On the User Portal Login window, the user clicks the New Account button.
6. The user enters details in the account creation fields.
7. The account is created and is either disabled OR granted access of a Full, Guest, or External User as set by the Administrator in Admin settings.
8. The Admin is notified about the new account.
9. The user will receive an account creation email using the email address provided during account creation.
10. The user is required to verify the email account to complete the account creation process.

Settings, Users settings ✅ User Account Search Mode = Exact Email with Implicit Account Invite OR Exact Email with Explicit Account Invite **Settings, Authentication settings** ✅ Authentication Type = DEFAULT **Customization settings, Login tab** ✅ New Account button = ENABLED **Settings, Admin settings** ✅ Allow Account Signups = True ❌ Automatic Account Approval = No automatic approval. Admin has to approve account.	**Settings, Users settings** ✅ User Account Search Mode = Exact Email with Implicit Account Invite OR Exact Email with Explicit Account Invite **Settings, Authentication settings** ✅ Authentication Type = DEFAULT **Customization settings, Login tab** ✅ New Account button = ENABLED **Settings, Admin settings** ✅ Allow Account Signups = True ✅ Automatic Account Approval = Automatically approve new accounts to Full, Guest, or External User Set **Create account on new user share** to **true** in the policy.	**Settings, Authentication settings** ✅ Authentication Type = ACTIVE DIRECTORY or LDAP **Customization settings, Login tab** ✅ New Account button = ENABLED **Settings, Admin settings** ✅ Allow Account Signups = Default ℹ Automatic Account Approval = any value

The scenarios where FileCloud automatically creates a new user account are described in Table 4.

Table 4. Automatic Account Creation

FileCloud automatically creates a new FileCloud account for Active Directory or LDAP Users on First Login
1. The Administrator configures the Authentication Type as Active Directory or LDAP. 2. (Optional) The Administrator imports AD or LDAP user accounts into FileCloud. 3. The Administrator provides the user with the URL for the User Portal. 4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the User Portal Login window, the user enters their AD or LDAP username and password. 6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.
Settings, Authentication settings ✅ Authentication Type = ACTIVE DIRECTORY or LDAP **Customization settings, Login tab** ✅ New Account button = ENABLED **Settings, Admin settings** ✅ Allow Account Signups = Default ✅ Automatic Account Approval = Automatically approve new accounts to Full or Guest User.

Also in this section:

Account Approval

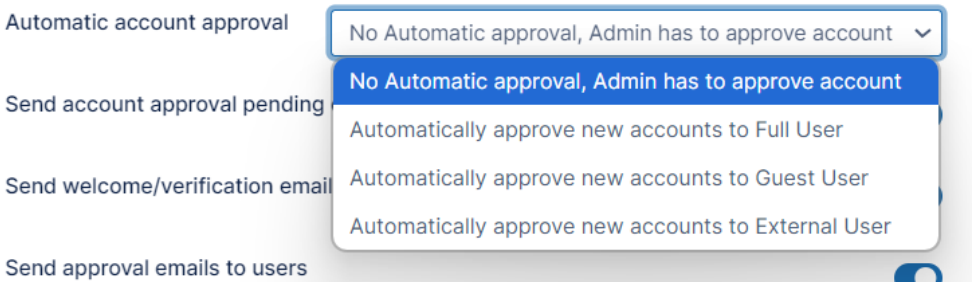
This feature is used to allow automatic account creation by a user who clicks the **New Account** button in user portal login page.

The admin can set account approval in the **Automatic account approval** field in the Admin settings page.

Account approval settings

To set Automatic account approval:

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 the **Automatic account approval** field.
3. Choose one of the values shown below:



Value	Description
No Automatic approval, Admin has to approve account	Default. The account can be created by the user but the user cannot log in. The account requires admin approval for the user to access it.
Automatically approve new accounts to Full User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has Full User permission.
Automatically approve new accounts to Guest User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has Guest User permission. Later the admin can change the permission to Full User permission.

Value	Description
Automatically approve new accounts to External User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has External User permission.

To know more about the difference between Full, Guest and External users, see the User Access page.

No Automatic approval, Admin has to approve account

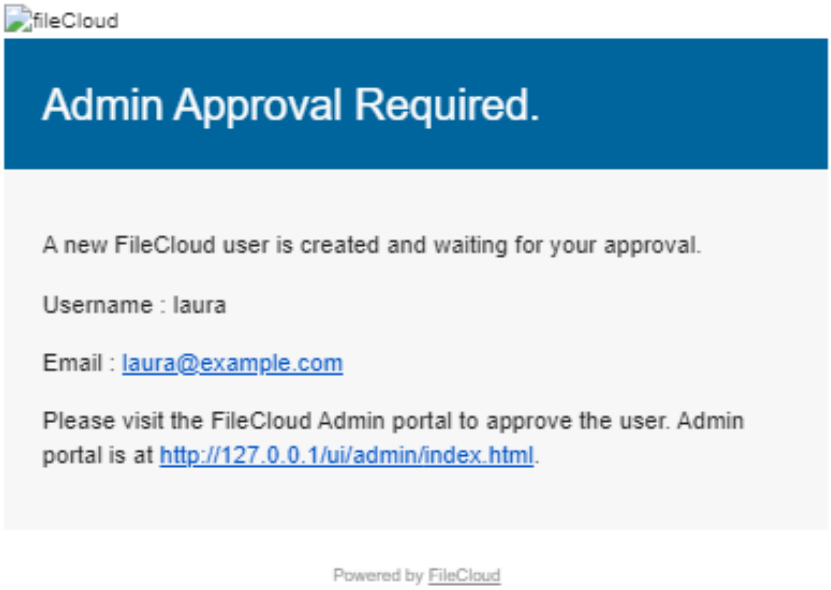
In this mode the user can create an account to access FileCloud but cannot log in until the admin approves the account, so the system sends an Approval Pending email to the admin. Once the admin approves the user, the user receives an Approval email, and can log in and access FileCloud.

Note

- Approval emails are sent only if the option **Send account approval pending emails** is enabled in the admin portal in the Admin settings page. The setting is enabled by default.
- If **Send account approval pending emails** is disabled, the admin is not notified about account creation. In this case, new accounts are approved only when admin user logs in.
- If **Send account approval pending emails** is enabled, the emails are sent to the Admin email in the Admin settings page.

Approving an account as an admin

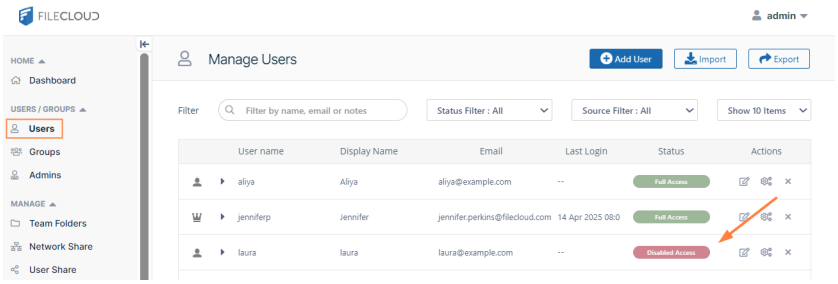
When users create their own accounts and the Admin setting field **Automatic account approval** is set to the default value of **No Automatic approval, Admin has to approve account**, by default you are sent an email to your admin account informing you that a new user has been created an your approval is required to enable it:



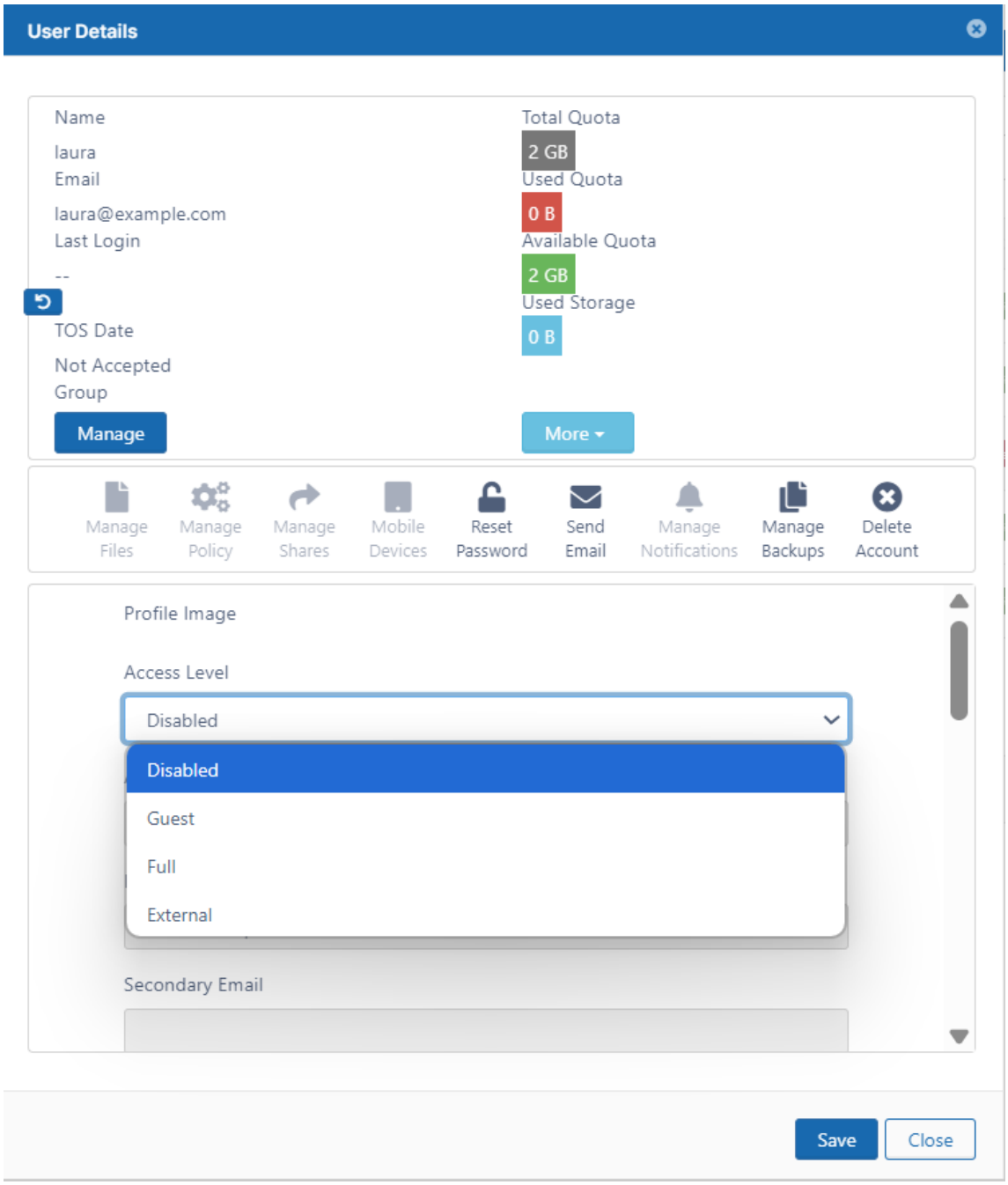
If you disable the **Send account approval pending emails** field in the Admin settings page, FileCloud does not notify you that a new account has been created, and you must be notified by a user or browse for new, disabled users in the Manage User page when you log in.

To approve a new, disabled user:

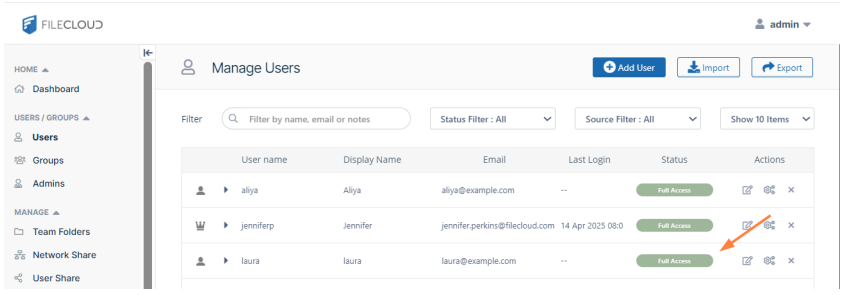
1. In the admin portal, in the navigation panel, click **Users**, and in the Manage Users page, locate the new user, who will have disabled access.



2. To open the **User Details**, click the edit icon for the user.
3. Change the **Access Level** from **Disabled** to one of the access levels with permissions.



The user is now approved and can log in to and use FileCloud.



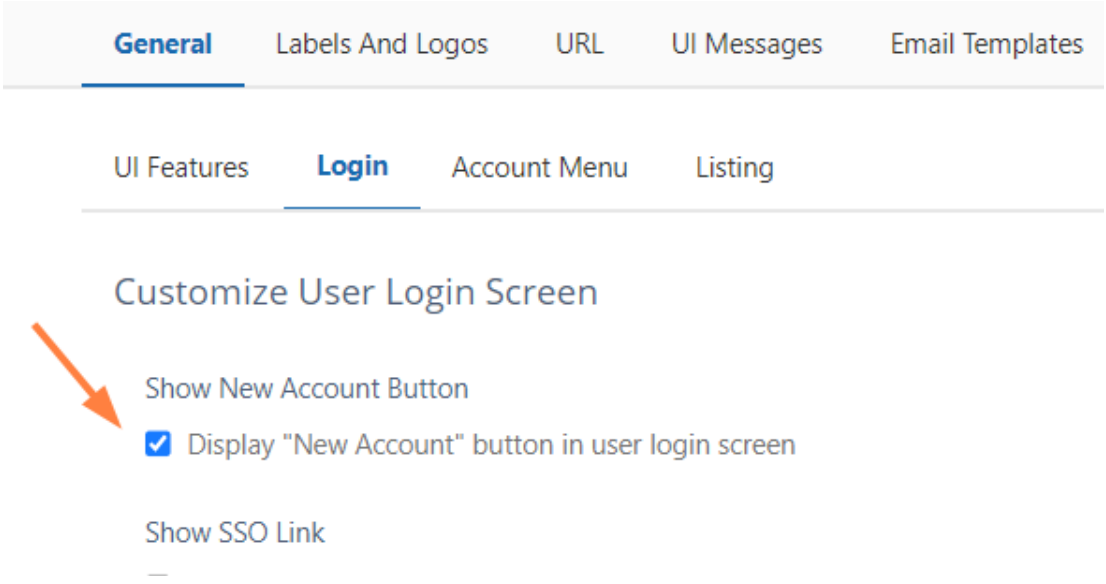
Allow AD or LDAP Users to Create a New Account

Administrators can allow AD or LDAP users to create a new FileCloud user account in one of the following ways:

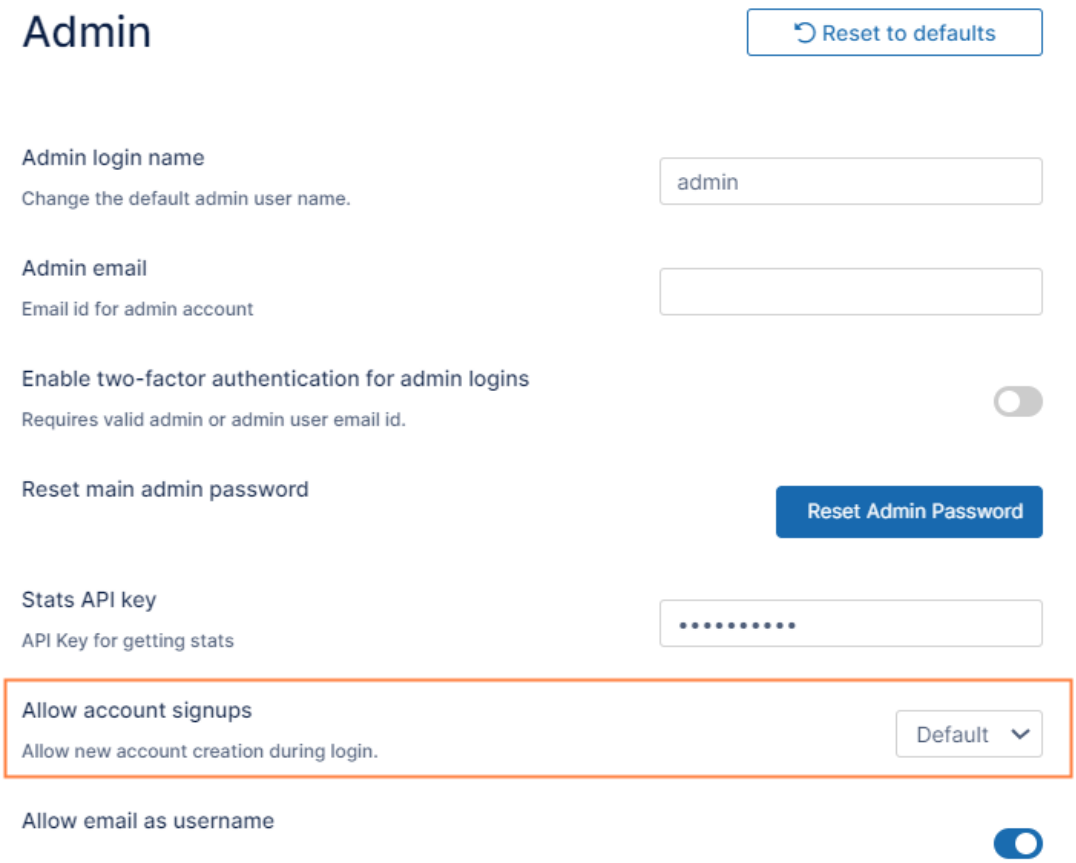
- Have FileCloud automatically create a new FileCloud account for AD or LDAP Users on first login (credentials are the same as their AD or LDAP credentials)
- Active Directory or LDAP users create a new FileCloud account different from their AD or LDAP credentials

To allow an AD or LDAP user to create a new FileCloud user account:

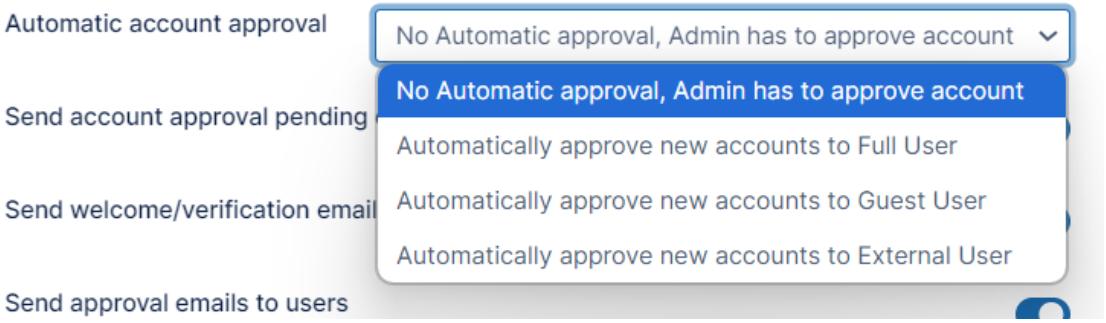
1. Set up AD or LDAP based authentication following the instructions in Active Directory Authentication or LDAP Based Authentication.
2. In the FileCloud admin portal, go to **Customization > Login**.
3. Check **Show New Account Button**.



4. Now, in the FileCloud admin portal, go to **Settings > Admin**.
5. In **Allow account signups**, select **Default**.



6. To set an approval method, in **Automatic account approval**, choose a value.



The user is notified by email when:

- Trying to connect (when admin approval is pending)
- When the admin has approved the device trying to connect

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		• Local users (who are not using AD or LDAP authentication) cannot create their own accounts. **True** = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed	

Setting	Location	Options	Description
		• LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	💡 If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

You can allow AD and LDAP users to create accounts with their AD and LDAP credentials or with different credentials.

Admins want FileCloud to automatically create a new FileCloud account for their Active Directory or LDAP Users on first login	**Active Directory or LDAP Users create a new FileCloud account different from their AD or LDAP credentials The Admin can configure the approval process**
1. The administrator configures the **Authentication type** as **Active Directory** or **LDAP**. 2. (Optional) The administrator imports AD or LDAP user accounts into FileCloud. 3. The administrator provides the user with the URL for the user portal. 4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client application. 5. On the login window, the user enters their AD or LDAP username and password. 6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.	1. The administrator configures the **Authentication Type** as **Active Directory** or **LDAP**. 2. (Optional) The administrator imports AD or LDAP user accounts into FileCloud. 3. The administrator provides the user with the URL for the user portal. 4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client application. 5. On the user portal login window, the user clicks the **New Account** button. 6. The user enters details in the account creation fields. 7. The account is created and is either disabled OR granted access of a Full User, Guest User, or External User as set by the administrator. 8. The admin is notified about the new account. 9. The user receives an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.
Settings, Authentication settings ✅ Authentication type = Active Directory or LDAP **Customization > Login** ✅ New Account button = Enabled **Settings, Admin settings** ✅ Allow account signups = Default ✅ Automatic account approval = The new user account is automatically approved with **Full** or **Guest** access.	**Settings, Authentication settings** ✅ Authentication Type = Active Directory or LDAP **Customization > Login** ✅ New Account button = Enabled **Settings, Admin settings** ✅ Allow Account Signups = Default ℹ Automatic Account Approval = any choice

For more information:

Configure Active Directory

Configure LDAP

Configuring a Scenario

FileCloud supports the following authentication modes:

- Default authentication
- Active Directory based authentication
- LDAP based authentication

The following table describes how each authentication mode impacts the users' ability to create a new account.

	Default Authentication	**AD**	**LDAP**
Authentication	Performed by FileCloud Server	In AD Server	In LDAP Server
Users can Create Accounts	Permitted	Not Permitted	Not Permitted
User Account Types	Full, Guest, External	Full, Guest	Full, Guest

Prerequisites

- Active Directory or LDAP service must be accessible from FileCloud (IP and Port must be accessible)
- Active Directory or LDAP must support Simple Authentication Method (Anonymous or Name/ Password Authentication Mechanism of Simple Bind)
- Active Directory or LDAP users must have an email attribute

Allow Only an Admin To Create New Accounts

Administrators can customize how new user accounts are created.

In this scenario, you will configure the FileCloud site so that only administrators can create new accounts.

The settings that you use to configure this scenario is described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		• Local users (who are not using AD or LDAP authentication) cannot create their own accounts. **True** = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

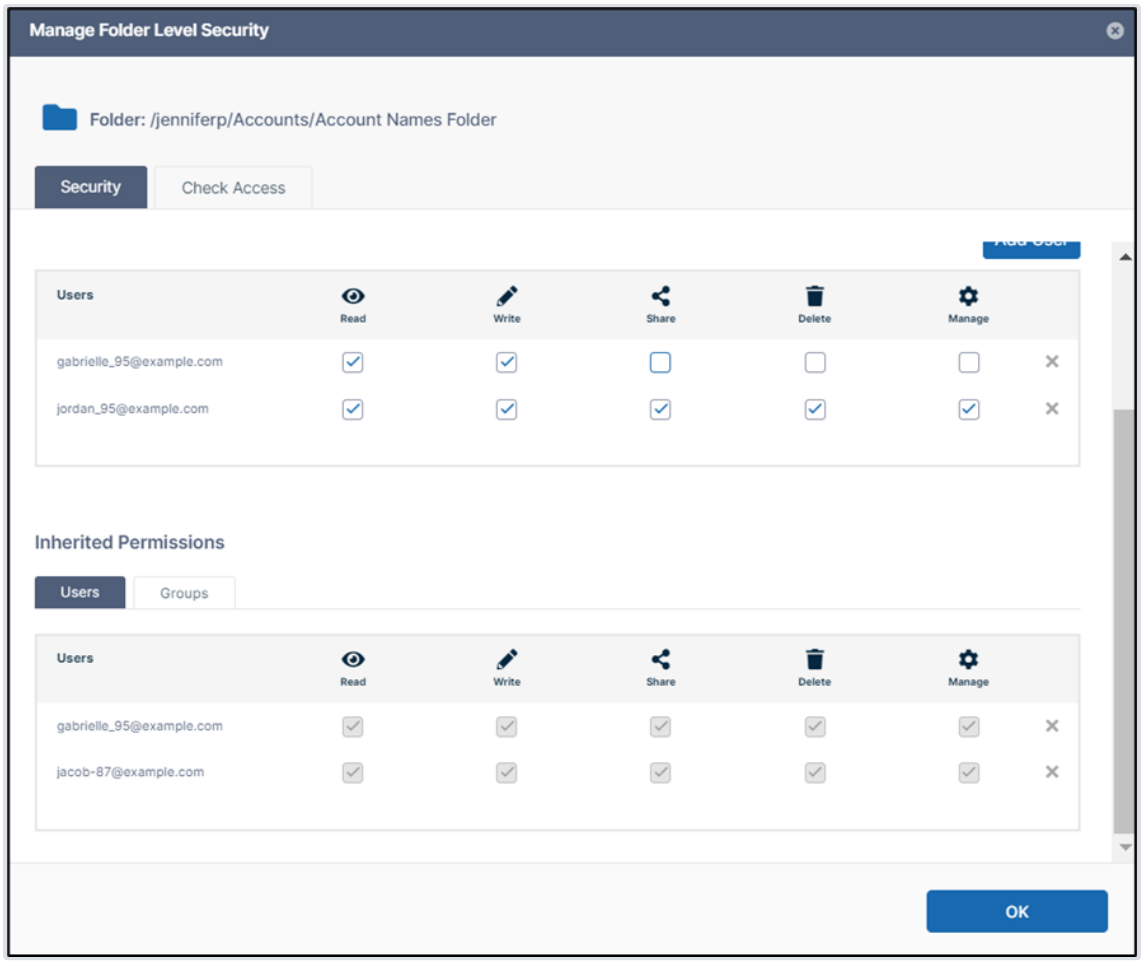
The scenario where only an administrator creates a new FileCloud account is described in the following table.

Only an Admin can create User accounts
1. The administrator creates the account in the admin portal. 2. The user receives a Welcome email with the account credentials and user portal URL.
Customization > Login New Account button = Disabled **Settings, Admin settings** Allow Account Signups = False Automatic Account Approval = No automatic approval, Admin has to approve account.

In this scenario, if you disable the **New Account** button, then the other settings can be left set to their defaults.

To configure these settings:

1. Log into the admin portal.
2. In the left menu panel, click **Customization**.
3. On the **General** tab, click the **Login** tab.
4. Make sure the **Show New Account Button** checkbox is not selected.
   FileCloud server will not display the **New Account** button in the user portal.



Allow Users to Create and Approve Accounts

Administrators can customize how new user accounts are created.

This scenario:

- allows users to create and approve their own accounts.
- allows an administrator set a default level of access.

- may be useful in systems where share invitations are sent to new users.

This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users.

The settings that you use to configure these scenarios are described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		• Local users (who are not using AD or LDAP authentication) cannot create their own accounts. **True** = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed	

Setting	Location	Options	Description
		• LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	💡 If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

The scenarios where a user can create a new FileCloud account are described in the following table.

Users can create their own accounts
Users can approve their own accounts
This scenario can also be used to allow new users to create an account when a Share invitation is sent.

⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users.

1. The administrator configures the User Search Mode.
2. The administrator configures New Account Creation settings.
3. The administrator provides the user with the URL for the user portal OR an invitation to create a new account is sent when a user shares a folder or file.
4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client app.
5. On the user portal login window, the user clicks the **New Account** button.
6. The user enters details in the account creation fields.
7. The account is created and is granted access of a Full User, Guest User, or External User as set by the Administrator.
8. The user receives an account creation email using the email address provided during account creation.
9. The user is required to verify the email account to complete the account creation process.

Settings, Misc > User settings

✅ User Account Search Mode = **Exact Email with Implicit Account Invite** or **Exact Email with Explicit Account Invite**

Settings, Authentication settings

✅ Authentication Type = DEFAULT

Customization > Login

✅ New Account button = ENABLED

Settings, Admin settings

✅ Allow Account Signups = TRUE

✅ Automatic Account Approval = Automatically approve new accounts to Full/Guest/External User.

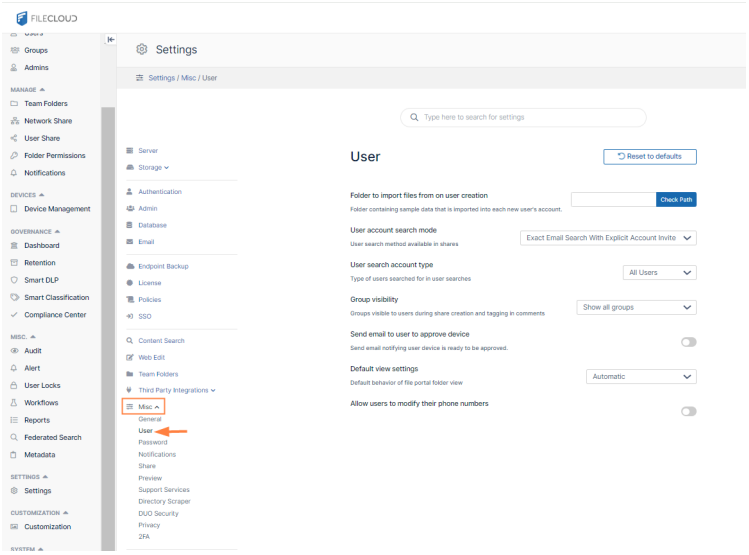
Settings, Policies

✅ Set **Create account on new user shares** to **yes** in users' policies.

To configure these settings:

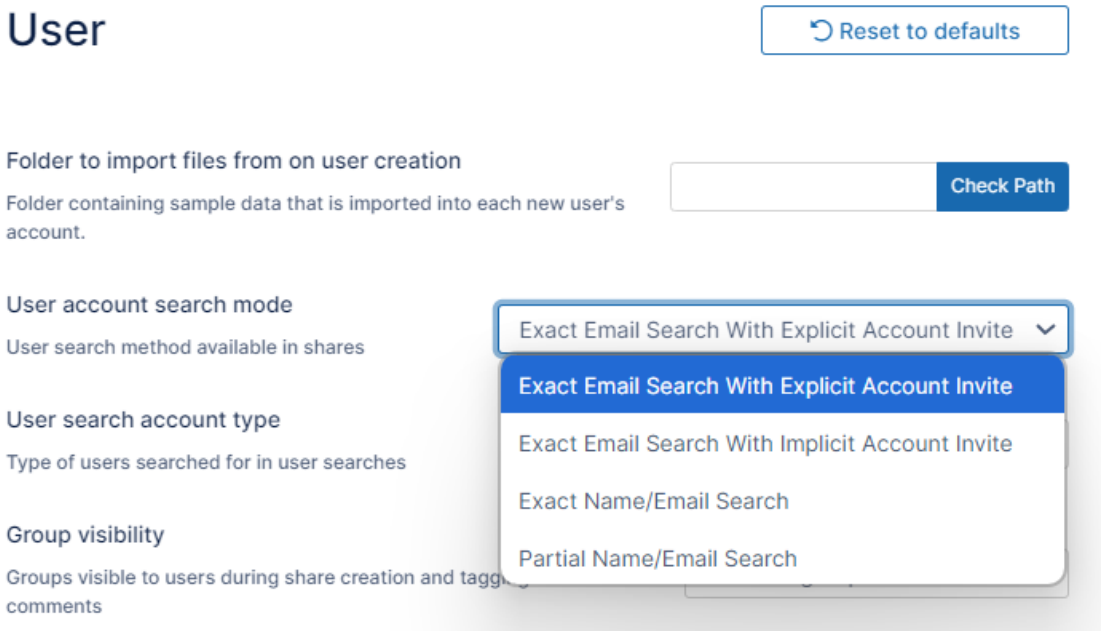
1. Open the User settings page.
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**

   .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **User**, as shown below.



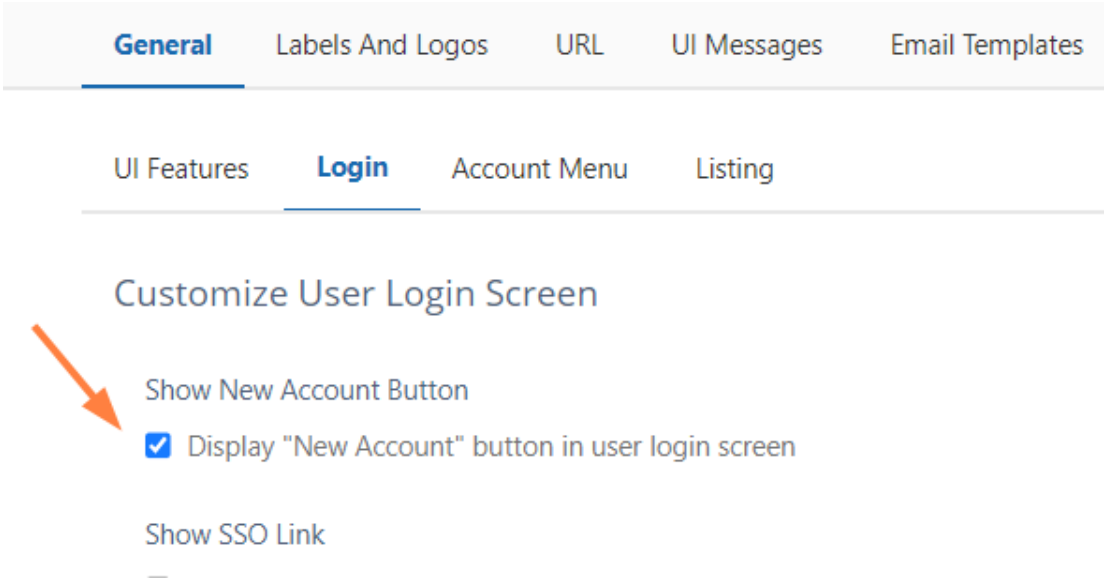
The **User** settings page opens.

2. In **User Account Search Mode**, select **Exact Email Search with Explicit Account Invite** or **Exact Email Search with Implicit Account Invite**.



Click **Save**.

3. In the FileCloud admin portal's left navigation bar, go to **Customization > General > Login**.
4. Check **Show New Account Button**.



5. Click **Save**.
6. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin** UNKNOWN ATTACHMENT.
   The **Admin** settings page opens.
7. In the **Allow Account Signups** field, select **True**.



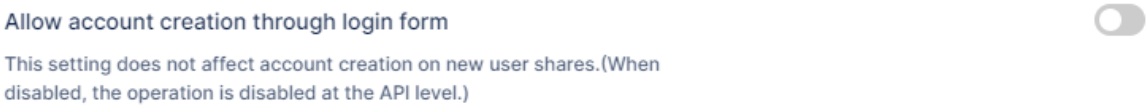
8. Click **Save**.

Blocking the createprofile API endpoint

The setting **Allow account creation through login form** has been added to enable you to block the createprofile API endpoint from the admin portal. The endpoint is used for account signups in the New Account form.

To disable the createprofile API endpoint:

1. Go to Settings > Admin.
2. Disable the **Allow account creation through login form** setting.



Allow Users to Create a New Disabled Account

Administrators can customize how new user accounts are created.

In this scenario you are allowing users to create their own accounts but they are disabled until an administrator approves them.

The settings that you use to configure this scenario are described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		• Local users (who are not using AD or LDAP authentication) cannot create their own accounts. **True** = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed	

Setting	Location	Options	Description
		• LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	💡 If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

The scenarios that enable a user to create a new FileCloud account are described in the following table.

Users can create their own accounts **The Admin must approve the accounts** **This scenario can also be used to allow new users to create an account when a Share invitation is sent.**
⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The Administrator provides the user with the URL for the User Portal. 2. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 3. On the User Portal Login window, the user clicks the New Account button. 4. The user enters details in the account creation fields. 5. The account is created but is disabled by default. 6. The Admin is notified about the new account. 7. The Admin approves the account. 8. The Admin sets the user account type to Full User or Guest User. 9. The user receives an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.
Settings, Authentication settings ✅ Authentication Type = Default **Customization settings, Login tab** ✅ New Account button = Enabled **Settings, Admin settings** ✅ Allow Account Signups = True ❌ Automatic Account Approval = No Automatic approval; Admin has to approve account

To configure these settings:

1. Log into the Administration Portal.
2. In the left menu panel, click **Customization**.
3. On the General tab, click the Login tab.
4. Make sure the **Show New Account Button** checkbox is selected.
5. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Admin** UNKNOWN ATTACHMENT.
6. Scroll down to the **Allow account signups** field, and select **True**.



The user is notified by email when:

- Trying to connect (admin approval pending)

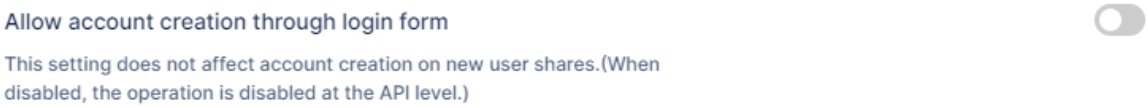
- When the administrator has approved the device trying to connect

Blocking the createprofile API endpoint

The setting **Allow account creation through login form** has been added to enable you to block the createprofile API endpoint from the admin portal. The endpoint is used for account signups in the New Account form.

To disable the createprofile API endpoint:

1. Go to Settings > Admin.
2. Disable the **Allow account creation through login form** setting.



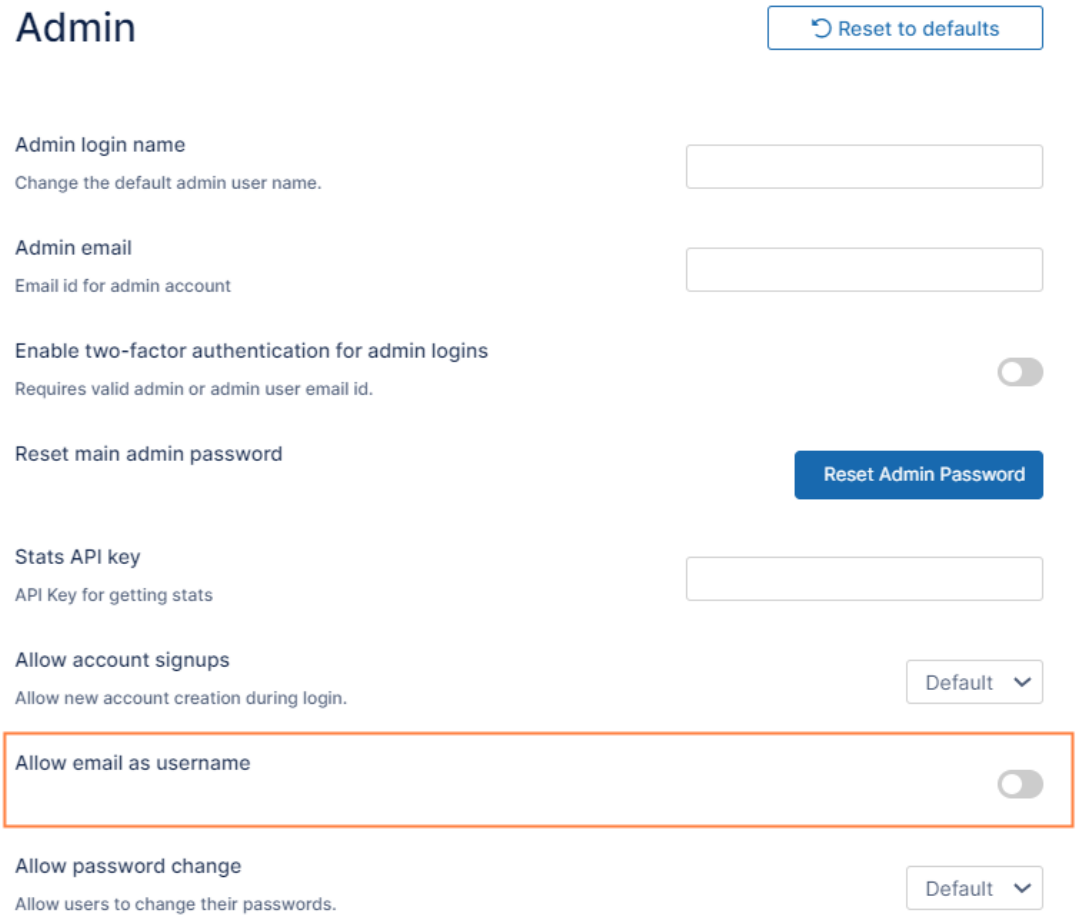
Prevent Email Addresses as Usernames

Beginning with FileCloud 23.241, **Allow Email as Username** is enabled by default.
Prior to FileCloud 23.241, **Allow Email as Username** was disabled by default.

By default, FileCloud usernames can be the same as the user's email address. You can prevent use of user's email addresses as usernames by disabling an **Admin** setting.

To prevent use of email addresses as user names:

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. Disable **Allow email as username**, and click **Save**.



Emails may no longer be used as usernames.

Prioritize Email as Username

When users are imported into FileCloud or created at login, their current usernames may be duplicates of existing ones in FileCloud. In these cases, you can prioritize using entered email over entered username as the FileCloud username to take advantage of the fact that email is always unique for each user.

When **TONIDOCLOUD_PRIORITIZE_EMAIL_AS_USERNAME** is set to **1** in the FileCloud configuration file, if **Allow account creation using the email as username** is also set, the FileCloud username is set from the entered email rather than the entered username in the following cases. However, if username is entered and email is not entered, username is used.

- Account is created on SSO login
- Account is created on AD login
- Account is created on AD import

- Account is created on a share invite

Notes: Email will not be prioritized over username when the user is created from the admin portal or on regular FileCloud login with the new account option.

To prioritize email over username:

1. In the **Settings > Admin** tab, check **Allow Email as Username**.
2. Open **cloudconfig.php**:
   Windows Location: **XAMPP DIRECTORY/htdocs/config/cloudconfig.php**
   Linux Location: **/var/www/config/cloudconfig.php**
3. Add the setting:

```
define("TONIDOCLOUD_PRIORITIZE_EMAIL_AS_USERNAME", 1);
```

Domain Limitations for External Users

Domain limitations for external users are effective for FileCloud beginning in version 22.1.
If external users have the same domains that at least 10% of licensed users have before the rule was put into effect, the external users are allowed to remain with their current emails.

Your FileCloud license limits the number of licensed (full and guest users) you can create, but allows you to create an unlimited number of external users. To prevent users from using external accounts for internal users, the system assumes that your FileCloud site domain (and its sub-domains and sibling domains) and any domain used by at least 10% of your licensed (full and guest) users are internal domains, and therefore prevents you from creating external users with those domains.

An exception is made for popular email domains like gmail and yahoo. Unlimited numbers of external users can be created with those domains. Users with those domains are not counted when the system calculates percents of users with specific domains.

Example:
A company has a FileCloud license that permits 30 licensed (full and guest) users. The FileCloud site domain is **company456.com**.

The 30 licensed users have emails with the following domains:
company456.com - 10 users
tech123.com - 8 users
gmail.com - 8 users
factory123.com - 3 users
sullivanlaw.com - 1 user

The 8 users with gmail.com as their domain are omitted when computing the percent of users with specific domains.

The admin adds an external user with the email: **jcarr@company456.com**. This is not permitted because it has the same domain as the FileCloud site.

The admin adds an external user with the email: **mfields@tech123.com**. This is not permitted because 36% of the licensed users have the same domain.

The admin adds an external user with the email: **hbarrett@gmail.com**. This is permitted because gmail.com is a popular domain.

The admin adds an external user with the email: **bsullivan@sullivanlaw.com**. This is permitted because only 4.5% of the licensed users have the same domain.

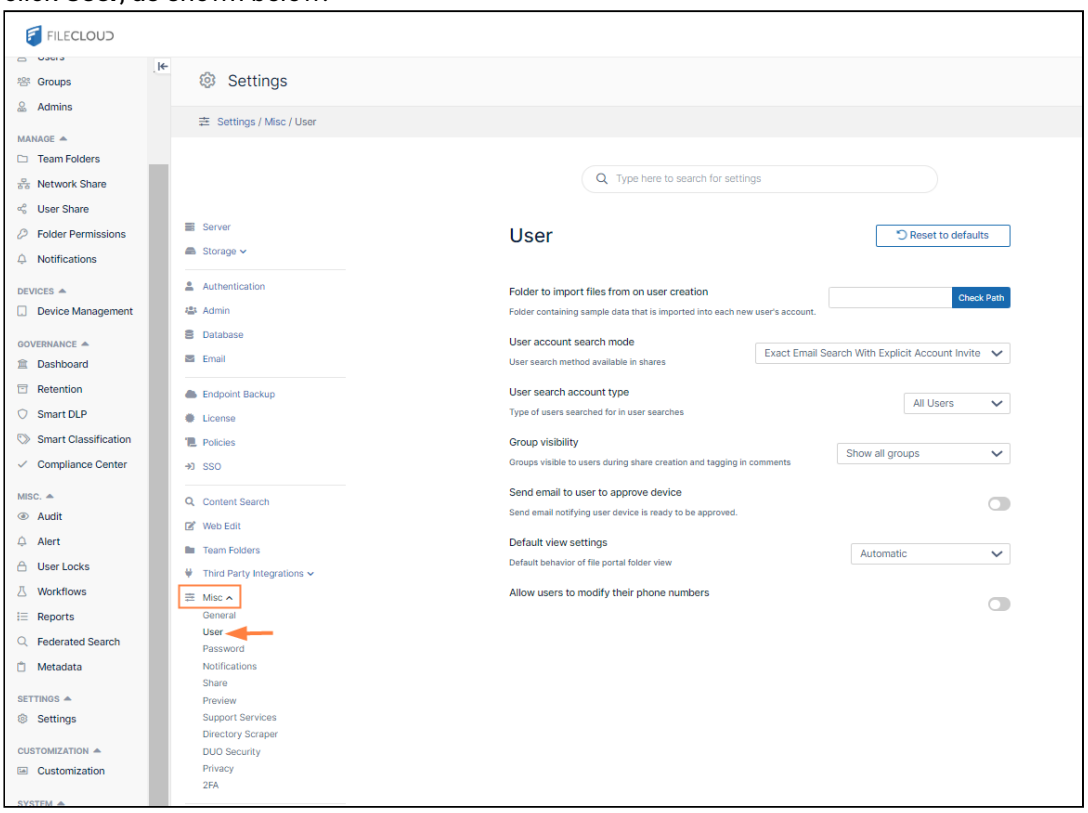
Preload data for new accounts

It is possible to preload user account with a set of sample files and folders. This could be useful to pre-populate a new user account with some help files etc.

To set up sample data folder when creating user account:

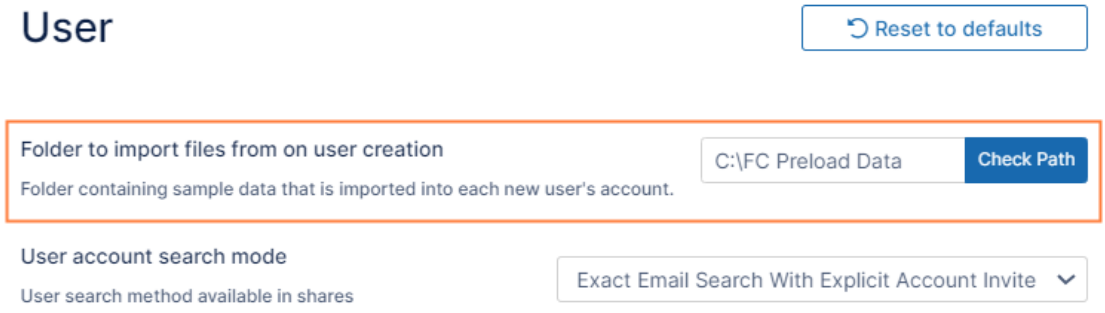
1. Open the User settings page.
   To open the User settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **User**, as shown below.



The **User** settings page opens.

2. In **Folder to import files from on user creation** enter the path containing the files and folders, and click **Save**.



Note: The following files are not imported:

1.

- Files in the server root in Linux and Windows
- In Windows, files in **xampp*** paths

- In Linux, files in the paths:
  /etc
  /var
  /usr
  /bin
  /sbin
  /lib

Password Settings

Beginning with FileCloud 23.241, the **New Accounts Must Change Password** setting is enabled by default.
Prior to FileCloud 23.241, the **New Accounts Must Change Password** setting was disabled by default.

Beginning with FileCloud 23.241, the **Skip password change on first login** setting is disabled by default.
Prior to FileCloud 23.241, the **Skip password change on first login** setting was enabled by default.

The following settings are applicable for the default FileCloud Admin, the Team Folder account and user accounts.

This section explains the password settings available in FileCloud installation.

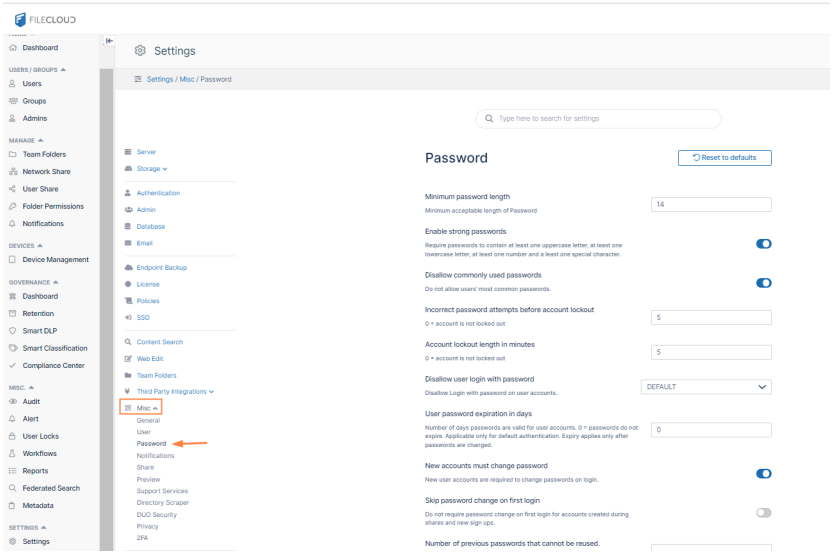
To view or change the password settings:

1. Open the **Password** settings page.

To go to the Password settings page

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

   .
2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Password**, as shown below.

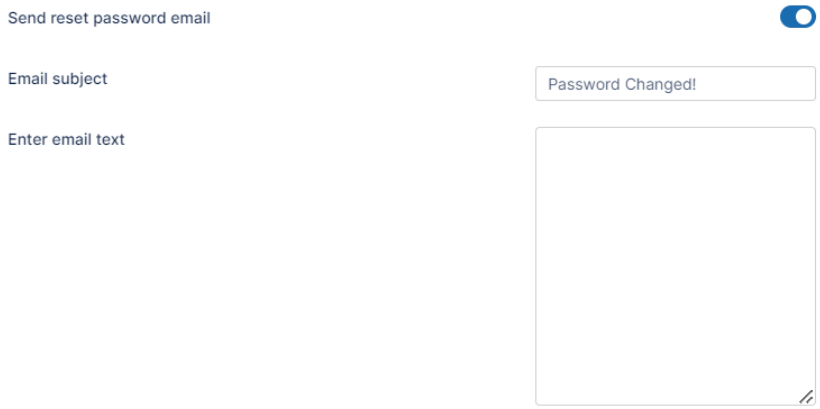


The **Password** settings page opens.

2. Change any of the settings according to your security requirements.

Type	Description
Minimum Password Length	Enforces minimum character length for password (Applies to local account and NOT to AD/LDAP accounts). Default value is 14.
Enable Strong Passwords	Enabling this will require the password to contain at least one uppercase, lowercase, number and a special character in the password. Checked by default. Applies only to local account and not to AD/LDAP account.
Disallow Commonly Used Passwords	Prevents users from using commonly used passwords for their user accounts. Enabled by default. For more information, see Restrict Commonly Used Passwords.
Incorrect attempts before account lockout	For higher security, if users try logging in with the wrong password for more than the times specified here, their account will be locked out and they cannot login even if they type in their correct password. Default value is 5. A value of 0 means account lockout with wrong password is disabled.
Account Lockout length in Minutes	Specifies time the account is locked out if wrong password is entered multiple times as specified in the option for max incorrect attempts. Default value is 5. A value of 0 means lockout is disabled.

Type	Description
Disallow user login with password	This setting will disallow login for user accounts. DEFAULT allows login with password for all users.
User Password Expires In Days	If a value above 0 is entered, when a new user is created or when a password is changed, an expiration date for the password is added automatically. NOTE: Automatic email notifications are sent to the user 7 days and 1 day before the actual password expiry date.
New accounts must change password	When enabled, this setting forces new users to change their password on initial login, with the following exceptions: • When the user creates the new account through a registration form (the user adds a password in the form). • When the user has an AD account (the user is automatically assigned an AD password). • When the user logs in using SSO. Default is enabled.
Skip password change on first login	Do not require password change on first login for accounts created during shared and new signups. Default is disabled.
Number of previous passwords that cannot be reused	Specifies the number of previous passwords that cannot be reused when password is changed. A value of 0 indicates that there are no restrictions.
Reset password attempt interval	Interval in minutes between consecutive reset password attempts. Default is 5. 0 indicates that there is no restriction.

Type	Description
Send reset password email	Allows you to create an email that is automatically sent to a user when an admin resets the user's password. There is no default email; when this is enabled, email subject and email content fields appear.  **Email subject** is set to **Password Changed!** but may be changed. The note in **Enter the text of the email below** must be entered. Disabled by default.

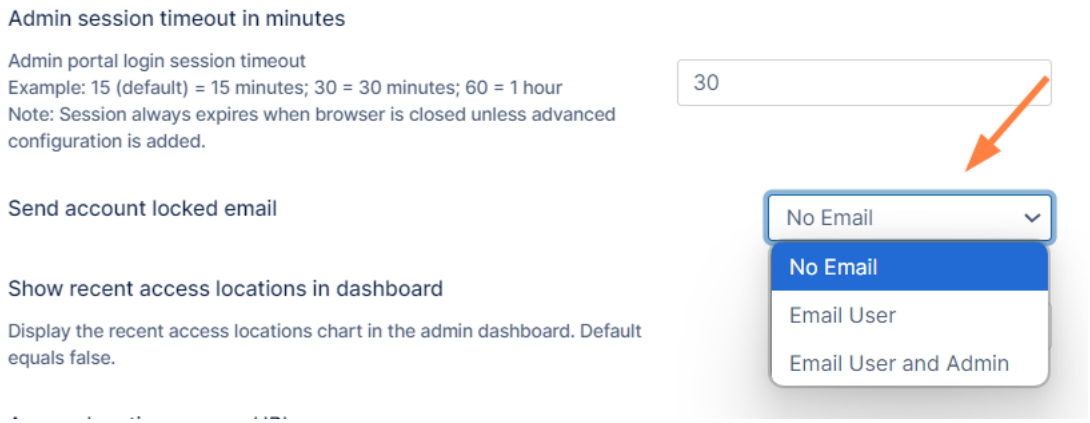
3. Click **Save**.

Setting Account Locked Alerts

By default, FileCloud is set to not send an email message to the user or admin to notify them that the account has been locked due to incorrect login attempts. However, you may change this setting.

To change the **Account Locked Alert** setting:

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 the **Send account locked email** setting.



3. In the drop-down list, choose one of the following settings:
   No Email - Neither the user nor the admin receives an email notification about the user account lockout.
   Email User - The user receives an email notification about their account lockout but the admin does not.
   Email User and Admin - Both the user and the admin receive an email about the user account lockout.

Restrict Commonly Used Passwords

Anytime a password is created or updated, before the password is accepted, FileCloud Server checks the suggested password against the US NIST Password Guidelines list.

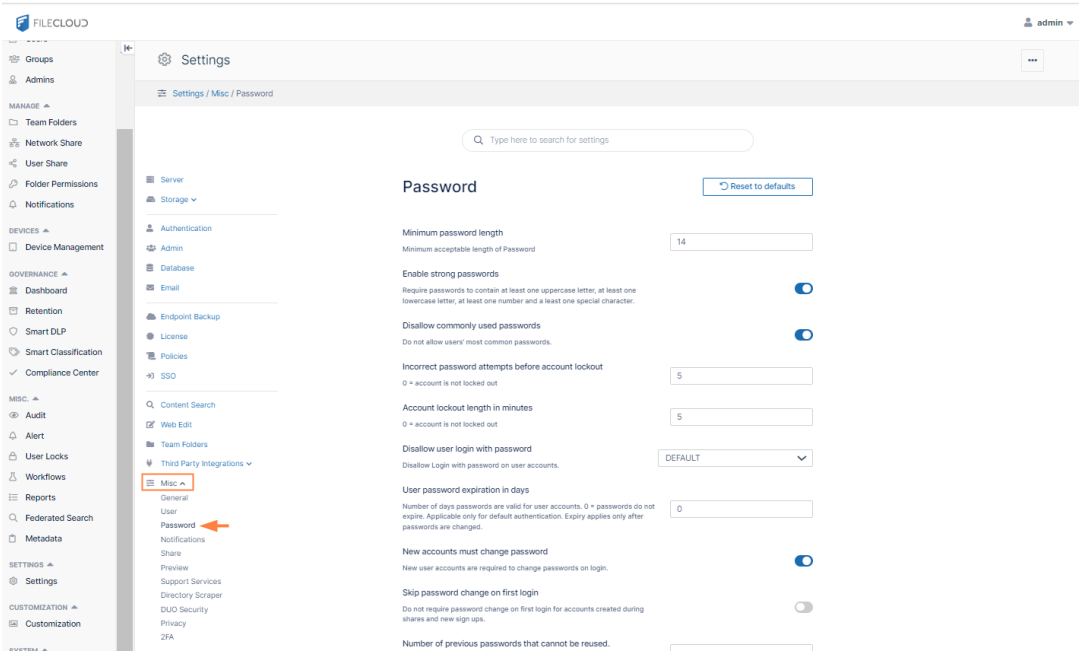
- This feature can be enabled or disabled by the administrator in the admin portal.
- The option is called **Disallow commonly used passwords** and if enabled it will prevent users from setting commonly used passwords for their user accounts.

The password entered is checked against the password guidelines list when:

- A new user is added.
- A user's password or the admin password is updated.
- The password is reset.
- User are imported using a CSV file.

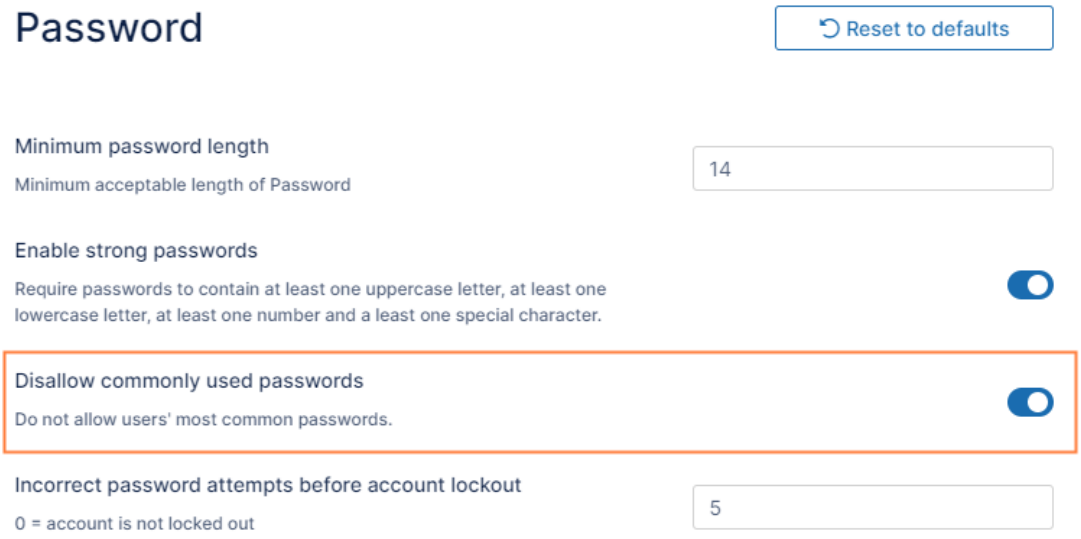
To set this option:

1. Go to the **Password** settings page.
   To go to the Password Settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Misc** page, expand the **Misc** menu, and click **Password**, as shown below.



The **Password** settings page opens.

2. Enable **Disallow Commonly Used Passwords**.



3. Click **Save**.

User Session Expiration

Default Behavior

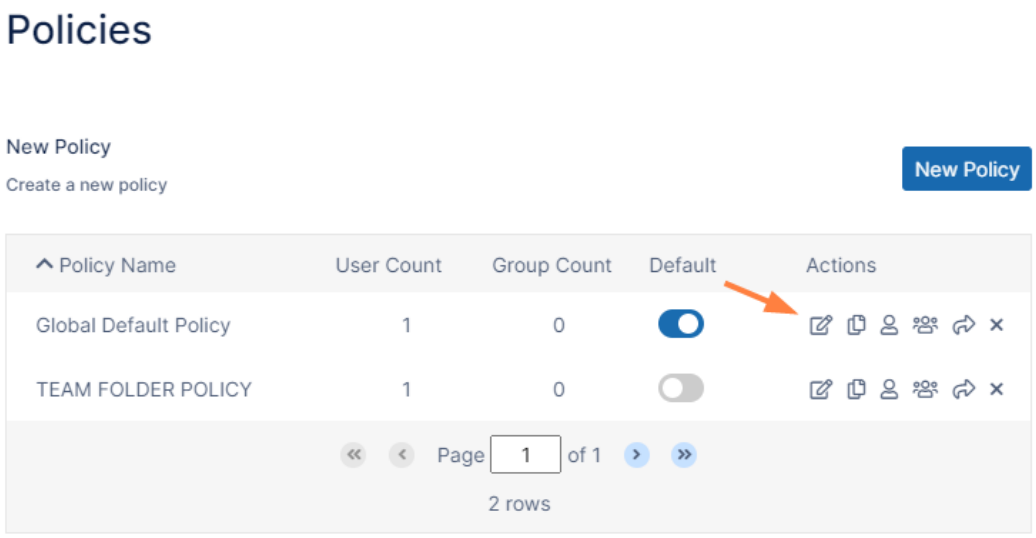
By default, when a user logs into FileCloud, their session remains authenticated for a specified amount of time.

Device	Time Session is Valid
User portal (web browser)	Specified by the value in Session Timeout in minutes setting. If the browser is closed, the session expires.
All other apps and clients	Doesn't expire. Session lasts until user logs out from app.

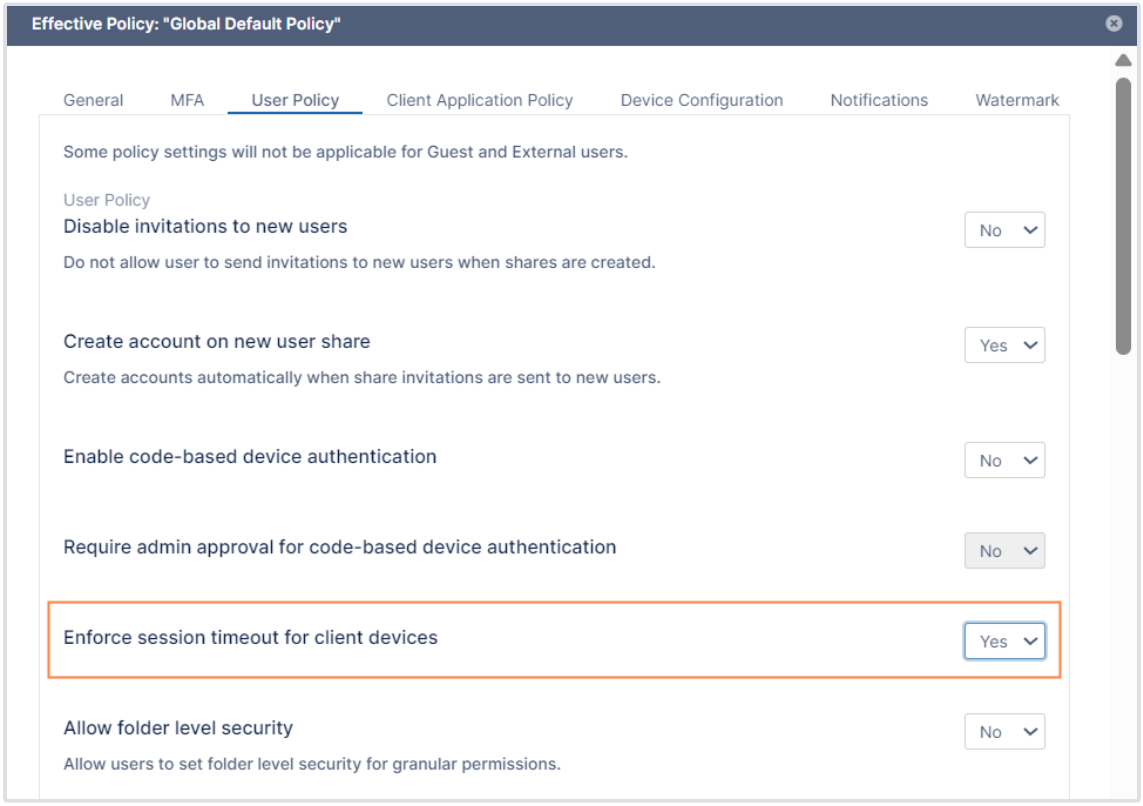
Enabling Session Expiration for all Devices

If you want all login sessions on FileCloud user client devices to expire and require re-login, set the policy to **Enforce session timeout for client devices**.

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. Click the Edit icon in the row for the users' policy.



3. Click the **User Policy** tab.
4. Set **Enforce session timeout for client devices** to **yes**.



5. Click **Save**.

Note: We don't recommend requiring session expiration for devices and other clients as it might impact functionality and reduce user friendliness.

Device	Time Session is Valid
Web Browser	Specified by the value in Session Timeout in minutes setting. If the browser is closed, the session expires.
All other apps and clients	Specified by the value in Session Timeout in minutes setting. Note: When log in used username and password, app will automatically re-login, so the session will not appear to expire. When log in used Device Authorization code, app will require user to re-login into FileCloud using the web browser.

Disabling Session Expiry when Browser is closed

Session expiry time is valid until timeout setting expires or the browser is closed. If the browser is reopened, the user must log in again.

If session should be valid even when the browser is closed, set the following config parameter to extend the browser timeout setting. For correct behavior, set this value to be significantly larger than the session timeout value, for example, if the session timeout is 30 days, then set this configuration to 90 days.

define("TONIDOCLOUD_BROWSER_COOKIE_TIMEOUT", 86400); // time in seconds that browser remains logged in irrespective of whether browser is closed

Changing the Storage Quota for Users

Administrators can manage the storage space allotted to a user account or a group of users through Policies.

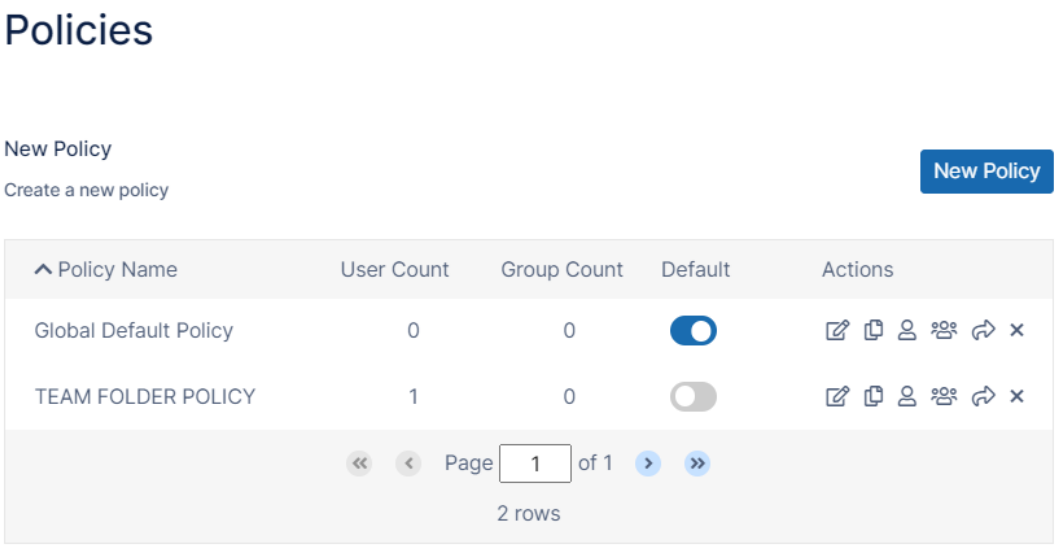
- Use the Global Default policy to set a quota for all user accounts
- Use a custom policy to set a quota for a specific user or for a select group of users

Set a Quota for a Specific User

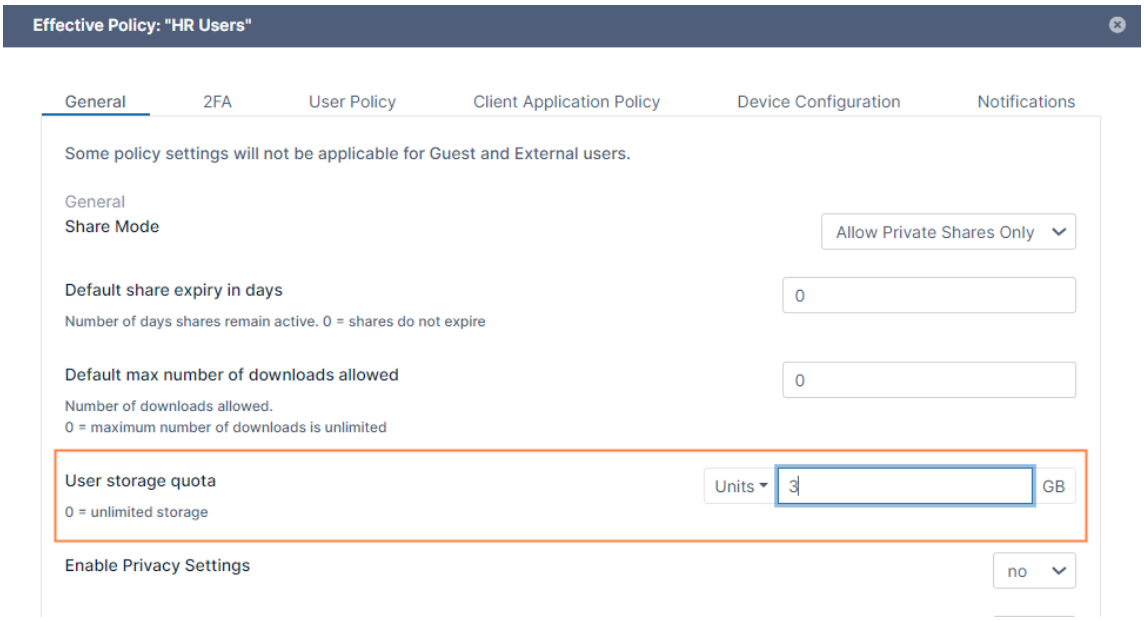
To set a storage quota for a specific user, create a custom policy and assign the user to that policy.

Create a Custom Policy for one user

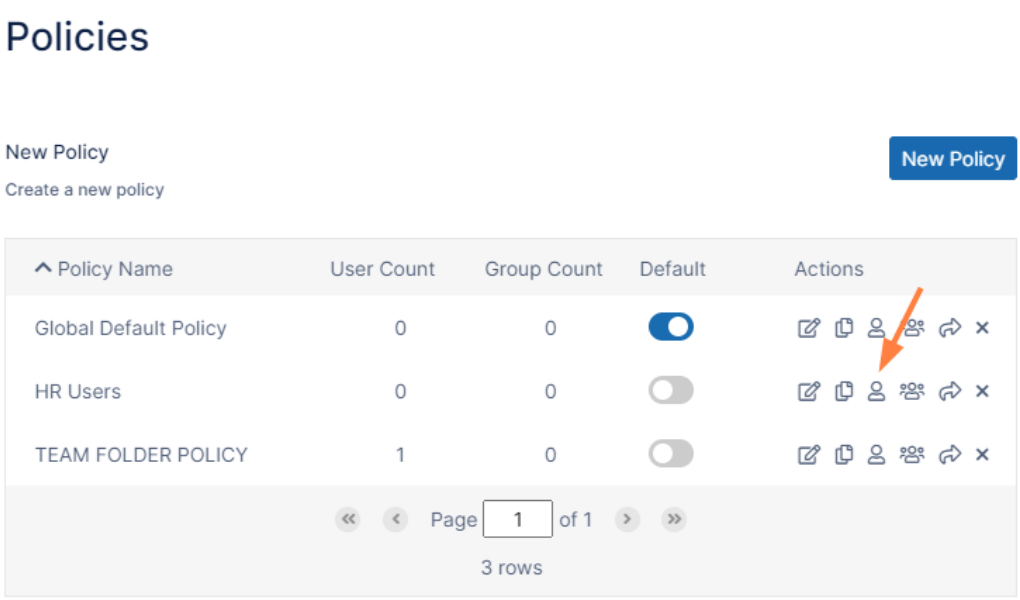
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.



2. Create the custom policy. See Policies.
3. Click the edit icon for the new policy, and in the **General** tab, in the **User storage quota** field, enter the storage quota for the user.

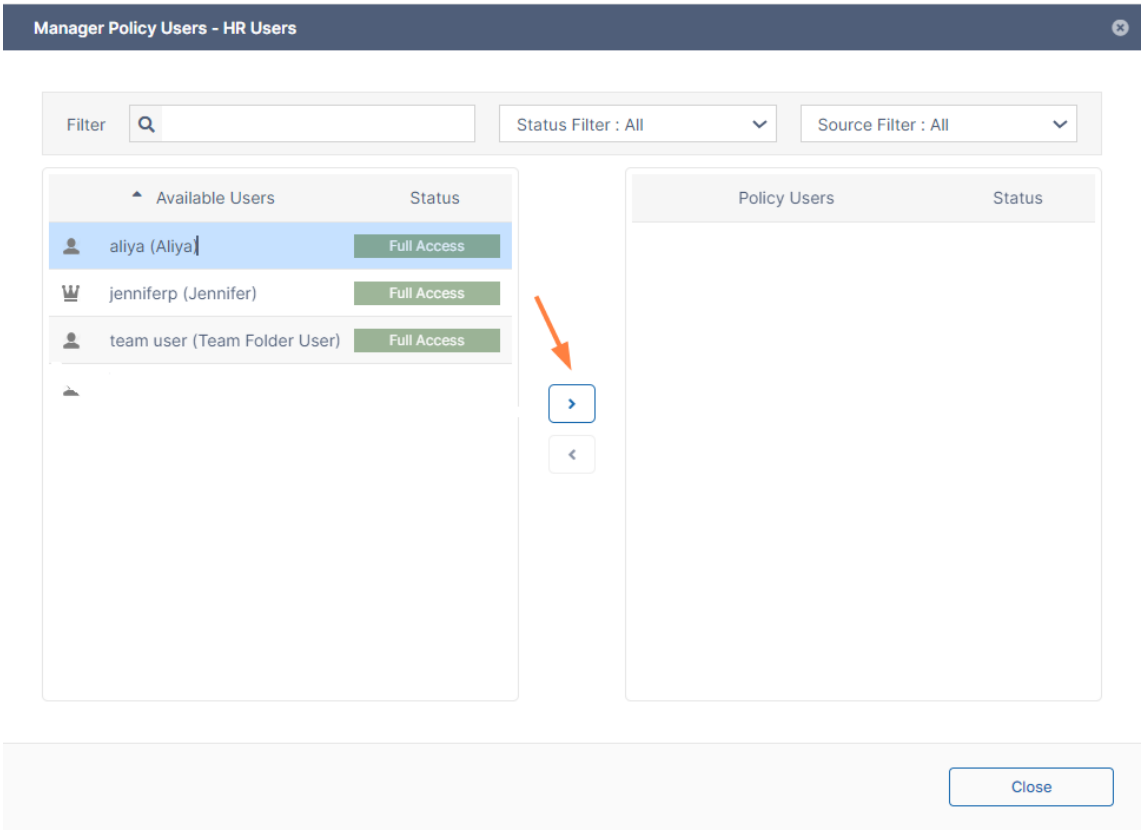


4. Click **Save**.
5. Click the user icon for the policy.



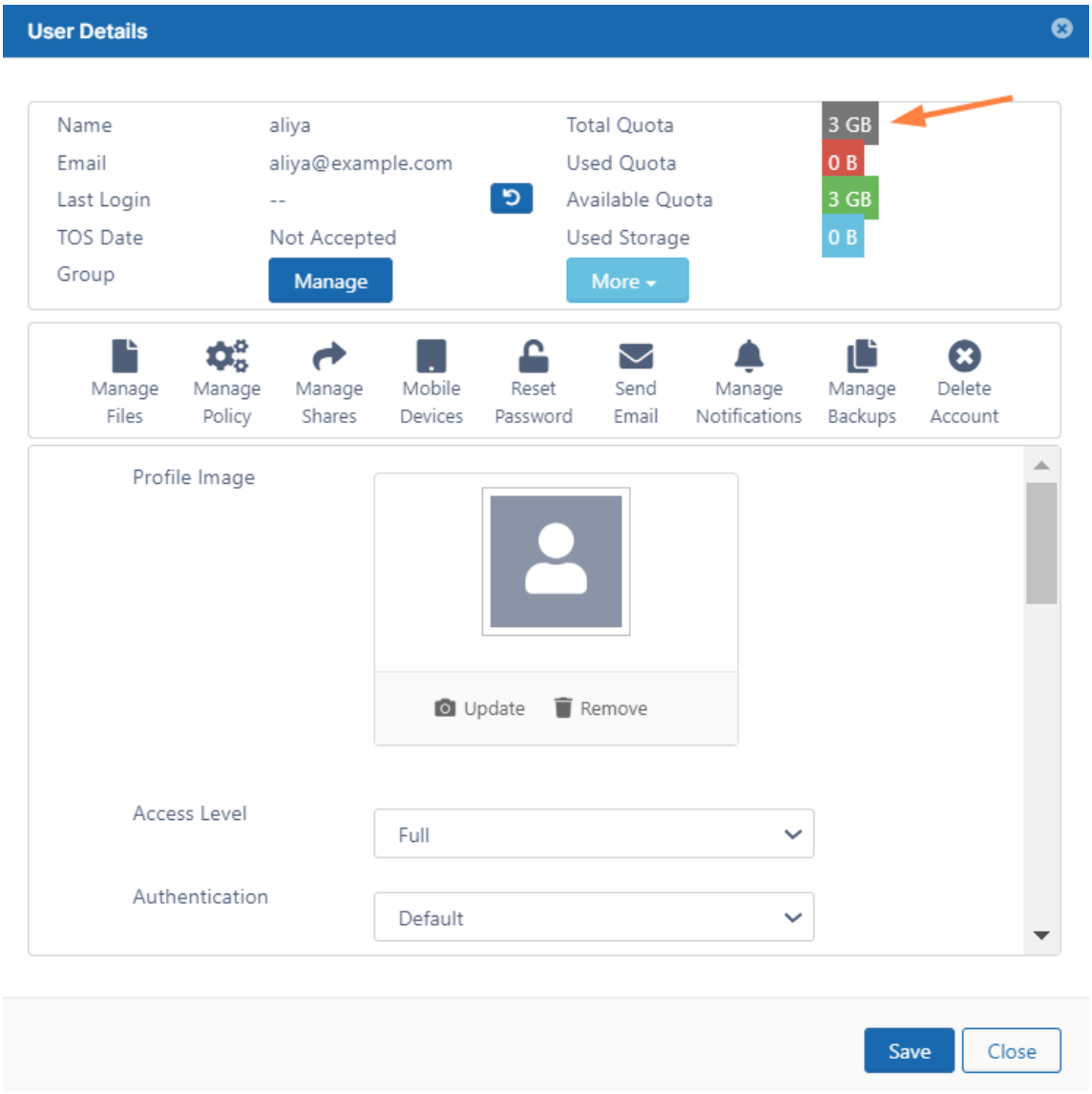
The **Manage Policy Users** dialog box opens.

6. Select the user in the **Available Users** box, and click the arrow to move the user into the **Policy Users** box.



The new policy automatically becomes the user's effective policy.

7. Click **Close**.
8. Confirm that the user's storage quota has changed by clicking **Users** in the navigation pane, and clicking the edit button for the user.
   In the **User Details** box that opens, the total quota should reflect the new value:



Set a Custom Quota for a Group

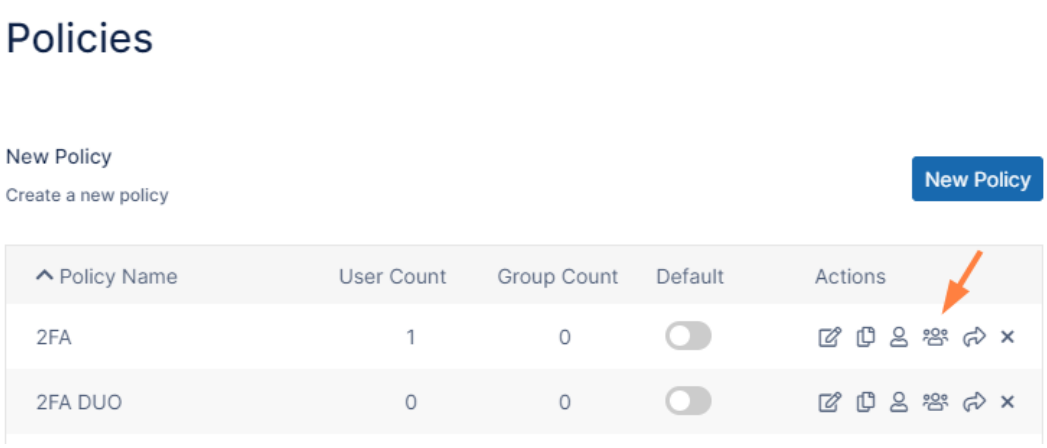
To set a storage quota for a specific group, create a custom policy and assign the group to that policy.

Create a Custom Policy to set the quota for a group of users

If you need to change the quota for a custom group of users, you can create a custom policy.

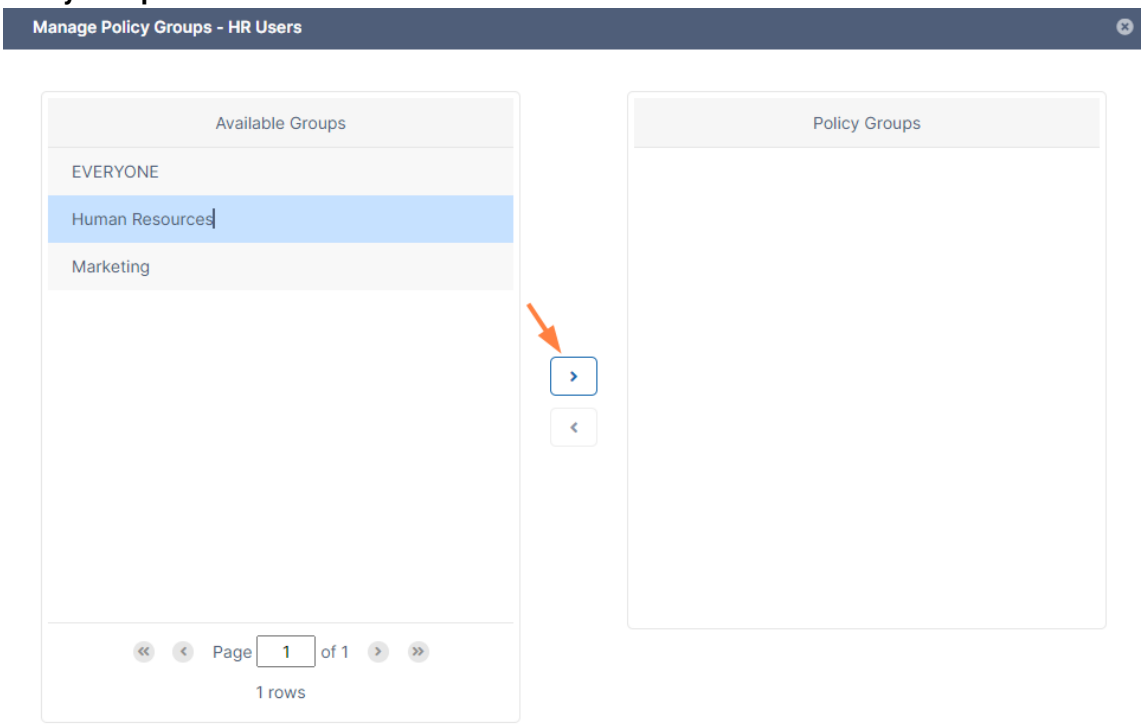
To create a group custom policy:

1. Follow steps 1 to 4 in Set a Quota for a Specific User, above.
2. Click the group icon for the policy.



The **Manage Policy Groups** dialog box opens.

3. Select the group in the **Available Groups** box, and click the arrow to move the group into the **Policy Groups** box.



The new policy automatically becomes the group's effective policy.

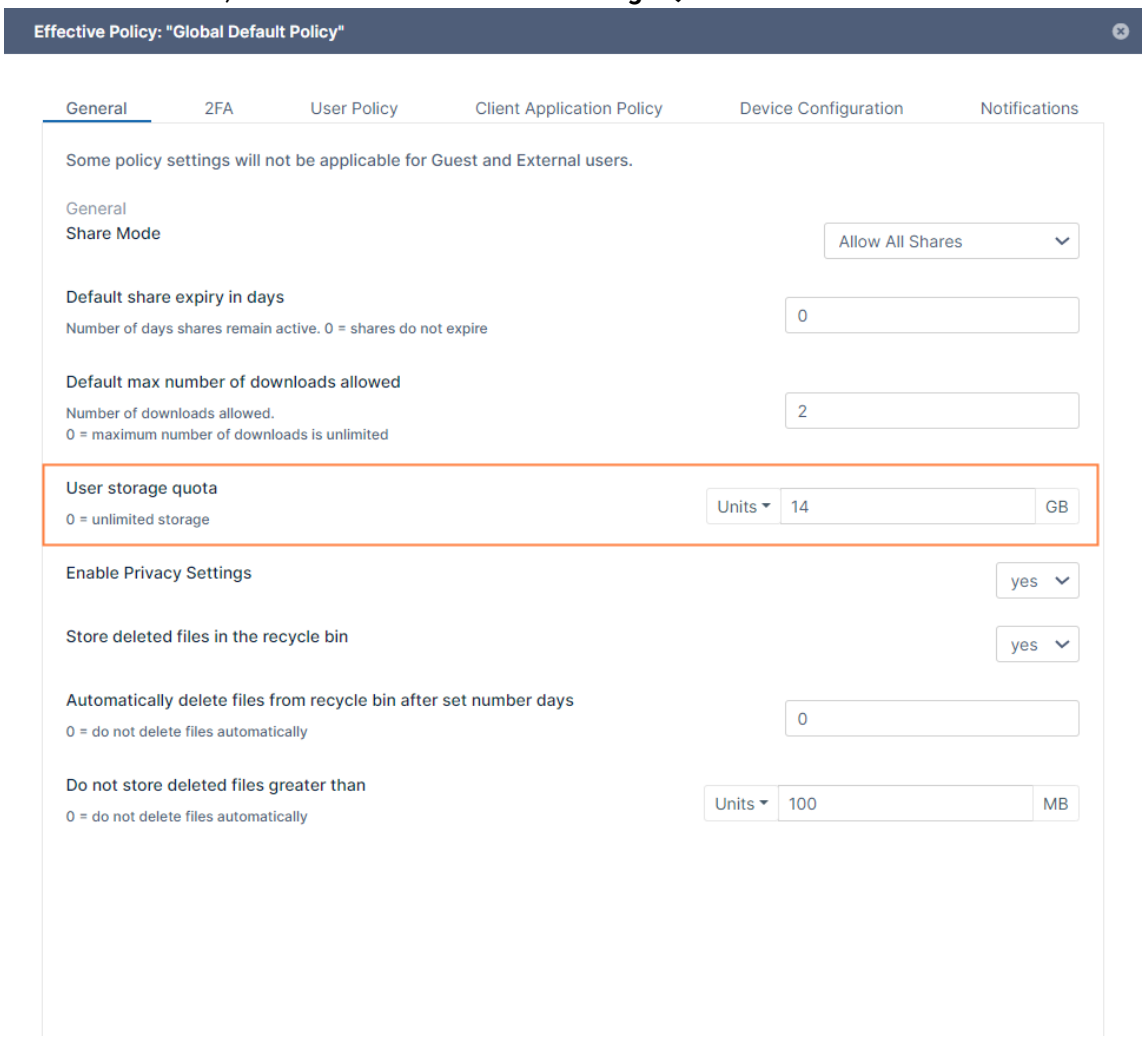
4. Click **Close**.

Set a Default Quota for All Users

To change the default storage quota, change the **User Storage Quota** in the **Global Default Policy**.

Edit the Global Policy

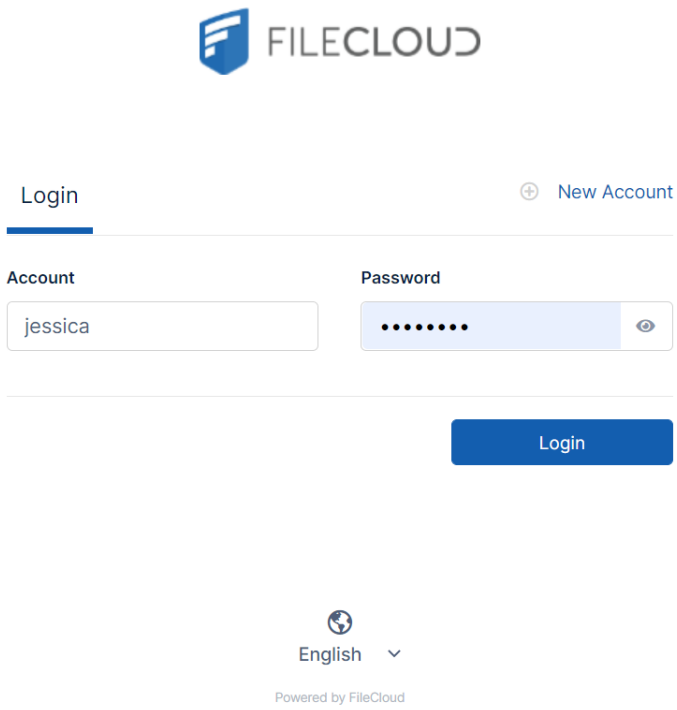
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** page opens.
2. Click the edit icon for the **Global Default Policy**.
3. On the **General** tab, enter the new value in **User Storage Quota**.



4. Click **Save**.

Customize the User Login Screen

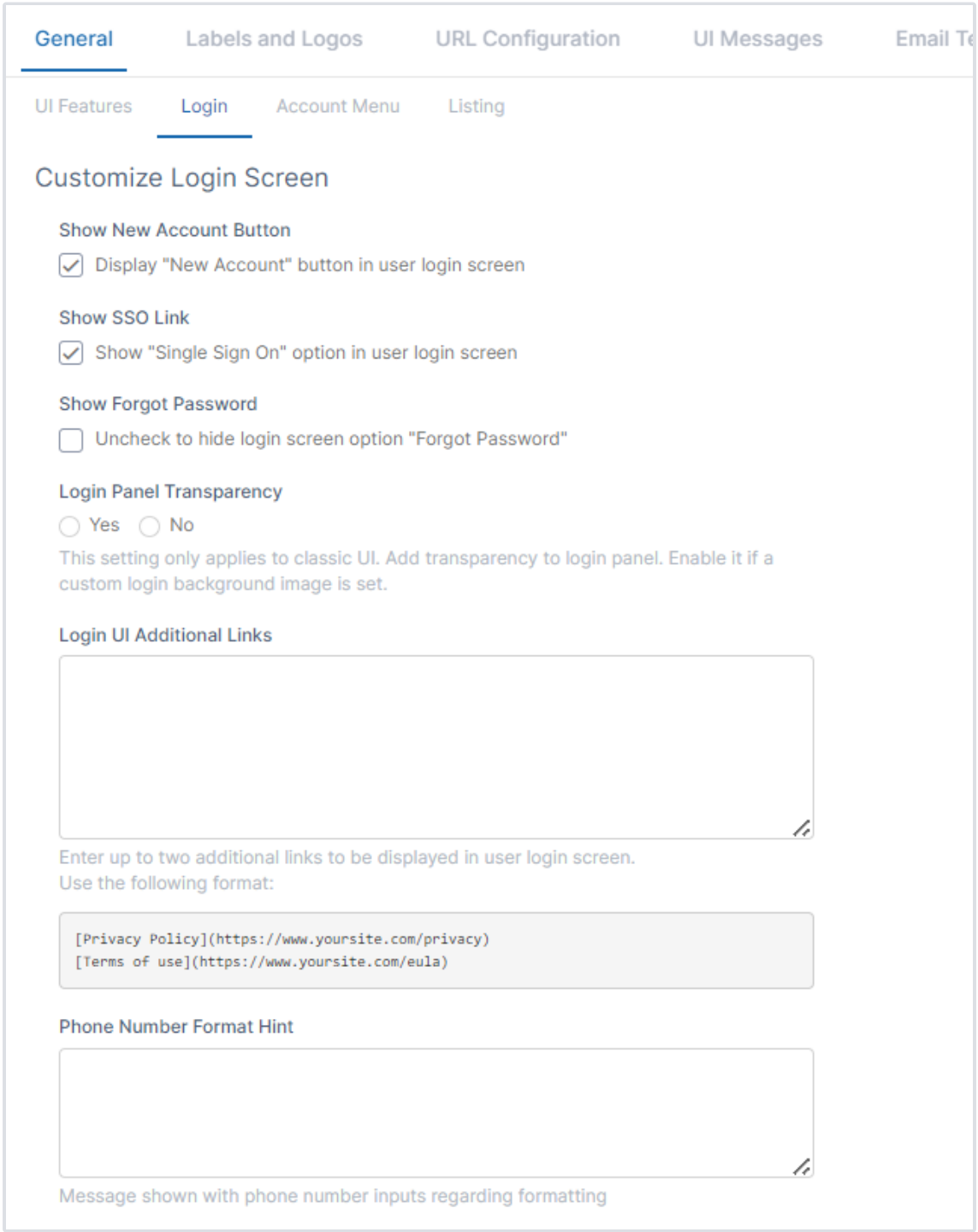
The following image displays the default FileCloud log-in screen, but you can customize the features that appear on it.

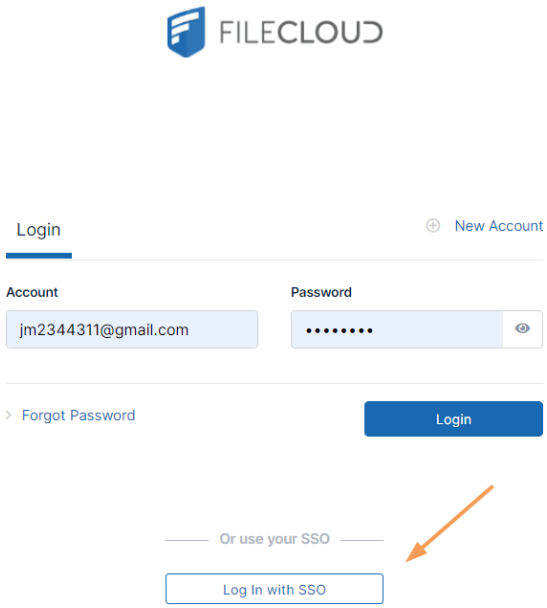


To customize the User Login screen

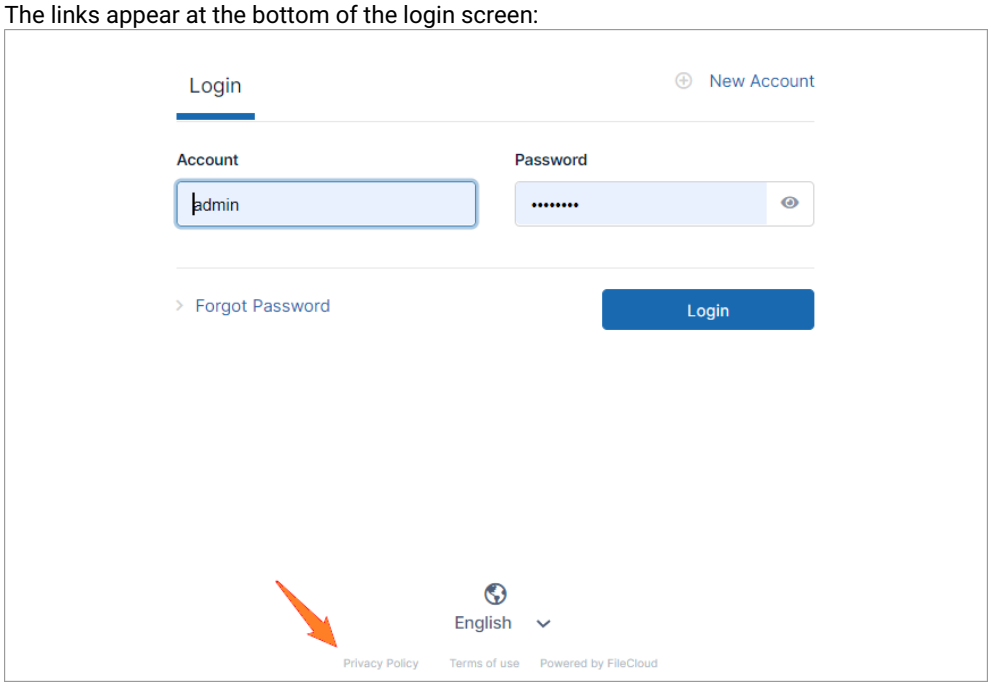
Admin users must have Customization permissions enabled to customize the user login screen. See Managing Admin Users for more information.

1. Open a browser and log in to the Admin Portal.
2. From the left navigation pane, click **Customization**.
3. Select the **General** tab, and then the **Login** sub-tab.


General
Labels and Logos
URL Configuration
UI Messages
Email Te
UI Features
Login
Account Menu
Listing
Customize Login Screen
Show New Account Button
Display "New Account" button in user login screen
Show SSO Link
Show "Single Sign On" option in user login screen
Show Forgot Password
Uncheck to hide login screen option "Forgot Password"
Login Panel Transparency
Yes
No
This setting only applies to classic UI. Add transparency to login panel. Enable it if a custom login background image is set.
Login UI Additional Links
Enter up to two additional links to be displayed in user login screen.
Use the following format:
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/eula)
Phone Number Format Hint
Message shown with phone number inputs regarding formatting

Option	Description
Show New Account Button	Displays **New Account** button in user log-in screen. Enabled by default. The **New Account** button allows a user to create a new account for themselves, and depending on the configuration of Automatic Account Approval, have it automatically approved.
Show SSO Link	Check to show **Single Sign On** link in the login page:  **Note**: If this is checked, but **Show Login Options** is unchecked, **Single Sign On** link is not shown. The functionality of this button is determined by how you configure Single Sign-On Access
Show Forgot Password	Uncheck to hide **Forgot Password**.
Login Panel Transparency	(Applies to classic UI only) Adds transparency to login panel. Set to: • YES (default) • NO Enable this option if you are using a custom login background image.

Option	Description

Login UI Additional Links	Enter up to two additional links to be displayed in user login screen.
	Use the format:
	`[Privacy Policy](https://www.yoursite.com/privacy)`
	`[Terms of use](https://www.yoursite.com/tos)`
	The links appear at the bottom of the login screen:
	 

Phone Number Format Hint	Enter a hint to appear on screens where users can enter phone numbers. For example **Include + and country code when entering phone number**.

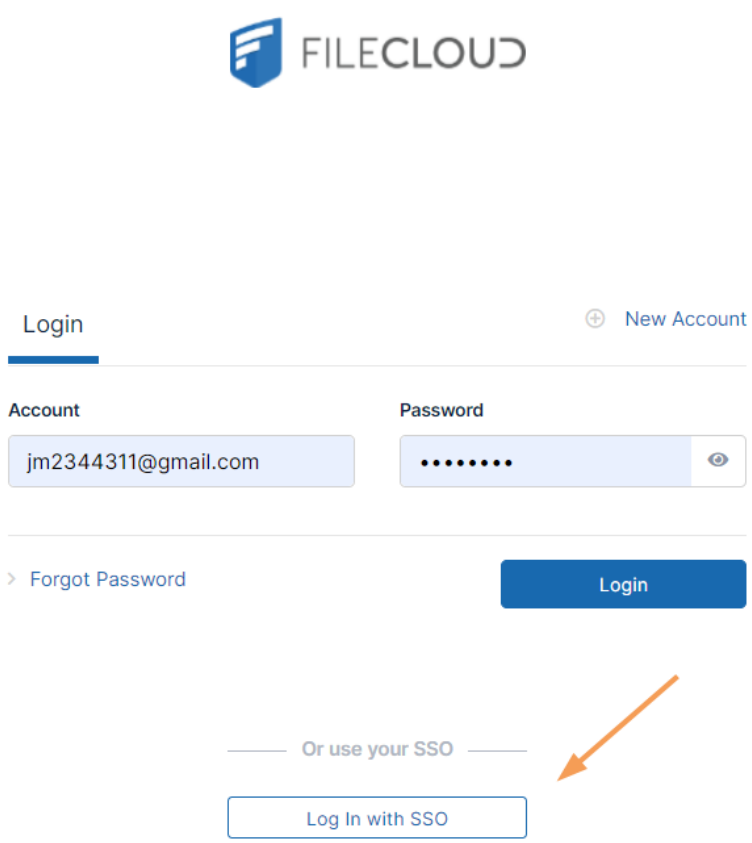
4. Modify the settings for any of the options.
5. To save your changes, click **Save**.

To customize for SSO log in

You can customize the user log-in screen to display the SSO log-in option along with the direct log-in option or to only display the SSO login.

To display the SSO log-in option along with the direct log-in option:

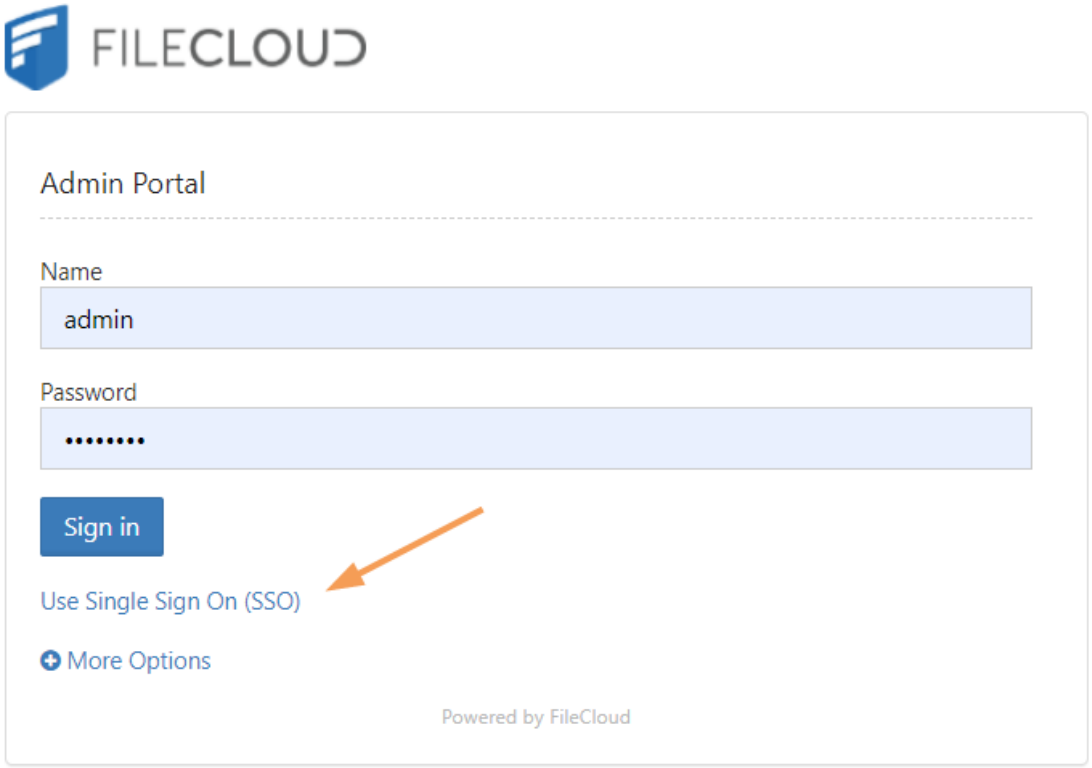
1. From the left navigation pane, click **Customization**.
2. Select the **General** tab, and then the **Login** sub-tab.
3. Check **Show SSO Link** and **Show Login Options**.
4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



On clicking the Single Sign-On link on the login page, the user is redirected to the SAML SSO Service web page.

The SSO log-in option in the admin portal:

FileCloud admin interface also supports single sign-on.



Default admin portal log-in screen

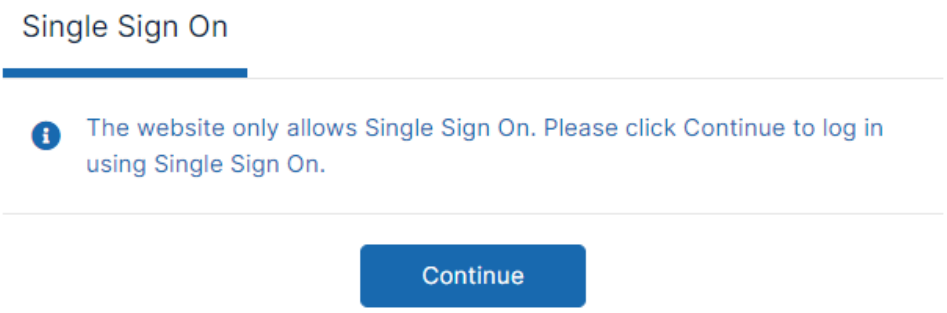
To only display the SSO log-in option:

In order to skip the FileCloud login page and send the user directly to the SAML SSO page you must add a setting to the cloudconfig.php file, as shown below. You can configure this option for the user portal login page and the admin portal login page.

To only display the SSO log-in option in the user portal:
This configuration option supports skipping the login page when the user accesses FileCloud with a domain name or with a full URL.

1. In the admin portal, go to **Customization,** and select the **General** tab, and then the **Login** sub-tab.
2. Check **Show SSO Link** and **Show Login Options**, and save your changes.
3. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
4. To only display the SSO log-in option:
   ```
   define("TONIDOCLOUD_SSO_DIRECT_ONLY", "1");
   ```

When users enter the log-in page they will see:



To return to displaying other log-in options:

```
define("TONIDOCLOUD_SSO_DIRECT_ONLY", "0");
```

To display only SSO log-in in the admin portal:

Starting with Version 20.1, FileCloud supports skipping the login page when the admin accesses FileCloud with a domain name or with a full URL.

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To only display the SSO log-in option:

Enter:

```
define ("TONIDOCLOUD_SSO_DIRECT_ONLY_ADMIN", "1");
```

An earlier version of this option is also effective in versions of FileCloud prior to 20.1, but this redirect is only effective if the user specifies a domain name rather than a full URL. Instead of the above setting, use:

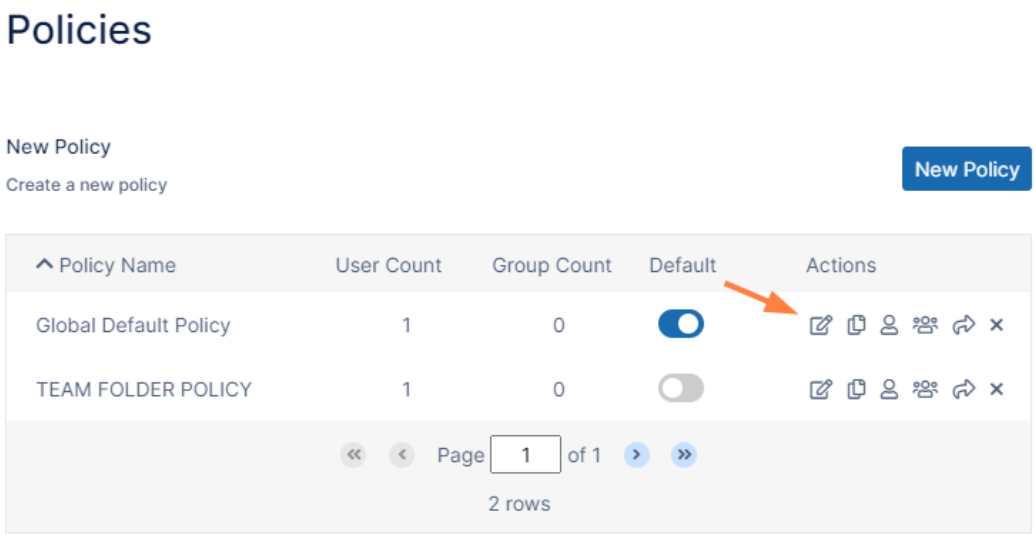
```
define("TONIDOCLOUD_SSO_DIRECT_ADMIN", "1");
```

Limiting File Upload Size for Users

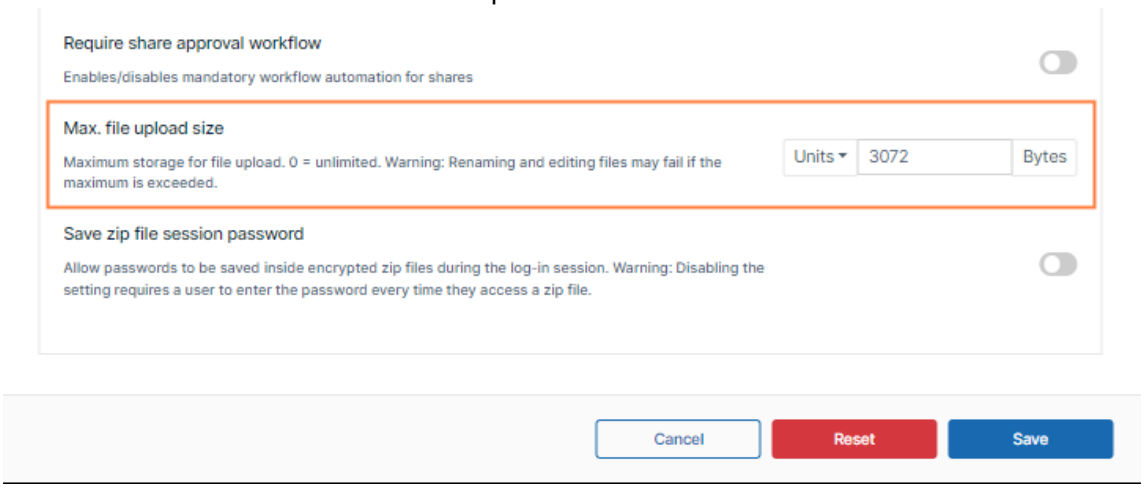
You can set a limit on the size of files that some or all of your users can upload into FileCloud by entering a value for **Max File Size Limit** in the users' policy or policies.

To change the **Max File Size Limit** setting:

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. Click the Edit icon for the policy of the users who you want to prevent from sharing with the **Everyone** group.



   The **Policy Settings** dialog box opens.
3. Click the **User Policy** tab.
4. Scroll down to the **Max. file upload size** setting.
5. Enter the maximum file size that can be uploaded.



6. Click **Save**.

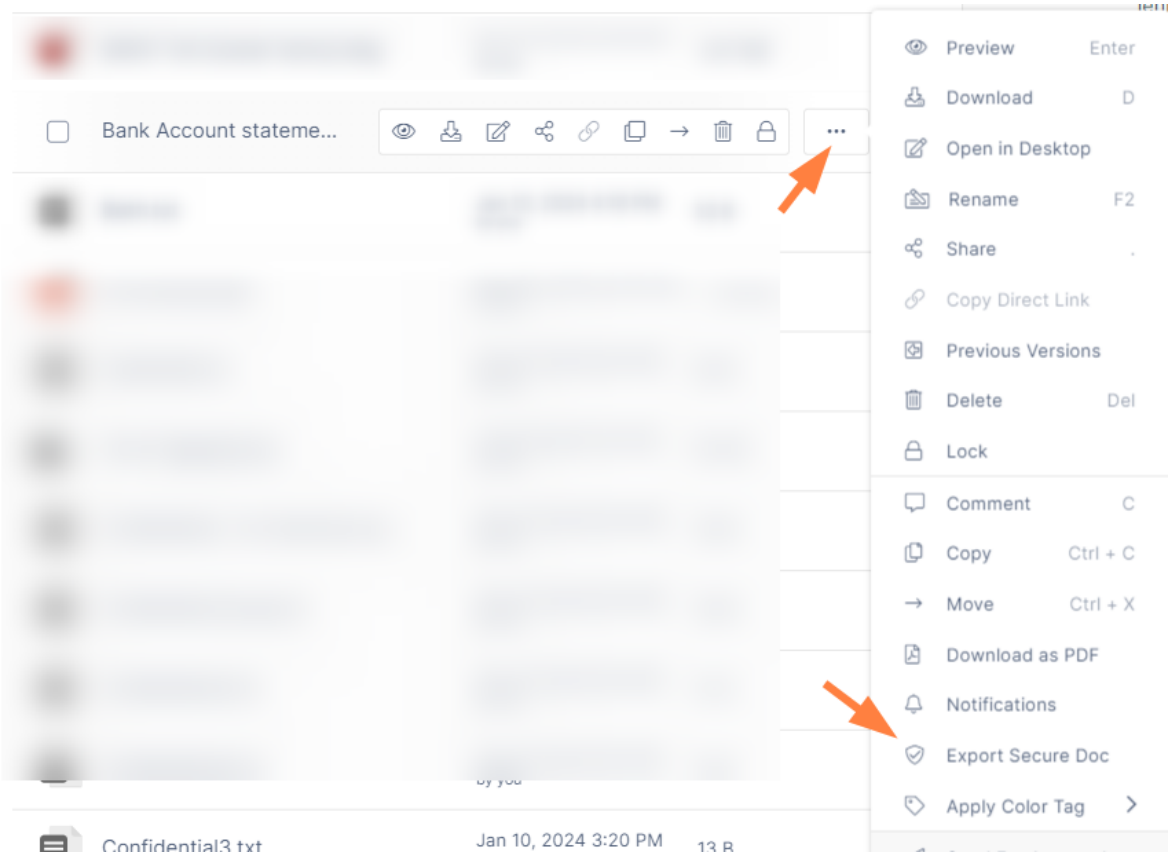
Max. file upload size does not apply to Sync and Drive and other non-Web FileCloud clients.

For help applying **Max. file upload size** to non-web FileCloud clients, please Contact FileCloud Support.

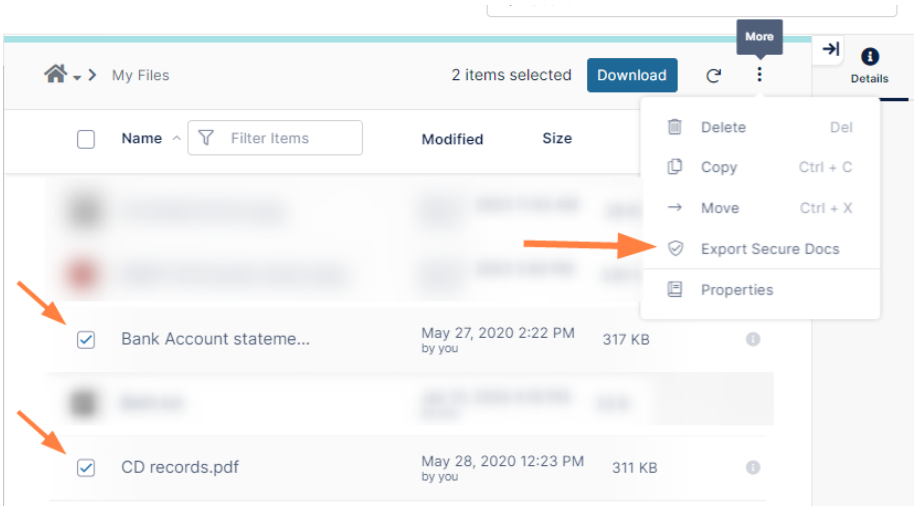
Remove the Export Secure Doc Option

If your FileCloud license includes DRM, any file of a type that is supported by DRM (**jpg**, **png**, **docx**, **pptx**, and **pdf**) has the **Export Secure Document** option enabled. When users choose this option, the downloaded file may only be viewed through the FileCloud Secure Document Viewer using an access key.

The option appears in the user portal either in the action menu for a file



or the action menu for multiple files:



To hide the Export Secure Docs option:

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

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

3. To return to the default, change **true** to **false** or remove the setting.

Disabling Send for Approval

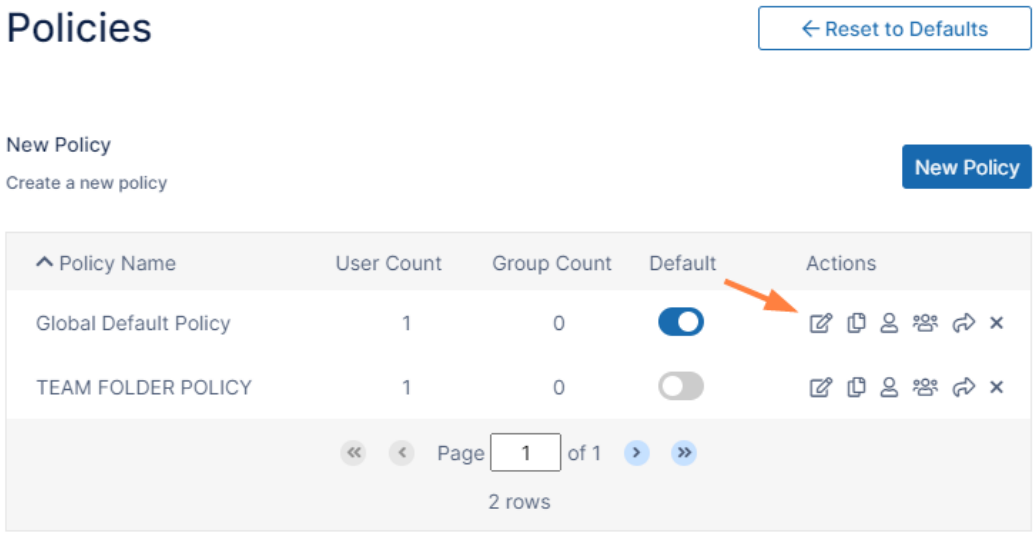
The ability to request file approval is available beginning in FileCloud 21.2.
Beginning with FileCloud 23.241.6:

- The **Disable Send for Approval** option is available.
- The file approval option is not available for External users and users who do not have access to share a file.

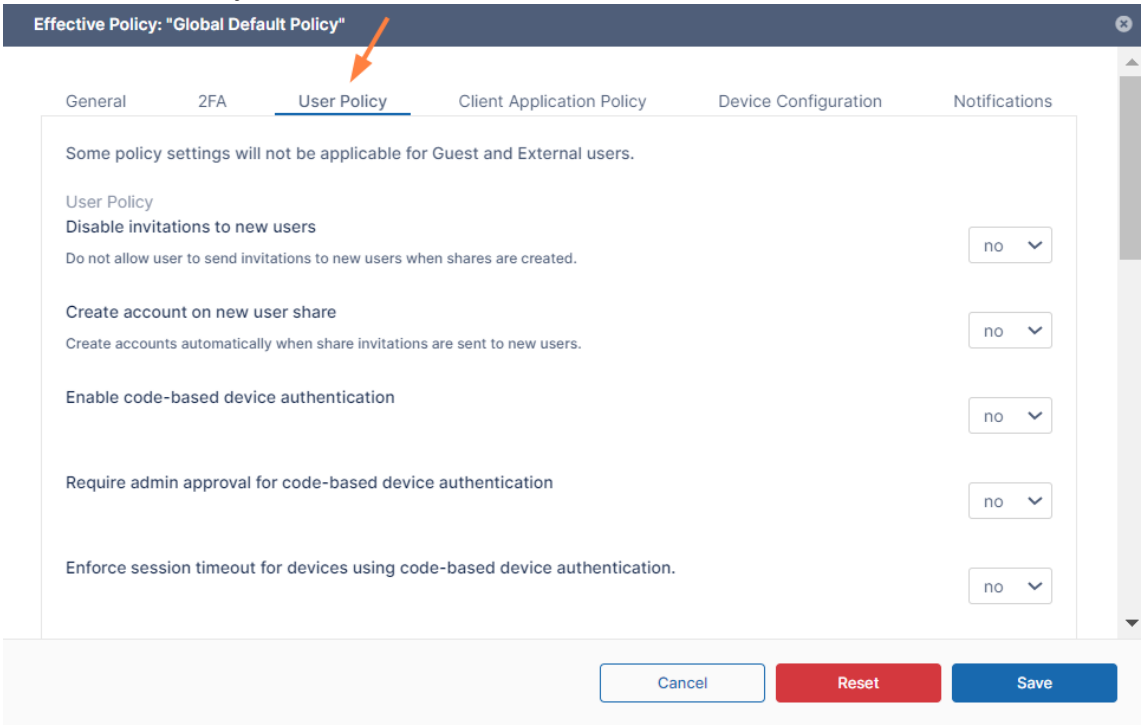
You can remove the ability for a group of users to send files for approval by through their policy.

To disable Send for Approval:

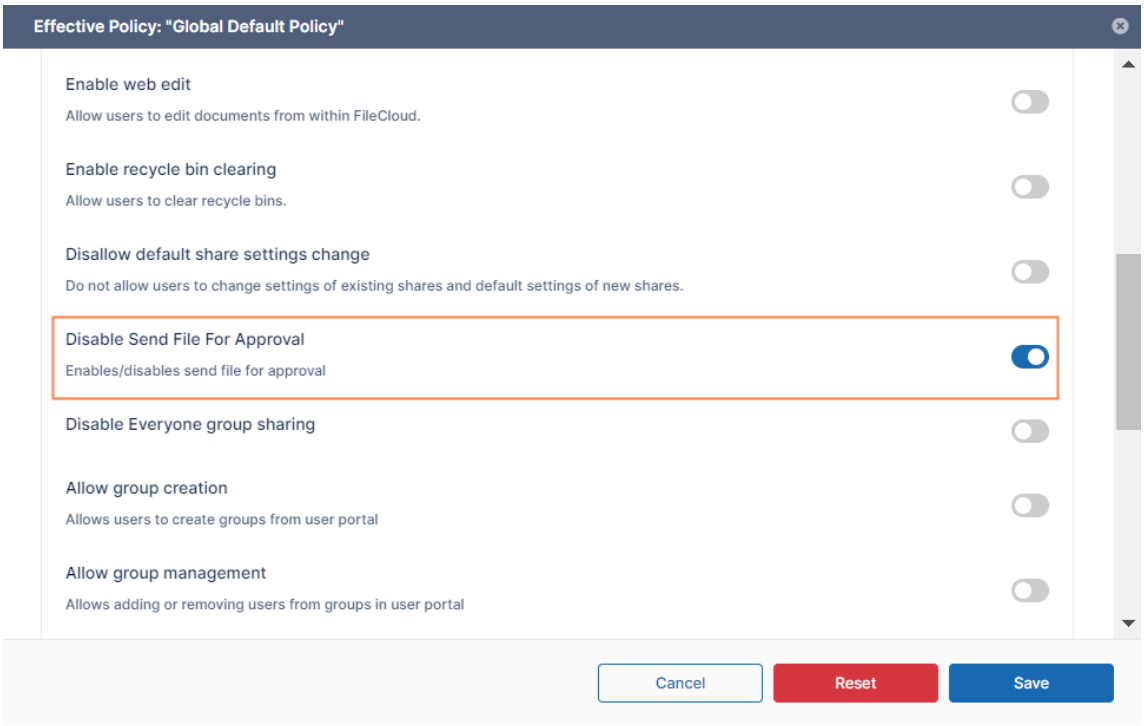
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



3. Click the **User Policy** tab.



4. Scroll down to **Disable Send File For Approval,** and enable it.


Effective Policy: "Global Default Policy"
Enable web edit
Allow users to edit documents from within FileCloud.
Enable recycle bin clearing
Allow users to clear recycle bins.
Disallow default share settings change
Do not allow users to change settings of existing shares and default settings of new shares.
Disable Send File For Approval
Enables/disables send file for approval
Disable Everyone group sharing
Allow group creation
Allows users to create groups from user portal
Allow group management
Allows adding or removing users from groups in user portal
Cancel
Reset
Save

5. Click **Save**.

Group Settings

The addition of the Externals group and the removal of External users from the Everyone group is effective beginning in FileCloud 23.252.

The feature for importing groups from an SSO provider is available in FileCloud 23.251 and later.

Administrators can create groups of users in FileCloud Server. Creating groups allows setting network share access and sharing of files and folders for multiple users.

The automatic groups **Everyone** and **Externals** are created by default for every FileCloud installation.
The **Everyone** group contains all Full and Guest users. External users are not included in the **Everyone** group.
The **Externals** group contains all External users.

Groups may contain the following attributes

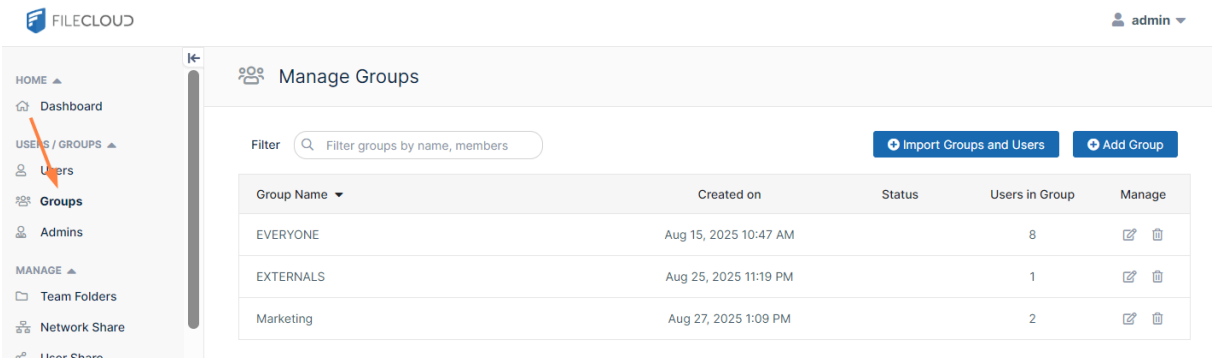
- **Group Name** - Name assigned by the administrator
- **Group Members** - List of users that are part of the group
- **Group Admins** - (optional) Users with the ability to view users, add users, and/or remove users from the group.
- **Group Policy** - The policy that applies to all members of the group. By default, the **Global Default Policy** is assigned.

Once a group is created, it can be populated with users using one of the following methods:

- Manually adding users that are already in the FileCloud system.
- Importing members of a group from an external AD server.
- Importing members of a group from an external SSO provider.

Show me where to manage groups in the Admin Portal

To manage groups, in the navigation panel, click **Groups**.

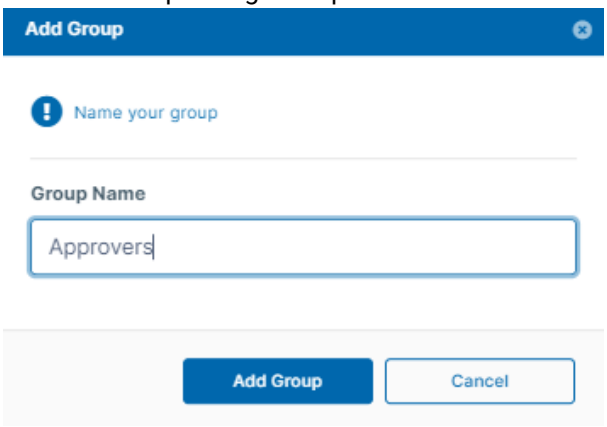


What do you want to do?

Manually create a FileCloud Group

To create a group:

1. Open a browser and log on the admin portal.
2. On the left control panel, click **Groups**.
3. Click the **Add Group** button.
   The Add Group dialog box opens.



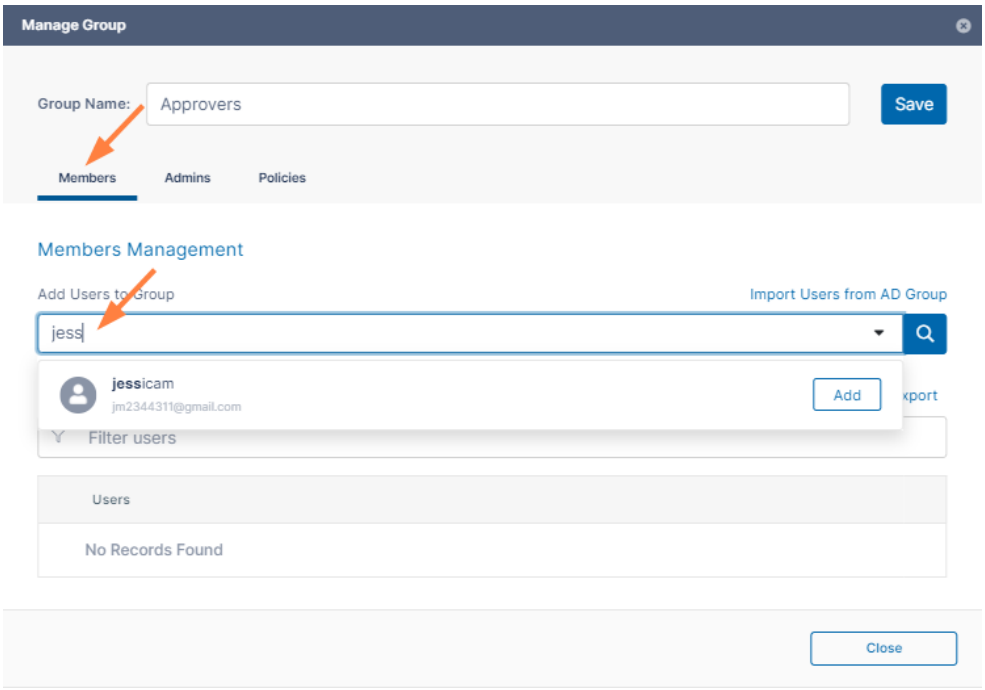
4. Click **Add Group**.
5. The group is added, and the **Manage Group** dialog box opens.

Add FileCloud Users to a Group

This method requires the user accounts to already exist in your local FileCloud Server.

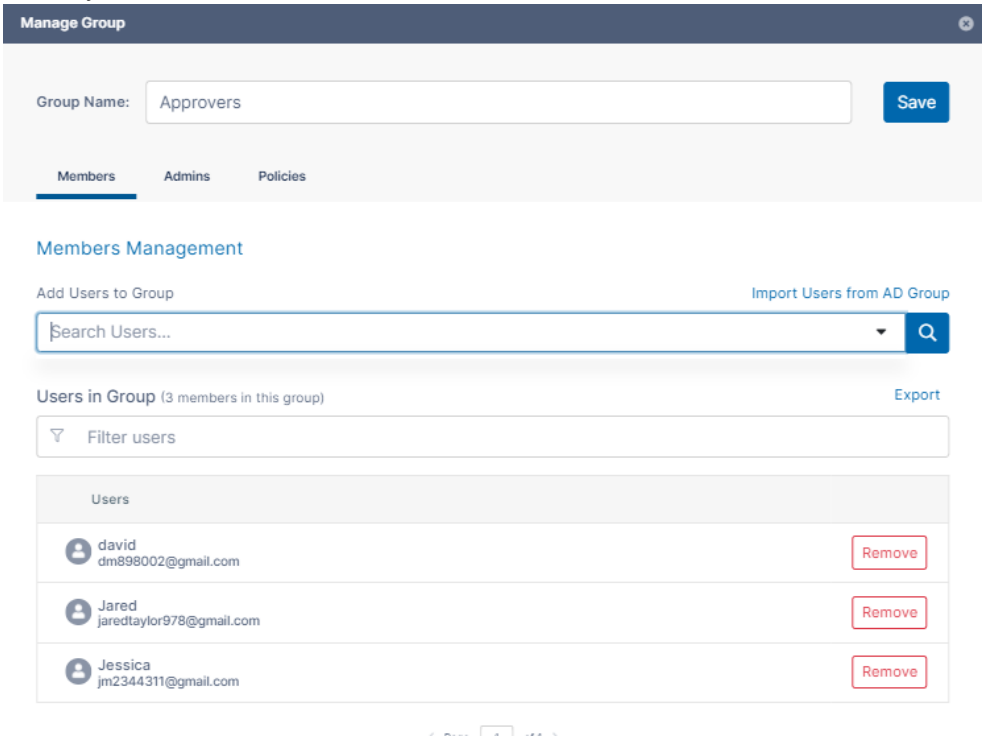
To add FileCloud users to a group:

1. In the navigation panel, click **Groups**.
2. Click the Edit icon next to the group that you want to add members to..
3. If it is not already selected, click the **Members** tab.
4. In **Add Users to Group**, enter the username or email of an existing FileCloud user, and click **Add**.



The user is listed under **Users in Group**.

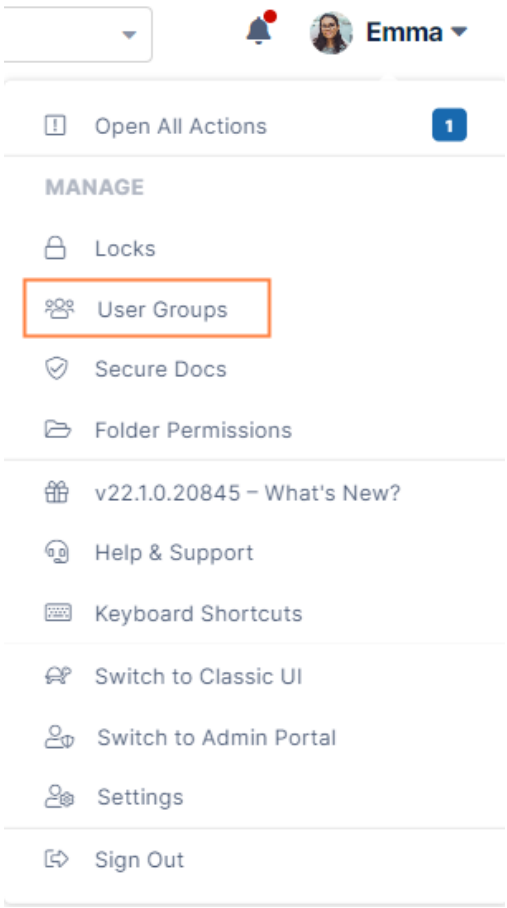
5. Add any number of users.



6. Either click **Save** to save the new members in the group, or click the **Admins** or **Policies** tab to further configure the group.

Add Group Admins

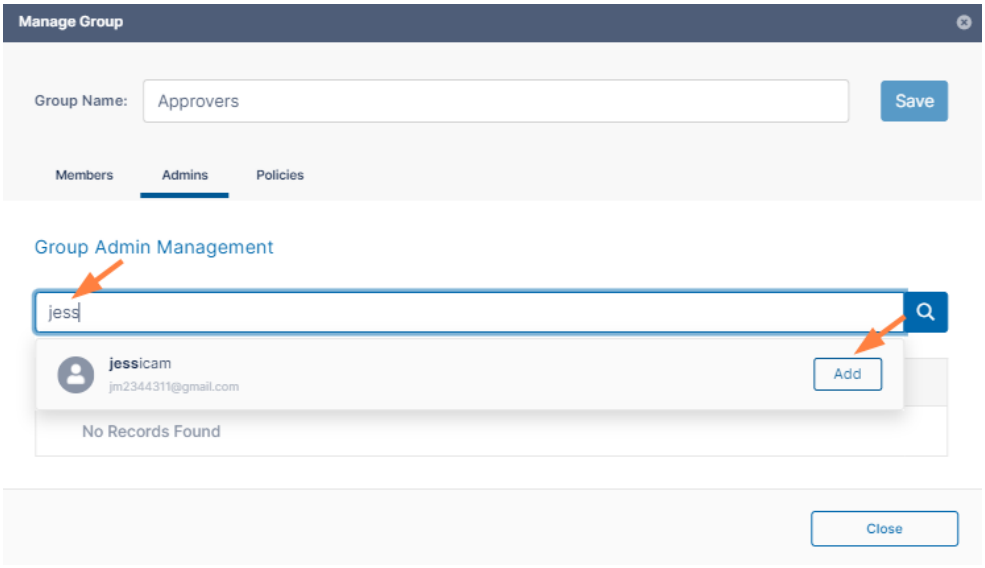
You can assign users to be admins of a group and give each group admin access to view, add, and/or remove users from the group.
A user's policy also may enable them to add and/or remove users from groups. See Giving Users Group Management Permissions for more information. If either a user's group admin access or policy settings gives the user the permission to add or remove users from a group, the user has that ability, and can manage user groups in the user portal by expanding the user drop-down list and clicking **User Groups**:



To Add Group Admins:

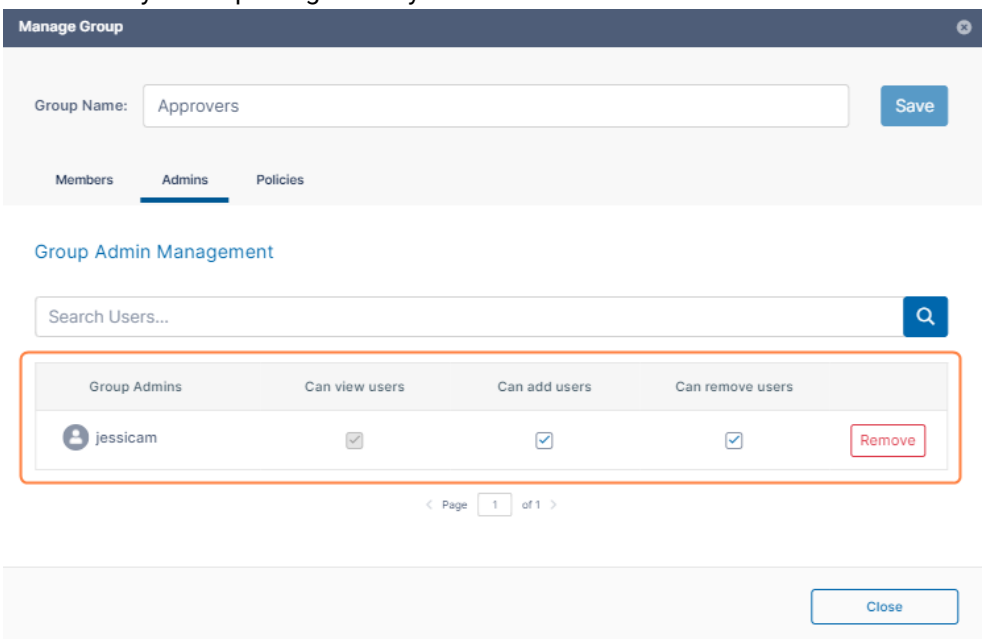
1. If you are not already inside the **Manage Group** dialog box, open it by clicking the Edit icon next to the group.
2. Click the **Admins** tab.

3. In the search box, enter a user that you want to add as an admin, and click **Add**.
   The user does not have to be a group member, but must be a current FileCloud user with Full or Guest status.



   The user is listed under Group Admins with **Can view users**, **Can add users**, and **Can remove users** checked by default.

4. Uncheck any of the privileges that you do not want the user to have.



5. Add any number of admins and set their privileges.
6. Either click **Save** to save the admins, or click one of the other tabs to further configure the group.

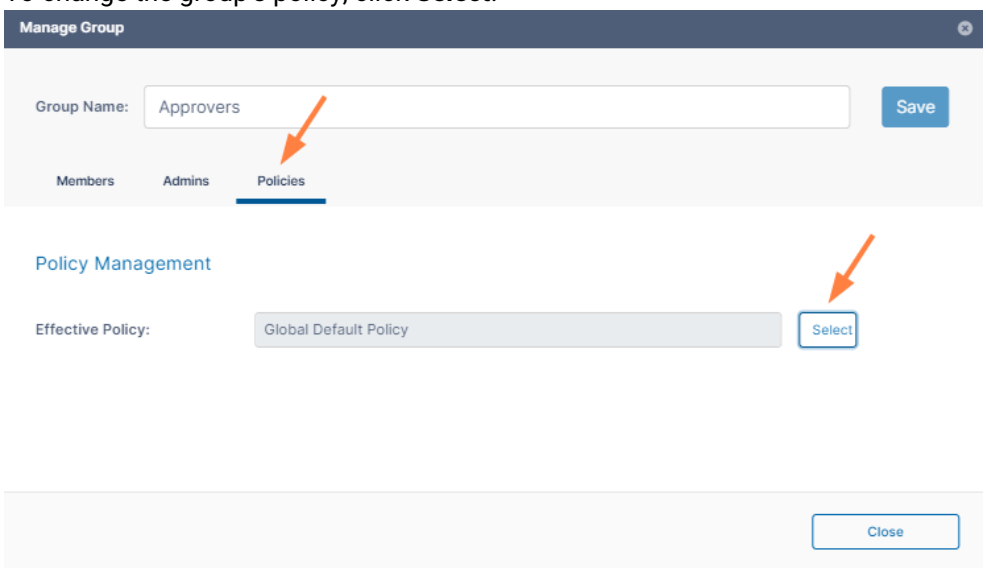
Change a Group's Policy

Members of a group have both their user policy and the group's policy. For each setting the user has the greatest access given in either policy.

By default, your groups are assigned the **Global Default Policy**. You can change that default when you initially create the group or later by editing it.

To change a group's policy:

1. If you are not already inside the **Manage Group** dialog box, open it by clicking the Edit icon next to the group.
2. Click the **Policies** tab.
3. To change the group's policy, click **Select**.



A list of policies opens.

4. Click a policy, and then click **Select**.
5. Click **Save**, and click **Close**.

Import Active Directory Users to a FileCloud Group

You can also import an existing AD group from an Active Directory Server connected to FileCloud.

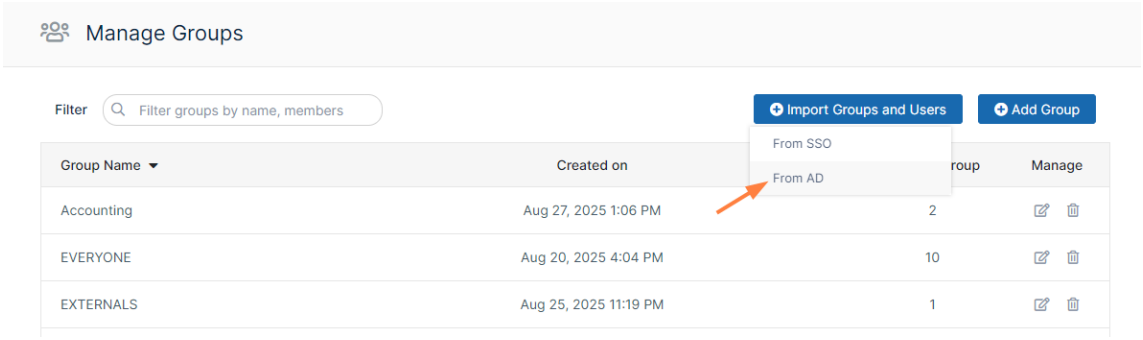
During AD import, if a user is not in the AD group, the account is not removed automatically from the FileCloud group. This logic is based on the scenario where an administrator manually adds other FileCloud users to the FileCloud group who are not in the AD group, and those users should not be removed.
However, there is now an option for an enterprise that uses a large number of temporary workers, such as a construction company that uses a large number of contractors. If they import a large number of users based on groups, when a contractor is no longer employed, and therefore not a member of the AD group any more, the admin can now select a checkbox on the **AD Group Members**

Import dialog box called **Remove Members.** This allows admins who need to remove accounts on import to do so automatically. If you have manually created users that you don't want deleted but aren't a member of a group any longer, then you would not select this option.

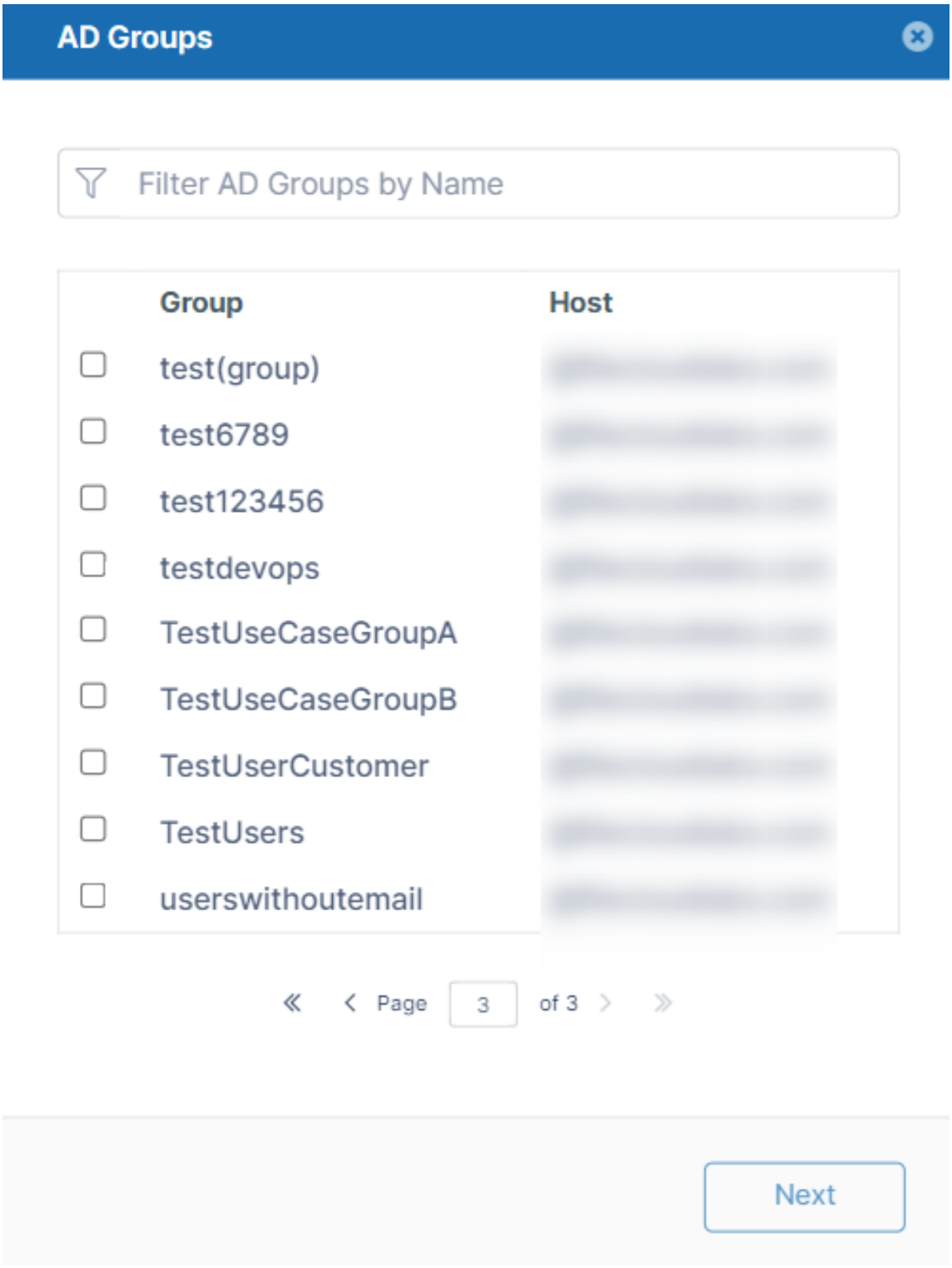
⚠ You must set up and verify Active Directory Settings before completing the following steps.

To add AD users to a FileCloud group:

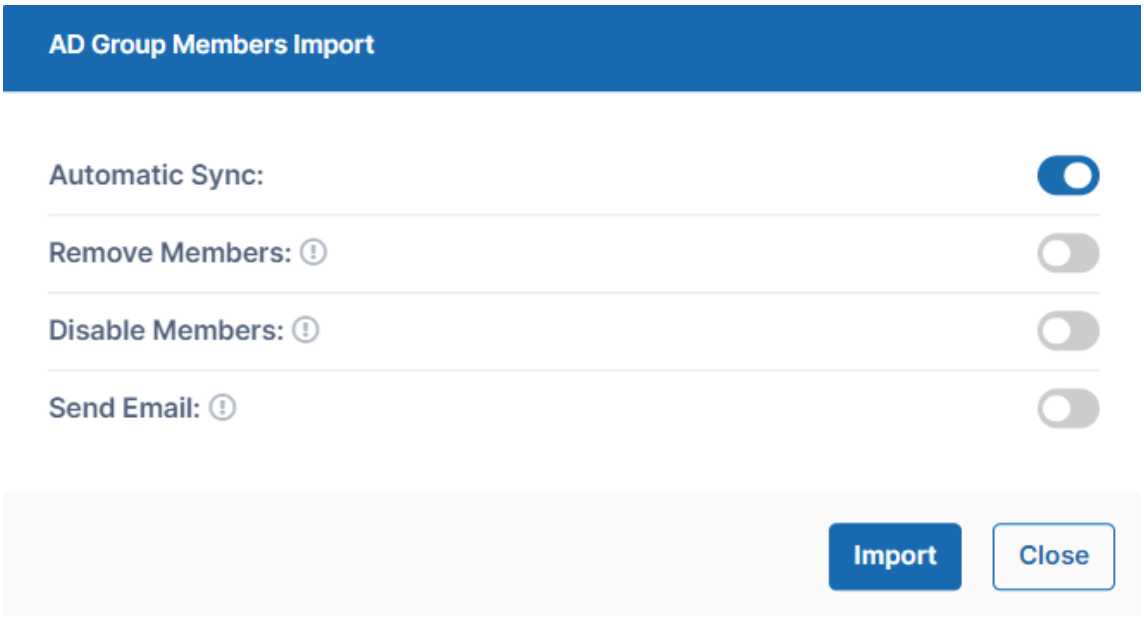
1. Open a browser and log in to the admin portal.
2. On the left control panel, click **Groups**.
3. Click the **Import AD Groups and Users** button, and choose **From AD**.



An **AD Groups** dialog box opens:

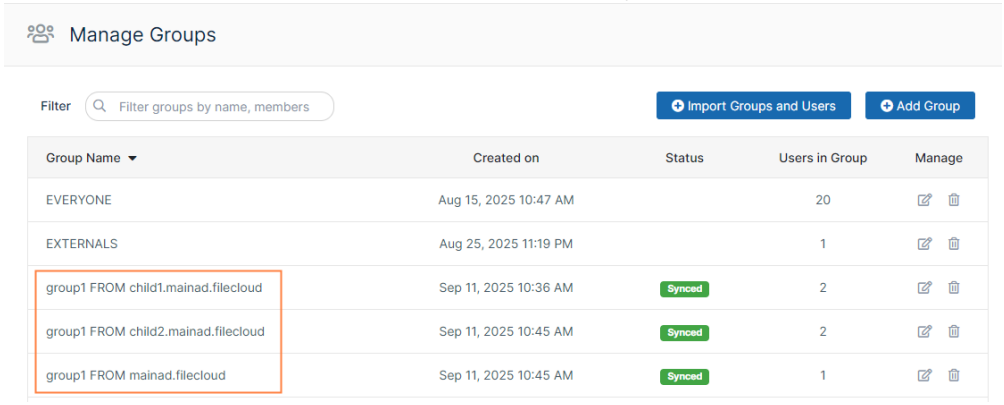


4. Check the groups you want to import, and click **Next**.
   An **AD Group Members Import** dialog box opens.



5. **Automatic Sync** is selected by default. Leave it selected to enable FileCloud to automatically add users to the FileCloud group that are added to the AD group. This sync is done every 24 hours.
   - The first time members from the AD group are imported as members of the FileCloud Group.
   - In the future, new members added to the AD group are synced automatically to the FileCloud group.
     To change the frequency of automatic syncing, see To change the automatic sync interval, below.
     When syncing begins, FileCloud logs display the message: **CRON: Starting Auto Sync AD Group**
6. Select any of the other options:
   - **Remove Members** - Enable FileCloud to remove members from the group f they are no longer in the AD group.
   - **Disable Members** - Enable FileCloud to disable members in FileCloud as users if they are disabled in the AD group.
   - **Send Email -** Enable FileCloud to send email to members of the AD group telling them they have been added to the FileCloud group.
7. To import the users from the AD group, click **Import**.
   If you do not have **Automatic Sync** enabled, rerun this operation at any time to add new members from the AD group into the FileCloud group.

If the Enable multiple AD domains setting is enabled, the imported group's name in FileCloud is: **[AD group name] FROM [full domain name including any sub-domains]**:



To change the automatic sync interval:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the following line.
   Set the value to the interval in hours to sync FileCloud groups with AD groups. The minimum is 1.

```
define("TONIDOCLOUD_ADGROUPSYNC_INTVL", 2);
```

3. Restart the FileCloud message queue.

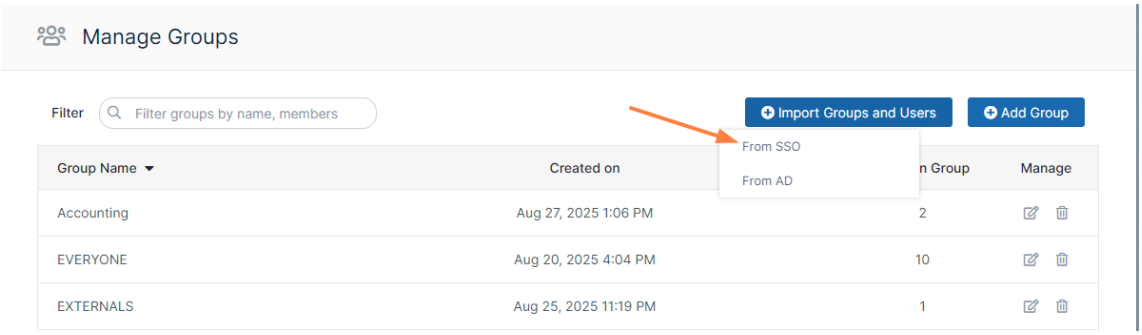
Import SSO Users to a FileCloud Group

You may configure FileCloud to import groups and users from the OKTA, Google, and Azure SSO providers. See Import Groups and Users from an SSO Provider for configuration instructions.

By default, the users are not placed into their groups when they are imported into FileCloud, but you may enable a setting to enable this function. Note that you cannot import SSO users into FileCloud separately from their groups.

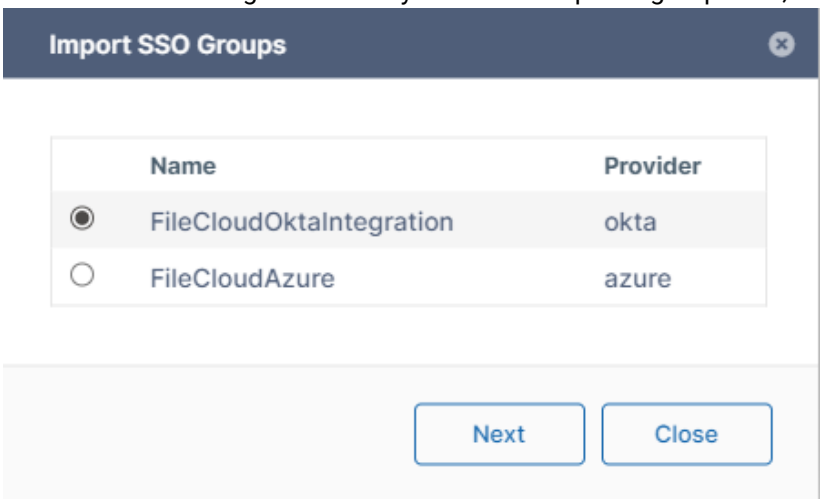
To import an SSO group into FileCloud:

1. In the admin portal, in the navigation panel, click **Groups**.
2. Click the **Import Groups and Users** button, and choose **From SSO**.

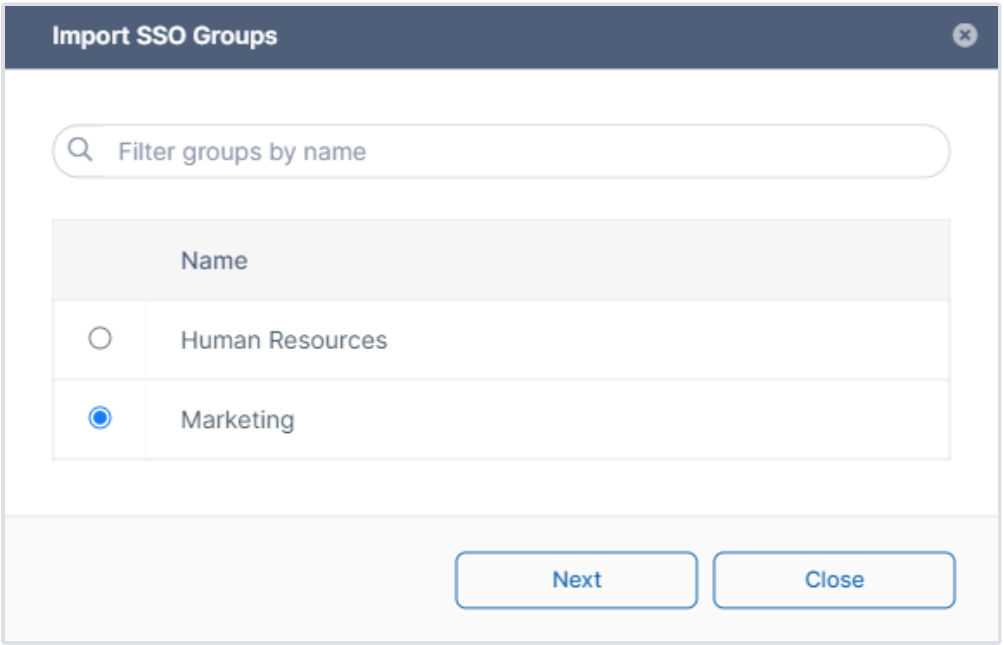


An **Import SSO Groups** dialog box opens.

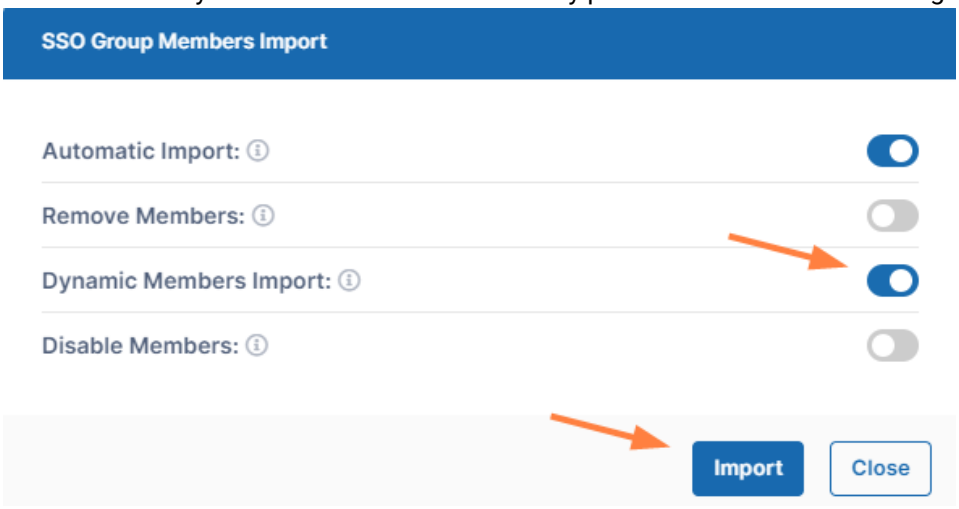
3. Select the SSO configuration that you want to import a group from, and click **Next**.



4. Select a group, and click **Next**.



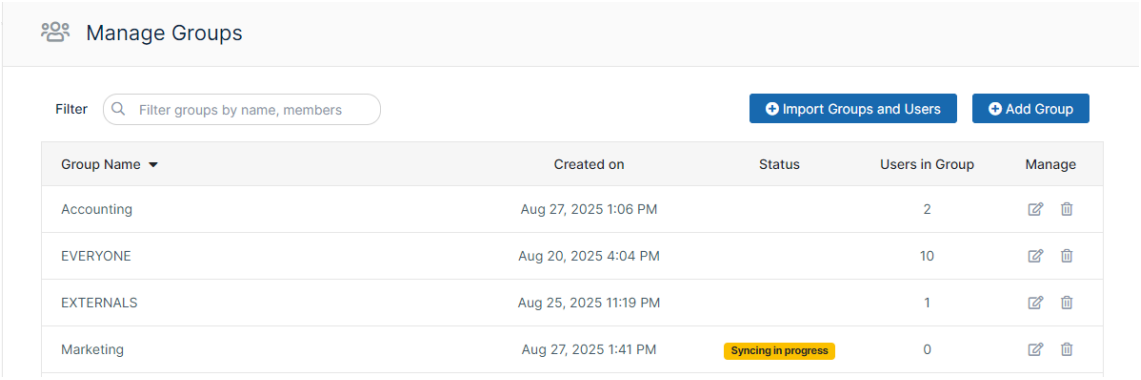
5. Enable or disable the options for the import.
   Automatic Import is enabled by default. In this example, the option **Dynamic Members** Import is also enabled so you can see how it automatically places users into the correct group.



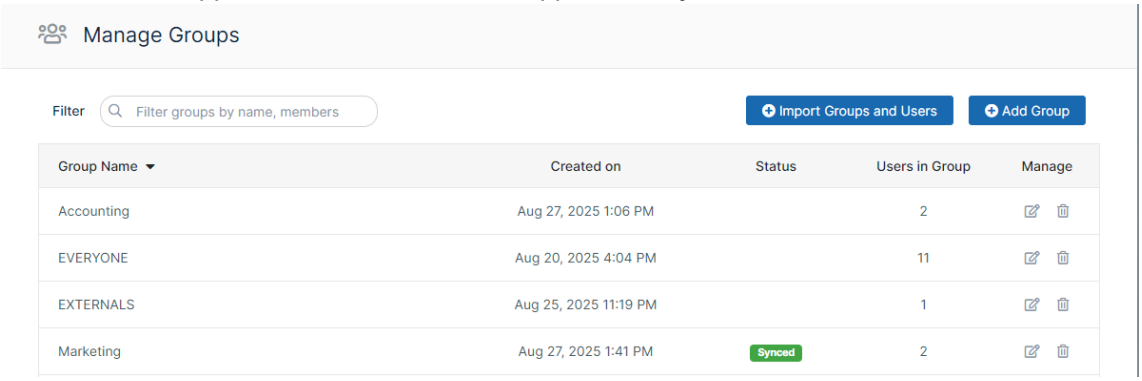
   The options function as follows:

Automatic Import	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.

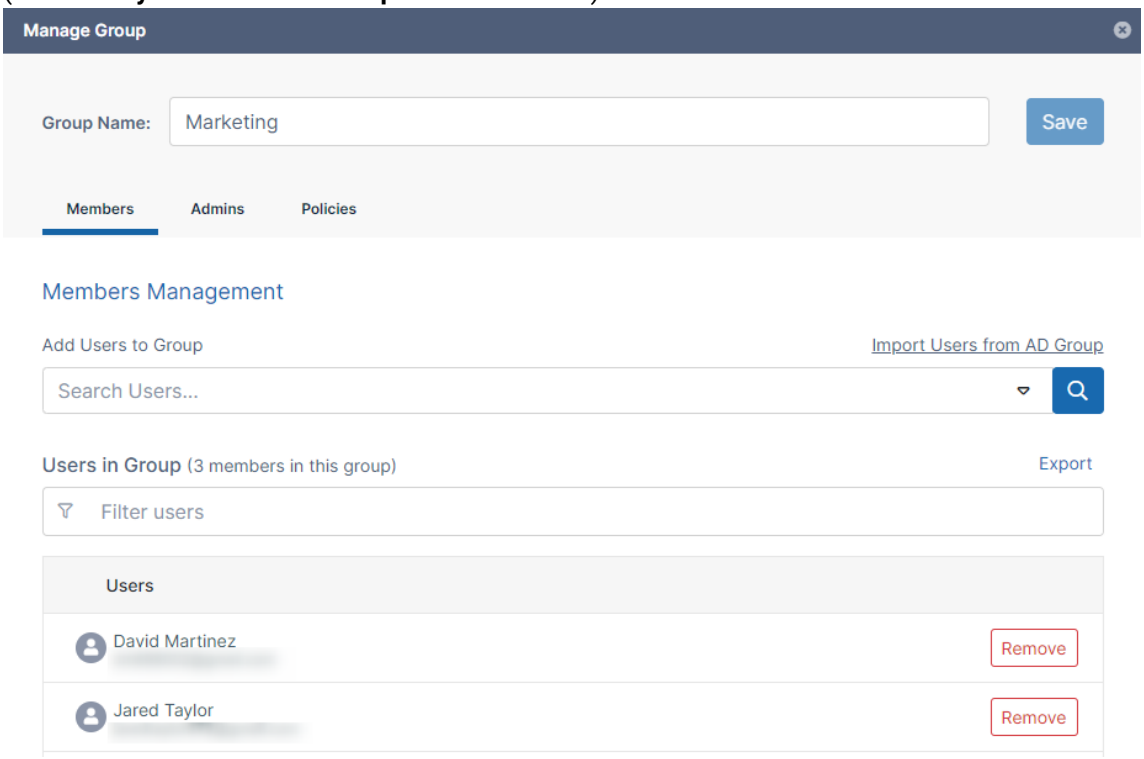
6. Click **Import**.
   Although **Dynamic Members Import** is selected, the group initially shows 0 users (members) and shows the **Status** as **Syncing in progress**. The user count will appear when the syncing is complete.



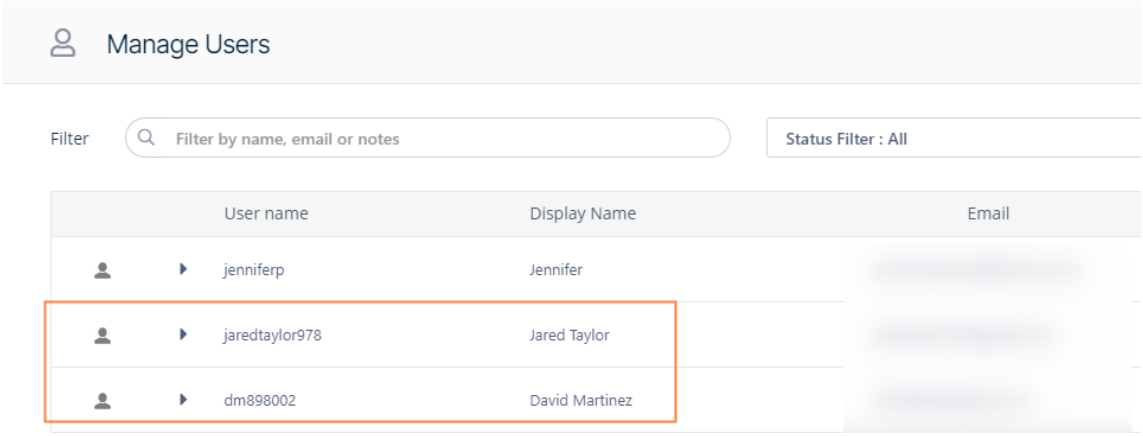
The user count appears when the the status appears as **Synced**.



7. Click the edit icon for the group to see which users were imported and placed into the group (because **Dynamic Members Import** was selected):



The users should also appear in the Manage Users screen:

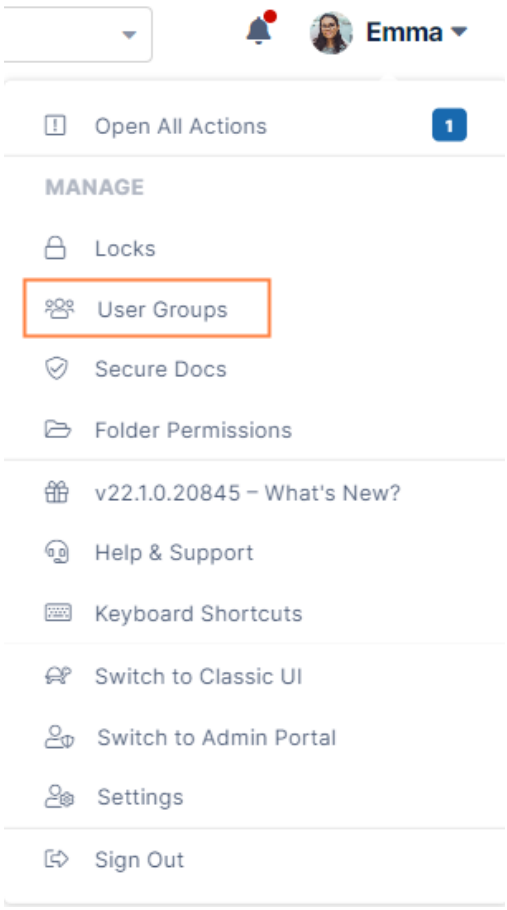


Giving Users Group Management Permissions

You can give users permission to add, edit, and delete groups by assigning them a policy that enables group permissions.

You can also give them permission to view, add members, or delete members for a specific group in the settings for the group. See Group Settings for more information about these types of settings.

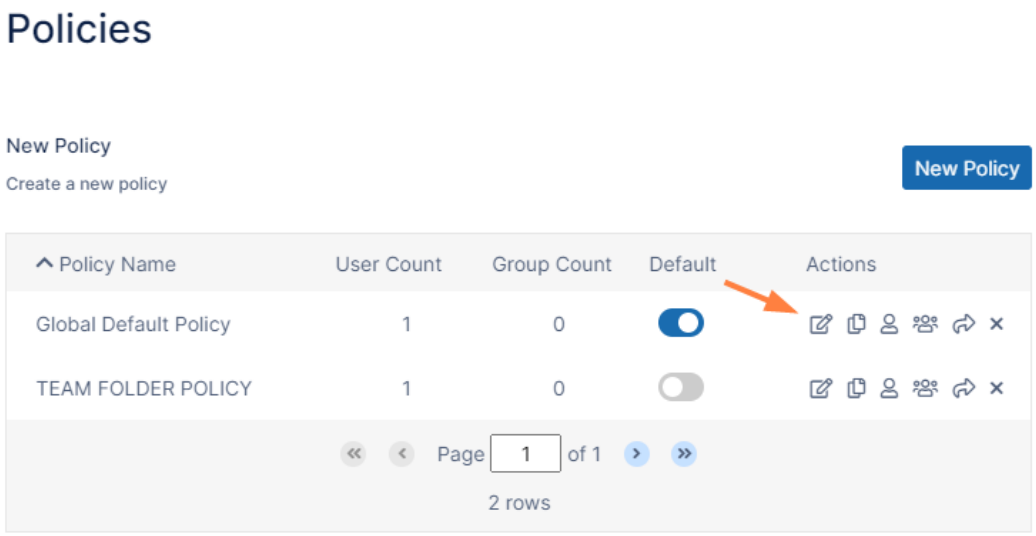
When users have either group permissions through their policies or through settings for a group, they have access to the **User Groups** option in the user portal:



For more information on user management of groups, see User Groups.

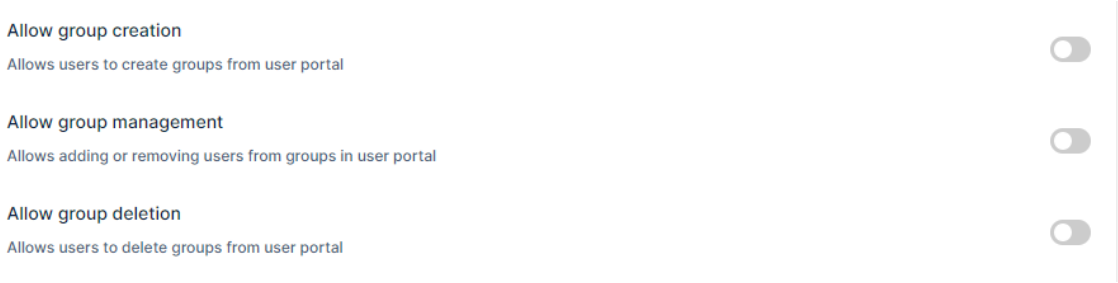
To add group permissions to a policy:

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** page opens.
2. Click the Edit icon for the policy of the users who you want to give group permissions.



The **Policy Settings** dialog box opens.

3. Click the **User Policy** tab.
4. Scroll down to see the Group policy settings.
   By default, each is disabled.



5. Change the group settings that you want to enable for users with this policy.

- **Allow group creation** - Allows the user to add new groups and manage members in the groups from the user portal.
- **Allows group management** - Allows the user to add and remove members from any group, including groups they have not created, from the user portal. This gives the user the ability to add and remove group members to groups created in the admin portal as well as groups created in the user portal.
- **Allow group deletion** - Allows the user to delete any groups, including groups they have not created, from the user portal. This gives the user the ability to delete groups created in the admin portal as well as groups created in the user portal.

  If none of these settings is enabled, users with the policy do not see the **Manage User Groups** option in the user portal unless group access is enabled for individual groups. See Group Settings.

Assign the Externals Group the Same File Access as the Everyone Group

The purpose of the Externals group is to limit the access external users have to shares and folders. However, if your use cases require that external users have the same access to files and folders as other users, you can give shares and folders that give permissions to the Everyone group the same permissions to the Externals group by running the tool **assignexternalsgroup.php**.

To run the Assign Externals Group tool:

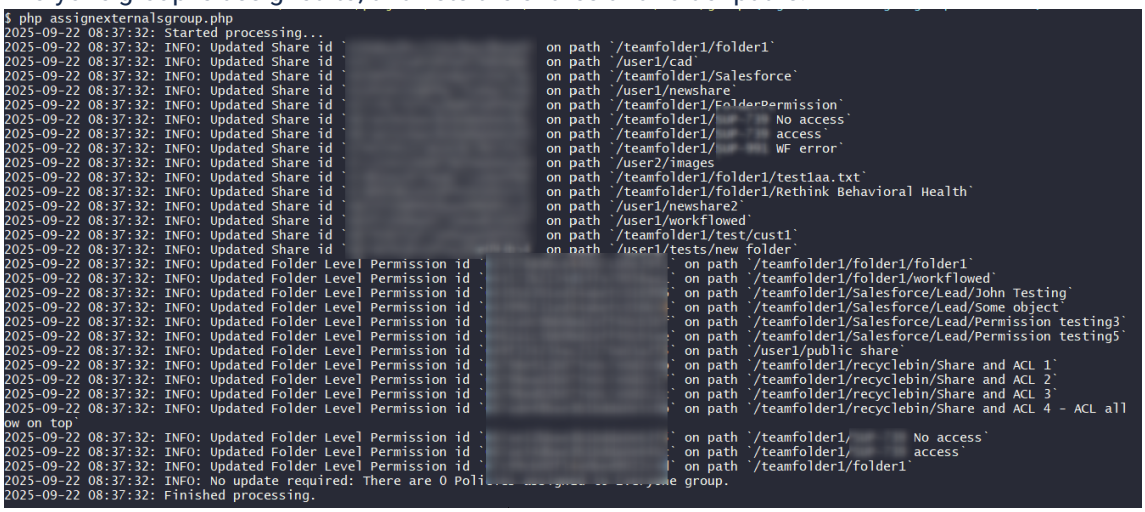
1. In a command line, go to the directory:
   Windows: **C:\xampp\htdocs\resources\tools\group**
   Linux: **/var/www/html/resources/tools/group**

2. In a command line, enter:

```
php assignexternalsgroup.php [--host="hostname"]
```

Parameters:
[optional] **--host** Site host name if different from default.

The tool adds the External group to the same shares, folder permissions, and policies that the Everyone group is assigned to, and lists the shares and folder paths:



> When the tool is run, it adds External users to all shares shared to the Everyone group, including Team Folder shares.

Admin User and Role Settings

Beginning in FileCloud 23.263, to change an email template's subject, promoted admin's must be in roles with **Customization/update** permission. Prior to this, promoted admins required roles with **System/update** permission to change an email template's subject.

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.

Main Admin. The admin account that is created when FileCloud is installed. There is only one Main Admin account in FileCloud.

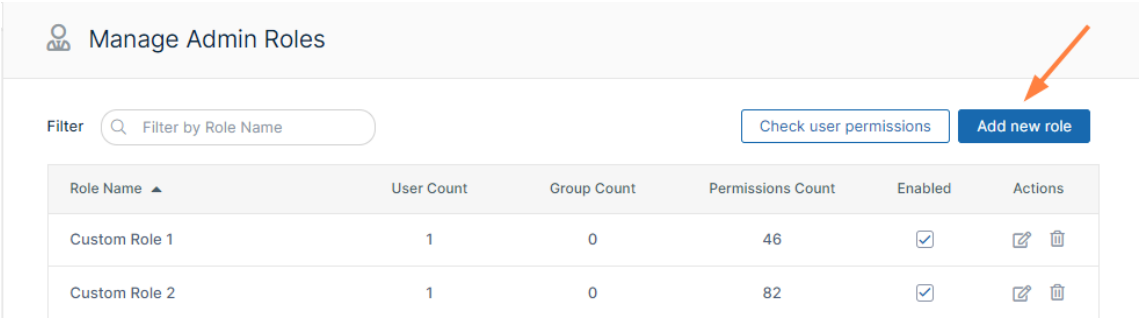
Admin User. User accounts that can access the FileCloud admin interface.

Admin Role. Role that defines the set of admin permissions for an admin user. If admin users have multiple admin roles, they have the combined admin permissions of all of the roles. For instructions on checking an admin user's permissions, see Managing Admin Users.

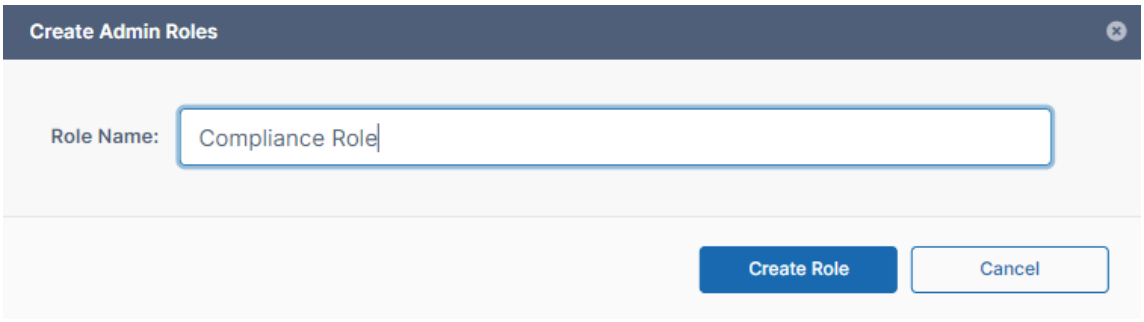
Creating admin roles and adding admin users

To create admin roles and add users to them:

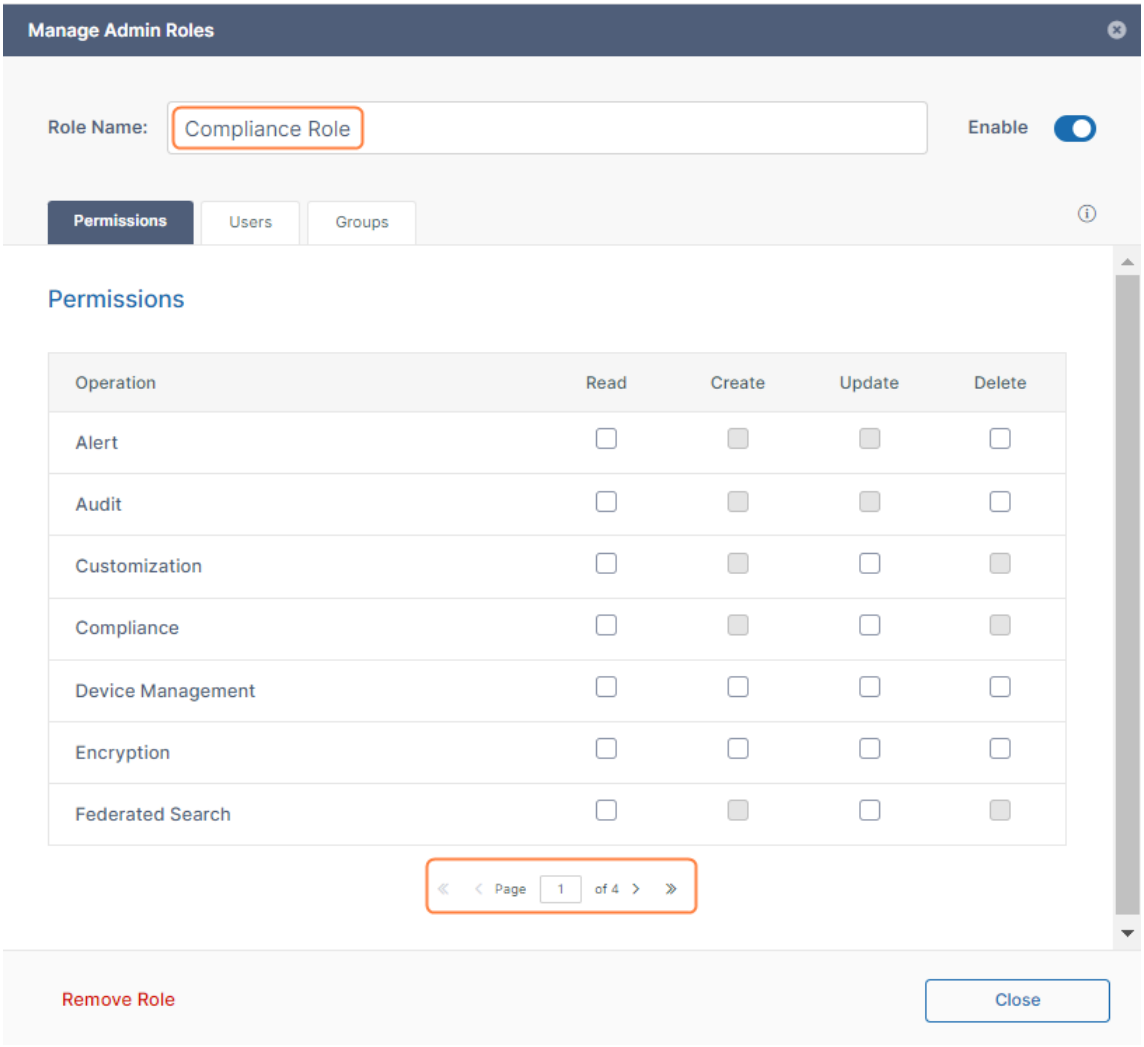
1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Add new role**.



   The **Create Admin Roles** dialog box opens.
3. In **Role Name**, enter a name for the role.

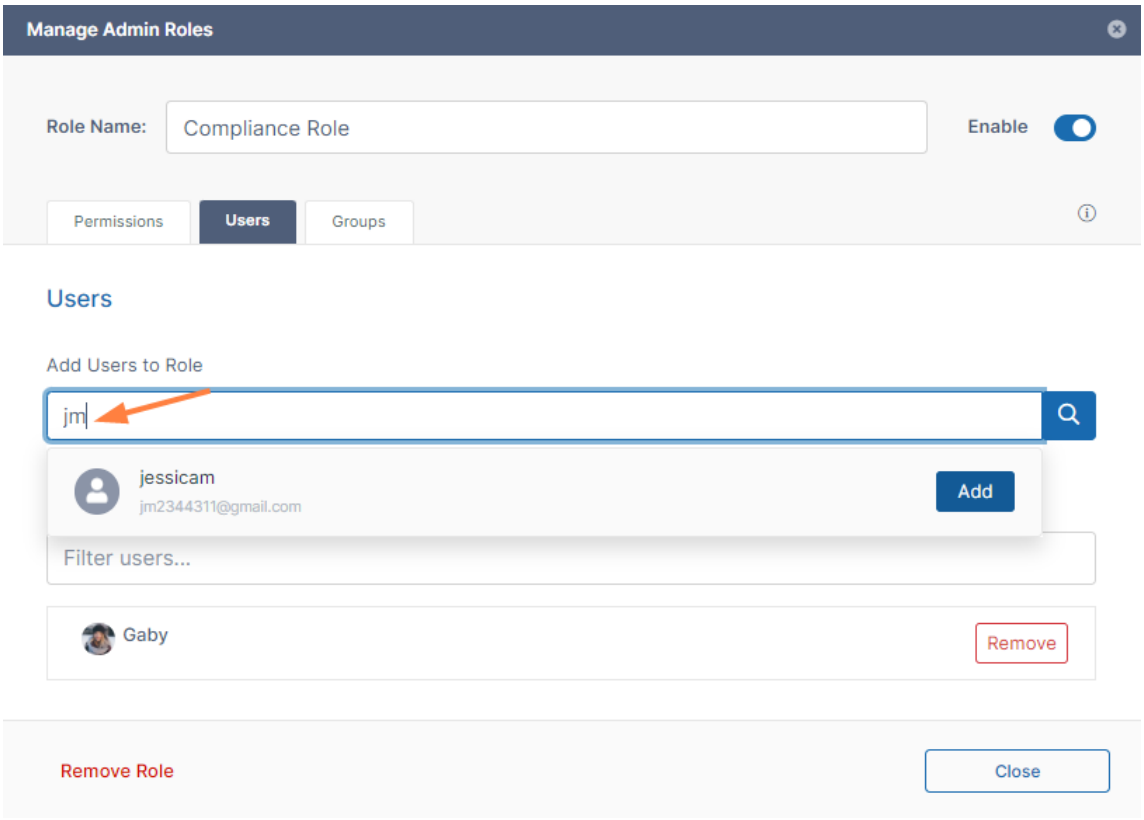


4. Click **Create Role**.
   The **Manage Admin Roles** dialog box opens to the first page of permissions. The new role is listed at the top of the dialog box.

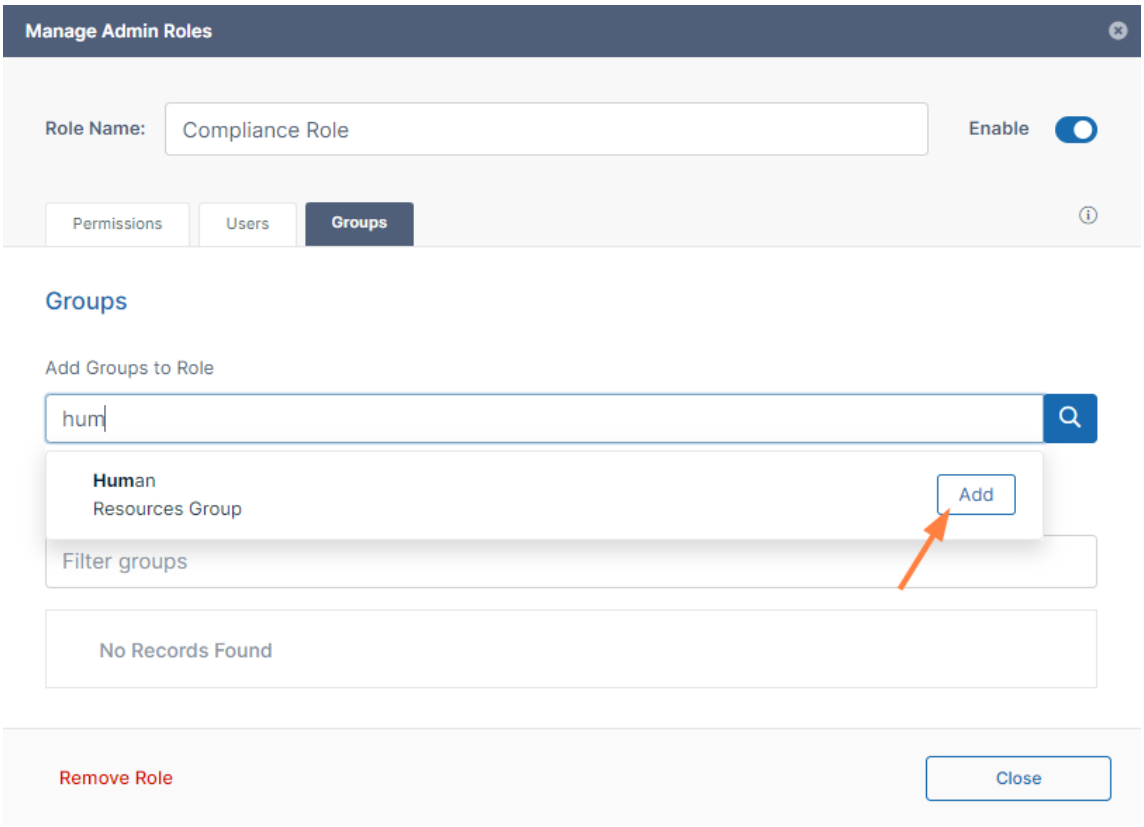


5. Go through each page of permissions, and check the permissions that you want to make available to the role.
6. When you have finished assigning permissions to the role, click the **Users** tab if you are ready to assign users to the role.

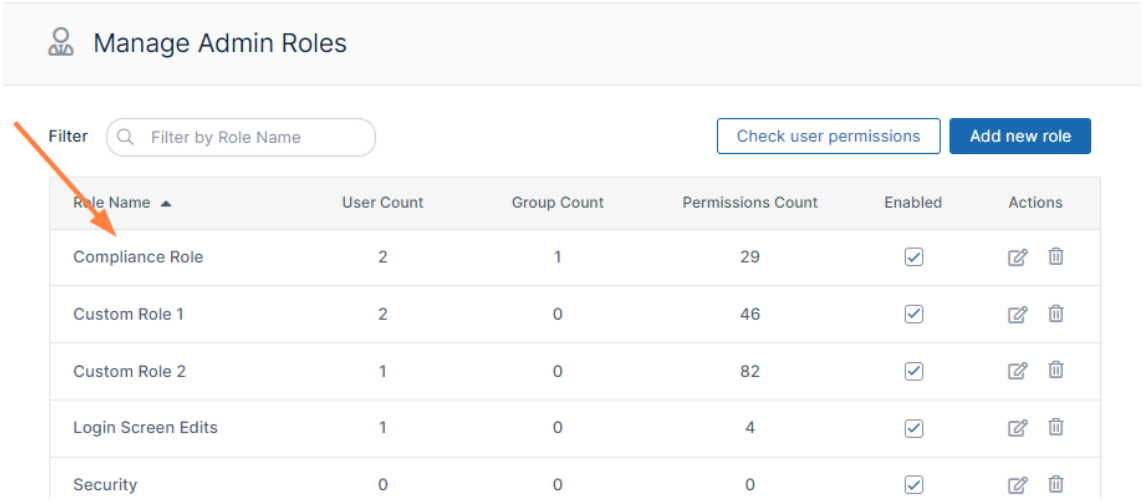
7. In **Add Users to Role**, enter each user that you want to add to the role. When the name appears, click **Add**.
   You can add **Full** and **Guest** users to roles, but not **External** users.
   If you add a user who is not an admin user to a role, the user automatically becomes and admin user.



8. To add groups to the role, click the **Groups** tab.
9. In **Add Groups to Role**, enter each group that you want to add to the role. When the name appears, click **Add**.
   Any users in a group who were not admin users automatically become admin users after the group is added to the role.



10. Click **Close**.
    The new role is listed on the page with its user, group, and permissions counts. It is enabled by default.



For instructions on removing an admin role, see Managing Admin Users.

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

Operation	Description
Alert	Alert item on the admin interface is visible. Authorization to view and clear alerts in admin interface.
Audit	Audit item on the admin interface is visible. Authorization to view, delete and export Audit Records.
Compliance	Compliance Dashboard on the admin interface is visible. Authorization to view and update compliance settings.
Customization	Customization item on the admin interface is visible. Authorization to customize the FileCloud interface. **Note**: Admin users must have **Customization > Update** enabled to be able to change the user login background and to change an email template's subject.
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.

Operation	Description
Reports	Reports menu item on the admin interface is available. Add, execute, edit and delete reports.
Retention	Retention menu item on the admin interface is available. Add, edit, and delete retention policies.
Rich Dashboard	View rich dashboard view including tables and graphs on the admin UI dashboard.
Settings	Settings item on the admin interface is visible. Authorization to view and modify FileCloud Settings.
Smart Classification	Smart Classification menu item on the admin interface is available. Add, update, run, and delete content classification rules.
Smart DLP	Smart DLP menu item on the admin interface is available. Add, edit, and delete DLP rules.
System	System item on the admin interface is visible. Authorization to run system checks, install check, generate logs and UPGRADE FileCloud to new version.
Team Folders	Set up Team Folders, add, edit, delete and manage team folder and corresponding permissions. *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.
Watermark	Watermark menu item on the admin interface is visible. Authorization to view, create, edit and delete watermarks.
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.

MFA Settings for Promoted Admins

When a user is configured as an admin user, if 2FA is enabled for admins, by default, the MFA delivery mode set for the user account (in the user's policy) is used for the Admin account. If the setting TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS is enabled, the 2FA method set for administrators is used for the admin account.
To use the 2FA method set for administrators:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To use the 2FA method set for administrators, add the line:

```
define("TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS", true);
```

User Authentication Settings

FileCloud provides multiple ways of authenticating a user account. This is applicable for both FULL and GUEST user accounts.

FileCloud supports the following Authentication modes:

- Default Authentication
- Active Directory based Authentication
- LDAP based Authentication

FileCloud also supports Single Sign-on technologies including SAML, ADFS, and NTLM.

Comparison of Default authentication, AD, and LDAP

A user account can only have one of these types of authentication.

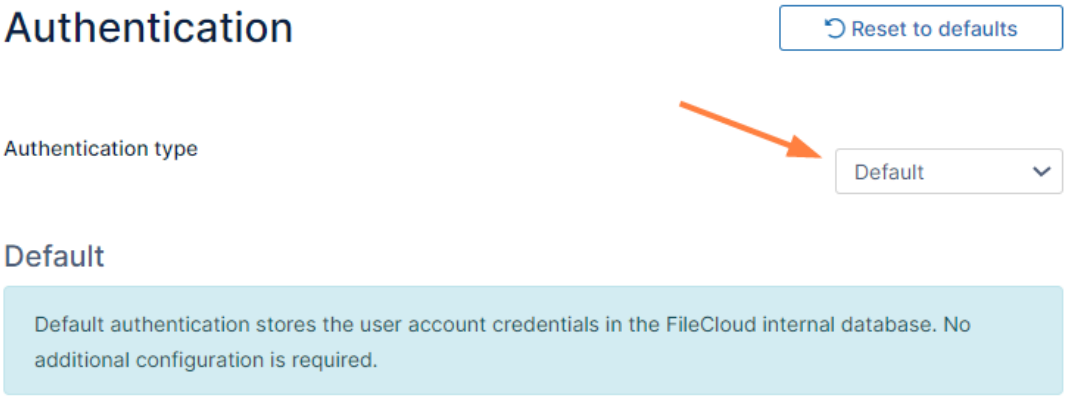
	Default Authentication	**AD**	**LDAP**
Authentication	Performed by FileCloud	In AD Server	In LDAP Server
Allowing Users to Create Accounts	Permitted	Not Permitted	Not Permitted
Bulk User creation	using CSV files	Import from AD group	Not Available
Can Admin Change Password	Password change for all users allowed	Passwords for Active Directory users are managed by Active Directory and cannot be changed directly within FileCloud.	Passwords for LDAP user can only be changed in LDAP server.
Can user change/ reset password	Yes	Passwords for Active Directory users are managed by Active Directory and cannot be changed directly within FileCloud.	Passwords for LDAP user can only be changed in LDAP server
User Account Types	Full, Guest, External	Full, Guest	Full, Guest

Enabling Default Authentication

Initially, FileCloud is set to default authentication mode. User accounts created when this authentication type is configured have credentials stored and managed within FileCloud.

To enable Default Authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication** .
   The **Authentication** settings page opens.
2. If **Authentication type** is not already set to **Default**, change it to **Default** and click **Save**.



Active Directory Authentication

For admins upgrading to FileCloud 23.251:

- Prior to version 23.251, FileCloud always used the AD attribute **mail** to authenticate AD users, even if the **AD mail attribute** field in FileCloud specified a different attribute.

  This has been fixed. However, if you used an AD attribute other than the **mail** prior to version 23.251, AD users imported into FileCloud prior to 23.251 will now receive an error when they try to log in to FileCloud (unless the non-**mail** attribute always has the same value as the **mail** attribute). If you have users who may have trouble logging in for this reason, prior to updating to 23.251, change the **AD mail attribute** field back to **mail**.

Note
AD users count towards the FileCloud license only after:

- The user account logs in to FileCloud

- A user from AD is explicitly imported

In this type of authentication mechanism, a user account is authenticated against an external Active Directory server.

Prerequisites

Required	Configuration Requirement	Notes
Active Directory service	Must be accessible from FileCloud	IP and Port must be accessible.
Active Directory	Must support Simple Authentication Method	Must use simple bind authentication, either anonymously or with a username and password.
Active Directory users	Must have an email attribute FileCloud username must match AD user login name **Important**: The FileCloud username cannot be changed.	Beginning in FileCloud 21.2, the AD Account name used in Active Directory settings must have an email ID in Active Directory. The email address is saved in the user's FileCloud profile. During login, validation requires the FileCloud email address and the AD email address to match; later modification of email address in AD or FileCloud will cause login to fail.
FileCloud Server		

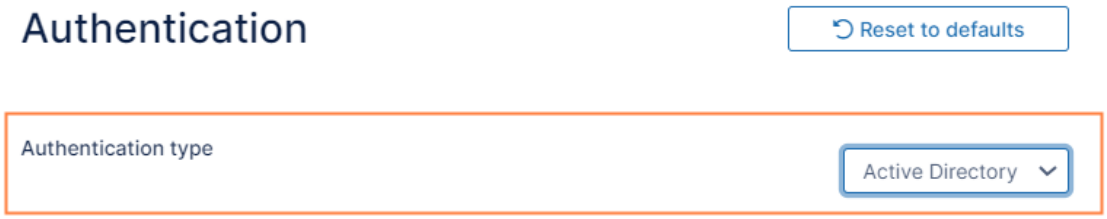
How To Enable AD Authentication

Enabling AD Authentication

To enable AD authentication in FileCloud:

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

2. Under **Authentication**, change **Authentication type** to **Active Directory**, and **click Save.**

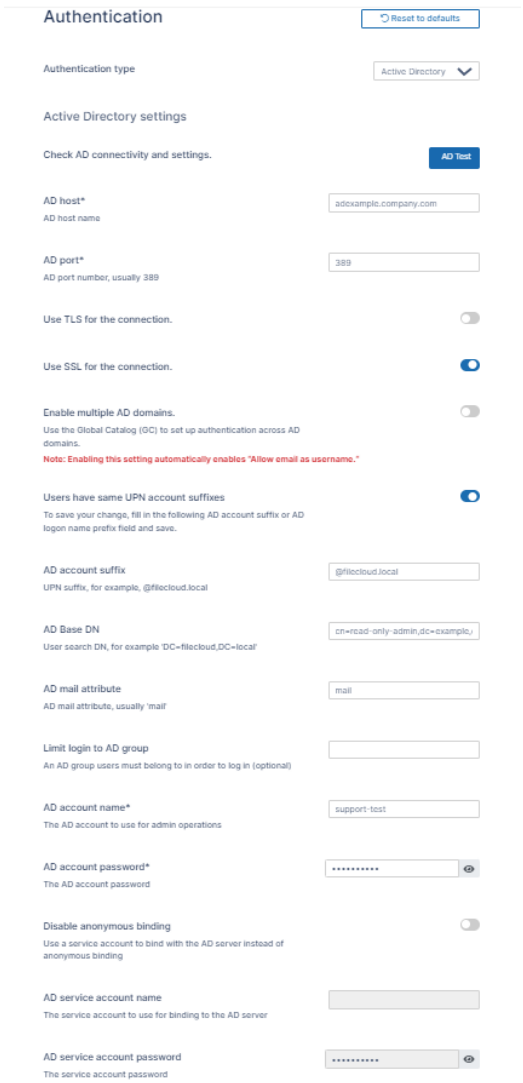


   Additional settings appear.

3. Enter the required information in the settings under **Active Directory Settings** (See **AD configuration parameters**, below) and then click **Save**.
   Note: The changed parameters must be saved before performing an AD test.

AD configuration parameters

To connect FileCloud with your AD environment, fill in the settings as shown in the following screenshot.



AD host - Required. Either the IP address or host name of the AD server.

AD port - Required. Enter **389** for non-SSL, or enter **636** for SSL.

Use TLS for the connection - Optional. Enable this setting if your AD server requires clients to use TLS to connect.

Use SSL for the connection - Optional. Enable this setting if your AD server requires clients to use SSL to connect. NOTE: Additional change required.

Enable multiple AD domains - Enable this setting to authenticate and sync users and groups across multiple trusted AD domains. For more information about this feature, see Authenticate Users Across Trusted AD Domains.

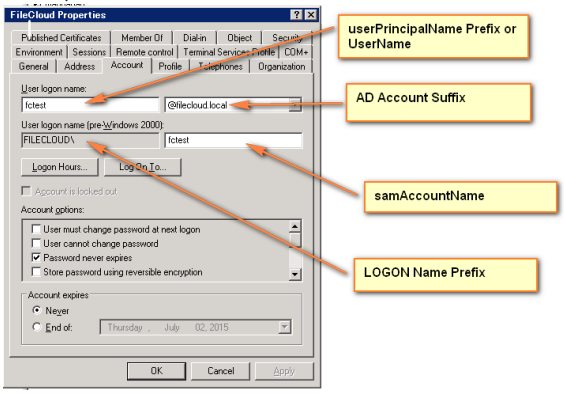
Users have same UPN account suffixes
Enabled by default. All of your AD users should have the same suffix.

- If your users have the same UPN suffixes:
  Leave this setting enabled, and enter the suffix in the next field, **AD account suffix**.

- Otherwise:
  Disable this setting. The next field changes to **AD logon name prefix** as in the following screenshot. Set **AD logon name prefix** (a trailing '\' is not required). See Mixed AD Authentication support.



To find the **AD logon name prefix** and the **AD account suffix**, refer to:



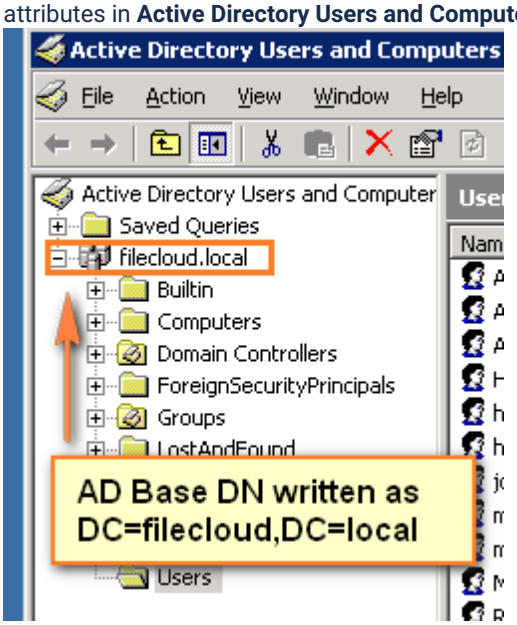
AD account suffix - The UPN suffix for your domain, the part after **User logon name** in the dropdown next to it in the above screenshot.

Instead of viewing the properties as shown above, you can get the account suffix by running the following query in the command line in the AD server:

*dsquery * <FULLY QUALIFIED NAME> -scope base -attr sAMAccountName userPrincipalName*



AD Base DN - Required. Do not enter value with quotes. The Base DN for your domain. Located in the extended attributes in **Active Directory Users and Computers MMC**:



You can also get the Base DN by running the following query in the command line in the AD server.

dsquery user -name <LOGON NAME>

	 **AD mail attribute** - Required. FileCloud requires each user account to have an associated email id. Typically the name of this attribute in AD is **mail**. If a user account has no mail attribute, then login to FileCloud will fail. If a mail attribute is present, and login fails, then check the base DN to ensure it is accurate and is without quotes. **Limit login to AD group** - Optional. To limit login to specific users, add them to a group and specify the group name here. (Typically this is left blank.) If you set this field, ensure that the account name specified in **AD account name** is part of the AD group. **AD account name** - Required. A valid account name is required here in order for FileCloud to query the AD server. This can be any account that can access the AD server, and is located in **User logon name** in the **FileCloud Properties** screenshot, above. **Notes:** Enter username, not email id in this field. This account must have an email address set in AD. **AD account password** - A password for the AD account name. **Disable anonymous binding** - Optional. Enable this checkbox if your AD does not allow anonymous binding. Enabling this checkbox enables the **AD service account name** and **AD service account password** text boxes. **AD service account name** - Optional. The service account name to use to bind with the AD server. **AD service account password** - Optional. The service account password to use to bind with the AD server.



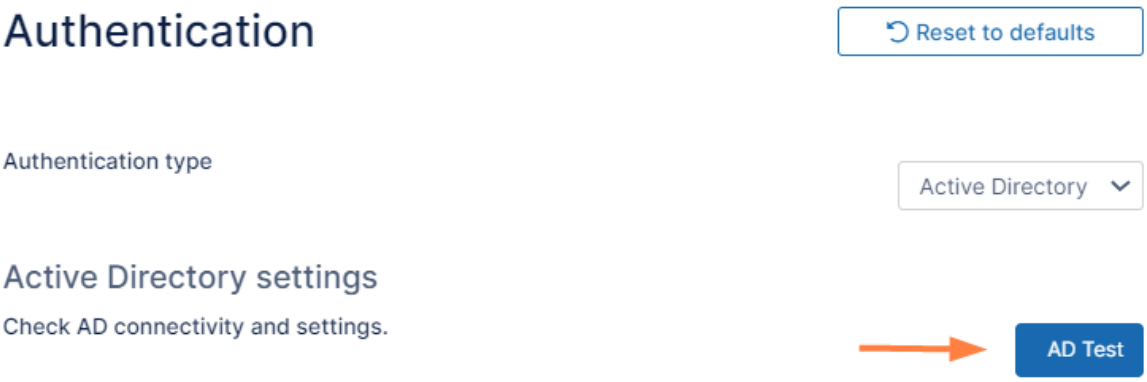
To connect to Active Directory over SSL, please follow the steps mentioned here.



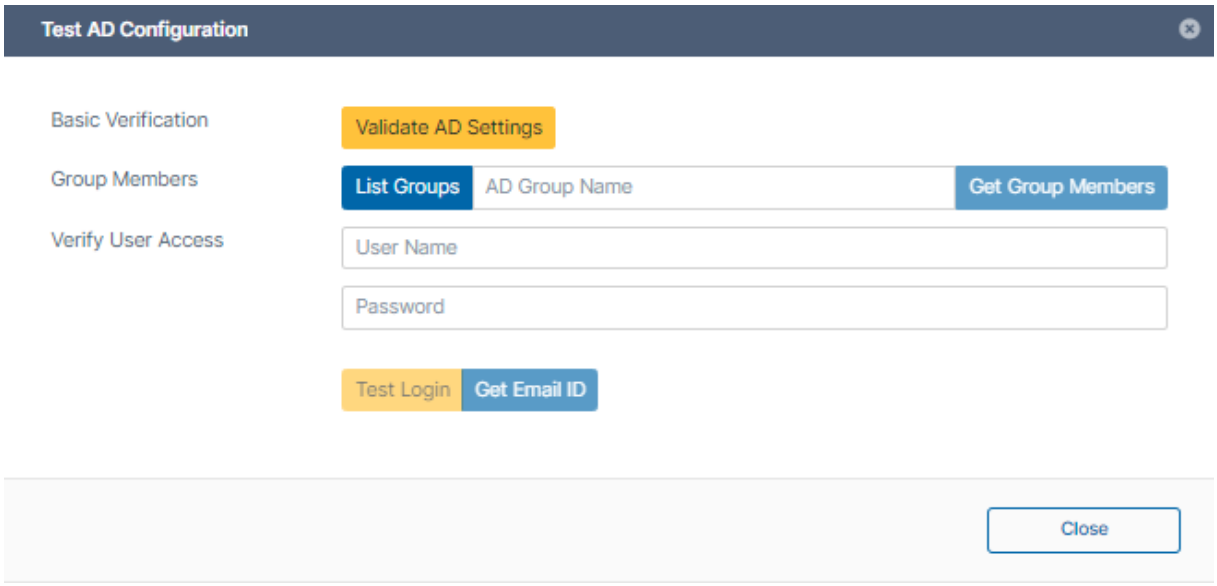
Make sure the settings are SAVED before trying the AD Tests to verify connectivity

Testing AD Connectivity

Once all data is entered and saved, test the AD settings by clicking the **AD Test** button.

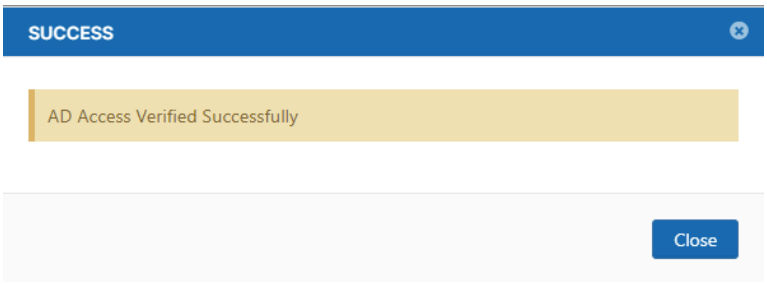


A **Test AD Configuration** dialog box opens:



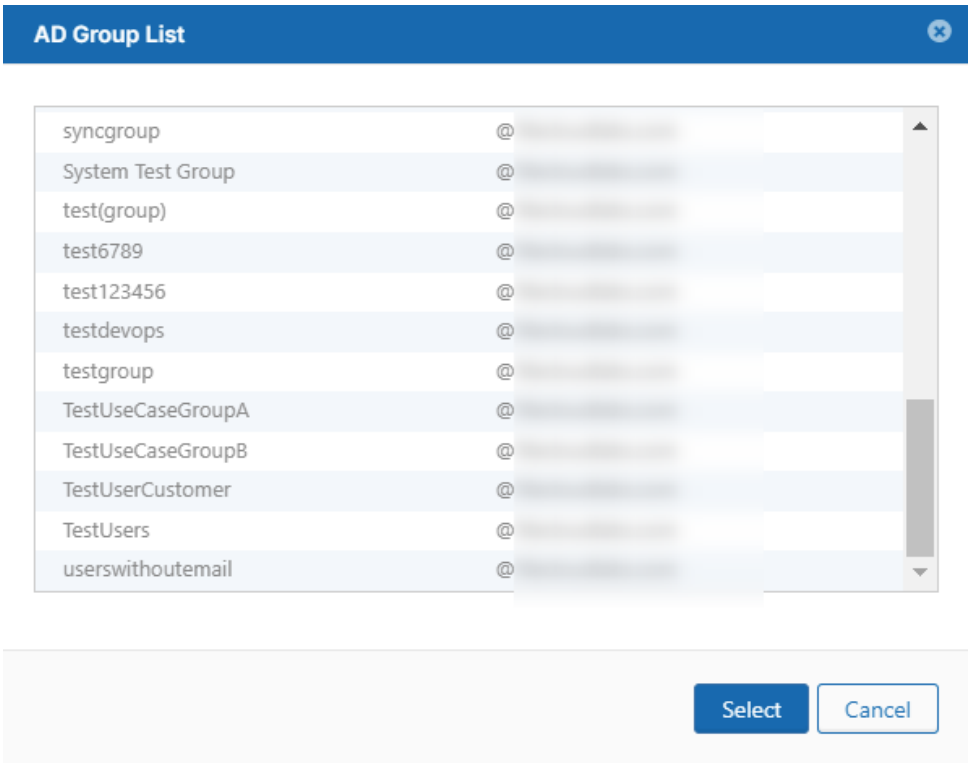
The following tests can be done.

1. Validate AD settings.
    a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server.
    You should receive the response:

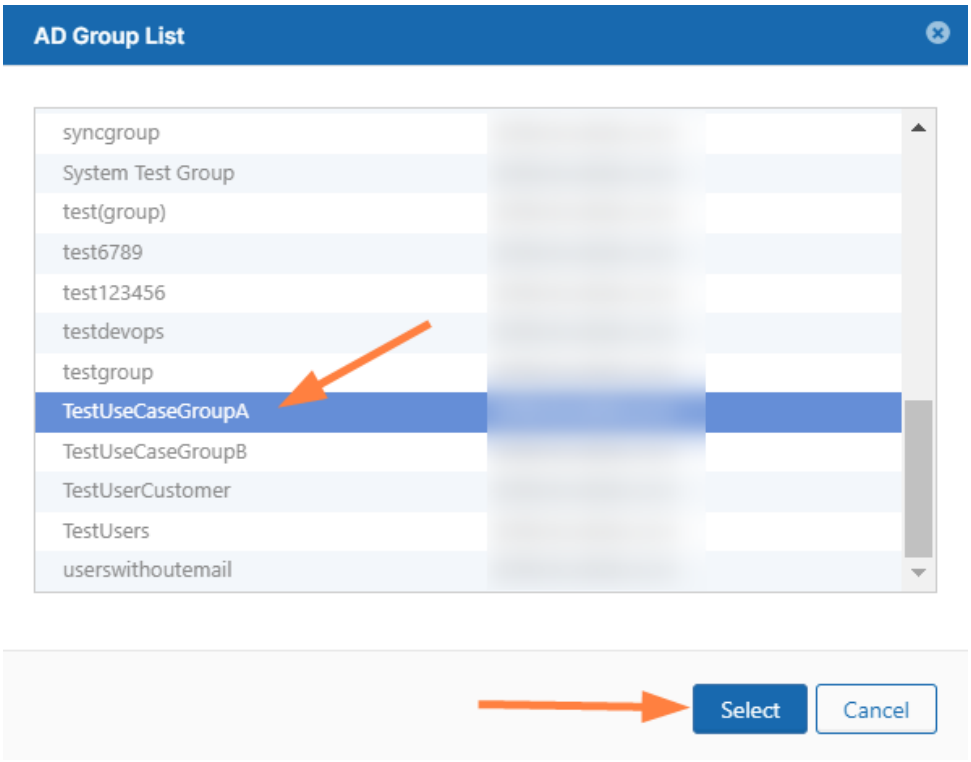


If the tests fail, then check your AD settings to ensure all the data is present and is accurate.

2. List Groups
   a. Once AD settings are validated, click **List Groups** to view the list of groups read from the server.
   You should see a list similar to:

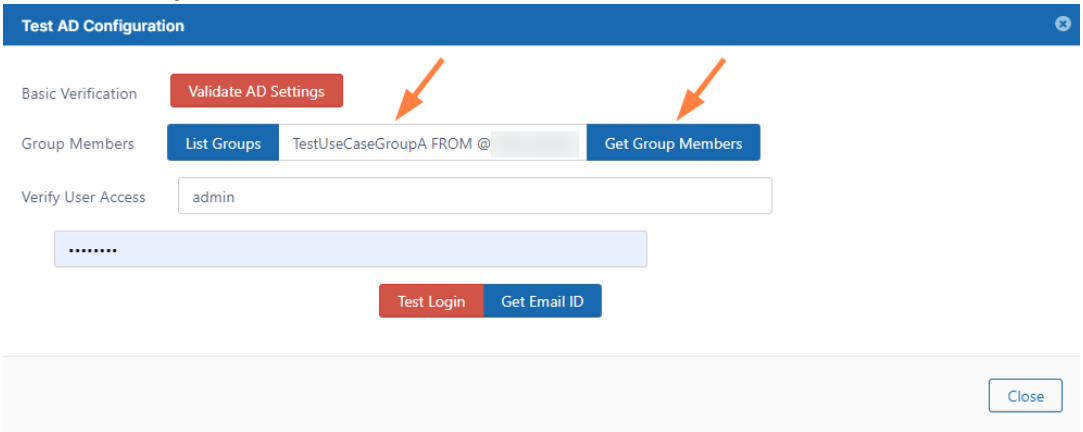


3. Get Group Member
   a. Click **List Groups**, then select a group and click **Select**.

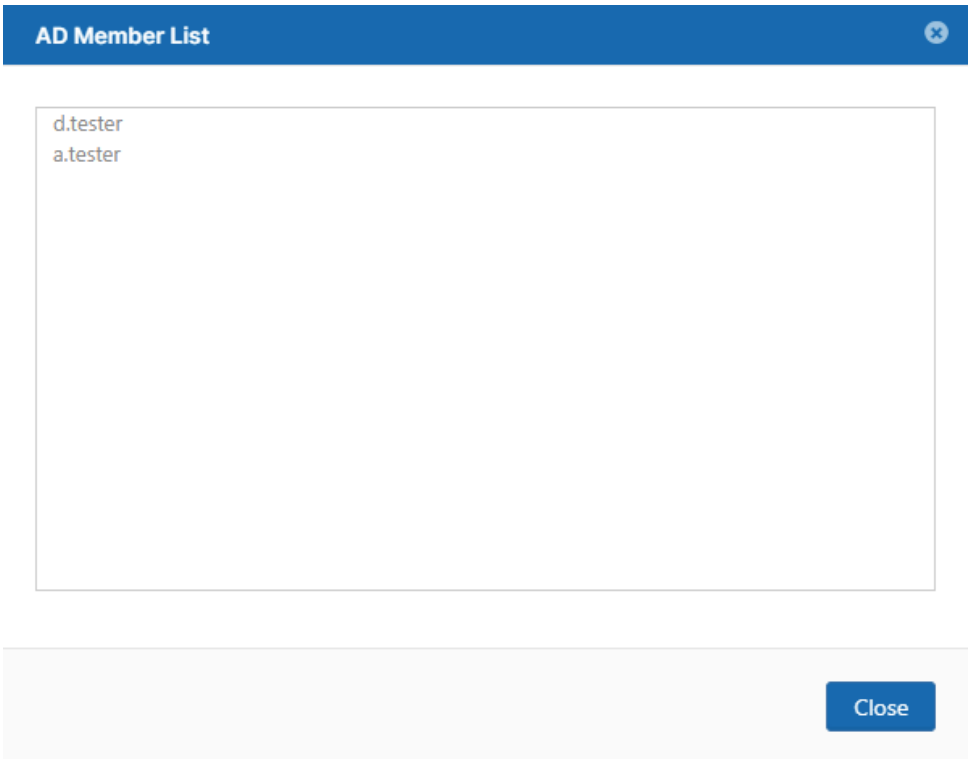


The Group name appears in the **Test AD Configuration** dialog box.
(You can also enter the group name directly into the text box without selecting from the **AD Group List** popup.)

b. Click **Get Group Members**.



The **AD Members List** should list the correct members of the group:



Note: The group members are NOT automatically added to FileCloud.

4. Verify User Access
   a. Enter a specific user name and password and click **Test Login** to make sure the user can log in to AD.
   If not, check if the AD suffix or AD prefix matches the one entered in the **AD account suffix** or **AD logon name prefix** in the FileCloud admin portal or the AD server.
   b. Enter a specific user name and password and click **Get Email ID.**
   This should return the correct email address for a user account from AD. If a valid email address is not returned, then FileCloud cannot import the user account. Check if the email address is included for the user on the AD Server.

In this section:

More Information:

FileCloud Blogs
Import Users to AD via PowerShell

Connecting to AD via SSL

If you want to securely add users, change passwords, or connect to the Active Directory server being used with your FileCloud site, then you will need to use an SSL certificate.

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to Active Directory. By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology.

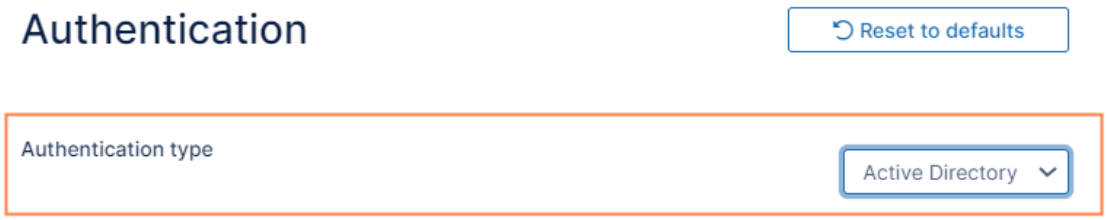
Before you can enable the use of SSL certificates in FileCloud Server, you must have completed the following steps:

1. Install and configure your Active Directory server
2. Install an SSL certificate on your Active Directory server

How do I enable the use of SSL in FileCloud Server?

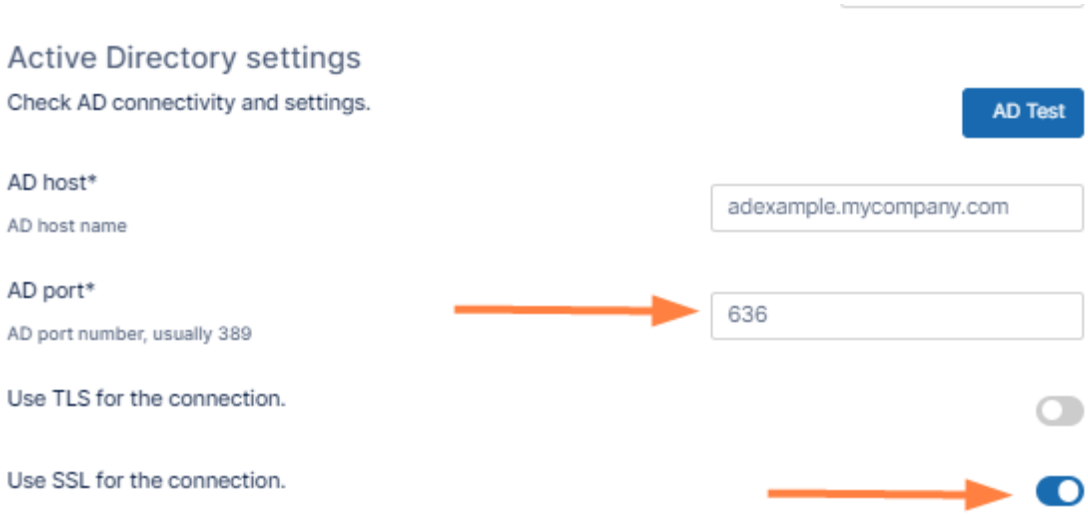
To enable the use of SSL Certificates in FileCloud Server:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication** .
   The **Authentication** settings page opens.
2. Under **Authentication**, change **Authentication type** to **Active Directory**, and **click Save.**



   Additional settings appear.
3. In **AD port**, change the number to **636**.

