



FileCloud Server Version 23.232

Storage, HA, Multitenancy, and Document Settings

Copyright Notice

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

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

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

Copyright Notice	2
Storage Settings.....	5
FileCloud Managed Storage	5
Setting Up Network Folders	105
FileCloud High Availability.....	198
Load Balancers.....	198
FileCloud Component: App server node	199
FileCloud Component: MongoDB Replica set.....	199
Deployment Instructions	200
Load Balancer	201
Creating MongoDB Cluster	201
Configuring FileCloud With MongoDB Cluster	204
Set Up Managed Storage	204
Checking the Health of the HA System	206
Other Considerations.....	207
Configure MongoDB Cluster to Use TLS-SSL with Cluster Authentication and Mongoddb Authentication on Linux.....	208
Enable MongoDB Cluster Authentication	214
HaProxy Setup in Ubuntu	218
Installation and Configuration of FileCloud in Webservers	221
Multi-Tenancy Settings.....	223
Multi-Tenancy Requirements	223
Enable Multi-Tenancy Support.....	224
Password encryption and logging in to a multi-tenant admin portal.....	224
Manage Different Sites	225
Enable Email Notifications if Cluster is Down.....	229
Enable Automatic License Renewal and Reporting	232
Document Settings	235




Setting up Content Search for Documents	235
Setting Up Document Preview	273
Enabling Watermarks On Previews	298
Import Files : Pre-seeding	301
Enabling Natural Sort Order Of User List	305
Enabling PDF Merge	306
Optimize PDF Preview.....	307
Managing File Extensions	310
Restricting File Names	315
Manage File Versioning	316
Configuring Zip Files and Zero Trust File Sharing	318

Storage Settings

Administrators can configure settings to control the space needed to get their FileCloud sites running.

With FileCloud, you are using the storage space you have locally in your infrastructure to store files.


- Managed Disk Storage is just a path to 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 allow FileCloud complete control over the management of user content.
- Managed storage can be a path to file systems, a local hard disk, and Storage Area Network (SAN) or Network Attached Storage (NAS) disks.

 <p>Managed Storage</p>	Setting up Managed Disk Storage
 <p>Network Folders</p>	Setting Up Network Folders
 <p>Protecting Your Storage</p>	Enable Antivirus Scanning Set Up Encryption for Managed Storage Create an IAM User Policy for S3 Access


FileCloud Managed Storage

Administrators can configure settings to control how users store data on FileCloud. These options can be set on the various types of storage devices that FileCloud Server supports. This type of FileCloud storage is called **Managed Storage**, and it is displayed to the admin and users as the **My Files** folder.

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, called Managed Disk Storage.

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

- Managed Storage provides FileCloud complete 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 > My Files** 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. Open a browser and log into the Admin portal.
2. On the left navigation panel, under Settings, click **Settings**.
3. Click the **Storage** tab.
4. Type the information into the fields as described below.

Setting	Description
Storage Path	This is the location where all FileCloud user files are stored. Be sure to allow enough options to expand storage in future. Note: Changing this Storage Path after installation and after users have uploaded files has to be done carefully. If 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 number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to 0. NOTE: Versioned files count towards the user's storage quota.
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 "My Files" section, the data will no longer be accessible. Certain functions that depend on My Files will no longer be available.

Setting	Description
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.
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. When unused storage is less than this value, an automatic email notification is sent to the admin. For example, if the value is set to 20, then the admin is notified if more than 80% of managed storage space is used.

5. Click **Save**.
6. Click the **Policies** tab.
7. For each policy that you want to change the default storage settings in:
 1. Click the edit button.
 2. Type the information into the fields as described below:
 3. Click **Save**.
 4. Assign the policy with relevant 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. <i>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.</i>
Store Deleted Files	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 Empty Recycle Bin After Specified 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.

 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);
```


This is useful especially when S3 is used as the managed storage backend.

Setting up FileCloud Managed S3 Storage

As an administrator, you can integrate FileCloud Server to store user data on an Amazon S3 storage server.



- **Amazon Simple Storage Service (Amazon S3) is storage for the Internet.**
- **You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.**
- **You can accomplish these tasks 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 very careful when changing the storage path, if done improperly it could lead to data loss.**
- When changing the storage type from local to Amazon S3, the files and folders that have already been saved to local storage will not automatically be moved 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 then please restart Cron and fcorchestrator (message queue) service.
- The S3 Bucket should NEVER be modified outside of FileCloud subsystem.
- Do not add/edit/modify files directly using S3 tools. Doing so will destabilize your FileCloud installation.

Integrate Amazon S3 Storage

1. Change the Storage Type to S3

NOTE:

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

Windows	Linux (later than Ubuntu 14.04)	Linux (earlier than Ubuntu 14.04)
c:\xampp\htdocs	/var/www/html	/var/www

To enable Amazon 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 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

After you have setup the storage implementation key in step 1, you can configure the following credentials:

Field	Description
S3 Key	This is your amazon authentication key (To get your access key, visit Amazon security portal) . For IAM user, it requires at least the following permissions .
S3 Secret	This is your amazon authentication secret (To get your access key, visit Amazon security portal). For IAM user, it requires at least the following permissions .
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, previously used buckets in FileCloud could be used). 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. <ul style="list-style-type: none"> • This folder will be created automatically.
S3 Region	Optional: Provide the region string. If the region is not provided, then US Standard region will be used. <ul style="list-style-type: none"> • 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 End Point URL	Optional: This is the S3 endpoint. <ul style="list-style-type: none"> • Use this to specify your own S3 endpoint (typically S3 compatible storage) • Use this if it is a unpublished region. <p>To use an AWS end point, it must be one of the values published AWS S3 endpoints</p>

My Files

Network

S3 Compatible Storage Settings (My Files)

S3 Key

S3 account key

S3 Secret

S3 account secret

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

(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 End Point 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

Save Settings

Verify S3 settings and auto-configure any needed S3 configuration

To configure Digital Ocean S3 Credentials

1. Open a browser and log into *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, select *Settings*.

3. On the *Manage Settings* screen, select the *Storage* tab.
4. Type in or select the settings for your environment.
5. Click *Save*.

3. 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 the S3 is setup correctly, a new field called *S3 Encryption* will be available under [Amazon S3 Storage Settings](#).

FileCloud supports the following Server Side Encryption:

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.
Server-Side Encryption with Customer-Provided Keys (SSE-C)	This is a new support available from FileCloud v15 on-wards. The data will be encrypted using customer supplied 32 bit encryption key. This option will have SLOWER performance due to restriction on how this data can be decrypted (Amazon server will NOT be able to decrypt the data and the data has be first downloaded to FileCloud server and decrypted). The data will NOT be accessible via S3 console as well.

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:

<p>⚠ If you are not running the current version of FileCloud Server:</p> <p>You must enable an additional extension in the php.ini file</p>	<ol style="list-style-type: none"> 1. On the FileCloud server, open the following file for editing: <div data-bbox="902 312 1453 401" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">WEBSITE\php\php.ini</div> 2. Add the following line to the file: <div data-bbox="902 464 1453 552" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">extension=php_com_dotnet.dll</div> 3. Save your changes and close the file. 4. Restart the Apache server.
<p>⚠ If you are running FileCloud Server on Windows AND</p> <p>Your xampp folder is installed in a location other than c:\xampp</p> <p>You must add a key to the cloudconfig.php file</p> <ul style="list-style-type: none"> • For example, if your xampp folder is in D:\xampp\htdocs\config\cloudconfig.php • Then you would add the following line: <code>define("PHPBIN_PATH","D:\\xampp\\php\\php.exe");</code> 	<ol style="list-style-type: none"> 1. On the FileCloud Server, open the following file for editing: <div data-bbox="902 753 1453 905" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"><your xampp folder>\htdocs\config\cloudconfig.php</div> 2. Add the following line anywhere: Replacing <i><location></i> with your path to the xampp folder <div data-bbox="902 1031 1453 1150" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;">define("PHPBIN_PATH","<location>:\xampp\php\php.exe");</div> 3. Save your changes and close the file.

Then:

The screenshot shows a dialog box titled "Manage S3 Encryption". It has a close button (X) in the top right corner. Below the title bar, there are two fields: "Encryption Status" with the value "Encryption is disabled" and "Encryption Type" with a dropdown menu showing "Amazon S3-Managed Key Encryption". Below these fields is a light blue note box with the text "1. Files are currently not encrypted". At the bottom right of the dialog, there are two buttons: "Enable encryption" (with a lock icon) and "Close".

1. Open a browser and log into *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, select the *Storage* tab.
4. On the *Storage* tab, click *Manage*.
5. On the *Manage S3 Encryption* dialog, in *Encryption Type*, select *Amazon S3*.
6. Click *Unencryption*.

Upload large files on an Amazon S3 storage server

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

KEY	VALUE	Description
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:

- Open the following file:
 - Windows: C:\xampp\htdocs\.htaccess
 - Linux: /var/www/html/.htaccess
- 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 AmazonS3 share object storage cannot be edited using a text editor, you can use a workaround to correct this.

Workaround:

- Change the Header set in the Content-Security-Policy
- 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:

- Open a command-line prompt.
- 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



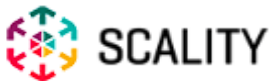
FileCloud officially supports only Amazon S3 storage.

- 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
- The robustness 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.

Click on the logo for the storage service you want to integrate with FileCloud:



How to Integrate FileCloud with Alibaba Cloud Object Based Storage

-  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
 - Scalify

- Wasabi
- Google Cloud object storage
- Backblaze B2
- Cloudian S3-Compatible Object Storage
- The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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
<code>c:\xampp\htdocs</code>	<code>/var/www/html</code>

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. 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.

Server **Storage** Authentication Admin Database Email Endpoint Back

My Files Network

S3 Compatible Storage Settings (My Files)

S3 Key

S3 account key

S3 Secret

S3 account 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

(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 End Point 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

5. 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.

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:

- Open the following file:
 - Windows: C:\xampp\htdocs\.htaccess
 - Linux: /var/www/html/.htaccess
- 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



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
 - Scalify
 - Wasabi
 - Google Cloud object storage
 - Backblaze B2
 - Cloudian S3-Compatible Object Storage
- The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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. Open a browser and log into the Admin Portal.
2. Go to **Settings > Storage > My Files**.

3. Enter the settings for your environment. See the table below for information about each setting.

S3 Compatible Storage Settings (My Files)

S3 Key	<input type="password" value="....."/>	
	<small>S3 account key</small>	
S3 Secret	<input type="password" value="....."/>	Reset to Defaults
	<small>S3 account secret</small>	
Use IAM role	<input type="checkbox"/>	
S3 Bucket Name	<input type="text" value=""/>	
	<small>(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.</small>	
S3 Storage Folder	<input type="text" value=""/>	
	<small>(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.</small>	
S3 Region	<input type="text" value="us-east-1"/>	
	<small>(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</small>	
S3 End Point URL	<input type="text" value=""/>	
	<small>(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</small>	
Save Settings	Save S3 Settings	
	<small>Verify S3 settings and auto-configure any needed S3 configuration</small>	
Number of old versions to keep for each file	<input type="text" value="5"/>	
	<small>Can be set to -1 to turn off versioning and prevent overwrite</small>	
S3 Encryption	Manage	
	<small>Manage encryption of data stored in S3 storage</small>	

4. Click **Save S3 Settings**.

- 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.
- 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. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> Endpoint: s3.us-west-004 </div>
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 , each upload of a file overwrites the previous one, and no versions are saved.
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.

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.

- 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:	[REDACTED]
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](#)

✕

Add Application Key

Name of Key:
(keyName)

Allow access to Bucket(s):
(optional)
(bucketName)

All
▼

Type of Access:
(optional)
(capabilities)

Read and Write

Read Only

Write Only

File name prefix:
(optional)
(namePrefix)

Allow access to file names that start with this.

Duration (seconds):
(optional)
(validDurationSeconds)

Positive integer less than 1000 days (in seconds).

Create New Key

Cancel

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



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
- The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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. Log into the admin portal.
2. Go to **Settings > Storage > My Files**.

3. Enter the settings for your environment.

Server **Storage** Authentication Admin Database Email Endpoint Back

My Files Network

S3 Compatible Storage Settings (My Files)

S3 Key

S3 account key

S3 Secret

S3 account 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

(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 End Point 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

4. 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.

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:

- Open the following file:
 - Windows: C:\xampp\htdocs\.htaccess
 - Linux: /var/www/html/.htaccess
- 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

-  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
 - The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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:

- To make sure that your server does not have any time variations, set up the time on your server to be synchronized.
 - [Configure an authoritative time server in Windows Server](#)
 - [Synchronize Time with NTP in Linux](#)
- Open the following file for editing:

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

- Find the following line:

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

- Change it to:

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

- Save and close the file.
- Find the following file:

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

- 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

- Open a browser and log into the Admin Portal.

- Go to **Settings > Storage > My Files**.
- Type in or select the settings for your environment. See the table below for information about each setting.

S3 Compatible Storage Settings (My Files)

S3 Key	<input type="text" value="....."/>	
	<small>S3 account key</small>	
S3 Secret	<input type="text" value="....."/>	Reset to Defaults
	<small>S3 account secret</small>	
Use IAM role	<input type="checkbox"/>	
S3 Bucket Name	<input type="text" value=""/>	
	<small>(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.</small>	
S3 Storage Folder	<input type="text" value=""/>	
	<small>(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.</small>	
S3 Region	<input type="text" value="us-east-1"/>	
	<small>(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</small>	
S3 End Point URL	<input type="text" value=""/>	
	<small>(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</small>	
Save Settings	Save S3 Settings	
	<small>Verify S3 settings and auto-configure any needed S3 configuration</small>	
Number of old versions to keep for each file	<input type="text" value="5"/>	
	<small>Can be set to -1 to turn off versioning and prevent overwrite</small>	
S3 Encryption	Manage	
	<small>Manage encryption of data stored in S3 storage</small>	

- Click **Save S3 Settings**.
- 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.

6. 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 , each upload of a file overwrites the previous one, and no versions are saved.N
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.

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.

The screenshot shows the Google Cloud Platform interface. The top navigation bar is blue with the Google Cloud Platform logo and a hamburger menu icon. Below the navigation bar, there is a sidebar on the left with a 'Storage' section containing icons for 'Browser', 'Transfer', 'Transfer Appliance', and 'Settings'. The 'Settings' option is highlighted. The main content area is titled 'Settings' and has two tabs: 'Project Access' and 'Interoperability'. The 'Interoperability' tab is active. The text under this tab explains that the Interoperability API allows for HMAC authentication and interoperability with other cloud storage systems. It notes that the API is enabled per project member and that each member can set a default project and maintain their own access keys. There are two sub-sections: 'Request endpoint' which provides instructions on changing the request endpoint to use the Cloud Storage URI (https://storage.googleapis.com) and a 'Learn more' link; and 'Default project for interoperable access' which states that the default project is used for all create bucket and list bucket requests.

The screenshot shows the 'Access keys for your user account' page. It features a table with two columns: 'Access key' and 'Secret'. The 'Access key' column contains a blurred key. The 'Secret' column contains a blurred secret with a copy icon and a trash icon. Below the table, there is 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

-  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
 - The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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. Open a browser and log into admin portal.
2. In the left navigation panel, click **Settings**.
3. On the **Manage Settings** screen, select **Storage > My Files**.

4. Type in or select the settings for your environment. See the table below for information about each setting.

Server **Storage** Authentication Admin Database Email Endpoint Back

My Files Network

S3 Compatible Storage Settings (My Files)

S3 Key

S3 account key

S3 Secret

S3 account 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

(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 End Point 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

5. 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.

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

-  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
 - The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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. 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.

S3 Compatible Storage Settings (My Files)

S3 Key	<input type="password" value="....."/>	
	S3 account key	
S3 Secret	<input type="password" value="....."/>	Reset to Defaults
	S3 account secret	
Use IAM role	<input type="checkbox"/>	
S3 Bucket Name	<input type="text" value=""/>	
	(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.	
S3 Storage Folder	<input type="text" value=""/>	
	(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	<input type="text" value="us-east-1"/>	
	(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 End Point URL	<input type="text" value=""/>	
	(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	
Save Settings	Save S3 Settings	
	Verify S3 settings and auto-configure any needed S3 configuration	
Number of old versions to keep for each file	<input type="text" value="5"/>	
	Can be set to -1 to turn off versioning and prevent overwrite	
S3 Encryption	Manage	
	Manage encryption of data stored in S3 storage	

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 , each upload of a file overwrites the previous one, and no versions are saved.
S3 Encryption	Select No encryption because Wasabi does not support managed key encryption.

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:

- Open the following file:
 - Windows: C:\xampp\htdocs\.htaccess
 - Linux: /var/www/html/.htaccess
- 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

-  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
 - The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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. Open a browser and log into the admin portal.
2. Go to **Settings > Storage**.

3. Enter the settings for your environment. See the following table for information about each setting.

S3 Compatible Storage Settings (My Files)

S3 Key	<input type="text" value="....."/>	
	<small>S3 account key</small>	
S3 Secret	<input type="text" value="....."/>	Reset to Defaults
	<small>S3 account secret</small>	
Use IAM role	<input type="checkbox"/>	
S3 Bucket Name	<input type="text" value=""/>	
	<small>(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.</small>	
S3 Storage Folder	<input type="text" value=""/>	
	<small>(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.</small>	
S3 Region	<input type="text" value="us-east-1"/>	
	<small>(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</small>	
S3 End Point URL	<input type="text" value=""/>	
	<small>(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</small>	
Save Settings	Save S3 Settings	
	<small>Verify S3 settings and auto-configure any needed S3 configuration</small>	
Number of old versions to keep for each file	<input type="text" value="5"/>	
	<small>Can be set to -1 to turn off versioning and prevent overwrite</small>	
S3 Encryption	Manage	
	<small>Manage encryption of data stored in S3 storage</small>	

4. 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 , each upload of a file overwrites the previous one, and no versions are saved.
S3 Encryption	Select No encryption because Cloudian does not support managed key encryption.

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; 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"
```


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 now supports FIPS licenses in version 18.2 and later. Enterprises who are subject to the FIPS regulations must install and run a FIPS-enabled operating system. For example, CentOS in FIPS mode.

When using a FIPS-enabled license, FileCloud Admins will see in the Admin Portal:

 - Running in FIPS mode is prominently displayed
 - SSO features are hidden
 - Storage encryption option is always shown

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](#)

FileCloud Blogs

- [Enable FIPS Encryption in FileCloud](#)

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

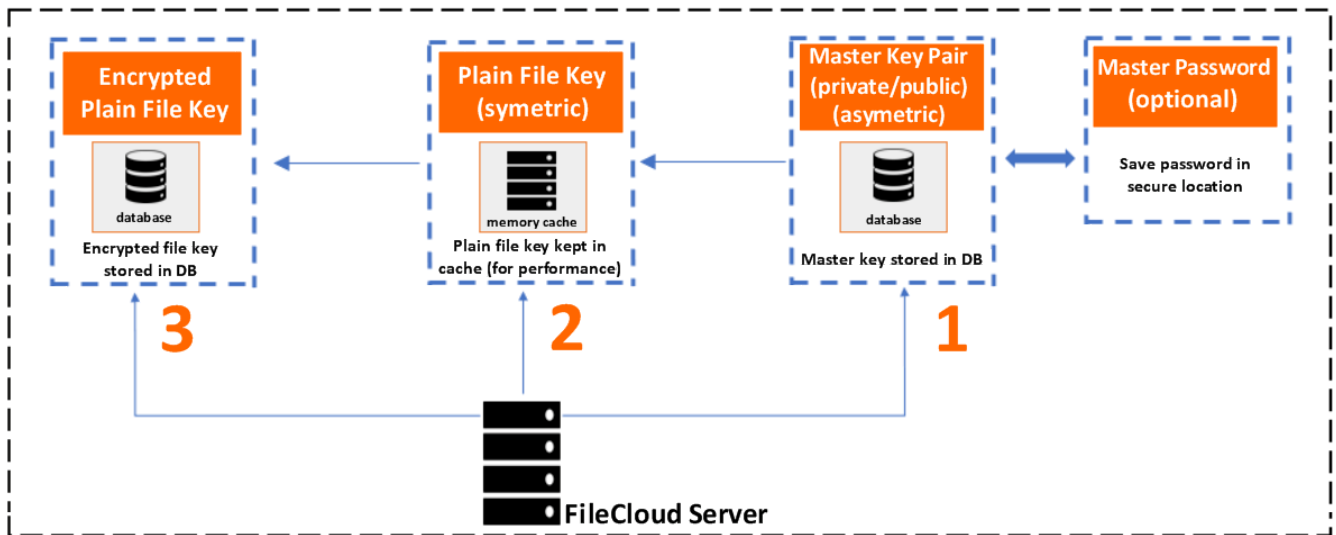


Warning On Master Password

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	<ul style="list-style-type: none"> Asymmetric 4096 bits RSA sha512 digest 	Password (optional)	Both private and public keys are persisted	<ul style="list-style-type: none"> It is important to save the password (if one was provided)

Key	Key Details	User Input	Persistence	Remarks
Plain File Key	<ul style="list-style-type: none"> • Symetric • AES • 128 bits 	None	Not persisted	<ul style="list-style-type: none"> • 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
Encrypted File Key	<ul style="list-style-type: none"> • Encrypted using master public key 	None	Encrypted file key is persisted	<ul style="list-style-type: none"> • 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 <p> Whenever you restart the server, the encrypted file key is decrypted again.</p>

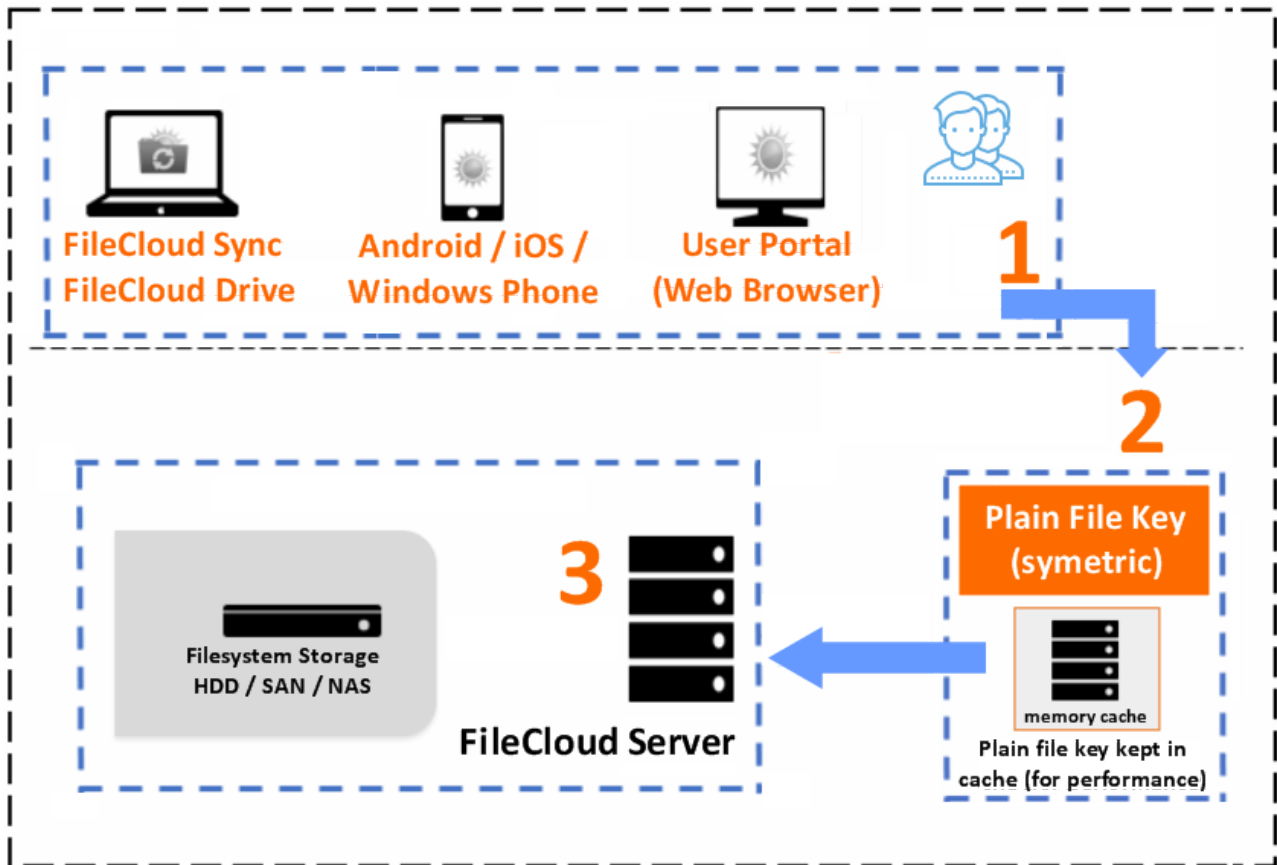
When are Files Encrypted?

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?

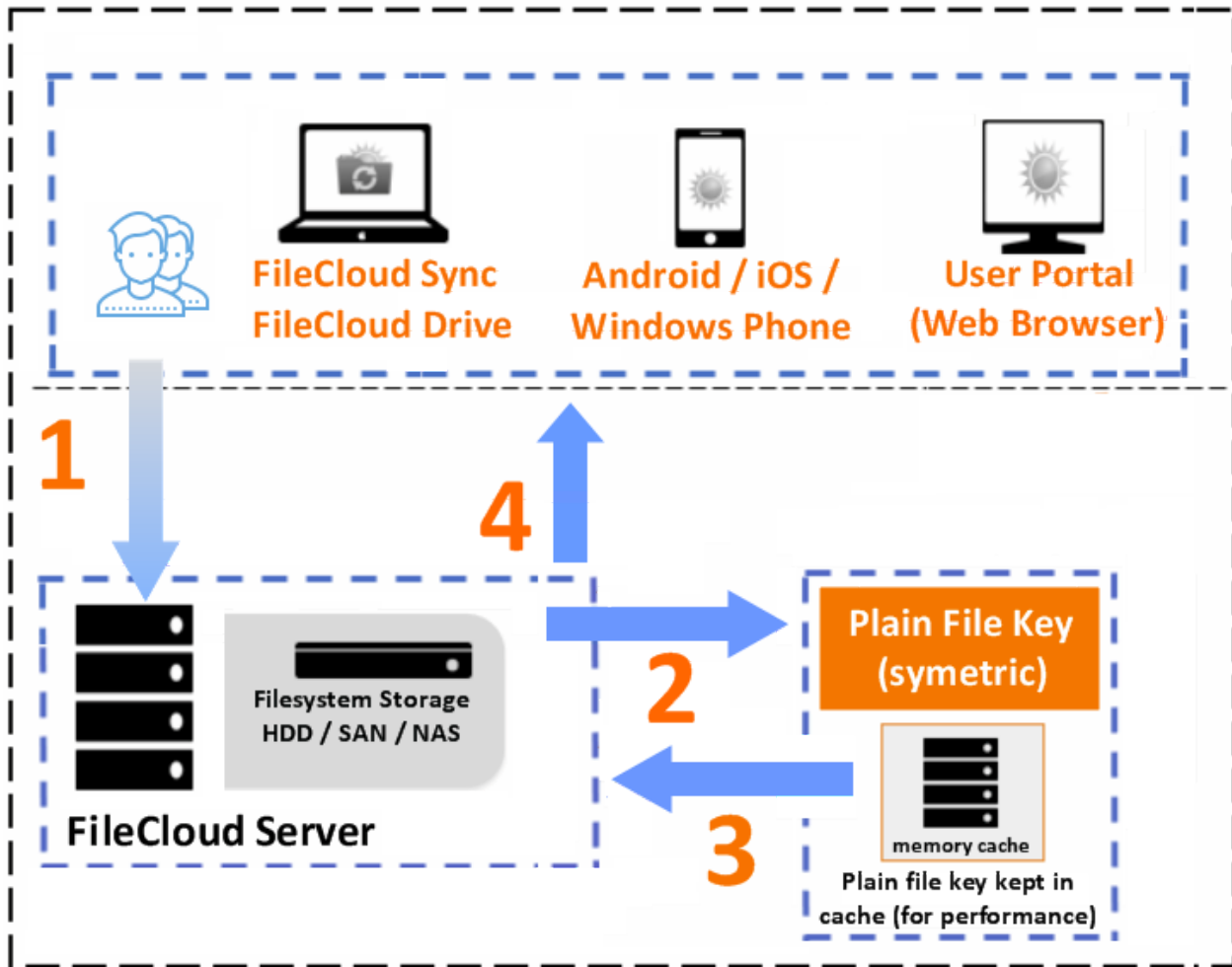
Storage decryption will occur without notifying the end user.

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 in FileCloud Server version 19.1 and later.

As an administrator, you can encrypt managed disk 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:

Requirements	
Required	Memcached installation
Only required if default path for openssl.cnf has been changed.	<p>Set your 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</p> <p>Windows: XAMPP_HOME\php\extras\ssl\openssl.cnf Linux: /etc/ssl/openssl.cnf</p> <p>In Windows, for example, if you have XAMPP installed in D:\xampp, then add the following line to cloudconfig.php.</p> <pre>define("SSL_CONF_FILE", "D:\xampp\php\extras\ssl\openssl.cnf");</pre>

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("TONIDO_CLOUD_FIPS140_ENABLED", 1);
- 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_INCLUDE ENCRYPTION	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.



Master Password

If an optional master password is specified, then retain the password for future use.
Without this password the encryption module cannot encrypt or decrypt files in FileCloud storage.

To manage encryption:

1. Open a browser and log in to the admin portal.
2. From the left navigation pane, under **SETTINGS**, select **Settings**.
3. Select the **Storage** tab and then the **My Files** sub-tab.

4. An **Encryption** option now appears.

The screenshot displays the 'Storage' configuration page in the FileCloud Server interface. The navigation menu at the top includes 'Server', 'Storage', 'Authentication', 'Admin', 'Database', 'Email', 'Endpoint Backup', 'License', and 'Policies'. Below this, there are sub-menus for 'Team Folders', 'Third Party Integrations', 'ServerLink', 'Misc', and 'Reset'. The main content area is titled 'My Files Storage Settings' and contains several configuration options:

- Storage Path:** A text input field containing 'c:\clouddata' with a 'Check Path' button to its right. Below the field, instructions specify that the location must be writable by the webserver, with examples for Windows and Linux. A red note states: '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:** A text input field containing the value '3'. A note below indicates it can be set to -1 to turn off versioning.
- Encryption:** A dropdown menu currently set to 'No Encryption' with a 'Manage' button to its right. An orange arrow points to this option.
- Disable My Files:** A checkbox that is currently unchecked, with a note 'Disable 'My Files' [Managed Storage]'.
- User Storage Usage Calculation:** A dropdown menu set to 'Exclude Shares'.

At the bottom of the page, a table is partially visible with columns for 'File Maximize Exp' and 'Units'.

5. To open the **Manage Storage Encryption** screen, click **Manage**.

Manage Storage Encryption
✕

Encryption Status No Encryption

Encryption is not enabled. Files are stored as-is.

Encryption Password Enter Encryption Password

Encryption Password (Repeat) Re-enter Encryption Password

Create recovery key

Create optional recovery key, in case encryption password is lost.

Note

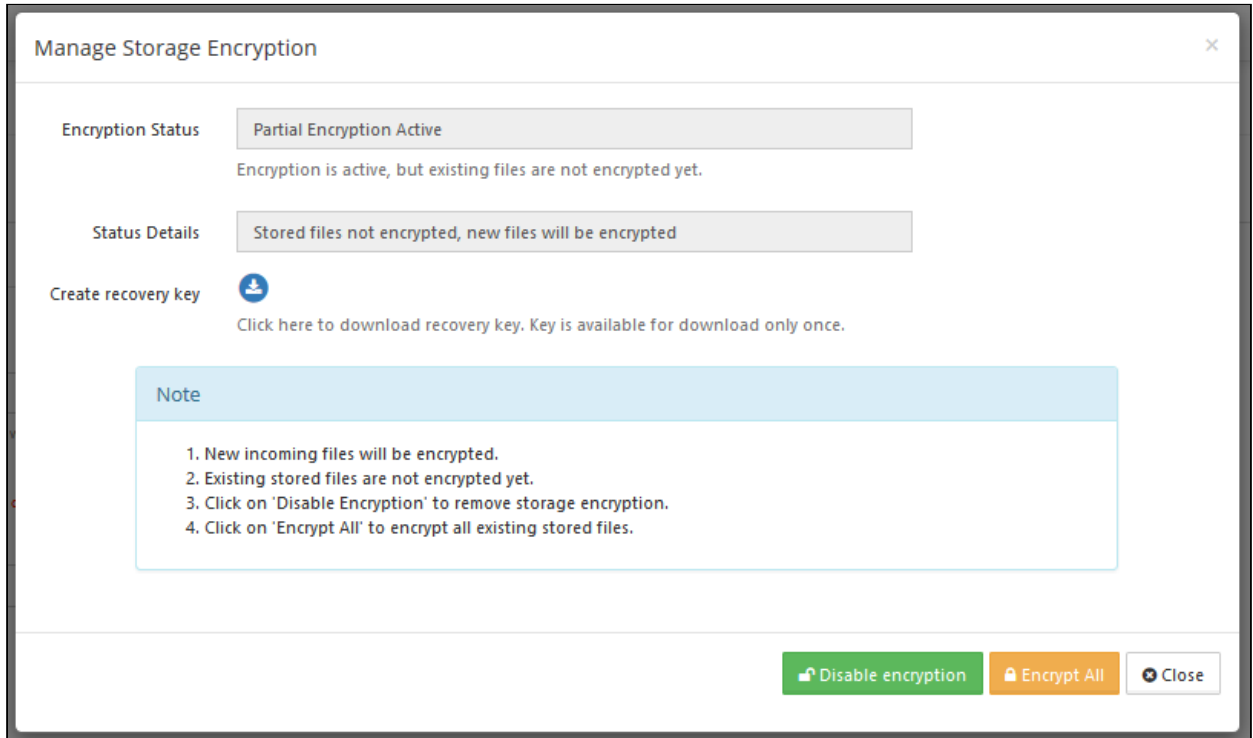
Encryption password is optional to enable encryption. If an encryption password is used:

1. Password has to be entered everytime server starts
2. If password is lost, files cannot be recovered
3. Memcache server is a necessary requirement.

🔒 Enable encryption
✕ Close

- ⚠️ You can set an optional password
- When you set a password while enabling encryption, you may create a recovery key.
 - This recovery key is a private key file, which 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 only once for download.**
- Once the recovery key is downloaded, the option to download it is not shown again.


6. To set an optional password, in **Encryption Password**, type in a strong password.
7. To perform the necessary initialization of the encryption module, click **Enable Encryption**.



Manage Storage Encryption ✕

Encryption Status Partial Encryption Active
Encryption is active, but existing files are not encrypted yet.

Status Details Stored files not encrypted, new files will be encrypted

Create recovery key 
Click here to download recovery key. Key is available for download only once.

Note

1. New incoming files will be encrypted.
2. Existing stored files are not encrypted yet.
3. Click on 'Disable Encryption' to remove storage encryption.
4. Click on 'Encrypt All' to encrypt all existing stored files.

🔒 Disable encryption 🔒 Encrypt All ✕ Close

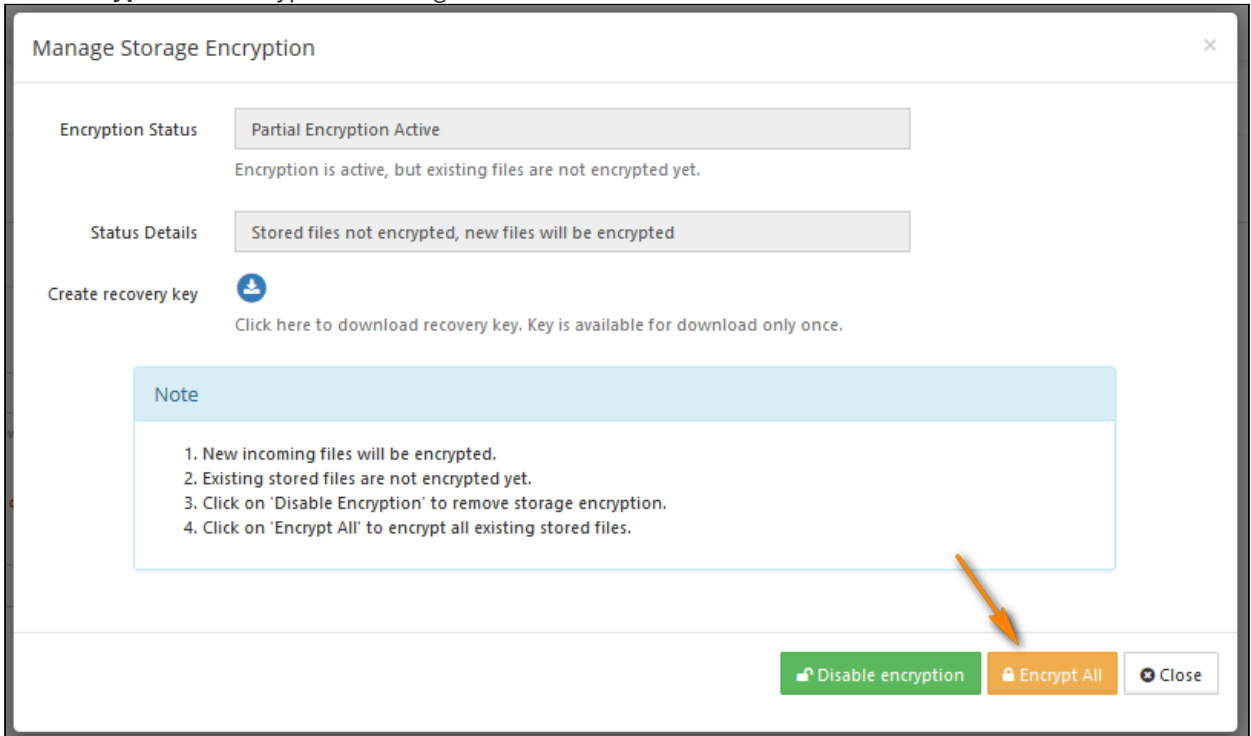
4. Encrypt any existing files

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

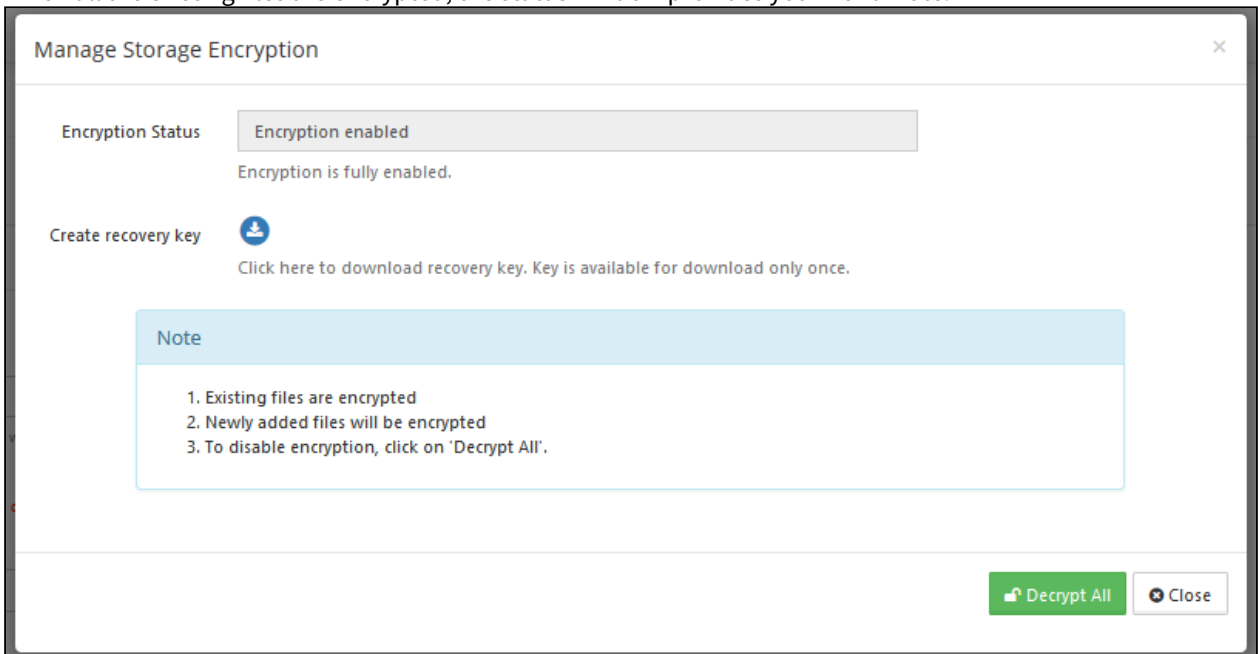
If your local storage already contains files:

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

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



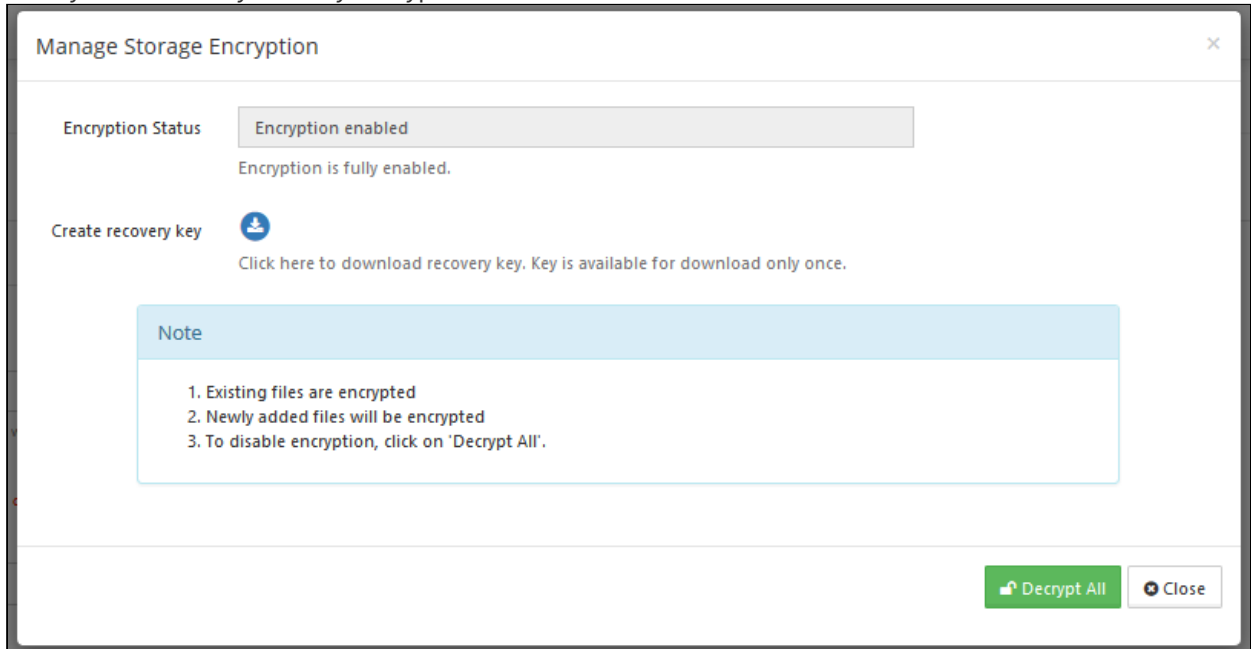
2. When all the existing files are encrypted, the status window provides you with a Note.



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.

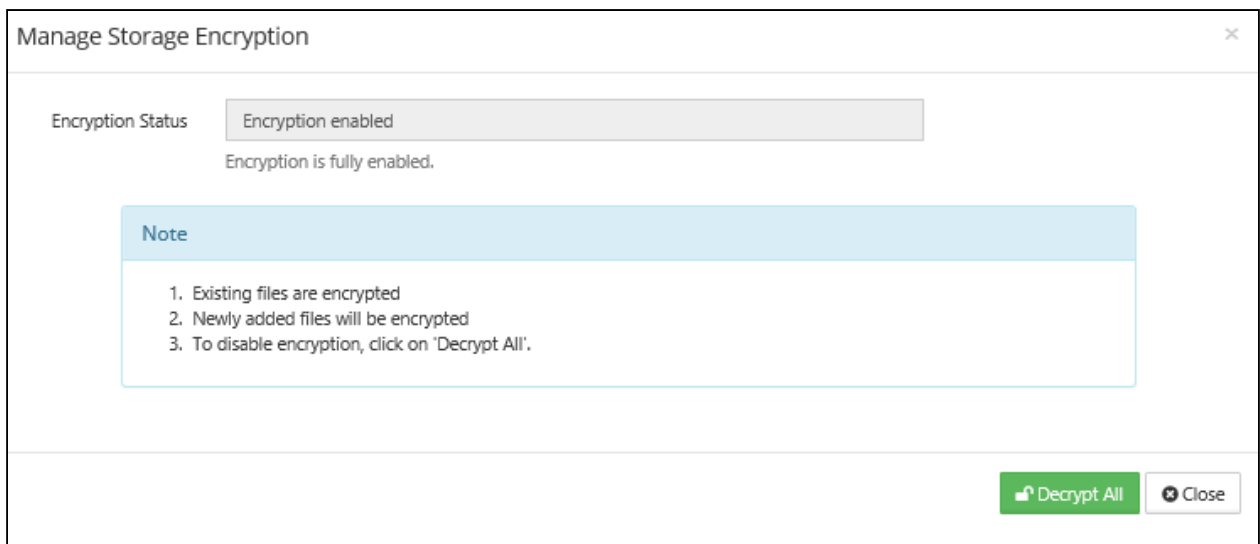


Disabling Storage Encryption

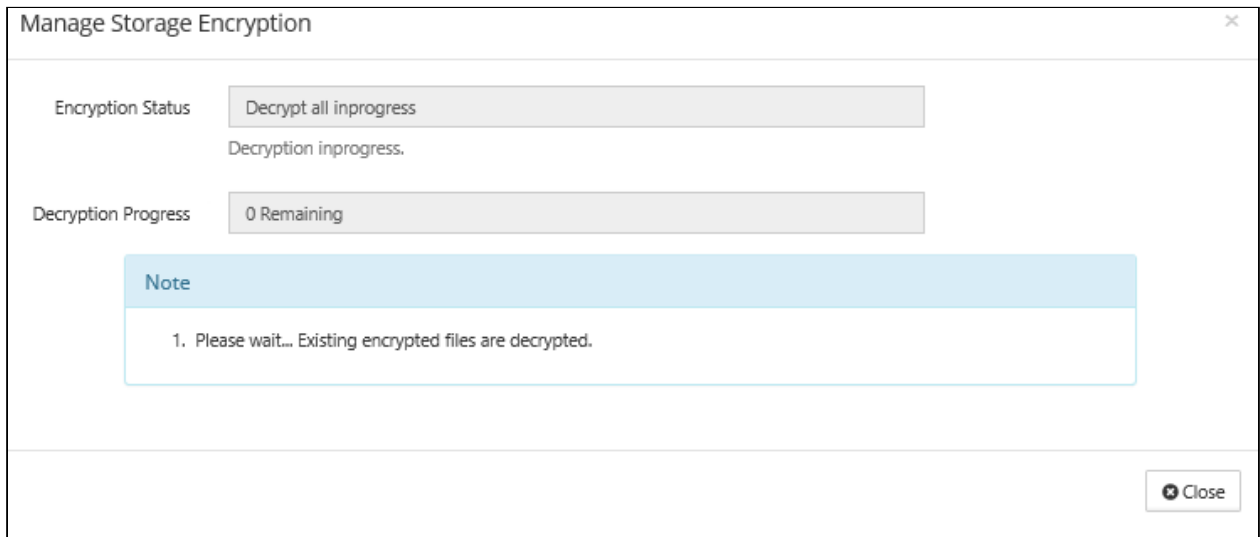
Administrators can disable storage encryption following the steps here.

