FileCloud Online Version 23.252

FileCloud Site Setup

Printed on 10/07/2025

Copyright Notice

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

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

Level of Priority	**Administrator Settings**	**Server Settings**	**Storage Settings**	**User Access Settings**
Required	Access the Admin Portal Admin Portal Dashboard Change the Admin Password Manage Account Approvals	Admin Settings Server Settings Manage Client Security Settings Configure Share Settings	Configure Team Folders	Create FileCloud Users Check User Access Level Create User Policies Create Groups Manage User Storage Quotas
Recommended	Configure Email Settings	Set Client Application Policies		Manage User Authentication • Configure Single Sign-On • Use LDAP Based Authentication • Active Directory Authentication Set Up 2FA Configure Microsoft Office Integration Options
Provides a Better Experience	Add Customization and Branding			Enable MS Teams Integration Set Up Notifications for File Changes Automate Business Workflows Enable Users to Set Folder-Level Permissions Enable reCaptcha

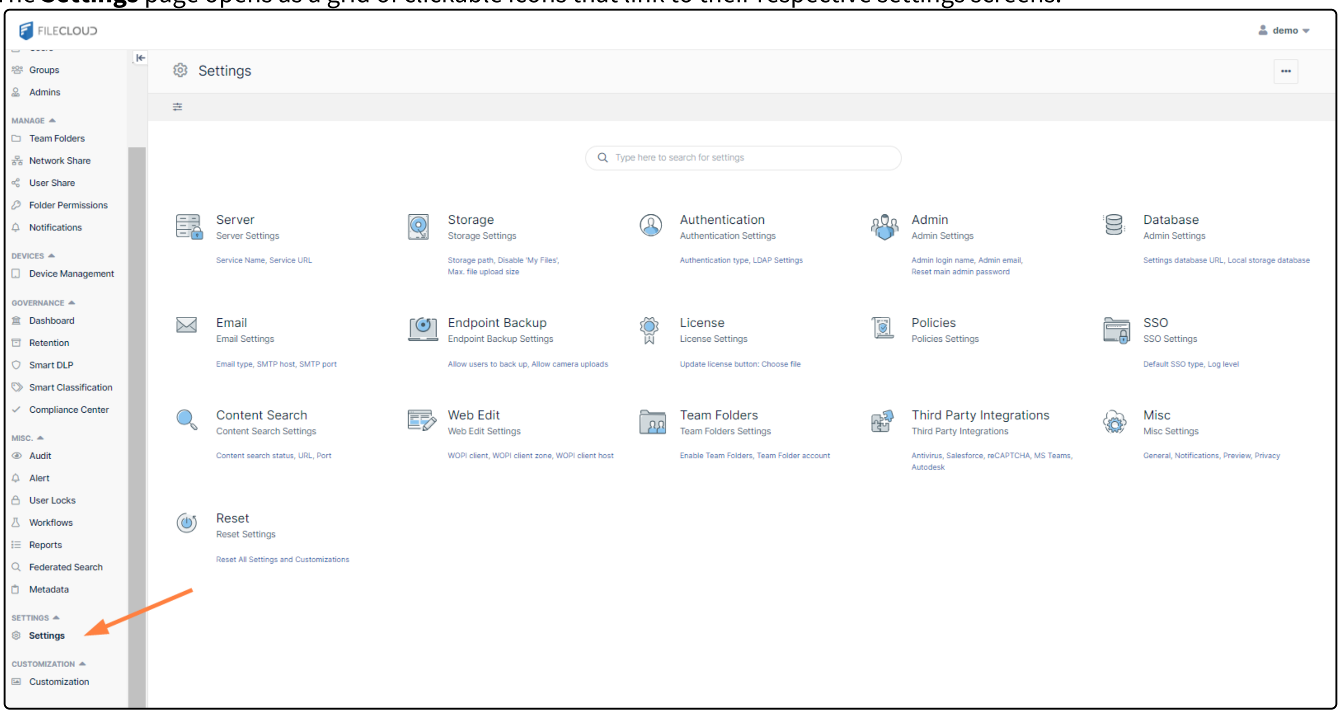
Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Advanced features	Set Up Compliance Checking • HIPAA • ITAR • GDPR • PDPL • NIST	Set Up Data Governance		

Navigating and Searching for Settings

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

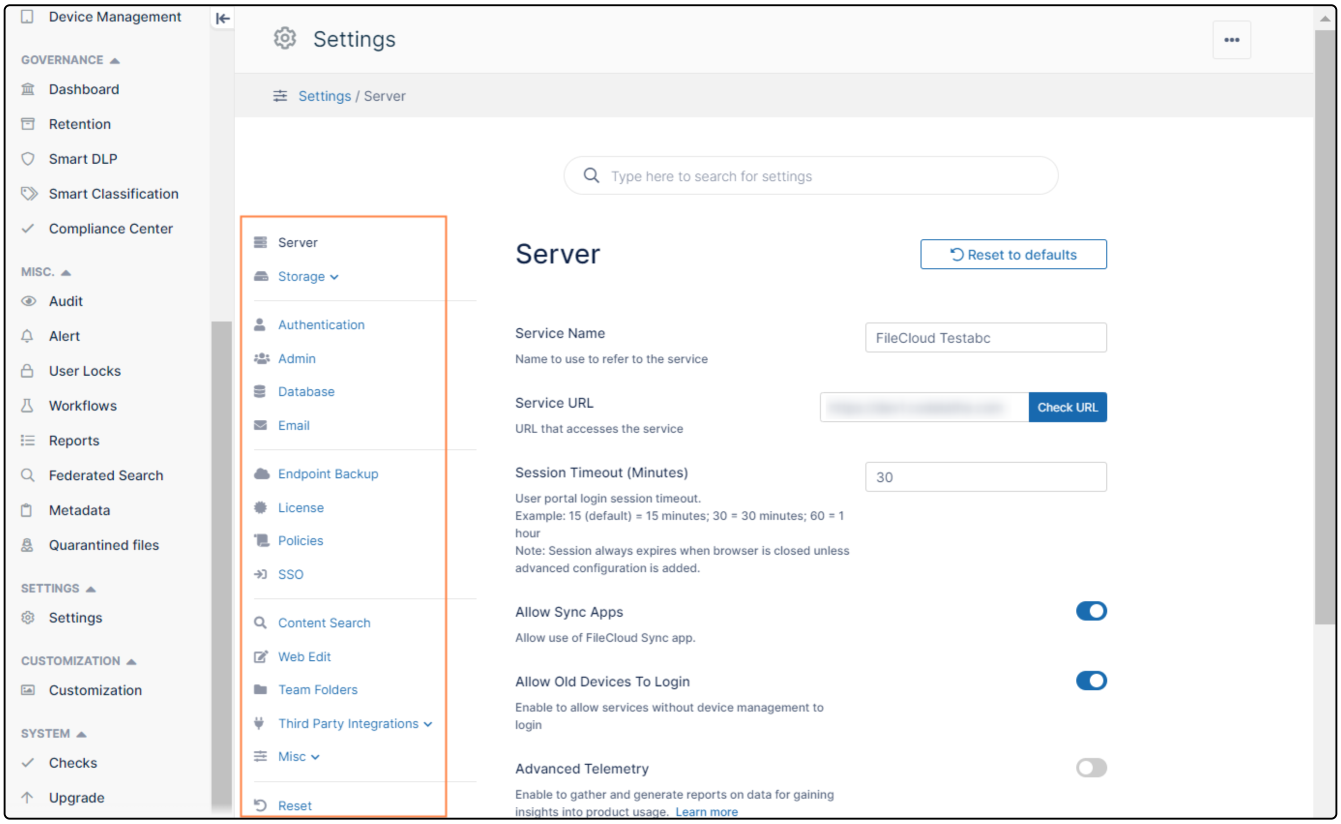
Going to the Settings landing page

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

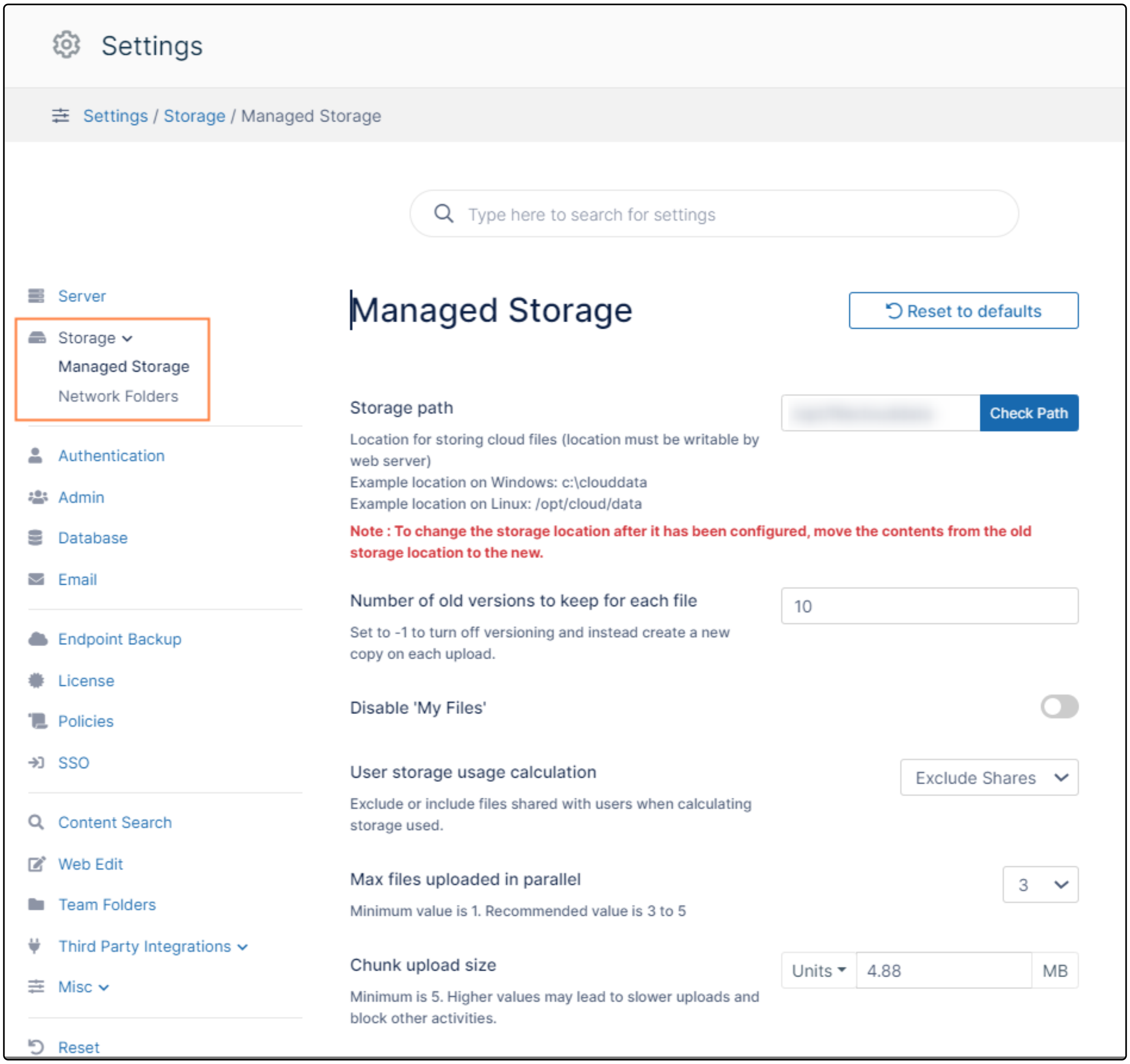


Go to a settings page

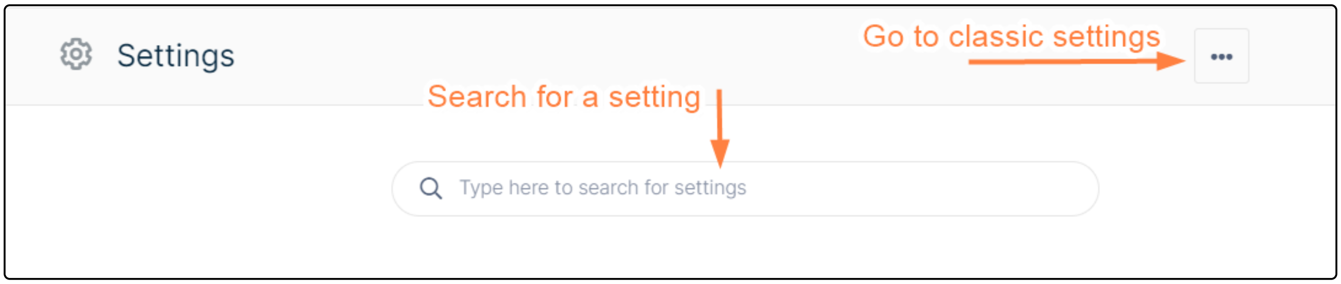
When you click a setting icon, it takes you to its settings page, and shows a navigation panel for going to other settings pages to its left.
In the following image, the Server icon has been clicked and the Server settings appear. The navigation panel to the left appear on every settings page and lets you to navigate to the other settings pages.



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



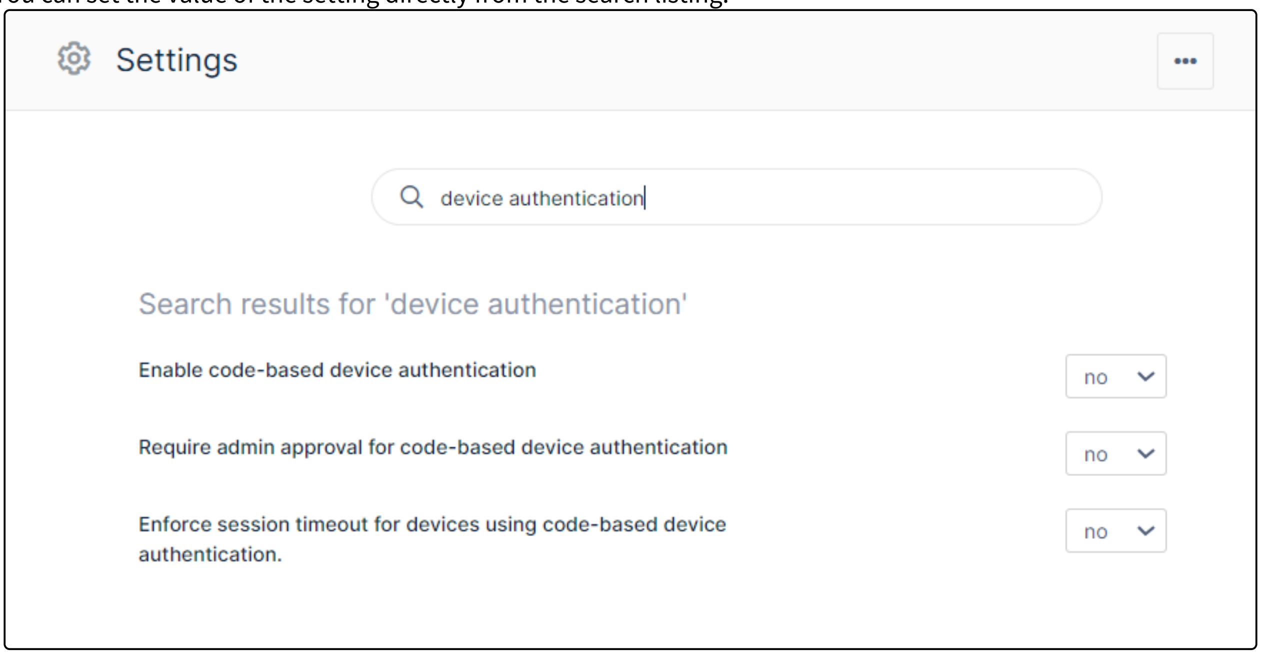
Above the settings icons, a search bar where you can search for settings and a link to the classic settings user interface appear.



Searching for settings

To search for a setting:

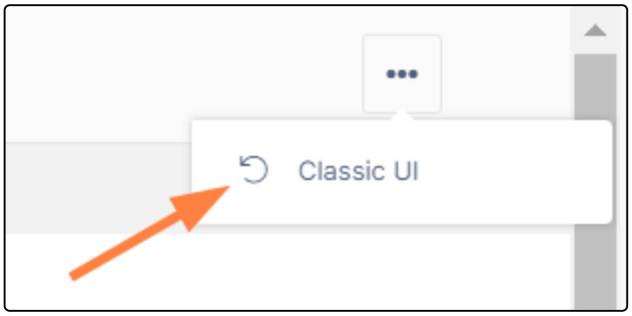
1. Enter the search string into the search bar.
2. Settings with a matching name or description are returned.
3. You can set the value of the setting directly from the search listing.



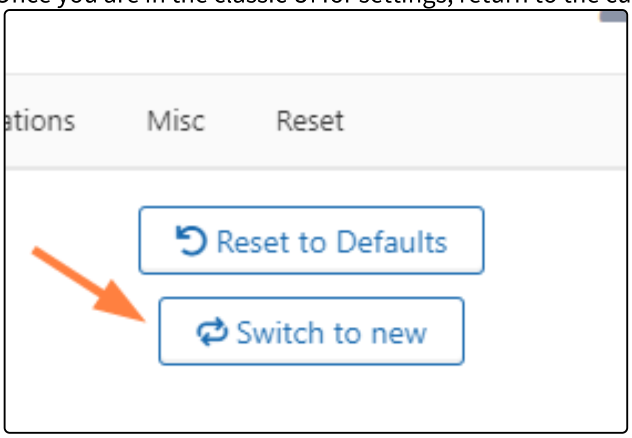
4. To return to the Settings landing page, clear the search box.

Going to classic settings

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

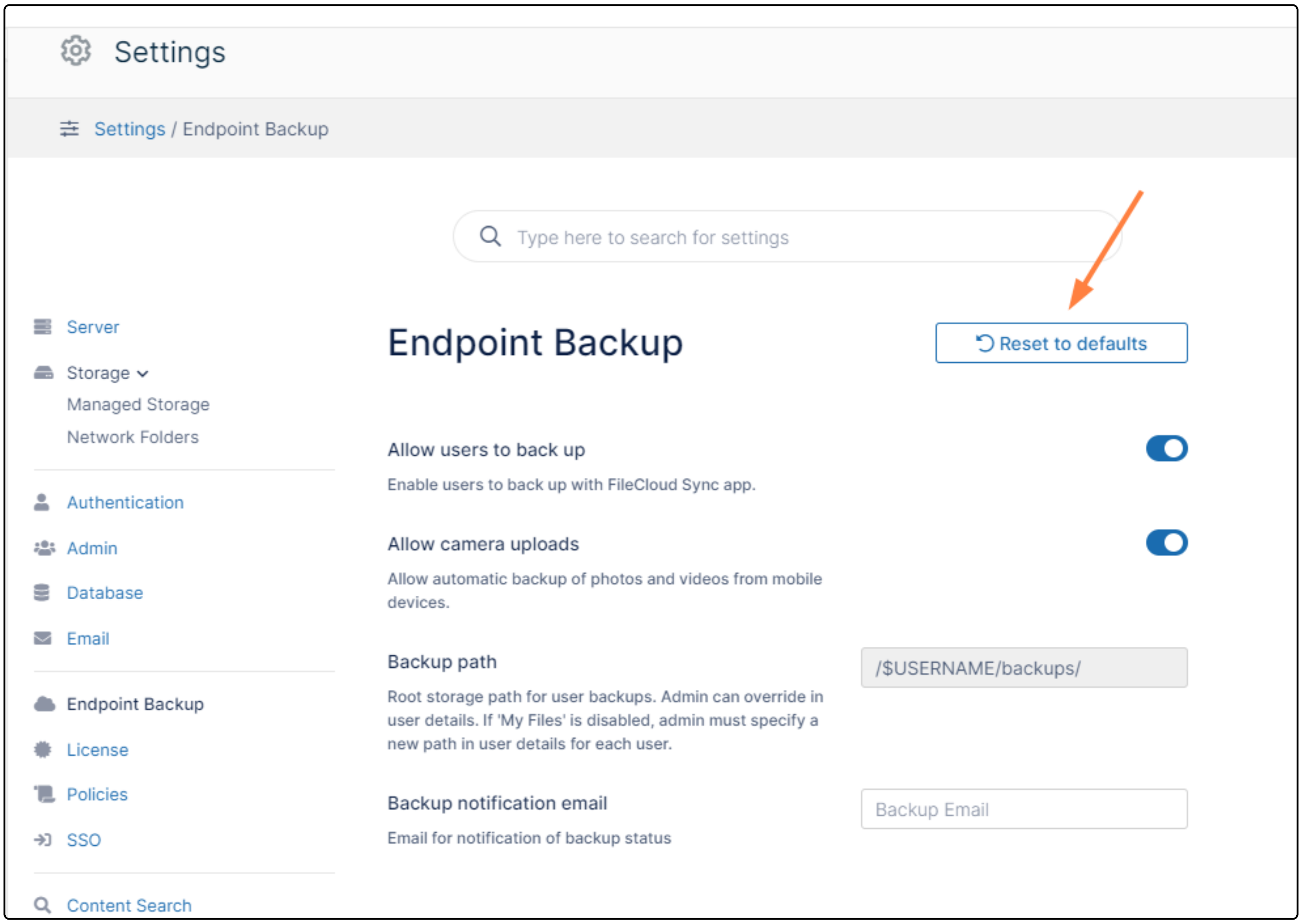


Once you are in the classic UI for settings, return to the current UI by clicking **Switch to new**.



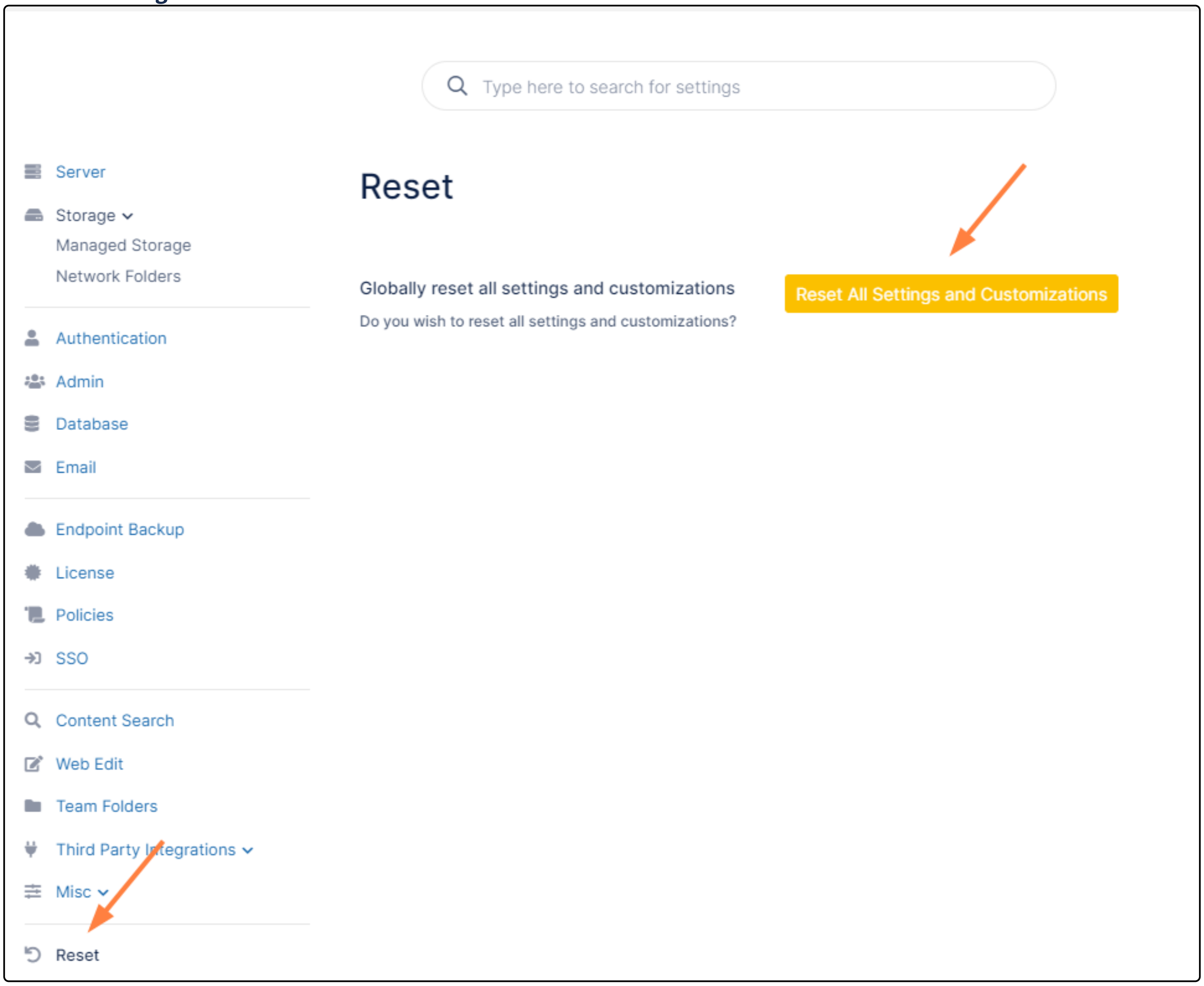
Reset settings

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



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

Reset All Settings and Customizations.

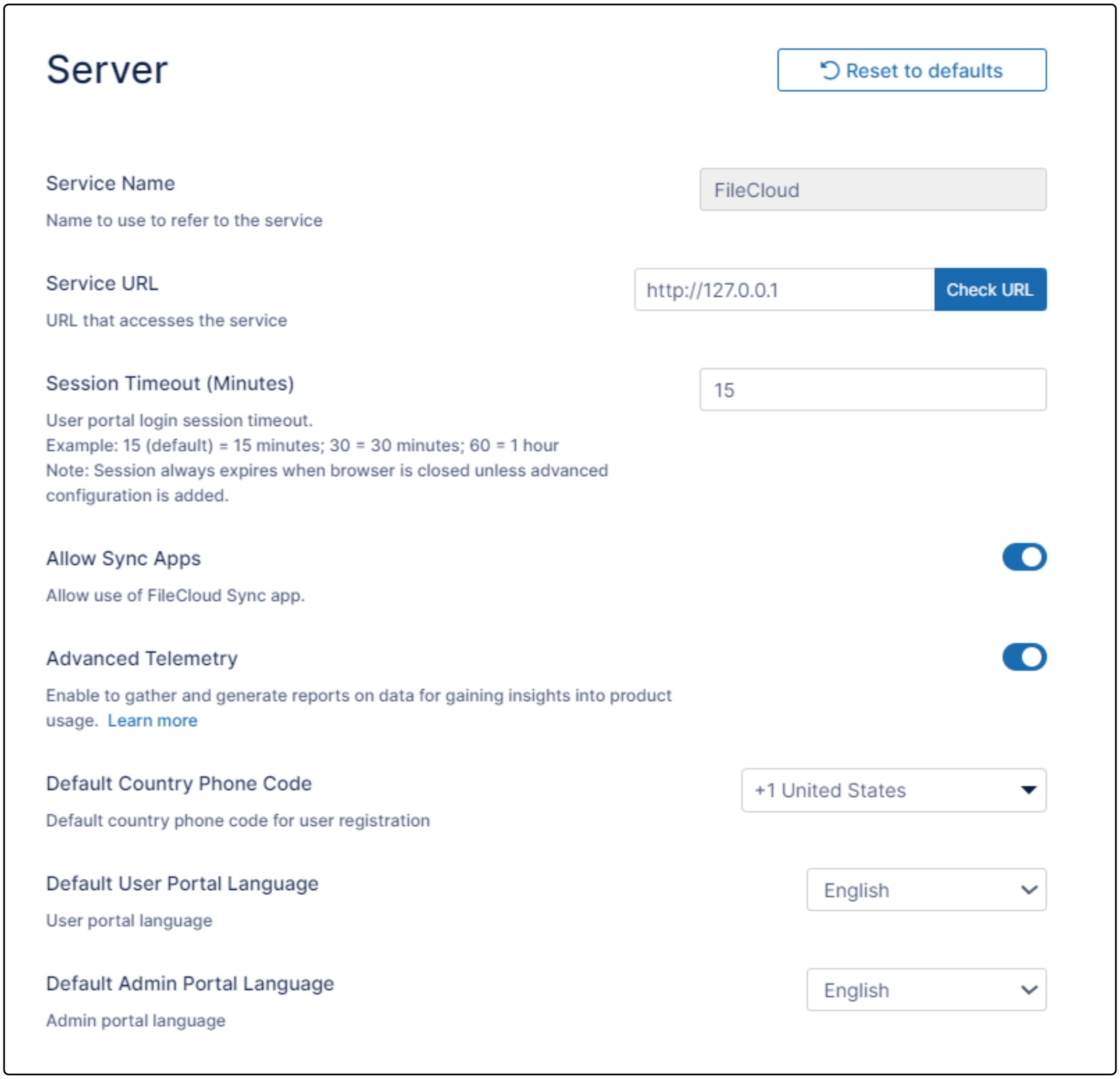


Server Settings

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

To set the Server settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server**  .
   The **Server** settings page opens.
2. Fill in the settings as shown in the following screenshot, using the table below as a guide.



<table>
<tr><th>Settings Name</th><th>Description</th></tr>
<tr><td>Service Name</td><td>The name to be used when referring to your FileCloud service. This is used in email messages, in the zip filename for multiple downloads, and anywhere else your service is referred to by its name.</td></tr>
<tr><td>Server URL</td><td>The URL by which users access your FileCloud site, for example, https://xyz.company.com.</td></tr>
<tr><td>Session Timeout</td><td>The number of minutes the browser session is valid.
If the browser is closed, the session is logged out.
By default Session Timeout value is only applicable for the user portal and not for other FileCloud clients such as Sync, Drive, and FileCloud Desktop. To apply Session Timeout to other clients, see User Session Expiration
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>15 (default value)</td><td>Session expires in 15 minutes (minimum session timeout)</td></tr>
<tr><td>1</td><td>Session Expires in 1 minute</td></tr>
<tr><td>60</td><td>Session Expires in 1 hour</td></tr>
</table></td></tr>
<tr><td>Allow Sync Apps</td><td>Enabled by default. Disable to block all Sync apps from connecting to this server and performing sync operations.</td></tr>
<tr><td>Allow Advanced Telemetry</td><td>Allow FileCloud to gather diagnostic and usage data.</td></tr>
<tr><td>Default Country Phone Code</td><td>The default country code that appears in the user portal when share creators invite users to a share and when users add/modify their phone numbers in settings.</td></tr>
<tr><td>Default User Portal Language</td><td>The language that is used when a user logs in to the user portal.</td></tr>
</table>

Settings Name	Description
Default Admin Portal Language	The language that is used when an administrator logs in to the admin portal.

Storage Settings

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

Managed Storage	Set Up Managed Storage
Protecting Your Storage	Set up Managed S3 Storage Encryption

FileCloud Managed Storage

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

Setting up Managed Storage

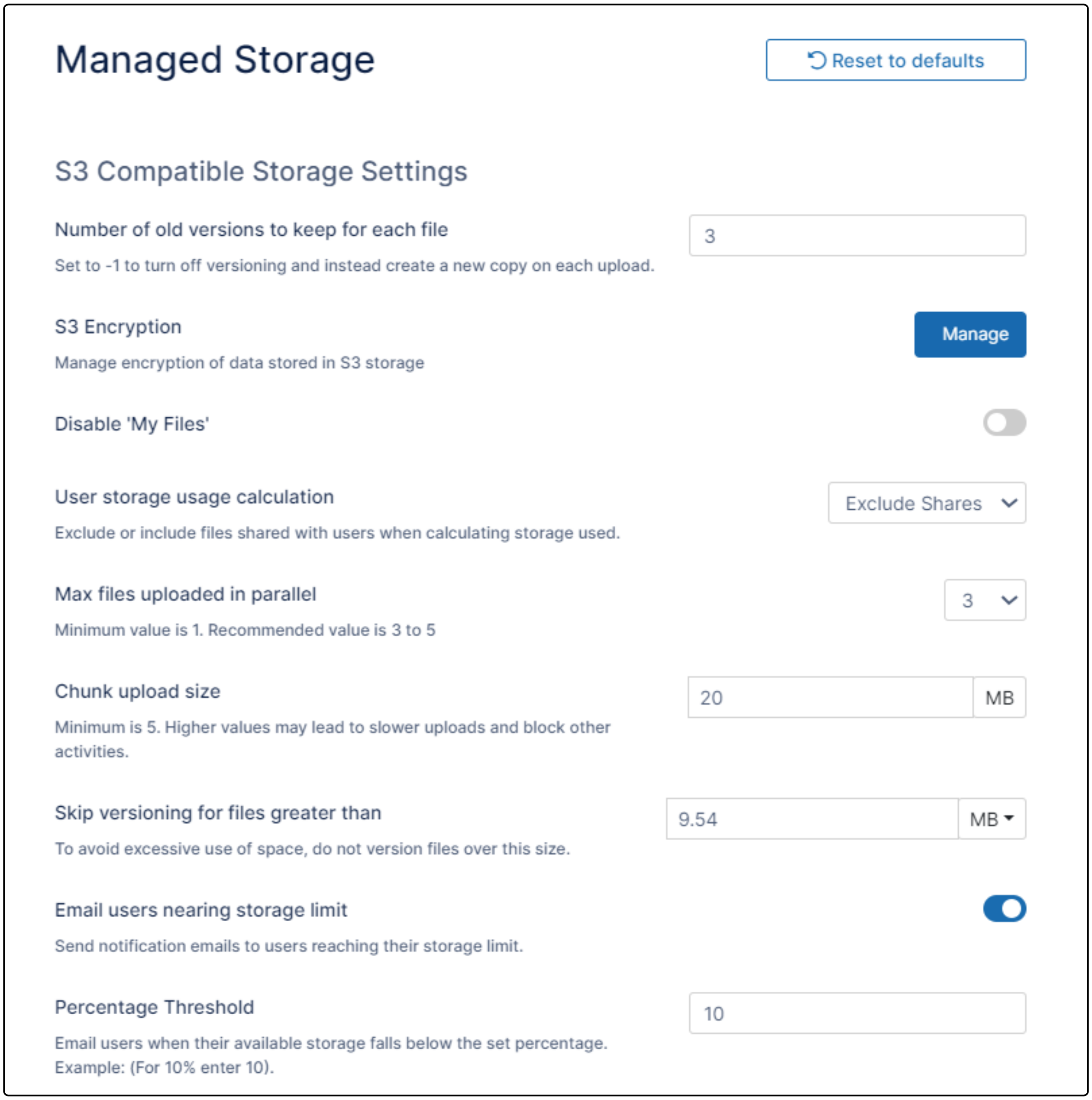
Administrators can configure how users store data in Managed Storage settings.

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
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.

Setting	Description
S3 Encryption	Appears when encryption is enabled in your system, and allows you to manage encryption. See Enabling S3 Storage Encryption.
Disable 'My Files'	If you are only using the "Network Folders" features of FileCloud and don't want to show "My Files", you can enable this checkbox. If there are existing data in the "My Files" section, the data will no longer be accessible. Certain functions that depend on My Files will no longer be available.
User storage usage calculation	When the user storage usage is reported, the shares used by the user can also be counted towards the quota. This can be changed by selecting the appropriate drop-down option.
Max files uploaded in parallel	Number of files that can be uploaded at the same time when multiple files are uploaded. Default is 3. The recommended number is 3 to 5. Higher values may slow down the upload process and lower system efficiency.
Chunk upload size	The maximum size in MB for chunks uploaded. Default is 20. If size is set too high, the upload process may slow down and other operations may be blocked.
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.

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.**
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.

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

Before you can set your S3 encryption options, S3 encryption must be configured in your system. If is not yet configured, contact your FileCloud representative for help.

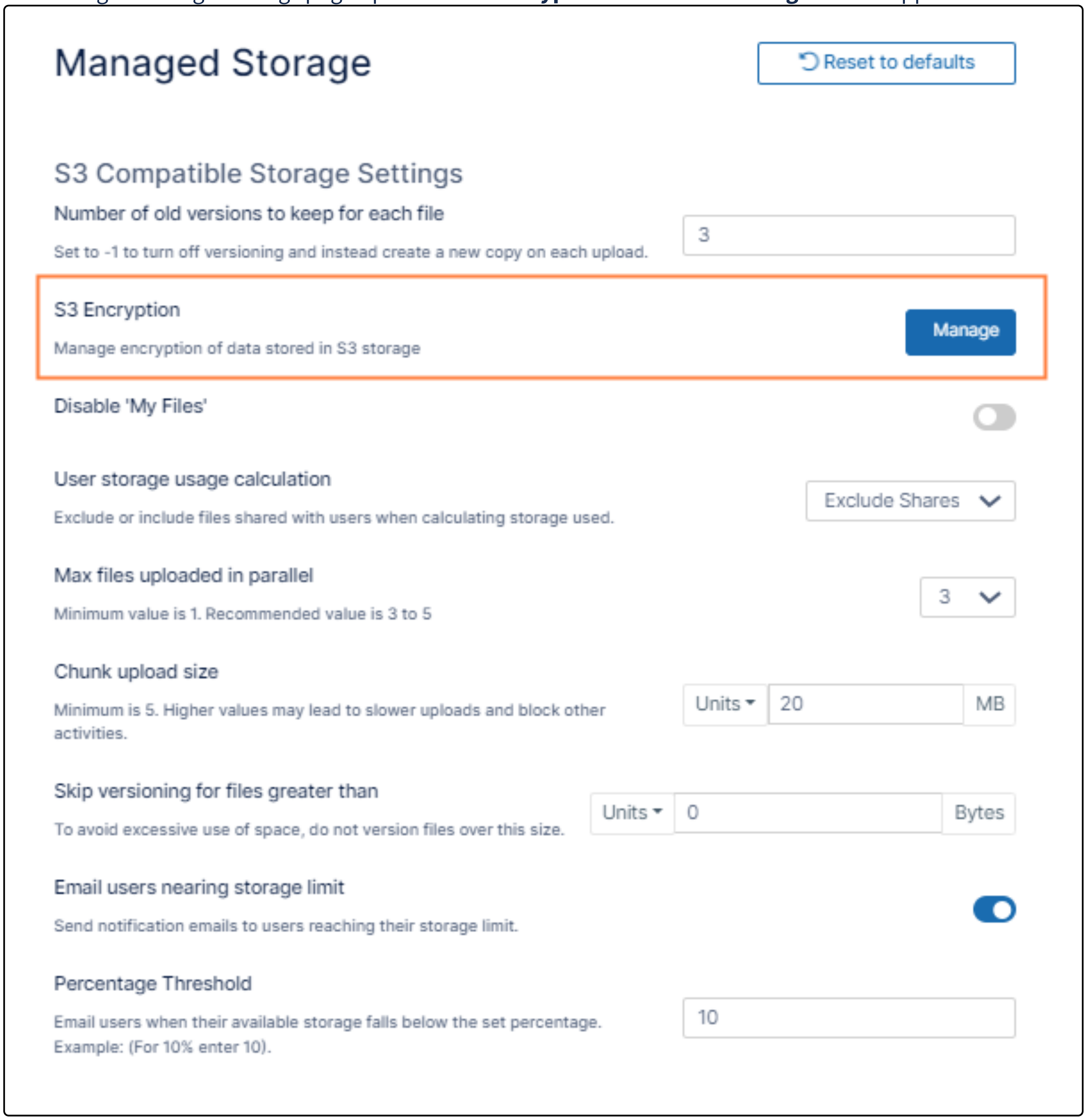
After S3 encryption is enabled, the Admin Portal will display new options for managing it.

> **Warning On Master Password**
>
> If an optional master password was specified, 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.

To manage S3 encryption:

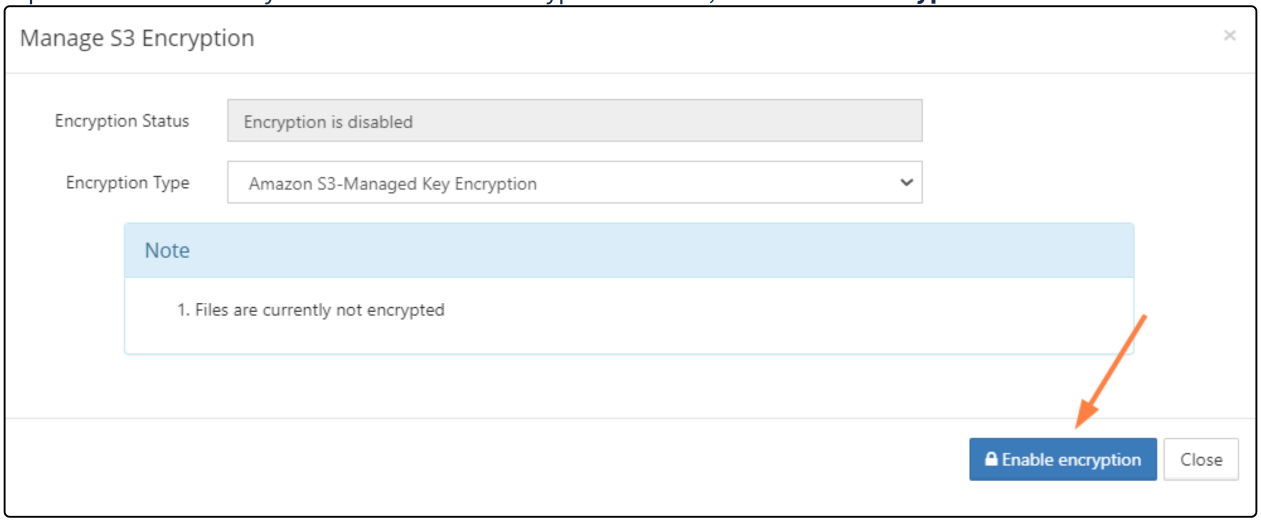
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .

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



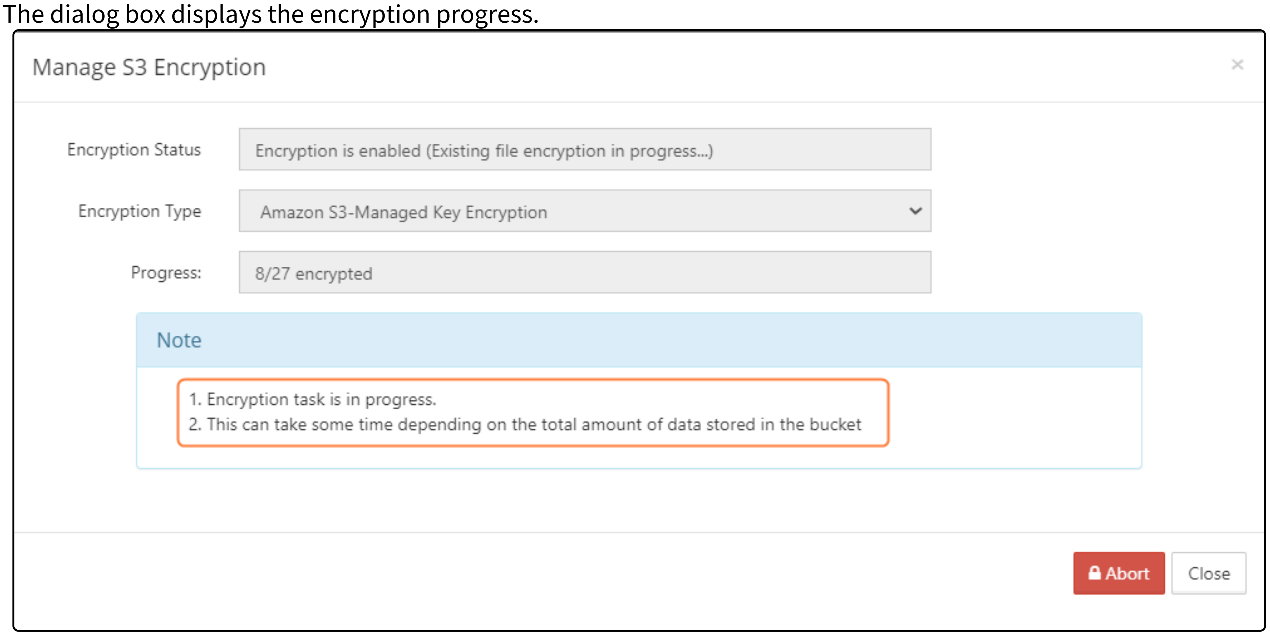
2. Click **Manage**.
   The **Manage S3 Encryption** dialog box opens

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

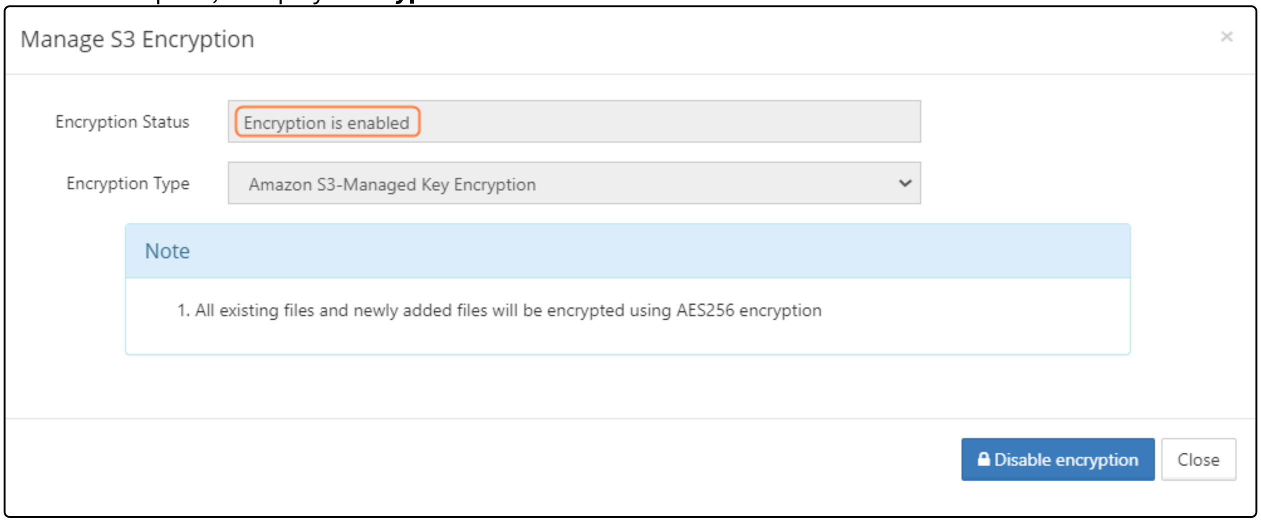


You are prompted to confirm encryption.

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



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



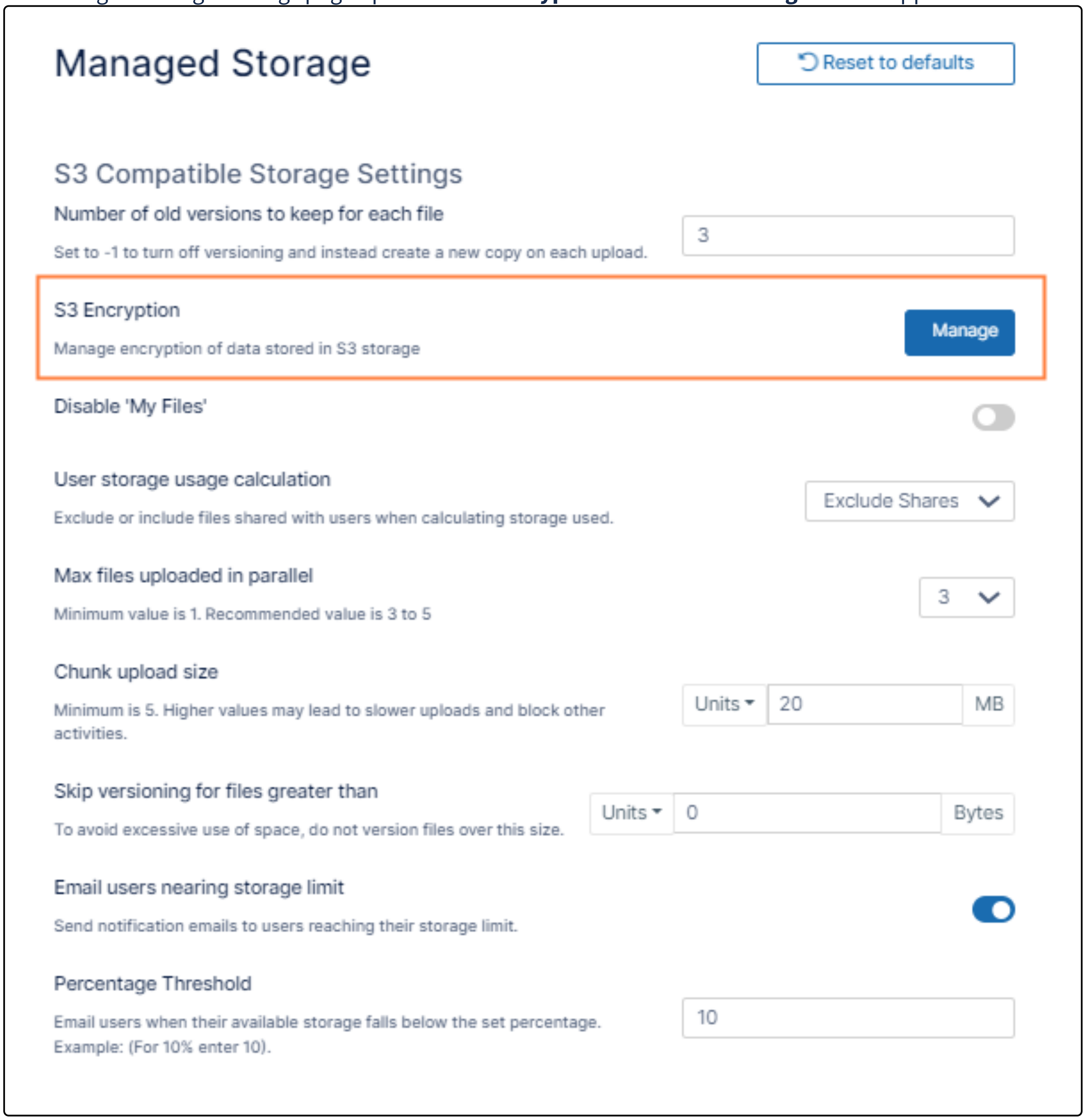
Disabling S3 Storage Encryption

Administrators can disable S3 storage encryption following the steps here.

To disable S3 encryption:

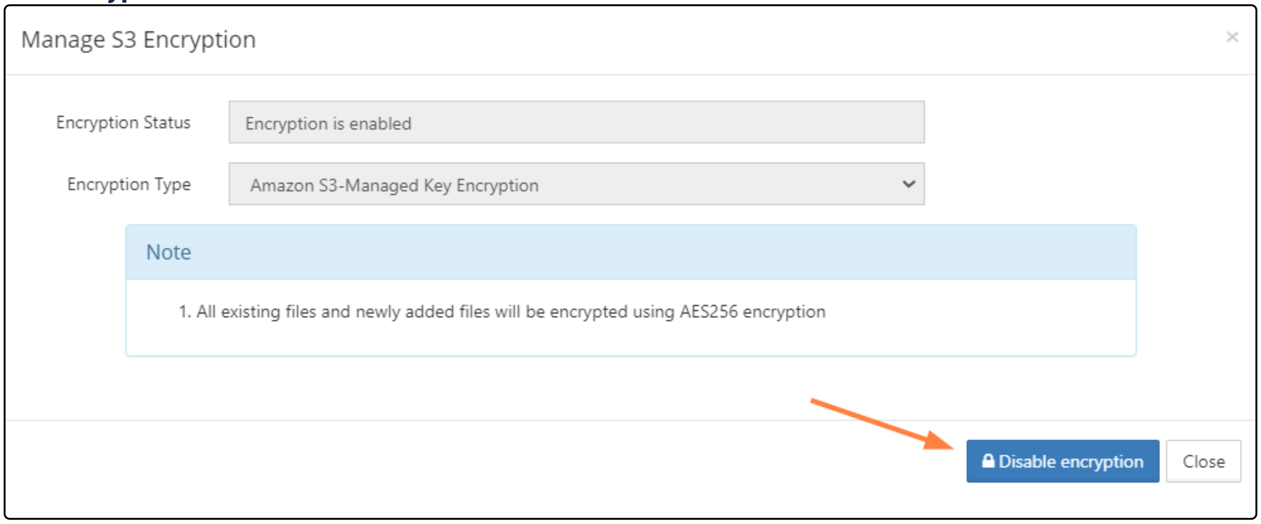
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .

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



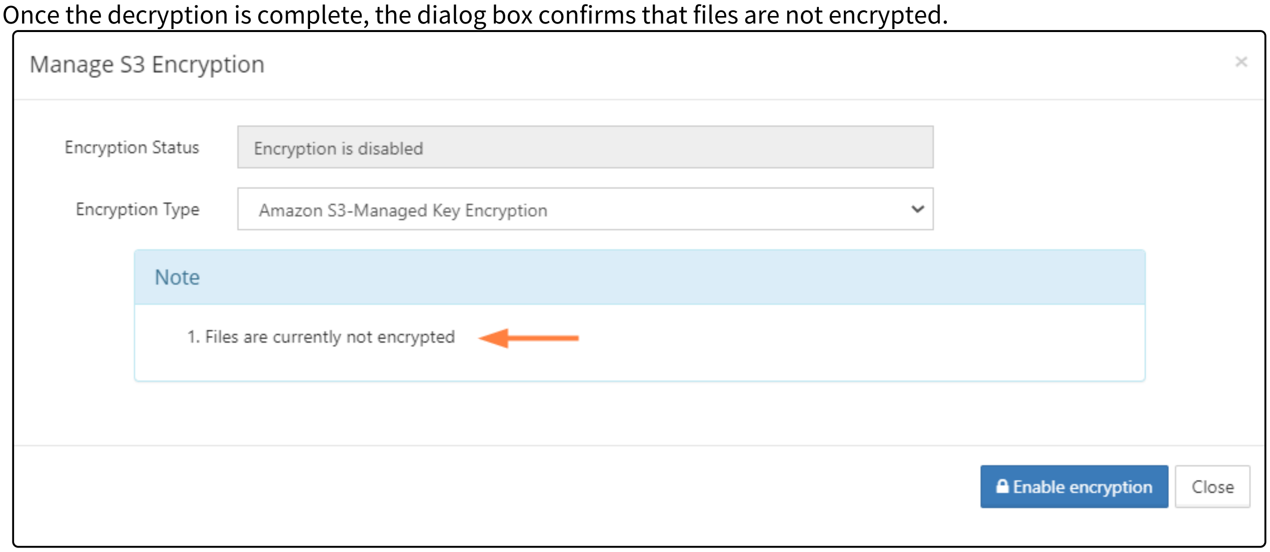
2. Click **Manage**.
   The **Manage S3 Encryption** dialog box opens

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 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.

Setting Up MongoDB Enterprise Advanced Server

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

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

Install MongoDB Enterprise Advanced

Installing on Ubuntu

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

```
sudo apt-get install gnupg curl

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

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

   --dearmor
```

2. Go to **/etc/apt/sources.list.d/**

3. Create the list file **mongodb-enterprise-6.0.list**:

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

4. Reload the local package database:

```
sudo apt-get update
```

5. Install MongoDB Enterprise Advanced:

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

Installing on RHEL

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

```
[mongodb-enterprise-6.0]

name=MongoDB Enterprise Repository

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

gpgcheck=1

enabled=1

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

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

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

Configure the connection to FileCloud for Ubuntu or RHEL

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

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

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

```
mongosh private_ip
```

   Then create the user:

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

   Finally, verify the connection from the FileCloud server:

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

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

```
// ... Cloud Database

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

// ... Audit Database

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

// … Settings Database

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

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

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

Installing on Windows

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

Configure the connection to FileCloud for Windows

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

   ```
   bindip: 127.0.0.1
   ```

   to

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

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

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

   Connect to the mongo shell.