4. Enable **Use SSL** for the connection.



5. Click **Save**.

How can I troubleshoot my AD/SSL connection?

If you have problems connecting after setting the above and non-SSL connections work OK, you might have to set this additional parameter.

1. Create an **ldap.conf** file.

Windows Location: **c:\openldap\sysconf\ldap.conf**
Ubuntu Location: **/etc/ldap/ldap.conf**
RHEL Location: **/etc/openldap/ldap.conf**

2. Add the following command to the **ldap.conf** file:

```
#
# LDAP Defaults
#
TLS_REQCERT never
```

3. Restart Apache server.

How do I connect to AD using TLS?

Connecting to Active Directory over TLS

TLS

To use TLS, use port **389** instead of port **636**, and enable **Use TLS for the connection** instead of **Use SSL for the connection**.

To disable use of TLS v1.2 behavior, if necessary, add the following to WWWROOT/thirdparty/adLDAP.php

```
if ($this->useSSL) {
putenv("LDAPTLS_CIPHER_SUITE=NORMAL:!VERS-TLS1.2");
$this->ldapConnection = ldap_connect("ldaps://" . $domainController, $this->adPort);
} else {
$this->ldapConnection = ldap_connect($domainController, $this->adPort);
}
```

Authenticating to Multiple AD servers

The instructions on this page show you how to authenticate to multiple AD servers by separately configuring each of the AD servers in your domain forest. To configure authentication of all of the AD servers in your domain forest using the Global Catalog (GC), see Authenticate Users Across Trusted AD Domains.

Although the latest versions of the Windows Server operating system handle large numbers of objects more efficiently, there are many reasons why organizations implement multidomain forests.

An example of this is a university.

- In the Faculty of Science, there are different departments or schools, such as the school of physics and the department of botany
- For political or organizational reasons it might have been decided that each department or school should have its own domain that is a part of the overall university forest
- Active Directory gives organizations the ability to create domain namespaces that meet their needs

Why would I use a multidomain AD structure?

The reasons for using multidomain AD structures can include but are not limited to:

- **Historical domain structure.** Some organizations have retained the forest structure that was established when the organization first adopted Active Directory.
- **Organizational or political reasons.** Some organizations are conglomerates, and they might be comprised of separate companies that share a common administrative and management core.

- **Security reasons Domains.** Some organizations need to create authentication and authorization boundaries. You can also use domains to partition administrative privileges so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it's possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

For more information on using multidomain AD infrastructure, on the Microsoft Web site, read AD Directory Services Getting Started.

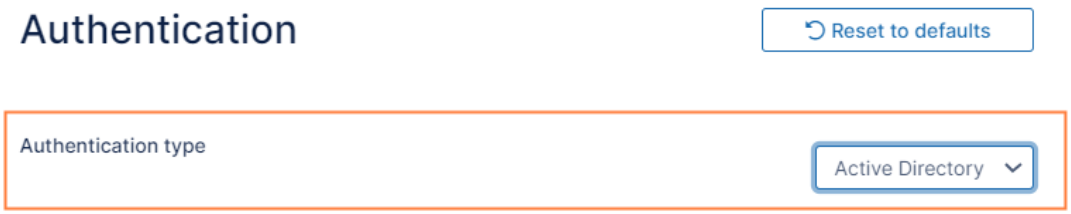
Enable multiple AD server authentication

To enable multiple AD server authentication, configure settings in the following places:

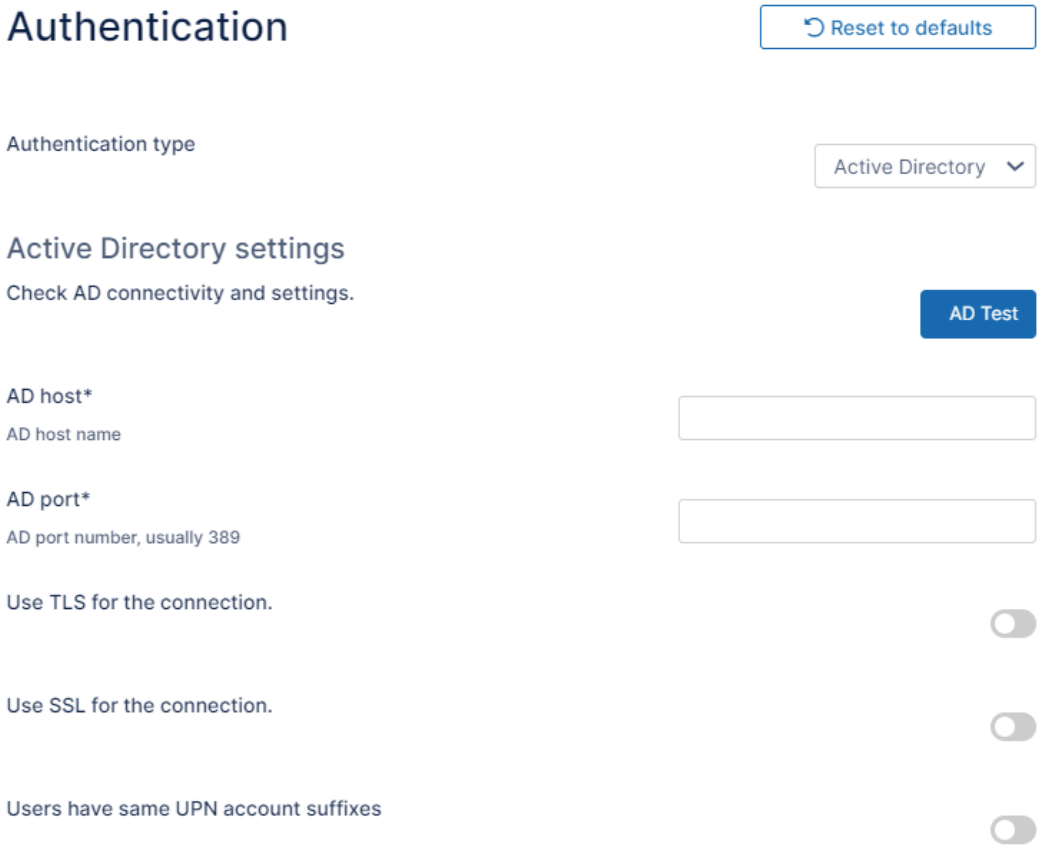
- adconfig.php file
- Admin Dashboard

To enable multiple AD server authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** settings page opens.
2. Under **Authentication**, change **Authentication type** to **Active Directory**, and **click Save.**



   Additional fields appear.



3. Fill in the fields as instructed on the page Active Directory Authentication.
4. Create a file called **adconfig.php** in one of the following locations, depending on your OS:

```
Windows Location
c:\xampp\htdocs\config\adconfig.php


Linux Location
/var/www/htdocs/config/adconfig.ph
```

5. Add the information for the other AD servers using the following example. ⚠ Do not add the same AD server detail that was already configured in Admin Dashboard.

```
<?php
/* Configuration values for ActiveDirectory Authentication */
// ... Multi-AD Server Support, set to 1 to enable additional AD servers
define("TONIDOCLOUD_MULTI_AD_ENABLE", 1);
//=============== SITE 1 ==============================
```

```
define("TONIDOCLOUD_AD_HOST_1", "ADSERVERHOST" ); // < ActiveDirectory Host
define("TONIDOCLOUD_AD_PORT_1", 389 ); // < ActiveDirectory port
define("TONIDOCLOUD_AD_ACCOUNTSUFFIX_1", "@mysite.internal"); // < User Login Name Suffix
//define("TONIDOCLOUD_AD_LOGONNAMEPREFIX_1","SST"); // use this if prefix is needed. Note use only prefix or suffix
define("TONIDOCLOUD_AD_BASEDN_1", "DC=mysite,DC=internal"); // < User Search DN
define("TONIDOCLOUD_AD_MAILATTRIBUTE_1", "mail"); // < Mail Attribute
define("TONIDOCLOUD_AD_LIMIT_GROUP_1", ""); // < If you want login users to be limited to a specific AD group
define("TONIDOCLOUD_AD_USETLS_1", false); //<< If you want to use TLS set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_USESSL_1", false); //<< If you want to use SSL set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_ACCOUNTNAME_1", "Administrator"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ACCOUNTPASSWORD_1", "adminpassword"); // < Account Password for Admin Operations
define("TONIDOCLOUD_AD_USEADMINBINDING_1", "0"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ADMINACCOUNTNAME_1", ""); // < AD Service Account Username
define("TONIDOCLOUD_AD_ADMINACCOUNTPASSWORD_1", ""); // < AD Service Account Password
//=============== SITE 2 ============================
define("TONIDOCLOUD_AD_HOST_2", "ADSERVERHOST2" ); // < ActiveDirectory Host
define("TONIDOCLOUD_AD_PORT_2", 389 ); // < ActiveDirectory port
define("TONIDOCLOUD_AD_ACCOUNTSUFFIX_2", "@mysite2.internal"); // < User Login Name Suffix
//define("TONIDOCLOUD_AD_LOGONNAMEPREFIX_1","SSK"); // use this if prefix is needed. Note use only prefix or suffix
define("TONIDOCLOUD_AD_BASEDN_2", "DC=mysite2,DC=internal"); // < User Search DN
define("TONIDOCLOUD_AD_MAILATTRIBUTE_2", "mail"); // < Mail Attribute
define("TONIDOCLOUD_AD_LIMIT_GROUP_2", ""); // < If you want login users to be limited to a specific AD group
define("TONIDOCLOUD_AD_USETLS_2", false); //<< If you want to use TLS set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_USESSL_2", false); //<< If you want to use SSL set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_ACCOUNTNAME_2", "Administrator"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ACCOUNTPASSWORD_2", "adminpassword"); // < Account Password for Admin Operations
define("TONIDOCLOUD_AD_USEADMINBINDING_2", "0"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ADMINACCOUNTNAME_2", ""); // < AD Service Account Username
define("TONIDOCLOUD_AD_ADMINACCOUNTPASSWORD_2", ""); // < AD Service Account Password
?>
```

Now additional users from these domains can also login into FileCloud.

To allow duplicate usernames for different domains

If you are using SSO, SSO API, or Active Directory (AD) to import users, FileCloud uses the imported user's email username (the portion before @) as the FileCloud username. However, by default, FileCloud does not allow creation of users with the same usernames.

If any of your users have multiple email addresses, there may be a situation where the email username (the portion before @) is the same but the domains are different in their multiple emails. In this case, FileCloud will attempt to convert the second email username (and any further emails with the same username) to the FileCloud username, which will fail because the username already exists.

However, if the multiple email addresses actually represent different users, you may use the following setting to enable creation of multiple users:

1. Open cloudconfig.php at
   - Windows: xampp/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Add the following and save:

   ```
   define("TONIDOCLOUD_ALLOW_DUPUSERNAMES",1);
   ```

   Now:
   If you create a a user with the username **jocelynp** and email **jocelynp@gmail.com**, FileCloud creates a user with the username **jocelynp**.
   Next, if you attempt to create a user with the username **jocelynp** and email **jocelynp@optimum.net**, FileCloud creates a user with the username **jocelynp_optimum**.
   This follows for any subsequent emails with the same username and a unique domain.

Use encrypted AD account password in the configuration file

To encrypt an AD password using the adpasswordencryption tool:

1. Open a command line.
2. Enter the following:
   Windows:

   ```
   $ cd C:\xampp\htdocs\resources\tools\security\
   $ C:\xampp\php\php adpasswordencryption.php
   ```

   Linux:

   ```
   $cd /var/www/html/resources/tools/security/
   php adpasswordencryption.php
   ```

3. At the prompt, enter your password:

   ```
   This tool encrypts an AD password string to be used in the adconfig.php
   configuration files of FileCloud
   ```

```
Enter your password: [your-password-string]
```

4. As instructed, copy the encrypted password string returned:

```
Carefully copy paste the following string to adconfig.php key
TONIDOCLOUD_AD_ENC_ACCOUNTPASSWORD or TONIDOCLOUD_AD_ENC_ADMINACCOUNTPASSWORD:
zk8aQV6+L1Q7kA7N6JGgj2MzNjRkNzMwMTU0OTY0MjAzMGVhNWI0NDM5NjIxMWI2N2UzMzRkZTcwNjE2Yz
gxOTk0YzVjNjI2ZGQ2NjgzMTZ1bTJBN0gwdmdabHYzQzlmQm9IZUN3PT0=
```

To paste the encrypted password into adconfig.php:

1. Navigate to the adconfig file:
   Windows: **xampp > htdocs > config**
   Linux: **/var/www/htdocs/config**
2. Rename **adconfig-sample.php** file to **adconfig.php**.
3. To add an encrypted password for AD admin operations, add:
   define("TONIDOCLOUD_AD_ENC_ACCOUNTPASSWORD", "encryptedpassword");
   To add an encrypted password for the ad service account, add:
   define("TONIDOCLOUD_AD_ENC_ADMINACCOUNTPASSWORD", "encryptedpassword");

FileCloud will decrypt the passwords when it makes the directory calls.

Authenticate Users Across Trusted AD Domains

> The ability for admins to configure FileCloud to sync users and groups across multiple trusted AD domains through the FileCloud admin portal is available in FileCloud 23.252.

Organizations may maintain multiple AD domains (and sub-domains) in a structure referred to as an **AD forest**, which authenticates user access to all of the included domains, enabling actions such as searching to be performed across all of the domains. A **Global Catalog (GC)** helps manage an AD forest by indexing all of its domains so they can be cross referenced easily.

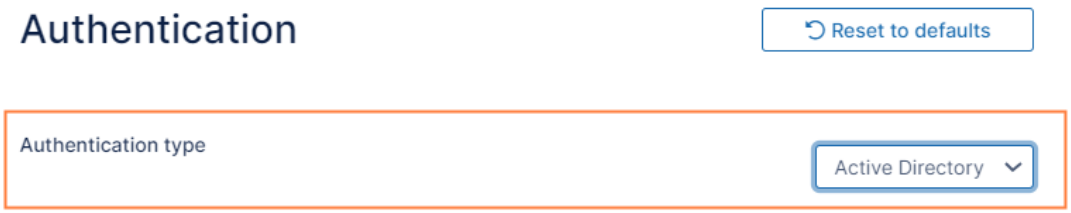
The instructions on this page show you how to configure authentication of all of the AD servers in your domain forest using the Global Catalog (GC). To authenticate to multiple AD servers by separately configuring each of the AD servers in your adconfig file, see Authenticating to Multiple AD servers.

You can sync FileCloud users and groups with all domains in an AD forest by enabling **Enable multiple AD domains** in the Authentication settings for Active Directory. When this setting is enabled, the users in that AD forest are required to log in with their full email addresses to enable cross-domain resolution.

For more information on using a multidomain AD infrastructure, see AD Directory Services Getting Started.

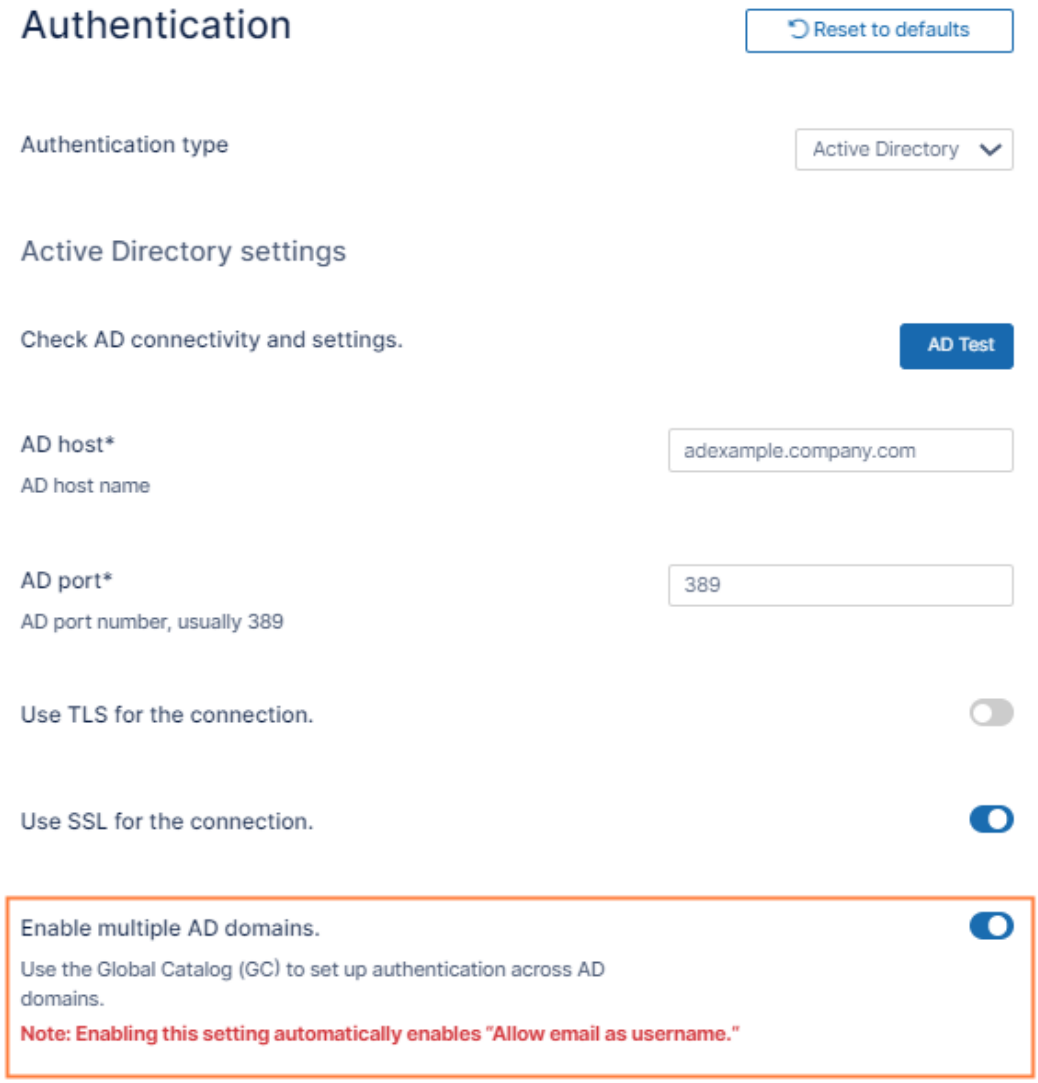
To enable multiple AD server authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** settings page opens.
2. Under **Authentication**, change **Authentication type** to **Active Directory**, and click **Save.**



   Additional fields appear.

3. Toggle on **Enable multiple AD domains**.



When **Enable multiple AD domains** is toggled on:

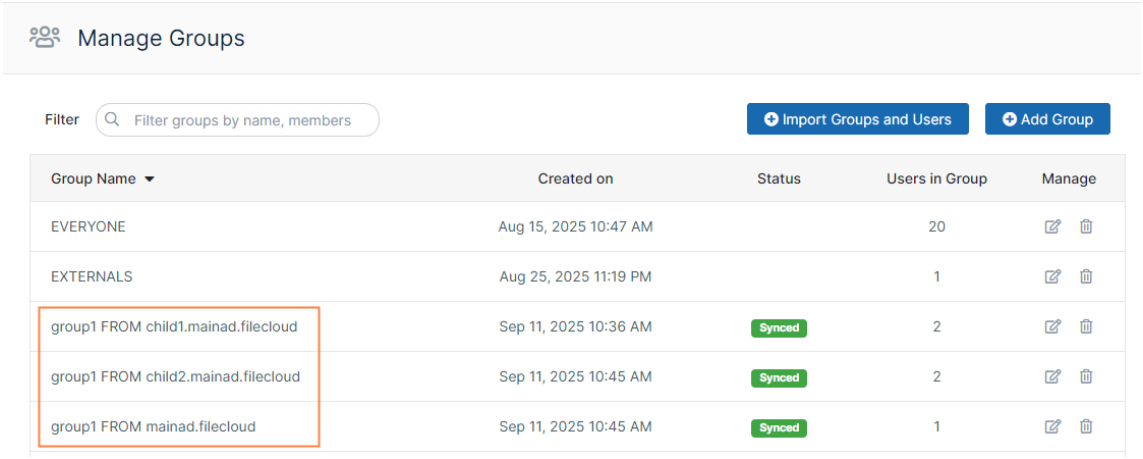
- the following account suffix and prefix fields are hidden, since multiple domains are defined by different account suffixes:
  - **Users have same UPN account suffixes**
  - **AD account suffix**
  - **AD logon name prefix**
- The **Allow email as username** setting available in Admin settings is automatically enabled because users stored in this AD domain forest are required to log in to FileCloud with their full email addresses, which are taken from the User Principal Name (UPN) in Active Directory. You are not permitted to disable **Allow email as username** as long as **Enable multiple AD domains** is enabled.

4. Fill in the other fields as instructed on the page Active Directory Authentication.

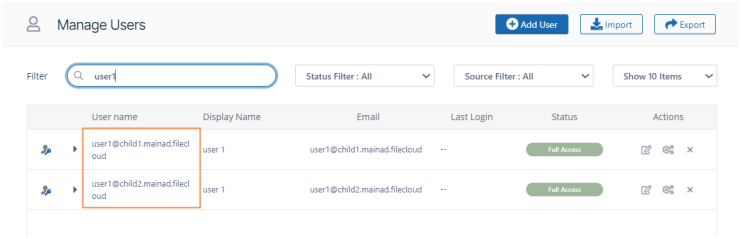
Handling of groups and users with the same names in different domains

In AD forests, it is not uncommon for different AD domains or sub-domains to have users or groups with the same names. For example, two divisions of a company may each have their own domain, but both divisions may have a Marketing group or a user named Michael in their domain. For this reason, when **Enable multiple AD domain** is enabled:

- When a group is imported from an AD domain, its name in FileCloud includes both the group name and the domain/subdomain name:



- When a user is imported through an AD group, its user name in FileCloud is its email address, including the full domain and sub-domains:



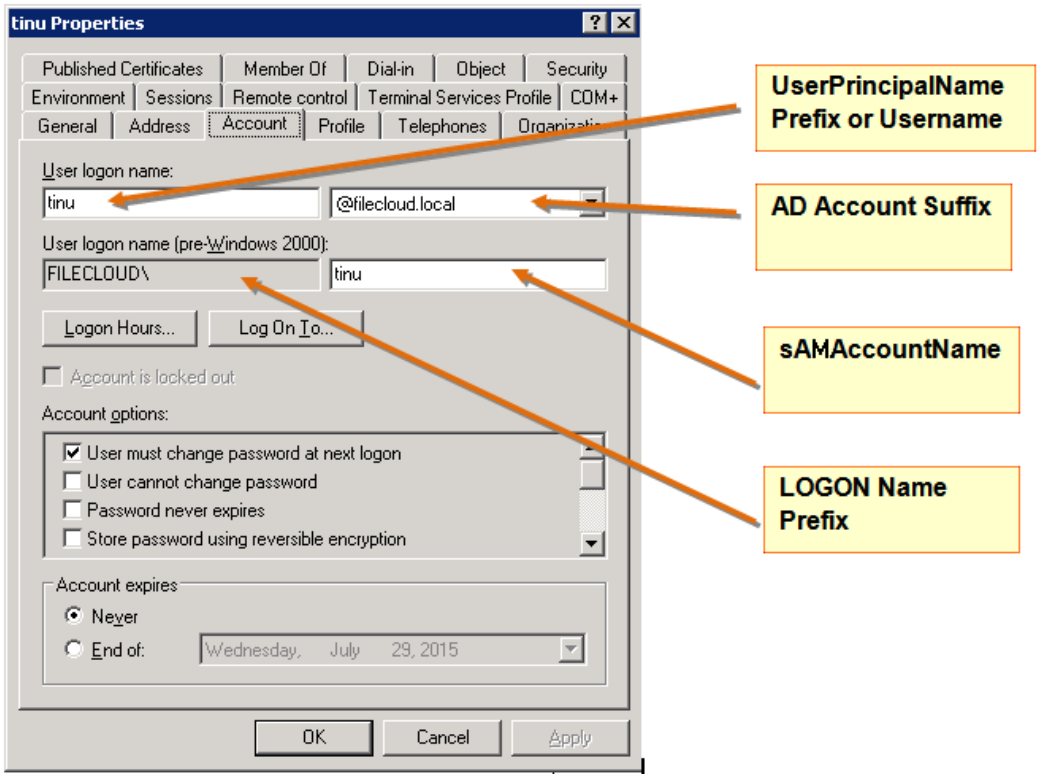
Mixed AD Domain Environments

In some AD environments, there may be multiple UPN domain suffixes set up in a mixed AD hosting setup and the UPN prefix names might not be unique in those cases.

Normally FileCloud uses the UPN prefix names as the usernames, and if they are not unique, FileCloud may not be able to identify the user account correctly.

Therefore, for FileCloud to authenticate in an environment where this occurs, you need to set up the AD connection information slightly differently. In these cases, the account sAMAccountName will be used as the user id.

1. Disable the checkbox "Users have the same UPN Account Suffixes"
2. Set the **AD Logon Name Prefix** parameter, which is the prefix used in the non-editable part of the **User logon name** (pre-Windows 2000).



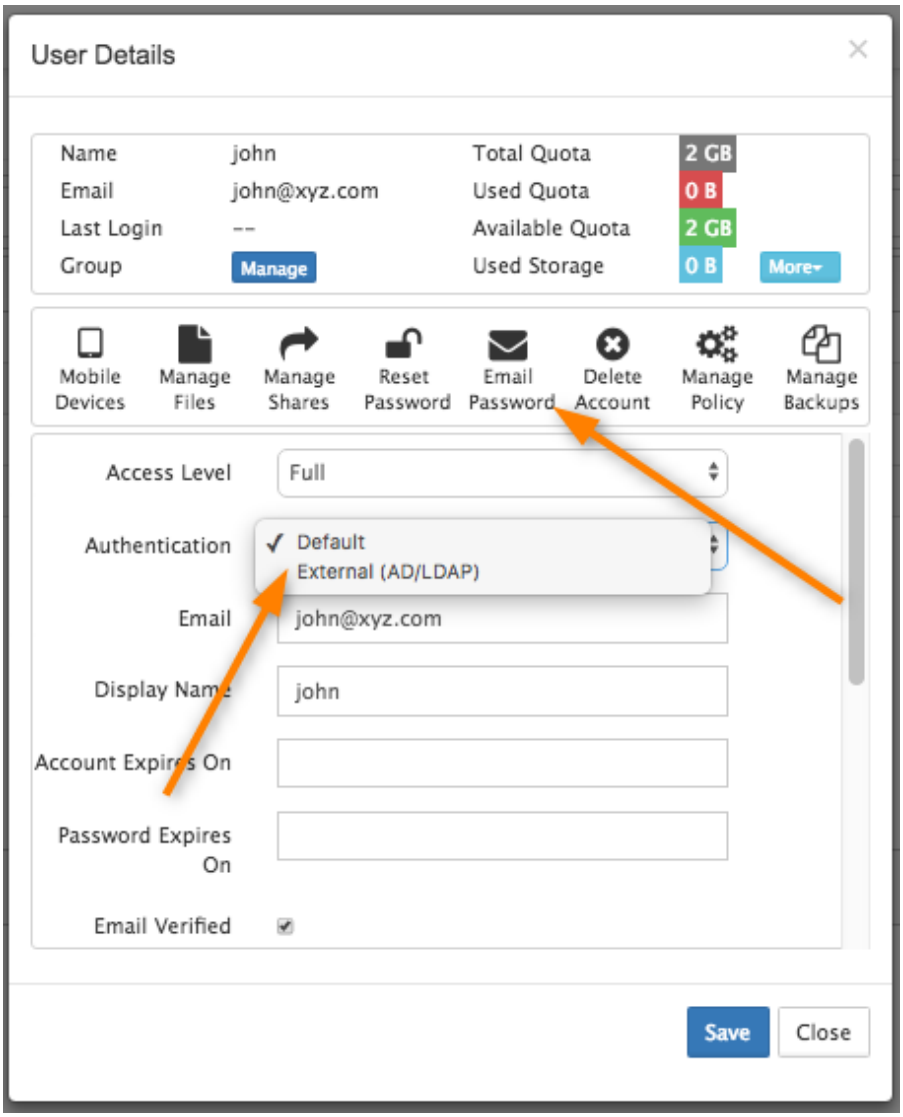
Users can log in using either their email or sAMAccountName.

How to migrate the data from a user that changes account name

When the account name for a user changes in Active Directory, FileCloud won't recognize this change. All the files the user owns still belong to the old account.

To migrate the account data to the new AD account:

1. Log in to the admin portal.
2. Go to the Users section and change the user authentication method form **External** to **Default** and assign a password:



The user can login using Sync App or from Web UI and download all their files.

3. Ask the user to log in via Web User Portal using the new account/password (AD).
4. Reset the Sync App settings and enter the user's new domain credentials without removing the data. See Sync Settings.
5. Log in to the Sync App with the new account credentials; don't remove the data from the computer.
   All the user's files will sync to the server.

In addition to this, all the user shares need to be created and, if the user belongs to any Team Folders, the account has to be added again and permissions created. If the user belongs to any Network Shares, please remember to add the account to them as well.

Once all the user's data is uploaded to the new account and verified; you can delete the old account.

Troubleshooting Active Directory

Common FileCloud Active Directory problems and solutions

Trouble establishing a connection with Active Directory:

1. Make sure you have followed the instructions for entering the settings shown in Active Directory Authentication under **AD configuration parameters**.
2. Check that the port you have specified (either 389 or 636) is open in the AD server for the FileCloud server.
   You can use the telnet command to confirm that it is open.
   telnet [ip address] [port]
   For example, if your IP address were 192.168.1.191 and your port were 389, you would enter:

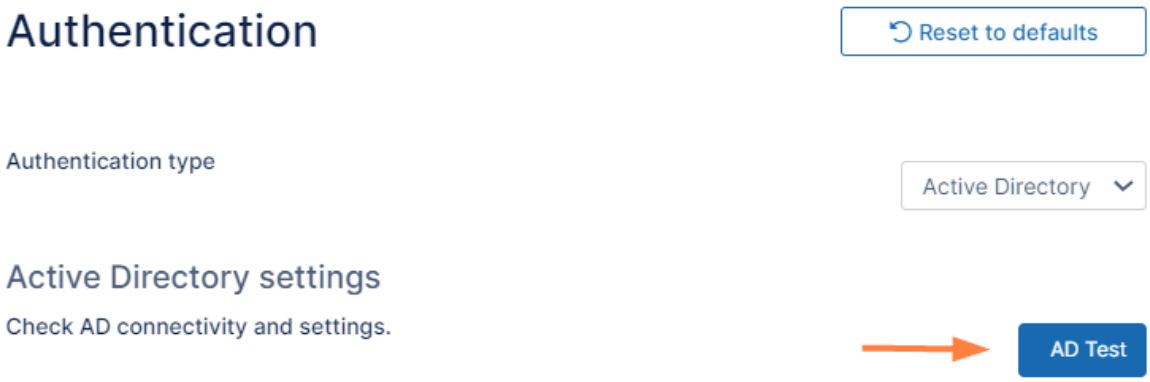
   ```
   telnet 192.168.1.191 389
   ```

3. Confirm that you have entered an account in **AD account name**. This account is used to query the AD server and must be present.
   If you have entered a value in **Limit login to AD group** (see below) the account you enter into **AD account name** must be a member of the AD group.
4. Confirm that you have entered an **AD account password** and that it is correct.

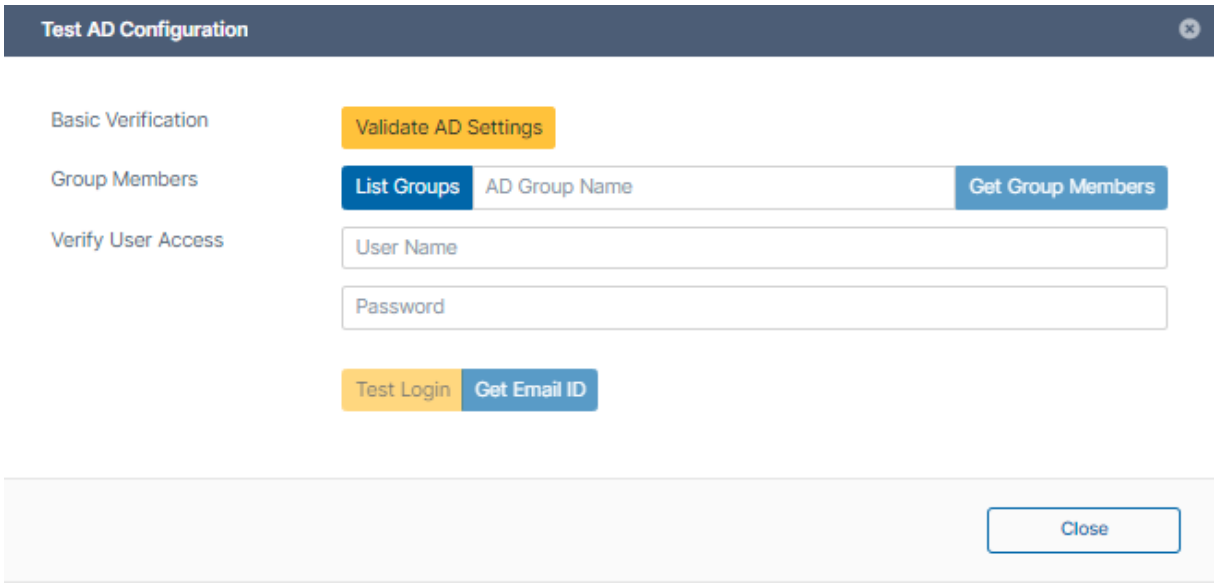
Verify your AD settings using the following steps:

Testing AD Connectivity

Once all data is entered and saved, test the AD settings by clicking the **AD Test** button.

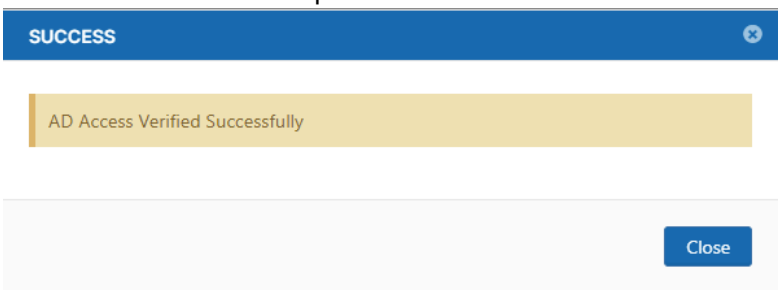


A **Test AD Configuration** dialog box opens:

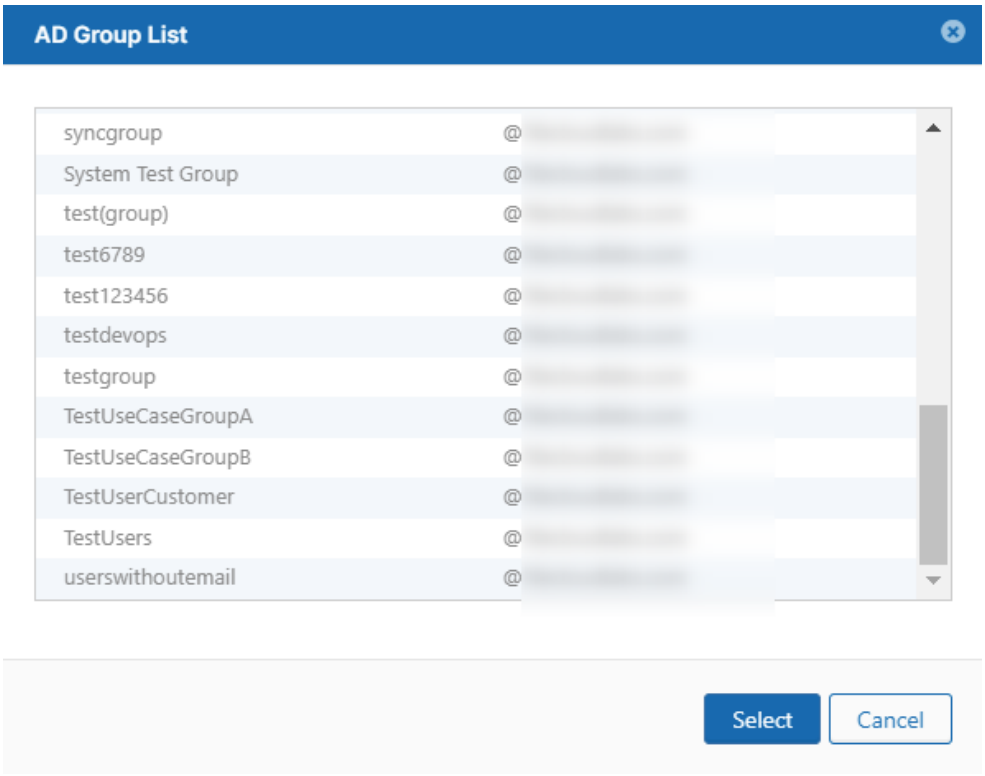


The following tests can be done.

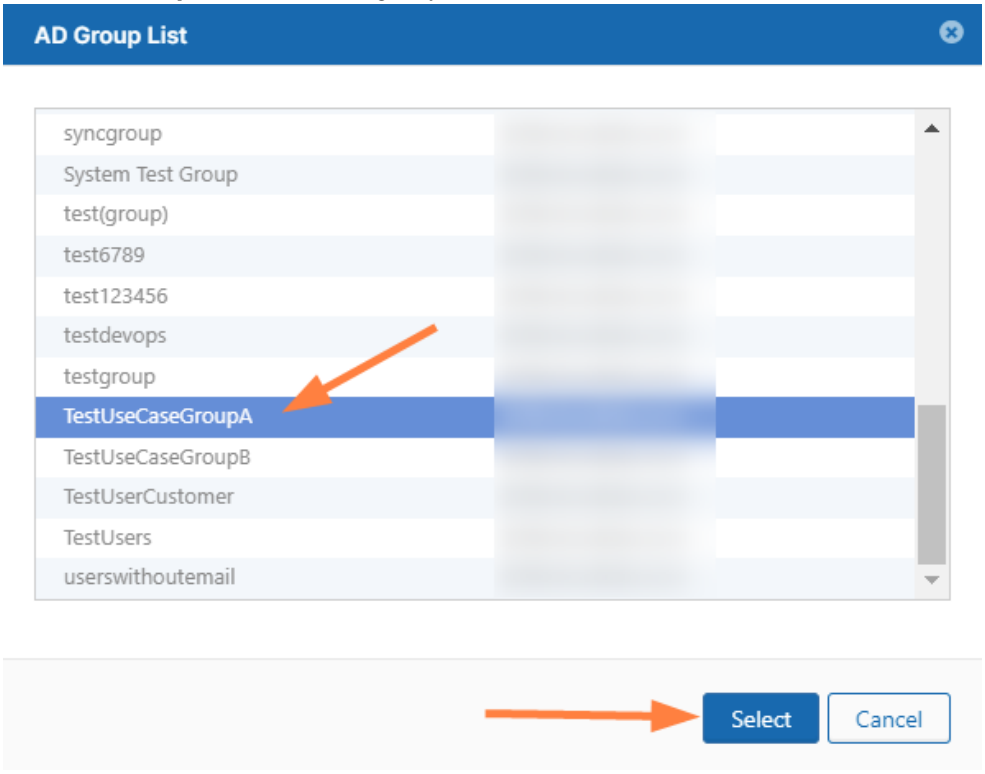
1. Validate AD settings.
   a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server.
   You should receive the response:



   If the tests fail, then check your AD settings to ensure all the data is present and is accurate.
2. List Groups
   a. Once AD settings are validated, click **List Groups** to view the list of groups read from the server.
   You should see a list similar to:

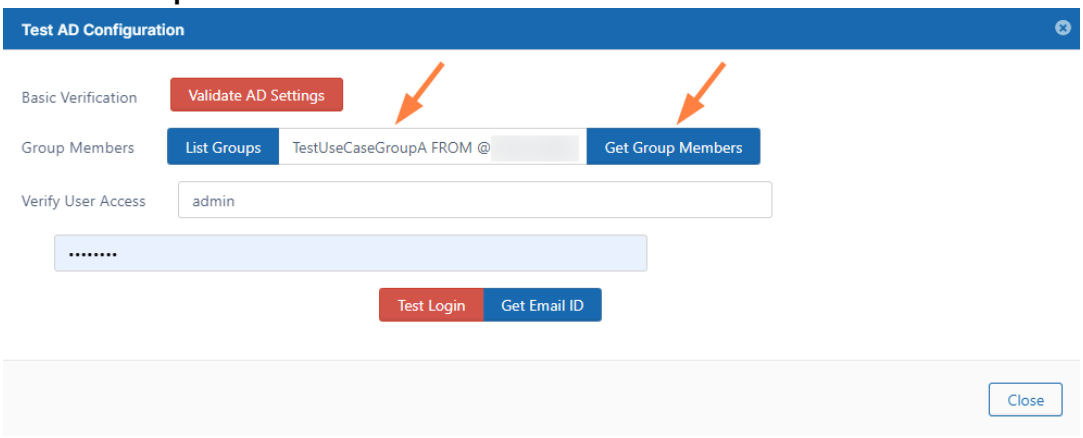


3. Get Group Member
   a. Click **List Groups**, then select a group and click **Select**.

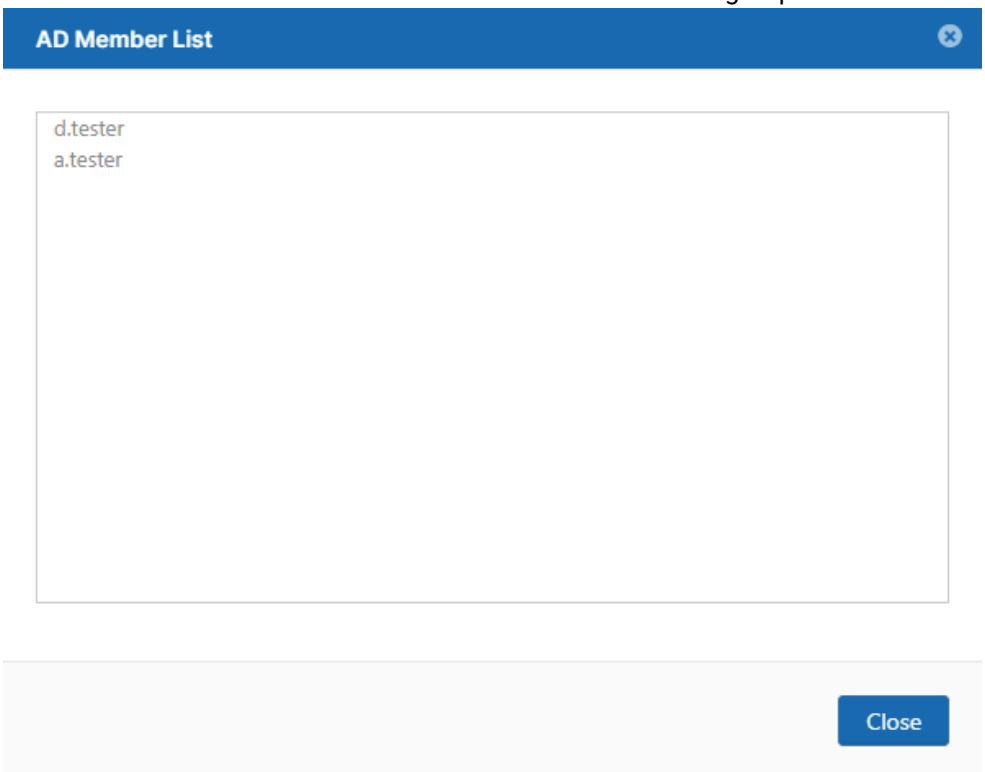


The Group name appears in the **Test AD Configuration** dialog box.
(You can also enter the group name directly into the text box without selecting from the **AD Group List** popup.)

b. Click **Get Group Members**.



The **AD Members List** should list the correct members of the group:



Note: The group members are NOT automatically added to FileCloud.

4. Verify User Access
   a. Enter a specific user name and password and click **Test Login** to make sure the user can log in to AD.

If not, check if the AD suffix or AD prefix matches the one entered in the **AD account suffix** or **AD logon name prefix** in the FileCloud admin portal or the AD server.

b. Enter a specific user name and password and click **Get Email ID.**
This should return the correct email address for a user account from AD. If a valid email address is not returned, then FileCloud cannot import the user account. Check if the email address is included for the user on the AD Server.

Here are some common AD connectivity error messages and their meanings:

Error messages

AD Access failed. Can't contact LDAP server

Either the Hostname or IP address is wrong or the FileCloud server is not able to contact the AD server on the port specified.

AD Access failed. Invalid credentials

Either the AD account name or password is incorrect or the Logon prefix or suffix is incorrect.

AD Access failed. Check if provided AD account name is part of Limit Login into AD group

Either the value in AD BASE DN is wrong or the limit group is set and the AD account name is not part of that group.

Some users have trouble logging in

If you check **Users have the same UPN account suffixes**, you are prompted to enter the **AD account suffix**. If you uncheck it, you are prompted to enter **AD logon name prefix**. Make sure that whichever you use applies to all of your AD users who access FileCloud. If it doesn't, users it does not apply to cannot log in to FileCloud.

All users cannot log in or you cannot import them into FileCloud:

Check if **AD mail attribute** is filled in. If it is not, users cannot log in or be imported. This is normally set to **mail**.

Using the logs to find errors

FileCloud stores all errors associated with AD in the logs.
By default, the log level in FileCloud is set to **PROD**.

1. Change the log level to DEV to create more detailed entries:

a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server** UNKNOWN ATTACHMENT.
The **Server** settings page opens.
b. Set **Log Level** to **DEV**.

2. Repeat the steps that caused the error.
3. Open the log file:
In Windows: C:\xampp\htdocs\scratch\logs
In Linux: /var/www/html/scratch/logs

If you see error messages similar to:

```
2022-05-18 23:03:12.265388 ERROR: [16529329921474] Unable to find provider by name:
0bf0d8c9a7544ce179a7fb1f802dde5f
2022-05-18 23:03:12.265559 ERROR: [16529329921474] Unable to connect to AD server with
david username:
2022-05-18 23:03:12.265608 DEBUG: [16529329921474] User `david` has not been
authenticated with provider
CodeLathe\Core\Subsystem\Security\Auth\AD\Provider\ADProvider class
2022-05-18 23:03:12.357099 DEBUG: [16529329921474] FAILED LOGIN: Invalid Username or
Password
```

Do the following:

-
  - Check if the AD login and password are correct.
  - Check if the user has an email address in the AD server.
  - If the user is already imported into the FileCloud server, check if the user's email in FileCloud and email in the AD server match.

If you were authenticating a user (for this example, authenticating user david on host 192.168.1.14), and see error messages similar to

```
2022-05-18 23:11:27.296483 NOTICE: [16529334871841] Phone number is invalid for
 imported user - david
2022-05-18 23:11:27.297668 DEBUG: [16529334871841] User email `david@test.com` does not
match AD user email `david@gmd.com`.
2022-05-18 23:11:27.297760 DEBUG: [16529334871841] User `david` has NOT been
authenticated.
```

These messages indicate that the user's email address in the AD server doesn't match the user's email address in FileCloud.

To restrict login to FileCloud to specific AD users only

1. Create a group in AD and add only those users who should able to log in to FileCloud.

2. In **Limit login to AD group**, enter the name of the AD group.

LDAP Based Authentication

In this mechanism, a user account is authenticated against an external LDAP server.

Accounts with this type of authentication are also known as external accounts.

By default, LDAP communications between client and server applications are not encrypted.

- This means that it could be possible to use a network monitoring device or software to view the communications traveling between LDAP client and server computers.
- This is especially problematic when an LDAP simple bind is used because credentials (username and password) are passed over the network unencrypted. This could quickly lead to the compromise of credentials.

Therefore, it is recommended that you enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

- SSL and TLS are also known as LDAPS
- Some applications authenticate with Active Directory Domain Services (AD DS) through simple BIND. If simple BIND is necessary, using SSL/TLS to encrypt the authentication session is strongly recommended.
- Use of proxy binding or password change over LDAP requires LDAPS. (e.g. Bind to an AD LDS Instance Through a Proxy Object)
- Some applications that integrate with LDAP servers (such as Active Directory or Active Directory Domain Controllers) require encrypted communications.

Prerequisites

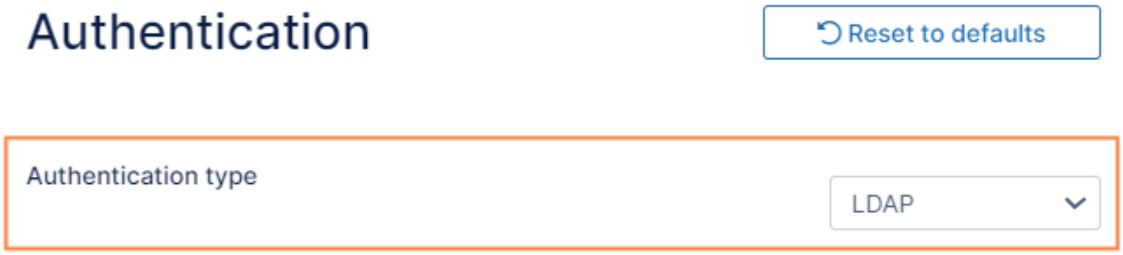
1. The LDAP service must be accessible from FileCloud (IP and Port must be accessible).
2. LDAP must support Simple Authentication Method (Anonymous or Name/Password Authentication Mechanism of Simple Bind).
3. LDAP users must have an email attribute.

- If LDAP Authentication is enabled, then Automatic User creation cannot be enabled (i.e, All user creation should be done in LDAP server)
- The LDAP user will count towards FileCloud License only after the user account logs into FileCloud

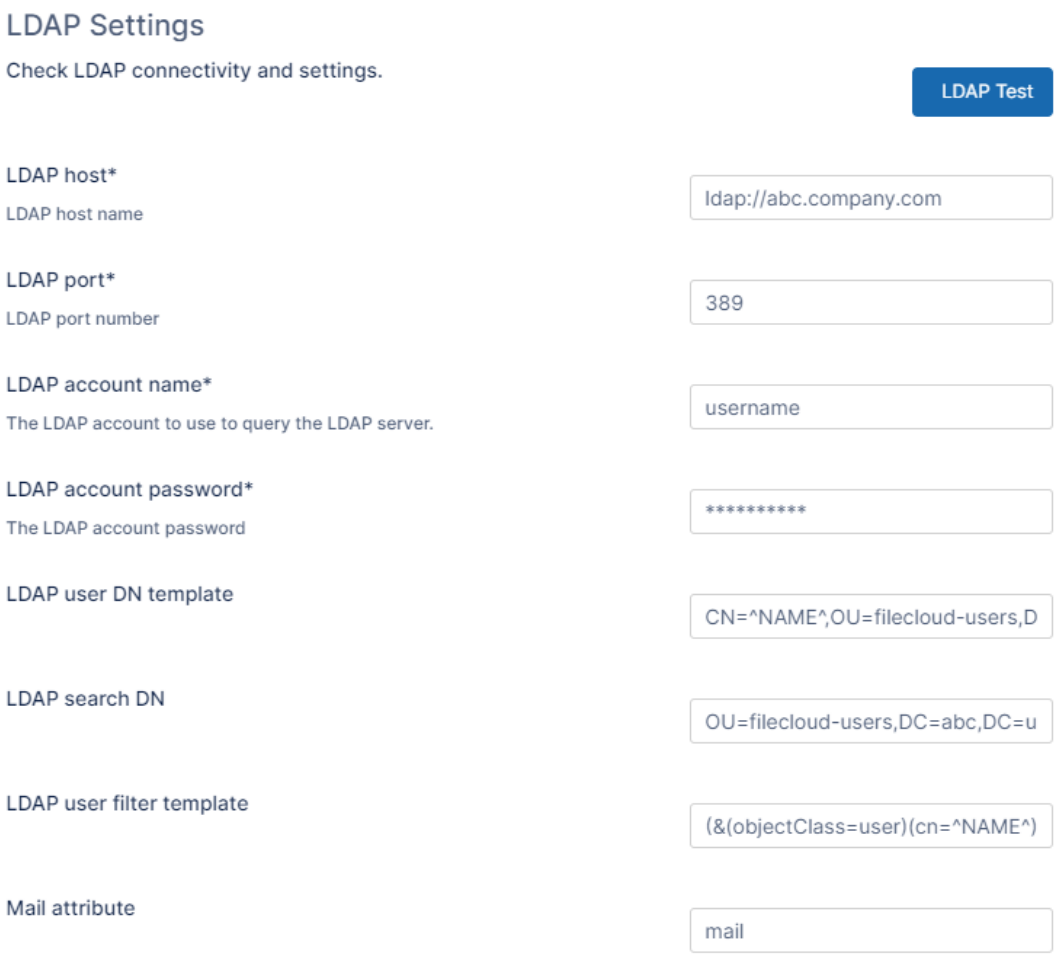
Enable LDAP Authentication

To enable LDAP Authentication in FileCloud:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** page opens.
2. Under **Authentication Settings**, in **Authentication Type** select **LDAP**.



3. In **LDAP Settings**, enter the required information, and then click **Save**.



Read a description of the LDAP Settings

LDAP Settings

SETTING	REQUIRED ?	DESCRIPTION	Example
LDAP host	REQUIRED	The hostname or IP address where the LDAP server is running, including the protocol definition ldap://	`ldap://mycompany.com`
LDAP port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	`389`
LDAP account name	REQUIRED	A valid LDAP login account required to perform queries	`<username>`
LDAP account password	REQUIRED	Password for the LDAP Account Name	`<password>`

LDAP User DN template	REQUIRED	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory.
		This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user.
		To use multiple OUs, set this equal to ^USE_USER_FULL_DN^
			Use the token ^NAME^ in place of user name:
			`cn=^NAME^,ou=someorg,dc=company,dc=com`
			`Multiple OU mode: ^USE_USER_FULL_DN^`

LDAP search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an *ou* encompassing all users, then the search DN would be pointing to that DN.	If all users are under the employees ou, then the search DN would be: `ou=employees,dc=company,dc=com`
LDAP user filter template	REQUIRED	**T**he filter to be used to identify a user entry record from results.	If the object class is inetOrgPerson, then you would use: `(&(objectClass=inetOrgPerson)(cn=^NAME^))`

SETTING	REQUIRED ?	DESCRIPTION	Example
Mail attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	`username_email_ID`

NOTE: For using with Zimbra, please use the following strings

User DN Template:
`uid=^NAME^,ou=someou,dc=company,dc=com`

LDAP Search DN
`ou=someou,dc=company,dc=com`
LDAP User Filter Template:
`(&(objectClass=zimbraAccount)(uid=^NAME^))`

NOTE: For using with JumpCloud, please use the following strings

User DN Template:
uid=^NAME^,ou=Users,o=xxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com

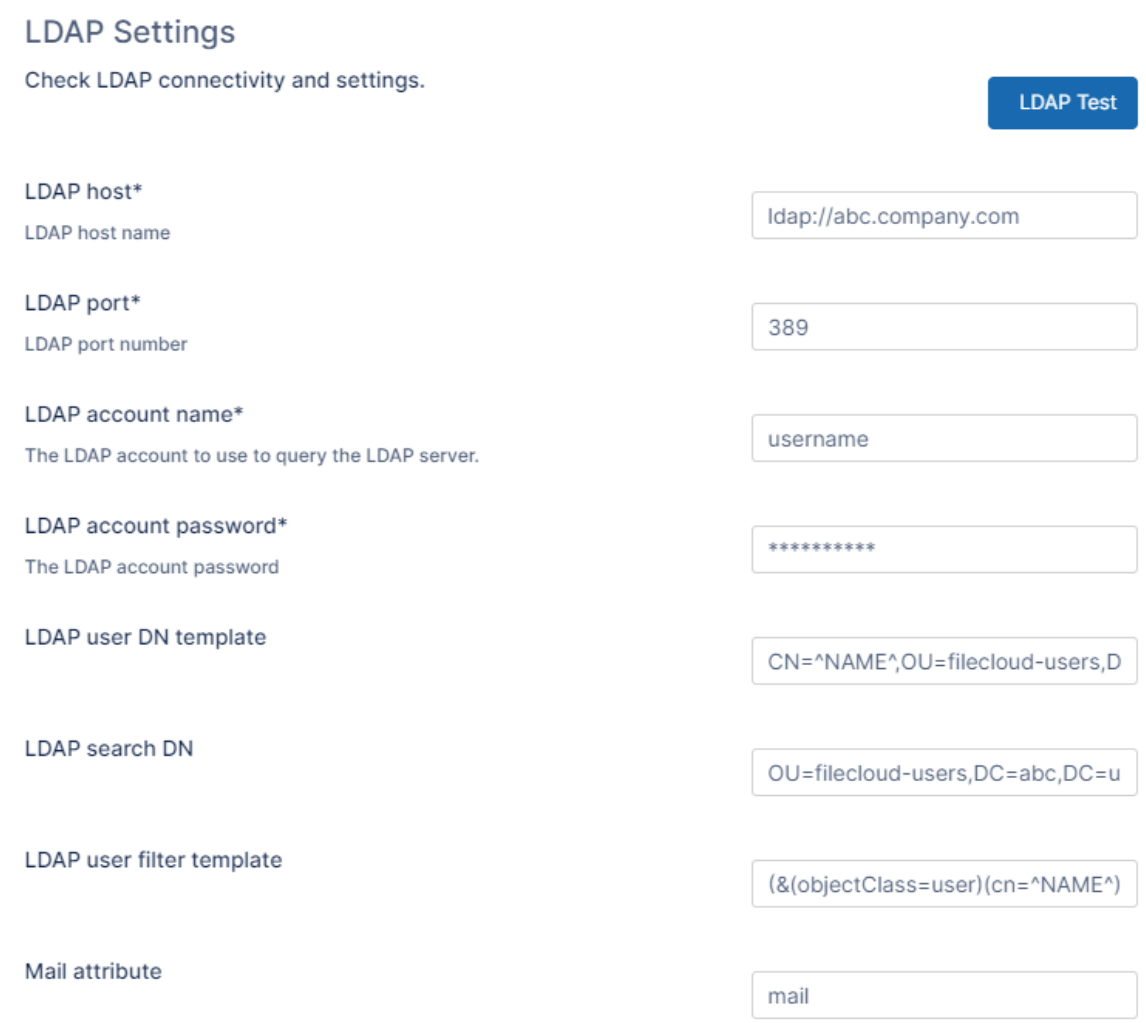
`LDAP Search DN`
`ou=users,o=xxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com`
LDAP User Filter Template:
`(&(objectClass=inetOrgPerson)(uid=^NAME^))`

Use LDAP with TLS

If you are using an LDAP connection with TLS, then you must configure the LDAP fields using the following information:

SETTING	REQUIRED?	DESCRIPTION	TLS Example
LDAP host	REQUIRED	The hostname or IP address where the LDAP server is running	ldaps:// *<your_server_hostname>*
LDAP port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	389
LDAP account name	REQUIRED	A valid LDAP login account required to perform queries	*<username>*
LDAP account password	REQUIRED	Password for the LDAP Account Name	<password>
LDAP user DN template	REQUIRED	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory. This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user. `Use the token ^NAME^ in place of user name` Example : cn=^NAME^,ou=someorg,dc=company,dc=com To use multiple OUs, set this equal to ^USE_USER_FULL_DN^	cn=<username>,ou=*<abc>*,dc=*<company>*,dc=com Multiple OU mode: ^USE_USER_FULL_DN^
LDAP search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an *ou* encompassing all users, then the search DN would be pointing to that DN. For example, if all users are under the *employees* ou, then the search DN would be *ou=employees,dc=company,dc=com*	*ou=company-users,dc=company,dc=com*
LDAP user filter template	REQUIRED	The filter to be used to identify a user entry record from results. For example, if the object class is inetOrgPerson, then you would use: `(&(objectClass=inetOrgPerson)(cn=^NAME^))`	(&(objectClass=*inetOrgPerson*)(cn=*^NAME^*))

SETTING	REQUIRED?	DESCRIPTION	TLS Example
Mail attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	*username_email_ID*



If you are using multiple LDAP servers, see Authenticate to Multiple LDAP Servers.

Authenticate to Multiple LDAP servers

A single installation of FileCloud can authenticate against multiple LDAP servers.

Enable multiple LDAP server authentication

To enable multiple LDAP server authentication, configure settings in the following places:

- ldapconfig.php file
- FileCloud admin portal

To enable multiple AD server authentication:

1. In the FileCloud admin portal, go to **Settings > Authentication**.
2. To enable the LDAP settings, under **Authentication Settings**, change the **Authentication Type** to **LDAP**.
3. Select the **LDAP** sub-tab, type in the required information, and then click **Save**.
4. Create a file called **ldapconfig.php** in one of the following locations, depending on your OS:

```
Windows Location
c:\xampp\htdocs\config\ldapconfig.php

Linux Location
/var/www/htdocs/config/ldapconfig.php
```

5. Add the information for the other LDAP servers using the following example. ⚠ Do not add information for the same LDAP server that was already configured in Admin Dashboard.

```
<?php
/*
* Copyright(c) 2014 CodeLathe LLC. All rights Reserved.
* This file is part of FileCloud  http://www.filecloud.com
*/

// ... Multi-AD Server Support, set to 1 to enable additional AD servers
define("TONIDOCLOUD_MULTI_LDAP_ENABLE", 1);
//=============== SITE 1 ============================
define("TONIDOCLOUD_LDAP_HOST_1", "ldap.mycompany.com" ); // < LDAP Server Host
define("TONIDOCLOUD_LDAP_PORT_1", 389 ); // < LDAP Server port
define("TONIDOCLOUD_LDAP_ACCOUNTNAME_1", "cn=admin,dc=mycompany,dc=com"); // <
Account name for Admin Operations
define("TONIDOCLOUD_LDAP_ACCOUNTPASSWORD_1", "3lkjASdf9802"); // < Account Password for
Admin Operations
define("TONIDOCLOUD_LDAP_USERDNTEMPLATE_1", "cn=^NAME^,ou=MyCompnay-
Support,dc=mycompany,dc=com"); // < USer DN template
```

```
define("TONIDOCLOUD_LDAP_SEARCHDN_1", "ou=MyCompany-
Support,dc=mycompany,dc=com"); // < USer DN template
define("TONIDOCLOUD_LDAP_USERFILTERTEMPLATE_1", "(&(objectClass=inetOrgPerson)
(cn=^NAME^))"); // < USer DN template
define("TONIDOCLOUD_LDAP_MAILATTRIBUTE_1", "mail"); // < Mail Attribute

?>
```

Now additional users from these domains can also log in into FileCloud.

Multi-Factor Authentication

Multi-factor authentication (MFA) refers to the multi-step verification process that is available in FileCloud and designed to provide an extra layer of security. With this function, in order to access FileCloud, the user is required to know not only the password and username but also an extra security code that is made available to them. The FileCloud administrator can enable multi-factor authentication for the user portal, and also, separately, for the admin portal. This can be done regardless of the authentication type (default, AD, or LDAP).

FileCloud supports the following modes of delivering MFA codes:

- Email
- Google Authenticator TOTP Code
- DUO Security (user portal only)
- SMS OTP Security Code

Multi-factor authentication using TOTP (Google Authenticator or similar TOTP code generators)

These instructions are written using Google Authenticator as an example TOTP code generator, however, any TOTP apps such as Microsoft Authenticator, etc. can be used.

To set up MFA with Google Authenticator:

- In the FileCloud user portal, choose **TOTP (Authenticator App)** when configuring MFA for the user portal. See Multi-Factor Authentication for User Portal for help.
- In the FileCloud admin portal, choose **TOTP Authentication** when configuring MFA for the admin portal. See Two-Factor Authentication for Admin Portal for help

When a user logs in for the first time, they are provided with an option to set up Google Authenticator. This involves entering a code or scanning a QR Code into the the Google Authenticator client. See Log in Using Multi-Factor Authentication for more information.

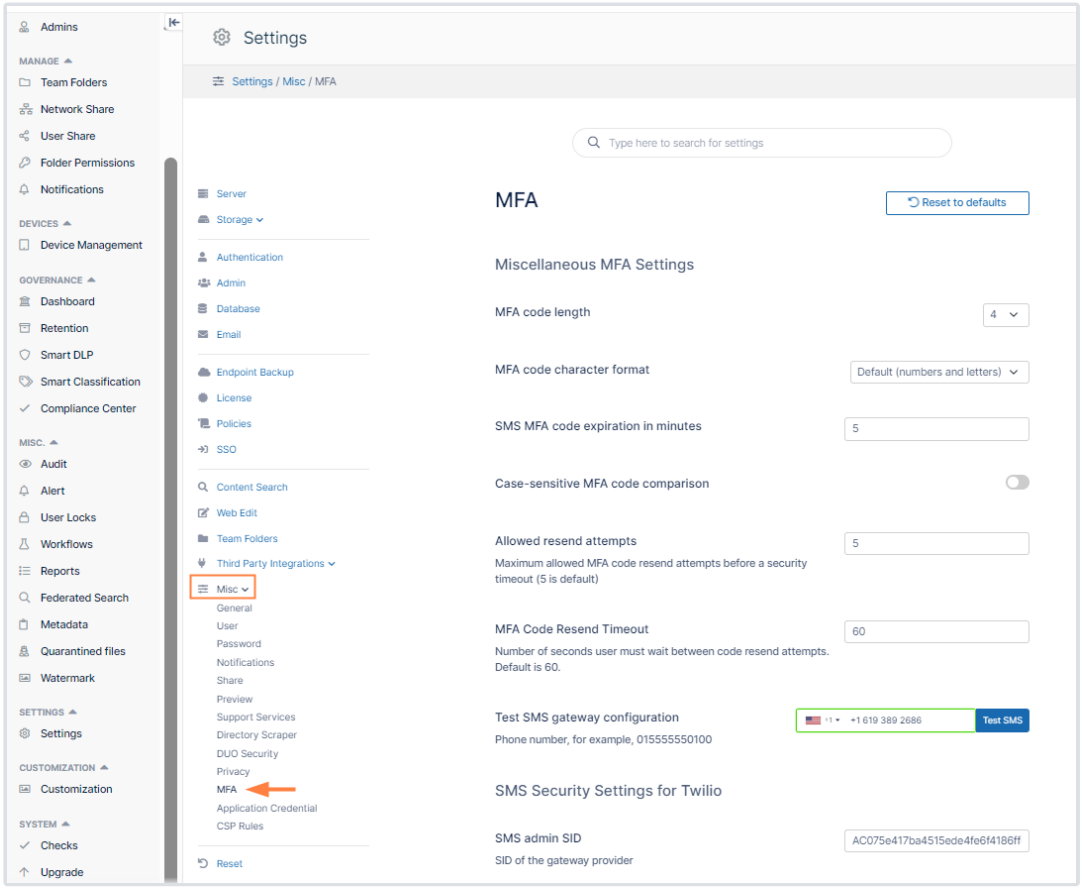
Note that once Google Authenticator is set up using the user portal, other client devices can be used to connect to the FileCloud account.

Once MFA with Google Authenticator is set up for the first time, the user is no longer able to set it up again. Only the Administrator can clear the Google Authenticator setup.

MFA using SMS: Setting up Twilio as the SMS gateway provider

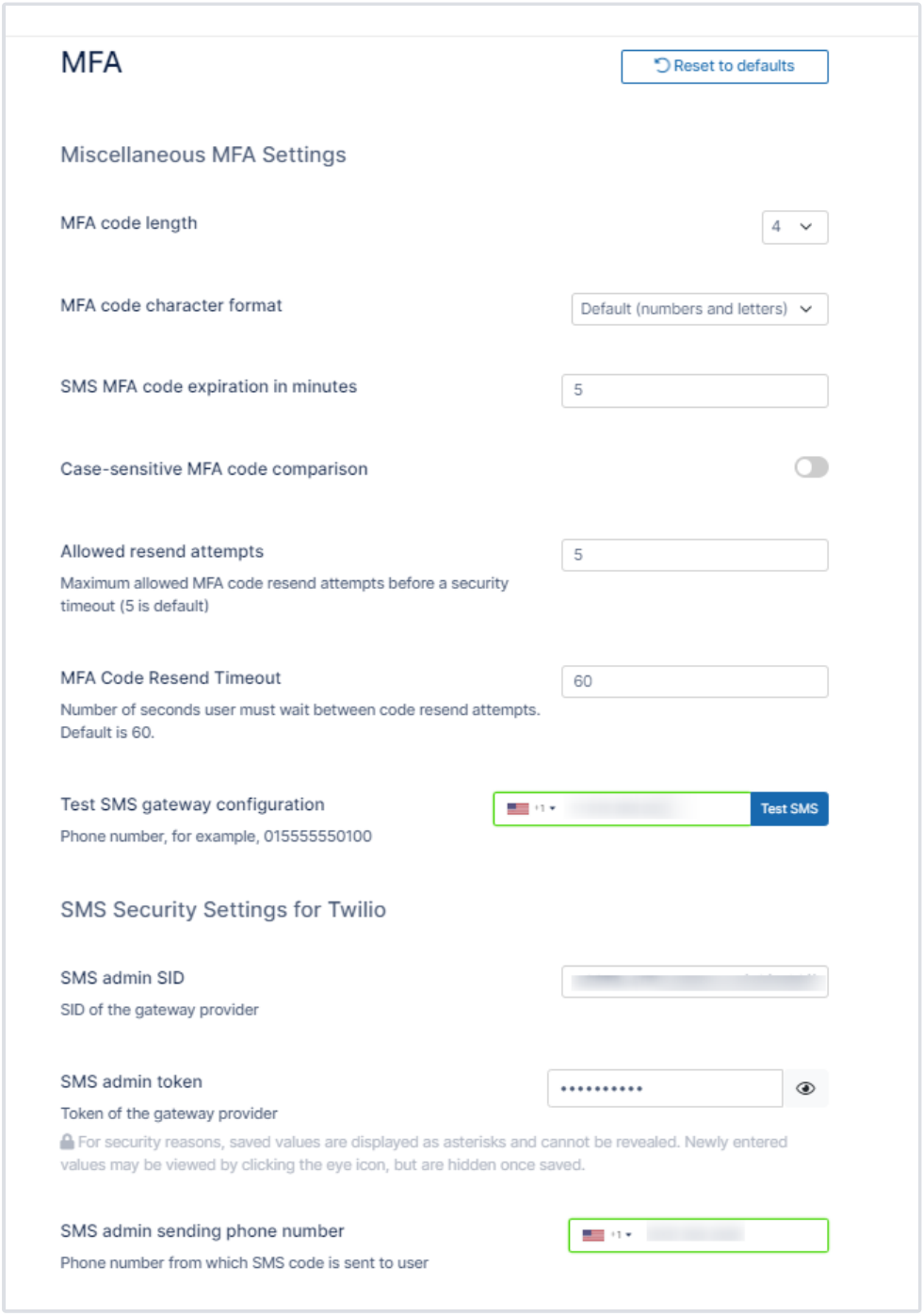
Currently, FileCloud has implemented Twilio as the default SMS Gateway Provider, although enterprise customers may add custom SMS providers and handlers to the system. In order to successfully use SMS security, admins must set up a Twilio account to receive the required security ID, authentication token and the phone number from which the codes will be sent.

1. Create a Twilio account.
   Follow instructions at https://www.twilio.com/docs/sms to obtain the required SID, Auth Token and create a phone number.
2. In the FileCloud admin portal, open the **MFA** settings page.
   To open the MFA settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **MFA**, as sho800wn below.



The **MFA** settings page opens.

3. Fill in the MFA settings.



MFA code length - The number of letters and digits in the MFA code. Default is 4.

MFA code character format- Type of characters permitted in MFA code. Options are:

- Numbers and letters (default)
- Numbers

- Letters
- Uppercase letters

SMS MFA code expiration in minutes - How long, in minutes, the security code remains valid. Default is 10.

Case-sensitive MFA code comparison - When checked, the code entered is case-sensitive.

Allowed resend attempts - Number of times the user may resend the code before logging in is timed out for the time set in **MFA Code Resend Timeout.**. Default is 5.

MFA Code Resend Timeout - Number of seconds between **Allowed resend attempts** that the user must wait before attempting to resend again. Default is 30.
For example, if **Allowed resend attempts** is 5, and **MFA Code Resend Timeout** is 30, a user can attempt to resend a code 5 times and then is forced to wait 30 seconds before being able to attempt to resend the code another 5 times. If those attempts fail, the user is forced to wait another 30 seconds, and so on.

Test SMS gateway configuration - Enter a secure known phone number, and save the settings. Click **Test SMS** to check if your SMS configuration is valid.

SMS admin SID - SID of gateway provider.

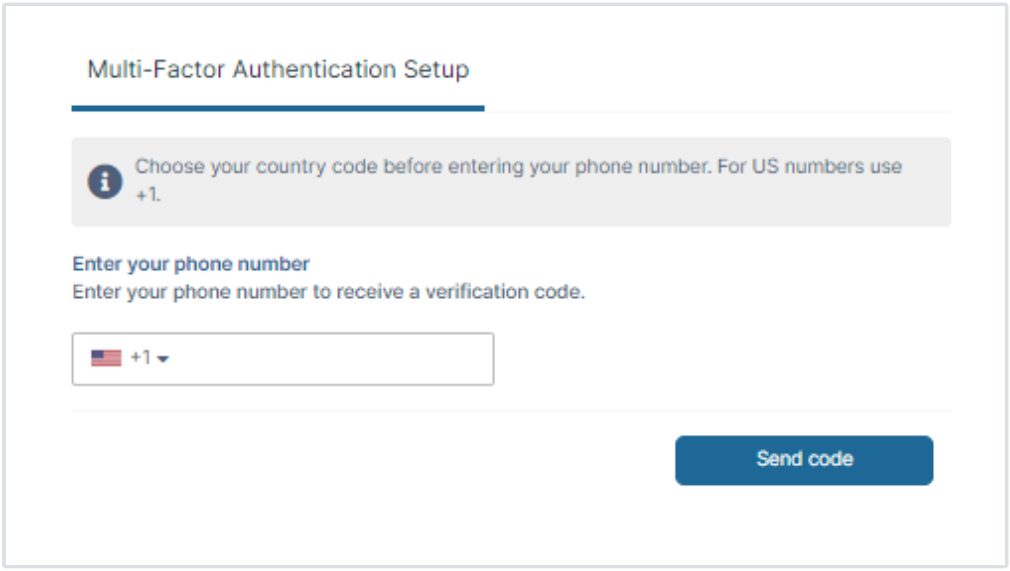
SMS admin token - Token of gateway provider.

SMS admin sending phone number - Phone number from which SMS code is sent to user.

Once the setup is complete, set up the policy for users and choose the appropriate SMS gateway provider, similarly to other MFA methods.

Users are required to set up a phone number once the SMS MFA Policy is enabled. Once the phone number is set up, client devices can be used to connect to the FileCloud account. Set up the phone number via the web UI or through your admin.

If users are required to use SMS with MFA, they will see the following dialog box during login after the policy is enabled:



Enable multi-factor authentication using SMS OTP security codes for specific user agents

FileCloud supports configuring multi-factor authentication using SMS OTP for specific user agents. For example, you could apply this configuration to mobile clients only, or to FileCloud Drive, FileCloud Sync, and Microsoft Outlook only.

1. Complete the instructions above in **Multi-Factor Authentication using SMS OTP Security Codes**.
2. Open cloudconfig.php at
   - Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
3. Add the following:

```
define("TONIDOCLOUD_TWOFA_REQUIRED_USERAGENT_LIST",
"useragent1,useragent2, ... ");
```

4. Replace the *useragent* values with any number of user agents from the following list:
   - Web browser
   - Android
   - iOS
   - MS Outlook
   - MS Office
   - MS Office Online
   - Cloud Sync
   - FileCloud Drive

- Any white labelled FileCloud Sync/Drive product name

  For example:
  `define("TONIDOCLOUD_TWOFA_REQUIRED_USERAGENT_LIST", "Android,iOS");`

Multi-factor authentication validity for Email based MFA

MFA Code validity: 10 minutes.

This can be changed by adding a key with a different timeout as shown (This key can be added <WEBROOT>/config/cloudconfig.php).
define ("TONIDOCLOUD_2FA_EMAIL_EXPIRATION_MINUTES", "10");
This can be changed by adding a key with a different timeout as shown (This key can be added <WEBROOT>/config/cloudconfig.php).
define ("TONIDOCLOUDN_MINUTES", "5");

For Web Apps, The MFA validity period is tied to the Session Timeout

For Client apps (iOS , Android App, Drive and Sync) the MFA code will be required only on very first access and subsequent access will not require the code. If the record of that device is removed using "Remove Client Device Record" action, then subsequent access for that mobile device will require the MFA code.
For instructions specific to the admin portal or the user portal, see:

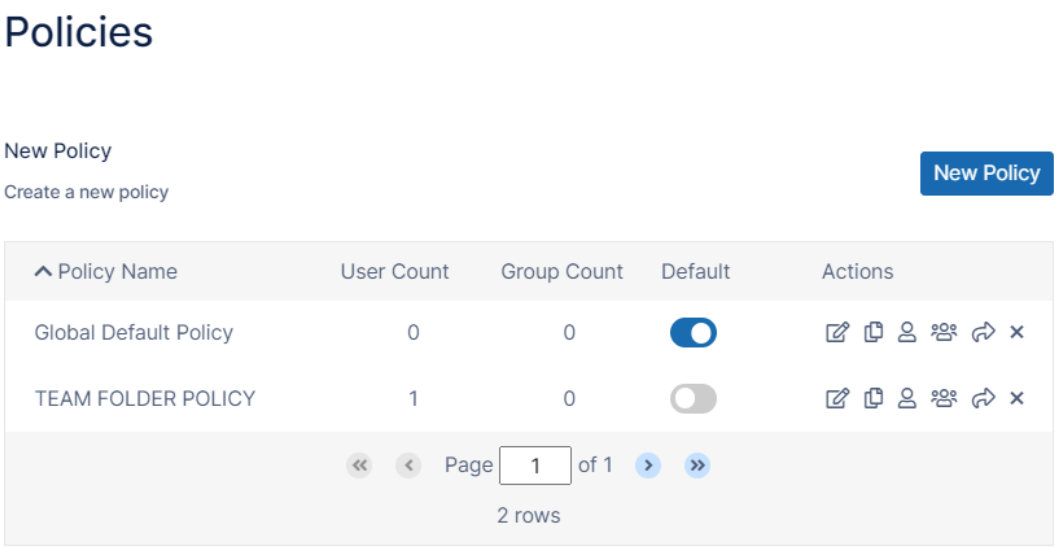
Multi-Factor Authentication for User Portal

Enable multi-factor authentication for user portal

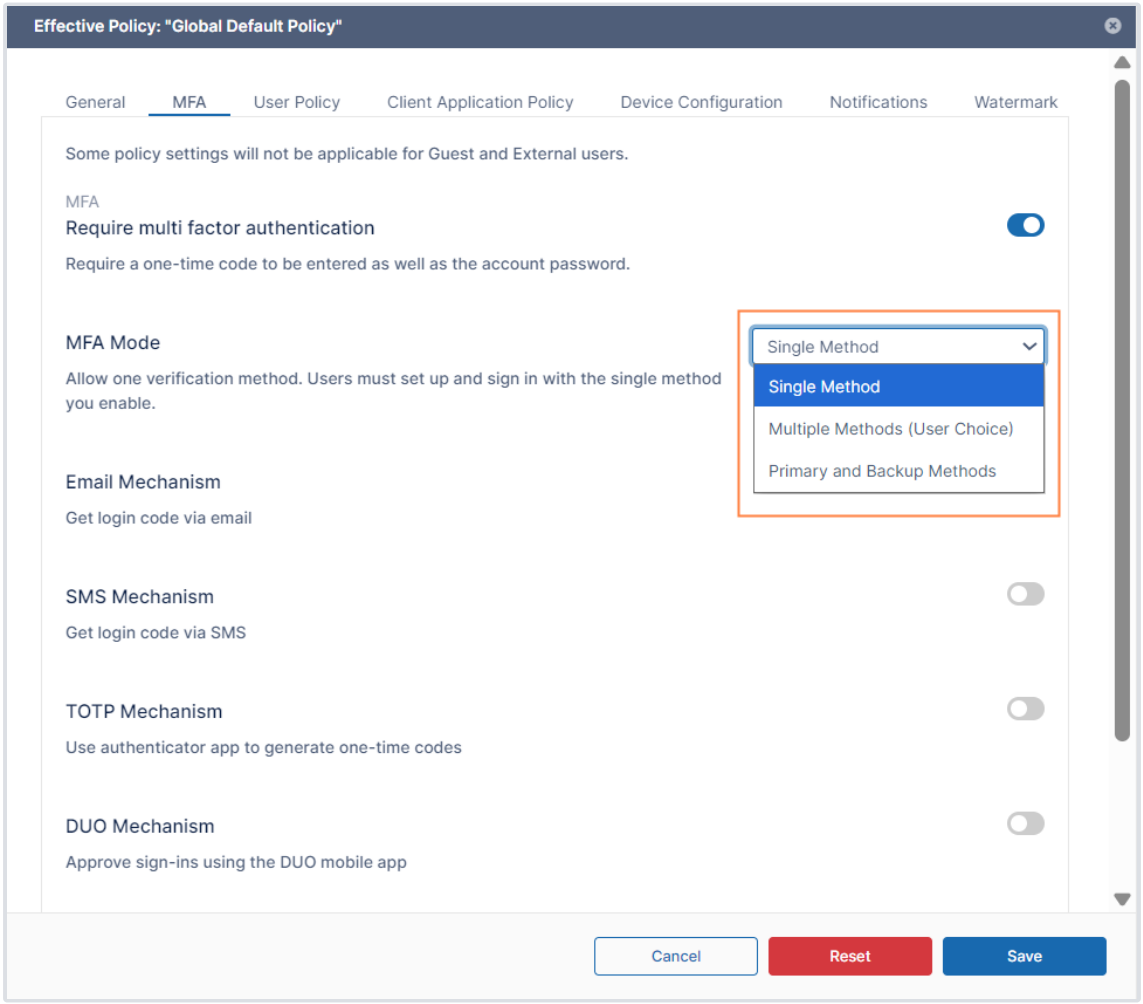
To enable multi-factor authentication for logging into the user portal:

> ⚠ If you are planning to enable DUO Security as the multi-factor authentication mechanism, first set up FileCloud to use DUO Security Service (instructions below).

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. Edit the policy for MFA users.
3. Click the **MFA** tab.
4. Enable **Require multi factor authentication**.
   Additional fields appear for setting up MFA.



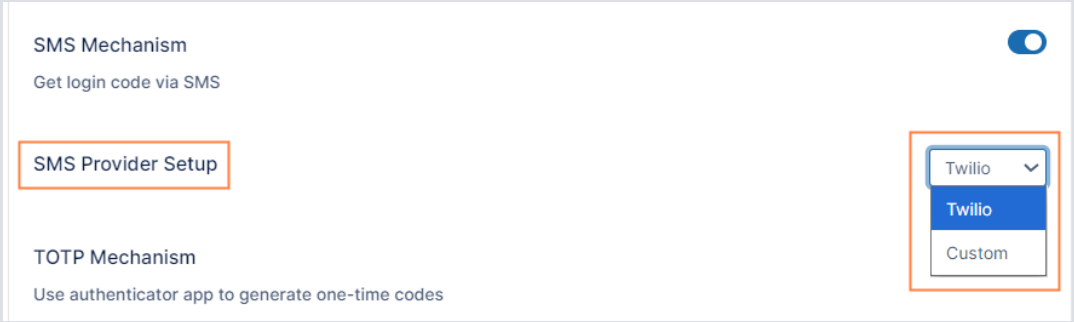
5. In the **MFA Mode** drop-down list, choose one of the options:
   - **Single Method** - Users must use the single authentication mechanism that you enable on this tab.
   - **Multiple Methods (User Choice)** - Users may choose one of the authentication mechanisms that you enable on this tab.
     - When this choice is selected, the option **Show all selected options at every login** appears below it.



When disabled (default), only the method the user chooses initially is shown on each login. When enabled, all admin-enabled MFA methods are displayed on each login, and if the user chooses one that is not yet configured, they are prompted to configure it.

- **Primary and Backup Methods** - Users may choose (and must set up) two of the authentication mechanisms that you enable on this tab, one as a primary method and one as a backup. On initial login, users choose the primary and secondary methods and do any set up necessary for them . On future logins, they are prompted to use the primary method on login, but can switch to the backup.

6. Depending on which of the methods you have chosen in **MFA Mode**, choose one or more of the following mechanisms:
   - **Email Mechanism** - Sends a one-time authentication code to the user's email address.
   - **SMS Mechanism** - Sends a one-time authentication code via the user's SMS number.
     If you choose **SMS Mechanism**, an **SMS Provider Setup** field appears below it. Choose either **Twilio**, our default SMS gateway provider or **Custom** if you are adding a custom provider.
     For more information about setting up your SMS provider, see Multi-factor authentication.



   - **TOTP Mechanism -** Generates a one-time authentication code via the user's authentication app.
   - **DUO Mechanism** - Enables the user to use their DUO app to either get a one-time code.

6. If you choose **SMS Security** and users are permitted to create accounts, add the following setting that enables users to add a phone number when creating a share with an external user:

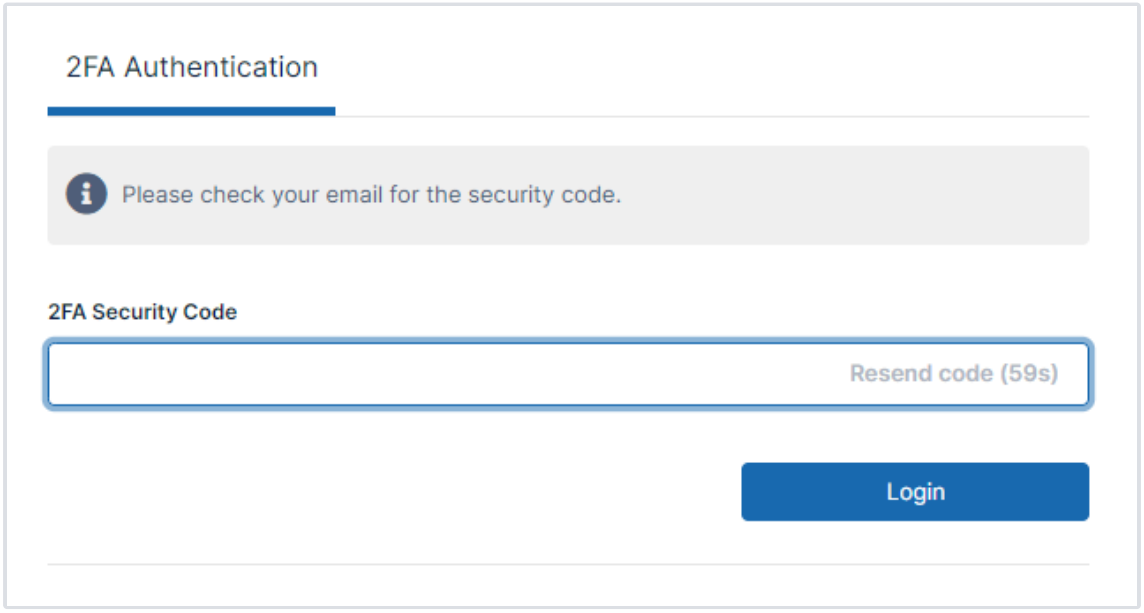
- Open the configuration file:
  Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
  Linux: /var/www/config/cloudconfig.php
- Add the line:

```
define ("TONIDOCLOUD_ENABLE_2FA_SMS_SHARE_INVITES", TRUE);
```

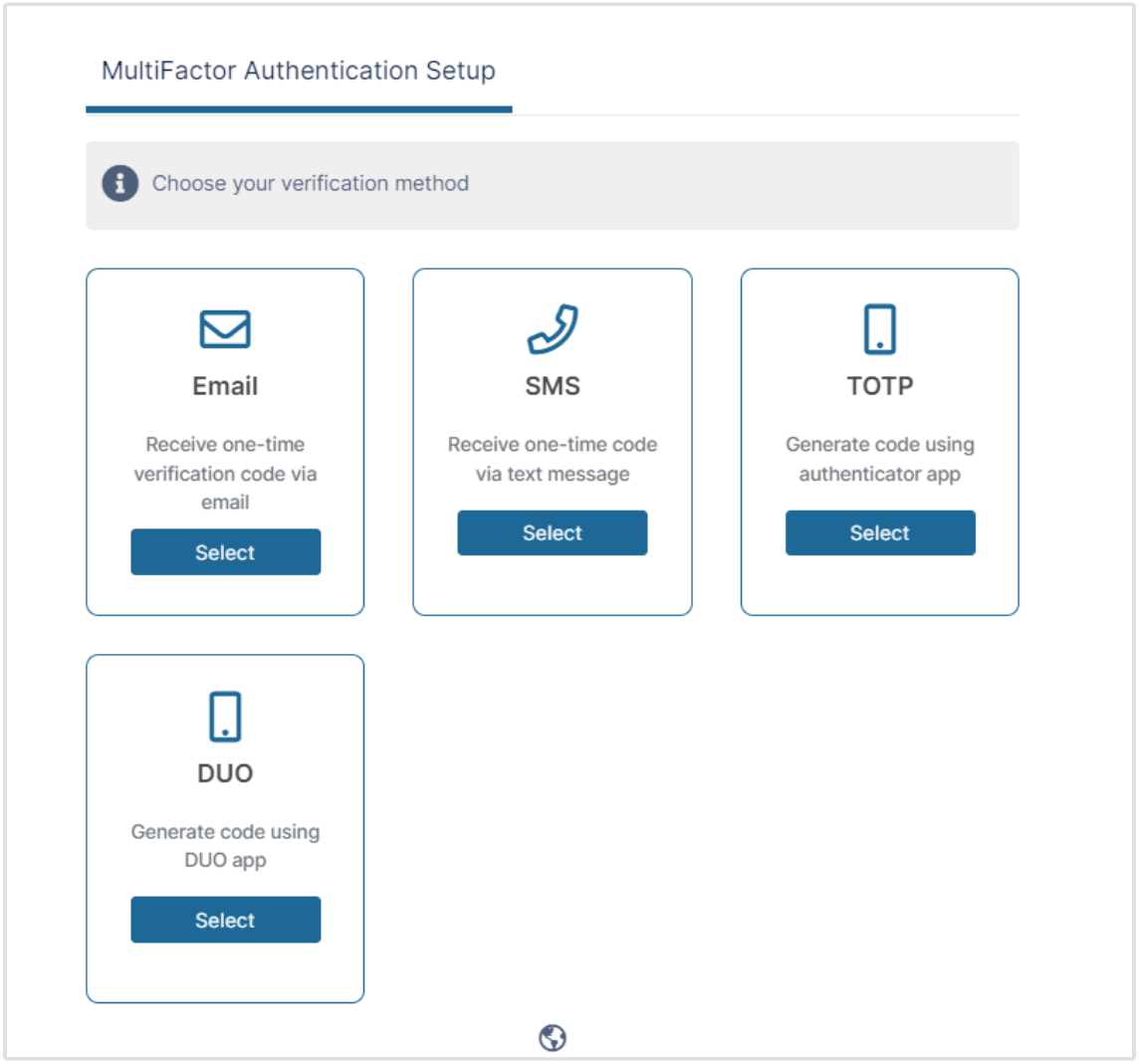
What Users See

When you require multi-factor authentication for a certain policy, the choices given to users in that policy depend on both the **MFA Method** you choose and the **MFA Mechanisms** that you enable.

- **MFA Mode: Single Method**
  Mechanism enabled in this example: **Email**
  When users in this policy log in, they see:



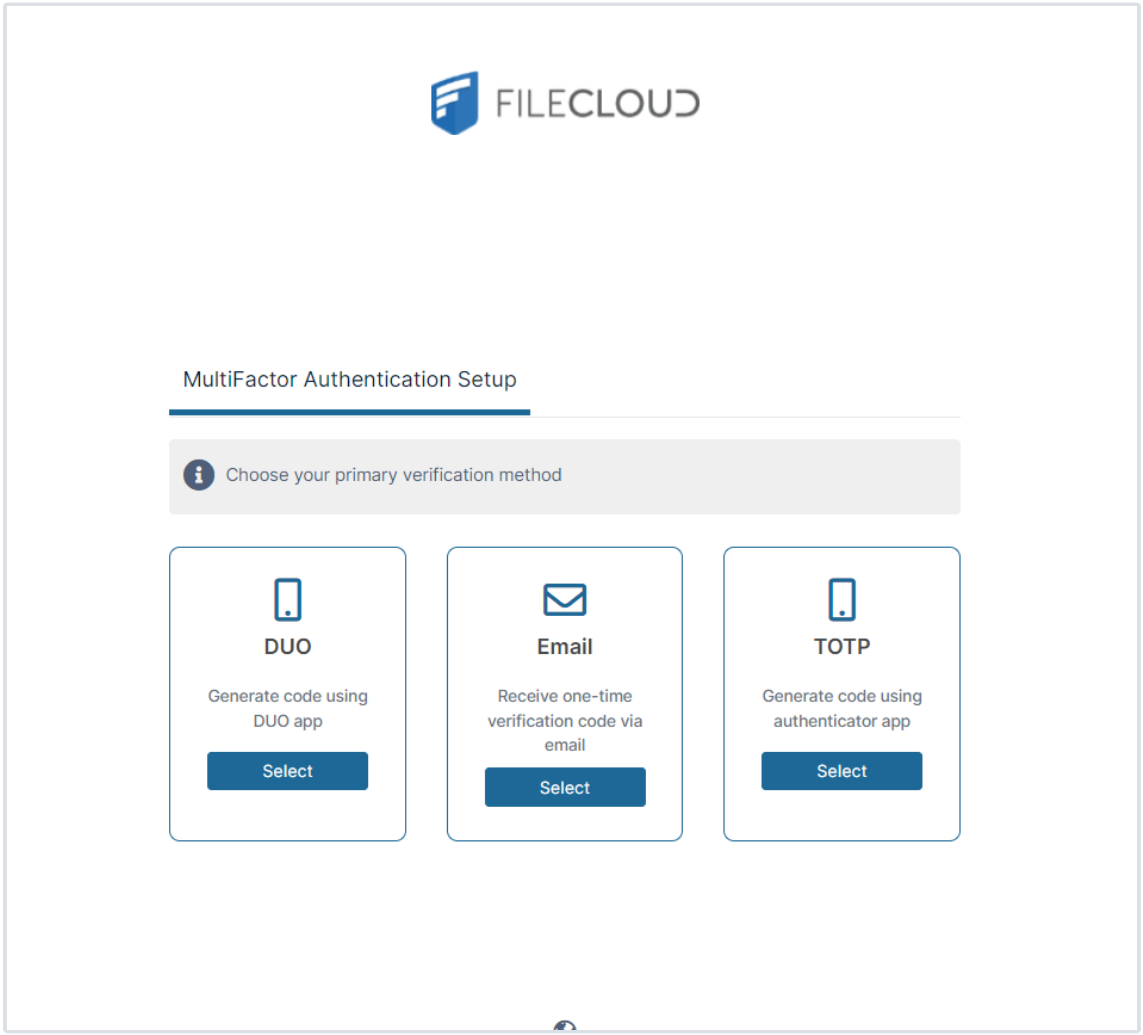
- **MFA Mode: Multiple Methods (User Choice)**
  Mechanisms enabled in this example: **Email**, **SMS**, **TOTP**, **DUO**
  When users in this policy log in initially, they see:



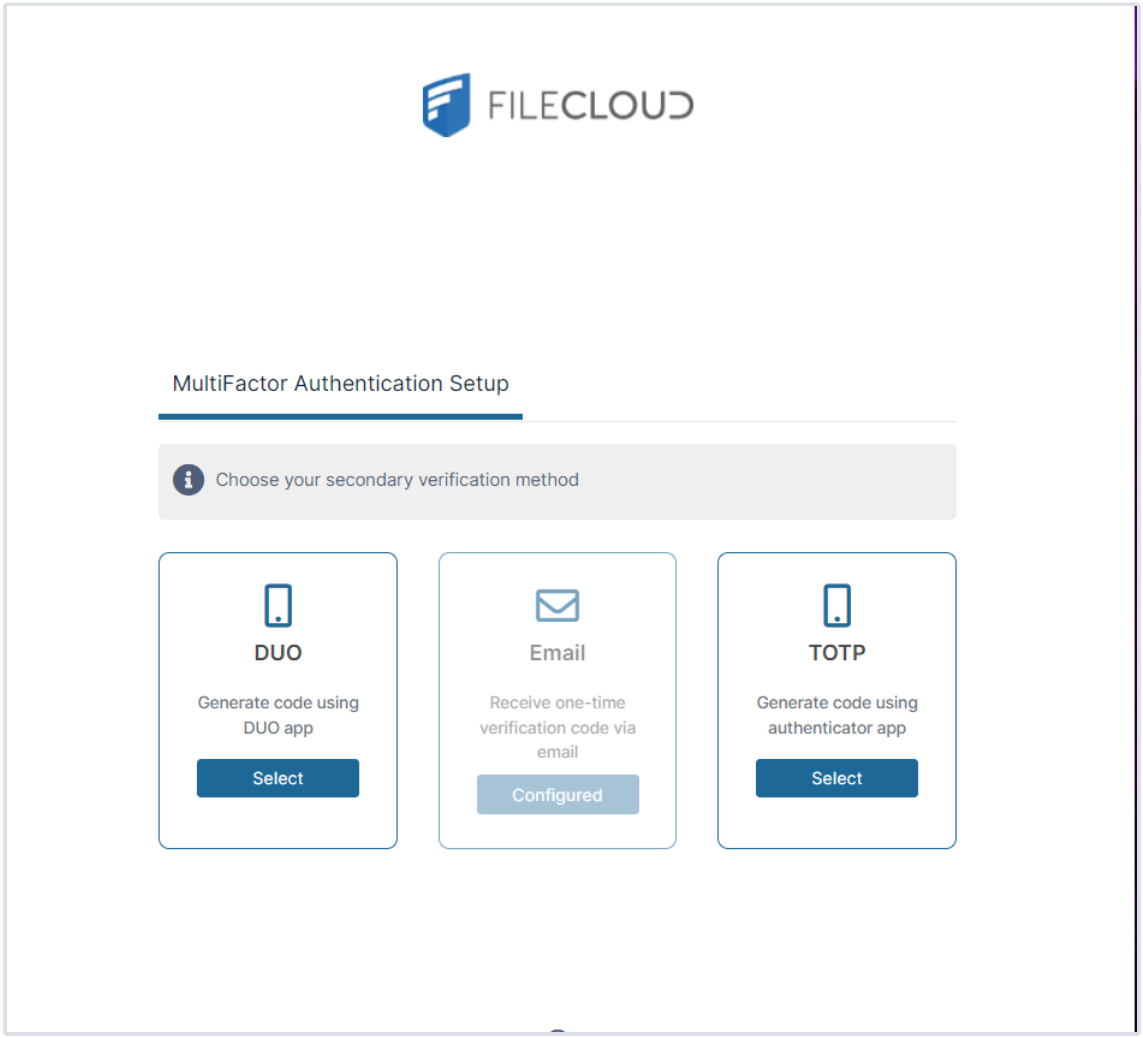
On subsequent logins:

- They see the verification method they initially selected, if **Show all selected options at every login** was disabled.
- They see all admin-enabled verification methods, if **Show all selected options at every login** was enabled.

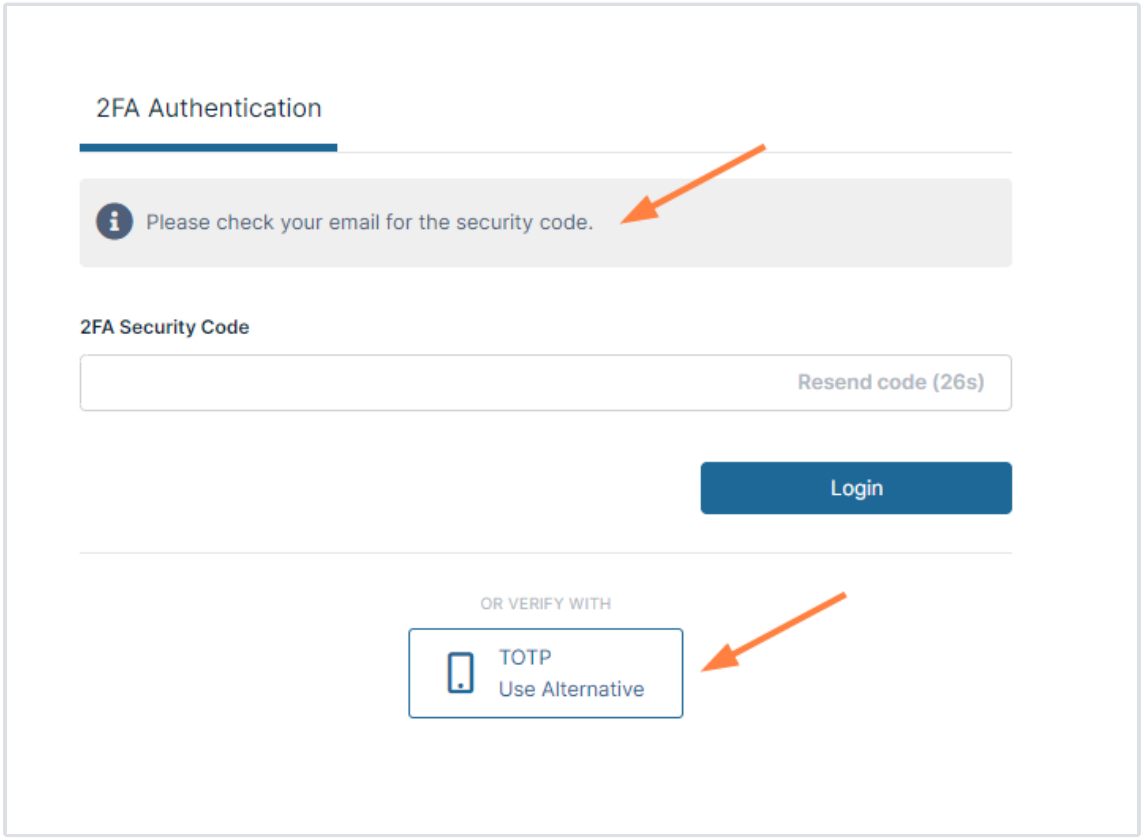
- **MFA Mode: Primary and Backup Methods**
  Mechanisms enabled in this example: **Email**, **TOTP**, **DUO**
  When users in this policy log in, they are prompted to choose a primary verification method:



If, for example, a user selects Email, they are prompted to log in with a code sent through email, and then they are prompted to choose a secondary verification method:



If the user chooses TOTP, they are prompted to set up TOTP login.
When they log in again, they are automatically prompted to enter a code sent to email, but they are also given the option of switching to TOTP:



If you switch from **Single Method** to **Multiple Methods** or **Primary and Backup Methods**, the user's chosen mechanism or primary mechanism automatically is made the same as their prior single mechanism unless you disable that mechanism as well. (For example, if you had set **Single Method, Email Mechanism** and changed to **Multiple Methods** with all mechanisms enabled, the user's choice method would be **Email Mechanism**.

MFA with SMS: Configuring the SMS Gateway Provider

To use SMS for MFA, you must configure an SMS gateway provider to deliver the MFA codes. By default, FileCloud uses Twilio as the SMS gateway provider although enterprise customers may add custom SMS providers and handlers to the system. To configure Twilio with FileCloud, see Multi-Factor Authentication | MFA using SMS: Setting up Twilio as the SMS gateway provider

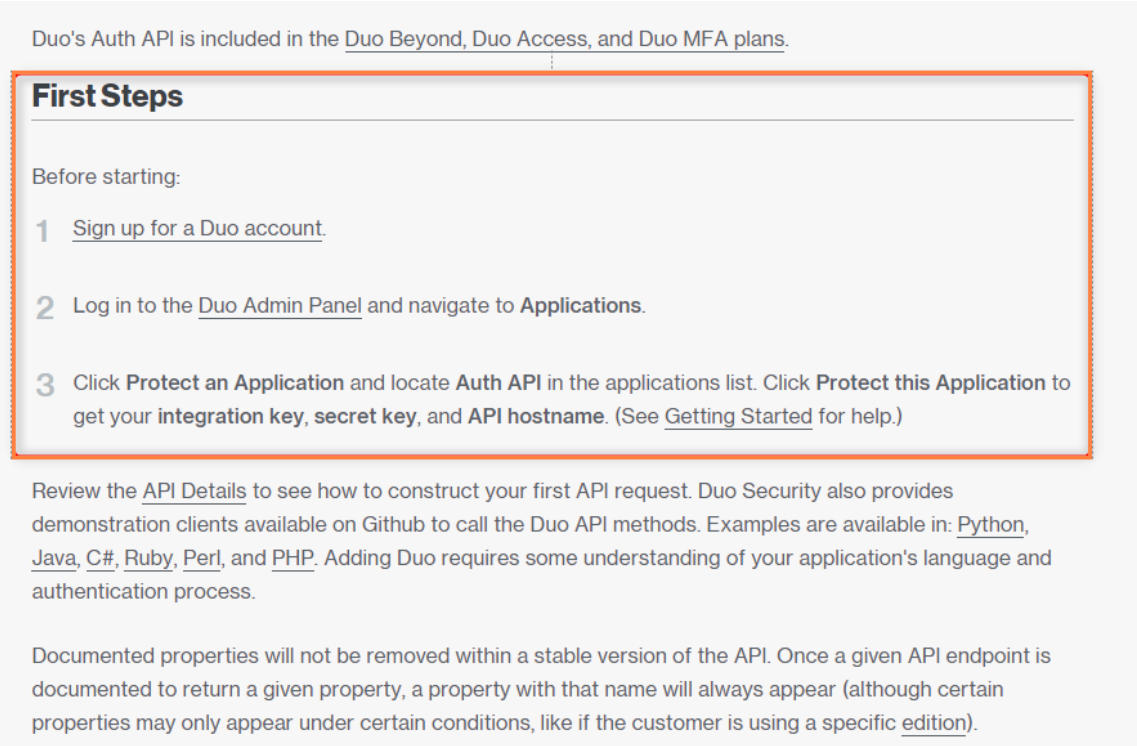
MFA using DUO security

FileCloud can be set up to use DUO security service to perform MFA. Note that DUO PUSH is not supported and requires code generated by DUO Mobile app to be entered to perform MFA.

The following steps are required to set up MFA using DUO.

1. ADD DUO Auth API

- Follow instructions at https://duo.com/docs/authapi to get **integration key**, **secret key**, and **API hostname.**



Duo's Auth API is included in the Duo Beyond, Duo Access, and Duo MFA plans.

First Steps

Before starting:

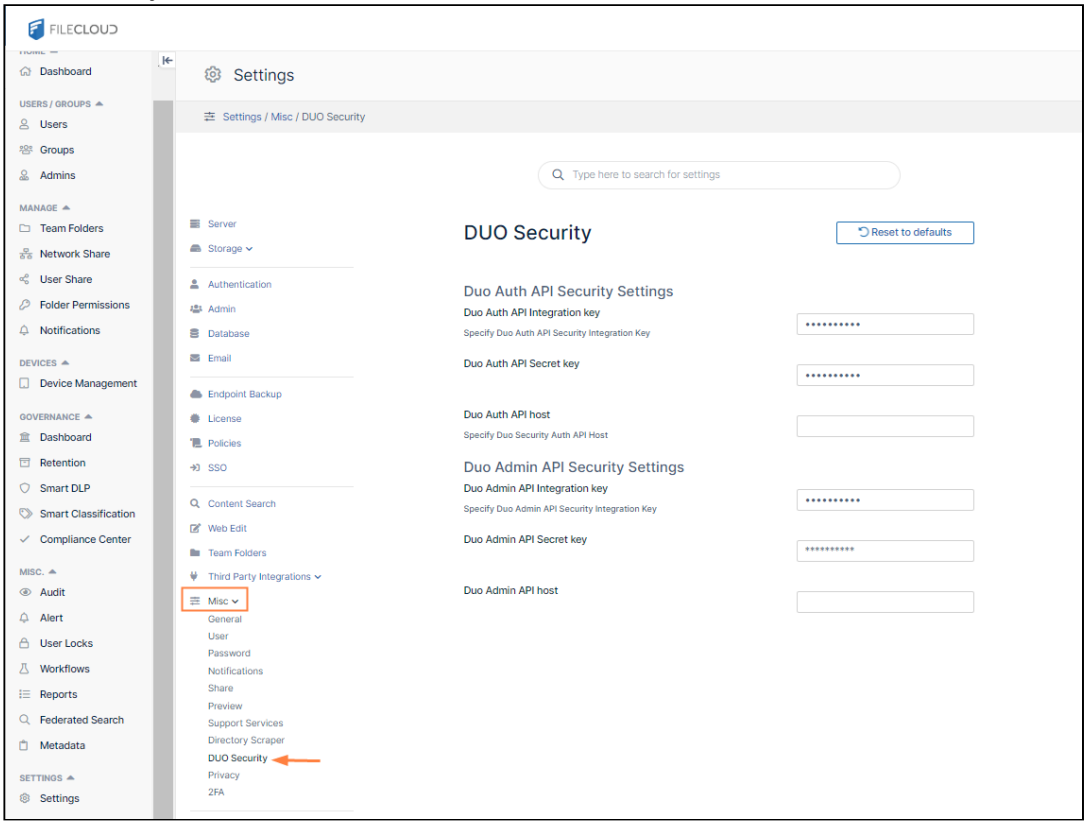
1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate **Auth API** in the applications list. Click **Protect this Application** to get your **integration key**, **secret key**, and **API hostname**. (See Getting Started for help.)

Review the API Details to see how to construct your first API request. Duo Security also provides demonstration clients available on Github to call the Duo API methods. Examples are available in: Python, Java, C#, Ruby, Perl, and PHP. Adding Duo requires some understanding of your application's language and authentication process.

Documented properties will not be removed within a stable version of the API. Once a given API endpoint is documented to return a given property, a property with that name will always appear (although certain properties may only appear under certain conditions, like if the customer is using a specific edition).

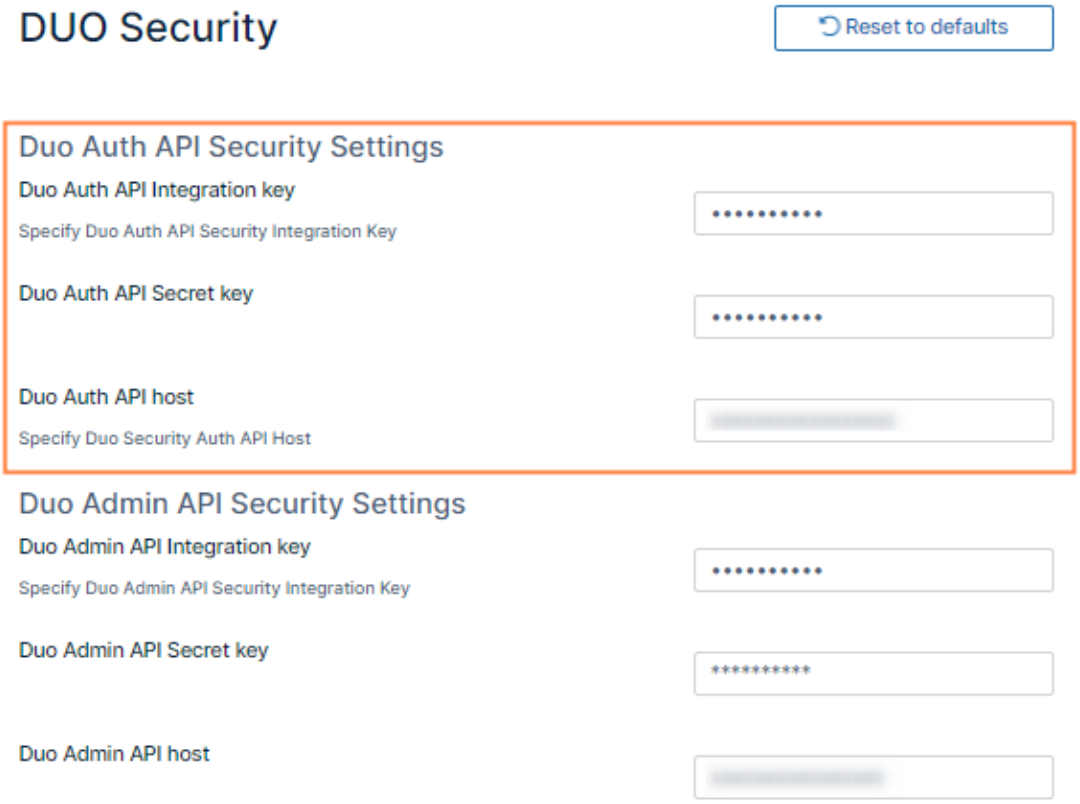
- In the FileCloud admin portal, open the **DUO Security** settings page.
  To go to the Duo Security settings page
  a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **DUO Security**, as shown below.

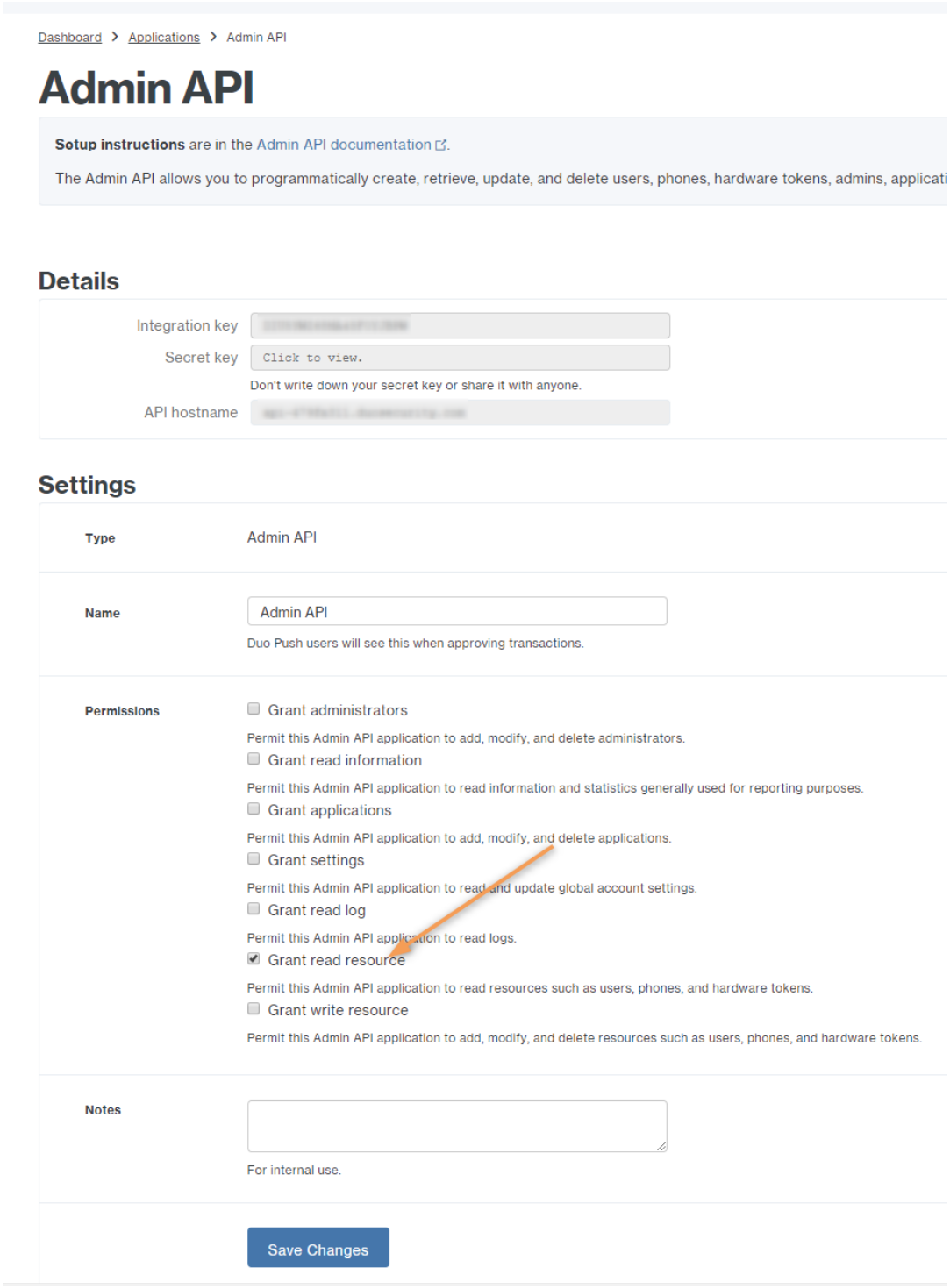


The **DUO Security** settings page opens.

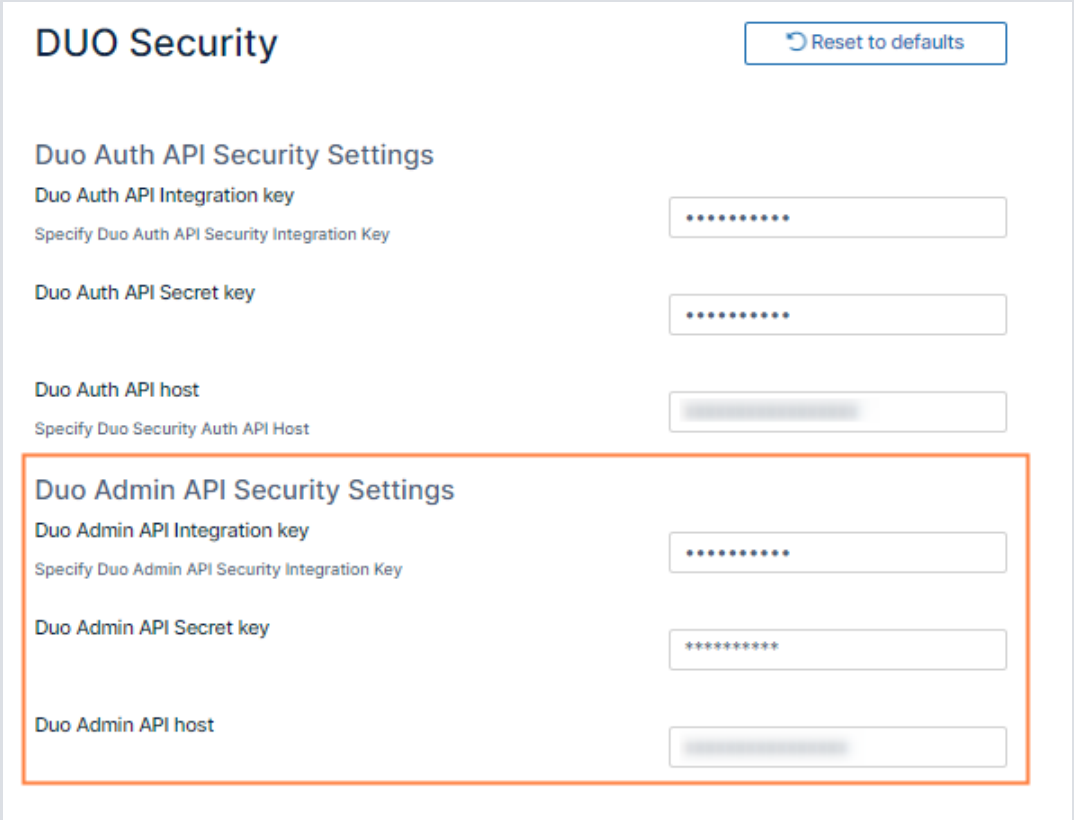
1. Fill in the **Duo Auth API Security Settings** fields on the page.



2. Add DUO Admin API
   - Follow instructions at https://duo.com/docs/adminapi to get values for **integration key**, **secret key**, and **API hostname**
   - Ensure it has **Grant read resource** permission.



- In the FileCloud admin portal, go to the **DUO Security** settings page.
- Fill in the **Duo Admin API Security Settings** fields on the page.



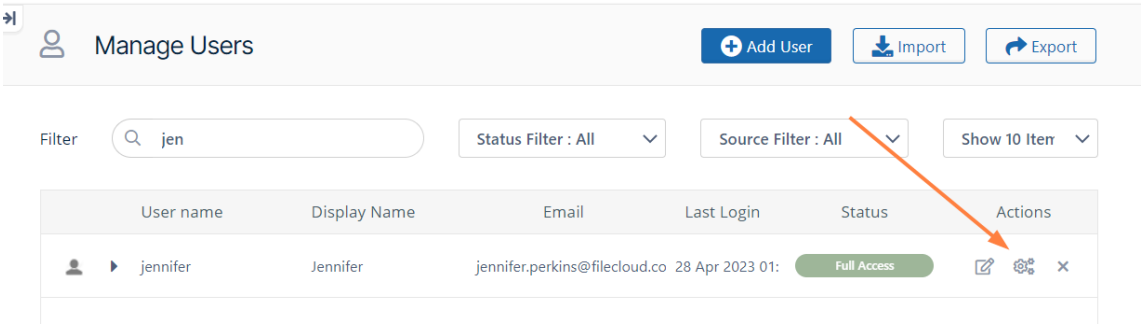
- Now follow the instructions above to enable MFA and specify the MFA mechanism as Duo Security.

  Note: When users who are enrolled in the Duo Admin Panel log in, they must use the text code from the default entry in their Duo App. When users who are not enrolled in the Duo Admin Panel attempt to log in, they are prompted to use a QR code scanner to enroll themselves, and then must use the text code from the entry they added in their Duo App. See Log in Using Multi-Factor Authentication for more information.

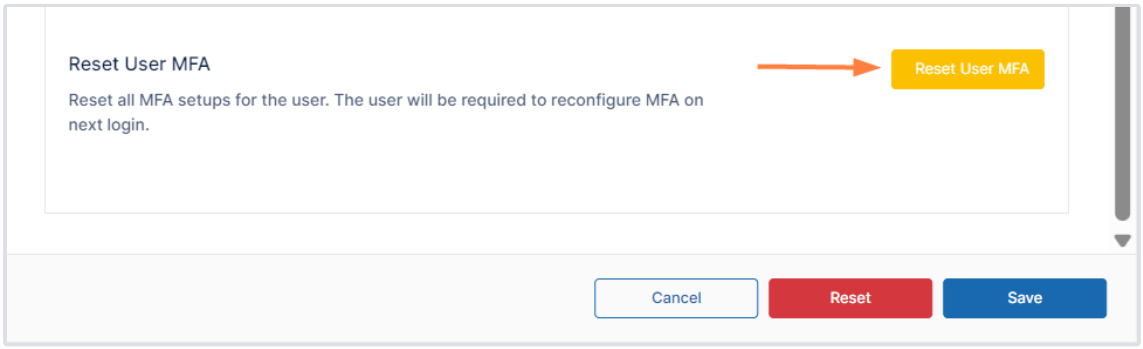
Reset TOTP or DUO settings for a user

When a user loses a TOTP (Google Auth) or DUO app enabled device or if they need to reset the code for any reason, you can reset the authenticator setup for that user using the following steps.

1. In the FileCloud admin portal, go to **Users** and click the **Manage Policy** icon in the row for the user.



2. Click the **MFA** tab.
3. Click the **Reset User MFA** to enable the user to reset their authenticator code.



After the secret is reset, the user is not required to redo the DUO setup on initial login as FileCloud will import access tokens from DUO automatically.
New devices can be registered from the DUO Admin Panel using the DUO Enrollment Email feature.

Multi-Factor Authentication for Admin Portal

> ⚠ TOTP authentication for the admin portal is available beginning in FileCloud 23.242. TOTP authentication should work correctly with any authenticator app; however, the following apps have been tested and performed successfully: Google Authenticator, TOTP Authenticator, Duo Mobile, Microsoft Authenticator, Authy, Okta Verify, 2FA Authenticator (2FAS)

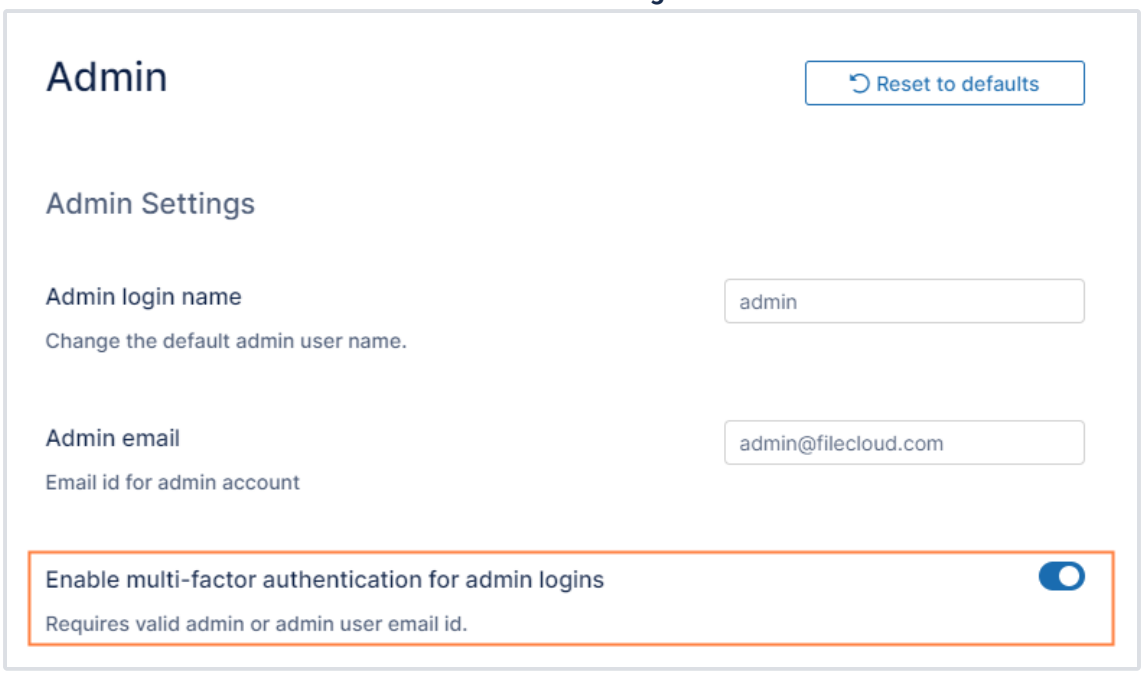
Support for multi-factor authentication is available for admin portal login. Both the primary FileCloud admin and the superadmin (for multitenancy) can be set to require the additional code in order to access the admin portal.

Multi-factor authentication for the admin portal supports authentication by email, SMS, and TOTP.

Enable multi-factor authentication for admins

To enable MFA for the first time an admin logs into the admin portal:

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. Enable **Enable multi-factor authentication for admin logins**.

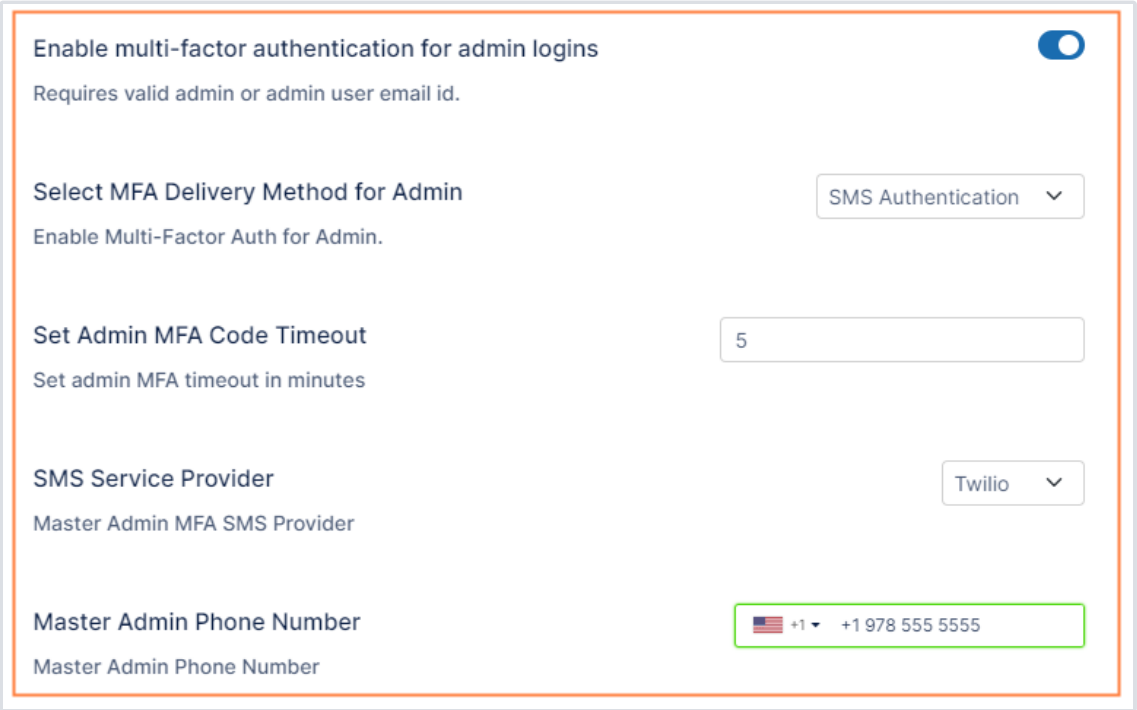


   MFA fields appear.

Setting MFA delivery method to SMS

Note: Currently SMS authentication is effective for the primary admin, but not for promoted admins.

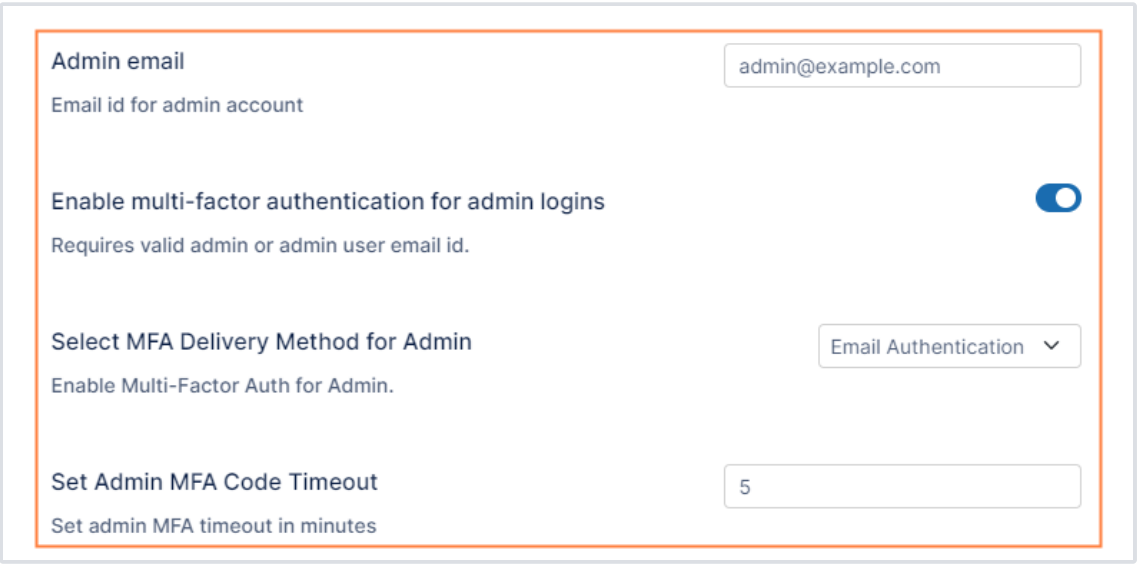
1. To use SMS authentication, In **Select MFA Delivery Method for Admin**, choose **SMS Authentication**.
   Additional fields appear.



2. In **Set Admin MFA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.
3. In **SMS Service Provider**, choose **Twilio** or **Custom**.
4. In **Master Admin Phone Number**, enter the main admin's SMS phone number.
   An invalid main admin phone number will cause lockout - the portal will not be accessible when SMS Authentication is chosen.

Setting MFA delivery method to email:

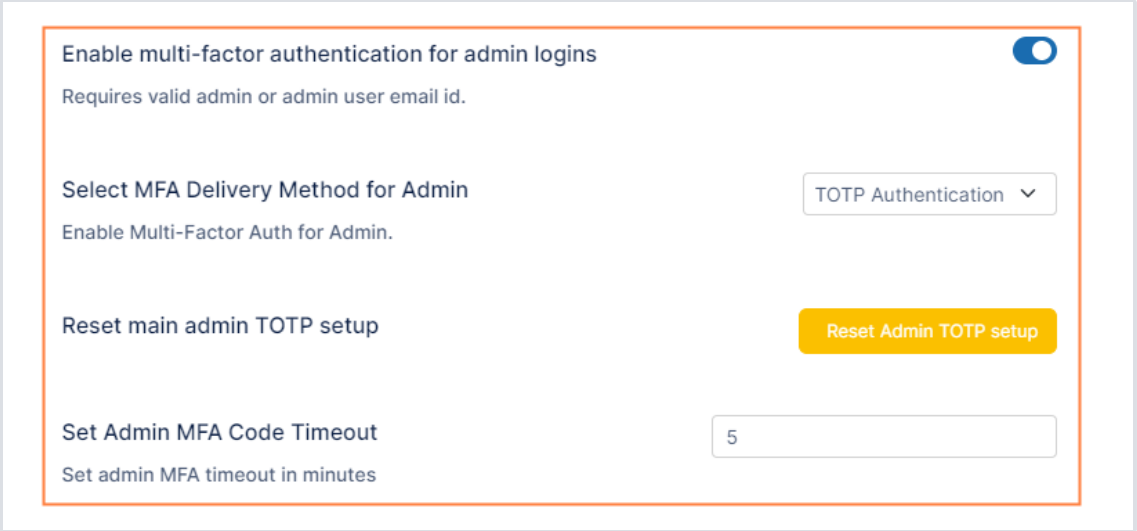
1. To use email authentication, in **Select MFA Delivery Method for Admin**, choose **Email Authentication**.



2. Enter a valid email in the **Admin email** field above the **Enable multi-factor authentication for admin logins** field.
3. In **Set Admin MFA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.

Setting MFA delivery method to TOTP

1. To use TOTP authentication, in **Select MFA Delivery Method for Admin**, choose **TOTP Authentication**.

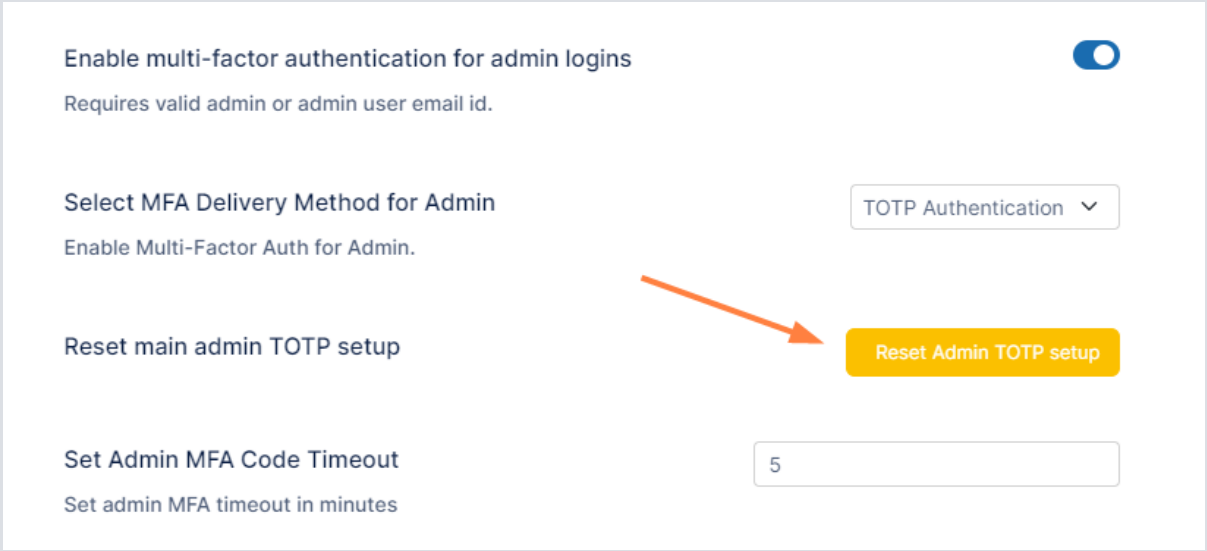


2. In **Set Admin MFA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.
3. See Log in Using Multi-Factor Authentication to set up Google Authenticator (or a similar authenticator app) to use for TOTP Authentication.

   Promoted admins, by default, use the method to log in to the admin portal that they use to log in to the user portal. However, if an MFA method is set for the admin portal, you may override this. See Require promoted admins to use admin portal MFA method, below, for instructions.

Reset TOTP settings for the primary admin

When you select TOTP Authentication for the MFA delivery method, the setting **Reset Admin TOTP setup** appears below it. If the primary admin loses their TOTP-enabled device or needs to reset the TOTP authenticator code for another reason, a promoted admin with **Settings** read and update role privileges can click **Reset Admin TOTP setup** to enable the admin to reset their authenticator code.



Reset TOTP settings for promoted admins

Since promoted admins use their user login method rather than their admin login method to log into the admin portal, a promoted admin will log in to the admin portal with TOTP if that is the method set for their user account, and therefore, to reset a promoted admin's TOTP authorization, use the method explained in Multi-Factor Authentication for User Portal.

However, if you require promoted admins to use the admin portal TOTP method to log in to the admin portal, the reset method is different, as explained below under **Reset TOTP settings for promoted admins when TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS is set to 1**.

Require promoted admins to use admin portal MFA method

You may require promoted admins to use the MFA configuration set up for admins when logging in to the admin portal, regardless of whether their user login is set MFA.

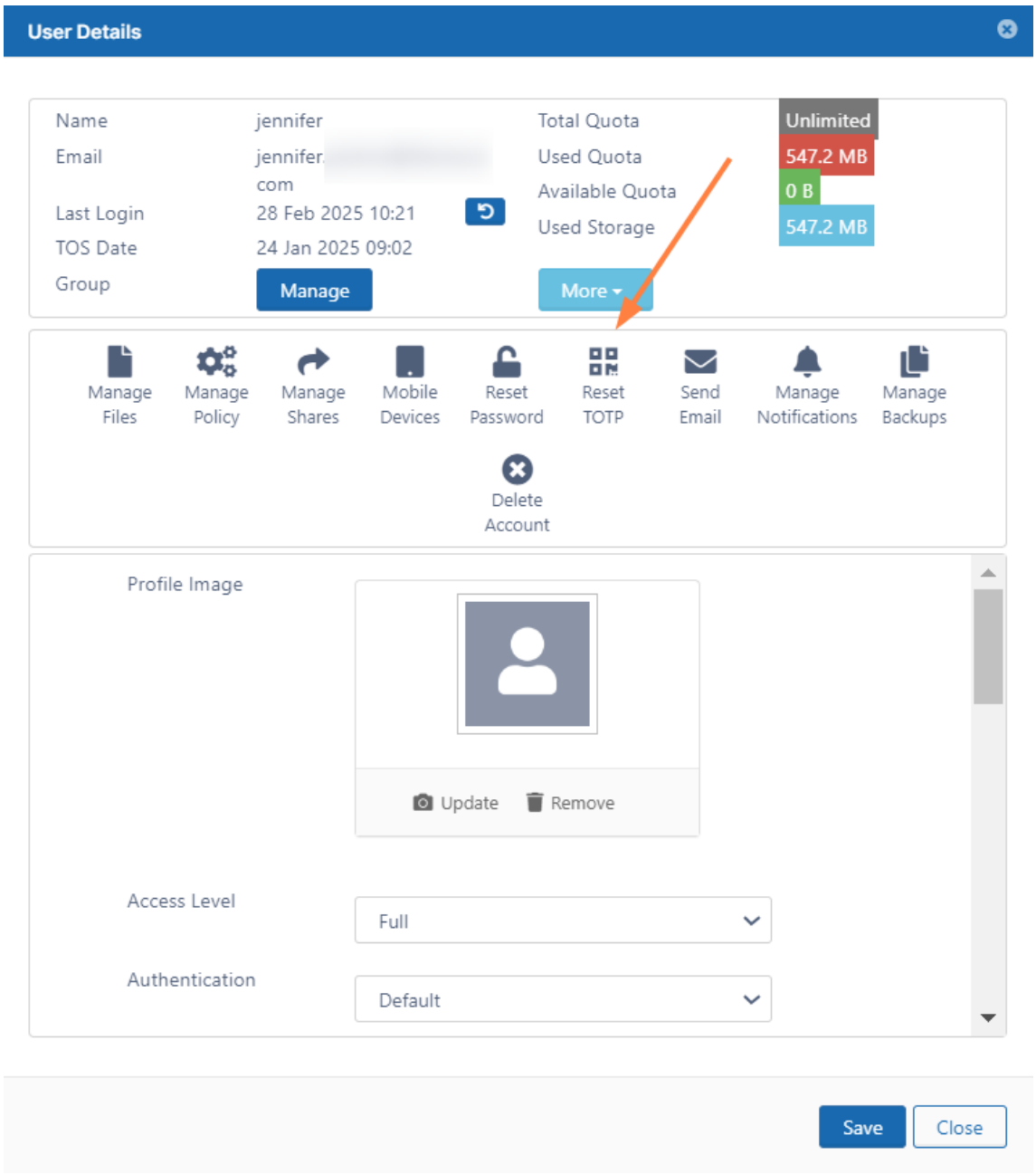
1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the following:

```
define('TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS', 1)
```

Reset TOTP settings for promoted admins when TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS is set to 1:

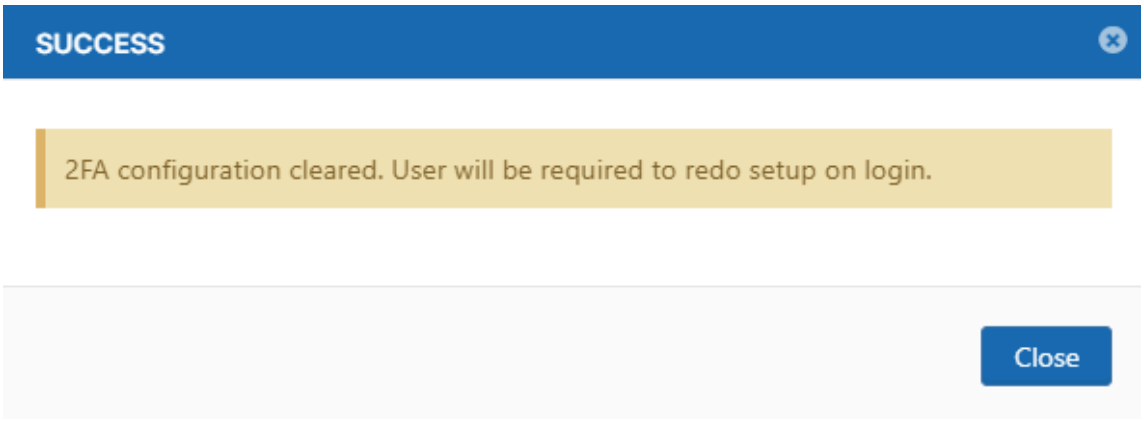
When **TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS** is set to **1**, a promoted admin's TOTP settings cannot be reset through their user account or through the **Reset Admin TOTP setup** button discussed above. Instead, a new button appears on the User Details window accessed from the admin portal's Manage Users page.

1. In the admin portal, click **Users** in the navigation pane.
   The Manage Users page opens.
2. Click the edit icon in the row for the promoted admin.
   The User Details window opens. A **Reset TOTP** icon appears in the user properties.
3. Click **Reset TOTP**.



A confirmation box opens.

4. Click **OK**.
   On successful reset, the following message appears:



Enable multi-factor authentication for SuperAdmin for multitenancy control panel access

Superadmin logins can be required to use MFA to access the multitenancy control panel.

Open "multi.php" (In Linux it is at /var/www/config/ and in Windows it is typically at c:\xampp\htdocs\config)

Add the lines:

```
define ("TONIDOCLOUD_SUPER_ADMIN_EMAIL_ID", "email@company.com");
define ("TONIDOCLOUD_ENABLE_SUPER_ADMIN_2FA","1");
```

In case the lines are commented "//", please remove the double slash symbol at the beginning of the line and save the changes.

Note that you need to provide valid email. If the email is invalid, then the Multi-tenancy control panel cannot be accessed.

Single sign-on (SSO)

Single sign-on (SSO) is a user authentication process that permits a user to enter one name and password in order to access multiple applications.

FileCloud supports the following types of single sign-on models.

When you import SSO users, FileCloud uses the email username (the portion before @) as the FileCloud username. However, since emails with the same username and different domains usually represent the same user, by default, FileCloud does not allow creation of users with the same usernames. However, you may override this default. See Allowing Duplicate Usernames.

SAML Single Sign-On Support

Version 23.241 of FileCloud has dropped support for Shibboleth 1.3 and SAML 1.1, and updated SimpleSAML to version 2.x. If you upgrade from a version below FileCloud 23.241 and your FileCloud build uses SSO, follow the instructions in **Configuring SSO after updating from a version older than 23.241** in (23.263a) Windows: Upgrading Versions <23.252 to the Latest Version or (23.263a) Linux: Upgrading from Versions <23.252 to the Latest Version or SSO will not work correctly in your system.

Note: As of FileCloud Version 20.3.2, to achieve high availability, you can configure FileCloud to support multiple memcache servers.

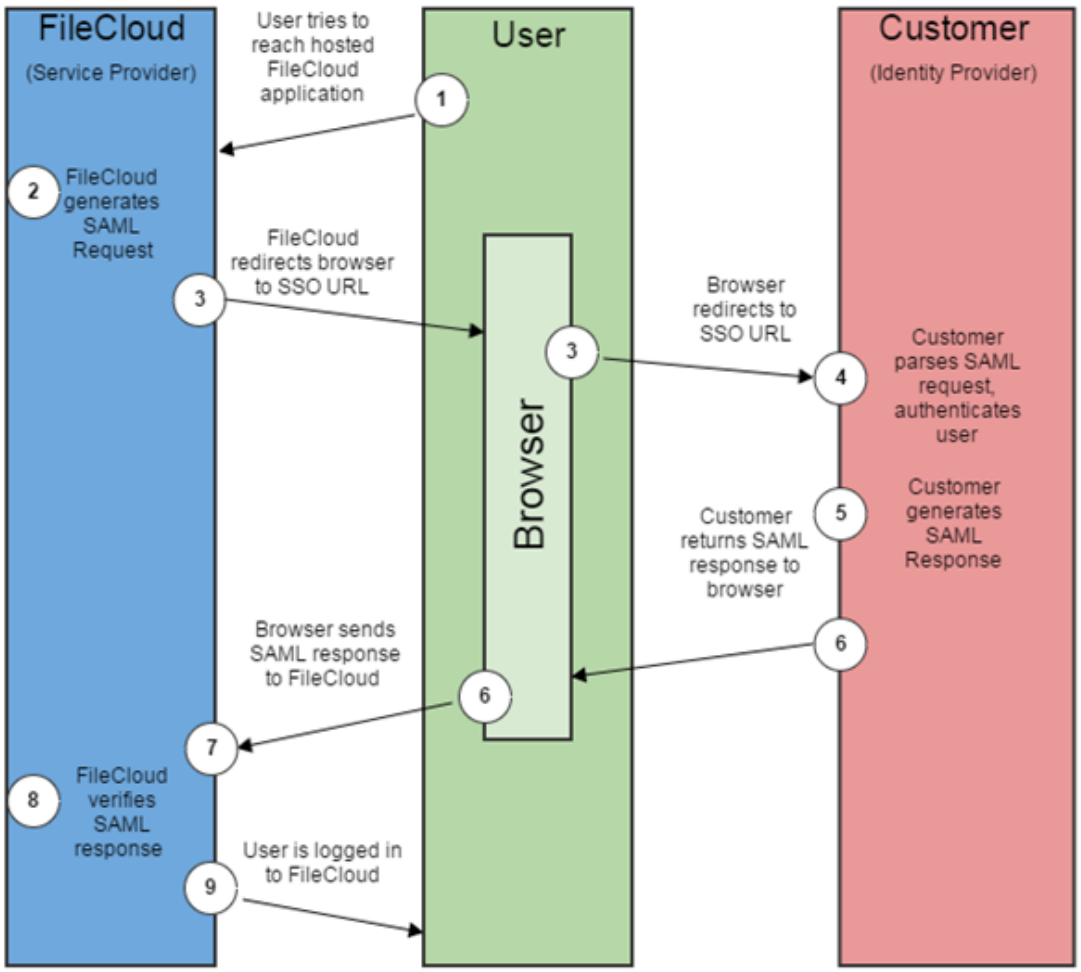
You can use SAML SSO to control the authorization and authentication of hosted user accounts that can access FileCloud Web based interface.

- SAML is an XML-based open standard data format for exchanging authentication and authorization data between parties.
- FileCloud supports SAML (Security Assertion Markup Language) based web browser Single Sign On (SSO) service
- FileCloud acts as a Service Provider (SP) while the Customer or Partner acts as the identity provider (IdP). FileCloud SAML SSO service is based on SAML v2.0 specifications.

SSO Login Diagram

SSO Login Diagram

The following process explains how the user logs into a hosted FileCloud application through customer-operated SAML based SSO service.



FileCloud SAML Transaction Steps

1. The user attempts to reach the hosted FileCloud application through the URL.
2. FileCloud generates a SAML authentication request. The SAML request is embedded into the URL for the customer's SSO Service.
3. FileCloud sends a redirect to the user's browser. The redirect URL includes the SAML authentication request and is submitted to customer's SSO Service.
4. The Customer's SSO Service authenticates the user based on valid login credentials.
5. The customer generates a valid SAML response and returns the information to the user's browser.
6. The customer SAML response is redirected to FileCloud.
7. The FileCloud authentication module verifies the SAML response.
8. If the user is successfully authenticated, the user will be successfully logged into FileCloud.

When the IdP successfully authenticates the user account, the FileCloud (SP) authentication module verifies that the user account exists in FileCloud.
If the user account does not exist in FileCloud, then a new user account is created and the user is logged into FileCloud.

SSO Configuration Steps

In order to successfully configure SAML SSO, the following steps must be followed.

1. Configure Apache server by adding the Alias directive to the simplesaml.php configuration file.
   Pre-requisite: The mcrypt module must be installed on the FileCloud Server.
   In Windows, it should be installed by default.
   In Linux, if mcrypt is not installed, it must be installed

   To add the Alias directive:
   The following are the typical entries in Linux and windows.
   You can change these settings if the FileCloud is installed under a different WEB ROOT Folder

Windows

1. Navigate to the following directory
   `c:\xampp\apache\conf\extra`
2. Open the following file for editing
   `httpd-filecloud.conf`
3. Add the following line at the end of the file
   `Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/public"`
4. Save the file.
5. Open the FileCloud Control Panel.
6. Use the control panel to stop and start the Webserver.

Ubuntu:

1. Open one of the the following files for editing:
   `/etc/apache2/sites-enabled/000-default.conf for HTTP (for port 80)`
   `/etc/apache2/sites-enabled/default-ssl.conf for HTTPS (for port 443)`
2. Add the following line within <VirtualHost *:80> for HTTP connection or <VirtualHost *.443> for HTTPS connection. You can place it under the line DocumentRoot /var/www/html.
   `Alias /simplesaml /var/www/html/thirdparty/simplesaml/public`
3. To restart the apache webserver, run the following command:
   service apache2 restart OR systemctl restart apache2

RHEL:

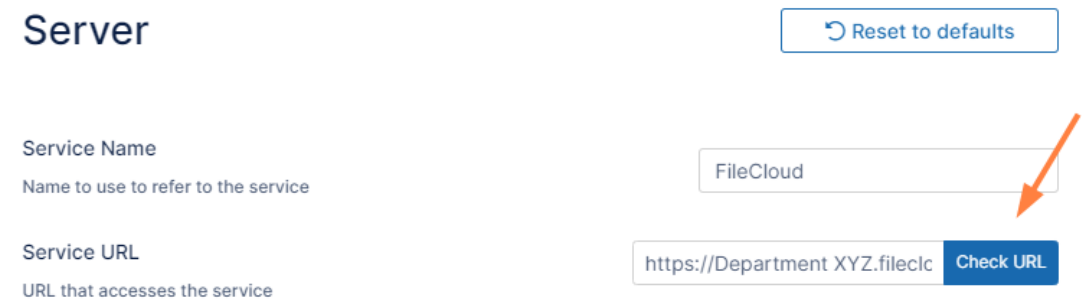
2. Open one of the the following files for editing:
   /etc/httpd/conf/httpd.conf (for port 80)
   /etc/httpd/conf.d/ssl.conf (for port 443)
3. Add the following line within <VirtualHost *:80> for HTTP connection or <VirtualHost *.443> for HTTPS connection. You can place it under the line DocumentRoot /var/www/html.

   ```
   Alias /simplesaml /var/www/html/thirdparty/simplesaml/public
   ```

4. To restart the webserver, run the following command:
   service httpd restart OR systemctl restart httpd

2. Ensure the correct FileCloud URL is set and uses HTTPS

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.
2. In the **Server URL** field, confirm that your URL begins with HTTPS.
3. Click **Check URL** to make sure your URL is valid.



3. Set SAML as the default single sign-on method in FileCloud

To set the SSO type in FileCloud:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. In **Default SSO Type**, select **SAML**.

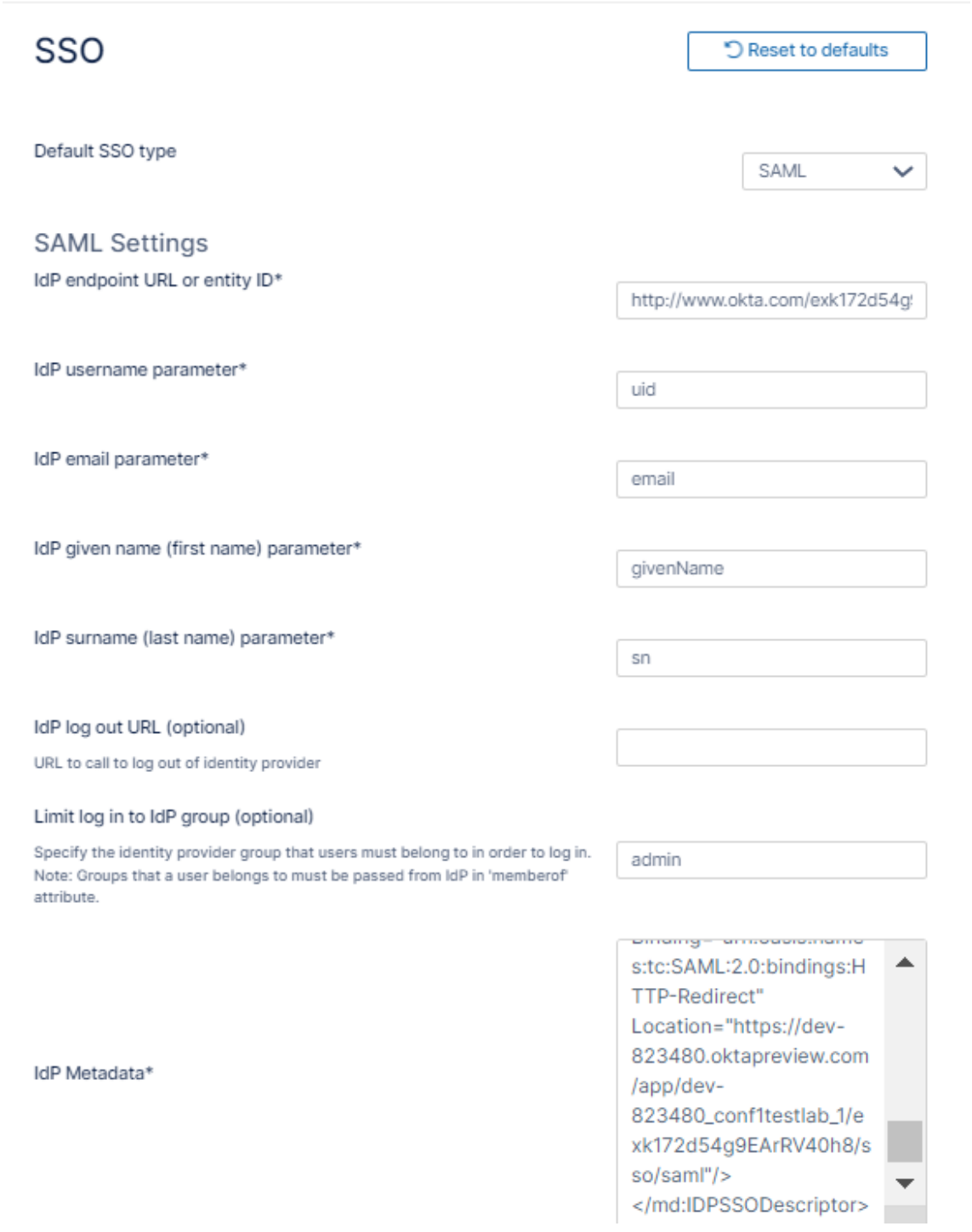


4. Configure IdP settings in FileCloud

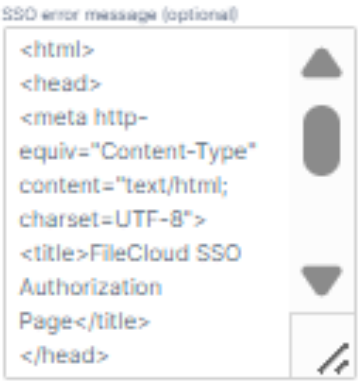
Note: If you are using Active Directory Federation Services (ADFS) Support for authentication, see ADFS Single Sign-On Support.

To configure IdP settings in FileCloud:

1. In the FileCloud admin portal **SSO** settings page, fill in the settings under **SAML Settings**.



SSO error message (optional)



Allow account signups

Allow new account creation through login process

Automatic account approval

3

Set Admin approval for creating new accounts.
0 - No automatic approval, Admin has to approve account.
1 - Automatically approve new accounts to Full User.
2 - Automatically approve new accounts to Guest User.
3 - Automatically approve new accounts to External User

Enable ADFS

Specify if IdP is Active Directory Federation Service (ADFS)

User login token expiration follows IdP token expiration rule

User authentication token will expire as specified by identity provider.

Enable browser-only SSO session timeout

If enabled, SSO session timeouts will be restricted to web browsers only

Show the Idp login screen

Redirect user login to IdP login screen automatically.

Log level

PROD

Use DEV only for testing.

Allow SSO for external users

Use the following table to understand the IdP settings.

FileCloud Parameters	IdP Settings
IdP End Point URL	Identity Provider URL
IdP Username Parameter	Identifies the Username (must be unique for each user) • Usually uid or agencyUID • Default value: uid **NOTE: The username must be unique**. If username sent by Idp is in email format, the email prefix will be used for username. The email prefix in this case must be unique.
IdP Email Parameter	Identifies the email of the user (must be unique) Default value: mail
IdP Given Name Parameter	Identifies the given name of the user Default value: givenName
IdP Surname Parameter	Identifies the surname of the user Default value: sn
IdP Log Out URL (Optional)	URL for logging out of IdP. This is required if you are syncing groups on every login.
Limit Logon to IdP Group	IdP Group Name • Specifying a group name means that a user can login through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group • The IdP must send this group name through the **memberof** parameter • The **memberof** parameter can include a comma separated value of all groups to which the user belongs
Show the IdP login screen	Identifies which Logon screen the user will see: • FileCloud screen = not selected • IdP screen = selected
IdP Metadata	Identity Provider metadata in XML Format

FileCloud Parameters	IdP Settings
SSO Error Message (Optional)	Custom error message that appears when a login is invalid. Enter in HTML format, and use the variable ^MESSAGE^, which shows error details when SSO login fails. For example: ** ^MESSAGE^ ** In a multiple IDP environment, this is the error message for the default IDP. See Integrating Multiple IDPs for help configuring multiple IDPs with error messages specific to each one.
Allow Account Signups	When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.
Automatic Account Approval	This setting works with the **Allow Account Signups** setting to determine: • If the account created by the user is disabled until the administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. • Possible values are: 0 - No automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User See Integrating Multiple IDPs for help configuring multiple IDPs with automatic account approval settings specific to each one.
Enable ADFS	If enabled, identifies IdP as Active Directory Federation Service.
User login token expiration match IdP expiration	If enabled the user token expiration will be set based on Idp expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)
Enable Browser-Only SSO Session Timeout Added in FileCloud 23.232.1	If enabled, SSO session timeouts apply to browser sessions but not to client sessions.
Show the IdP login screen	If enabled, automatically redirect user to Idp log-in screen.

FileCloud Parameters	IdP Settings
Log Level	Set the Log mode for the SAML Calls. Default Value: prod (Do not use DEV for production systems)
Allow SSO for external users Added in FileCloud 23.253	Only appears if feature is included in license. If enabled, external users can log in to FileCloud using SSO. Default value: Disabled.

5. Register FileCloud as a Service Provider (SP) with the IdP

Use the following URL (Entity ID) to register FileCloud as an SP with IdP or ADFS. The URL below also provides the metadata of the FileCloud SP:

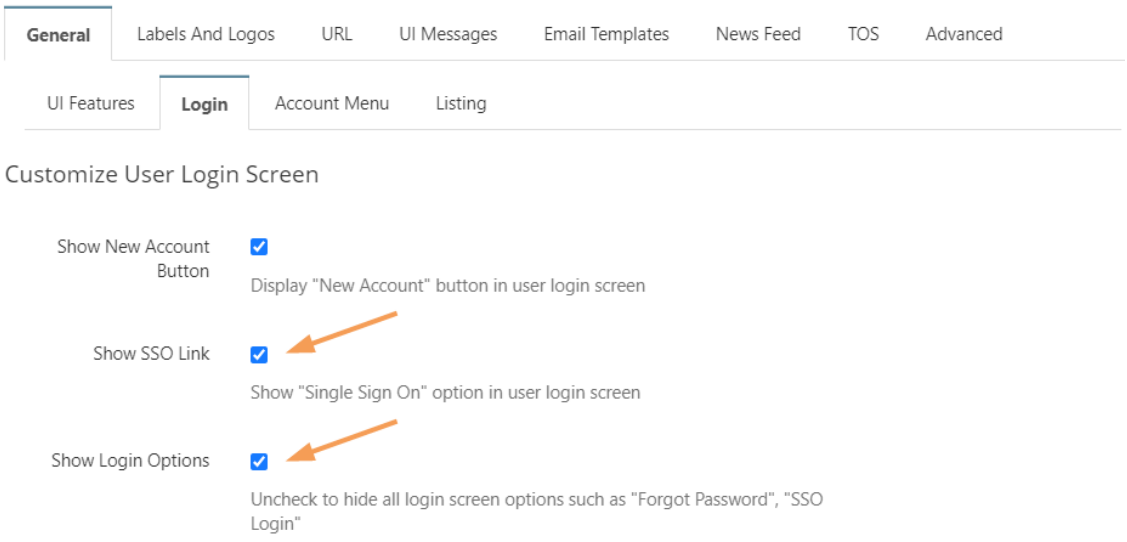
http://<Your Domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp

6. Enable the SSO link on the login page

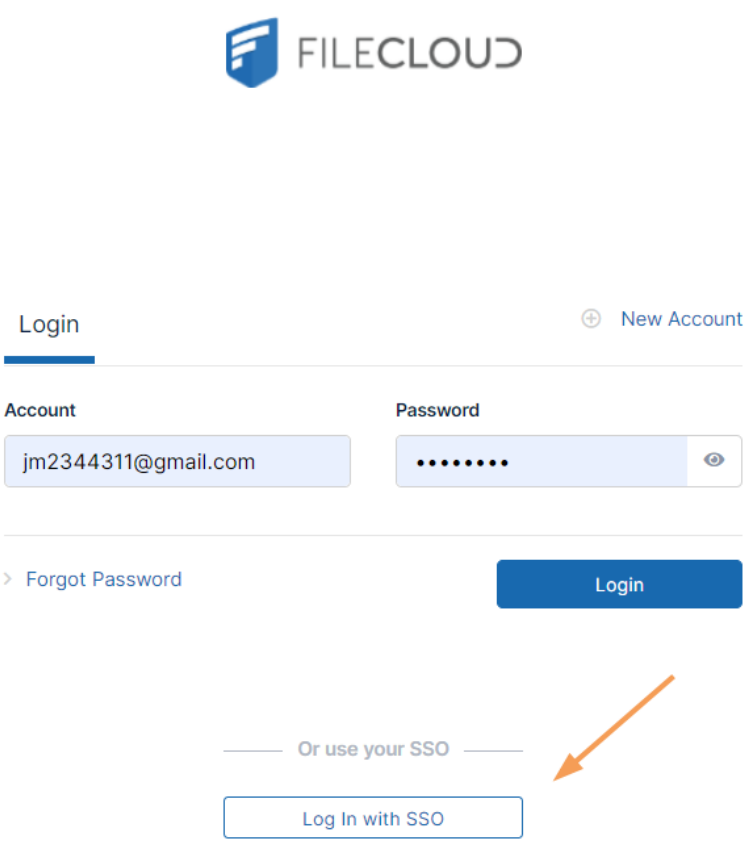
You can customize the user log-in screen to display the SSO log-in option along with the direct log-in option or to only display the SSO log-in.

To display the SSO log-in option along with the direct log-in option:

1. From the left navigation pane, click **Customization**.
2. Select the **General** tab, and then the **Login** sub-tab.
3. Check **Show SSO Link** and **Show Login Options**.



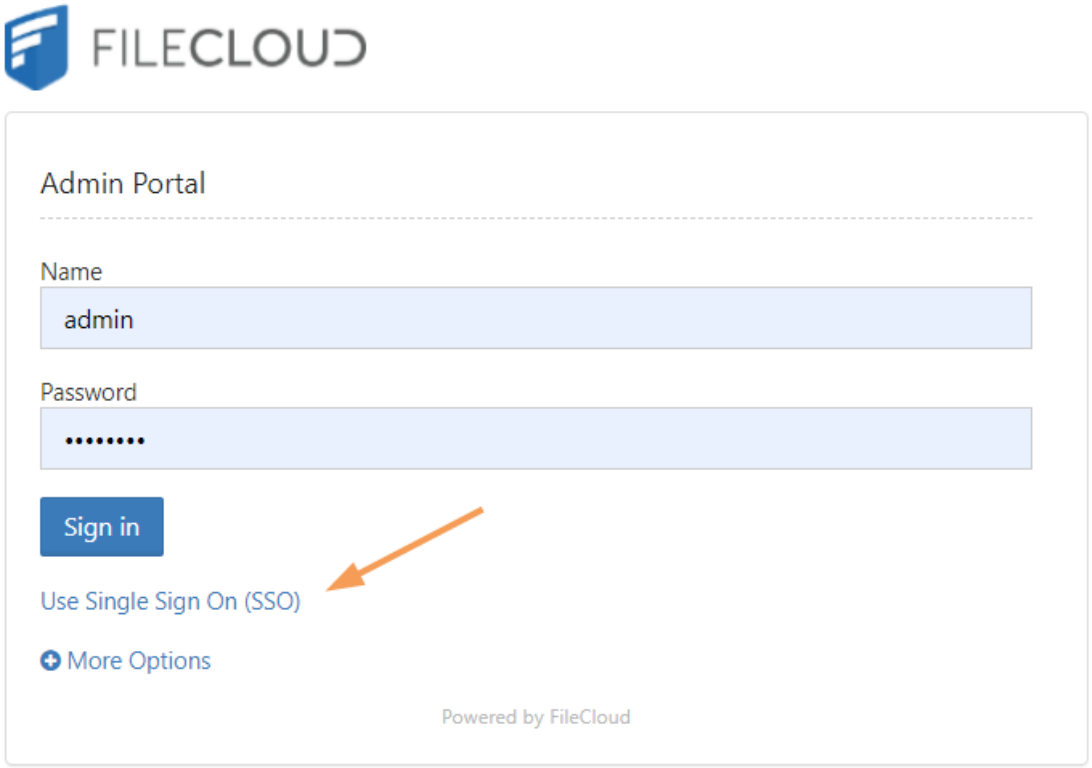
4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



On clicking the Single Sign-On link on the login page, the user is redirected to the SAML SSO Service web page.

The SSO log-in option in the admin portal:

FileCloud admin interface also supports Single Sign-On.



Default admin portal log-in screen

To only display the SSO log-in option:

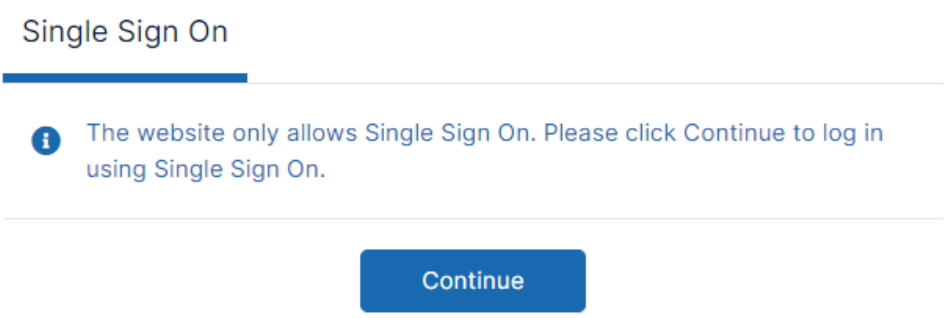
In order to skip the FileCloud login page and send the user directly to the SAML SSO page you must add a setting to the cloudconfig.php file, as shown below. You can configure this option for the user portal login page and the admin portal login page.

To only display the SSO log-in option in the user portal:
This configuration option supports skipping the login page when the user accesses FileCloud with a domain name or with a full URL.

1. In the admin portal, go to **Customization,** and select the **General** tab, and then the **Login** sub-tab.
2. Check **Show SSO Link** and **Show Login Options**, and save your changes.
3. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
4. To only display the SSO log-in option:

```
define("TONIDOCLOUD_SSO_DIRECT_ONLY", "1");
```

When users enter the log-in page they will see:



To return to displaying other log-in options:

```
define("TONIDOCLOUD_SSO_DIRECT_ONLY", "0");
```

To display only SSO log-in in the admin portal:
FileCloud supports skipping the login page when the admin accesses FileCloud with a domain name or with a full URL.

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To only display the SSO log-in option:

Enter:

```
define ("TONIDOCLOUD_SSO_DIRECT_ONLY_ADMIN", "1");
```

7. Enable secure cookies for SimpleSAML

To enable secure cookies when using SimpleSAML to authenticate, proceed on the following.

1. Open the SimpleSAML configuration file:
   Windows: XAMPP DIRECTORY/htdocs/thirdparty\simplesaml\config\config.php
   Linux: /var/www/config/thirdparty/simplesaml/config/config.php
2. Change **session.cookie.secure** from **FALSE** to **TRUE**:
   ```
   'session.cookie.secure' => true,
   ```
3. (Optional) For better cookie security set the **session.cookie.samesite** attribute to **Strict** or **Lax** according to the environment's needs.
   If the FileCloud site is embedded in an external site, it may be necessary to leave this setting null or set it to **None** to enable cookie sharing with the external site.
   ```
   'session.cookie.samesite' => 'Strict',
   ```

8. Best Practices

Avoid Open Redirect

FileCloud may be vulnerable to an open redirect when SSO is implemented.

- An open redirect is an application vulnerability that takes a parameter and redirects the user to the supplied parameter value without any validation.

This can be avoided by configuring the following setting:

1. Navigate to the following directory:
   `<FileCloud WEB ROOT>/thirdparty/simplesaml/config`
2. Open the following file for editing:
   `config.php`
3. Add the following line:
   `'trusted.url.domains' => array()`

Restrict the Available Admin Login Resources

The FileCloud admin portal can possibly allow 2 administrative login interfaces:

- One at admin API interface: /admin
- One at simpleSAML admin resource: /simpleSAML.

This can be avoided by changing the log level to "PROD" in SSO settings under settings in FileCloud admin interface. This will disable the SSO admin page under simpleSAML.

The password to the SSO admin page under /simpleSAML can be changed under 'auth.adminpassword' key in <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php

Troubleshooting

Troubleshooting

Issues that you may encounter and how to resolve them.

Issue

FileCloud is hosted behind a Proxy

Solution
When FileCloud is hosted behind a proxy server, SAML will not automatically work.

Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/filecloudconfig.php

Add Proxy Server Information here.

Format is as follows user:password@yourproxyserverurl.com

define("TONIDOCLOUD_SAML_PROXY", "ADD PROXY INFO HERE");

Issue

System Timezone Settings

Solution

After setting SAML log level to DEV. Log file will be created under <FileCloud WEB ROOT>/thirdparty/simplesaml/log/simplesamlphp.log

SimpleSAML_Error_Exception: Error 2 - strftime(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function.

Solution: date.timezone setting must be set explicitly in php.ini

Issue

FileCloud is hosted behing a reverse proxy

Solution

When FileCloud is hosted behind a proxy server, SAML will not automatically work.

Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php

set the base url to 'baseurlpath' => 'http(s)://YOURFILECLOUDOMAIN/simplesaml/'

Issue

Debug page login

Solution

https://YOURFILECLOUDDOMAIN/simplesaml/module.php/core/frontpage_welcome.php

Issue

FileCloud in HA (High Availability) environment with multiple servers

Solution

In this scenario, SimpleSAML will most likely not work with default configuration and will require to run Memcache to manage the session.

Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php

set the store.type => memcache

and set

'memcache_store.servers' => array(
array(
array('hostname' => 'localhost'),

),
),

where 'localhost' must be replaced with IP of memcache server as appropriate.

Issue

Autofill Username or Email on the IDP screen when configured:

TONIDOCLOUD_SAML_DOMAINS_ALLOWED

Solution

When autofill will only work when username or email address is sent through POST from the FileCloud login page to IDP. Therefore, ensure that the IDP metadata accepts requests through only POST. For example, if the Idp Metadata contains the following 2 similar lines, remove the Redirect and only have the POST

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://mailinator-raja.okta.com/app/mailinatororg747392_myidp_1/exkgimvocj18Exx9g4x6/sso/saml"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://mailinator-raja.okta.com/app/mailinatororg747392_myidp_1/exkgimvocj18Exx9g4x6/sso/saml"/>

Override the default SSO port

To override the default port:

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

```
define("TONIDOCLOUD_SSO_FULLURL_OVERRIDE", "https://filecloud.test.com");
```

Use multiple memcache servers

In FileCloud Versions 20.3.2 and higher, you can use multiple memcache servers with SAML SSO to achieve high availability.

To use multiple memcache servers:

1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the following lines, including a hostname for each of the memcache servers.

In this example, the IP addresses of the servers are 79.97.83.70 and 79.97.83.71.

```
function SSO_MEMCACHED_SERVERS() {
return [
  [
    ['hostname' => '79.97.83.70']
  ],
  [
    ['hostname' => '79.97.83.71']
  ],
];
}
```



In HA environments with SSO, either point all FileCloud server nodes to the same memcache server or to the same memcache cluster.
Any of the following will break SSO:

- Pointing each FileCloud server node to the local memcache server, IP 127.0.0.1
- Point each FileCloud server node to a different memcache server.

Integrate Auth0 SSO with Filecloud

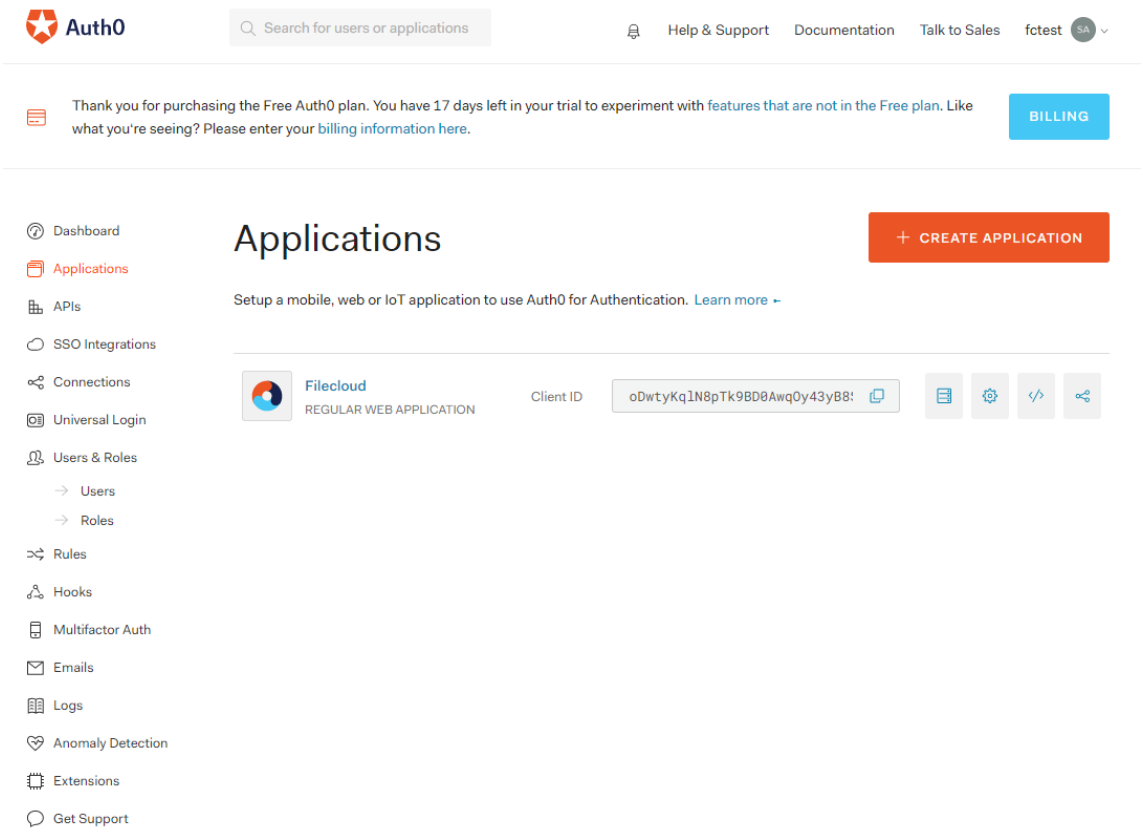


Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

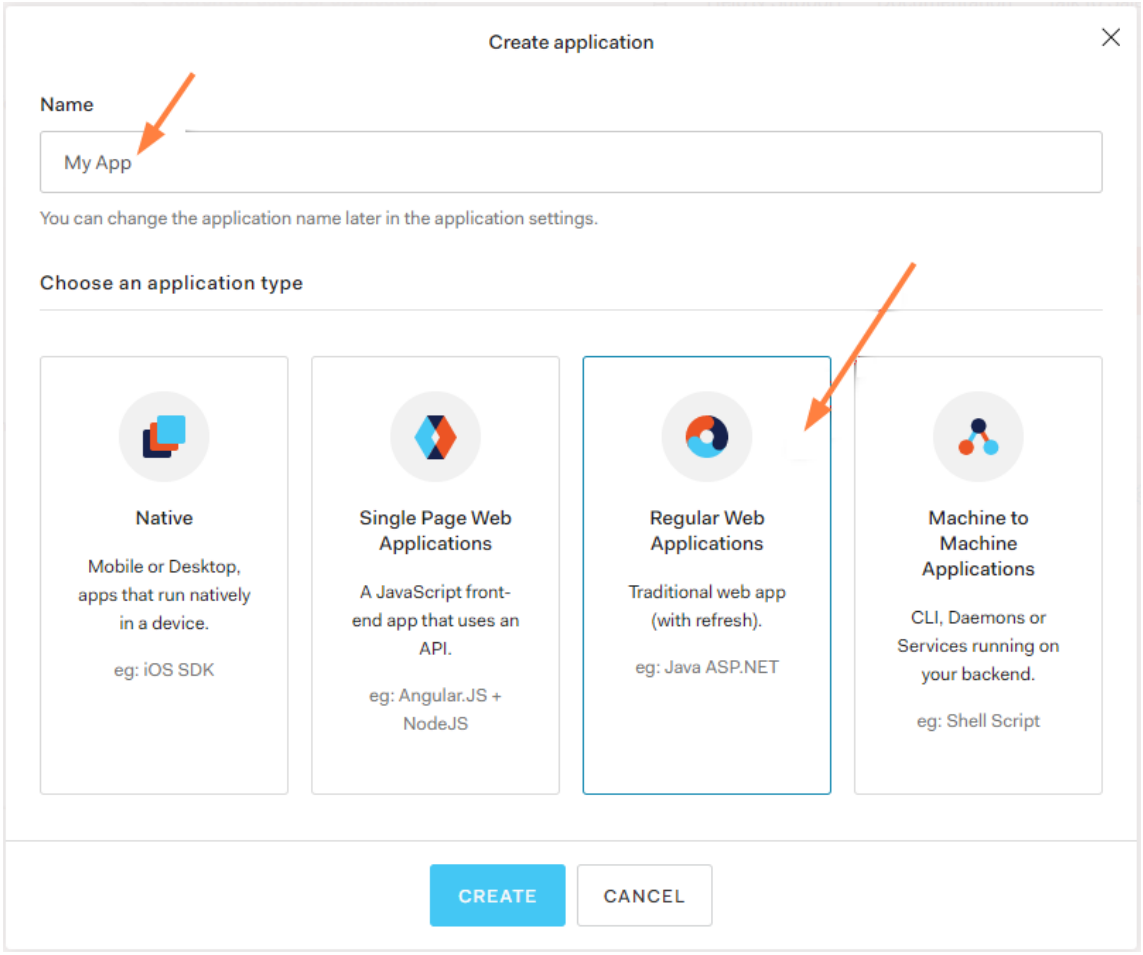
You can integrate Auth0 SSO with Filecloud using the SAML 2 protocol. Below are the steps to achieve this.

Configuration in Auth0 portal

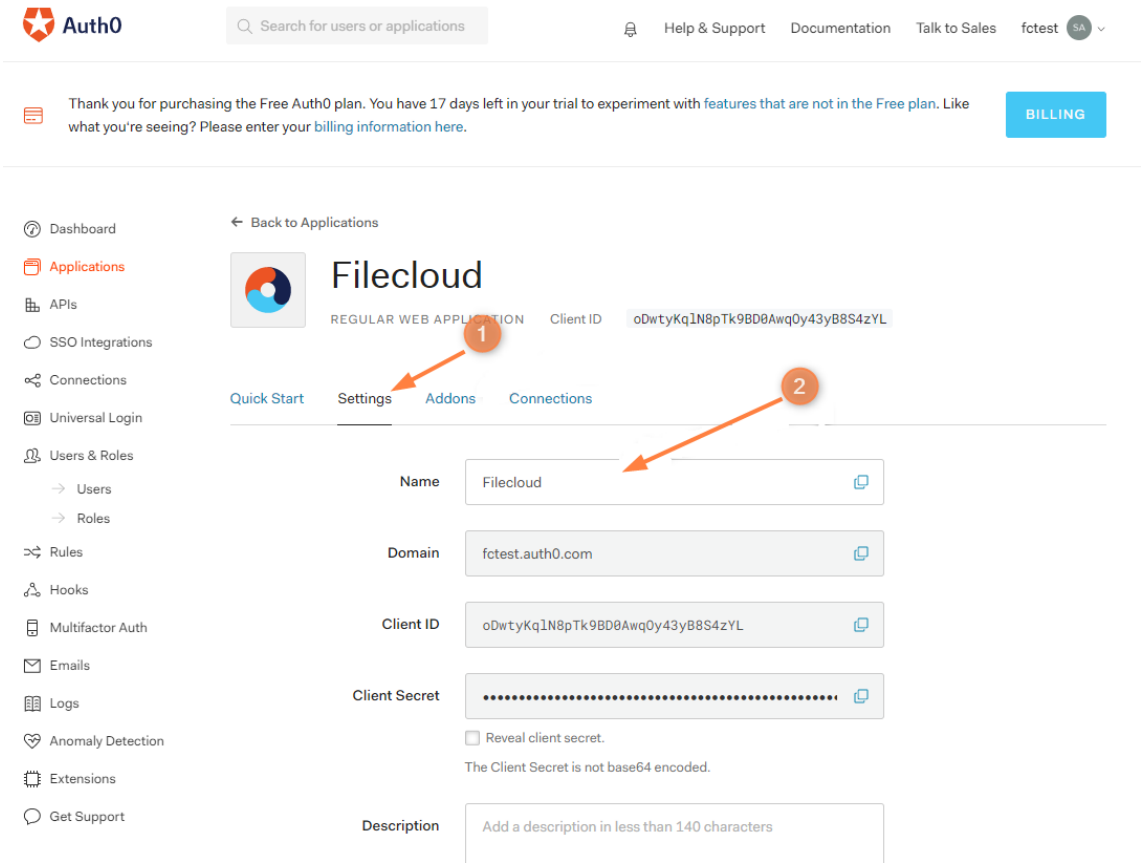
1. Log in to the Auth0 Dashboard and click the tab **Application** on the left panel.
2. Create the application.



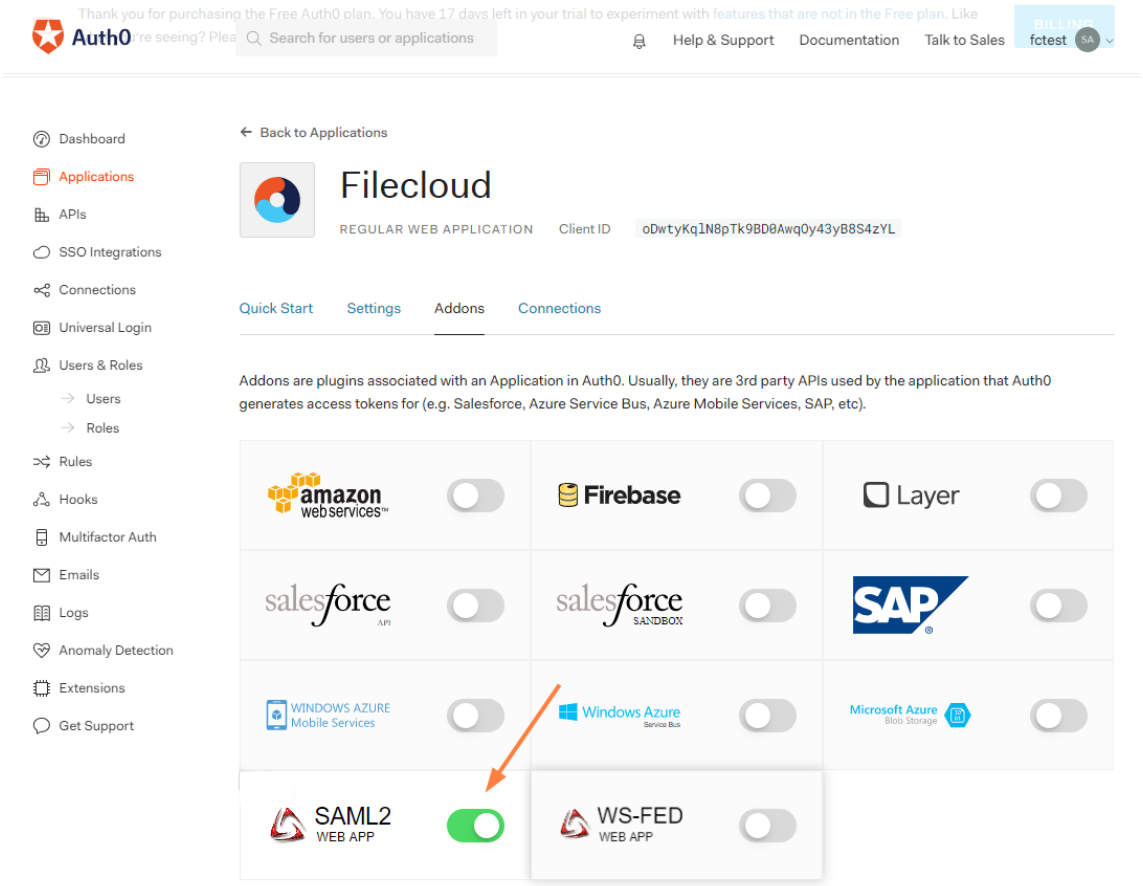
3. Name the application and click **Regular Web Applications**.



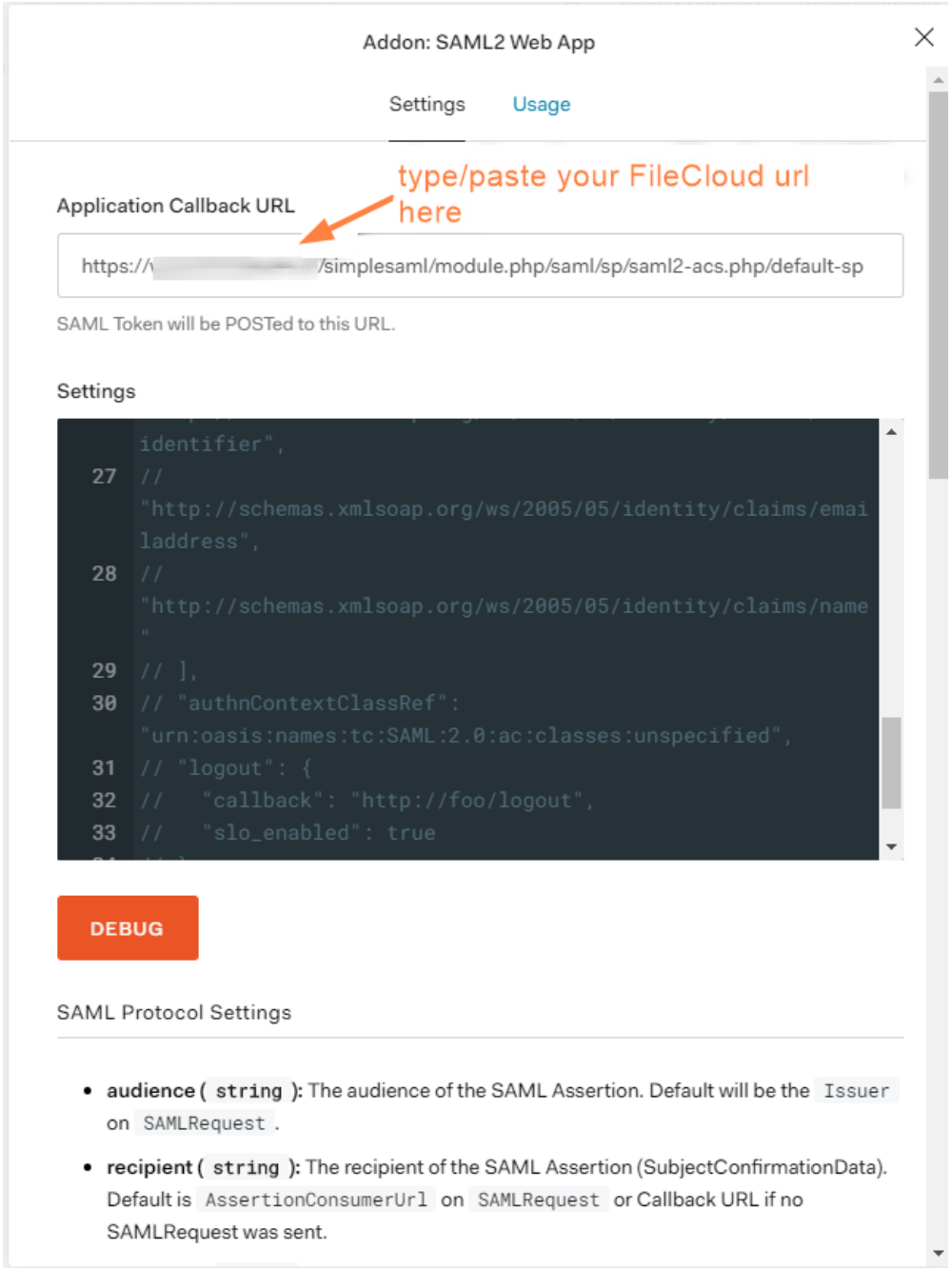
4. Click the created application again and go to the settings tab. Confirm that the application name is in the **Name** field and click **Addons**.



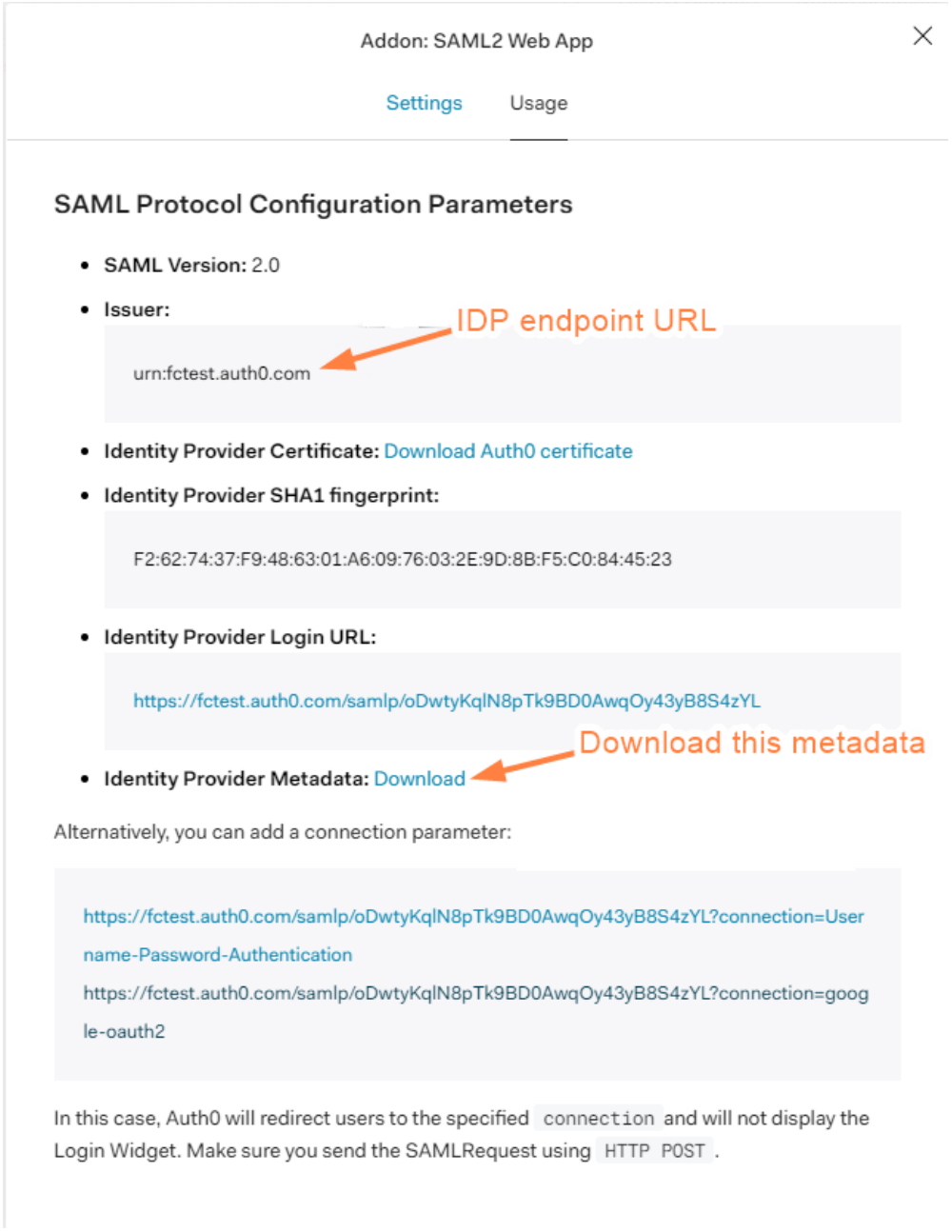
5. Click **SAML2 Web App**.



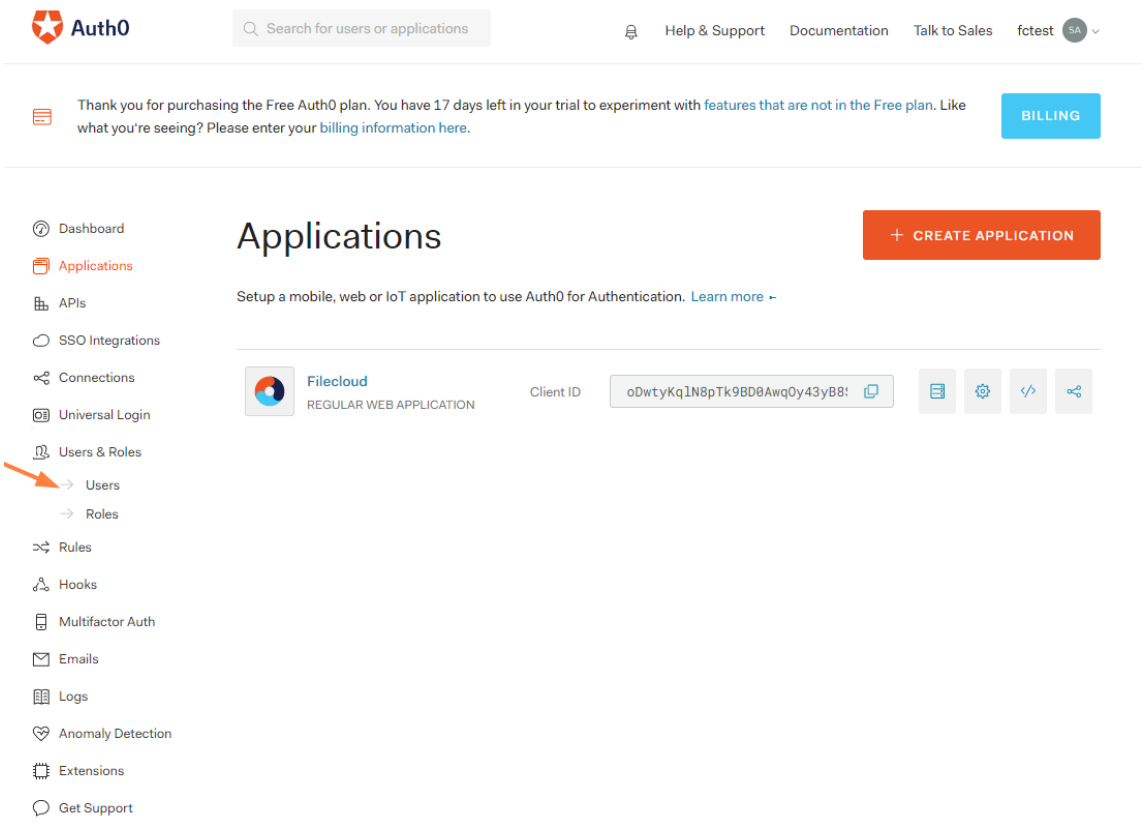
6. Enter your FileCloud URL in the **Application Callback URL**.
   https://your_filecloud_url/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp



7. Scroll down and click **Enable**.
8. Click **Usage**.

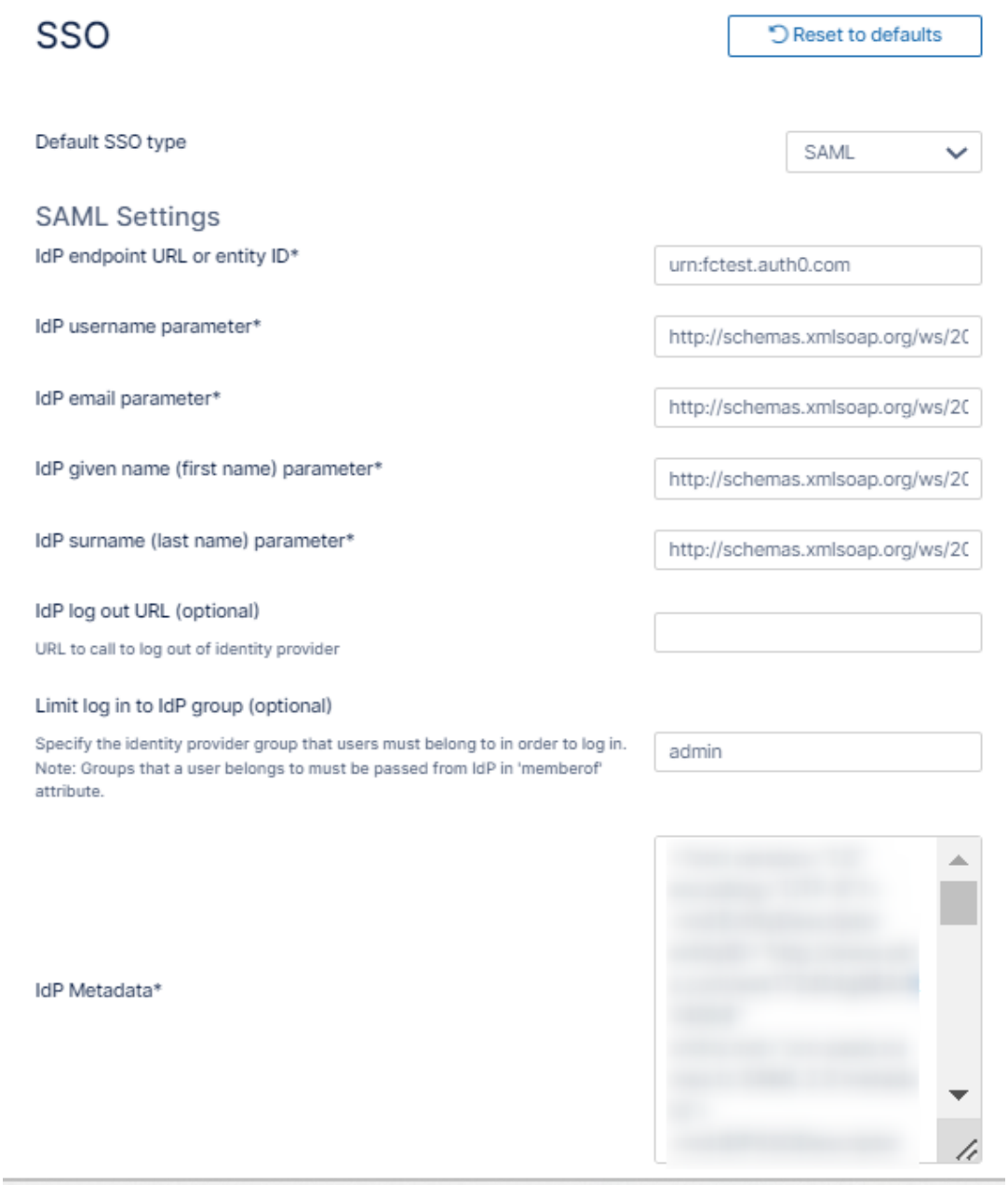


9. Note down the value in the field **Issuer**.
10. Scroll down and download the metadata from **Identity Provider Metadata**.
11. Go to **Users** in the Auth0 Dashboard and create the user.



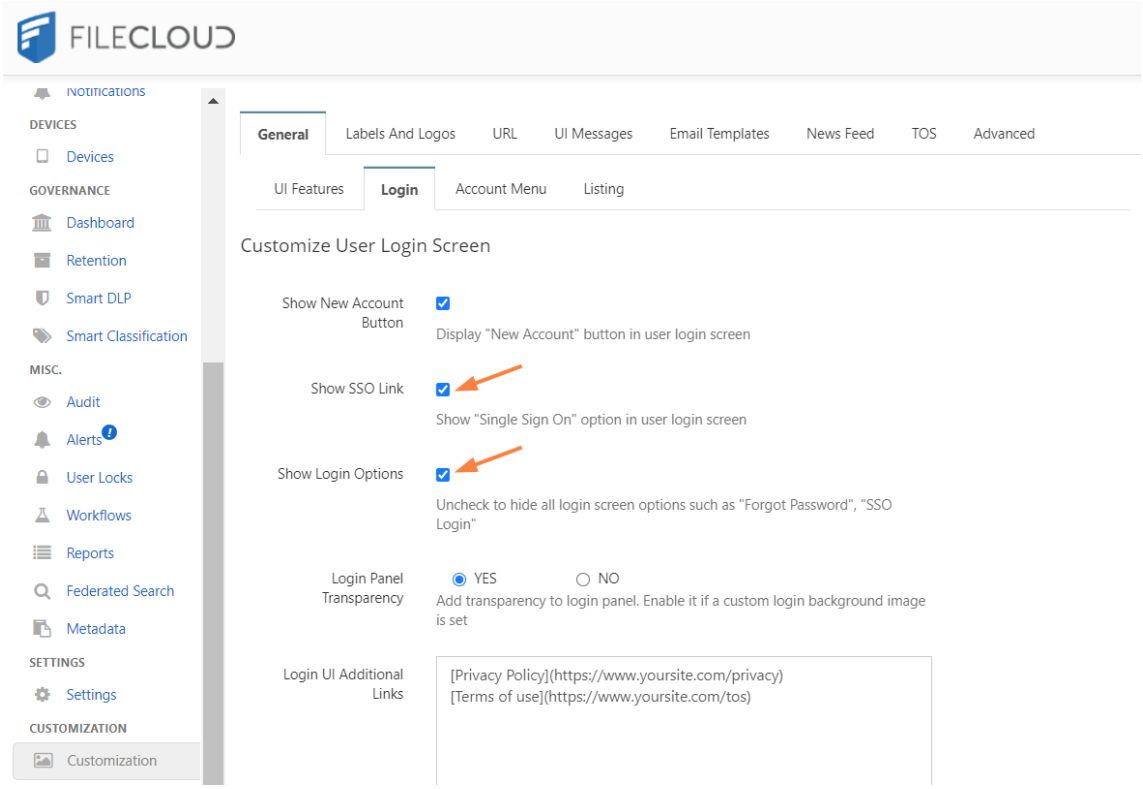
Configuration in FileCloud admin portal

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. Enter the below details in the required fields
   - **IdP End Point URL**: Paste here the value we note down from **Issuer:** (step 9, above)
   - **IdP Username Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
   - **IdP Email Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
   - **IdP Given Name Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
   - **IdP Surname Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
   - **IdP Metadata**: Open the metadata file we have downloaded using notepad and copy paste value here.



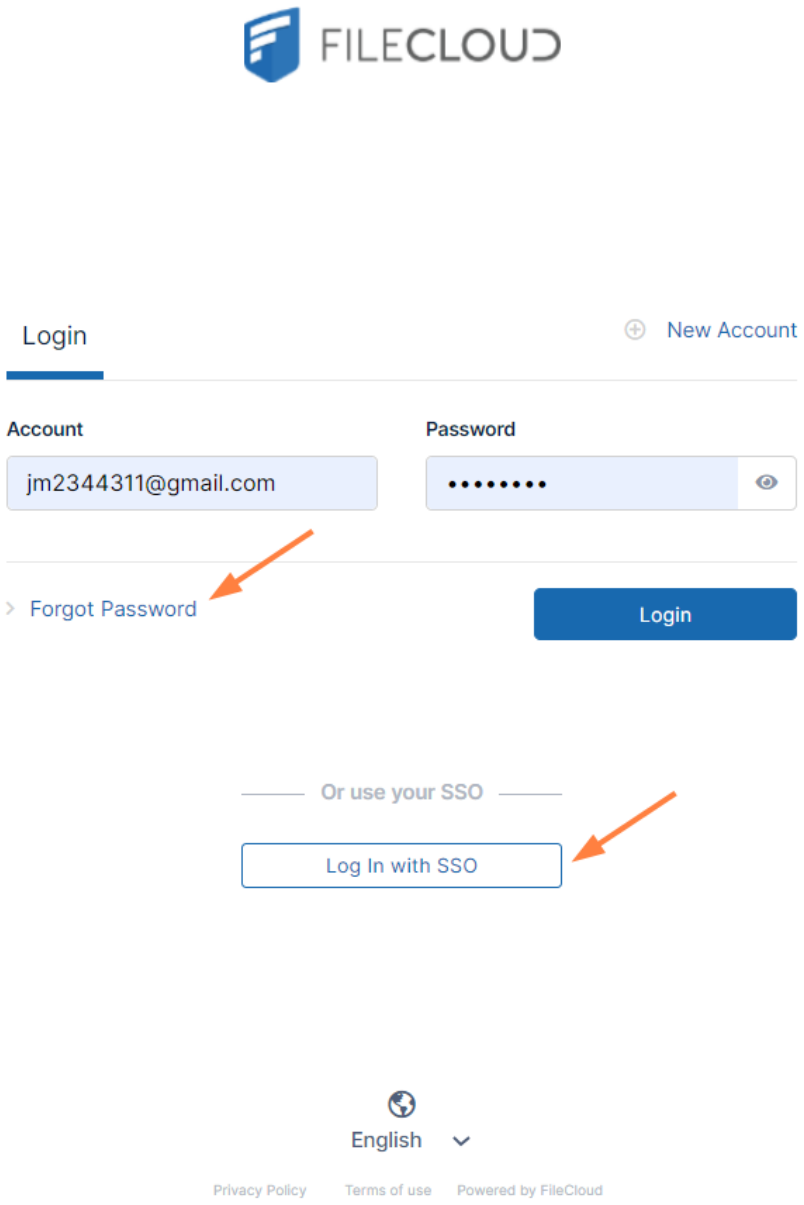
3. For help filling the remaining files on the page, see SAML Single Sign-On Support.
4. Click **Save**.

5. Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.



6. In the FileCloud user portal login page, click on the more option and access SSO. This will first redirect you to the Auth0 login page where you can authenticate as the user that you have created in Auth0.
   If that user doesn't exist in FileCloud, it will be created automatically after successful

authentication.



Integrate Microsoft Entra ID with FileCloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

Note: Microsoft Entra ID can only be integrated if FileCloud has an SSL certificate in place, as Microsoft requires HTTPS URLs when configuring FileCloud in Entra ID.

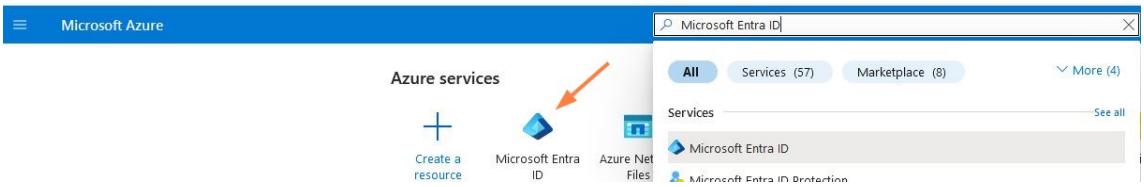
FileCloud can be integrated with Microsoft Entra ID.

- Microsoft Entra ID must be configured as an Identity Provider (IdP)
- FileCloud acts as the Service Provider (SP)
- By default, this integration does not synchronize a user's SSO groups and FileCloud groups each time a user logs in with SSO. Without synchronization, unauthorized access to content as well as improper access blocking may occur. To prevent this see **Syncing Group Changes on Every Login**, below.

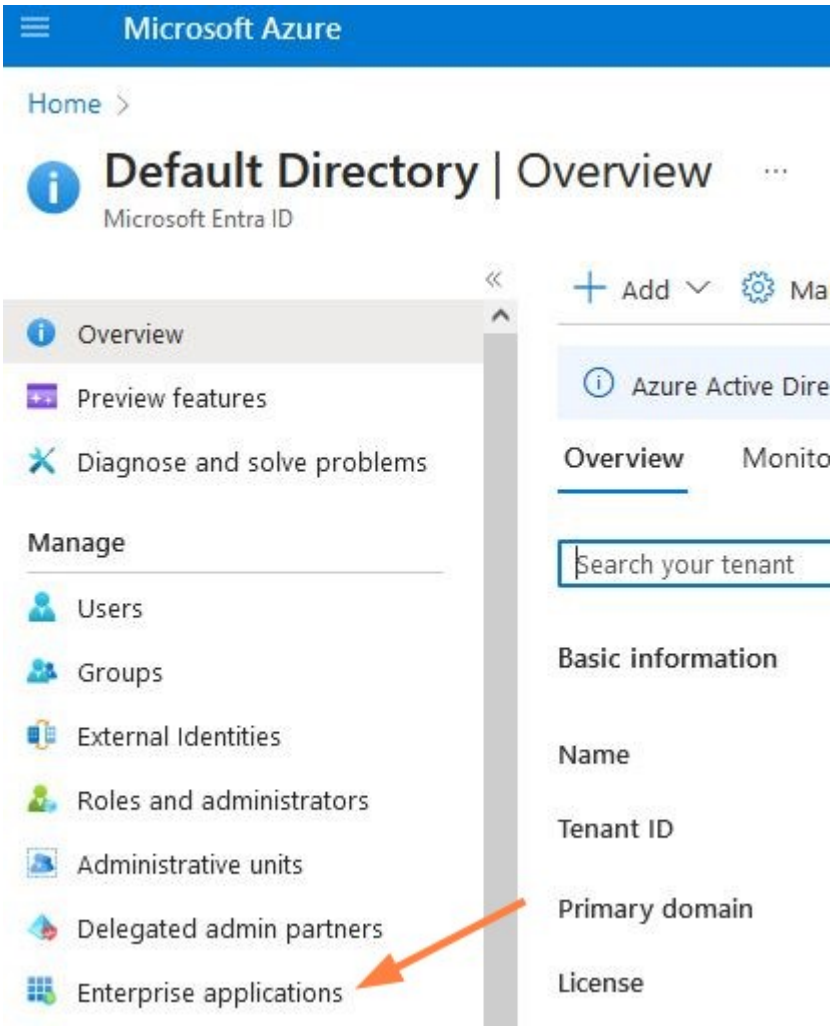
To integrate Microsoft Entra ID with FileCloud:

Log in to the Azure Portal (https://portal.azure.com).

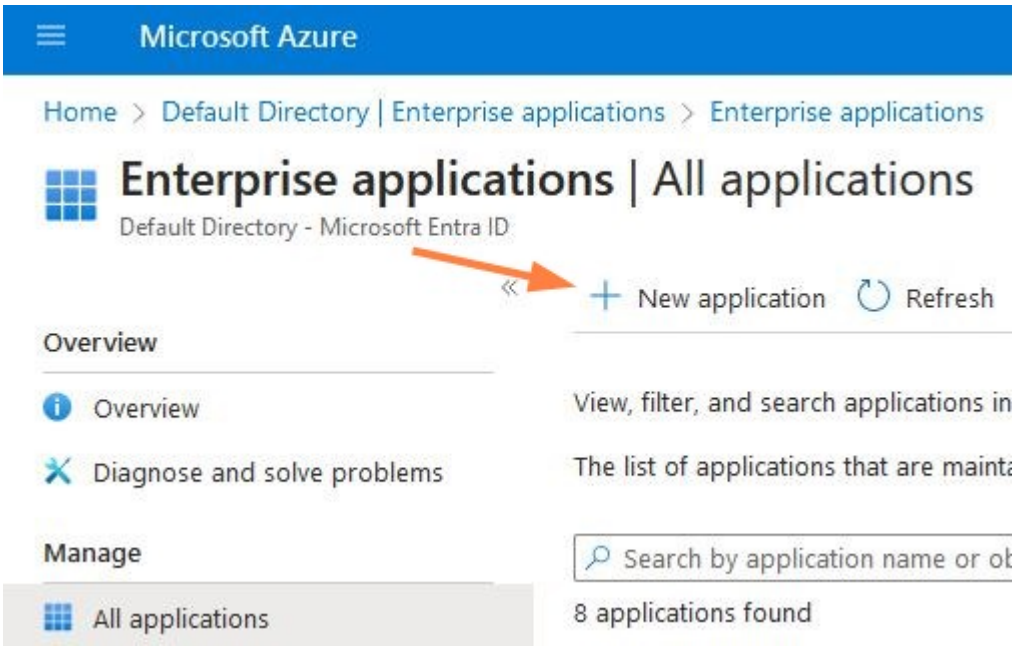
1. Search for **Microsoft Entra ID**, and then click the **Microsoft Entra ID** icon.



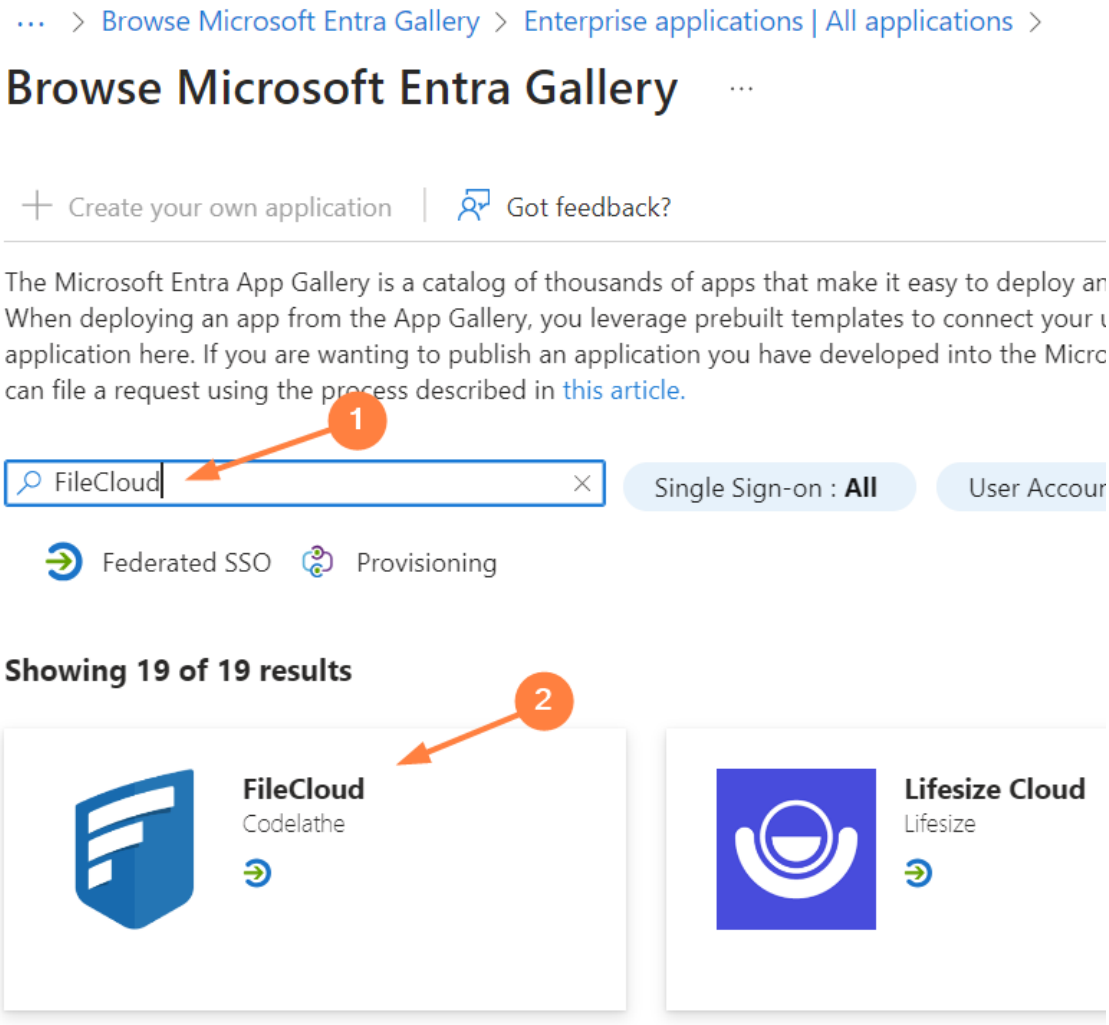
2. If you see a directory list, select the directory you want to integrate with FileCloud.
3. Select **Enterprise applications** in the left navigation menu.



4. Click **New application**.

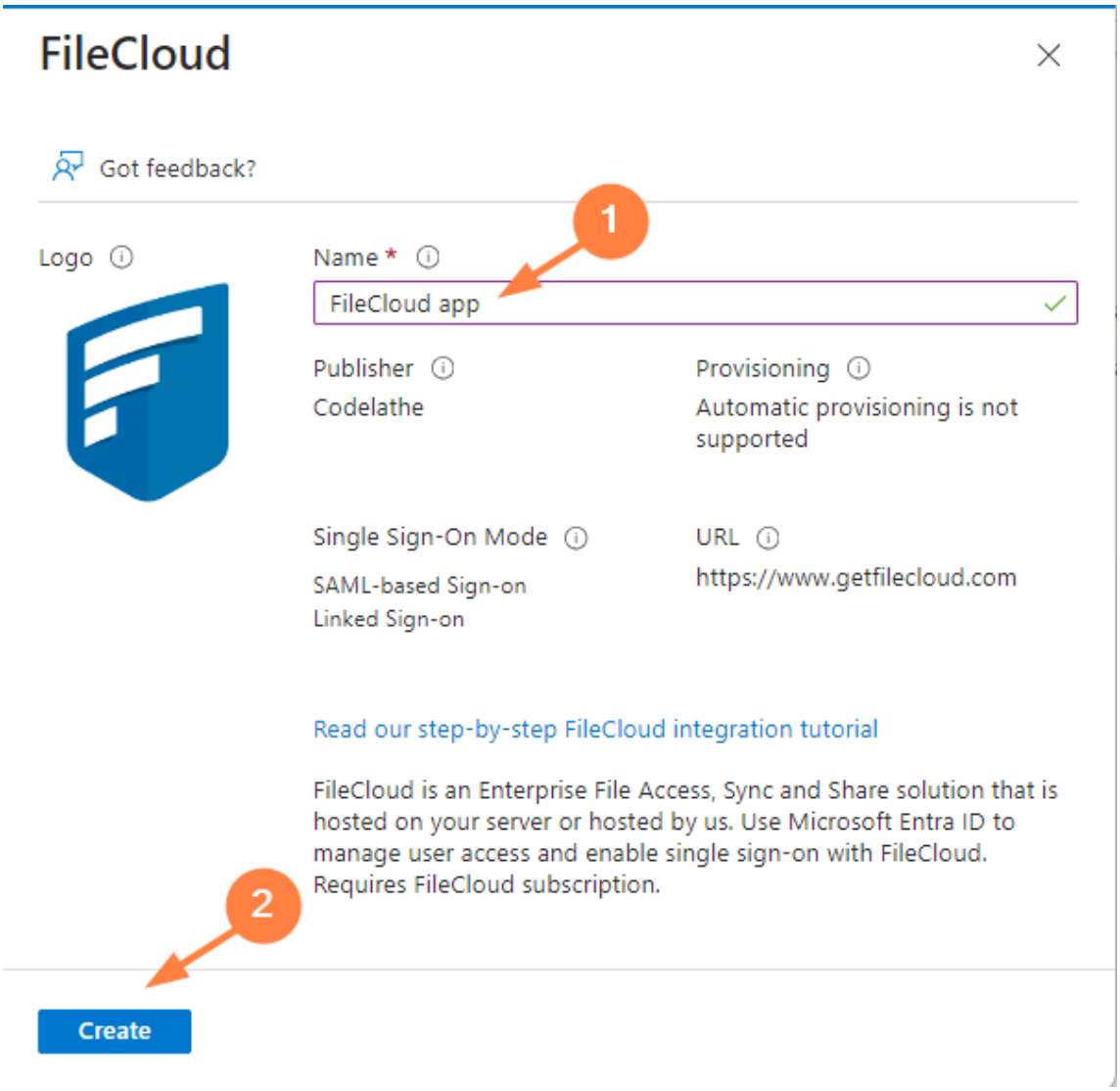


5. In the **Browse Microsoft Entra Gallery** page**,** enter **FileCloud** in the search box, and click the FileCloud icon.



