FileCloud Server Version 23.252

Storage, High Availability, and Multitenancy

Printed on 10/08/2025

Copyright Notice

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

Storage Settings

FileCloud can access and manage content that is stored locally in your system and content stored remotely in locations available in your network.

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

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

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

FileCloud Managed Storage

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

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

Can I also configure network storage?

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

Setting Up Network Folders

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

Setting up Managed Storage

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

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

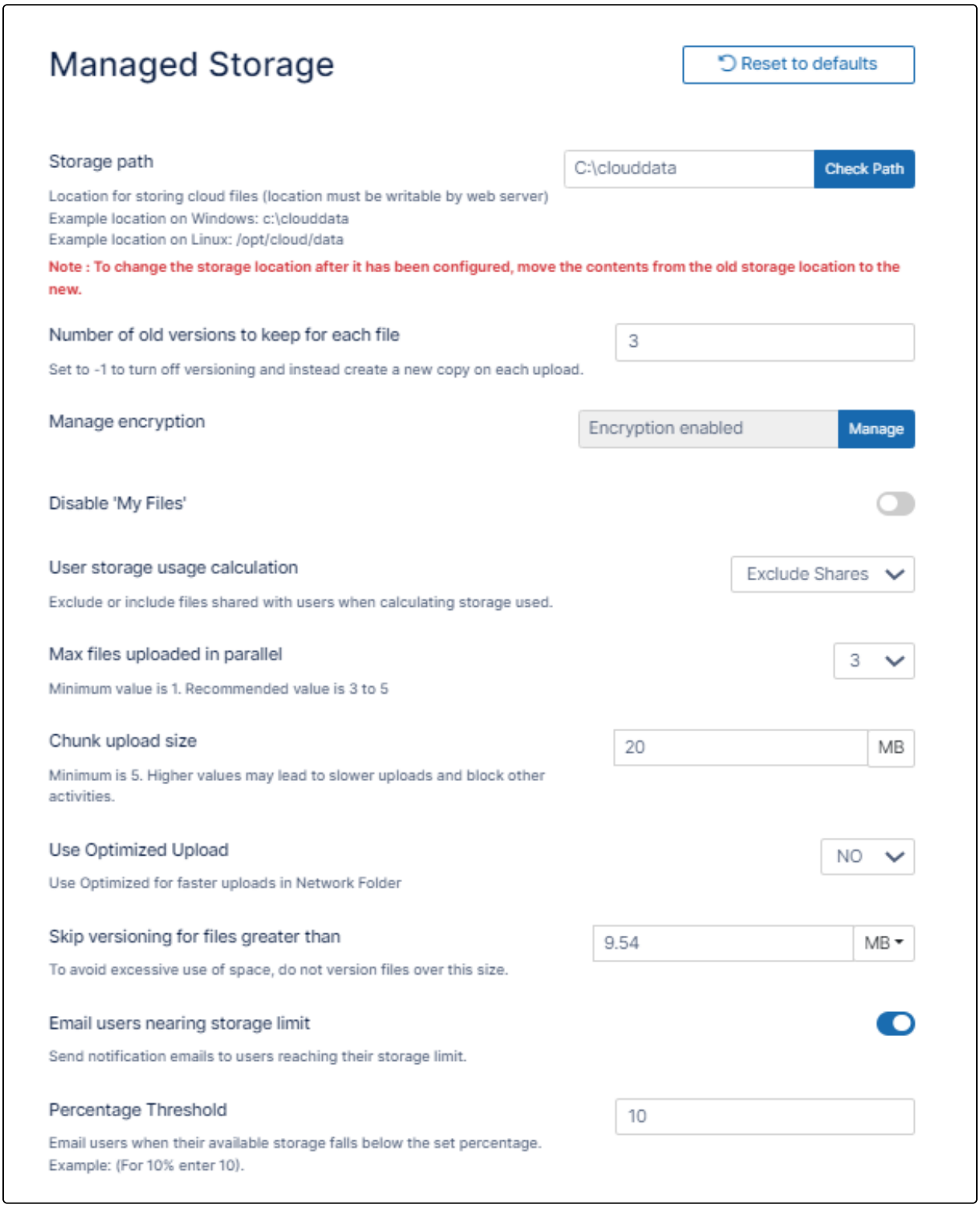
- Managed Storage provides FileCloud complete control over the management of user content.
- The storage can be on filesystems on a local hard disk, SAN, or NAS disks.

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

To set up Managed Storage:

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

2. Type the information into the fields as described below.



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.
User storage usage calculation	When the user storage usage is reported, the shares used by the user can also be counted towards the quota. This can be changed by selecting the appropriate drop-down option.
Max files uploaded in parallel	Number of files that can be uploaded at the same time when multiple files are uploaded. Default is 3. The recommended number is 3 to 5. Higher values may slow down the upload process and lower system efficiency.
Chunk upload size	The maximum size in MB for chunks uploaded. Default is 20. If size is set too high, the upload process may slow down and other operations may be blocked.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Use Optimized Upload</td><td>
Optimized upload is available in FileCloud 23.241, and uses a faster method for uploading. Choose YES to use optimized upload for S3 Network Folders only. If you don't use Network Folders or your Network Folders do not use S3 storage, this setting does not have any effect.

If you choose YES, additional fields appear:


Use the following information to determine the values you want to give these fields:
<table>
<tr><td>Max chunks uploaded in parallel</td><td>The number of file chunks that can be sent simultaneously to the server. Choose the highest number of chunks you can send without having a detrimental effect on efficiency. The default value is 10, and the minimum value is 1. Mid-range values are 4 - 20. Values above 20 may decrease efficiency by blocking other activities and slowing down uploads.</td></tr>
<tr><td>Number of minutes pre-signed URL is valid (minutes)</td><td>How long the pre-signed URL can be used. Choose a value that is high enough to enable uploads on large files, and low enough to close the url in a timely manner so it is not a security risk. The recommended value is 30 to 60.</td></tr>
<tr><td>Use Accelerated Endpoint</td><td>If you have the accelerated feature in the S3 bucket enabled, set to YES to use the feature to complete downloads and uploads more quickly.</td></tr>
</table>

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

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

Setting	Description
Skip versioning for files greater than	Any file larger than the specified value will not be versioned.
Email users nearing storage limit	If this option is enabled then automatic emails with notifications will be sent to users reaching their storage limit.
Percentage Threshold	Defines at what point the percentage of unused managed storage space is considered low. For example, if the value is set to 20, then storage is considered low if more than 80% of managed storage space is used. When unused storage is less than this value, an automatic email notification is sent to the admin. If the above option, **Email Users Nearing Storage Limit** is enabled, an automatic email notification is also sent to the user if their available storage falls below the set percentage.

3. Click **Save**.
4. Click the **Policies** tab.
5. For each policy that you want to change the default storage settings in:
    1. Click the edit button.
    2. Remain on the **General** tab.
    3. Type the information into the fields as described below:
    4. Click **Save**.
    5. 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. *For example, if a user has 2 GB quota and if this setting is changed to 10 GB, it only affects newly created users after this point. To update the quota for an existing user, use the user details panel in Users section.*
Store deleted files in the recycle bin	Enable this setting if you wish to provide a way to keep deleted files in a Recycle Bin. When this option is enabled and a user deletes a file/folder, the deleted item gets moved into their personal deleted files area. Then the user can restore files from their recycle bin or empty the recycle bin completely. **Note: Files in the recycle bin count towards a user's storage quota.**

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

Warning

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

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

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

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

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

Setting up FileCloud Managed S3 Storage

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

As an administrator, you can 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

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

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

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. (Optional) Configure System to Use Optimized Upload

When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud 23.241 includes an Optimized Upload feature which can be enabled in your system by following the instructions below to configure a CORS policy with the required settings, and to confirm that your service address is in the .**htaccess** file.

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

Required CORS policy for Optimized Upload

To use the Optimized Upload feature, configure a CORS policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings.
For more information about CORS, see:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/enabling-cors-examples.html
https://docs.aws.amazon.com/AmazonS3/latest/userguide/ManageCorsUsing.html

To configure the CORS policy:

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

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
```

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

5. Click **Save**.

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

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

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

3. Restart the FileCloud server.

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

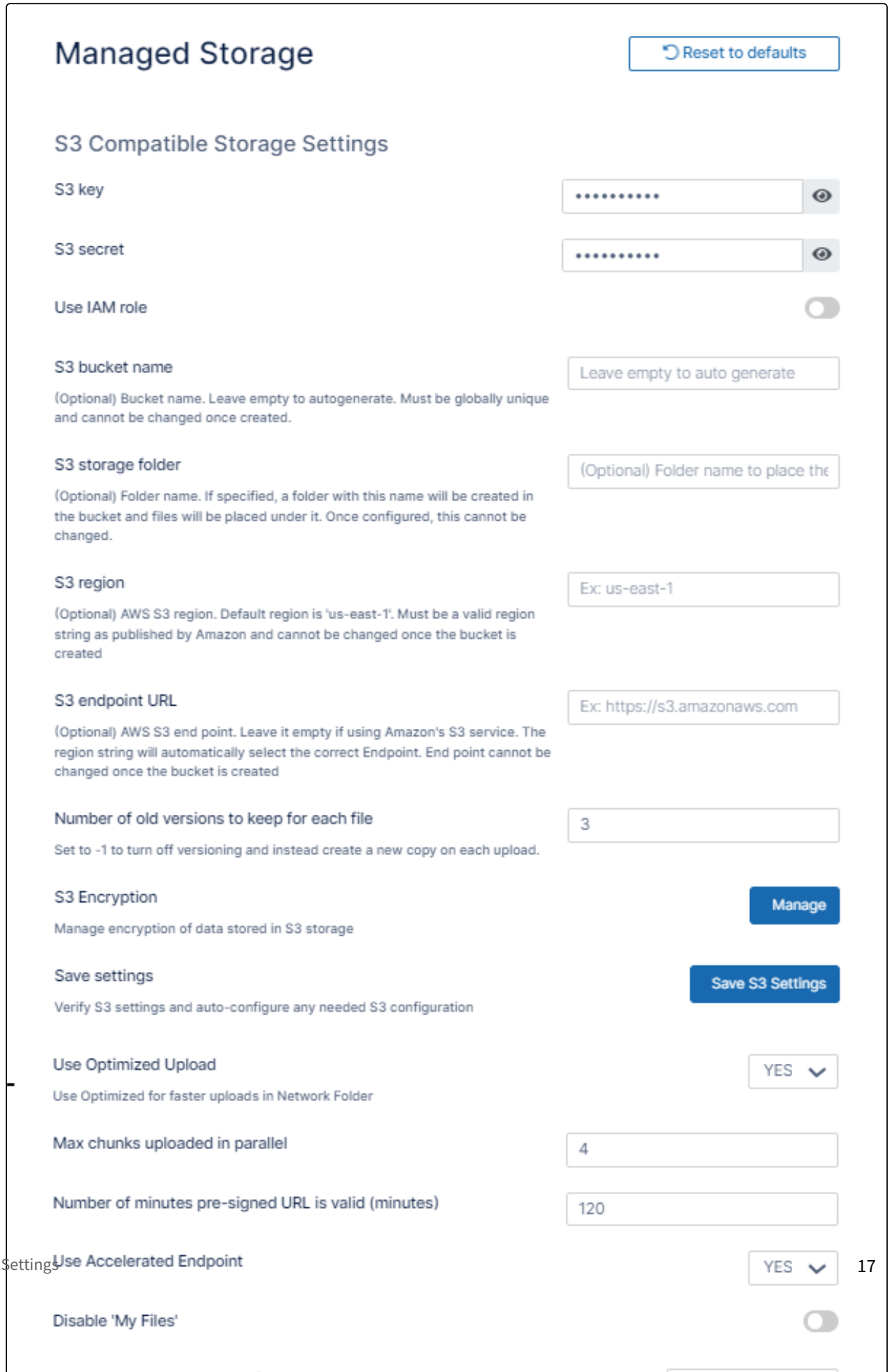
3. Configure Credentials and Settings

Now configure your S3 credentials and storage settings.

To configure S3 storage credentials and settings:

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

5. Click **Save.**


Managed Storage
Reset to defaults
S3 Compatible Storage Settings
S3 key
S3 secret
Use IAM role
S3 bucket name
(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.
Leave empty to auto generate
S3 storage folder
(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.
(Optional) Folder name to place the
S3 region
(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created
Ex: us-east-1
S3 endpoint URL
(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be changed once the bucket is created
Ex: https://s3.amazonaws.com
Number of old versions to keep for each file
Set to -1 to turn off versioning and instead create a new copy on each upload.
3
S3 Encryption
Manage encryption of data stored in S3 storage
Manage
Save settings
Verify S3 settings and auto-configure any needed S3 configuration
Save S3 Settings
Use Optimized Upload
Use Optimized for faster uploads in Network Folder
YES
Max chunks uploaded in parallel
4
Number of minutes pre-signed URL is valid (minutes)
120
Use Accelerated Endpoint
YES
Disable 'My Files'

Field	Description	FileCloud Version
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 .	
Use IAM role	Either check **Use IAM role** or type in authentication credentials in **S3 Key** and **S3 Secret**. **Note**: To use an IAM role, you must attach it to your E2 instance. See the page Attach an IAM role to an instance in the AWS documentation for instructions.	
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. • 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. • If your bucket is in a different region, (Europe, Asia) provide the correct region string. The strings should match the region string published by amazon. • **Note: For govcloud installs, you must use region string: us-gov-west-1**	
S3 endpoint URL	Optional: This is the S3 endpoint. • Use this to specify your own S3 endpoint (typically S3 compatible storage) • Use this if it is a unpublished region. To use an AWS end point, it must be one of the values published AWS S3 endpoints	
Number of old versions to keep for each file	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines 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.	

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

Field	Description	FileCloud Version
Max files uploaded in parallel	Number of files that can be uploaded at the same time when multiple files are uploaded. Default is 3. The recommended number is 3 to 5. Higher values may slow down the upload process and lower system efficiency.	23.241
Chunk upload size	The maximum size in MB for chunks uploaded. Default is 40. If size is set too high, the upload process may be slow down and other operations may be blocked.	23.241
Skip versioning for files greater than	Any file larger than the specified value will not be versioned.	
Email users nearing storage limit	If this option is enabled then automatic emails with notifications are sent to users reaching their storage limit.	
Percentage Threshold	Defines at what point the percentage of unused managed storage space is considered low. For example, if the value is set to 20, then storage is considered low if more than 80% of managed storage space is used. When unused storage is less than this value, an automatic email notification is sent to the admin. If the above option, **Email Users Nearing Storage Limit** is enabled, an automatic email notification is also sent to the user if their available storage falls below the set percentage.	

4. Enable Encryption

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

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

FileCloud supports the following server side encryption types:

Encryption Type	Notes
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)	All data is encrypted at rest using AES256 bit encryption. The data can only be accessed using the supplied key/secret credentials. The data will be accessible via S3 Console (which should NOT done for FileCloud Managed storage data)

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

WARNINGS:

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

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

To enable S3 encryption:

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

If you are running FielCloud Server on Windows

AND

Your xampp folder is installed in a location other than c:\xampp

You must add a key to the cloudconfig.php file

- For example, if your xampp folder is in D:\xampp\htdocs\config\cloudconfig.php
- Then you would add the following line: define("PHPBIN_PATH","D:\\xampp\\php\\php.exe");

1. On the FileCloud Server, open the following file for editing:

```
<your xampp folder>\htdocs\config\cloudconfig.php
```

2. Add the following line anywhere:
Replacing *<location>* with your path to the xampp folder