   ```
   mongosh private_ip
   ```

4. Switch to the admin user:

   ```
   use admin
   ```

5. Create a new db user:

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

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

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

7. From the FileCloud server, verify the connection:

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

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

```
// ... Cloud Database

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

// ... Audit Database

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

// … Settings Database

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

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

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

Manage the Recycle Bin Using Policies

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

Why?

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

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

Do you want to store deleted files for recovery purposes?

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

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

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

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

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

This is configured by the setting called:

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

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

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

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

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

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

This is configured in the following setting:

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

Files less than this size are stored

Files greater than this size are permanently deleted

You can specify the file size in the following ways:

- GB
- MB
- KB
- B

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

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

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

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

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

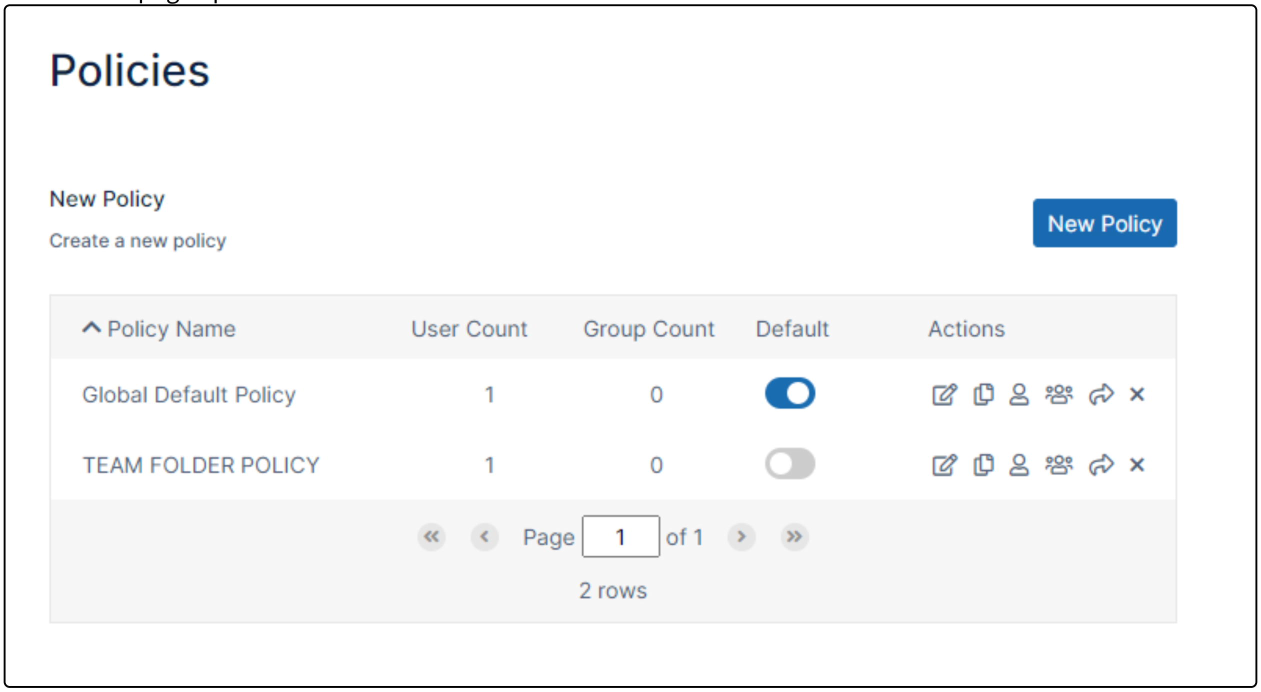
Setting	Option	Description
Automatically delete files from recycle bin after set number of days	Whole number	Number of days after a file was deleted that it will be automatically cleared from the recycle bin (and therefore, no longer be present in FileCloud). A value of 0 indicates that deleted files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

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

To configure a recycle bin policy for users or groups:

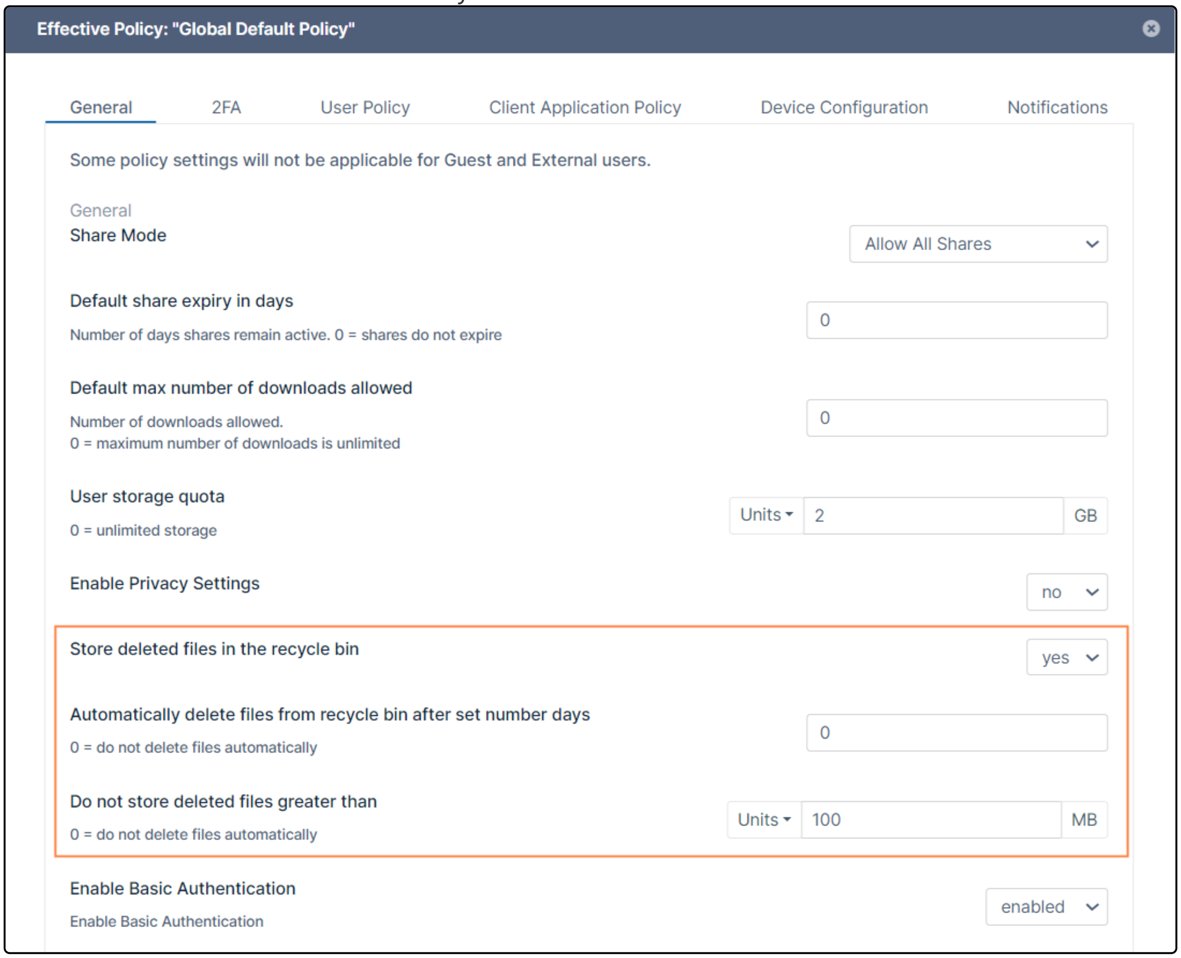
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .

The **Policies** page opens.



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

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



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

Disable My Files

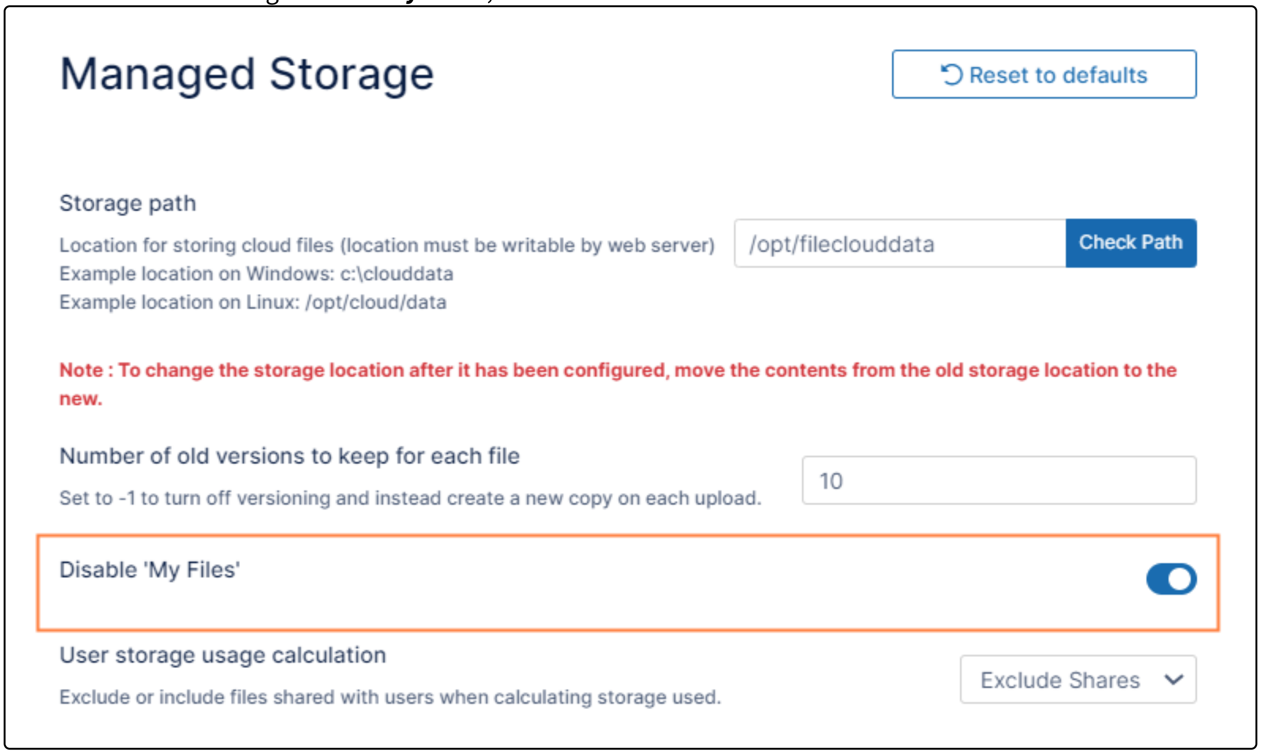
My Files can be disabled completely if users need to access only Network Folders, Team Folders or shared data.

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

To disable My Files:

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

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



3. Click **Save.**

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.

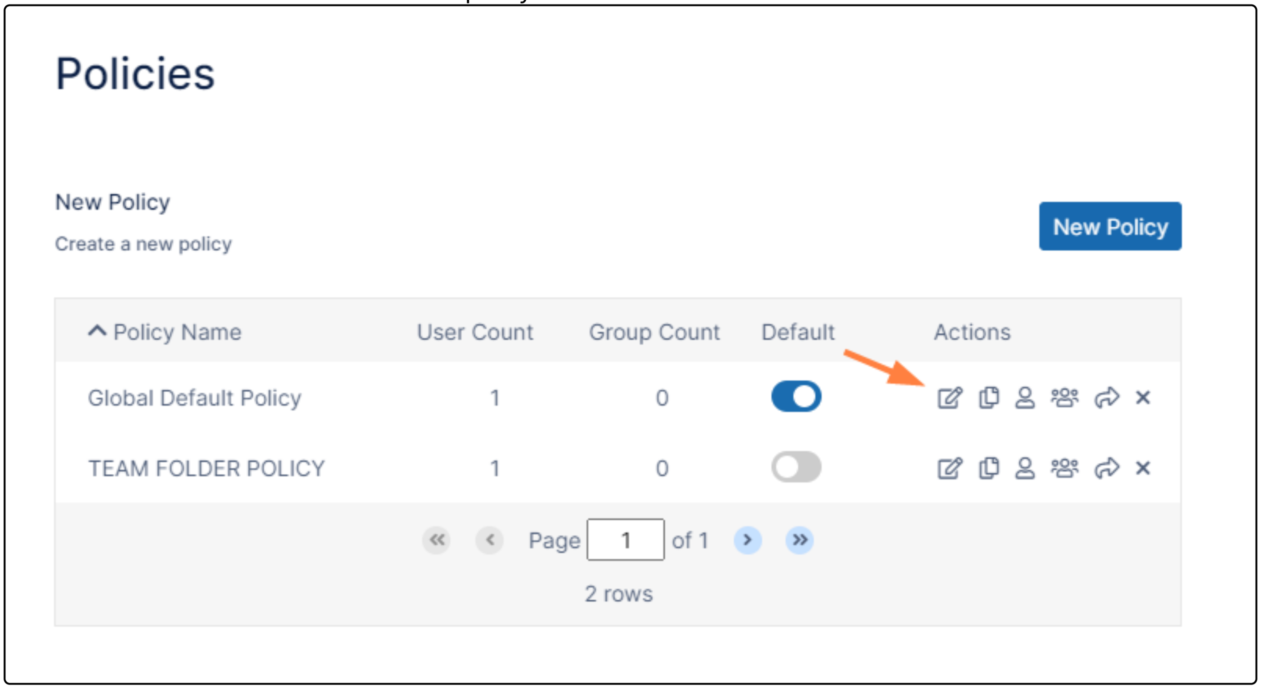
If **Enable recycle bin clearing** is disabled in a policy, users belonging to the policy do not see a **Clear Deleted Files** button in the recycle bin.

⚠ 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:

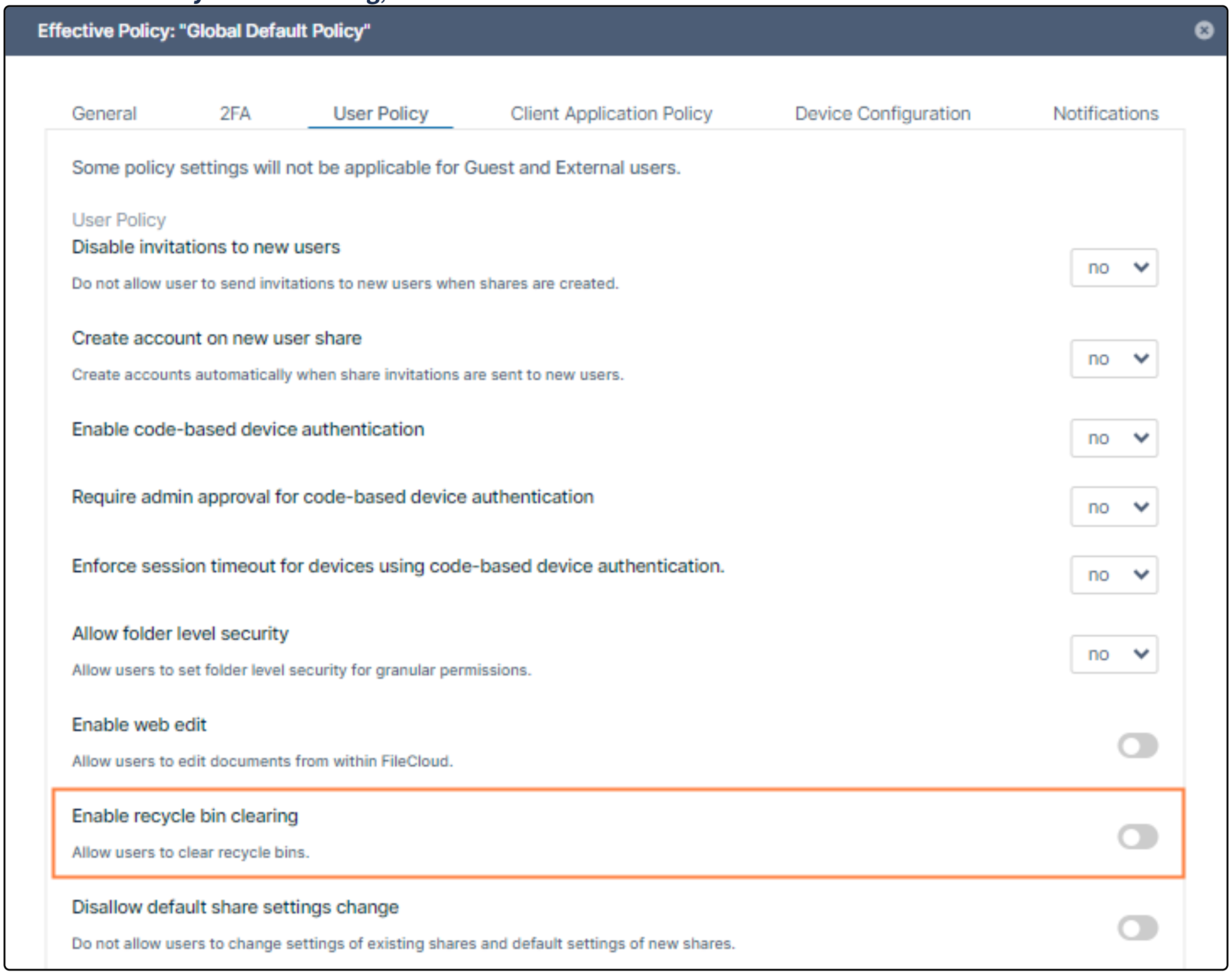
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.

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**.

Administrator Settings

This section describes how an administrator can access FileCloud management user interface.

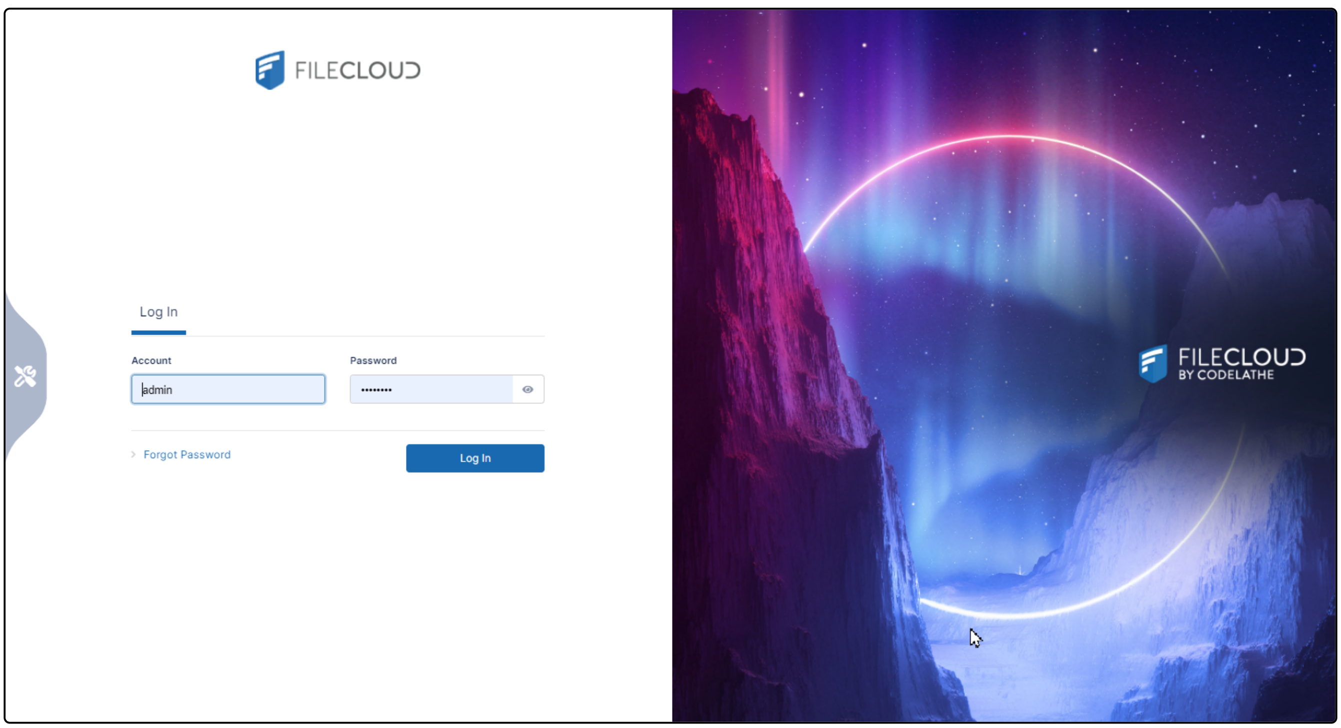
Logging In to the Admin Portal

Log in using your admin account to perform administrative tasks.

Accessing the Admin Portal

In a supported web browser, type in the URL to your Administrator dashboard. For example, ***https://<yourteamname>***.filecloudonline.com/admin

If you are an admin user (an end user with admin privileges), you may be required to accept terms of service the first time you log in to the admin portal. Once you accept the terms of service, the login screen opens.
If you are the main admin of the system (your username is Admin) you can log in directly the first time.



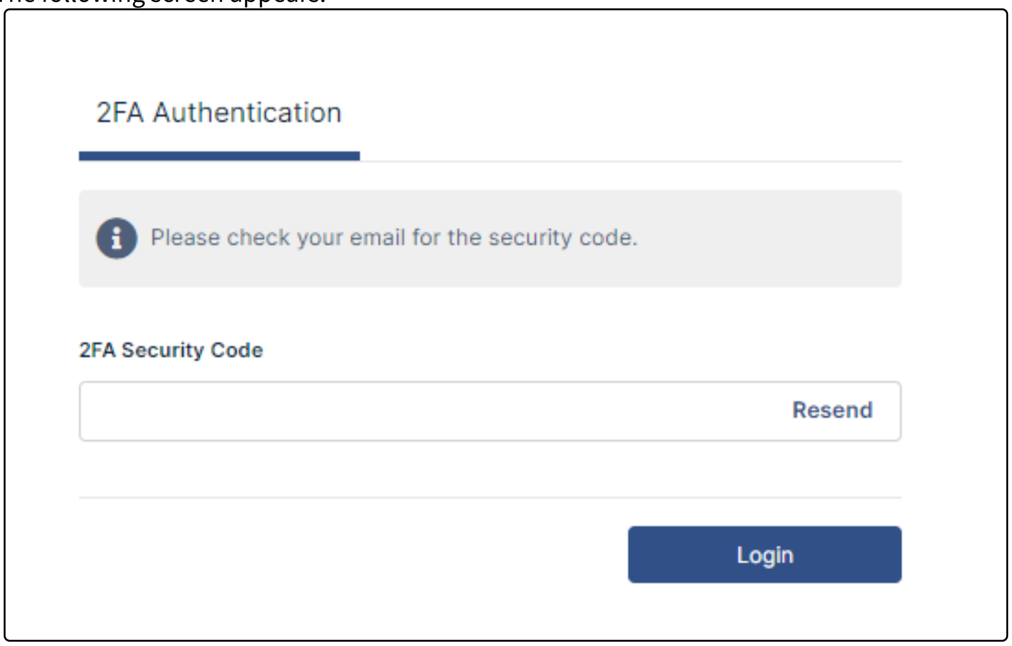
Logging in using 2FA

- 2FA validation codes remain valid for 5 minutes by default. After 5 minutes, you must click **Resend** to get a new code.

- If you are a promoted admin the login method set up for you user portal login is used for your admin portal login. However, if 2FA is set up for your admin portal login, your admin may require you to use that method for logging in to the admin portal.

Two-factor authentication via email code delivery

If two-factor authentication is set up to use your email id, then the 2FA security code is sent to the email address associated with your FileCloud account.

1. Log in to FileCloud using your username and password.
   The following screen appears:
   

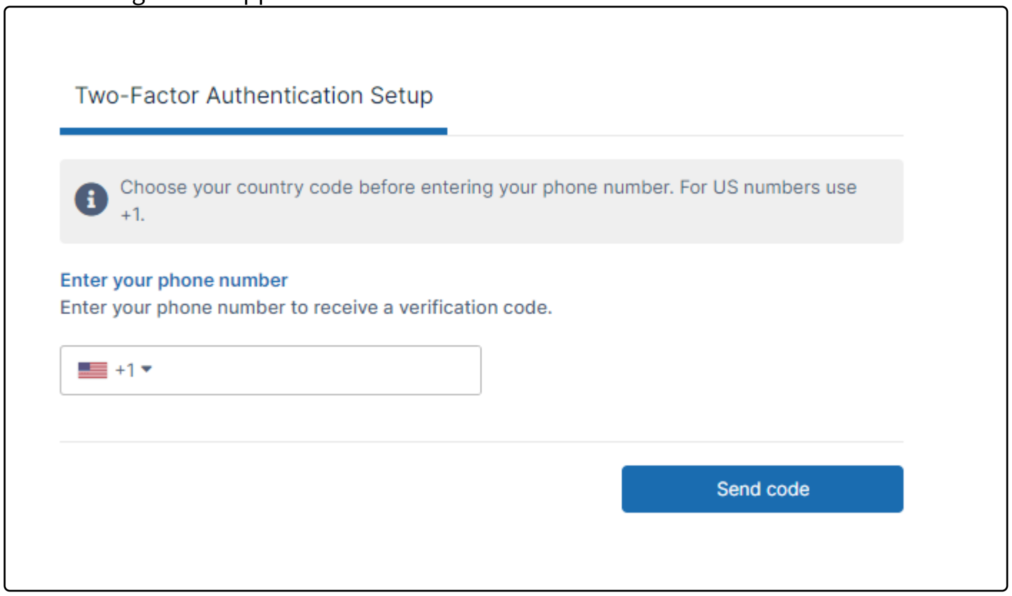
2. Check your email for the message with the code, and enter it into **2FA Security Code**.
3. Click **Login**.
   You are logged in to FileCloud.

Two-factor authentication via SMS code delivery

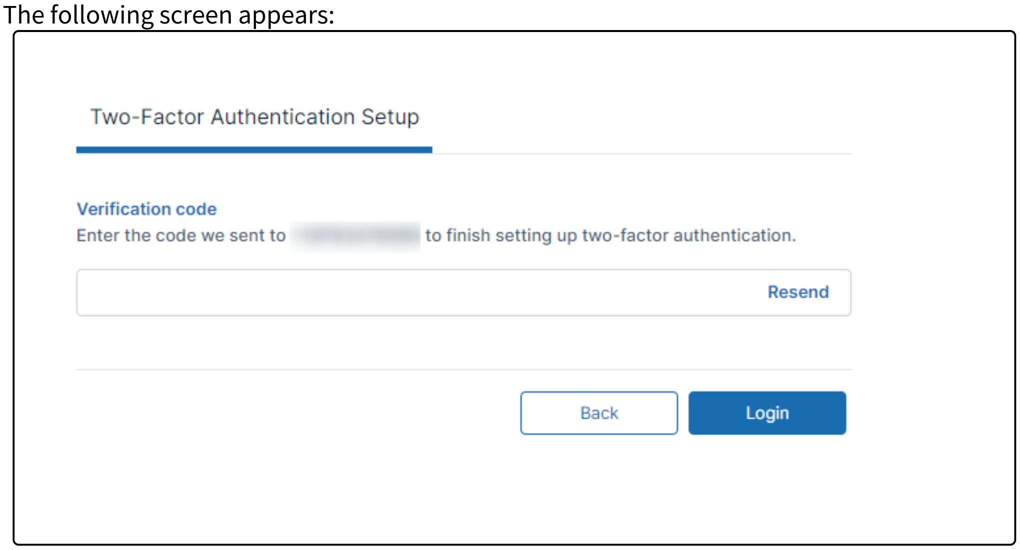
If two-factor authentication is set up to use SMS, then you will receive a code via the phone number associated with the account.

The initial time you log in using SMS

1. Log in to FileCloud using your username and password.
   The following screen appears:



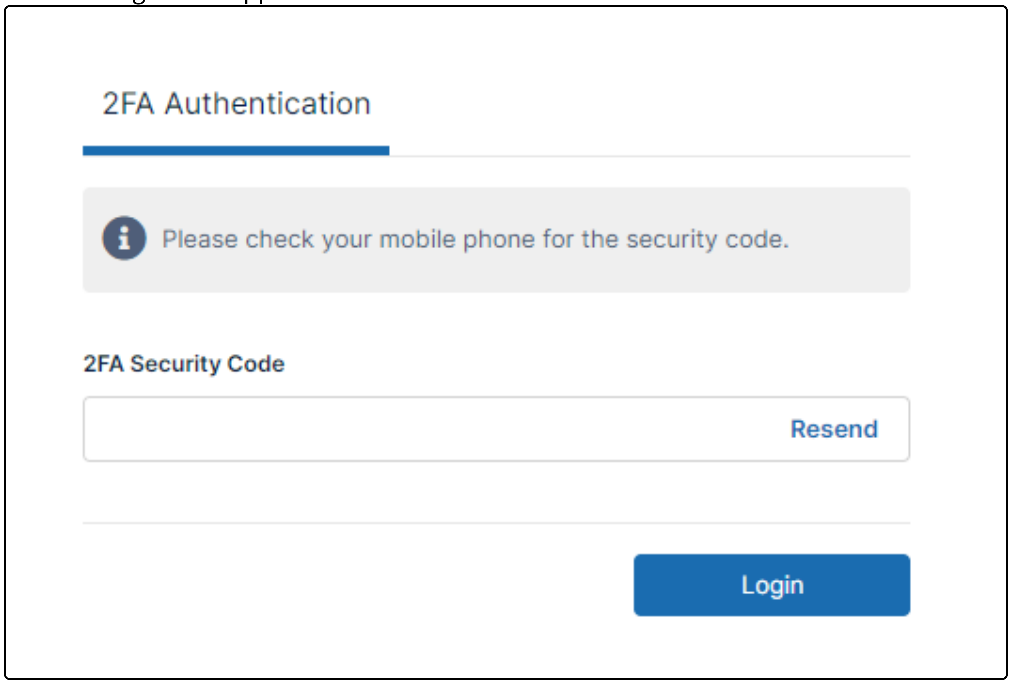
2. Enter your phone number and click **Send code**.
   The following screen appears:



3. Check your phone for the code, and enter it into **Verification code**.
4. Click **Login**.
   You are logged in to FileCloud.

After the initial time you log in using SMS

FileCloud has saved your phone number the first time you logged in using SMS, so you do not have to enter it again.

1. Log in to FileCloud using your username and password.
   The following screen appears:
   

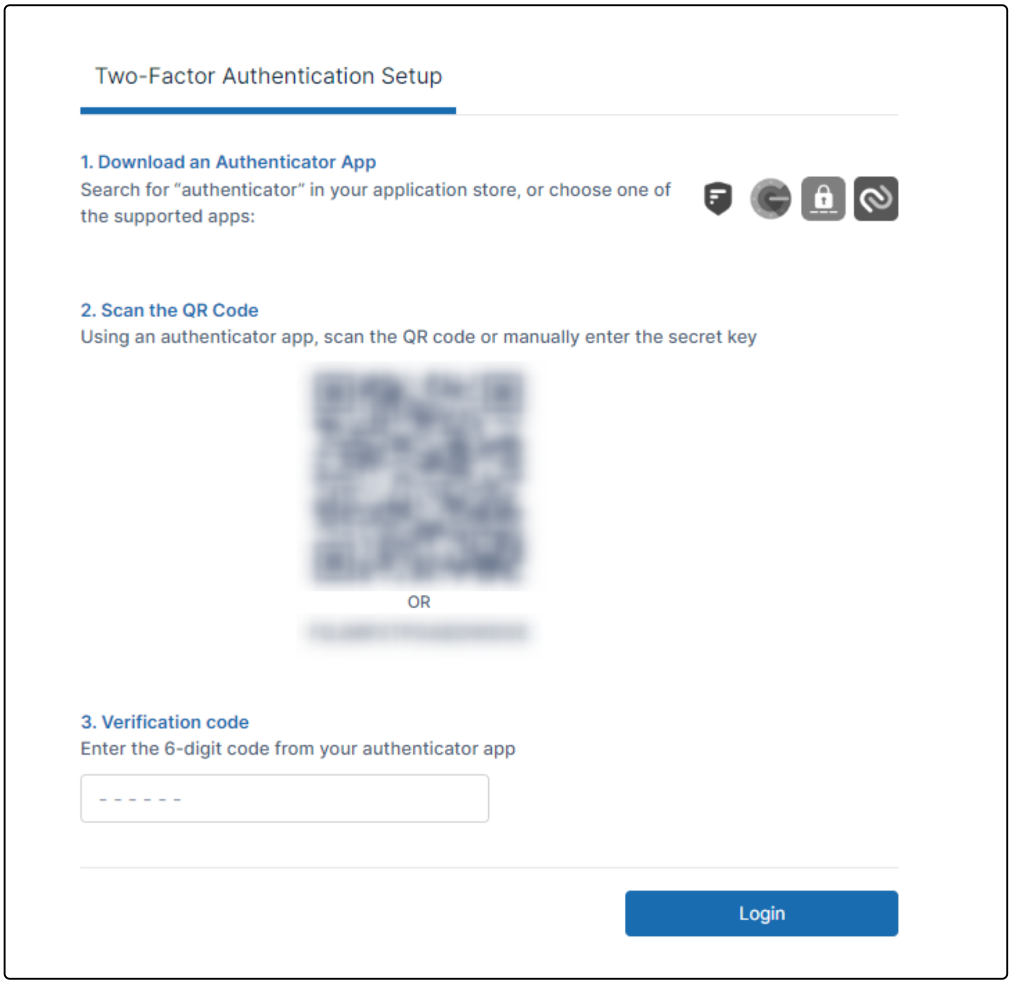
2. Check your phone for the code, and enter it into **2FA Security Code.**
3. Click **Login**.
   You are logged in to FileCloud.

Two Factor Authentication with TOTP

If your admin sets up 2FA with TOTP, the dialog box prompting you for your security code will direct you to check your authenticator app for the code.

The initial time you log in using TOTP

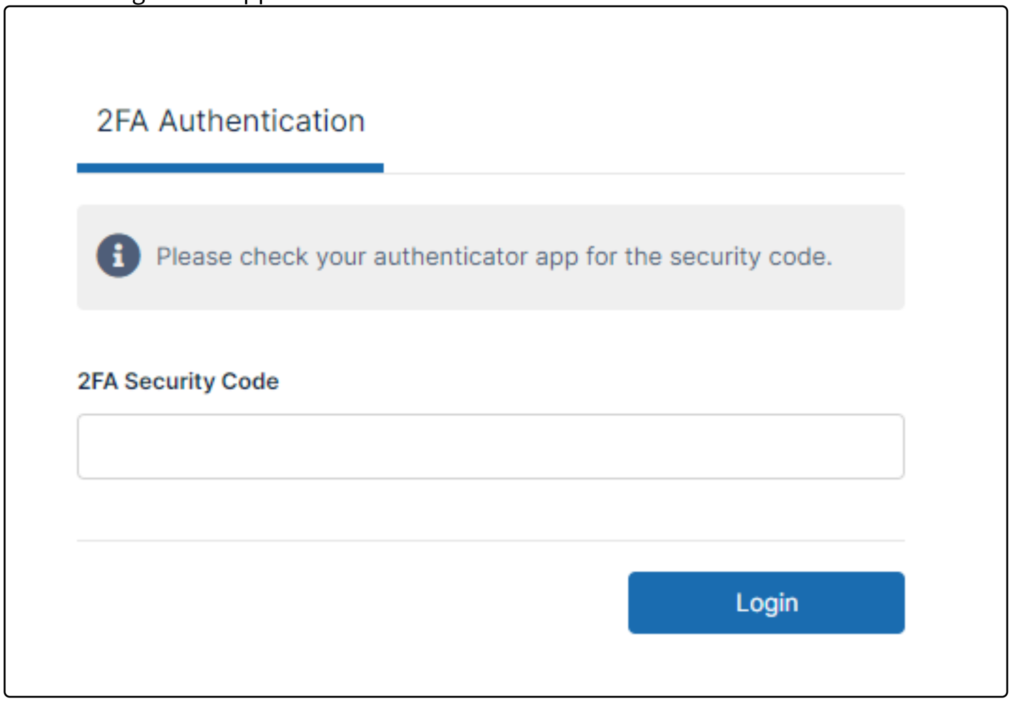
1. Log in to FileCloud using your FileCloud username and password.
   The following screen appears:



2. If an authenticator app is not yet set up, install it in your smart device; you may click one of the download icons to install it.
3. Either scan the QR code or type the text code into the authenticator app.
   The authenticator app creates the account and lists it with a code.
4. Enter the code listed on the authenticator app for your account into **Verification code**, and click **Login**.
   You are logged in to FileCloud.

After your initial login with TOTP

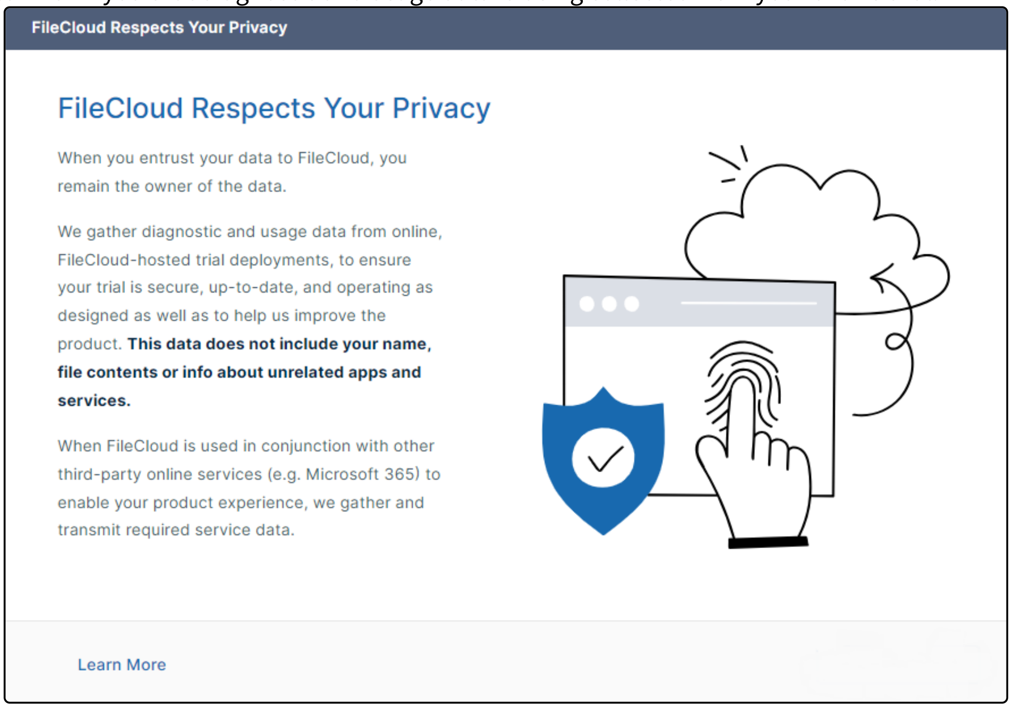
The authenticator app has saved your account the first time you logged in using TOTP, so you do not have to enter it again.

1. Log in to FileCloud using your FileCloud username and password.
   The following screen appears:
   

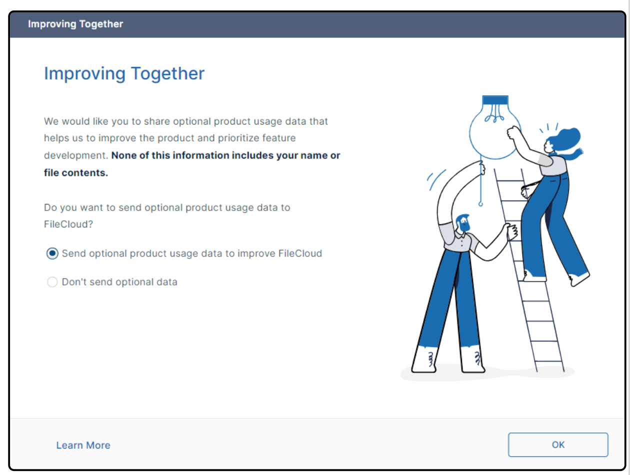
2. Enter the code listed on the authenticator app for your account into **2FA Security Code**, and click **Login**.
   You are logged in to FileCloud.

Collection of usage data

If you are logging in to a trial version of FileCloud Online for the first time, after you log in, the following screen appears to inform you that diagnostic and usage data is being collected from your online trial:

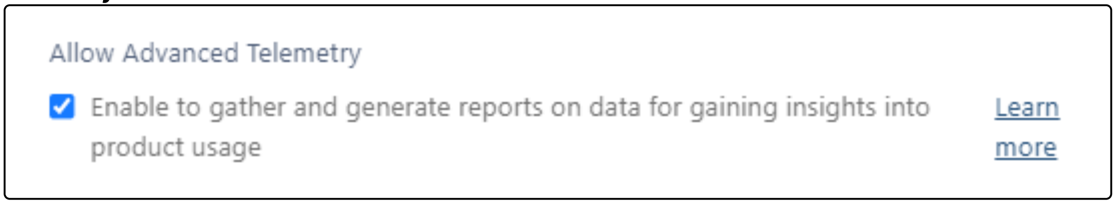


Once you convert from from an online trial license to an online product license, the first time you log in to the the admin portal a wizard opens with the following two screens:



To allow sending of optional product usage data to FileCloud, leave **Send optional product usage data to improve FileCloud** selected, and click **OK**.
To prevent sending of optional product usage data to FileCloud, select **Don't send optional data**, and click **OK**.

You can change the option at any time by going to **Settings > Server** and checking or unchecking **Allow Advanced Telemetry**.



Customizing the Login Page

To customize the image on the admin login screen, see Themes, Labels, and Logos.

Resetting Admin Password

When Auth Type is set to AD or LDAP, the admin password cannot be changed using the procedure on this page, but must be changed in the AD or LDAP server by the AD or LDAP admin. See User Authentication Settings.

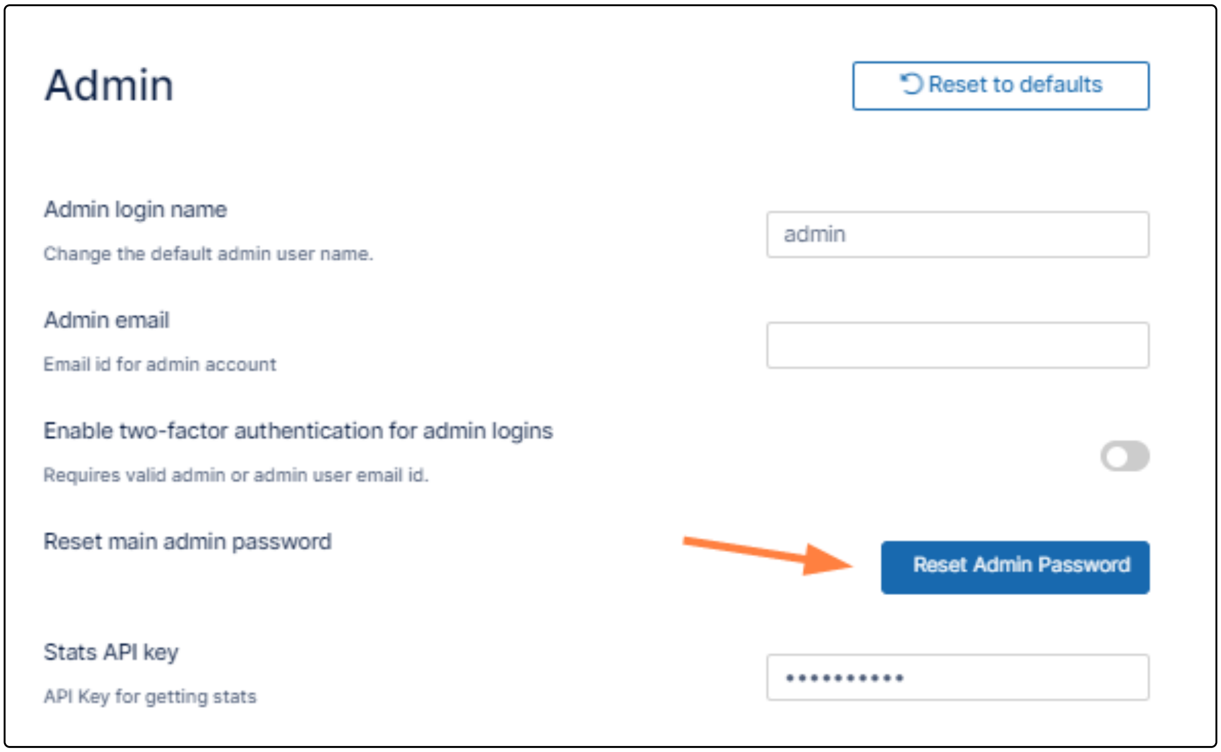
Reset the main admin's password in the Admin settings screen

Reset in admin settings...

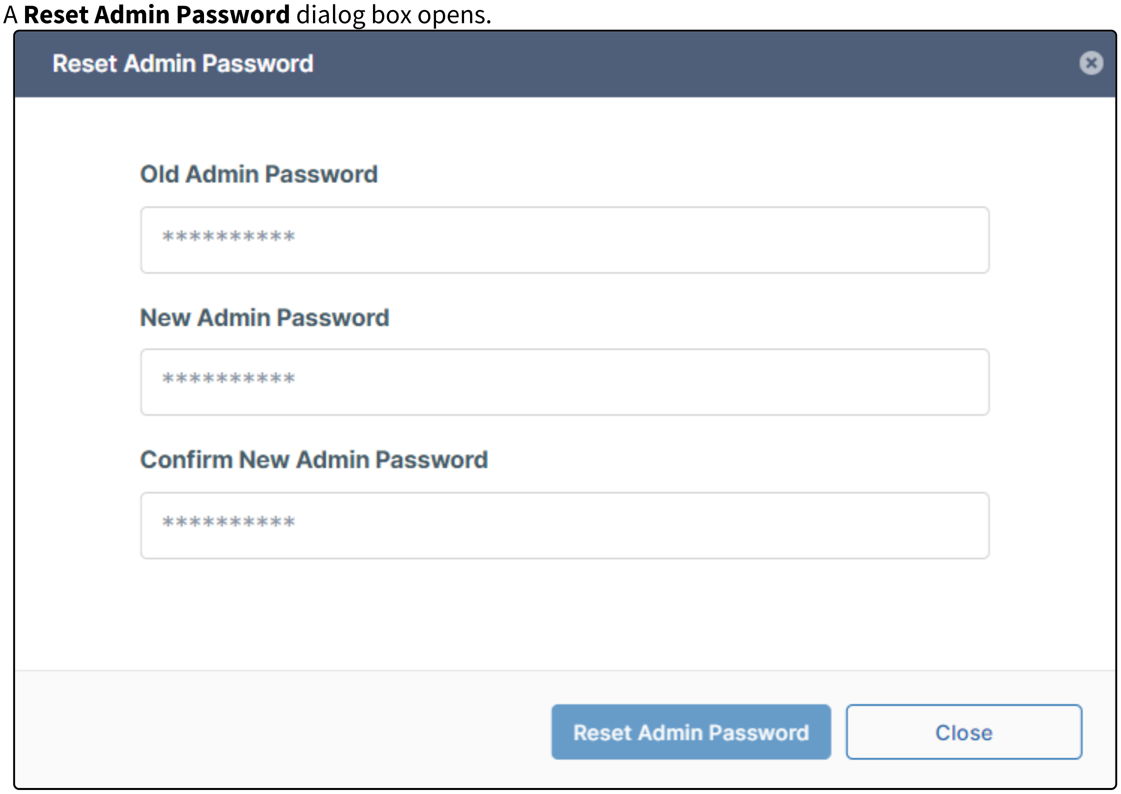
This setting can only be used to reset the main admin password. It cannot be used to change user admin (promoted admin) passwords.

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

2. Click **Reset Admin Password**.



A **Reset Admin Password** dialog box opens.



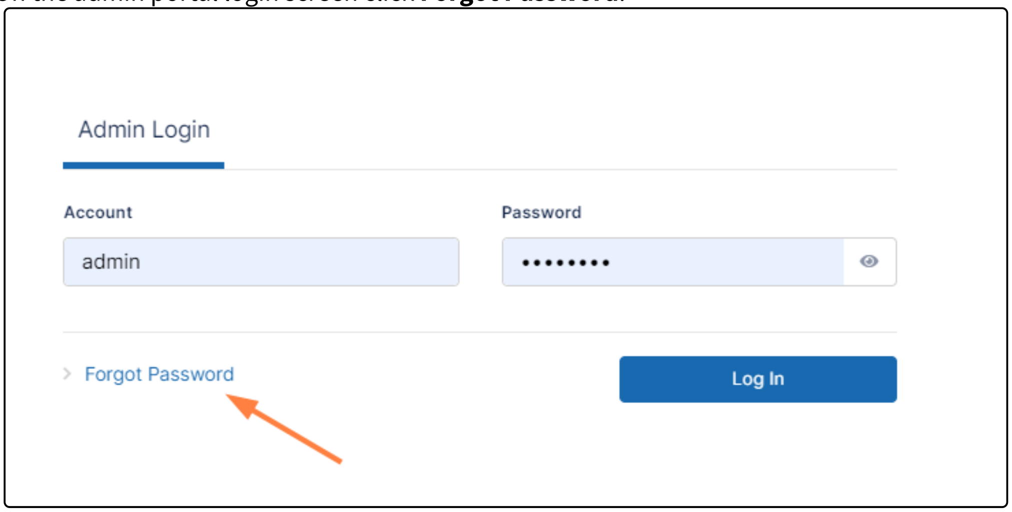
3. Enter the old and new password values, and click **Reset Admin Password**.

Reset a forgotten admin password from the login screen

Reset from login screen...

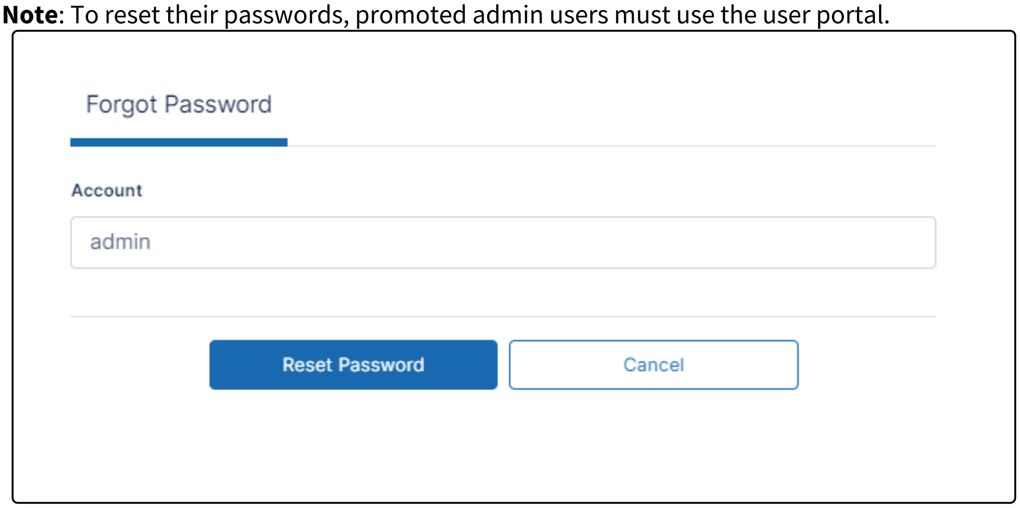
This method can be used to reset the main admin password as well as user admin passwords.

1. On the admin portal login screen click **Forgot Password**.

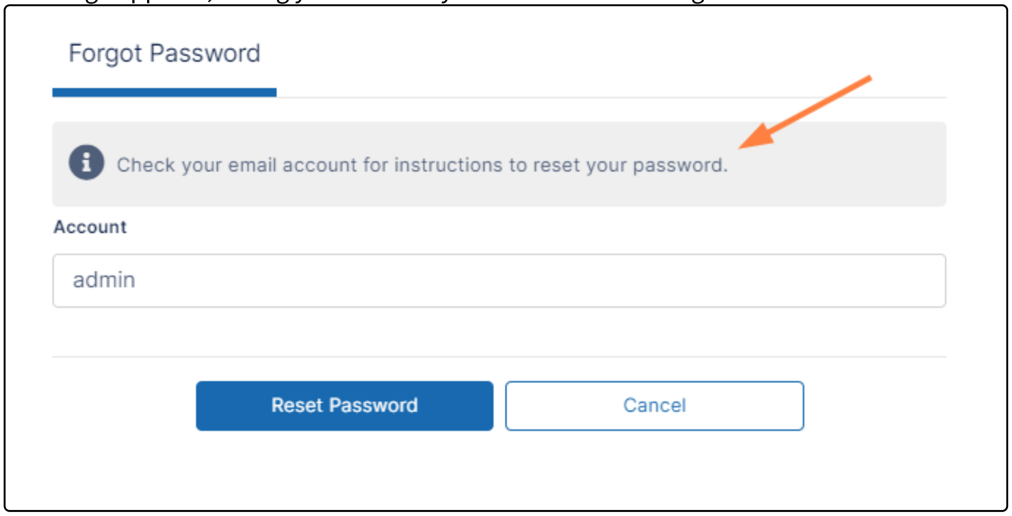


A dialog box prompts you to enter your user account.

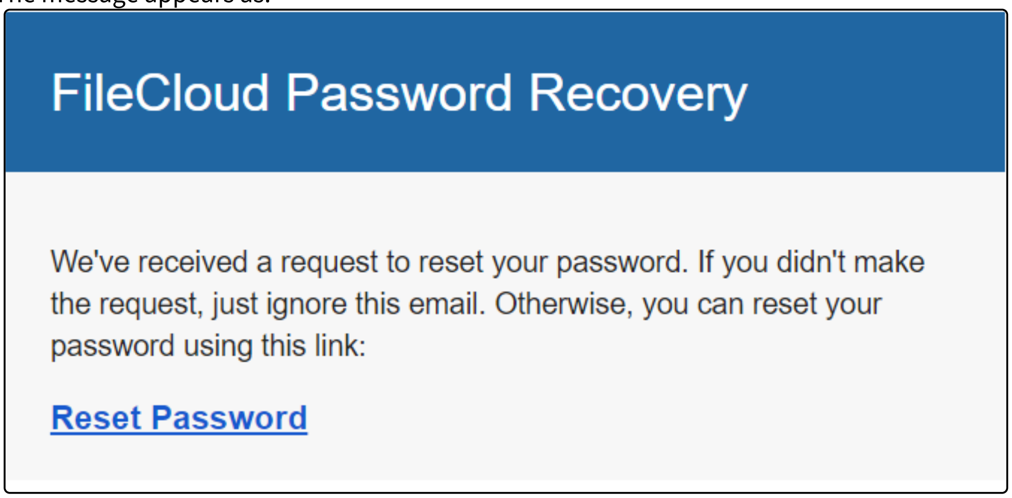
2. Enter your admin account name, and click **Reset Password**.
Note: To reset their passwords, promoted admin users must use the user portal.



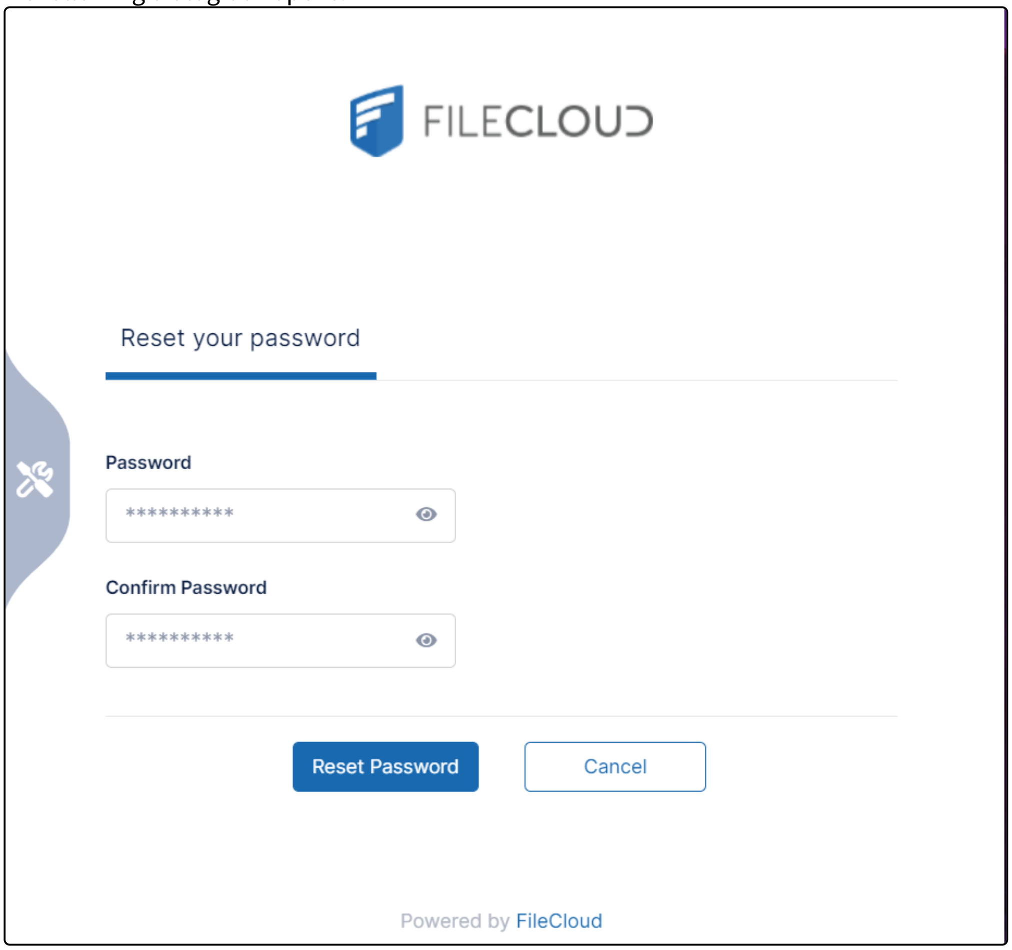
A message appears, telling you to check your email for a message.



3. Find and open the message in your email.
   The message appears as:



4. Click **Reset Password**.
   The following dialog box opens:



5. In **Password**, enter your new password. In **Confirm Password** enter it again.
6. Click **Reset Password**.
   Your password is reset.

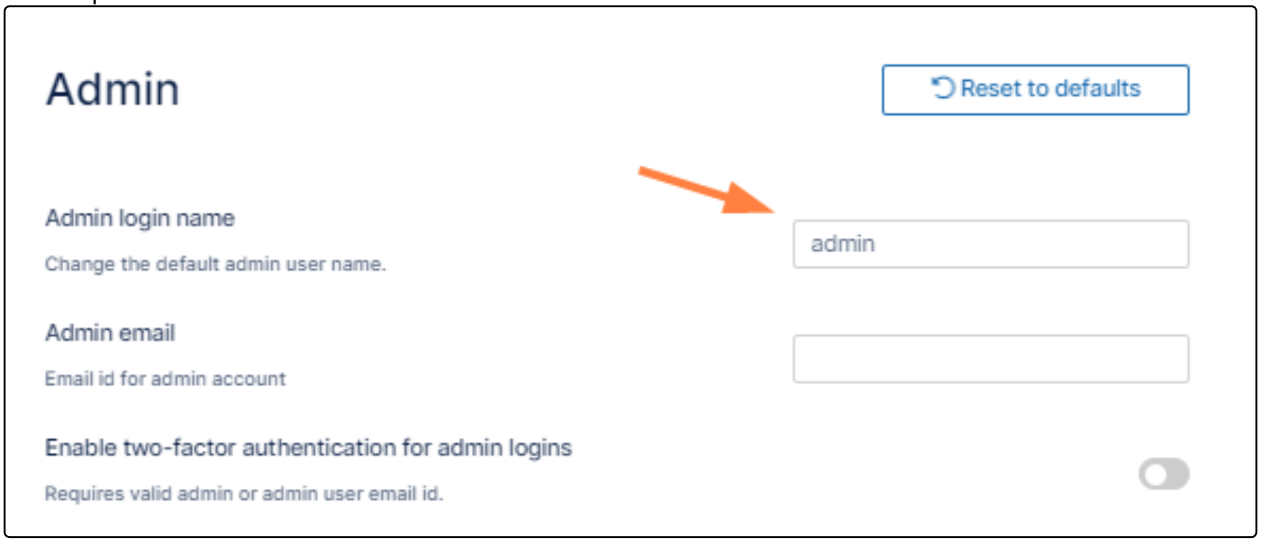
Changing the Default Login Name

FileCloud has a built-in admin account to log in to the admin portal and manage the site.

The name of the account is **admin**. This name can be changed in the **Admin login name** setting.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin**  .
   The **Admin** settings page opens.
2. Enter the new name in **Admin login name**.
   The name can only contain letters, numbers, spaces, hyphens, underscores and periods. It cannot be the same

as the superadmin name.

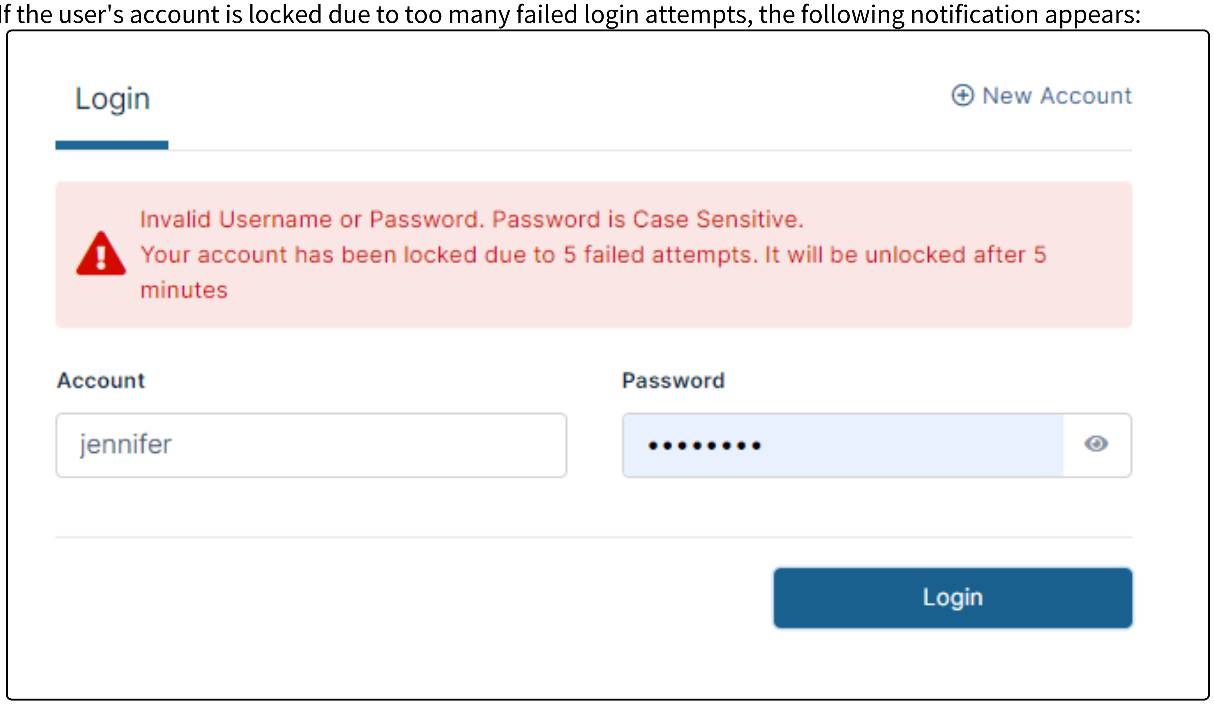


3. Click **Save.**

Account Locked Alerts

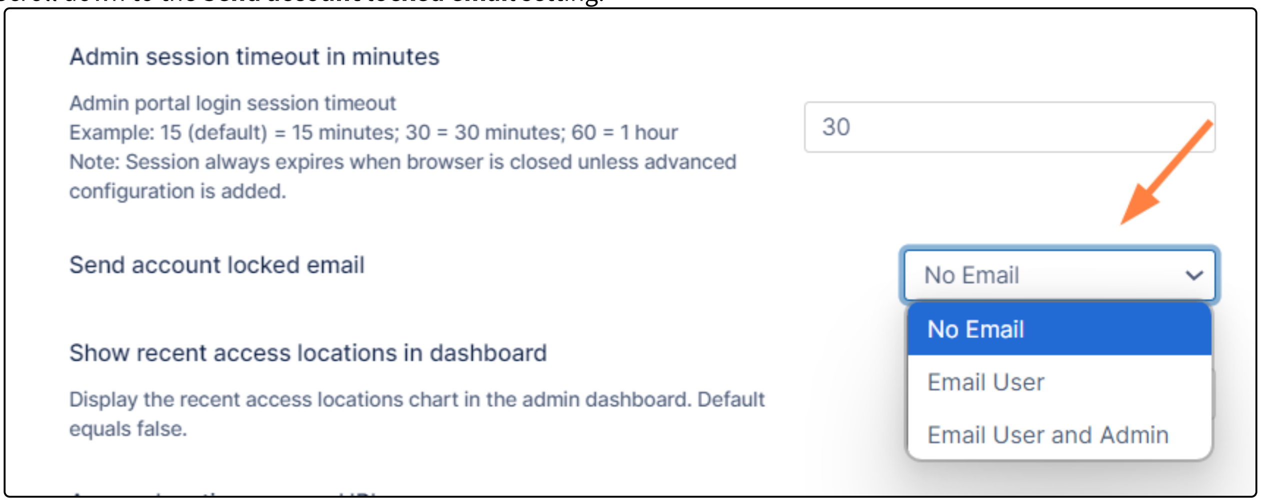
By default, FileCloud locks a FileCloud user's account for 5 minutes after 5 incorrect log in attempts. (You may change the default values in Password settings.)

Each time the user makes a failed login attempt, a warning notification appears on the login screen telling the user how many attempts are remaining.
If the user's account is locked due to too many failed login attempts, the following notification appears:



By default, FileCloud is set to not send an email message to the user or admin to notify them that the account has been locked due to incorrect login attempts. However, you may change this setting.

To change the **Account Locked Alert** setting:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin**  .
   The **Admin** settings page opens.
2. Scroll down to the **Send account locked email** setting.
   

3. In the drop-down list, choose one of the following settings:
   No Email - Neither the user nor the admin receives an email notification about the user account lockout.
   Email User - The user receives an email notification about their account lockout but the admin does not.
   Email User and Admin - Both the user and the admin receive an email about the user account lockout.

Folder-Level Permissions

Folder-level permissions are permissions that are applied directly to a folder. They add additional restrictions to the share permissions when the folder is shared. Note that whichever is more restrictive, folder-level or share permissions, apply.

Folder-Level Permissions Support	Folder-Level Permissions Do Not Support
Interaction with share permissions. Allowing or restricting access by specifying a user's email account Folders in Managed Storage Configuration by admins, and configuration by the owner of the folder, if permitted.	Folders in Network Storage Permissions set by a user other than the owner

You can apply folder-level permissions to:

- a user's folders
- Team folders

You can also enable users to apply folder-level permissions to their folders.

It's important to understand what takes precedence when there are folder-level and share permissions on the same folder, and when sub-folders inherit the permissions of their parent folders. It's also necessary to know which permissions apply when a user and the user's group(s) have different permissions for the same folder.

It would be very difficult to work out how the different permissions interact each time there is an overlap, so FileCloud provides effective permissions calculators that show you which permissions apply in these situations. The different effective permissions calculators are explained in the topics in this section.

The topics in this section show you how to enable and apply folder-level permissions and explain which permissions take precedence when multiple permissions are applied.

- Setting Folder-Level Permissions from the Admin Portal
- Enabling Users to Set Folder-Level Permissions
- Setting Folder-Level Permissions on Team Folders
- How Folder-Level Permissions and Share Permissions Work Together
- More Examples

Setting Folder-Level Permissions from the Admin Portal

Apply folder-level permissions for users or groups to certain folders if you want to limit their access to the folders when they are shared.

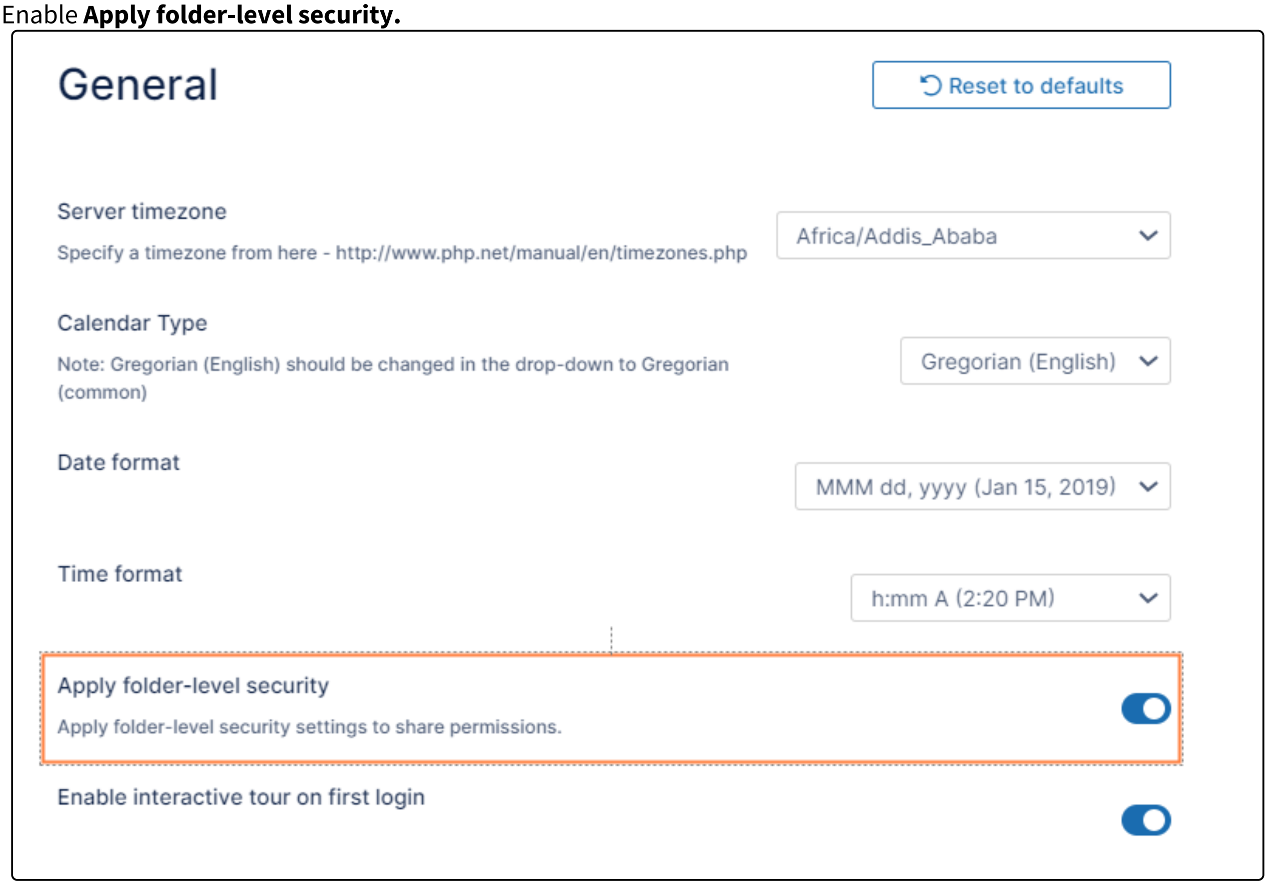
- You can apply folder-level permissions directly to user folders from the **Manage Users** page.
- You can apply folder-level permissions to Team Folders from the Manage Team Folders page. See instructions at Setting Folder-Level Permissions on Team Folders.
- You can edit folder-level permissions set by users and folder-permissions set on Team Folders from the **Folder Permissions** link in the navigation panel.

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
    - Subfolders inherit the folder-level permissions of their immediate parent folders.
    - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.
- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

To configure FileCloud to allow setting folder-level permissions

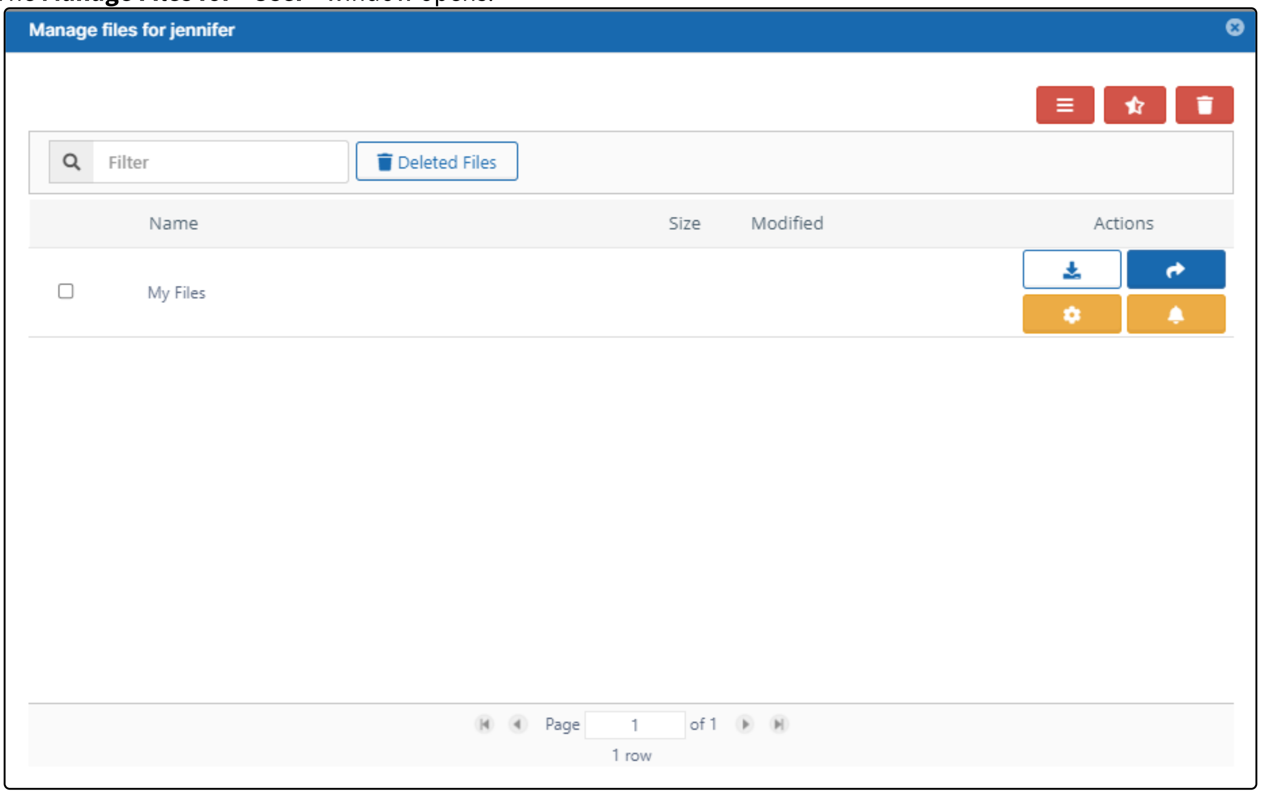
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Enable **Apply folder-level security.**



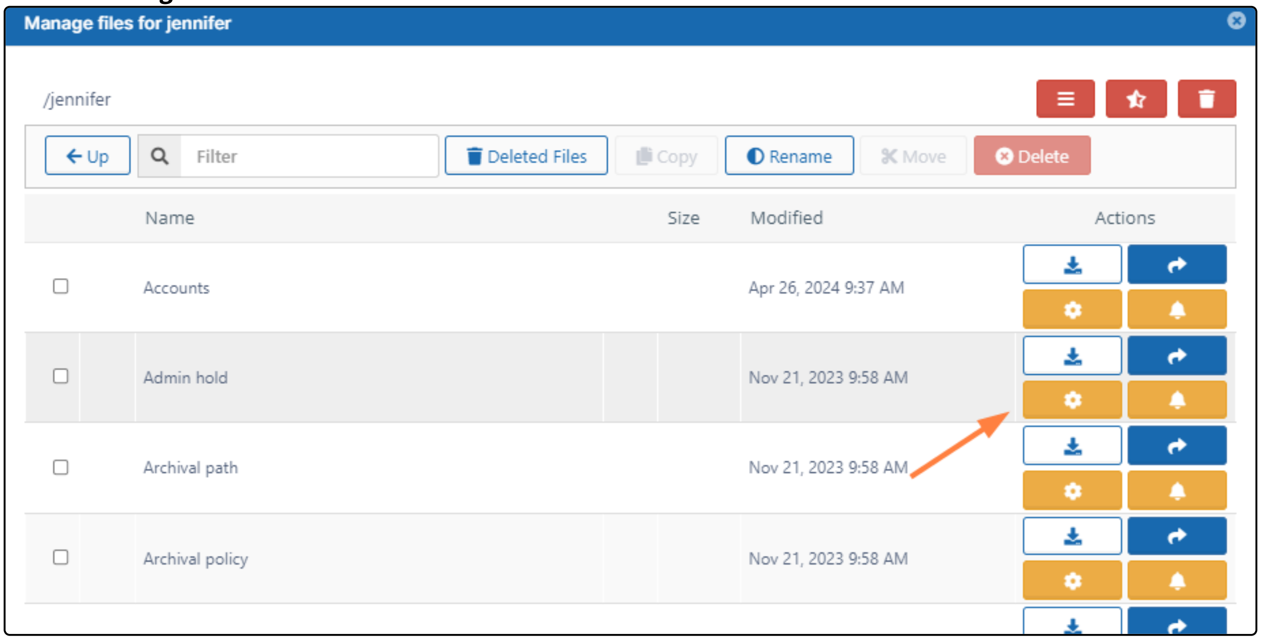
Now, folder-level permissions can be set.

To apply folder-level permissions to user folders:

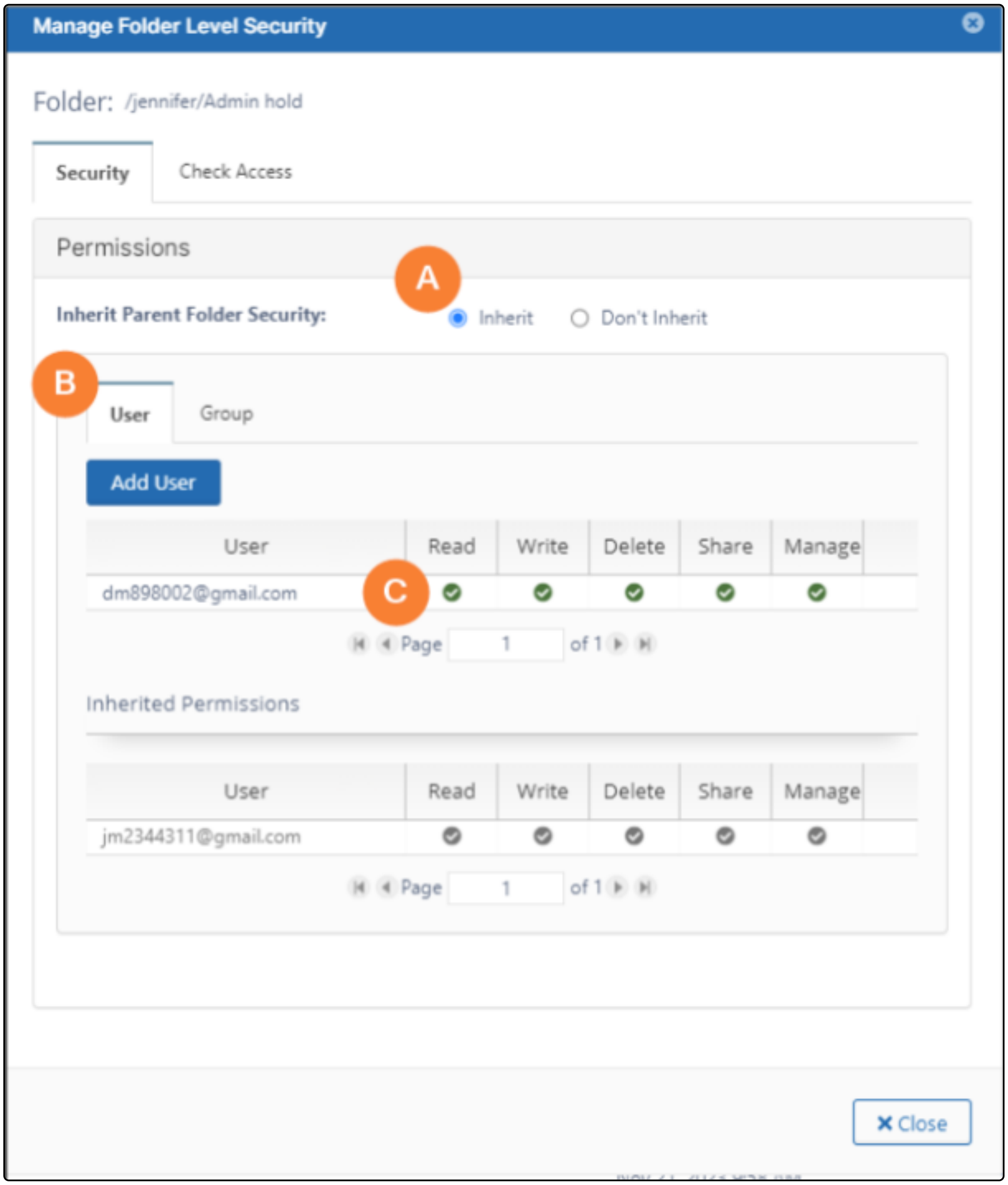
1. In the admin portal's left navigation panel, click **Users**.
2. On the **Manage Users** page, select a user, and then click the Edit icon.
3. On the **User Details** dialog box, click **Manage Files.**
   The **Manage Files for <User>** window opens.



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

5. Click the **Manage Access**  button in the folder's row.


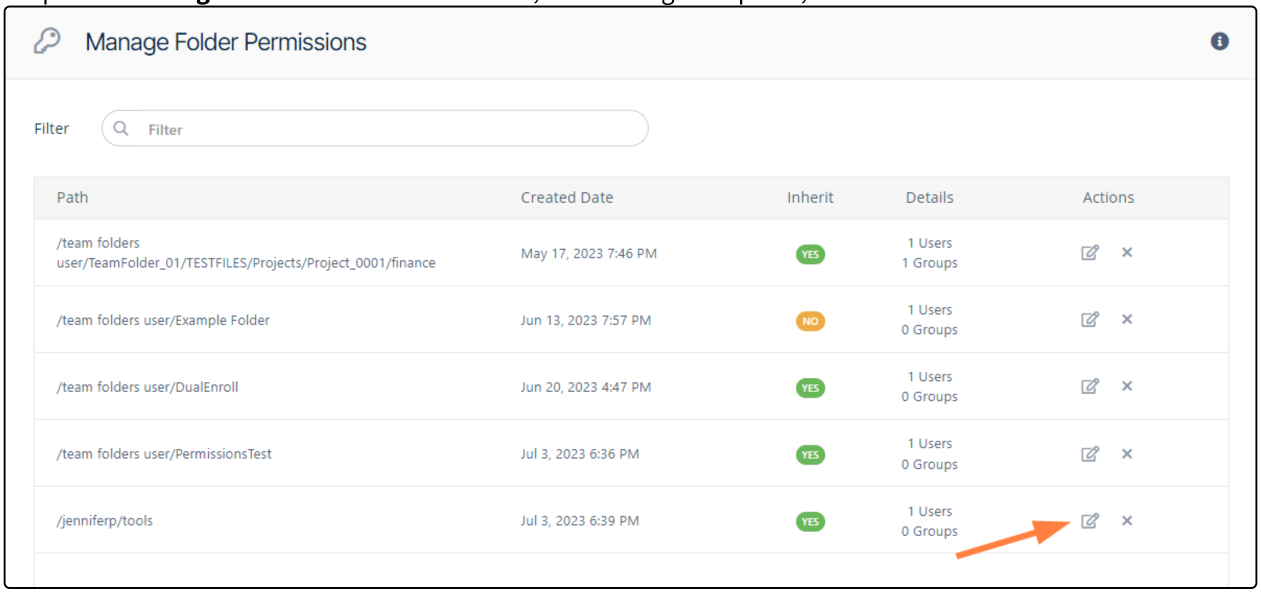
The **Manage Folder Level Security** dialog box opens. Any folder-level permissions that are already effective appear.
6. Follow the steps below to assign and change user and group folder-level permissions. Users who do not appear on the list have all folder-level permissions to the folder (unless their group permissions are limited)



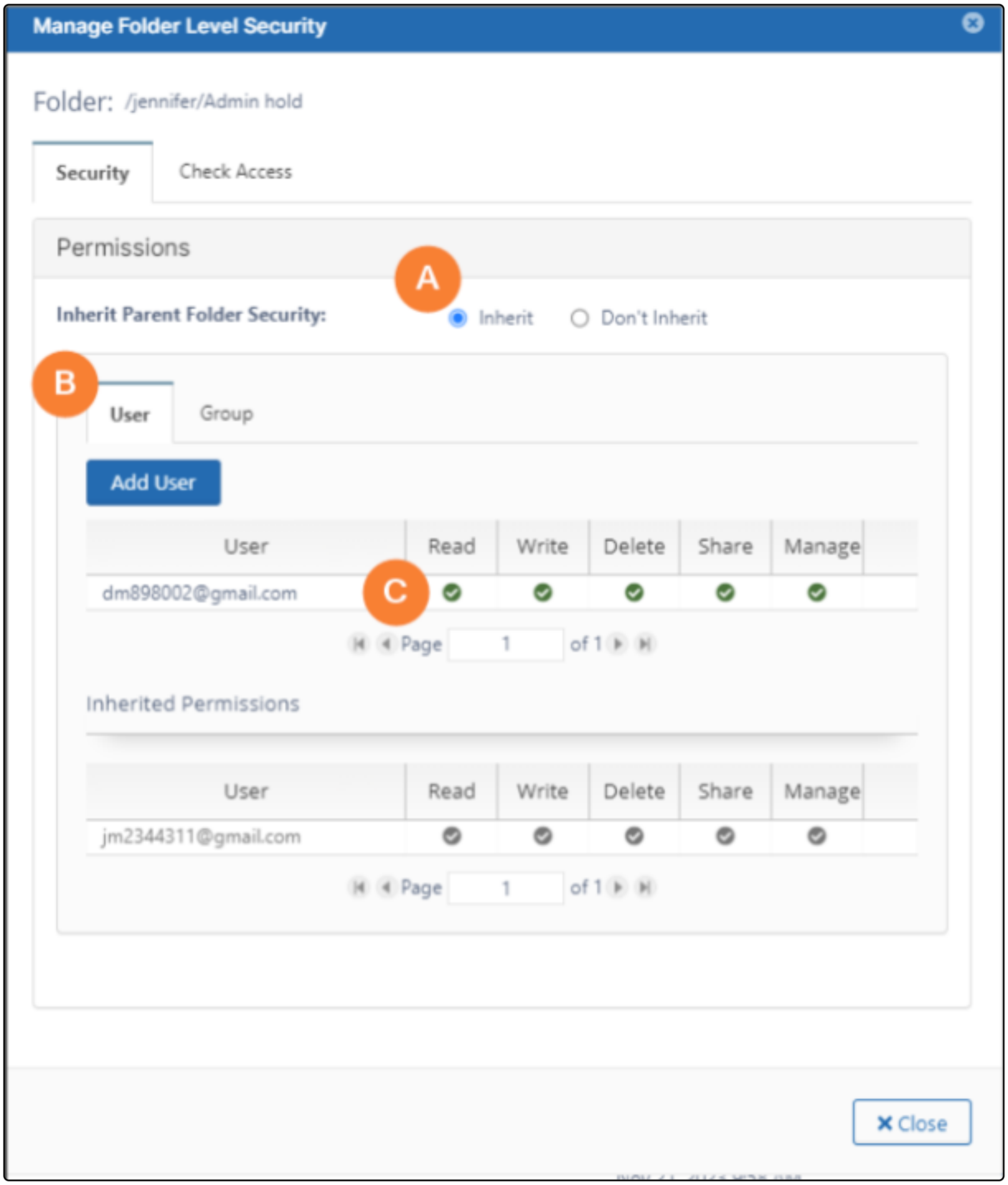
A By default, **Inherit** is selected. If you select **Don't Inherit**, users do not inherit permissions from this folder's parent folder, and the lower **Inherited Permissions** section no longer appears.
B Click **Add User** to add a user and limit their access to the folder, or click the Group tab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

To edit folder-level permissions set by admins on Team Folders and set by users on user folders:

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



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



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

Checking Effective Permissions

Check Effective Permissions

Administrators can check to see which effective folder permissions a user has to a folder. Effective permissions are the actual permissions when various permissions assigned to a user for the same folder are combined (for example, effective permissions show which permissions apply when a user has both individual and group permissions).

However, when you are using the methods shown on this page, this does not take into account which share permissions may have been given to the user for the folder. So, when the folder is shared, the share permissions may change the actual access the user has to the folder.

> When a user checks effective permissions for Team Folders in the user portal, share permissions and folder-level permissions are taken into account.

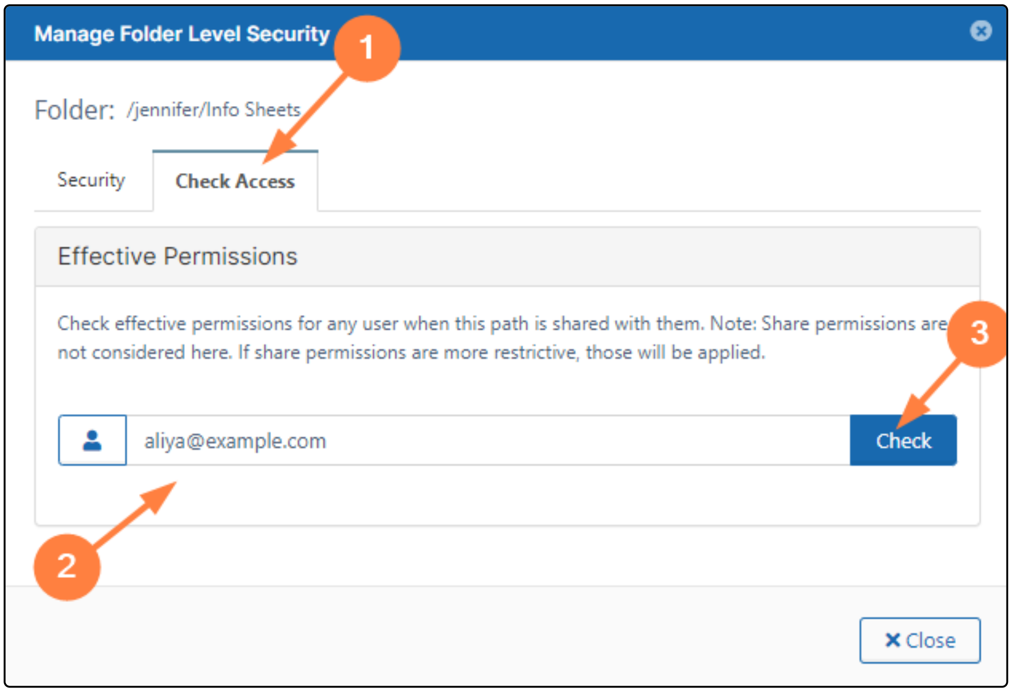
The possible folder-level permissions are:

Permission	Description
Read	• Allows Downloading Files • Allows Previewing Files
Write	• Allows uploading and modifying existing files • Allows creating files and folders • Allows renaming files and folders
Delete	• Allows deleting files and folders
Share	• Allows sharing files and folders
Manage	• Allow managing folder-level permissions for this folder

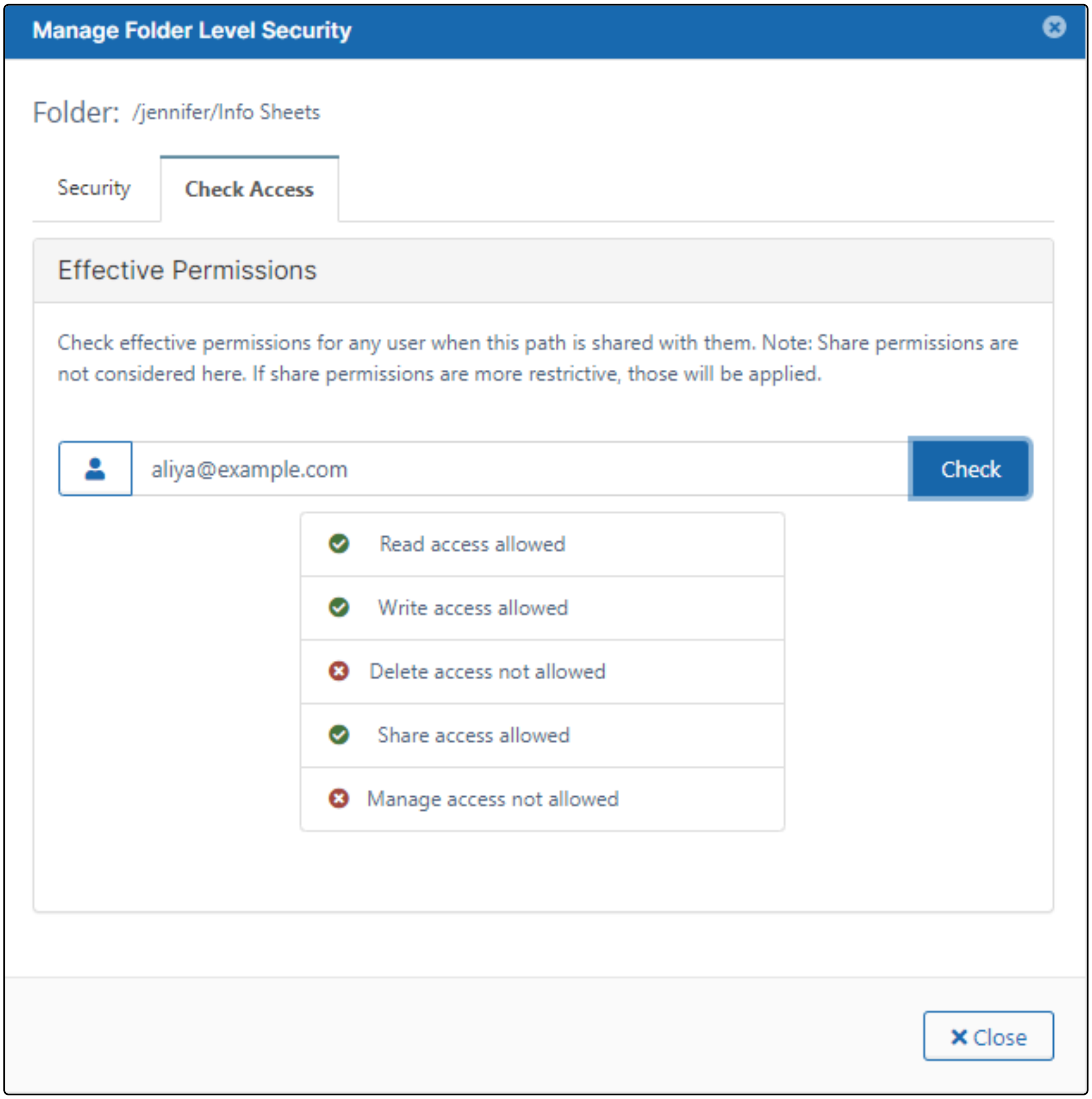
To check a user's effective permissions on a folder from the Manage Folder Permissions or Manage Users screen:

1. Access the **Manage Folder Level Security** dialog box in one of the ways shown on this page.
2. Select the **Check Access** tab.
3. In the box next to the user icon, enter the user's email id for their FileCloud account.

4. Click **Check**.



The user's permissions to the folder are listed:



Permission inheritance

How Do Inherited Permissions Work?

In general, a **folder** can be in one of the following states:

- The sub-folder has all of the same permissions as its parent folder
- The sub-folder has all of the same permissions as its parent folder, plus additional permissions
- The sub-folder has all of the same permissions as its parent, minus additional permissions
- The sub-folder's permissions are not connected in any way to the parent folder and the sub-folder retains a separate set of permissions

When setting folder-level permissions in FileCloud, you have the following options:

Option	Description
Inherit Permissions	Permissions set by default in this folder are exactly the same as its parent folder's permissions.
Don't Inherit Permissions	Permissions set in this folder don't inherit from its parent folder's permissions and are specific to only this folder.

Enabling Users to Set Folder-Level Permissions

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
  - Subfolders inherit the folder-level permissions of their immediate parent folders.
  - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.
- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

To enable users to set folder-level permissions:

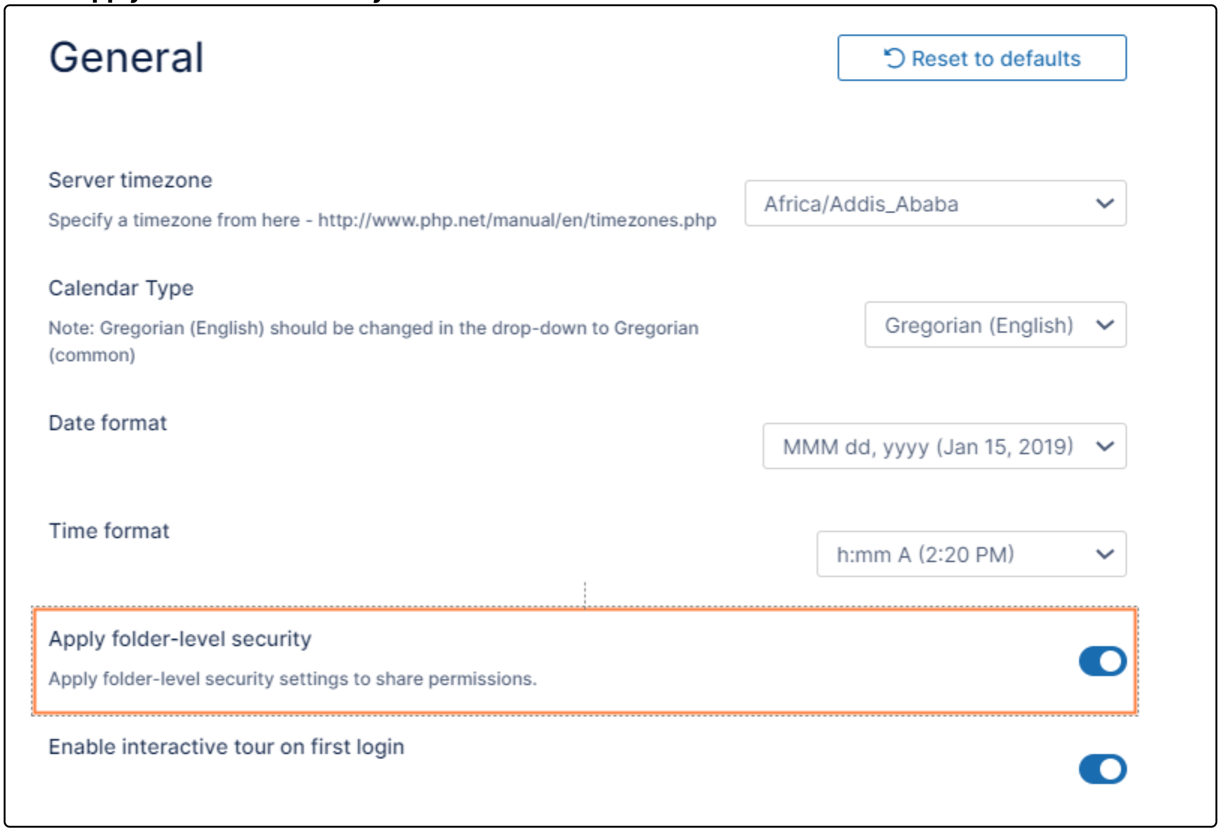
First enable folder-level security settings, then enable setting folder-level permissions in the user policy.

1. Enable folder-level permissions in Misc > General settings

To enable folder-level permissions in your system:

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

2. Enable **Apply folder-level security.**

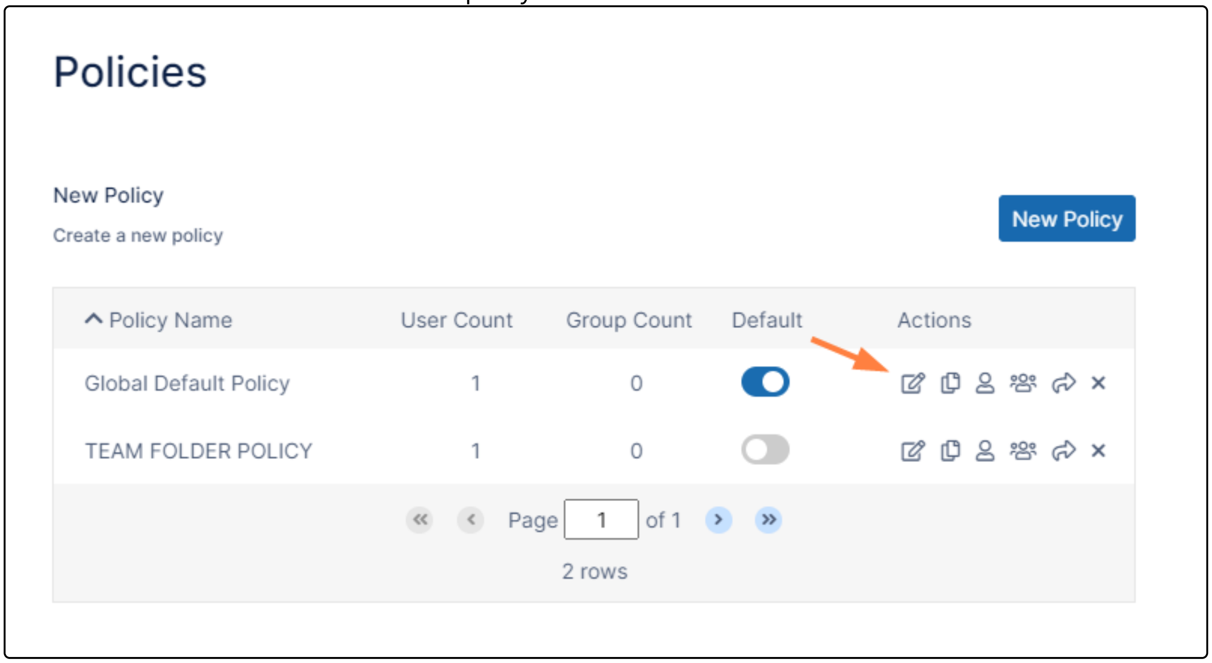


Now, folder-level permissions can be set.

2. Enable users to set folder permissions in their user policies

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

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



The **Policy Settings** dialog box opens.

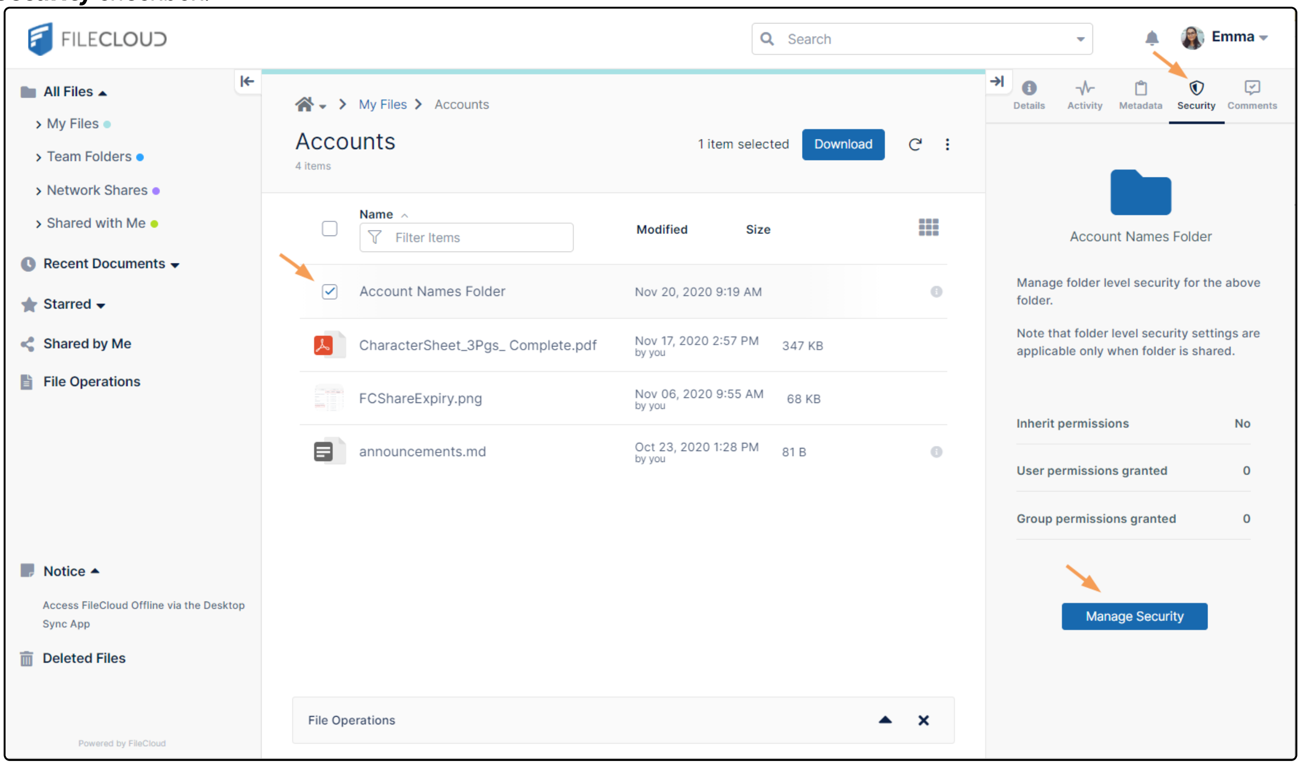
3. Click the **User Policy** tab.
4. Scroll down to the setting **Allow Folder Level Security** and set it to **yes**.

5. Click **Save**.

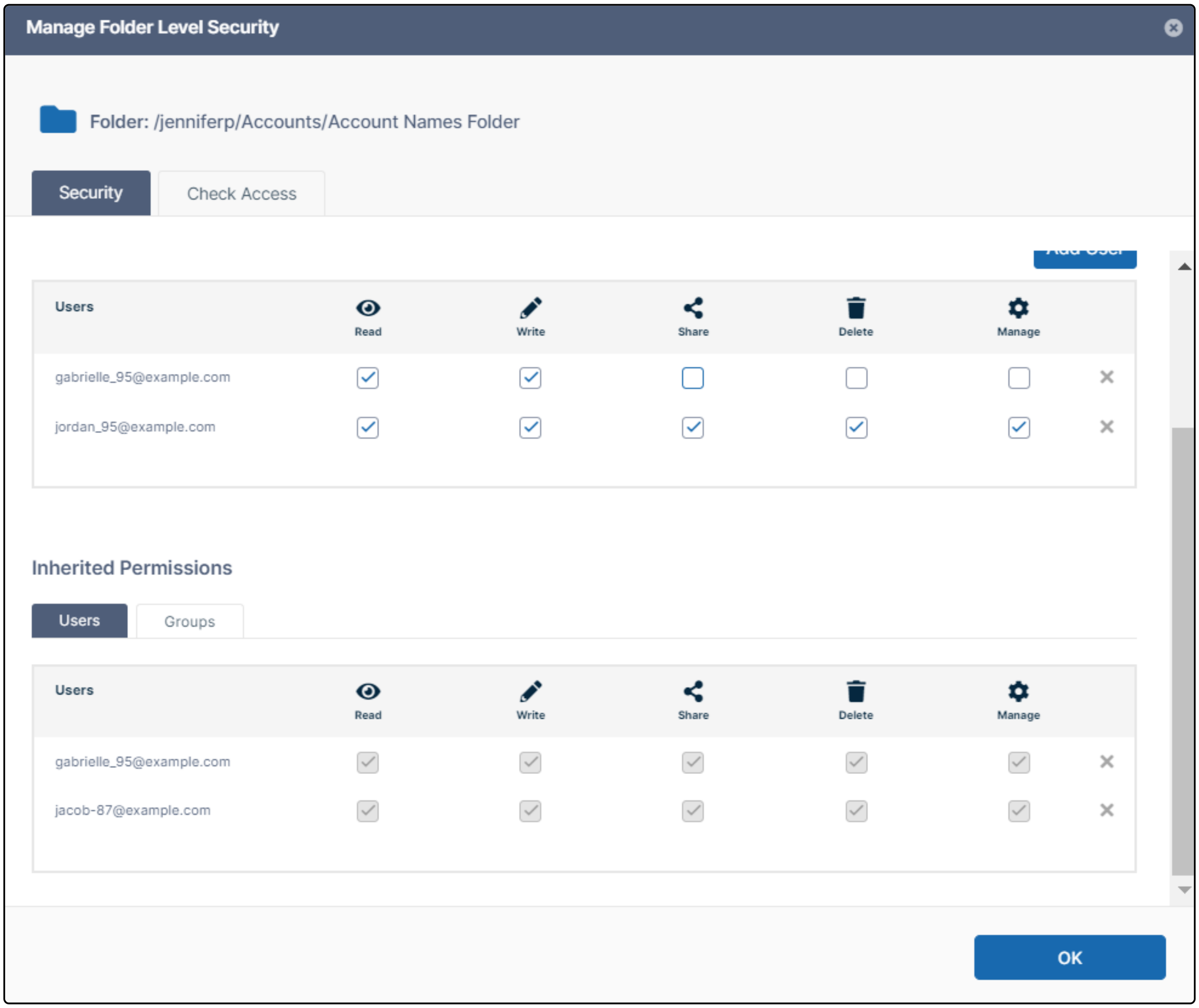
How a user sets folder permissions

How a user sets folder permissions

Once a user is permitted to set folder-level permissions, they can select a folder's checkbox and click the **Security** tab in the right panel. In the **Security** tab, the user clicks **Manage Security** to open the **Manage Folder Level Security** checkbox.



They can then add users and select one or more of the following folder-level permissions:



Permission	Description
Read	• Allows Downloading Files • Allows Previewing Files
Write	• Allows uploading and modifying existing files • Allows creating files and folders • Allows renaming files and folders
Delete	• Allows deleting files and folders

Permission	Description
Share	• Allows sharing files and folders
Manage	• Allow managing folder-level permissions for this folder

See Set Permissions on Folders in the User Dashboard for more information.