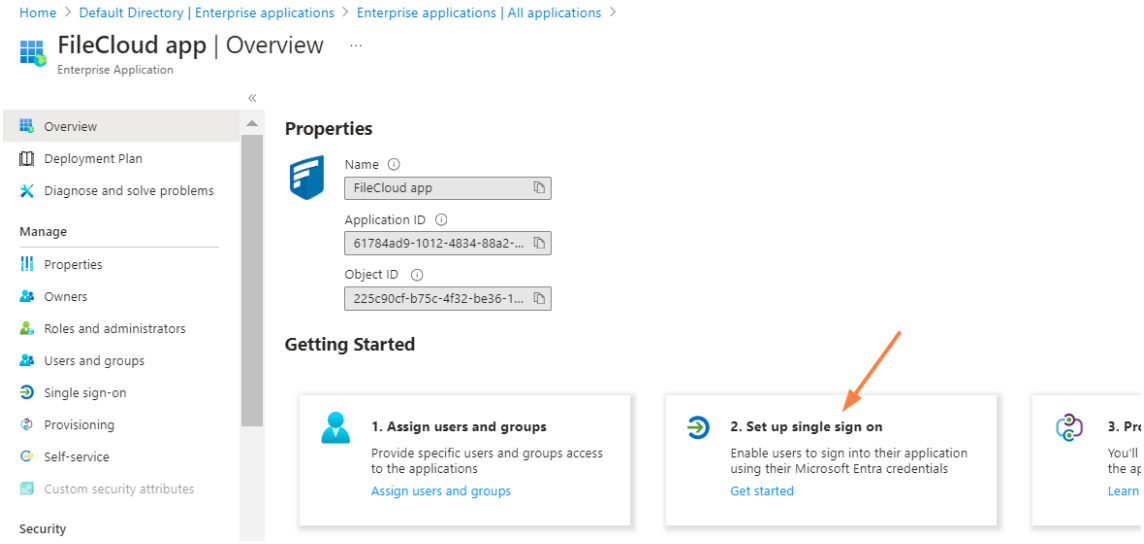
FileCloud information appears in the right panel.

6. Enter a name for your FileCloud app, and click **Create**.



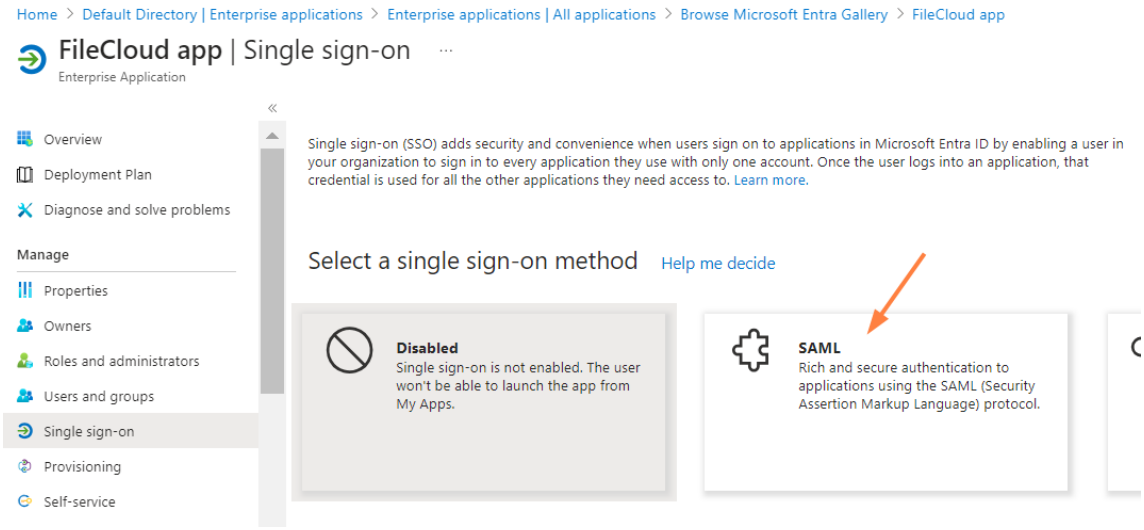
The **Overview** page for the new application opens.

7. In the **Set up single sign on** box, click **Get started**.



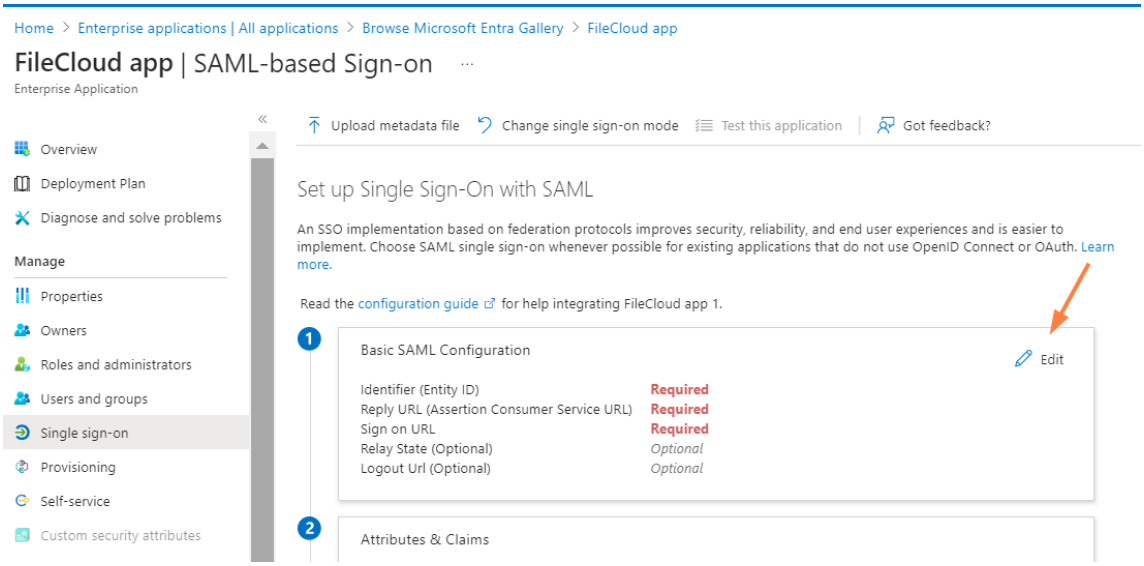
The **Single sign-on** screen opens.

8. Click **SAML**.

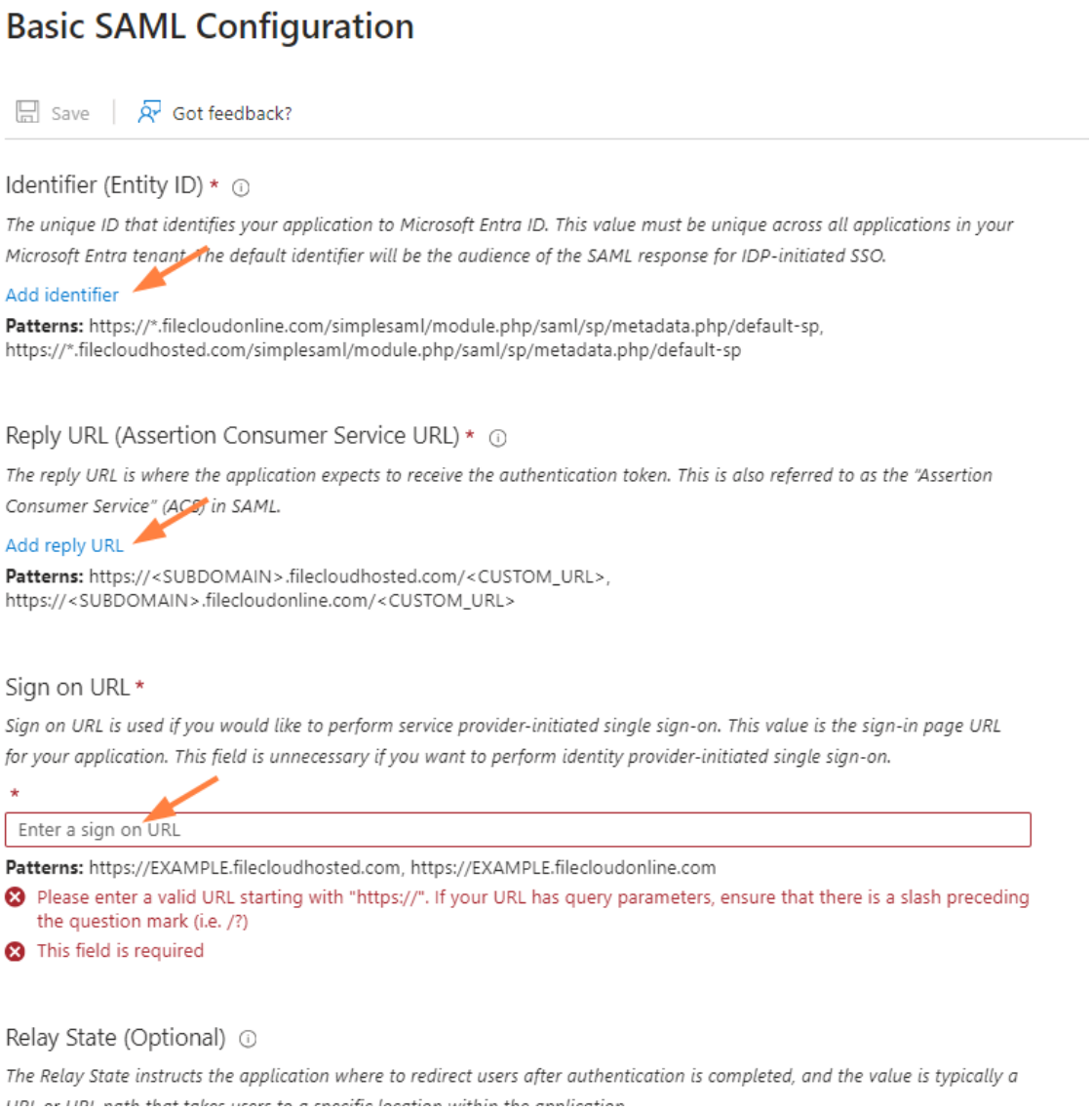


The **SAML-based Sign-on** screen opens.

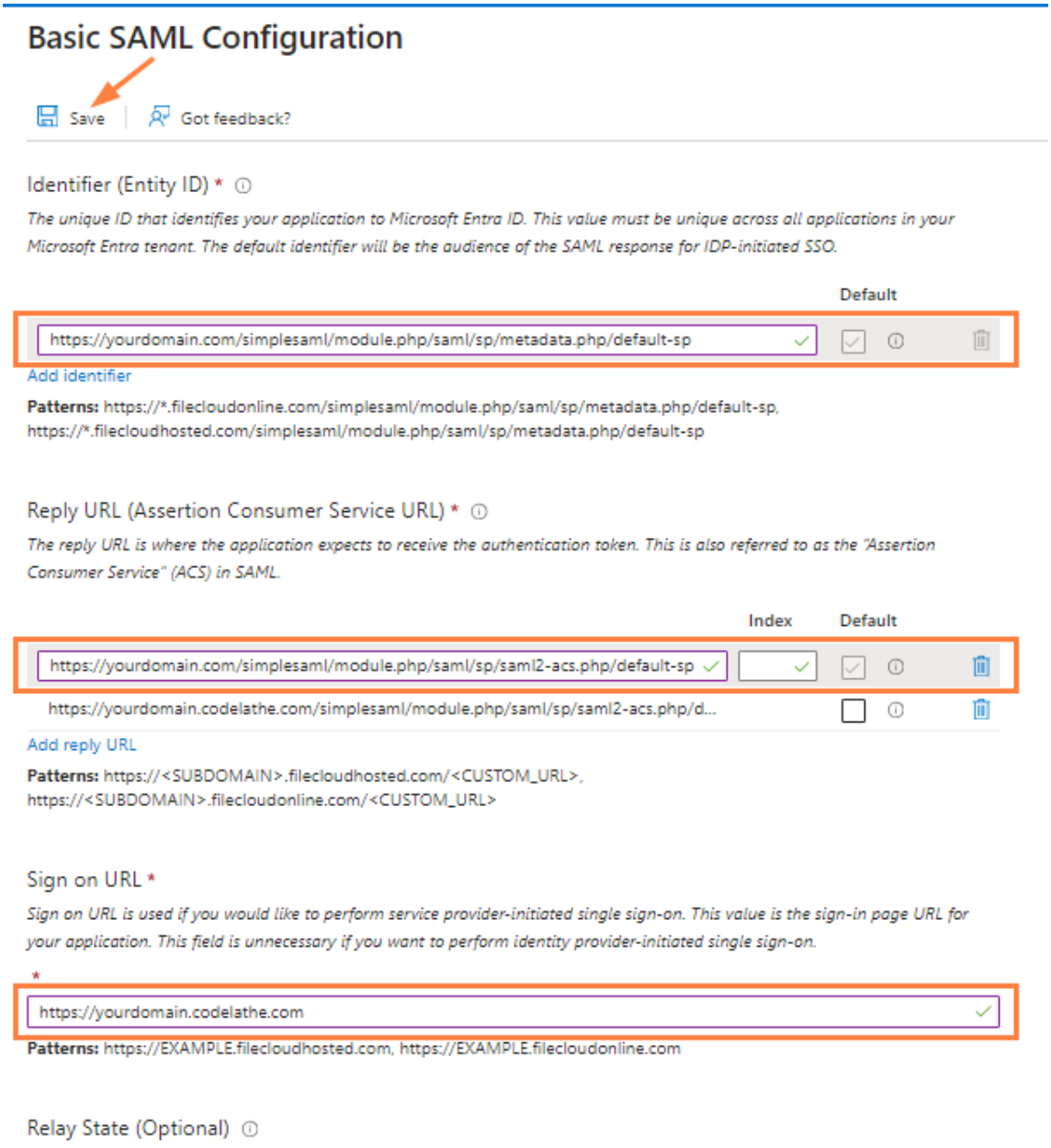
9. In the **Basic SAML Configuration** box, click **Edit**.



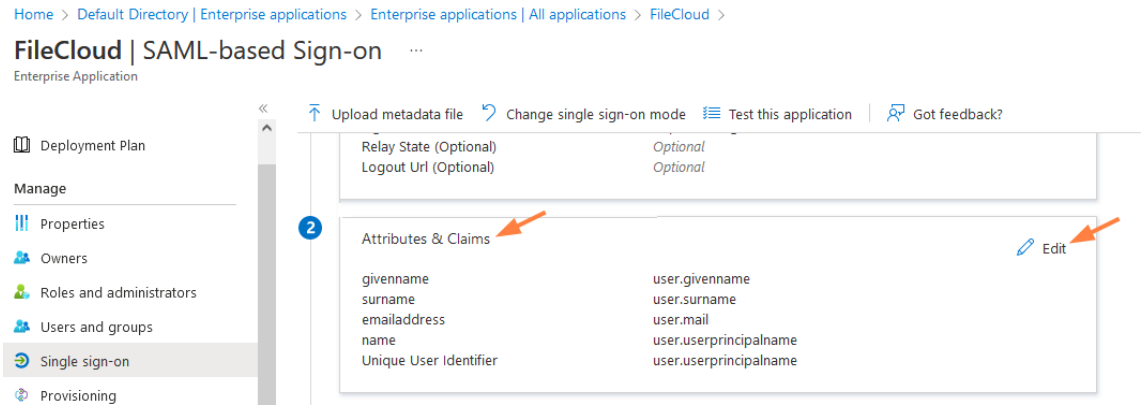
In the right panel, the **Basic SAML Configuration** form opens.



10. Enter the top three fields, **Identifier (Entity ID)**, **Reply URL**, and **Sign on URL** using your FileCloud domain, then click **Save**.
    Identifier (Entity ID) - the FileCloud SSO endpoint, for example, https://yourdomain.com/simplesaml/module.php/saml/sp/metadata.php/default-sp
    Reply URL - your FileCloud domain with the additional path indicated, https://yourdomain.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
    Sign on URL - Your FileCloud site URL, for example, https://yourdomain.com



11. Close the panel.
12. **Optional**: If you have chosen to sync FileCloud and Microsoft Entra ID groups on every login, add the **memberof** claim:
    Scroll down to **Attributes and Claims**, and click **Edit**.



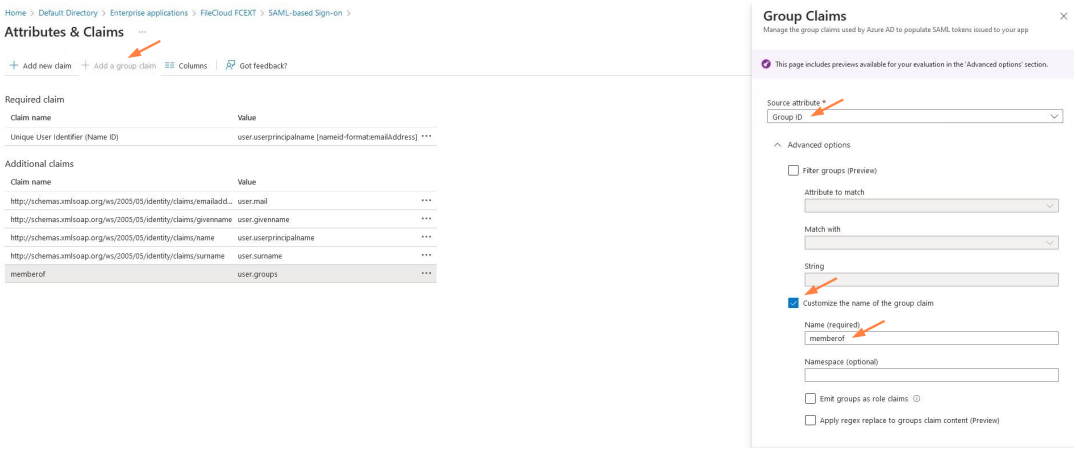
a. Click **Add a group claim.**
   A **Group Claims** form opens in the right panel.

b. In **Source attribute**, choose **Group ID**.

c. Check **Customize the name of the group claim**.

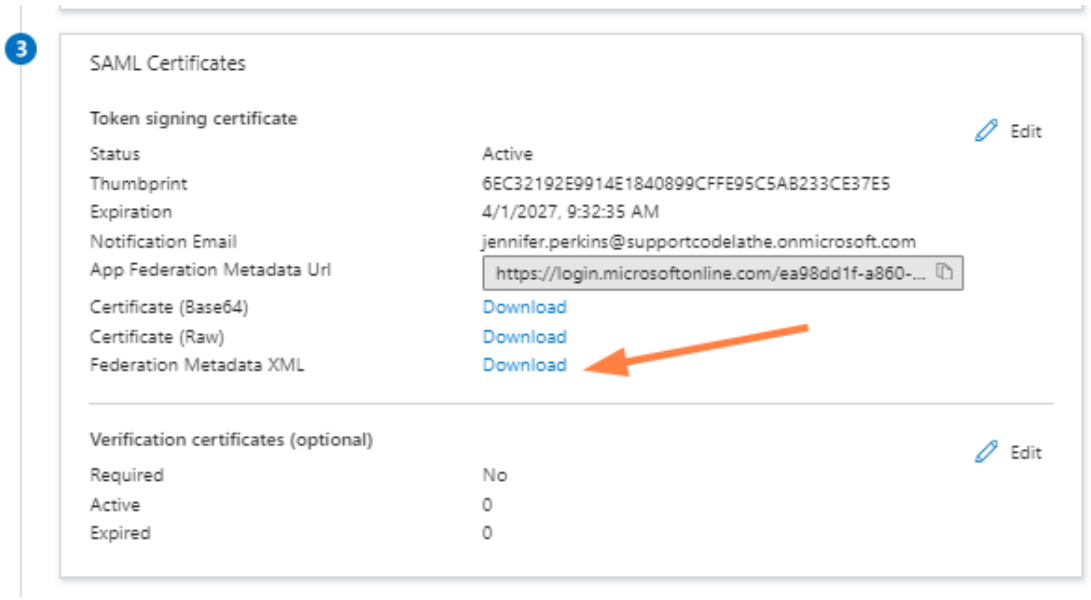
d. In **Name**, enter **memberof.**

e. Click **Save**.
   The new claim is listed under **Additional claims** with the value **user.groups**.

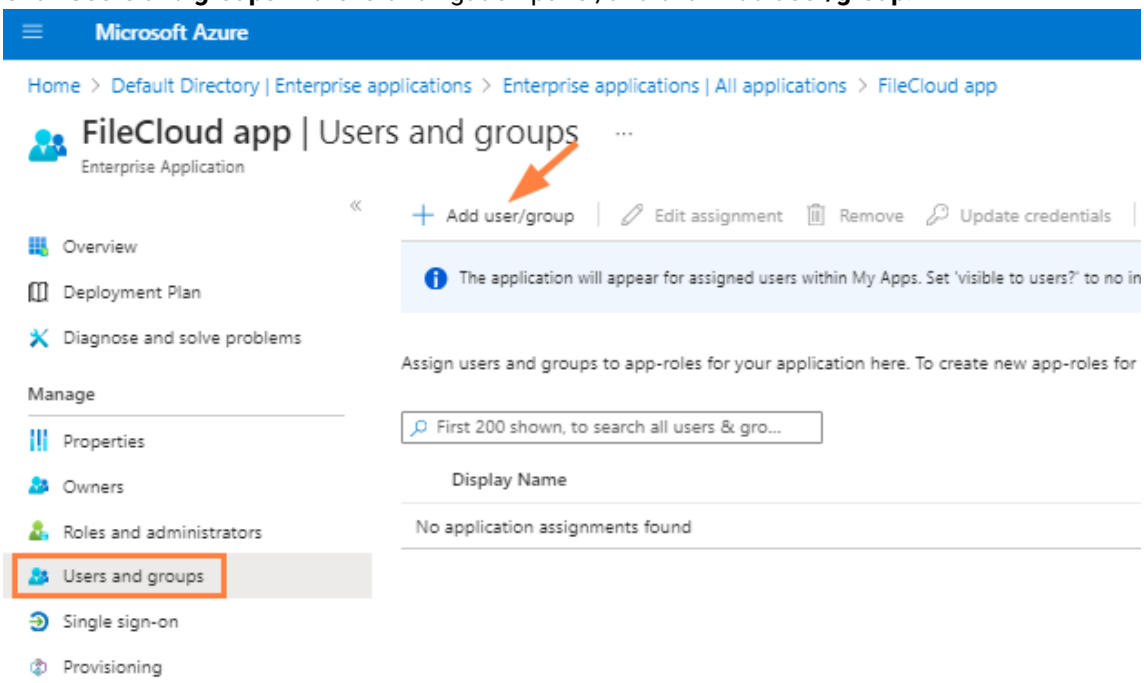


Note: To sync groups on every login, you must also complete the step in Syncing group changes on every login, below.

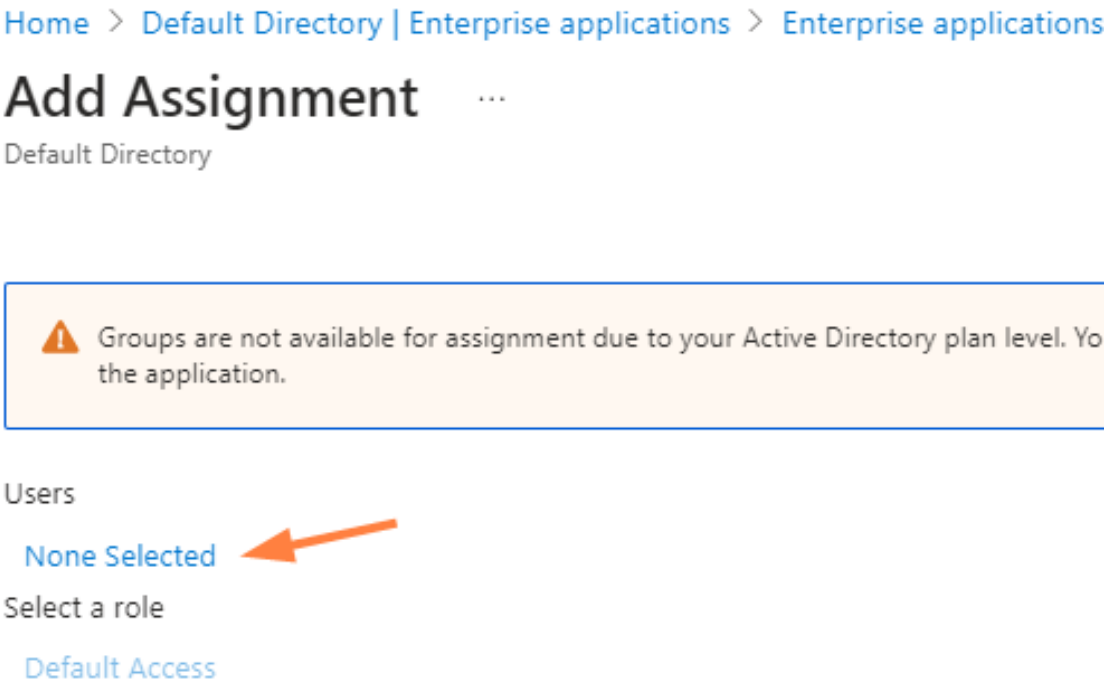
13. Scroll down to the **SAML Certificates** box.
14. Download and save the **Federation Metadata XML**.



15. Click **Users and groups** in the left navigation panel, and click **Add user/group**.

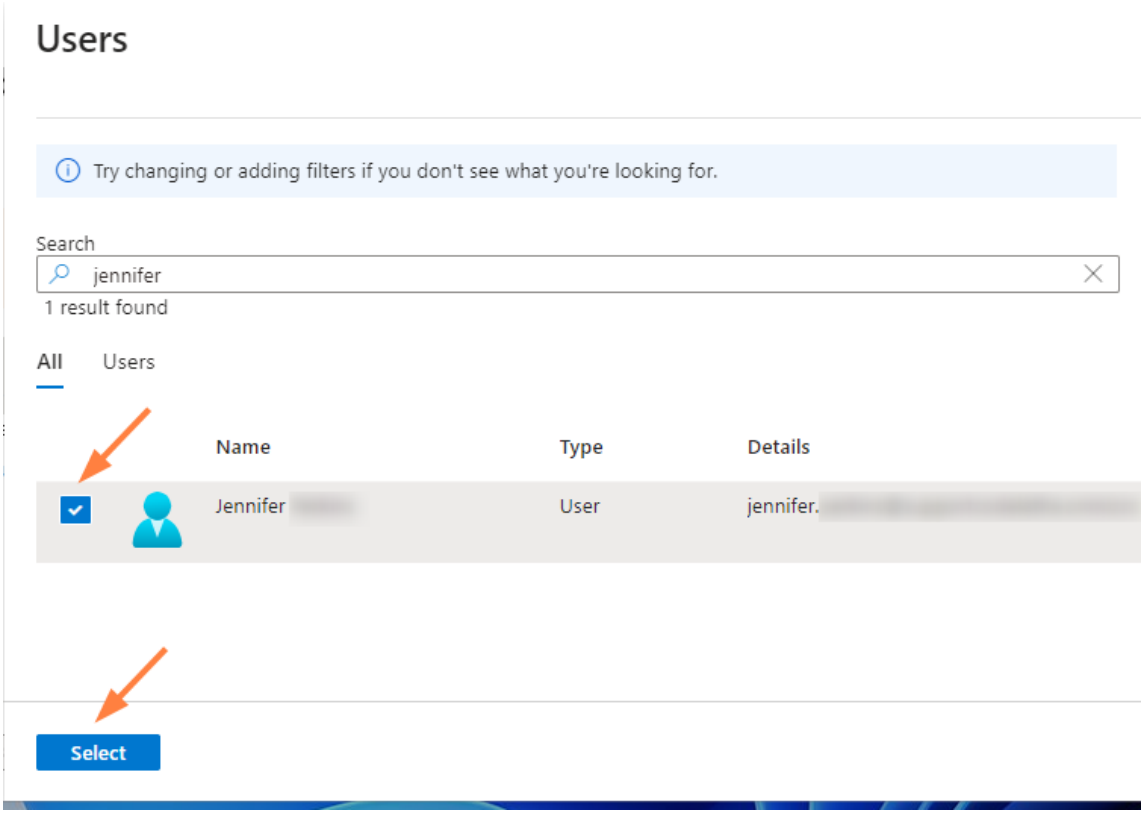


16. In the **Add Assignment** page, click the link under **Users** or **Groups** to add users and groups.

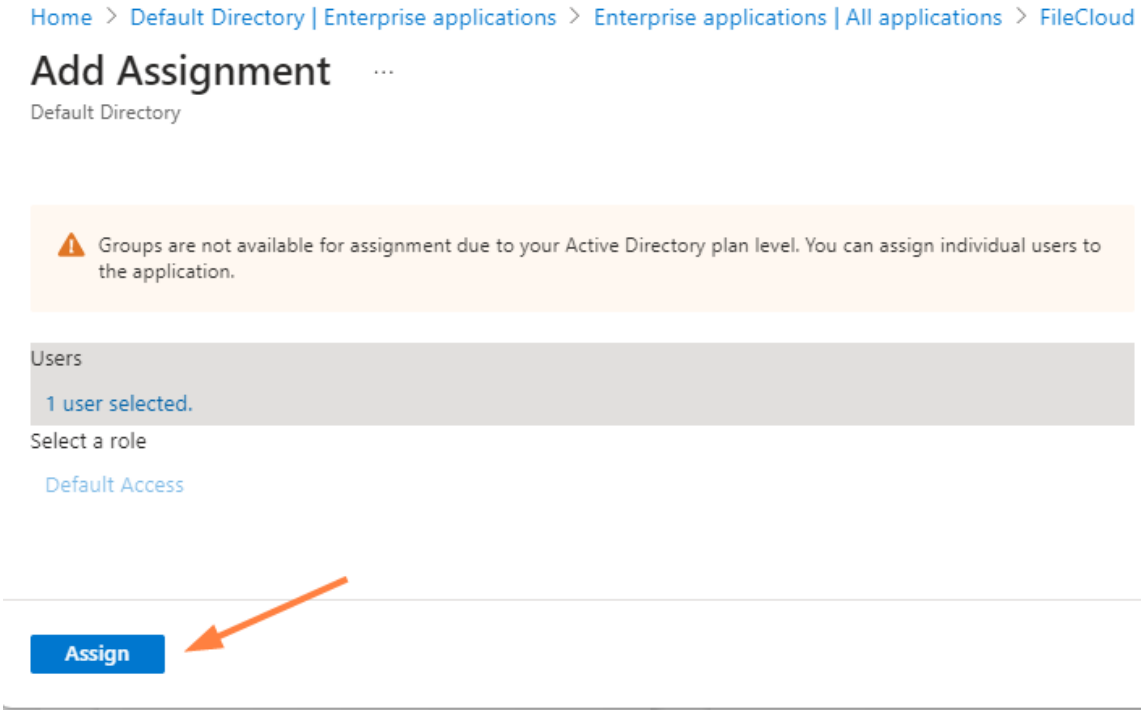


The **Users** or **Groups** page opens.

17. Search for and check the users or groups that you want to assign to the app, and choose **Select** (at the bottom of the page).



18. At the bottom of the **Add Assignment** page, click **Assign**.

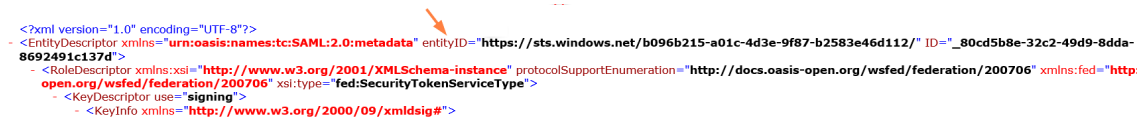


19. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** .
The **SSO** settings page opens.

20. In the **Default SSO Type** drop-down list, choose **SAML**.
21. Enter the following details:

Settings	Value
Default SSO type	SAML
IdP endpoint URL or entity ID	From the metadata XML downloaded, copy the entity ID on the first line of the XML document.
IdP username parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
IdP email parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
IdP given name (first name) parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
IdP surname (last name) parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
IdP Metadata	Copy the complete contents of the metadata XML downloaded.

To get the **IdP endpoint URL**, open your downloaded xml data and copy the **entityID** as shown in the screen shot below.



22. Save the above settings.
    This completes the Microsoft Entra ID SSO integration with FileCloud.

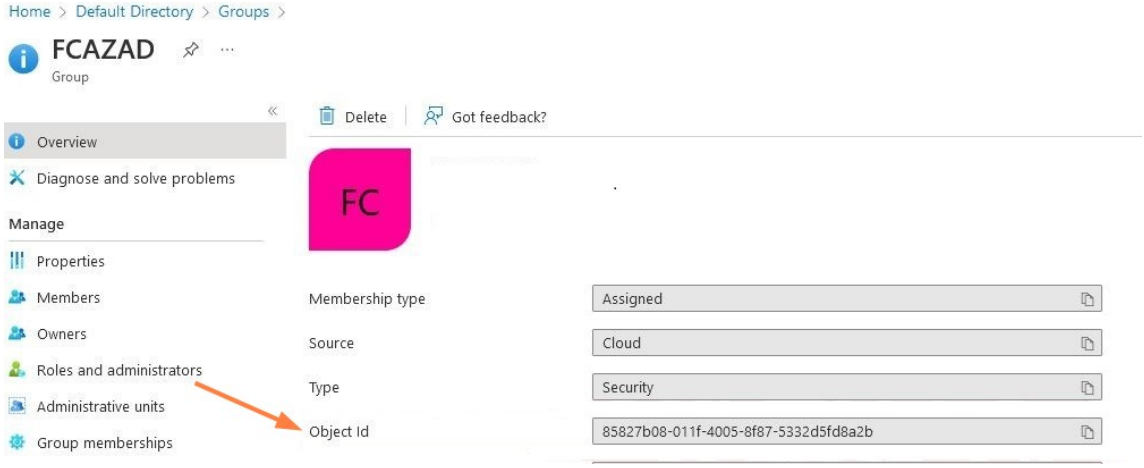
Troubleshooting failed SSO login for a member of an IdP group

An IdP group is a group of users in Microsoft Entra ID who are authorized to log in to FileCloud. When a user logs in to FileCloud with SSO using Entra ID, FileCloud automatically checks the login user's FileCloud group name to see if it is the same as the user's IdP group name. However, this fails because Entra ID can only send the **Group ID**, not the group name, to FileCloud. To fix this, add a custom claim parameter named **memberof** in Entra ID to send the group's **Object ID** (**Group ID**) to be compared with the field **Limit log in to IdP group** in FileCloud SSO settings. Since the two values are identical, the user is able to log in to FileCloud.

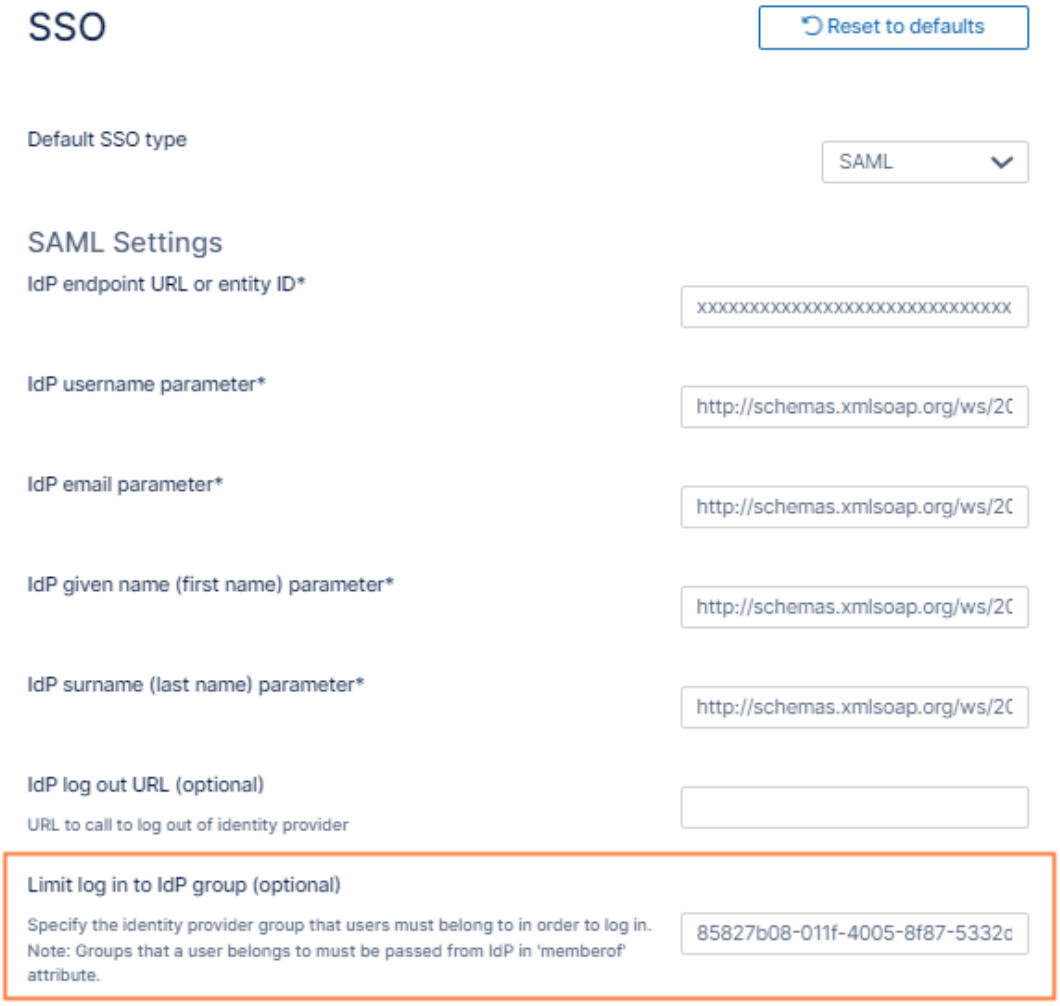
To get the group's **Object ID**, in Microsoft Entra ID:

1. Log in the the Azure portal, and in the navigation panel, click **Microsoft Entra ID**.

2. In the navigation panel, click **Groups**, and then click the **Group** to limit the login to.
3. In the **Overview** screen for the group, copy the **Object ID** field:

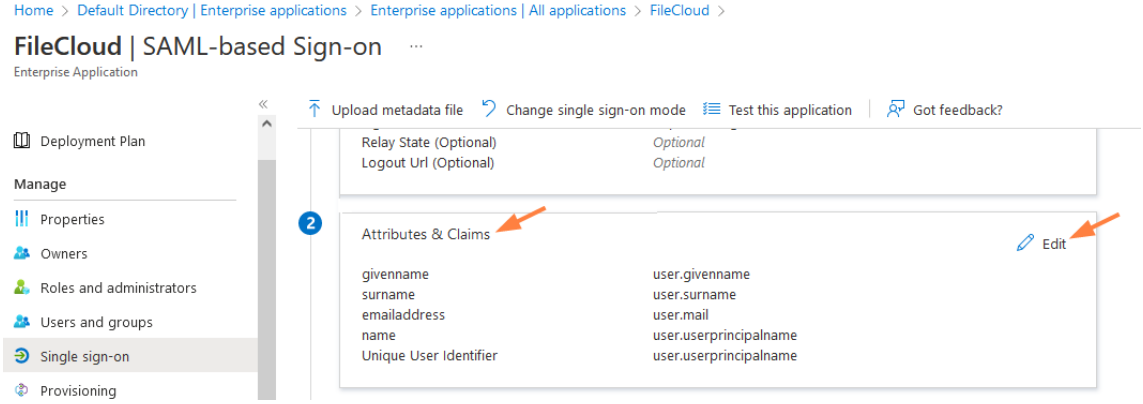


4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** .
5. In **Limit log in to IdP group**, enter the **Object Id.**

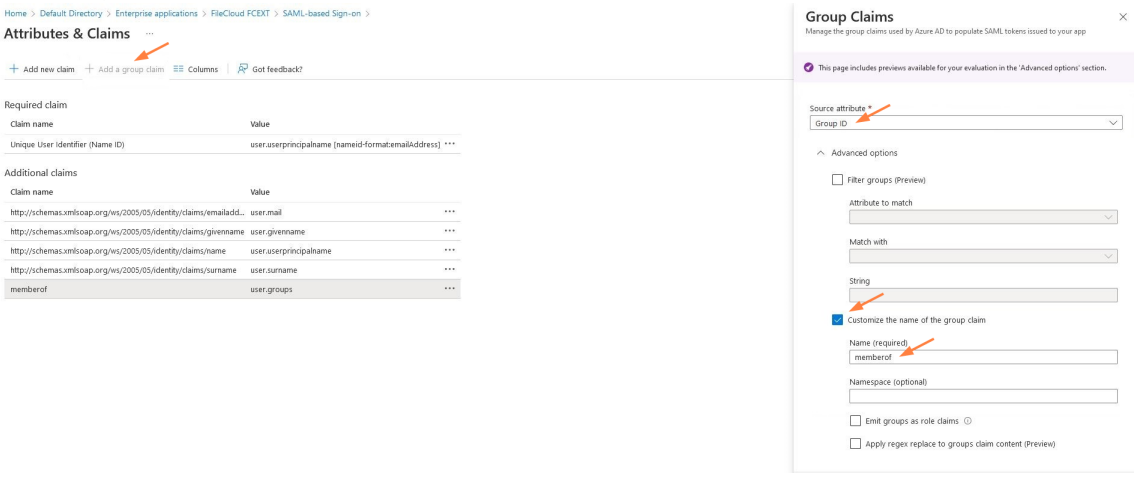


Note: If you completed optional step 12 in the procedure above, you have already completed the remaining steps in this Troubleshooting section.

6. In Microsoft Entra ID, go to the **Enterprise Applications** screen, and choose the FileCloud application.
7. In the navigation panel, click **Single sign-on**.
8. Scroll down to **Attributes and Claims**, and click **Edit**.



9. Click **Add a group claim.**
   A **Group Claims** form opens in the right panel.
10. In **Source attribute**, choose **Group ID**.
11. Check **Customize the name of the group claim**.
12. In **Name**, enter **memberof.**
13. Click **Save**.
    The new claim is listed under **Additional claims** with the value **user.groups** (which is equal to **Object Id**).



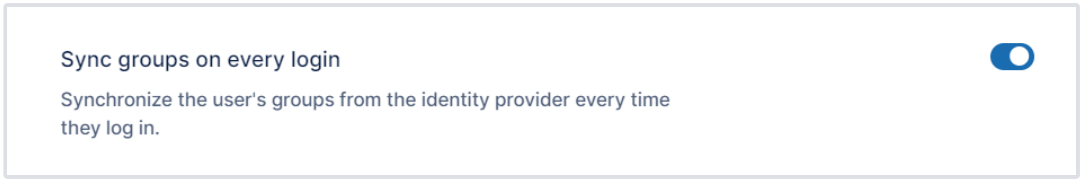
Now **memberof** will be sent to FileCloud with the value of the user group, and when FileCloud compares it with the **Idp Group**, the values match, so FileCloud will allow the login.

Syncing group changes on every login

If changes to your users' group membership may affect the content they have access to, you may sync a user's group changes each time they log into FileCloud with their SSO login.

To configure SSO login to sync groups on each login:

1. In the FileCloud admin portal, go to **Settings > SSO**.
   a. Enable the setting **Sync groups on every login**.



   b. In **IDP log out URL (optional)** enter https://login.microsoftonline.com/common/oauth2/logout



   Note: This is required, not optional for syncing groups on each login.
2. Complete Step 12 under **To integrate Microsoft Entra ID with FileCloud**, above.

Integrate Centrify with FileCloud

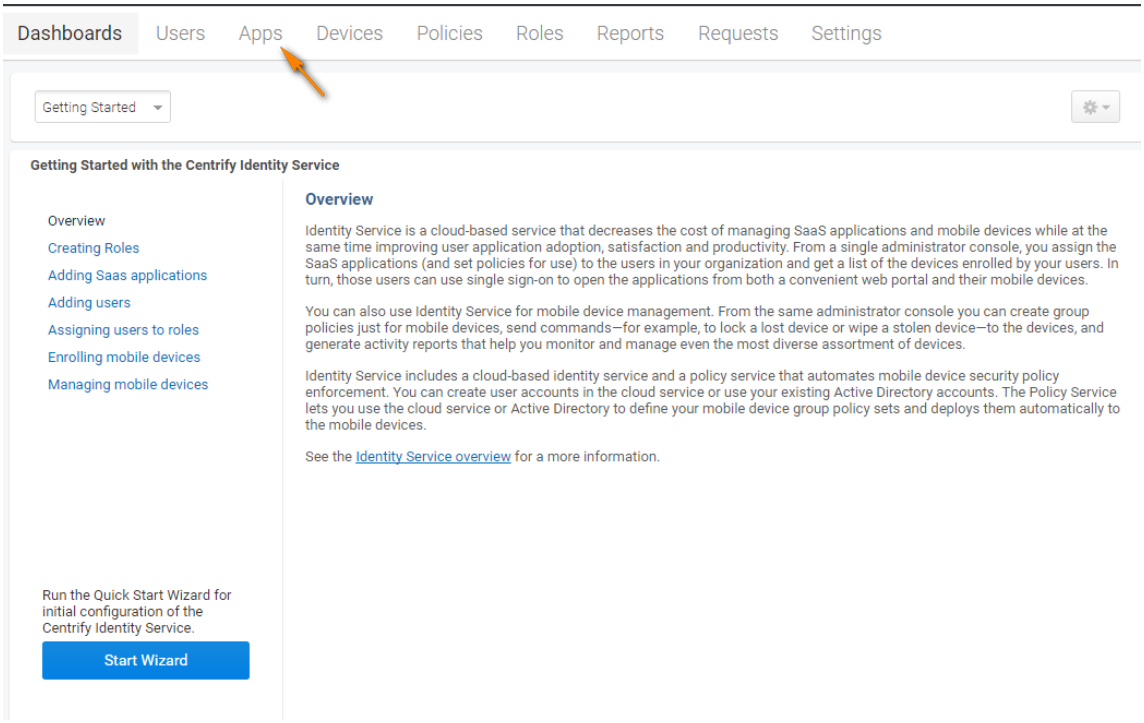
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

FileCloud can be integrated with Centrify. Centrify must be configured as an Identity Provider (IdP), and FileCloud will act as the Service Provider (SP).

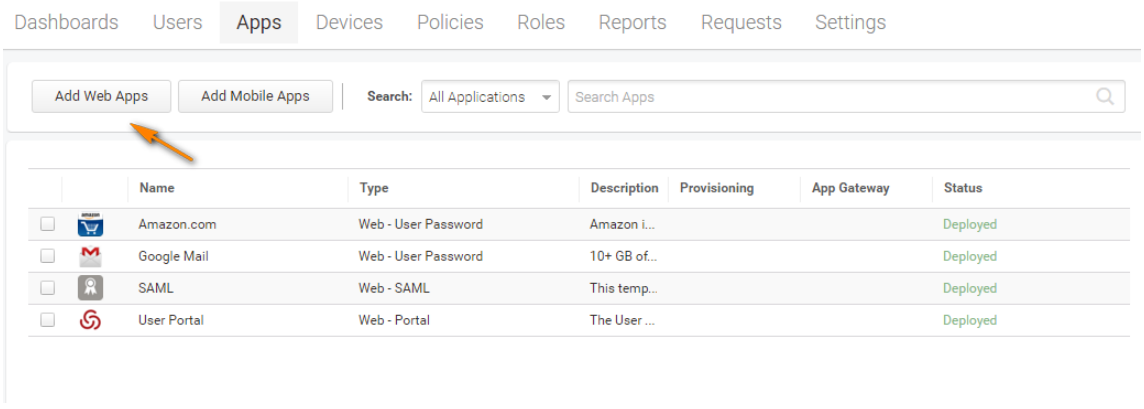
To configure FileCloud with Centrify:

PLEASE NOTE: Any reference to samldev.codelathe.com in this article should be replaced with your own FileCloud URL.

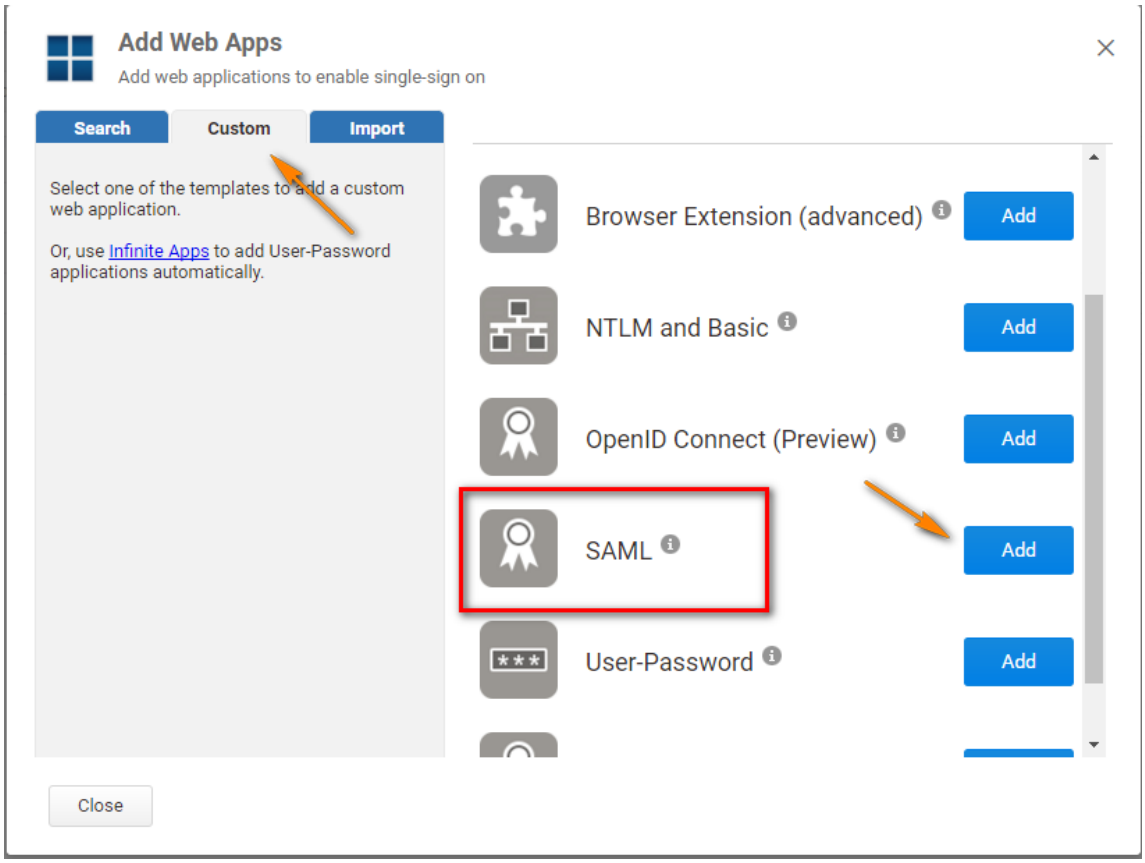
1. Log in to your Centrify issued URL.
2. After successful login to Centrify, go to the admin section and to the dashboard.
3. Create a new application as shown below.



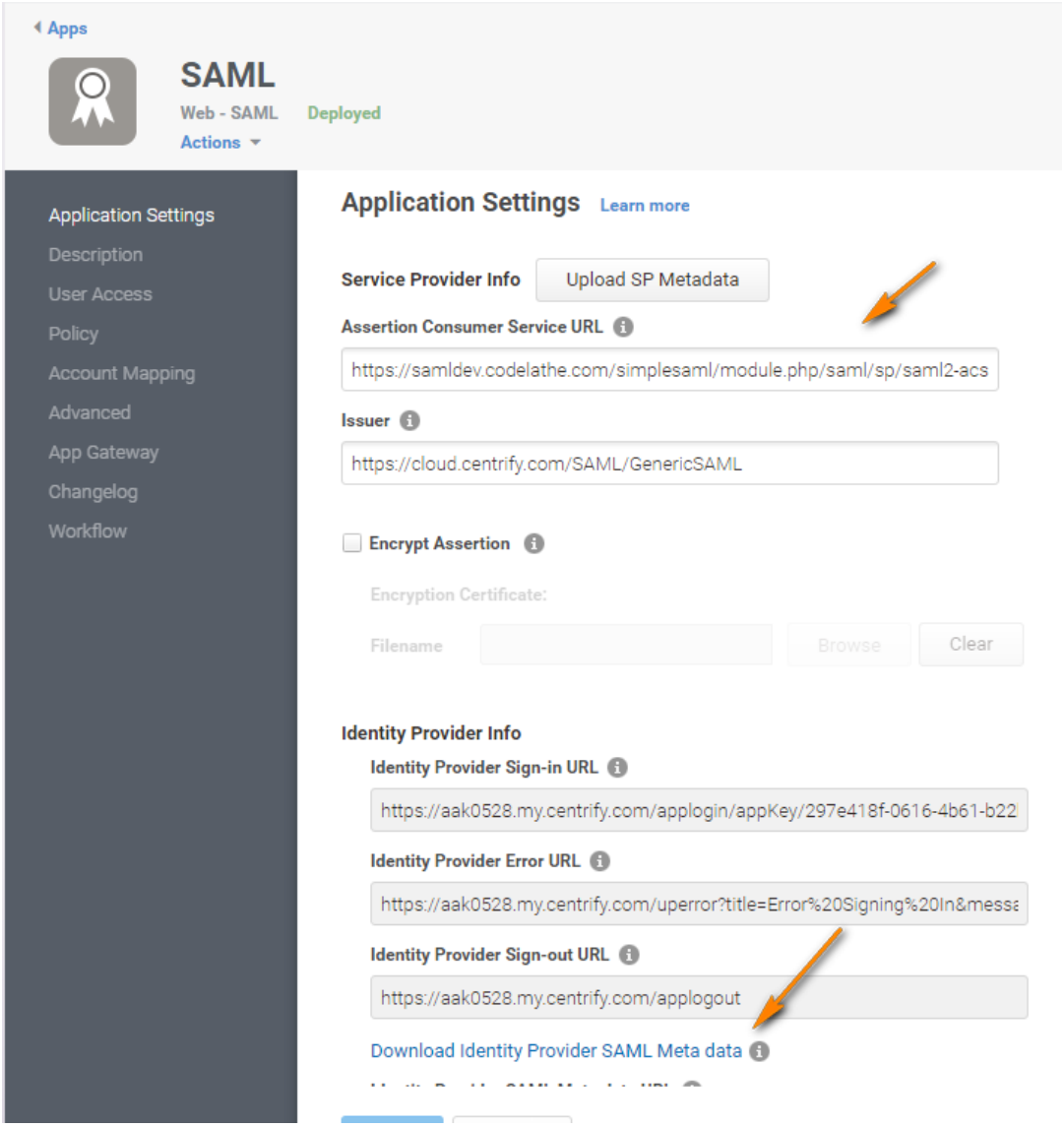
4. From the **Apps** menu, click **Add Web Apps**.



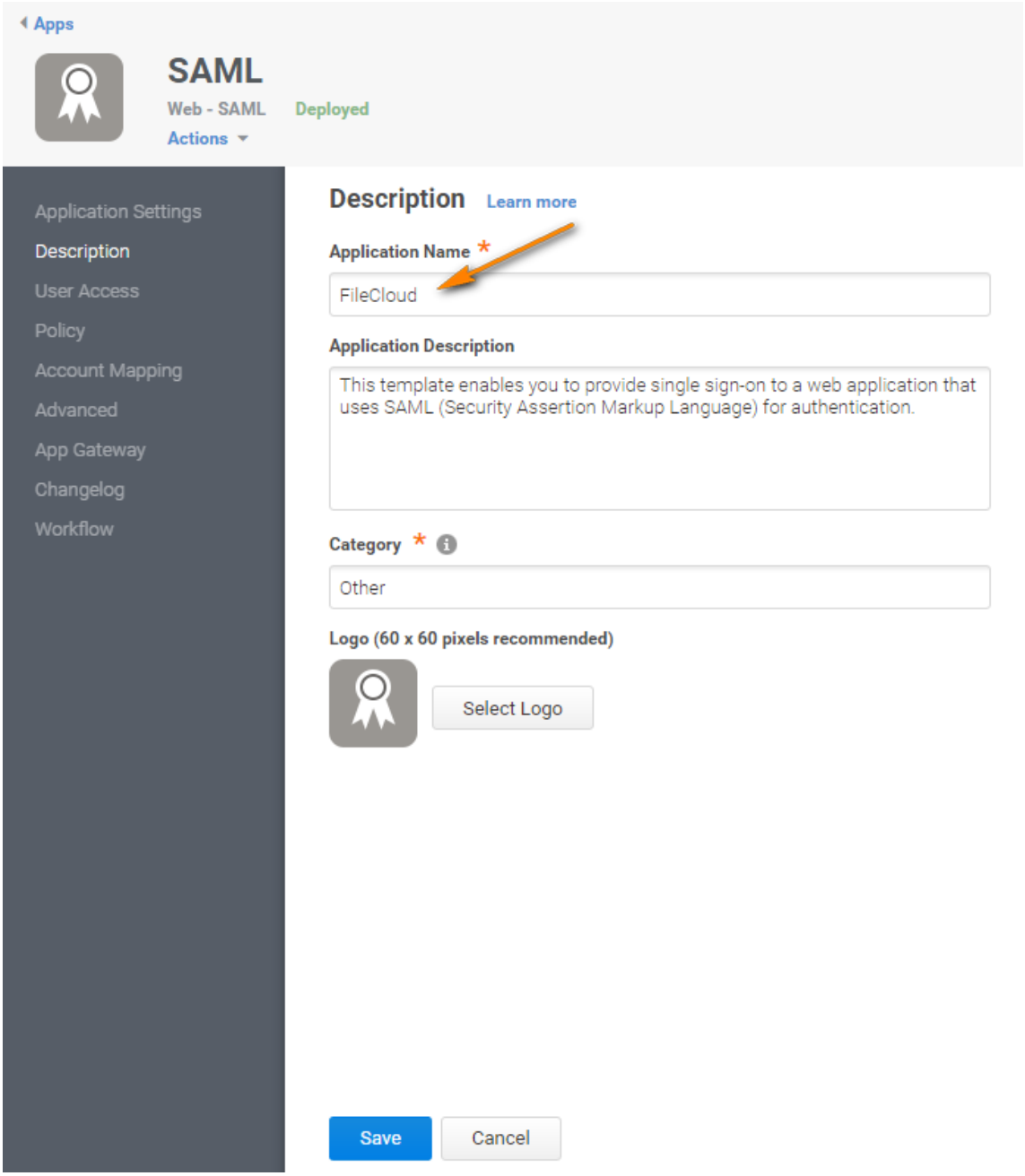
5. On the **Add Web Apps** screen, click the **Custom** tab and choose **SAML**, then click **Add**.



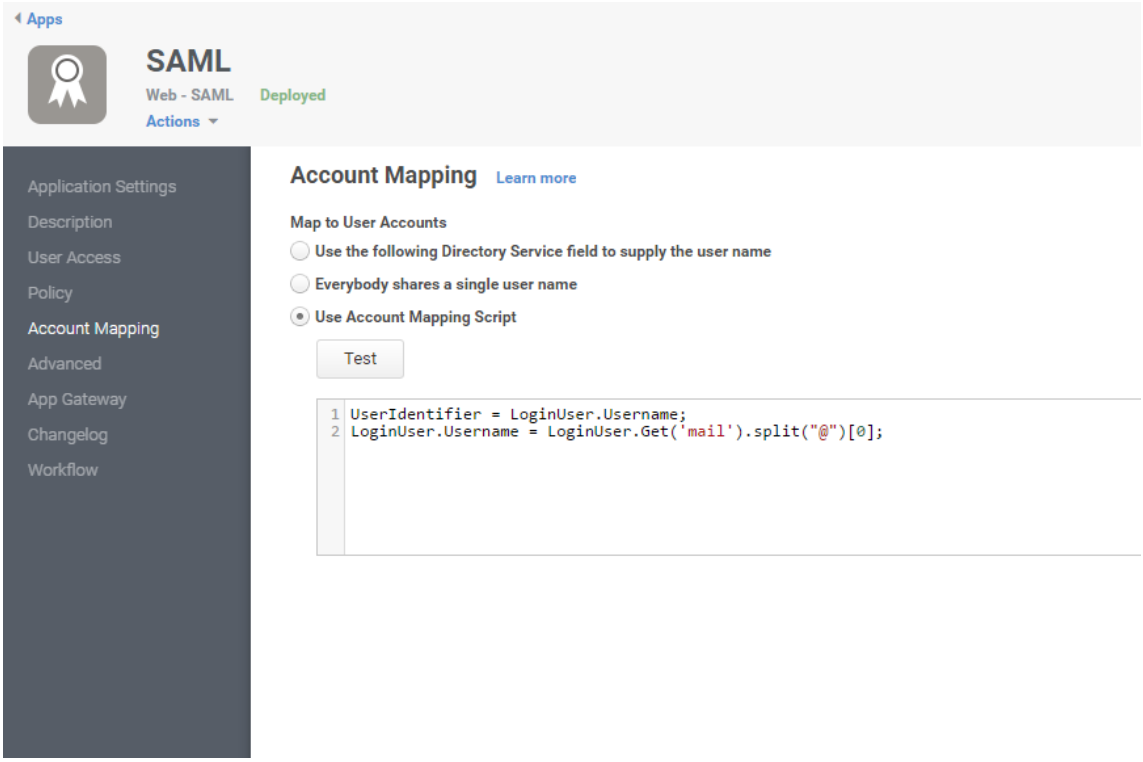
6. In the SAML Web App Screen, click **Application Settings** in the navigation panel.
7. In **Assertion Consumer Service URL** enter the FileCloud assertion URL **http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp**
8. Download the **Identity Provider SAML Metadata** as shown below. Get the details for configuring FileCloud on this screen in the FileCloud admin portal on the **Settings > SSO** tab.
    a. The Identity Provider Single Sign On URL must match the **Issuer** URL in the screenshot below.
    b. The metadata downloaded from this screen must match the **IdP Metadata** in the FileCloud admin portal on the **Settings > SSO** tab.



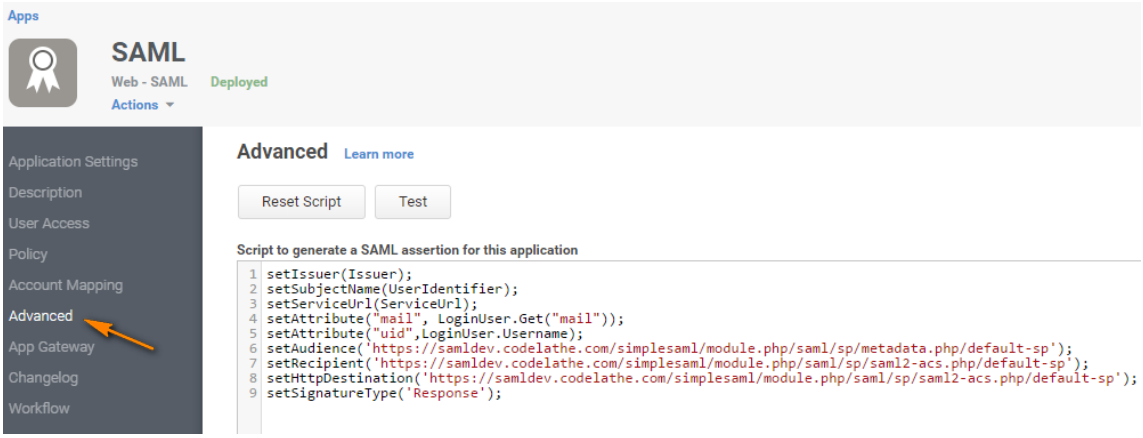
9. In the SAML Web App Screen, click **Description** in the navigation panel.
10. Add the **Application Name** and **Application Description**.



11. In the SAML Web App Screen, click **Account Mapping** in the navigation panel.
12. Select **Use Account Mapping Script** as shown below. This enables you to use your email as your username.

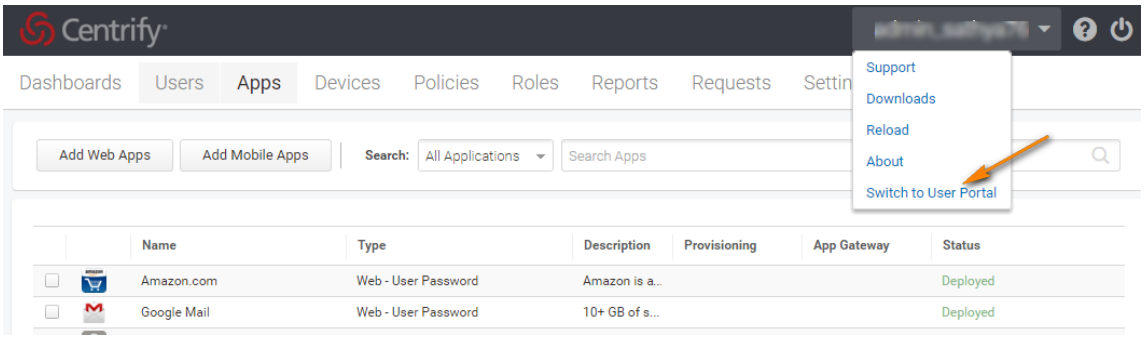


13. In the SAML Web App Screen, click **Advanced** in the navigation panel.
14. Add the script as follows:

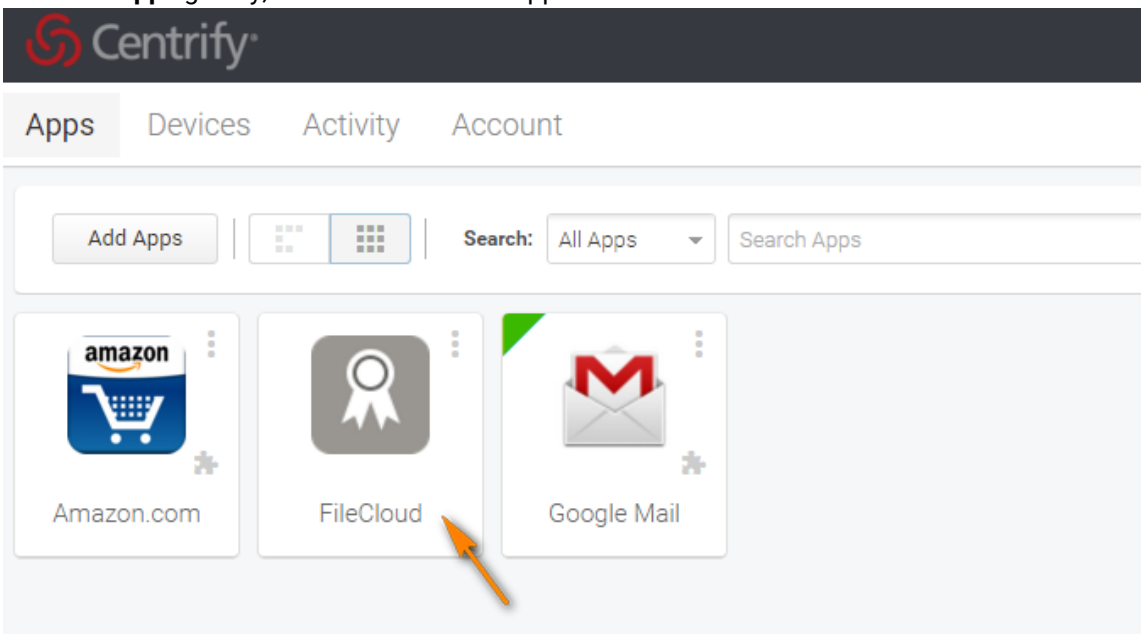


The configuration is now complete.

15. Choose **Switch to User Portal** and click **Apps**.



16. From the **Apps** gallery, select the FileCloud app.



From the FileCloud login screen, you can now select Single Sign-On to log in through Centrify.

Integrate CYBERARK with FileCloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator, you can integrate CYBERARK SSO via SAML into FileCloud. Once integrated your users will be able to access FileCloud with their CYBERARK credentials.

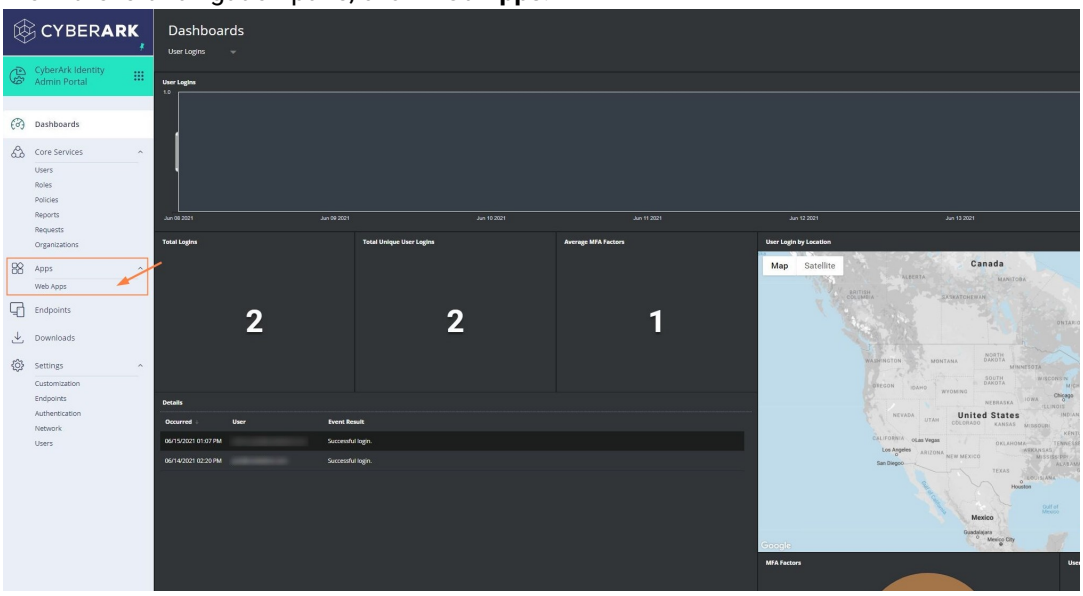
CYBERARK	CYBERARK is a cloud-based platform • Manage privileged accounts and credentials • Secure workforce and customer identities • Secure and manage access for applications and other non-human identities

In this integration scenario:

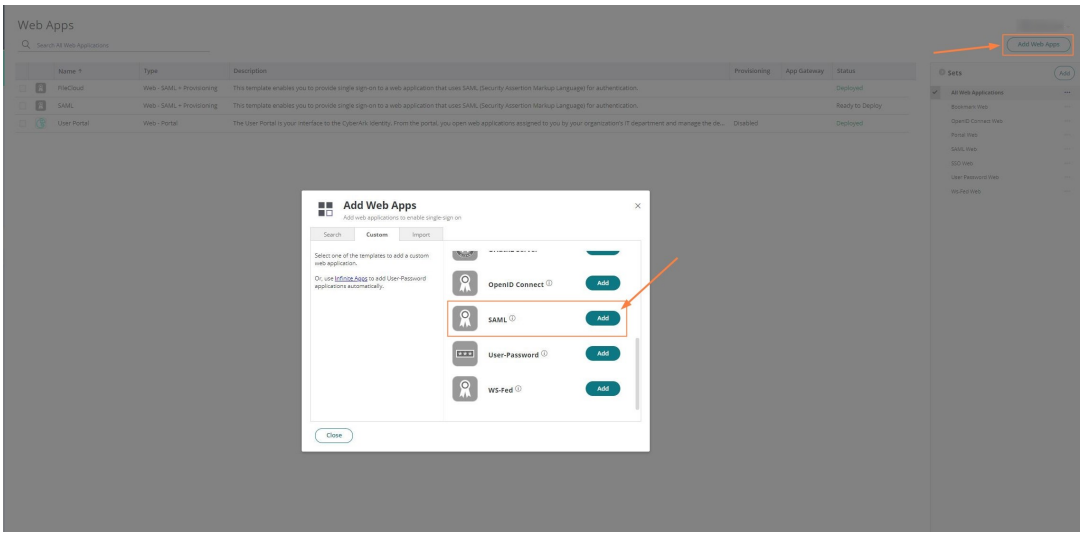
- CYBERARK must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

Configure FileCloud with CYBERARK

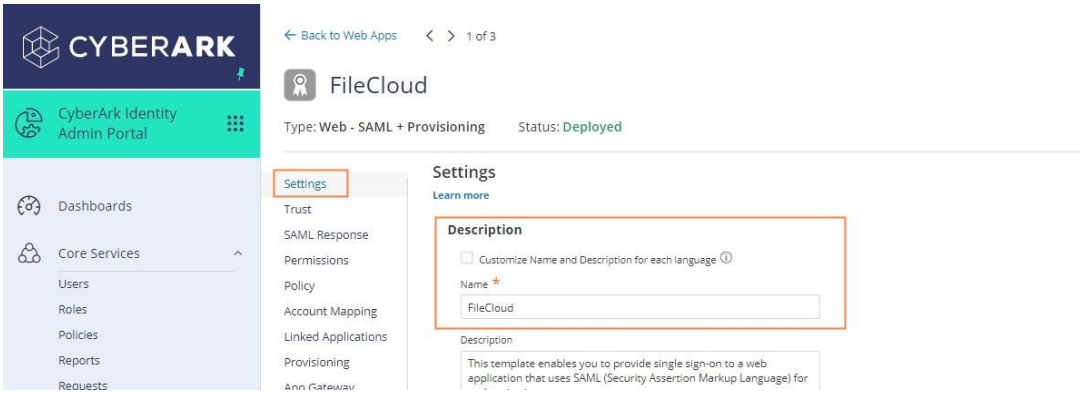
1. In CYBERARK, create a new web app.
   a. Open a browser and log in to your CYBERARK admin portal.
   b. From the left navigation pane, click **Web Apps**.



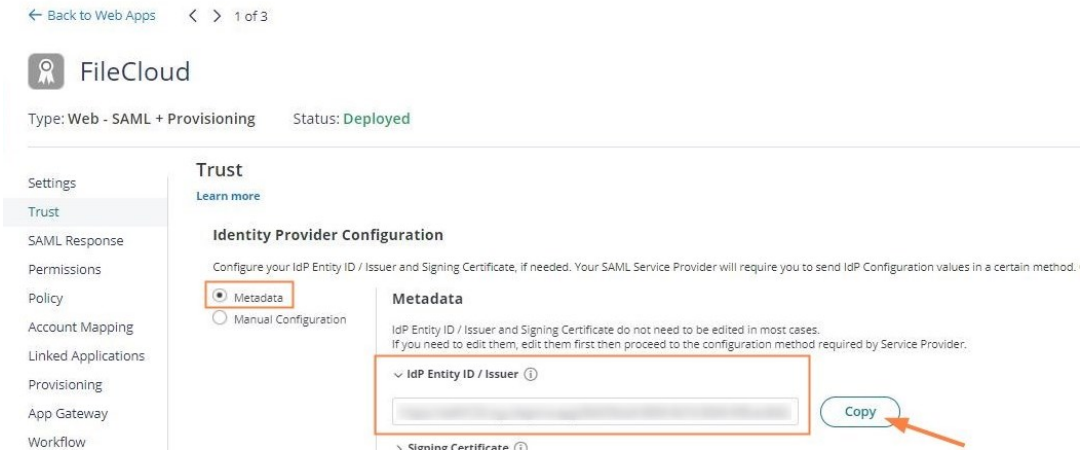
   c. On the Web Apps screen, in the top right corner, click **Add Web Apps**.
   d. In the **Add Web Apps** popup, select the **Custom** tab and scroll down until you find **SAML**, and click **Add**. A confirmation panel may appear. Click **Yes**, and then close to access the added SAML Web App.



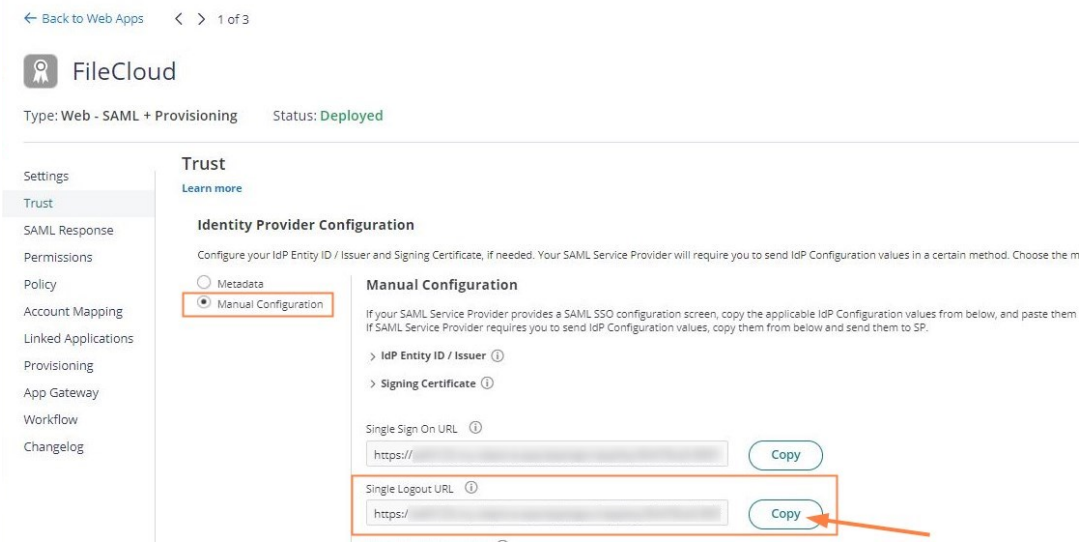
2. In CYBERARK, configure the added SAML Web App.
   a. Click **Settings** in the navigation panel. In **Description**, enter a meaningful name such as FileCloud SSO. Click **Save** at the bottom-center of the screen.



   b. Click **Trust** in the navigation panel, and download the metadata file.
   c. Under **Identity Provider Configuration**, expand **IdP Entity ID /Issuer** and copy the URL into a notepad.

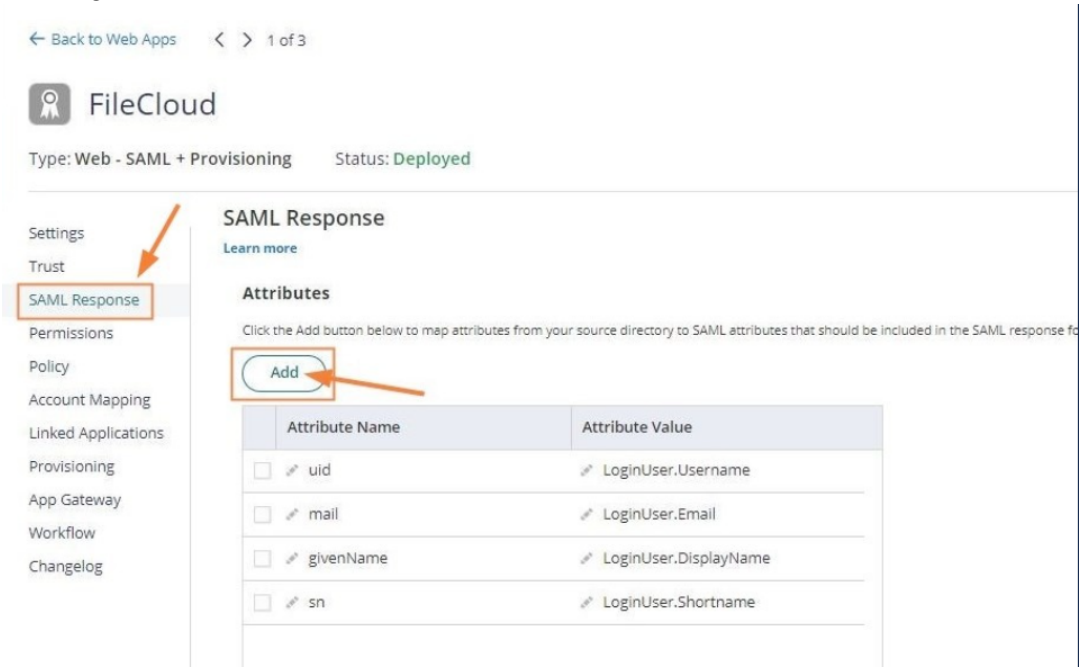


d. Select **Manual Configuration**, and copy the **Single Logout URL** into a notepad as it will be used in the next steps.



e. Access the **SAML Response** tab in the navigation panel, and add the following attribute values:

uid = LoginUser.Username
mail = LoginUser.Email
givenName = LoginUser.DisplayName
sn = LoginUser.Shortname



3. Export the metadata file into FileCloud and configure SSO.

a. Configure Apache Webserver

b. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** UNKNOWN ATTACHMENT.
The **SSO** page opens.

   i. Configure the following attributes:
   IdP Username Parameter = uid
   IdP Email Parameter = mail
   IdP Given Name Parameter = givenName
   IdP Surname Parameter = sn

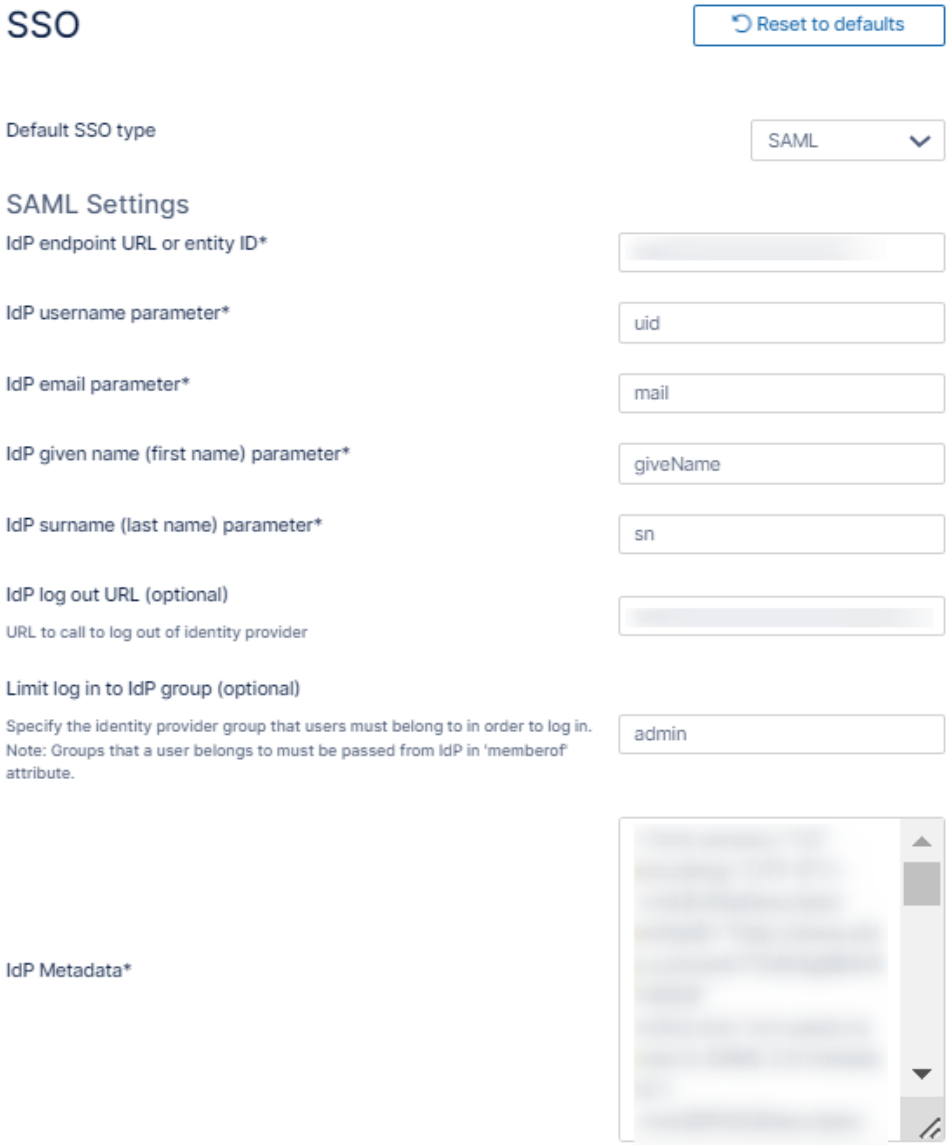
   ii. Paste the **Single Logout URL** copied in step 2d into **IdP Log Out URL** (Optional)

   iii. Paste the **IdP Entity ID/Issuer URL** copied in step 2c into **Idp Endpoint URL or EntityID**

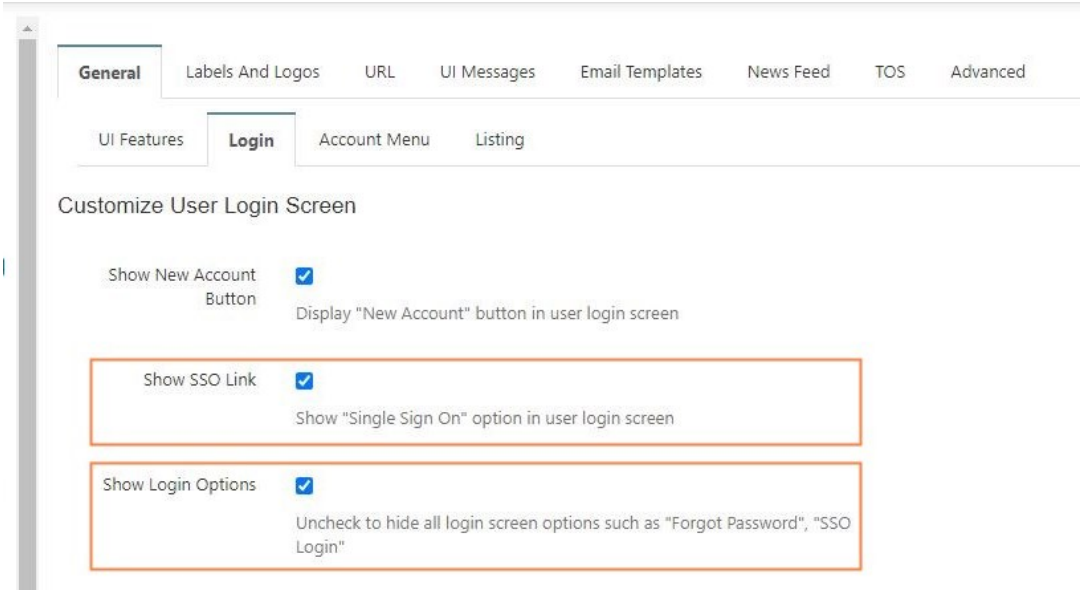
   iv. Open the metadata file downloaded in step 2b, and copy its content into **IdP Metadata**.

   v. Fill in the other settings on the page as shown in SAML Single Sign-On Support.

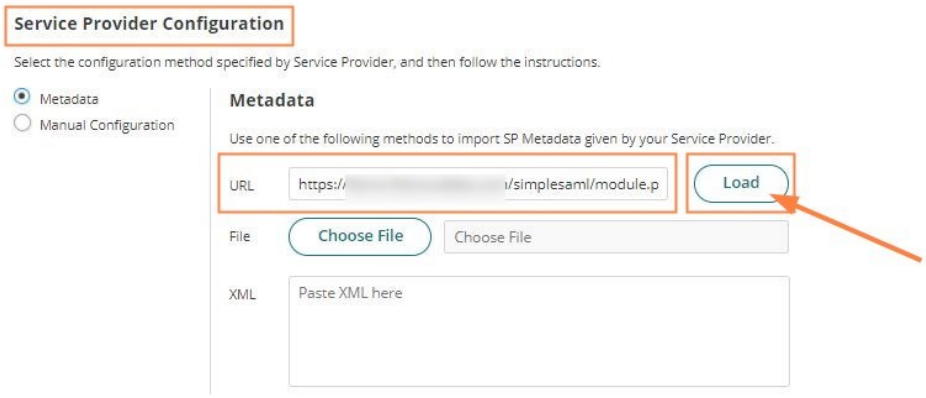
   vi. Click **Save**.



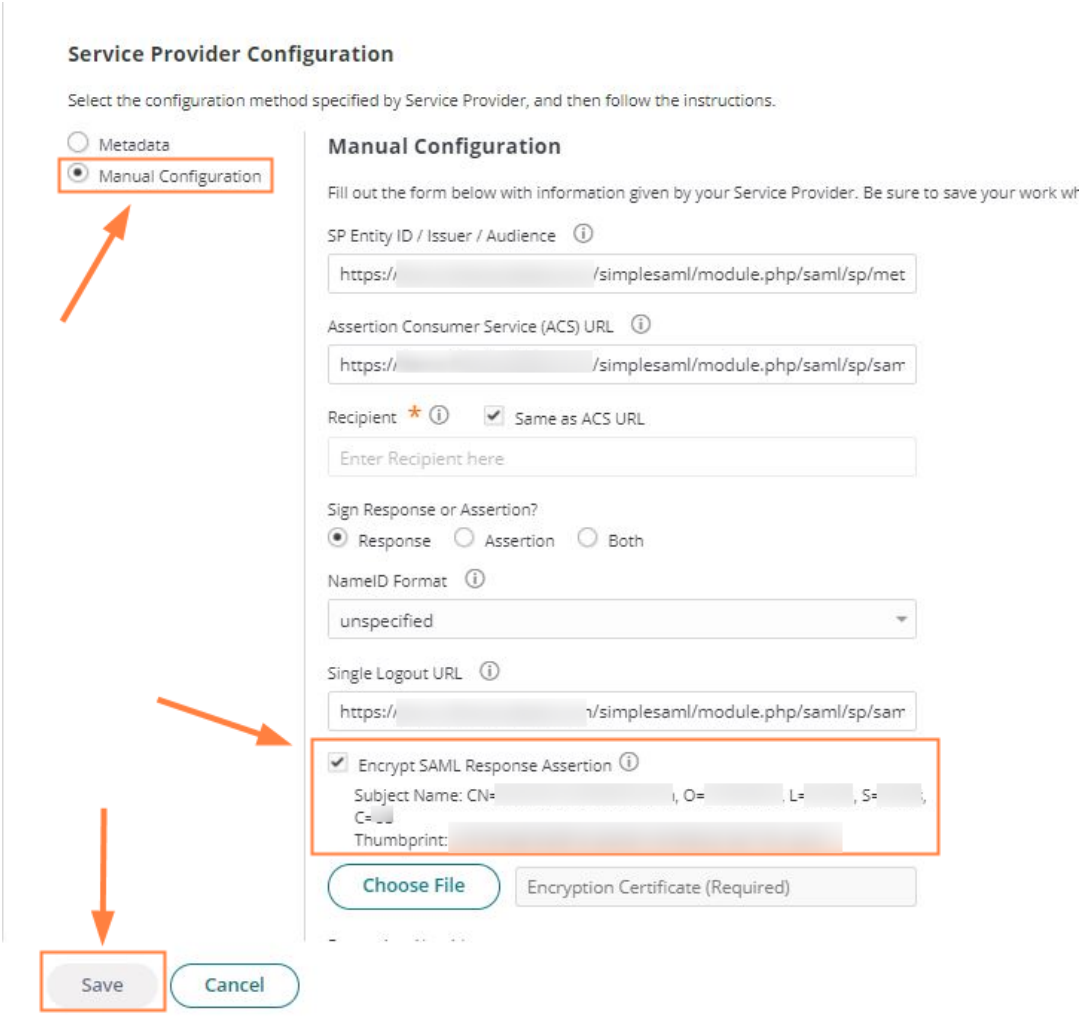
c. Enable SSO Login. In the FileCloud admin portal, go to **Customization > General > Login**. Enable **Show SSO Link** and **Show Login Options**.



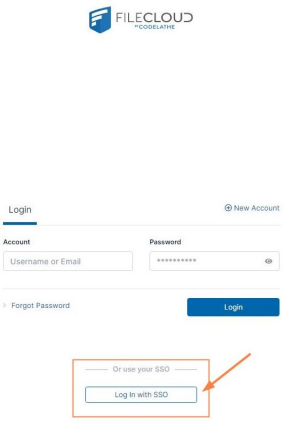
4. Configure the service provider in CYBERARK.
   a. Click the **Trust** tab in the navigation panel for the Web App, and scroll down to **Service Provider Configuration**.
   b. In URL, add the following: https://YOUR-FILECLOUD-URL/simplesaml/module.php/saml/sp/metadata.php/default-sp and click **Load** to download FileCloud's metadata.



   c. Once you have loaded FileCloud's metadata, change the settings from **Metadata** to **Manual Configuration** and disable **Encrypt SAML Response Assertion**. Click **Save**.

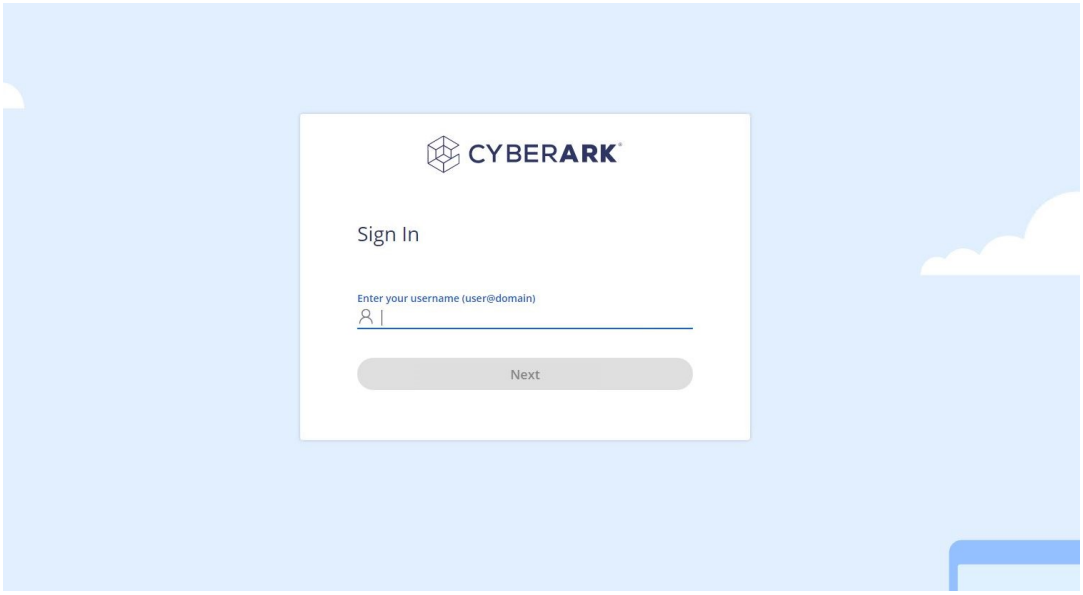


5. Complete CYBERARK SSO integration.
    a. Access FileCloud's user portal and click **Login In with SSO**.

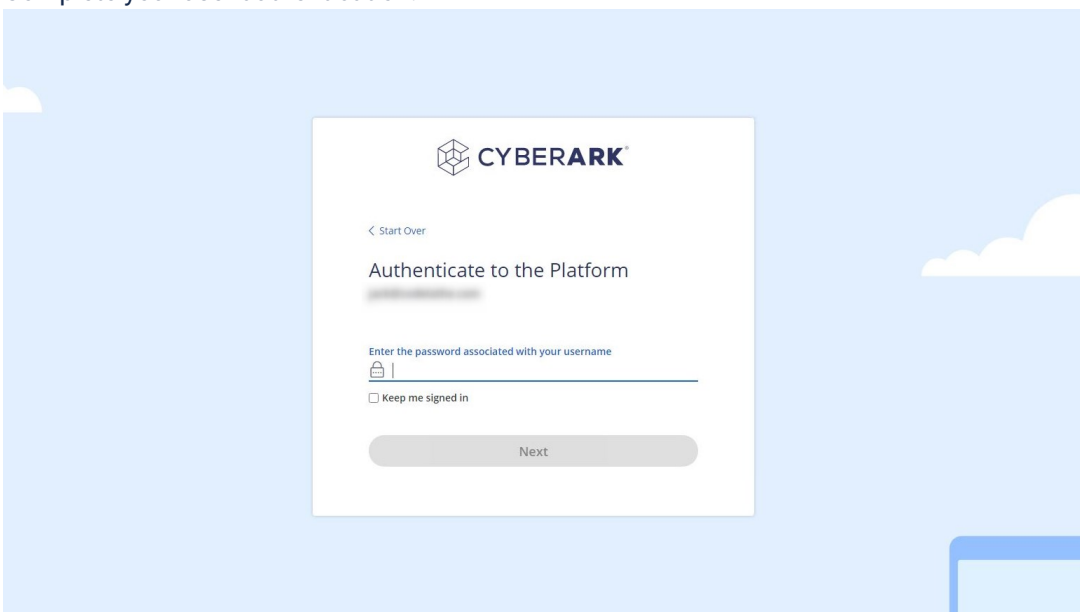




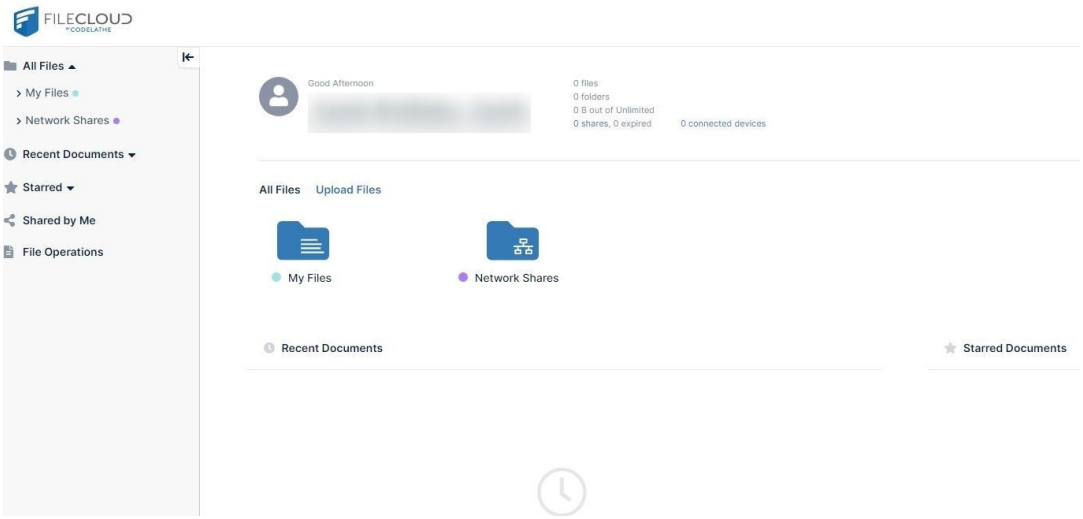
You are redirected to your CYBERARK login page.



b. Complete your user authentication.



You are redirected to FileCloud.



Now you can use single sign-on with CYBERARK from FileCloud.

Integrate JumpCloud with FileCloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator you can integrate these two systems so that your JumpCloud users can access their FileCloud account without having to enter their credentials a second time.

JumpCloud Directory-as-a-Service	JumpCloud's is a cloud-based platform • It enables IT teams to securely manage user identities • It connects teams them to resources they need regardless of provider, protocol, vendor, or location

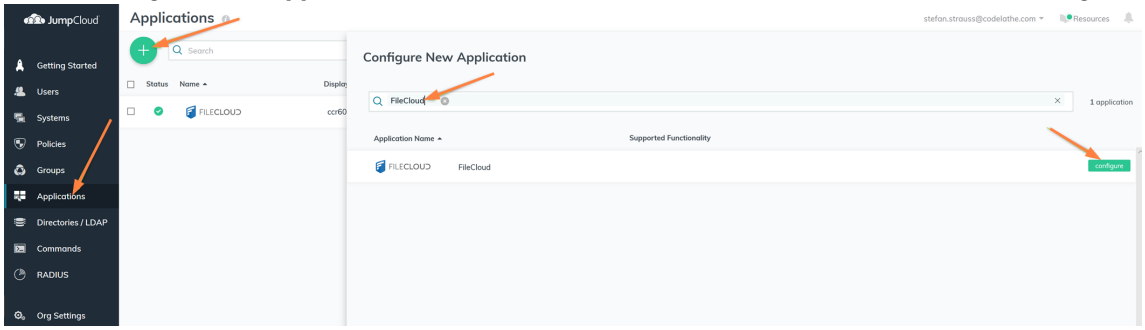
In this integration scenario:

- JumpCloud must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

Configure FileCloud with JumpCloud

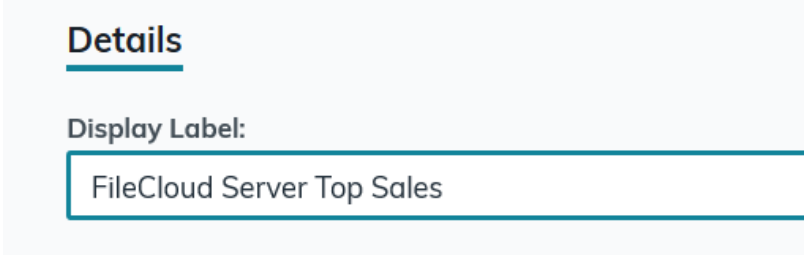
1. In JumpCloud, create a new application.

1. Open a browser and log in to your JumpCloud admin interface at https://console.jumpcloud.com/login.
2. From the left navigation pane, click **Applications**.
3. On the **Applications** screen, to add a new application, click the plus sign.
4. In the **Configure New Application** screen, enter **FileCloud** in the search field and click **configure**.

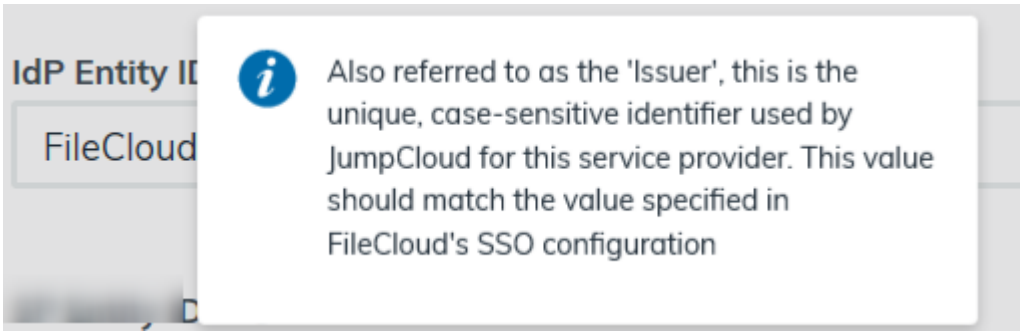


2. In JumpCloud, configure the FileCloud application

1. In **Display Label**, enter a meaningful name.



2. In **IDP Entity ID**, enter a unique, case-sensitive identifier to be used by JumpCloud for this FileCloud service provider.



3. Replace **YOUR_DOMAIN** with your domain name in all fields.

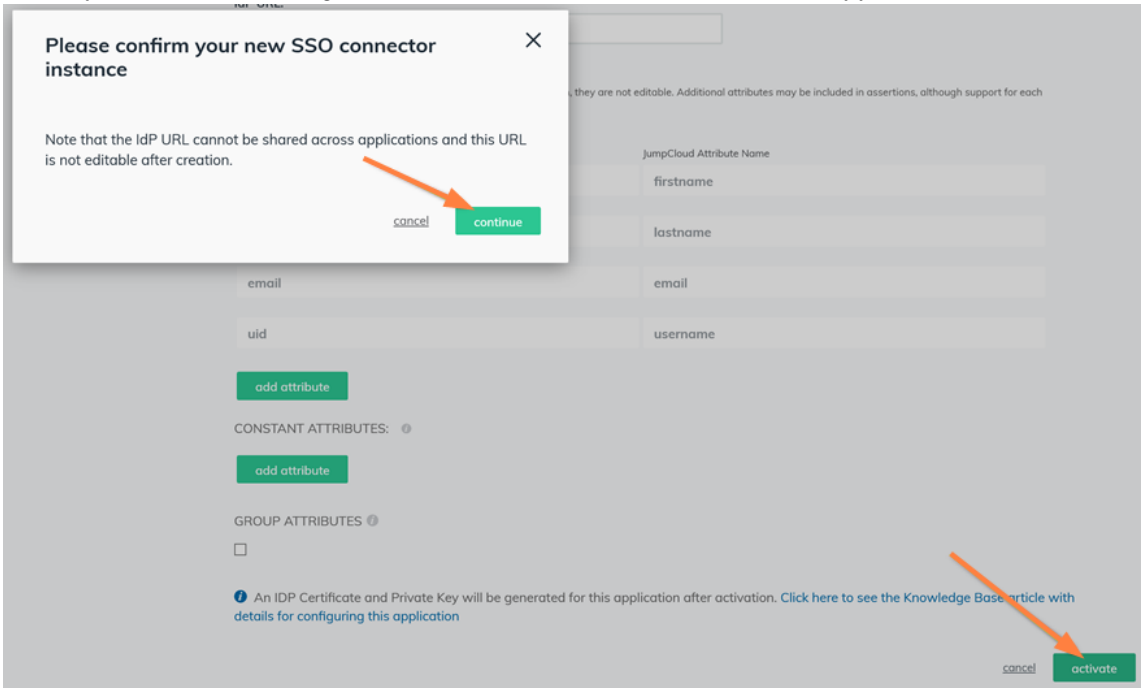


4. Enter a unique value for **IdP URL**.
   Note that the IdP URL cannot be shared across applications, and this URL is not editable after creation.

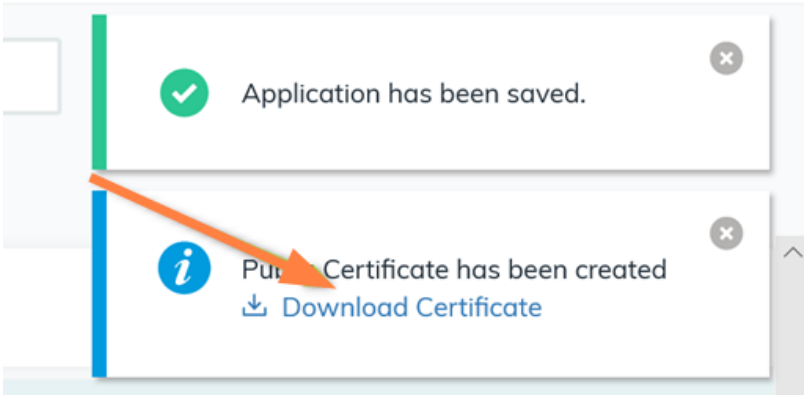


3. In JumpCloud, activate the new application and export metadata and certificate

1. In JumpCloud, on the configuration screen, save and activate the new application.



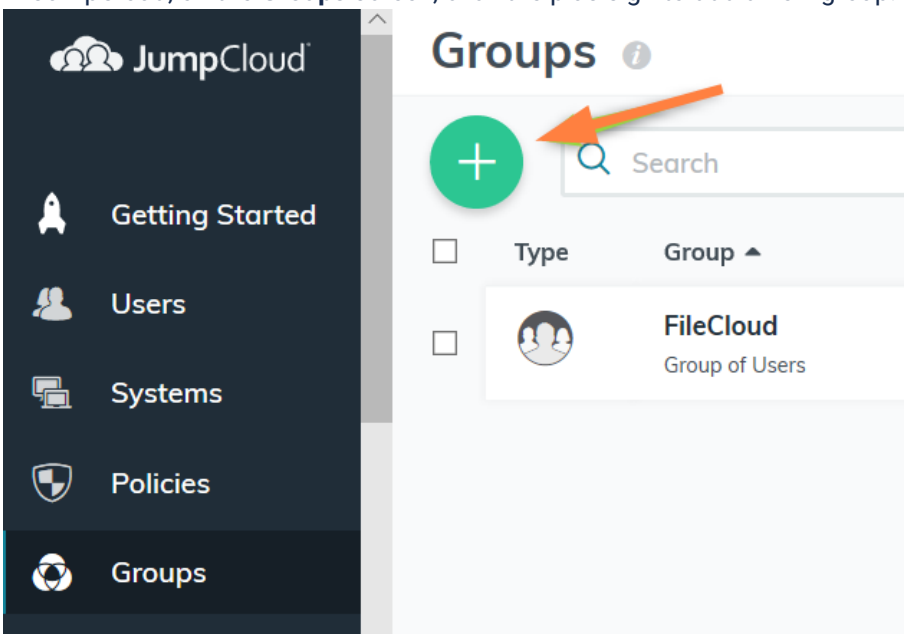
2. Download the generated certificate.



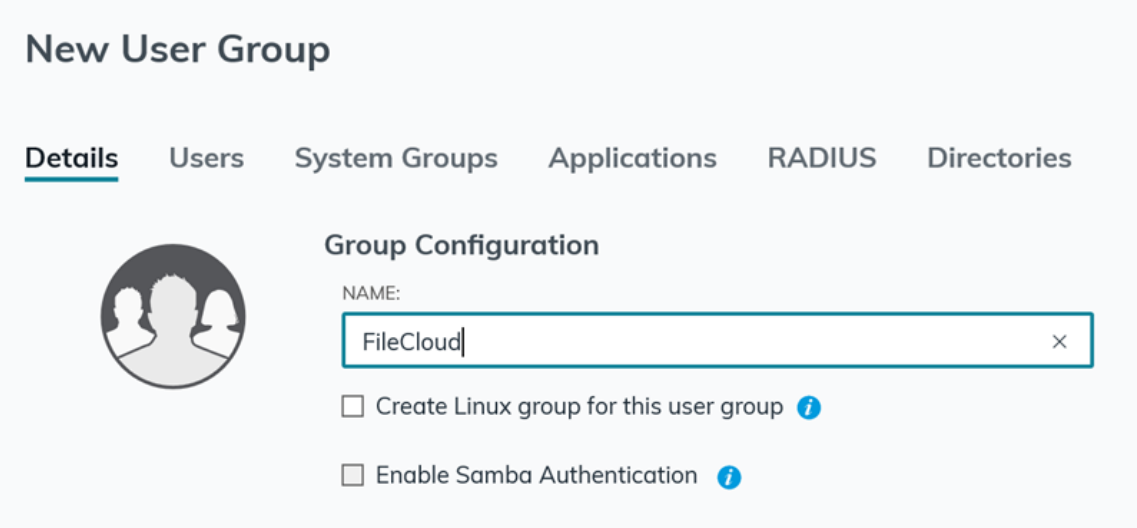
Copy the certificate into your FileCloud in the location for Linux /var/www/html/thirdparty/simplesaml/cert/saml.crtor Windows: C:\xampp\htdocs\thirdparty\simplesaml\cert\saml.crt

4. In JumpCloud, create a group and add users

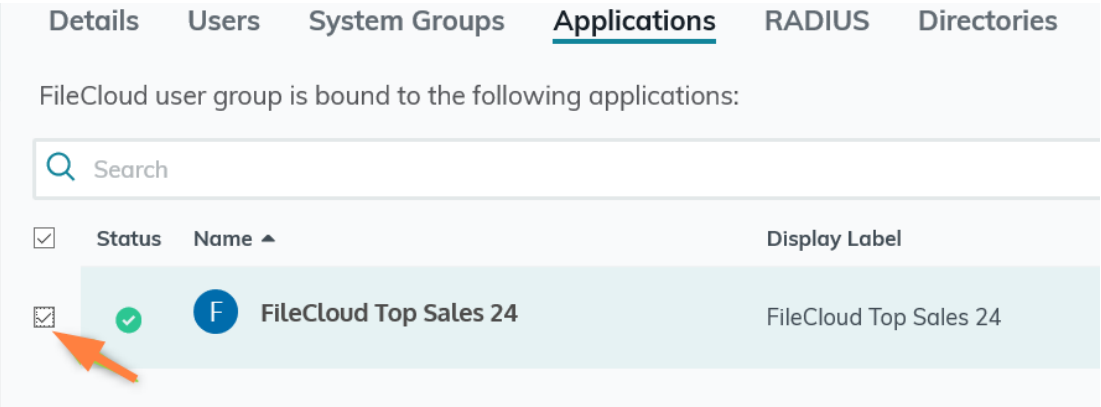
1. In JumpCloud, on the **Groups** screen, click the plus sign to add a new group.



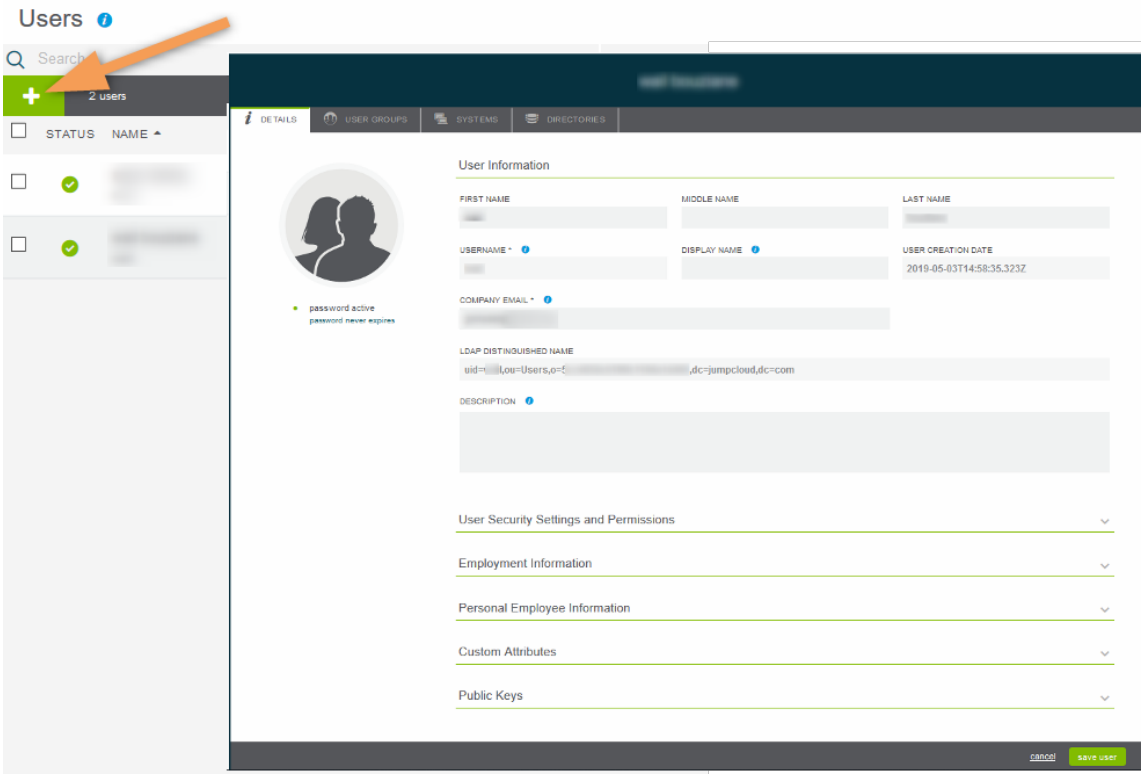
2. Enter the group name.



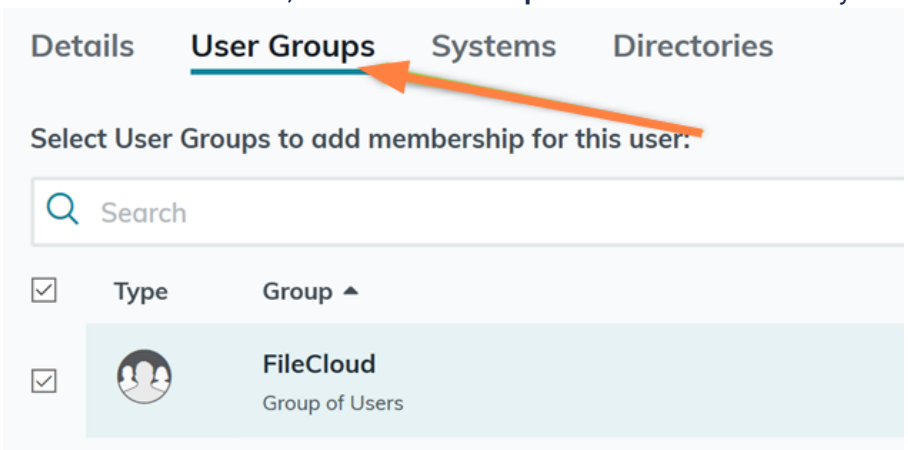
3. Enable the group to access FileCloud.



4. On the **Users** screen, click the plus sign to add a new user.



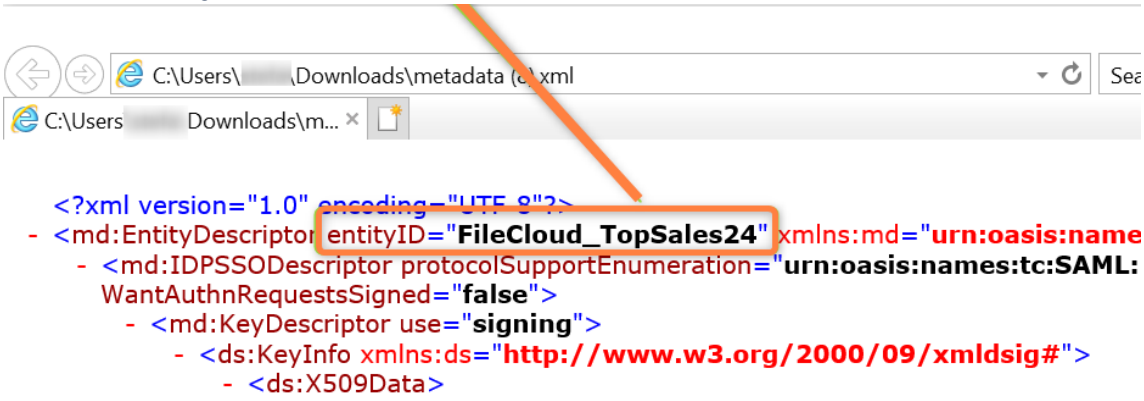
5. On the **New User** screen, click the **Details** tab and type in the user's information.
6. On the **New User** screen, click the **User Groups** tab and add the user to your FileCloud group.



7. Click **Save User**.

5. In FileCloud, configure the SSO settings.

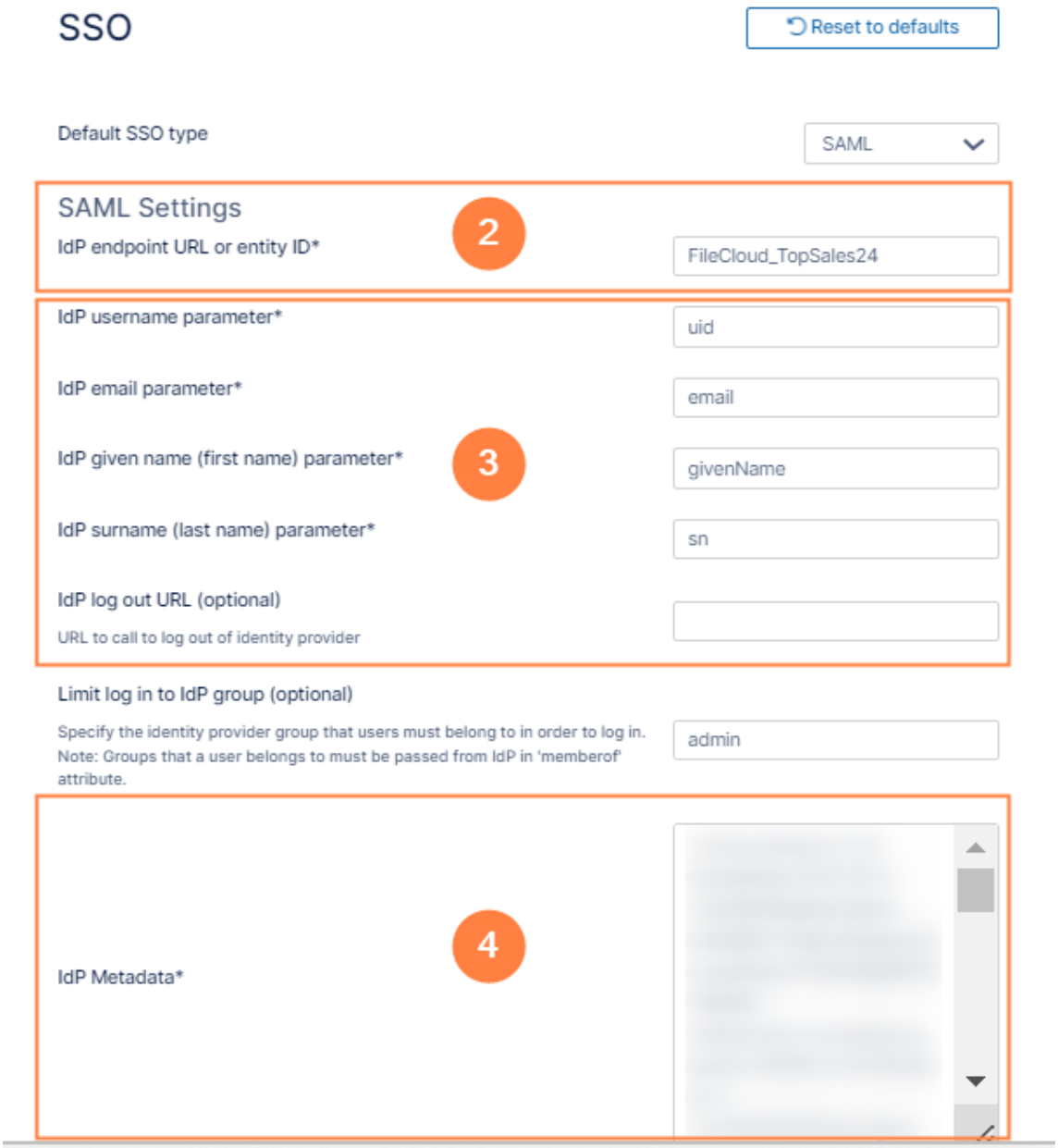
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** .
   The **SSO** page opens.
2. In **Idp End Point URL**, type or paste in the same value as the **IdP Entity ID** that you entered into JumpCloud.
   The correct string can also be seen in the metadata xml file:



3. Input the **Service Provider Attribute Name** information from the JumpCloud configuration screen into the corresponding fields in the FileCloud **Settings > SSO** tab.
   Copy these values from JumpCloud:



   Enter them into the corresponding settings in FileCloud on the **Settings > SSO** tab.
4. On the server, open the XML file that contains the metadata you exported from JumpCloud. Copy the metadata in the file and paste it into the **IdP Metadata** field in FileCloud.



5. Fill in the other settings on the page as shown at SAML Single Sign-On Support.
6. Click **Save** and minimize the browser.

Now you can start using single sign-on with JumpCloud from FileCloud.

Integrate Okta with FileCloud

To integrate with the Okta browser plugin, please see Integrate with Okta using browser plugin.

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

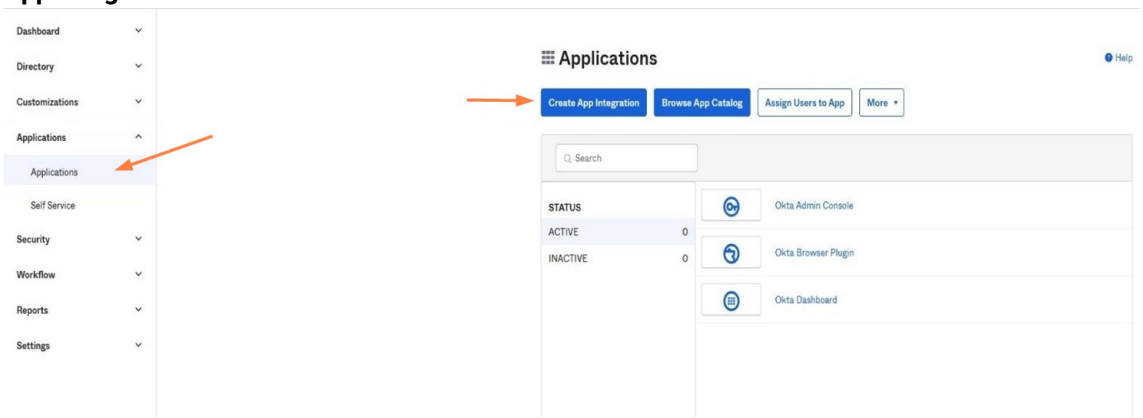
When FileCloud is integrated with Okta, Okta is configured as an Identity Provider (IdP) and FileCloud acts as the Service Provider (SP).

FileCloud can be integrated with Okta.

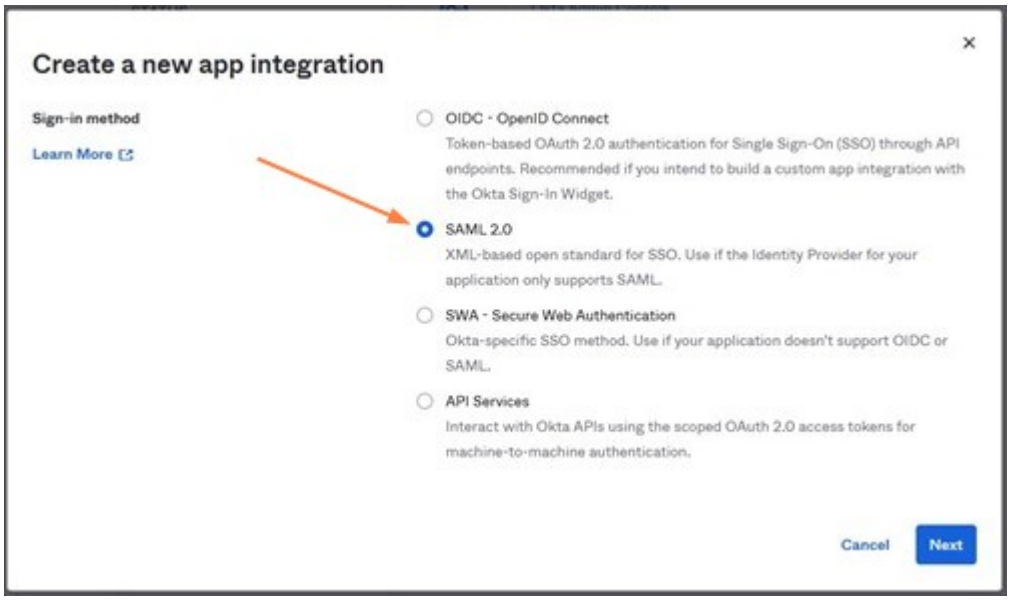
- Okta must be configured as an Identity Provider (IdP)
- FileCloud acts as the Service Provider (SP)
- By default, this integration does not synchronize a user's SSO groups and FileCloud groups each time a user logs in with SSO. This can result in unauthorized access to content as well as missing access where it's needed. To prevent this:
  a. Complete the optional steps 11 and 14 when you follow the To configure FileCloud with Okta procedure below.
  b. Complete the step in see **Syncing Group Changes on Every Login**, below.

To configure FileCloud with Okta:

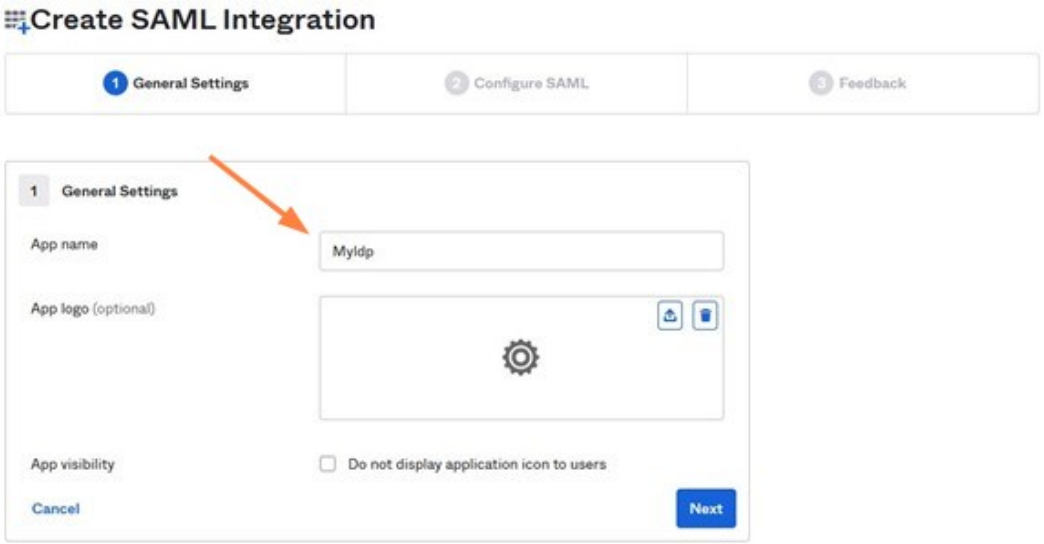
1. Log in to your Okta-issued URL, which has the format: https://yourdomain-admin.okta.com/admin/dashboard
2. After successful login to Okta, go **Applications and Resources > Applications**, and click **Create App Integration**.



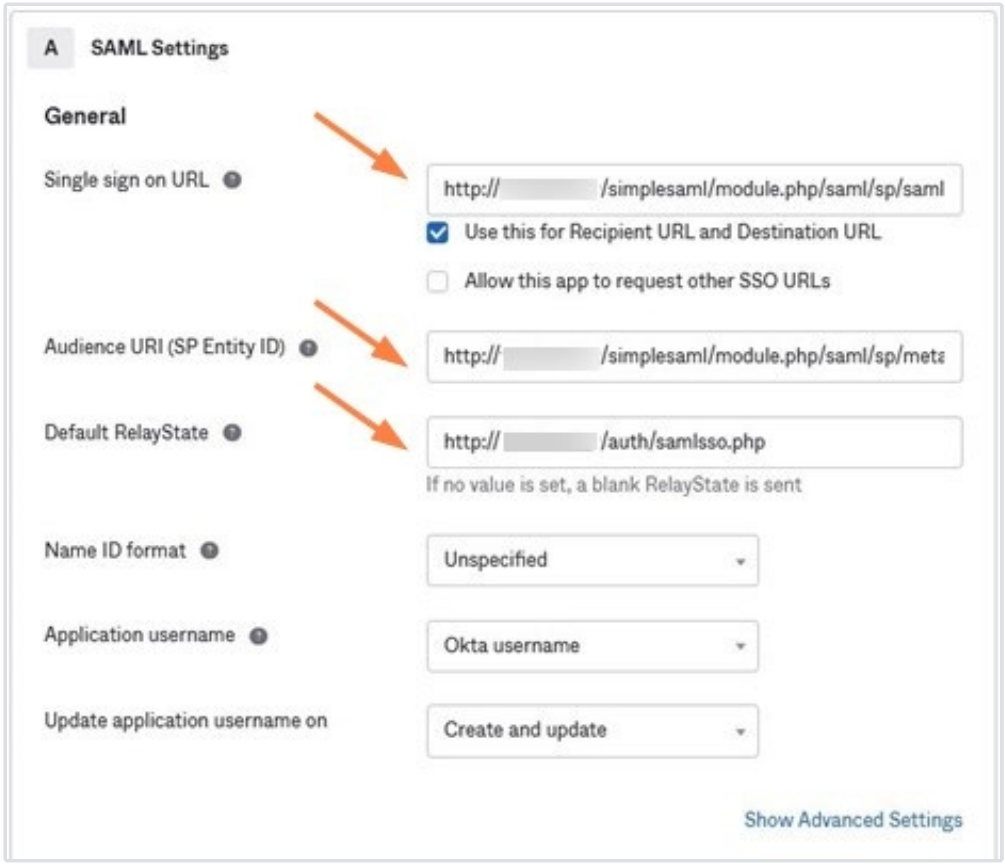
3. In the **Create a new app integration** screen, select **SAML 2.0**, and click **Next**.



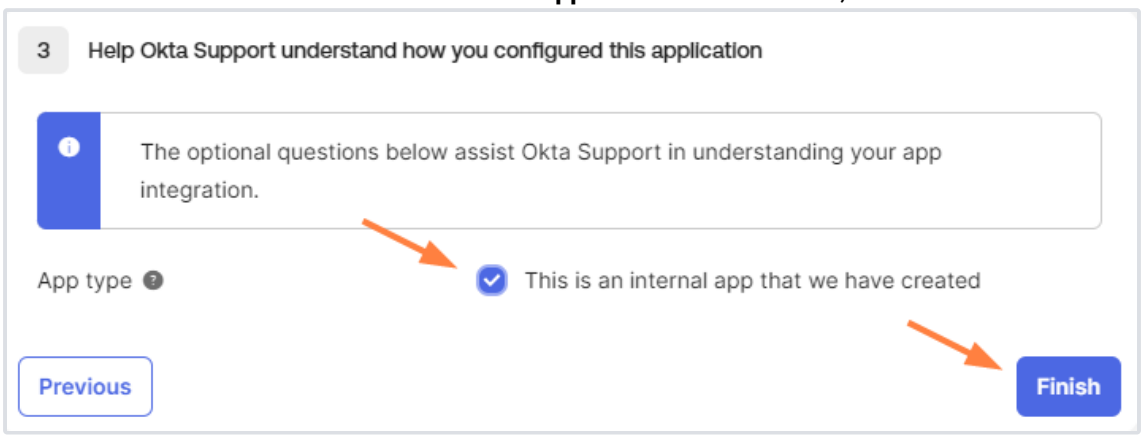
4. In the **General Settings** tab of the **Create SAML Integration** screen, enter a name for **App name**, and click **Next**.



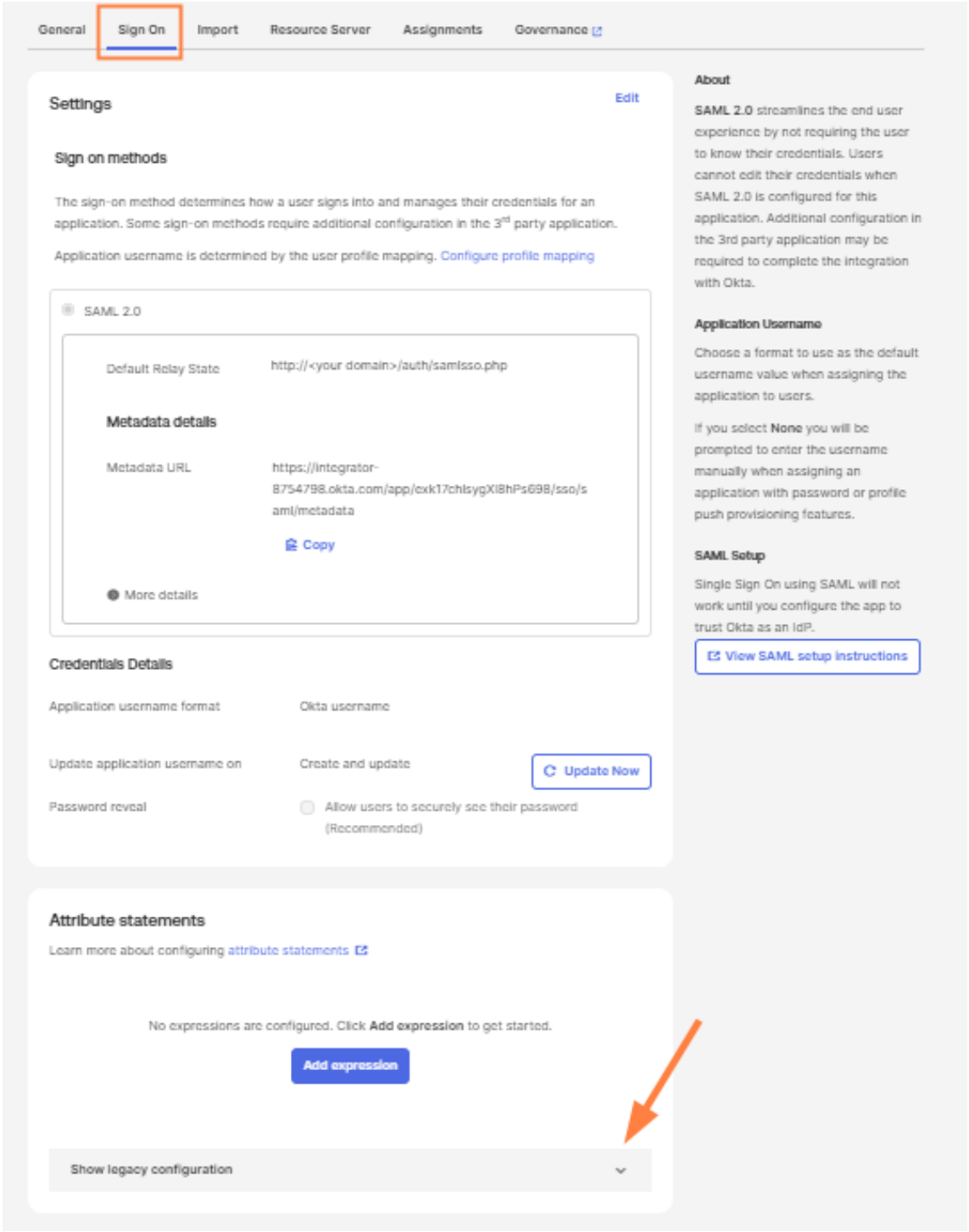
5. In the **SAML Settings** screen, set the values as follows:
   - Set **Single sign on URL** to the FileCloud assertion URL **http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp**
   - Set **Audience URI (SP Entity ID)** to **http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp**
   - Set **Default Relay State** to **http://<your domain>/auth/samlsso.php**



6. Click **Next.**
7. In the **Feedback** tab select **This is an internal app that we have created**, and click **Finish**.

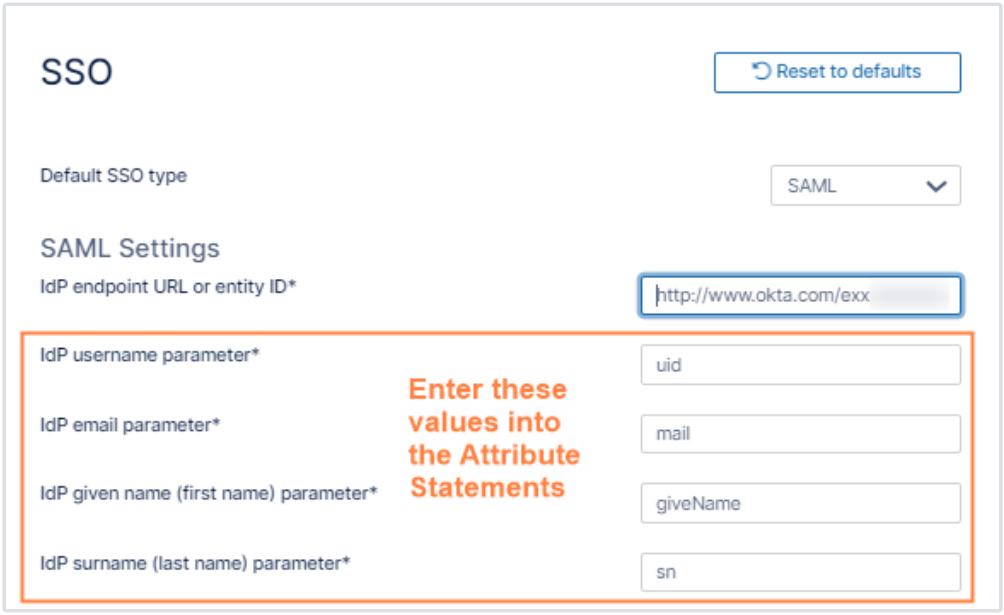


8. Go to the **Sign On** tab.
9. Scroll down to **Attribute statements** and expand **Show legacy configuration**.

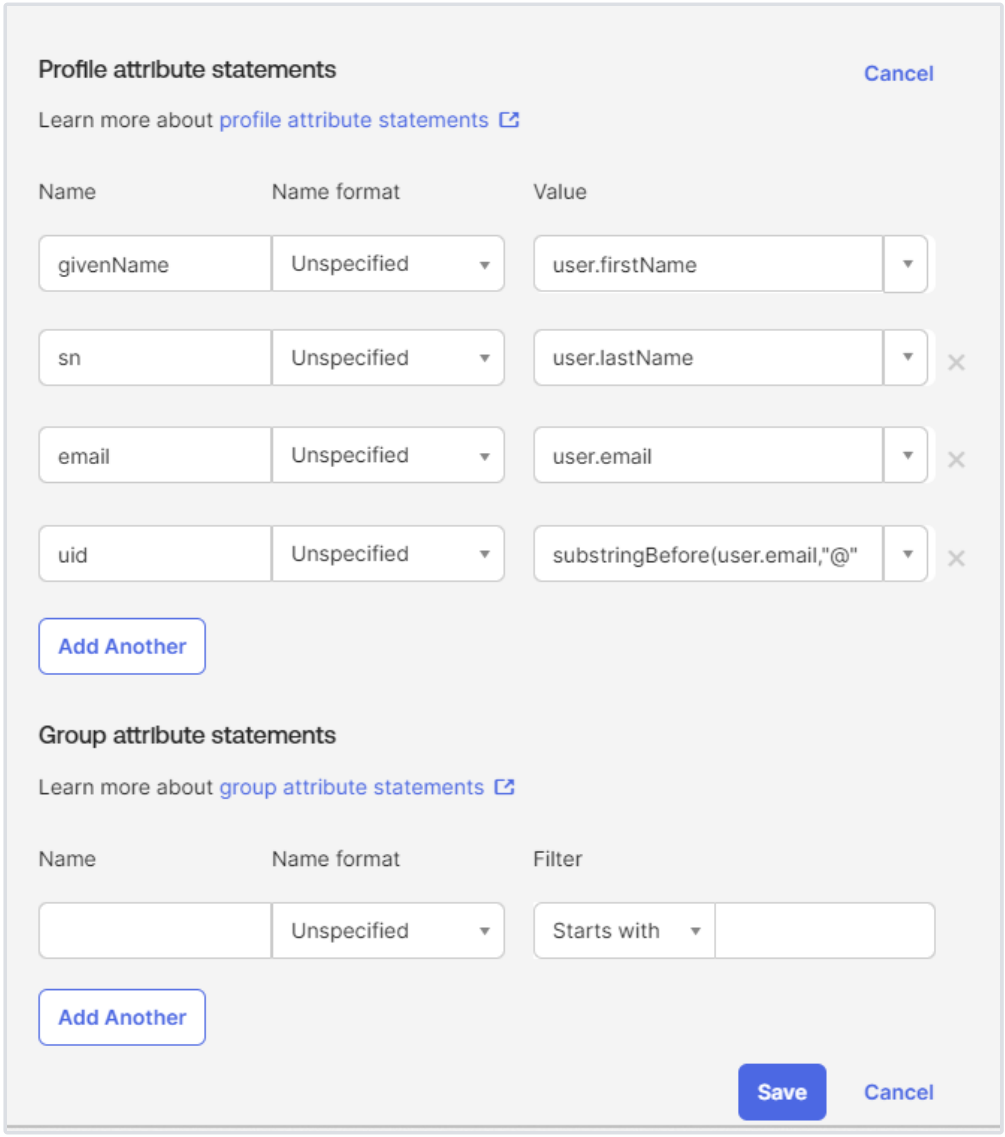
10. 

Under **Profile attribute** statements, add attribute names. that match the names set in the FileCloud admin portal in **Settings > SSO** for **Idp Username Parameter**, **Idp Email Parameter**, **Idp Given Name Parameter**, and **IDP Surname Parameter**:

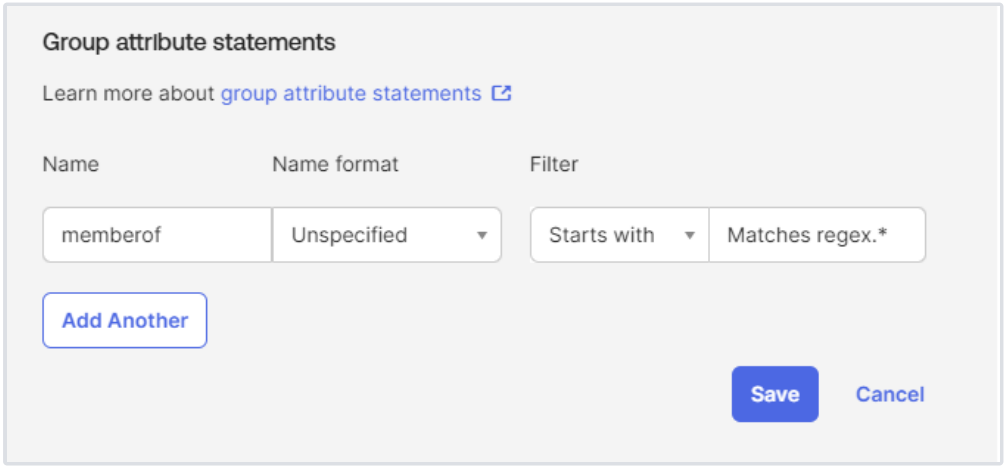
a. Copy the the values entered in the FileCloud screen **Settings > SSO** for **Idp Username Parameter**, **Idp Email Parameter**, **Idp Given Name Parameter**, and **IDP Surname Parameter**. These will become the **Names** of the **Profile attribute statements** in Okta.



b. In Okta, set the **Names** and **Values** to the following:
givenName: **user.firstName**
sn: **user.lastName**
email: **user.email**
uid: **substring Before(user.email,"@")**

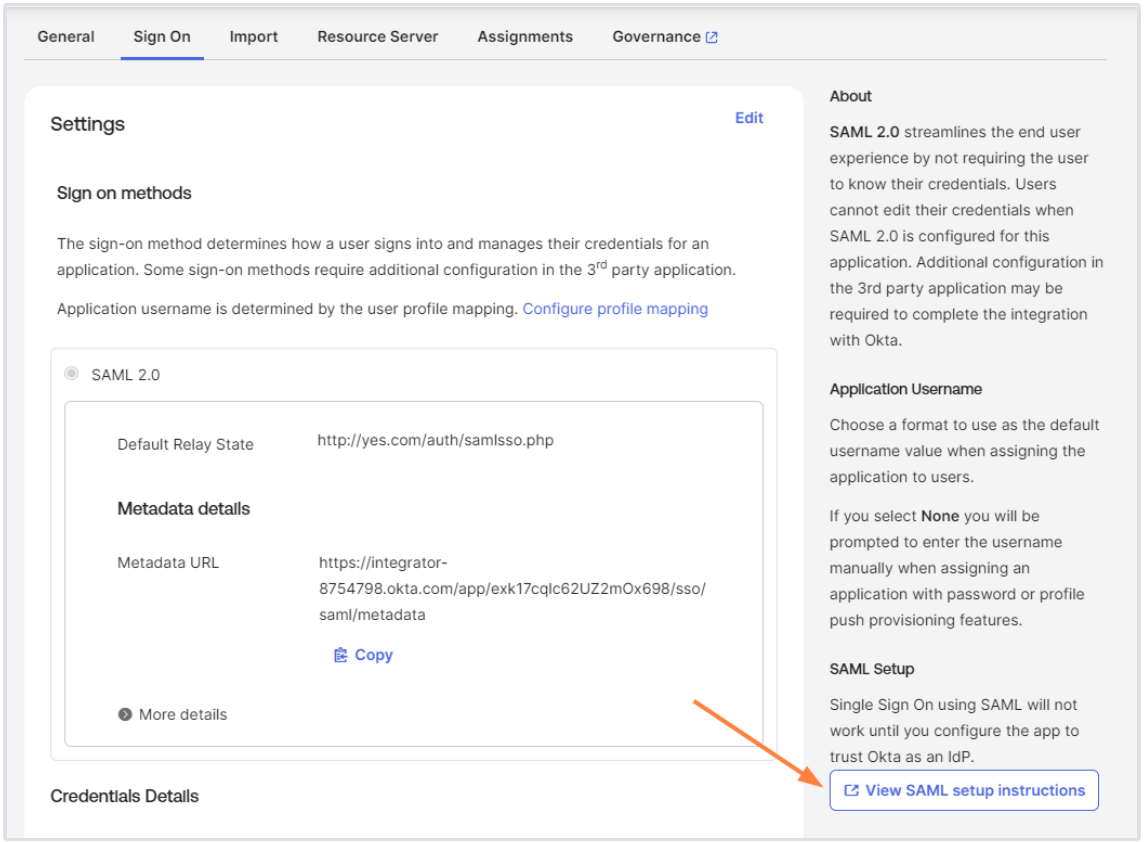


11. **Optional** - If you have chosen to sync FileCloud and Okta groups on every login, add the following **Group Attribute Statement**:
    In **Name**, enter **memberof**.
    In **Filter**, choose **Matches regex**, and then enter **.***:

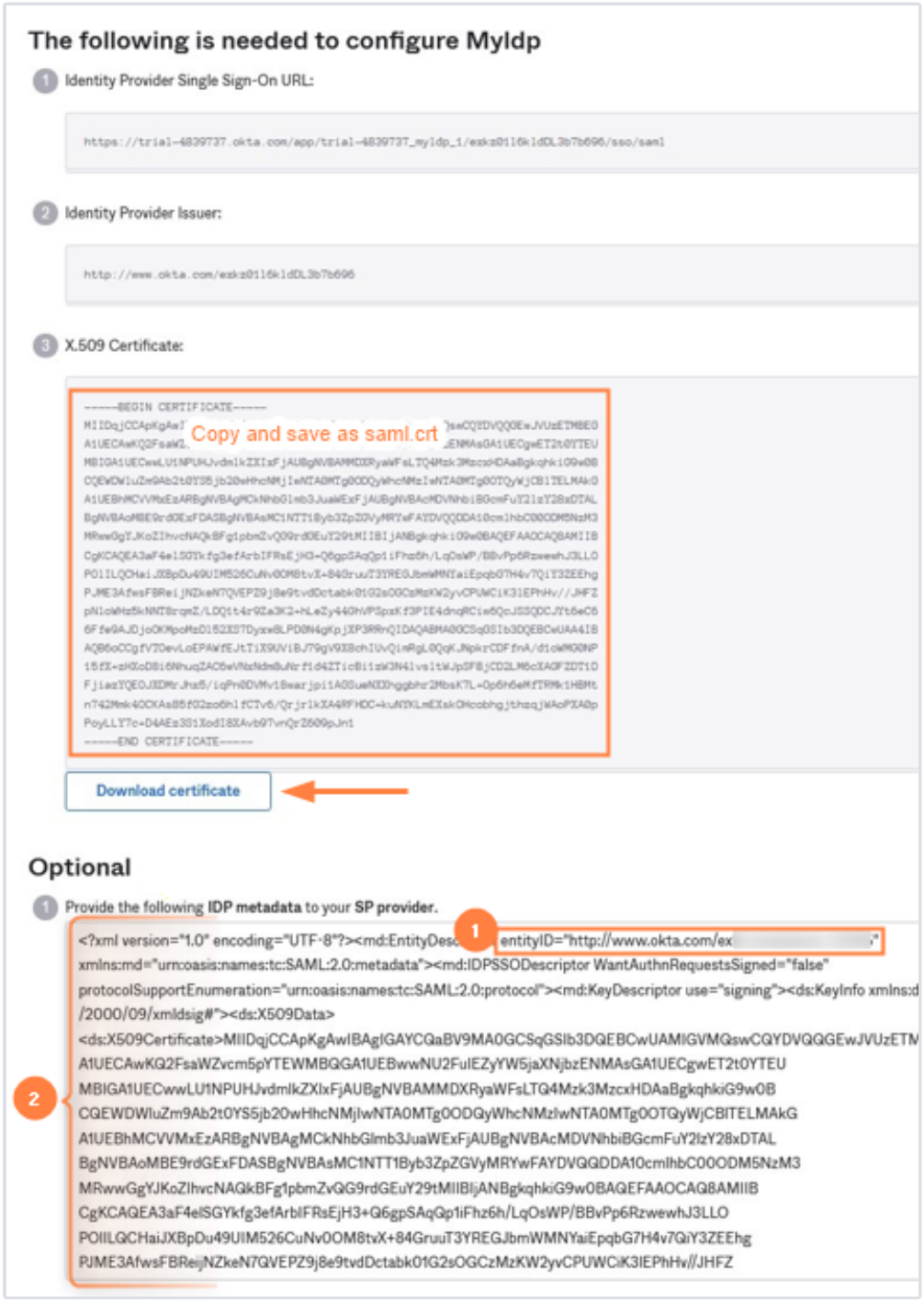


Note: To sync groups on every login, you must also complete step 14, and the steps in Syncing group changes on every login, below.

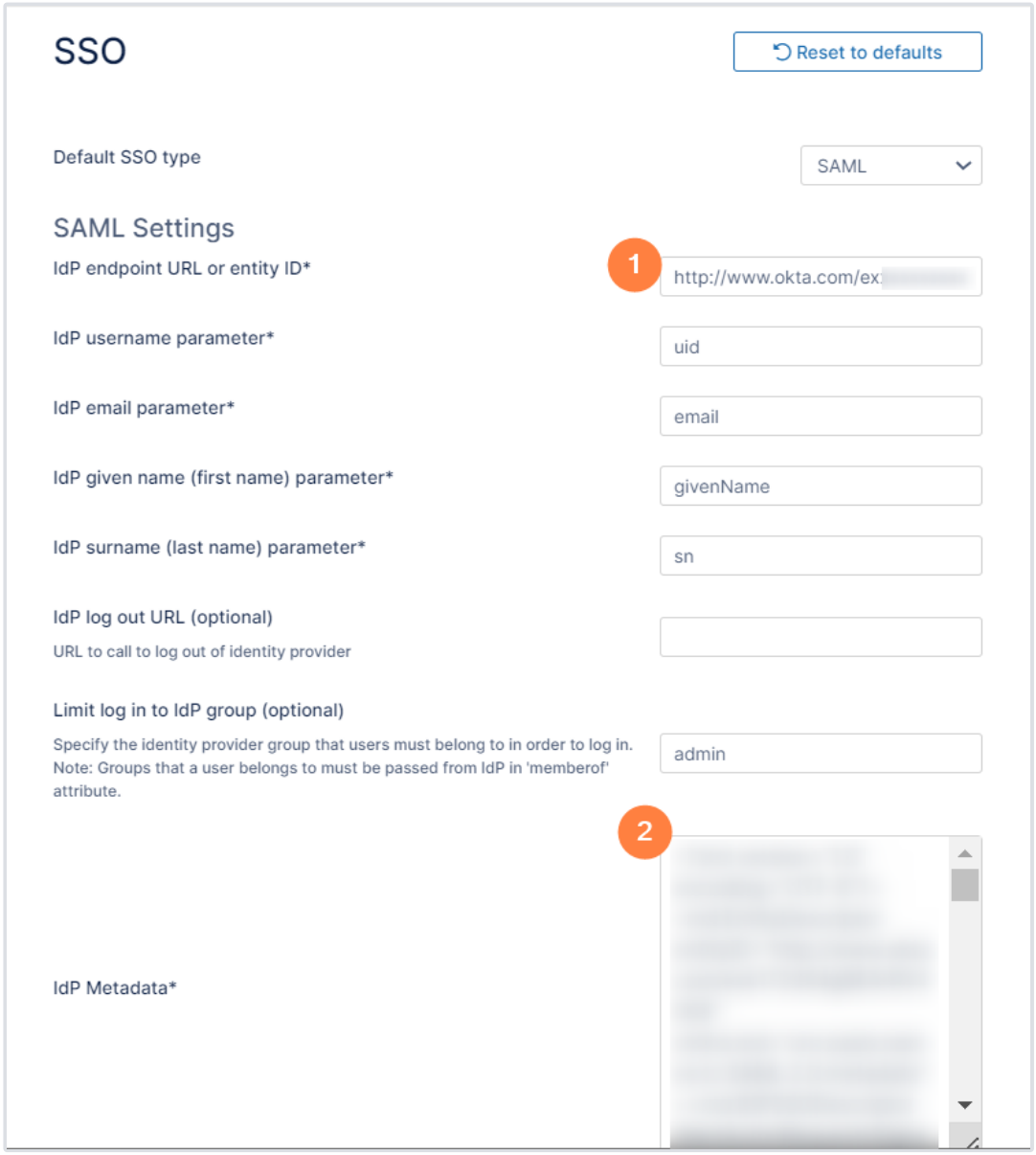
12. Scroll back up and click **View SAML Setup Instructions** to view FileCloud SSO configuration details .



A screen with information similar to the following image opens.



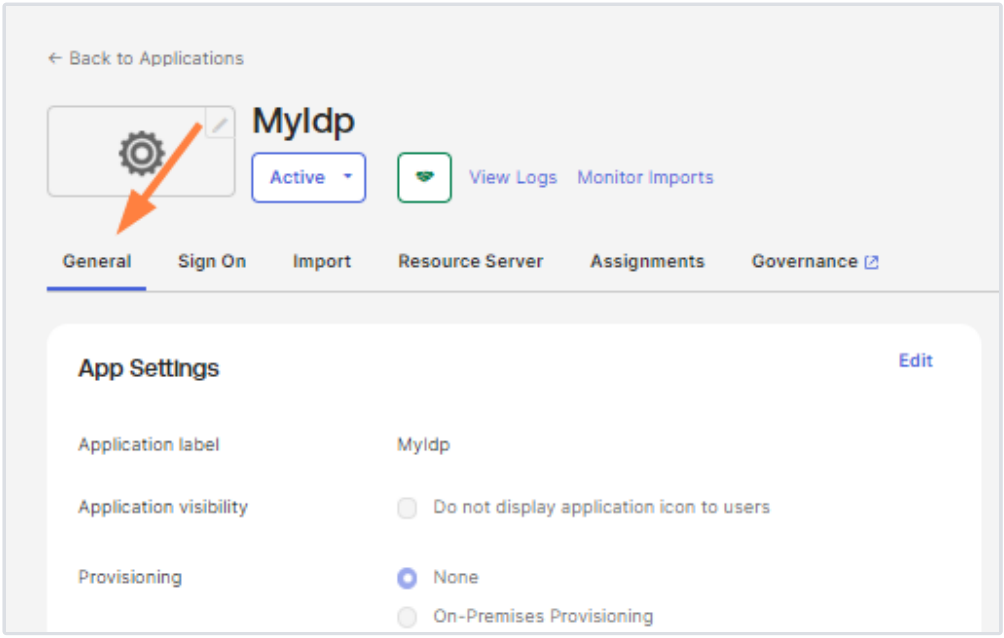
13. Use the details in this screen to configure additionalsettings in the FileCloud admin portal's **Settings > SSO** screen and to create a **saml.crt** file.
    a. Using the **IDP Metadata** text under **Optional**:
    (1) Copy the **entityID** field from the text box into **Idp Endpoint URL or EntityID** in FileCloud admin UI interface under **Settings > SSO**.
    (2) Copy the text in the **IDP metadata** box into **Idp Metadata** in FileCloud admin UI interface under **Settings > SSO**.



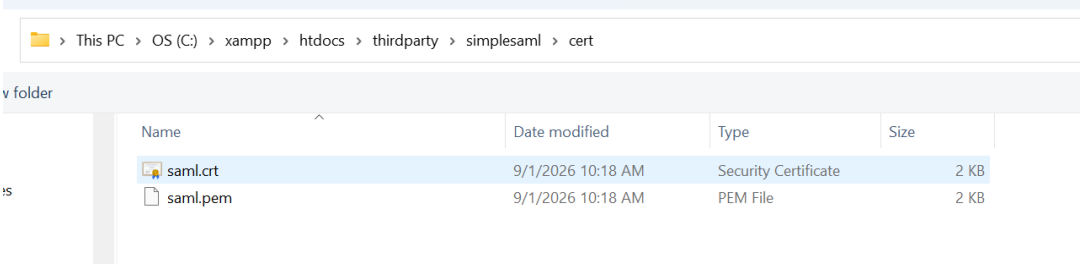
b. Click **Download certificate**, then copy the certificate file and rename it to **saml.crt**.

   Copy the saml.crt file in the FileCloud server in the following place <FileCloud WEB ROOT>/thirdparty/simplesaml/cert.

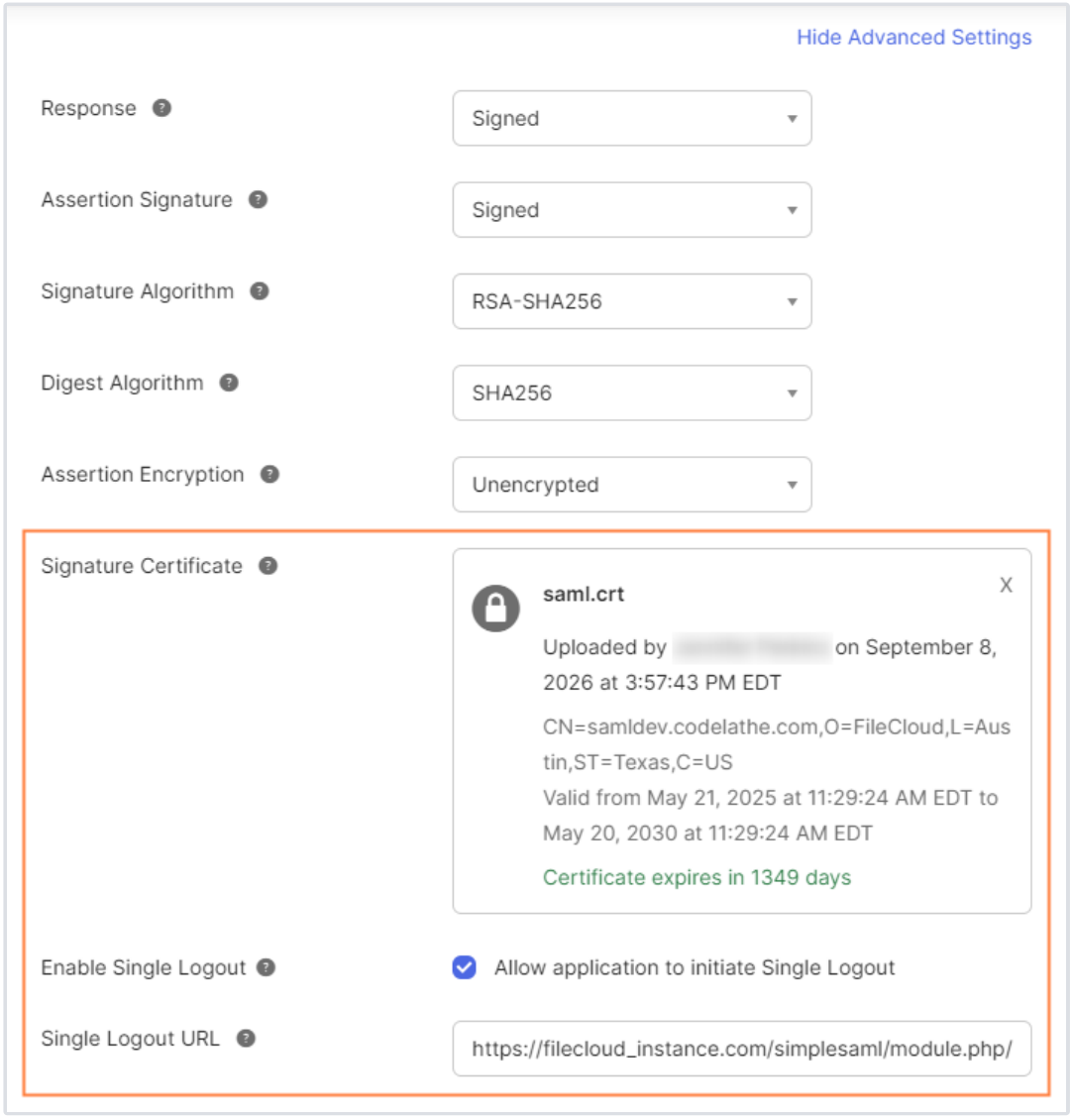
14. **Optional -** If you have chosen to sync FileCloud and Okta groups on every login:
    a. Click the **General** tab.



b. Scroll down to **SAML Settings** and click **Edit**.
c. Click **Next** to go to the **Configure SAML** screen.
d. Click **Show Advanced Settings**.
e. In **Signature Certificate**, upload the signature certificate file you saved in:

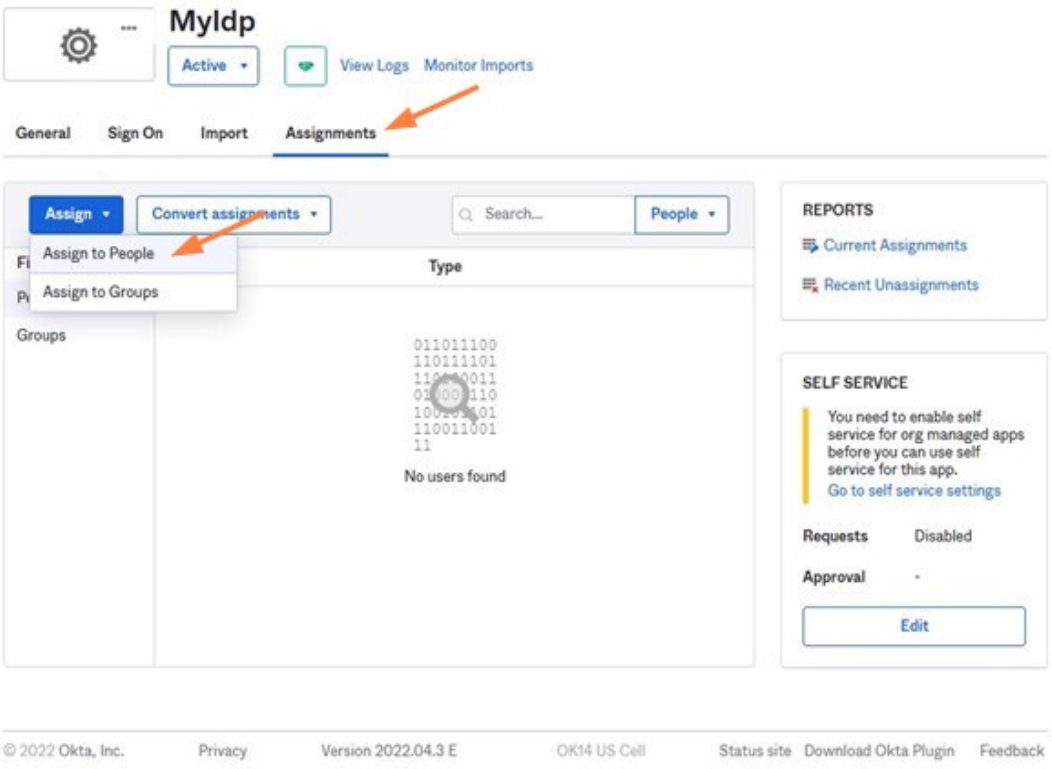


f. Check **Enable Single Logout**.
g. In **Single Logout URL**, enter



h. Click **Next**, and then click **Finish**.

15. To assign the Okta FileCloud integration to users so they can log in to FileCloud with Okta, click the **Assignments** tab in Okta.
16. In the **Assign** drop-down list, choose **Assign to People**.



A list of users who have both Okta and FileCloud accounts opens.

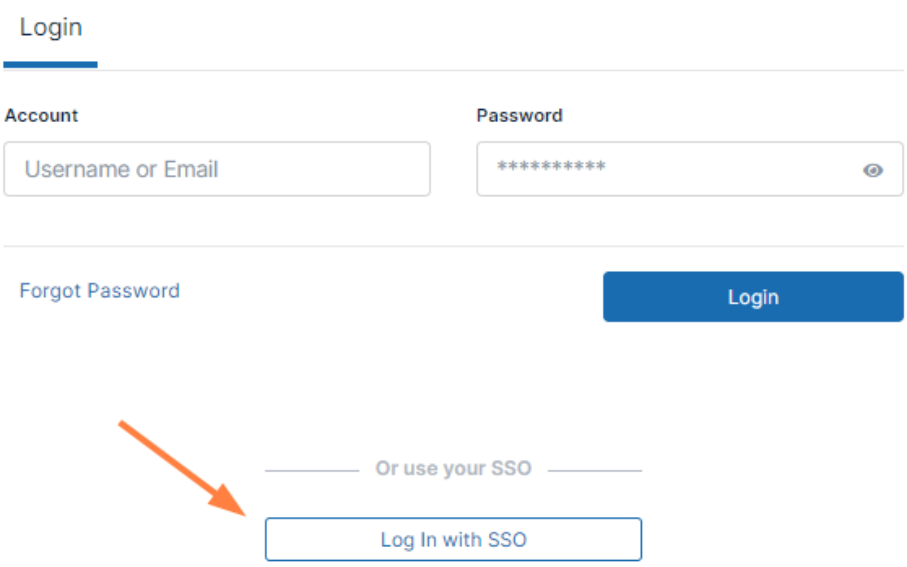
17. Select users from the list to allow them to sign in to FileCloud using Okta.

Once the application is created and FileCloud is configured you can start using single sign-on with Okta from FileCloud.

Log in to FileCloud using Single Sign-on with Okta

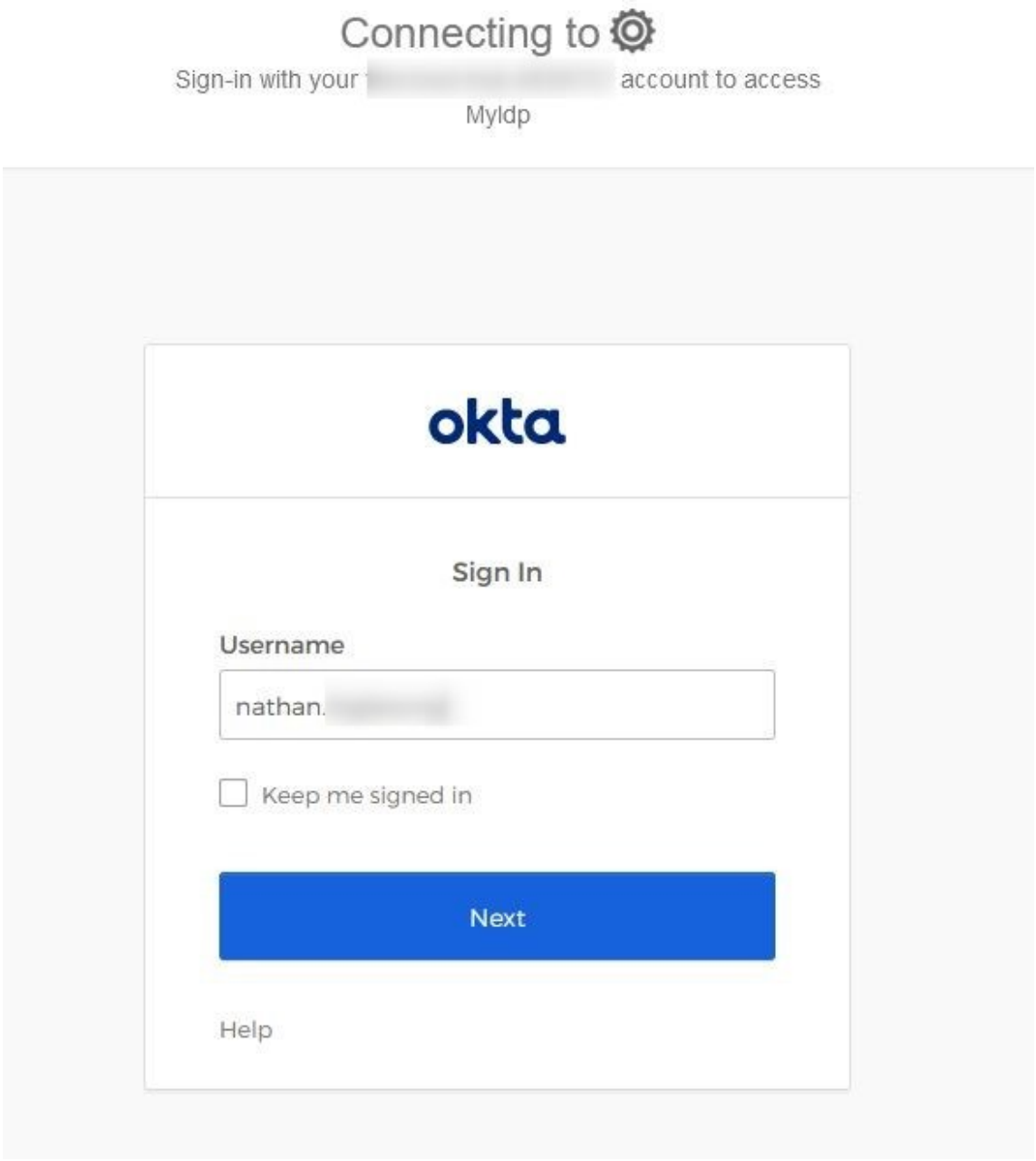
Users can sign in to the user portal or admin portal with SSO using Okta.

1. In the FileCloud login screen, the user chooses **Log in with SSO**.



If the user is already logged in to Okta, they are automatically logged in to FileCloud.

If the user not logged in to Okta, they are first redirected to the Okta sign in page, and after signing in to Okta, they are immediately redirected to FileCloud and logged in.



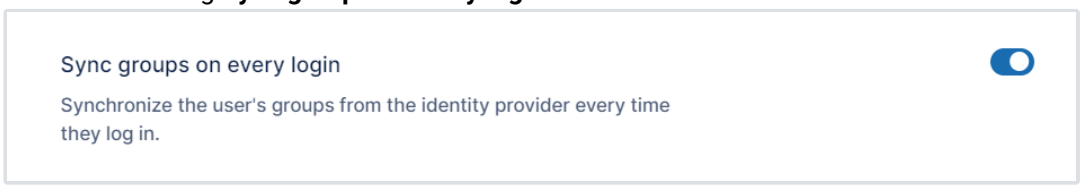
Syncing group changes on every login

If changes to your users' group membership may affect the content they have access to, you may sync a user's group changes each time they log into FileCloud with their SSO login.

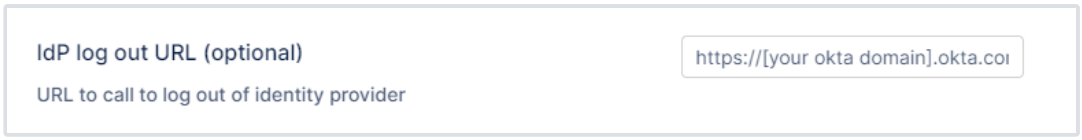
To configure SSO login to sync groups on each login:

1. In the FileCloud admin portal, go to **Settings > SSO**.

a. Enable the setting **Sync groups on every login**.



b. In **IDP log out URL (optional)** enter https://[your okta domain].okta.com/login/signout



Note: This is required, not optional for syncing groups on each login.

2. In the integration configuration procedure on this page, To configure FileCloud with Okta, make sure you complete optional steps 11 and 14.
(If you have already configured your integration, edit your configuration and perform steps 11 and 14).

Integrate with Okta using browser plugin

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

The Okta plugin for browsers works by storing FileCloud user credentials in a web application that you add to Okta. After a user chooses to log in with Okta, the credentials are entered in the FileCloud page and log in proceeds automatically.

The Okta plugin works with default FileCloud login, not SSO. Do not configure SSO settings in FileCloud. If the setting: define("TONIDOCLOUD_SSO_DIRECT_ONLY",1) appears in your cloudconfig.php file, remove or disable it.

Procedure:

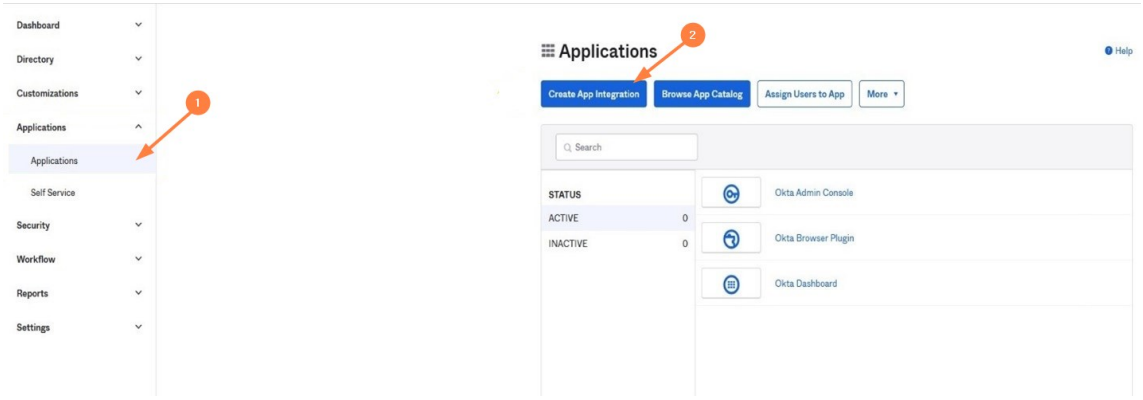
Note: You must have an Okta account before completing these steps.

1. Set up the FileCloud application in the Okta admin panel
2. Assign the FileCloud application to users
3. Install the plugin on the user browser.
4. User logs in to FileCloud using the plugin.

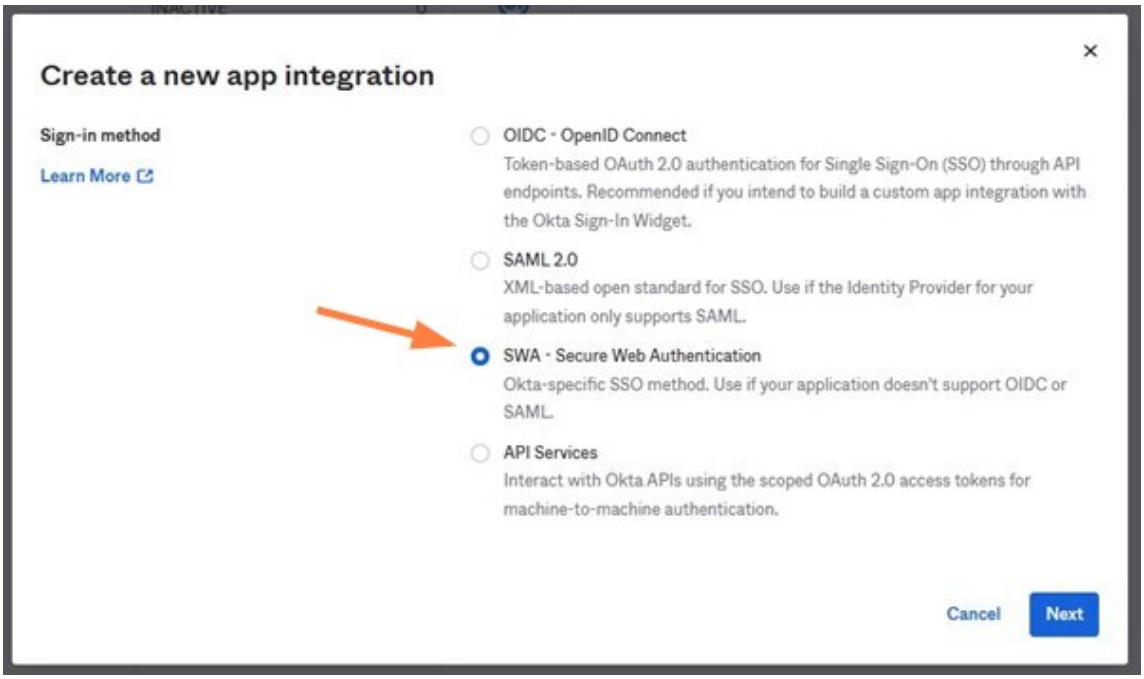
The plugin supports different browsers. Setup and tests for this guide use Google Chrome.

Set up the FileCloud application in Okta admin panel

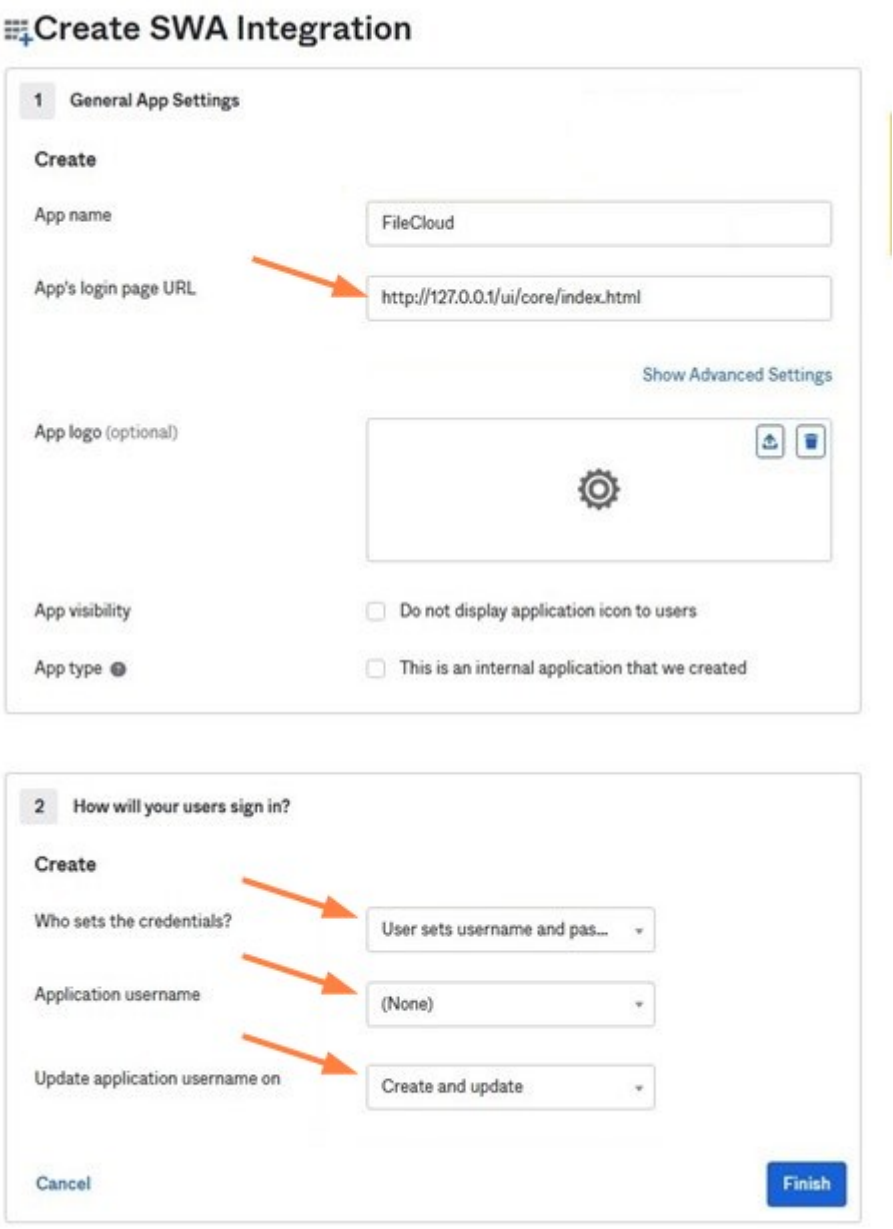
1. Log in as Admin in Okta.
2. In the navigation panel, click **Applications > Applications**.
3. In the **Applications** screen, click **Create App Integration**.



4. In the **Create a new app integration** screen, choose **SWA - Secure Web Authentication**, and click **Next**.



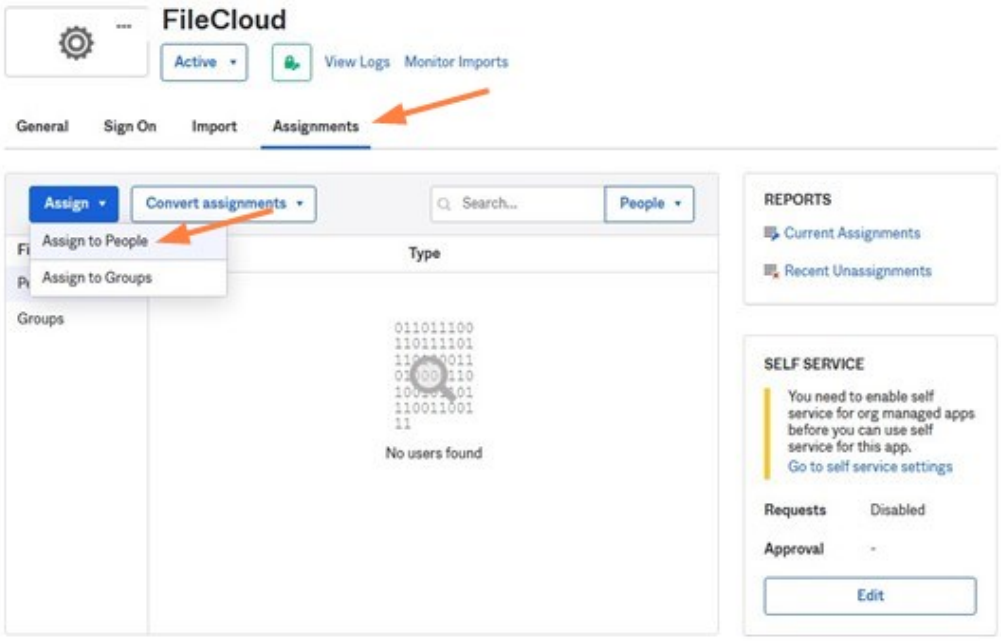
5. Fill in the **Create SWA Integration** screen as shown in the following screenshot, and click **Finish**. In **App's login page URL**, enter the login page URL for the corresponding FileCloud installation.



Assign application to users

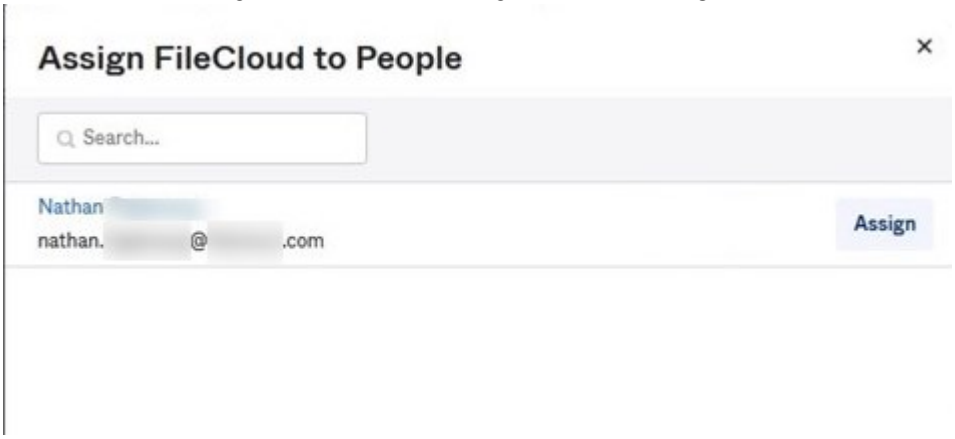
Now assign the Okta FileCloud integration to users so they can log in with Okta.

1. Click the **Assignments** tab in Okta.
2. In the **Assign** drop-down list, choose **Assign to People**.

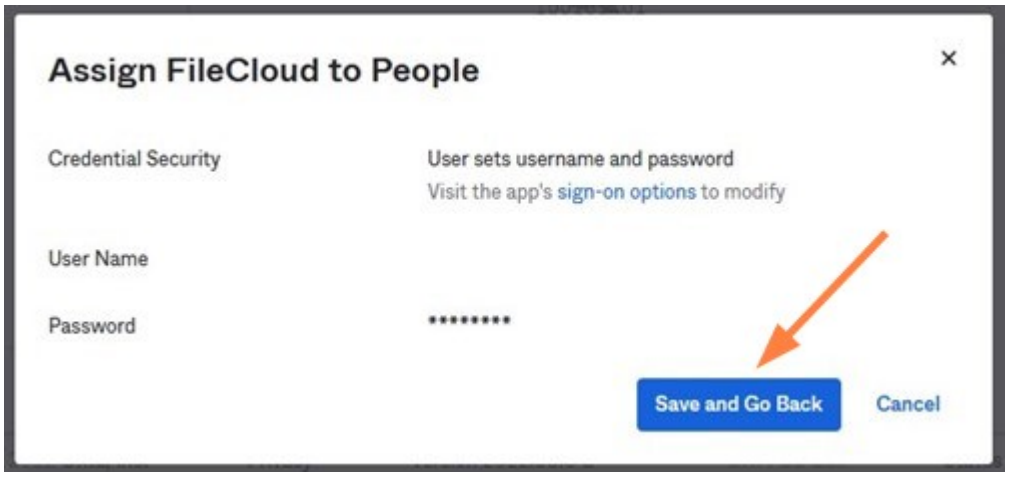


A list of users who have both Okta and FileCloud accounts opens.

3. To allow users to sign in to FileCloud using Okta, click **Assign** in the row with their email.

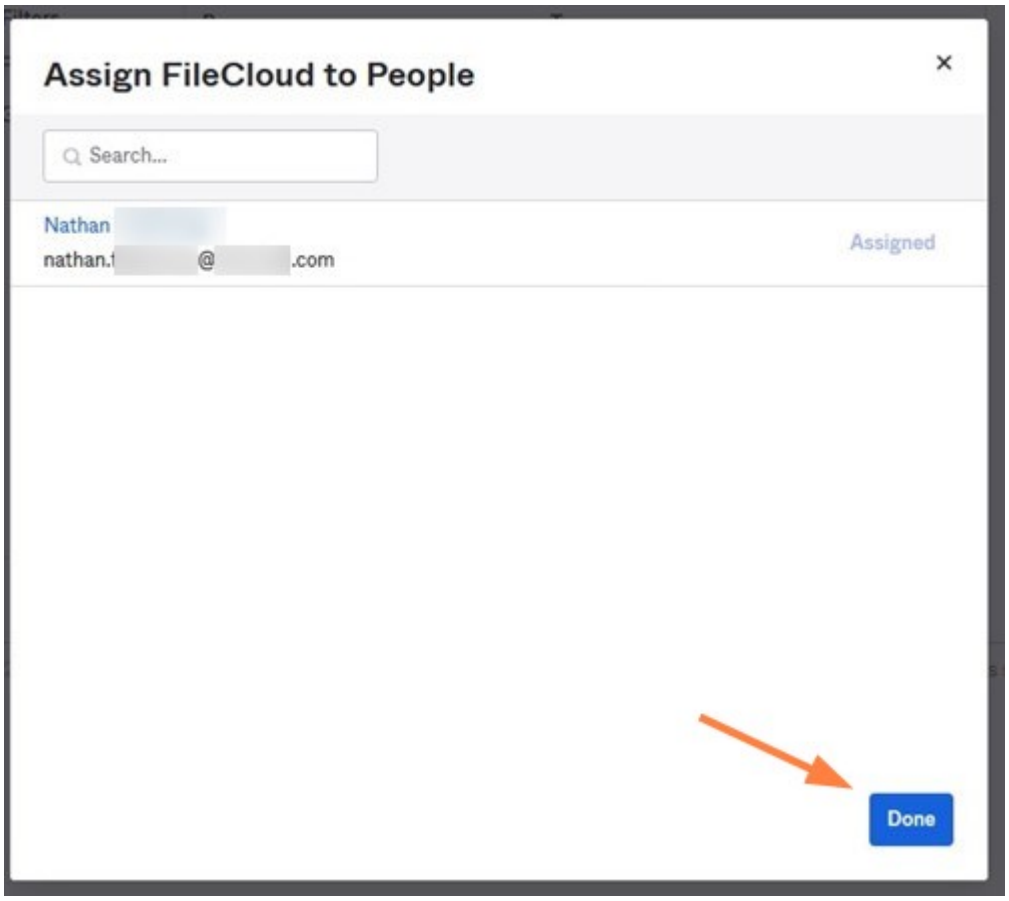


4. Enter a **User Name** and **Password** for the user, then click **Save and Go Back**.



ck

5. Click **Done**.



6. Repeat this process for all users you want to assign to the integration.

Install the Plugin in the Browser

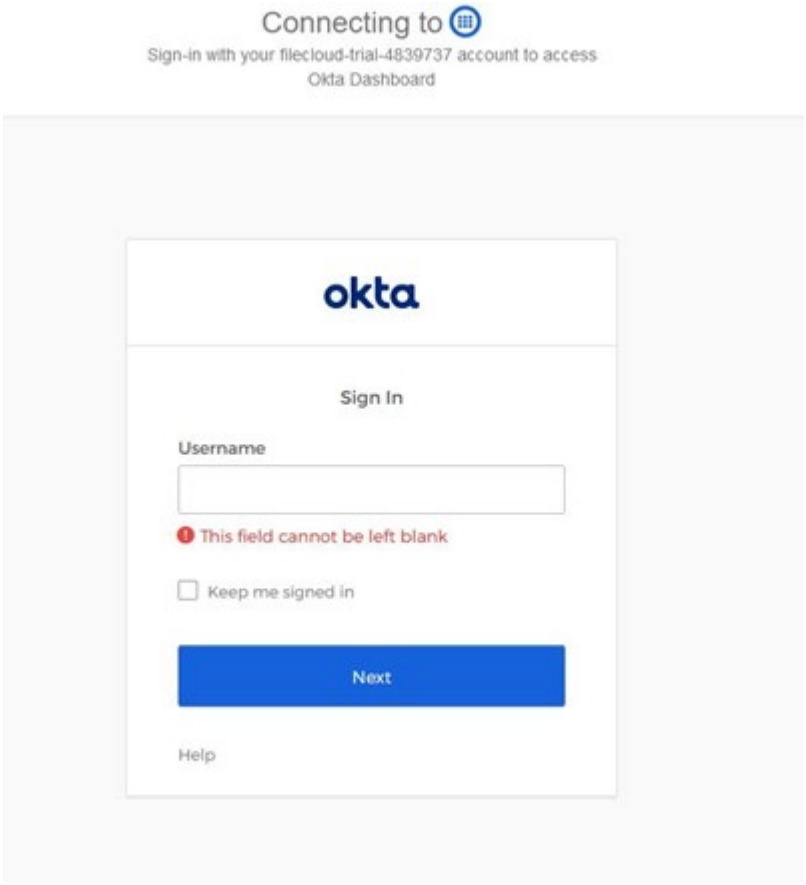
Information on plugin installation is available here:

https://help.okta.com/oie/en-us/content/topics/browser-plugin/admin-plugin-settings.htm

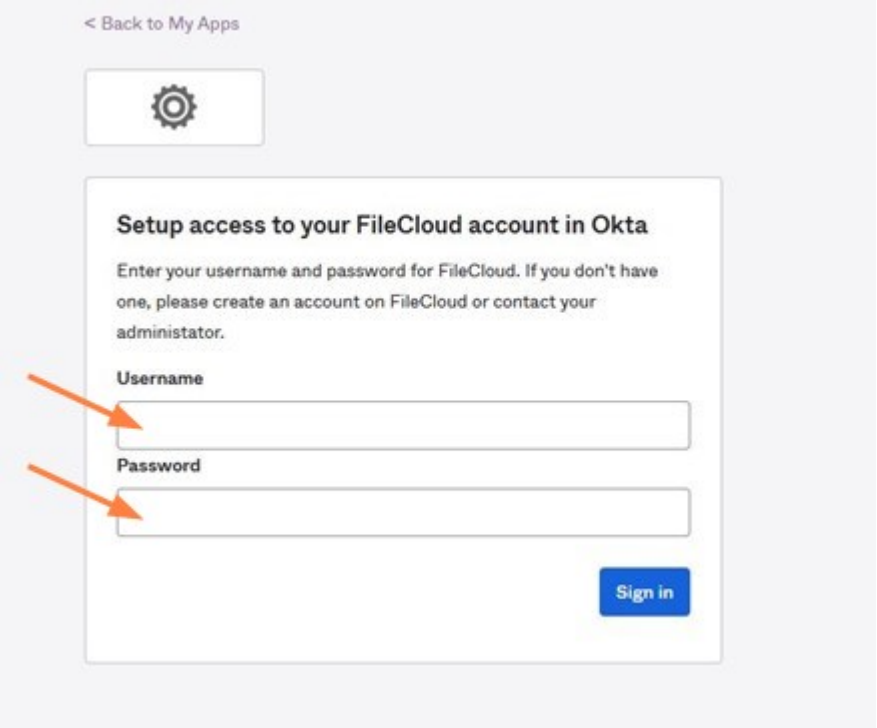
Users log in to FileCloud using the plugin

Users can sign in to the user portal or admin portal with SSO using the Okta plugin..

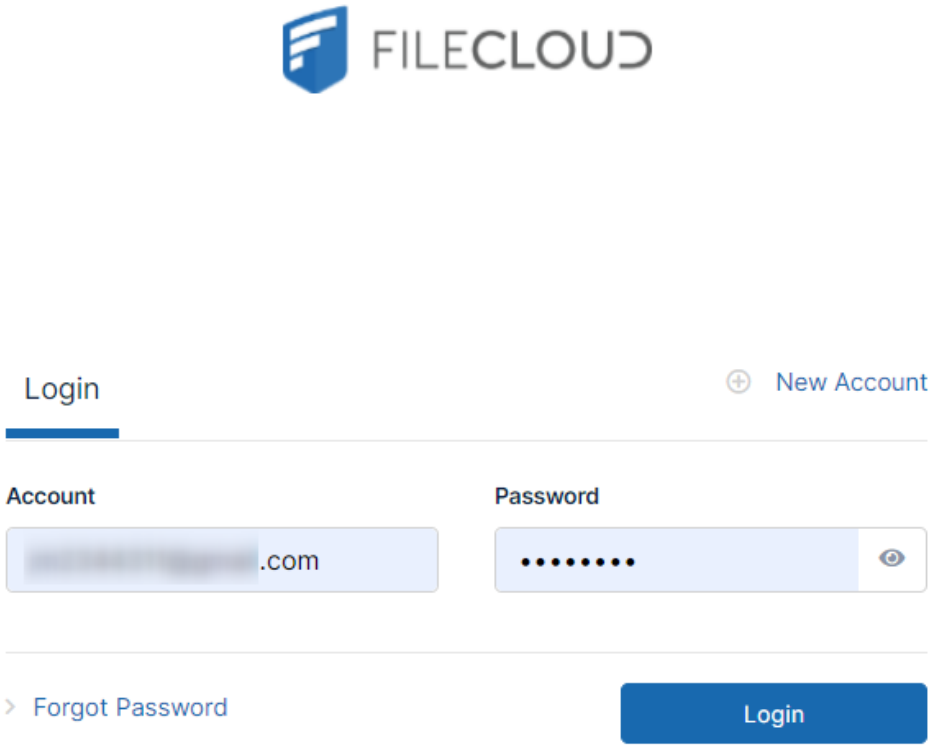
1. In a browser where the Okta Plugin is installed, the user clicks the Okta plugin icon, and selects the FileCloud application.
2. If the user is not already logged in to Okta, they are prompted to log in.



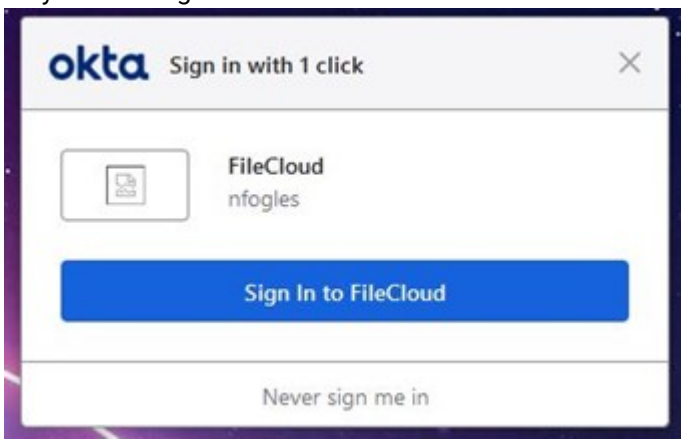
3. In the plugin **Setup access** dialog box, the user enters their FileCloud **Username** and **Password**. In the future, when they open the plugin, they will not be prompted to enter credentials again.



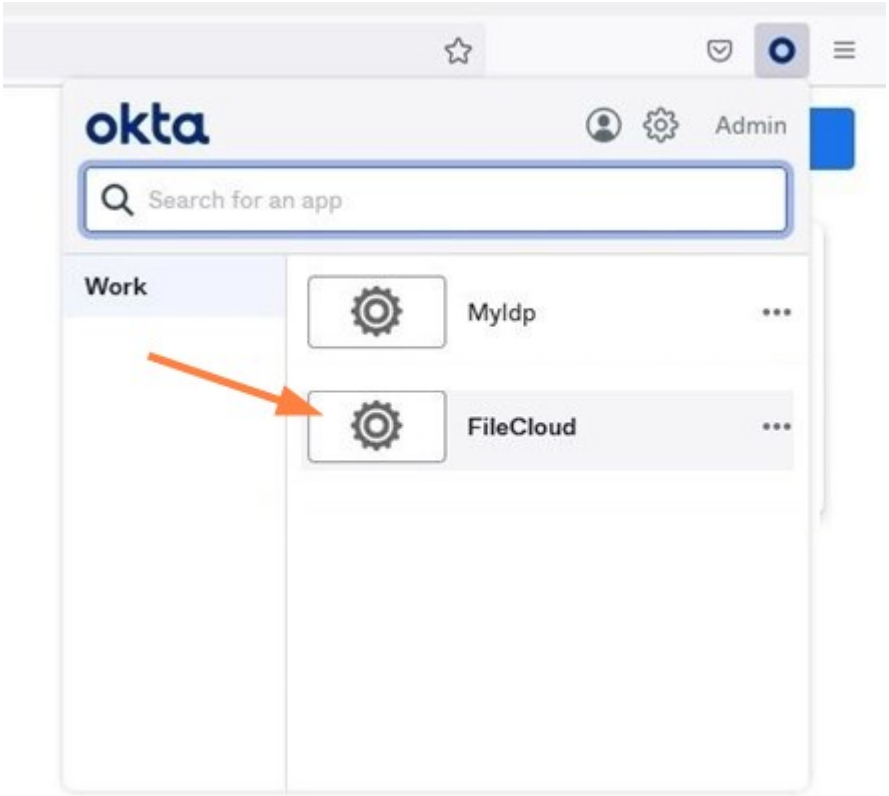
4. The browser redirects the user to the FileCloud login page in the Okta Admin Panel. The login screen with credentials filled in may appear first, and after a few seconds the FileCloud user portal should open (the user does not need to click **Login**).



Depending on the browser, when the user accesses the FileCloud login page again, the plugin may offer to log in for them:



Alternately, the user can access the application by choosing it directly in the plugin:



Integrate Google with FileCloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator you can integrate Google and FileCloud so that your Google users can access their FileCloud account without having to enter their credentials a second time.

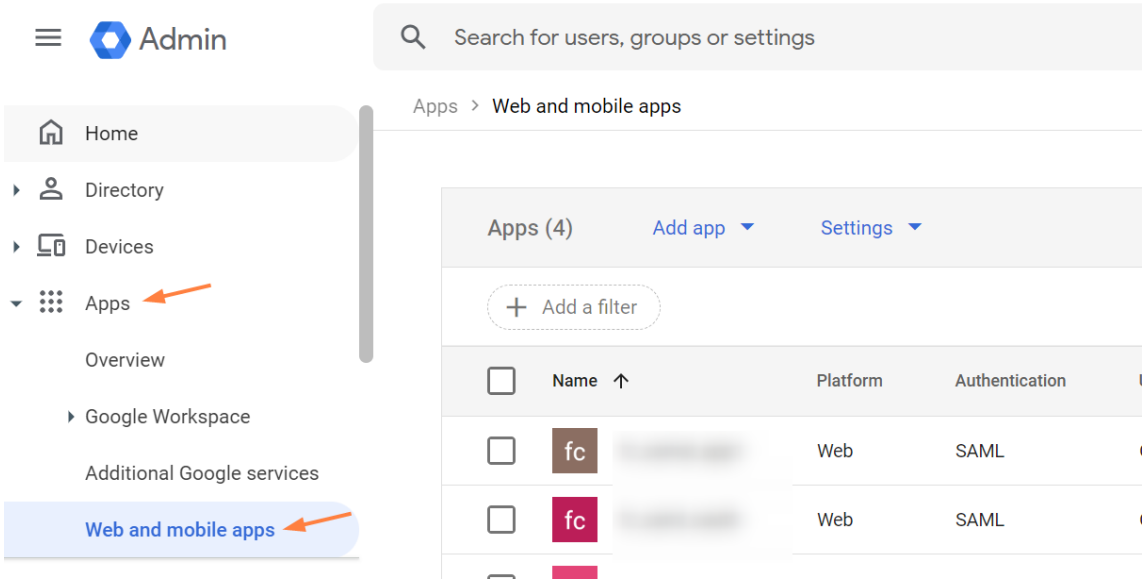
When FileCloud is integrated with Google, Google is configured as an Identity Provider (IdP) and FileCloud acts as the Service Provider (SP).

Sync a user's FileCloud and Google groups
By default, this integration does not synchronize a user's SSO groups and FileCloud groups each time a user logs in with SSO. This can result in unauthorized access to content as well as missing access where it's needed. To prevent this:

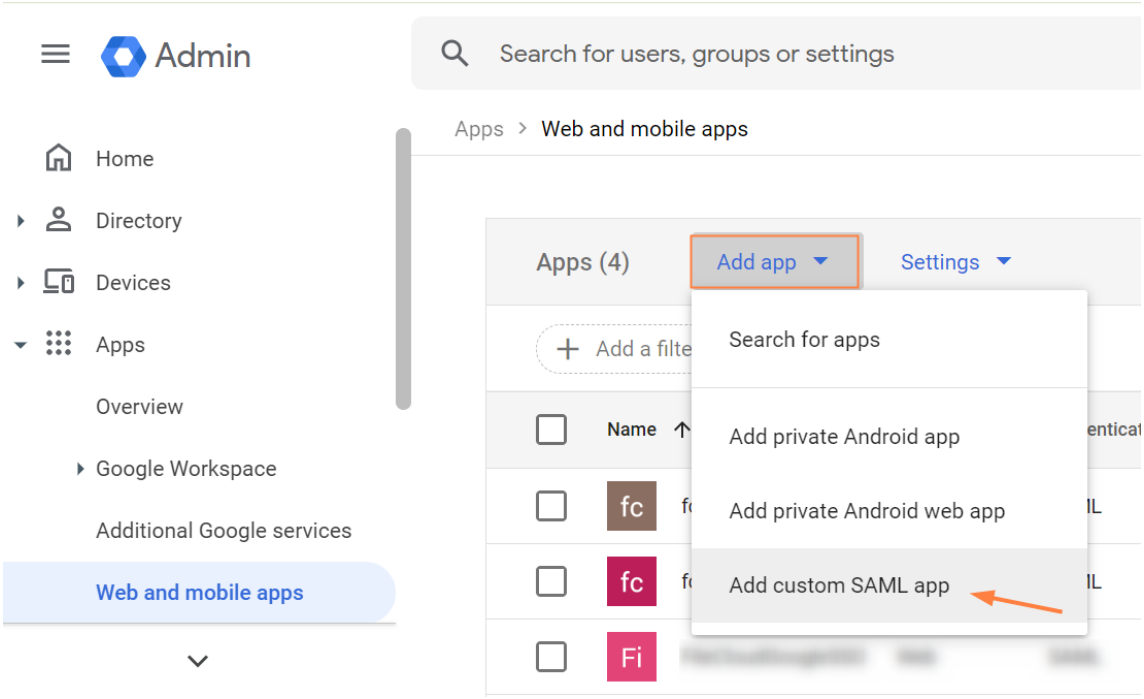
1. Complete step 9 in the procedure below.
2. Complete the step in **Syncing Group Changes on Every Login**, below.

To configure FileCloud with Google:

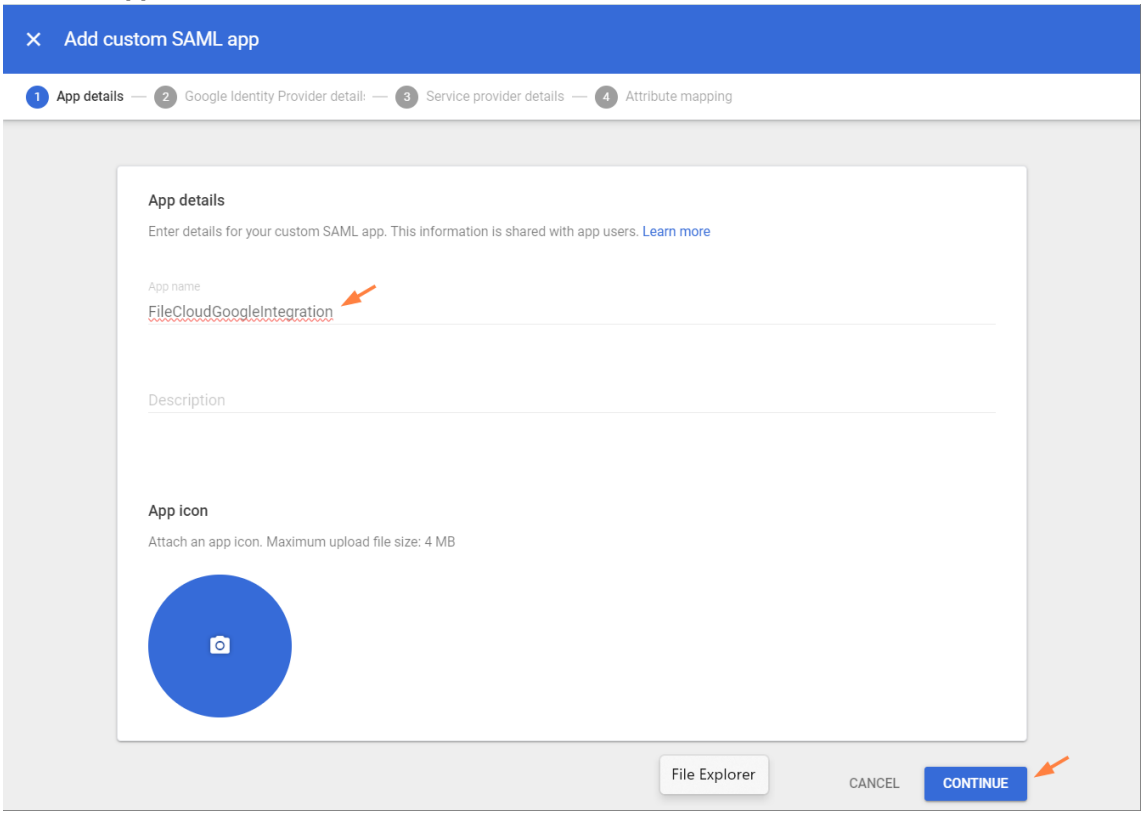
1. Log in to the Google Workspace Admin Center at admin.google.com.
2. In the left navigation pane, go to **Apps > Web and mobile apps**.



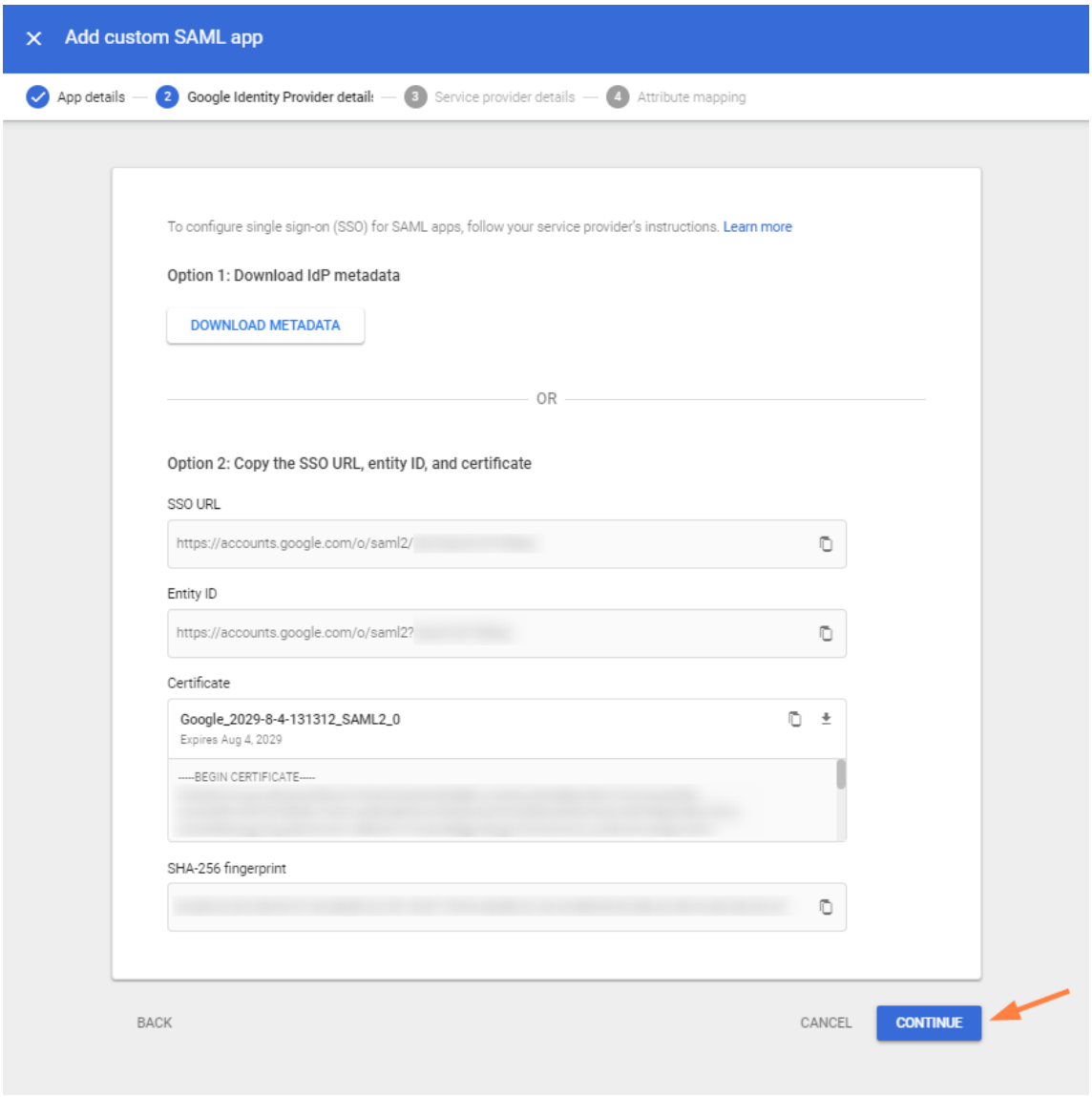
3. Click **Add app** and choose **Add custom SAML** app.



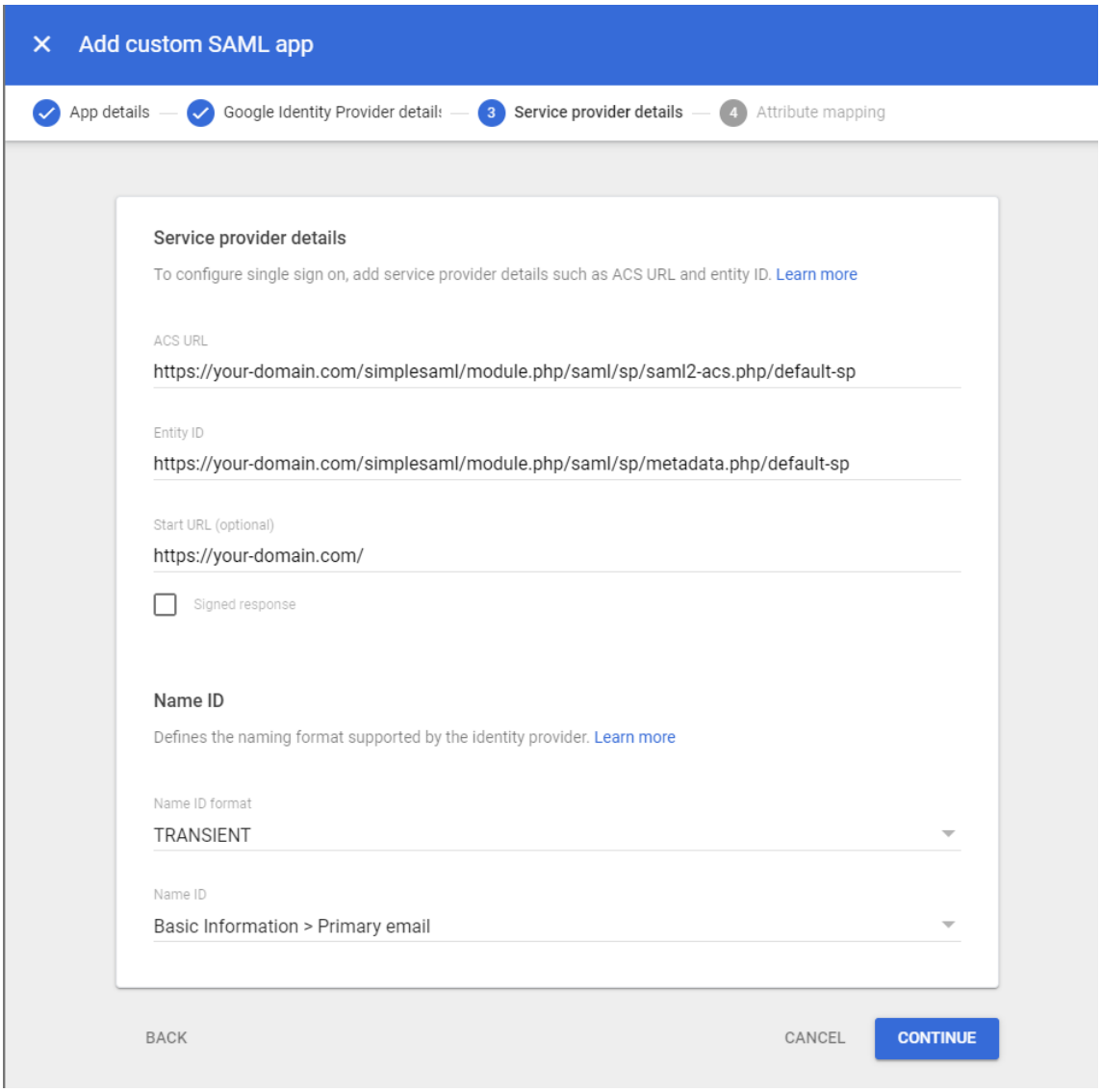
4. Enter an **App name**, and click **CONTINUE**.



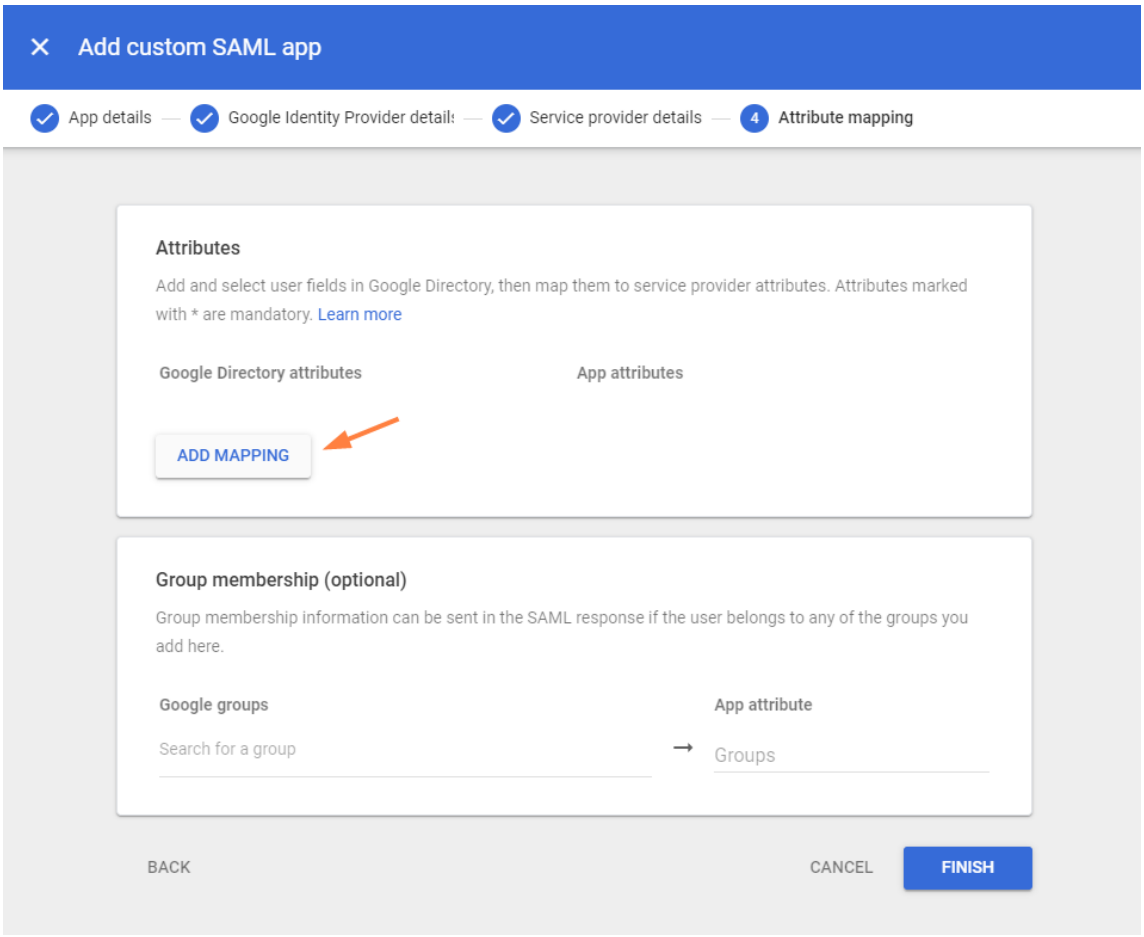
5. Click **CONTINUE**.