To disable encryption:

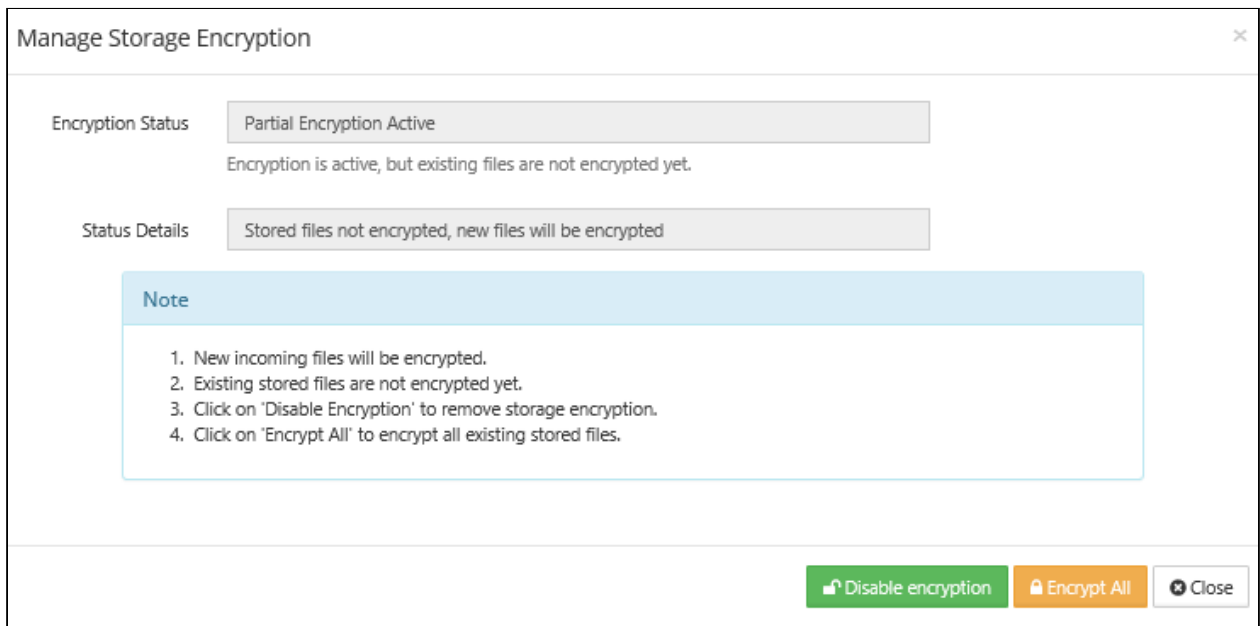
1. Login into admin UI as an admin user with necessary permissions.
2. Goto Settings -> Storage.
3. Click on "Decrypt All".



4. Now all the files are decrypted. To disable encryption completely, click on "**Decrypt All**". There will be "decrypt in progress" screen as below.



Once the decryption is complete, the following screen is shown.



Activating Password Protected Storage Encryption

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

When FileCloud server needs storage activation, it can be done in two ways:

Activating With Password

This is the normal activation method, where the admin user enters the encryption password and activates the storage system.

From encryption management dialog, enter the password and click 'Activate' button.

Manage Storage Encryption
✕

Encryption Status No Encryption

Encryption is not enabled. Files are stored as-is.

Encryption Password

Encryption Password (Repeat)

Create recovery key [Click here to download recovery key. Key is available for download only once.](#)

Note

Encryption password is optional to enable encryption. If an encryption password is used:

1. Password has to be entered everytime server starts
2. If password is lost, files cannot be recovered
3. Memcache server is a necessary requirement.

🔒 Enable encryption
✕ Close

Activating With Recovery Key

Note

This option is available only when a recovery key was created during [initialization](#).

This method can be used to activate storage system, when the recovery password is lost.

From encryption management dialog, click 'Browse' and select the recovery key. Finally, click 'Activate' to activate the storage.

Manage Storage Encryption ✕

Encryption Status Encryption In-Active
Cryptfs requires password for activation.

Encryption Password Enter Encryption Password

Activation Key Browse...
Activate with a recovery key file (.PPK), instead of encryption password.

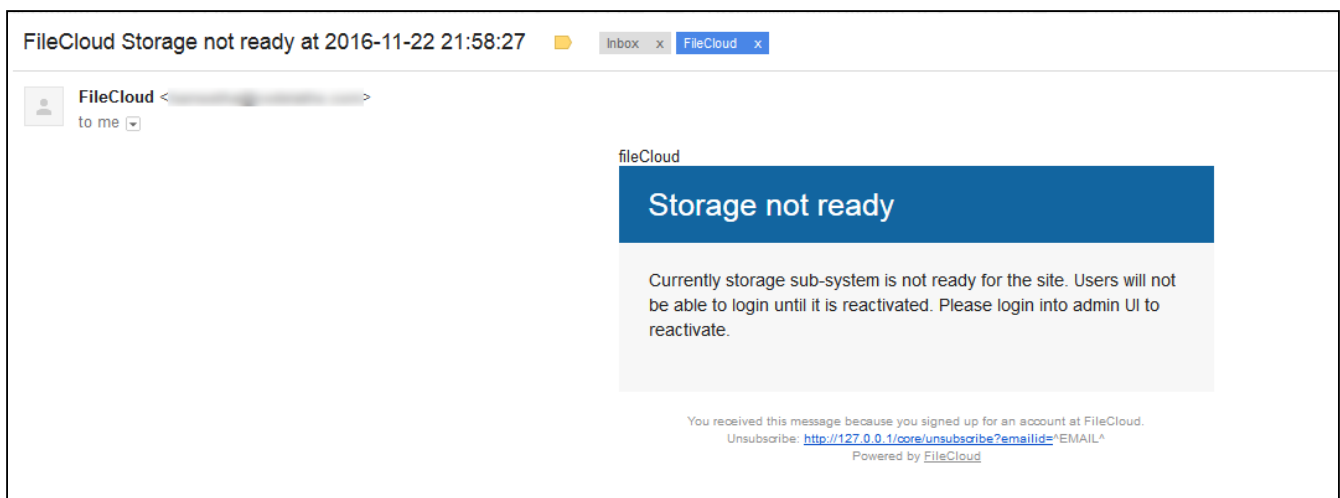
Note

1. A password that was used to initialize encryption, is needed again for activation .
2. If encryption is not active, stored files cannot be accessed by users.

✔ Activate
✕ Close

Note: Email notification when the encryption password needs to be entered

An email will be sent to user ,
"Storage not ready - Currently storage sub-system is not ready for the site. Users will not be able to login until it is reactivated. Please login into admin UI to reactivate"



User will have to enter encryption password in admin UI and then login into the user.

Activating Encrypted Protected Storage From Command Line

Introduction

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

FileCloud server storage activation can be also done from command line.

Prerequisites

Enable PHP CLI Mode

To run the following commands, PHP CLI mode needs to be enabled.

In 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
```

In Windows, the PHP cli mode is already enabled in FileCloud installer.

Activating Storage

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. To **activate storage using 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 only 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

Administrators can enable S3 storage-level encryption supported by FileCloud.



FileCloud Server now supports FIPS licenses.

Enterprises who are subject to the FIPS regulations must install and run a FIPS-enabled operating system. For example, Windows in FIPS mode.

When using a FIPS-enabled license, the Admin Portal shows:

- Running in FIPS mode prominently displayed
- SSO features hidden
- Storage encryption option

What do you want to do?



[Enabling S3 Storage Encryption](#)



[Disabling S3 Storage Encryption](#)

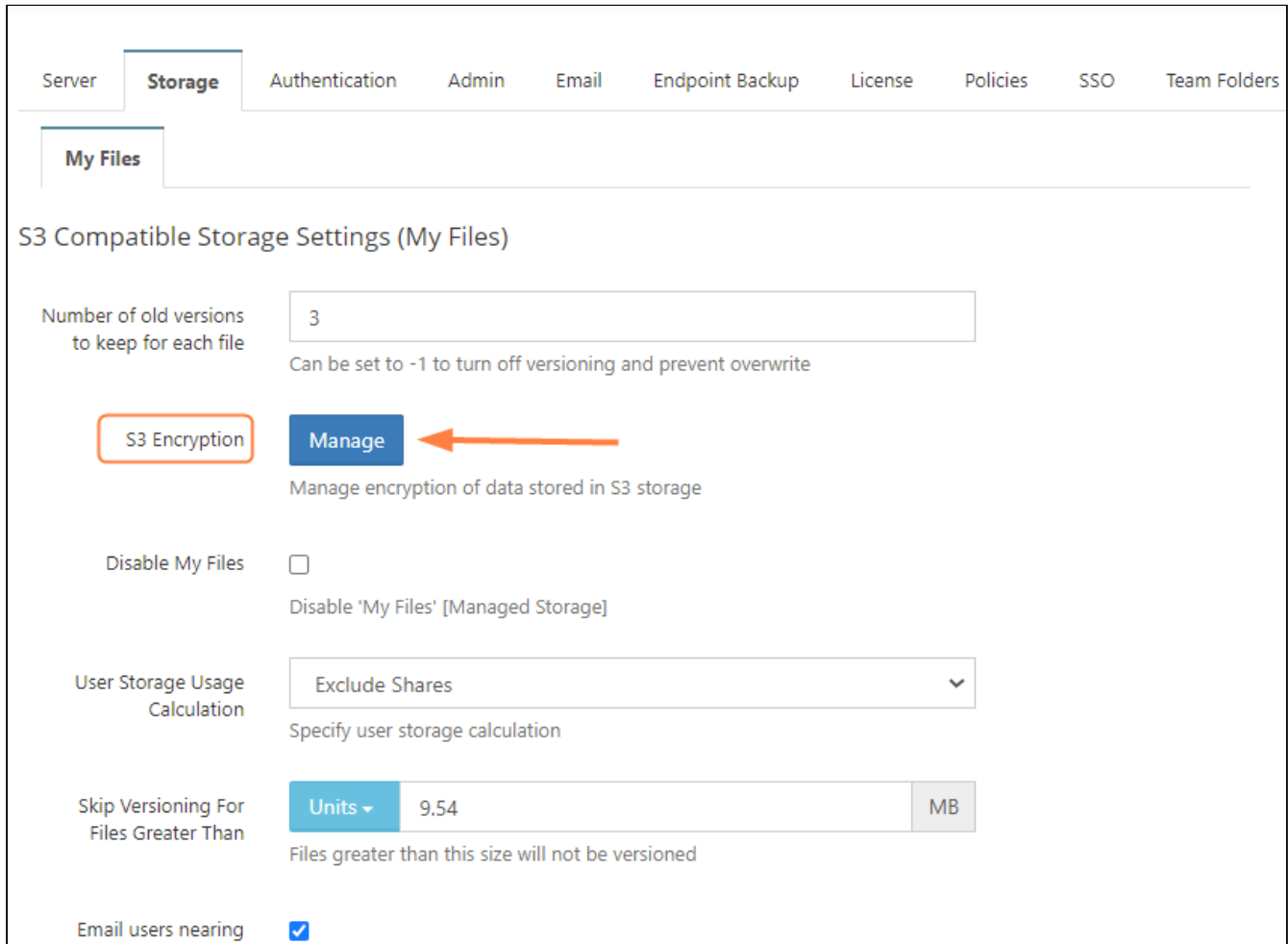


Read more about [Choosing S3 Encryption Type](#)

Enabling S3 Storage Encryption

In FileCloud Server version 19.1 and later, 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 S3 Storage for compliance and security reasons.



Server **Storage** Authentication Admin Email Endpoint Backup License Policies SSO Team Folders

My Files

S3 Compatible Storage Settings (My Files)

Number of old versions to keep for each file
Can be set to -1 to turn off versioning and prevent overwrite

S3 Encryption **Manage** ←
Manage encryption of data stored in S3 storage

Disable My Files
Disable 'My Files' [Managed Storage]

User Storage Usage Calculation
Specify user storage calculation

Skip Versioning For Files Greater Than 9.54 MB
Files greater than this size will not be versioned

Email users nearing

To enable storage encryption:

1. Encryption Pre-Requisites

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

Order	Requirements
1	FileCloud Installation (v13 or higher)
2	Memcached installation

Order	Requirements
3	<p>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: <code>XAMP_HOME\php\extras\openssl\openssl.cnf</code> (till v17.3) Windows: <code>XAMP_HOME\php\extras\ssl\openssl.cnf</code> (from v18.1) Linux: <code>/etc/ssl/openssl.cnf</code></p> <p>In Windows, for example if you have XAMPP installed in <code>D:\xampp</code>, then you will be adding the following line to cloudconfig.php. define("SSL_CONF_FILE", "D:\\xampp\\php\\extras\\ssl\\openssl.cnf");</p>
4	<p>Only in windows, <code>php_com_dotnet.dll</code> is needed, which will be installed automatically with FileCloud v9.0 installer onwards.</p>
5	<p>For Windows, if your xampp is installed in location other than <code>C:\xampp</code>, then add the following key in <code><WWWROOT>\config\cloudconfig.php</code> For example, if your xampp is in <code>D:\xampp</code>, then in file <code>D:\xampp\htdocs\config\cloudconfig.php</code>, add the following string (any location before the bottom <code>"?>"</code> line) define("PHPBIN_PATH", "D:\\xampp\\php\\php.exe");</p>

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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *SETTINGS*, select *Settings*.
3. On the *Manage Storage* screen, select the *Storage* tab and then the *My Files* sub-tab.
4. You will see a new option called *S3 Encryption*.

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

Server **Storage** Authentication Admin Email Endpoint Backup License Policies SSO Team Folders

My Files

S3 Compatible Storage Settings (My Files)

Number of old versions to keep for each file
Can be set to -1 to turn off versioning and prevent overwrite

S3 Encryption **Manage** ←

Manage encryption of data stored in S3 storage

Disable My Files
Disable 'My Files' [Managed Storage]

User Storage Usage Calculation ▾
Specify user storage calculation

Skip Versioning For Files Greater Than MB
Files greater than this size will not be versioned

Email users nearing

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

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

Manage S3 Encryption

Encryption Status

Encryption Type ▾

Note

1. Files are currently not encrypted

Enable encryption Close

You are prompted to confirm encryption.

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

Manage S3 Encryption
✕

Encryption Status Encryption is enabled (Existing file encryption in progress...)

Encryption Type Amazon S3-Managed Key Encryption ▼

Progress: 8/27 encrypted

Note

1. Encryption task is in progress.
2. This can take some time depending on the total amount of data stored in the bucket

Abort
Close

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

Manage S3 Encryption
✕

Encryption Status Encryption is enabled

Encryption Type Amazon S3-Managed Key Encryption ▼

Note

1. All existing files and newly added files will be encrypted using AES256 encryption

Disable encryption
Close

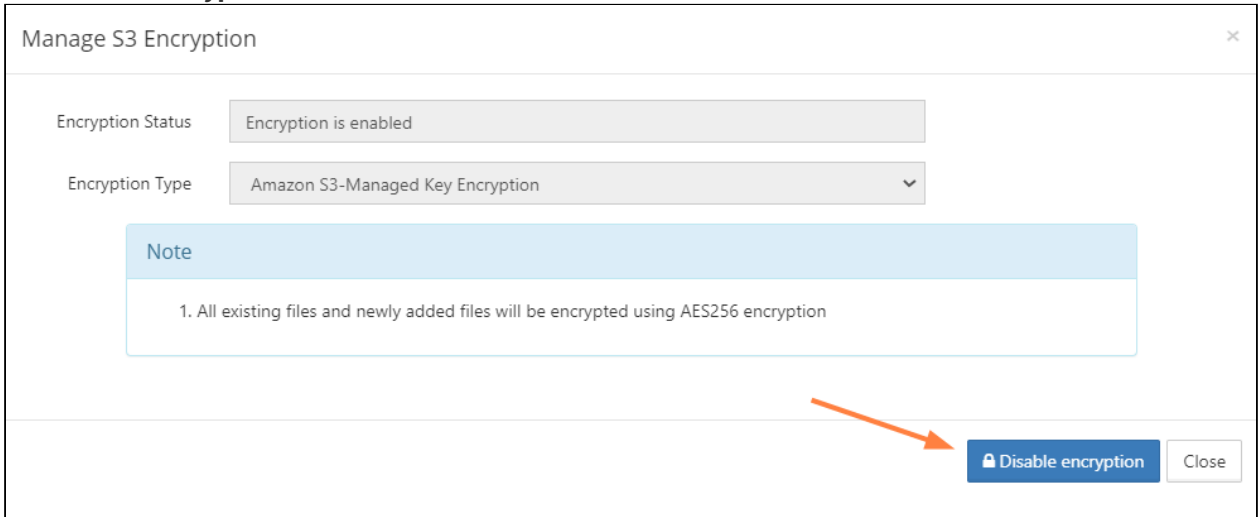
Disabling S3 Storage Encryption

Administrators can disable S3 storage encryption following the steps here.

To disable S3 encryption:

1. Login into admin UI.
2. Goto **Settings -> Storage**.
3. Click **Manage**.

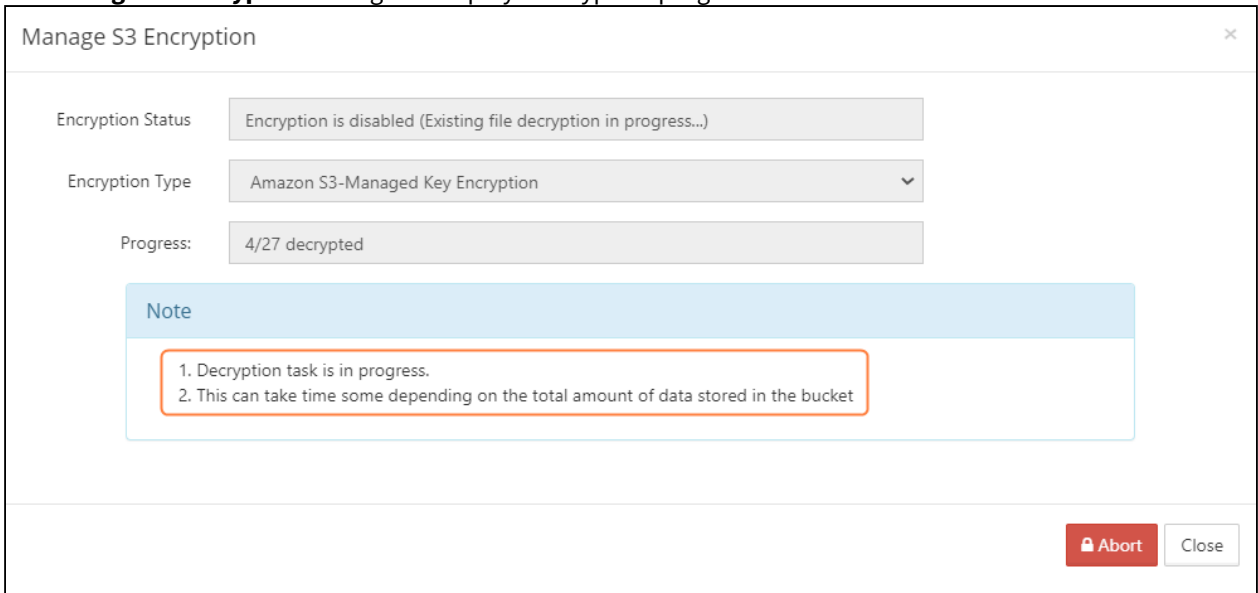
The **Manage S3 Encryption** dialog box opens.

4. Click **Disable encryption**.

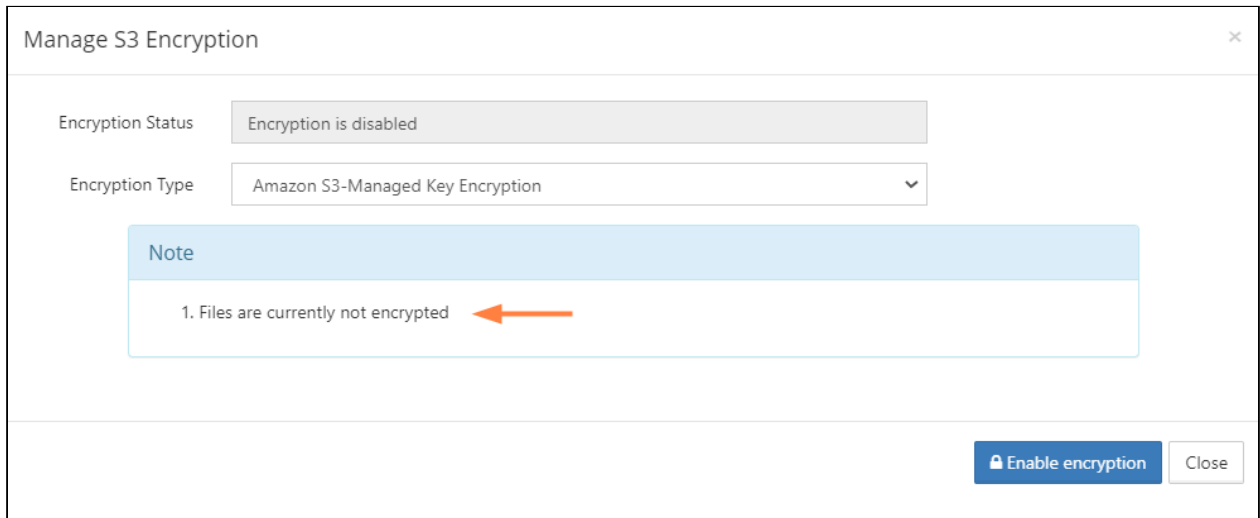
You are prompted to confirm disabling encryption.

5. Click **OK**.

The **Manage S3 Encryption** dialog box displays decryption progress:



Once the decryption is complete, the dialog box confirms that files are not encrypted.



Choosing S3 Encryption Type

When you use S3 Storage Encryption:

- The communication from FileCloud to AWS will use SSL encryption resulting in complete protection for data in transit.
- Once the S3 is setup correctly, a new field called *S3 Encryption* will be available under [Amazon S3 Storage Settings](#).

FileCloud supports the following Server Side Encryption:

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 Note: Even though the encrypted data is accessible directly from the S3 console, do not access the data if it was created by FileCloud Managed storage, as doing so will cause data corruption to occur. In this case, the data should only be modified by FileCloud.
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.
Server-Side Encryption with Customer-Provided Keys (SSE-C)	This is a new support available from FileCloud v15 on-wards. The data will be encrypted using customer supplied 32 bit encryption key. This option will have SLOWER performance due to restriction on how this data can be decrypted (Amazon server will NOT be able to decrypt the data and the data has to be first downloaded to FileCloud server and decrypted). The data will NOT be accessible via S3 console as well.

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.

IAM User Policy for S3 Access

FileCloud requires access in order to create bucket and manage it.

The IAM user used to manage it must have the following permissions. This shows access to all buckets in your S3 console. You can restrict to specific bucket using the appropriate resource arn. Something like `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::*"
      ]
    }
  ]
}
```

You can provide access to only a specific bucket, your Permission should look as follows:

```


{
  "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'.

The screenshot shows the 'Configure key' step in the AWS KMS console. The left sidebar shows the navigation menu with 'Customer-managed keys' selected. The main content area is titled 'Configure key' and shows a progress indicator for five steps: Step 1 (Configure key), Step 2 (Add labels), Step 3 (Define key administrative permissions), Step 4 (Define key usage permissions), and Step 5 (Review). The 'Configure key' section has two radio button options: 'Symmetric' (selected) and 'Asymmetric'. Below this is the 'Advanced options' section, which includes 'Key material origin' (with 'KMS' selected) and 'Regionality' (with 'Single-region key' selected). At the bottom right, there are 'Cancel' and 'Next' buttons.

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

The screenshot shows the 'Add labels' step in the AWS KMS console. The left sidebar shows the navigation menu with 'Customer managed keys' selected. The main content area is titled 'Add labels' and shows a progress indicator for five steps: Step 1 (Configure key), Step 2 (Add labels), Step 3 (Define key administrative permissions), Step 4 (Define key usage permissions), and Step 5 (Review and edit key policy). The 'Add labels' section has a heading 'Create alias and description' and a text input field for the 'Alias' containing 'MyAccount-Key'. Below this is a text area for the 'Description - optional'. At the bottom, there is a section for 'Tags - optional' with two input fields for 'Tag key' and 'Tag value', and an 'Add tag' button. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

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

Key Management Service (KMS) X

- AWS managed keys
- Customer managed keys**
- Custom key stores

KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

Define key administrative permissions

Key administrators
Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Q MyAdmin X < 1 >

Name	Path	Type
No matches No results match your query		

[Clear filter](#)

Key deletion

Allow key administrators to delete this key.

Cancel [Previous](#) [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.**

Key Management Service (KMS) X

- AWS managed keys
- Customer-managed keys**
- Custom key stores

KMS > Customer-managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Define key usage permissions

This account
Select the IAM users and roles that can use the CMK in cryptographic operations. [Learn more](#)

Q MyUser X < 1 >

Name	Path	Type
No matches No results match your query		

[Clear filter](#)

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam:: 123456789012 :root [Remove](#)

[Add another AWS account](#)

Cancel [Previous](#) [Next](#)

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".

Manage S3 Encryption
✕

Encryption Status Encryption is disabled

Encryption Type Amazon KMS-Managed Key Encryption ▼

KMS SSE Key ID <ARN for the KMS key from KMS Account>

Note

1. Files are currently not encrypted

🔒 Enable encryption
Close

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**.

The screenshot shows the AWS KMS console interface. On the left, there is a navigation menu with 'AWS managed keys', 'Customer managed keys' (highlighted in orange), and 'Custom key stores'. The main content area is titled 'General configuration' and shows the following details:

Alias	-	Status	Enabled
Description	-	Creation date	Feb 06, 2020 20:02 GMT+5:30

Below this, there is a section for 'Cryptographic configuration' with three tabs: 'Key policy', 'Tags', and 'Key rotation' (highlighted in orange). Under the 'Key rotation' tab, there is a yellow highlight around the 'Key rotation' heading and a checked checkbox for 'Automatically rotate this CMK every year'. A 'Learn more' link with an external icon is also present.

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.

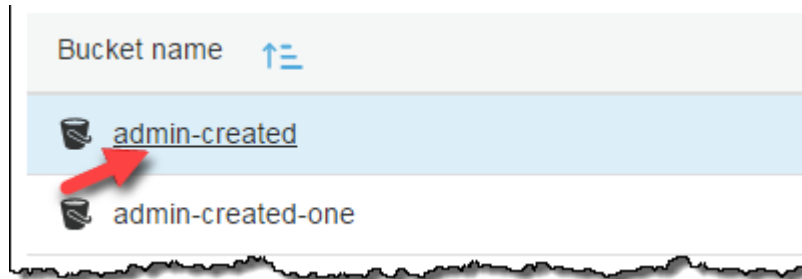
However, automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key.

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/>.

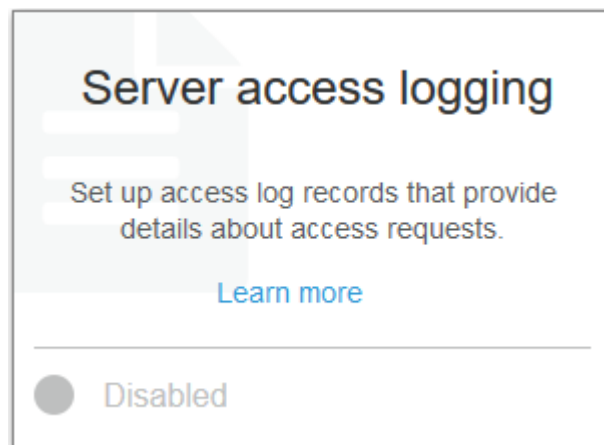
2. In the **Bucket name** list, choose the name of the bucket that you want to enable server access logging for.



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.

Manage the Recycle Bin Using Policies

Administrators can configure FileCloud to deal with the site's Recycle Bin 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 a user's ability to empty their own recycle bin.

➔ [Restrict User's Recycle Bin Options](#)

All of these scenarios can be managed by configuring the built-in policy called *Global Default Policy*.

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.
- Administrators can set global recycle bin policies using the Global Default Policy.
- 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
<i>Store Deleted Files</i>	YES or NO	Move the file from its location in My Files to the recycle bin when the user deletes it
<i>Automatically Delete Files from Recycle Bin After Set Number of Days</i>	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.

Setting	Option	Description
<i>Do Not Store Deleted Files Greater Than</i>	Any positive number of Units: <ul style="list-style-type: none"> • GB • MB • KB • B 	Files Greater than the specified size are permanently deleted. The number can contain decimals. For example: <ul style="list-style-type: none"> • 0.09765625 GB

Policy Settings - Global Default Policy ✕

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

Enables/disables privacy settings

Store Deleted Files NO ▾

Move file to recycle bin on delete action


Automatically Delete Files from Recycle Bin After Set Number of Days 0

Number of days once deleted files will be cleared. Value of 0 indicates that deleted files will not be cleared automatically.


Do Not Store Deleted Files Greater Than Units ▾ 0.09765625 GB

Files Greater than the specified size are permanently deleted.

Save
Reset
✕ Close

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


To configure the recycle bin policy:

1. Log into the *Admin Portal*.
2. From the left navigation pane, under **SETTINGS**, click *Settings*.
3. Click the *Policies* tab, select the *Global Default Policy*, and then click the *Edit policy* button (.
4. In the *Policy Settings* window, in *Store Deleted Files*, select **YES** or **NO**.
5. If you selected **NO**, to save your changes, click *Save* and to close the policy window click *Close*.

6. If you selected *YES*, in *Automatically delete File from the Recycle Bin After Set Number of Days*, to enable this option, type in a number. To disable this option, type in 0.
7. If you selected *YES*, in *Do Not Store Deleted Files Greater Than*, select the type of unit in *Units*, and then type in a number.
8. To save your changes, click *Save* and to close the policy window click *Close*.

Disable Managed Storage (MyFiles section)

Managed storage (shown as My Files in the user portal) can be disabled completely if users need to access only [network folders](#) or [shared data](#).

 This should be done during initial server setup. If Managed storage 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.

The following steps should be followed to set up Managed storage.

1. Log into the [Administration portal](#)
2. Click **Settings** in the navigation panel
3. Click the **Storage** tab.

4. Check **Disable My Files**.

Server **Storage** Authentication Admin Database Email Endpoint Backup License Policies SSO

My Files Network

My Files Storage Settings

Storage Path

Specify the location to store Cloud Files, this must be writable by Webserver.
 Example path on Windows : c:\clouddata
 Example path 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
 Can be set to -1 to turn off versioning and prevent overwrite

Disable My Files
 Disable 'My Files' [Managed Storage]

User Storage Usage Calculation
 Specify user storage calculation

Skip Versioning For Files Greater Than
 Files greater than this size will not be versioned

Email users nearing storage limit

5. Click **Save** at the bottom of the page.

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, you need to disable a setting in the WWWROOT/.htaccess file

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




Change that to

```
i <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**.

Share link for Accounts

Share Link
http://127.0.0.1/url/nbernub4fka2qmhd Modify Link   

Shared File
/jenniferp/Accounts

Share Options | Share History

Share Name: VpZ6slwQdMrvixjv [Change](#)


Expires: Never

Upload Size Limit (MB): Unlimited

Send Email Notifications: Yes

Sharing Permissions:

Allow anyone with link

Allow Upload Only 

Allow anyone with link and a password

Allow selected users or groups

[Remove Share](#) OK

Step 3:

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

The screenshot shows the FileCloud web interface. The top navigation bar includes the FileCloud logo, a search bar, and a user profile for Emma. The left sidebar contains navigation options: All Files, My Files, Team Folders, Network Shares, Shared with Me, Recent Documents, Starred, Shared by Me, File Operations, Notice, and Deleted Files. The main content area displays the 'Accounts' folder, which contains 4 items. A table lists these items:

Name	Modified	Size
AccountNames	Oct 23, 2020 2:13 PM	
CharacterSheet_3Pgs_Complete.pdf	Nov 17, 2020 2:57 PM by you	347 KB
FCShareExpiry.png	Nov 06, 2020 9:55 AM by you	68 KB
announcements.md	Oct 23, 2020 1:28 PM by you	81 B

The right sidebar shows details for the 'Accounts' folder, including its path (/jenniferp/Accounts), permissions, share settings (1 users, 0 groups), and retention policy (No retention policies applied).

The screenshot shows a 'Sample Upload Form' dialog box. It contains the following HTML snippet:

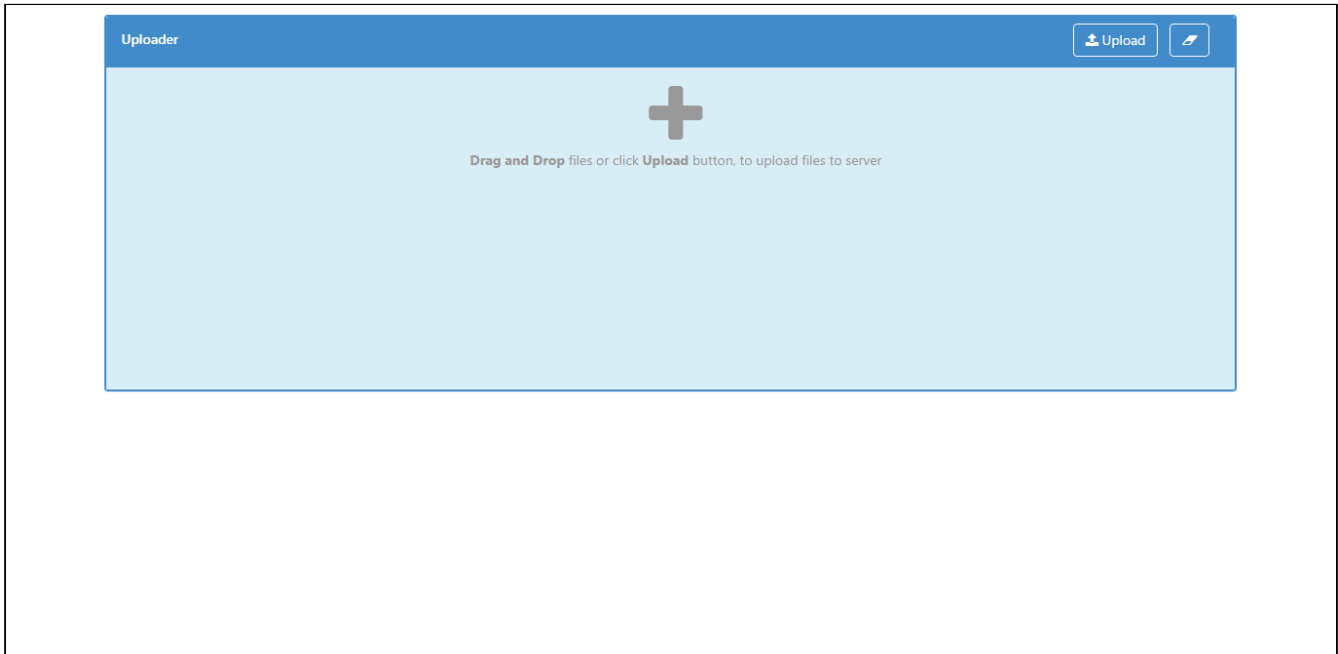
```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8" />
  <title>Upload Form</title>
</head>
<body>
<h1>Upload Form</h1>
<iframe src="http://[redacted]" scrolling="yes" width="500px"
height="500px" frameborder="0"></iframe>
</body>
</html>
```

Below the snippet, there is a note: "Use the HTML snippet to embed in your own websites" and a "Close" button.

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

The ability to use a checkbox to allow or restrict a user's ability to clear all files at once from their recycle bins is available in FileCloud Server version 19.1 and later.

Administrators can configure how FileCloud users can interact with the site's Recycle Bin through policies.

- Use a checkbox to allow or restrict a user's ability to clear all files at once from their recycle bins.

By default, all users:

- Belonging to the *Global Default Policy*
- Logged in to the *User Portal*
- Can click on *Folder Actions* and select *Clear Deleted Files*

If this option is not selected by clearing the checkmark, users:

- Belonging to the *Global Default Policy*
- Logged in to the *User Portal*
- Can click on *Folder Actions* but will not see a *Clear Deleted Files* option.

⚠ This policy doesn't block the delete operation! Users can still remove files from the recycle bin on a file-by-file basis.

Policy Settings - Global Default Policy ✕

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

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications

User Policy

Disable Invitations to New Users NO ▼

Do not allow user to send invitations to new users when shares are created.

Create account on new user shares NO ▼


Create accounts automatically when share invitations are sent to new users.

Enable Recyclebin Clear Feature YES ▼

Allow users to clear recyclebins.

Save
Reset
✕ Close

To configure this option:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, click *Settings*.
3. On the *Manage Settings* screen, select the *Policies* tab.
4. On the *Manage Policies* screen, select the *Global Default Policy* to change this for all users, or select the policy you want to use.
5. In the row of the policy, click the edit icon ().
6. In the *Policy Settings* window, select the *User Policy* tab.
7. Scroll down until you see a checkbox labeled *Enable Recyclebin Clear Feature*.

Setting up FileCloud Managed Azure Blob Storage

As an administrator, you can integrate FileCloud Server to store user data on an Azure Blob storage server.



- Azure Blob storage (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 accomplish these tasks using the Azure Console**

 [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 (later than Ubuntu 14.04)	Linux (earlier than Ubuntu 14.04)
c:\xampp\htdocs	/var/www/html	/var/www

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 this:


```
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
```

 **Nothing needs to be added or edited in azureblobstorageconfig.php**

2. Configure Credentials

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

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 (To get your account key, visit Amazon security portal). For an RBAC user, it requires at least the following permissions .
Container Name	<p>Provide a storage container name.</p> <p>The container should be new (in some circumstances, containers previously used in FileCloud could be used).</p> <p>It is very important that the Azure storage container is never modified outside of the FileCloud subsystem.</p> <div style="border: 1px solid #ffc107; padding: 10px; margin-top: 10px;"> <p> Container name rules</p> <ul style="list-style-type: none"> The name of the container has to be unique and follow the naming rules. If container name is not provided, FileCloud will auto-generate it when setting up the storage. Container name cannot be changed once storage is set up. </div>

Field	Description
Endpoint Suffix	<p>Optional: This is the Azure Blob storage endpoint.</p> <ul style="list-style-type: none">• Use this to specify your own Azure storage endpoint (typically Azure-compatible storage)• Use this if it is an unpublished region. <p>To use an Azure endpoint, it must be one of the values published here.</p> <ul style="list-style-type: none">• Note: For govcloud installs, you must use the following endpoint suffix: <code>blob.core.usgovcloudapi.net</code>
Blob Storage Folder	<p>Optional: All files will be stored inside this root storage folder.</p> <ul style="list-style-type: none">• This folder will be created automatically.

Manage Settings

Server

Storage

Authentication

Admin

Database

Email

Endpoint Backup

License

My Files

Network

Azure BLOB Storage Settings (My Files)

Account Name

Azure Blob account name

Account Key

Azure Blob account key

Container name

(Optional) Container name. Leave empty to autogenerate. Cannot be changed once created.

Endpoint Suffix

(Optional) Azure Storage service end point. Leave it empty if using standard Azure's Blob service. This is required for regions or instances with different endpoint suffixes, such as for Azure China 21Vianet or Azure Government. End point cannot be changed once the bucket is created

Blob 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.

Save Settings

Verify Azure Blob settings and auto-configure any needed configuration

To configure Azure Blob storage Credentials

1. Open a browser and log into *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, select the *Storage* tab.
4. Type in or select the settings for your environment.

5. Click Save.**3. Data Encryption****i 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 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 *.amazonaws.com
*.core.windows.net; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline'
'unsafe-eval' 'self';font-src 'self' data;;img-src 'self' data: *.duosecurity.com
*.live.com *.amazonaws.com *.core.windows.net"
```


Setting Up Network Folders

Administrators can control how users 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.

 In the following section, to display more information, click on a topic.

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:

- [LAN Based Network Folders](#)
- [Amazon S3 Bucket Based Network Folders](#)
- [Azure Blob Storage Based Network Folders](#)
- [Network Folder Limitations](#)
- [Enabling Directory Scraping](#)
- [FileCloud Helper Service](#)
- [Clearing Deleted Files from Network Folders](#)
- [Display Names that Start with a Dot](#)
- [Wasabi S3 Bucket Based Network Folders](#)
- [Backblaze B2 Bucket Based Network Folders](#)
- [Cloudian S3-Compatible Object Storage Network Folders](#)

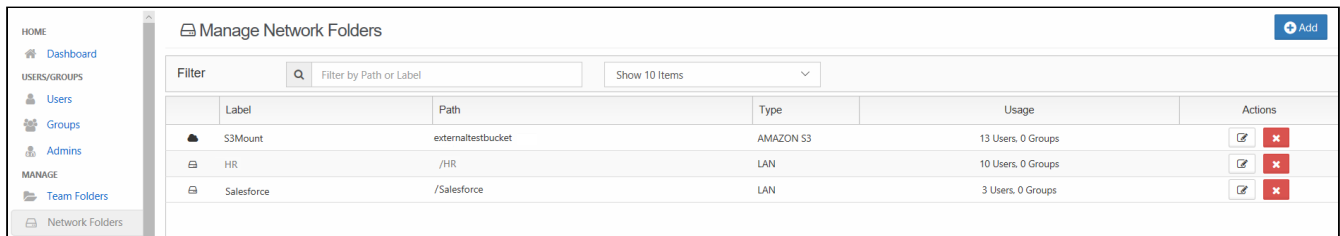
FileCloud Blogs

- [Connect Your SFTP to FileCloud](#)

LAN Based Network Folders

Administrators can integrate local storage, or pre-existing files on your corporate Windows and/or Linux servers, into FileCloud.

- This gives FileCloud users access to files on your corporate servers
- Network folders can be mounted in FileCloud
- Network appears as a location on the User Portal inside the Network Shares folder



Label	Path	Type	Usage	Actions
S3Mount	externaltestbucket	AMAZON S3	13 Users, 0 Groups	
HR	/HR	LAN	10 Users, 0 Groups	
Salesforce	/Salesforce	LAN	3 Users, 0 Groups	

In this section:

- [Create a LAN-Based Network Folder](#)
- [Smart Mounted Network Folders](#)
- [Network Folders with NTFS permissions](#)
- [Indexing of Network Folders](#)
- [Searching in Network Folders](#)
- [Web Server Permissions for Network Shares](#)

Create a LAN-Based Network Folder

To configure Network Folders, first enable them and prohibit their creation on certain paths, then add the folder paths as Network Folders and give users and groups permission to access them.

Enable mounting share paths

The `TONIDOCLOUD_ENABLE_NETWORK_SHARE_MOUNTS` command has been added in FileCloud 22.1. In FileCloud versions prior to this, no configuration file setting is required for enabling or disabling Network Folders.

Prior to creating new Network Folders or changing the mount paths on existing Network Folders, you must enable mounting network share paths.

1. Open `cloudconfig.php`.

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

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

3. Change the value **false** to **true**.

Block locations from mounting as share paths

i The TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST command has been added in FileCloud 22.1. In FileCloud versions prior to this, C:/xampp is not permitted to be mounted as a Network Folder, but no configuration file setting exists 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 command for blocking locations, or 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');
```

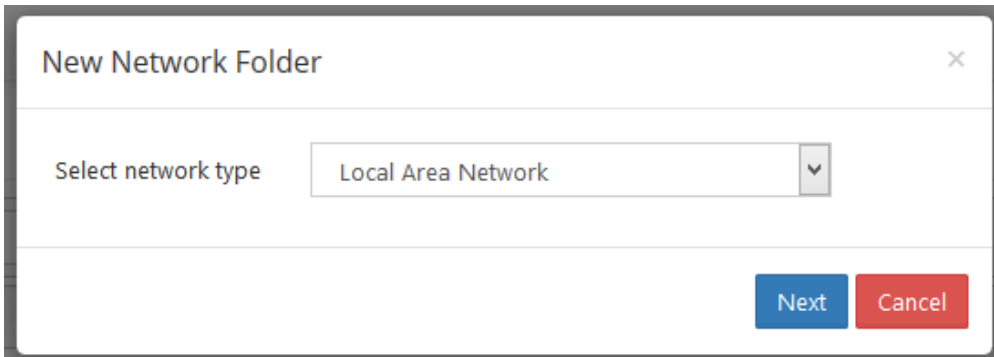
3. Add any locations that you do not want to be shared, for example:

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

Create a Network Folder

To create a Network Folder:

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

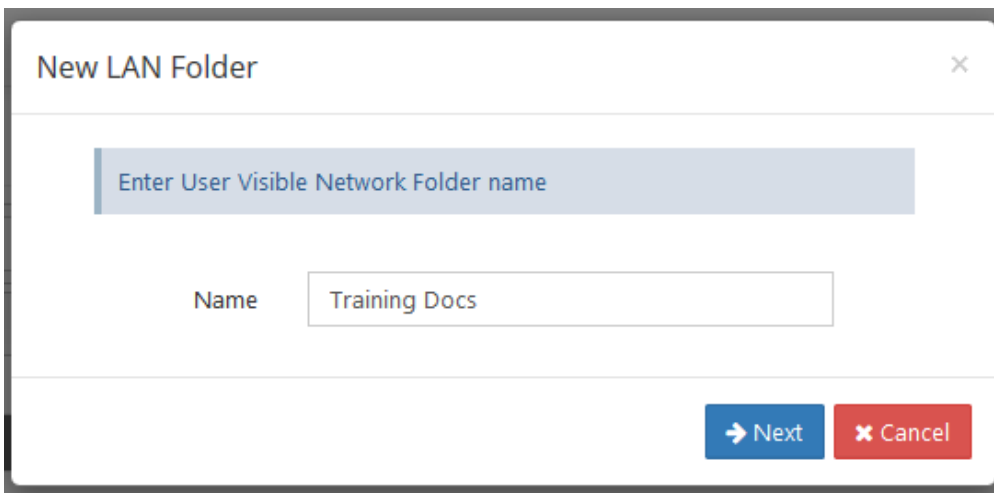


New Network Folder

Select network type Local Area Network

Next Cancel

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 can have only alpha numeric characters.



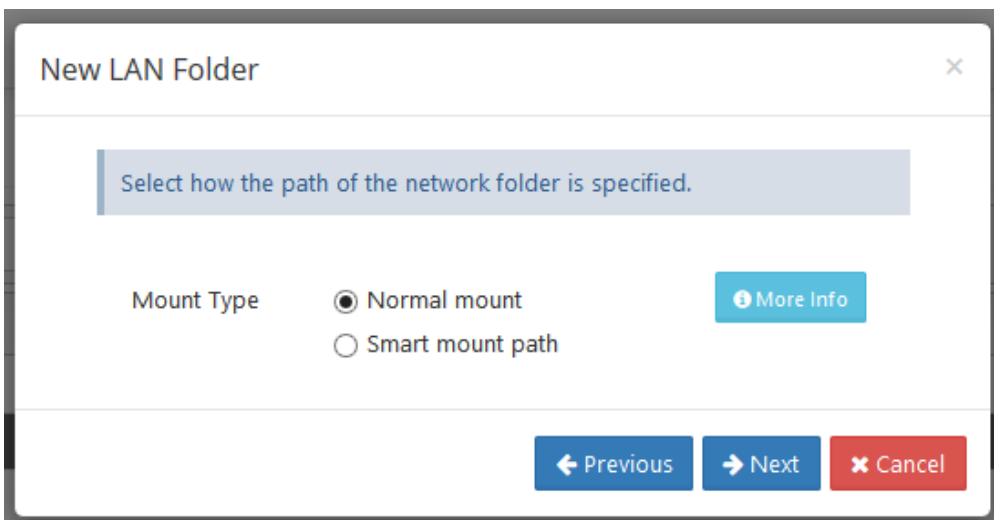
New LAN Folder

Enter User Visible Network Folder name

Name Training Docs

Next Cancel

6. Select whether you want to use Normal Mount Paths or use Smart Mounts. [Read more](#) about Smart Mounts.



New LAN Folder

Select how the path of the network folder is specified.

Mount Type

Normal mount [More Info](#)

Smart mount path

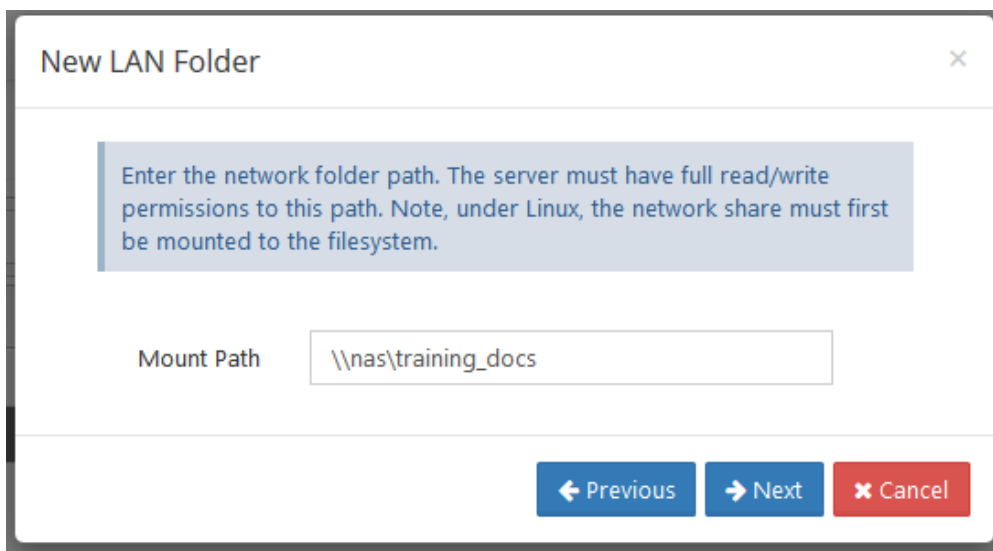
Previous Next Cancel

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 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.