Setting Folder-Level Permissions on Team Folders

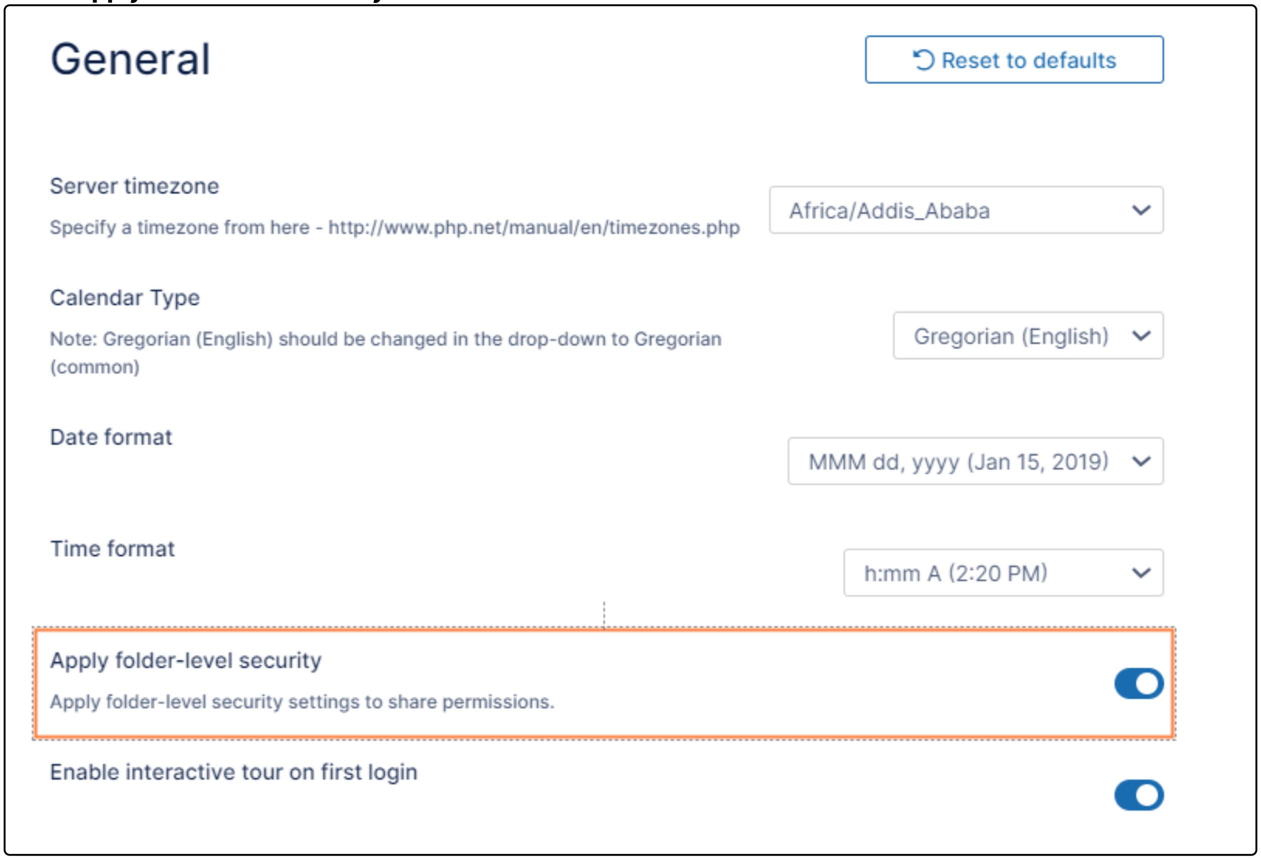
Once a Team Folder is shared, all users with access to the share will see the folder in Team Folders in the navigation panel of the user portal and all FileCloud clients such as Sync, Drive, Outlook and the Office Add-In. A user's actions on a Team Folder are generally limited by the share permissions given to them on the Team Folder. However, additional limitations may be added to the share permissions for specific users and groups in the form of folder-level permissions.

For more information on folder **share** permissions, read about the Private Share Permissions for Folders.

Enable folder-level permissions

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

2. Enable **Apply folder-level security.**



Apply folder-level permissions to Team Folders:

You can apply folder-level permissions to the top-level Team Folder or to its subfolders.

Here, we will demonstrate how folder-level permissions can be used to enhance share permissions on Team Folders through an example.

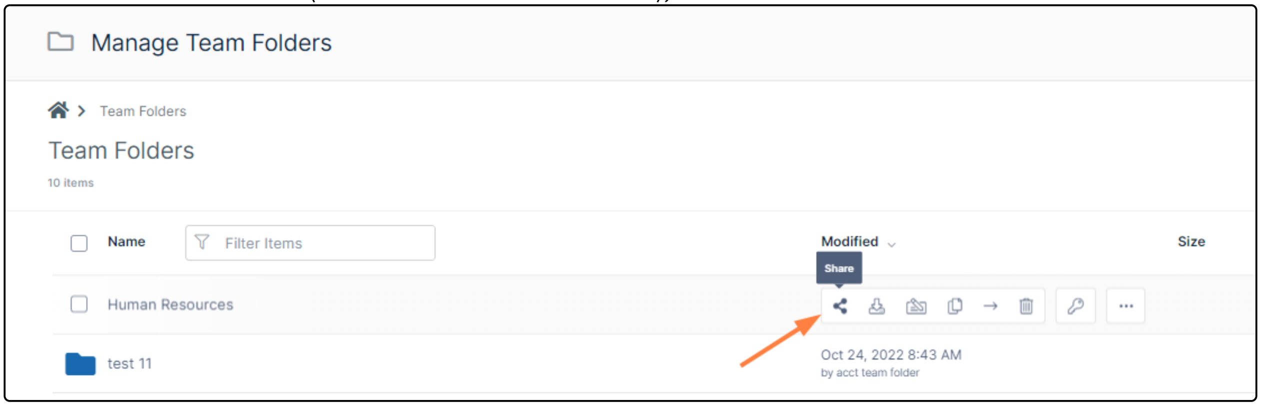
This example uses a common scenario, in which a top-level Team Folder stores various subfolders for the team. The entire team is given access to some of the subfolders, for example, those that contain general information. But only team members whose jobs require more secure information, such as employee ID numbers, are given access to the subfolders that contain that information.

In this example, we will give the entire **Human Resources** team access to the **HR Files** subfolder, but we will only give the users **HR Manager** and **Jessica** access to the **Employee Records** and **Forms** subfolders.

Share the top-level Team Folder with the entire group with all permissions

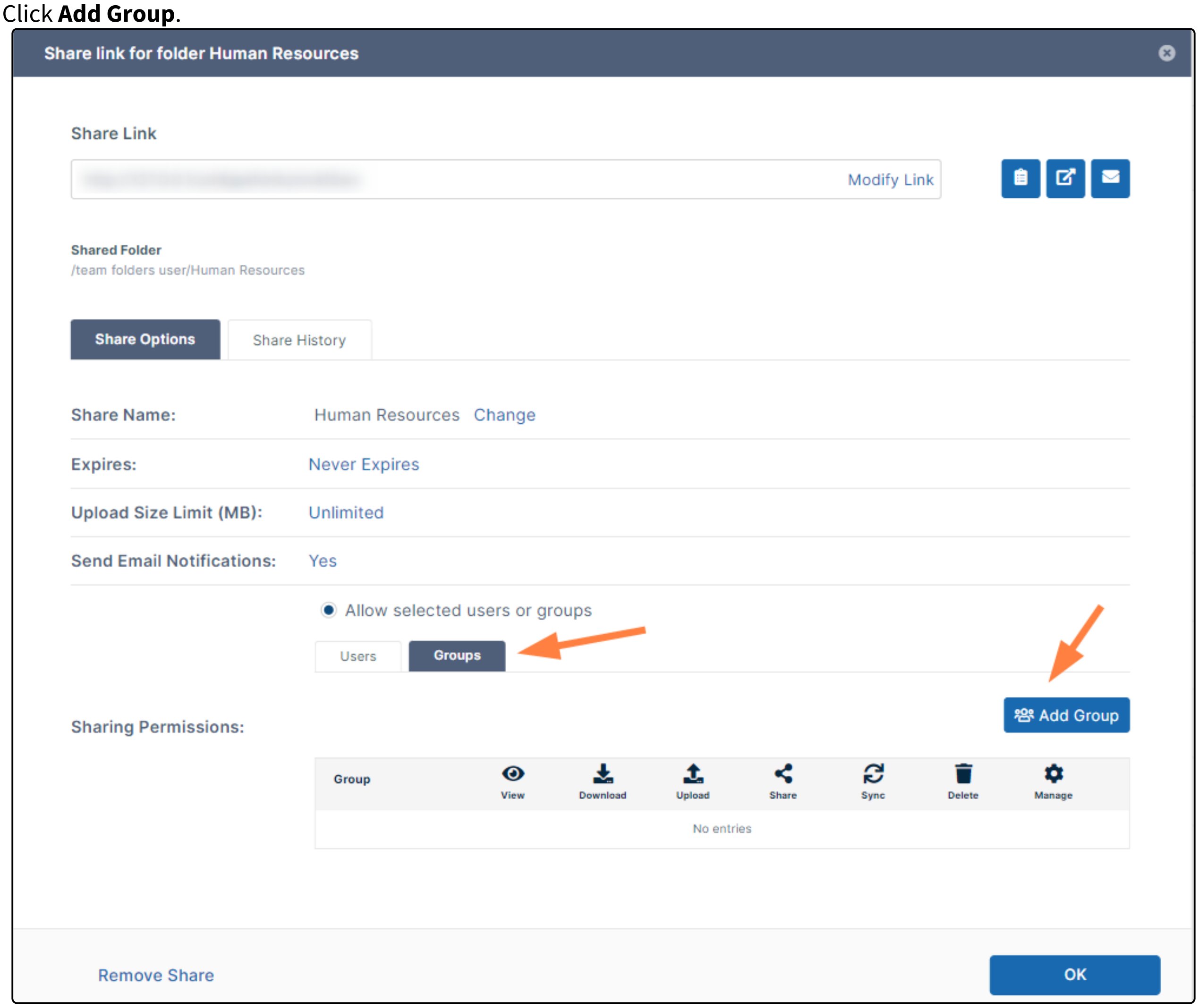
1. From the left navigation panel, click **Team Folders**.

2. Hover over the Team Folder (in this case **Human Resources**), and click the share icon.



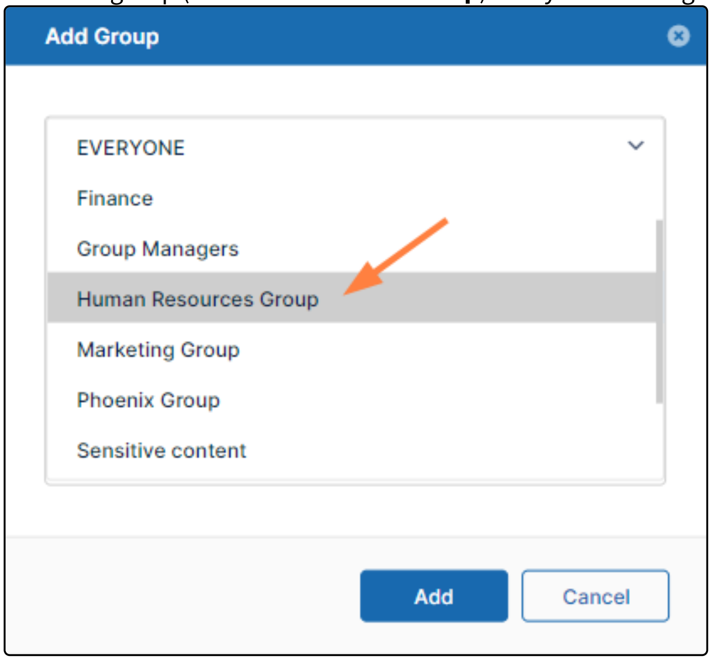
A **Share link for folder** dialog box opens.
First give the entire **Human Resources Group** access to the **Human Resources** folder.

3. Click **Allow selected users or groups,** and then click the **Groups** tab.
4. Click **Add Group**.

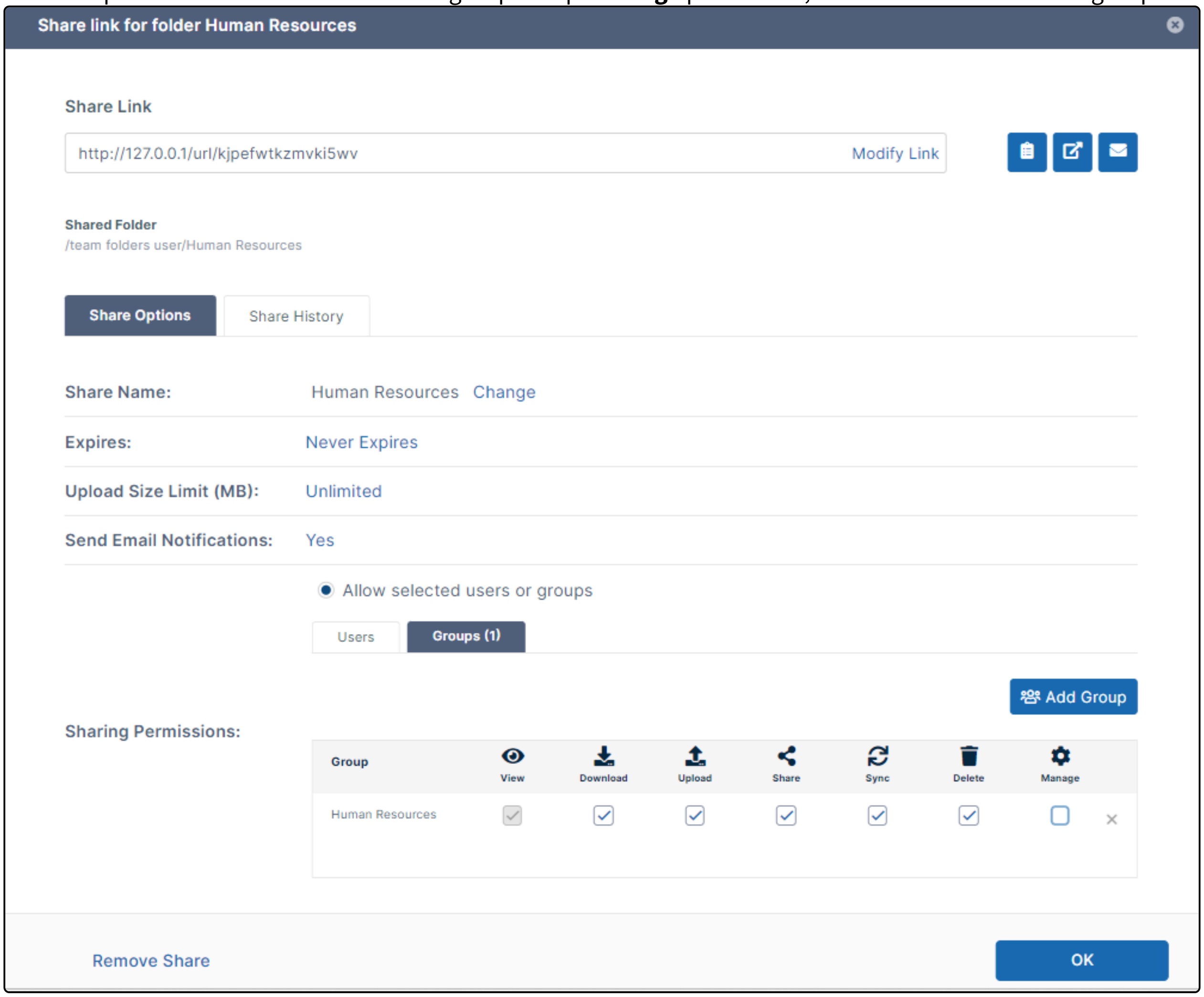


An **Add Group** dialog box listing your FileCloud groups opens.

5. Select the group (**Human Resources Group**) that you want to give access to the Team Folder and click **Add**.



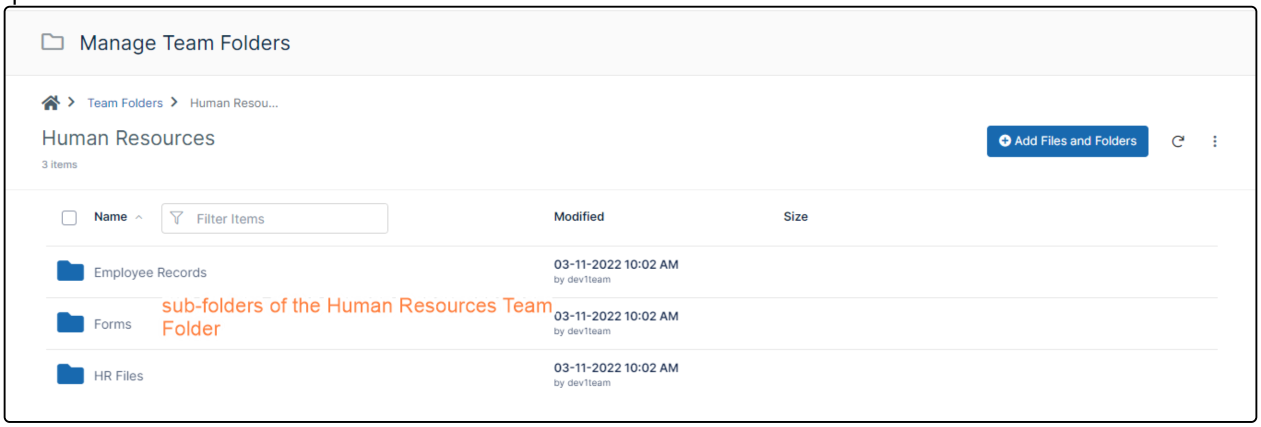
6. Enable all permissions to the folder for the group except **Manage** permission, which is not allowed for a group.



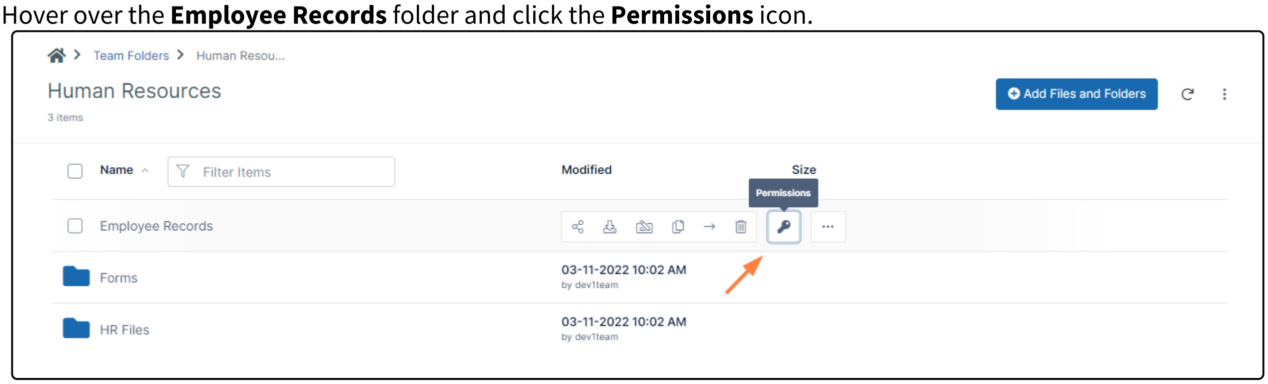
7. Click **OK** and close the dialog box.

Restrict permissions to specific users within the group

1. Open the Human Resources folder to view its subfolders.



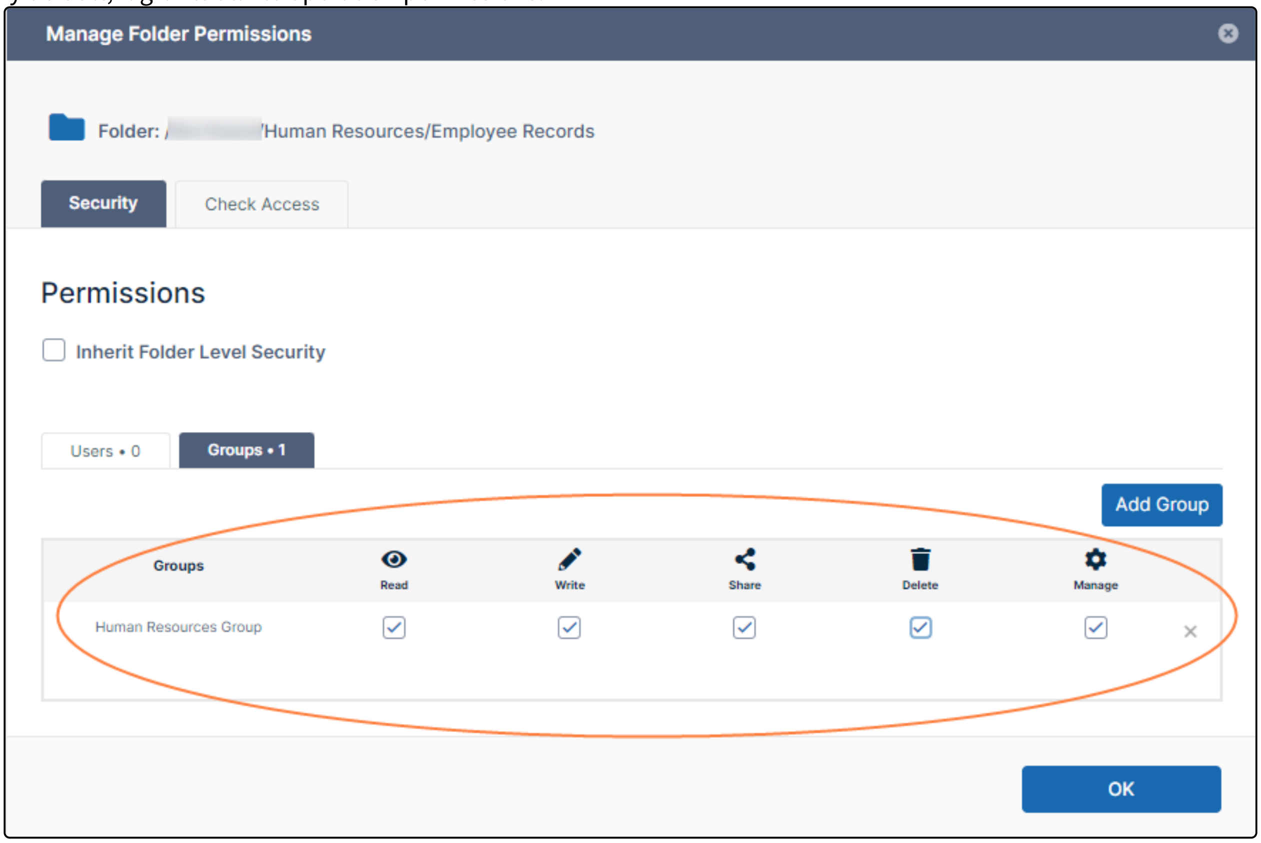
2. We want to give the users **HR Manager** and **Jessica** full access to the **Employee Records** and **Forms** subfolders. We don't want to give the other members of the team any access to these subfolders, but they will still have access to the **HR Files** folder.
3. Hover over the **Employee Records** folder and click the **Permissions** icon.



The **Manage Folder Level Security** dialog box opens for the **Employee Records** subfolder.

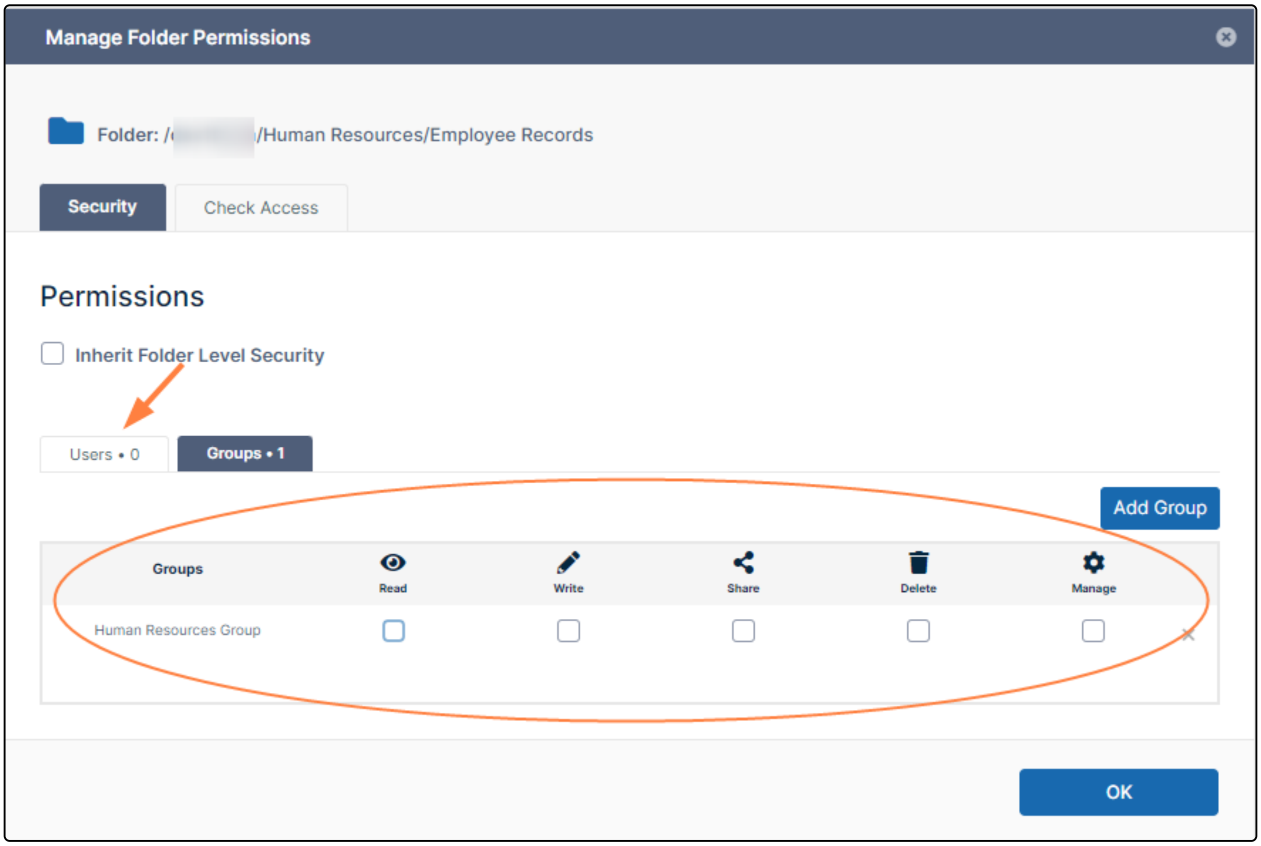
4. Uncheck **Inherit Folder Level Security**.

5. Click the **Groups** tab, then click the **Add Group** button and add **Human Resources Group**.
   By default, it grants all file operation permissions.

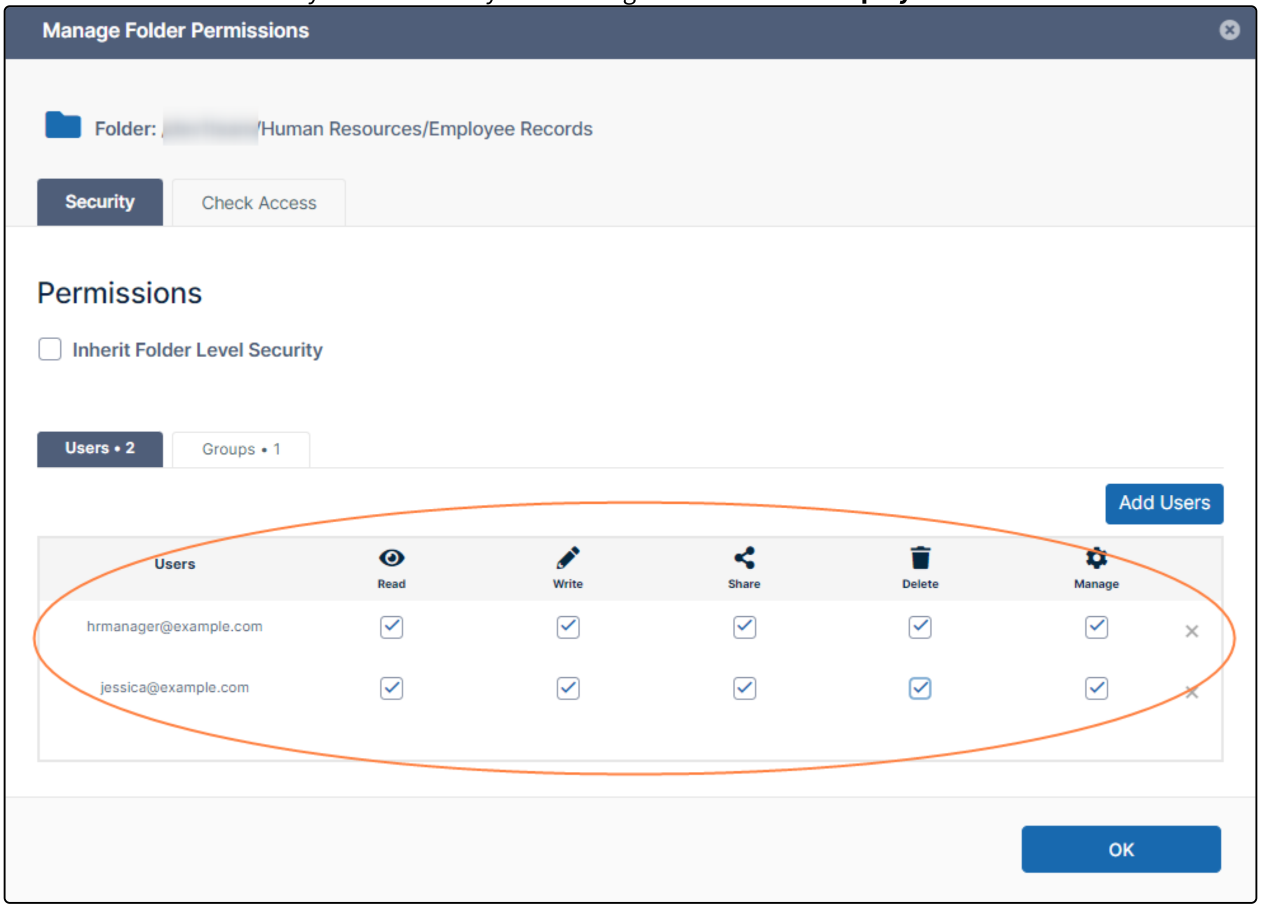


6. To disable the group's access to the **Employee Records** folder, uncheck the boxes under the operations.

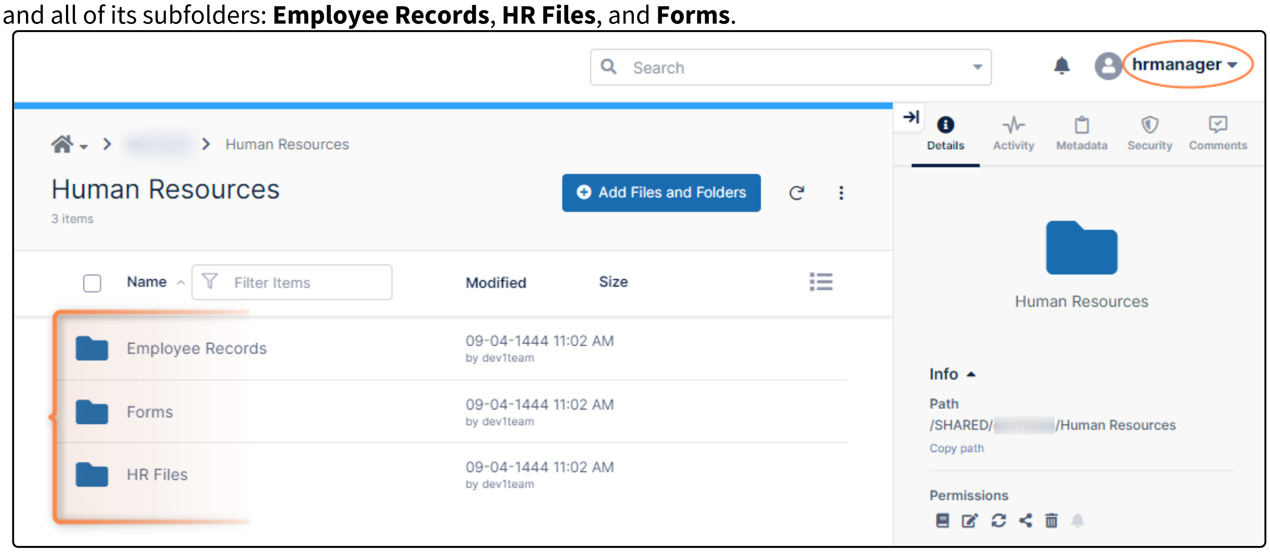
7. Then click the **Users** tab.



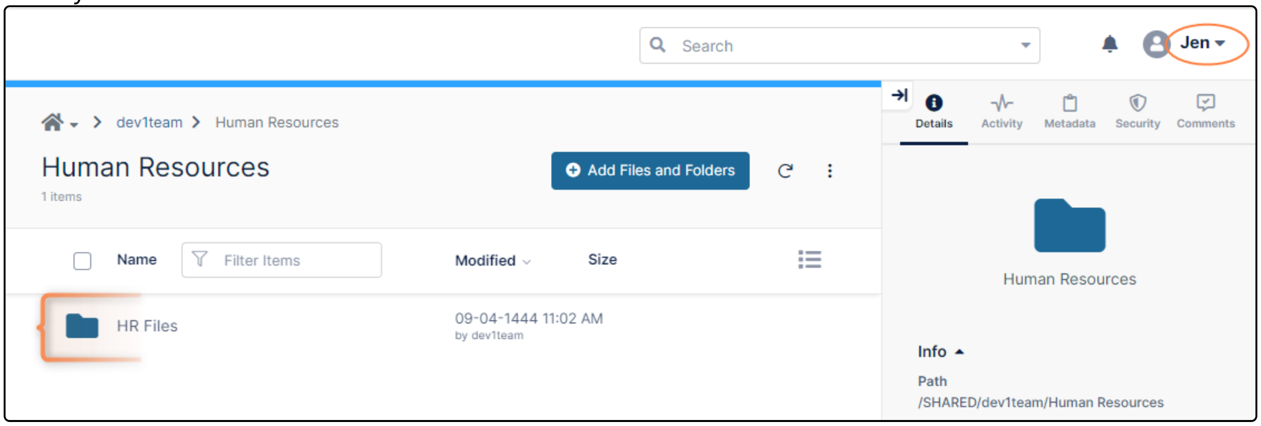
8. Click **Add Users** and add only the users who you want to give access to the **Employee Records** folder.



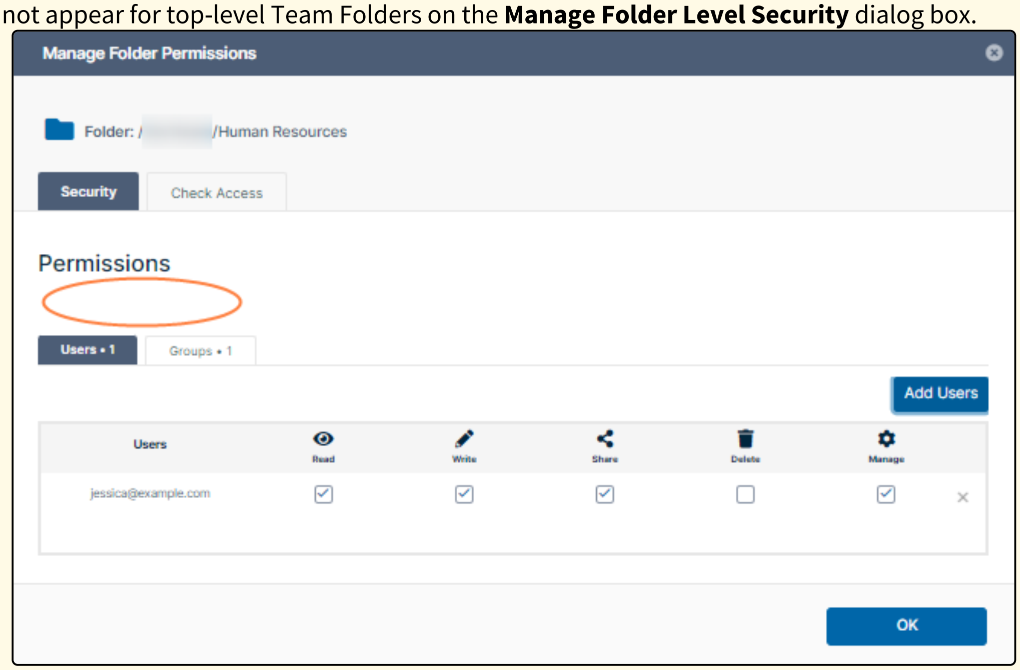
9. Repeat steps 3 through 8 for the **Forms** folder.
   Now, when either **HR Manager** or **Jessica** logs in to the user portal, they see the **Human Resources** Team Folder and all of its subfolders: **Employee Records**, **HR Files**, and **Forms**.



When another member of the **Human Resources** group logs in, they see the **Human Resources** Team Folder, but only the **HR Files** subfolder:



Note: Top-level Team Folder permissions cannot be inherited, and the **Inherit Folder Level Security** checkbox does not appear for top-level Team Folders on the **Manage Folder Level Security** dialog box.



Checking Effective Permissions

A user may have been assigned multiple types of permissions for a Team Folder. For example, the Team Folder shared with the user gave the user certain permissions but you may also have applied different folder-level permissions to the folder. In addition, the user may have permissions through a group it belongs to.

You can check the Team Folder's effective permissions to see the actual permissions the user has to the folder when all of these permissions are combined.

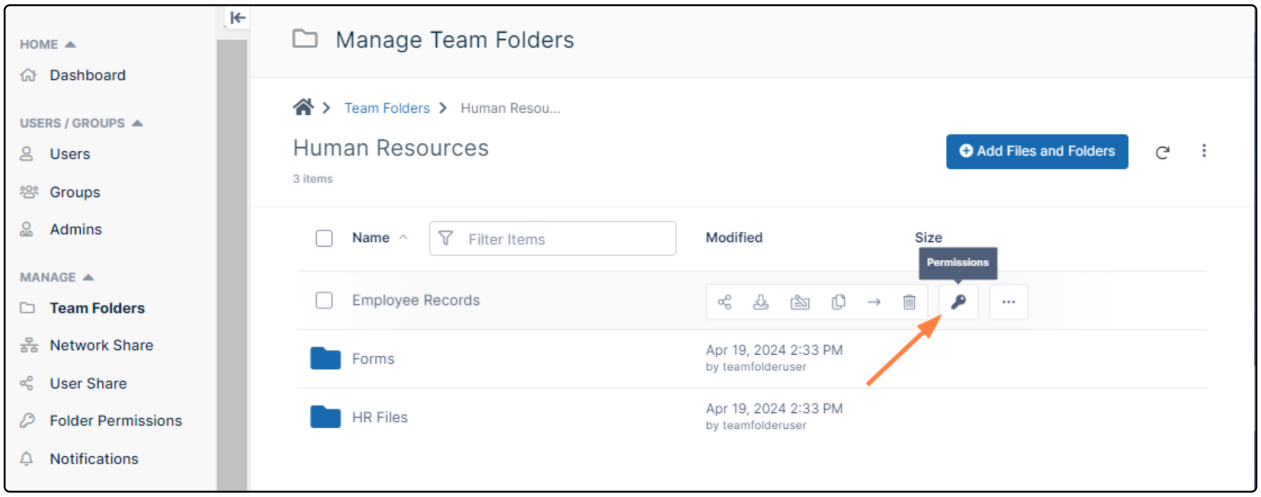
Effective permissions take into account that:

- If a user has both share and folder-level permissions to a folder, the more restrictive of the two apply.
- If a user has folder-level permissions assigned to them individually, and folder-level permissions assigned through a group they belong to, the user assigned permissions take precedence.

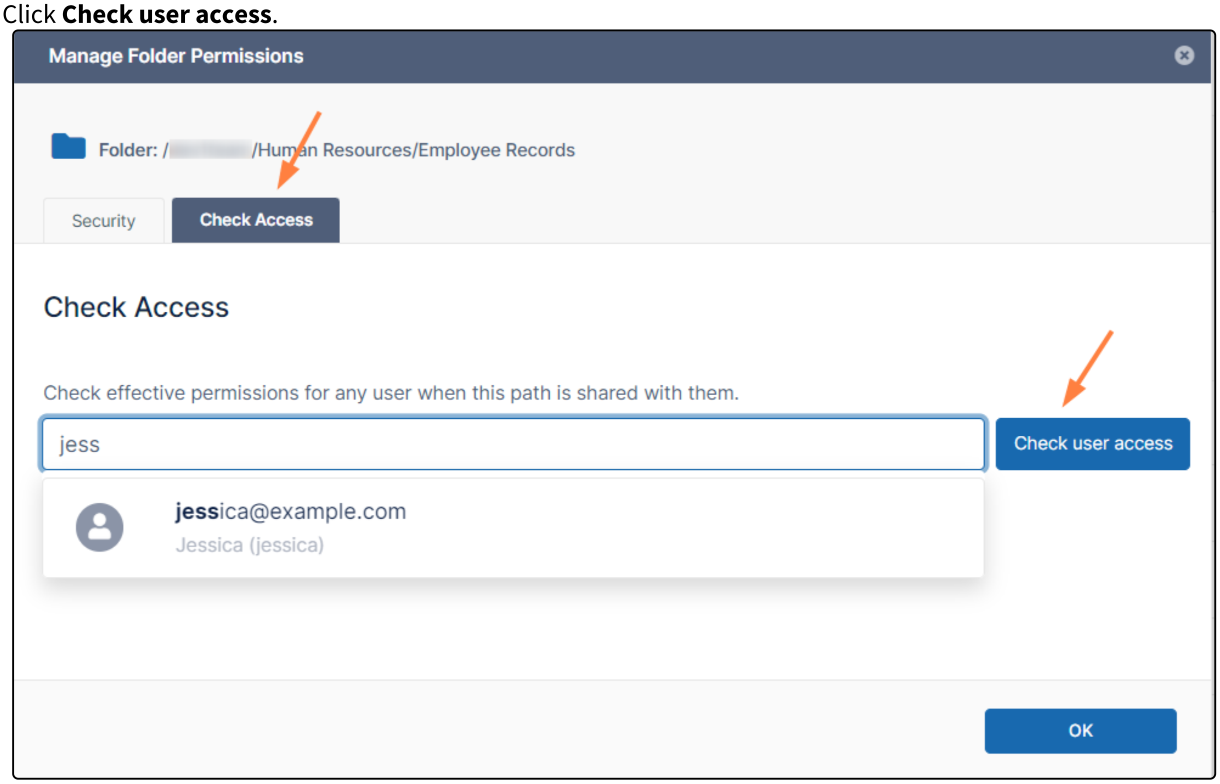
To check effective Team Folder permissions:

In this example, we'll check the effective permissions for the example above.

1. Navigate to the Human Resources/Employee Records Team Folder and click the permissions icon (the Key icon) in its row.

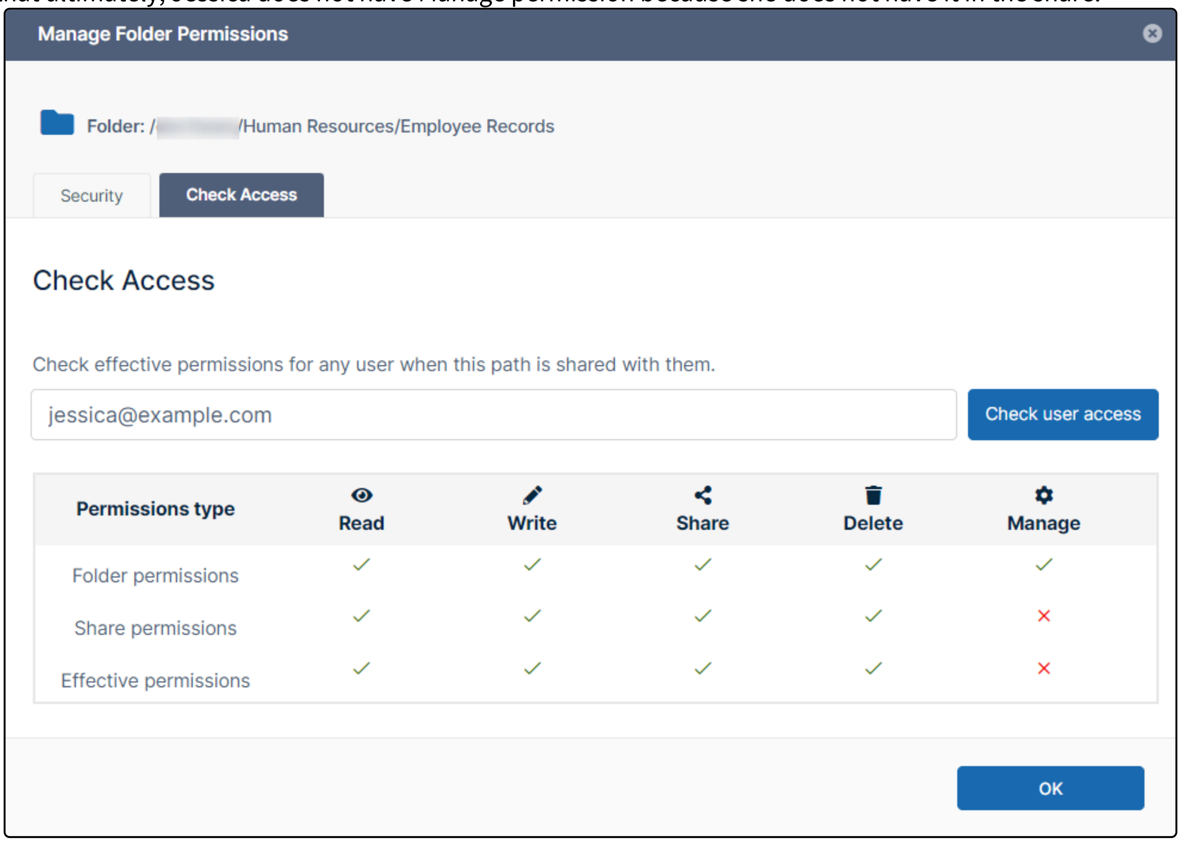


   The **Manage Folder Level Security** dialog box opens with the **Security** tab selected.
2. Click the **Check Access** tab.
3. Enter the email or username for Jessica, one of the users we gave folder-level permissions to this folder.
4. Click **Check user access**.



The dialog box lists Jessica's permissions.

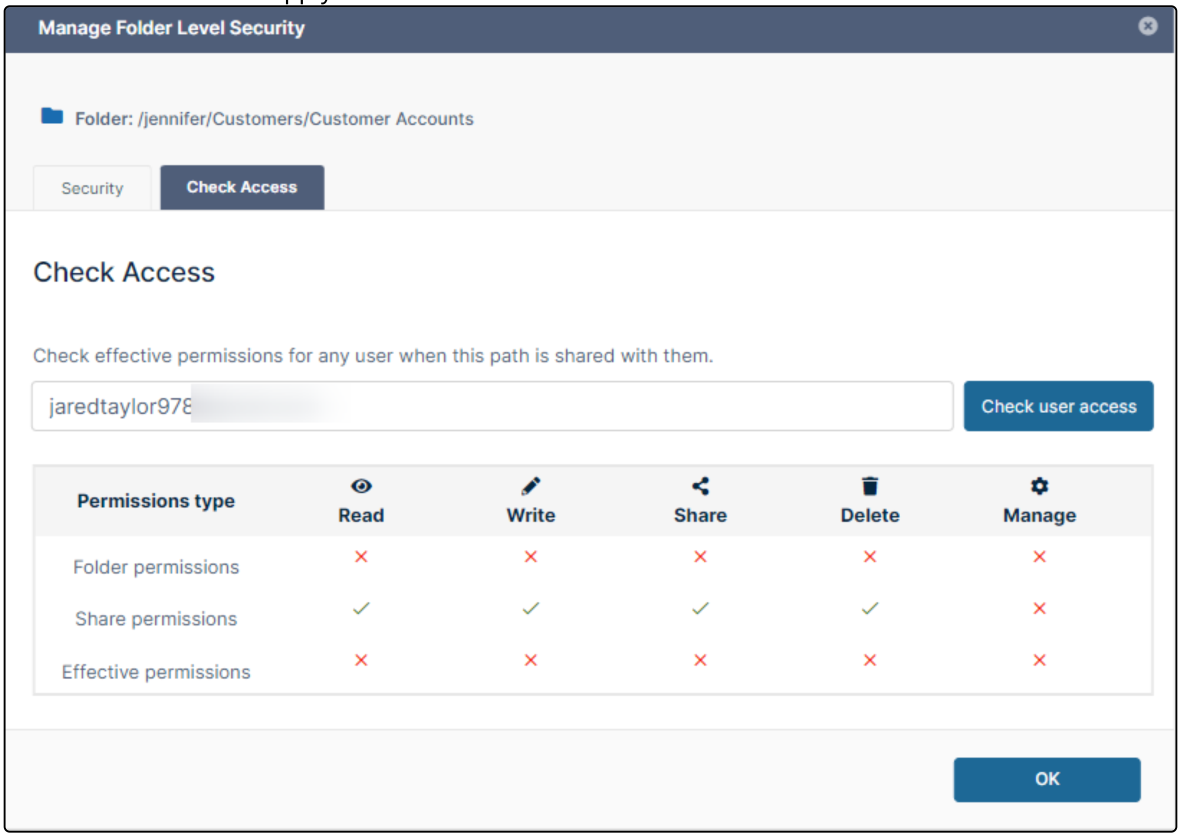
- The **Folder Permissions** row shows that she has all folder-level permissions to the Employee Records folder.
- In the share of the folder, Jessica's group, **Human Resources**, was given all but Manage permissions for the folder, which is shown in the **Share permissions** row.
- The more restrictive of folder-level or share permissions apply, so the **Effective permissions** row shows that ultimately, Jessica does not have Manage permission because she does not have it in the share.



Now let's look at the effective permissions for Aliya, another user in the **Human Resources** group who has not been given any user folder-level permissions to the **Employee Records** folder. Her group has had all folder-level permissions for the Human Resources folder removed.

- The **Folder permissions** row shows that she has no folder-level permissions for accessing the folder.
- On the share of the folder, her group is given read, write, share, and delete permissions, so the **Share permissions** row shows those permissions.
- The combined permissions, which appear in the **Effective permissions** row, show that Aliya has no access to the folder, because her group has both folder-level and share permissions assigned, and in this

case the most restrictive apply.



More Information:

FileCloud Blogs
• Using “Allow Manage” on FileCloud Team Folders • User-Based Management of Team Folder Permissions

How Folder-Level Permissions and Share Permissions Work Together

Permission rules: How permissions interact

- Whichever is more restrictive, share permissions or folder-level permissions, apply.
- Inheritance of folder-level permissions is turned on by default for all folders and sub-folders.
    - Subfolders inherit the folder-level permissions of their immediate parent folders.
    - If you manually turn off inheritance for a folder, its subfolders still have inheritance turned on.
- In a share, greatest share permissions given to a user or the user's group apply.
- In folder-level permissions, user permissions override permissions of a group the user is in.

- When a user belongs to multiple groups with conflicting permissions, the effective permissions are the enabled permissions from all their groups combined.

The following examples illustrate the above permission rules using these components:

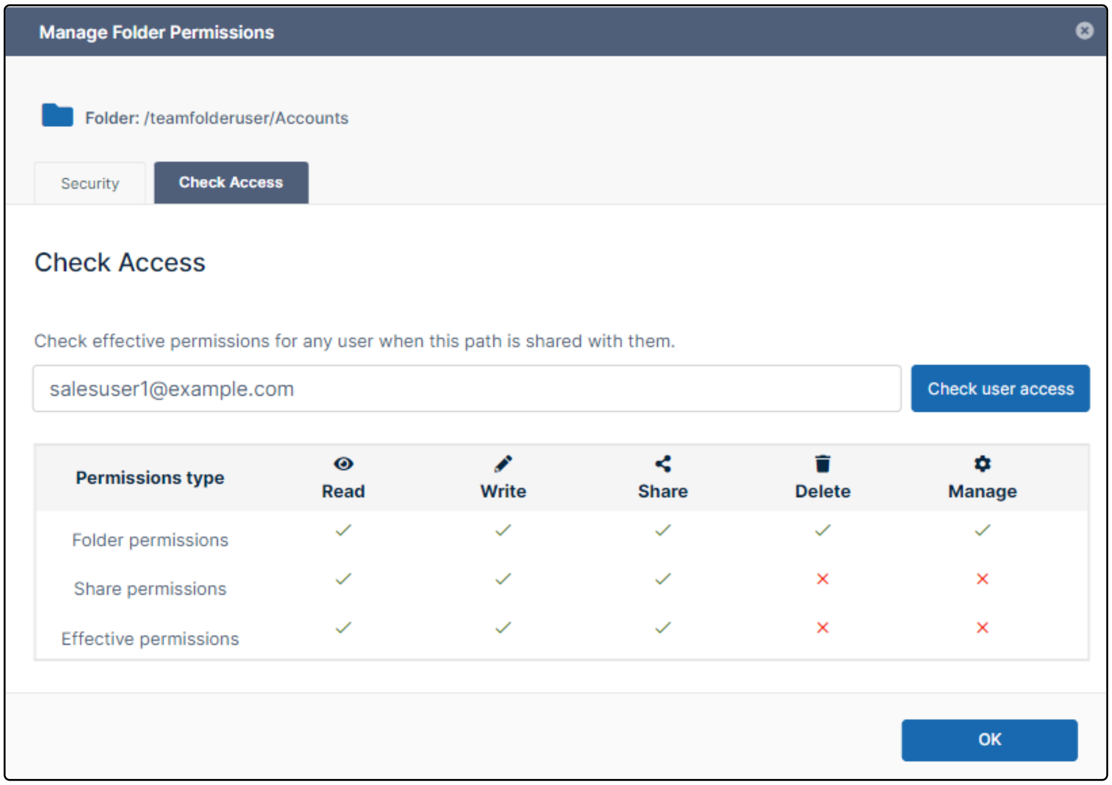
Group: **Sales Group** **Members:** **SalesUser1** **SalesUser2**	**Folder:** **Accounts** **Subfolder:** **MillerAcct**

Example 1:
The more restrictive of folder-level and share permissions apply.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **Accounts** are **read**, **write**, and **share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
	EFFECTIVE	SalesUser1	Y	Y	Y		



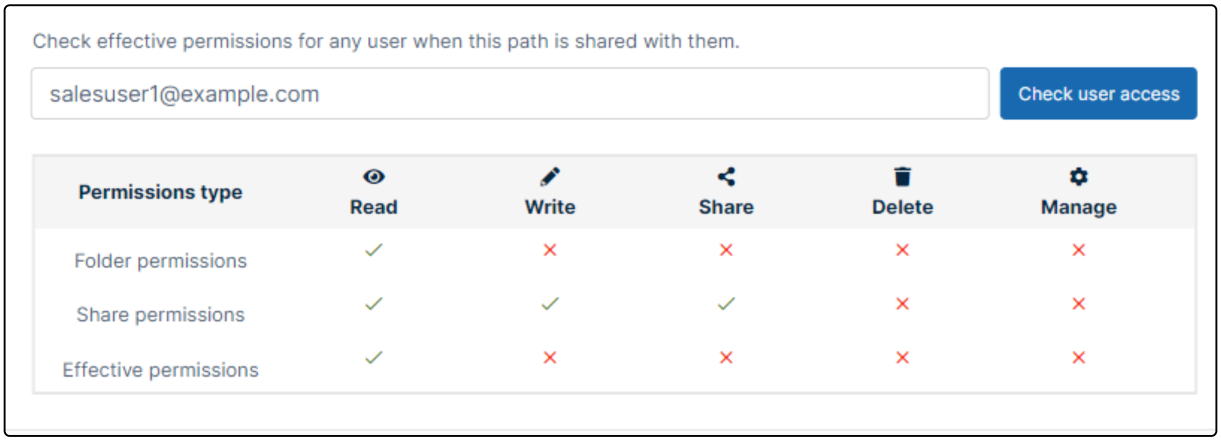
Example 2:

The more restrictive of folder-level and share permissions apply.
User folder-level permissions supersede group folder-level permissions.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1** is given **read** folder-level permission to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permission to the Team Folder **Accounts** is **read**.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **Accounts** are **read, write, and share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1	Y				
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE						
		SalesUser1	Y				
		SalesUser2	Y	Y	Y		

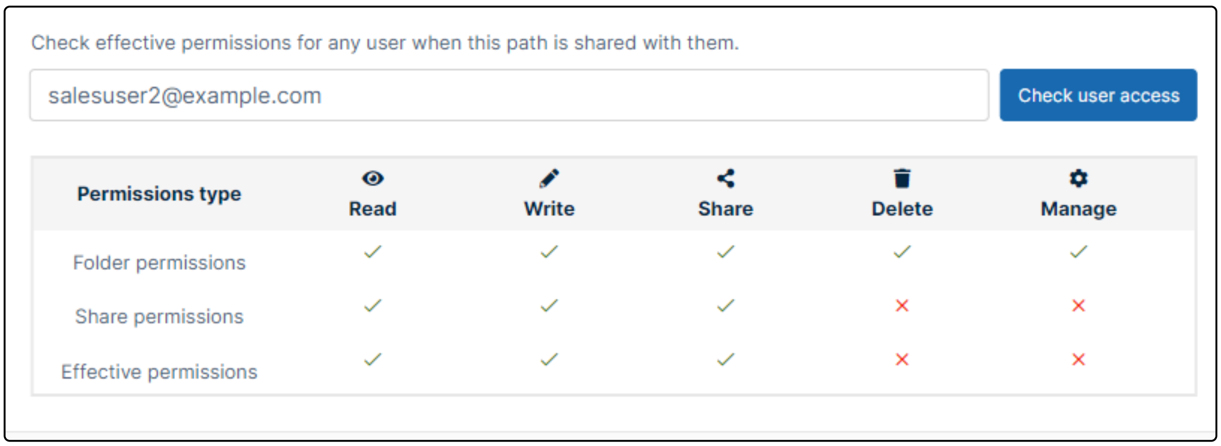


Check effective permissions for any user when this path is shared with them.

salesuser1@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✗	✗	✗	✗
Share permissions	✓	✓	✓	✗	✗
Effective permissions	✓	✗	✗	✗	✗



Check effective permissions for any user when this path is shared with them.

salesuser2@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✓	✓	✓	✓
Share permissions	✓	✓	✓	✗	✗
Effective permissions	✓	✓	✓	✗	✗

Example 3:

The more restrictive of folder-level and share permissions apply.
In a share, greatest share permissions given to a user or the user's group apply.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, **share**, **delete**, and **manage** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- **SalesUser1** has **all** share permissions to the Team Folder **Accounts**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **Accounts** are **all** permissions.

- **SalesUser2**'s effective (actual) permissions to the Team Folder **Accounts** are **read**, **write**, and **share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts folder	ACL	Sales Group	Y	Y	Y	Y	Y
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1	Y	Y	Y	Y	Y
		SalesUser2					
	EFFECTIVE						
		SalesUser1	Y	Y	Y	Y	Y
		SalesUser2	Y	Y	Y		

Check effective permissions for any user when this path is shared with them.

salesuser1@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✓	✓	✓	✓
Share permissions	✓	✓	✓	✓	✓
Effective permissions	✓	✓	✓	✓	✓

Check effective permissions for any user when this path is shared with them.

salesuser2@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✓	✓	✓	✓
Share permissions	✓	✓	✓	✗	✗
Effective permissions	✓	✓	✓	✗	✗

Example 4:

By default, subfolders inherit the permissions of their parent folders.
User folder-level permissions supersede group folder-level permissions.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.

- The Team Folder **MillerAcct** inherits the permissions from the Team Folder **Accounts**.
- **SalesUser1** is given the folder-permission read to the Team Folder **MillerAcct**.
- **SalesUser1**'s effective (actual) permission to the Team Folder **MillerAcct** is **read** permission.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share**.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts Folder	ACL	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE						
		SalesUser1	Y	Y	Y		
		SalesUser2	Y	Y	Y		

Inherited by

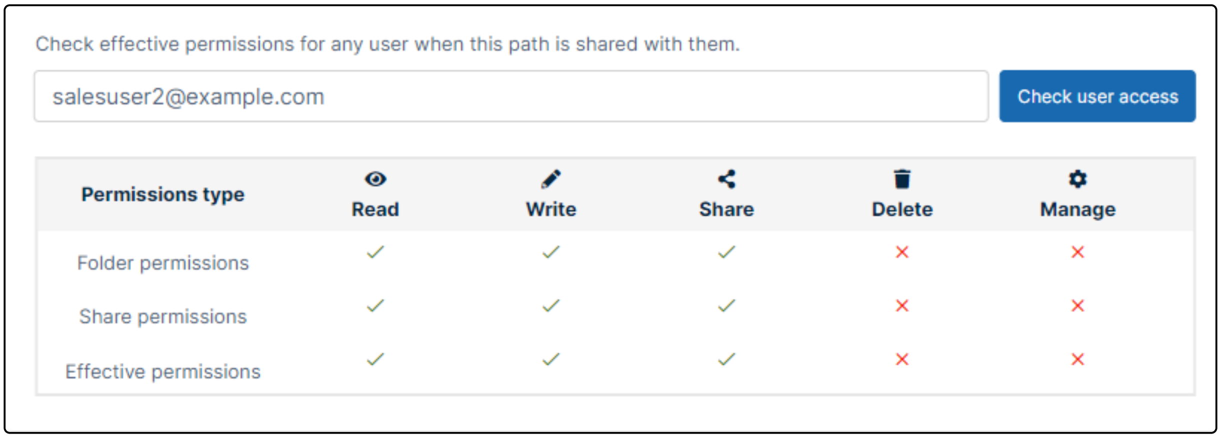
	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
MillerAcct	ACL	Sales Group	Y	Y	Y		
		SalesUser1	Y				
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE						
		SalesUser1	Y				
		SalesUser2	Y	Y	Y		

Check effective permissions for any user when this path is shared with them.

salesuser1@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	×	×	×	×
Share permissions	✓	✓	✓	×	×
Effective permissions	✓	×	×	×	×



Example 5:
By default, subfolders inherit the permissions of their parent folders.
In a share, greatest share permissions given to a user or the user's group apply.

View the example

- The **Sales Group** is given the folder-level permissions **read**, **write**, and **share** to the Team Folder **Accounts**.
- The **Sales Group** has the share permissions **read**, **write**, and **share** to the Team Folder **Accounts**.

- The Team Folder **MillerAcct** inherits the permissions from the Team Folder **Accounts**.
- **SalesUser1** is given the share permission read to the Team Folder **MillerAcct**.
- **SalesUser1**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share** permission.
- **SalesUser2**'s effective (actual) permissions to the Team Folder **MillerAcct** are **read**, **write**, and **share** permission.

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
Accounts Folder	ACL	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	EFFECTIVE	SalesUser1	Y	Y	Y		
		SalesUser2	Y	Y	Y		

Inherited by

	PERMISSION		READ	WRITE	SHARE	DELETE	MANAGE
MillerAcct	ACL	Sales Group	Y	Y	Y		
		SalesUser1					
		SalesUser2					
	SHARE	Sales Group	Y	Y	Y		
		SalesUser1	Y				
		SalesUser2					
	EFFECTIVE	SalesUser1	Y	Y	Y		
		SalesUser2	Y	Y	Y		

Check effective permissions for any user when this path is shared with them.

salesuser1@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✓	✓	✗	✗
Share permissions	✓	✓	✓	✗	✗
Effective permissions	✓	✓	✓	✗	✗

Check effective permissions for any user when this path is shared with them.

salesuser2@example.com

Check user access

Permissions type	Read	Write	Share	Delete	Manage
Folder permissions	✓	✓	✓	✗	✗
Share permissions	✓	✓	✓	✗	✗
Effective permissions	✓	✓	✓	✗	✗

How folder permissions affect copy and move actions

In some cases, combined share and folder-level permissions on folders limit whether **copy** and **move** for files or folders and **copy file or folder** and **move file or folder** in automated (user) workflows are permitted. In the scenarios in the following table, copy and move or move only is not allowed, and if you attempt to perform the action an error message is returned.

1	View	-	NOT allowed	NOT allowed
2	View+Download	-	allowed	NOT allowed
3	View	Read	NOT allowed	NOT allowed
4	View+Download	Read	allowed	NOT allowed

More Examples

Scenario 1: Give folder permissions only to specific users or groups

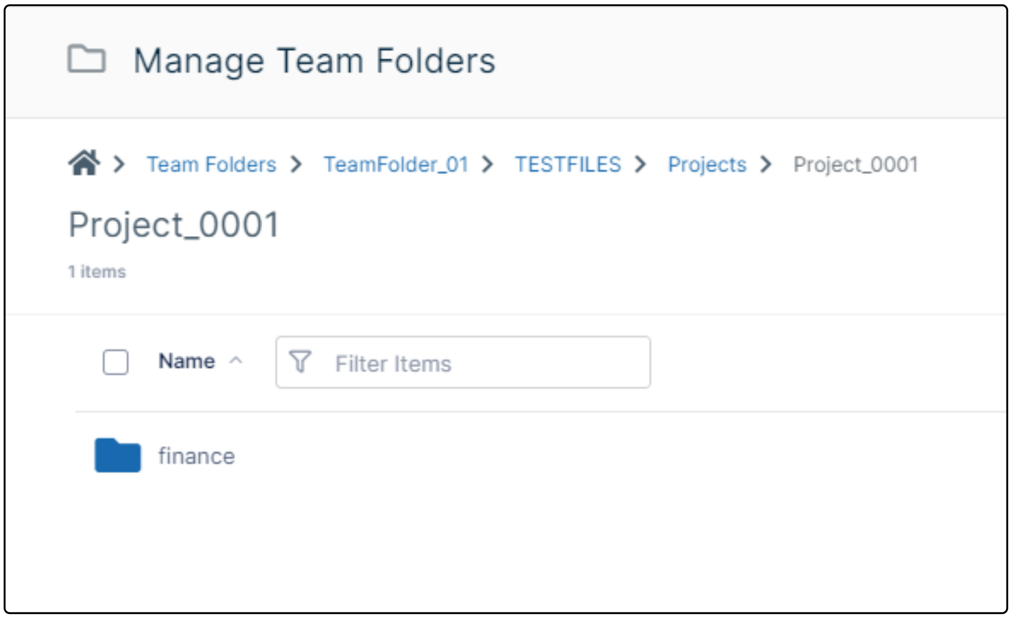
In this scenario, an administrator gives two groups access to a folder, but only gives one group access to one of its subfolders.

Example of giving permissions to only specific users or groups

In this example, the folder **TeamFolder_01** is only shared with the groups:

- **ProjectManagers**
- **ProjectTeam**

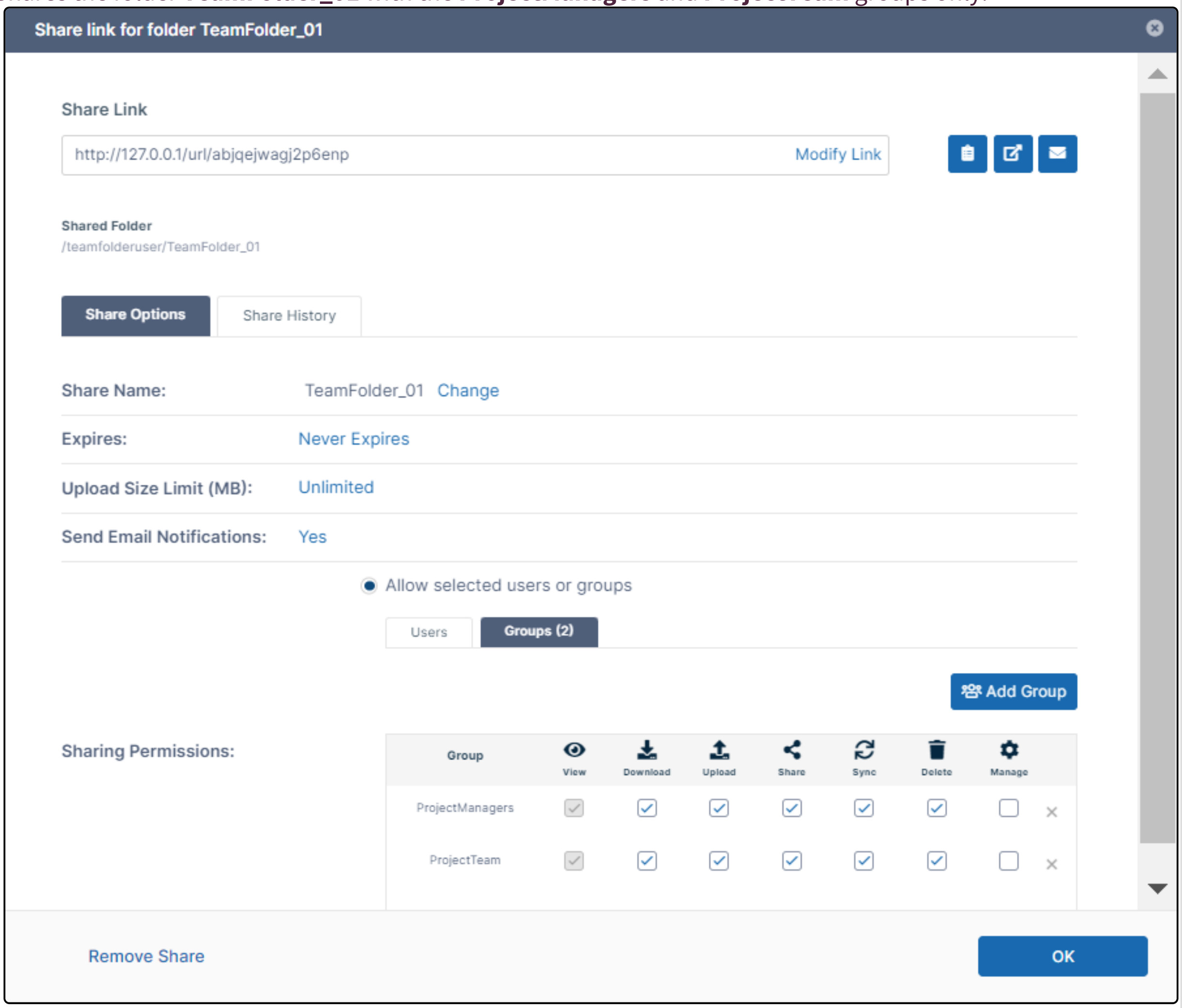
Only the group **ProjectManagers** is given access to the embedded subfolder **Project_0001/finance.**



Example of giving permissions to only specific users or groups

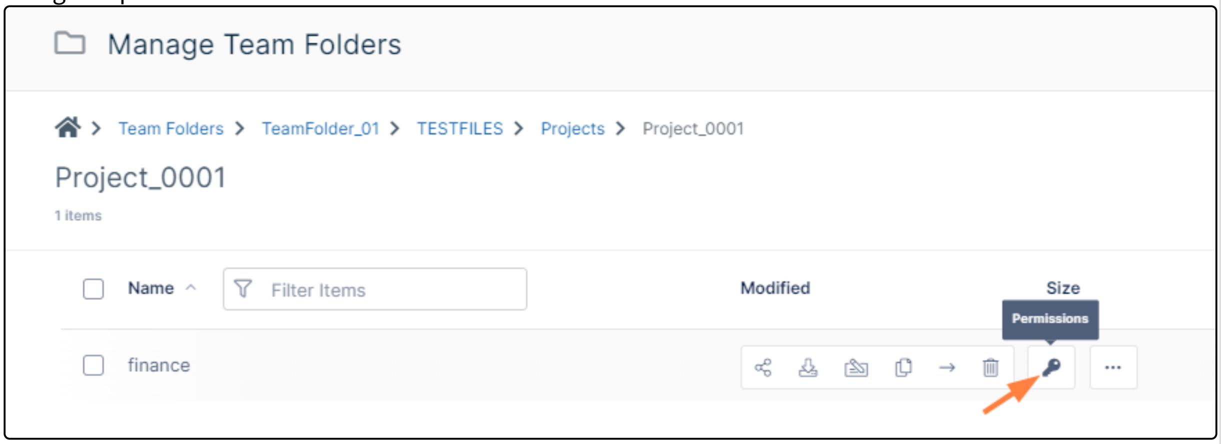
To accomplish this, the administrator:

1. Shares the folder **TeamFolder_01** with the **ProjectManagers** and **ProjectTeam** groups only.



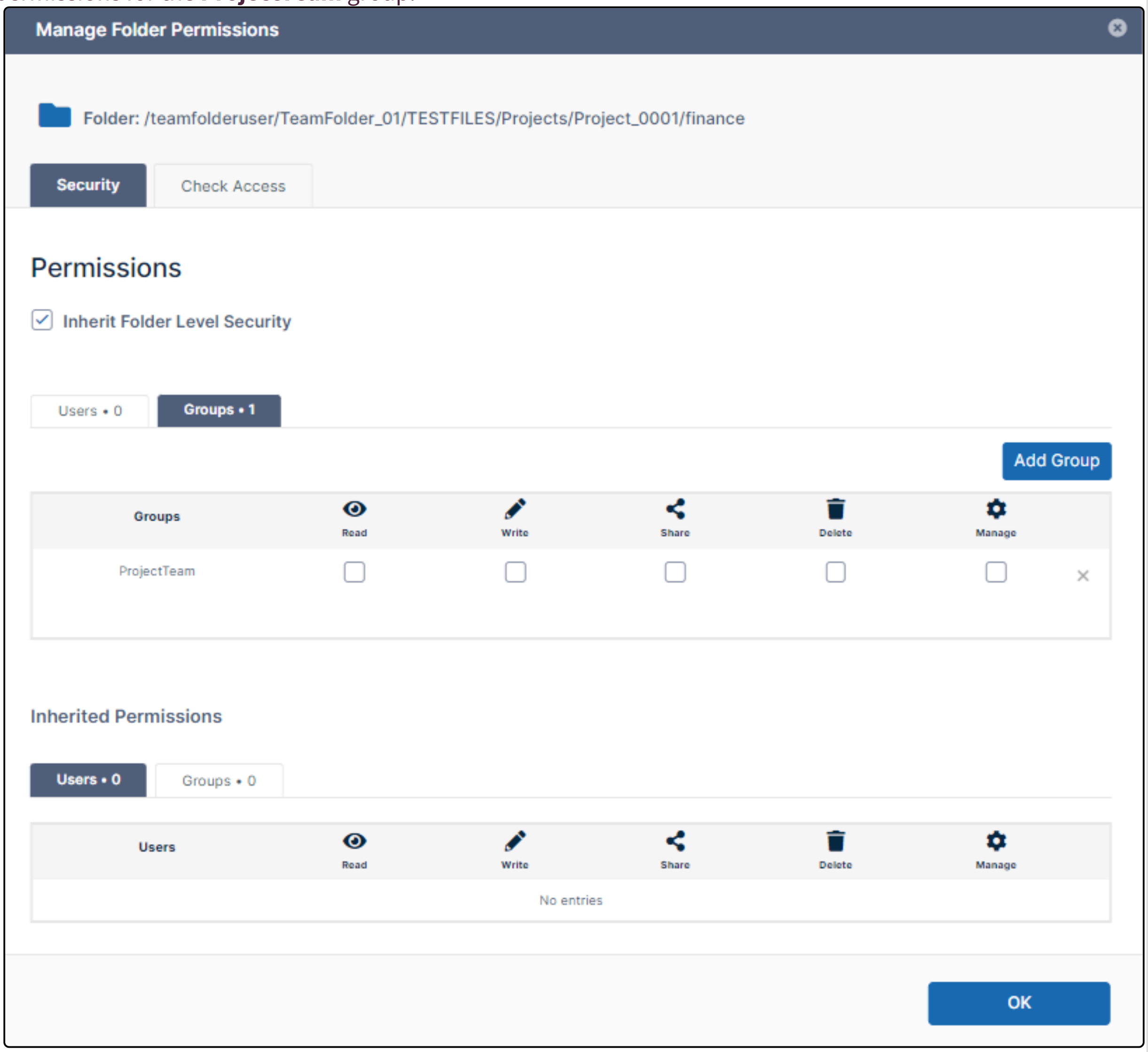
Example of giving permissions to only specific users or groups

2. Configures permissions on the **finance** subfolder:



Example of giving permissions to only specific users or groups

3. Adds **ProjectTeam** group to the **finance** folder in **Manage Folder Permissions**. Then removes all permissions for the **ProjectTeam** group.

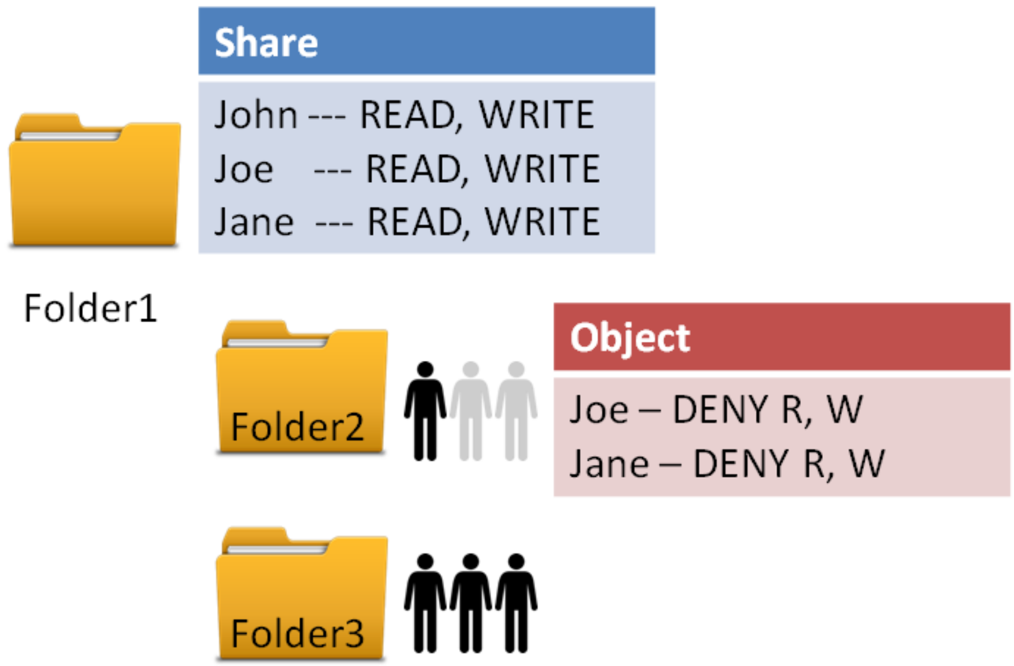


Now, members of the **ProjectManagers** group are able to access the finance folder, but members of the **ProjectTeam** group are not.

Scenario 2: Remove access to specific folders for certain users

In this scenario, an administrator sets different permissions on parent and child folders.

Example of a Sharing Scenario



In this example, Folder1 is shared with Read and Write permissions to the following users:

- John
- Joe
- Jane

This means all three users can:

- Read files in Folder1
- Write files in Folder1

In this example, the administrator wants to allow only John access to the subfolder, Folder2.

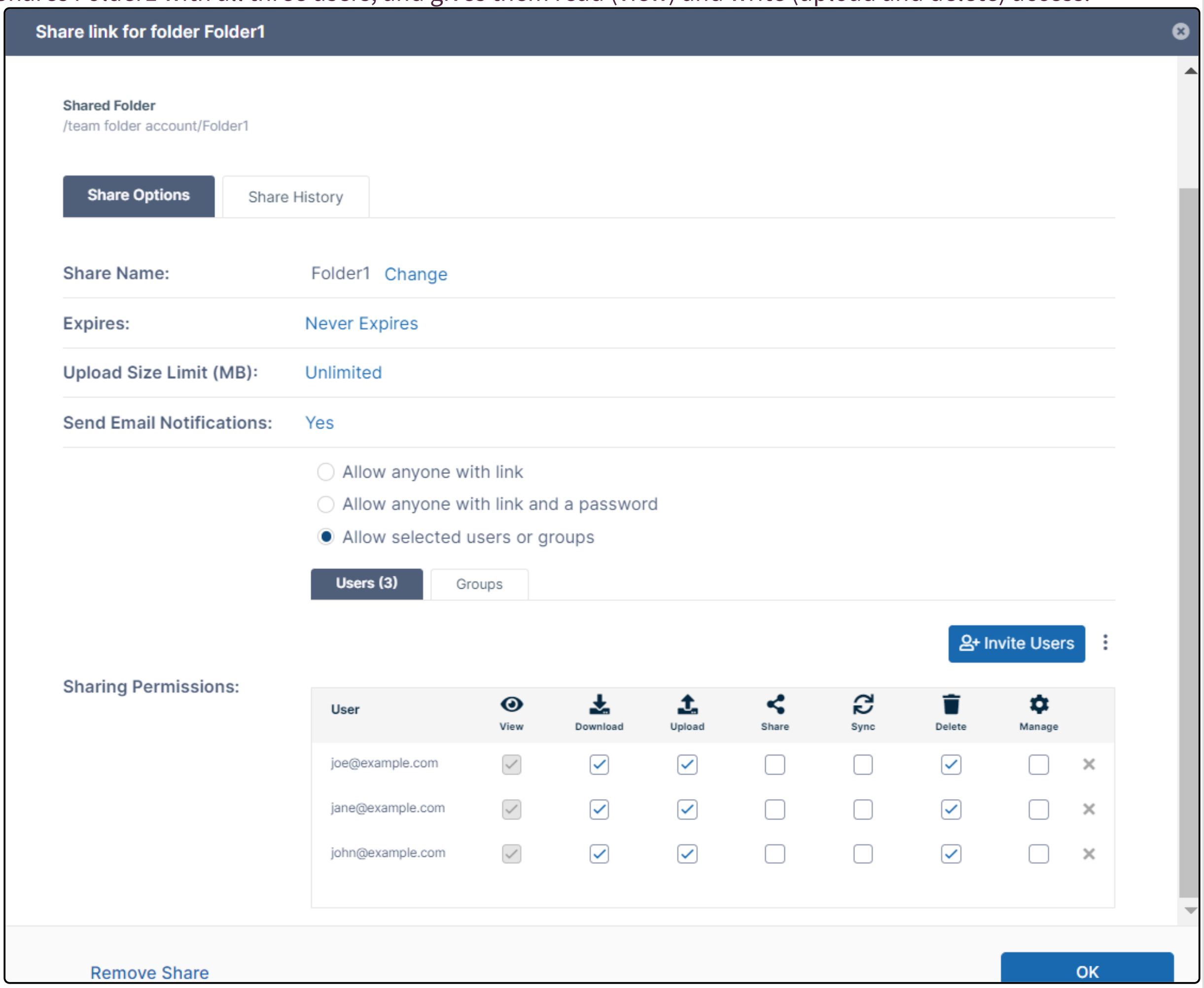
The administrator therefore wants the folder access to be the following:

- Folder1 - accessible to John, Joe, and Jane
- Folder2 - accessible to John
- Folder3 - accessible to John

Example of a Sharing Scenario

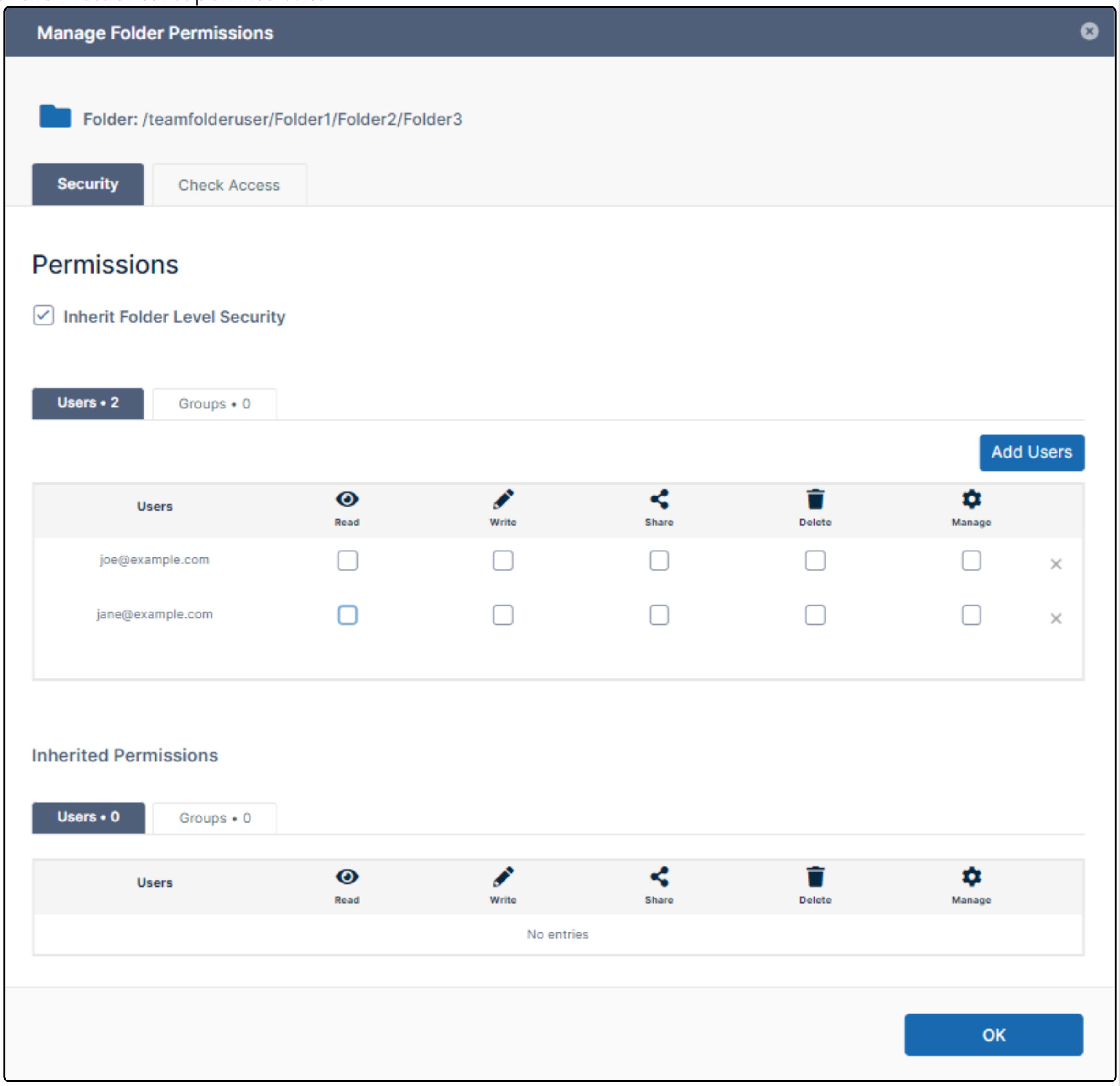
To accomplish this, the administrator:

1. Shares Folder1 with all three users, and gives them read (view) and write (upload and delete) access.



Example of a Sharing Scenario

2. Removes folder-level security permissions for the two users who will not have access to Folder2 removing all of their folder-level permissions.



When John, Joe, and Jane access the folders:

User	Folder1	Folder2	Folder3
John	✅ See it listed ✅ Access its content	✅ See it listed ✅ Access its content	✅ See it listed ✅ Access its content

Example of a Sharing Scenario

User	Folder1	Folder2	Folder3
Joe	✅ See it listed ✅ Access its content	❌ See it listed ❌ Access its content	❌ See it listed ❌ Access its content
Jane	✅ See it listed ✅ Access its content	❌ See it listed ❌ Access its content	❌ See it listed ❌ Access its content

Team Folders

The ability to upload files by dragging and dropping them from file explorer or another application onto a Team Folder is available in FileCloud version 22.1 and later.

As an administrator, you may be asked to manage folders that are shared to allow for collaboration among certain users or groups in your company.

- In FileCloud, these folders are called Team Folders.
- Team folders provide a single place where teams in a company can store and organize files and folders.
- Team folders are normally created by admins or authorized users and instantly made available to all members of a team.

Team Folders use managed storage and are not available for network storage. Therefore, Team Folders are created on managed storage where all files and folders under Team Folders are stored.

How do Team Folders help administrators?

- **Centralized Content Management**: Team Folders facilitate organizing files and folders in a centralized place.
- **Easy Provisioning of Users, Files and Folders**: New users can be provisioned quickly with access to specific files and folders through Team Folders. Similarly, new files can be granted immediate access to all relevant users by uploading the file to the relevant Team Folder.
- **Granular Control of Folders:** Team Folders and their sub folders can give users granular permissions such as Read, Write, Share and Sync access.
- **Manage Selective Sync:** Admins can select specific Team Folders and enable or disable sync permissions on an easy to use user interface.

How can a size limit be placed on a Team Folder?

You can place a size limit on a Team Folder when you share it. You must share a Team Folder to give users and groups access to it. As with any shared folder, when you share a Team Folder, you can set an upload limit that applies to the total amount that can be uploaded to the folder. See Share the Team Folder and Set Permissions.

To Manage Team Folders

Set Up Team Folders	1. Configure the Team Folder Account. 2. Seed and Organize the Team Folder Data. 3. Share a Team Folder and Set Share Permissions for users and groups. 4. Set Granular Folder Permissions on Team Folders (Optional)
Manage Team Folders	Search for a Team Folder Recover Deleted Files View and Restore Previous Versions Promoting Existing User Account to Team Folders

Configure the Team Folders Account

As an administrator, you must enable Team Folders and set up a Team Folder account.

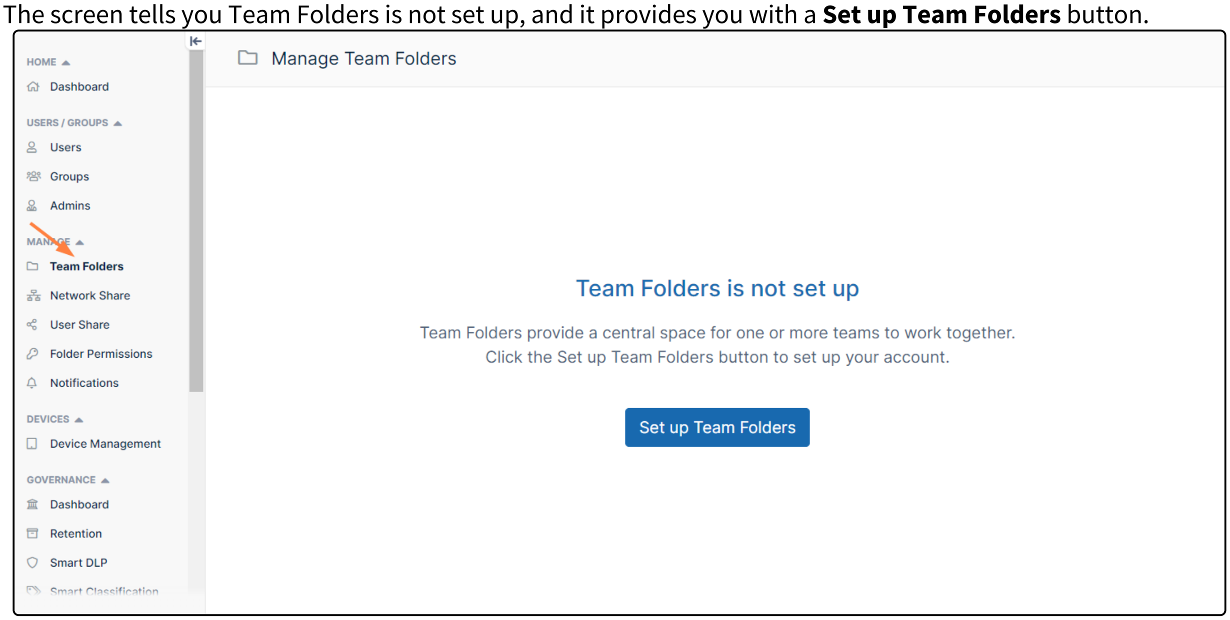
The Team Folder account is a system-designated FULL USER account.

- FileCloud can create the account for you - you just need to choose the name you want to use.
- The Team Folder account is not counted towards your user license.
- FileCloud can also create an email account where it will send Team Folder notifications.
- The email address for Team Folder notifications should take the form of <newalias@mycompany.com>.
- Alternatively, you can promote a user account currently used for company-wide communication as the Team Folder account.

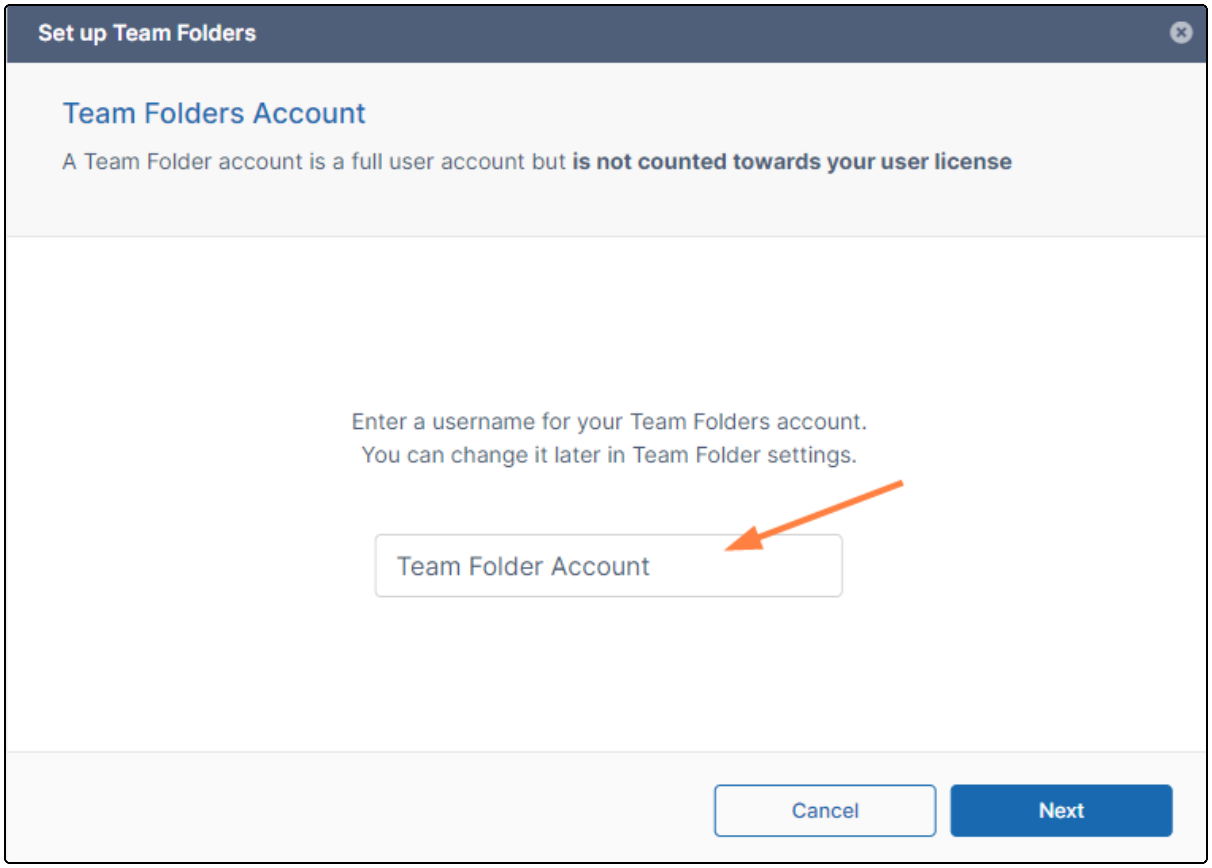
To allow FileCloud to create the Team Folders account

Choose one of the following options:

Create a new account through the Team Folders screen

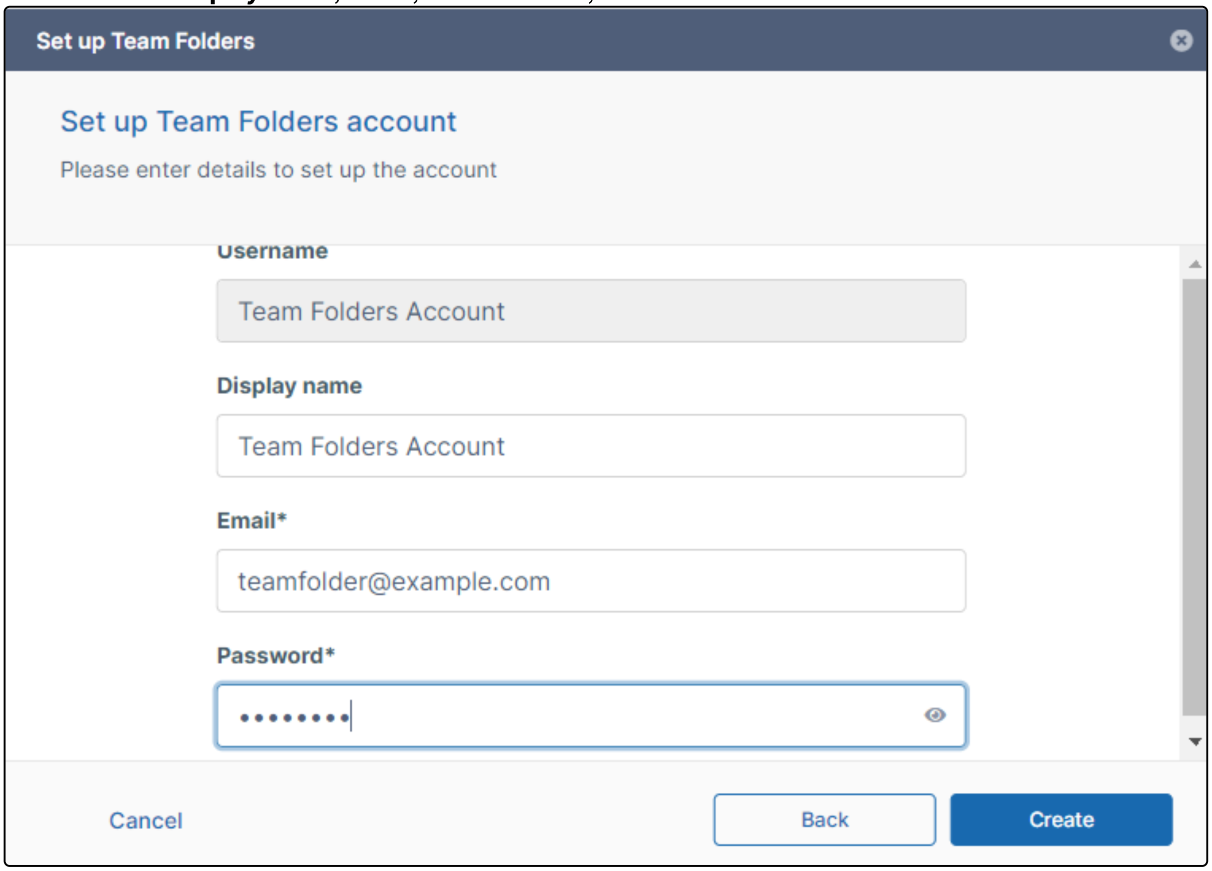
1. In the admin portal's navigation pane, click **Team Folders**.
   The screen tells you Team Folders is not set up, and it provides you with a **Set up Team Folders** button.
   

2. Click the **Set up Team Folders** button.
   A wizard for setting up Team Folders opens.
3. In the **Username** field, enter a name for your Team Folders account (in the example below, we've entered **Team Folder Account**).

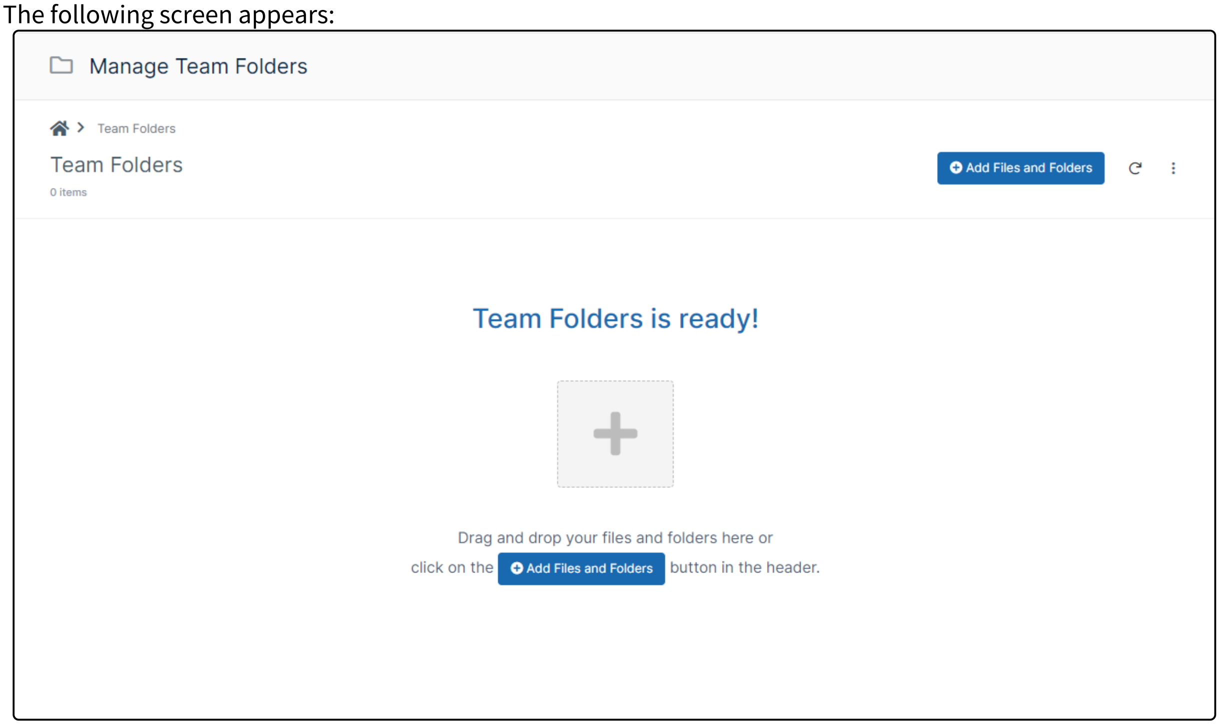


4. Click **Next**.
   The next window of the wizard displays additional fields.

5. Enter values for **Display Name**, **Email**, and **Password**, and click **Create**.

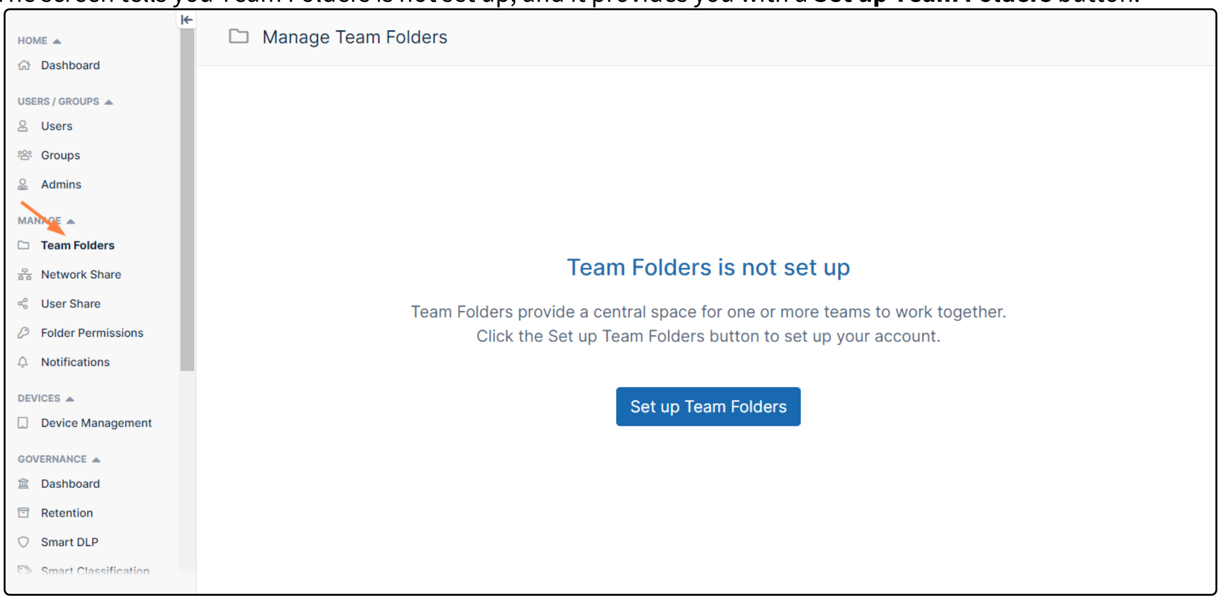


The following screen appears:

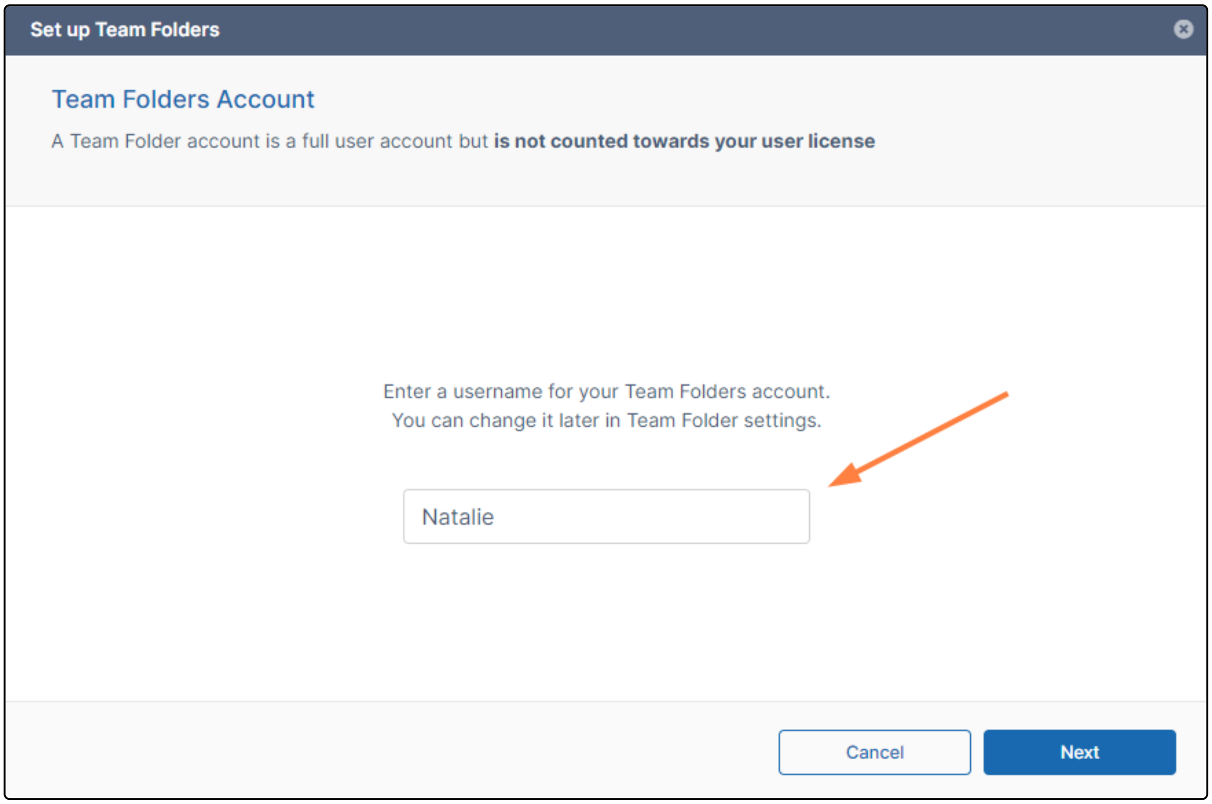