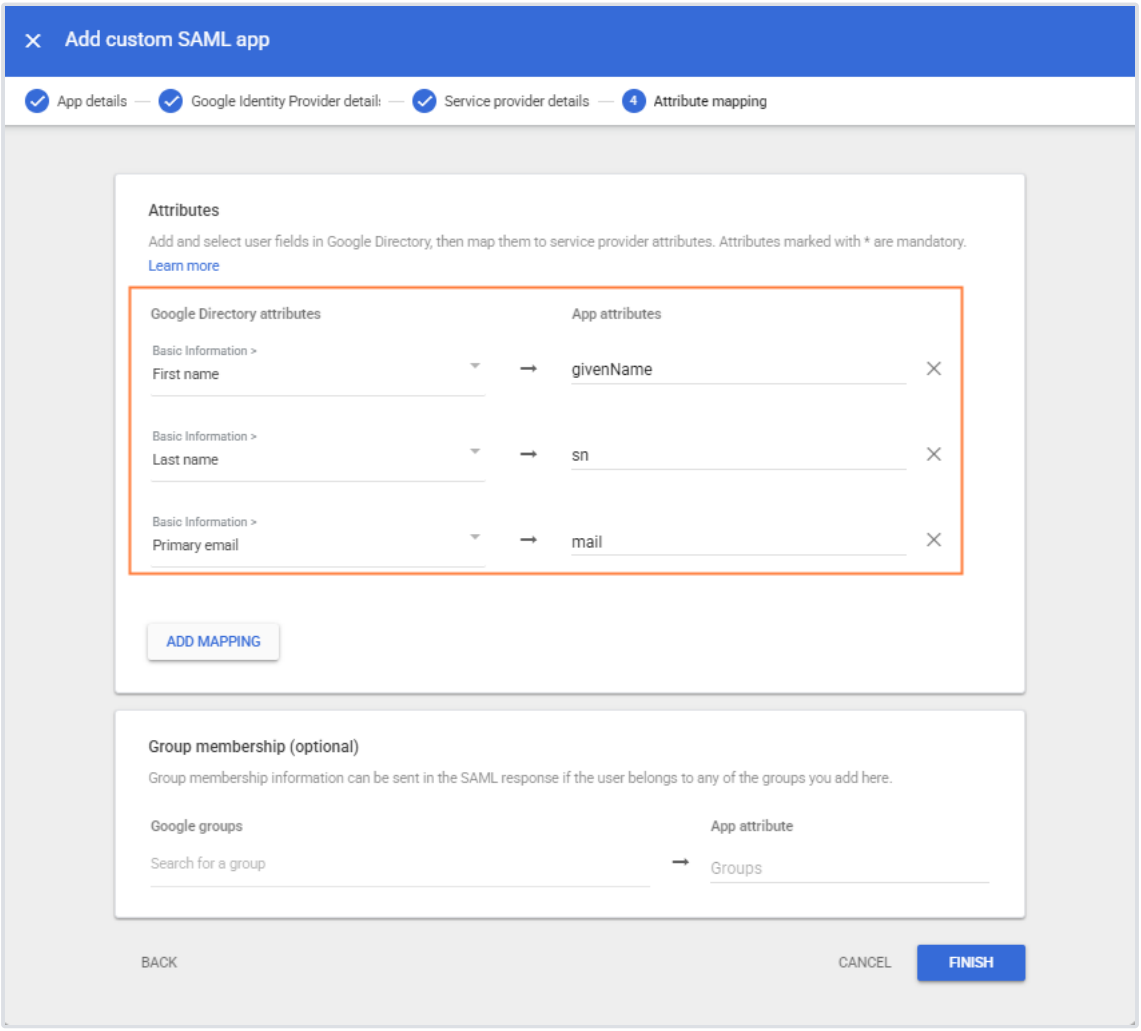
6. Fill in the fields as follows, replacing http://your-domain.com with your FileCloud domain. Click **CONTINUE**.
   ACS URL: https://your-domain/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
   Entity ID: https://your-domain/simplesaml/module.php/saml/sp/metadata.php/default-sp
   Start URL: https://your-domain/
   Name ID Format: **TRANSIENT**
   NameID: **Basic Information > Primary Email**



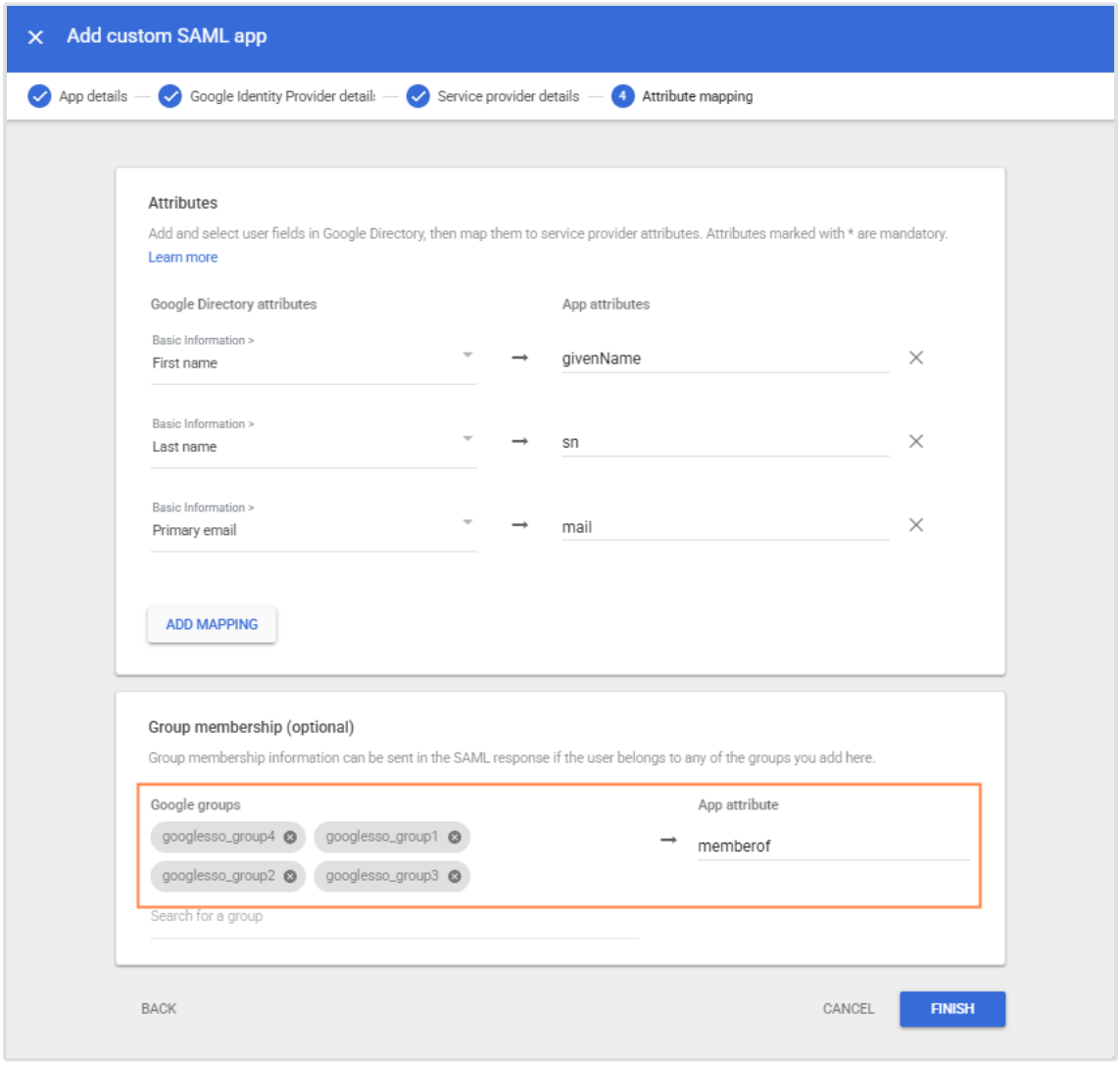
7. Click **ADD MAPPING**.



8. Choose the **Google Directory attributes** below, and add the specific values shown to **App attributes**.

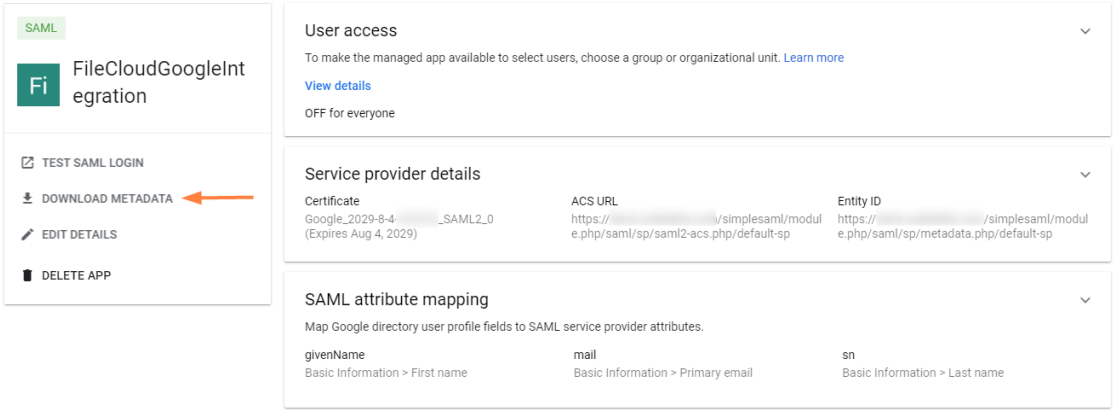
9. 

Optional: If you have chosen to sync FileCloud and Google groups on every login, under **Group membership**, set the attribute **memberof** to the Google groups each user may belong to.

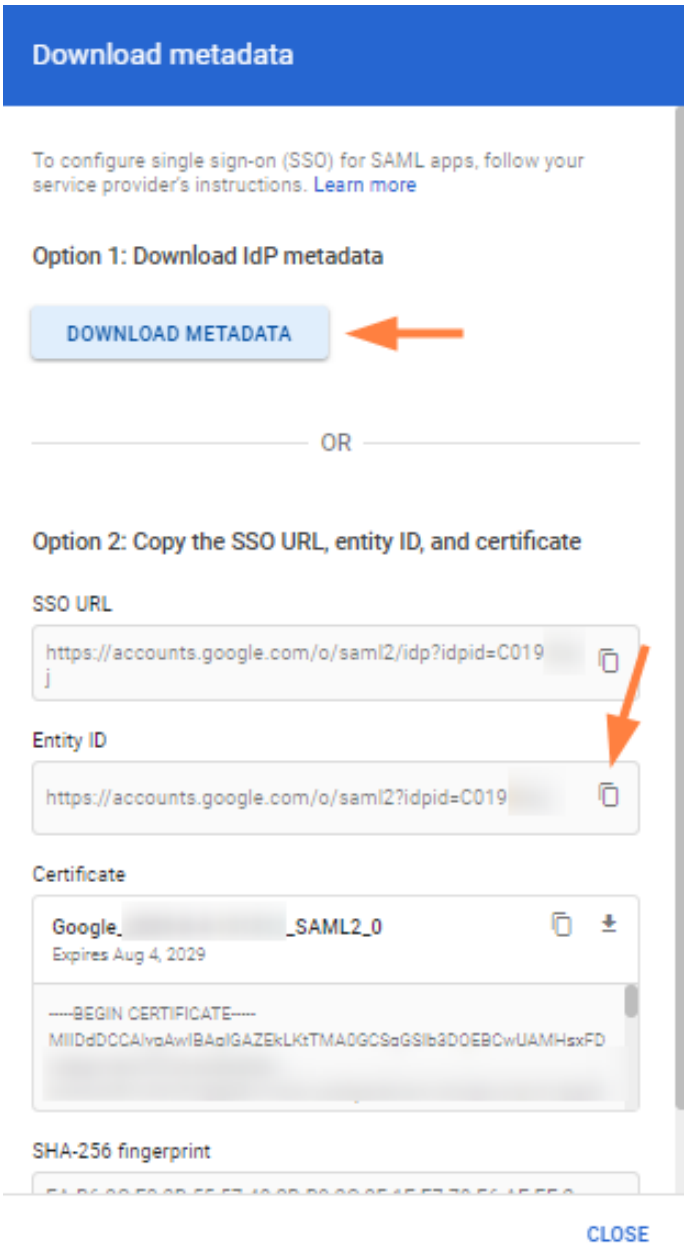


Note: To sync groups on every login, you must also complete the step in Syncing group changes on every login, below.

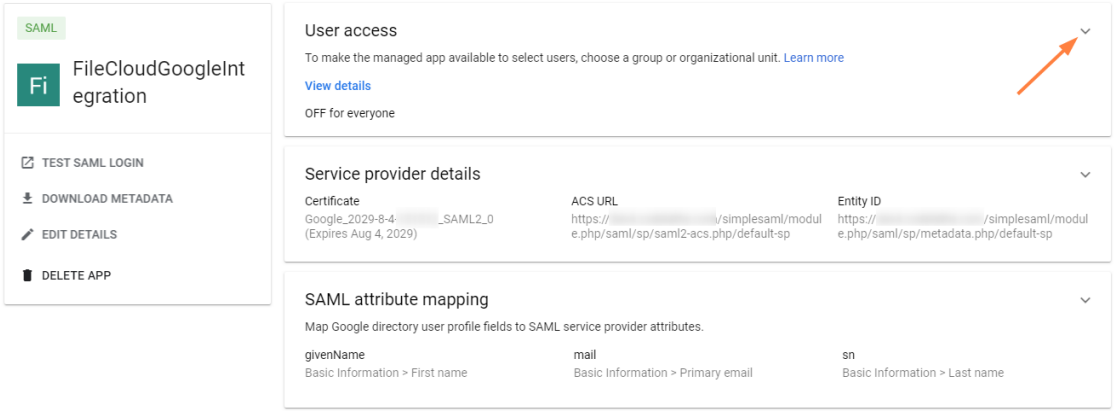
10. Then click **FINISH**.
11. In the screen that appears, click **DOWNLOAD METADATA**.



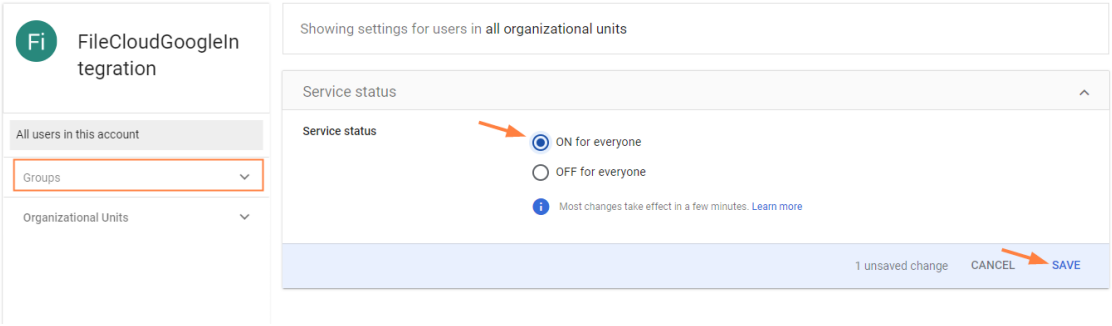
12. In the **Download metadata** popup, click **DOWNLOAD METADATA**.
    The file **GoogleIDPMetadata.xml** is automatically downloaded.
13. Click the copy icon next to **Entity ID**, and save it. You will need it to complete your configuration in FileCloud.



14. Click **CLOSE**.
15. Click the down arrow in the User access box.



16. Select **ON for everyone**.
    If you want to only enable this for certain groups, click the **Groups** down arrow and add the groups.



17. Click **SAVE.**

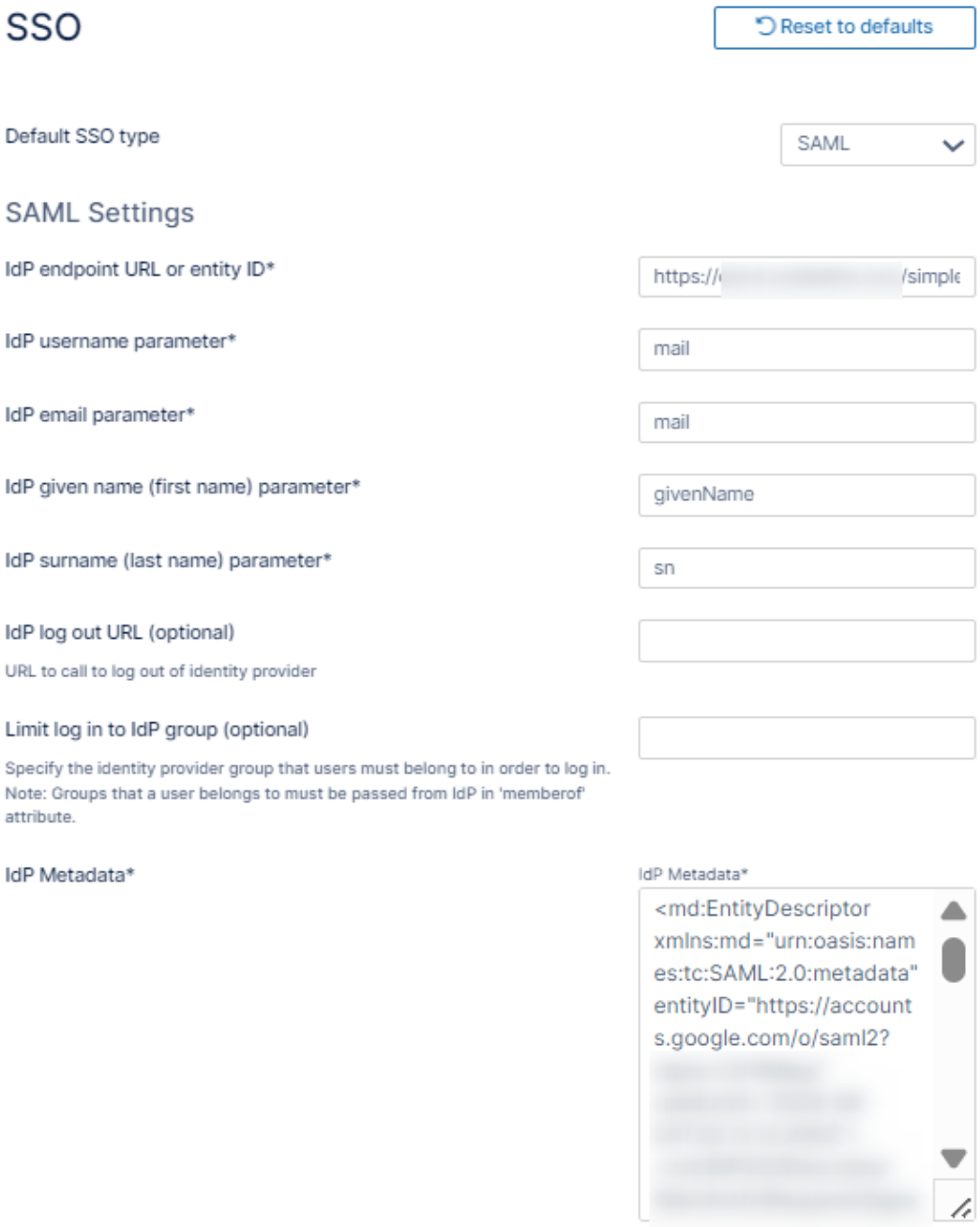
Configure Google SSO in the FileCloud admin portal

Now, add the values from your integration in the Google admin portal into the corresponding fields in FileCloud.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** .
   The **SSO** page opens.
2. In **Default SSO Type**, select **SAML**.

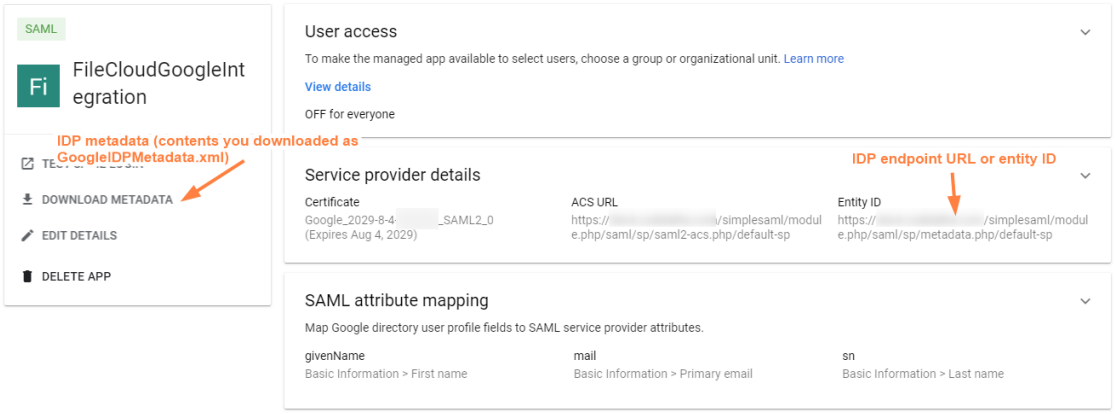


3. Fill in the settings under **SAML Settings**. The table below the image shows what to enter in each required IdP value.



Setting	Value
IdP endpoint URL or entity ID	Enter the value of Entity ID from your Google/FileCloud app in the Google admin portal, See the image below.

Setting	Value
IdP username parameter	mail
IdP email parameter	mail
IdP given name (first name) parameter	givenName
IdP surname (last name) parameter	sn
IdP log out URL	See SAML Single Sign-On Support
Limit log in to IdP group	See SAML Single Sign-On Support
IdP Metadata	Enter the content of the metadata file you downloaded from your Google/ FileCloud app in the Google admin portal. It should have been downloaded as GoogleIdPMetadata.xml.



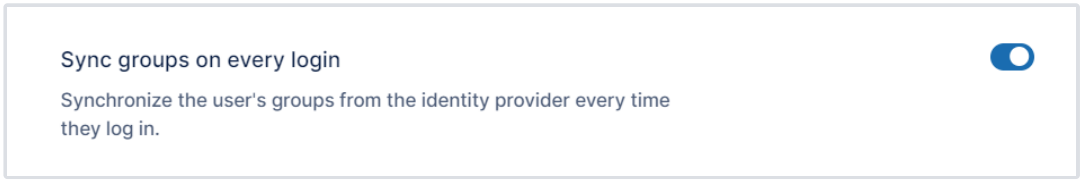
4. For help filling the remaining settings on the page, see Step 4 on page SAML Single Sign-On Support.
5. To display the SSO option on the user login page, see Step 6 on page SAML Single Sign-On Support

Syncing group changes on every login

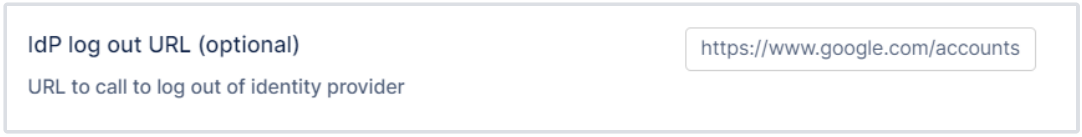
If changes to your users' group membership may affect the content they have access to, you may sync a user's group changes each time they log into FileCloud with their SSO login.

To configure SSO login to sync groups on each login:

1. In the FileCloud admin portal, go to **Settings > SSO**.
   a. Enable the setting **Sync groups on every login**.



   b. In **IDP log out URL (optional)** enter https://www.google.com/accounts/Logout?continue=https://appengine.google.com/_ah/logout?continue=**[https://your_filecloud_instance.com]**
   replacing **[https://your_filecloud_instance.com]** with your actual FileCloud server URL.



   Note: This is required, not optional for syncing groups on each login.
   ⚠ It will logout and close all the Google sessions in the browser, including Gmail.

3. Complete Step 12 under **To configure FileCloud with Google**, above.

Integrate OneLogin with FileCloud

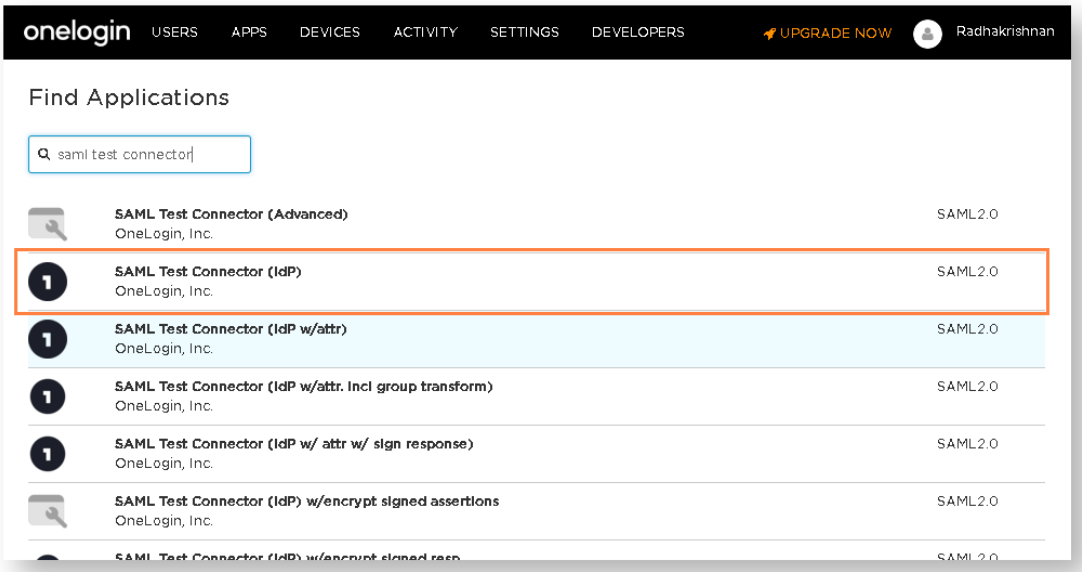
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

This article describes how to integrate OneLogin as an SSO provider with FileCloud.

Pre-requisite: The mcrypt module must be installed on FileCloud. In Windows, it should be installed by default. In Linux, if mcrypt is not installed, it must be installed

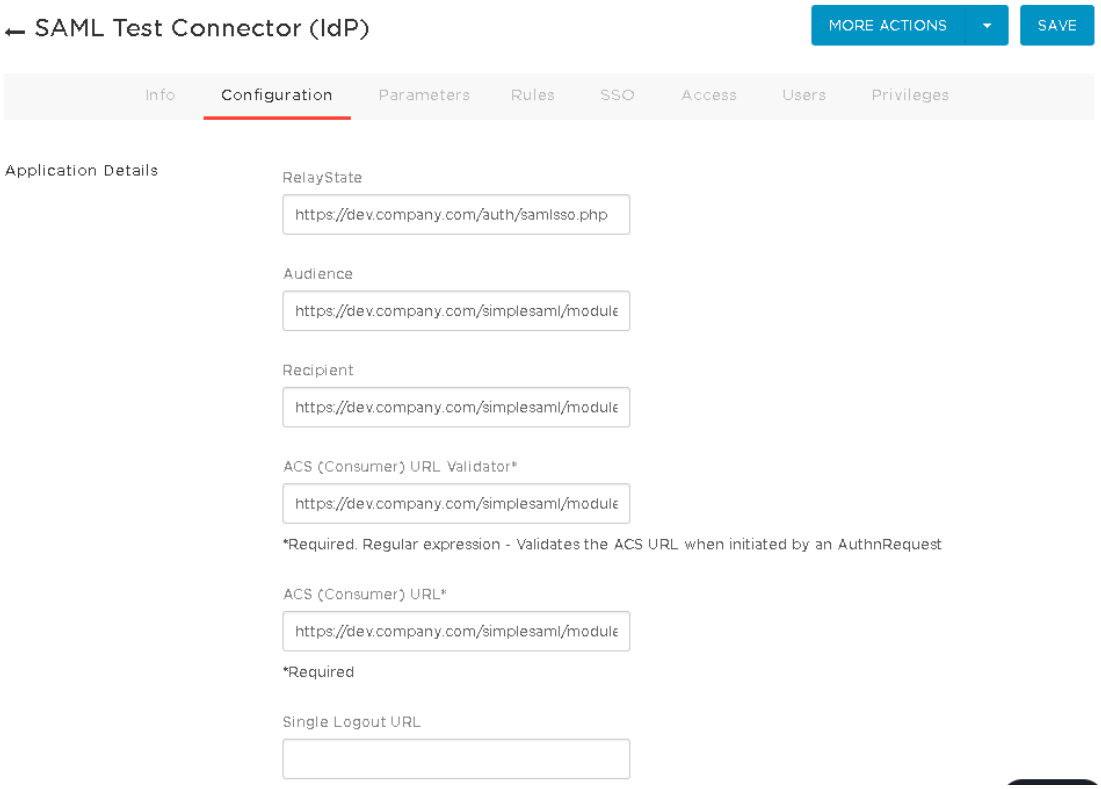
OneLogin: Create App Connector

1. Login into the OneLogin web UI.
2. Click **Apps > Add Apps**.
3. Search for **SAML Test Connector** and select **SAML Test Connector (IdP)**.



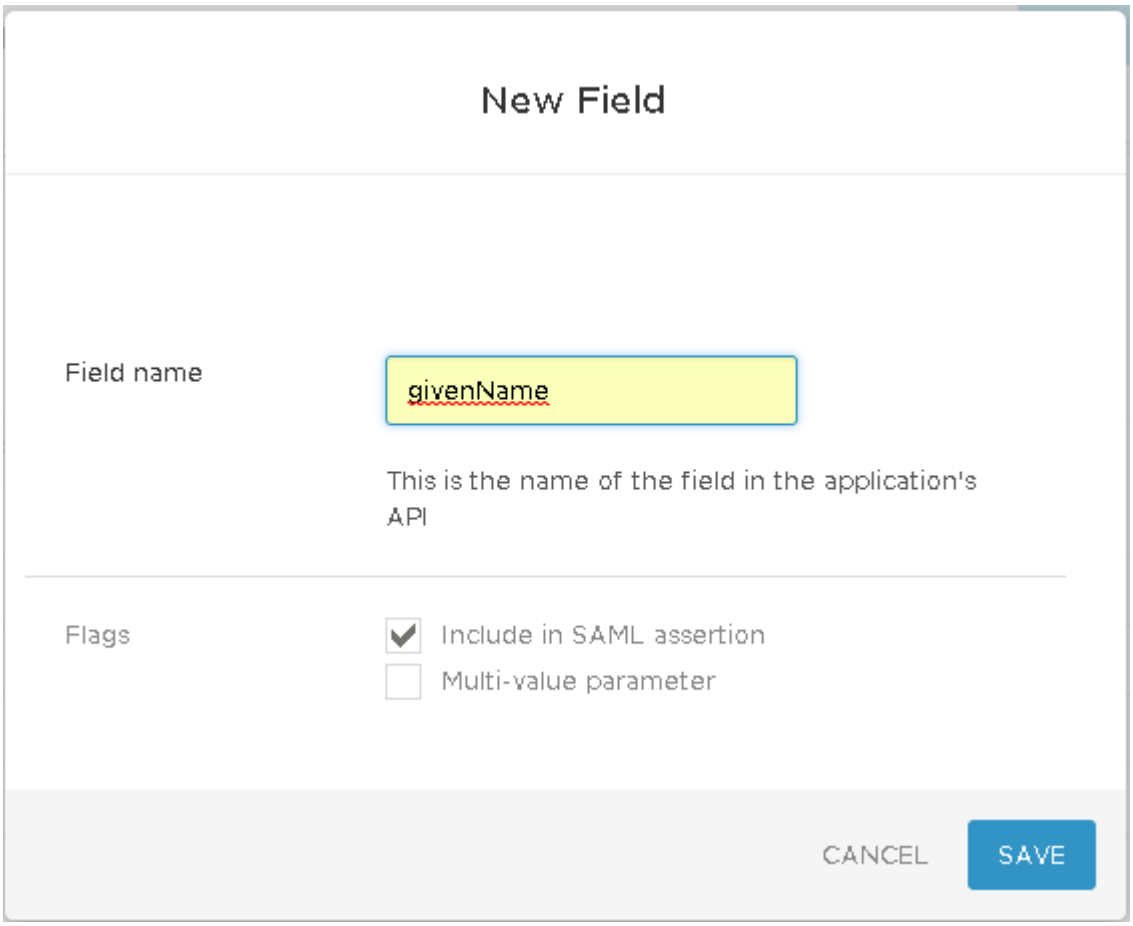
4. In the add screen, enter a name for the connector. For example, something like **FileCloud Connector**.
5. Click **Save**.
6. Open the created connector and click the **Configuration** tab.
7. Fill the following values into the configuration tab. Replace **dev.company.com** with your FileCloud site.

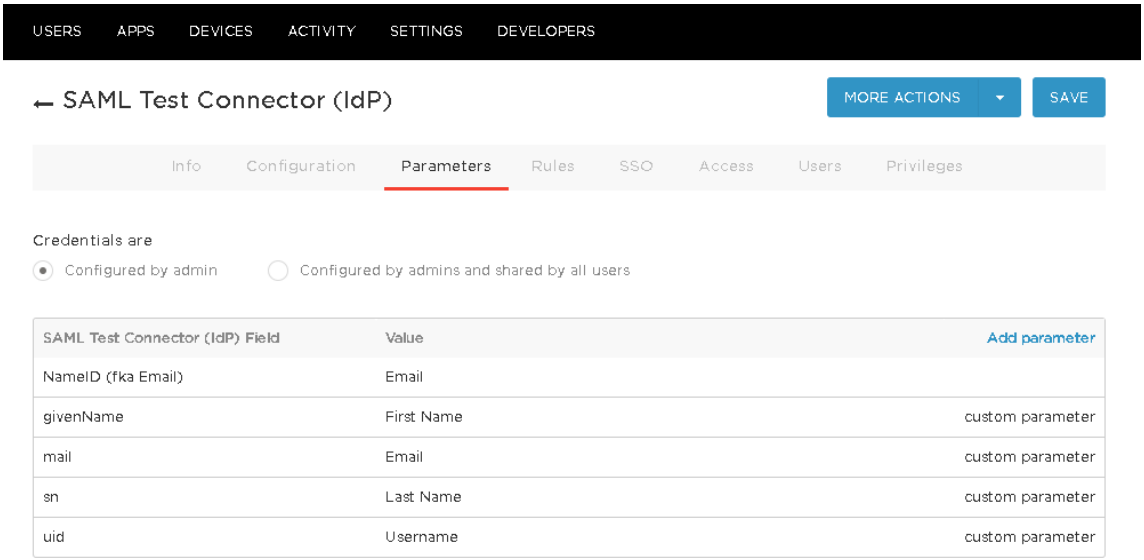
Configuration	Value
RelayState	https://**dev.company.com**/auth/samlsso.php
Audience	https://**dev.company.com**/simplesaml/module.php/saml/sp/metadata.php/default-sp
Recipient	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL Validator*	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL*	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp



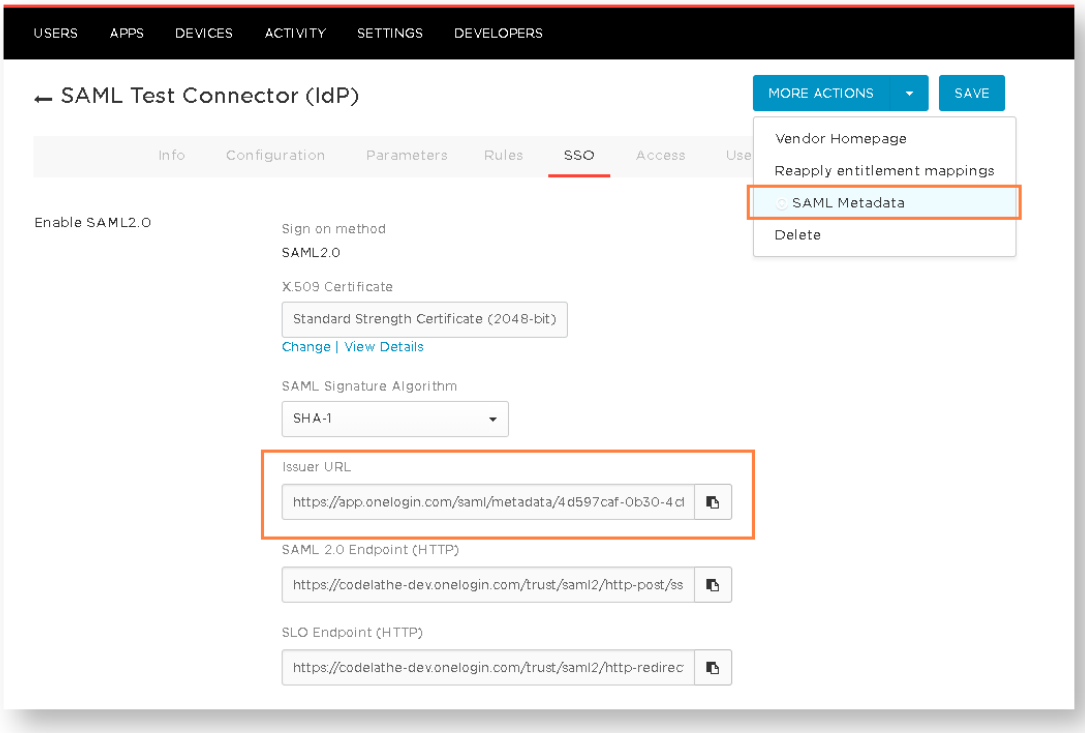
8. Once the configuration tab is completed, click the **Parameters** tab.
9. Add the following four parameters:

Field name	Flags	Value
givenName	Include in SAML assertion	First Name
mail	Include in SAML assertion	Email
sn	Include in SAML assertion	Last Name
uid	Include in SAML assertion	Username





10. Save these changes. Then click the **SSO** tab.
11. In the **SSO** tab, copy and save **Issuer URL**.
12. Click **More Actions > SAML Metadata** and download the metadata file.



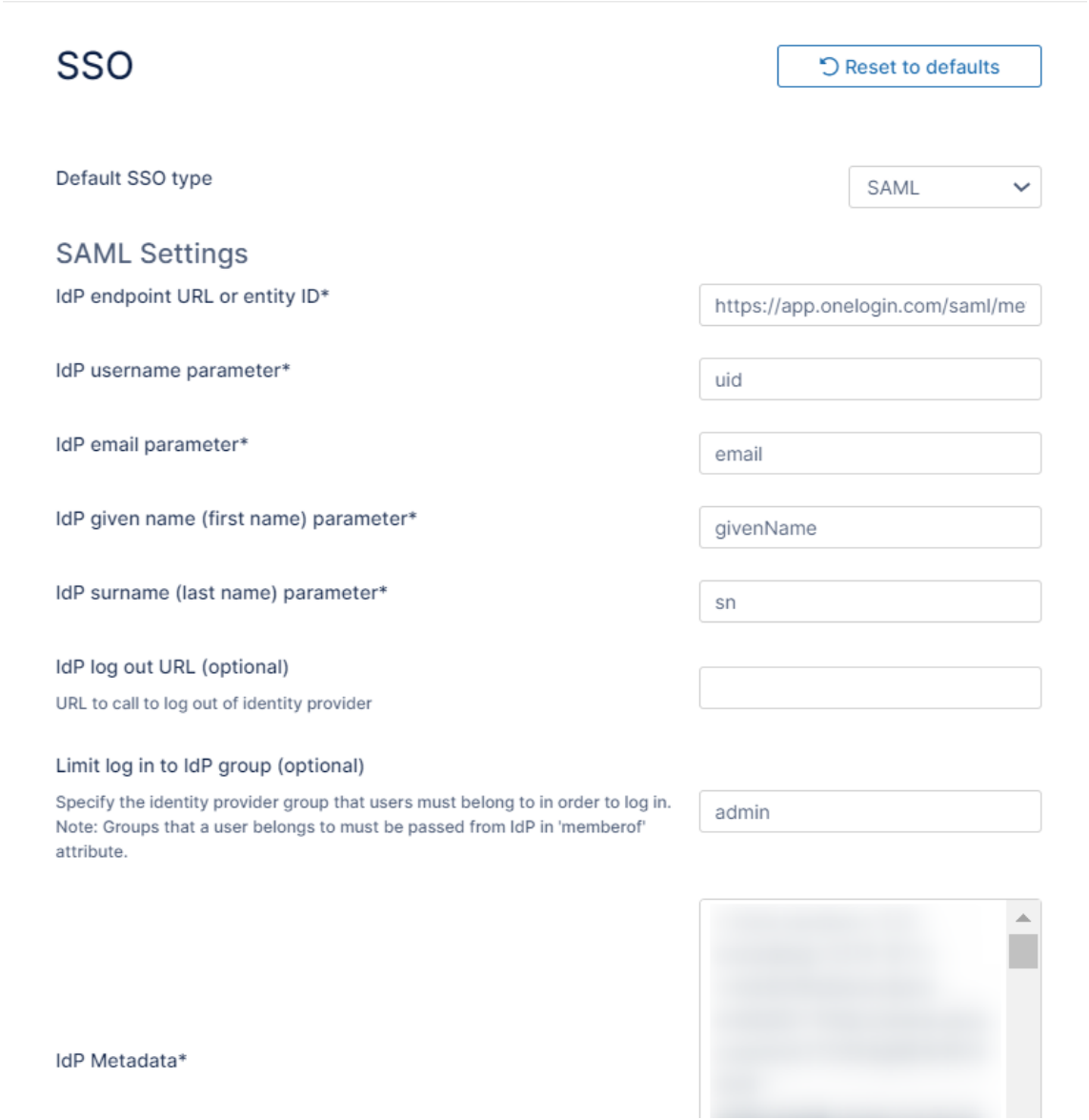
13. Finally, add users to the newly created FileCloud Connector either individually or as group.

Integrate FileCloud with OneLogin SSO

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO.**
   The **SSO** page opens.
2. In **Default SSO Type** choose **SSO**.
3. Use the following table to fill in the SAML configuration.

SAML Settings	Value
IdP Endpoint URL	**Issuer URL** saved in the previous section from OneLogin SSO tab
IdP Username Parameter	uid
IdP Email Parameter	mail
IdP Given Parameter	givenName
IdP Surname Parameter	sn

SAML Settings	Value
IdP Metadata	Copy and the paste the contents of SAML metadata from OneLogin.



4. Save the changes.

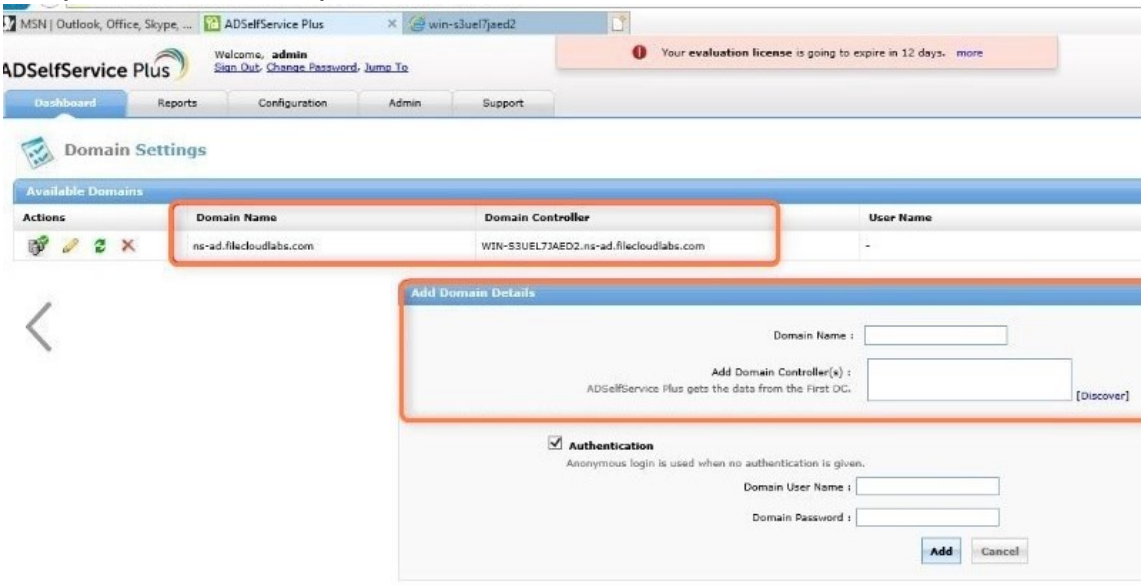
Integrate ADSelfService Plus with FileCloud

Integrate ADSelfService Plus with SimpleSAML SSO

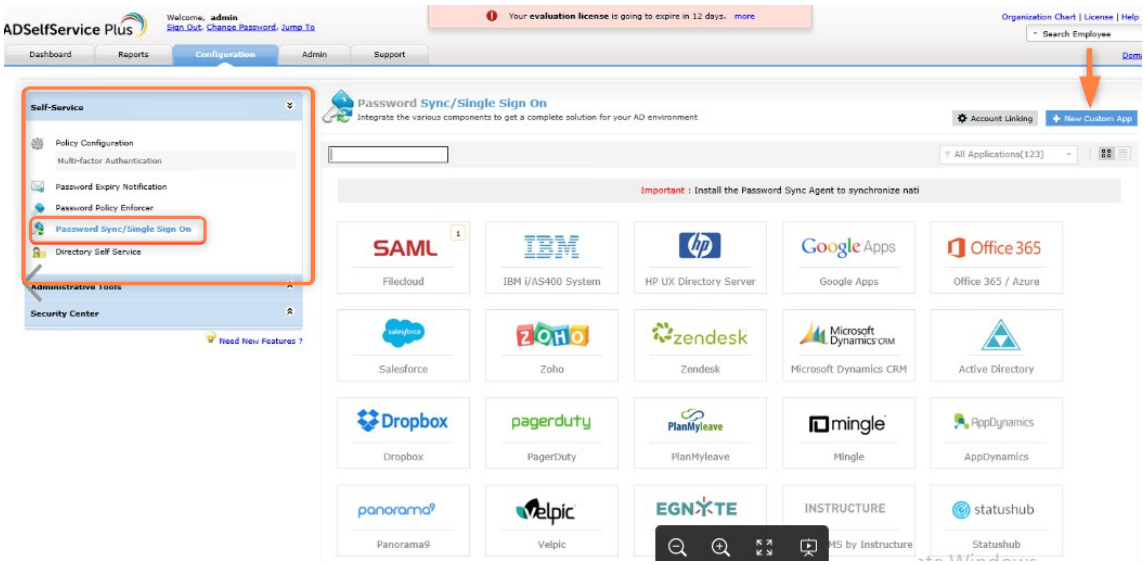
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

Step 1: Install ADSelfService Plus and configure it to integrate with SimpleSAML SSO in FileCloud

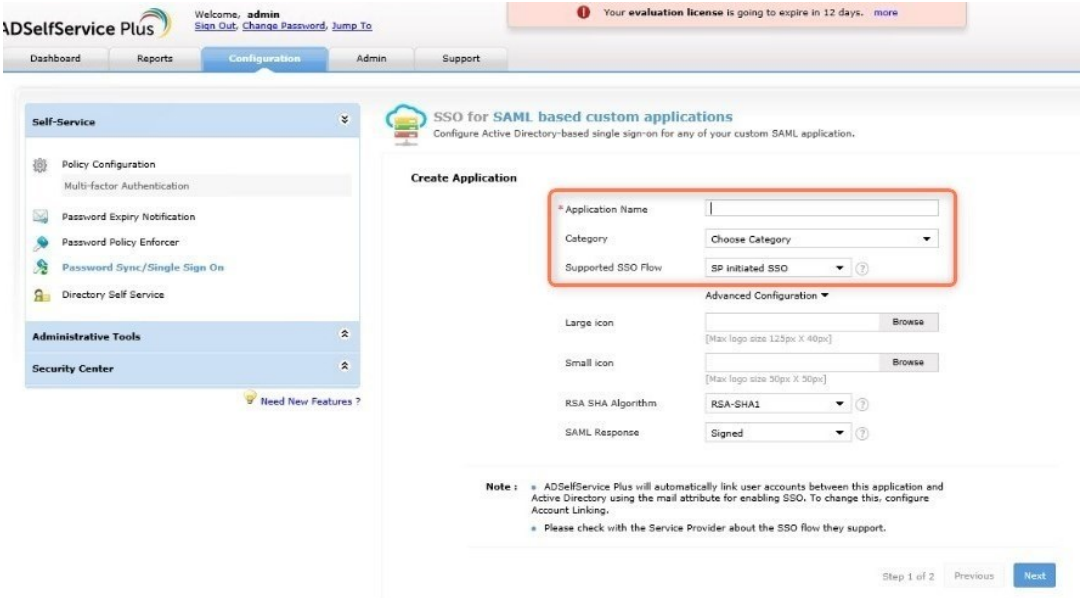
1. Install ADSelfService Plus.
2. Open the ADSelfService admin portal. Your URL should be similar to http://win-s3uexxjaed2:8888/authorization.do.
   The **Dashboard** tab should be selected, and the server name should be similar to: win-s3uexxjaed2
3. If AD is already installed, **Domain Name** and **Domain Controller** are automatically detected and entered for you.
   If they are not automatically entered, in **Add Domain Details**, enter them, and click **Add**.



4. Click the **Configuration** tab.



5. In the navigation bar, expand **Self-Service** and click **Password Sync/Single-Sign-On**.
6. Click **New Custom App**.
7. Fill in the following **Create Application** fields:
   a. In **Application Name** enter **FileCloud.**
   b. In **Category** drop-down list, choose any option.
   c. In the **Supported SSO flow** drop-down list,choose **SP initiated SSO.**
   The **Large icon** and **Small icon** fields are optional. You can leave the defaults for the remaining fields.



8. To go to the **SSO for SAML based custom applications/Configure Application** page, click **Next.**
9. Fill in the following **Configure Application** fields:

a. In **Domain Name**, enter the domain name of your user's email address in AD.
For example, if the email address is fc@test.com, enter test.com as the domain name.
b. In **Display Name** enter any name.
c. In **SAML Redirect URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/metadata.php/default-sp
d. In **ACS URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/saml2-acs.php/default-s

10. Click **Save**.
11. Click **Download SSO certificate** in the upper-right of the page.
The **SSO/SAML Details** dialog box opens.



12. Click **Download Metadata file,** and save the metadata file (**metadata.xml**).

Step 2: In FileCloud, configure your SSO settings for ADSelfService Plus

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**.
The **SSO** page opens.
2. In **Default SSO Type**, choose **SAML**.
3. Fill in the SAML settings:
a. In **IDP Endpoint URL,**
open the metadata.xml file you downloaded, and copy the URL after entityID. It should look similar to: entityID="http://yourFileclouddomainname:8888/iamapps/ssologin/custom_saml_10000/e6c2b84d31da852eac8e0f88ee5c4703b9974c2f
b. In **IDP Username Parameter,** enter **mail.**
c. In **IDP Email parameter** enter **mail**
d. In **IDP Given Name Parameter** enter **givenName.**
e. In **IDP Surname Parameter** enter **sn.**
f. In I**DP Metadata** paste the entire contents of the metadata.xml file.

By default, ADSelfService Plus passes the **mail** attribute, and FileCloud creates the user from the username portion of the email address. For example, if the email is sam@fc.com, FileCloud creates an account with **sam** as the username.
If you want to pass **userPrincipalName** as the parameter, contact the ADSelfService support team to make necessary changes in the database to pass that parameter. For example, to pass **userPrincipalName** instead of **mail**, ADSelfService must add the following entry to their database:

```
"userPrincipalName":"uid"
```

After they have added the entry, set **IDP Username Parameter** to **uid**.

Integrating Multiple IDPs

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

In some cases you may want to use different IDPs for your users, for example, if your users sign in to FileCloud from different platforms.

Beginning with FileCloud version 20.1, you can configure up to six different IDPs (the default and five additional ones) for single sign-on (SSO). The configuration assigns an email domain to each IDP, and chooses which IDP to apply depending on the domain of the sign-in email address.

To configure multiple IDPs

1. Set up SSO, and configure your default IDP according to the instructions in SAML Single Sign-On Support. The Idp Configured on this UI is the default Identity Provider.
2. Rename the file idpconfig-sample.php to idpconfig.php in:
   - Windows: xampp/htdocs/config
   - Linux: /var/www/config
3. Open idpconfig.php.
4. Use the help comments in idpconfig.php to set the configuration parameter values for each IDP. If something is not applicable leave it empty.
   You can configure up to 5 IDPs in idpconfig.php. Attach the suffix _1, _2 , _3, _4, or _5 to the parameters for each one so that the system knows which IDP they refer to.
   Please Note that any email domains not added as part of TONIDOCLOUD_SAML_EMAIL_DOMAINS_1,TONIDOCLOUD_SAML_EMAIL_DOMAINS_2, TONIDOCLOUD_SAML_EMAIL_DOMAINS_3, TONIDOCLOUD_SAML_EMAIL_DOMAINS_4, TONIDOCLOUD_SAML_EMAIL_DOMAINS_5 will automatically be considered to be part of the default Identity Provider configured through the admin UI - Settings - SSO

5. Open cloudconfig.php at
   - Windows: xampp/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php

6. Add the following, and include up to five domains: These domains are the domains for the email address.
   `define("TONIDOCLOUD_SAML_DOMAINS_ALLOWED","domain1.com,domain2.com,domain3.com,domain4.com,domain5.com");`

   for
   example: `define("TONIDOCLOUD_SAML_DOMAINS_ALLOWED","gmail.com,optimum.com,comcast.net");`

   The domains are associated with the values for TONIDOCLOUD_SAML_EMAIL_PARAM_1, TONIDOCLOUD_SAML_EMAIL_PARAM_2, TONIDOCLOUD_SAML_EMAIL_PARAM_3, and so on in idpconfig.php.
7. Users must sign in with their email addresses so FileCloud can determine which IDP they are using.



For IDP initiated single sign-on, the IDP url, which is the entityID, must be passed as a query string parameter to the relay state URL.
`For example:`
`https://<FileCloudDomain>/auth/samlsso.php?entityid=<ENTITYID>`

To configure custom error messages for each IDP

With this functionality, you have the ability to configure custom SAML/SSO invalid sign-in messages for each IDP.

1. Open idpconfig.php in
   - Windows: xampp/htdocs/config
   - Linux: /var/www/config
2. Add the following:

```
define("TONIDOCLOUD_SAML_ERROR_MSG_n", "<error message>");

where n is the number of the IDP configured in idpconfig that the error message
applies to.
For example:

define("TONIDOCLOUD_SAML_ERROR_MSG_4", "<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
```

```
        <title>FileCloud SSO Authorization Page</title>
    </head>
    <link rel="stylesheet" href="bootstrap.min.css">
    <body>
    <div class="container">
    <h2 align="center"> <img src="../core/getcustomimage?type=login"></img></h2>
        <h2 align="center"><u>Single Sign-on Login</u></h2>
        <br/><br/>
        <p align="center">Failed to login automatically via SAML Single Sign-on
(SSO). <br/>Please return to the main login page and login normally. </p>
        <div align ="center">
           <p><b>^MESSAGE^</b></p>
        <br/>
        <A HREF="/" class="btn btn-primary btn-sm" role="button">Back to Login</A>
        </div>
        </div>
    <br/>
    </body>
</html>");
```

3. The value you enter for <error message> appears when your screen displays the **SSO Error Message** in the SAML Settings for the corresponding IDP.

   For more information, see **3. Configure Idp settings in FileCloud** on the help page SAML Single Sign-On Support.

(23.263a) Allowing Duplicate Usernames

To allow duplicate usernames for different domains

If you are using SSO, SSO API, or Active Directory (AD) to import users, FileCloud uses the imported user's email username (the portion before @) as the FileCloud username. However, by default, FileCloud does not allow creation of users with the same usernames.

If any of your users have multiple email addresses, there may be a situation where the email username (the portion before @) is the same but the domains are different in their multiple emails. In this case, FileCloud will attempt to convert the second email username (and any further emails with the same username) to the FileCloud username, which will fail because the username already exists.

However, if the multiple email addresses actually represent different users, you may use the following setting to enable creation of multiple users:

1. Open cloudconfig.php at
   - Windows: xampp/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Add the following and save:

```
define("TONIDOCLOUD_ALLOW_DUPUSERNAMES",1);
```

Now:
If you create a a user with the username **jocelynp** and email **jocelynp@gmail.com**, FileCloud creates a user with the username **jocelynp**.
Next, if you attempt to create a user with the username **jocelynp** and email **jocelynp@optimum.net**, FileCloud creates a user with the username **jocelynp_optimum**. This follows for any subsequent emails with the same username and a unique domain.

To configure custom settings for automatic account creation for each IDP

Beginning in FileCloud version 20.1, you have the ability to configure custom automatic account creation settings for each IDP.

1. Open idpconfig.php in
   - Windows: xampp/htdocs/config
   - Linux: /var/www/config
2. Add code such as the following, which enables new account to be created during login and automatically approved with Full User permissions. The code below configures settings for domain 1 because parameters are suffixed with _1. See To configure multiple IDPs, above for information about adding suffixes to IDP parameters.

```
/* Allow new account to be created during the login process, when authenticated
through this IDP
allowed values FALSE or TRUE */
define("TONIDOCLOUD_SAML_ACCOUNT_CREATION_MODE_1","TRUE");

/*
Set Status of new accounts created automatically when authenticated through this
IDP
0 - No Automatic approval, Admin has to approve account
1 - Automatically approve new accounts to Full User
2 - Automatically approve new accounts to Guest User
3 - Automatically approve new accounts to External User
*/
define("TONIDOCLOUD_SAML_AUTOMATIC_ACCOUNT_APPROVAL_1","1");
```

Note: Configure the settings for the main IDP in the Admin user interface in **Settings > SSO**. See **3. Configure Idp settings in FileCloud** on the help page SAML Single Sign-On Support. for instructions.

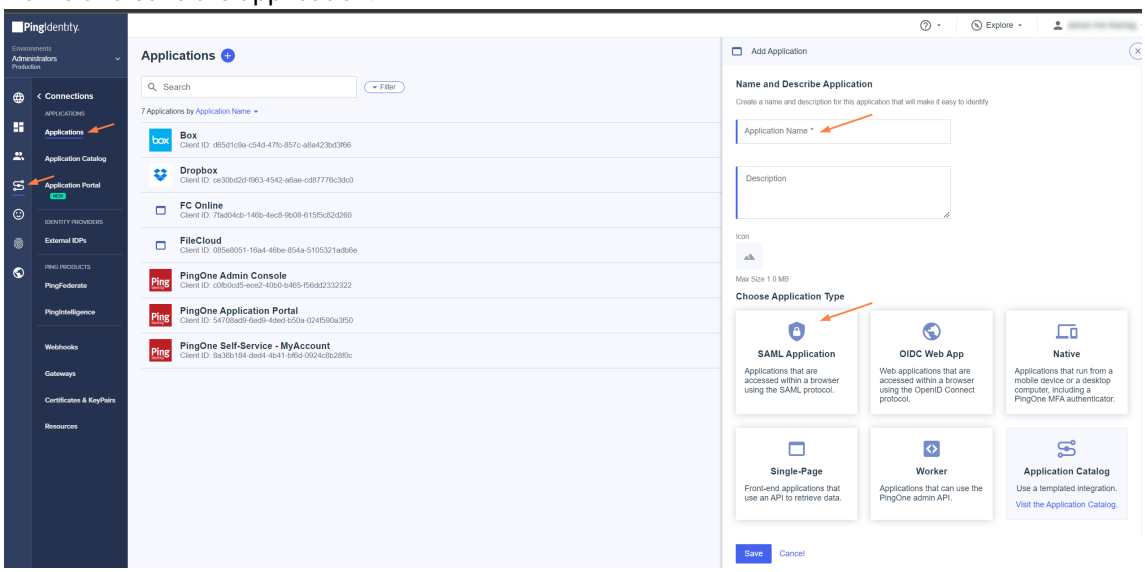
Integrate Ping Identity SSO with Filecloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

This article describes how to integrate PingOne as an SSO provider with FileCloud.

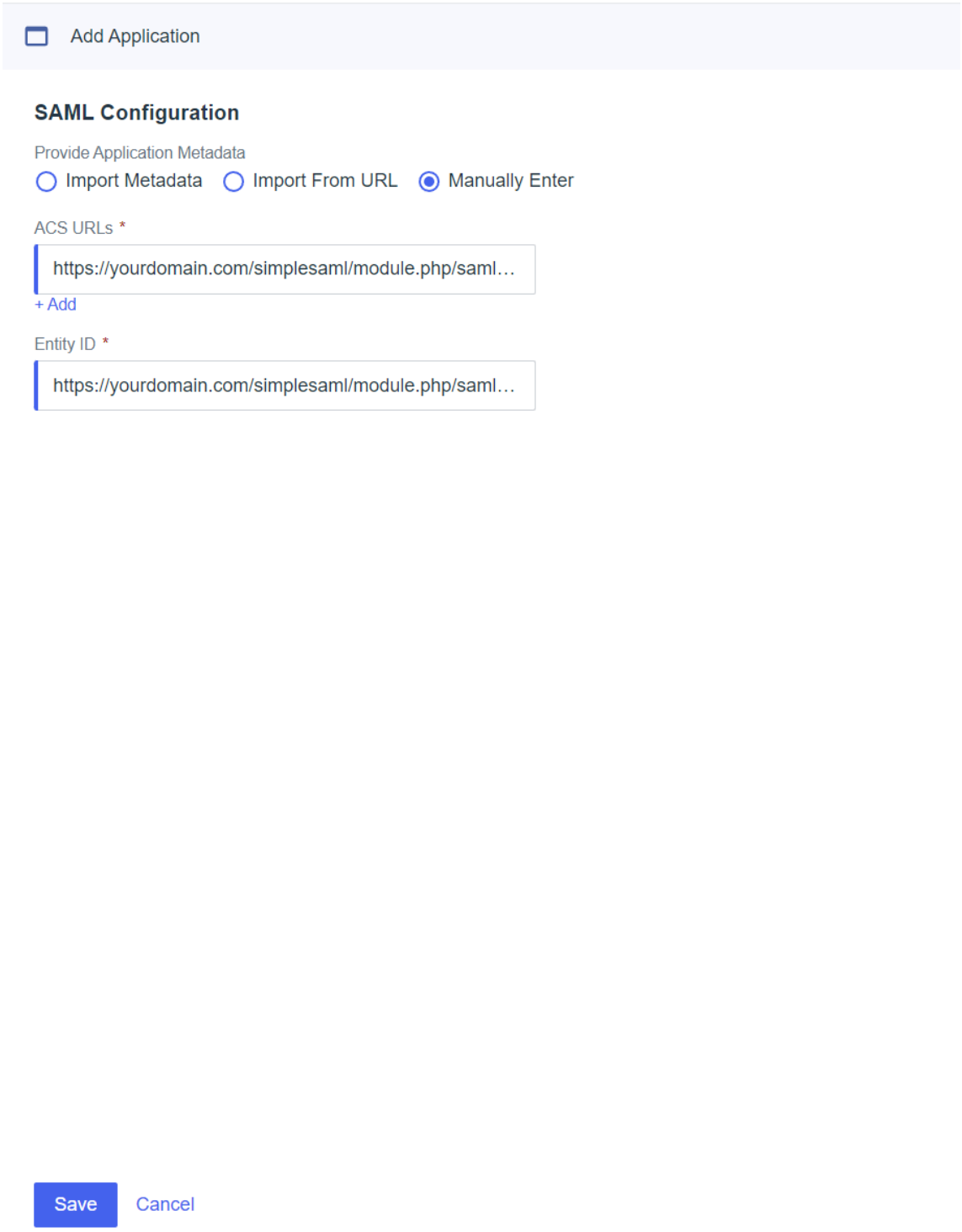
Configuration in Ping Identity portal

1. Log in to the Ping Identity dashboard, and click the **Connections** icon in the navigation panel.
2. Click **Applications**, then click the **+** button.
3. In the right panel, click **SAML Application**.
4. Name and save the application.



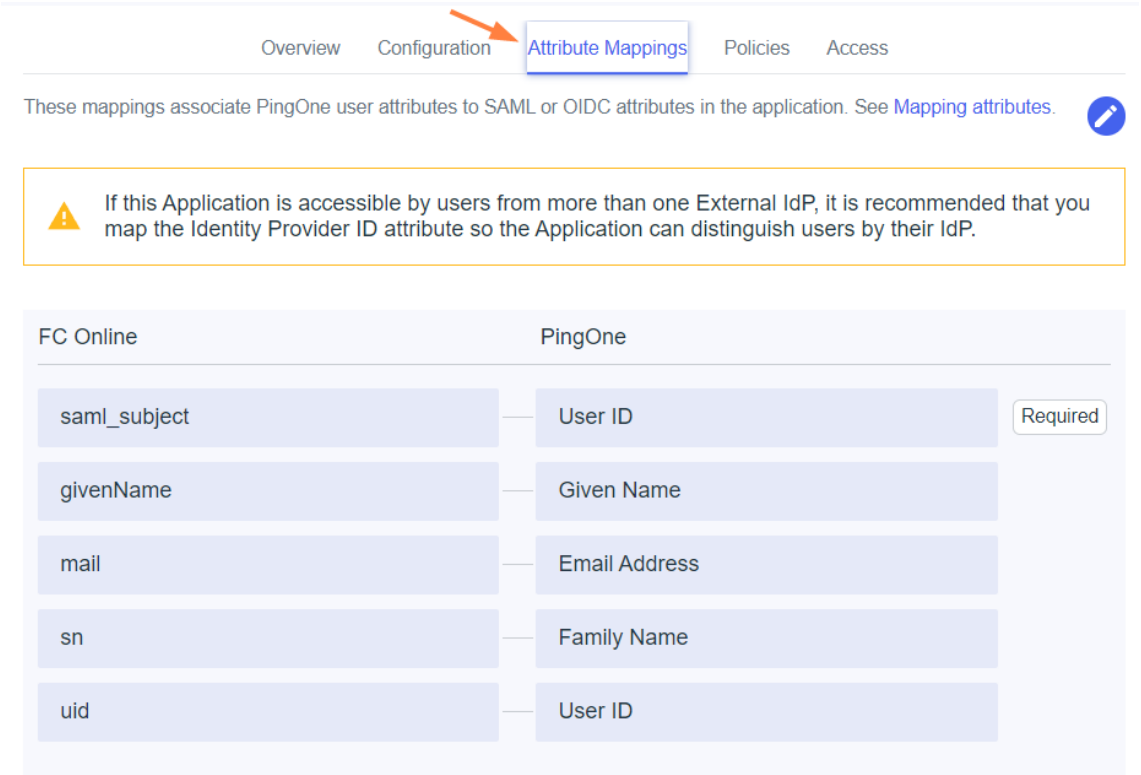
   The **SAML Configuration** screen appears in the right panel.
5. Select **Manually Enter**, and fill in the fields as follows:
   ACS URLs:
   https://<your_filecloud_url>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

   Entity ID:
   https://<your_filecloud_url>/simplesaml/module.php/saml/sp/metadata.php/default-sp

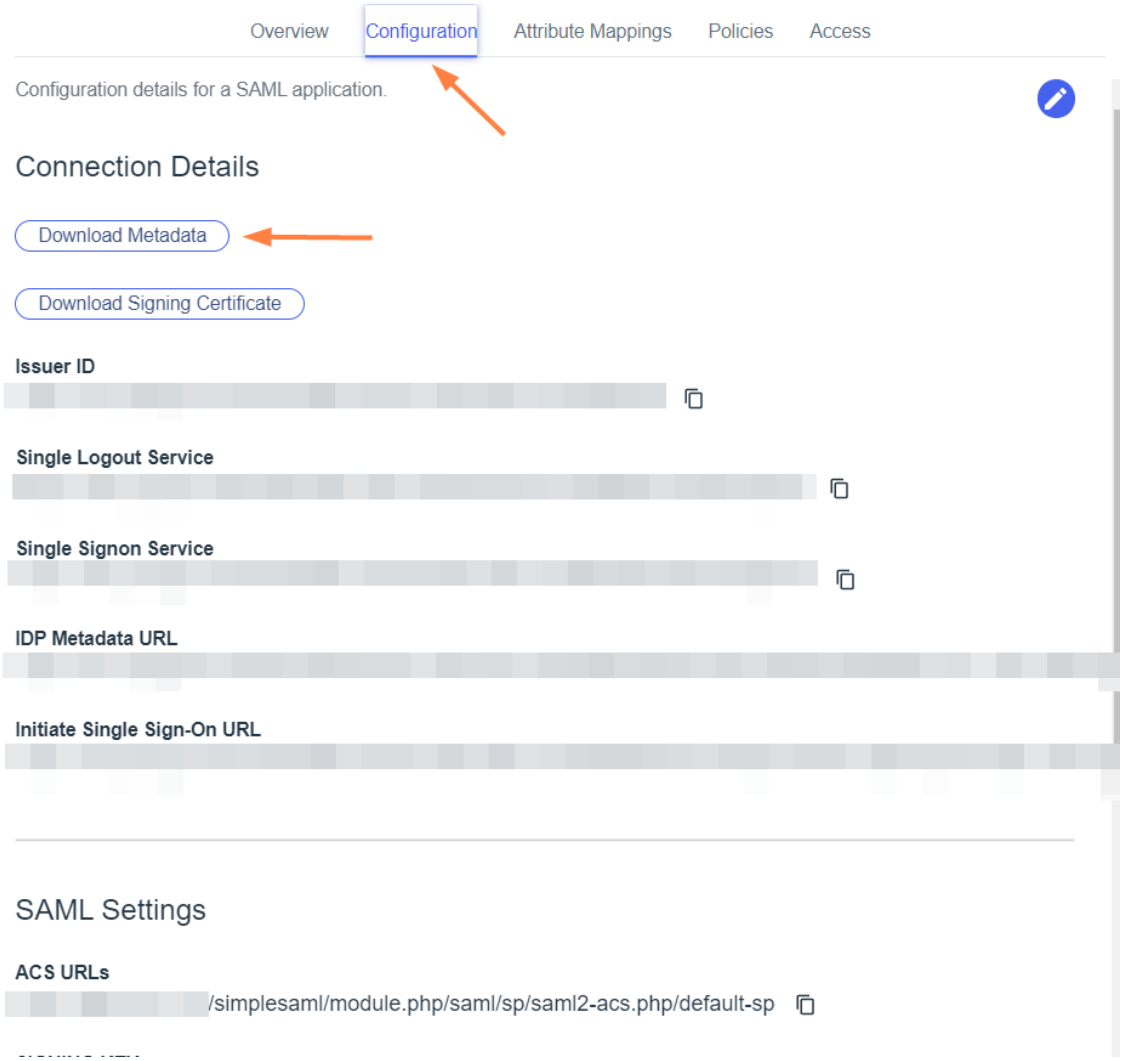


6. Click **Save**.
   Several tabs appear in the right panel.
7. Select the **Attribute Mappings** tab, then click , and add the following attributes:

Field name	Flags	Ping One Value
givenName	Include in SAML Assertion	Given Name
mail	Include in SAML Assertion	Email Address
sn	Include in SAML Assertion	Family Name
uid	Include in SAML Assertion	User ID

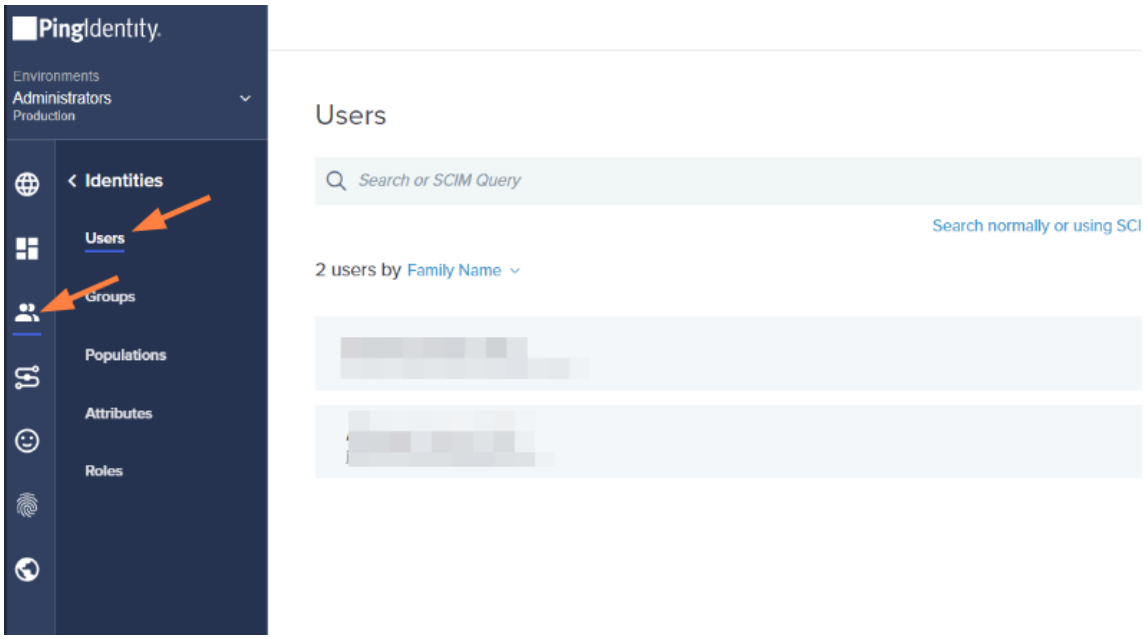


8. Click the **Configuration** tab.
9. To get a copy of the metadata file associated with the configuration, click **Download Metadata**. Save the file so you can enter its contents into the FileCloud admin portal.



Your application configuration is now complete.

10. Click the Identities icon in the Ping Identity navigation panel.
11. Click **Users**, and then add your users.

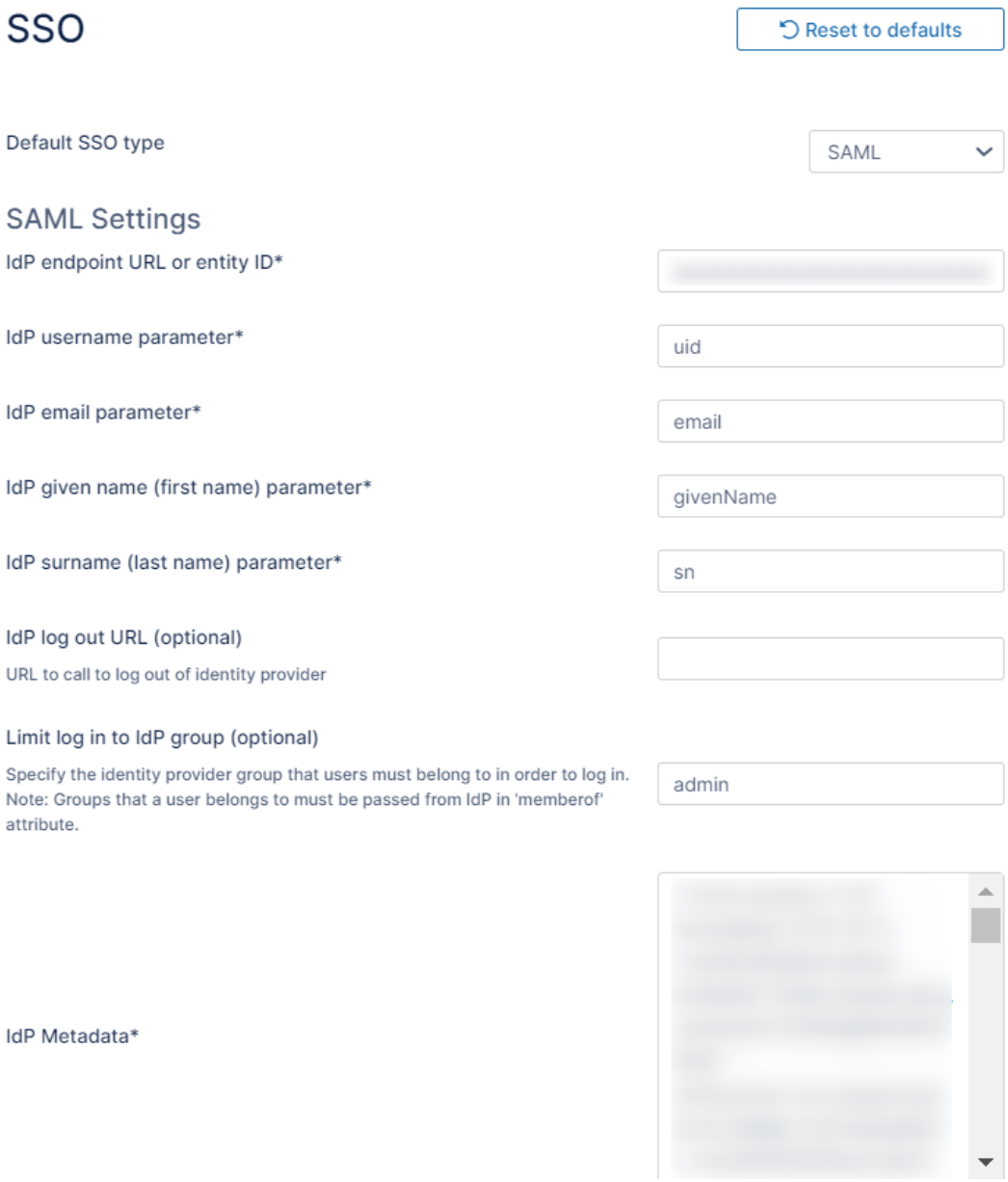


Configuration in Filecloud Admin portal

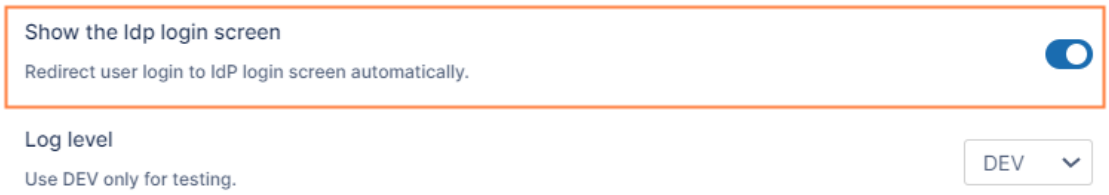
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO** .
   The **SSO** page opens.
2. Enter the following information:

Field	Value
IdP End Point URL	Enter the value of **Issuer Id:** (Configuration tab → Issuer ID just below the "Download Metadata" button)
IdP Username Parameter	uid
IdP Email Parameter	mail
IdP Given Name Parameter	givenName
IdP Surname Parameter	sn

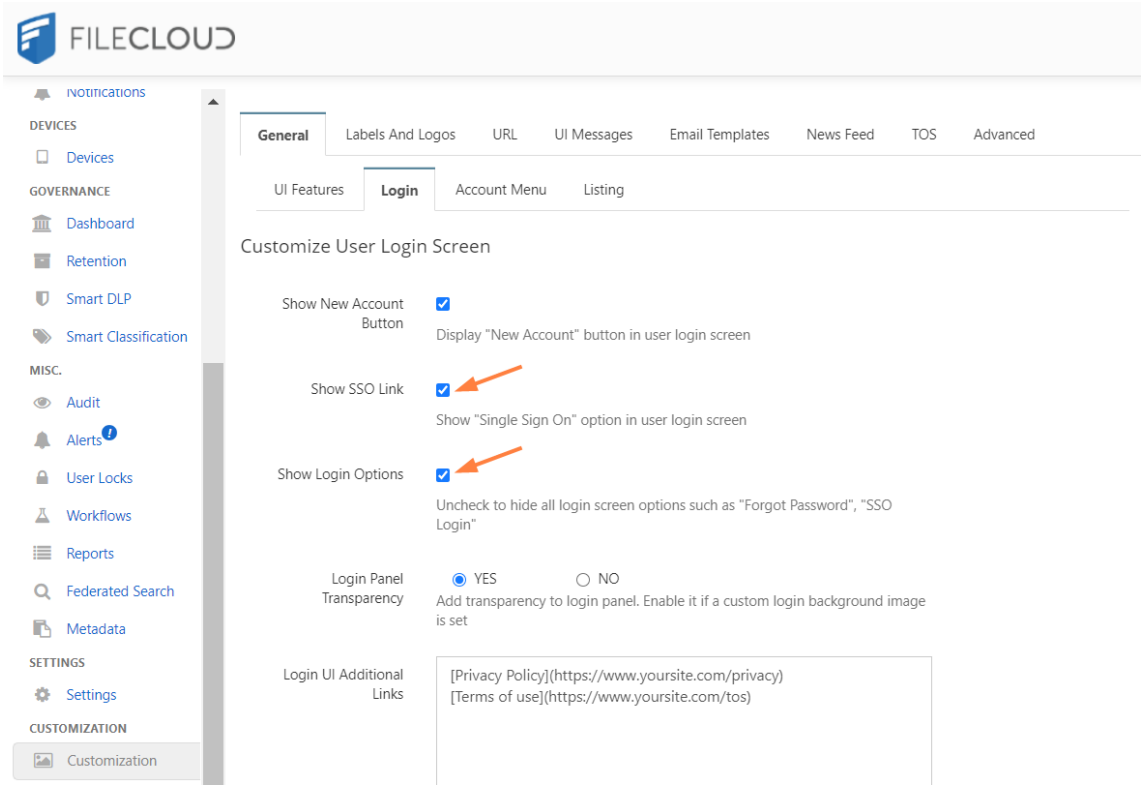
Field	Value
IdP Metadata	Copy the contents of the metadata file downloaded above paste them here.



3. If you want users to see the Ping Identity login after they click **Login with SSO**, scroll to the bottom of the screen and enable **Show the Idp Login Screen**.
   If you want users to be directly logged into FileCloud after they click **Login with SSO**, do not enable **Show the Idp Login Screen**.

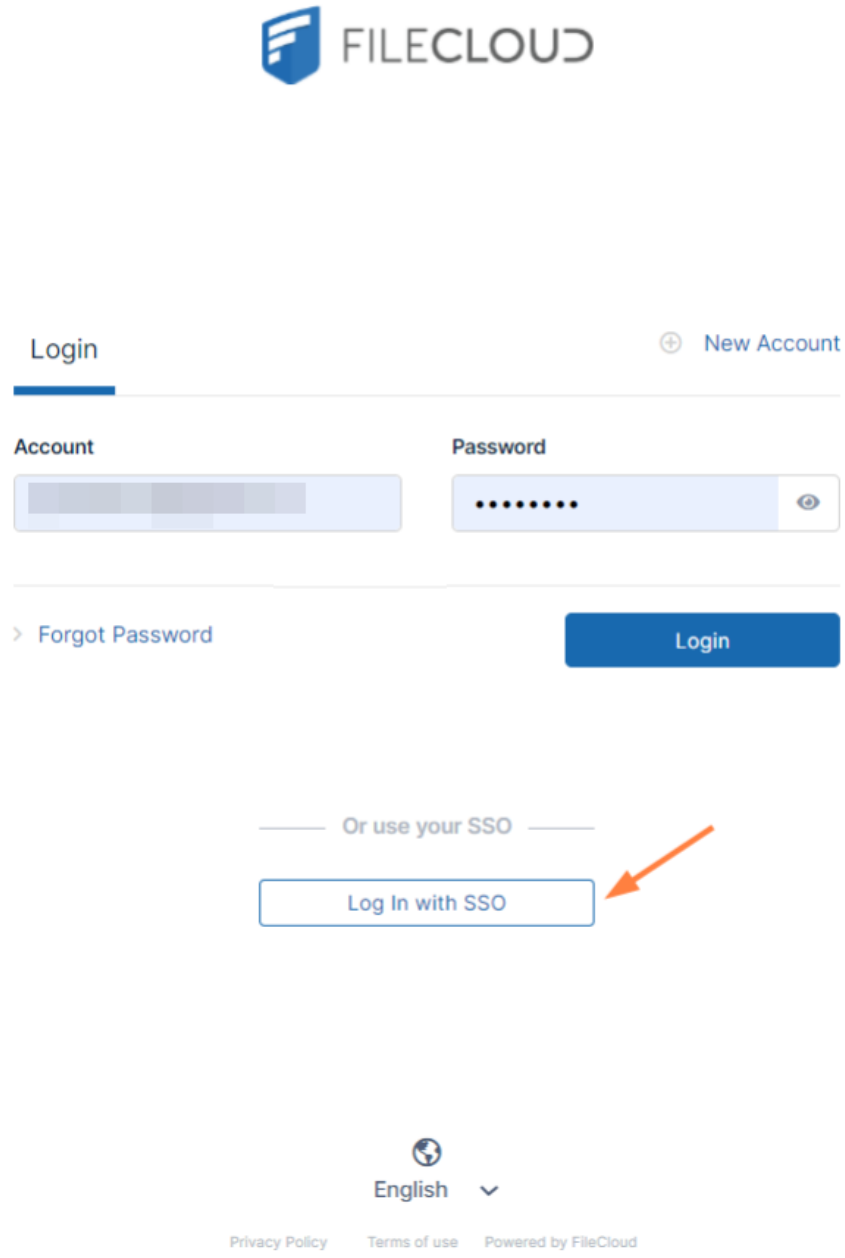


4. Fill in the other fields on the page as shown at SAML Single Sign-On Support.
5. Click **Save**.
6. Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.

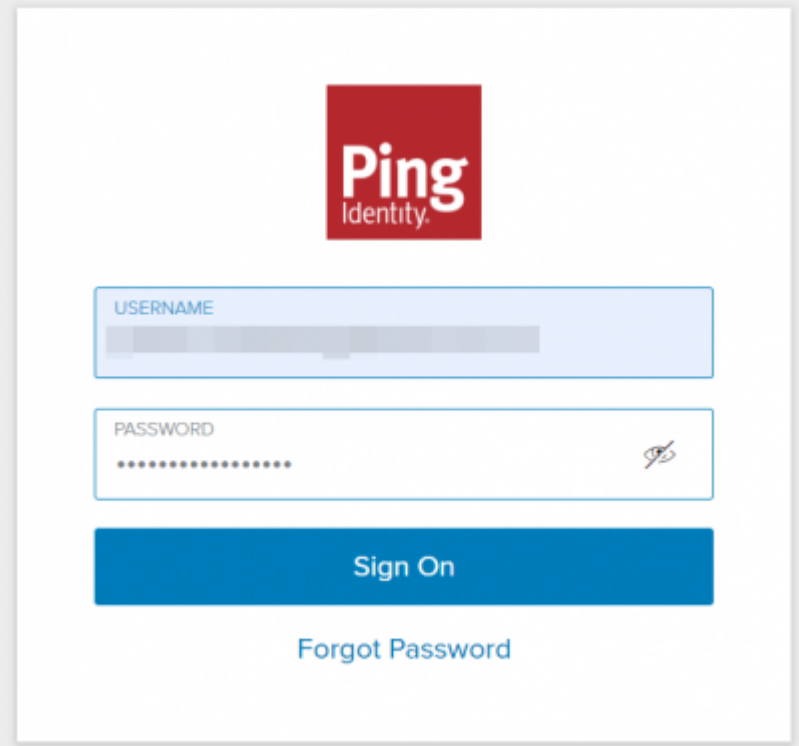


Log in to FileCloud using Single Sign-on with Ping Identity

1. In the Filecloud User login page, the user chooses **Login with SSO**.



If you have checked **Show the Idp Login Screen** in the FileCloud SSO settings, the user is redirected to the Ping Identity login screen, and must click **Sign On**.



Otherwise, the user is directly logged in to FileCloud.

Setting Up and Configuring Certificates when Upgrading SSO

When you upgrade SSO, take the following steps to avoid overwriting your current certificates with the default certificates sent with the library.

For a non-multitenant set up with one Idp:

1. Create a folder named **samlcerts** in WWWROOT/resources/.
2. Copy the **saml.crt** and **saml.pem** files into the **samlcerts** folder.

For a non-multitenant or a multi-tenant set up with different Idp's:

1. Create a folder named **samlcerts** in WWWROOT/resources/ .
2. Create a folder with the same name as the site in WWWROOT/resources/samlcerts/<SITENAME>.
   For the default site, name the folder **default.** For other sites, give the folder the name of the site on the super admin user interface.
3. Calculate the sha1 of idp url using the following command:
   #echo -n "https://<IDP-URL>/adfs/services/trust" | openssl sha1
   (stdin)= bea10f29becf8acab8d8d6e8b9b7ee52f35ada8a
4. Use the sha1 value from step 3 to create a new folder in WWWROOT/resources/samlcerts/<SITENAME>.

For example, for the above case, create the folder: WWWROOT/resources/samlcerts/<SITENAME>/bea10f29becf8acab8d8d6e8b9b7ee52f35ada8a.

5. Place the **saml.pem** and **saml.crt** files into the folder created in step 4.

ADFS Single Sign-On Support

Introduction

FileCloud offers a SAML-based Single Sign-On (SSO) service that provides customers with full control over the authorization and authentication of hosted user accounts.

Using the SAML model, FileCloud acts as the **service provider** and also a **claims-aware application**. FileCloud customers that host FileCloud can authenticate against Active Directory Federation Services (ADFS) and log in to FileCloud.

FileCloud acts as a Service Provider (SP) while the ADFS server acts as the identity provider (IdP).

Active Directory Federation Services (ADFS) Support
When SAML SSO Type is selected and ADFS is enabled in FileCloud, FileCloud accepts claims in the form of ADFS security tokens from the Federation Service, and can use ADFS claims to support Single Sign-On (SSO) into FileCloud.
To specify the identity claims that are sent to the FileCloud refer to the IdP Configuration section below.

Prerequisites

- A Working ADFS implementation. This is beyond the scope of FileCloud. Please refer to articles available on the internet on setting up ADFS.
- FileCloud must be running on HTTPS using SSL. (Default self-signed SSLs that ship with FileCloud do not work). ADFS does not allow adding a relying party that is running on HTTP or self-signed SSL. For help setting up SSL in FileCloud, see set up SSL in FileCloud.

FileCloud SSO Configuration Steps

In order to successfully configure SSO:

1. Configure Apache Webserver.
2. Set SAML as a the default single sign-on method in FileCloud and configure IdP settings.
3. Enable single sign-on link on the login page.
4. Register FileCloud as a service provider (SP) with IdP by adding FileCloud as a Relying Party Trust in ADFS.

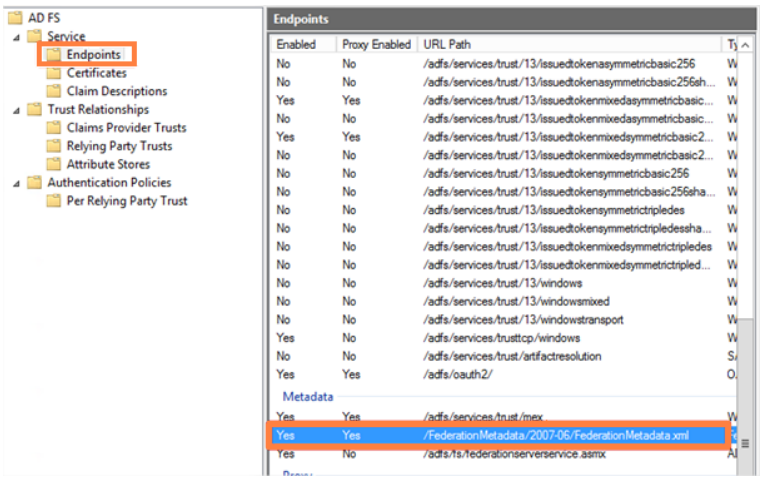
Step 1: Apache Web Server Configuration

Follow the steps in SAML Single Sign-On Support to set up the Web Server configuration and enable SSO.

Step 2: Set SAML as the default SSO method and configure IdP/ADFS

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. Set **Default SSO Type** to **SAML**.
3. Set the other fields as specified in the following table.

FileCloud Parameters	**ADFS as IdP** **Data can be obtained from Federation Metadata**	
Default SSO Type	For ADFS, select SAML	
IdP End Point URL	Identity Provider URL (Entity ID) e.g. http://yourADFSdomainName/adfs/services/trust	
IdP username Parameter	Identifies the username (must be unique for each user) Usually SAMAccountName or User Principal Name defined in claim rules. **NOTE: The username must be unique**. If username sent by Idp is in email format, the email prefix will be used for username. The email prefix in this case must be unique. value: **uid** or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn <Attribute Name="**http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn**" NameFormat="**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**" FriendlyName="**UPN**" xmlns="**urn:oasis:names:tc:SAML:2.0:assertion**" />	
IdP email Parameter	Identifies the email of the user (must be unique) value: **mail** or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress <Attribute Name="**http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress**" NameFormat="**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**" FriendlyName="**E-Mail Address**" xmlns="**urn:oasis:names:tc:SAML:2.0:assertion**" />	

IdP given name (first name) Parameter	Identifies the given name (first name) of the user. value: **givenName** or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Given Name" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP surname (last name) Parameter	Identifies the surname (last name) of the user value: **sn** or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Surname" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP Log Out URL (Optional)	URL for logging out of IdP	
Limit Logon to IdP Group (Optional)	IdP Group Name • Specifying a group name means that a user can log in through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group • The IdP must send this group name through the **memberof** parameter • The **memberof** parameter can include a comma-separated list of all groups to which the user belongs	
IdP Metadata	Federation Metadata in xml format. Usually ADFS metadata is found at the URL Path below: e.g.https://yourADFSDomain/federationmetadata/2007-06/federationmetadata.xml 	

SSO Error Message (Optional) Added in FileCloud 20.1	Custom error message that appears when a signin is invalid. Enter in HTML format. In a multiple IDP environment, this is the error message for the default IDP. To include a message specific to each IDP, include the parameter <MESSAGE>. See Integrating Multiple IDPs for help configuring multiple IDPs with error messages specific to each one..	
Allow Account Signups Added in FileCloud 20.1	When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.	
Automatic Account Approval Added in FileCloud 20.1	This setting works with the **Allow Account Signups** setting to determine: • If the account created by the user is disabled until the administrator approves it • If the account is approved with a specific level of access automatically without intervention from the administrator. • Possible values are: 0 - No Automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User	
Enable ADFS	Yes	
User login token expiration match Idp expiration	If enabled the user token expiration will be set based on ADFS expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)	
Enable Browser-Only SSO Session Timeout Added in FileCloud 23.232.1	If enabled, SSO session timeouts apply to browser sessions but not to client sessions.	
Show the IdP Login Screen	If enabled, automatically redirect user to IdP log-in screen.	
Log Level	Set the Log level for SAML calls. Default Value: PROD (Do not use DEV for production systems)	

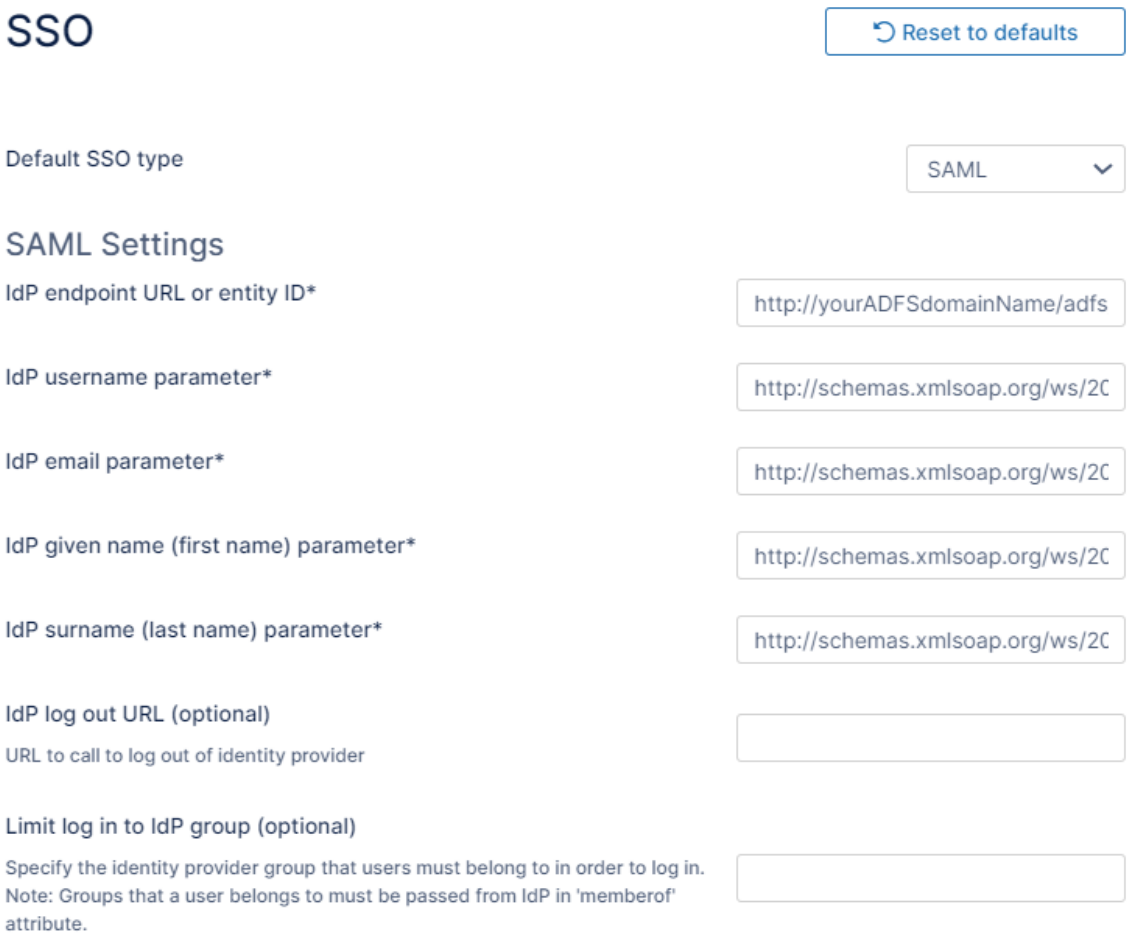
Allow SSO for external users Added in FileCloud 23.253	Only appears if feature is included in license. If enabled, external users are able to log in to FileCloud using SSO. Default value: Disabled.	

Notes:

For **IDP Log Out URL** to be effective, request that FileCloud Support add the corresponding setting to your FileCloud configuration. to be effective, you must also add a setting to the FileCloud config file:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To make the **IdP Log Out URL** setting effective, add:
   define("TONIDOCLOUD_SAML_SIGNED_LOGOUT", 1);

For help configuring multiple IDPs with **Automatic Account Approval** settings specific to each one, see Integrating Multiple IDPs.



Step 3: Enable SSO link on the login page

Follow the steps in SAML Single Sign-On Support (under SSO Configuration Steps, Step 6) to enable SSO sign-in on the user portal or admin portal.

Step 4: Register FileCloud as SP in IdP/ADFS

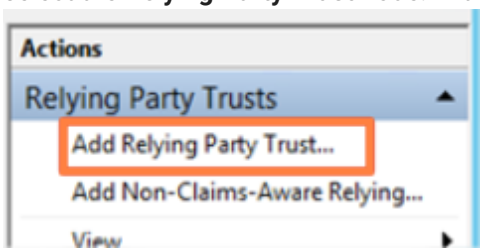
Registering FileCloud as SP in ADFS involves series of steps from adding FileCloud as a Relying Party Trust in ADFS to setting up Claim Rules for FileCloud in ADFS. Please follow the steps below to successfully register FileCloud in ADFS.

Before you proceed, you must be able to download the metadata of FileCloud from the following Entity ID URL. (Note HTTPS).

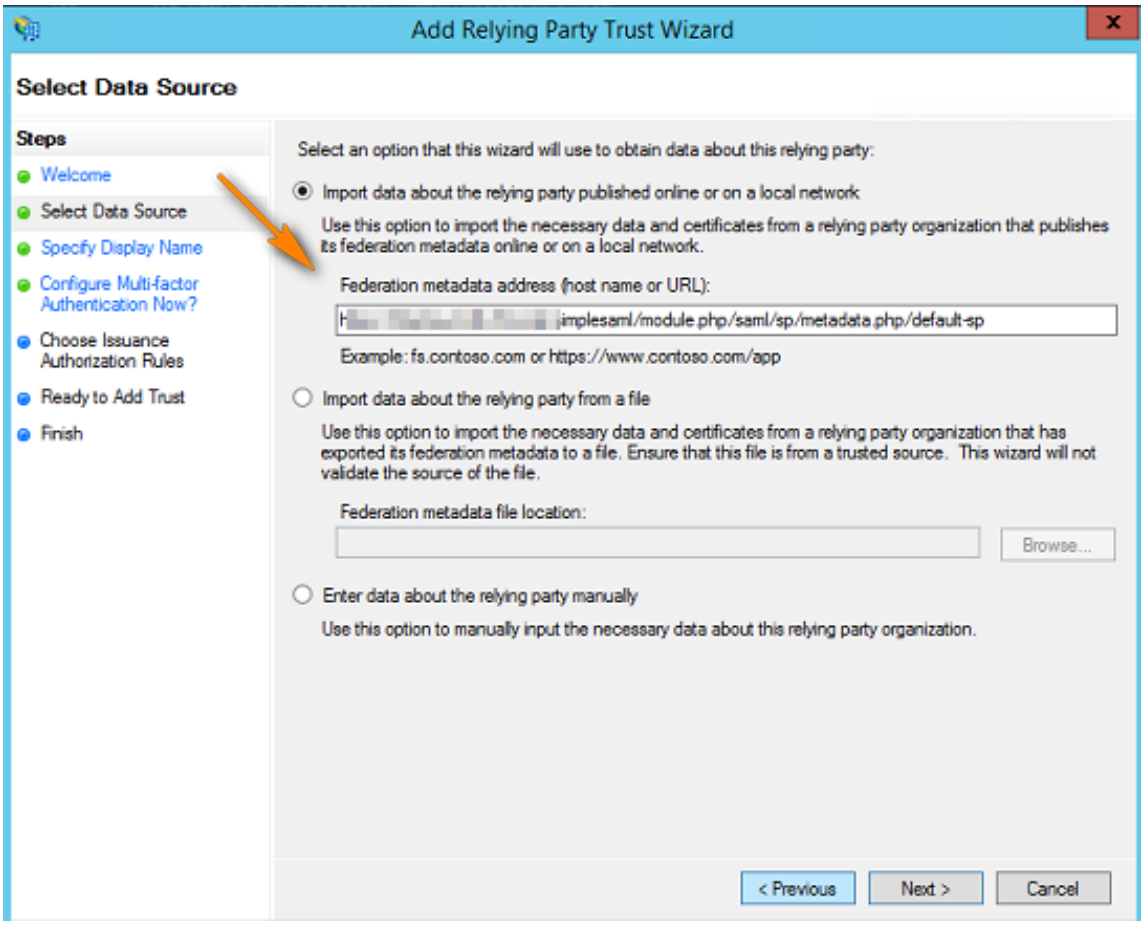
https://<Your Domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp

If you have trouble downloading the metadata from the above URL, please check if HTTPS is working and Steps 1, 2 and 3 above were completed successfully.

1. On your ADFS server, open the ADFS management console, expand **Trust Relationships** and select the **Relying Party Trust** node. In the **Actions** pane, click **Add Relying Party Trust**.



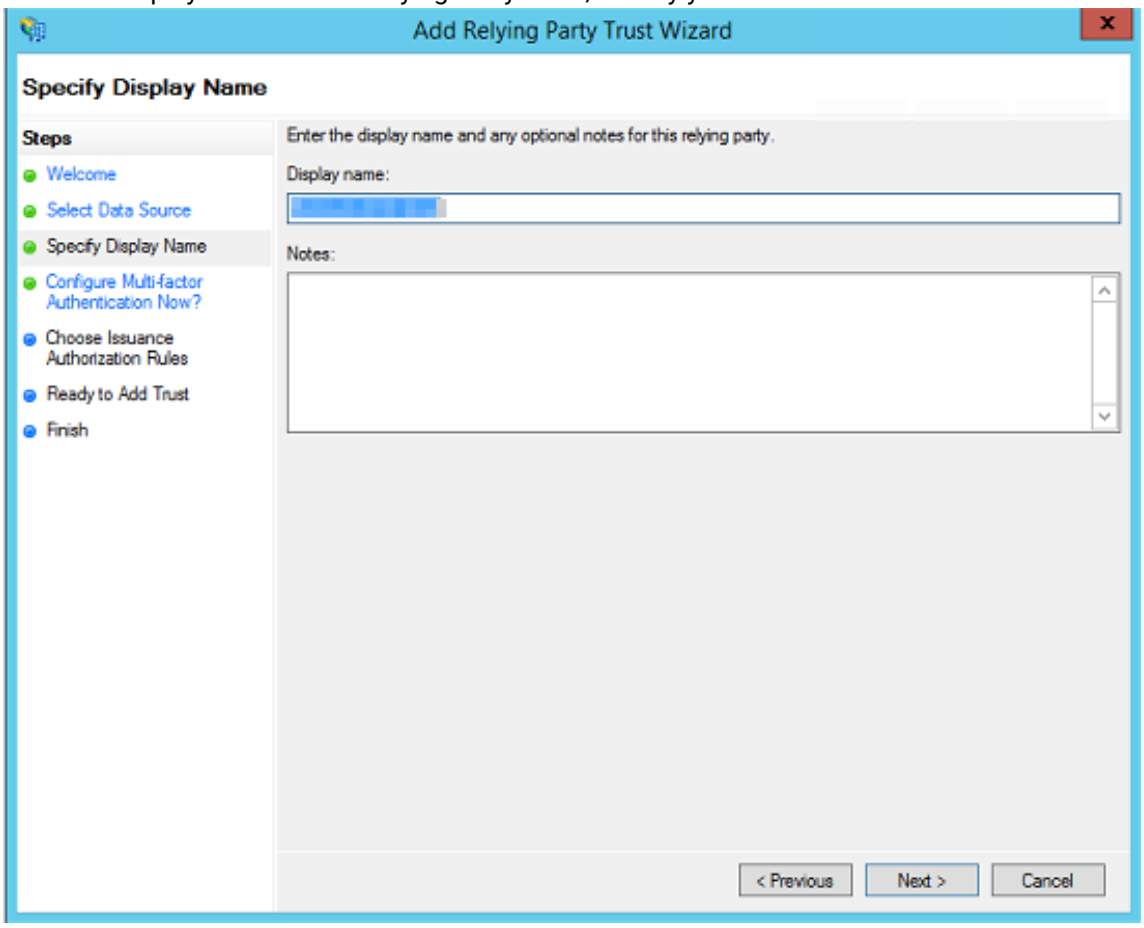
2. Click **Start**, then paste the **Entity ID URL** from above into the **Federation Metadata address** field and click **Next**.



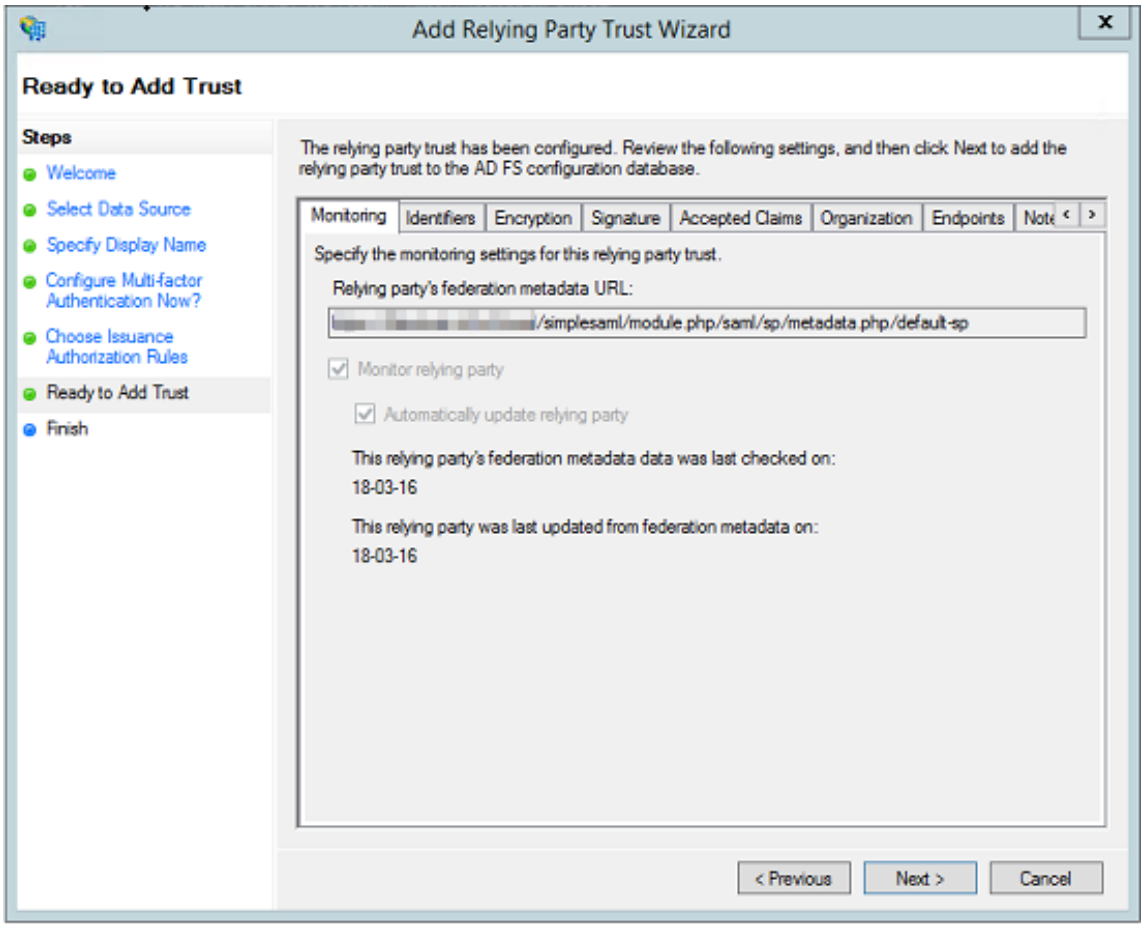
Note: You can do this manually by downloading your metadata file from http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp and importing it into ADFS by choosing **Import data about the relying party from a file**.

Once you access the metadata URL you need to enter admin credentials to be able to download the metadata file. The username is **admin** and the password can be found in: **<FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php**

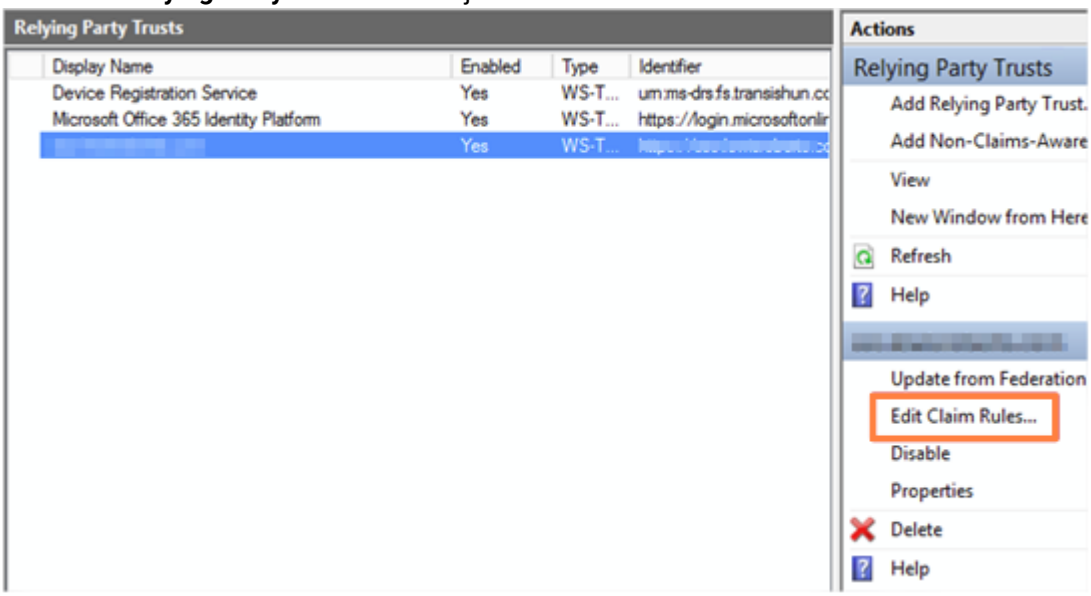
3. Accept the warning
4. Enter the display name for the Relying Party Trust, usually your FileCloud URL.



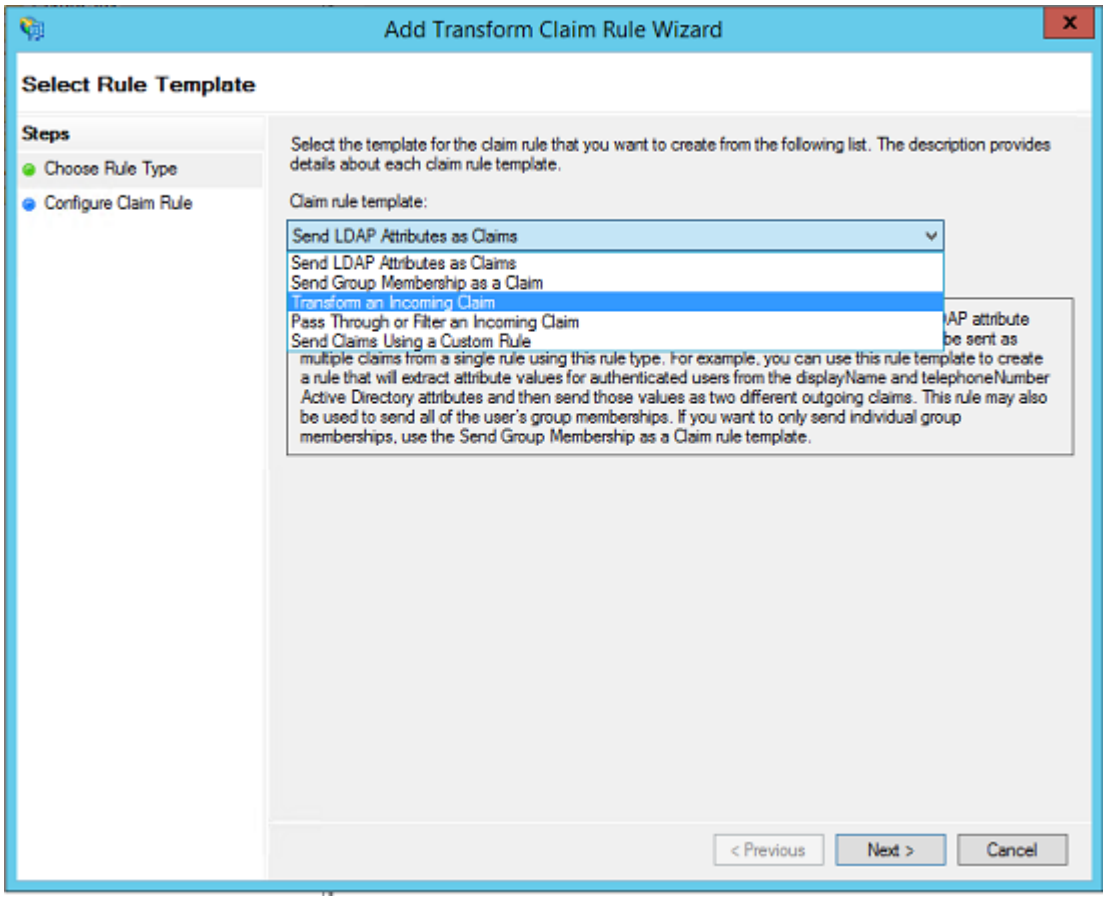
5. Click **Next** several times in the wizard until you reach the **Ready to Add Trust** page. Here, review the tabs. The **Encryption** and **Signature** tabs must have values associated with them.



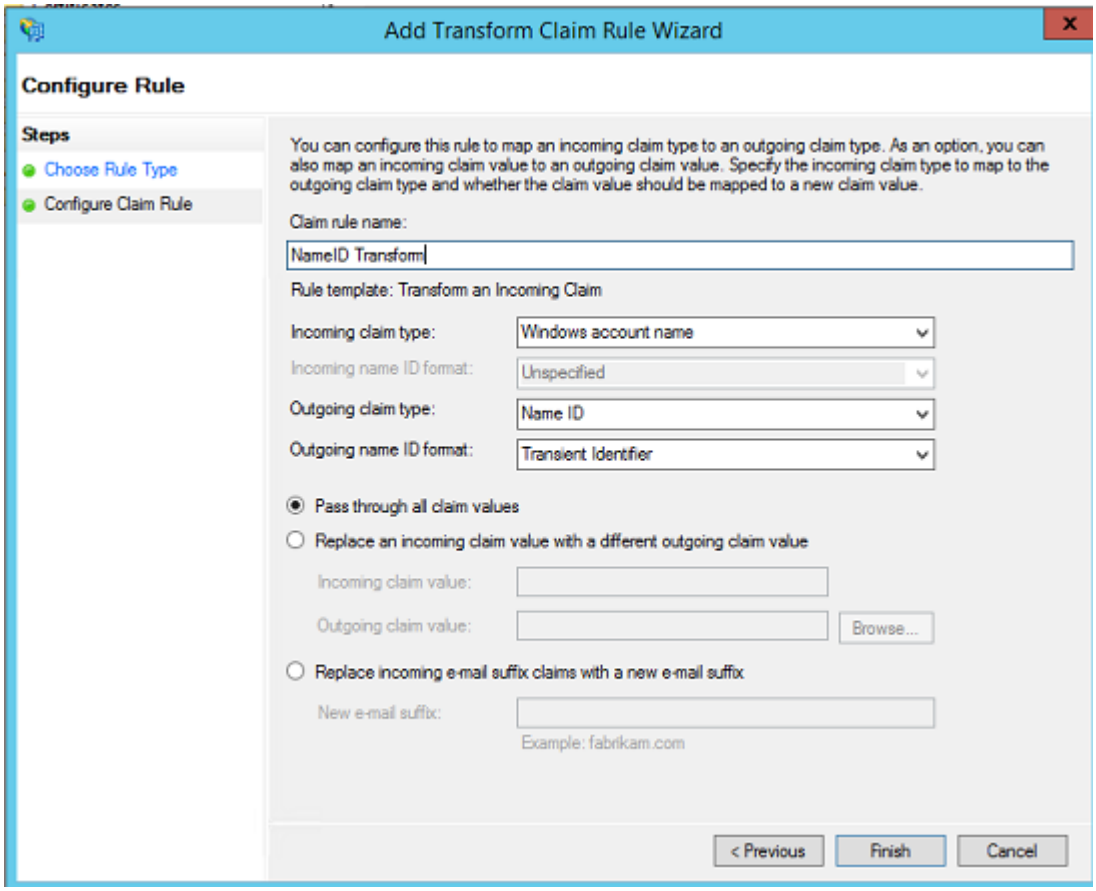
6. Click **Next**. The new **Relying Party Trust** is now added.
7. Select the **Relying Party Trust** we have just added and then click **Edit Claim Rules**.



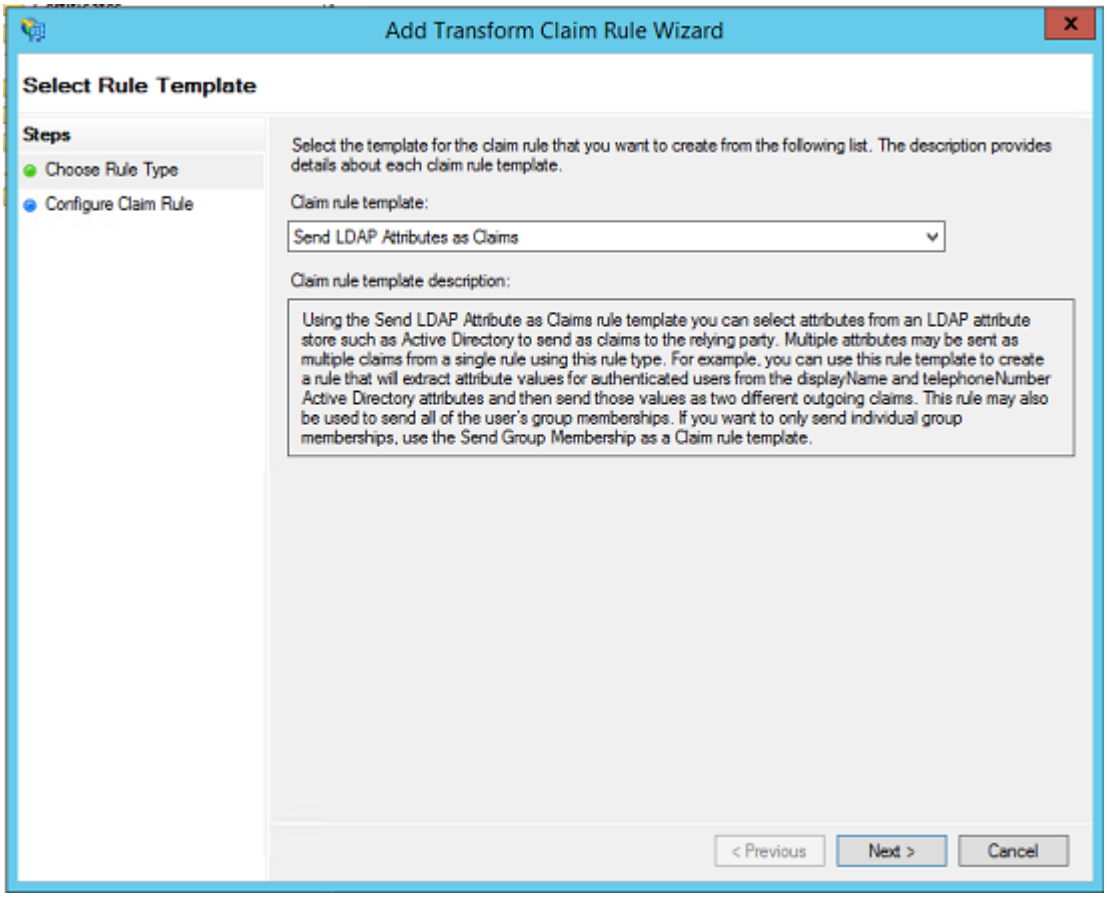
8. Add an **Issuance Transform Rule**. Choose the **Transform an Incoming Claim** rule template.



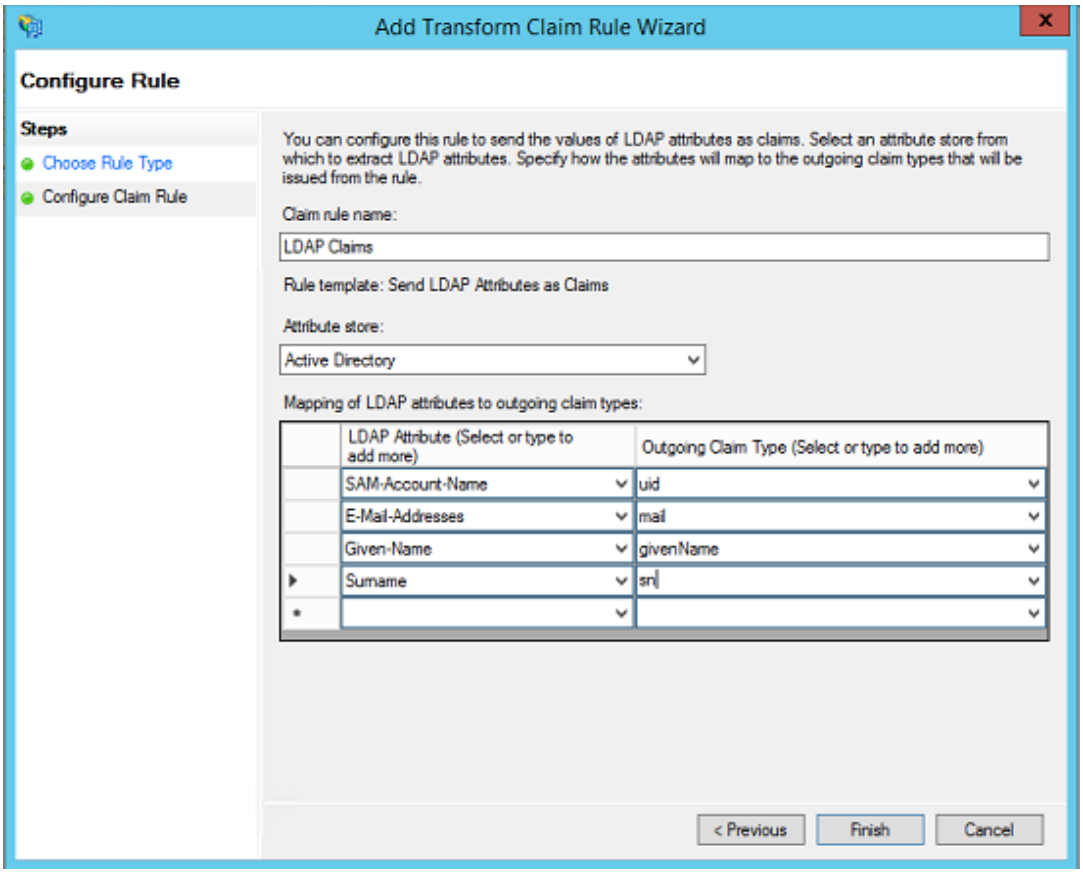
9. Give a **Claim rule name** (Name ID Transform - can be anything). Choose **Windows account name** as **Incoming claim type** and **Name ID** as **Outgoing claim type**. Choose **Transient Identifier** for **Outgoing name ID format**. Select the radio button **Pass through all claim values.** Click **Finish** to add the claim rule.



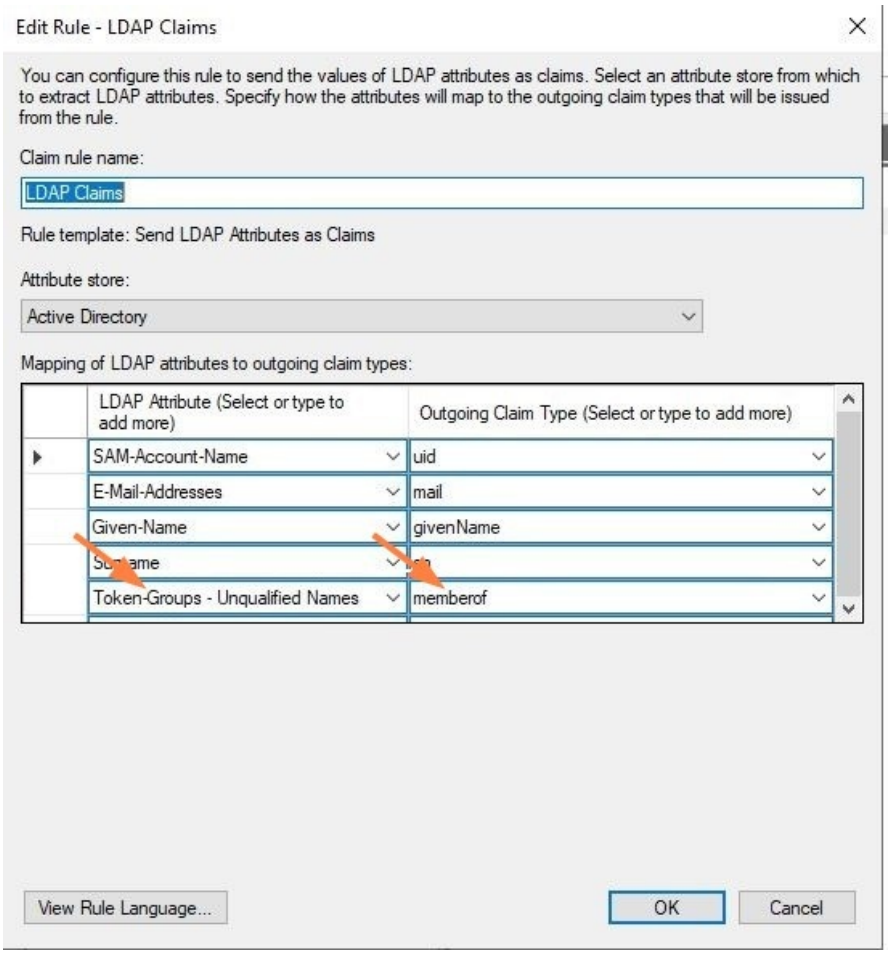
10. Add another issuance transform rule. Select **Send LDAP Attributes as Claims** template.



11. Fill in the rule fields:
    - Enter a **Claim rule name** (LDAP Claims - can be anything).
    - Select **Active Directory** as **Attribute store**.
    - Enter the mapping values of **LDAP Attributes** to **Outgoing Claim Types**. The outgoing claim type must match the names as specified in FileCloud SSO Settings UI Page (the screenshot below follows the FileCloud SSO Settings as documented above).
    - For **Outgoing Claim Type, uid** and **mail** are required. **SAM-Account-Name** in the screenshot below can be replaced with **UPN** if desired.

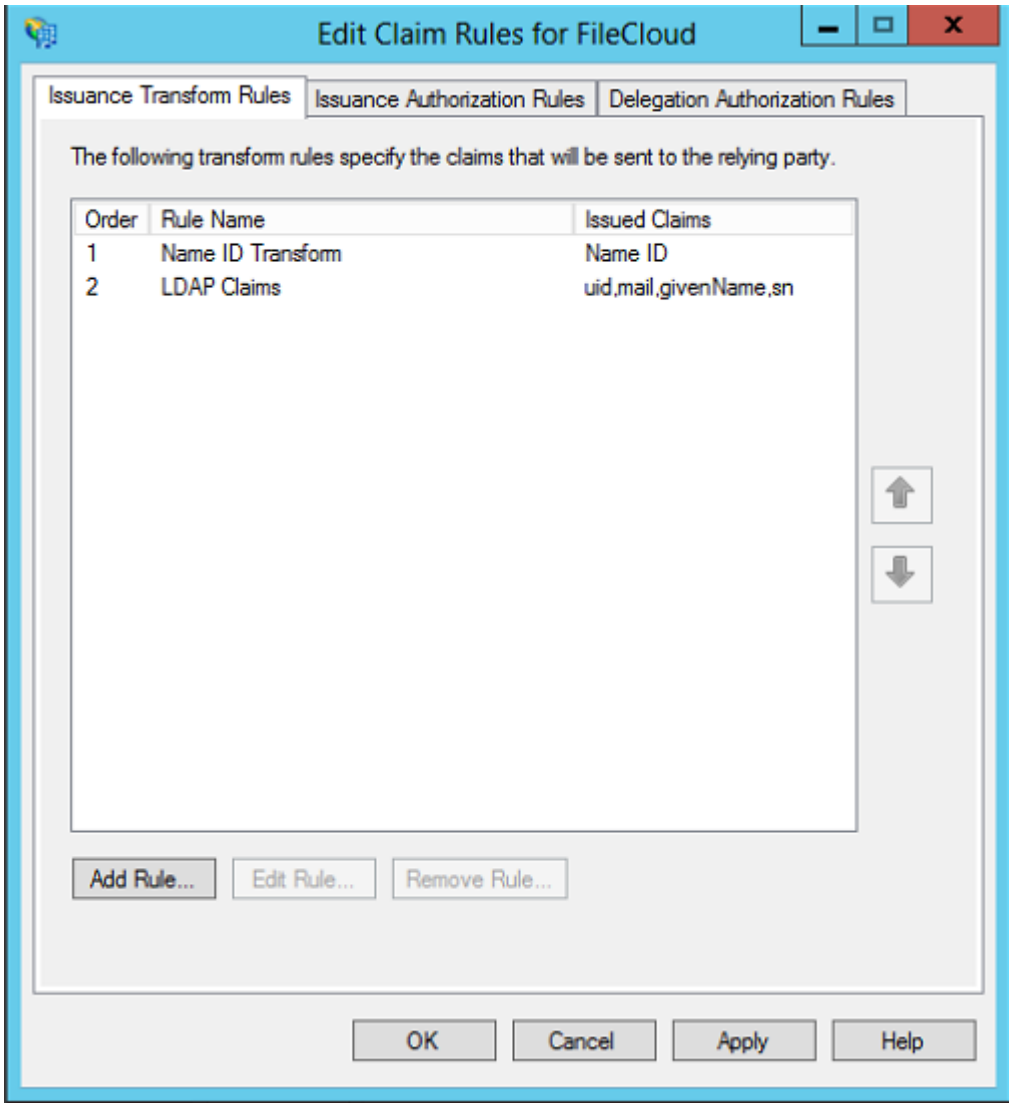


- For ADFS configuration, add an additional claim parameter (**Token-Groups - Unqualified Names > memberof**).



- Click **Finish** to add the rule.

12. Once configured, you should have two issuance transform rules (**Name ID Transform** and **LDAP Claims** if you followed the steps above). Click **Apply** and **Exit**.



This completes the ADFS configuration and FileCloud is added as a Relying Party Trust in the ADFS server. You can now test SSO from FileCloud by going to the FileCloud login page and clicking the Single Sign-On link as mentioned in Step 3, above.

Troubleshooting

Please check the troubleshooting section from SAML Single Sign-On Support.

NTLM Single Sign-On Support

FileCloud supports NTLM for User Login through SSO.

Prerequisites

For NTLM SSO to work, the FileCloud Server must be connected to the AD domain.

Web Server Settings

1. Ensure the file "mod_authn_ntlm.so" exists in the c:\xampp\apache\modules folder
2. Edit the Webserver configuration file at c:\xampp\apache\conf\httpd.conf and add the following section.

```
<Location /auth >
  #AllowOverride None
  AuthName "Private location"
  AuthType SSPI
  NTLMAuth On
  NTLMAuthoritative On
  <RequireAll>
    <RequireAny>
      Require valid-user
      #require sspi-user EMEA\group_name
    </RequireAny>
    <RequireNone>
      Require user "ANONYMOUS LOGON"
      Require user "NT-AUTORITÄT\ANONYMOUS-ANMELDUNG"
    </RequireNone>
  </RequireAll>
  # use this to add the authenticated username to you header
  # so any backend system can fetch the current user
  # rewrite_module needs to be loaded then
  RewriteEngine On
  RewriteCond %{LA-U:REMOTE_USER} (.+)
  RewriteRule . - [E=RU:%1]
  RequestHeader set X_ISRW_PROXY_AUTH_USER %{RU}e
 </Location>
```

3. Ensure the module is loaded by ensuring the following line is enabled and not disabled.

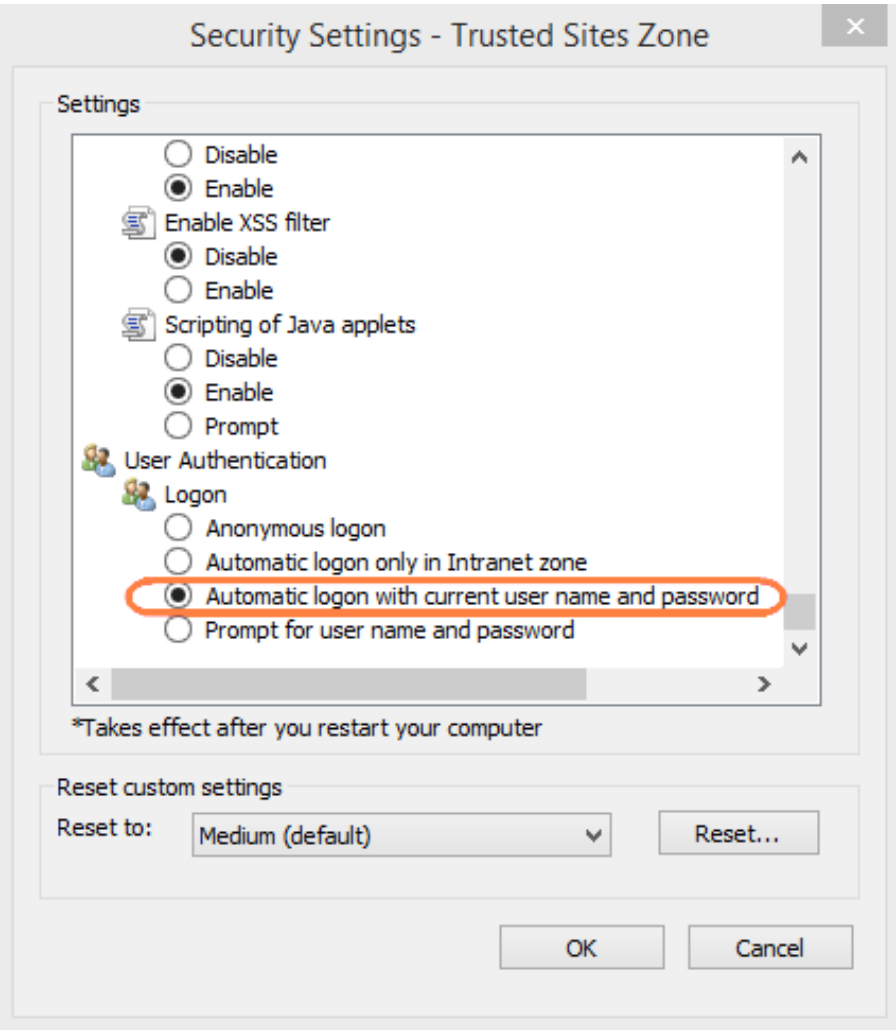
```
LoadModule auth_ntlm_module modules/mod_authn_ntlm.so
```

4. Ensure you have the "auth" folder available at WWWROOT
5. Restart the Web server.
6. In your browser open http://<HOSTNAME>/auth URL; it will automatically login if everything works correctly. Make sure in your browser SSO has been enabled for the site.

Browser Settings to Enable Domain User SSO Login

For Internet Explorer and Google Chrome

1. Add the site URL to trusted site.
2. In the settings for trusted sites, enable user login to be sent, see screenshot below.



Troubleshooting

In some environments, additional code may be needed to complete authentication from the server.

After configuration, if you attempt to login with the AD username and password and are repeatedly prompted to enter your AD credentials instead of being transferred to the user portal:

1. Edit the file at c:\xampp\htdocs\.htaccess
2. Locate this section:

```
#-----------------------------------------------------
```

```
# ADVANCED CUSTOMIZATION SECTION - END
#-------------------------------------------------

#Route all requests to our handler
RewriteRule   ^(.*)/?$ public/index.php [L]
```

3. Above the line:

```
#Route all requests to our handler
```

add the code:

```
RewriteRule ^auth/index\.php$ - [L]
```

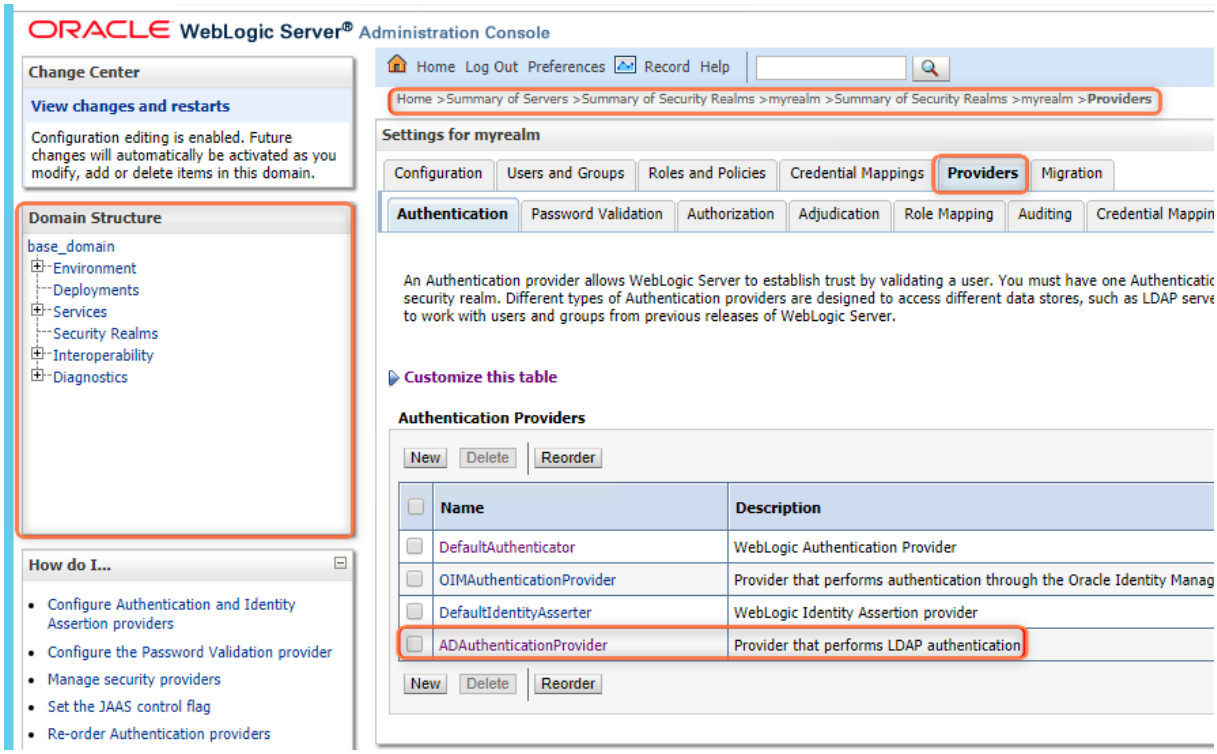
Oracle Identity Manager LDAP integration with FileCloud

Oracle Identity Manager
Oracle Identity Management enables system administrators to integrate multiple Active Directories and control them from one location. To ensure a smooth configuration please ensure:

- The server that is hosting FileCloud is able to communicate to the server that is hosting OIM.
- You have access to the Admin user and are able to access WebLogic Admin server.
- Both server's firewalls accept the incoming connection.

Integrating OIM's LDAP with FileCloud

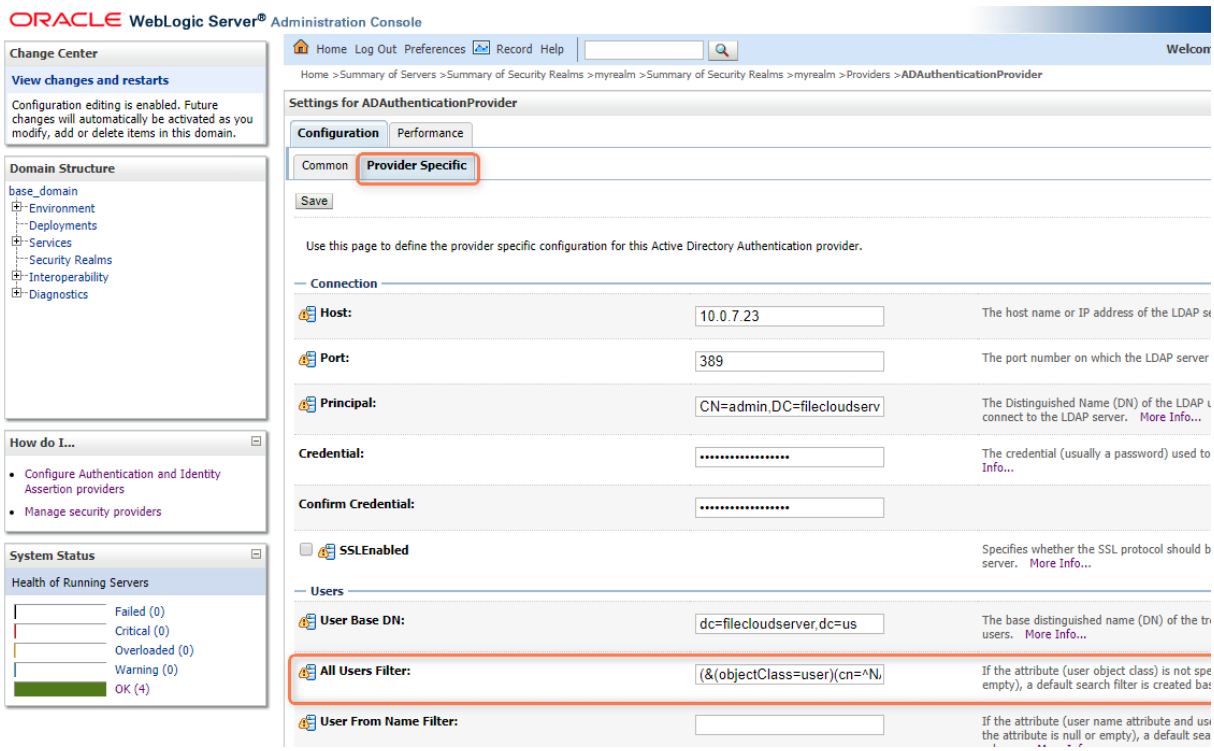
To successfully integrate OIM's LDAP with FileCloud, ensure that FileCloud is able to pull the corresponding attributes such as Name, Email, and password. To verify this, please review your connection settings under
Oracle's WebLogic Admin Server under **Domain Structure> Services> Security Realms > [myrealm] > Providers**. Under **Providers > Authentication** select the authentication provider to use to connect to FileCloud via LDAP.



Click the authentication provider name to access its settings. Navigate to the **Provider Specific** tab. To enable FileCloud LDAP to pull the necessary attributes add the following ObjectClass string under **All Users Filter**.

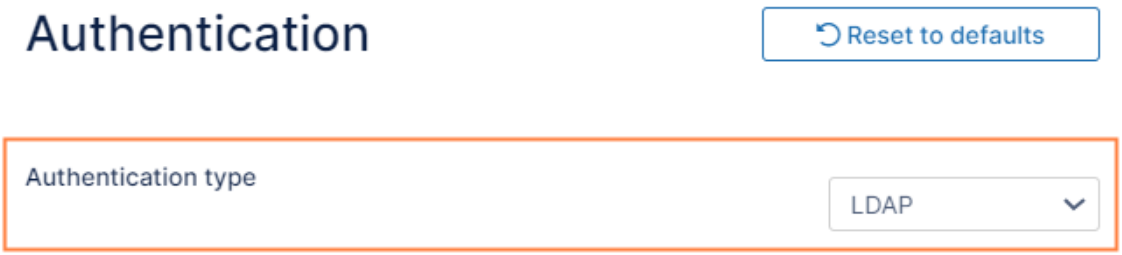
(&(objectClass=user)(cn=^NAME^))

Then, fill out the other required fields based on your Active Directory configuration.



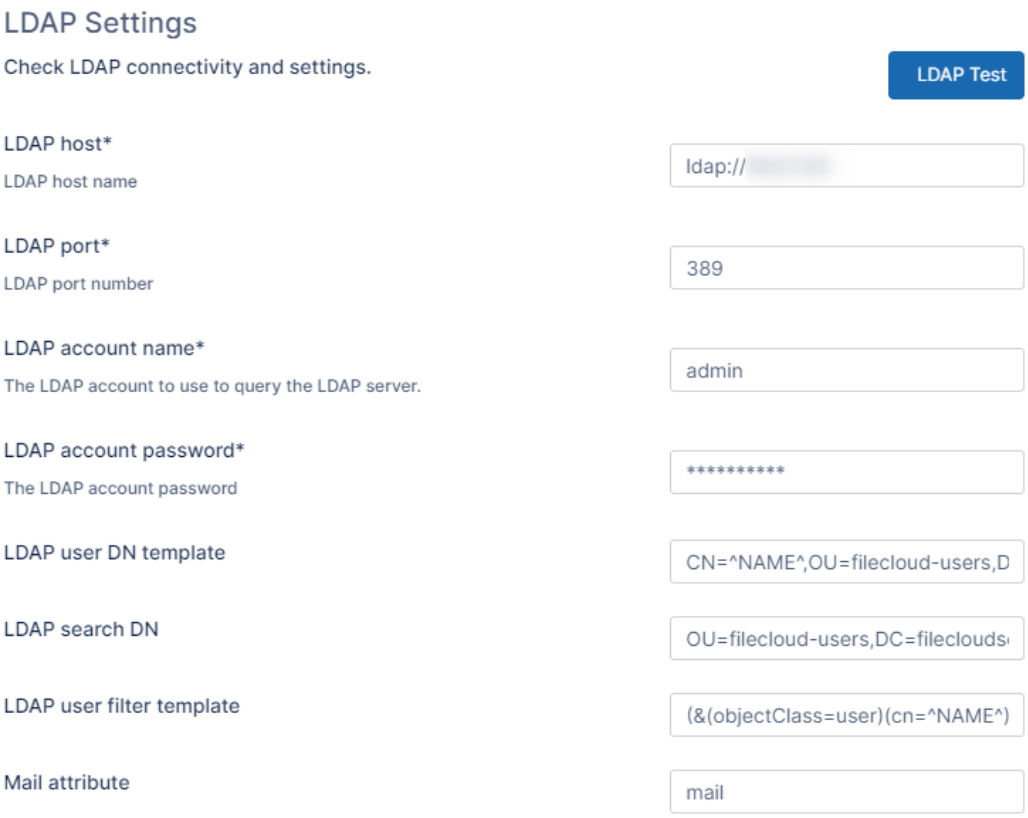
Once you have added the **ObjectClass** attribute on the WebLogic Server realm provider's configuration, access FileCloud's admin portal.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** page opens.
2. Under **Authentication Settings**, in **Authentication Type** select **LDAP**.

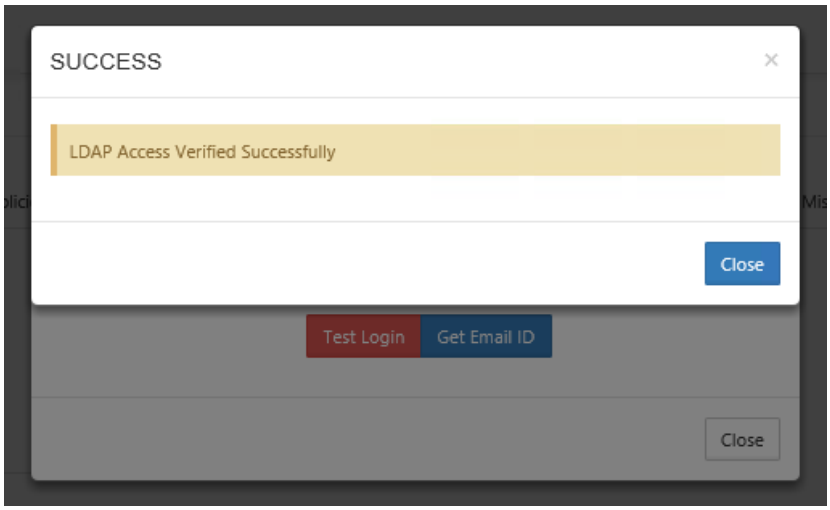


3. To successfully configure LDAP, see LDAP Based Authentication.

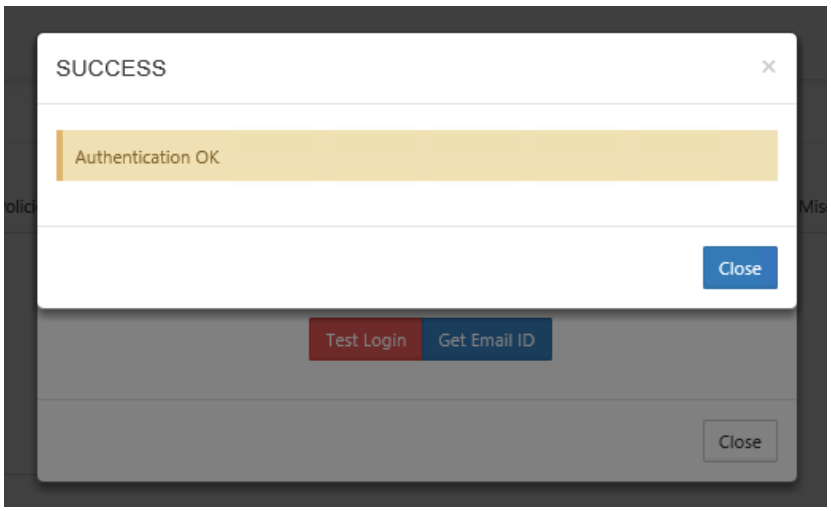
4. To ensure a successful connection, in **LDAP User Filter Template** add: (&(objectClass=user)(cn=^NAME^))

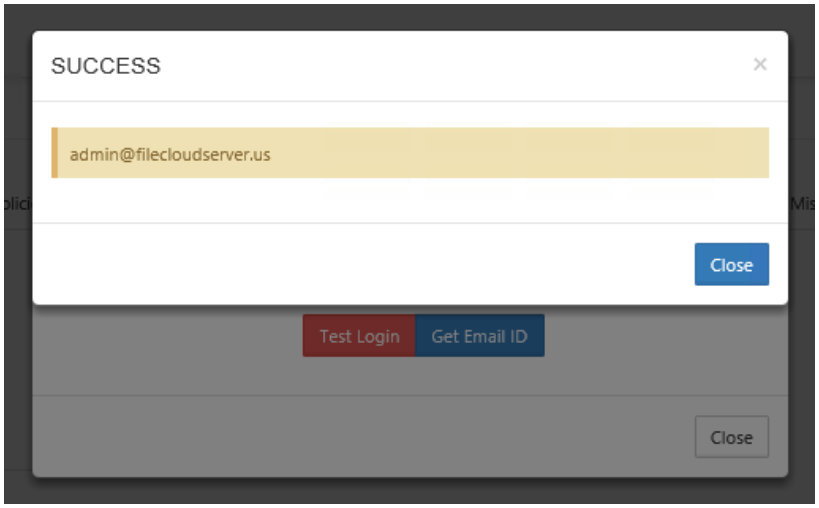


Next, verify your connectivity to OIM's LDAP by clicking **LDAP Test** and clicking **Validate LDAP Settings**.



If you obtain a successful confirmation message proceed to verify that FileCloud is able to login and obtain the email ID as seen on the screenshots below. Upon completion without any errors FileCloud has been successfully integrated with OIM'S LDAP connection.





Desktop Apps Code-Based Authentication

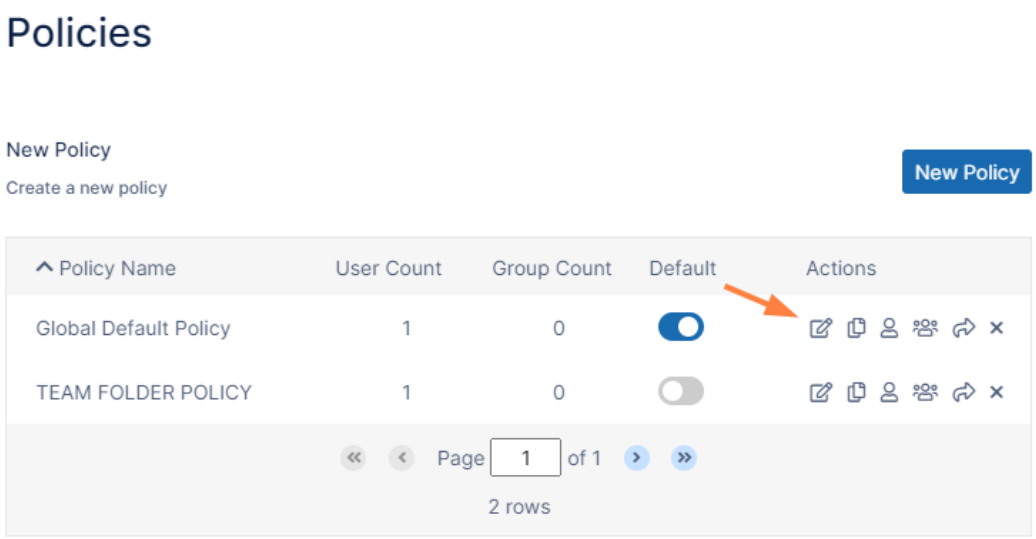
Code-based device authentication is set by policy. It requires users to request approval to log in to a desktop app or mobile app. When the request is approved, a code is created which the user must enter into the app to log in. Requests are approved in the user portal, but additional admin approvals may also be required.

Enabling code-based device authentication

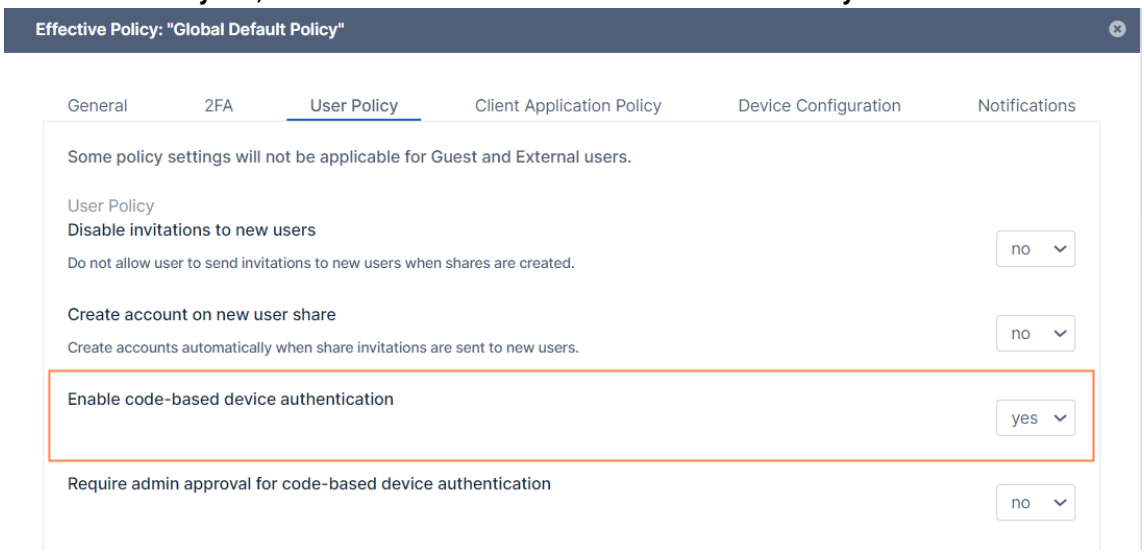
Enable Code based device authentication

To enable code-based device authentication:

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. Click the Edit icon in the row for the users' policy.



   The **Policy Settings** dialog box opens.
3. Click the **User Policy** tab.
4. In the **User Policy** tab, set **Enable code-based device authentication** to **yes**.



   Now, when a user logs in to a client app, an approval request appears in in the user portal. The user must approve the request to receive a code that is entered into the client app to

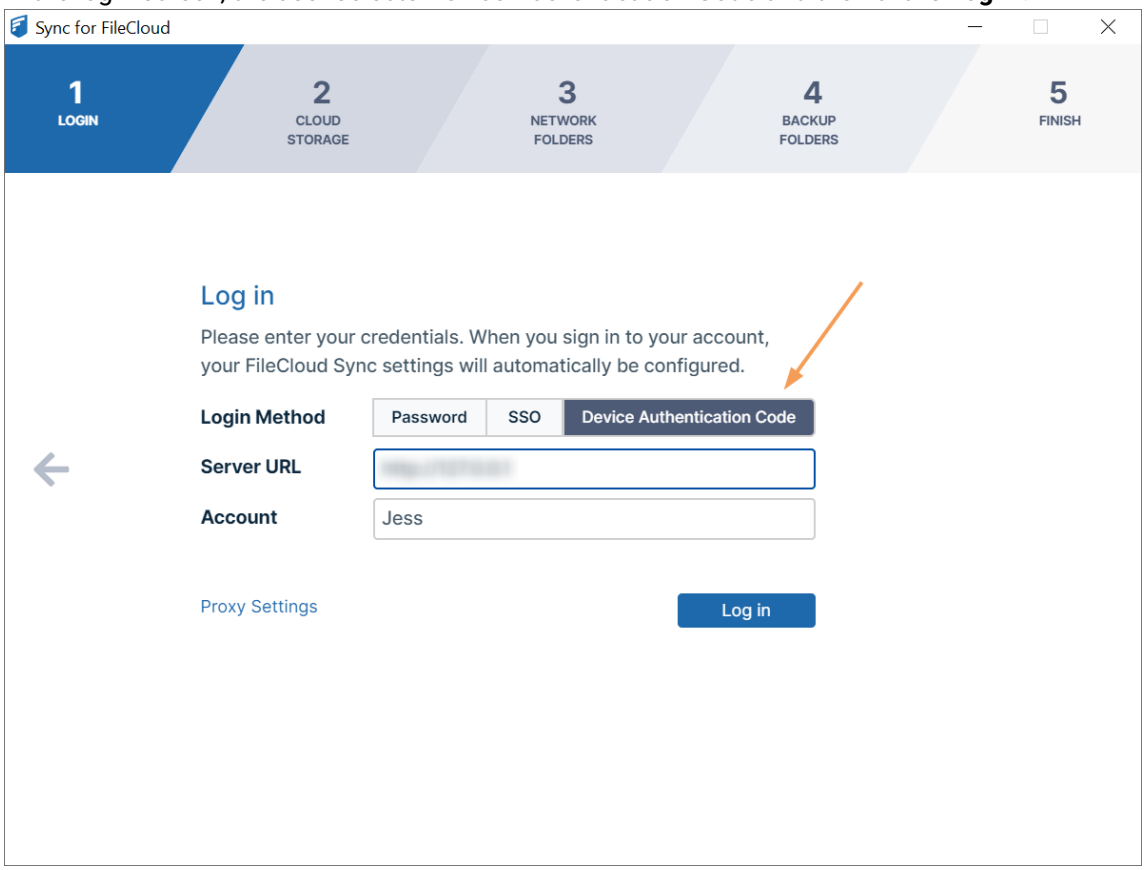
successfully log in.
How users log in with device authentication, below, shows how this process works.

How users log in with device authentication

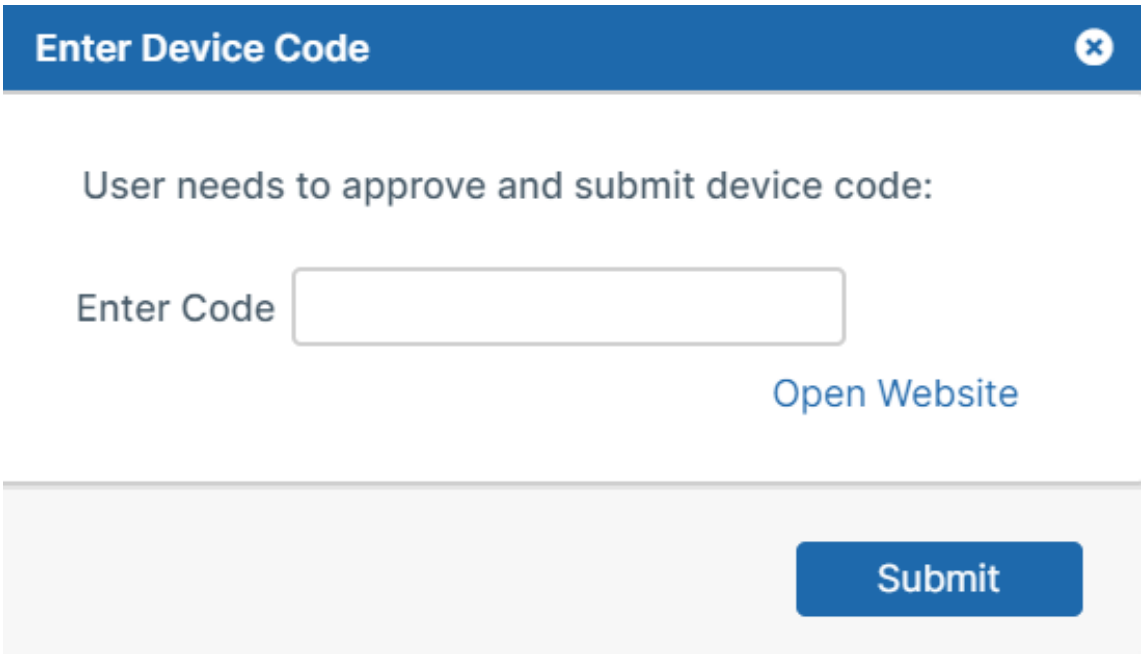
How users log in with device authentication to desktop apps

Once code based authentication is enabled, the user can follow these steps to log in via a desktop app.
The following example uses the Sync application, but the procedure is the same for all of the desktop applications and the mobile apps.

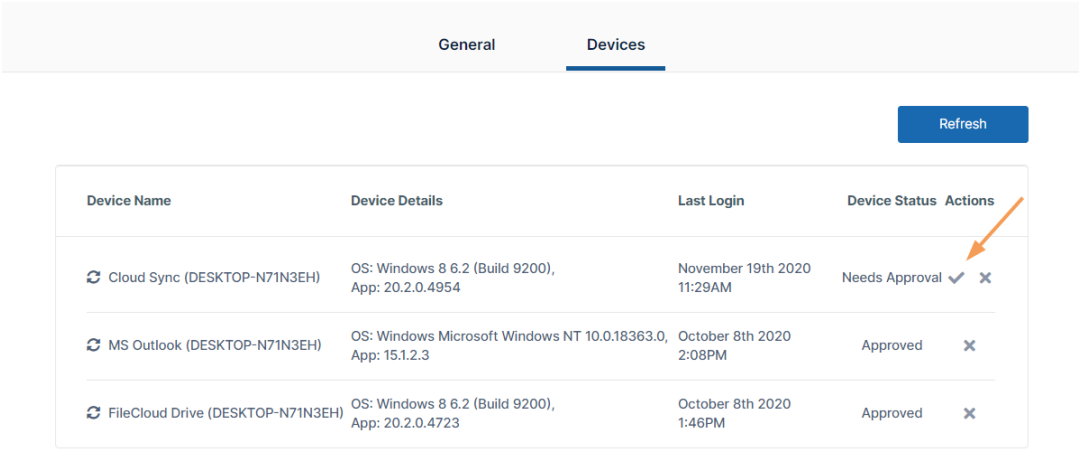
1. In the login screen, the user selects **Device Authentication Code** and then clicks **Log in**.



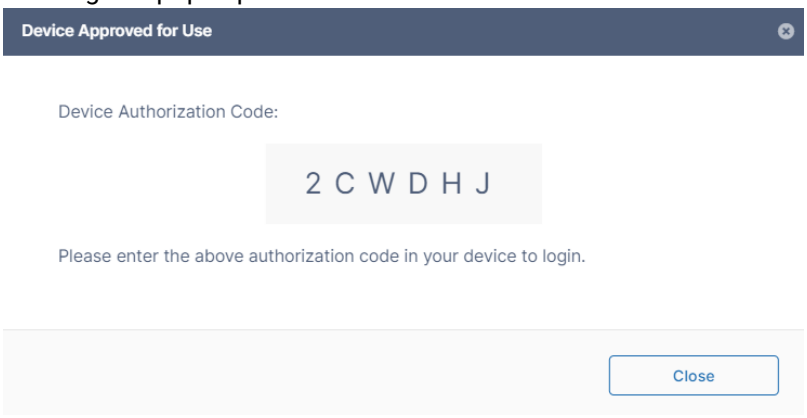
The following dialog box opens.



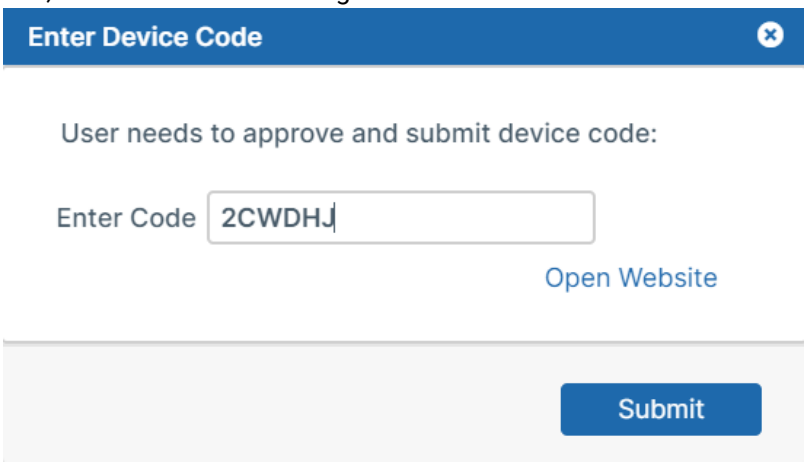
2. To get the device authorization code:
   a. The user logs in to the user portal, then clicks the arrow next to the username and chooses **Settings**..
   b. In the **Settings** screen, the user click the **Devices** tab.
   c. The user clicks the check next to **Needs Approval**.



A dialog box pops up with the **Device Authorization Code**:



3. The user copies the **Device Authorization Code** and pastes it into the **Enter Device Code** dialog box, then clicks **Submit** to log in.



Requiring admin approval as well as user approval for devices

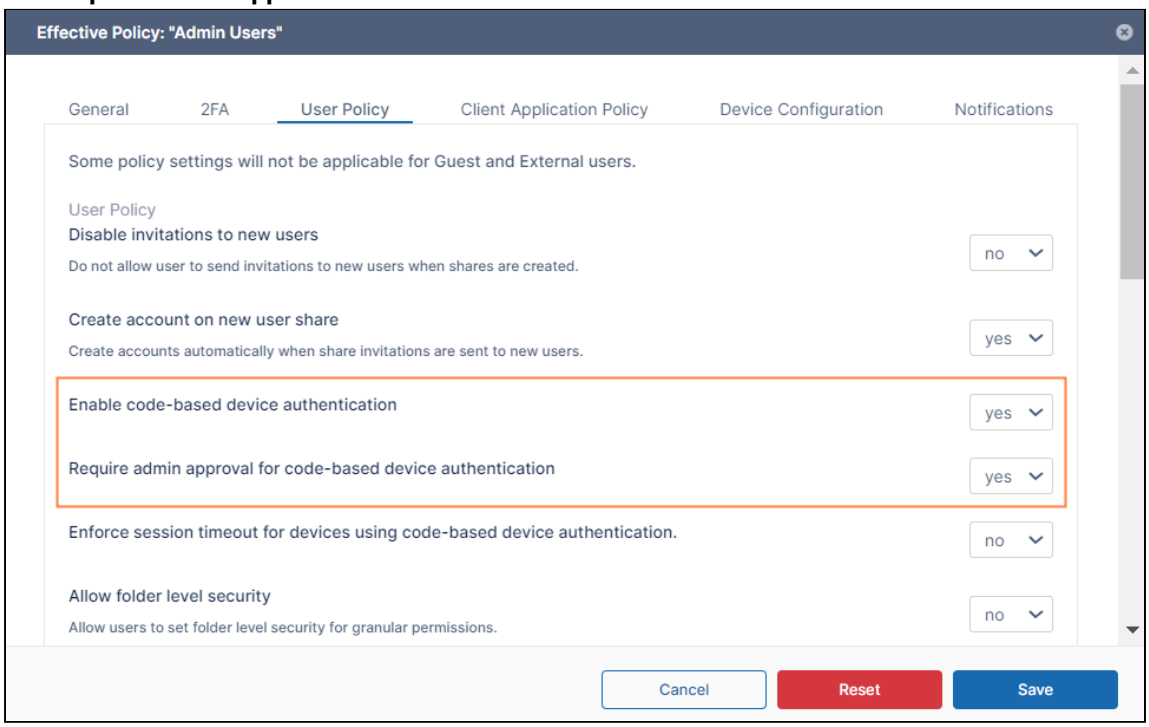
Requiring admin approval to log in with client devices

The **Enable code based device authentication** setting lets users log in to desktop apps using a device authorization code without admin approval. You can also can configure FileCloud to require logins to desktop apps to be approved by admins before being approved by users.

To require admin approval for device authentication:

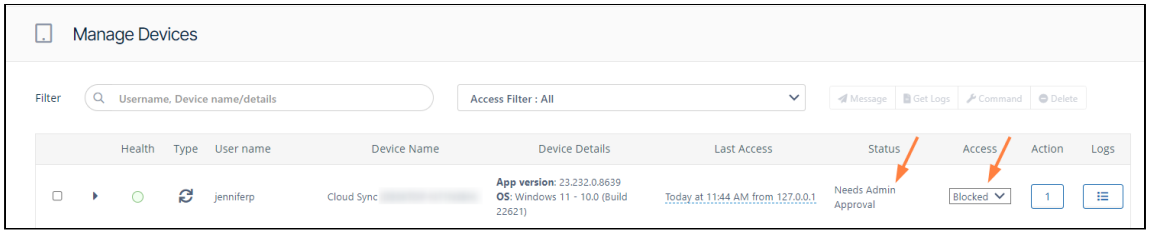
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Open a policy for edit.
3. In the **User Policy** tab, set **Enable code based device authentication** to **YES**.
   The **Require Admin Approval for Device Authentication** setting becomes enabled.

4. Set **Require Admin Approval for Device Authentication** to **YES.**

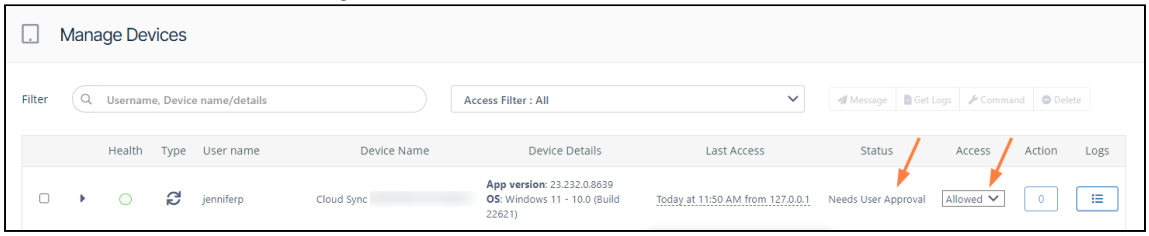


To approve a client device that has been sent to you for admin approval

1. Go to **Device Management** in the admin portal to view the listing for the device approval.
The device is listed with **Status** showing **Needs Admin Approval** and **Access** set to **Blocked**.



2. In the **Access** column, change **Blocked** to **Allowed**.
Now the **Status** column shows **Needs User Approval**, and the user must approve the client device (as shown above in **How users log in with device authentication**) and get an authorization code before log in can occur.



Enabling Basic Authentication

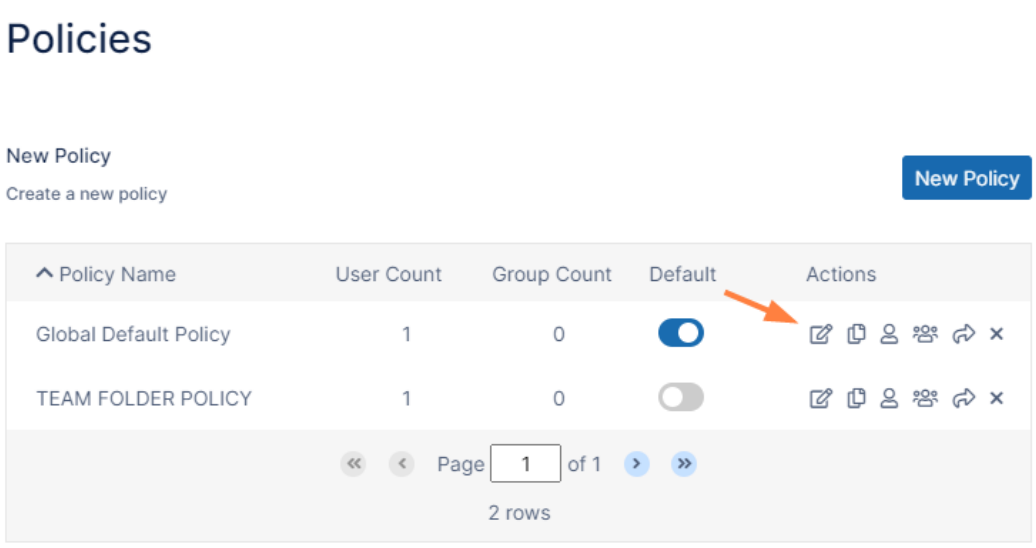
FileCloud supports enabling basic authentication for users through a policy setting.

To enable basic authentication:

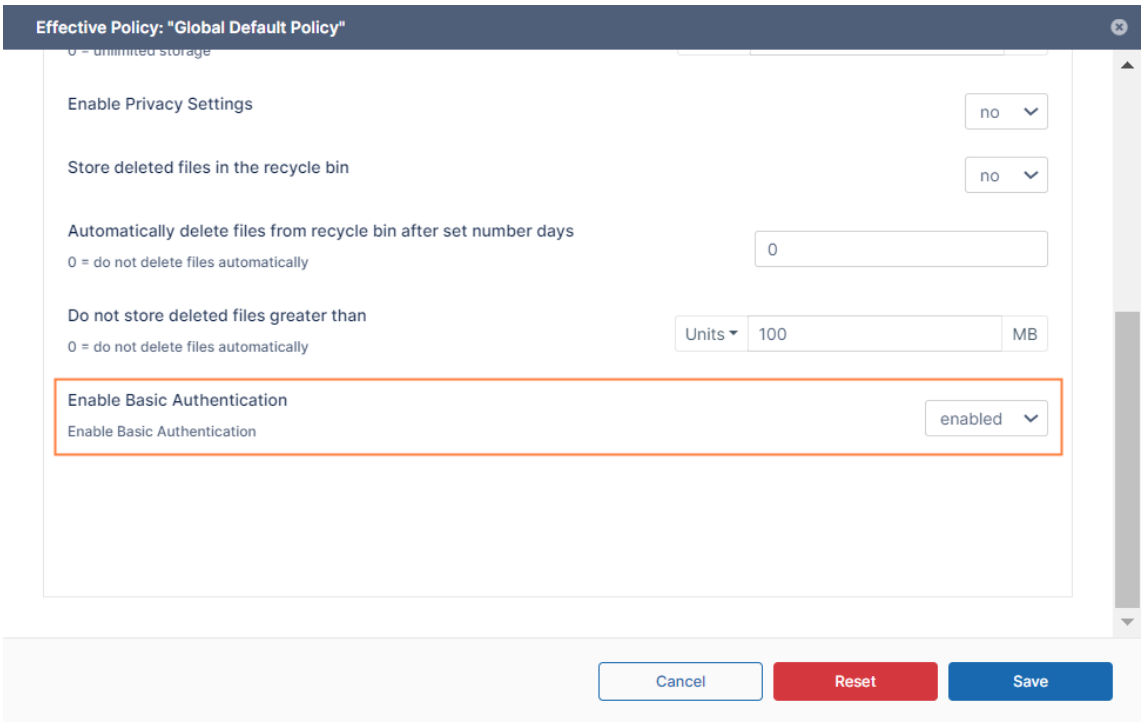
1. Add the setting for basic configuration to cloudconfig.php:
   a. Open cloudconfig.php.
      - Windows Location : C:\xampp\htdocs\config\cloudconfig.php
      - Linux Location : /var/www/html/config/cloudconfig.php
   b. Add the following and save:

```
define("TONIDOCLOUD_ENABLE_BASIC_AUTHENTICATION",1);
```

2. 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.
3. Click the Edit icon in the row for the users' policy.



   The **Policy Settings** dialog box opens.
4. Scroll to the bottom of the policy's **General** tab.
5. Set **Enable Basic Authentication** to **enabled**.



6. Click **Save**.
7. To enable specific users to use basic authentication, assign the policy to them.

Allowing Duplicate Usernames

To allow duplicate usernames for different domains

If you are using SSO, SSO API, or Active Directory (AD) to import users, FileCloud uses the imported user's email username (the portion before @) as the FileCloud username. However, by default, FileCloud does not allow creation of users with the same usernames.

If any of your users have multiple email addresses, there may be a situation where the email username (the portion before @) is the same but the domains are different in their multiple emails. In this case, FileCloud will attempt to convert the second email username (and any further emails with the same username) to the FileCloud username, which will fail because the username already exists.

However, if the multiple email addresses actually represent different users, you may use the following setting to enable creation of multiple users:

1. Open cloudconfig.php at
   - Windows: xampp/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Add the following and save:

```
define("TONIDOCLOUD_ALLOW_DUPUSERNAMES",1);
```

Now:
If you create a a user with the username **jocelynp** and email **jocelynp@gmail.com**, FileCloud creates a user with the username **jocelynp**.
Next, if you attempt to create a user with the username **jocelynp** and email **jocelynp@optimum.net**, FileCloud creates a user with the username **jocelynp_optimum**.
This follows for any subsequent emails with the same username and a unique domain.

Share Settings

The **Attach Share Password by Default for Public Shares** setting is available beginning in FileCloud 20.1.

File sharing allows users to provide public or private access to files stored in FileCloud Server with various levels of access privileges.

To control how users share files and folders in ways that are appropriate for your organization, administrators configure share settings.

Configure Sharing Defaults

The field **Allow comments for external users** is available beginning in FileCloud 23.251.

The fields **Public share default password length** and **Require complex public share passwords** are available beginning in FileCloud 23.242. Shares created with passwords prior to 23.242 maintain the passwords they were created with and are not required to comply with the new settings.

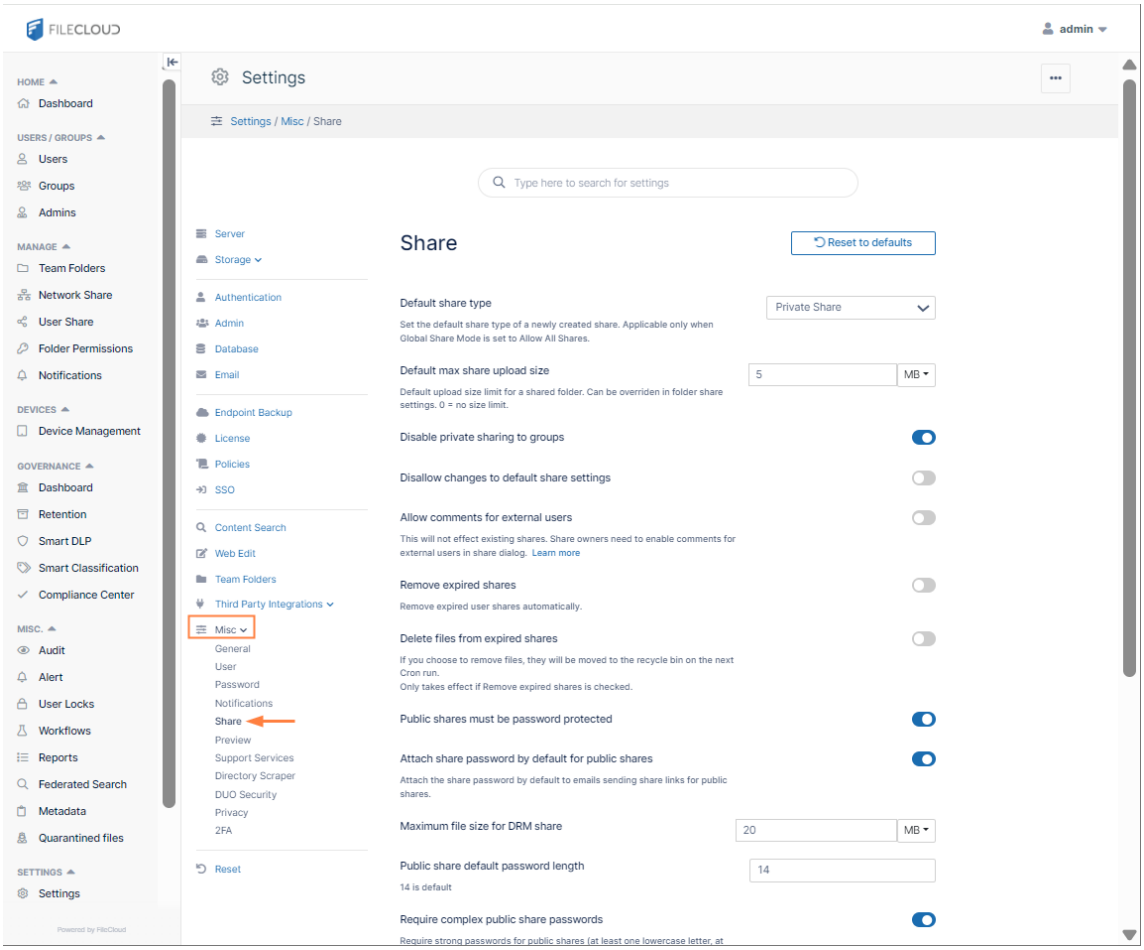
Beginning with FileCloud 23.241, the **Default Share Type** is **Private Share**.
Prior to FileCloud 23.241, the **Default Share Type** was **Public Share**.

When a user wants to share a file or folder, administrators can decide which options should be automatically selected.

> The settings are really just a recommendation and can be changed by the user, unless you disable the ability to change the defaults.
>
> Most of the settings below are set the Share settings page.

To open the Share settings page:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



The **Share** settings page opens.

Follow the procedures below to change the sharing defaults.

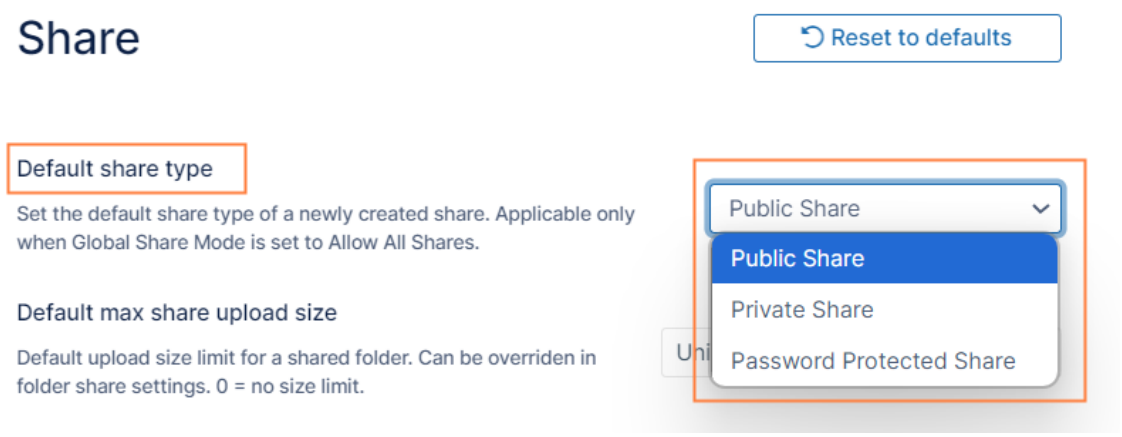
Default Share Type

This option tells FileCloud Server what type of share to automatically select when a user shares a file or folder. By default it is set to **Private Share**, but you may change it.

- Applicable only when **Share Mode** is set to **Allow All Shares**.
- This type can be changed by the user unless **Disallow Default Share Settings Change** is set.

To change the Default Share Type:

1. Open the Share settings page.
2. In **Default share type**, select the option you want to use.



Public Share	Allows users to share with anyone who has the link to the share. • Does not require the user you want to share with to have a FileCloud account. • Share a file with everyone with or without restrictions. • Share a file with everyone and require a password.
Private Share (Default)	Allows users to share with anyone who has the link and can log in to a FileCloud account. • Does require the user you want to share with to have a FileCloud account. • Requires an invitation to be sent to someone to create a FileCloud account if they don't already have one. • Share a file with all FileCloud users with or without restrictions. • Share a file with specific FileCloud users with or without restrictions.
Password Protected Share	Forces users to create a password when sharing a file or folder. • Recipients of the share are given the password when they receive the link to the share. • The share can be public or private.

3. Click Save.

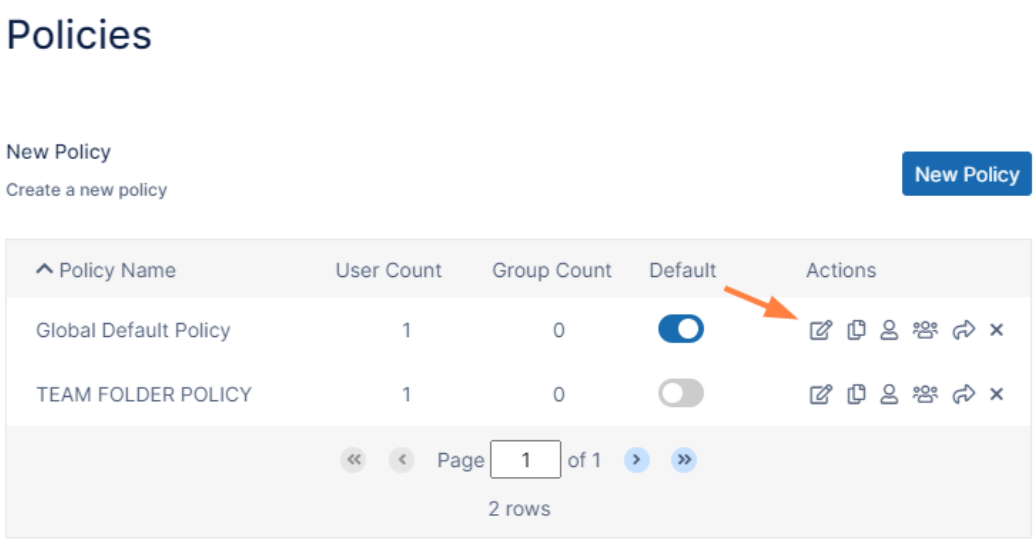
Set Expiration Days Default

You can allow users to share files and folders for as long as they exist, or you can set the number of days that a share remains active by default.

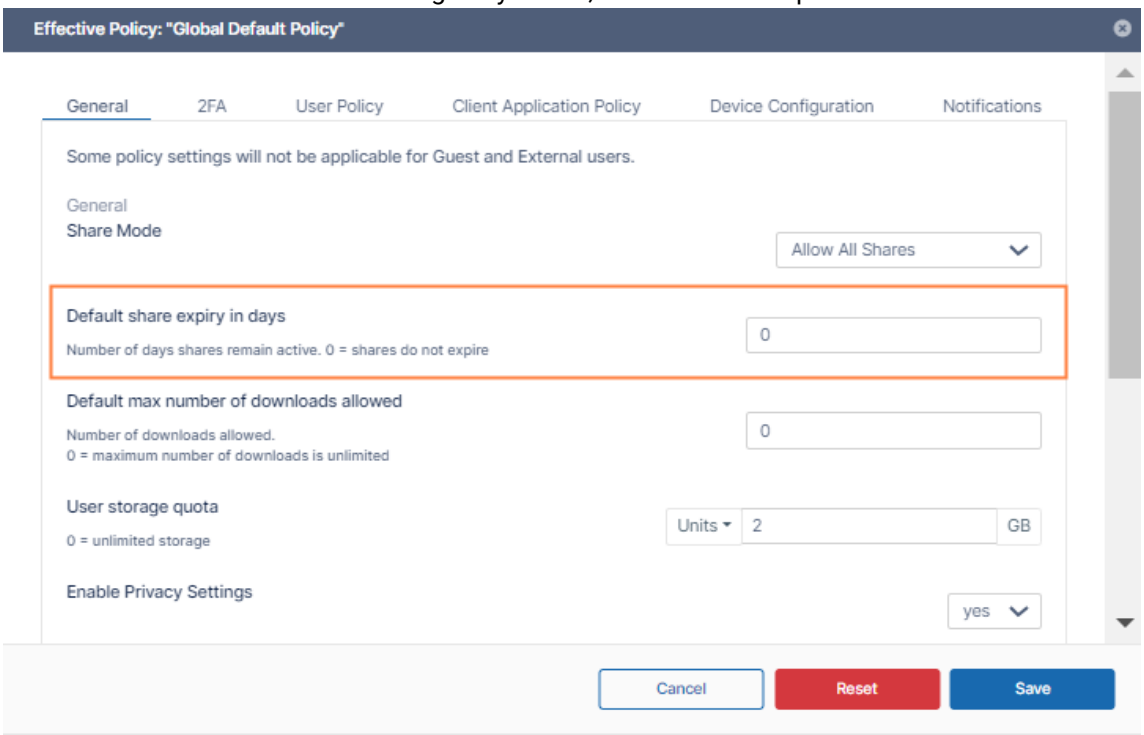
Note: This setting can be changed by the user unless **Disallow changes to default share settings** is set in the Share settings page.

To set the Share Expiry default 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. Click the Edit icon in the row for the users' policy.



3. Click the **General** tab.
4. Change the value of the **Default Share Expiry in Days** setting.
   A value of **0** means that unless changed by a user, shares do not expire.



5. Click **Save**.
   The value is only changed for users who are using this policy.

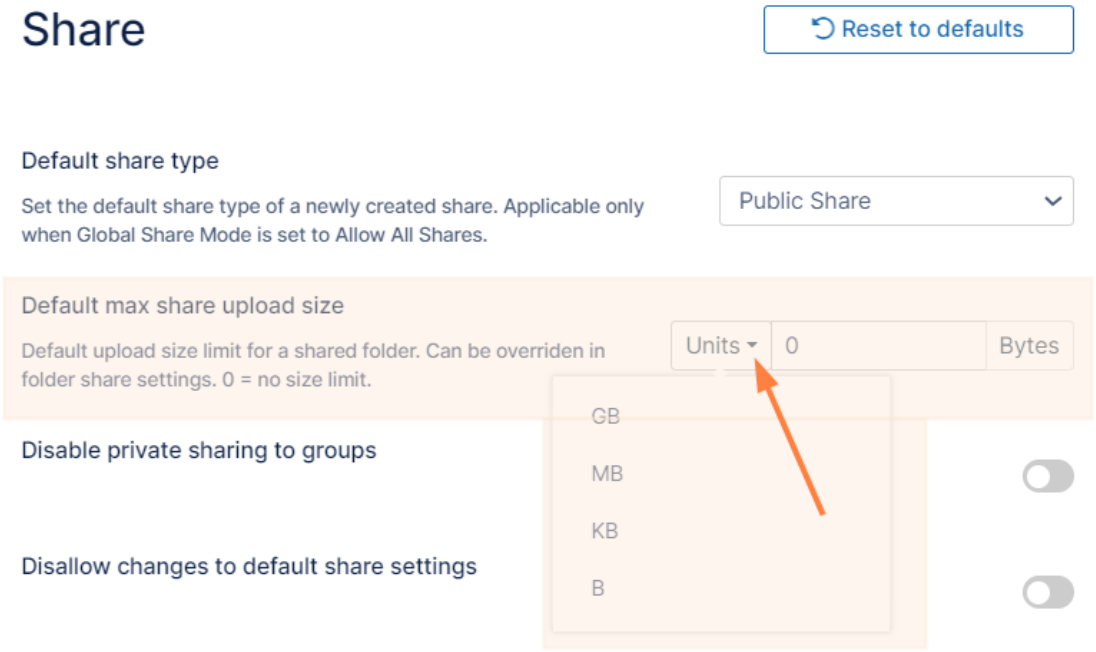
Default Max Share Upload Size

Administrators can allow users to upload files into a shared folder no matter how big it is, or you can set a suggested size limit.

- You can set a maximum size limit in any of the following units: **B**, **KB**, **MB**, **GB**.
- Using a value of **0** means that users can upload files into a shared folder no matter how big it is.
- This setting can be changed by the user in the shared folder settings.

To set the Max Upload size default for Shares:

1. Open the Share settings page.
2. In **Default max share upload size**, select a choice in **Units**, and then type in the file size limit you want to use.



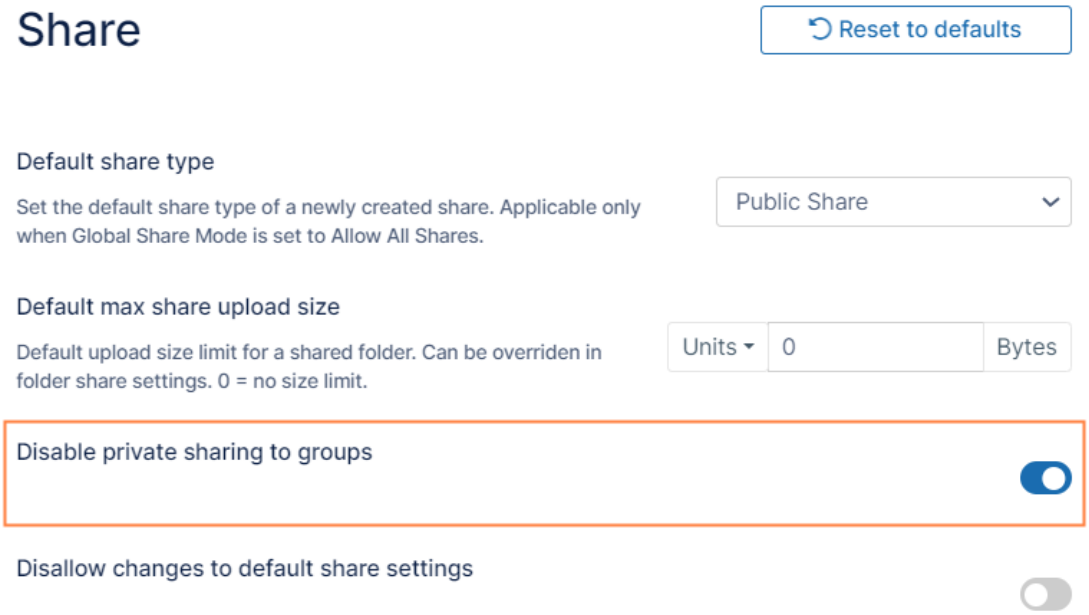
3. Click **Save**.

Disable Sharing to Groups for Private Share

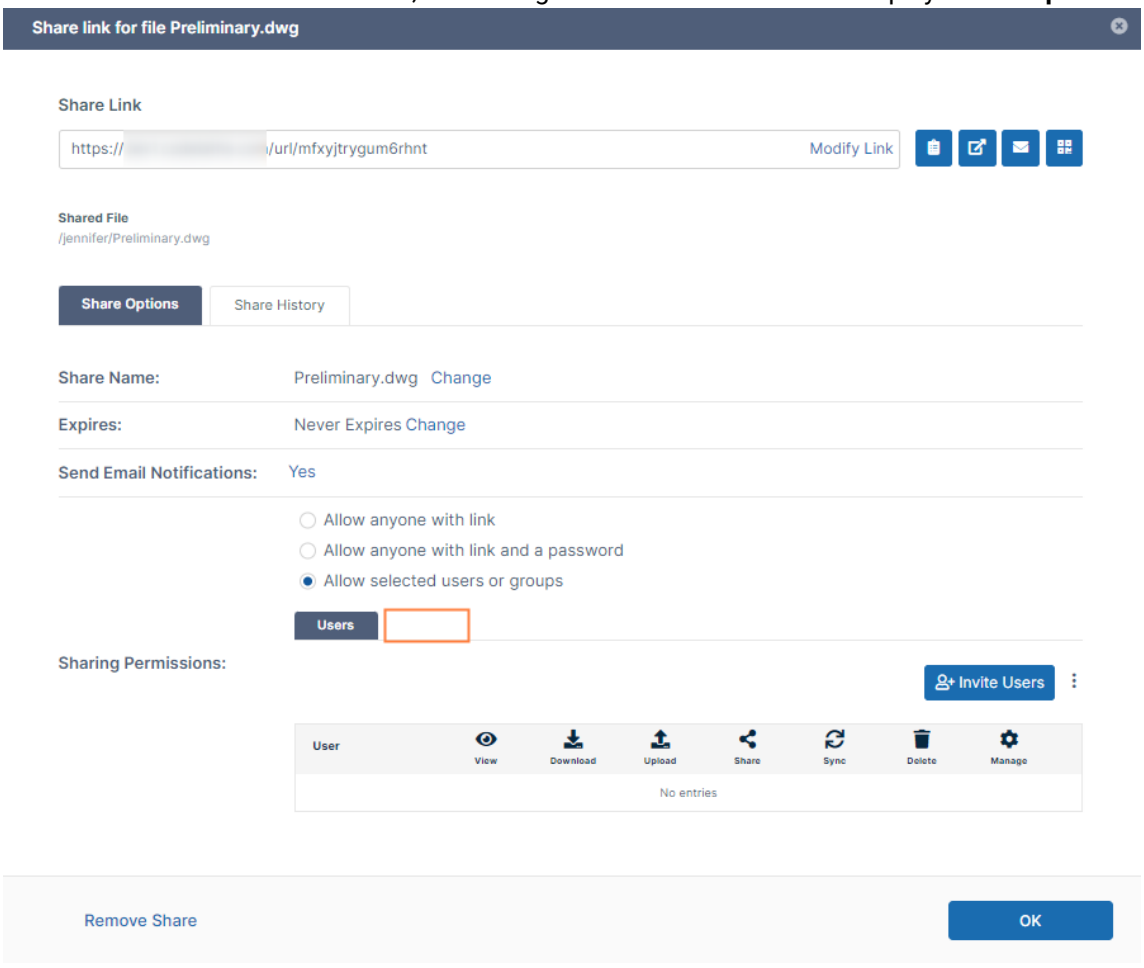
You can check **Disable private sharing to groups** to hide the Group option when users or admins privately share a file or folder.

To disable users and admins from sharing to groups:

1. Open the Share settings page.
2. Scroll down to **Disable private sharing to groups** and enable it.



3. Click **Save**.
   Now when a file or folder is shared, the Manage Share window does not display the **Group** tab.

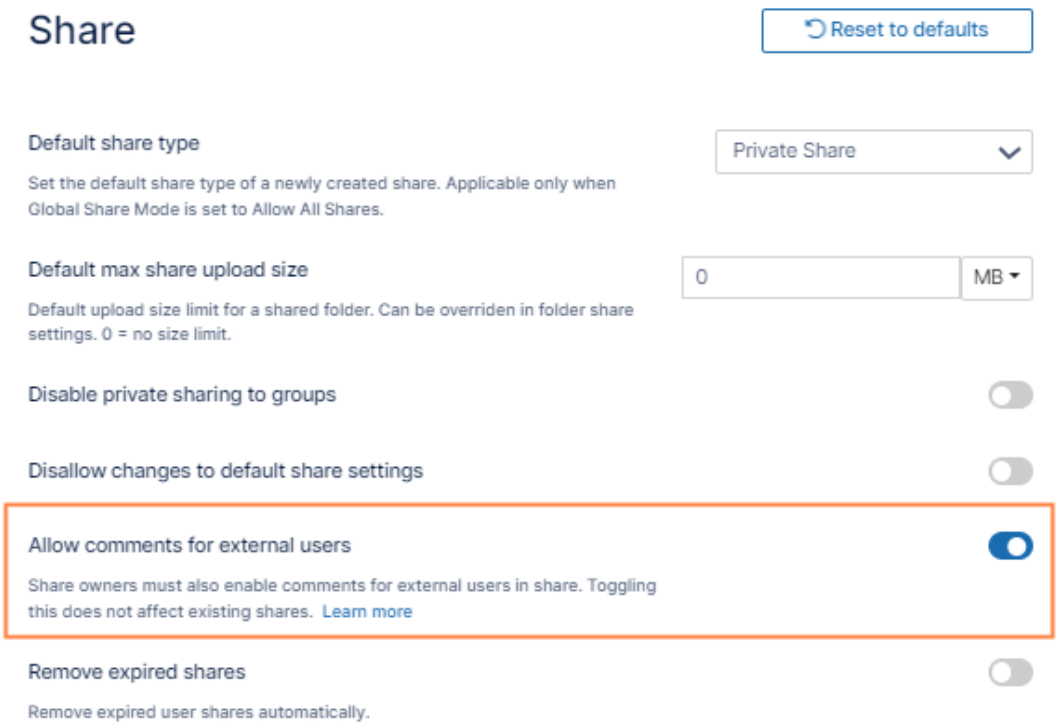


Allow External Users to Add Comments

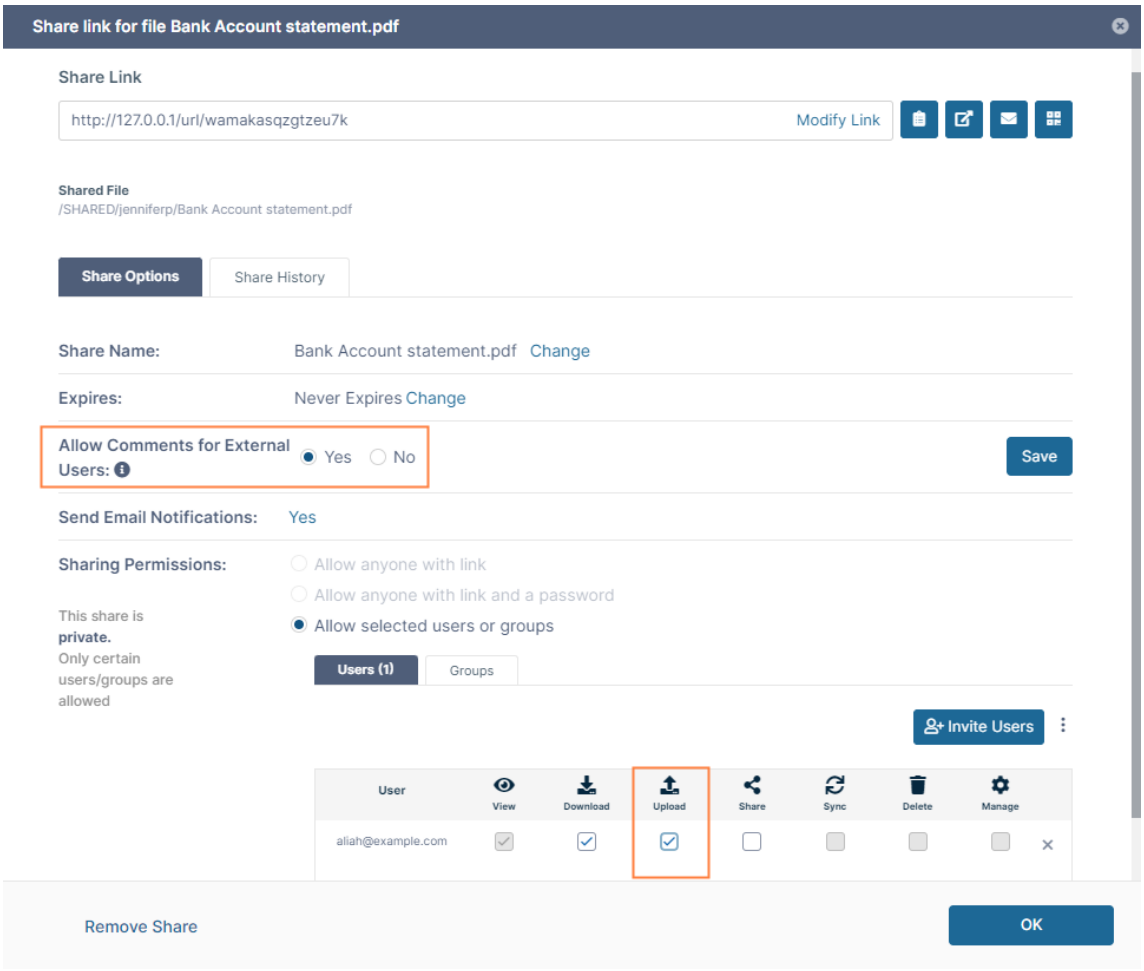
By default, external users cannot add comments to shares. However, you can enable the **Allow comments for external users** setting to allow external users to add comments to private shares of files and folders. Note that for this setting to be effective, the share creator must also allow comments by external users and give the external user write access to the share.

To allow external users to add comments:

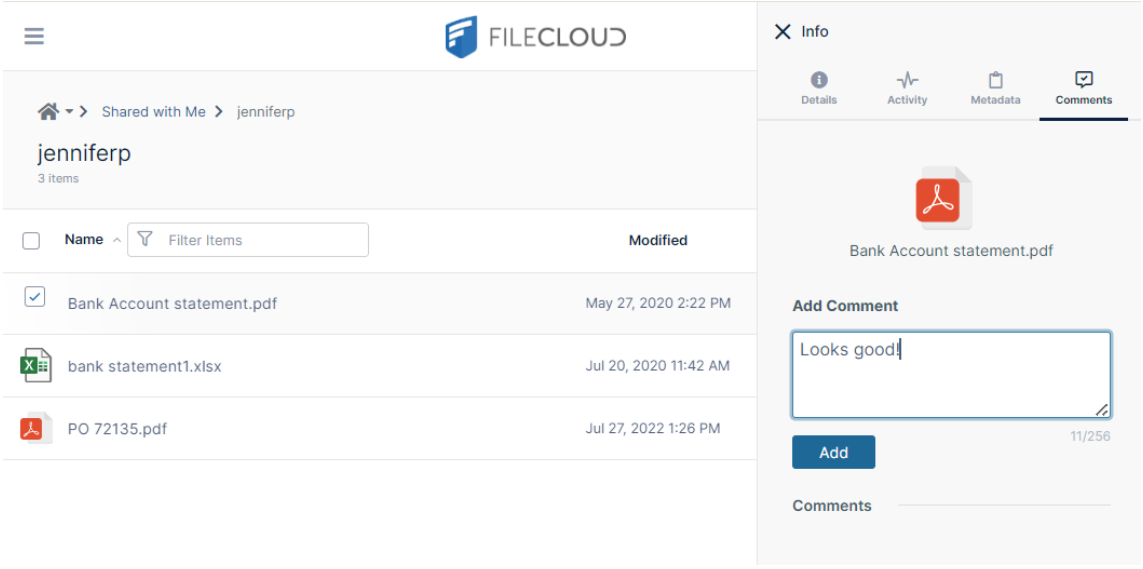
1. Open the Share settings page.
2. Scroll down to **Allow comments for external users** and enable it.



Now, if a share creator enables the option **Allow Comments for External Users** and gives the external user write (upload) access, as shown below . . .

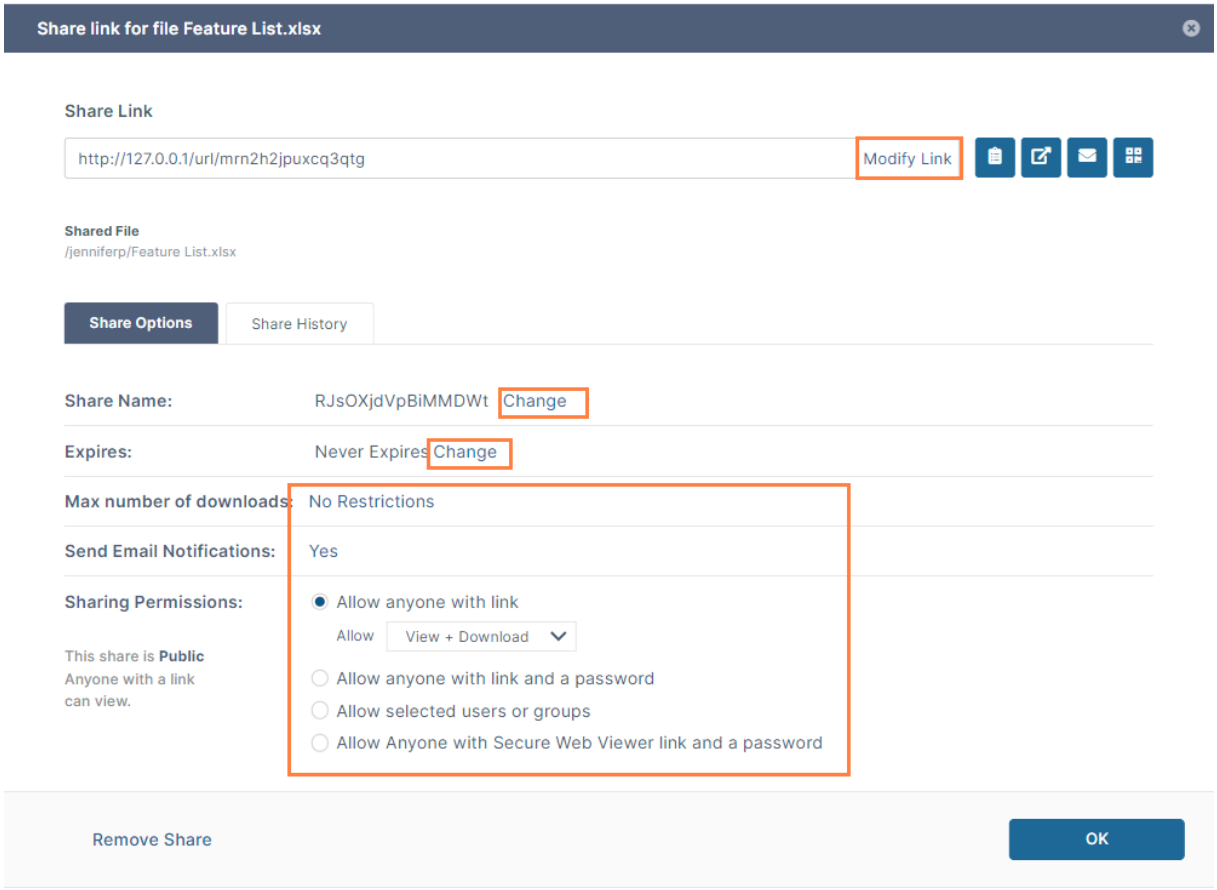


. . . the external user can select the share in the **Shared with Me** listing, click the Comments tab, and add a comment to the share:



Disallow/Allow Default Share Settings Change

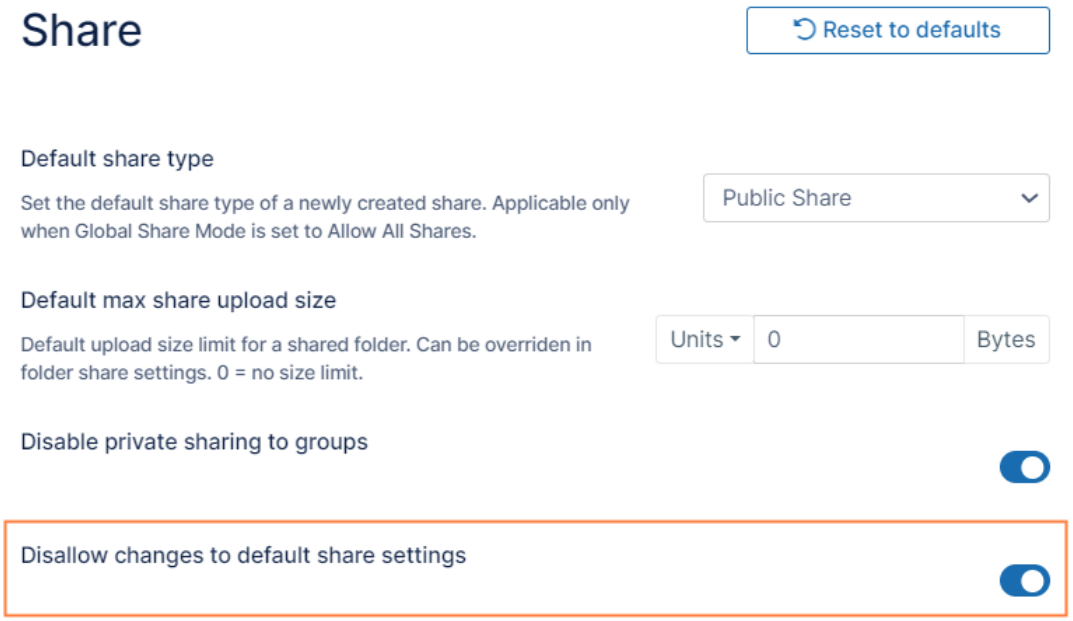
The **Share link** dialog box appears with settings that the user can modify:



However, you can prevent users from changing these settings.

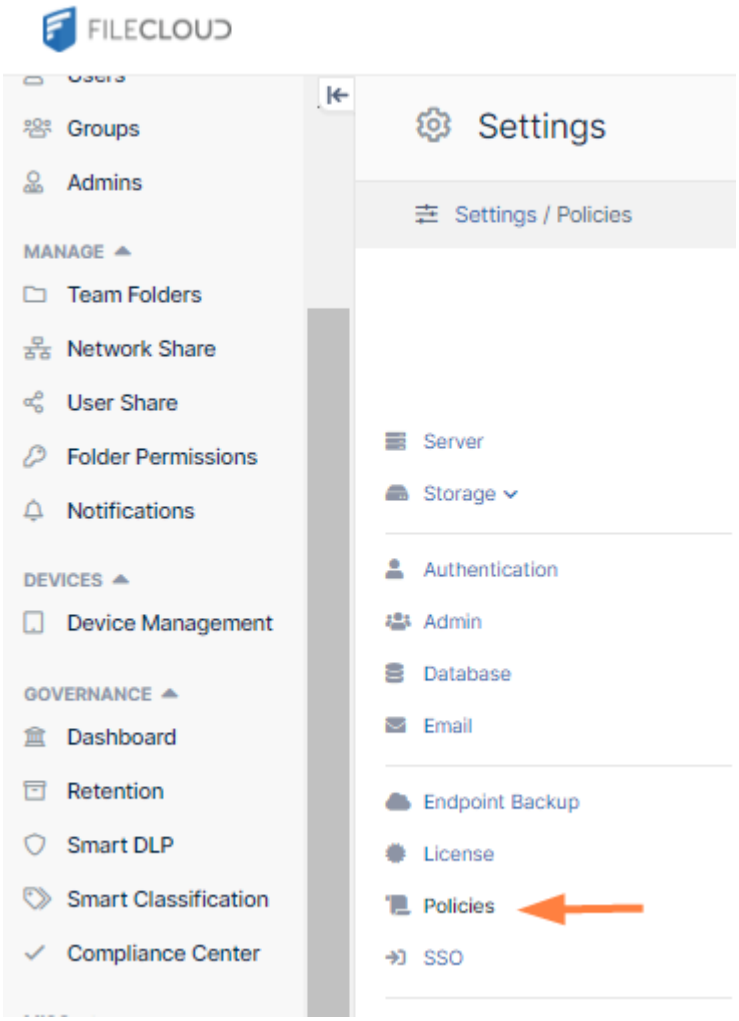
To require users to share files and folders with the default settings you have configured:

1. Open the Share settings page.
2. Scroll down to **Disallow changes to default share settings** and enable it**:**

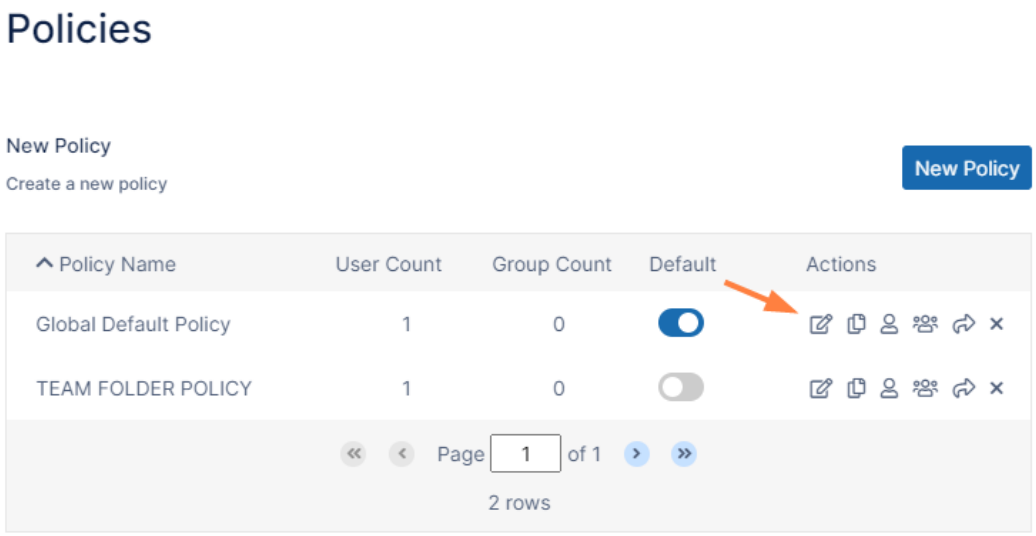


AND

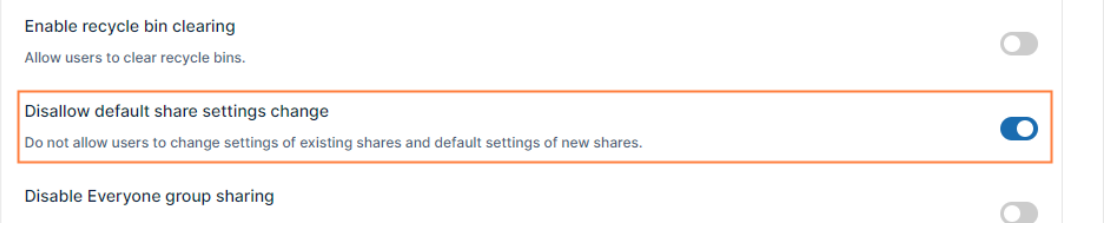
3. In the inner navigation bar on the left of the page, click **Policies**



4. The **Policies** page opens.
5. Click the Edit icon for the policy of the users who you want to prevent from changing default share settings.