```
define("PHPBIN_PATH","<location>:\\xampp\\php\\php.exe");
```

3. Save your changes and close the file.

Then go to Enabling S3 Storage Encryption

Upload large files on an Amazon S3 storage server

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

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

To set a custom chunk size:

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

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

Troubleshoot

Using Override Configuration Keys

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

KEY	VALUE	Description
TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER	"/somepath/location"	In HA installs, temp folder must be a commonly accessible location. This key must be set in each of the HA nodes

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:

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

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

How to Correct Issues with Text Editors

If you encounter issues where documents stored in AmazonS3 share object storage cannot be edited using a text editor, you can use a workaround to correct this.

Workaround:

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

Change the Content-Security-Policy

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

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

To change the Header set in CSP:

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

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

Add a CORS Policy

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

To allow the use of a text editor:

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

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

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

5. Click Save.

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

Add a CORS Policy

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

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

To allow the use of a text editor:

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

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

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

5. Click Save.

Setting up S3 Compatible Services

FileCloud officially supports only Amazon S3 storage.

- Other Amazon S3 compatible storage systems are supported through our Amazon S3 drivers, including:
  - Alibaba Cloud object-based storage
  - Digital Ocean S3 object storage
  - Scality
  - Wasabi
  - Google Cloud object storage
  - Backblaze B2
  - Cloudian S3-Compatible Object Storage
  - Oracle Cloud Infrastructure
  - Storj
- The 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.

Integrate with any of the available S3 compatible storage services:

- How to Integrate FileCloud with Alibaba Cloud Object Based Storage
- How to Integrate Filecloud with Backblaze (B2) Cloud Storage
- How to Integrate FileCloud with Digital Ocean Spaces
- How to Integrate FileCloud with Google Cloud Object Based Storage
- How to integrate FileCloud with Scality Storage
- How to Integrate FileCloud with Wasabi Object Based Storage
- How to Integrate Filecloud with Cloudian S3-Compatible Object Storage
- How to Integrate FileCloud with Oracle Cloud Infrastructure
- How to Integrate Filecloud with Storj

How to Integrate FileCloud with Alibaba Cloud Object Based Storage

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

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

WARNINGS:

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

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

1. Enable Alibaba cloud object storage

NOTES:

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

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

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

To enable Alibaba cloud object storage as the backend:

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

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

3. Find the following line:

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

4. Change it to this line:

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

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

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

7. Rename it to:

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

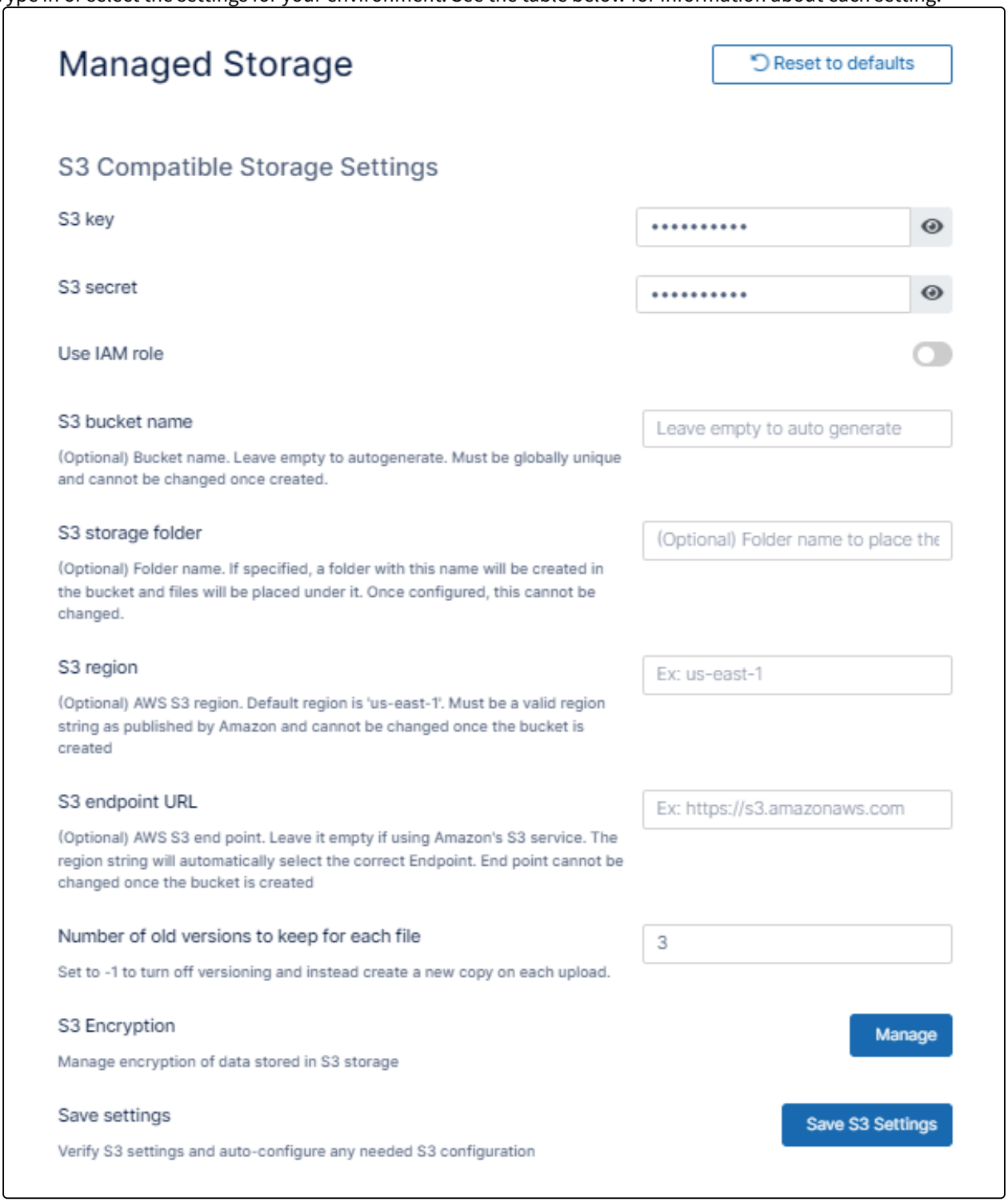
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Alibaba cloud-based object storage:

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

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



3. Click **Save S3 Settings**.

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

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

Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

How to Integrate Filecloud with Backblaze (B2) Cloud Storage

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

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

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

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

1. Enable B2 object storage

NOTES:

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

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

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

To enable B2 object storage as the backend:

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

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

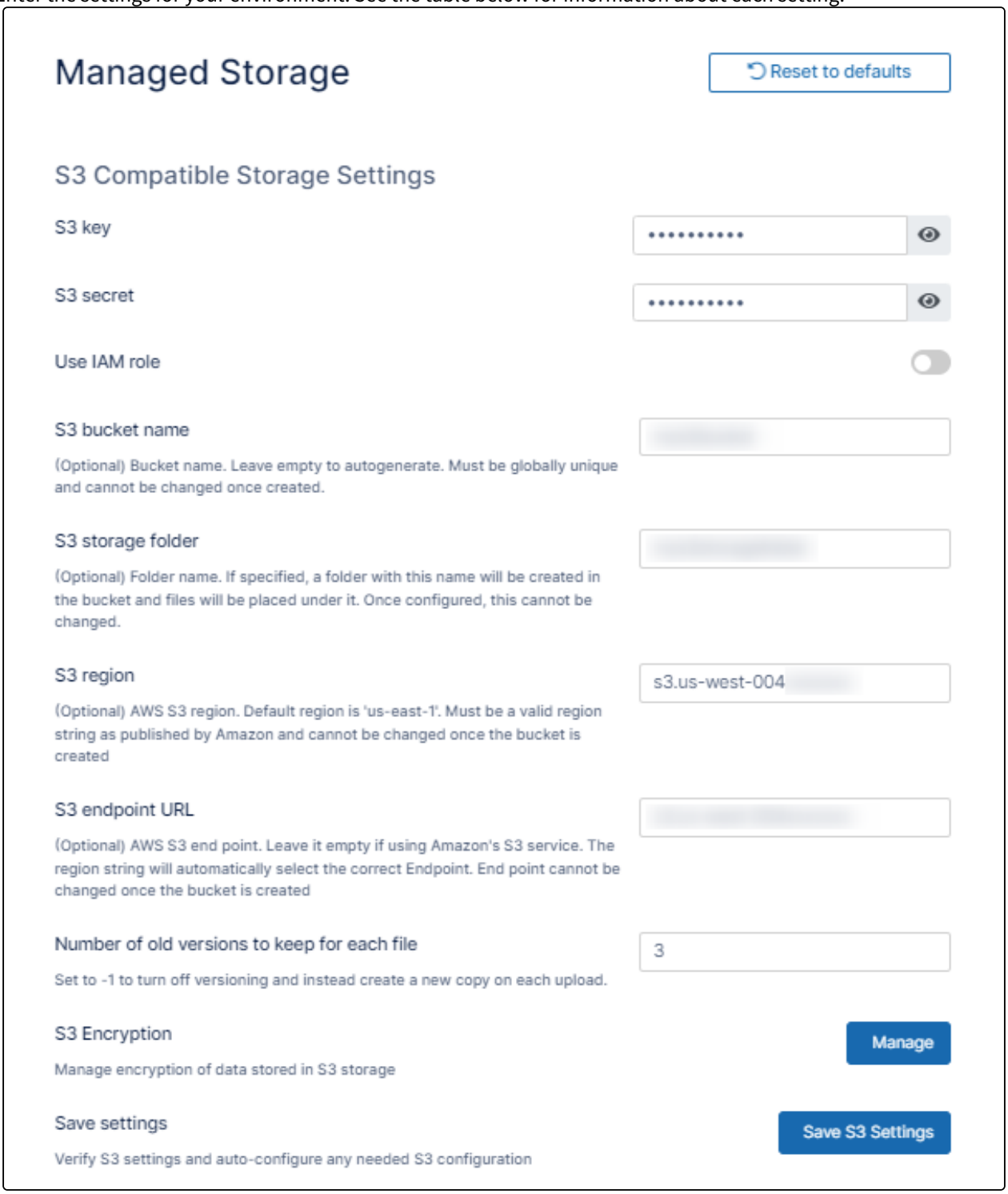
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Backblaze (B2) Credentials

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

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



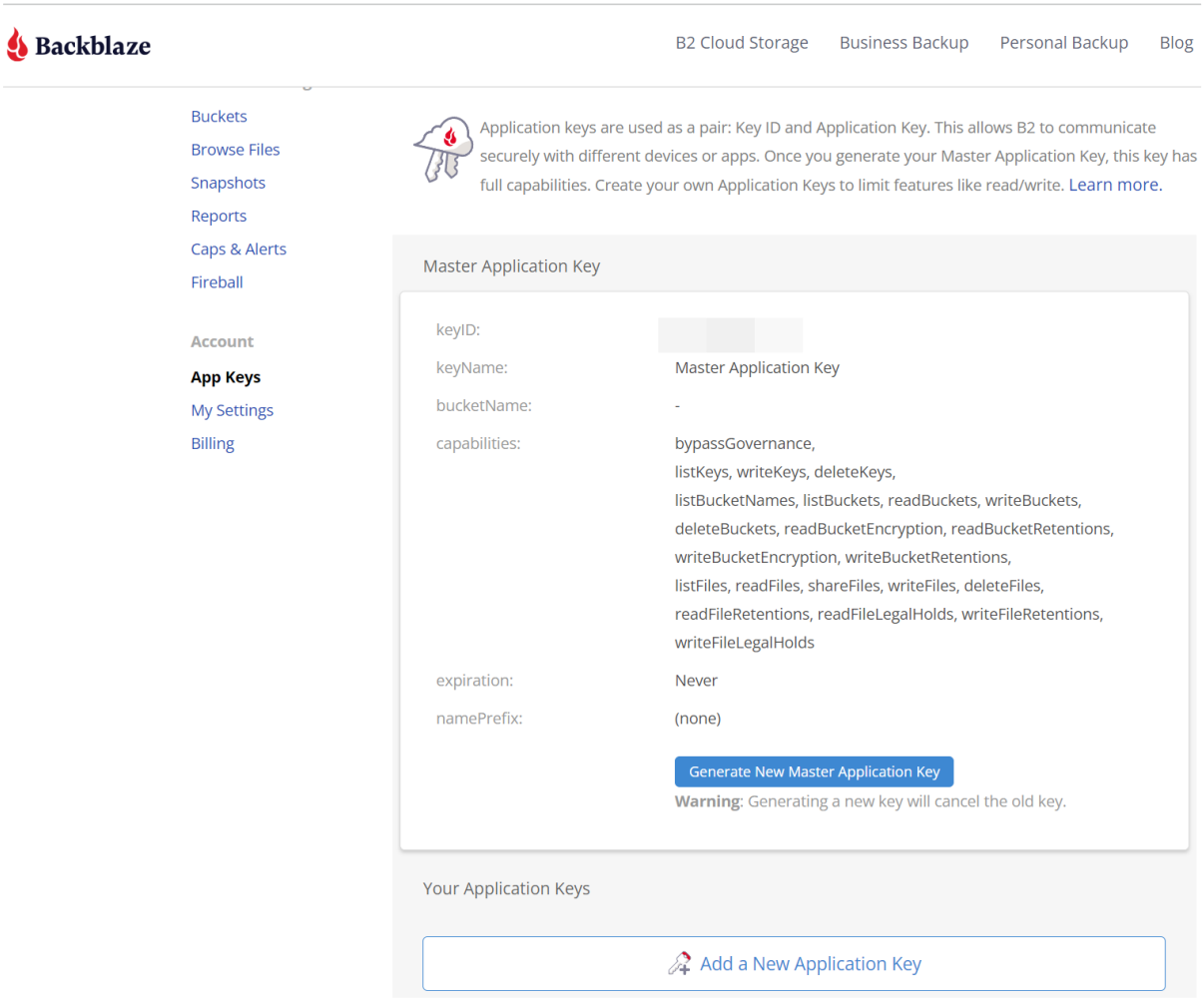
3. Click **Save S3 Settings**.
4. Enter values for **Number of old versions to keep for each file**, and, if you are using encryption, click **Manage** for **S3 Encryption** to set the encryption type.
5. Click **Save**.

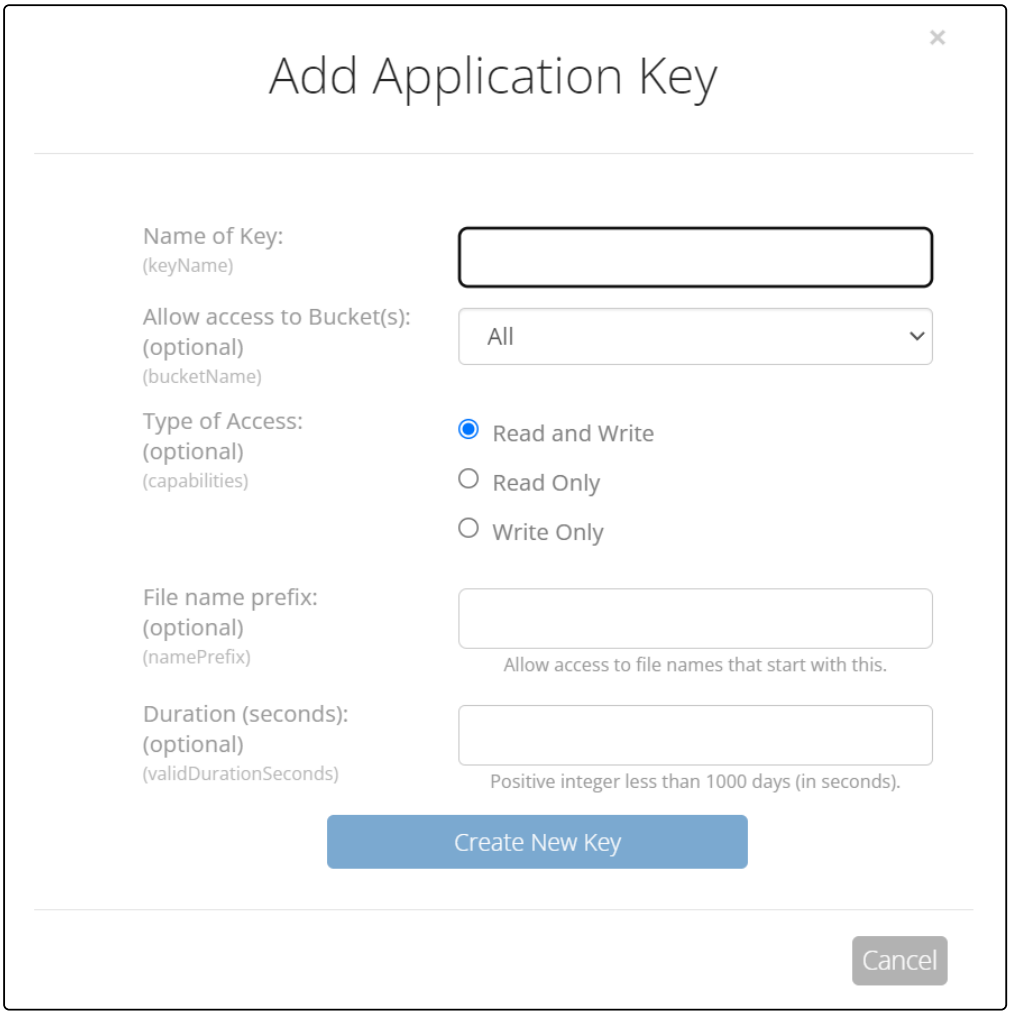
Field	Description
S3 Key	Your B2 authentication key.
S3 Secret	Your B2 authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem, The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string. 
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL.
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, 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.

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

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

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


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



Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

How to Integrate FileCloud with Digital Ocean Spaces

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

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

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

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

1. Enable Digital Ocean S3 object storage

Notes:

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

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

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

To enable Digital Ocean s3 storage as the backend:

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

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

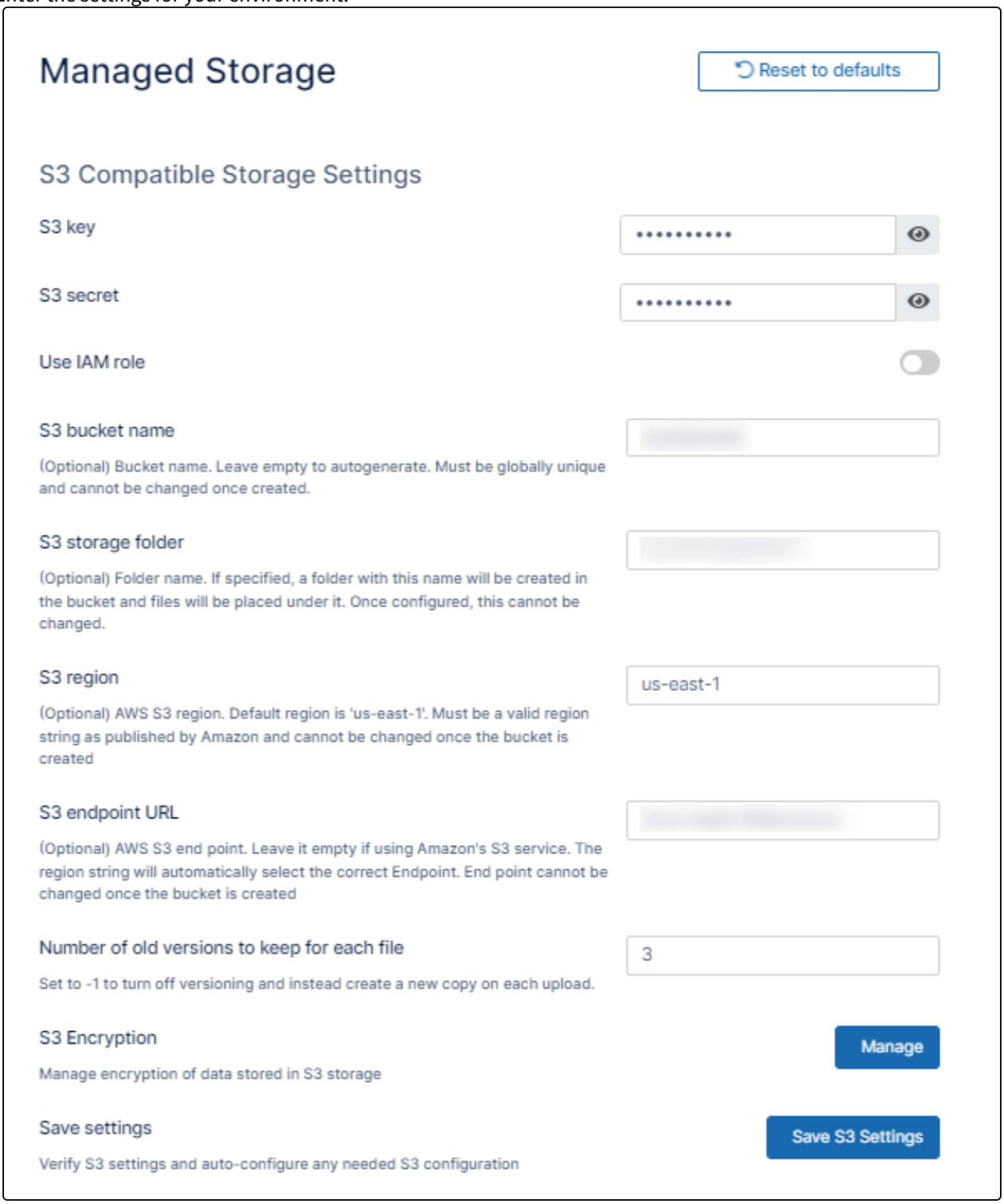
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Digital Ocean S3 Credentials

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

2. Enter the settings for your environment.



3. Click **Save S3 Settings**.

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

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

Troubleshooting:

How to correct issues with image previews

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

To add a line to the .htaccess file:

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

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

How to correct Issues with mp4 videos

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

To add a line to the .htaccess file:

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

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

How to Integrate FileCloud with Google Cloud Object Based Storage

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

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

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

1. Enable GCP object storage

NOTES:

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

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

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

To enable GCP object storage as the backend:

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

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

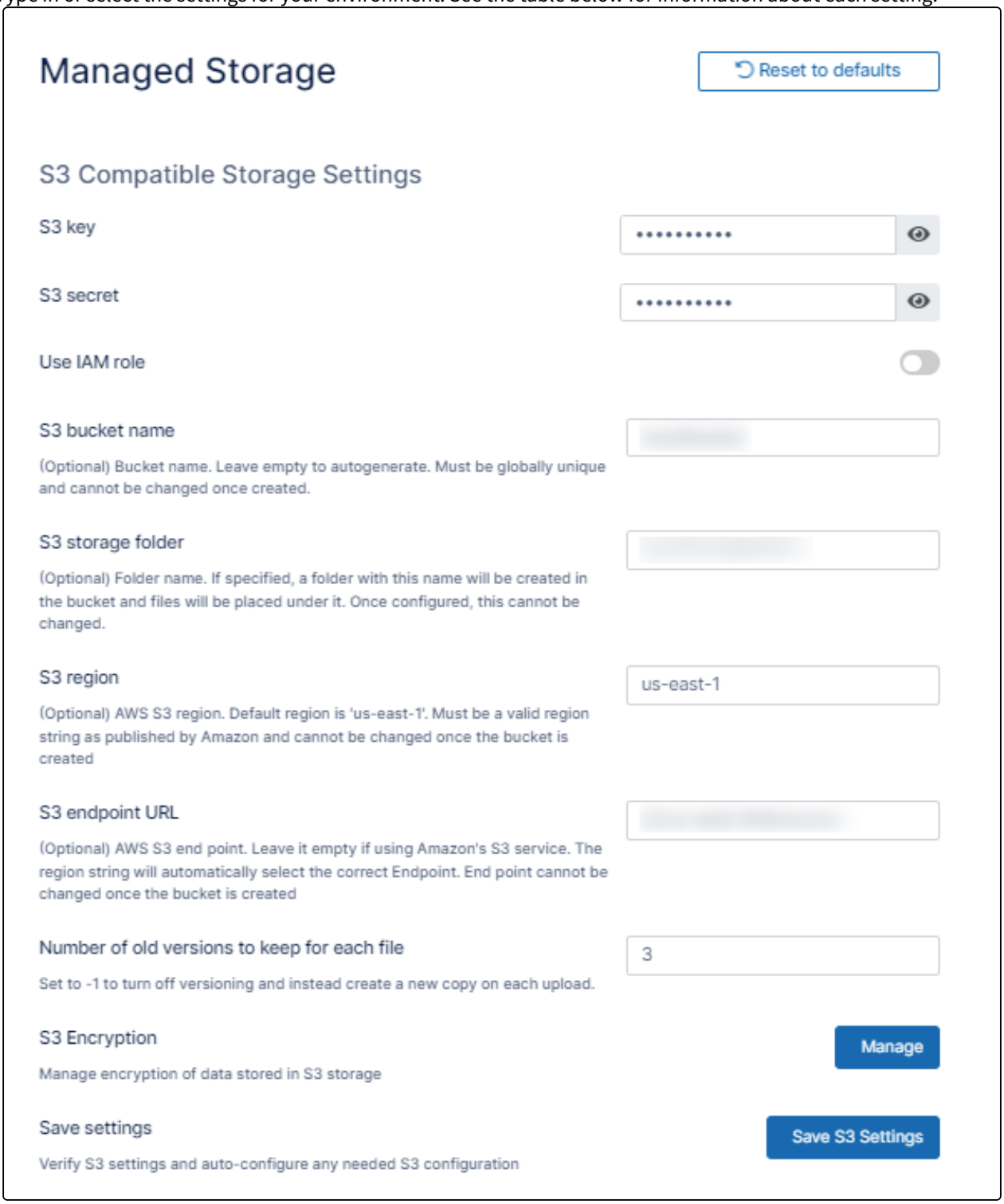
💡 Nothing needs to be added or edited in **amazons3storageconfig.php**

2. Configure Credentials

To configure Digital Ocean S3 Credentials

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

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

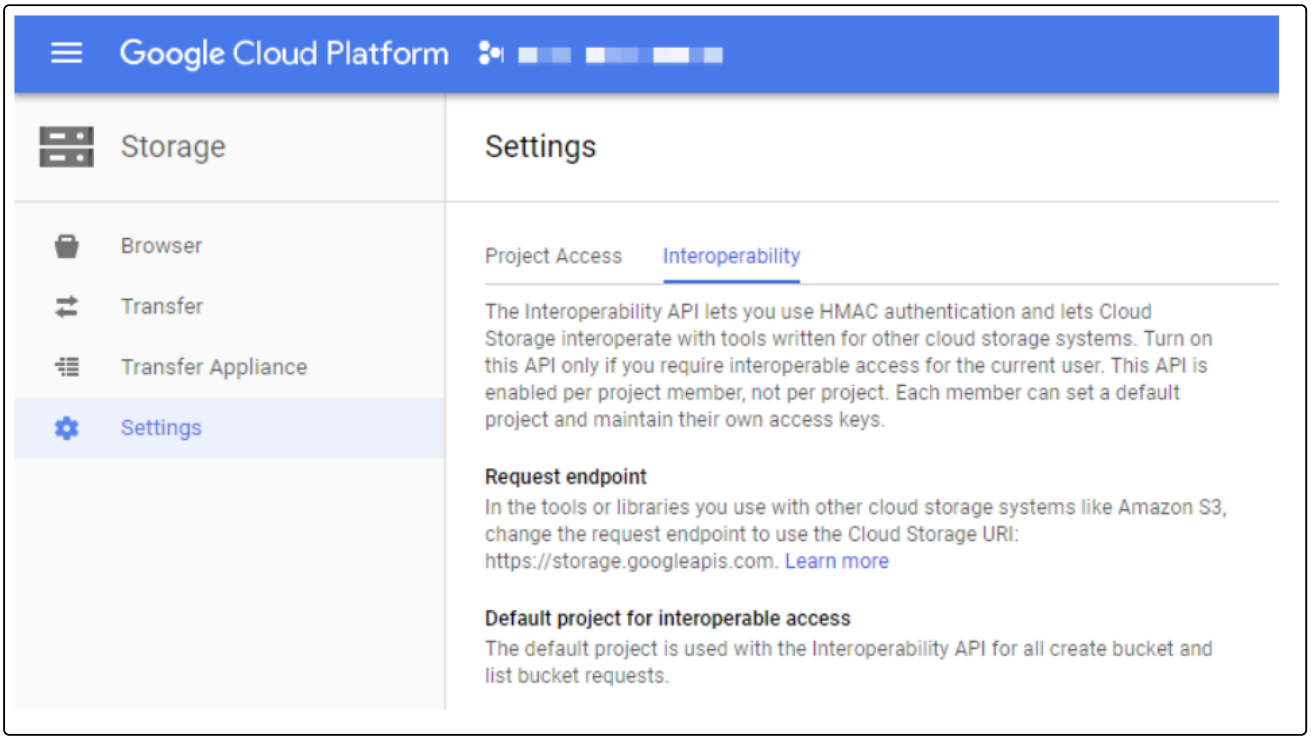


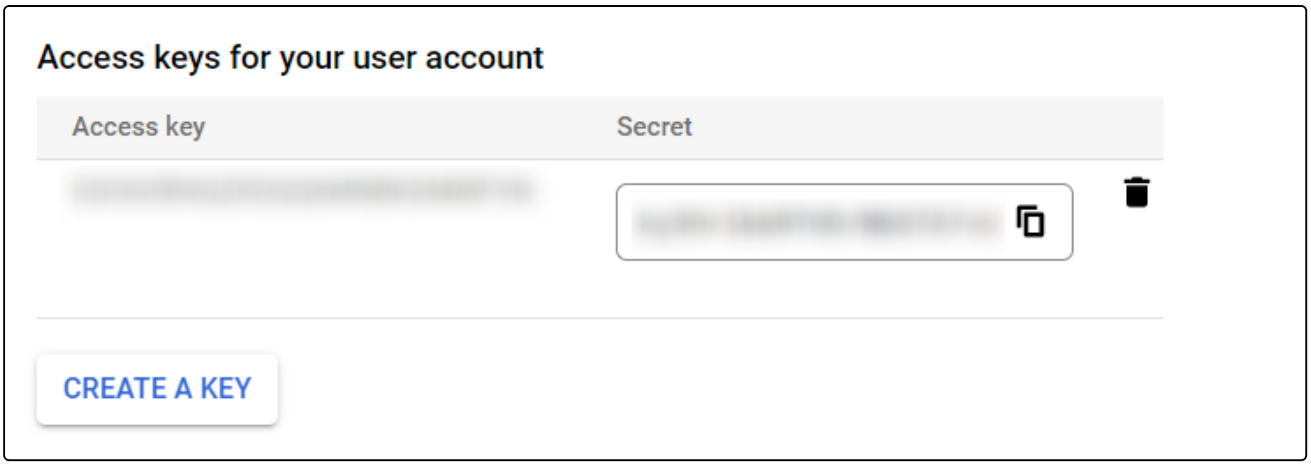
3. Click **Save S3 Settings**.
4. Enter values for **Number of old versions to keep for each file**, and, if you are using encryption, click **Manage** for **S3 Encryption** to set the encryption type.
5. Click **Save**.

Field	Description
S3 Key	Your GCP HMAC authentication key.
S3 Secret	Your GCP HMAC authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem, The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string. Generally use: **auto**
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL. Generally, it is: https://storage.googleapis.com
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, 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.

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

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





Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

How to integrate FileCloud with Scality Storage

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

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

WARNINGS:

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

To change the FileCloud storage path from LOCAL to SCALITY:

1. Enable Scality object storage

NOTES:

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

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

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

To enable Scality storage as the backend:

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

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

3. Find the following line:

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

4. Change it to this line:

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

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

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

7. Rename it to:

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

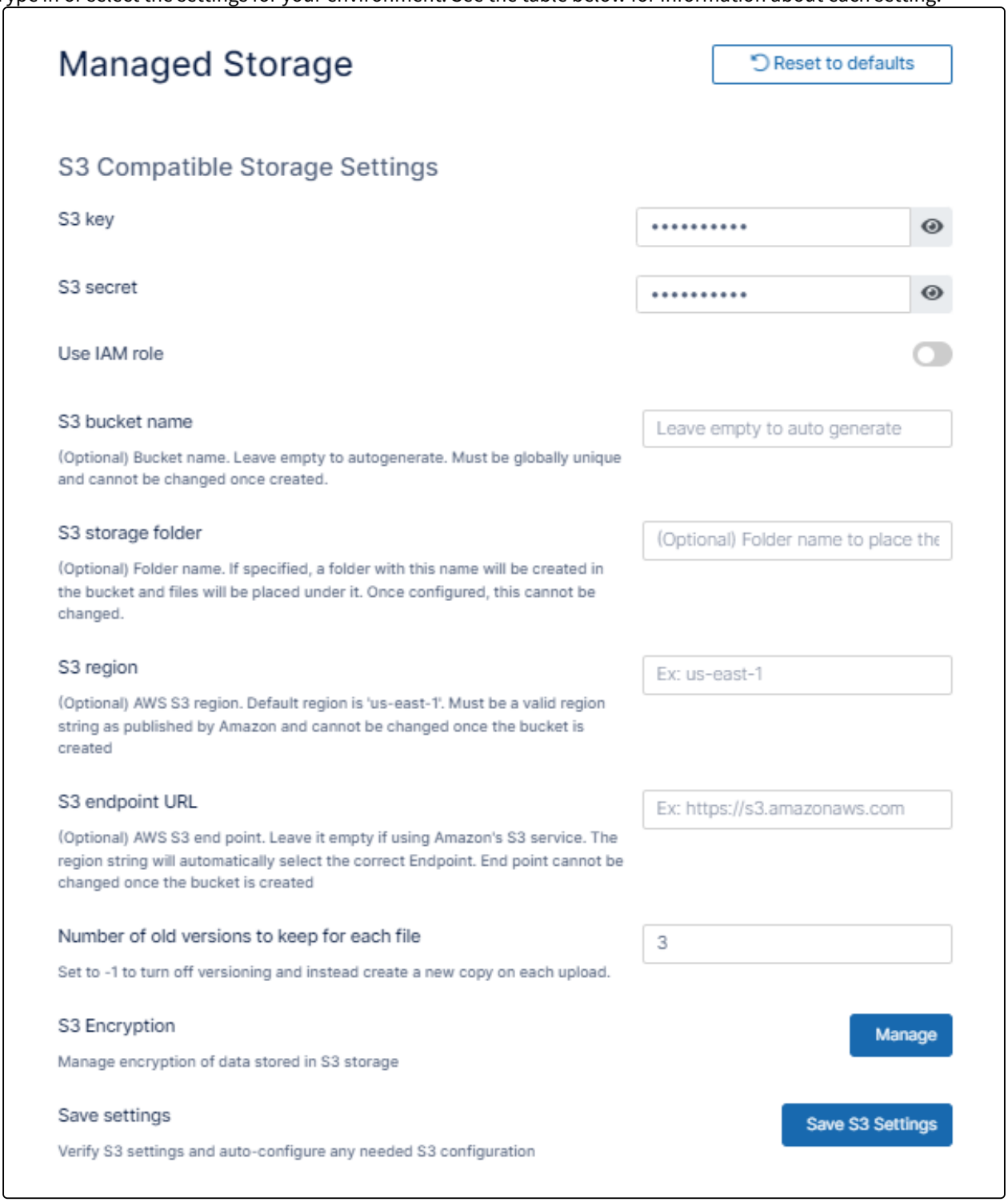
💡 **Nothing needs to be added or edited in amazons3storageconfig.php**

2. Configure Credentials

To configure Digital Ocean S3 Credentials:

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

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



3. Click **Save S3 Settings**.

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

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

Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

How to Integrate FileCloud with Wasabi Object Based Storage

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

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

WARNINGS:

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

To change the FileCloud storage path from LOCAL to WASABI

1. Enable Wasabi object storage

NOTES:

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

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

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

To enable Wasabi storage as the backend:

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

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

3. Find the following line:

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

4. Change it to this line:

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

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

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

7. Rename it to:

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

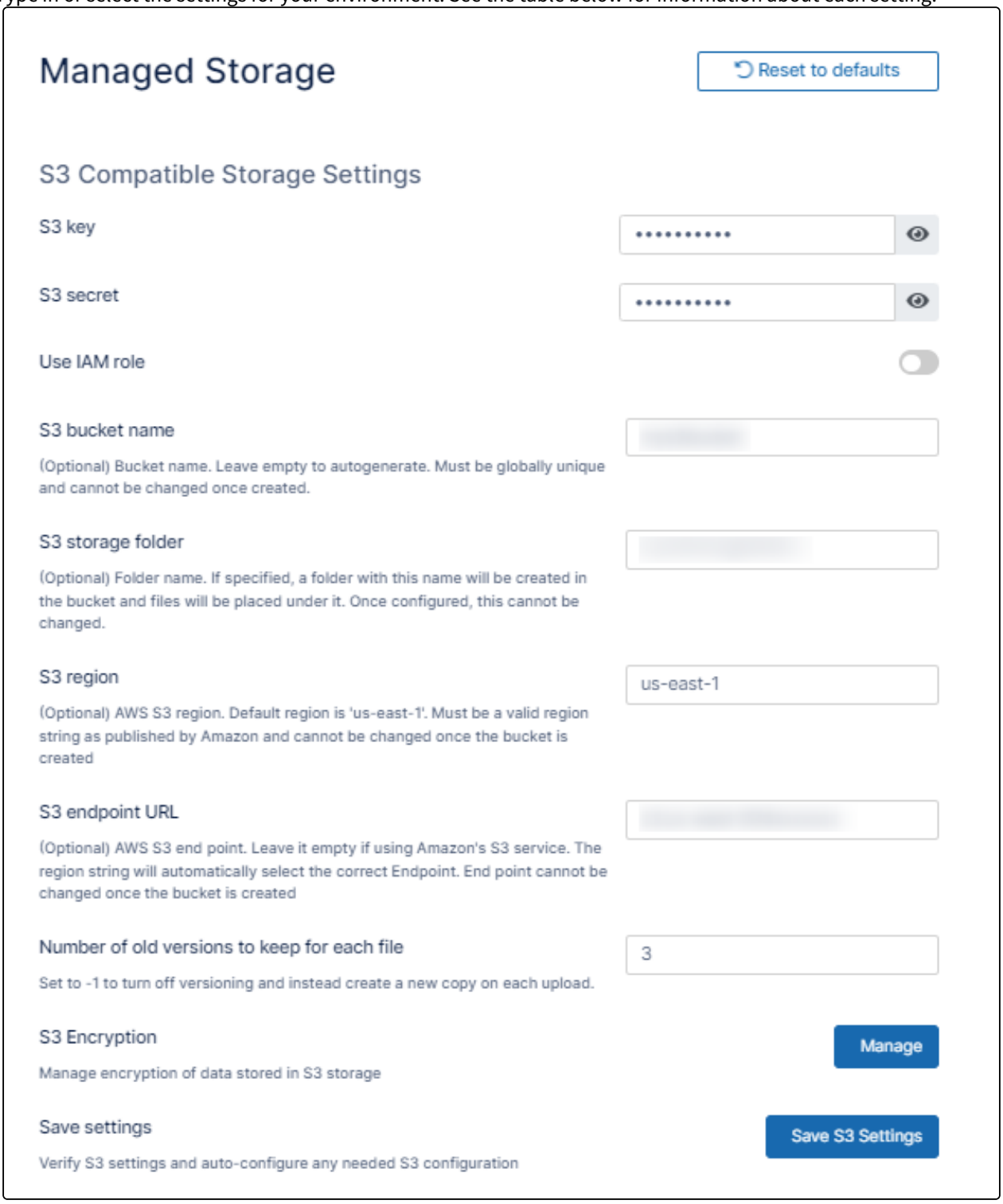
💡 **Nothing needs to be added or edited in amazons3storageconfig.php**

2. Configure Credentials

To configure Wasabi object-based storage:

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

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



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.

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

Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

FileCloud Blogs

- Migrating Storage Between Regions

How to Integrate Filecloud with Cloudian S3-Compatible Object Storage

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

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

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

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

1. Enable Cloudian S3-Compatible Object Storage

NOTES:

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

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

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

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

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

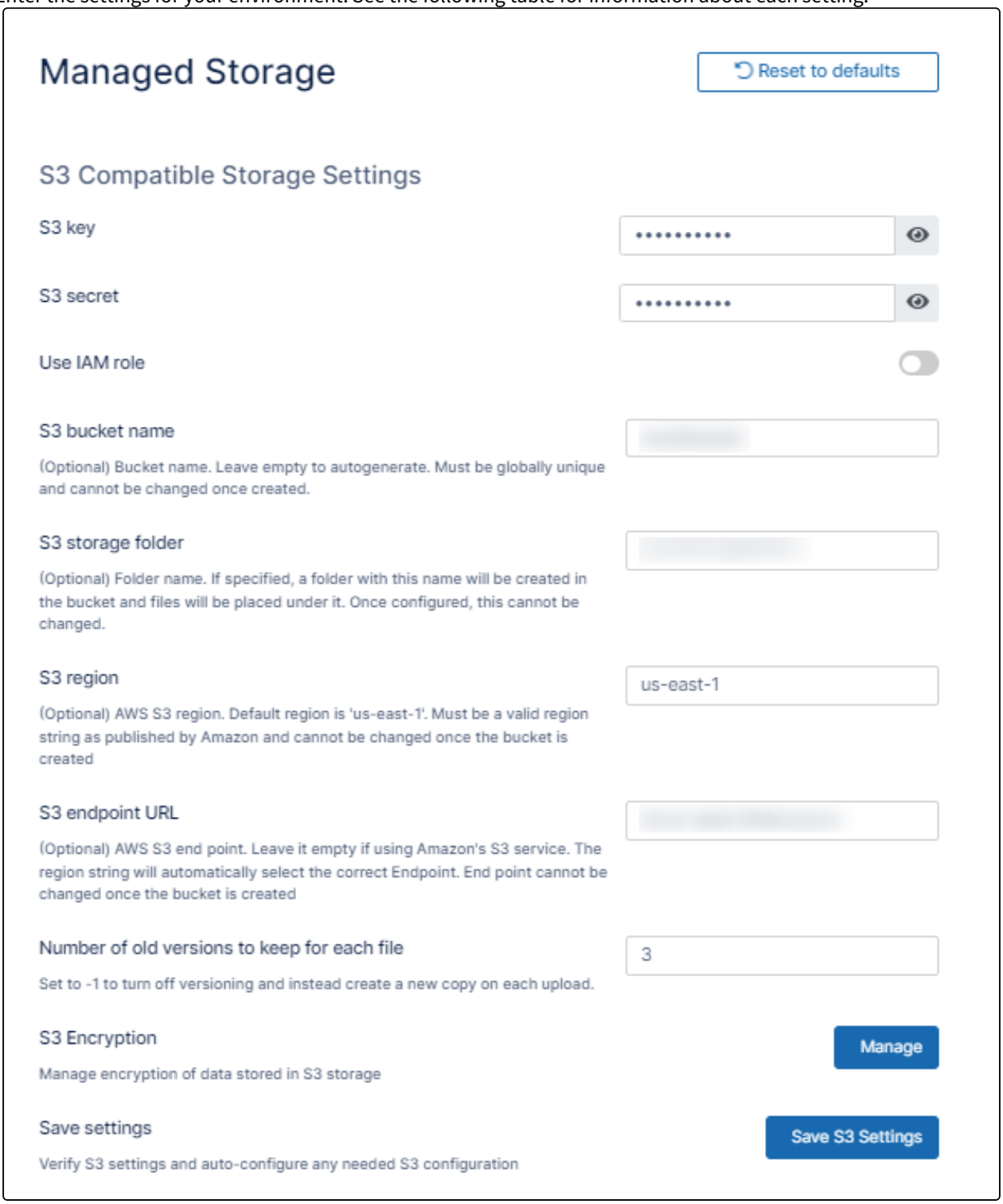
   ```
   WWWROOT/config/amazons3storageconfig.php
   ```

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

2. Configure Credentials

To configure Cloudian S3-compatible object storage:

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



3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Cloudian S3 authentication key.
S3 Secret	Your Cloudian S3 authentication secret.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem. The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Optional: All files are stored inside this root storage folder (it is created automatically).
S3 Region	Optional: Provide the region string.
S3 End Point URL	This is the S3 endpoint. note that for each region there is a specific endpoint URL.
Number of old versions to keep for each file	When a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** versions are kept. When set to **-1**, 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.

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

Troubleshooting:

How to Correct Issues with Image Previews

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

To add a line to the .htaccess file:

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

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

How to Correct Issues with playing mp4 videos

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

To add a line to the .htaccess file:

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

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

How to Integrate FileCloud with Oracle Cloud Infrastructure

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

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

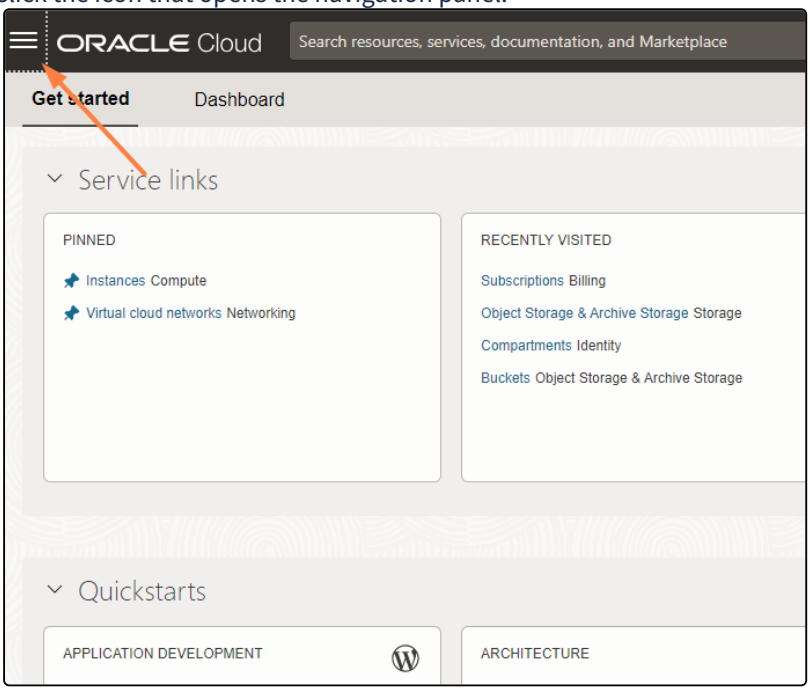
WARNINGS:

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

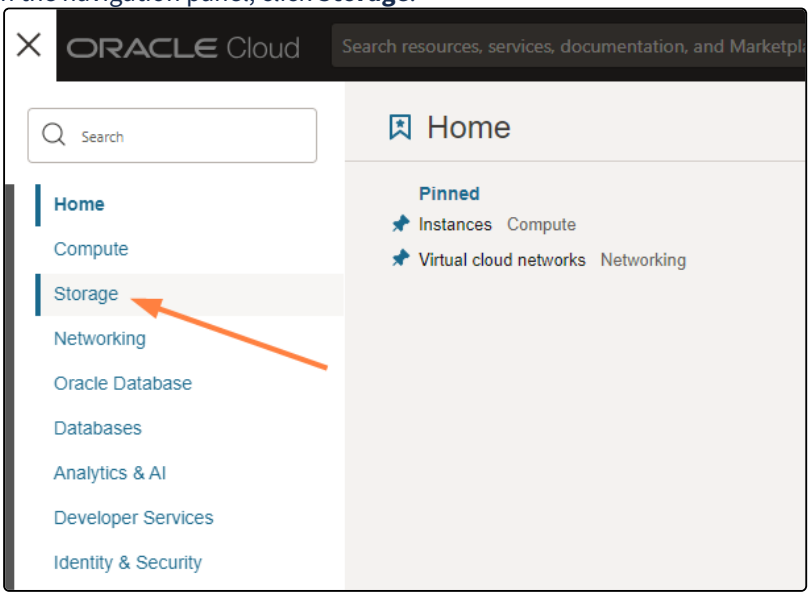
To create the S3 storage bucket and get your S3 key values in Oracle Cloud Infrastructure

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

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

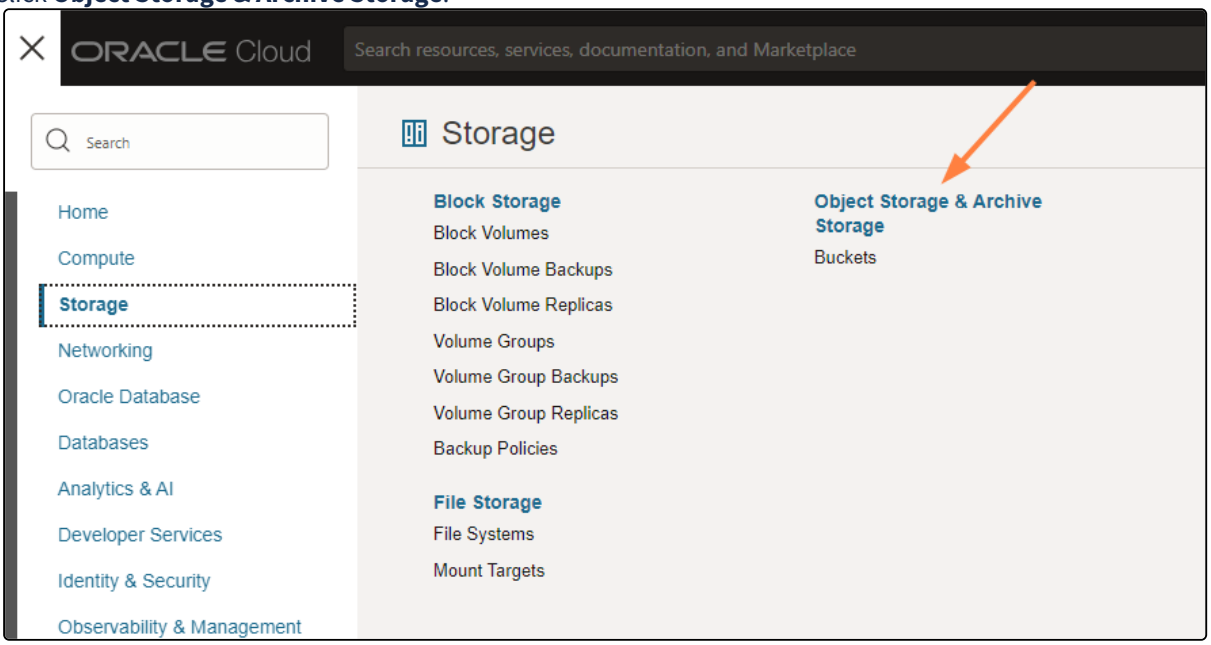


3. In the navigation panel, click **Storage**.



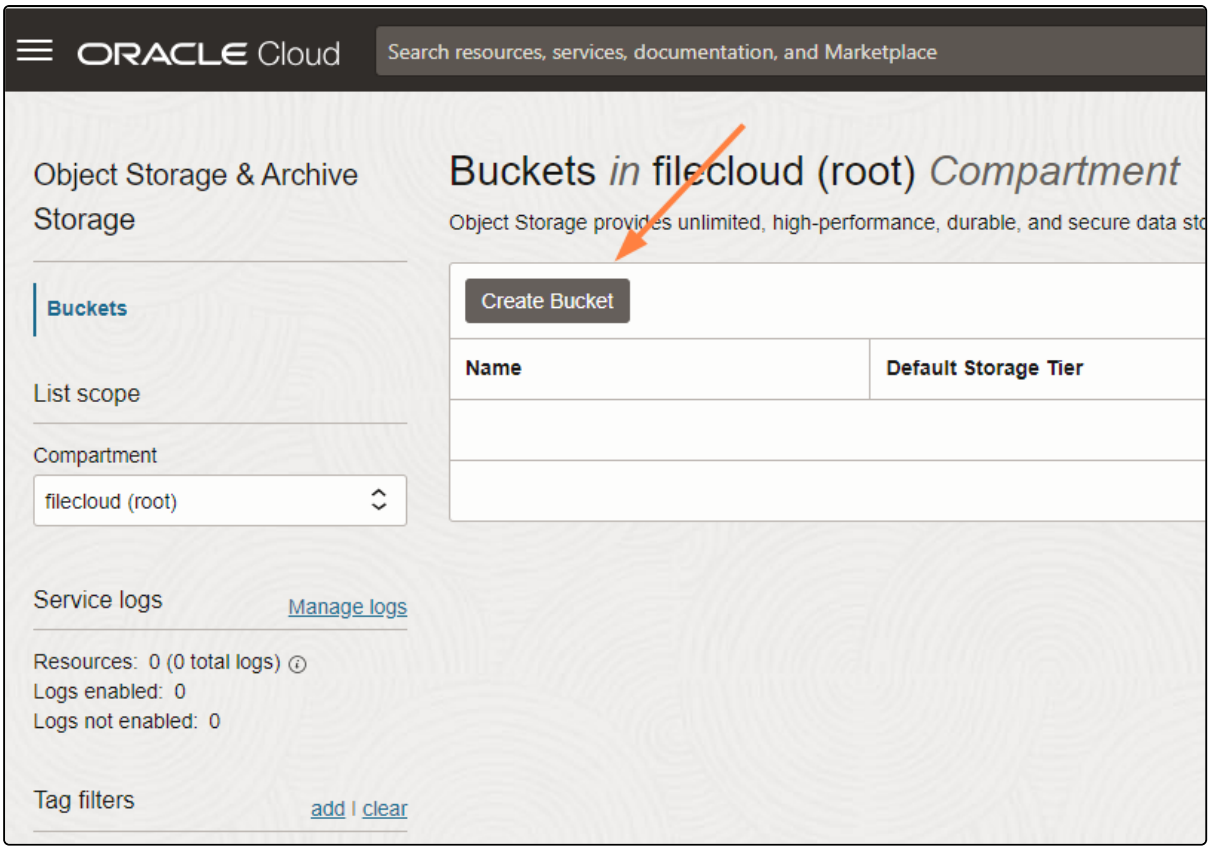
A list of storage-related pages opens.

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



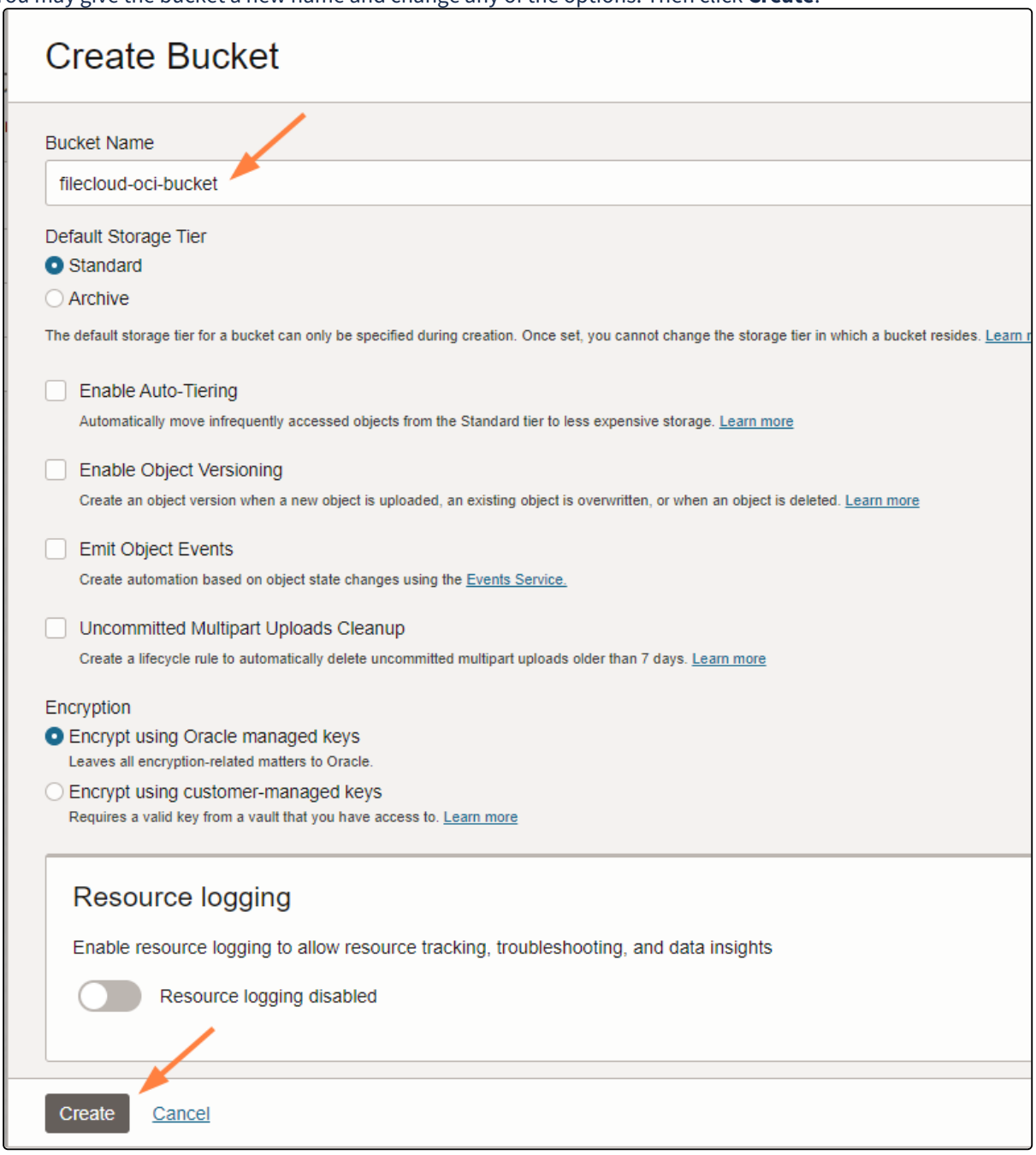
The **Object Storage & Archive Storage** page opens.

5. Click **Create Bucket**.



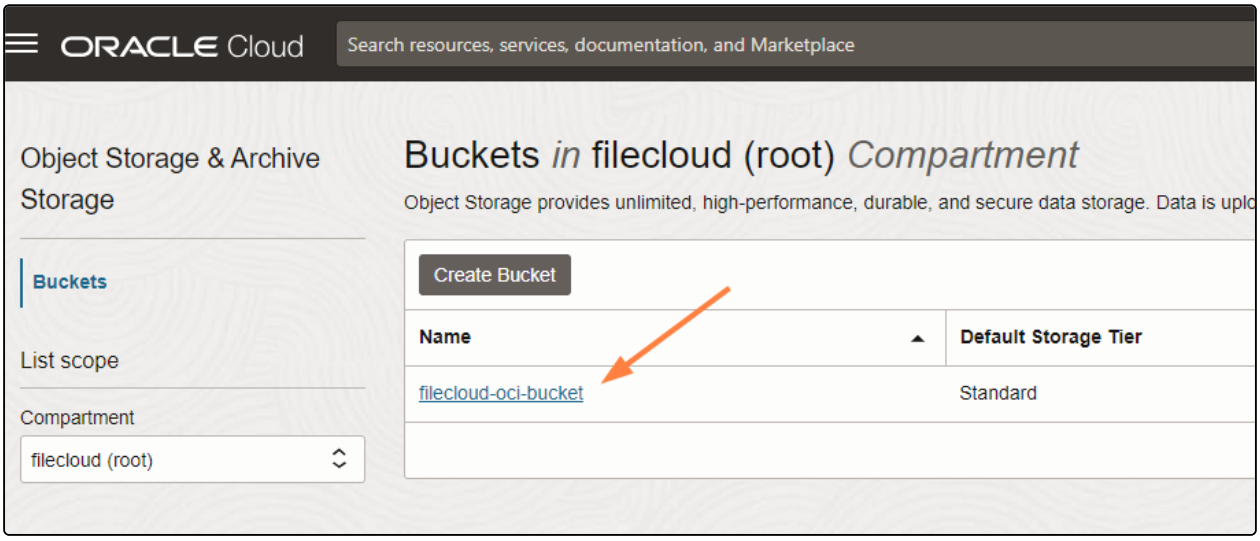
A **Create Bucket** dialog box opens.

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



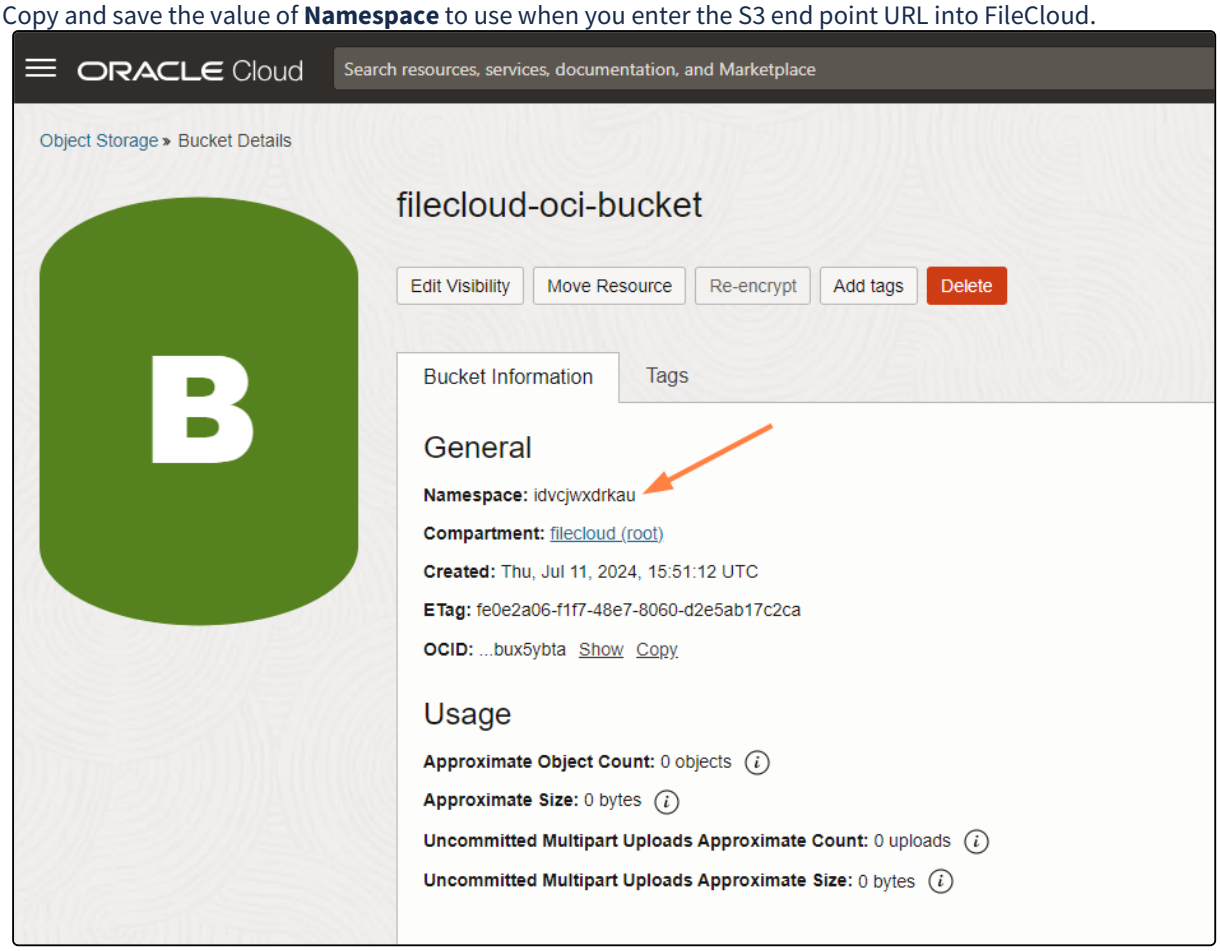
The bucket appears in the list of buckets.

7. Click the bucket name.

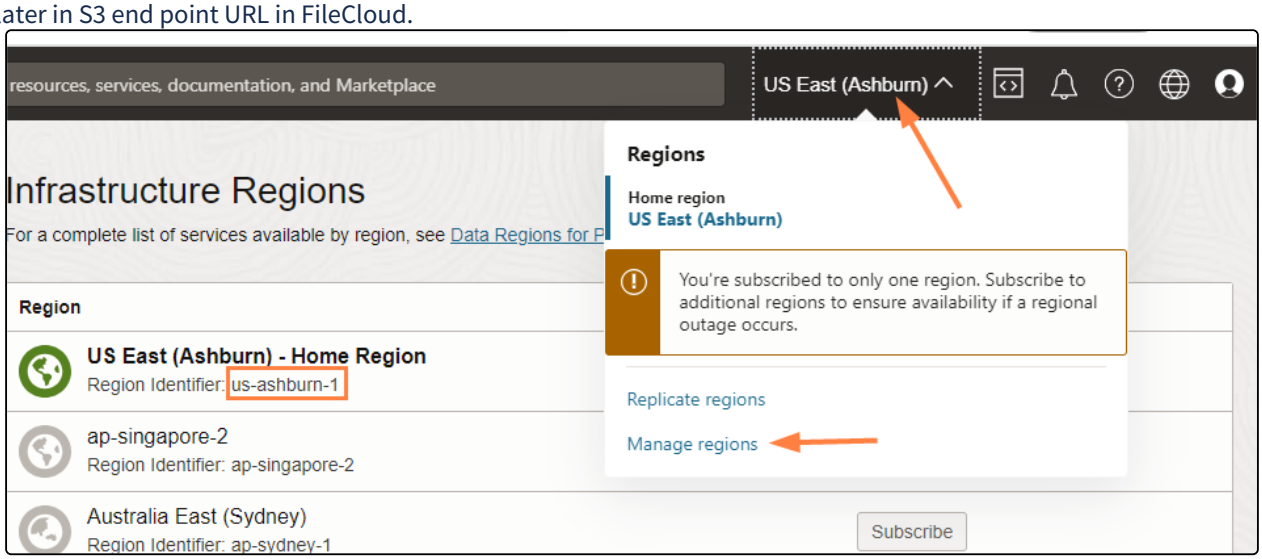


A tab with bucket information opens.

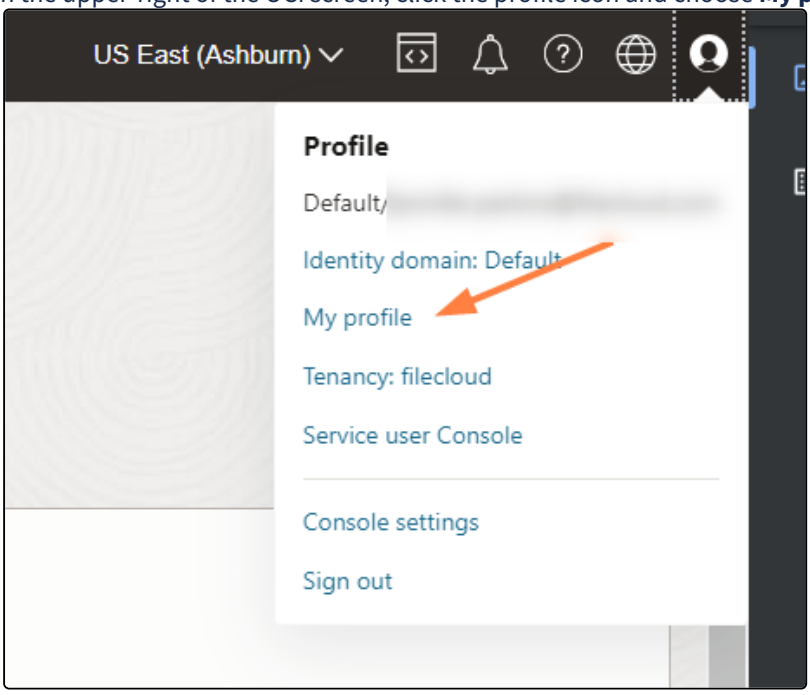
8. Copy and save the value of **Namespace** to use when you enter the S3 end point URL into FileCloud.



9. Get your region by clicking the name of your region at the top of the OCI screen, and choosing **Manage regions** in the drop-down list.
   Copy the **Region Identifier** from the top region shown (the region with the green globe icon) and save it to enter later in S3 end point URL in FileCloud.

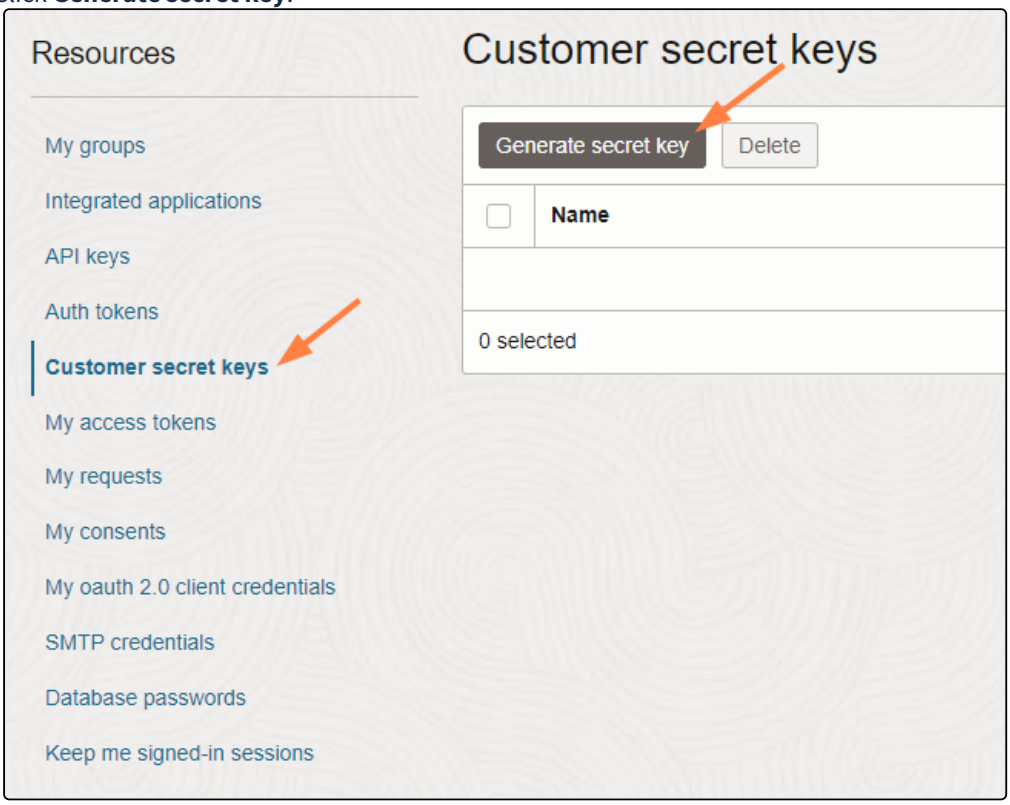


10. In the upper-right of the OCI screen, click the profile icon and choose **My profile**.



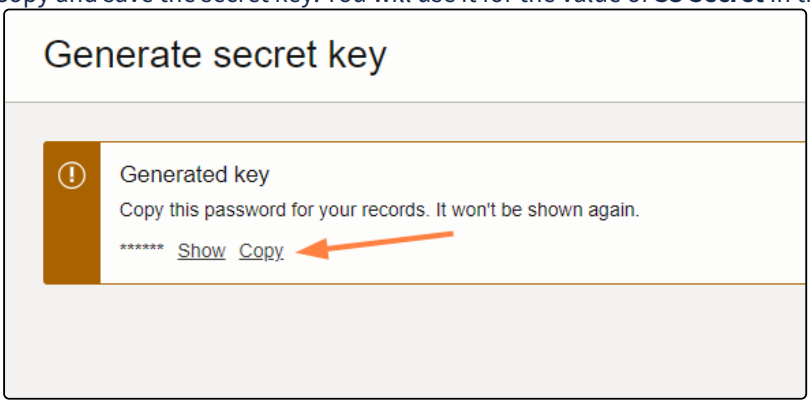
11. In the **My profile** screen navigation panel, scroll down to **Resources**, and click **Customer secret keys**.