6. Now you are ready to create your Team Folders and fill them with contents. You can proceed from where you are by dragging and dropping folders onto the page or by clicking **Add Files and Folders**. This is a good option if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.
   If you already have a folder structure that you want to use, FileCloud Sync is the preferred method.
   For instructions on using these methods and others, see Seed and Organize Team Folder Data.

Convert an existing user account into the Team Folders account

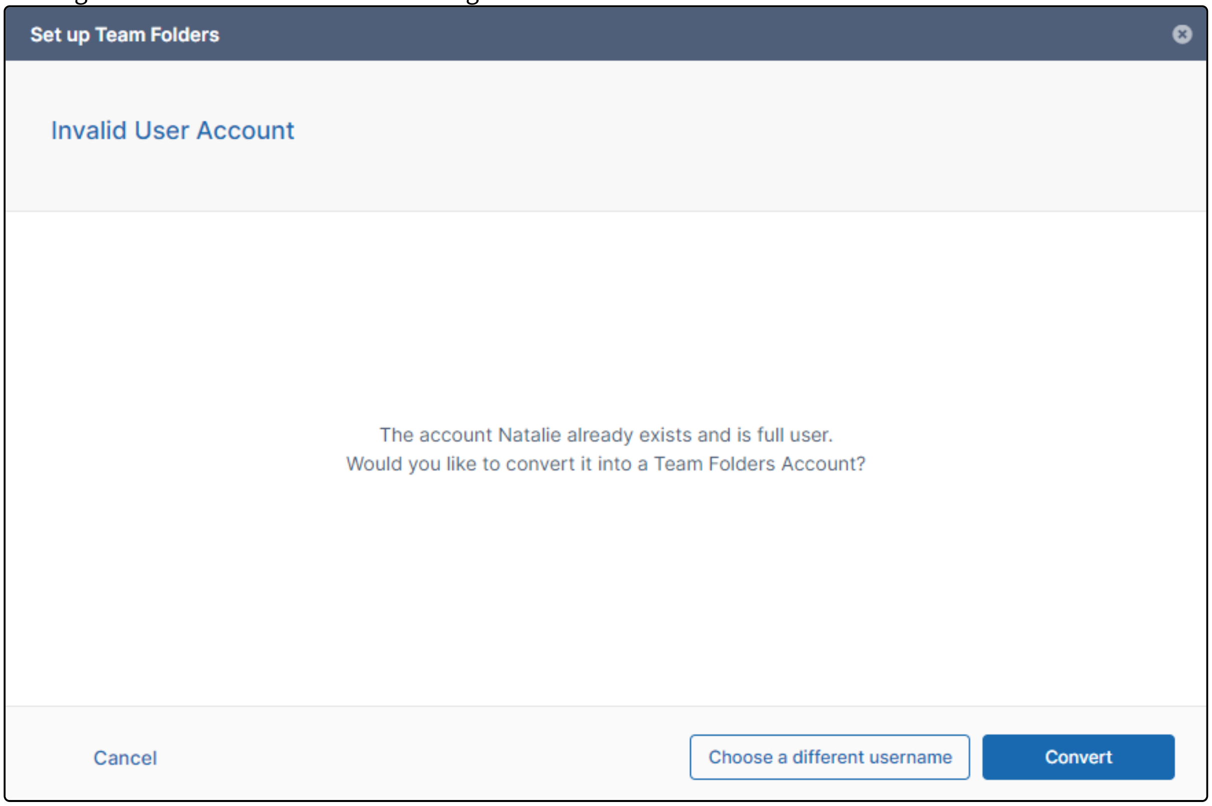
1. In the admin portal's navigation pane, click **Team Folders**.
   The screen tells you Team Folders is not set up, and it provides you with a **Set up Team Folders** button.
   

2. Click the **Set up Team Folders** button.
   A wizard for setting up Team Folders opens.
3. In the **Username** field, enter the username of the account that you want to convert into the Team Folder account.

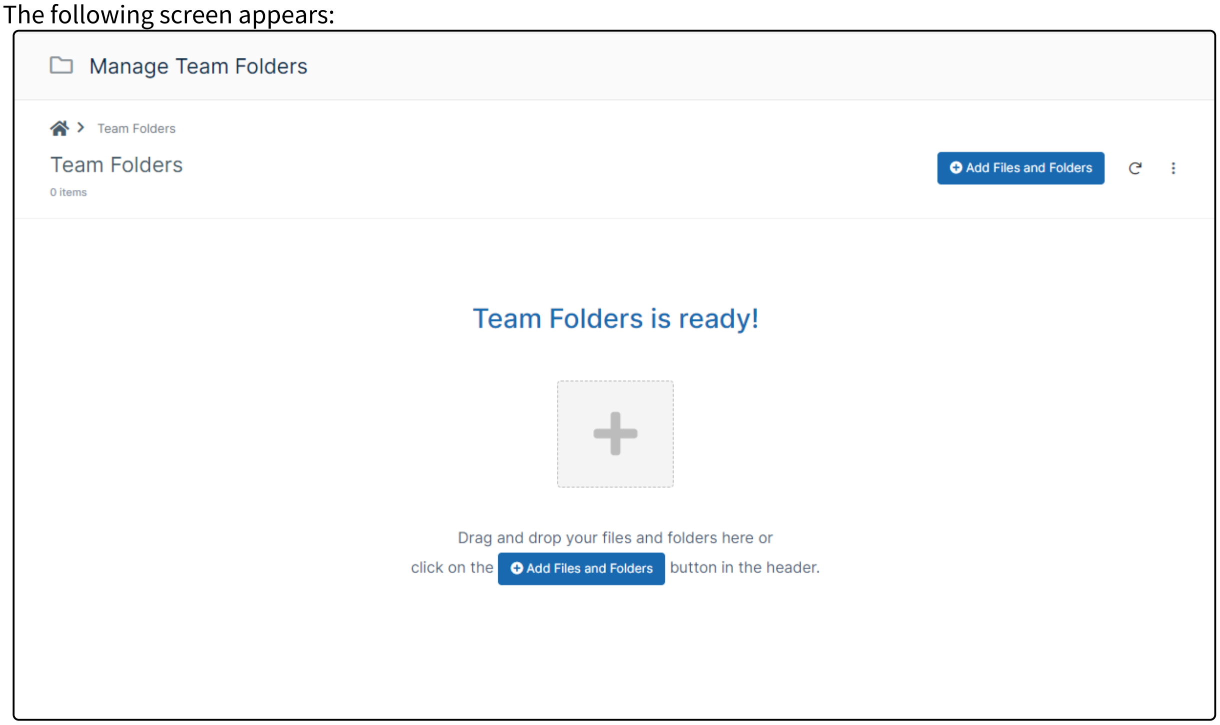


4. Click **Next**.
   The next window of the wizard indicates that the username already exists, and gives you the option of

entering a different username or converting this user:



5. Click **Convert**.
   The following screen appears:

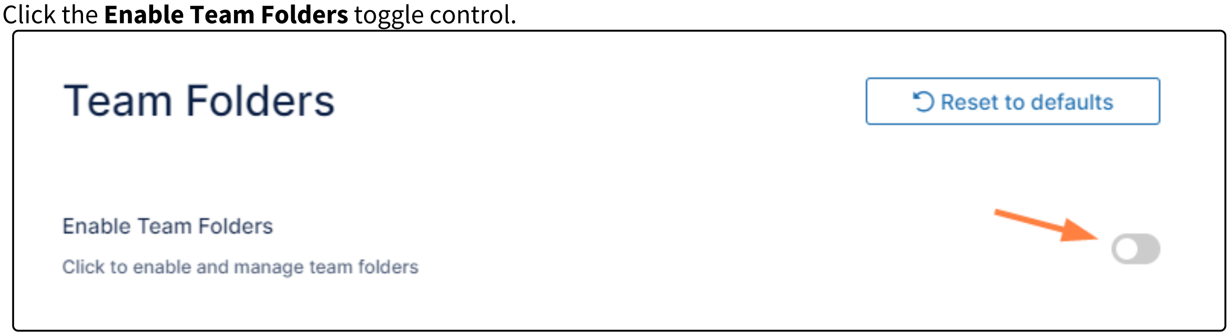


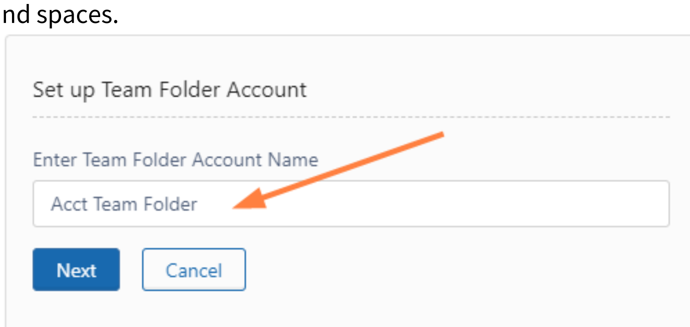
Now you are ready to create your Team Folders and fill them with contents. You can begin by dragging and dropping folders onto the page or clicking **Add Files and Folders**. These are good options if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.

If you already have a folder structure that you want to use, FileCloud Sync is the preferred method. For instructions on using these methods and others, see Seed and Organize Team Folder Data.

Create a new account through the Team Folders settings page

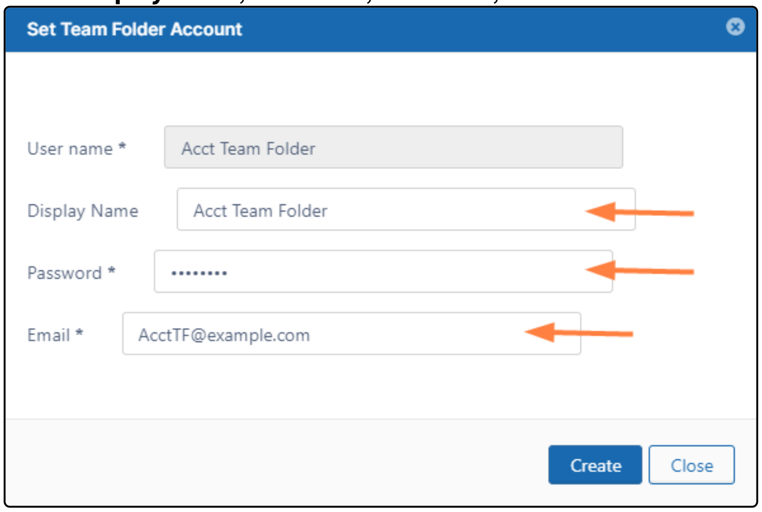
To enable team folders and create an account through Team Folders settings:

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

3. Click **Save.**
   The **Set up Team Folder Account** dialog box **opens.**
4. in **Enter Team Folder Account Name**, type in a unique name.
   The **Team Folder Account Name** can contain alphanumeric characters and underscores, periods, dashes and spaces.
   

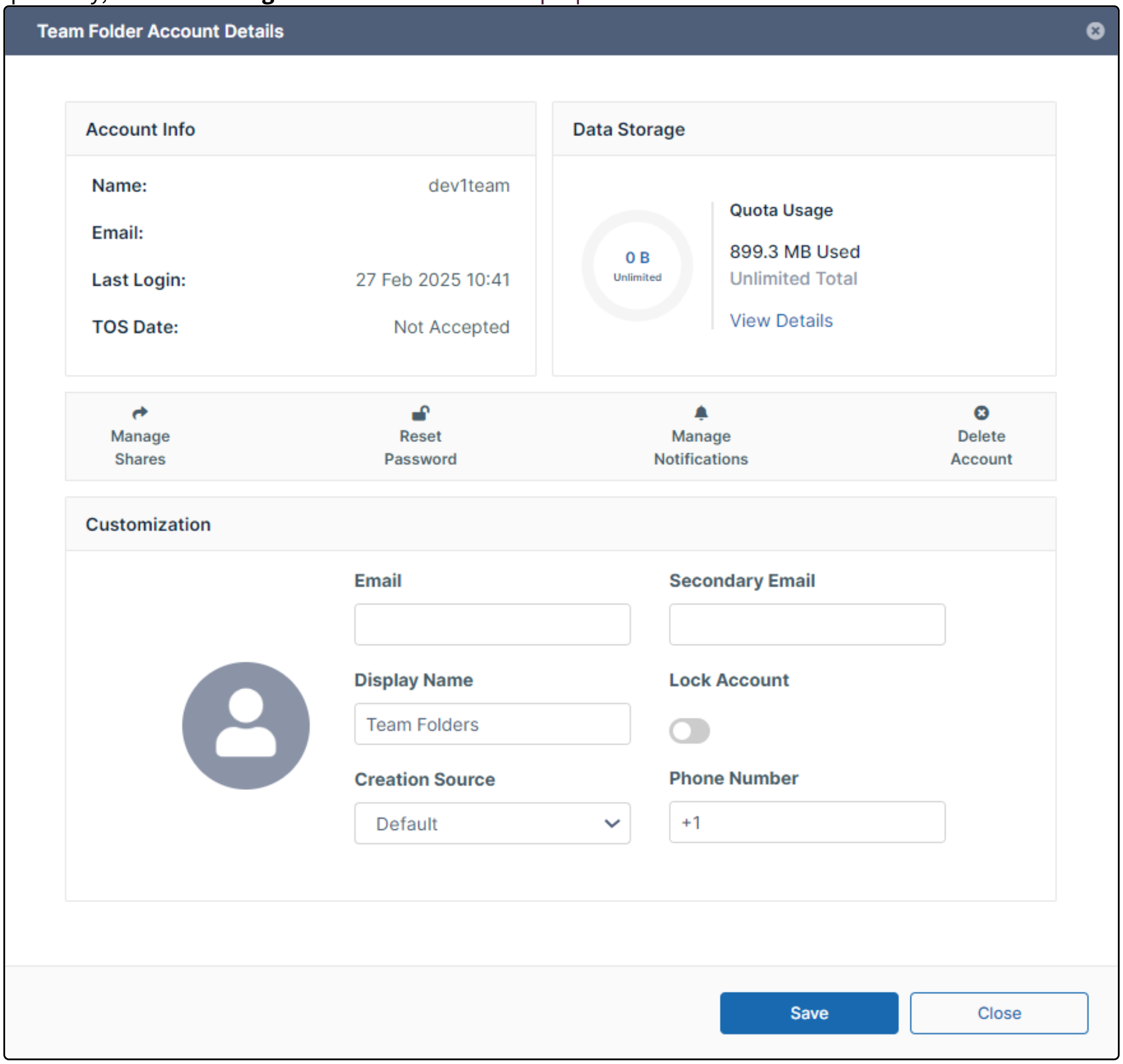
5. In the confirmation window, click **OK**.
   The **Set Team Folder Account** dialog box opens.

6. Enter a **Display Name**, **Password**, and **Email**, and click **Create**.



The Team Folder account is created and team folders are enabled.

Optionally, click the **Manage** button to set additional properties for the Team Folder account.



Action	Description
Manage Shares	View all the shares that are created under the Team Folder account.
Reset Password	Reset the password for the Team Folder account.
Manage Notifications	Edit notifications configured on the Team Folder account's file and folder paths.

Action	Description
Delete Account	Delete the Team Folder account. This will delete all the files and folders under the Team Folders.

Property Name	Property Description
Profile image	Image for the Team Folder account.
Email	Email address for the Team Folder account.
Secondary Email	Alternate email address.
Display Name	Display Name for Team Folders that appears in the user interface.
Lock Account	Automatically checked when too many login errors occur. Click to remove check and unlock account.
Creation Source	Where the Team Folder account was created. Options are: • Default (Admin user interface or import) • SSO (During SSO sign in)
Phone Number (added in FileCloud 20.1)	Used when logging in with 2FA.

Now you are ready to create your Team Folders and fill them with contents. You can go to the Team Folders screen and add the folders there. This is a good option if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.
If you already have a folder structure that you want to use, FileCloud Sync is the preferred method.
For instructions on using these methods and others, see Seed and Organize Team Folder Data.

Convert an existing account through the Team Folder settings

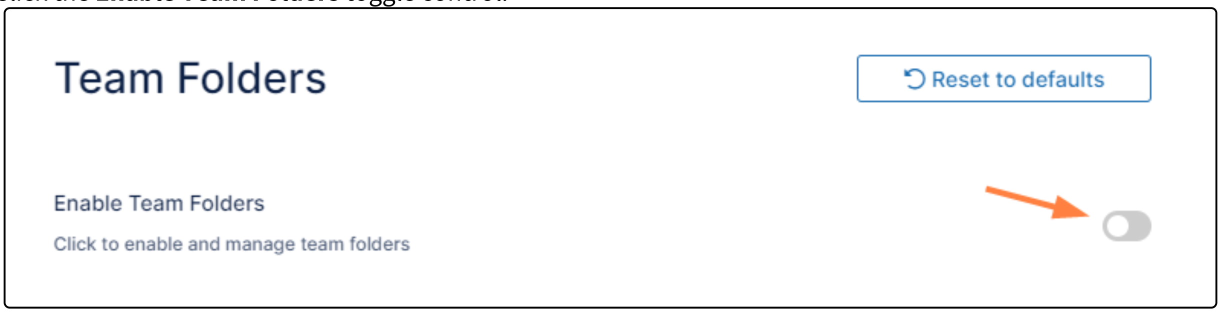
You can also create the Team Folder account by promoting a user account that is already in use for company-wide communication.

Promoting existing user accounts to team folders should be done only after understanding all the consequences of such an action.

- This can cause company-wide changes to Sync app users

- Promoting an existing account can potentially cause re-downloading of existing content

To move an existing user account to a Team Folder account:

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

3. Click **Save.**
   The **Set up Team Folder Account** dialog box **opens.**
4. Click the **Enable Team Folders** checkbox.
5. On the **Set up Team Folder Account** window, in **Enter Team Folder Account Name**, type in the existing full user account name you want to use.
6. On the **Set Team Folder Account** window, type in the existing **Password** and **Email** for the existing full user.
7. Click **Create**.
8. Have each user connecting with the Sync app, log out of Sync and restart it.
   If any files in the user account that was converted to the Team Folder account were originally shared with any Sync users, the shared data was synced previously to **Shared With Me**, but is now synced to **Team Folders** → ***foldername***.
   After all the data has been downloaded, delete the old folders in **Shared with Me**.

Seed and Organize Team Folder Data

When you log into the FileCloud user portal with the Team Folder account, the files that appear in the My Files folder are the Team Folders for your FileCloud system. You can create and seed Team Folders by logging into Sync, Drive, or the user portal as the Team Folder account and moving the folders that you want to become Team Folders into the Team Folder account's My Files folder. The recommended method is to log into the Sync client and sync the folders.

Alternately, as an admin, you can log into the admin portal, and manually create Team Folders.

Sync Client (Recommended)

Seeding Team Folder data with FileCloud Sync Client is both simple and quick. Follow these steps:

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Download and install the FileCloud Sync Client.
3. Log in to the Sync Client using the Team Folder account credentials created during the Team Folder Account Setup.
4. Open the My Files folder.
5. In file explorer, copy the folders created in Step 1 into My Files.

6. Wait for Sync to run automatically or click Sync Now.
   The folders are synced to My Files in your Team Folder Account. The folders become Team Folders for all other users.

Once the sync is complete, you can log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Note: Alternately, use the ServerSync Client instead of the Sync Client.

Drive Client

Team Folder data can be seeded using the Drive Client. The following steps must be followed to seed data using Drive Client.

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Download and install the FileCloud Drive Client.
3. Log in to the Drive Client using the Team Folder account credentials created during the Team Folder Account Setup.
4. Locate Drive in your file explorer, and copy the folders created in Step 1 into My Files.
   Drive will automatically detect the new folders and add them to My Files in your Team Folder Account. The folders become Team Folders for all other users.

Once the files and folders are copied, you can log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Open a browser and log in to the User Portal

The FileCloud web user interface can be used to seed and organize Team Folder data. The following steps must be followed to set up Team Folder data using the user portal.

1. First, create the Team Folders outside of FileCloud and copy the Team Folder data into them.
2. Using a web browser, go to the FileCloud user portal.
3. Log in using the Team Folder account credentials created during the Team Folder account set up.
4. Browse to My Files
5. Copy the folders that you created in Step 1 into My Files.
   These folders become Team Folders for all other users.

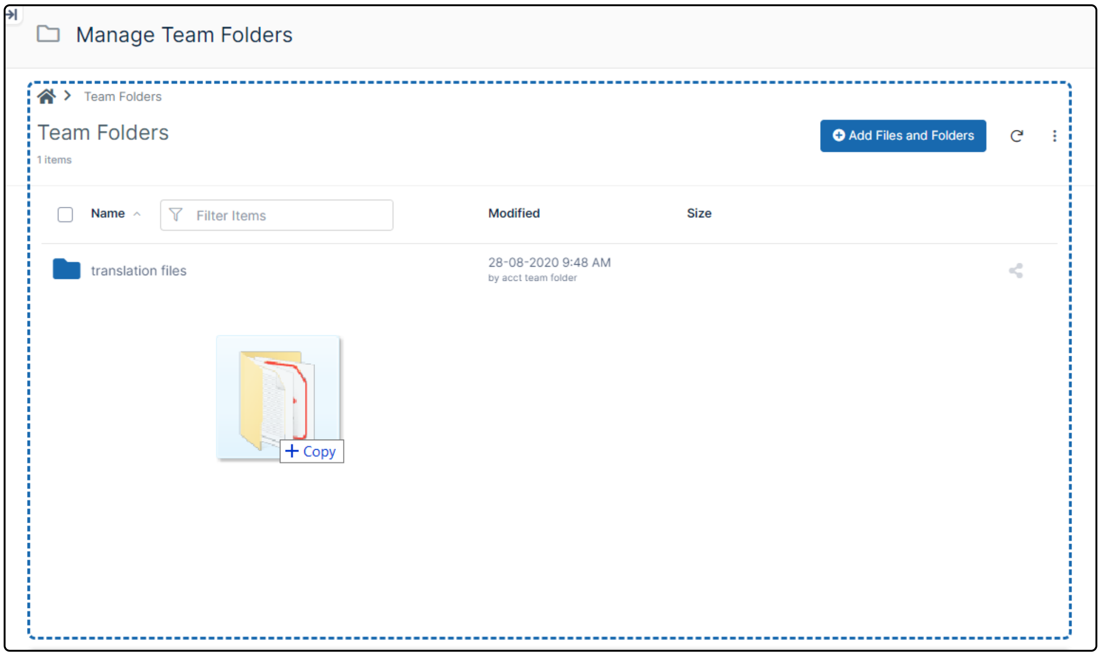
Now, log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Admin Portal

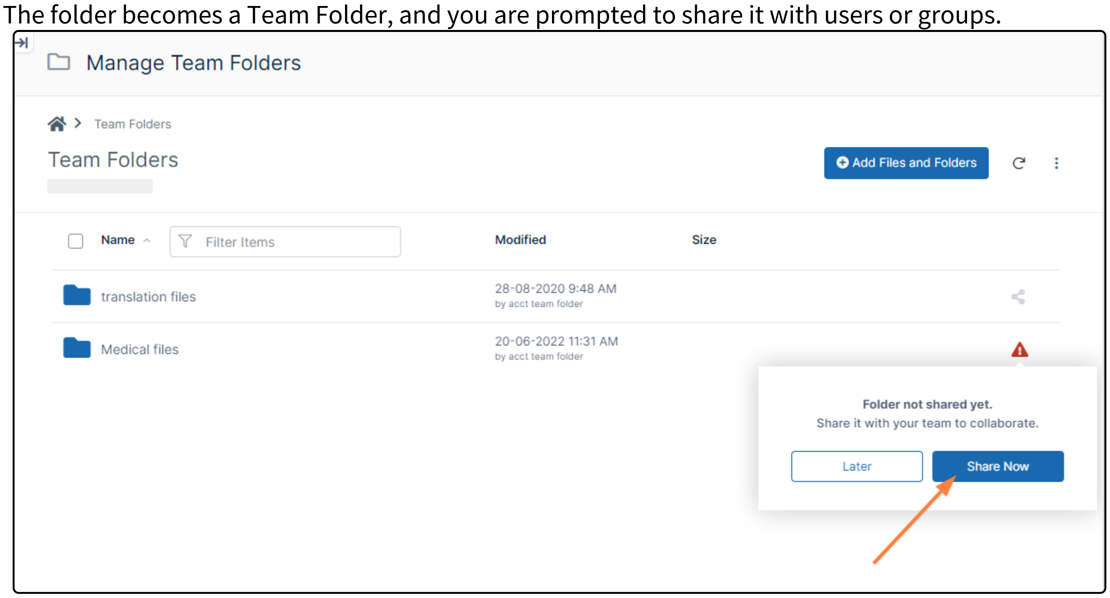
Go to the **Team Folders** page in the admin portal to create Team Folders and seed them with files.

1. Open a browser and log in to the admin portal.
2. Ensure the account that is used to log in has permissions to access Team Folders.
   The main admin account has automatic access to Team Folders. To set Team Folder access to additional admin accounts, see Managing Admin Users.
3. From the left navigation panel, click **Team Folders**.
4. Add Team Folders.
   Add Team Folders by dragging and dropping

a. Drag and drop an existing folder (with or without contents) from your file system onto the Team folders screen.



b. The folder becomes a Team Folder, and you are prompted to share it with users or groups.

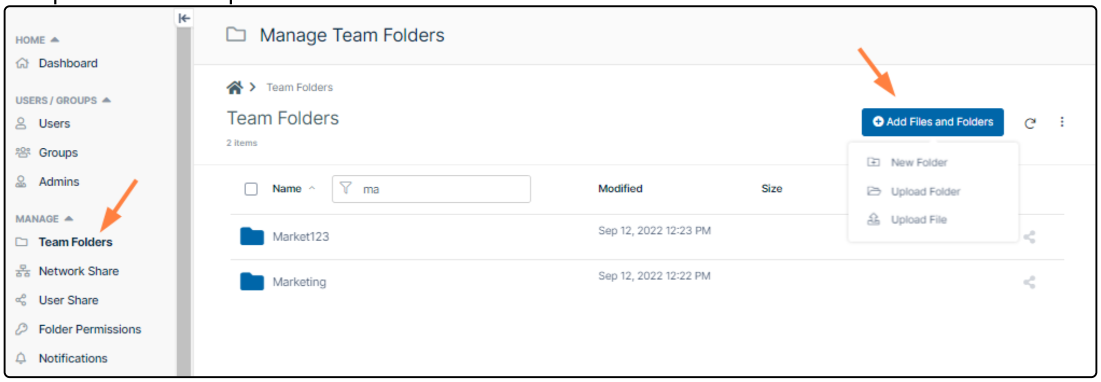


c. Click **Share Now** to share the Team Folder with users and/or groups.

d. To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

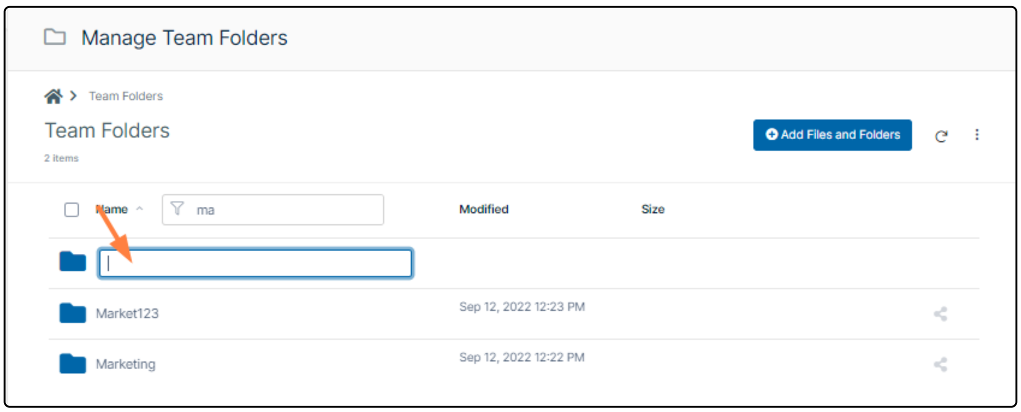
Add Team Folders by clicking the button

a. Click the **Add Files and Folders** button.
A drop-down menu opens.

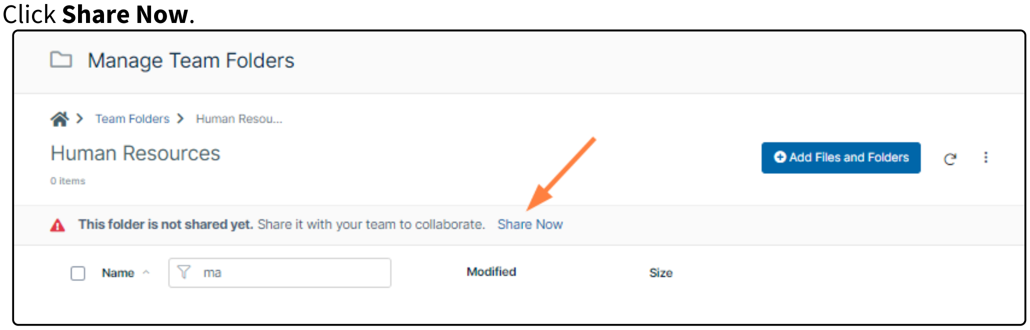


b. Either choose **New Folder** to create a new Team Folder, or click **Upload Folder** to upload an existing folder (with or without contents) and make it a Team Folder.
If you choose **New Folder:**

- A new folder appears in the list. Your cursor is positioned so that you may give the folder a name.



- Add a name and click Enter.
  The folder opens and displays a reminder to share the file.
- Click **Share Now**.

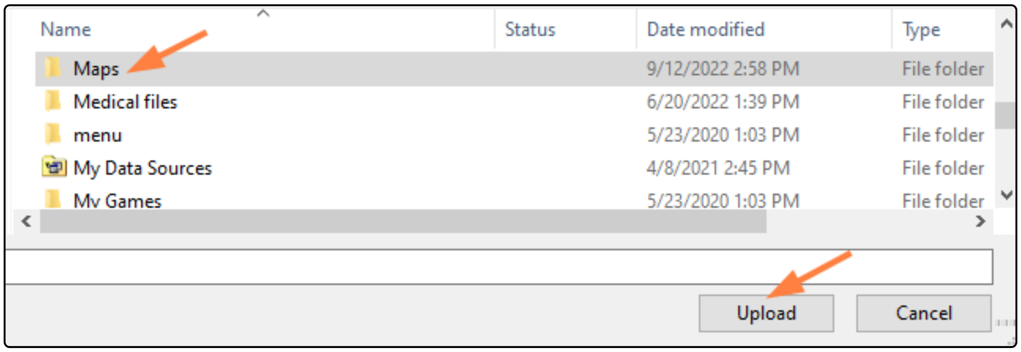


A share dialog box opens.

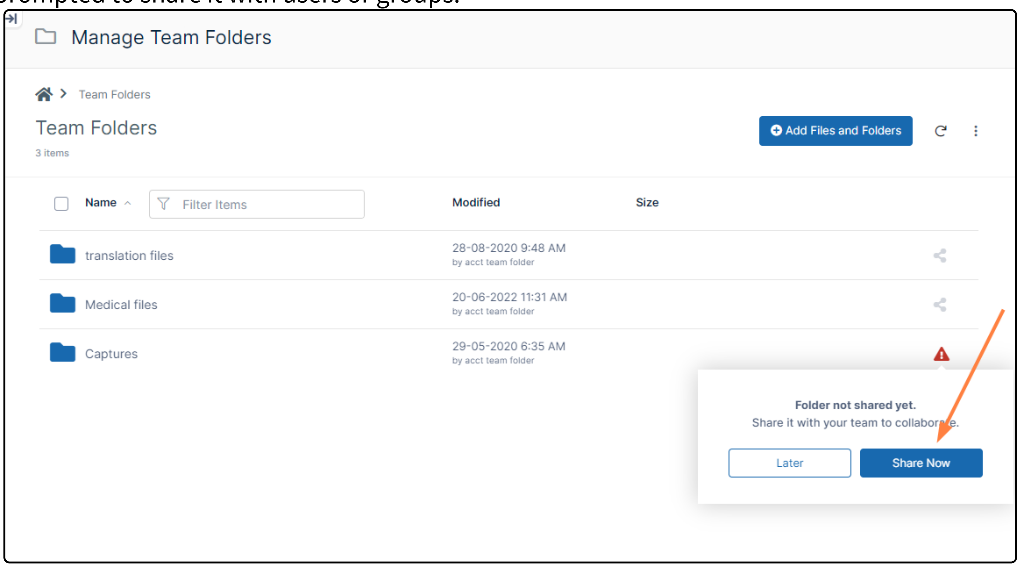
- To share the folder with users, see Share the Team Folder and Set Permissions.
- To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

If you choose **Upload Folder**, your file explorer opens.

- Select the folder to use as a Team Folder and upload it. Agree to upload the its files if prompted.



The folder and its contents are uploaded. The folder becomes a Team Folder, and you are prompted to share it with users or groups.



- Click **Share Now** to share the Team Folder with users and/or groups.
- To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

Share the Team Folder and Set Permissions

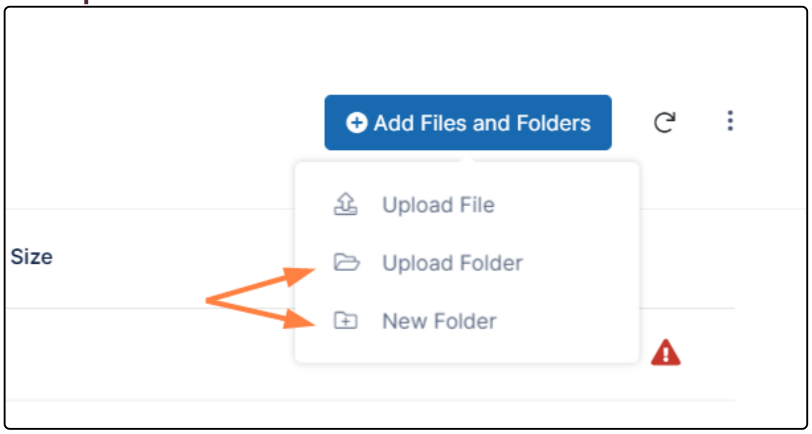
> Beginning with FileCloud 23.241, admins can share Team Folders with external users. Prior to FileCloud 23.232, they were unable to share Team Folders with external users.
>
> Beginning with FileCloud 23.1, by default, you can no longer share a top-level Team Folder publicly. To enable public sharing, please Contact FileCloud Support.

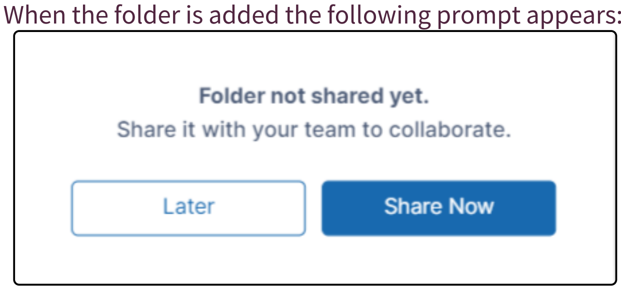
You must share Team Folders before users can access them.

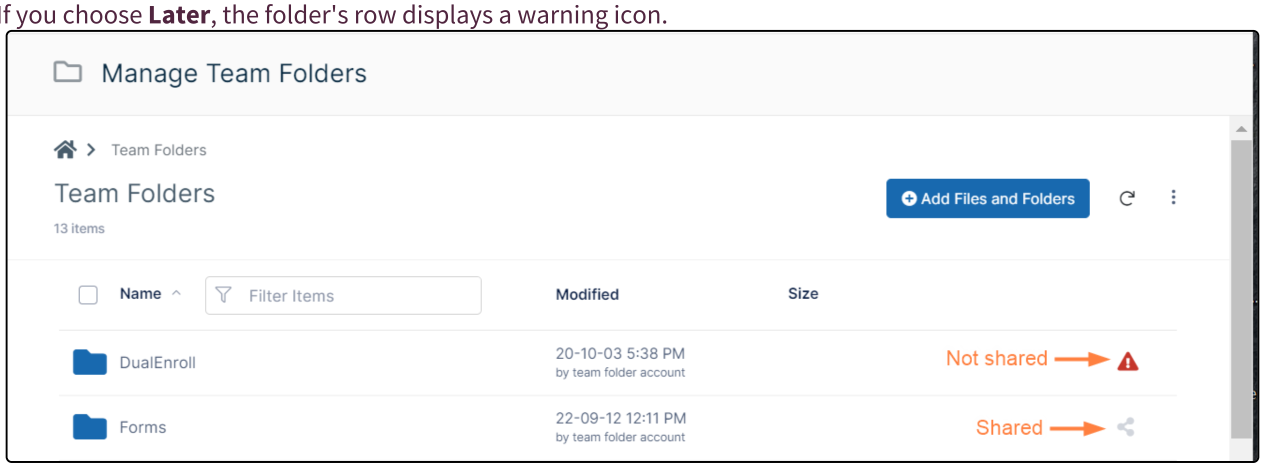
- Team folders that are not shared do not appear under any user's account and are not accessible.
- Team Folders are shared from the admin portal, and may be shared privately with specific groups or users.

You can share a Team Folder when you add it or at a later time.

To share a new Team Folder when adding it:

1. In the admin portal, click **Team Folders** in the navigation panel.
2. Drag and drop the folder onto the **Team Folders** screen or use the **Add Files and Folders** button and choose either **Upload Folder** or **New Folder**.


When the folder is added the following prompt appears:


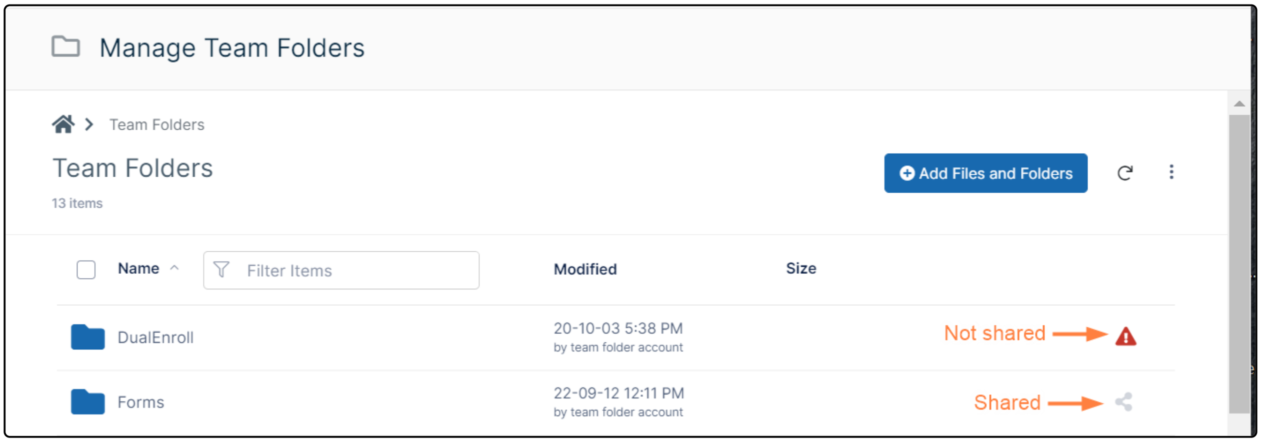
3. Click **Share Now**, to configure the share and share it with users now, or click **Later** to configure and share it at a later time.
If you choose **Later**, the folder's row displays a warning icon.


If you choose **Share Now** a **Share link for folder** dialog box opens.
4. To configure the share, see To complete the Team Folder share, below.

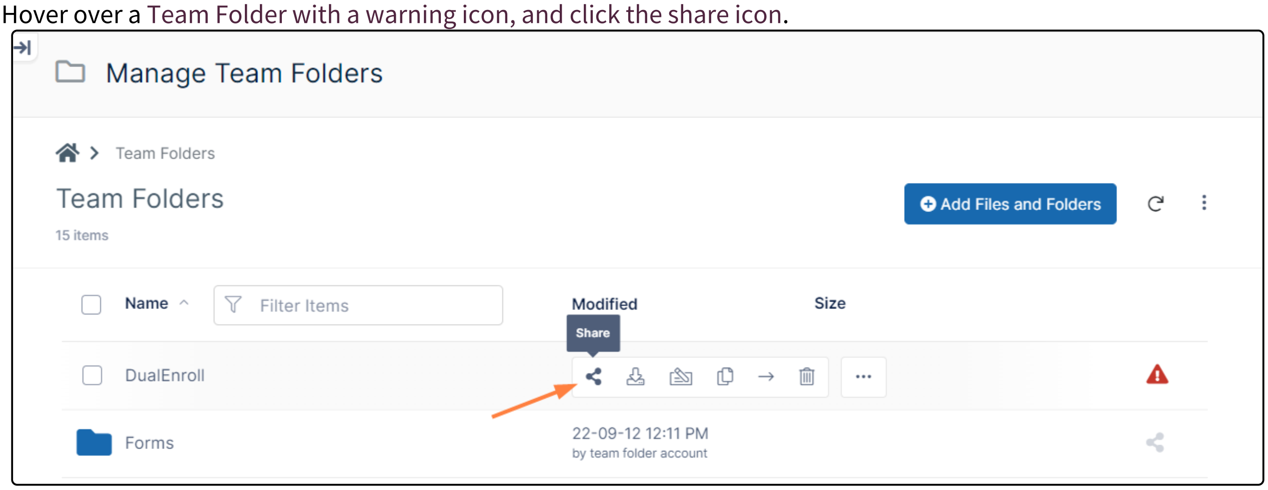
To share an existing Team Folder:

1. In the admin portal, click **Team Folders** in the navigation panel.

2. The row for a Team Folder displays a share icon if it has already been shared or a warning icon if it has not been shared.



3. Hover over a Team Folder with a warning icon, and click the share icon.

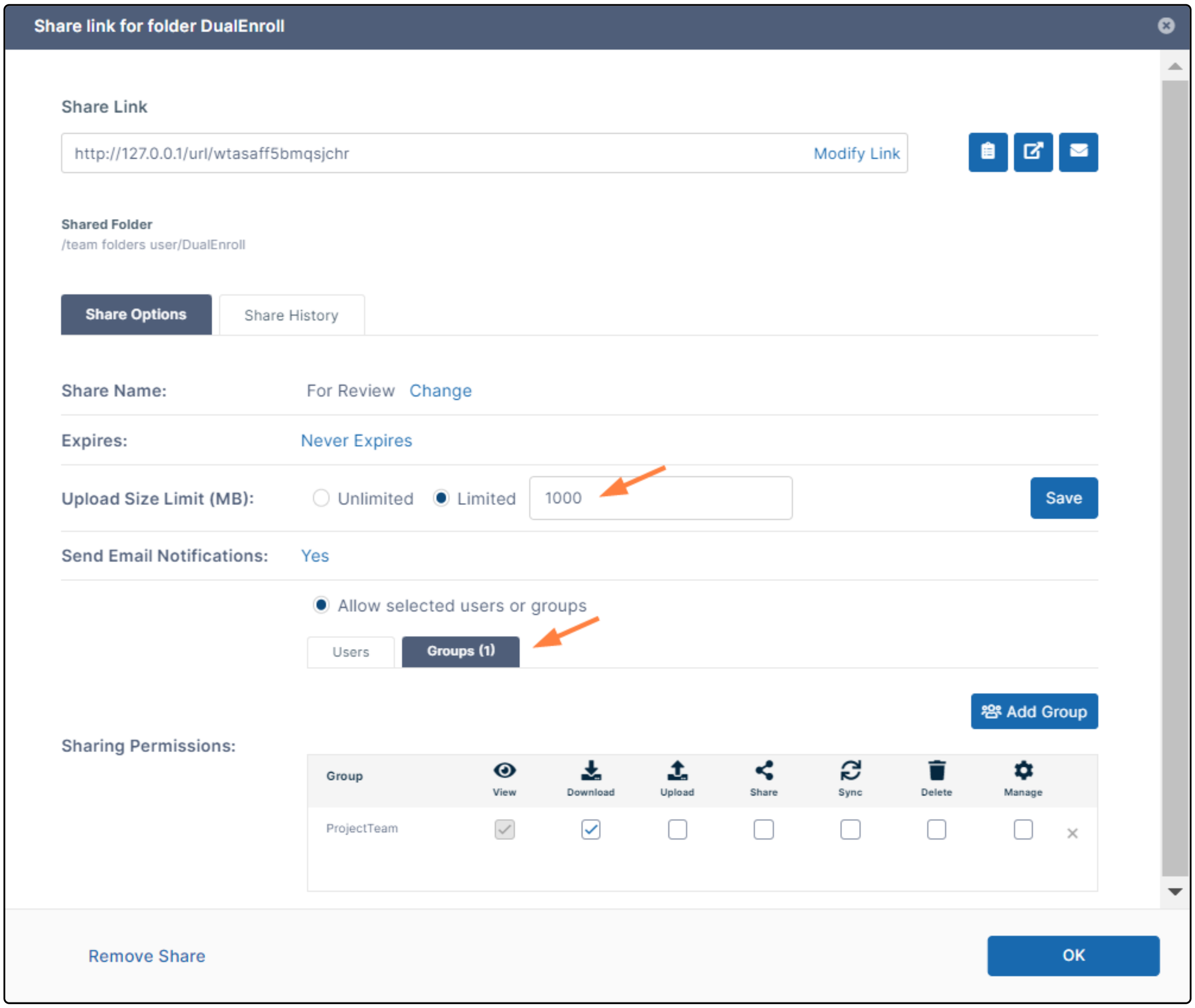


The **Share link for folder** dialog box opens.

4. To configure the share, see To complete the Team Folder share, below.

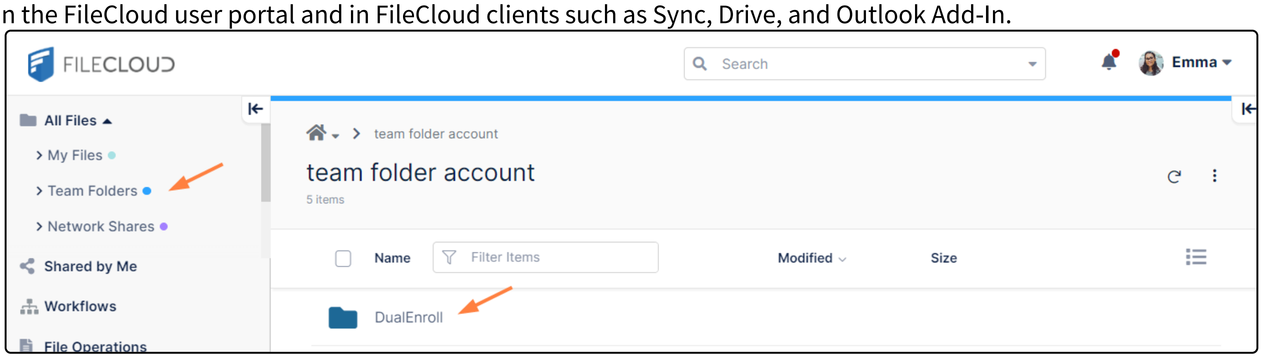
To complete the Team Folder share:

1. In the **Share link for folder** dialog box, configure the settings for the share.
For example, you may want to share the folder with a specific group only or limit the upload size.



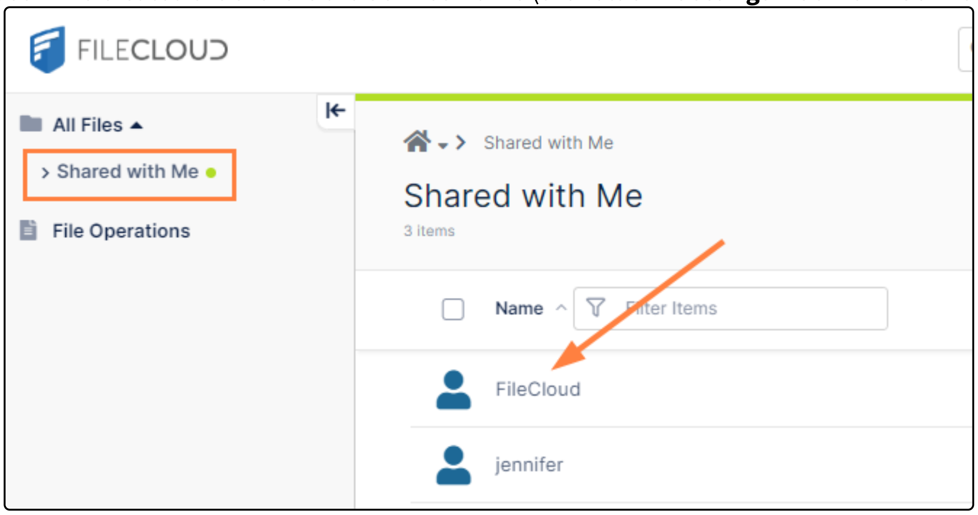
For information about share settings, see Share Options for Public and Private Folders.
For information about sharing permissions, see Public Share Permissions for Folders or Private Share Permissions for Folders.
Note: You cannot share a top-level Team Folder publicly,

Once the Team Folder is shared, it appears to all users that have access to it under Team Folders in their account in the FileCloud user portal and in FileCloud clients such as Sync, Drive, and Outlook Add-In.

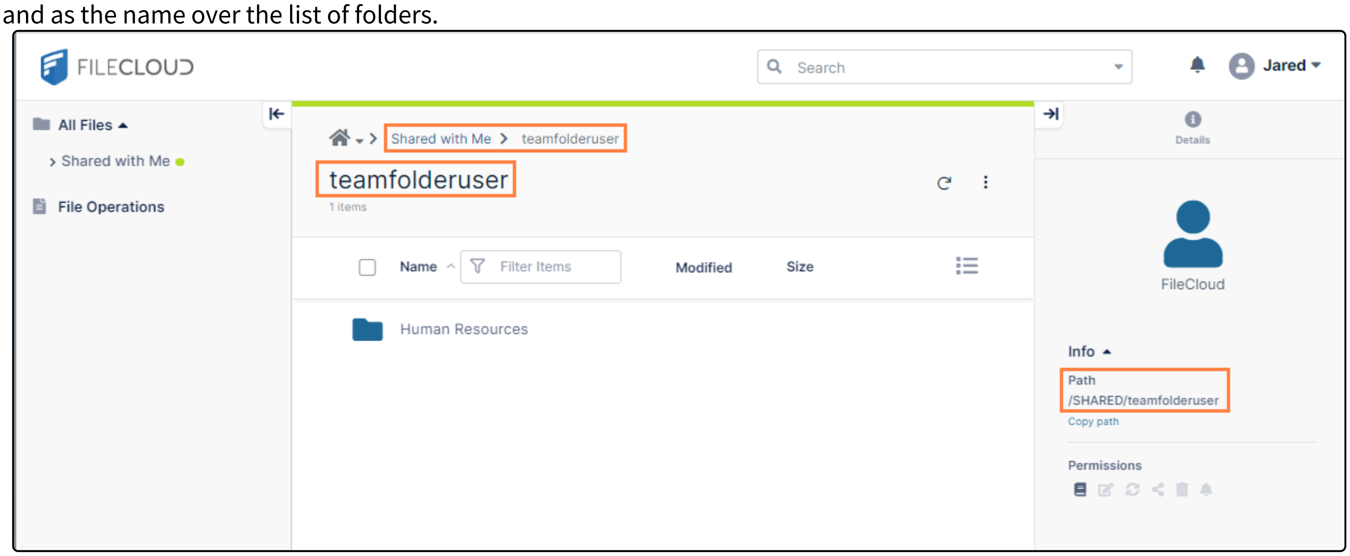


When you share a Team Folder with an external user

When you share a Team Folder with an external user, the folder appears under **Shared with Me**, and the name of the user who created the share is the **Service Name** (the value in **Settings > Server > Service Name**).

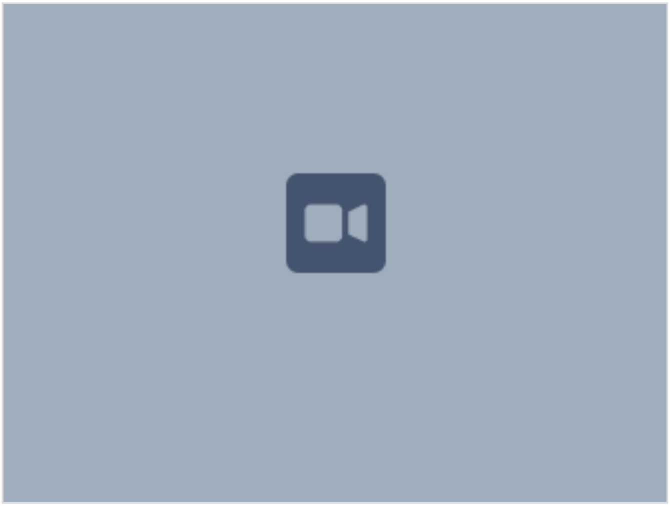


When the external user clicks the **Service Name** to access the share, the Team Folder username appears in path names and as the name over the list of folders.



If you rename a Team Folder

If you rename a folder, but do not change the name of the Team Folder share, users will continue to see the original Team Folder name. To help you remember to change the share name, FileCloud automatically asks you if you want to change the share name when you change a Team Folder name, as shown in the following video:



User Settings

Your FileCloud site provides your users with a place to store and share files.

- Every user of FileCloud needs a user account before they can store and access files
- You can configure user accounts to authenticate with the system you already have in place

Administrators cannot create users with the account names **admin** or **superadmin**.

Add User Accounts	Create or Import New Accounts Allow Users to Create Accounts
Configure User Authentication	User Authentication Settings Enabling Default Authentication Active Directory Authentication Connecting to AD via SSL Using Single Sign-On
Manage User Accounts	Migrate data after an account name change Changing the Storage Quota for Users User Session Expiration Restrict Commonly Used Passwords Customize the User Login Screen

Create FileCloud Users

You can control access to files stored in FileCloud by configuring permissions for user accounts.

- Every user who has access to FileCloud storage must have an account.
- Once a user account is created, it can be assigned different access levels.

In FileCloud version 20.1 and later, special characters from the extended UTF8 alphabet are supported in display names.
Beginning in FileCloud version 23.251, you can also import users when you import their groups from certain SSO providers. For instructions, see Group Settings.

Administrators cannot create users with the account names **admin** or **superadmin**.

In this section

User Access Levels and User Types

When you create a user, you assign it an access level.

There are four different access levels for users.

Level	Access	Notes
Admin Access	The default Admin has complete control over the FileCloud system. Other admin users have those admin permissions given to them.	The default Admin account is used to manage the FileCloud. The default admin user account is 'admin'. Other users can be marked as 'admins' and given limited set of permissions. Read more about Multiple Admins
Full Access	Control over its own private cloud storage space in My Files.	These user accounts can: • store files in their own private cloud storage space • view and download files stored in their storage space • view and download files shared with them by other users
Guest Access	Restricted access to the FileCloud system.	These user accounts: • Do not have private cloud storage • Can only view/upload/download files shared to them by other user accounts • Can re-share content if they have permissions

Level	Access	Notes
External Access	Access to FileCloud only through a Web browser.	These user accounts: • Can only view/upload/download content shared with them • Do not count towards the user license limit • Cannot be authenticated via AD and can only be local user accounts • Have external linked email accounts and cannot use the same domain as the FileCloud URL • Can't be added directly to network shares via the admin portal • Can access content from network folders if they are shared

- **Both Full and Guest users accounts are counted towards user accounts specified in the license.**
- **External Access accounts are NOT counted towards the license.**

User Types Comparison

User Access Feature	Full Access	Guest Access	External Access
User Portal (Web Browser) Access	Permitted Fully functional	Permitted Not all functions available	Permitted Not all Functions Available
View shared files	Permitted	Permitted	Permitted
---	---	---	---
Authentication	Local / ActiveDirectory	Local / ActiveDirectory	Local Only
Mobile App Access	Permitted Fully functional	Permitted Not all functions available	**Not Available**

User Access Feature	Full Access	Guest Access	External Access
Personal storage in FileCloud	Available	**Not Available**	**Not Available**
Share files with other users	Permitted	Permitted	**Not Available**
Access storage using Cloud Drive	Permitted	Permitted	**Not Available**
Sync storage using Cloud Sync	Permitted	Permitted	**Not Available**
SSO Login	Permitted	Permitted	**Not Available**
Group Membership	Can be member of any group	Can be member of any group	Can be member of any group except Everyone.
Admin Account	Can be Admin Account	Can be Admin Account	Cannot be an Admin Account
Team Folders	Permitted	Permitted	Permitted
Automation App	Permitted	Permitted	**Not Available**
File and Folder Comments	Permitted	Permitted	**Not Available**
2FA	Permitted	Permitted	Available by license beginning in Version 20.2 for Enterprise Advanced customers.

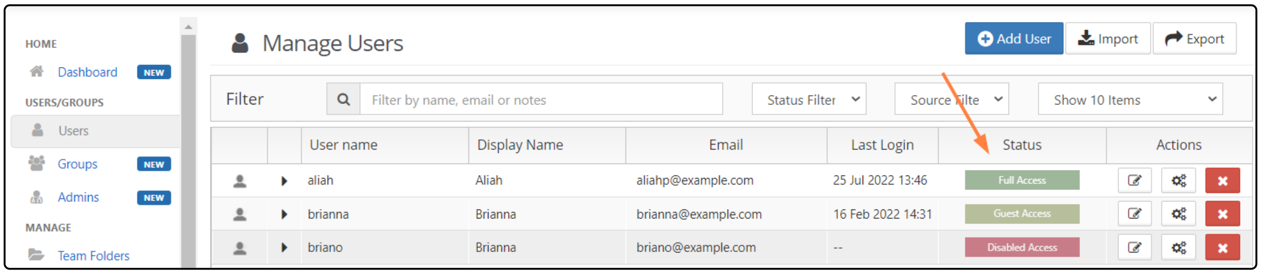
Checking User Access Level

The access level of any user account can be checked by the Administrator using the admin portal.

To check a user's access level:

1. Log on to Administration Portal.
2. Click **Manage Users** in the navigation panel.
3. In **Filter**, enter the name or the email of user

4. The **Access** for the user will be listed in the **Status** column.

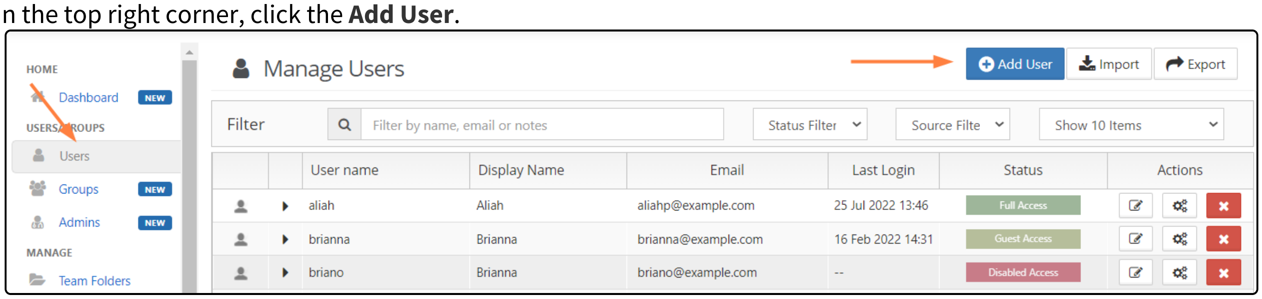


Manually Create a New User Account

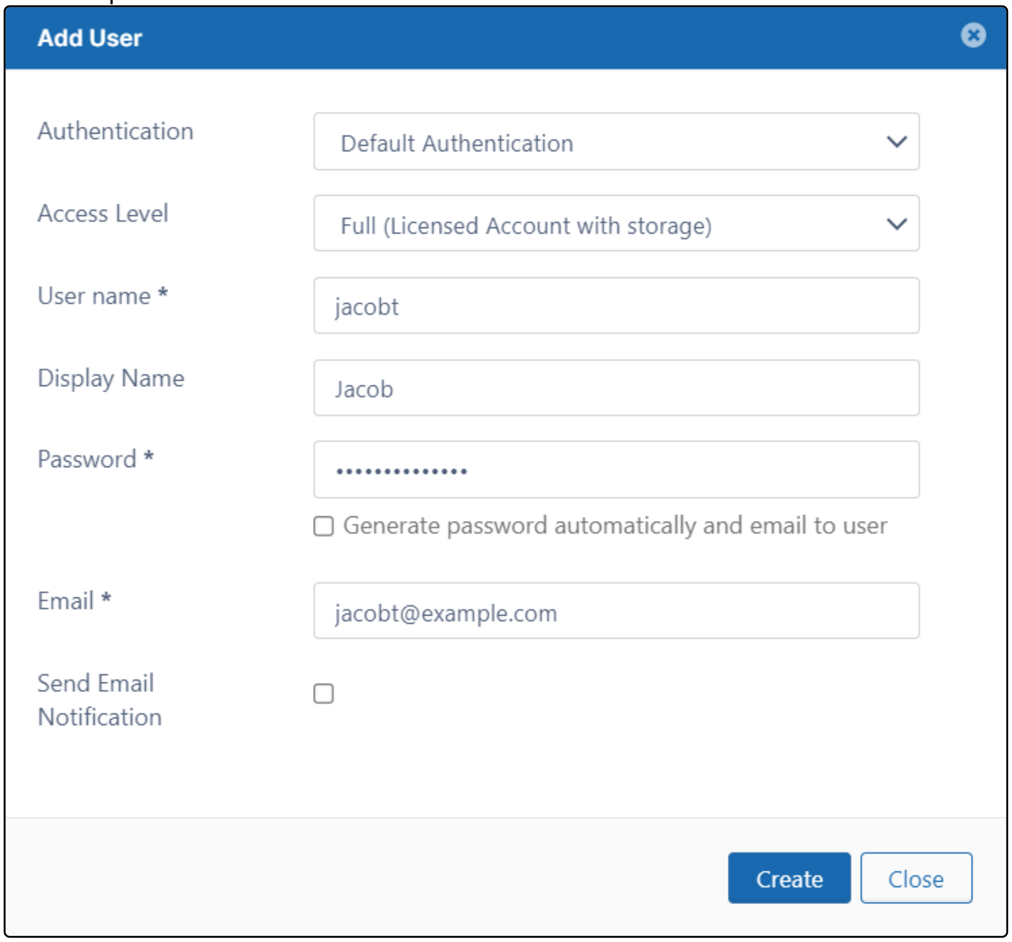
> The default user storage quota for every new user is set in Managed Storage. See Setting up Managed Disk Storage

To create a FileCloud user with default authentication:

1. Log on to Admin Portal.
2. In the left navigation panel, click **Users.**
3. In the top right corner, click the **Add User**.



4. Set the required account information.



Settings	Description
Authentication	Allows you to select the authentication type for granting access into the system. • Default Authentication **-** creates a local user account. User credentials are stored and authenticated within FileCloud. • LDAP or AD Authentication **-** creates an external user account. User credentials are stored and authenticated from an external LDAP or AD server.
Access Level	Allows you to select the user type. A user account with Full or Guest access counts as a license.
User name	Name to be used to log into the system. By default, **User name** can only contain numbers, spaces, hyphens, periods, underscores, and letters from the Latin alphabet (A-Z, uppercase and lowercase), and email addresses may not be used as usernames. **Note**: To also enable use of apostrophes in the **User name**, go to **Settings > Admin** and check **Allow Email as Username**.

Settings	Description
Display name	Name that appears on user interface
Password	Password for the user (Should adhere to password length and strength requirements for your organization). Either enter a password here, or check the following box.
Generate password automatically and email to user	FileCloud generates a password according to your settings for password limitations and emails it to the user. Anything entered into the **Password** field is ignored.
Email	An email id that is unique in the FileCloud system
Send Email Notification	When checked, a welcome email is sent to the new user. Unchecked by default. Beginning with FileCloud 20.1, if you uncheck this, you can send a welcome email with a newly generated password later. See Send Email from User Details.
Include Password in Email	When checked, the new user's password is included in the welcome email. Checked by default. Beginning with FileCloud 20.1, if you uncheck this, you can send a welcome email with a newly generated password later. See Send Email from User Details.

5. Click **Create**.

Bulk creation of User Accounts from a CSV File

You can create multiple accounts at one time using a CSV file.

Format of CSV file for creating user

To import from a CSV, create a simple text file with the all the user account information. The format of the created file is explained below:

CSV import format