ℹ When adding Network Shares to FileCloud Server in a Windows Environment please note that File Paths can't be greater than 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/>



New LAN Folder

Enter the network folder path. The server must have full read/write permissions to this path. Note, under Linux, the network share must first be mounted to the filesystem.

Mount Path

← Previous → Next × Cancel

⚠ 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.

1. 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.](#)

The screenshot shows a dialog box titled "New LAN Folder" with a close button (X) in the top right corner. Below the title bar is a light blue header bar with the text "Specify permissions for this network folder". Underneath, the "Access Permission" section contains two radio button options: "Use assigned permissions" (which is selected) and "Use NTFS permissions". At the bottom of the dialog, there are three buttons: "Previous" (with a left arrow), "Create share" (with a right arrow), and "Cancel" (with an X).

2. 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.

The screenshot shows the same "New LAN Folder" dialog box, but now the light blue header bar contains the text "Assign users and groups access to this network folder". Below this, there are two buttons: "Add User Access" and "Add Group Access". At the bottom right of the dialog, there is a "Finish" button with a right arrow.

3. 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 share, the following steps should be performed

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.

Network Folder Details ×

Network Folder Name	<input type="text" value="Business Docs"/>
Network Folder Path	<input type="text" value="C:\data\business"/>
Permissions	<input type="text" value="NTFS"/> ▼
Smart Mount	<input type="checkbox"/>
Enable ABE (NTFS)	<input type="text" value="Global Policy"/> ▼
Disable Offline Sync	<input type="checkbox"/>
Disable Notifications	<input type="checkbox"/>
Sharing	<input type="text" value="Allow All Shares"/> ▼
Allow Remote Deletion of Files via Offline Sync	<input type="checkbox"/>
Realtime Index for Automatic Sync and Search (Beta)	<input checked="" type="checkbox"/> <input type="button" value="Reindex"/>
Realtime Index Status	<input type="text" value="5 folders, 17 files"/> <input type="button" value="Check"/>

4. Set the appropriate Access level
The access level for a user or group can be

Access	Description
Full Access	This allows the user to 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.

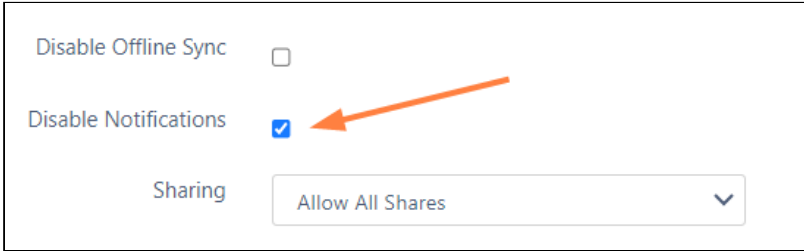
Notifications for Network Folders

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 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.



The screenshot shows a dialog box with three settings:

- Disable Offline Sync**:
- Disable Notifications**: (An orange arrow points to this checked checkbox.)
- Sharing**:

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 Folders Behavior

You can configure some of the behaviors of Network Folders by using the settings below found in Settings->Storage tab.

Server **Storage** Authentication Admin Database Email Endpoint Backup Li

My Files **Network**

Network Storage Settings

Network Folders Display Name

Display name for Network Folders

Users Can Share Network Folders

Allow sharing of Network Folders

Sync Network Folder

Enable to sync of Network Folders using CloudSync

Max. File Size Limit ⓘ

Units ▾ 0 MB

Specify maximum storage quota for file upload. 0 implies Unlimited quota. Warning: Renaming and editing files might fail if the limit is exceeded.

Number of old versions to keep for each file

Can be set to -1 to turn off versioning and prevent overwrite

Skip Versioning For Files Greater Than

Units ▾ 9.54 MB

Files greater than this size will not be versioned

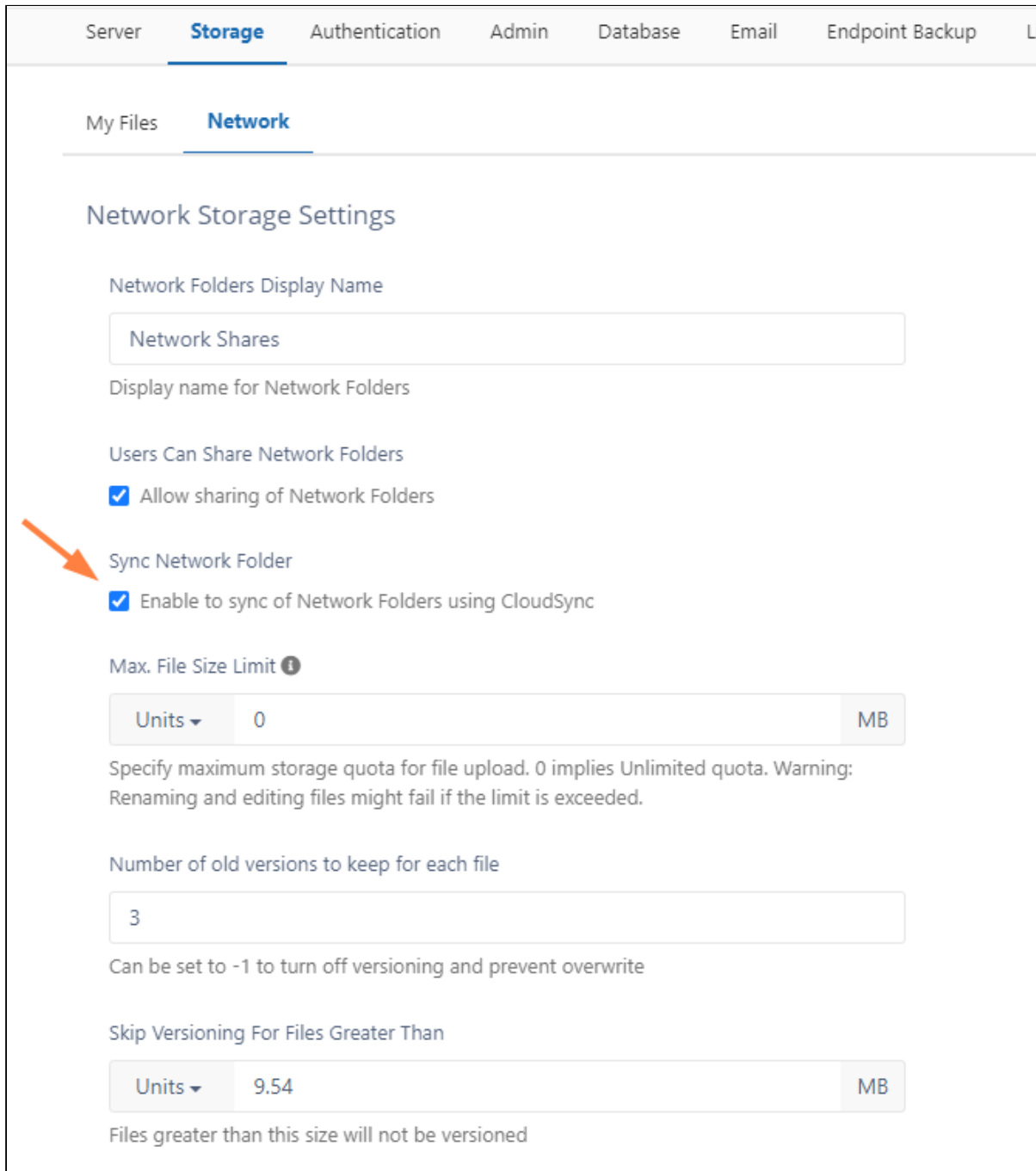
Function	Description
Network Folders Display Name	<p>This label will be displayed in the User portal when the user logs into their account.</p> <p>Please Note: Once setup, don't change it as this will affect existing sync apps that have started syncing. Existing sync apps will continue to sync to the older name and only new network shares configured via Sync will use the new name.</p>
User can share Network Folder	<p>This setting controls whether or not a network share location can be shared by a user</p>
Sync Network Folder	<p>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.</p>
Max File Size Limit	<p>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 uploading of files of unlimited sizes.</p>
Number of old versions to keep for each file	<p>Enables versioning of files in network location. To maintain no versions enter 0.</p>
Skip Versioning for files Greater than	<p>The file size limit in bytes beyond which the versioning will not be applied</p>
Skip Names	<p>This is a regex filter which can be used to exclude files that match the regex expression from file listing. Example of a Regular Expression that skips some names from displaying is <code>/(sub.* copy.*)/</code> This skips all files which start with "sub" or "copy"</p>
Enable Access Based Enumeration for NTFS	<p>When browsing network folders with NTFS permissions, folders that users don't have access to (no permissions) are hidden from view. Enabling ABE increases load on server. Note that ABE can be disabled for specific Network Shares if needed.</p>
Store Deleted Files in Network Folder	<p>Enable this to store deleted files from network folders in a special deleted items folder</p>

Function	Description
Do not store deleted files greater than	Files greater than this size specified in bytes do not get stored in Deleted Files.
Enabled Indexed Search	To enable indexing of network folders to allow fast searching. See this topic for more information.

Offline Access to Network Folders

FileCloud Sync app can provide offline access to Network Folders by allowing users to download files from Network Folders automatically similar to how synced folders work.

To enable Offline Access, you need to enable the **Sync Network Folder** option in Settings->Storage->Network Storage Settings.



The screenshot shows the 'Network Storage Settings' page in the FileCloud Server interface. The top navigation bar includes 'Server', 'Storage' (selected), 'Authentication', 'Admin', 'Database', 'Email', and 'Endpoint Backup'. Below this, there are tabs for 'My Files' and 'Network' (selected). The main content area is titled 'Network Storage Settings' and contains several configuration options:

- Network Folders Display Name:** A text input field containing 'Network Shares'.
- Display name for Network Folders:** A descriptive label for the display name.
- Users Can Share Network Folders:** A section with a checked checkbox labeled 'Allow sharing of Network Folders'.
- Sync Network Folder:** A section with a checked checkbox labeled 'Enable to sync of Network Folders using CloudSync'. An orange arrow points to this checkbox.
- Max. File Size Limit:** A section with a dropdown menu set to 'Units', a text input field containing '0', and a unit selector set to 'MB'. Below this is a warning: 'Specify maximum storage quota for file upload. 0 implies Unlimited quota. Warning: Renaming and editing files might fail if the limit is exceeded.'
- Number of old versions to keep for each file:** A text input field containing '3'. Below this is a note: 'Can be set to -1 to turn off versioning and prevent overwrite'.
- Skip Versioning For Files Greater Than:** A section with a dropdown menu set to 'Units', a text input field containing '9.54', and a unit selector set to 'MB'. Below this is a note: 'Files greater than this size will not be versioned'.

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.

Network Folder Details ✕

Network Folder Name	<input type="text" value="HR Docs"/>
Network Folder Path	<input type="text" value="C:\data\HR"/>
Permissions	<input style="border-bottom: 1px solid gray;" type="text" value="DEFAULT"/> ▼
Smart Mount	<input type="checkbox"/>
Disable Offline Sync	<input checked="" type="checkbox"/>
Disable Notifications	<input type="checkbox"/>
Sharing	<input style="border-bottom: 1px solid gray;" type="text" value="Allow All Shares"/> ▼
Allow Remote Deletion of Files via Offline Sync	<input type="checkbox"/>
Realtime Index for Automatic Sync and Search (Beta)	<input type="checkbox"/> <input type="button" value="Reindex"/>

Sharing Restrictions on Network Folders

To restrict sharing on network folder, following steps should be performed.

1. Navigate to "**Network Folders**" in the Administration panel and Click on the "**Edit**" button 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 is restricted to be shared.

The following are the option available to set Sharing for Network Folder:

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

Network Folder Details ✕

Network Folder Name

Network Folder Path

Permissions

Smart Mount

Disable Offline Sync

Disable Notifications

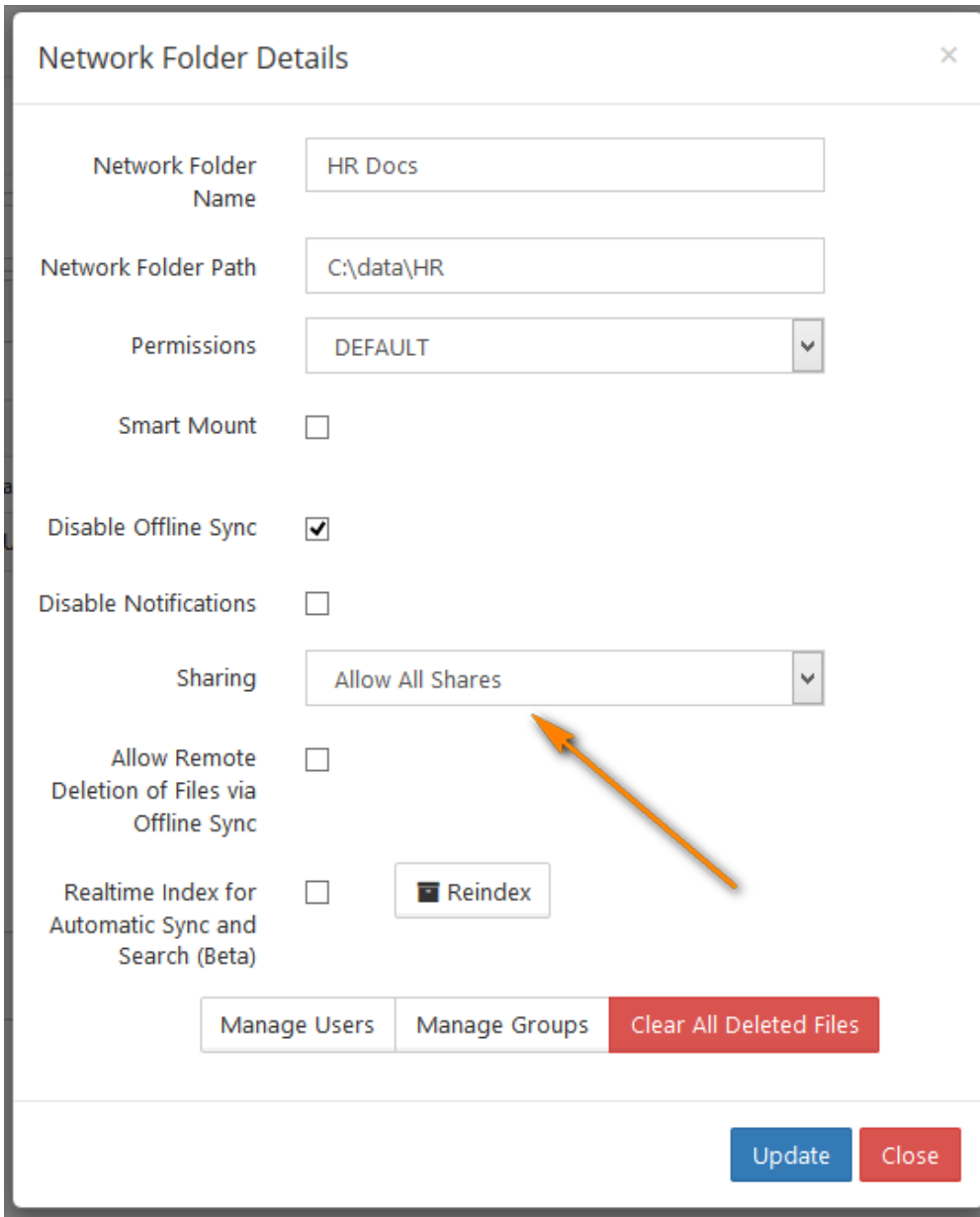
Sharing

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search (Beta) Reindex

Manage Users
Manage Groups
Clear All Deleted Files

Update
Close

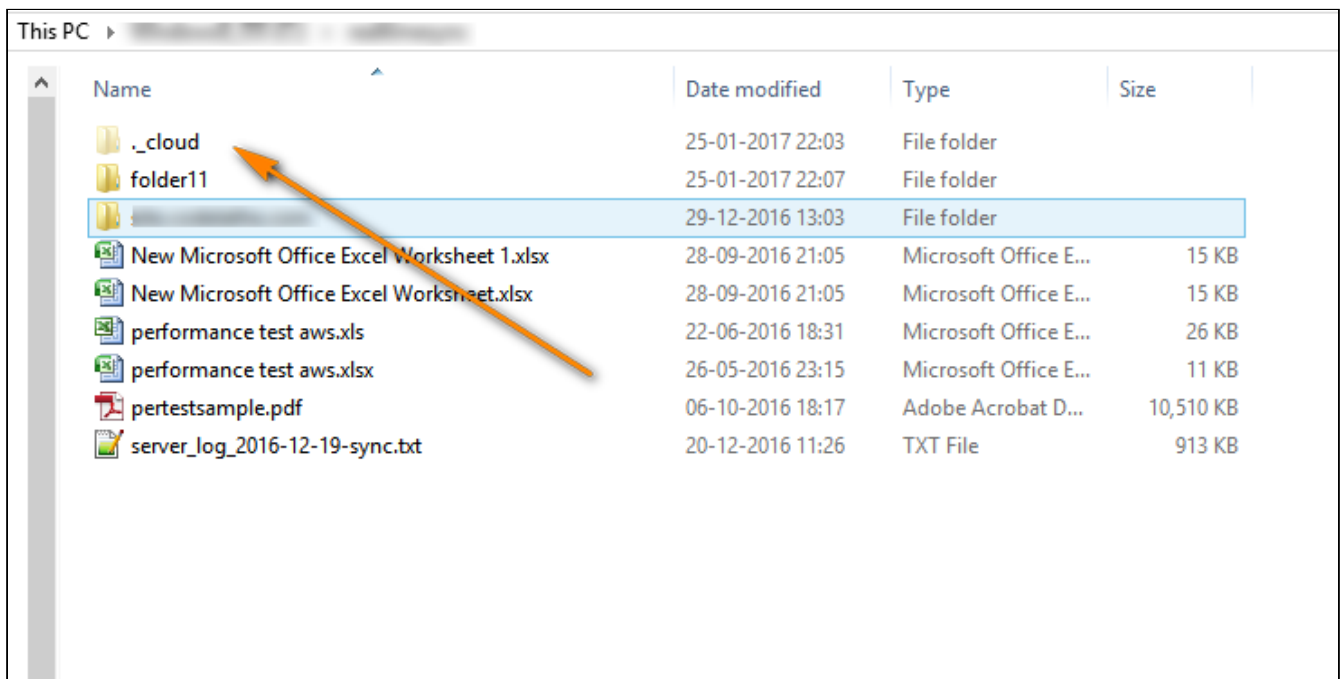


Miscellaneous: ._cloud Folder

Network folders at times will create a ._cloud sub folders for various reasons that include:-

- Store previous versions of Files
- Store the deleted files under that Network Folder
- Storing the image thumbnails.

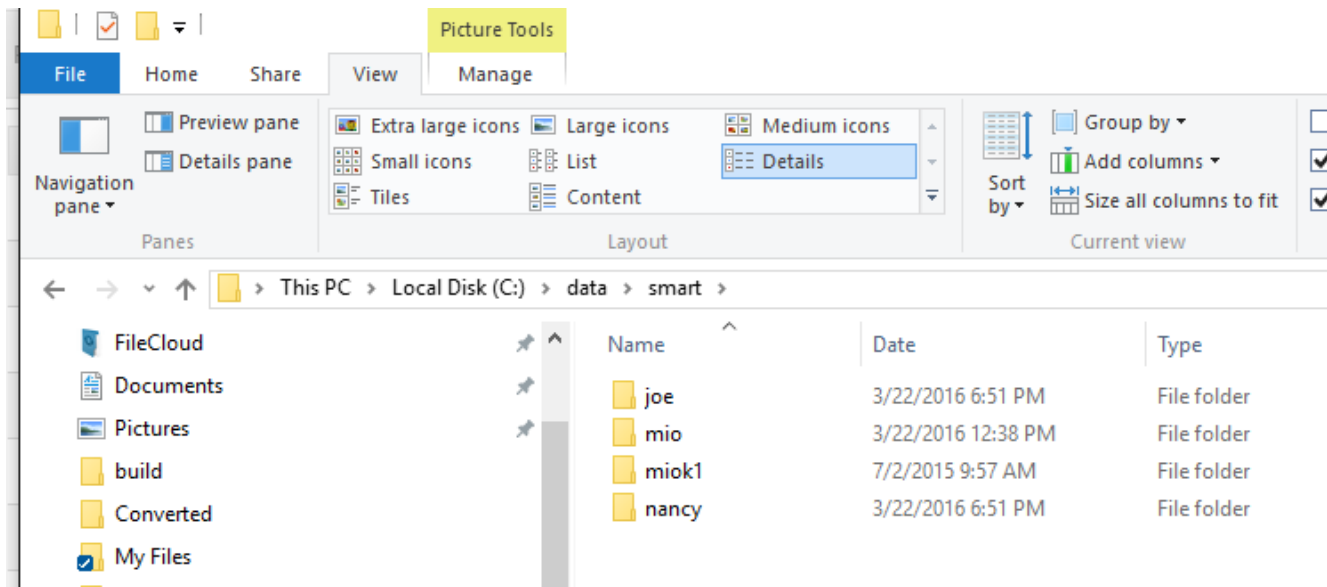
There is no option to automatically delete the ._cloud folder. However, the previous versions of the files can be deleted by the user and the stored deleted files can be emptied by the admin by using the Clear All Deleted Files in the screenshot above. Even if thumbnails are deleted, they will be recreated once the image file is accessed again through FileCloud interface.



Smart Mounted Network Folders

Smart mounts are special type of Network share whose file system paths contain variables. The variables will be translated to get 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 setup the Network share in such a way that:

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

To achieve this, create a network share with smart mount path like 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, the steps are

1. Navigate to "**Network Folders**" in the Administration panel and Click on the "**Add**" button
2. In the "**New Network Folder**" dialog, enter the Network Folder Name and select the "**Smart Mount**" checkbox. IGNORE THE "**Network Folder Path**" textbox
3. Set the "**Smart Mount Type**" to "Path Pattern" using the dropdown box
4. Enter the "Smart Mount" path in the "**Smart Mount Parameter**" text box
5. Click "**Add**" to create the smart mount
6. Select the newly created smart mount entry and assign access by clicking "Users" or "Groups" in the Network Share Details

i If you want to assign this to all users in the system, simply assign it to the EVERYONE group. The EVERYONE group is a special group which has all the members in the FileCloud system

Network Folder Details ✕

Network Folder Name

Permissions

Smart Mount

Smart mount path

Disable Offline Sync


Disable Notifications

Sharing

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search (Beta)

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:

- Step 1: please set permissions type to **NTFS**.

Network Folder Details

Network Folder Name*

Network Folder Path*

Permissions

Smart Mount

Enable ABE (NTFS)

Disable Offline Sync

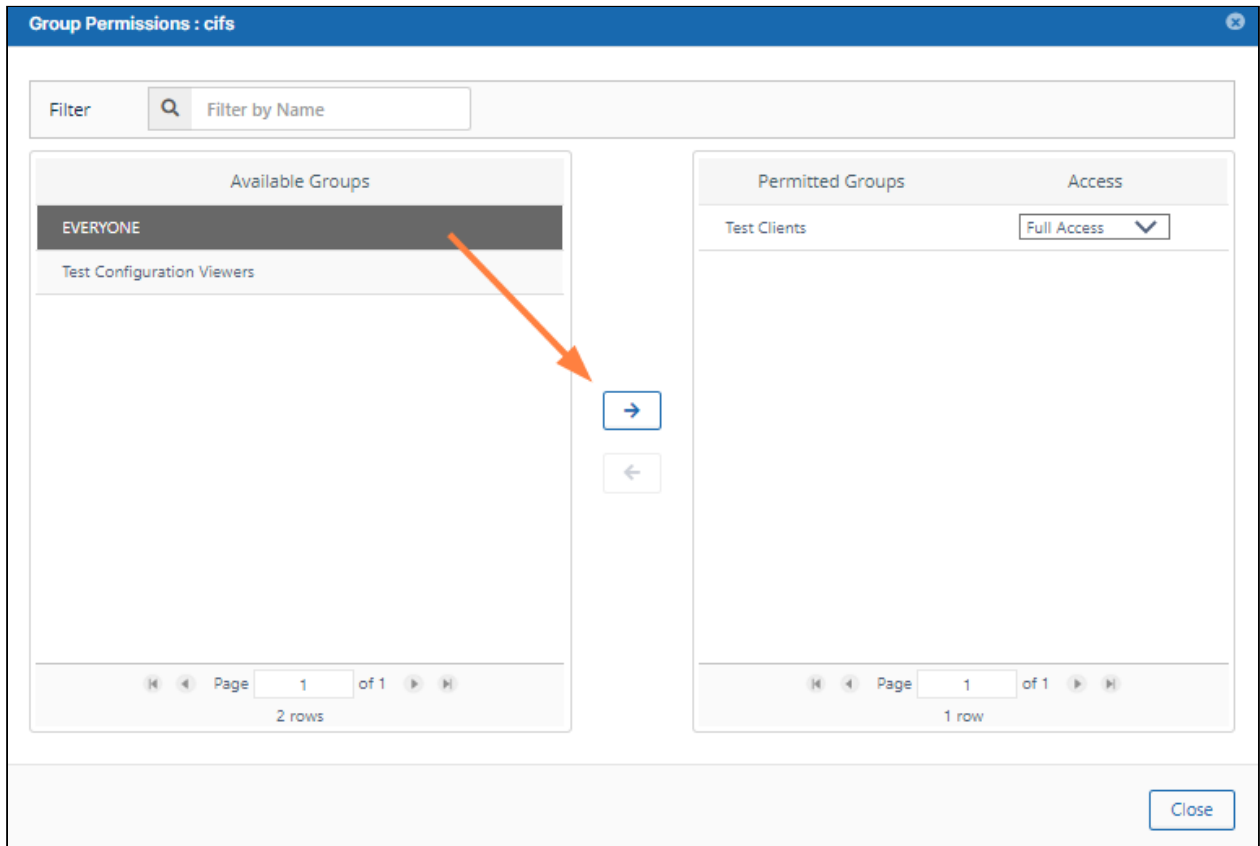
Disable Notifications

Sharing

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search

- Step 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.



- Step 3: If you are running FileCloud on Linux, you might need to **optionally** [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 authinitializecontextfromsid 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.

i 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 granular.

Permission Entry for Shared

Principal: FileCloud (FileCloud@filecloudserver.com) [Select a principal](#)

Type: Allow

Applies to: This folder only

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these permissions to objects and/or containers within this container [Clear all](#)

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

[Add a condition](#)

OK Cancel

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 don't have access by enabling Access Based Enumeration (ABE) settings.

To enable ABE, go to Admin Portal->Settings->Storage->Network Storage tab and enable the "Enable Access Based Enumeration for NTFS" checkbox. This will enable ABE globally.

To disable or enable ABE only for specific network folders you can open up the specific Network Folder Properties dialog. Admin Portal->Network Folders, click on "Edit" for a network folder.

The screenshot displays the FileCloud Server Administration interface. The left sidebar contains a navigation menu with categories: Folder Permissions, Notifications, DEVICES (Devices), GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), CUSTOMIZATION (Customization), and SYSTEM (Checks). The main content area is titled 'Storage' and has sub-tabs for 'My Files' and 'Network'. The 'Network' sub-tab is active, showing 'Network Storage Settings'.

The settings listed are:

- Network Folders Display Name:** Network Shares (Display name for Network Folders)
- Users Can Share Network Folders:** (Allow sharing of Network Folders)
- Sync Network Folder:** (Enable to sync of Network Folders using CloudSync)
- Number of old versions to keep for each file:** 3 (Can be set to -1 to turn off versioning and prevent overwrite)
- Skip Versioning For Files Greater Than:** 9.54 MB (Files greater than this size will not be versioned)
- Skip Names:** (Hide names that match the regular expression)
- Enable Access Based Enumeration For NTFS:** (Hide sub folders without read access in Network Folder (Applicate only for NTFS permissions based Network Folder))

An orange arrow points to the 'Enable Access Based Enumeration For NTFS' checkbox.

Select "Global Policy" to use the global setting, or use the "NO" or "YES" options to disable or enable ABE only for this

network share.

Network Folder Details

Network Folder Name*

Network Folder Path*

Permissions

Smart Mount

Enable ABE (NTFS)

Disable Offline Sync

Disable Notifications

Sharing

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search

Realtime Index Status

Search Index Status

Indexed entry count for search.

i NTFS permission checks reads 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 once in the memcache server.

For this caching to work, memcache server needs to be installed and running. By default, note that once permissions are cached, they are stored till memcache is restarted. So if you are changing any NTFS Permissions and want FileCloud to pick up the new permissions, make sure to restart the memcache service.

Network Folders	Allow sharing of Network Folders
Sync Network Folder	<input type="checkbox"/>
	Enable to sync of Network Folders using CloudSync
Number of old versions to keep for each file	<input type="text" value="3"/>
	Number of versions to store for Network share files
Skip Versioning For Files Greater Than	<input type="text" value="Units"/> <input type="text" value="0.009313225746154785"/> <input type="text" value="GB"/>
	Files greater than this size will not be versioned
Skip Names	<input type="text"/>
	Hide names that match the regular expression
Enable Access Based Enumeration For NTFS	<input checked="" type="checkbox"/>
	Hide sub folders without read access in Network Folder (Applicate only for NTFS permissions based Network Folder)
Enable Caching Of NTFS Permissions	<input checked="" type="checkbox"/>
	Use Memcache to cache NTFS Permissions

Guide to FileCloud Network folders with NTFS Permissions

Quick help on NTFS setup network share

This guide explains "Prerequisites and Basic steps " to set up NTFS on your network files. Common doubts 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, setup for various AD users and groups.

Please refer to network folder creation here: [Setting Up Network Folders](#)

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

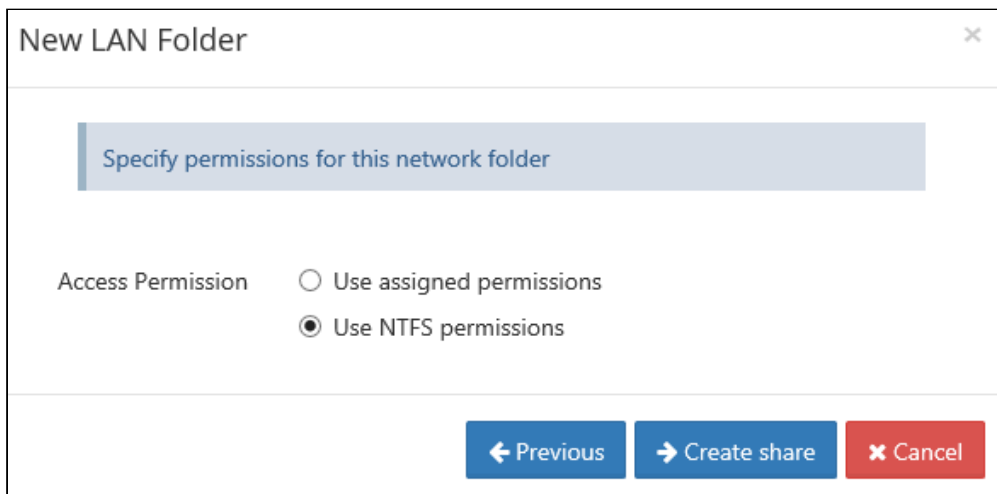
Pre-Requisites for NTFS setup

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

Please refer to network folder creation here: [Setting Up Network Folders](#)

Please note: If Web Server is running as a service, please make sure to have this running with a user account that has "Full control" permissions over the Network Share in NTFS.

1. NTFS is Applicable Only on network Folder with "NTFS permissions set" during network folder creation



Network Folder Details ✕

Network Folder Name	<input type="text" value="network local"/>
Network Folder Path	<input type="text" value="C:\FC local network"/>
Permissions	<div style="border: 1px solid black; padding: 2px;"> DEFAULT NTFS </div>
Smart Mount	<input type="checkbox"/>
Enable ABE (NTFS)	<input style="width: 100%;" type="text" value="Global Policy"/>

2. FileCloud Helper service (optional)

i **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 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

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

3. Content search of Documents for Network Folders in Windows and Linux Server

Optional

FileCloud Helper: Running SVC Start Stop [Install](#) [Config](#)


4. For more information on FileCloud Helper service refer to: [FileCloud Helper Service](#)

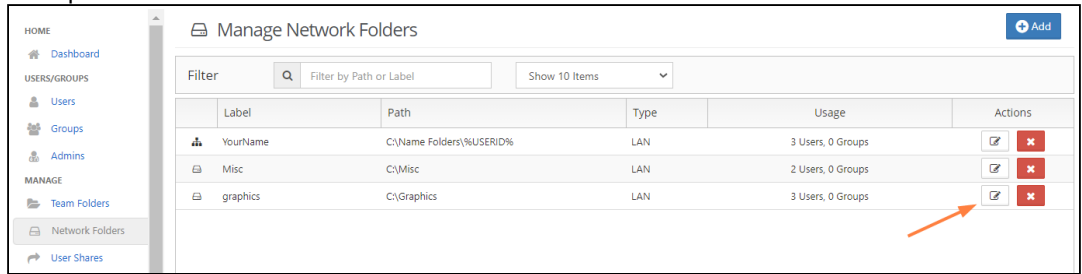
5. Assign users (AD Users)

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, Please refer to: [Active Directory Authentication](#)

Steps to give permissions:

- From Admin dashboard -> Network folders ; click the  icon of the network folder with NTFS permission.



The screenshot displays the 'Manage Network Folders' page. On the left is a navigation sidebar with categories: HOME (Dashboard), USERS/GROUPS (Users, Groups, Admins), and MANAGE (Team Folders, Network Folders, User Shares). The main content area has a title 'Manage Network Folders' and an 'Add' button. Below the title is a filter section with a search input and a 'Show 10 Items' dropdown. A table lists the network folders:

Label	Path	Type	Usage	Actions
YourName	C:\Name Folders%\%USERID%	LAN	3 Users, 0 Groups	 
Misc	C:\Misc	LAN	2 Users, 0 Groups	 
graphics	C:\Graphics	LAN	3 Users, 0 Groups	 

An orange arrow points to the edit icon in the Actions column for the 'graphics' folder.

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

Network Folder Details

Network Folder Name*

Network Folder Path*

Permissions

Smart Mount

Disable Offline Sync

Disable Notifications

Sharing

Allow Remote Deletion of Files via Offline Sync

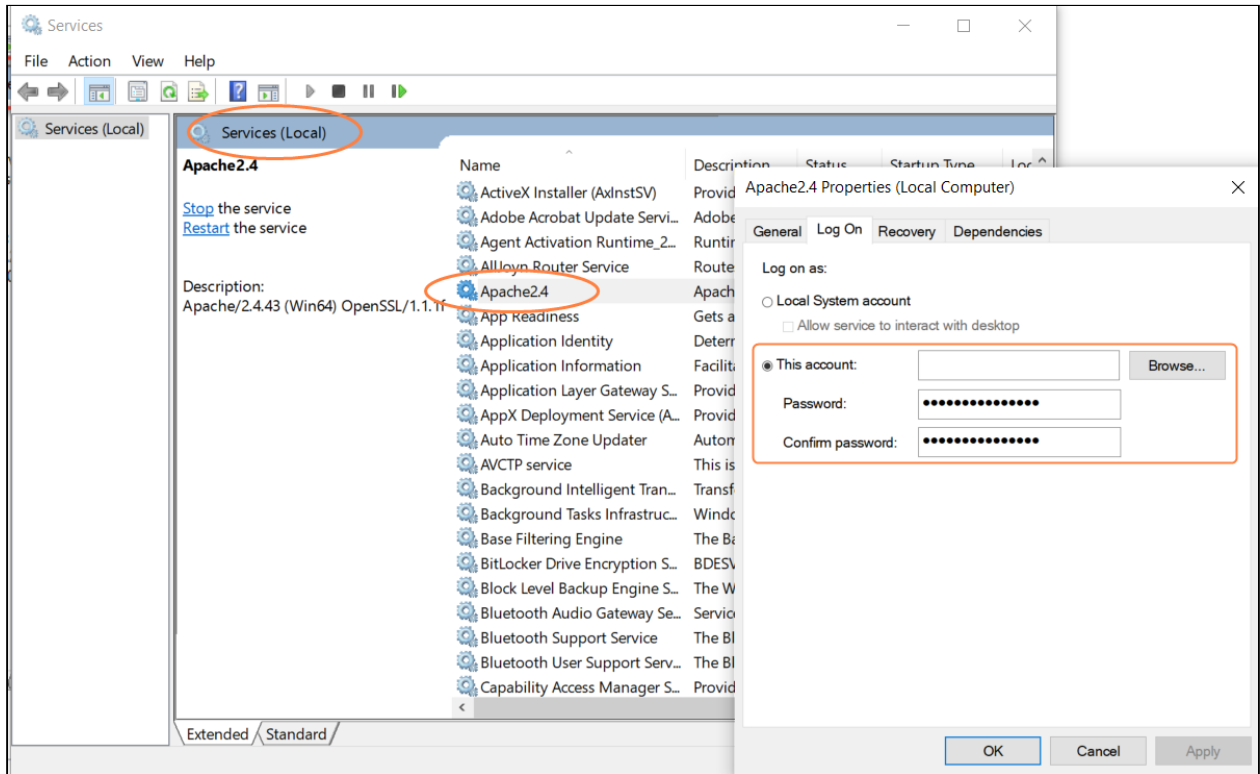
Realtime Index for Automatic Sync and Search

- Select users or groups to which permissions need to be given for this network folder. Only the AD users in the group, will be able to 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 "Total control" permissions on the Network Share.



2. Are there any restrictions or limitations on network folders?

- Yes, Please note that 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 article, the "Limits" section: [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 are passing this restriction.

3. Can a regular user be given access to NTFS Network folder?

Yes, the regular users can be given access, but they will not be able to see the sub folders 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?

Yes, by enabling Access Based Enumeration (ABE) settings on the Network folders.

For more info please refer to: [Network Folders with NTFS permissions](#)

5. What happens when a user permission is changed in AD ?

When user membership in a AD group is modified, that change is not propagated immediately and is cached by Windows. For more information, please check the following article: [Microsoft help](#)

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.

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 will still need the Helper Service to perform NTFS permission checks.

i 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 Server
- Content search of Documents for Network Folders in Windows and Linux Server

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);
```

- i** If Set Owner doesn't work, make sure to add the service account that runs the webserver to the local administrators group in your Windows file share servers or run it as a domain admin.

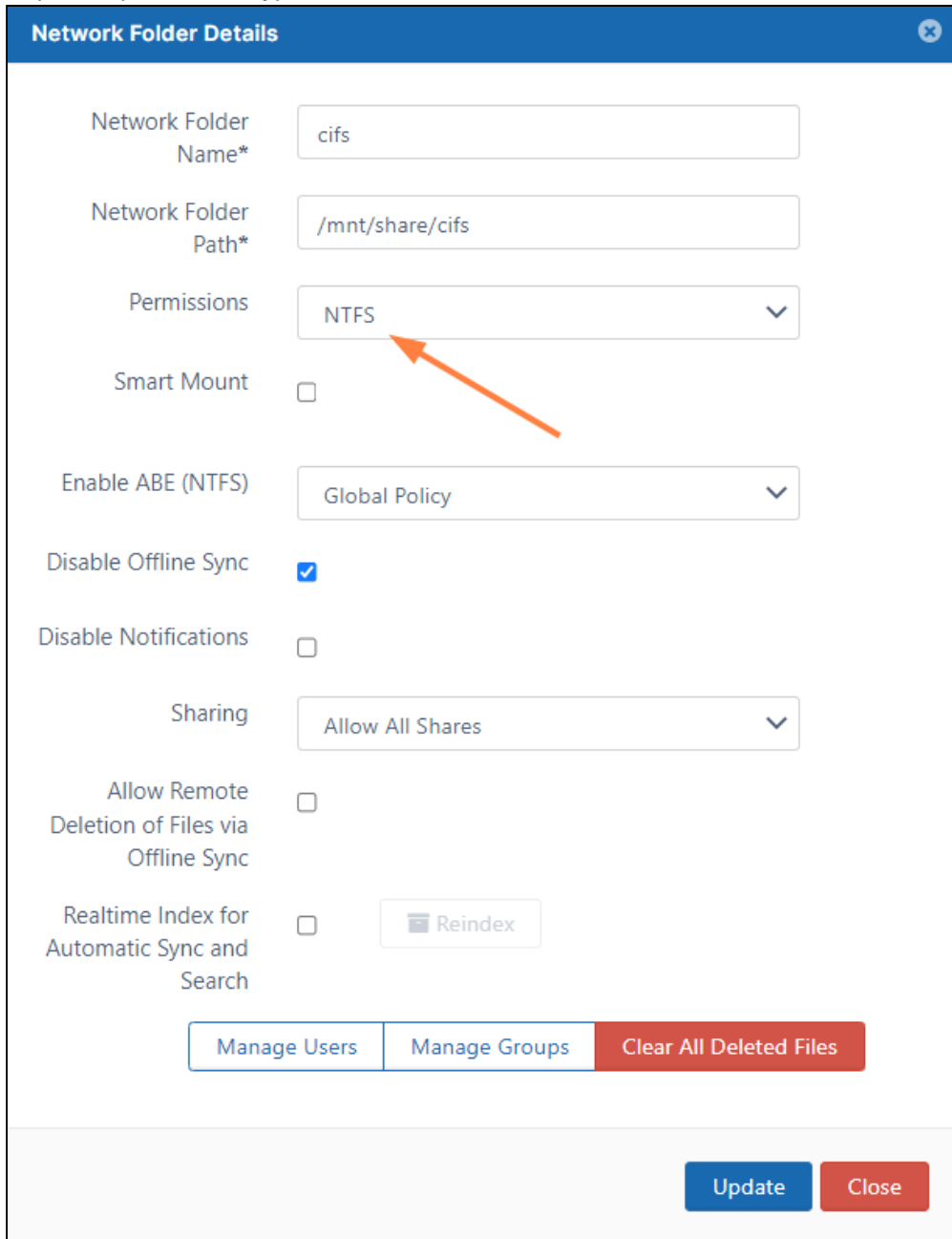
Network Folders with NTFS permissions [Staging]

- i**
- If you need to use Network Folders and preserve NTFS permissions, it is strongly recommended to run [FileCloud on Windows Servers instead of Linux](#).
 - If you are running FileCloud on Linux and want to preserve NTFS Permissions, a Windows Server running the FileCloud Helper Service is required (See more information)
 - Starting with FileCloud 15.0, it is recommended to install and use Memcache to improve performance when using network folders with NTFS permissions

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:

- Step 1: Set permissions type to **NTFS**:



Network Folder Details

Network Folder Name*

Network Folder Path*

Permissions

Smart Mount

Enable ABE (NTFS)

Disable Offline Sync

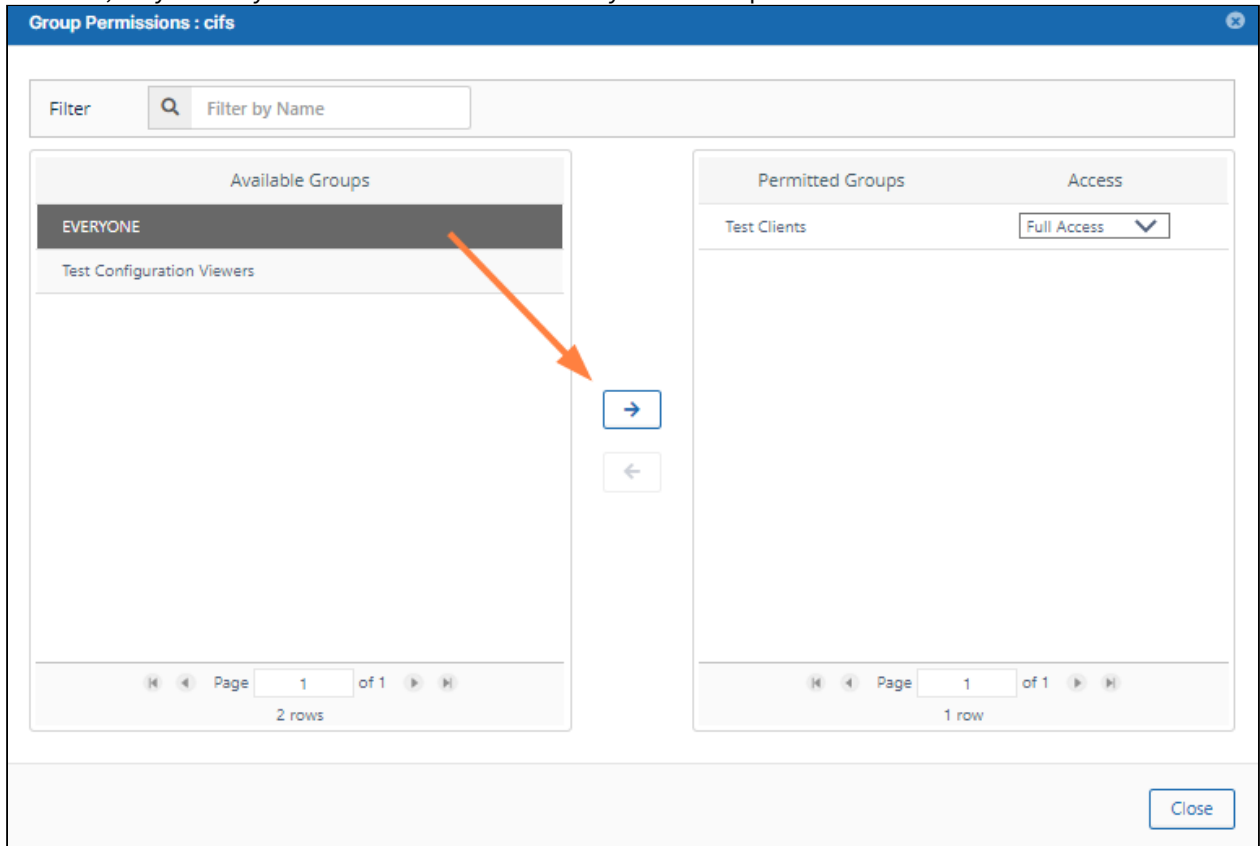
Disable Notifications

Sharing

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search

- Step 2: Click on Manage Users or Manage Groups and add users to the share as needed. For example, you might want to give 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.



- Step 3: If you are running FileCloud on Linux, you might need to **optionally** [configure and install the FileCloud helper service](#)

Additional Information and Troubleshooting

- **i** 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 authinitializecontextfromsid 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.

i 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 granular.

Permission Entry for Shared

Principal: FileCloud (FileCloud@filecloudserver.com) [Select a principal](#)

Type:

Applies to:

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these permissions to objects and/or containers within this container

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

[Add a condition](#)

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

i Use Qualified names in multidomain AD networks

Most organizations that have more than one domain have a legitimate need for users to access shared resources that are located in a different domain.

- Controlling this access requires that users in one domain can also be authenticated and authorized to use resources in another domain.
- To provide authentication and authorization capabilities between clients and servers in different domains, there must be a trust between the two domains.
- Trusts are the underlying technology by which secured Active Directory communications occur and are an integral security component of the Windows Server network architecture.

For example, in an organization called MyCompany, there are two internal domains: domainA and domainB.

- Active Directory communications between `domainA` and `domain` occur through a trust
- `USER1` is authenticated in `domainA`
- There is a shared NTFS permissions based LAN folder on `domainA`
- Suppose FileCloud is installed on `domainB` and a `USER1` wants to logon and access the Shared folder on `domainA`, FileCloud needs to do verification of NTFS permissions using a fully qualified username which looks like `USER1@domainA` instead of just `USER1`.

A Fully Qualified User Name is required in this case to correctly look up the User Name who is not in the current domain that FileCloud is running on.

To configure FileCloud Server to use qualified user names:

1. On the FileCloud server, navigate to the following directory:

```
c:\xampp\htdocs\config
```

2. Open the following file for editing:

```
cloudconfig.php
```

3. Add the following line:

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

4. Save and close the file.

NTFS Network Folders with Access Based Enumeration

When using Network Folders with NTFS permissions, it is possible to automatically hide folders that users don't have access by enabling Access Based Enumeration (ABE) settings.

To enable ABE, go to Admin Portal->Settings->Storage->Network Storage tab and enable the "Enable Access Based Enumeration for NTFS" checkbox. This will enable ABE globally.

To disable or enable ABE only for specific network folders you can open up the specific Network Folder Properties dialog. Admin Portal->Network Folders, click on "Edit" for a network folder.

Server **Storage** Authentication Admin Database Email Endpoint Backup

My Files **Network**

Network Storage Settings

Network Folders Display Name

Display name for Network Folders

Users Can Share Network Folders

 Allow sharing of Network Folders

Sync Network Folder

 Enable to sync of Network Folders using CloudSync

Max. File Size Limit ⓘ

Units ▾ 0 MB

Specify maximum storage quota for file upload. 0 implies Unlimited quota. Warning: Renaming and editing files might fail if the limit is exceeded.

Number of old versions to keep for each file

Can be set to -1 to turn off versioning and prevent overwrite

Skip Versioning For Files Greater Than

Units ▾ 9,54 MB

Files greater than this size will not be versioned

Skip Names

Hide names that match the regular expression

Enable Access Based Enumeration For NTFS

 Hide sub folders without read access in Network Folder (Applicate only for NTFS permissions based Network Folder)

Select "Global Policy" to use the global setting, or use the "NO" or "YES" options to disable or enable ABE only for this network share.

Network Folder Details ✕

Network Folder Name*

Network Folder Path*

Permissions ▼

Smart Mount

Enable ABE (NTFS) ▼

Disable Offline Sync

Disable Notifications

Sharing ▼

Allow Remote Deletion of Files via Offline Sync

Realtime Index for Automatic Sync and Search

Realtime Index Status

Search Index Status


Indexed entry count for search.

i NTFS permission checks reads 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 once in the memcache server. For this caching to work, memcache server needs to be installed and running. By default, note that once permissions are cached, they are stored till memcache is restarted. So if you are changing any NTFS Permissions and want FileCloud to pick up the new permissions, make sure to restart the memcache service.

Number of old versions to keep for each file	<input type="text" value="3"/>
	Number of versions to store for Network share files
Skip Versioning For Files Greater Than	Units ▾ <input type="text" value="0.009313225746154785"/> GB
	Files greater than this size will not be versioned
Skip Names	<input type="text"/>
	Hide names that match the regular expression
Enable Access Based Enumeration For NTFS	<input checked="" type="checkbox"/>
	Hide sub folders without read access in Network Folder (Applicate only for NTFS permissions based Network Folder)
Enable Caching Of NTFS Permissions	<input checked="" type="checkbox"/> 
	Use Memcache to cache NTFS Permissions

Indexing of Network Folders

Introduction

Unlike Managed Storage, network folder files exist outside of FileCloud and therefore changes occurring in the network folders might not be propagated into 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 "Logon as" user is set to 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 on the "Helper Status" button and ensure the status shows as realtime indexing is enabled.

Helper Status ×

Helper Version: 8
Running as user account: SYSTEM

Realtime Indexing is ENABLED
== REALTIME INDEXING STATUS ==

/EXTERNAL/Local
Path: C:\data\networkfolders\local
Total Realtime Records: 740
Active Realtime Files: 740
Recent Changes: 740

Close

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

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

- Now add a network folder and edit the settings to enable "realtime scanning"


Network Folder Details ✕

Network Folder Name*	<input type="text" value="Misc"/>
Network Folder Path*	<input type="text" value="\Misc"/>
Permissions	<input style="border-bottom: 1px solid #ccc;" type="text" value="DEFAULT"/>
Smart Mount	<input type="checkbox"/>
Disable Offline Sync	<input type="checkbox"/>
Disable Notifications	<input type="checkbox"/>
Sharing	<input style="border-bottom: 1px solid #ccc;" type="text" value="Allow All Shares"/>
Allow Remote Deletion of Files via Offline Sync	<input type="checkbox"/>
Realtime Index for Automatic Sync and Search	<input checked="" type="checkbox"/> <input type="button" value="Reindex"/>
Realtime Index Status	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between;"> 0 Folders, 0 Files Check </div>
Search Index Status	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between;"> 0 Check </div> <p style="font-size: small; margin-top: 2px;">Indexed entry count for search.</p>

- Always, restart the NTFS helper after enabling realtime index options for network folders or after adding or removing network folders
- If indexing is happening correctly, you will soon see the Realtime Index Status containing stats of the indexed files and folders.

Network Folder Details ✕

Network Folder Name	<input type="text" value="Local"/>
Network Folder Path	<input type="text" value="C:\data\networkfolders\local"/>
Permissions	<input type="text" value="DEFAULT"/>
Smart Mount	<input type="checkbox"/>
Disable Offline Sync	<input type="checkbox"/>
Disable Notifications	<input type="checkbox"/>
Sharing	<input type="text" value="Allow All Shares"/>
Allow Remote Deletion of Files via Offline Sync	<input type="checkbox"/>
Realtime Index for Automatic Sync and Search (Beta)	<input checked="" type="checkbox"/> <input type="button" value="Reindex"/>
Realtime Index Status	<input type="text" value="30 folders, 710 files"/> <input type="button" value="Check"/>



Searching in Network Folders

FileCloud will normally search Network Folders by searching the files and folders directly recursively in the operating system and it can take considerable time for large folders with many number of 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](#).

FileCloud supports indexed search for files in managed storage. Starting with 11.0, FileCloud supports indexed search for network folder to speed up search process. Enabling this function can significantly improve searching speed for indexed network folders. By default, searching for Files in Network Folders will not use indexed search therefore the files will be searched directly on the OS which takes considerable time for large folders with large number of files.

To enable Indexed Search in Network Folders:

1. In the admin portal, go to **Settings > Storage > Network**.
2. Scroll to the bottom of the **Network** tab, and check the **Enable Indexed Search** checkbox .

Enable Access Based Enumeration For NTFS

Hide sub folders without read access in Network Folder (Applicate only for NTFS permissions based Network Folder)

Enable Caching Of NTFS Permissions

Use Memcache to cache NTFS Permissions

NTFS Permissions Cache Expiry

NTFS Permissions Cache Expiry in seconds (0 means no expiry)


Store Deleted Files In Network Folder

Enable recycle bin support for LAN based Network Folders. This option will take more space to store deleted files.

Do Not Store Deleted Files Greater Than

Units ▾ 100 MB

Permanantly delete Network Folder files greater than the specified size.

 **Enable Indexed Search**

Enable search index for LAN based Network Shares. Requires 'Real time indexing' to be enabled for Network Share and Requires FileCloud Helper service to be configured.

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

4. Edit each Network Folder that you want to apply indexed searching to and check **Enable Indexed Search**.

Network Folder Details [X]

Network Folder Name: HR Docs

Network Folder Path: C:\data\HR

Permissions: DEFAULT [v]

Smart Mount:

Disable Offline Sync:

Disable Notifications:

Sharing: Allow All Shares [v]

Allow Remote Deletion of Files via Offline Sync:

Realtime Index for Automatic Sync and Search (Beta): [Reindex]

Realtime Index Status: 0 folders, 0 files [Check]

[Manage Users] [Manage Groups] [Clear All Deleted Files]

[Update] [Close]

Web Server Permissions for Network Shares

FileCloud Web Server, forchestrator and Document Preview permissions on Windows

⚠ To properly make Network Folders accessible via FileCloud, the FileCloud Web Server, forchestrator, cron, and Document Preview services must run as accounts with full permissions on Network Folders, otherwise there may be problems accessing network shares.

To configure this, run the Web Server and forchestrator as Windows services.

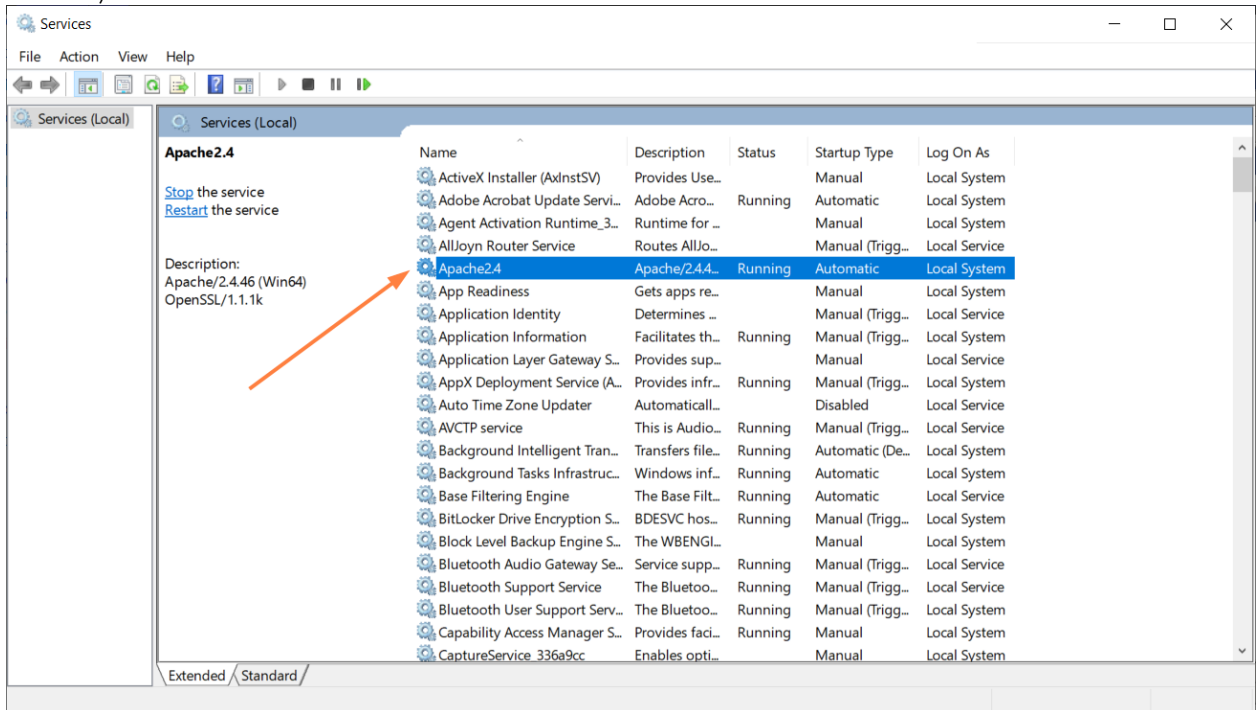
1. In the **FileCloud Control Panel**, click on the **Make Service** link.

The screenshot shows the FileCloud Control Panel interface. At the top, it displays the version (v: 21.2.0.16651) and base components (21.1.1.15106). Below this, there are links for 'Initial Setup' (Install Check) and 'Web Portal' (Admin Portal, User Website). The main section is titled 'Servers' and lists several services:

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

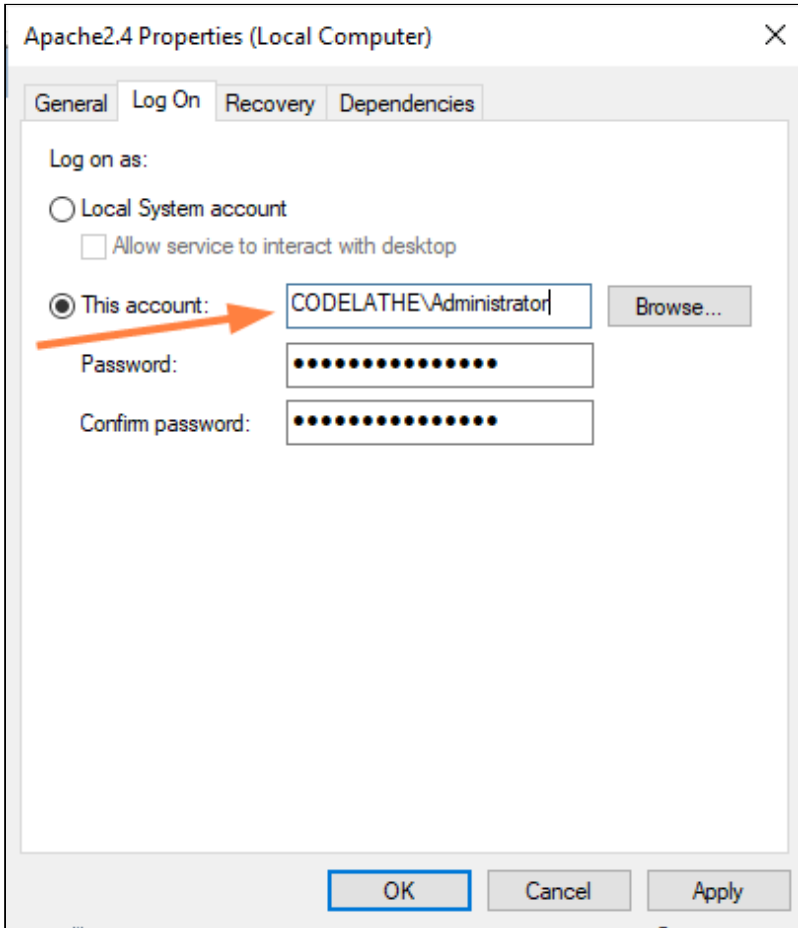
An orange arrow points to the 'Message Queue' service, with the text 'Message Queue = forchestrator service' written next to it. Below the 'Servers' section is an 'Optional' section with services like FileCloud Helper, Memcache, Document Preview, and Content Search. At the bottom, there are sections for 'Miscellaneous' (Configuration, SSL) and 'Technical Support' (Need Help?, Documentation, Contact Support, Demo and Training).

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



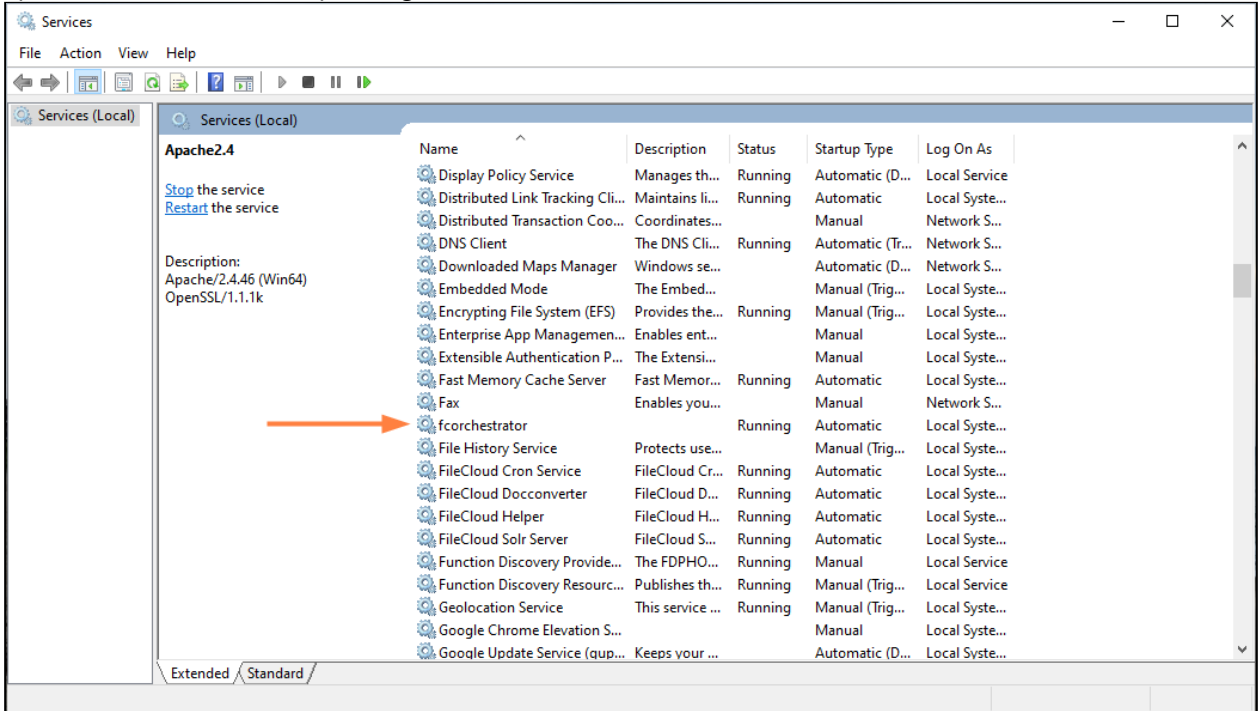
3. Right-click on the service and choose **Properties**.
4. In the **Properties** dialog box, click the **Log On** tab.

5. Set **This account** to an AD user that has full access to the network share.



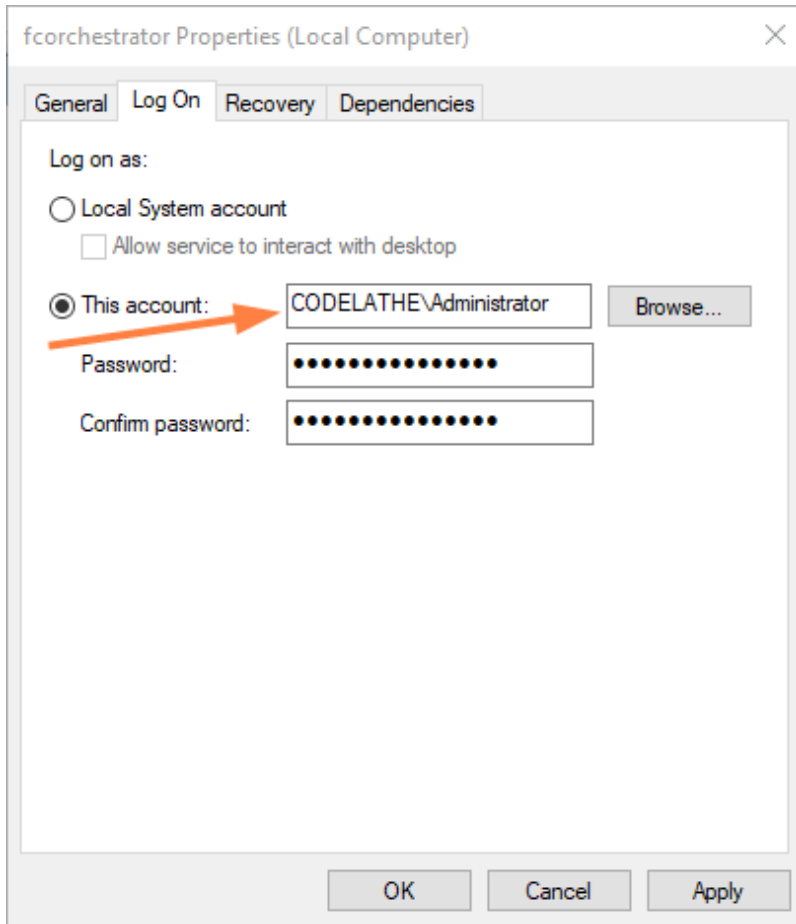
6. Restart the service. Now the Web server is running as a user account with full access to the network share.

7. Open the Windows **Services** panel again, and access the **forchestrator** 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.



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

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


- There is no versioning support (version key is ignored and file will be overwritten).
- No real time network sync or indexed search is allowed (regular file search works).

What do you want to do?

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

Create a Network Folder Based on an Amazon S3 Bucket

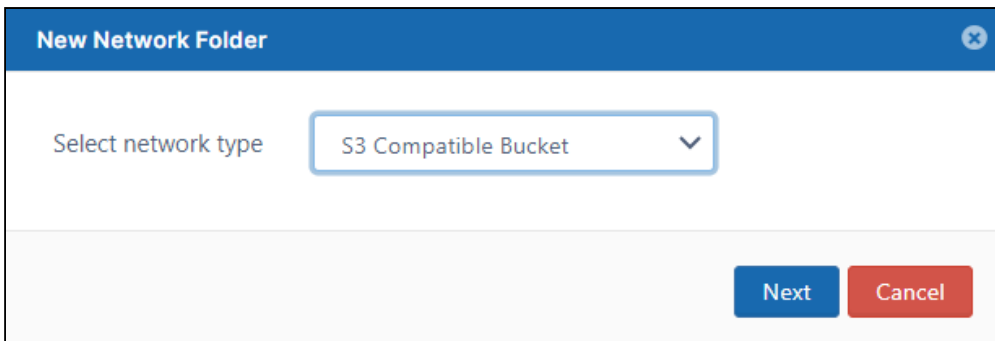
Administrators can integrate Amazon's AWS S3 buckets with FileCloud Server to give users access to this data inside FileCloud Server portals and clients.

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

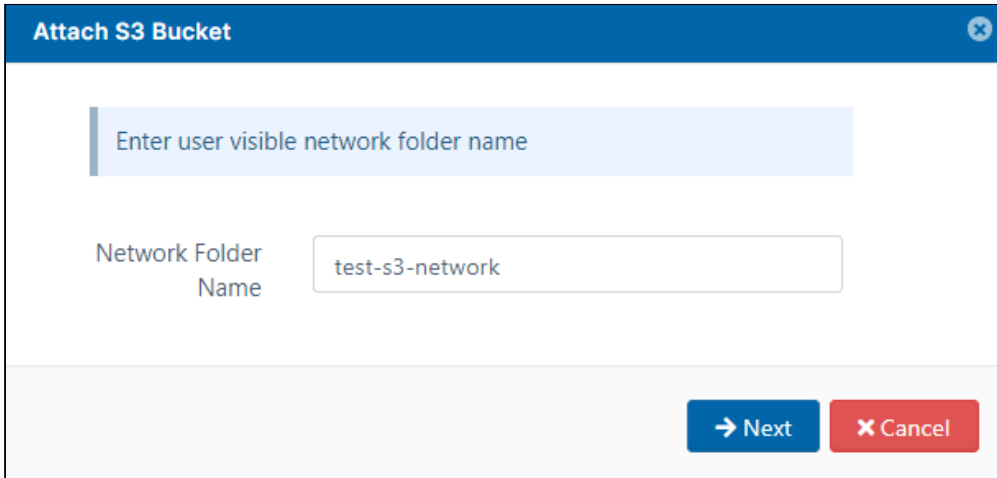
1. There is no versioning support (version key is ignored and file is overwritten).
2. No real time network sync or indexed search is allowed (regular file search works).

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**.

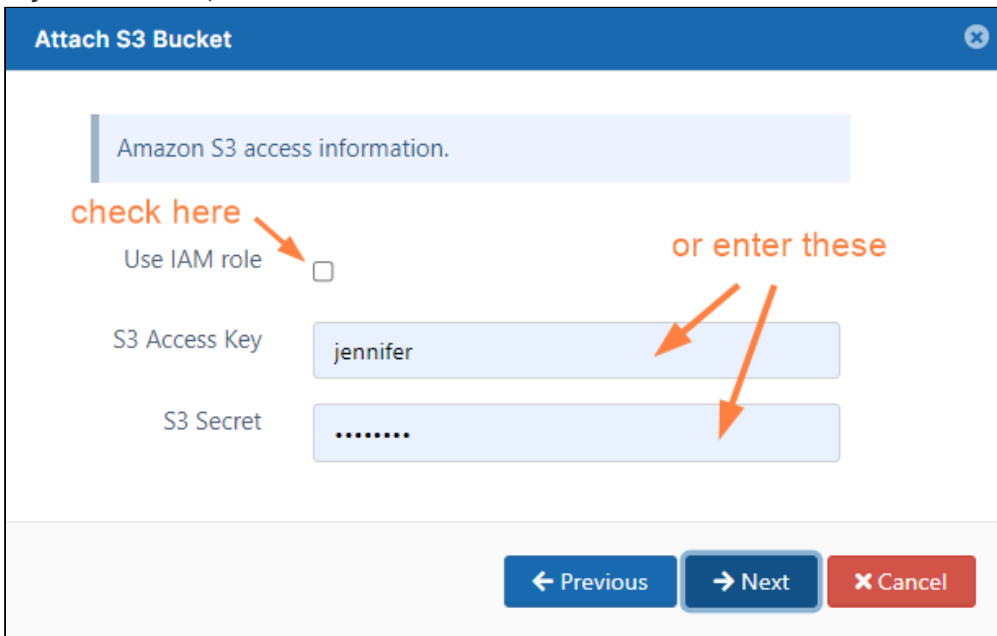


5. On the **Attach S3 Bucket** window, type in a unique **Network Folder Name** and then click **Next**.



The screenshot shows a window titled "Attach S3 Bucket" with a blue header and a close button. Below the header is a light blue box with the text "Enter user visible network folder name". Underneath, the label "Network Folder Name" is followed by a text input field containing "test-s3-network". At the bottom right, there are two buttons: a blue "Next" button with a right-pointing arrow and a red "Cancel" button with a close icon.

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**.



The screenshot shows the "Attach S3 Bucket" window with a blue header and a close button. Below the header is a light blue box with the text "Amazon S3 access information.". Underneath, there is a checkbox labeled "Use IAM role" with the text "check here" and an orange arrow pointing to it. Below the checkbox are two text input fields: "S3 Access Key" containing "jennifer" and "S3 Secret" containing ".....". There is text "or enter these" with two orange arrows pointing to the "S3 Access Key" and "S3 Secret" fields. At the bottom, there are three buttons: a blue "Previous" button with a left-pointing arrow, a blue "Next" button with a right-pointing arrow, and a red "Cancel" button with a close icon.

7. On the **Attach S3 Bucket** window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:

The screenshot shows the 'Attach S3 Bucket' window with a blue header and a close button. A light blue box contains the text: 'Encryption Settings. Applicable only to newly added files and does not affect existing files'. Below this, the 'S3 Encryption Setting' label is next to a dropdown menu. The dropdown menu is open, showing four options: 'Amazon S3-Managed Key Encryption' (selected), 'No Encryption', 'Amazon S3-Managed Key Encryption', and 'Amazon KMS-Managed Key Encryption'. At the bottom, there are three buttons: 'Previous' (blue), 'Next' (blue), and 'Cancel' (red).

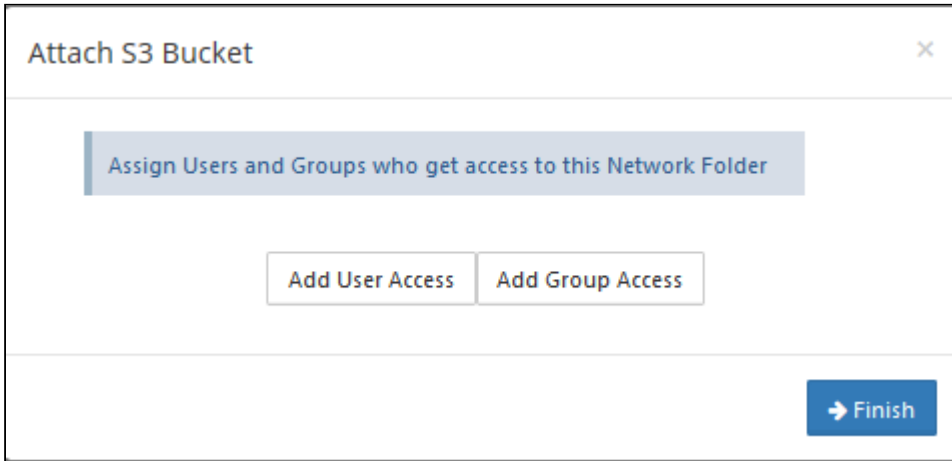
8. On the **Attach S3 Bucket** window, type in the **Bucket** name, **Region**, and optionally the **End Point** and **Prefix**.
9. Click **Next**.

The screenshot shows the 'Attach S3 Bucket' window with a blue header and a close button. A light blue box contains the text: 'Information to connect to your Bucket'. Below this, there are four input fields: 'Bucket' (containing 's3bucket'), 'End Point' (containing 'OPTIONAL: (ex) https://s3.amazonaws.com'), 'Region' (containing 'us-east-1'), and 'Prefix' (containing 'OPTIONAL: (ex) folder1/sub1'). At the bottom, there are three buttons: 'Previous' (blue), 'Next' (blue), and 'Cancel' (red).

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 Server Network Folder, you can update any of the original settings.

S3 Network Folder Details ✕

S3 Key*

S3 Secret*

Use IAM role

Network Folder Name*

Bucket Name*

End Point

S3 Region

Prefix

S3 Encryption Setting ▼

Disable Offline Sync

Disable Notifications

Sharing ▼


Allow Remote Deletion of Files via Offline Sync

Manage Users
Manage Groups
Clear All Deleted Files

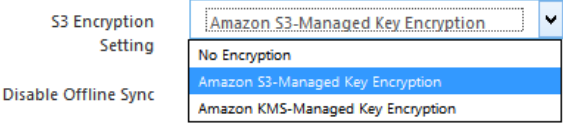
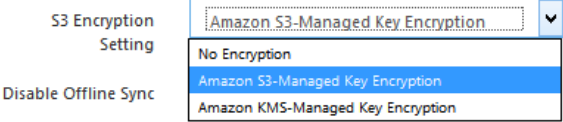
Update
Close


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	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	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 TONIDOCLLOUD_S3_USE_PATH_STYLE_ENDPOINT in the file <code>amazons3storageconfig.php</code> 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
<p>S3 Encryption Setting</p>	<p>No Encryption</p> <p>When this option is set the files in the S3 network share are not encrypted.</p> <p>Amazon S3-Managed Key encryption</p> <p>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.</p> <p>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.</p> <p>Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.</p> <div style="text-align: right;">  <p>S3 Encryption Setting Disable Offline Sync</p> </div> <p>Amazon KMS-Managed Key Encryption</p> <p>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.</p> <div style="text-align: right;">  <p>S3 Encryption Setting Disable Offline Sync</p> </div> <p>Note: Unlike S3 managed storage encryption, enabling encryption in Network Shares encrypts only newly added files and does not encrypt existing files.</p>
<p>Disable Offline Sync</p>	<p>Enabling this option will prevent this network share from being available for sync via FileCloud sync client</p>
<p>Disable Notifications</p>	<p>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.</p>

Option	Description
Sharing	Sharing the content of the network share can be disabled or enabled using this option <div style="text-align: right; margin-top: 10px;">  </div>
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.

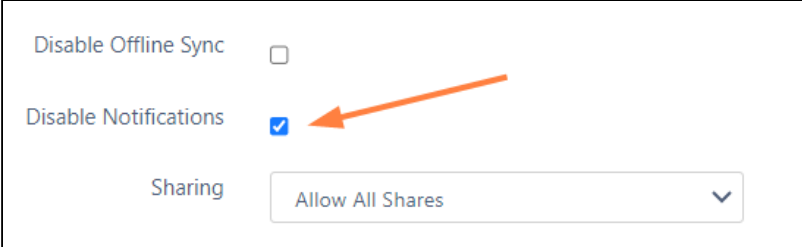
Disable notifications for Amazon S3 Network Folders

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.



The screenshot shows a dialog box with the following elements:

- Disable Offline Sync** with an unchecked checkbox.
- Disable Notifications** with a checked checkbox, highlighted by an orange arrow.
- Sharing** dropdown menu set to **Allow All Shares**.

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](#).


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 recycle bin (if enabled).
- The files in recycle bin will 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**.

S3 Network Folder Details ✕

S3 Key*

S3 Secret*

Use IAM role

Network Folder Name*

Bucket Name*

End Point

S3 Region

Prefix

S3 Encryption Setting ▼

Disable Offline Sync


Disable Notifications

Sharing ▼

Allow Remote Deletion of Files via Offline Sync



Azure Blob Storage Based Network Folders

 The ability to mount an existing Azure Blob Container as a Network Folder is available in FileCloud Server version 19.2 and later.

Administrators can integrate Azure's 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.), you first create a Blob Storage container in one of the Azure Regions.

You can then upload any number of objects to the bucket.

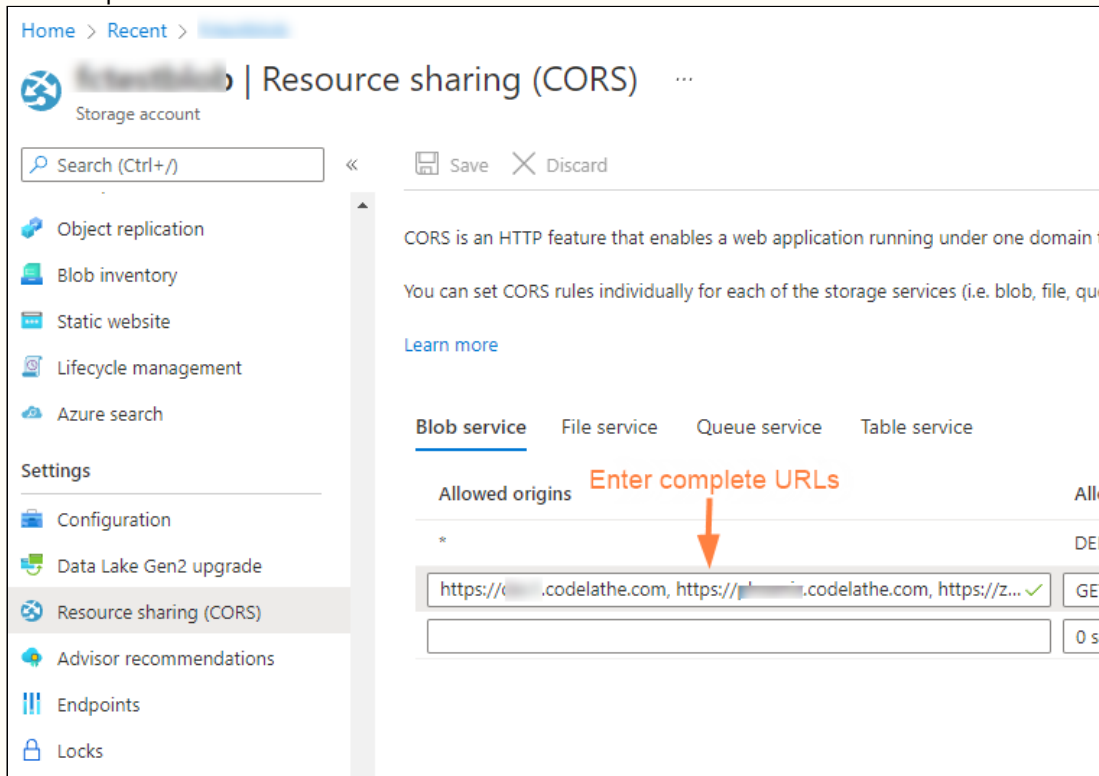
[Working with Azure Blob Storage](#)

 There are 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. No real time network sync or indexed search is allowed (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:



What do you want to do?

Attach Azure Blob Storage container to a Network Folder	➔ Create a Network Folder for the Azure Blob Storage
Configure the container-based Network Folder	➔ Configure Azure Blob Storage Network Folder ➔ Clear All Deleted Files

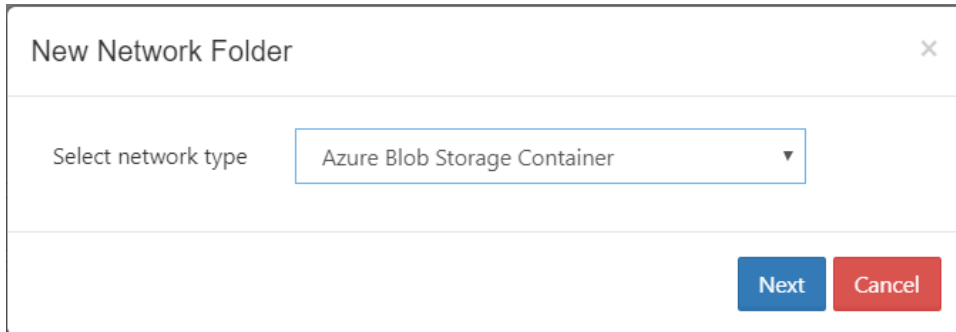
Create a Network Folder Based on an Azure Blob Storage

i The ability to mount an existing Azure Blob Storage container as a Network Folder is available in FileCloud Server version 19.2 and later.

Administrators can integrate Azure Blob Storage container 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 Azure Blob Storage network folders

1. No versioning support (Version key will be ignored and file will be overwritten)
2. No real time network sync or indexed search is allowed (Regular file search will work)

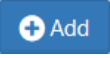


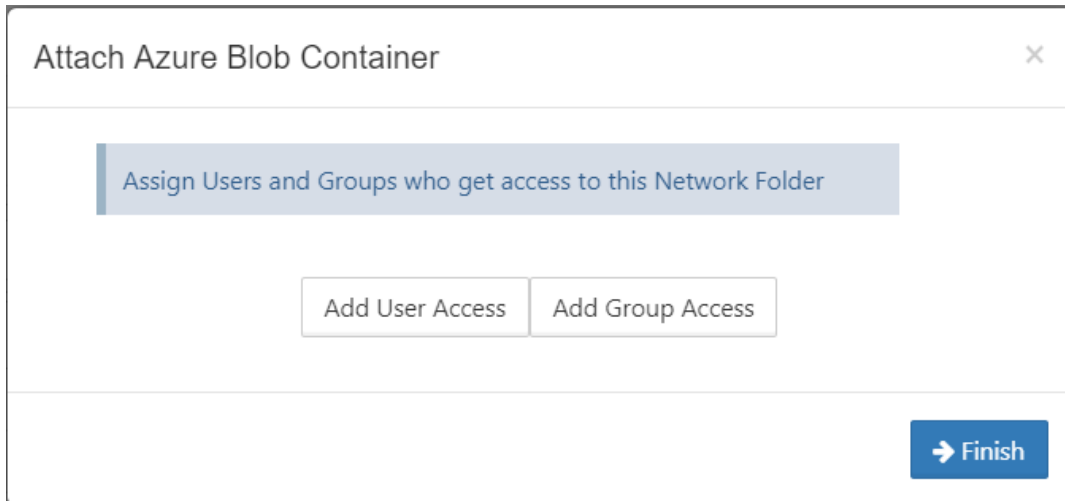
New Network Folder

Select network type: Azure Blob Storage Container

Next Cancel

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 the **Enter User Visible Network Folder name** step, type in a unique name for the Network Folder and then click Next.
6. In the **Azure Blob Storage access information** step, type in the authentication credentials in Azure - Account Name and Account Key, and then click Next.
7. In the **Information to connect to your container** step, type in the Container Name and (optional) the Endpoint Suffix, and then click Next
8. When the Azure Blob Storage container 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 Access User](#)
 - c. [User Group](#)



Configure Azure Blob Storage Container-Based Network Folders

i The ability to mount an existing Azure Blob Storage container as a Network Folder is available in FileCloud Server version 19.2 and later.

After you attach an Azure Blob Storage container to a FileCloud Server Network Folder, you can update any of the original settings.

Azure Blob Network Folder Details
✕

Account Name

storageaccount

Account Key

.....

Network Folder Name

azure-nsa

Container Name

fc-networkshare

Endpoint Suffix

OPTIONAL: (ex) core.windows.net

Disable Offline Sync

Sharing

Allow All Shares ▼

Allow Remote Deletion of Files via Offline Sync

Manage Users

Manage Groups

Clear All Deleted Files

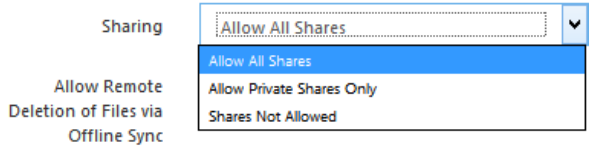
Update

Close

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 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
Account Key	Azure's Storage account key
Network Folder Name	Name of the network share

Option	Description
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 <div style="text-align: right; margin-top: 10px;">  </div>
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?

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

Azure Blob Network Folder Details
✕

Account Name

Account Key

Network Folder Name

Container Name

Endpoint Suffix

Disable Offline Sync

Sharing

Allow Remote Deletion of Files via Offline Sync

Manage Users


Manage Groups

Clear All Deleted Files

Update

Close

To clear deleted files in an S3 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 of sync folders with more than 5,000 folders or more is needed, 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 decrease the 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 cannot exceed 256 characters:** When using network folders on Windows, file paths cannot exceed 256 characters.
- **Very large amounts of content in Network Folders** can cause the folder listing to time out when end users view it in the user portal. The maximum size is determined by your environment's OS and resource limitations.

Enabling Directory Scraping

FileCloud allows you to share network folders with any number of users. If FileCloud is running on Windows OS but the 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. Log into the FileCloud admin portal.
 2. Navigate to **Settings > Misc > Directory Scraper**.
 3. Select the check box **Enable Directory Scraper**.
 4. Correct the system date format, if needed. See [Setting Date Format](#), below, for help finding your system date format.
 5. Click **Save**.
- Now network shares will use directory scraping to get file listings.

The screenshot displays the FileCloud Manage Settings interface. On the left is a vertical navigation sidebar with categories: HOME (Dashboard), USERS/GROUPS (Users, Groups, Admins), MANAGE (Team Folders, Network Folders, User Shares, Folder Permissions), DEVICES (Devices), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), and SETTINGS (Settings). The main content area is titled "Manage Settings" and features a horizontal menu with tabs: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, Policies, and SSO. Below this is a sub-menu with tabs: General, User, Password, Notifications, Share, Preview, Helper, Directory Scaper (selected), and Anti-Virus. Under the Directory Scaper tab, there are sub-sections for Duo Security and Privacy. The "Directory Scaper" section includes: "Enable Directory Scaper" (disabled checkbox), "Date Format" (text input field containing "d-m-Y hi"), and "Sample Output" (a "Show" button). Descriptive text explains that the Directory Scaper is an experimental module for speeding up file listing in network shares (Windows only) and that the date format is for the 'dir' command output.

Manage Settings

Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO

General User Password Notifications Share Preview Helper **Directory Scrapper** Anti-Virus

Duo Security Privacy

Directory Scrapper

Enable Directory Scrapper Enable an experimental module that speeds up file listing in network shares (only Windows).

Date Format Date format of 'dir' command output. [Format Help](#)

Sample Output Show sample of 'dir' command output from server.

```
Volume in drive C is OS
Volume Serial Number is 46F7-039F

Directory of C:\xampp\htdocs

27-04-2018 13:45 <DIR> .
27-04-2018 13:45 <DIR> ..
16-04-2018 07:07      1692 .htaccess
27-04-2018 08:09      1692 .htaccess_2018-04-27-08-09-18
27-04-2018 08:09 <DIR> admin
```

Use the above sample output to construct date format string

Setting Date Format

Since directory scraping relies on the exact location and format of the listing output to populate the directory listing, this can be an issue if the date format is different from the FileCloud default.

To set the correct date format, open the command prompt on the Windows server, and run a dir command.