    The **Customer secret keys** section opens.

12. Click **Generate secret key**.



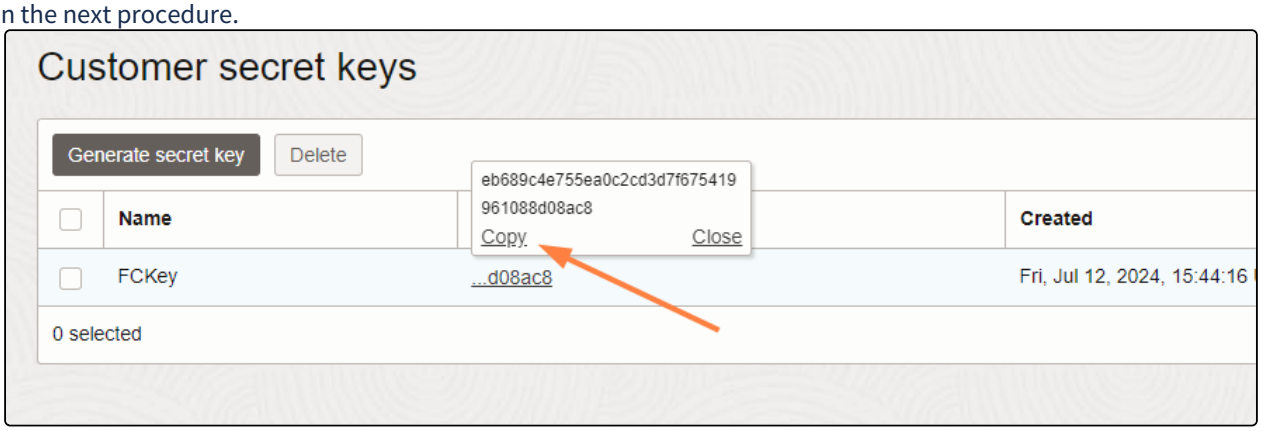
The screen confirms that the secret key was generated and prompts you to copy and save it.

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



It is now listed in the list of secret keys.

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



To integrate FileCloud and OCI

1. Enable OCI cloud object storage

NOTES:

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

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

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

To enable OCI cloud object storage as the backend:

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

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

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

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

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

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

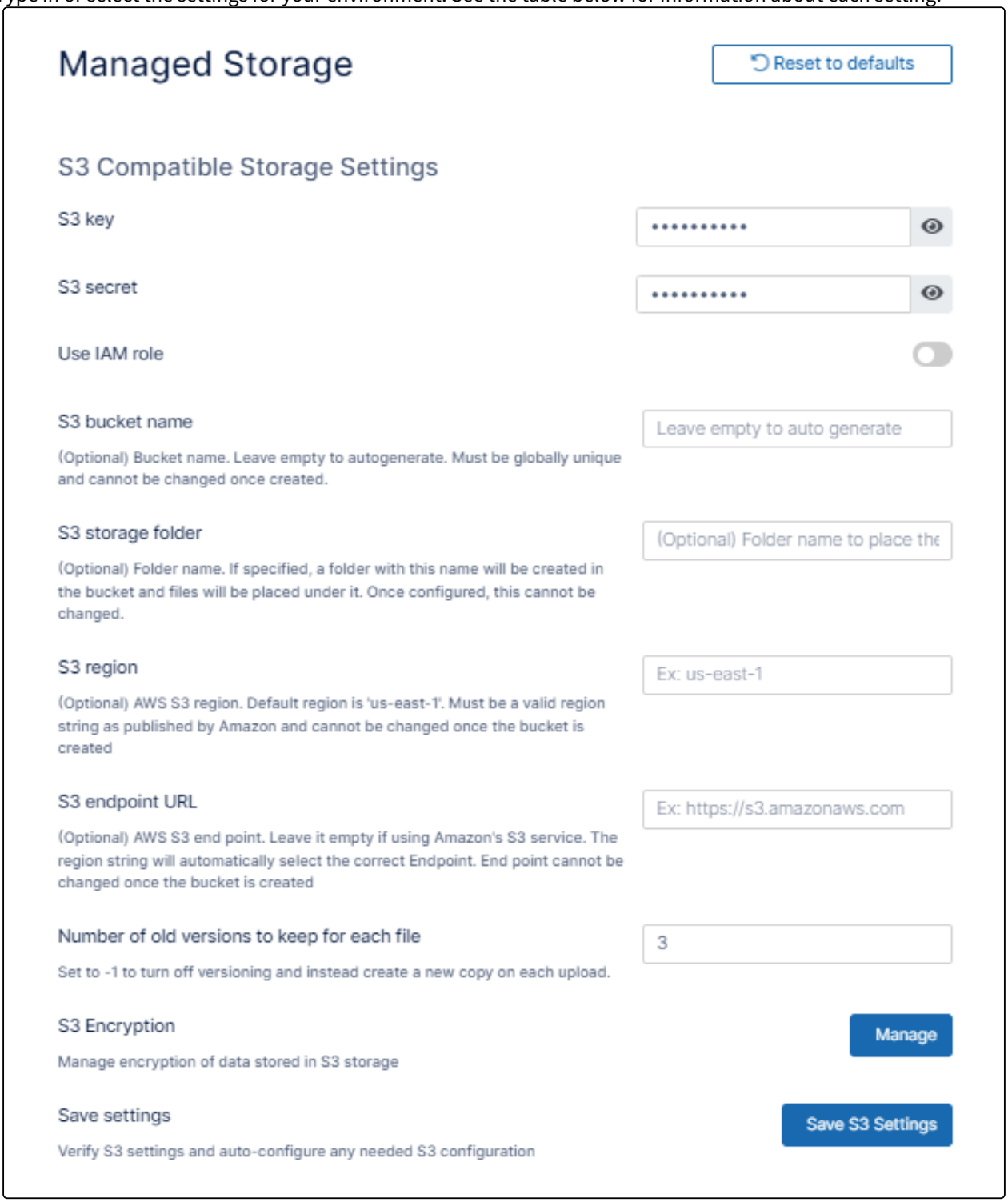
10. Save and close the file.

2. Configure Credentials in FileCloud for Managed Storage

To configure OCI object storage:

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

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



5. Click **Save S3 Settings**.

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

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

How to Integrate Filecloud with Storj

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

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

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

To change the FileCloud storage path from LOCAL to Storj:

1. Enable Storj S3-Compatible Object Storage

NOTES:

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

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

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

To enable Storj as backend storage:

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

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

3. Find the following line:

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

4. Change it to:

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

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

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

7. Rename it to:

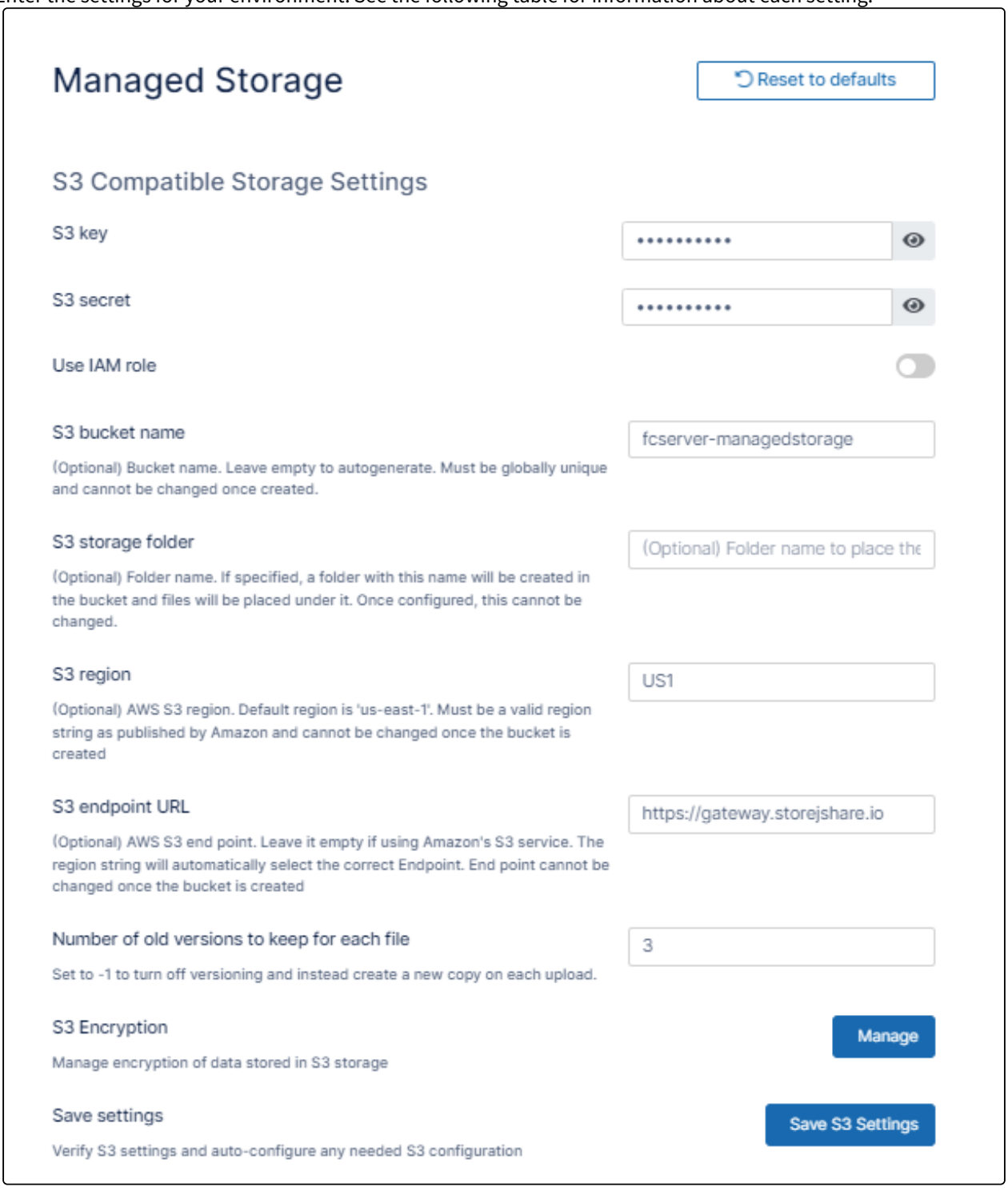
```
WWWROOT/config/amazons3storageconfig.php
```

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

2. Configure Credentials

To configure FileCloud to access the Storj S3 bucket:

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



3. Click **Save S3 Settings**.

Field	Description
S3 Key	Your Storj authentication key.
S3 Secret	Your Storj authentication secret.
Use IAM role	Do not check; this option is not supported in Storj.
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstances, a previously used bucket in FileCloud can be used). It is important that the S3 bucket is never modified outside of the FileCloud subsystem. The bucket name is case sensitive; make sure you are using the exact name of the bucket.
S3 Storage Folder	Leave blank. Not supported in Storj.
S3 Region	US1, EU1, or AP1
S3 End Point URL	https://gateway.storjshare.io
Number of old versions to keep for each file	Storj has a beta feature supporting versioning. See https://docs.storj.io/dcs/buckets/object-versioning for more information. In FileCloud, when a user uploads a new version of a file, it is saved, and the latest **Number of old versions to keep for each file** are kept. When set to **-1**, each upload of a file overwrites the previous one, and no versions are saved.
S3 Encryption	Select **No Encryption** or **Amazon S3-Managed Key Encryption**. See https://docs.storj.io/learn/concepts/encryption-key for more information.

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

Setting up Managed Storage Encryption

Administrators can enable storage-level encryption supported by FileCloud.

Currently encryption is supported only for:

- Managed Storage (local)
- Amazon S3 storage

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

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

- 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

Storage Encryption Technical Details

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

This topic describes:

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

How a Plain File Key is Created

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

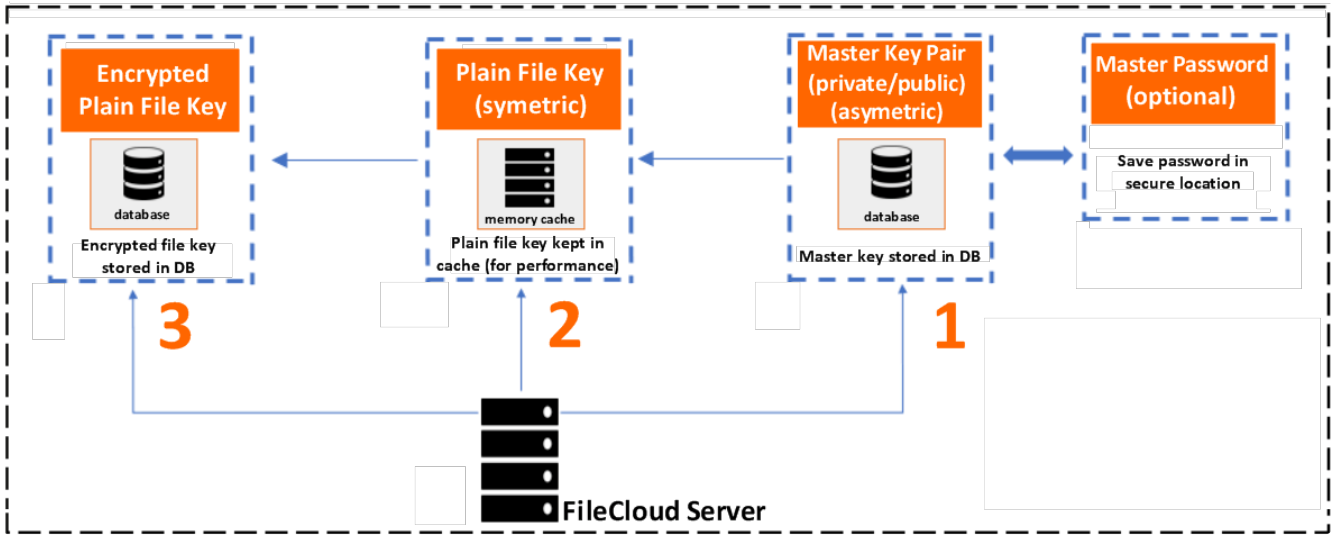
- A plain file key will be used to encrypt and decrypt all files using symmetric encryption
- If you set a password when you enable encryption, you will need to supply the master password before the initialization process can start

Warning On Master Password

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

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

Figure 1. How a Plain File Key is Created



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

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

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

Technical Details about Encryption Keys

Additional details on the keys:

Key	Key Details	User Input	Persistence	Remarks
Master public/ private key pair	• Asymetric • 4096 bits • RSA • sha512 digest	Password (optional)	Both private and public keys are persisted	• It is important to save the password (if one was provided)
Plain File Key	• Symetric • AES • 256 bits	None	Not persisted	• The plain file key will be used to encrypt decrypt all files using symmetric encryption • This key will not be persisted but will be cached for performance • The cache will be valid for the lifetime of the FileCloud server process
Encrypted File Key	• Encrypted using master public key	None	Encrypted file key is persisted	• Decryption of the encrypted file key results in plain file key • Decryption of the encrypted file key will be done using the master private key and optional master password • The plain key that is a result of decryption process is cached for the lifetime of the FileCloud server process 💡 Whenever you restart the server, the encrypted file key is decrypted again.

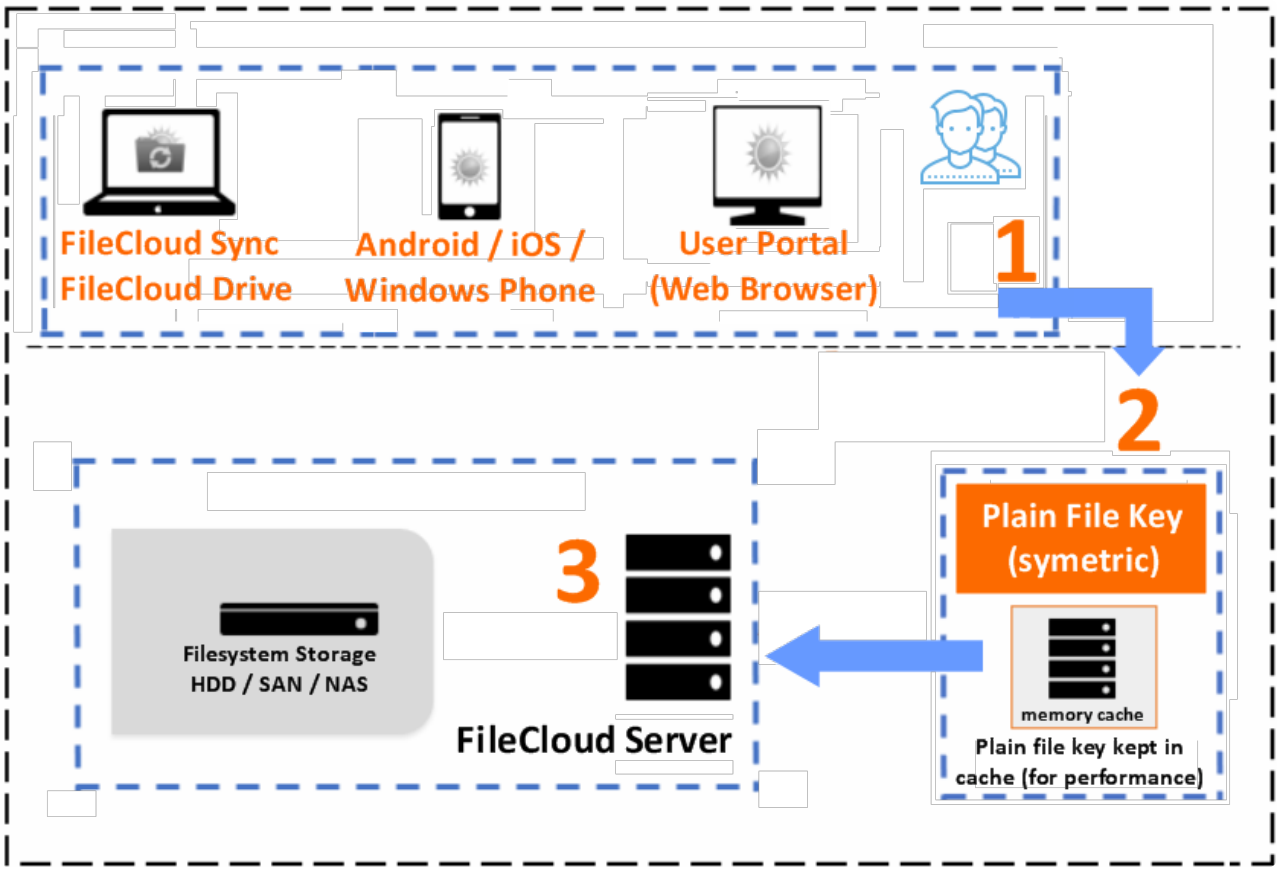
When are Files Encrypted?

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

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

The file encryption process is described in Figure 2.

Figure 2. How Files Are Encrypted



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

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

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

When are Files Decrypted?

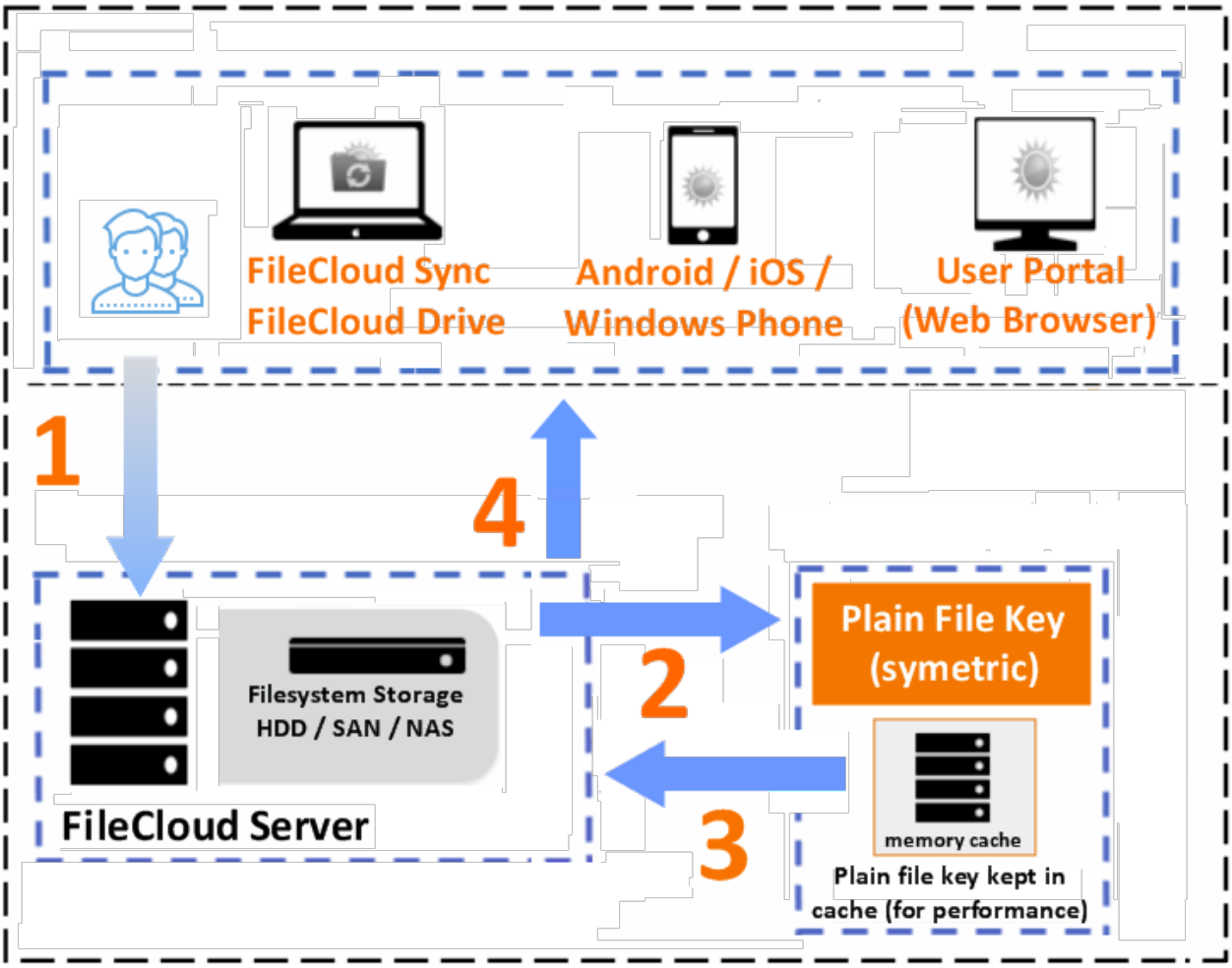
Storage decryption will occur without notifying the end user.

This means that:

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

The file decryption process is described in Figure 3.

Figure 3. How Files Are Decrypted



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

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

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

Enabling Storage Encryption

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

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

To enable storage encryption:

1. Encryption 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.	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 **Windows: XAMPP_HOME\php\extras\ssl\openssl.cnf** **Linux: /etc/ssl/openssl.cnf** In Windows, for example, if you have XAMPP installed in D:\xampp, then add the following line to cloudconfig.php. **define("SSL_CONF_FILE","D:\\xampp\\php\\extras\\ssl\\openssl.cnf");**

2. Enable the Encryption Module

By default, the encryption module is not enabled.

You can enable the encryption module in two ways:

- If FIPS mode is active:
  In order to ensure FIPS Mode is on, enable the FIPS Admin Banner by accessing (**WEBROOT/config/localstorageconfig.php** file) and adding the following:
  define("TONIDOCLOUD_FIPS140_ENABLED", 1);
  Note: When enabling FIPS mode, you must also enable managed storage encryption. See Step 3 that follows.

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

Additional Parameter To Enable Encryption
`define("TONIDO_LOCALSTORAGE_INCLUDEENCRYPTION", 1 );`

where:

Parameter	Expected Value	Additional Notes

TONIDO_LOCALSTORAGE_INCLUDEENCRYPTION	1	1 - enable encryption for local managed storage 0 - disable encryption

3. Manage Storage Encryption

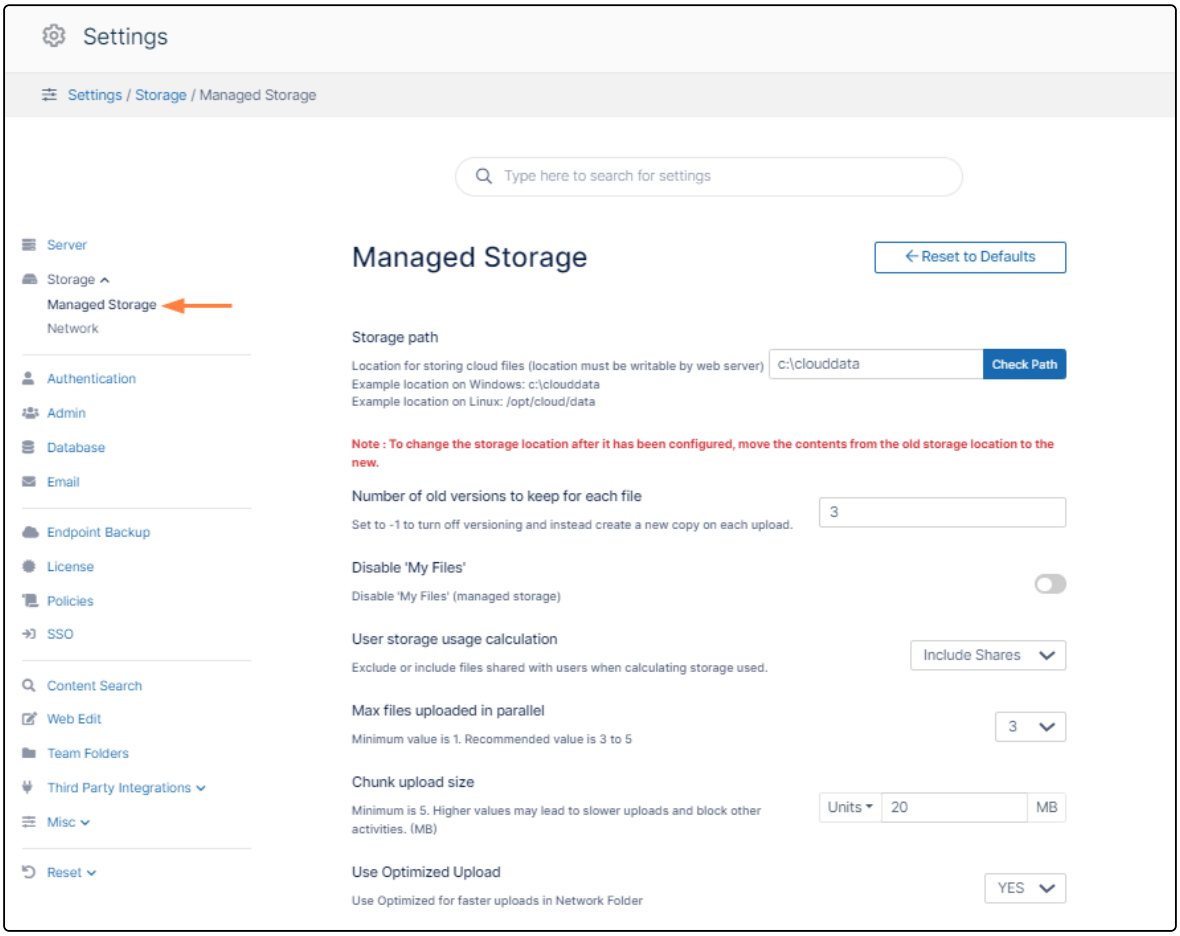
After you enable the encryption module, the admin portal displays the encryption option.

Encryption Password

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

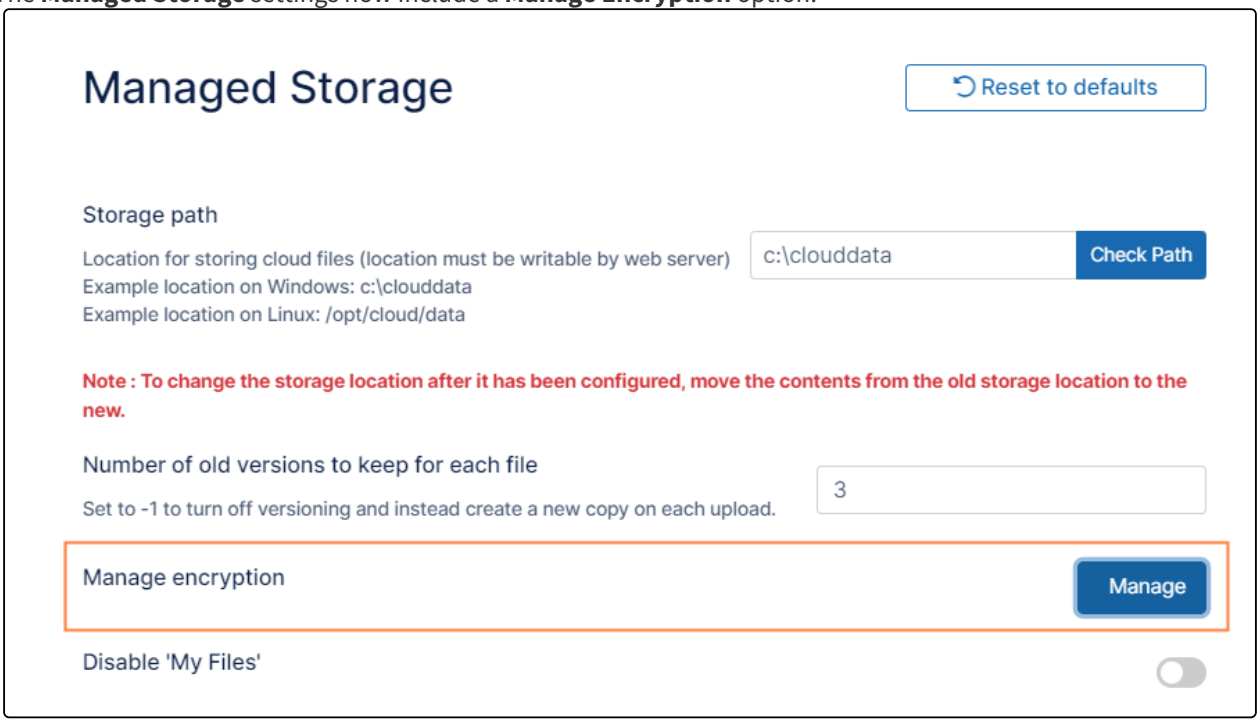
To manage encryption:

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



The **Managed Storage** settings page opens.

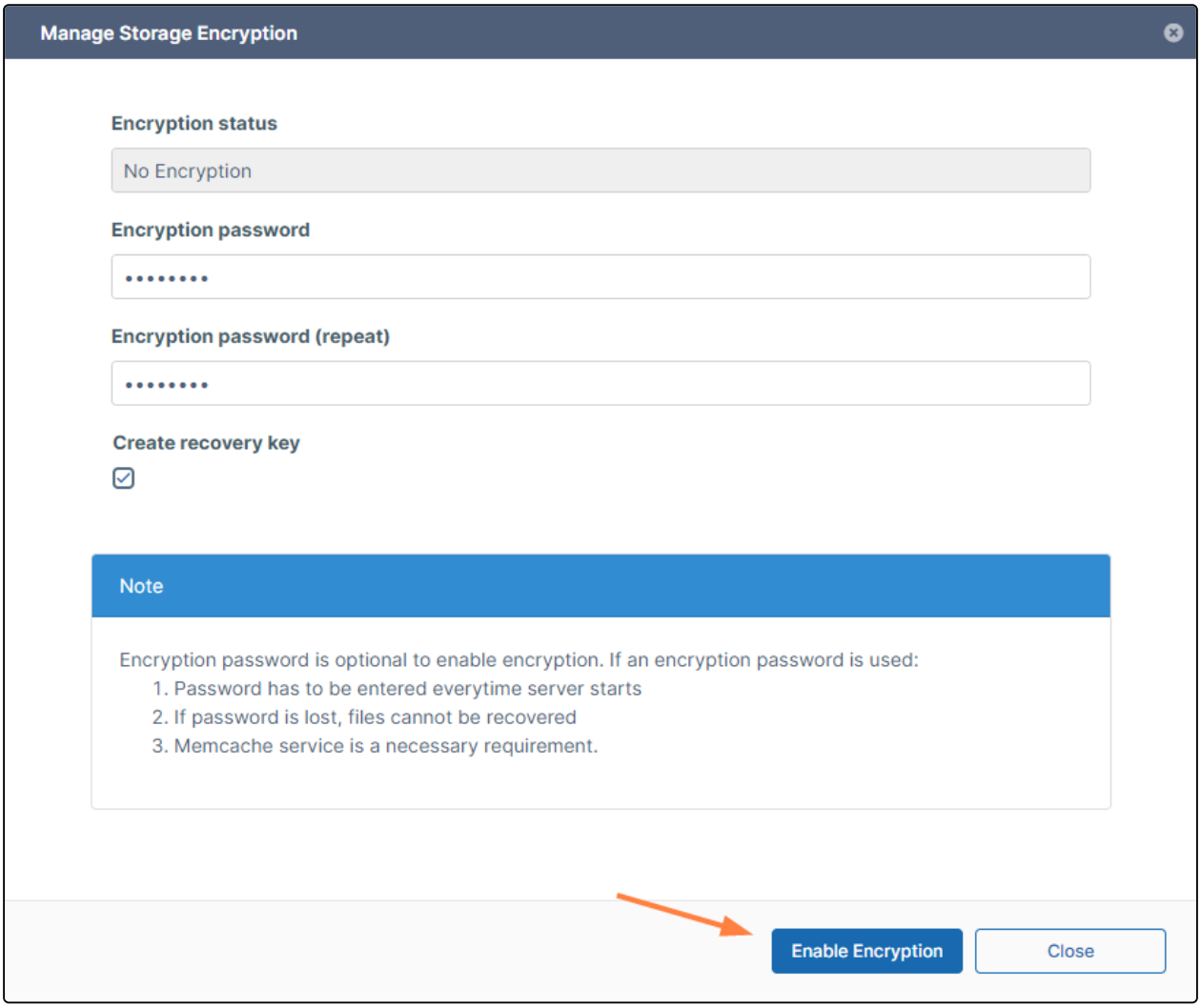
The **Managed Storage** settings now include a **Manage Encryption** option.



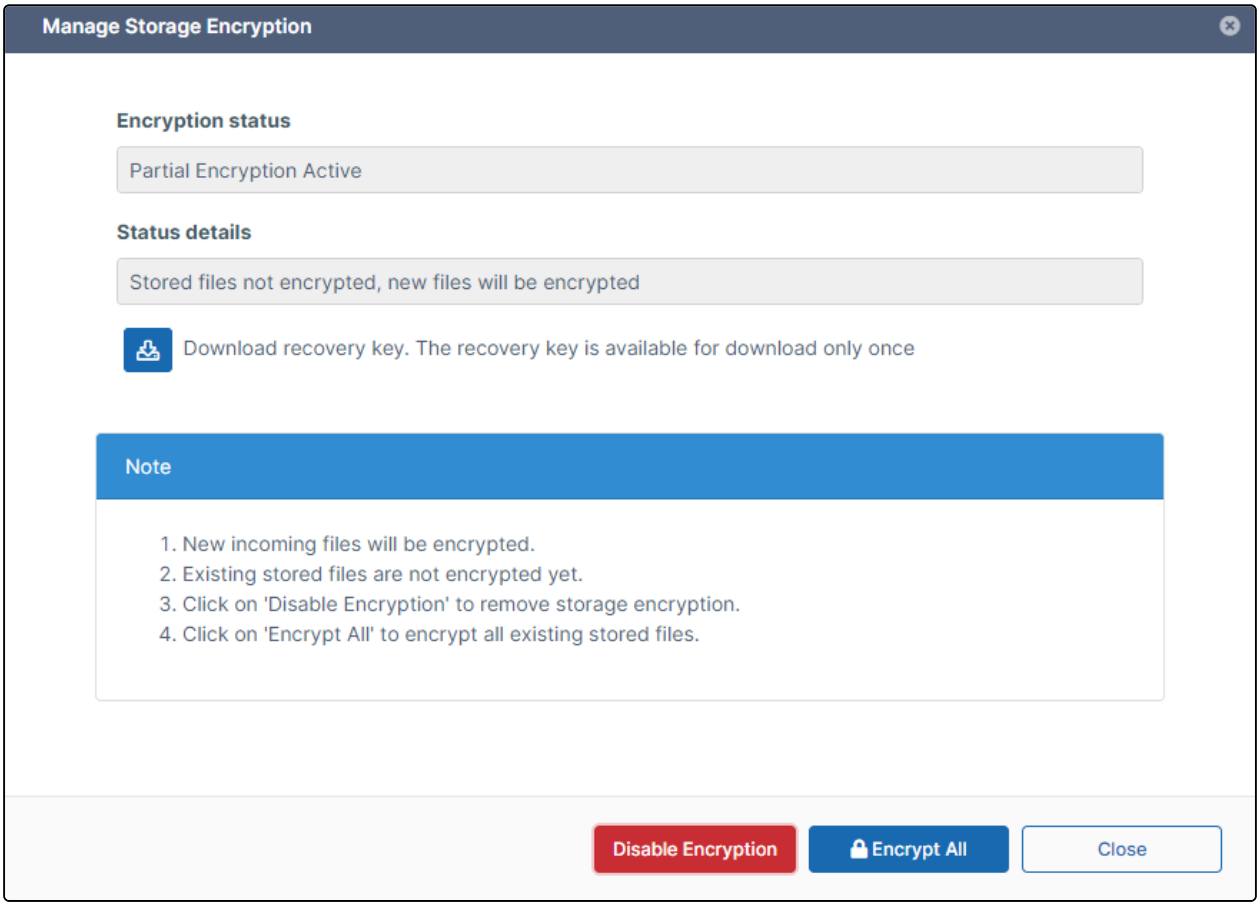
2. To open the **Manage Storage Encryption** dialog box, click **Manage**.
3. To set an optional password, in **Encryption password**, type in a strong password.

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

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



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



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

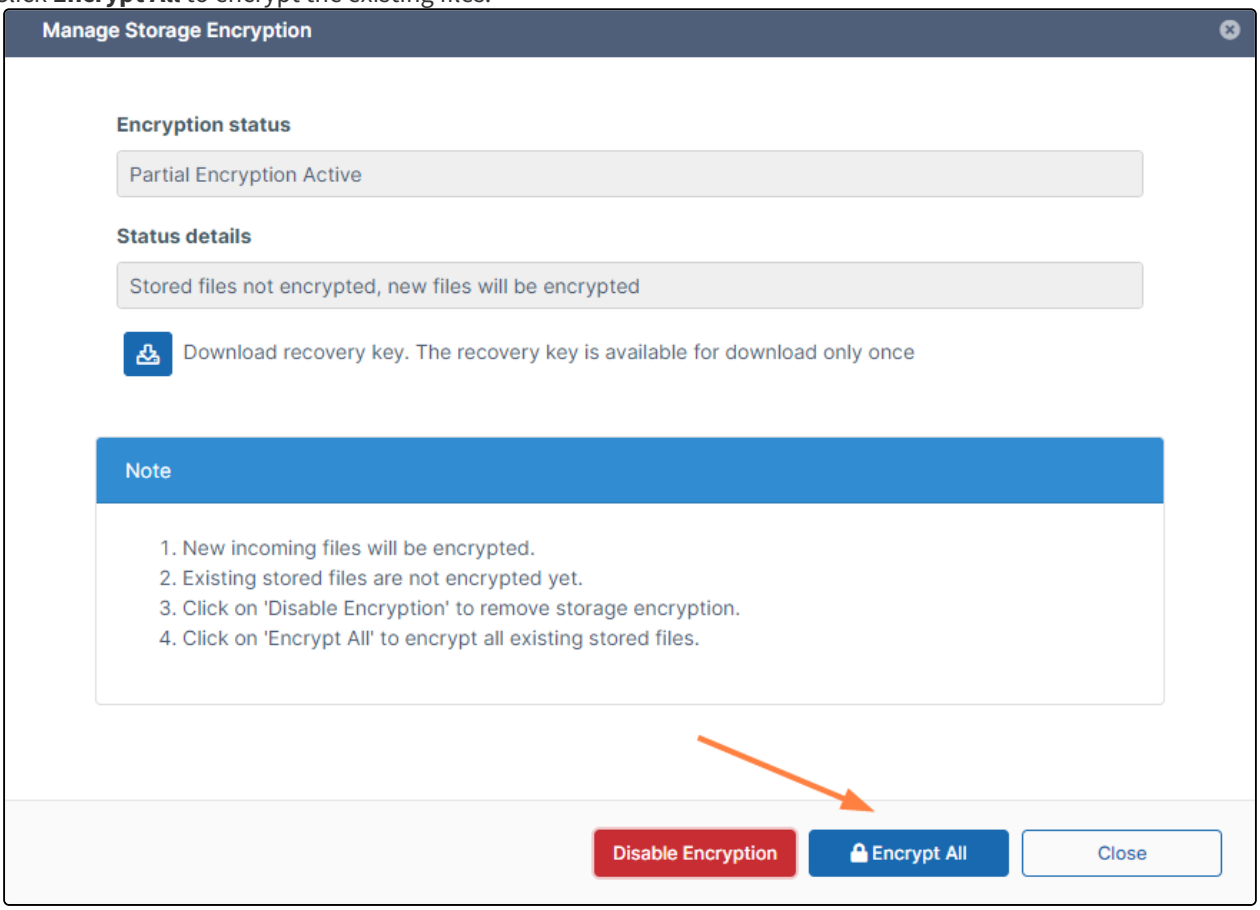
4. Encrypt any existing files

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

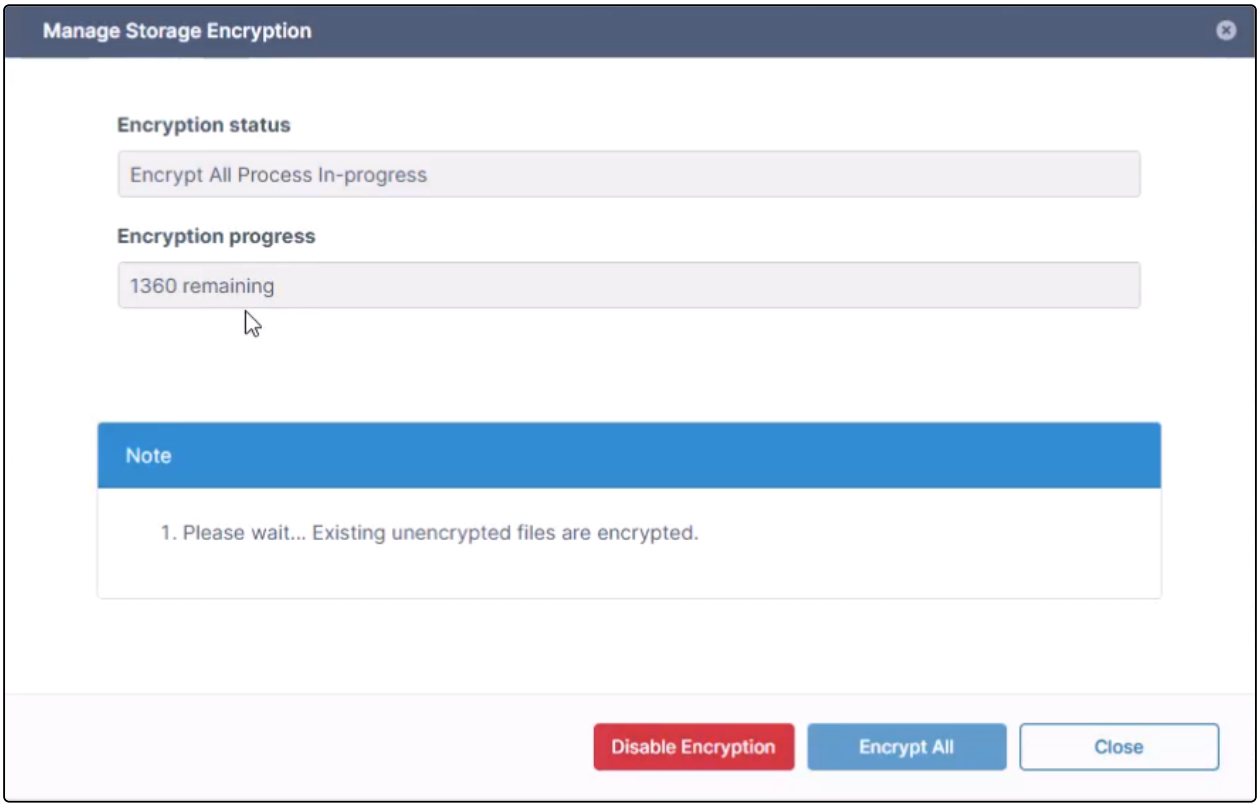
If your local storage already contains files:

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

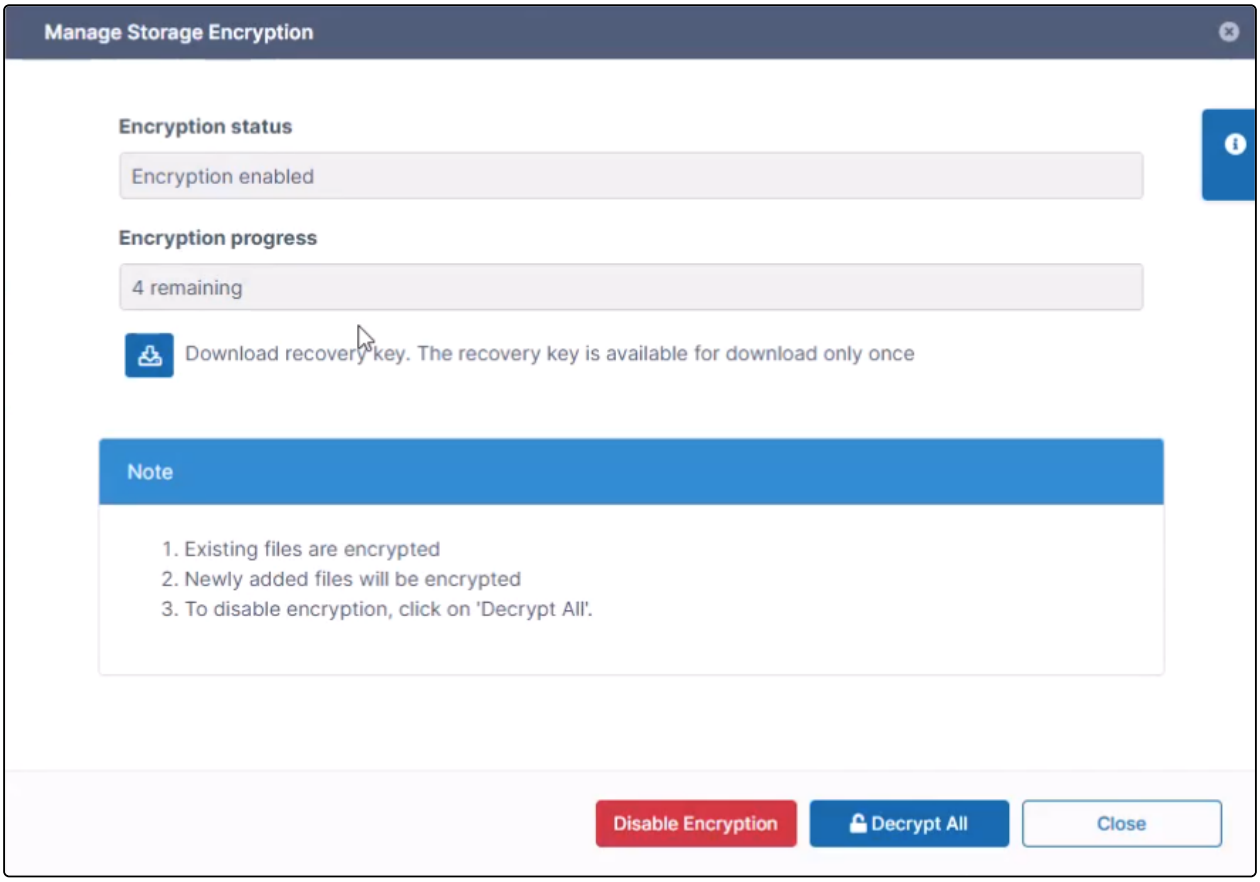
1. Click **Encrypt All** to encrypt the existing files.



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



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



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

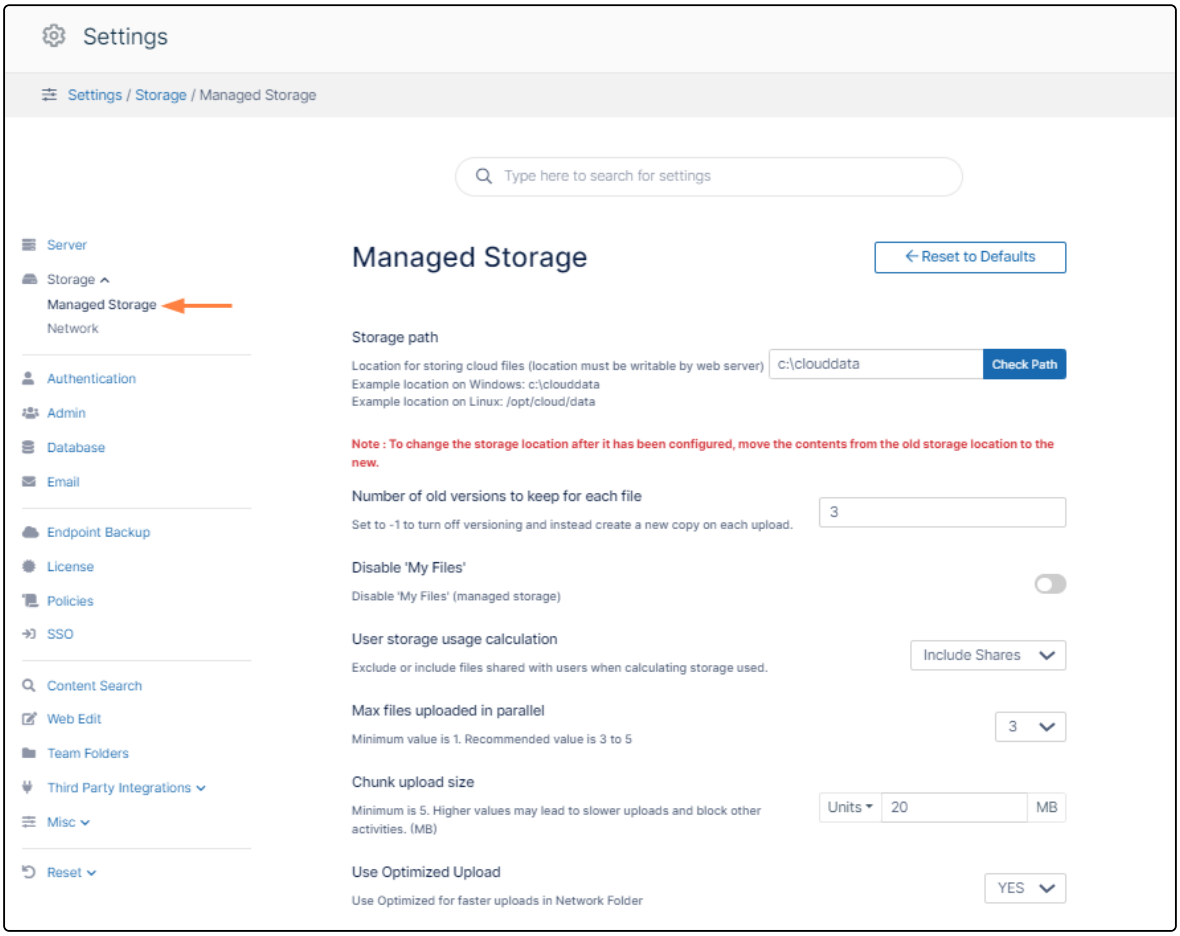
- You will not see an **Encrypt All** button.
- Your system is already in a fully-encrypted state.

Disabling Storage Encryption

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

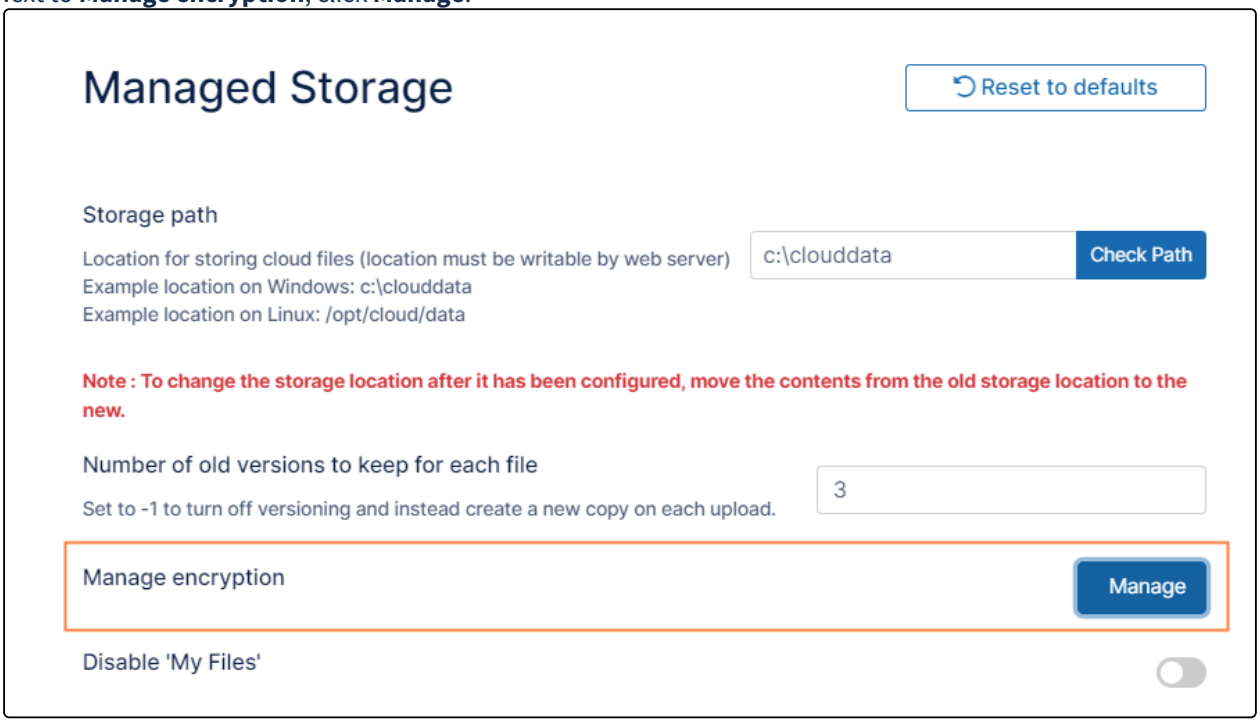
To decrypt files:

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

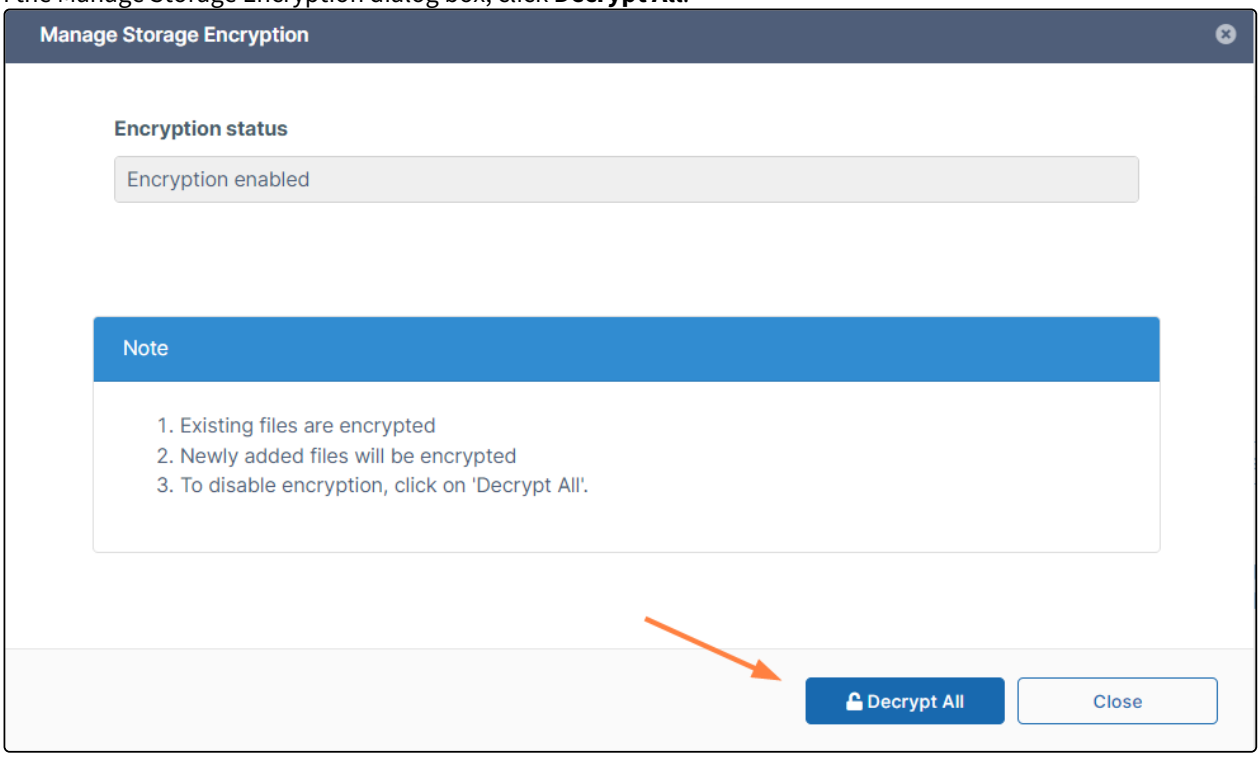


The **Managed Storage** settings page opens.

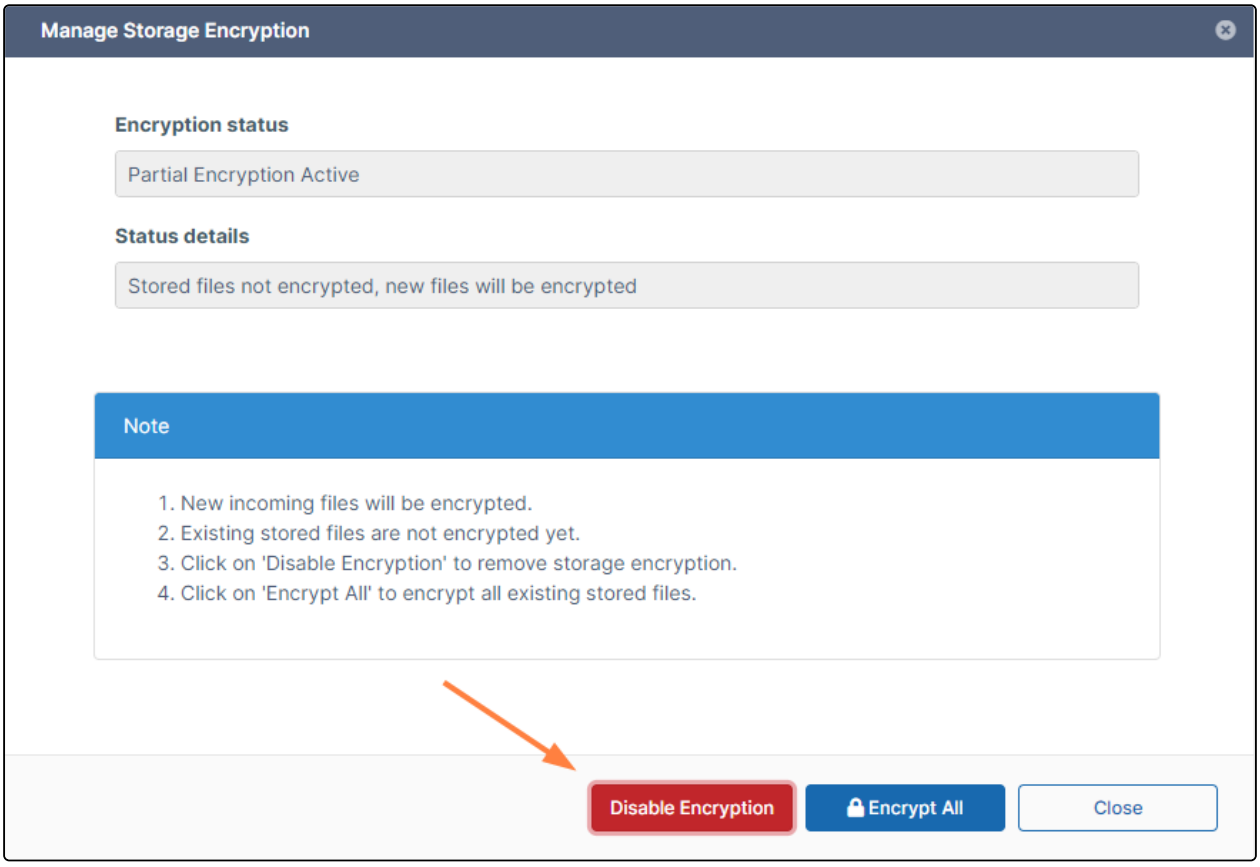
2. Next to **Manage encryption**, click **Manage**.



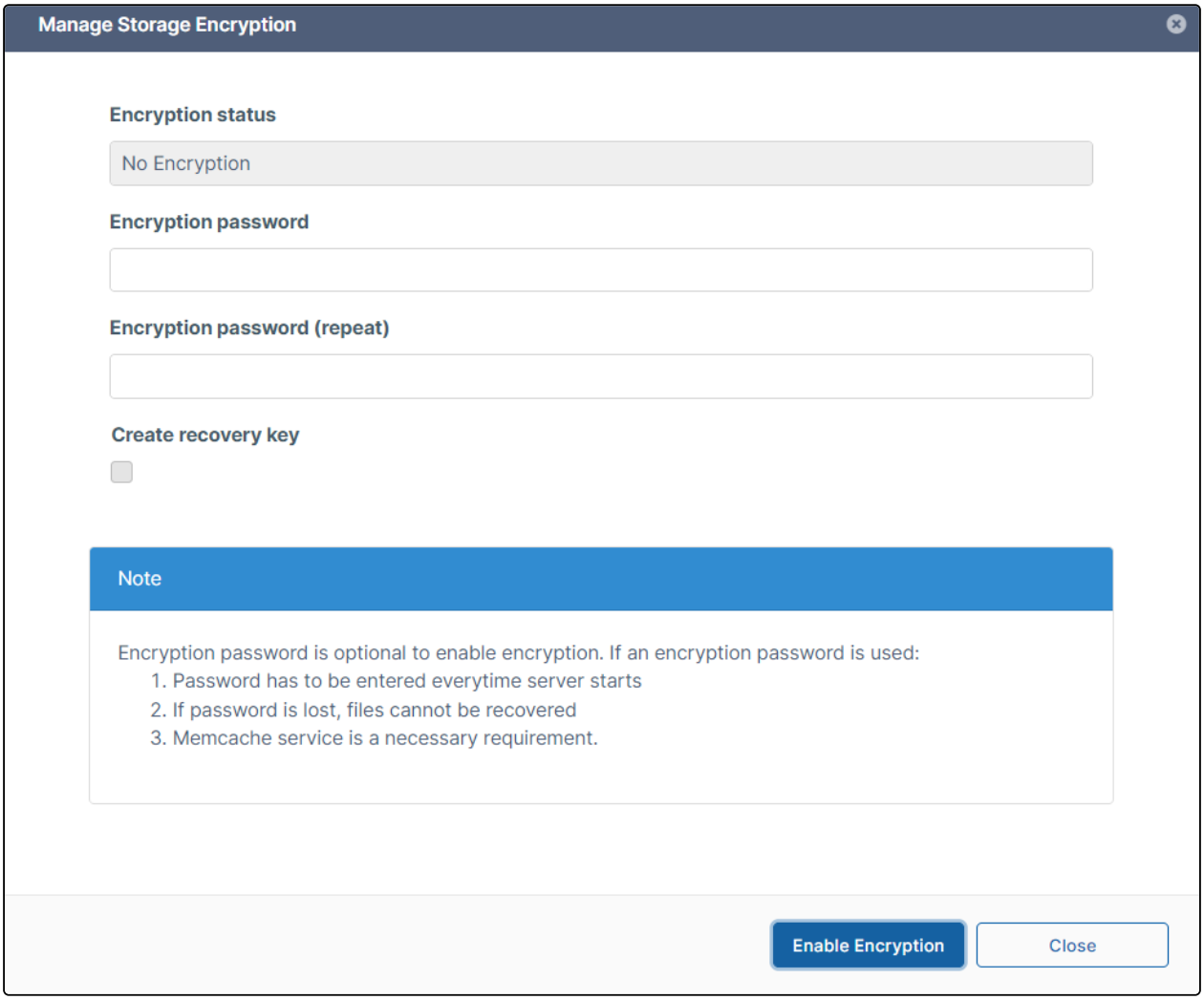
3. In the Manage Storage Encryption dialog box, click **Decrypt All**.



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



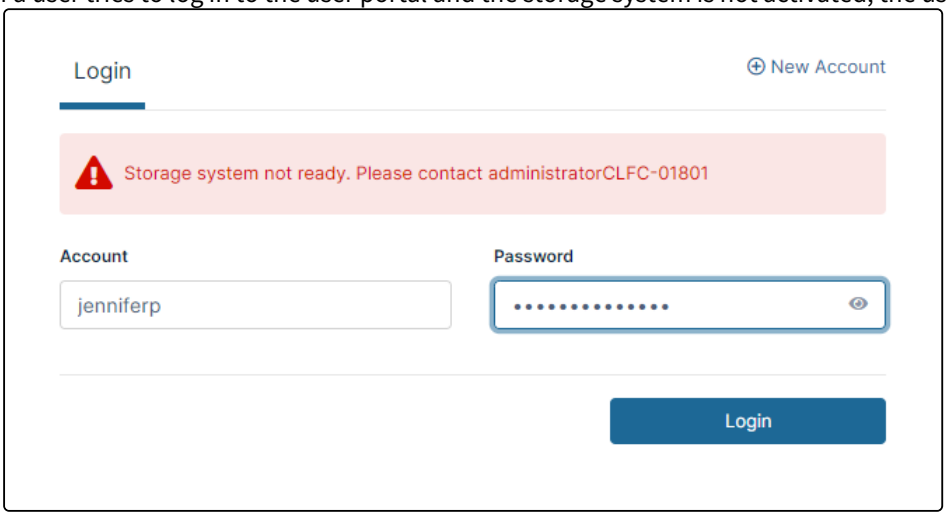
The dialog box shows notifications that decryption is in progress.
Once decryption is complete, the following screen is shown.



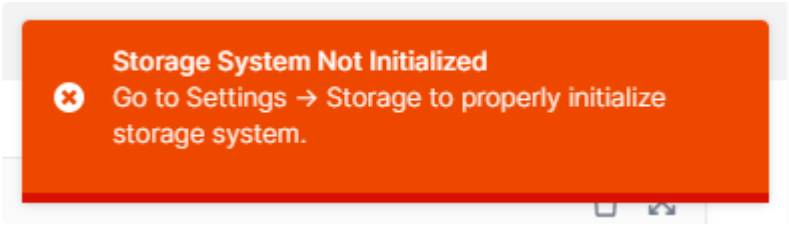
Activating Password Protected Storage Encryption

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

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



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

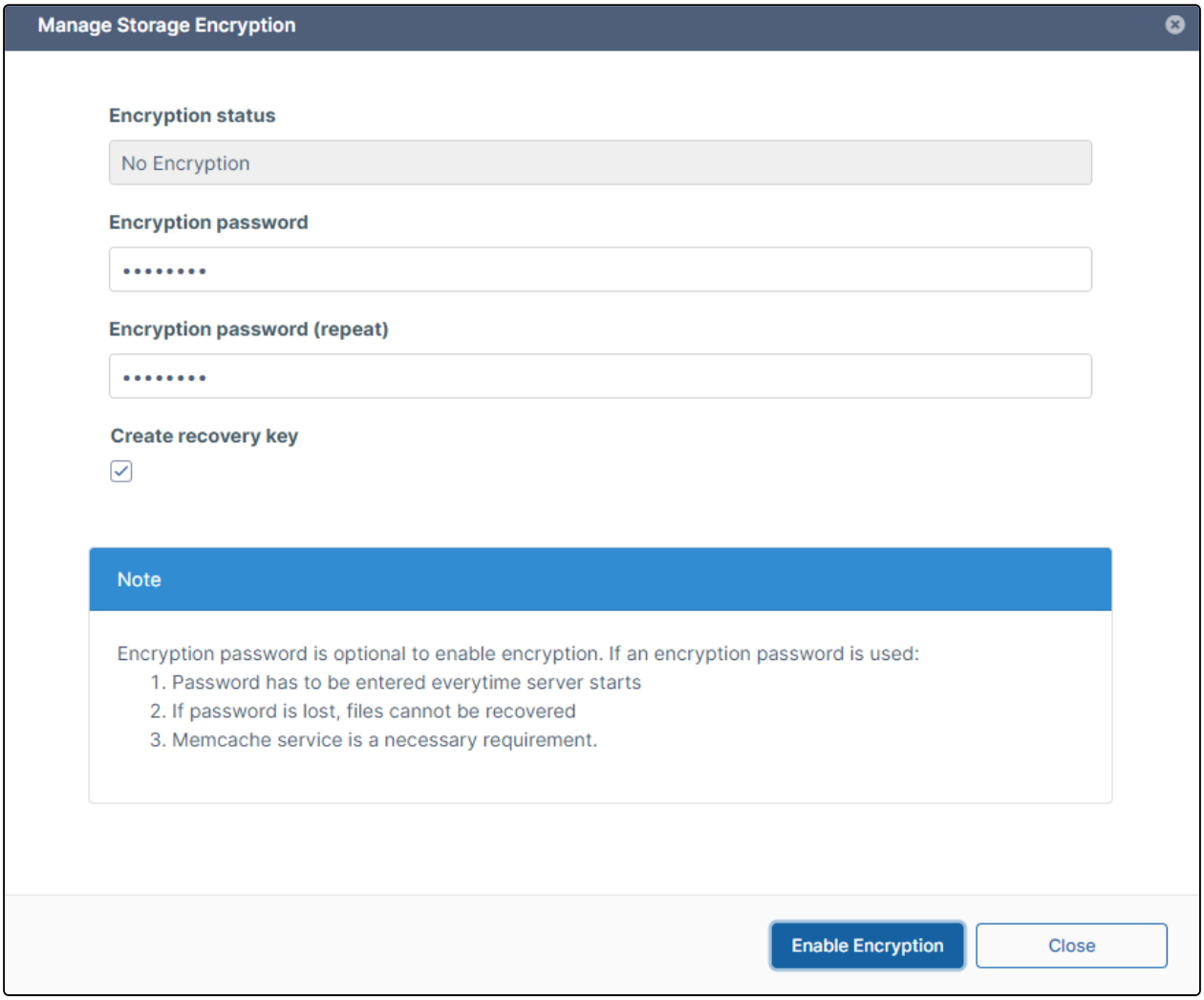


You can reactivate the storage system using the encryption password or the recovery key.

Activating with password and recovery key

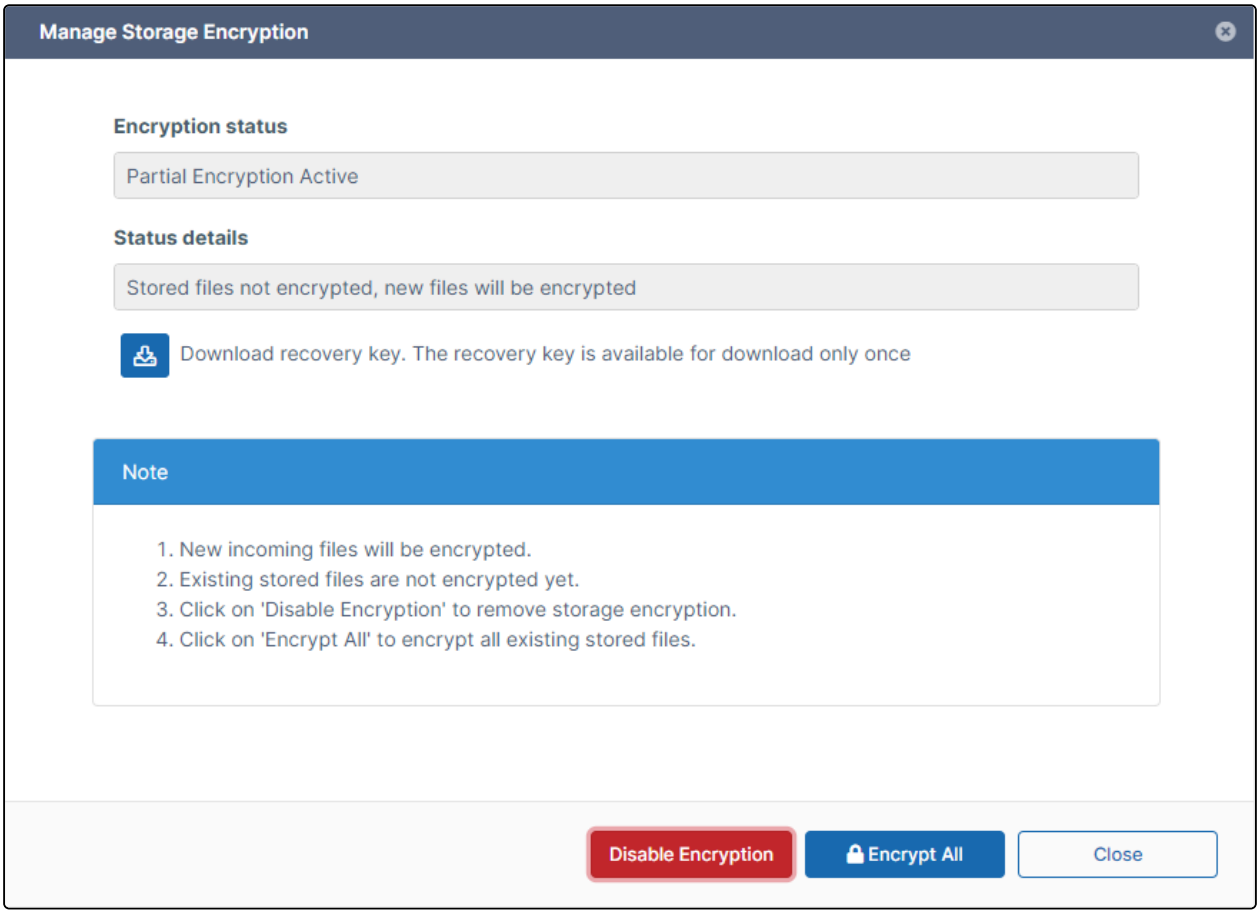
1. Enter the encryption password, in **Encryption password** and **Encryption password (repeat)**.
2. Check **Create recovery key**.

3. Click **Enable Encryption**.



The following screen appears.

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



5. Click **Encrypt All**.

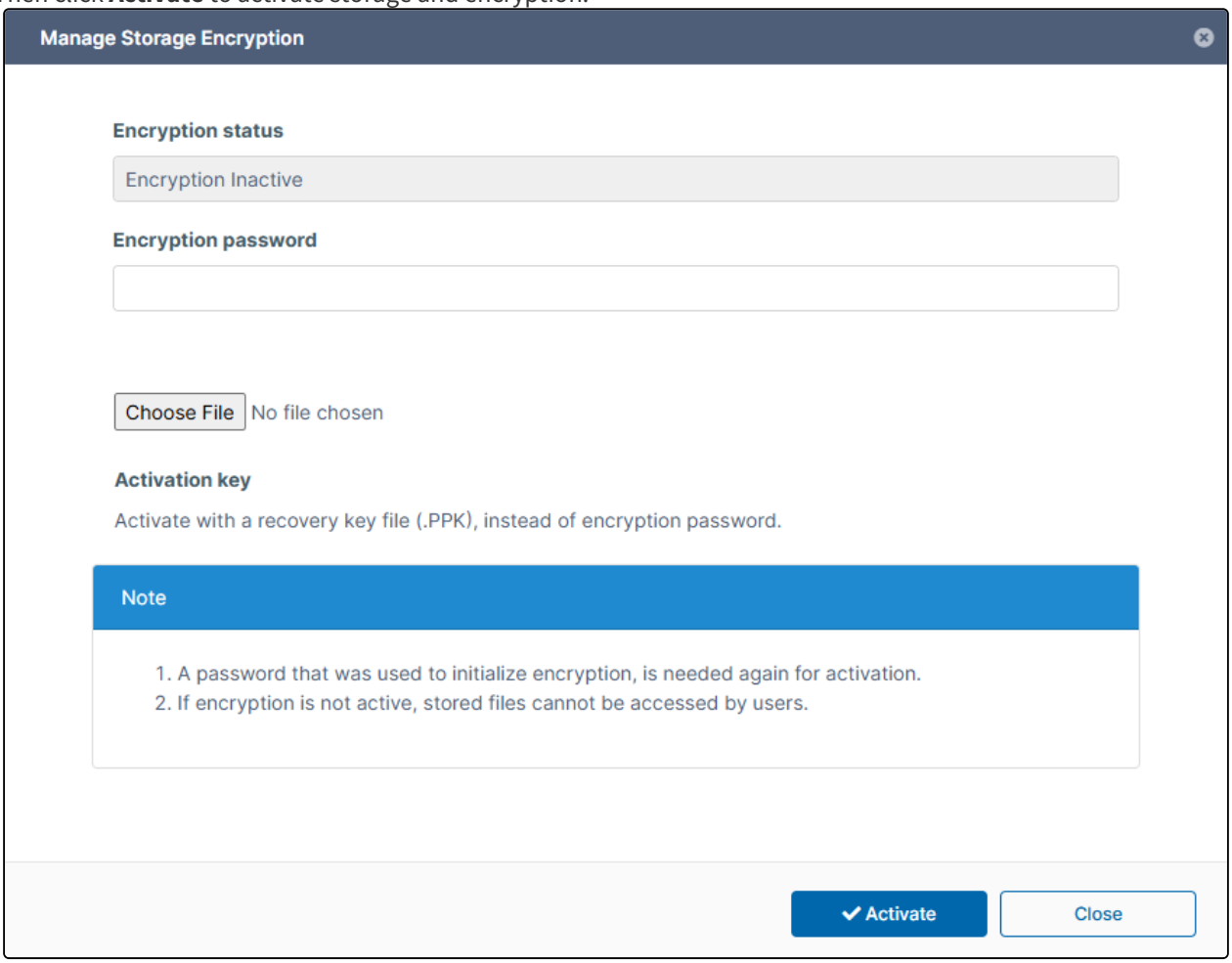
Activating With Recovery Key

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

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

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

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



Activating Encrypted Protected Storage From Command Line

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

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

To enable storage encryption:

1. Encryption Pre-Requisites

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

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

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

2. Manage Storage Encryption

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

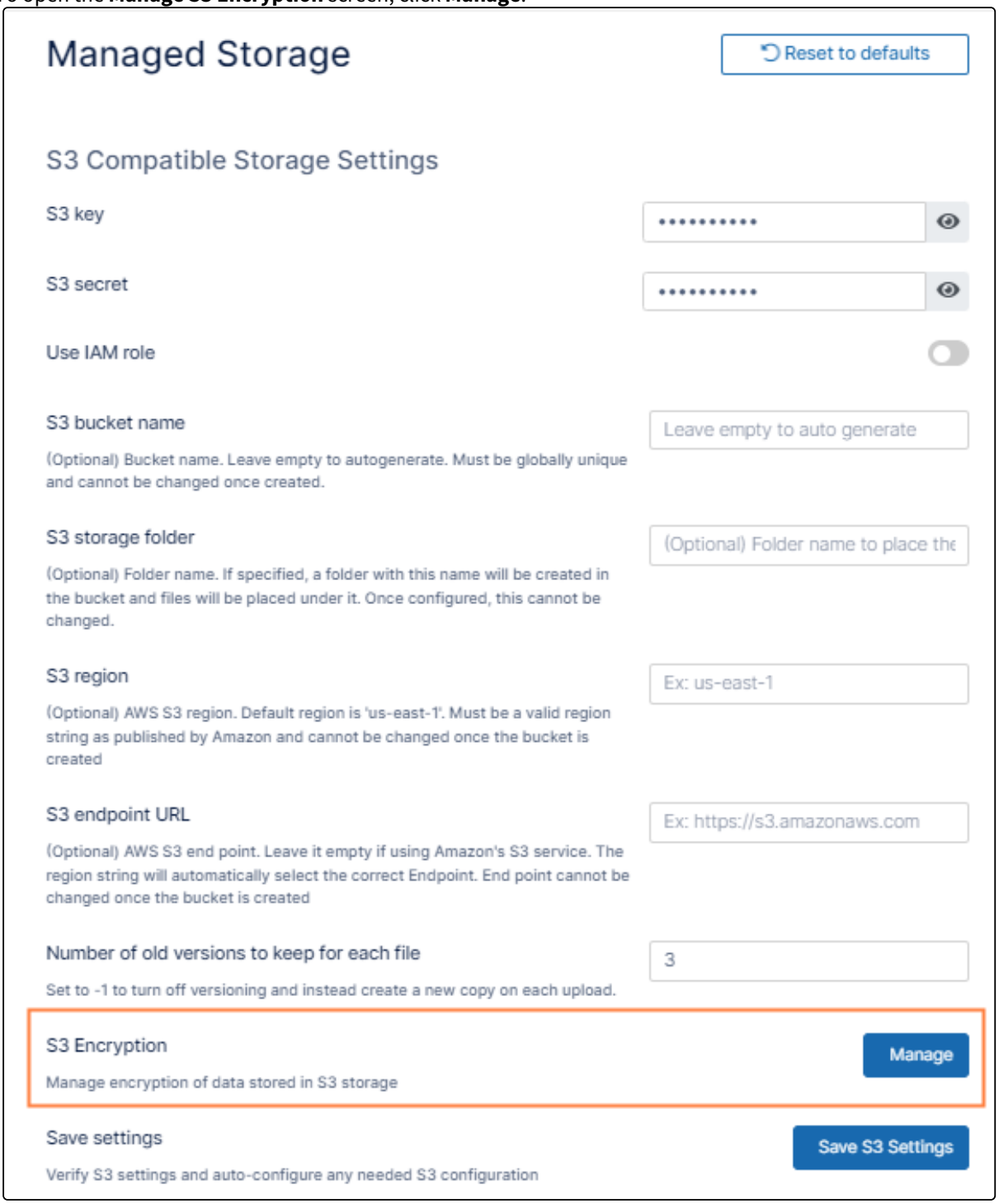
Warning On Master Password

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

To manage S3 encryption:

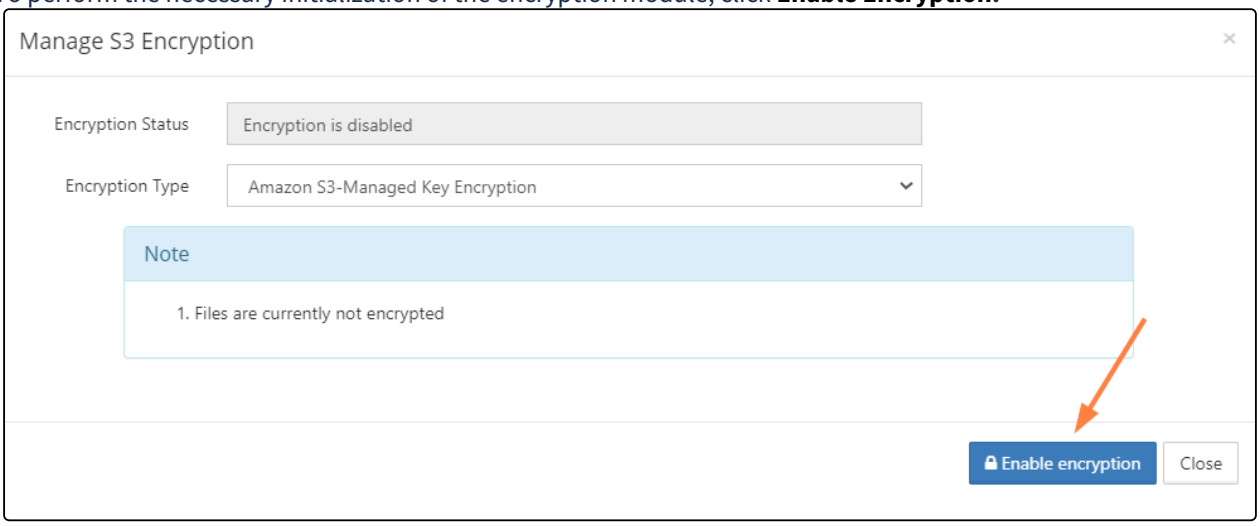
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The Managed Storage settings page opens. An **S3 Encryption** field with a **Manage** button appears.

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



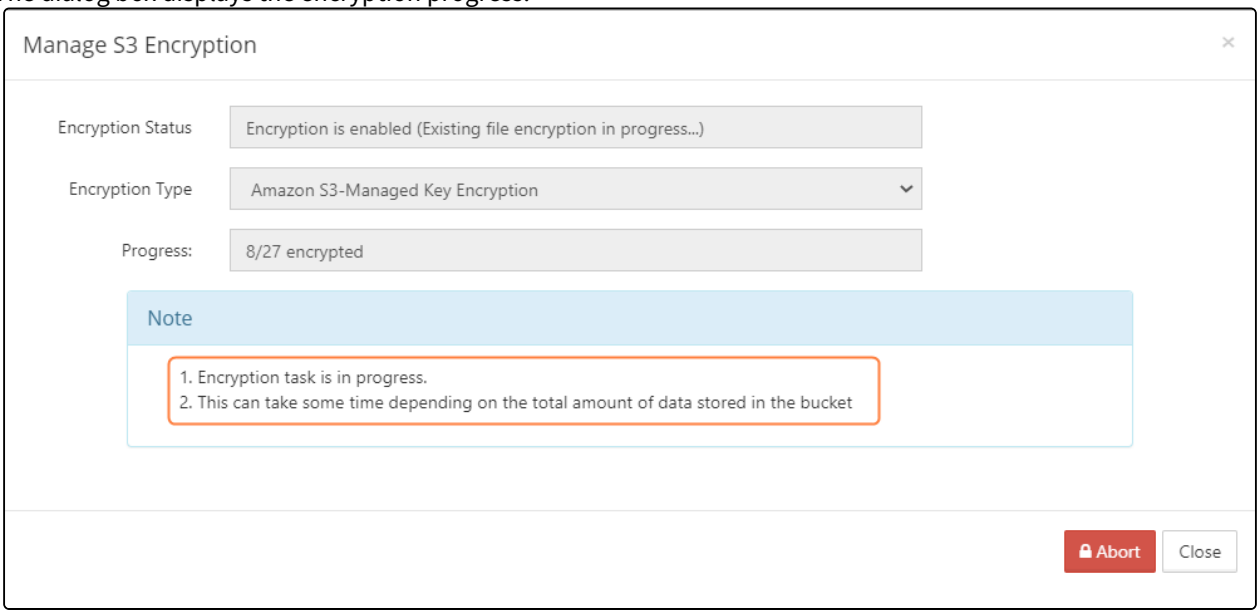
The **Manage S3 Encryption** dialog box opens:

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

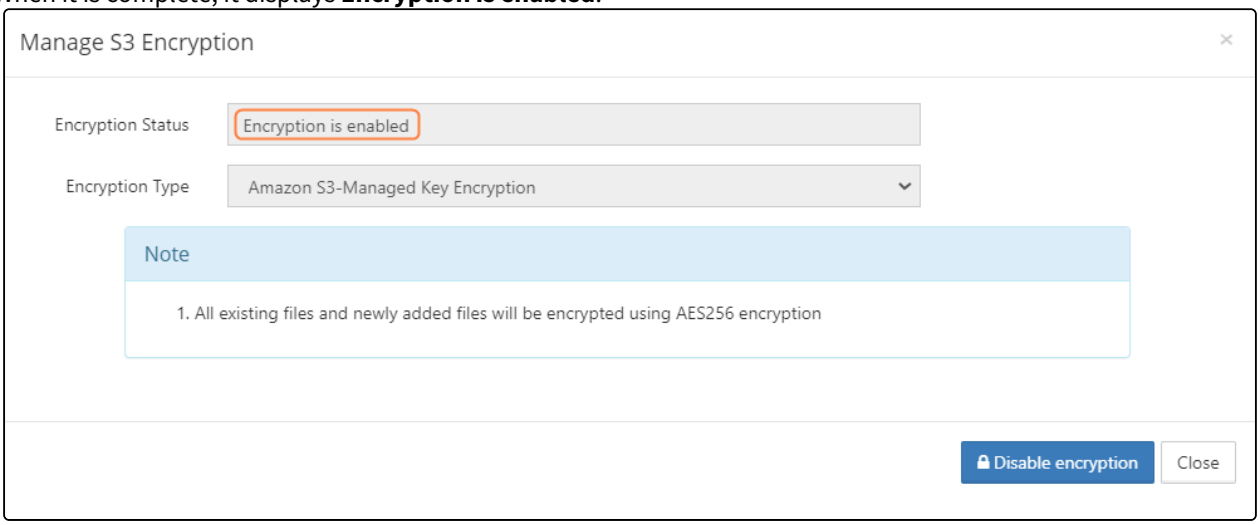


You are prompted to confirm encryption.

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



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



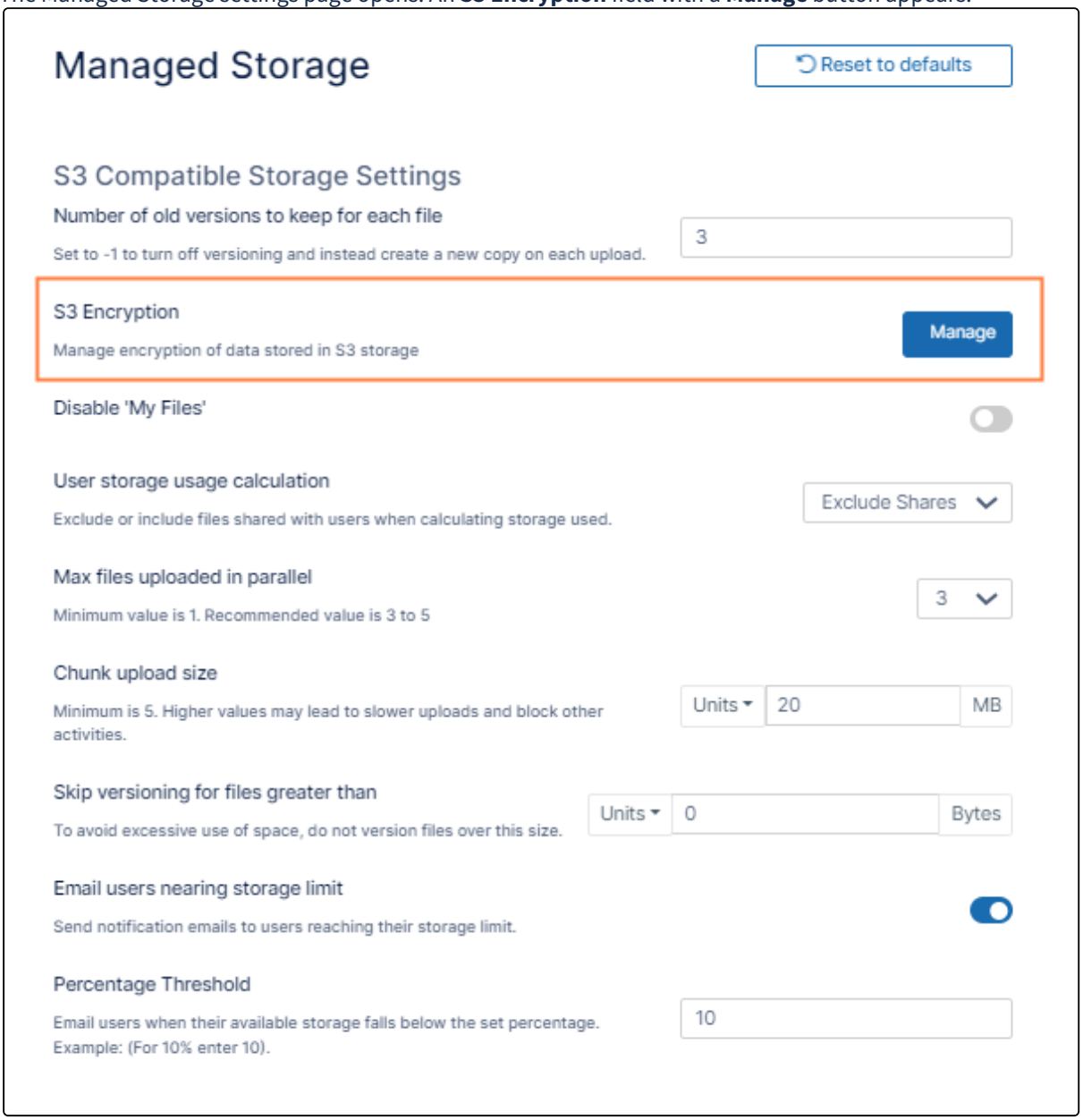
Disabling S3 Storage Encryption

Administrators can disable S3 storage encryption following the steps here.

To disable S3 encryption:

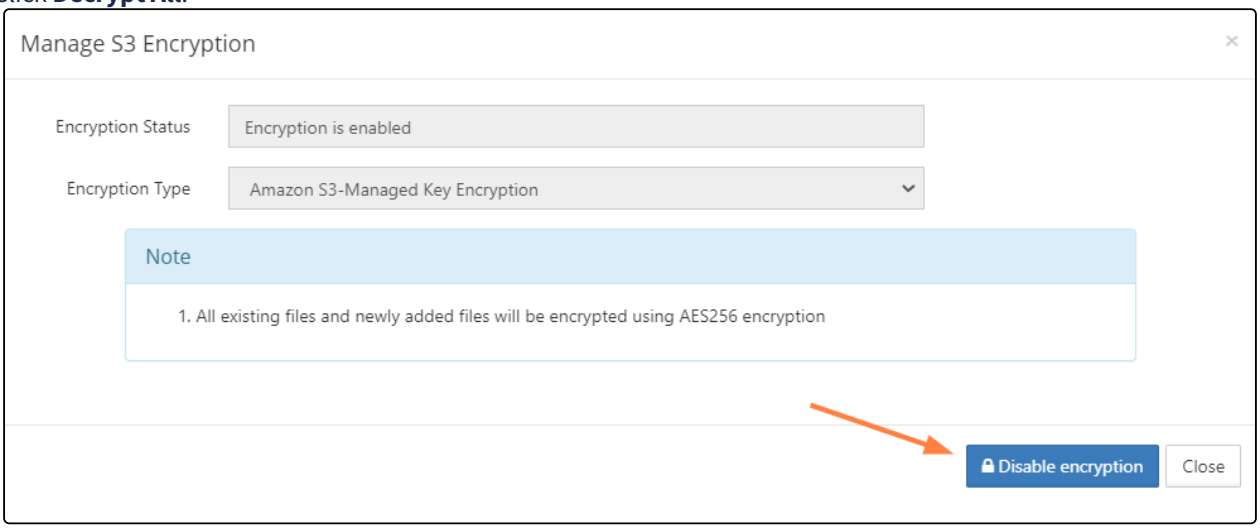
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .

The Managed Storage settings page opens. An **S3 Encryption** field with a **Manage** button appears.



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

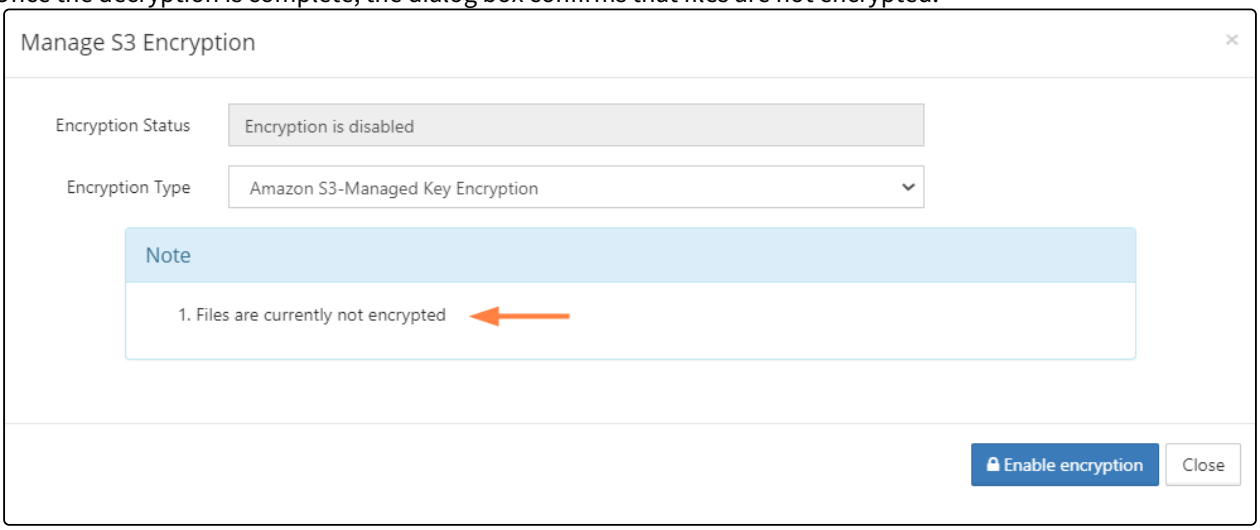
3. Click **Decrypt All**.



You are prompted to confirm disabling encryption.

4. Click **OK**.

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



Choosing S3 Encryption Type

When you 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 types:

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

WARNINGS:

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

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

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

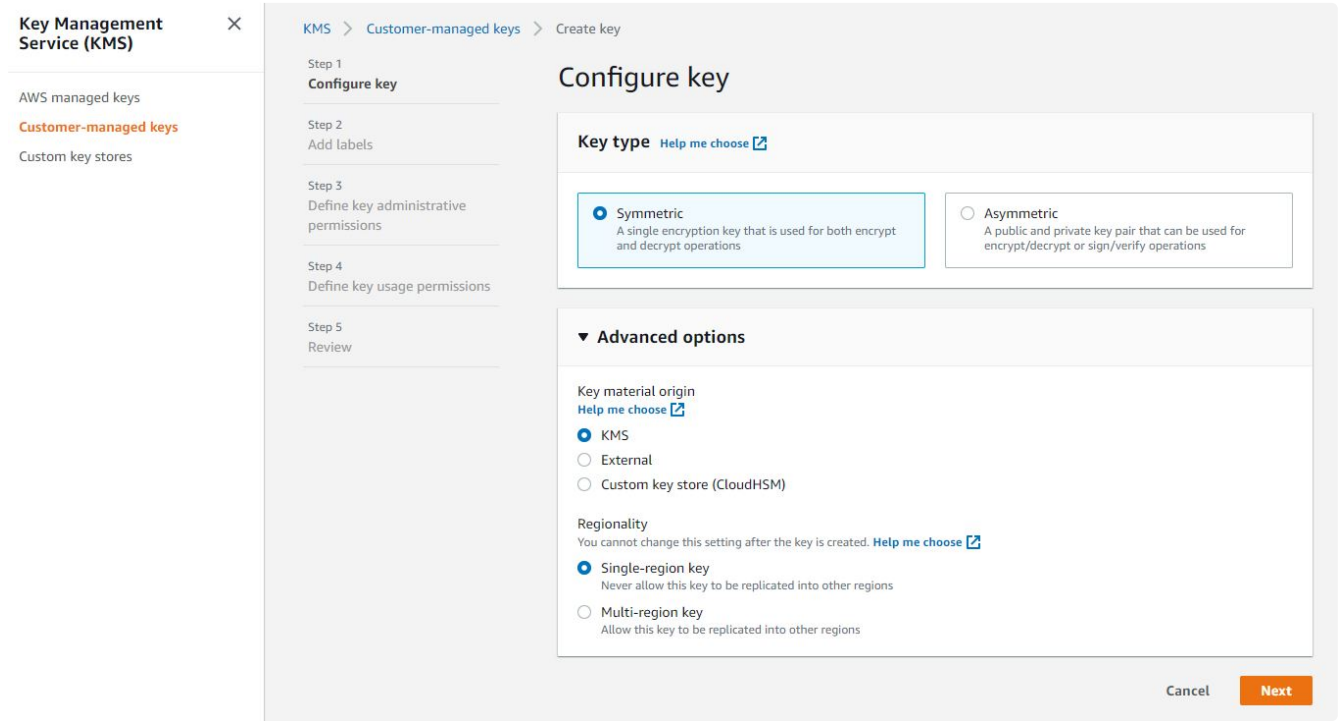
- A Symmetric Customer Managed Key created on an AWS account which will hold the key for encryption. Let's say for example, this account is called, **KMS Account**.
- Key Policy added to the above created key on KMS Account, which gives access to the other AWS account, let's say for example, this account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

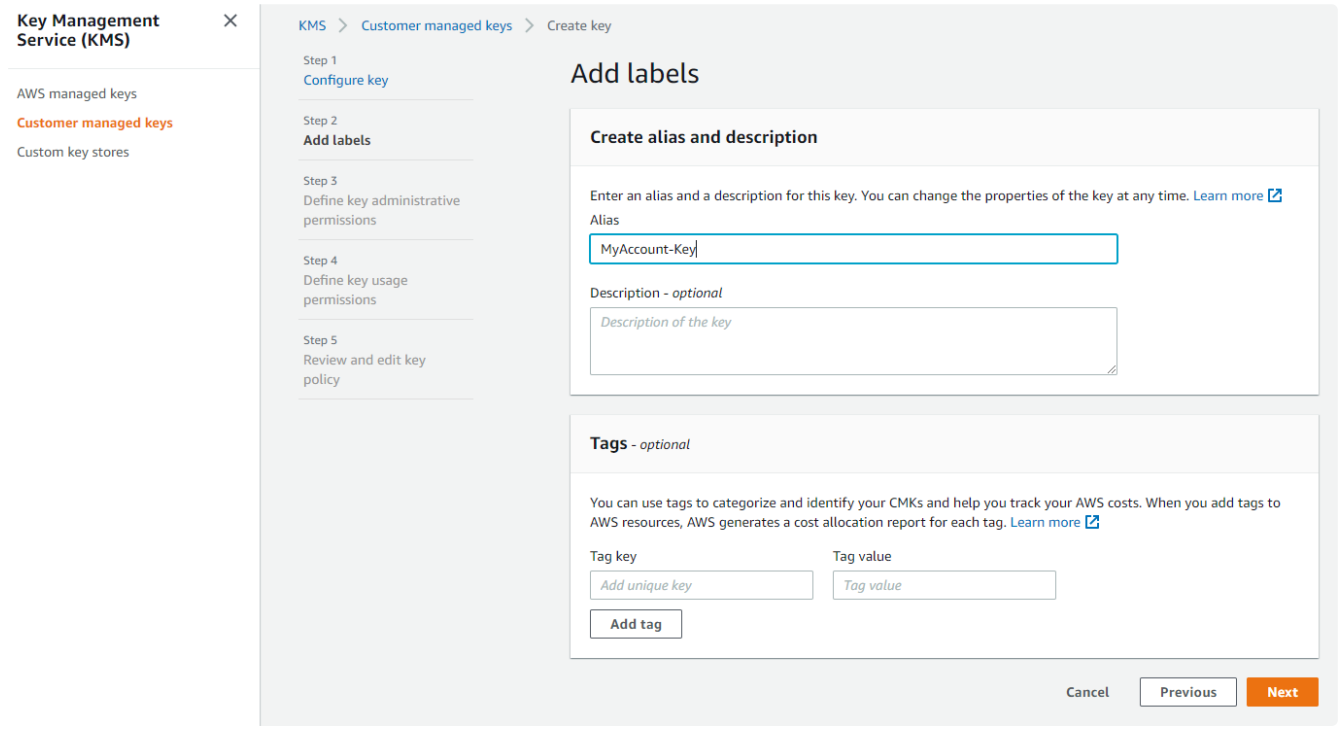
Configuring S3 Storage Encryption with AWS cross-account KMS key

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

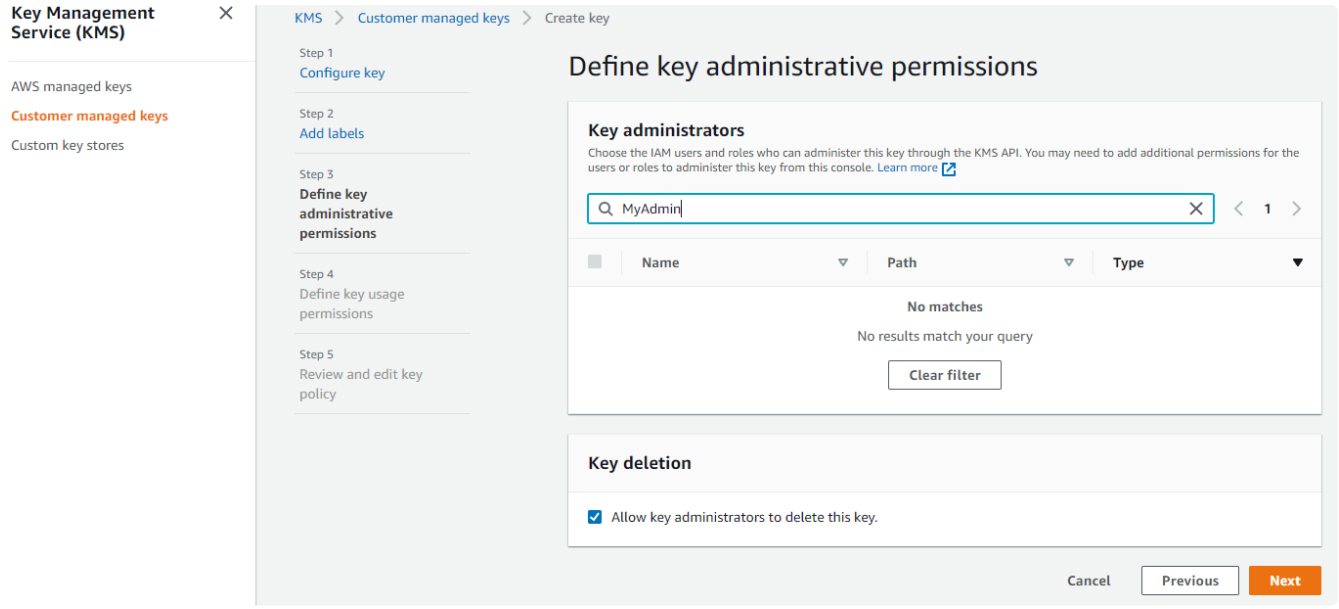
1) From AWS Console, navigate to KMS > Customer Managed Keys and click on "Create Key". Choose the default options as in below screenshot and click on 'Next'.



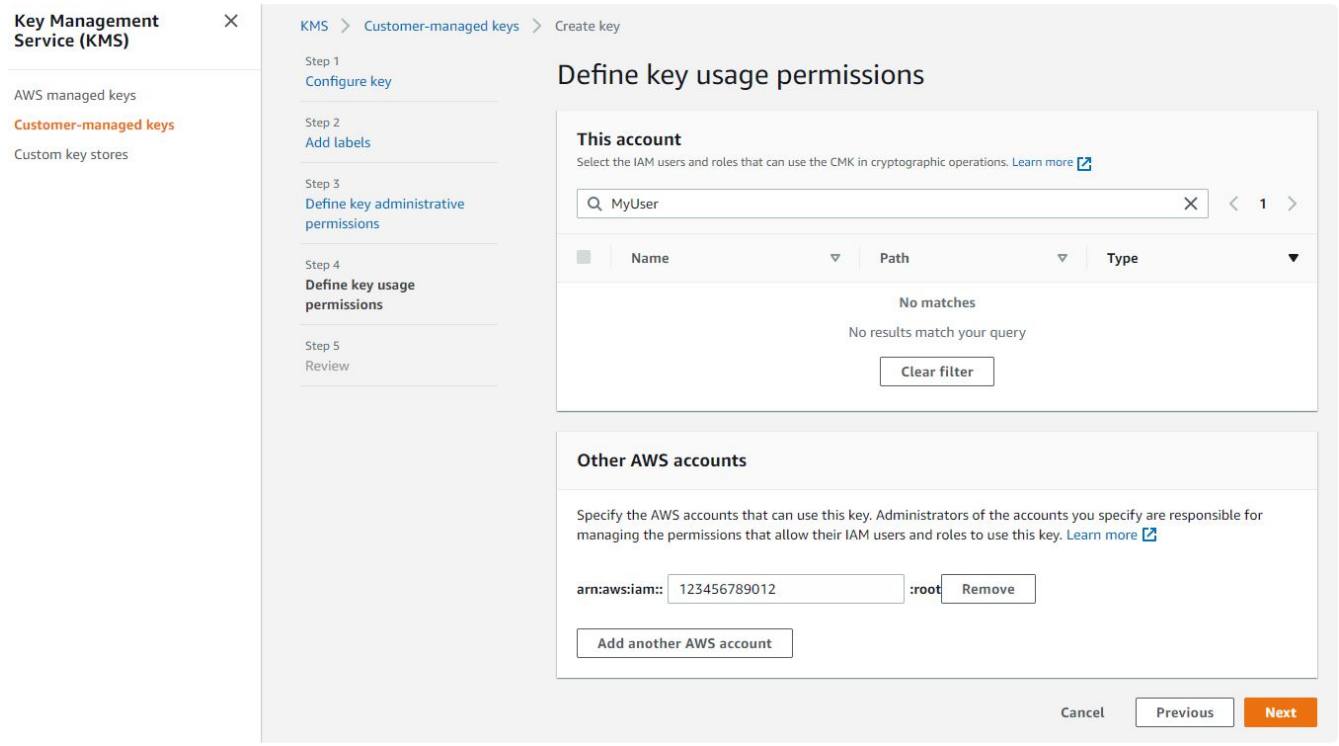
2) Provide an Alias or Name for the key and click on 'Next'.



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



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



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

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

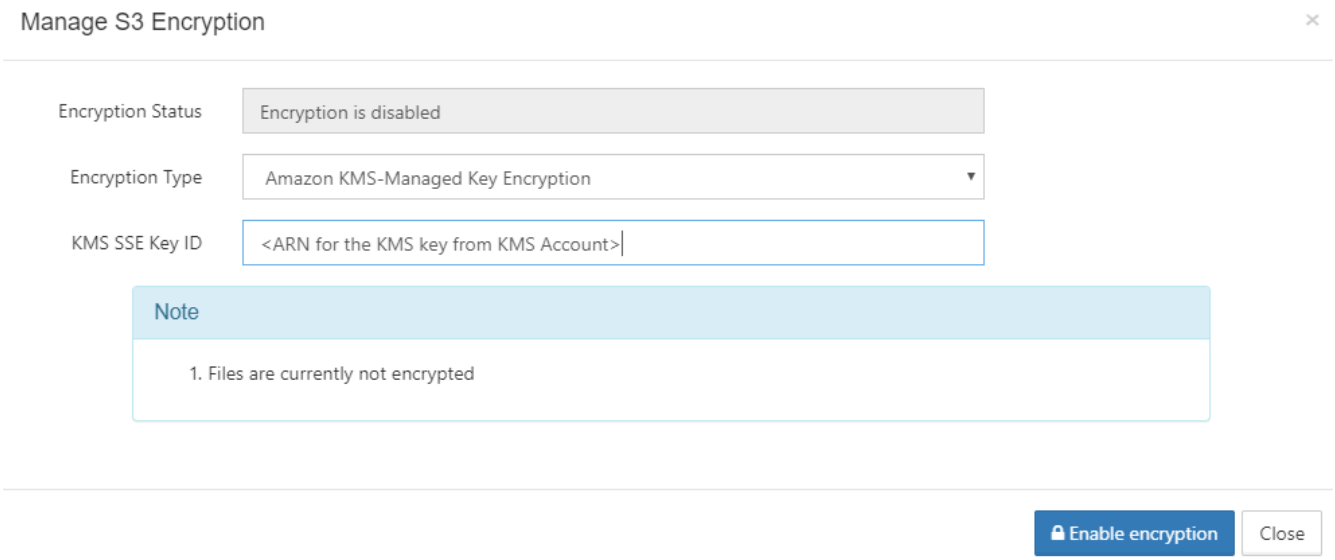
```
            ],
            "Resource": "*"
        }
    ]
}
```

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

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

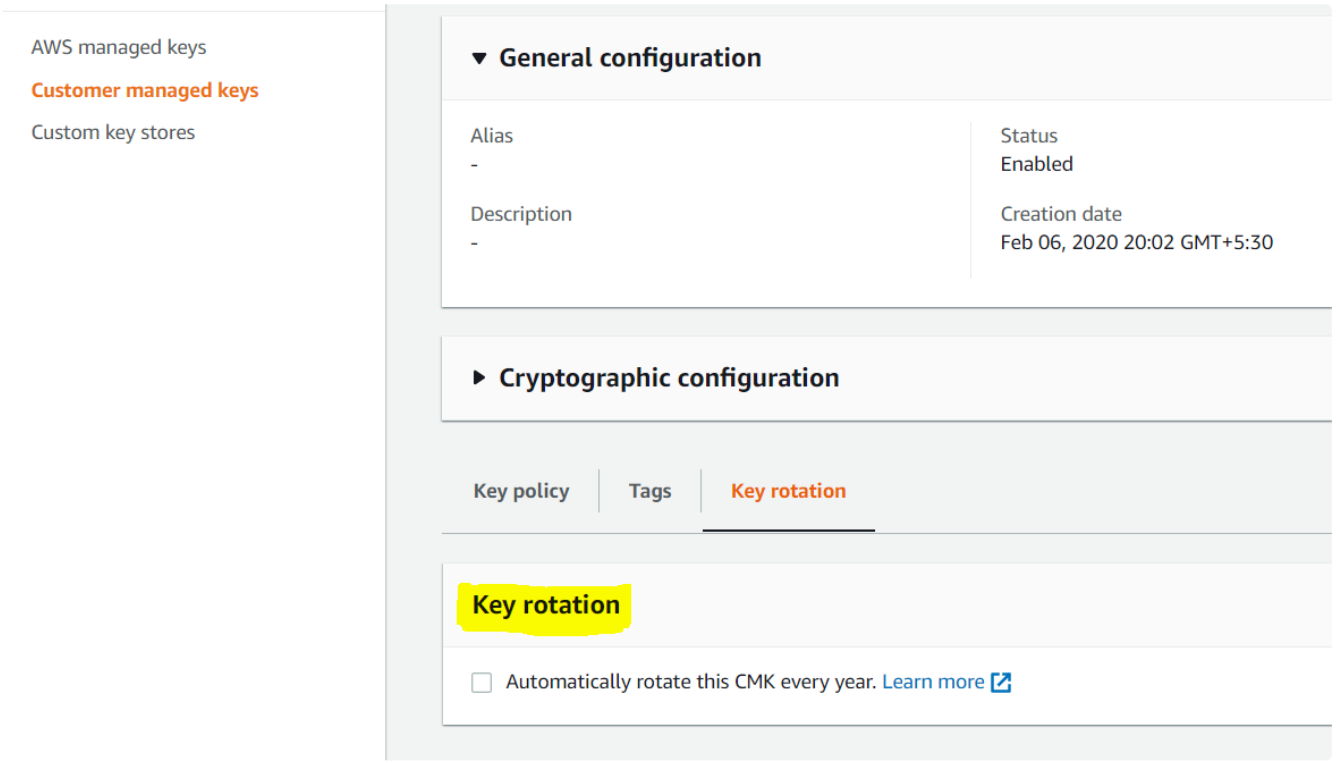
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CMK",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"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

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



Rotating AWS Customer Managed Keys

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



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

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

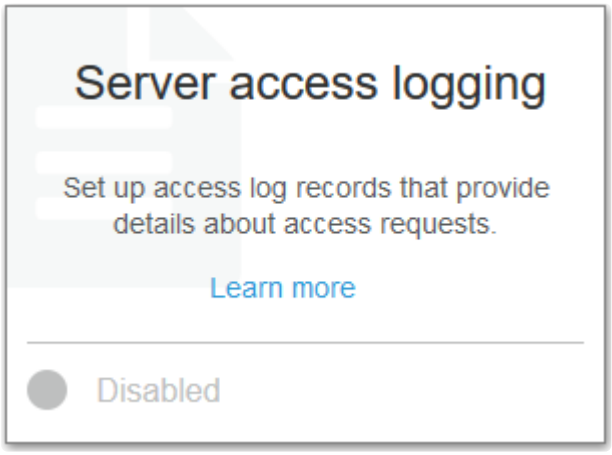
NOTE : Manual key rotation is not supported by FileCloud.

Enabling access logging for an S3 bucket

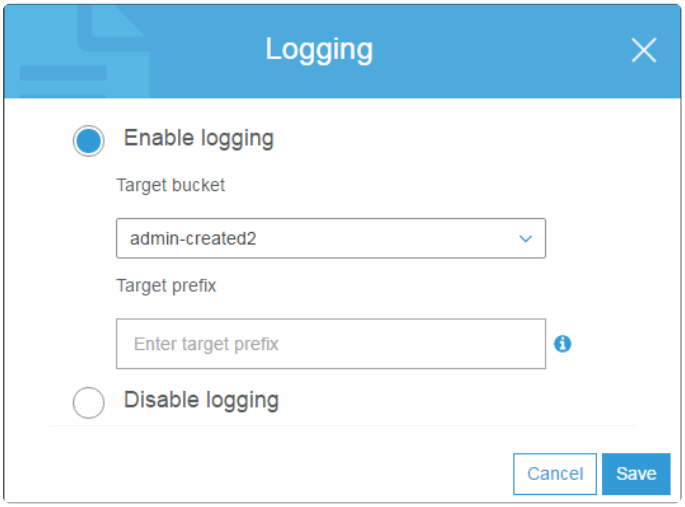
1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the **Bucket name** list, choose the name of the bucket that you want to enable server access logging for.

3. Choose **Properties**.

4. Choose **Server access logging**.



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



6. (Optional) For **Target prefix**, type a key name prefix for log objects, so that all of the log object names begin with the same string.
7. Choose **Save**.
   You can view the logs in the target bucket. If you specified a prefix, the prefix shows as a folder in the target bucket in the console. After you enable server access logging, it might take a few hours before the logs are delivered to the target bucket.

Setting Up MongoDB Enterprise Advanced Server

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

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

Install MongoDB Enterprise Advanced

Installing on Ubuntu

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