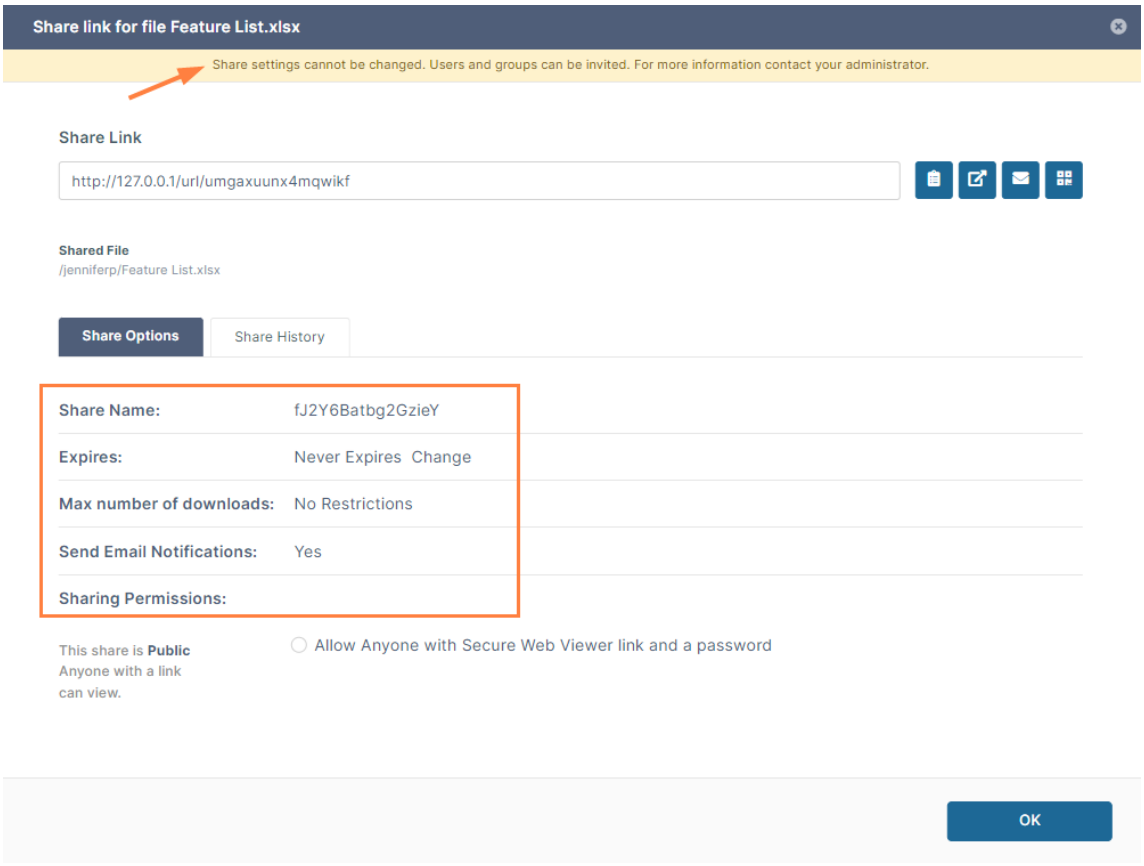


6. Click the **User Policy** tab.
7. Scroll down to **Disallow Default Share Settings Change**, and enable it.



8. Repeat steps 5, 6, and 7 for the policies of all users who you want to prevent from changing default share settings.

   Now, for users with those policies, the **Share link** dialog box has a message at top that share settings cannot be changed, and there are no change buttons or clickable options:



Disable Manage Share Options

After a user opens a browser and logs in to the User Portal, they can share a folder privately.

- This share has the ability to be shared again by members.
- Share owners can also designate another user to manage those re-shares of the original shared folder by selecting the **Allow Manage option.**

If the folders being shared are in Network Folders, and there are a large number of shares and users working with Network Folders, displaying a list of shares may take too long or even timeout.

Now you can configure FileCloud to disable the **Allow Manage** option for shares in Network Folders to decrease the time it takes to display the list of shares.

- **TONIDOCLOUD_MANAGE_SHARE_ENABLE** is a new config that can be set to 0 to completely disable the **Allow Manage** sharing option for Network Folders.

To disable the Allow Manage option for Network Folders:

1. Open the following file for editing:

For Windows:

```
c:\xampp\htdocs\config\cloudconfig.php
```

For Linux:

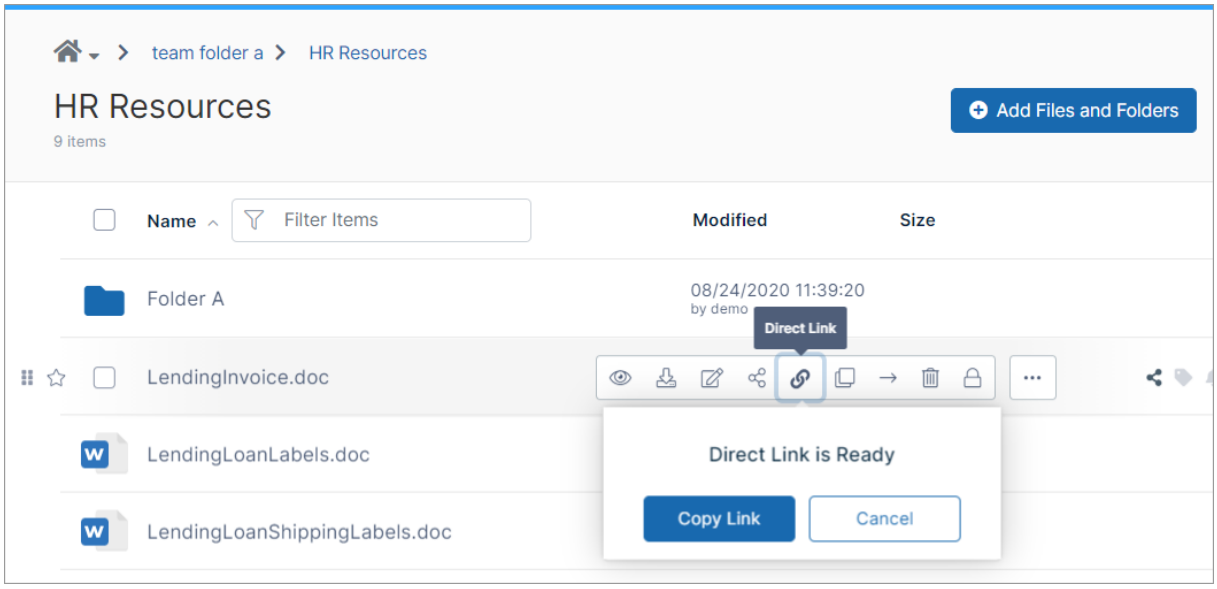
```
/var/www/html/config/cloudconfig.php
```

2. Add the following line:

```
define("TMANAGE_SHARE_ENABLE", "0");
```

Hide Direct Link option for shared files and folders

In the User portal, the **Direct Link** action is available when users select a file or folder in Team Folders or Shared with Me:



Beginning in FileCloud 20.2, you can configure FileCloud to hide the **Direct Link** action.

To hide the Direct Link action:

1. Open the following file for editing:
   For Windows:

   ```
   XAMPP/htdocs/config/cloudconfig.php
   ```

   For Linux:

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

2. Add the following line:

```
define('TONIDOCLOUD_HIDE_SHARE_DIRECTLINK_OPTION', 1);
```

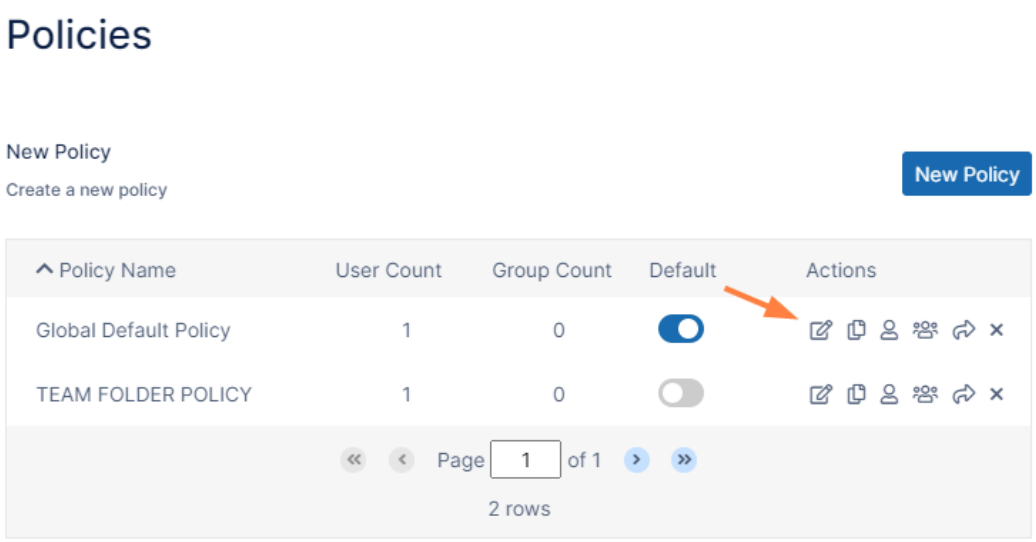
When a user selects a file or folder in Team Folders or Shared with Me, the direct link option no longer appears.

Disable sharing to the Everyone group

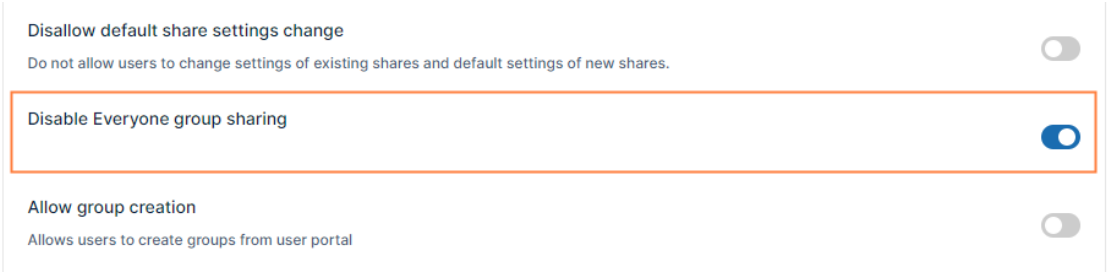
The **Everyone** group includes all of your active Full users. If you do not want to allow sharing of files or folders with all of your users at once, you can disable sharing to the **Everyone** group.

To disable sharing to the Everyone group:

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. Click the Edit icon for the policy of the users who you want to prevent from sharing with the **Everyone** group.



3. The **Policy Settings** dialog box opens.
4. Click the **User Policy** tab.
5. Scroll down to **Disable Everyone group sharing** and enable it.



6. Click **Save.**
7. Repeat steps 2 through 5 for the policies of all users who you want to prevent from sharing with the **Everyone** group.

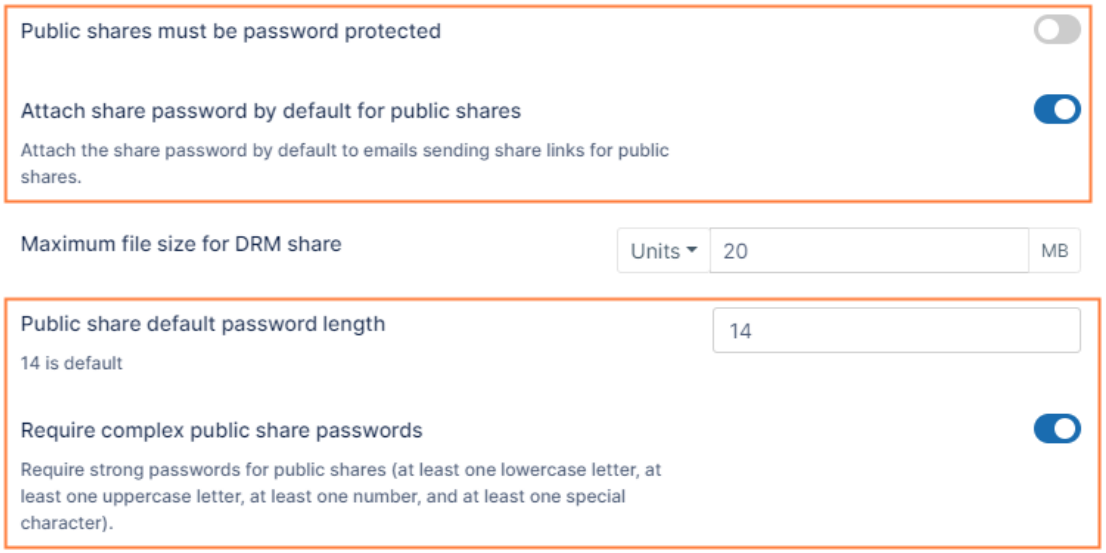
   Now, when these users select a group to share with, the **Everyone** group does not appear.

Default settings for public share passwords

There are several share settings that enable you to set defaults for public share passwords.

To access and configure the public share password settings:

1. Open the Share settings page.
2. Scroll down to the public share settings:



3. To require users to password protect public shares, enable **Public shares must be password protected**.
   The option **Allow anyone with link** is now unavailable when a user shares a file or folder.
4. When **Attach share password by default for public shares** is set to **enabled** (the default value), share passwords are included in share link emails sent from the share. Disable the setting to avoid including share passwords in the emails.
5. **Public share default password length** is **14**. Enter a new value to change the minimum length.

6. By default, **Require complex public share passwords** is enabled. This requires share passwords to have at least one lowercase letter, one uppercase letter, one number, and one special character. To allow users to enter any combination of characters, disable the setting.

To require users to accept FileCloud Terms of Service before accessing a public share or a password-protected share, see Terms of Service

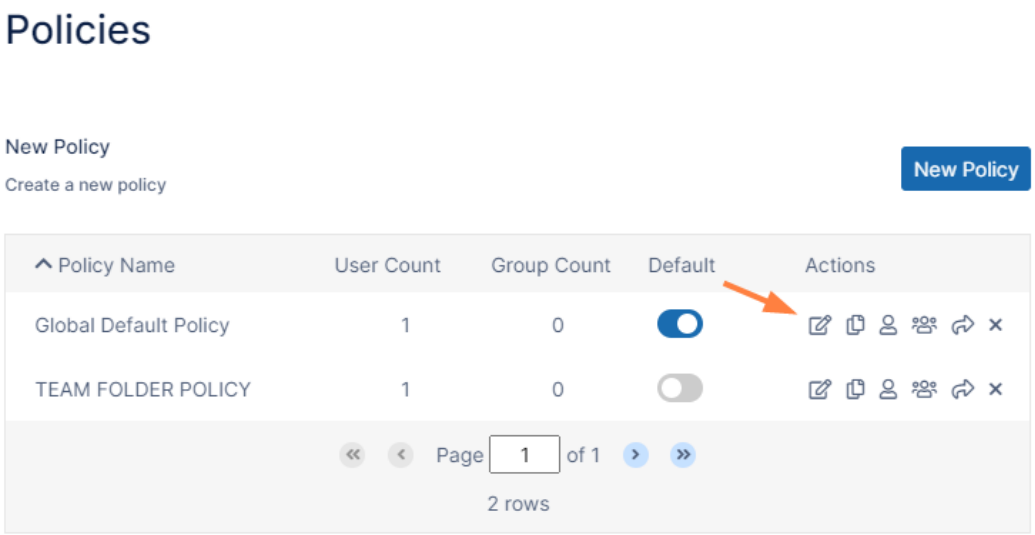
Set the Share Mode

FileCloud allows administrators to manage file shares created by their users.

- You can choose to allow or restrict file sharing for accounts in FileCloud by setting the **Share Mode**.
- The **Share Mode** setting appears in policies on the **General** tab of a policy, and is set to **Allow All Shares** by default.

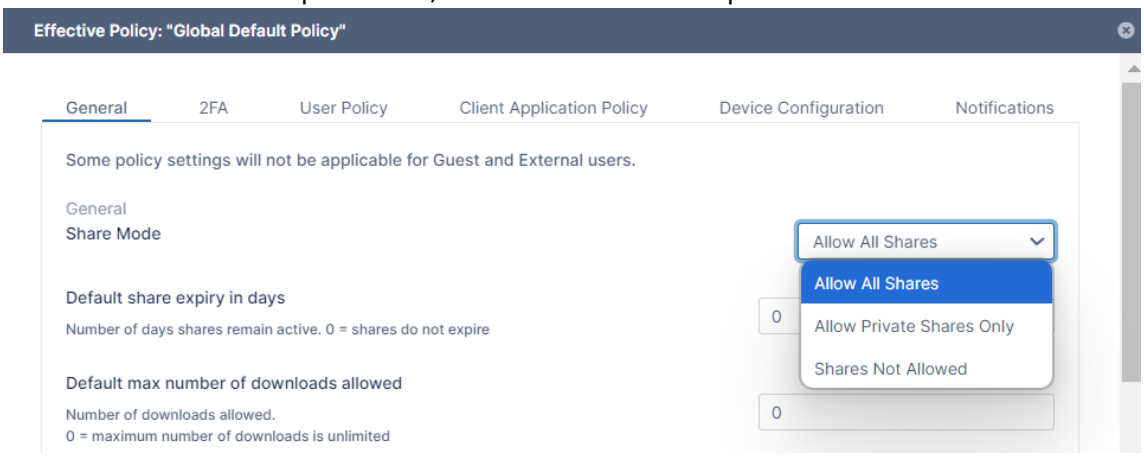
To manage the share mode for a set of users:

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. Click the Edit icon for the policy associated with the set of users.



3. Click the **General** tab.

4. Click the **Share Mode** drop-down list, and choose one of the options. Then click **Save**.



Option	Description
Allow All Shares	Allows users to share any file or folder with custom permissions. A file or folder can be shared with: • Anyone with access to the link (Public Share). **No FileCloud account required.** • Anyone with access to the link (Public Share) and a password. **No FileCloud account required.** • Another user in FileCloud (Private share). **FileCloud account required.** The shared files will show up in the **Shared with Me** folder.
Allow Private Shares Only	Allows users to share any file or folder with a user that has an existing FileCloud account. Sharing Privately requires: • The recipient(s) to be another user in FileCloud (Private share). **FileCloud account required.** The shared files will show up in the "Shared with Me" folder. • An invitation to be sent to someone to create a FileCloud account so that they can access a share. • Users to configure the share with or without restrictions.
Shares Not Allowed	Prevents users from sharing any file or folder. ⚠ If you choose this option, then no other sharing settings that you configure will be in effect.

Specify Sharing Expiration

Administrators can configure 3 main expiration features of a shared file or folder.

Feature	Options	Description
Number of days	• No expiration (0) • Expire in a certain number of days	Allow sharing to happen for a temporary time, or allow shares to exist as long as the file or folder exists.
Remove share links/shared files	• Remove the URL links to shares automatically • Remove shared files automatically	Specify what happens when a shared file or folder is no longer accessible from the Share link. • Expired URL links will be removed automatically on the next Cron run (In this case the files will not be affected.). • If you choose to remove files, they will be moved to the Recycle Bin on the next Cron run.
Notifications	• Alert users with access to a share that it will expire soon • Specify the number of days before the share expires that you want to send the email notification	You can have FileCloud send email to everyone who has access to the shared file or folder.

Set Expiration Period

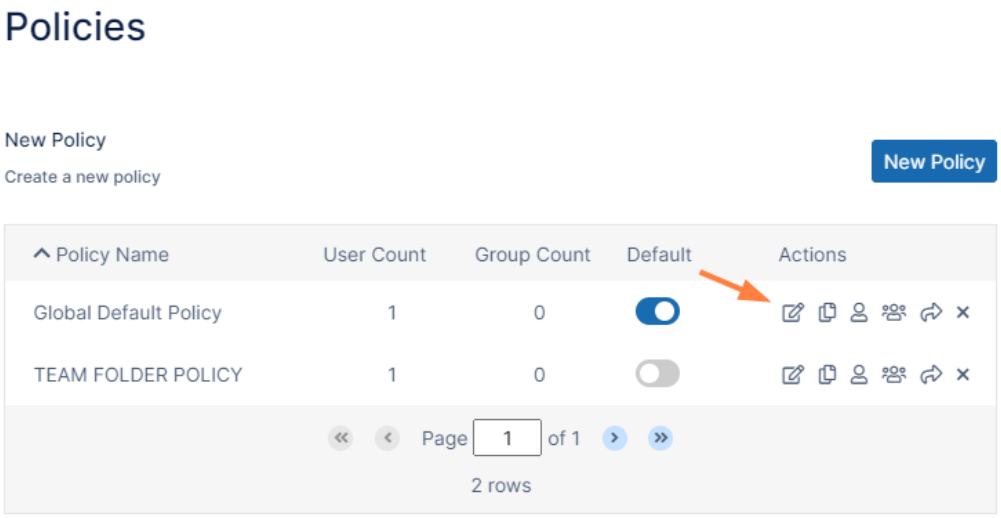
Set Expiration Days Default

You can allow users to share files and folders for as long as they exist, or you can set the number of days that a share remains active by default.

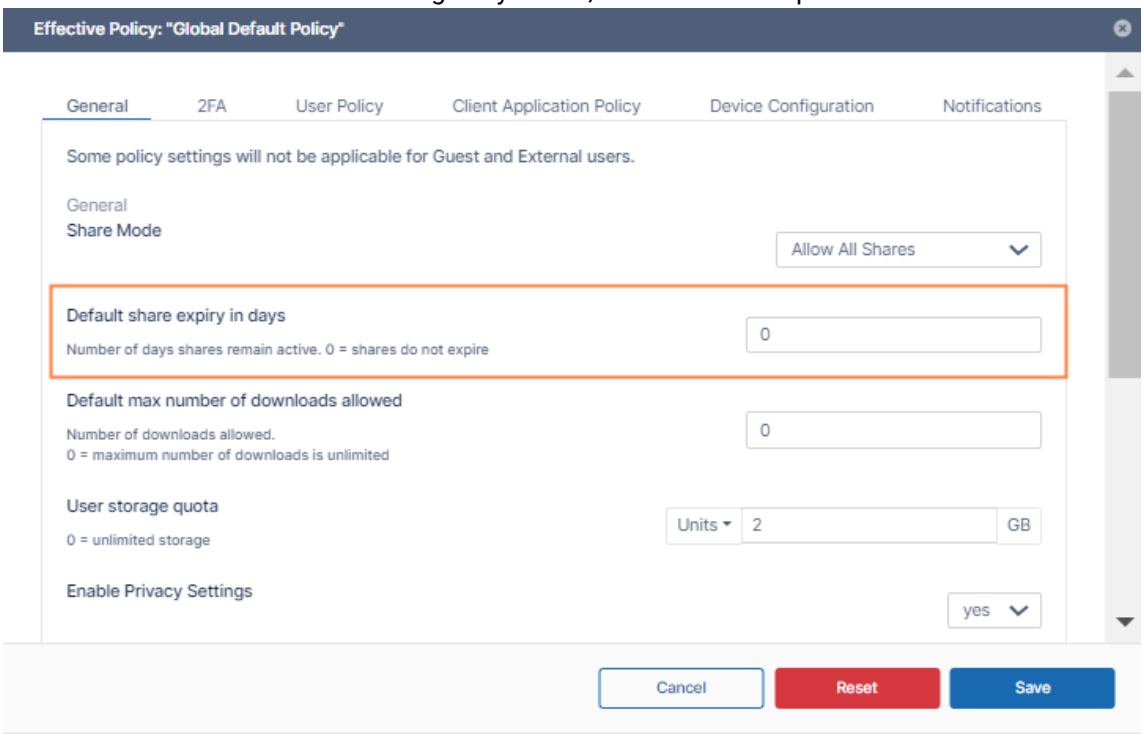
Note: This setting can be changed by the user unless **Disallow changes to default share settings** is set in the Share settings page.

To set the Share Expiry default 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. Click the Edit icon in the row for the users' policy.



3. Click the **General** tab.
4. Change the value of the **Default Share Expiry in Days** setting.
   A value of **0** means that unless changed by a user, shares do not expire.



5. Click **Save**.
   The value is only changed for users who are using this policy.

Set Expiration Actions

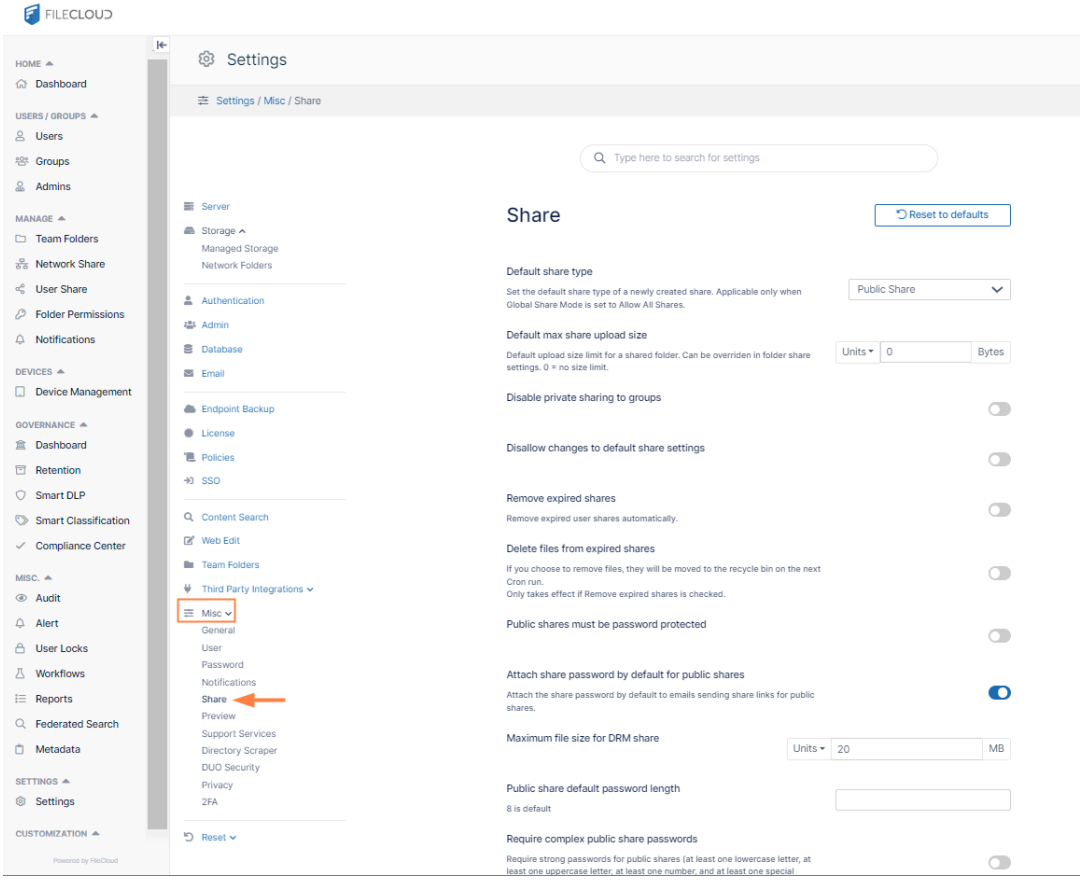
Remove Expired Shares

Expired URL links will be removed automatically on the next Cron run (In this case the files will not be affected.)

If you choose to remove files, they will be moved to the Recycle Bin on the next Cron run

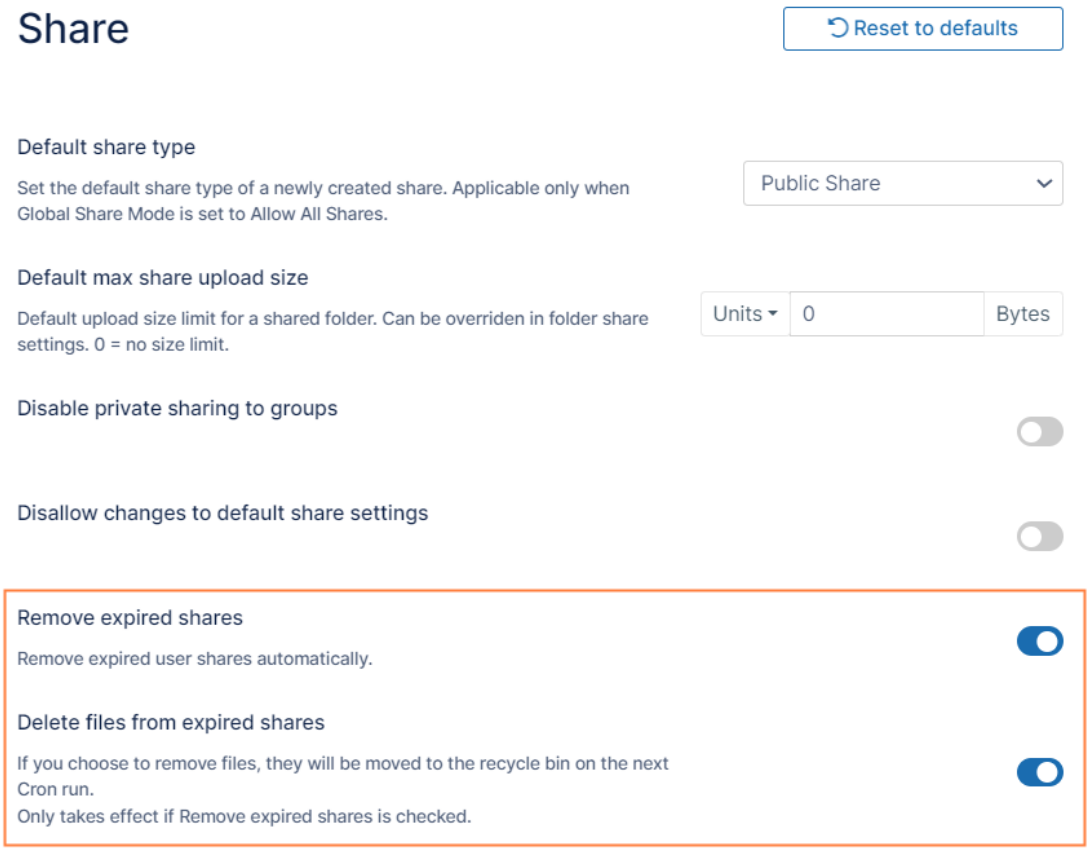
To automatically remove expired links or expired files:

1. Open the Share settings page.
   To open the Share settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



   The Share settings page opens.
2. Enable **Removed expired shares,**
   or
   enable both **Remove expired shares** and **Delete files from expired shares.**
   Note: **Delete files from expired shares** is not effective unless **Removed expired shares** is also

enabled.



3. Click **Save**.

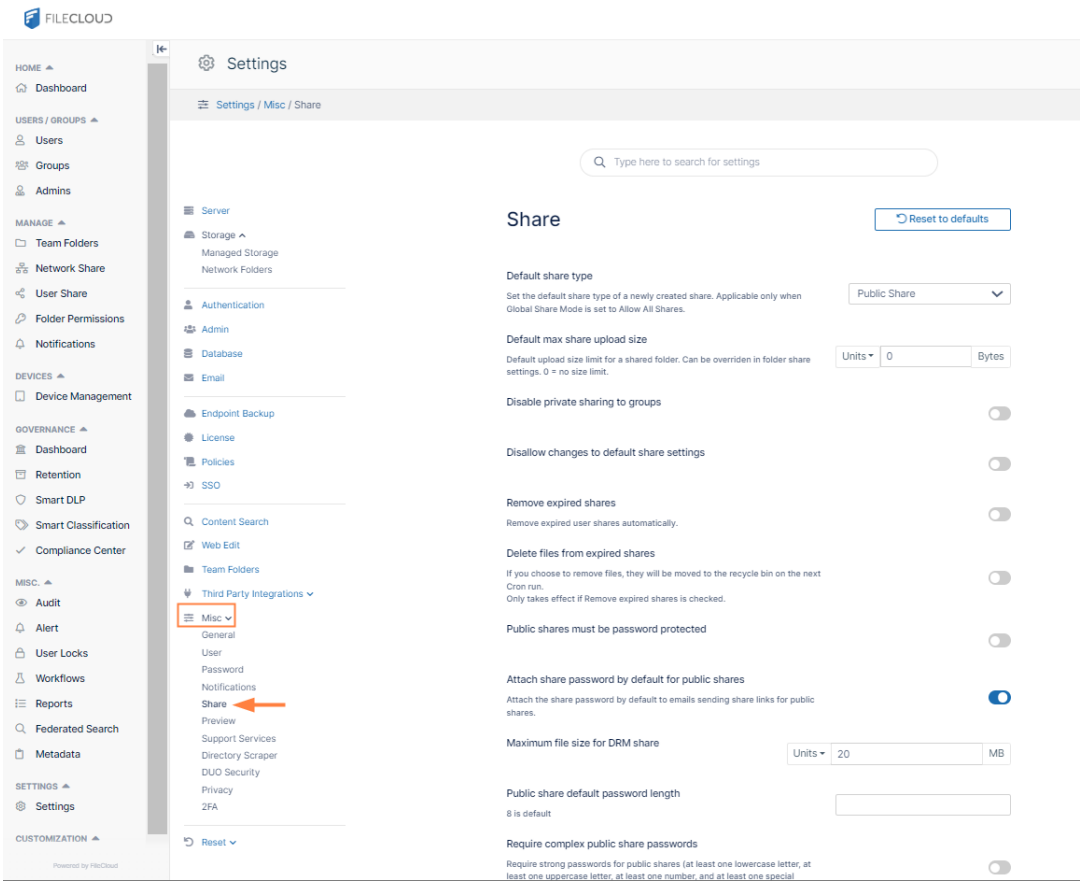
Send Expiration Notifications

Alert share Users About Upcoming Expiration

You can have FileCloud send email to all of a share's recipients to notify them that the share will expire soon. You can also specify how many days before the share expires that the email notification is sent.

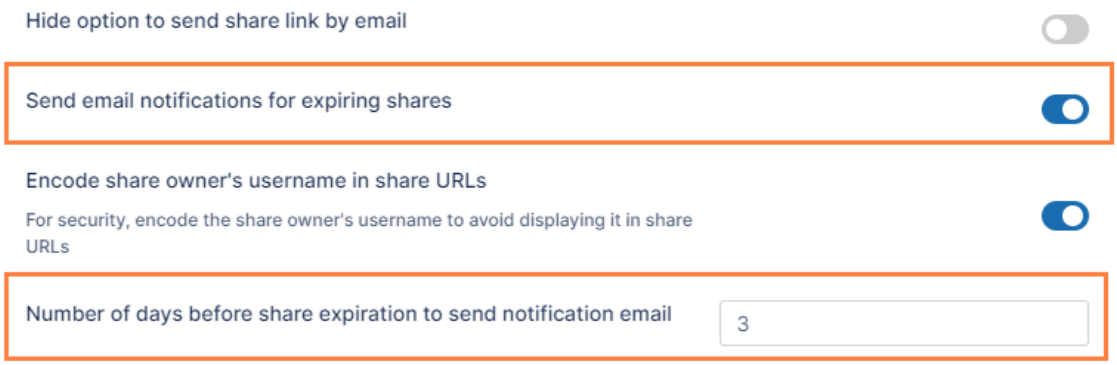
To send an email alert that a share will soon expire, and to specify the number of days before expiration the email is sent:

1. Open the Share settings page.
   To open the Share settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



The Share settings page opens.

2. Scroll to the bottom of the page.
3. To send emails notifying share recipients that shares are expiring, enable **Send email notifications for expiring shares**.
   By default, the number of days before a share expires that an email is sent is **3**.
4. To change the number of days before a share expires that an email is sent, change the value in **Number of days before share expiration to send notification email**.
   This setting only applies if **Send email notifications for expiring shares** is enabled.

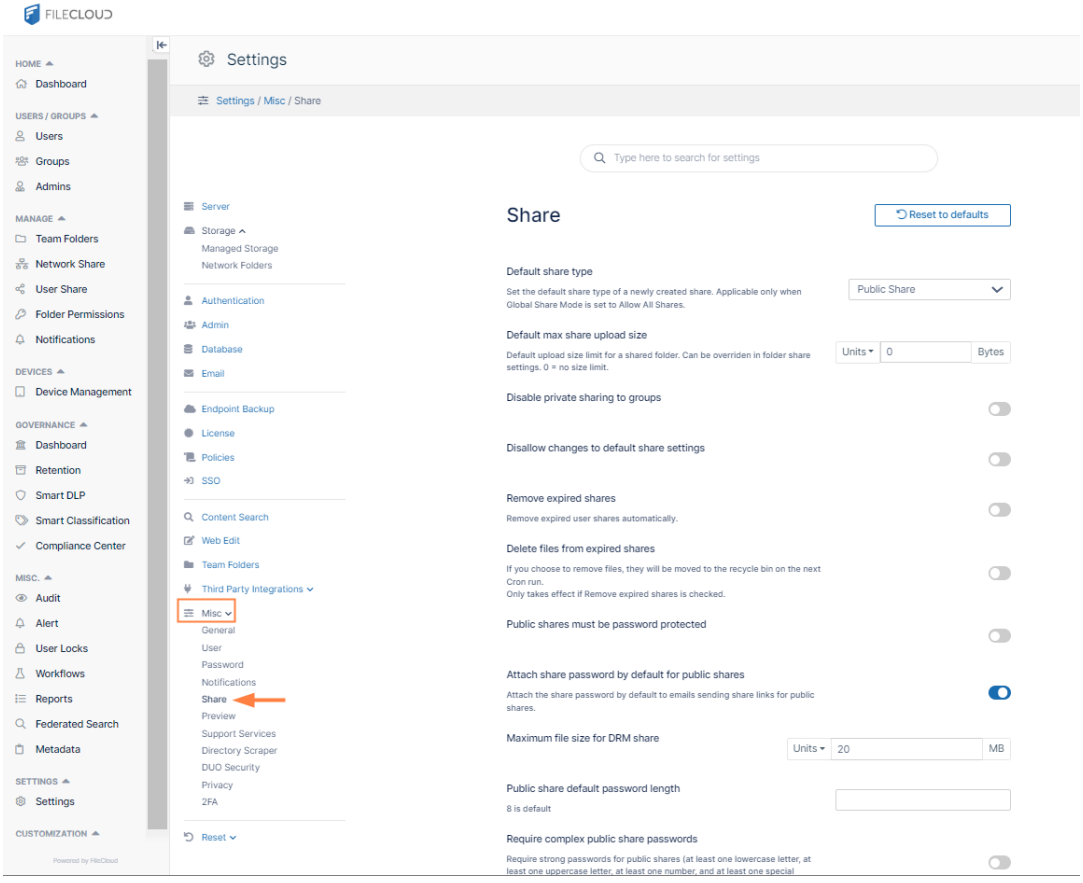


Secure Shares

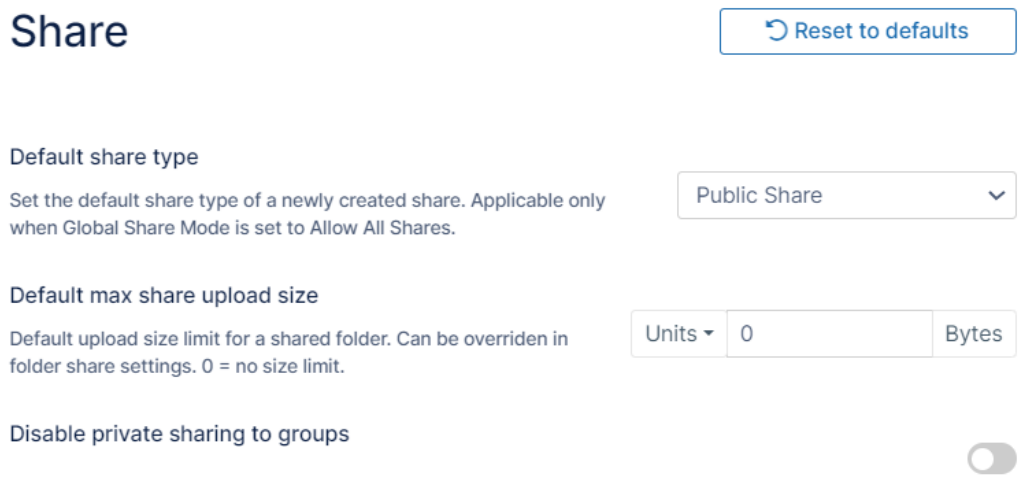
Instead of just communicating the most secure sharing procedure to your users, administrators can configure special settings to ensure a more secure environment when users are sharing files.

To password protect shares, prevent share name changes, or hide the option for sending share links by email:

1. Open the Share settings page.
   To open the Share settings page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



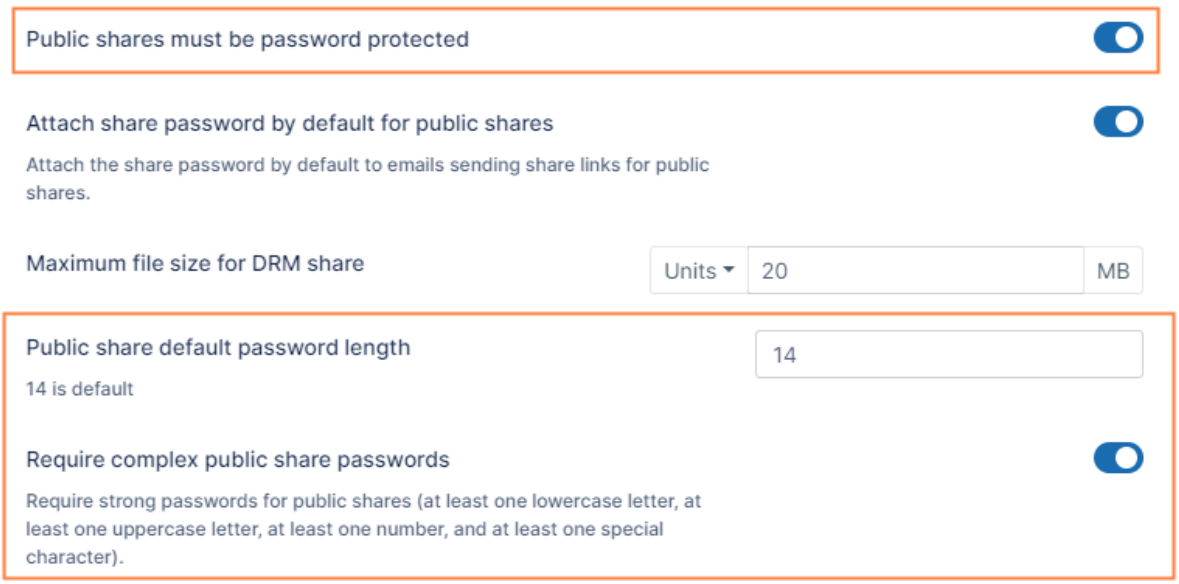
The **Share** settings page opens.



2. Configure any of the following secure share settings:

Password Protect Shares and Require Complex Passwords

Administrators can require users to create all public shares with a password for an extra layer of security. Users cannot disable the use of passwords when this is set.
By default, FileCloud requires public share passwords of 14 characters in length that include at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character. Administrators may change these settings.



To require strong password protection:

1. In the **Share** settings page, scroll down to the password settings.

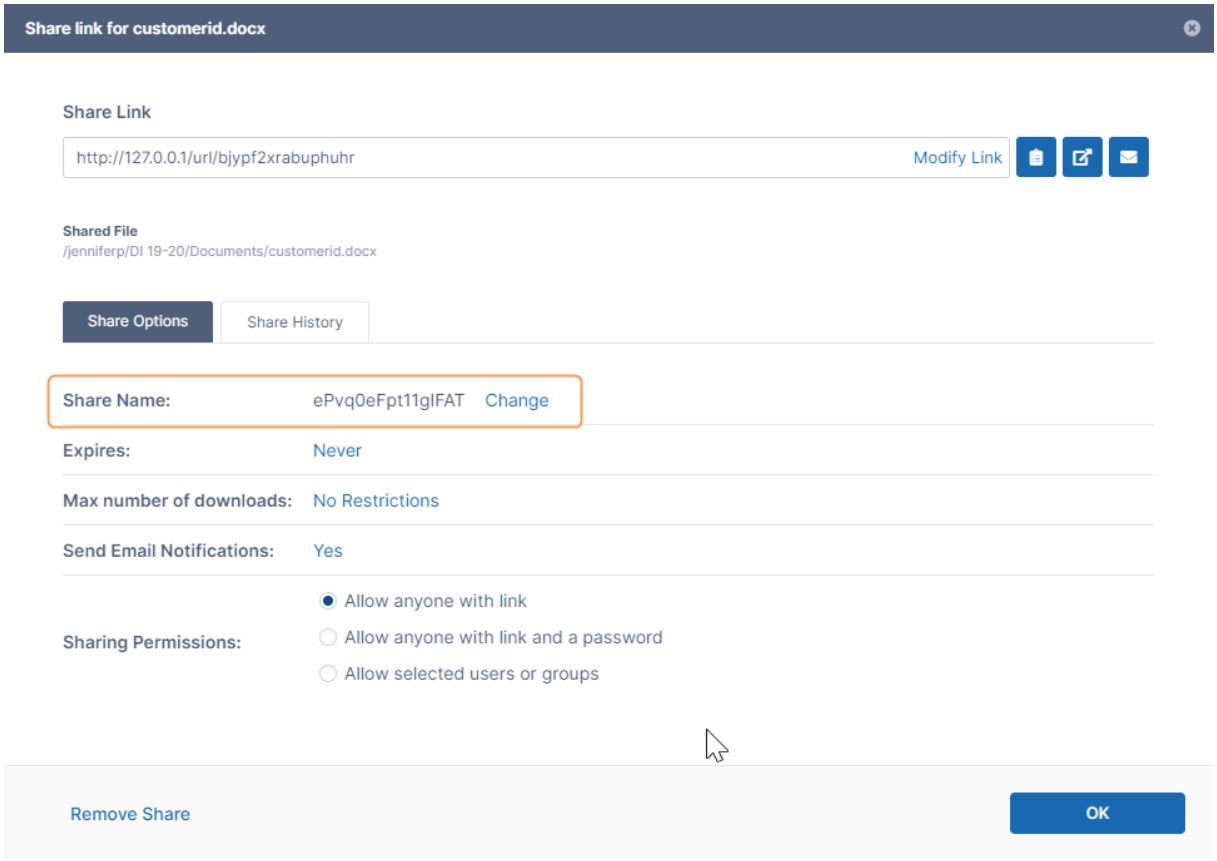
2. Enable **Public shares must be password protected**.
3. Leave **Public share default password length** at **14**, or change it to another number.
4. Leave **Require complex public share passwords** enabled.

Disallow Share Name Change

For security reasons, shares have a randomly generated name that is created by default.

- Randomly generated names are more difficult for attackers to guess.
- Randomly generated names do not expose user names or a description of the data.

This is how the randomly generated name looks in the user portal when creating a share:



By default, users may change randomly generated share names to custom names. However, you may prevent users from changing share names.

To prevent users from changing randomly generated share names:

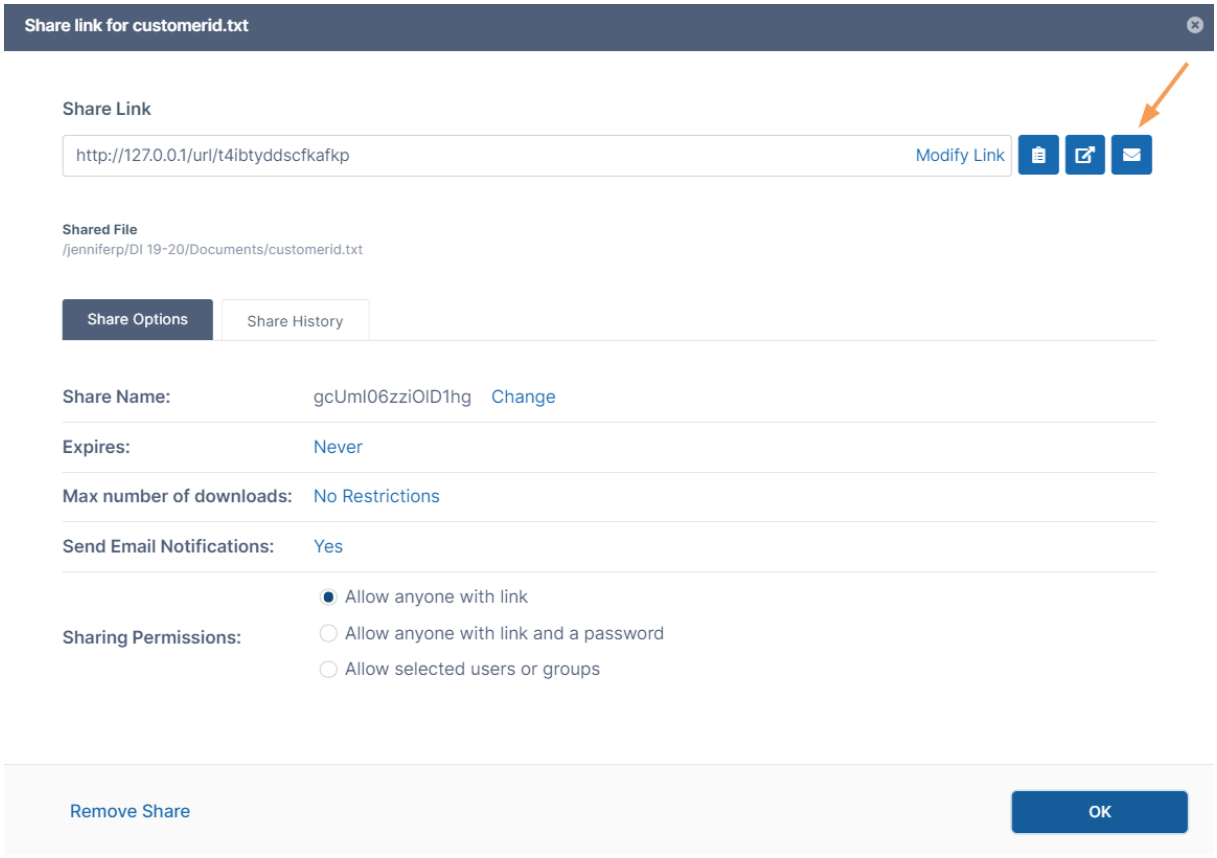
1. In the **Share** settings page, scroll down to the setting **Disallow share name change**, and enable it.



2. Click **Save**.

Hide Send Share Link Via Email

Users can send a share link by email by clicking the mail icon shown in the following image. To secure share links, you can hide the mail icon to make it unavailable to users.



To hide the option for sending a link to the share in email:

1. In the **Share** settings page, scroll down to the setting **Hide option to send share link by email**, and enable it.



2. Click **Save**.

To limit user account searches:

Limit User Account Searches

You can limit how users search for other user accounts.

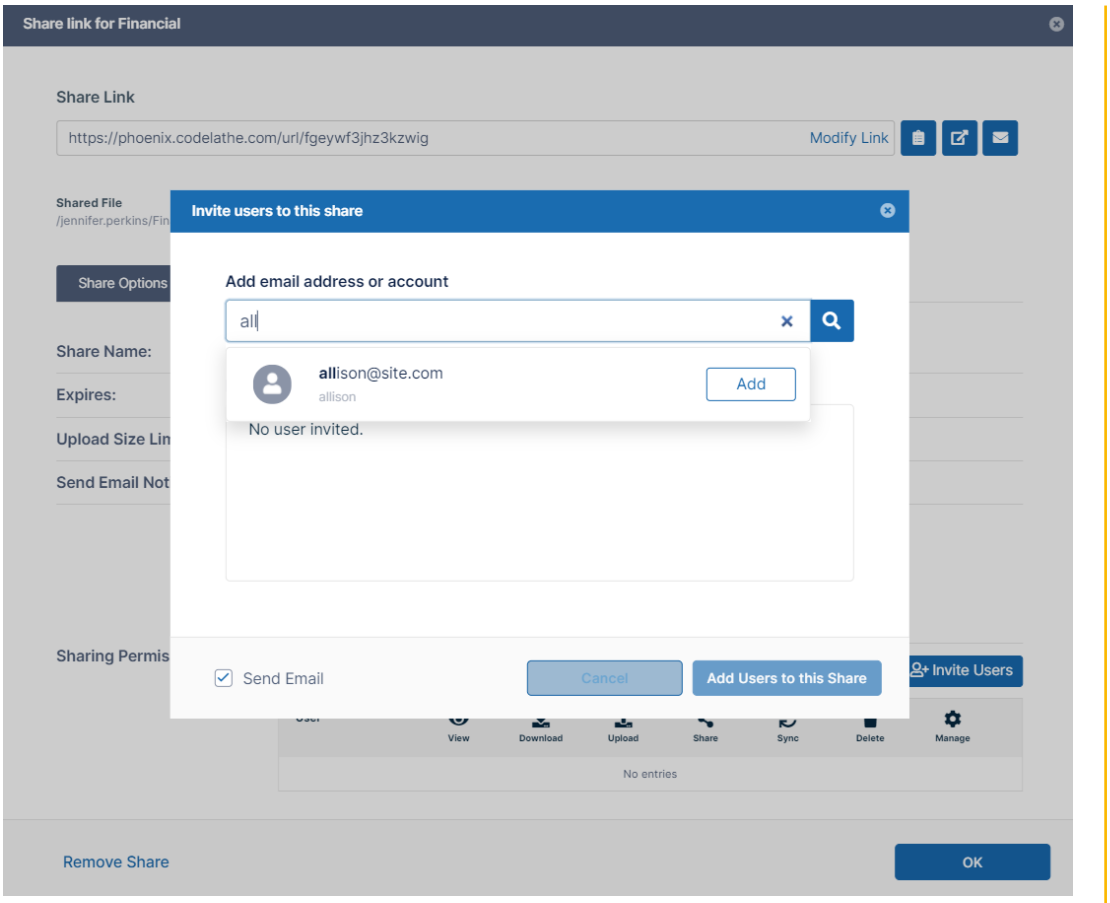
By default, when user1 shares a file or folder with user2, user1 can search for user2's account by the user name or email id. The search results list both exact and partial matches.

However, this is not desirable in certain cases and organizations, as the search results reveal user accounts that exist in the FileCloud system.

Therefore, FileCloud allows you to restrict user searches using two search modes:

User Account	User Account Type
• Exact Email Search With Explicit Account Invite • Exact Email Search With Implicit Account Invite • Exact Name/Email Search • Partial Name/Email Search	• ALL • FULL • GUEST • EXTERNAL
How to enable User Account Search Mode	How to enable User Search Account Type
NOTE: You can use these search limitations together. For example, you can set the **User Account Search Mode** to **Partial Name/Email Search**, and then use the **User Account Type** search mode to limit the results to only accounts with FULL access.	

Note
Using a search mode limits account searches for all the users in the FileCloud system.
These settings affect searches in shares for share recipients.



To make it clearer which user has shared a file:

Use Display Name as well as User Account Name

To make it clearer which user has shared a file, you can change how a user name is displayed in sharing details.

How user names are defined in FileCloud

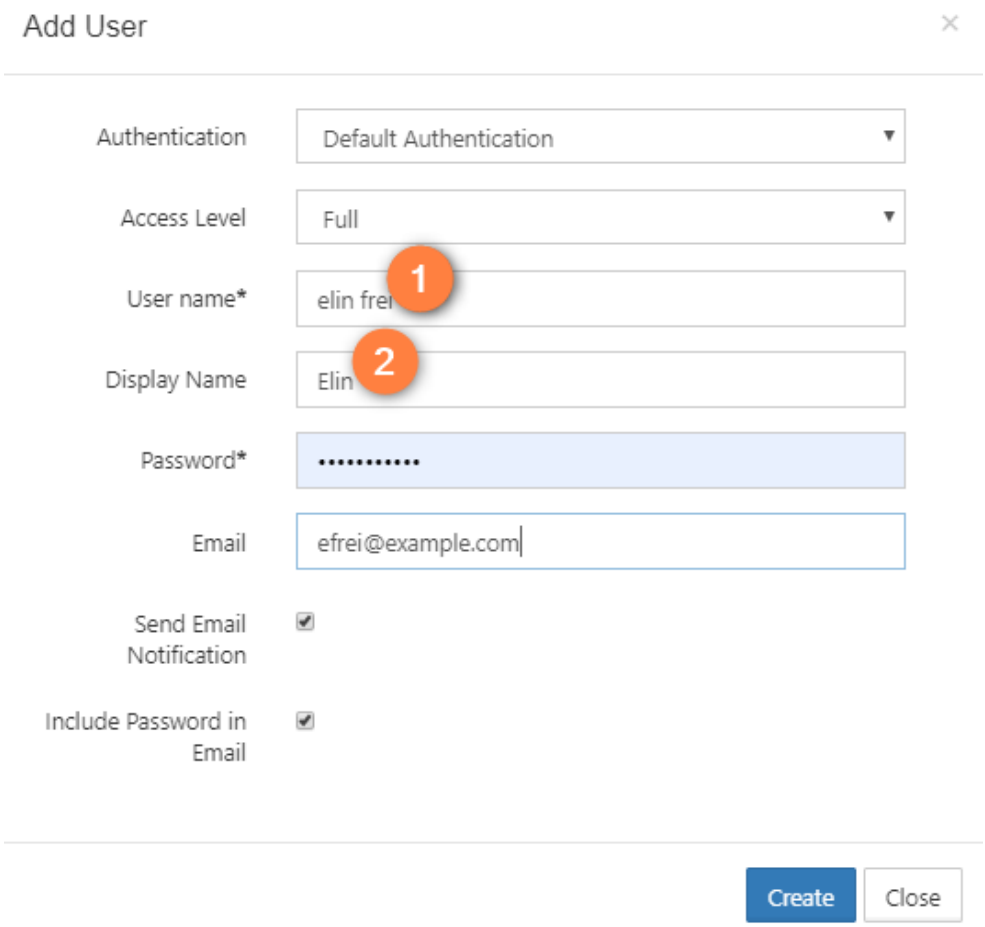
In the admin portal, when you create a user, you set 2 different names.

1. **User name**

- In the user portal, by default, FileCloud displays the **User name**.
- It may not be clear to users who is sharing the file with them, especially if **User name** includes only abbreviations and numbers.
- The **User name** cannot be changed after the user has been created.

2. **Display name**

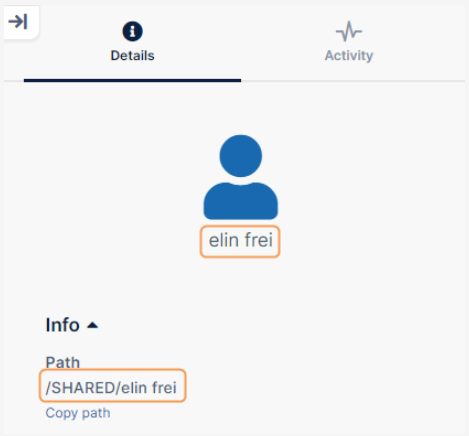
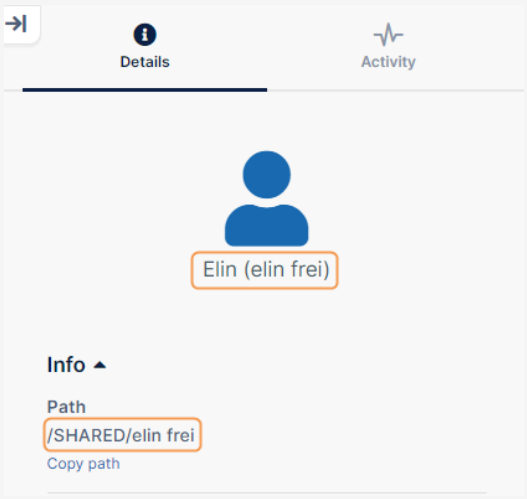
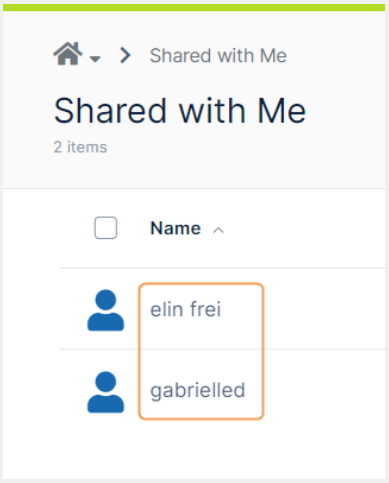
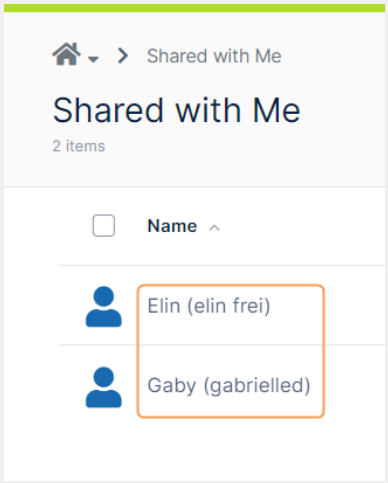
- You can have FileCloud use the **Display name** as well as the **User name** on the **Details** tab when showing the share information.
- Using the **Display name** makes it clearer to users who is sharing the file with them.
- The **Display name** can be changed after the user has been created.



Where Your Changes Appear

In the user portal, the user's name is displayed differently after you change the default display to include the **Display name**.

	BEFORE (User Name)	AFTER (Display Name and User Name)

Details Pane		
Shared With Me list		

How to Change the Display of a User's Name in Sharing Details

Changing the display in sharing details requires you to edit the cloudconfig file and restart the server.

To change the default from User Name to Display Name in sharing details:

1. On the FileCloud Server, open the following file for editing:
   For Windows

   ```
   XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   ```

   For Linux

   ```
   /var/www/config/cloudconfig.php
   ```

2. Add the following code to use the **Display Name**:

```
define("TONIDOCLOUD_USE_DISPLAYNAME_FOR_SHARED", 1);
```

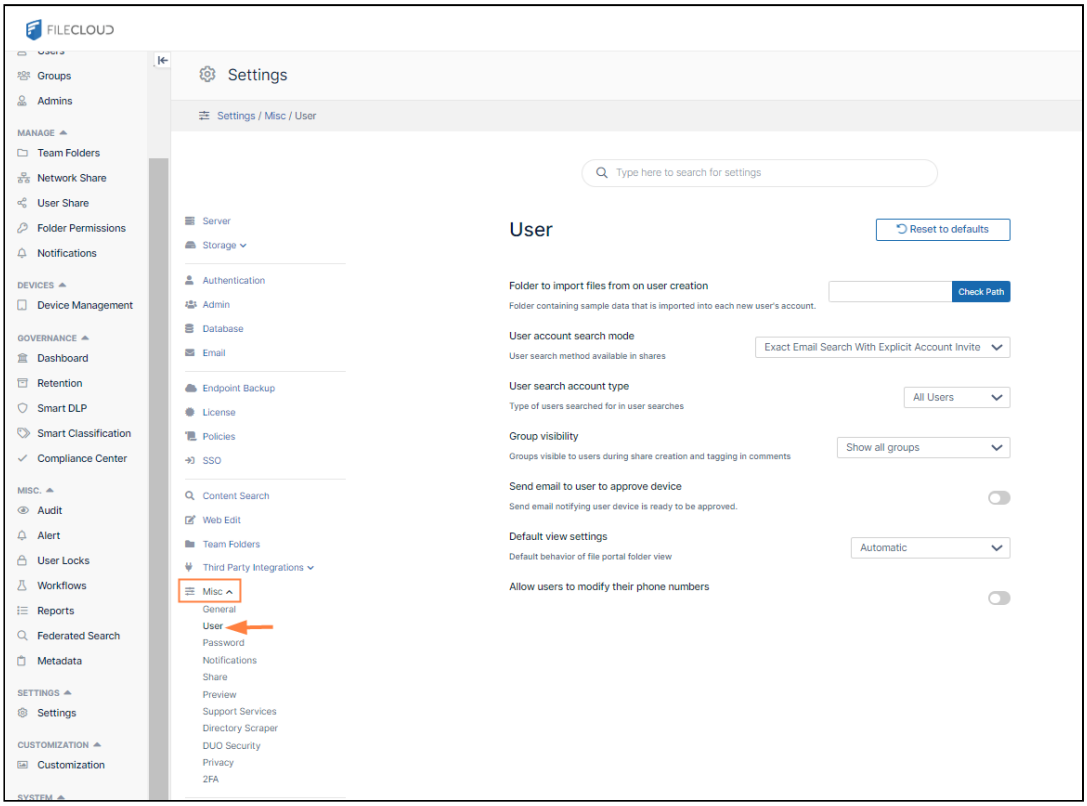
3. Save and close the file.
4. Restart the Apache server.

User Account Search Mode

For security reasons, you can restrict user searches so that your users have to know the exact email address of the person they want to add to a share or a workflow. Alternatively, you can set this option to allow users to search for another user with just a known partial email address.

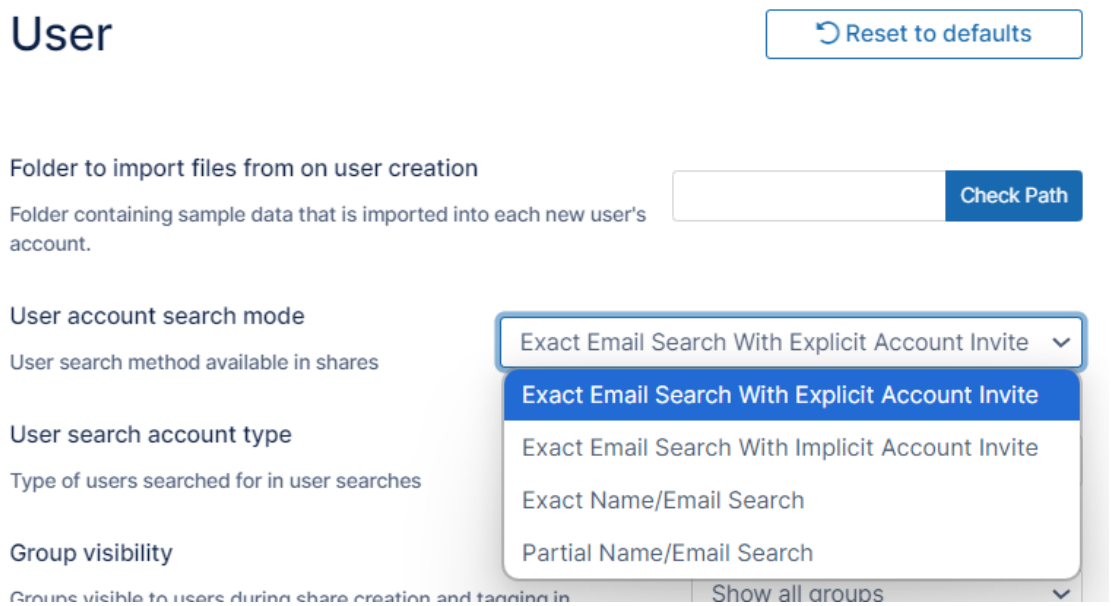
To access the User Account Search Mode Settings:

1. Open the **User** settings page.
   To open the User settings page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **User**, as shown below.



The **User** settings page opens.

2. Click the **User account search mode** drop-down list:



3. Choose a search mode, and click **Save**.

Search Mode	Example	When this search mode is set by admin, the following behavior will be seen during sharing by users:
Exact Email Search With Explicit Account Invite	JoeCarpenter@MyFileCloud.com	• Only email search is allowed • If the email doesn't exist in the system, an explicit invite option will be shown • With this option, a user may still figure out other users that exist in the system
Exact Email Search With Implicit Account Invite	JoeCarpenter@MyFileCloud.com	• Only email search is allowed • If the email doesn't exist in the system, then the system will send an invite to the entered email address without notifying the user • With this option, a user cannot figure out other users that exist in the system
Exact Name / Email Search	Joe Carpenter	• Both name and email search is allowed • No partial matches are allowed. • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the email doesn't exist in the system, the system will give the user option to invite the specified user

Search Mode	Example	When this search mode is set by admin, the following behavior will be seen during sharing by users:
Partial Name / Email Search	Joe C	• Both name and email search is allowed • Partial matches are allowed • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the searched email doesn't exist in the system, the system will give the user option to invite the specified user

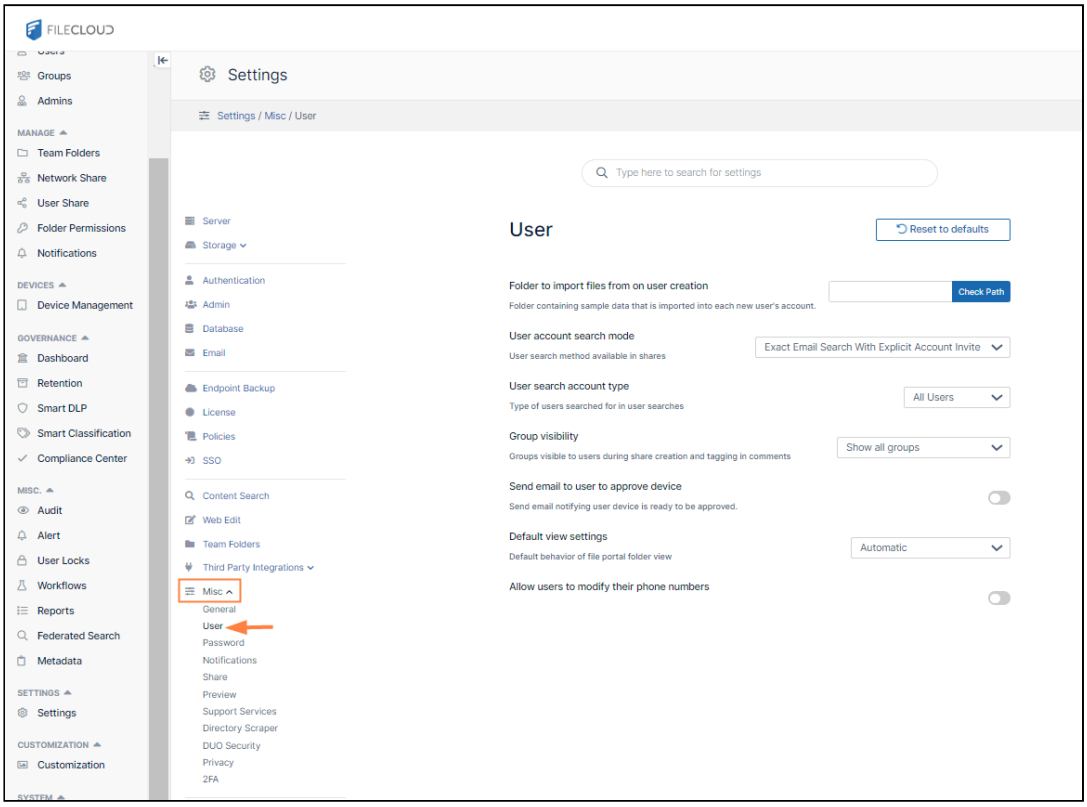
User Search Account Type

For security reasons, you can restrict user searches so that your users can only search for user accounts that are assigned a specific level of access.

To access the User search account type setting:

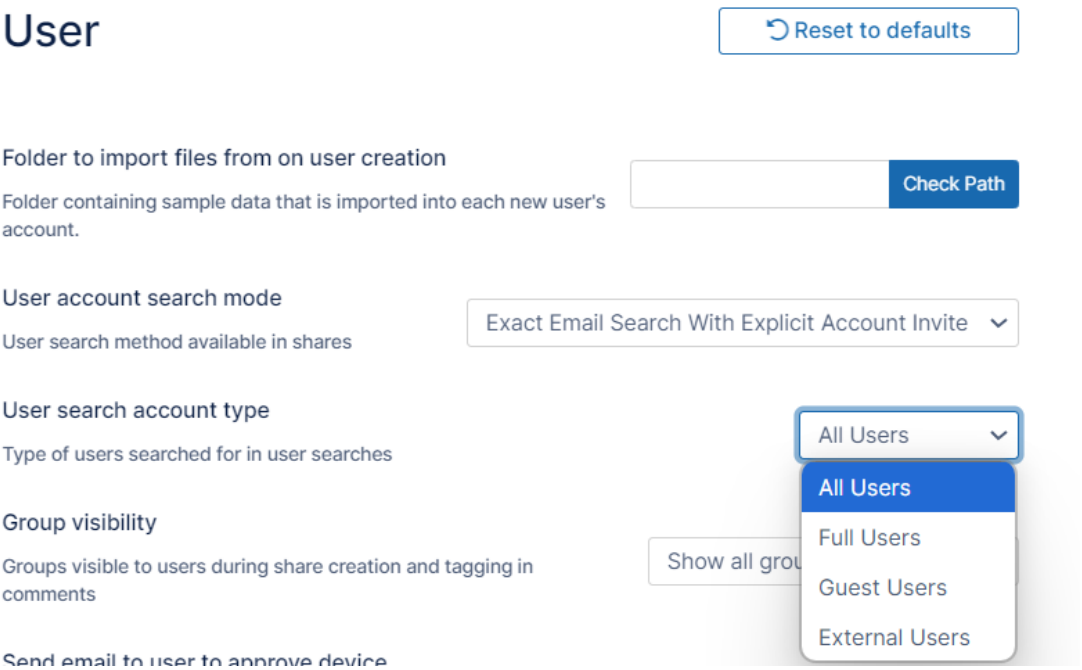
1. Open the **User** settings page.
   To open the User settings page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **User**, as shown below.



The **User** settings page opens.

2. Click the **User search account type** drop-down list:



3. Choose the account type to search on, and click **Save**.

User account type	Level of access
ALL	No restriction of account searches
FULL	An account with full access has its own private cloud storage space in the "My Files" area. These users can: • store files in their own private cloud storage space • view/download files stored in their storage space • view/download files shared with them by other user accounts
GUEST	An account with guest access level has restricted access to the FileCloud system. These user accounts do not have private cloud storage. These users can: • view/upload/download files shared to them by other user accounts • re-share content if they have permission
EXTERNAL	An account that can only be used to access the User Portal through a Web browser. External Accounts can: • view/upload/download content shared with them External Access accounts can only be local user accounts.

Document Settings

In this section:

Setting up Content Search for Documents

Administrators can enable content search to provide users with the following features:

- Searching through the file contents of the supported file types
- Support for file types such as txt, pdf, doc, docx, xls, xlsx, ppt, pptx
- Regex support for file/folder name searches

Note: Content of files larger than 10 MB is not indexed.

In this section:

Install Content Search for Windows

Advanced content searching capabilities for documents in FileCloud uses Solr and requires the correct Java Development Kit (JDK).

Solr is an open source enterprise search platform, written in Java.

FileCloud now fully supports OpenJDK 17 or higher instead of Oracle Java.

- Java Development Kit (JDK) consists of the Java Runtime Environment (JRE) along with tools to compile and debug Java code for developing Java applications.
- OpenJDK is an open source implementation of the Java Standard Edition platform with contributions from Oracle and the open Java community.
- OpenJDK is the official reference implementation for Java Standard Edition from Java SE 7.
- OpenJDK is released under license GPL v2 wherein Oracle JDK is licensed under Oracle Binary Code License Agreement.
- Oracle JDK's build process builds from OpenJDK source code.

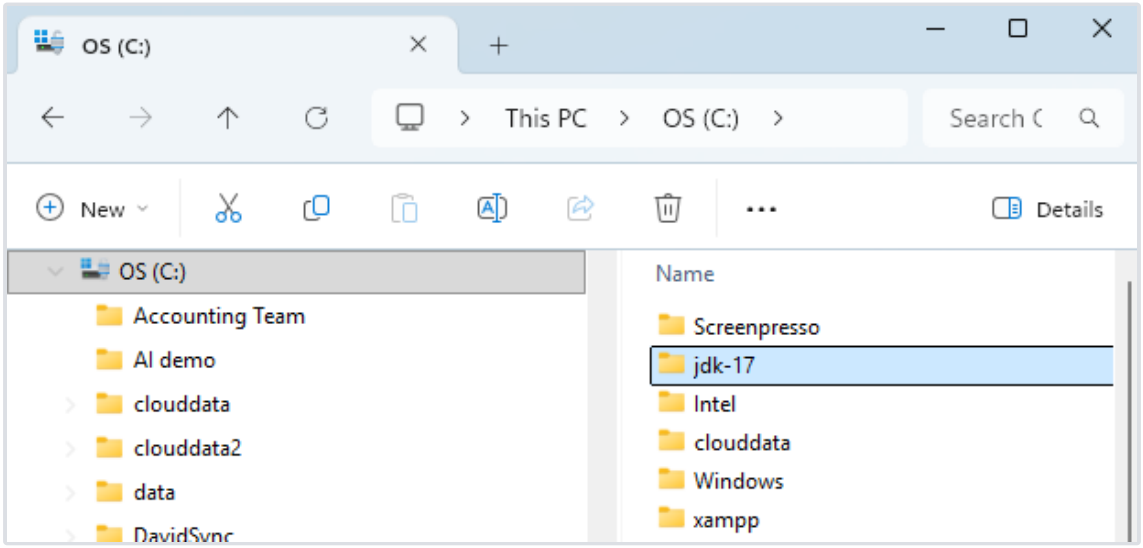
💡If you already have OpenJDK 17 or higher installed, you can skip the following steps.

To install OpenJDK for Windows:

1. Install OpenJDK.

To install OpenJDK:

1. Download **Open JDK 17** from https://jdk.java.net/archive/ .
2. Create a new folder in the C: drive.
   (In the example screenshot, jdk-17 is the name of the new folder.)



3. Extract the Open JDK file you downloaded into the new folder.

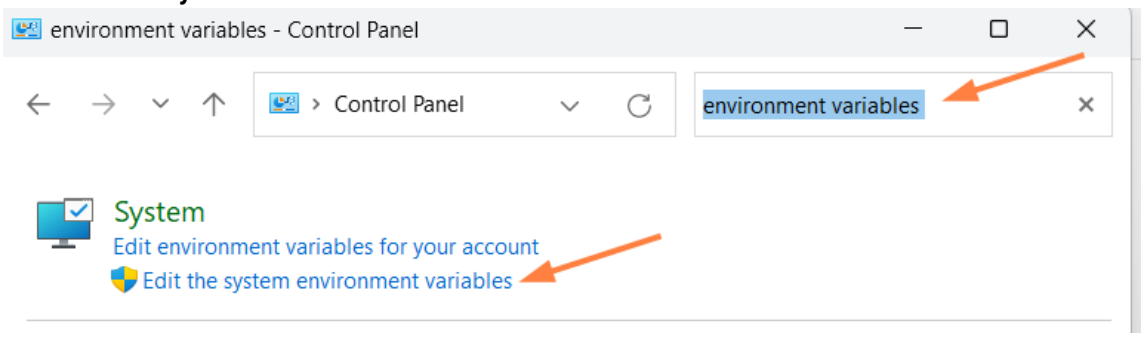
2. Set the JAVA_HOME path and add the bin path

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

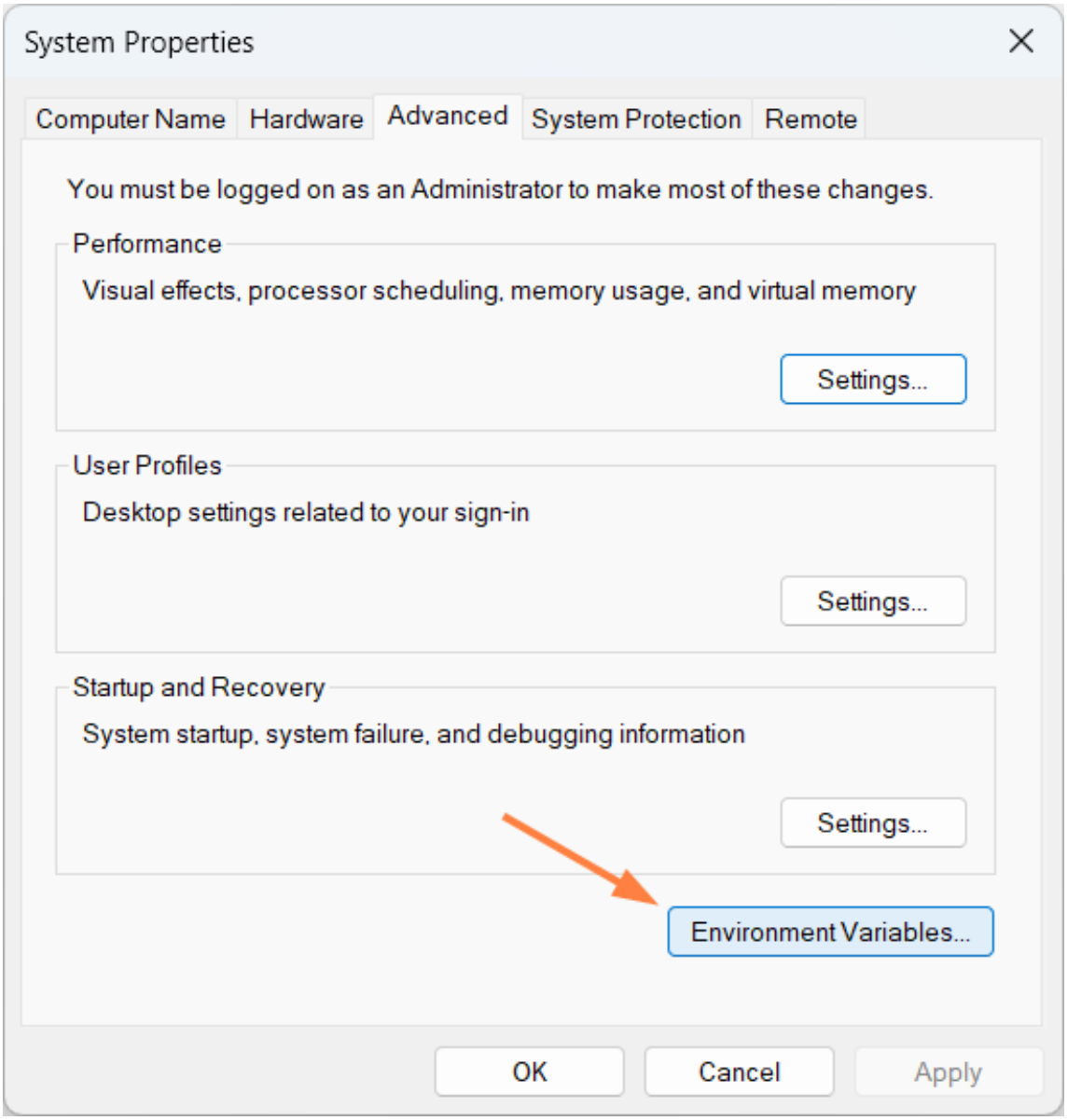
⚠ Administrator privileges are required to modify the path and environment variables.

To set the JAVA_Home path and add the bin path:

1. Open the Windows Control Panel.
2. Enter **environment variables** in the search bar.
3. Click **Edit the system environment variables.**

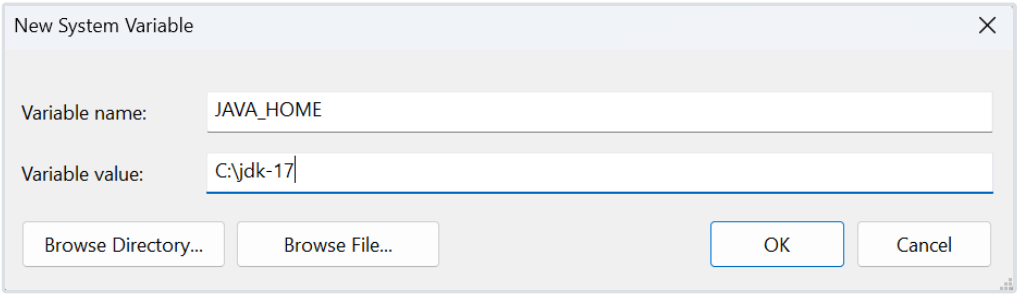


4. In the **System Properties** dialog box, click **Environment Variables.**



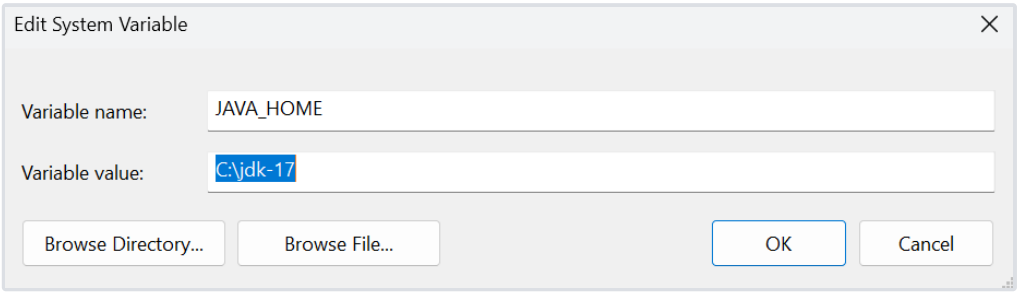
The **Environment Variables** dialog box opens.

5. Edit or create the **JAVA_HOME** variable and set it to your jdk folder address.
   - If you do not see the **JAVA_HOME** variable listed under **System variables**:
     i. Below the **System variables** window, click **New**.
     ii. In the **New System Variable** dialog box:
     iii. In **Variable name** enter **JAVA_HOME**.
     iv. In **Variable value**, enter the address of the folder you created for jdk.

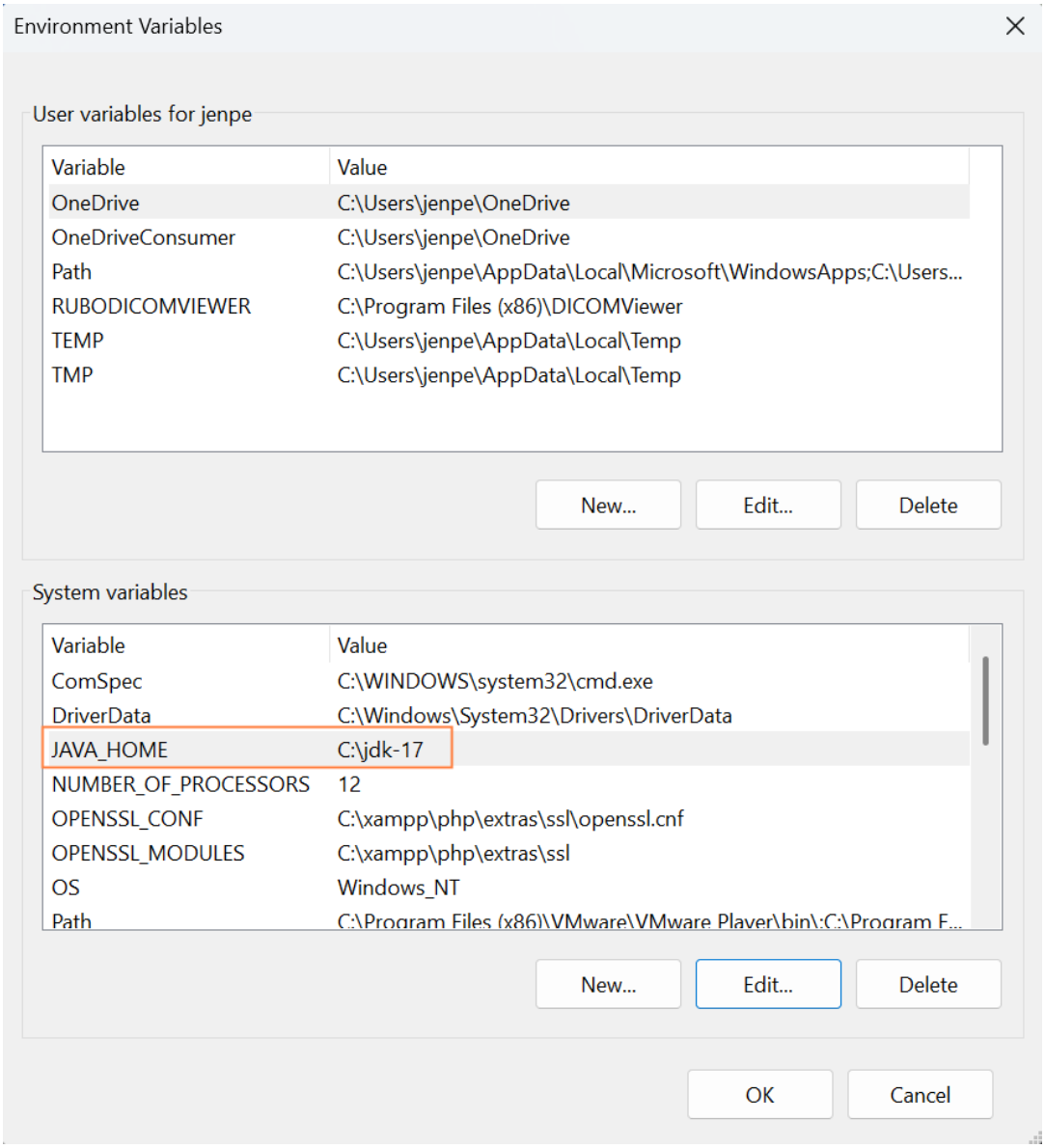


v. Click **OK**.

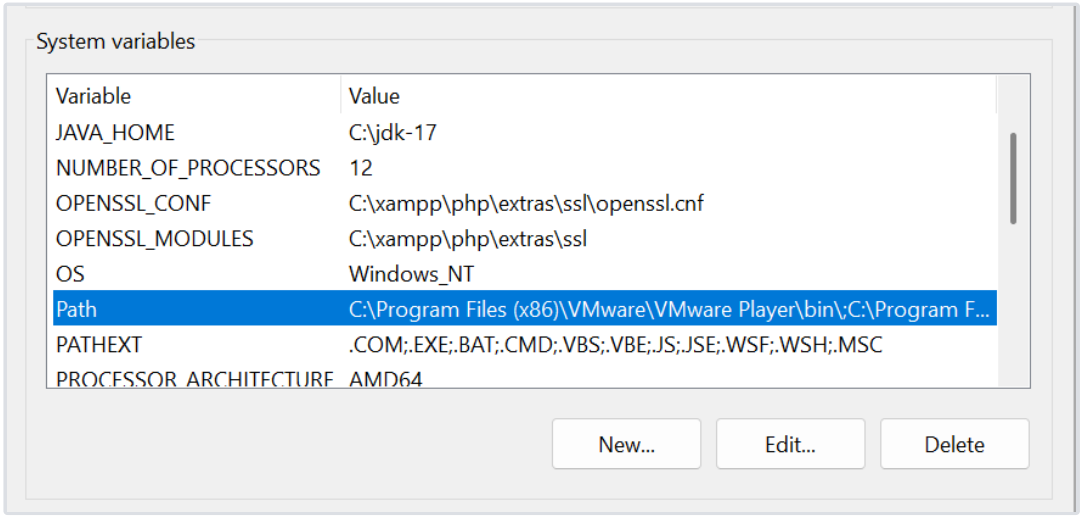
- If you see the **JAVA_HOME** variable listed under **System variables**:
  i. In the **System variables** box, click **JAVA_HOME**, and then click **Edit**.
  The **Edit System Variable** dialog box opens.
  ii. Change **Variable value** to the address of the folder you created for jdk, and click **OK**.



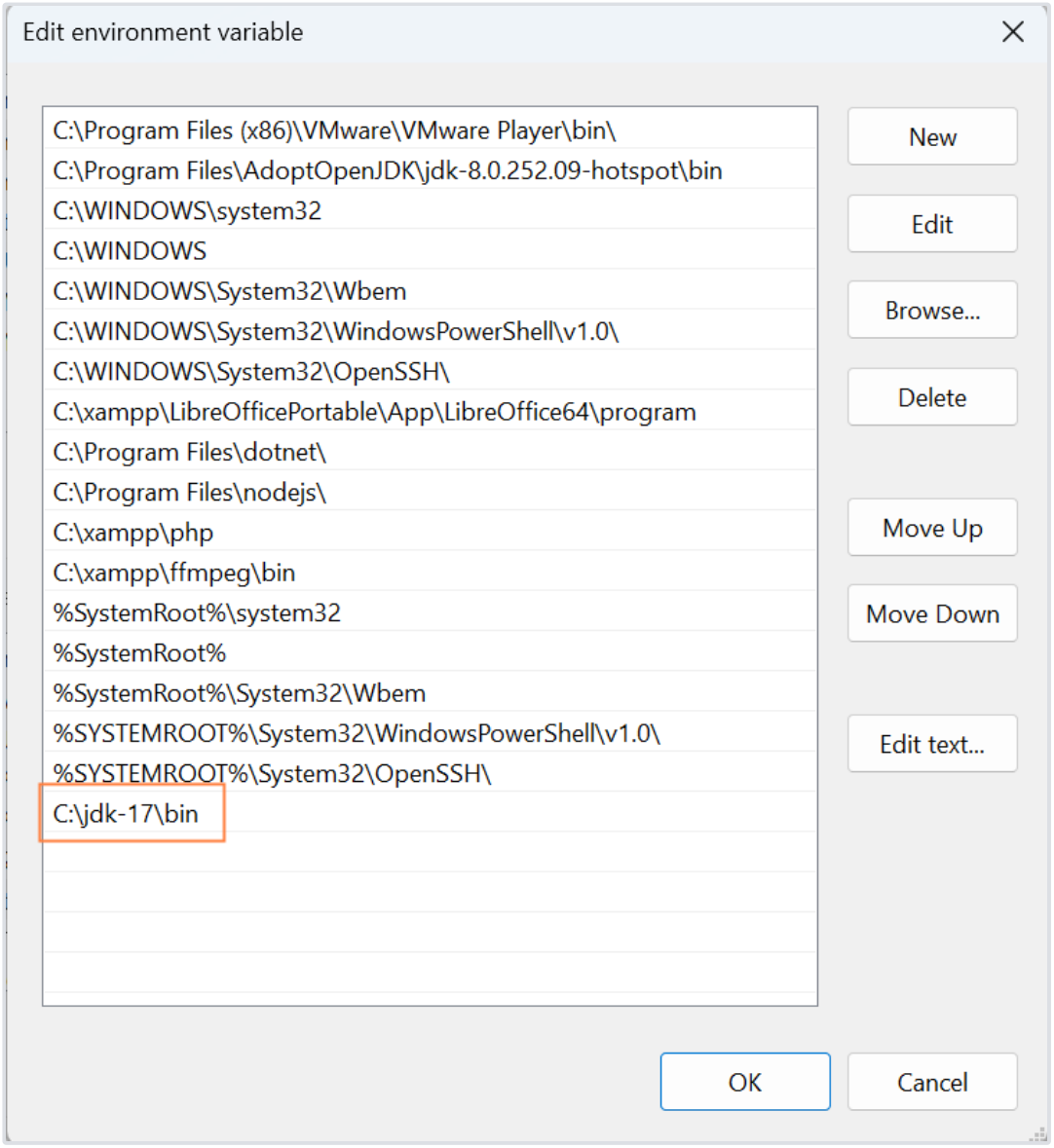
- If the value appears correctly in the **Environment Variables** dialog box, click **OK**.



6. Now add the bin path to the **Path** variable.
    - Click and edit the **Path** variable which also appears in System variables:



- In the Edit environment variable dialog box, add the OpenJDK bin path. It is the JAVA_HOME path with **\bin** appended to the end, for example:
  C:\jdk-17\bin

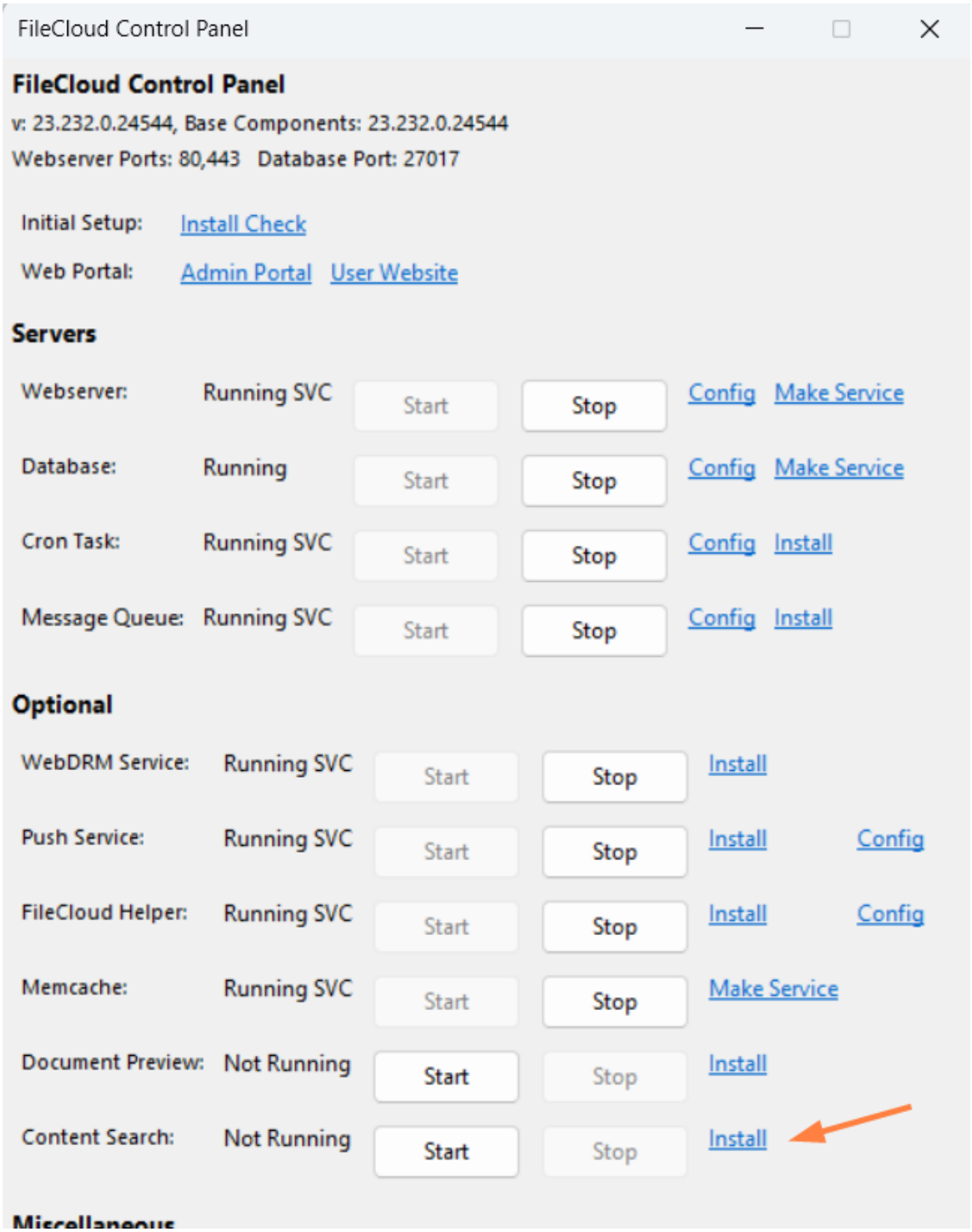


- Click **OK** in each dialog box until you exit the Windows Control Panel.

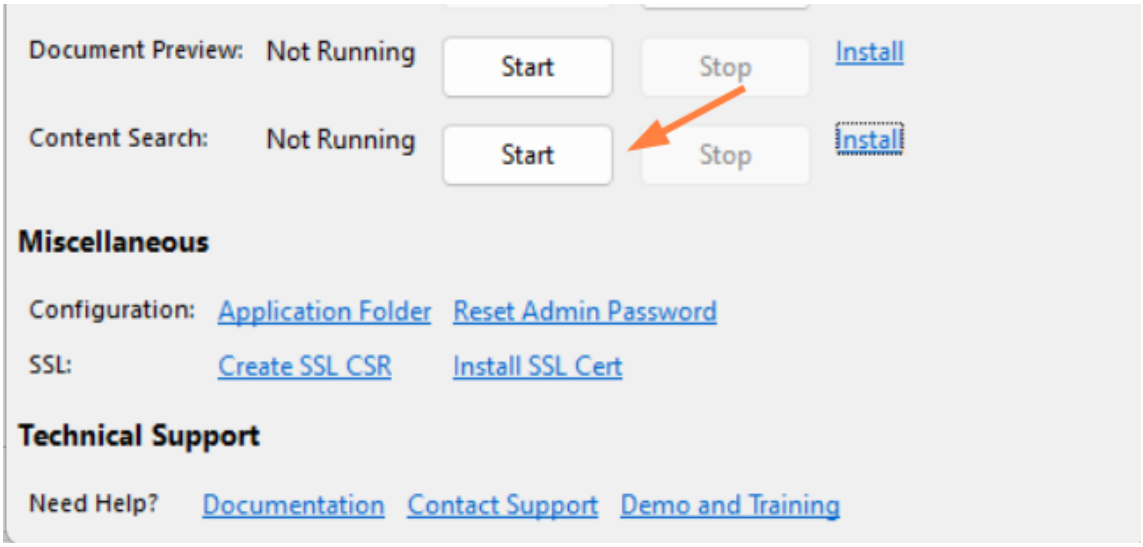
3. Use the FileCloud Control Panel to install Content Search

To install and start Content Search:

1. Open the FileCloud Control Panel.
2. Next to **Content Search**, click **Install**.



3. To start the **Content Search** service, click the **Start** button.



Install Content Search for Linux

FileCloud advanced search uses Solr (an open source component) for its content search capabilities and Tesseract OCR for optical character recognition (OCR) in content searches. Install Solr and Tesseract on Linux using the following procedures:

Solr installation and upgrade

- If you have installed FileCloud on a single server, install or upgrade Solr on the same server using the command:

```
filecloudcp --install-solr
```

- If you have installed FileCloud on multiple servers for high availability, install or upgrade Solr's stand-alone application using the commands:

```
curl --location 'https://repo.filecloudlabs.com/static/fcp/filecloudcp' -o /usr/
bin/filecloudcp
chmod 755 /usr/bin/filecloudcp
filecloudcp --install-solr
```

- For recent versions of Solr, the following messages should be returned:

```
root@node2:~# filecloudcp --install-solr
Solr exists
Already running in the Latest SOLR VERSION which is 9.5.0",
```

Tesseract installation and upgrade

Install Tesseract on the same server as FileCloud.

- To install Tesseract, enter the command:

```
filecloudcp --install-tesseract
```

- To upgrade Tesseract, use the install command, above.

If you experience problems with any of the above installations or upgrades, please Contact FileCloud Support.

Configure Content Search for Managed Storage

Administrators must configure FileCloud to use Solr before it can be used for advanced search.

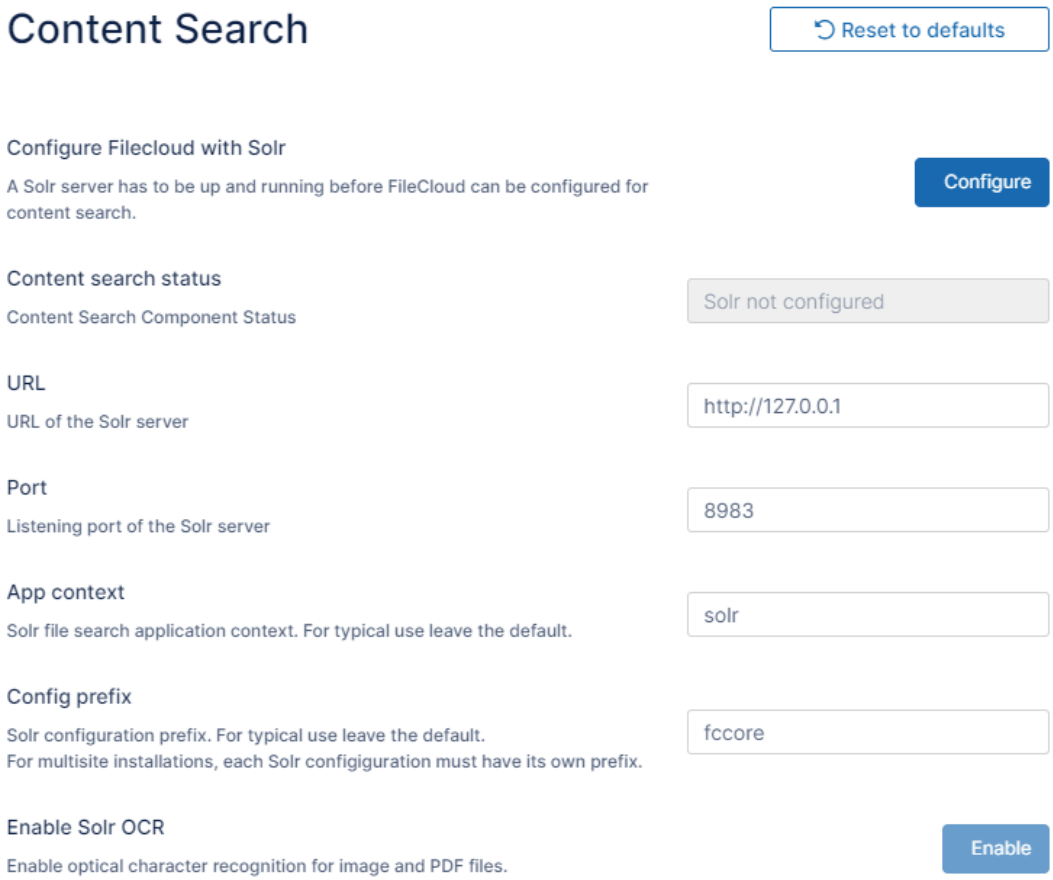
- Configure FileCloud with the URL of the Solr server and the port number.
- Create an index to allow Solr to search the files in managed storage.

1. Configure Solr in the Content Search tab.

Configure a Single Site

Follow these steps to configure FileCloud with Solr after it is installed.

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

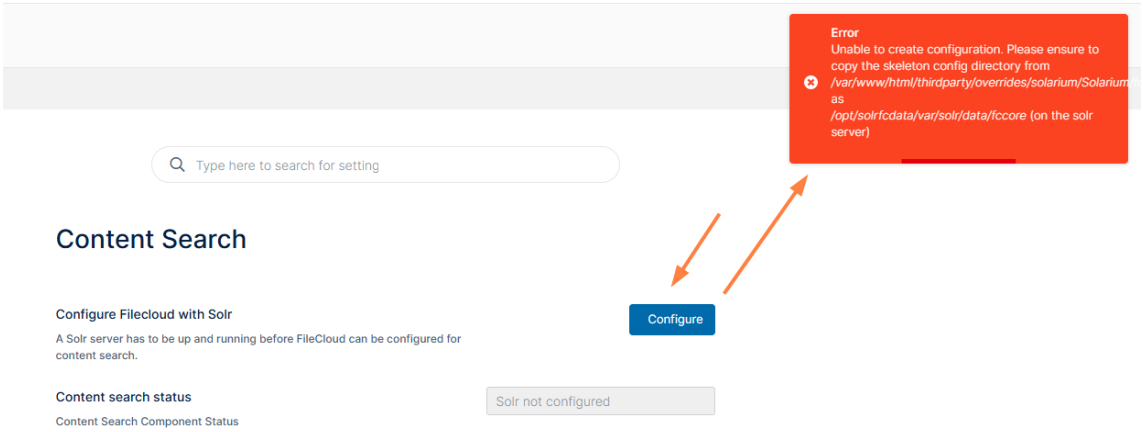


2. Update the settings depending on your environment.

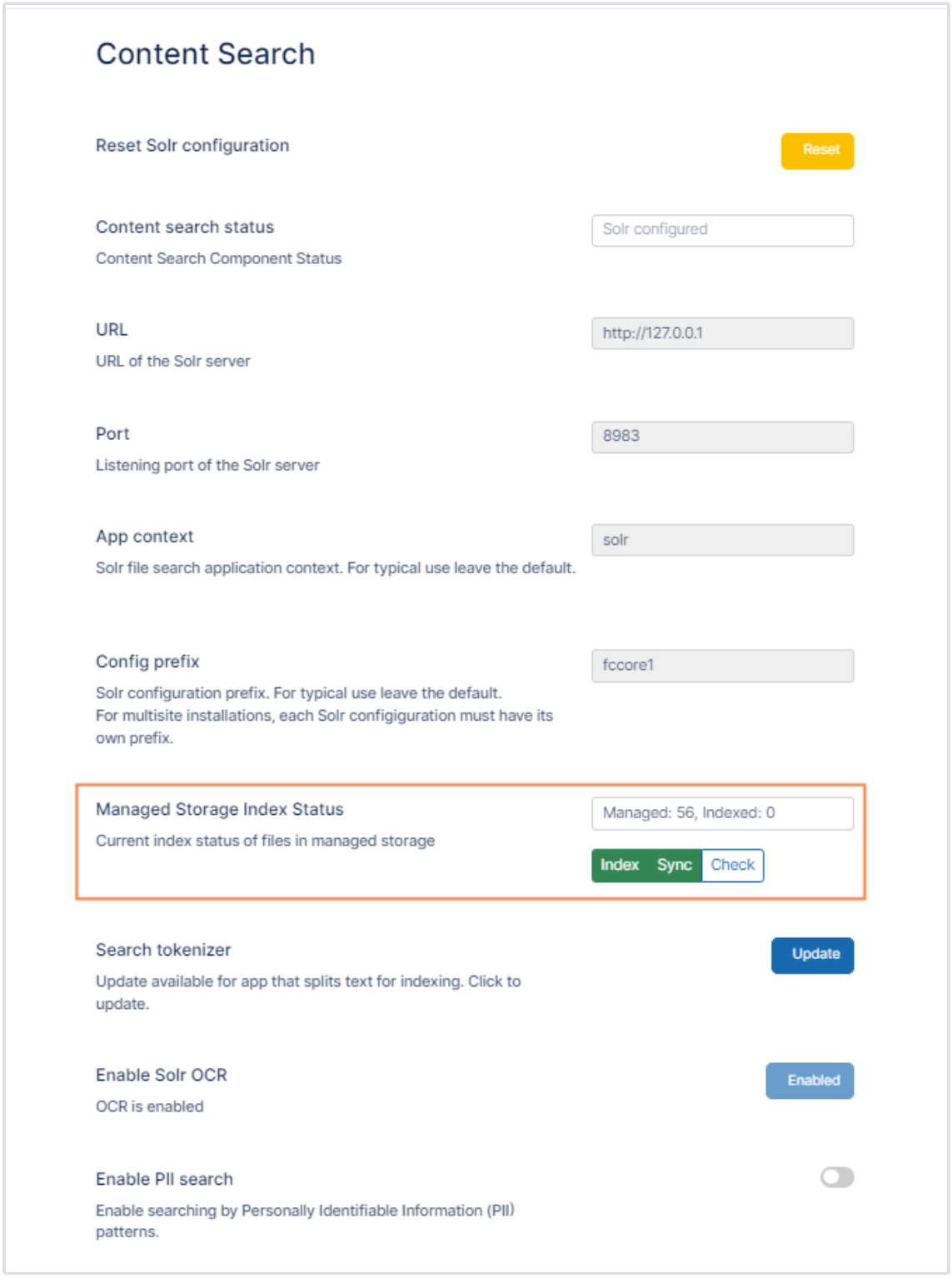
Parameter	Remarks
Content search status	This is a read-only field that displays the status of FileCloud Solr configuration.
URL	The http url of the Solr server. Default value is http://127.0.0.1. If Solr is installed on a different server, use its IP address. **Note**: Do not use the port number as part of the URL. It is entered in the next field.
Port	Port number of the Solr server. Default value is 8983. If Solr is running on a different port, update this value.
App context	This is the application context under which the Solr server is hosted. Default value is solr.

Parameter	Remarks
Config prefix	Unique prefix for the current sites configuration. Default value is fccore. **Note:** In multisite FileCloud installations, each site should have a unique prefix if they use the same Solr server.
Enable Solr OCR	Enables optical character recognition so search can find matches in images.

3. Click **Configure** to configure FileCloud with Solr, using the entered information.
   If this fails, a message may appear that prompts you to copy a configuration directory from a source directory to a target directory.
   If the message appears, follow the instructions to copy the template folder. In the following example, the folder **<FileCloud web root>/thirdparty/overrides/solarium/Solarium/fcskel** should be copied to **<FileCloud web root>/server/solr** and renamed **fccore**.
   Directories and target folder name for your environment might be different.

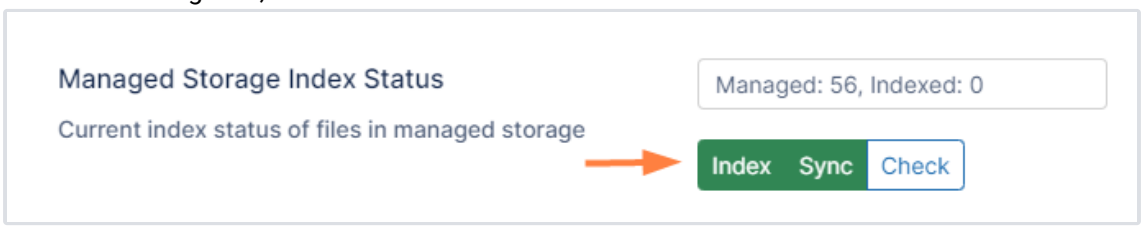


4. If you are prompted to copy the configuration directory, after you copy it, click the **Configure** button again.
   Upon successful configuration, a new field appears and shows the index status of all Managed Storage files.

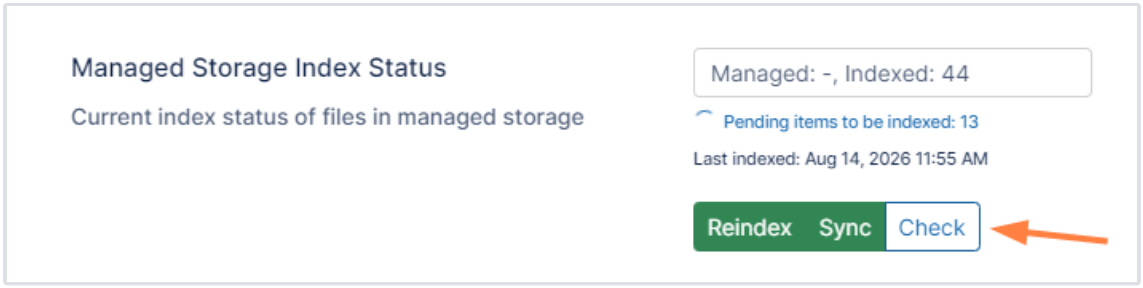


If it is a fresh installation, each new file is indexed when it is uploaded.
If it is an existing installation, managed files already exist. Though the new files will be indexed, the existing files have to be indexed separately.

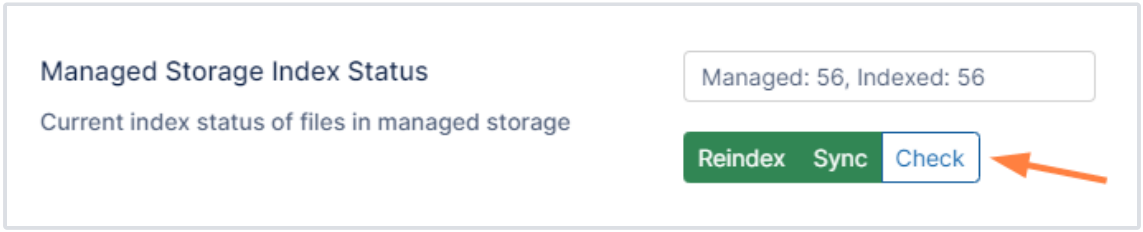
5. To index existing files, click the **Index** button.



6. When the button appears as **Reindex**, click the **Check** button to see the number of indexed files and the number pending indexing.

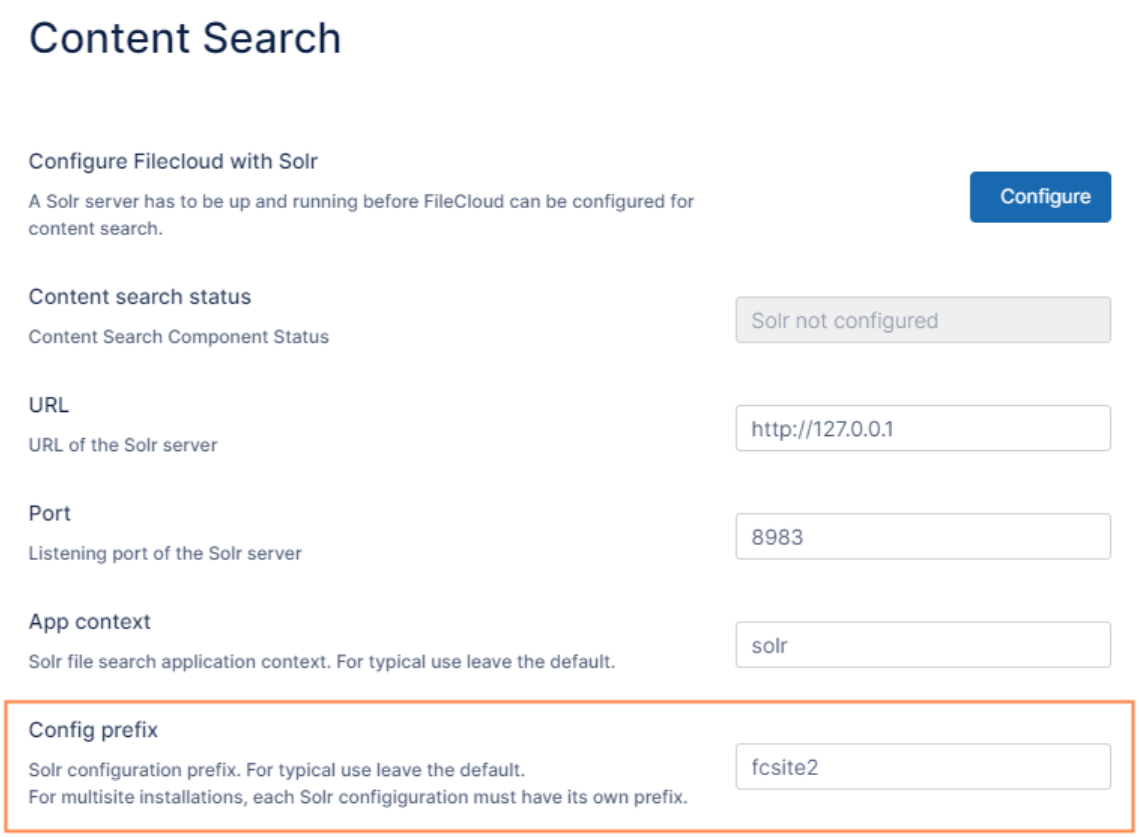


To refresh the numbers indexed or to see if indexing is complete, click the **Check** button again.
Note: The user interface will not automatically show that syncing has completed; you must click Check to see if all files have been synced.



Configure a Multi-Site

Multi-site Solr configuration is similar to single site configuration. After a new site is created, repeat the above steps, but in the **Config Prefix** field, specify a unique prefix for the new site.
This configures Solr with a separate index database for each new site.



2. Index Files in Managed Storage.

Indexing Network Folders
Unlike managed storage, Network Folder files exist outside of FileCloud and therefore changes occurring in the network folders might not be propagated into FileCloud.
Monitoring such changes are important in the following scenarios:

- Faster searching
- Content Search
- Automatic Realtime Syncing of Network Folders
- Pattern Searches for GDPR

For these scenarios, you must index network folders and keep them indexed as files and folders change.

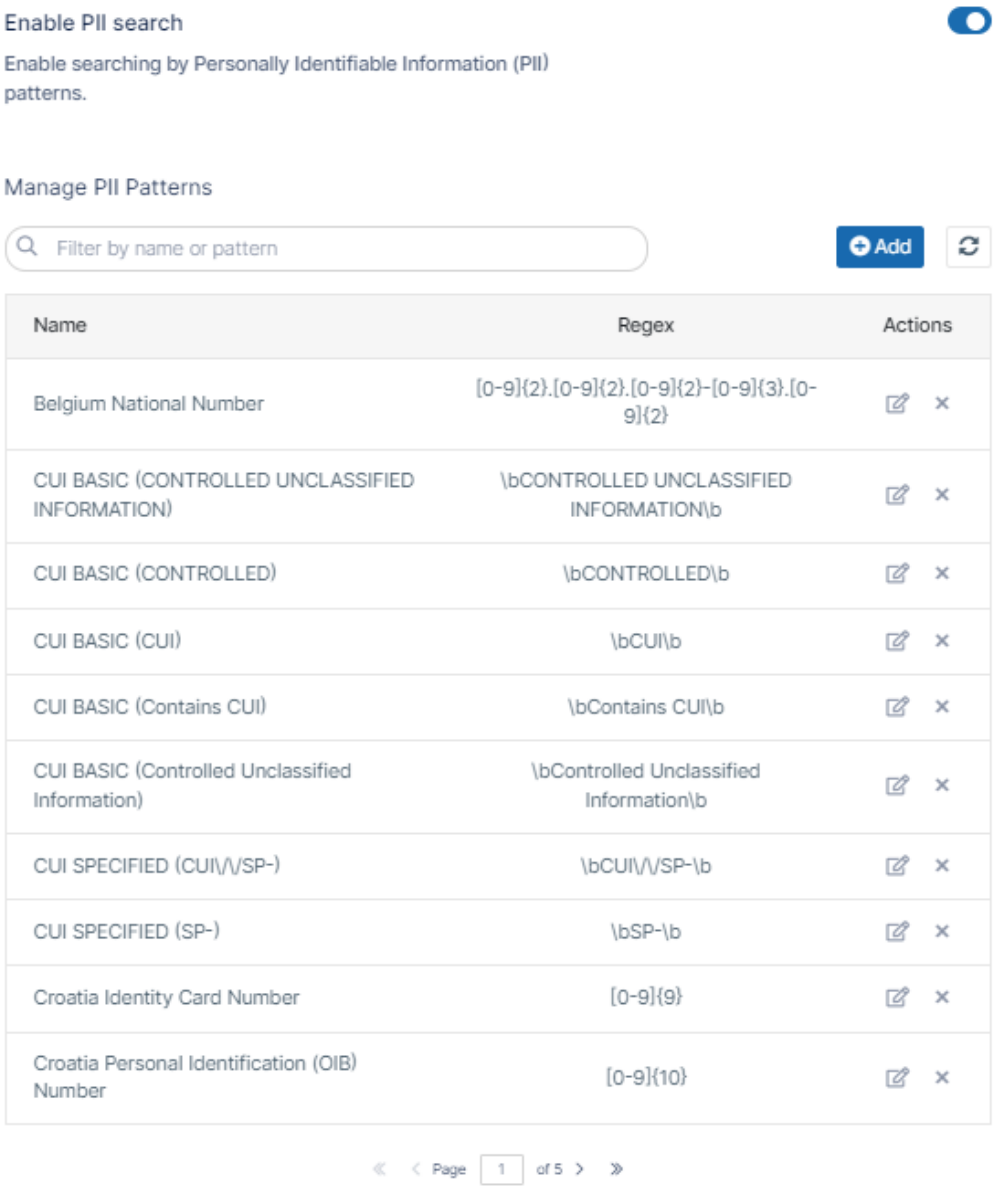
- To index network folders, the FileCloud Helper service is required

Indexing Network Folders

3. Enable and Configure PII Search

To enable and configure PII Search:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search** .
   The **Content Search** settings page opens.
2. Scroll down to the **Enable PII Search** field and enable it.
   The **Manage PII Patterns** section opens.



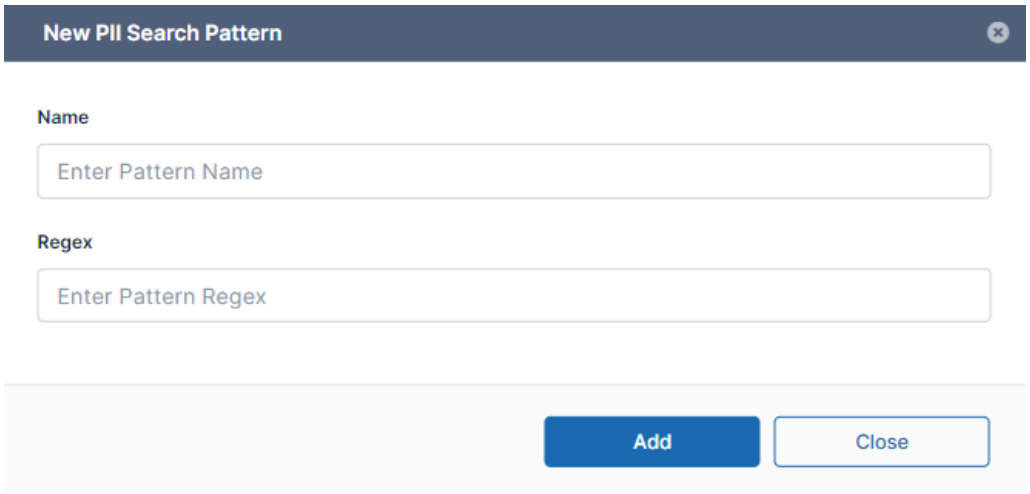
In the **Manage PII Patterns** section, you can add, edit, search for, and remove patterns.

- To add a new pattern to the list, in the **Manage PII Patterns** section, in the top right corner, click **Add**.

- To edit an existing pattern, in the **Manage PII Patterns** section, click the edit icon ( ) for the pattern.
- To remove an existing pattern, in the **Manage PII Patterns** section, click the delete icon (x) for the pattern.

Pattern format

A pattern contains the following information:



Regex is short for regular expression. This is a special alphanumeric string used to describe a search pattern.

If you need to create a new pattern or edit an existing one, use the following table to understand the Regex format used by FileCloud.

	Name	Input Type	Length of Input	RegEx Format
Description	Identifies the type of protected information	• enclosed in square brackets [ ] • a number range • uppercase letter range • lowercase letter range	• enclosed in curly brackets '{ '} • a number	[Type]{Length}
Numerical Example	U.S. Social Security Number	0-9 (can contain any number 0-9)	3 (for the first number) 2 (for the second number) 4 (for the third number)	[0-9]{3}-[0-9]{2}-[0-9]{4} 012-34-5678

	Name	Input Type	Length of Input	RegEx Format
Letter example	Poland Passport	a-zA-Z 0-9	2 letters (followed by) 7 numbers	[a-zA-Z]{2}[0-9]{7} ME0123456

4. Search with PII Patterns

The list of patterns you configure here is shown on the Admin portal search screen in the **Advanced options** dialog box as options to choose from.

To search the site's content for PII patterns, see **PII Search** on the page Search in the Admin Portal.

Indexing Managed Storage

Administrators must index the files in managed storage to allow Solr to search the files.

You have the following options when working with an index:

- **Index**. After you configure content search, use this option to index any files that are already in managed storage. After this initial indexing action, each new file is indexed when it is uploaded.
- **Reindex**. Use this option to remove the existing index data completely and do a fresh indexing of all managed storage files. This option is only available after the system has been indexed at least once.
- **Sync**. Use this whenever there is mismatch between the number of managed files and the number of indexed files. Sync only indexes the files that are not already indexed.
- **Check**. This displays the latest status of the managed store index and the counts of files indexed and pending indexing.

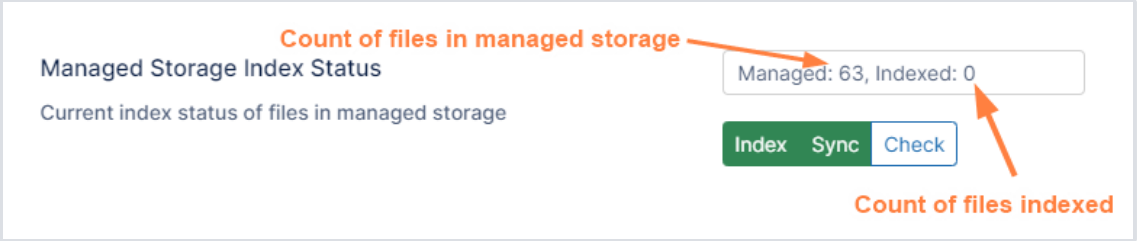
What do you want to do?

Initially index files

If you configure content search on a fresh install of FileCloud before you have stored content in managed storage, you do not have to click **Index**. This button only indexes unindexed files that exist in managed storage. Once indexing has is initiated, files are indexed automatically when they are uploaded to FileCloud.

To initially index files:

1. Configure Content Search as described in Configure Content Search for Managed Storage.
   If Managed Storage Index Status shows a number of files after **Managed**, but 0 files after **Indexed**, you are required to index the files existing in managed storage.



2. Scroll down and click the **Index** button.

Sync unindexed files

Sync can be done whenever there is mismatch between the number of managed files and the number of indexed files.

⚠ Sync will only index the files that are not already indexed.

To index files not yet indexed:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search** .
   The **Content Search** settings page opens.
2. Scroll down and click the **Sync** button.



Do a complete re-index

Use the **Reindex** button to remove the existing index data completely and do a fresh indexing of all managed storage files.

The **Reindex** button is available after the system has been indexed at least once.

To reindex managed storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search** .
   The **Content Search** settings page opens.
2. Scroll down and click the **Reindex** button.

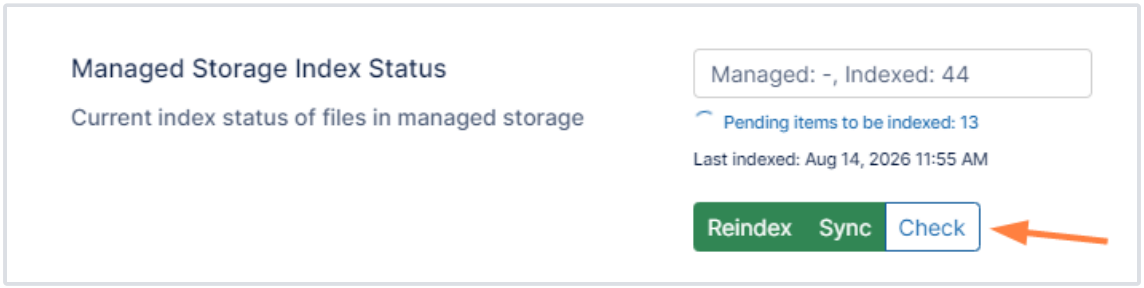


Check the status of the index

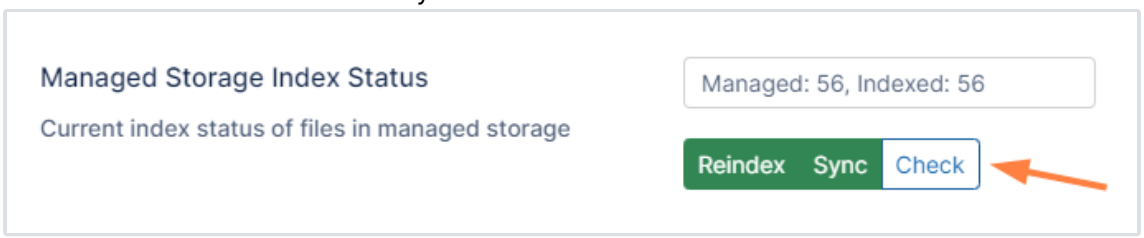
Use the **Check** button to see the status of indexing after you click **Index**, **Reindex**, or **Sync**.

To check the index status:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search**  .
   The **Content Search** settings page opens.
2. Click **Index**, **Reindex**, or **Sync**.
3. While indexing is in progress, click the **Check** button.
   The Managed Storage Index Status field shows the number of files indexed at this point, and the current index status below it shows the number of files remaining to be indexed.



4. Click the **Check** button again to refresh the count and to see if indexing has completed.
   Note: The user interface will not automatically show that syncing has completed; you must click **Check** to see if all files have been synced.



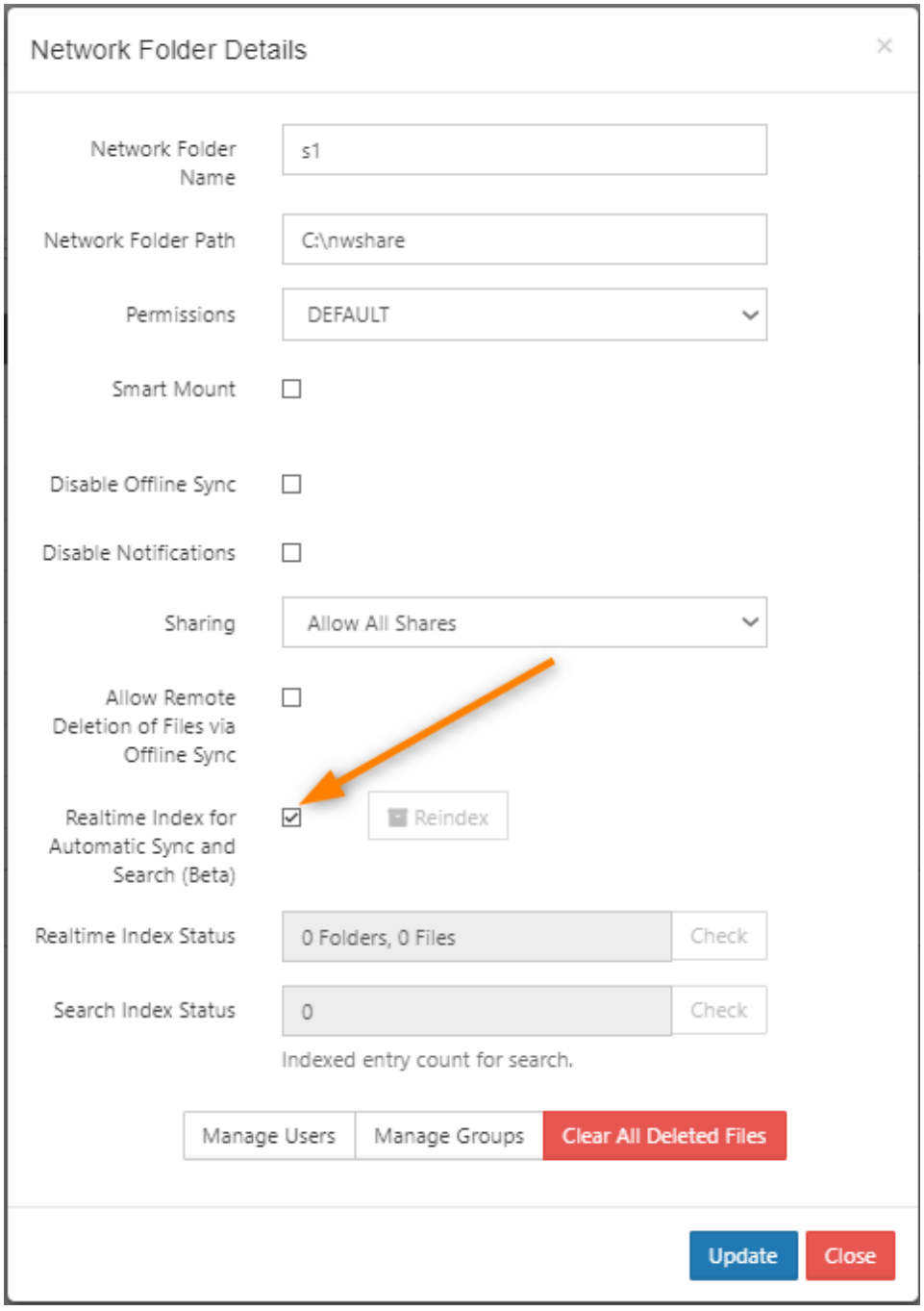
Configure Content Search for Network Storage

In addition to providing content search capabilities for managed storage files, admins also can configure FileCloud to provide content search for network shares.

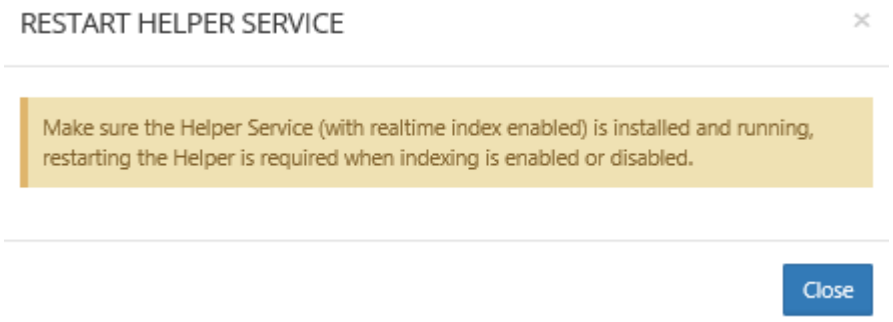
To configure FileCloud with Solr:

1. Ensure you are familiar with indexing for Network Folders and have configured FileCloud Helper for indexing.
2. Login into admin UI. Navigate to Network Folders tab. Select an existing network share or create a new share with required permissions.
3. Open the properties of the share, by clicking on the "Edit" button.

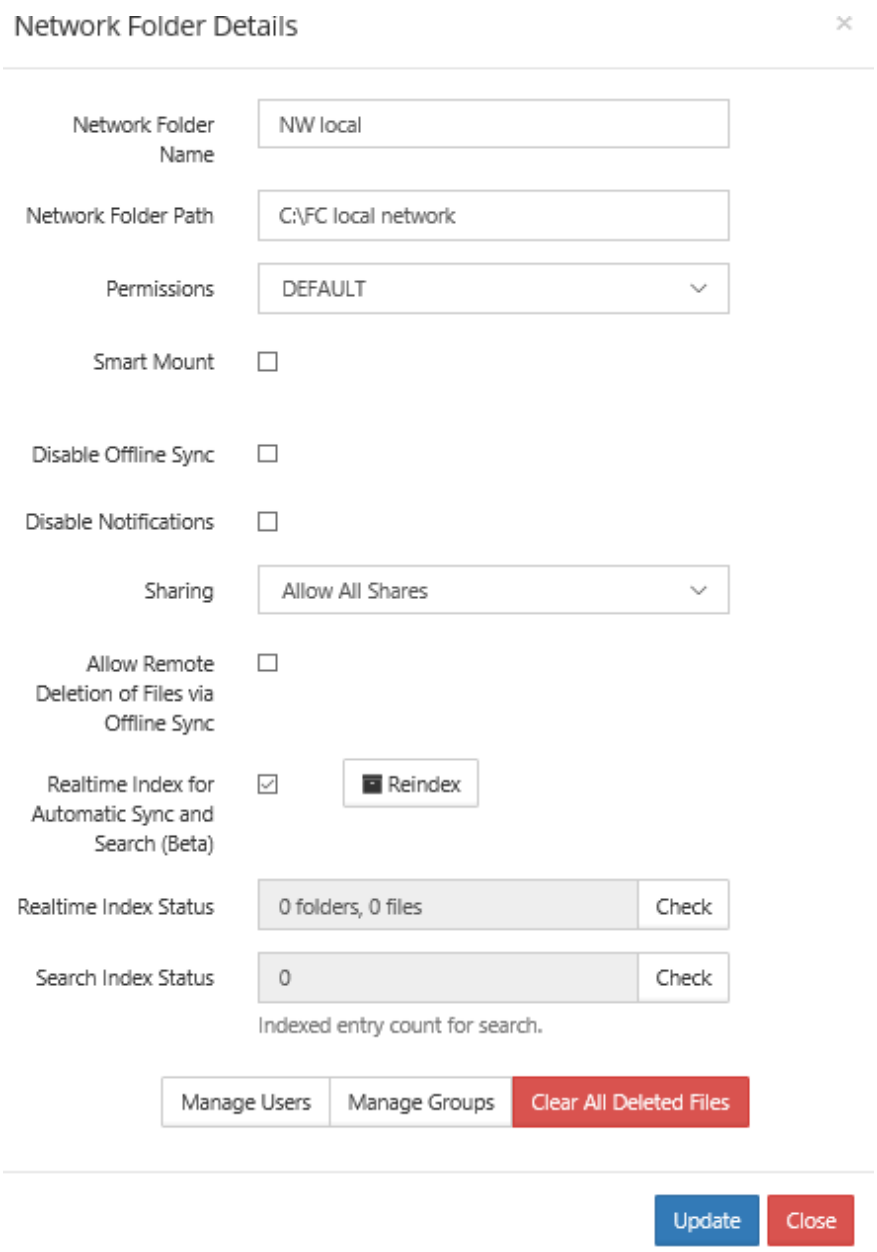
4. In the share settings dialog, select the check box labeled **Realtime Index for Automatic Sync and Search (Beta)**



5. Click **Update**. A popup prompting you to restart NTFS helper service opens. Remember to restart the NTFS helper server. Without a restart, the changes do not go into effect.



6. Select the same share again and open the settings dialog for the share. Now the dialog has status information on realtime indexing and content search.
   Note: Depending on the number, size and type of files in the share, full indexing will take a few minutes to hours.



Enabling Solr OCR

Beginning in FileCloud 23.261, clicking **Enable** for OCR activates OCR for PDFs as well as other image files.

Solr OCR is available for Enterprise users and users with OCR licenses.

> ⚠ We recommend adding 4-8 CPUs to your system before enabling OCR indexing, which is resource-intensive.

When you enable OCR:

- FileCloud's content search engine searches image files and PDF files for your search string.
- FileCloud's content classification engine (CCE) scans image files and PDFs for pattern-matching text.

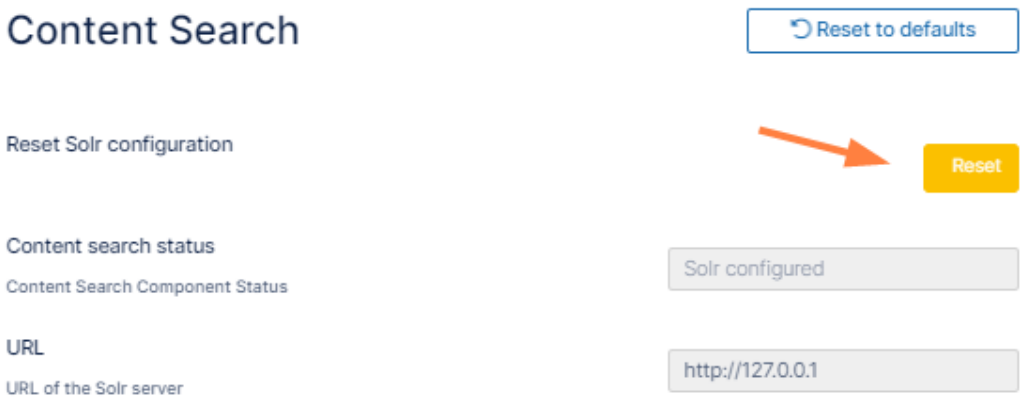
Install and enable Solr OCR on Windows

Follow these instructions on Windows when performing a fresh installation of FileCloud or when performing an upgrade to the OCR component license.

1. Open cloudconfig.php at XAMPP DIRECTORY/htdocs/config/cloudconfig.php
2. Add the following:

```
define("TESSERACTOCR_BIN_DIR", "C:\\xampp\\tesseractocr");
define("TESSERACTOCR_TESSDATA_DIR", "C:\\xampp\\tesseractocr\\tessdata");
```

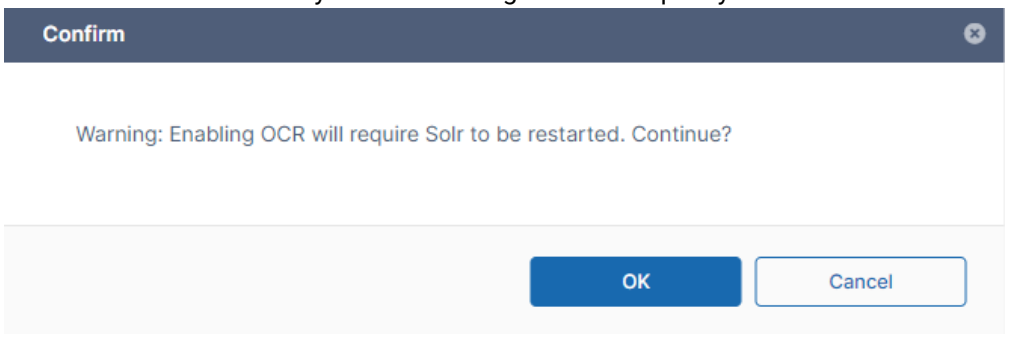
   Note:
   TESSERACTOCR_BIN_DIR is the path to the TesseractOCR installation directory which contains the tesseract binary. In windows, this is typically at C:\xampp\tesseractocr\
   TESSERACTOCR_TESSDATA_DIR is the path to the TesseractOCR training data. In windows, this is typically at C:\xampp\tesseractocr\tessdata
3. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search**  .
   The **Content Search** settings page opens.
4. If you are performing an upgrade, click **Reset**.
   If you are performing a fresh installation, click **Configure**.



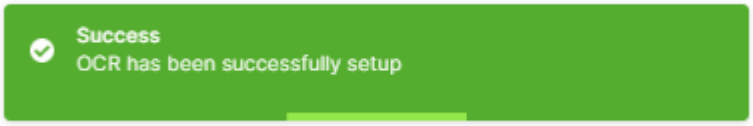
5. Beside **Enable Solr OCR**, click the **Enable** button.



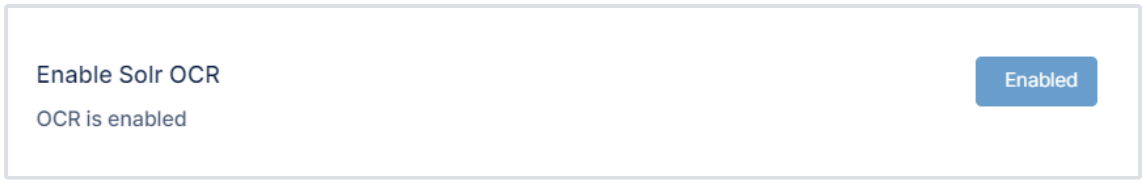
A confirmation box warns you that enabling OCR will require you to restart Solr.



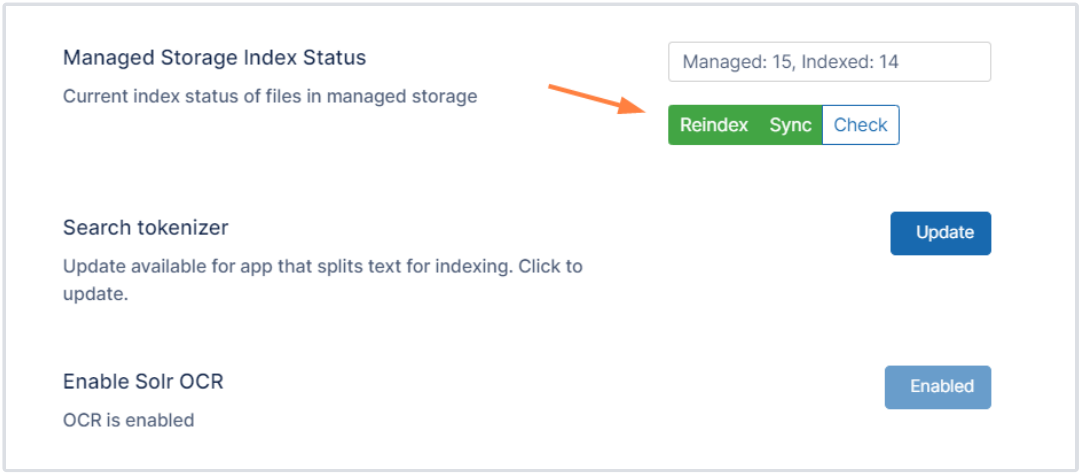
6. Click **OK**.
   A notification confirms that OCR is enabled.



7. Restart the Solr (Content Search) service from the FileCloud control panel.
8. In the admin portal, go to the Content Search settings page again.
   The text **OCR is enabled** appears under **Enable Solr OCR**.



   You have finished enabling OCR.
9. To build or rebuild the search index with OCR for images with text and PDFs, under **Managed Storage Index Status**:
   - If you are performing a fresh installation, click **Index**.
   - If you are performing an upgrade, click **Reindex.**



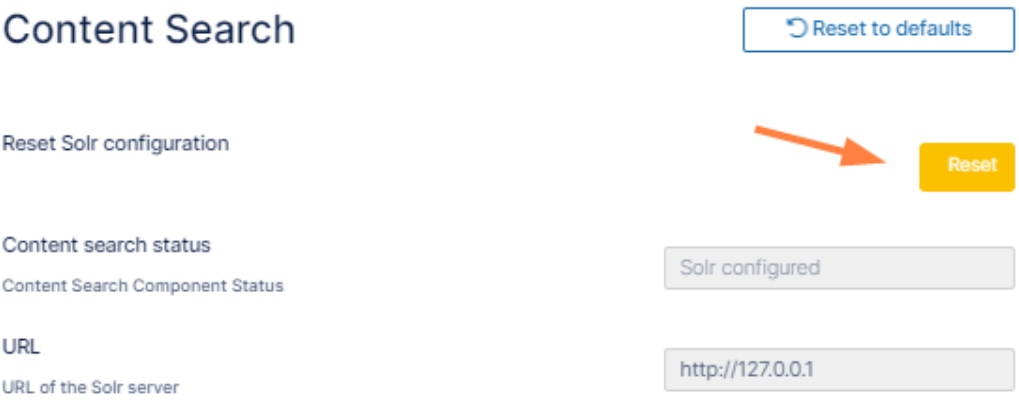
Install and enable Solr OCR on Linux Ubuntu

Follow these instructions on Linux when performing a fresh installation of FileCloud or when performing an upgrade to the OCR component license.

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

```
filecloudcp -t
```

3. If you are performing an upgrade, click **Reset** and delete the current **fccore** if it exists (run command : **rm -rf /opt/solrfcdata/var/solr/data/fccore/**).



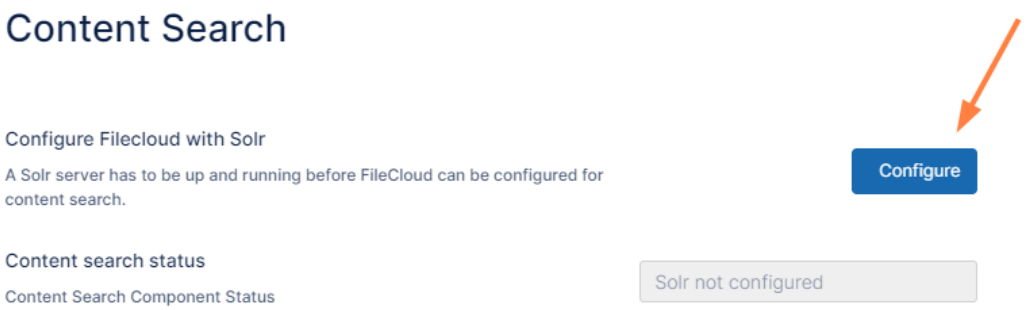
4. Inspect the file **solrconfig.xml** inside **/var/www/html/thirdparty/overrides/solarium/Solarium/fcskel/conf** and uncomment the line containing **parseContext.xml.**
5. In **/var/www/html/thirdparty/overrides/solarium/Solarium**, copy the folder **fcskel** into **/opt/solrfcdata/var/solr/data** (on the solr server) and rename it **fccore**.

Note: For a multi-tenant setup, rename it **fccore_** *site name* (for example, if site name is **mysite**, rename it **fccore_mysite**).

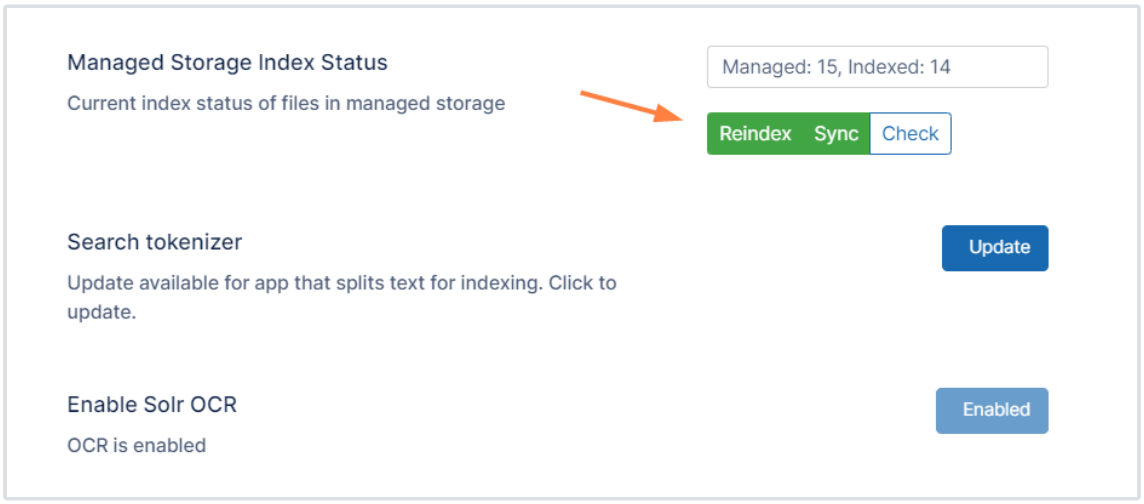
6. After copying the folder as **fccore**, set the ownership for the folder and its contents to solr by running:

```
chown solr.solr -R /opt/solrfcdata/var/solr/data/fccore
```

7. In the admin portal, go to the **Content Search** settings page again.
8. Click **Configure**.



9. Confirm that the message below **Enable Solr OCR** is **OCR is enabled**.
10. To build or rebuild the search index with OCR for images and PDFs with text, click **Index** or **Reindex**.



Install and enable Solr OCR on other Linux distributions:

1. To confirm that Tesseract is set up, enter:

```
filecloudcp -t
```

You should receive the response **Tesseract is already installed and configured**.

2. To assign the Apache user (usually named **www-data**) to the solr group (for example **solr:x:123**) open **/etc/group** for edit, and append the apache user name to the solr group.

```
solr:x:123:www-data
```

3. Restart Apache.

```
systemctl restart apache2
```

4. Assign read and write permissions to the solr group for the Solr core directory of the site/tenant that OCR is being set up for.

```
chmod -R g+rw /opt/solrfcdata/var/solr/data/fccore__<sitename>
```

5. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search**  .
The **Content Search** settings page opens.
6. Follow steps 6 through 9 under **Install and enable Solr OCR on Windows**, above.

Enable OCR manually

If your system is unable to configure OCR automatically, use the following instructions to enable it manually when performing a fresh installation of FileCloud or when performing an upgrade to the OCR component license.

1. Set the Tesseract environment variables:
   - For Windows, add the following to solr.in.cmd:

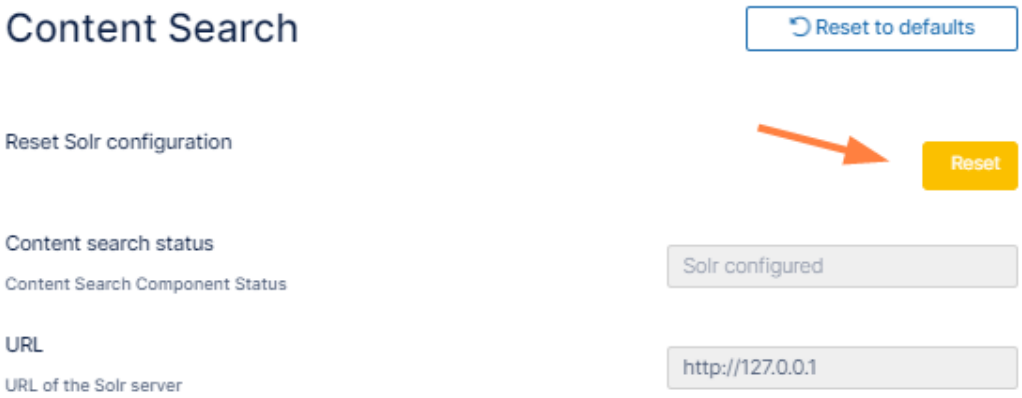
```
SET PATH=%PATH%;C:\xampp\tesseractocr
SET TESSDATA_PREFIX=C:\xampp\tesseractocr\tessdata
```

   - For Linux, add the following to to solr.in.sh (or define the environment variables globally)

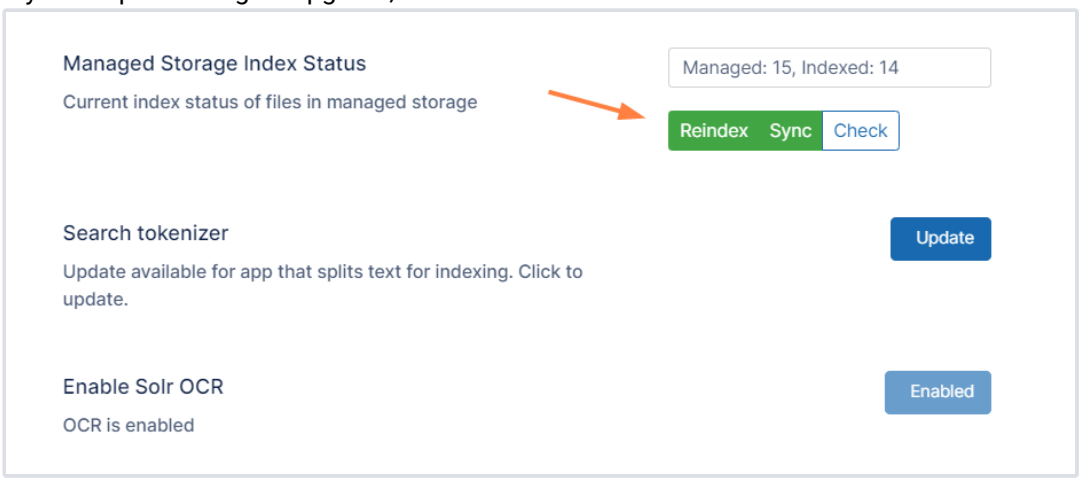
```
PATH="/path/to/tesseractocr:$PATH"
```

```
TESSDATA_PREFIX=/path/to/tesseractocr/tessdata
```

2. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search** .
   The **Content Search** settings page opens.
3. If you are performing an upgrade, click **Reset**.
   If you are performing a fresh installation, clicking **Reset** is not necessary.



4. In **C:\xampp\htdocs\thirdparty\overrides\solarium\Solarium** copy the folder **fcskel** and rename it **fccore**.
   Then move it into **C:\xampp\solr\server\solr**.
5. Restart the Solr (Content Search) service from the FileCloud control panel.
6. In the Admin portal, go to the Content Search settings page again.
7. Confirm that **OCR is enabled** appear under **Enable Solr OCR**.
8. To build or rebuild the search index with OCR for images with text and PDFs:
   - If you are performing an upgrade, click **Reindex.**



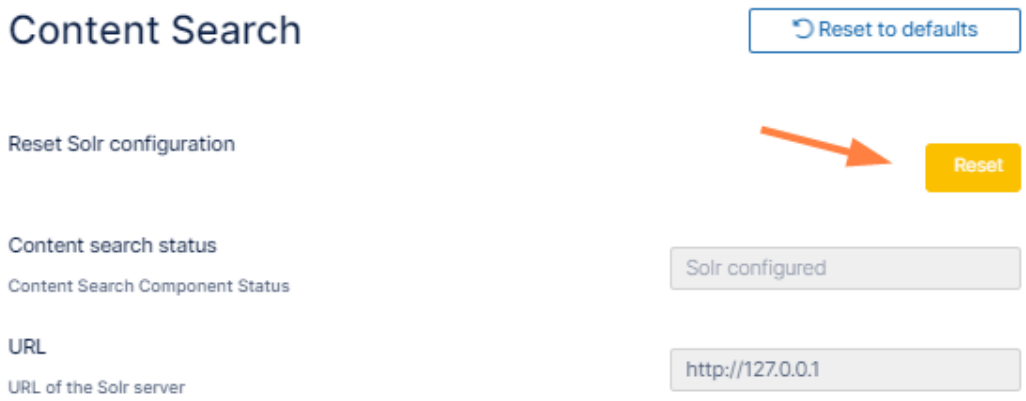
Enable OCR manually when FileCloud and and Solr are on different servers

On the Solr server:

1. In **C:\xampp\solr\bin** open the file **solr.in.cmd** and add the following lines:

```
SET PATH=%PATH%;C:\xampp\tesseractocr
SET TESSDATA_PREFIX=C:\xampp\tesseractocr\tessdata
SET SOLR_SECURITY_MANAGER_ENABLED=false
```

2. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Content Search** .
   The **Content Search** settings page opens.
3. Click **Reset** to reset Solr configuration.



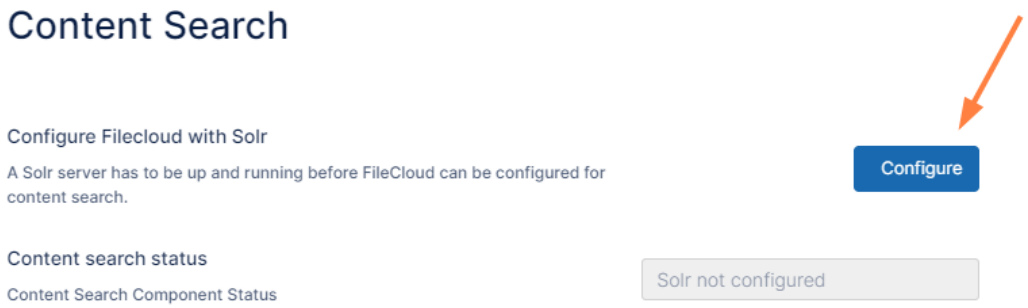
4. From the FileCloud server, copy the folder **C:\xampp\htdocs\thirdparty\solarium\fcskel** to the Solr server as **C:\xampp\solr\server\solr\fccore** (rename **fcskel** to **fccore**).
5. In **C:\xampp\solr\server\solr\fccore\conf** open the file **solrconfig.xml** and uncomment the line containing **parseContext.xml**. Save the file.
   Change:

```
<!-- <str name="parseContext.config">parseContext.xml</str>
```

   to:

```
<str name="parseContext.config">parseContext.xml</str>
```

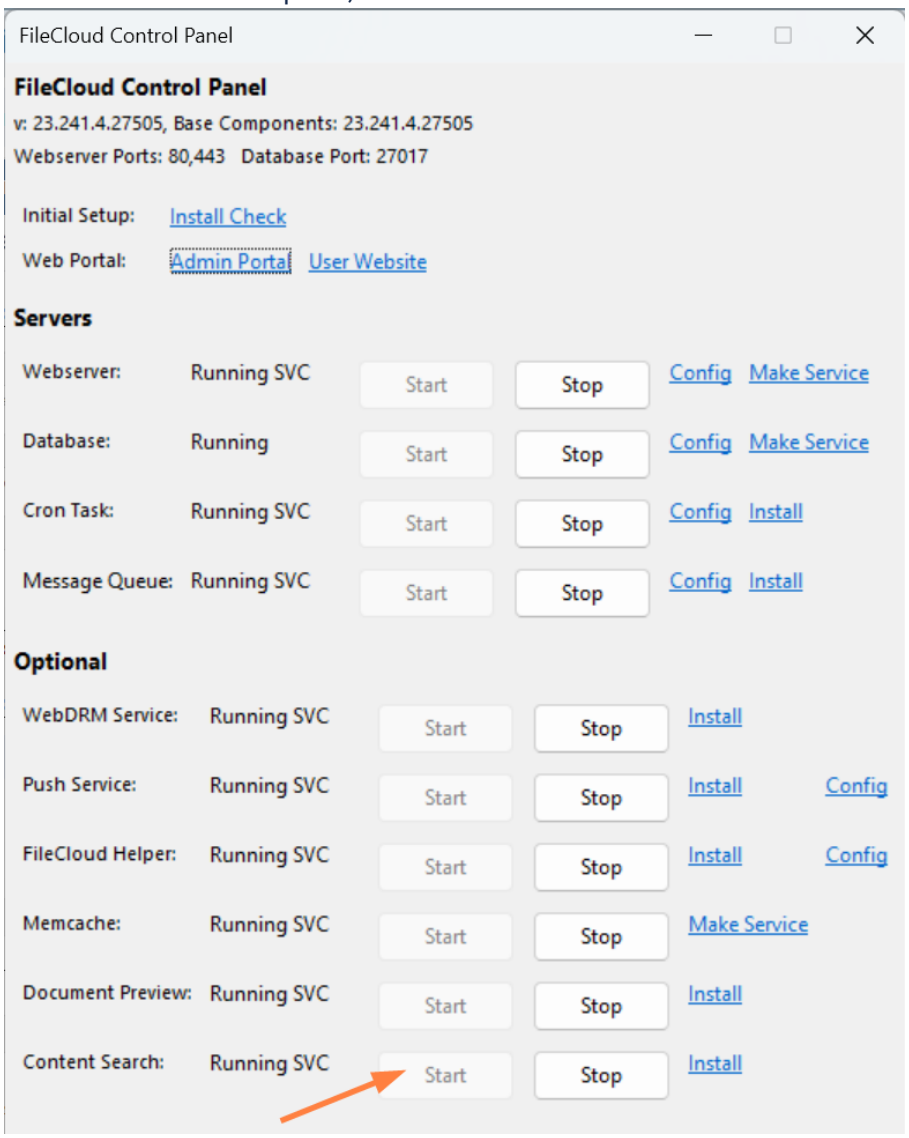
6. In the FileCloud admin portal, go back to the Content Search settings page and click **Configure.**



7. Run the following command to stop Solr:

```
cd C:\xampp\solr\server
java -DSTOP.PORT=7983 -DSTOP.KEY=solrrocks -jar start.jar --stop
```

8. In the FileCloud control panel, start Content Search.



On the FileCloud server:

1. In **c:\xampp\htdocs\config\cloudconfig.php** add the following lines:

```
define("TESSERACTOCR_BIN_DIR", "C:\\xampp\\tesseractocr");
define("TESSERACTOCR_TESSDATA_DIR", "C:\\xampp\\tesseractocr\\tessdata");
```

2. In the FileCloud admin portal, go to the Content Search settings page and verify that the message **OCR is enabled** appears under **Enable Solr OCR**.



SOLR Config Tips

Increasing Solr Heap Size

If you manage a large number of files (especially text-based documents) and are seeing Solr crash with an **out of memory** error in its logs, try the following tip to solve the issue.

By default, Solr ships with 512MB for heap size. In some installations with large numbers of files (especially text-based documents), this heap memory is not enough. Solr might crash in these cases and show an **out of memory** error in its logs.

- Follow these steps to increase the heap size.
- In this example, the heap size is increased to 2G.
- Administrators can increase it more depending on their site needs.

To increase the Solr heap size:

1. If Solr server does not stop when stopped from services, open the control panel and kill the java process. Make sure no process is listening at port 8983.
2. Solr may require more memory depending on the amount of data being indexed (JAVA OOM errors). In that case, the only option is to bump of the system memory and increase the JAVA heap limit.

   To update the Java heap limit for SOLR To 2GB:

   ```
   In the registry under
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\solrservice\
   Look for the APP Parameters and add -m 2G
   Restart the service.
   ```

3. Start the Solr service from FileCloud control panel or Windows services panel.

Changing Solr Temporary folder

To change the java.io.tmpdir variable:

```
1- in Linux
Add the following line to /etc/default/solr.in.sh:
SOLR_OPTS="$SOLR_OPTS -Djava.io.tmpdir=/your/tmp/dir"

2- in Windows
Add the following line to C:\xampp\solr\bin\solr.in.cmd
SOLR_OPTS="$SOLR_OPTS -Djava.io.tmpdir=/your/tmp/dir"
```

Make sure to restart Solr for the changes to take effect.

Enabling Authentication for Solr

1. Create a new file with name **security.json** at **/opt/solr76data/var/solr/data/security.json** for Linux or **C:\xampp\solr\server\solr\security.json** for Windows
2. Add the following lines to **security.json** file. This enables login with username **solr** and password **SolrRock**

   To enable Solr authentication:

```
{
    "authentication":
    {
        "blockUnknown": true,
        "class":"solr.BasicAuthPlugin",
        "credentials": {
            "solr":"IV0EHq1OnNrj6gvRCwvFwTrZ1+z1oBbnQdiVC3otuq0=
Ndd7LKvVBAaZIF0QAVi1ekCfAJXr1GGfLtRUXhgrF8c="
        }
    },
    "authorization":
    {
        "class":"solr.RuleBasedAuthorizationPlugin",
        "permissions":
        [
            {
                "name":"security-edit",
                "role":"admin"
            }
        ],
        "user-role":
        {
            "solr":"admin"
        }
    }
}
```

3. Restart Solr and check http://localhost:8983/solr for authentication
4. Add the following entries to the cloudconfig:

   cloudconfig.php entries:

```
define("TONIDOCLOUD_SOLR_USERNAME", "solr");
define("TONIDOCLOUD_SOLR_PASSWORD", "SolrRocks");
```

5. Restart the Message Queue (you can restart from the FileCloud Control Panel).
6. To change the password use the following command:

```
curl -user solr:SolrRocks http://localhost:8983/solr/admin/authentication -H
'Content-type:application/json' -d '{"set-user":{"solr":"NewPassword"}}'
```

7. To change the password for SSL protected Solr server use the following command:

```
curl -u solr:SolrRocks https://your_domain_name:8983/solr/admin/authentication -H
'Content-type:application/json' -d '{"set-user":{"solr": "codelathe"}}'
```

NOTE: the username **solr** can be changed to anything but it has to be replaced for all the steps (including the initial config).

8. To make solr daemon detect Solr status you need to update the following config files.

To change the java.io.tmpdir variable:

```
1- in Linux
Add the following line to /etc/default/solr.in.sh:
SOLR_AUTH_TYPE="basic"
SOLR_AUTHENTICATION_OPTS="-Dbasicauth=solr:codelathe"

2- in Windows
Add the following line to C:\xampp\solr\bin\solr.in.cmd
SOLR_AUTH_TYPE="basic"
SOLR_AUTHENTICATION_OPTS="-Dbasicauth=solr:codelathe"
```

This is necessary only if authentication is enabled on Solr.

SOLR With SSL

To setup SSL with Solr requires:

- Private or self-signed SSL certificates
- A working Solr installation

Option 1: To configure SSL using private certificates:

1. Combine the SSL certificate, intermediate certificates and root CA certificate (if any) into one file

```
cat server.crt <(echo) server-ca.crt <(echo) root-ca.crt > server-chain.crt
```

Required: Put the server certificate file first, and then if applicable, the intermediate certificate file(s), and then the root CA certificate file.

2. Combine the private key and the above created certificate chain file into a PKCS12 format file to load into a new keystore. Enter a password when OpenSSL asks for an *export password*.

```
openssl pkcs12 -export -inkey server.key -in server-chain.crt -out server.pkcs12
```

⚠ If you are running in a FIPS environment, the above command will result in a failure. Instead, enter:

```
openssl pkcs12 -export \
  -nomac \
  -name solr \
  -inkey [yourdomain].com_key.txt \
  -in [yourdomain].com.crt \
  -certfile [yourdomain].com.ca-bundle \
  -out solr-ssl.keystore.p12
```

3. Load the resulting PKCS12 file into a JSSE keystore. The keystore file should ideally be stored in "server/etc" folder under solr installation directory. Enter the export password for source password and a destination password.

```
keytool -importkeystore -srckeystore server.pkcs12 -srcstoretype PKCS12
-destkeystore /opt/solr-7.6.0/server/etc/keystore.jks
```

4. Add/Modify as required the following properties into the file /etc/default/solr.in.sh. Replace key store password and trust store password below with the destination password provided above.

```
# Enables HTTPS. It is implicitly true if you set SOLR_SSL_KEY_STORE. Use this
 config
# to enable https module with custom jetty configuration.
SOLR_SSL_ENABLED=true
# Be sure to update the paths to the correct keystore for your environment
SOLR_SSL_KEY_STORE=etc/keystore.jks
SOLR_SSL_KEY_STORE_PASSWORD=secret
SOLR_SSL_TRUST_STORE=etc/keystore.jks
SOLR_SSL_TRUST_STORE_PASSWORD=secret
# Require clients to authenticate
SOLR_SSL_NEED_CLIENT_AUTH=false
# Enable clients to authenticate (but not require)
SOLR_SSL_WANT_CLIENT_AUTH=false
# SSL Certificates contain host/ip "peer name" information that is validated by
default. Setting
# this to false can be useful to disable these checks when re-using a certificate
on many hosts
SOLR_SSL_CHECK_PEER_NAME=true
# Override Key/Trust Store types if necessary
```

```
SOLR_SSL_KEY_STORE_TYPE=JKS
SOLR_SSL_TRUST_STORE_TYPE=JKS
```

5. Restart Solr

```
service solr restart
```

Option 2: To configure SSL using self-signed certificates:

1. Create a self-signed keystore file. Replace <private-ip> with the private IP of machine running Solr in -ext parameter (Example: IP:192.168.1.2). Enter a keystore password and key password when prompted.

```
keytool -genkeypair -alias solr-ssl -keyalg RSA -keysize 2048 -validity 9999
 -keystore /opt/solr-7.6.0/server/etc/solr-ssl.keystore.jks -ext
SAN=DNS:localhost,IP:<private-ip>,IP:127.0.0.1 -dname "CN=localhost,
OU=Organizational Unit, O=Organization, L=Location, ST=State, C=Country"
```

2. Add/Modify as required the following properties into the file /etc/default/solr.in.sh. Replace key store password and trust store password below with the keystore password provided above.

```
# Enables HTTPS. It is implictly true if you set SOLR_SSL_KEY_STORE. Use this
 config
# to enable https module with custom jetty configuration.
SOLR_SSL_ENABLED=true
# Be sure to update the paths to the correct keystore for your environment
SOLR_SSL_KEY_STORE=etc/solr-ssl.keystore.jks
SOLR_SSL_KEY_STORE_PASSWORD=secret
SOLR_SSL_TRUST_STORE=etc/solr-ssl.keystore.jks
SOLR_SSL_TRUST_STORE_PASSWORD=secret
# Require clients to authenticate
SOLR_SSL_NEED_CLIENT_AUTH=false
# Enable clients to authenticate (but not require)
SOLR_SSL_WANT_CLIENT_AUTH=false
# SSL Certificates contain host/ip "peer name" information that is validated by
default. Setting
# this to false can be useful to disable these checks when re-using a certificate
on many hosts
SOLR_SSL_CHECK_PEER_NAME=true
# Override Key/Trust Store types if necessary
SOLR_SSL_KEY_STORE_TYPE=JKS
SOLR_SSL_TRUST_STORE_TYPE=JKS
```

3. Turn off verification for Solr's SSL certificate:

a. Open the cloudconfig.php file
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/html/config/cloudconfig.php

b. Add the setting:

```
define("TONIDOCLOUD_VERIFY_SOLR_SSL_CERTIFICATE", false);
```

c. Save your change.

4. Restart Solr.

```
service solr restart
```

Solr High Availability Setup with Pacemaker and Corosync



This setup requires two Linux Solr hosts with an NFS resource mounted on them, a quorum device, and an HAProxy load balancer. These resources must be in an active/passive configuration.
In the following documentation, the Solr servers run on Linux CentOS 7, but you may use any Linux distribution that enables you to set up a Pacemaker/Corosync cluster.

Introduction

FileCloud provides advanced search capabilities using Solr (an open source component) in the backend. For some cases, service continuity requires a high availability setup for Solr, which you can configure using the following instructions.

Prerequisites

- The cluster in the setup used in these instructions includes the following. Your setup should have similar components.

solr01 – Solr host cluster node
solr02 – Solr host cluster node
solr03 – quorum device cluster node
solr-ha – HAProxy host
NFSShare – NFS resource mounted on **solr01** and **solr02**

1. Install all patches available for FileCloud.
2. Perform the following steps for **sor01**, **solr02**, and **solr03**.
   a. To update all packages, run:

```
yum update
```

b. Reboot the system.

3. To install the package which provides the nfs-client subsystems, run:

```
yum install -y nfs-utils
```

4. To install wget, run:

```
yum install -y wget
```

Install Solr

On **solr01**:

1. Perform a clean install of your Linux operating system.
2. To download the FileCloud installation script, **filecloud-liu.sh**, enter:

```
wget http://patch.codelathe.com/tonidocloud/live/installer/filecloud-liu.sh
```

3. To create the folder **/opt/sorfcdata**, enter:

```
mkdir /opt/solrfcdata
```

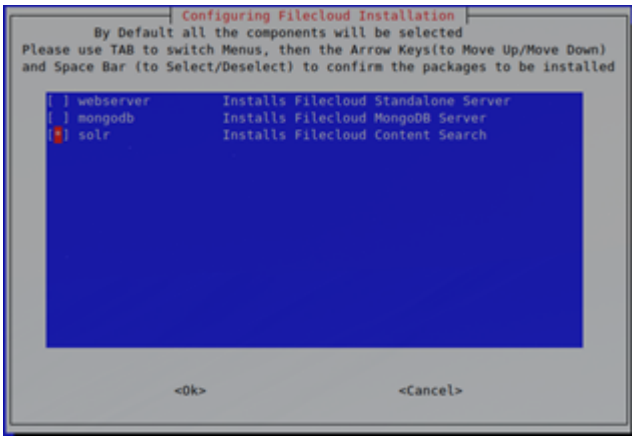
4. Mount the NFS filesystem under **/opt/sorfcdata**:

```
mount -t nfs ip_nfs_server:/path/to/nfs_resource /opt/solrfcdata
```

5. Install solr by running the FileCloud installation script:
   a. Run:

```
sh ./filecloud-liu.sh
```

   b. Follow the instructions in the windows until you reach the selection screen:



c. Select **solr** only, then wait a few minutes until you receive confirmation that installation is complete.

6. Bind **solrd** to the external interface instead of localhost only:
   a. On **solr01** and **solr02** open:
   /opt/solr/server/etc/jetty-http.xml
   and change:
   <Set name="host"><Property name="jetty.host" default="127.0.0.1" /></Set>
   to:
   <Set name="host"><Property name="jetty.host" default="0.0.0.0" /></Set>

7. Change from **systemV** daemon control to **systemd**.
   a. To stop Solr on **solr01** and **solr02**, enter:

```
/etc/init.d/solr stop
```

   b. To remove the existing service file in **/etc/init.d/solr**, enter:

```
rm /etc/init.d/solr
```

   c. To create a new **solrd.service** file, enter:

```
touch /etc/systemd/system/solrd.service
```

   d. To edit the **solrd.service** file, enter:

```
vi /etc/systemd/system/solrd.service
```

e. Enter the following service definition into the file:

```
### Beginning of File ###
[Unit]
Description=Apache SOLR

[Service]
User=solr
LimitNOFILE=65000
LimitNPROC=65000

Type=forking

Restart=no

ExecStart=/opt/solr/bin/solr start
ExecStop=/opt/solr/bin/solr stop

### End of File ###
```

f. Save the **solrd.service** file.

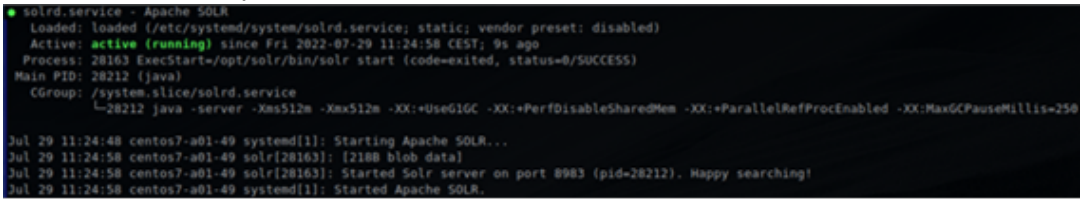
8. Verify that the service definition is working. Perform the following steps on **solr01** and **solr02**:
   a. Enter:

```
systemctl daemon-reload
systemctl stop solrd
```

   b. Confirm that no error is returned.
   c. Restart the server by entering:

```
systemctl start solrd
systemctl status solrd
```

   d. Confirm that the output returned resembles:



e. Remove the content of folder **/opt/solrfcdata** on **solr02** only.

```
systemctl stop solrd
rm -rf /opt/solrfcdata/*
```

9. Update the firewall rules on **solr01** and **solr02** if necessary:

```
firewall-cmd --permanent --add-port 8983/tcp
firewall-cmd --reload
```

Set Up the Pacemaker Cluster

1. On **solr01**, **solr02**, and **solr03**, open the **/etc/hosts** file and add the following. Substitute the IP address for each cluster node with the correct one).

```
cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1  localhost localhost.localdomain localhost6 localhost6.localdomain6


192.168.101.59 solr01
192.168.101.60 solr02
192.168.101.61 solr03
```

2. To install the cluster packages for **solr01** and **solr02**, for each, enter:

```
yum -y install pacemaker pcs corosync-qdevice sbd
```

3. To enable and start the main cluster daemon for **solr01** and **solr02**, for each, enter:

```
systemctl start pcsd
systemctl enable pcsd
```

4. Set the same password on **solr01** and **solr02** for **hacluster** (the HA cluster user):

```
[passwd] hacluster
```

5. On **solr01** and **solr02**, open network traffic on the firewall.

```
firewall-cmd --add-service=high-availability -permanent
firewall-cmd --reload
```

6. On **solr01** only, authorize the cluster node.
   a. On **solr01** only, enter.

```
pcs cluster auth solr01 solr02
```

   b. When prompted, enter your username and password.
   c. Confirm that the following is returned:

```
solr01      Authorized
solr02      Authorized
```

7. To create the initial cluster instance on **solr01**, enter:

```
pcs cluster setup --name solr_cluster solr01 solr02
```

8. To start and enable the cluster instance on **solr01**, enter:

```
pcs cluster start --all
pcs cluster enable --all
```

Set up the Qdevice (Quorum Node)

1. Install corosync on **solr03**:

```
yum install pcs corosync-qnetd
```

2. Start and enable the pcs daemon (pcsd) on **solr03**:

```
systemctl enable pcsd.service
systemctl start pcsd.service
```

3. Configure the Qdevice daemon on **solr03**:

```
pcs qdevice setup model net --enable -start
```

4. If necessary, open firewall traffic on **solr03**:

```
firewall-cmd --permanent --add-service=high-availability
firewall-cmd --add-service=high-availability
```

5. Set the password for the HA cluster user on **solr03** to the same value as the passwords on **solr01** and **solr02**:

```
[passwd] hacluster
```

6. On **solr01,** authenticate **solr03:**

```
pcs cluster auth solr03
```

When prompted, enter your username and password.

7. On **solr01**, add the Qdevice (**solr03)** to the cluster:

```
pcs quorum device add model net host=solr03 algorithm=lms
```

8. On solr01, check the status of the Qdevice (solr03)

```
pcs quorum status
```

Confirm that the information returned is similar to:

```
Quorum information
------------------
Date:             Wed Aug  3 10:27:26 2022
Quorum provider:  corosync_votequorum
Nodes:            2
Node ID:          1
Ring ID:          2/9
Quorate:          Yes

Votequorum information
```

```
----------------------
Expected votes:   3
Highest expected: 3
Total votes:      3
Quorum:           2
Flags:            Quorate Qdevice

Membership information
----------------------
    Nodeid      Votes    Qdevice Name
         2          1    A,V,NMW solr02
         1          1    A,V,NMW solr01 (local)
         0          1            Qdevice
```

Install soft-watchdog

1. On **solr01** and **solr02**, set up automatic soft-watchdog module to load whenever you reboot:

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

2. Reboot **solr01** and **solr02** to activate soft-watchdog. First reboot **solr01**, and wait for confirmation. Then reboot **solr02**.

```
reboot
```

Enable the stonith block device (sbd) mechanism in the cluster

The sbd mechanism manages the watchdog and initiates stonith.

1. In **solr01** and **solr02**, enter the enable sbd command:

```
pcs stonith sbd enable
```

2. On **solr01**, restart the cluster to activate enabling of sbd.

```
pcs cluster stop --all
pcs cluster start --all
```

3. On **solr01**, check the status of sbd:

```
pcs stonith sbd status
```

Confirm that the information returned is similar to:

```
SBD STATUS
<node name>: <installed> | <enabled> | <running>
solr01: YES | YES | YES
solr02: YES | YES | YES
```

Create cluster resources

1. On **solr01**, create **nfsmount**.

```
pcs resource create NFSMount Filesystem device=192.168.101.70:/mnt/rhvmnfs/solrnfs
directory=/opt/solrfcdata fstype=nfs --group solr
```

Note: Set the parameter **device** to the nfs server and nfs share which is being used in the configuration.

2. On **solr01**, check the status of **nfsmount**.

```
pcs status
```

Confirm that the information returned is similar to:

```
Cluster name: solr_cluster
Stack: corosync
Current DC: solr01 (version 1.1.23-1.el7_9.1-9acf116022) - partition with quorum
Last updated: Wed Aug  3 12:22:36 2022
Last change: Wed Aug  3 12:20:35 2022 by root via cibadmin on solr01

2 nodes configured
1 resource instance configured

Online: [ solr01 solr02 ]

Full list of resources:

 Resource Group: solr
     NFSMount   (ocf::heartbeat:Filesystem):    Started solr01

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
  sbd: active/enabled
```

3. Change the recovery strategy for **nfsmount**.

```
pcs resource update NFSMount meta on-fail=fence
```

4. On **solr01**, create the cluster resource **solrd**.

```
pcs resource create solrd systemd:solrd --group solr
```

5. On **solr01**, check the status of **solrd**:

```
pcs status
```

Confirm that the information returned is similar to:

```
Cluster name: solr_cluster
Stack: corosync
Current DC: solr01 (version 1.1.23-1.el7_9.1-9acf116022) - partition with quorum
Last updated: Wed Aug  3 12:25:45 2022
Last change: Wed Aug  3 12:25:22 2022 by root via cibadmin on solr01

2 nodes configured
2 resource instances configured

Online: [ solr01 solr02 ]

Full list of resources:

 Resource Group: solr
     NFSMount   (ocf::heartbeat:Filesystem):    Started solr01
     solrd      (systemd:solrd):        Started solr02

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
  sbd: active/enabled
```

6. On **solr01**, set additional cluster parameters:

```
pcs property set stonith-watchdog-timeout=36
pcs property set no-quorum-policy=suicide
```

Configure haproxy on its dedicated host

Note: Make sure solr-ha is cleaned up before you install **haproxy** on it.

1. On **solr-ha**, install haproxy:

```
yum install -y haproxy
```

2. On **solr-ha**, configure **haproxy** to redirect to an active solr node.
   a. Back up **/etc/haproxy/haproxy.cfg**.

```
mv /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg_bck
```

   b. Create a new empty copy of **/etc/haproxy/haproxy.cfg**, and enter the content below into it. Make sure that the parameters **solr01** and **solr02** point to the full DNS name or to the IP address of the cluster nodes.

```
#### beginning of /etc/haproxy/haproxy.cfg ###
global
    log         127.0.0.1 local2
    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon
    stats socket /var/lib/haproxy/stats
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 3000

frontend solr_front *:8983
     default_backend solr_back

backend static
    balance     roundrobin
    server      static 127.0.0.1:4331 check

backend solr_back
```

```
        server solr01   solr01:8983 check
        server solr02   solr02:8983 check

#### beginning of /etc/haproxy/haproxy.cfg ###
```

3. On **solr-ha**, start **haproxy.**

```
systemctl enable haproxy
systemctl start haproxy
```

Solr service is now available on host **solr-ha** on port **8983**. However, it is really running on **solr01** or **solr02**.

Find and Index Unindexed Files

The tool for searching for and indexing unindexed files is available in FileCloud 21.2 and later.

FileCloud provides a command line tool that searches for unindexed files and indexes them.

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

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

To locate and index unindexed files using the tool:

1. First, run the tool with the **--exportunindexed** parameter to find and export unindexed files as a csv file:

```
cd C:\xampp\htdocs\resources\tools\contentsearch
C:\xampp\php\php.exe searchindexcli.php --exportunindexed
```

The tool will generate a csv file of any unindexed files:

```
$ php searchindexcli.php --exportunindexed
Searching unindexed files...
1: /tester223
2: /tester223/SensitivityLabel.xlsx
3: /tester223/SensitivityLabel.docx
Done in 107.1632ms. Found 3 unindexed files.
CSV was generated: D:\Workspace\FileCloud\cl-fc-server\server\src\Module\SearchExt\unindexed-1626184138.csv.
```

2. Next, run the tool with the **--importunindexed** parameter and the **--targetfile** parameter set equal to the exported filename. This imports and indexes the unindexed files.

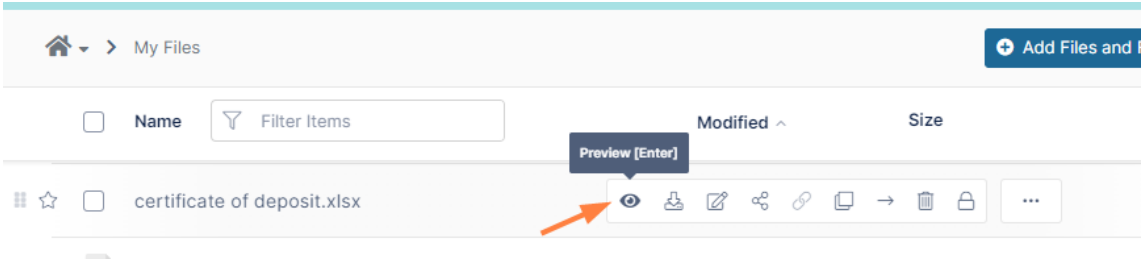
```
C:\xampp\php\php.exe searchindexcli.php --importunindexed --
targetfile=unindexedfilename.csv
```

```
$ php searchindexcli.php --importunindexed --targetfile=unindexed-1626184138.csv
1: Meta indexed /tester223
2: Content indexed /tester223/SensitivityLabel.xlsx
3: Content indexed /tester223/SensitivityLabel.docx
Done in 5754.4114ms. Indexed 3 files.
```

Setting Up Document Preview

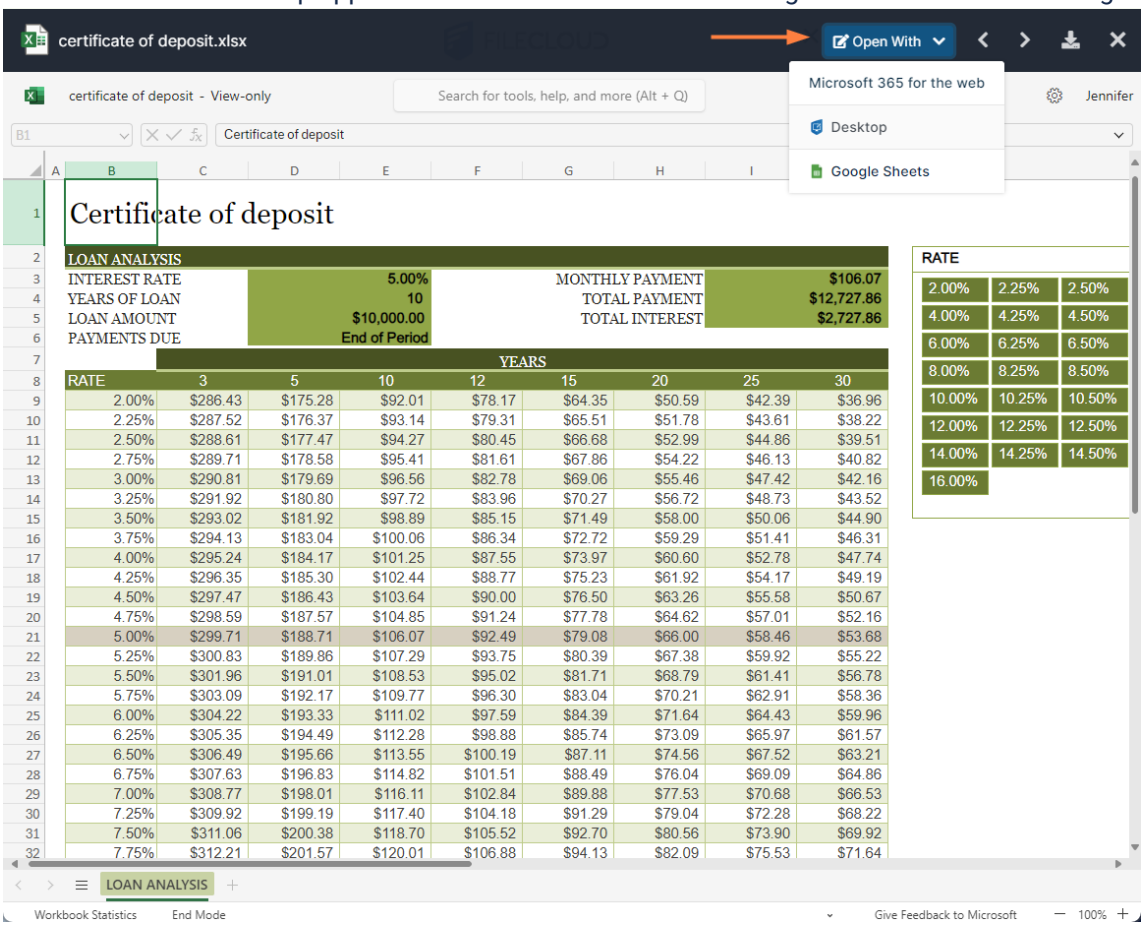
When users preview supported file types directly in the User Portal through the web browser, they can see part of the file without having to install the application that created it.
This type of preview commonly uses the Quick JS Preview feature which enables previewing of DOCX, PPTX, XLSX, and PDF files when DocConverter is enabled. See LibreOffice Windows Instructions.

1. When a user selects a file in the User Portal, a Preview button becomes available.



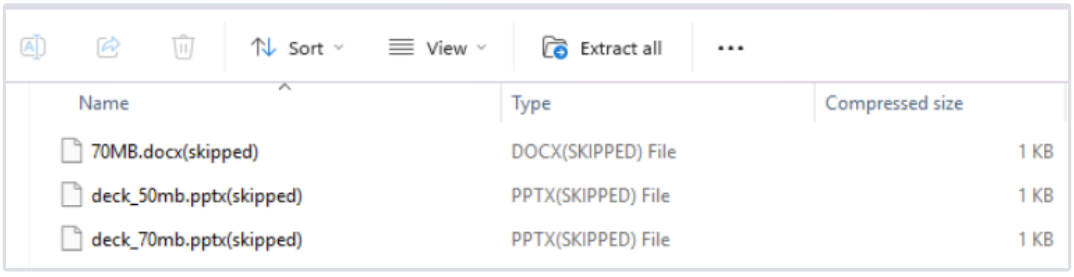
2. When the user clicks the **Preview** button, a separate window opens showing an image of the file. Beginning in FileCloud 22.1, many of the previews can be edited with the same Web edit/Office

Online and Edit in Desktop applications that are available for editing the file from the file listing.



To include watermarks on previewed documents, see Watermark Settings.

When watermarks are enabled for previews, Office files larger than TONIDOCLOUD_DOCPREVIEW_SIZELIMIT are listed but not downloaded in the Zip file containing the previewed files and **skipped** appears beside them:



File types that can be previewed

	Extension	Registered To	Available in FileCloud Version	Description
 Illustrator	.AI	Adobe	18.2	An Adobe Illustrator format is a proprietary file format developed by Adobe Systems for representing single-page vector-based drawings in either the EPS or PDF formats.
 DICOM	.DICOM	DICOM	18.2	Medical files such as X-rays, CT scans, Ultrasounds and MRIs. Beginning with version 23.242 of FileCloud, previewed DICOM files are displayed in the Rubo DICOM viewer. For help using the various functions that this viewer makes available to you, see the section *How can I use the DICOM images in preview?* at the bottom of the page (23.263a) Preview a File.
 AutoCAD	.DWF, .DWG, .DXF (and 60+ other AutoCAD formats).	AutoCAD	22.1	2D and 3D architectural drawings in AutoCAD file formats.
High Efficiency Image Container	.HEIC		23.251	.HEIC files are compressed image files, often used on iOS devices.
Oasis graphic and spreadsheet files	.ODF .ODS			Binary files used to define data structures.
OpenDocument text	.ODT			Documents created by word processors that use OpenDocument Text File format, such as LibreOffice and OpenOffice.

	Extension	Registered To	Available in FileCloud Version	Description
 PDF	.PDF	Adobe	4.0	Portable Document Format (PDF) is a file format used to present documents in a manner independent of application software, hardware, and operating systems. Each PDF file encapsulates a complete description of a fixed-layout flat document, including the text, fonts, graphics, and other information needed to display it. PDF file preview will work even if Document Preview is not installed. For Adobe, Document Preview is required to preview files like PSD, and ai.
 Photoshop	.PSD	Adobe	18.2	Java 10 and above is required for PSD viewing. A .PSD file is a layered image file used in Adobe PhotoShop. PSD, which stands for Photoshop Document, is the default format that Photoshop uses for saving data. PSD is a proprietary file that allows the user to work with the images' individual layers even after the file has been saved.
Microsoft				
 Word	.DOC	Microsoft	4.0	Microsoft WORD files created in versions 2003 and earlier.
 Word	.DOCX	Microsoft	4.0	Microsoft WORD files created in versions 2007 and later.
 PowerPoint	.PPT	Microsoft	4.0	Microsoft PowerPoint files created in versions 2003 and earlier.
 PowerPoint	.PPTX	Microsoft	4.0	Microsoft PowerPoint files created in versions 2007 and later.

	Extension	Registered To	Available in FileCloud Version	Description
 Excel	.XLS	Microsoft	4.0	Microsoft Excel files created in versions 2003 and earlier.
 Excel	.XLSX	Microsoft	4.0	Microsoft Excel files created in versions 2007 and later.
Apple iWork Suite	.pages, .numbers, .key	Apple	23.252	Apple's app suite for documents, spreadsheets, and presentations Currently, .numbers file previews appear with table gridlines and numbers only. Additional table formatting does not appear in the previews. Preview only. Editing is not available from the previewed files.
Video formats	.MP4 .M4V .WEBM .OGV .MOV			The video files listed can only be viewed correctly if they have video and audio codecs in the following formats: .MP4 and .M4V - H.264 video codec and AAC audio codec .WEBM - VP8 video codec and Vorbis audio codec .OGV - Theora video codec and Vorbis audio codec; .OGV file viewing is not supported in Safari .MOV - H.264 video codec and AAC audio codec
Audio formats	.MP3 .OGG .WAV .M4A			

PDF file preview will work even if Document Preview is not installed. Document Preview is required to preview files like PSD and AI.
Previewing AutoCAD files is available in FileCloud 22.1 and later, when you configure AutoDesk Viewer integration with FileCloud.

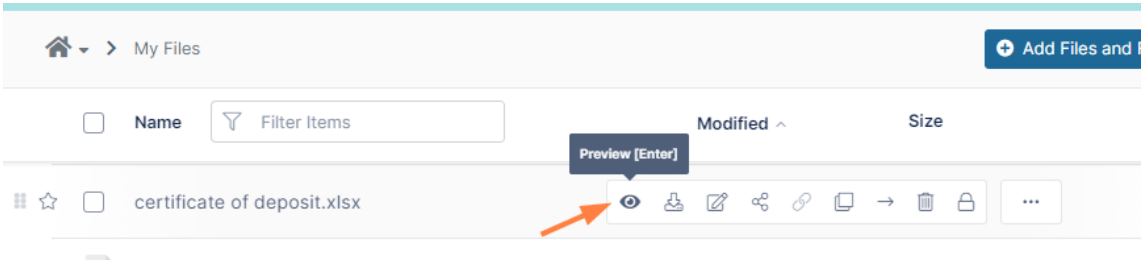
Note: Administrators can also show a sample of the content in a file through a thumbnail image shown beside the file where it is listed in the user portal using FileCloud Document Converter

Also see: Document Preview

Document Preview

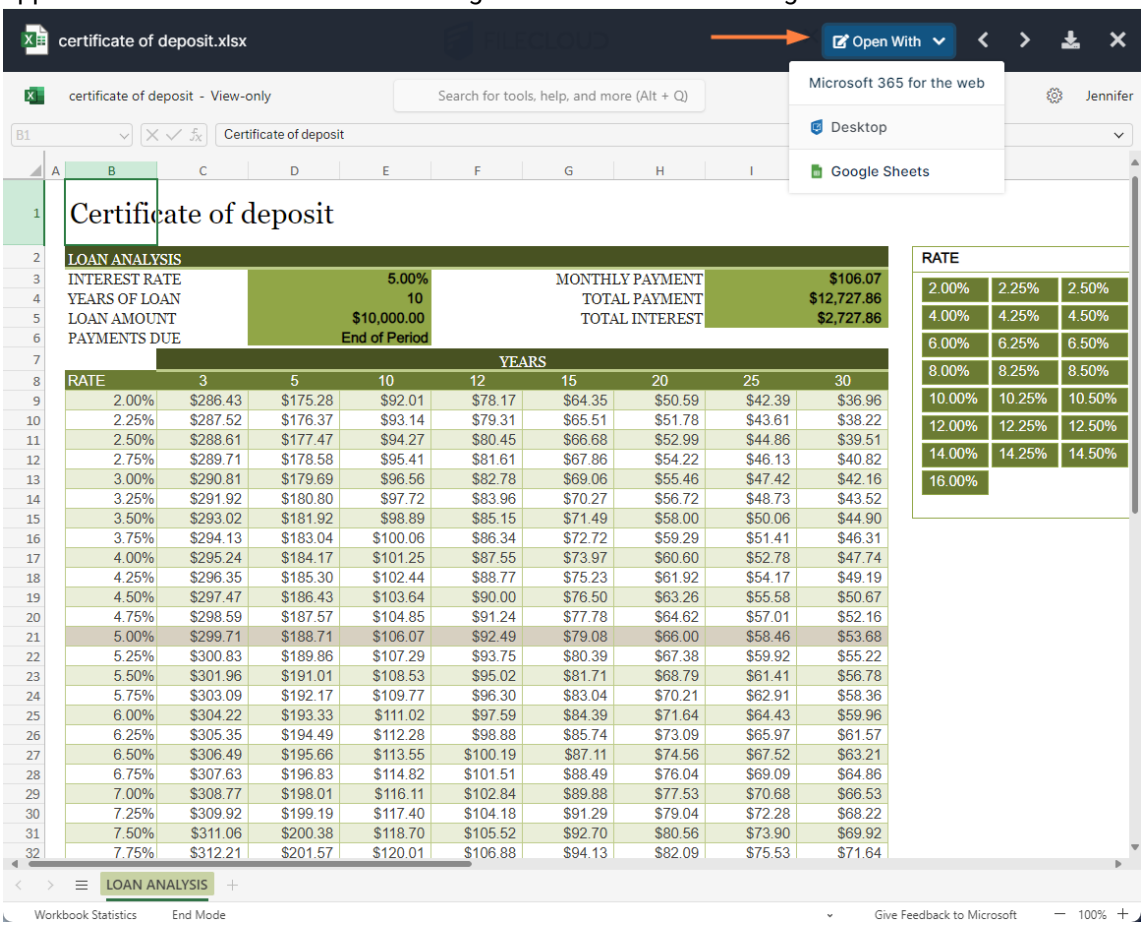
As an administrator, you can provide preview tools to your users so that they can quickly view a portion of a document to determine if it is the one they need to work with.

1. After selecting a file in the user portal, a Preview button is available.



2. After clicking the Preview button, a separate window opens showing an image of the file.

   The preview can be edited with the same Web edit/Office Online and Edit in Desktop applications that are available for editing the file from the file listing.



There are a few different ways an administrator can provide preview tools in FileCloud:

- Quick JS Preview
- DocConverter with LibreOffice
- WOPI - Web Application Open Platform Interface Protocol (supports online web editing features)

- Integration with AutoDesk Viewer (FileCloud version 22.1 and later) for previewing AutoCAD files only. See Setting Up AutoCAD File Preview with Autodesk Viewer for instructions.

What is DocConverter?

FileCloud uses a Java-based service called FileCloud Document Converter to:

- Enable thumbs for Microsoft Office files (DOC, DOCX, PPT, PPTX, XSL, XSLX)
- Enable thumbs for Apple iSuite files (.pages, .numbers, .key)
- Enable thumbs for Adobe documents (AI, PDF, PSD)
- Enable thumbs for TIFF images
- Interface with LibreOffice for document preview generation

For this FileCloud uses a java program based on Apache's PDFBox. Document converter also will use LibreOffice libraries to convert documents to PDF.

1. Start the DocConverter service and configure it with FileCloud.

Linux: LibreOffice Ubuntu/RHEL Instructions

Windows: LibreOffice Windows Instructions

2. Enable thumbnail images on the Admin Portal.



Enable Document Thumbs

What Other Online Web Editing Features Are Available?

Administrators can configure online editing to allow FileCloud users to select any supported document and edit the document from within the User Portal.

- FileCloud uses the WOPI (Web Application Open Platform Interface) protocol to support online web editing

To use WOPI, you must install or have already available one of the following to provide the web editing capability:

- Microsoft Office Online
- Collabora Code



Manage Online Web Editing

You can choose which tool to use not only by the version of FileCloud you are using, but also by the functionality.

Tool	File Types Previewed	Preview Keys	Interactions with Other Tools/Other Notes
Quick JS Preview	• AI • DICOM • HEIC • PDF • PSD • Microsoft - DOCX, PPTX, XLSX • audio: MP3, OGG, WAV, M4A • video: MP4, WebM, MOV	None	• If DocConverter is also in use, then previews can also be shown by using the SHIFT + Preview keys for a DocConverter view • If WOPI is also in use, then WOPI will override QuickJS functionality • Both QuickJS and DocConverter must be in use to enable users to preview Office files. See LibreOffice Windows Instructions.
DocConverter with LibreOffice	• AI • DICOM • ODG (Oasis graphic files) • ODS (Oasis spreadsheets) • ODT (OpenDocument text created by LibreOffice and others) • PDF • TXT • Apple iWork Suite - .pages, .numbers, .key • Microsoft - DOC, DOCX, PPT, PPTX, XLS, XLSX • audio: MP3, OGG, WAV, M4A • video: MP4, WebM, MOV	SHIFT + Preview	• If Quick JS is also in use, then previews can also be shown without using any preview keys • If WOPI is also in use, then WOPI will override DocConverter functionality • Currently, .numbers file previews appear with table gridlines and numbers only. Additional table formatting does not appear in the previews.

Tool	File Types Previewed	Previe w Keys	Interactions with Other Tools/Other Notes
WOPI	• Microsoft - DOC, DOCX, PPT, PPTX, XLS, XLSX • audio: MP3, OGG, WAV, M4A • video: MP4, WebM, MOV	None	• WOPI will override any Quick JS or DocConverter functionality • To preview a file using WOPI, the user must have download permission to the file.

💡 To configure document preview, click on a method to see the steps:

Configure Quick JS Preview

PREREQUISITES for Quick JS Previews:

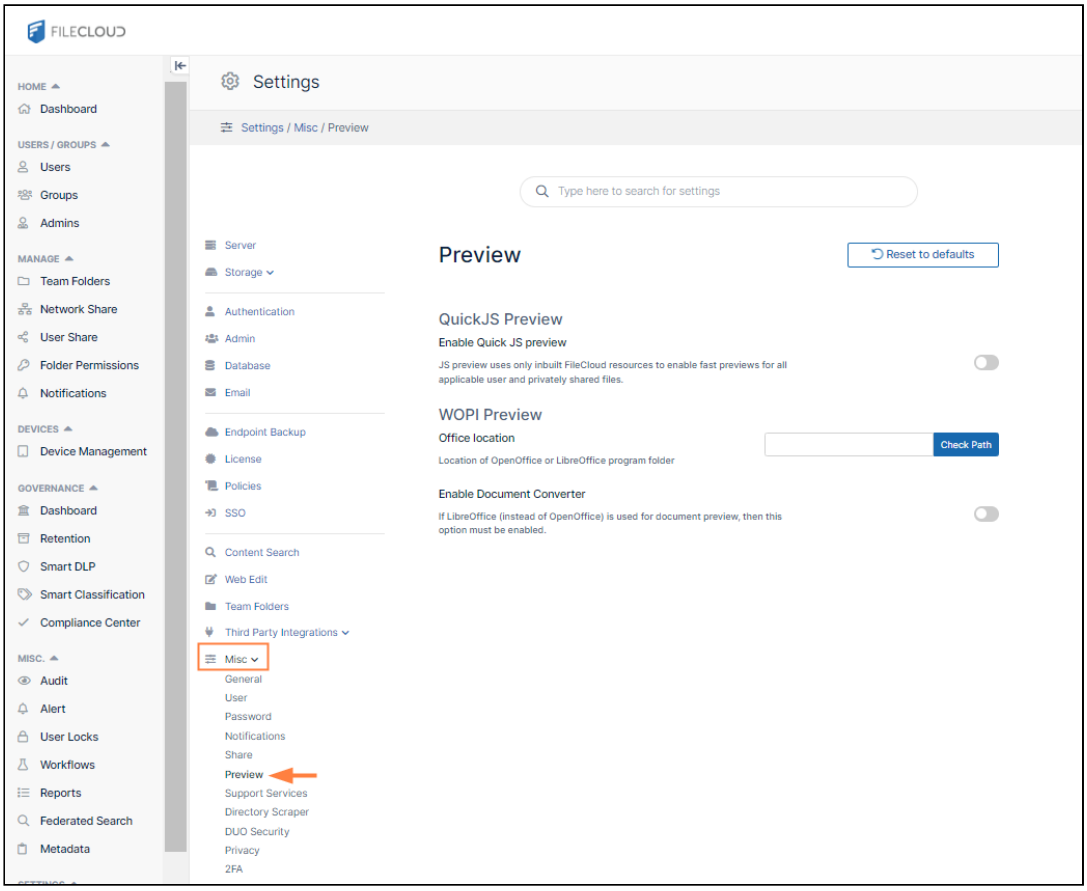
1. You must be running FileCloud version 19.1 and later.
2. You must stop the Document Converter service according to the OS you are using.
   a. For Windows, open the FileCloud Control Panel and stop the DocConverter Service if it is running.
   b. For Linux, run the following command:

```
# sudo service fcdocconverter stop
```

To enable preview using Quick JS:

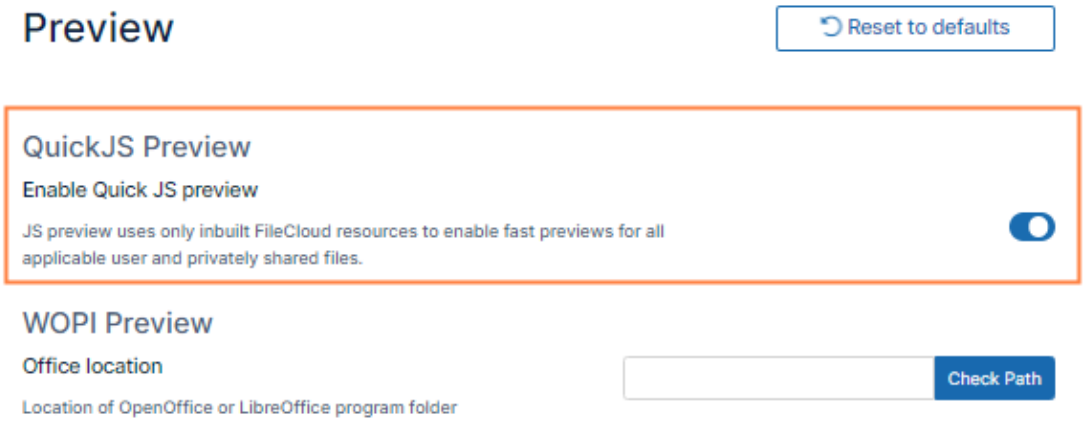
1. Open the Preview settings page.
   To open the Preview settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.



The **Preview** settings page opens.

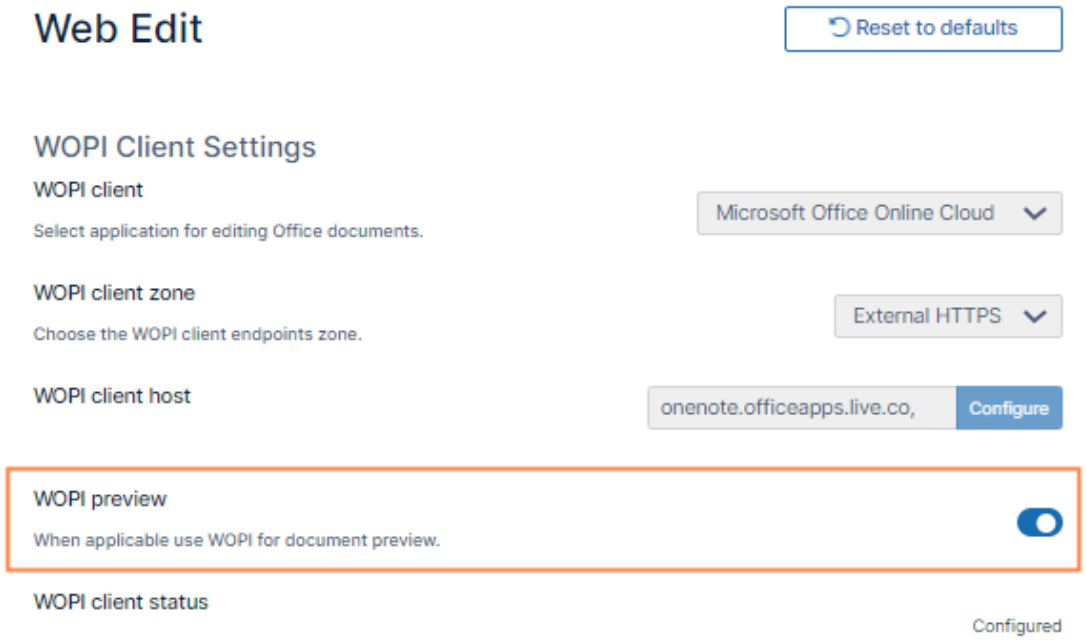
2. On the **Preview** screen, enable the field **Enable Quick JS preview**.



Configure Preview using WOPI

Administrators can configure online previewing using WOPI for any supported document from within the User Portal.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click **Web Edit** .
   The Web Edit settings page opens.
2. Configure online editing using WOPI. See Microsoft Office Online Cloud For Web Edit.
3. During your configuration, check **WOPI Preview**.



To include watermarks on previewed documents, see Watermark Settings.

Setting up Document Preview for large file size

To enable this option, open cloudconfig.php at

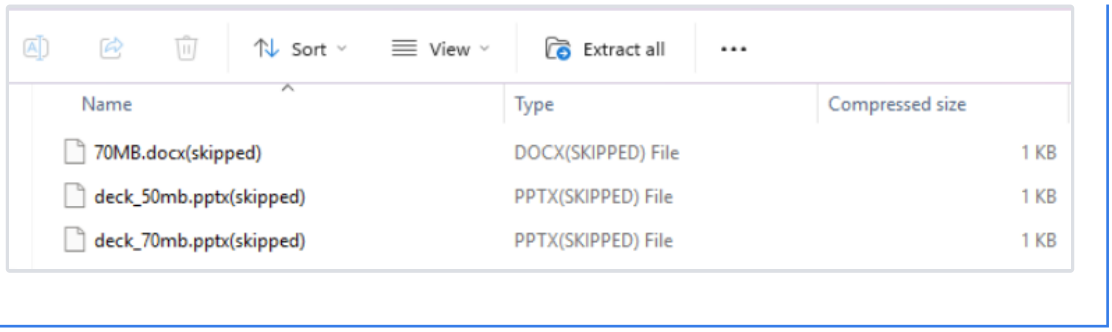
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php

Linux Location: /var/www/config/cloudconfig.php

and add the following

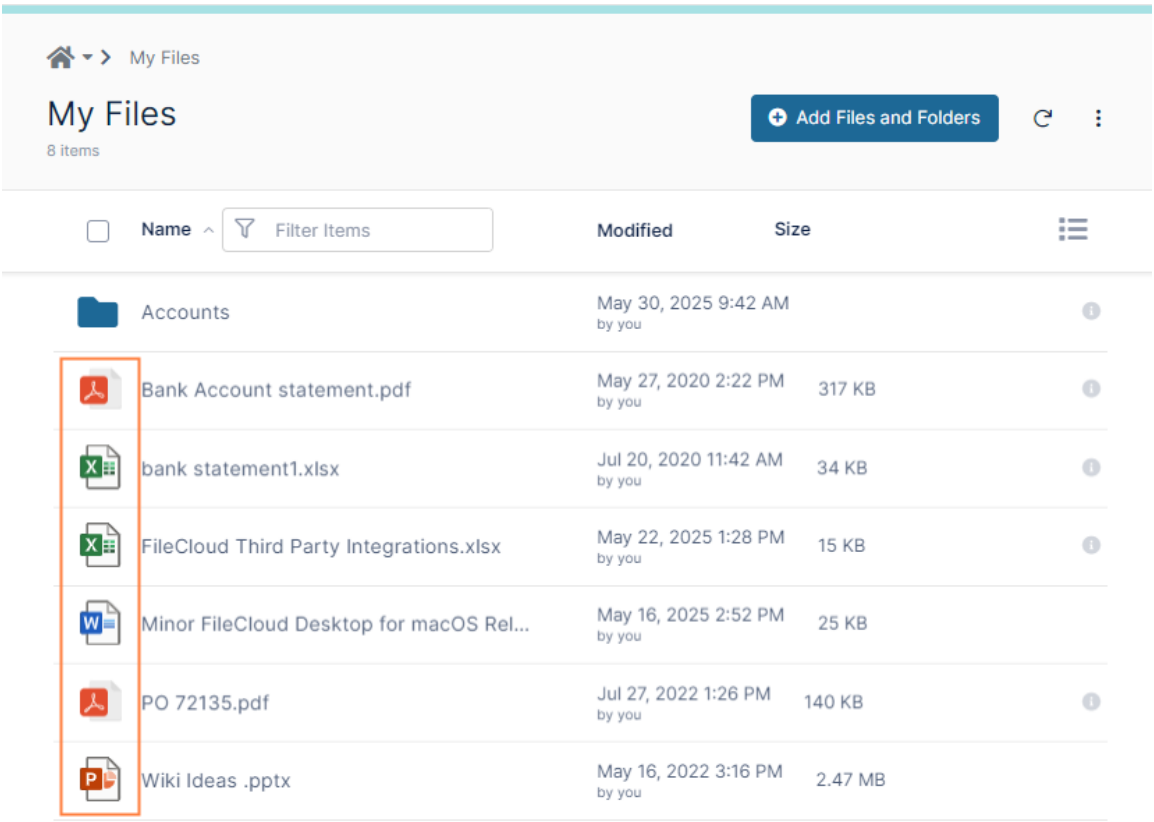
```
define("TONIDOCLOUD_DOCPREVIEW_SIZELIMIT", "20485760"); //20MB
```

When watermarks are enabled for previews, Office files larger than TONIDOCLOUD_DOCPREVIEW_SIZELIMIT are listed but not downloaded in the Zip file containing the previewed files and **skipped** appears beside them:



FileCloud Document Converter

Administrators can use a Java-based service called FileCloud Document Converter to provide thumbnail images.



For this FileCloud uses a java program based on Apache's PDFBox.

Document converter also uses LibreOffice libraries to convert documents to PDF.

Document converter:

- Enables thumbs for all Microsoft Office documents (DOC, DOCX, PPT, PPTX, XSL, XSLX)

- Enable thumbs for Apple iSuite files (.pages, .numbers, .key)
  Note: Thumbs for Apple iSuite use corresponding Office icons.
- Enables thumbs for Adobe documents (AI, PDF, PSD)
- Enables thumbs for TIFF images
- Interfaces with LibreOffice for document preview generation

Configure Document Converter

For Windows

⚠ Document Converter for Windows is automatically installed and ready to enable in the admin portal.

See LibreOffice Windows Instructions and Installing and Running Document Converter for Windows

Install and Upgrade Document Converter for Linux

You can use a Java-based service called FileCloud Document Converter to provide thumbnail images for file listing. Install Document Converter on the same server as FileCloud.

- FileCloud requires LibreOffice to install and run Document Converter. If you are not sure if you have installed the latest version of LibreOffice that FileCloud is using, enter the following command, which checks the LibreOffice version and upgrades it if necessary:

  ```
  filecloudcp --libreoffice-check
  ```

  To install and configure LibreOffice for Linux, see LibreOffice Ubuntu/RHEL Instructions.
- To install Document Converter, enter the command:

  ```
  filecloudcp --install-preview
  ```

- To upgrade Document Converter, use the install command, above.

To start the Document Converter service and configure it with FileCloud, go to Enabling Document Converter and Thumbs

Adding Security to FileCloud Document Converter

To make the Document Converter more secure when converting certain types of files

First configure Document Converter to use a security key:

1. Create an ini file under /opt/fcddocconverter (Linux) or C:/XAMPP (Windows) with the name fcdocconverter.ini

2. Enter the following line into the file and save it:
   FCDOCCONVERTER_SECURITY_KEY=hello#$%world
3. Start the Document Converter service. See LibreOffice for help.
4. Look into converter logs and make sure it starts in secure mode
   Look for a log line that reads: "Found a security key in the ini. Will be check this key for all requests."

Then configure FileCloud to send the security key with every request to Document Converter:

1. Configuring FileCloud to send security key with every request to FC Docconverter
   a. Edit the file WWWROOT/config/cloudconfig.php and add the following definition line:
   define('TONIDOCLOUD_FCDOCCONVERTER_SECURITY_KEY','hello#$%world');

Installing and Running Document Converter for Windows

FileCloud Document Converter is a Java-based service that allows users to see thumbnail images for a file.

- Document Converter requires the correct Java Development Kit (JDK).

⚠ FileCloud now fully supports OpenJDK 17 instead of Oracle Java.

To install and run Document Converter for Windows:

1. Install OpenJDK for Windows.
2. Start Document Preview from the FileCloud control panel.

To run Document Converter on a different port from 8080, see Running FCDocConverter on different port from 8080.

Install OpenJDK for Windows

FileCloud now fully supports OpenJDK 17 or higher instead of Oracle Java.

- Java Development Kit (JDK) consists of the Java Runtime Environment (JRE) along with tools to compile and debug Java code for developing Java applications.
- OpenJDK is an open source implementation of the Java Standard Edition platform with contributions from Oracle and the open Java community.
- OpenJDK is the official reference implementation for Java Standard Edition from Java SE 7.
- OpenJDK is released under license GPL v2 wherein Oracle JDK is licensed under Oracle Binary Code License Agreement.
- Oracle JDK's build process builds from OpenJDK source code.

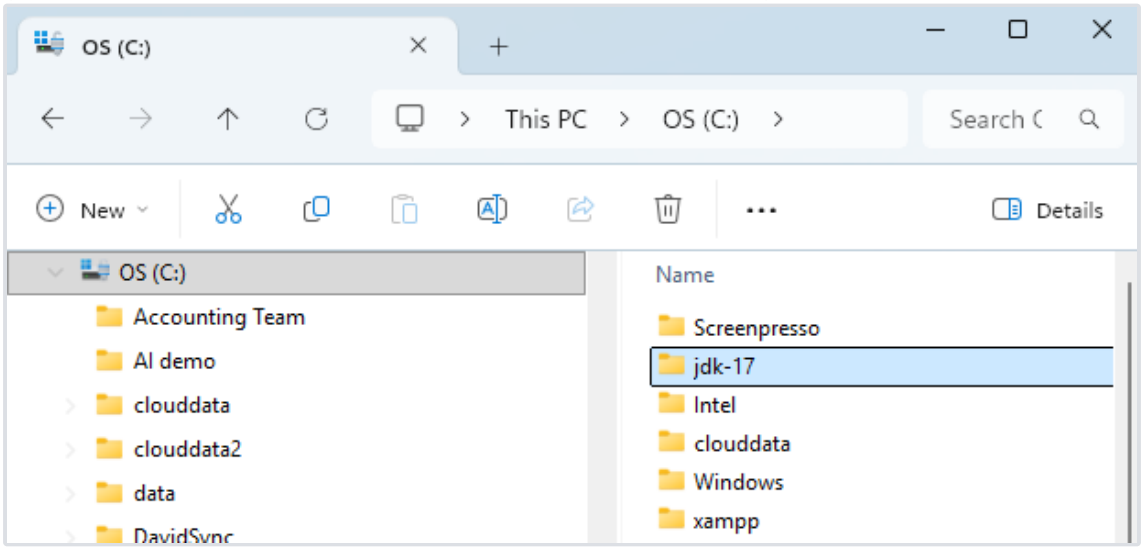
💡If you already have OpenJDK 17 or higher installed, you can skip the following steps.

To install OpenJDK for Windows:

1. Install OpenJDK.

To install OpenJDK:

1. Download **Open JDK 17** from https://jdk.java.net/archive/ .
2. Create a new folder in the C: drive.
   (In the example screenshot, jdk-17 is the name of the new folder.)



3. Extract the Open JDK file you downloaded into the new folder.

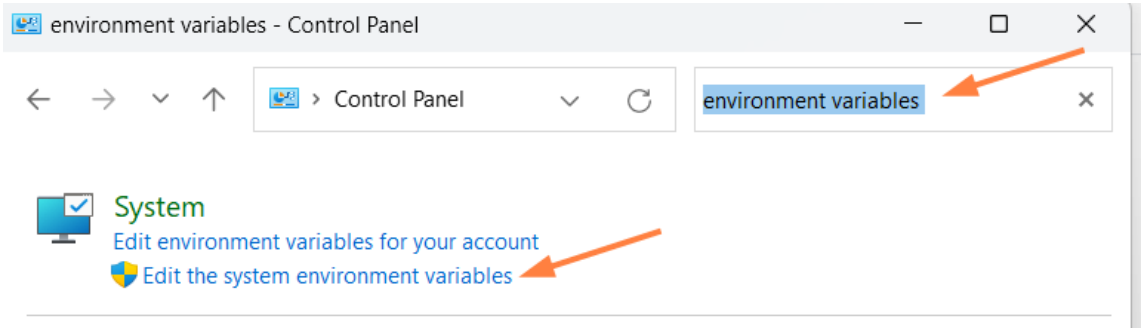
2. Set the JAVA_HOME path and add the bin path

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

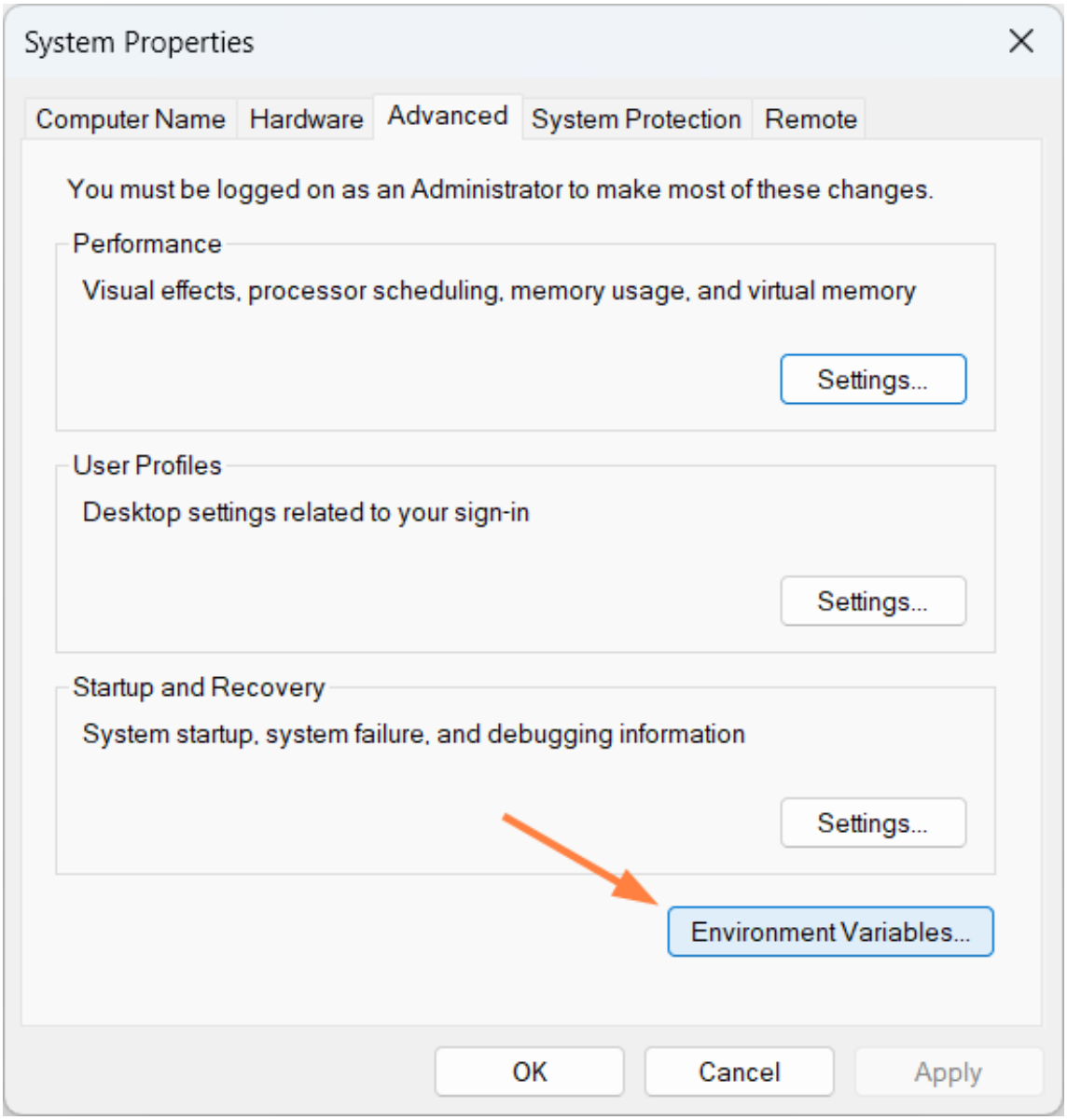
⚠ Administrator privileges are required to modify the path and environment variables.

To set the JAVA_Home path and add the bin path:

1. Open the Windows Control Panel.
2. Enter **environment variables** in the search bar.
3. Click **Edit the system environment variables.**

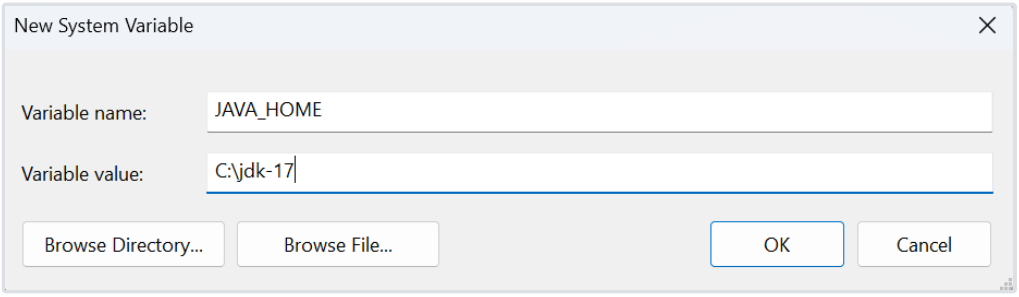


4. In the **System Properties** dialog box, click **Environment Variables.**



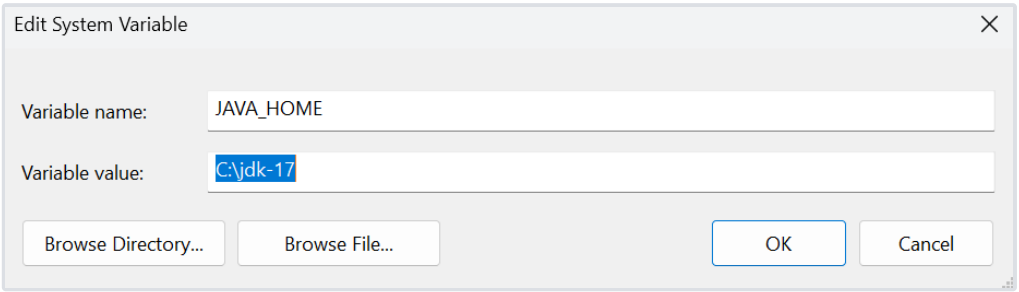
The **Environment Variables** dialog box opens.

5. Edit or create the **JAVA_HOME** variable and set it to your jdk folder address.
   - If you do not see the **JAVA_HOME** variable listed under **System variables**:
     i. Below the **System variables** window, click **New**.
     ii. In the **New System Variable** dialog box:
     iii. In **Variable name** enter **JAVA_HOME**.
     iv. In **Variable value**, enter the address of the folder you created for jdk.

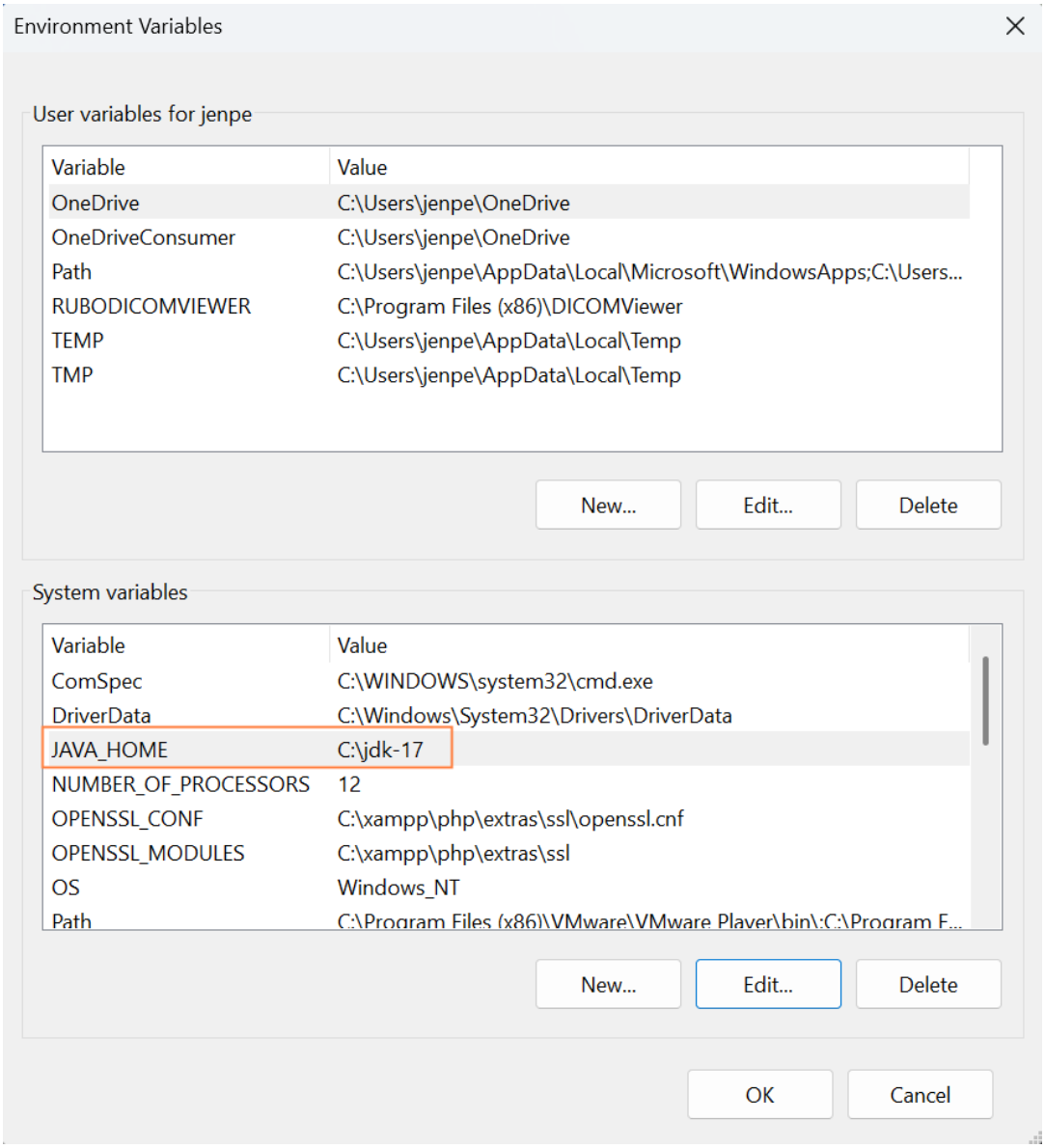


v. Click **OK**.

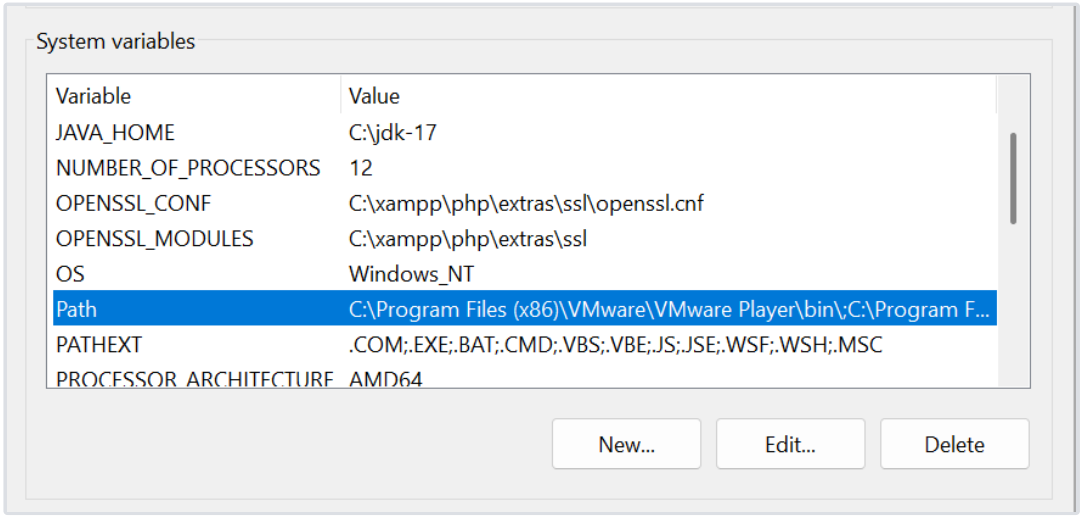
- If you see the **JAVA_HOME** variable listed under **System variables**:
  i. In the **System variables** box, click **JAVA_HOME**, and then click **Edit**.
  The **Edit System Variable** dialog box opens.
  ii. Change **Variable value** to the address of the folder you created for jdk, and click **OK**.



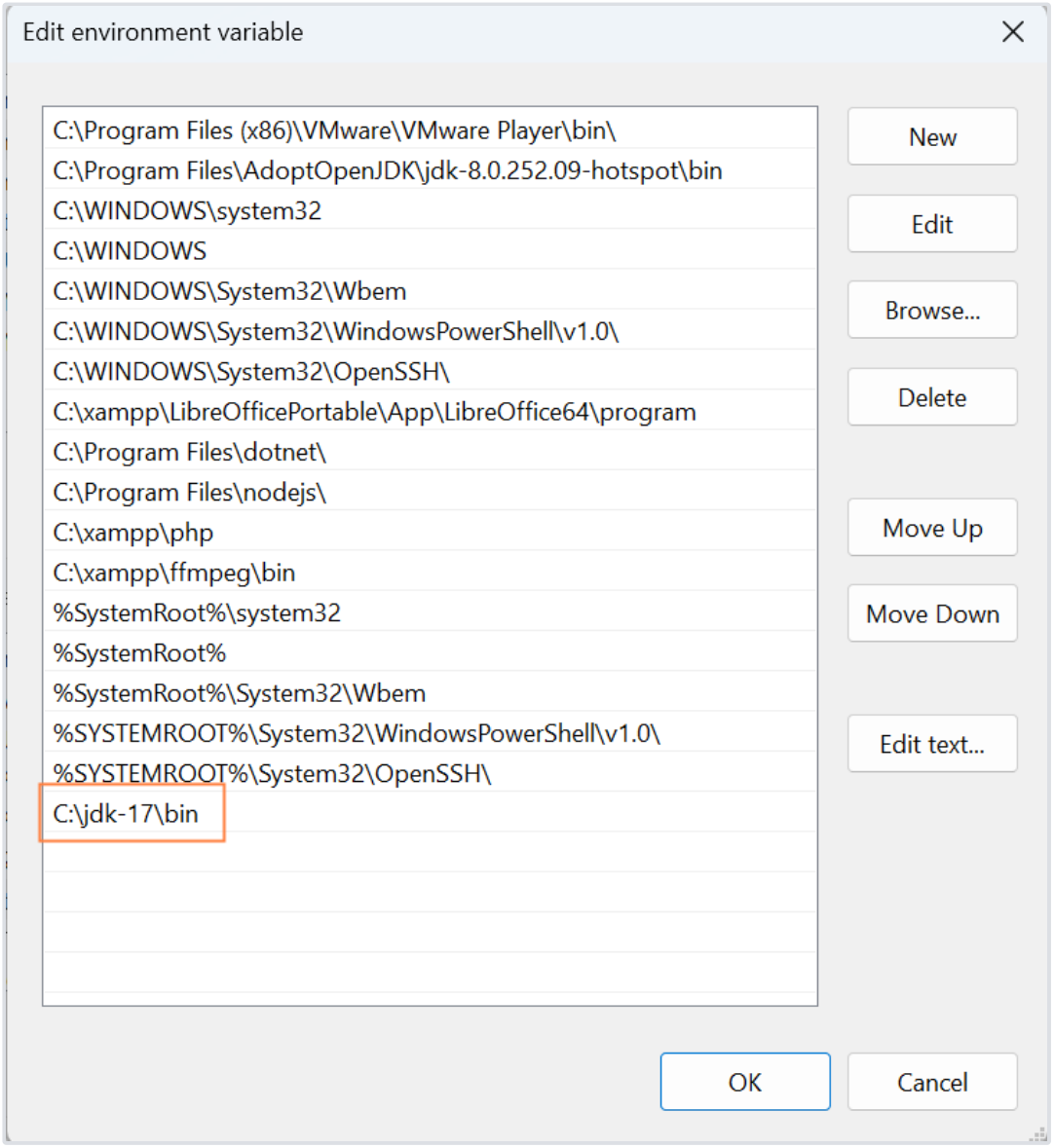
- If the value appears correctly in the **Environment Variables** dialog box, click **OK**.



6. Now add the bin path to the **Path** variable.
    - Click and edit the **Path** variable which also appears in System variables:



- In the Edit environment variable dialog box, add the OpenJDK bin path. It is the JAVA_HOME path with **\bin** appended to the end, for example:
  C:\jdk-17\bin

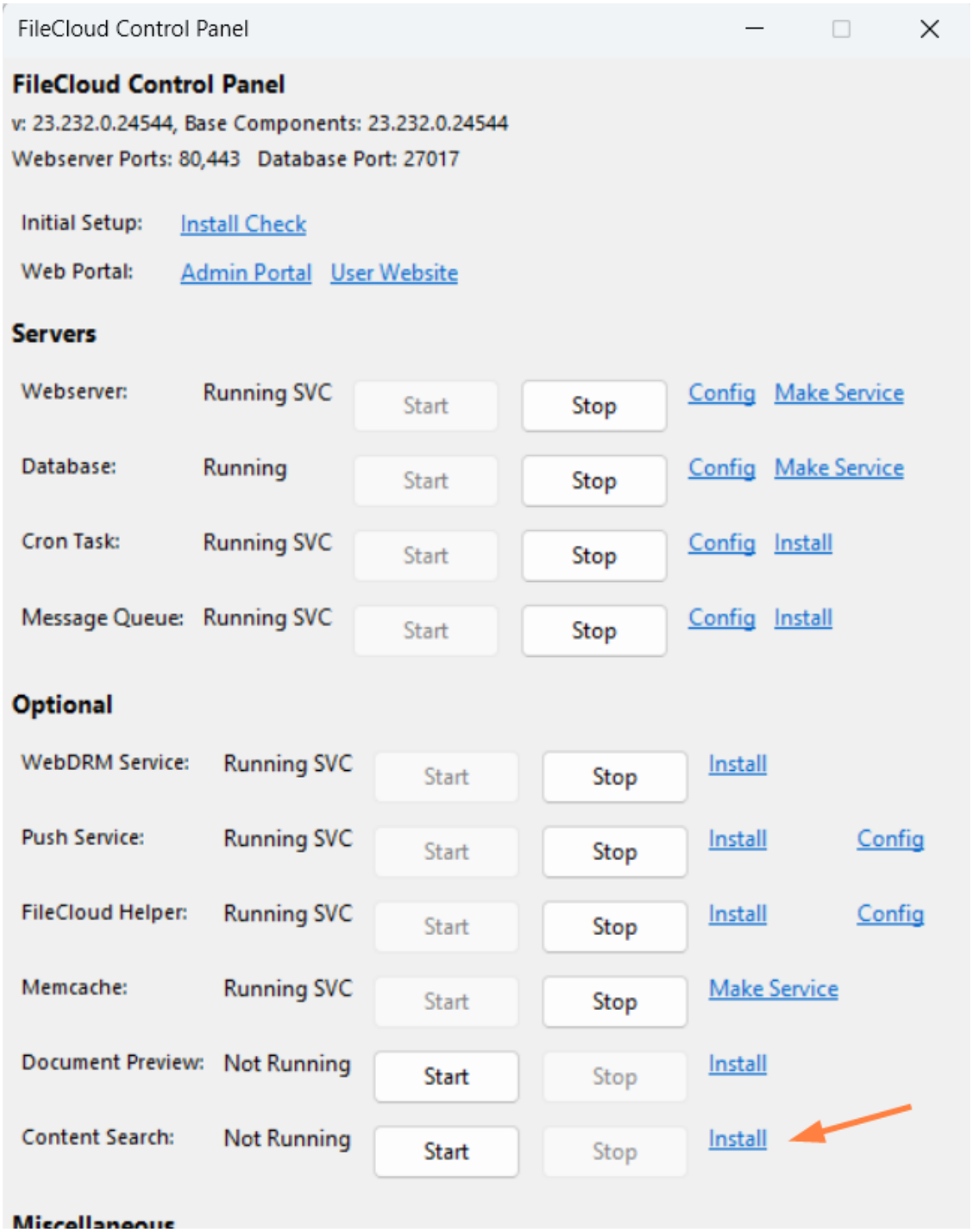


- Click **OK** in each dialog box until you exit the Windows Control Panel.

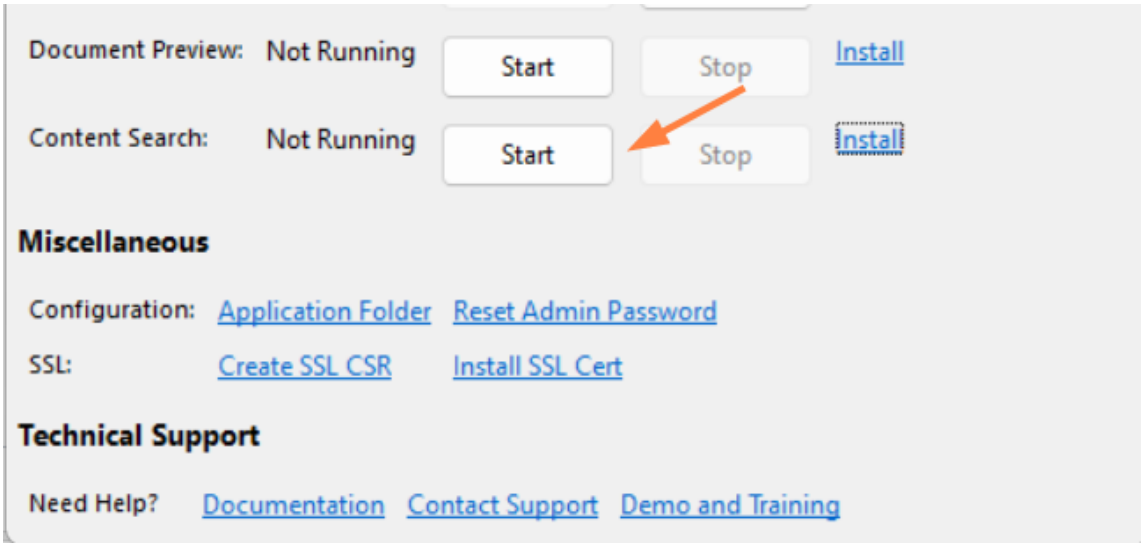
3. Use the FileCloud Control Panel to install Content Search

To install and start Content Search:

1. Open the FileCloud Control Panel.
2. Next to **Content Search**, click **Install**.



3. To start the **Content Search** service, click the **Start** button.



Running FCDocConverter on different port from 8080

FCDocConverter service uses port 8080 by default.

In some cases, this port may be in use by a different application in your server. If that is the case, you can change the port the service uses.

Change the default port in the service in Windows

Change the default port in the service

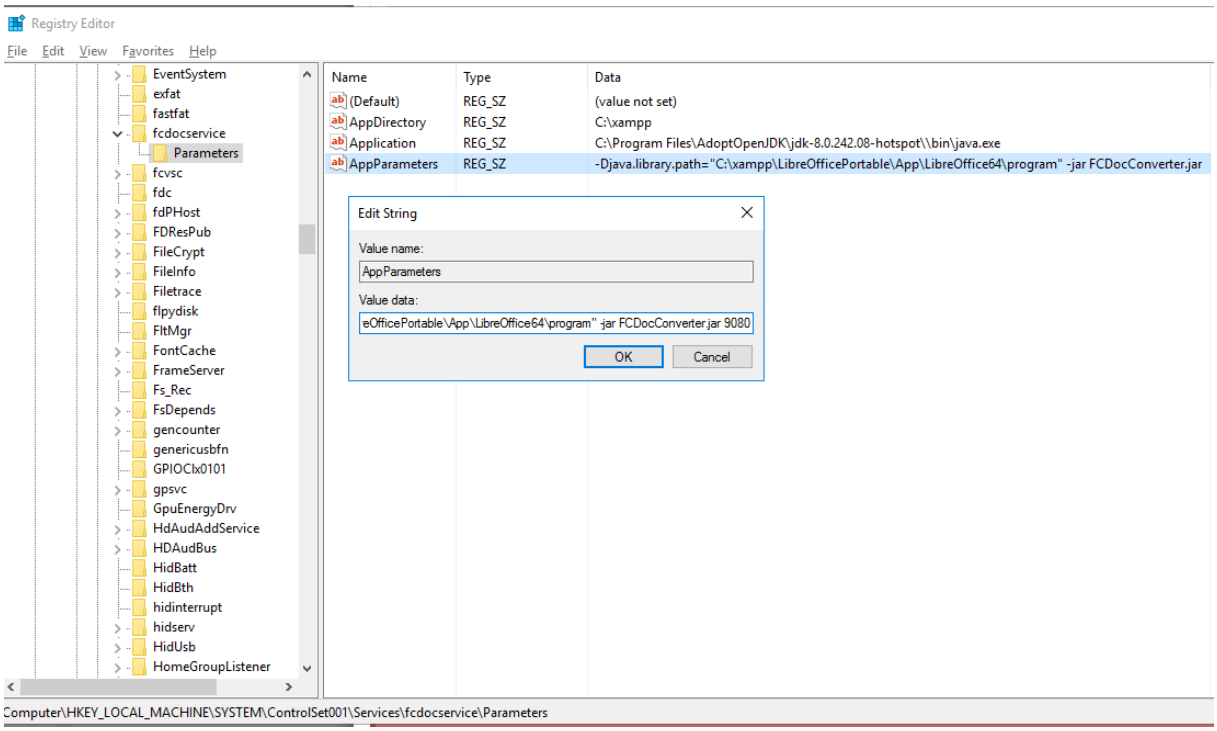
To change the default port on the service, you need to change the execute command string.

In Windows, you can do this by changing the Registry Entry at:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\fcdocservice

```
"-Djava.library.path="C:\xampp\LibreOfficePortable\App\LibreOffice64\program" -jar
FCDocConverter.jar 9080"
```

It will look like this:



Restart the Windows service from the FileCloud control panel to make this change effective.

Change the port that FileCloud uses for Docconverter

Open the FileCloud config file (cloudconfig.php) typically located at C:\xampp\htdocs\config

Go to the end of the file, and add the following entry (in case the parameter already exists, only change the port number):

```
define("TONIDOCLOUD_FCDOCCONVERTER_URL", "http://127.0.0.1:9080");
```

Now, all preview requests will go to the new URL/port.

Changing the IP address for Docconverter

In case 127.0.0.1 can't be used, you can change this in the registry and the config file.
⚠ Exposing the docconverter service to the network, as shown here, is not advised, and will introduce security risks.

The IP address can be added at the end:

```
java -Djava.library.path="D:\xampp\LibreOfficePortable\App\LibreOffice64\program" -jar
FCDocConverter.jar 9080 192.168.1.108
```

You can make this change and restart the service.

Then, you can change the config file to have this URL/IP address used:

```
define("TONIDOCLOUD_FCDOCCONVERTER_URL", "http://192.168.1.108:9080");
```

Change the default port in the service in Linux

Change the default port in the service

To change the default port on the service, you need to change the execute command string.

In Linux:

1. Go to **/etc/systemd/system/fcdocconverter.service** and open **fcdocconverter.service** for edit.
2. Find the line:

   ```
   ExecStart=/bin/sh -c '/usr/bin/env  HOME=/var/www/html  java
   -Djava.library.path="/usr/lib/libreoffice/program/" -jar /opt/app/fcdocconverter/
   FCDocConverter.jar'
   ```

   and add the value of the port at the end of the line:

   ```
   ExecStart=/bin/sh -c '/usr/bin/env  HOME=/var/www/html  java
   -Djava.library.path="/usr/lib/libreoffice/program/" -jar /opt/app/fcdocconverter/
   FCDocConverter.jar 9080'
   ```

3. Save your changes.
4. Execute the following four commands, one after the other:

   ```
   > systemctl stop fcdocconverter.service
   ```

```
> systemctl daemon-reload
```

```
> systemctl start fcdocconverter.service
```

```
> systemctl status fcdocconverter.service
```

5. Test if the port is listening by executing the following command:

```
> netstat -nltp | grep -i 9080
```

Enabling Document Converter and Thumbs

Administrators can enable thumbs for all office documents (DOC, DOCX, PDF, PPT, PPTX etc.,).

A thumb, also known as a thumbnail file, contains a small JPEG icon representing the application that created the document or the document type.

To display thumbnails, FileCloud uses a document converter server.

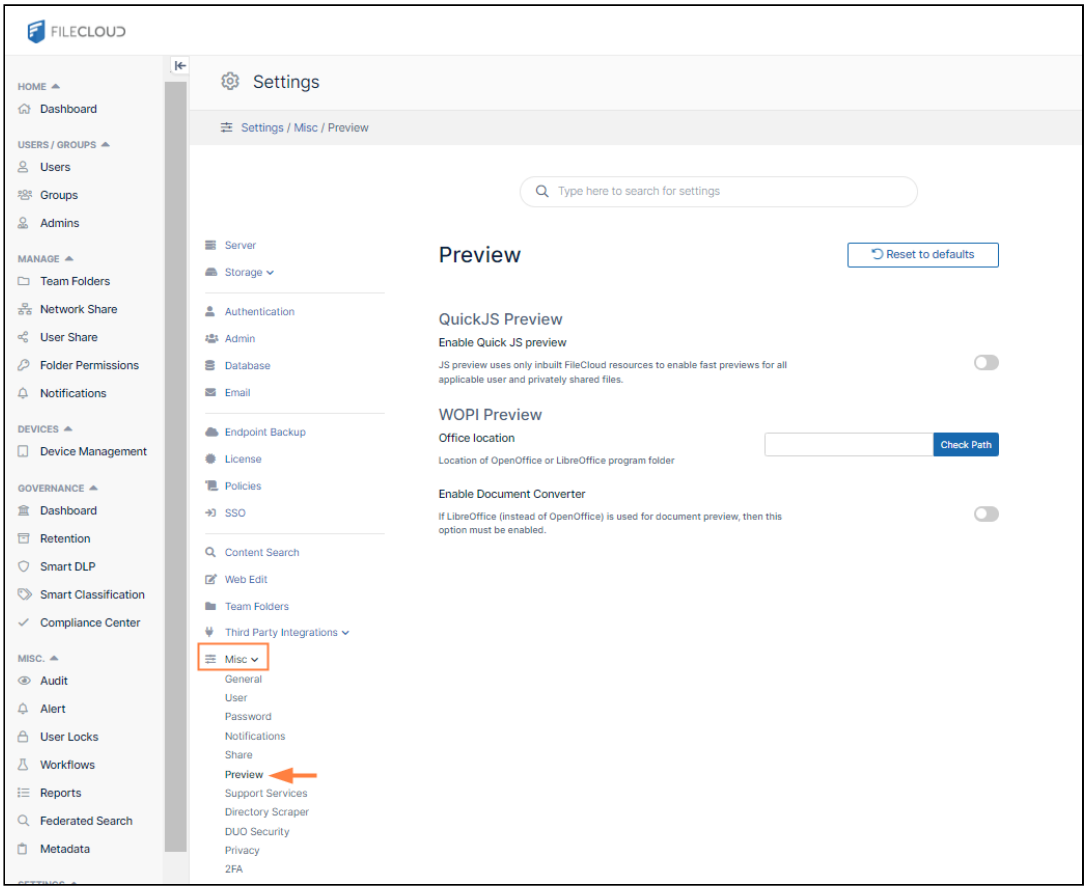
Before enabling the use of thumbnails you must:
Install and Run FileCloud Document Converter

Note: FileCloud always displays thumbs for graphic files (jpg, png, ...) regardless of this setting.

To enable thumbnails for a document in FileCloud:

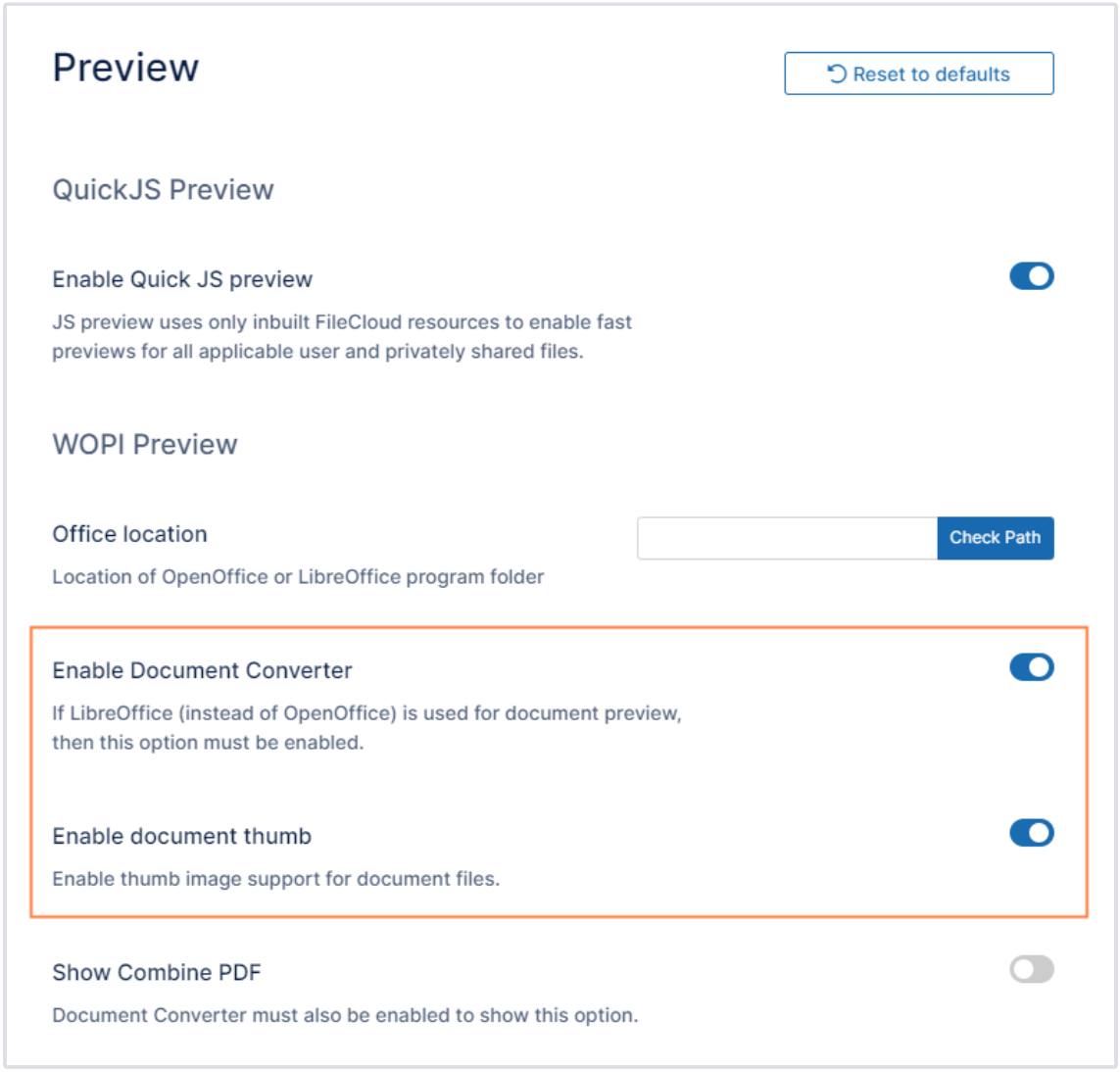
1. Open the Preview settings page.
   To open the Preview settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.

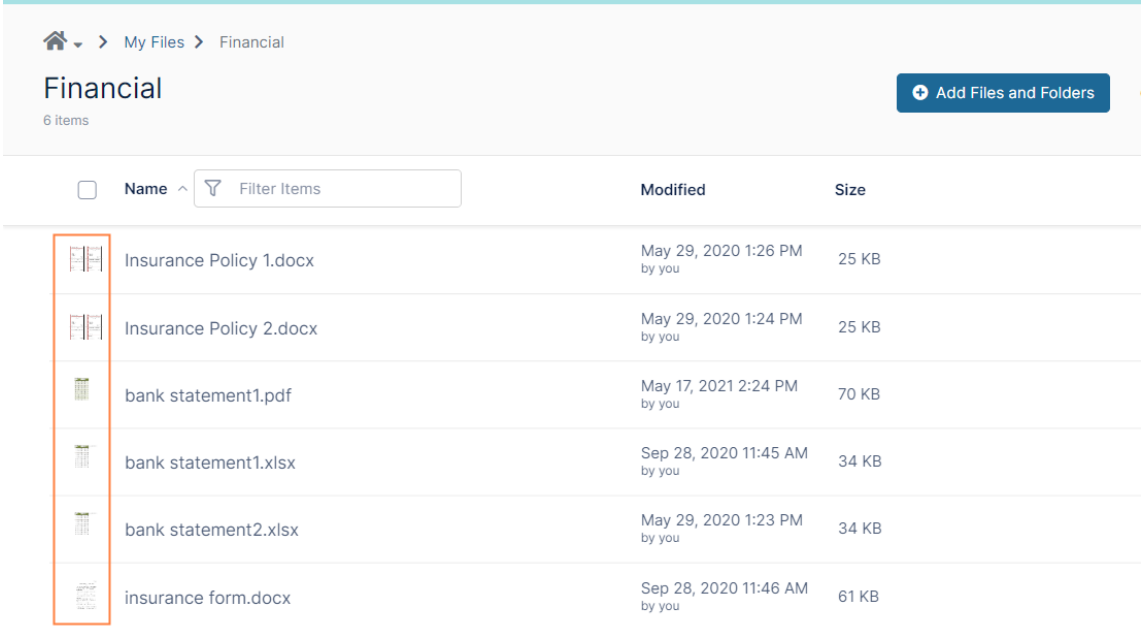


The **Preview** settings page opens.

2. Activate **Enable Document Converter**. Additional fields appear.
3. Activate **Enable document thumb**.


Preview
Reset to defaults
QuickJS Preview
Enable Quick JS preview
JS preview uses only inbuilt FileCloud resources to enable fast previews for all applicable user and privately shared files.
WOPI Preview
Office location
Check Path
Location of OpenOffice or LibreOffice program folder
Enable Document Converter
If LibreOffice (instead of OpenOffice) is used for document preview, then this option must be enabled.
Enable document thumb
Enable thumb image support for document files.
Show Combine PDF
Document Converter must also be enabled to show this option.

Now when a user logs on to the user portal, the file listing will show the thumbnail:



Overriding Thumb and Preview Size Limits

By default, the size limit for for files used for thumbnails and document previews is 10MB for most files and 100MB for some image file types (.jpg, .png, .gif) . Files larger than the specified limits appear as broken images when displayed as thumbnails and fail to be generated as previews.

You can override the limits by customizing them in your cloudconfig file.

> When PDF, text and Office files are previewed in FileCloud, they are actually downloaded and opened, and therefore, are not subject to the 10MB limit for thumbnails and previews.

To customize the size limit for files other than .jpg, .png, and .gif:

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_DOCUMENT_THUMB_SIZE_MB', 10);
```

3. Change 10 to the custom size limit in MB.

To customize the size limit for images:

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_IMAGE_THUMB_SIZE_MB', 100);
```

3. Change 100 to the custom size limit in MB.

   Additionally, increase your system's memory limit depending on the size of the files you are uploading.
4. Open .htaccess:
   Windows Location: XAMPP DIRECTORY/htdocs/.htaccess
   Linux Location: /var/www/.htaccess
5. Find the following setting:

```
php_value memory_limit 500M
```

6. Increase the value for memory_limit.

LibreOffice

The necessary conversion for office documents to make it previewable in a browser can also be done with LibreOffice. Check below for installation and configuration of LibreOffice in different operating systems.

LibreOffice Windows Instructions

FileCloud supports LibreOffice for document preview generation. Use the following instructions to enable file preview using LibreOffice.

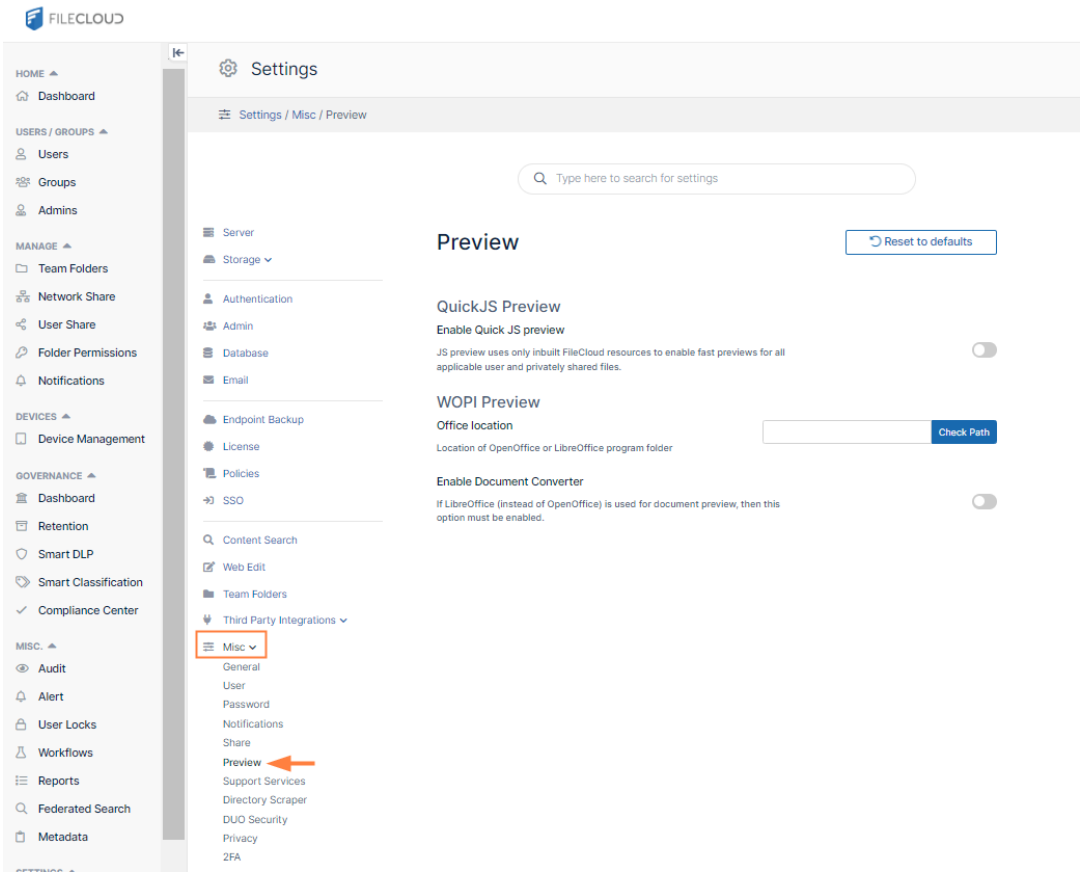
1. Install FileCloud Document Converter
   FileCloud needs document converter to work with LibreOffice. Follow the instructions from this section to install and run FileCloud document converter.
2. Enable preview in FileCloud.

Multisite

If you are running a multi-site configuration, please follow these steps on the root site.

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

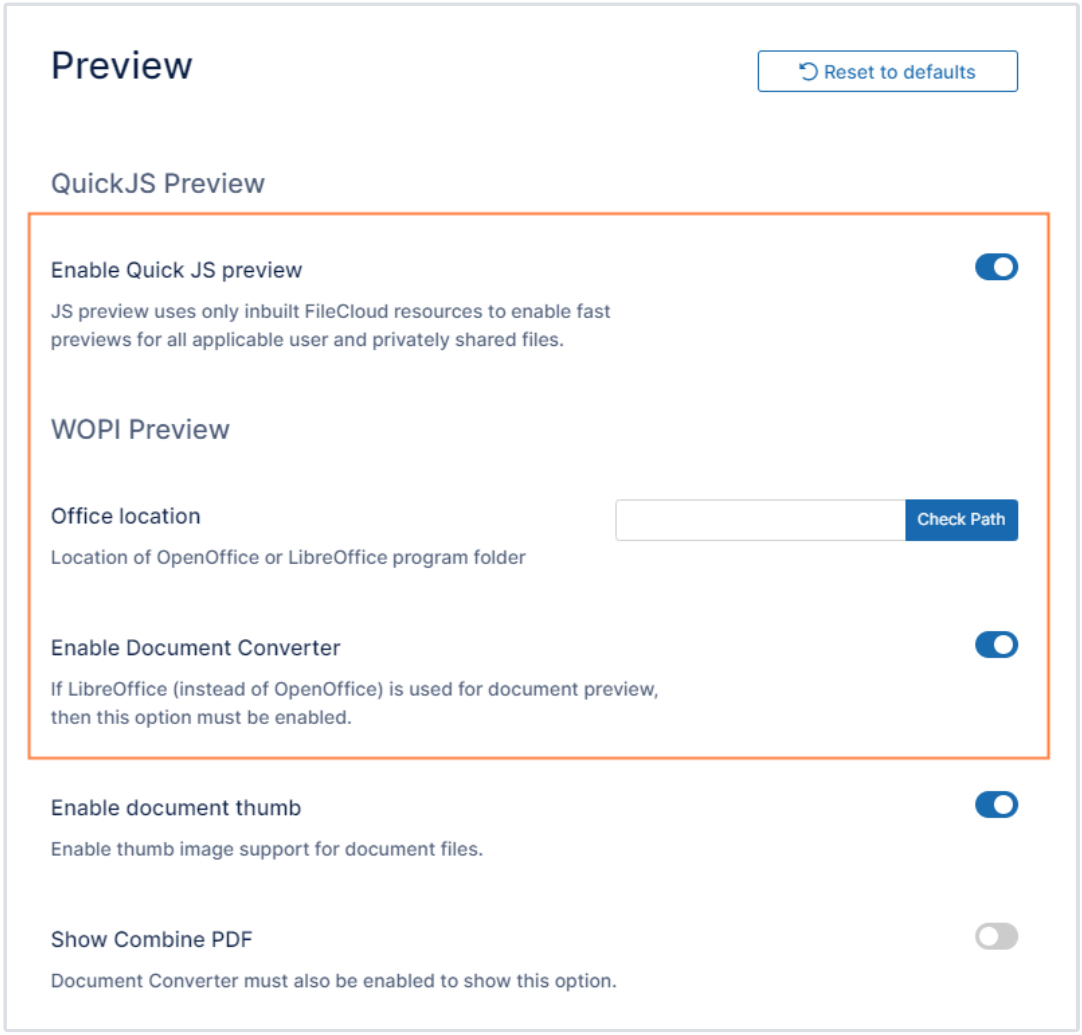
b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.



c. Enable **Quick JS Preview** if it is not already enabled.

d. In **Office location**, enter the correct path for LibreOffice (**C:\xampp\LibreOfficePortable\App\LibreOffice64\program**).

e. Enable the field **Enable Document Converter**. **Note**: Enabling this is allowed only when LibreOffice is used for document preview.



LibreOffice Ubuntu/RHEL Instructions

Installing LibreOffice

You can install LibreOffice on Ubuntu/RHEL during installation.

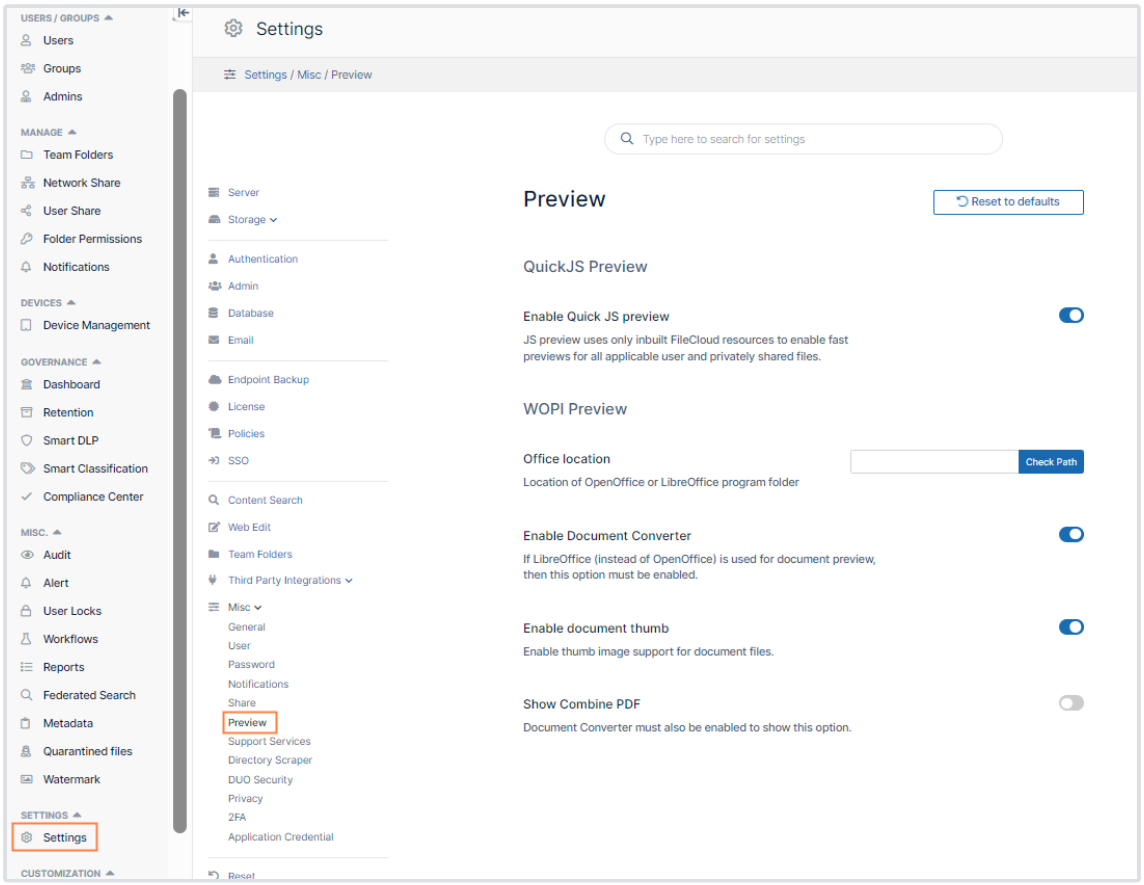
To install it later, enter the filecloudcp command:

```
root@localhost:~# filecloudcp --install-preview
```

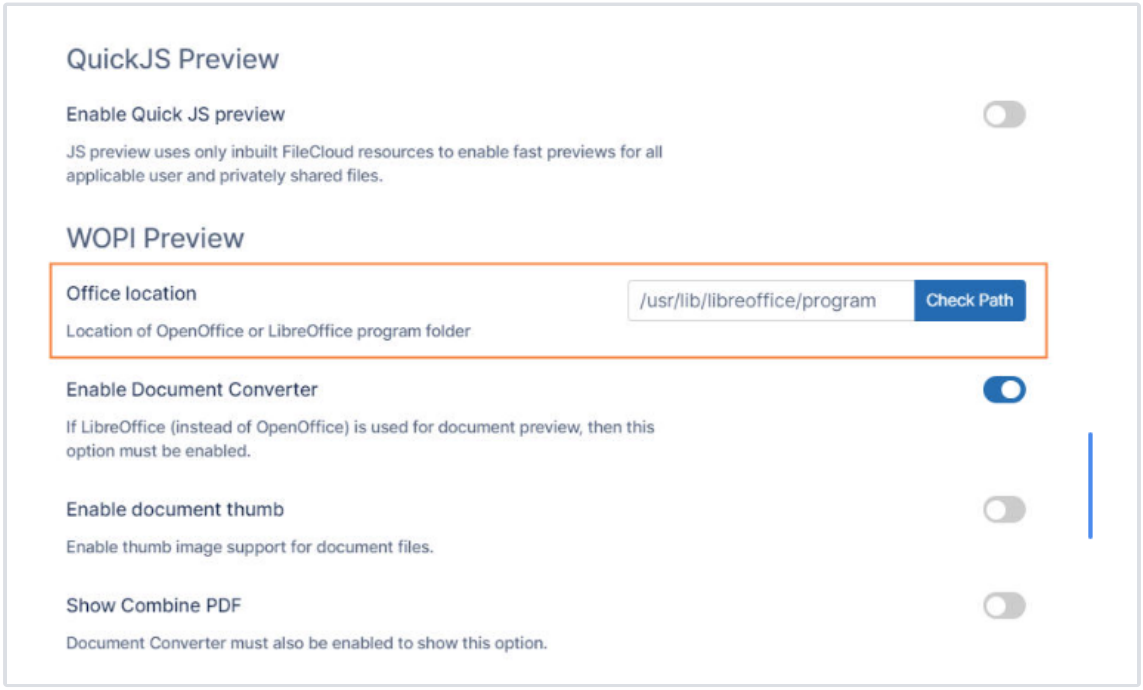
Configure FileCloud with LibreOffice

Follow these steps to enable document preview in FileCloud.

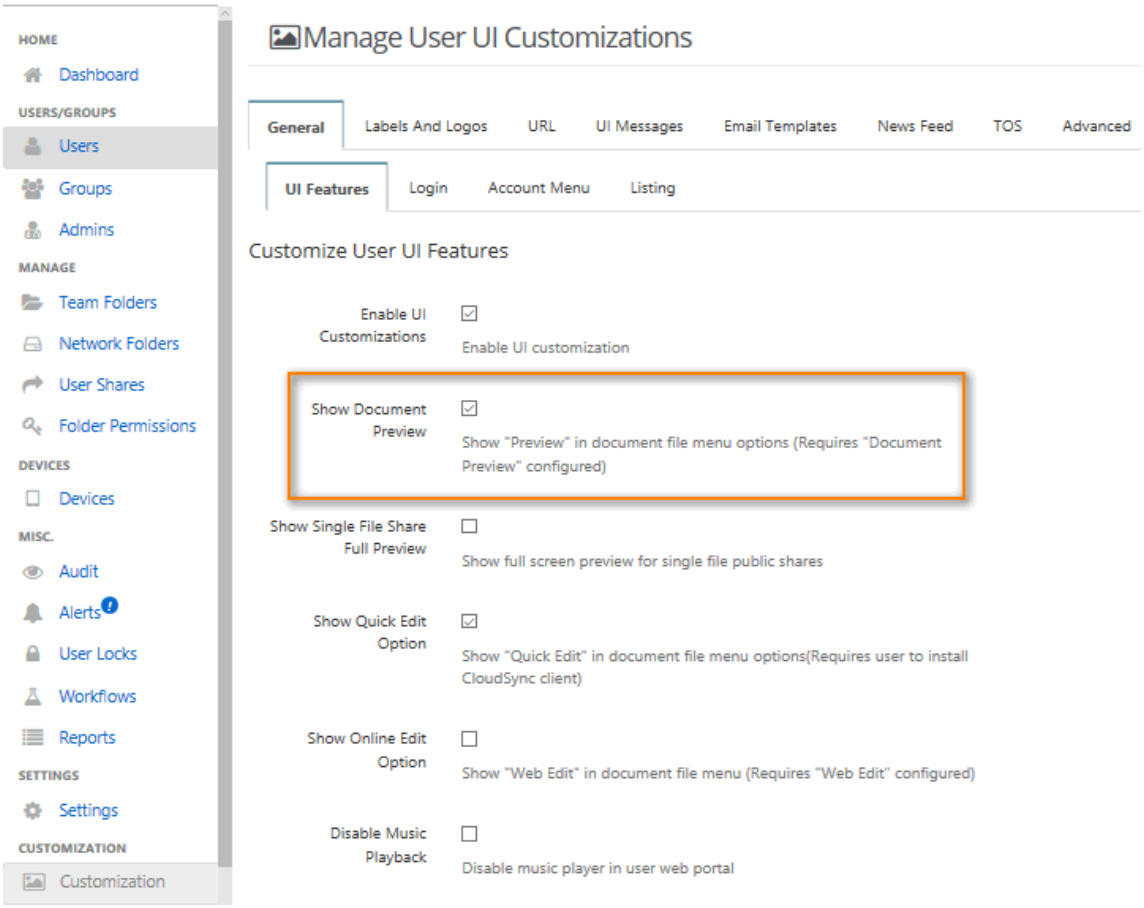
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.



3. Enter the path to the LibreOffice program folder.



4. Click **Customization** on the left navigation panel.
5. Click the **General** tab.
6. Check **Show Document Preview**.



Import Files : Pre-seeding

Administrators can import files to managed storage configuration to prepare FileCloud for users.

⚠ NOTES:

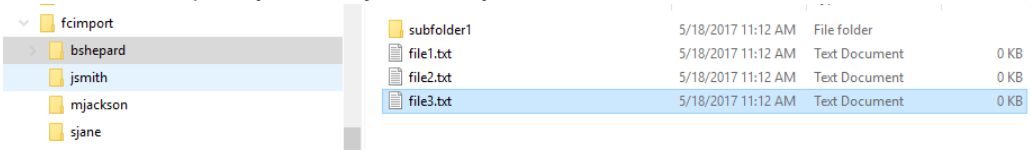
- During the seeding operation, the system is operating under a special mode and user access must not be allowed (though it is not prevented automatically).
- Therefore, ideally, seeding should be done during initial system setup.
- Once seeding is done, indexing must be done manually.

Import Files into Local Managed Storage

Prerequisite:

In order for the data to be imported, the following conditions must be met.

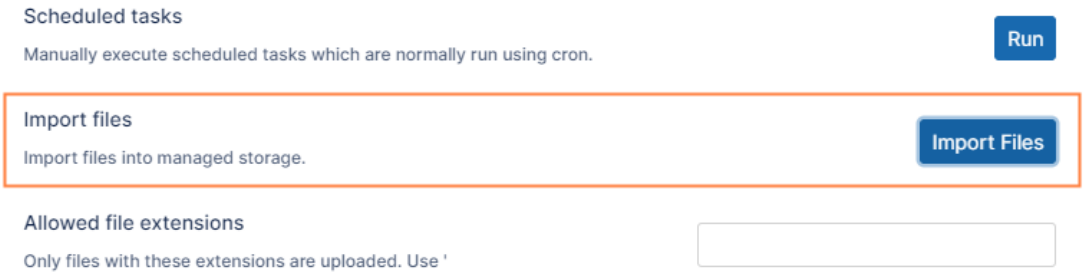
1. The data must be in locally accessible disk. Ideally, the data must reside in the same drive as the managed storage (for example, if managed storage is in C:\filecloud data, then the import data must also be in C: drive)
2. The data must be in following structure. <ImportPath><users><data>. For example, if you have four users, bshepard, jsmith, mjackson, sjane, then the structure should be:



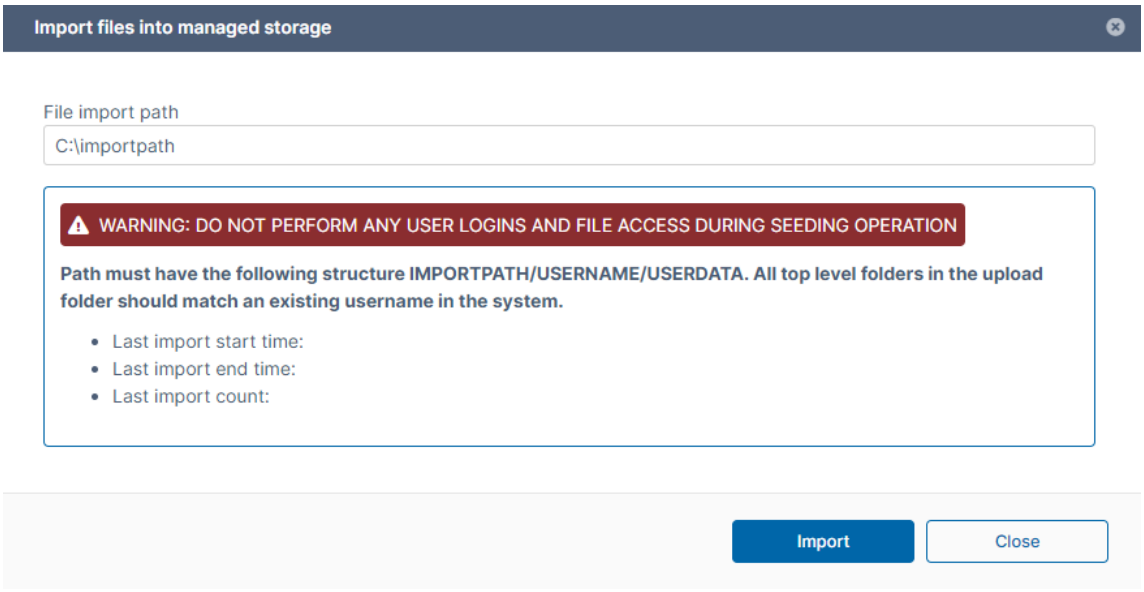
3. The users must already be created in the system (bshepard, jsmith, mjackson, sjane must already be valid full users in the system).
4. The users must have enough quota assigned to allow the data import.

To import files into local managed storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** UNKNOWN ATTACHMENT.
   By default, **General** settings are opened.
2. Scroll down to **Import Files**, and click the **Import Files** button.



3. On the **Import files into managed storage** dialog box, in **File Import Path**, type the location to the files you want to import in the format **C:\importpath** or **\import\data**.



4. Click **Import**.

Import files into S3 Managed Storage

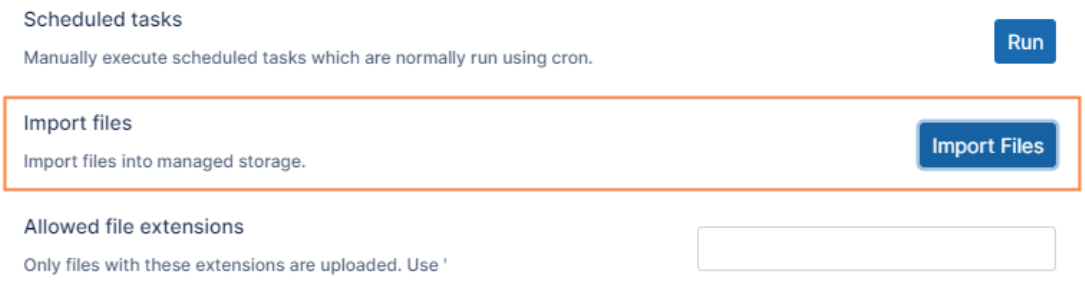
Prerequisite:

In order for the data to be imported, the following conditions must be met

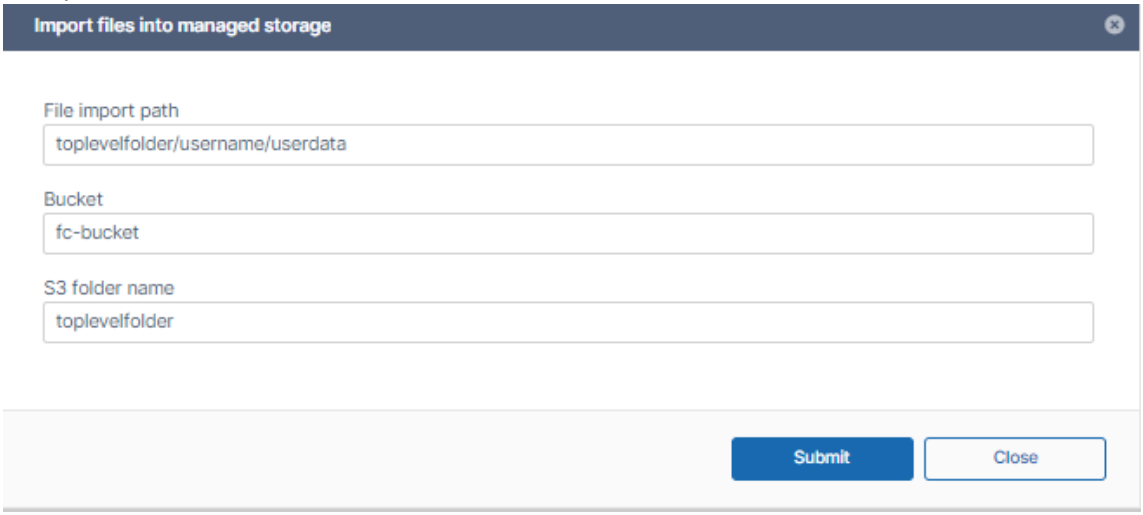
1. The data must be in a bucket that is accessible with the same credentials as the Managed Storage bucket
2. Both Managed Storage as well as the seeding bucket should not have encryption enabled.
3. The data must be in following structure. <Toplevel Folder><List of valid user account folders><data for each of the folder>
4. The users must already be created in the system with full user status.
5. The users must have enough quota assigned to allow the data import.

To import files into S3 managed storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** UNKNOWN ATTACHMENT.
   By default, **General** settings are opened.
2. Scroll down to **Import Files**, and click the **Import Files** button.



3. On the **Import files into managed storage** dialog box, fille in the fields as follows:
   File import path - The originating folder of the content to be imported.
   Bucket - the name of the bucket that contains the files you want to import.
   S3 folder name - the name of the top level folder in the bucket that contains the files you want to import.



4. Click **Submit**.

Import Files into S3 Managed Storage

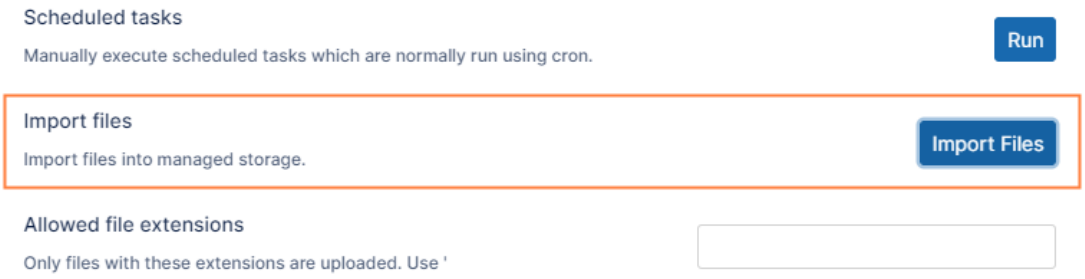
Prerequisite:

In order for the data to be imported, the following conditions must be met

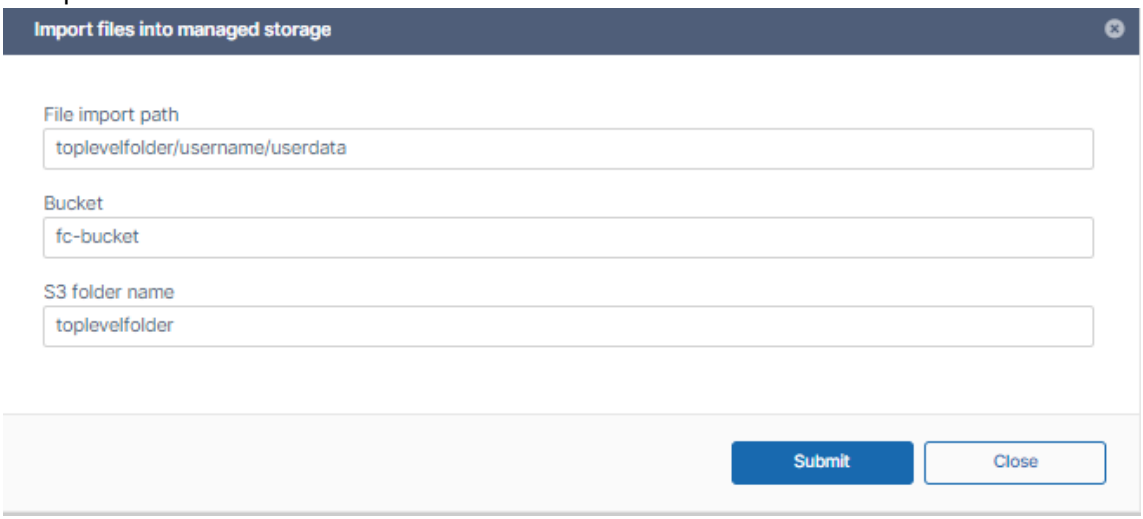
1. The data must be in a bucket that is accessible with the same credentials as the Managed Storage bucket
2. Both Managed Storage as well as the seeding bucket should not have encryption enabled.
3. The data must be in following structure. <Toplevel Folder><List of valid user account folders><data for each of the folder>
4. The users must already be created in the system with full user status.
5. The users must have enough quota assigned to allow the data import.

To import files into S3 managed storage:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** UNKNOWN ATTACHMENT.
   By default, **General** settings are opened.
2. Scroll down to **Import Files**, and click the **Import Files** button.



3. On the **Import files into managed storage** dialog box, fille in the fields as follows:
   File import path - The originating folder of the content to be imported.
   Bucket - the name of the bucket that contains the files you want to import.
   S3 folder name - the name of the top level folder in the bucket that contains the files you want to import.



4. Click **Submit**.

Enabling ASCII Sort order for Listings of Users, Files and Folders

Beginning with FileCloud 23.241, natural sort order is the default for listings of user names, files, and folders. Prior to FileCloud 23.241, ASCII sort order was the default.

- Natural sort order is used by default for listings of users, files, and folders in FileCloud. This option uses case-insensitive ordering of entries.
- The default can be changed to ASCII sort order using the setting shown below.

Natural Sort Order	ASCII Sort Order
1. Items sorted on numerals. 2. Items sorted without case sensitivity.	1. Items sorted on numerals. 2. Items sorted on uppercase letters. 3. Items sorted on lowercase letters.

To switch from Natural sort order to ASCII:

Enable ASCII sorting by setting the following key in the file WWWROOT\config\cloudconfig.php .

```
define("TONIDOCLOUD_NATURALORDER_SORTING", 0);
```

Natural sorting can be reenabled by setting the key value to 1.

For systems running prior to FileCloud 23.241

If you have not previously switched from ASCII sort order to Natural sort order and wish to do that now, use the following procedure:

1. If your FileCloud instance started running at version 21.1 or higher, skip to step 2.
   If your FileCloud instance started running prior to FileCloud 21.1, first run the following command from the command line.
   a. On Linux

```
# cd /var/www/resources/backup
# php ./preparenaturalsort.php
```

b. On Windows

```
> cd c:\xampp\htdocs\resources/backup
> C:\xampp\php\php.exe ./preparenaturalsort.php
```

This command can be run multiple times if needed to make sure there are no unprepared items.

2. Enable natural sorting by setting the following key in WWWROOT\config\cloudconfig.php.

```
define("TONIDOCLOUD_NATURALORDER_SORTING", 1);
```

ASCII sorting can be reenabled by setting the key value to 0 or completely removing it.

Enabling PDF Merge

Administrators can enable the option to allow users to combine multiple PDFs together.

- For this FileCloud uses a Document Converter server

To enable PDF Merge:

1. Install Document Converter

Administrators can use a Java-based service called FileCloud Document Converter to:

- Enable thumbs for all Microsoft Office documents (DOC, DOCX, PPT, PPTX, XSL, XSLX)
- Enable thumbs for Adobe documents (AI, PDF, PSD)
- Enable thumbs for TIFF images
- Interface with LibreOffice for document preview generation
- Add watermarks to all previews generated in FileCloud

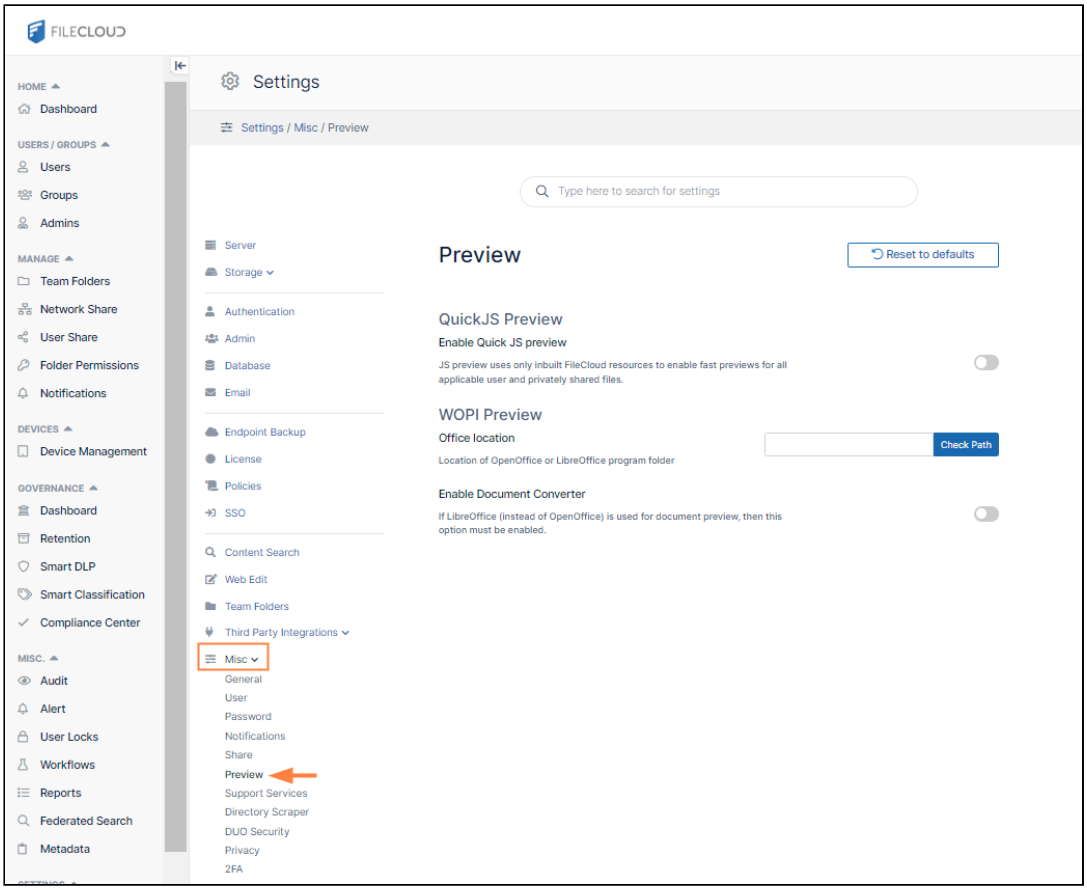
For this FileCloud uses a java program based on Apache's PDFBox. Document converter also will use LibreOffice libraries to convert documents to PDF.

If you have not already done so, Install Document Converter.

2. Enable the Combine PDF Option

To enable the ability to combine for PDFs:

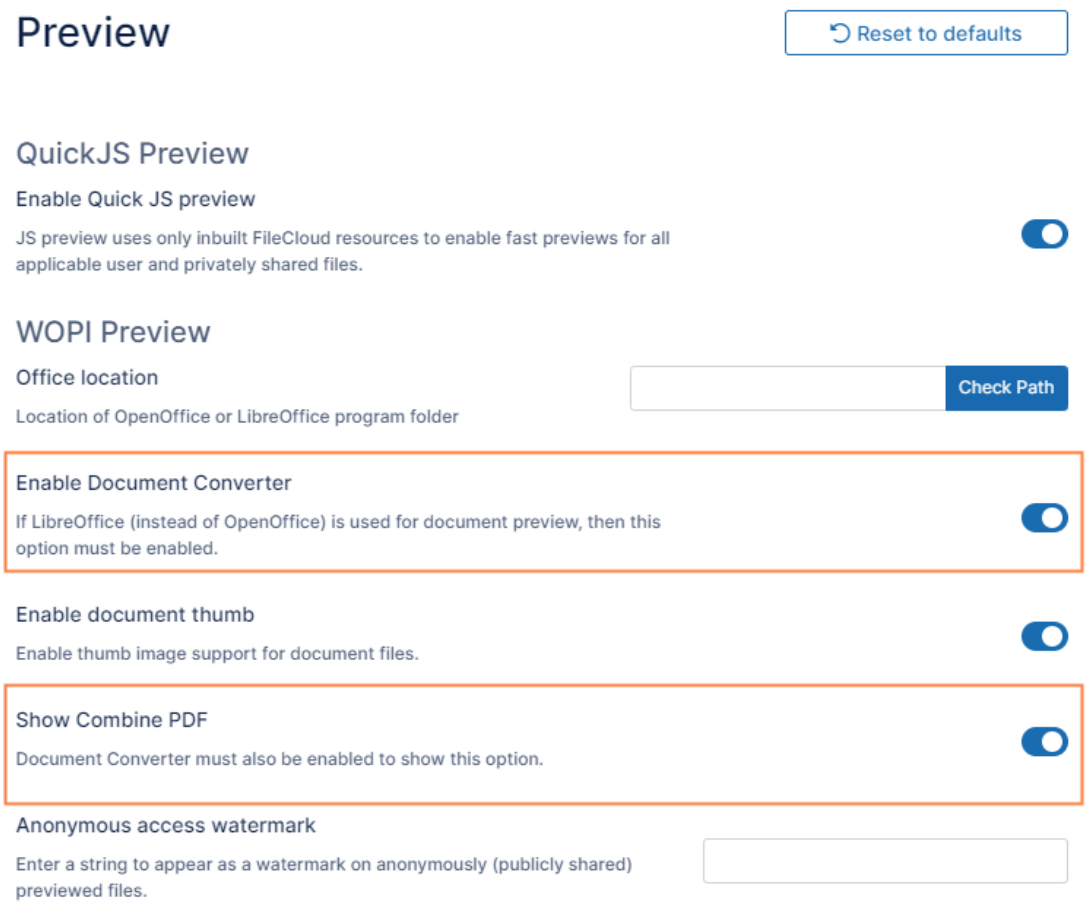
1. Open the **Preview** settings page.
   To open the Preview settings page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.



   The **Preview** settings page opens.

2. Enable **Enable Document Converter**.

3. Enable **Show Combine PDF**.



4. Click **Save**.
   Now when users select multiple PDF files from the user portal, an additional option for combining PDFs will appear. Selecting this will result in a popup containing merged PDFs.

Optimize PDF Preview

Administrators can configure FileCloud to show a preview of PDF files directly in the User Portal without forcing a user to download the file first.

This is configured when you Set Up Document Preview.

How users experience PDF previews

If you choose to allow previews of PDF files, you should be aware of what the user's experience will be on the user portal.

In some cases, viewing PDF files can take more time than expected.

The time it takes to generate a preview of a PDF depends on the how the file is created.

In general, a PDF can be categorized in to two main types:

- Native (quicker)
- Scanned (slower)

Why is a Native PDF quicker to preview?

Native

Information is saved as text when you save a file as PDF if you have created the file from the following sources:

- A word processing program such as Microsoft Word, Excel or PowerPoint
- A browser page printed to PDF
- A file saved directly from PDF generation software such as Nitro PDF, Adobe PDF, etc.

When information is saved as text, searching, copying, and other text-based operations on the PDF are quicker.

💡 It also takes less time to generate a preview of a native PDF file than a scanned PDF file.

Scanned

When PDFs are created from scanning, there is no information about the content because the PDF file just serves as a container of images.

💡 While this format is useful when the objective is to showcase graphics material, the rendering of this file can take a long time.

When a scanned PDF needs to be previewed in FileCloud:

1. The client's User Portal needs to check the entire PDF embedded text to allow search, copy or any other text based operations.
2. This text processing operation is done at the moment when the client's User Portal requests a preview.
3. The processing on the client-side portal can make the preview loading slow for general use.

NOTE: Enabling Solr OCR has no effect on the speed of previewing a scanned PDF.

If you have a scanned PDF file that has been created from one of the following sources, your best option is to convert the file to native PDF before uploading it to FileCloud:

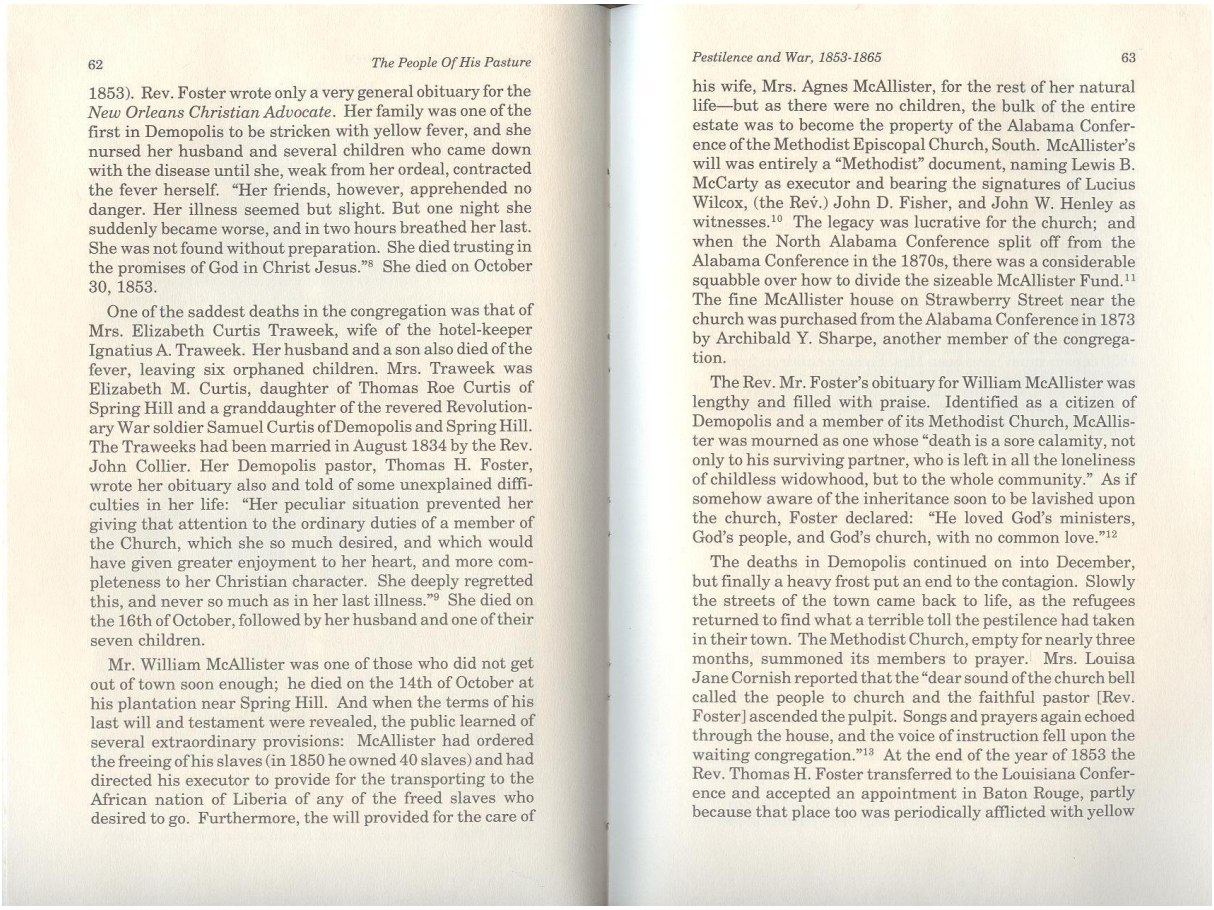
- Legal documents
- Insurance patient documents
- Blueprints and manuals

Optimizing files in this way allows a file to be opened with less processing time and generates a preview quicker.

How Do I Convert a Scanned PDF to Native?

There are several tools in the market you can use to convert scanned PDF files to native PDF files (OCR reading).

For example, if you have a scanned image similar to the following, you should convert it Native PDF:



62 *The People Of His Pasture*

1853). Rev. Foster wrote only a very general obituary for the *New Orleans Christian Advocate*. Her family was one of the first in Demopolis to be stricken with yellow fever, and she nursed her husband and several children who came down with the disease until she, weak from her ordeal, contracted the fever herself. "Her friends, however, apprehended no danger. Her illness seemed but slight. But one night she suddenly became worse, and in two hours breathed her last. She was not found without preparation. She died trusting in the promises of God in Christ Jesus."[8] She died on October 30, 1853.

One of the saddest deaths in the congregation was that of Mrs. Elizabeth Curtis Traweek, wife of the hotel-keeper Ignatius A. Traweek. Her husband and a son also died of the fever, leaving six orphaned children. Mrs. Traweek was Elizabeth M. Curtis, daughter of Thomas Roe Curtis of Spring Hill and a granddaughter of the revered Revolutionary War soldier Samuel Curtis of Demopolis and Spring Hill. The Traweeks had been married in August 1834 by the Rev. John Collier. Her Demopolis pastor, Thomas H. Foster, wrote her obituary also and told of some unexplained difficulties in her life: "Her peculiar situation prevented her giving that attention to the ordinary duties of a member of the Church, which she so much desired, and which would have given greater enjoyment to her heart, and more completeness to her Christian character. She deeply regretted this, and never so much as in her last illness."[9] She died on the 16th of October, followed by her husband and one of their seven children.

Mr. William McAllister was one of those who did not get out of town soon enough; he died on the 14th of October at his plantation near Spring Hill. And when the terms of his last will and testament were revealed, the public learned of several extraordinary provisions: McAllister had ordered the freeing of his slaves (in 1850 he owned 40 slaves) and had directed his executor to provide for the transporting to the African nation of Liberia of any of the freed slaves who desired to go. Furthermore, the will provided for the care of

Pestilence and War, 1853-1865 63

his wife, Mrs. Agnes McAllister, for the rest of her natural life—but as there were no children, the bulk of the entire estate was to become the property of the Alabama Conference of the Methodist Episcopal Church, South. McAllister's will was entirely a "Methodist" document, naming Lewis B. McCarty as executor and bearing the signatures of Lucius Wilcox, (the Rev.) John D. Fisher, and John W. Henley as witnesses.[10] The legacy was lucrative for the church; and when the North Alabama Conference split off from the Alabama Conference in the 1870s, there was a considerable squabble over how to divide the sizeable McAllister Fund.[11] The fine McAllister house on Strawberry Street near the church was purchased from the Alabama Conference in 1873 by Archibald Y. Sharpe, another member of the congregation.

The Rev. Mr. Foster's obituary for William McAllister was lengthy and filled with praise. Identified as a citizen of Demopolis and a member of its Methodist Church, McAllister was mourned as one whose "death is a sore calamity, not only to his surviving partner, who is left in all the loneliness of childless widowhood, but to the whole community." As if somehow aware of the inheritance soon to be lavished upon the church, Foster declared: "He loved God's ministers, God's people, and God's church, with no common love."[12]

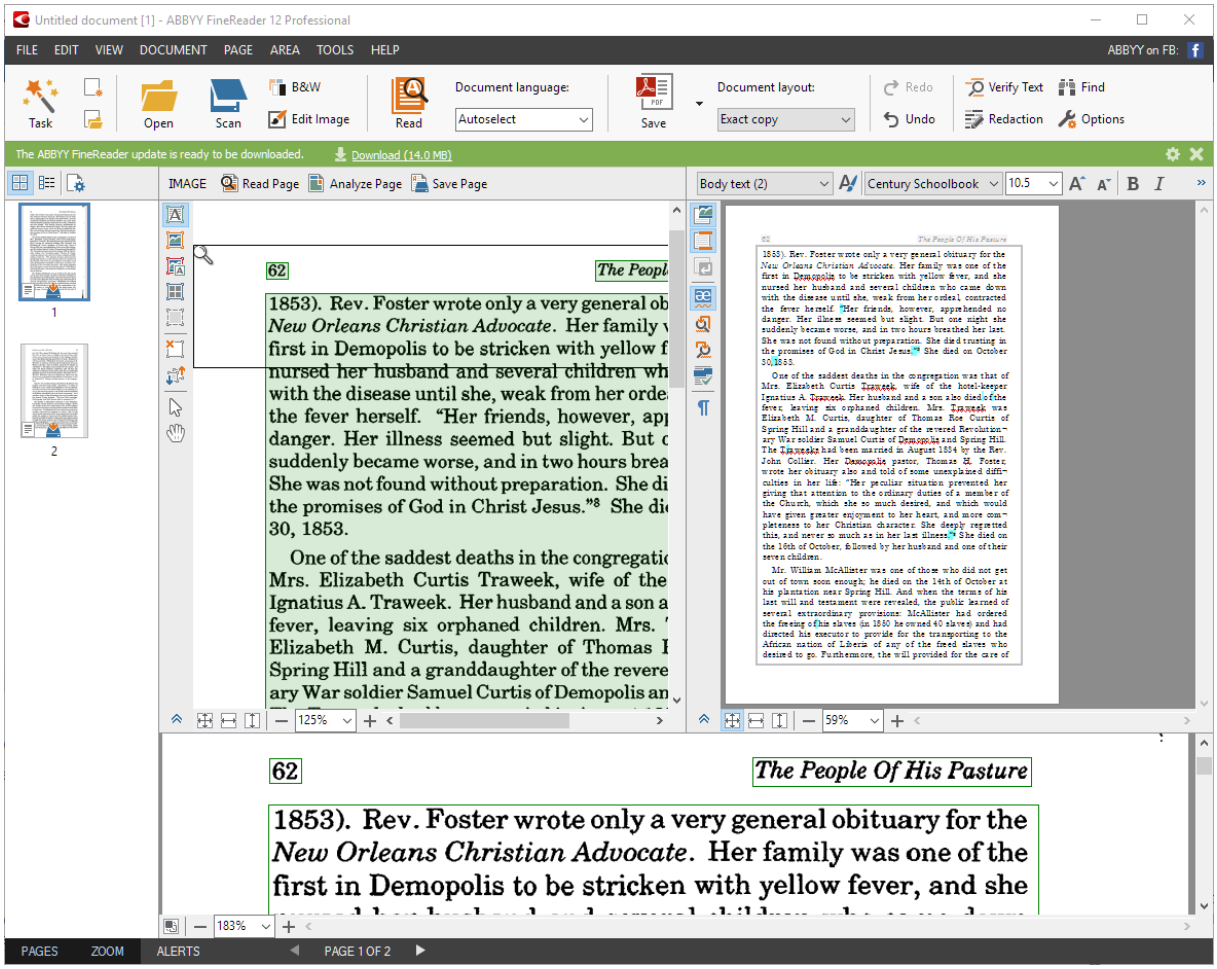
The deaths in Demopolis continued on into December, but finally a heavy frost put an end to the contagion. Slowly the streets of the town came back to life, as the refugees returned to find what a terrible toll the pestilence had taken in their town. The Methodist Church, empty for nearly three months, summoned its members to prayer. Mrs. Louisa Jane Cornish reported that the "dear sound of the church bell called the people to church and the faithful pastor [Rev. Foster] ascended the pulpit. Songs and prayers again echoed through the house, and the voice of instruction fell upon the waiting congregation."[13] At the end of the year of 1853 the Rev. Thomas H. Foster transferred to the Louisiana Conference and accepted an appointment in Baton Rouge, partly because that place too was periodically afflicted with yellow

In our example:

- this file is scanned and saved as a PDF named **Scanned_PDF.pdf**
- If we use this file as it is, the FileCloud Preview will take a longer than expected time to render this on the User Portal

For test purposes, CodeLathe has tested and recommends the following tool to optimize PDF files for generating a preview:

- ABBYY produces FineReader, an all-in-one OCR and PDF software application for increasing business productivity when working with documents.
- Using ABBYY Fine Reader software, you can open and convert this PDF file to a Native PDF file.



The use of ABBYY FineReader was used for explanation purposes only. Any other tool that can read a PDF file can be used to optimize the PDF files for web viewing.

Managing File Extensions

As of Version 23.232.1, FileCloud lists **php**, **php5**, **phar**, **phtml**, **php7**, and **htaccess** as disallowed file extensions. If you are using a version of FileCloud earlier than 23.232, you are advised to add any of these extensions that are not include by default onto the **Disallowed File** list.

For security reasons you may want to restrict uploading of files with specific extensions.

- You can either create a list of file extensions to restrict, or create a list of file extensions to allow.
- If you create an Allowed list of file extensions, then any settings in the Disallowed list will be ignored.
- These restrictions help to prevent users from uploading malicious attachments and viewing them.
- By default FileCloud restricts users from uploading any files with **php** extensions. This is to prevent any code injection.

In FileCloud's **Misc/General** settings you may specify allowed and disallowed file extensions.



Which list should I use? Allowed or Disallowed?

- If you know which file types you don't want to allow and this list is short, you can use the **Disallowed** setting.
- If you want to allow only a few file types to be uploaded, you can use the **Allowed** setting.
- If you create an **Allowed** list of file extensions, then any settings in the **Disallowed** list will be ignored.

What Do You Want to Do?

Allow File Extensions

If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.

- An empty space is defined as a delimiter character followed by no value.

Examples	Description	Impact on Uploading Files
`png | jpg |`	Allow files to be uploaded with an extension of: • png • jpg • *empty*	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group • Any file without an extension (for example, a file named *config*)
`png | jpg`	Allow files to be uploaded with an extension of: • png • jpg	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group

To allow extensions in the Admin Portal:

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. Scroll down until you see the **Allowed File Extensions** box.
3. In the **Allowed File Extensions** box, specify the allowed extensions, using the "|" character to separate each extension.

   Notes:

⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.

⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.



This list of extensions must use the following character as the delimiter:

-
  - '|'
  - For example, to restrict the mp4 and mp3 extensions:
    `mp4|mp3`

Disallow File Extensions

To disallow extensions in the Admin Portal:

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. Scroll down until you see the **Disallowed File Extensions** box.
3. In the **Disallowed File Extensions** box, add the additional restricted extensions.

Notes:
⚠️ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.



This list of extensions must use the following character as the delimiter:

- '|'
- For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions: php|php5|phar|phtml|php7|htaccess|mp3|mp4

Restricting File Extensions

As an administrator, for security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud.

- This helps prevent users from uploading malicious attachments and viewing them.
- By default FileCloud will restrict files with php extensions. This is to prevent any code injection.

To manage extensions in the Admin Portal:

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. Scroll down until you see the **Disallowed File Extensions** box.
3. In the **Disallowed File Extensions** box, specify the restricted extensions.



This list of extensions must use the following character as the delimiter:

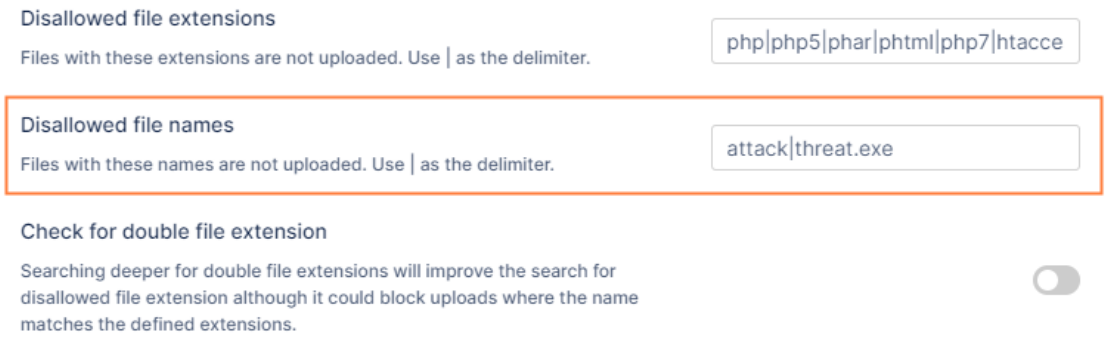
- '|'
- For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions:
  `php|php5|phar|phtml|mp3|mp4`

Restricting File Names

For security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud Server. In this case, you may want to make sure that certain files are not available.

To restrict names of files that can be uploaded:

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. Add the file names to the **Disallowed file names** field.
   Separate multiple names with |.



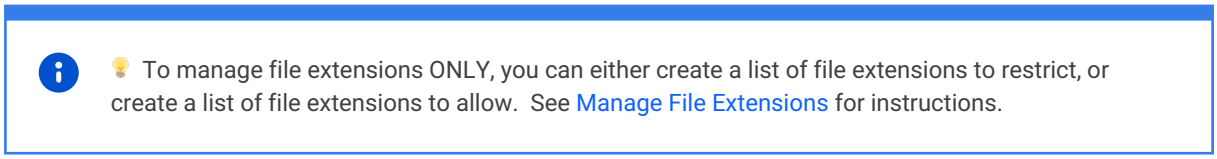
Files matching or including any term entered are not uploaded. If you do not specify an extension, files matching or including the term and any extension are not uploaded.

To understand how to create a list of file names, use the examples below.

If you leave an empty space in your list:

- In the User Portal, all files are blocked from being uploaded.
- The Sync client does not check for restricted names.

⚠ If you add an extension to the file name, then only the combination of name + extension is restricted.



Example	Description	Impact on Uploading Files
`attack | threat.exe |`	Restrict any file from being uploaded if it contains any of the 3 strings in the file name: • attack • threat.exe • *empty*	The following files cannot be uploaded by users: • *attack*.* • *threat.exe • Any file The following files can be uploaded by users: • No files can be uploaded until the *empty delimiter* is removed.
`attack | threat.exe`	Restrict any file from being uploaded if it contains any of the 2 strings in the file name: • attack • threat.exe	The following files cannot be uploaded by users: • *attack*.* • *threat.exe The following files can be uploaded by users: • Any file not containing *attack* • Any file not containing *threat.exe* • threat.* *(where * is NOT .exe)*

Manage File Versioning

You can allow a user to uploaded changes to a file and create another version of a file. This is called file versioning.

- This allows users to have an older version of the file on the site
- Users can download a previous version
- Users can remove previous versions to save space

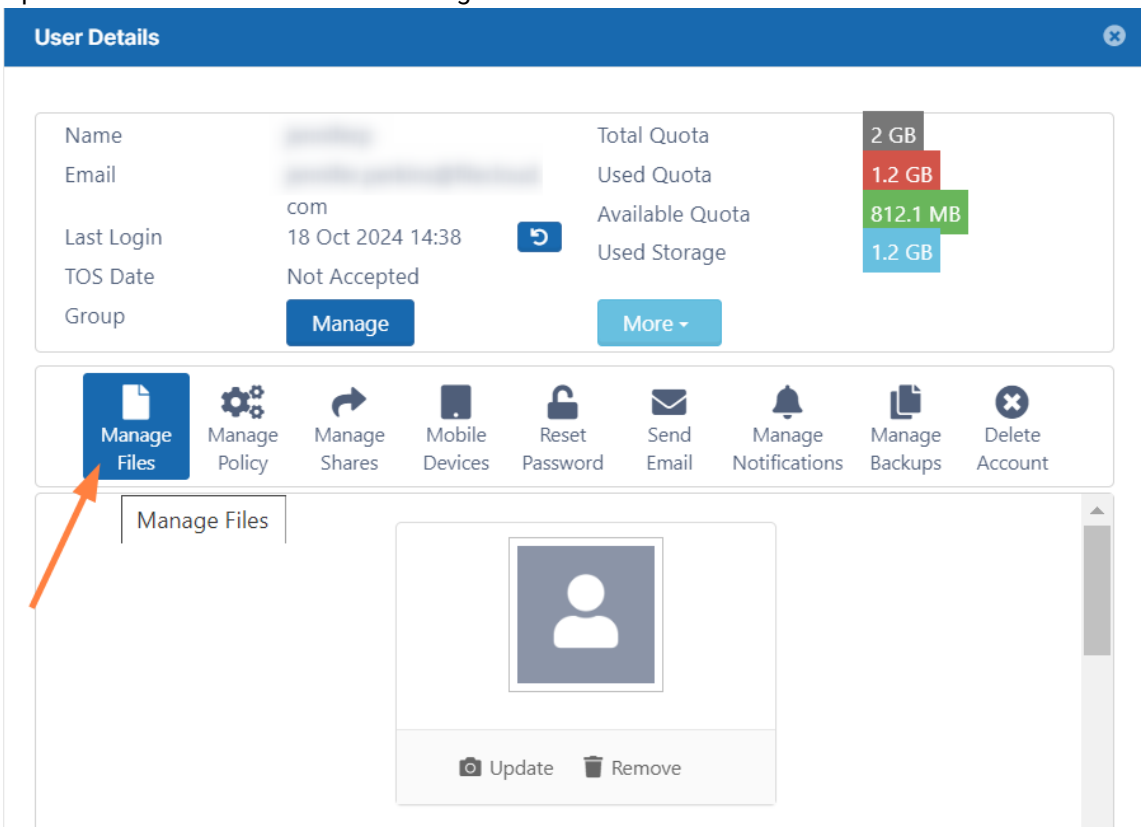
File versioning can be used with the following storage types:

- Managed
- LAN-Based Network Folders

- Managed S3

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

1. Open the user's details and click Manage Files.



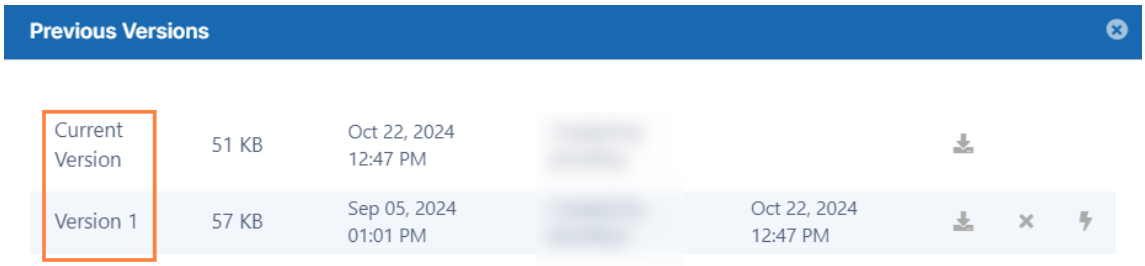
2. In the **Manage files** screen, navigate to a file and click its Versions icon



.



3. The **Previous Versions** window opens and lists all versions of the file.



If file versioning is causing issues, you can turn it off.

- File versioning can cause loss of data when a user accidentally overwrites a file with the same name.
- Users may be storing too many unnecessary versions of a file and are taking up too much space.

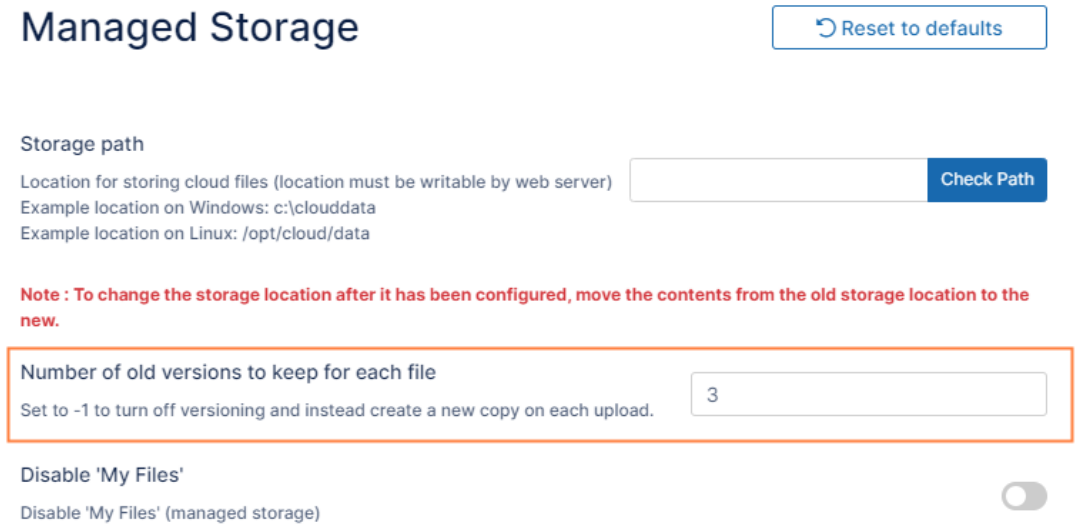
When you configure file versioning, use the following values:

Option	Setting	Result
Number of old versions to keep for each file	-1	The user tries to upload another version but the upload will FAIL
Number of old versions to keep for each file	any number greater than 0	When the user uploads a new version of a file, it is saved, and the latest <Number of old versions to keep for each file> versions are kept.

To manage file versioning:

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

2. In **Number of old versions to keep for each file** type in **-1** to turn versioning off or any number greater than **0** to use versioning.



3. To save your changes, click **Save**.

Configuring Zip Files and Zero Trust File Sharing

Beginning with FileCloud 23.241, zip files are enabled by default. Prior to FileCloud 23.241, zip files were disabled by default.
Functionality for creating and working with content in zip files in My Files is available beginning with FileCloud 22.1.
Functionality for creating and working with content in zip files in Network Shares is available beginning with FileCloud 23.232.

If you use encrypted storage and have zip files enabled, FileCloud creates temporary unencrypted copies of the files when performing actions on them. These files are only present briefly; however, if you want to avoid having the unencrypted data on your system, disable zip files. See **To enable and disable the zip file feature**, below.

Users can create and upload zip files into their My Files and Network Shares folders, and then preview, download, add, and delete contents of these zip files.

When users create zip files within FileCloud, they may add a password to them to create them as encrypted Zero Trust folders The password (decryption key) must be entered by the user who created the zip file or anyone they share the file with to access it. Note that the decryption key is not stored in FileCloud or known by the FileCloud system, and therefore makes the file invulnerable to attacks where the system is compromised.

For information about how users add and work with zip files, see Working with Zip Files.

By default, after the password is entered the first time during a log-in session, it does not have to be entered again during that session, but a setting in policies enables you to require users to enter the password each time they access it during a session.

To disable or re-enable the zip file feature

By default, the zip file feature described above is enabled. To make it unavailable to users, disable it in the FileCloud configuration file.

1. Open cloudconfig.php at
   - Windows: XAMPP DIRECTORY\htdocs\config\cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Locate the setting:

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

3. Change the value of TONIDOCLOUD_ZIP_FOLDER_ENABLE from **true** to **false**:

   ```
   define("TONIDOCLOUD_ZIP_FOLDER_ENABLE", false);
   ```

   The zip feature is now disabled for users. To re-enable it, change the value for TONIDOCLOUD_ZIP_FOLDER_ENABLE back to **true**.

Zip File Settings

The following are default settings for zip files. These may be modified in the FileCloud configuration file.

Setting	Default value
Encryption method	WinZip AES-256
Compression level	Normal
Compression method	Deflated
Fallback character set	None

Setting	Default value
Max zip file size	100 MB



WinZip AES-256 encryption is not supported by default in Windows. To enable use of Windows' default decryption method, change the encryption method to **PKWARE**, as shown in **To change the encryption method**, below.

To open the configuration file:

- Open cloudconfig.php at
  - Windows: XAMPP DIRECTORY\htdocs\config\cloudconfig.php
  - Linux: /var/www/config/cloudconfig.php
- Use the following steps to change any of the settings:

To change the encryption method:

Locate the setting:

```
define("TONIDOCLOUD_ZIP_FOLDER_ENCRYPTION_METHOD", 1);
```

Change the value to one of the following:

Value	Definition
0	PKWARE
1 (default)	WinZip AES-256 ***Note**: WinZip AES256 encryption works in Windows only with 7-Zip, winRAR, and WinZip third party compression software. Use **PKWARE** as an alternative.*
2	WinZip AES-128
3	WinZip AES-192

To change the compression level:

Locate the setting.

```
define("TONIDOCLOUD_ZIP_FOLDER_COMPRESSION_LEVEL", 5);
```

Change the value to one of the following:

Value	Definition
1	Super fast
2	Fast
5 (default)	Normal
9	Maximum

To change the compression method:

Locate the setting.

```
define("TONIDOCLOUD_ZIP_FOLDER_COMPRESSION_METHOD", 8);
```

Change the value to one of the following:

Value	Definition
0	Stored
8 (default)	Deflated

To change the fallback character set:

Locate the setting.

```
define("TONIDOCLOUD_ZIP_FOLDER_CHARSET_FALLBACK", null);
```

Change the value to one of the following:

Value	Definition
GREEK	cp737

Value	Definition
BALT_RIM	cp775
LATIN1	cp850
LATIN2	cp852
CYRILLIC	cp855
TURKISH	cp857
PORTUGUESE	cp860
ICELANDIC	cp861
HEBREW	cp862
CANADA	cp863
ARABIC	cp864
NORDIC	cp865
CYRILLIC_RUSSIAN	cp866
GREEK2	cp869
THAI	cp874

To change the max file size:

Locate the setting:

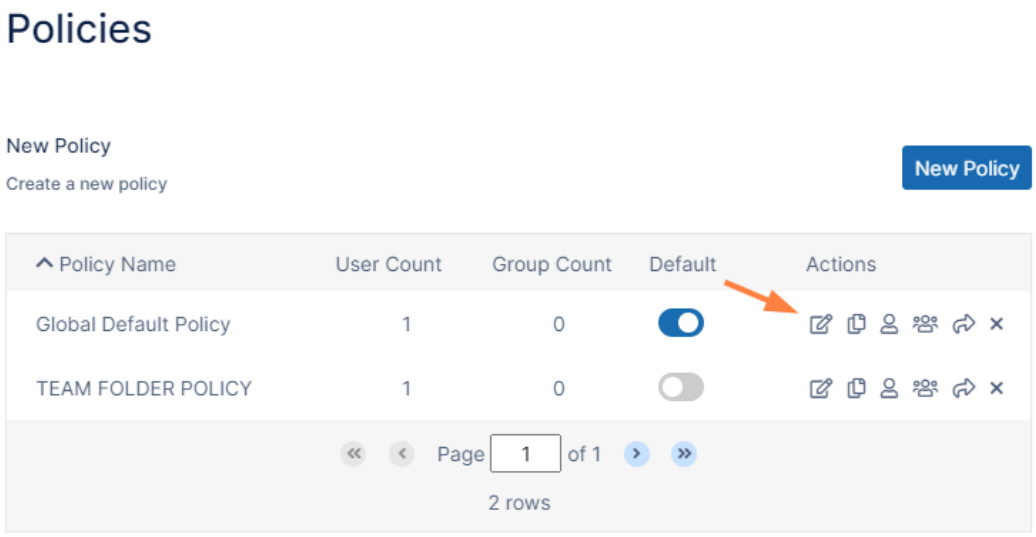
```
define("TONIDOCLOUD_ZIP_FOLDER_MAX_FILE_SIZE", "100");
```

The value is given in MB.

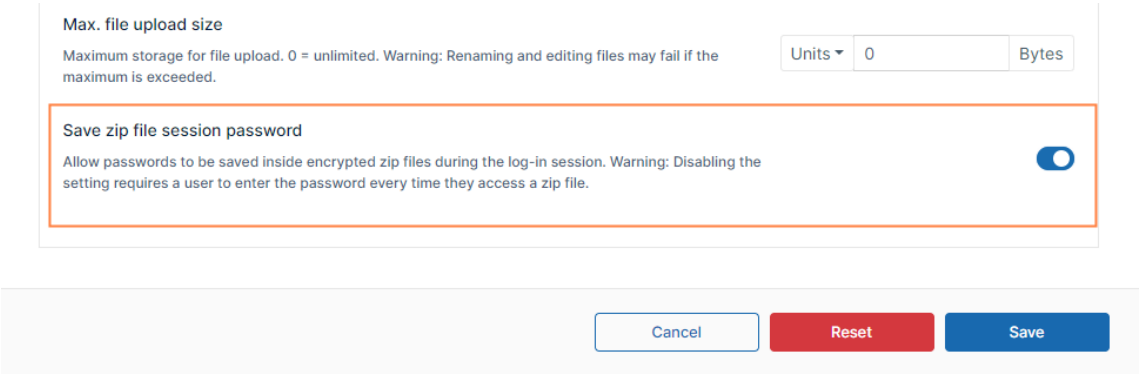
You can change the value to any number, but the maximum size of zip files supported in FileCloud is 4 GB (4000 MB) so any value higher than 4000 defaults to a maximum file size of 4000 MB.

To require the password each time an encrypted zip file is accessed:

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. Click the Edit icon for the policy of the users who you want to apply the restriction to.



3. The **Policy Settings** dialog box opens.
4. Click the **User Policy** tab.
5. Scroll down to **Save zip file session password** and enable it.



6. Click **Save**.
   Now, the users must enter the password each time they access the contents of the zip file.

Permissions in shared zip files

When a zip file is shared publicly, share users can view the contents of the zip file and download them. When a zip file is shared privately, the operations that share users can perform on its contents depends on their share permissions.

The following table shows what each share permission allows share users to do with the contents of a zip file

Permission	Description
View	Preview files and open folders in the zip file.
Download	Download files in the zip file and save them. Downloading folders in the zip file is not permitted.
Upload	Upload files into the zip file and delete files in the zip file.
Share	Share the zip file. Sharing of files and folders inside the zip file is not permitted.

Watermark Settings

The option of adding watermarks to downloaded files is available beginning in FileCloud 23.262.

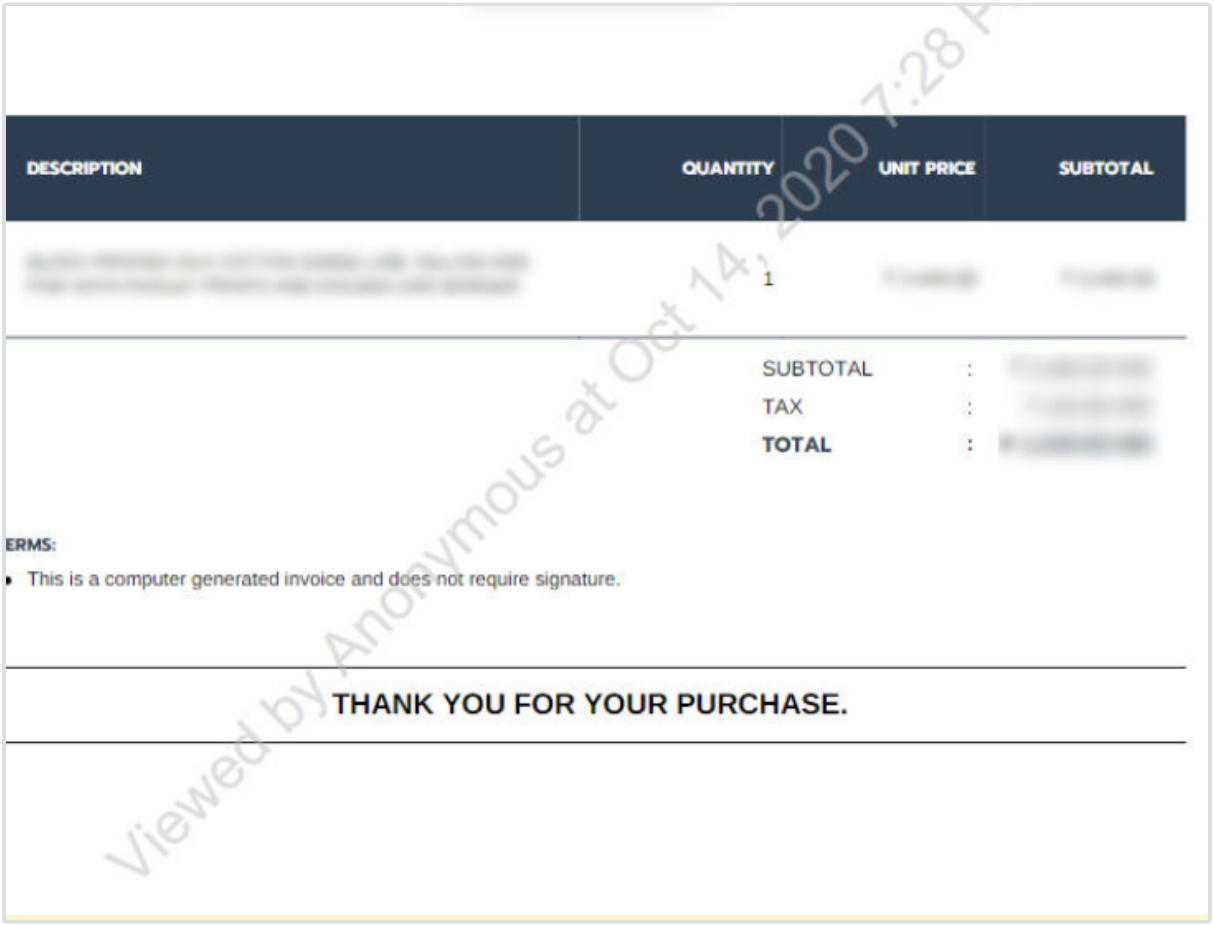
The Watermark Management page is available beginning in FileCloud 23.261 and introduces the ability to create watermark rules that are applied to specific users, groups, roles, or policies.
Prior to FileCloud 23.261, watermarks were configured on the Preview settings page.

Password protected PDF and Office file previews are not showing watermarks. This is an issue with the third-party application used for previewing PDFs, and will be resolved when an update of the application becomes available.
Adding watermarks to downloaded files is currently supported in the FileCloud user portal (web browser); it is not supported in client and mobile applications for security reasons,. When watermarks are included on downloads, watermarked files are not accessible from those applications

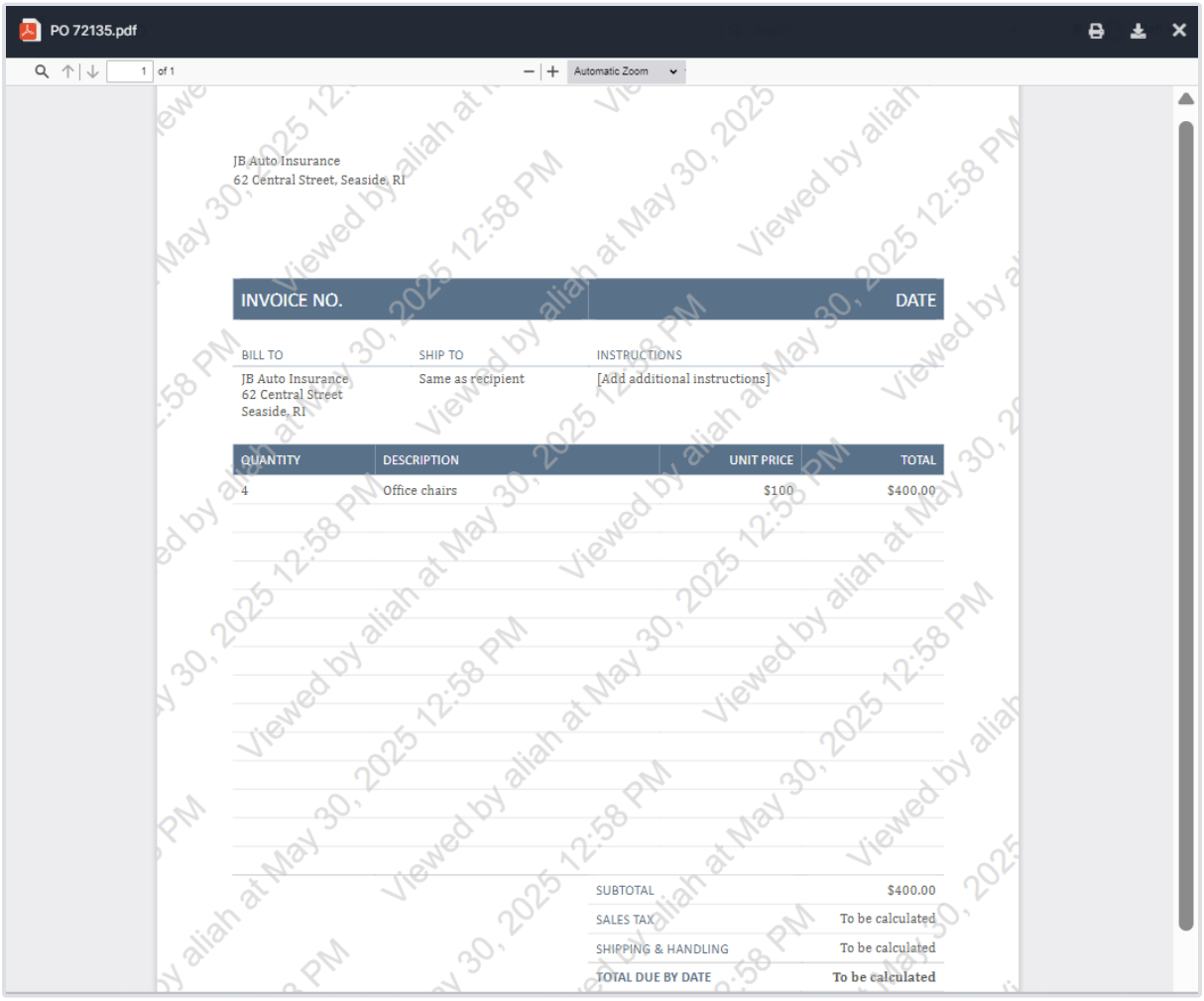
Watermarks are text that appears grayed out in the background of previewed or downloaded files in FileCloud. Administrators can add single line or multiline watermarks to PDF, Office, and image files when previewed and downloaded in FileCloud.

Note: Watermarks also appear on documents when edited in Collabora.

Single line watermark:



Multiline watermark:



On the Watermarks page in the admin portal, you can configure rules that determine which files have watermarks applied to them. For example, you could apply a watermark to:

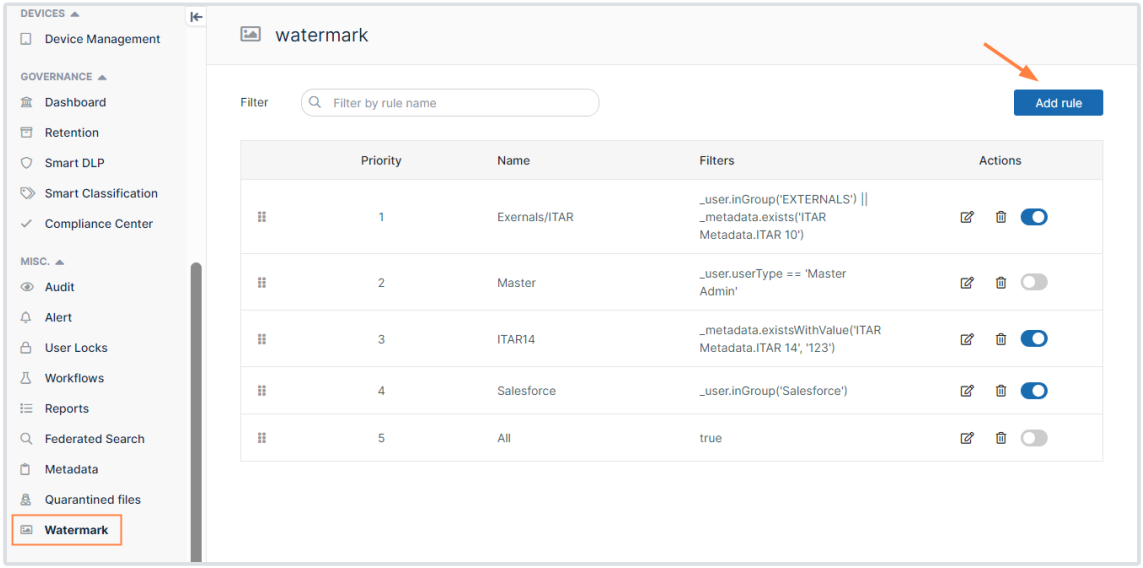
- all files previewed or downloaded by users in a certain group
- all files previewed or downloaded containing ITAR metadata.

Once you have specified the watermark filter conditions, you can add the watermark text, choose the single-line or multiline watermark template, and select the watermark font size.

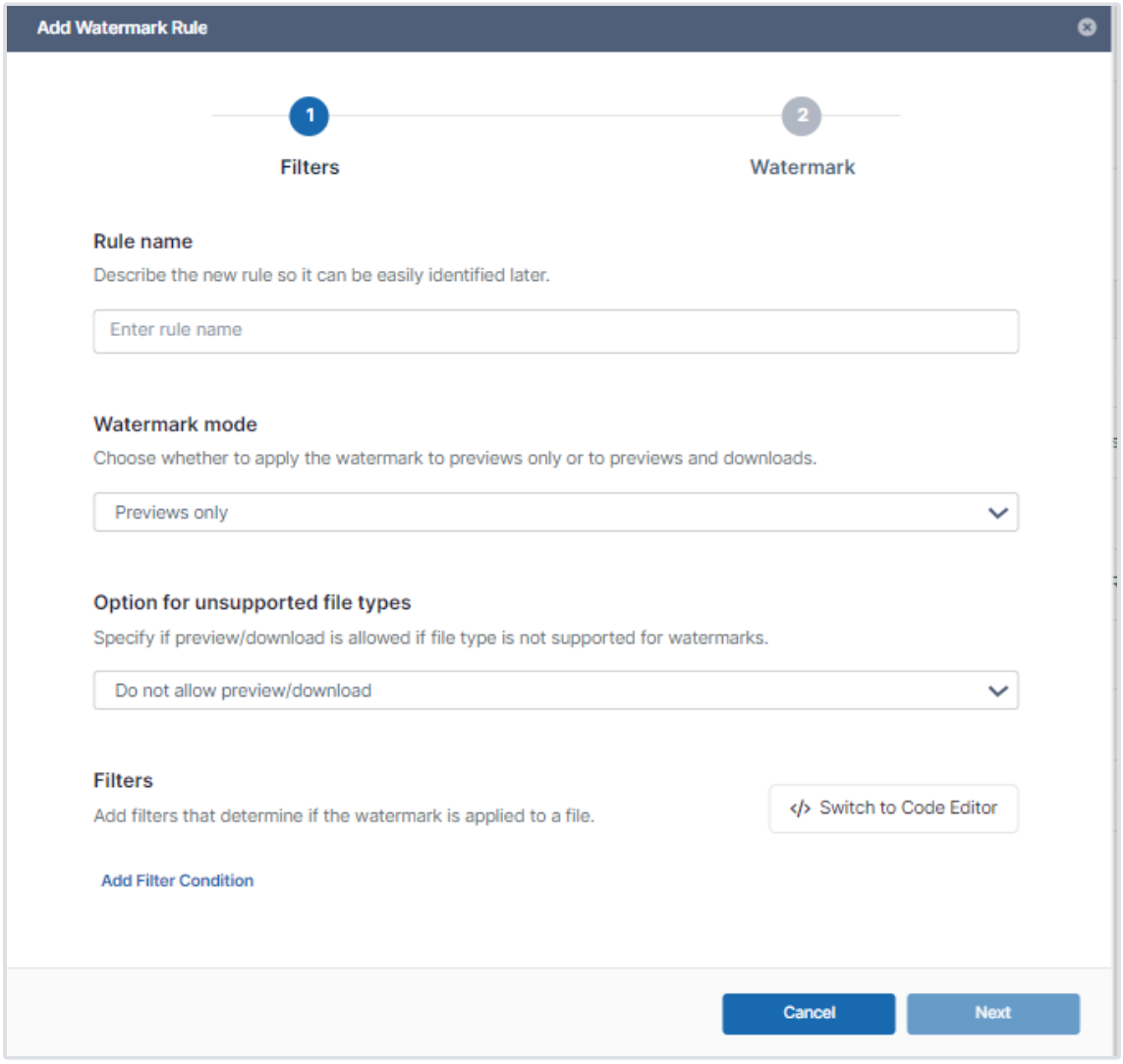
Adding a watermark rule

To add a watermark rule:

1. In the admin portal navigation pane, click **Watermark**.
   The Watermark page opens.
2. In the upper-right corner, click **Add rule**.



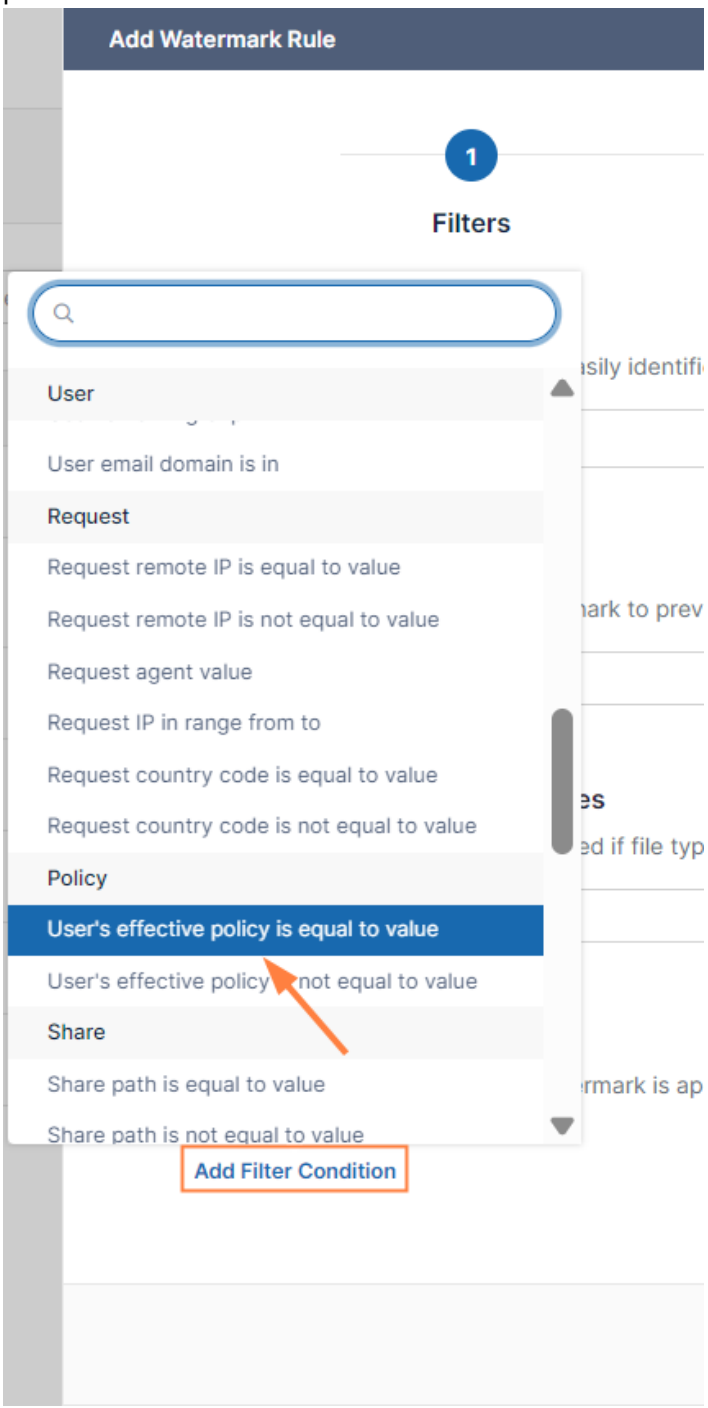
The **Add Watermark Rule** dialog box opens to the **Filters** window.



3. In **Rule name**, enter a name for the watermark rule.
4. In **Watermark mode**, choose an option:
   - **Previews only** - only apply watermarks to previewed files
   - **Previews and Downloads** - apply watermarks to both previewed files and downloaded files
5. In **Option for unsupported file types**, choose what to do on download when a file type is not supported for watermarks. PDFs, Office files, and images are supported; all other file types are unsupported.
   When a folder with multiple files is downloaded, the files of supported types in the folder are downloaded with watermarks, and the files of unsupported types are either not downloaded or downloaded without watermarks depending on which of the following options is chosen:
   - **Do not allow preview/download** - Do not allow the user to download or preview unsupported file types.
   - **Allow preview/download without watermark** - Allow the user to download or preview unsupported file types although watermarks will not appear.
6. Click **Add Filter Condition**.

A drop-down list of predefined filter conditions opens. See Filter conditions, below, for information about the predefined conditions.

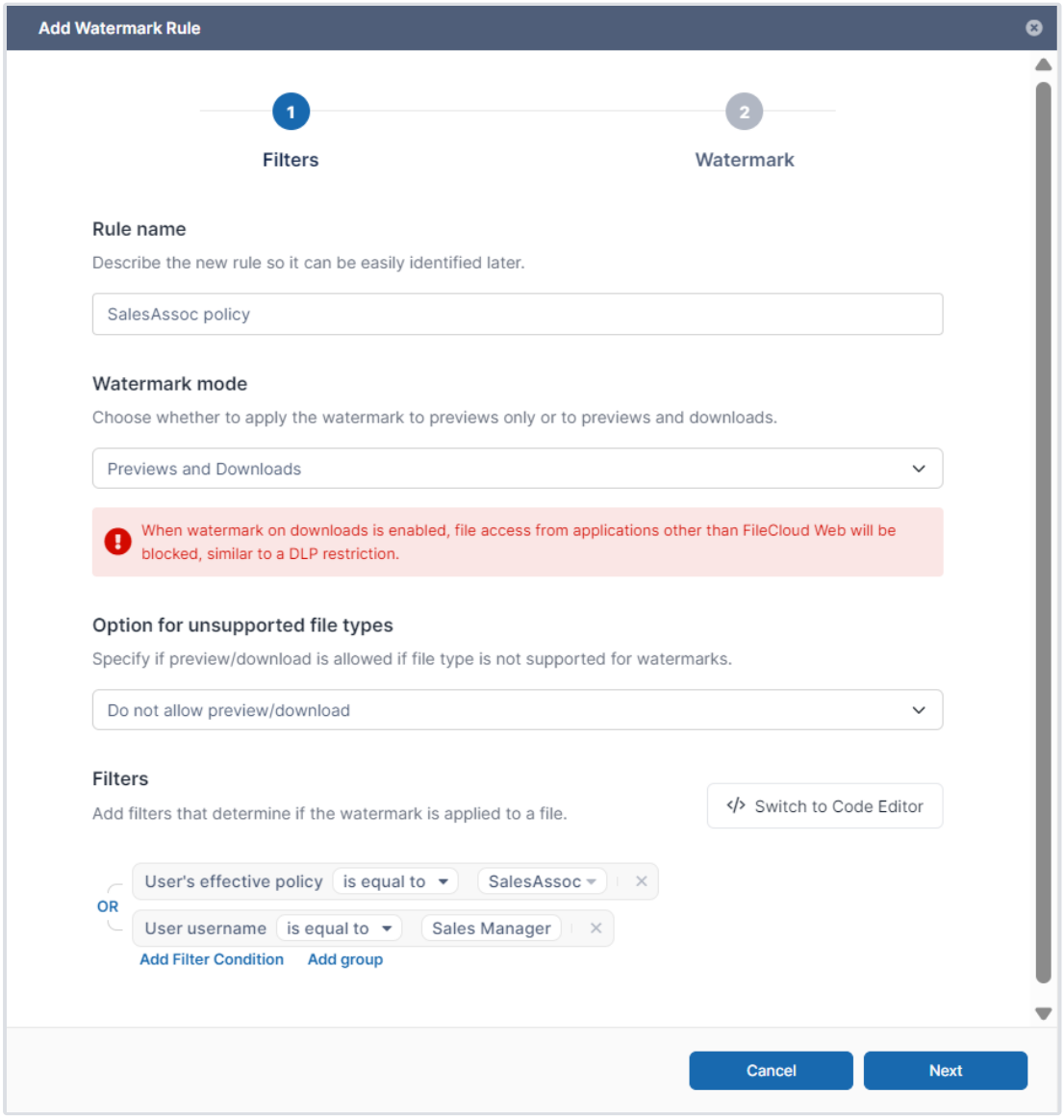
7. In the example below, we first choose **User's effective policy is equal to [SalesAssoc]**. Users with the policy **SalesAssoc** are selected by the filter and their files display the watermark when previewed or downloaded.



*Note: Instead of choosing a predefined condition, you may click **Switch to Code Editor** and write your condition in Expression Language using Watermark Parameters for Code Editor. For help*

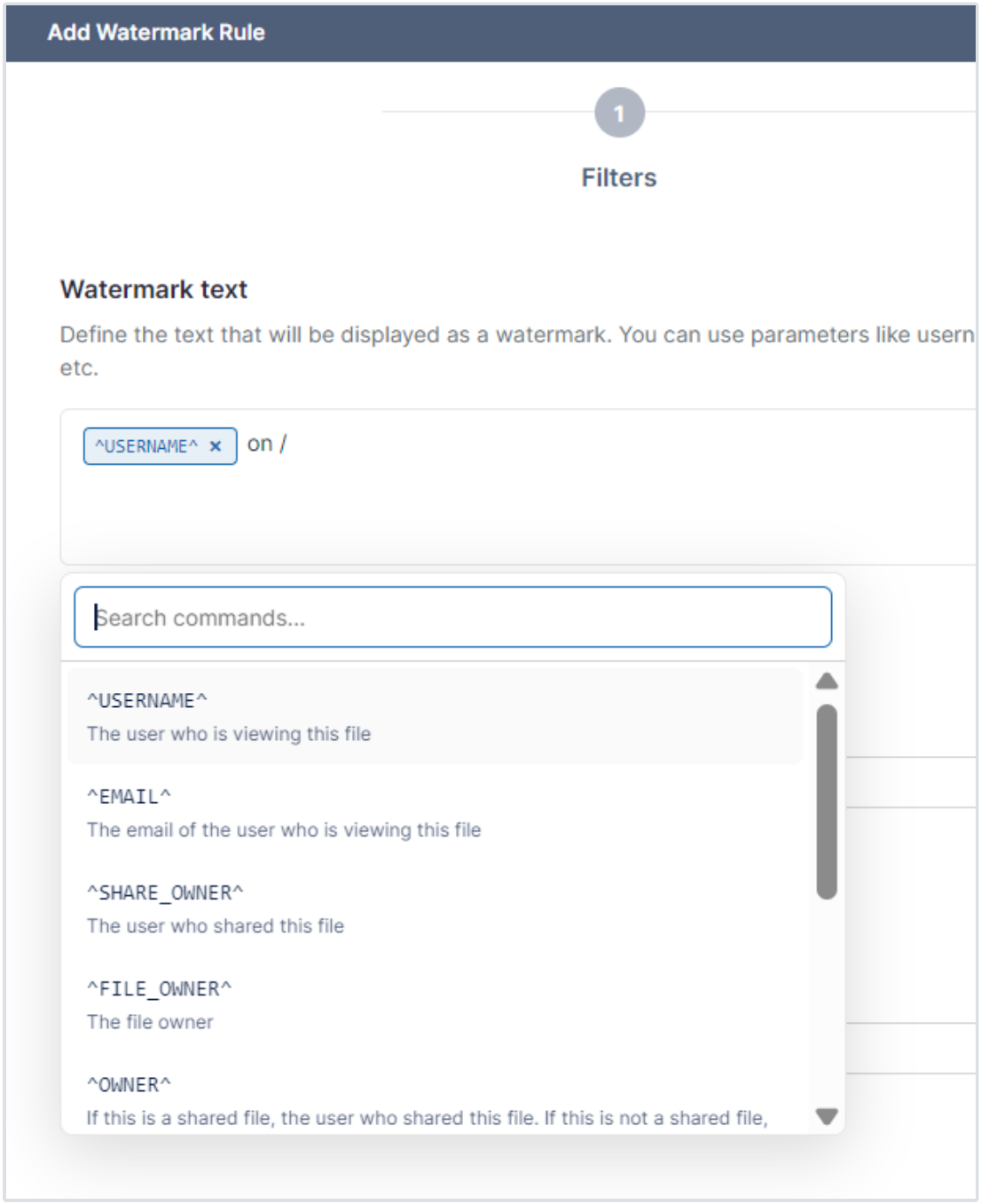
with expression language, see https://symfony.com/doc/current/reference/formats/expression_language.html.

8. Once you have selected a condition, enter any values it requires.
9. Enter any number of filters.
   In the example, the filter condition **User username is equal to [Sales Manager]** is also chosen.
   By default, multiple filters are given an OR relationship, but you can click **OR** to change it to **AND**.

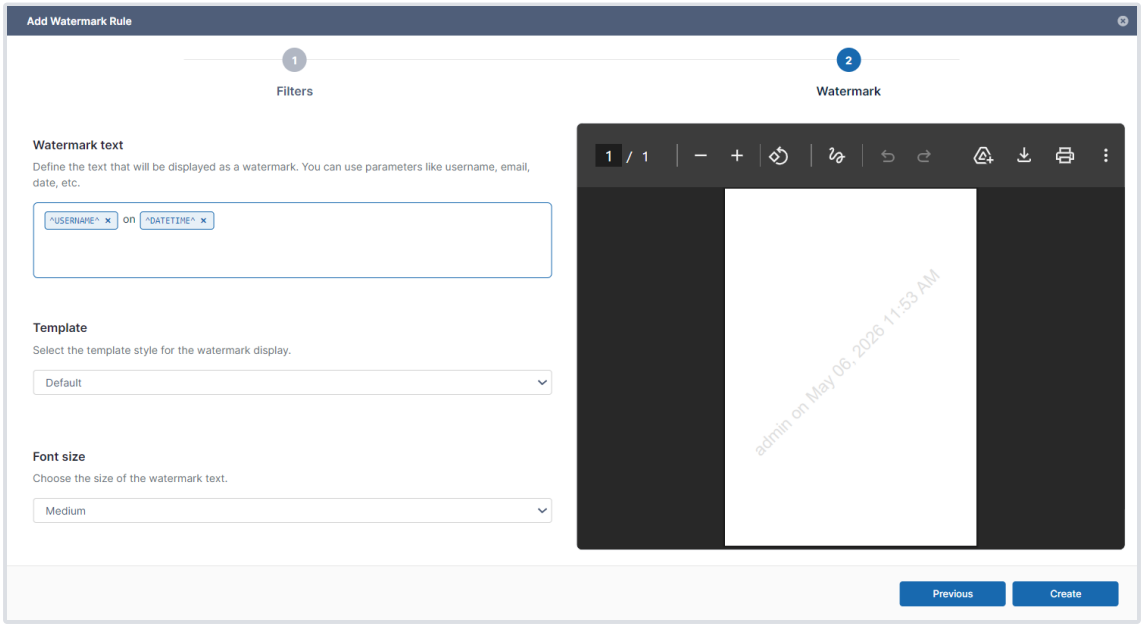


Note: The red warning under **Watermark mode** in the image above only appears if you choose **Previews and Downloads** as the **Watermark mode**. It indicates that when watermarks on downloads are enabled, watermarked files cannot be viewed on client and mobile applications.

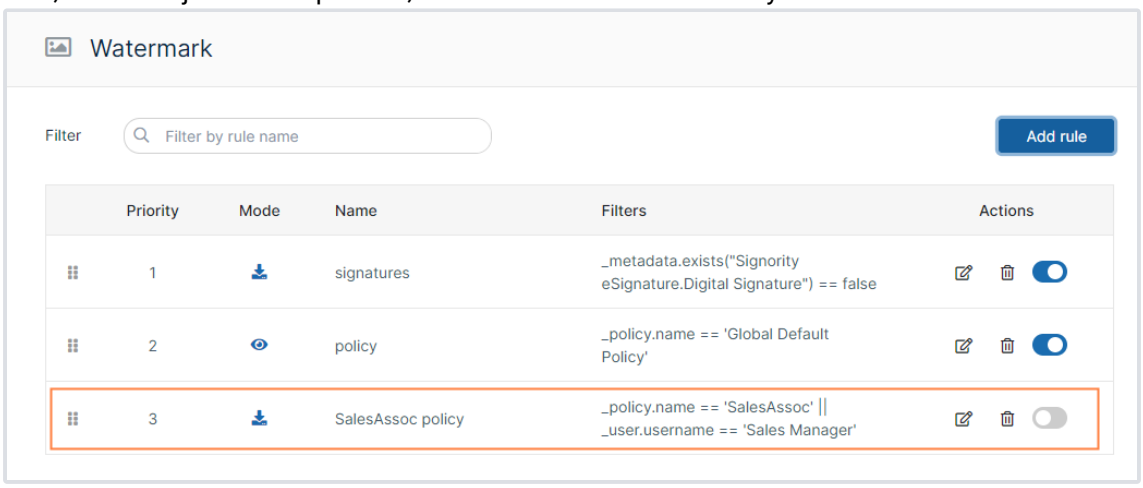
10. To go to the **Watermark** window, click **Next**.
11. In **Watermark text**, enter the text of the watermark. Parameters are available for you to use.
    To select from a list of available parameters, enter **/** in the **Watermark text** box, then click a parameter:



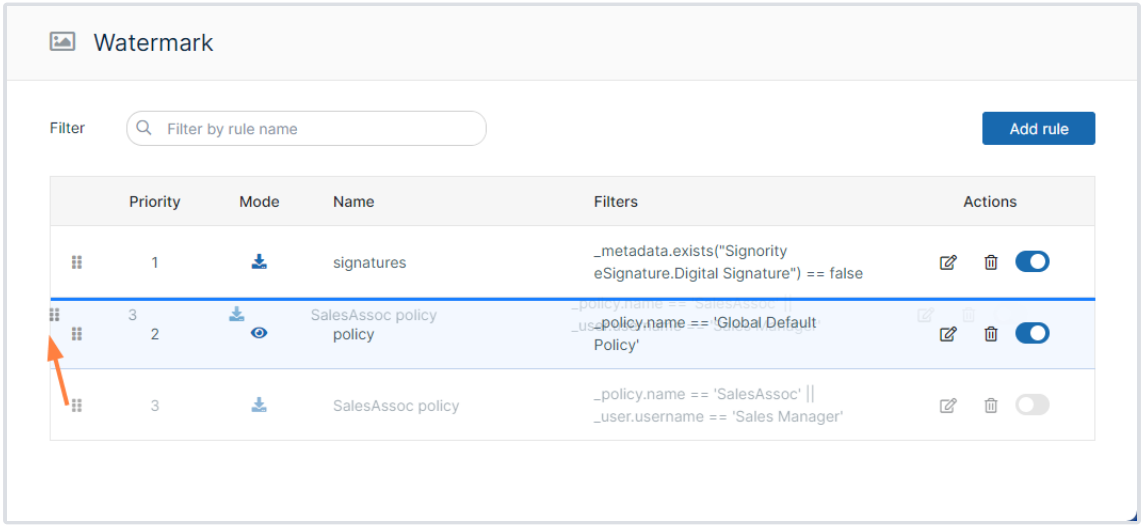
12. In **Template**, leave **Default** selected for a single line watermark, or choose **Multiline** for a multiline watermark.
13. In **Font size**, choose the font size of the watermark.
    The window shows a preview of the watermark.



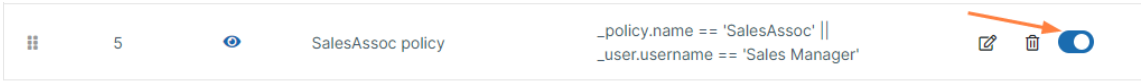
14. Click **Create**.
    The watermark rule is listed on the Watermark page. If it is the first watermark you are creating, its **Priority** is listed as 1; otherwise it is listed as the lowest rule in priority, and will be checked if none of the other rules are true.
    If the watermark rule allows both preview and download, the **Mode** column shows a download icon; if the rule just allows preview, the **Mode** column shows an eye icon.



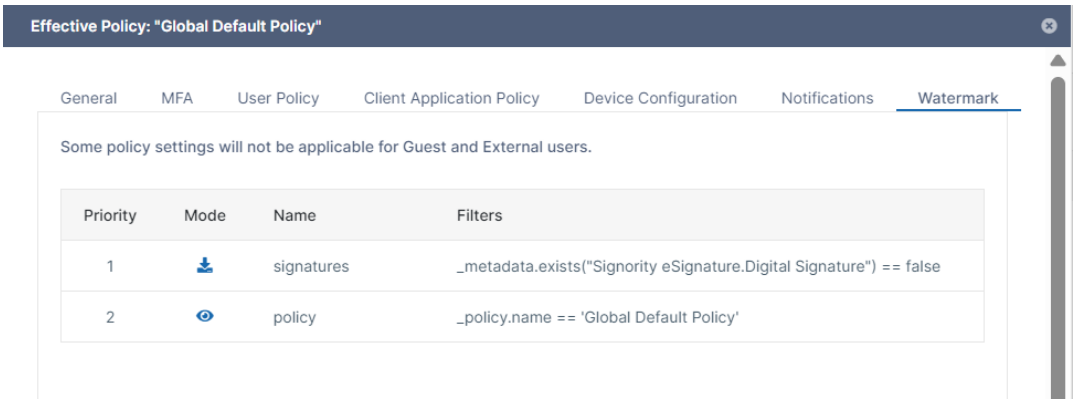
15. To change a rule's priority, drag and drop it to a new position from the drag bars:



16. Under **Actions**, click the toggle button to activate the watermark rule.



Once you enable a watermark rule, it is listed on the Watermark tab in of the Policy settings for all policies that it applies to.
If a watermark rule does not apply to specific policies, it is listed for all policies; if a watermark rule applies to specific policies, it is only listed for those policies.
For example, in the following image, the Watermark tab shows that the watermark rules **signatures** and **policy** apply to users and groups in the **Global Default Policy**. Since the policy rule specifically applies to the **Global Default Policy**, it only appears in this policy's Watermark tab.



Filter conditions

In the **Filter Condition** drop-down list, choices are provided for you and required formats are shown in the value fields where applicable. For a guide to all of the expressions you can use for specifying conditions in the code editor, See Watermark Parameters for Code Editor.

Utils
The only option under utils is **Anything**. Select **Anything** to apply the watermark to all files.

File
File conditions apply to the file extension, path, name, size, and word count.

User
User conditions apply to the user's username, email, type, group, and email domain.

Request
Request conditions apply to the IP address or country code of the user making the request, or the agent (client application) making the request.

Policy
Policy conditions look at the policy name.

Share
Share conditions look at the share path, the type of share (public or private), or the emails or domains of the users shared with.

Metadata
Metadata conditions look at metadata values. These conditions check if a a certain metadata attribute on the file has a specified value (or any value).

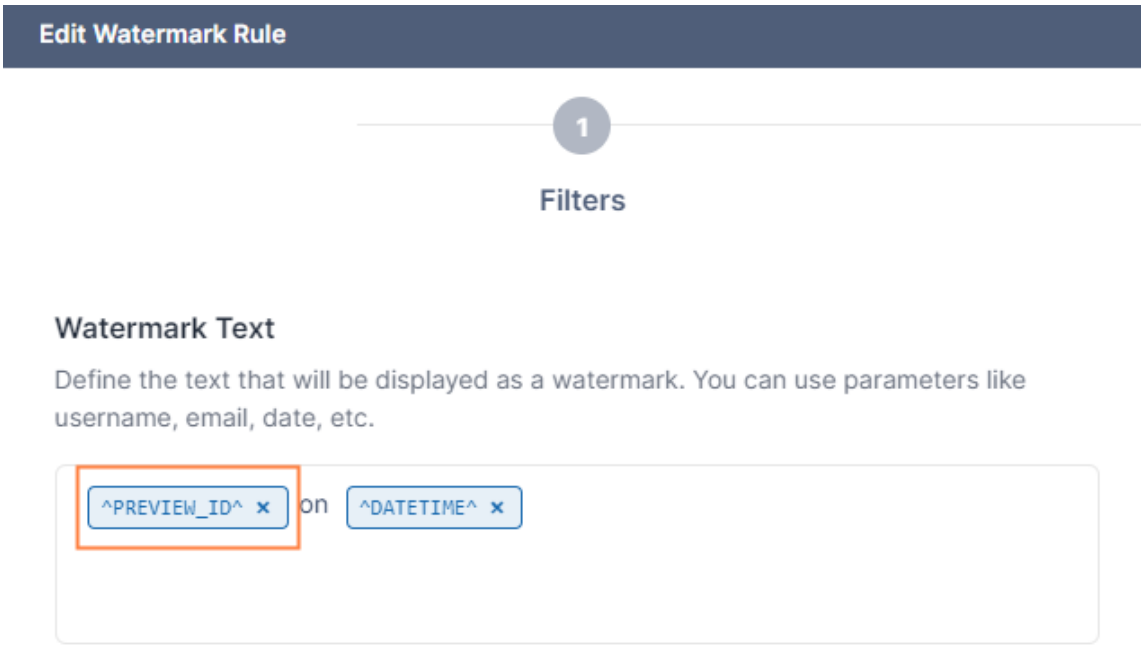
Esignature

There are two options under Esignature, **File is signed** and **File has digital signature**. The primary purpose of these settings is to enable admins to choose not to apply watermarks to signed files, which enables them to be successfully downloaded. For more information on these settings, see Watermark Settings , below.

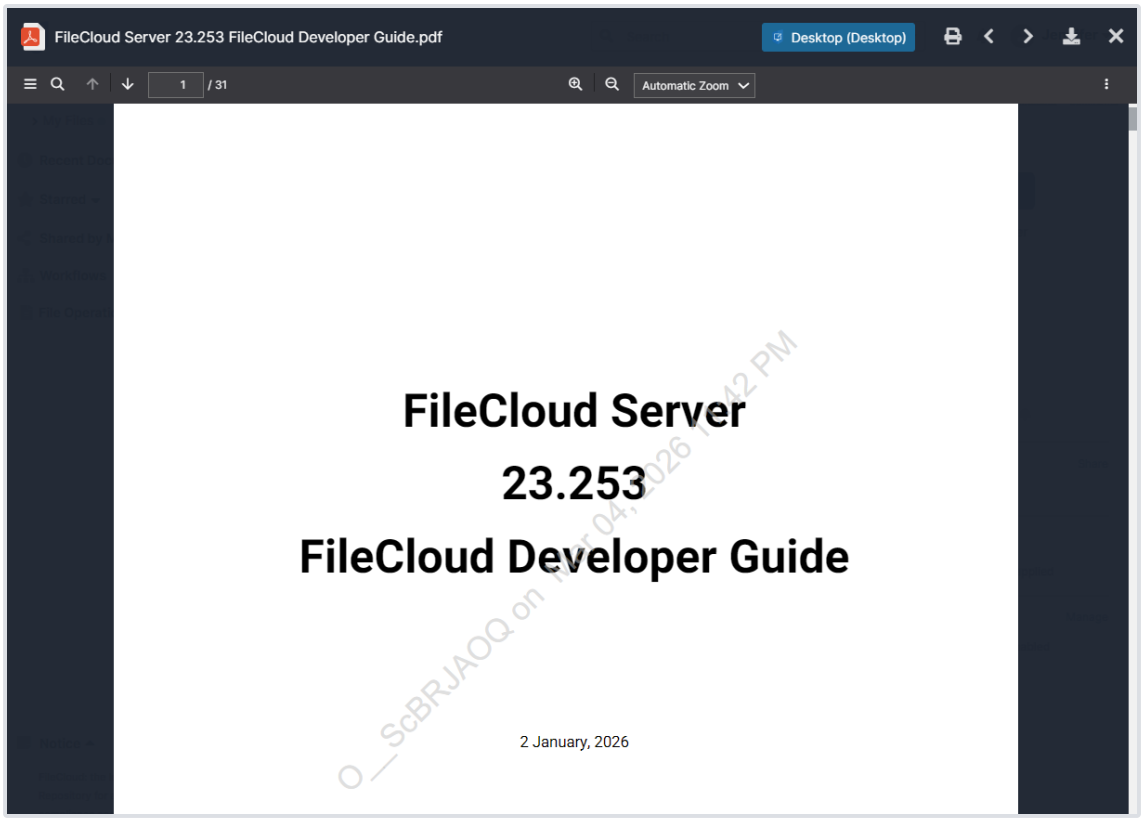
Displaying an encrypted User ID in a watermark

To display an encrypted User ID instead of the actual User ID in a watermark:

1. In the **Watermark Text**, use the parameter **^PREVIEW_ID^** instead of **^USERNAME^**

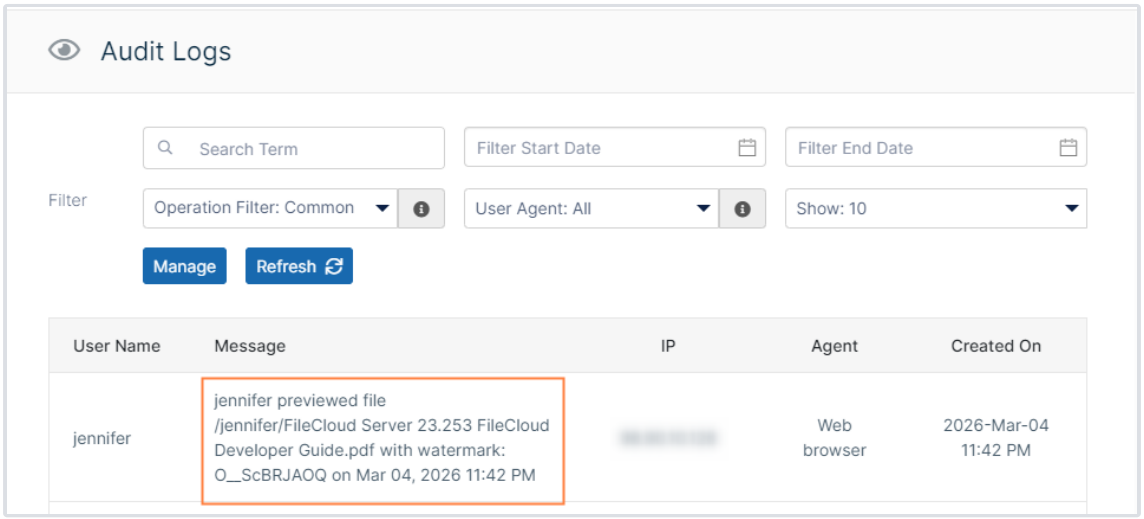


This produces a preview or download with a watermark like the following one:



Note that if the user previews or downloads the file additional times, it will have different preview IDs each time.

2. To identify the user who previewed or downloaded the file, go to the Audit Logs, and locate the log with the encrypted ID in the message. The message will identify the actual user who previewed or downloaded the file, and, as with any audit log record, the IP address of the device where the action was performed.



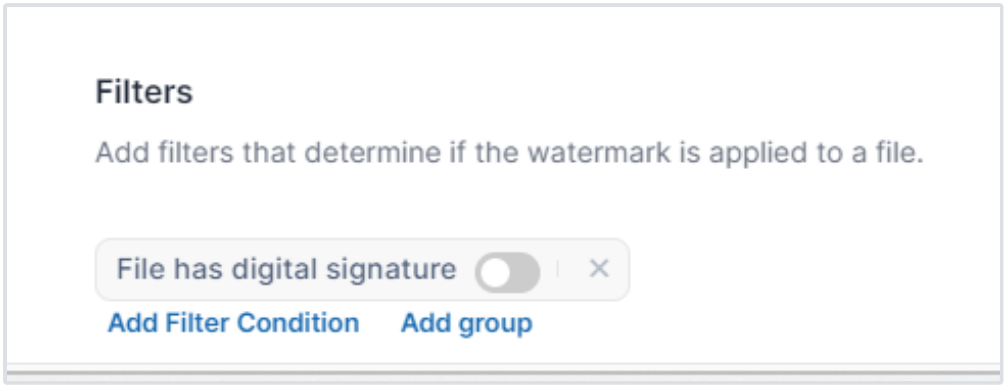
Ensuring that signed files are downloaded

Edits to digitally signed files are not permitted after they are signed; therefore, if FileCloud attempts to apply a watermark to a digitally signed file, it fails and the file is not downloaded.

Edits to eSigned files are permitted after they are signed; therefore, if FileCloud attempts to apply a watermark to an eSigned file, it is successful unless a filter prevents this operation.

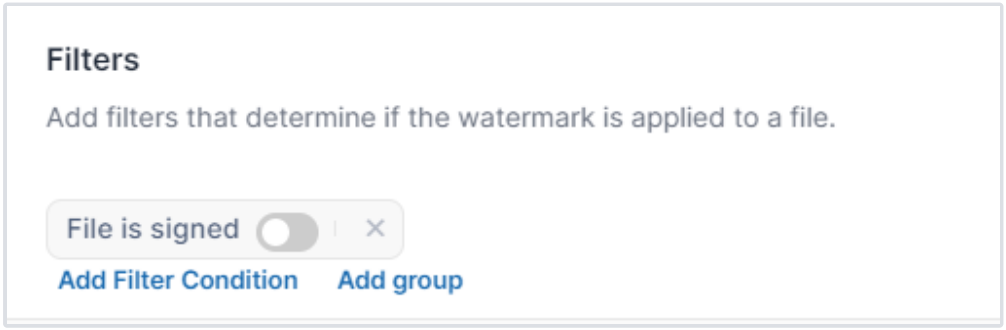
To enable users to download signed files, when creating your filter for watermarks, either:

- Omit digitally signed files but allow other eSigned files by including the option **File has digital signature** and setting it to false:



OR

- Omit both digitally signed files (if they are present) and other eSigned files by including the option **File is signed** and setting it to false:



Customizing preview IDs

Note: Preview IDs are the alphanumeric codes that appear in watermarks on both previews and downloads.

Use the following two parameters to customize the preview ID size and length:

Parameter	Description
define("TONIDOCLOUD_PREVIEW_ID_SIZE", "small");	The length of the preview ID. The possible values are **small**, **medium** and **large**. If you are using the default value for TONIDOCLOUD_PREVIEW_ID_CUSTOM_DICTIONARY the values will show preview ID's with the following lengths: **small** - (default) 11-12 character preview ID **medium** - 21-22 character preview ID **large**: - 43 -44 character preview ID
define("TONIDOCLOUD_PREVIEW_ID_CUSTOM_DICTIONARY", "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-_");	The characters that may be used in the preview id. The characters in the example to the left are the default value.

To customize ^PREVIEW_ID^ size and length:

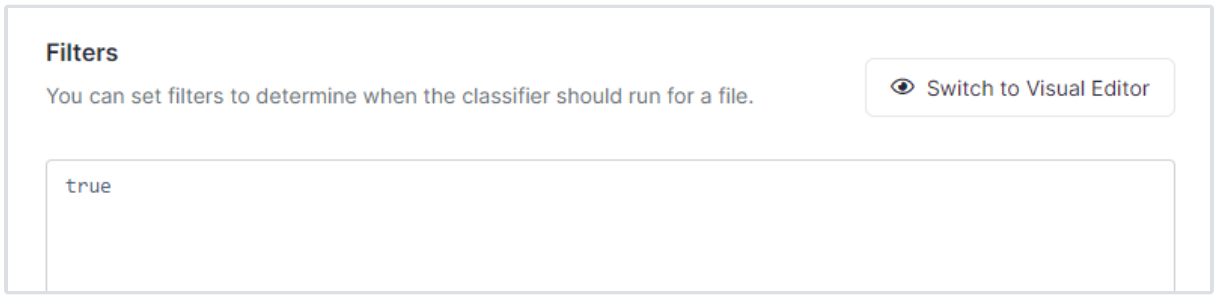
1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the above parameters with custom values:

```
define("TONIDOCLOUD_PREVIEW_ID_SIZE", "medium");
define("TONIDOCLOUD_PREVIEW_ID_CUSTOM_DICTIONARY", "0123456789ABCDEF");
```

Watermark Parameters for Code Editor

If you are an advanced user, you can use the code editor in the Add Watermark Rule wizard to write your conditions for adding watermarks to files. With the code editor, you can create conditions that are more complex and can use a wider range of parameters.

Note: To indicate in the code editor that you want to include the watermark on all files, enter the word **true**



Parameter	Description	Sample returned value
File Information		
'_file.path'	The full path of the file being accessed	'_file.path == '/myuser/mydir/myfile.pdf''
'_file.pathStartsWith(start)'	Returns `true` if the file path starts with the given string	'_file.pathStartsWith('/confidential/')'
'_file.ext'	The file extension (without the dot)	'_file.ext == 'pdf''
'_file.extIs(extensions)'	Returns `true` if the file extension matches the given value or any value in the given array	'_file.extIs(['pdf', 'docx'])'
'_file.pathContains(text)'	Returns `true` if the file path contains the given string	'_file.pathContains('/legal/')'
'_file.pathMatches(pattern)'	Returns `true` if the file path matches the given pattern. Supports `*` (any characters) and `#` (any single character) wildcards	`_file.pathMatches('/myuser/reports/*')`

Parameter	Description	Sample returned value
'_file.fileNameContains (text)'	Returns `true` if the file name (last segment of the path) contains the given string	'_file.fileNameContains('mrn')'
User information		
'_user.anonymous'	Returns `true` if the user is anonymous (not authenticated)	'_user.anonymous == true'
'_user.username'	The username of the authenticated user	'_user.username == 'john.doe''
'_user.email'	The email address of the authenticated user	'_user.email == 'john.doe@mail.com''
'_user.userType'	The user's account type. Possible values: 'Full Access', 'Limited Access', 'Guest Access', 'Master Admin' **Note**: Formerly, External users were referred to as Limited users; however, the DLP rule expression still requires the use of the value 'Limited Access' to refer to External users.	'_user.userType == 'Guest Access''
'_user.groups'	Array of group names the user belongs to	''Finance' in _user.groups'
'_user.inGroup(groupName)'	Returns `true` if the user belongs to the specified group	'_user.inGroup('managers')'
'_user.isMasterAdmin'	Returns `true` if the user is the primary admin	'_user.isMasterAdmin == false'
'user.isEmailInDomain(domain1, domain2, . . .)'	Returns `true` if the user's email belongs to any of the specified domains	'_user.isEmailInDomain('example.com', 'mail.com')'
Request information		

Parameter	Description	Sample returned value
'_request.remoteIp'	Returns the IP address of the incoming request	'_request.remoteIp == '43.12.45.78''
'_request.isAdminLogin'	Returns `true` if the request is made by an admin user	'_request.isAdminLogin == true'
'_request.agent'	The client agent type. Possible values: 'Cloud Drive', 'Cloud Sync', 'Web browser', 'Android', 'iOS', 'MS Outlook', 'MS Office', 'Unknown'	'_request.agent == 'Web browser''
'_request.inIpv4Range(lowIp, highIp)'	Returns `true` if the request IP is within the given IPv4 range (inclusive)	'_request.inIpv4Range('138.204.26.254', '138.204.26.1')'
'_request.inIpV4CidrRange(cidrRange)'	Returns `true` if the request IP matches the given CIDR range	'_request.inIpV4CidrRange('138.204.26.254/24')'
'_request.remoteCountryCode'	Two-character ISO country code of the requester **Note**: To use this expression, the **Show Geo IP Chart** setting in the **Settings > Admin** screen must be set to **TRUE**.	'_request.remoteCountryCode == 'US''
User policy information		
'_policy.id'	The ID of the policy applied to the user	'_policy.id == 'abc123''
'_policy.name'	The name of the policy applied to the user	'_policy.name == 'Human Resources''
'_policy.default'	Returns `true` if the user is under the default policy	'_policy.default == true'
'_policy.exists(policyKey)'	Returns `true` if the policy key exists and is enabled	'_policy.exists('SHARE_ALLOW_PUBLIC')'

Parameter	Description	Sample returned value
'_policy.getValue(policyKey)'	Returns the string value of the policy key, or an empty string if not found	'_policy.getValue('MAX_UPLOAD_SIZE') == '100''
'_policy.getFlag(policyKey)'	Returns the boolean value of the policy key, or `false` if it is not a flag	'_policy.getFlag('ALLOW_DOWNLOAD') == false'
Share information		
Note: In any of the expressions including **share.path**, specify the original path of the shared file (for example / user1/textfile1.txt), not the path in the Shared with Me folder (for example, /SHARED/user1/textfile1.txt)		
'_share.path'	The path of the share	'_share.path == '/myuser/mydir''
'_share.owner'	The username of the share owner	'_share.owner == 'alice''
'_share.public'	Returns true if the share is public (no authentication required)	'_share.public == true'
'_share.onlyAllowedEmails(email1, email2, ...)`	Returns `true` if all allowed users match the given emails. Supports wildcard `*@domain.com`	'_share.onlyAllowedEmails('*@acme.com', 'partner@external.com')'
'_share.allowedUsers'	Array of email addresses of users explicitly allowed in the share	''john.snow@mail.com' in _share.allowedUsers'
'_share.allowedGroups'	Array of group names allowed in the share	''Contracors' in _share.allowedGroups'
'_share.hasUsersFromDomain(domain1, domain2, . . .)'	Returns `true` if **any** allowed user belongs to one of the specified domains	'_share.hasUsersFromDomain('gmail.com')'

Parameter	Description	Sample returned value
'_share.onlyUsersFromDomain(domain1, domain2, . . .)'	Returns `true` if **all** allowed users belong to the specified domains ⚠ Do not use this expression in an OR condition with another expression; this could cause shares to be denied unintentionally. Instead use _share.onlyAllowedEmails with a wildcard. For example, instead of: (_share.onlyUsersFromDomain('gmail.com') || _share.onlyAllowedEmails('testuser@test.com')) use: _share.onlyAllowedEmails('*@gmail.com','testuser@test.com')	'_share.onlyUsersFromDomain('mycompany.com')'
'_share.pathStartsWith(start)'	Returns `true` if the share path starts with the given string	'_share.pathStartsWith('/myuser/mydir')'
'_share.pathContains(text)'	Returns `true` if the share path contains the given string	'_share.pathContains('/reports/')'
'_share.pathMatches(pattern)'	Returns `true` if the share path matches the pattern. Supports `*` and `#` wildcards	'_share.pathMatches('/myuser/*/public')'
File metadata		

Parameter	Description	Sample returned value
Note: When you set a _metadata rule, the metadata set and the attribute specified cannot contain periods within their names. For example, cce.pii is valid, but cce.x.pii.y is not valid.		
'_metadata.exists(metadataPath)'	Returns `true` if the metadata attribute exists on the file	'_metadata.exists('cce.pii')'
'_metadata.existsAll(metadataPath)'	Returns `true` if all files in the current path have the metadata attribute	'_metadata.existsAll('cce.sensitive')'
'_metadata.existsWithValue(metadataPath, value)'	Returns `true` if the metadata attribute exists and equals the given value	'_metadata.existsWithValue('content.category', 'confidential')'
'_metadata.existsWithValueInArray(metadataPath, value)'	Returns `true` if the metadata attribute is an array containing the given value	'_metadata.existsWithValueInArray('content.categories', 'pii')'
'_metadata.existsWithCondition(metadataPath, operator, value)'	Returns `true` if the metadata attribute satisfies the condition. Supported operators: `==`, `!=`, `<>`, `>`, `<`, `>=`, `<=`, `in`	'_metadata.existsWithCondition('cce.score', '>=', '80')'
Signed files		
_metadata.exists("Signority eSignature.Digital Signature")	Returns `false` if the file is not digitally signed or eSigned. Used to prevent watermarks on signed files to enable download.	_metadata.exists("Signority eSignature.Digital Signature") == false
_metadata.existsWithValue("Signority eSignature.Digital Signature", true)	Returns `false` if the file is not digitally signed Used to prevent watermarks on digitally signed files to enable download.	_metadata.existsWithValue("Signority eSignature.Digital Signature", true) == false

Email Settings

Beginning with version 23.253, you may automatically embed QR codes in share emails. To configure automatic embedding of QR codes, see (23.263a) Email Templates .

Beginning with version 23.241.1, Azure XOAUTH XMTP with GCC High is supported.

Microsoft is replacing basic authentication with oAuth for emails sent using Office 365 in 2023. To address this change, beginning with version 22.1.1, FileCloud supports oAuth as an SMTP authentication method. To use SMTP oAuth with FileCloud, you must use Azure as an authorization provider.

FileCloud can send various messages to users via email, including:

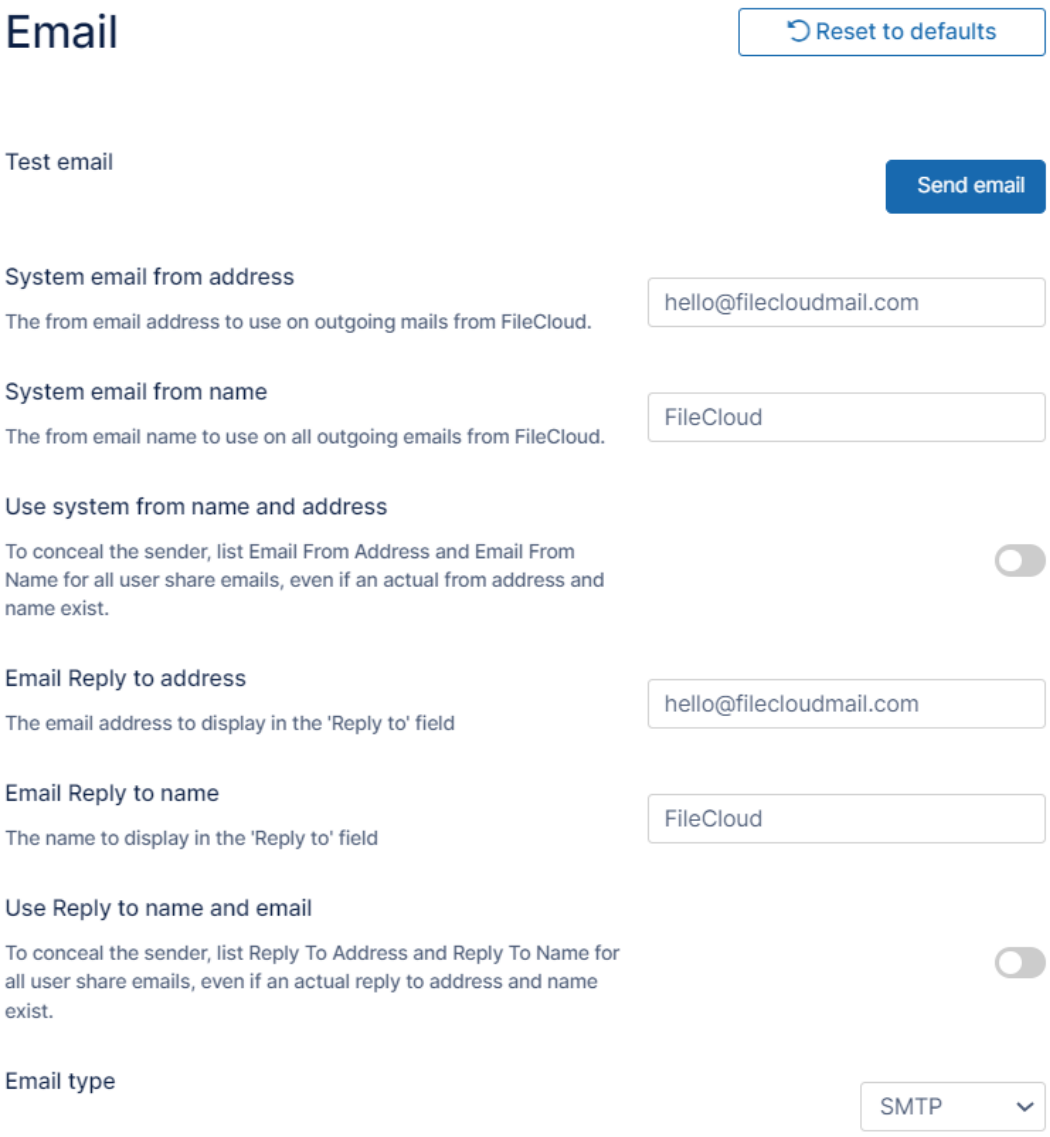
- share notifications
- file change notifications
- error notifications

For email to work smoothly with your system, configure the Email Settings below.

To configure email settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Email** .
   The **Email** settings page opens.
   The general settings on the page begin with **System email from address** and go through **Email type**, as shown in the screenshot below.

2. Fill in the settings as shown in the following screenshot, using the table below as a guide.



General email setting information:

Setting	Description
System email from address	By default, **System email from address** is listed on emails if there is no email from address (for example, when emails are sent by the system or by workflows). If you are using **SMTP** as your email type, and set **SMTP AUTH type** (listed below, under **SMTP Configuration**) to **XOAUTH2**, then set **System email from address** to the same value as **SMTP AUTH username**. This is required for successful use of Azure as the authentication provider.
System email from name	By default, **System email from name** is listed as the from display name from which email messages are sent to users. It is used if there is no email from name (for example, when emails are sent by the system or by workflows).
Use system from name and address	To conceal the sender, list the **System email from address** and **System email from name** for all user share emails, even if an actual from address and name exist.
Email Reply to address	By default, **Email Reply to address** is listed on emails if a reply to address does not exist (for example, when emails are sent by the system or by workflows).
Email Reply to name	By default, **Email Reply to name** is listed on emails when a recipient replies to an email without a reply to name (for example, when emails are sent from the system or by workflows).
Use Reply to name and address	To conceal the sender, list **Email Reply to address** and **Email Reply to name** for all user share emails, even if an actual reply to address and name exist.
Email Type	Specify the email facility to be used. The type can be **SMTP**, **Mail** or **SendMail**. Note that **Mail** and **SendMail** use the underlying OS's function (and are available only for Debian/Ubuntu installation). The recommended setting is **SMTP**.

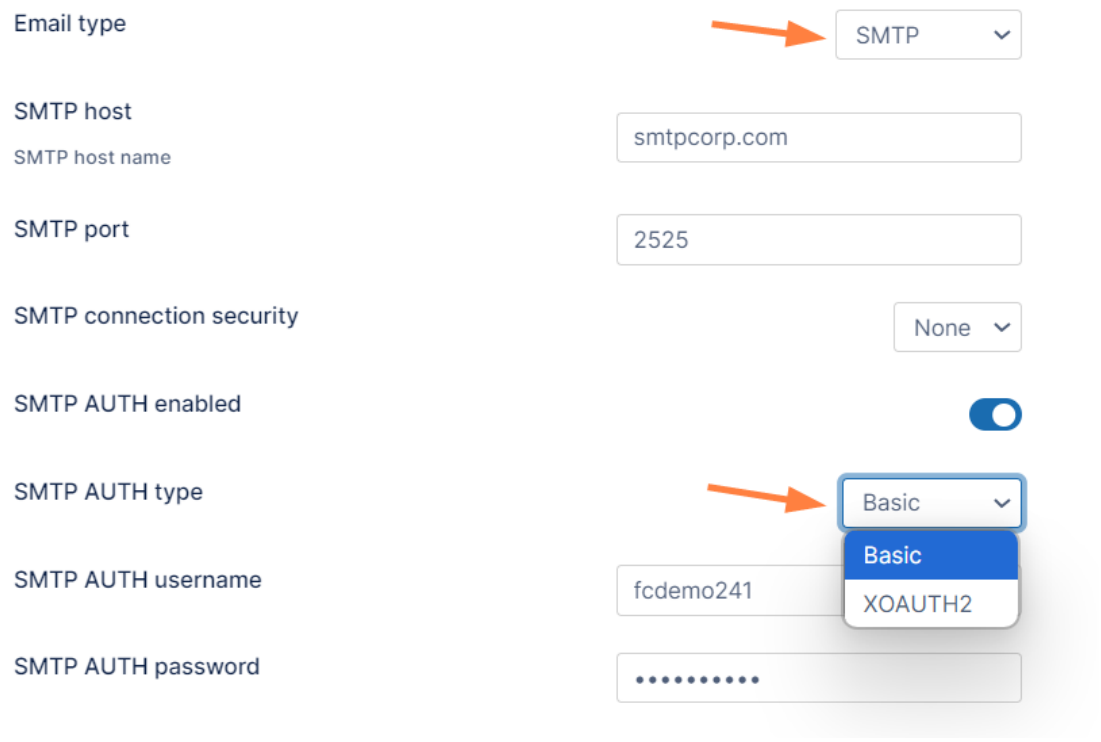
3. If you choose **SMTP** for **Email Type**, complete the following steps for filling in the SMTP fields. If you choose **Mail** or **SendMail** for **Email Type**, skip these steps, and go to Do Not Email Settings.

SMTP Configuration

Note: You must have an SMTP account to set up email using SMTP.

To configure SMTP in Email settings:

1. In **Email Type**, choose **SMTP**.
   The SMTP fields below it become enabled.



2. Fill in the SMTP fields according to the descriptions in the following tables.
   The value you choose for **SMTP Auth Type** determines which additional SMTP fields are displayed below.

> **Office 365 Settings**
> When using Office 365, SMTP settings must be set to the following values:

Setting	Recommended value
SMTP host	smtp.office365.com

Setting	Recommended value
SMTP port	587
SMTP connection security	TLS
SMTP AUTH username, SMTP AUTH password	Enter the sign in credentials of the hosted mailbox being used.

For more information about SMTP configuration for Office 365 accounts see the Microsoft Office Support Article.

SMTP Setting	Description
SMTP Host	SMTP Server to use for sending email
SMTP Port	The SMTP port to use to connect to SMTP Host (provided by your SMTP provider)
SMTP Security	If your SMTP provider uses SSL or TLS security then select the appropriate value.
SMTP AUTH enabled	If SMTP requires authentication, then check this to enable and enter the authentication settings.
SMTP AUTH type	**SMTP Auth Type** may be **Basic** or **XOAUTH2**. The option you choose determines which additional SMTP fields follow. • **Basic** authentication requires the user to enter a username and password. It is supported by many email providers, but is being deprecated in Microsoft 365 in Exchange Online in early 2023. • **XOAUTH2** refers to OAuth 2.0 authentication, which uses temporary single-use tokens to provide a more secure method of verification. XOAUTH2 will now be used with Microsoft 365 for Exchange Online and is also the method used by a number of other providers.

If you choose **Basic** for **SMTP Auth Type**, enter values for the following fields:

Field	Value to enter
SMTP AUTH username	The authentication username.

SMTP AUTH password	The password for SMTP AUTH username.

If you choose **XOAUTH2** for **SMTP Auth type**:

a. Review the following information.

> ⚠ XOAUTH2 token generation must be performed by the FileCloud master admin and not by a promoted admin user.
> To avoid configuration issues with Microsoft 365 XOAUTH2 setup due to Azure permissions settings, we recommend the following:
> **If you are able to use an Azure global admin as the SMTP AUTH username in FileCloud**:
>
> i. Use an Azure global admin account to create the FileCloud XOAUTH2 application.
> ii. Use the same Azure global admin account in the FileCloud email settings **System Email from address**, **Email Reply to address**, and **SMTP AUTH username**.
> iii. Use the Azure global admin account to grant permissions when generating the XOAUTH2 token.
>
> **If you are not able to use an Azure global admin as the SMTP AUTH username in FileCloud**:
>
> i. Use an Azure global admin account to create the FileCloud XOAUTH2 application.
> ii. Do not use the same Azure global admin account for the FileCloud email settings **System Email from address**, **Email Reply to address**, and **SMTP AUTH username**, but do set all three of these fields to a single email address.
> iii. Assign the email entered into **SMTP AUTH username** to the FileCloud XOAUTH2 application:
>
> 1. Log into **portal.azure.com** and go to **Microsoft Entra ID > App registrations**.
> 2. Click the FileCloud XOAUTH2 application, and in the navigation panel, click **Roles and administrators**.
> 3. Click **Cloud Application Administrator**, and then click **Add assignments** and assign the FileCloud **SMTP AUTH username** to the FileCloud XOAUTH2 application.
>
> iv. Use the **SMTP AUTH username** to grant permissions when generating the XOAUTH2 token.
>
> **If neither of the above options work, confirm that SMTP AUTH is enabled for the SMTP AUTH username and your Organization**:
> To check if SMTP AUTH is enabled for the **SMTP AUTH username**:
>
> i. Open Microsoft 365 admin center and go to **Users > Active Users** and check the **SMTP Auth User**.
> ii. In the right panel, click **Mail**, and then click **Manage Email** apps.
> iii. If **Authenticated SMTP** is not checked, check it.

To check if SMTP AUTH is enabled for your **Organization**:

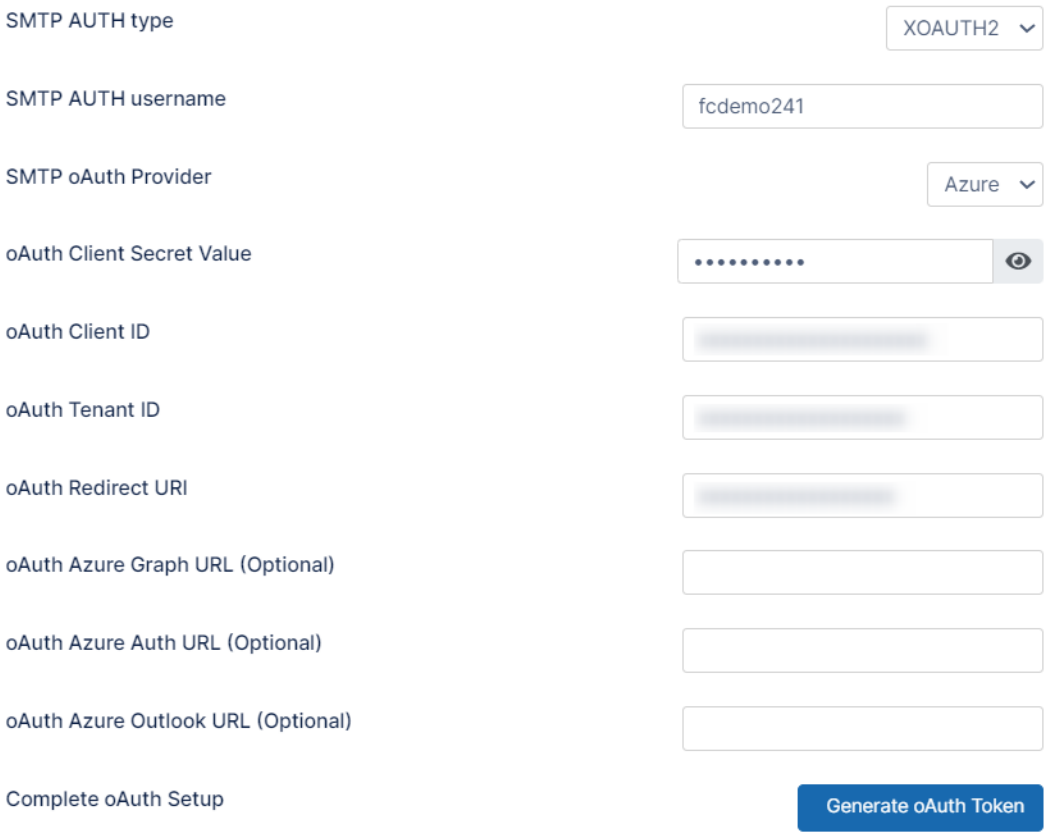
i. Go to the Microsoft Exchange admin center and click **Settings**, then click **Mail flow.**

ii. If **Turn Off SMTP Auth Protocol for your Organization** is not checked, check it and click **Save.**

If none of these options work, contact Microsoft Support for help.

b. Go to the page Microsoft Azure and XOAUTH2 setup guide and follow the instructions under **Configure an OAuth2 app in Microsoft Azure** to register your oAuth application in portal.azure.com.

c. In the **Email** settings page, scroll down to **SMTP Auth type** and the **oAuth** fields.

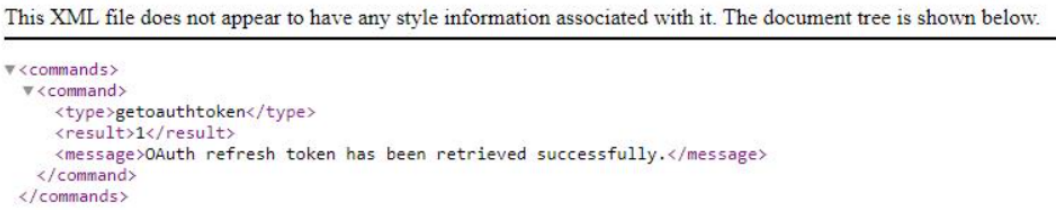


d. Fill in the SMTP oAuth fields on the Email Settings page listed in the table below:
For the fields **oAuth Client Secret Value**, **oAuth Client ID**, **oAuth Tenant ID**, and **oAuth Redirect URI** , retrieve the values from portal.azure.com after registering the oAuth application.

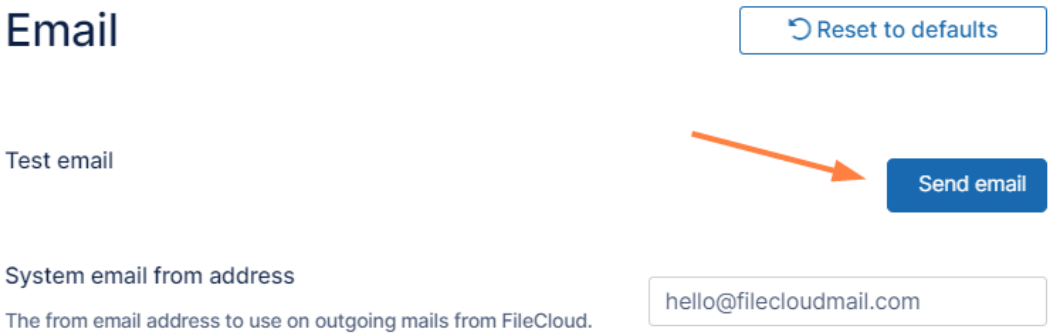
SMTP Auth User	Enter the authentication username You must set **Email From Address** (described above under **General email setting configuration**) to the same value as **SMTP Auth User**. This is required for successful use of Azure as the authentication provider.
SMTP oAuth Provider	Choose the oAuth provider (authorization server). Currently, the only available option is **Azure**.
oAuth Client Secret Value	The secret key your FileCloud system uses to get a temporary token from the authorization server.
oAuth Client ID	Application (client) ID from the SMTP provider application. This ID is used to get the temporary token from the authorization server.
oAuth Tenant ID	Directory (tenant) ID used to get the temporary token from the authorization server. (This field is applicable only when Azure is the provider; when other providers are added, it will not be required for them.)
oAuth Redirect URI	The location (appended with the parameter holding the token) where the authorization server should send the user after the token has been generated. The location specified should be your FileCloud domain. Use the format https://your-filecloud-domain.com/admin/getoauthtoken

oAuth Azure Graph URL oAuth Azure Auth URL oAuth Azure Outlook URL	⚠ **Required**: If you are using Azure XOAUTH SMTP with GCC High, fill in these fields as follows: oAuth Azure Graph URL (Optional) https://graph.microsoft.us oAuth Azure Auth URL (Optional) https://login.microsoftonline.us oAuth Azure Outlook URL (Optional) https://outlook.office365.us If you are using Azure XOAUTH SMTP without GCC High, these settings default to the correct values for the non-GCC High setup, and it is not necessary to enter them. However, you may enter the correct values, which are: https://graph.microsoft.com https://login.microsoftonline.com https://outlook.office.com
Complete oAuth Setup	Click **Generate oAuth Token** so you can begin using email with oAuth.

e. If your **SMTP AUTH type** is **XOAUTH2**, do the following:
After you have filled in the SMTP fields, click **Generate OAuth Token**.
If you are not logged in to your Microsoft authenticator app, you are prompted to log in so you can access Azure to generate the token.
Once the OAuth token is generated, the following XML appears on your screen:



3. Click **Send email** at the top of the screen to test the settings.



If your setup is valid, the email is sent to the admin's email, and a success notification appears on your screen.

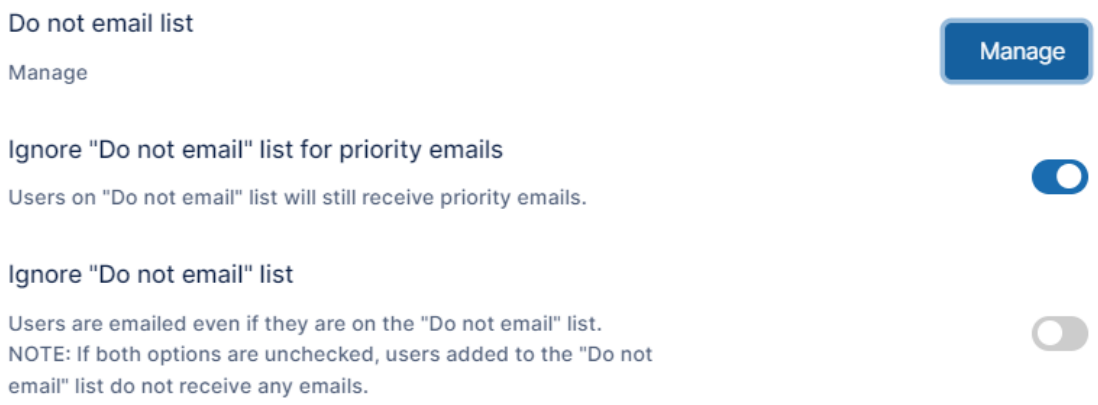
Do Not Email Settings

- Emails get added to the **Do not email** list when users click **unsubscribe** in the email body.
- Beginning with FileCloud version 20.3, admins can add or remove users from the **Do not email** list by clicking **Manage** beside **Do not email list**.
- Admins can specify the maximum number of emails that system can send in a 24 hour span.
- Users on the **Do not email** list do not receive any emails unless **Ignore "Do not email" list for priority emails** or **Ignore "Do not email" list** are checked.

To send emails to users on the Do not email list

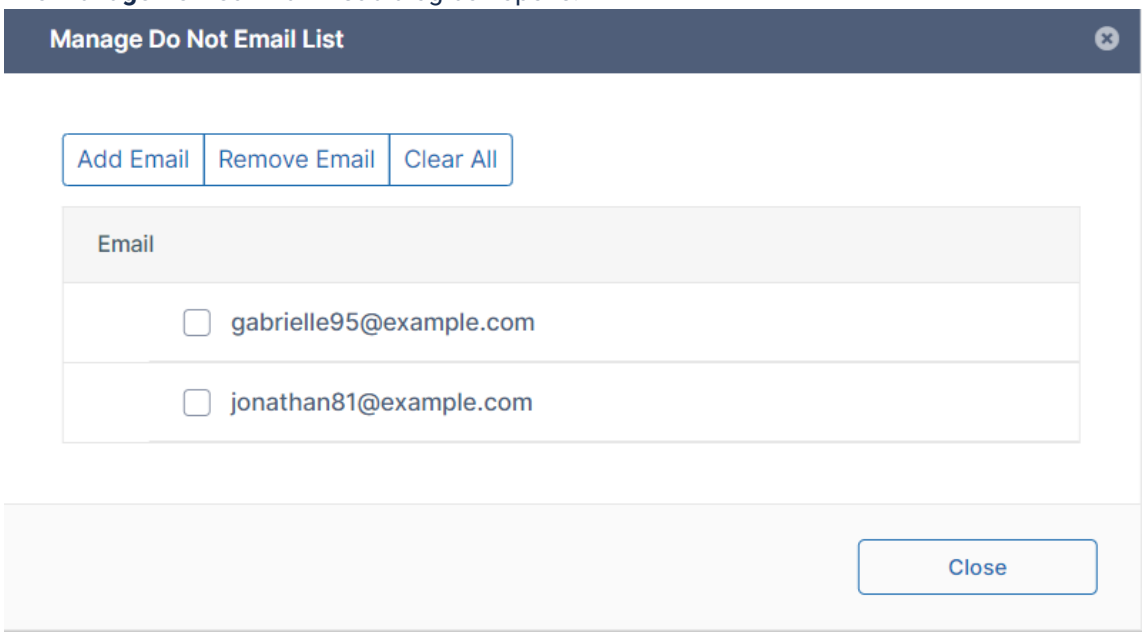
By default, users on the **Do not email** list do not receive any emails

- To allow users on the **Do not email** list to receive important emails like password recovery and 2FA, check the **Ignore "Do not email" list for priority emails** checkbox .
- To ignore the **Do not email** list and send all emails to users who are on the list., check the **Ignore "Do not email" list** checkbox.



To add or remove users from the Do Not Email list:

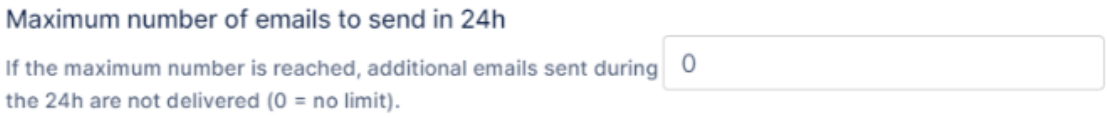
1. Next to **Do not email list**, click **Manage**.
   The **Manage Do Not Email List** dialog box opens.



2. To add an email to the list, click **Add Email**, then enter and save an email address.
3. To remove an email from the list, check the box next to the email and click **Remove Email**.

To limit the number of emails sent to a user

If your users are receiving too many email notifications, you can limit the number of FileCloud system-generated emails sent to them in 24 hours.
In the field **Maximum number of emails to send in 24h** at the bottom of the **Email** settings page, enter the maximum number of system emails to be sent each user per day.



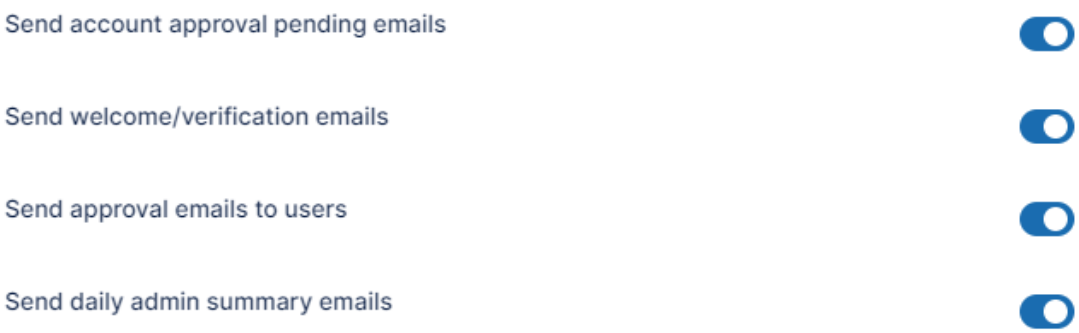
Configuring System Generated Emails

Controlling System Generated Automatic Emails

It is possible to control which emails are sent by the system.

To change the email settings:

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 the email settings, and enable or disable the settings to send or not send the specific email types.



Send account approval pending emails	Send an approval pending email to the admin when a new user account is created and admin approval is required.
Send welcome/ verification emails	Send verification emails to users to verify their email addresses.
Send approval emails to users	Send account approval emails to users.
Send daily admin summary emails	Send daily system summary emails to the main admin account, This only works if a Cron Task or Windows Task Manager is setup.

3. Click **Save**.

Change the frequency of Admin summary emails

By default, an Admin summary email is sent to the FileCloud Admin once per day. However, you can configure your system to send it weekly or monthly instead.

To change the frequency of Admin summary emails:

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_ADMIN_SUMMARY_EMAIL_FREQUENCY', 'DAILY');
```

3. Change the value of **DAILY** to **WEEKLY** or **MONTHLY**.

Endpoint Backup Settings

FileCloud lets you configure automatic backup settings for users' files and folders to ensure their data is secure.

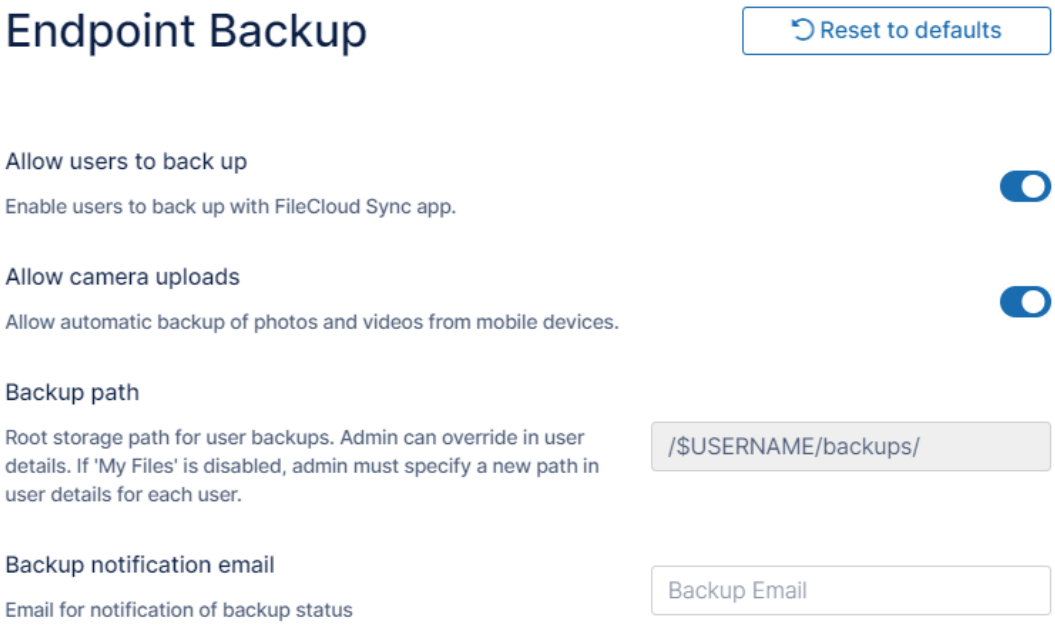
Note: FileCloud supports backing up files and photos from different devices.

What Do You Want To Do?

Configure backup settings for all users

To configure the backed up settings for all users:

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. Fill in the settings as shown in the following screenshot using the table below as a guide.



Settings Name	Description
Allow users to back up	Allow users to back up files and folders using the FileCloud Sync app. See Backing Up Files. This setting also enables you to configure Sync backup of specific files and folders for all users. See Globally Backing Up User Files and Folders.
Allow camera uploads	Allow mobile clients to automatically back up photos and videos to their FileCloud accounts. Turning off this setting prevents this server from being used to back up audio/video files. All camera uploads are stored in the user's backup folder. This location cannot be changed. For example, if the user name is jdoe, the camera uploads are stored in /jdoe/backups/<phone name>
Backup path	The location where automatically updated media and backup files are stored. This is a read-only field meant for display only. You can override this path for specific users to have them back up to a different location in the **User Details** screen (see below).
Backup notification email	An additional email ID to which Backup Complete notifications are sent.

Configure a specific user's backup folder

It is possible to set a different backup folder path for each user, overriding the default global path specified.

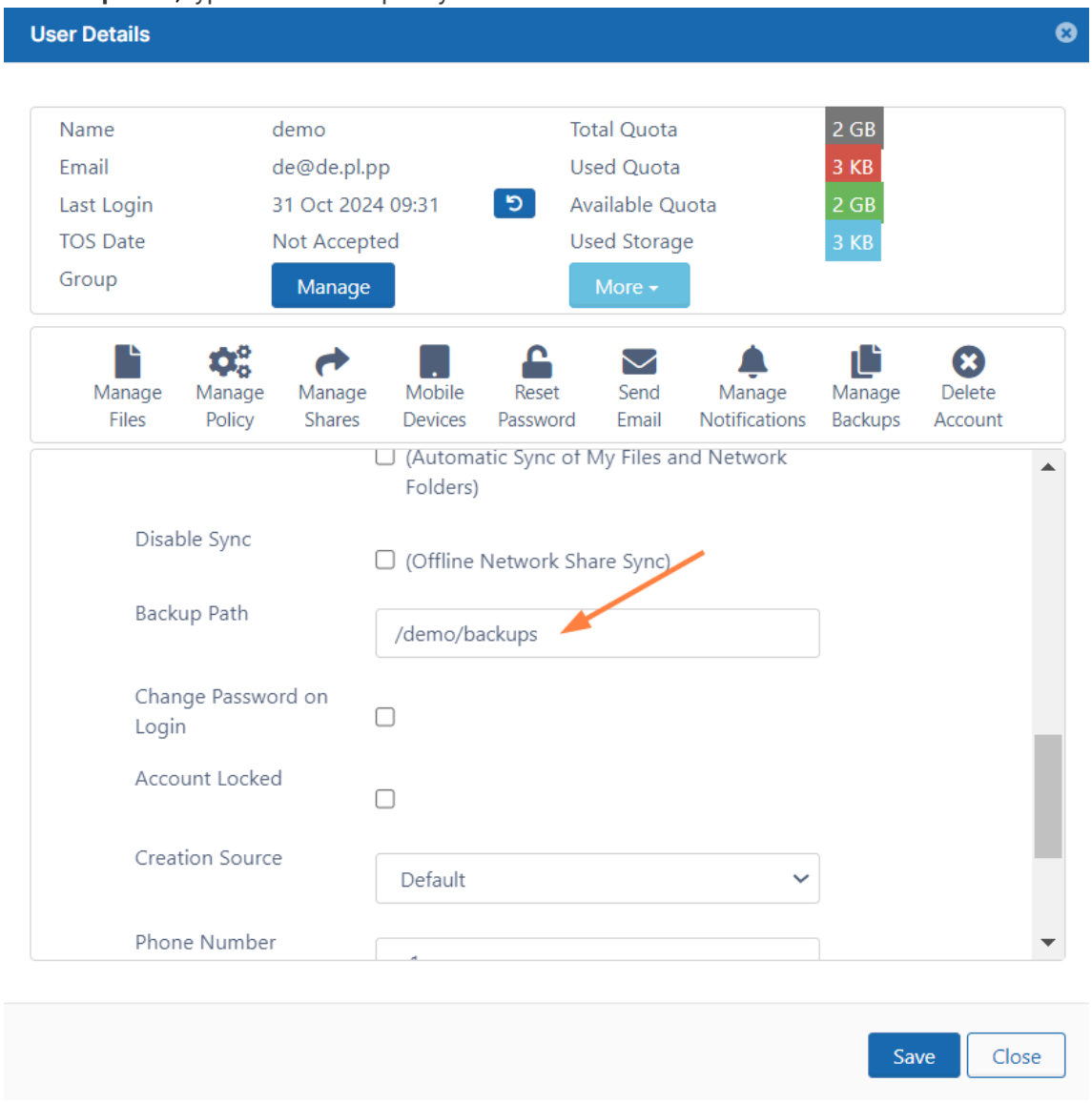
You must know the exact folder path you want to use.

For more information, see Identifying a FileCloud Specific Path.

To set the Backup Path for a user:

1. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Users**.
3. Click the **Edit** icon for the user whose path you want to change.
4. On the **User Details** screen, scroll down to the **Backup Path** field.

5. In **Backup Path**, type in the folder path you want to use.

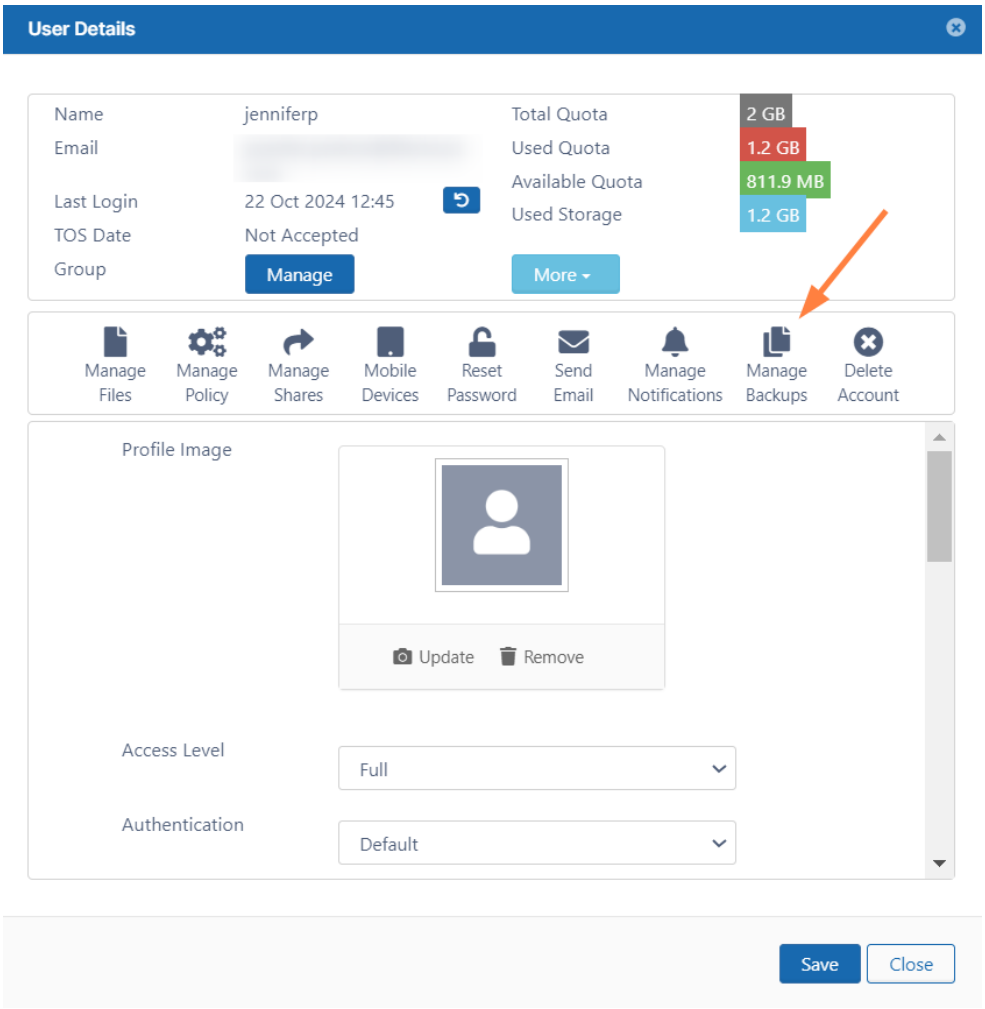


6. To save your changes, click **Save**.

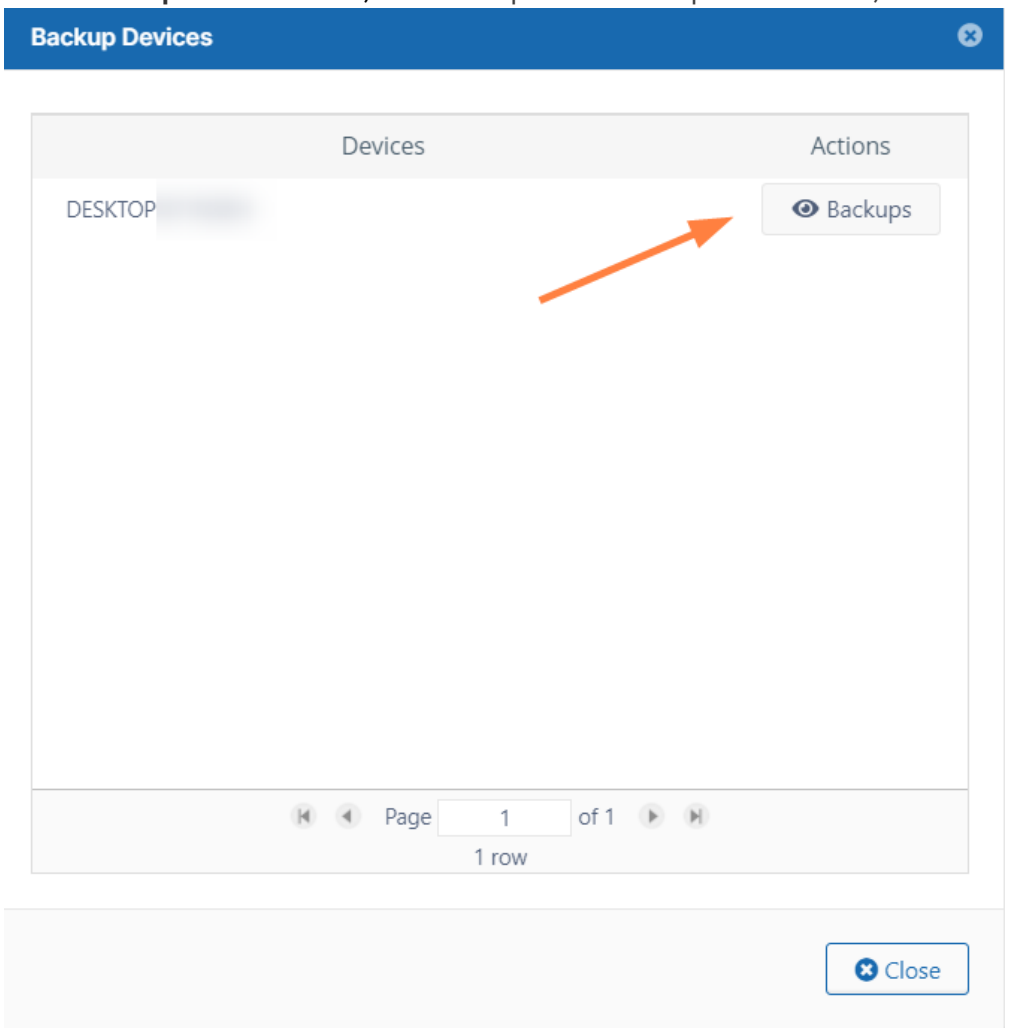
View a user's backed-up files

To view details of the backed up files for a specific user:

1. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Users**.
3. Click the **Edit** icon for the user whose path you want to change.
4. On the **User Details** screen, click **Manage Backups**.

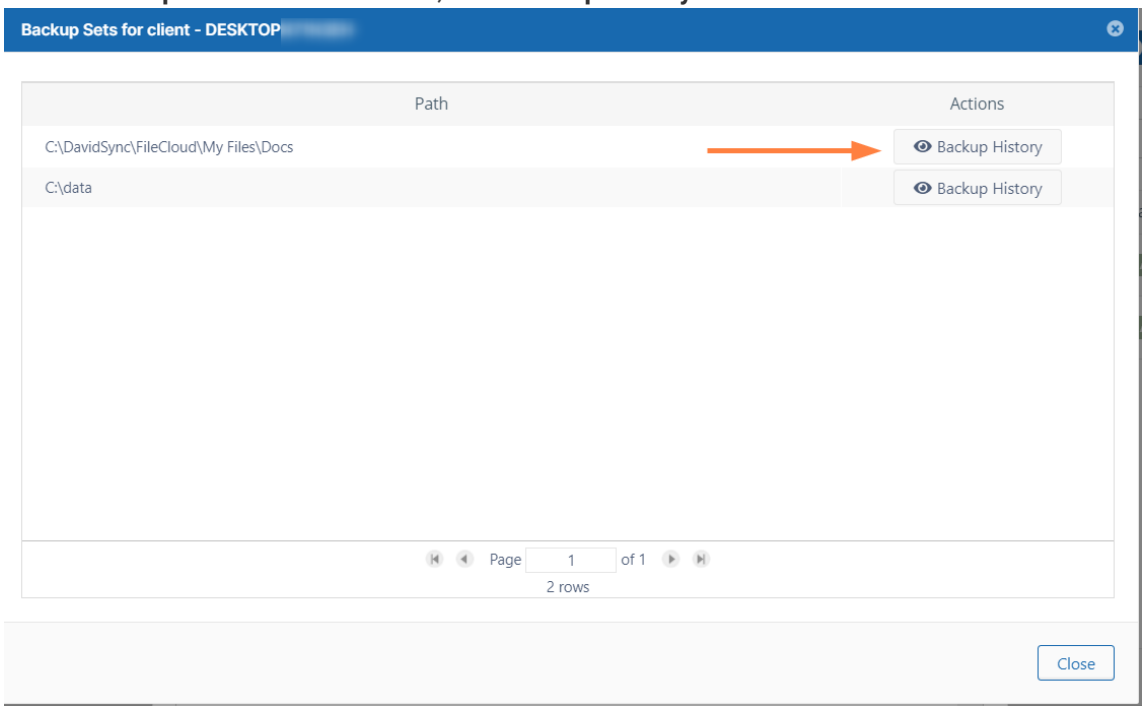

User Details
Name
jenniferp
Email
Last Login
22 Oct 2024 12:45
TOS Date
Not Accepted
Group
Manage
Total Quota
2 GB
Used Quota
1.2 GB
Available Quota
811.9 MB
Used Storage
1.2 GB
More
Manage Files
Manage Policy
Manage Shares
Mobile Devices
Reset Password
Send Email
Manage Notifications
Manage Backups
Delete Account
Profile Image
Update
Remove
Access Level
Full
Authentication
Default
Save
Close

5. On the **Backup Devices** screen, to view the paths backed up from a device, click **Backups.**

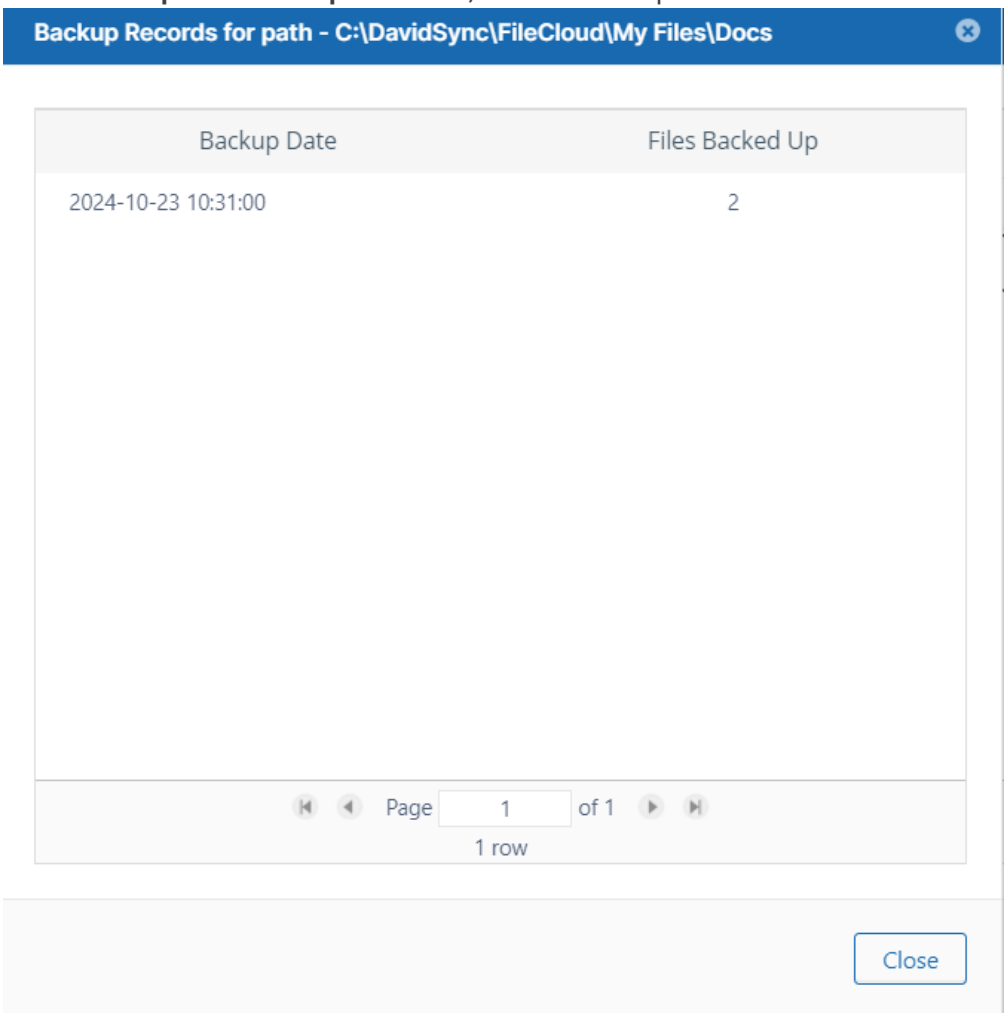


.

6. On the **Backup Sets for client** screen, click **Backup History** for a client.



7. On the **Backup Records for path** screen, view the backup dates and number of files backed up.



Also see:

Automatic Database Backup

> In environments where high availability architecture is being used, automatic backups are performed during Cron runs.

By default, automatic database backups are enabled with the following configuration:

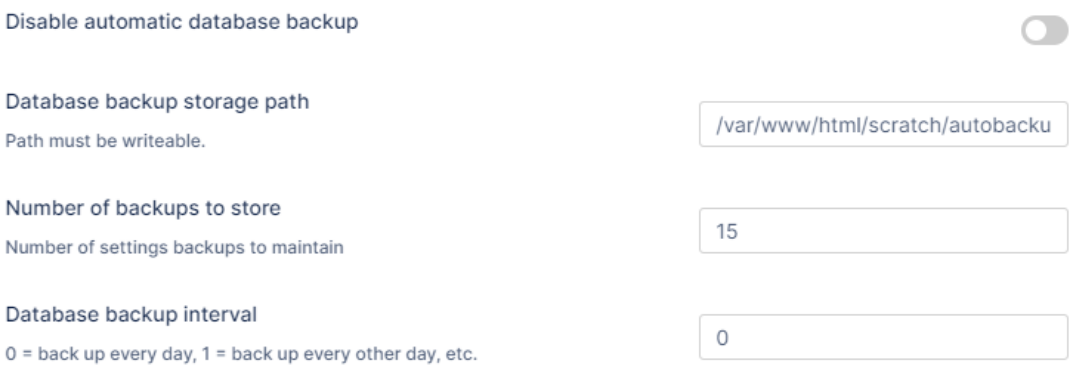
- Daily backups are stored in the following directory: .../scratch/autobackups/
- Backups are maintained for the last 15 days before being overwritten with new backups

The auto backup function requires the Cron function to be working properly.
Cron is a requirement for FileCloud Server in general, so you should already have this service running.
If you have not done this yet, Set up Cron.