```
c:\work\solr\solr-5.3.1\bin>dir
Volume in drive C has no label.
Volume Serial Number is D2AA-19F2

Directory of c:\work\solr\solr-5.3.1\bin

03/20/16 09:45 PM <DIR> .
03/20/16 09:45 PM <DIR> ..
10/29/15 09:51 AM <DIR> init.d
08/12/15 02:46 PM      8,293 install_solr_service.sh
08/12/15 02:46 PM      1,255 oom_solr.sh
08/12/15 02:46 PM      7,754 post
08/12/15 02:46 PM     47,759 solr
03/20/16 09:45 PM          6 solr-8983.port
08/12/15 02:46 PM     42,654 solr.cmd
08/12/15 02:46 PM      4,417 solr.in.cmd
08/12/15 02:46 PM      4,892 solr.in.sh
      8 File(s)      117,030 bytes
      3 Dir(s)     275,033,083,904 bytes free
```

Note the date format from the directory output. See [function.date.php](#) for help setting the correct value for the date format in the **Date Format** text box.

FileCloud Helper Service

You can use the FileCloud Helper service to perform the following important functions on Network folders:











- Handle NTFS Permission checks for Network Folders configured with NTFS permissions (Only needed under some conditions after v12.0)
- Provide an indexed search of Network Folders
- Allow content search of documents for Network Folders

Starting with 12.0

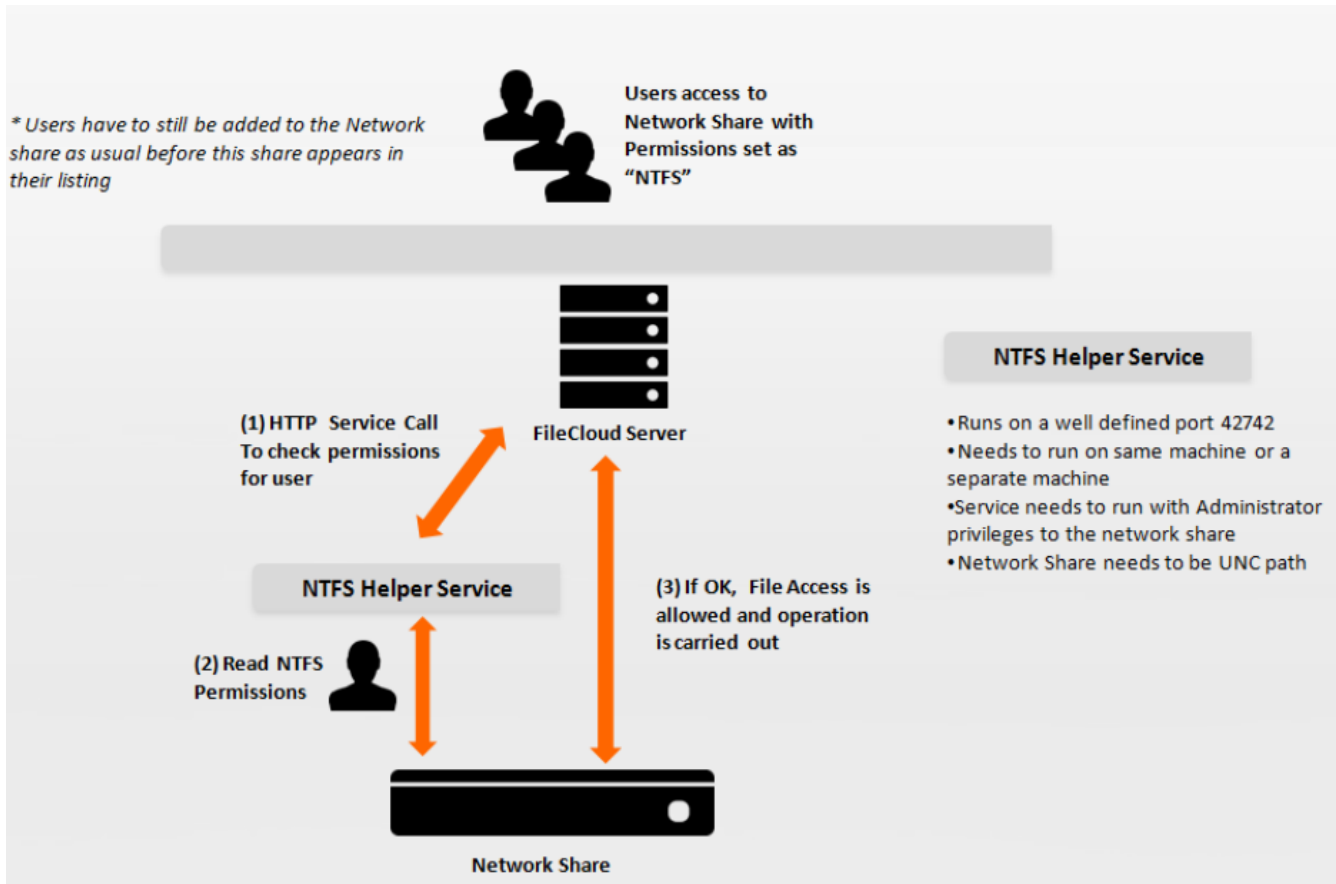
If you are running FileCloud on a Windows Server, you **do not need** the Helper Service for NTFS permission checks as the Web Server itself can perform access checks.

If you are running FileCloud on a Linux Server, you will still need the Helper Service to perform NTFS permission checks.

What Do You Want to Do?

	 Learn about FileCloud NTFS Helper Architecture
	 Install Helper Service
	 Run Server and Helper and Different Machines
	 Exclude Specific Folder Paths from Indexing
	 Improve Helper Performance

Helper Service Architecture



Install Helper Service

For FileCloud Server instances running on Windows, Helper Service is a separate installation.

FileCloud Control Panel

v: 17.3.0.37651, Base Components: 17.3.0.37625
 Webserver Ports: 80,443 Database Port: 27017

Initial Setup: [Install Check](#)

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

Servers

Webserver:	Running SVC	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Config	Make Service
Database:	Running	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Config	Make Service
Cron Task:	Running SVC	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Config	Install

Optional

FileCloud Helper:	Running SVC	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Install	Config
Memcache:	Not Running	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Make Service	
Document Preview:	Running SVC	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Install	
Content Search:	Running SVC	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	Install	

Miscellaneous

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


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

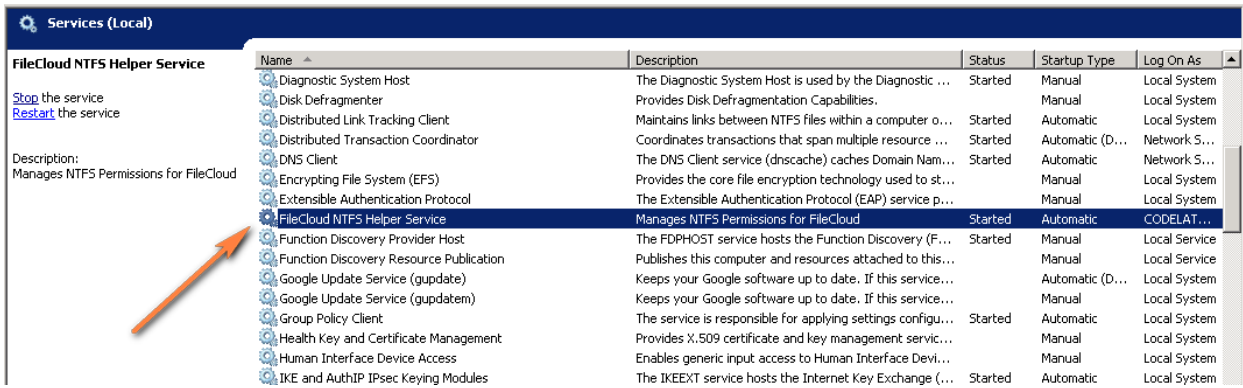
Technical Support

Need Help? [Documentation](#) [Contact Support](#)

To install the FileCloud Helper Service:

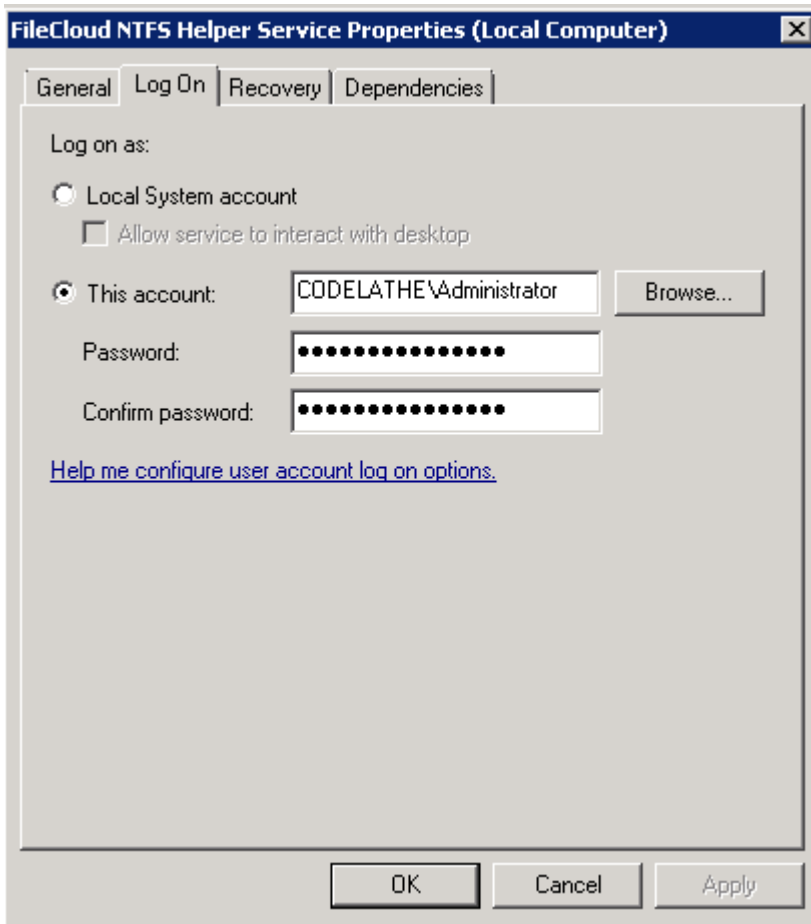
1. The download link for this service can be found in the customer portal. FileCloud helper service can also be installed from the FileCloud control panel using the install link.

 FileCloud Helper can only be installed on a the local hard drive, so if your APPDATA folder points to a network location, installation will fail.



1. After installation, change the logon information for the FileCloud Helper Service to the user account that has full access to the all the network shares.

i 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 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 you will need to 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.

Helper Service

Helper Service Host Helper Status

Specify helper service server URL or hostname. Required for functions such as content search

Message Queue Service

Check message queue status.

Restart Message Queue Service

Restart message queue server and workers.

To configure FileCloud Server to Find Helper on Another Machine:

1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. On the *Setting* screen, select the *Misc.* tab, and then the *Support Services* tab.
4. In the *Helper Service* section, in *Helper Service Host*, set the hostname of the computer running the Helper service.
5. On the Helper server, open the following location:

```
%appdata%\FileCloudHelper
```

6. 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
```

7. 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
```

8. 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.

Helper Service

Helper Service Host	127.0.0.1	Helper Status
	Specify helper service server URL or hostname. Required for functions such as content search	
Message Queue Service	<input type="button" value="Check"/>	
	Check message queue status.	
Restart Message Queue Service	<input type="button" value="Restart"/>	
	Restart message queue server and workers.	

Check the Status of Helper

To check the status of Helper Service:

1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. On the *Setting* screen, select the *Misc.* tab, and then the *Support Services* tab.
4. In the *Helper Service* section, click *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.
- Expiring cached results quicker allows existing results to be returned faster.

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.

Network Folder Details ✕

Network Folder Name	<input type="text" value="Salesforce"/>
Network Folder Path	<input type="text" value="/Salesforce"/>
Permissions	<input style="border-bottom: 1px solid #ccc;" type="text" value="DEFAULT"/> ▾
Smart Mount	<input type="checkbox"/>
Disable Offline Sync	<input type="checkbox"/>
Disable Notifications	<input type="checkbox"/>
Sharing	<input style="border-bottom: 1px solid #ccc;" type="text" value="Allow All Shares"/> ▾
Allow Remote Deletion of Files via Offline Sync	<input checked="" type="checkbox"/>
Realtime Index for Automatic Sync and Search (Beta)	<input checked="" type="checkbox"/> <input type="button" value="Reindex"/>
Realtime Index Status	5 folders, 6 files <input type="button" value="Check"/>
<input type="button" value="Manage Users"/> <input type="button" value="Manage Groups"/> <input style="background-color: #e74c3c; color: white; padding: 5px 15px;" type="button" value="Clear All Deleted Files"/>	
<input style="background-color: #2980b9; color: white; padding: 5px 15px;" type="button" value="Update"/> <input style="background-color: #e74c3c; color: white; padding: 5px 15px;" type="button" value="Close"/>	

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?

 <p>Attach an AWS S3 Bucket to a Network Folder</p>	<p>→ Create a Network Folder for Wasabi S3 Bucket</p>
 <p>Configure the bucket-based Network Folder</p>	<p>→ Configure the AWS S3 bucket-based Network Folder</p> <p>→ Clear All Deleted Files</p>

Create a Network Folder Based on an Wasabi S3 Bucket

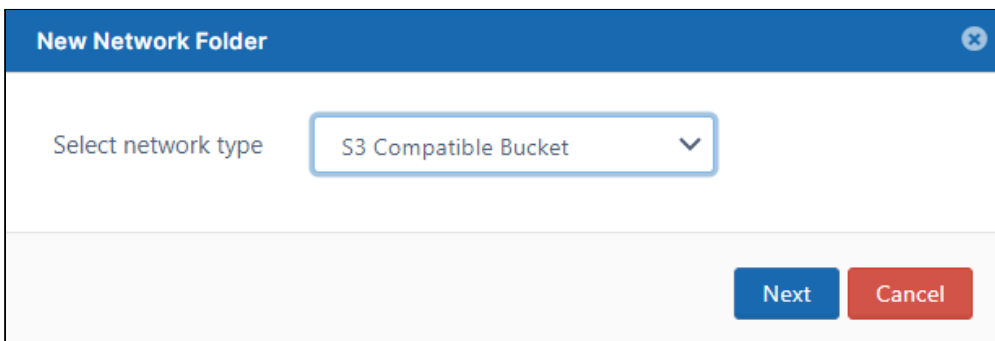
Administrators can integrate Wasabi S3 buckets with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

! 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**.

The screenshot shows a window titled "Attach S3 Bucket" with a close button in the top right. Below the title bar is a light blue header with the text "Enter user visible network folder name". Underneath, there is a label "Network Folder Name" next to a text input field containing the text "test-s3-network". At the bottom right of the window, there are two buttons: a blue "Next" button with a right-pointing arrow and a red "Cancel" button with a close symbol.

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**.

The screenshot shows the "Attach S3 Bucket" window with a close button. Below the title bar is a light blue header with the text "Amazon S3 access information.". Below this, there is a section titled "check here" in orange text with an arrow pointing to an unchecked checkbox labeled "Use IAM role". To the right, there is another section titled "or enter these" in orange text with two arrows pointing to the "S3 Access Key" and "S3 Secret" input fields. The "S3 Access Key" field contains the text "jennifer" and the "S3 Secret" field contains a series of dots. At the bottom of the window, there are three buttons: a blue "Previous" button with a left-pointing arrow, a blue "Next" button with a right-pointing arrow, and a red "Cancel" button with a close symbol.

7. On the **Attach S3 bucket** window, select **No Encryption** because Wasabi does not provide managed key encryption as AWS does.

Attach S3 Bucket [X]

Encryption Settings. Applicable only to newly added files and does not affect existing files

S3 Encryption Setting: No Encryption [v]

← Previous → Next × Cancel

8. On the **Attach S3 bucket** window, type in the bucket name and **Region**, and optionally the **End Point** and **Prefix**.
9. Click **Next**.

Attach S3 Bucket [X]

Information to connect to your Bucket

Bucket: s3bucket

End Point: OPTIONAL: (ex) https://s3.amazonaws.com

Region: us-east-1

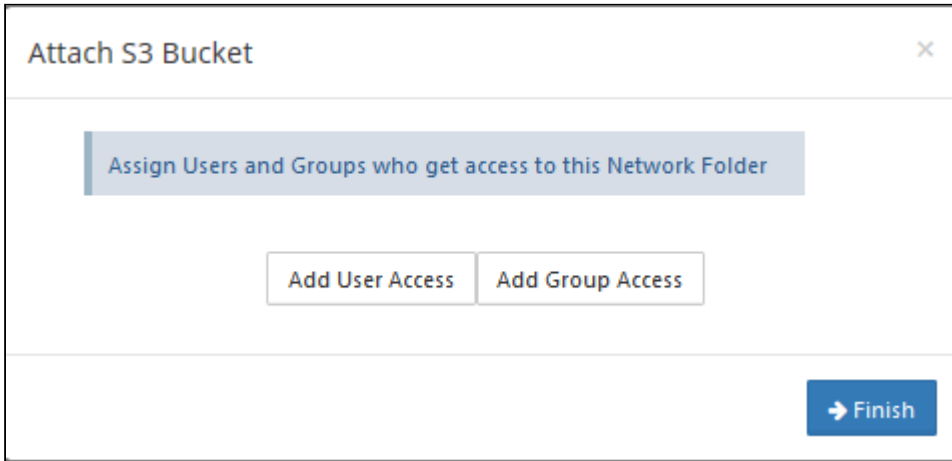
Prefix: OPTIONAL: (ex) folder1/sub1

← Previous → Next × Cancel

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.

S3 Network Folder Details
✕

S3 Key*

S3 Secret*

Use IAM role

Network Folder Name*

Bucket Name*

End Point

S3 Region

Prefix

S3 Encryption Setting ▼

Disable Offline Sync

Disable Notifications

Sharing ▼


Allow Remote Deletion of Files via Offline Sync

Manage Users
Manage Groups
Clear All Deleted Files

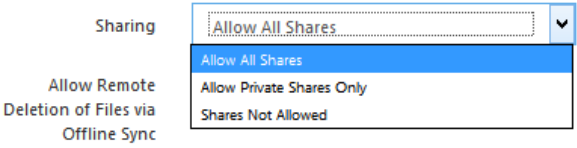
Update
Close

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.

Option	Description
Sharing	Sharing the content of the network share can be disabled or enabled using this option <div style="text-align: right; margin-top: 10px;">  </div>
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.

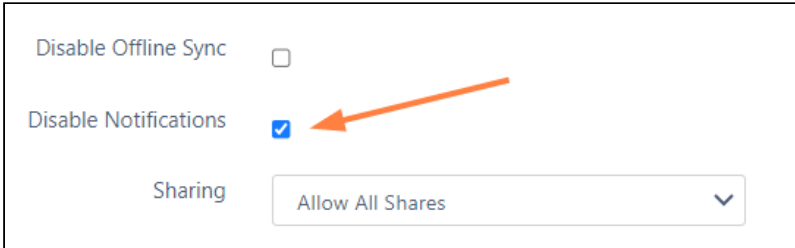
Disable notifications for Amazon S3 Network Folders

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.



Disable Offline Sync

Disable Notifications

Sharing

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.

S3 Network Folder Details ✕

S3 Key*

S3 Secret*

Use IAM role

Network Folder Name*

Bucket Name*

End Point

S3 Region

Prefix

S3 Encryption Setting ▼

Disable Offline Sync

Disable Notifications

Sharing ▼


Allow Remote Deletion of Files via Offline Sync


Manage Users
Manage Groups
Clear All Deleted Files

Update
Close

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**.

- On the **Manage Network Folders** window, click the Backblaze B2 bucket-based network folder, and then click the edit icon ().
- 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 <div style="text-align: right; margin-top: 10px;">  </div>

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.

S3 Network Folder Details ✕

S3 Key*

S3 Secret*

Use IAM role

Network Folder Name*

Bucket Name*

End Point

S3 Region

Prefix

S3 Encryption Setting ▼

Disable Offline Sync

Disable Notifications

Sharing ▼


Allow Remote Deletion of Files via Offline Sync

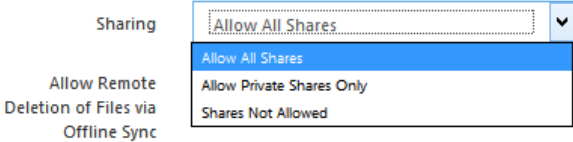
Manage Users
Manage Groups
Clear All Deleted Files

Update
Close

To edit a Clodian 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:

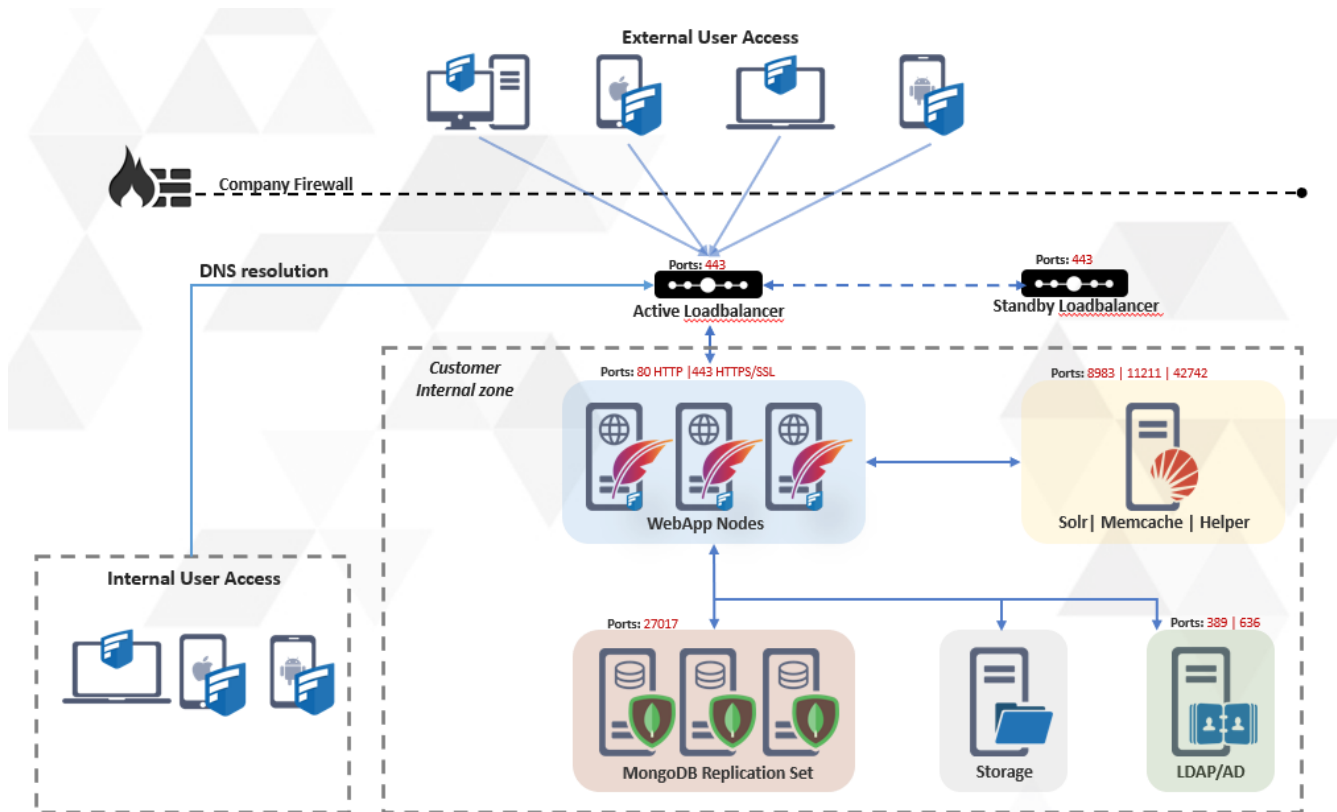
Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked, the S3 Key and S3 Secret fields disappear and the IAM role is used to connect to the S3 bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
End Point	URL where API requests are sent.
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 <div style="text-align: right; margin-top: 10px;">  </div>

Option	Description
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.

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 (LB) provide advantages to serving requests from your FileCloud servers because they allow you to better control how the traffic is handled in order to provide the best performance.. 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

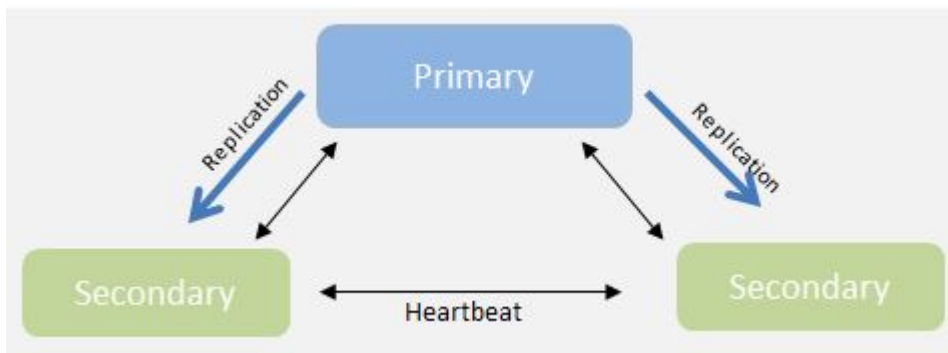
respond in an appropriate amount of time, the client times out on that request and moves on to the next IP address until the list is exhausted or it finds a connection that's valid.

FileCloud Component: App server node

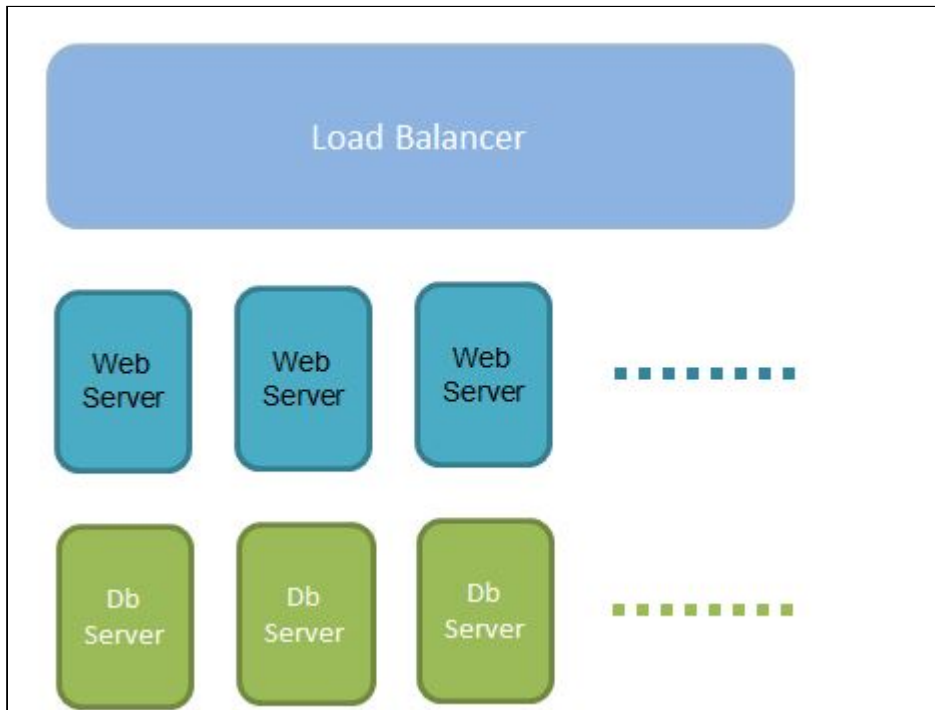
The FileCloud app server node consists of the Apache webserver as well as the FileCloud Application code to serve the client requests. The FileCloud app server nodes do not contain any application-specific data. The data is retrieved from the MondoDB replica sets. Because of this, the FileCloud app server 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 DB node. The minimum number of DB nodes 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.

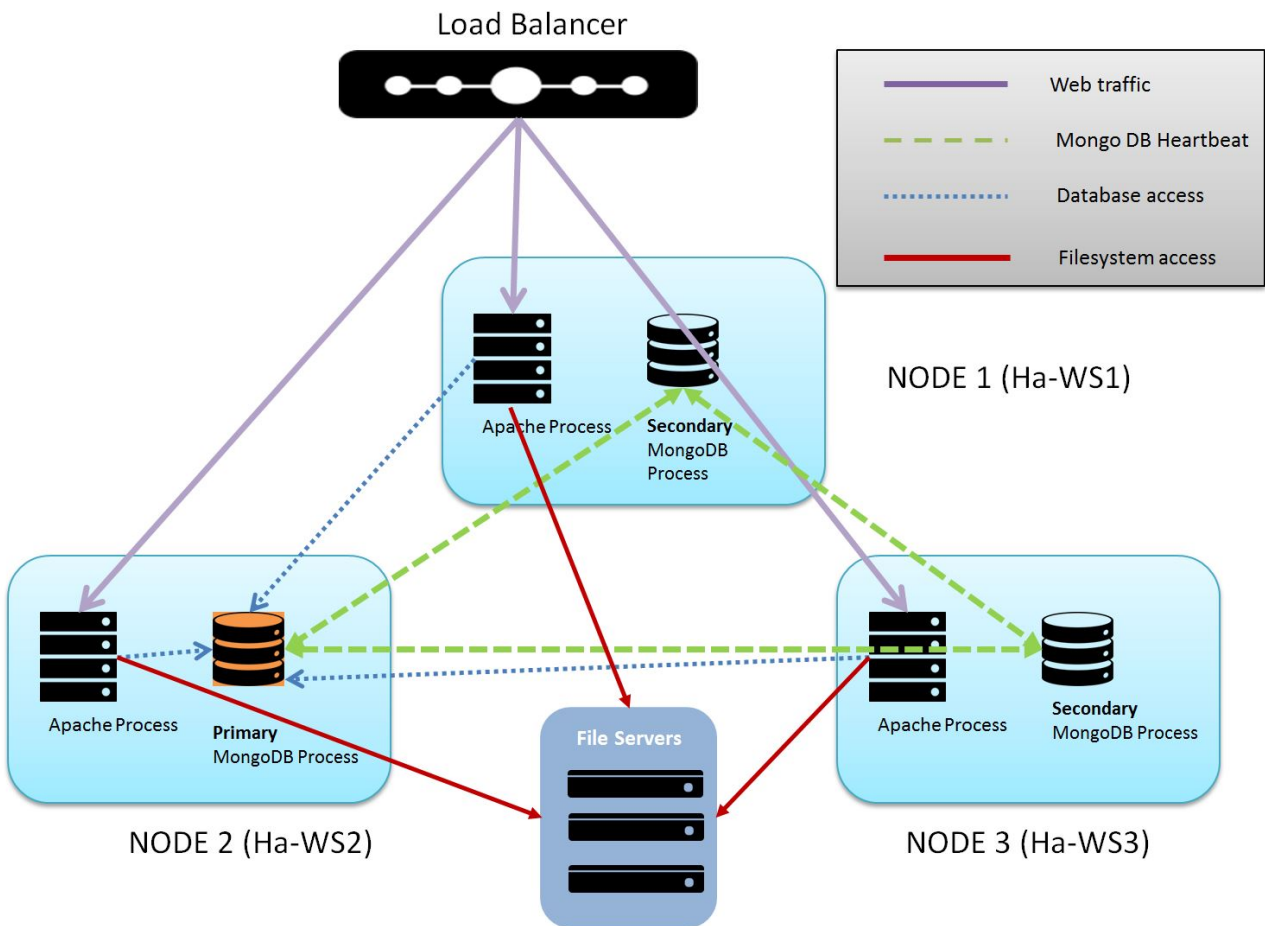


Deployment Instructions



1. You must have at least three systems because the database replica set requires a minimum of three servers
2. If you are using local storage, the local storage must be a location that is accessible by all the webserver nodes. The local storage CANNOT be a location inside any of the computers that run the FileCloud service. The location must be mounted on the same path string on each of the nodes (/mount/fcstorage or H:\storage)
3. Ports 27017 (MongoDB Ports) must not be blocked by a firewall (ideally drop the firewall until the install is over)
4. Temp storage should be commonly accessible as well (must be a network mounted location). The temp storage should be mounted on each of the nodes and the path must be specified in the `amazons3storageconfig.php` (on each node) with key `"TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER"` set to the path to the temp storage, for example: `define("TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER", "/mount/temp space");`
5. Each Web node must have UNIQUE host name; otherwise, temp folder clean up will not work properly

The following setup will be created with this set of instructions:



Load Balancer

- i The load balancer is not a part of this install, but for completeness sake, we are using HaProxy as an example. Skip this section if you already have a load balancer setup

Go to [Loadbalancer \(HaProxy\) install instructions](#).

Creating MongoDB Cluster

- i 1. MongoDB HA requires an odd number of nodes for voting of Primary.

2. MongoDB requires a majority of nodes to be available in order to hold an election (or majority of votes which is controlled by the node's priority).
3. The Timeout parameter might be needed to reduce latency in case of loss of nodes ([mongodb://Ha-WS1,Ha-WS2,Ha-WS3/?replicaSet=rs0&connectTimeoutMS=1000](#))
4. Use host name instead of IP address to be robust.
5. Ensure port 27017 is open in order for DB communication to work.

Ensure every node is at the same software level. (OS, FileCloud software level and its dependencies must be at the same level.)

1. Install MongoDB on all the designated DB nodes. These nodes can be collocated with the Apache server or can be on a different machine. In this section, we will assume there are three nodes (which is the minimum number needed for a MongoDB cluster).
2. Edit **mongo.conf** (In Linux it is at **/etc/mongodb.conf** and in Windows it is **c:\xampp\mongodb\bin\mongodb.conf**) in each DB node and enable DB replication. In case of MongoDB on Windows (all versions) uncomment **replSet** and set it like the following (or add this line if not present)

```
replSet = rs0
```

In case of MongoDB on Linux, uncomment line containing replication and add the replica set name as follows:

```
replication:
  replSetName: rs0
```

3. **Important:** Update the `bind_ip` value of the MongoDB node to listen to its local IP address:

```
bind_ip = [local ip address]
```

Note

After making the above changes, please restart your MongoDB service.

4. Open the mongo shell by running the `mongosh` command (in Linux it is **/usr/bin/mongo** and in Windows it is **c:\xampp\mongodb\bin\mongo**)
5. **This applies to ONLY one node. Select a node (say Ha-Ws1) and issue the following command. If you issue this in more than one system, the configuration will become invalid.** Initialize the replica set with the following command

```
rs.initiate()
rs.add("ip address of other Ha-Ws2")
rs.add("ip address of other Ha-Ws3")
```

6. In each of the three database server nodes, connect to the mongo shell and enter **rs.status()** to see the actual value (One of the nodes should show as **Primary** and other two nodes should show as **Secondary**) It should show appear similar to:

```

rs.status()
{
  "set" : "rs0",
  "date" : ISODate("2014-09-03T20:52:14Z"),
  "myState" : 2,
  "members" : [
    {
      "_id" : 0,
      "name" : "<ip of other DB>:27017",
      "health" : 1,
      "state" : 2,
      "stateStr" : "PRIMARY",
      "uptime" : 749,
      "optime" : Timestamp(1409777412, 1),
      "optimeDate" : ISODate("2014-09-03T20:50:12Z"),
      "errmsg" : "syncing to: ha-db1.codelathe.com:27017",
      "self" : true
    },
    {
      "_id" : 1,
      "name" : "<Ip of other DB>:27017",
      "health" : 1,
      "state" : 2,
      "stateStr" : "SECONDARY",
      "uptime" : 749,
      "optime" : Timestamp(1409777412, 1),
      "optimeDate" : ISODate("2014-09-03T20:50:12Z"),
      "errmsg" : "syncing to: ha-db1.codelathe.com:27017",
      "self" : true
    }
  ],
}

```

⚠ It is important that the "name" field for each of the members in the replica match the name used in the connection string.

For example, if hostnames are used `"mongodb://node0,node1,node2/?replicaSet=rs0&connectTimeoutMS=1000"`

then the `rs.status()` output should show the "name" field as `node0`, `node1`, `node2`. Also note that the hostname must be accessible from each of the nodes.

The name can be changed using mongo client commands in primary. For example, to change the name field of the first member of the replica set (0th element of the output of `rs.conf`)

```
cfs = rs.conf()
```

```
cfg.members[0].host="host0:27017"
```

```
printjson(cfg)
```

```
rs.reconfig(cfg)
```

```
rs.status()
```

Configuring FileCloud With MongoDB Cluster

After MongoDB cluster is installed and configured, use the following steps to configure FileCloud to use this cluster as its database.

1. If the app servers are different from DB servers, install the app server portion (Apache web server) of FileCloud on the app server nodes, using latest FileCloud server installer. If they are collocated, proceed to next step.
2. Open the file `$XAMPPROOT/config/cloudconfig.php` (In linux it is `/var/www/html/config/cloudconfig.php`, in windows it is `c:\xampp\htdocs\config\cloudconfig.php`)

```
// ... Cloud Database
define("TONIDO_CLOUD_DBSERVER", "mongodb://ip of Ha-ws1,ip of Ha-ws2,ip of Ha-ws3/?
replicaSet=rs0&connectTimeoutMS=1000");
// ... Audit Database
define("TONIDO_CLOUD_AUDIT_DBSERVER", "mongodb://ip of Ha-ws1,ip of Ha-ws2,ip of
Ha-ws3/?replicaSet=rs0&connectTimeoutMS=1000");
// ... Settings Database
define("TONIDO_CLOUD_SETTINGS_DBSERVER", "mongodb://ip of Ha-ws1,ip of Ha-ws2,ip of
Ha-ws3/?replicaSet=rs0&connectTimeoutMS=1000");
```

Example: `"mongodb://192.168.0.2,192.168.0.3,192.168.0.4/?replicaSet=rs0"`

3. Edit `localstorageconfig.php` and add/replace the following keys (In linux it is `/var/www/html/config/localstorageconfig.php`, in windows it is `c:\xampp\htdocs\config\localstorageconfig.php`)

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://ip of Ha-ws1,ip of Ha-ws2,ip of
Ha-ws3/?replicaSet=rs0&connectTimeoutMS=1000");
```

Example: `"mongodb://192.168.0.2,192.168.0.3,192.168.0.4/?replicaSet=rs0"`

4. **<Step required only for S3 storage>** : If you are using Amazon S3 for backend storage, then edit `amazons3storageconfig.php` and add/replace the following keys (In linux it is `/var/www/html/config/amazons3storageconfig.php`, in windows it is `c:\xampp\htdocs\config\amazons3storageconfig.php`)
If this file is not found, copy the storage sample file and rename it (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` in windows).

```
define("TONIDO_CLOUD_NODE_COMMON_TEMP_FOLDER", "/mount/fctemp");
```

Set Up Managed Storage

Since the FileCloud app server nodes do not store any of the application data, the managed storage must be an external location (A NAS, ISCSI, SAN, Amazon S3 or Open stack)

In this example, we assume that either NAS or NFS mount is already available and mounted on each of the webserver nodes.

1. Open the FileCloud Admin portal at **http://<load balancer IP/ui/admin/index.html** and log in.
2. Navigate to **Settings>Storage**, set the mounted path, and click **Save**.

The screenshot shows the 'Manage Settings' interface with the 'Storage' tab selected. The 'My Files' sub-tab is active, displaying the following settings:

- Storage Path:** C:\Fileclouddata (with a 'Check Path' button). Description: Specify the location to store Cloud Files, this must be writable by Webserver. Example path on Windows : c:\clouddata. Example path 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. Description: Number of versions to keep.
- Encryption:** Manage (button). Description: Manage encryption.
- Disable My Files:** . Description: Disable 'My Files' [Managed Storage].
- Default User Storage Quota:** 2 GB. Description: Default storage quota for new user. Can be overridden in user details. This does not affect existing user.
- User Storage Usage Calculation:** Exclude Shares. Description: Specify user storage calculation.
- Store Deleted Files:** . Description: Move file to recycle bin on delete action.
- Automatically Empty Recycle Bin After Specified Days:** 0. Description: Number of days once deleted files will be cleared. Value of 0 indicates that deleted files will not be cleared automatically.
- Do not store deleted files greater than:** 0.09765625 GB. Description: Files Greater than the specified size are permanently deleted.

3. Once the setup is complete, create user accounts by connecting to the admin portal. and tThen log into the user accounts using the load balancer IP (which will route the traffic to one of the app server nodes).

4. To test app server HA, turn off one of the app servers by logging into the app server (for example, Ha-WS1) and stopping Apache (using `service apache2 stop`). The service will be accessible because HaProxy will reroute traffic to Ha-WS2 or Ha-WS3 (depending on the routing selected).

Checking the Health of the HA System

FileCloud servers can be configured for a High Availability (HA) environment to improve service reliability and reduce downtime in your IT environment.

The admin portal has been enhanced to display all information about the health of each node.

- Administrators can run a system check and it will show one record for each node of the HA system, with data about its health.
- Cron will continue adding node information to the checks.
- This data will help 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.

FILECLOUD

GROUPS

- Groups
- Admins

MANAGE

- Team Folders
- Network Folders
- User Shares
- Folder Permissions

DEVICES

- Devices

GOVERNANCE

- Dashboard
- Retention

MISC

- Audit
- Alerts
- User Locks
- Workflows
- Reports
- Federated Search
- Metadata

SETTINGS

- Settings

CUSTOMIZATION

- Customization

SYSTEM

- Checks
- Upgrade

NODE Information

qahaone_10_0_3_6

- REPORT_TIME : 04/02/2019 01:56:01 pm
- NODEIP : 10.0.3.6
- NODENAME : qahaone
- PHP_OS : Linux
- PHP_VERSION : 7.2.16-1+ubuntu16.04.1+deb.sury.org+1
- FILECLOUD_VERSION : 19.1.0.3130
- MESSAGE_QUEUE : ACTIVE
- SCRATCH_FOLDER_SIZE : 6.15 MB
- SCRATCH_DISK_TOTAL_USED : 29.02 GB
- SCRATCH_DISK_FREE : 24.38 GB

qahatwo_10_0_3_7

- REPORT_TIME : 04/02/2019 01:52:10 pm
- NODEIP : 10.0.3.7
- NODENAME : qahatwo
- PHP_OS : Linux
- PHP_VERSION : 7.2.16-1+ubuntu16.04.1+deb.sury.org+1
- FILECLOUD_VERSION : 19.1.0.3130
- MESSAGE_QUEUE : ACTIVE
- SCRATCH_FOLDER_SIZE : 81.96 MB
- SCRATCH_DISK_TOTAL_USED : 29.02 GB
- SCRATCH_DISK_FREE : 24.25 GB

qahathree_10_0_3_8

- REPORT_TIME : 04/02/2019 01:56:49 pm
- NODEIP : 10.0.3.8
- NODENAME : qahathree
- PHP_OS : Linux
- PHP_VERSION : 7.2.16-1+ubuntu16.04.1+deb.sury.org+1
- FILECLOUD_VERSION : 19.1.0.3130
- MESSAGE_QUEUE : ACTIVE
- SCRATCH_FOLDER_SIZE : 28.54 MB
- SCRATCH_DISK_TOTAL_USED : 29.02 GB
- SCRATCH_DISK_FREE : 24.26 GB

To see the System Check:

1. Open a browser and log in to the admin portal.
2. From the left navigation pane, under **SYSTEM**, select **Checks**.

Other Considerations

NTFS Service

If you are using NTFS, then the NTFS service must be started on ALL nodes. The local webserver will use the local NTFS service in order to handle NTFS permissions. Please note, if you are doing real time indexing of network folders, you should only enable indexing on one NTFS helper.

Document Preview

If you have enabled document preview, then Open Office service must be started in ALL nodes. The local webserver will use the local Open Office service to handle document preview

Configure MongoDB Cluster to Use TLS-SSL with Cluster Authentication and Mongodb Authentication on Linux

Introduction:

When a MongoDB HA cluster is created, it is configured to listen to external requests. This is mandatory as all nodes in the cluster should be able to sync with each other. While hosting such a configuration in a private dedicated network is secure, hosting it in an intranet or public network is not secure. In such cases, 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 need 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, as in the sample deployment we created in part 2. Having RBAC enabled is mandatory for encryption.

A DB user has to be first created in MongoDB, and this user can be later used in FileCloud for secure database access. In this example, the user has the following details:

User Name	Password
dbuser	passw0rd1
OS	Command
Linux	<pre>\$ use admin \$ db.createUser({user: 'dbuser', pwd: 'passw0rd1', roles:['root']})</pre>

Now to connect to MongoDB we issue the following command::

OS	Command
Linux	\$ mongosh -u dbuser-p passwd0rd1 --authenticationDatabase "admin"

Configuration of mongod 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, Remember to 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 could 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	<pre>\$ 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</pre>

Apply the same for the second and third nodes.

4 - Create certificate for FileCloud web nodes

OS	Command
Linux	<pre>\$ cat psmdb1.pem psmdb2.pem psmdb3.pem > filecloud-mongo.pem</pre>

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	<pre>\$ 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</pre>

- 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	<pre>net: ssl: mode: requireSSL PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem CAFile: /etc/mongodb/ssl/mongoCA.crt</pre>

Restart Mongod Daemon:

OS	Command
Linux	\$ Systemctl restart mongod

Make sure to 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	<pre>\$ mongosh --authenticationDatabase "dbuser" --host mongossl1:27017 --ssl -- sslCAFile /etc/ssl/mongoCA.crt --sslPEMKeyFile /etc/mongodb/ssl/mongossl1.pem -u dbuser -p passw0rd1</pre>

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	<pre>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</pre>

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	<pre>\$ sudo openssl rand -base64 741 > /etc/mongodb-keyfile \$ sudo chmod 600 /etc/mongodb-keyfile \$ sudo chown mongodb.mongoddb /etc/mongodb-keyfile</pre>

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	<pre>net: ssl: mode: requireSSL PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem CAFile: /etc/mongodb/ssl/mongoCA.crt security: keyFile: /etc/mongodb-keyfile</pre>

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:passwd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://dbuser:passwd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://dbuser:passwd1@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 passwd1 --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, the password parameter embedded in the characters \"password\"
For example:

```
define("AUTOBACKUP_MONGODUMP_PARAMS", "--host 'rs0/HOST1,HOST2,HOST3' --username dbuser
--password \"passwd1?]}\" --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:passwd1@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.

Enable MongoDB Cluster Authentication

Introduction

When a MongoDB HA cluster is created, it is configured to listen to external requests. This is mandatory as each node in the cluster should be able to sync with other nodes in the cluster. While hosting such a configuration in a private dedicated network is secure, hosting it in intranet or public network will not be secure. In such cases, it is necessary to enable authentication on these clusters. Follow the steps outlined here to enable authentication on a MongoDB cluster.

Enable Cluster Node Authentication

In order for the cluster nodes to communicate with each other in a secure mode, enable what is called "Internal Authentication". This is done by creating a secure key and configuring each cluster node to use that key.

1. Create secure key
Create a secure key with the following command.

OS	Command
Linux	<pre>\$ sudo -s /bin/bash -c 'openssl rand -base64 741 > /etc/mongodb-keyfile' \$ sudo -s /bin/bash -c 'chmod 600 /etc/mongodb-keyfile' \$ sudo -s /bin/bash -c 'chown mongodb.mongodb /etc/mongodb-keyfile'</pre>
Windows	<pre>C:\xampp\apache\bin>openssl rand -base64 741 >"C:\xampp\apache\conf\mongodb-keyfile"</pre>

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	<pre>security: keyFile: /srv/mongodb/keyfile</pre>
Windows	<p><i>In case of mongodb on Windows(all versions) and mongodb v2.x on Linux, uncomment (or add) security.keyfile and set it like the following (or add this line if not present)</i></p> <pre>keyFile = C:\xampp\apache\conf\mongodb-keyfile</pre>

4. Restart MongoDB server nodes.
Save the configuration changes and restart the server. Make sure the cluster is back to normal operation.

Setup DB User

A DB user has to be first created in MongoDB and this user can be later used in FileCloud for secure database access. Assuming we will add a user with following details:

User Name	Password
dbuser	passw0rd1

Use a command line mongo client and execute the following commands to create the required DB user.

Mongo Client
<pre>> use admin;</pre>

```
> db.createUser({ user: 'dbuser', pwd: 'password1', roles: [ { role: "clusterAdmin", db:
"admin" }, { role: "userAdminAnyDatabase", db: "admin" }, { role:
"readWriteAnyDatabase", db: "admin" } ] });
```

Upon executing the above commands, 'dbuser' will be added as valid database user.

Optional: Setting Restrictive DB User Policy

In certain cases, when the DB server doesn't run on a private network, it will be preferable to setup more restrictive permissions. In these situations, follow the steps below to create a more restrictive policy.

So we need to create explicit policies for the following databases that FileCloud uses.

Database name
tonidoauditdb
tonidoclouddb
tonidosettings
tonidostoragedb
tonidosyncdb

Use a command line mongo client and execute the following commands to create the required DB user.

Mongo Client

```
> use admin;
> db.createUser({ user: 'dbuser', pwd: 'password1', "roles" : [
    {
        "role" : "dbOwner",
        "db" : "tonidosyncdb"
    },
    {
        "role" : "dbOwner",
        "db" : "tonidostoragedb"
    },
    {
        "role" : "dbOwner",
        "db" : "tonidosettings"
    },
    {
        "role" : "dbOwner",
        "db" : "tonidoclouddb"
    }
] });
```

```

    },
    {
        "role" : "dbOwner",
        "db" : "tonidoauditdb"
    }
] });

```

Upon executing the above commands, 'dbuser' will be added as valid database user.

Note

If you are running a multisite installation, then each site will have its own set of databases of the format dbname_siteid. You will need to add roles or create separate db user for each database set specific to the site.

Configure Other DB URLs In Config File

If you have never updated the database URLs in the admin UI, follow this sub-section. If not, skip to the next sub-section.

Other database URLs required for FileCloud needs to be changed to reflect the database user as well. To do this, 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:passwd1@192.168.1.10,192.168.1.20,192.168.1.30/?
replicaSet=rs0&connectTimeoutMS=1000");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://
dbuser:passwd1@192.168.1.10,192.168.1.20,192.168.1.30/?
replicaSet=rs0&connectTimeoutMS=1000");
// ... Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://
dbuser:passwd1@192.168.1.10,192.168.1.20,192.168.1.30/?
replicaSet=rs0&connectTimeoutMS=1000");

```

and configuration file WWWROOT/config/cloudconfig.php and update the following line:

Update DB URLs in localstorageconfig.php

```

// ... Cloud Database

```

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://
dbuser:password1@192.168.1.10,192.168.1.20,192.168.1.30/?
replicaSet=rs0&connectTimeoutMS=1000");
```

Restart Services

Finally, it is necessary to 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, mongodb security key has to be disabled and the database URLs has to be reverted back.

HaProxy Setup in Ubuntu

Introduction

The following instructions apply to deploying FileCloud HA in an Ubuntu 22.04 environment. This can easily be adapted to other Linux flavors as well. This example uses HTTP but can be expanded easily to use HTTPS as well. Some of the instructions will have to be adapted to your specific environment. Every HA setup has a load balancer as its core component.

Load Balancer

The load balancer is the component that distributes incoming requests among a group of servers. In this case, the load balancer of choice is HaProxy (<http://www.haproxy.org/>). HaProxy is a high performance and battle tested load balancer and allows you to scale your FileCloud deployment quickly as well.

NOTE: Before starting the install, ensure the servers are already available and their IP addresses are known.

Setting up Ha-Proxy

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. Create a file named haproxy.cfg and add the following in the empty haproxy.cfg file

```
global  
  log 127.0.0.1 local0 notice  
  maxconn 2000  
  user haproxy  
  group haproxy
```

Logging

The log directive mentions a syslog server to which log messages will be sent. On Ubuntu, rsyslog is already installed and running but it doesn't listen on any 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 changes the HAProxy process to the specified user/group. These shouldn't be changed.

```
defaults  
  log global  
  mode http  
  option httplog  
  option dontlognull  
  retries 3  
  option redispatch  
  timeout connect 5000  
  timeout client 10000  
  timeout server 10000
```

Host Configuration

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.

The names used for the three web servers in these instructions are `Ha-WS1`, `Ha-WS2`, `Ha-WS3`.

```
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
```

Additional Notes

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`).

Information about each algorithm can be obtained from the official documentation.

The `server` directive declares a backend server with the syntax:

```
server <name> <address>[:port] [param*]
```

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.

Starting Ha-Proxy

From command line, start haproxy, using the following command:

```
service haproxy start
```


Installation and Configuration of FileCloud in Webservers

Installation and Configuration of FileCloud in Webservers

Install FileCloud in webserver nodes using the script below:

```
dnf module disable httpd -y
dnf module disable php -y

cat <<EOF > /etc/yum.repos.d/filecloud-23.1.repo
[filecloud-23.1]
name=FileCloud 23.1
baseurl=https://repo.filecloudlabs.com/yum/redhat/\$releasever/filecloud/23.1/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://repo.filecloudlabs.com/static/pgp/filecloud.asc
module_hotfixes=true
EOF

cat <<EOF > /etc/yum.repos.d/mongodb-org-6.0.repo
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/\$releasever/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-6.0.asc
EOF

yum update -y
yum install yum-utils -y
yum-config-manager --enable filecloud-23.1

ACCEPT_EULA=Y yum install filecloud -y
```

Configuring FileCloud With MongoDB Cluster

After MongoDB cluster is installed and configured, use the following steps to configure FileCloud to use this cluster as its database.

1. If the app servers are different from DB servers, install the app server portion (Apache web server) of FileCloud on the app server nodes, using the latest FileCloud server installer. If they are collocated, proceed to the next step.
2. Open the file `/var/www/html/config/cloudconfig.php`.