```
sudo apt-get install gnupg curl

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

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

   --dearmor
```

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

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

4. Reload the local package database:

```
sudo apt-get update
```

5. Install MongoDB Enterprise Advanced:

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

Installing on RHEL

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

```
[mongodb-enterprise-6.0]

name=MongoDB Enterprise Repository

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

gpgcheck=1

enabled=1

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

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

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

Configure the connection to FileCloud for Ubuntu or RHEL

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

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

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

```
mongosh private_ip
```

   Then create the user:

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

   Finally, verify the connection from the FileCloud server:

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

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

```
// ... Cloud Database

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

```
// ... Audit Database

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

// … Settings Database

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

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

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

Installing on Windows

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

Configure the connection to FileCloud for Windows

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

```
bindip: 127.0.0.1
```

   to

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

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

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

   Connect to the mongo shell.

```
mongosh private_ip
```

4. Switch to the admin user:

```
use admin
```

5. Create a new db user:

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

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

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

7. From the FileCloud server, verify the connection:

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

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

```
// ... Cloud Database

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

// ... Audit Database

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

// … Settings Database

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

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

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

Manage the Recycle Bin Using Policies

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

Why?

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

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

Do you want to store deleted files for recovery purposes?

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

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

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

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

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

This is configured by the setting called:

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

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

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

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

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

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

This is configured in the following setting:

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

Files less than this size are stored

Files greater than this size are permanently deleted

You can specify the file size in the following ways:

- GB
- MB
- KB
- B

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

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

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

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

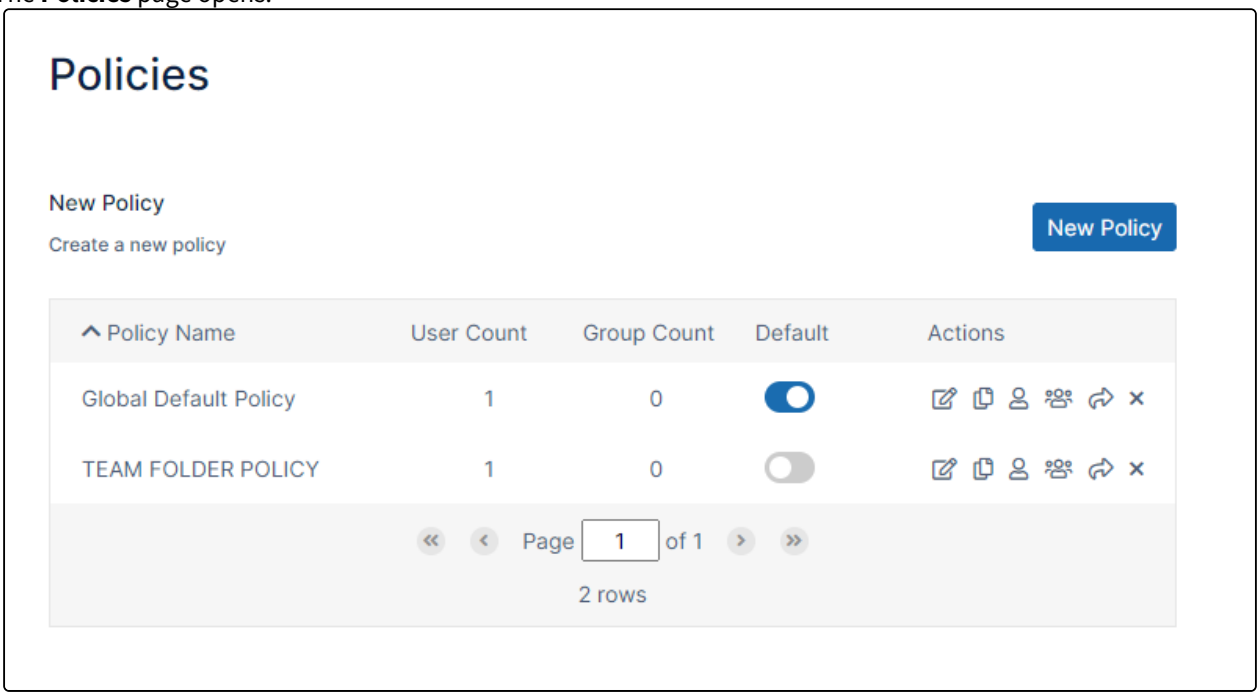
Setting	Option	Description
Store deleted files in the recycle bin	yes or no	Move the file from it's location in My Files to the recycle bin when the user deletes it
Automatically delete files from recycle bin after set number of days	Whole number	Number of days after a file was deleted that it will be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

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

To configure a recycle bin policy for users or groups:

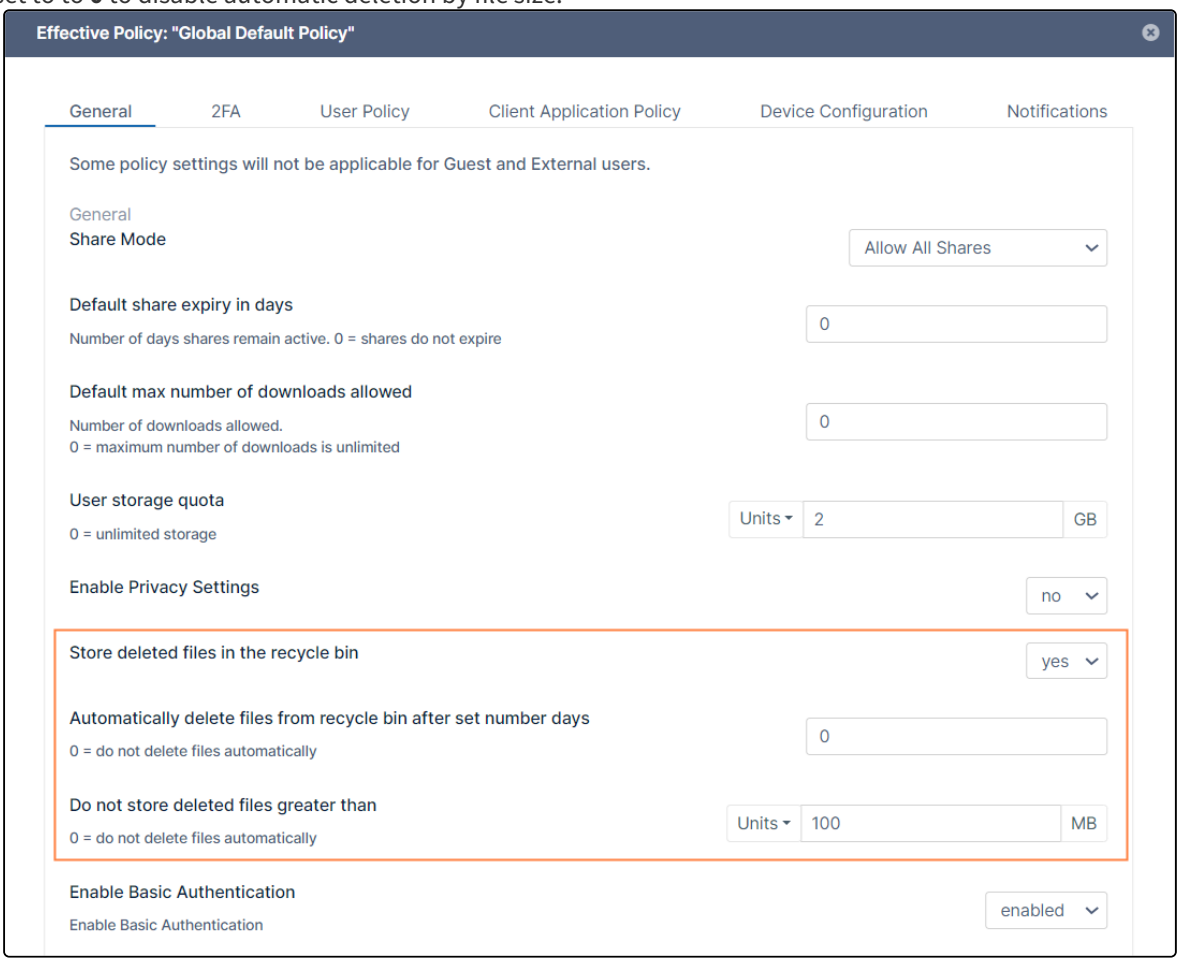
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .

The **Policies** page opens.



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

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



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

Disable My Files

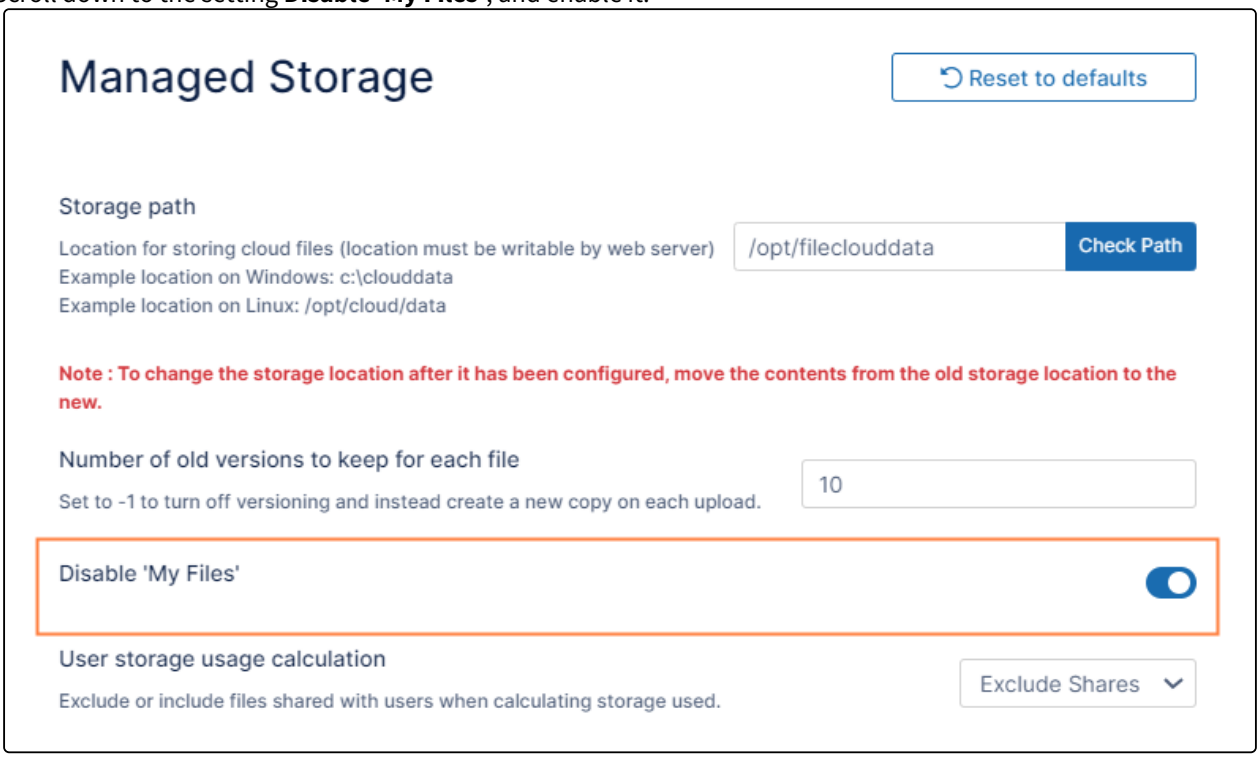
My Files can be disabled completely if users need to access only Network Folders, Team Folders or shared data.

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

To disable My Files:

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

2. Scroll down to the setting **Disable 'My Files'**, and enable it.



3. Click **Save.**

Manually Clearing Large Recycle Bins

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

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

- 100K of files
- 1000 folders

Why?

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

To manually clear an overfilled recycle bin:

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

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

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

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

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

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

Embedded File Upload Website Form

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

Step 1:

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

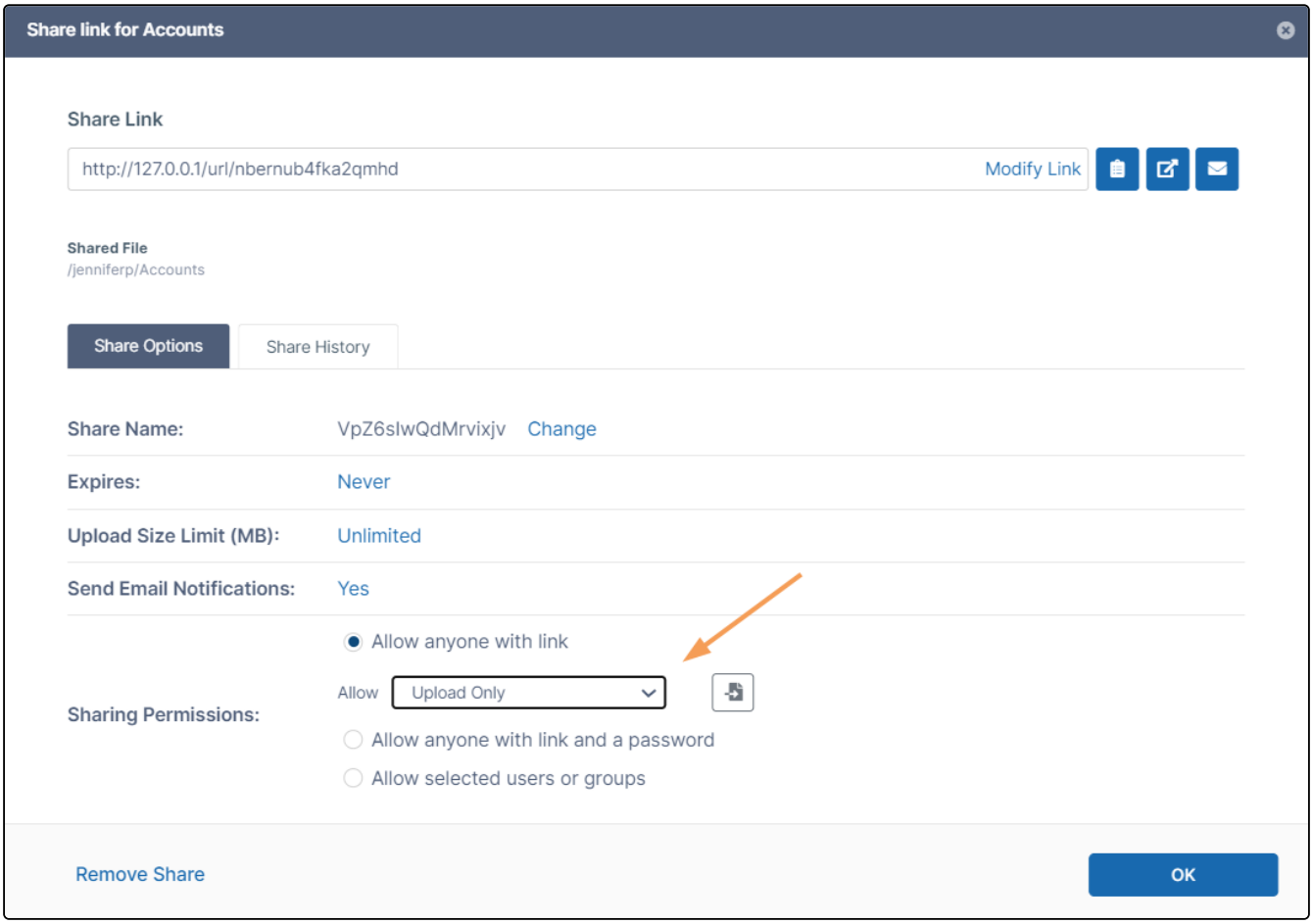
```
<IfModule mod_headers.c>
Header set X-Frame-Options "SAMEORIGIN"
</IfModule>
```

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

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

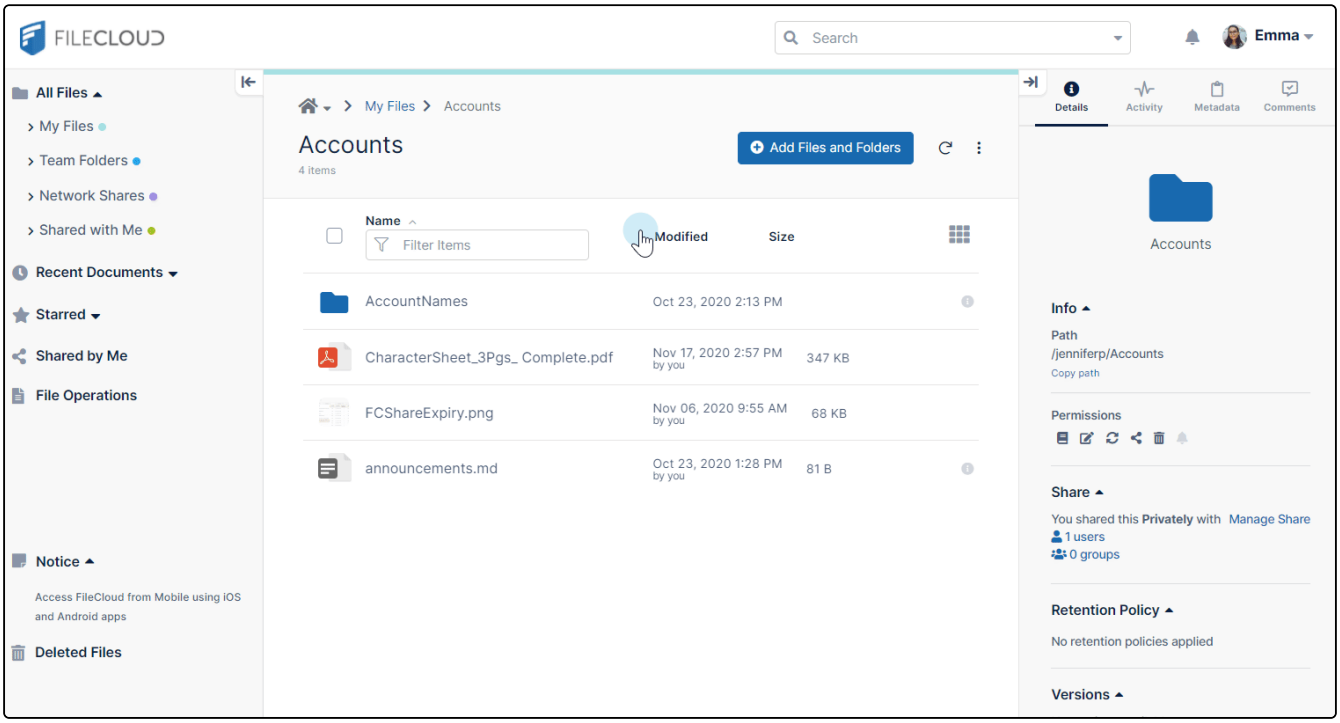
Step 2:

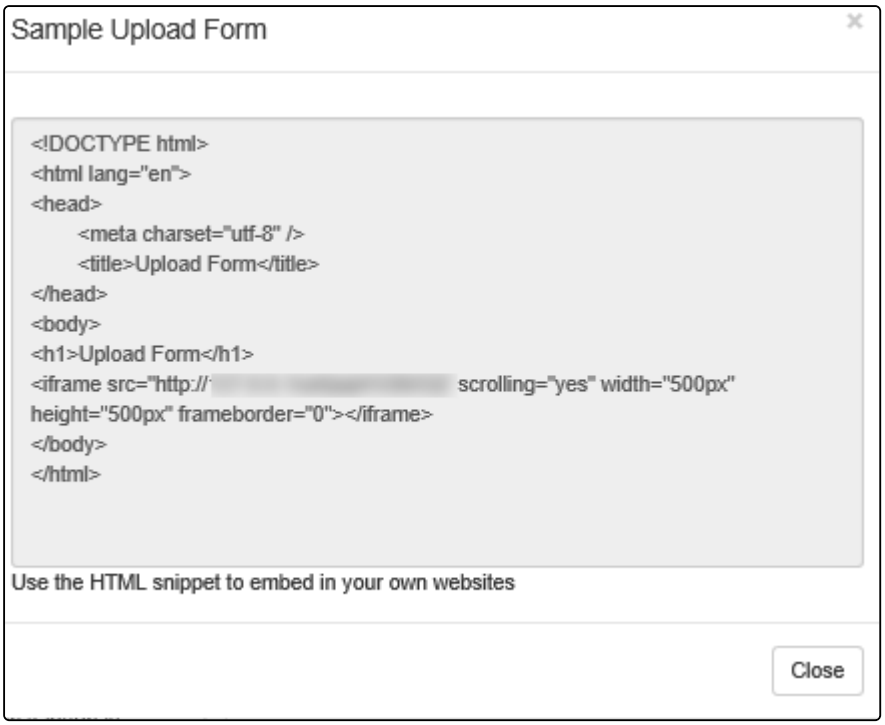
Create a public share for a folder and set Share Permissions to Allow Everyone with **Upload Only**.



Step 3:

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

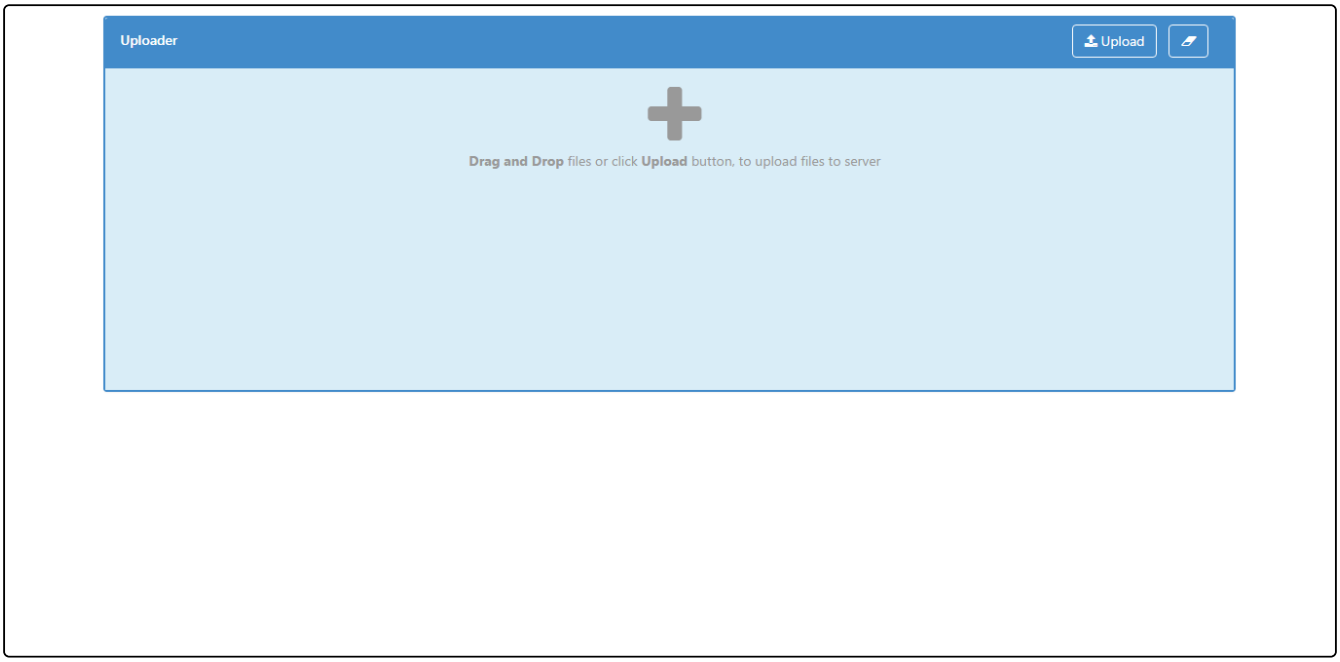




Step 4:

Embed the form in your existing web page or website.

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



Restrict a User's Recycle Bin Options

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

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

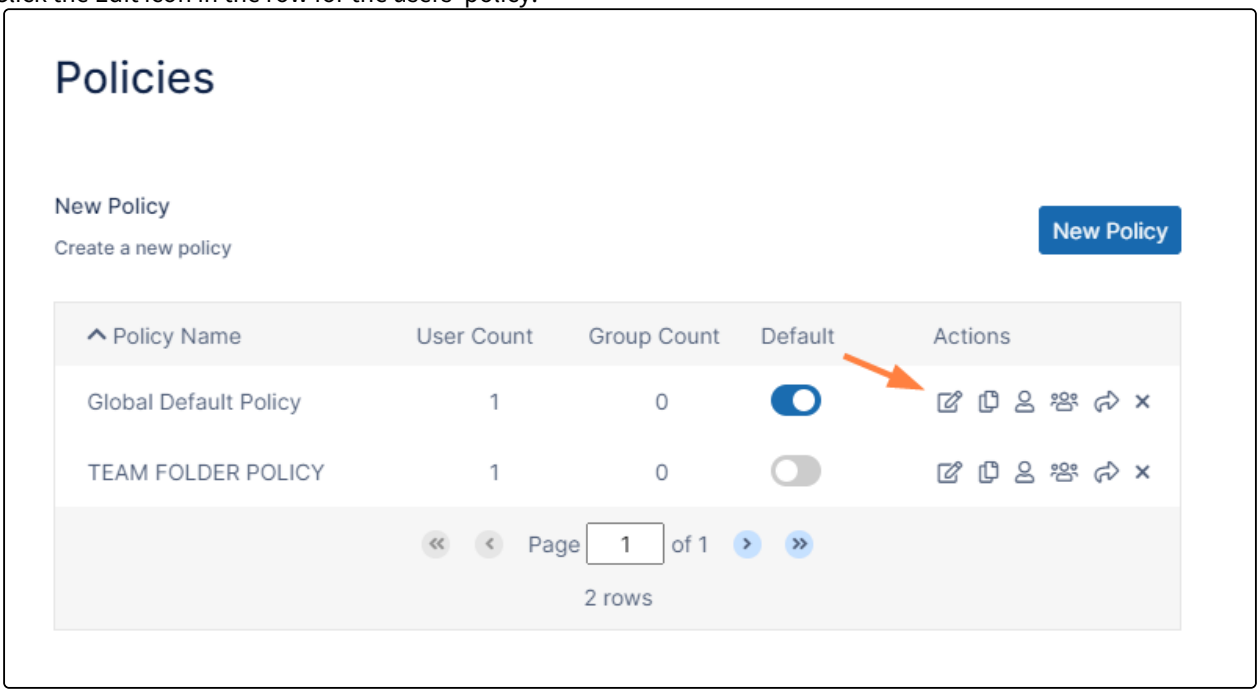
If **Enable recycle bin clearing** is disabled in a policy, users belonging to the policy do not see a **Clear Deleted Files** button in the recycle bin.

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

To enable or disable recycle bin clearing:

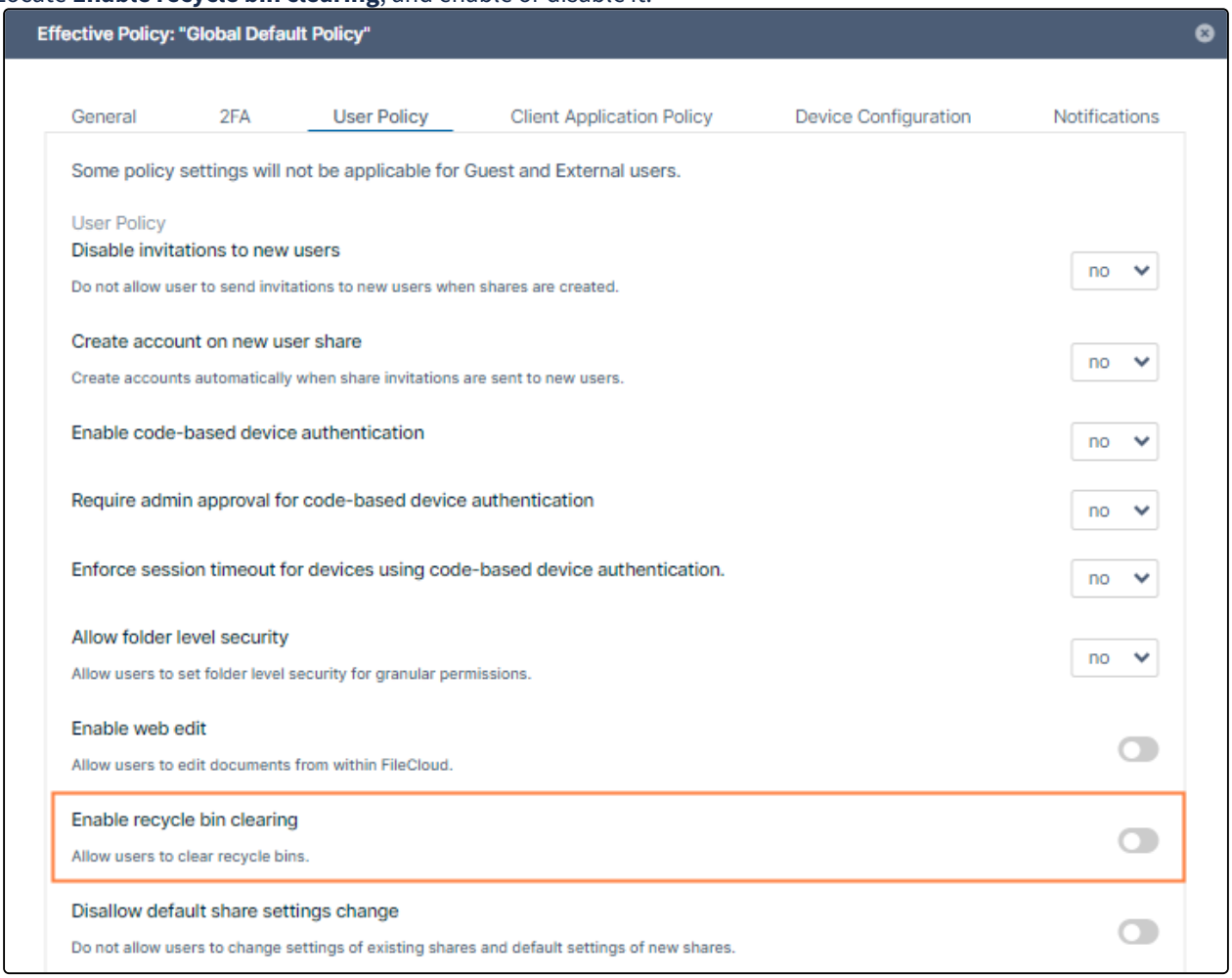
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.

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



3. The **Policy Settings** dialog box opens.
4. Click the **User Policy** tab.

5. Locate **Enable recycle bin clearing**, and enable or disable it.



6. Click **Save**.

Setting up FileCloud Managed Azure Blob Storage

As an administrator, you can integrate FileCloud Server to store user data 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
c:\xampp\htdocs	**/var/www/html**

To enable Azure Blob storage as the backend:

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

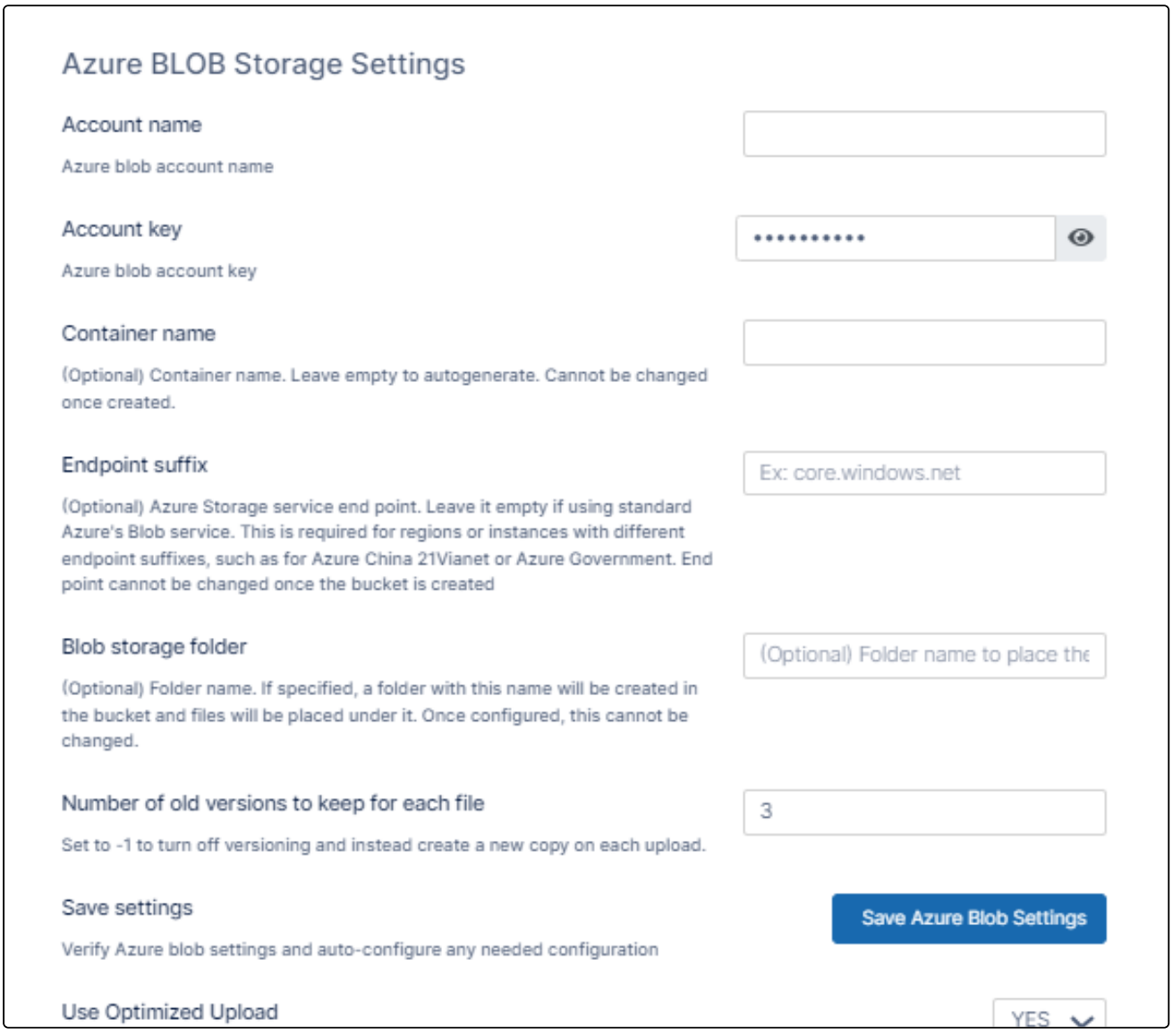
💡 Nothing needs to be added or edited in **azureblobstorageconfig.php**

2. Configure Credentials

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

To configure Azure Blob storage Credentials:

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



Field	Description
Account Name	This is your Azure storage account name. For an RBAC user, it requires at least the following permissions.
Account Key	This is your Azure storage account key (To get your account key, visit Amazon security portal). For an RBAC user, it requires at least the following permissions.
Container Name	Provide a storage container name. The container should be new (in some circumstances, containers previously used in FileCloud could be used). It is very important that the Azure storage container is never modified outside of the FileCloud subsystem. **Container name rules** • The name of the container has to be unique and follow the naming rules. • If 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.
Endpoint Suffix	Optional: This is the Azure Blob storage endpoint. • Use this to specify your own Azure storage endpoint (typically Azure-compatible storage) • Use this if it is an unpublished region. To use an Azure endpoint, it must be one of the values published here. • **Note: For govcloud installs, you must use the following endpoint suffix: blob.core.usgovcloudapi.net**
Blob Storage Folder	Optional: All files will be stored inside this root storage folder. • This folder will be created automatically.
Number of old versions to keep for each file	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to 0. **NOTE**: Versioned files count towards the user's storage quota.

3. Data Encryption

Encryption at rest

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

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

Troubleshooting

Using Override Configuration Keys

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

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

How to Correct Issues with Image Previews

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

To add the domain to the .htaccess file:

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

2. Locate the following line and add the domain ***.core.windows.net** to the locations shown in the example below. The first instance may already be included.

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

Setting Up Network Folders

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

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

Can I also configure the FileCloud Server site storage?

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

FileCloud Managed Storage

In this section:

- 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
- Oracle Cloud Infrastructure S3 Bucket Based Network Folders
- Storj S3 Bucket Based Network Folders

FileCloud Blogs

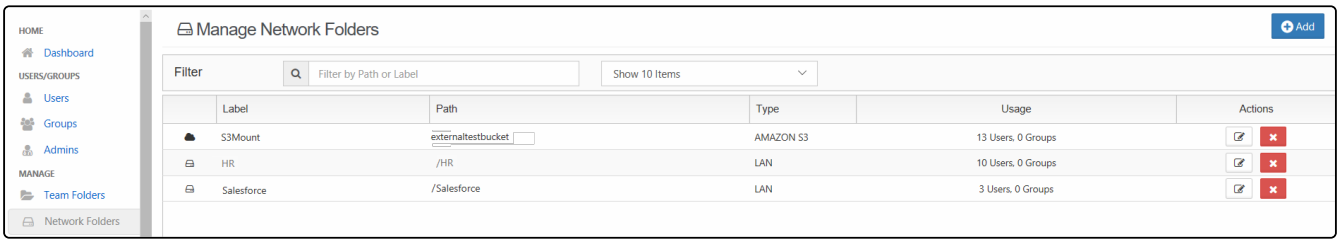
- Connect Your SFTP to FileCloud

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



In this section:

Create a LAN-Based Network Folder

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

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

Block locations from mounting as share paths

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

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

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

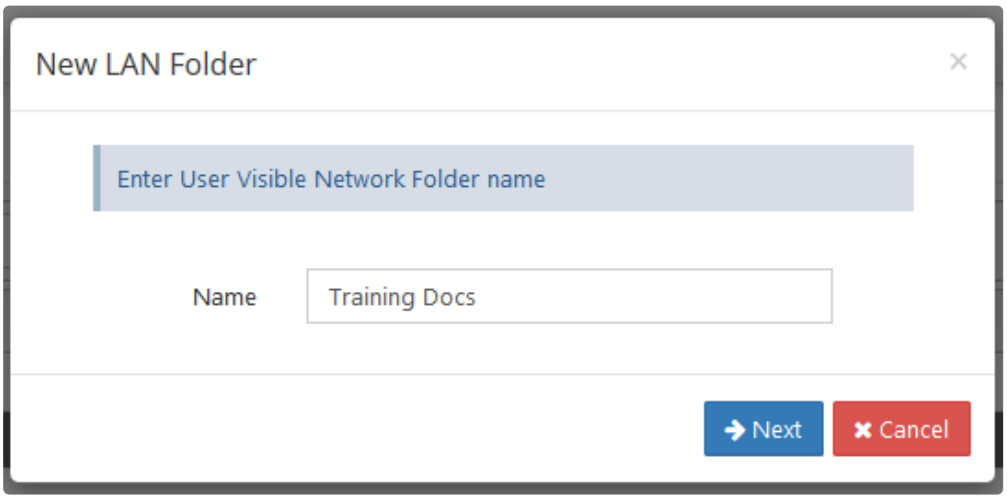
```
define("TONIDOCLOUD_NETWORK_FOLDER_MOUNT_PATH_BLOCK_LIST", 'C:/xampp|c$/xampp,C:/
PatientRecords');
```

Create a Network Folder

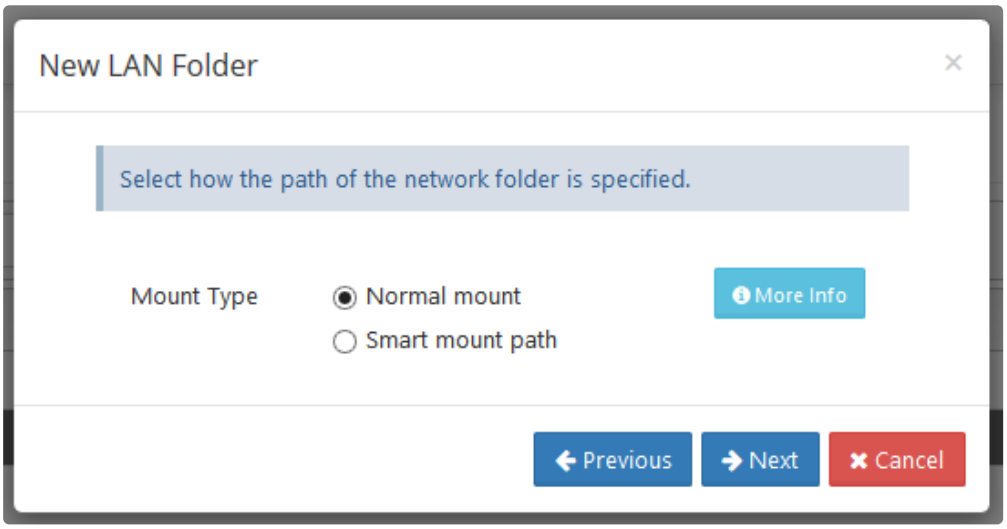
To create a Network Folder:

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.

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.



6. Select whether you want to use Normal mount paths or Smart mount paths. Read more about Smart mounts.

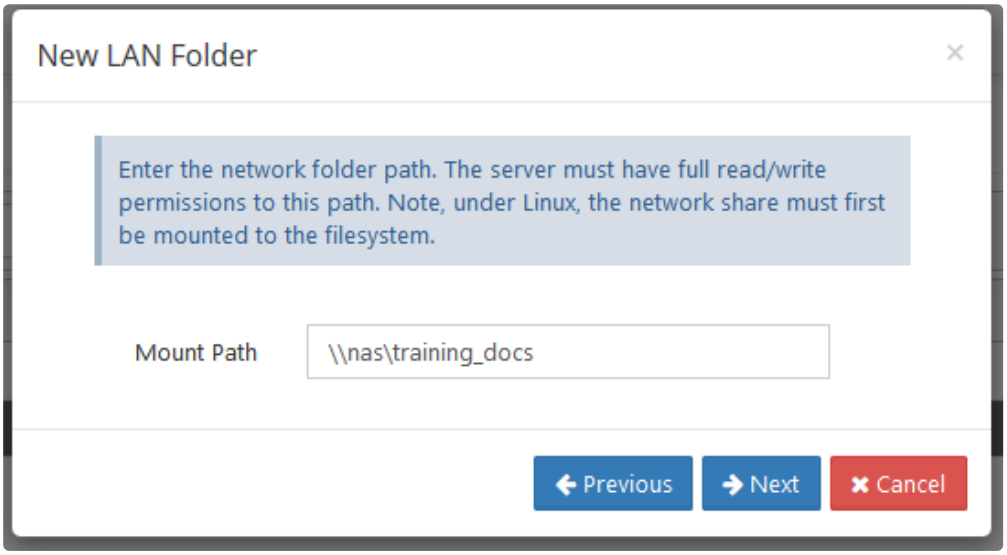


7. For Normal mount paths: select the remote folder to use as the network share

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

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

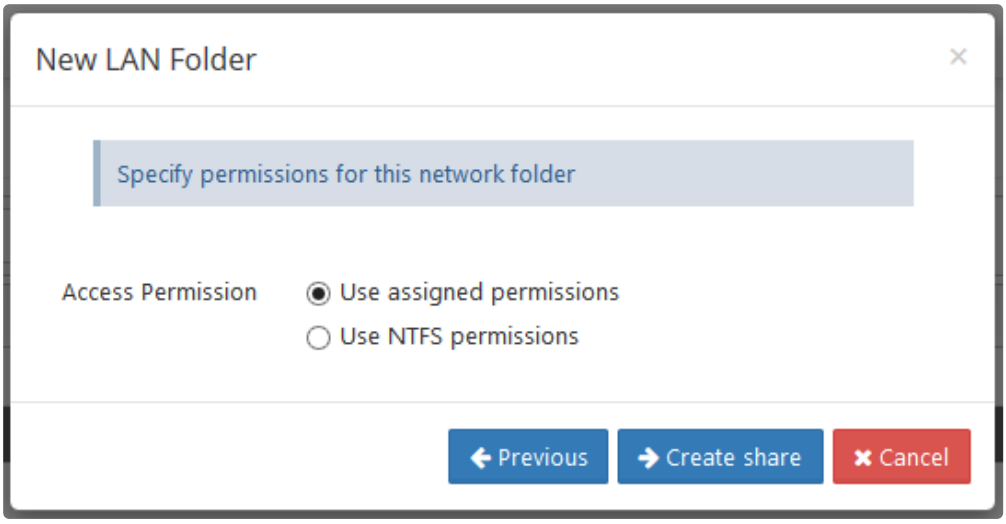
When adding Network Shares to FileCloud Server in a Windows Environment please note that File Paths can't be greater than 260 characters, due to a PHP limitation. If you want to find out if you have files with a path greater than 260 you can use a 3rd party tool like Path Length Checker, which will read 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/



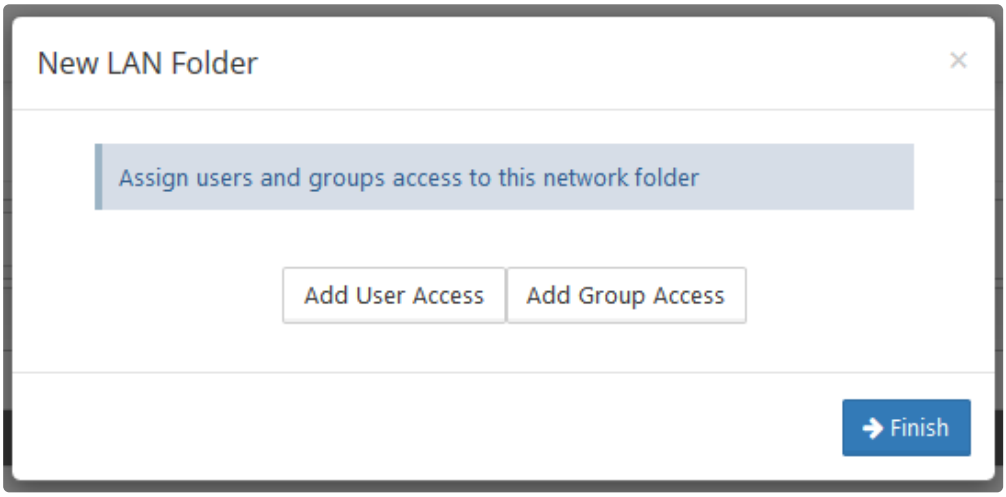
Network Folders function to give FileCloud users who are assigned to them access to their content; when you enter the **Mount Path**, please be careful to avoid entering:

- 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.



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.



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

Granting access to Network Folder

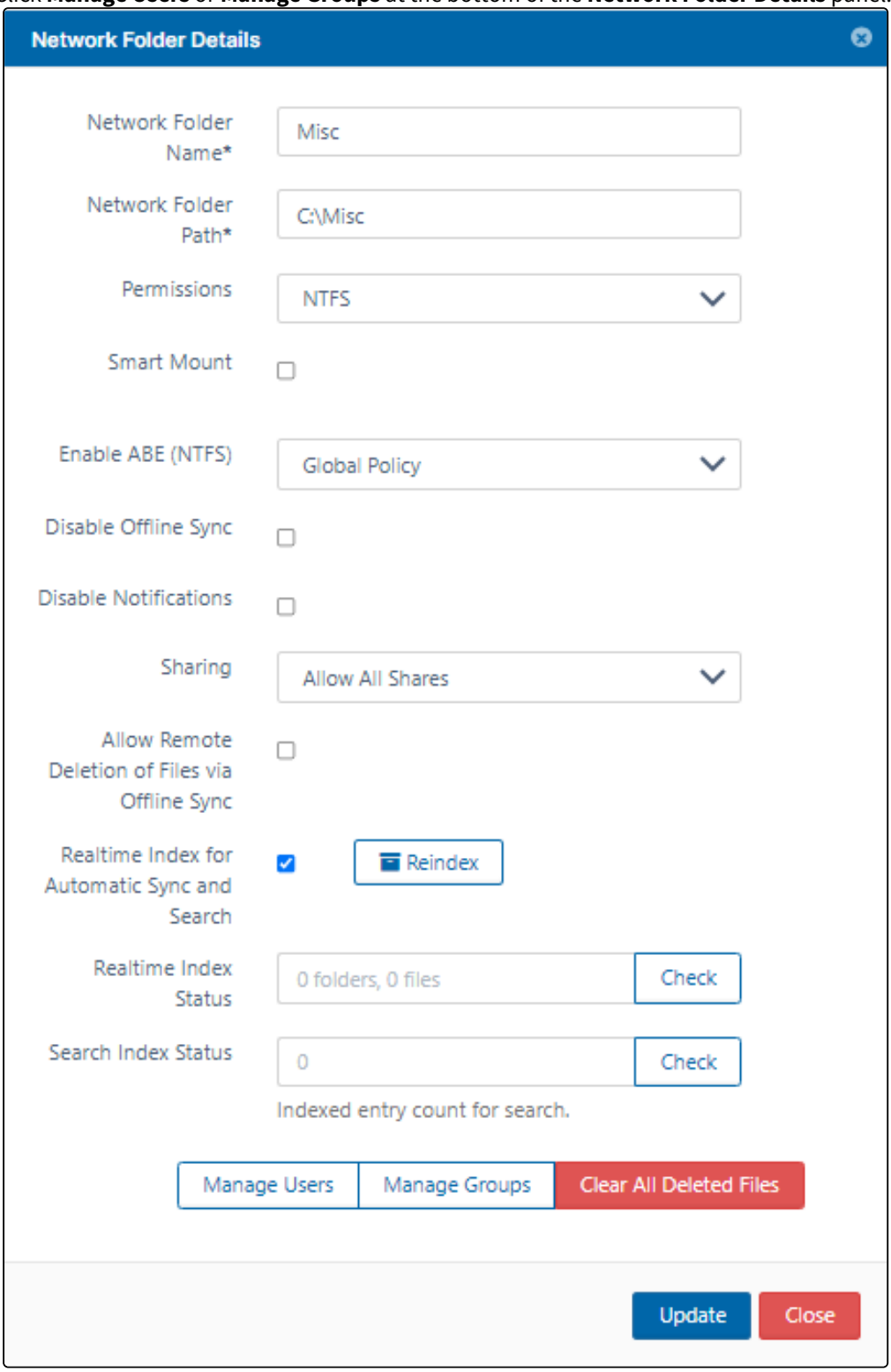
After the network share is created, you may add and remove user access to it.
The network share access can be granted to Full users, Guest users or User Groups.

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.



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.

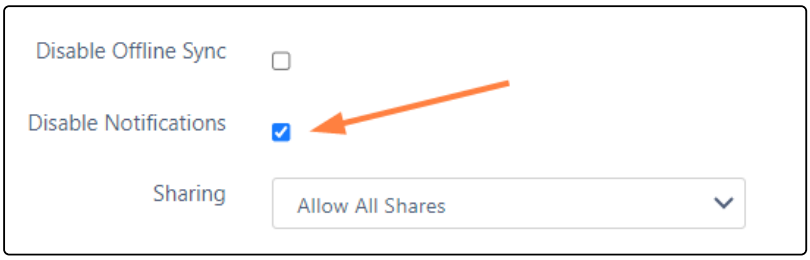
Notifications for Network Folders

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.



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

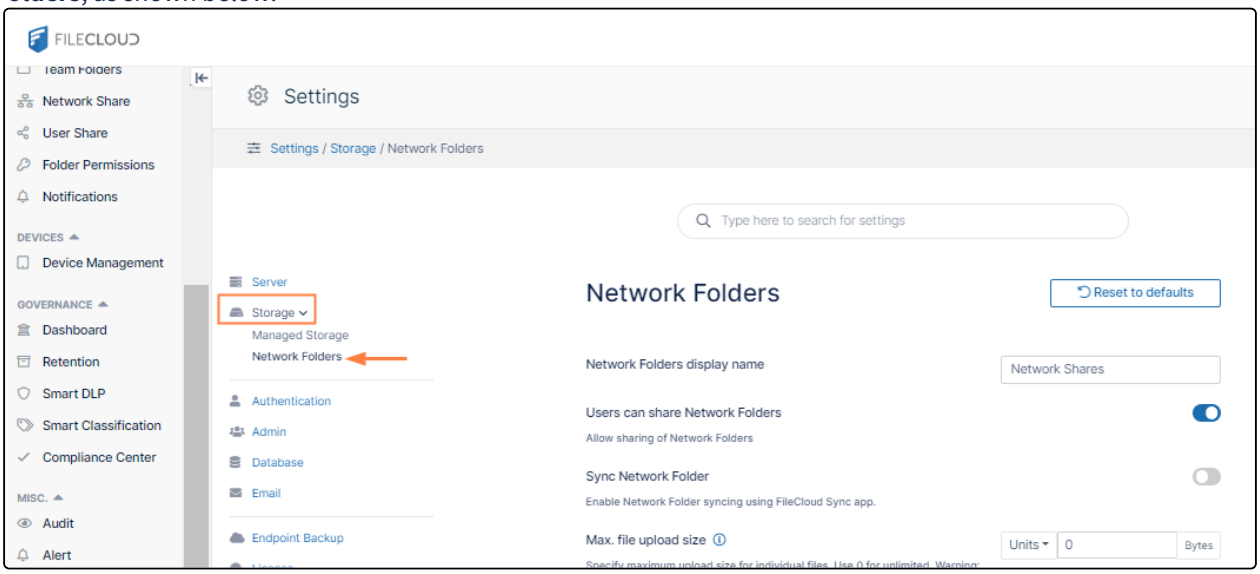
Notifications.

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

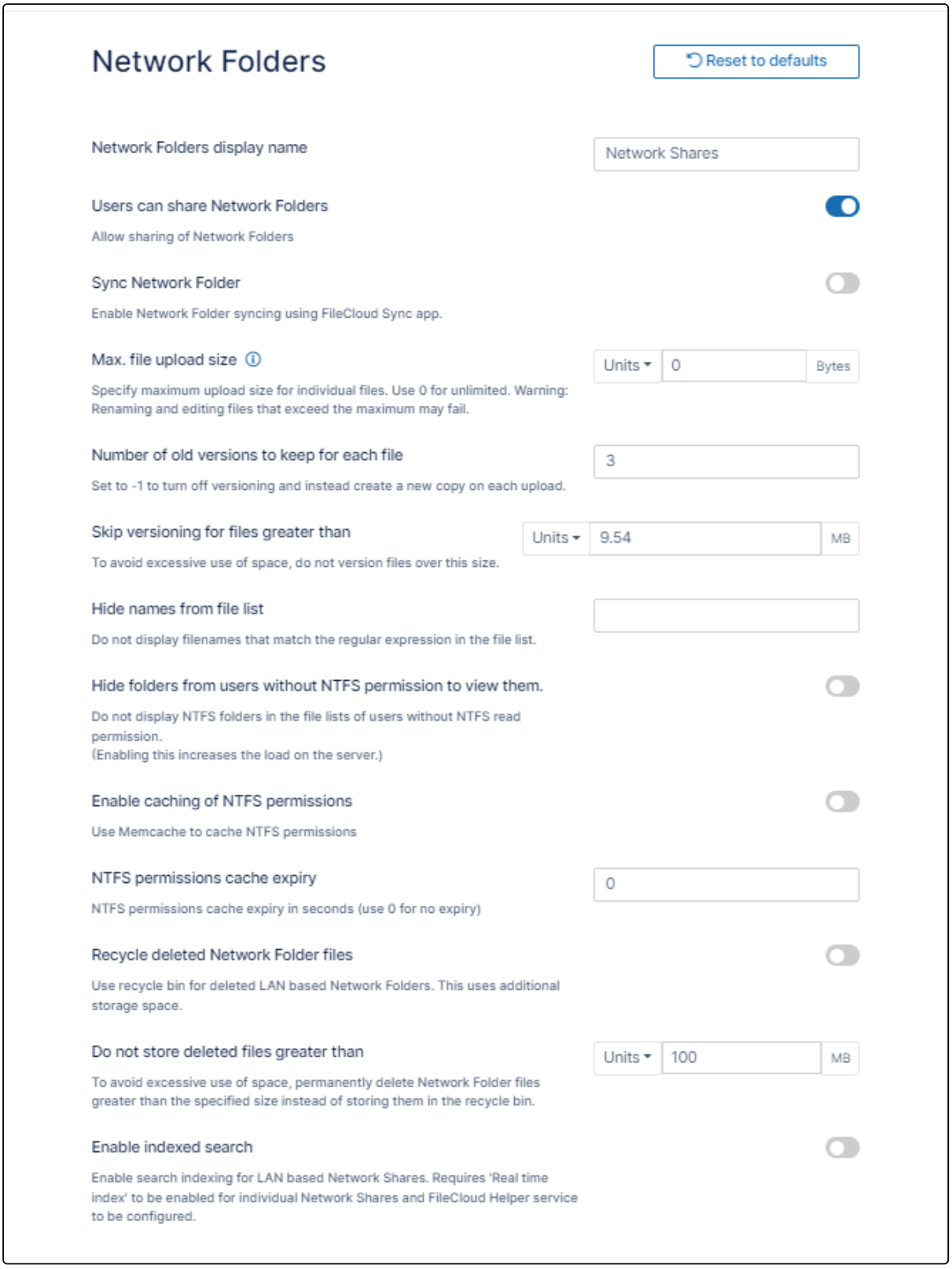
Configuring Network Folders Behavior

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

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



The Network Folders settings appear as:


Network Folders
Reset to defaults
Network Folders display name
Network Shares
Users can share Network Folders
Allow sharing of Network Folders
Sync Network Folder
Enable Network Folder syncing using FileCloud Sync app.
Max. file upload size
Units
0
Bytes
Specify maximum upload size for individual files. Use 0 for unlimited. Warning: Renaming and editing files that exceed the maximum may fail.
Number of old versions to keep for each file
3
Set to -1 to turn off versioning and instead create a new copy on each upload.
Skip versioning for files greater than
Units
9.54
MB
To avoid excessive use of space, do not version files over this size.
Hide names from file list
Do not display filenames that match the regular expression in the file list.
Hide folders from users without NTFS permission to view them.
Do not display NTFS folders in the file lists of users without NTFS read permission.
(Enabling this increases the load on the server.)
Enable caching of NTFS permissions
Use Memcache to cache NTFS permissions
NTFS permissions cache expiry
0
NTFS permissions cache expiry in seconds (use 0 for no expiry)
Recycle deleted Network Folder files
Use recycle bin for deleted LAN based Network Folders. This uses additional storage space.
Do not store deleted files greater than
Units
100
MB
To avoid excessive use of space, permanently delete Network Folder files greater than the specified size instead of storing them in the recycle bin.
Enable indexed search
Enable search indexing for LAN based Network Shares. Requires 'Real time index' to be enabled for individual Network Shares and FileCloud Helper service to be configured.

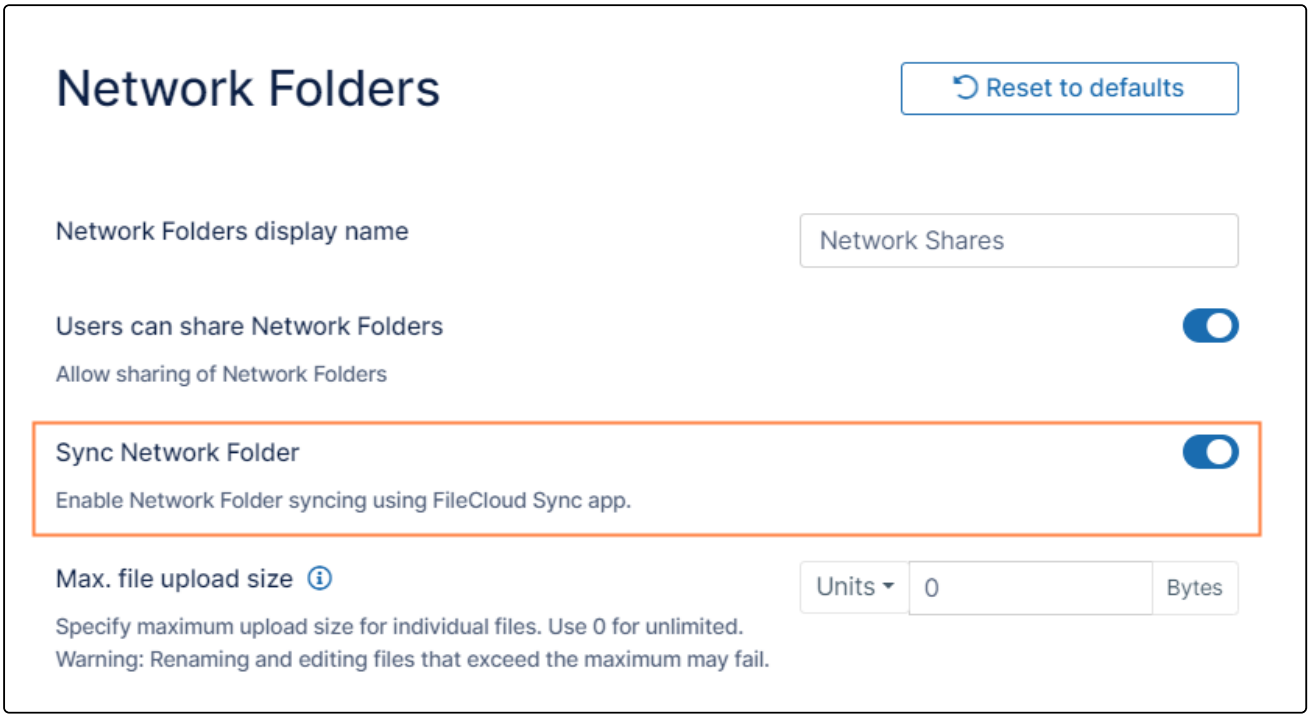
3. Fill in the settings as described in the following table.

Function	Description
Network Folders display name	This label will be displayed in the User portal when the user logs into their account. 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.
Users can share Network Folders	This setting controls whether or not a network share location can be shared by an user
Sync Network Folder	This setting controls whether or not a network share location can be synced by a user using sync client for offline access. You can disable offline sync for individual network folders as well. See Sync Network Folders for Offline Access for more information about syncing network folders.
Max. file upload size	Limits file size when uploading in Web clients. By default, this setting is not honored in Sync and Drive. It could affect folders that are renamed in Sync, since they are deleted and reuploaded during rename operations. Use 0 to allow uploading of files of unlimited sizes.
Number of old versions to keep for each file	Enables versioning of files in network location. To maintain no versions enter 0.
Skip versioning for files greater than	The file size limit in bytes beyond which the versioning will not be applied
Hide names from file list	This is a regex filter which can be used to exclude files that match the regex expression from file listing. An example of a regular expression that skips some names from displaying is /(sub.*|copy.*)/ This skips all files which start with "sub" or "copy"
Hide folders from users without NTFS permission to view them	When browsing network folders with NTFS permissions, folders that users don't have read access to are hidden from view. Enabling this increases the load on server.
Enable caching of NTFS permissions	Enable this to use Memcache to cache NTFS permissions.
NTFS permissions cache expiry	Number of seconds after which NTFS permissions are no longer cached in the system.

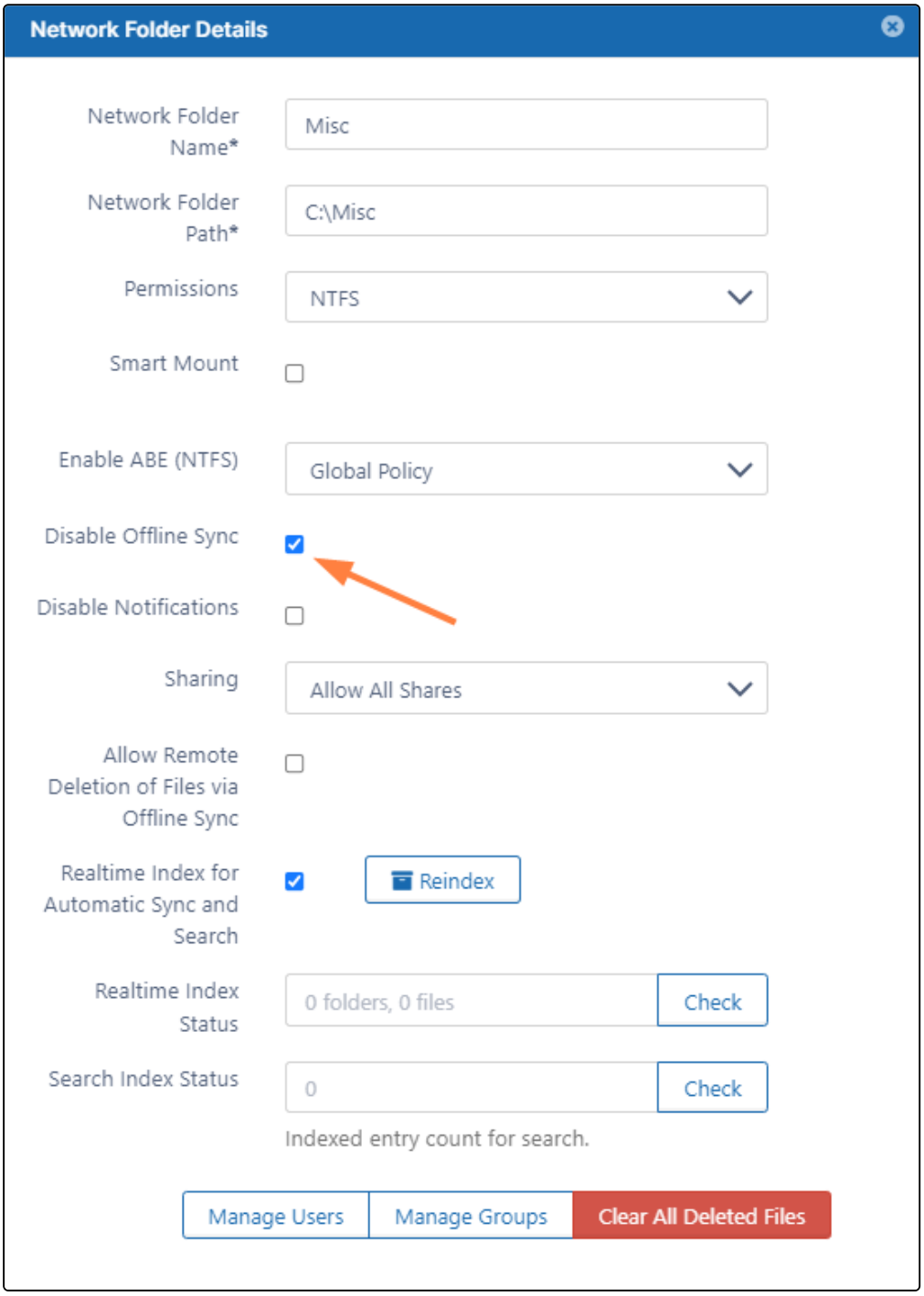
Function	Description
Recycle deleted Network Folder files	Enable this to store deleted files from Network Folders in the recycle bin.
Do not store deleted files greater than	Do not store files greater than this size in the recycle bin.
Enabled indexed search	Enable indexing of Network Folders for fast searching. See Searching in Network Folders for more information.

Offline Access to Network Folders

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



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



Sharing Restrictions on Network Folders

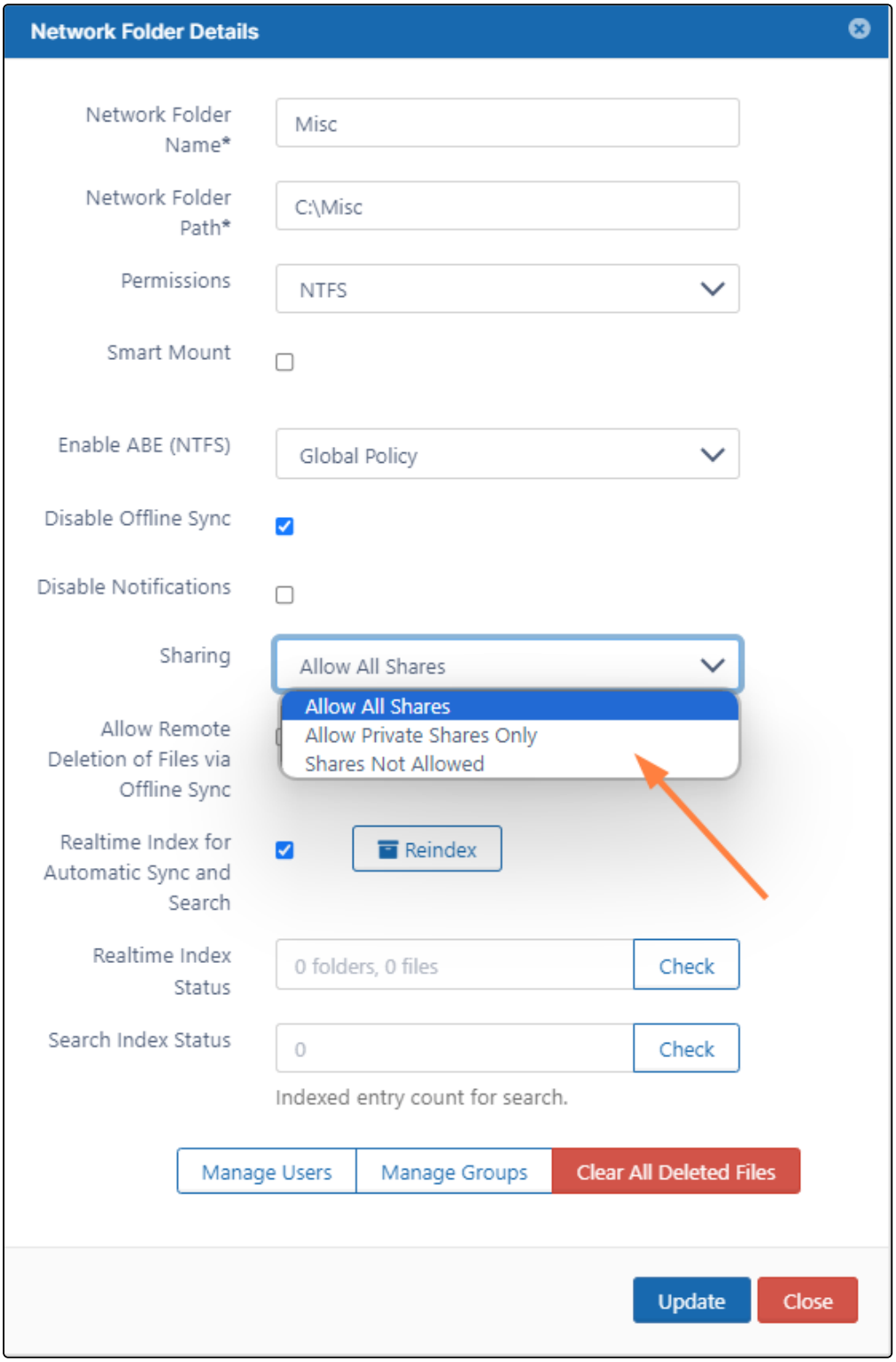
To restrict sharing on network folder, following steps should be performed.

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*
Misc
Network Folder Path*
C:\Misc
Permissions
NTFS
Smart Mount
Enable ABE (NTFS)
Global Policy
Disable Offline Sync
Disable Notifications
Sharing
Allow All Shares
Allow All Shares
Allow Private Shares Only
Shares Not Allowed
Allow Remote Deletion of Files via Offline Sync
Realtime Index for Automatic Sync and Search
Reindex
Realtime Index Status
0 folders, 0 files
Check
Search Index Status
0
Check
Indexed entry count for search.
Manage Users
Manage Groups
Clear All Deleted Files
Update
Close

Disabling Network Folders

To disable Network Folders:

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

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

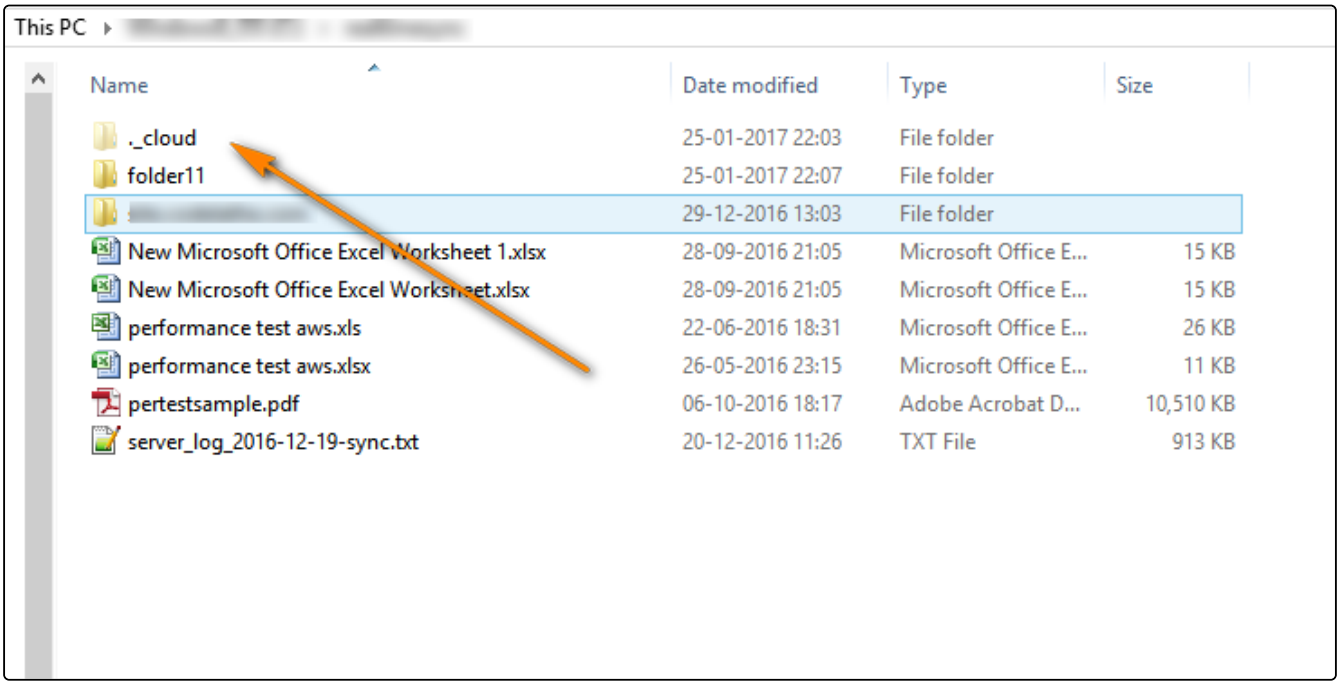
3. Change the value **true** to **false**.
4. To re-enable Network Folders, change the setting back to **true**.

Miscellaneous: ._cloud Folder

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

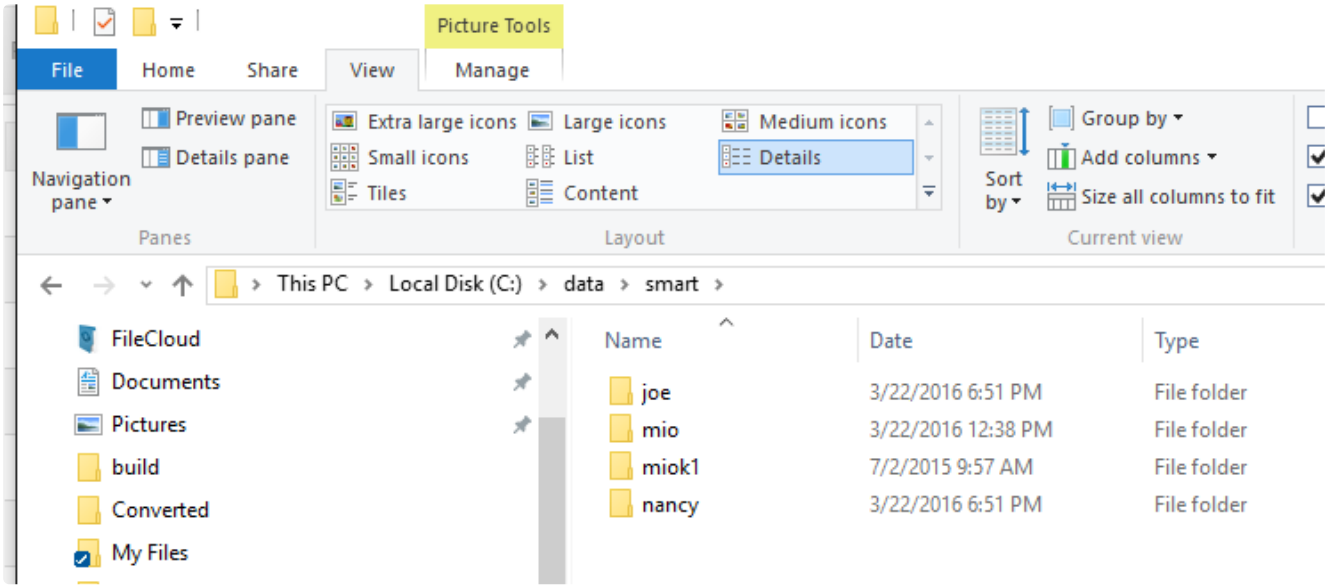
- Store previous versions of Files
- Store the deleted files under that Network Folder
- Storing the image thumbnails.

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

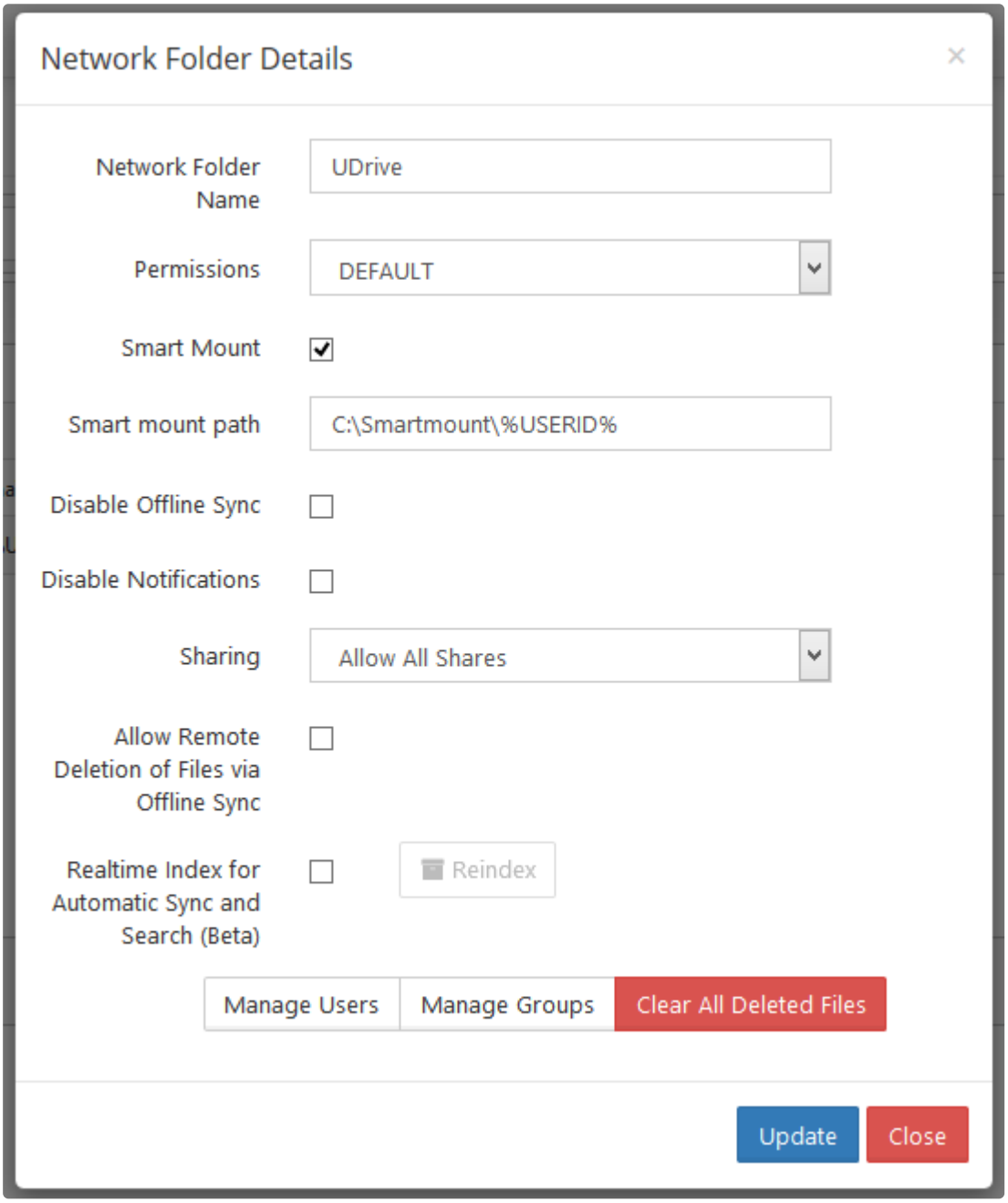
Creating a smart LAN based network folder

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 path** 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

If you want to assign this to all full users in the system, simply assign it to the EVERYONE group.



Network Folders with NTFS permissions

If you are using Network Folders with NTFS permissions:

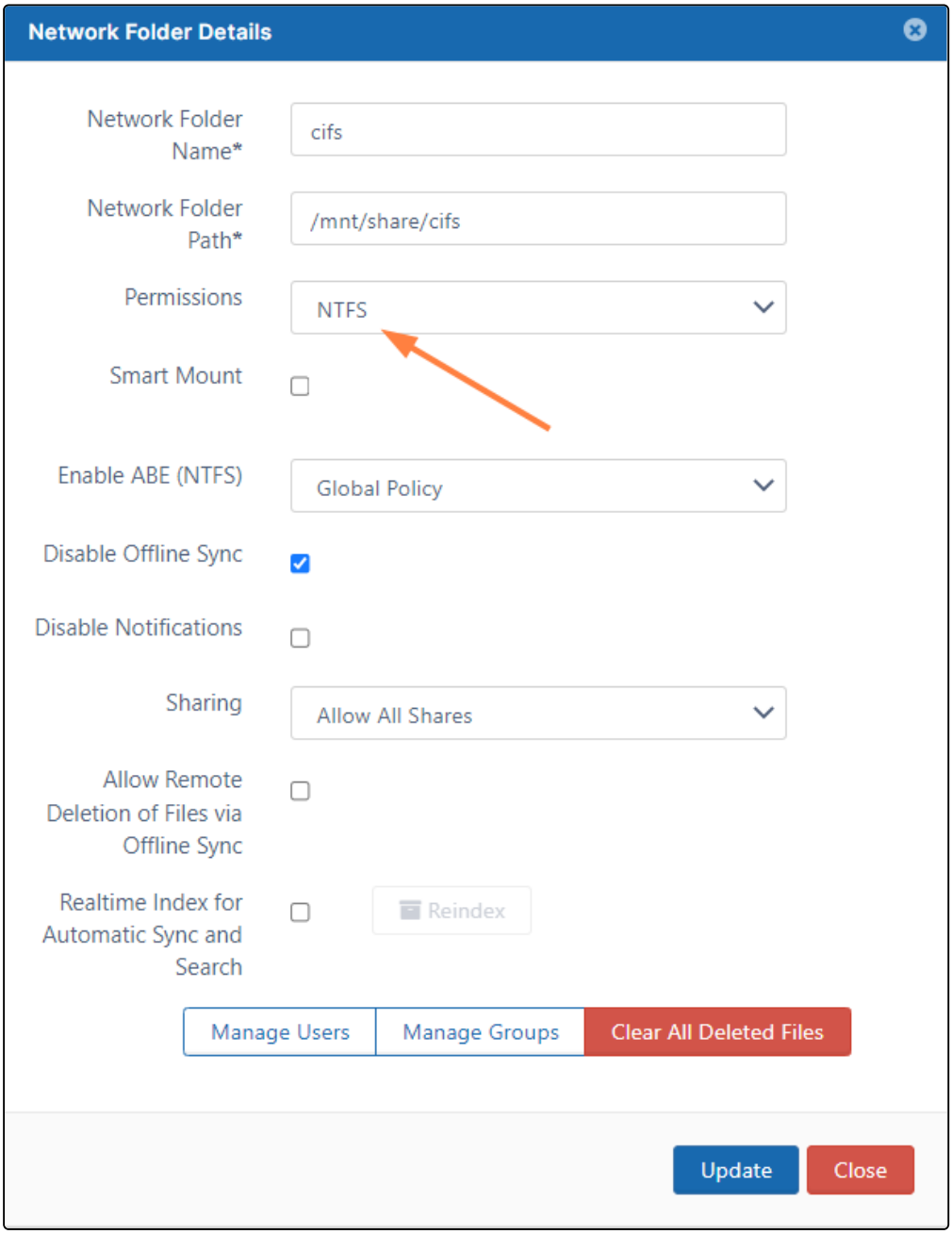
- It is recommended that you run FileCloud on Windows Servers instead of Linux.
- Authenticate user accounts with Active Directory. Users with default authentication can't leverage NTFS permissions due to security issues.
- If you are running FileCloud on Linux, a Windows Server running the FileCloud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

- Install and use memcache to improve performance.

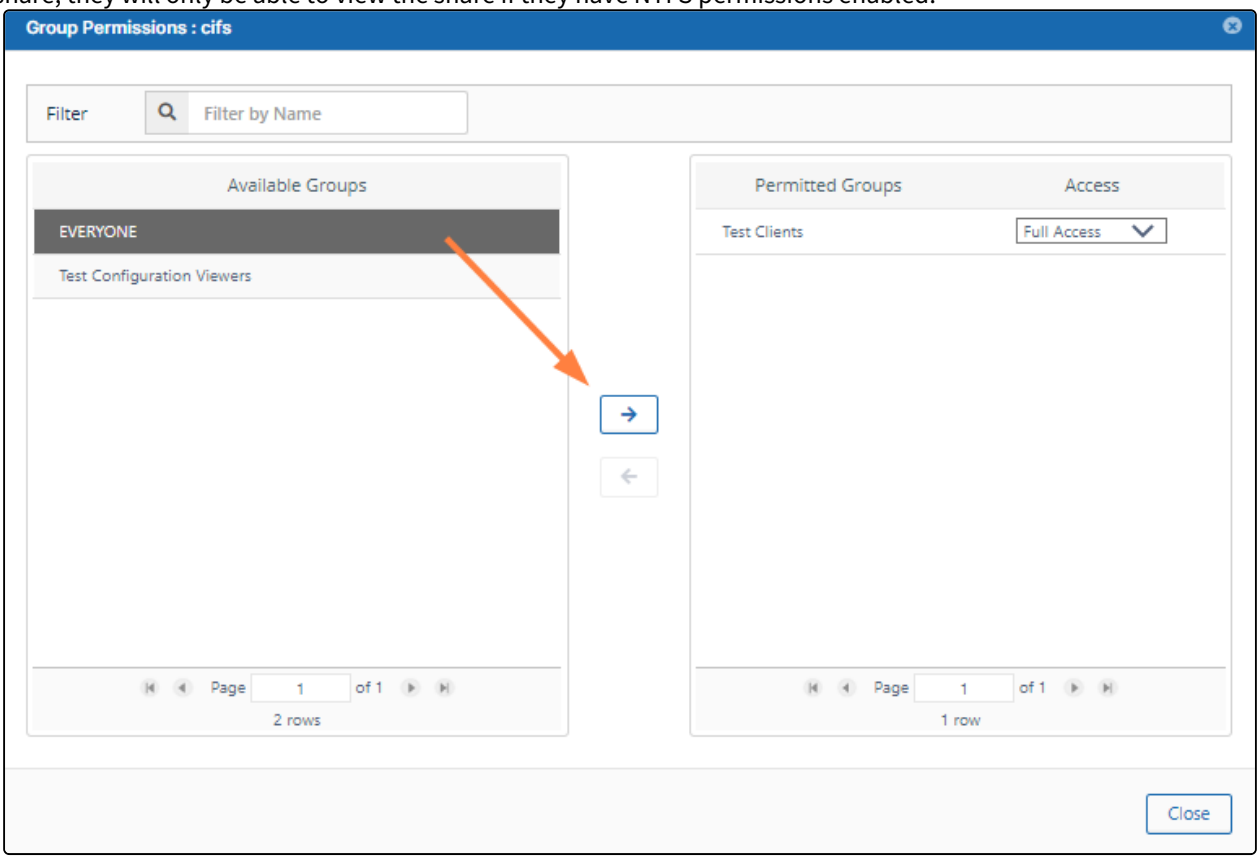
Many organizations have Windows based Network Folders that are shared with employees. The permissions on these Network Folders are managed using NTFS rights setup for various users and groups (usually from Active Directory). FileCloud can use the same NTFS permissions on the Network Folders for user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

To setup a network Folder with NTFS permissions:

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



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



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

Additional Information and Troubleshooting

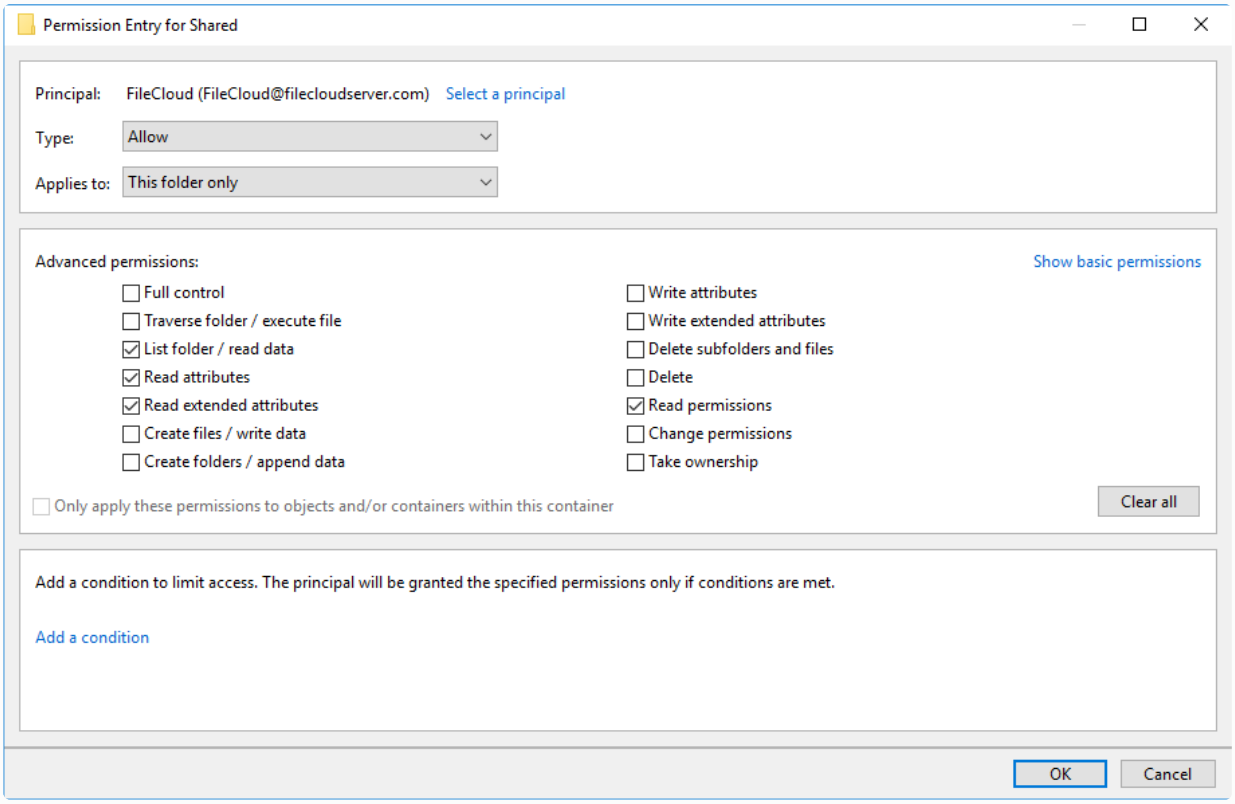
- When user membership in a AD group is modified, that change is not propagated immediately and is cached by Windows. As a result, if you change a user group membership, it might not be picked up NTFS helper immediately. It might take some time ranging from 10 minutes to several hours before the change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

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

NTFS special permissions

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

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

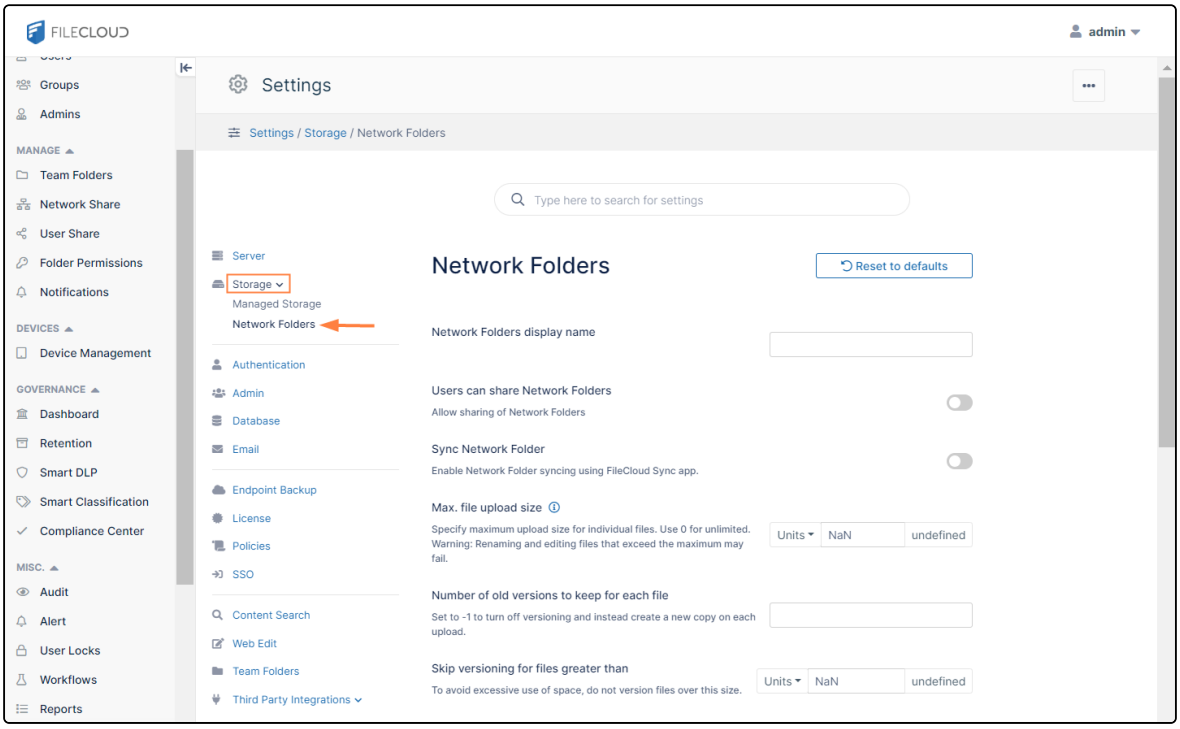


For Microsoft Documentation (https://technet.microsoft.com/en-us/library/2006.01.howitworksntfs.aspx)

NTFS Network Folders with Access Based Enumeration

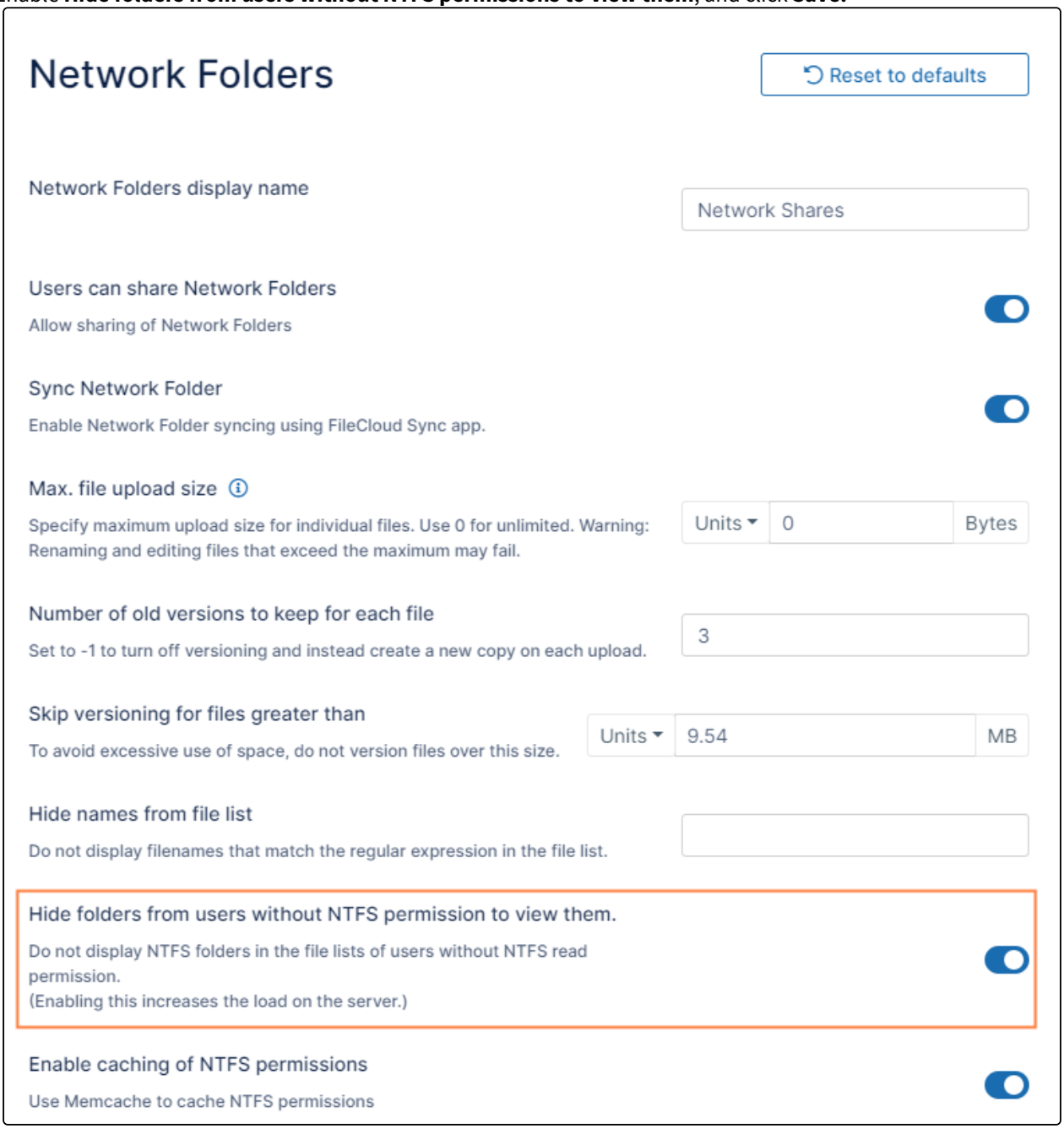
When using Network Folders with NTFS permissions, it is possible to automatically hide folders that users who don't have permission to view them.

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



The **Network Folders** settings page opens.

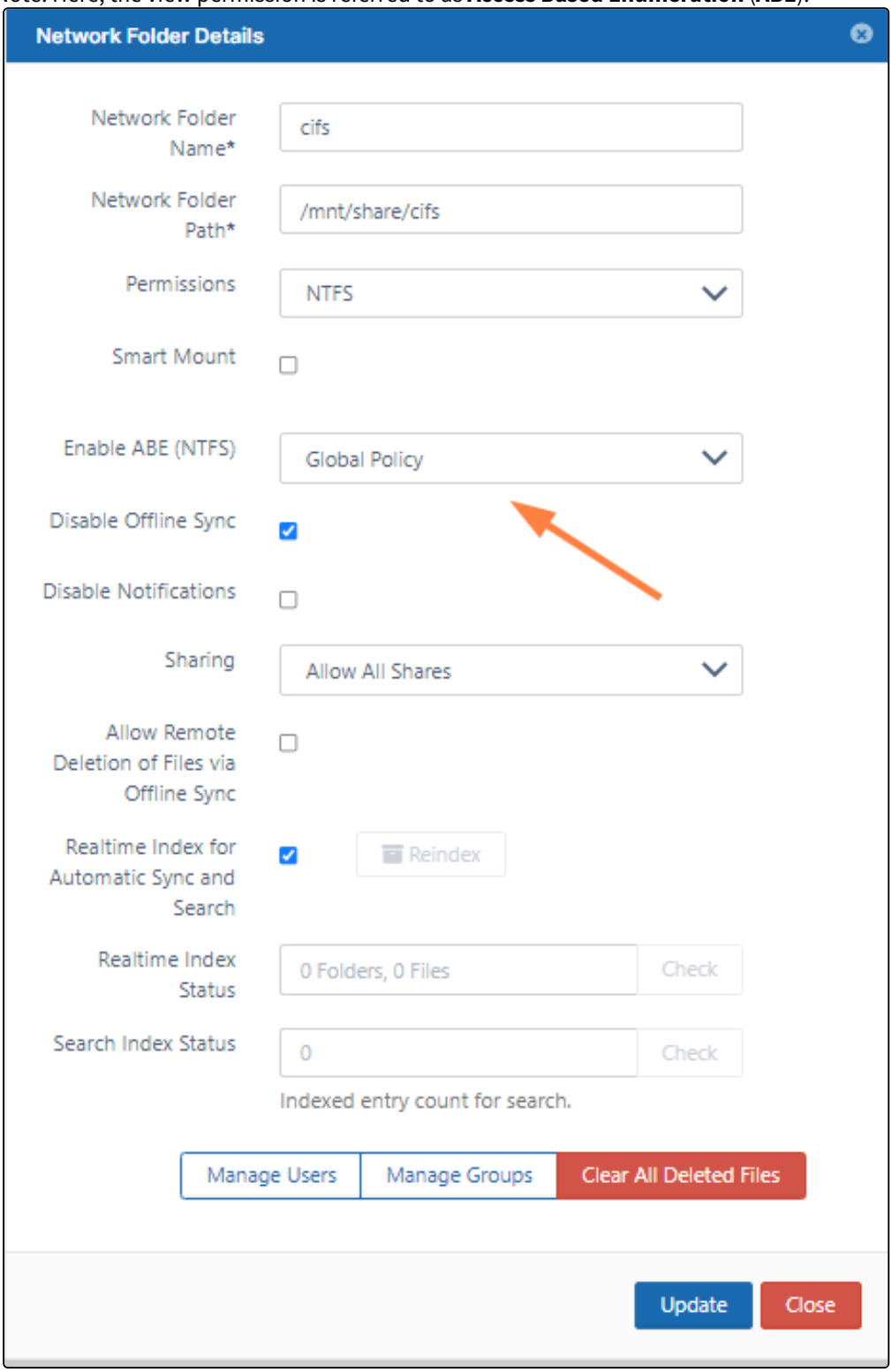
2. Enable **Hide folders from users without NTFS permissions to view them**, and click **Save.**



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

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

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



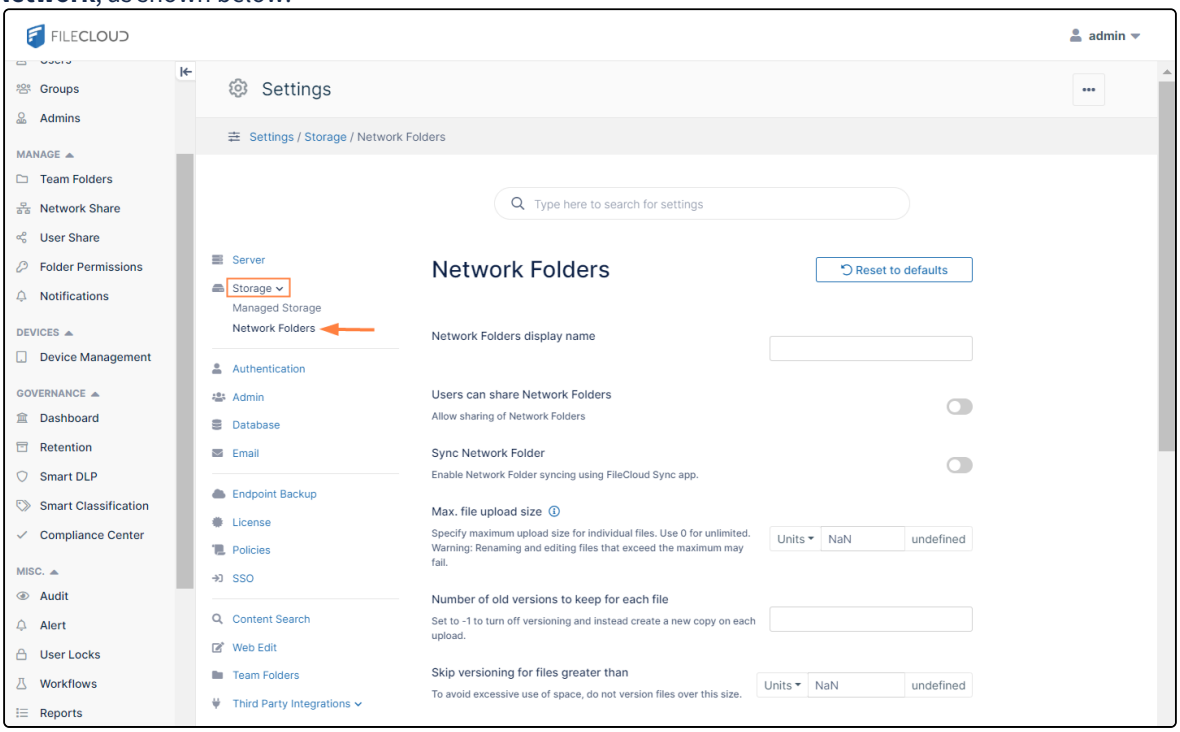
NTFS permission checks read the **tokenGroupsGlobalAndUniversal** attribute of the SID specified in the call to determine the current user's group memberships. To simplify granting accounts permission to query a user's group information, add accounts that need the ability to look up group information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

Improving performance of NTFS Network Folders

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

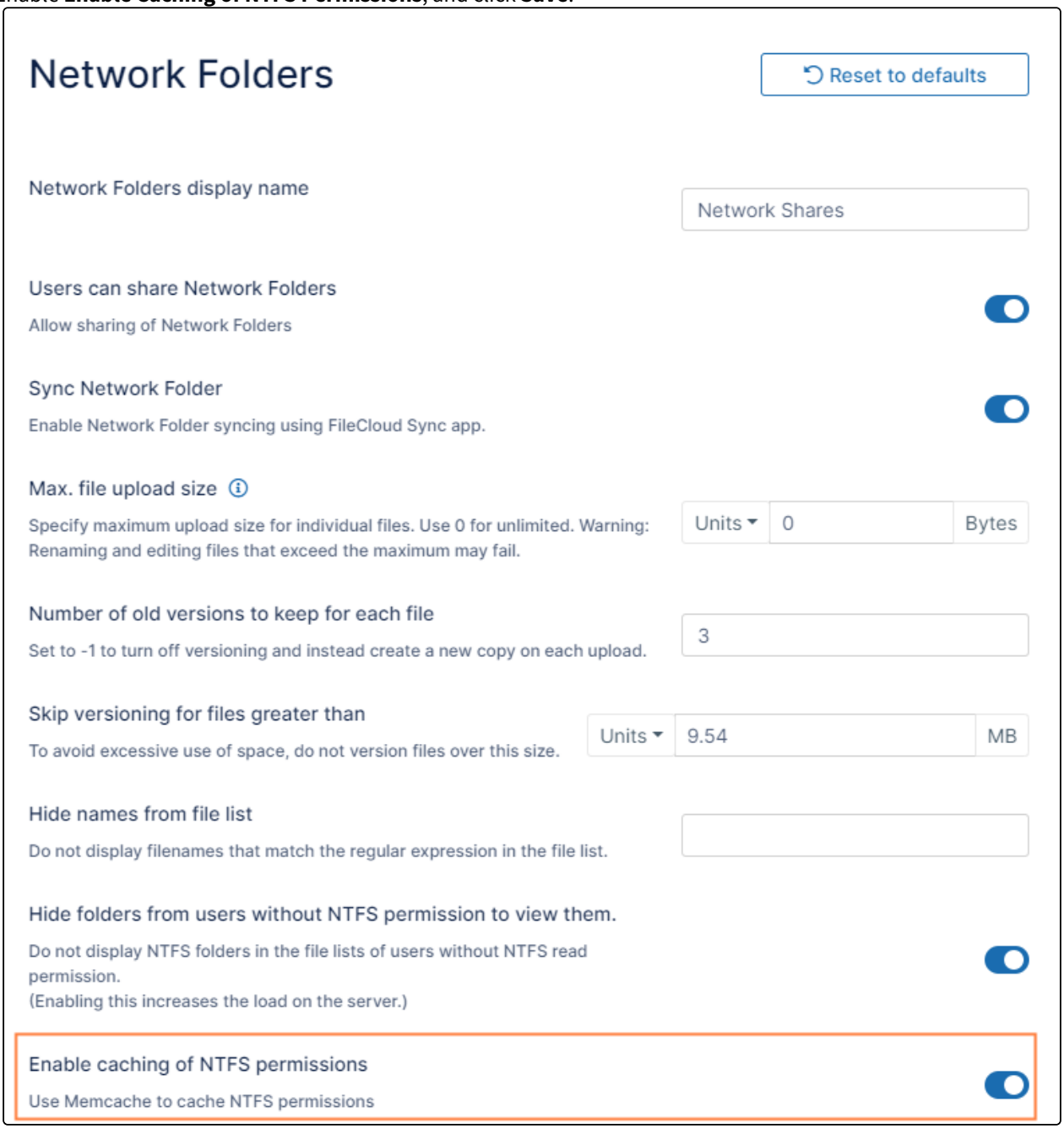
To enable caching of NTFS permissions:

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



The **Network Folders** settings page opens.

2. Enable **Enable Caching of NTFS Permissions**, and click **Save**.



Guide to FileCloud Network folders with NTFS Permissions

Quick help on setting up NTFS network shares

This guide explains prerequisites and basic steps for setting up NTFS on your network files. Common questions regarding NTFS FileCloud integration are also addressed in this page.

FileCloud Network Folders

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

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

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

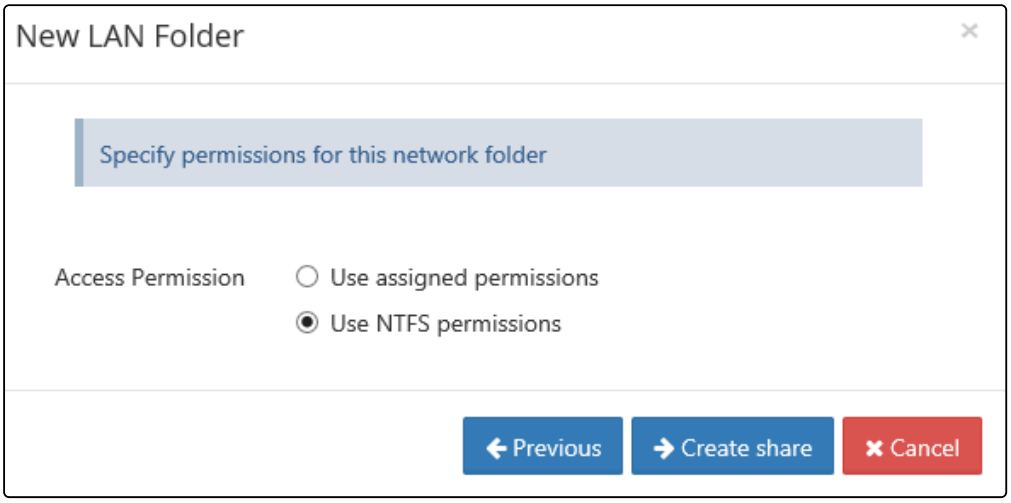
Pre-Requisites for NTFS setup

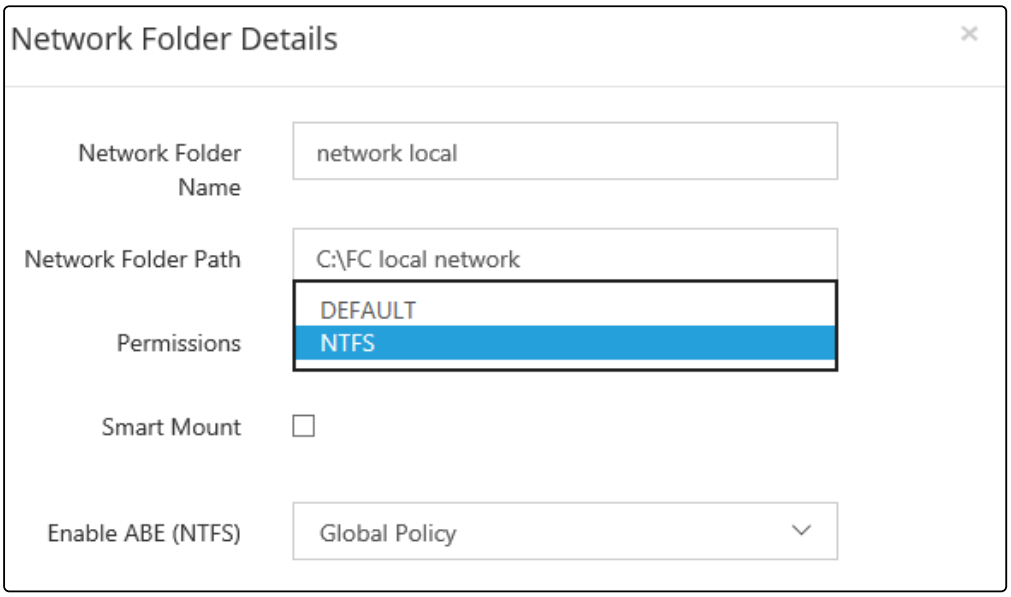
When Network Folders are added to FileCloud, permission needs to be set as NTFS. This uses all the NTFS permissions already set on the Network Share.

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

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

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





Prerequisite 2: FileCloud Helper service (optional)

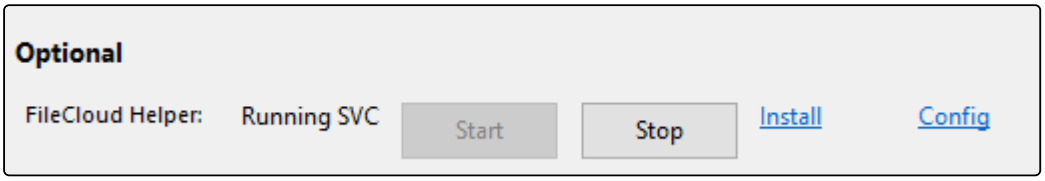
Helper Optional

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

The FileCloud Helper service performs:

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

- Content search of documents in Network Folders in Windows and Linux Server



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

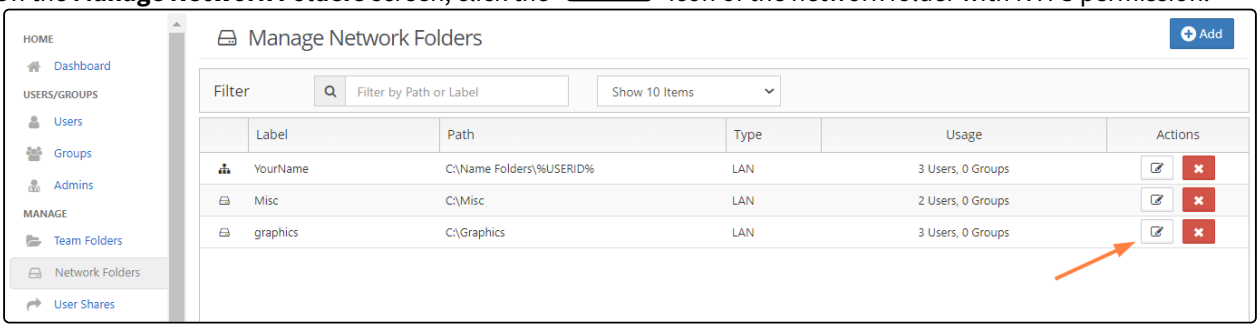
Prerequisite 3: Assign users (AD Users)

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

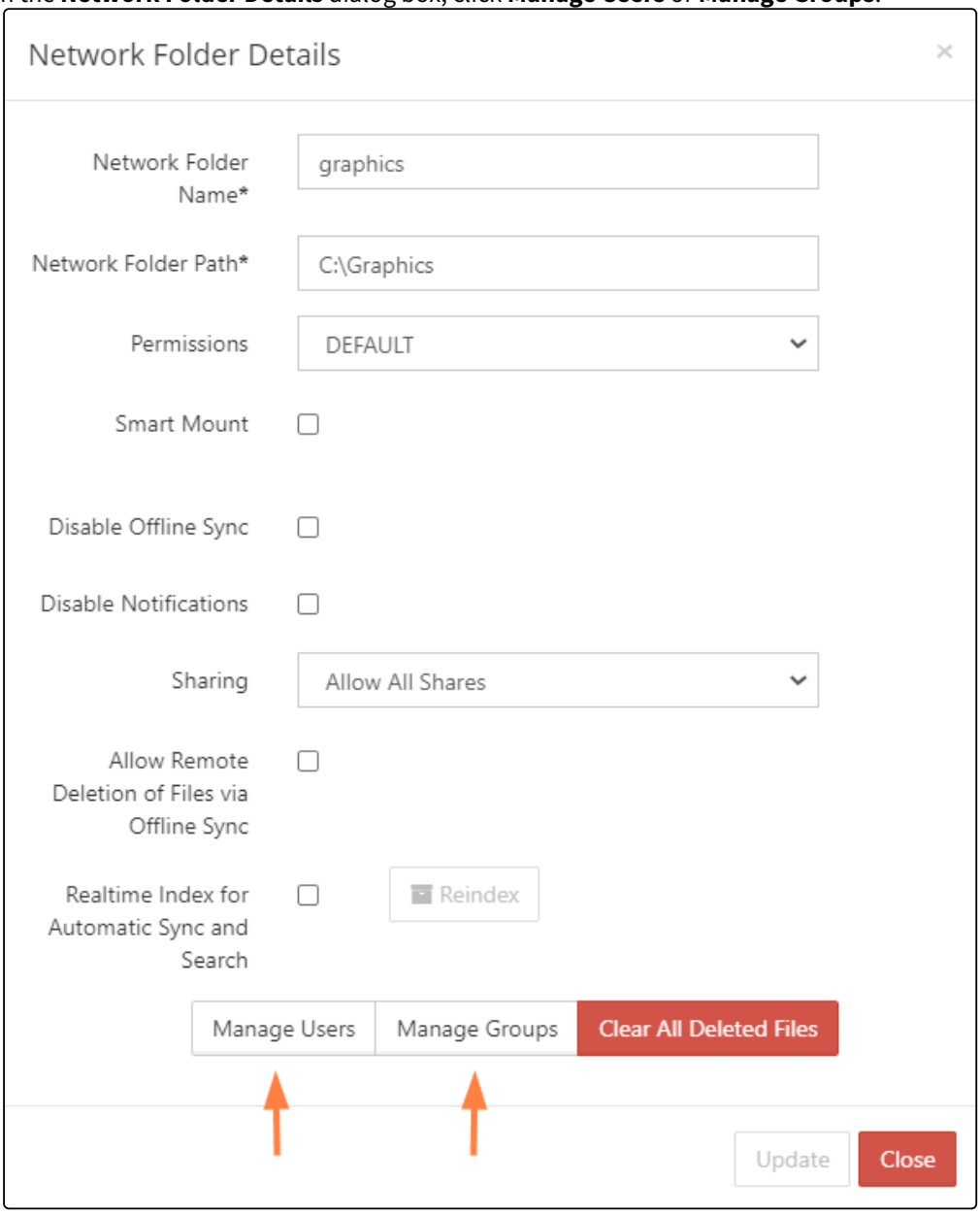
To set up AD users, see Active Directory Authentication

To give permissions:

1. On the **Manage Network Folders** screen, click the  icon of the network folder with NTFS permission.



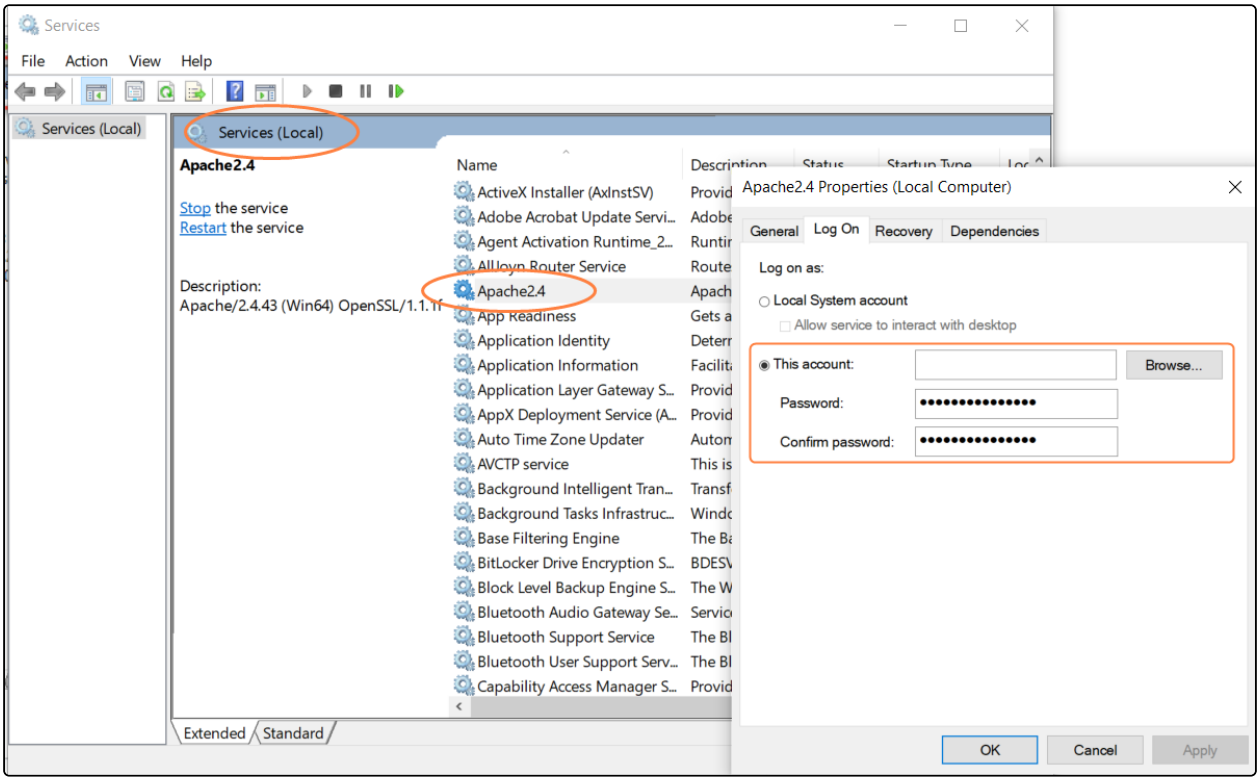
2. In the **Network Folder Details** dialog box, click **Manage Users** or **Manage Groups**.



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

Helpful information

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



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

   Note:

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

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

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

5. **What happens when a user permission is changed in AD?**
   When user membership in an AD group is modified, that change is not propagated immediately and is cached by

Windows. For more information, see Microsoft help
As a result, if you change a user group membership, it might take some time ranging (10 minutes to several hours) before the change is picked up by NTFS. If the changes must be picked up immediately, restart the Helper service.

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

For your reference

The FileCloud Helper service performs:

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

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

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

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

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

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

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

Indexing of Network Folders

Introduction

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

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

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

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

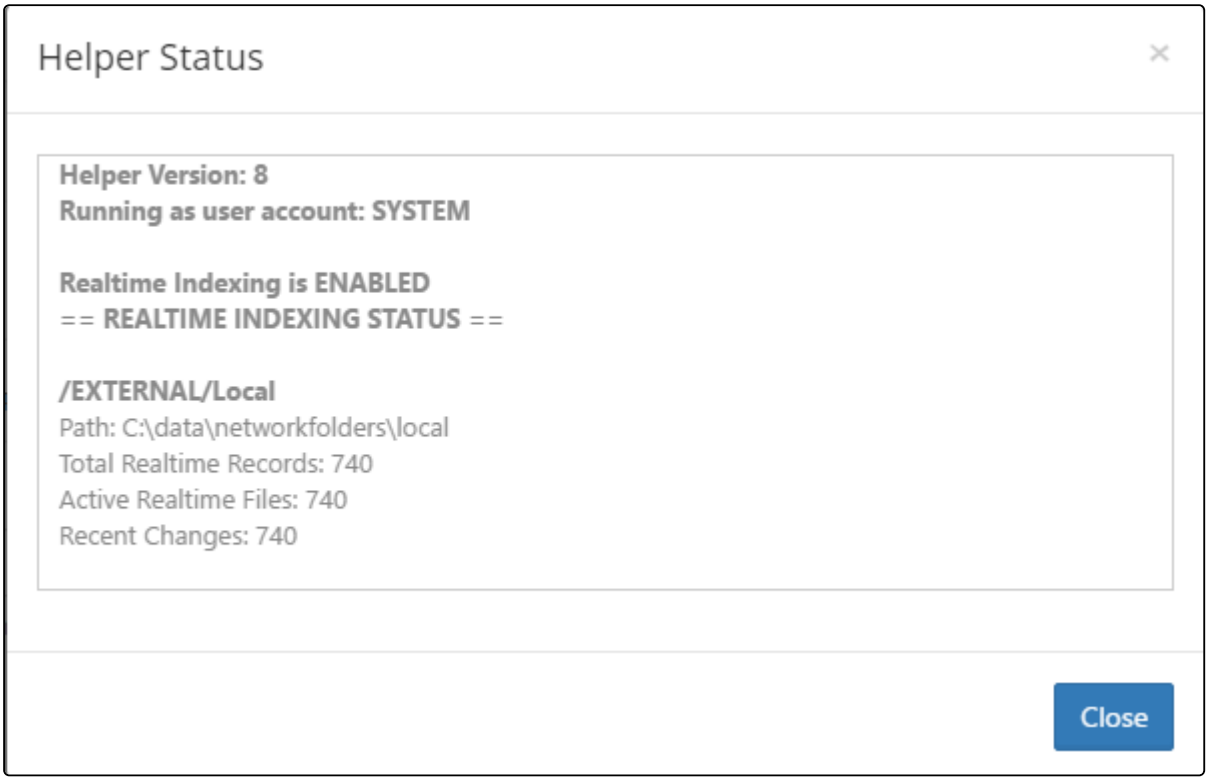
Setting up Indexing of Network Folders

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

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


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

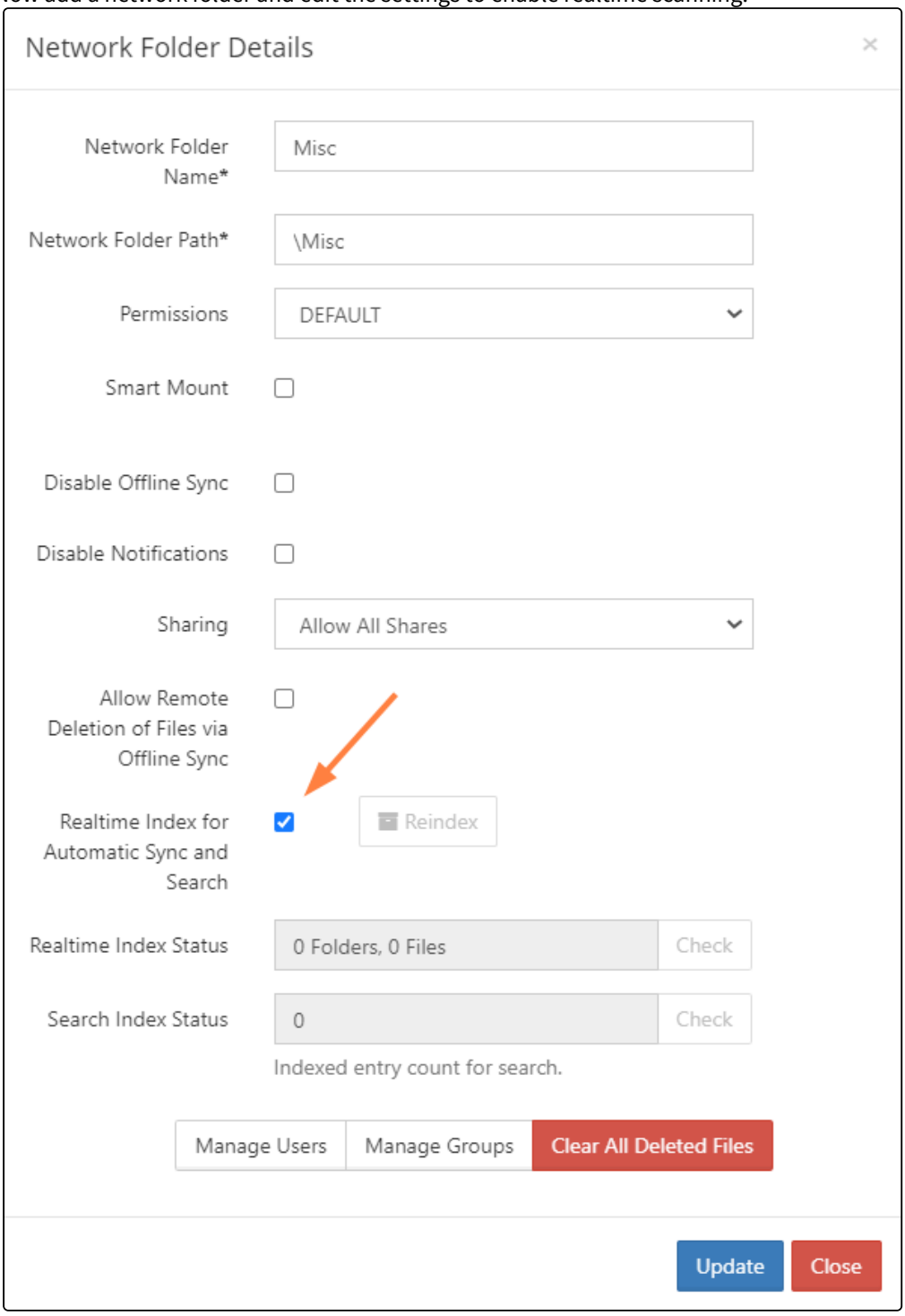
   a. Change the database settings if not using the default.
   b. Change the **enable** setting to **enable=1**
   c. change the **securitykey** value from the default to any other password value.
   d. Restart the Helper.
3. Verify that the Helper is configured correctly by opening **Settings > Misc > Support Services** in the admin portal. Click the **Helper Status** button and ensure the status shows that realtime indexing is enabled.



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

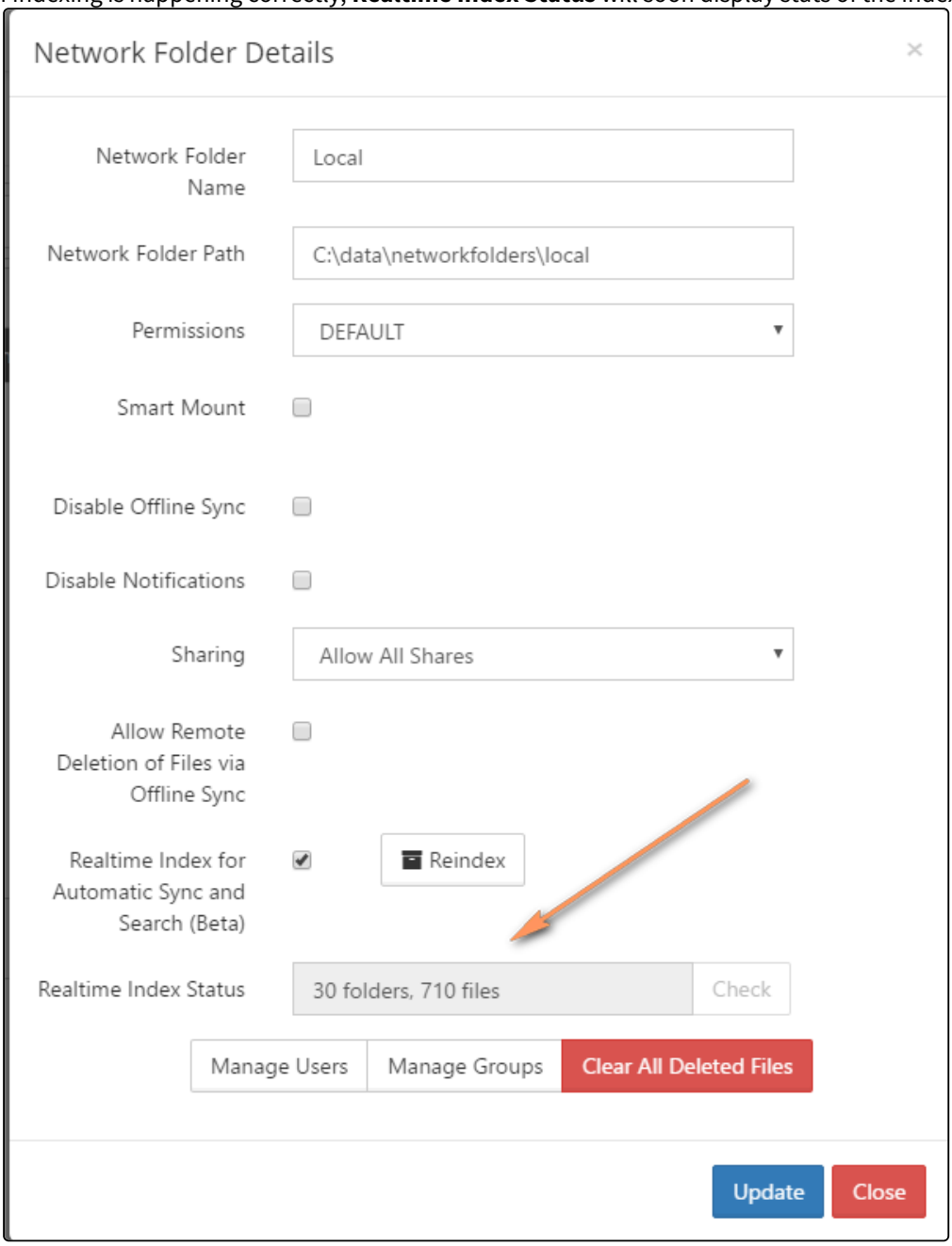
```
define("TONIDOCLOUD_PUSH_KEY", "nosoup4u");
```

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



6. Always, restart the NTFS helper after enabling realtime index options for Network Folders or after adding or removing Network Folders

7. If indexing is happening correctly, **Realtime Index Status** will soon display stats of the indexed files and folders.



Searching in Network Folders

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

For faster searching, you can

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

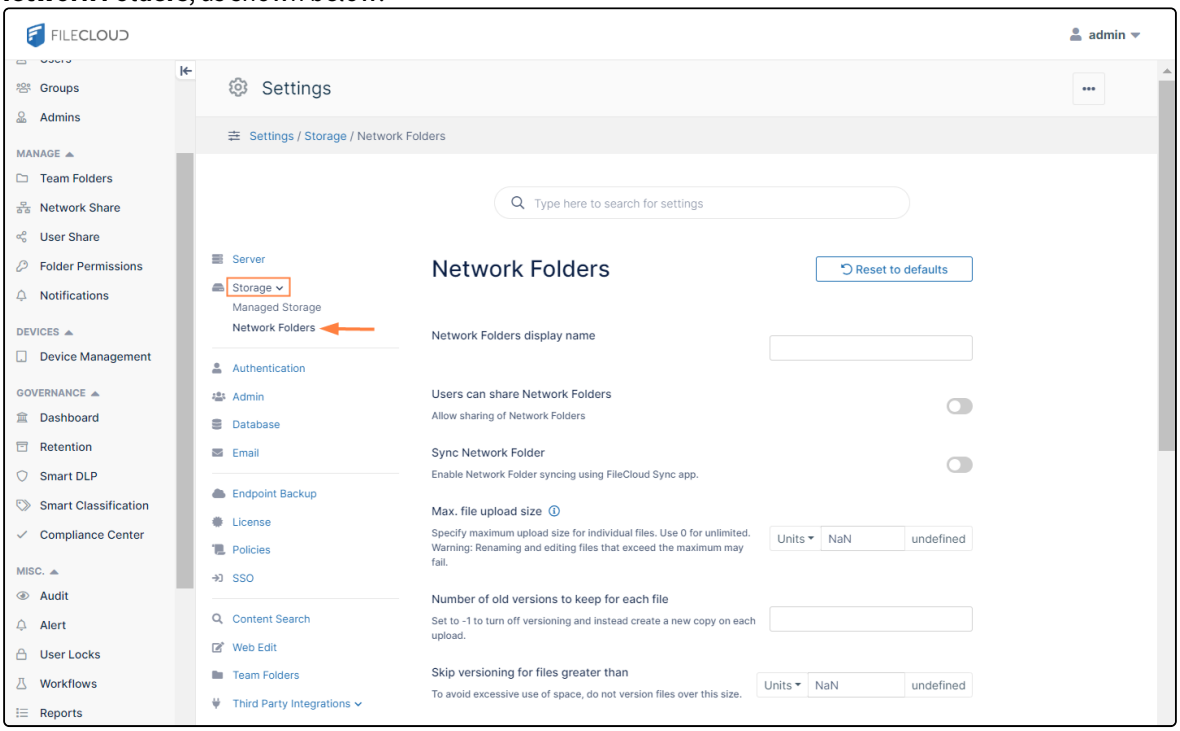
Both options require that you have enabled indexing of Network Folders.

Enable indexed search of Network Folders

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

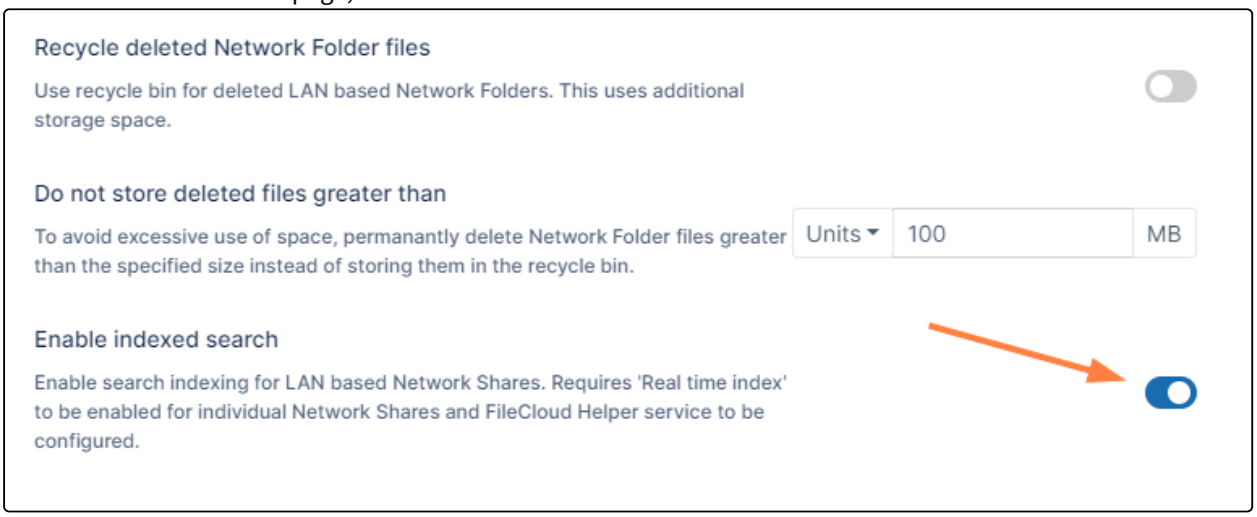
To enable Indexed Search in Network Folders:

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



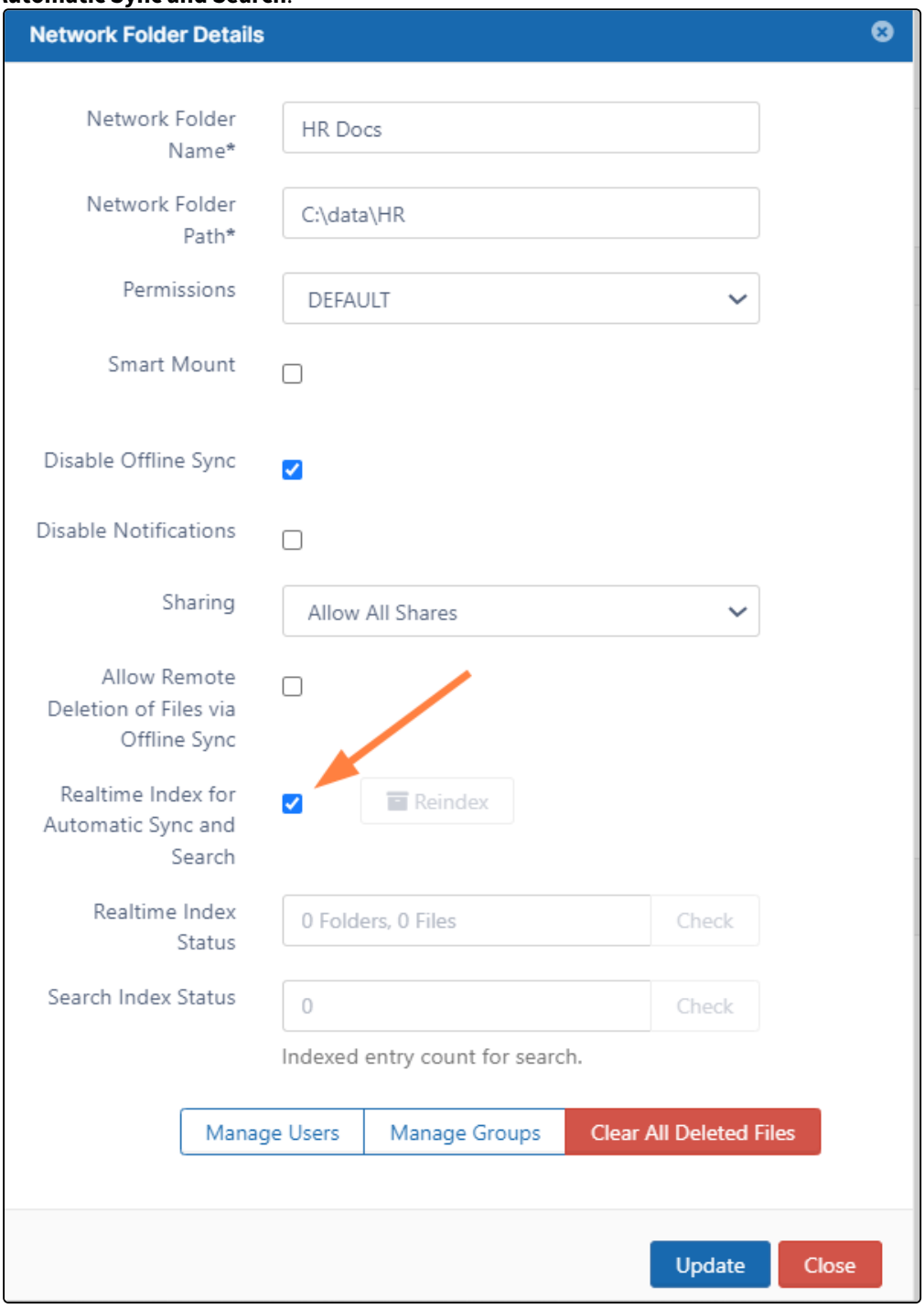
   The **Network Folders** settings page opens.

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



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

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



Web Server Permissions for Network Shares

FileCloud Control Panel names and corresponding Windows Services names

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

The following table lists the corresponding names:

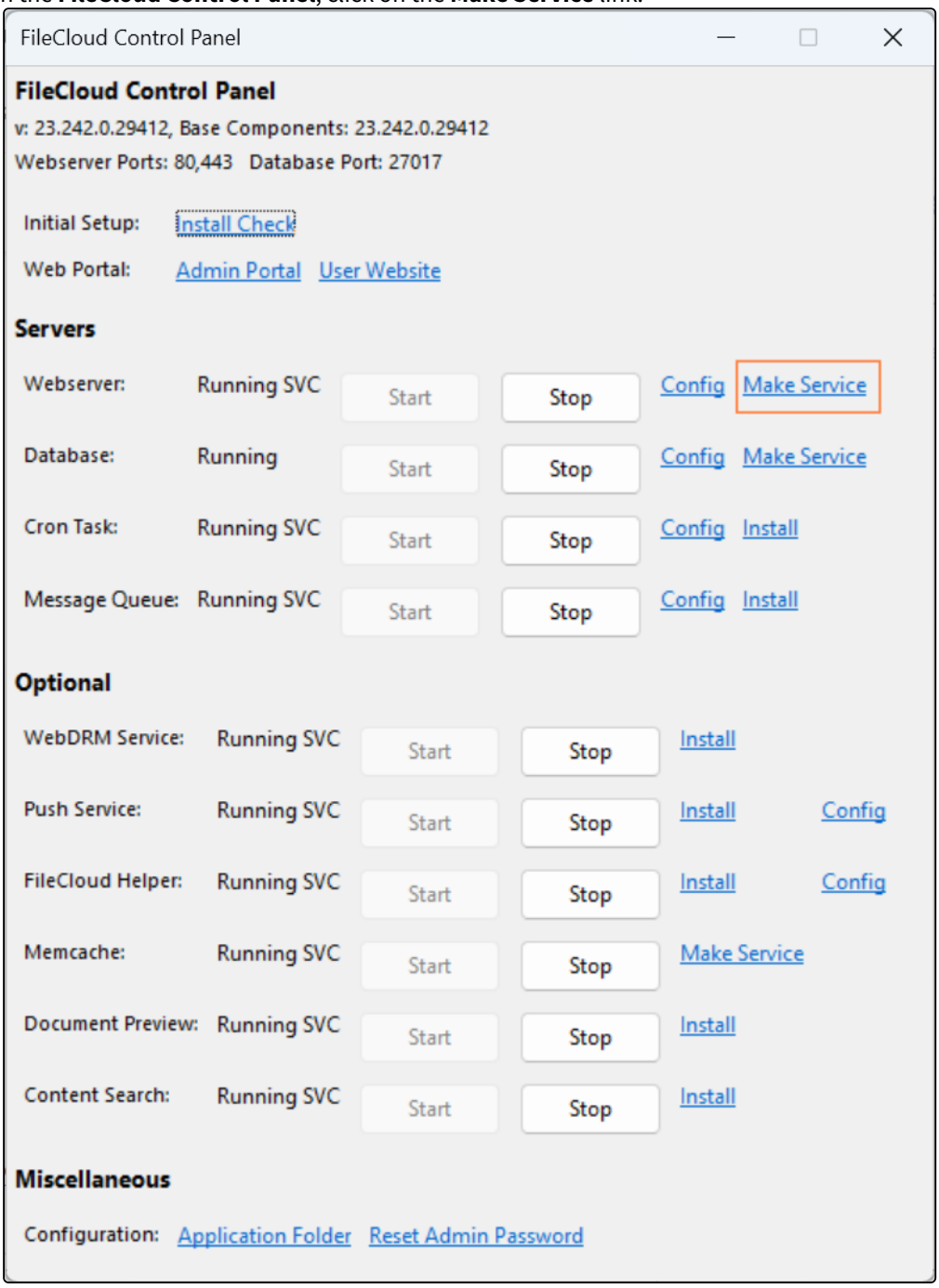
FileCloud Control Panel name	Windows Services name
Webserver	Apache or Apache#.# (for example, Apache2.4)
Message Queue	fcorchestrator
Cron Task	FileCloud Cron Service
Document Preview	FileCloud Docconverter

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

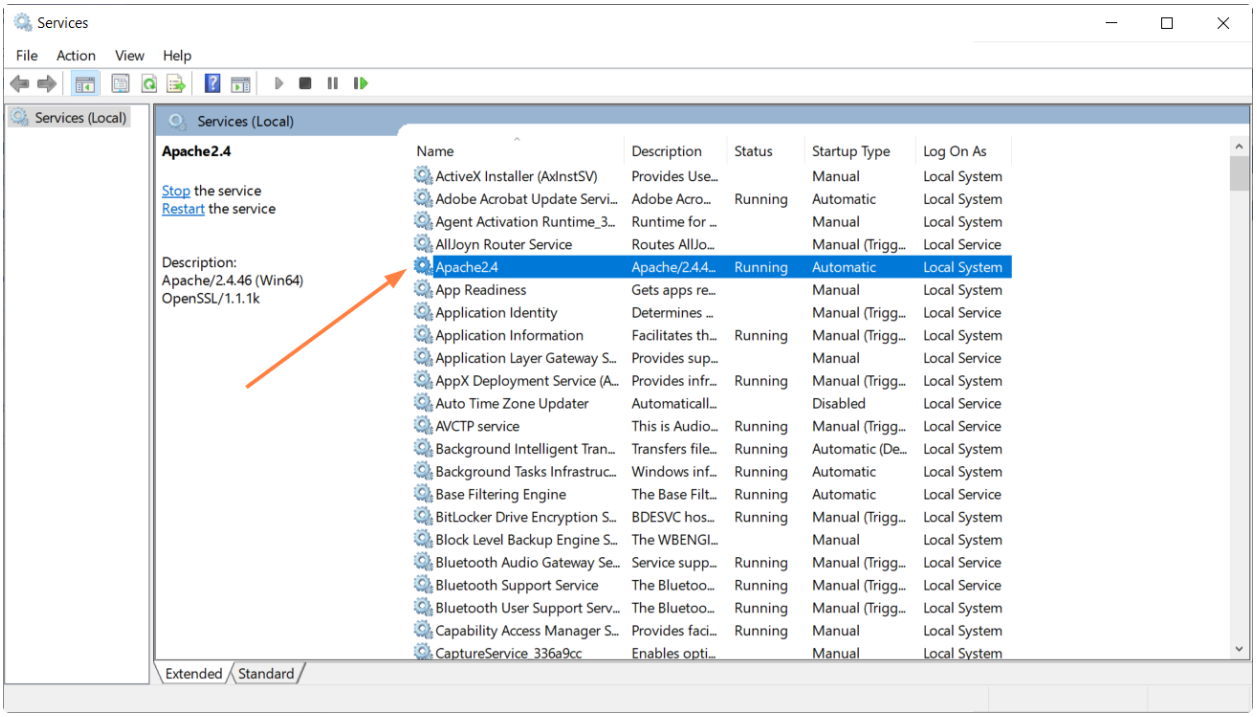
To make Network Folders accessible via FileCloud, the Webserver (Apache), Message Queue (fcorchestrator), Cron Task (FileCloud Cron Service), and Document Preview (FileCloud Docconverter) services must run as accounts with full permissions on Network Folders, otherwise there may be problems accessing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

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

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

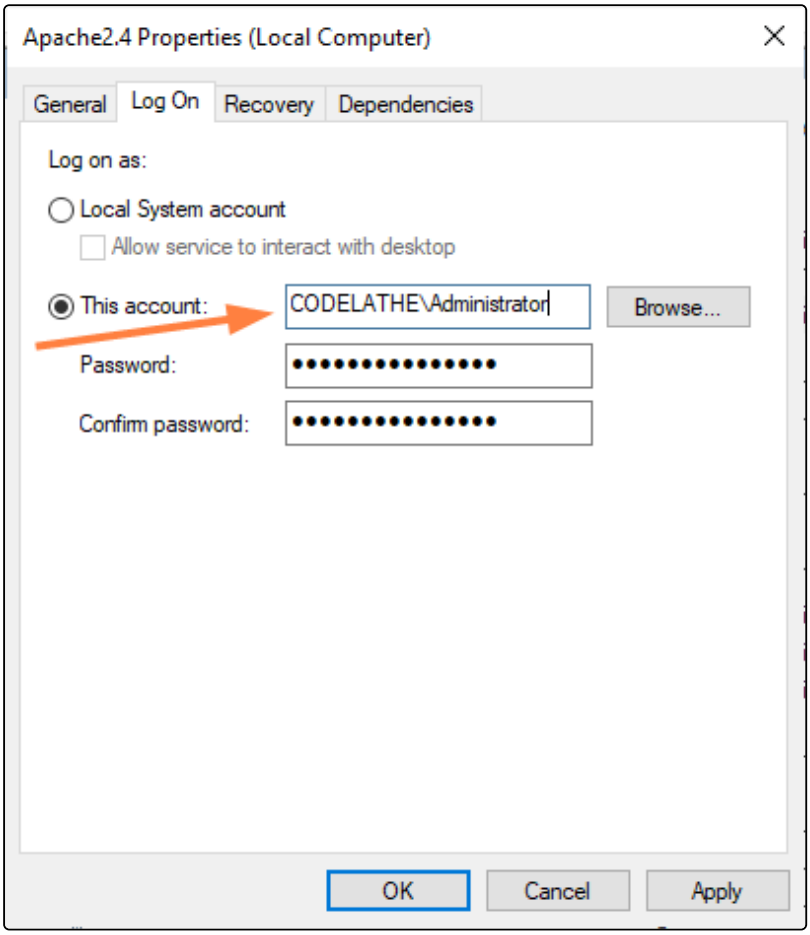


2. Open the Windows **Services** panel, then access the **Apache** service (the name may include the version of Apache installed).



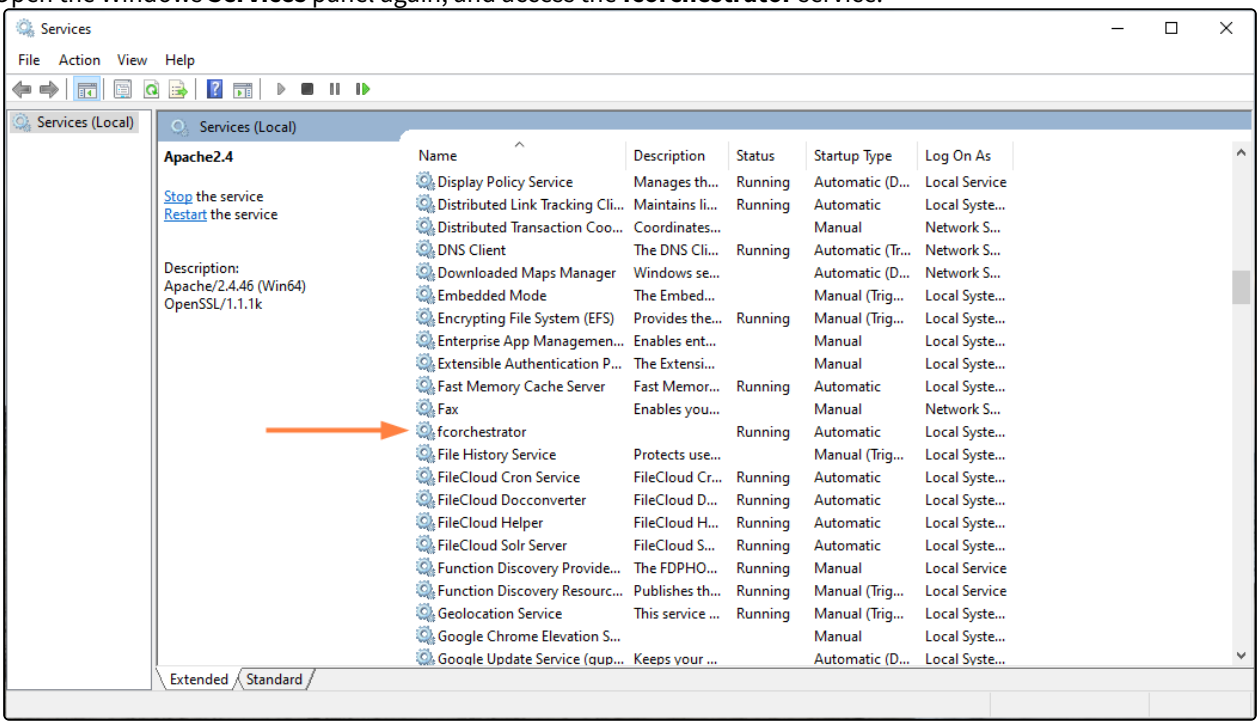
3. Right-click on the service and choose **Properties**.
4. In the **Properties** dialog box, click the **Log On** tab.

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



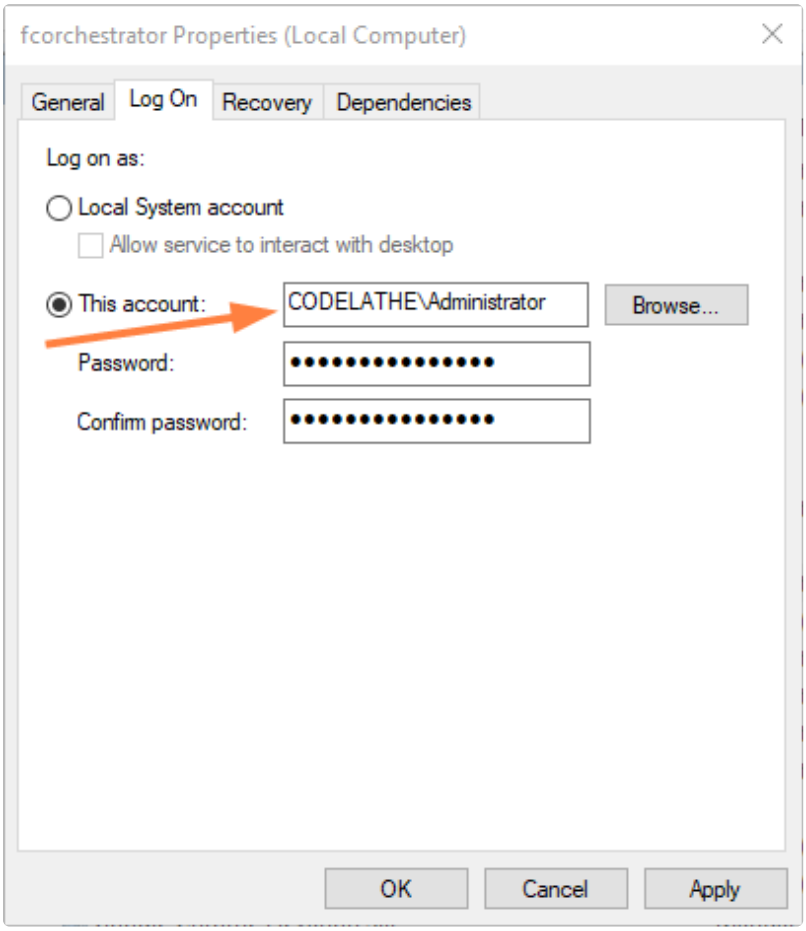
6. Restart the service. Now the web server is running as a user account with full access to the network share.

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



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

that has full access to the network share.



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

Running the Network Share Scanner (Beta)

> The beta version of the Network Share Scanner is available in FileCloud 23.251.1 and later.

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

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

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

The Network Share Scanner is available on both Linux and Windows systems. It is currently in **beta** and requires manual setup. In a future release, the service will be configurable through the FileCloud control panel.

Start/Manage Network Share Scanner

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

Windows

To start the Network Share Scanner in Windows:

1. Navigate to the folder:
   `C:\xampp\eventsapi`
2. Start the Event API and Network Share Scanner (NSS) services by entering:

   ```
   FC-EventApi.exe run
   FC-NSS_Maestro.exe start
   ```

   For more information about running the service, enter:

   ```
   FC-EventApi.exe run --help
   OR
   FC-EventApi.exe --help
   ```

   or

   ```
   FC-NSS_Maestro.exe start --help
   OR
   FC-NSS_Maestro.exe --help
   ```

Linux

To install the Network Share Scanner in Linux:

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

To manage the Network Share Scanner in Linux:

On Linux, the services start automatically after you install them.

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