```
UserName, EmailID, Password, DisplayName, Status, ExpirationDate, Groups, EmailVerified
```

Field	Description
UserName	The user id.

Field	Description
EmailID	A unique email id to be associated with the user.
Password	Password for the user. Must follow password requirements (minimum length, etc.)
DisplayName (optional)	The name that appears in the user interface for the user. Default is same as UserName.
Status (optional)	The user's account type (access level). Options are Guest|Full|External. Default is Full.
ExpirationDate (optional)	The date the user account will expire. Default is none.
Groups (optional)	The group or groups the user belongs to. If there are multiple groups, separate them with the | character. Default is none. All users other than External users are automatically placed into the **Everyone** group. External users are automatically placed into the **Externals** group. **Note**: FileCloud can only recognize group names if you do not insert spaces between the group names and the | characters: • Valid: **GROUP 1|GROUP 2** • Invalid: **GROUP 1 | GROUP 2**
EmailVerified (optional)	Whether or not the user can initially log in without administrator approval after the account is created. YES - Email is verified, so user can log in without account approval. Default. NO - Email is not verified, so administrator must approve account before user can log in. Administrator approval is only required for the initial login.

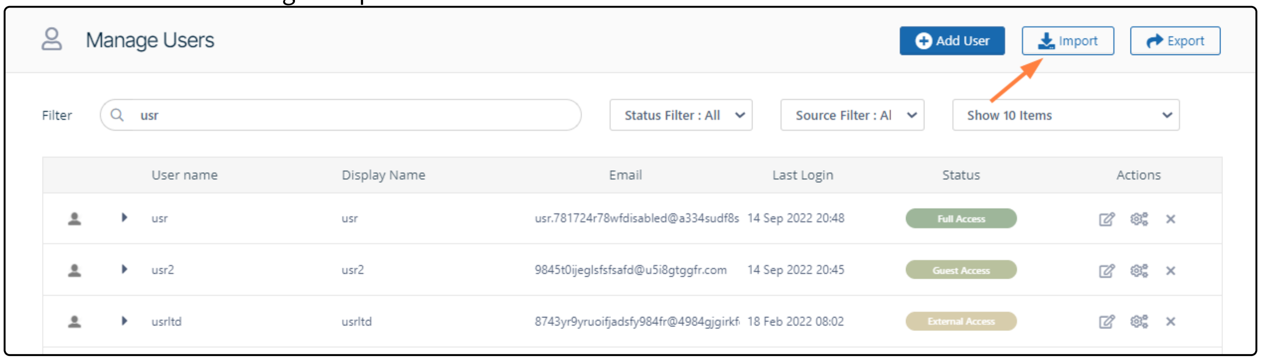
Below is a sample csv file for import.

1	UserName	EmailID	Password	DisplayName	Status	Expiration	Groups	EmailVerified
2	nick	nick@mycompany.com	[illegible]	Nick	FULL			NO
3	joe	joe@mycompany.com	[illegible]	Joe	FULL		Accounting|Human Reso	YES
4	lisa	lisa@lisat.com	[illegible]	Lisa	EXTERNAL			YES
5	demozzz	demozzz@mycompany.c	[illegible]	demozzz	DISABLED		Accounting	YES
6								

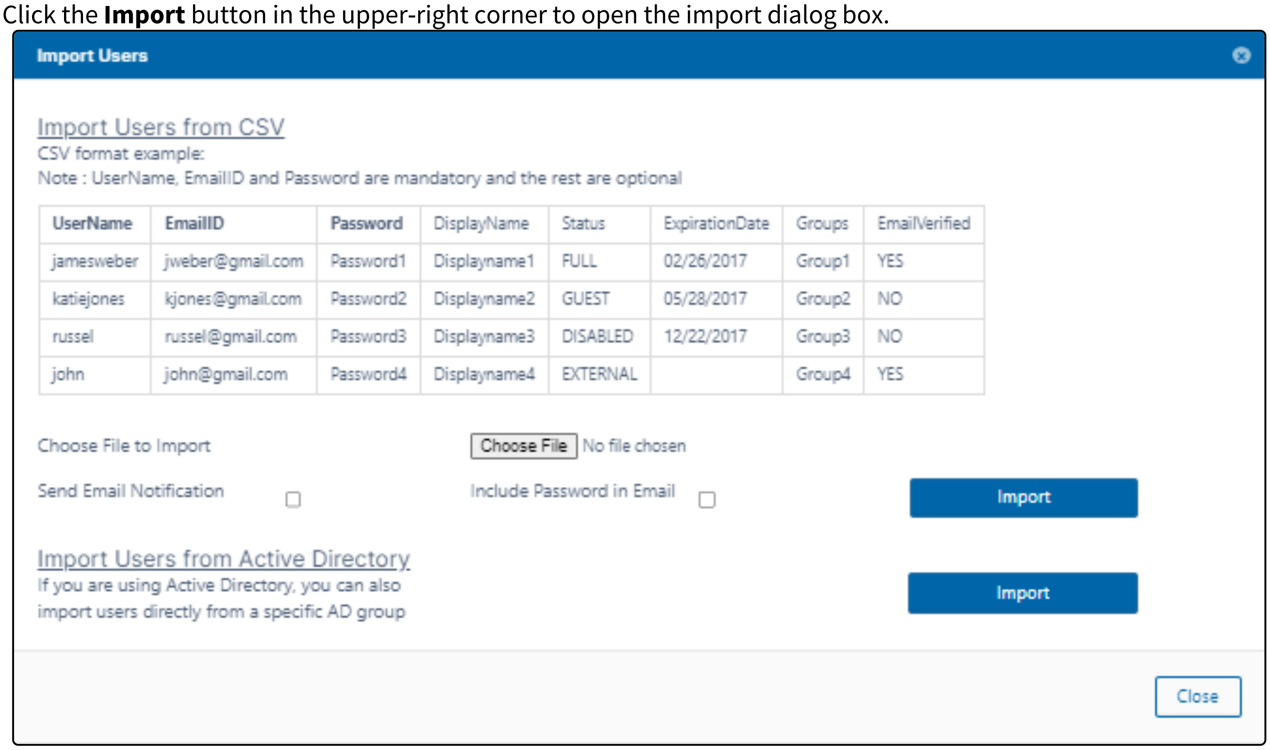
Importing a CSV File

To import a CSV File:

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



3. Click the **Import** button in the upper-right corner to open the import dialog box.



4. Click **Choose File**, and select the CSV file containing the entries of users to be created.
5. To send a notification to each user imported, check **Send Email Notification**. (*Added in FileCloud 20.1)*
   - To include each user's password in the email, check **Include Password in Email**.
6. Click **Import.**
   When the process is complete, a report is generated indicating the status of each user account creation.

Note: To export a CSV file of the users in your system, click the **Export** button.

The fields exported are the same as the imported fields with the addition of the fields **DisableNotifications**,

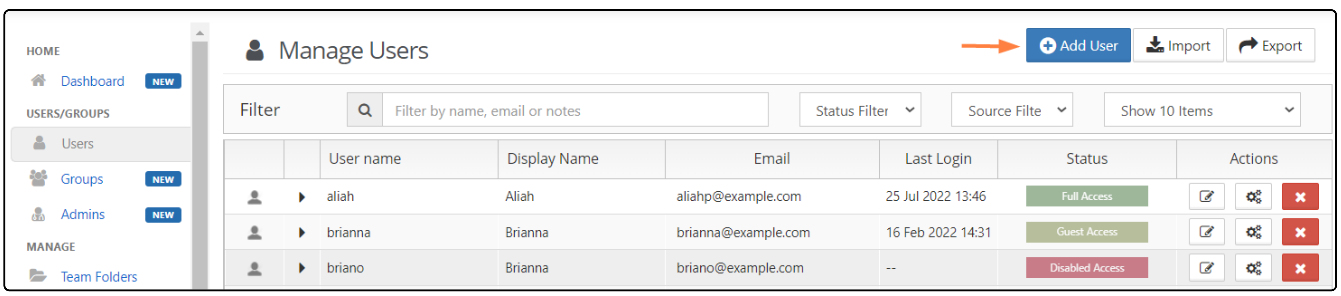
LastLogin, **Authentication Type**, **MobilePhone,** and **Effective Policy**.
Notice that the **Password** value is not exported.

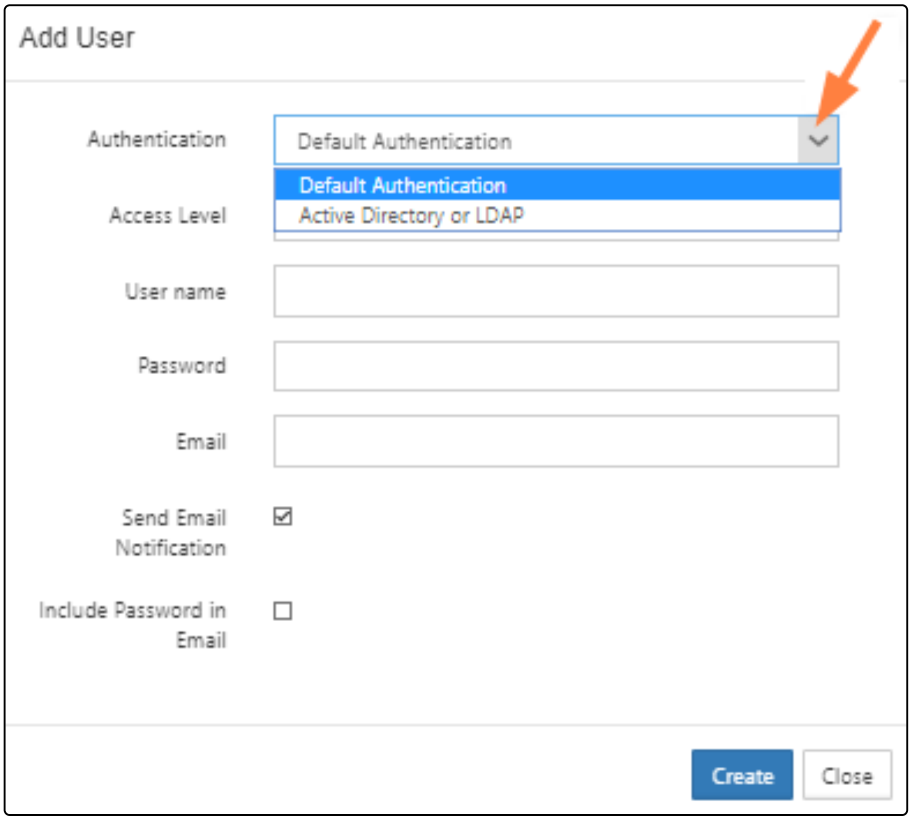
UserName	EmailID	Password	DisplayNa	Status	Expiration	Groups	EmailVerif	DisableNo	LastLogin	Authentica	MobilePhc	Effective Policy
gaby	gabrielle_95@exampl		Gaby	FULL		EVERYONE	YES	NO	11/28/2022 14:28	Default		Global Default Policy
keira	keira@example.com		Keira	FULL		EVERYONE	YES	NO		Default		Global Default Policy
brianna	brianna@example.co		Brianna	GUEST		EVERYONE	YES	NO	9/16/2022 9:54	Default	1.44E+10	Global Default Policy
laurel	laurel@example.com		Laurel	FULL		EVERYONE	YES	NO		Default		Global Default Policy
marion	marion@example.co		Marion	FULL		EVERYONE	YES	NO	3/11/2022 12:02	Default		Global Default Policy
briano	briano@example.con		Brianna	DISABLED		EVERYONE	YES	NO		Default		Global Default Policy

Import a user account from AD or LDAP Service

1. Log on to Administration Portal.
2. Set up AD configuration or LDAP configuration depending on your requirements.
3. Click **Users** on the left navigation panel.
4. Click **Add User** button.
5. Select **Active Directory or LDAP** as the authentication type.
6. Set the required account information as shown and click save.

Settings	Description
Authentication	Set to **Active Directory or LDAP**
AD/LDAP User name	AD/LDAP User name to import
AD/LDAP Password	AD/LDAP User name's Password
Email	Disabled: This will be imported from AD/LDAP service





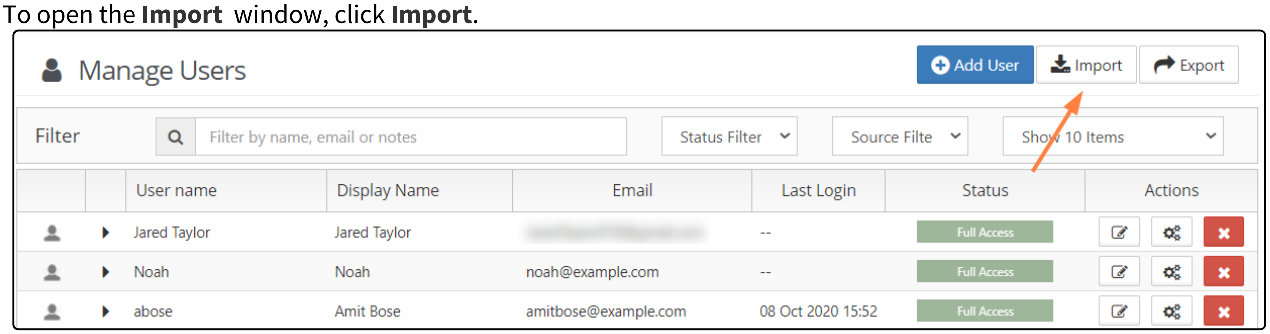
Bulk Import User Accounts from AD Server

As an administrator, you can create FileCloud user accounts by importing existing accounts from an AD group in your existing AD server.

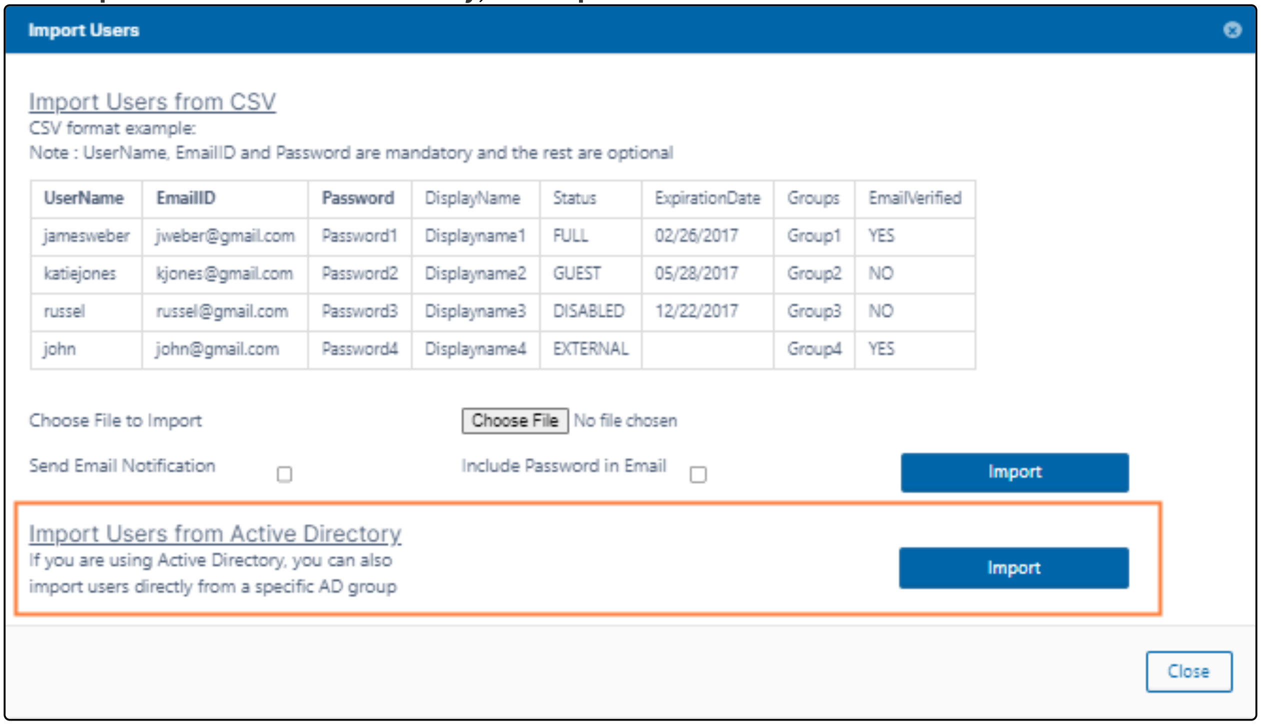
Import users from an AD Server

To import users from an AD server:

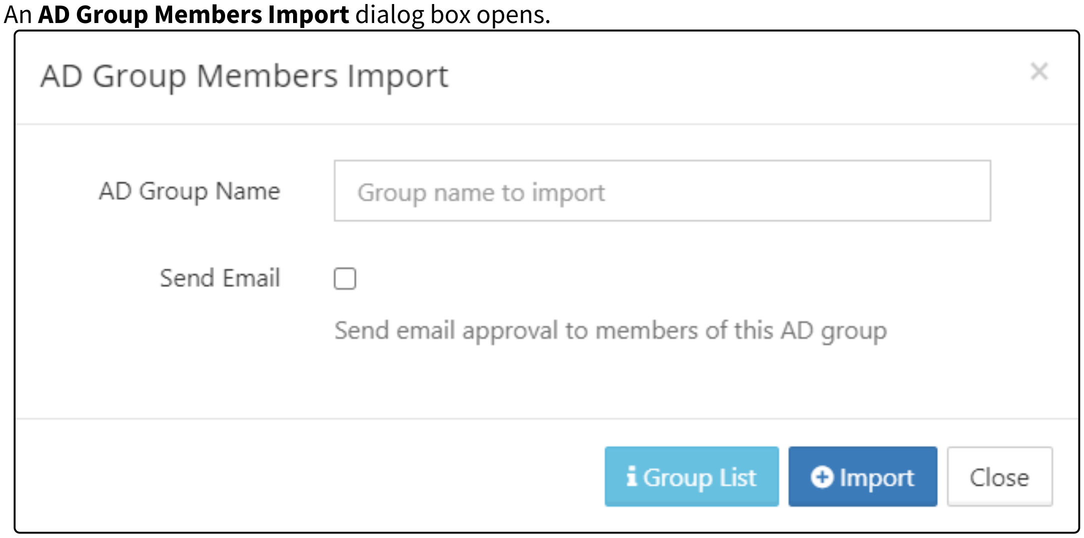
1. Open a browser and log on to Admin Portal.
2. Setup AD configuration or LDAP configuration depending on your requirements.
3. From the left navigation panel, under USERS/GROUPS, click **Users**.
4. To open the **Import** window, click **Import**.



5. Under **Import Users from Active Directory**, click **Import**.



An **AD Group Members Import** dialog box opens.



6. Type in the **AD Group Name**. A list of existing groups can also be viewed by clicking the **Group List** button.
7. To send an email to notify each user after their account is approve, check **Send Email**.
8. Click the **Import** button.

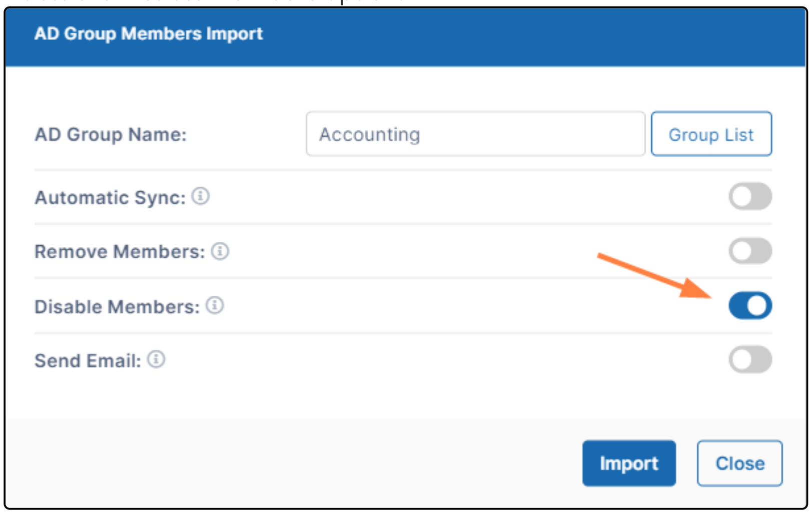
Import Disabled Users from Active Directory as Disabled

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

To use this option:

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

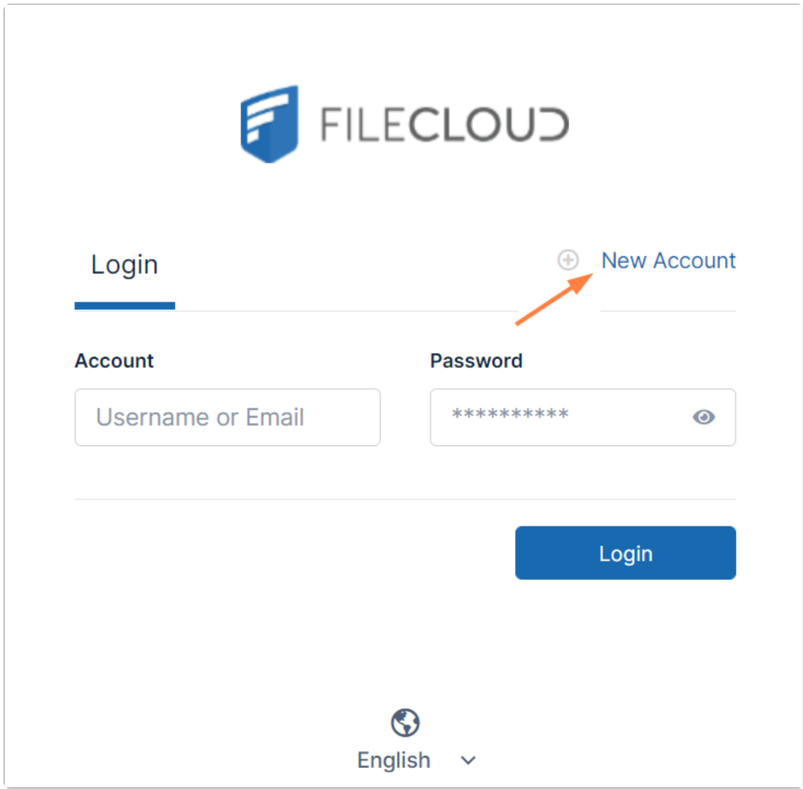
2. In then navigation panel, click **Groups**.
3. Select the **group** that you want to add users to, and then click the Edit icon.
4. On the **Members** tab, click **Import Users from AD Group**.
5. In **AD Group Name**, enter the AD group to import.
6. Enable the **Disable Members** option.



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

New Account Creation

By default, a **New Account** button appears on the log-in page that users can click to create or sign up for a new account.



Administrators can customize how new user accounts are created.

> If you are enabling FileCloud users to create new accounts when sharing with external individuals, and SMS 2FA is enabled, you must add a setting that allows the user to enter the individual's phone number with the share. To add the setting, see the section **Enable Two Factor Authentication for User Portal (Global setting)** in Two-Factor Authentication.

Who can create and approve accounts

New account settings

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed • Local users (who are not using AD or LDAP authentication) cannot create their own accounts.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		True = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

Scenarios

FileCloud supports the ability to customize the creation of user accounts in the following ways:

- Only an Administrator can create new user accounts.
- Users can create their own account but it is disabled. An administrator approves it or denies approval by deleting it.
- Users can create and approve their own accounts.
  - With a default level of access set by an administrator.
  - When Share invitations are sent to new users.
  - AD or LDAP users can create a new FileCloud account different from their AD or LDAP credentials.

Table 2. Only an Admin Creates New Accounts

Only an Admin can create (or deny) User accounts
1. The administrator enables the account in the Admin Portal on the Users page by changing the user's status from **Disabled Access** to one of the enabled access statuses. 2. The user receives a Welcome email with the account credentials and user portal URL. Note: An administrator denies approval by deleting a user account. In this case the user receives an email to inform them that the account has not been approved.
Customization settings, Login tab New Account button = DISABLED **Admin settings** Allow Account Signups = False Automatic Account Approval = No automatic approval. Admin has to approve account.

The scenarios where a user can create a new FileCloud account are described in Table 3.

Table 3. Users Can Create New Accounts

Users can create their own accounts

Users can create their own accounts The Admin must approve the accounts This scenario can also be used to allow new users to create an account when a Share invitation is sent.	Users can create their own accounts Users can approve their own accounts This scenario can also be used to allow new users to create an account when a Share invitation is sent.	Active Directory or LDAP Users create a new FileCloud account different from their AD or LDAP credentials The Admin can configure the approval process

⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The Administrator configures the User Search Mode. 2. The Administrator configures New Account Creation settings. 3. The Administrator provides the user with the URL for the User Portal OR an invitation to create a new account is sent when a user shares a folder or file. 4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the user portal login window, the user clicks the New Account button. 6. The user enters details in the account creation fields. 7. The account is created but is disabled by default. 8. The Admin will be notified about the new account. 9. The Admin will approve the account. 10. The Admin will set the user account type to Full or Guest. 11. The user will receive an account creation email using the email address provided during account creation. 12. The user is required to verify the email account to complete the account creation process.	⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The Administrator configures the User Search Mode. 2. The Administrator configures New Account Creation settings. 3. The Administrator provides the user with the URL for the User Portal OR an invitation to create a new account is sent when a user shares a folder or file. 4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the User Portal Login window, the user clicks the New Account button. 6. The user enters details in the account creation fields. 7. The account is created and is granted access of a Full, Guest, or External User as set by the Administrator in Settings > Admin. 8. The Admin is notified about the new account. 9. The user will receive an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.	1. The Administrator configures the Authentication Type as Active Directory or LDAP. 2. The Administrator imports AD or LDAP user accounts into FileCloud. 3. The Administrator provides the user with the URL for the User Portal. 4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the User Portal Login window, the user clicks the New Account button. 6. The user enters details in the account creation fields. 7. The account is created and is either disabled OR granted access of a Full, Guest, or External User as set by the Administrator in Admin settings. 8. The Admin is notified about the new account. 9. The user will receive an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.

Settings, Users settings User Account Search Mode = Exact Email with Implicit Account Invite OR Exact Email with Explicit Account Invite **Settings, Authentication settings** Authentication Type = DEFAULT **Customization settings, Login tab** New Account button = ENABLED **Settings, Admin settings** Allow Account Signups = True Automatic Account Approval = No automatic approval. Admin has to approve account.	**Settings, Users settings** User Account Search Mode = Exact Email with Implicit Account Invite OR Exact Email with Explicit Account Invite **Settings, Authentication settings** Authentication Type = DEFAULT **Customization settings, Login tab** New Account button = ENABLED **Settings, Admin settings** Allow Account Signups = True Automatic Account Approval = Automatically approve new accounts to Full, Guest, or External User Set **Create account on new user share** to **true** in the policy.	**Settings, Authentication settings** Authentication Type = ACTIVE DIRECTORY or LDAP **Customization settings, Login tab** New Account button = ENABLED **Settings, Admin settings** Allow Account Signups = Default Automatic Account Approval = any value

The scenarios where FileCloud automatically creates a new user account are described in Table 4.

Table 4. Automatic Account Creation

FileCloud automatically creates a new FileCloud account for Active Directory or LDAP Users on First Login
1. The Administrator configures the Authentication Type as Active Directory or LDAP. 2. (Optional) The Administrator imports AD or LDAP user accounts into FileCloud. 3. The Administrator provides the user with the URL for the User Portal. 4. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the User Portal Login window, the user enters their AD or LDAP username and password. 6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.

FileCloud automatically creates a new FileCloud account for Active Directory or LDAP Users on First Login

Settings, Authentication settings

✅ Authentication Type = ACTIVE DIRECTORY or LDAP

Customization settings, Login tab

✅ New Account button = ENABLED

Settings, Admin settings

✅ Allow Account Signups = Default

✅ Automatic Account Approval = Automatically approve new accounts to Full or Guest User.

Also in this section:

- Account Approval
- Allow AD or LDAP Users to Create a New Account
- Allow Only an Admin To Create New Accounts
- Allow Users to Create and Approve Accounts
- Allow Users to Create a New Disabled Account
- Prevent Email Addresses as Usernames
- Domain Limitations for External Users

Account Approval

This feature is used to allow automatic account creation by a user who clicks the **New Account** button in user portal login page.

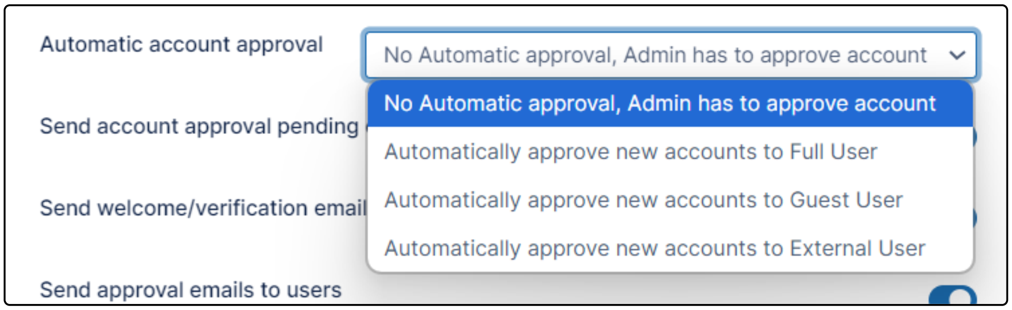
The admin can set account approval in the **Automatic account approval** field in the Admin settings page.

Account approval settings

To set Automatic account approval:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click **Admin**  .
   The Admin settings page opens.
2. Scroll down to the **Automatic account approval** field.

3. Choose one of the values shown below:



Value	Description
No Automatic approval, Admin has to approve account	Default. The account can be created by the user but the user cannot log in. The account requires admin approval for the user to access it.
Automatically approve new accounts to Full User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has Full User permission.
Automatically approve new accounts to Guest User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has Guest User permission. Later the admin can change the permission to Full User permission.
Automatically approve new accounts to External User	The user can create the account and immediately log in to FileCloud without waiting for admin approval. The account has External User permission.

To know more about the difference between Full, Guest and External users, see the User Access page.

No Automatic approval, Admin has to approve account

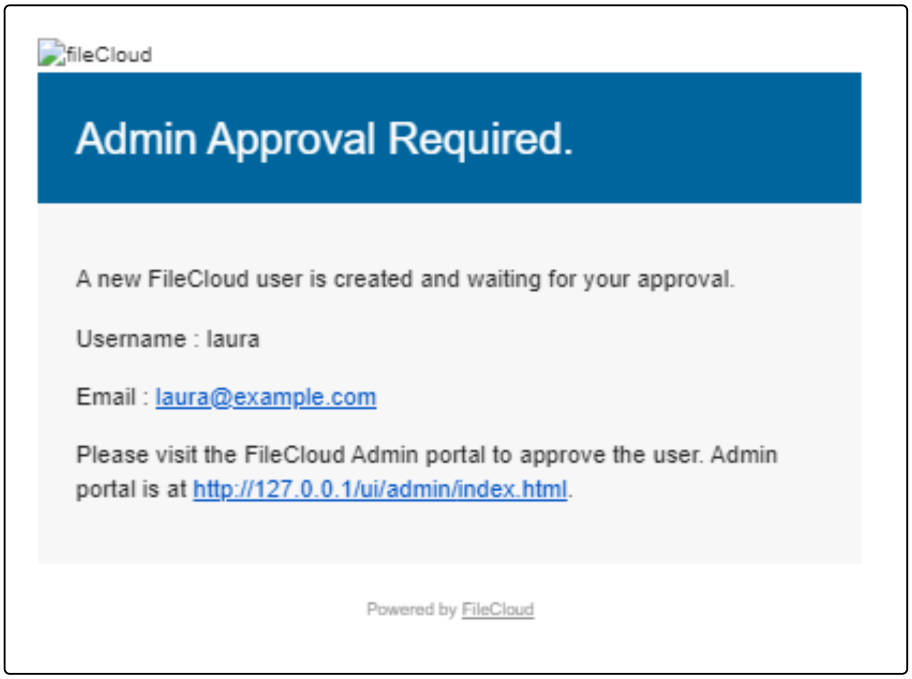
In this mode the user can create an account to access FileCloud but cannot log in until the admin approves the account, so the system sends an Approval Pending email to the admin. Once the admin approves the user, the user receives an Approval email, and can log in and access FileCloud.

Note

- Approval emails are sent only if the option **Send account approval pending emails** is enabled in the admin portal in the Admin settings page. The setting is enabled by default.
- If **Send account approval pending emails** is disabled, the admin is not notified about account creation. In this case, new accounts are approved only when admin user logs in.
- If **Send account approval pending emails** is enabled, the emails are sent to the Admin email in the Admin settings page.

Approving an account as an admin

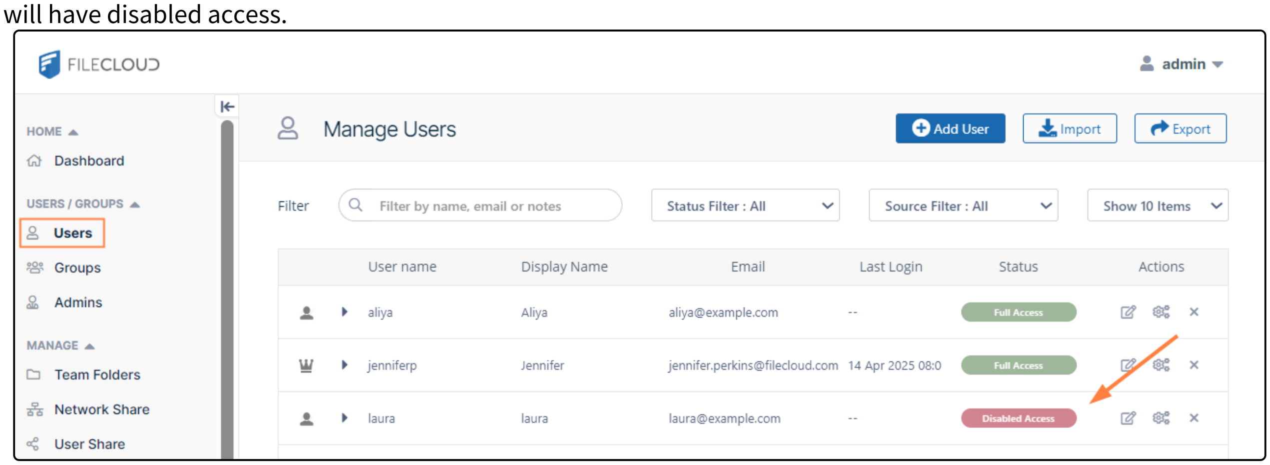
When users create their own accounts and the Admin setting field **Automatic account approval** is set to the default value of **No Automatic approval, Admin has to approve account**, by default you are sent an email to your admin account informing you that a new user has been created an your approval is required to enable it:



If you disable the **Send account approval pending emails** field in the Admin settings page, FileCloud does not notify you that a new account has been created, and you must be notified by a user or browse for new, disabled users in the Manage User page when you log in.

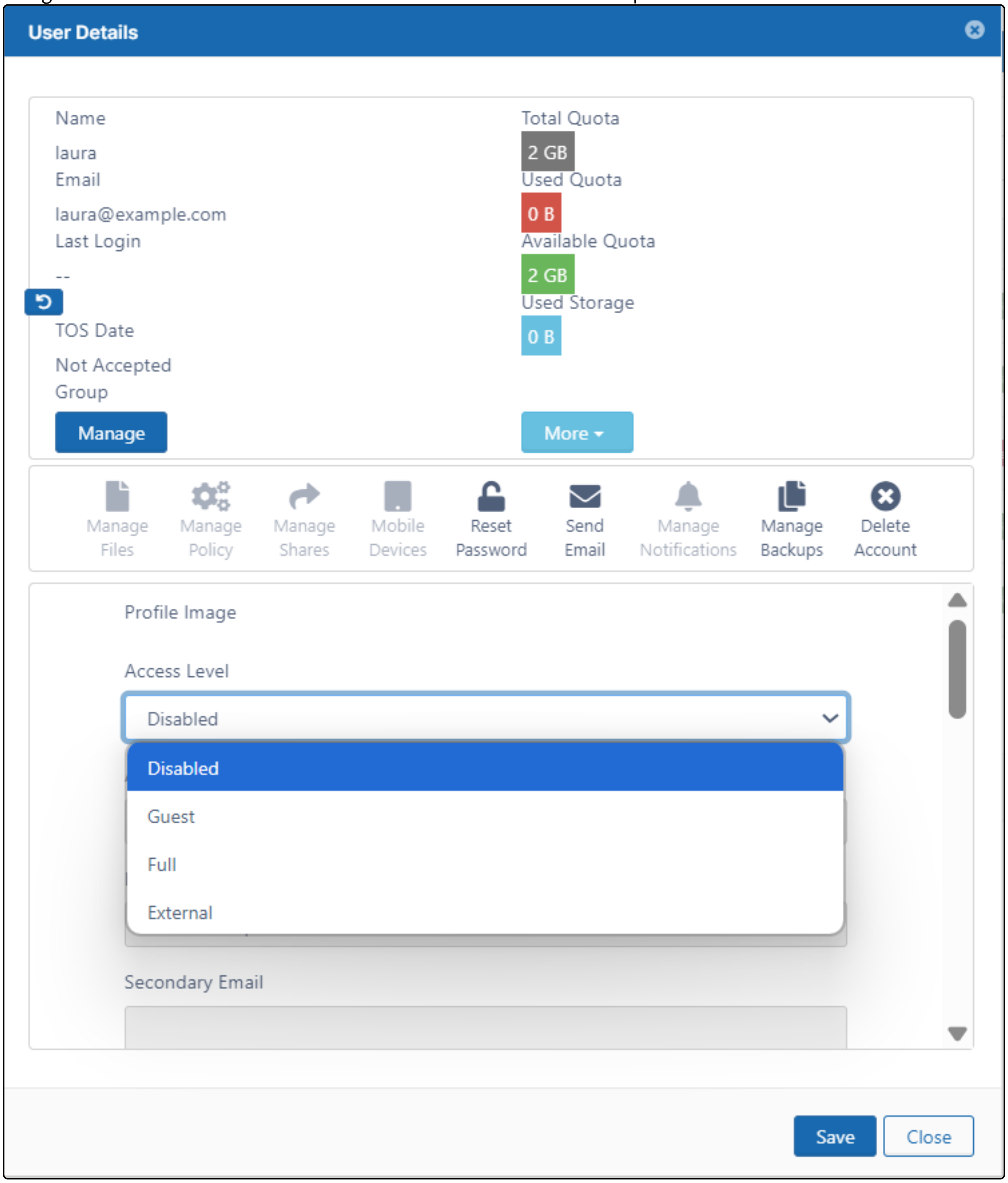
To approve a new, disabled user:

1. In the admin portal, in the navigation panel, click **Users**, and in the Manage Users page, locate the new user, who will have disabled access.

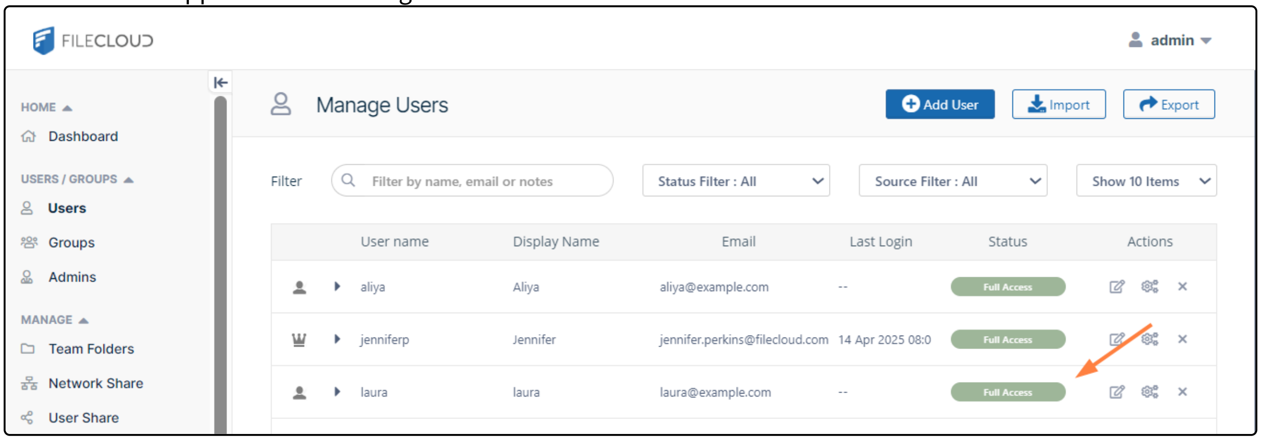


2. To open the **User Details**, click the edit icon for the user.

3. Change the **Access Level** from **Disabled** to one of the access levels with permissions.



The user is now approved and can log in to and use FileCloud.



Allow AD or LDAP Users to Create a New Account

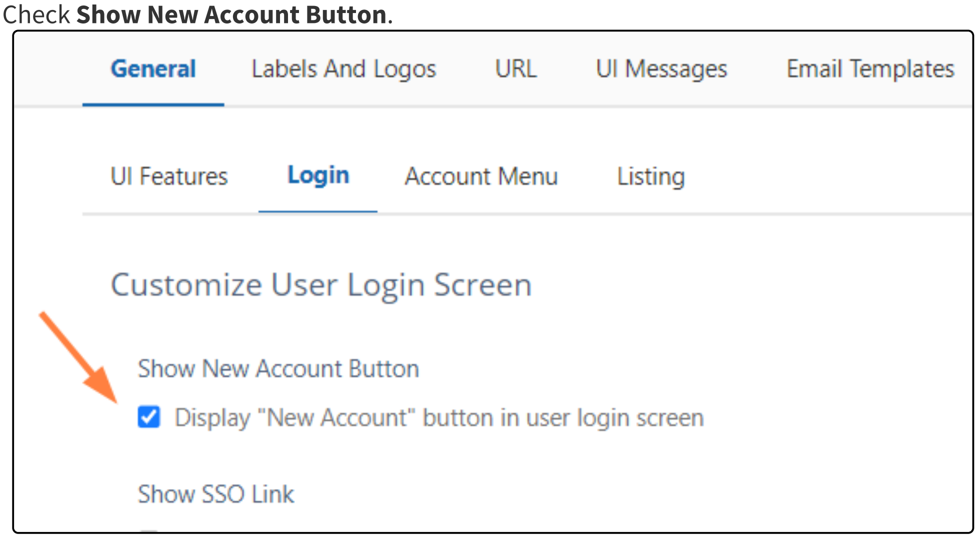
> Active Directory (AD) accounts are only available in some versions of FileCloud Online.

Administrators can allow AD or LDAP users to create a new FileCloud user account in one of the following ways:

- Have FileCloud automatically create a new FileCloud account for AD or LDAP Users on first login (credentials are the same as their AD or LDAP credentials)
- Active Directory or LDAP users create a new FileCloud account different from their AD or LDAP credentials

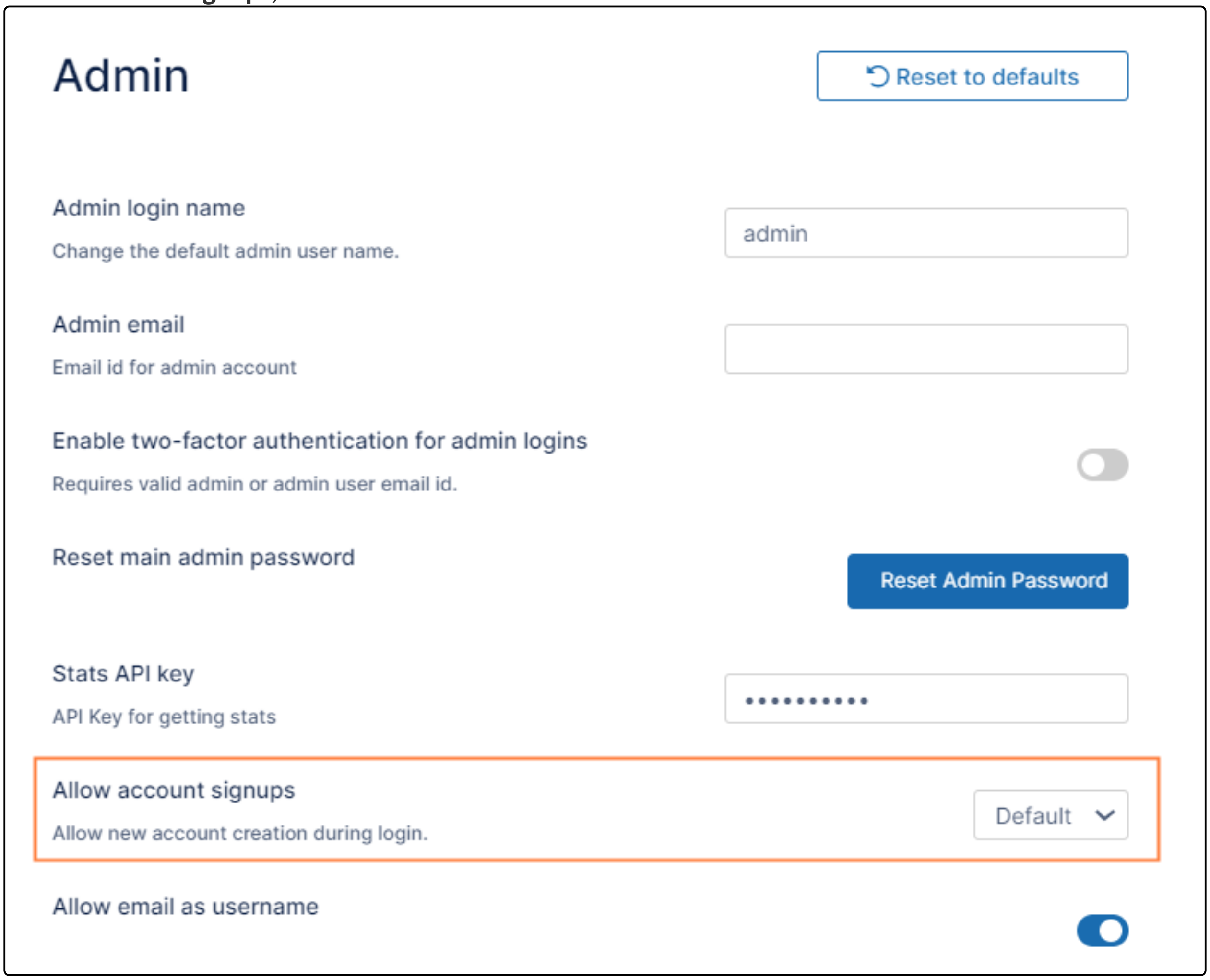
To allow an AD or LDAP user to create a new FileCloud user account:

1. Set up AD or LDAP based authentication following the instructions in Active Directory Authentication or LDAP Based Authentication.
2. In the FileCloud admin portal, go to **Customization > Login**.
3. Check **Show New Account Button**.

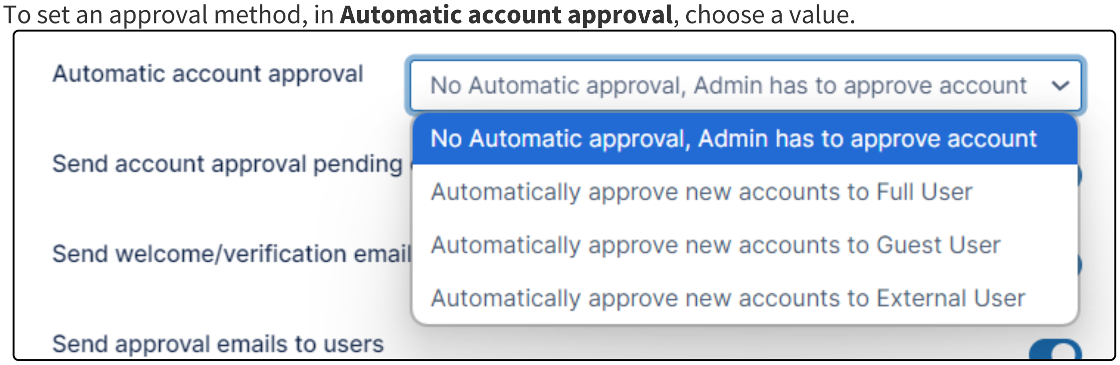


4. Now, in the FileCloud admin portal, go to **Settings > Admin**.

5. In **Allow account signups**, select **Default**.



6. To set an approval method, in **Automatic account approval**, choose a value.



The user is notified by email when:

- Trying to connect (when admin approval is pending)
- When the admin has approved the device trying to connect

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

<table>
<tr><th>Setting</th><th>Location</th><th>Options</th><th>Description</th></tr>
<tr><td>Allow account signups</td><td>Admin settings page</td><td>Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing:
Default
True
False
Can Create an Account
Prerequisite: Show New Account Button = Enabled
Default = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the New Account button).
Active Directory authentication allowed
LDAP authentication allowed
Local users (who are not using AD or LDAP authentication) cannot create their own accounts.</td><td>This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the Automatic Account Approval setting.
Do I choose Default or True?
Default
If you are using AD or LDAP authentication.
You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts.
Note: If you are not using AD or LDAP authentication, users cannot create their own accounts.
True
If you are NOT using AD or LDAP authentication
You want to allow your users to create their own user accounts by clicking the New Account button. By default, the account is disabled until an Administrator approves it.
Note: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the New Account button.</td></tr>
</table>

Setting	Location	Options	Description
		True = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

You can allow AD and LDAP users to create accounts with their AD and LDAP credentials or with different credentials.

Admins want FileCloud to automatically create a new FileCloud account **for their Active Directory or LDAP Users on first login**	**Active Directory or LDAP Users create a new FileCloud account different from their AD or LDAP credentials** **The Admin can configure the approval process**

1. The administrator configures the **Authentication type** as **Active Directory** or **LDAP**. 2. (Optional) The administrator imports AD or LDAP user accounts into FileCloud. 3. The administrator provides the user with the URL for the user portal. 4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client application. 5. On the login window, the user enters their AD or LDAP username and password. 6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.	1. The administrator configures the **Authentication Type** as **Active Directory** or **LDAP**. 2. (Optional) The administrator imports AD or LDAP user accounts into FileCloud. 3. The administrator provides the user with the URL for the user portal. 4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client application. 5. On the user portal login window, the user clicks the **New Account** button. 6. The user enters details in the account creation fields. 7. The account is created and is either disabled OR granted access of a Full User, Guest User, or External User as set by the administrator. 8. The admin is notified about the new account. 9. The user receives an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.
Settings, Authentication settings ✅ Authentication type = Active Directory or LDAP **Customization > Login** ✅ New Account button = Enabled **Settings, Admin settings** ✅ Allow account signups = Default ✅ Automatic account approval = The new user account is automatically approved with **Full** or **Guest** access.	**Settings, Authentication settings** ✅ Authentication Type = Active Directory or LDAP **Customization > Login** ✅ New Account button = Enabled **Settings, Admin settings** ✅ Allow Account Signups = Default ℹ️ Automatic Account Approval = any choice

For more information:

Configure Active Directory

Configure LDAP

Configuring a Scenario

FileCloud supports the following authentication modes:

- Default authentication
- Active Directory based authentication
- LDAP based authentication

The following table describes how each authentication mode impacts the users' ability to create a new account.

	Default Authentication	AD	LDAP
Authentication	Performed by FileCloud Server	In AD Server	In LDAP Server
Users can Create Accounts	Permitted	Not Permitted	Not Permitted
User Account Types	Full, Guest, External	Full, Guest	Full, Guest

Prerequisites

- Active Directory or LDAP service must be accessible from FileCloud (IP and Port must be accessible)
- Active Directory or LDAP must support Simple Authentication Method (Anonymous or Name/Password Authentication Mechanism of Simple Bind)
- Active Directory or LDAP users must have an email attribute

Allow Only an Admin To Create New Accounts

Administrators can customize how new user accounts are created.

In this scenario, you will configure the FileCloud site so that only administrators can create new accounts.

The settings that you use to configure this scenario is described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

<table>
<tr><th>Setting</th><th>Location</th><th>Options</th><th>Description</th></tr>
<tr><td>Allow account signups</td><td>Admin settings page</td><td>Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing:
Default
True
False
Can Create an Account

Prerequisite: Show New Account Button = Enabled

Default = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the New Account button).
Active Directory authentication allowed
LDAP authentication allowed
Local users (who are not using AD or LDAP authentication) cannot create their own accounts.</td><td>This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the Automatic Account Approval setting.

Do I choose Default or True?

Default
If you are using AD or LDAP authentication.
You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts.
Note: If you are not using AD or LDAP authentication, users cannot create their own accounts.
True
If you are NOT using AD or LDAP authentication
You want to allow your users to create their own user accounts by clicking the New Account button. By default, the account is disabled until an Administrator approves it.
Note: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the New Account button.</td></tr>
</table>

Setting	Location	Options	Description
		True = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

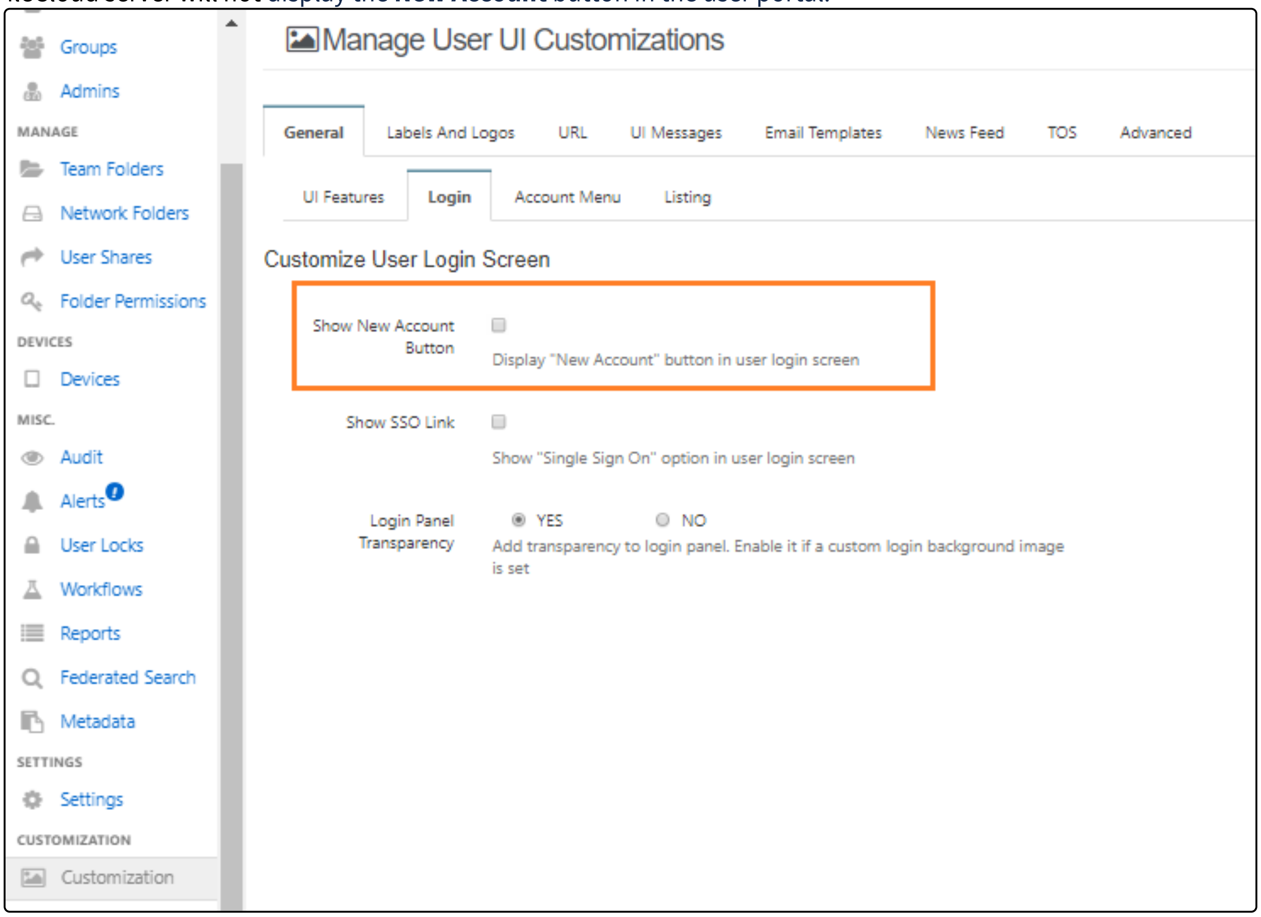
The scenario where only an administrator creates a new FileCloud account is described in the following table.

Only an Admin can create User accounts
1. The administrator creates the account in the admin portal. 2. The user receives a Welcome email with the account credentials and user portal URL.
Customization > Login New Account button = Disabled **Settings, Admin settings** Allow Account Signups = False Automatic Account Approval = No automatic approval, Admin has to approve account.

In this scenario, if you disable the **New Account** button, then the other settings can be left set to their defaults.

To configure these settings:

1. Log into the admin portal.
2. In the left menu panel, click **Customization**.
3. On the **General** tab, click the **Login** tab.
4. Make sure the **Show New Account Button** checkbox is not selected.
   FileCloud server will not display the **New Account** button in the user portal.



Allow Users to Create and Approve Accounts

Administrators can customize how new user accounts are created.

This scenario:

- allows users to create and approve their own accounts.
- allows an administrator set a default level of access.
- may be useful in systems where share invitations are sent to new users.

This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users.

The settings that you use to configure these scenarios are described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description
Allow account signups	Admin settings page	Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing: • **Default** • **True** • **False** **Can Create an Account** Prerequisite: **Show New Account Button** = Enabled **Default** = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the **New Account** button). • Active Directory authentication allowed • LDAP authentication allowed • Local users (who are not using AD or LDAP authentication) cannot create their own accounts.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the **Automatic Account Approval** setting. Do I choose Default or True? **Default** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **True** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts by clicking the **New Account** button. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the **New Account** button.

Setting	Location	Options	Description
		True = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

The scenarios where a user can create a new FileCloud account are described in the following table.

Users can create their own accounts
Users can approve their own accounts **This scenario can also be used to allow new users to create an account when a Share invitation is sent.**
This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The administrator configures the User Search Mode. 2. The administrator configures New Account Creation settings. 3. The administrator provides the user with the URL for the user portal OR an invitation to create a new account is sent when a user shares a folder or file. 4. The user accesses the user portal from a Web browser, mobile device, or FileCloud client app. 5. On the user portal login window, the user clicks the **New Account** button. 6. The user enters details in the account creation fields. 7. The account is created and is granted access of a Full User, Guest User, or External User as set by the Administrator. 8. The user receives an account creation email using the email address provided during account creation. 9. The user is required to verify the email account to complete the account creation process.

Users can create their own accounts

Users can approve their own accounts

💡 **This scenario can also be used to allow new users to create an account when a Share invitation is sent.**

Settings, Misc > User settings

✅ User Account Search Mode = **Exact Email with Implicit Account Invite** or **Exact Email with Explicit Account Invite**

Settings, Authentication settings

✅ Authentication Type = DEFAULT

Customization > Login

✅ New Account button = ENABLED

Settings, Admin settings

✅ Allow Account Signups = TRUE

✅ Automatic Account Approval = Automatically approve new accounts to Full/Guest/External User.

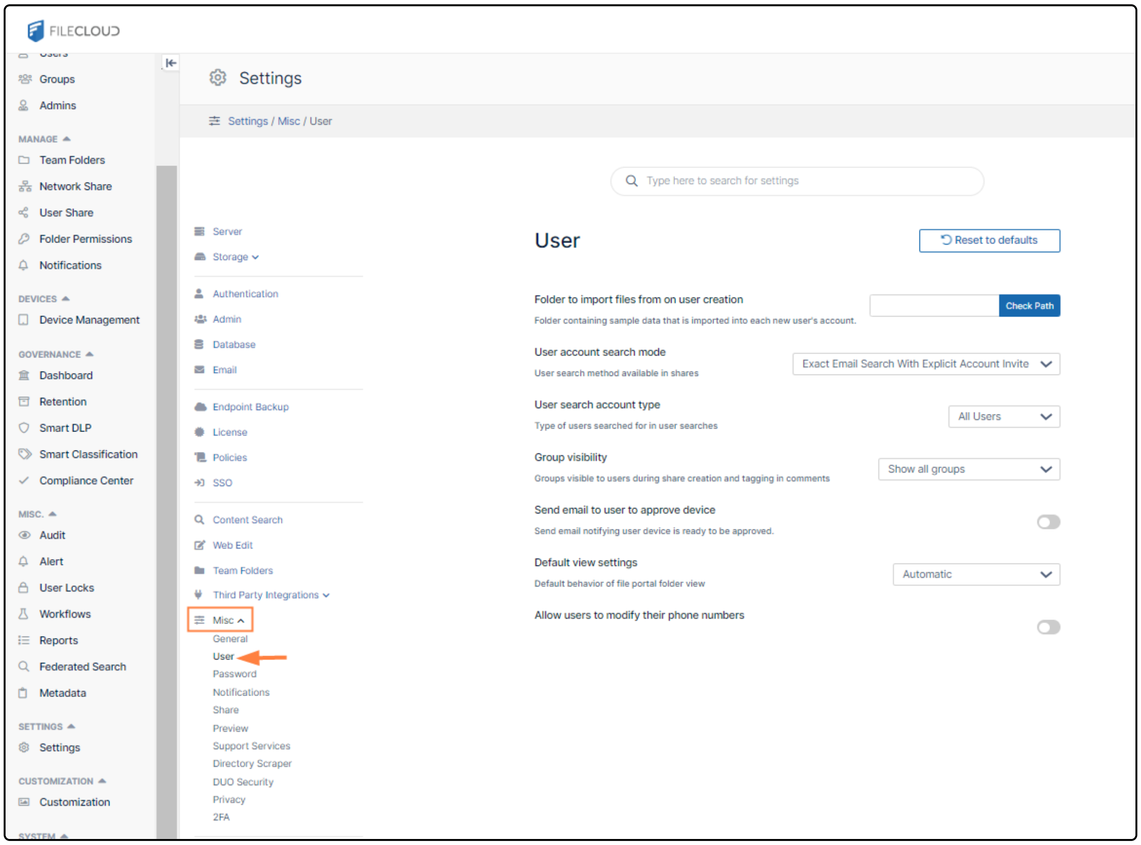
Settings, Policies

✅ Set **Create account on new user shares** to **yes** in users' policies.

To configure these settings:

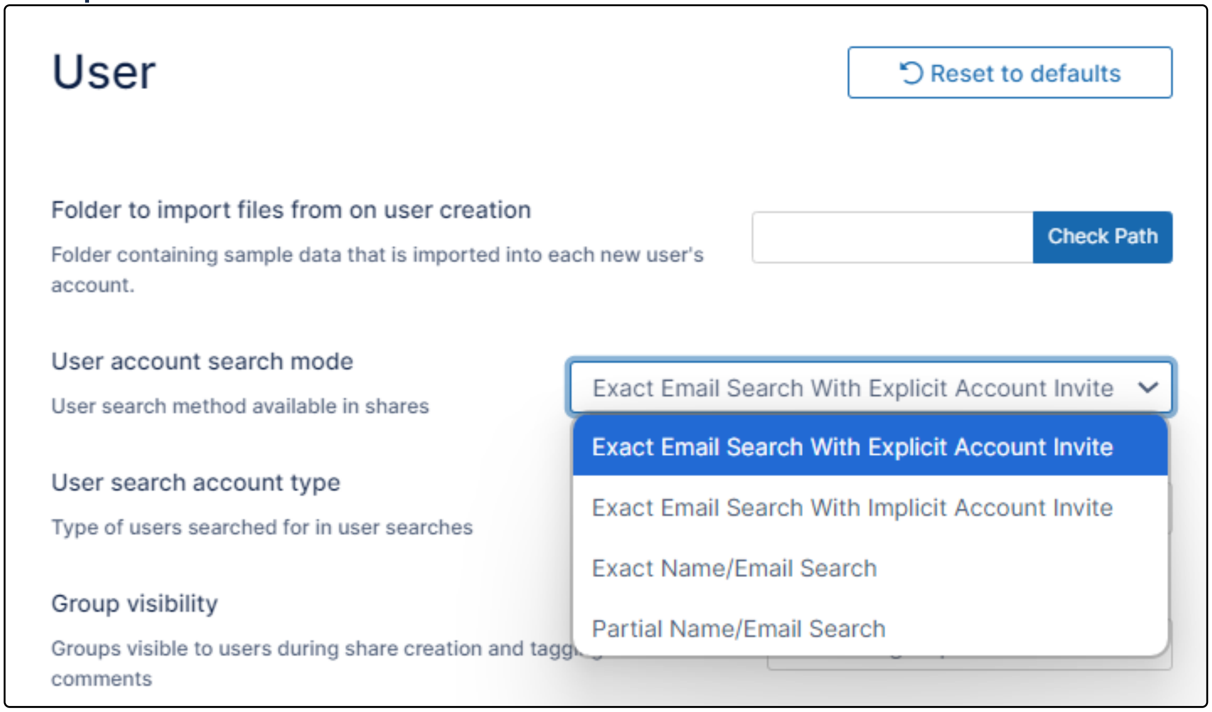
1. Open the User settings page.
   To open the User settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .

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

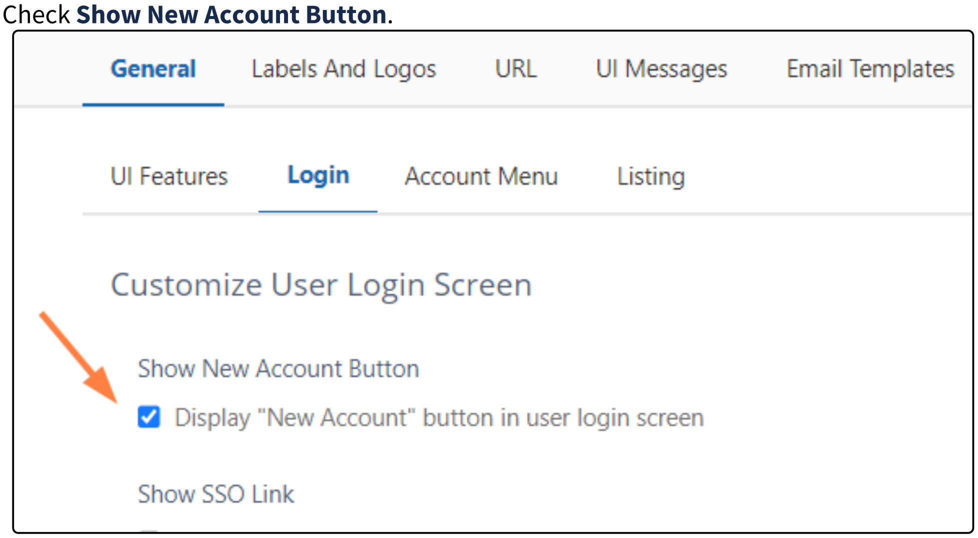


The **User** settings page opens.

2. In **User Account Search Mode**, select **Exact Email Search with Explicit Account Invite** or **Exact Email Search with Implicit Account Invite**.



3. Click **Save**.
4. In the FileCloud admin portal's left navigation bar, go to **Customization > General > Login**.
5. Check **Show New Account Button**.



6. Click **Save**.
7. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin**  .
The **Admin** settings page opens.

8. In the **Allow Account Signups** field, select **True**.

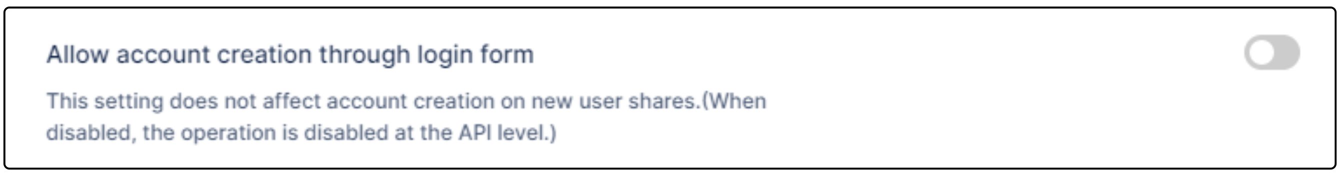
9. Click **Save**.

Blocking the createprofile API endpoint

The setting **Allow account creation through login form** has been added to enable you to block the createprofile API endpoint from the admin portal. The endpoint is used for account signups in the New Account form.

To disable the createprofile API endpoint:

1. Go to Settings > Admin.
2. Disable the **Allow account creation through login form** setting.



Allow Users to Create a New Disabled Account

Administrators can customize how new user accounts are created.

In this scenario you are allowing users to create their own accounts but they are disabled until an administrator approves them.

The settings that you use to configure this scenario are described in Table 1.

Table 1. The Settings

Setting	Location	Options	Description
Show New Account Button	Customization > General > Login	**ENABLED** = Displays **New Account** button on user log-in page. opens a window for the user to type in new account information **DISABLED** = Hides **New Account** button on user log-in page.	This setting determines whether the **New Account** button appears on the user portal log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • **Allow Account Signups** • **Automatic Account Approval**