As an administrator, you can change the location where backups are stored, the number of backups to maintain, and the number of days between backups. Or, if you already have a back-up strategy, you can disable automatic backups.

To configure automatic database backups:

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. Scroll down to the backup settings and modify them depending on your system's needs.



Disable automatic database backup - Enable to prevent database back up during a Cron run. When disabled, automatic backup runs, and the last automatic backup run date is displayed.

Database backup storage path - The path to the directory where backed-up database files are saved. You must use a path that is accessible to the FileCloud server, can have files saved to it, and has enough room for the backup files

Number of backups to store -The number of days you want stored in a single backup file. By default, each backup file contains 15 days worth of data. If you want smaller files, you can lower this number. For example, if you type in 2 for **Number of backups to store**, the backup file will only contain 2 days worth of data. After those 2 days, the backup file is overwritten to store the next 2 days worth of data. This setting controls how far back you can recover data.

Database backup Interval - The interval in days between each backup. The default is 0 which creates a daily backup of the number of days set in **Number of backups to store**.

3. Click **Save**.

Example

The Cherry Road Real Estate company needs to back up data from the last 30 days and wants the back-up refreshed every week. To do this, these are the settings they use:

- **Disable automatic database backup** = not selected
- **Database backup storage path** = /var/scratch/autobackups
- **Number of backups to store** = 30
- **Database backup Interval** = 7

Setting Up Persona Backup Using Sync

As an admin, you can use the FileCloud Sync app to set up a persona backup for all users of your FileCloud System. A persona backup saves individual settings and preferences for users across their FileCloud devices, making it easy for you to restore them.

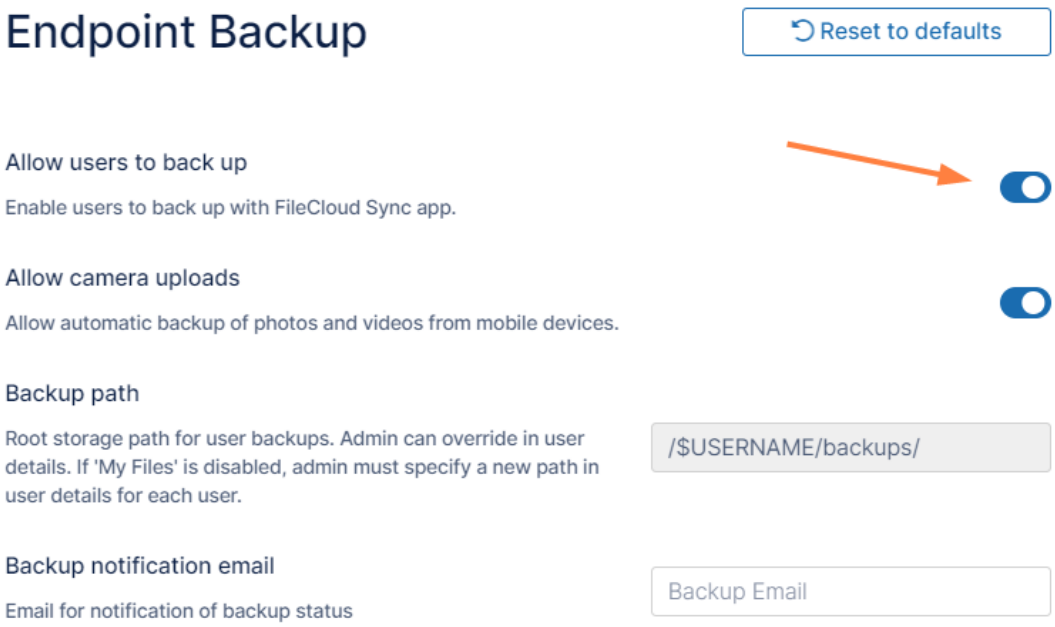
To set up persona backup for users, open the policy used by them in the admin portal, and add device configuration code for Sync backup that includes the local paths that contain user specific configurations.

Steps:

1. Enable Endpoint Backup for FileCloud Sync from the Admin Portal.
2. Install FileCloud Sync on the users' computers, and enable Remote Management in Sync.
3. Set a default device configuration for Sync in the users' policy from the admin portal.

1) Enable Endpoint Backup for FileCloud Sync from the Admin Portal

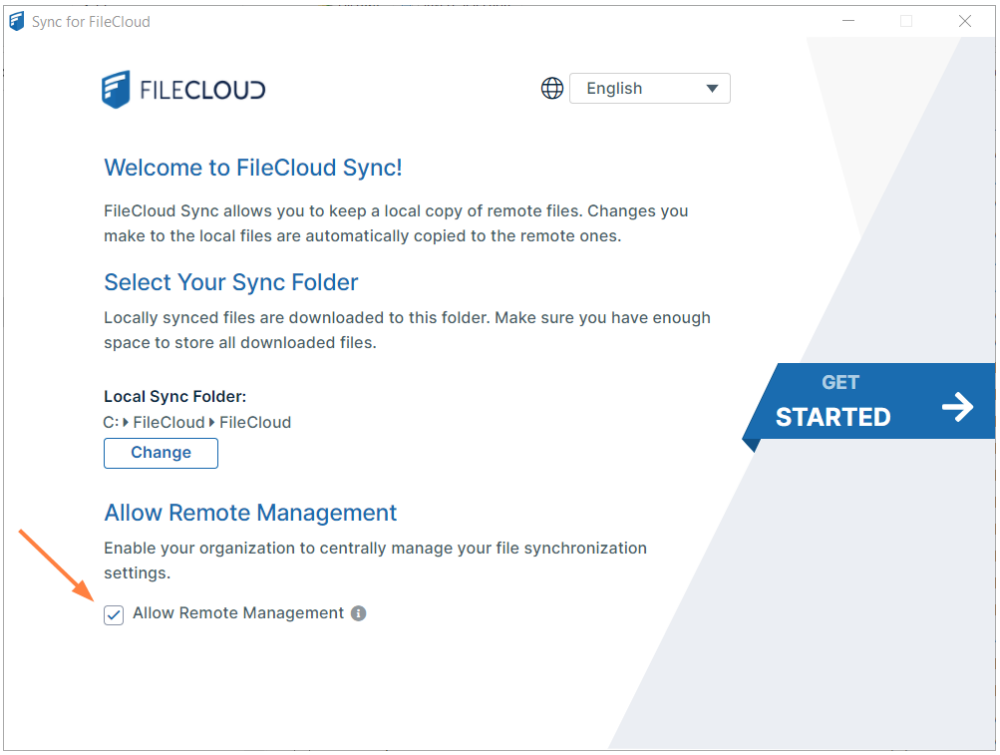
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Endpoint Backup**  .
   The **Endpoint Backup** settings page opens.
2. Enable the **Allow Users To Backup** option, and click **Save**.



2) Install FileCloud Sync and enable Remote Management

For backup to take place using the device configuration set up in the policy, Remote Management must be enabled in the FileCloud Sync App. This can be done by either:

- The user manually enabling the option in the FileCloud Sync App



- On a Mass Deployment, an admin enabling remote management by setting the **allowcentralmgmt** parameter to **1**. This requires registry entries to be created before FileCloud Sync is initialized on the users' local machines.
  Note: If FileCloud Sync is initialized prior to the creation of registry keys in the users' local machines, the configuration to enable remote management will not take effect.

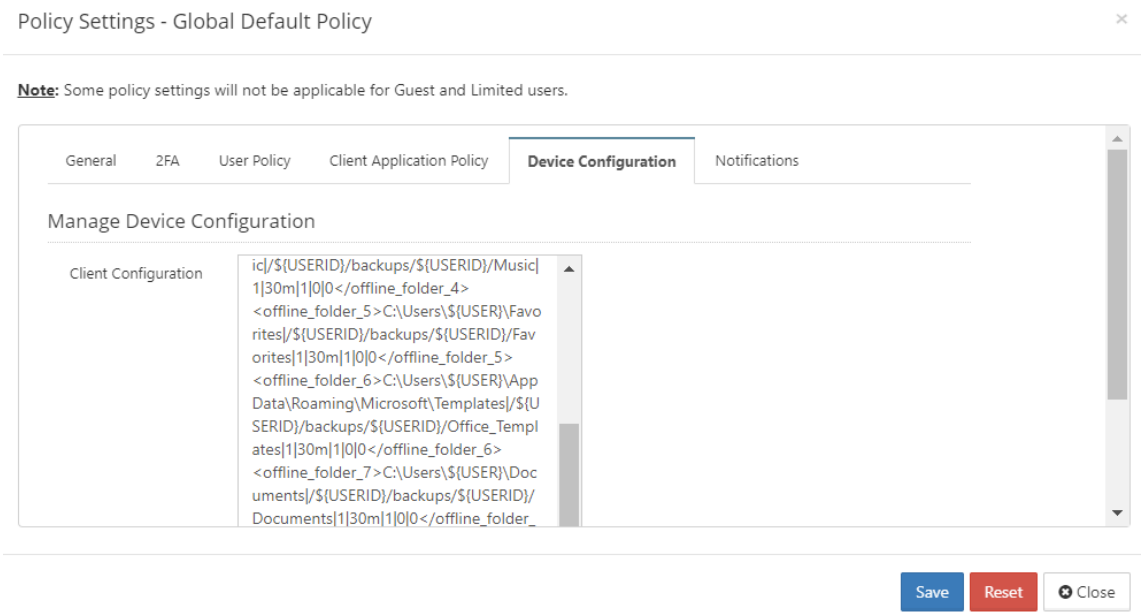
3) Set a default device configuration for Sync in the user's policy

Note: You must identify the local paths from the user's computer to include in the Sync Backup before creating the device configuration XML. Refer to the Device Configuration XML documentation for Sync.

1. Log in to the admin portal.
2. Navigate to **Settings > Policies** and edit the users' policy.
3. Go to the **Device Configuration** tab and enter the configuration in XML format. Below is a sample script to use.
   The first parameter of the XML, **<offline_folder_1>**, is a local path in the user's computer. The lines after it are the other local directories that must be included in the Sync Backup.

```
<xml>
<cloudsync>
<allowuserconfigforbackup>0</allowuserconfigforbackup>
<offline_folder_count>7</offline_folder_count>
<offline_folder_1>C:\Users\${USER}\AppData\Roaming\Microsoft\Outlook|/${USERID}/
backups/${USERID}/Outlook|1|30m|1|0|0</offline_folder_1>
```

```
<offline_folder_2>C:\Users\${USER}\Pictures|/${USERID}/backups/${USERID}/Pictures|
1|30m|1|0|0</offline_folder_2>
<offline_folder_3>C:\Users\${USER}\Desktop|/${USERID}/backups/${USERID}/Desktop|1|
30m|1|0|0</offline_folder_3>
<offline_folder_4>C:\Users\${USER}\Music|/${USERID}/backups/${USERID}/Music|1|30m|
1|0|0</offline_folder_4>
<offline_folder_5>C:\Users\${USER}\Favorites|/${USERID}/backups/${USERID}/
Favorites|1|30m|1|0|0</offline_folder_5>
<offline_folder_6>C:\Users\${USER}\AppData\Roaming\Microsoft\Templates|/${USERID}/
backups/${USERID}/Office_Templates|1|30m|1|0|0</offline_folder_6>
<offline_folder_7>C:\Users\${USER}\Documents|/${USERID}/backups/${USERID}/
Documents|1|30m|1|0|0</offline_folder_7>
</cloudsync>
</xml>
```



Disabling Deletion of Backup Files

By default, users may delete backup files. Beginning in FileCloud Version 21.1, you can disable users' ability to delete backup files..

To prevent users from deleting backup files:

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

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

3. To return to the default, change **true** to **false** or remove the setting.

Client Security Settings

Preventing an attacker from bypassing 2fa

Beginning in FileCloud 20.1, FileCloud only allows a user to set their phone number once. Once the phone number has been added, the user must contact their admin to change it. This prevents an attacker from obtaining a user name and password and then modifying the user's phone number to bypass two-factor authentication (2fa). It also prevents an attacker who has obtained the original phone number from restoring it to prevent the user from realizing there has been an attack.

To enable a user to only set their phone number once, the following setting appears in the config file:

```
define("TONIDOCLOUD_ENABLE_USER_SET2FASMS", 1);
```

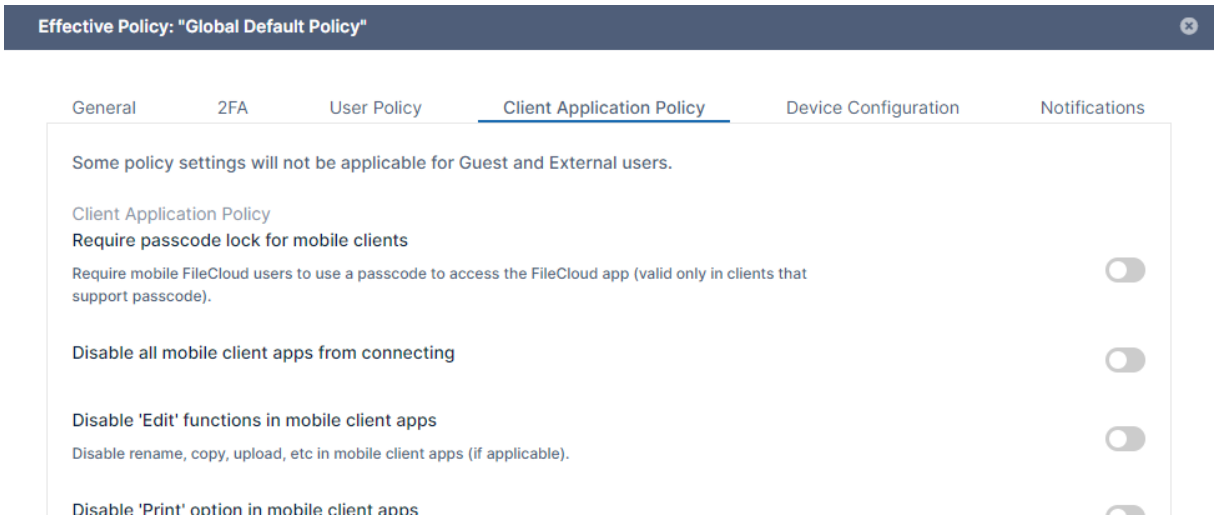
To require users to contact their admin to set their phone number initially and to change it, set TONIDOCLOUD_ENABLE_USER_SET2FASMS to 0:

```
define("TONIDOCLOUD_ENABLE_USER_SET2FASMS", 0);
```

In addition, to prevent an attacker from gaining access with another user's token, if a token is invalid, the system clears it and requires the user to sign in again.

Setting Client Application Policies

FileCloud allows customization of the client application (mobile clients) policies.



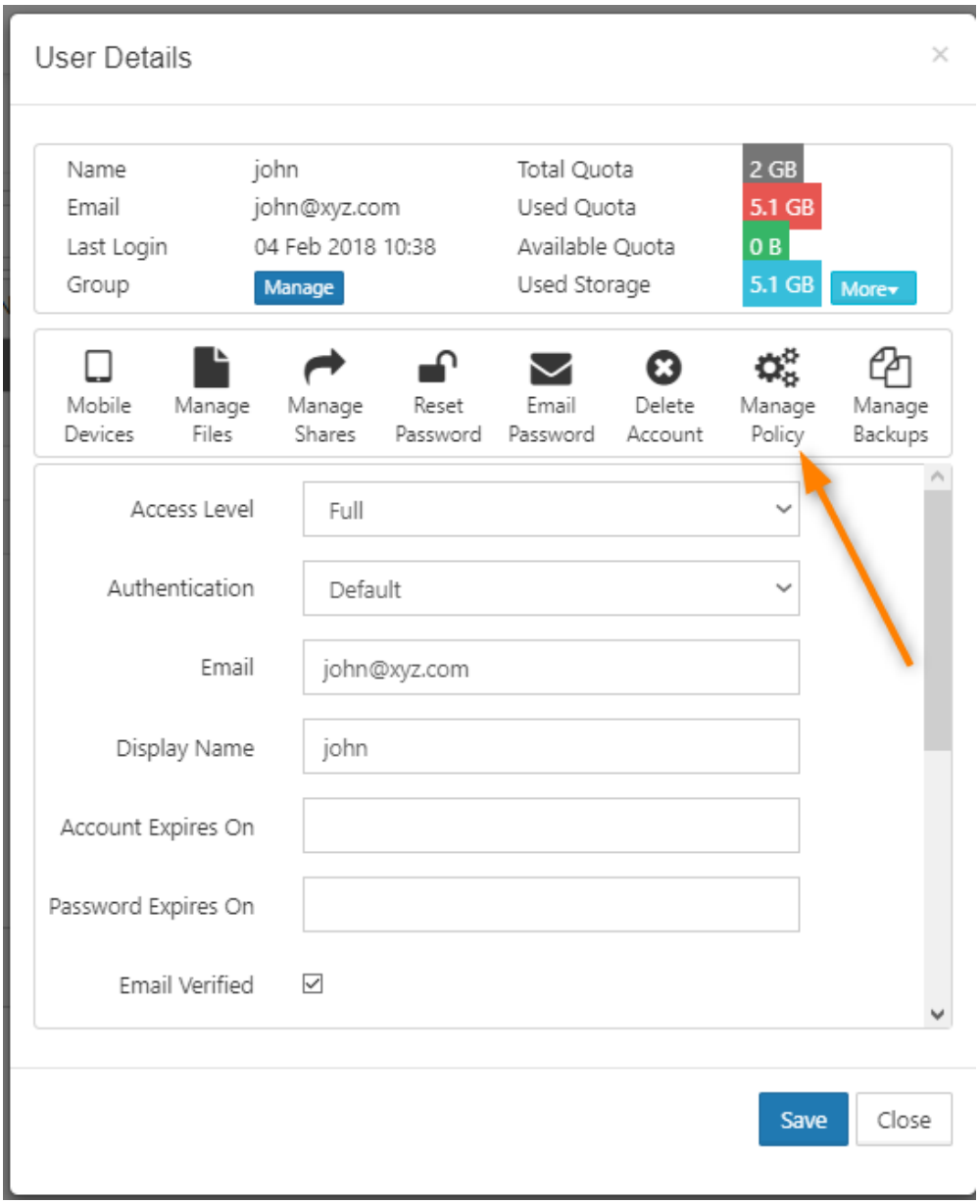
Type	Description
Require Passcode lock for mobile clients	Force mobile clients to enable FileCloud app pincode. If the pincode is not enabled, the login is rejected with an appropriate message.
Disable all mobile client apps from connecting	Prevent login to FileCloud system using mobile client apps (users are allowed to login only via the web browser).
Disable edit functions in mobile client apps	Prevent delete, copy, and move operations from being performed from mobile client apps.
Disable "Print" option in mobile client apps	Prevent printing from mobile client apps (At this point only iOS app provides print function)
Disable "Download" option in mobile client apps	Prevent file downloads in mobile client apps.
Disable "Open with" option in mobile client apps	Hide option to open a file in third party apps. NOTE: In Android, all files are opened in third party apps and this setting has no effect.
Disable "Share" options in mobile client apps	Hide file and folder sharing from mobile client apps.

Type	Description
Disable "Add to favorites" options in mobile client apps	Hide "Add to favorites" option from mobile client apps

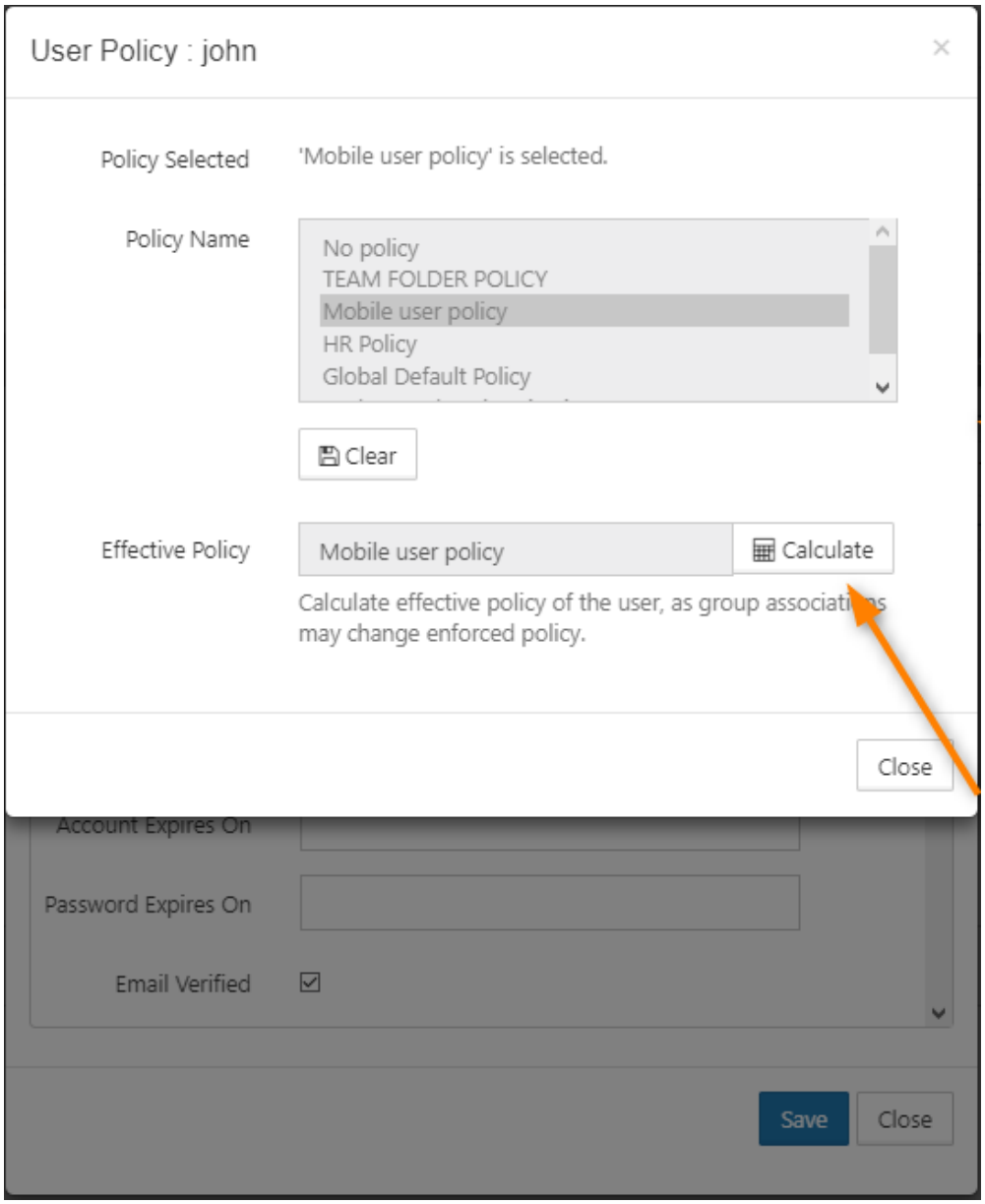
You may override a policy when you are editing the user details for a specific user; however, the new policy settings apply to all users who are assigned that policy.

To change a policy through a user's details:

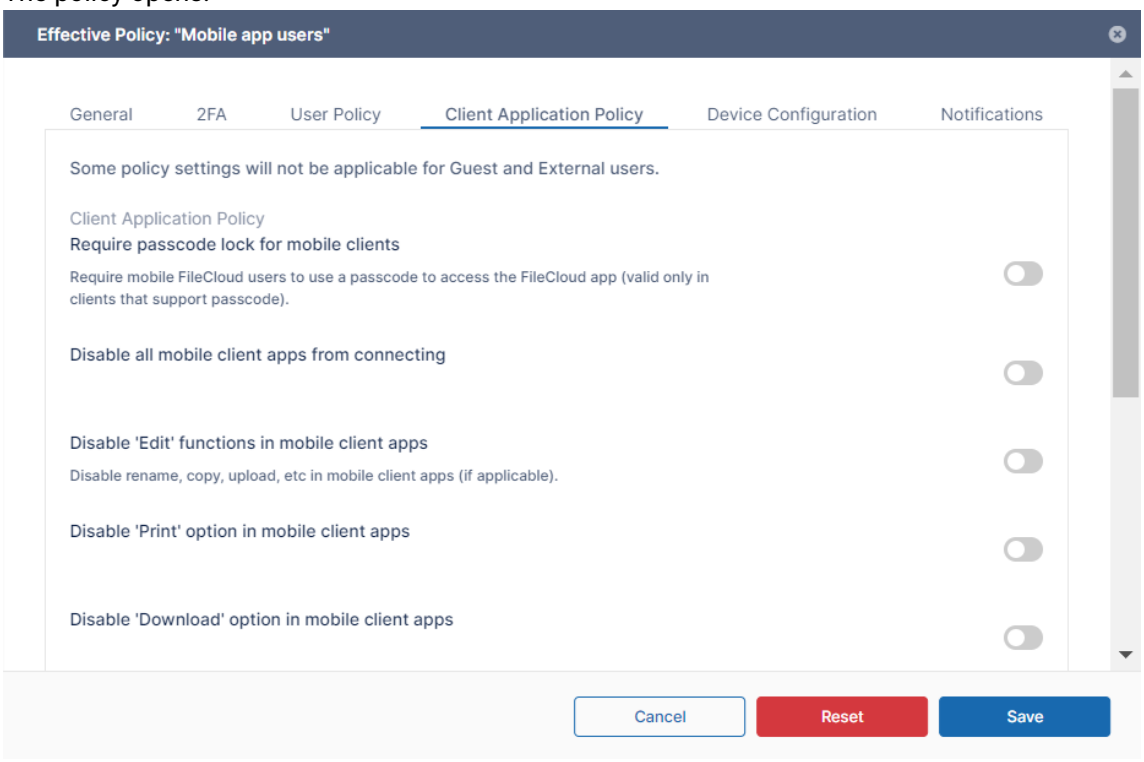
1. In the admin portal, go to **Users**.
2. Edit the user record.
3. Click **Manage Policy.**



4. Next to **Effective Policy**, click **Calculate**.


User Policy : john
Policy Selected
'Mobile user policy' is selected.
Policy Name
No policy
TEAM FOLDER POLICY
Mobile user policy
HR Policy
Global Default Policy
Clear
Effective Policy
Mobile user policy
Calculate
Calculate effective policy of the user, as group associati
may change enforced policy.
Close
Account Expires On
Password Expires On
Email Verified
Save
Close

5. Next to **Effective Policy**, click **Open**.
   The policy opens.



6. Change the settings and click **Save**.
   Note that the settings are changed for all users who belong to the policy.

Using a Proxy Server

As an Administrator, you can configure proxy network settings.

What is a proxy server?

A proxy server is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers.

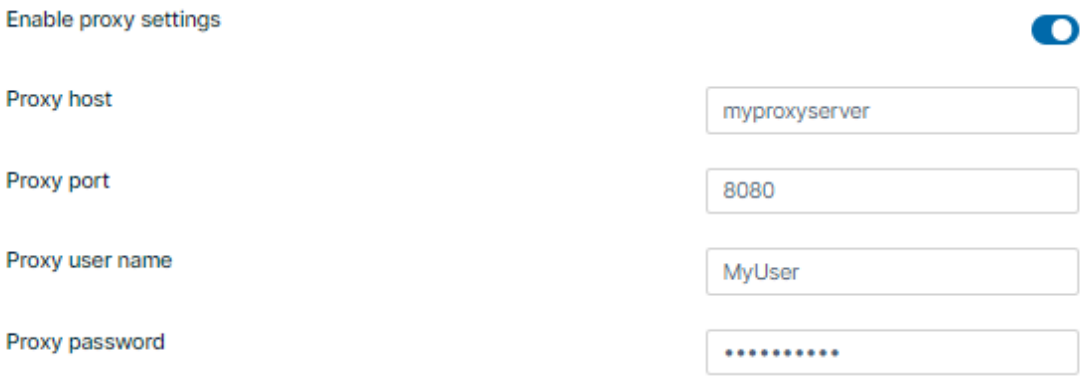
1. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server.
2. The proxy server evaluates the request as a way to simplify and control its complexity.

Proxies are used to add structure and encapsulation to distributed systems.

Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and bypassing IP address blocking.

To configure proxy settings:

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. Scroll down to **Enable Proxy Settings**, and enable it.
   Additional proxy settings appear.
3. Enter values for **Proxy host**, **Proxy port**, **Proxy user name**, and **Proxy password**.



4. Click **Save**.

Improving Cookie Security

In FileCloud versions prior to 23.1 and in FileCloud version 23.241 and later, TONIDOCLOUD_SECURE_COOKIE is disabled by default.
In FileCloud versions 23.1 and 23.232, TONIDOCLOUD_SECURE_COOKIE is enabled by default.

Defending your browser from CSRF attacks

To defend your browser from cross-site request forgery (CSRF) attacks , you can add a cookie same-site setting to FileCloud.

The cookie same-site value can be set to the following, as stated in the MDN Web Docs site at https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite:

- **Lax** - Cookies are not sent on normal cross-site subrequests (for example to load images or frames into a third party site), but are sent when a user is *navigating* to the origin site (i.e., when following a link).
- **Strict** - Cookies will only be sent in a first-party context and not be sent along with requests initiated by third-party websites.
- **None** - Cookies will be sent in all contexts, i.e. in responses to both first-party and cross-origin requests. If SameSite=None is set, the cookie Secure attribute must also be set (or the cookie will be blocked).
  To set the Secure attribute, see Adding httponly and secure flags, below.

For more information, see https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite.

To specify a cookie same-site value:

1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
   - To set the cookie same-site setting to strict, add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
     ```

   - To set the cookie same-site setting to lax (the default), add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Lax");
     ```

   - To set the cookie same-site setting to none, add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
     ```

Adding httponly and secure flags

You can take additional steps to make your cookies secure from external attacks by adding **httponly** and **secure flags** when sending cookies through HTTP headers.

What do httponly and secure flags do?

- A cookie can be accessed through http or through client-side Javascript. An **httponly flag** blocks access to a cookie from the client side (Javascript) by only allowing it to be accessed by http.
- Most sites are accessed by https, but some sites may also be accessed by http or some of their components may be sent through http. This leaves cookies vulnerable to being accessed over http. A **secure flag** prevents them from being accessed through http by only allowing them to be transmitted over https.

To configure FileCloud to always use the httponly and secure flags in HTTP headers:

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_SECURE_COOKIE", 1);
   ```

```
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

Recommended and default settings

The recommended values for the cookie settings are the following:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

However, if you are using FileCloud for Office, you must set the same-site cookie value to **None** for the feature to function.

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
```

If you are using FileCloud 23.241 or later:
Your default settings are:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
define("TONIDOCLOUD_SECURE_COOKIE", 0);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

If you are using FileCloud 23.1 or later:

The above recommended settings are the same as your default settings:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

If you are using a version of FileCloud prior to 23.1:

Your default settings are:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
define("TONIDOCLOUD_SECURE_COOKIE", 0);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 0);
```

You may copy the recommended settings, which are stored in cloudconfig-sample.php into cloudconfig.php to override the defaults.

Integration with MS Teams

If you have integrated your system with MS Teams, and login frequently redirects users back to the login page:

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

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

Configuring OAuth for SCIM Integration

Configuration of OAuth credentials that give external applications access to FileCloud resources is available beginning in FileCloud 23.252. SCIM is currently the only application that can gain access through this OAuth configuration, but in the future, additional applications may be added.
FileCloud supports SCIM integration with Azure, Okta, and OneLogin, but most other SCIM IdPs should be able to connect to FileCloud using OAuth. Please contact your authentication service for support in configuring its integration with FileCloud.

OAuth 2.0 authorization enables an application to securely access FileCloud resources without requiring a manual action or scheduled command to trigger the access request. OAuth 2.0 provides secure access by specifying scopes (permitted actions) associated with the access, and by creating unique tokens for accessing FileCloud. A token remains valid for an interval set in the configuration that may range from 1 hour to 5 years.

Currently, SCIM (System for Cross-domain Identity Management) is the only application that uses this OAuth configuration in FileCloud. SCIM is a protocol that enables you to update FileCloud user and group information by syncing it with changes made to user and group information in other applications. When SCIM detects a change in one of the apps, it uses OAuth 2.0 to gain access to FileCloud and update its user/group data.

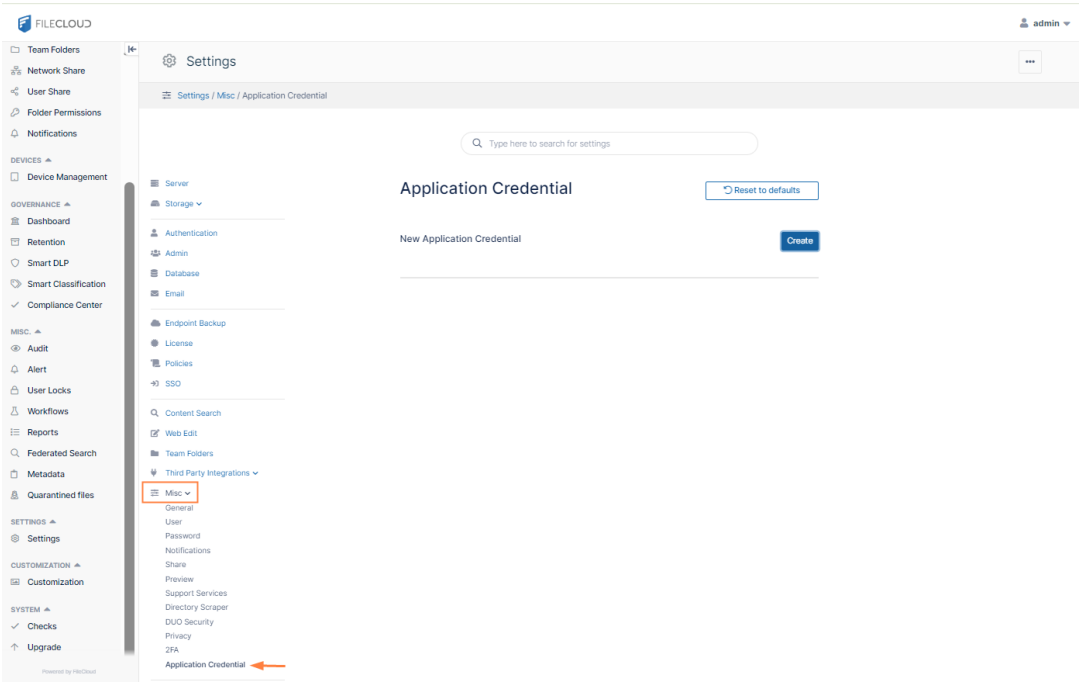
To configure SCIM for integration with FileCloud:

Note for Azure users: You do not have to change anything in your existing SSO SAML application configuration. This configuration is separate from your SCIM configuration.

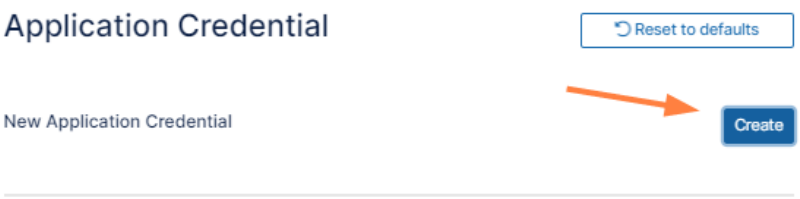
1. Create the SCIM application in your currently supported IdP. Follow the instructions provided in the IdP's documentation.
   a. The FileCloud SCIM endpoint in the application must be set to: **https://<your-filecloud-domain>/api/v1/scim**

To configure OAuth application credentials for SCIM in FileCloud:

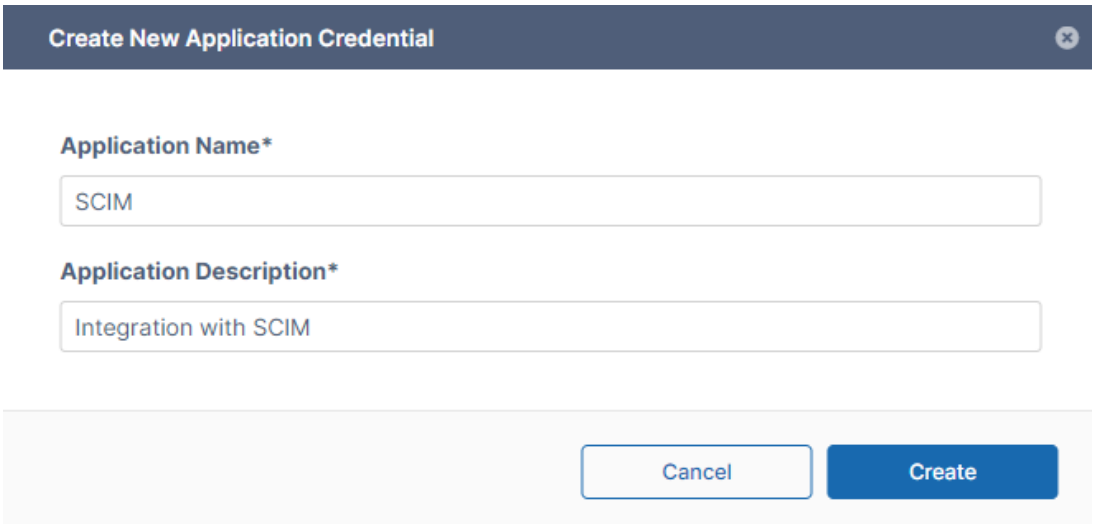
1. In the FileCloud admin portal, open the Application Credentials page.
   To go to the Application Credentials page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Application Credential**, as shown below.



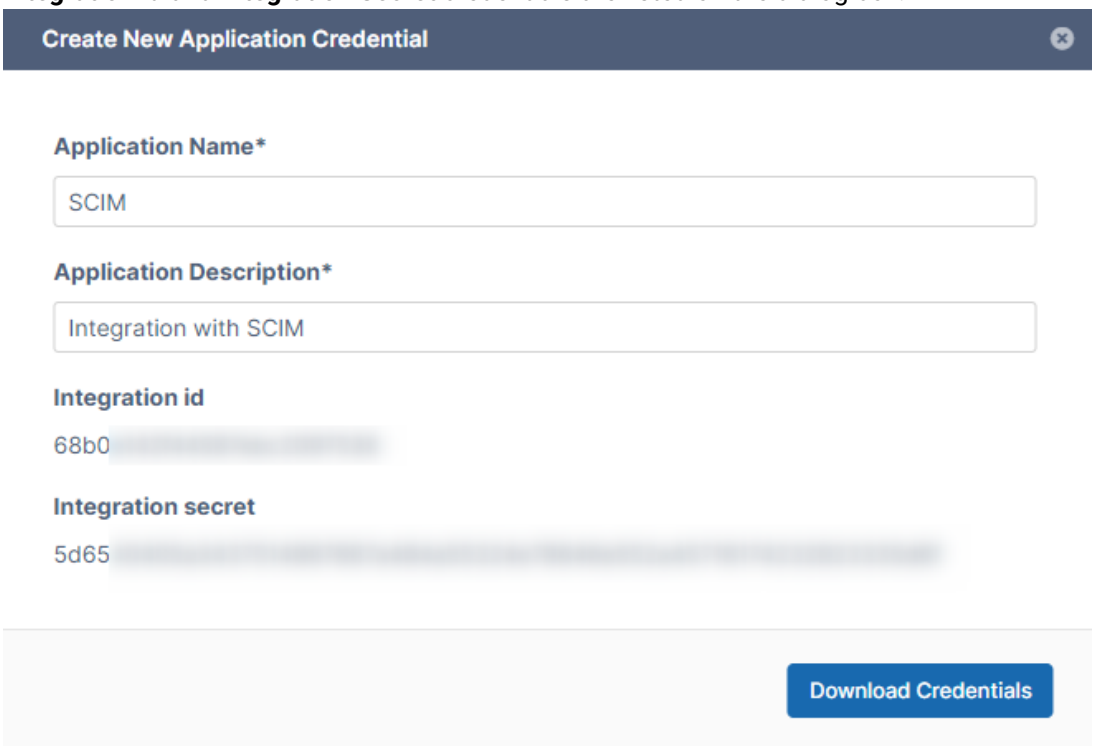
   The Application Credentials page opens.
2. Click **Create**.



   The **Create New Application Credential** dialog box opens.
3. Enter the **Application Name** and an **Application Description**.



4. Click **Create**.
   Integration id and **Integration Secret** credentials are listed on the dialog box.



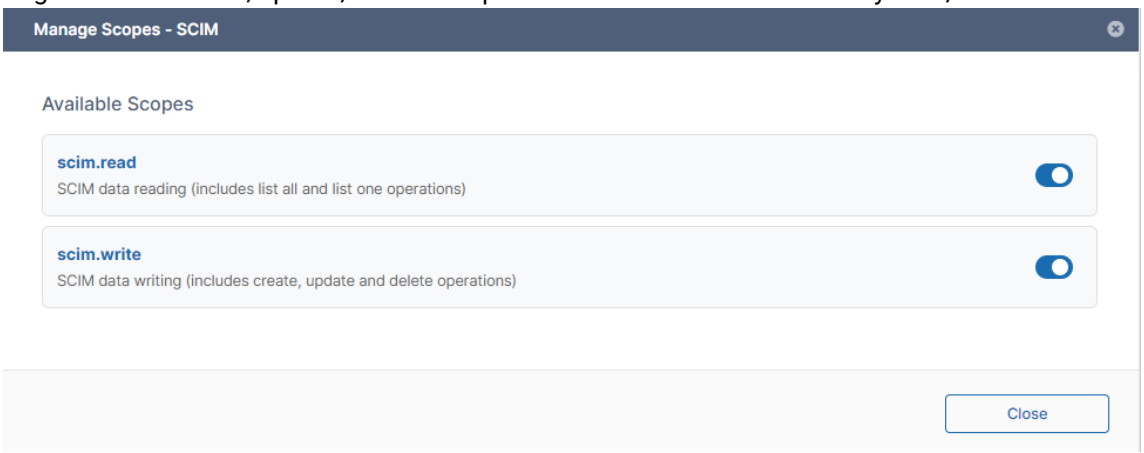
   The credentials will not be shown to you again, but you will be required to enter the **Integration secret** to create the token.

5. Click **Download Credentials** to save them in a file named **file credentials for [Application Name].txt**
   The dialog box closes and the credential is now listed.
   Click the key icon.



The **Manage Scopes** dialog box opens.

6. Enable **scim.read** to grant SCIM read permission to FileCloud's identity data, enable **scim.write** to grant SCIM create, update, and delete permissions to FileCloud's identity data, or enable both.

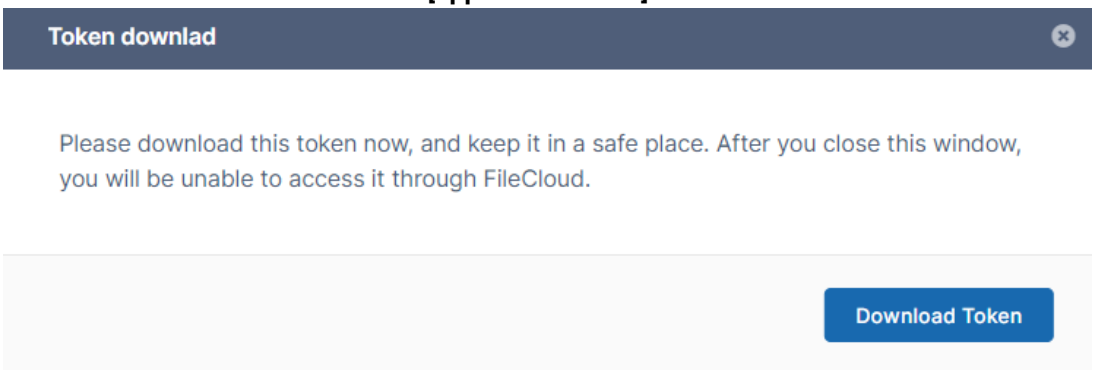


7. Click **Close**.
8. Click the ticket icon.

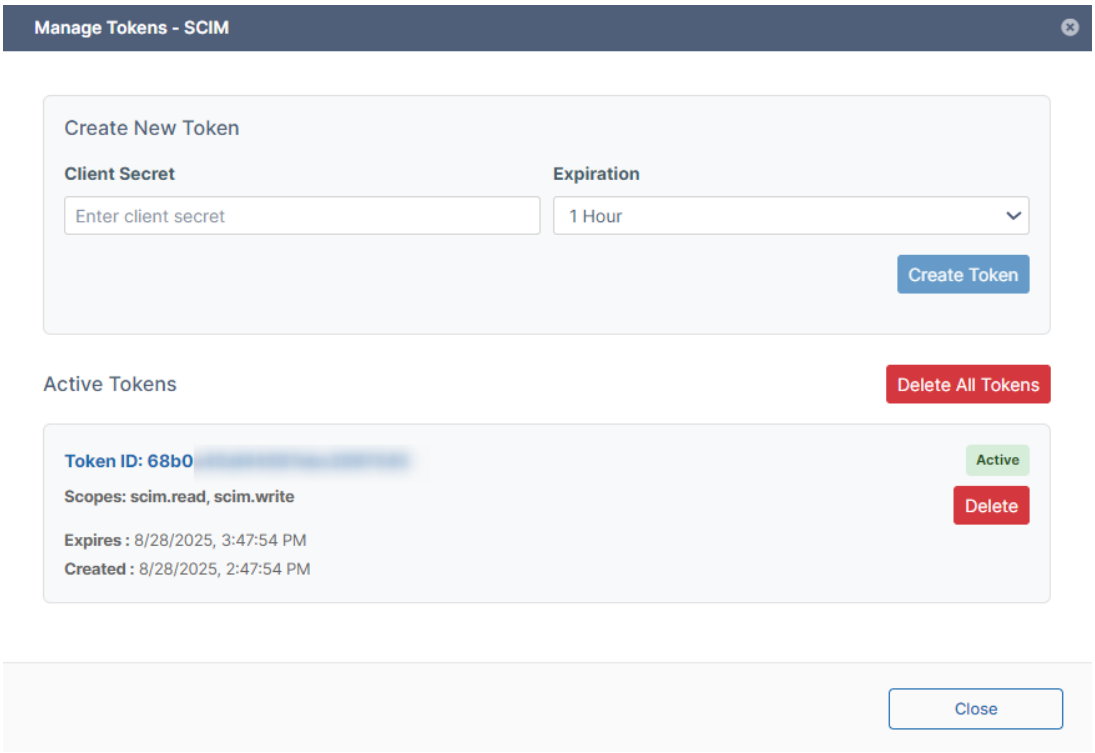


The **Manage Tokens** dialog box opens.

9. In **Client Secret** enter the **Integration secret** you saved above.
10. In **Expiration**, choose the interval that the token will remain usable. By default the interval is 1 hour.
11. Click **Create Token**.
    You are prompted to save the token.
12. Click **Download Token**.
    It is saved to the file **credentials for [application name].text**



The **Token ID** and its create and expire dates and times are shown. It is automatically made active.



13. Click **Close**.
    SCIM will now automatically update FileCloud with the connected apps' identity information.

Dynamic CSP in FileCloud

Beginning with version 23.253, FileCloud uses a dynamic CSP by default.

A dynamic Content Security Policy (CSP) adds protection to a site depending on which features you are using. This enables a granular level of security that allows potentially harmful resources to be blocked when not essential, but permitted when necessary. For example, in FileCloud, certain resources could be permitted if your system were integrating with Google Apps, but blocked if Google Apps resources were not required.

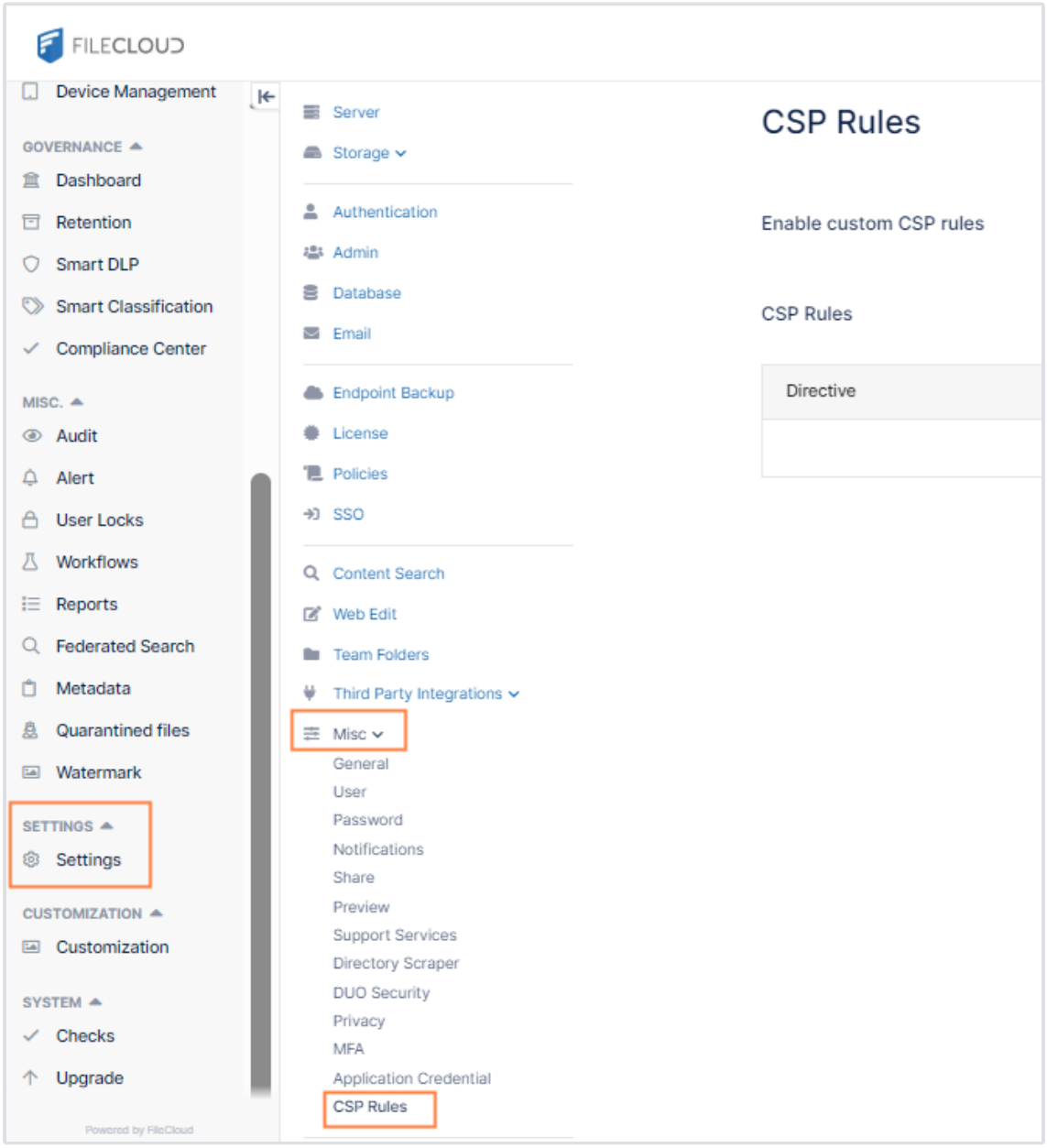
By default, FileCloud uses a dynamic CSP to offer you protection according to your specific implementation.

Disabling dynamic CSP

If you want a stricter or more permissive security policy, you may disable dynamic CSP and use the content security policy included in the .htaccess file.

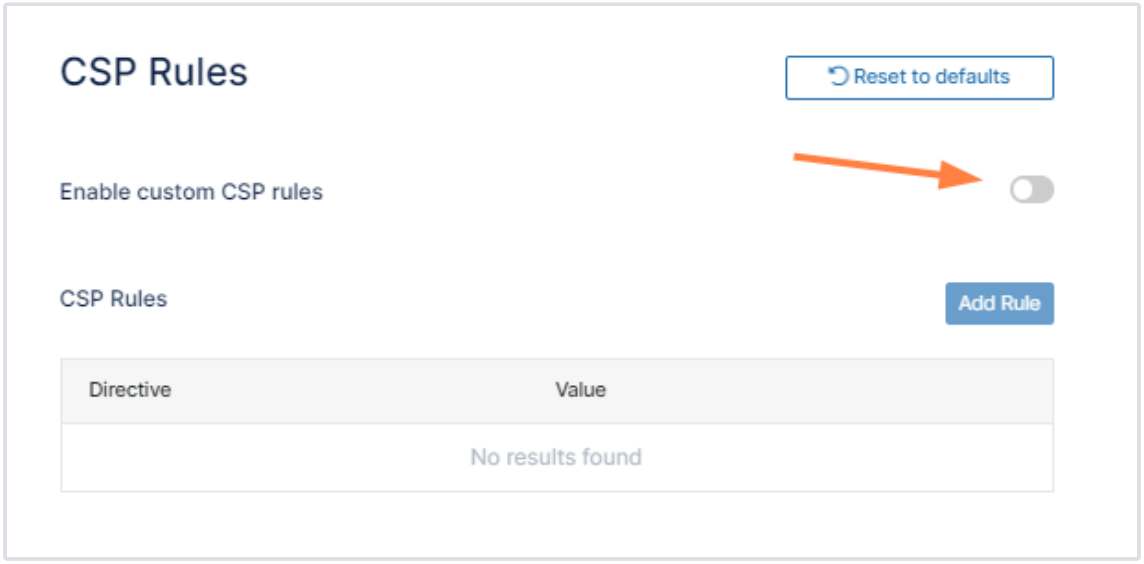
To disable dynamic CSP:

1. In the FileCloud admin portal, go to **Settings > Misc > CSP Rules**.



By default, **Enable custom CSP rules** is toggled on.

2. Toggle **Enable custom CSP rules** off.



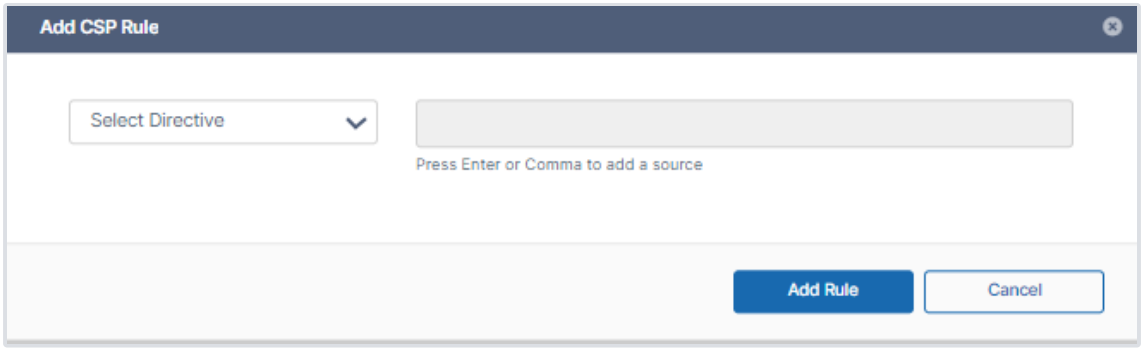
Once you disable dynamic CSP, FileCloud uses the content security policy in your .htaccess file.

Creating custom rules for dynamic CSP

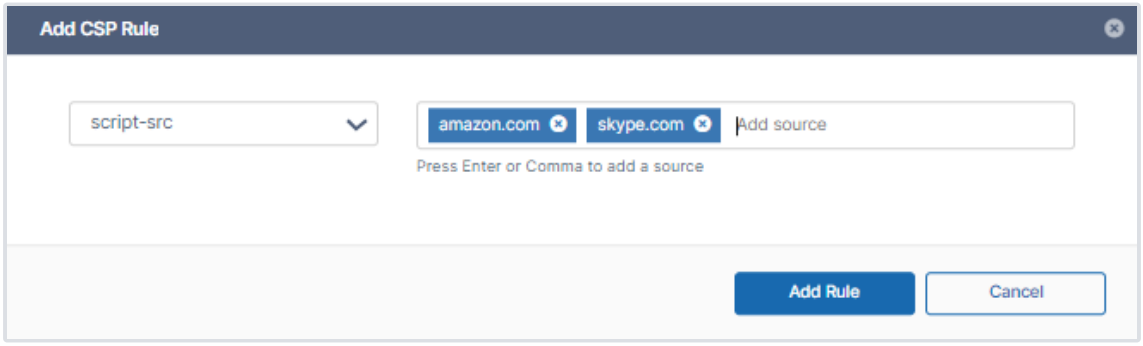
In addition to the rules that dynamic CSP automatically applies after determining which features your system uses, you may create custom rules for dynamic CSP. You add a custom CSP rule by choosing a directive (which specifies a resource type) and then entering the source or sources (which specify where the resource may be accessed from).

To create custom rules for dynamic CSP:

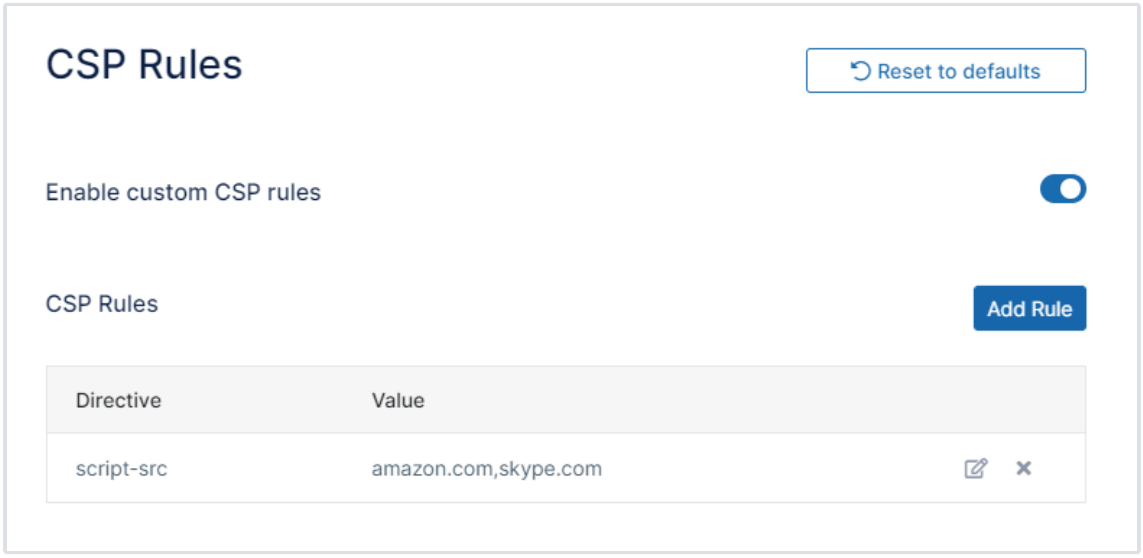
1. Toggle on **Enable custom CSP rules** if it is not already toggled on.
2. Click **Add Rule**.
   The Add CSP Rule dialog box opens.



3. In the **Select Directive** drop-down list, choose a directive.
4. Then in **Add source**, enter the source or multiple sources.
   To save a source in **Add source**, enter a comma or click [Enter].
   For example, in the following image, the directive chosen is **script-src** and the permitted sources entered are amazon.com and skype.com. The rule specifies that scripts may only be imported into your site from the amazon.com and skype.com domains.



5. Click **Add Rule**.



The rule is added to the list of CSP rules.

6. Add any number of CSP rules.
Note: if a directive exists in a default dynamic CSP rule and a custom dynamic CSP rule, the sources in both the default and custom rules are permitted.

Customizing the CSP in the .htaccess file

If you have disabled dynamic CSP, you may customize the CSP rules for the static CSP in the .htaccess file.

To customize the CSP in the .htaccess file:

1. Open the file in:
Windows:
C:\xampp\htdocs\.htaccess
Linux:
/var/www/html/.htaccess
2. Add your custom rules to the **Content-Security-Policy** header, indicated below. Use the format: **directive source1 source2 . . . sourceN;**

```
<IfModule mod_headers.c>
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header setifempty Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileass
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com
\
    frame-src 'self' blob: www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.wind
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com; \
    worker-src 'self' blob: *.autodesk.com"
Header set Cache-Control no-cache="Set-Cookie"
</IfModule>
```

Identify Company Devices in FileCloud Desktop for Windows Logins

If your organization uses Windows Integrated Authentication (WIA), you may add a setting that enables you to determine if logins are from company-managed devices or from employees' personal devices.

To identify devices that are part of your company's domain with the user agent **Cloud Storage Client (WIA)**, add the following registry key and set its value to **1**:

`HKLM\SOFTWARE\FileCloud\FileCloudDesktop\DefaultCfg\alternateuseragentenabled`

This setting can be deployed using a device management tool (like an MDM system).

Once this is set, company-managed devices identify themselves with the user agent **Cloud Storage Client (WIA)** when they connect to FileCloud.

Online Web Editing

Beginning in FileCloud 22.1, Office extensions .doc, .xls, and .ppt are no longer editable in Web Edit. In Desktop Edit, users may still edit .doc, .xls, and .ppt files.

Administrators can configure online editing to allow FileCloud users to select any supported document and edit the document from within the User Portal.

- All the changes made by the user are saved in FileCloud automatically.
- Depending on the versioning settings in FileCloud, additional versions may be created.
- FileCloud uses the WOPI (Web Application Open Platform Interface) protocol to support online web editing.

Read more about the WOPI protocol to support document editing.

To use WOPI, you must install or have already available one of the following to provide the web editing capability:

- Microsoft Office Online
- Collabora Code
- OnlyOffice

Use the instructions from the following sections to install and configure online web editing.

Microsoft Office Online Web Editing

You can integrate FileCloud with Microsoft Office Online to allow your users to edit documents in a browser. FileCloud uses the WOPI protocol for this integration.

Administrators can configure Web Edit in the following ways:

FileCloud can integrate with your Microsoft-hosted Office online server to edit office documents.	Microsoft Office Online for Cloud Web Editing
FileCloud can integrate with your on-premises Office online server installation to edit office documents.	Microsoft Office Online Server Web Editing

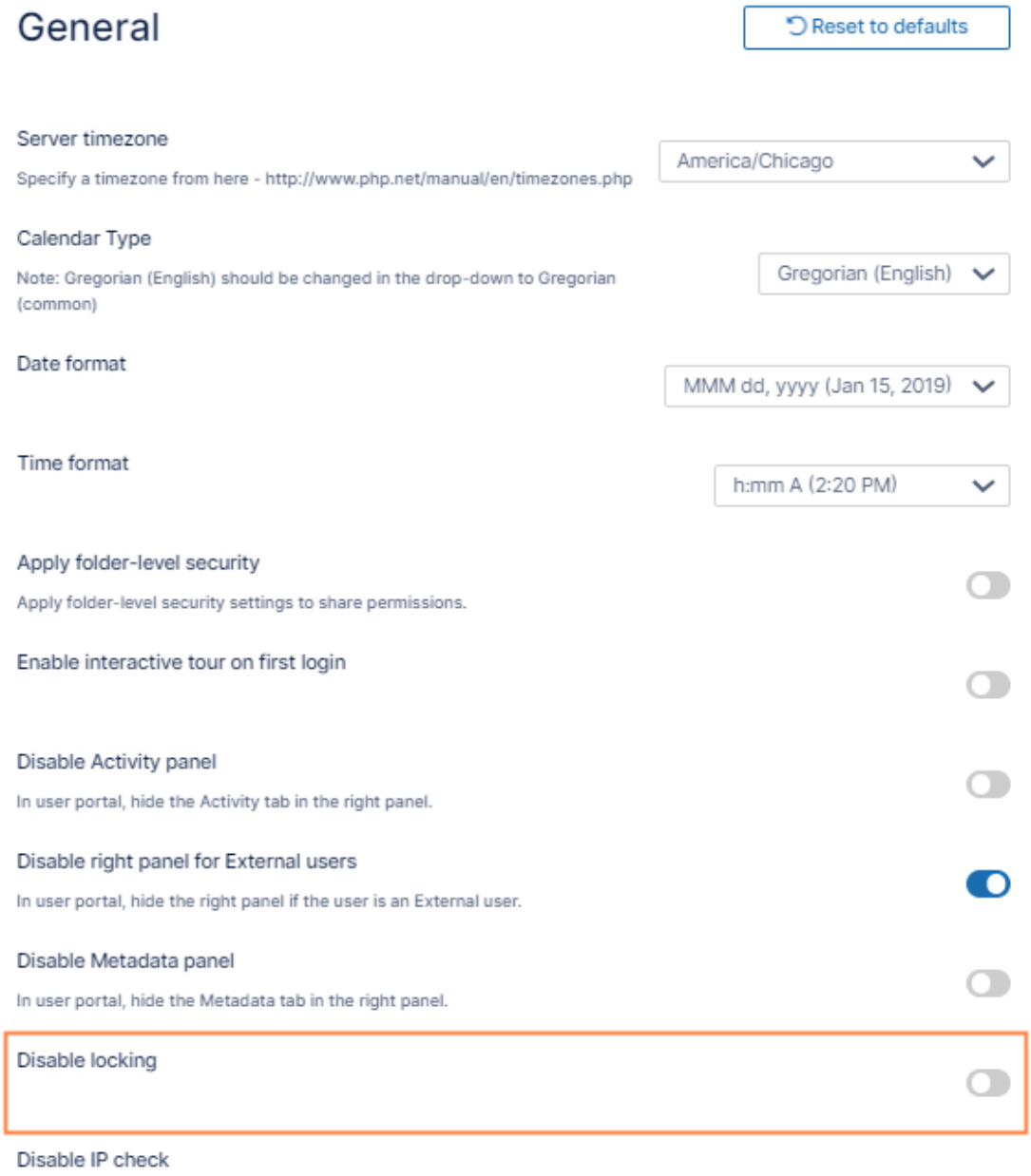
Troubleshooting Office Web Editing

Document always opens in read-only mode

This issue can happen if locking is disabled.

To enable 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. Scroll down to the **Disable Locking** setting, and disable it.



3. Click **Save**.

Microsoft Office Online Cloud For Web Edit

FileCloud can integrate with your Microsoft-hosted Office online server to edit office documents.

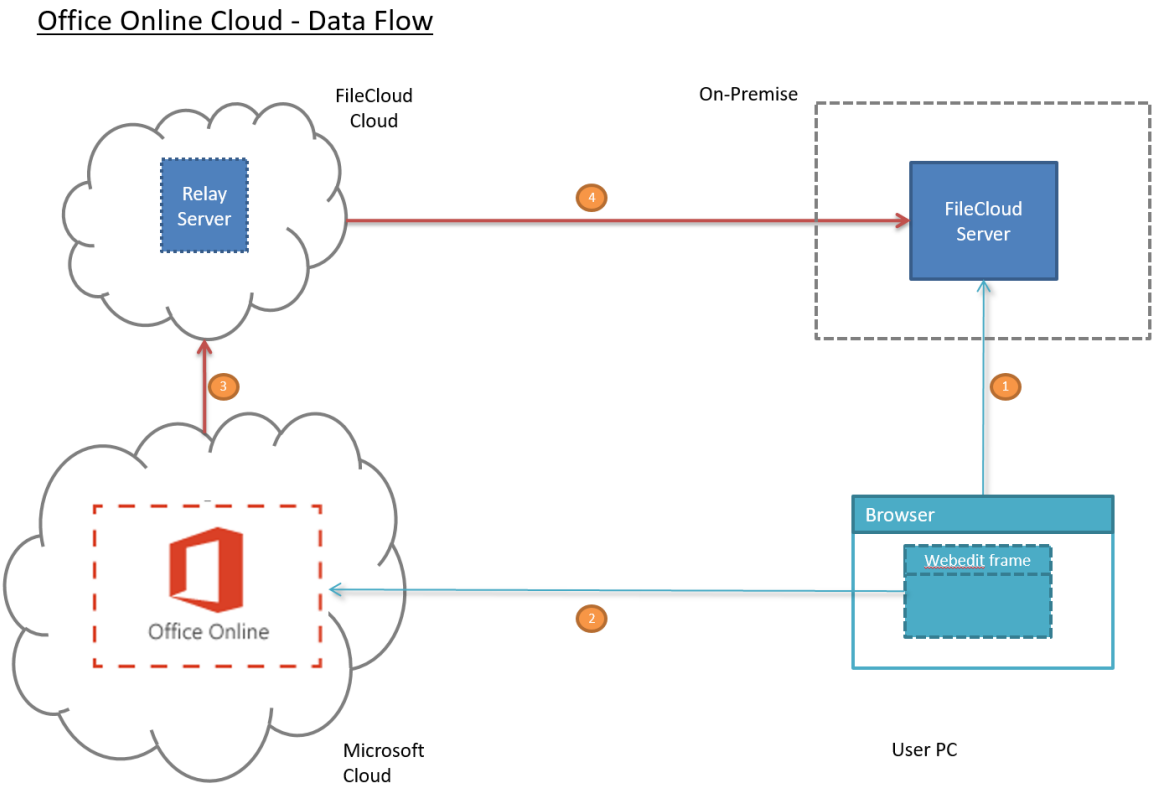
Tips

- Please note that for using this type of web editing, users should have an **Office365** account.
- When configuring Office365, please use the default 'admin' user to login into FileCloud admin UI. For security reasons, this configuration is not allowed as a normal user promoted as admin.
- Support for large file sizes may vary depending on the speed between FileCloud and the relay servers.

Office 365 Office product page

Dataflow

Following diagram depicts the interaction between Microsoft Office Online cloud and an on-premises FileCloud server.



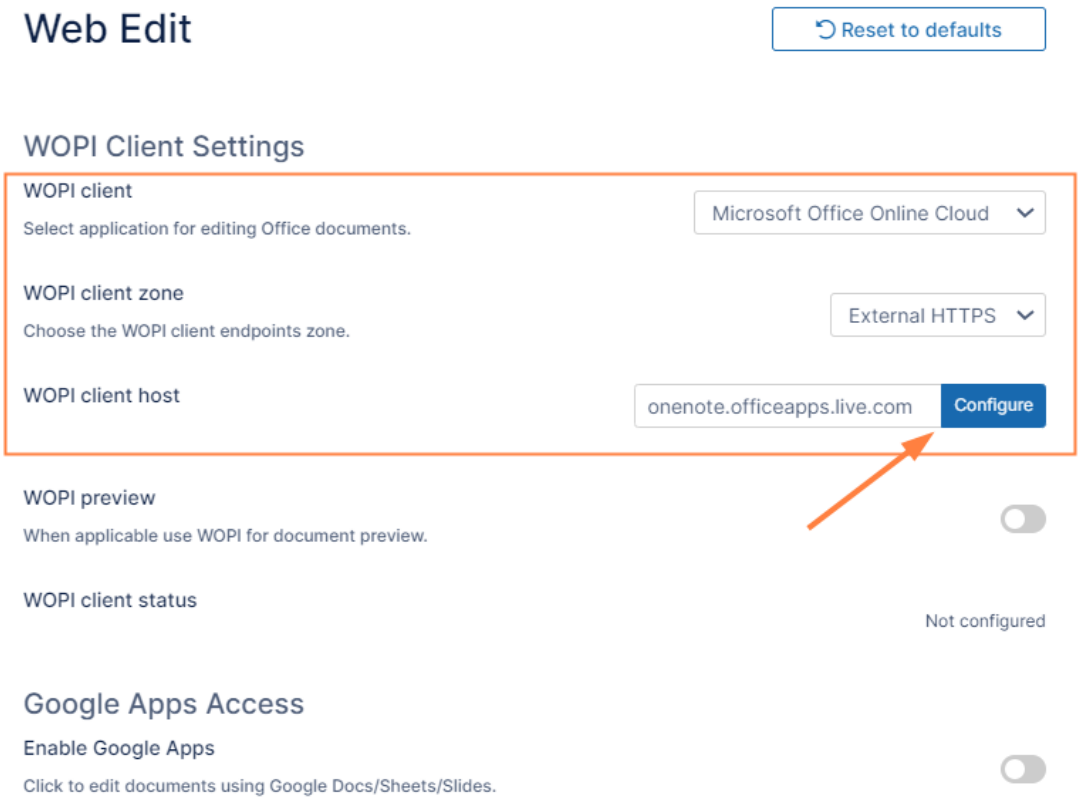
Steps:

1. User selects a document file in office online from FileCloud user UI. It loads a HTML page with embedded IFRAME pointing to the Microsoft Office Online cloud.
2. IFRAME loaded in the previous step loads the document specific application from the Microsoft cloud. This in turn instructs the Office Online cloud to load the document from FileCloud server.
3. Since Office Online cloud supports only pre-approved URLs it cannot load the document directly from FileCloud server. So the download request is forwarded to a relay server (hosted by FileCloud).
4. Relay server in turn forwards the request to FileCloud server and returns the response back. In summary, relay server serves as a bridge between Office Online cloud and FileCloud server making the communication back and forth work seamlessly.

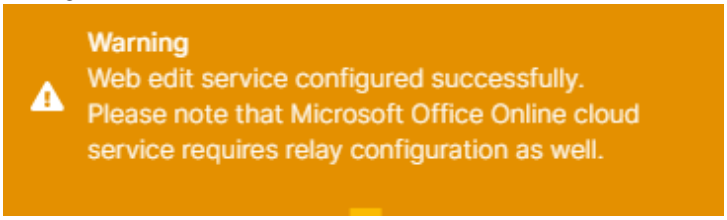
Configuring FileCloud With Office Online Cloud

To configure FileCloud with Office Online Cloud:

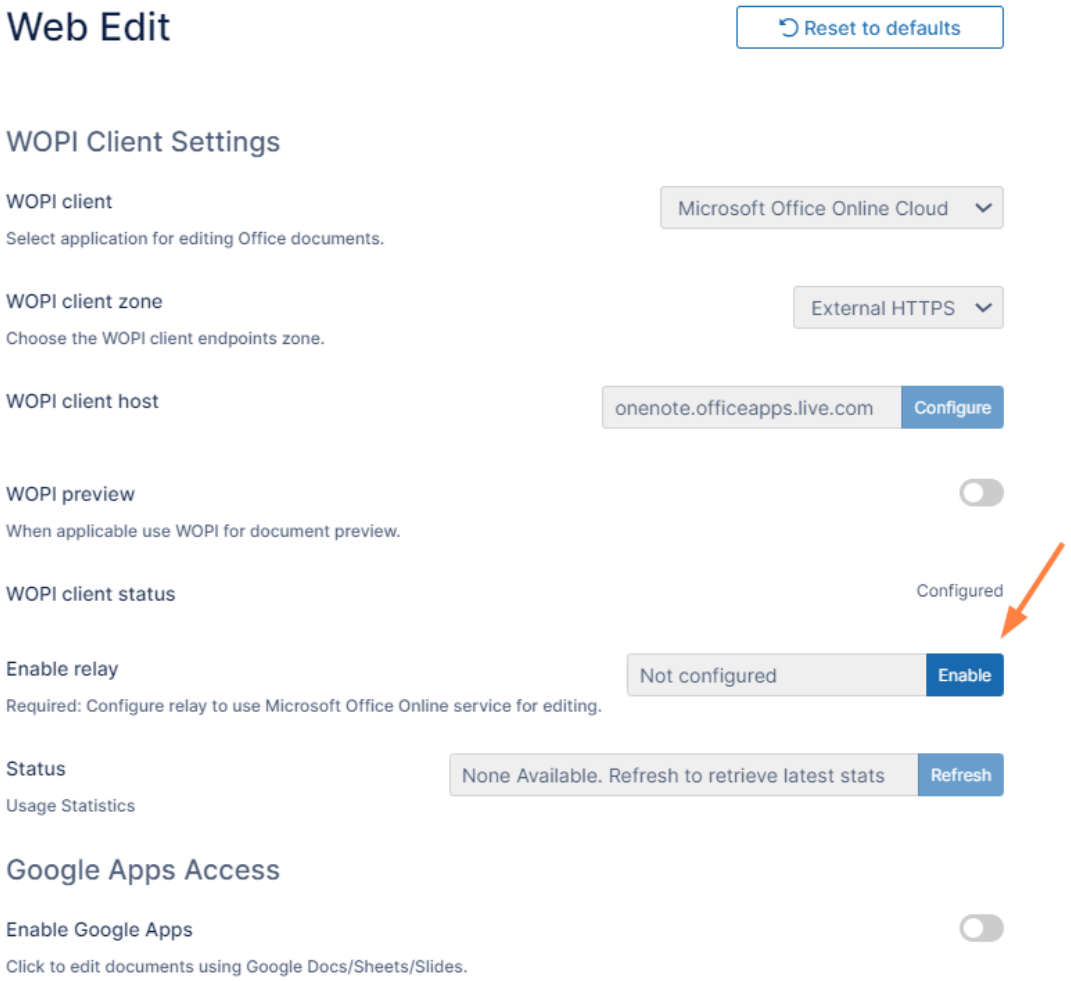
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Web Edit**  .
   The **Web Edit** settings page opens.
2. Fill in the following values for the first three settings:
   WOPI client: Microsoft Office Online Cloud
   WOPI client zone: External HTTPS
   WOPI client host: onenote.officeapps.live.com
3. Click **Configure**.



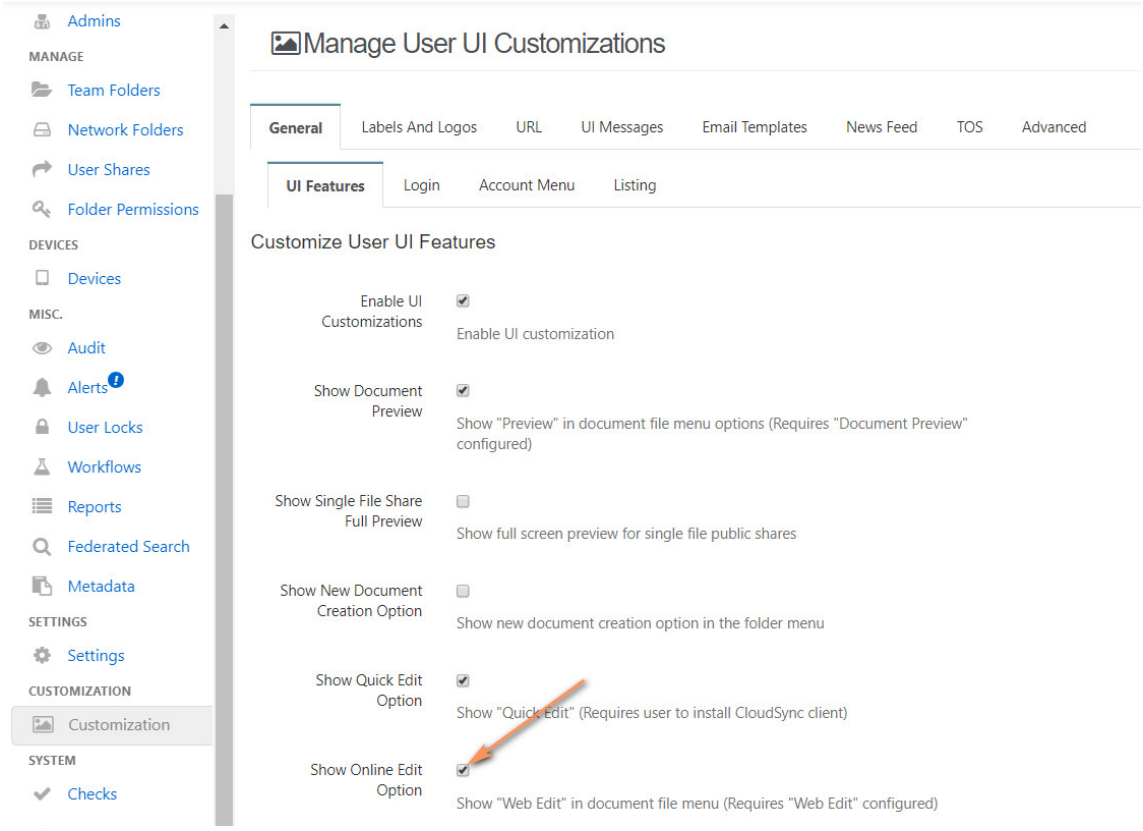
Upon successful configuration, the following notification instructs user to enable relay configuration.



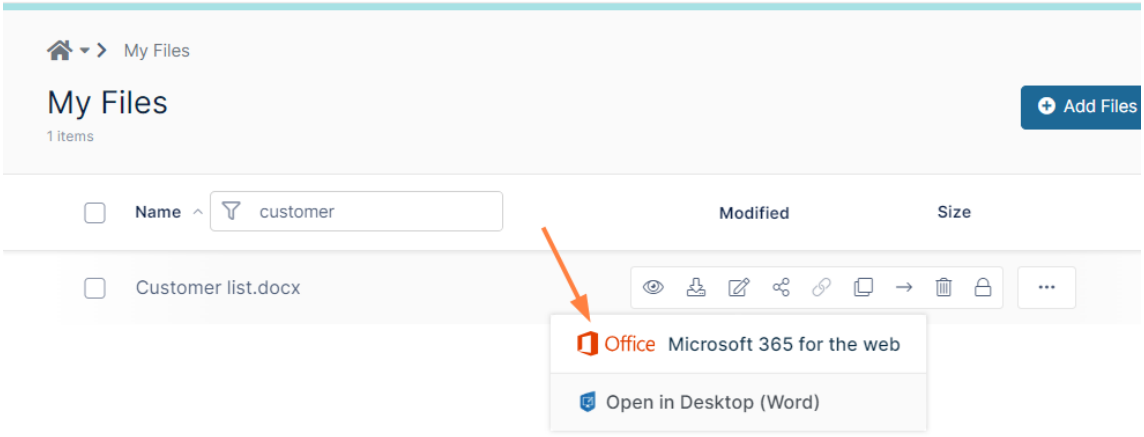
4. Beside **Enable relay**, click **Enable**.



5. When WOPI edit over cloud is selected, FileCloud uses WOPI for all document previews, since the WOPI web editor provides a more faithful reproduction of the document. To disable this behavior, disable **WOPI preview** in the WOPI Client Settings screen.
6. Now that FileCloud server is configured with office online server, administrator might need to enable the web edit option for users.
   To enable web edit in the user portal, navigate to **Customizations > General > UI Features** and check the option **Show Online Edit Option**. Click **Save**.



7. Now log in to the user portal and hover over an editable Office document. Hover over the Web Edit icon, and ensure that you see the Office icon and Microsoft 365 for the Web.
8. Click the icon.
   The file is opened in the Office for the web editor.



9. When the Office for the web editor application loads, it prompts the user to enter an Office 365 account. Upon logging in the selected document is loaded in the editor.

> Depending the browser's cookie policies, after a user logs into their Microsoft account for WOPI edit, their FileCloud session could be closed. To avoid this problem, set TONIDOCLOUD_COOKIE_SAME_SITE_TYPE to Lax.

Microsoft Office Online Server For Web Edit

Introduction

FileCloud can integrate with an on-premises Office online server installation to edit office documents.

This section explains how to install office online server on a Windows 2012 server and configure FileCloud to use this installation for web editing.

Installing Office Online Server on Windows 2012 R2 Server

> This documentation is only for reference purposes; installation of Office Online On-Premises server is outside of FileCloud Support's scope. For updated Microsoft instructions or changes please refer to the official Microsoft documentation https://learn.microsoft.com/en-us/officeonlineserver/deploy-office-online-server

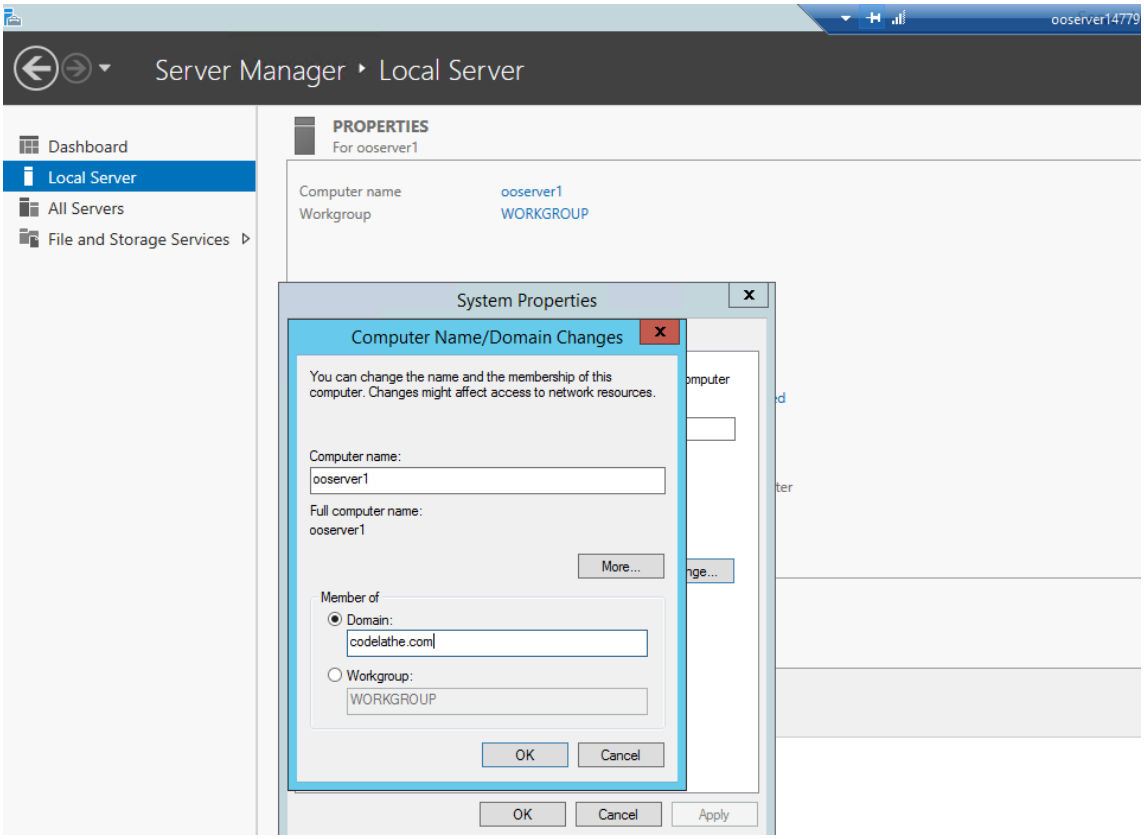
Introduction

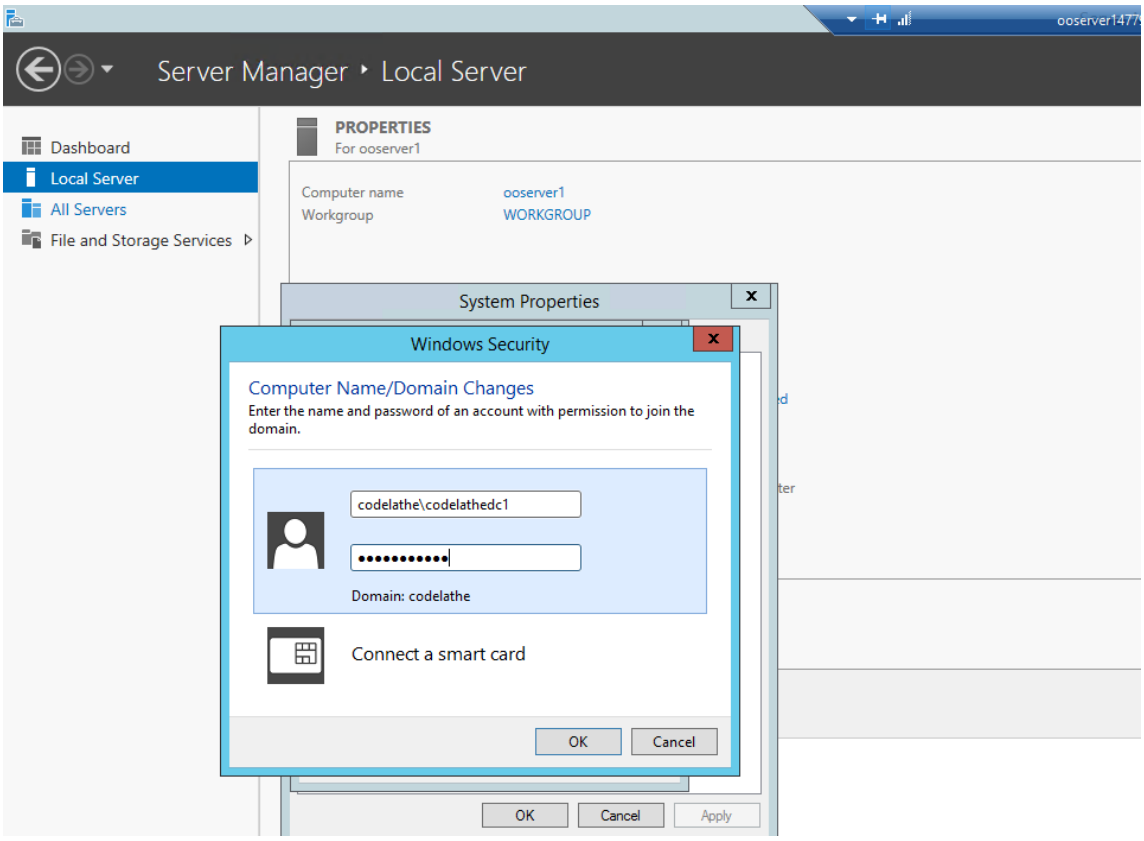
FileCloud can integrate with an on-premises Office Online server installation to edit Office documents (word, excel and powerpoint) from a browser. The following guide explains how to install office online server on Windows 2012 server.

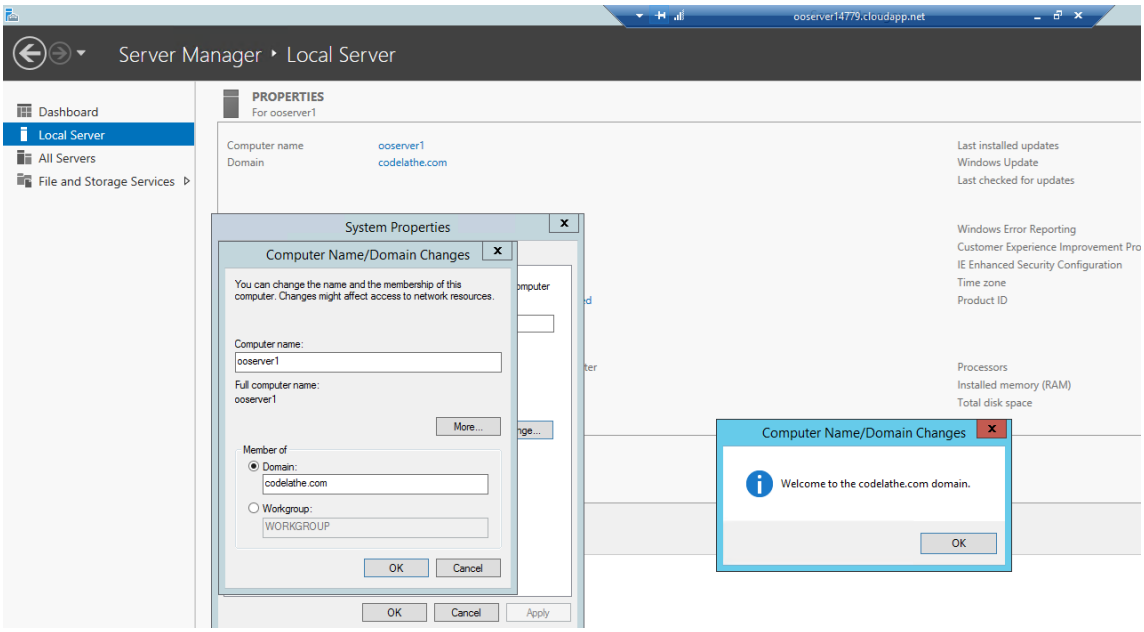
> It is recommended to install Office Online Server on its own Windows server. Don't install it on Active Directory domain controller, sharepoint server or Exchange server. Also the windows server where you are installing the office online server has to be connected to an Active Directory domain.

First Steps

1. Connect the windows server where you be installing office online server to an active directory domain.





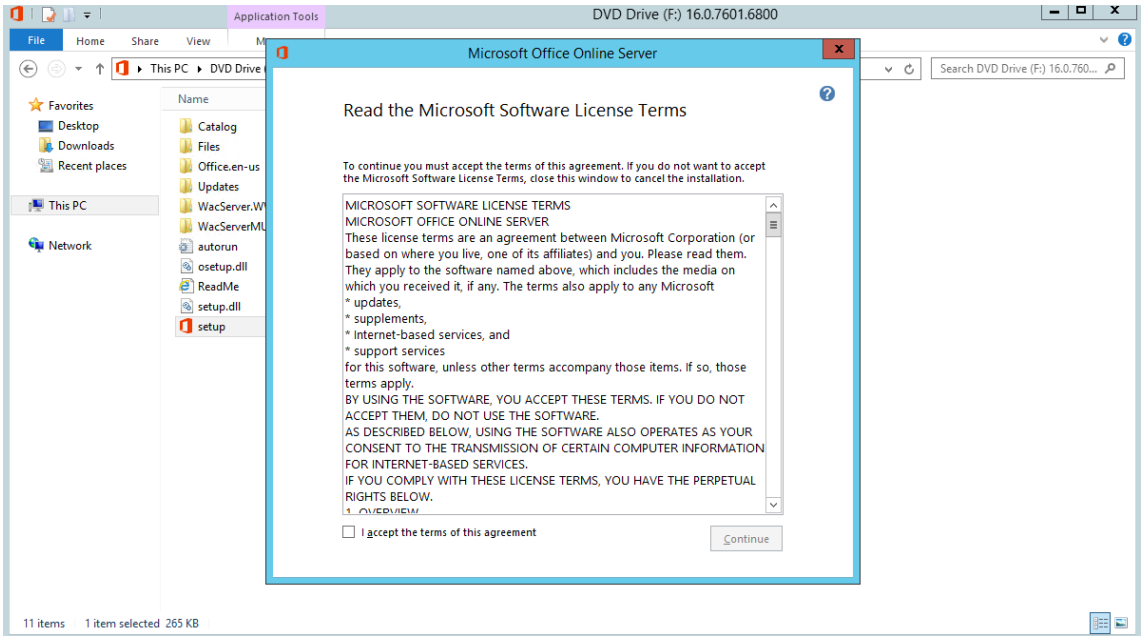


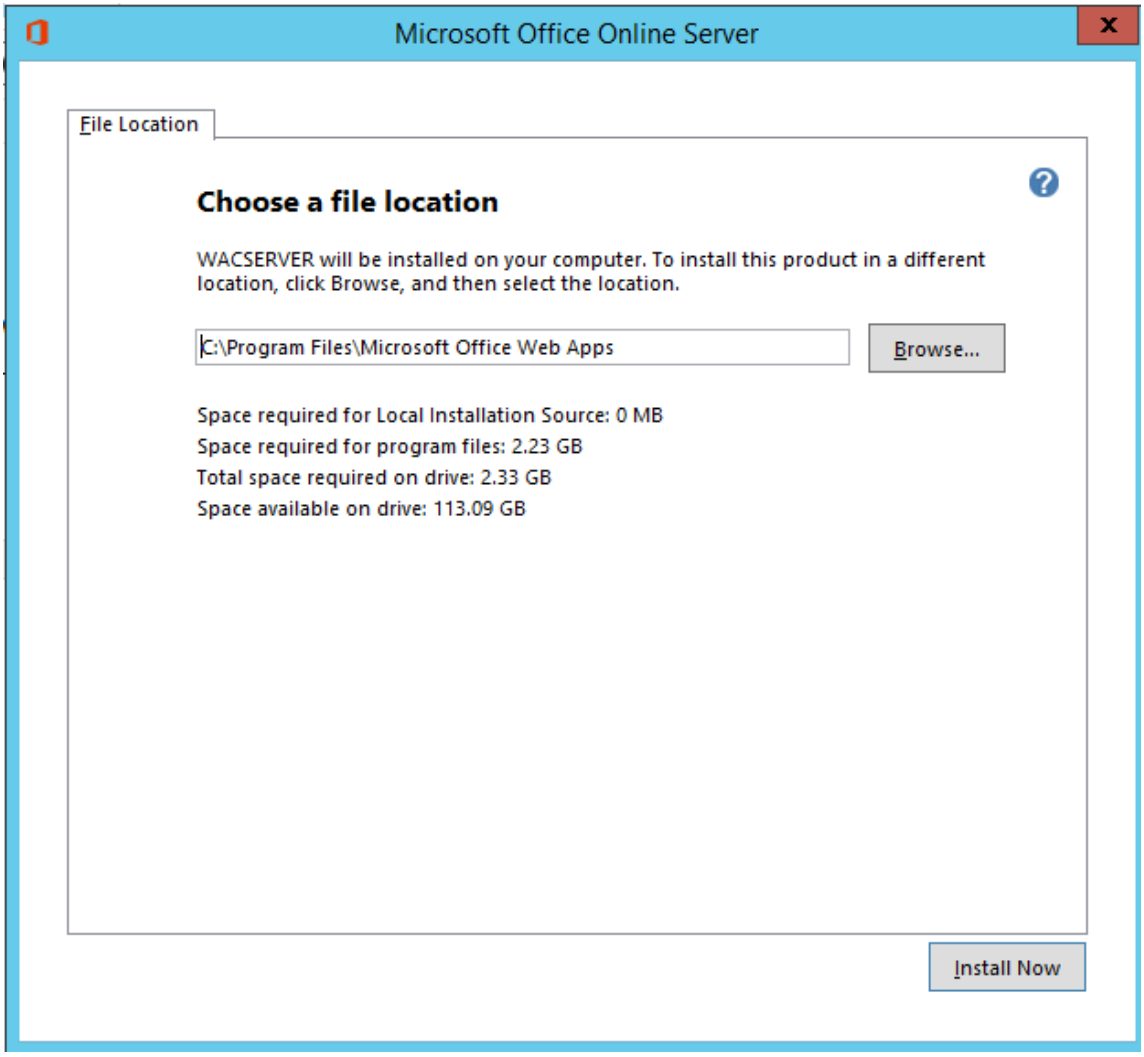
2. Restart the server to apply the changes.
3. Install all available windows updates and restart the server if prompted.
4. Open the Windows PowerShell prompt as an administrator and run the following command to install the required roles and services. After the installation restart the server.

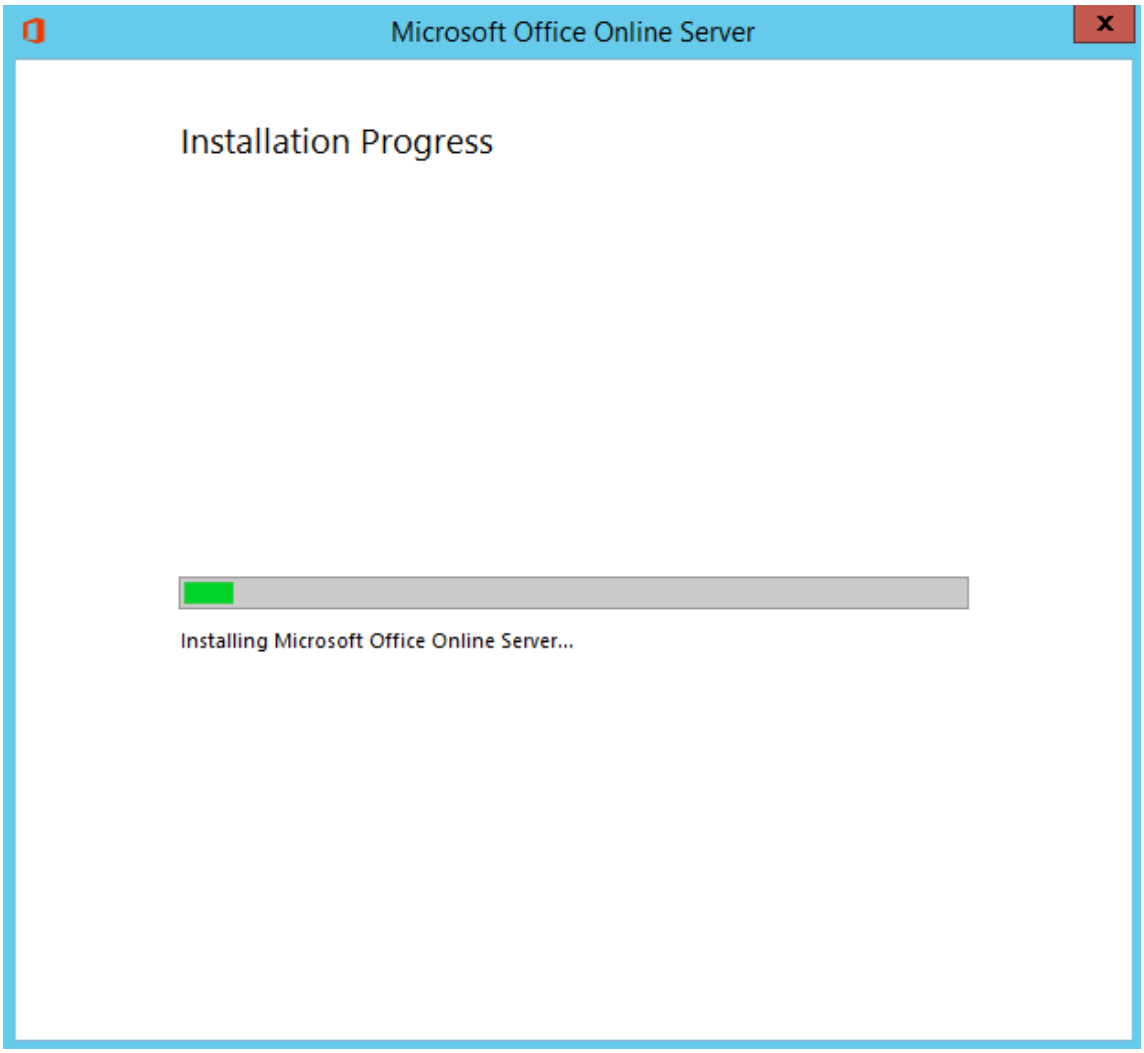
```
Add-WindowsFeature

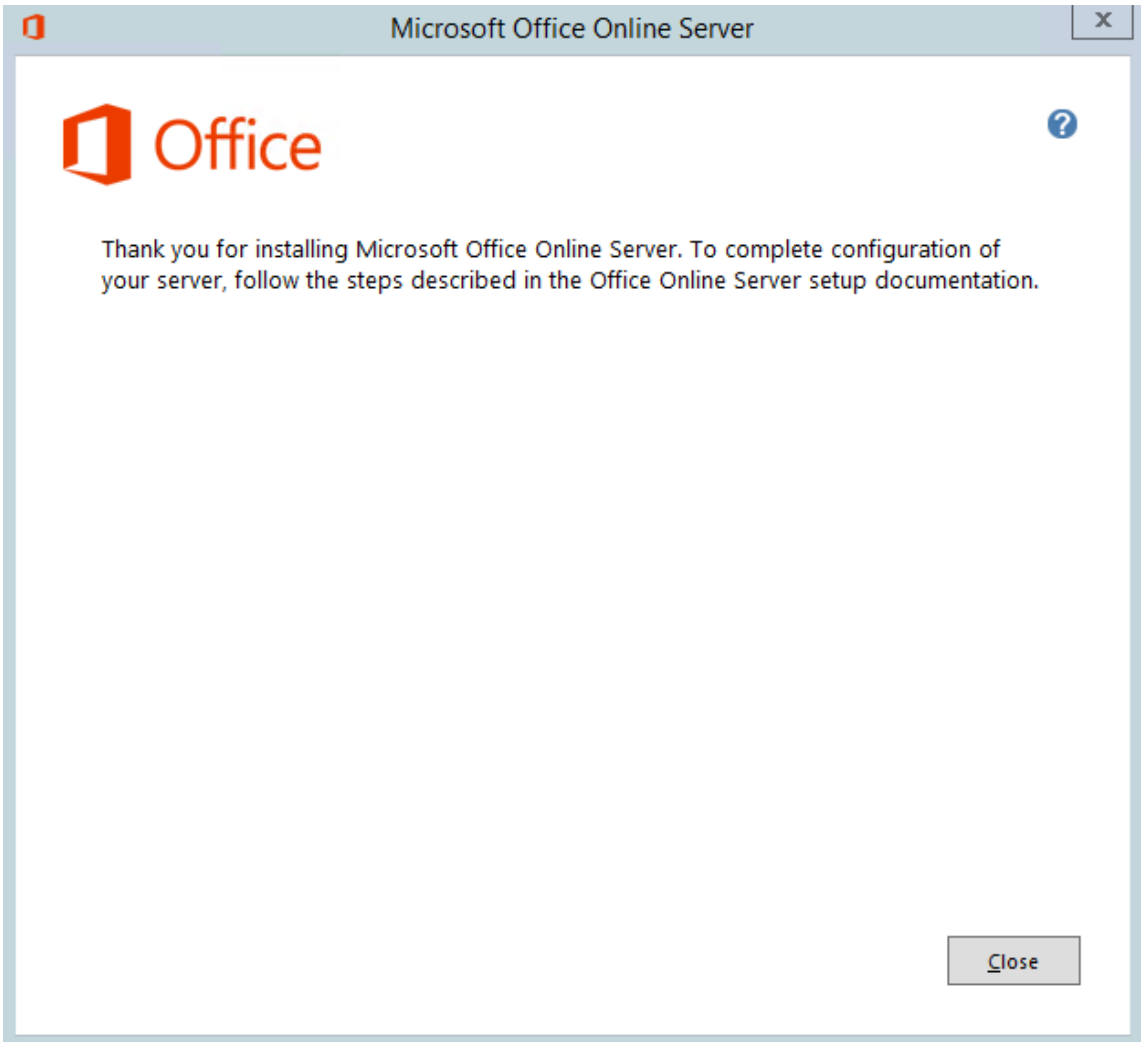
Web-
Server,Web-
Mgmt-
Tools,Web-
Mgmt-
Console,Web-
WebServer,Web-
Common-
Http,Web-
Default-
Doc,Web-
Static-
Content,Web-
Performance,Web-
Stat-
Compression,Web-
Dyn-
Compression,Web-
Security,Web-
Filtering,Web-
Windows-
Auth,Web-
App-
Dev,Web-
Net-
Ext45,Web-
Asp-
Net45,Web-
ISAPI-
Ext,Web-
ISAPI-
Filter,Web-
Includes,InkandHandwritingServices,NET-
Framework-
Features,NET-
Framework-Core,NET-HTTP-Activation,NET-Non-HTTP-Activ,NET-WCF-HTTP-Activation45
```

5. Download Office Online Server from the Volume License Service Center. Go to the location where you downloaded Office Online Server and run setup.exe.


DVD Drive (F:) 16.0.7601.6800
Application Tools
File
Home
Share
View
This PC
DVD Drive
Search DVD Drive (F:) 16.0.760...
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Catalog
Files
Office.en-us
Updates
WacServer.W
WacServerML
autorun
osetup.dll
ReadMe
setup.dll
setup
11 items
1 item selected 265 KB
Microsoft Office Online Server
Read the Microsoft Software License Terms
To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT OFFICE ONLINE SERVER
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
* updates,
* supplements,
* Internet-based services, and
* support services
for this software, unless other terms accompany those items. If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.
AS DESCRIBED BELOW, USING THE SOFTWARE ALSO OPERATES AS YOUR CONSENT TO THE TRANSMISSION OF CERTAIN COMPUTER INFORMATION FOR INTERNET-BASED SERVICES.
IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE PERPETUAL RIGHTS BELOW.
I accept the terms of this agreement
Continue


Microsoft Office Online Server
File Location
Choose a file location
WACSERVER will be installed on your computer. To install this product in a different location, click Browse, and then select the location.
C:\Program Files\Microsoft Office Web Apps
Browse...
Space required for Local Installation Source: 0 MB
Space required for program files: 2.23 GB
Total space required on drive: 2.33 GB
Space available on drive: 113.09 GB
Install Now


Microsoft Office Online Server
Installation Progress
Installing Microsoft Office Online Server...



6. Open the Windows PowerShell prompt as an administrator and run the following command to Import the OfficeWebApps powershell module.

```
import-module “C:\Program Files\Microsoft Office Web
Apps\AdminModule\OfficeWebApps\OfficeWebApps.psd1”
```

Note: Windows powershell for Office Online Server provide offers powershell cmdlets to create and manage Office Web Apps. You can find complete reference document here: https://technet.microsoft.com/en-us/library/jj219436.aspx

Deploy as single-server Office Online Server farm that uses HTTP

1. Open the Windows PowerShell prompt as an administrator and run the **New-OfficeWebAppsFarm** command to create a new Office Online Server farm that consists of a single server, as shown in the following example. This example creates an Office Online Server farm on the local server that has editing enabled as well as http access.

   > You need to login as the Domain Administrator to run the New-OfficeWebAppsFarm cmdlet. Local administrator account is not sufficient. Make sure you replace the URL with your domain names.

   ```
   New-OfficeWebAppsFarm -InternalUrl "http://ooserver.internal.contoso.com"
   -ExternalUrl "http://oos.contoso.com" -AllowHttp -EditingEnabled
   ```

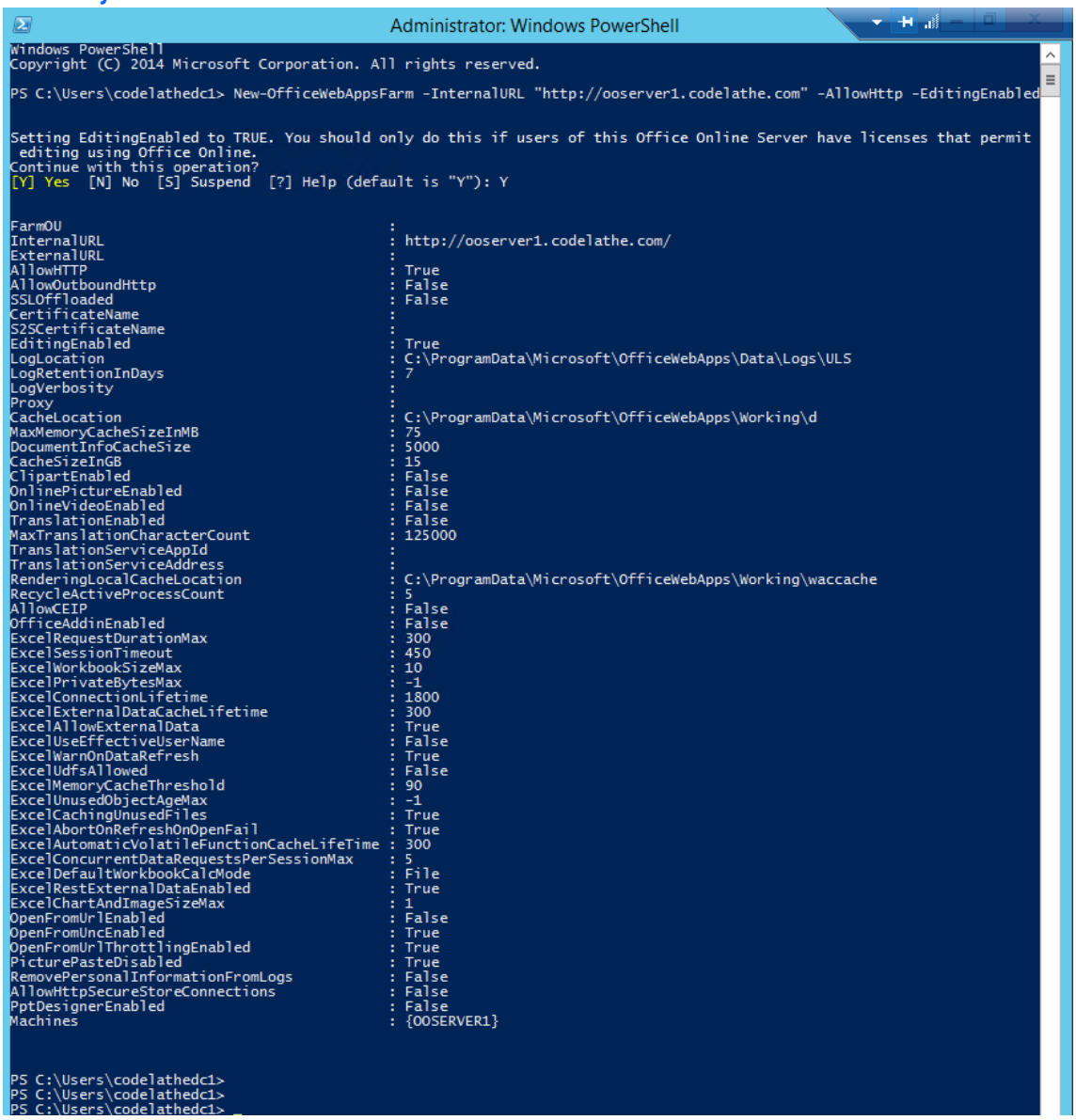
   Parameters

   - **–InternalURL** is the name of the server that runs Office Online Server
   - **–ExternalURL** Specifies the URL that clients use to access the Office Online Server from the Internet
   - **–AllowHttp** configures the farm to use HTTP.
   - **–EditingEnabled** enables editing in Office Online Server when used with FileCloud.

   Additional parameters that configure translation services, proxy servers, ClipArt support, and Online Viewers are described in New-OfficeWebAppsFarm.

2. Verify that Office Online Server Farm was created successfully. After the farm is created, details about the farm are displayed in the Windows PowerShell prompt like given below. To verify that Office Online Server is installed and configured correctly, use a web browser to access the Office Online Server discovery URL, as shown in the following example. The discovery URL is the *InternalUrl* parameter you specified when you configured your Office Online Server farm, followed by **/hosting/discovery**, for example: **http://oos.yourdomain.com/hosting/**

discovery



Deploy as single-server Office Online Server farm that uses HTTPS

1. Obtain and import an SSL certificate with the fully qualified domain name(s) (FQDN) of the Office Online Server server. You only need to configure one FQDN on the certificate. For example, oos.contoso.com. If you have different internal and external FQDNs, you'll need to configure both FQDNs on the certificate. For example, oos.internal.contoso.com and oos.contoso.com.
2. Configure DNS records to point the FQDN(s) on the certificate to your Office Online Server server. If you have different DNS servers for internal and external users, you'll need to configure the appropriate FQDN on each server.

3. Open Windows PowerShell and run the following commands. When you run the commands, replace the example FQDNs and certificate friendly name with your own.

   Same internal and external FQD

```
New-OfficeWebAppsFarm -InternalURL "https://oos.contoso.com" -ExternalURL
"https://oos.contoso.com" -CertificateName "OfficeOnlineCertificate"
```

   Different internal and external FQDNs

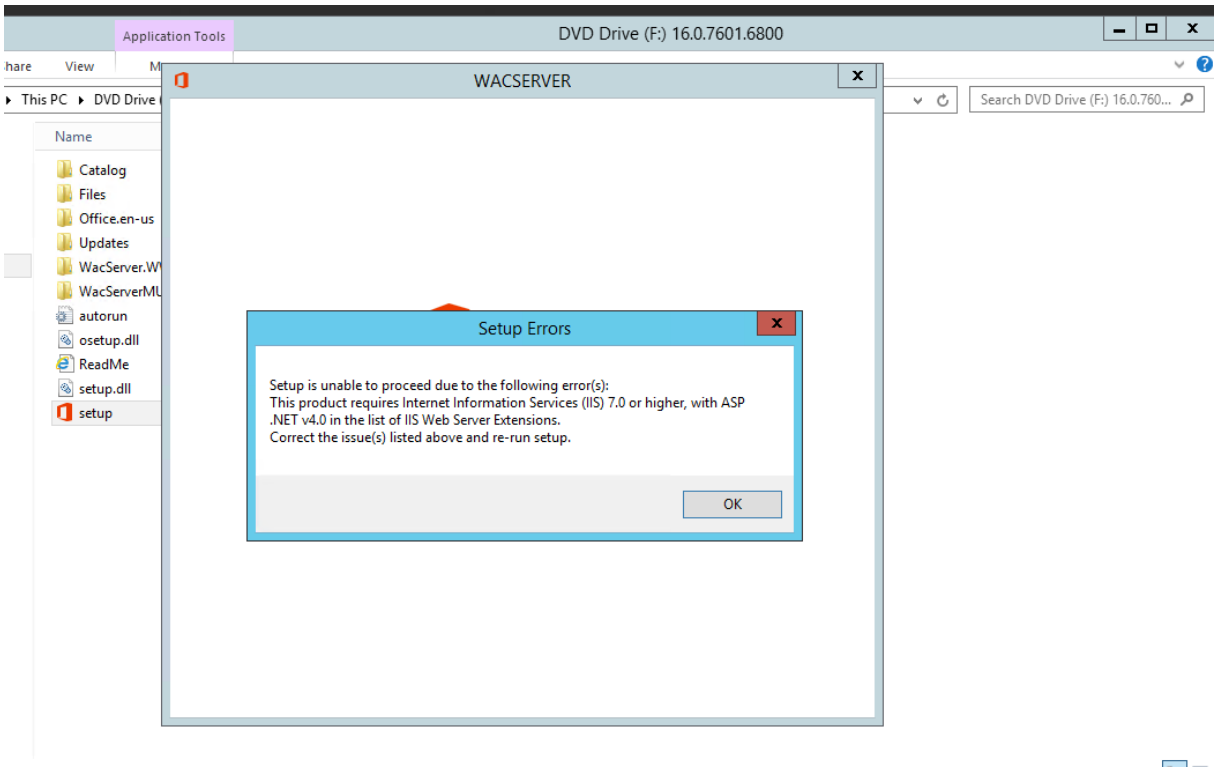
```
New-OfficeWebAppsFarm -InternalURL "https://oos.internal.contoso.com" -ExternalURL
"https://oos.contoso.com" -CertificateName "OfficeOnlineCertificate"
```



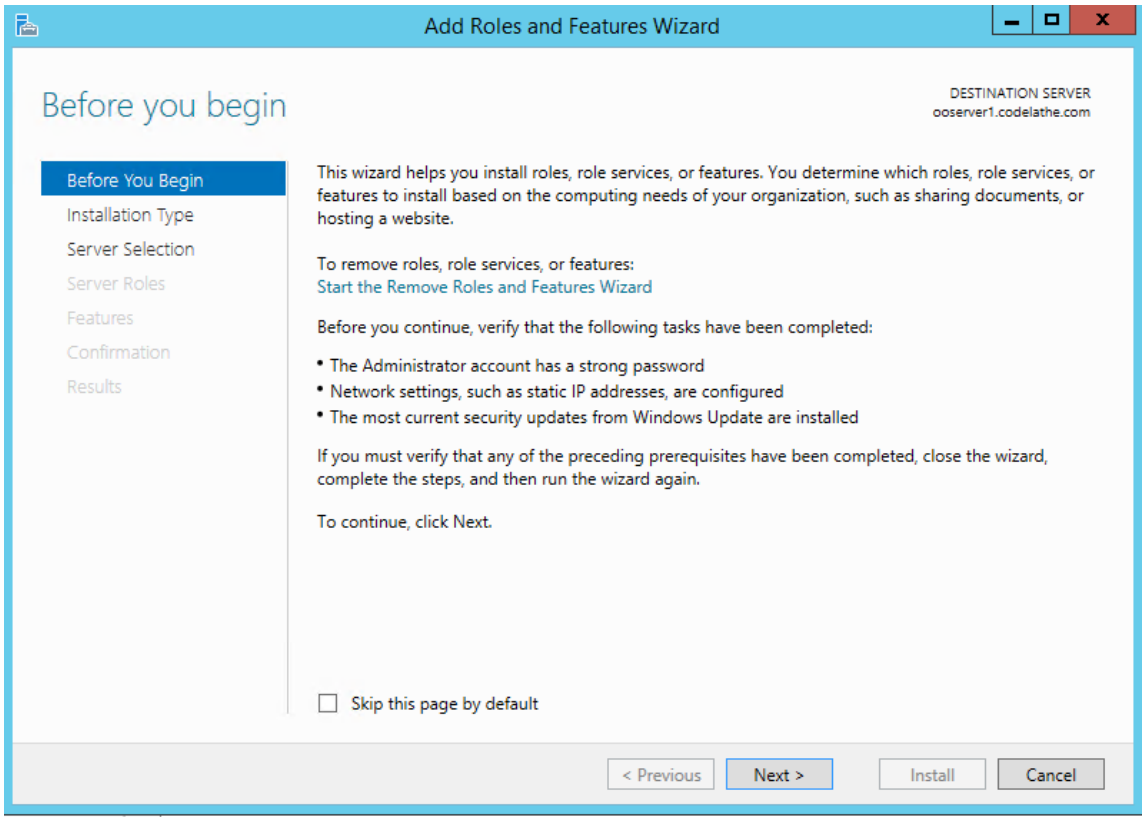
It is possible to use the wildcard ssl certificate. You need to import the ssl certificate to you certificate store.

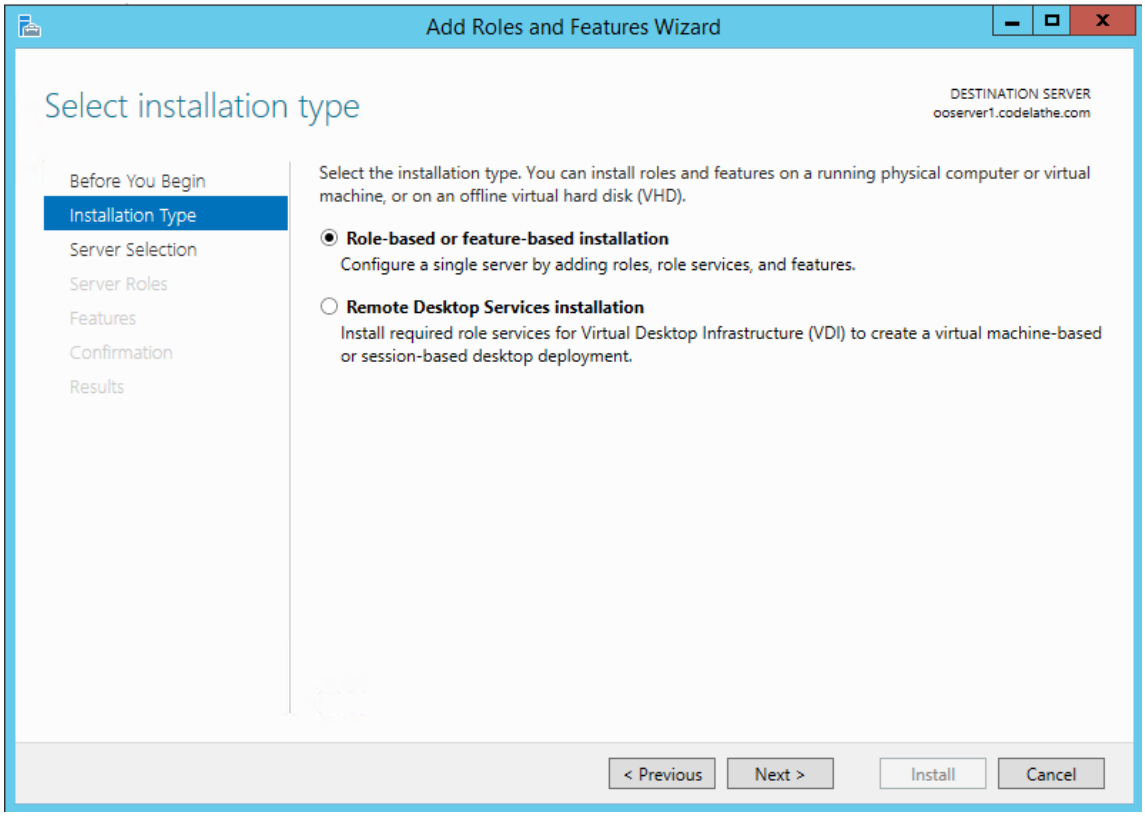
Troubleshooting Tips

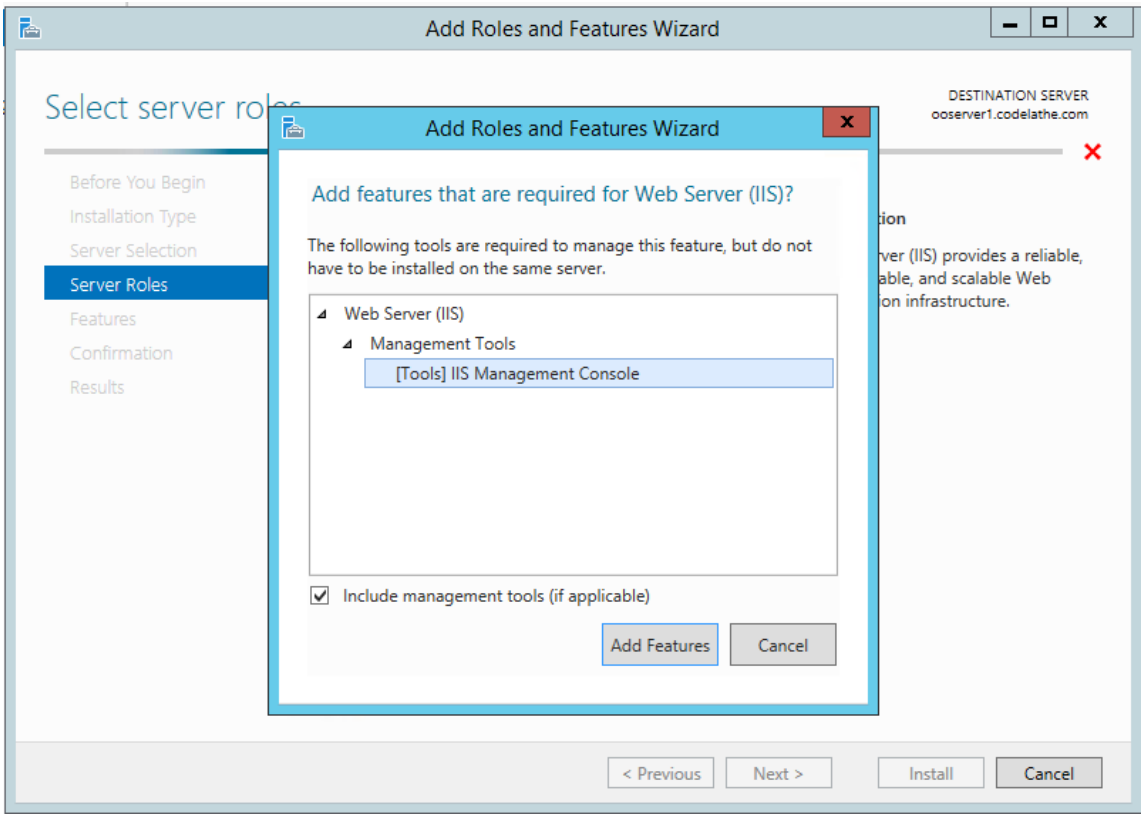
If you receive an error during the setup, You need to enable web server role and ASP.NET 45

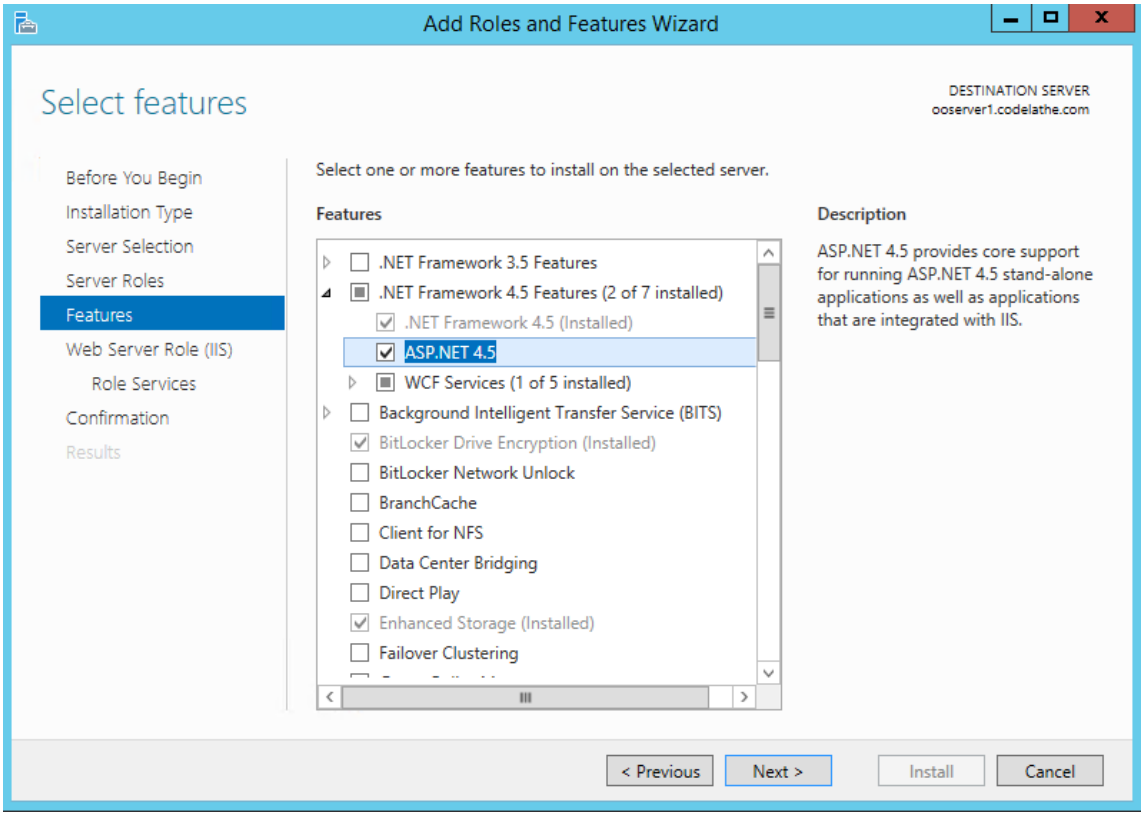


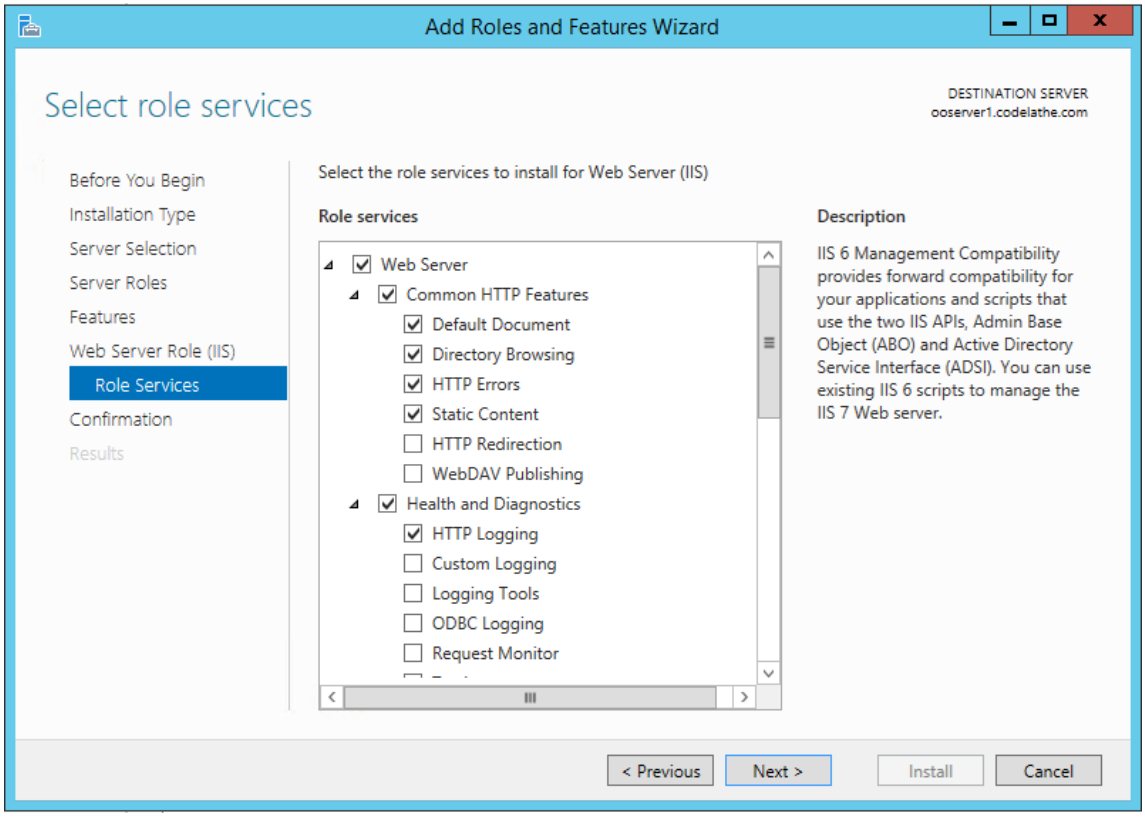
- Start Add Roles, Features Wizard from Server Manager --> Manage --> Add Roles and Features. Enable IIS Web Server Role and ASP.Net Feature. Confirm the selections and install.

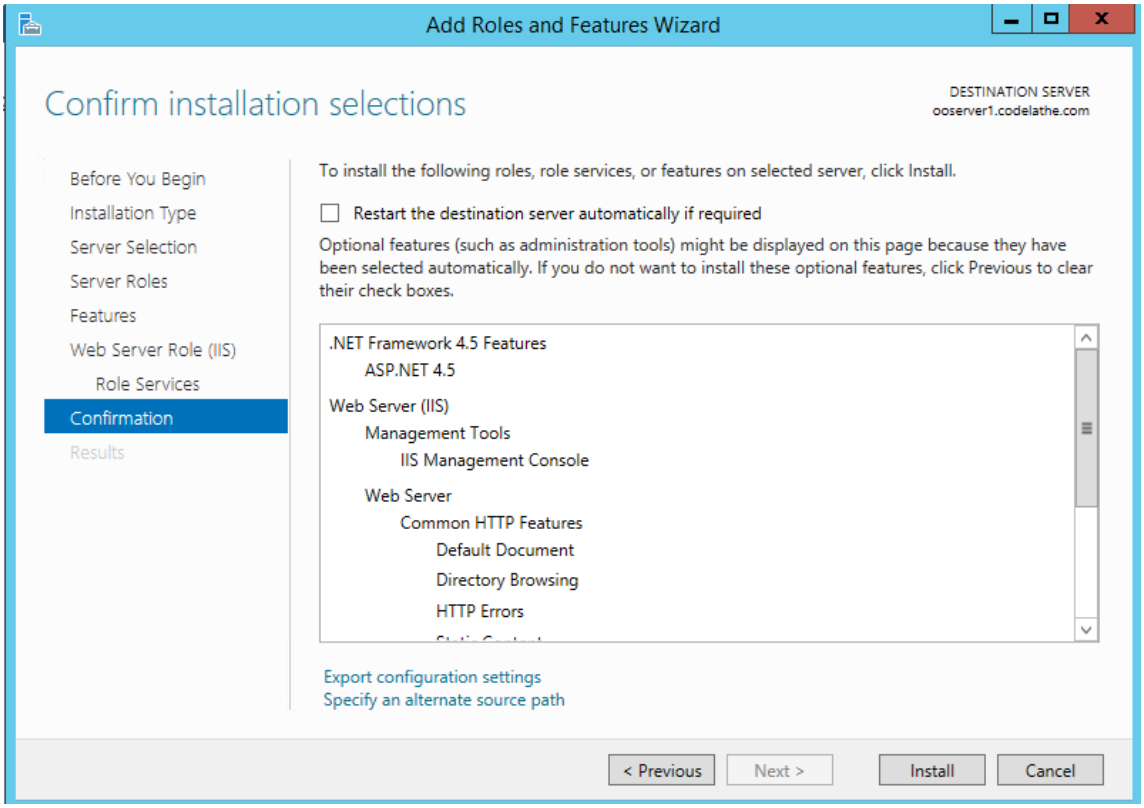

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select features
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.5 Features (2 of 7 installed)
.NET Framework 4.5 (Installed)
ASP.NET 4.5
WCF Services (1 of 5 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption (Installed)
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Direct Play
Enhanced Storage (Installed)
Failover Clustering
Description
ASP.NET 4.5 provides core support for running ASP.NET 4.5 stand-alone applications as well as applications that are integrated with IIS.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Description
IIS 6 Management Compatibility provides forward compatibility for your applications and scripts that use the two IIS APIs, Admin Base Object (ABO) and Active Directory Service Interface (ADSI). You can use existing IIS 6 scripts to manage the IIS 7 Web server.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
ooserver1.codelathe.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
.NET Framework 4.5 Features
ASP.NET 4.5
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Configuring FileCloud To Use Office Online On-Premises Server For Web Edit

Introduction

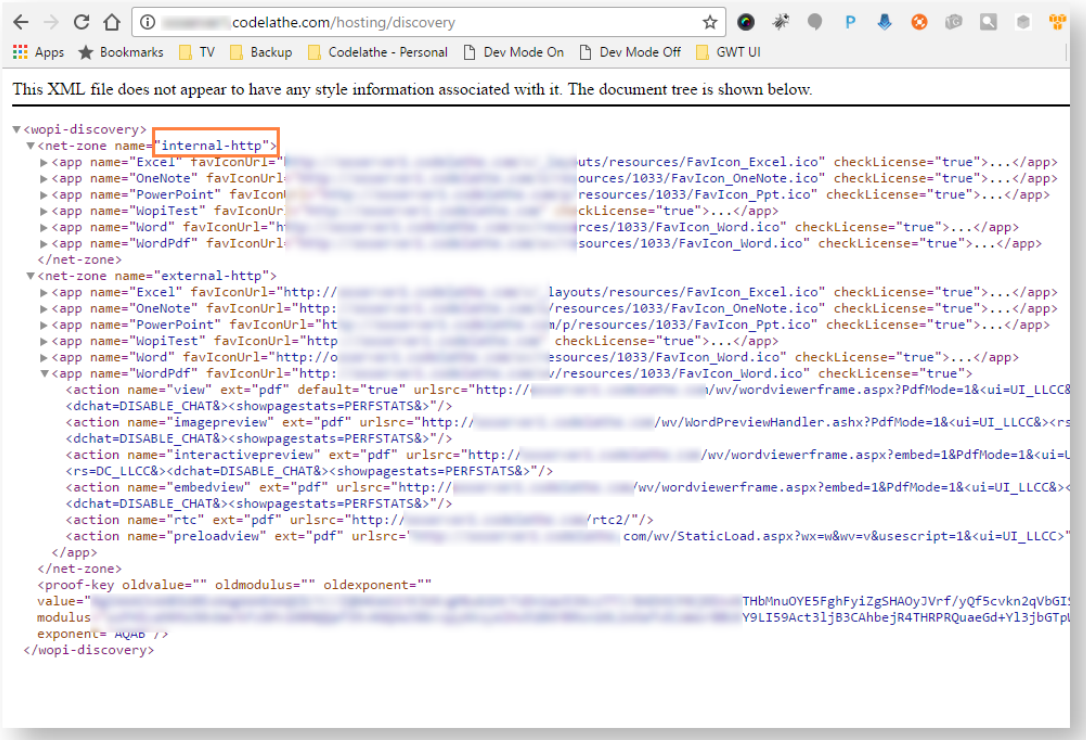
FileCloud supports web based document editing using Microsoft Office Online. FileCloud uses the WOPI protocol to connect to Office Online for web based editing.
This document assumes that you have already installed an Office Online server.

Configuration Tips

- When configuring FileCloud with Office Online on-premises server, please use the default admin user to log in into FileCloud admin portal. For security reasons, this configuration is not allowed as a normal user promoted as admin.

Configuring FileCloud With Office Online

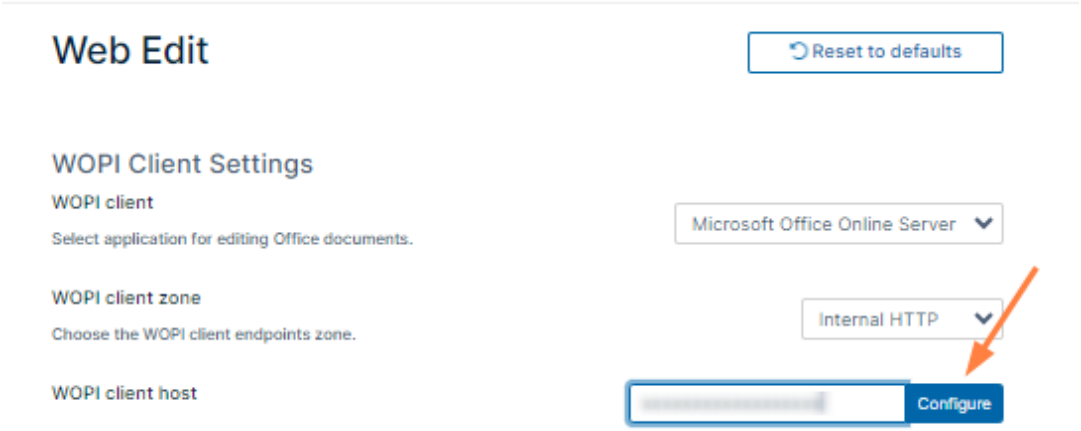
1. Navigate to the URL http[s]://IPAddressOfYourOfficeOnlineServer/hosting/discover using a browser. This is the page that contains all the information about the various editors supported by Office Online server.
2. From the resulting page, note zone of editors to be used by FileCloud. The selection depends on the requirement of where the web edit feature will be used. In our case, we will choose "internal-http", as we want to offer web-editing only to internal users.



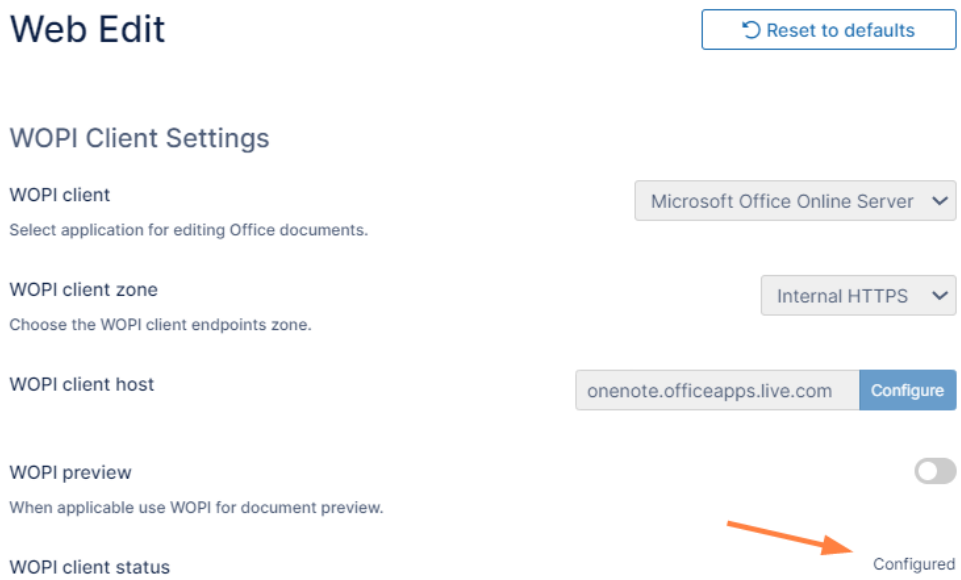
3. Ensure that the Office Online server has access to the FileCloud server (To verify: navigate to FileCloud user login page from Office Online server).
4. Add the Office Online server to the Content Security policy in the .htaccess file.
   a. Open the .htacess file:
   Windows: C:\xampp\htdocs\.htaccess
   Linux: /var/www/html/.htaccess
   b. Find the line: **Header set Content-Security-Policy**, and add your Office Online server url without http or https, for example **oos.company.com** to the url's listed for **default-src**, **script-src**, **frame-src**, and **img-src**:

   ```
   Header set Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com
   *.core.windows.net oos.company.com www.google.com
   http://127.0.0.1:34320/v1/fileassociations; style-src 'unsafe-inline' 'self';script-src 'unsafe-
   inline' 'unsafe-eval' 'self' www.google.com oos.company.com www.gstatic.com
   teams.microsoft.com *.teams.microsoft.com *.skype.com;frame-src 'self' www.google.com
   oos.company.com *.live.com docs.google.com accounts.google.com; font-src 'self' data:;img-
   src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com
   *.core.windows.net oos.company.com *.office.net; frame-ancestors 'self'
   teams.microsoft.com *.teams.microsoft.com *.skype.com;
   ```

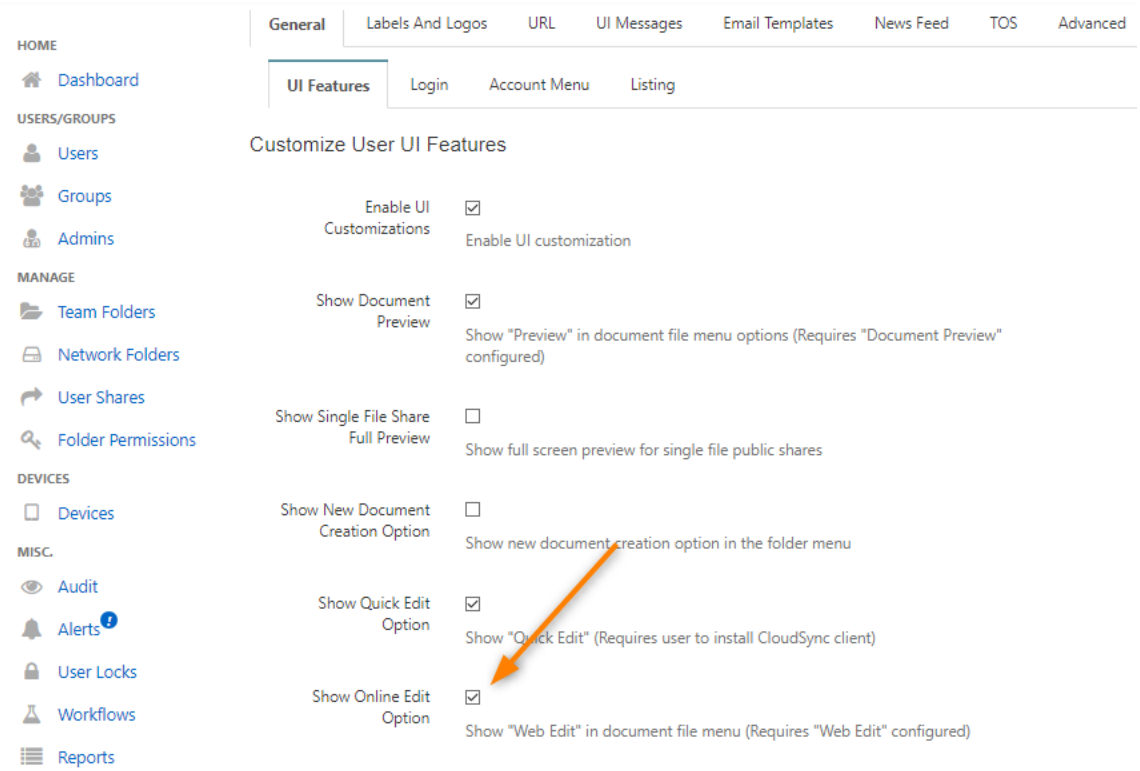
   c. Save your changes.
5. Configure FileCloud with Office Online Cloud.
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Web Edit**  .
   The **Web Edit** settings page opens.
   b. Fill in the following values for the first three settings:
   WOPI client: Microsoft Office Online Server
   WOPI client zone: Internal HTTP
   WOPI client host: IP address/URL of office online server used as WOPI client host.
   c. Click **Configure.**



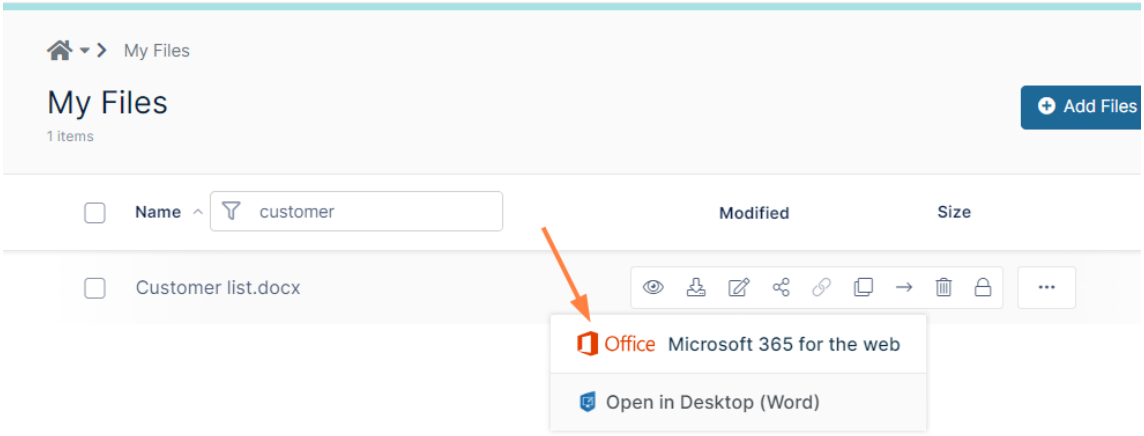
Upon successful configuration, the following screen should appear.



6. Now that FileCloud server is configured with office online server, enable the web edit option for users.
   To enable web edit in user portal and user clients, navigate to **Customizations > General > UI Features** and check **Show Online Edit Option**. Click **Save**.



7. Now login in to the user portal and hover over an editable Office document. Hover over the Web Edit icon, and ensure that you see the Office icon and Microsoft 365 for the web.



8. Click the icon and confirm that the document opens in its Office for the web editor.

Web Editing With Collabora Code

This section explains how to configure FileCloud to use Collabora Code for web editing.

Prerequisites

- The Collabora server must be installed. For help, see Collabora's Installation Guide.
- Reverse Proxy must be set up for the Collabora URL. For help, see Collabora's Installation Guide, Proxy Settings.

In this section

Configuring FileCloud To Use Collabora CODE For Web Edit

> Beginning in FileCloud 23.261, watermarks appear on documents when edited using Collabora CODE.

FileCloud supports web based document editing using Collabora CODE. FileCloud uses the WOPI protocol to connect to office online for web based editing.

Note: This document assumes that the administrator has already installed Collabora CODE completely and ready for use.

For Collabora CODE installation, refer to the official Collabora documentation at:

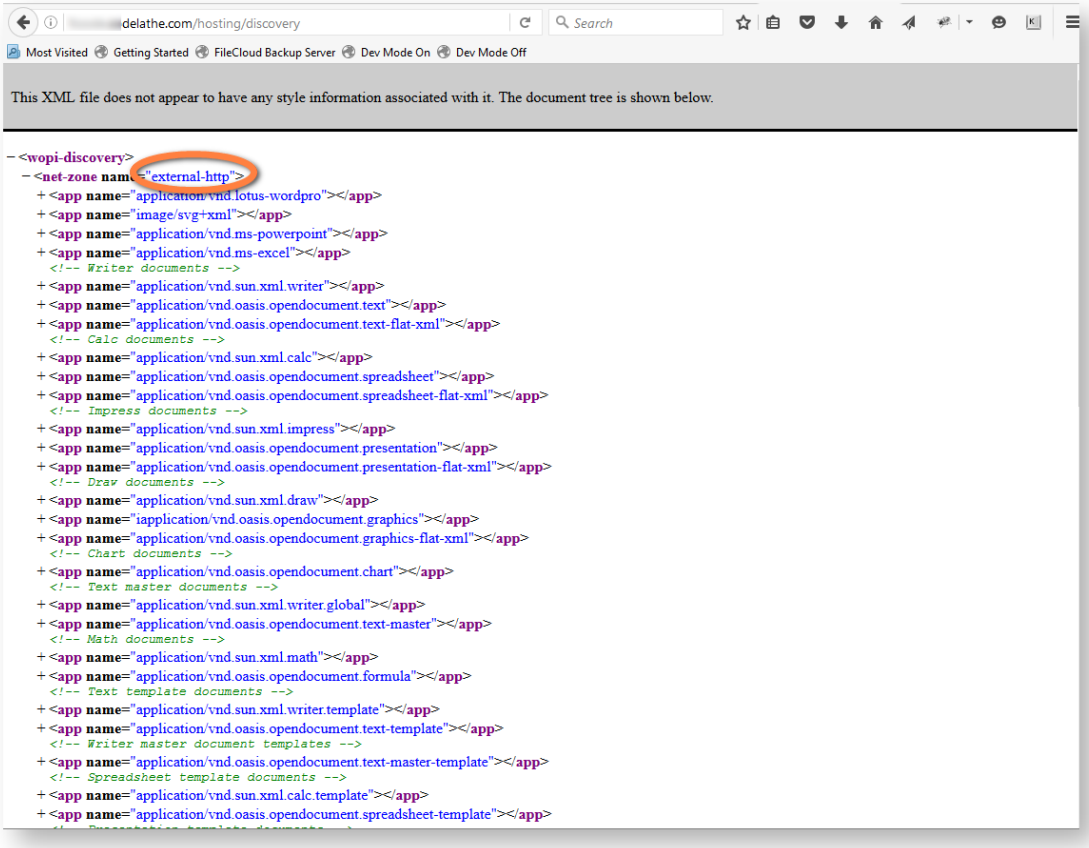
https://sdk.collaboraonline.com/docs/installation/CODE_Docker_image.html
https://sdk.collaboraonline.com/docs/installation/Proxy_settings.html#reverse-proxy-with-apache-2-webserver

Configuration Tips

- When configuring FileCloud with Collabora CODE, please use the default 'admin' user to login into FileCloud admin UI. For security reasons, this configuration is not allowed as a normal user promoted as admin.

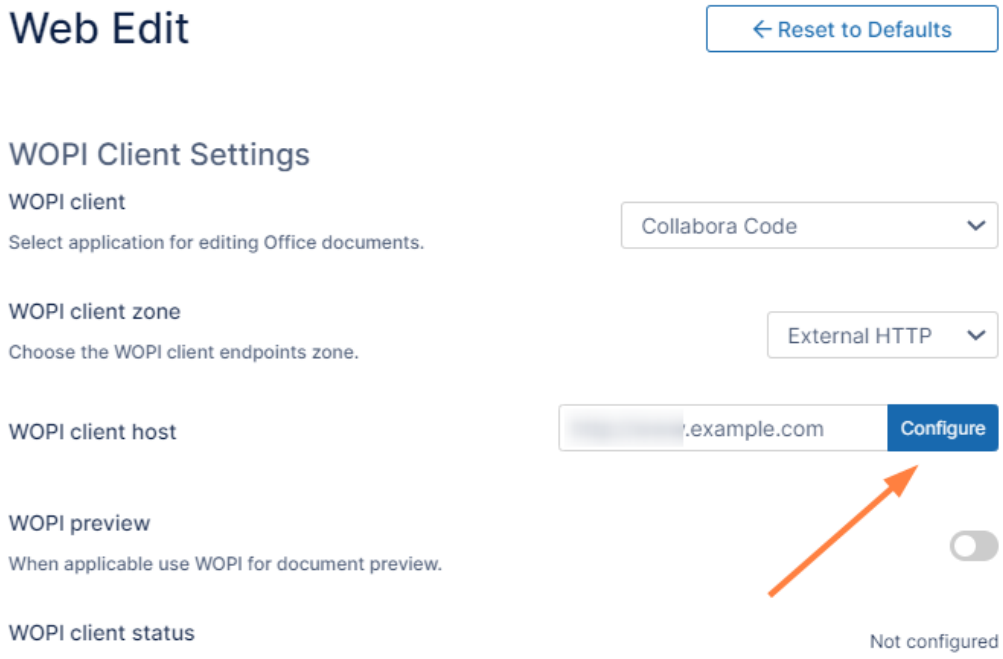
Configuring FileCloud With Collabora CODE

1. Navigate to the URL http[s]://IPAddressOfYourCODEServer/hosting/discovery using a browser. This is the page that contains all the information of various editors supported by CODE server.
2. From the resulting page, note zone of editors to be used by FileCloud. The selection depends on the requirement of where the web edit feature will be used. In our case, we will choose "external-http", as we want to offer web-editing to external users.

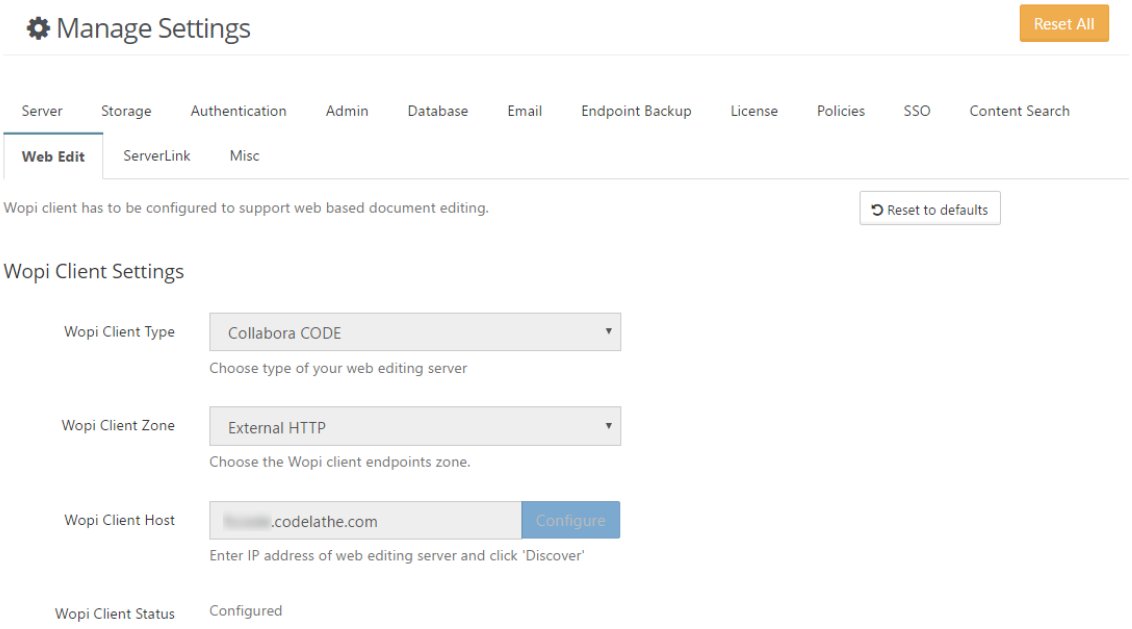


3. Ensure that the CODE server has access to the FileCloud server (To verify: navigate to FileCloud user login page from code server).

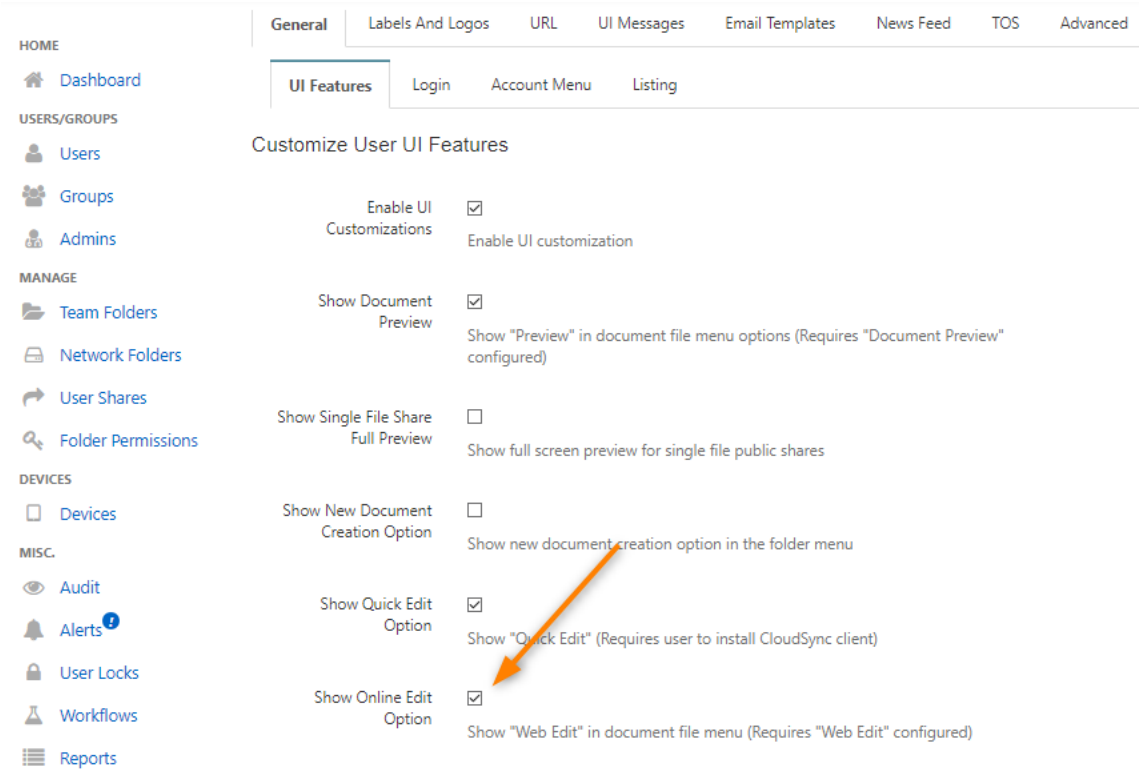
4. Configure FileCloud with Collabora CODE.
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Web Edit** .
   The **Web Edit** settings page opens.
   b. Fill in the following values for the first three settings:
   WOPI client: Collabora CODE
   WOPI client zone: External HTTP
   WOPI client host: IP address/URL of office online server used as WOPI client host.
   c. Click **Configure**.



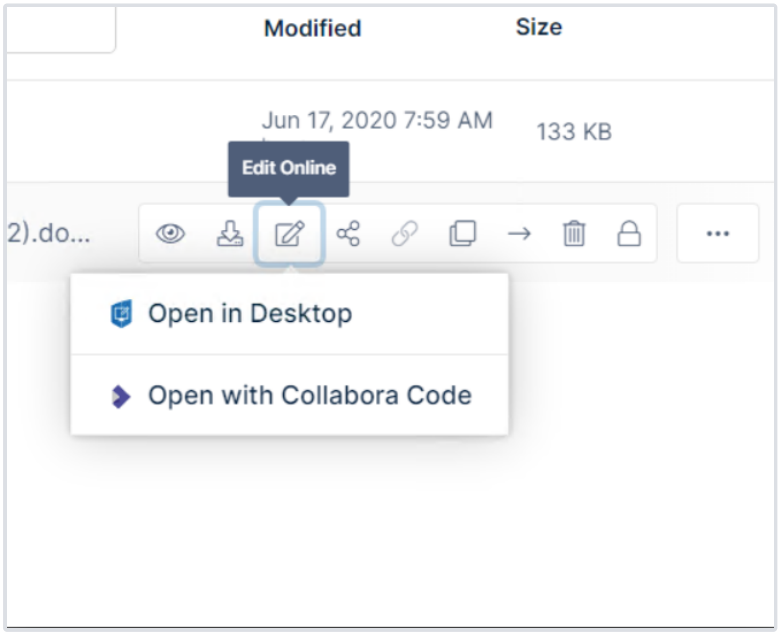
5. WOPI client status should now be **Configured**:



6. Now that FileCloud server is configured with Collabora CODE, enable web edit for users if it is not already enabled.
   To enable web edit in the user portal and client user interfaces, navigate to **Customizations > General > UI** Features tab and check the option **Show Online Edit Option**. Click **Save**.



7. Now log in to the user portal, hover over a document and click the **Web Edit** icon. Ensure **Open with Collabora Code appears**.



Watermarks in Collabora CODE

Watermarks configured using FileCloud's Watermark Settings appear on pages edited using Collabora CODE.
However, the watermark is displayed as tiles on the page with fixed font size and style. The watermarks are not saved to the file, and do not appear when the file is downloaded or printed.

Note: Collabora includes its own watermark feature for Office files, which are saved to the document; these watermarks do appear when the file is downloaded or printed.

Configuring FileCloud to use Collabora CODE for File Creation

To configure FileCloud to use Collabora Code for file creation:

1. Configure FileCloud to use Collabora CODE according to the instructions in Configuring FileCloud To Use Collabora CODE For Web Edit.
2. Create a folder for storing templates such as *C:\documenttemplates*.
3. In the folder, create empty Office templates, each having the filename *template*, for example, *template.docx, template.pptx, template.xlsx*.
4. In **C:\xampp\htdocs\config\cloudconfig.php** add the following line:
   define("WOPI_CLIENT_TEMPLATE_DIR", "C:\documenttemplates");
   You can now create files that match the template types you have added.

Web Editing with OnlyOffice

> FileCloud version 23.261.2 and above require an OnlyOffice secret key of 256 characters minimum. If you are using OnlyOffice and have a secret key that is less than 256 characters, regenerate it so that it is the required length, and replace the value in the Web edit settings.

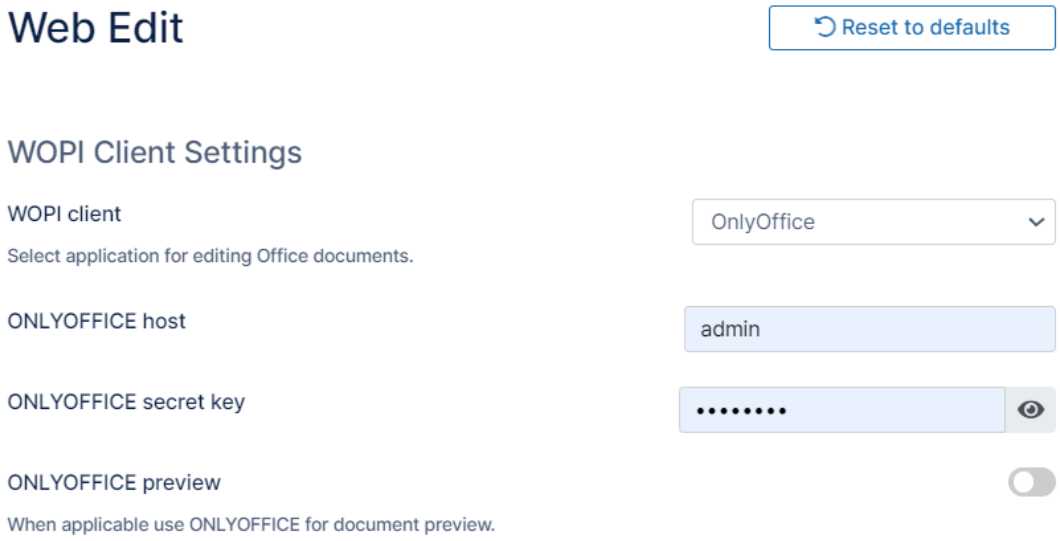
> For OnlyOffice integration to be effective, the OnlyOffice URL must be accessible over HTTPS with a valid SSL certificate and chain certificate.

FileCloud supports web based document editing using OnlyOffice. The following procedures assume you have already installed OnlyOffice.

Configuring FileCloud with OnlyOffice

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

2. In **WOPI Client Type**, choose **Only Office**.
   The screen displays OnlyOffice settings.



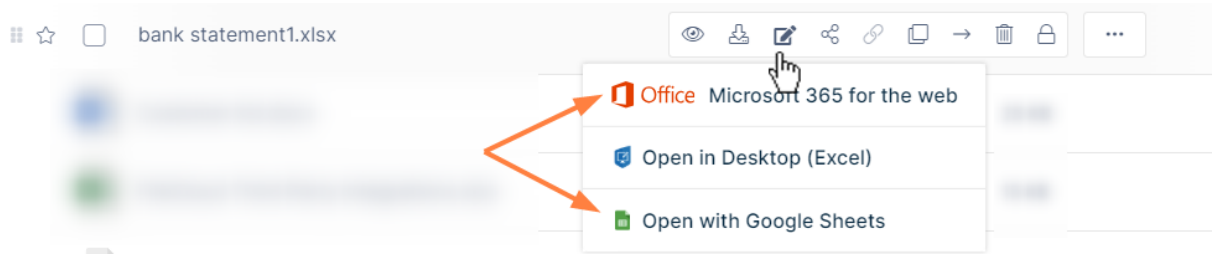
3. Enter the **OnlyOffice host** and **OnlyOffice secret key.**
4. To preview as well as edit supported file types in OnlyOffice, check **OnlyOffice preview**.
5. Click **Save**.
6. Add the OnlyOffice Server to the Content Security Policy in the .htaccess file.
   a. Open the .htacess file:
   Windows: C:\xampp\htdocs\.htaccess
   Linux: /var/www/html/.htaccess
   b. Find the line: **Header set Content-Security-Policy**, and add your url without http or https, for example **youronlyoffice.serveraddress.com** to the url's listed for **script-src** and **frame-src**:

```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.amazonaws.com *.core.windows.net
www.google.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com
www.gstatic.com youronlyoffice.serveraddress.com;frame-src 'self' www.google.com *.live.com
youronlyoffice.serveraddress.com; font-src 'self' data:;img-src www.gstatic.com 'self' data: blob:
*.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net"
```

   c. Save your changes.
   Now users can Web edit with OnlyOffice.

Web Editing with Google Apps

Beginning with FileCloud 21.3, you can integrate FileCloud with Google Apps to make an additional Web Edit option. Google Apps cannot replace your current WOPI client, but may be added as an additional option, so that when users select to Web Edit docx, xlsx, pptx files, both the WOPI client and the Google app are listed as options for opening it:



In FileCloud's mobile apps, files can be viewed but not edited in Google Apps.

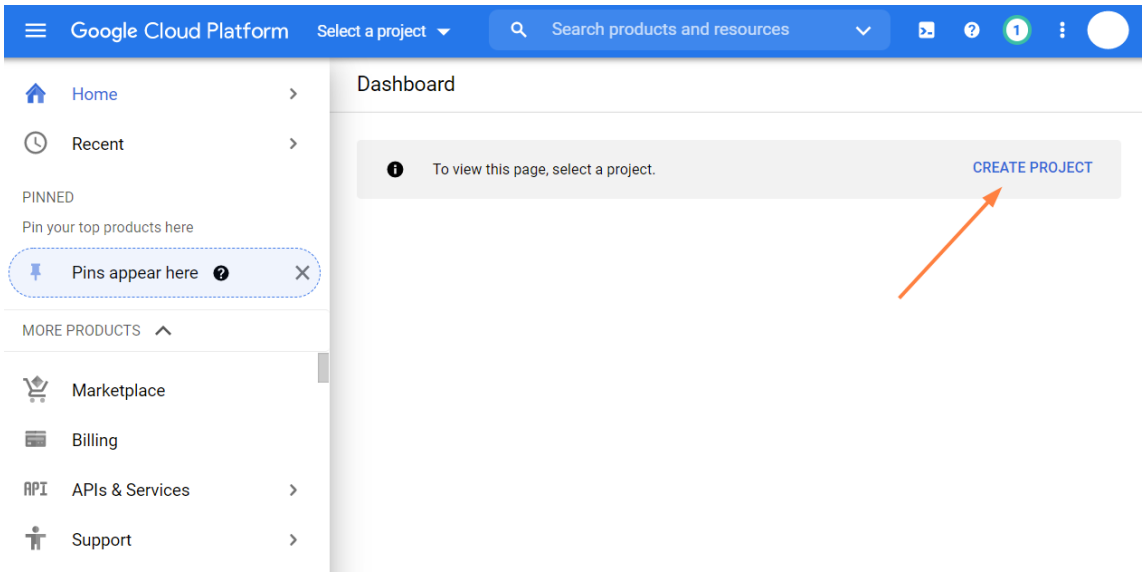
- Editing of some large files is not supported in Google Apps. See Files you can store in Google Drive for specific size limitations.
- To open a Google Apps editor in incognito windows, you may first have to grant Google Docs the correct permissions or unblock third party cookies.

To integrate with Google Apps:

Set up Google Apps - FileCloud integration in the Google Cloud platform:

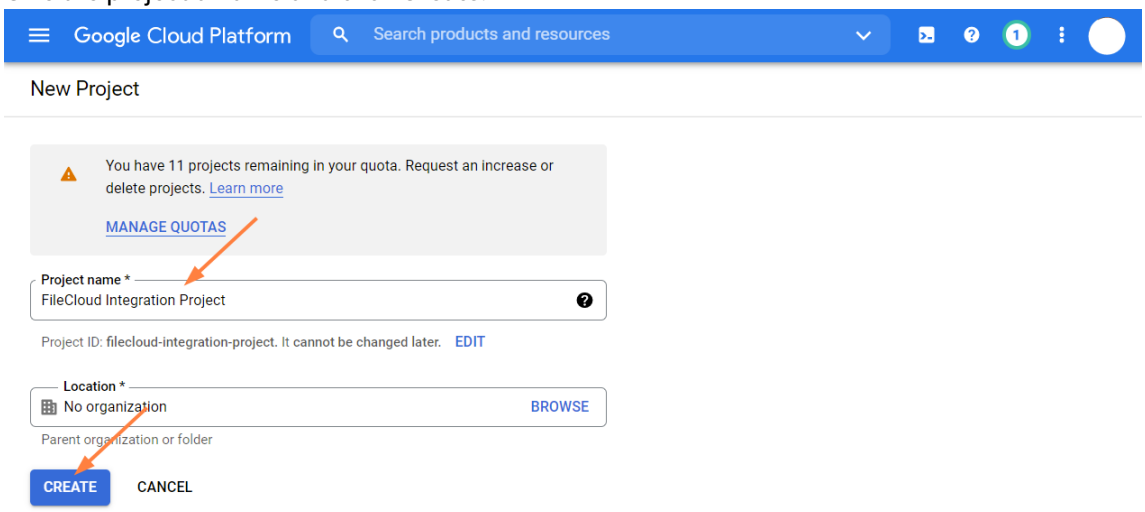
You must have a Google account that you can use to sign in to the Google Cloud Console in order to integrate your system with Google Apps.

1. Access the Google Cloud Console at https://console.cloud.google.com and sign in.
2. Go to **Home > Dashboard**.
3. Click **Create Project**.



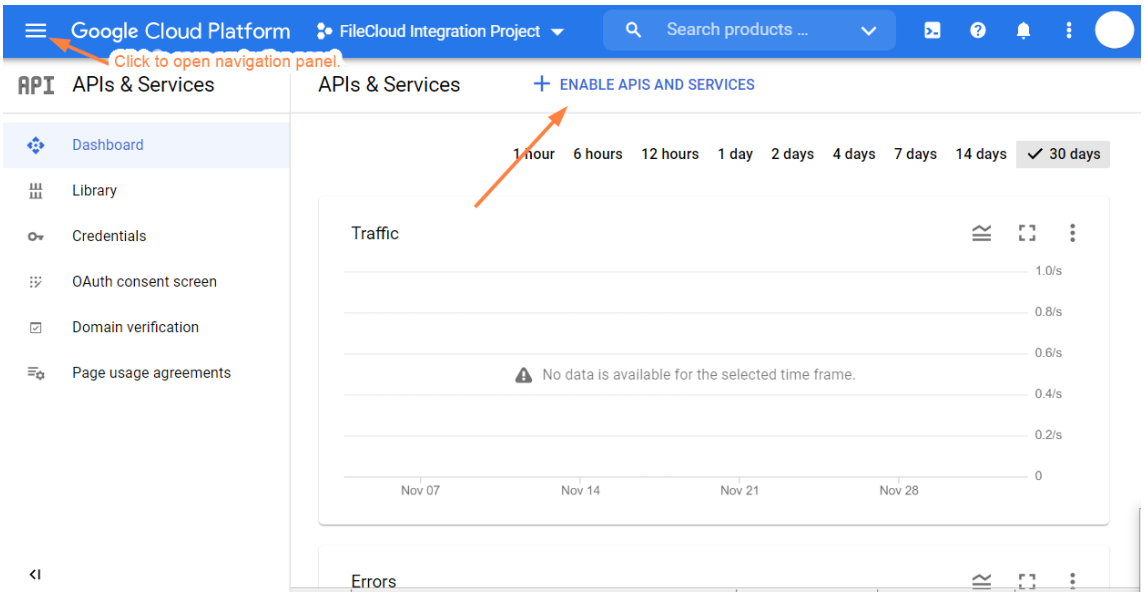
A **New Project** screen opens.

4. Give the project a name and click **Create**.

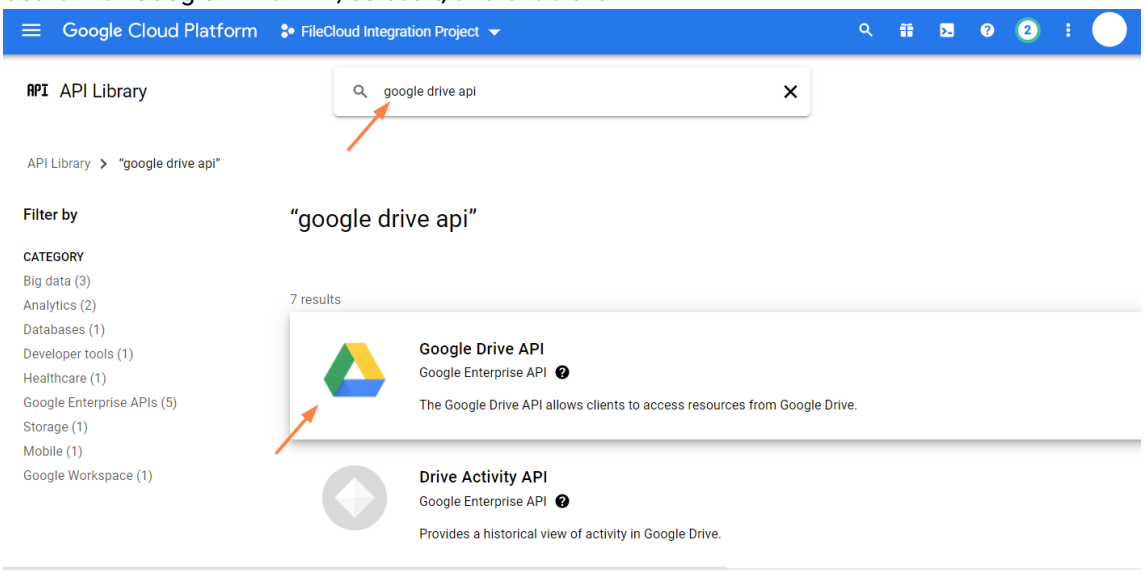


The project opens in the dashboard.

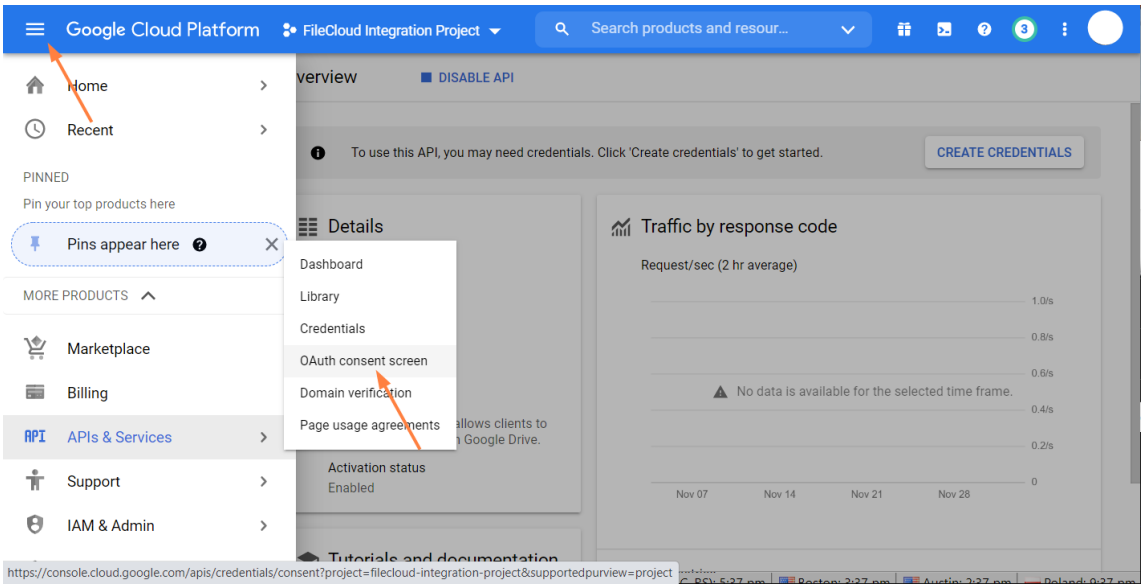
5. In the navigation panel, click **APIs & Services > Dashboard**.
   (If the navigation panel is not visible, click the three bars in the upper-left corner of the screen to open it.)
6. Click **Enable APIs and Services**.



7. Search for Google Drive API , select it, and enable it.



8. Then go back to the main navigation pane, and choose **APIs & Services > OAuth consent screen**.



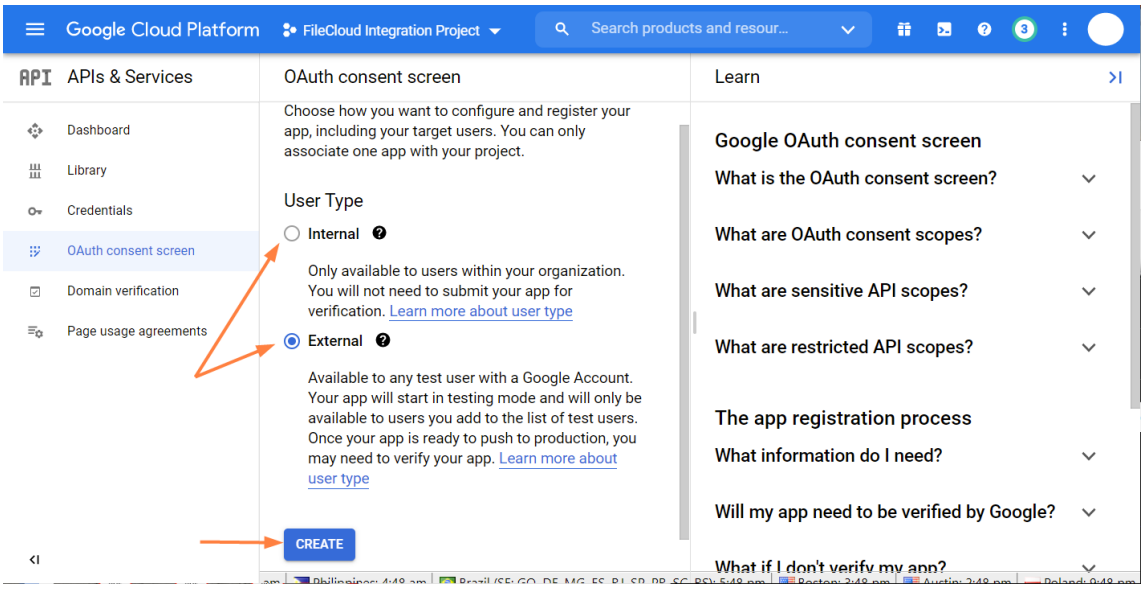
9. For **User Type**, choose **Internal** or **External** depending on the following guidelines:

   Internal means the integration is limited to Google Workspace users within the organization (email domain). **External** allows any Google account.

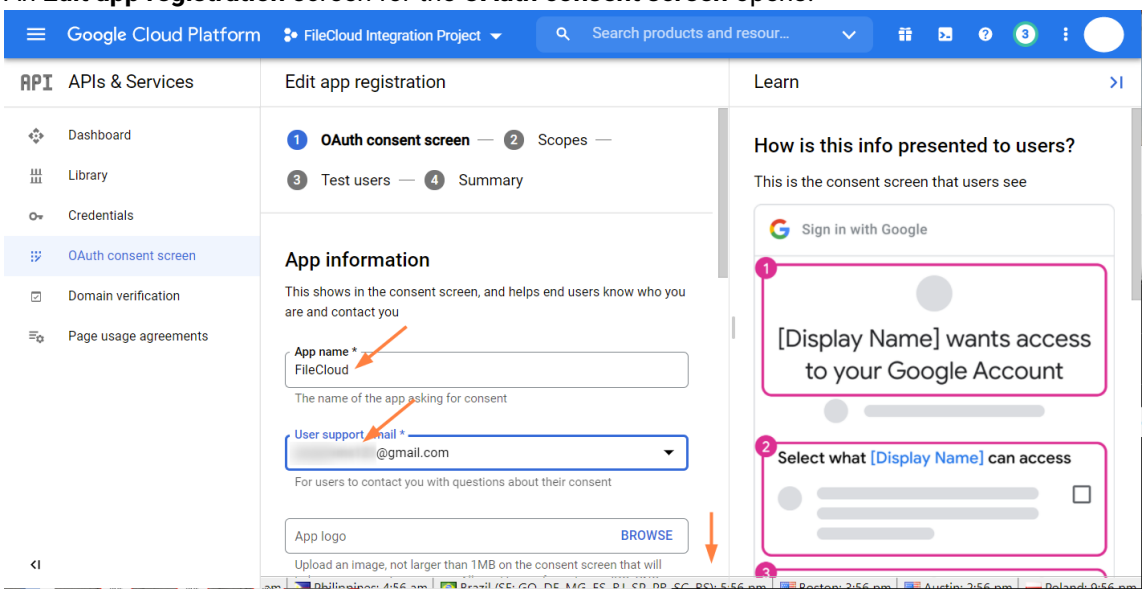
   Free google accounts only allow **External** users, because there is no Google Organization. Paid google accounts can use both, but **Internal** is only allowed if there's a Google Organization set up

   External requires the Google Project to be published into production status. It also may require the Google Project to be verified if it displays an icon or display name for the project on the OAuth consent screen.

10. Click **Create**.

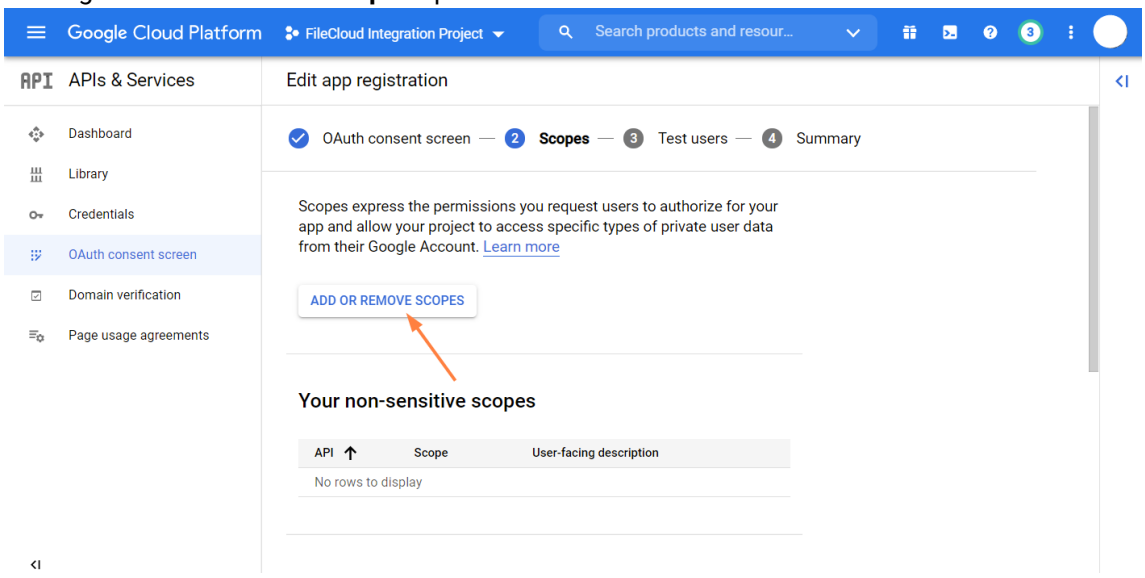


An **Edit app registration** screen for the **OAuth consent screen** opens.



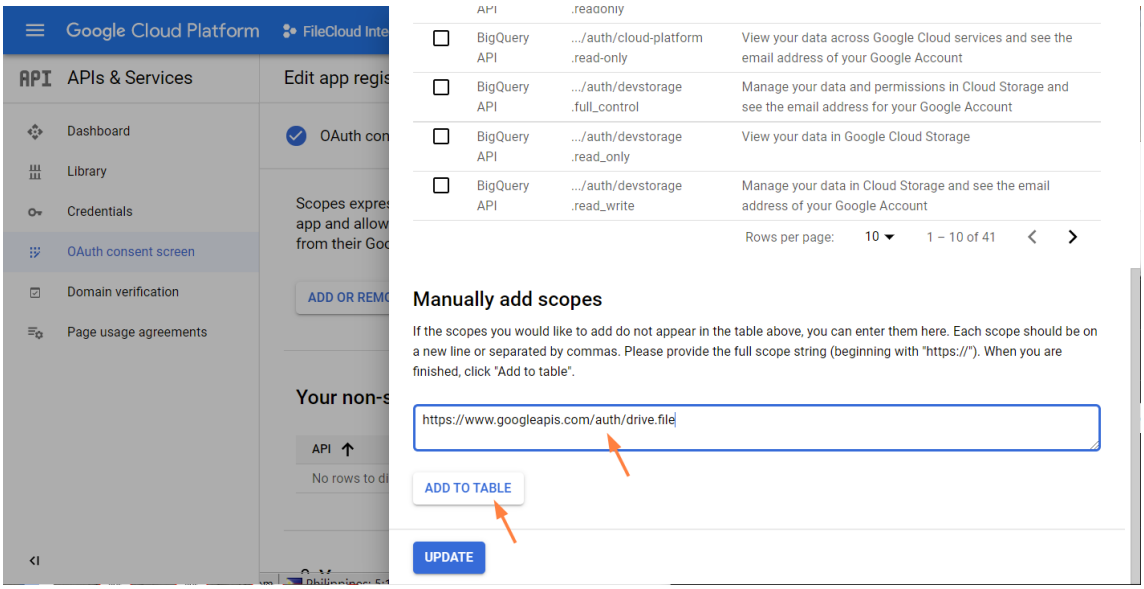
11. Fill in the required information, and then click **Save and Continue**.

The registration screen for **Scopes** opens:

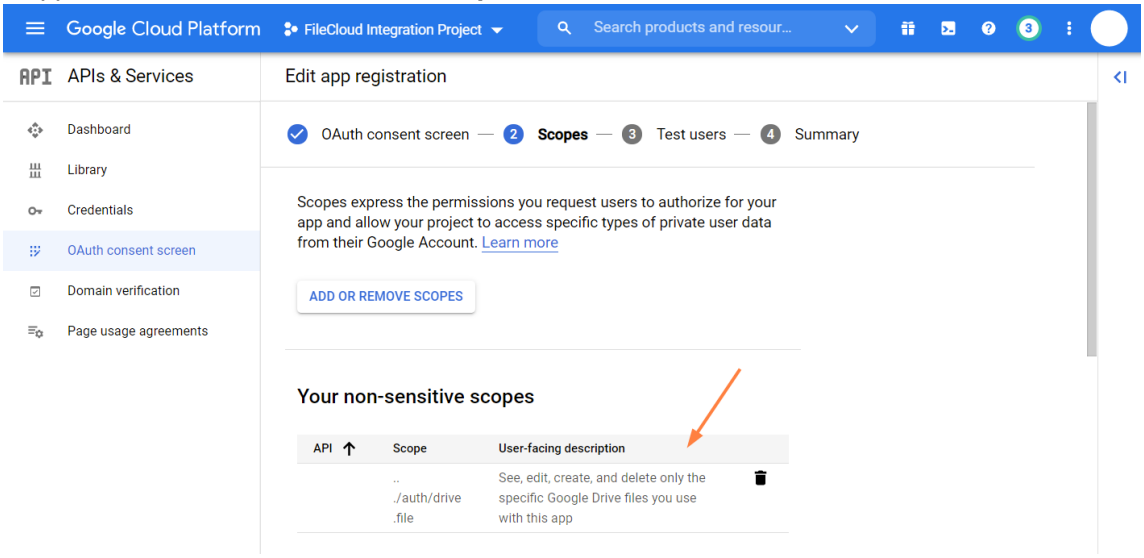


12. Click **Add or Remove Scopes**.
    An **Update Selected Scopes** screen opens.

13. Scroll to the bottom of the screen and manually add https://www.googleapis.com/auth/drive.file. Then click **Add to Table**.

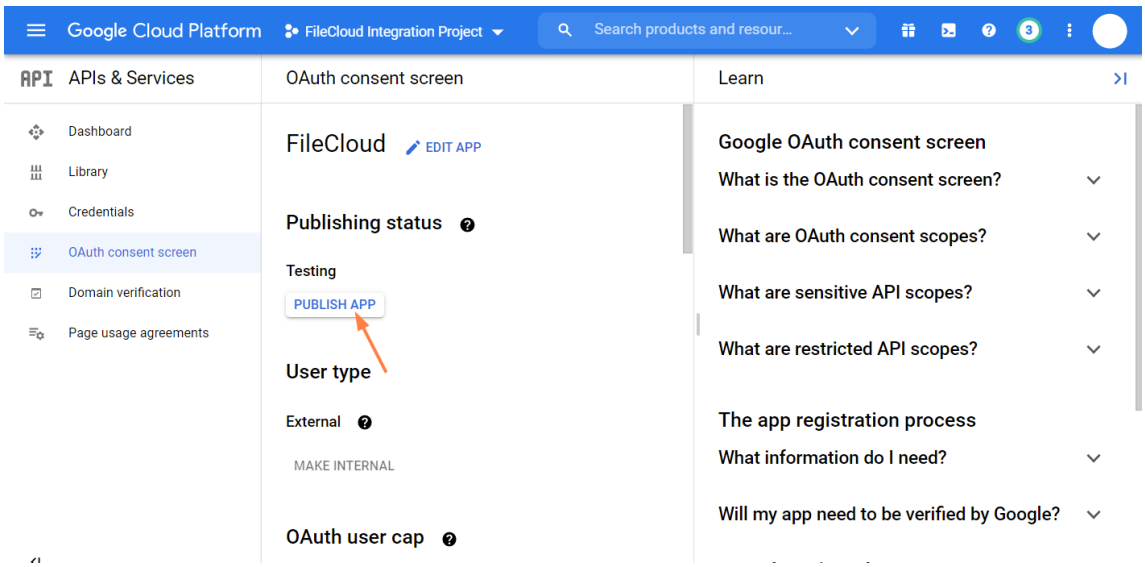


14. Check it in the table and click **Update**.
It appears under **Your non-sensitive scopes**.

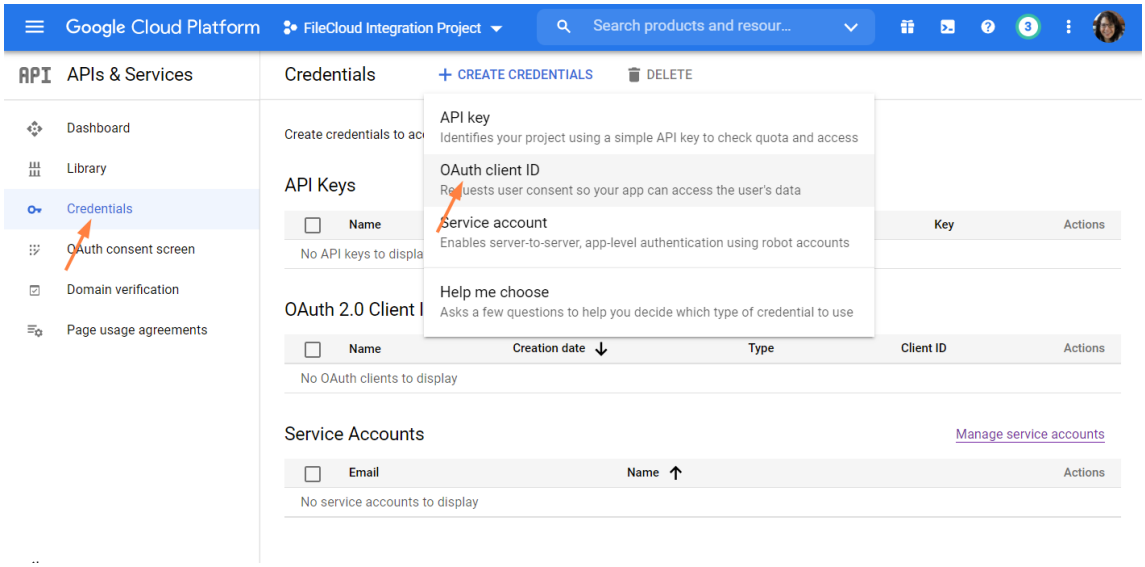


15. Scroll to the bottom of the screen and click **Save and Continue**.
16. In the **Test Users** screen, click **Save and Continue**.

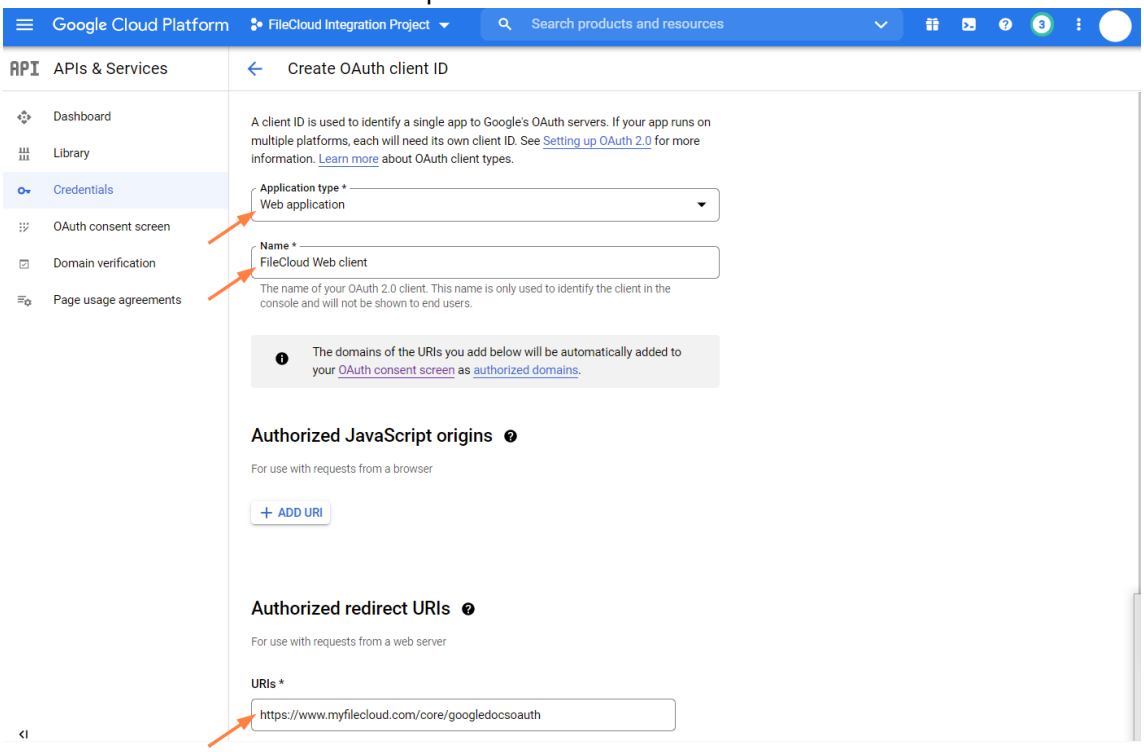
17. In the navigation panel, click **OAuth consent screen** again, and click **Publish App**, and then click **confirm**.



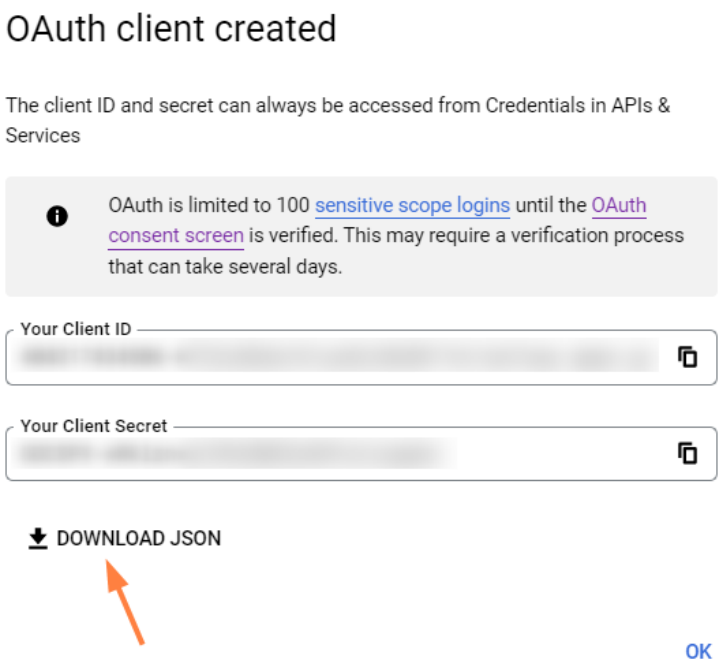
18. In the navigation panel, click **Credentials**, and in the **Credentials** screen, click **Create Credentials**, and choose **OAuth client ID.**



The Create OAuth Client ID screen opens.



19. In **Application type,** select **Web application**.
    In **Name**, enter any name.
    In **URIs** under **Authorized redirect URIs** enter your FileCloud URL appended with **/core/googledocsoauth**, for example, **https://www.myfilecloud.com/core/googledocsoauth**.
20. Click **Create**.
    An OAuth client created message box opens:

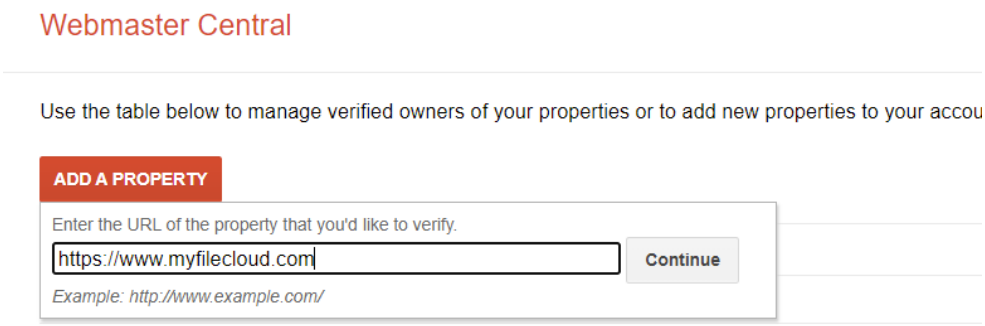


21. Click **Download JSON**, and download and save the JSON file.

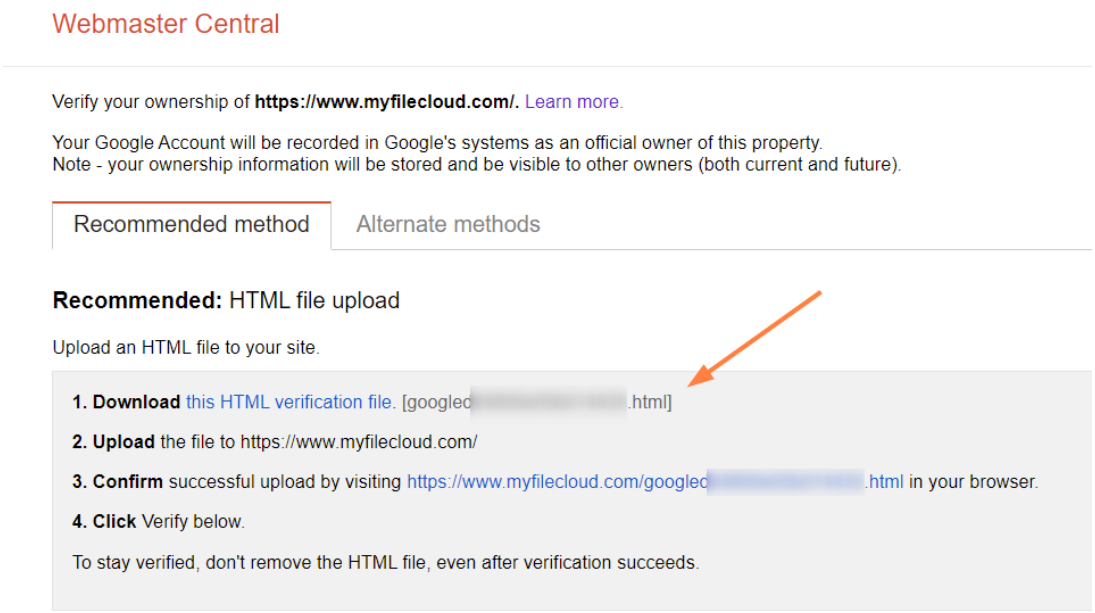
Configure Google Apps in FileCloud

Now we need set up Google Apps in FileCloud by adding the OAuth file and the HTML verification file.

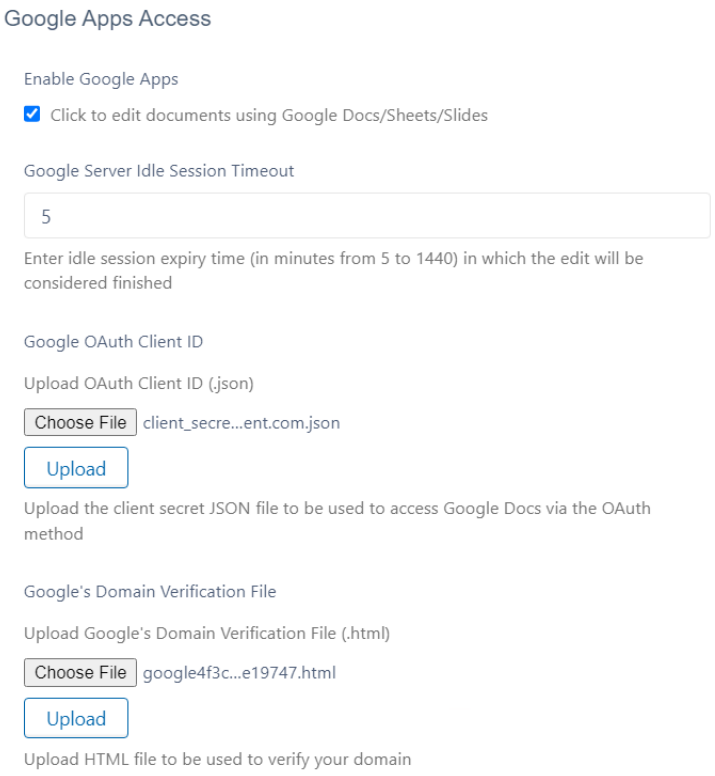
1. Go to https://www.google.com/webmasters/verification/home
2. Click **Add a Property**, put your FileCloud URL (no endpoint appended this time).



3. Click **Continue**.



4. Download the HTML verification file.
5. Now open the FileCloud Admin UI and go to **Settings > Web Edit**, and scroll down to **Google Apps Access**.
6. Check **Enable Google Apps**.
7. For **Google OAuth Client ID**, click **Choose File** to select the JSON file you downloaded and saved in the previous procedure, and then click **Upload** to upload it.
8. For **Google's Domain Verification File**, click **Choose File** to select the HTML file that you just downloaded.



9. Now go back to the https://www.google.com/webmasters/verification page where you have just downloaded the HTML file, and confirm you are not a robot.
10. Click **Verify**.

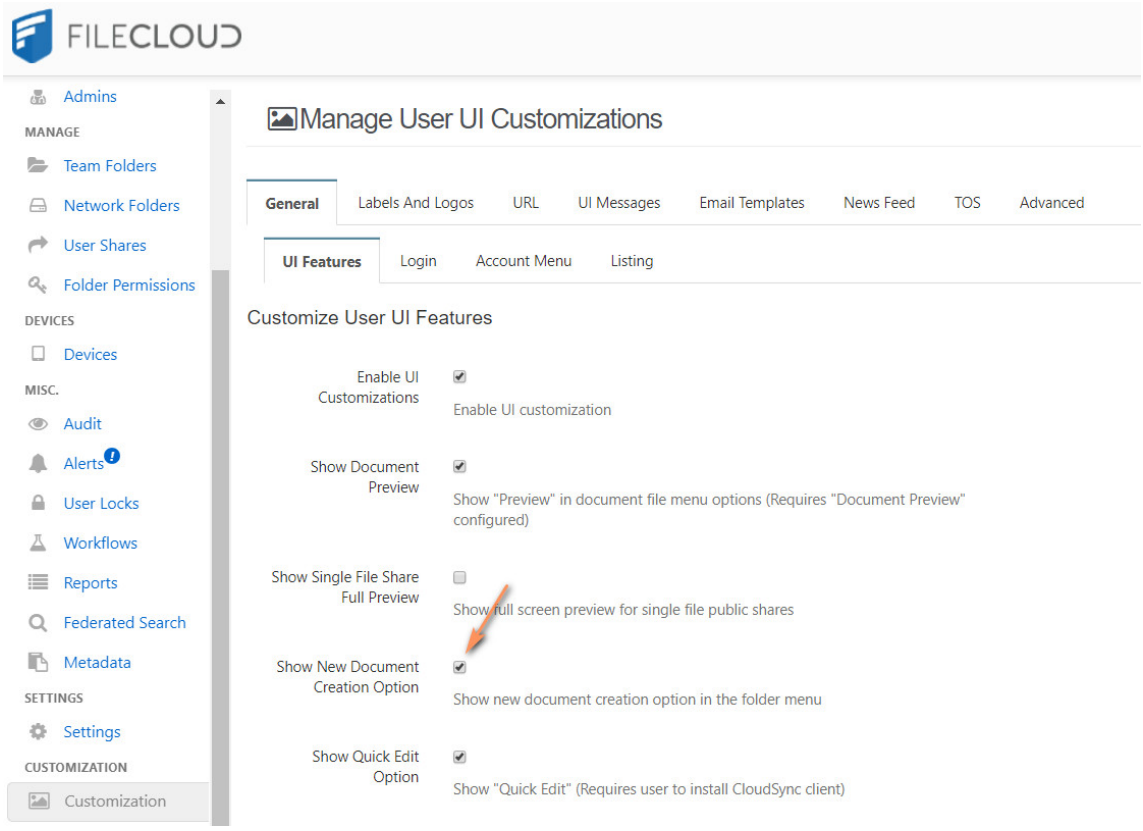
Your users can now view and use the **Open in Google [app]** option for docx, xlsx, and pptx files.

New Document Creation via Web Browser

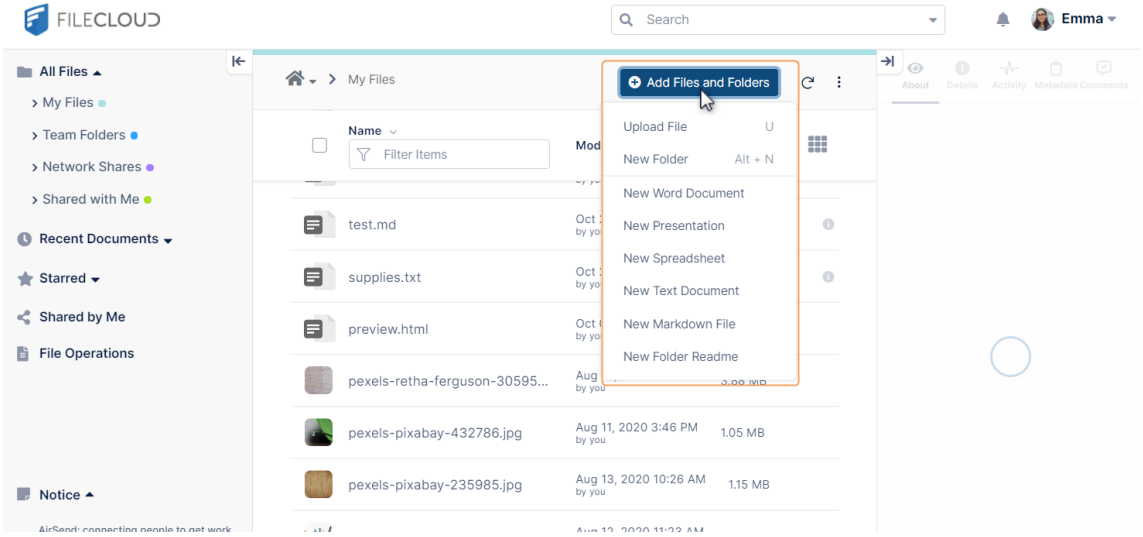
Once online editing is configured by the administrator, FileCloud users can log in to their portal and create new documents and edit them from within the web browser.

To enable new document creation

1. Enable **Show New Document Creation Option** in **Customization > General >UI Features**.

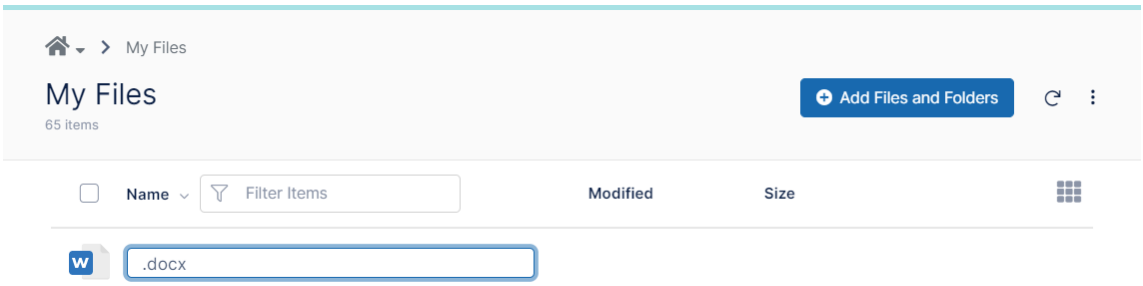


2. Now, in the user portal, users can click **Add Files and Folders** above the list of files. A drop-down list with options for creating new files or a new folder appears.



If the user chooses to create a file, the file appears at the top of the list of files and folders. The extension is already entered.

3. The user must type in a name, and click Enter.



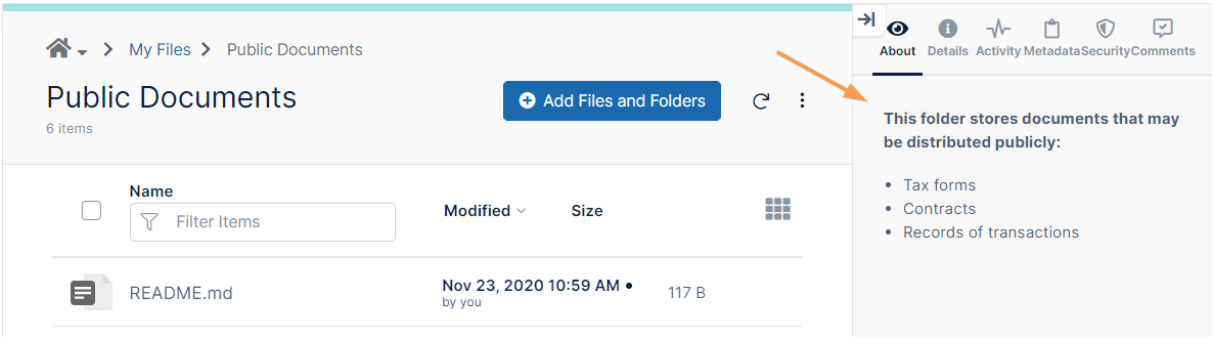
The document opens for edit.

Readme files

There can only be one readme file in a folder, and it is always named **readme.md**.

After a user creates the readme file, when they click **Add Files and Folders** and choose **New Folder Readme**, the existing readme is opened for edit.

When a user selects a folder that includes a readme file, the contents of the readme are displayed in the **About** panel to the right of the screen.



Web Editing Text Files

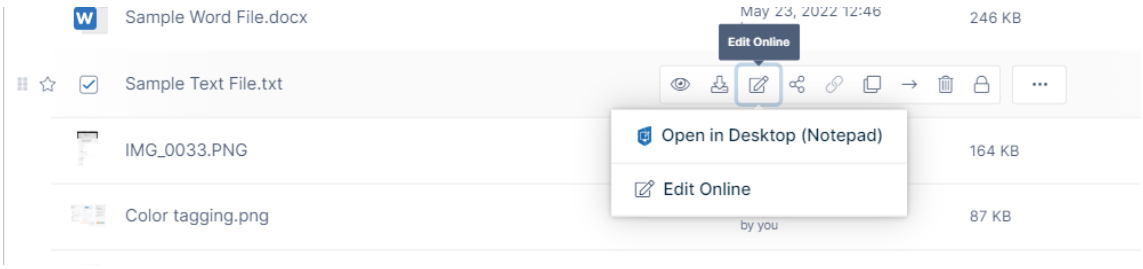
FileCloud supports editing text files from within a browser session. This support is enabled regardless of WOPI configuration, as editing of text files uses a built-in widget.

To create a new text file, see New Document Creation via Web Browser

Editing text files

To edit a text file:

1. Navigate to the text file, hover over it, and click the Edit icon.



2. Choose the edit option (there may be one or more).
   The file opens in the text editor you have chosen..
3. Edit and save the file.
   Note: You can also add and read comments about the file in the right panel.

Web Editing Markdown and Readme Files

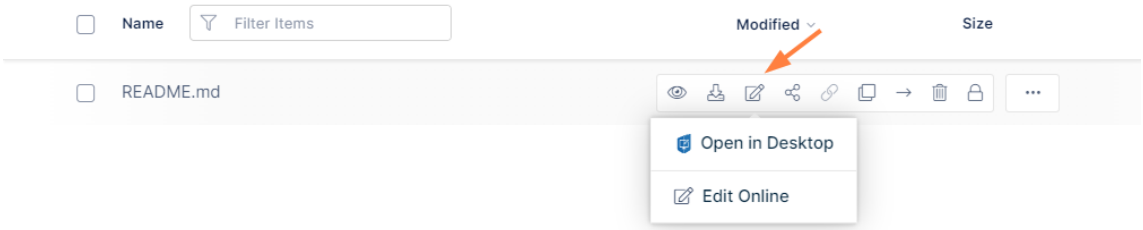
Starting with version 20.2, FileCloud supports editing markdown files from within a browser session. It also supports editing readme files, which are a form of markdown files and use the same types of editors.

To create a new markdown or readme file, see New Document Creation via Web Browser

Editing markdown and readme files

To edit a markdown or readme file:

1. Navigate to the file, hover over it, and click the Edit icon.



2. Choose the edit option (there may be one or more).
   The file opens in the text editor you have chosen..

> There can only be one readme file in a folder, and it is always named **readme.md**. After you create the file, it is displayed in the **About** section to the right of the page when you select the folder.

Coauthoring Office Documents Using Web Edit

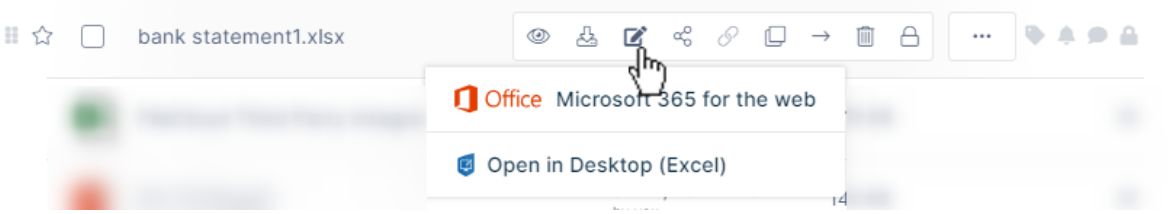
FileCloud supports coauthoring of Office document files from within a browser session.

Introduction

Coauthoring occurs when two users are editing the same document and can view each other's changes as they make them.

Only .docx, .xslx, and .pptx documents can be coauthored.

To open an Office file in web edit, hover over the file and click the **Web Edit** icon. In the drop-down list, choose **Microsoft 365 for the web**.



Coauthoring Flow

The following steps demonstrate the flow of coauthoring.

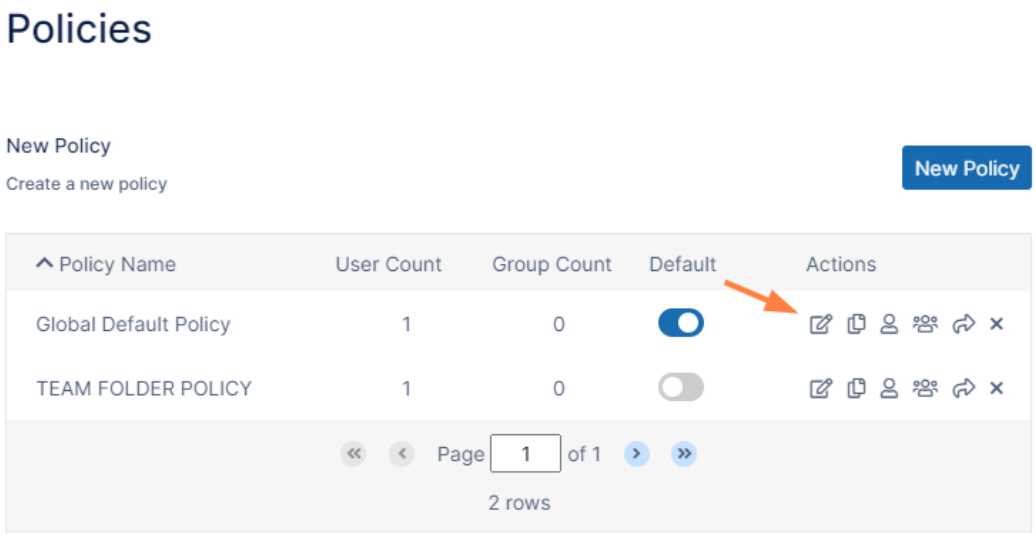
1. User A wants to coauthor a document with user B.
2. User A shares the folder containing the document to user B. The share should have view, download and upload permissions to user B.
3. User A opens the file in web edit.
4. User B opens the same file that was received via sharing in web edit.
5. Now both users can edit the document and they can see each other editing the file.
6. The web edit service will handle the coordination and will ensure saving both user changes.

Disable Online Web Editing

You can decide not to allow your users to edit documents in a browser.