```
systemctl stop fceventapisystemctl stop fcnetworksharescanner
```

Operation Modes

The Network Share Scanner supports two operation modes:

- **Adaptive Mode**
  (Default) Monitors file system events in real time and updates the index accordingly. If this mode fails, the service falls back to polling.
- **Polling Mode**
  Periodically scans the file system for changes and updates the index.

To change the operation mode:

1. In C:\xampp\eventsapi, open **networker-config.yaml**.
2. Scroll down to the line:

   ```
   watch_strategy: adaptive # adaptive or polling
   ```

   The default setting is **adaptive**.
3. You may change it to **polling** to scan periodically, and change it back to **adaptive** to scan in real time.
4. Restart **FCC-NSS_Maestro.exe** for the change to take effect.

Log management

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

To manage your logs:

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

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

   The settings options are shown in the following table:

Setting	Options
stdout	**false** (default) - do not print logs to command line interface **true** - print logs to command line interface

level	**info** (default) Enter an option to indicate how granular the logs should be. The options, from most granular to least granular are: **debug** **info** **warn** **error** **fatal** **panic**
path	**logs** (default) The path to the log directory. Change to use a different path.
filename	**log.json** (default) The log file name. Change to use a different name.

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

Amazon S3 Bucket Based Network Folders

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

What is an AWS bucket?

Amazon S3 is cloud storage for the internet.

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

Working with Amazon S3 Buckets

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

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

What do you want to do?

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

Create a Network Folder Based on an Amazon S3 Bucket

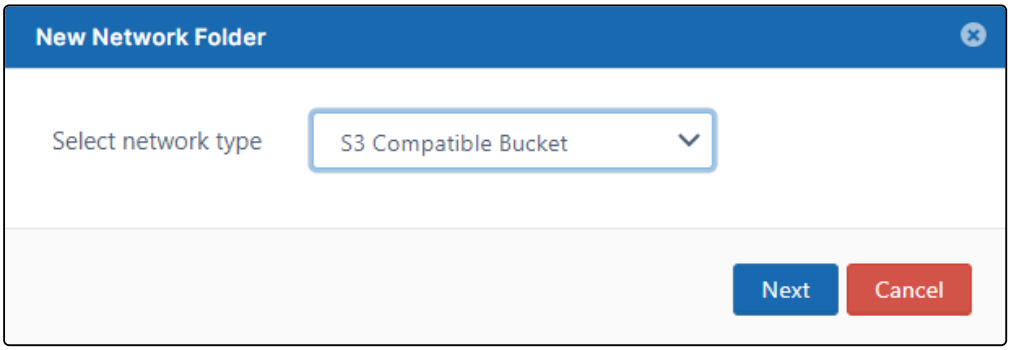
Administrators can integrate Amazon's AWS S3 buckets with FileCloud Server to give users access to this data inside FileCloud Server portals and clients.

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

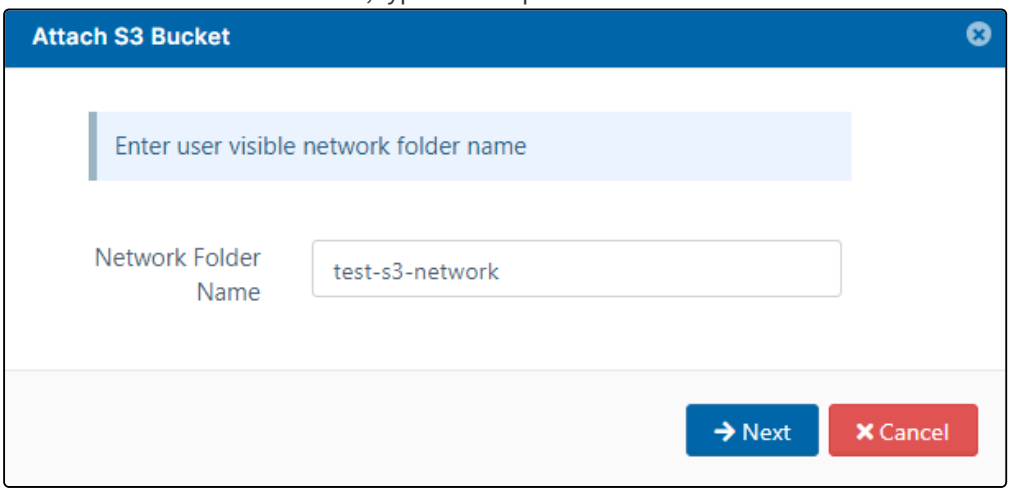
1. There is no versioning support (version key is ignored and file is overwritten).
2. No real time network sync or indexed search is allowed (regular file search works).

To create a network share from an S3 bucket:

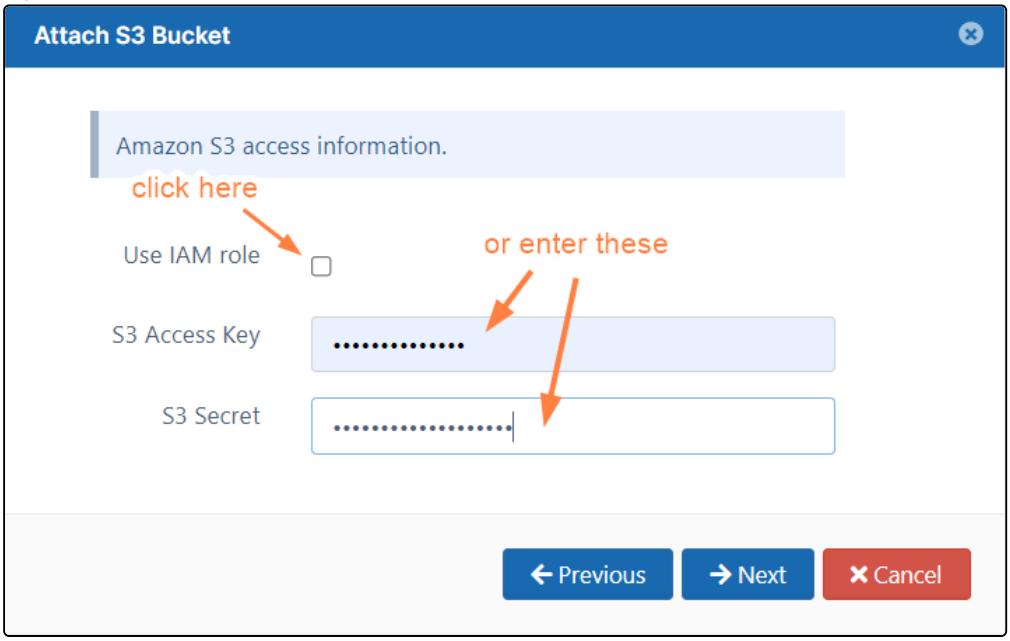
1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



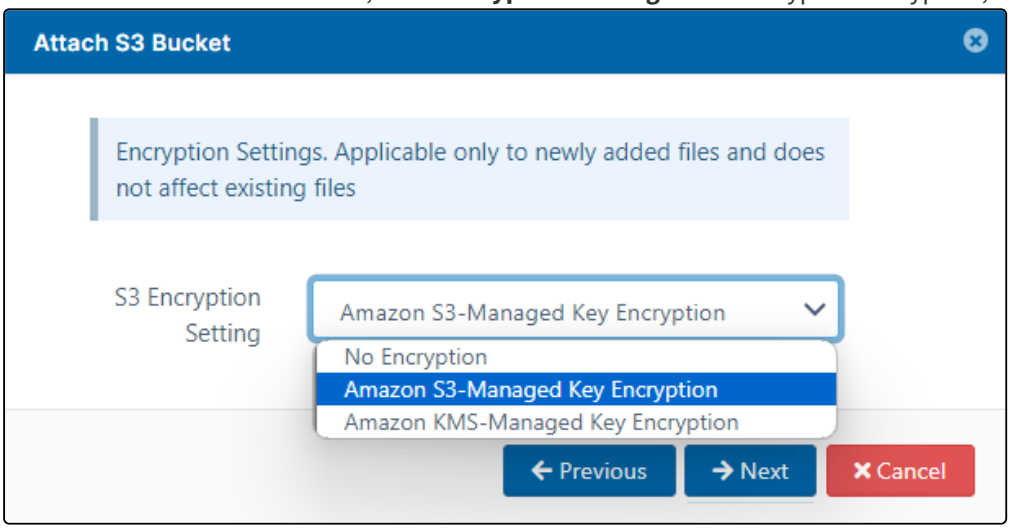
5. On the **Attach S3 Bucket** window, type in a unique **Network Folder Name** and then click **Next**.



6. On the **Attach S3 Bucket** window, either check **Use IAM role** or type in authentication credentials in **S3 Access Key** and **S3 Secret**, and then click **Next**.

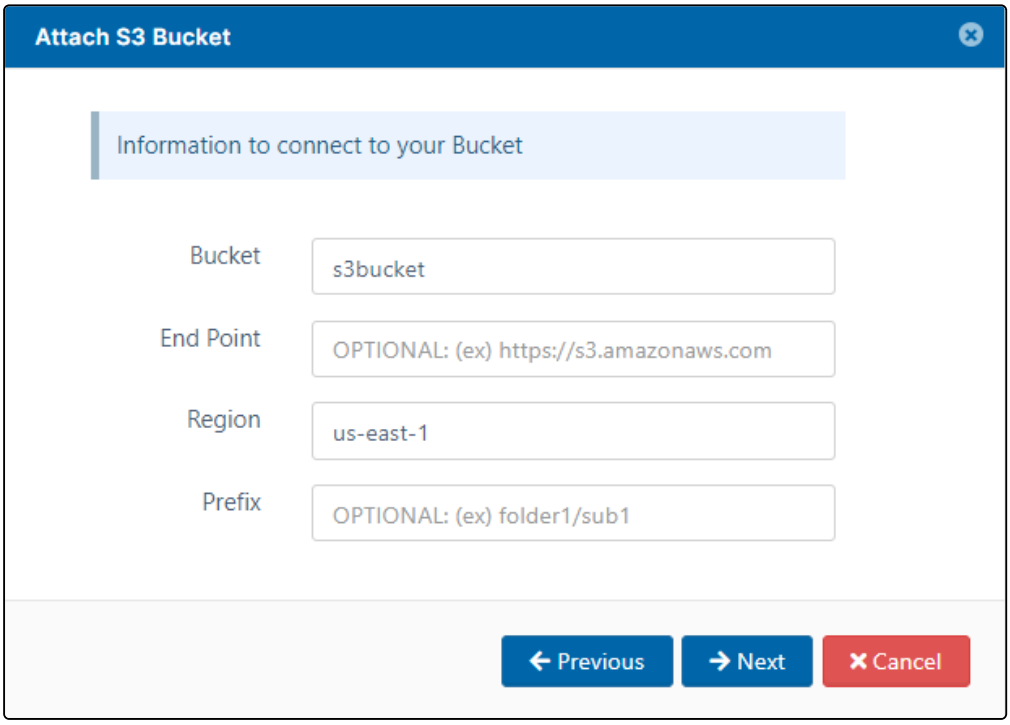


7. On the **Attach S3 Bucket** window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:



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

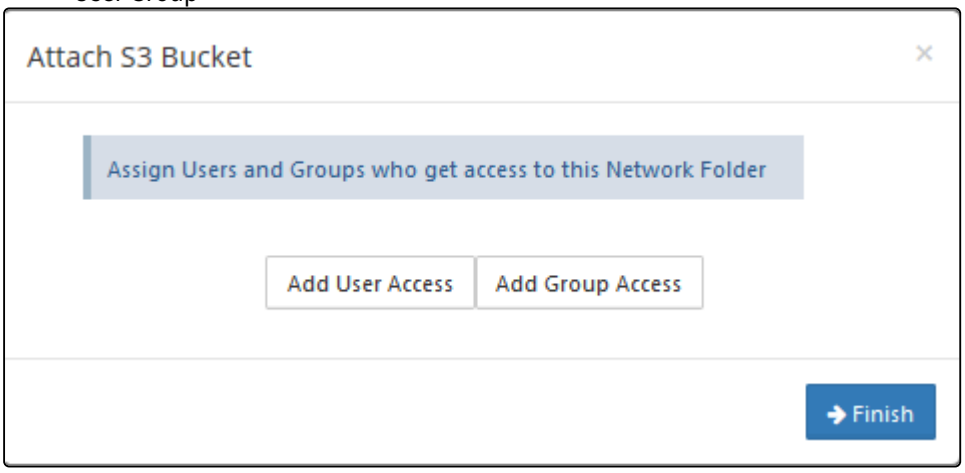
9. Click **Next**.



10. When the S3 bucket is mounted as a network share, permissions need to be assigned to users or groups to allow access.

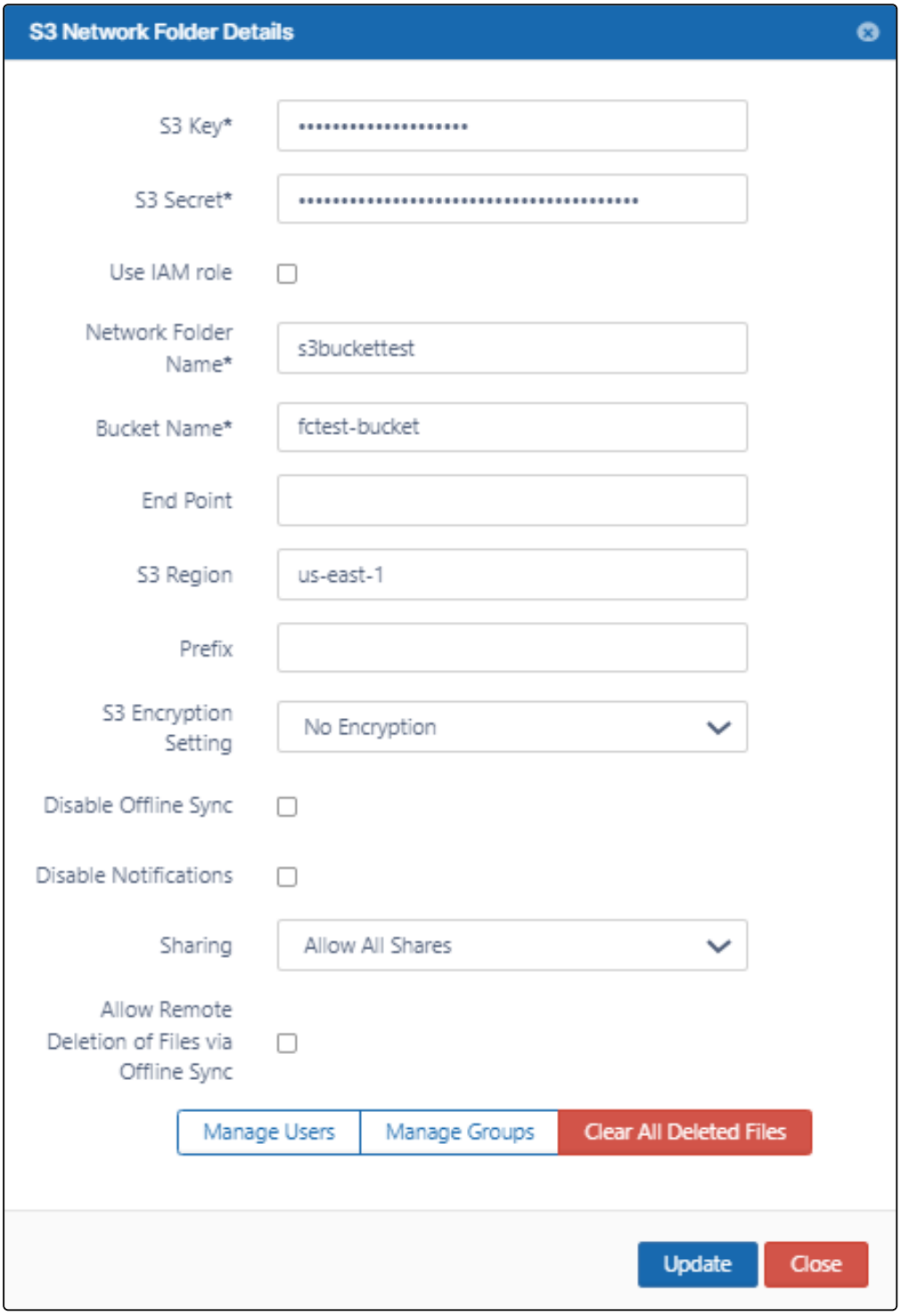
    The network share access can be granted to:

    - Guest User
    - Full User
    - User Group



Configure AWS S3 Bucket-Based Network Folders

After you attach an AWS S3 bucket to a FileCloud Server Network Folder, you can update any of the original settings.

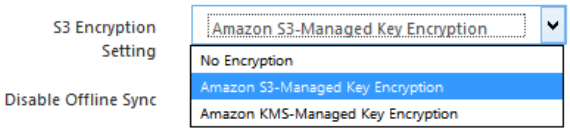
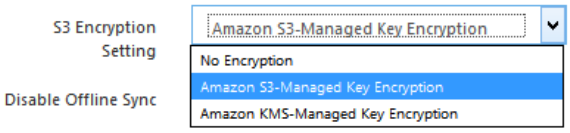


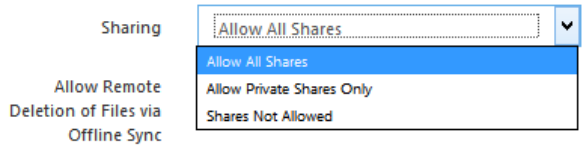
To edit an AWS S3 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the AWS S3 bucket-based network folder, and then click the edit icon ( ).

4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	S3 access key
S3 Secret	S3 secret access key
Use IAM role	Either check **Use IAM role** or type in authentication credentials in **S3 Key** and **S3 Secret**. **Note**: To use an IAM role, you must attach it to your E2 instance. See the page Attach an IAM role to an instance in the AWS documentation for instructions.
Network Folder Name	Display name of network folder
Bucket Name	Name of bucket attached to network folder After September 2020, new AWS bucket names with a "." in them are invalid. However, bucket names with a "." in them created in September 2020 or earlier are still supported. To allow S3 buckets created after September 2020 to have a "." in the bucket name, include the flag **TONIDOCLOUD_S3_USE_PATH_STYLE_ENDPOINT** in the file amazons3storageconfig.php and set it to **1**.
End Point	(Optional) AWS S3 endpoint URL. Leave empty if using Amazon's S3 service; the region string automatically selects the correct endpoint. This value cannot be changed once the bucket is created.
S3 Region	The geographical AWS region where the bucket is created.
Prefix	A prefix to add to the network share paths to create different paths within buckets

Option	Description
S3 Encryption Setting	**No Encryption** When this option is set the files in the S3 network share are not encrypted. **Amazon S3-Managed Key encryption** When this option is set the files are encrypted. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.  **Amazon KMS-Managed Key Encryption** When this option is set the files are encrypted using AWS KMS key. AWS KMS uses customer master keys (CMKs) to encrypt your Amazon S3 network share. You use AWS KMS via the Encryption Keys section in the IAM console or via AWS KMS APIs to centrally create encryption keys, define the policies that control how keys can be used, and audit key usage to prove they are being used correctly.  **Note**: Unlike S3 managed storage encryption, enabling encryption in Network Shares encrypts only newly added files and does not encrypt existing files.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Disable Notifications	Disable some or all S3 Network Folder notifications for users with access to the folders. See Disable notifications for Amazon S3 bucket-based Network Folders, below.

Option	Description
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to S3 bucket when deleted via Sync client.

Configure optimized upload for Amazon S3 Network Folders

When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud 23.241 includes an Optimized Upload feature.

- If you are using Amazon S3 storage for your managed storage in FileCloud, follow the instructions in Setting up FileCloud Managed S3 Storage under **Integrate Amazon S3 Storage**. Make sure you follow **Step 2 (Optional) Configure System to Use Optimized Upload** and **Step 3 Configure Credentials and Settings.** This sets up optimized upload for both S3 managed storage and S3 Network Folders.

- If you are not using Amazon S3 storage for managed storage in FileCloud:
    a. Create a CORS file and confirm that your service address is configured in the .htaccess file.

> **Setting up FileCloud Managed S3 Storage**
>
> When you are using Amazon S3 storage, certain default procedures may cause uploads to be slower and less efficient than necessary. For this reason, FileCloud 23.241 includes an Optimized Upload feature which can be enabled in your system by following the instructions below to configure a CORS policy with the required settings, and to confirm that your service address is in the .**htaccess** file.
>
> **Note: Although Use Optimized Upload and its associated settings appear in the Managed Storage settings page, they also apply to S3 Network Folders.**
>
> **Required CORS policy for Optimized Upload**
>
> To use the Optimized Upload feature, configure a CORS policy for your S3 bucket. The CORS policy enables you to access resources from other domains while you are using the optimized upload settings.

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

To configure the CORS policy:

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

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

v. Click **Save**.

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

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

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

iii. Restart the FileCloud server.

b. Set up Optimized Upload in your managed storage settings. On page Setting up Managed Storage, read the instructions for the **Use Optimized Upload** setting in the table to configure your S3 Network Folders to use optimized upload.

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

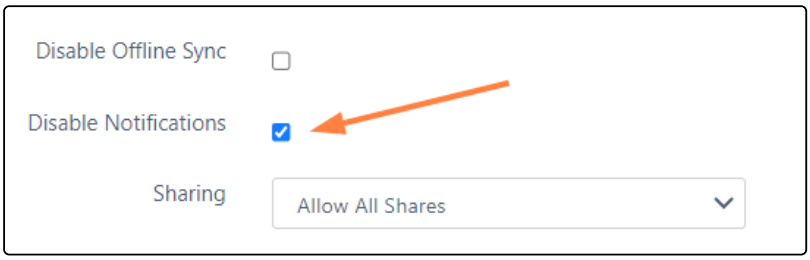
Disable notifications for Amazon S3 Network Folders

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

However, since multiple users may have access to the same network folder, users may receive notifications about actions that don't interest or don't apply to them.

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

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



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

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

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

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

Clearing Deleted Files from S3 Network Folders

Administrators can clear the files deleted by users in Network Folders.

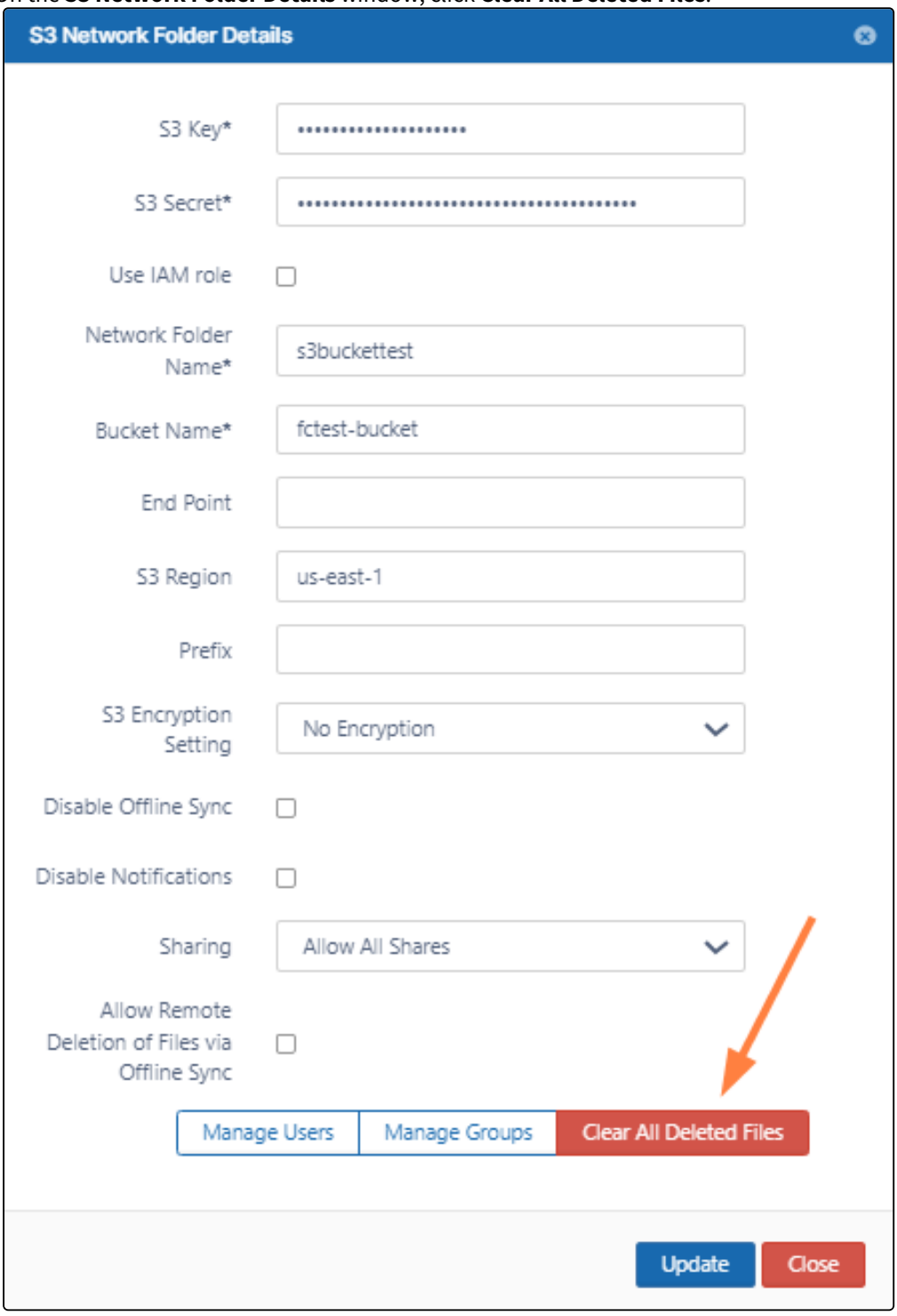
Why?

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

To clear deleted files in an S3 Network Folder:

1. Open a browser and log on to the admin portal.
2. In the left navigation panel, click **Network Folders**.
3. In the **Manage Network Folders** window, click the row containing the folder you want to clear of deleted files.
4. Click the edit icon ( ).

5. On the **S3 Network Folder Details** window, click **Clear All Deleted Files**.



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

Azure Blob Storage Based Network Folders

Administrators can integrate 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.

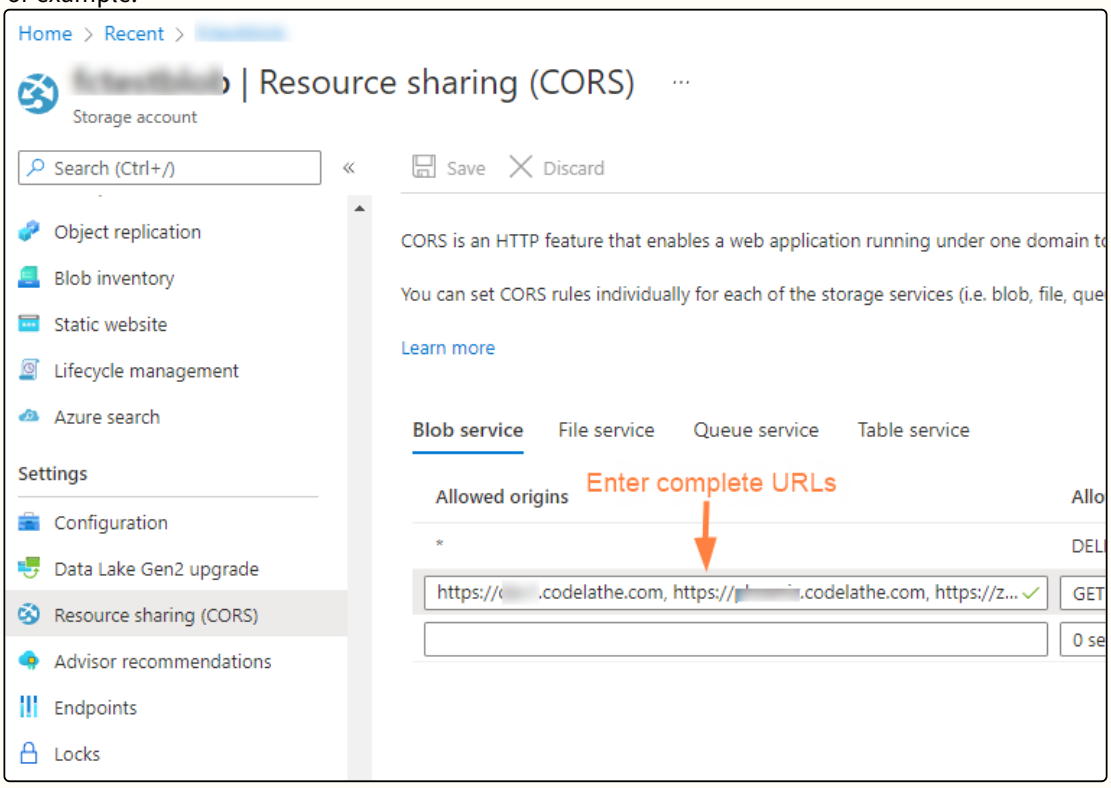
You can then upload any number of objects to the bucket.

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

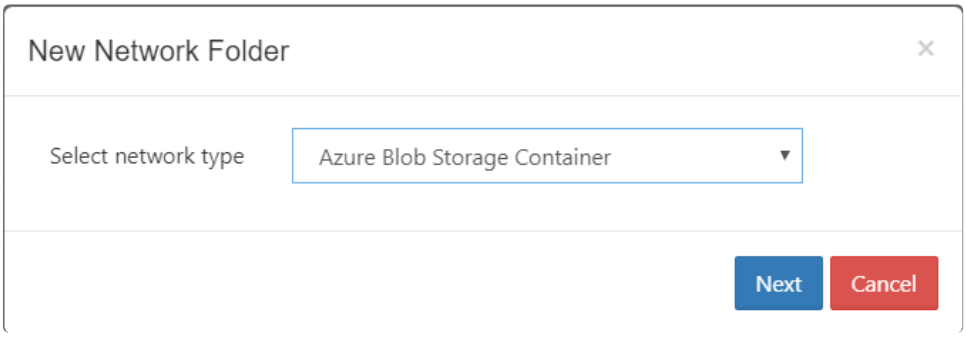
Create a Network Folder Based on an Azure Blob Storage

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

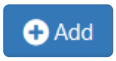
Administrators can integrate Azure Blob Storage container with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

⚠ 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)

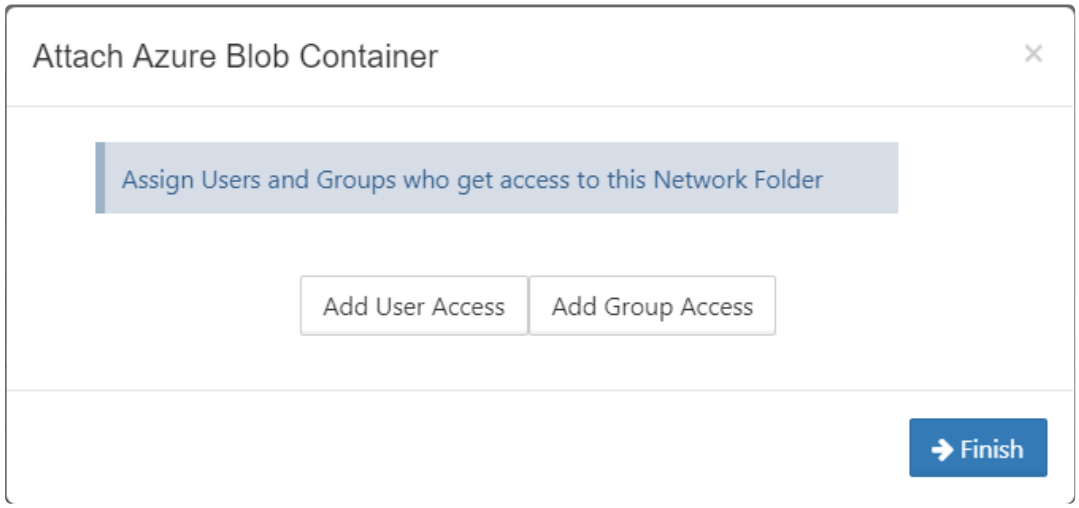


To create a network share from the Azure Blob Storage Container:

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 ().

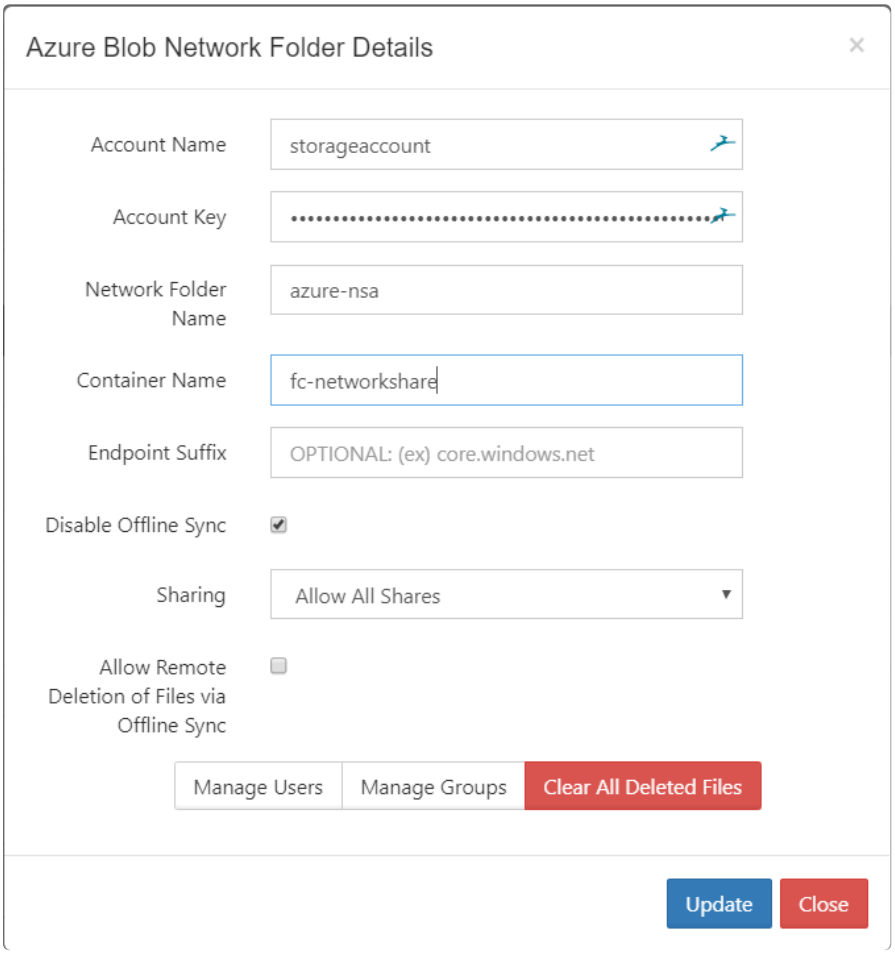
4. On the New Network Folder dialog box, in Select network type, select Azure Blob Storage Container, and then click Next.
5. In the **Enter User Visible Network Folder name** step, type in a unique name for the Network Folder and then click Next.
6. In the **Azure Blob Storage access information** step, 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:
    - Guest User
    - Full Access User
    - User Group



Configure Azure Blob Storage Container-Based Network Folders

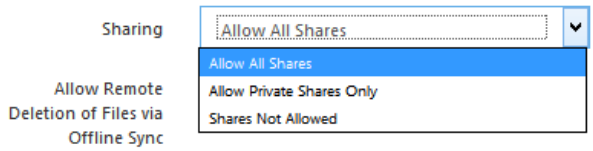
After you attach an Azure Blob Storage container to a FileCloud Server Network Folder, you can update any of the original settings.



To edit an 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

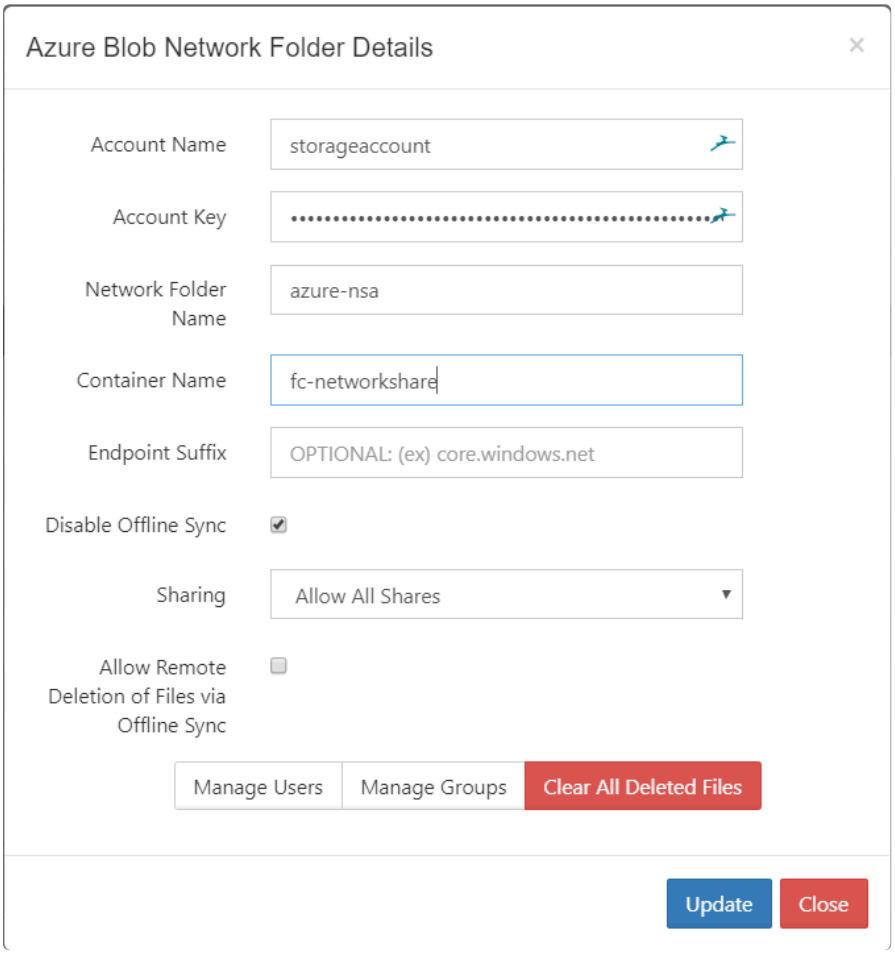
Option	Description
Container Name	Name of the container - it has to exist in Azure when creating a share
Endpoint Suffix	Endpoint suffix. To use an Azure end point, it must be one of the values published here.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the Azure Blob Storage container if the files are deleted in the synced client. By default deletes are not propagated to Azure Blob Storage container when deleted via Sync client.

Clearing Deleted Files from Azure Blob Storage Network Folders

Administrators can clear the files deleted by users in Network Folders.

Why?

The files deleted by users that are moved to the recycle bin (if enabled) take up space over time.



To clear deleted files in an 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 that exceed 255 characters:** When using network folders on Windows, file paths that exceed 255 characters cannot be processed.
To fix this problem use the prefix \\?\ in front of your Network Folder path. Using this prefix enables you to use paths of up to 1024 characters.
With the prefix, the path is formatted as:
\\?\C:\[Network Folder name]

  Note: FileCloud Drive and FileCloud Sync can handle paths of up to 32,000 characters in Windows. However, in some cases, this may be limited by the application or the server.

- **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

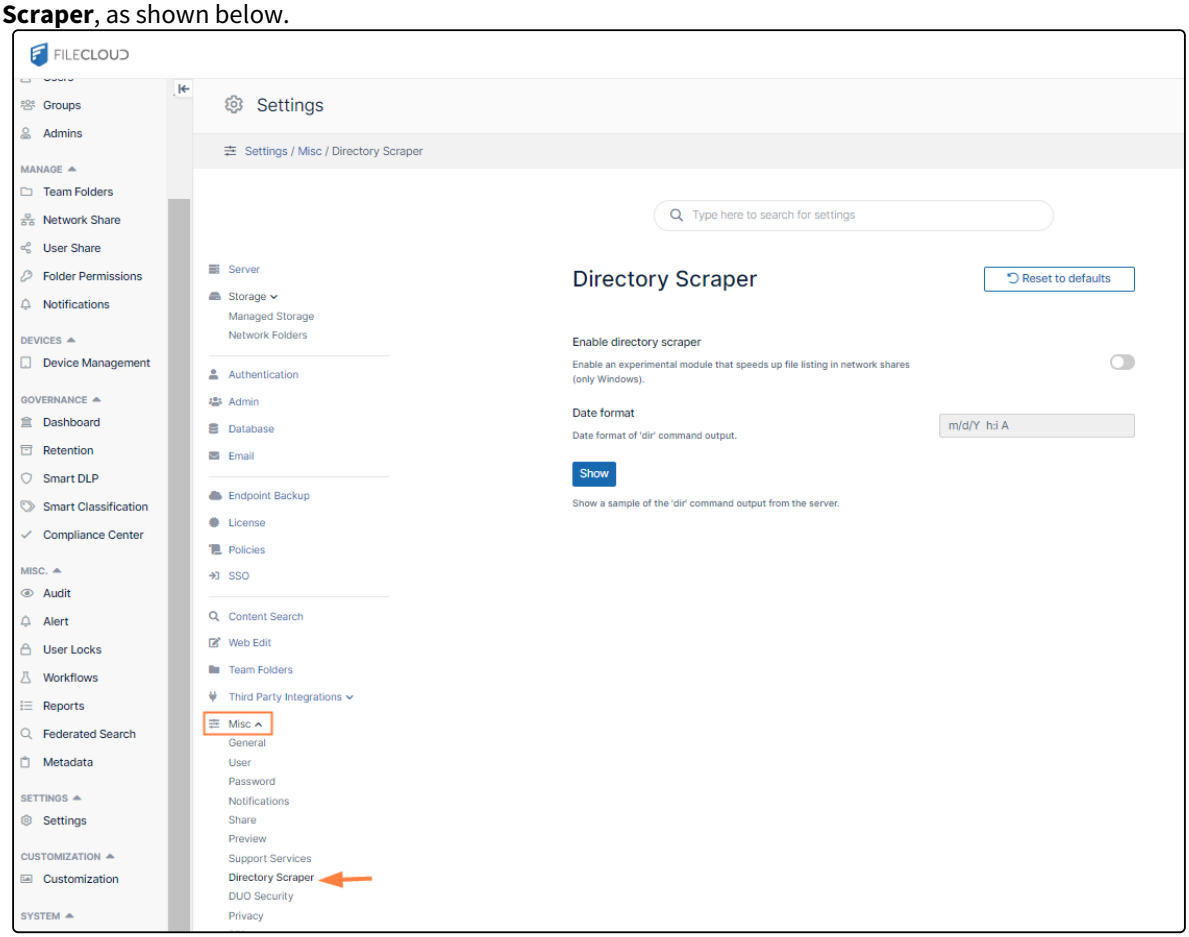
FileCloud allows you to share network folders with any number of users. If FileCloud is running on Windows OS but the network folders are on a slower network, then listing of files/folders in network shares will be very slow.
To list network files and folders more quickly, enable directory scraping.

Enabling Directory Scraping

1. Open the Directory Scraper settings page.
   To open the Directory Scraper settings page

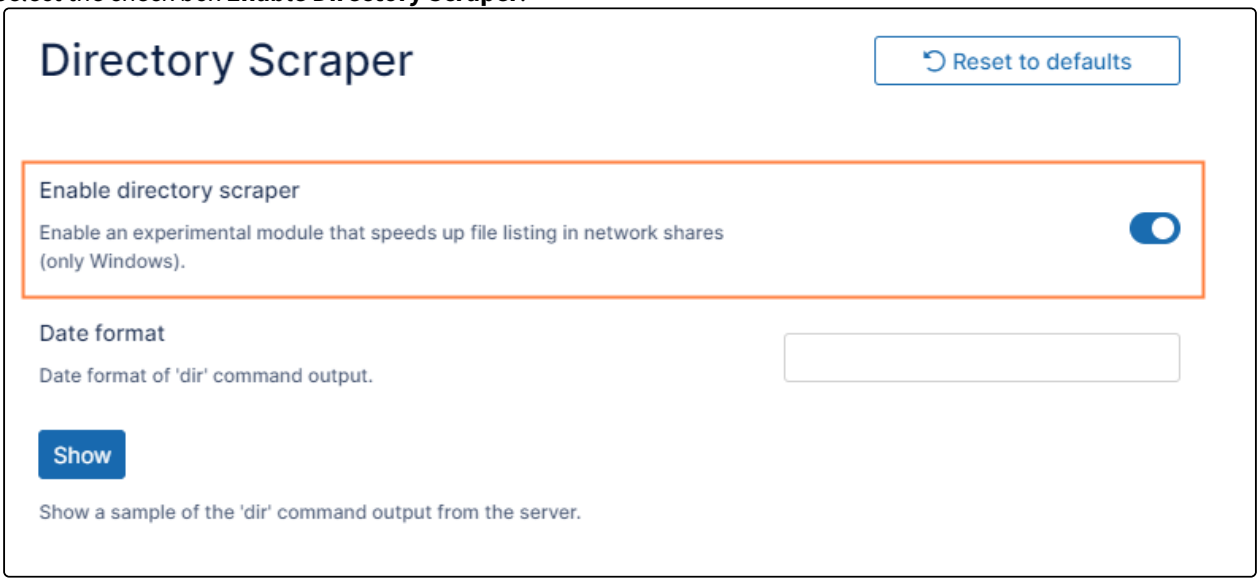
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Directory Scraper**, as shown below.



The **Directory Scraper** settings page opens.

2. Select the check box **Enable Directory Scraper**.



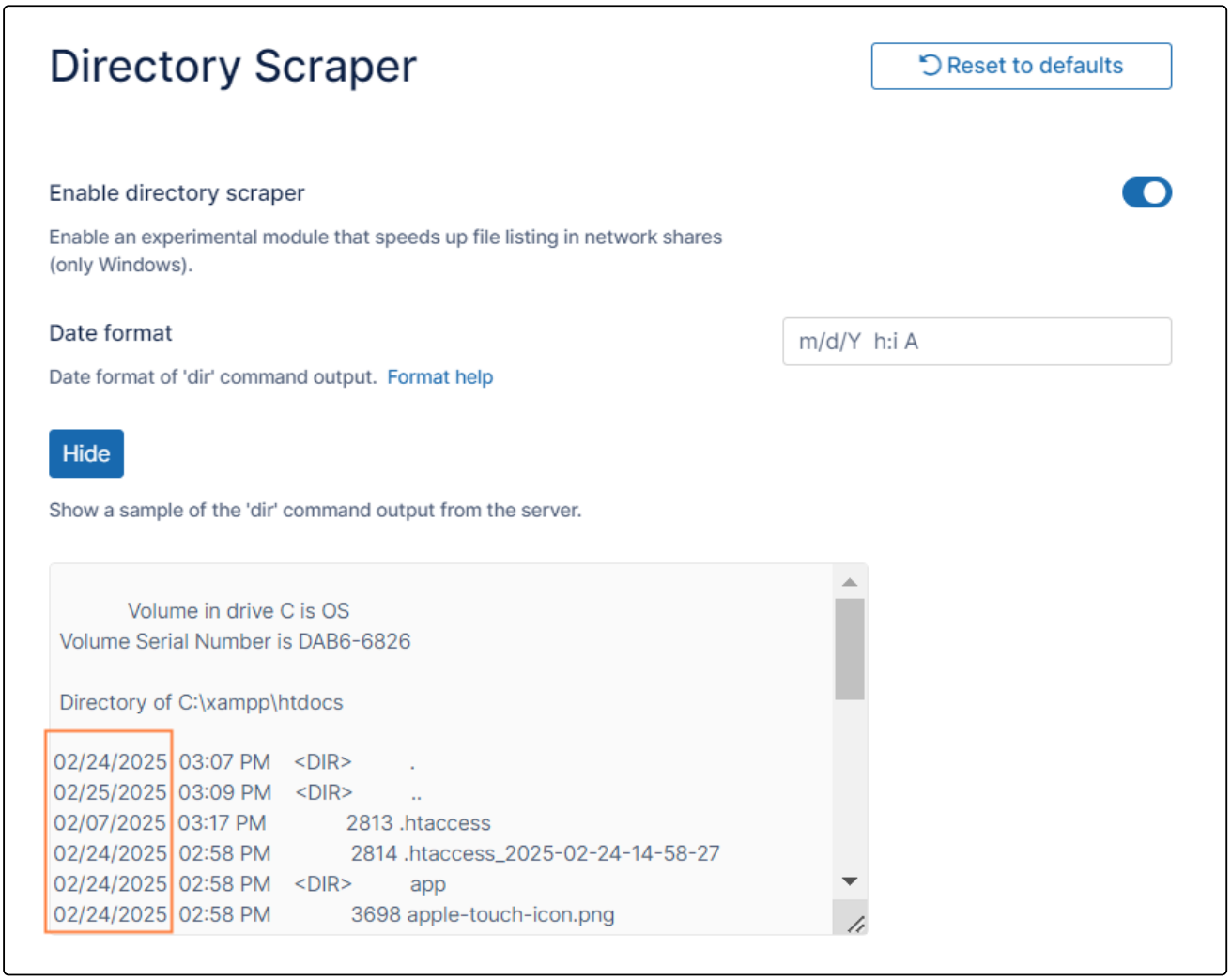
3. Correct the system date format, if needed. See To find the date format, below, for help finding your system date format.
4. Click **Save**.
   Now network shares will use directory scraping to get file listings.

To find the date format:

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

To see the correct date format, click **Show**.

You are shown a sample of server output from the dir command, which includes the formatted date for you to reference.



FileCloud Helper Service

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

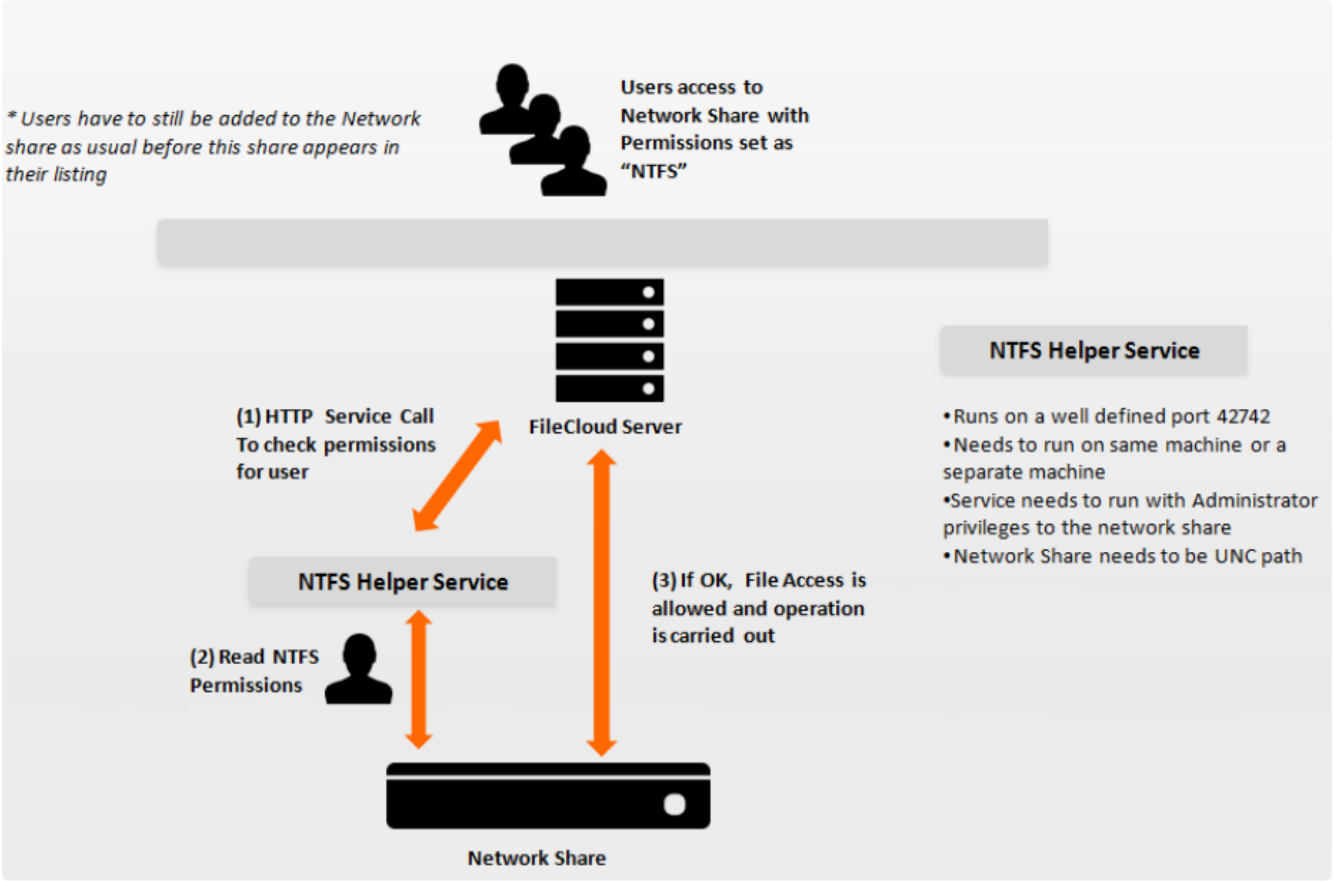
- Handle NTFS Permission checks for Network Folders configured with NTFS permissions (Only needed under some conditions after v12.0)
- Provide an indexed search of Network Folders
- Allow content search of documents for Network Folders

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.

What Do You Want to Do?

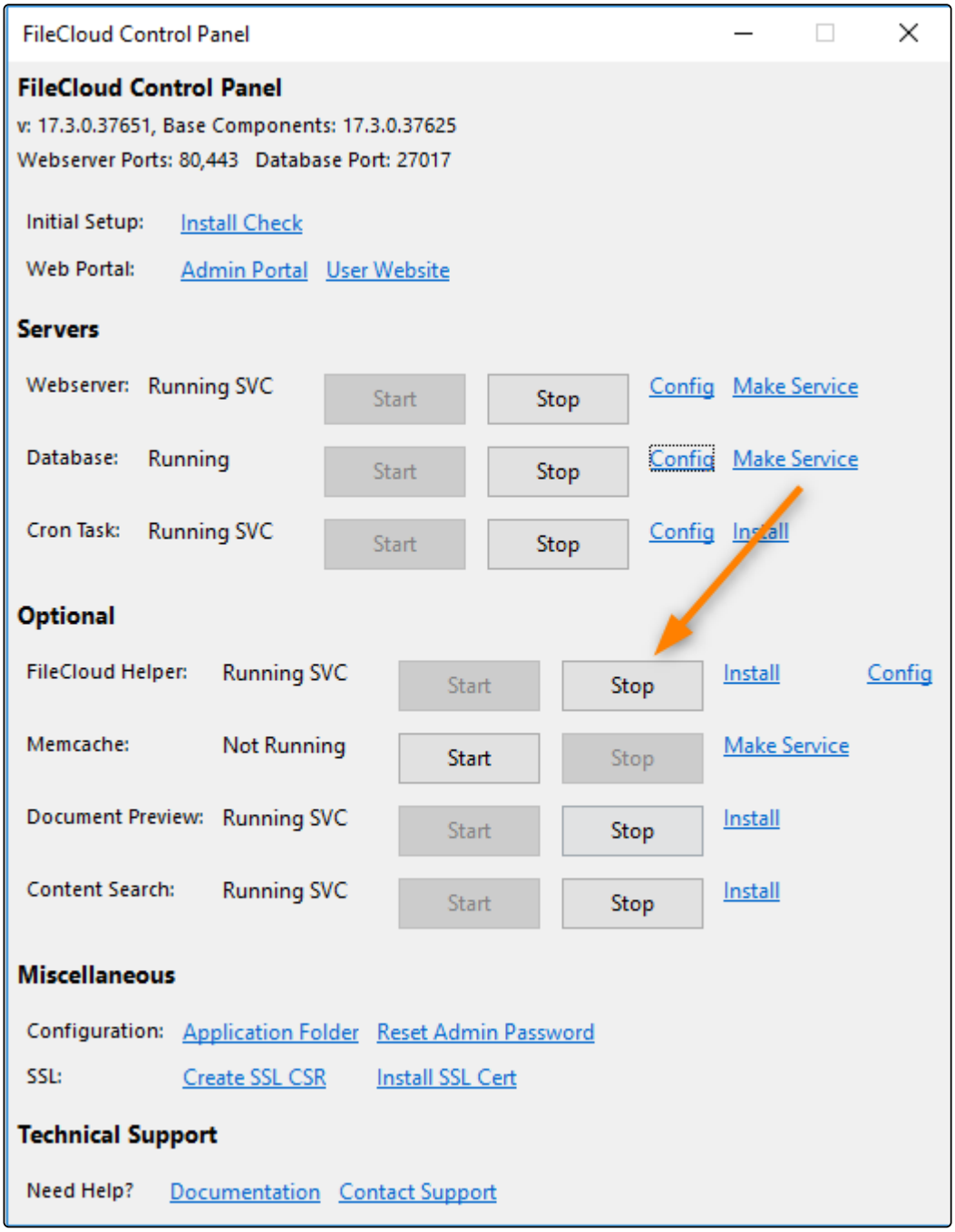
Learn about FileCloud NTFS Helper Architecture
Install Helper Service
Run Server and Helper and Different Machines
Exclude Specific Folder Paths from Indexing
Improve Helper Performance

Helper Service Architecture



Install Helper Service

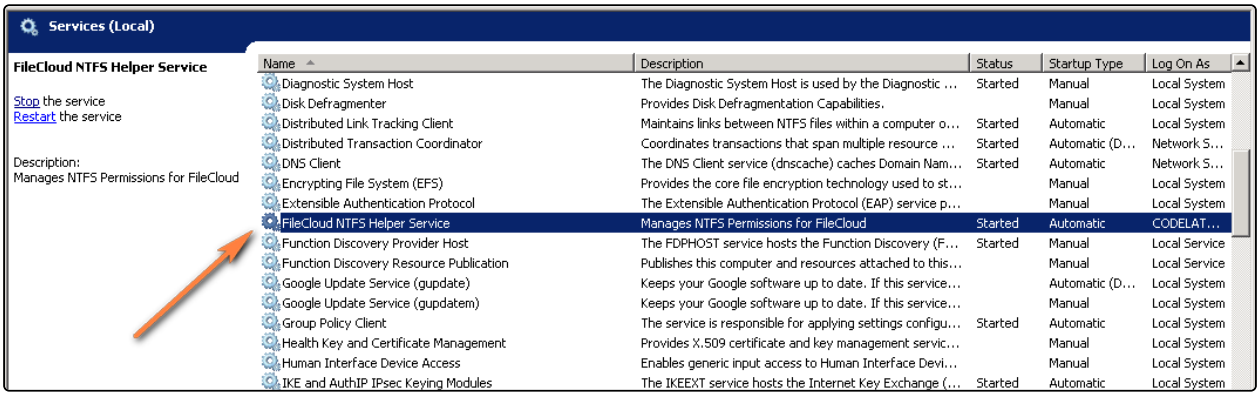
For FileCloud Server instances running on Windows, Helper service is a separate installation.



To install the FileCloud Helper service:

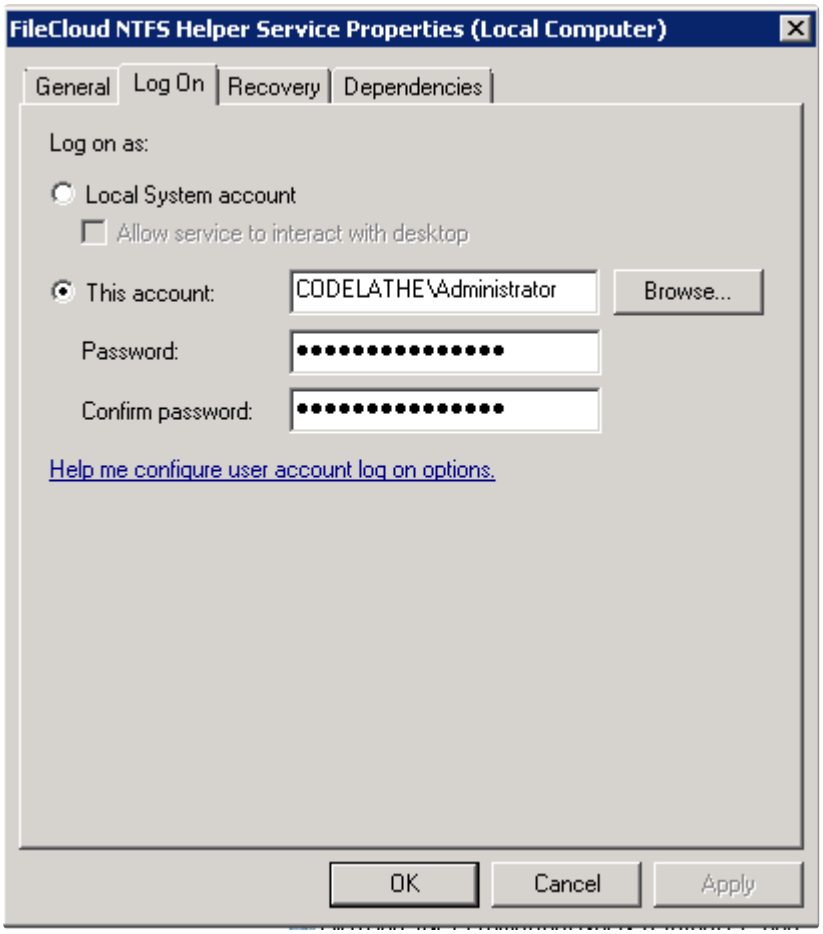
1. The download link for this service can be found in the customer portal. FileCloud helper service can also be installed from the FileCloud control panel using the install link.

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



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

Important: Note that this service cannot work properly when operating as a local system account. It has to run as a specific user account with permissions to the network share folder that is being shared via FileCloud.



Exclude Folder Paths from Indexing

As an administrator, you may see errors when FileCloud Helper service indexes Network Folders.

- FileCloud Server may return exceptions instead of skipping folders during real-time indexing of Network Folders for the specific paths.
- The best way to tell Helper service that you want to ignore some folders when indexing is to add regexes (regular expressions) paths to the folders.

To exclude files or folders from indexing:

1. Open the following file for editing

   ```
   realtimeconfig.ini
   ```

2. Add the following line, replacing REGEX with a path to the files or folders that you want to skip during indexing of Network Folders.

   ```
   skipregex=REGEX
   ```

For example:

The following line tells the Helper service to ignore all files in the Network Folders sub-folder called **archived**.