```
// ... Cloud Database define("TONIDOCLOUD_DBSERVER", "mongodb://
dbuser:passwd@hostname of Mongo1,hostname of Mongo2,hostname of Mongo3/?
replicaSet=rs0&connectTimeoutMS=1000");
// ... Audit Database define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://
dbuser:passwd@hostname of Mongo1,hostname of Mongo2,hostname of Mongo3/?
replicaSet=rs0&connectTimeoutMS=1000");
// ... Settings Database define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://
dbuser:passwd@hostname of Mongo1,hostname of Mongo2,hostname of Mongo3/?
replicaSet=rs0&connectTimeoutMS=1000");
```

3. Edit `/var/www/html/config/localstorageconfig.php`, and add/replace the following keys:

```
define("TONIDO_LOCALSTORAGE_DBSERVER", "'mongodb://dbuser:passwd@hostname of
Mongo1,hostname of Mongo2,hostname of Mongo3/?
replicaSet=rs0&connectTimeoutMS=1000'");
```

FC Push Service Configuration

In FileCloud version 23.1, a Push Service has been added to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload, share).

1. Open and edit the `.env` file from path: `/opt/fcpushservice/`

```
vi /opt/fcpushservice/.env
```

2. Update the MongoDB connection string:

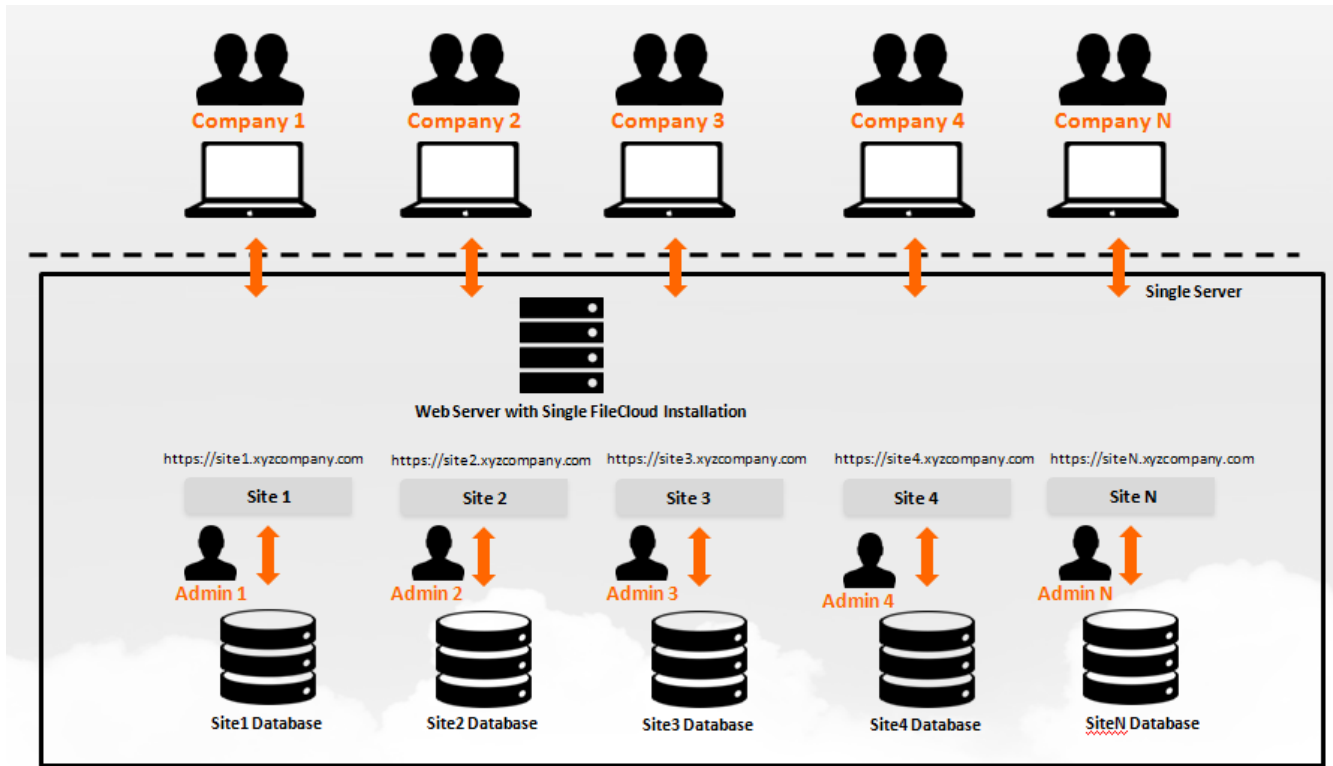
```
FCPS_DB_DSN=mongodb://dbuser:passwd1@ dbserver01, dbserver02, dbserver03:27017
```

3. Restart the `fcpushservice`.

```
systemctl restart fcpushservice
```

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](#)
- [Enable Multi-Tenancy Support](#)
- [Password encryption and logging in to a multi-tenant admin portal](#)
- [Manage Different Sites](#)
- [Enable Email Notifications if Cluster is Down](#)
- [Enable Automatic License Renewal and Reporting](#)

Multi-Tenancy Requirements

Administrators can install a single deployment of FileCloud Server but still have many different 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 Admin portal are without errors.
2. Only a single SSL certificate can be installed for all the sites, so therefore, it is recommended that you use a wildcard SSL certificate for a main domain say: https://*.xyzcompany.com and then setup each site as a subdomain of the main site, say 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 the site or the 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

Administrators can log in to a multi-tenancy admin portal by logging 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 Version 20.1 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$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtfrVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw

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("TONIDO_CLOUD_MULTISITE_ADMIN_PASSWORD", 'Vrwfq7xNHV');
```

7. Paste the string generated by passwordenc.php over the password value:

```
define("TONIDO_CLOUD_MULTISITE_ADMIN_PASSWORD", '$pbkdf2-
sha512$50000$ENIGvUsu3T6rIbI5Bz9DXw$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtfrVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw');
```

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 [Two Factor Authentication](#) access is enabled, then you will need to provide an additional code to continue.












Manage Different Sites

Once you login as superadmin you will see the Manage Sites screen.

- **Storage Quota** - this column indicates the current storage quota and the maximum allowed storage quota limit in GB for that site.
- **Users** - this column indicates the current users and maximum allowed user limit for that site.

⚠ Please note that in order for the current storage quota and current users to be calculated the [Cron job](#) must be set up by the admin.

Figure 1. Admin portal for superadmin management of multi-tenant sites.

Site Name	Site URL	Created On	Site Expiry	Installed License Validity	Storage Quota	Users	Actions
default	*	2020-Nov-06 01:59:21	No Expiry	2021-10-26	9.18 GB / Unlimited	4 Used / No Limit Set	  
golgre	tew.vom	2020-Nov-18 02:05:27	No Expiry	Not Valid	0 / Unlimited	0 Used / No Limit Set	   
filecloudo	vrseg.com	2020-Nov-18 02:06:14	No Expiry	Not Valid	0 / Unlimited	0 Used / No Limit Set	   

Page 1 of 1
3 rows

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 bring up the Site Detail dialog.

- Provide a site name, you cannot change the site name later. The site name has to be alphanumeric only and is used to prefix database names for this site.
- Provide the site hostname (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. This will create the new site with the settings from the site to be duplicated.
- Notes is optional.

New Site
✕

Site Name
(AlphaNumeric only)

Site HostName (e.g.
xyz.domain.com)

Duplicate Site
Settings

Site Settings to
Duplicate

default
▼

Notes

notes;

- 1.
- 2.
3. |

Save

Close

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.

Starting with the 17.3 version it is possible to set up an **Admin password** for a site directly in the **Site Settings** dialog box.

Site Settings ×

Maximum User Limit
 Maximum Users Allowed on the Site. Enter 0 for unlimited users.

Maximum Quota in GB Per Site
 Max Quota in GB allowed per Site. Enter 0 for unlimited Quota


Expiration Date (Optional)

Admin password
 Admin password

Access a newly added site

To access the newly added site, you need to use the domain name setup for the site. for example : <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 setup 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 done in multisites.


Remove a site

Select the site entry and click on "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 is accessible from the local site. This is 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 under `/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
```

In case of centOS, use the following:

```
crontab -u apache -e
```

2. At the end of the crontab file add the following line:

```
php ./tools/mongohealth/index.php
```

3. Save and Exit

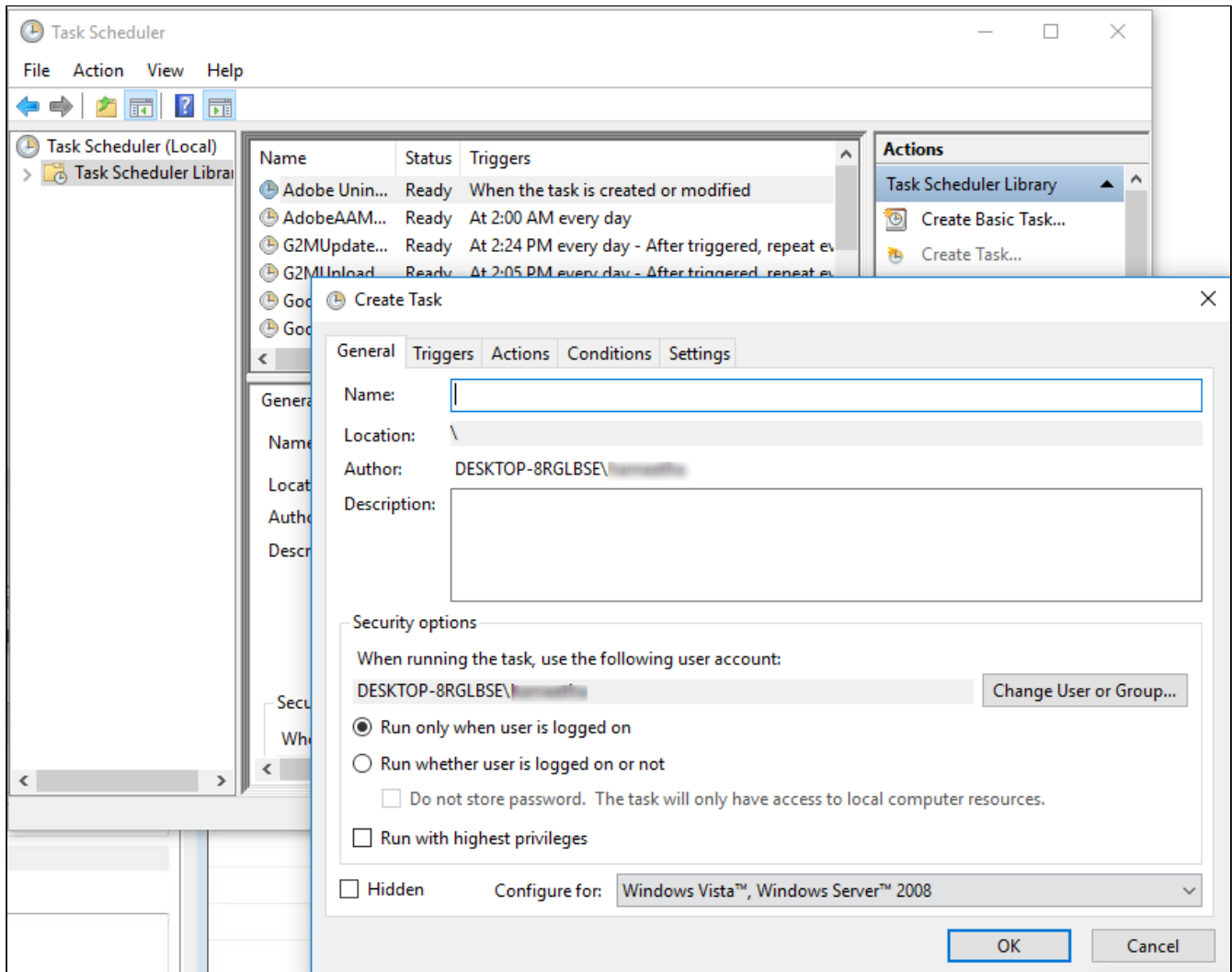
Add a PHP file to Scheduler

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, how often you 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/Cron Job is not setup for a multi-tenancy site with a SPLA license, license renewal/reporting will not happen automatically. The site will not acquire license automatically after every month and can only be acquired by the admin logging in. If the monthly report is not completed, then users will get a license error when they login.

 **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 doesn't get renewed automatically when using the SPLA license, please follow the following steps to troubleshoot.

1. Open the Admin Portal for the specific site ; click on "checks" and verify that the cron job was run recently

The screenshot shows the FileCloud installation checks page. The left sidebar contains navigation options: Network Folders, User Shares, Folder Permissions, DEVICES (Devices), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), CUSTOMIZATION (Customization), and SYSTEM (Checks, Upgrade). The main content area lists various checks, with several highlighted in yellow to indicate failures:


- Mod Rewrite Apache Configuration Setup OK
- Config Directory Readable OK C:\xampp\htdocs\config
- cloudconfig.php readable OK C:\xampp\htdocs\config\cloudconfig.php
- localstorageconfig.php readable OK C:\xampp\htdocs\config\localstorageconfig.php
- Scratch Directory Writable OK C:\xampp\htdocs\scratch
- Local Storage Path (Managed Storage) Writable OK C:\Clouddata
- Local Storage Path(Managed Storage) Checks OK
- License Installed OK
- License Valid OK
- Database Ensure Index OK
- Admin Password NOT changed from Default
- Admin Email NOT 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)
- Last Cron Job was run at 24-May-2018 02:45:27 AM (0.0 hours ago)
- Memcache Server available OK 1.4.4-14-g9c660c0
- Audit Database records less than 1M OK (9 found)
- Server time set OK. Time Skew: 17 secs

1. If the cron job was not run recently, it is **critical** that a Task Scheduler or Cron Job is setup to run properly when running a multi-tenant system. See [instructions on how to set this up](#). When running cron jobs with multi-tenant scenarios, make sure all sites are accessible by their domain names from the local system that is running the cron job.

The cron job **uses the Server URL setting specified in the Admin->Settings page** to access the site. Make sure the Server URL works on the local system correctly.

If you are using a HTTPS site, ensure that the Server URL has the correct prefix (https instead of http). After making the Server URL change, you can wait for 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.



Manage Settings

- HOME
 - Dashboard
- USERS/GROUPS
 - Users
 - Groups
 - Admins
- MANAGE
 - Team Folders
 - Network Folders
 - User Shares
 - Folder Permissions
- DEVICES
 - Devices
- MISC.
 - Audit
 - Alerts
 - User Locks

Server | Storage | Authentication | Admin | Database | Email | Endpoint Backup | License | Policies | SSO

Server Settings

Service Name:
Specify the service name to be used to refer to the service

Server URL: [Check URL](#)
Server URL is the url via which users access the service.

Session Timeout (Days):
Specify user web login session timeout.
Example: 0 = Default timeout of 15 minutes, 0.25 = 6 hours, 1 = 1 day.
Note: Session will always expire when browser is closed unless advanced configuration is done.

WebDAV:
Enable to allow WebDAV access to server

Document Settings


The purpose of FileCloud is to provide enterprises with a file storage and sync solution.

- Since documents are at the core of this solution, providing as many tools as you can to your users to interact with files on a daily basis is critical
- Besides installing additional tools, there are built-in options that you can simply enable to provide a better experience for users when working with documents
- Once users start working with documents, you can manage file extensions and file change notifications to help users manage their document processes

Administrators can configure the following options to provide the best experience possible to FileCloud users:

- [Setting up Content Search for Documents](#)
- [Setting Up Document Preview](#)
- [Enabling Watermarks On Previews](#)
- [Import Files : Pre-seeding](#)
- [Enabling Natural Sort Order Of User List](#)
- [Enabling PDF Merge](#)
- [Optimize PDF Preview](#)
- [Managing File Extensions](#)
- [Restricting File Names](#)
- [Manage File Versioning](#)
- [Configuring Zip Files and Zero Trust File Sharing](#)






Setting up Content Search for Documents

 Beginning with FileCloud Version 19.3, content of files larger than 10MB is not indexed. Beginning with FileCloud Version 20.3, searching image and PDF files with optical character recognition (OCR) is available for Enterprise users and users with an OCR license. See [Enabling Solr OCR](#).

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

What do you want to do?

-  [Install Content Search for Windows](#)
-  [Install Content Search for Linux](#)
-  [SOLR Configuration Tips](#)
-  [Configure Content Search for Managed Storage](#)
-  [Configure Content Search for Network Storage](#)

➔ Configure Pattern Search

Install Content Search for Windows

Advanced content searching capabilities for documents in FileCloud uses Solr and requires the correct Java Development Kit (JDK).



is an open source enterprise search platform, written in Java.

FileCloud now fully supports OpenJDK 11.02 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.

💡 FileCloud's Doc Converter feature also requires OpenJDK 11. If you already have this installed, you can skip the first two steps.

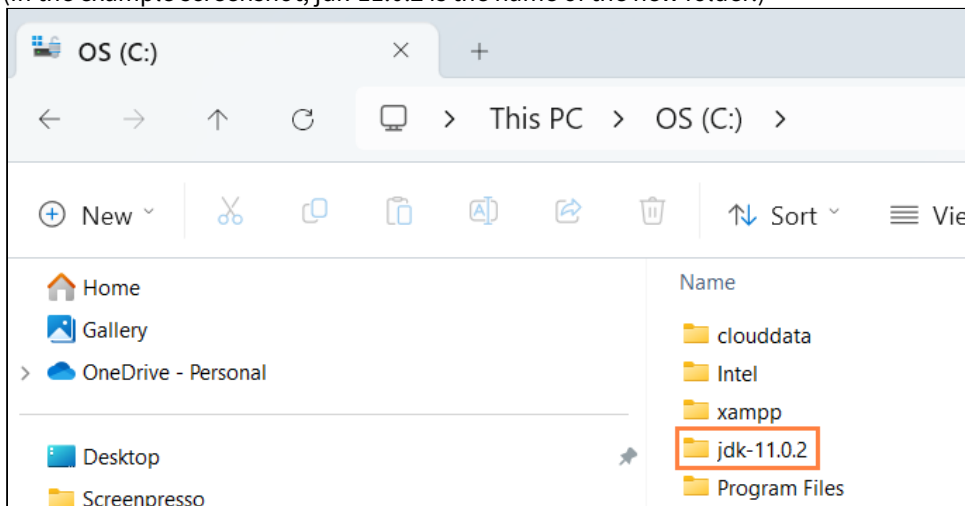
To install OpenJDK and Content Search for Windows:

1. Install OpenJDK.

To install OpenJDK:

1. Download **Open JDK 11.02+9** from <https://jdk.java.net/archive/>.
2. Create a new folder in the C: drive.

(In the example screenshot, jdk-11.0.2 is the name of the new folder.)



3. Extract the Open JDK file you downloaded into the new folder.

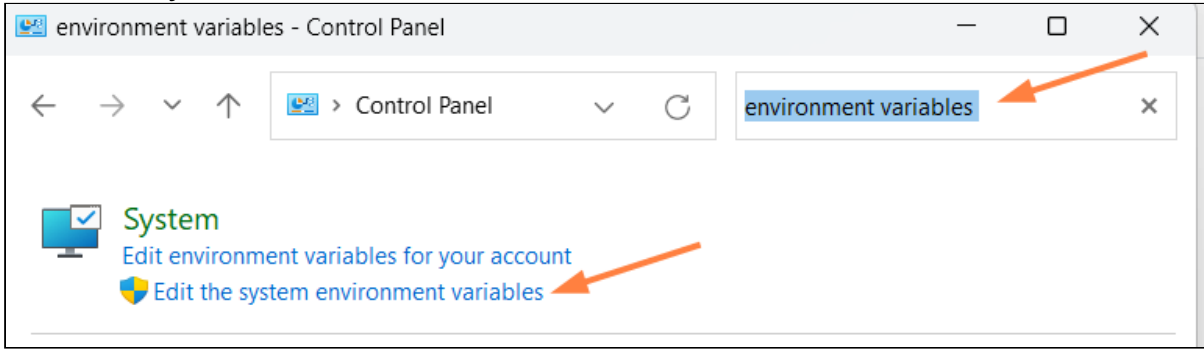
2. Set the JAVA_HOME path

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.

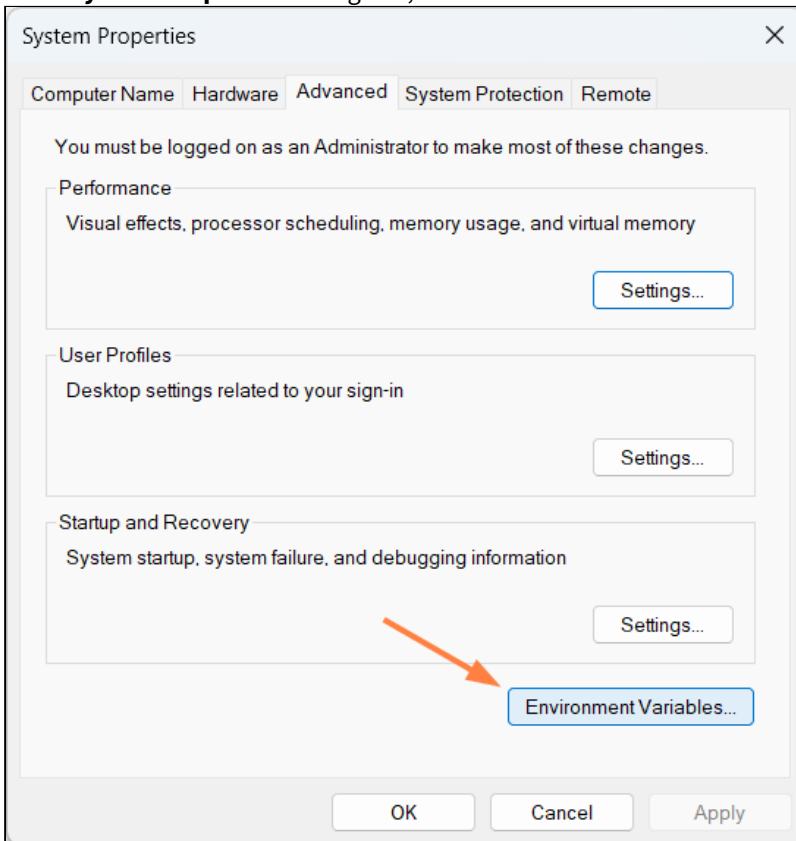
⚠ Administrator privileges are required to modify the path and environment variables.

To set the **JAVA_Home** path:

1. Open the Windows Control Panel.
2. Enter **environment variables** in the search bar.
3. Click **Edit the system environment variables**.



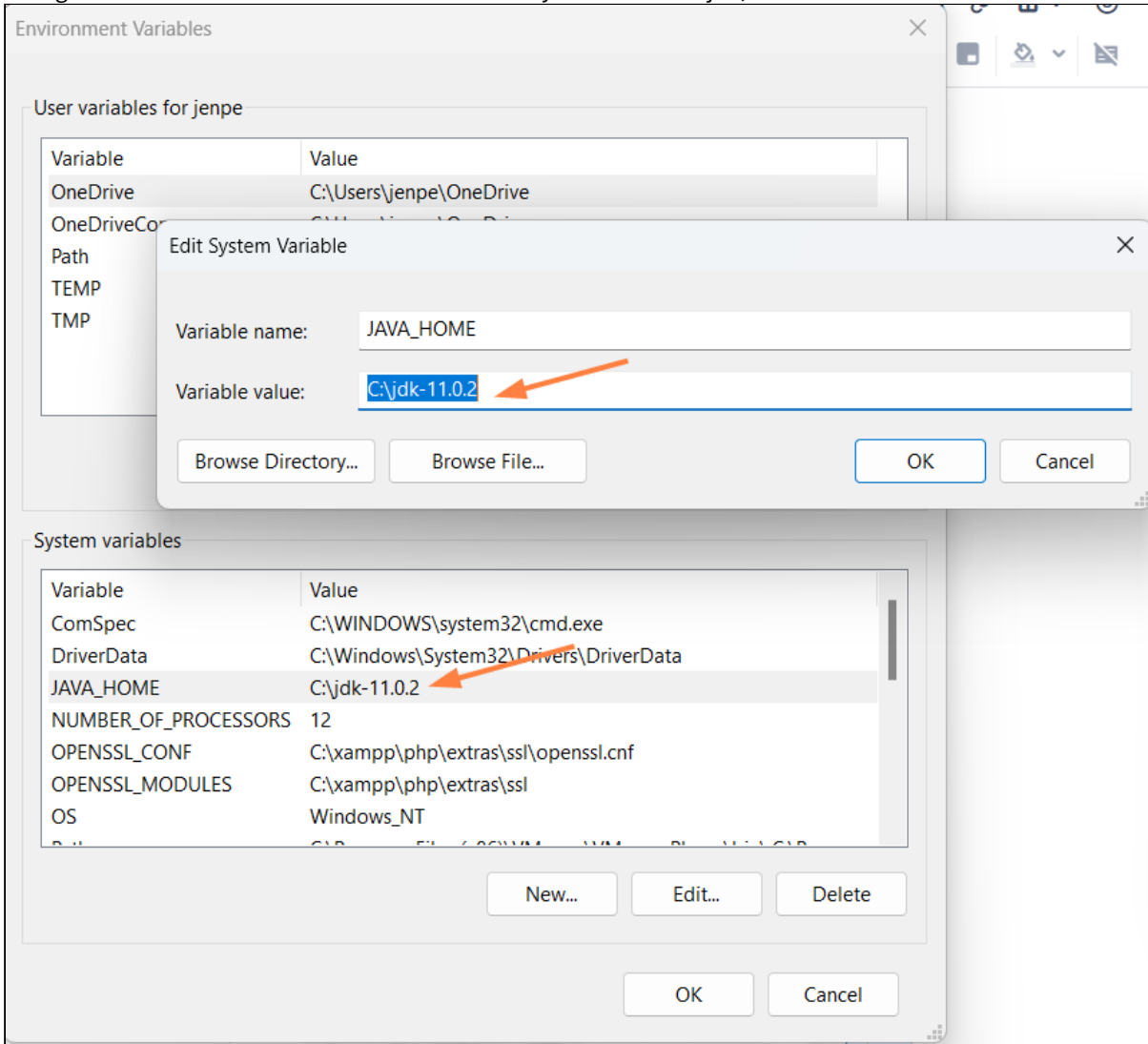
4. In the **System Properties** dialog box, click **Environment Variables**.



The **Environment Variables** dialog box opens.

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

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



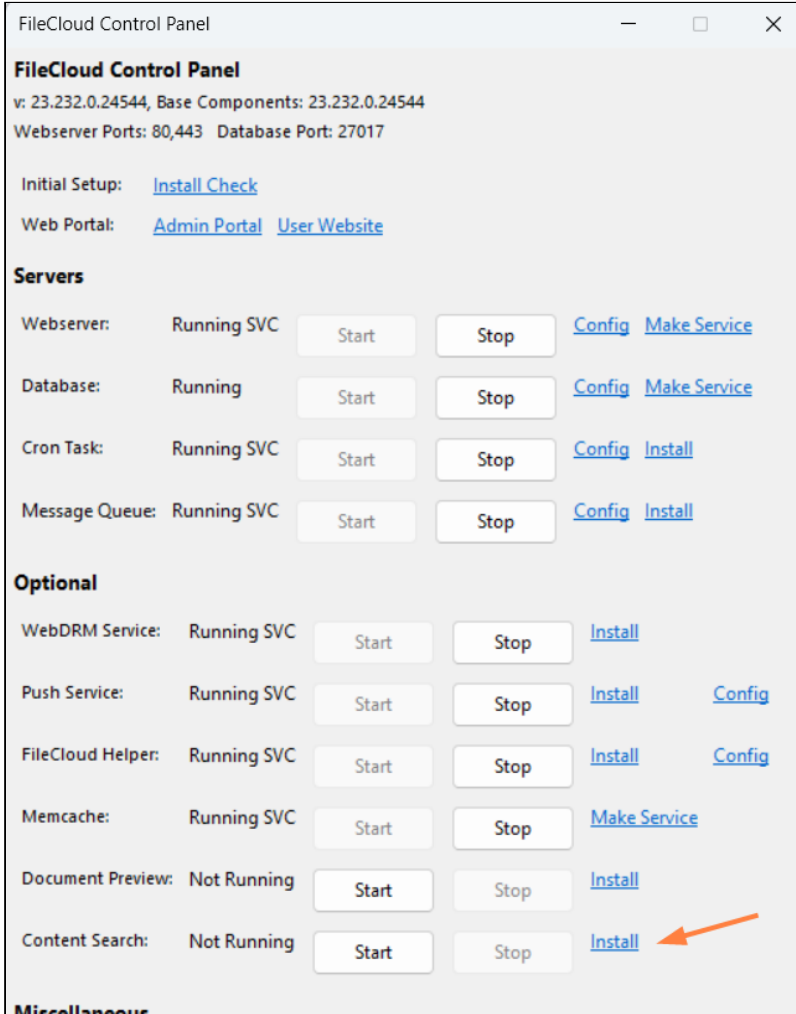
7. In the **Environment Variables** dialog box, click **OK**.

3. Use the FileCloud Control Panel to install Content Search

To install and start Content Search:

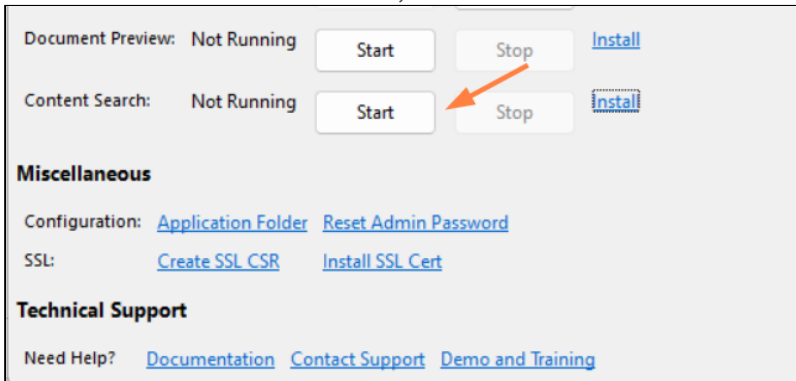
1. Open the FileCloud Control Panel.

- Next to **Content Search**, click **Install**.



The screenshot shows the FileCloud Control Panel interface. At the top, it displays the version (v: 23.232.0.24544) and base components (23.232.0.24544). Below this, there are links for 'Initial Setup' (Install Check) and 'Web Portal' (Admin Portal, User Website). The 'Servers' section lists several services: Webserver (Running SVC), Database (Running), Cron Task (Running SVC), and Message Queue (Running SVC). Each service has 'Start' and 'Stop' buttons and links for 'Config' and 'Make Service' or 'Install'. The 'Optional' section lists services like WebDRM Service, Push Service, FileCloud Helper, Memcache, Document Preview, and Content Search. The 'Content Search' service is currently 'Not Running' and has 'Start', 'Stop', and 'Install' buttons. An orange arrow points to the 'Install' button for Content Search. The 'Miscellaneous' section is partially visible at the bottom.

- To start the **Content Search** service, click the **Start** button.



This is a close-up view of the 'Content Search' service controls. It shows the service status as 'Not Running'. There are three buttons: 'Start', 'Stop', and 'Install'. An orange arrow points to the 'Start' button. Below this, the 'Miscellaneous' section includes links for 'Configuration' (Application Folder, Reset Admin Password) and 'SSL' (Create SSL CSR, Install SSL Cert). The 'Technical Support' section includes links for 'Need Help?' (Documentation, Contact Support, Demo and Training).

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 Solr on the same server using the command:

```
filecloudcp --install-solr
```

- If you have installed FileCloud on multiple server for high availability, install Solr stand-alone application using the commands:

```
curl --location 'https://repo.filecloudlabs.com/static/misc/filecloudcp' -o /usr/bin/filecloudcp  
chmod 755 /usr/bin/filecloudcp  
filecloudcp --install-solr
```

- To upgrade Solr, use the same command above that corresponds to your single-server or multiple-server installation. For recent versions of Solr, the following messages should be returned:

```
root@fcsrv:~# filecloudcp --install-solr  
Solr exists  
SOLR VERSION is 8.11.1  
Already running in the Latest SOLR VERSION which is 8.11.1  
root@fcsrv:~# █
```

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, installed in the previous section.

1. Login into admin UI. Navigate to Settings -> Content Search.

The screenshot shows the 'Manage Settings' page in the FileCloud admin UI, specifically the 'Content Search' tab. The page title is 'Manage Settings' and the sub-tab is 'Content Search'. Below the navigation tabs, there is a note: 'Content search uses Solr server. A Solr server has to be up and running before FileCloud can be configured for content search.' The 'Solr Configuration' section contains the following fields:

- Content Search Status:** A read-only field displaying 'Solr not configured.' A 'Configure' button is highlighted with a red box, with the text 'Configure FileCloud with Solr' below it.
- Content Search Component Status:** A read-only field.
- URL:** A text input field with a blurred value. Below it, the label 'URL of the Solr server' is shown.
- Port:** A text input field containing '8983'. Below it, the label 'Listening port of the Solr server' is shown.
- App Context:** A text input field containing 'solr'. Below it, the label 'Solr application context. For typical use no need to change the default' is shown.
- Config Prefix:** A text input field containing 'fccore'. Below it, the label 'Solr configuration prefix. For typical use no need to change the default' is shown.

The content search details form has default values for each field.

2. Update these values, 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 will be 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: For multisite FileCloud editions, each site should have a unique prefix, if they use the same Solr server.

- 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 `C:\xampp\htdocs\thirdparty\overrides\solarium\Solarium\fcskel` should be copied to `C:\work\solr\solr-5.3.1\server\solr\` and renamed `fccore`. Directories and target folder name for your environment might be different.

The screenshot shows the 'Manage Settings' interface with the 'Content Search' tab selected. The 'Solr Configuration' section contains the following fields:

- Content Search Status: Solr not configured.
- Content Search Component Status: (empty)
- URL: http:// (with a red arrow pointing to the 'Configure' button)
- URL of the Solr server: (empty)
- Port: 8983
- Listening port of the Solr server: (empty)
- App Context: solr
- Solr application context. For typical use no need to change the default: (empty)
- Config Prefix: fccore
- Solr configuration prefix. For typical use no need to change the default: (empty)

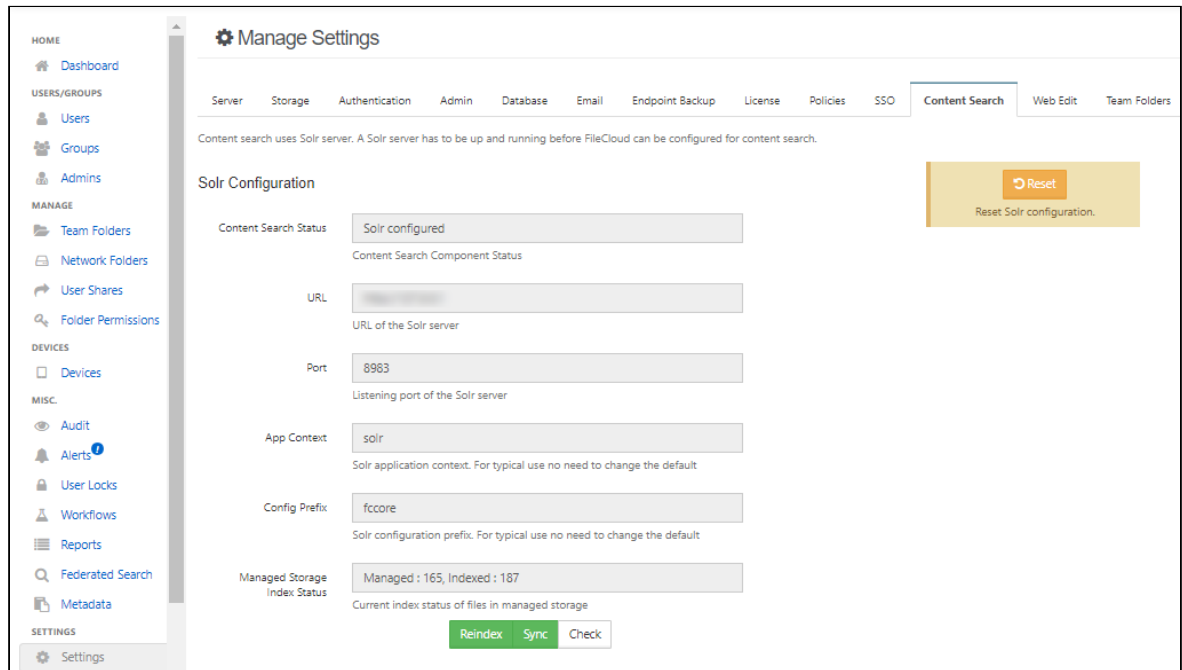
An error message is displayed in a yellow box:

```

ERROR
Unable to create configuration. Please ensure to copy the skeleton config directory
from
/var/www/html/thirdparty/solarium/fcskel as
/opt/solr-5.3.1/server/solr/fccore (on the solr server)
  
```

A red arrow points to the 'Close' button on the error message.

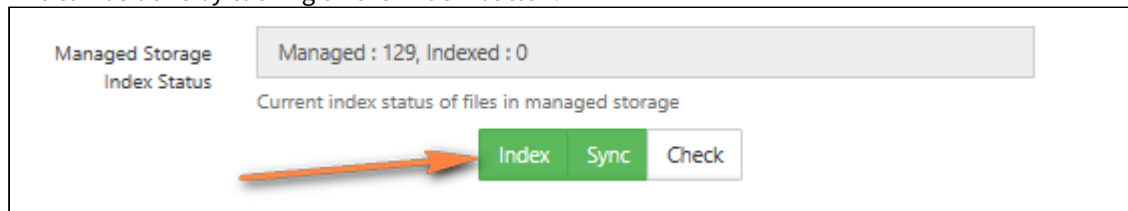
- If you are prompted to copy the configuration directory, after you copy it, click the 'Configure' button again. Upon successful configuration, a new field will appear showing the index status of all 'Managed Storage' files.



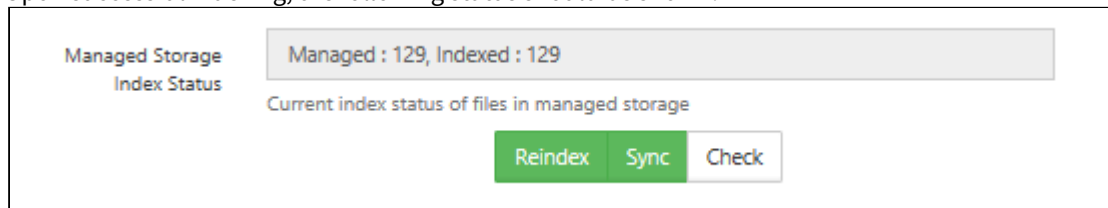
If it is a fresh installation, there will not be any user files. All the new files will be indexed as they get uploaded.

If it is an existing installation, there will be files already managed. Though the new files will be indexed, the existing files has to be indexed separately.

5. This can be done by clicking on the 'Index' button.



Upon successful indexing, the following status should be shown.



Configure a Multi-Site

Multi site Solr configuration is similar to the single site configuration. After a new site is created, repeat the above steps for single except in step 2, specify a unique prefix for the new site. This will configure Solr to create separate index database for each new site.

Note:

Use Unique Prefix for each site.

The screenshot shows the 'Manage Settings' page with the 'Content Search' tab selected. The 'Solr Configuration' section includes the following fields:

- Content Search Status: Solr configured
- Content Search Component Status: (empty)
- URL: (empty)
- Port: 8983
- App Context: solr
- Config Prefix: fcore (highlighted with a red box)
- Managed Storage Index Status: Managed : 165, Indexed : 187

Buttons for 'Reindex', 'Sync', and 'Check' are located at the bottom of the configuration section. A 'Reset' button is also present in the top right corner of the configuration area.

2. Index Files in Managed Storage.

i 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 to 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

After you set up content searching in the Content Search tab, it displays a new section is displayed called **Manage PII Patterns**. In the **Manage PII Patterns** section, you can:

- Add new patterns
- Edit existing patterns
- Search for patterns
- Remove patterns you don't need

Enable PII Search

Enable/Disable searching by advanced Personally Identifiable Information(PII) patterns

☰ Manage PII Patterns + Add ↻

🔍 Filter by name or pattern

Name	Regex	Actions
Belgium National Number	[0-9]{2}.[0-9]{2}.[0-9]{2}-[0-9]{3}.[0-9]{2}	
Croatia Identity Card Number	[0-9]{9}	
Croatia Personal Identification (OIB) Number	[0-9]{10}	
Denmark Personal Identification Number	[0-9]{6}-[0-9]{4}	
EU Debit Card Number	[0-9]{16}	
Finland National ID	[0-9]{6}[-+a][0-9]{3}[0-9a-zA-Z]{1}	
Finland Passport Number	[a-zA-Z]{2}[0-9]{7}	
France Driver's License Number	[0-9]{12}	

💡 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.

A pattern contains the following information:

New PII Search Pattern ✕

Name



Regex

Regex is short for a 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	<ul style="list-style-type: none"> enclosed in square brackets [] a number range uppercase letter range lowercase letter range 	<ul style="list-style-type: none"> 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
Letter example	Poland Passport	a-zA-Z 0-9	2 letters (followed by) 7 numbers	[a-zA-Z]{2}[0-9]{7} ME0123456

To enable and configure PII Search:

1. **Open a browser and log in to the *Admin Portal*.**
2. **From the left navigation panel, click *Settings*.**
3. **On the *Manage Settings* screen, click the *Content Search* tab.**
4. On the *Content Search* tab, after Solr Configuration, check the *Enable PII Search* checkbox.
- e. To add a new pattern to the list, in the *Manage PII Patterns* section, in the top right corner, click *Add*.
- f. To edit an existing pattern, in the *Manage PII Patterns* section, select the pattern and then click the edit icon ().
- g. To remove an existing pattern, in the *Manage PII Patterns* section, select the pattern and then click the delete icon ().
- h. Click *Save*.

4. Search with PII Patterns

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:

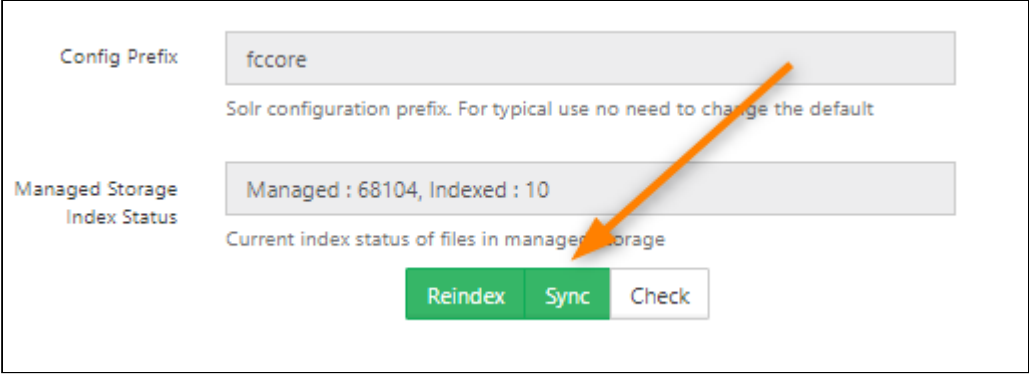
- **Reindex.** Use this option to remove the existing index data completely and do a fresh indexing of all managed storage files. This option is only available after the system has been indexed at least once.
- **Sync.** Use this whenever there is mismatch between the number of managed files and the number of indexed files. Sync will only index the files that are not already indexed.
- **Check.** This displays the latest status of the managed store index.

What do you want to do?

Re-Sync the Index

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.



The screenshot shows a configuration interface with the following elements:

- Config Prefix:** A text input field containing "fccore". Below it, a note reads: "Solr configuration prefix. For typical use no need to change the default".
- Managed Storage Index Status:** A section containing a text box with "Managed : 68104, Indexed : 10" and a note below it: "Current index status of files in managed storage".
- Buttons:** Three buttons are located below the status section: "Reindex" (green), "Sync" (green), and "Check" (white with grey border). An orange arrow points to the "Sync" button.

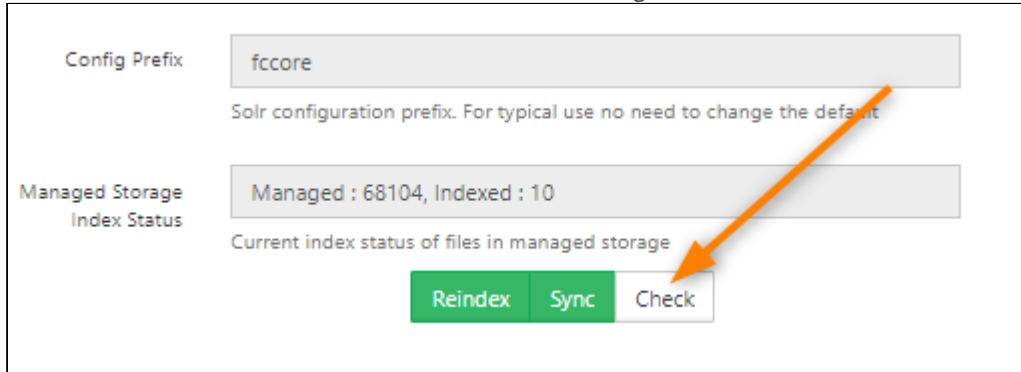
To index files not yet indexed:

1. Open a browser and log in to the *Admin Portal*.

2. From the left navigation panel, click *Settings*.
3. On the *Manage Settings* screen, click the *Content Search* tab.
4. On the *Content Search* tab, under Solr Configuration, click *Sync*.

Check the Status of the Index

Use the *Check* button to see the latest status of the managed store index.



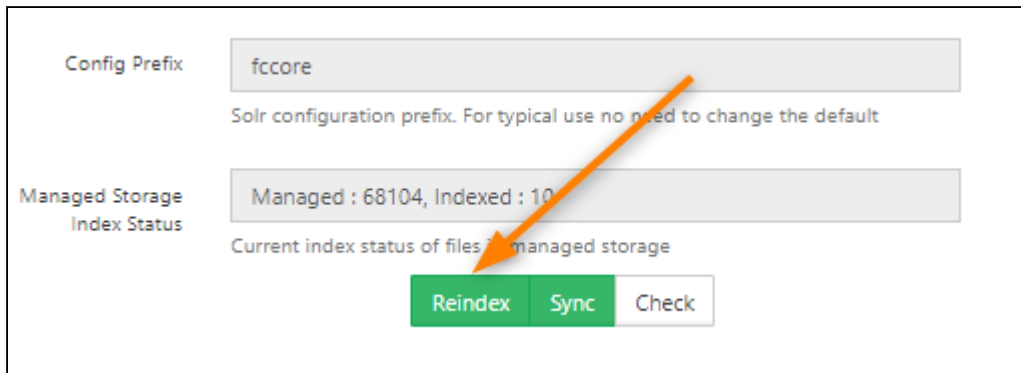
To check the index status:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation panel, click *Settings*.
3. On the *Manage Settings* screen, click the *Content Search* tab.
4. On the *Content Search* tab, under Solr Configuration, click *Check*.

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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation panel, click *Settings*.
3. On the *Manage Settings* screen, click the *Content Search* tab.
4. On the *Content Search* tab, under Solr Configuration, click *Reindex*.

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)**"

Network Folder Details ✕

Network Folder Name:

Network Folder Path:

Permissions:

Smart Mount:

Disable Offline Sync:

Disable Notifications:

Sharing:

Allow Remote Deletion of Files via Offline Sync:

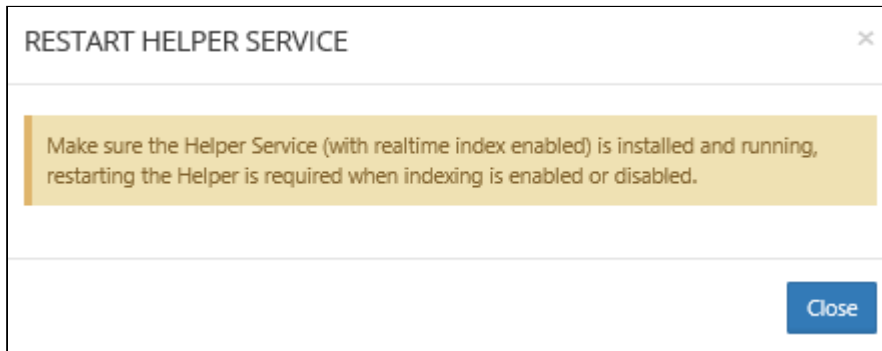
Realtime Index for Automatic Sync and Search (Beta):

Realtime Index Status:

Search Index Status:

Indexed entry count for search.

5. Click 'Update'. A popup prompting to restart NTFS helper service will be shown. Remember to restart the NTFS helper server. Without a restart, the changes will not be in effect.



6. Select the same share again and open the settings dialog for the share. Now the dialog will have 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 few minutes to hours.

Network Folder Details ✕

Network Folder Name	<input type="text" value="NW local"/>		
Network Folder Path	<input type="text" value="C:\FC local network"/>		
Permissions	<input style="border-bottom: 1px solid #ccc;" type="text" value="DEFAULT"/> ▾		
Smart Mount	<input type="checkbox"/>		
Disable Offline Sync	<input type="checkbox"/>		
Disable Notifications	<input type="checkbox"/>		
Sharing	<input style="border-bottom: 1px solid #ccc;" type="text" value="Allow All Shares"/> ▾		
Allow Remote Deletion of Files via Offline Sync	<input type="checkbox"/>		
Realtime Index for Automatic Sync and Search (Beta)	<input checked="" type="checkbox"/>	<input type="button" value="Reindex"/>	
Realtime Index Status	<input type="text" value="0 folders, 0 files"/>	<input type="button" value="Check"/>	
Search Index Status	<input type="text" value="0"/>	<input type="button" value="Check"/>	
Indexed entry count for search.			
<input type="button" value="Manage Users"/>		<input type="button" value="Manage Groups"/>	
<input type="button" value="Clear All Deleted Files"/>			
			<input type="button" value="Update"/> <input type="button" value="Close"/>

Enabling Solr OCR

i Solr OCR is available for Enterprise users and users with OCR licenses beginning with FileCloud Version 20.3.

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. Upgrade to FileCloud 20.3 or higher.
2. Open cloudconfig.php at XAMPP DIRECTORY/htdocs/config/cloudconfig.php
3. 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

4. In the Admin portal, click **Settings** in the navigation pane, and then click the **Content Search** tab.
5. If you are performing an upgrade, click **Reset**.
If you are performing a fresh installation, click **Configure**.
6. Beside **Enable Solr OCR**, click the **Enable** button.

The screenshot displays the 'Content Search' settings in the FileCloud Admin portal. The settings include:

- App Context***: solr (Solr application context. For typical use no need to change the default)
- Config Prefix***: fccore (Solr configuration prefix. For typical use no need to change the default)
- Managed Storage Index Status**: Managed : 241, Indexed : 106 (Current index status of files in managed storage). Below this are buttons for Reindex, Sync, and Check.
- Search Tokenizer**: Update (Search tokenizer update available. Click to update.)
- Enable Solr OCR**: Enable (OCR is disabled)
- Enable PII Search**:

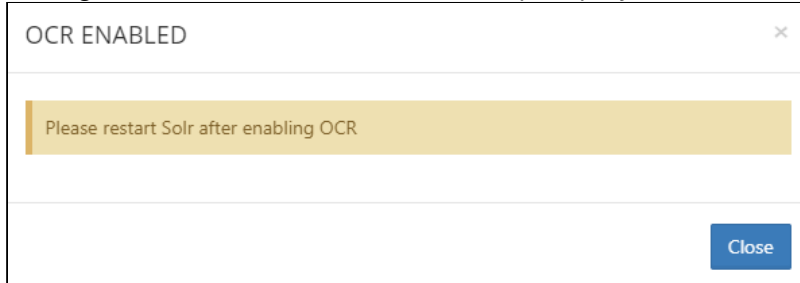
On the right side, there is a yellow box containing a **Reset** button and the text "Reset Solr configuration." A red arrow points to this button.

A confirmation box warns you that enabling OCR will require you to restart Solr.

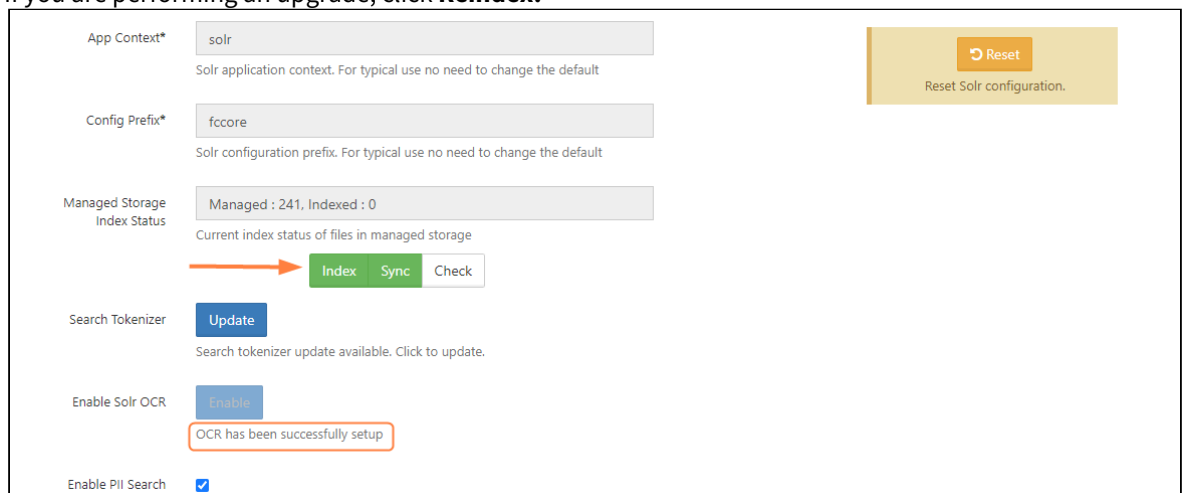


7. Click **OK**.

A dialog box confirms that OCR is enabled and prompts you to restart Solr.



8. Restart the Solr (Content Search) service from the FileCloud control panel.
9. In the Admin portal, go to **Settings**, and click the **Content Search** tab again.
10. Confirm that:
 - The **Enable** button is disabled
 - The message below the button says **OCR has been successfully setup**.
11. 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**.

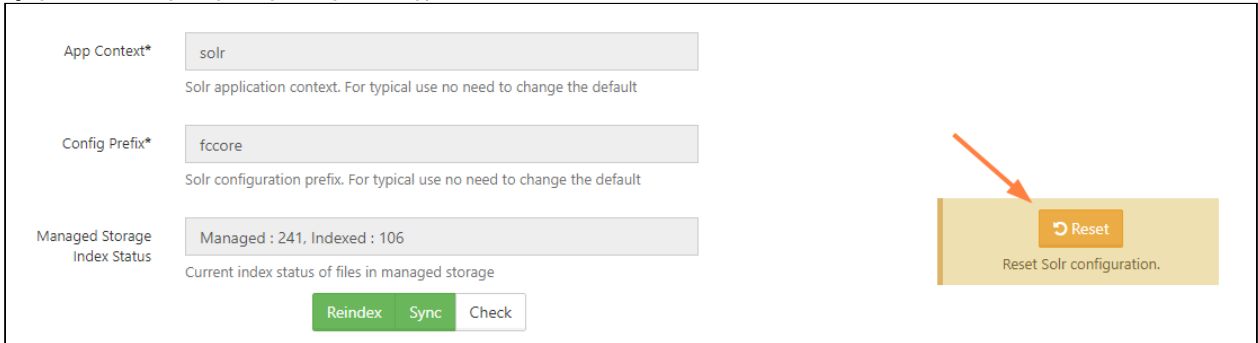


Install and enable Solr OCR on Linux Ubuntu

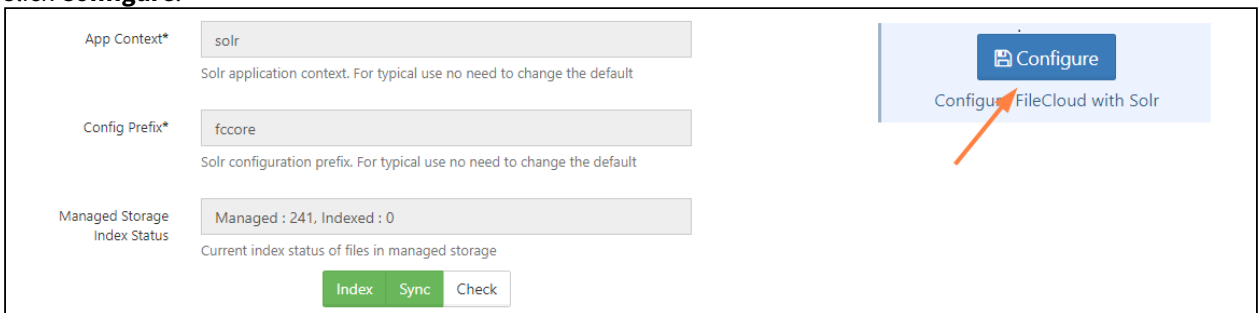
Follow these instructions on Linux when performing a fresh installation of FileCloud or when performing an upgrade to the OCR component license.

1. Upgrade to FileCloud 20.3 or higher.

2. Run `fileclouddcp -t`
3. In the Admin portal, click **Settings** in the navigation pane, and then click the **Content Search** tab.
4. 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/`).



5. Inspect the file **solrconfig.xml** inside `/var/www/html/thirdparty/overrides/solarium/Solarium/fcshell/conf` and uncomment the line containing **parseContext.xml**.
6. In `/var/www/html/thirdparty/overrides/solarium/Solarium`, copy the folder **fcshell** 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**).
7. In the Admin portal, go to **Settings**, and click the **Content Search** tab again.
8. Click **Configure**.



9. Confirm that the **Enable** button is disabled and the message below the button is **OCR has been successfully setup**.

10. To build or rebuild the search index with OCR for images and PDFs with text, click **Index**.

App Context*
Solr application context. For typical use no need to change the default

Config Prefix*
Solr configuration prefix. For typical use no need to change the default

Managed Storage Index Status
Managed : 241, Indexed : 0
Current index status of files in managed storage

Index Sync Check

Search Tokenizer
Search tokenizer update available. Click to update.

Enable Solr OCR
OCR has been successfully setup

Enable PII Search

Install and enable Solr OCR on other Linux distributions:

- To confirm that Tesseract is set up, enter:

```
filecloudcp -t
```

You should receive the response **Tesseract is already installed and configured.**

- 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
```

- Restart Apache.

```
systemctl restart apache2
```

- 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/fcore_<sitename>
```

- In the FileCloud admin portal, go to **Settings > Content Search**, and click **Enable** next to **Enable Solr OCR**.

Enable Solr OCR
OCR is disabled

- Restart Solr.

```
systemctl restart solr
```

7. Reload the FileCloud **Content Search** screen.
The note below the **Enable** button should say **Image and PDF OCR is enabled**.

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.

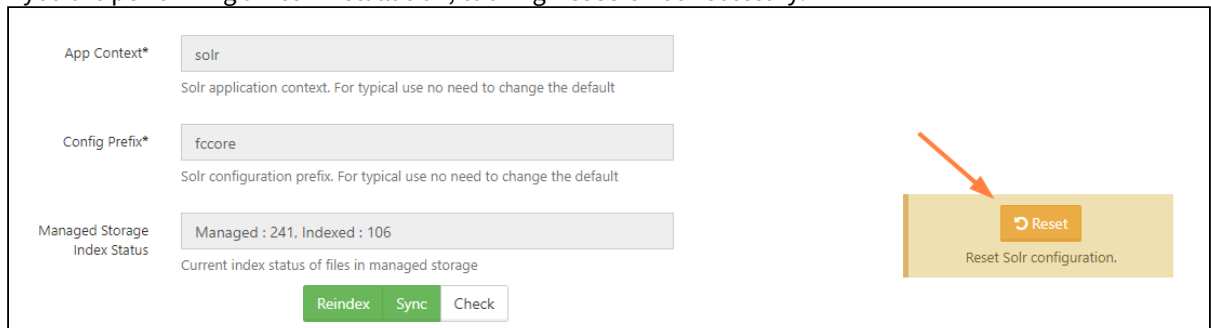
1. Upgrade to FileCloud 20.3 or higher
2. Set the Tesseract environment variables:
 - For Windows, add the following to solr.in.cmd:

```
SET PATH=%PATH%;C:\xampp\tesseractocr
SET TESSDATA_PREFIX=C:\xampp\tesseractocr\tessdata
```

- For Nix, add the following to solr.in.sh (or define the environment variables globally)

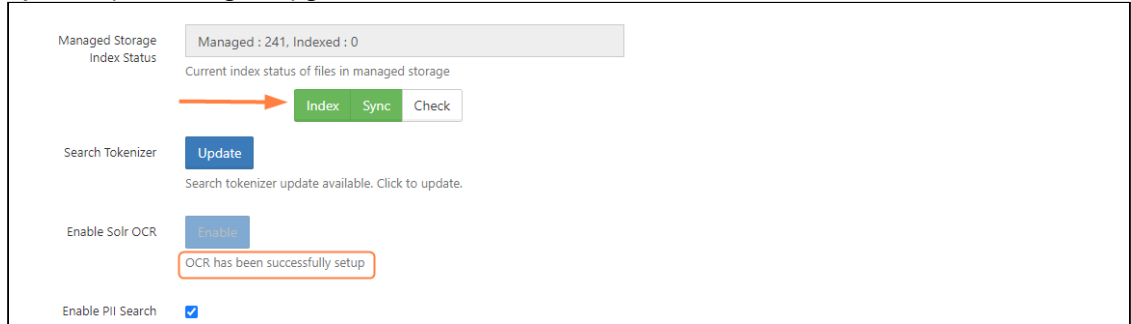
```
PATH="/path/to/tesseractocr:$PATH"
TESSDATA_PREFIX=/path/to/tesseractocr/tessdata
```

3. In the Admin portal, click **Settings** in the navigation pane, and then click the **Content Search** tab.
4. If you are performing an upgrade, click **Reset**.
If you are performing a fresh installation, clicking **Reset** is not necessary.



5. 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**.
6. Restart the Solr (Content Search) service from the FileCloud control panel.
7. In the Admin portal, go to **Settings**, and click the **Content Search** tab again.
8. Confirm that the label beneath the **Enable Solr OCR** button says **OCR has been successfully setup**.
9. To build or rebuild the search index with OCR for images with text and PDFs.
 - If you are performing a fresh installation, click **Index**.

- If you are performing an upgrade, click **Reindex**.



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 *out of memory* error in its logs, you can use the following tip to see if this solves the issue.

By default, Solr ships with 512MB for heap size. In some installations with large number of files (especially text based documents), this heap memory is not enough. SOLR might crash in these cases with 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 is not stopping 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 up of the system memory and increase the JAVA heap limit

Update 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:

Changing 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 "SolrRocks"

Enable Solr authentication

```
{
  "authentication":
  {
    "blockUnknown": true,
    "class":"solr.BasicAuthPlugin",
    "credentials": {
      "solr":"IV0EHq10nNrj6gvRCwvFwTrZ1+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. To change the password please use the following command:

```

curl -user solr:SolrRocks http://localhost:8983/solr/admin/authentication -H 'Content-type:application/json' -d '{"set-user":{"solr":"NewPassword"}}'

```

6. To change the password for SSL protected SOLR server please 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: "solr" username can be changed to anything but it has to be replaced for all the steps (including the initial config).

7. To make solr daemon detect Solr status you need to update the following config files:

Changing 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 necessary only if authentication is enabled on solr

SOLR With SSL

To setup SSL with Solr, you would need the following :

- Private or Self Signed SSL certificates
- A working Solr installation

Option (1) To configure SSL using private certificates, the steps below need to be followed

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
```

i It is required to put the server certificate file first, and then if applicable, the intermediate certificate file(s) ending with 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
```

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, the steps below need to be followed

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 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/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. Restart Solr

```
service solr restart
```

Solr High Availability Setup with Pacemaker and Corosync

i 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 **solr01**, **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/solrfcdata**, enter:

```
mkdir /opt/solrfcdata
```

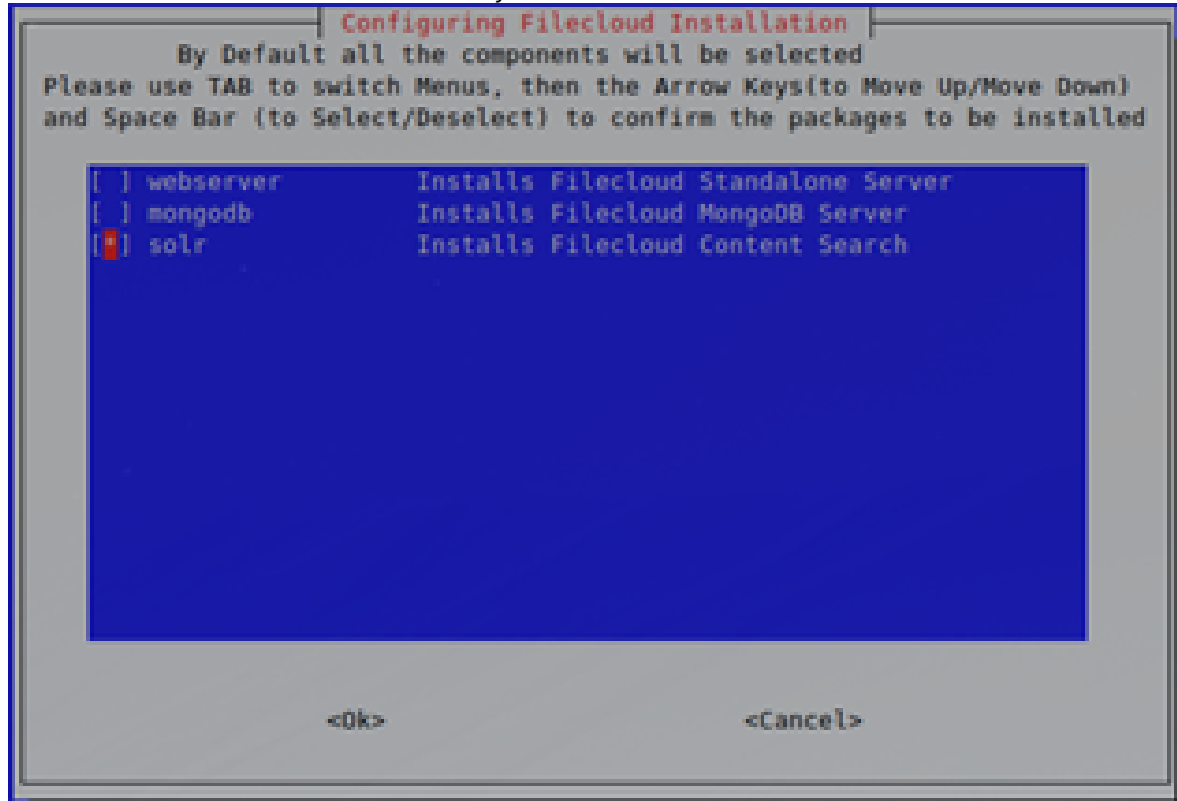
4. Mount the NFS filesystem under **/opt/solrfcdata**:

```
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:

```
● solrd.service - Apache SOLR
   Loaded: loaded (/etc/systemd/system/solrd.service; static; vendor preset: disabled)
   Active: active (running) since Fri 2022-07-29 11:24:58 CEST; 9s ago
     Process: 28163 ExecStart=/opt/solr/bin/solr start (code=exited, status=0/SUCCESS)
    Main PID: 28212 (java)
      CGroup: /system.slice/solrd.service
              └─28212 java -server -Xms512m -Xmx512m -XX:+UseG1GC -XX:+PerfDisableSharedMem -XX:+ParallelRefProcEnabled -XX:MaxGCPauseMillis=250

Jul 29 11:24:48 centos7-a01-49 systemd[1]: Starting Apache SOLR...
Jul 29 11:24:58 centos7-a01-49 solr[28163]: [2188 blob data]
Jul 29 11:24:58 centos7-a01-49 solr[28163]: Started Solr server on port 8983 (pid=28212). Happy searching!
Jul 29 11:24:58 centos7-a01-49 systemd[1]: Started Apache SOLR.
```

- 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.

- On **solr01**, add the Qdevice (**solr03**) to the cluster:

```
pcs quorum device add model net host=solr03 algorithm=lms
```

- 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

- On **solr01** and **solr02**, set up automatic soft-watchdog module to load whenever you reboot:

```
echo softdog > /etc/modules-load.d/watchdog.conf
```

- 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
```

- 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.

- On **solr-ha**, install haproxy:

```
yum install -y haproxy
```

- On **solr-ha**, configure **haproxy** to redirect to an active solr node.
 - Back up **/etc/haproxy/haproxy.cfg**.

```
mv /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg_bck
```

- 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.
```

- 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
```

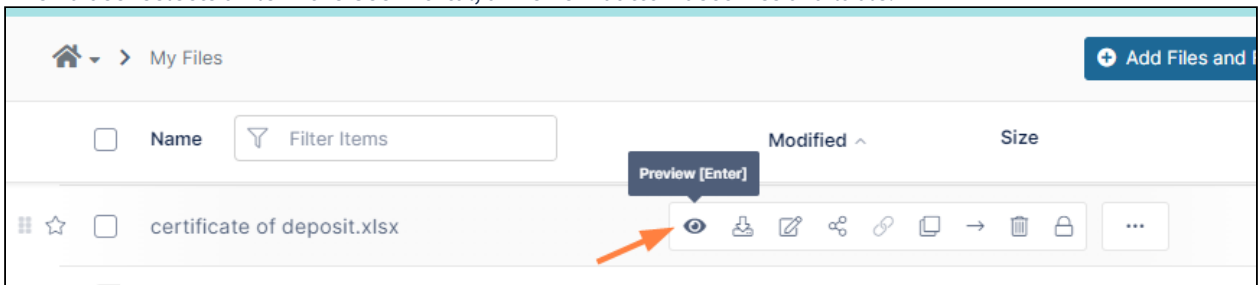
```
$ php searchindexcli.php --importunindexed --targetfile=unindexed-1626184138.csv
1: Meta indexed /tester223
2: Content indexed /tester223/SensitivityLabel.xlsx
3: Content indexed /tester223/SensitivityLabel.docx
Done in 5754.4114ms. Indexed 3 files.
```

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](#).

- When a user selects a file in the User Portal, a Preview button becomes available.



When the user clicks the **Preview** button, a separate window opens showing an image of the file. Beginning in FileCloud 22.1, 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.

The screenshot shows a preview window for a file named "certificate of deposit.xlsx". An orange arrow points to the "Open With" button in the top right corner. A dropdown menu is open, showing three options: "Desktop (Excel)", "Google Sheets", and "Office Online". Below the menu, a spreadsheet is visible with columns labeled "YEARS" (5, 10, 12, 15, 20, 25, 30) and rows of numerical values. A "Rate slicer to filter table" is visible on the right side of the spreadsheet.

YEARS						
5	10	12	15	20	25	30
\$175.28	\$92.01	\$78.17	\$64.35	\$50.59	\$42.39	\$36.96
\$176.37	\$93.14	\$79.31	\$65.51	\$51.78	\$43.61	\$38.22
\$177.47	\$94.27	\$80.45	\$66.68	\$52.99	\$44.86	\$39.51
\$178.58	\$95.41	\$81.61	\$67.86	\$54.22	\$46.13	\$40.82
\$179.69	\$96.56	\$82.78	\$69.06	\$55.46	\$47.42	\$42.16
\$180.80	\$97.72	\$83.96	\$70.27	\$56.72	\$48.73	\$43.52
\$181.92	\$98.89	\$85.15	\$71.49	\$58.00	\$50.06	\$44.90
\$183.04	\$100.06	\$86.34	\$72.72	\$59.29	\$51.41	\$46.31
\$184.17	\$101.25	\$87.55	\$73.97	\$60.60	\$52.78	\$47.74
\$185.30	\$102.44	\$88.77	\$75.23	\$61.92	\$54.17	\$49.19
\$186.43	\$103.64	\$90.00	\$76.50	\$63.26	\$55.58	\$50.67
\$187.57	\$104.85	\$91.24	\$77.78	\$64.62	\$57.01	\$52.16
\$188.71	\$106.07	\$92.49	\$79.08	\$66.00	\$58.46	\$53.68
\$189.86	\$107.29	\$93.75	\$80.39	\$67.38	\$59.92	\$55.22
\$191.01	\$108.53	\$95.02	\$81.71	\$68.79	\$61.41	\$56.78
\$192.17	\$109.77	\$96.30	\$83.04	\$70.21	\$62.91	\$58.36
\$193.33	\$111.02	\$97.59	\$84.39	\$71.64	\$64.43	\$59.96
\$194.49	\$112.28	\$98.88	\$85.74	\$73.09	\$65.97	\$61.57
\$195.66	\$113.55	\$100.19	\$87.11	\$74.56	\$67.52	\$63.21








2.







To include watermarks on previewed documents, see [Enabling Watermarks On Previews](#)

i PDF file preview will work even if Document Preview is not installed. Document Preview is required to preview files like PSD and AI.
The ability to preview a file without using LibreOffice is available in FileCloud version 19.1 and later.
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](#)


File types that can be previewed

	Extensi on	Registe red To	Availa ble in FileClo ud Versio n	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.
 WORD	.DOC	Microsof t	4.0	Microsoft WORD files created in versions 2003 and earlier.
 WORD	.DOCX	Microsof t	4.0	Microsoft WORD files created in versions 2007 and later.
 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.
 PowerPoint	.PPT	Microsof t	4.0	Microsoft PowerPoint files created in versions 2003 and earlier.

	Extensi on	Registe red To	Availa ble in FileClo ud Versio n	Description
 PowerPoint	.PPTX	Microsof t	4.0	Microsoft PowerPoint files created in versions 2007 and later.
 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.
 Excel	.XLS	Microsof t	4.0	Microsoft Excel files created in versions 2003 and earlier.
 Excel	.XLSX	Microsof t	4.0	Microsoft Excel files created in versions 2007 and later.
 AutoCAD	.DWF, . DWG, .D XF (and 60+ other AutoCA D formats).	AutoCA D	22.1	2D and 3D architectural drawings in AutoCAD file formats.
OpenDocu ment text	.ODT			Documents created by word processors that use OpenDocument Text File format, such as LibreOffice and OpenOffice.

	Extensi on	Registe red To	Availa ble in FileClo ud Versio n	Description
Oasis graphic and spreadshee t files	.ODF .ODS			Binary files used to define data structures.
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			

For everything besides the DICOM and AutoCAD files, FileCloud uses LibreOffice to do the document conversion so that you can see the preview.

 Looking for instructions on how to install Document Preview on Ubuntu or RHEL?
Starting in FileCloud version 18.1, by default everything you need for Libre and DocConverter is installed.

Also see: [Document Preview](#)

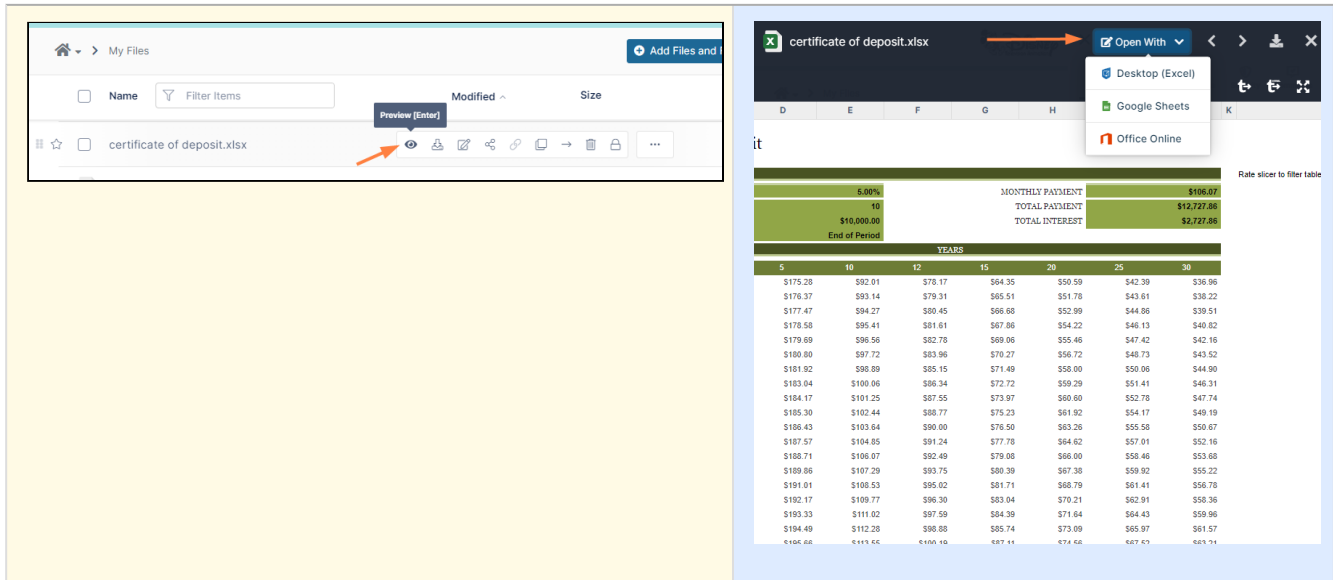
Document Preview

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:

- Enable Quick JS Preview (*FileCloud version 19.1 and later*)
- DocConverter with LibreOffice (*FileCloud version 18.2 and earlier*)
- 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 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

For this FileCloud uses a java program based on Apache's [PDFBox](#). Document converter also will use LibreOffice libraries to convert documents to PDF.

- i** FileCloud version 19.1 and later already includes the Doc Converter jar file and it is installed automatically.
- You do not need to download it as you did in earlier versions.

1. Start the Doc Converter 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	<ul style="list-style-type: none"> • DOCX • PPTX • XLSX • PDF • video: MP4, WebM, MOV • audio: MP3, OGG, WAV, M4A • AI • DICOM • PSD 	None	<ul style="list-style-type: 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.

Tool	File Types Previewed	Preview Keys	Interactions with Other Tools/ Other Notes
DocConverter with LibreOffice	<ul style="list-style-type: none"> • DOC, DOCX • PPT, PPTX • XLS, XLSX • TXT • ODT (<i>OpenDocument text created by LibreOffice and others</i>) • ODG (<i>Oasis graphic files</i>) • ODS (<i>Oasis spreadsheets</i>) • PDF • video: MP4, WebM, MOV • audio: MP3, OGG, WAV, M4A • AI • DICOM 	SHIFT + Preview	<ul style="list-style-type: none"> • 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
WOPI	<ul style="list-style-type: none"> • DOC, DOCX • PPT, PPTX • XLS, XLSX • video: MP4, WebM, MOV • audio: MP3, OGG, WAV, M4A 	None	<ul style="list-style-type: 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.

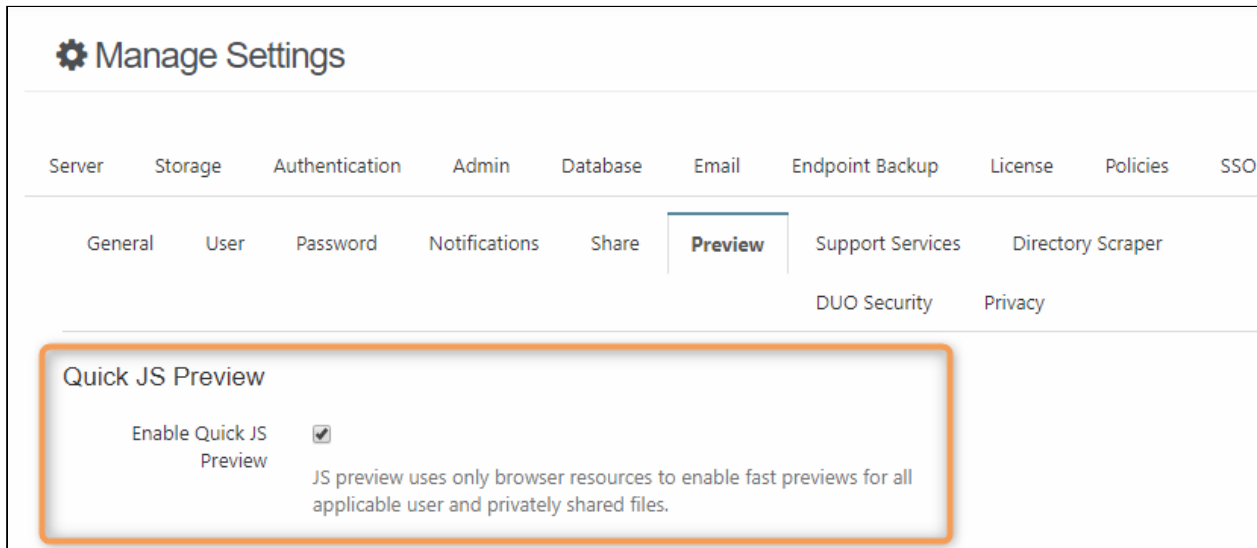
 To configure document preview, click on a method to see the steps:

Configure Quick JS Preview for FileCloud 19.1 and Later

PRE-REQUISITES 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 fcdoconverter stop
```


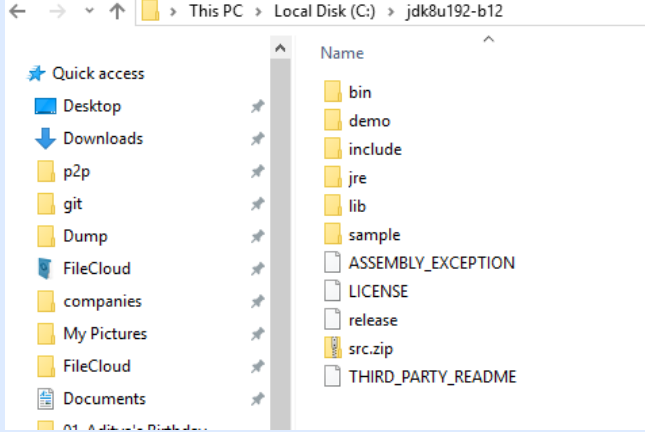


To provide a preview using Quick JS:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation panel, under *SETTINGS*, click *Settings*.
3. On the *Manage Settings* window, select the *Misc.* tab, and then the *Preview* tab.
4. On the *Preview* screen, next to *Enable Quick JS Preview*, select the checkbox.

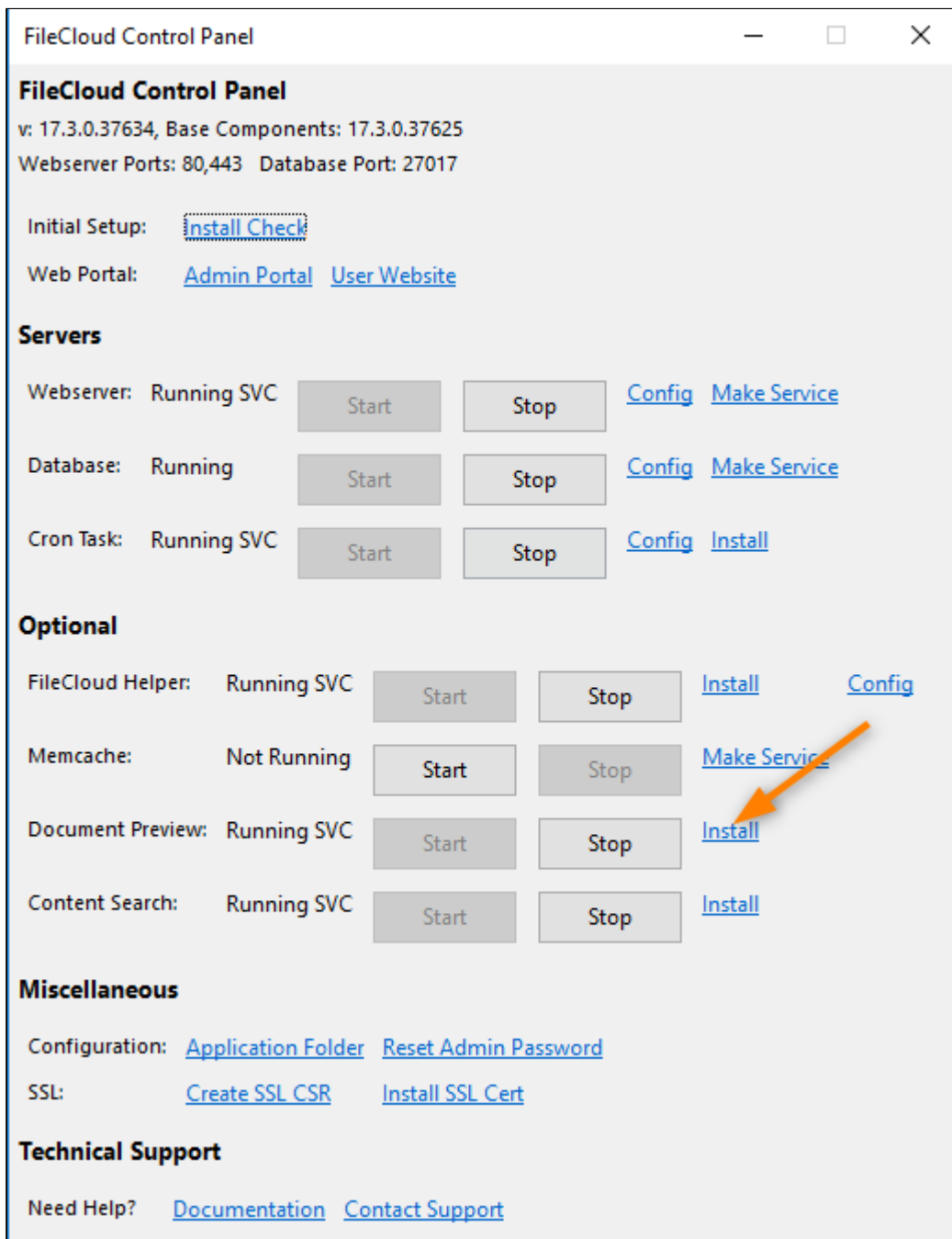
Configure Document Preview for FileCloud 18.2 and Earlier

1. Install OpenJDK:

	<p>1. Download Open JDK 8 from https://adoptopenjdk.net/</p>
	<p>2. Create a new folder in the C: directory. (In the example diagram, jdk8u192-b12 is the name of the new folder.)</p> <p>3. Extract the Open JDK file you downloaded into the new folder.</p>

2. Install Document Preview

- a. Open FileCloud Control Panel.
- b. To install Document Preview, click *Install*.



The screenshot displays the FileCloud Control Panel interface. At the top, it shows the version (v: 17.3.0.37634) and base components (17.3.0.37625), along with webserver and database ports. Below this, there are links for 'Initial Setup' (Install Check) and 'Web Portal' (Admin Portal, User Website).

The 'Servers' section lists three services: Webserver (Running SVC), Database (Running), and Cron Task (Running SVC). Each has 'Start' and 'Stop' buttons, and links for 'Config' and 'Make Service'.

The 'Optional' section lists four services: FileCloud Helper (Running SVC), Memcache (Not Running), Document Preview (Running SVC), and Content Search (Running SVC). Each has 'Start' and 'Stop' buttons. The 'Document Preview' service has an 'Install' button, which is highlighted by an orange arrow. Other services have 'Install' and 'Config' buttons.

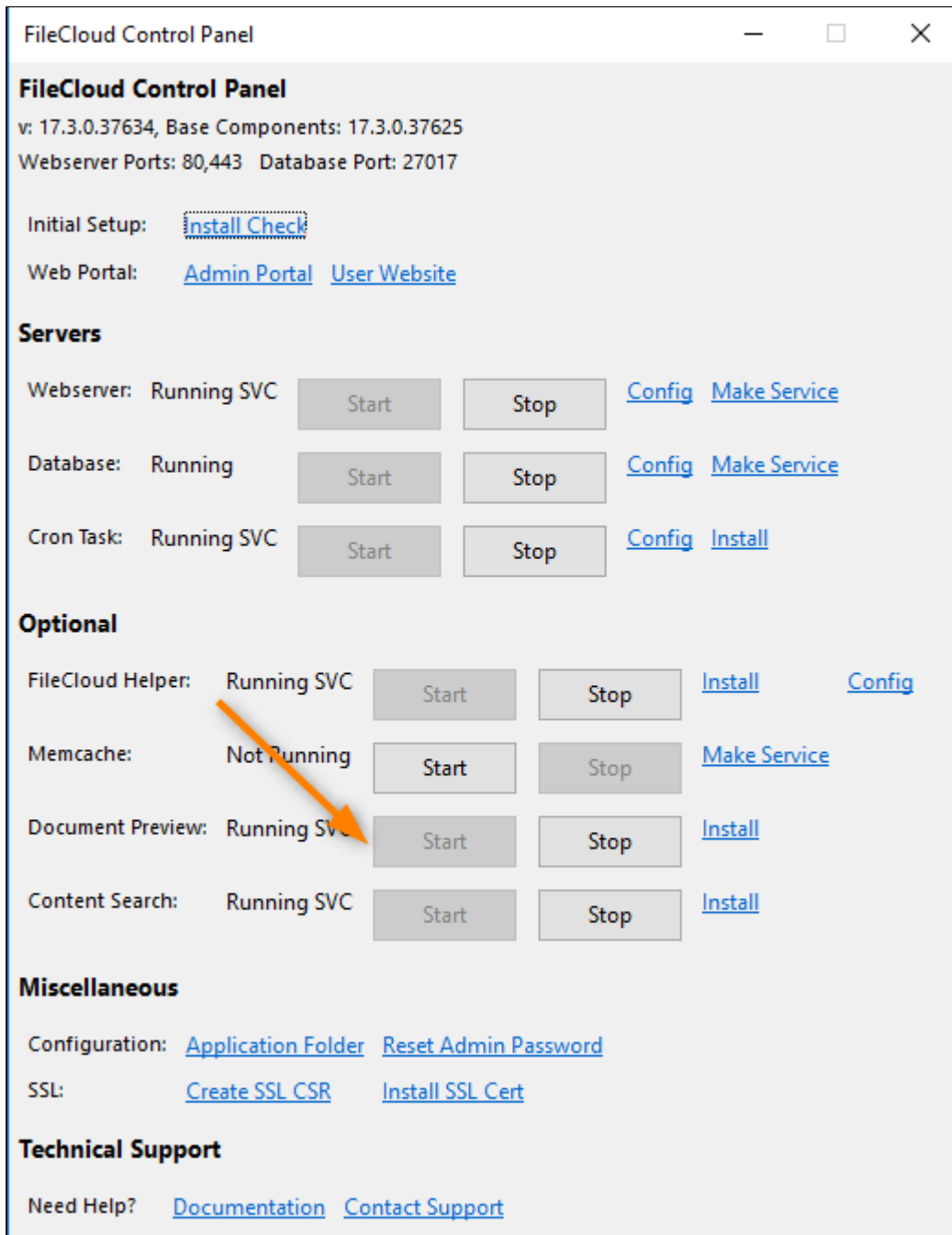
The 'Miscellaneous' section includes links for 'Configuration' (Application Folder, Reset Admin Password) and 'SSL' (Create SSL CSR, Install SSL Cert).

The 'Technical Support' section includes links for 'Need Help?' (Documentation, Contact Support).

3. Start the Service:

- a. Open FileCloud Control Panel.

b. To start the Document Preview service, click *Start*.



FileCloud Control Panel

v: 17.3.0.37634, Base Components: 17.3.0.37625
 Webserver Ports: 80,443 Database Port: 27017

Initial Setup: [Install Check](#)

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

Servers

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

Optional

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

Miscellaneous

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

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

Technical Support

Need Help? [Documentation](#) [Contact Support](#)

4. Configure FileCloud

⚠ If you are running the multi-site configuration, please follow these steps on the root site.

- Open a browser and log in to the *Admin Portal*.
- From the left navigation panel, under *SETTINGS* click *Settings*.

c. On the *Manage Settings* screen, select the *Misc.* sub-tab.

d. In *Office Location*, type in the correct path for the Libre Office portable installation. Normally you would type in the following path:

```
C:\xampp\LibreOfficePortable\App\LibreOffice64\program
```

e. Next to *Enable FC Document Converter*, select the checkbox.

Configure Preview using WOPI

Administrators can configure online previewing using WOPI for any supported document from within the User Portal.

1. In the Admin UI, go to Settings > Web Edit tab.
2. Configure online editing using WOPI at [Microsoft Office Online Cloud For Web Edit](#)
3. During your configuration, check **WOPI Preview**.

To include watermarks on previewed documents, see [Enabling Watermarks On Previews](#)

Setting up Document Preview for large file size

To enable this option, open cloudconfig.php at

Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php

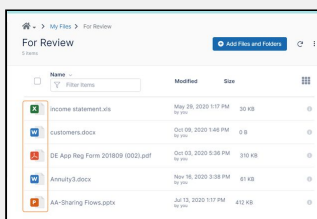
Linux Location: /var/www/config/cloudconfig.php

and add the following