Setting	Location	Options	Description

<table>
<tr><th>Setting</th><th>Location</th><th>Options</th><th>Description</th></tr>
<tr>
<td>Allow account signups</td>
<td>Admin settings page</td>
<td>Specifies if a user can or cannot create a new FileCloud user account from the login page. by choosing:
Default
True
False
Can Create an Account
Prerequisite: Show New Account Button = Enabled
Default = AD and LDAP users can create their own accounts by logging in to the user portal (they do not have to click the New Account button).
Active Directory authentication allowed
LDAP authentication allowed
Local users (who are not using AD or LDAP authentication) cannot create their own accounts.
</td>
<td>This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the Automatic Account Approval setting.
Do I choose Default or True?
Default
If you are using AD or LDAP authentication.
You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, instruct the users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create their new FileCloud accounts.
Note: If you are not using AD or LDAP authentication, users cannot create their own accounts.
True
If you are NOT using AD or LDAP authentication
You want to allow your users to create their own user accounts by clicking the New Account button. By default, the account is disabled until an Administrator approves it.
Note: If you are using AD or LDAP authentication, AD or LDAP users can create accounts which do not use their AD credentials by clicking the New Account button.
</td>
</tr>
</table>

Setting	Location	Options	Description
		True = Local users can create their own accounts • Local users (who are not using AD or LDAP authentication) can create their own accounts by clicking the **New Account** button when they initially log in. • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** **False** = No users can create their own accounts • If the **New Account** button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Admin settings page	**(Default) No automatic approval. Admin has to approve account**. **Automatically approve new accounts to Full User** **Automatically approve new accounts to Guest User** **Automatically approve new accounts to External User**	If the total number of licenses has been reached, share invitations to new users are blocked unless **Automatic Account Approval** is set to **Automatically approve new accounts to External User.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = Default or True This setting determines: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

The scenarios that enable a user to create a new FileCloud account are described in the following table.

Users can create their own accounts **The Admin must approve the accounts** **This scenario can also be used to allow new users to create an account when a Share invitation is sent.**
This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The Administrator provides the user with the URL for the User Portal. 2. The User accesses the user portal from a Web browser, mobile device, or FileCloud client app. 3. On the User Portal Login window, the user clicks the New Account button. 4. The user enters details in the account creation fields. 5. The account is created but is disabled by default. 6. The Admin is notified about the new account. 7. The Admin approves the account. 8. The Admin sets the user account type to Full User or Guest User. 9. The user receives an account creation email using the email address provided during account creation. 10. The user is required to verify the email account to complete the account creation process.

Users can create their own accounts

The Admin must approve the accounts

This scenario can also be used to allow new users to create an account when a Share invitation is sent.

Settings, Authentication settings

Authentication Type = Default

Customization settings, Login tab

New Account button = Enabled

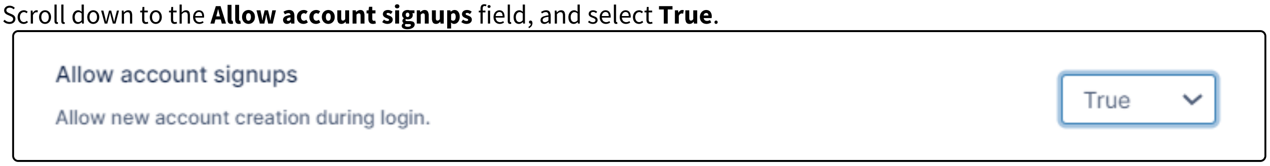
Settings, Admin settings

Allow Account Signups = True

Automatic Account Approval = No Automatic approval; Admin has to approve account

To configure these settings:

1. Log into the Administration Portal.
2. In the left menu panel, click **Customization**.
3. On the General tab, click the Login tab.
4. Make sure the **Show New Account Button** checkbox is selected.
5. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Admin** .
6. Scroll down to the **Allow account signups** field, and select **True**.



The user is notified by email when:

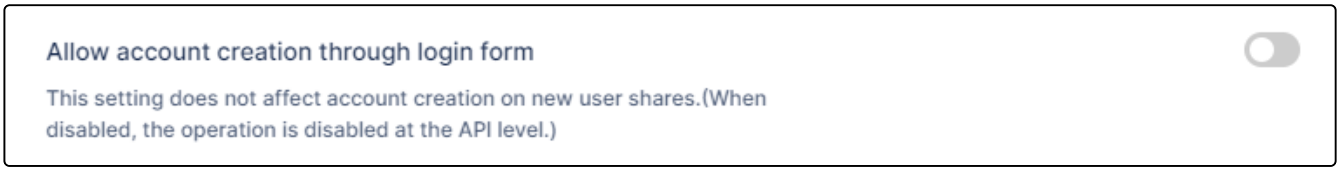
- Trying to connect (admin approval pending)
- When the administrator has approved the device trying to connect

Blocking the createprofile API endpoint

The setting **Allow account creation through login form** has been added to enable you to block the createprofile API endpoint from the admin portal. The endpoint is used for account signups in the New Account form.

To disable the createprofile API endpoint:

1. Go to Settings > Admin.
2. Disable the **Allow account creation through login form** setting.



Domain Limitations for External Users

> Domain limitations for external users are effective for FileCloud beginning in version 22.1.
> If external users have the same domains that at least 10% of licensed users have before the rule was put into effect, the external users are allowed to remain with their current emails.

Your FileCloud license limits the number of licensed (full and guest users) you can create, but allows you to create an unlimited number of external users. To prevent users from using external accounts for internal users, the system assumes that your FileCloud site domain (and its sub-domains and sibling domains) and any domain used by at least 10% of your licensed (full and guest) users are internal domains, and therefore prevents you from creating external users with those domains.

An exception is made for popular email domains like gmail and yahoo. Unlimited numbers of external users can be created with those domains. Users with those domains are not counted when the system calculates percents of users with specific domains.

Example:
A company has a FileCloud license that permits 30 licensed (full and guest) users. The FileCloud site domain is **company456.com**.

The 30 licensed users have emails with the following domains:
company456.com - 10 users
tech123.com - 8 users
gmail.com - 8 users
factory123.com - 3 users
sullivanlaw.com - 1 user

The 8 users with gmail.com as their domain are omitted when computing the percent of users with specific domains.

The admin adds an external user with the email: **jcarr@company456.com**. This is not permitted because it has the same domain as the FileCloud site.

The admin adds an external user with the email: mfields@tech123.com. This is not permitted because 36% of the licensed users have the same domain.

The admin adds an external user with the email: **hbarrett@gmail.com**. This is permitted because gmail.com is a popular domain.

The admin adds an external user with the email: **bsullivan@sullivanlaw.com**. This is permitted because only 4.5% of the licensed users have the same domain.

Password Settings

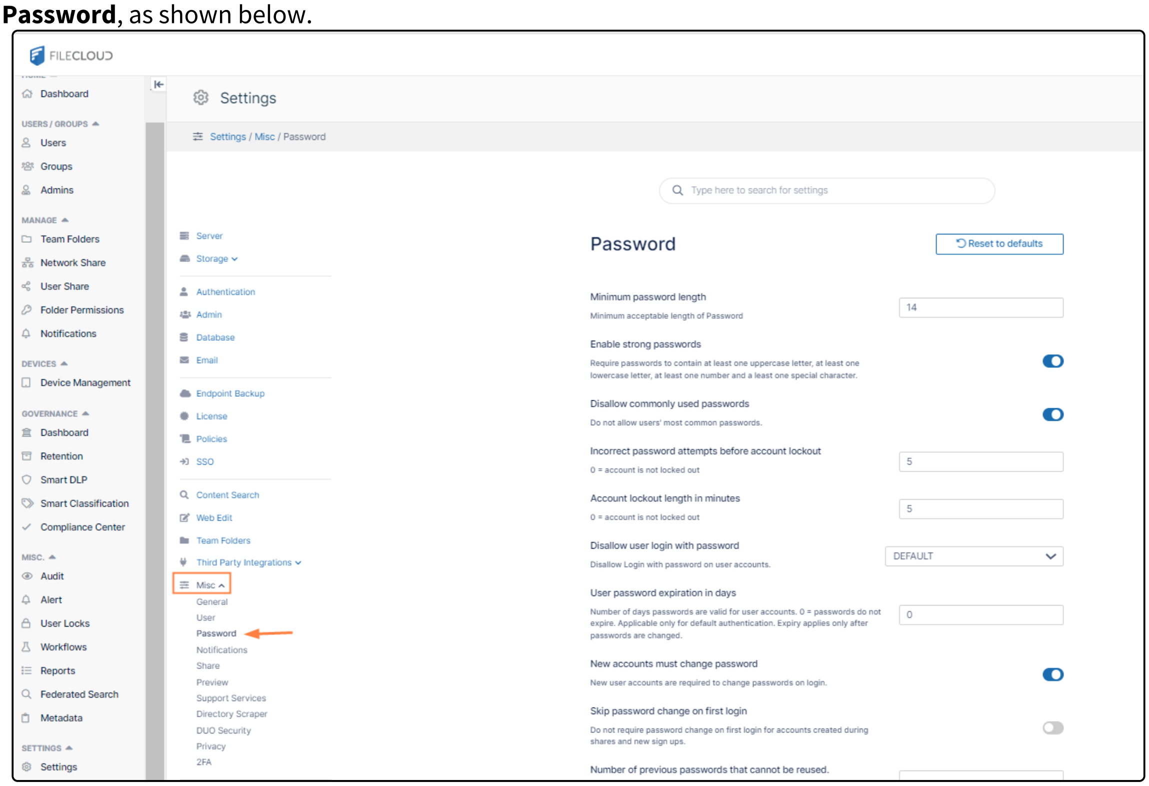
> Beginning with FileCloud 23.241, the **New Accounts Must Change Password** setting is enabled by default. Prior to FileCloud 23.241, the **New Accounts Must Change Password** setting was disabled by default.
>
> Beginning with FileCloud 23.241, the **Skip password change on first login** setting is disabled by default. Prior to FileCloud 23.241, the **Skip password change on first login** setting was enabled by default.

> The following settings are applicable for the default FileCloud Admin, the Team Folder account and user accounts.

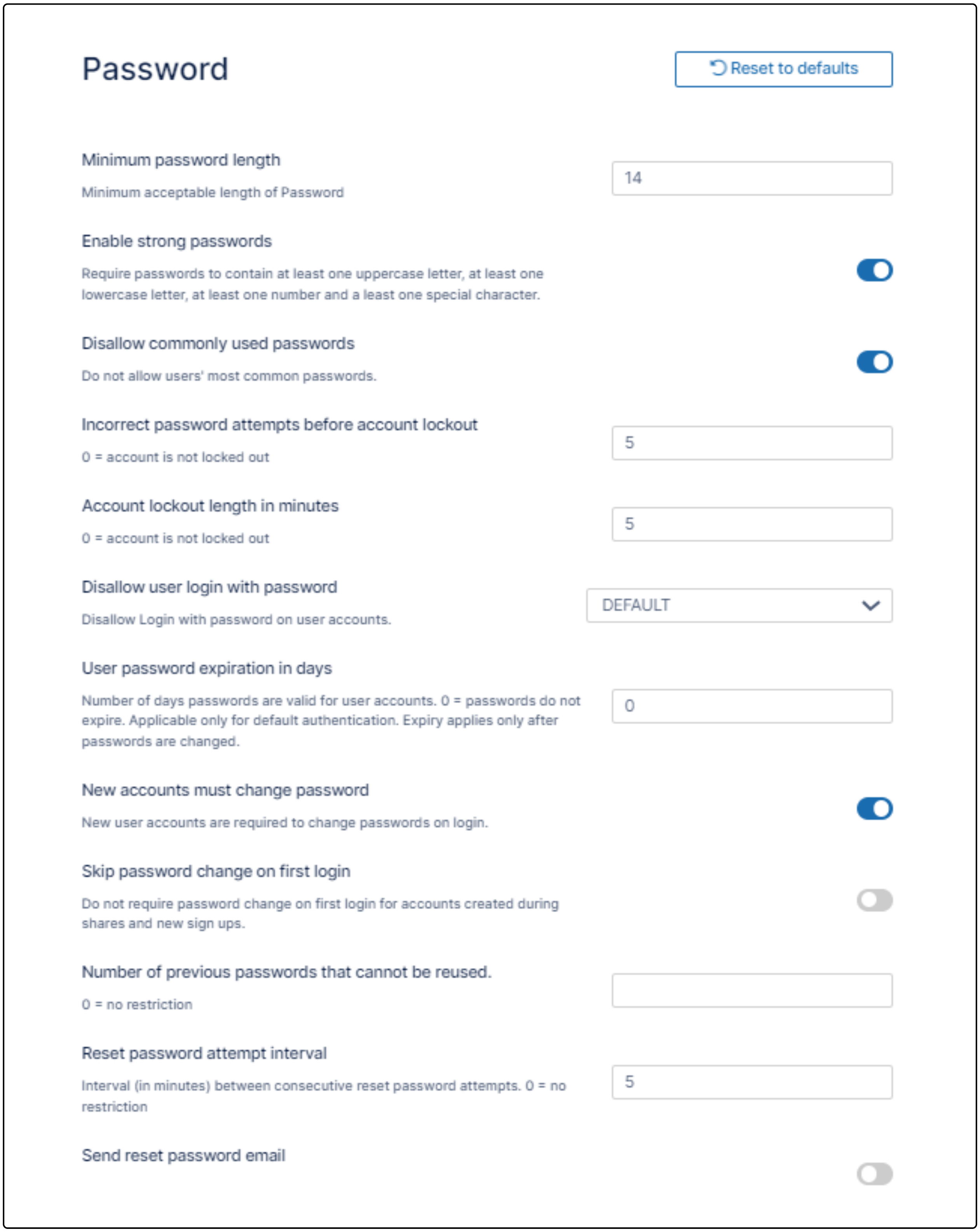
This section explains the password settings available in FileCloud installation.

To view or change the password settings:

1. Open the **Password** settings page.
   To go to the Password settings page
   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 **Password**, as shown below.

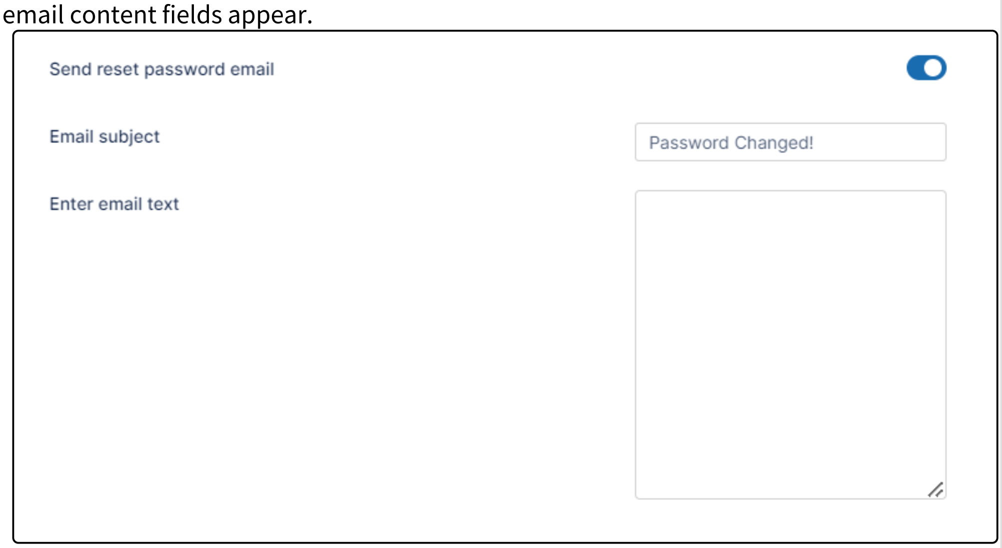


The **Password** settings page opens.



2. Change any of the settings according to your security requirements.

Type	Description
Minimum Password Length	Enforces minimum character length for password (Applies to local account and NOT to AD/LDAP accounts). Default value is 14.
Enable Strong Passwords	Enabling this will require the password to contain at least one uppercase, lowercase, number and a special character in the password. Checked by default. Applies only to local account and not to AD/LDAP account.
Disallow Commonly Used Passwords	Prevents users from using commonly used passwords for their user accounts. Enabled by default. For more information, see Restrict Commonly Used Passwords.
Incorrect attempts before account lockout	For higher security, if users try logging in with the wrong password for more than the times specified here, their account will be locked out and they cannot login even if they type in their correct password. Default value is 5. A value of 0 means account lockout with wrong password is disabled.
Account Lockout length in Minutes	Specifies time the account is locked out if wrong password is entered multiple times as specified in the option for max incorrect attempts. Default value is 5. A value of 0 means lockout is disabled.
Disallow user login with password	This setting will disallow login for user accounts. DEFAULT allows login with password for all users.
User Password Expires In Days	If a value above 0 is entered, when a new user is created or when a password is changed, an expiration date for the password is added automatically. NOTE: Automatic email notifications are sent to the user 7 days and 1 day before the actual password expiry date.
New accounts must change password	When enabled, this setting forces new users to change their password on initial login, with the following exceptions: • When the user creates the new account through a registration form (the user adds a password in the form). • When the user has an AD account (the user is automatically assigned an AD password). • When the user logs in using SSO. Default is enabled.

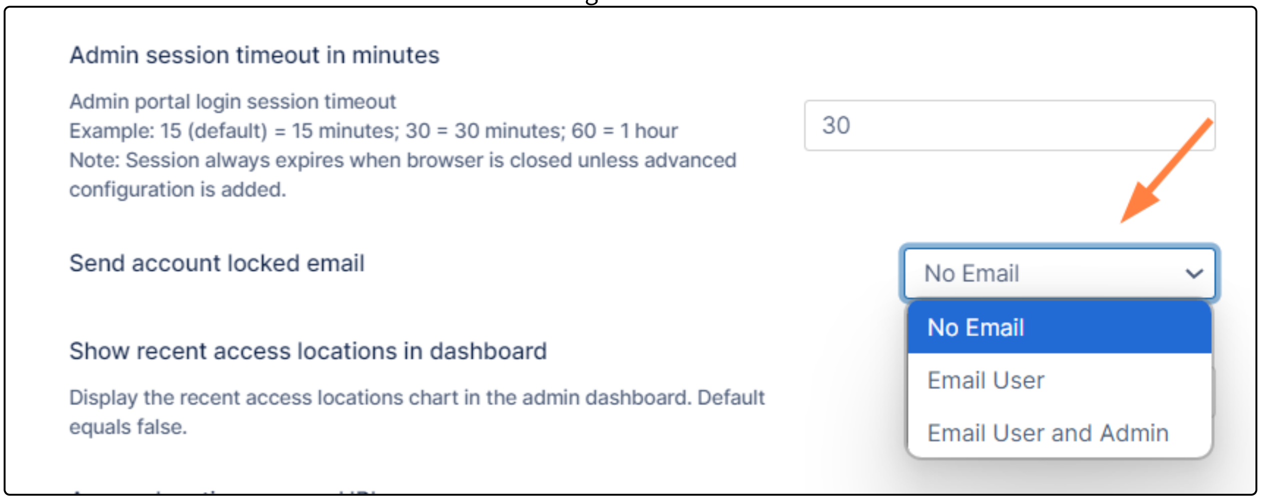
Type	Description
Skip password change on first login	Do not require password change on first login for accounts created during shared and new signups. Default is disabled.
Number of previous passwords that cannot be reused	Specifies the number of previous passwords that cannot be reused when password is changed. A value of 0 indicates that there are no restrictions.
Reset password attempt interval	Interval in minutes between consecutive reset password attempts. Default is 5. 0 indicates that there is no restriction.
Send reset password email	Allows you to create an email that is automatically sent to a user when an admin resets the user's password. There is no default email; when this is enabled, email subject and email content fields appear.  **Email subject** is set to **Password Changed!** but may be changed. The note in **Enter the text of the email below** must be entered. Disabled by default.

3. Click **Save**.

Setting Account Locked Alerts

By default, FileCloud is set to not send an email message to the user or admin to notify them that the account has been locked due to incorrect login attempts. However, you may change this setting.

To change the **Account Locked Alert** setting:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin**  .
   The **Admin** settings page opens.
2. Scroll down to the **Send account locked email** setting.
   

3. In the drop-down list, choose one of the following settings:
   No Email - Neither the user nor the admin receives an email notification about the user account lockout.
   Email User - The user receives an email notification about their account lockout but the admin does not.
   Email User and Admin - Both the user and the admin receive an email about the user account lockout.

Restrict Commonly Used Passwords

Anytime a password is created or updated, before the password is accepted, FileCloud Server checks the suggested password against the US NIST Password Guidelines list.

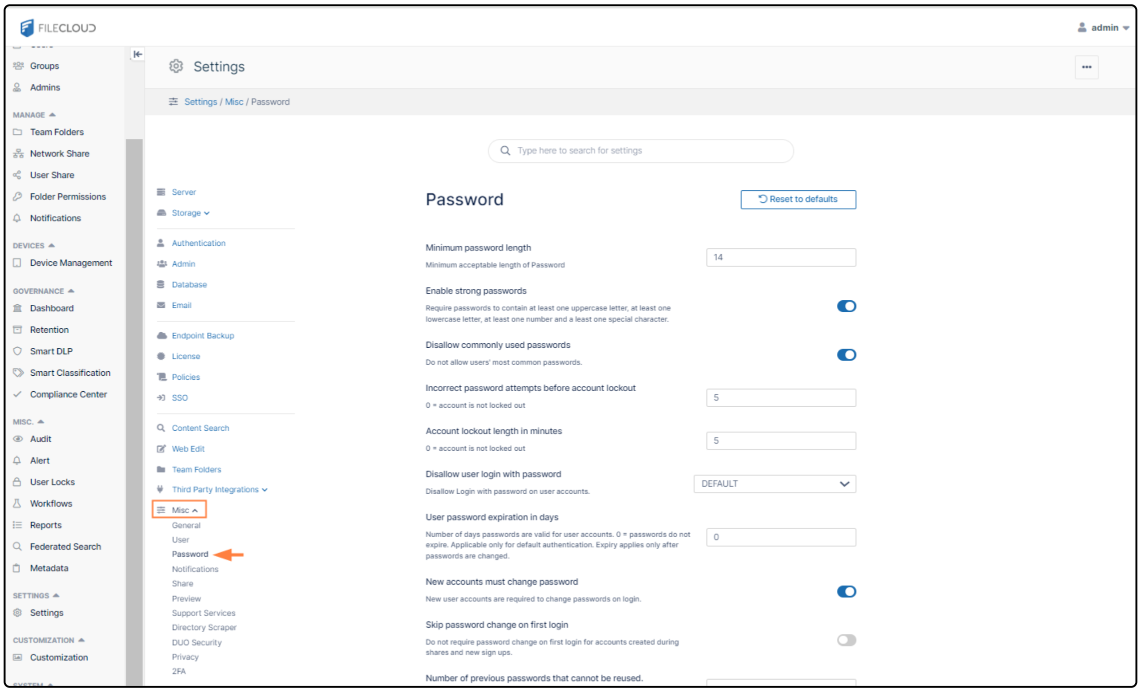
- This feature can be enabled or disabled by the administrator in the admin portal.
- The option is called **Disallow commonly used passwords** and if enabled it will prevent users from setting commonly used passwords for their user accounts.

The password entered is checked against the password guidelines list when:

- A new user is added.
- A user's password or the admin password is updated.
- The password is reset.
- User are imported using a CSV file.

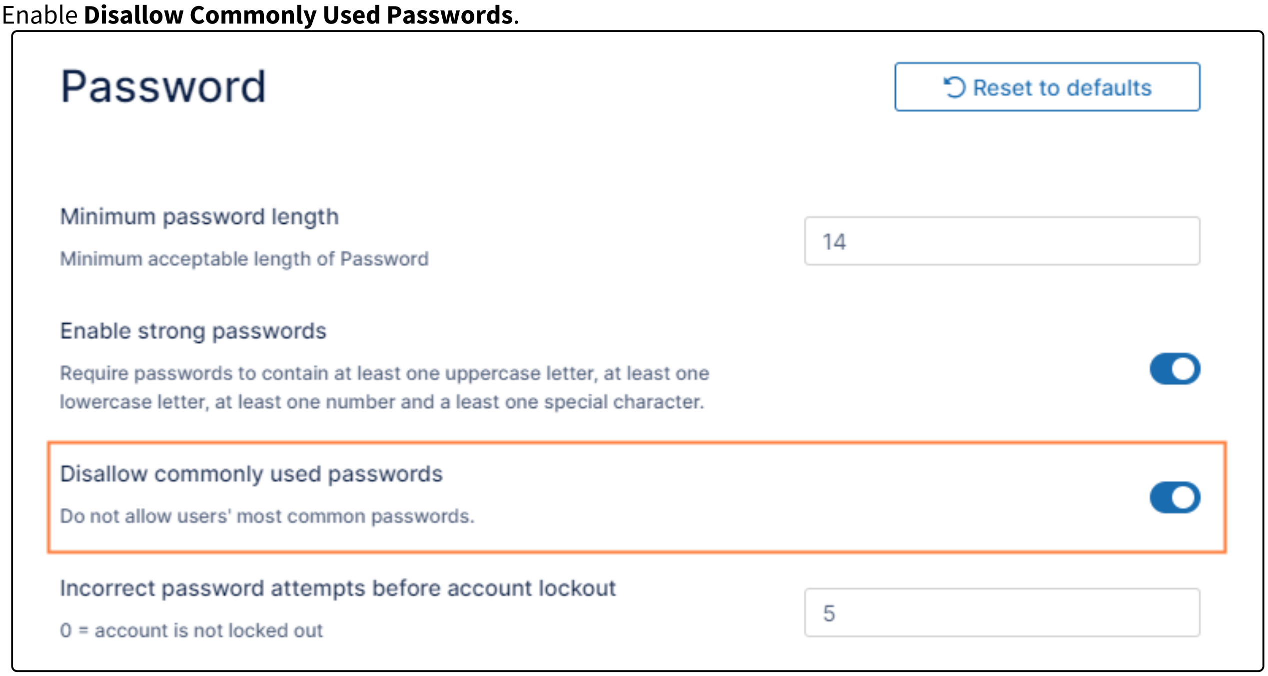
To set this option:

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



The **Password** settings page opens.

2. Enable **Disallow Commonly Used Passwords**.



3. Click **Save**.

User Session Expiration

Default Behavior

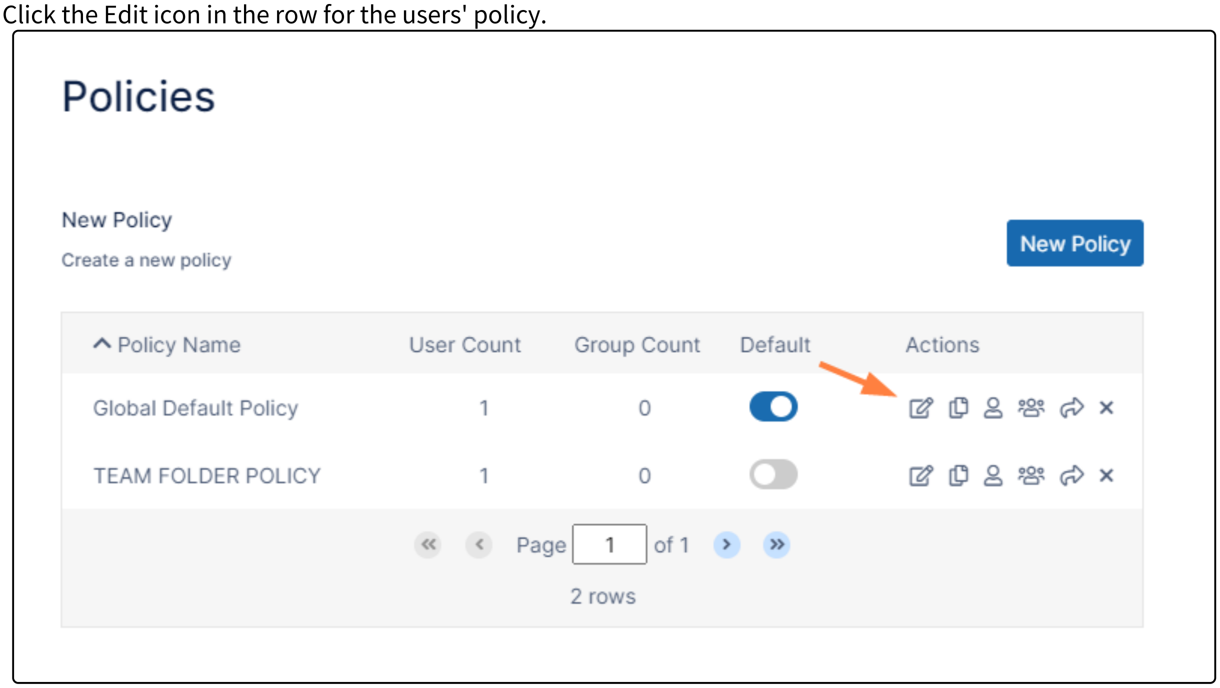
By default, when a user logs into FileCloud, their session remains authenticated for a specified amount of time.

Device	Time Session is Valid
Web Browser	Specified by the value in Session Timeout in minutes setting. If the browser is closed, the session expires.
All other apps and clients	Doesn't expire. Session lasts until user logs out from app.

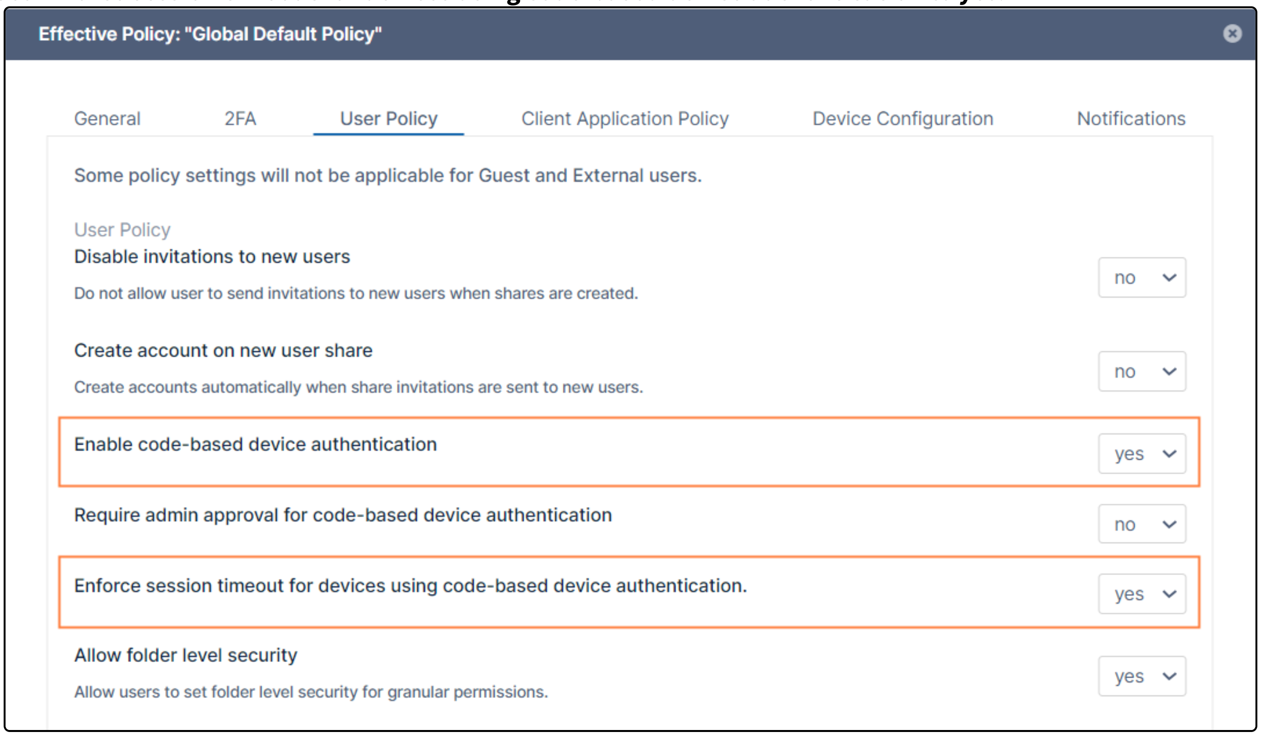
Enabling Session Expiration for all Devices

If you want all login sessions for all user devices (including web browsers) to expire and require re-login, set the policy to **Enforce Session Timeout for All Devices**.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



3. Click the **User Policy** tab.
4. In order to enable the **Enforce session timeout for devices using code-based device authentication** setting, scroll down to the setting **Enable code-based device authentication** and set it to **yes**.
   Now **Enforce session timeout for devices using code-based device authentication** is enabled.
5. Set **Enforce session timeout for devices using code-based device authentication** to **yes**.



6. Click **Save**.

Note: We don't recommend requiring session expiration for devices and other clients as it might impact functionality and reduce user friendliness.

Device	Time Session is Valid
Web Browser	Specified by the value in Session Timeout in minutes setting. If the browser is closed, the session expires.
All other apps and clients	Specified by the value in Session Timeout in minutes setting. Note: When log in used username and password, app will automatically re-login, so the session will not appear to expire. When log in used Device Authorization code, app will require user to re-login into FileCloud using the web browser.

Changing the Storage Quota for Users

Administrators can manage the storage space allotted to a user account or a group of users through Policies.

- Use the Global Default policy to set a quota for all user accounts

- Use a custom policy to set a quota for a specific user or for a select group of users

Set a Quota for a Specific User

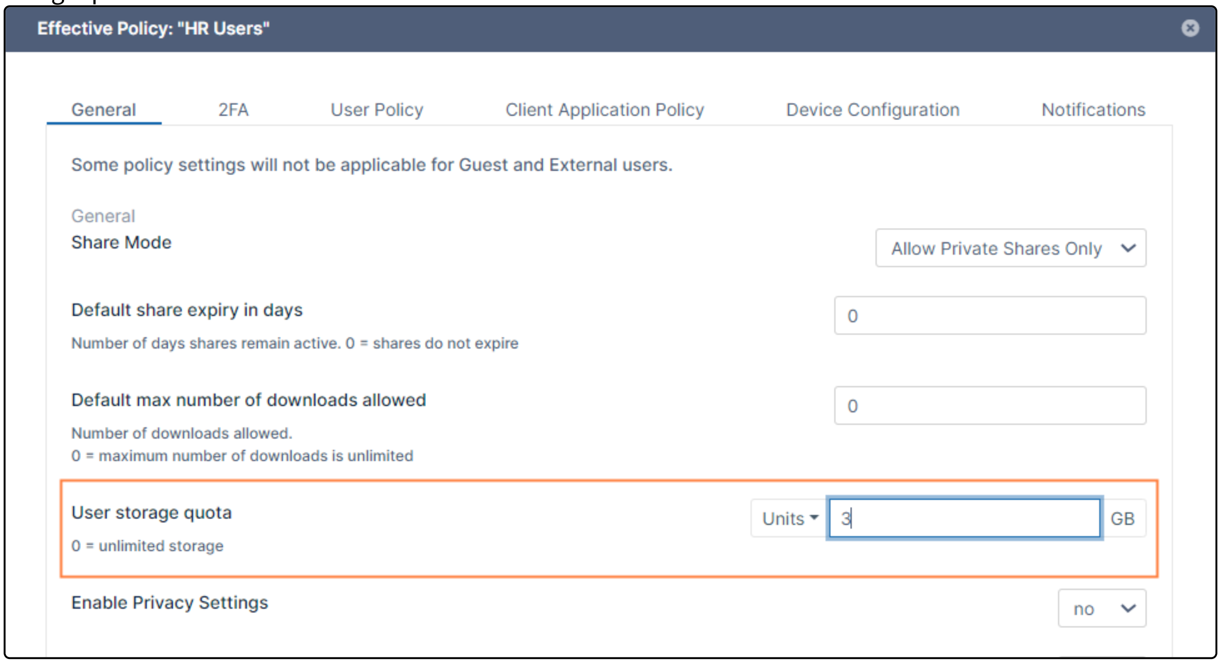
To set a storage quota for a specific user, create a custom policy and assign the user to that policy.

Create a Custom Policy for one user

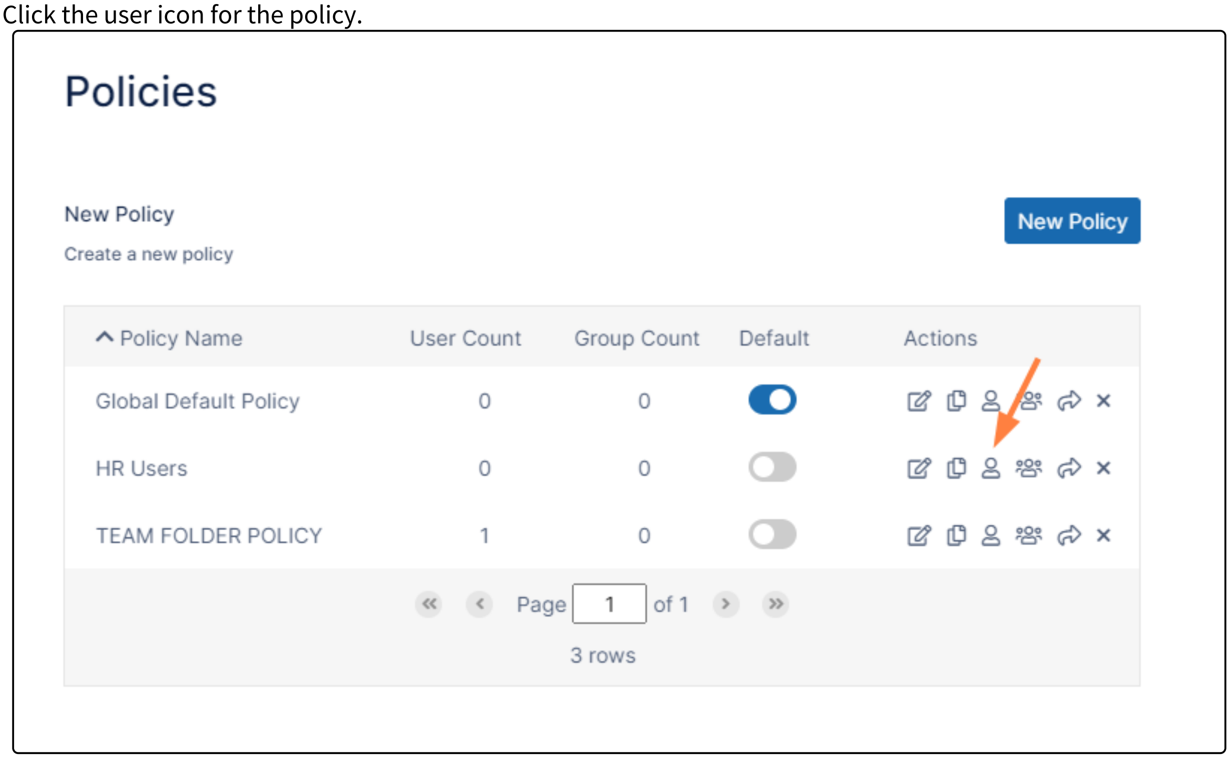
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
   

2. Create the custom policy. See Policies.

3. Click the edit icon for the new policy, and in the **General** tab, in the **User storage quota** field, enter the storage quota for the user.

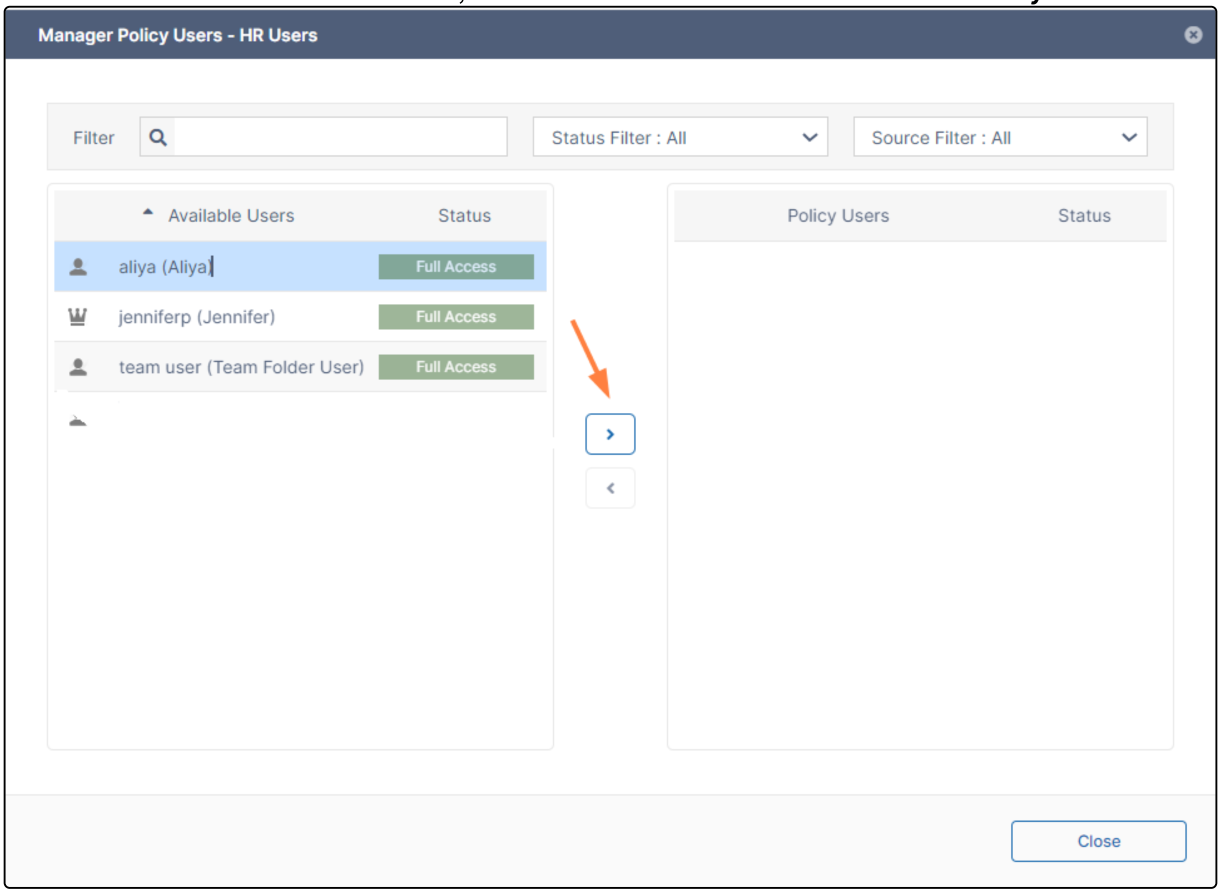


4. Click **Save**.
5. Click the user icon for the policy.



The **Manage Policy Users** dialog box opens.

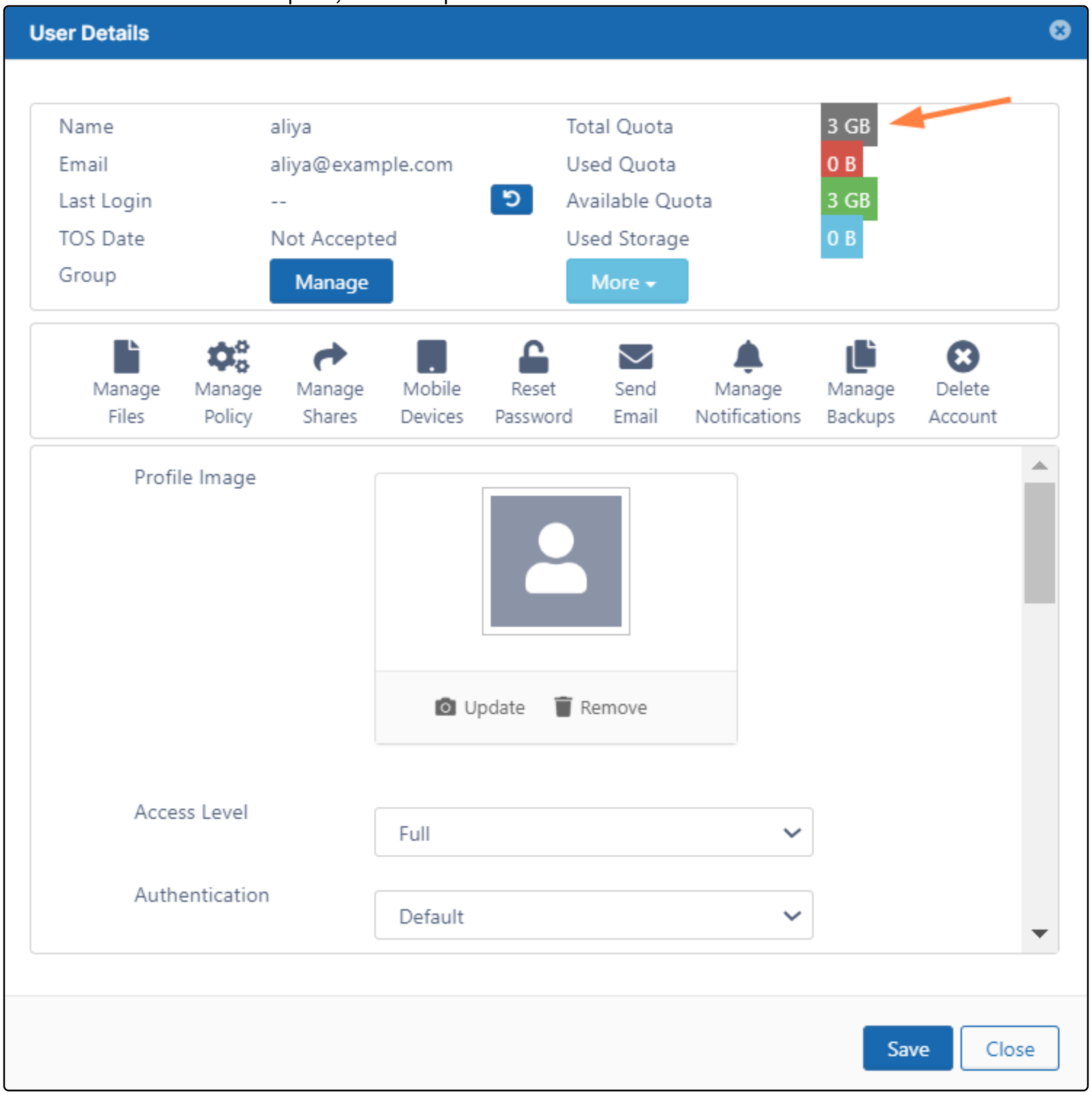
6. Select the user in the **Available Users** box, and click the arrow to move the user into the **Policy Users** box.



The new policy automatically becomes the user's effective policy.

7. Click **Close**.
8. Confirm that the user's storage quota has changed by clicking **Users** in the navigation pane, and clicking the edit button for the user.

In the **User Details** box that opens, the total quota should reflect the new value:



Set a Custom Quota for a Group

To set a storage quota for a specific group, create a custom policy and assign the group to that policy.

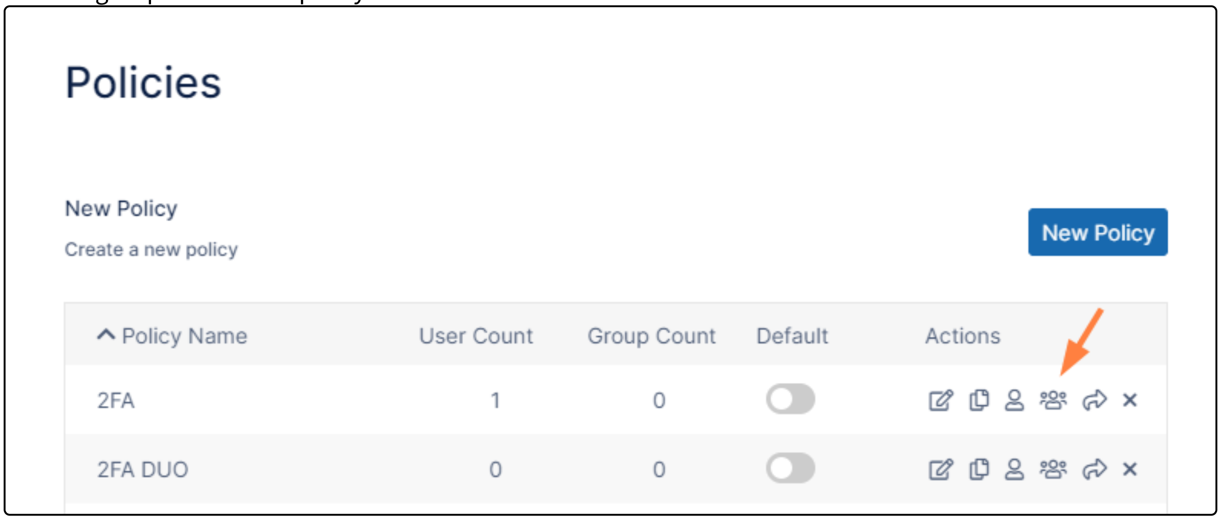
Create a Custom Policy to set the quota for a group of users

If you need to change the quota for a custom group of users, you can create a custom policy.

To create a group custom policy:

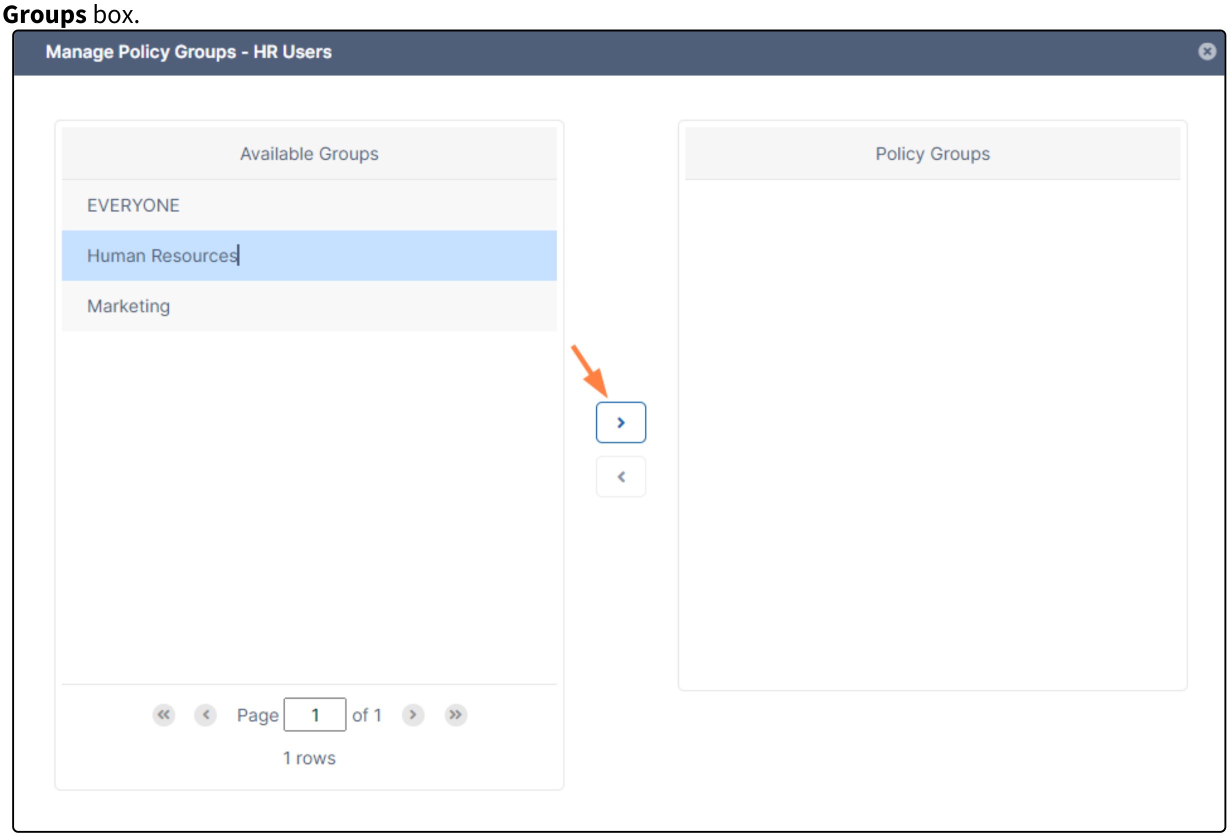
1. Follow steps 1 to 4 in Set a Quota for a Specific User, above.

2. Click the group icon for the policy.



The **Manage Policy Groups** dialog box opens.

3. Select the group in the **Available Groups** box, and click the arrow to move the group into the **Policy Groups** box.



The new policy automatically becomes the group's effective policy.

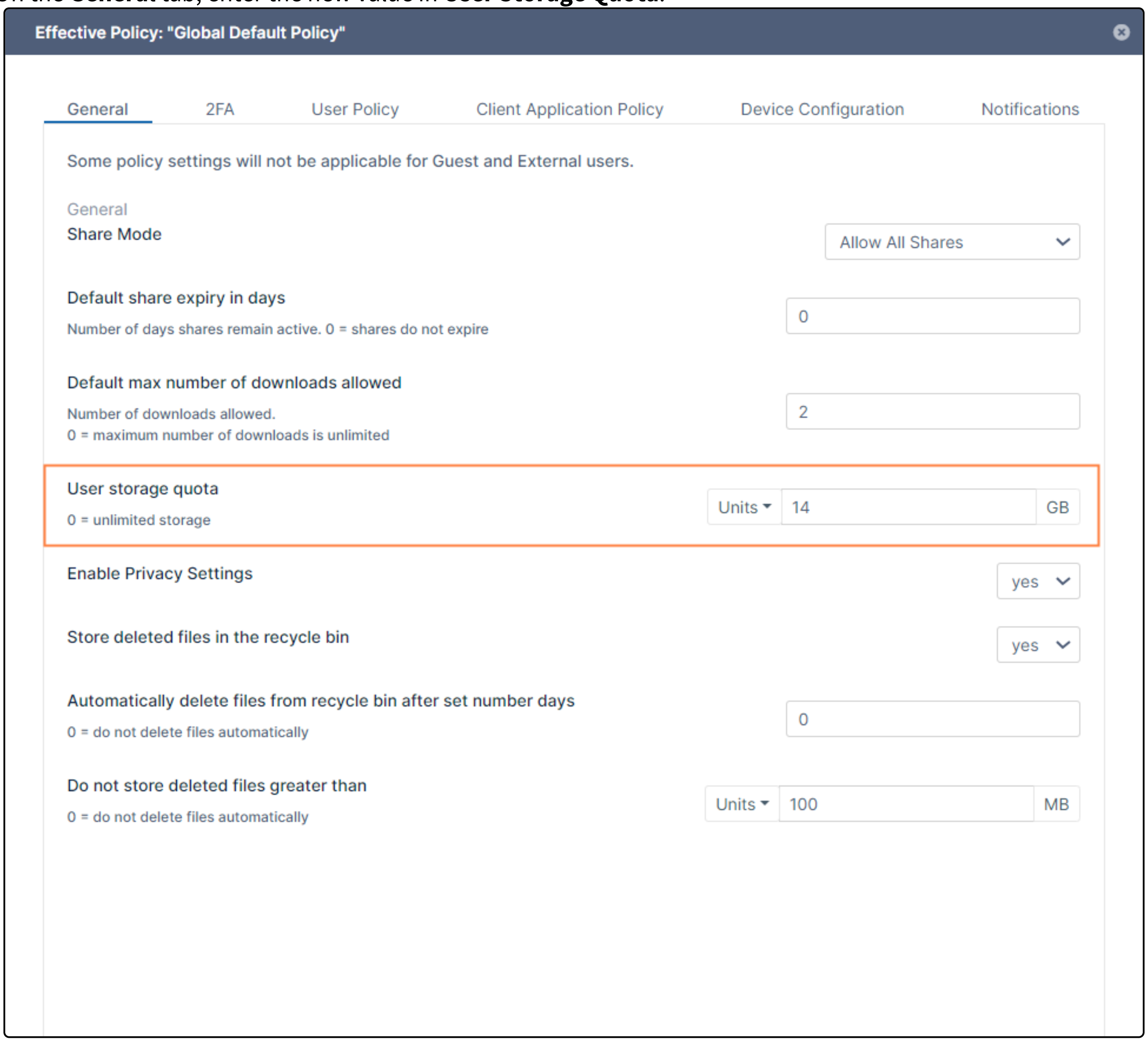
4. Click **Close**.

Set a Default Quota for All Users

To change the default storage quota, change the **User Storage Quota** in the **Global Default Policy**.

Edit the Global Policy

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
2. Click the edit icon for the **Global Default Policy**.
3. On the **General** tab, enter the new value in **User Storage Quota**.



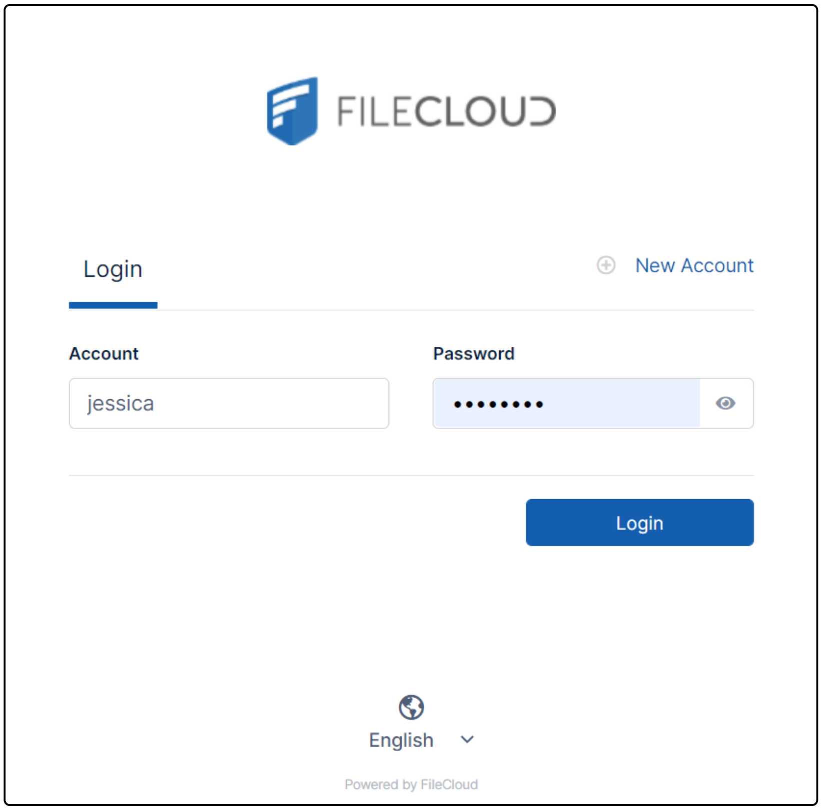
4. Click **Save**.

Enable WebDAV

WebDAV is no longer available as of FileCloud version 23.241.

Customize the User Login Screen

The following image displays the default FileCloud log-in screen, but you can customize the features that appear on it.

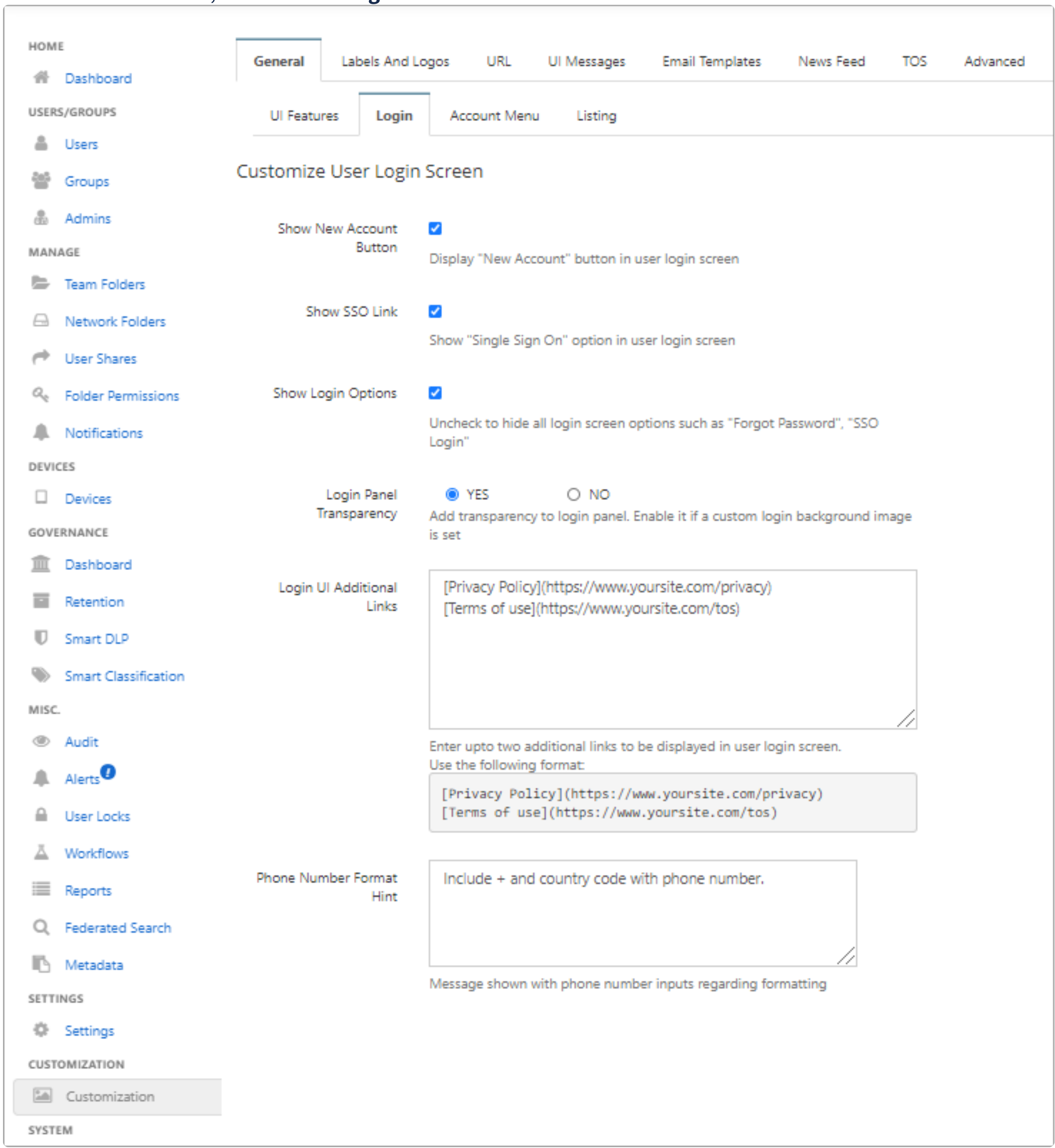


To customize the User Login screen

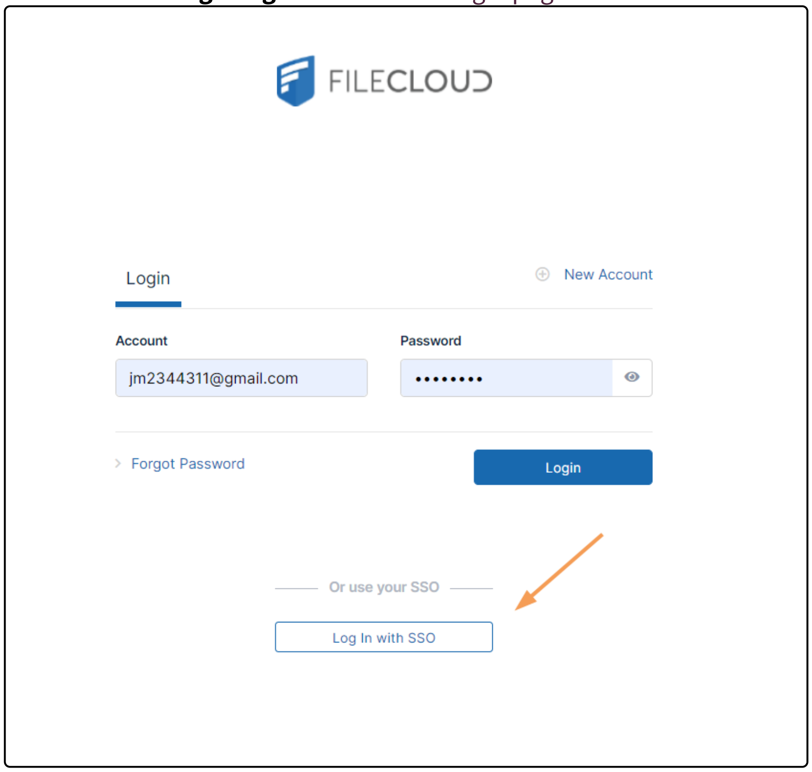
> Admin users must have Customization permissions enabled to customize the user login screen. See Managing Admin Users for more information.

1. Open a browser and log in to the Admin Portal.
2. From the left navigation pane, click **Customization**.

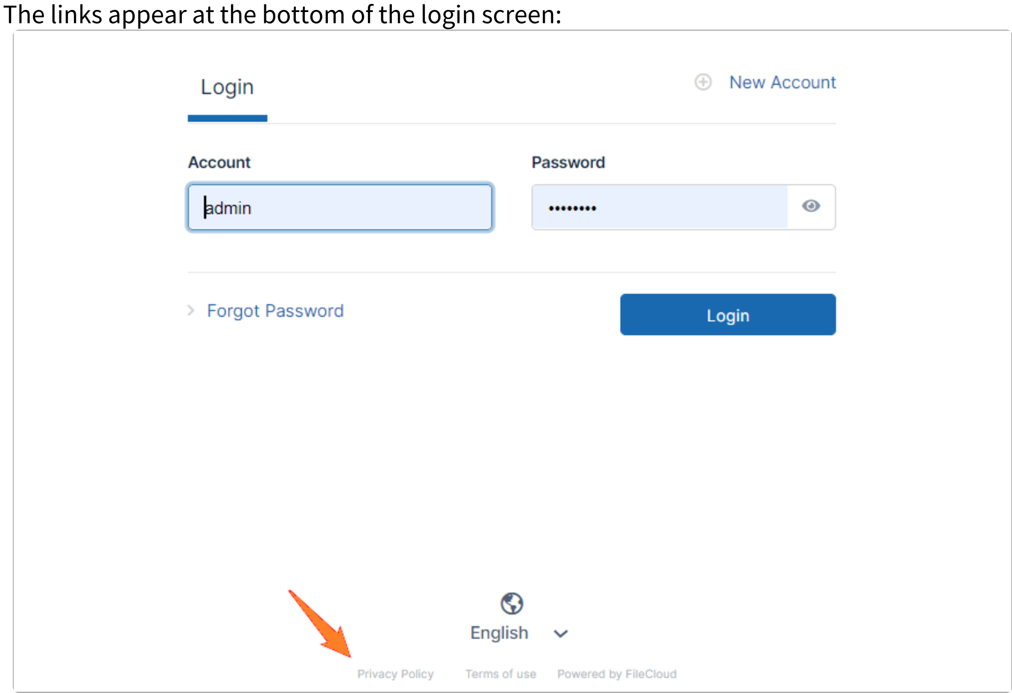
3. Select the **General** tab, and then the **Login** sub-tab.



Option	Description
Show New Account Button	Displays **New Account** button in user log-in screen. Enabled by default. The **New Account** button allows a user to create a new account for themselves, and depending on the configuration of Automatic Account Approval, have it automatically approved.

Option	Description
Show SSO Link	Check to show **Single Sign On** link in the login page:  **Note**: If this is checked, but **Show Login Options** is unchecked, **Single Sign On** link is not shown. 💡 The functionality of this button is determined by how you configure Single Sign-On Access
Show Login Options	Uncheck to hide options in login screen such as **Forgot Password** and **Single Sign On** link even if **Show SSO Link** is checked.
Login Panel Transparency	Adds transparency to login panel. Set to: • YES (default) • NO 💡 Enable this option if you are using a custom login background image.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Login UI Additional Links</td><td>Enter up to two additional links to be displayed in user login screen.
Use the format:
<code>[Privacy Policy](https://www.yoursite.com/privacy)</code>
<code>[Terms of use](https://www.yoursite.com/tos)</code>

The links appear at the bottom of the login screen:

</td></tr>
<tr><td>Phone Number Format Hint</td><td>Enter a hint to appear on screens where users can enter phone numbers. For example Include + and country code when entering phone number.</td></tr>
</table>

4. Modify the settings for any of the options.
5. To save your changes, click **Save**.

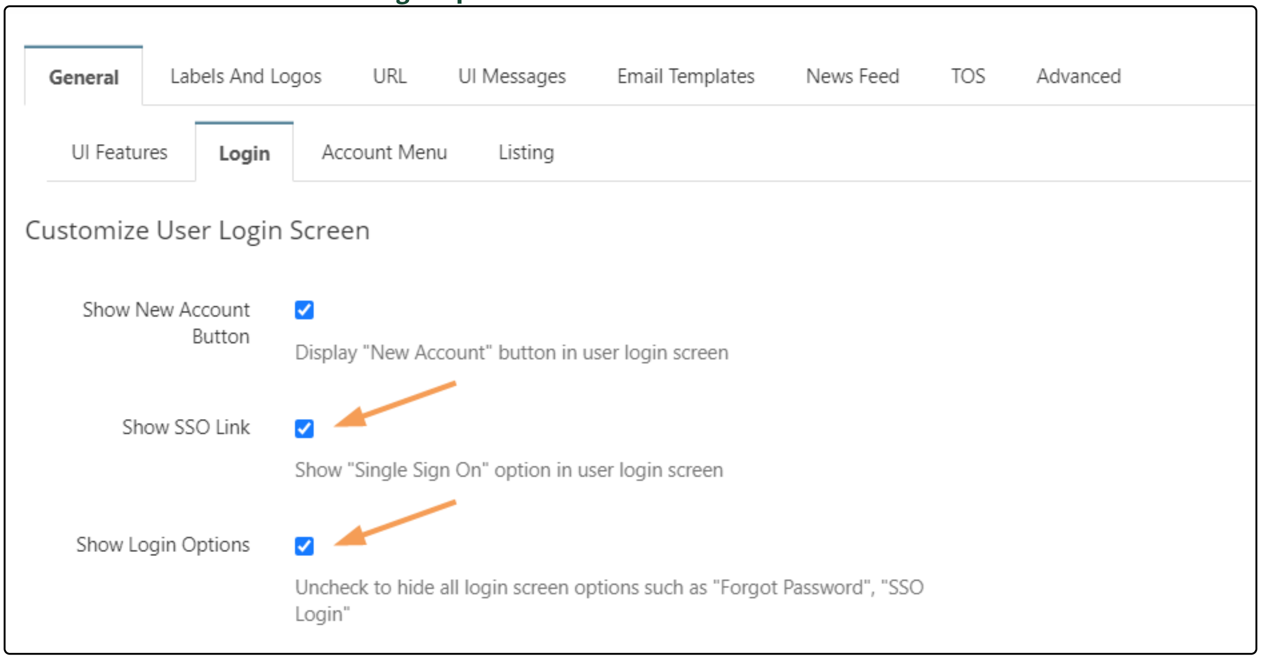
To customize for SSO log in

You can customize the user log-in screen to display the SSO log-in option along with the direct log-in option or to only display the SSO login.

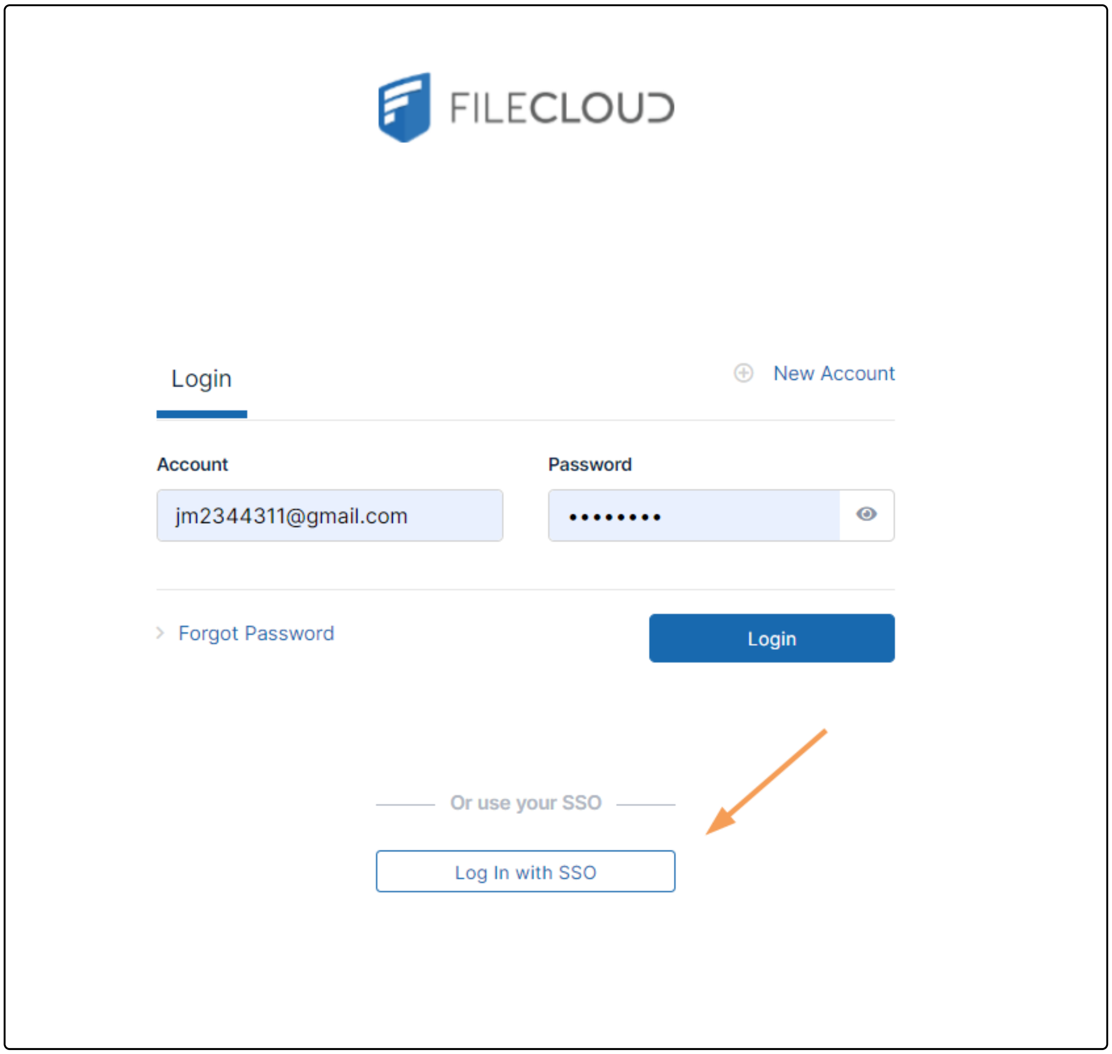
To display the SSO log-in option along with the direct log-in option:

1. From the left navigation pane, click **Customization**.
2. Select the **General** tab, and then the **Login** sub-tab.

3. Check **Show SSO Link** and **Show Login Options**.



4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



On clicking the Single Sign-On link on the login page, the user is redirected to the SAML SSO Service web page.

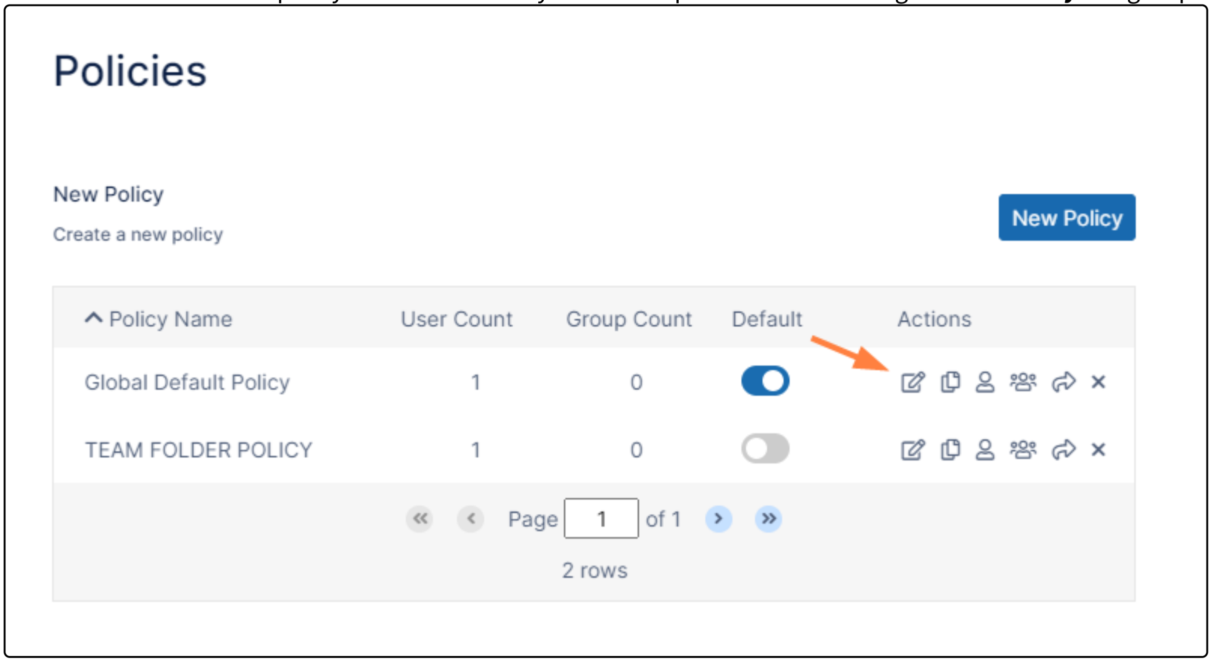
Limiting File Upload Size for Users

You can set a limit on the size of files that some or all of your users can upload into FileCloud by entering a value for **Max File Size Limit** in the users' policy or policies.

To change the **Max File Size Limit** setting:

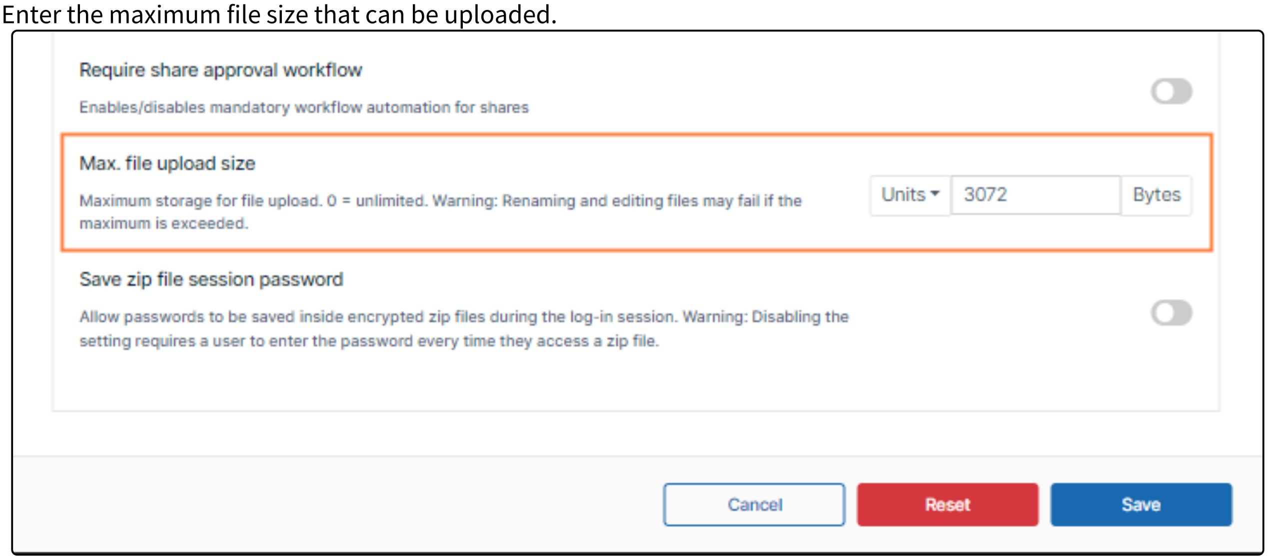
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.

2. Click the Edit icon for the policy of the users who you want to prevent from sharing with the **Everyone** group.



The **Policy Settings** dialog box opens.

3. Click the **User Policy** tab.
4. Scroll down to the **Max. file upload size** setting.
5. Enter the maximum file size that can be uploaded.



6. Click **Save**.

> **Max. file upload size** does not apply to Sync and Drive and other non-Web FileCloud clients.
>
> For help applying **Max. file upload size** to non-web FileCloud clients, please Contact FileCloud Support.

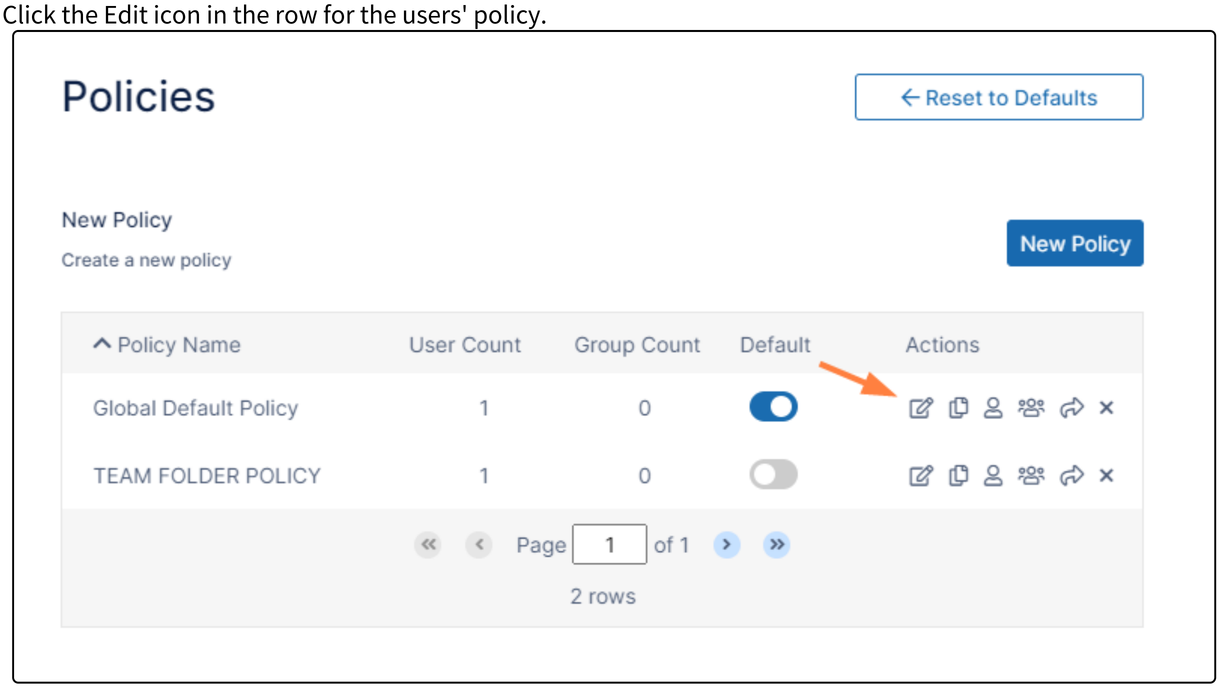
Disabling Send for Approval

> The ability to request file approval is available beginning in FileCloud 21.2.
> Beginning with FileCloud 23.241.6:
> - The **Disable Send for Approval** option is available.
> - The file approval option is not available for External users and users who do not have access to share a file.

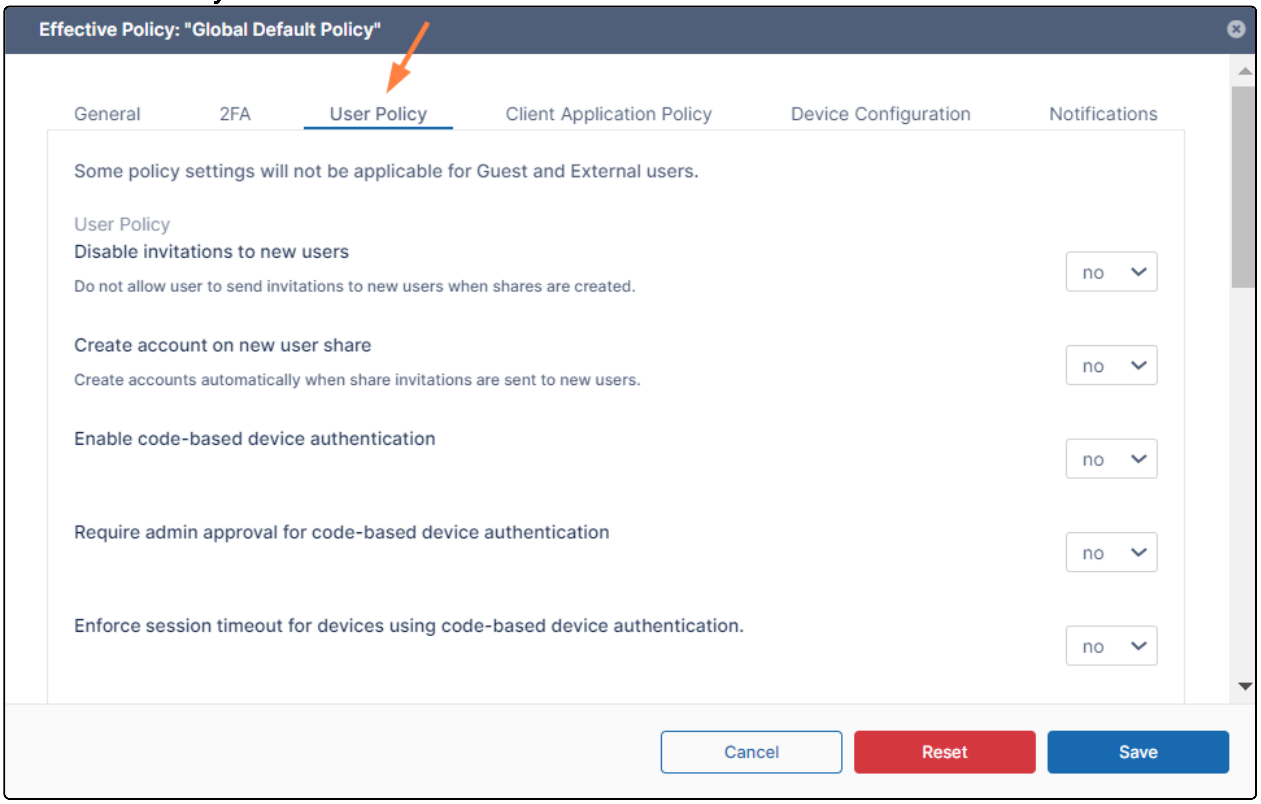
You can remove the ability for a group of users to send files for approval by through their policy.

To disable Send for Approval:

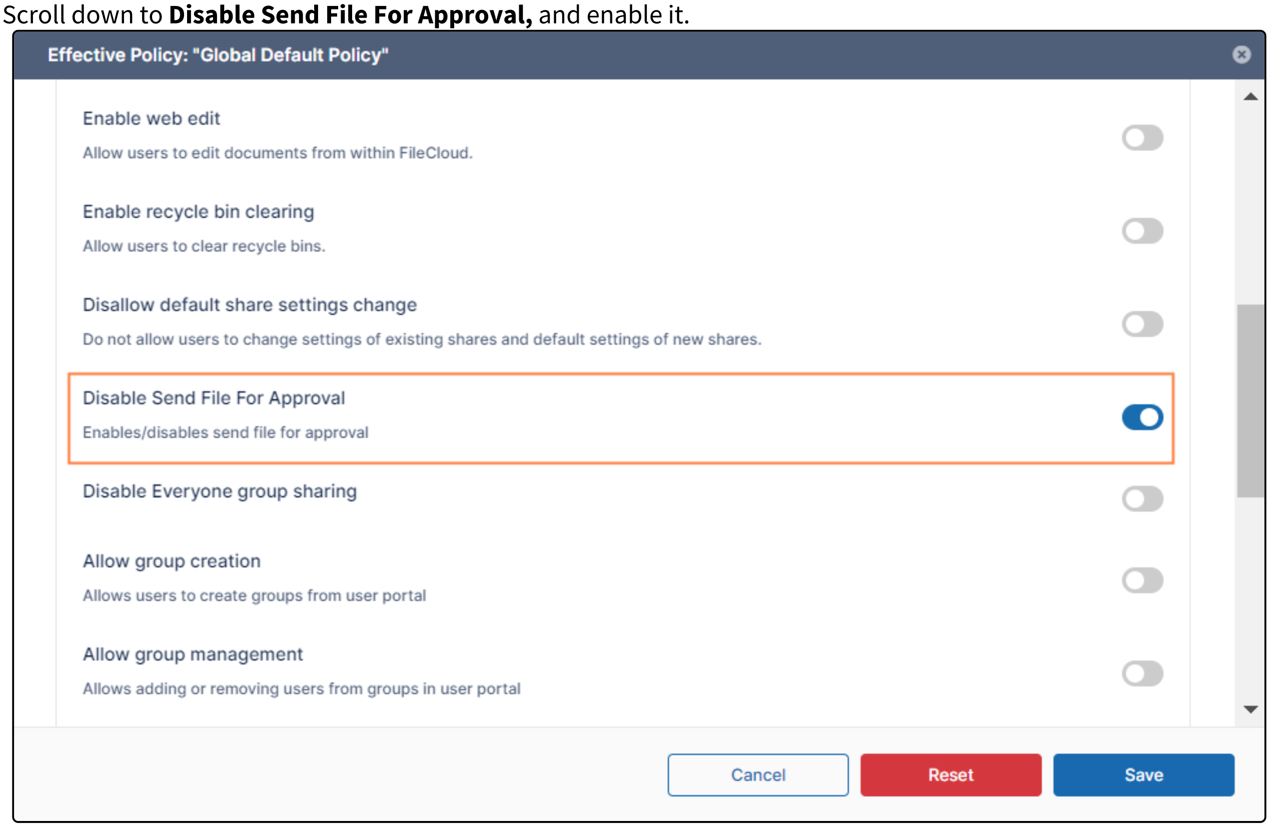
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



3. Click the **User Policy** tab**.**



4. Scroll down to **Disable Send File For Approval,** and enable it.



5. Click **Save**.

Group Settings

The addition of the Externals group and the removal of External users from the Everyone group is effective beginning in FileCloud 23.252.

The feature for importing groups from an SSO provider is available in FileCloud 23.251 and later.

Administrators can create groups of users in FileCloud Server. Creating groups allows sharing of files and folders for multiple users.

The automatic groups **Everyone** and **Externals** are created by default for every FileCloud installation.
The **Everyone** group contains all Full and Guest users. External users are not included in the **Everyone** group**.**
The **Externals** group contains all External users.

Groups may contain the following attributes

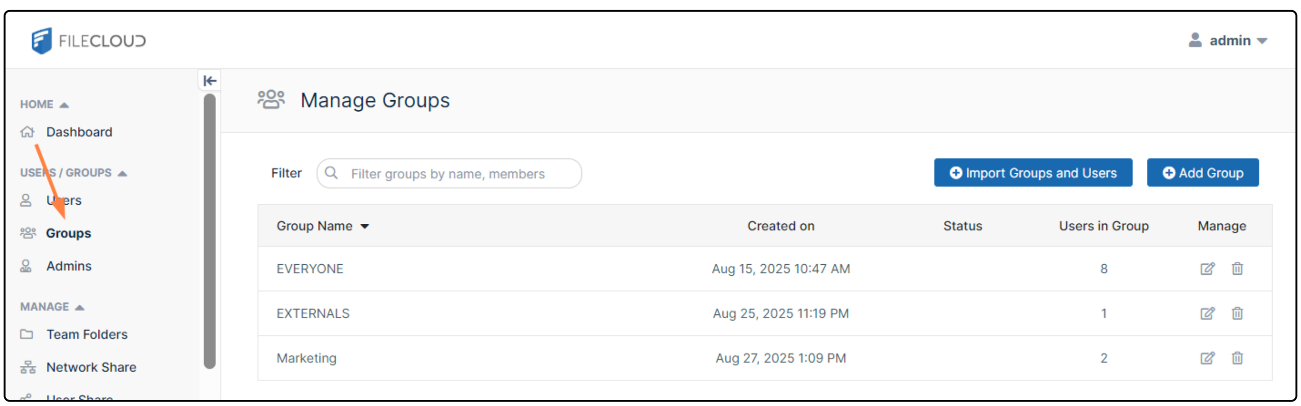
- **Group Name** - Name assigned by the administrator
- **Group Members** - List of users that are part of the group
- **Group Admins** - (optional) Users with the ability to view users, add users, and/or remove users from the group.
- **Group Policy** - The policy that applies to all members of the group. By default, the **Global Default Policy** is assigned.

Once a group is created, it can be populated with users using one of the following methods:

- Manually adding users that are already in the FileCloud system.
- Importing members of a group from an external AD server.
- Importing members of a group from an external SSO provider.

Show me where to manage groups in the Admin Portal

To manage groups, in the navigation panel, click **Groups**.

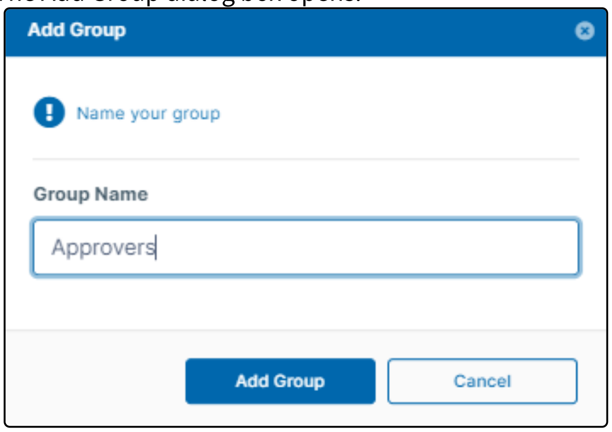


What do you want to do?

Manually create a FileCloud Group

To create a group:

1. Open a browser and log on the admin portal.
2. On the left control panel, click **Groups**.
3. Click the **Add Group** button.
   The Add Group dialog box opens.



4. Click **Add Group**.
5. The group is added, and the **Manage Group** dialog box opens.

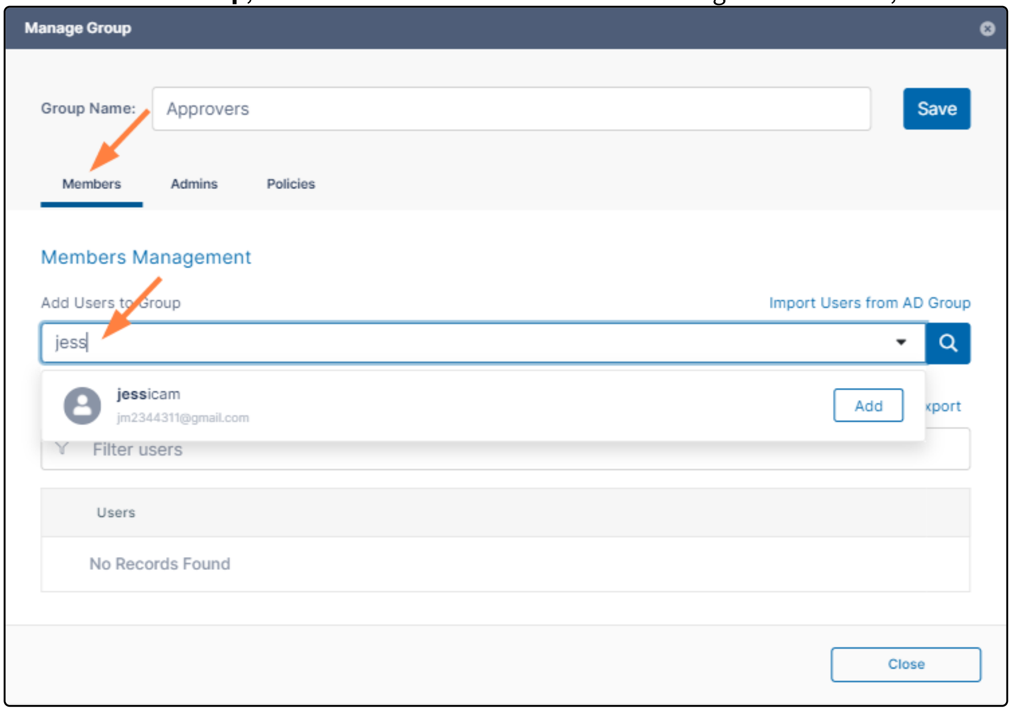
Add FileCloud Users to a Group

This method requires the user accounts to already exist in your local FileCloud Server.

To add FileCloud users to a group:

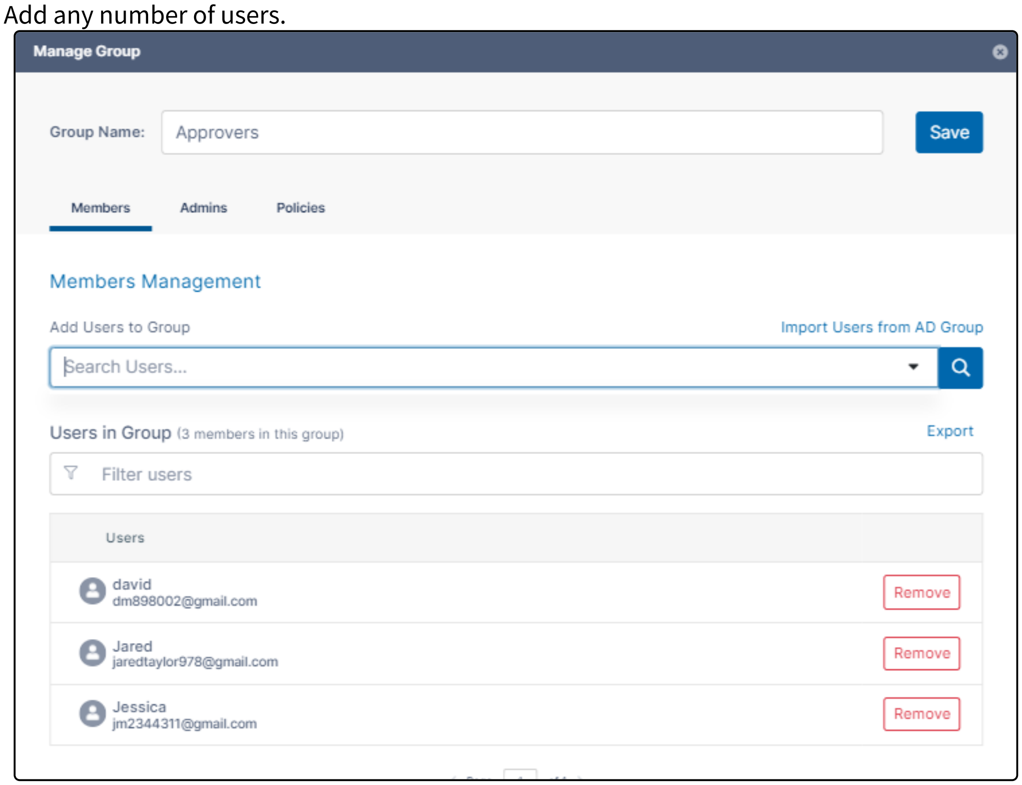
1. In the navigation panel, click **Groups**.
2. Click the Edit icon next to the group that you want to add members to..
3. If it is not already selected, click the **Members** tab.

4. In **Add Users to Group**, enter the username or email of an existing FileCloud user, and click **Add**.



The user is listed under **Users in Group**.

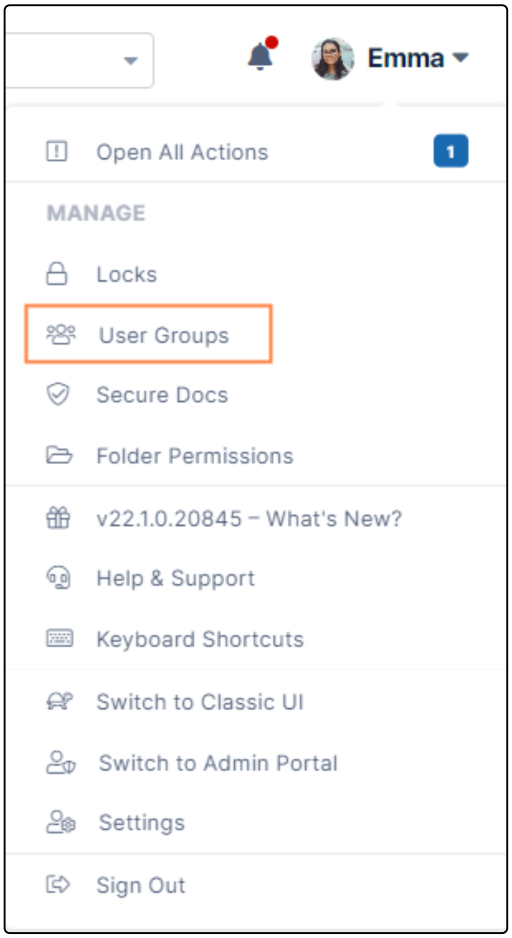
5. Add any number of users.



6. Either click **Save** to save the new members in the group, or click the **Admins** or **Policies** tab to further configure the group.

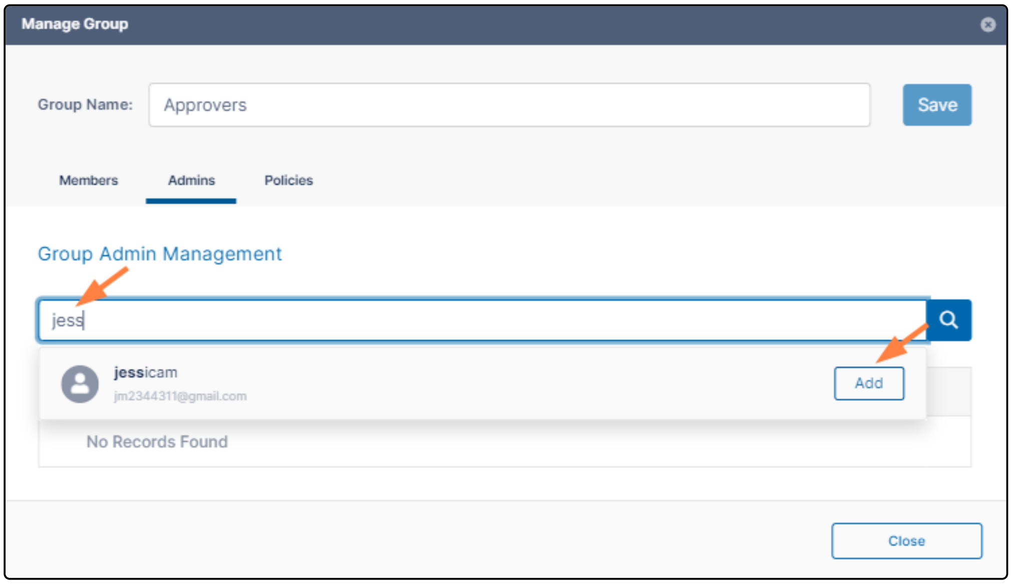
Add Group Admins

You can assign users to be admins of a group and give each group admin access to view, add, and/or remove users from the group.
A user's policy also may enable them to add and/or remove users from groups. See Giving Users Group Management Permissions for more information. If either a user's group admin access or policy settings gives the user the permission to add or remove users from a group, the user has that ability, and can manage user groups in the user portal by expanding the user drop-down list and clicking **User Groups**:



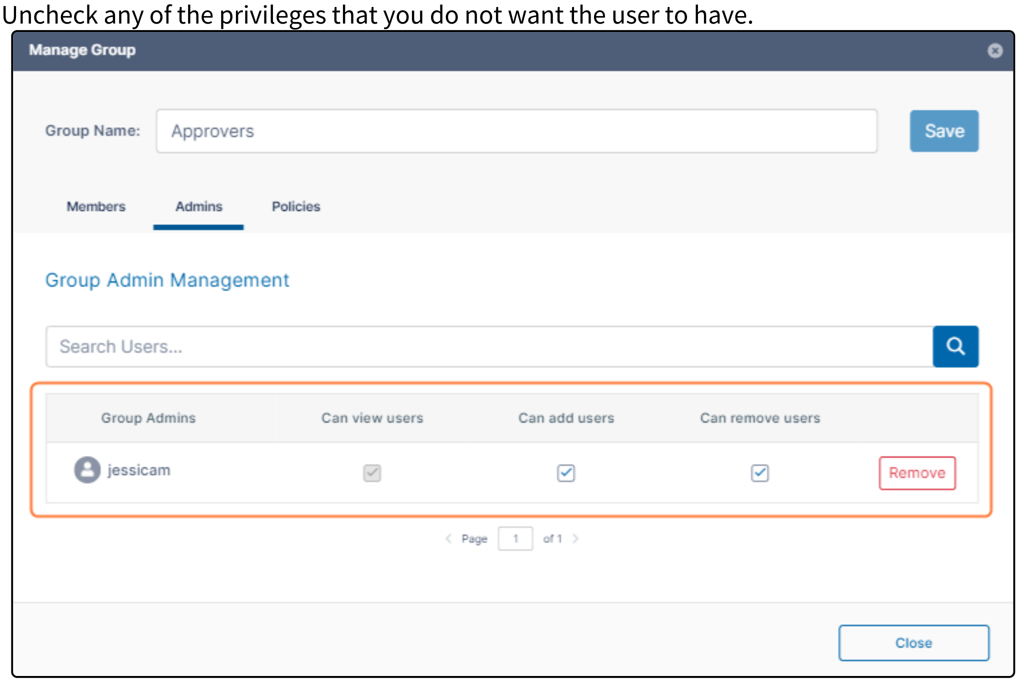
To Add Group Admins:

1. If you are not already inside the **Manage Group** dialog box, open it by clicking the Edit icon next to the group.
2. Click the **Admins** tab.
3. In the search box, enter a user that you want to add as an admin, and click **Add**.
   The user does not have to be a group member, but must be a current FileCloud user with Full or Guest status.



The user is listed under Group Admins with **Can view users**, **Can add users**, and **Can remove users** checked by default.

4. Uncheck any of the privileges that you do not want the user to have.



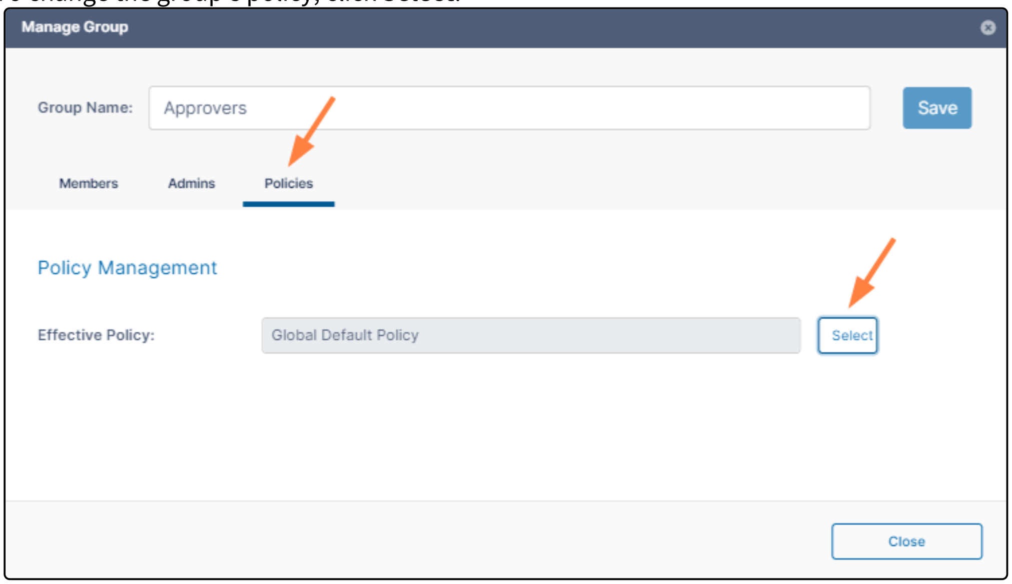
5. Add any number of admins and set their privileges.
6. Either click **Save** to save the admins, or click one of the other tabs to further configure the group.

Change a Group's Policy

Members of a group have both their user policy and the group's policy. For each setting the user has the greatest access given in either policy.

By default, your groups are assigned the **Global Default Policy**. You can change that default when you initially create the group or later by editing it.

To change a group's policy:

1. If you are not already inside the **Manage Group** dialog box, open it by clicking the Edit icon next to the group.
2. Click the **Policies** tab.
3. To change the group's policy, click **Select**.


A list of policies opens.
4. Click a policy, and then click **Select**.
5. Click **Save**, and click **Close**.

Import Active Directory Users to a FileCloud Group

You can also import an existing AD group from an Active Directory Server connected to FileCloud.

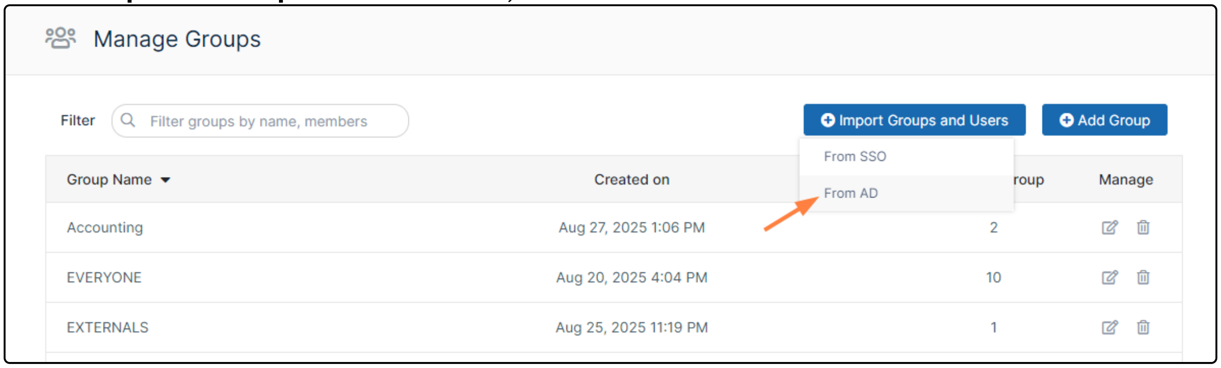
During AD import, if a user is not in the AD group, the account is not removed automatically from the FileCloud group. This logic is based on the scenario where an administrator manually adds other FileCloud users to the FileCloud group who are not in the AD group, and those users should not be removed. However, there is now an option for an enterprise that uses a large number of temporary workers, such as a construction company that uses a large number of contractors. If they import a large number of users based on groups, when a contractor is no longer employed, and therefore not a member of the AD group any more, the admin can now select a checkbox on the **AD Group Members Import** dialog box called **Remove Members.** This allows admins who need to remove accounts on import to do so automatically. If you have manually created users that you don't want deleted but aren't a member of a group any longer, then you would not select this option.

You must set up and verify Active Directory Settings before completing the following steps.

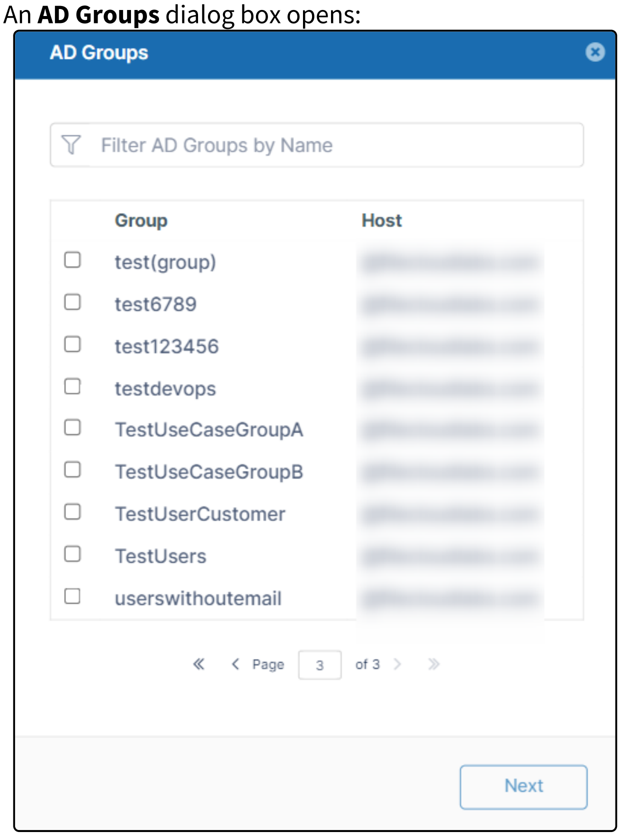
To add AD users to a FileCloud group:

1. Open a browser and log in to the admin portal.
2. On the left control panel, click **Groups**.

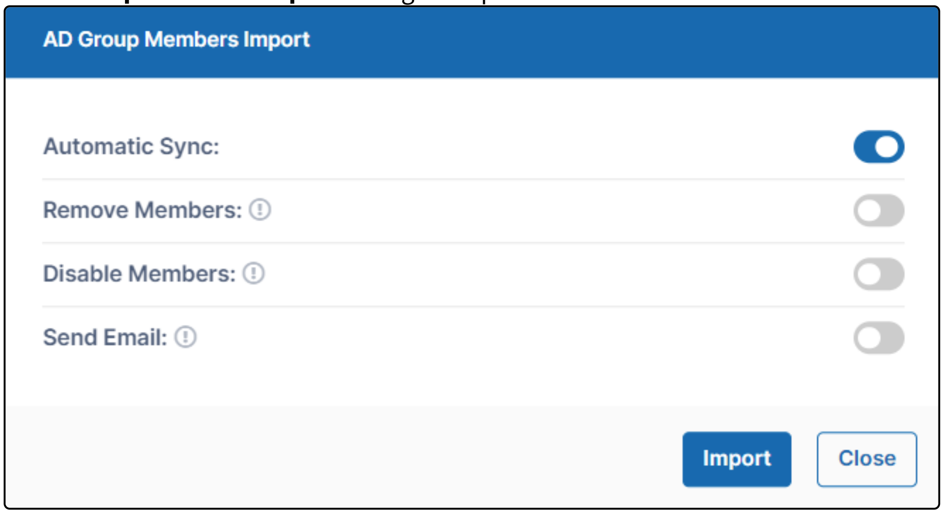
3. Click the **Import AD Groups and Users** button, and choose **From AD**.



An **AD Groups** dialog box opens:

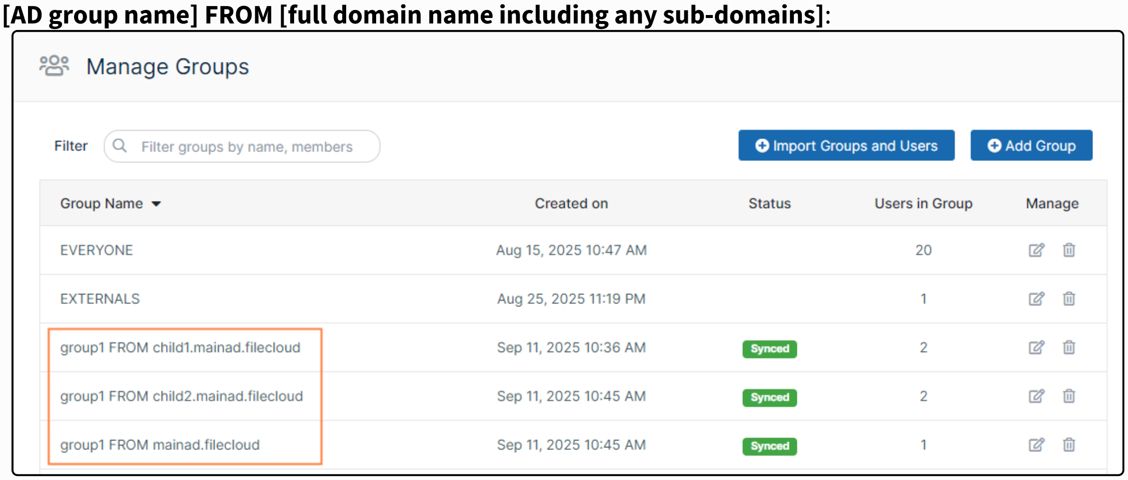


4. Check the groups you want to import, and click **Next**.
   An **AD Group Members Import** dialog box opens.



5. **Automatic Sync** is selected by default. Leave it selected to enable FileCloud to automatically add users to the FileCloud group that are added to the AD group. This sync is done every 24 hours.
   - The first time members from the AD group are imported as members of the FileCloud Group.
   - In the future, new members added to the AD group are synced automatically to the FileCloud group.
6. Select any of the other options:
   - **Remove Members** - Enable FileCloud to remove members from the group f they are no longer in the AD group.
   - **Disable Members** - Enable FileCloud to disable members in FileCloud as users if they are disabled in the AD group.
   - **Send Email -** Enable FileCloud to send email to members of the AD group telling them they have been added to the FileCloud group.
7. To import the users from the AD group, click **Import**.
   If you do not have **Automatic Sync** enabled, rerun this operation at any time to add new members from the AD group into the FileCloud group.

If the Enable multiple AD domains setting is enabled, the imported group's name in FileCloud is:
[AD group name] FROM [full domain name including any sub-domains]:



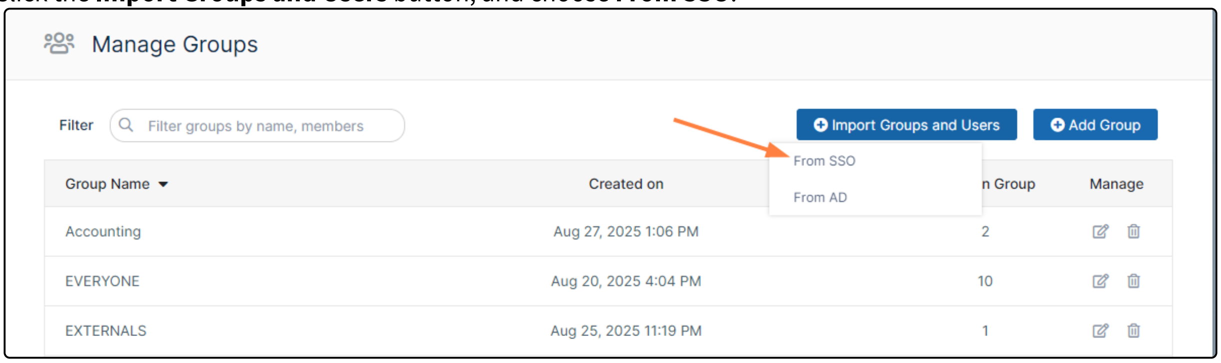
Import SSO Users to a FileCloud Group

You may configure FileCloud to import groups and users from the OKTA, Google, and Azure SSO providers. See Import Groups and Users from an SSO Provider for configuration instructions.

By default, the users are not placed into their groups when they are imported into FileCloud, but you may enable a setting to enable this function. Note that you cannot import SSO users into FileCloud separately from their groups.

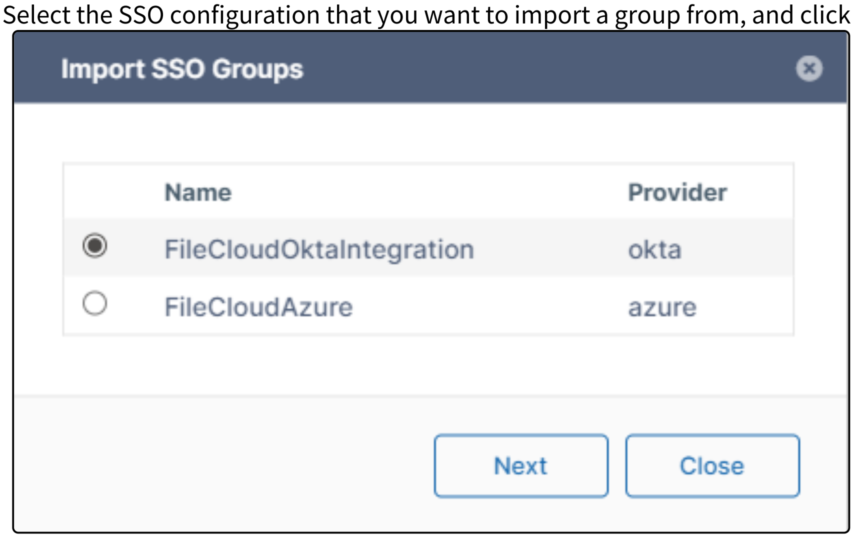
To import an SSO group into FileCloud:

1. In the admin portal, in the navigation panel, click **Groups**.
2. Click the **Import Groups and Users** button, and choose **From SSO**.

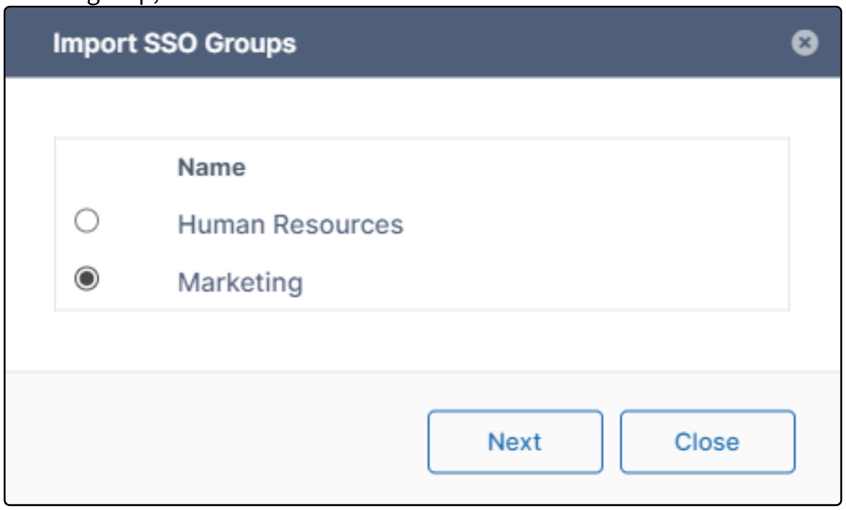


An **Import SSO Groups** dialog box opens.

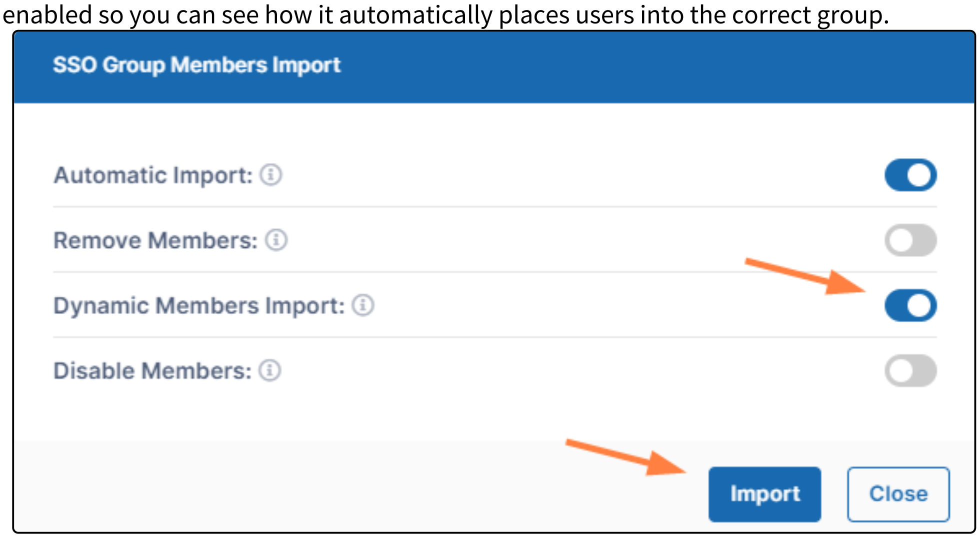
3. Select the SSO configuration that you want to import a group from, and click **Next**.



4. Select a group, and click **Next**.