```
skipregex=mynetwork/ntfs/archived
```

Run Server and Helper on Different Machines

Normally FileCloud and Helper are run on the same machine.

- If you are running FileCloud on Linux, then it is impossible to run Helper on Linux as well.
- In this case install the Helper on a Windows machine.

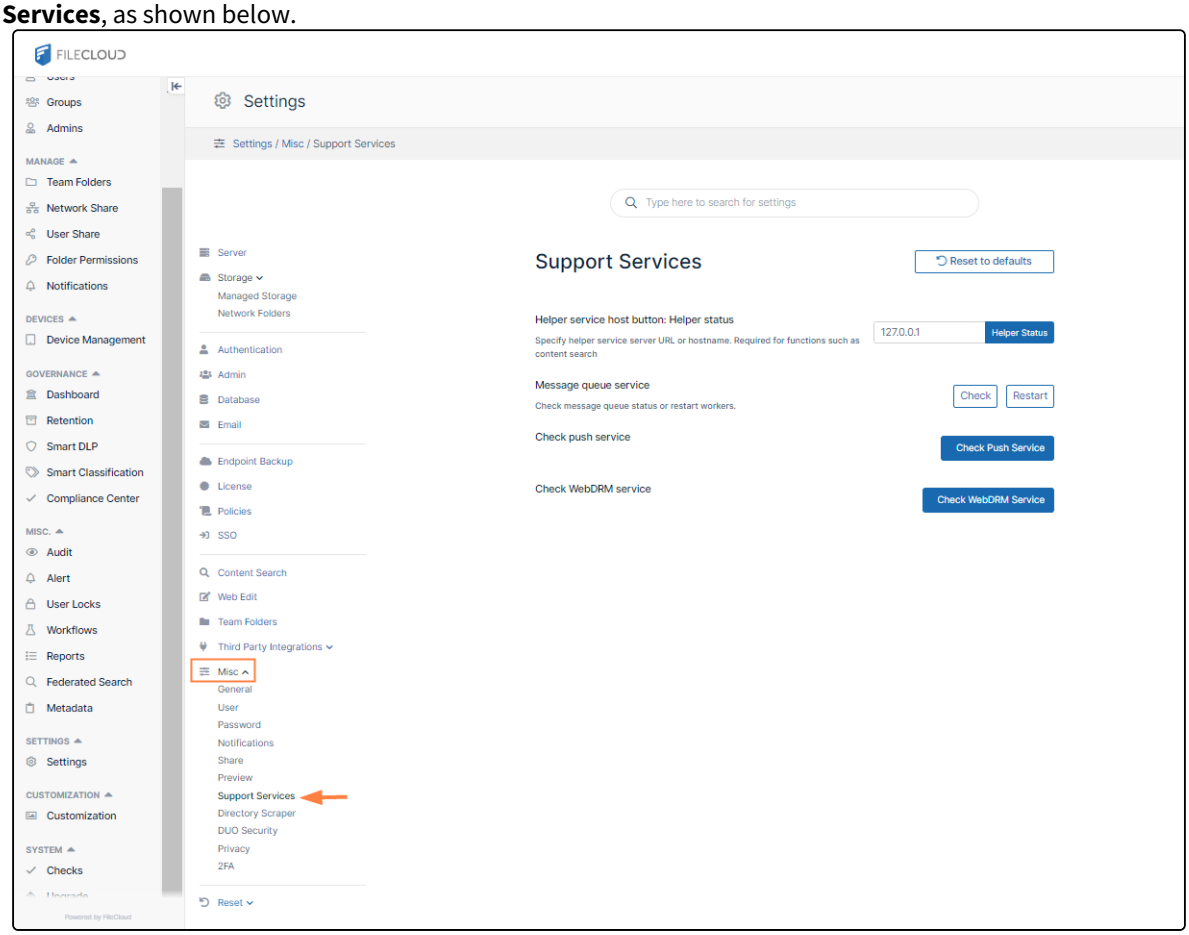
You can use these steps to configure the FileCloud Server with the right location and map path information required.

💡 It is recommended that if possible you run both Helper and FileCloud on Windows.

To configure FileCloud Server to Find Helper on Another Machine:

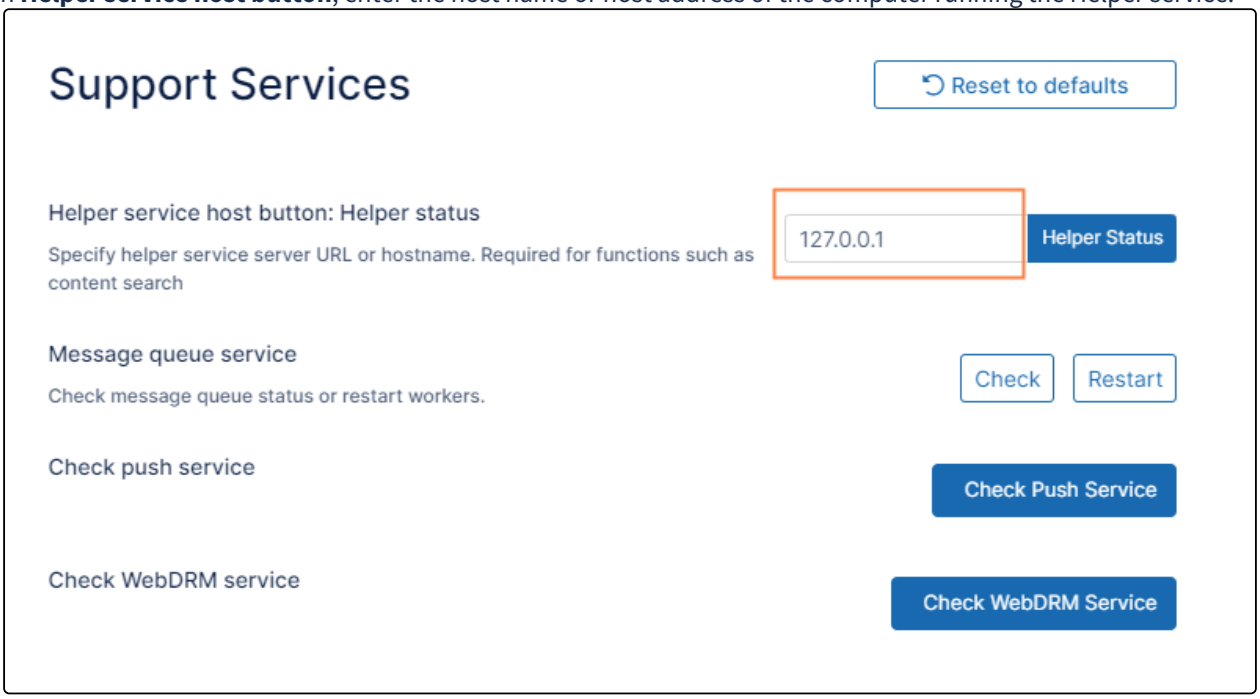
1. Open the Support Services settings page.
   To open the Support Services settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Support Services**, as shown below.



The Support Services settings page opens.

2. In **Helper service host button**, enter the host name or host address of the computer running the Helper service.



3. Click **Save**.
4. On the Helper server, open the following location:

```
%appdata%\FileCloudHelper
```

5. Edit or create (if not available) config.ini in the install folder and change the following lines:

```
; Settings for FileCloud Helper
[settings]
address=0.0.0.0
```

6. Edit the pathmap.ini file and add the network path to the same path used by Linux but accessed by Windows:

```
; Path maps for FileCloud Helper
; Example format is <remote path> = <local path>
; e.g. /network/share1=\\share1comp\sharedfolder\share1
[pathmaps]
/mnt/share1=\\share1comp\sharedfolder\share1
```

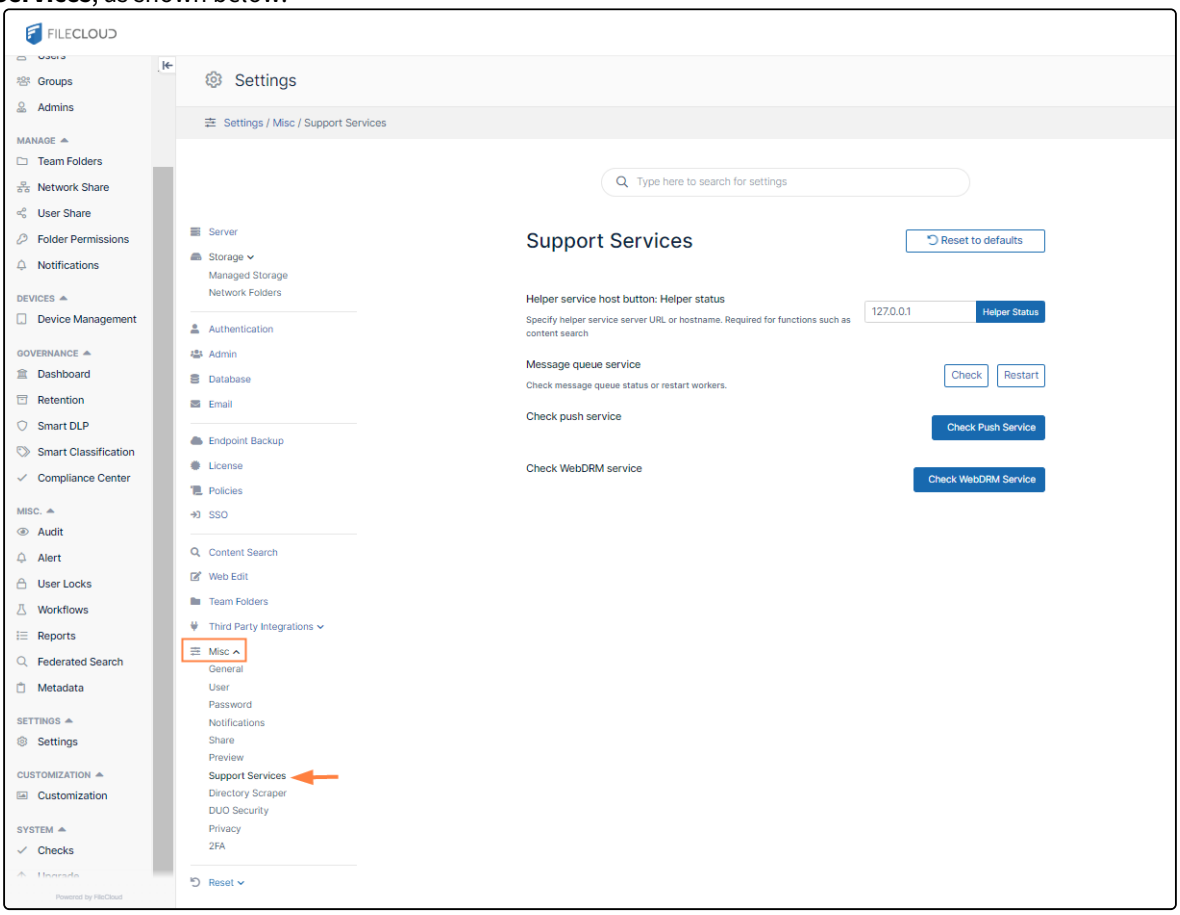
7. Restart the FileCloud Helper service.

Improve Helper Performance

As an administrator, you can use built-in tools to check the status of the service and you can also increase the expiry time of the cached results so that existing results can be returned faster.

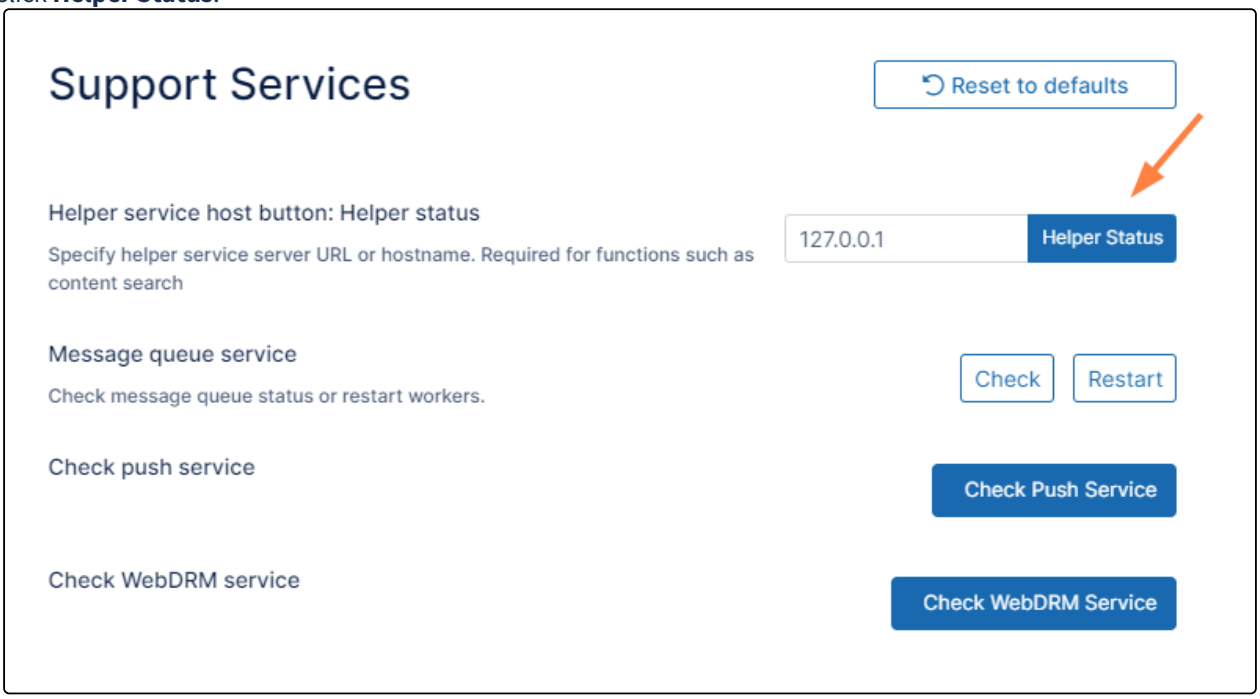
To check the status of Helper Service:

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

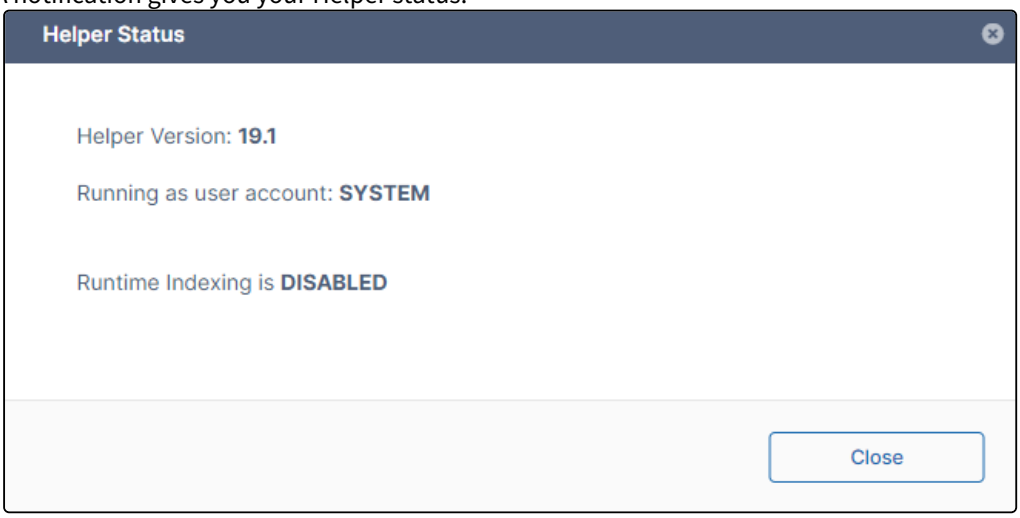


The Support Services settings page opens.

2. Click **Helper Status**.



A notification gives you your Helper status:



Return Permission Results Faster

By default, Permissions check results are cached for 30 seconds.

- For systems where the permissions are not changing dynamically, you can increase the expiry time of the cached results.
- 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

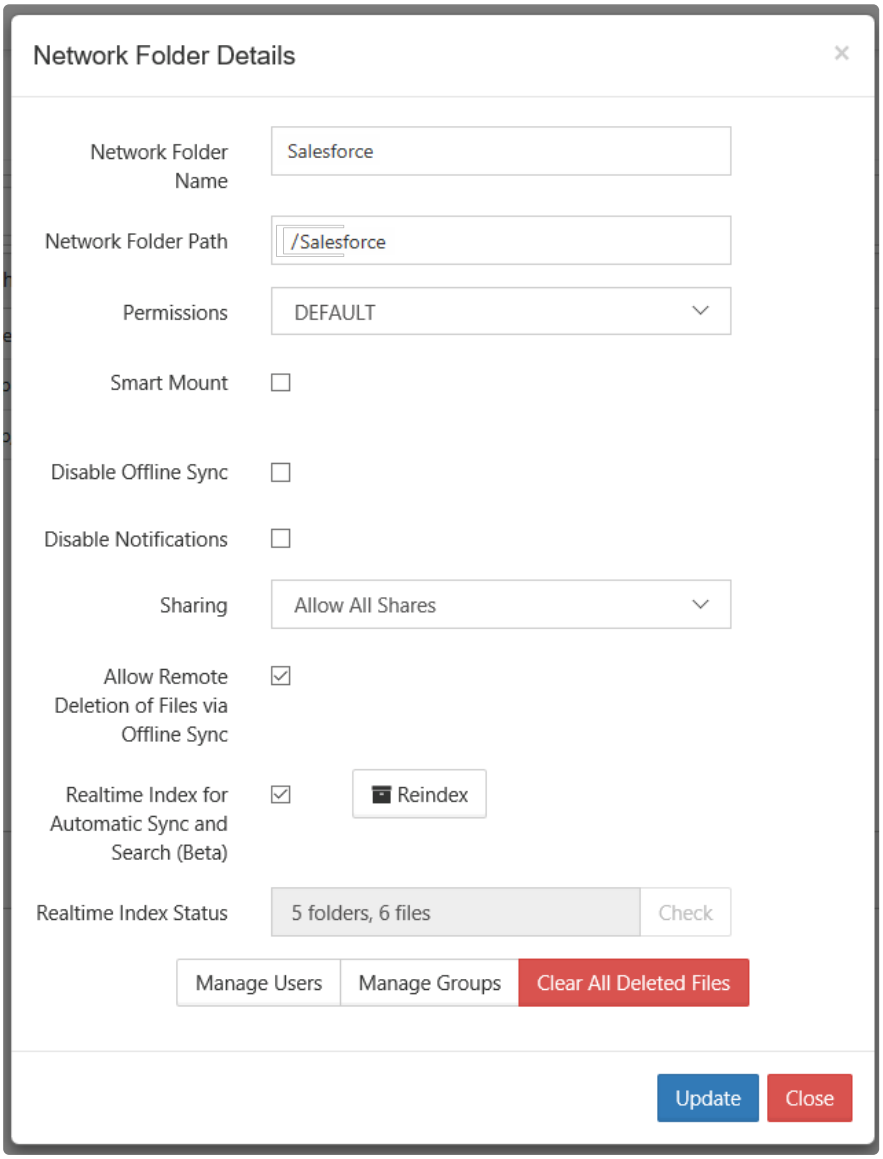
Parameter	Notes	Default Value
cacheexpiry	specifies how long cached results are stored in memory for faster performance. Specified in microseconds	30000 us (30 secs)
threadpoolsize	specifies the number of threads pre-created in the threadpool for fast spin up	40
threadmaxqueued	sets the maximum number 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.



To clear deleted files in Network Folders:

1. Open a browser and log on to the **Admin Portal**.
2. On the left navigation pane, under **Manage**, click **Network Folders**.
3. On the **Manage Network Folders** window, click the row containing the folder you want to clear of deleted files.
4. Click the edit icon ( ).
5. On the **Network Folder Details** window, click **Clear All Deleted Files**.
6. To save your changes, click **Update**.

Display Names that Start with a Dot

As an administrator you have the option to display files and folders that have a name starting with a (.) dot.

- This option can be set for network shares.

By default, if you:

- Create a network share from a folder that has a name starting with a dot (.), for example, .SystemTest
- Share it with another user
- When the user browses to the share the folder will not be displayed and it will appear empty

Similarly, if you:

- Create a network share from a folder with a name that does not start with a dot (.), for example, AdminTest
- Create files inside this folder that have a filename that starts with a dot (.), for example .Atest1, .ATest2
- Share it with another user
- When the user browses to the share the folder will be displayed but the files inside will not and it will appear empty

To display folders and files that start with a dot (.) :

1. Open the following file for editing:

```
cloudconfig.php
```

2. Add the following line:

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

3. Refresh User Portal web page and the folders and files are now visible.

Wasabi S3 Bucket Based Network Folders

⚠ FileCloud officially supports only Amazon S3 storage to be configured as Network Folders.
- Other Amazon S3 compatible storage systems are supported through our Amazon S3 drivers, including:
  - Wasabi
  - Backblaze B2
  - Cloudian
- The robustness of these S3 compatible storage systems depends on their compatibility with Amazon S3 API.

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

What is a Wasabi bucket?

Wasabi S3 is cloud storage for the internet.

To upload your data (photos, videos, documents etc.), you first create a bucket in one of the Wasabi Regions.

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

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

1. No versioning support (Version key will be ignored and the file will be overwritten)

2. No real-time network sync or indexed search is allowed (Regular file search will work)

What do you want to do?

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

Create a Network Folder Based on an Wasabi S3 Bucket

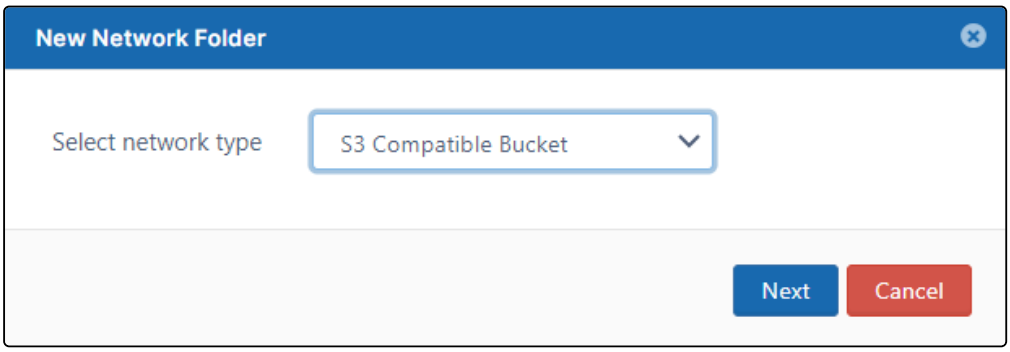
Administrators can integrate Wasabi S3 buckets with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients.

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

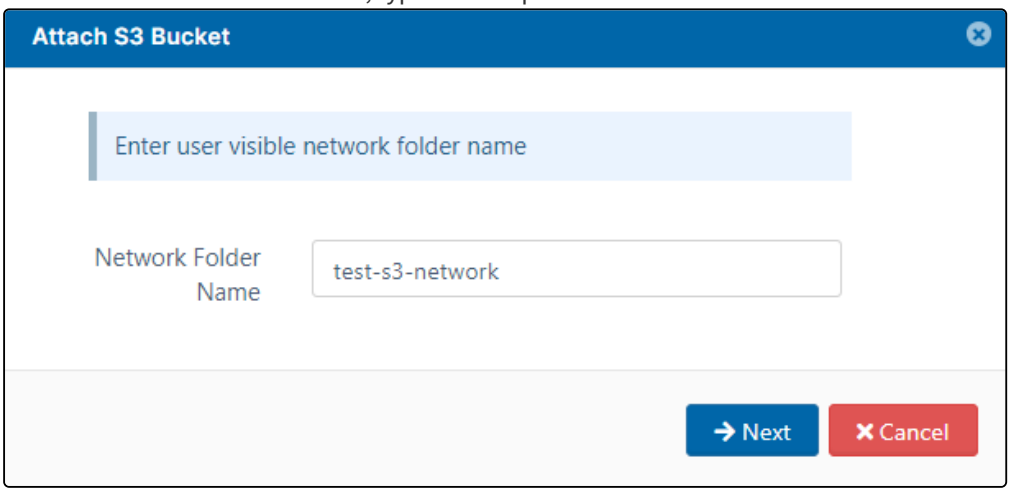
1. No versioning support (Version key will be ignored and the file will be overwritten)
2. No real-time network sync or indexed search is allowed (Regular file search will work)

To create a Network Folder from an S3 bucket:

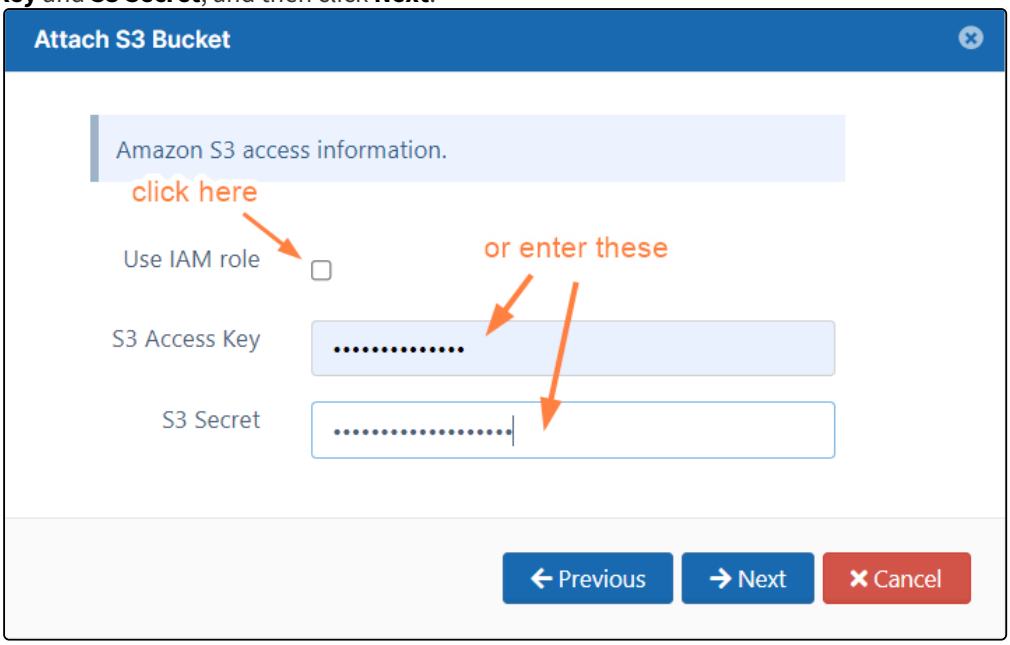
1. Open a browser and log in to the Admin Portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



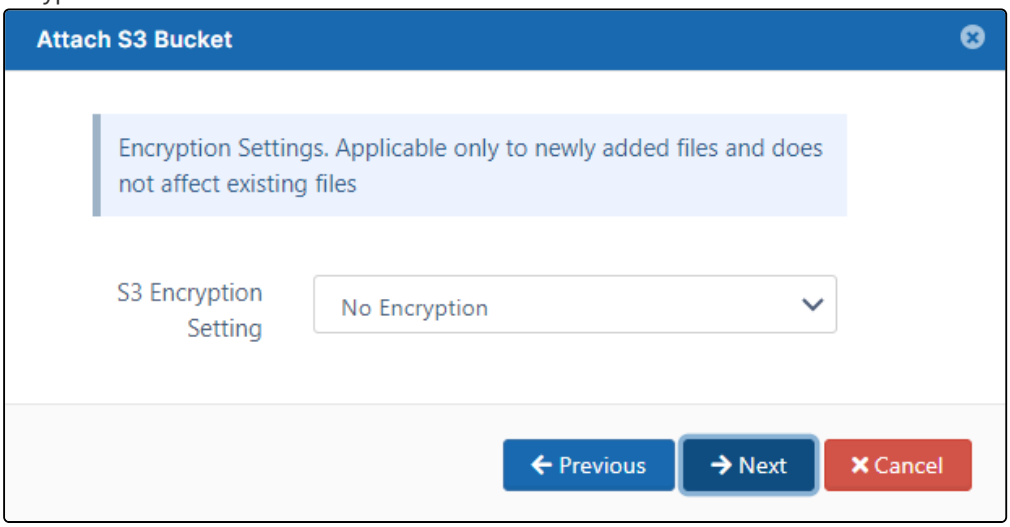
5. On the **Attach S3 bucket** window, type in a unique **Network Folder Name** and then click **Next**.



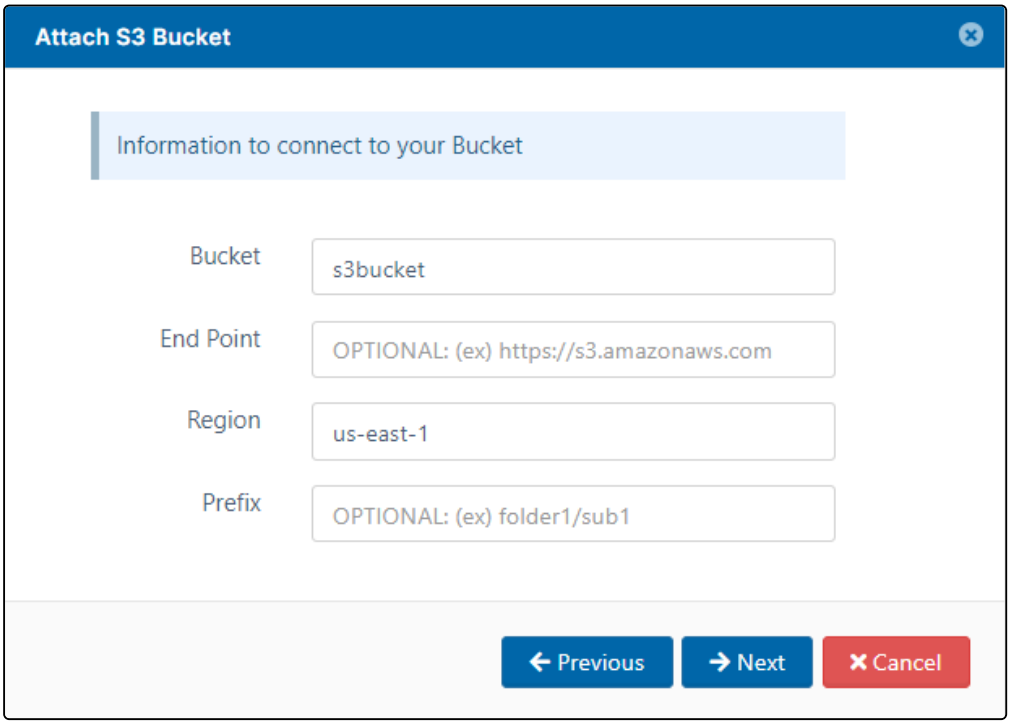
6. On the **Attach S3 Bucket** window, either check **Use IAM role** or type in authentication credentials in **S3 Access Key** and **S3 Secret**, and then click **Next**.



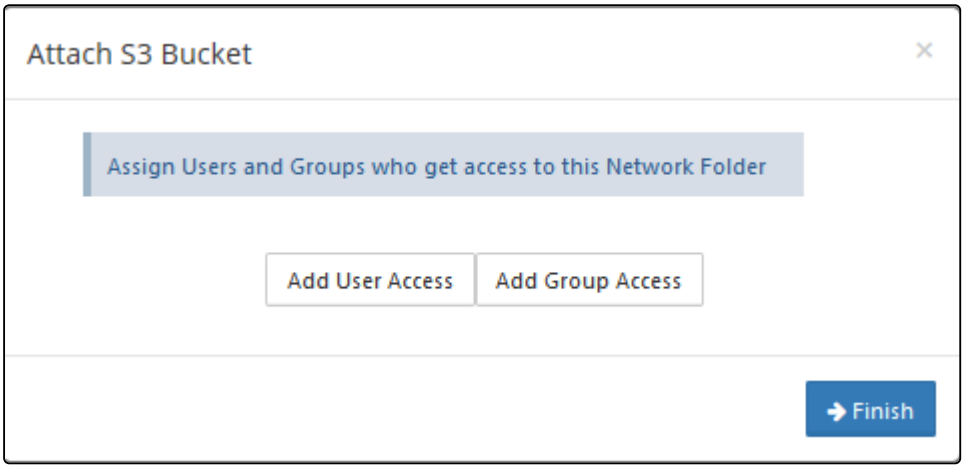
7. On the **Attach S3 bucket** window, select **No Encryption** because Wasabi does not provide managed key encryption as AWS does.



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

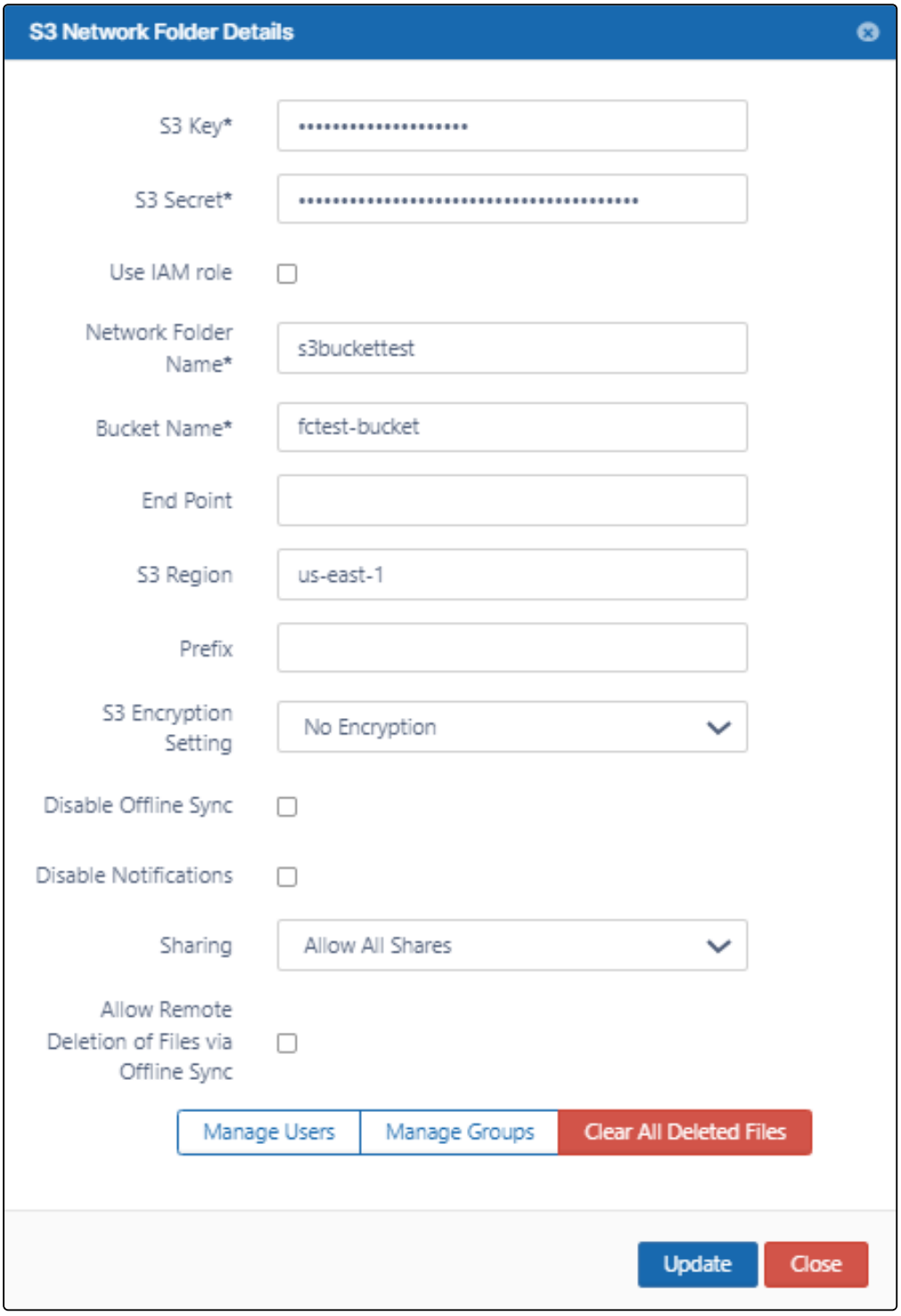


10. When the S3 bucket is mounted as a network share, permissions need to be assigned to users or group to allow access.
    The network share access can be granted to
    a. Guest User
    b. Full User
    c. User Group



Configure Wasabi S3 Bucket-Based Network Folders

After you attach a Wasabi S3 bucket to a FileCloud Server Network Folder, you can update any of the original settings.



To edit a Wasabi S3 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Wasabi S3 bucket-based network folder, and then click the edit icon ( ).

4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
S3 Region	Physical region where buckets are created.
End Point	URL where API requests are sent.
S3 Encryption Setting	On the **Attach S3 bucket** window, select the type as **No encryption** because Wasabi does not support managed key encryption.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud Sync client
Disable Notifications	Disable some or all S3 Network Folder notifications for users with access to the folders. See Disable notifications for Amazon S3 bucket-based Network Folders, below.
Sharing	Sharing the content of the network share can be disabled or enabled using this option 

Option	Description
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to S3 bucket when deleted via Sync client.

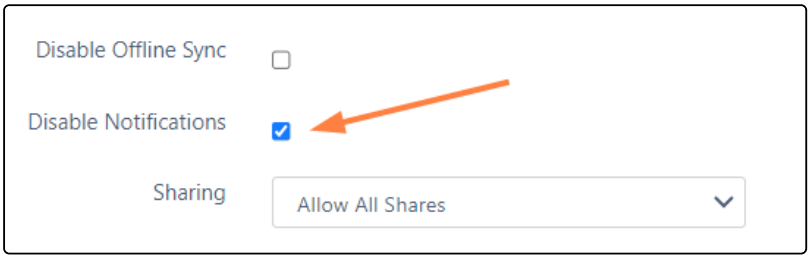
Disable notifications for Amazon S3 Network Folders

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

However, since multiple users may have access to the same network folder, users may receive notifications about actions that don't interest or don't apply to them.

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

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



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

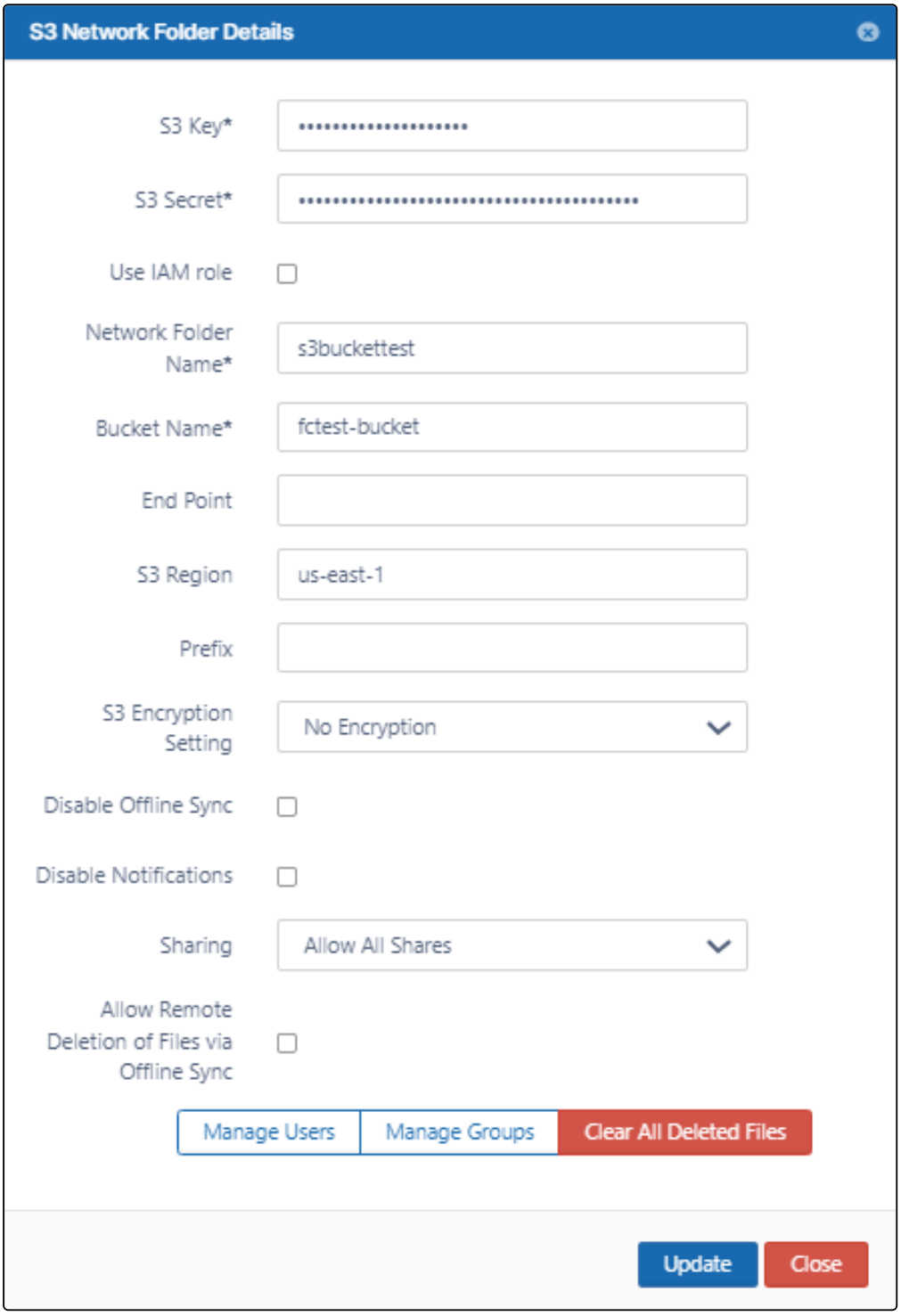
- **Leave all notifications about actions in the folder disabled.**
  By default, admins and users can override this setting. An admin can enable notifications about the folder for specific users, or users can enable their own notifications for the folder.
  If you do not want users to be able to override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

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

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

Backblaze B2 Bucket Based Network Folders

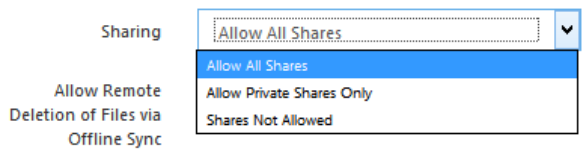
After you attach a Backblaze B2 bucket to a FileCloud Server Network Folder, you can update any of the original settings.



To edit a Backblaze B2 bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Backblaze B2 bucket-based network folder, and then click the edit icon ( ).

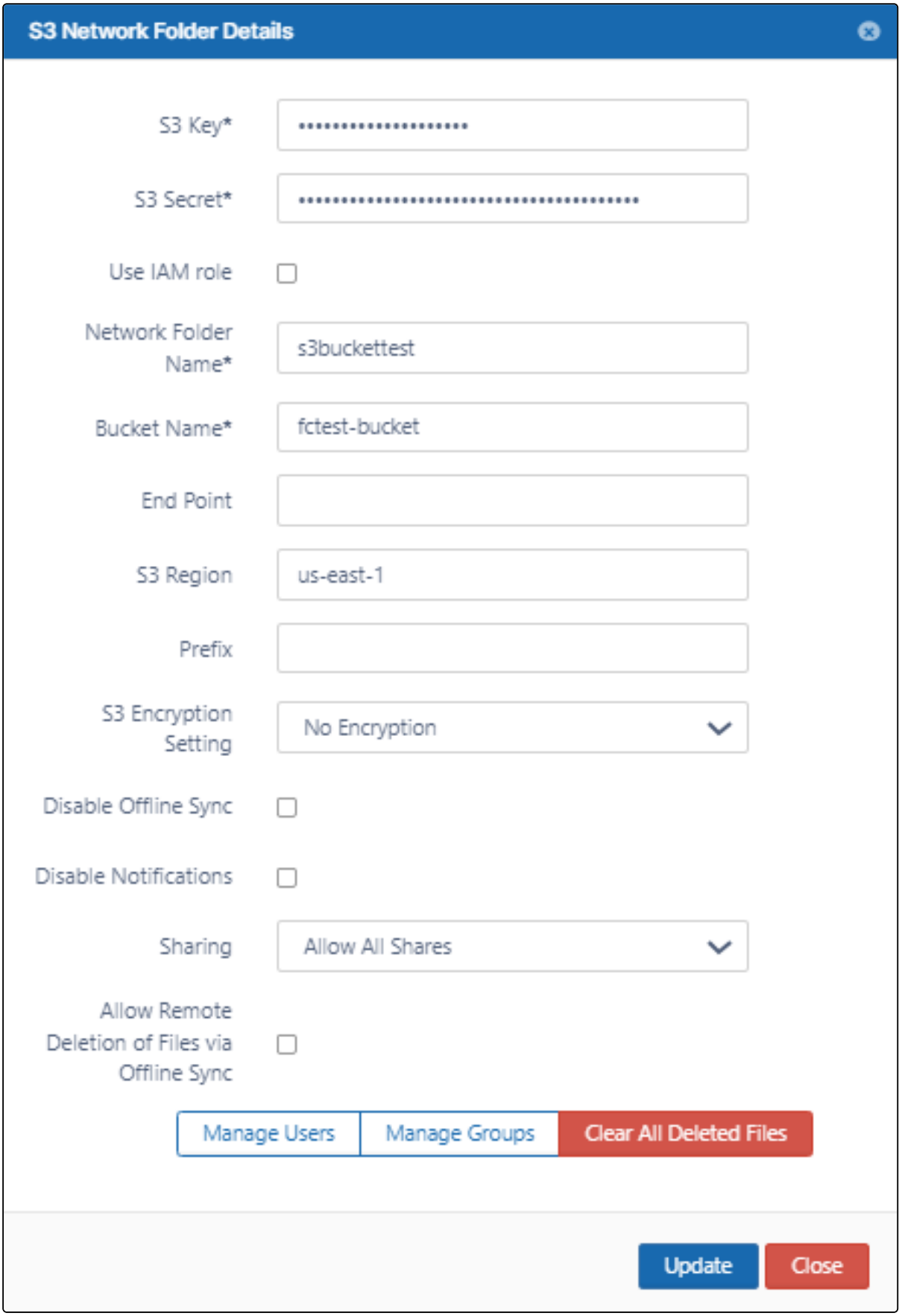
4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
S3 Region	Physical region where buckets are created.
End Point	URL where API requests are sent.
S3 Encryption Setting	**No Encryption** On the **Attach S3 bucket** window, select the type as **No encryption** because Backblaze does not support managed key encryption.
Disable Offline Sync	Enabling this option will prevent this network share from being available for sync via FileCloud sync client
Sharing	Sharing the content of the network share can be disabled or enabled using this option 

Option	Description
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the B2 Bucket if the files are deleted in the synced client. By default deletes are not propagated to B2 bucket when deleted via Sync client.

Cloudian S3-Compatible Object Storage Network Folders

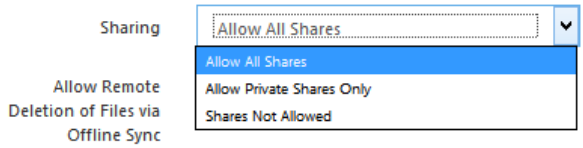
After you attach a Cloudian S3-Compatible Object Storage bucket to a FileCloud Server Network Folder, you can update any of the original settings.


S3 Network Folder Details
S3 Key*
S3 Secret*
Use IAM role
Network Folder Name*
s3buckettest
Bucket Name*
fctest-bucket
End Point
S3 Region
us-east-1
Prefix
S3 Encryption Setting
No Encryption
Disable Offline Sync
Disable Notifications
Sharing
Allow All Shares
Allow Remote Deletion of Files via Offline Sync
Manage Users
Manage Groups
Clear All Deleted Files
Update
Close

To edit a Cloudian S3-Compatible Object Storage bucket-based Network Folder:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click the Cloudian S3-Compatible Object Storage bucket-based network folder, and then click the edit icon ().
4. On the **S3 Network Folder Details** window, set any of the following options:

Option	Description
S3 Key	The key that identifies the bucket.
S3 Secret	Secret access key used with S3 key to gain access.
Use IAM role	When checked, the **S3 Key** and **S3 Secret** fields disappear and the IAM role is used to connect to the S3 bucket.
Network Folder Name	Name of the network folder that will contain the bucket.
Bucket Name	Name identifying the bucket.
End Point	URL where API requests are sent.
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

Option	Description
Sharing	Sharing the content of the network share can be disabled or enabled using this option 
Allow Remote Deletion of Files via Offline Sync	Enabling this function will allow deleting files in the Cloudian S3 Bucket if the files are deleted in the synced client. By default deletes are not propagated to Cloudian S3 bucket when deleted via Sync client.

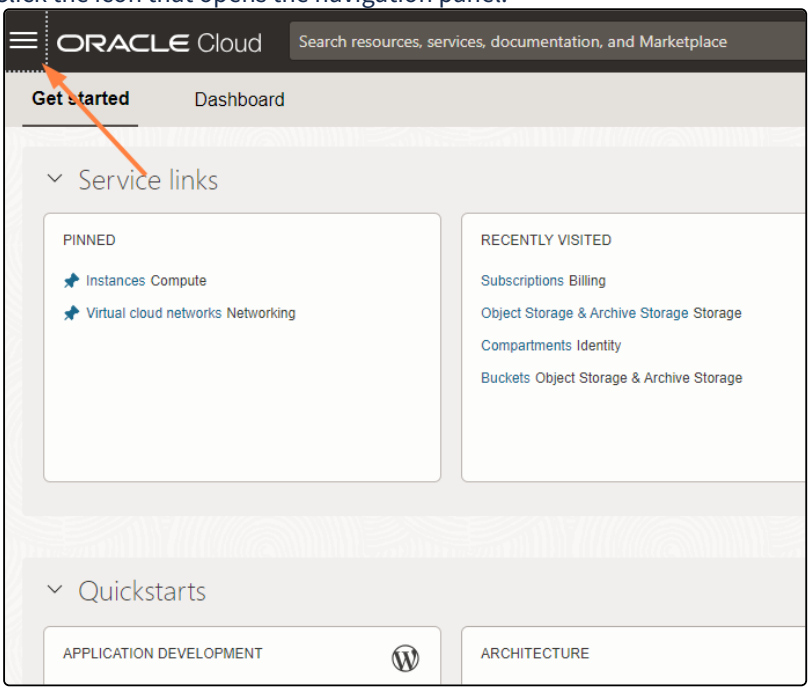
Oracle Cloud Infrastructure S3 Bucket Based Network Folders

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

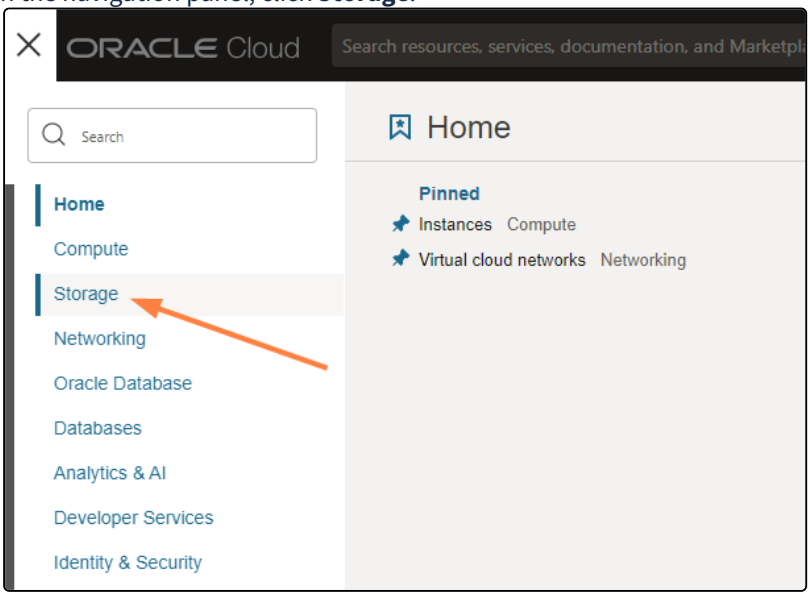
Create the S3 storage bucket and generate your S3 keys. In addition, save the values you will need to enter when you are configuring the OCI/FileCloud integration in the next procedure on this page.

1. Log in to https://cloud.oracle.com.

2. Click the icon that opens the navigation panel:

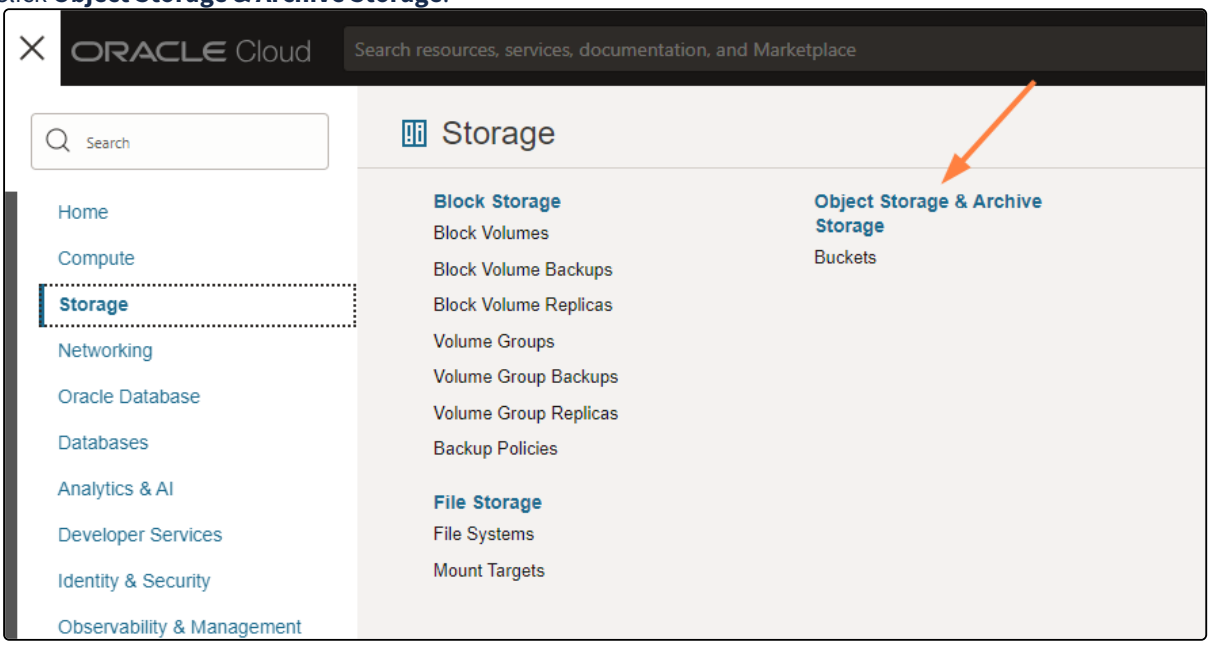


3. In the navigation panel, click **Storage**.



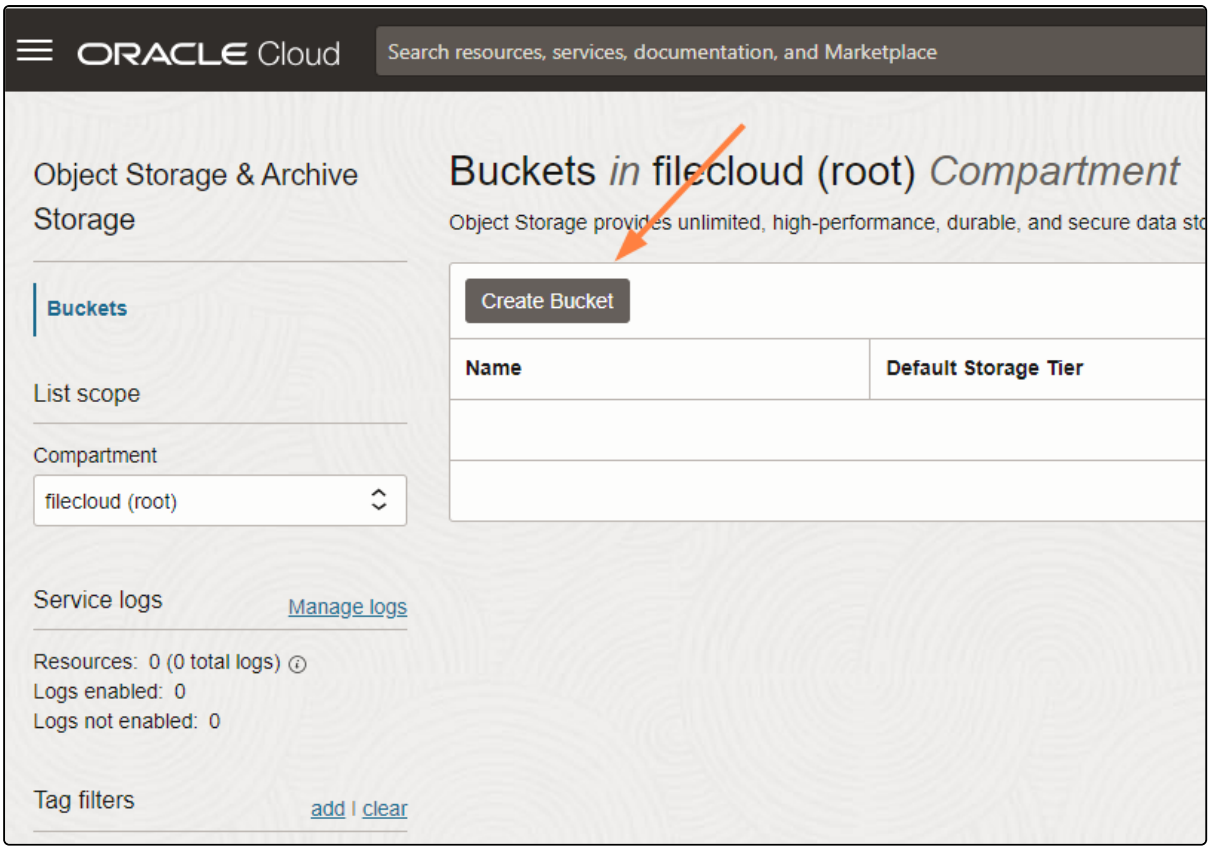
A list of storage-related pages opens.

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



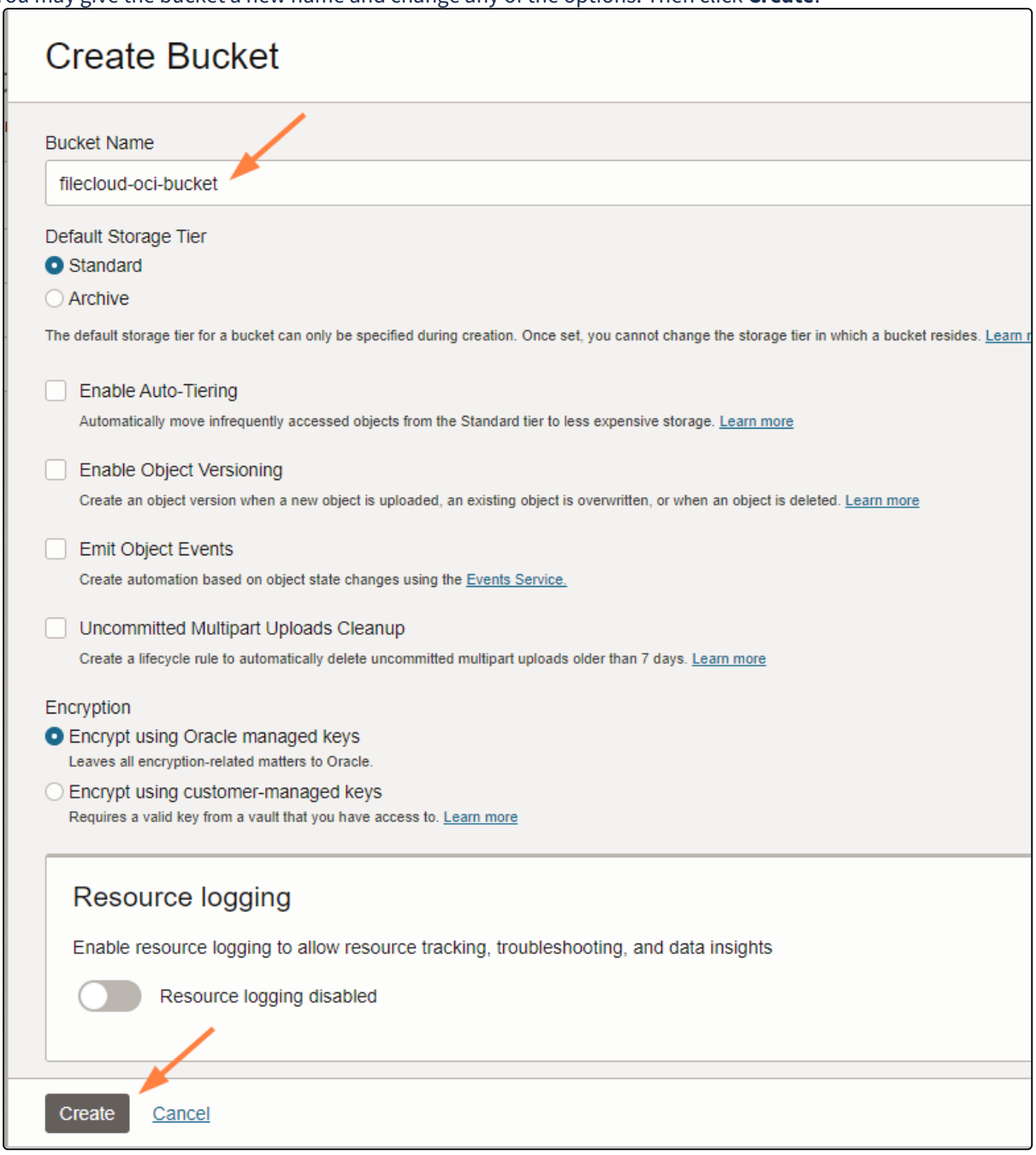
The **Object Storage & Archive Storage** page opens.

5. Click **Create Bucket**.



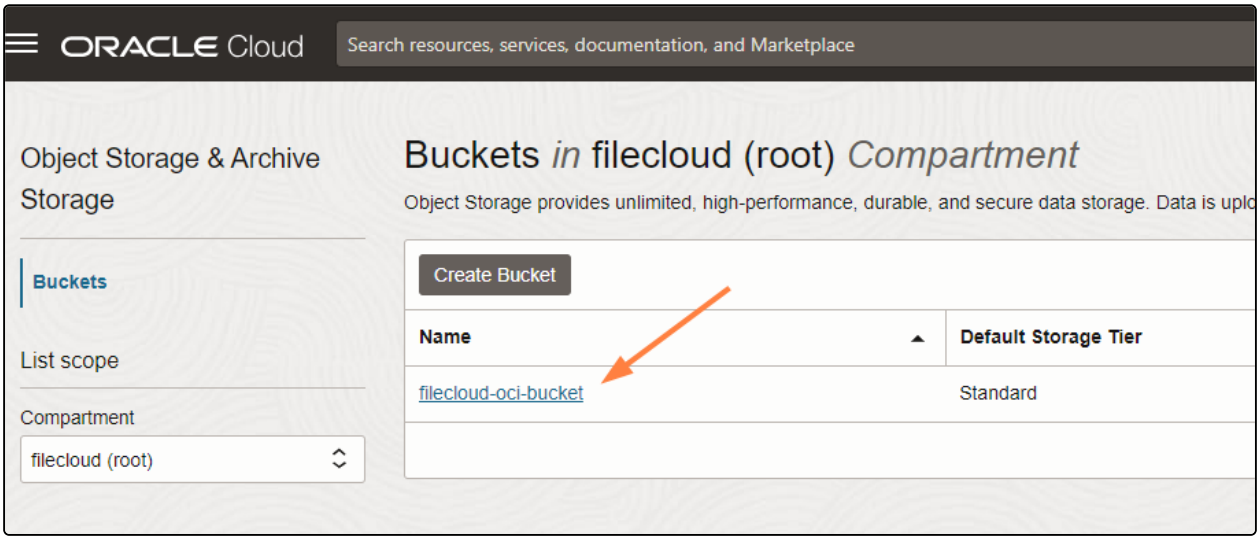
A **Create Bucket** dialog box opens.

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



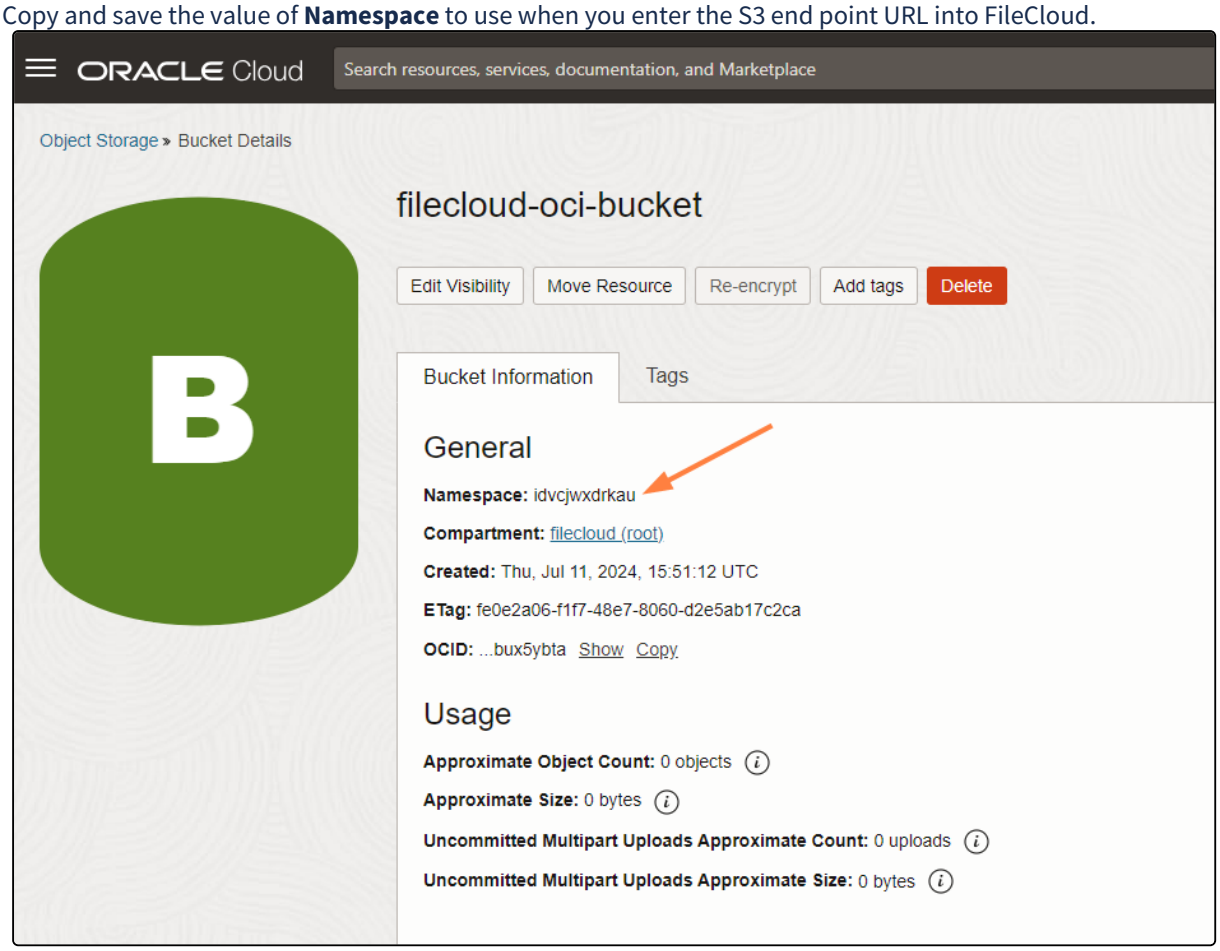
The bucket appears in the list of buckets.

7. Click the bucket name.

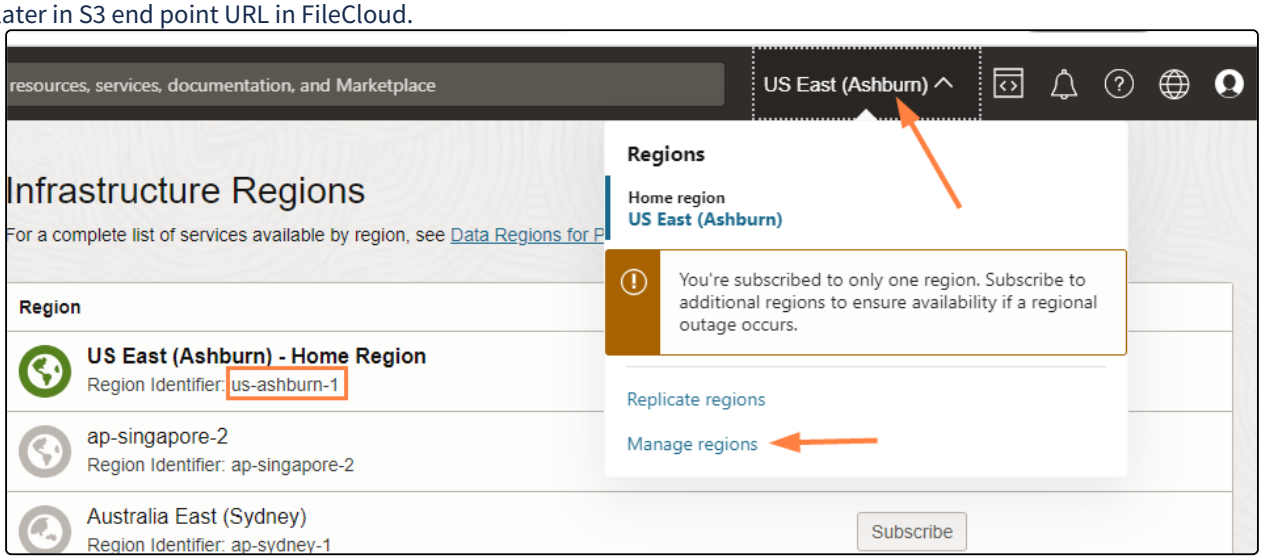


A tab with bucket information opens.

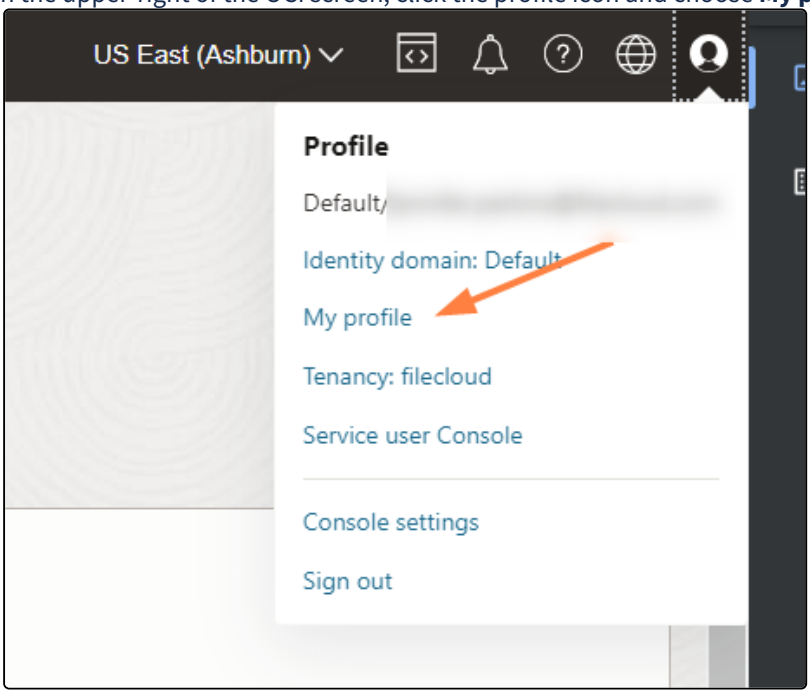
8. Copy and save the value of **Namespace** to use when you enter the S3 end point URL into FileCloud.



9. Get your region by clicking the name of your region at the top of the OCI screen, and choosing **Manage regions** in the drop-down list.
   Copy the **Region Identifier** from the top region shown (the region with the green globe icon) and save it to enter later in S3 end point URL in FileCloud.

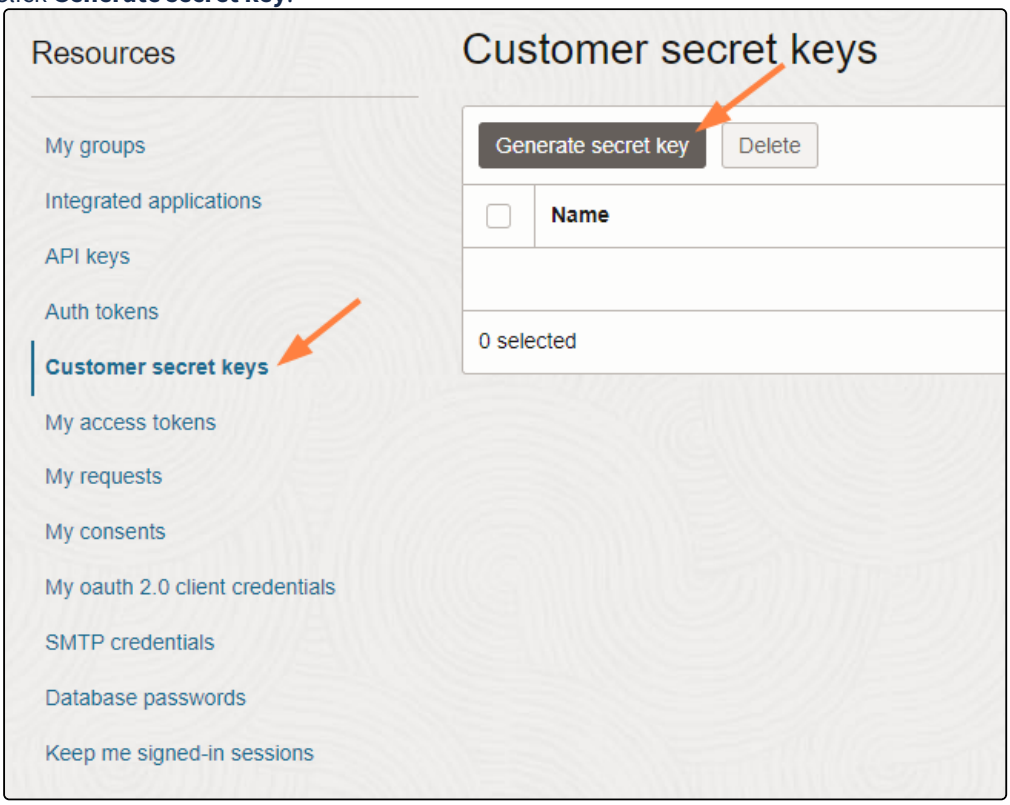


10. In the upper-right of the OCI screen, click the profile icon and choose **My profile**.



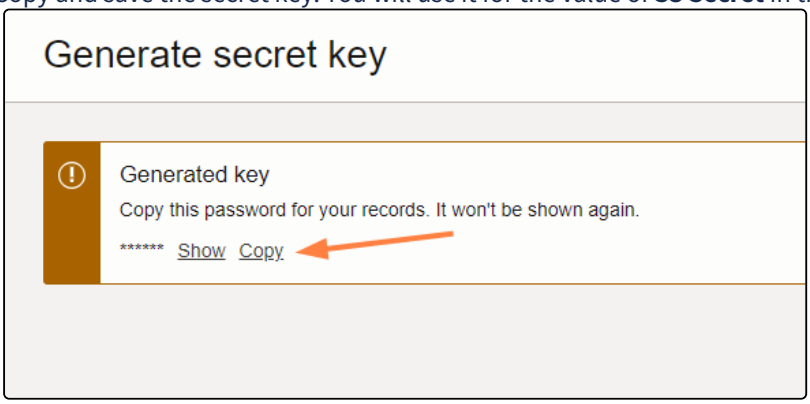
11. In the **My profile** screen navigation panel, scroll down to **Resources**, and click **Customer secret keys**.
    The **Customer secret keys** section opens.

12. Click **Generate secret key**.



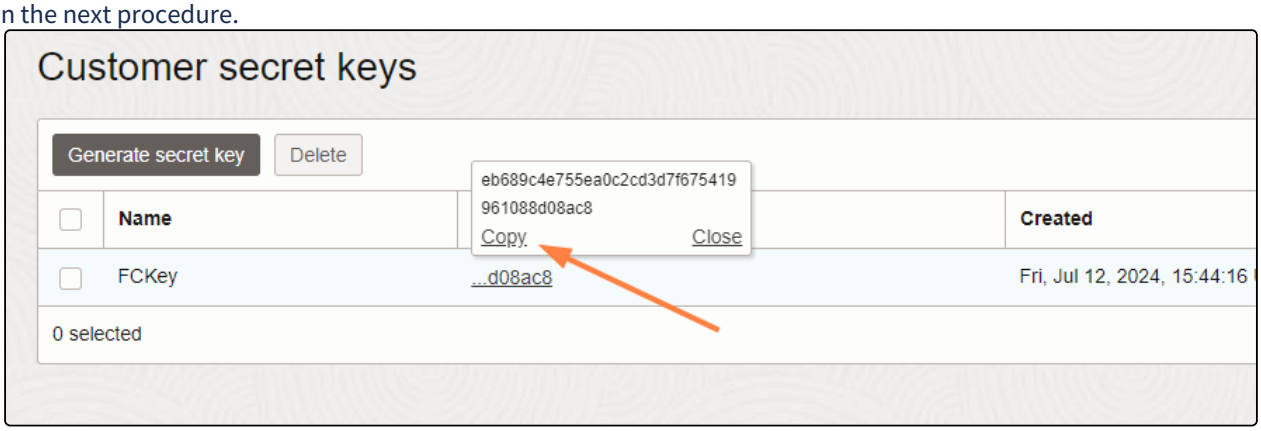
The screen confirms that the secret key was generated and prompts you to copy and save it.

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



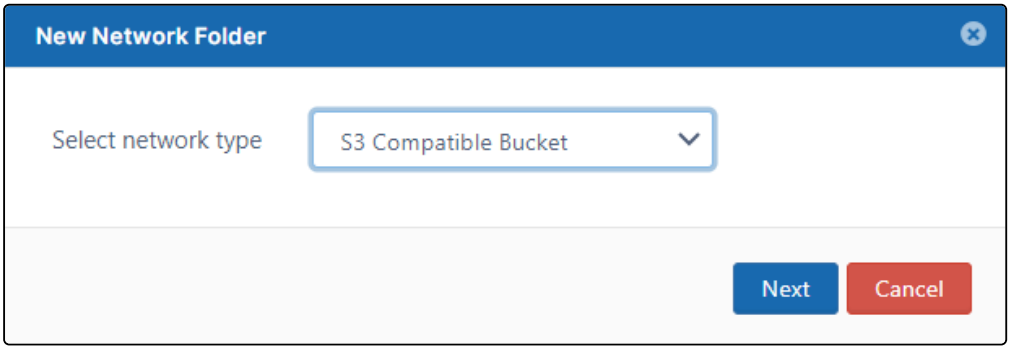
It is now listed in the list of secret keys.

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

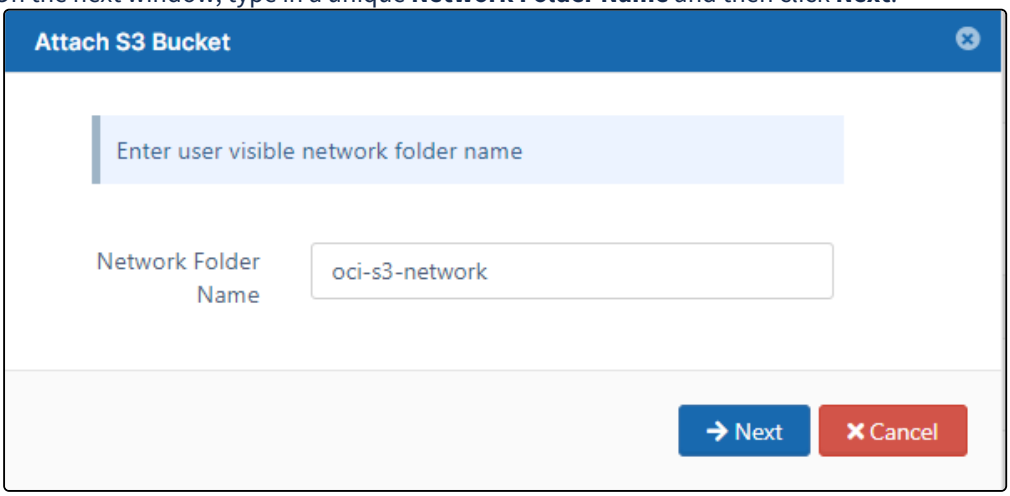


Connect the OCI bucket as a Network Share:

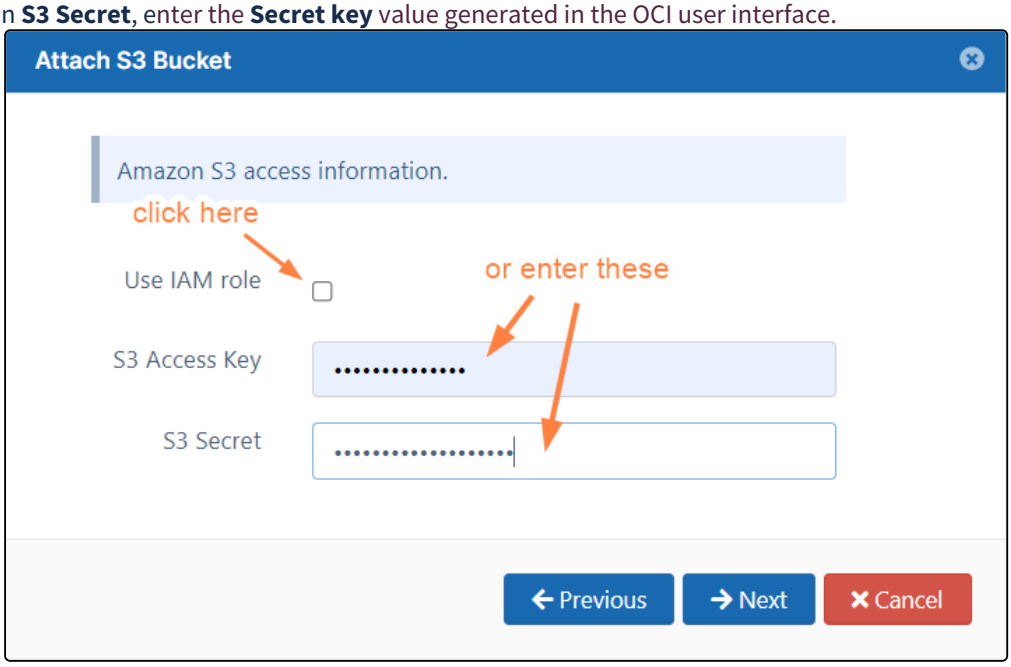
1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.
4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.



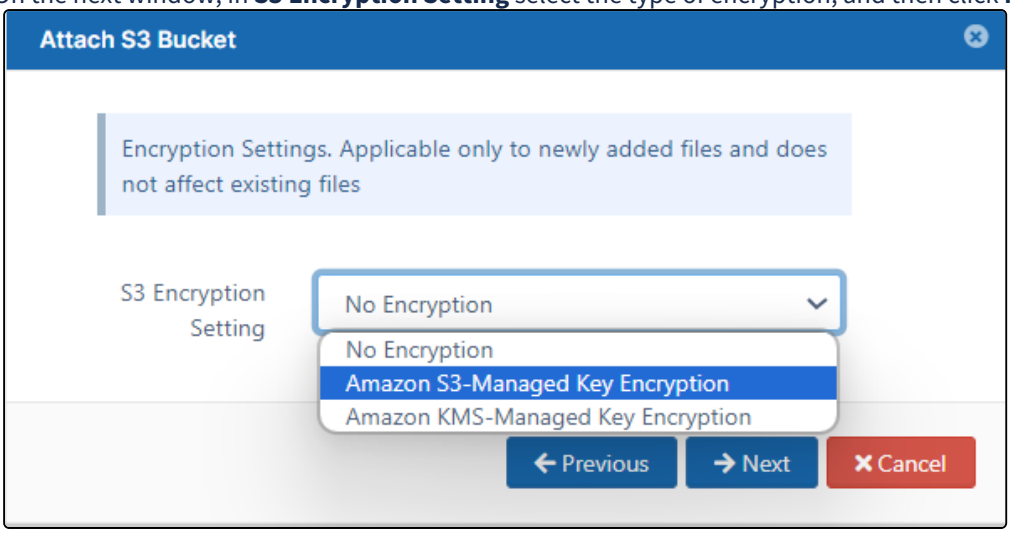
5. On the next window, type in a unique **Network Folder Name** and then click **Next**.



6. In the next window:
   In **S3 Access Key** enter the **Access key** value generated in the OCI user interface.
   In **S3 Secret**, enter the **Secret key** value generated in the OCI user interface.

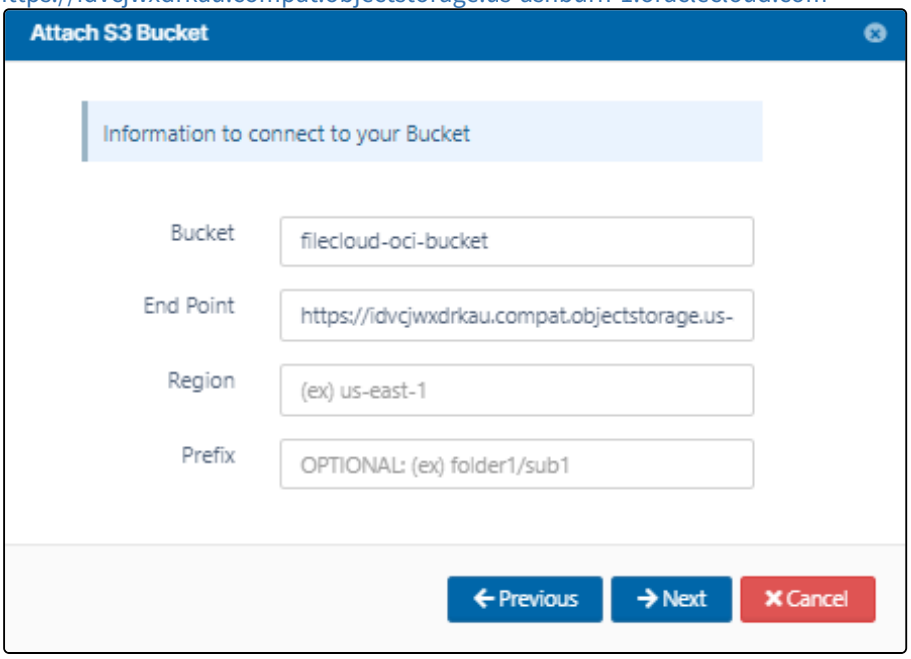


7. On the next window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:



8. In the next window, fill in the fields as shown. You may leave **Region** and **Prefix** blank.
   - **Bucket** - Enter the name of the bucket you created in Oracle.
   - **End Point** - Use the format: https://[namespace].compat.objectstorage.[region].oraclecloud.com where **namespace** and **region** are the values you copied from Oracle as shown in the previous procedure. In the example shown, **End Point** is:

https://idvcjwxdrkau.compat.objectstorage.us-ashburn-1.oraclecloud.com



9. Click **Next**.
   The bucket is connected to FileCloud as a Network Share. You may assign users and groups access before finishing.

Storj S3 Bucket Based Network Folders

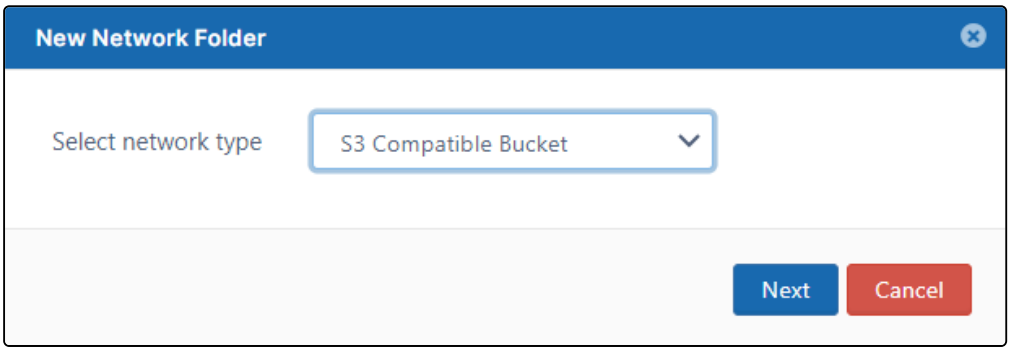
To create the S3 storage bucket and get your S3 key values in Storj

1. Log in to www.storj.io.
2. Create a bucket.
3. Create an access key and a secret key with full access to the bucket.

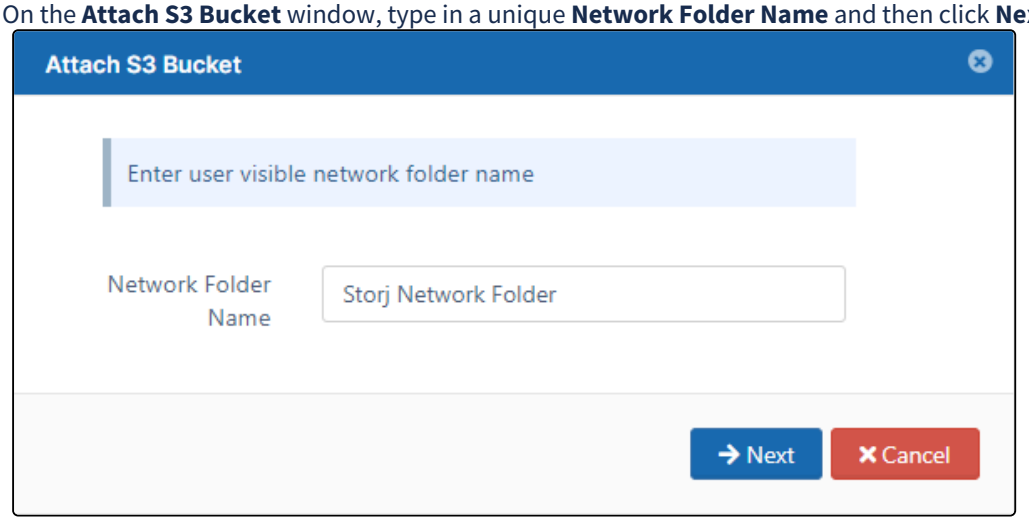
Connect the Storj bucket to FileCloud as a Network Share:

1. Open a browser and log in to the admin portal.
2. In the left navigation panel, select **Network Folders**.
3. On the **Manage Network Folders** window, click **Add**.

4. On the **New Network Folder** dialog box, in **Select network type**, select **S3 Compatible Bucket**, and then click **Next**.

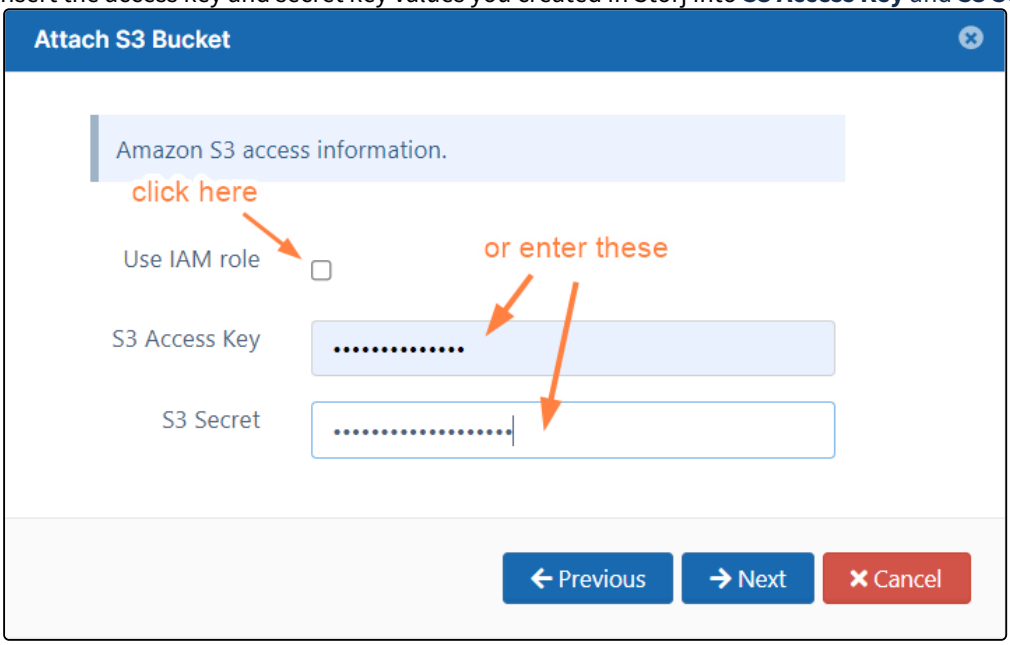


5. On the **Attach S3 Bucket** window, type in a unique **Network Folder Name** and then click **Next**.

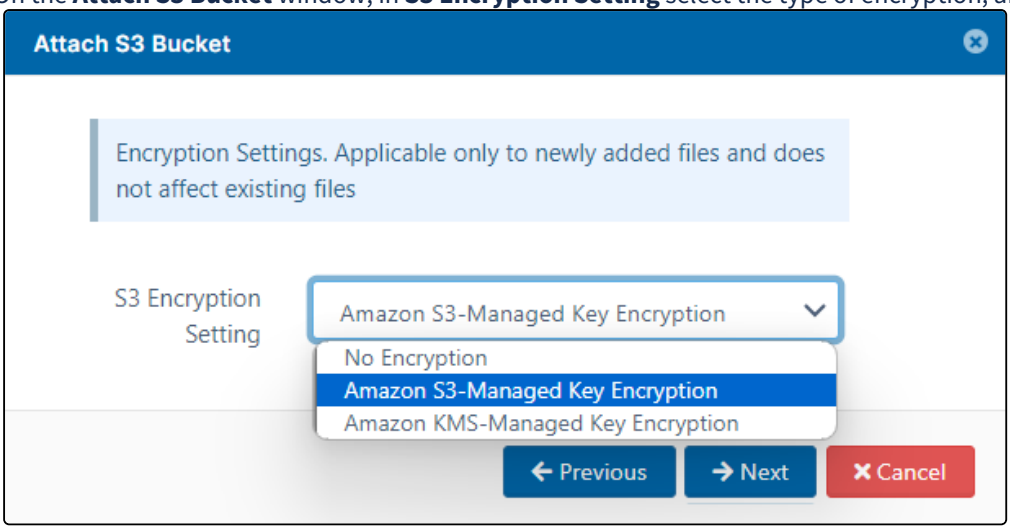


6. In the fields shown:
   Leave **Use IAM** role blank. It is not supported in Storj.

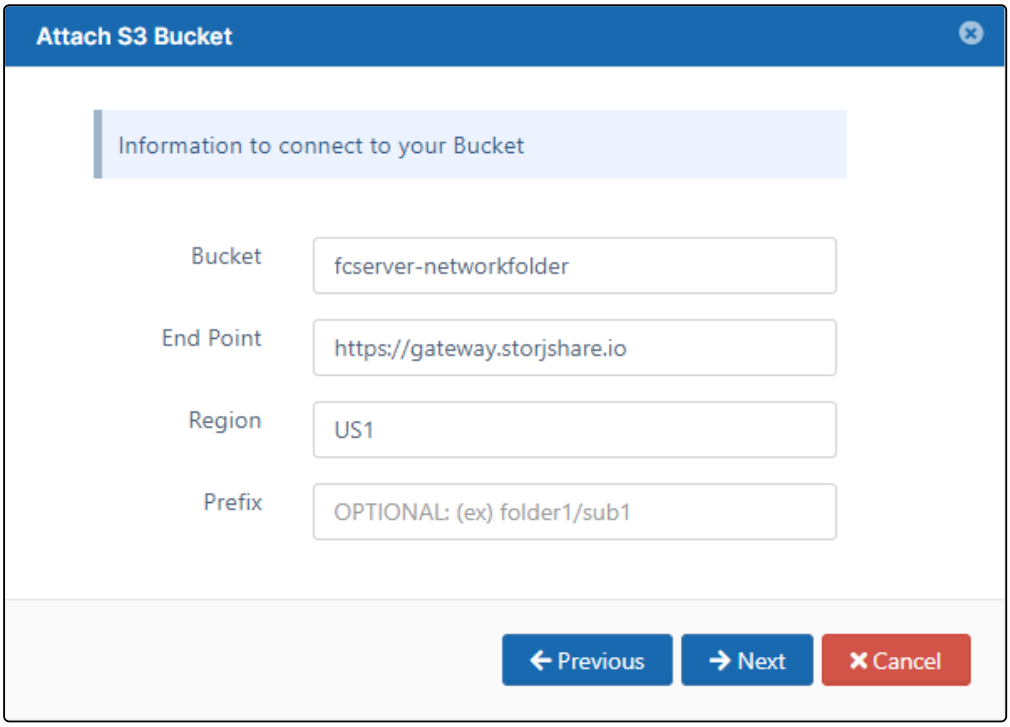
Insert the access key and secret key values you created in Storj into **S3 Access Key** and **S3 Secret**.



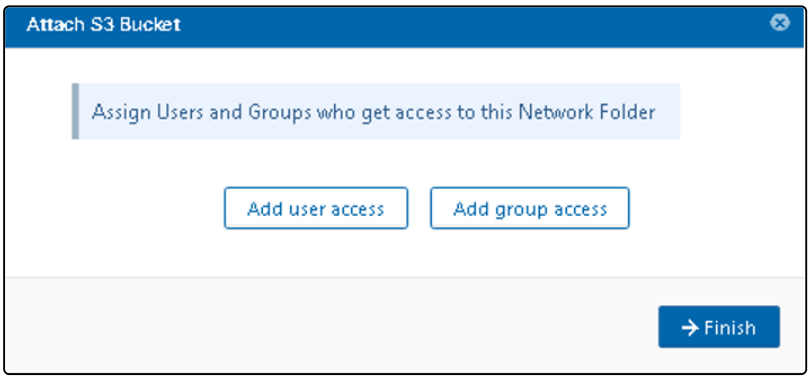
7. On the **Attach S3 Bucket** window, in **S3 Encryption Setting** select the type of encryption, and then click **Next**:



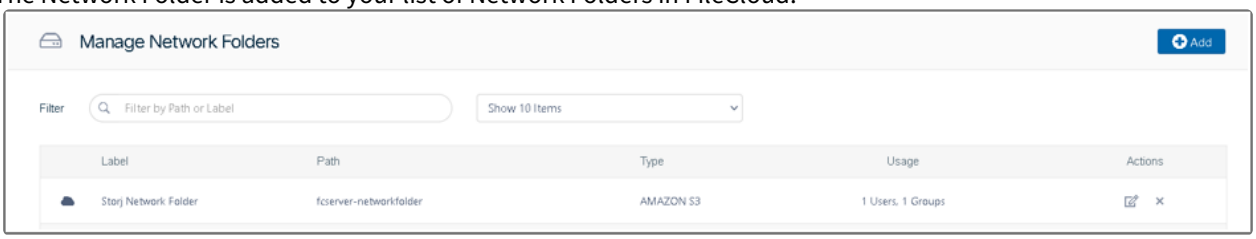
8. Enter the next set of values as follows:
   Bucket: The bucket name (case-sensitive)
   End Point: https://gateway.storjshare.io
   Region: **US1**, **EU1** or **AP1**
   Prefix: Leave blank



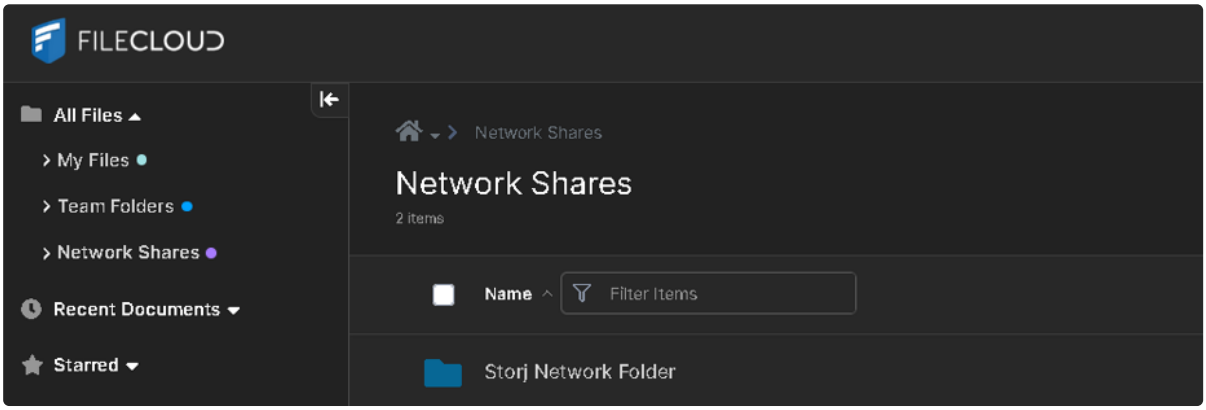
9. Click **Next**.
   The bucket is connected to FileCloud as a Network Share, and you are prompted to give users and groups access.



10. Give users and/or groups access and click **Finish**.
    The Network Folder is added to your list of Network Folders in FileCloud.



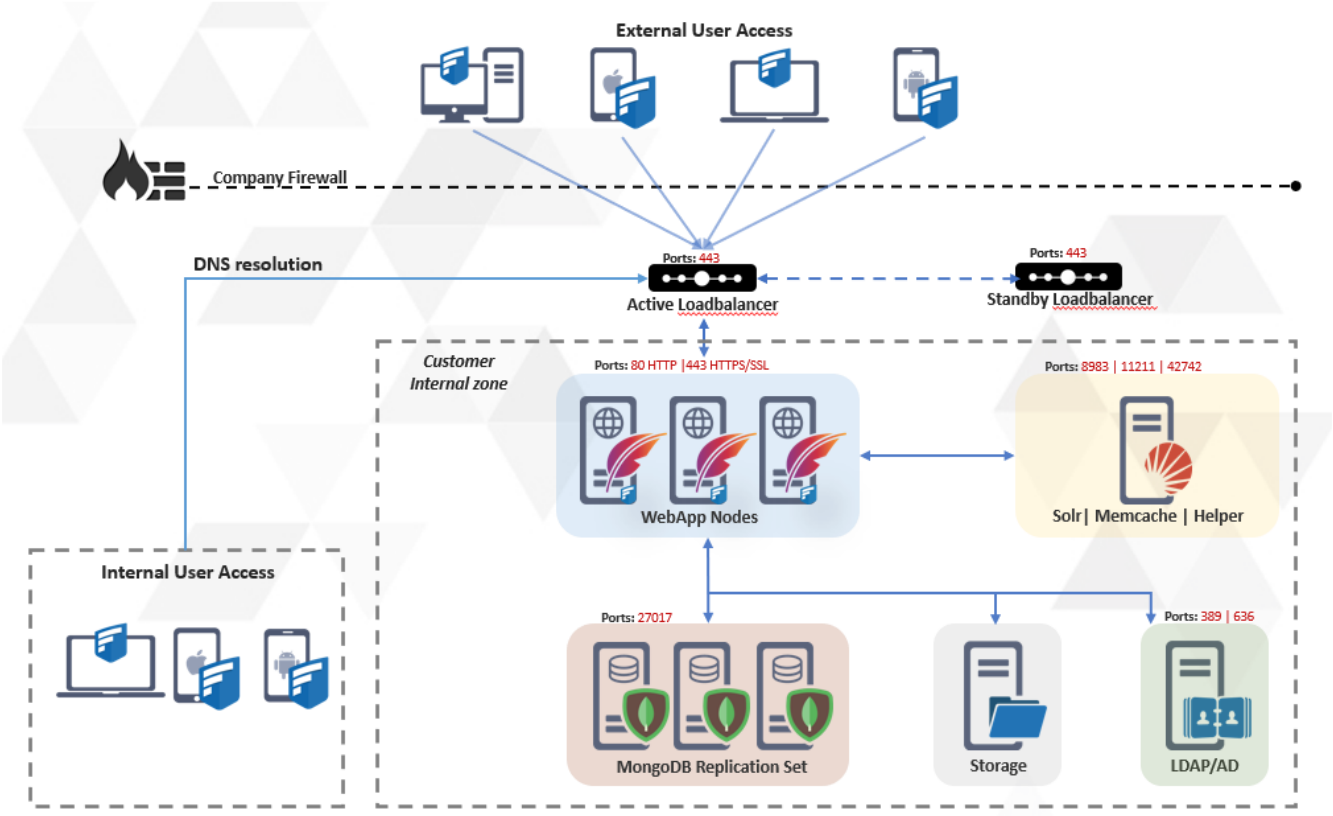
The users you have given access see it in their Network Shares folder in the FileCloud user portal:


FILECLOUD
All Files
My Files
Team Folders
Network Shares
Recent Documents
Starred
Network Shares
Network Shares
2 items
Name
Filter Items
Storj Network Folder

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

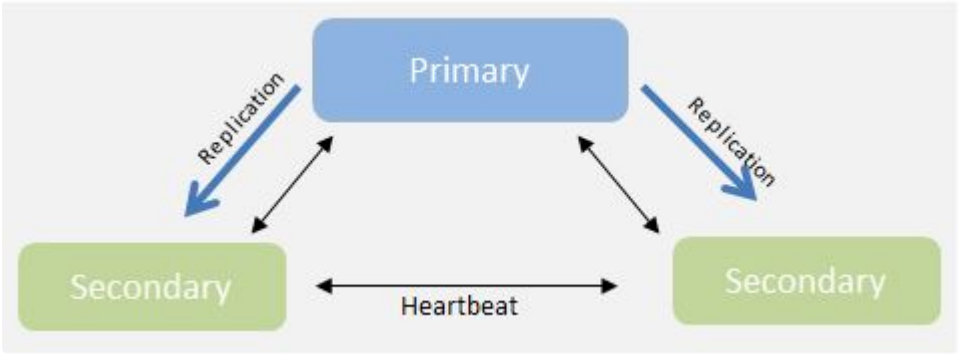
respond in an appropriate amount of time, the client times out on that request and moves on to the next IP address until the list is exhausted or it finds a connection that's valid.

FileCloud Component: App server node

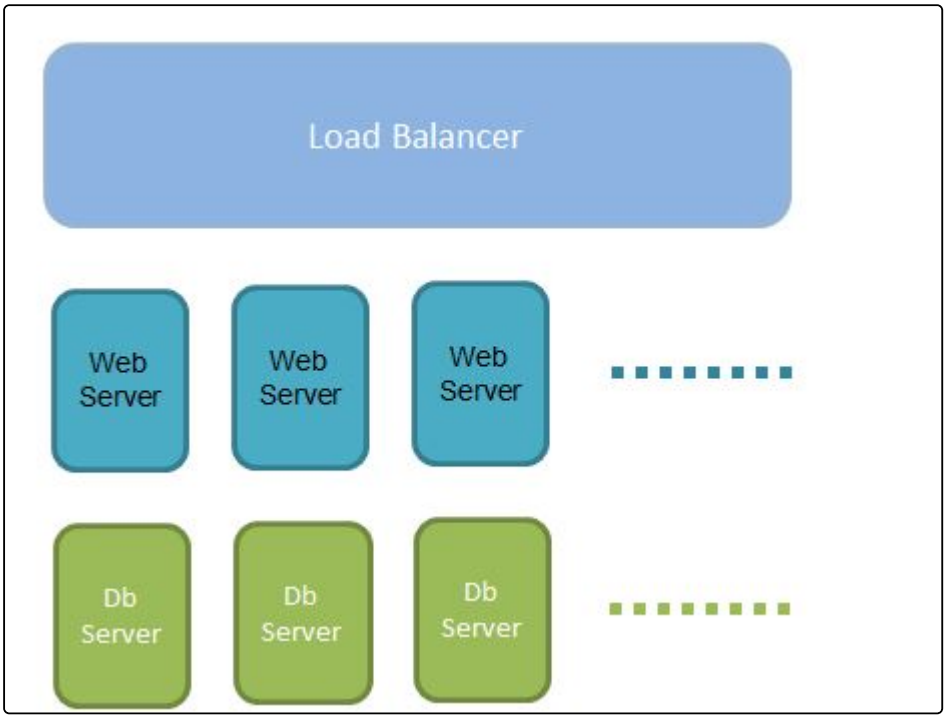
The FileCloud app server node consists of the Apache webserver as well as the FileCloud Application code to serve the client requests. The FileCloud app server nodes do not contain any application-specific data. The data is retrieved from the MondoDB replica sets. Because of this, the FileCloud app server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



To set up a High Availability FileCloud system, use the instructions on the following pages in order:

- Installation and Configuration of 3 server MongoDB cluster
- Configure Memcache for HA Environments
- Configure Solr for HA Environments
- Install and Configure FileCloud Web Servers for HA
- Configure Storage for HA
- Set Up Load Balancing
- Installation and Configuration of Standalone Backup Server
- HA System Tests and License Installation
- Configure Cluster Authentication with SSL

Configure Memcache for HA Environments

In FileCloud, Memcache is used as a storage cache for NTFS permissions, storage encryption, and SSO session handling. Memcache can be used in FileCloud HA mode only for SSO session handling. NTFS permissions and storage encryption can use only one Memcache server.

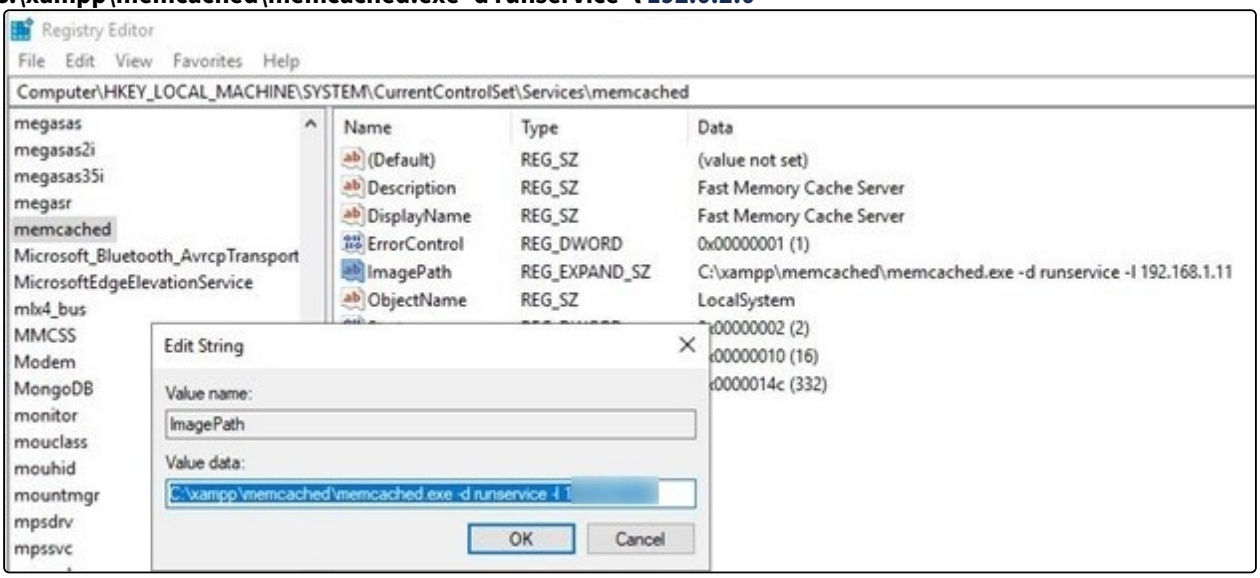
In HA configurations, bind the Memcache service to the private IP of the Memcache server that is accessible by the application servers.

To change the Memcache IP binding:

Windows:

1. Edit the Registry entry **ImagePath** under:
   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\memcached

2. To change the localhost binding to the private IP of the servers where Memcache is running, in **Value data**, enter the following, replacing 192.0.2.0 with your server's IP address:
   C:\xampp\memcached\memcached.exe -d runservice -l 192.0.2.0



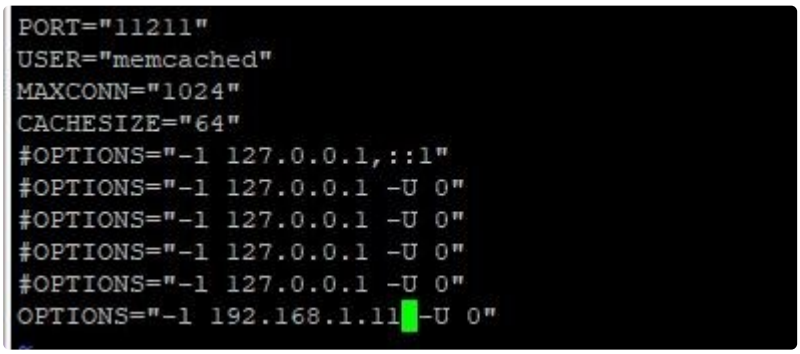
3. Click **OK**.
4. Restart the Memcache service from FileCloud control panel or Windows Services.

Ubuntu:

1. Edit the file **/etc/memcached.conf**.
2. Locate the line **-l 127.0.0.1** and change it to the private IP of your server.
   For example, if the private server is 192.0.2.0, enter:
   -l 192.0.2.0
3. Once the changes are made, restart the Memcache service by entering:
   service memcached restart
   or
   systemctl restart memcached

RHEL:

1. Edit the file **/etc/sysconfig/memcached**.
2. Locate the line **OPTIONS="-l 127.0.0.1 -U 0"** and change it to the private IP of your server.
   For example, if the private server is 192.0.2.0, enter:
   OPTIONS="-l 192.0.2.0 -U 0"



3. Once the changes are made restart the Memcache service by entering:
   service memcached restart
   or
   systemctl restart memcached

To configure Memcached in FileCloud, see Install and Configure FileCloud Web Servers for HA.

Configure Solr for HA Environments

Solr, which is used for content search and automatic content classification in FileCloud, can be configured only as a standalone system for HA environments. Solr service can be run on an application server or on a separate server. When deploying FileCloud with multiple web application servers, Solr service should only run on one server whether it's in the same application node or a separate server.

See Install Content Search for Windows to install Solr on Windows Server or Install Content Search for Linux to install Solr on Linux. Solr service should be binded to an IP/hostname that is accessible from the web node in this setup.

1. **Change the Solr IP binding.**

   In Windows:

   a. Open the file **xampp\solr\bin**solr.in**.cmd**
   b. Locate the line:
      REM set SOLR_JETTY_HOST=127.0.0.1
      and replace it with the following, using the IP or hostname of the Solr server in place of 192.0.2.1.
      set SOLR_JETTY_HOST=192.0.2.1
   c. Restart the **Content Search** service from FileCloud control panel. (The service is located at xampp\cloudcp.exe).

   In RHEL/Ubuntu:

   a. Open the file **/opt/solr/server/etc/jetty-http.xml**
   b. Locate the line:
      <Set name="host"><Property name="solr.jetty.host" default="127.0.0.1"/></Set>
      and replace it with the following, using the IP address of the Solr server in place of 192.0.2.0.
      <Set name="host"><Property name="solr.jetty.host" default="192.0.2.0"/></Set>
   c. Restart the Solr Service by entering:
      service solr restart
      or
      systemctl restart solr

2. Configure Solr in FileCloud.

   Setting up Content Search for Documents
   For help, see .

Install and Configure FileCloud Web Servers for HA

Installing FileCloud web servers for high availability

1. To install the FileCloud web servers, see Direct Installation.
2. After installation, make sure that each web server node has the following services running on it:
   Apache
   Cron
   Message queue
   Web DRM
   Push service
   Memcache (If multiple memcache server are needed for SSO session caching)
   Document preview
3. In Linux environments:
   - Add the MongoDB repository to install MongoDB tools.
   - When you are hosting MongoDB on separate servers, disable the instance of MongoDB running on the web application server, by running:

```
systemctl stop mongodb
systemctl disable mongodb
```

Configuring FileCloud Web Application nodes with MongoDB Cluster and Memcache

Connect a MongoDB Replica Set with an encrypted DB Password

The following steps explain how to connect to a MongoDB replica set with an encrypted MongDB user password so that it does not appear as plain text in cloudconfig.php.

To encrypt the password:

1. Generate a secure key for encryption.
   First run the tool **genkey.php** to create a random password.
   a. In a command line enter:
   In Windows:

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

   In Linux:

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

b. Then, for both Windows and Linux, enter the genkey.php script to generate the secure key for encrypting the plain text password. Since genkey.php outputs to the screen by default, direct the output to the file securekey.key:

```
php genkey.php > securekey.key
```

2. Use the **fcencrypt.php** script with the key generated in the previous step (securekey.key) to encrypt the plain text password ("aSecretPassword" in the example below).
   a. At the command prompt, enter:

```
php fcencrypt.php --message "aSecretPassword" --key "securekey.key"
```

The encrypted message is returned:

```
Encrypted message:
PgxQKdMU+k5756194hlIcUcp5Qod7oXe2XgaQNO+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/vQ==
```

   b. Copy and save the encrypted message, which you will use as your encrypted password.

Connect Web Server nodes to MongoDB Cluster:

After the MongoDB user password is encrypted, follow the steps below to configure all FileCloud web nodes to connect to the Mongo replica cluster as its database.

1. Open the configuration file and change the following configurations to match the replica set details. Repeat this step for each web node.
   Windows Location: **xampp/htdocs/config/cloudconfig.php**
   Linux Location: **/var/www/html/config/cloudconfig.php**

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

2. Add the key file and the encrypted password in cloudconfig.php. Repeat this step for each web node.

```
define('TONIDOCLOUD_ENCRYPTION_KEYFILE', 'c:
\xampp\htdocs\resources\tools\security\securekey.key');
```

```
define('TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD',
'PgxQKdMU+k5756194hlIcUcp5Qod7oXe2XgaQNO+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/vQ==');
```

Where the value for TONIDOCLOUD_ENCRYPTION_KEYFILE is the location of your securekey.key tool and the value for TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD is your encrypted password.

3. Add the MongoDB user and encrypted password string using MongoDB URI function. Repeat this step for each web node.

```
function
FC_MONGODB_URI_OPTIONS(){
    return [
            "username" => "dbuser",
            "password" => "%tonidocloud_mongodb_password%"
    ];
}
```

4. Edit the configuration file at:
   Windows location: **xampp/htdocs/config/localstorageconfig.php**
   Linux location: **/var/www/html/config/localstorageconfig.php**

   Add/replace the following keys in the file. Repeat this step for each web node.

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

5. Add the auto backup mongodump parameter. Repeat this step for each web node.

```
define("AUTOBACKUP_MONGODUMP_PARAMS", '--host "rs0/ hostname of Mongo1,hostname of
Mongo2,hostname of Mongo3" --username dbuser --password
%tonidocloud_mongodb_password% --authenticationDatabase admin');
```

Memcache Configuration:

Beginning in FileCloud 23.242, HA availability for memcache is supported. Encryption remains active as long as at least one server or memcache service, without being restarted since activation, stays up. Storage reactivation is required when the final active server or memcache service is restarted.

1. Configure memcache for NTFS caching and storage encryption. Repeat this step for each web node.

   a. Edit cloudconfig.php:
      Windows Location: **xampp/htdocs/config/cloudconfig.php**
      Linux Location: **/var/www/html/config/cloudconfig.php**

   b. Comment out the lines:

```
//define("TONIDOCLOUD_MEMCACHED_SERVER", "127.0.0.1");
//define("TONIDOCLOUD_MEMCACHED_PORT", 11211);
```

c. Add the line:

```
define("TONIDOCLOUD_MEMCACHED_SERVERS",
"192.168.1.149:11211;192.168.1.150:11211;192.168.1.195:11211;192.168.1.196:11
211");
```

IP values in this configuration can be replaced by the IP or hostname of servers running memcache (in the above example, the memcache service is running on 3 Web servers and 1 Solr server).
Servers can be also grouped for load balancing using "," and ";". This is recommended only for NTFS permission caching.

```
define("TONIDOCLOUD_MEMCACHED_SERVERS",
"192.168.1.149:11211,192.168.1.150:11211;192.168.1.195:11211,192.168.1.196:11
211");
```

2. SSO in the FileCloud HA setup requires Memcache to handle the login session. Repeat this step for each web node.
   Edit the configuration file:
   Windows: **xampp/htdocs/thirdparty/simplesaml/config/config.php**
   Linux: **/var/www/html/thirdparty/simplesaml/config/config.php**
   a. Locate the line **'store.type' => 'phpsession'** and change the reference to **'store.type' => 'memcache'**
   b. Set the Memache hostname to the Memcache server IP or hostname.

```
'memcache_store.servers' => array(
array(
array('hostname' => 'memcachehostname/ip'),
),
),
```

   c. If multiple Memcache servers are used then the Memcache server hostname or IP needs to be specified in FileCloud configuration file. Instead of Step b, above, do the following:.
   Edit the configuration file:
   Windows Location: **xampp/htdocs/config/cloudconfig.php**
   Linux Location: **/var/www/html/config/cloudconfig.php**

   Set the Memache hostnames to each Memcache server IP or hostname.

```
function SSO_MEMCACHED_SERVERS() {
return [
[
['hostname' => ' memcachehostname/ip1'],
['hostname' => ' memcachehostname/ip2'],
],
```

```
];
}
```

For more details, see SAML Single Sign-On Support.

FC Push Service Configuration:

Note: Push service configuration currently doesn't support using an encrypted MongoDB password.

Push service is essential to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload and share notifications).

To configure Push service:

RHEL/Ubuntu:

1. Open and edit the .env file:
   Linux: **/opt/fcpushservice/.env**
   Windows: **xampp\pushservice\.env**

2. Update the MongoDB connection string:

   ```
   FCPS_DB_DSN=mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
   ```

3. Restart the **fcpushservice**.
   In **Linux**, enter:

   ```
   systemctl restart fcpushservice
   ```

   In **Windows**, restart the Push service from the FileCloud Control Panel.

FileCloud Helper Configuration

Note: FileCloud Helper configuration currently doesn't support using an encrypted password.

FileCloud Helper service can be deployed only in a Windows Server environment, and is used for network share solr indexing and realtime syncing of network shares.

1. To configure the IP binding for FileCloud Helper, edit the file **C:\xampp\FileCloudHelper\config.ini** and change the address binding to the IP of the FileCloud Helper server.

   ```
   ; Settings for FileCloud NTFS Helper
   [settings]
   address=helper.filecloudlabs.com
   ```

2. To configure FileCloud Helper to connect to the MongoDB replica set edit the file **C:\xampp\FileCloudHelper\realtime.ini** and change the db connection string to match the replica set value.

```
settingsdb= mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
clouddb= mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
syncdb= mongodb://dbusToer:passw0rd1@dbserver01,dbserver02,dbserver03:27017
```

To enable the Helper service, see Indexing of Network Folders.

The Helper service should be running with a logon account. For help, see Install Helper Service.

Additional Configurations and considerations:

For S3 storage:

1. If you are using Amazon S3 for backend storage, then edit the **amazons3storageconfig.php** file.
   Linux location: **/var/www/html/config/amazons3storageconfig.php**
   Windows location: **c:\xampp\htdocs\config\amazons3storageconfig.php**

   If the file is not found, copy **amazons3storageconfig-sample.php** and rename it **amazons3storageconfig.php** on each of the nodes.

   A temp space must be mounted to the same mount point on each of the nodes (For example /mount/fctemp in linux or F:\fctemp or //hostname/tempfolder in windows).

2. Add/replace the following key:

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

Document Preview

If you have enabled Document Converter service, it must be started in each node.

The local webserver will use the local service to handle document preview.

See Document Preview for help setting up Document Converter on the web nodes.

Apache Logon Account

For Windows systems connected to a domain, it is recommended that you run the below services using a logon account.

Apache Service or Web Server
Message Queue or fcorchestrator
FileCloud Cron Service
FileCloud Docconverter
FileCloud Helper (Only on one server)
FileCloud Solr(Only on one server)

Configure Storage for HA

The storage setup covered here is intended to help you set up your HA environment, but is outside the scope of FileCloud Support.

We use SAMBA Share on RHEL in our example, but you may use the file sharing software that best serves your needs.

In a Windows environment, the Apache service should be able to read and write to the storage path; this typically requires modifying the Apache service log-on permissions to run as a user account with full privileges to the storage path.

The storage path created to store FileCloud data should be accessible across all the web nodes in the setup and readable/writable for Apache.

1. To install Samba in RHEL, run:

```
yum update -y
yum install samba -y
```

2. Then, enable and check Samba status:

```
systemctl enable --now smb
systemctl status smb
```

3. Now that Samba is installed, create a directory for it to share.
   The command below creates a new folder **/data/filecloud** and sets proper Samba permissions by an authenticated user who should have full permissions to the share.

```
mkdir -p /data/filecloud
adduser --home /data/filecloud --no-create-home --shell /usr/sbin/nologin --group
sambashare filecloud
chmod 2770 /data/filecloud
chown filecloud:sambashare /data/filecloud
```

4. Samba keeps its own database of users and passwords, which it uses to authenticate logins. In order to log in, all users must be added to the Samba server and enabled.
   Execute the following `smbpasswd` commands to accomplish both of these tasks:

```
smbpasswd -a filecloud
smbpasswd -e filecloud
```

5. The configuration file for Samba is located at **/etc/samba/smb.conf**. To add the new directory as a share, edit the file by running:

```
vi /etc/samba/smb.conf
```

   Below is the samba conf sample used in this setup:

```
[global]
 server string = samba_server
 server role = standalone server
 interfaces = 192.0.2.0
 bind interfaces only = yes
 disable netbios = yes
 smb ports = 445
 log file = /var/log/samba/smb.log
 max log size = 10000

[filecloud]
 path = /data/filecloud
 browseable = yes
 read only = no
 force create mode = 0660
 force directory mode = 2770
 valid users = filecloud
```

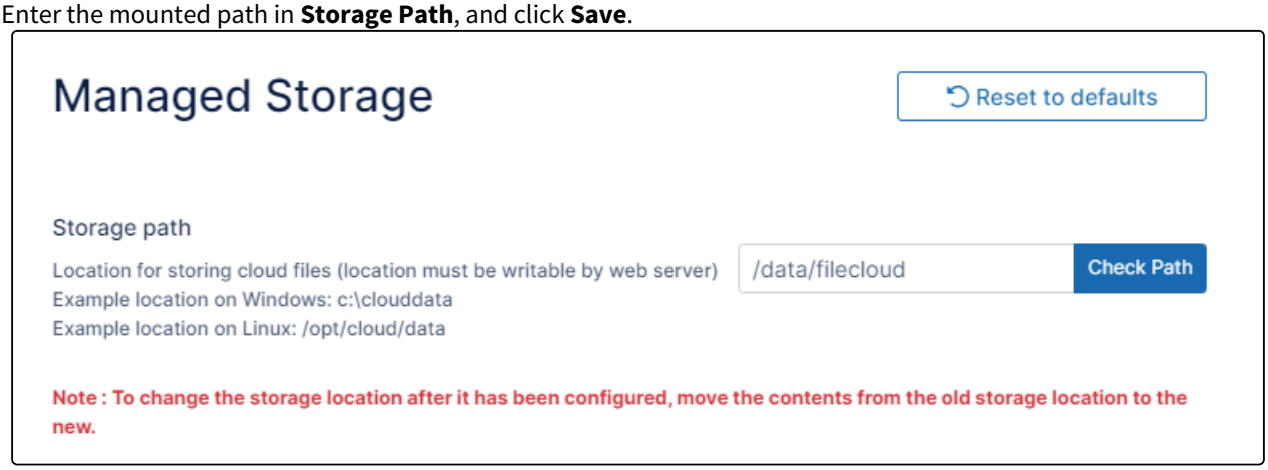
To mount the Samba share in your FileCloud web server nodes, see How to properly mount a CIFS share on RHEL for FileCloud.

Set up the managed storage path in FileCloud

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

In this example, the storage path is **/data/filecloud** which is already available and mounted on each of the Linux webserver nodes.

1. Open the FileCloud Admin portal at **http://<load balancer IP>/ui/admin/index.html** or http://<Private IP **of Web Server>/ui/admin/index.html** and log in.
2. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  **.**
   The **Managed Storage settings** page opens by default.
3. Enter the mounted path in **Storage Path**, and click **Save**.



In Windows, the path must be a UNC path that is accessible from all web nodes. Here the example path is **//storagehostname/FolderName**.

To enable encryption for FileCloud managed storage, see Enabling Storage Encryption.

If you are using S3 object storage see Setting up FileCloud Managed S3 Storage.

If you are using Azure blob storage, see Setting up FileCloud Managed Azure Blob Storage.

Set Up Load Balancing

The core component of an HA setup is its load balancer.

The load balancer installation and configuration processes covered here are intended to help you set up your HA environment, but they are outside the scope of FileCloud Support.

We use HaProxy in an Ubuntu 22.04 environment in our example, but you may adapt our instructions to the load balancing software and environment that best serves your needs. This example uses HTTP but can be expanded to use HTTPS as well.

Load Balancer

The load balancer is the component that distributes incoming requests among a group of servers. In this example, the load balancer is HaProxy (http://www.haproxy.org/). HaProxy is a high performance load balancer that allows you to scale your FileCloud deployment quickly.

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

Setting up 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. Add the following in the empty haproxy.cfg file.
   The log directive mentions a syslog server to which log messages are sent. On Ubuntu, rsyslog is already installed and running but it doesn't listen on an IP address. We'll modify the config files of rsyslog later.
   The maxconn directive specifies the number of concurrent connections on the frontend. The default value is 2000 and should be tuned according to your VPS' configuration.
   The user and group directives change the HAProxy process to the specified user/group. These shouldn't be changed.

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

Defaults

This section demonstrates how to specify default values. The values to be modified are the various timeout directives. The connect option specifies the maximum time to wait for a connection attempt to a VPS to succeed.

The client and server timeouts apply when the client or server is expected to acknowledge or send data during the TCP process. HAProxy recommends setting the client and server timeouts to the same value.

The retries directive sets the number of retries to perform on a VPS after a connection failure.

The option redispatch enables session redistribution in case of connection failures. So session stickiness is overridden if a VPS goes down.

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

```
    timeout client 10000
    timeout server 10000
```

Host Configuration

This contains the configuration for both the frontend and backend and shows how to configure HAProxy to listen on port 80 for filecloud (which is just a name for identifying the application).

The stats directives enable the connection statistics page and protect it with HTTP Basic authentication using the credentials specified by the stats auth directive.

This page can be viewed with the URL mentioned in stats uri, so in this case, it is http://<loadbalancerip>/haproxy?stats;

The balance directive specifies the load balancing algorithm to use. Options available are Round Robin (roundrobin), Static Round Robin (static-rr), Least Connections (leastconn), Source (source), URI (uri) and URL parameter (url_param).

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*]

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

In the directive server Ha-WS1 xx.xx.xx.xx:80, replace xx.xx.xx.xx with the actual IP address of the app server nodes.

```
listen filecloud
    bind 0.0.0.0:80
    mode http
    stats enable
    stats uri /haproxy?stats
    stats realm Strictly\ Private
    stats auth  proxyuser:proxypassword
    balance roundrobin
    option http-server-close
    timeout http-keep-alive 3000
    option forwardfor
    server Ha-WS1 xx.xx.xx.xx:80 check
    server Ha-WS2 xx.xx.xx.xx:80 check
    server Ha-WS3 xx.xx.xx.xx:80 check
```

Starting Ha-Proxy

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

```
service haproxy start
```

HA System Tests and License Installation

Install the FileCloud license
To install the FileCloud license, follow the instructions at Install the FileCloud License.

HA setup system health checks

The Installation Checks page on the admin portal gives information about the health of each node.

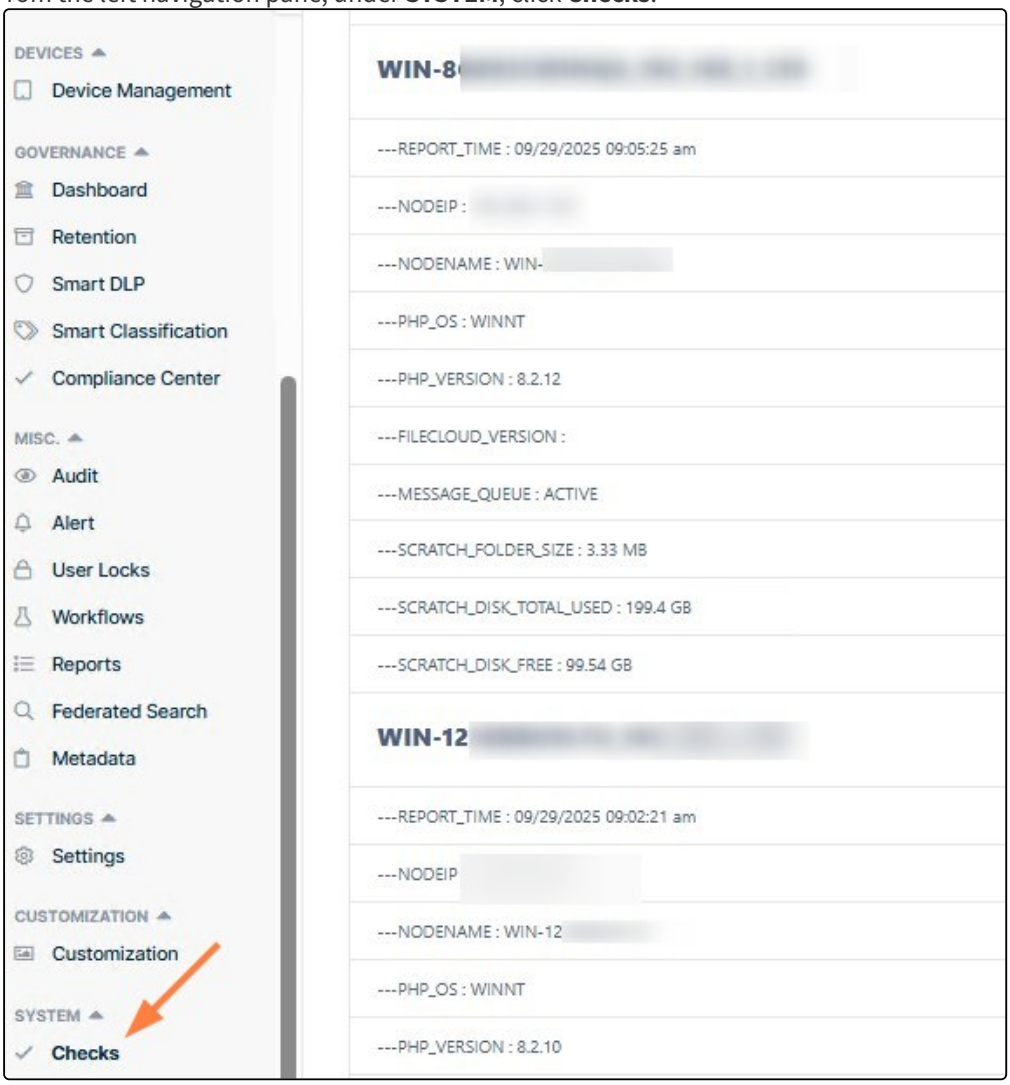
- When you run a system check, the Installation Checks page shows one record with health information for each node of the HA system.
- Cron continues adding node information to the checks.
- This data helps you determine node information such as code level and MQ status.

Since Cron is providing the data for the system check, it can take a few minutes for Cron to run and collect the data.

To see the System Check:

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

2. From the left navigation pane, under **SYSTEM**, click **Checks**.



System Availability Tests:

Application Servers:
To test app server HA, turn off one of the app servers by logging into the app server (for example, Web Node1) and stopping the Apache service. The service should be accessible because the loadbalancer will reroute traffic to Web Node2 or Web Node3.

Database Servers:
To test database replica set redundancy, stop MongoDB service on one of the MongoDB nodes and service should be accessible with the two other database servers running.

Configure Cluster Authentication with SSL

A MongoDB HA cluster is configured to listen to external requests so that all nodes in the cluster are able to sync with one another. Hosting such a configuration in a private dedicated network is secure, but hosting it in an intranet or public network is not. It is necessary to enable authentication on these clusters. Follow the steps outlined here to enable authentication on a MongoDB cluster and upgrade it to use SSL/TLS certificates.

As a prerequisite you are required to have a working HA cluster. It can either be a replica set cluster or a sharding cluster.

Enable Mongodb Authentication:

Enable Role-Based Access Control

For encryption to be used in your replica set, first activate Role-Based Access Control (RBAC). By default, a MongoDB installation permits anyone to connect and see the data. Having RBAC enabled is mandatory for encryption.

Create a DB user in MongoDB to use in FileCloud for secure database access.
In this example, the user has the following credentials:

User Name	Password
dbuser	passw0rd1

To create the user, enter:

OS	Command
Linux	$ use admin $ db.createUser({user: 'dbuser', pwd: 'passw0rd1', roles:['root']})

Now to connect to MongoDB in Linux, enter following command:

OS	Command
Linux	$ mongosh -u dbuser-p passw0rd1 --authenticationDatabase "admin"

Configuration of mongodb to use TLS/SSL:

In order to use encryption, create certificates on all nodes and have a certification authority (CA) that signs them.

For testing purposes (to ensure encryption is working) you can use self-signed certificates; for a production environment, it's better to use valid certificates.

To proceed with certificate generation make sure you have **OpenSSL** installed on your system and that your certificates satisfy these requirements:

- all certificates need to be signed by the same CA
- the common name (CN) required during certificate creation must correspond to the hostname of the host
- any other field requested in certificate creation should be a non-empty value and should reflect your organization details
- all fields, except CN, should match those from the certificates for the other cluster members

The following guide describes all the steps to configure internal X.509 certificate-based encryption.

1 – Connect to one of the hosts and generate a new private key using openssl:

OS	Command
Linux	$ openssl genrsa -out mongoCA.key -aes256 8192

This creates a new 8192-bit private key and saves it in the file mongoCA.key. Enter a strong passphrase when requested.

2 – Sign a new CA certificate

Now, create the “test” local certification authority that you’ll use later to sign each node certificate.

During certificate creation, values must be entered into some fields. You may choose these values randomly but it is better if they correspond to your organization’s details.

OS	Command
Linux	$ openssl req -x509 -new -extensions v3_ca -key mongoCA.key -days 365 -out mongoCA.crt

3 – Issue self-signed certificates for all nodes

For each node, generate a certificate request and sign it using the CA certificate created in the previous step.

Remember: Fill out all fields requested with the same values for each host, except fill out a different common name (CN) for each host - use a common name that corresponds to the particular hostname.

For the first node issue the following commands.

OS	Command

Linux	$ openssl req -new -nodes -newkey rsa:4096 -keyout mongossl1.key -out mongossl1.csr
	$ openssl x509 -CA mongoCA.crt -CAkey mongoCA.key -CAcreateserial -req -days 365 -in mongossl1.csr -out mongossl1.crt
	$ cat mongossl1.key mongossl1.crt > psmdb1.pem

Issue the same commands for the second and third nodes.

4 - Create certificate for FileCloud web nodes

OS	Command
Linux	$ cat psmdb1.pem psmdb2.pem psmdb3.pem > filecloud-mongo.pem

5 – Place the files

You could execute all of the commands in the previous step on the same host, but instead copy the generated files to the proper nodes:

- Copy to each node the CA certificate file: **mongoCA.crt**
- Copy each self-signed certificate **<hostname>.pem** into the relative member
- Create on each member a directory that only the MongoDB user can read, and copy both files there

OS	Command

Linux	$ sudo mkdir -p /etc/mongodb/ssl
	$ sudo chmod 700 /etc/mongodb/ssl
	$ sudo chown -R mongod:mongod /etc/mongodb
	$ sudo cp mongossl1.pem /etc/mongodb/ssl
	$ sudo cp mongoCA.crt /etc/mongodb/ssl

- Copy these files to all web nodes and make sure apache has access:
  /etc/ssl/filecloud-mongo.pem
  /etc/ssl/mongoCA.crt

6 – Configure mongod

Finally, inform mongod about the certificates to enable encryption.

Change the configuration file **/etc/mongod.conf** on each host adding the following rows:

OS	Command
Linux	net: ssl: mode: requireSSL PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem CAFile: /etc/mongodb/ssl/mongoCA.crt

Restart Mongod Daemon:

OS	Command
Linux	$ Systemctl restart mongod

Put the proper file names on other hosts (mongossl2.pem on mongossl2 hosts, and so on)

Now you should have a properly configured replica set that uses encrypted connections.

Issue the following command to connect on node mongossl1:

OS	Command
Linux	$ mongosh --authenticationDatabase "dbuser" --host mongossl1:27017 --ssl --sslCAFile /etc/ssl/mongoCA.crt --sslPEMKeyFile /etc/mongodb/ssl/mongossl1.pem -u dbuser -p passw0rd1

Certificate Notice :

For production use, your MongoDB deployment should use valid certificates generated and signed by a single certificate authority. You or your organization can generate and maintain an independent certificate authority, or use certificates generated by a third-party TLS/SSL vendor.
MongoDB can use any valid TLS/SSL certificate issued by a certificate authority or a self-signed certificate. If you use a self-signed certificate, although the communications channel is encrypted, there is no validation of server identity. Although such a situation prevents eavesdropping on the connection, it leaves you vulnerable to a man-in-the-middle attack. Using a certificate signed by a trusted certificate authority will permit MongoDB drivers to verify the server's identity. In general, avoid using self-signed certificates unless the network is trusted.

Enable Cluster Node Authentication

To enable the cluster nodes to communicate with each other in a secure mode, enable what is called "Internal Authentication". This is done by using an x509 certificate or secure keyfile and configuring each cluster node to use that key.

1-Using x509 certificate:

You can use the same Pem file created for each node in the previous step for the cluster authentication between nodes, or you can generate another Pem file used for this purpose only.

MongoDB configuration should appear as follows:

OS	Command

Linux	net:
	  ssl:
	  mode: requireSSL
	  PEMKeyFile: /etc/mongodb/ssl/mongossl1.pem
	  CAFile: /etc/mongodb/ssl/mongoCA.crt
	  clusterFile: /etc/mongodb/ssl/mongossl1.pem
	security:
	authorization: enabled
	clusterAuthMode: x509

Each node has its own PEMKeyFile and clusterFile.

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

2-Using Keyfile:

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

OS	Command
Linux	$ sudo openssl rand -base64 741 > /etc/mongodb-keyfile $ sudo chmod 600 /etc/mongodb-keyfile $ sudo chown mongodb.mongodb /etc/mongodb-keyfile

2- Copy secure key to all nodes
After the key is generated, copy the key file to all the cluster nodes.

3- Modify configuration file to use the key
Edit mongodb.conf file and make the following changes

OS	Command

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

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

Configure Other DB URLs In Config File

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

Update DB URLs in cloudconfig.php

```
// ... Cloud Database
define("TONIDOCLOUD_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// ... Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
// connection parameter for db backups:
define("AUTOBACKUP_MONGODUMP_PARAMS", "--host 'rs0/HOST1,HOST2,HOST3' --username dbuser
--password passw0rd1 --authenticationDatabase admin --ssl --sslCAFile=/etc/ssl/
mongoCA.crt --sslPEMKeyFile=/etc/ssl/filecloud-mongo.pem " );
```

Note: If the password you supply in AUTOBACKUP_MONGODUMP_PARAMS doesn't work or contains special characters, use the password parameter embedded in the characters \"password\"
For example:

```
define("AUTOBACKUP_MONGODUMP_PARAMS", "--host 'rs0/HOST1,HOST2,HOST3' --username dbuser
--password \"passw0rd1?]\" --authenticationDatabase admin --ssl --sslCAFile=/etc/ssl/
mongoCA.crt --sslPEMKeyFile=/etc/ssl/filecloud-mongo.pem " );
```

Add WWWROOT/config/cloudconfig.php at the bottom:

Update DB URLs in cloudconfig.php

```
function
FC_MONGODB_URI_OPTIONS(){
    return [
        "tlsCertificateKeyFile" => "/etc/ssl/filecloud-mongo.pem",
        "tlsCAFile" => "/etc/ssl/mongoCA.crt"
    ];
}
```

and update the following line in WWWROOT/config/localstorage.php:

Update DB URLs in localstorageconfig.php

```
// ... Cloud Database
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://dbuser:passw0rd1@HOST1,HOST2,HOST3/?
replicaSet=rs0&connectTimeoutMS=1000&ssl=true");
```

Restart Services

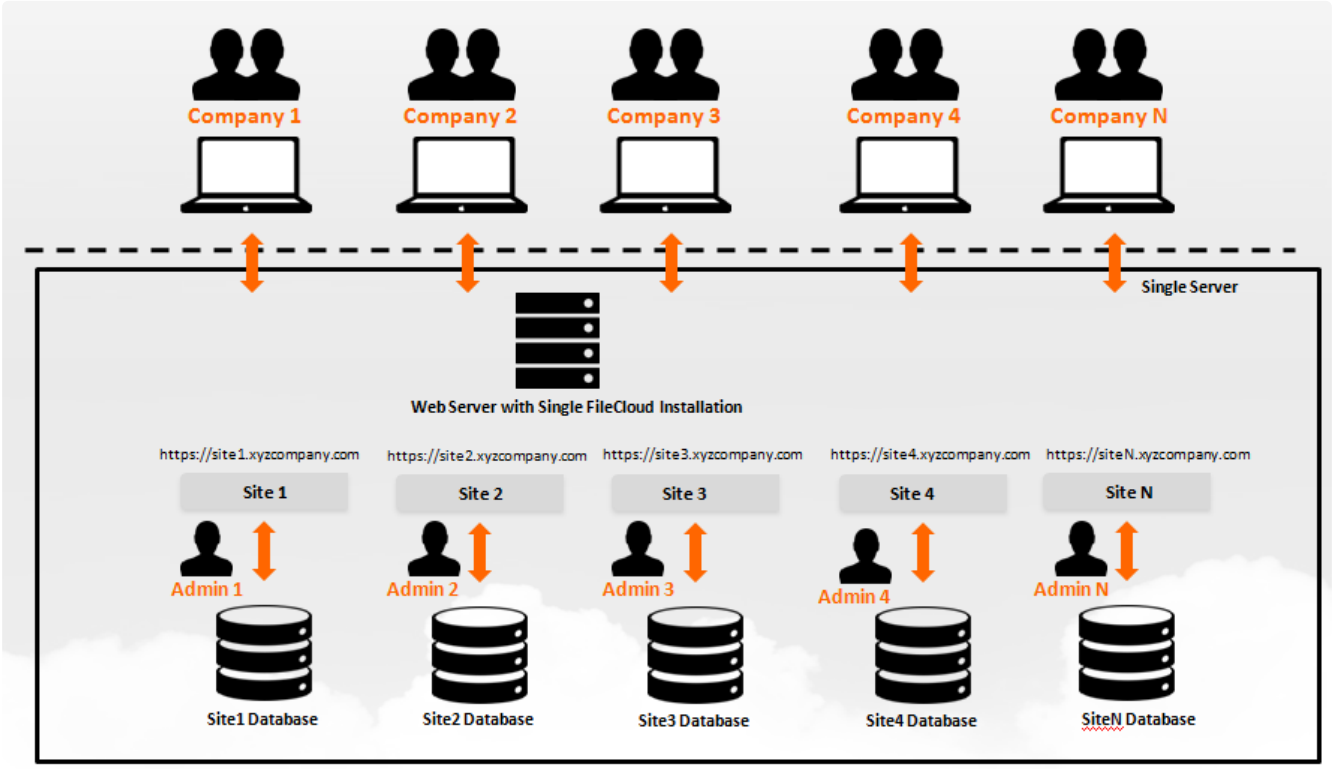
Finally, restart both MongoDB and Apache to get the security in-place.

Note

- In case of any issues, disable security in mongodb and fix the problems.
- To disable security, the mongodb security key has to be disabled and the database URLs have to be reverted back.

Multi-Tenancy Settings

It is possible with FileCloud to have a single install but still have many different independent FileCloud sites available.



In this section:

Multi-Tenancy Requirements

Administrators can install a single deployment of FileCloud Server but still have many independent FileCloud sites available.

General Requirements

1. You must have a fully working FileCloud installation before you proceed with multi-tenancy. Make sure all the install checks pass and all the checks in the admin portal are without errors.
2. Only a single SSL certificate can be installed for all the sites, so, it is recommended that you use a wildcard SSL certificate for a main domain, such as: https://*.xyzcompany.com and then set up each site as a subdomain of the main site, for example, site1.xyzcompany.com and site2.xyzcompany.com

3. After adding a new site, you need to add an entry in your DNS configuration for the new site to point to the server on which FileCloud is installed.
4. When removing a site added previously, only the site is removed from the list; however, any data associated with 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 includes a script that admins must use to generate an encrypted superadmin password and paste it into the multi-tenant configuration file.

Note: The default password in the multi-tenant configuration file cannot be used to sign in to the system.

To generate the password:

1. Locate the script file:
   Windows: C:/xampp/htdocs/resources/tools/security/passwordenc.php
   Linux: /var/www/html/resources/tools/security/passwordenc.php
2. Run the script. Your password should look similar to the password generated in the following code:

```
C:\xampp\htdocs\resources\tools\security>set path=C:\xampp\php

C:\xampp\htdocs\resources\tools\security>php passwordenc.php
This tool generates an encrypted password string
to paste into FileCloud configuration files

Enter your desired password: testpassword
Copy and paste the following string:
$pbkdf2-
sha512$50000$ENIGvUsu3T6rIbI5Bz9DXw$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtf
rVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw

Finished
```

3. Copy the string.
4. Find the sample multi-tenant config file:
   Windows: **C:/xampp/htdocs/config/multi-sample.php**
   Linux: **/var/www/config/multi-sample.php**
5. Copy **multi-sample.php**, and rename the copy **multi.php**.
6. Open **multi.php** and find the setting:

```
define("TONIDOCLOUD_MULTISITE_ADMIN_PASSWORD", 'Vrwfq7xNHV');
```

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

```
define("TONIDOCLOUD_MULTISITE_ADMIN_PASSWORD", '$pbkdf2-
sha512$50000$ENIGvUsu3T6rIbI5Bz9DXw$EwNxMRnJrMMjR8xP4nNwgq19voIzmp3bh9ATHXFn41tTybtf
rVYTyJVqSxG4jDmMjtGdY7fIH2TopwuNjgFPYw');
```

   Note: The encrypted password must be surrounded by single quotes (not double-quotes) or it will be broken.
8. Save and close **multi.php**.
   The user superadmin can now sign in using the clear text password you entered as your desired password in **passwordenc.php**.

To login into the special multi-tenancy admin portal:

1. Open a browser and access the FileCloud admin portal.
2. In **User**, type in superadmin.
3. In **Password**, type in the clear text password you entered in **passwordenc.php**.
4. If Two-Factor Authentication access is enabled, then provide the additional code to continue.

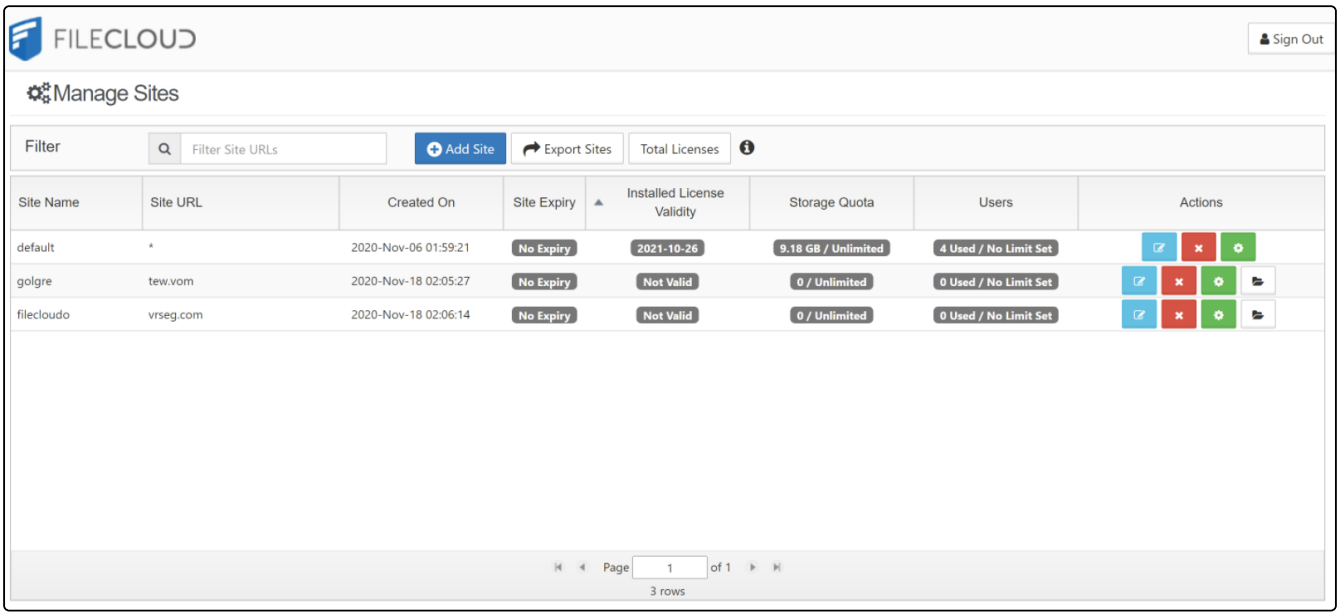
Manage Different Sites

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 a Cron job must be set up by the admin.**

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



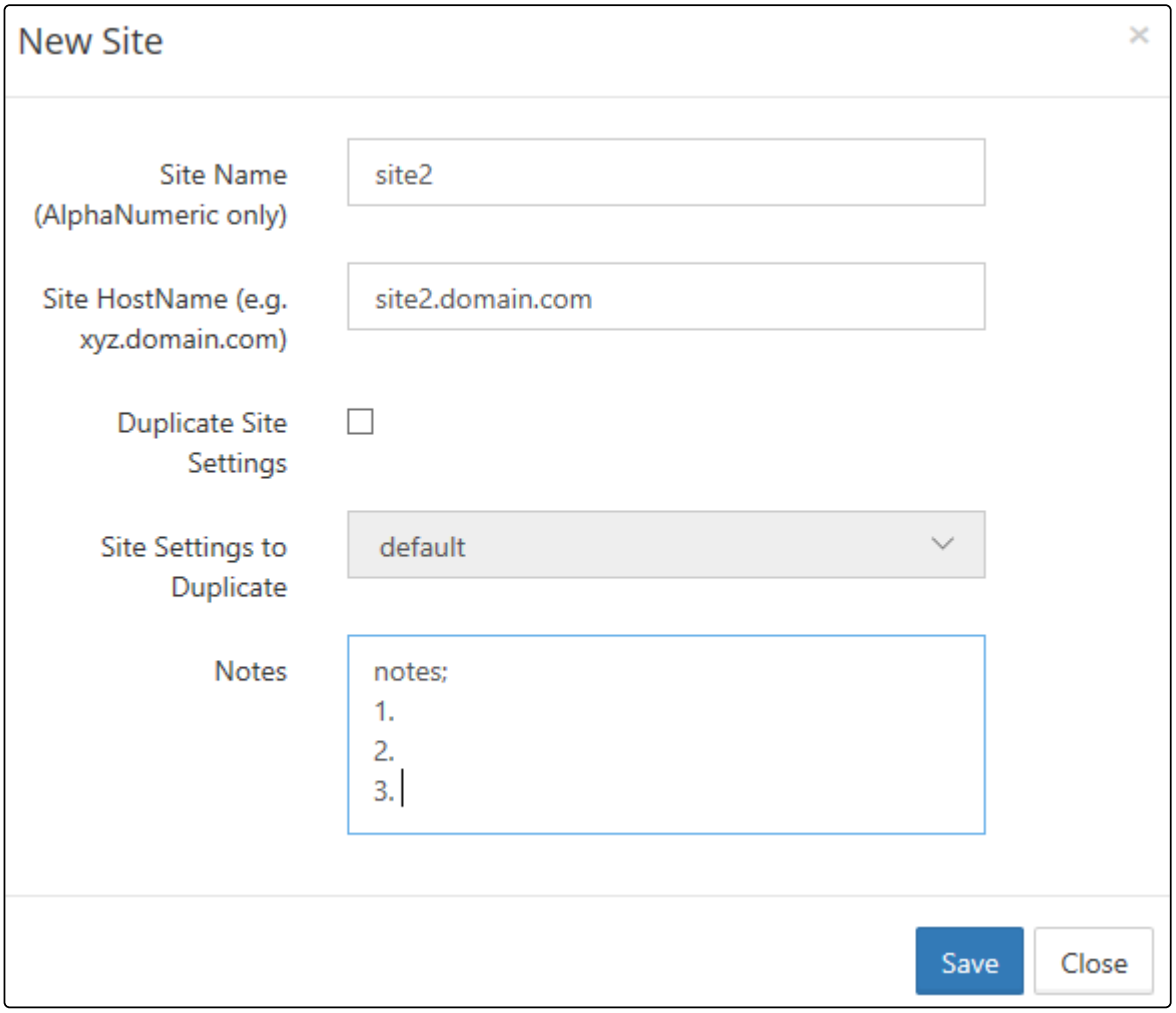
Since the report runs only once a month, updates to **Installed License Validity** may be delayed.

What do you want to do?

Add a new site

To add a new site, click on the **Add Site** button to open the **New Site** dialog box.

- Provide a **Site Name**, you cannot change the **Site Name** later. The **Site Name** must be alphanumeric and is used to prefix database names for this site.
- Provide the **Site HostName** (for example: site1.xyzcompany.com). Do not provide any http or https prefixes. The character @ is not permitted in site names.
- Make sure to add a DNS entry for the domain name to point to the server running FileCloud.
- You can duplicate the site settings by checking the **Duplicate Site Settings** check box. The new site is created with the settings from the duplicated site.
- **Notes** is optional.



View Site Settings

Site settings can be used to enforce limits on the total number of users and total storage quota in GB per site.

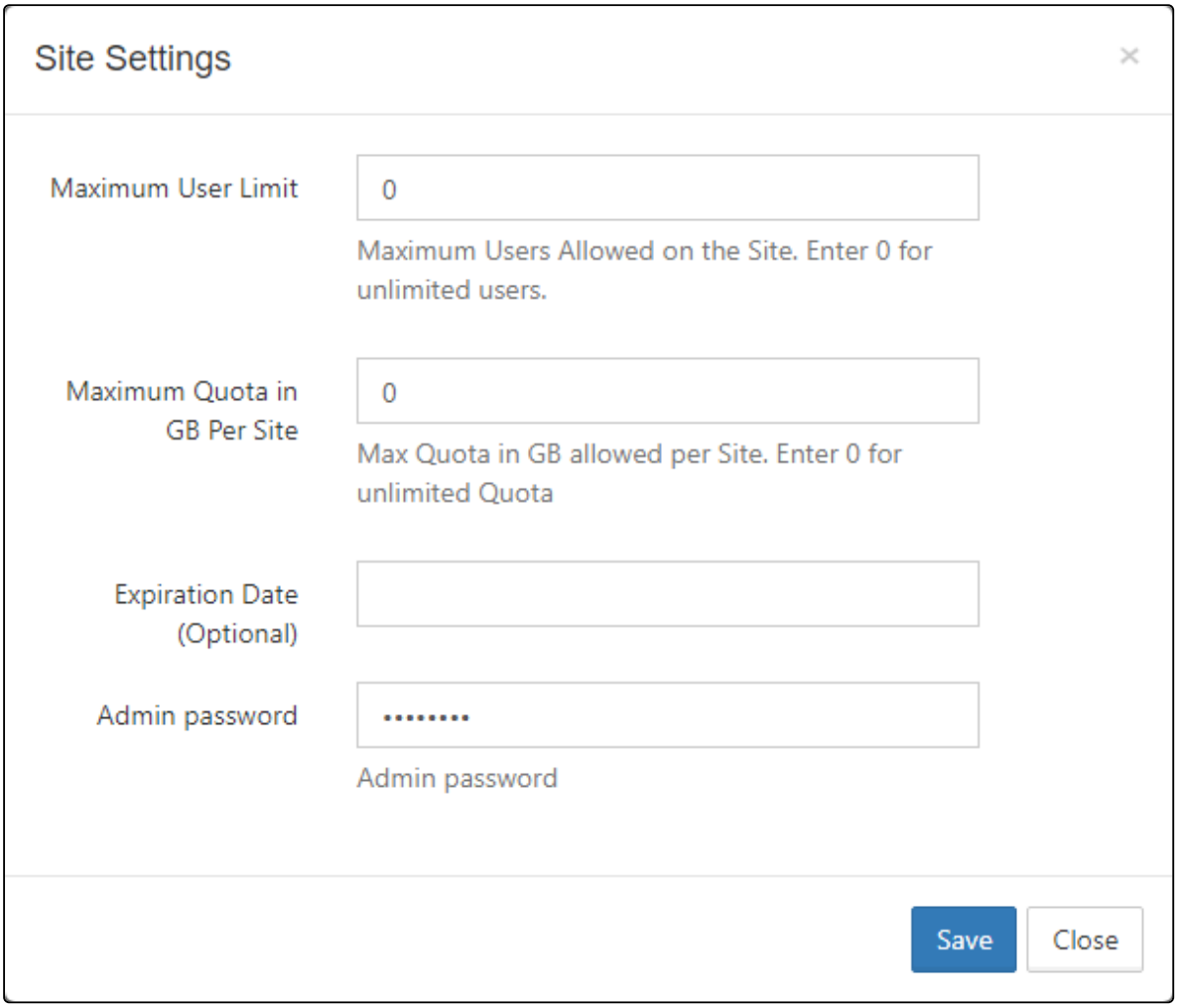
When **Maximum User Limit** is specified for a site, FileCloud does not allow additional users to be added when the limit is reached. 0 implies there is no limit to the number of users that can be added.

When **Maximum Quota in GB Per Site** is specified for a site, FileCloud limits the total GB of files added to ensure that total size of all files added will not be more than the quota specified. 0 implies unlimited quota.
Note: If the **User Storage Quota** (set in users' policies) for all users combined exceeds **Maximum Quota in GB Per Site** then new user creation is blocked. To enable admins to create additional users, the Superadmin must do one of the following:

- Increase **Maximum Quota in GB Per Site**.
- Set **Maximum Quota in GB Per Site** to 0 (unlimited).
- Set **User Storage Quota** (in all user policies) to 0 (unlimited).

When **Expiration Date** is specified, users cannot log in to the site after the expiration date is passed.

It is possible to set up an **Admin password** for a site directly in the **Site Settings** dialog box.



Access a newly added site

To access the newly added site, use the domain name setup for the site. For example, use https://site1.xyzcompany.com to access the user site and https://site1.xyzcompany.com/ui/admin/index.html to access the admin site.

Make sure to set up the site using the admin portal before opening up the site to new users.

> ⚠ All operations, including, use s3 backend, add files, enable encryption, disable encryption, create reports, and create workflows can be performed in multisites.

Remove a site

Select the site entry and click **Delete** to remove the site entry. Note that you have to manually remove the sites database and data. These are not removed automatically.

Note that the default site is the fallback site when a user tries to access FileCloud without using any of the domains specified and therefore cannot be edited or removed.

Enable Email Notifications if Cluster is Down

If you are running a multi-tenant system with FileCloud, make sure all site URLs for each site are accessible from the local site. They are used by the task scheduler/cron to run automated tasks for each site.

Email can be used to monitor not only clusters in a multi-tenancy but any MongoDB replica you have set up.

FileCloud uses a cron job (on Linux) or Windows Task Scheduler (on Windows) to perform certain ongoing maintenance tasks.
One of these tasks can be to send an email when one of the cluster instances or any MongoDB replica is down.

The email settings used for this notification are in **cloudconfig.php**.

- The email will be sent from: **TONIDOCLOUD_REPLY_TO_EMAIL**
- The email will be sent to the address configured in: **TONIDOCLOUD_DBSERVER**

These settings should already be configured in your **cloudconfig.php** file.

What do you want to do?

Add a PHP file to Cron

These instructions assume your FileCloud installation is 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
```

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

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

3. Save and exit.

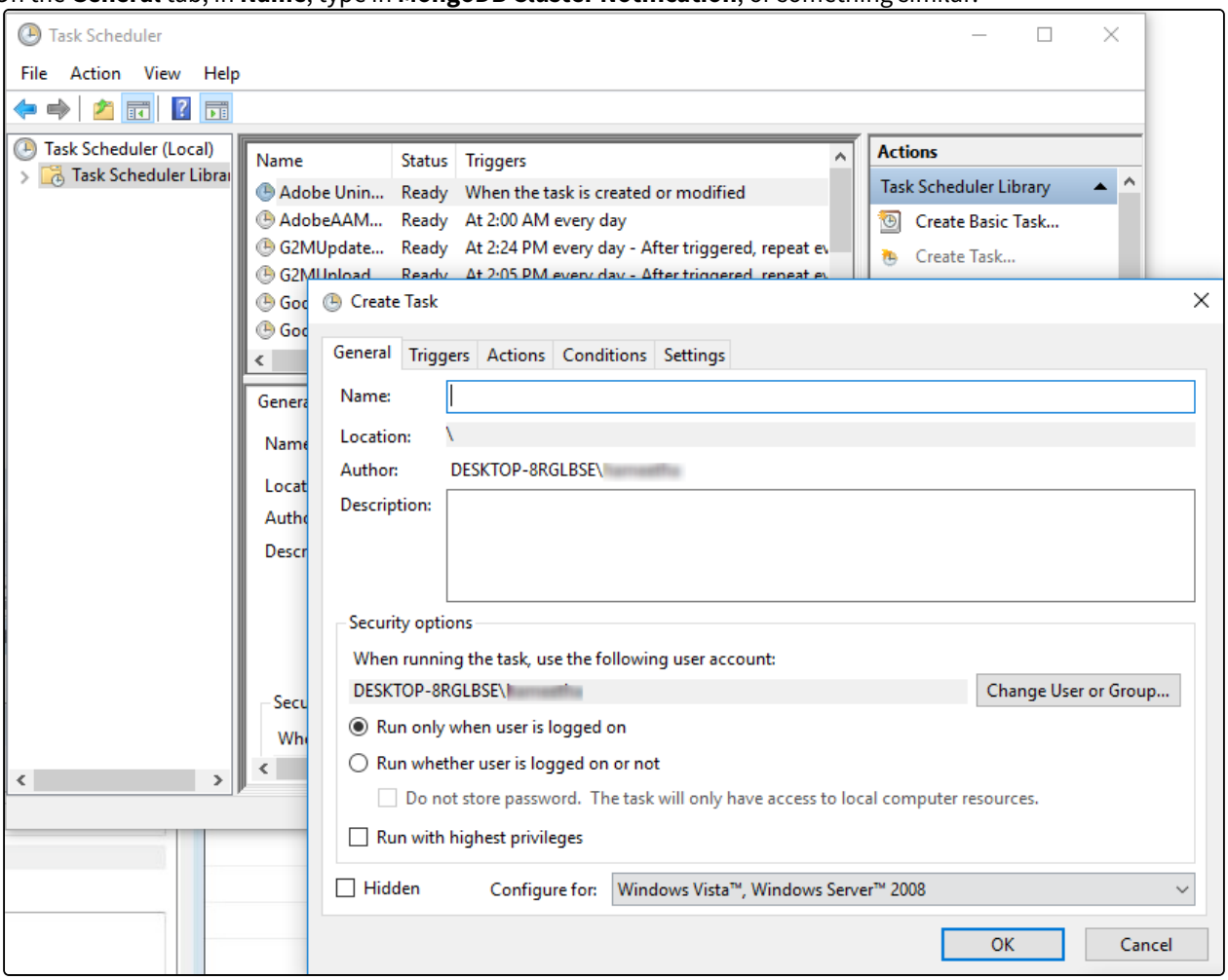
Add a PHP file to Scheduler

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**, as 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.

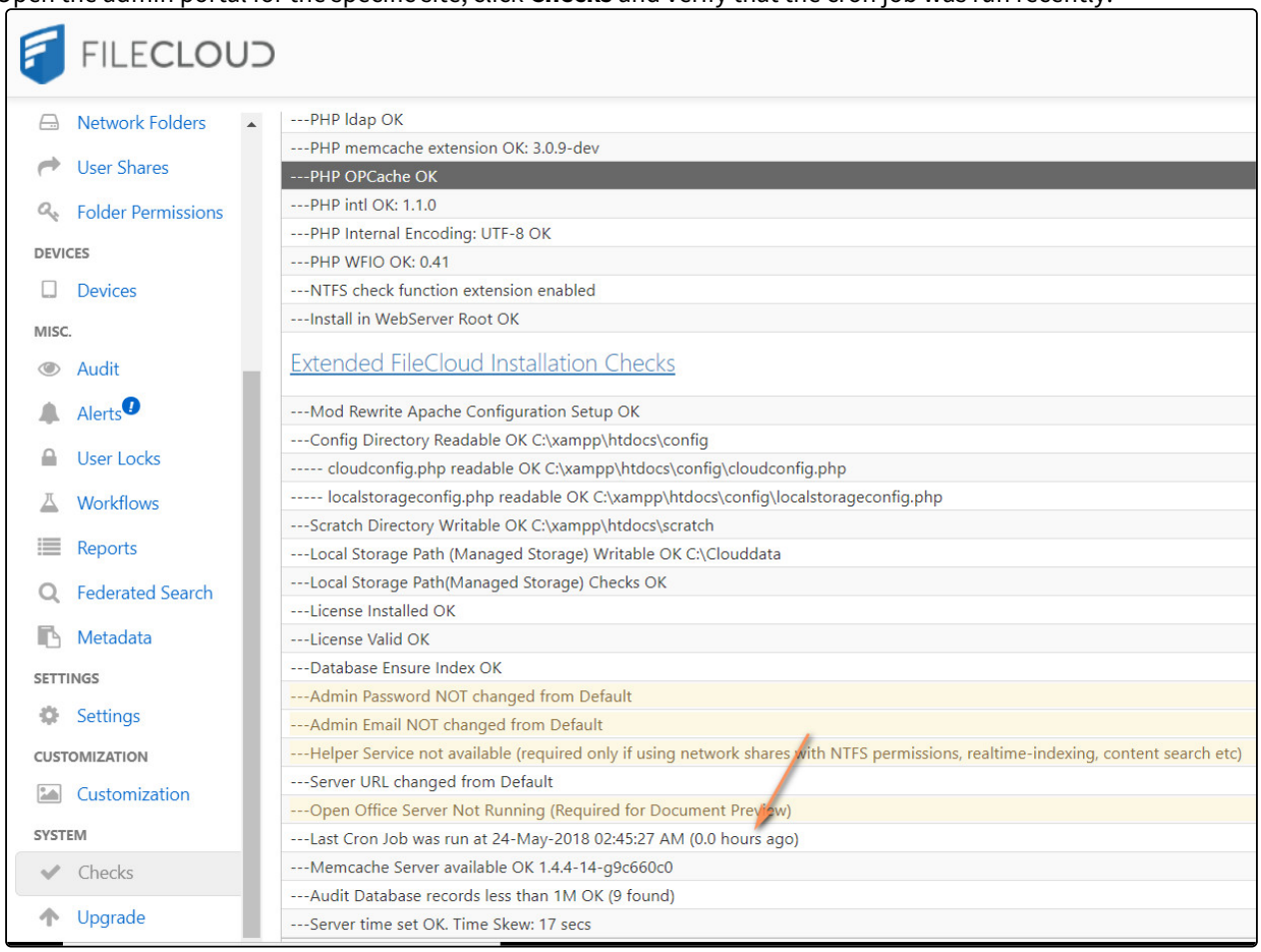
If a Task Scheduler/cron job is not set up for a multi-tenancy site with an SPLA license, license renewal/ reporting does not happen automatically.
The site does not acquire a license automatically after every month and the license can only be acquired by the admin logging in. If the monthly report is not completed, then users get a license error when they log in.

Name resolution and HTTPS:

- The URLs of all tenants must be resolvable on the FileCloud server. A workaround is to enter the tenant URLs in the local hosts file.
- If HTTPS is used, the SSL certificates must be installed in Apache even if the SSL termination is done in an external load balancer.

If site licensing expires every month and doesn't get renewed automatically when using the SPLA license, please follow the following steps to troubleshoot.

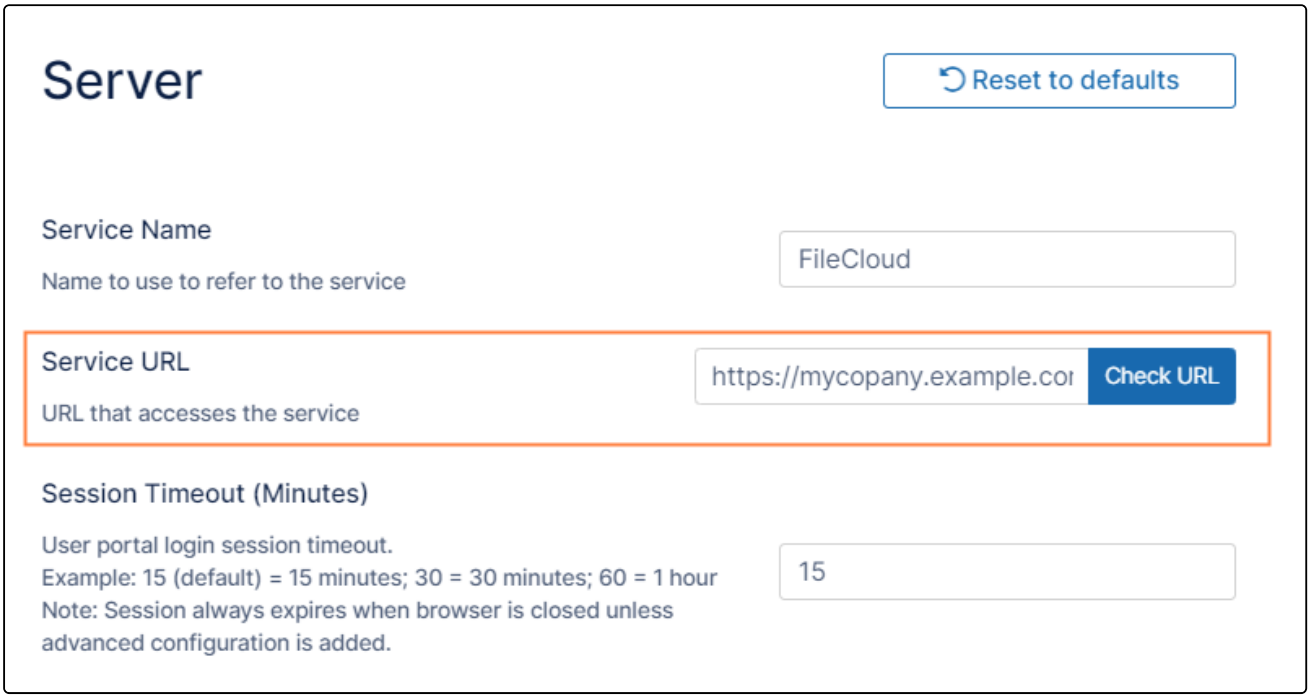
1. Open the admin portal for the specific site; click **Checks** and verify that the cron job was run recently.



2. If the cron job was not run recently, it is **critical** that a Task Scheduler or cron job be set up to run properly when running a multi-tenant system. See instructions on how to set this up. When running cron jobs 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 Server settings page to access the site. Make sure the Server URL works on the local system correctly.
If you are using an HTTPS site, ensure that the Server URL has the correct prefix (https instead of http). After making the Server URL change, wait some time to see if the cron job is now reported as working correctly.

> Note: If your DNS doesn't resolve the site URL inside the FileCloud server, you can work around it by adding an entry to the domain name to the local Windows HOSTS file in the server.


Server
Reset to defaults
Service Name
Name to use to refer to the service
FileCloud
Service URL
URL that accesses the service
https://mycopany.example.cor
Check URL
Session Timeout (Minutes)
User portal login session timeout.
Example: 15 (default) = 15 minutes; 30 = 30 minutes; 60 = 1 hour
Note: Session always expires when browser is closed unless advanced configuration is added.
15