```
define("TONIDO_CLOUD_DOCPREVIEW_SIZE_LIMIT", "20485760"); //20MB
```

FileCloud Document Converter

Administrators can use a Java-based service called FileCloud Document Converter to provide thumbnail images.



Name	Modified	Size
income statement.xls	May 29, 2020 1:17 PM	30 KB
customers.docx	Oct 09, 2020 1:48 PM	0 B
DE App Reg Form 201809 0002.pdf	Oct 01, 2020 5:38 PM	310 KB
Annuity3.docx	Nov 16, 2020 3:28 PM	61 KB
AA-Sharing Flows.pptx	Jul 13, 2020 1:17 PM	412 KB


For this FileCloud uses a java program based on Apache's [PDFBox](#).

Document converter also will use LibreOffice libraries to convert documents to PDF.

- 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

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/fcdocconverter (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 Doconverter
 - a. Edit the file WWWROOT/config/cloudconfig.php and add the following definition line:
define('TONIDOCLOUD_FCDOCCONVERTER_SECURITY_KEY','hello#\$\$%world');

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 Server

Note: FileCloud always displays thumbs for graphic files (jpg, png, ...) regardless of this setting.

To enable thumbnails for a document in FileCloud:

1. Open a browser and log into the *Admin Portal*.
2. From the left navigation panel, click *Settings*.
3. Click the *Misc* tab.
4. Click the *Preview* sub tab.
5. Next to *Enable Document Converter*, select the checkbox.
6. Next to *Enable Document Thumb*, select the checkbox.

Figure 1. The Admin Portal option to enable Document Converter and thumbs.

The screenshot shows the FileCloud Server settings interface. At the top, there are navigation tabs: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, and Policies. Below these, there are sub-tabs: Team Folders, Third Party Integrations, **Misc**, and Reset. The 'Misc' tab is active, and within it, the 'Preview' sub-tab is selected. Other sub-tabs include General, User, Password, Notifications, Share, Support Services, and Directory Scraper. Below the sub-tabs, there are additional settings: DUO Security, Privacy, and 2FA.

Quick JS Preview

Enable Quick JS Preview

- JS preview uses only browser resources to enable fast previews for all applicable user and privately shared files.

Document Preview Support

Office Location

[Check Path](#)

Specify 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

- Show combine PDF Option. 'Document Converter' is necessary for this functionality.

Anonymous Access Watermark

Enter non-empty string to watermark all public access of previews

Now when a user logs on to the User Portal, the file listing will show the thumbnail as seen in Figure 2.

Figure 2. User Portal display of thumbnails.

Home > My Files > Financial

Financial

6 items

[+ Add Files and Folders](#)

<input type="checkbox"/>	Name ^	Filter Items	Modified	Size
<input checked="" type="checkbox"/>	Insurance Policy 1.docx		May 29, 2020 1:26 PM by you	25 KB
<input checked="" type="checkbox"/>	Insurance Policy 2.docx		May 29, 2020 1:24 PM by you	25 KB
<input checked="" type="checkbox"/>	bank statement1.pdf		May 17, 2021 2:24 PM by you	70 KB
<input type="checkbox"/>	bank statement1.xlsx		Sep 28, 2020 11:45 AM by you	34 KB
<input type="checkbox"/>	bank statement2.xlsx		May 29, 2020 1:23 PM by you	34 KB
<input type="checkbox"/>	insurance form.docx		Sep 28, 2020 11:46 AM by you	61 KB

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 11 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 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 11.02 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.

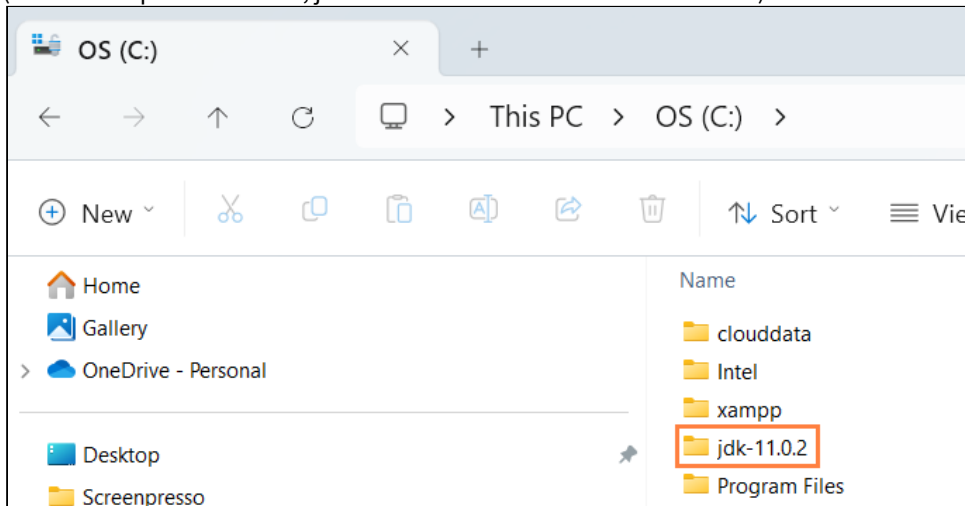
💡 FileCloud's Content Search feature also requires OpenJDK 11.02. If you already have this installed, you can skip these steps.

To install Doc Converter for Windows:

1. Install OpenJDK.

To install OpenJDK:

1. Download **Open JDK 11.02+9** from <https://jdk.java.net/archive/>.
2. Create a new folder in the C: drive.
(In the example screenshot, jdk-11.0.2 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

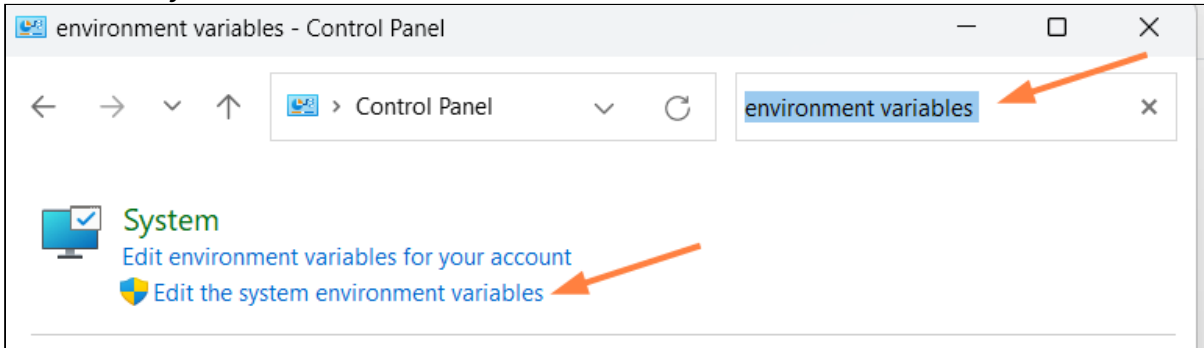
Setting the path and environment variables will differ depending on the version of Windows you have on your computer. These instructions were designed for Windows 11.

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

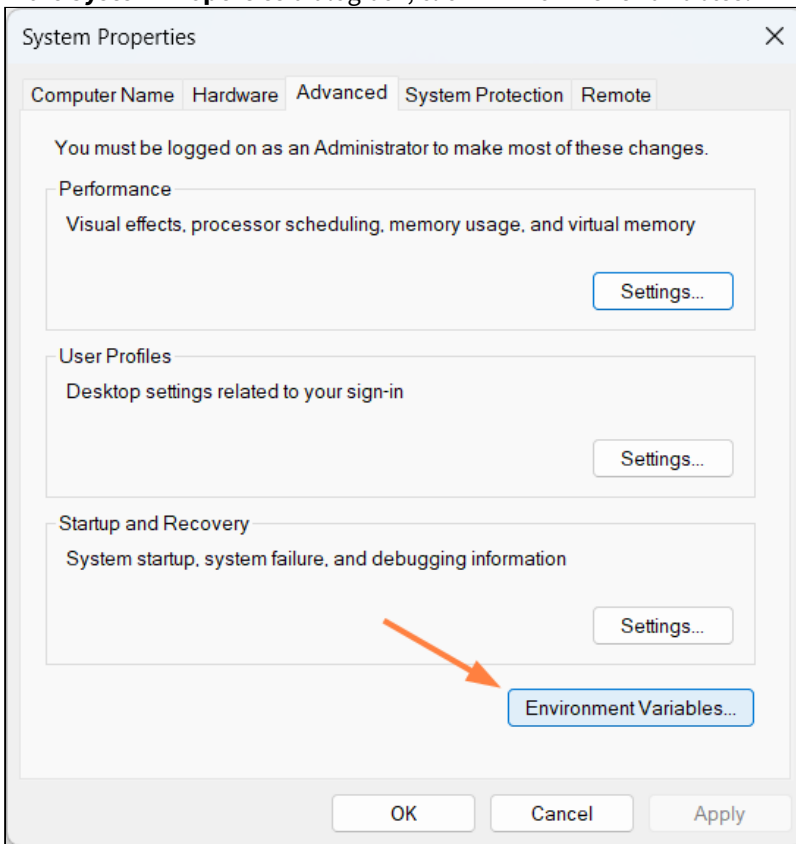
To set the JAVA_Home path:

1. Open the Windows Control Panel.
2. Enter **environment variables** in the search bar.

3. Click **Edit the system environment variables**.



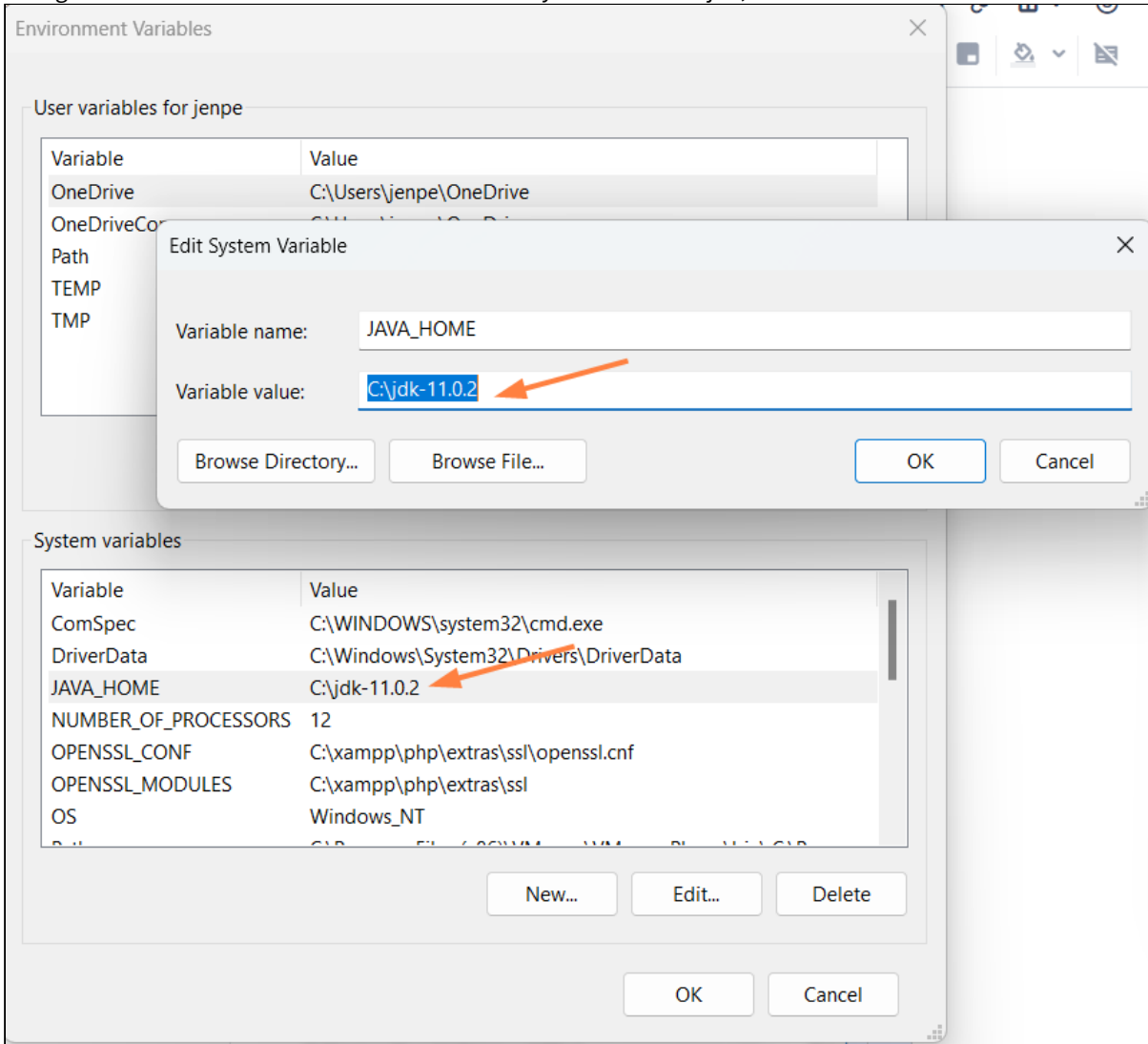
4. In the **System Properties** dialog box, click **Environment Variables**.



The **Environment Variables** dialog box opens.

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

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



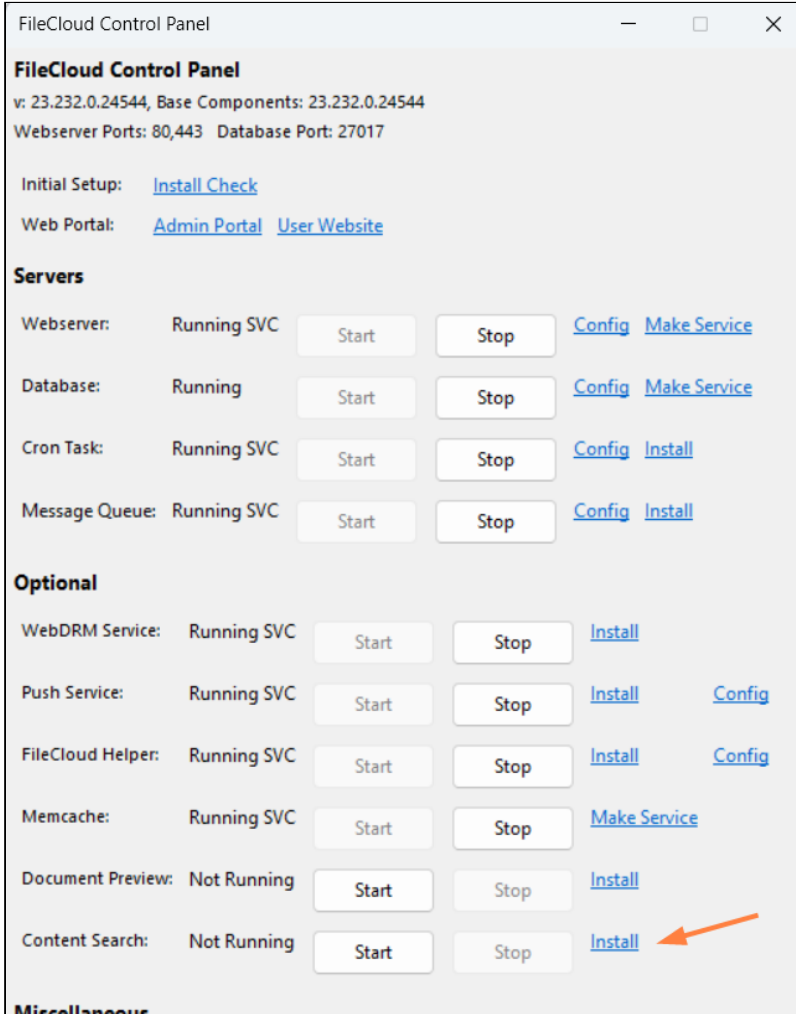
7. In the **Environment Variables** dialog box, click **OK**.

3. Use the FileCloud Control Panel to install Content Search

To install and start Content Search:

1. Open the FileCloud Control Panel.

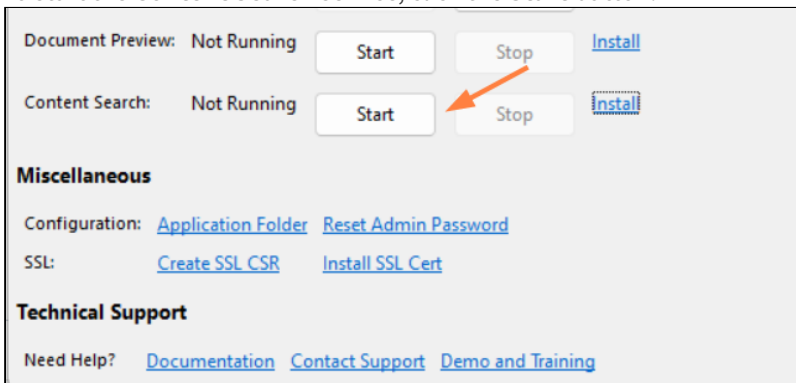
- Next to **Content Search**, click **Install**.



The screenshot shows the FileCloud Control Panel interface. At the top, it displays the version (v: 23.232.0.24544) and base components (23.232.0.24544). Below this, there are links for 'Initial Setup' (Install Check) and 'Web Portal' (Admin Portal, User Website). The main section is divided into 'Servers' and 'Optional' services. Each service row includes its status, 'Start' and 'Stop' buttons, and links for 'Config' and 'Install' or 'Make Service'. An orange arrow points to the 'Install' link for the 'Content Search' service, which is currently 'Not Running'.

Service	Status	Start	Stop	Config	Install/Make Service
Webserver:	Running SVC	Start	Stop	Config	Make Service
Database:	Running	Start	Stop	Config	Make Service
Cron Task:	Running SVC	Start	Stop	Config	Install
Message Queue:	Running SVC	Start	Stop	Config	Install
Optional					
WebDRM Service:	Running SVC	Start	Stop	Install	
Push Service:	Running SVC	Start	Stop	Install	Config
FileCloud Helper:	Running SVC	Start	Stop	Install	Config
Memcache:	Running SVC	Start	Stop	Make Service	
Document Preview:	Not Running	Start	Stop	Install	
Content Search:	Not Running	Start	Stop	Install	

- To start the **Content Search** service, click the **Start** button.



This is a close-up view of the 'Content Search' service row from the previous screenshot. It shows the 'Not Running' status, a 'Start' button, a 'Stop' button, and an 'Install' link. An orange arrow points to the 'Start' button.

Document Preview:	Not Running	Start	Stop	Install
Content Search:	Not Running	Start	Stop	Install

Miscellaneous

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

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

Technical Support

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

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 and the configuration on the FileCloud config to reach the service.

Change the default port in the service

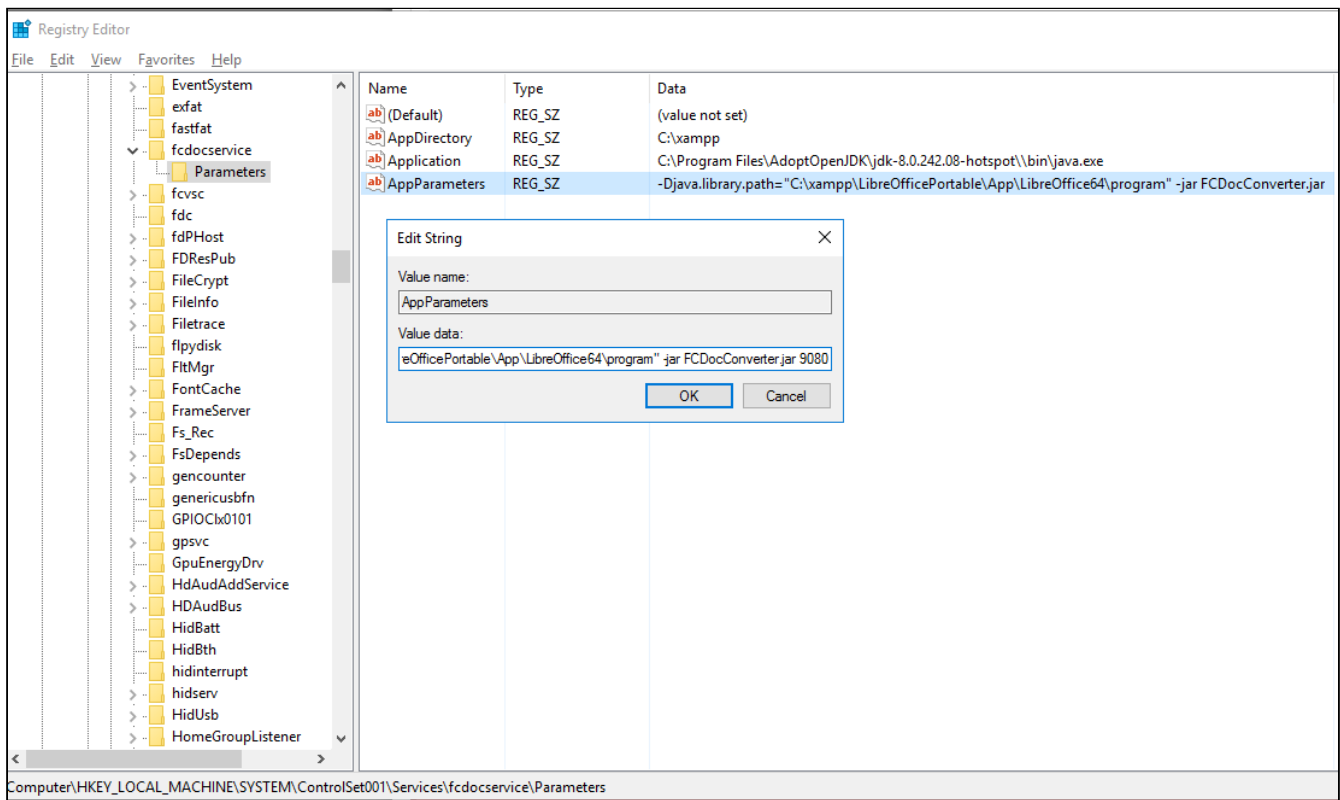
To change the default port on the service, you need to change the execute command string.

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("TONIDO_CLOUD_FCDOC_CONVERTER_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.

The IP address can be added at the end:

```
java -Djava.library.path="D:\xampp\LibreOfficePortable\App\LibreOffice64\program" -jar
FCDocConverter.jar 8080 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("TONIDO_CLOUD_FCDOC_CONVERTER_URL", "http://192.168.1.108:9080");
```

Overriding Thumb and Preview Size Limits

By default, the size limit 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.

i 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('TONIDO_CLOUD_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](#)
- [LibreOffice Ubuntu/RHEL Instructions](#)

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.
There are two steps to enable preview.

Multisite

If you are running a multi-site configuration, please follow these steps on the root site.

- a. Log in to the Administration Portal
- b. Click **Settings** on the left navigation panel
- c. Click the **Misc** tab
- d. Check **Quick JS Preview** if it is not already checked.
- e. Enter the correct path for LibreOffice (**C:\xampp\LibreOfficePortable\App\LibreOffice64\program**)
- f. Check **Enable FC Document Converter**. **Note:** Enabling this is allowed only LibreOffice is used for document preview.

The screenshot shows the 'Preview' tab in the FileCloud Server configuration interface. The navigation bar includes: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, Policies, SSO, and Cont. The sub-navigation bar includes: General, User, Password, Notifications, Share, **Preview**, Support Services, Directory Scraper, and DUO Security.

Quick JS Preview

- Enable Quick JS Preview
 - JS preview uses only browser resources to enable fast previews for all applicable user and privately shared files.

Document Preview Support

- Office Location
 - [Check Path](#)
 - Specify 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
 - Show combine PDF Option. 'Document Converter' is necessary for this functionality.
- Anonymous Access Watermark
 -
 - Enter non-empty string to watermark all public access of previews
- Authorized Access Watermark
 -
 - Enter non-empty string to watermark all authorized access of previews

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. Log into Administration Portal
2. Click on "Settings" on the left navigation panel
3. Click on "Misc" Tab
4. Click on "Preview" Tab
5. Enter the path to the LibreOffice program folder.
6. Click on "Customization" on the left navigation panel
7. Click on "General Tab
8. Check the "Show Document Preview" checkbox

Manage Settings

Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO Content Search Web Edit Team Folders **Misc**

General User Password Notifications Share **Preview** Helper Directory Scraper Anti-Virus

Document Preview Support

Office Location [Check Path](#)
Specify location of OpenOffice or LibreOffice program folder

[Reset to defaults](#)

[Save](#)
You have unsaved changes.

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
Show combine PDF Option. 'Document Converter' is necessary for this functionality.

The screenshot shows the 'Manage User UI Customizations' page in FileCloud. The left sidebar contains navigation menus for HOME, USERS/GROUPS, MANAGE, DEVICES, MISC., SETTINGS, and CUSTOMIZATION. The main content area is titled 'Manage User UI Customizations' and has several tabs: General, Labels And Logos, URL, UI Messages, Email Templates, News Feed, TOS, and Advanced. Under the 'UI Features' sub-tab, there are three sub-tabs: Login, Account Menu, and Listing. The 'Customize User UI Features' section contains a list of settings:

- Enable UI Customizations: Enable UI customization
- Show Document Preview: Show "Preview" in document file menu options (Requires "Document Preview" configured)
- Show Single File Share Full Preview: Show full screen preview for single file public shares
- Show Quick Edit Option: Show "Quick Edit" in document file menu options(Requires user to install CloudSync client)
- Show Online Edit Option: Show "Web Edit" in document file menu (Requires "Web Edit" configured)
- Disable Music Playback: Disable music player in user web portal

Enabling Watermarks On Previews

Administrators can add watermarks to all previews generated in FileCloud.

- This feature requires Document Converter
- Watermarks on previews is available in FileCloud version 17.3 and later

⚠ Password protected PDF 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.

- Enable thumbs for TIFF images
- Interface with LibreOffice for document preview generation
- Add watermarks to previews generated in FileCloud for Office docs and PDFs.

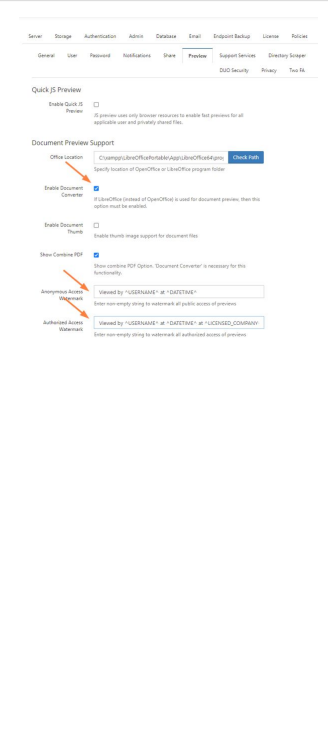
For this FileCloud uses a java program based on Apache's [PDFBox](#). Document converter also will use LibreOffice libraries to convert documents to PDF.

➔ If you have not already done so, [Install Document Converter](#).

2. Enable watermarks

NOTES:

- To disable the use of watermarks, clear the same checkbox you use to enable them
- Watermark settings are global
- Watermarks can't be enabled for a specific set of files or file types, they are applied globally
- Once watermarks are enabled, they will appear on all document previews generated in FileCloud



To display watermarks for previews:

1. Open a browser and log in to the **Admin Portal**.
2. From the left navigation pane, click **Settings**.
3. On the **Manage Settings** screen, select the **Misc.** tab
4. Select the **Preview** sub-tab.
5. Next to **Enable Document Converter**, select the checkbox.
6. Next to **Anonymous Access Watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by anonymous users.
7. Next to **Authorized Access Watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by authorized users.

Available parameters:

- ^USERNAME^ - The user who is viewing this file.
- ^SHARE_OWNER^ - The user who shared this file.
- ^FILE_OWNER^ - The file owner.
- ^OWNER^ - If this is a shared file, the user who shared this file. If this is not a shared file, the file owner.
- ^DATETIME^ - Date and time of preview.
- ^GEOIP_LOCATION^ - Geographic location of IP performing preview.
- ^LICENSED_COMPANY^ - The company listed on the current license.

Now whenever a user previews a document, they will see the watermark for anonymous or authorized access embedded in the preview.

DESCRIPTION	QUANTITY	UNIT PRICE	SUBTOTAL
	1		
		SUBTOTAL	:
		TAX	:
		TOTAL	:
TERMS:			
<ul style="list-style-type: none"> This is a computer generated invoice and does not require signature. 			
THANK YOU FOR YOUR PURCHASE.			

2 Preview doc showing watermark

Import Files : Pre-seeding

 The option to import or pre-seed user files into the system is available in FileCloud version 15 and later.

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.

Show me where the option is...

Go to **Settings > Misc > General**,

The screenshot shows the FileCloud Server Settings interface. On the left sidebar, under the 'SETTINGS' section, the 'Settings' option is highlighted with an orange arrow. The top navigation bar shows 'Misc' highlighted with an orange arrow. Below 'Misc', the 'General' tab is highlighted with an orange arrow. The 'General System Settings' section is visible, including options for Server Timezone (America/Chicago), Calendar Type (Gregorian (English)), Date Format (MMM dd, yyyy (Jan 15, 2019)), and Time Format (h:mm A (2:20 PM)).

and scroll down to the **Import** button:

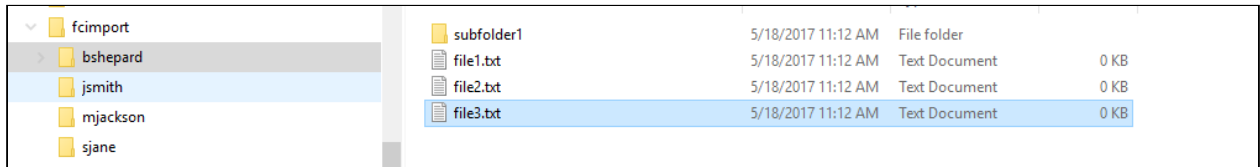
The screenshot shows the 'Import Files' section of the FileCloud Server Settings. The 'Import' button is highlighted with an orange arrow. The section includes a checkbox for 'Is hosted behind a proxy server?', a 'Run' button for 'Scheduled Tasks', and a description: 'Import files into managed storage'. Below this is an 'Allowed File Extensions' field with a placeholder text: 'Specify file extensions that will be allowed for uploading (only files of those extensions)'.

Import Files into Local Managed Storage

Prerequisite:

In order for the data to be imported, the following conditions must be met

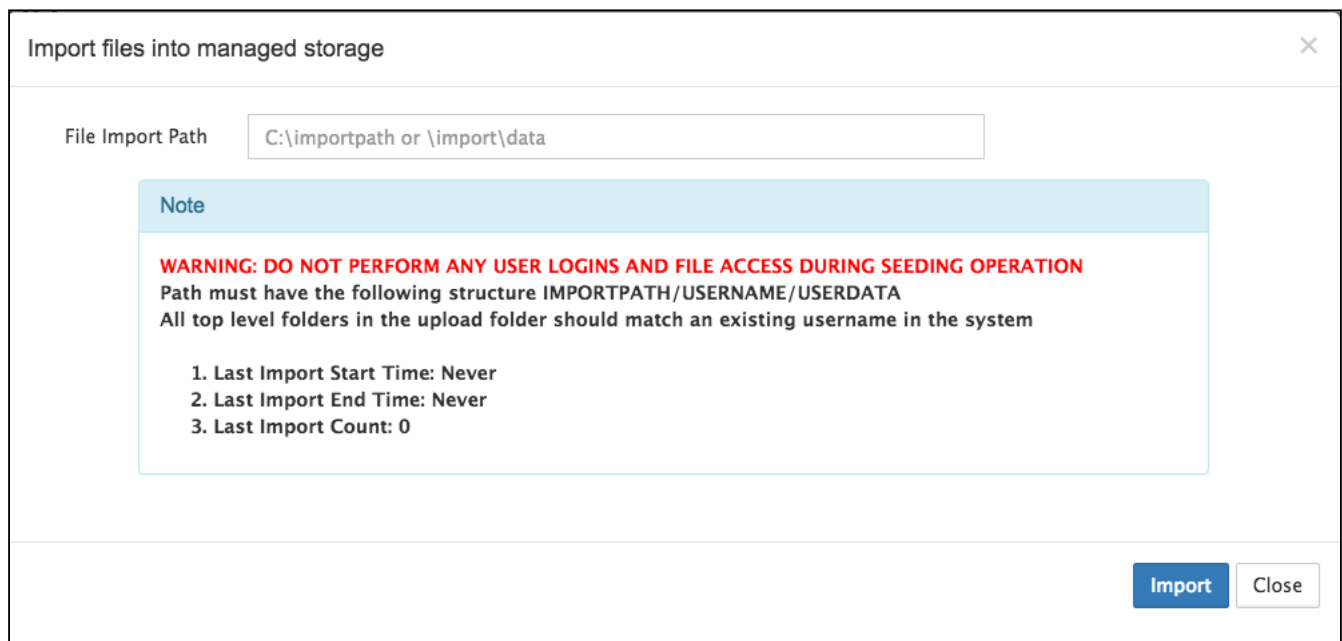
1. The data must be in locally accessible disk. Ideally, the data must reside in the same drive as the managed storage (say, Managed storage is in C:\fileclouddata, then the import data must also be in C: drive)
2. The data must be in following structure. <ImportPath><users><data>. For example, if you have four users, say, bshepard, jsmith, mjackson, sjane, then the structure should be as shown below



3. The users must already be created in the system (bshepard, jsmith, mjackson, sjane must already be a valid full user in the system)
4. The users must have enough quota assigned to allow the data import

To import files into local managed storage:

1. Open a browser and log in to the *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, click *Settings*.
3. On the *Manage Settings* window, click the *Misc.* tab, and then the *General* sub-tab.
4. On the *General* screen, next to *Import Files*, click the *Import* button.
5. On the *Import files into managed storage* dialog, in *File Import Path*, type the location to the files you want to import.
6. 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 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

Import files into managed storage
✕

Bucket

S3 Folder Name

Note

WARNING: DO NOT PERFORM ANY USER LOGINS AND FILE ACCESS DURING SEEDING OPERATION

Bucket should be accessible using the same credentials as managed storage bucket

Bucket should be in the same region as managed storage bucket

All top level folders in the upload folder should match an existing username in the system

Bucket should have the following structure TOPLEVELFOLDER/USERNAME/USERDATA

Managed storage encryption should not be enabled during import

- 1. Last Import Start Time: 2017-May-09 19:43:40
- 2. Last Import End Time: 2017-May-09 22:38:47
- 3. Last Import Count: 59764



To import files into local managed storage:

1. Open a browser and log in to the *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, click *Settings*.
3. On the *Manage Settings* window, click the *Misc.* tab, and then the *General* sub-tab.
4. On the *General* screen, next to *Import Files*, click the *Import* button.
5. On the *Import files into managed storage* dialog, in *Bucket*, type the name of the bucket that contains the files you want to import.
6. On the *Import files into managed storage* dialog, in *S3 Folder Name*, type the name of the top level folder in the Bucket that contains the files you want to import.
7. Click *Import*.

Enabling Natural Sort Order Of User List

As an administrator, you can configure the sort order which determines how user lists are displayed in the Admin portal.

- By default for users, the ASCII sort order is used because this is what is provided by the MongoDB backend.,
- The default for users can be changed to natural sort order beginning with FileCloud version 20.3 using the setting shown below.

ASCII Sort Order	Natural Sort Order
<ol style="list-style-type: none"> 1. Users sorted on numerals. 2. Users sorted on uppercase letters. 3. Users sorted on lowercase letters. 	<ol style="list-style-type: none"> 1. Users sorted on numerals. 2. Users sorted without case sensitivity.
<p> This is the default sort order when listing users in FileCloud.</p>	<p> This option uses a case-insensitive ordering of entries in the user list.</p>

To switch from ASCII to Natural sort order:

1. Prepare for Natural Sort Order

To enable natural sorting on all unprepared items:

1. 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
```

2. This command can be run multiple times if needed to make sure there are no unprepared items.

2. Enable Natural Sort Order

Once the system is fully prepared, enable natural sorting by setting the following key in the file WWWROOT\config\cloudconfig.php .

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

Natural sorting can be disabled 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
- This feature is available in FileCloud version 14.0 and later

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 a browser and log in to the [Admin Portal](#).
2. From the left navigation pane, under [SETTINGS](#) click [Settings](#).
3. On the [Manage Settings](#) screen, select the [Misc](#). tab
4. Select the [Preview](#) sub-tab.
5. Next to [Enable Document Converter](#), select the checkbox.

6. Next to **Show Combine PDF**, select the checkbox.

The screenshot shows the 'Manage Settings' page for FileCloud. The 'Preview' tab is selected. Under the 'Document Preview Support' section, the following settings are visible:

- Office Location:** C:\xampp\LibreOfficePortable\App\LibreOffice64\progr... (with a 'Check Path' button)
- Enable Document Converter:** (Note: If LibreOffice (instead of OpenOffice) is used for document preview, then this option must be enabled.)
- Enable Document Thumb:** (Note: Enable thumb image support for document files)
- Show Combine PDF:** (Note: Show combine PDF Option. 'Document Converter' is necessary for this functionality.)
- Watermark Previews:** (Empty text input field)

Now when users select multiple PDF files from the user UI, 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](#).

! 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:

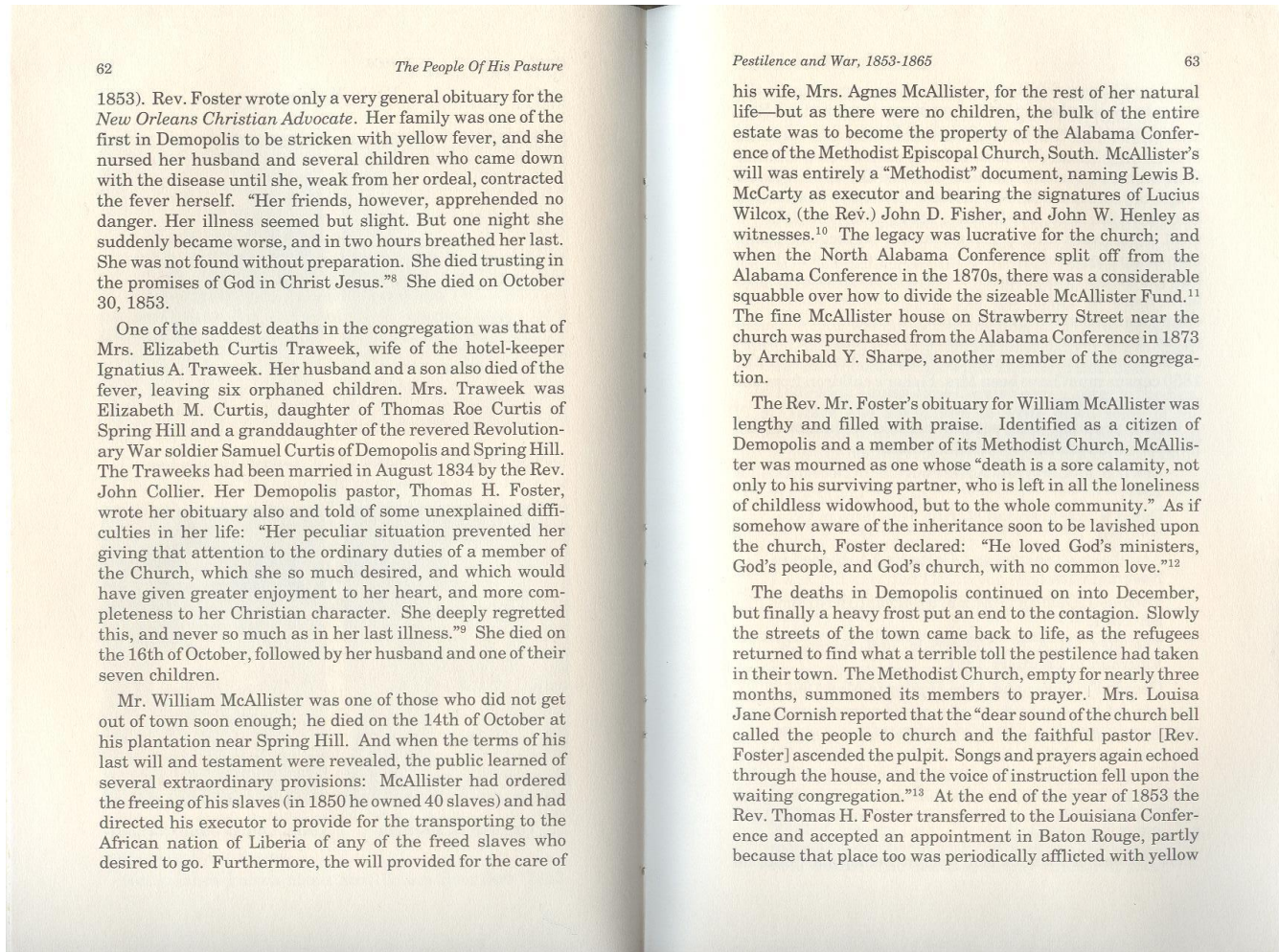
- Legal documents
- Insurance patient documents
- Blueprints and manuals

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:

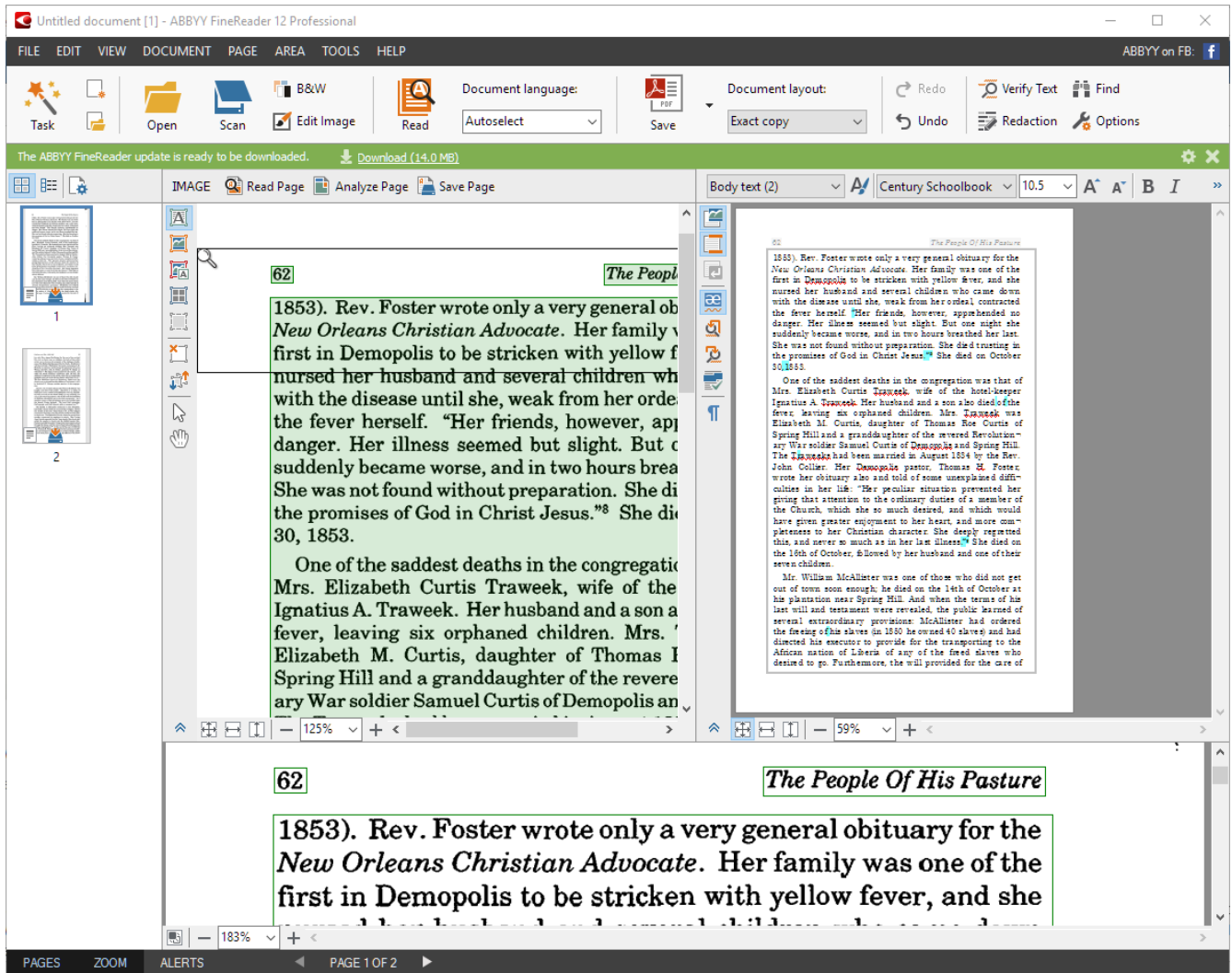


In our example:

- 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

📘 You can prevent specific file extensions from being uploaded in FileCloud 10.0 and later. Existing files cannot be renamed to use a restricted file extension in FileCloud 17.3 and later. You can create a list of only the file extensions you want to allow to be uploaded in FileCloud 19.1 and later.

⚠️ Prior to FileCloud Version 21.2, **Disallowed File Extensions** listed **php** and **php5** by default; from Version 21.2 on, it lists **php**, **php5**, **phar**, and **phtml**. If you are using a version of FileCloud earlier than 21.2, you are advised to add **phar** and **phtml** to the **Disallowed File** list. See [Advisory 2021-09 Upload of Potentially Unsafe File Types](#) for more information.

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.

- 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.

Allowed File Extensions	<input type="text"/>
	Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use ' ' as the delimiter.
Disallowed File Extensions	<input type="text" value="php php5 phar phtml"/>
	Specify file extensions that will be prevented from uploading. Use ' ' as the delimiter.

Which list should I use? The 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
<input type="text" value="png jpg "/>	Allow files to be uploaded with an extension of: <ul style="list-style-type: none"> • png • jpg • <i>empty</i> 	Only the following files can be uploaded by users: <ul style="list-style-type: none"> • Portable Network Graphics • Joint Photographic Experts Group • Any file without an extension (for example, a file named <i>config</i>)
<input type="text" value="png jpg"/>	Allow files to be uploaded with an extension of: <ul style="list-style-type: none"> • png • jpg 	Only the following files can be uploaded by users: <ul style="list-style-type: none"> • Portable Network Graphics • Joint Photographic Experts Group

FileCloud Version	Method	Instructions	Notes
19.1	Admin Portal	<p>To manage extension in the Admin Portal:</p> <ol style="list-style-type: none"> 1. Log into <i>Admin Portal</i>. 2. From the left navigation panel, select Settings. 3. On the <i>Settings</i> screen, select the <i>Misc.</i> tab, and then the <i>General</i> tab. 4. Scroll down until you see the <i>Allowed File Extensions</i> box. 5. In the <i>Allowed File Extensions</i> box, specify the allowed extensions, using the " " character to separate each extension. 	<p>⚠ If you add extensions to the Allowed File Extensions list, then any extensions in the Disallowed File Extension list will be ignored.</p> <p>⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.</p> <div data-bbox="841 558 1461 657" style="border: 1px solid black; padding: 5px;"> <p>Allowed File Extensions</p> <p>Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use ' ' as the delimiter.</p> </div> <p>This list of extensions must use the following character as the delimiter:</p> <ul style="list-style-type: none"> • ' ' • For example, to restrict the mp4 and mp3 extensions: mp4 mp3

Disallow File Extensions

FileCloud Version	Method	Instructions
Earlier than 17.3	Direct Coding	<p>To add file extension restrictions:</p> <ol style="list-style-type: none"> Open the following file <pre data-bbox="446 443 1453 531">WWWROOT\config\cloudconfig.php</pre> <ol style="list-style-type: none"> Add the following code <pre data-bbox="446 590 1453 709">define("TONIDOCLOUD_DISALLOWED_RESTRICTIONS", "php php5 phar phtml");</pre> <p>To remove all file extension restrictions:</p> <ol style="list-style-type: none"> Open the following file <pre data-bbox="446 835 1453 924">WWWROOT\config\cloudconfig.php</pre> <ol style="list-style-type: none"> Edit the code to match this: <pre data-bbox="446 982 1453 1071">define("TONIDOCLOUD_DISALLOWED_RESTRICTIONS", "");</pre> <p>Note: This list of extensions must use the following character as the delimiter:</p> <ul style="list-style-type: none"> ' ' For example, to restrict php extensions: php php5 phar phtml

FileCloud Version	Method	Instructions
17.3 and later	Admin Portal Direct Coding	<p>To manage extensions in the Admin Portal:</p> <ol style="list-style-type: none"> 1. Log into Admin Portal. 2. From the left navigation panel, select Settings. 3. On the Settings screen, select the Misc. tab, and then the General tab. 4. Scroll down until you see the Disallowed File Extensions box. 5. In the Disallowed File Extensions box, add the additional restricted extensions. <p>Notes:</p> <p>⚠ If you add extensions to the Allowed File Extensions list, then any extensions in the Disallowed File Extension list will be ignored.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Disallowed File Extensions</p> <div style="border: 1px solid gray; padding: 5px; display: inline-block;">php php5 phar phtml</div> <p>Specify file extensions that will be prevented from uploading. Use ' ' as the delimiter.</p> </div> <p>This list of extensions must use the following character as the delimiter:</p> <ul style="list-style-type: none"> • ' ' • For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions: php php5 phar phtml mp3 mp4

Restricting File Extensions

- ⚠ Prior to FileCloud Version 21.2, **Disallowed File Extensions** listed **php** and **php5** by default; from Version 21.2 on, it lists **php**, **php5**, **phar**, and **phtml**. If you are using a version of FileCloud earlier than 21.2, you are advised to add **phar** and **phtml** to the **Disallowed File** list. See [Advisory 2021-09 Upload of Potentially Unsafe File Types](#) for more information.

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. Log into Admin Portal.
2. From the left navigation panel, select **Settings**.
3. **On the Settings screen, select the Misc. tab, and then the General tab.**
4. Scroll down until you see the **Disallowed File Extensions** box.
5. In the **Disallowed File Extensions** box, specify the restricted extensions.


Disallowed File Extensions

Specify file extensions that will be prevented from uploading. Use '|' as the delimiter.

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

 You can create a list of file names that cannot be uploaded by users in FileCloud 19.1 and later.

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.

To restrict names of files that can be uploaded:


1. In the admin portal, go to **Settings > Misc > General**.
2. Add the file names to the **Disallowed File Names** field.
Separate multiple names with |.


Disallowed File Names



Specify file names that will be prevented from uploading. Use '|' as the delimiter.

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 will be blocked from being uploaded.
 - In the Sync client, it will ignore checking for restricted names.

 If you add an extension to the file name, then only the combination of name + extension will be restricted.

  To manage file extensions ONLY, you can either create a list of file extensions to restrict, or create a list of file extensions to allow. See [Manage File Extensions](#) for instructions.

Example	Description	Impact on Uploading Files
<div style="border: 1px solid gray; padding: 5px; width: fit-content;"> attack threat.exe </div>	Restrict any file from being uploaded if it contains any of the 3 strings in the file name: <ul style="list-style-type: none"> • attack • threat.exe • <i>empty</i> 	The following files cannot be uploaded by users: <ul style="list-style-type: none"> • *attack*.* • *threat.exe • Any file The following files can be uploaded by users: <ul style="list-style-type: none"> • No files can be uploaded until the <i>empty delimiter</i> is removed.
<div style="border: 1px solid gray; padding: 5px; width: fit-content;"> attack threat.exe </div>	Restrict any file from being uploaded if it contains any of the 2 strings in the file name: <ul style="list-style-type: none"> • attack • threat.exe 	The following files cannot be uploaded by users: <ul style="list-style-type: none"> • *attack*.* • *threat.exe The following files can be uploaded by users: <ul style="list-style-type: none"> • Any file not containing <i>attack</i> • Any file not containing <i>threat.exe</i> • <i>threat.*</i> (where * is NOT .exe)

Manage File Versioning

You can allow a user to upload 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 file?

 Look for the Versions icon 

Manage files for me ✕

/me ☰ ☆ 🗑️

← Up
🗑️ Deleted Files
📄 Copy
↶ Move
Delete

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

💡 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, you can use the following values:

Option	Setting	Result
<i>Number of old versions to keep for each file</i>	-1	The user tries to upload another version but the upload will FAIL
<i>Number of old versions to keep for each file</i>	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. Open a browser and log on to the *Admin Portal*.
2. From the left navigation menu, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, select the *Storage* tab, and then the *My Files* sub-tab.
4. On the *My Files* sub-tab, 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.
5. To save your changes, click *Save*.

Configuring Zip Files and Zero Trust File Sharing

- i** 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.

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 enable the zip file feature

By default, the zip file feature described above is disabled. To make it available to users, enable 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", false);
```

3. Change the value of `TONIDOCLOUD_ZIP_FOLDER_ENABLE` from **false** to **true**:

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

The zip feature is now enabled for users. To disable it, change the value for `TONIDOCLOUD_ZIP_FOLDER_ENABLE` back to **false**.

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
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:

1. Open cloudconfig.php at
 - Windows: XAMPP DIRECTORY\htdocs\config\cloudconfig.php
 - Linux: /var/www/config/cloudconfig.php
2. Use the following steps to change any of the settings:

To change the encryption method:

- a. Locate the setting:

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

- b. Change the value to one of the following:

Value	Definition
0	PKWARE
1 (default)	WinZip AES-256 <i>Note: WinZip AES256 encryption works in Windows only with 7-Zip, winRAR, and WinZip third party compression software. Use PKWARE as an alternative.</i>
2	WinZip AES-128
3	WinZip AES-192

To change the compression level:

- a. Locate the setting.

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

- b. 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:

- a. Locate the setting.

```
define("TONIDOCLOUD_ZIP_FOLDER_COMPRESSION_METHOD", 8);
```

- b. Change the value to one of the following:

Value	Definition
0	Stored
8 (default)	Deflated

To change the fallback character set:

- a. Locate the setting.

```
define("TONIDOCLOUD_ZIP_FOLDER_CHARSET_FALLBACK", null);
```

- b. Change the value to one of the following:

Value	Definition
GREEK	cp737
BALT_RIM	cp775

Value	Definition
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:

- a. Locate the setting:

```
define("TONIDOCLOUD_ZIP_FOLDER_MAX_FILE_SIZE", "100");
```

The value is given in MB.

- b. 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 admin portal, go to **Settings > Policies**, and open the policy you want to change.

- Click the **User Policy** tab:

Policy Settings - Global Default Policy

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

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

User Policy

Disable Invitations to New Users
NO

Do not allow user to send invitations to new users when shares are created.

Create account on new user shares
YES

Create accounts automatically when share invitations are sent to new users.

Enable code based device authentication

Save Reset Close

- Scroll down to the bottom of the tab.
By default **Save Zip File Session Password** is set to **Yes**. This enables users to enter the password once per log-in session to access the contents of the zip file.
- Change the value of **Save Zip File Session Password** to **No**.

Policy Settings - Global Default Policy

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

NO

Enables/disables mandatory workflow automation for shares

Max. File Size Limit ⓘ

Units 0 MB

Specify maximum storage quota for file upload. 0 implies Unlimited quota. Warning: Renaming and editing files might fail if the limit is exceeded.

Save Zip File Session Password
NO

Allow passwords to be saved inside encrypted zip files. Warning: Disabling the setting will require a password every time you access a file.

Save Reset Close

- Click **Save**.
Now 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.