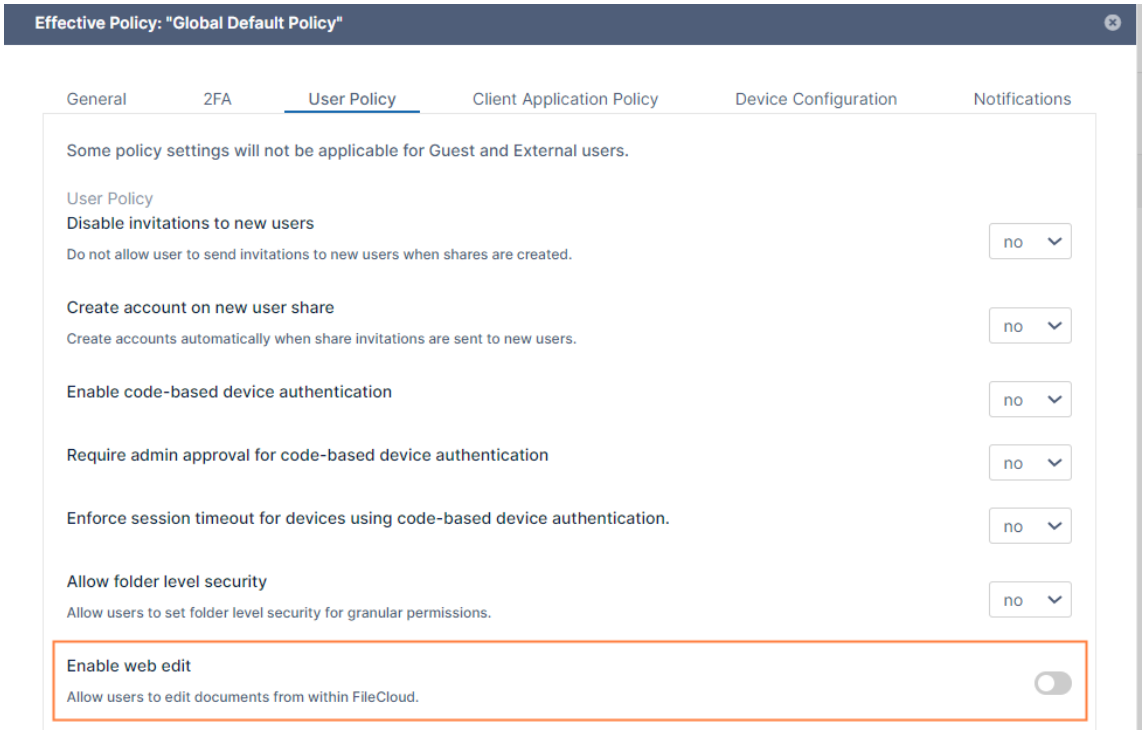
> After you configure online editing, FileCloud users can log in to the user portal, select any supported document and click a Web Edit button to edit the document from within the web browser. All the changes made by the user are saved in FileCloud automatically.
>
> If you do not want to support this feature for certain users, the Web Edit button can be removed from the user portal through the users' policies.
>
> **To hide the Web Edit button for the users associated with 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. Click the Edit icon in the row for the users' policy.



The **Policy Settings** dialog box opens.

3. Click the **User Policy** tab.
4. Locate **Enable web edit**, and disable it.



5. Click **Save**.

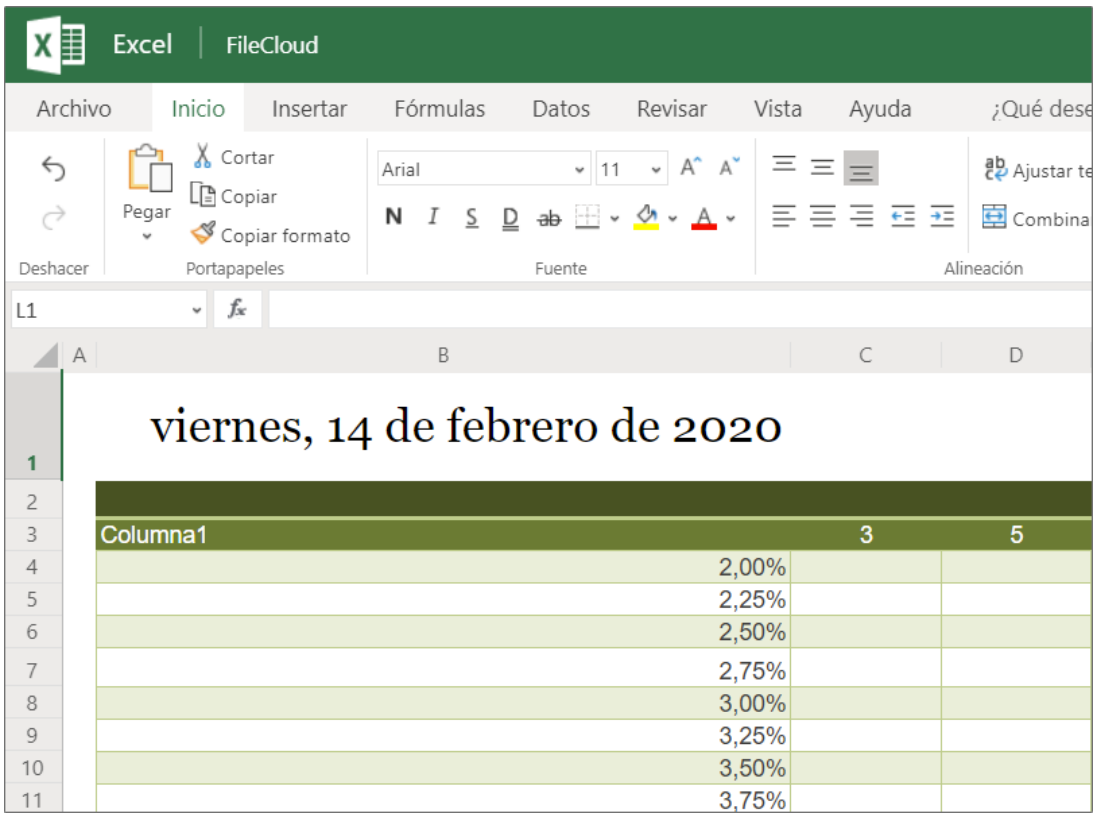
Changing the locale in online Office documents

If you want online Office documents to open in a different locale than the default (en-US), you must change the locale in WOPI.

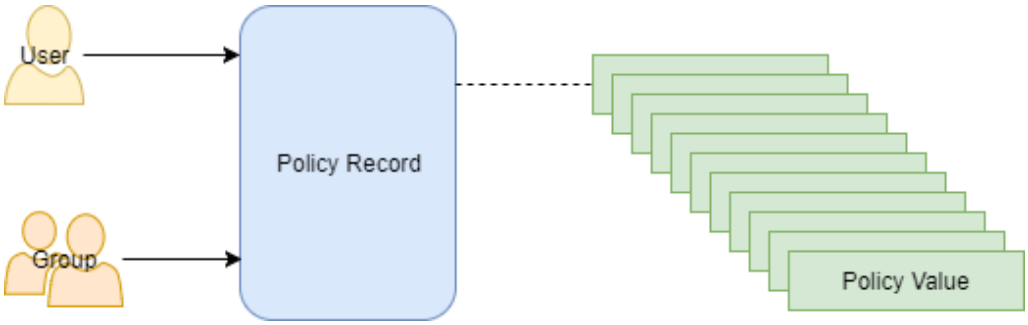
1. Choose any of the WOPI locales included in https://wopi.readthedocs.io/en/latest/faq/languages.html.
2. Change the WOPI locale:
   a. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
   b. Add the line following line, changing *en-US* to the new locale:

```
define("WOPI_CLIENT_LOCALEID", "en-US");
```

Now when you open a FileCloud document in Office online, the labels appear in the new locale, and if you add locale-sensitive features, like dates, they appear in the correct format. For example, the WOPI locale for the following document opened in FileCloud is es-ES:



Policies



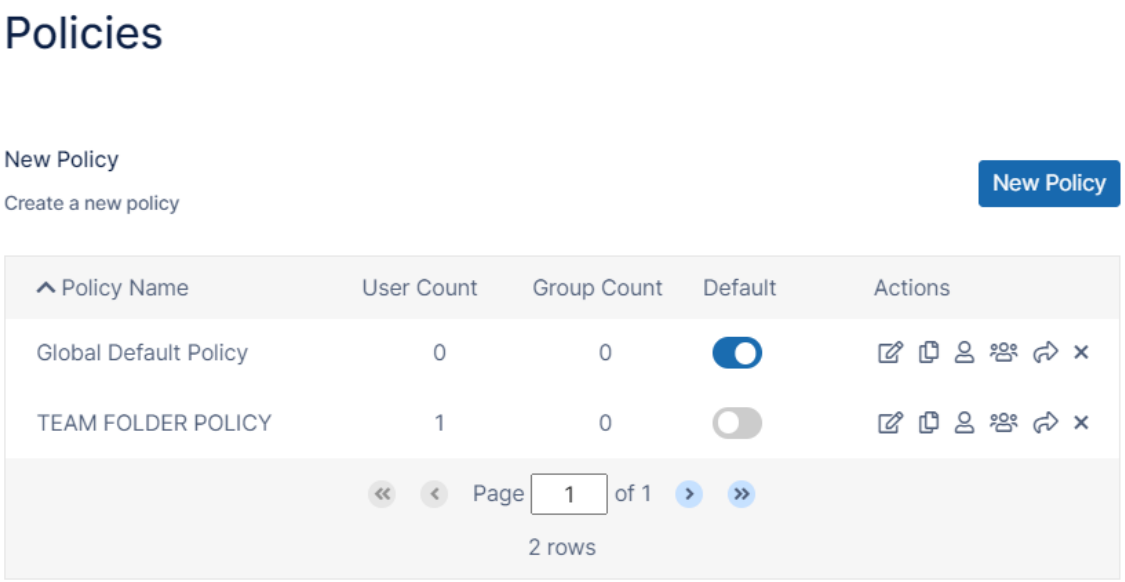
You can manage users and groups easily using policies.

- Policies enable you to manage settings at the user or group level
- One policy record manages multiple policy settings
- The policy record can be associated with a user or group

To manage FileCloud policies, click **Settings** in the navigation pane, and then, on



the **Settings** navigation page, click **Policies** .



The policy values in Table 1 are managed in a policy record.

Table 1. Policy Values

General		
Share Mode	All (public and private)	
Default share expiry in days	0	
Default max number of downloads allowed	0	
User storage quota	2GB	
Enable Privacy Settings	NO	
Store deleted files in the recycle bin	NO	
Automatically delete files from recycle bin after set number days	0	
Do not store deleted files greater than	100 MB	
Enable Basic Authentication (appears if enabled, see Enabling Basic Authentication)	Disable	
MFA		
See Multi-Factor Authentication for User Portal for information about these policy settings.		
User Policy		
Disable invitations to new users	NO	
Create account on new user share	NO	
Enable code-based device authentication	NO	

Require admin approval for code-based device authentication	NO (Only enabled if **Enabled Code Based Client Authentication** is set to YES.)	
Enforce session timeout for client devices.	NO	
Allow folder level security	YES	
Enable web edit	YES	
Enable recycle bin clearing	YES	
Disallow default share settings change	NO	
Disable Send File For Approval	NO	
Disable Everyone group sharing	NO	
Allow group creation	NO	FileCloud 21.2
Allow group management (add and remove users)	NO	FileCloud 21.2
Allow group deletion	NO	FileCloud 21.2
Allow workflow automation sharing	NO	FileCloud 23.251
Disable workflow automation	NO	FileCloud 21.2
Require share approval workflow	NO	FileCloud 21.2
Selected Workflow (only appears if Require Share Approval Workflow is set to YES)	Select a Workflow	FileCloud 21.2
eSignature	YES	FileCloud 23.241.4
Max. file upload size	0	FileCloud 22.1
Save zip file session password	YES	FileCloud 22.1

Client Application Policy	Default Value	Version Available
Require passcode lock for mobile clients	NO	
Disable all mobile client apps from connecting	NO	
Disable 'Edit' functions in mobile client apps	NO	
Disable 'Print' option in mobile client apps	NO	
Disable 'Download' option in mobile client apps	NO	
Disable 'Open with' option in mobile client apps	NO	
Disable 'Share' options in mobile client apps	NO	
Disable 'Add to favorites' option in mobile client apps	NO	
Device Configuration		
See (23.263a) Configure Centralized Device Management for information about this setting.		
Notifications		
Disable Notifications	NO	
Disable User Override	NO	
Disable Add notifications	NO	
Disable update notifications	NO	
Disable delete notifications	NO	
Disable Download notifications	NO	
Disable Preview notifications	NO	
Disable Lock/Unlock notifications	NO	

Disable Share notifications	NO	
Disable Rename notifications	NO	
Disable self notifications	NO	
Watermark		
List of watermark rules	A list of watermark rules that apply to users in this policy. When these users preview or download content, the highest priority watermark that applies appears on the preview or download. See Watermark Settings.	23.261

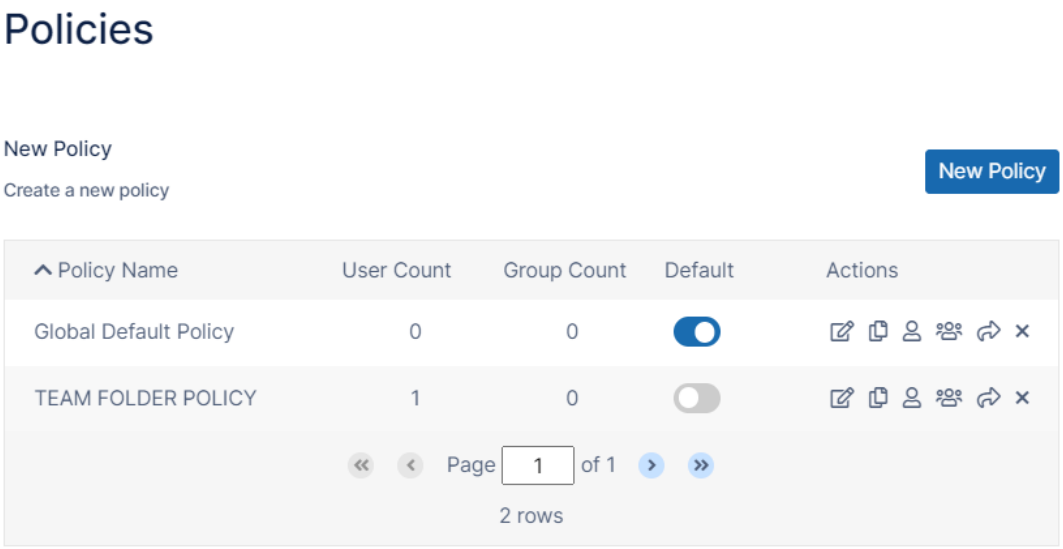
Working with Policy Records

Accessing Policy Records

To access a policy record:

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.

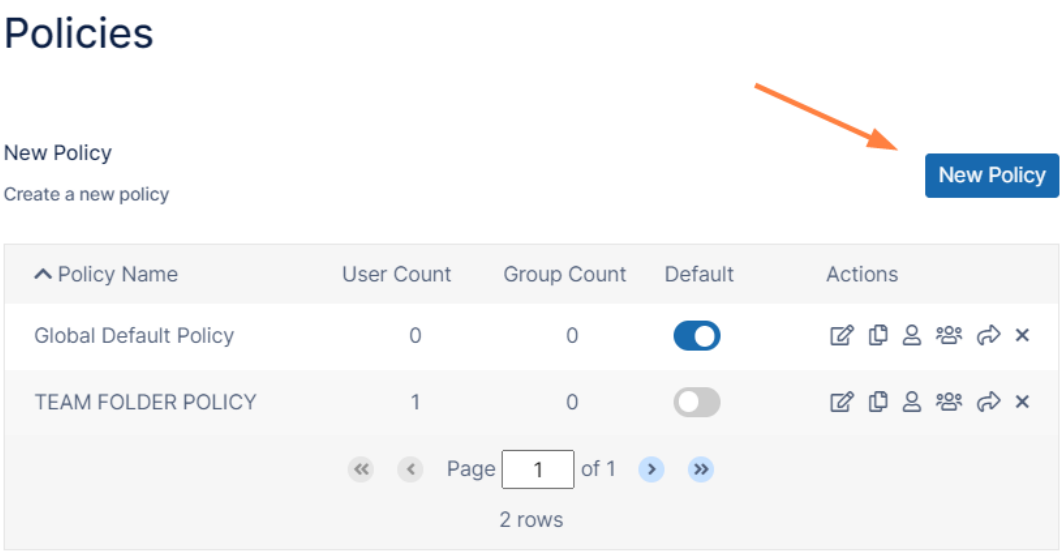


Creating a New policy Record

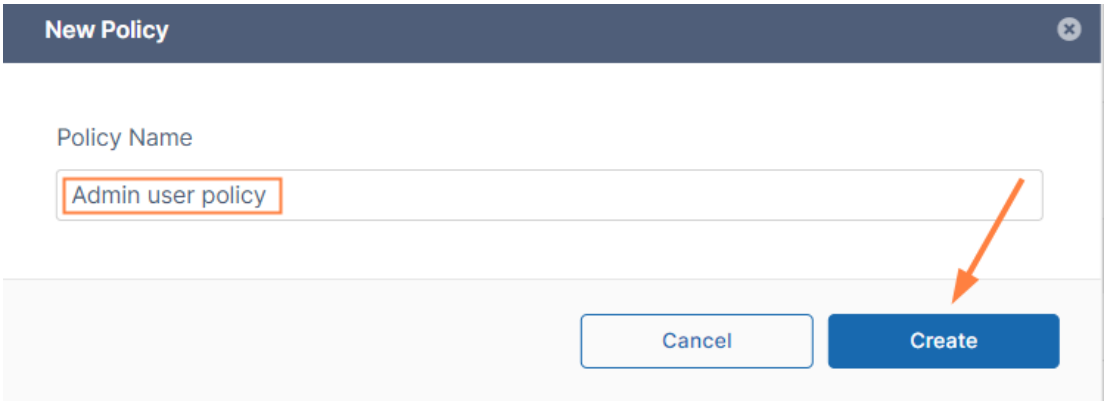
To create a policy:

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** page opens.

2. Click **New Policy**.

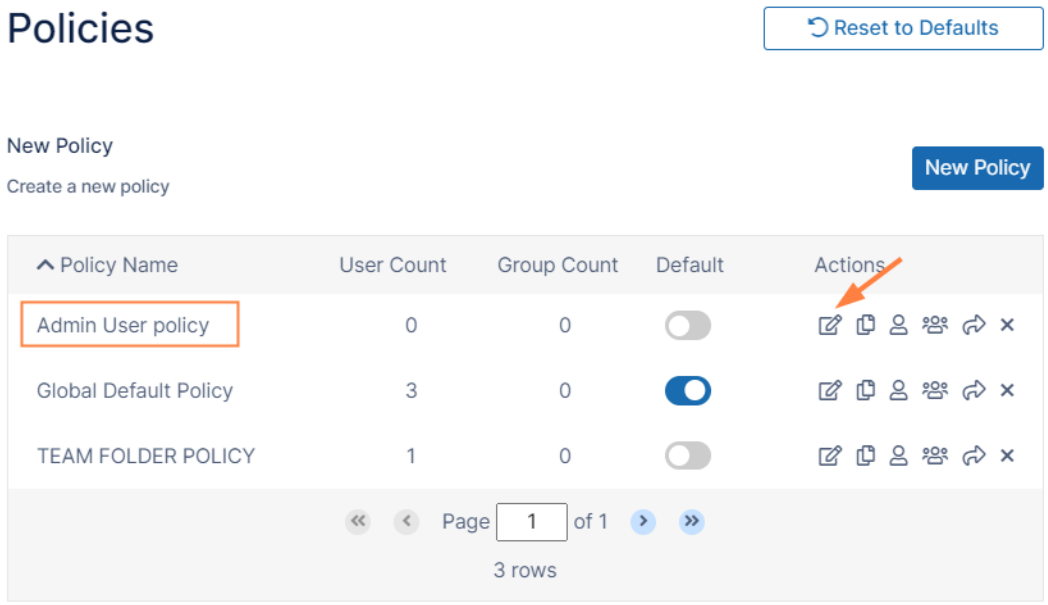


3. In the **New policy** window, in **Policy Name**, type in a unique name for this policy, and then click **Create**.



The policy is created and appears in the **Policies** list.

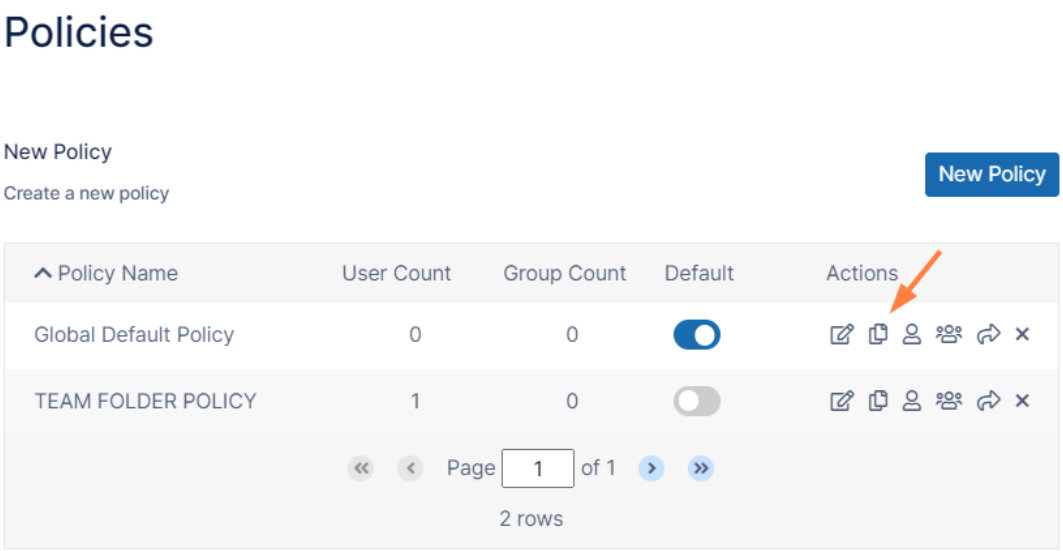
4. Edit the new policy to configure settings.



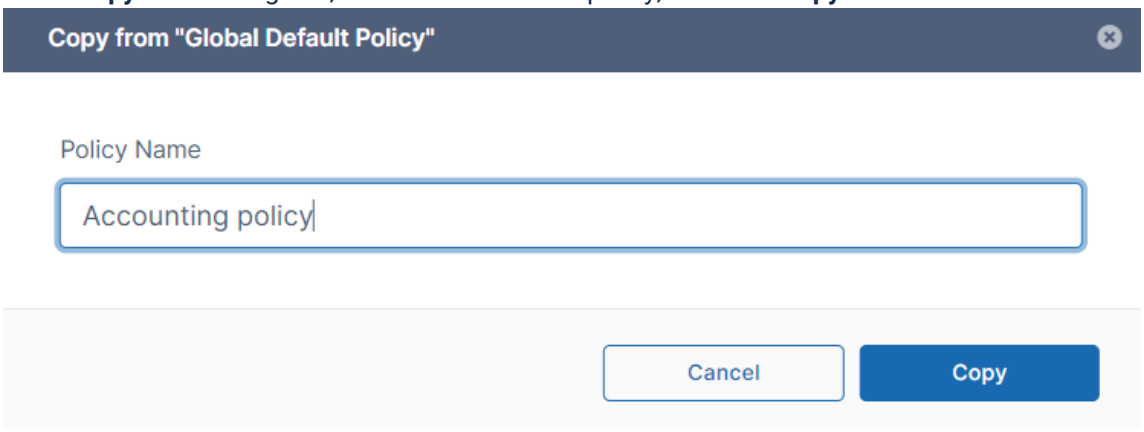
💡 Instead of creating a new policy, you have the option to copy an existing policy including changes you have made to its settings..

To copy a policy:

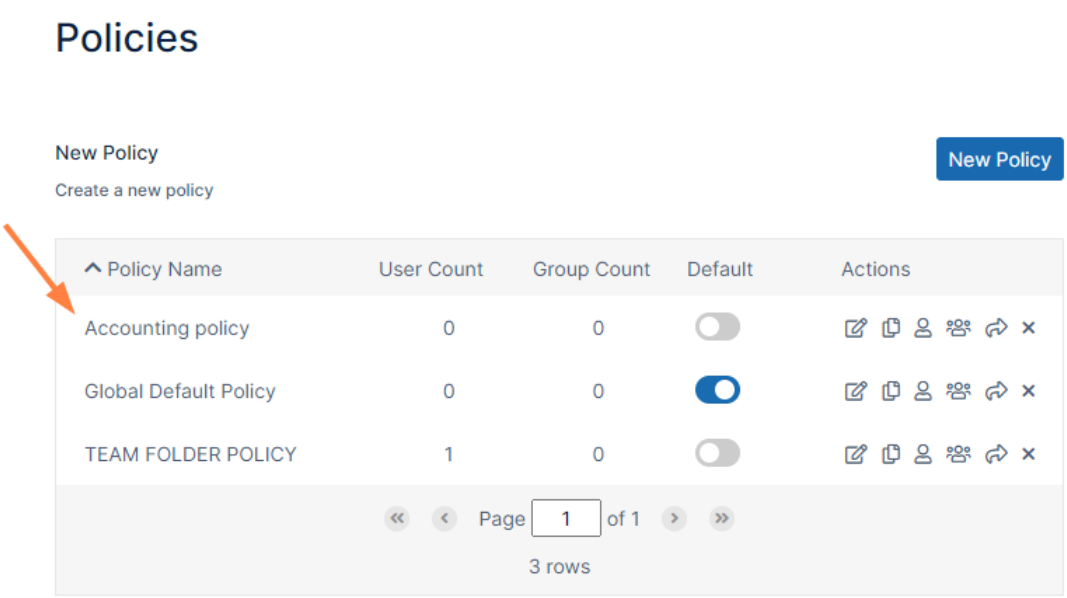
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
2. Click the copy icon next to the policy that you want to copy



In the **Copy from** dialog box, enter a name for the policy, and click **Copy**.



The new policy appears in the list of policies:



Managing Policy Users and Groups

A policy can be assigned to one ore more user or group.

To assign a user to 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** page opens.
2. Click the user icon next to the policy that you want to assign a user to.
3. Use the arrow to move the user to the **Policy Users** list box.

4. To save your changes, click **Close**.

To assign a group to a policy:

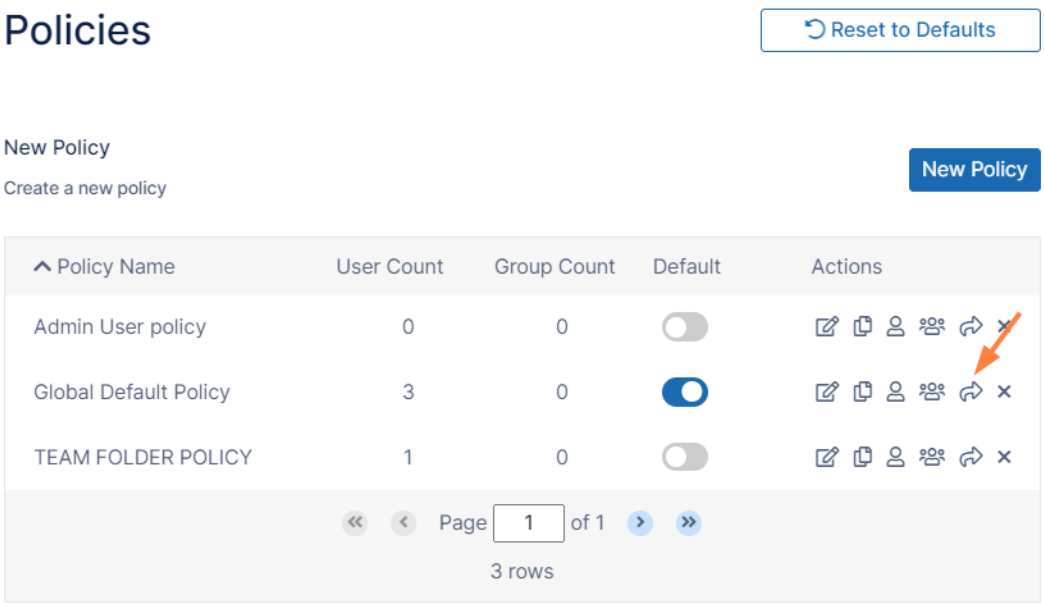
1. Log into the Admin Portal.
2. Click **Settings**.
3. On the **Policies** tab, to open the **Manage Policy Groups** window, click the groups icon.
4. In the **Manage Policy Groups** window, in **Available Groups**, select a group.
5. Use the arrows to move the group to the **Policy Groups** list box.
6. To save your changes, click **Close**.

Exporting a list of policy members

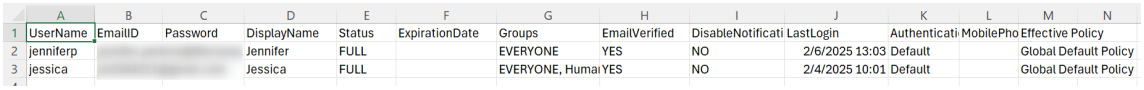
Beginning with FileCloud Version 21.3, you can see which users and groups are members of a policy by exporting them.

To export policy members:

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. To export a policy's users and groups to a csv file, click the export (right arrow) icon next to the policy.



A csv file listing the individual users in the policy and users in groups in the policy is exported. The file includes the following fields:

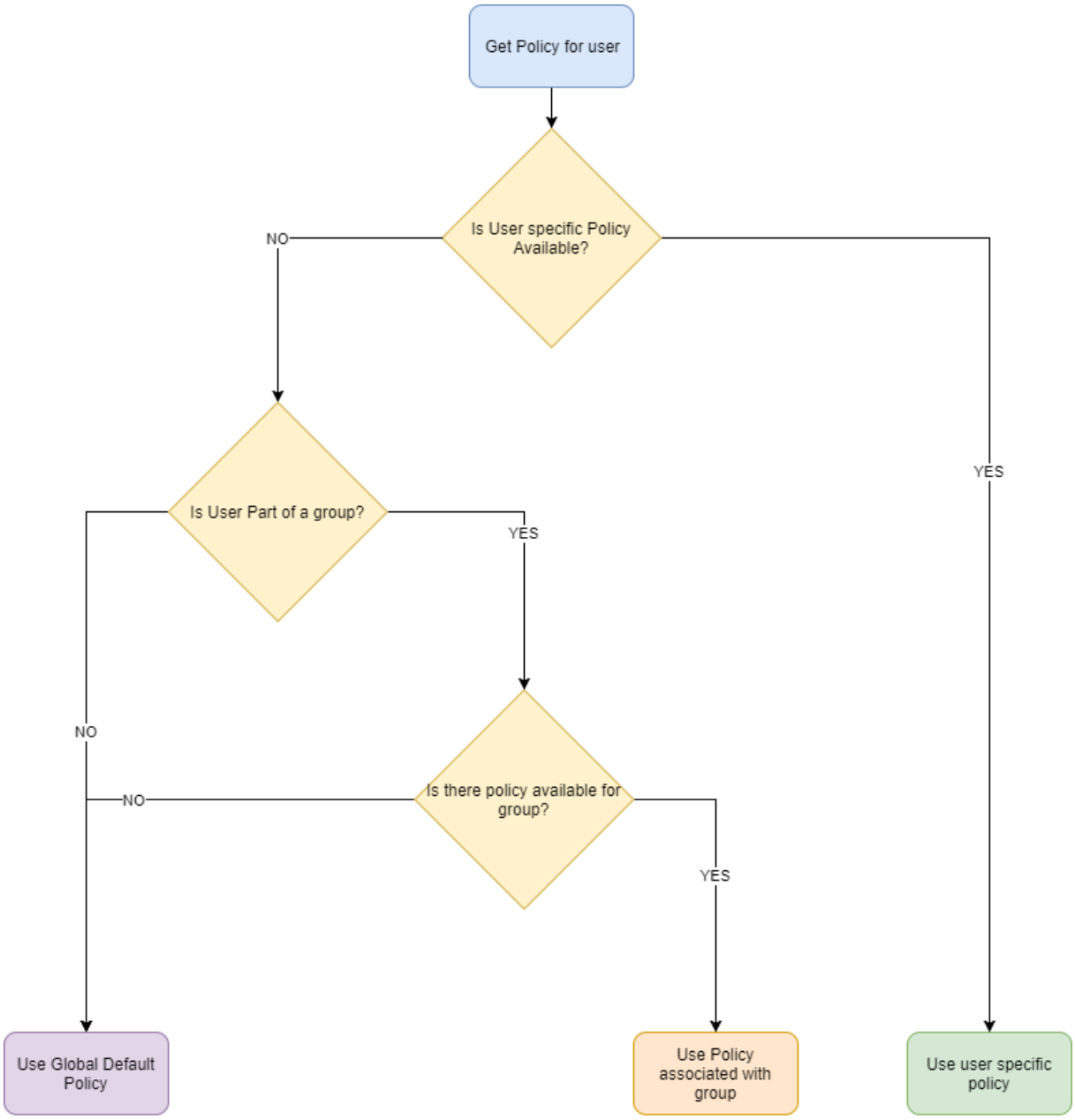


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotificati	LastLogin	Authenticati	MobilePho	Effective Policy	
2	jenniferp	[redacted]		Jennifer	FULL		EVERYONE	YES	NO	2/6/2025 13:03	Default		Global Default Policy	
3	jessica	[redacted]		Jessica	FULL		EVERYONE, Humai	YES	NO	2/4/2025 10:01	Default		Global Default Policy	

Manage the Recycle Bin Using Policies

Policy Calcuations Best Practices

An effective policy for a user is calculated on multiple factors



Policy Selection Scenarios

Case 1: User with no policy assigned : **Global Default Policy will be used**

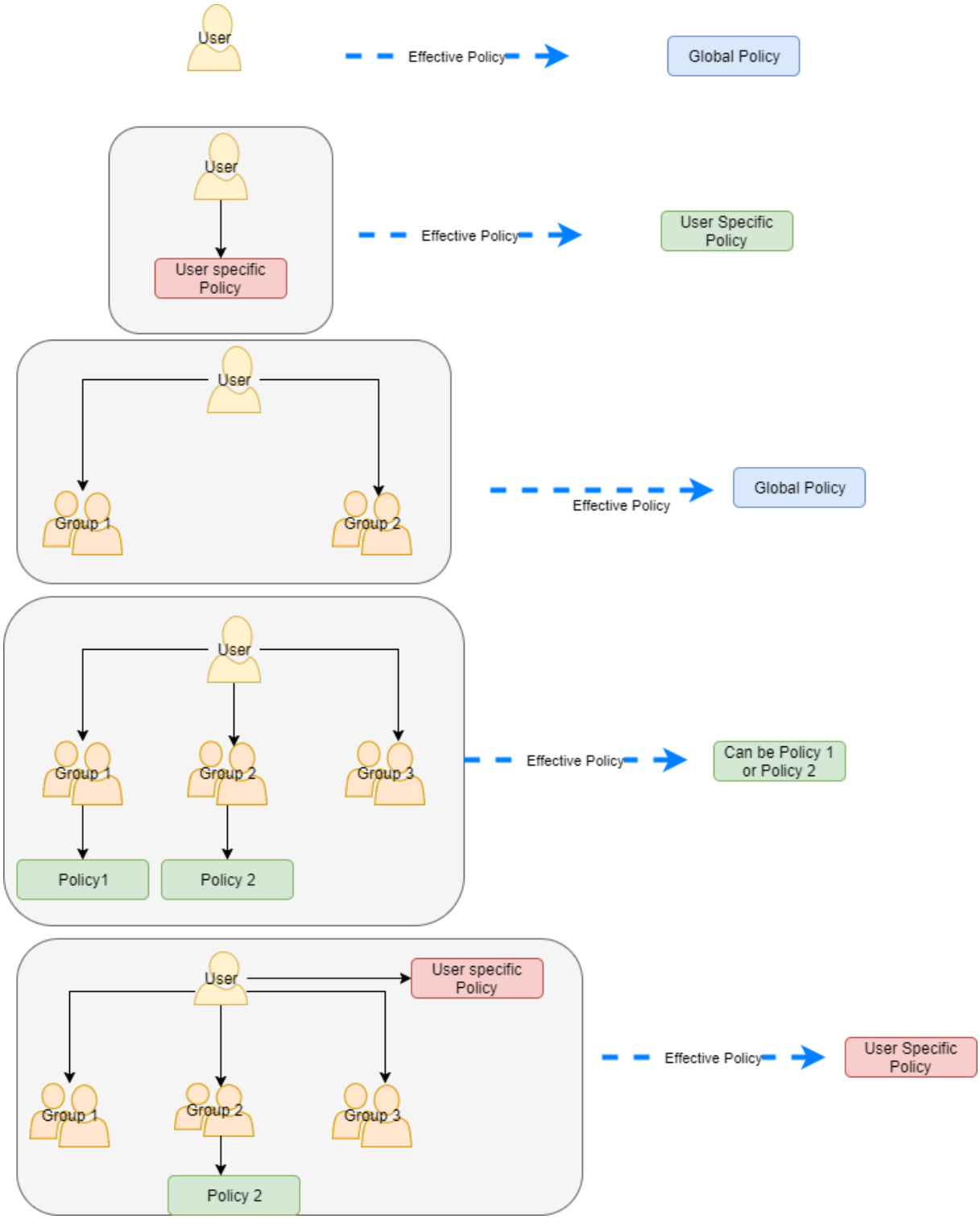
Case 2: User with specific policy assigned: **Assigned policy will be used**

Case 3: User is a member of multiple groups, No Policy is assigned to user or group: **Global Default Policy will be used**

Case 4: User is member of multiple groups and multiple groups have policies: **One of the group policies will be used (Randomly selected).**

Case 5: User is a member of multiple groups and has specific policy assigned and groups have their own policies: **User assigned policy will be used**

Selecting a Policy Scenario Flow Chart


User
Effective Policy
Global Policy
User
User specific Policy
Effective Policy
User Specific Policy
User
Group 1
Group 2
Effective Policy
Global Policy
User
Group 1
Group 2
Group 3
Policy1
Policy 2
Effective Policy
Can be Policy 1 or Policy 2
User
User specific Policy
Group 1
Group 2
Group 3
Policy 2
Effective Policy
User Specific Policy

Creating a New Policy Video



Managing Policy Users and Groups Video



Notifications for File Changes

FileCloud automatically sends you an email notification when:

- a file or folder is shared with you
- one of the following actions is performed (by you or another user) on a file or folder you have access to:
  - a file or folder is uploaded
  - a file or folder is downloaded
  - a file or folder is shared
  - a file or folder is deleted
  - a file or folder is renamed
  - a file is updated
  - a file is previewed in the browser or one of the mobile apps
  - a file or folder is locked

Administrators can set notifications at the global level and users can override them at the user level.

FAQ's

How Do Notifications Work?

By default, when users make any of the changes listed above to their own files or folders, FileCloud sends them a notification. When a user makes any of the changes listed above to shared files or folders, all users that the file or folder has been shared with receive a notification.

All file change notifications are consolidated and emails are are sent by FileCloud at regular notification frequencies (15 minutes, 1 hour, 1 day etc) as set by your FileCloud administrator as part of the Cron Job Setting.

Why is the user not getting a notification?

If you have enabled file and folder change notifications and a user is not receiving a notification, it may be because:

- the file change was made directly on the LAN
- that specific file change was blocked in the Admin user interface in Policy settings or in Notifications settings.

Where was the change made?

To receive a notification, actions must occur in one of the following places:

- The FileCloud Admin Portal
- The FileCloud User Portal

- The FileCloud Sync client
- The FileCloud Drive client
- The FileCloud Mobile App

This applies to both My Files and Network Folders.

For network folders, when files are changed directly on the LAN, FileCloud does not have any knowledge of file changes and will not send a notification.

Is the Notification Blocked in Another Place?

File change notifications can be blocked for a specific action in any of the following places:

- Global settings
- Policy settings
- Share settings
- Network folder settings,
- File or folder settings
- NTFS Permissions
- Account settings for external users

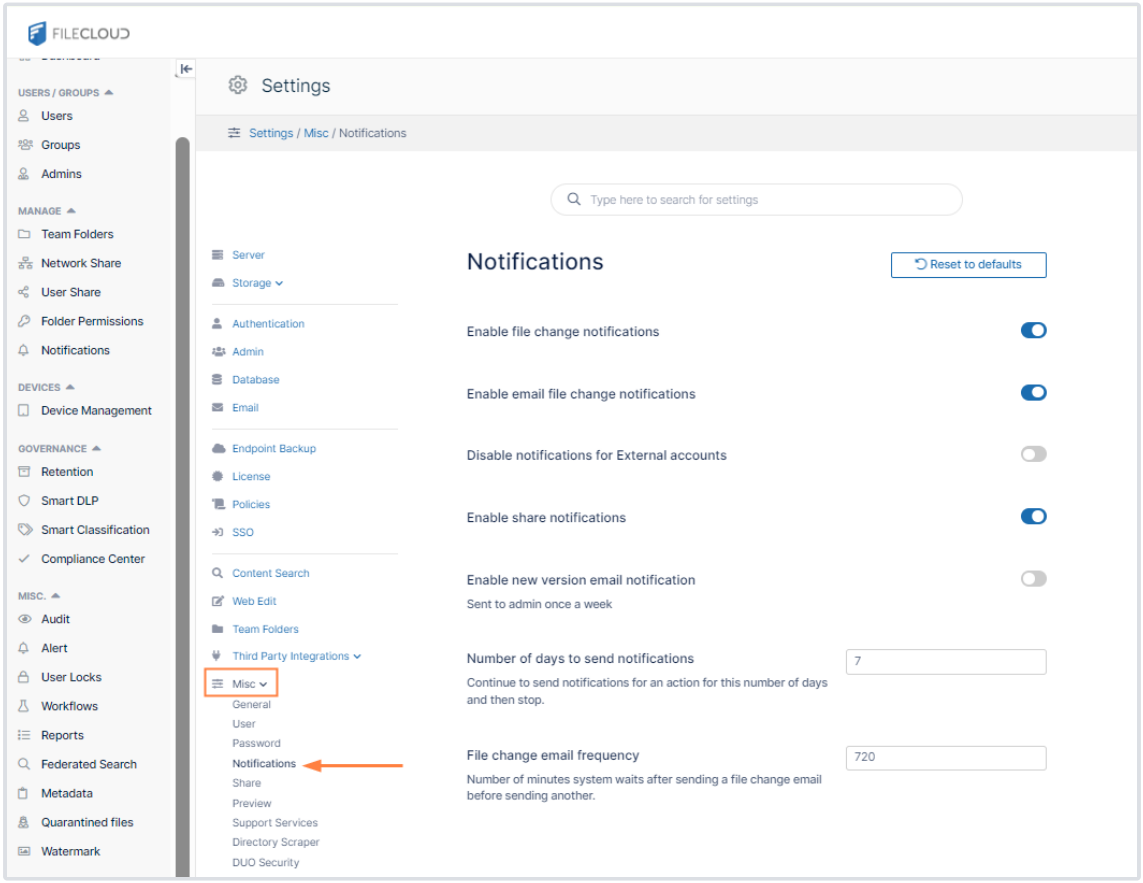
If a user is not receiving a notification, check to see if that file action is disabled at any level.

Are you using a trial account?

Trial accounts have notification limits. If you are using a trial account and have been able to send notifications previously, the notification limit may have been reached.

How to access notification settings in the admin portal

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Notifications**, as shown below.



Changing the time when digest emails are sent

By default, FileCloud uses the following schedule for sending daily and weekly digest emails:

- Weekly digest emails are sent on Fridays at 8 am.
- Daily digest emails are sent at 9 am.

However, beginning with FileCloud Version 20.1, you can override these times by adding settings to the cloudconfig.php file.

1. Open cloudconfig.php in
   - Windows: xampp/htdocs/config
   - Linux: /var/www/config

2. To set:
   a. The day of the week that weekly digests are sent, add the setting:

```
define("TONIDOCLOUD_WEEKLY_DIGEST_DAY_NUMERIC", 5);

enter 0 - 6, where  0 = Sunday and 6 = Saturday
```

b. The hour of the day that weekly digests are sent, add the setting:

```
define("TONIDOCLOUD_WEEKLY_DIGEST_HOUR", 8);

enter 0 - 23, where 0 = 12:00 am and  23 = 11:00 pm
```

c. The hour of the day that daily digests are sent, add the setting:

```
define("TONIDOCLOUD_DAILY_DIGEST_HOUR", 9);

enter 0 - 23, where 0 = 12:00 am and  23 = 11:00 pm
```

Notes: These settings do not affect other settings for notifications. If Email notification frequencies are set to run every 60 minutes, these emails are sent as well as the daily and weekly digests.

Digests are processed by cron, so if you schedule a mailing at 9, but the cron process is scheduled to run at 9.30, the emails are sent at 9:30.

Changing notification settings

Global notification settings

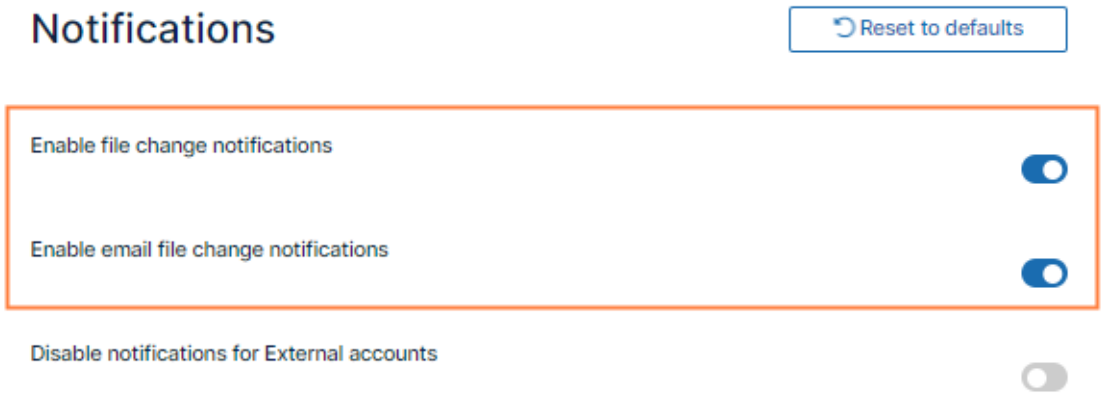
Enable or Disable ALL Notifications

Prerequisites

Cron jobs must be set up. See Setting Up a Cron Job or Scheduled Task.

To enable file change notifications:

1. Access the **Notifications** settings page.
2. To display notifications of file changes on the user portal, check **Enable file change notifications**.
3. To send email notifications of file changes to users, also check **Enable email file change notifications**.
   This setting is not enabled unless **Enable file change notifications** is checked.



4. Click **Save**.

Beginning with FileCloud 20.1, if **Enable file change notifications is unchecked**, users cannot override the admin notification settings.

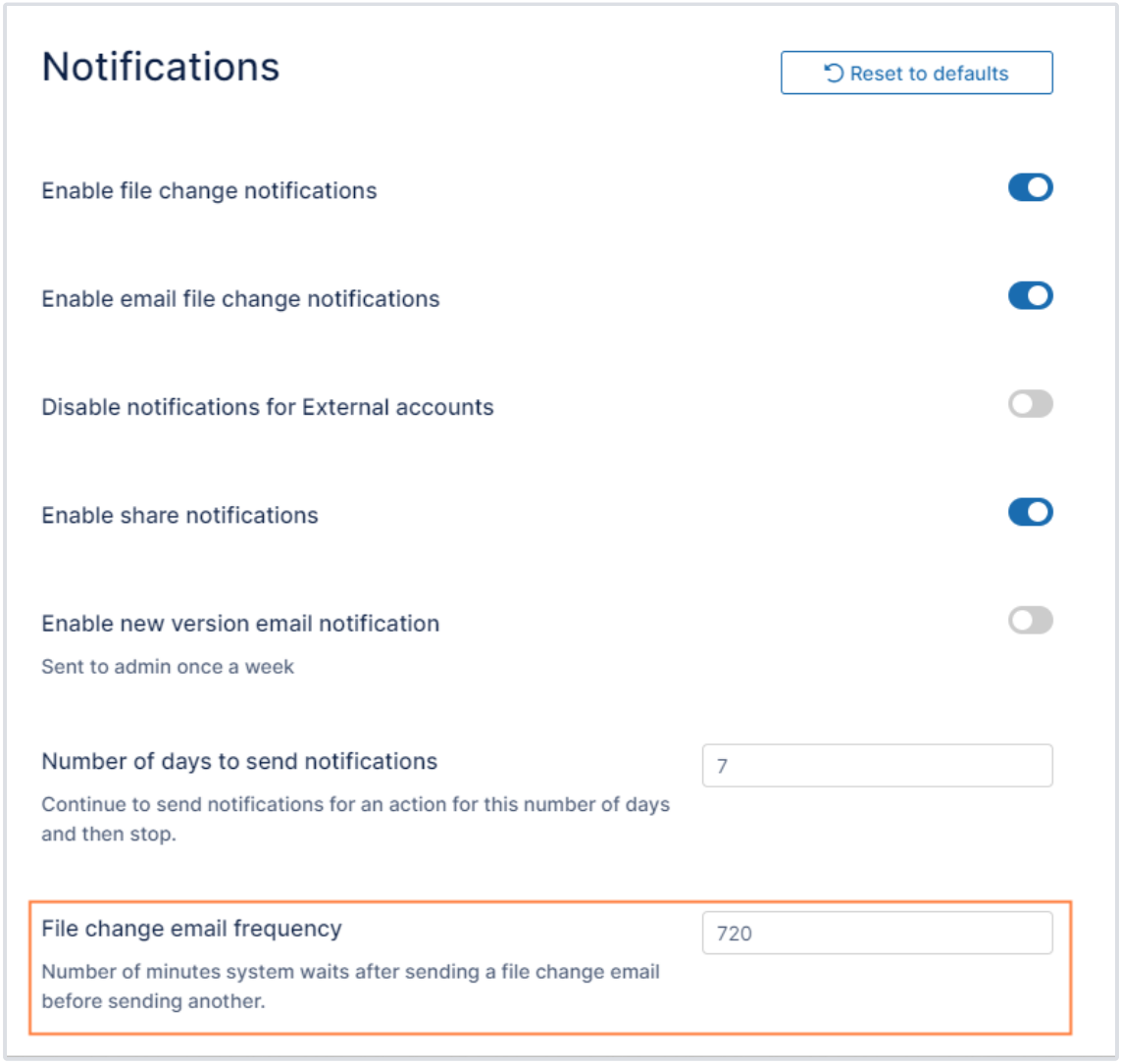
Set the Frequency for ALL Notifications

Increase the Frequency of Notifications

You can set the file change notification frequency level in the Admin portal, and users can override this and set their own frequency in the User portal.

To set file change notification frequency in the admin portal:

1. Access the **Notifications** settings page.
   The default file change email frequency is 720 minutes (12 hours).
2. Change the number of minutes in **File change email frequency**.



3. Change the value.
4. Save your changes.

To see how users can set their own notification frequency, see the help topic Notifications.

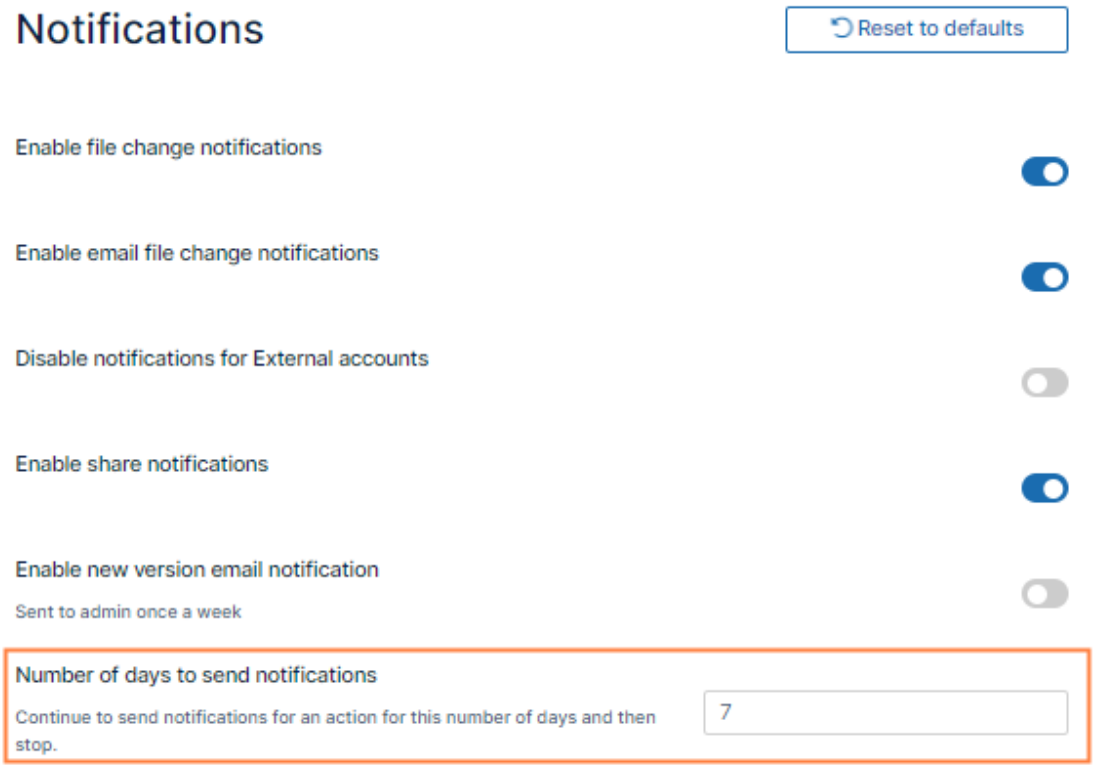
Do not send outdated email notifications

Do not send notifications that were created a number of days ago

You can configure FileCloud Server to stop sending email notifications for an action after a specified number of days (by default, 7 days). This prevents the system from sending notifications that are no longer relevant.

To prevent sending notifications after a specific number of days:

1. Access the **Notifications** settings page.
2. In **Number of days to send notifications**, type in a number.
   Enter **0** to disable notifications.



3. Save your changes.

External User Account Notifications

User accounts with external access can manage FileCloud content only through a Web browser.

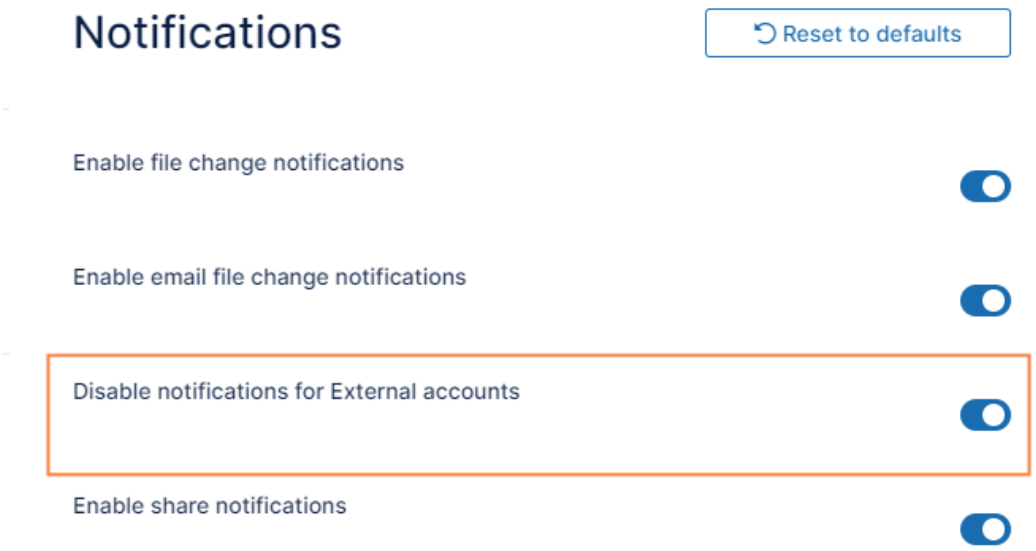
These user accounts:

- Can only view/upload/download to content shared with them
- Do not count towards the user license limit
- Cannot be authenticated via AD and can only be local user account
- Linked email accounts cannot use the same domain specified in the FileCloud URL
- Can't be added directly to network shares via the Admin Portal
- Can access content from network folders if they are shared

If you have users with external access to content, you may want to avoid confusion that may occur when an email is sent about content that users with external accounts cannot access.

To set the file change notification frequency for external accounts:

1. Access the **Notifications** settings page.

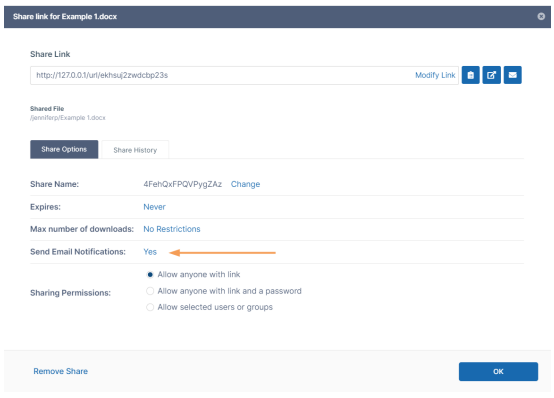
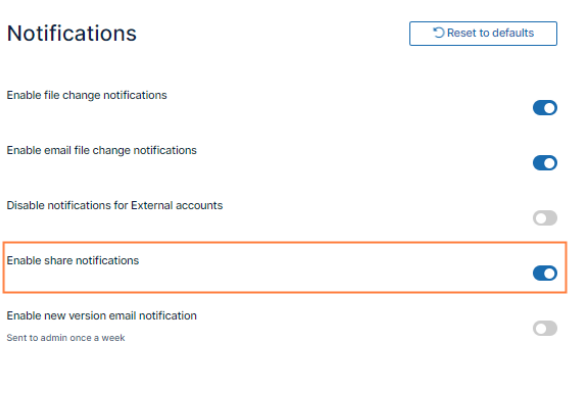


2. To stop sending notifications, locate the setting Disable notifications for External accounts and enable it.
3. Click **Save**.

Sharing Notifications

When a File or Folder is shared, the owner can allow or restrict sending file change notifications to all users that have access to that share.

- Enabling this setting sends an email notification when a publicly shared file is opened or downloaded.
- Notifications can be enabled or disabled by the user in the User Portal
- Notifications can also be enabled or disabled by the admin in the Admin Portal.
- The user can override these settings by setting custom notifications for a file or folder path.

User Portal	Admin Portal
	

User Portal	Admin Portal
To share a file with everyone without restrictions: 1. Open a browser and log in to the user portal. 2. Click My Files. 3. Hover over the file you want to share. 4. Click the share icon. 5. On the Share Link for File dialog box, click **Share Options**. 6. In **Share Options**, set **Send Email Notifications** to **Yes**.	**To enable file change notifications for shares:** 1. Log in to the admin portal. 2. Access the Notifications settings page. 3. Enable **Enable share notification**. 4. Click **Save**.

Customize notification settings for individual users and groups

User and Group Notifications

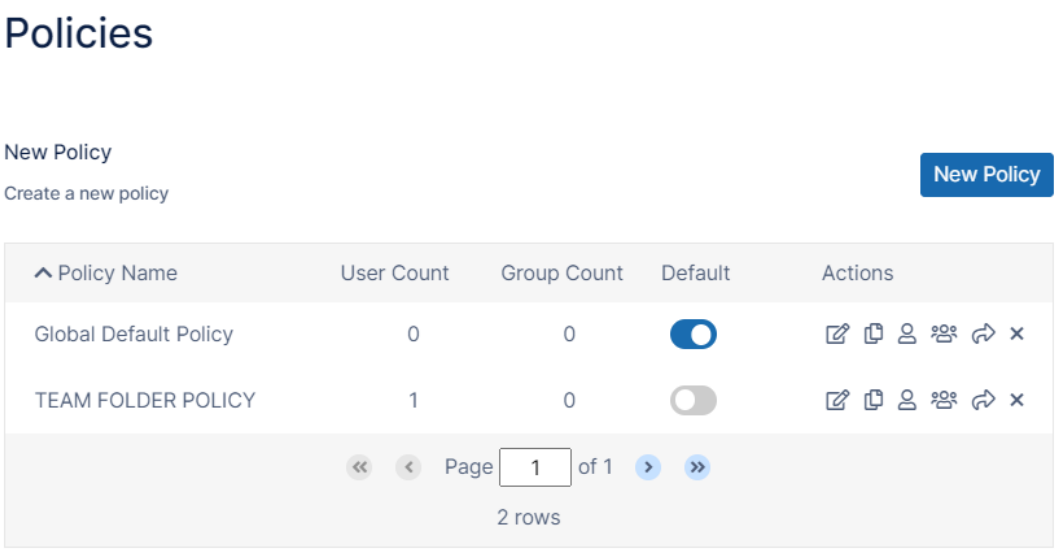
You can customize notifications for specific users or groups by customizing the notifications settings on their policies.

For example, notifications can be disabled for a specific user or group by disabling notifications in their policy.

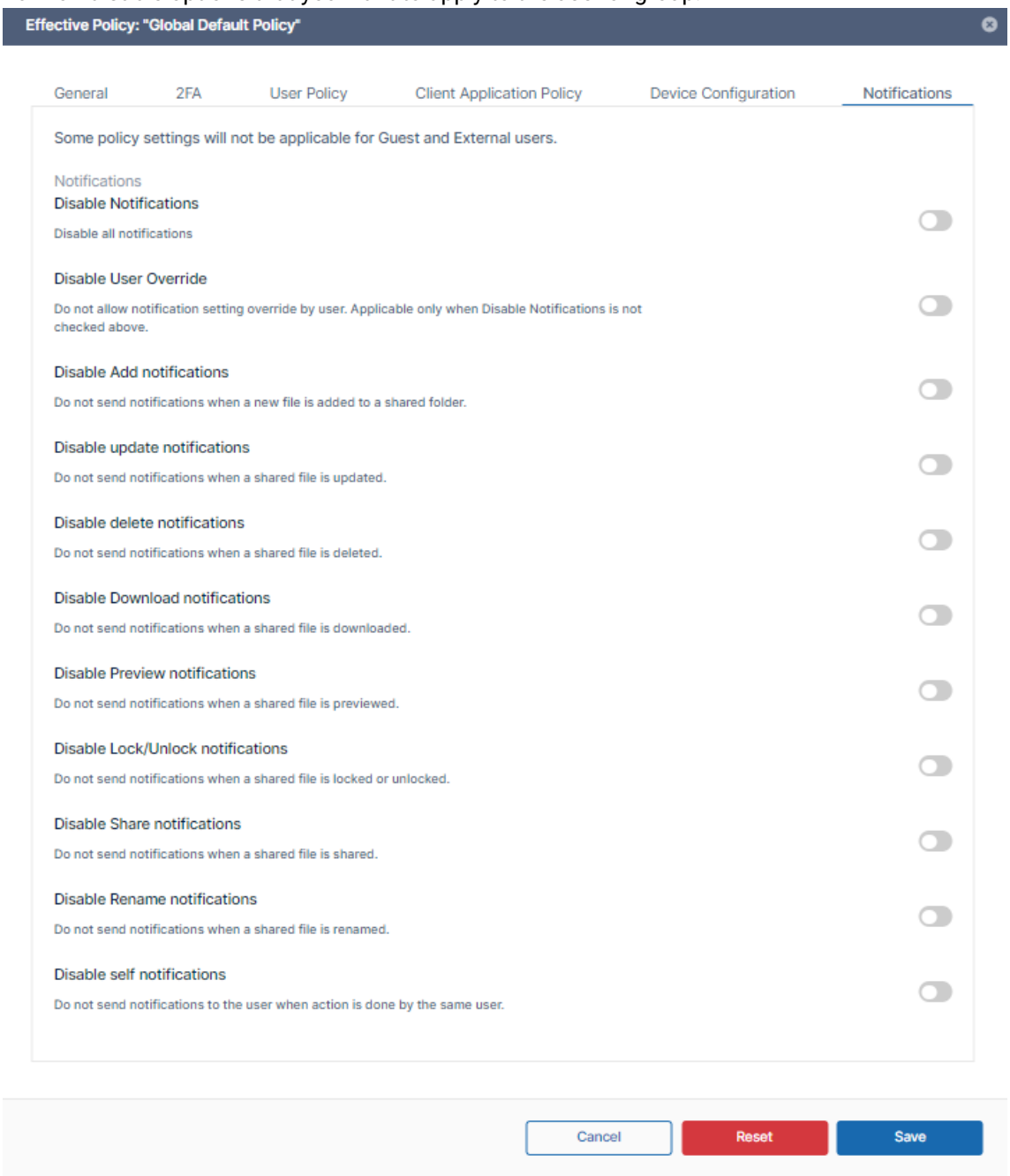
Note that unless **Disable User Override** is checked, users can override all of these settings except for **Disable Notifications**.

To customize notifications through 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 assigned to the user or group.
3. Click the **Notifications** tab.
4. Turn on disable options that you want to apply to the user or group.



Disable Notifications - When checked, disable all notifications. This setting cannot be overridden.

Disable User Override - When checked, disable user override of these settings. Applicable only when the above setting, **Disable Notifications**, is not checked.

Disable Add notifications - Do not send notifications when a new file is added to a shared folder.

Disable update notifications - When YES, do not send notifications when a shared file is updated.

Disable delete notifications - When YES, do not send notifications when a shared file is deleted.

Disable Download notifications - When YES, do not send notifications when a shared file is downloaded.

Disable Preview notifications - When YES, do not send notifications when a shared file is previewed.

Disable Lock/Unlock notifications - When YES, do not send notifications when a shared file is locked or unlocked.

Disable Share notifications - When YES, do not send notifications when a shared file is shared.

Disable Rename notifications - When YES, do not send notifications when a shared file is renamed.

Disable self notifications - When YES, do not send notifications to a user when any of these actions are done to a file or folder (shared or not shared) owned by the user.

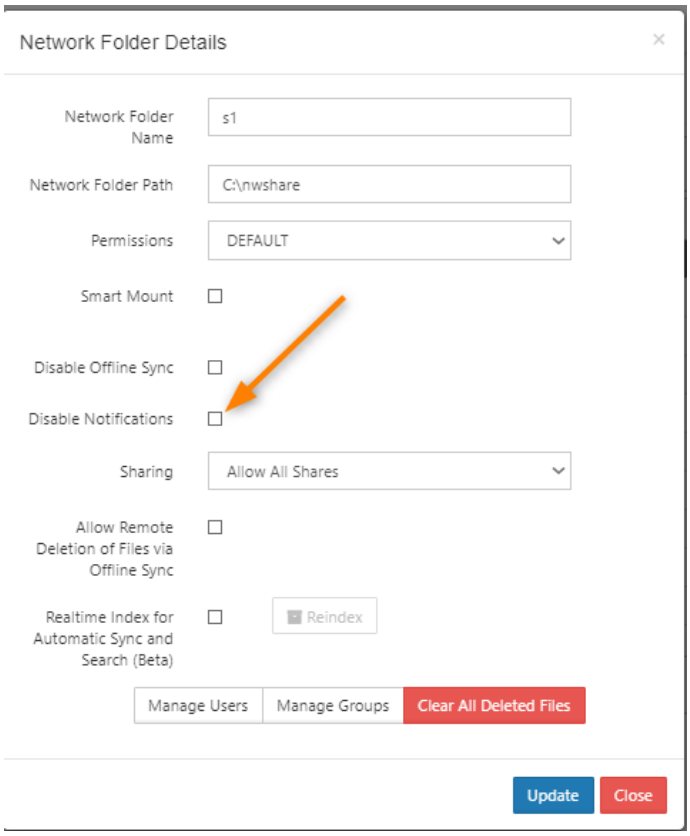
5. Click **Save**.

Network Folder Notifications

Network Folder Notifications

Administrators can disable notifications for specific network folders.

Users can override these settings by setting custom notifications for a file or folder paths.



To enable File Change Notifications for Network Folders:

1. Open a browser and log in to the admin portal.
2. From the left navigation pane, select Network Folders.
3. On the **Manage Network Folders** screen, select a folder to change the notification settings for.
4. Click the edit button.
5. On the **Network Folder Details** screen, to enable notifications, clear the **Disable Notifications** checkbox.
6. To save your changes, click **Update**.

NTFS Folders

Many organizations have Windows-based Network Folders that are shared with employees.

- The permissions on these Network Folders are managed using NTFS rights setup for various users and groups (usually from Active Directory).
- FileCloud can use the same NTFS permissions on the Network Folders for user authorization and access to these resources.

For more information, read about Network Folders with NTFS Permissions

💡 By default, file change notifications are disabled for Network folders with NTFS Permissions.

- To enable notifications, you will need to edit a configuration file
- By default, configuration files for FileCloud installation will be under WEBROOT/config

Setting	Option	Description
TONIDOCLOUD_NOTIFICATION_ENABLE_NTFS	0	**Disable notifications for NTFS folders**
TONIDOCLOUD_NOTIFICATION_ENABLE_NTFS	1	**Allow notifications for NTFS folders**

To configure file change notifications for Network folders with NTFS Permissions:

1. Navigate to the following directory:

```
WEBROOT/config
```

2. Open the following file for editing:

```
cloudconfig.php
```

3. Add the following line, using **1 to allow notifications and 0 to disable notifications for NTFS Folders.**

```
define("TONIDOCLOUD_NOTIFICATION_ENABLE_NTFS", "1");
```

Also see:

Customize notifications in user settings

Example Setup: Fixed Notifications for Uploads and Deletions

In this example, a company shares FileCloud support folders with customers so the customers can upload help requests that are then viewed by Support. The customers are also permitted to delete requests that no longer have to be addressed.

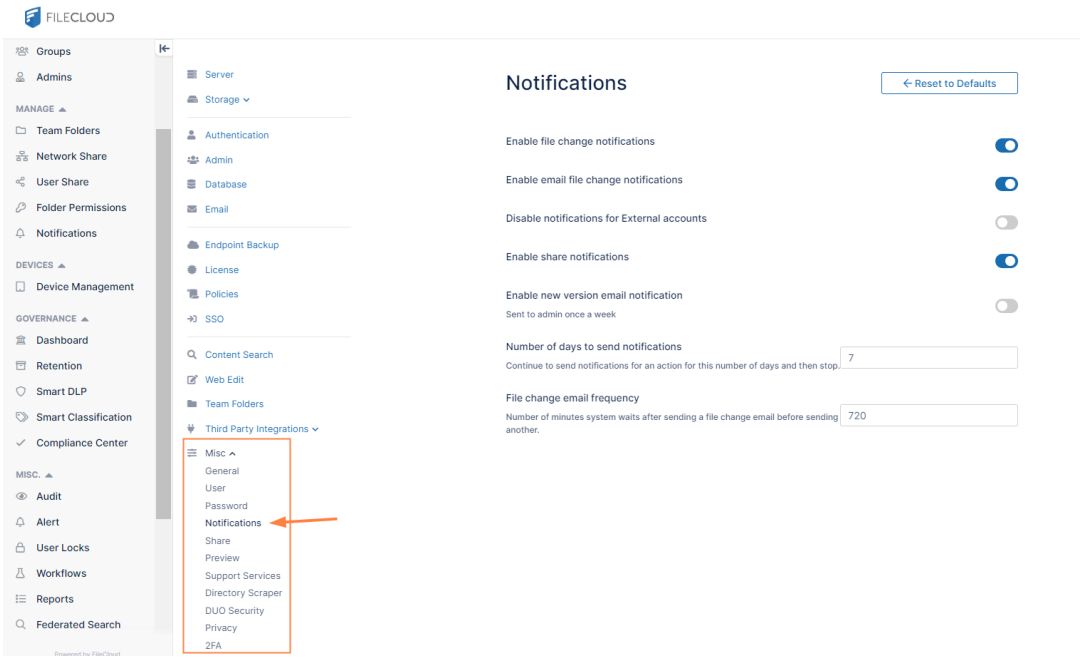
As the admin you must set up email notifications that inform Support staff when:

- new help requests are uploaded so they can begin processing them
- existing help requests are deleted in case they have begun addressing them.

To prevent accidental changes to these notifications, you do not allow users to change the notification settings.

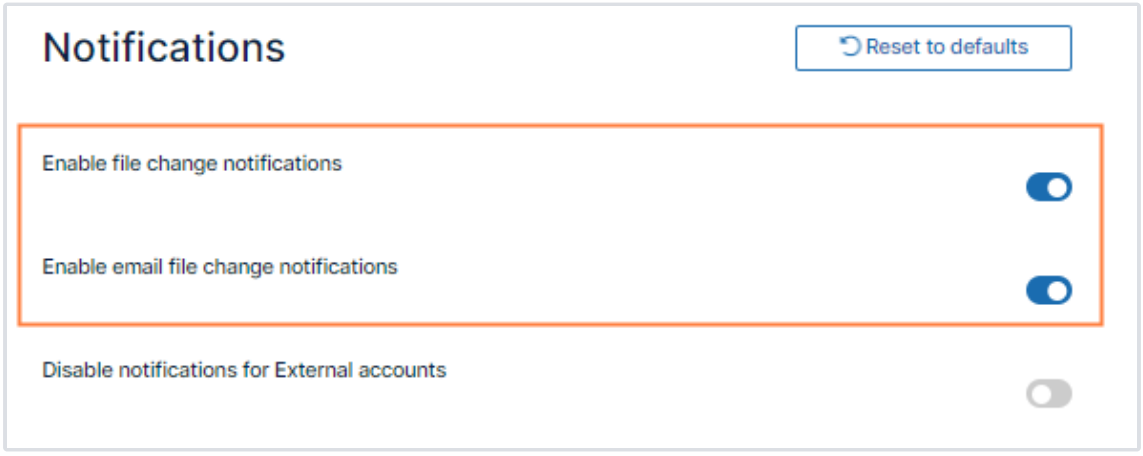
To configure these settings:

1. To enable email notifications globally, open the Notifications settings page.
   To open the Notification settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Notifications**, as shown below.

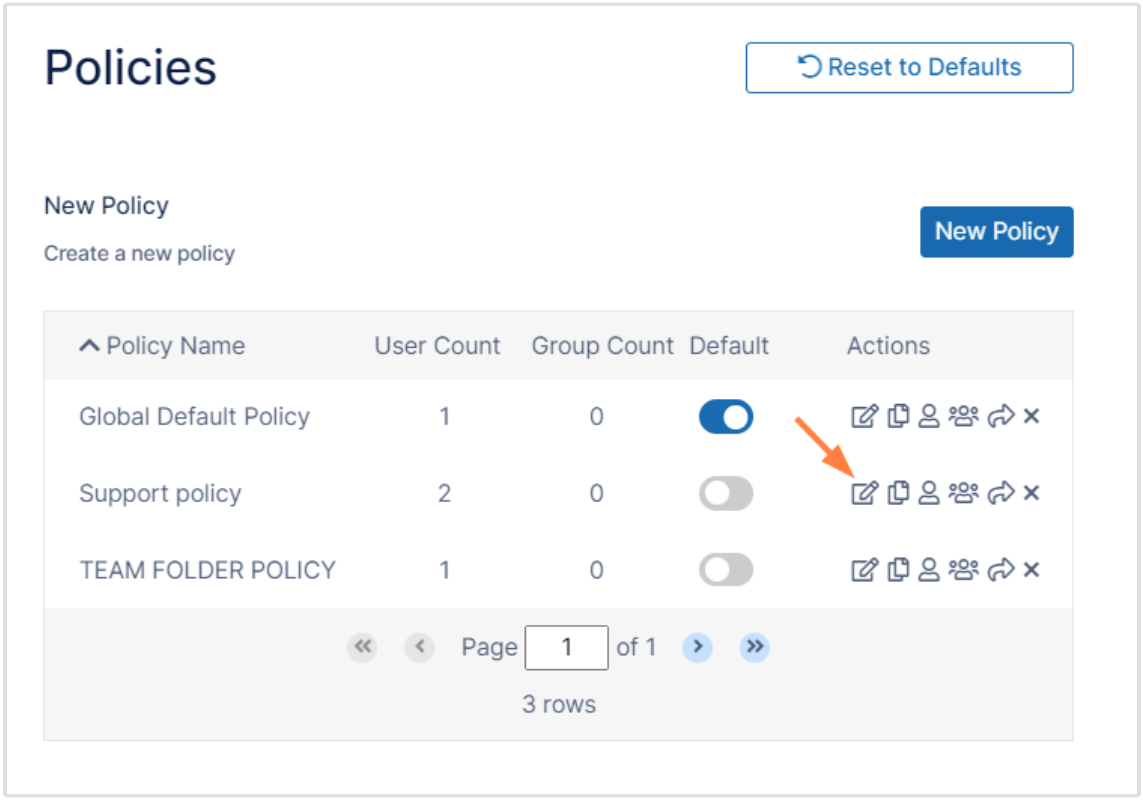


The **Notifications** settings page opens.

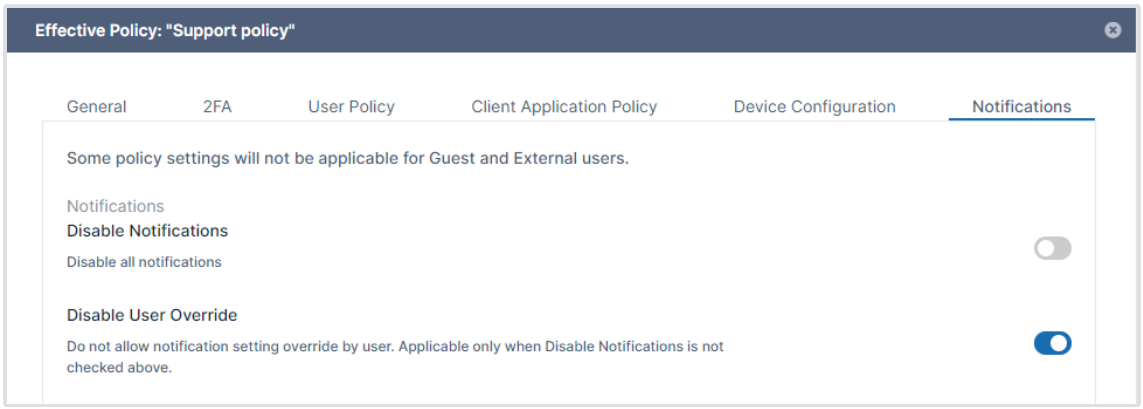
2. Make sure **Enable file change notifications** is enabled. if it is not enabled, **Enable email file change notifications** is not available.
3. Enable **Enable email file change notifications**.



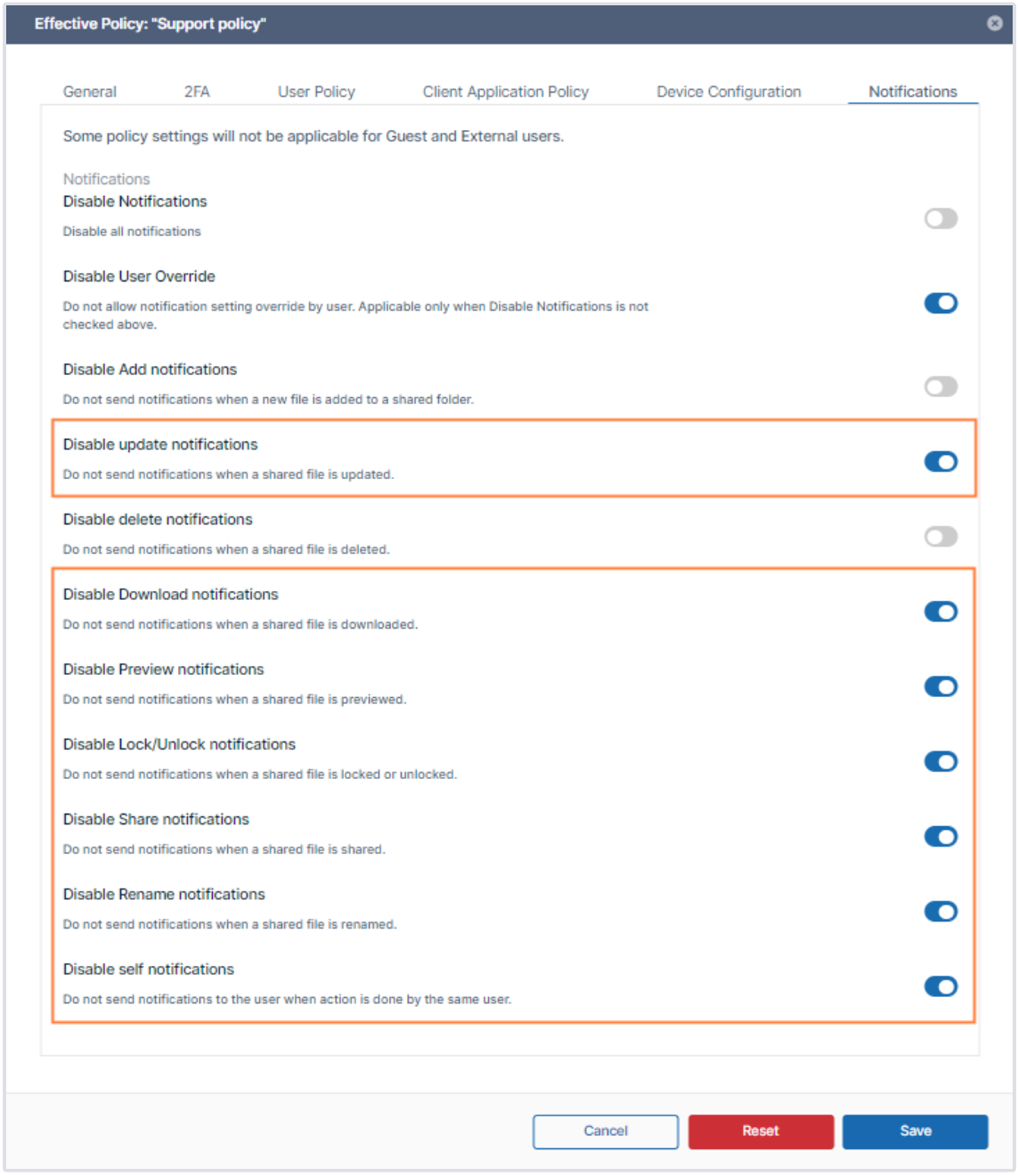
4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** settings page opens.
5. Edit the policy assigned to support personnel.



6. Click the **Notifications** tab.
7. Disable the field **Disable Notifications**, and enable the field **Disable User Override**.



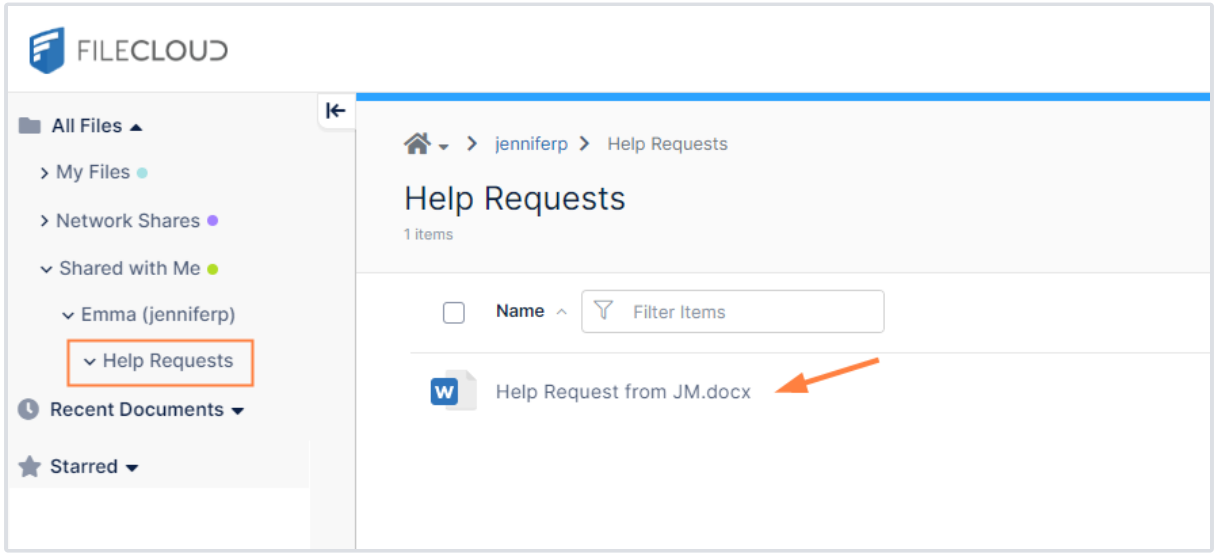
8. Scroll down so that you can view the individual **Disable Notifications** settings, and only leave **Disable Add Notifications** and **Disable Delete Notifications** set to off. Set the other **Disable Notification** settings to on.



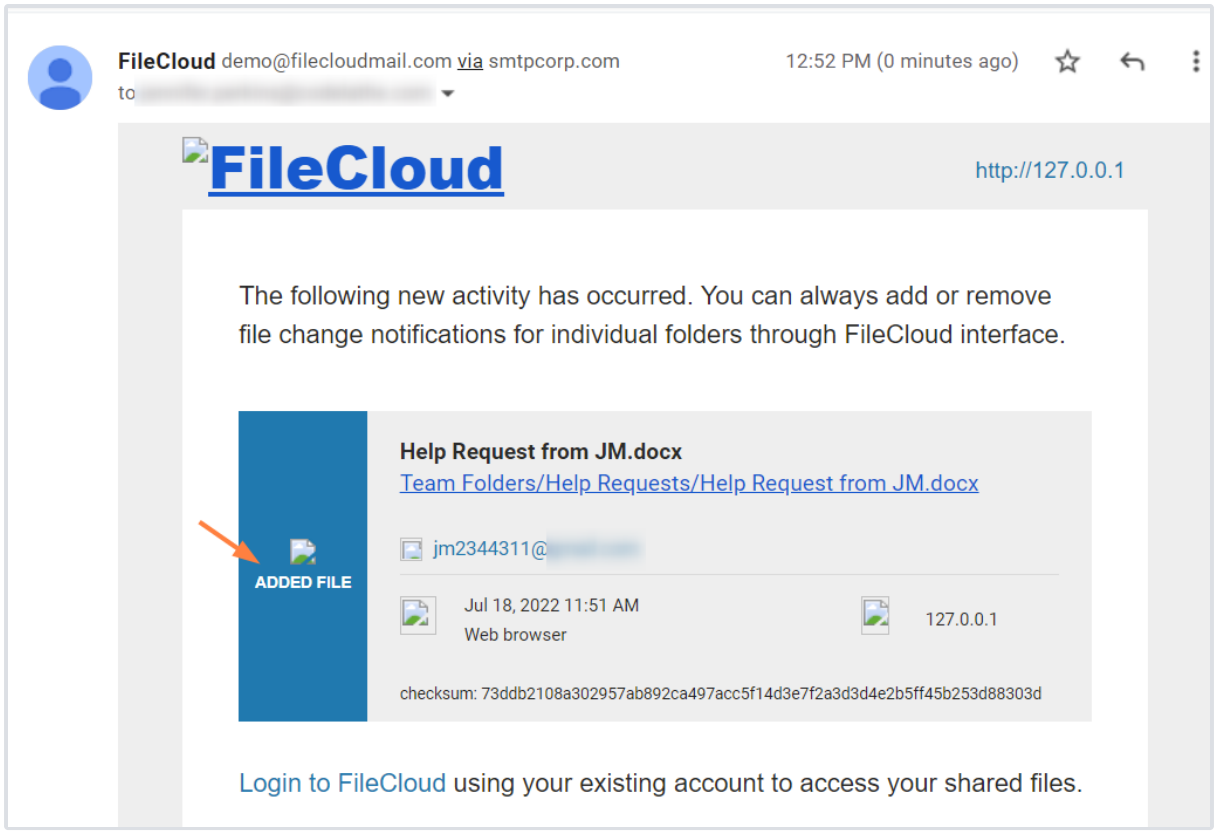
9. Save your changes.

When a customer uploads a help request

Now, when customer JM uploads a help request to the **User Help Requests** folder which has been shared with them (the folder is in **Shared with Me**) . . .

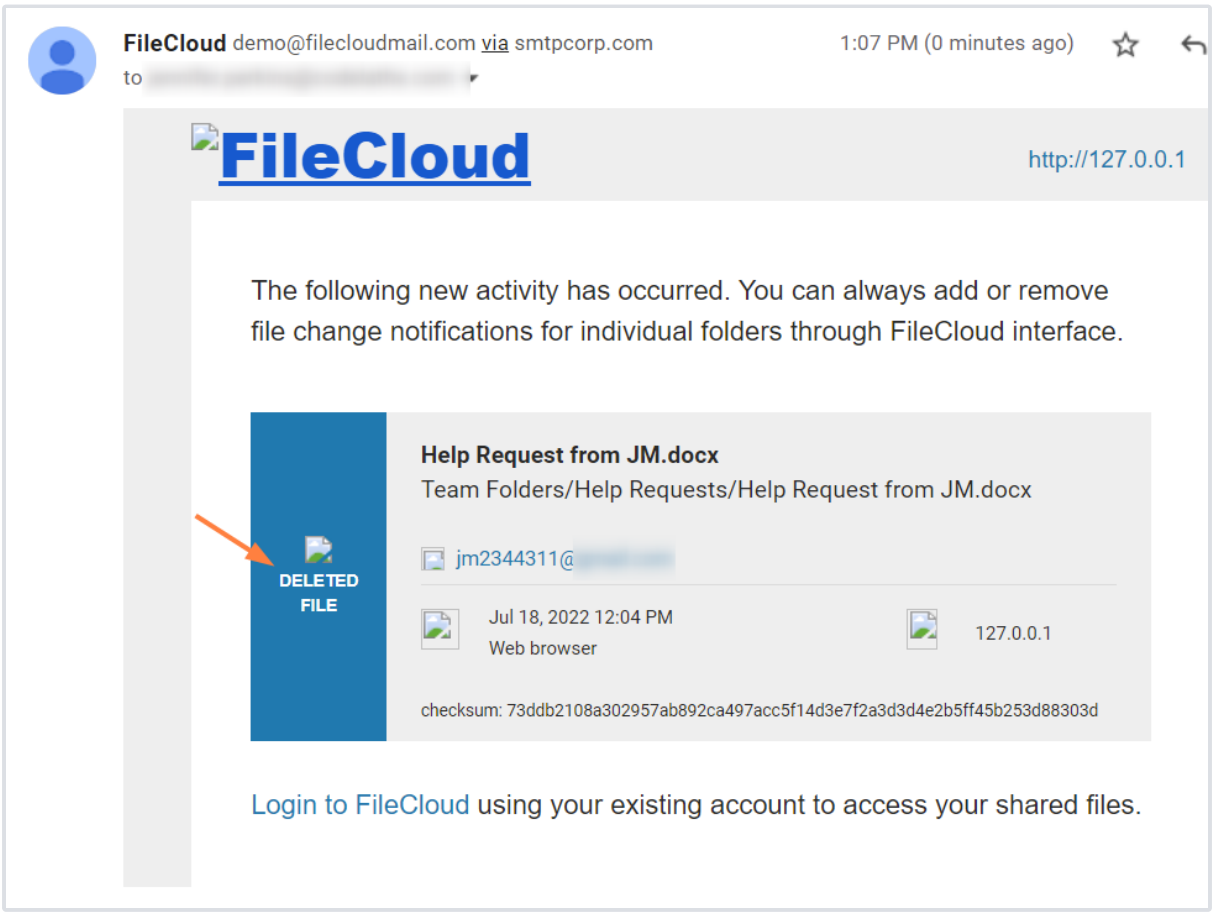


. . . users in support receive an email informing them that a new request file has been uploaded:



When a customer deletes a help request:

If customer JM deletes the help request file, users in support receive an email informing them that it has been deleted:



Example Setup: User-enabled Notifications on Folders

In this example, a telecommunications company uses FileCloud to share Team Folders that hold the latest product and pricing information with everyone in its sales department.

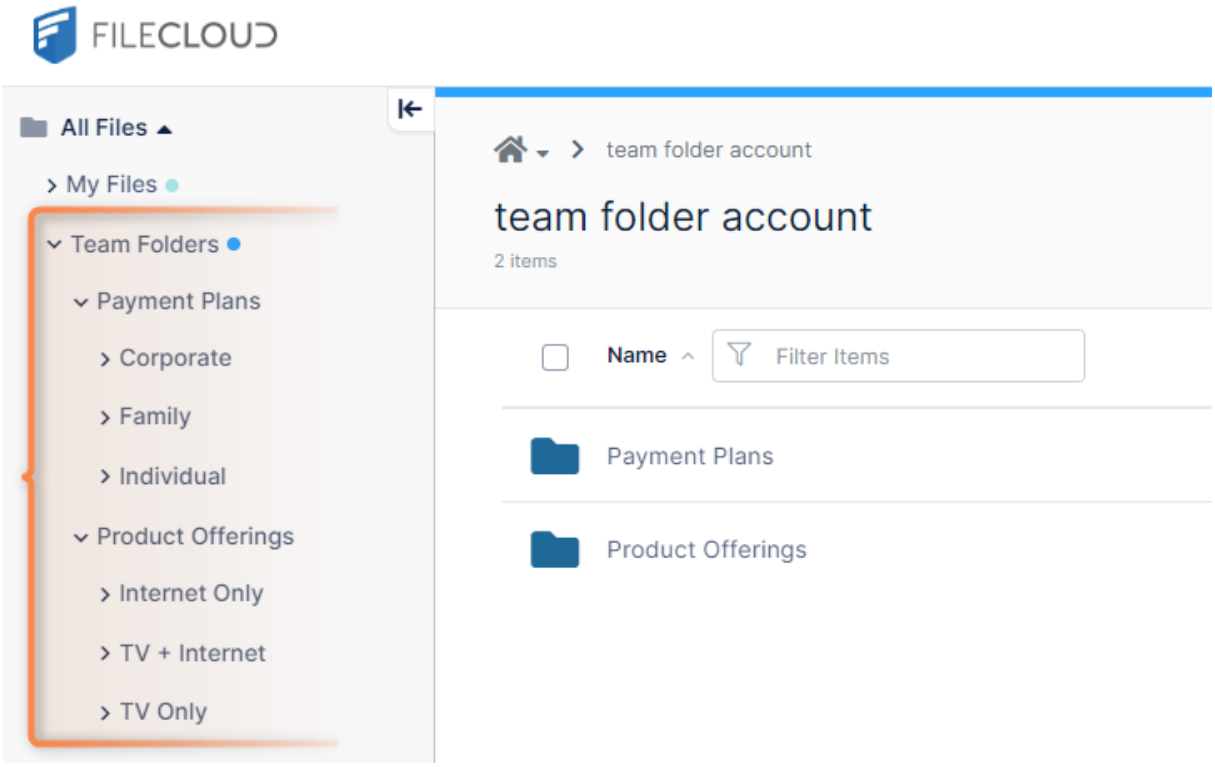
The company has three product offering categories:

- **Internet Only**
- **TV Only**
- **Internet + TV**

and it has three pricing plans:

- **Corporate**
- **Family**
- **Individual**

The company has a Team Folder with information that is available to all sales reps on each product offering and pricing plan. All sales reps see the following under Team Folders:



Each sales representatives works with a specific payment plan and product offering and only needs notifications about the product and pricing plans they work with, and do not want to receive updates about other offerings.

Therefore, as the FileCloud admin, you want each sales rep to be able to customize their file change notifications depending on which campaigns or pricing plans they are currently working with, so they know immediately when these product offerings and prices change. In addition, you want to give sales reps the opportunity to eliminate notifications about information they are not interested in.

After you configure these capabilities, each sales rep must log in to the user portal and choose the paths of the Team Folders that pertain to them and add notifications to them.

To configure these settings

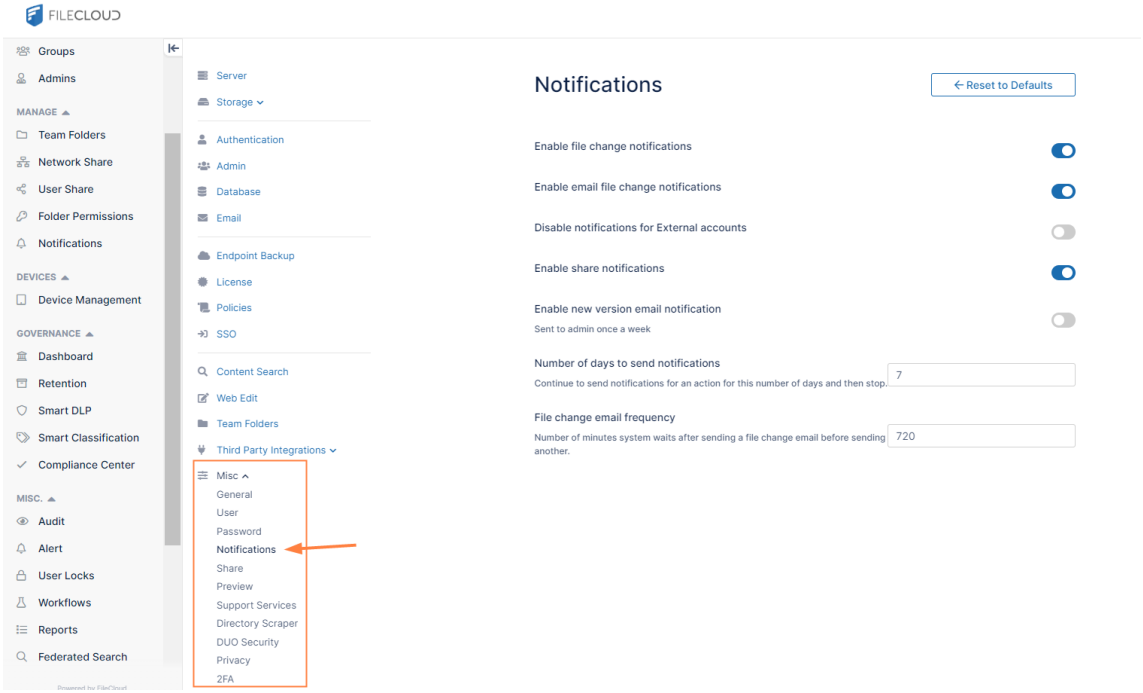
These are the steps you (the admin) use to set up the notifications according to these requirements:

1. To enable email notifications globally, open the Notifications settings page.

To open the Notification settings page

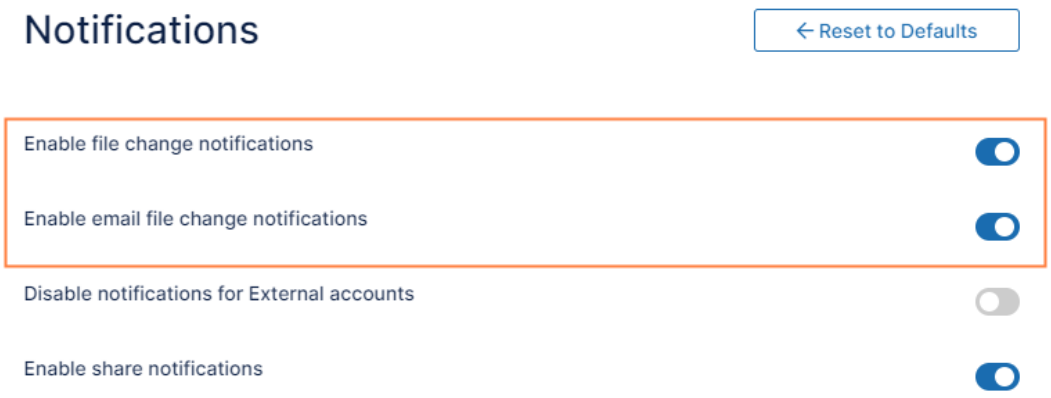
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .

2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Notifications**, as shown below.

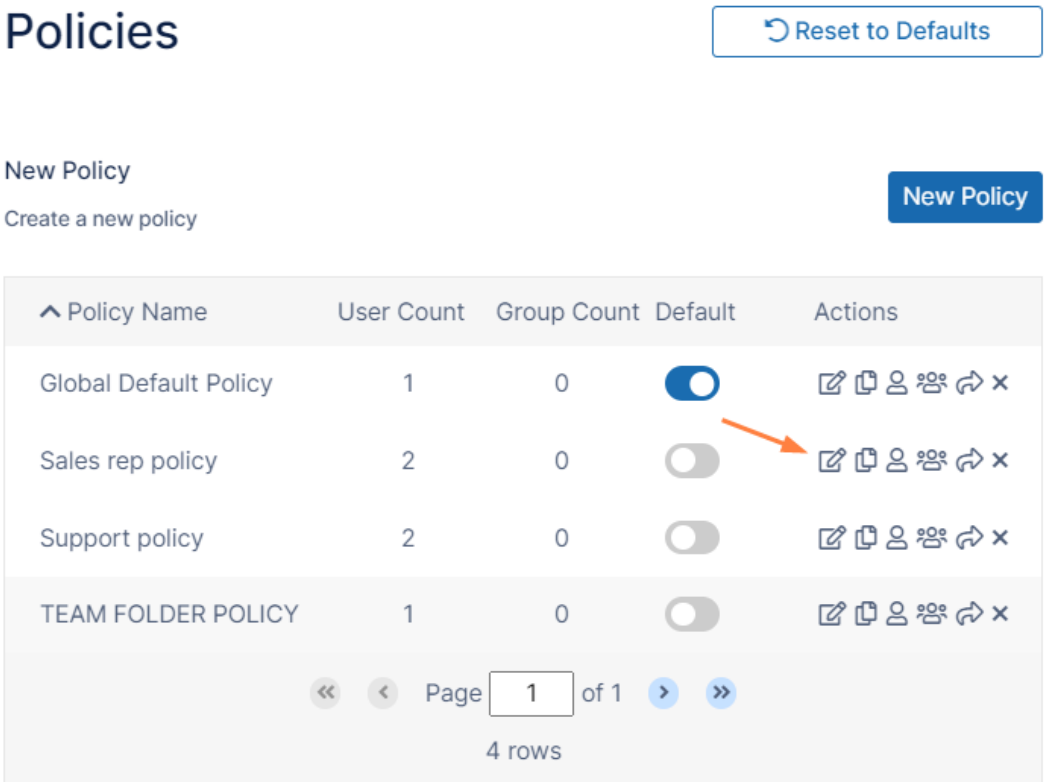


The **Notifications** settings page opens.

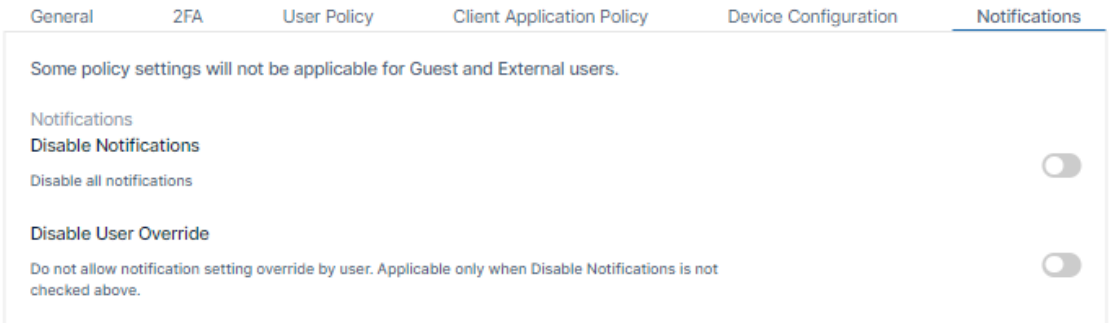
2. Make sure **Enable file change notifications** is enabled. if it is not enabled, **Enable email file change notifications** is not available.
3. Enable **Enable email file change notifications**.



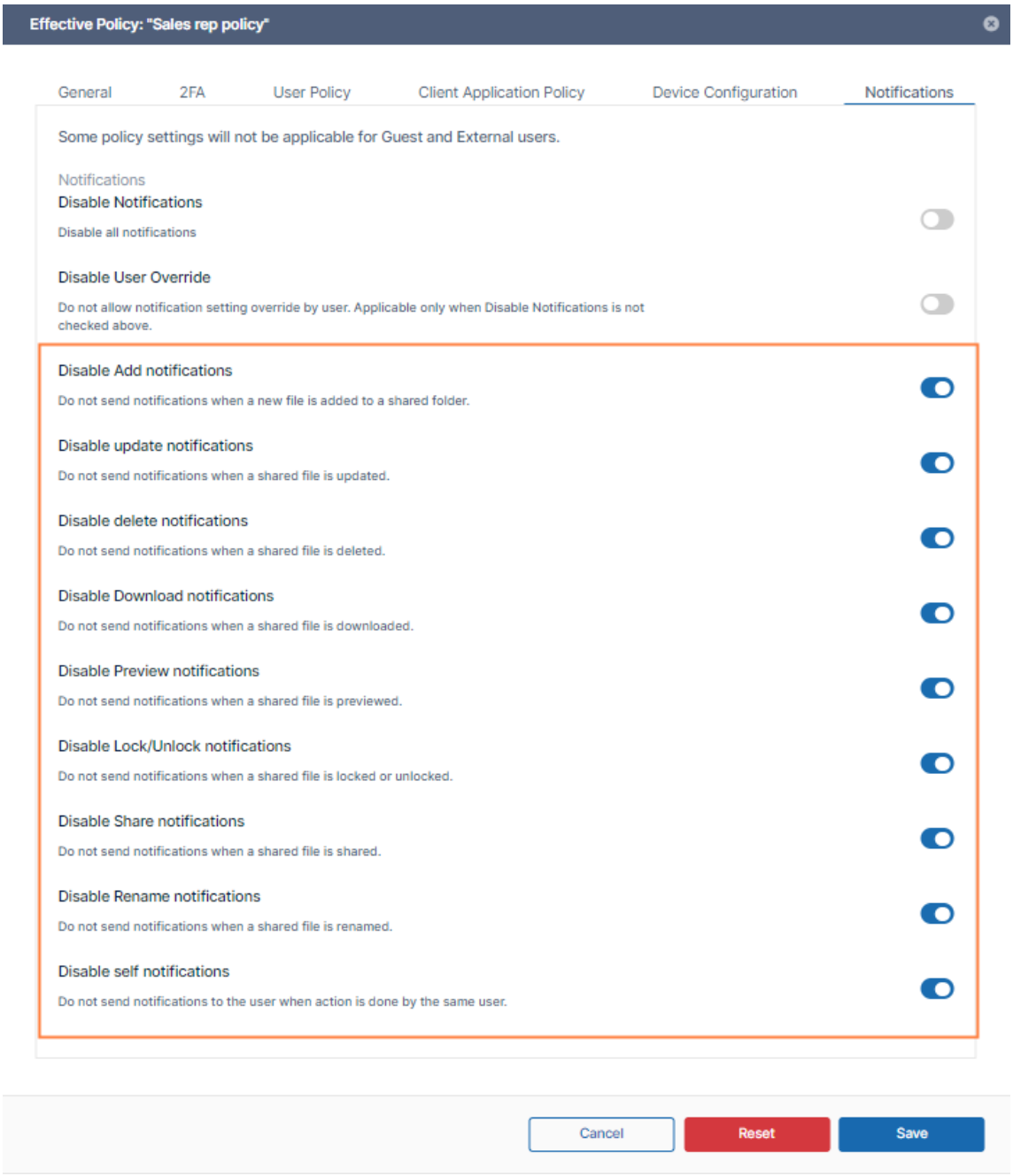
4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** UNKNOWN ATTACHMENT.
   The **Policies** settings page opens.
5. Edit the policy assigned to the sales reps.



6. Set **Disable Notifications** and **Disable User Override** to off.



7. Scroll down so that you can view the individual **Disable Notifications** settings, and set all of the **Disable Notification** settings to on.



8. Save your changes.

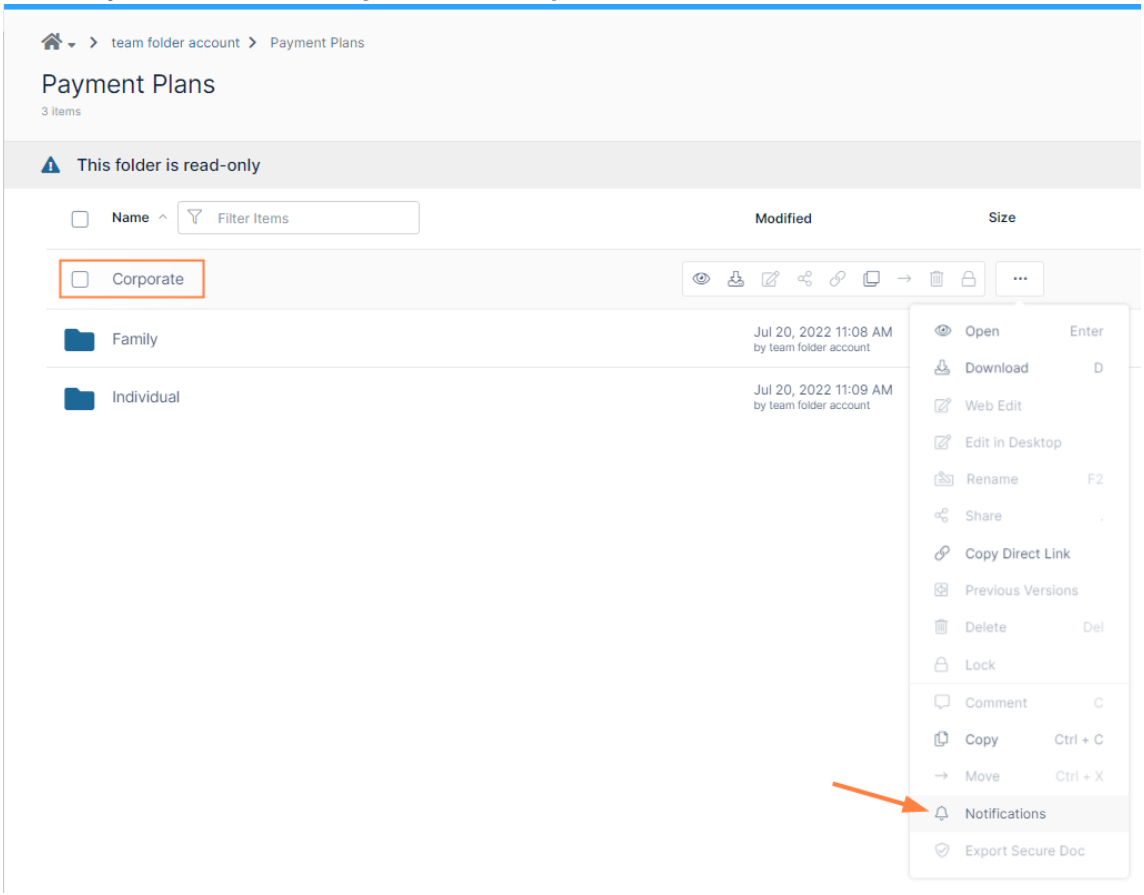
How a Sales Rep sets up notifications about information particular to their clients:

In this example, the sales rep only works with corporate customers who purchase internet only.

Instructions for the sales rep to configure notifications for just the Corporate and Internet Only Team Folders:

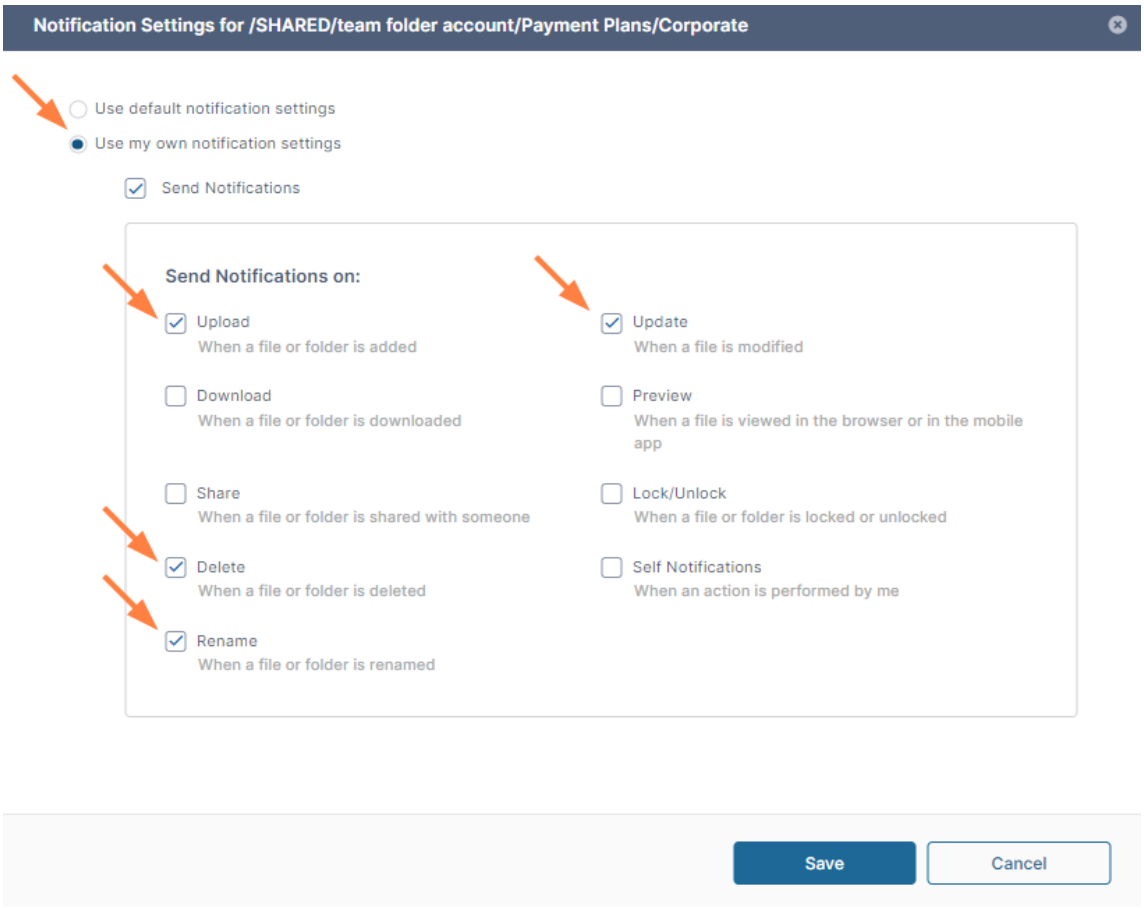
1. Log in to the user portal and go to Team Folders.

2. In the **Payment Plans** folder, right click the **Corporate** sub-folder, and choose **Notifications**.



Notifications settings for the **Corporate** Team Folder open.

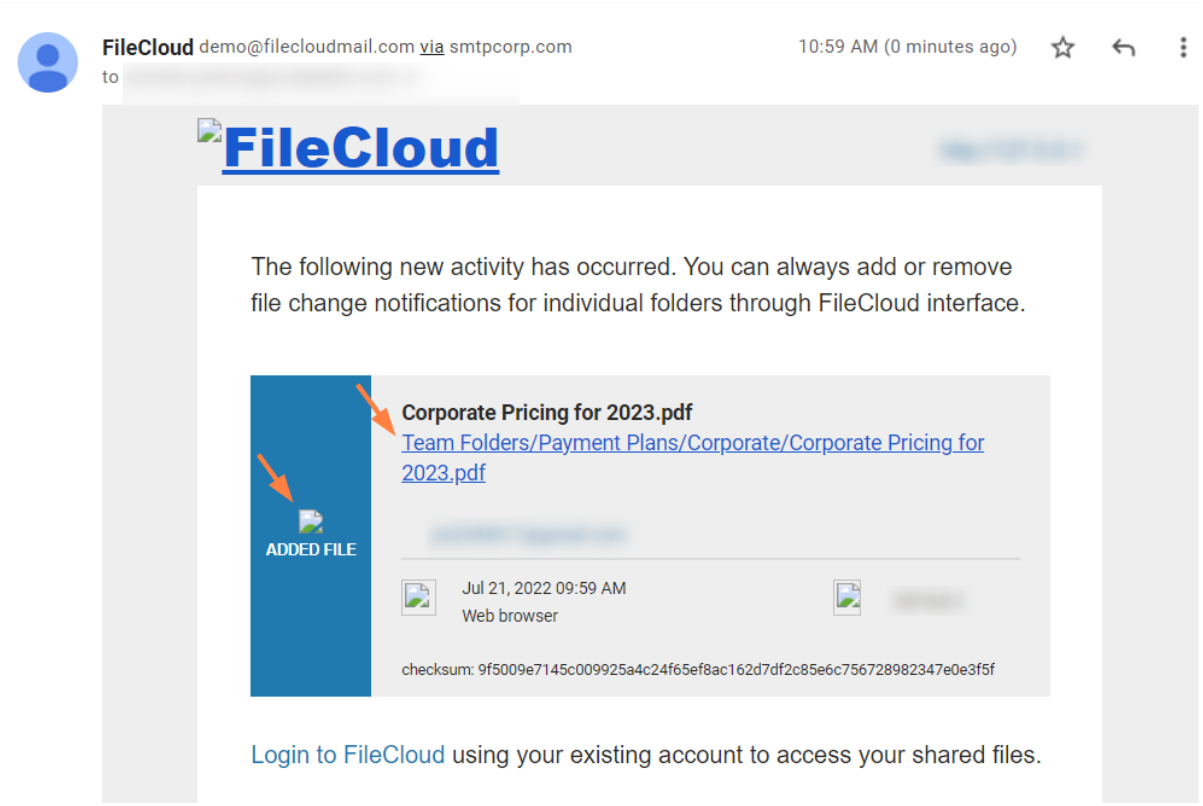
3. Select **Use my own notification settings**.
4. Check the actions that you want to be notified about in the folder (for example **Upload**, **Delete**, **Rename**, and **Update**).



5. Click **Save**.
6. Navigate to the **Product Offerings/Internet Only** folder, and repeat steps 2 through 5, above, to set notifications for the folder.

When content is changed in one of the folders:

If content is added to the **Corporate** or **Internet Only** Team Folder, the sales rep who set up notifications for those folders receives an email similar to the following:



If content is modified in any of the other Team Folders, the sales rep does not receive notifications about them.

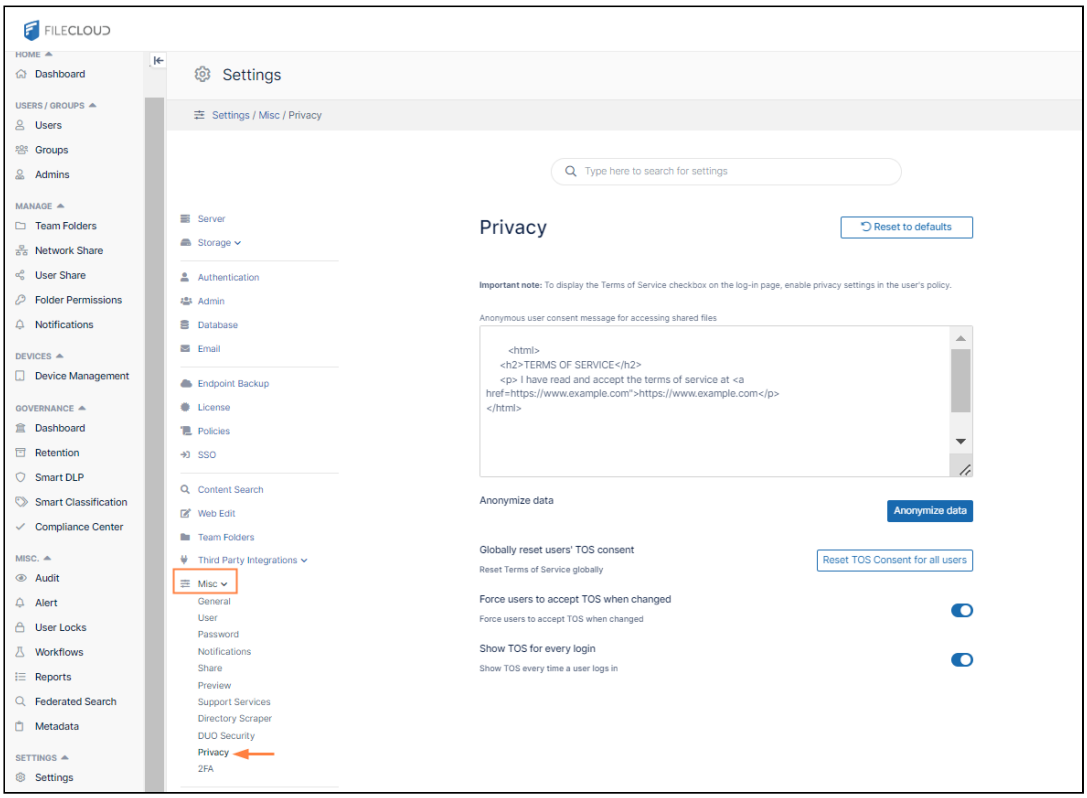
Anonymizing User Data



You can search for and replace specific names, emails, and IP addresses with a non-traceable ID in the activity logs.
This action cannot be undone.
The process does not make activity outside this FileCloud instance anonymous. This includes any backup system, web site logs, or database server logs. You must search and remove references from those separately.

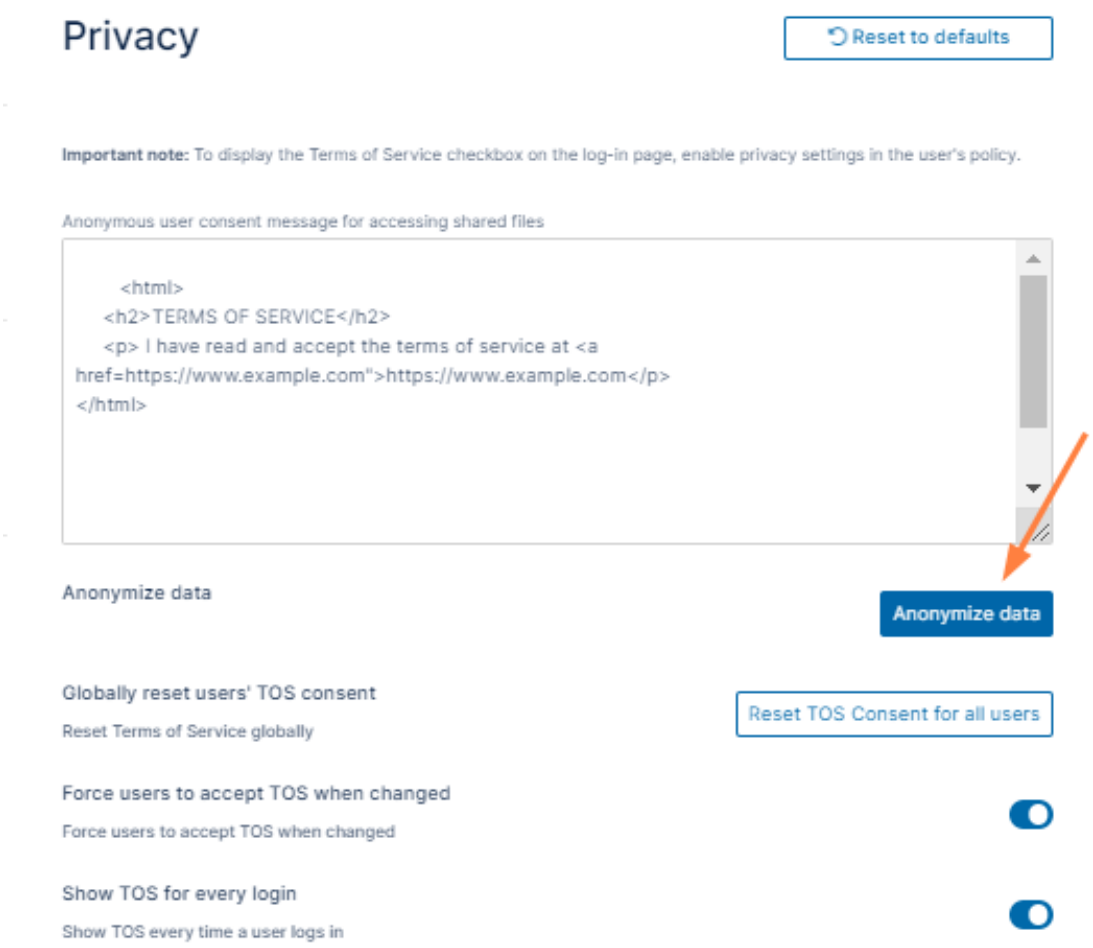
To anonymize user data:

1. Open the Privacy settings page.
   To go to the Privacy settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click **Misc**  .
   b. In the inner navigation bar on the left of the Settings page, expand the **Misc** menu, and click **Privacy**, as shown below.



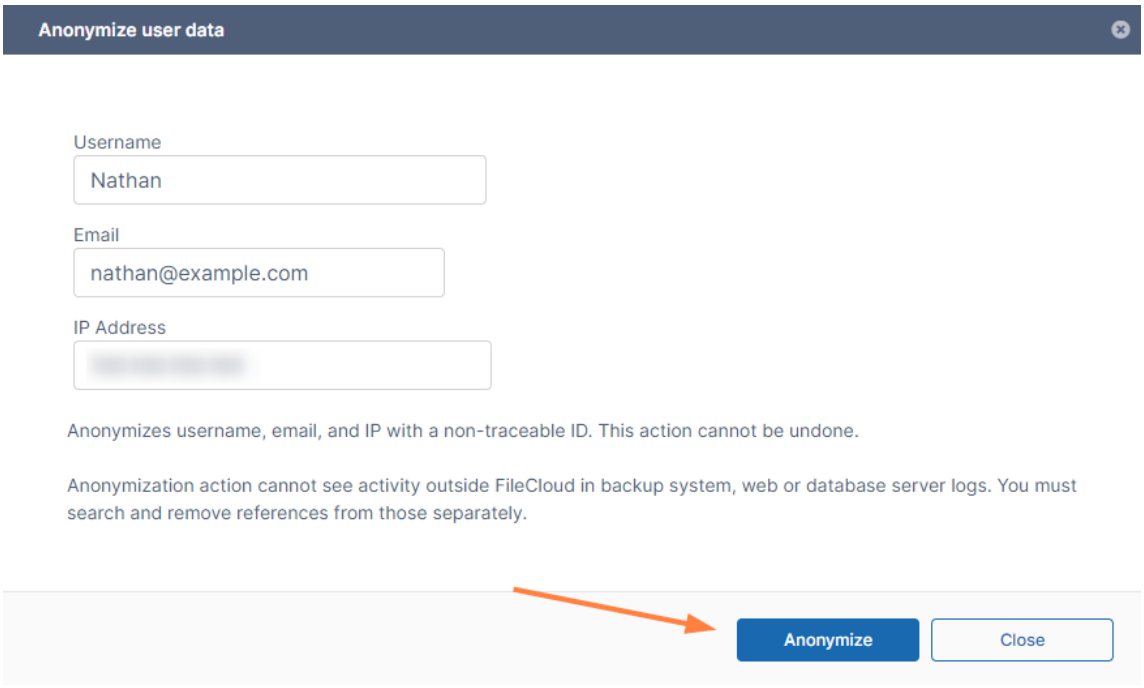
The Privacy settings page opens.

2. Click **Anonymize data**.



The Anonymize user data dialog box opens.

3. Type in the username, email, and IP address you want to replace with a non-traceable ID.



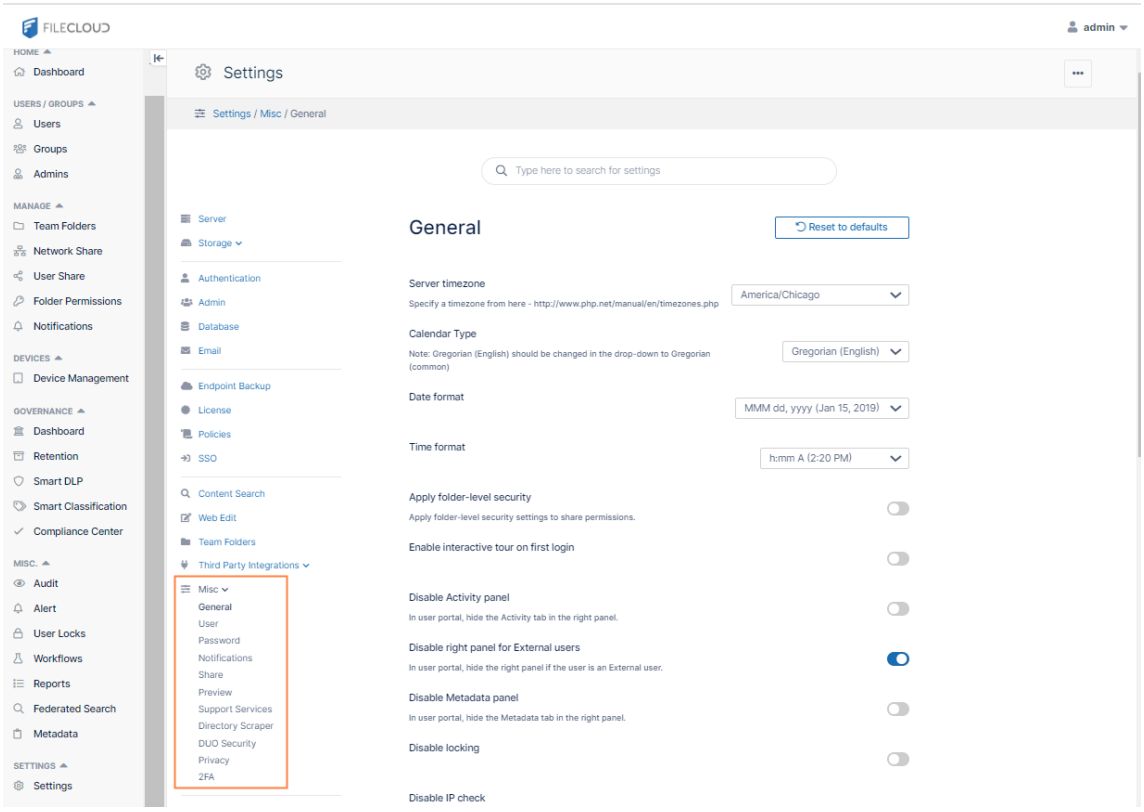
4. Click **Anonymize**.

Misc Settings

Misc settings include many options for you to change default values.

To access the Misc settings:

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. To access other pages of **Misc** settings, in the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click the name of the **Misc** settings category, as shown below.



General settings

Setting	Tab	Description	Version Added
Server timezone	General	Sets the time zone for the server	

Setting	Tab	Description	Version Added
Calendar Type	General	Choose the format of the choices that appear in the following **Date format** and **Time format** drop-down lists. The **Calendar Type** chosen is used for dates in the user portal as well as the Drive client. It is not used in the admin portal. Options: • **Gregorian** (English, default)) - Show Western formats. • **Hijri** (Islamic) - Show Arabic formats.	FileCloud 22.1
Date format	General	Choose one of the options in the drop-down list. The options shown depend on whether **Gregorian** or **Hijri** is selected in the **Calendar Type** field. The **Date format** chosen is used for dates in the user portal as well as the Drive client. It is not used in the admin portal.	
Time format	General	Choose one of the options in the drop-down list. The options shown depend on whether **Gregorian** or **Hijri** is selected in the **Calendar Type** field. The **Time format** chosen is used in the user portal as well as the Drive client, and in share windows in both the user portal and admin portal.	
Apply folder-level security	General	Allow folder level security permissions to share.	
Enable interactive tour on first login	General	Displays interactive tour to users the first time they log in to the FileCloud user portal.	
Disable Activity panel	General	This setting hides the right panel that displays activities, comments, permissions and other details in the user interface. Note that activity records are not generated when this is enabled..	
Disable right panel for External users	General	Hides right panel if the user is a External user. Check by default.	
Disable Metadata panel	General	Hides metadata panel and disables metadata search option in user portal.	
Disable locking	General	Disables supports for file and folder locking. See File Locking for more information about locking files and folders.	

Setting	Tab	Description	Version Added
Disable IP check	General	Disables IP check on every request. Use if it is valid for IP addresses to change while users are using the system to avoid unwanted session termination.	
Email domain names to block	General	Enter the comma separated email domain names to block.	
Enable proxy settings	General	Enter the settings of a proxy network if needed.	
Scheduled tasks	General	Manually execute cron tasks.	
Import files	General	Import files to managed storage,	
Allowed file extensions	General	Specify file extensions that are allowed to be uploaded. Leave this empty to allow all file extensions except any specified in **Disallowed file extensions**.	
Disallowed file extensions	General	Specify file extensions that cannot be uploaded.	
Disallowed file names	General	Specify file names that cannot be uploaded.	
Check for double file extension	General	Include additional checks for double extensions to increase security.	
Forbidden Network Folder paths	General	Network Folder paths that are prohibited from being used	
Disable automatic database backup	General	Disables automatic database backup	
Database backup store path	General	Specify a writable path to store backed up database.	
Number of backups to store	General	Number of backups to maintain.	
Database backup Interval	General	Interval between backup process. 0 = daily backup.	

Setting	Tab	Description	Version Added
Disable content classification	General	Do not allow content classification.	
Enable WebSockets	General	Enable WebSocket in order to run the Push service or other client/server communications.	FileCloud 23.232
Enable WebDRM	General	Enable use of the Secure Web Viewer option.	

User settings

Setting	Tab	Description
Folder to import files from on user creation	User	See: Preload data for new accounts
User account search mode	User	See: Securing Shares by Limiting User Account Searches
User search account type	User	Restrict user searches so that your users can only search for users in certain account types. See User Search Account Type.
Group visibility	User	Control what groups are listed to a user when a private share is created by that user. By default, all user groups are shown, you can change that to only show groups that the user actually belongs to. This can prevent sharing of files inadvertently to large groups.
Send email to user to approve device	User	Send email to users when a new device is ready for approval.

Setting	Tab	Description
Default view settings	User	Select how files appear to users by default. (See: (23.263a) Viewing Files by List or Grid). The options are: (size varies depending on screen resolution) • **Automatic** - The default. Initially, **Automatic** is List view. Once the view is changed by the admin or by the user, **Automatic** is the user's most recent view. • **Large Thumbnails** - Grid of thumbnails that are approximately 400 by 400 pixels. • **Medium Thumbnails** - Grid of thumbnails that are approximately 280 by 280 pixels. • **Small Thumbnails** - Grid of thumbnails that are approximately 200 by 200 pixels. • **List View**
Allow users to modify their phone numbers	User	Allow users to change their phone numbers in the user portal Settings screen.

Notifications settings

Setting	Tab	Description
Enable file change notifications	Notifications	When checked, enables recent activity notifications to appear on the user portal when files are created, updated, deleted and downloaded on a shared folder. Checked by default.
Enable email file change notifications	Notifications	When checked, enables the system to send Email notifications when files are created, updated, deleted and downloaded on a shared folder. Enable File Change Notifications must be checked for this setting to be enabled. Checked by default.
Disable notifications for External accounts	Notifications	When this option is enabled no share notifications will be sent to the external user.
Enable share notification	Notifications	When this option is enabled share notifications will be set to NO by default. The "Email FileChange Notifications" will be set to NO in Manage Share → advanced options.
Enable new version email notification	Notifications	When checked, emails about new versions of FileCloud are sent to the administrator once a week.

Setting	Tab	Description
Number of days to send notifications	Notifications	Send notifications for actions for the specified number of days
File change email frequency	Notifications	How frequently, in minutes, email notifications are sent. Beginning in FileCloud 23.241, the default frequency is 720 minutes (12 hours).

Other Misc. tab settings

For password settings, see Password Settings

For share settings, see Share Settings

For document preview settings, see Document Preview and Enabling Document Converter and Thumbs.

For support service settings, see Improve Helper Performance.

For directory scraper, see Enabling Directory Scraping.

For DUO security settings, see Multi-Factor Authentication.

For privacy settings, see Terms of Service and Anonymizing User Data,

For MFA settings, see Multi-Factor Authentication

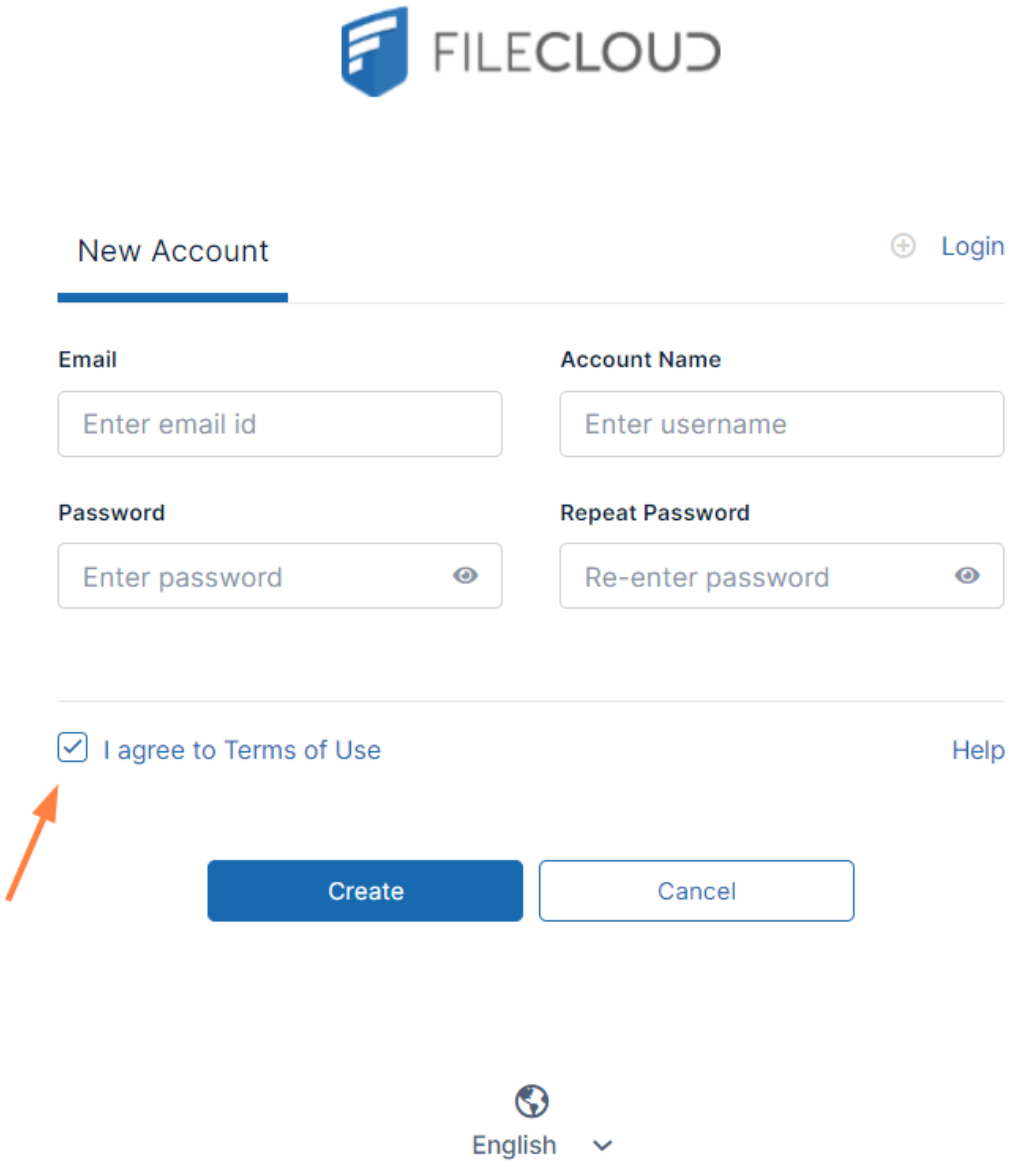
Terms of Service

Beginning with FileCloud Version 21.3, when **Enable Privacy Settings** is set to **yes** in their user policies, admin users are required to accept terms of service the first time they log into the admin portal.

Beginning with FileCloud Version 22.232, the default link to FileCloud terms of service has changed to https://www.filecloud.com/eula/. The link will only be changed automatically on new installations of FileCloud. Although the previous link will automatically redirect users to the new page, if you are upgrading FileCloud to version 23.232 or using an earlier version, we recommend that you change the link in **Customization > TOS** to https://www.filecloud.com/eula/

By default, FileCloud requires users to accept terms of service (TOS) when:

- they initially create an account
- the content of terms of service changes.

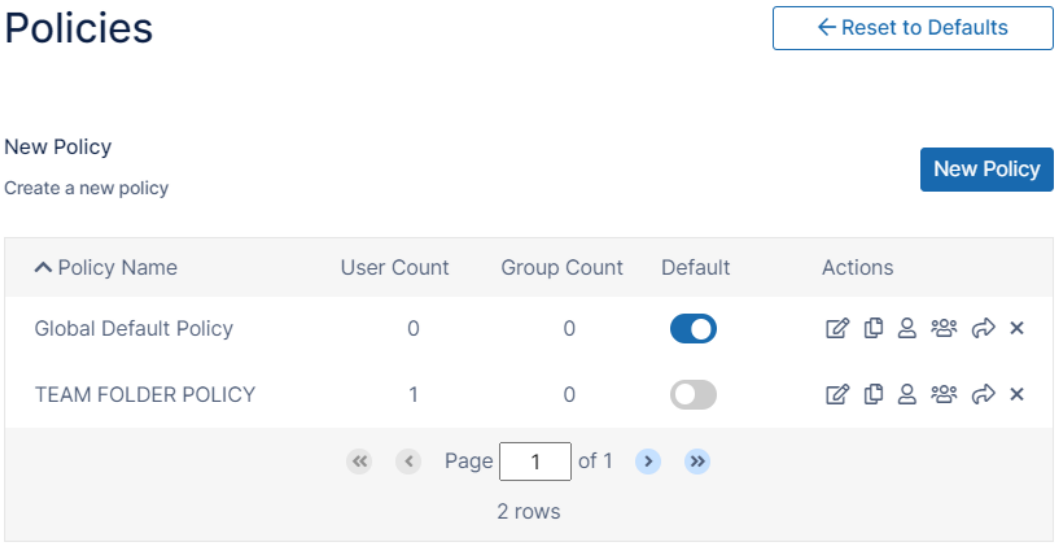


Enabling privacy settings and the Terms of Use checkbox

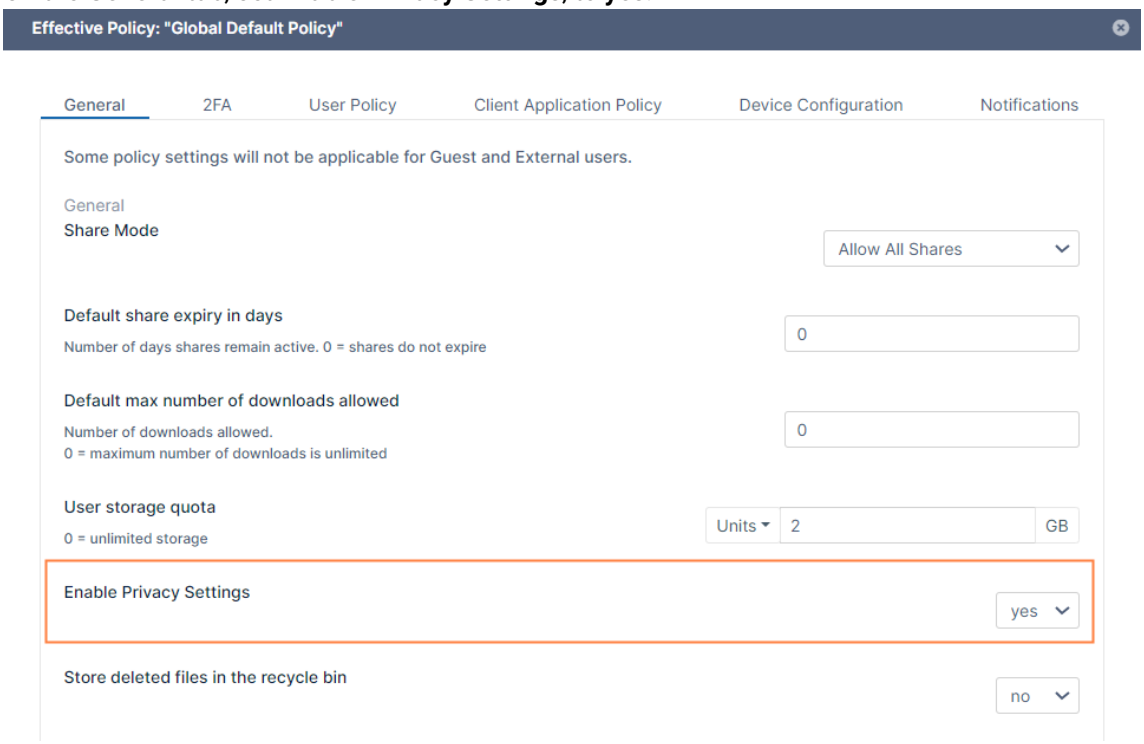
To display the **Terms of Use** checkbox on the log-in page, you must enable privacy settings. **Enable Privacy Settings** is set to **no** by default.

To enable privacy settings:

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



2. Edit the policy of the users whose privacy settings you want to modify.
3. On the **General** tab, set **Enable Privacy Settings**, to **yes**.



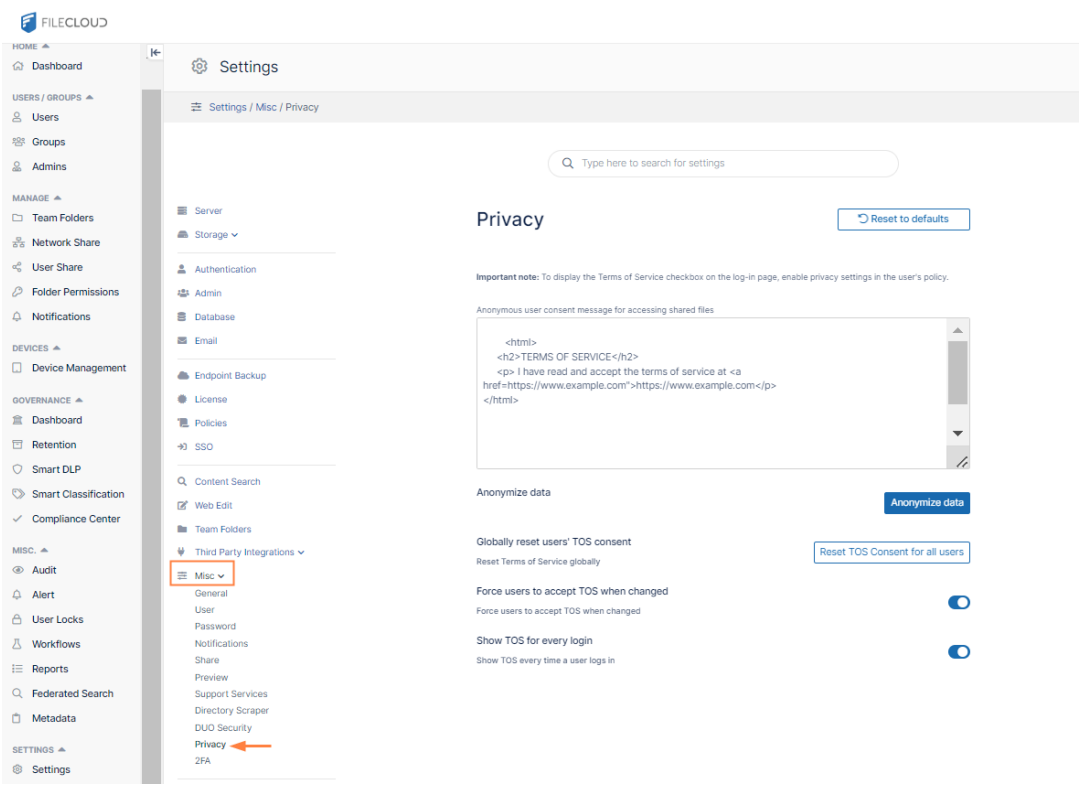
4. Click **Save**.

Showing TOS when users access public and password-protected shares

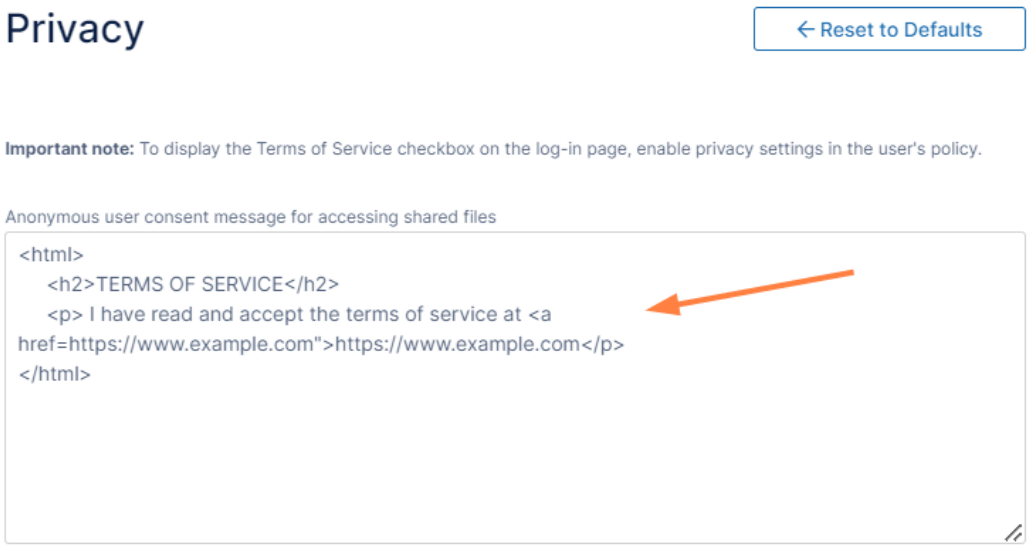
If **Enable Privacy Settings** in the General tab of a user's policy is set to **yes**, you can require users who log in to public and password-protected shares to accept FileCloud terms of service by adding text to the **Anonymous User Consent Dialog Text** field.

To require that a user accept of terms of service to access public and password-protected shares:

1. Set **Enable Privacy Settings** to **Yes** in the General tab of the user's policy as shown in the above procedure.
2. Open the **Privacy** settings page.
   To go to the Privacy settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** UNKNOWN ATTACHMENT .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Privacy**, as shown below.



   The **Privacy** settings page opens.
3. Add the content that you want to appear with the **Accept Terms of Service** button when users attempt to access the link for a public or password-protected share:



4. Click **Save**.
   Note: If you do not enter text here, the **Accept Terms of Service** button is not shown when users enter the link for a public or password-protected share, and the share is opened directly.

Terms of service settings

Administrators are able to configure the following terms of service settings:

- Enable/disable whether users must re-accept terms of service when the content changes
- Enable/disable whether users must accept terms of service each time they log in to FileCloud
- Globally reset all users' terms of service consent

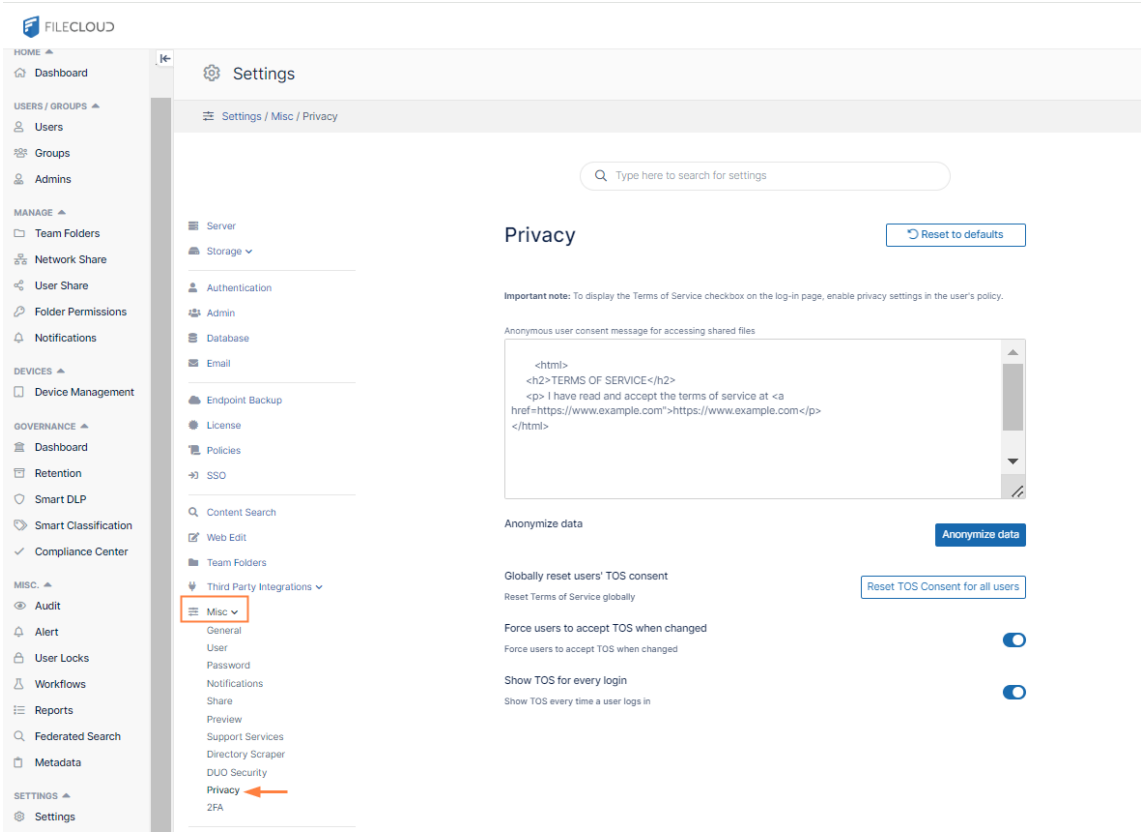
> In versions of FileCloud prior to version 20.2,
> the fields **Globally reset users' TOS consent**, **Force users to accept TOS when changed**, and **Show TOS for every login** appear in the **Customization > TOS** tab. Now these fields appear in the **Settings > Misc > Privacy** tab.

To configure terms of service settings:

1. Open the **Privacy** settings page.

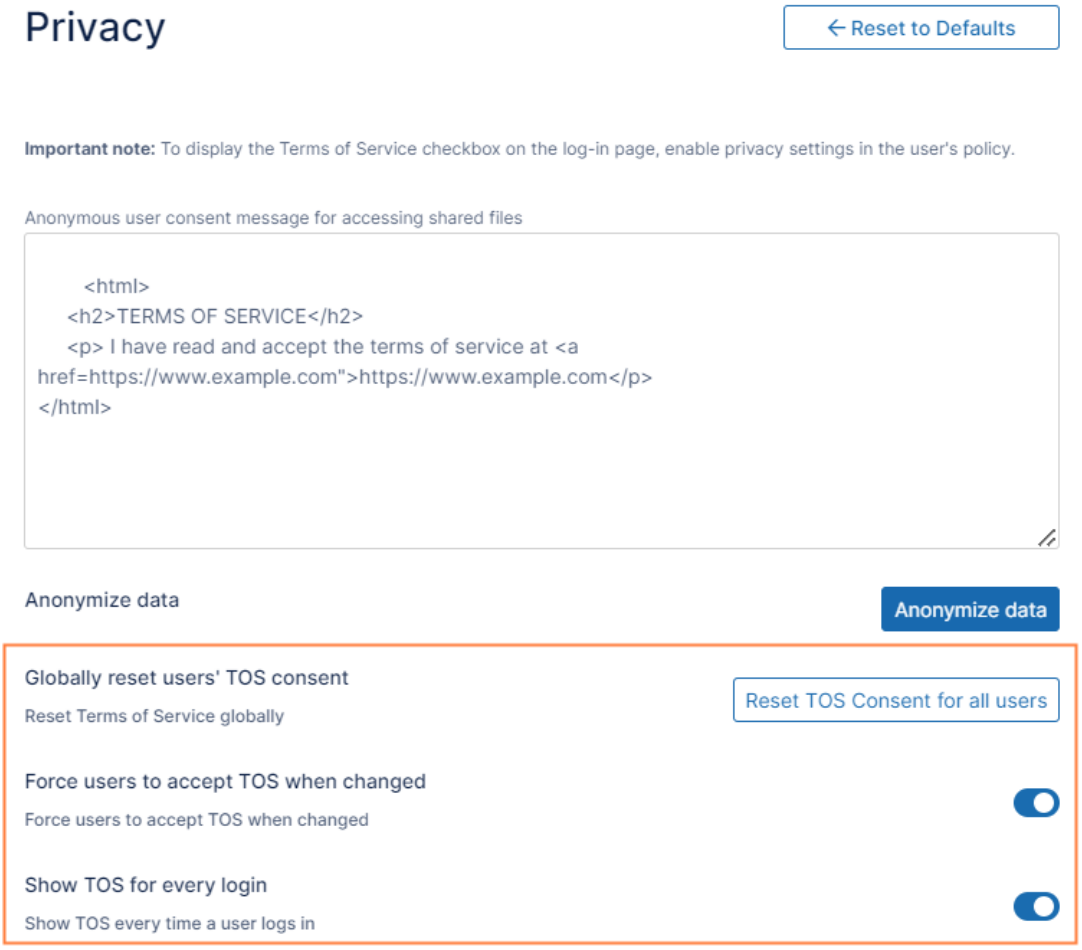
To open the Privacy settings page

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
2. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Privacy**, as shown below.



The **Privacy** settings page opens.

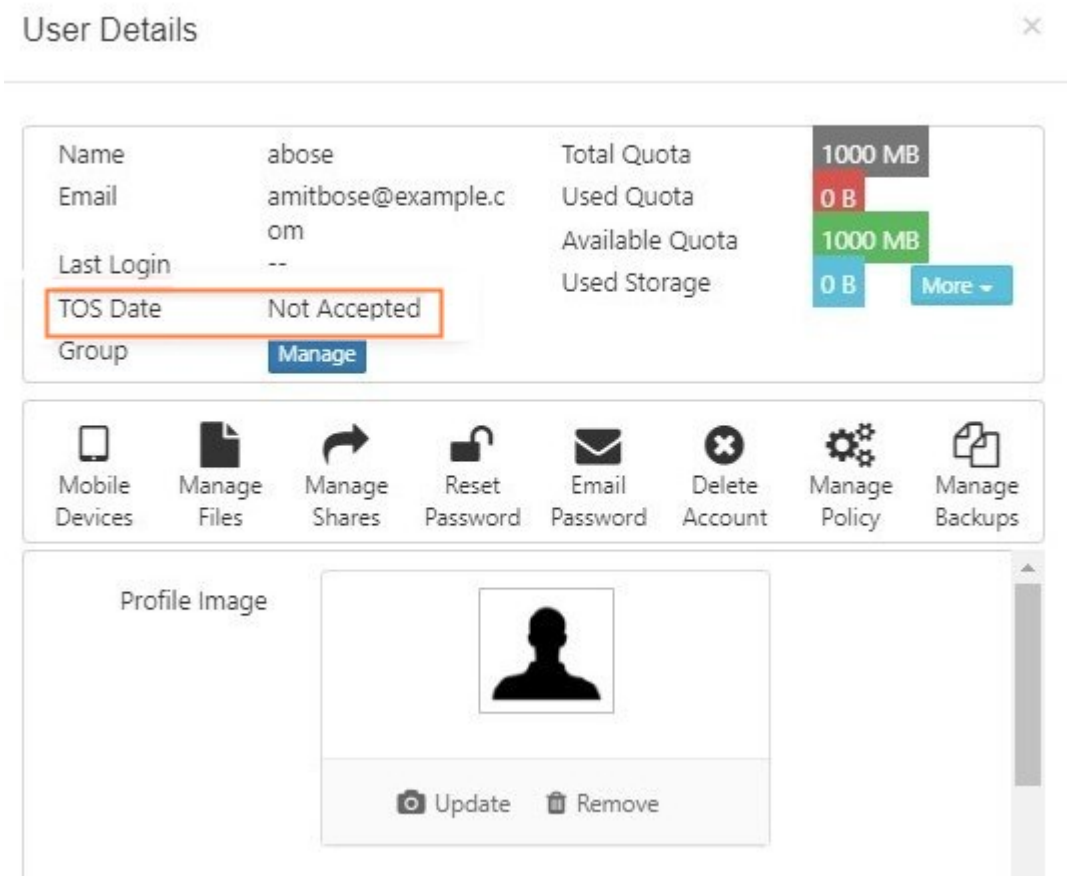
2. To globally reset TOS consent so that all users are required to re-accept the terms of service when they log in (to the user portal only), click **Reset TOS Consent for all users**
3. By default, **Force users to accept TOS when changed** is disabled.
   To require users to accept changed terms of service before logging in (to the user portal only), enable **Force users to accept TOS when changed**.
4. By default, **Show TOS for every login** is disabled.
   To require users to accept the TOS every time they log in, enable **Show TOS for every login**.
   This feature applies to all users when they sign in to the user portal and to admin users when they sign in to the admin portal.



5. Click **Save**.

See if a user has accepted terms of service

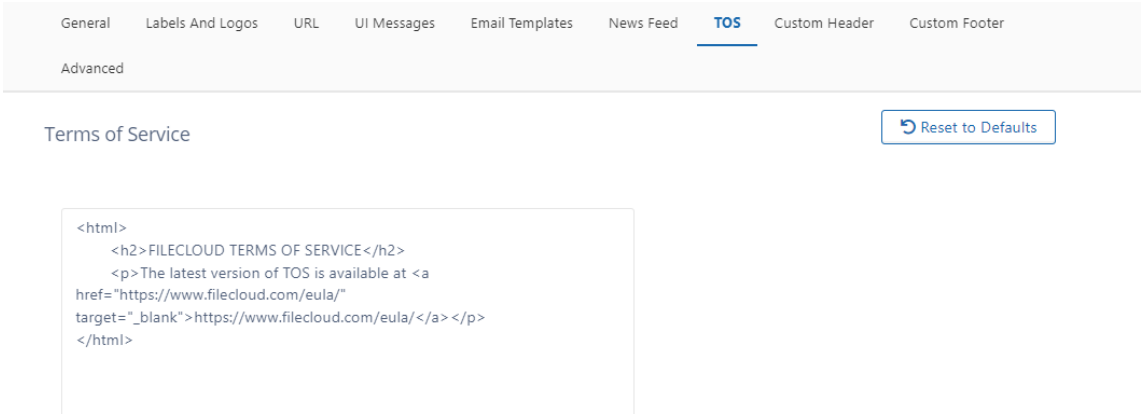
Administrators can view the user details for a user to see if they have accepted the latest terms of service. **TOS Date** either displays the date that the user accepted the terms of service or displays **Not Accepted.**
Note: TOS Date only shows if admin users have accepted the latest terms of service for the user portal; it does not show whether they have accepted it in the admin portal.



Change the content of the Terms of Service

To change the content of the Terms of Service:

1. Click **Customization** in the left navigation panel.
2. Click the **TOS** tab
3. To enter new terms of service, change the HTML code in **Terms of Service**.



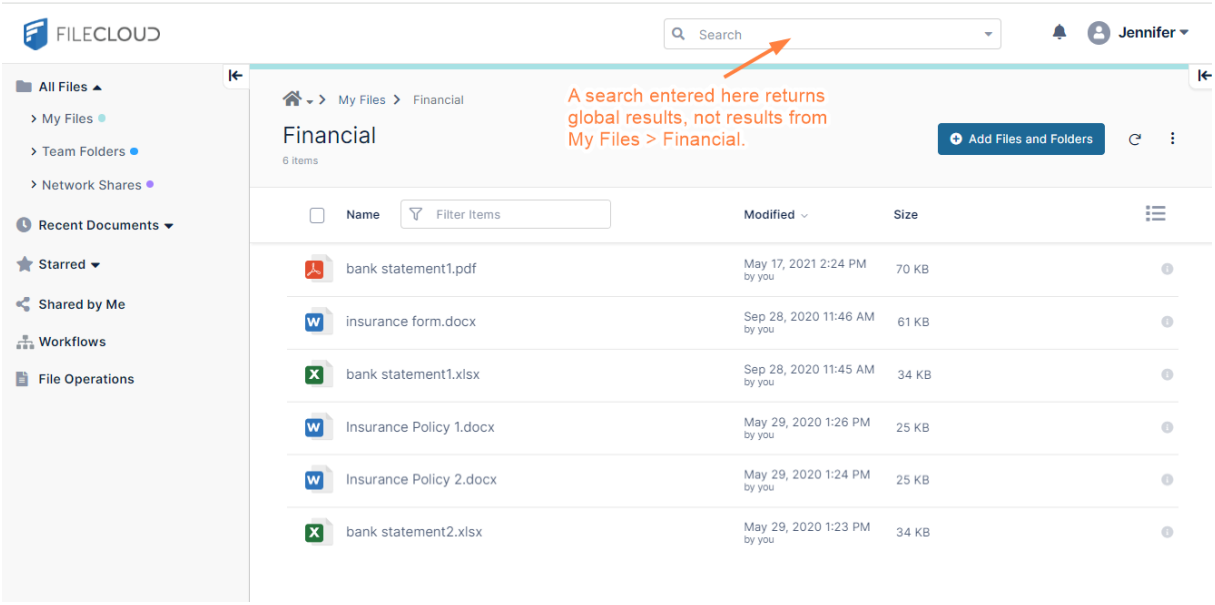
Note: This text is not shown when users open a public or password-protected share; instead the

text in **Anonymous user consent message for accessing shared files** in **Privacy settings** page, if it is entered, is shown.

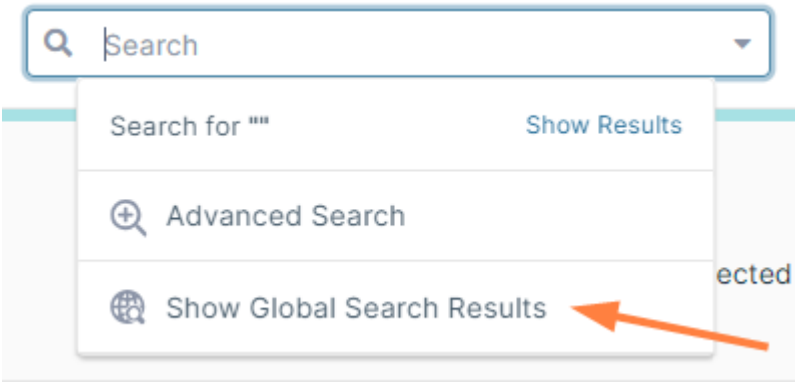
4. Click **Save**.

Set Search Location

By default, basic searches from the user portal header's search bar are performed globally, regardless of where the user has navigated in the folders shown in the main part of the screen.



A setting is available for changing the default search location to the current path shown in the user portal. In the above screen, if the setting were turned on, searches would begin at the **My Files/ Financial** folder.
The setting adds the option **Show Global Search Results** when users click in the Search bar so users still have the ability to search globally:



To set the search to begin from the current path but include the global search option:

1. Open cloudconfig.php at

- Windows: XAMPP DIRECTORY\htdocs\config\cloudconfig.php
- Linux: /var/www/config/cloudconfig.php

2. Add the setting:

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

To return to a global search only:

1. Change the value of **TONIDOCLOUD_START_SEARCHES_ON_CURRENT_NAVIGATION_LOCATION** from **true** to **false**.

```
define("TONIDOCLOUD_START_SEARCHES_ON_CURRENT_NAVIGATION_LOCATION", false);
```

Migrating your data from Varonis DatAnywhere to FileCloud

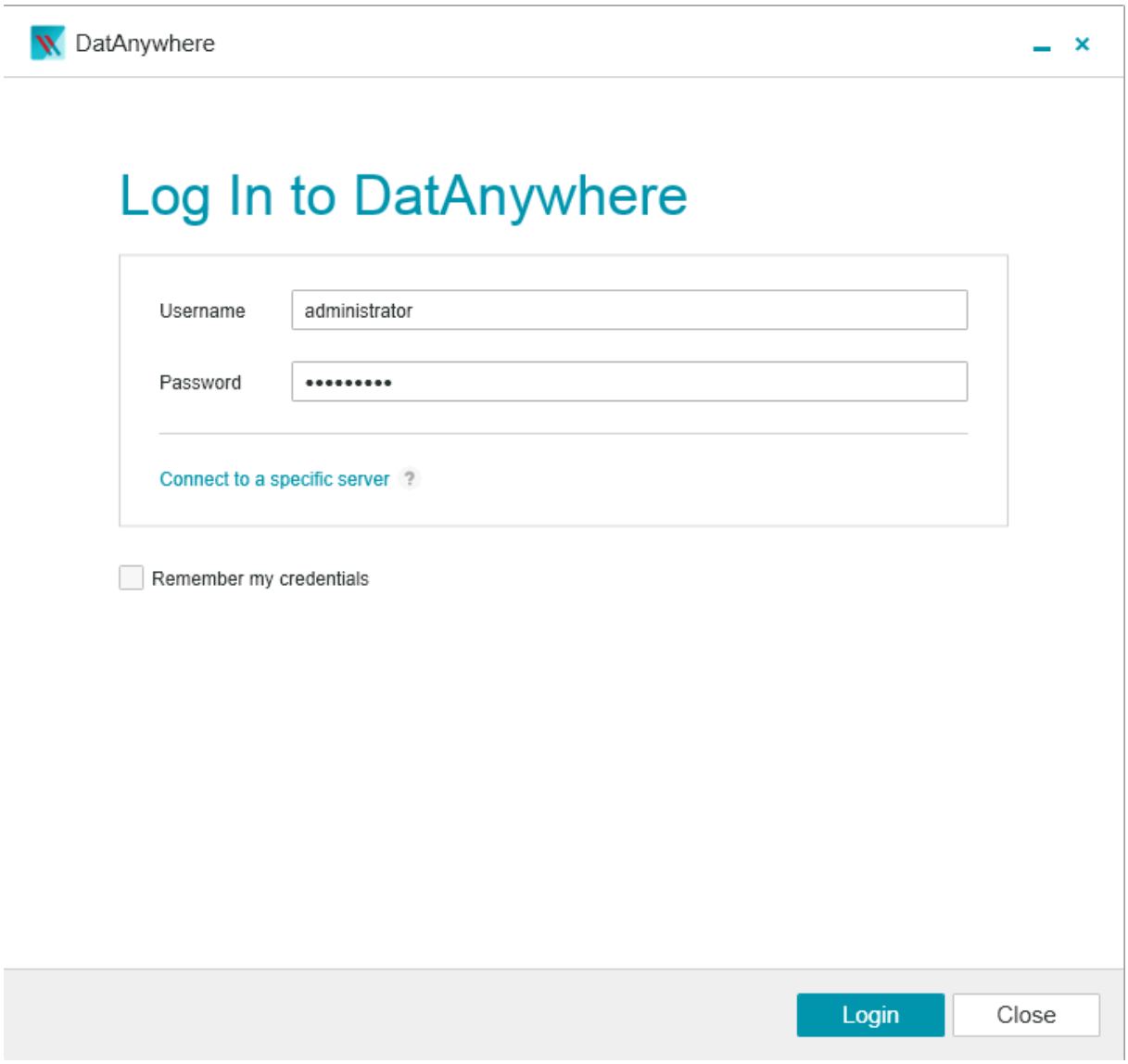
Varonis Datanywhere will enter End of Life (EOL) in February 2020. What does this mean for existing users of Datanywhere? This means no further product development and a limited support from Varonis. It is a suitable time to look for an alternate product which offers more security and support. There may be multiple EFSS solutions similar to Varonis Datanywhere but, FileCloud is the only solution which offers all Datanywhere features and much more. For instance, FileCloud is also an on-premise solution just like Varonis Datanywhere, FileCloud can also be used on Windows Server like Datanywhere allowing use of Windows based network folders and preserve NTFS permissions. FileCloud integrates with Active Directly Credentials so, there is no need to recreate them.

The below guide will assist you towards migrating your data from DatAnywhere to FileCloud in just a few easy steps!

Download your files and folder from DatAnywhere

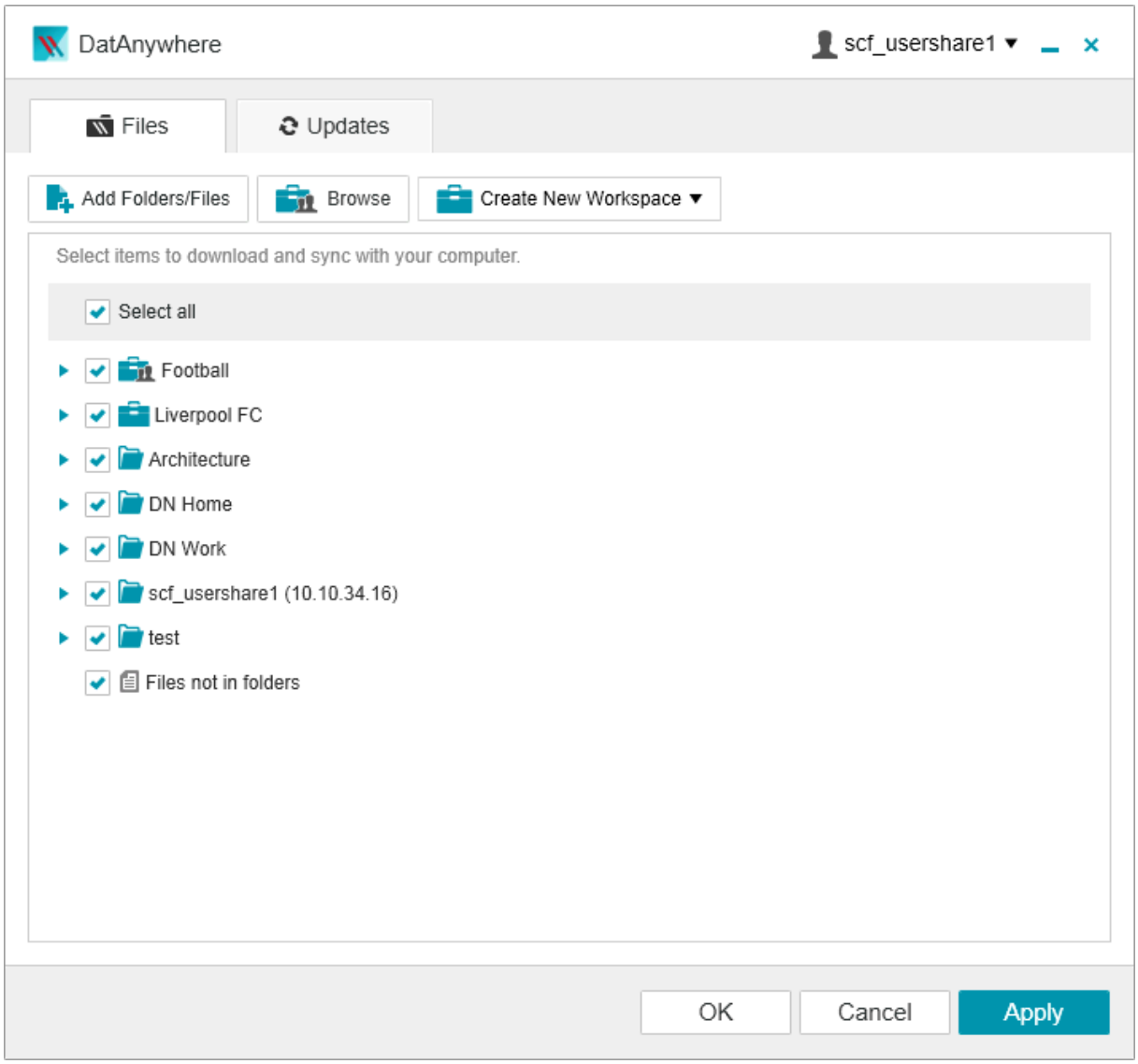
1) To download your files from Varonis DatAnywhere can be done from the Web-client / Web Portal or from Varonis DatAnywhere desktop client which is available for both Mac and Windows.
Once you download and install the desktop client you can login using your Varonis DatAnywhere credentials.

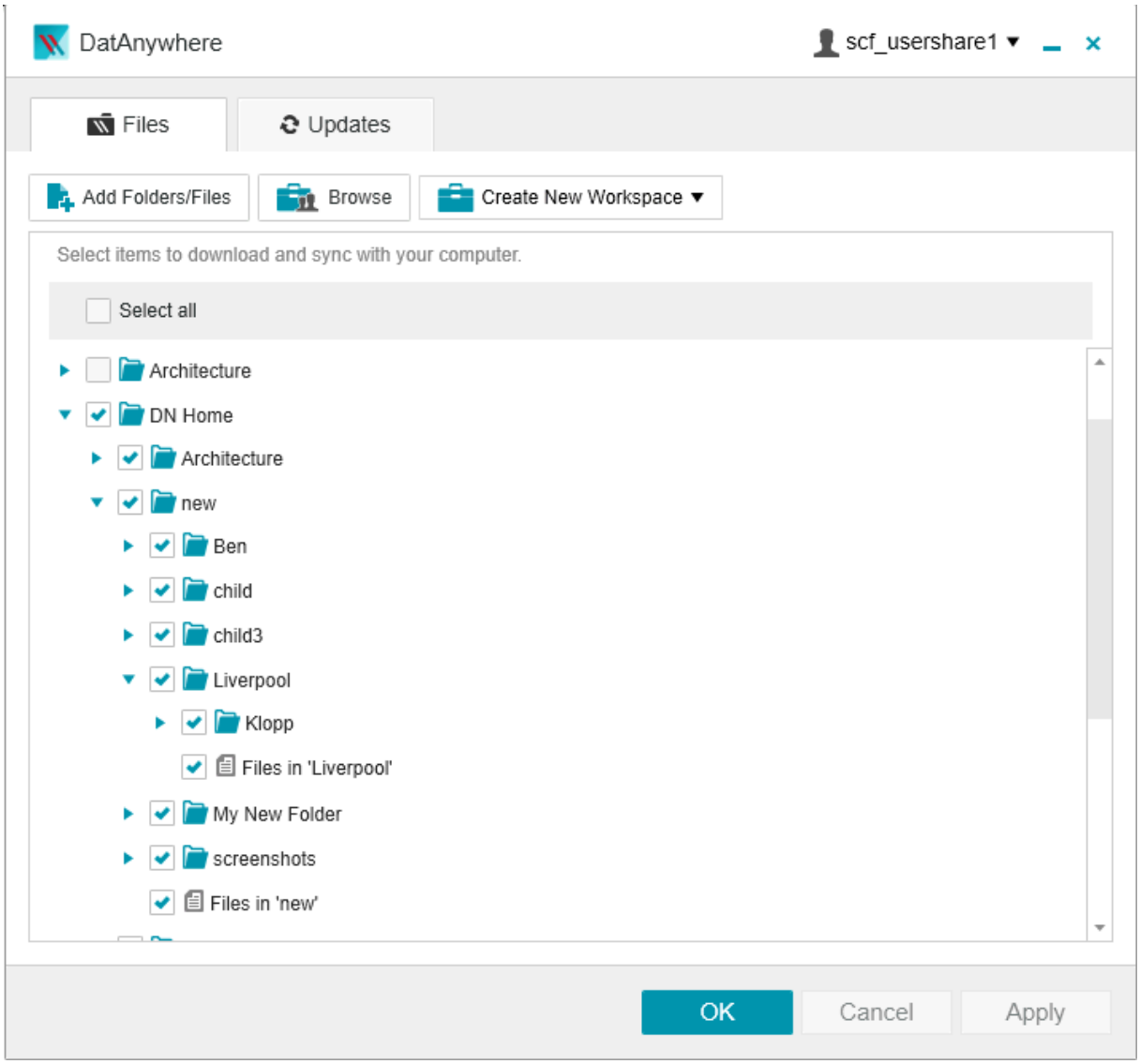
Note: The first time you login to Varonis DatAnywhere client you might be asked to enter your server URL. To obtain such information please contact your system Administrator,



2) Once you have logged in to Varonis DatAnywhere client from your Windows or Mac computer you can select which folders you would like to be sync'ed to your local desktop/computer.
When a specific item is synced, the selected item and all its parent folders are created in your DatAnywhere folder. You can also sync individual files in case you do not wish to download all the folders content.

Upon selecting the files and folders you wish to sync, you can proceed on clicking "Apply"

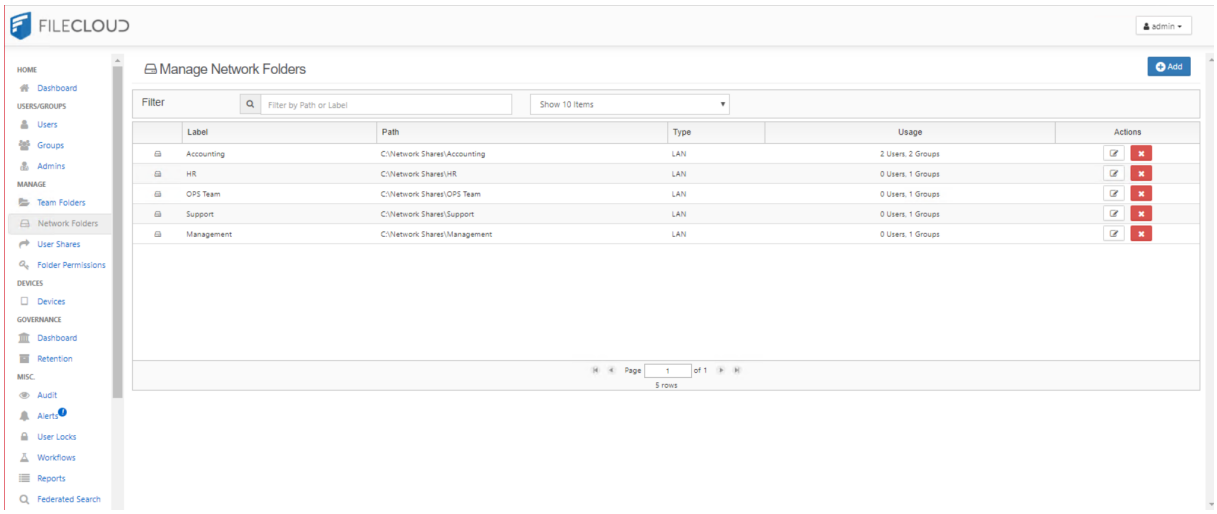

DatAnywhere
scf_usershare1
Files
Updates
Add Folders/Files
Browse
Create New Workspace
Select items to download and sync with your computer.
Select all
Football
Liverpool FC
Architecture
DN Home
DN Work
scf_usershare1 (10.10.34.16)
test
Files not in folders
OK
Cancel
Apply



3) Once your files have completed the Sync/Download process you can access them on your Windows explorer or Mac Finder under the folder DatAnywhere.

Integrate your Network shares with FileCloud!

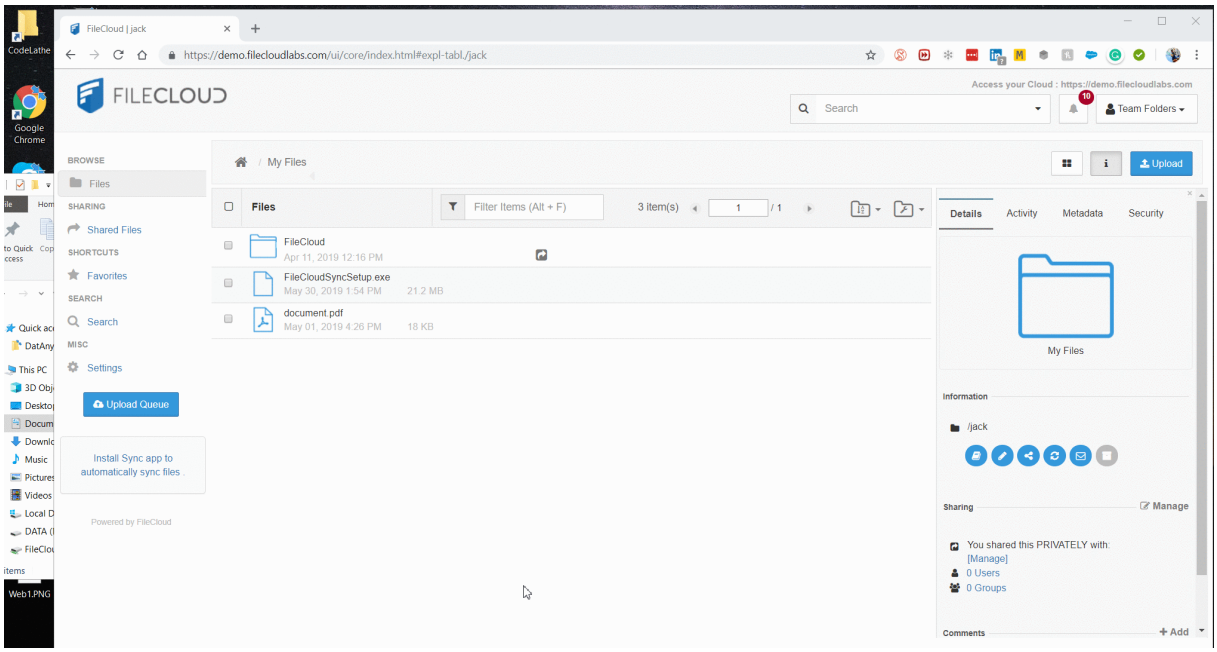
An easy alternative to migrate to FileCloud is to simply integrate your current Network shares to FileCloud.
To accomplish this please see Create a LAN-Based Network Folder.
Once done your users will simply access FileCloud using our desktop clients or from their Web browser to obtain immediate access to all their data!



Migrating your files and folder to FileCloud

Users can upload files by either one of the two methods.

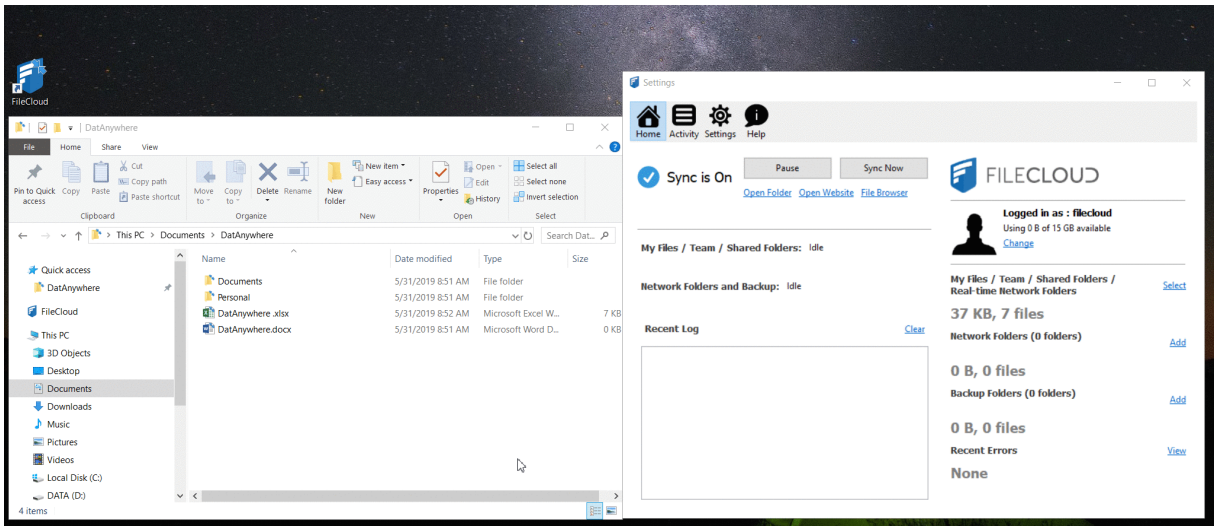
- You can navigate to any folder and click on the "Upload Icon" and select files to upload. You can select multiple files.
- You can also drag and drop files from your desktop into the FileCloud Web Browser window to upload the file.



Migrating your DatAnywhere files and folders using FileCloud's Sync Client

FileCloud offers a variaty of desktop clients to simplfy the way you interact with your files and folders. When migrating your files and folder from Varonis DatAnywhere to FileCloud we recommend that you use our FileCloud Sync client.
FileCloud Sync will securely upload your data to FileCloud in just 3 easy steps.
1) Download FileCloud Sync using the following LINK.
2) Install FileCloud Sync on your computer
3) Login to FileCloud Sync and Open FileCloud's Sync folder.
4) Select and Drag your files/ folders from Varonis DatAnywhere folder into FileCloud's Folder as seen below.

Once done FileCloud Sync will upload your data to FileCloud!



FileCloud Support

If you need assistance to migrate your data please (23.263a) Contact FileCloud Support. Please do keep in mind that FileCloud's support team will not be able to assist you in downloading your data from Varonis DatAnywhere.

If you need assistance downloading your data from Varonis DatAnywhere we kindly ask that you contact your system administrator.

Migrating Content with the Seeding Tool

These instructions should be used only for new installations (or, as shown in the last procedure, for migrating from FileCloud Server to FileCloud Online).

These instructions will not work if you are seeding a system with ServerLink enabled. Contact support.

Initially, when FileCloud is ready for production purposes, you may need to pre-populate the server with files and folders for FileCloud users.

- FileCloud is bundled with a tool to pre-load files and folders before you grant users access.
- These instructions explain how to use the FileCloud Server tool for seeding data into your deployment.

How To Seed Data

1. Enable MongoDB

To use the seeding tool, MongoDB should be enabled and running in PHP CLI mode.

- This may require you to edit the PHP.ini file.
- In Windows, the MongoDB module is already enabled by default.
- If MongoDB is not enabled for PHP CLI mode, the tool will fail.

Enable MongoDB:

In Linux enter:

```
[root@cnfc php.d]# php -m | grep mongodb
mongodb
[root@cnfc php.d]#
```

In Windows enter:

```
C:\Windows\system32>C:\xampp\php\php.exe -m | findstr mongodb
mongodb

C:\Windows\system32>
```

If you do not get the above results, please Contact FileCloud Support.

2. Use the seed command

1. In a command line enter:
   For Windows:

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

   For Linux:

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

   Then, for both Windows and Linux, enter:

```
php  seed.php -h <hostname> -p <from path> -i -d <storagepath> -m <s3inipath> -u
<user> -r --trim-dot
```

   Parameters:
   [required] -h <host> Site host name or 'default' for default site.
   [required] -p <from path> Source path from which files are seeded.
   [optional] -i Seed files. Set this flag to seed files.
   [optional] -d <storagepath> Seed files from source path specified with -p to this existing storage path.
   [optional] -m <s3inipath> Path to migrate.ini. This ini file will be used to migrate existing local storage to S3 storage.
   [optional] -u <user> User whose files are to be imported. File with the user name should exist in the source path. Applicable only with -i.
   [optional] -r Reset existing database. This will reset the databases, so use it with caution.
   [optional] -s Only import files that are not already present in FileCloud for the user to avoid duplicates. (Available in FileCloud 23.261.1 and later).
   [optional] --trim-dot For right-to-left languages, removes periods the tool perceives as being in the wrong position and therefore invalid characters. --trim-dot is a flag; it does not have a value.



The seed command deletes the source files after uploading (unless you are using the -s parameter, and the files are already present in FileCloud).

Seeding Scenarios

Seed files for multiple users without resetting databases

To seed files for multiple users at the same time, prepare a top directory(source path) with separate folders for each user to be seeded with data. Under the user specific folder place files/folders to be seeded for that user.
Run the following command to seed all the users from the prepared source path.

Linux seeding files/folders for multiple users - Default site

```
php seed.php -h default -p /tmp/seedfolder -i
```

The following code shows how to export files for user 'jdoe' from site site21.hostedcloud.com to directory 'cloudexport'.

Windows seeding files/folders for multiple users - Default site

```
php seed.php -h default -p C:\temp\seedfolder -i
```

Note

- If user account exists, seeded files/folders will be imported to those accounts
- If user accounts doesn't exist, user accounts will be created before seeding.

Seed files for multiple users resetting databases

To seed files for multiple users at the same time, prepare a top directory(source path) with separate folders for each user to be seeded with data. Under the user specific folder place files/folders to be seeded for that user.
Run the following command to delete all the existing data and seed from the prepared source path.

Linux resetting and seeding files/folders for multiple users - Default site

```
php seed.php -h default -p /tmp/seedfolder -i -r
```

Windows resetting and seeding files/folders for multiple users - Default site

```
php seed.php -h default -p C:\temp\seedfolder -i -r
```

Note

- All the existing user accounts and its associated data will be deleted before the seeding.
- New user accounts will be created before seeding. Default username and password will be used (i.e password → password)

Seed files for a single user; do not seed files already present in the user's FileCloud account

Windows seeding files/folders for single user - Default site

```
php seed.php -h default -p C:\temp\seedfolder -u jdoe -i -s
```

Note

- Data is seeded for a single user.
- In this case, command expects a folder **jdoe** to exist under the source path.

Seed files into an existing path

To seed files into an existing FileCloud storage path, prepare a top directory(source path) with a single folder under which files/folders to be seeded are placed.
Run the following command to seed the single folder and its contents to an existing FileCloud storage path.

Linux seeding files/folders into an existing storage path - Default site

```
php seed.php -h default -p /tmp/seedfolder -d /jdoe/march
```

Windows seeding files/folders into an existing storage path - Default site

```
php seed.php -h default -p C:\temp\seedfolder -d /jdoe/march
```

Note

- In this case, the command imports a single folder under the source path into the FileCloud storage path **/jdoe/march**. All contents of **seedfolder** are copied to **/jdoe/march**, but the folder **seedfolder** is not copied.

Migrate local storage to S3 storage

The seeding tool can also migrate files from local storage to S3 storage. When the tool is run in this mode, it does the following steps:

1. Checks if AWS CLI is installed on the system running the tool
2. Checks if a valid migration ini file is specified. Look below for the file format.
3. Important: Deletes the existing S3 storage database. If the site was never configured for S3 before, then this should not be an issue.
4. Creates a new S3 storage database and imports the data from local storage database converting it into S3 storage database format on the fly.
5. Creates multiple AWS CLI commands to upload data from the local storage to the S3 bucket. The details of this transfer are generated using the specified ini file.
6. Executes the AWS CLI commands prepared in the previous step.

Run the following command to migrate from local storage to S3 storage

Linux migrating from local storage to S3 storage

```
php seed.php -h default -m /tmp/migrates3.ini
```

Windows migrating from local storage to S3 storage

```
php seed.php -h default -m C:\temp\migrates3.ini
```

S3 migration ini file (sample values)

```
aws_storage_bucket = "company.bucket"
aws_storage_folderprefix = "site1"
aws_access_key_id = "AKIAT4YDRDUSRO863KJJ"
aws_secret_access_key = "stPwbS3Y1KrZGUkVbNcYJx+8S/ZZKFROOjUdG9e9"
aws_region = "us-east-1"
```

Migrate from FileCloud Server to FileCloud Online

If you are migrating to FileCloud Online, the full set of databases has to be exported along with migration. This can be achieved with the following commands.
Linux migrating from local storage to S3 storage

```
php seed.php -h default -m /tmp/migrates3.ini -e /tmp/dbexport
```

Windows migrating from local storage to S3 storage

```
php seed.php -h default -m C:\temp\migrates3.ini -e C:\temp\dbexport
```

Contact FileCloud Support for help with this procedure.

Migrate Local Storage to an Azure Blob Storage Network Folder

Beginning with FileCloud Version 20.2, the seeding tool supports migrating local data to Azure Blob storage.

Run the following command to migrate from local storage to Azure storage:

```
php seed.php -h default -z C:\AzureMigrate\migrate.ini
```

Related help:

Migrating your data from Varonis DatAnywhere to FileCloud

FileCloud Best Practices

In this section:

Deployment

FileCloud Deployment Scenarios

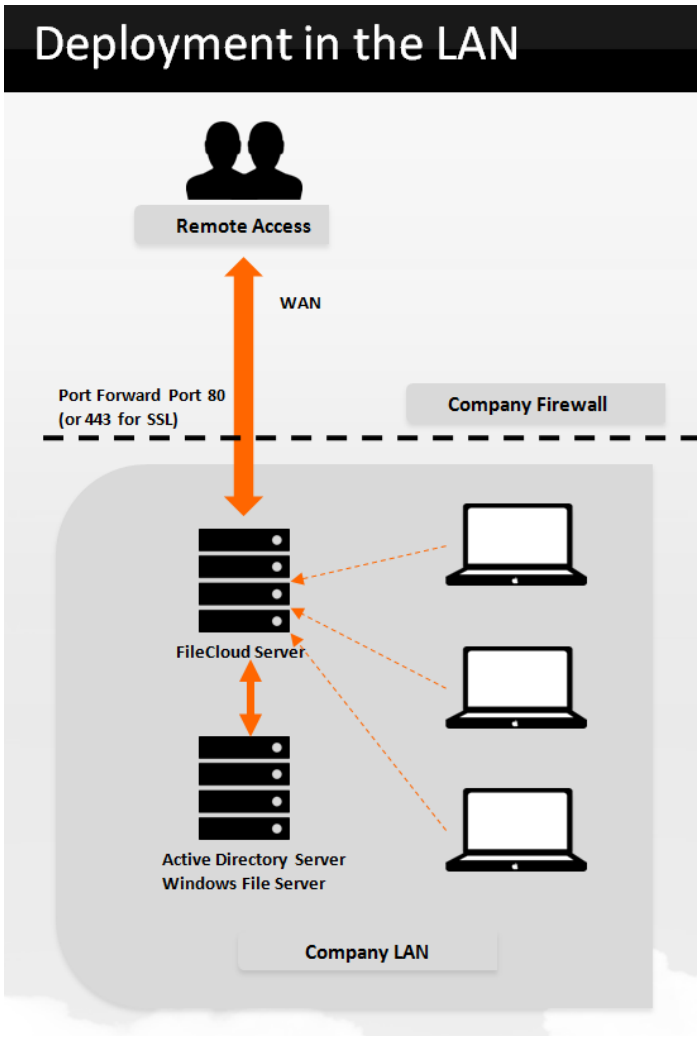
FileCloud can be deployed in several configurations, but we discuss the two most common and recommended ways.



As a best practice, ensure that your outgoing firewall rules are enforced.

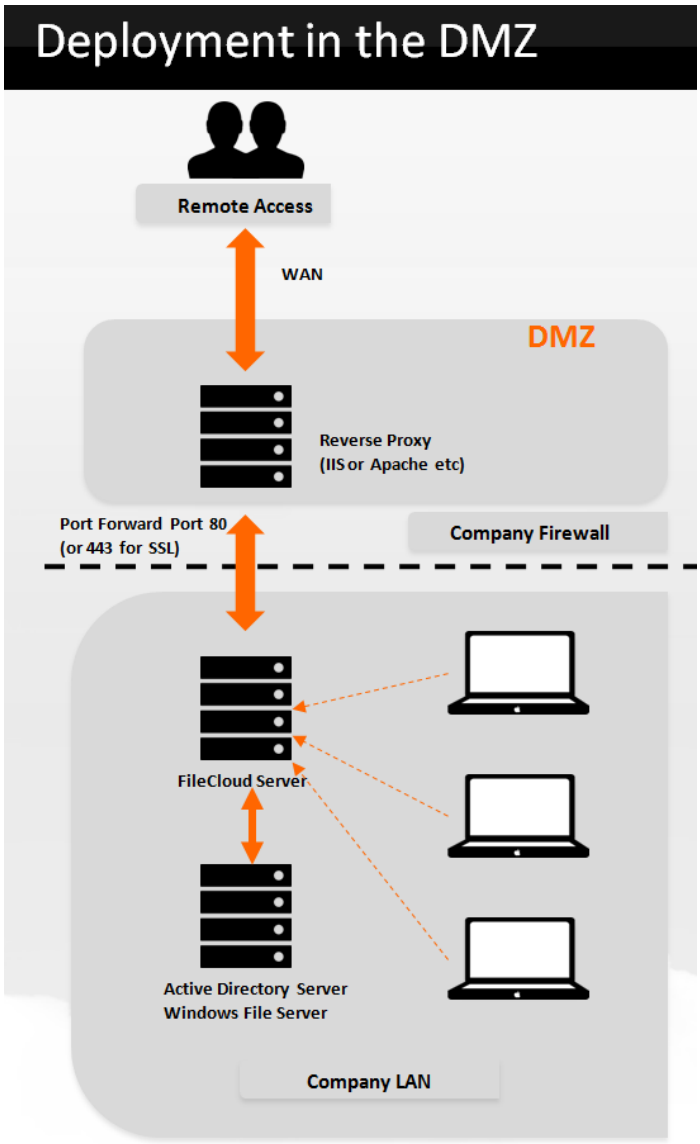
Deployment in the LAN

In this scenario, FileCloud server is deployed directly in the LAN along side the file servers and Windows Active Directory servers. The port 80 or port 443 is then opened and forwarded to the server running FileCloud.



Deployment in the DMZ

In some networks, it might not be possible or desired to open the firewall port directly to a machine on the LAN, in this case, a server running a HTTP reverse proxy (Microsoft IIS, NGINX or Apache and others) in the DMZ outside the LAN can forward HTTP requests to the actual FileCloud server in the LAN.



Performance

Introduction

- Enabling Local Storage File Encryption will affect performance. Consider not using encryption unless absolutely required.
- Use SSD disks for storage for running the Server. It will have significant performance boost.
- Having a large number of CPU cores will help with scaling when there are a lot of incoming requests

Optimizing Mongo Database Performance

- For large databases, MongoDB might require a lot of RAM, so ensure your server running MongoDB has enough RAM.
- Consider using SSD storage to store MongoDB databases
- Consider moving MongoDB to a separate server outside of the webserver node. This might improve performance.

Improving Upload Speeds

There are many factors that can affect upload speeds.

- Your internet connection bandwidth speed
- Where the storage is location (local to the filecloud server or on the network). Local is faster.
- Type of storage (SSD vs Hard Disk) . SSD is fastest.

Improving File Synchronization Speeds

- Use realtime sync for optimum sync performance
- Offline sync of large network folders will be slow and might severely impact server performance when there are lots of users using the system.

Restricting Access To Admin UI Based On IP Addresses

Introduction

Administrators would like to restrict access to admin web UI only for intranet IP addresses or even only when accessed from their PC. Follow these steps, to restrict admin UI access for certain IP addresses.

Steps

1. Stop Apache Server.
2. Edit the following file, based on the OS on which FileCloud server is installed (adjust these paths for your environment).

Operating System	Typical Configuration File Location
Windows	C:\xampp\apache\conf\extra\httpd-filecloud.conf
Ubuntu	/etc/apache2/sites-enabled/000-default.conf

Operating System	Typical Configuration File Location
RHEL	/etc/httpd/conf/httpd.conf

3. Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration.

```
<Location /ui/admin2>
Order deny,allow
deny from all
allow from 192.168.
allow from 33.201.24.69
</Location>
```

4. Restart apache, after making this change. Now admin UI will be accessible only from subnet 192.168.x.x and IP 33.201.24.69.

Old installations which use **http(s)://<your filecloud address>/ui/admin** to restrict access should change this to **http(s)://<your filecloud address>/ui/admin2** and restart Apache for changes to take effect

Restricting Access To User UI Based On IP Addresses

Introduction

Administrators might like to restrict access to user web UI only for intranet IP addresses. If this is the case, please follow these steps to restrict user UI access to certain IP addresses.

Steps

1. Stop Apache Server.
2. Edit the following file, based on the OS on which FileCloud server is installed (adjust these paths for your environment).

Operating System	Typical Configuration File Location
Windows	C:\xampp\apache\conf\httpd.conf
Linux	/etc/apache2/sites-enabled/000-default.conf

3. Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration.

```
      <Location /ui/core>
                  Order deny,allow
                  deny from all
                  allow from 192.168.
                  allow from 33.201.24.69
      </Location>
```

4. Restart apache, after making this change. Now admin UI will be accessible only from subnet 192.168.x.x and IP 33.201.24.69.



Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration for blocking client apps also

```
      <Location />
                  Order deny,allow
                  deny from all
                  allow from 192.168.
                  allow from 33.201.24.69
      </Location>
Restart apache, after making this change. Now filecloud will be
accessible only from subnet 192.168.x.x and IP 33.201.24.69
```

Manage IP Checks

In FileCloud Server, the IP address used when an administrator or user requests data is checked against the IP stored on the session.

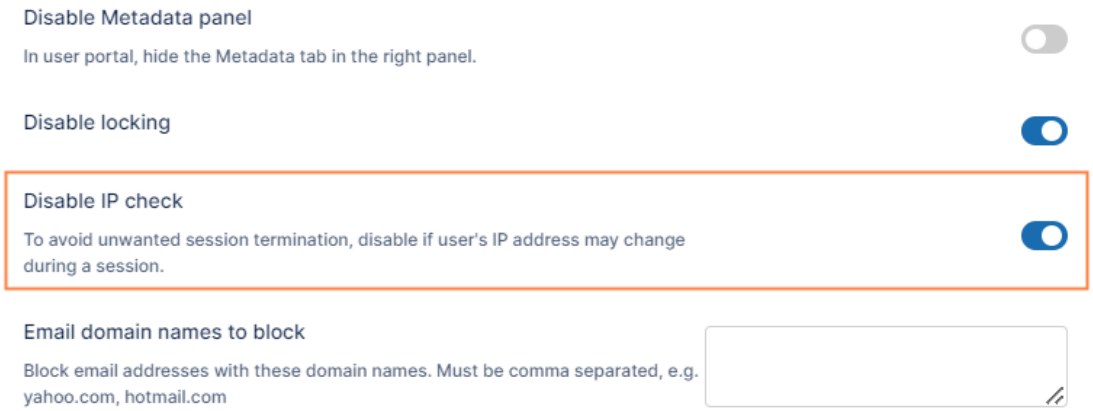
- This means that the session is invalidated if the user IP address changes (the user is automatically logged out).
- For some environments, the IP address change is common and expected.

Now there is a setting labeled **Disable IP Check** that allows an administrator to control this behavior.

- Enable the setting to disable the IP check on every request. This allows you to avoid IP comparison on cookies.
- The use of this option is only recommended if your IP address can change while using the system.

To configure this option:

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. Scroll down to the **Disable IP Check** checkbox, and enable it.



3. Click **Save**.

Changing default config and log directory for FileCloud

Introduction

Out of the box, FileCloud has the configuration and log directories under the WEBROOT. This document discusses how to move these directories to different location.

Changing Config Directory

By default configuration files for FileCloud installation will be under WEBROOT/config. To change this directory, move the WEBROOT/config directory to the new location and then update the WEBROOT/localconfig.php file to notify this change to FileCloud.

Change from: define("TONIDOCLOUD_CONFIG_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."config"); // < VALID config directory path, needs to be read/write by www-data
To:
For Linux: define("TONIDOCLOUD_CONFIG_PATH", "/home/tonidocloud/config"); // < VALID config directory path, needs to be read/write by www-data
For Windows: define("TONIDOCLOUD_CONFIG_PATH", "c:\\tonidocloud\\config"); // < VALID config directory path, needs to be read/write by webserver

Note: As the comment says, the new path should have read/write permissions for the user account that is used to run apache. For instance, www-data in Linux.

Changing Log Directory

By default FileCloud log files will be placed under WEBROOT/scratch. To change this directory, update the WEBROOT/localconfig.php file to notify the new log path to FileCloud.

Change from: define("TONIDOCLOUD_SCRATCH_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."scratch"); // < VALID scratch directory path, needs to be writable by www-data
To:
For Linux: define("TONIDOCLOUD_SCRATCH_PATH", "/home/somenewpath/scratch"); // < VALID directory path, with read-write permission for www-data user
For windows: define("TONIDOCLOUD_SCRATCH_PATH", "c:\\somenewpath\\scratch"); // < VALID config directory path, with read-write permission for the webserver.

Note: As the comment says, the new path should have write permissions for the user account that is used to run apache. For instance, www-data in Linux.

Disable CONNECT Method in HTTP

Introduction

Some security vulnerability scanners might report that your Apache server is vulnerable because CONNECT method is being allowed. For example, a scanner might report:

- CONNECT Method Allowed in HTTP Server Or HTTP Proxy Server Vulnerability
- The HTTP server or the HTTP proxy server accepts the "CONNECT" method.

Following section explains how to disable the CONNECT method on your installation.

Disabling CONNECT Method

There is no inherent vulnerability with the CONNECT method but you should not leave it enabled since it would allow Apache httpd to be used a proxy. This should only be enabled if you intent for Apache httpd to be used as a proxy.

In case of errors like CONNECT Method Allowed in HTTP Server Or HTTP Proxy Server Vulnerability; you will need to disable the connect method in HTTP.

To disable connect method in HTTP, please make the changes in .htaccess file.

Generally, the file location for linux is /var/www/html/.htaccess and for Windows is C:\xampp\htdocs\.htaccess

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^CONNECT
RewriteRule .* - [R=405,L]

The above code will redirect any connect method to 405 method not allowed, which will automatically rejects any connect request with no acknowledgement.

Enforcing TLS 1.2 and TLS 1.3 and Strong Ciphers

Introduction

FileCloud can be configured to use stronger SSL Protocol (TLSv1.2 and 1.3 only) instead of the default protocols. This article shows how to configure FileCloud server and clients to make use of the TLSv1.2 and TLSv1.3 protocols.

Server Configuration

1. In order to enable TLS 1.2 or TLS 1.3 , please edit the httpd configuration file.

OS	Remarks
Windows	Configuration file is located at XAMPPROOT\apache\conf\extra\httpd-ssl.conf For example, if you have installed xampp in c:\, then it will be C:\xampp\apache\conf\extra\http-ssl-conf
Ubuntu	/etc/apache2/sites-enabled/000-default.conf If you use a non-default site, please use appropriate configuration file.

2. Locate the SSLCipherSuite key and change it to
   SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
3. Locate the SSLProtocol key and change it to
   SSLProtocol -all +TLSv1.3 +TLSv1.2
4. This is the highest level of security possible.

Security: Changing a Default Port or Web Server Setting

The ports and Web servers used by FileCloud are normally set during installation. After installation is completed, if you need to, you can change the default listening ports and Web servers.

By default, FileCloud uses these 3 ports:

- **80 (web server)**
- **443 (web server)**

- **27017 (database)**

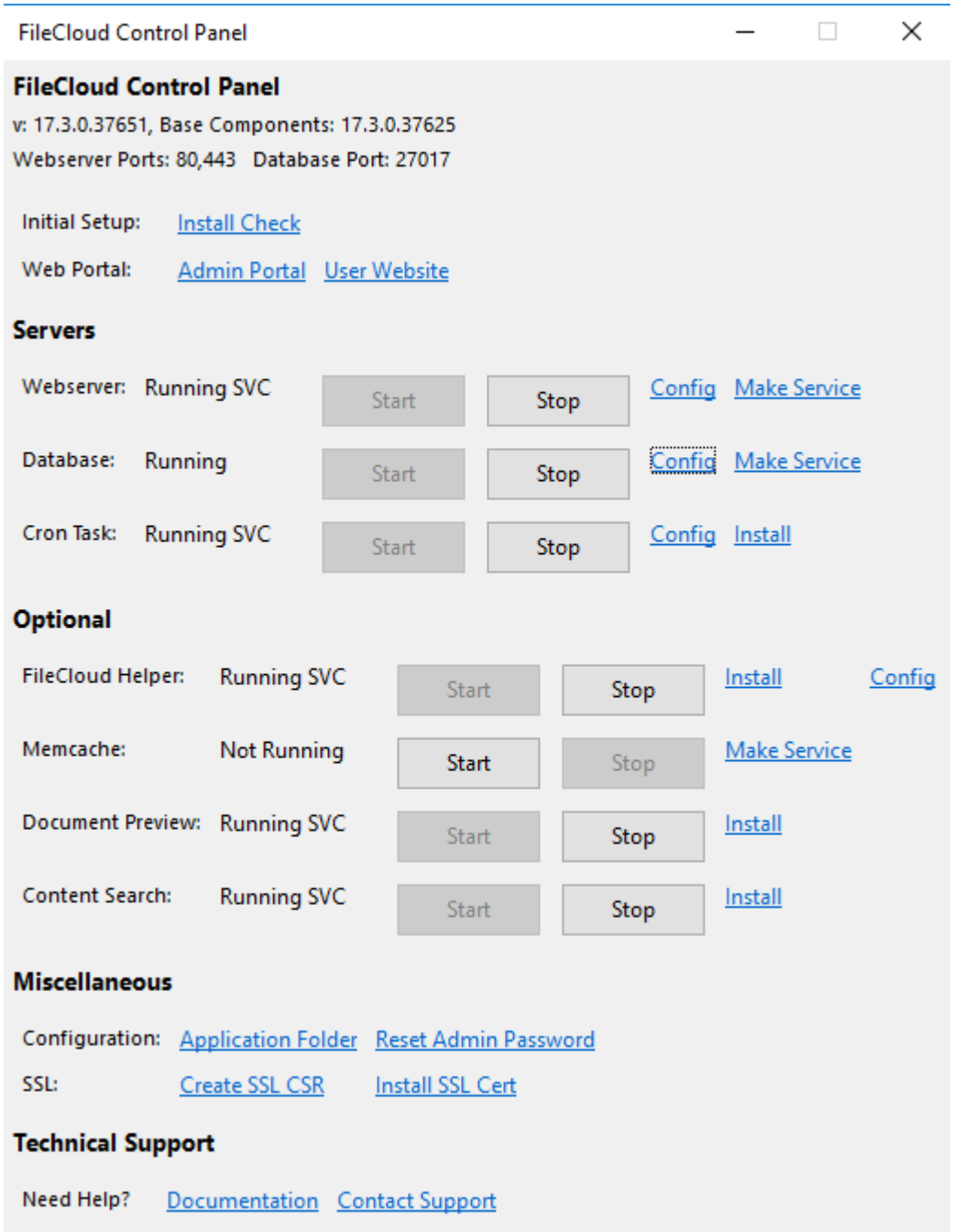
If other programs are using these ports, the FileCloud server will not start up properly.

You might want to change the port numbers or Web servers in some of the following scenarios:

- You need to disable anything that uses port 80 and 443
- You want Apache to run on non standard ports or servers or use firewall rules
- You need to use IIS on standard ports

It is also recommended that you disable HTTP port on the FileCloud server.

To change the ports, open the FileCloud Control Panel.



To change a port or Web server setting:

1. On the server, from the *Windows Start* menu, select the FileCloud Control Panel, or double-click the **xampp/cloudcp.exe** file.
2. In the Servers section, for Webserver, click **Stop**.
3. Change the Port configuration according to HTTPS Best Practices for FileCloud.
4. To start the web server, click **Start** next to **Webserver**.
5. In the **Servers** section, for **Database**, click **Stop**, then **Config**.

6. Make your changes, save them, and next to **Database**, click **Start**.
7. If you have changed the default web server, open **localconfig.php** at:
   Windows Location: **XAMPP DIRECTORY/htdocs/config/localconfig.php**
   Linux Location: **/var/www/config/localconfig.php**
   and add the following, replacing n.n.n.n with the correct IP address.

```
define("TONIDOCLOUD_APACHE_BIND_IP", "n.n.n.n");
```

Security: HTTPS Best Practices for FileCloud

FileCloud recommends that you run all servers in a production environment only on:

- HTTPS (SSL)
- Port 443

This ensures that all communications between clients and FileCloud are completely encrypted.

To access these secured sites, users will have to type in:

https://<SITENAME>

Best Practice	Reason	Steps
Disable the existing HTTP port.	So that FileCloud can be accessed only securely via HTTPS. Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security) Therefore removing the HTTP port completely is the best option. If you must use a redirect, Configure HTTP SSL Redirects.	**To disable HTTP (port 80) for Windows**: 1. Open the webserver config file for editing: `c:\xampp\apache\conf\httpd.conf` and 2. Comment out the line with Listen 80. 3. Save and close the file. 4. Restart the server. **To disable HTTP (port 80) for Linux**: 1. Open the webserver config file for editing: `/etc/apache2/ports.conf` 2. Comment out the line with Listen 80. 3. Save and close the file. 4. Restart the server.

Best Practice	Reason	Steps
Verify your certificates are valid.	If you have an invalid SSL configuration, your users would receive various errors on the browser, and iPhone/iPad apps **cannot preview Office documents**.	You can check the validity of the SSL certificate by testing your install against a SSL certificate checker like https://www.sslshopper.com/ssl-checker.html Provide your FileCloud URL and it will report any potential problems your SSL installation might have. These tools should report no errors for your FileCloud to function properly in SSL mode.

Best Practice	Reason	Steps
Change the default listening port (80).	If you have are conflicts with other ports.	**For Windows**: 1. Open the following file for editing: `c:\xampp\apache\conf\httpd.conf` 2. Locate the following two lines: `Listen 80` `ServerName localhost:80` 3. Change these lines to the following: `Listen your_new_port` `ServerName localhost:your_new_port` 4. Save and close the file. **For Linux**: 1. Open the following file for editing: `/etc/apache2/ports.conf` 2. Locate the following line: `Listen 80` 3. Change it to `Listen Your_new_port` 4. Open the following file for editing: `/etc/apache2/sites-enabled/000-default.conf` 5. Locate the following line `<VirtualHost *:80>` 6. Change it to `<virtualHost _default:your_new_port>` 7. Save and close the file.

Best Practice	Reason	Steps
Change the default HTTPS port (443).	If you have are conflicts with other ports.	**For Windows**: 1. Open the following file for editing: `c:\xampp\apache\conf\extra\httpd-ssl.conf` 2. Locate the following line `Listen 443` 3. Change it to `Listen your_new_port` 4. Locate the following line `<VirtualHost _default_:443` 5. Change it to `<VirtualHost _default_:your_new_port>` 6. Save and close the file. **For Linux**: 1. Open the following file for editing: `/etc/apache2/ports.conf` 2. Locate the following lines `<IfModule mod_ssl.c>Listen 443</IfModule>` 3. Change it to `<IfModule mod_ssl.c>Listen Your_New_Port</IfModule>` 4. Open the following file for editing: `/etc/apache2/sites-available/default-ssl` 5. Locate the following line: `<VirtualHost _default_:443>` 6. Change it to `<VirtualHost _default_:your_new_port>` 7. Save and close the file.

Best Practice	Reason	Steps

Disable server information in headers.	To prevent the Web application from disclosing the server name and server version in the response header.	1. Open the Apache configuration file:
		Ubuntu location: /etc/apache2/apache2.conf
		RHEL location: /etc/httpd/conf/httpd.conf
		Windows location: C:\xampp\apache\conf\httpd.conf
		2. Add the following:
		`ServerSignature Off`
		`ServerTokens Prod`
		3. Restart the Apache server.

HTTP To HTTPS Redirects

It is recommended that you configure FileCloud Server so that it can be accessed securely only via HTTPS.

Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security).

Therefore removing the HTTP port completely is the best option.

If you must use a redirect, add the following lines:

```
<VirtualHost *:80>
 RewriteEngine On
 RewriteCond %{HTTPS} off
 RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
 </VirtualHost>
```

- In Windows, the above lines should we added to file c:\xampp\apache\conf\extra\httpd-vhosts.conf. Restart the apache server.
  Also make sure the following line is uncommented in the file C:\xampp\apache\conf\httpd.conf.

```
# Virtual hosts
Include conf/extra/httpd-vhosts.conf
```

- In Linux, the above lines should be added to the /etc/apache.d/sites-enabled/000-default.conf file. If you already have a VirtualHost directive, add only the lines starting with "Rewrite". Restart the apache server.

Also see: Configure HTTP SSL Redirects

Security: Managing File Extensions

As of Version 23.232.1, FileCloud lists **php**, **php5**, **phar**, **phtml**, **php7**, and **htaccess** as disallowed file extensions. If you are using a version of FileCloud earlier than 23.232, you are advised to add any of these extensions that are not include by default onto the **Disallowed File** list.

For security reasons you may want to restrict uploading of files with specific extensions.

- You can either create a list of file extensions to restrict, or create a list of file extensions to allow.
- If you create an Allowed list of file extensions, then any settings in the Disallowed list will be ignored.
- These restrictions help to prevent users from uploading malicious attachments and viewing them.
- By default FileCloud restricts users from uploading any files with **php** extensions. This is to prevent any code injection.

In FileCloud's **Misc/General** settings you may specify allowed and disallowed file extensions.



Which list should I use? Allowed or Disallowed?

- If you know which file types you don't want to allow and this list is short, you can use the **Disallowed** setting.
- If you want to allow only a few file types to be uploaded, you can use the **Allowed** setting.
- If you create an **Allowed** list of file extensions, then any settings in the **Disallowed** list will be ignored.

What Do You Want to Do?

Allow File Extensions

If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.

- An empty space is defined as a delimiter character followed by no value.

Examples	Description	Impact on Uploading Files
`png | jpg |`	Allow files to be uploaded with an extension of: • png • jpg • *empty*	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group • Any file without an extension (for example, a file named *config*)
`png | jpg`	Allow files to be uploaded with an extension of: • png • jpg	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group

To allow extensions in the Admin Portal:

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. Scroll down until you see the **Allowed File Extensions** box.
3. In the **Allowed File Extensions** box, specify the allowed extensions, using the "|" character to separate each extension.

   Notes:

⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.

⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.



This list of extensions must use the following character as the delimiter:

-
  - '|'
  - For example, to restrict the mp4 and mp3 extensions:
    `mp4|mp3`

Disallow File Extensions

To disallow extensions in the Admin Portal:

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. Scroll down until you see the **Disallowed File Extensions** box.
3. In the **Disallowed File Extensions** box, add the additional restricted extensions.

Notes:
⚠️ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.



This list of extensions must use the following character as the delimiter:

- '|'
- For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions: php|php5|phar|phtml|php7|htaccess|mp3|mp4

Security: Bind MongoDB to 127.0.0.1 Only

For security, MongoDB needs to bind only to 127.0.0.1 network interface (or localhost) so that **only** connections from the local webserver are allowed to connect to it.

The default MongoDB behaviour up to version 2.60 appears to be to bind to all available network interfaces.

We recommend all FileCloud administrators take steps to verify and make the changes to ensure you are running a secure configuration.

For FileCloud running on Windows

1. Open the c:/xampp/mongodb/bin/mongodb.conf
2. Ensure that the following line is in the file, add it in if it is not found.

```
bind_ip=127.0.0.1
```

3. Save the file and restart the MongoDB database.

For FileCloud running on Linux

1. Open the /etc/mongodb.conf (Ubuntu)
2. Ensure that the following line is in the file, add it in if it is not found.

```
bind_ip=127.0.0.1
```

3. Save the file
4. Restart MongoDB

```
sudo /etc/init.d/mongodb restart
```