5. Enable or disable the options for the import.
Automatic Import is enabled by default. In this example, the option **Dynamic Members** Import is also enabled so you can see how it automatically places users into the correct group.

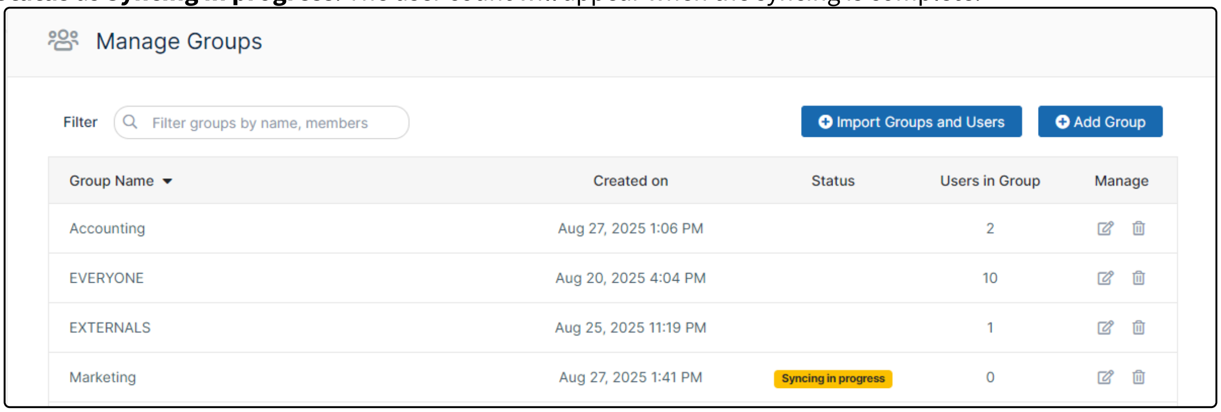


The options function as follows:

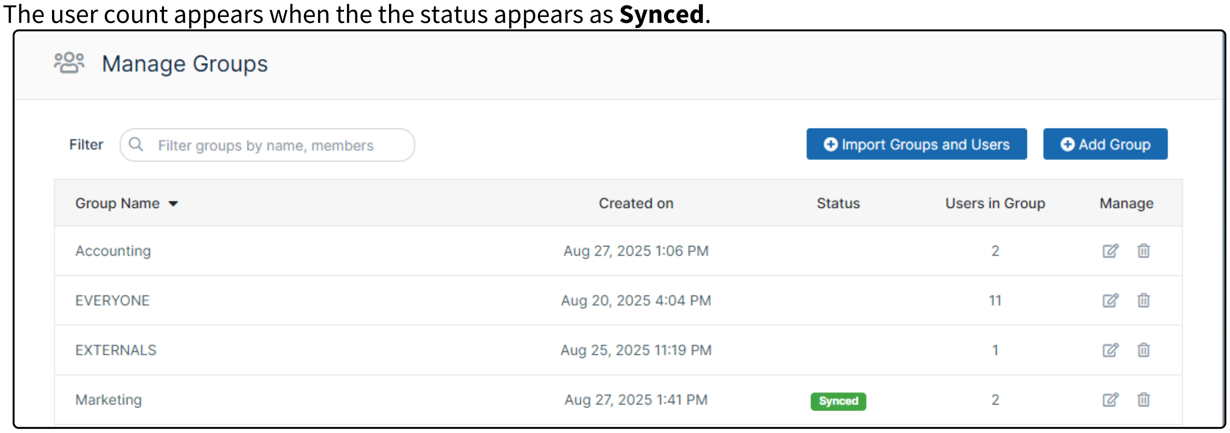
Automatic Import	Enabled by default. FileCloud periodically imports new users from the group in the SSO provider to the group in FileCloud.
Remove Members	Disabled by default. The group and its permissions are imported without its users. When a member of the group logs into FileCloud for the first time,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

Disable Members	Disabled by default. FileCloud users that are disabled in the SSO group are also disabled in the FileCloud group.

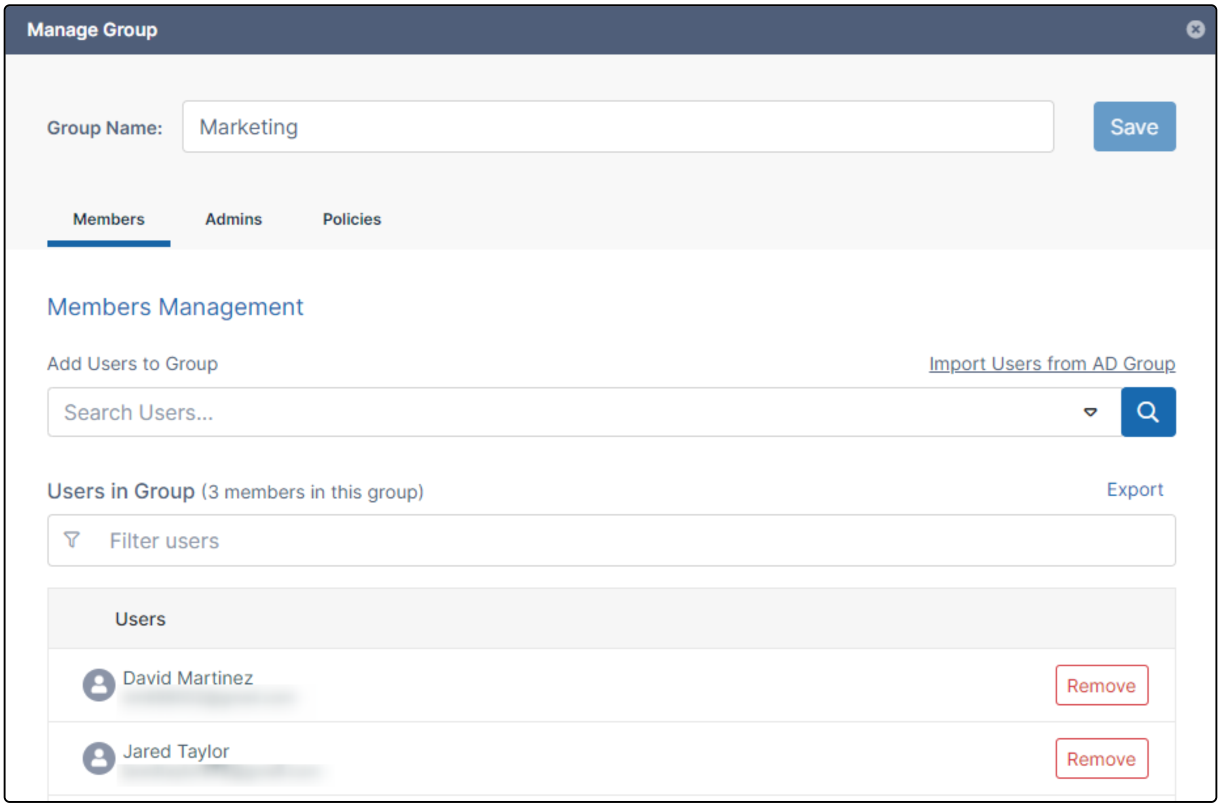
6. Click **Import**.
   Although **Dynamic Members Import** is selected, the group initially shows 0 users (members) and shows the **Status** as **Syncing in progress**. The user count will appear when the syncing is complete.



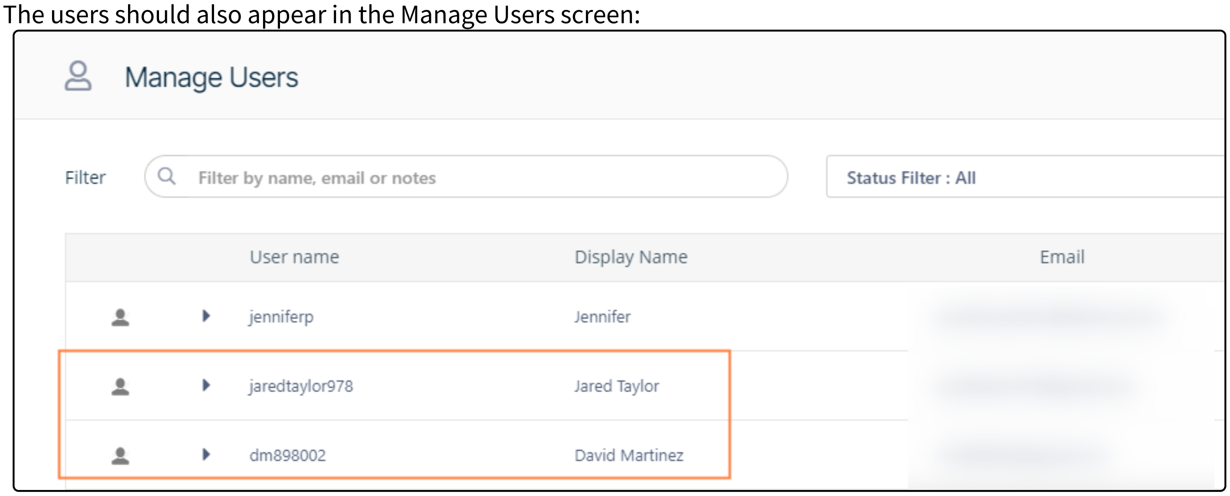
The user count appears when the the status appears as **Synced**.



Click the edit icon for the group to see which users were imported and placed into the group (because **Dynamic Members Import** was selected):



The users should also appear in the Manage Users screen:

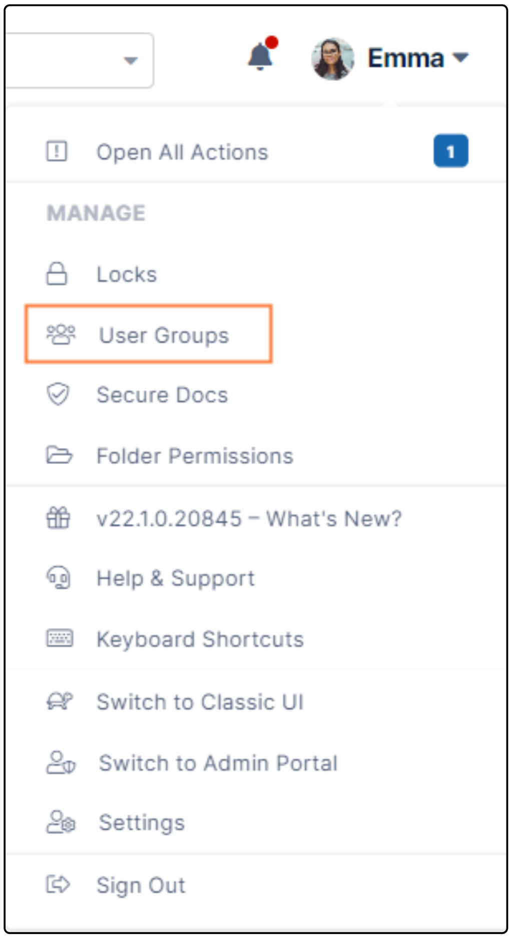


Giving Users Group Management Permissions

You can give users permission to add, edit, and delete groups by assigning them a policy that enables group permissions.

You can also give them permission to view, add members, or delete members for a specific group in the settings for the group. See Group Settings for more information about these types of settings.

When users have either group permissions through their policies or through settings for a group, they have access to the **User Groups** option in the user portal:

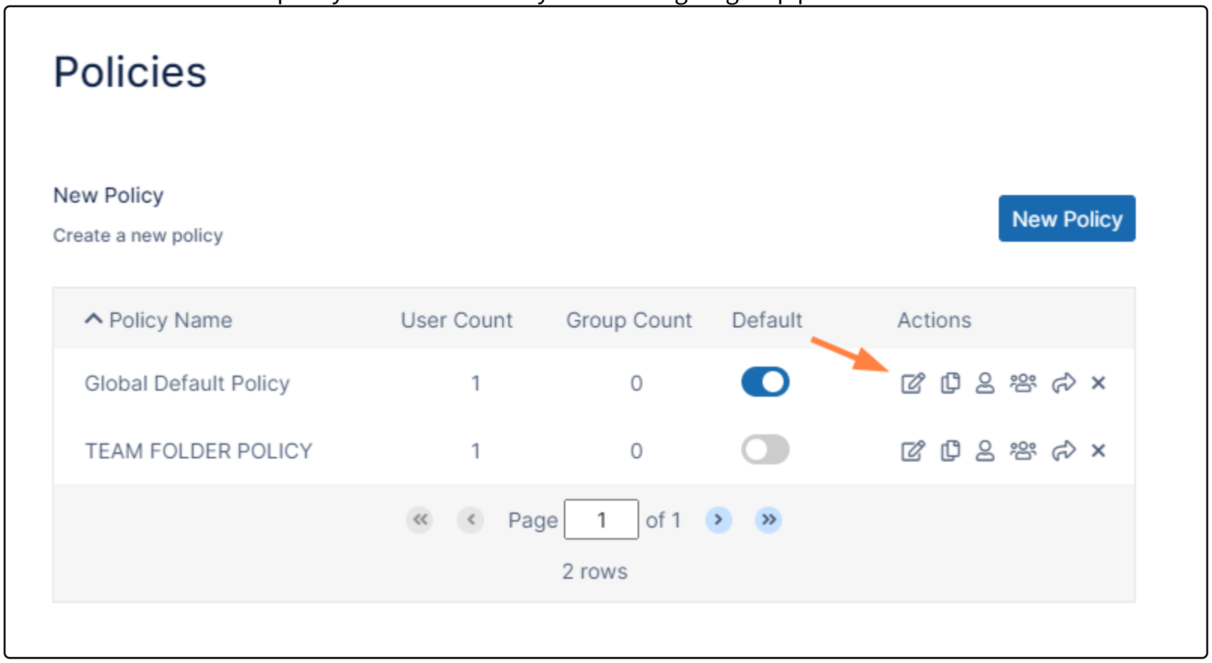


For more information on user management of groups, see User Groups.

To add group permissions to a policy:

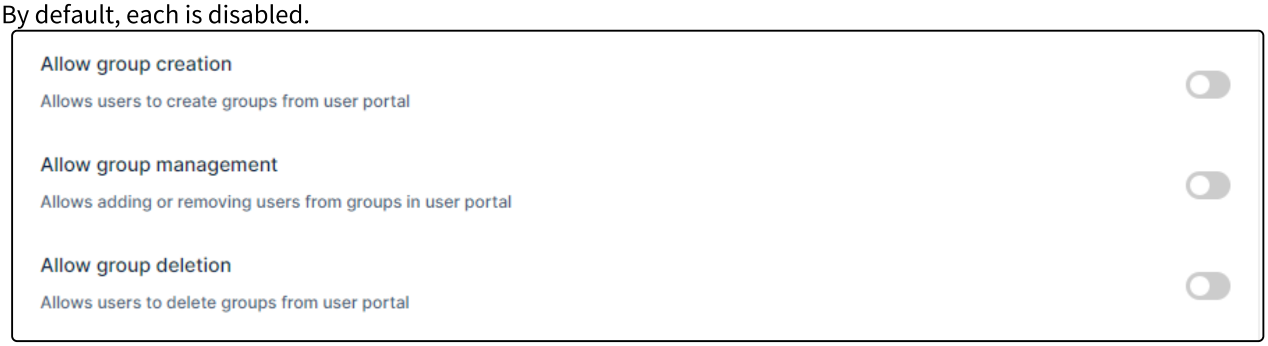
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.

2. Click the Edit icon for the policy of the users who you want to give group permissions.



The **Policy Settings** dialog box opens.

3. Click the **User Policy** tab.
4. Scroll down to see the Group policy settings.
   By default, each is disabled.



5. Change the group settings that you want to enable for users with this policy.
   - **Allow group creation** - Allows the user to add new groups and manage members in the groups from the user portal.
   - **Allows group management** - Allows the user to add and remove members from any group, including groups they have not created, from the user portal. This gives the user the ability to add and remove group members to groups created in the admin portal as well as groups created in the user portal.
   - **Allow group deletion** - Allows the user to delete any groups, including groups they have not created, from the user portal. This gives the user the ability to delete groups created in the admin portal as well as groups created in the user portal.

   If none of these settings is enabled, users with the policy do not see the **Manage User Groups** option in the user portal unless group access is enabled for individual groups. See Group Settings.

Admin User and Role Settings

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

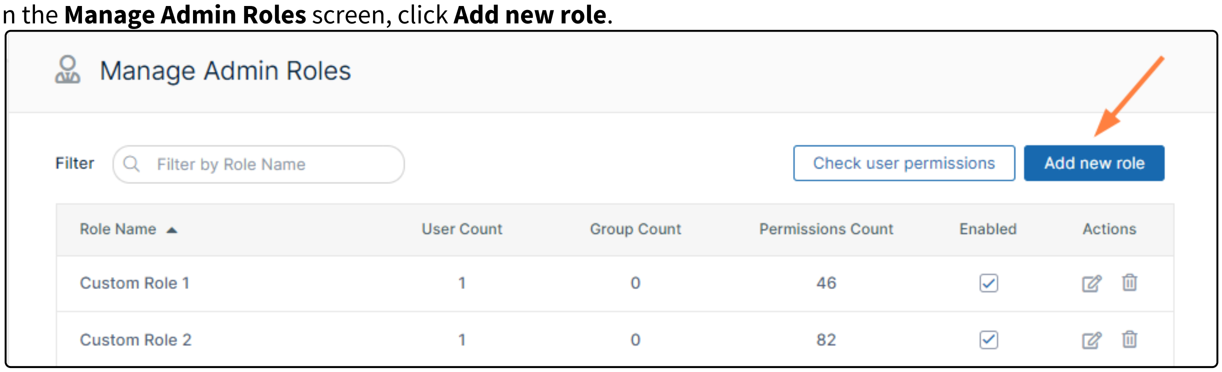
Main Admin. The admin account that is created when FileCloud is installed. There is only one Main Admin account in FileCloud.

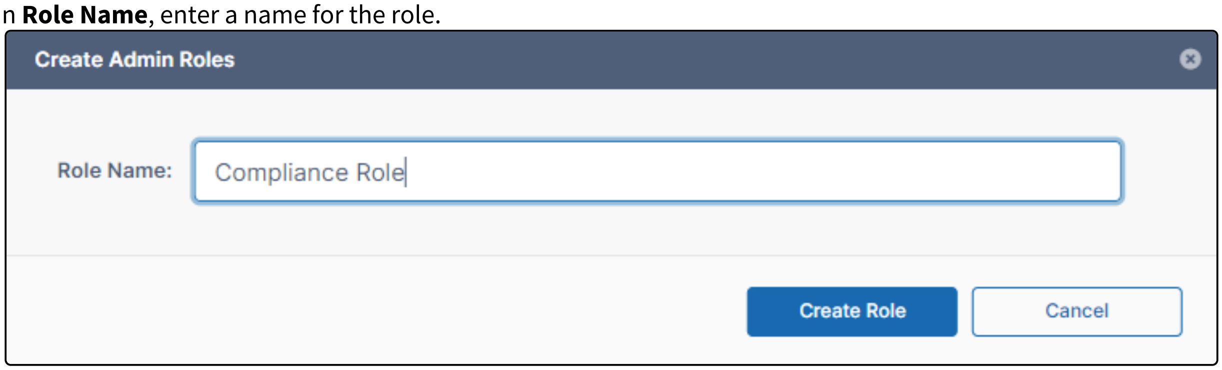
Admin User. User accounts that can access the FileCloud admin interface.

Admin Role. Role that defines the set of admin permissions for an admin user. If admin users have multiple admin roles, they have the combined admin permissions of all of the roles. For instructions on checking an admin user's permissions, see Managing Admin Users.

Creating admin roles and adding admin users

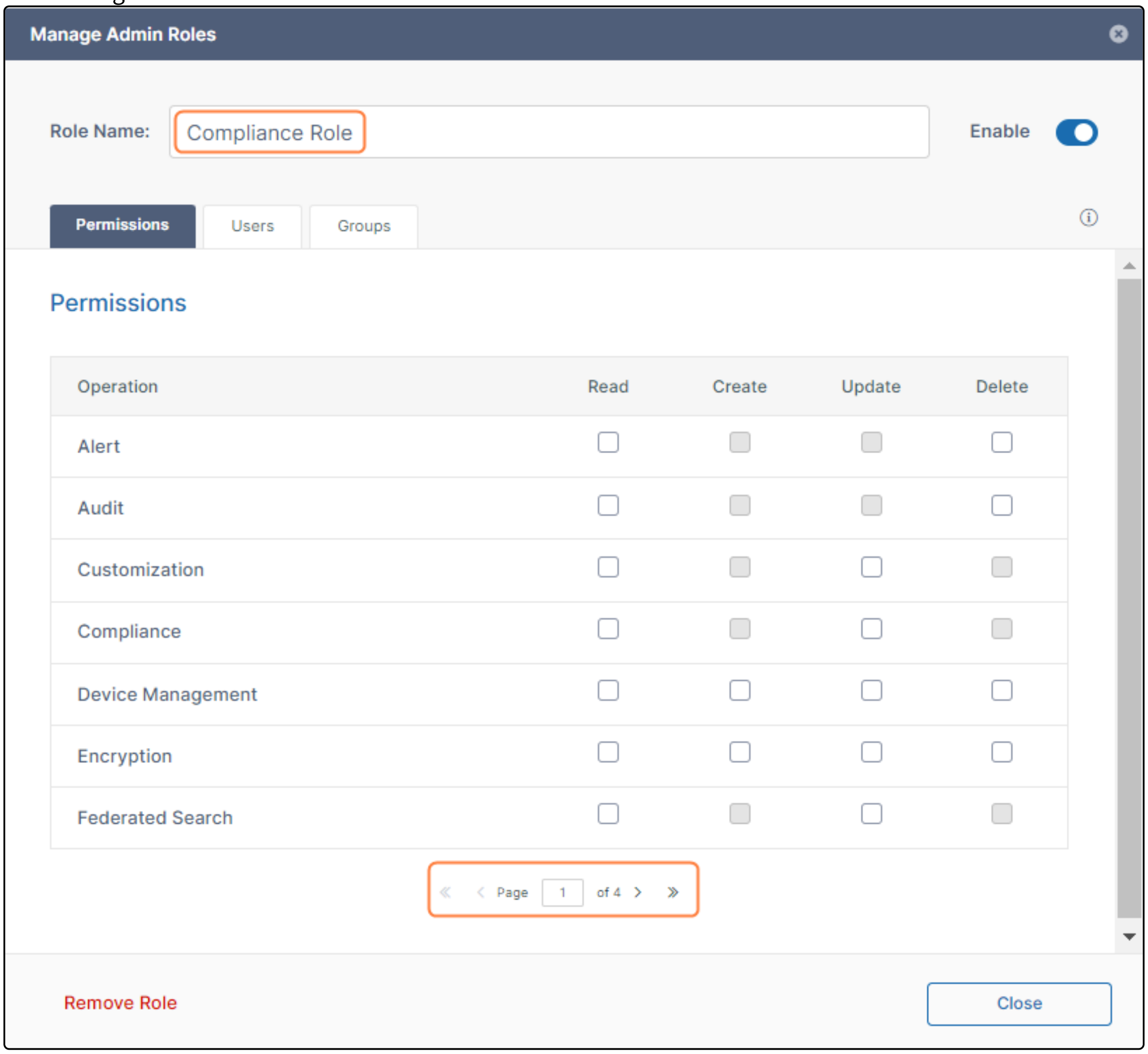
To create admin roles and add users to them:

1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Add new role**.


The **Create Admin Roles** dialog box opens.
3. In **Role Name**, enter a name for the role.


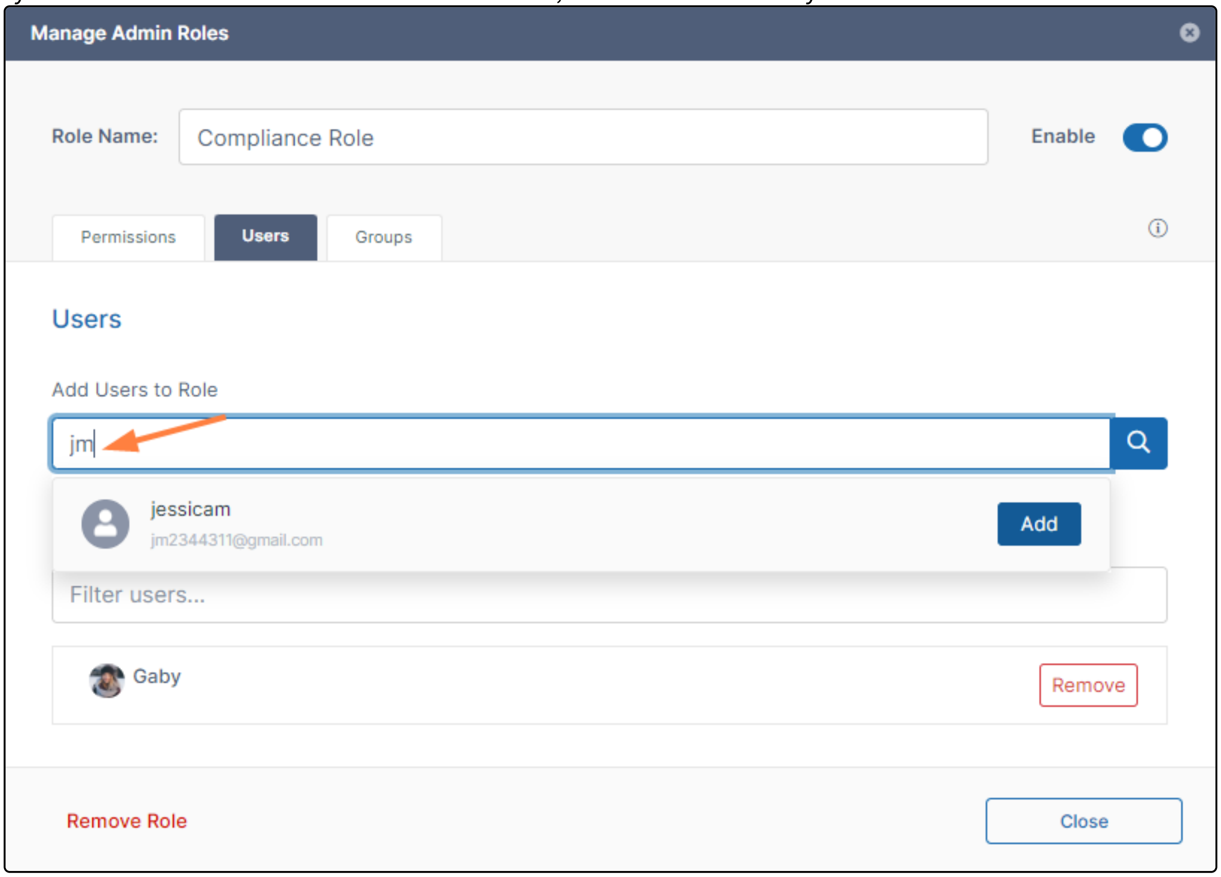
4. Click **Create Role**.
The **Manage Admin Roles** dialog box opens to the first page of permissions. The new role is listed at the top

of the dialog box.



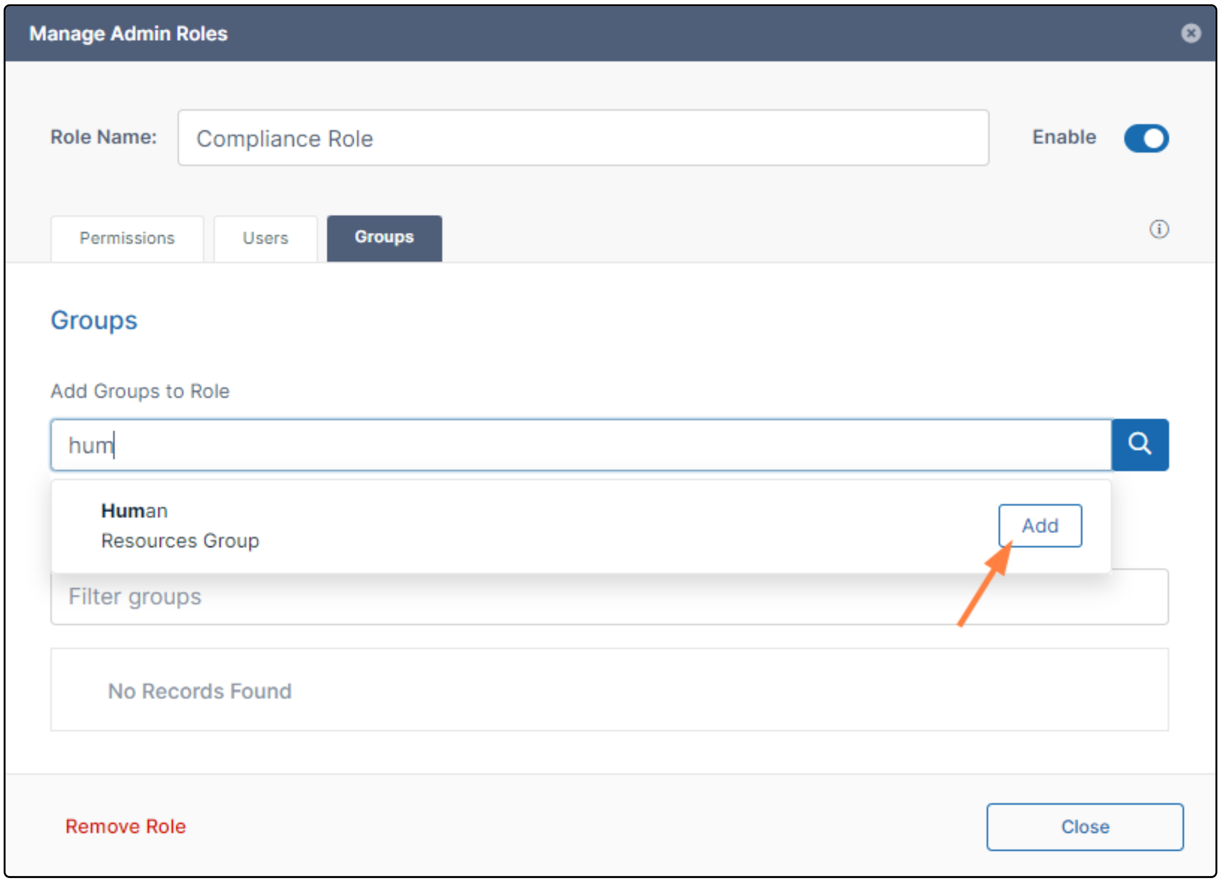
5. Go through each page of permissions, and check the permissions that you want to make available to the role.
6. When you have finished assigning permissions to the role, click the **Users** tab if you are ready to assign users to the role.
7. In **Add Users to Role**, enter each user that you want to add to the role. When the name appears, click **Add**. You can add **Full** and **Guest** users to roles, but not **External** users.

If you add a user who is not an admin user to a role, the user automatically becomes and admin user.

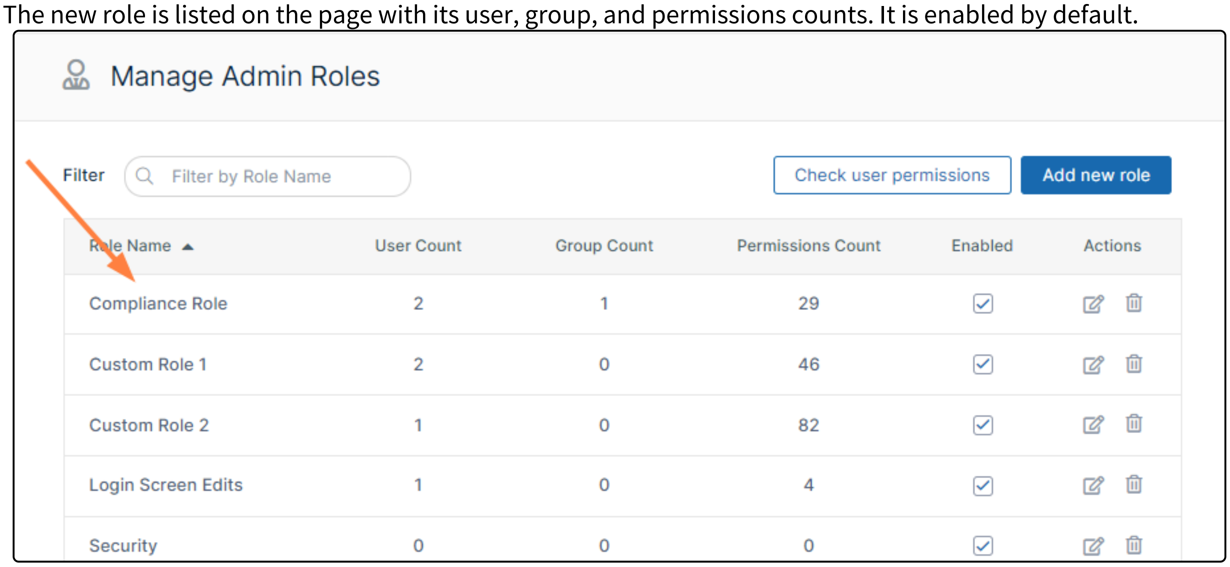


8. To add groups to the role, click the **Groups** tab.
9. In **Add Groups to Role**, enter each group that you want to add to the role. When the name appears, click **Add**.
   Any users in a group who were not admin users automatically become admin users after the group is added

to the role.



10. Click **Close**.
The new role is listed on the page with its user, group, and permissions counts. It is enabled by default.



For instructions on removing an admin role, see Managing Admin Users.

Definitions of Permissions

The following permissions represent functions that admin users may be permitted to perform.

Operation	Description
Alert	Alert item on the admin interface is visible. Authorization to view and clear alerts in admin interface.
Audit	Audit item on the admin interface is visible. Authorization to view, delete and export Audit Records.
Compliance	Compliance Dashboard on the admin interface is visible. Authorization to view and update compliance settings.
Customization	Customization item on the admin interface is visible. Authorization to customize the FileCloud interface. **Note**: Admin users must have **Customization > Update** enabled to be able to change the user login background.
Device Management	Devices item on the admin interface is visible. Authorization to view, create, delete and update Devices.
Encryption	Authorization to manage all Encryption at Rest settings.
Federated Search	Support to perform federated search through the admin interface.
Files	Manage Files. Authorization to view, dreate, modify, download, and delete user files.
Folder Permissions	Manage Folder Level Permissions. Authorization to view and manage Folder Permissions.
Groups	Groups menu item on the admin interface is visible. Authorization to view, create, modify and delete Groups. Manage group members. Import group members from Active Directory.
Locks	View , create, and delete Locks on Files and Folders in FileCloud.
Manage Administrators	Allows promoted admin users to manage the permissions of other promoted admin users.
Metadata	View, create, update and delete metadata set definitions, attributes and permissions.

Operation	Description
Mini Admin	View allows promoted users to open mini admin and perform all permitted actions except adding users. Create allows promoted users to open mini admin and perform all permitted actions including adding users.
Network Share	Network Folders item on the admin interface is visible. Authorization to view, create, modify and delete Network Folders. Manage User and Group Access to Network Folders.
Notifications	Notifications menu item on the admin interface is available. Add, edit, update, and delete notification rules.
Reports	Reports menu item on the admin interface is available. Add, execute, edit and delete reports.
Retention	Retention menu item on the admin interface is available. Add, edit, and delete retention policies.
Rich Dashboard	View rich dashboard view including tables and graphs on the admin UI dashboard.
Settings	Settings item on the admin interface is visible. Authorization to view and modify FileCloud Settings.
Smart Classification	Smart Classification menu item on the admin interface is available. Add, update, run, and delete content classification rules.
Smart DLP	Smart DLP menu item on the admin interface is available. Add, edit, and delete DLP rules.
System	System item on the admin interface is visible. Authorization to run system checks, install check, generate logs and UPGRADE FileCloud to new version.
Team Folders	Set up Team Folders, add, edit, delete and manage team folder and corresponding permissions. *Note: The corresponding Folder Permission must be enabled to be able to perform a Team Folder operation.*
User Share	User Shares item on the admin interface is visible. Authorization to view, create, modify and delete User Shares.
Users	Users menu item on the admin interface is visible. Authorization to view, create, modify and delete Users. Import New Users. Reset Password for Users.

Operation	Description
Workflow	Workflow menu item on the admin interface is visible. Add, edit and delete workflows on FileCloud.

Admin users can log in to the admin portal using either their username or email id.

User Authentication Settings

FileCloud provides multiple ways of authenticating a user account. This is applicable for both FULL and GUEST user accounts.

FileCloud supports the following Authentication modes

- Default Authentication
- Active Directory based Authentication
- LDAP based Authentication

Passwords for LDAP user can only be changed in the LDAP server

	Default Authentication	AD	LDAP
Authentication	Performed by FileCloud	In AD Server	In LDAP Server
Allowing Users to Create Accounts	Permitted	Not Permitted	Not Permitted
Bulk User creation	using CSV files	Import from AD group	Not Available
Can Admin Change Password	Password change for all users allowed	Passwords for AD user can only changed in the active directory.	Passwords for LDAP user can only be changed in LDAP server.
Can user change/ reset password	Yes	Passwords for AD user can only changed in the active directory	Passwords for LDAP user can only be changed in LDAP server
User Account Types	Full, Guest, External	Full, Guest	Full, Guest

Note

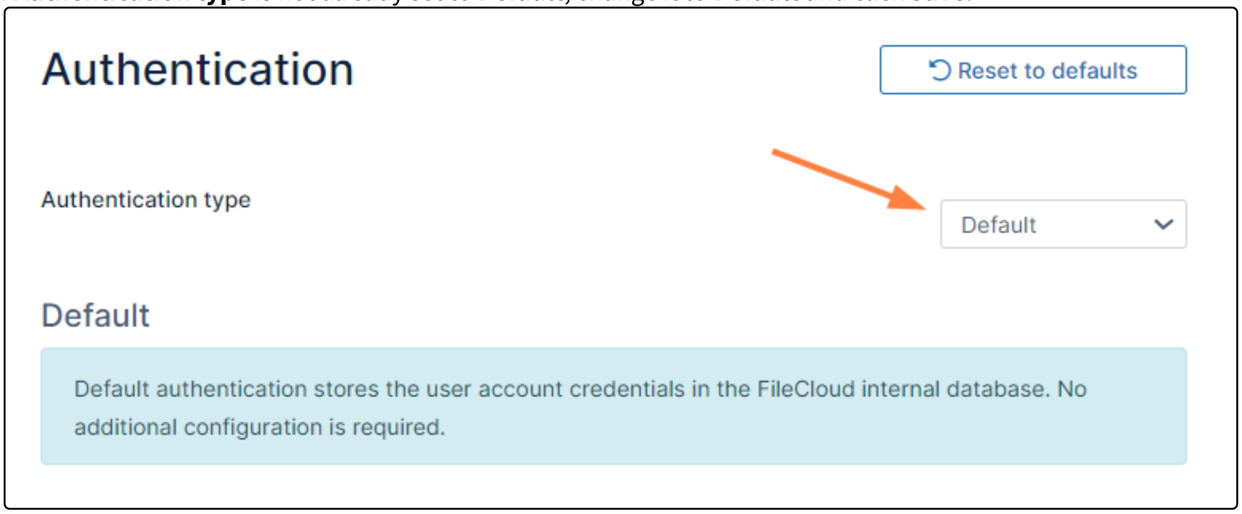
- A user account can only have a single type of authentication mechanism.

Enabling Default Authentication

Initially, FileCloud is set to default authentication mode. User accounts created when this authentication type is configured have credentials stored and managed within FileCloud.

To enable Default Authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** settings page opens.
2. If **Authentication type** is not already set to **Default**, change it to **Default** and click **Save**.



Active Directory Authentication

For admins upgrading to FileCloud 23.251:

- Prior to version 23.251, FileCloud always used the AD attribute **mail** to authenticate AD users, even if the **AD mail attribute** field in FileCloud specified a different attribute.

  This has been fixed. However, if you used an AD attribute other than the **mail** prior to version 23.251, AD users imported into FileCloud prior to 23.251 will now receive an error when they try to log in to FileCloud (unless the non-**mail** attribute always has the same value as the **mail** attribute). If you have users who may have trouble logging in for this reason, prior to updating to 23.251, change the **AD mail attribute** field back to **mail**.

Note

AD users count towards the FileCloud license only after:

- The user account logs in to FileCloud
- A user from AD is explicitly imported

In this type of authentication mechanism, a user account is authenticated against an external Active Directory server.

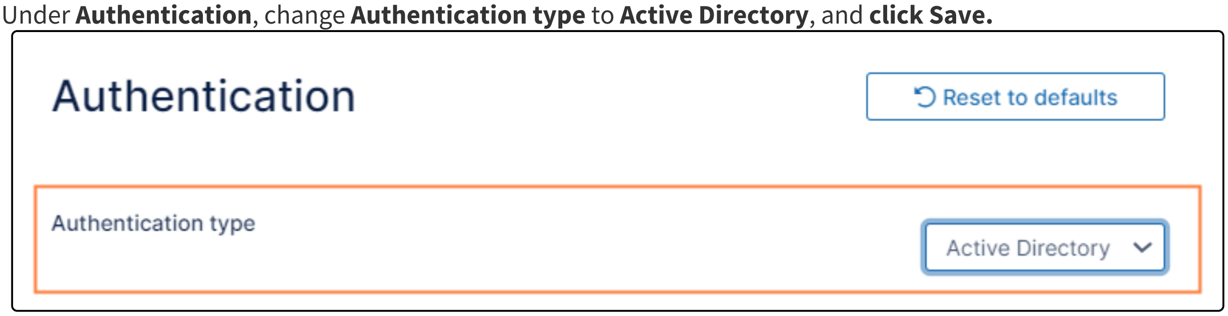
Prerequisites

Required	Configuration Requirement	Notes
Active Directory service	Must be accessible from FileCloud	IP and Port must be accessible.
Active Directory	Must support Simple Authentication Method	Must use simple bind authentication, either anonymously or with a username and password.
Active Directory users	Must have an email attribute FileCloud username must match AD user login name **Important**: The FileCloud username cannot be changed.	Beginning in FileCloud 21.2, the AD Account name used in Active Directory settings must have an email ID in Active Directory. The email address is saved in the user's FileCloud profile. During login, validation requires the FileCloud email address and the AD email address to match; later modification of email address in AD or FileCloud will cause login to fail.
FileCloud Server		

How To Enable AD Authentication

Enabling AD Authentication

To enable AD authentication in FileCloud:

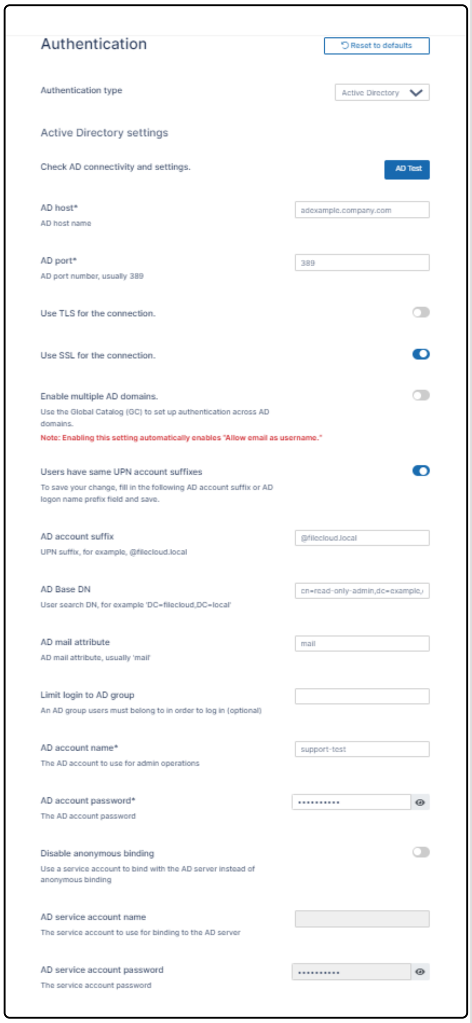
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** settings page opens.
2. Under **Authentication**, change **Authentication type** to **Active Directory**, and **click Save.**
   

   Additional settings appear.

3. Enter the required information in the settings under **Active Directory Settings** (See **AD configuration parameters**, below) and then click **Save**.
   Note: The changed parameters must be saved before performing an AD test.

AD configuration parameters

To connect FileCloud with your AD environment, fill in the settings as shown in the following screenshot.



AD host - Required. Either the IP address or host name of the AD server.

AD port - Required. Enter **389** for non-SSL, or enter **636** for SSL.

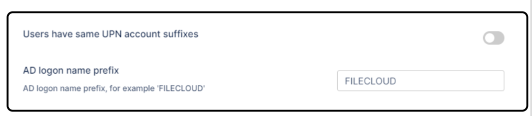
Use TLS for the connection - Optional. Enable this setting if your AD server requires clients to use TLS to connect.

Use SSL for the connection - Optional. Enable this setting if your AD server requires clients to use SSL to connect.
NOTE: Additional change required.

Enable multiple AD domains - Enable this setting to authenticate and sync users and groups across multiple trusted AD domains. For more information about this feature, see Authenticate Users Across Trusted AD Domains.

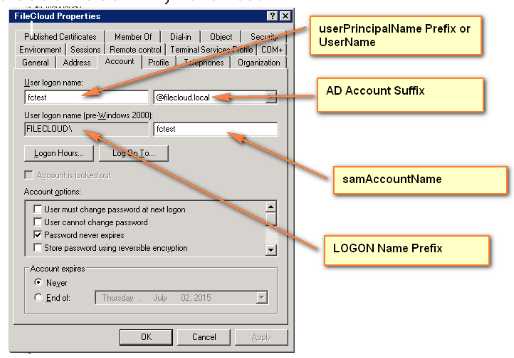
Users have same UPN account suffixes
Enabled by default. All of your AD users should have the same suffix.

- If your users have the same UPN suffixes:
  Leave this setting enabled, and enter the suffix in the next field, **AD account suffix**.
- Otherwise:
  Disable this setting. The next field changes to **AD logon name prefix** as in the following screenshot. Set **AD logon name prefix** (a trailing '\' is not required). See Mixed AD Authentication support.



<table>
<tr><th></th><th></th></tr>
<tr><td></td><td>

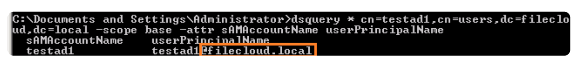
To find the **AD logon name prefix** and the **AD account suffix**, refer to:



AD account suffix - The UPN suffix for your domain, the part after **User logon name** in the dropdown next to it in the above screenshot.

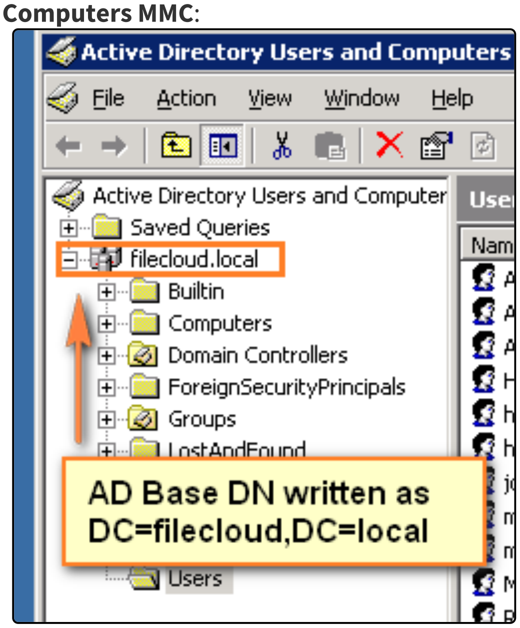
Instead of viewing the properties as shown above, you can get the account suffix by running the following query in the command line in the AD server:

*dsquery * <FULLY QUALIFIED NAME> -scope base -attr sAMAccountName userPrincipalName*



</td></tr>
</table>

AD Base DN - Required. Do not enter value with quotes.
The Base DN for your domain. Located in the extended attributes in **Active Directory Users and Computers MMC**:



You can also get the Base DN by running the following query in the command line in the AD server.

dsquery user -name <LOGON NAME>

AD mail attribute - Required. FileCloud requires each user account to have an associated email id. Typically the name of this attribute in AD is **mail**. If a user account has no mail attribute, then login to FileCloud will fail. If a mail attribute is present, and login fails, then check the base DN to ensure it is accurate and is without quotes.

Limit login to AD group - Optional. To limit login to specific users, add them to a group and specify the group name here. (Typically this is left blank.) If you set this field, ensure that the account name specified in **AD account name** is part of the AD group.

	AD account name - Required. A valid account name is required here in order for FileCloud to query the AD server. This can be any account that can access the AD server, and is located in **User logon name** in the **FileCloud Properties** screenshot, above. **Notes:** Enter username, not email id in this field. This account must have an email address set in AD. **AD account password** - A password for the AD account name. **Disable anonymous binding** - Optional. Enable this checkbox if your AD does not allow anonymous binding. Enabling this checkbox enables the **AD service account name** and **AD service account password** text boxes. **AD service account name** - Optional. The service account name to use to bind with the AD server. **AD service account password** - Optional. The service account password to use to bind with the AD server.

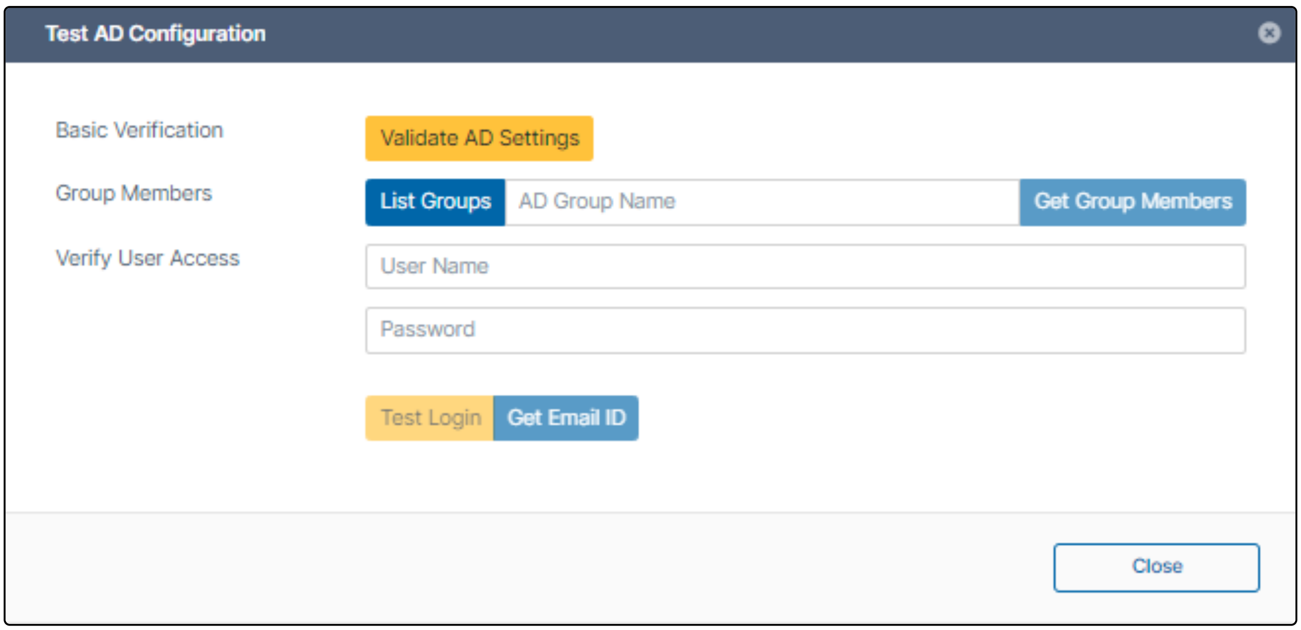
To connect to Active Directory over SSL, please follow the steps mentioned here.

Make sure the settings are SAVED before trying the AD Tests to verify connectivity

Testing AD Connectivity

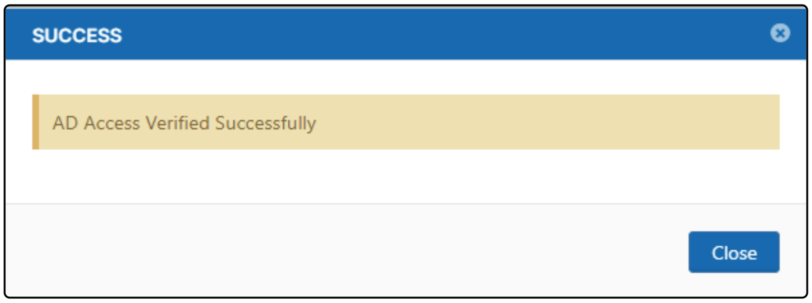
Once all data is entered and saved, test the AD settings by clicking the **AD Test** button.

A **Test AD Configuration** dialog box opens:



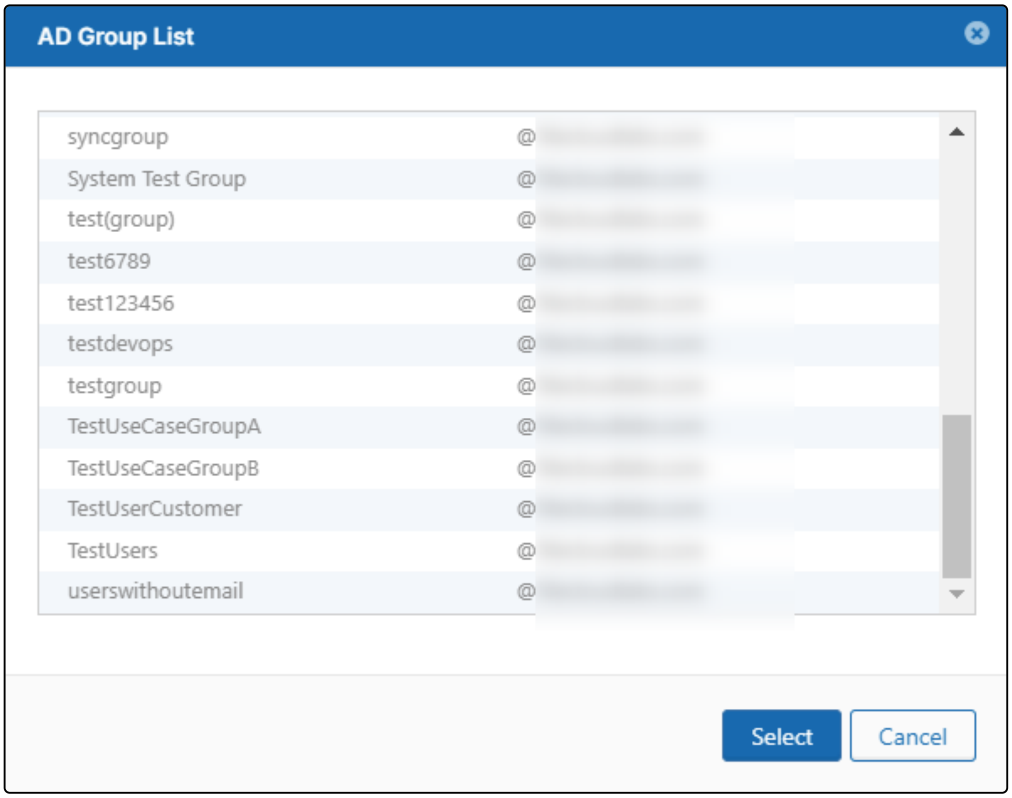
The following tests can be done.

1. Validate AD settings.
   a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server.
      You should receive the response:



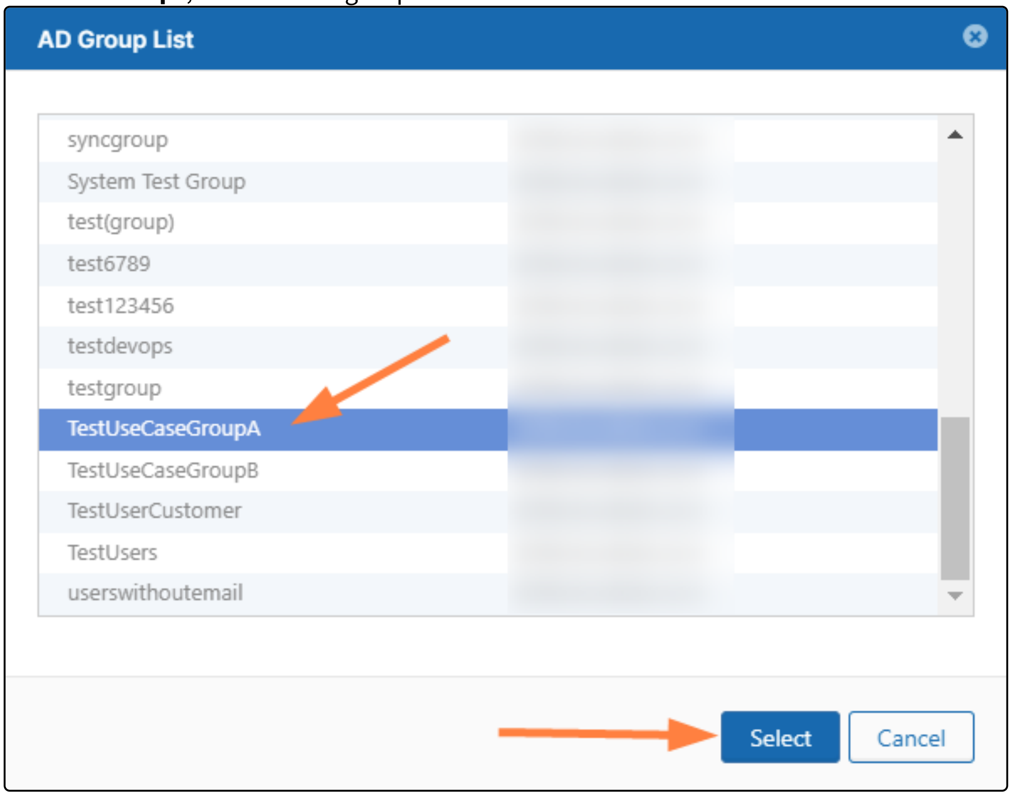
If the tests fail, then check your AD settings to ensure all the data is present and is accurate.

2. List Groups
   a. Once AD settings are validated, click **List Groups** to view the list of groups read from the server. You should see a list similar to:



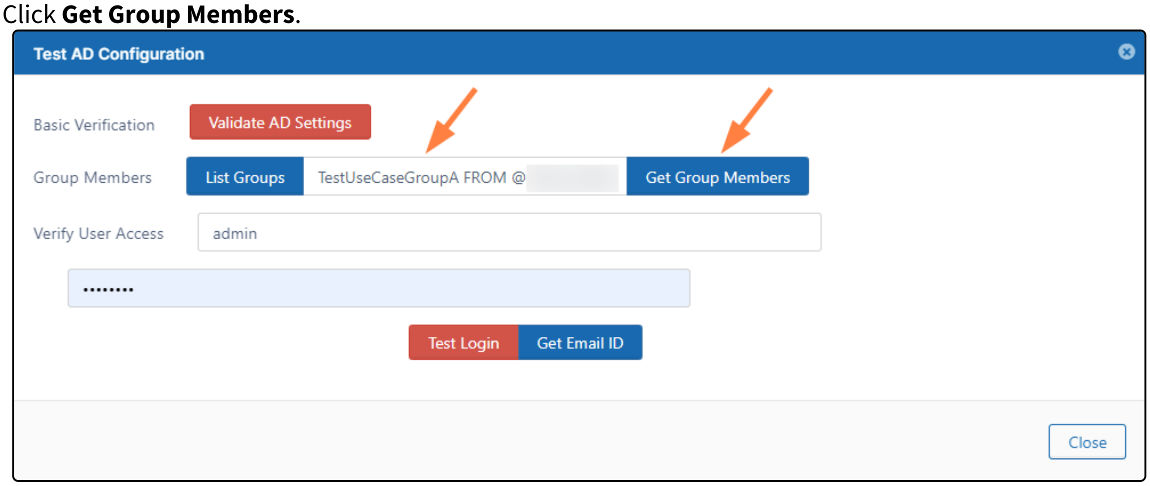
3. Get Group Member

1. Click **List Groups**, then select a group and click **Select**.

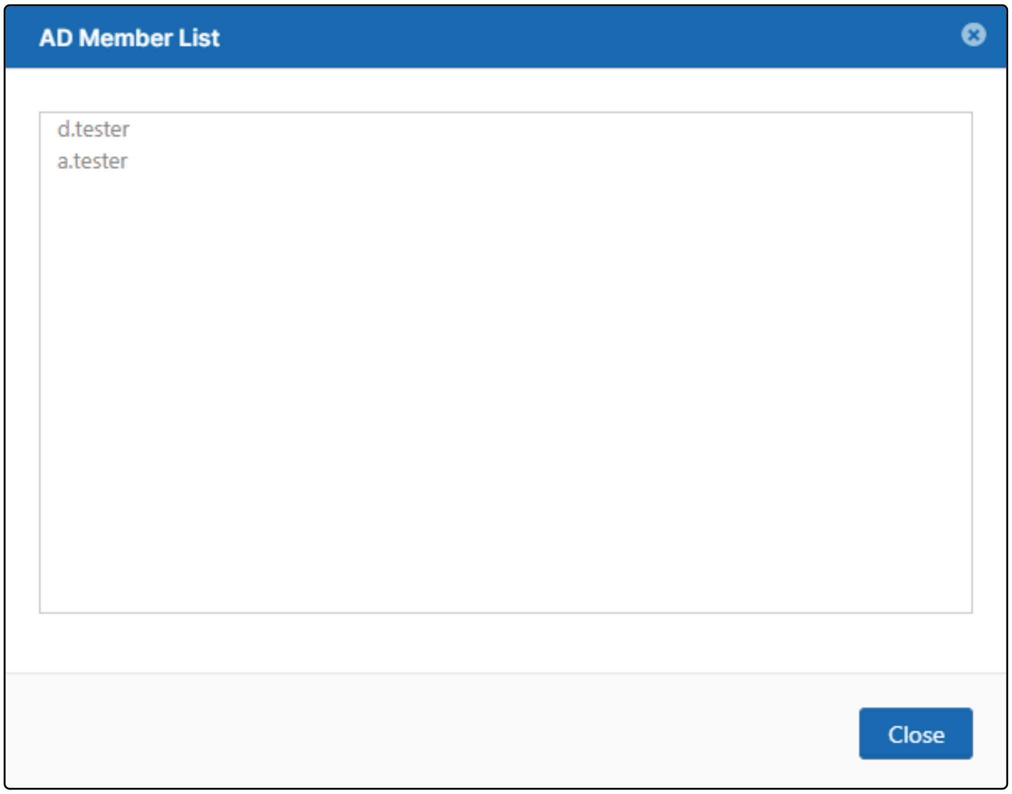


The Group name appears in the **Test AD Configuration** dialog box.
(You can also enter the group name directly into the text box without selecting from the **AD Group List** popup.)

2. Click **Get Group Members**.



The **AD Members List** should list the correct members of the group:



Note: The group members are NOT automatically added to FileCloud.

4. Verify User Access
   a. Enter a specific user name and password and click **Test Login** to make sure the user can log in to AD. If not, check if the AD suffix or AD prefix matches the one entered in the **AD account suffix** or **AD logon name prefix** in the FileCloud admin portal or the AD server.
   b. Enter a specific user name and password and click **Get Email ID.** This should return the correct email address for a user account from AD. If a valid email address is not returned, then FileCloud cannot import the user account. Check if the email address is included for the user on the AD Server.

AD Options

Connecting to AD via SSL
Mixed AD Domain Environments
Migrate Data from a Changed User Account Name

More Information:

Video	FileCloud Blogs
Active Directory Settings	Import Users to AD via PowerShell

Connecting to AD via SSL

If you want to securely add users, change passwords, or connect to the Active Directory server being used with your FileCloud site, then you will need to use an SSL certificate.

The Lightweight Directory Access Protocol (LDAP) is used to read from and write to Active Directory. By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology.

Before you can enable the use of SSL certificates in FileCloud Server, you must have completed the following steps:

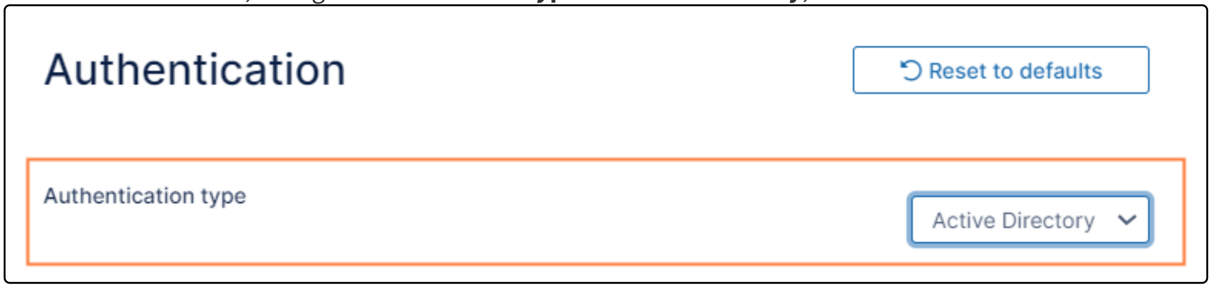
1. Install and configure your Active Directory server
2. Install an SSL certificate on your Active Directory server

How do I enable the use of SSL in FileCloud Server?

To enable the use of SSL Certificates in FileCloud Server:

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

2. Under **Authentication**, change **Authentication type** to **Active Directory**, and **click Save.**



Additional settings appear.

3. In **AD port**, change the number to **636**.
4. Enable **Use SSL** for the connection.

5. Click **Save**.

How do I connect to AD using TLS?

Connecting to Active Directory over TLS

> **TLS**
>
> To use TLS, use port **389** instead of port **636**, and enable **Use TLS for the connection** instead of **Use SSL for the connection**.

Authenticate Users Across Trusted AD Domains

> The ability for admins to configure FileCloud to sync users and groups across multiple trusted AD domains through the FileCloud admin portal is available in FileCloud 23.252.

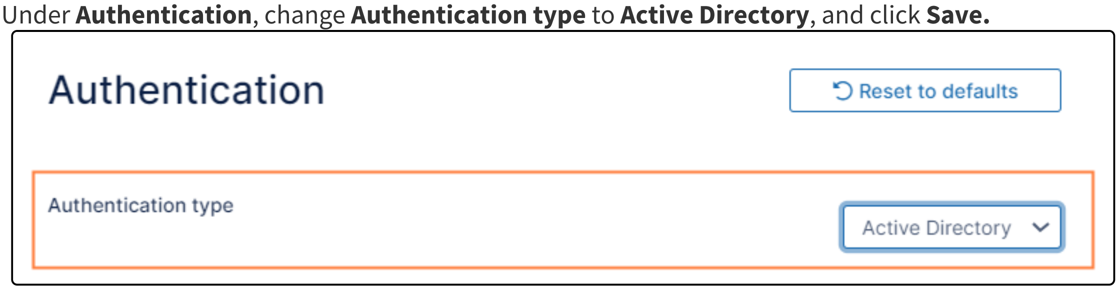
Organizations may maintain multiple AD domains (and sub-domains) in a structure referred to as an **AD forest**, which authenticates user access to all of the included domains, enabling actions such as searching to be performed across all of the domains. A **Global Catalog (GC)** helps manage an AD forest by indexing all of its domains so they can be cross referenced easily.

The instructions on this page show you how to configure authentication of all of the AD servers in your domain forest using the Global Catalog (GC). To authenticate to multiple AD servers by separately configuring each of the AD servers in your adconfig file, see Authenticating to Multiple AD servers.

You can sync FileCloud users and groups with all domains in an AD forest by enabling **Enable multiple AD domains** in the Authentication settings for Active Directory. When this setting is enabled, the users in that AD forest are required to log in with their full email addresses to enable cross-domain resolution.

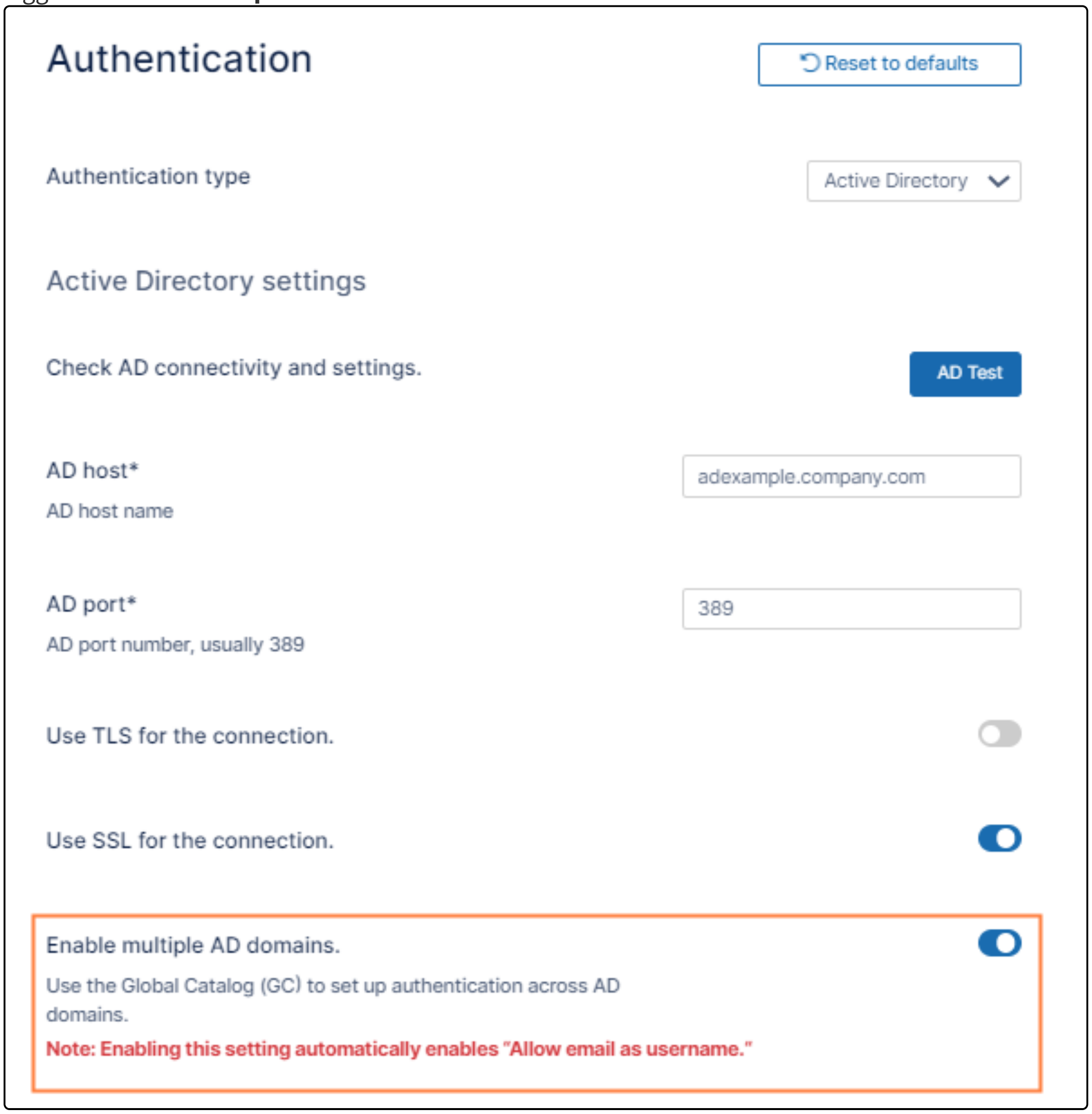
For more information on using a multidomain AD infrastructure, see AD Directory Services Getting Started.

To enable multiple AD server authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** settings page opens.
2. Under **Authentication**, change **Authentication type** to **Active Directory**, and click **Save.**
   

   Additional fields appear.

3. Toggle on **Enable multiple AD domains**.



When **Enable multiple AD domains** is toggled on:

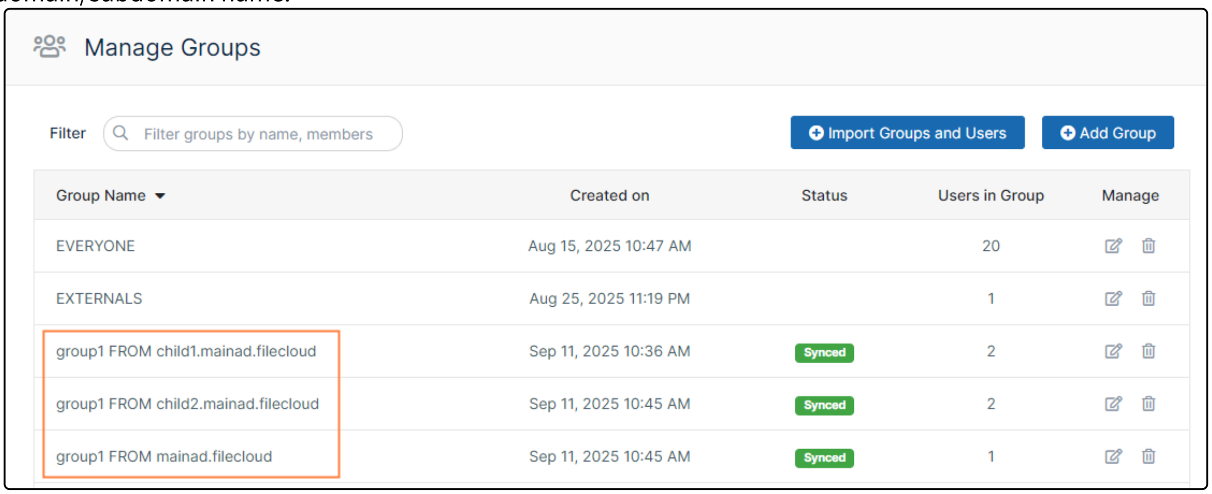
- the following account suffix and prefix fields are hidden, since multiple domains are defined by different account suffixes:
  - **Users have same UPN account suffixes**
  - **AD account suffix**
  - **AD logon name prefix**
- The **Allow email as username** setting available in Admin settings is automatically enabled because users stored in this AD domain forest are required to log in to FileCloud with their full email addresses, which are taken from the User Principal Name (UPN) in Active Directory. You are not permitted to disable **Allow email as username** as long as **Enable multiple AD domains** is enabled.

4. Fill in the other fields as instructed on the page Active Directory Authentication.

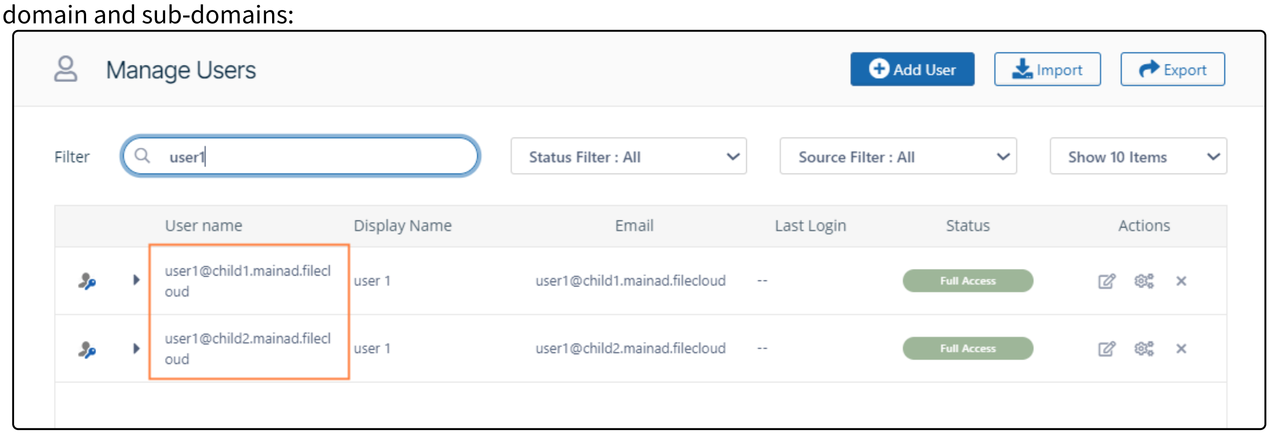
Handling of groups and users with the same names in different domains

In AD forests, it is not uncommon for different AD domains or sub-domains to have users or groups with the same names. For example, two divisions of a company may each have their own domain, but both divisions may have a Marketing group or a user named Michael in their domain. For this reason, when **Enable multiple AD domain** is enabled:

- When a group is imported from an AD domain, its name in FileCloud includes both the group name and the domain/subdomain name:



- When a user is imported through an AD group, its user name in FileCloud is its email address, including the full domain and sub-domains:



Mixed AD Domain Environments

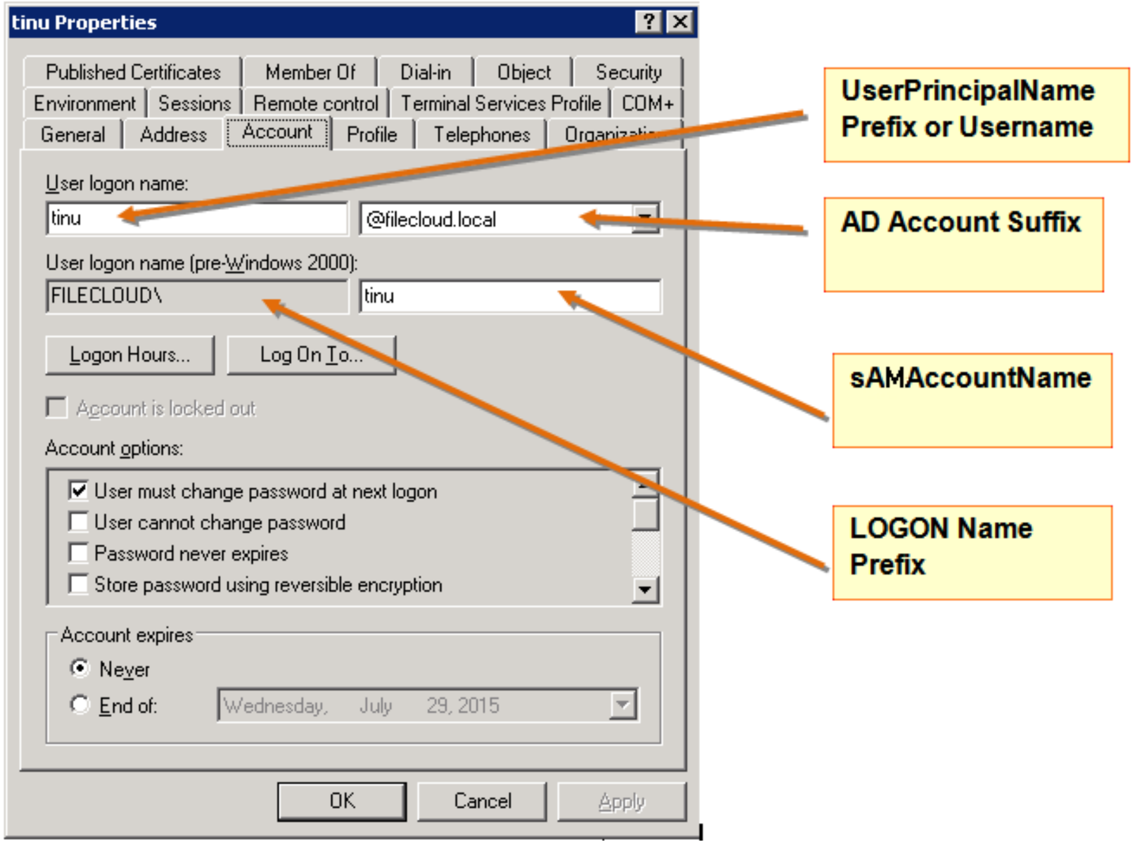
In some AD environments, there may be multiple UPN domain suffixes set up in a mixed AD hosting setup and the UPN prefix names might not be unique in those cases.

Normally FileCloud uses the UPN prefix names as the usernames, and if they are not unique, FileCloud may not be able to identify the user account correctly.

Therefore, for FileCloud to authenticate in an environment where this occurs, you need to set up the AD connection information slightly differently. In these cases, the account sAMAccountName will be used as the user id.

1. Disable the checkbox "Users have the same UPN Account Suffixes"

2. Set the **AD Logon Name Prefix** parameter, which is the prefix used in the non-editable part of the **User logon name** (pre-Windows 2000).



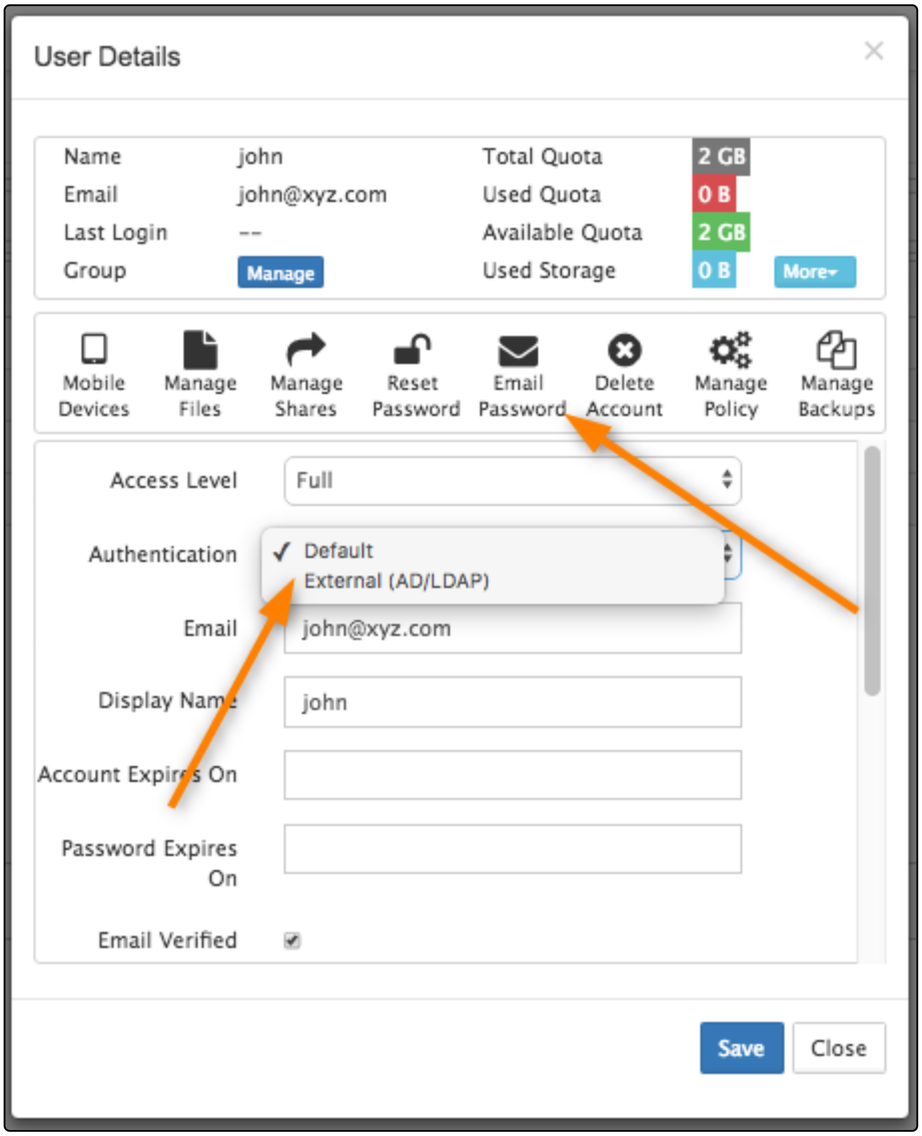
Users can log in using either their email or sAMAccountName.

How to migrate the data from a user that changes account name

When the account name for a user changes in Active Directory, FileCloud won't recognize this change. All the files the user owns still belong to the old account.

To migrate the account data to the new AD account:

1. Log in to the admin portal.
2. Go to the Users section and change the user authentication method form **External** to **Default** and assign a password:



The user can login using Sync App or from Web UI and download all their files.

3. Ask the user to log in via Web User Portal using the new account/password (AD).
4. Reset the Sync App settings and enter the user's new domain credentials without removing the data. See Sync Settings.
5. Log in to the Sync App with the new account credentials; don't remove the data from the computer. All the user's files will sync to the server.

In addition to this, all the user shares need to be created and, if the user belongs to any Team Folders, the account has to be added again and permissions created. If the user belongs to any Network Shares, please remember to add the account to them as well.
Once all the user's data is uploaded to the new account and verified; you can delete the old account.

Troubleshooting Active Directory

Common FileCloud Active Directory problems and solutions

Trouble establishing a connection with Active Directory:

1. Make sure you have followed the instructions for entering the settings shown in Active Directory Authentication under **AD configuration parameters**.
2. Check that the port you have specified (either 389 or 636) is open in the AD server for the FileCloud server.
   You can use the telnet command to confirm that it is open.
   telnet [ip address] [port]
   For example, if your IP address were 192.168.1.191 and your port were 389, you would enter:

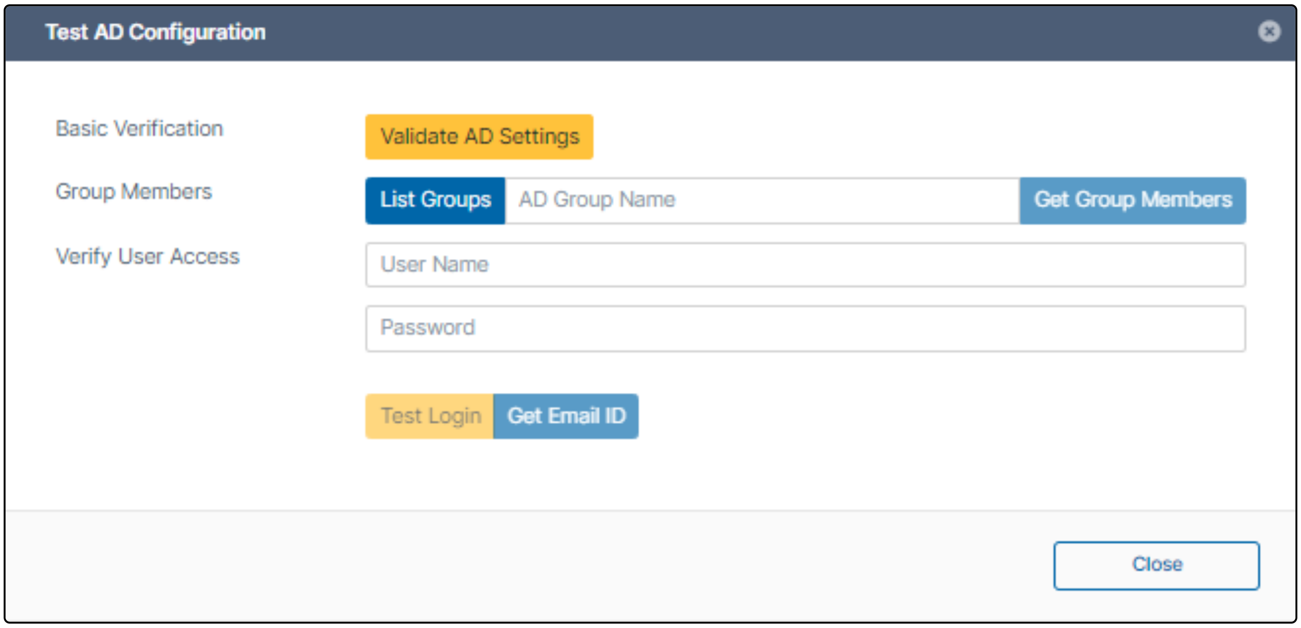
   ```
   telnet 192.168.1.191 389
   ```
3. Confirm that you have entered an account in **AD account name**. This account is used to query the AD server and must be present.
   If you have entered a value in **Limit login to AD group** (see below) the account you enter into **AD account name** must be a member of the AD group.
4. Confirm that you have entered an **AD account password** and that it is correct.

Verify your AD settings using the following steps:

Testing AD Connectivity

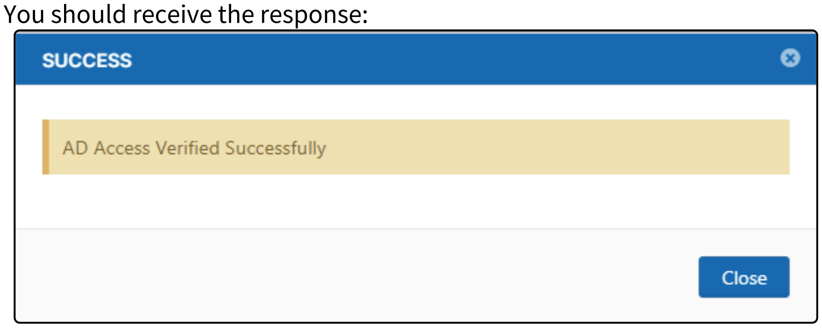
Once all data is entered and saved, test the AD settings by clicking the **AD Test** button.

A **Test AD Configuration** dialog box opens:

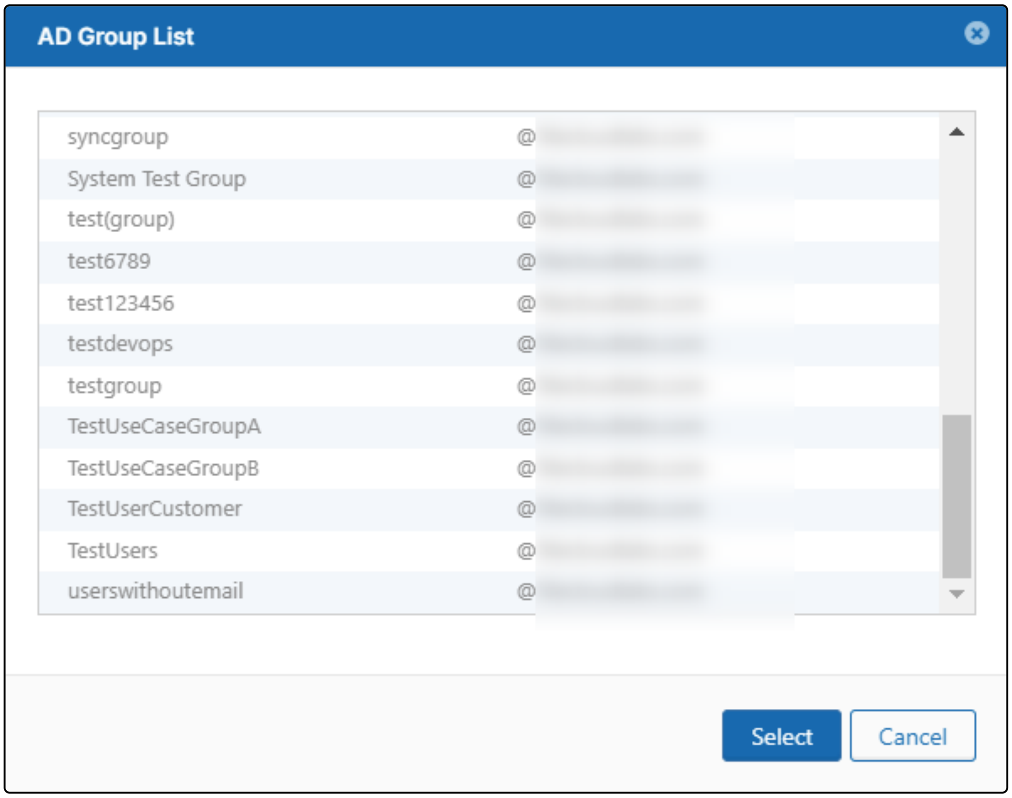


The following tests can be done.

1. Validate AD settings.
    a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server.
    You should receive the response:

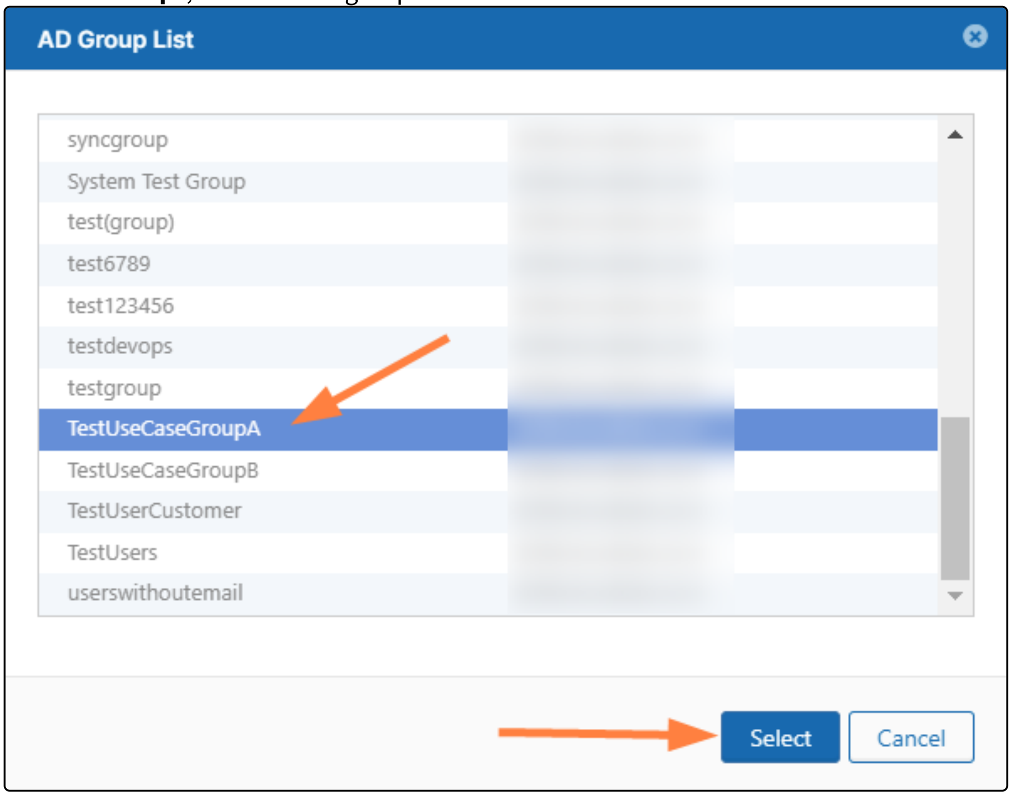
    

    If the tests fail, then check your AD settings to ensure all the data is present and is accurate.
2. List Groups
    a. Once AD settings are validated, click **List Groups** to view the list of groups read from the server.
    You should see a list similar to:



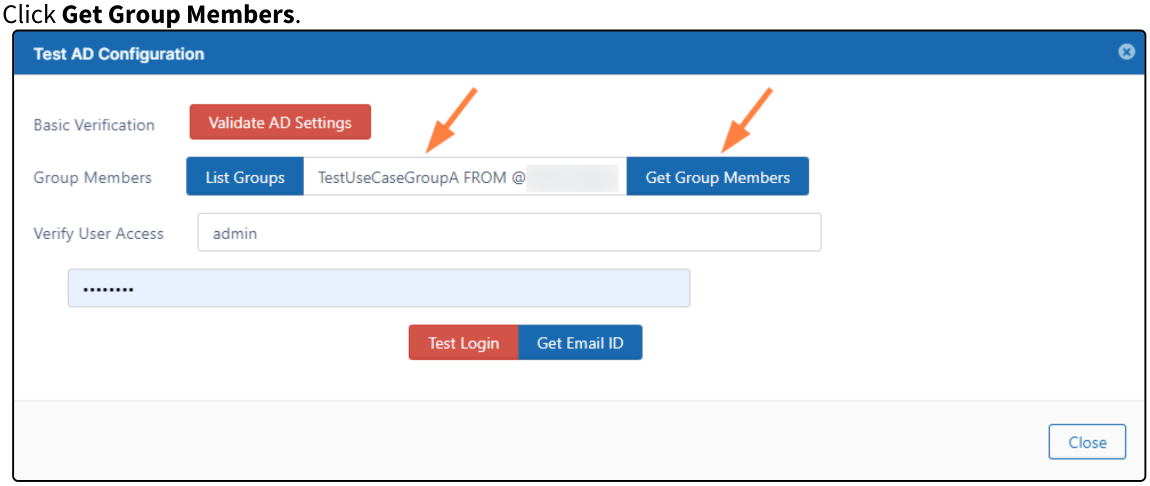
3. Get Group Member

1. Click **List Groups**, then select a group and click **Select**.

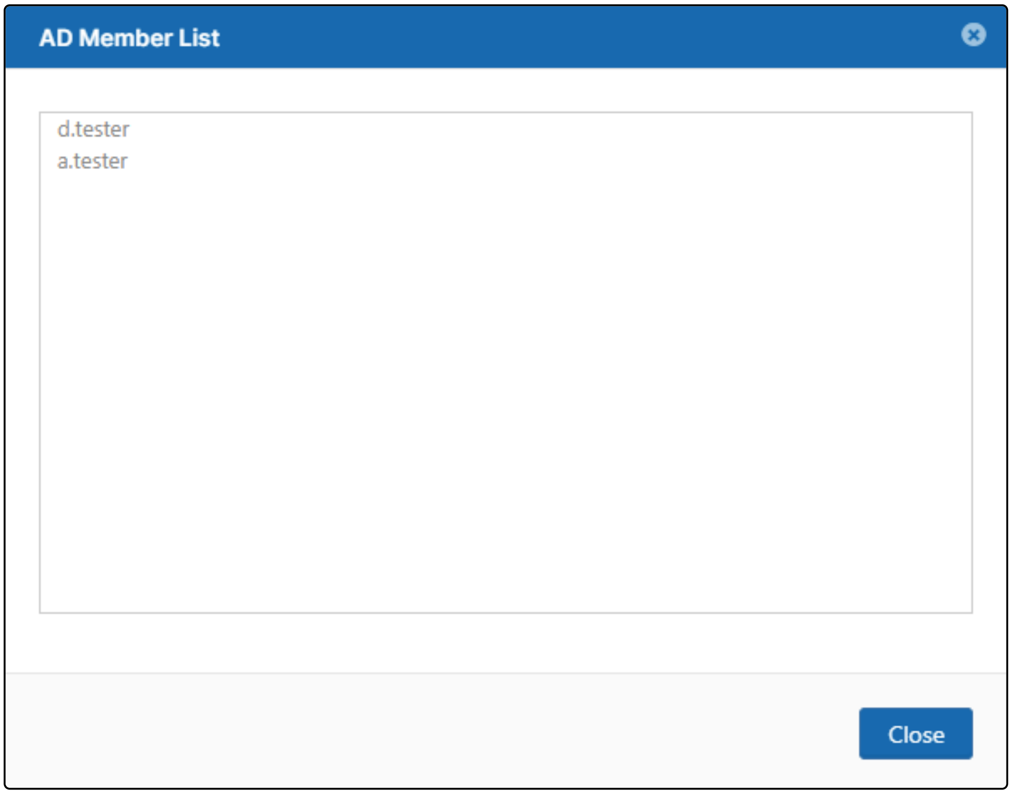


The Group name appears in the **Test AD Configuration** dialog box.
(You can also enter the group name directly into the text box without selecting from the **AD Group List** popup.)

2. Click **Get Group Members**.



The **AD Members List** should list the correct members of the group:



Note: The group members are NOT automatically added to FileCloud.

4. Verify User Access
   a. Enter a specific user name and password and click **Test Login** to make sure the user can log in to AD. If not, check if the AD suffix or AD prefix matches the one entered in the **AD account suffix** or **AD logon name prefix** in the FileCloud admin portal or the AD server.
   b. Enter a specific user name and password and click **Get Email ID.** This should return the correct email address for a user account from AD. If a valid email address is not returned, then FileCloud cannot import the user account. Check if the email address is included for the user on the AD Server.

Here are some common AD connectivity error messages and their meanings:

Error messages

AD Access failed. Can't contact LDAP server

Either the Hostname or IP address is wrong or the FileCloud server is not able to contact the AD server on the port specified.

AD Access failed. Invalid credentials

Either the AD account name or password is incorrect or the Logon prefix or suffix is incorrect.

AD Access failed. Check if provided AD account name is part of Limit Login into AD group

Either the value in AD BASE DN is wrong or the limit group is set and the AD account name is not part of that group.

Some users have trouble logging in

If you check **Users have the same UPN account suffixes**, you are prompted to enter the **AD account suffix**. If you uncheck it, you are prompted to enter **AD logon name prefix**. Make sure that whichever you use applies to all of your AD users who access FileCloud. If it doesn't, users it does not apply to cannot log in to FileCloud.

All users cannot log in or you cannot import them into FileCloud:

Check if **AD mail attribute** is filled in. If it is not, users cannot log in or be imported. This is normally set to **mail**.

Using the logs to find errors

FileCloud stores all errors associated with AD in the logs.
By default, the log level in FileCloud is set to **PROD**.

1. Change the log level to DEV to create more detailed entries:
    a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server**  .
    The **Server** settings page opens.
    b. Set **Log Level** to **DEV**.
2. Repeat the steps that caused the error.
3. Open the log file:
   In Windows: C:\xampp\htdocs\scratch\logs
   In Linux: /var/www/html/scratch/logs

If you see error messages similar to:

```
2022-05-18 23:03:12.265388 ERROR: [16529329921474] Unable to find provider by name:
0bf0d8c9a7544ce179a7fb1f802dde5f
2022-05-18 23:03:12.265559 ERROR: [16529329921474] Unable to connect to AD server with
david username:
2022-05-18 23:03:12.265608 DEBUG: [16529329921474] User `david` has not been
authenticated with provider
CodeLathe\Core\Subsystem\Security\Auth\AD\Provider\ADProvider class
2022-05-18 23:03:12.357099 DEBUG: [16529329921474] FAILED LOGIN: Invalid Username or
Password
```

Do the following:

- Check if the AD login and password are correct.
- Check if the user has an email address in the AD server.
- If the user is already imported into the FileCloud server, check if the user's email in FileCloud and email in the AD server match.

If you were authenticating a user (for this example, authenticating user david on host 192.168.1.14), and see error messages similar to

```
2022-05-18 23:11:27.296483 NOTICE: [16529334871841] Phone number is invalid for imported user - david
2022-05-18 23:11:27.297668 DEBUG: [16529334871841] User email `david@test.com` does not match AD user email `david@gmd.com`.
2022-05-18 23:11:27.297760 DEBUG: [16529334871841] User `david` has NOT been authenticated.
```

These messages indicate that the user's email address in the AD server doesn’t match the user's email address in FileCloud.

To restrict login to FileCloud to specific AD users only

1. Create a group in AD and add only those users who should able to log in to FileCloud.
2. In **Limit login to AD group**, enter the name of the AD group.

LDAP Based Authentication

In this mechanism, a user account is authenticated against an external LDAP server.

Accounts with this type of authentication are also known as external accounts.

By default, LDAP communications between client and server applications are not encrypted.

- This means that it could be possible to use a network monitoring device or software to view the communications traveling between LDAP client and server computers.
- This is especially problematic when an LDAP simple bind is used because credentials (username and password) are passed over the network unencrypted. This could quickly lead to the compromise of credentials.

Therefore, it is recommended that you enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

- SSL and TLS are also known as LDAPS
- Some applications authenticate with Active Directory Domain Services (AD DS) through simple BIND. If simple BIND is necessary, using SSL/TLS to encrypt the authentication session is strongly recommended.
- Use of proxy binding or password change over LDAP requires LDAPS. (e.g. Bind to an AD LDS Instance Through a Proxy Object)
- Some applications that integrate with LDAP servers (such as Active Directory or Active Directory Domain Controllers) require encrypted communications.

Prerequisites

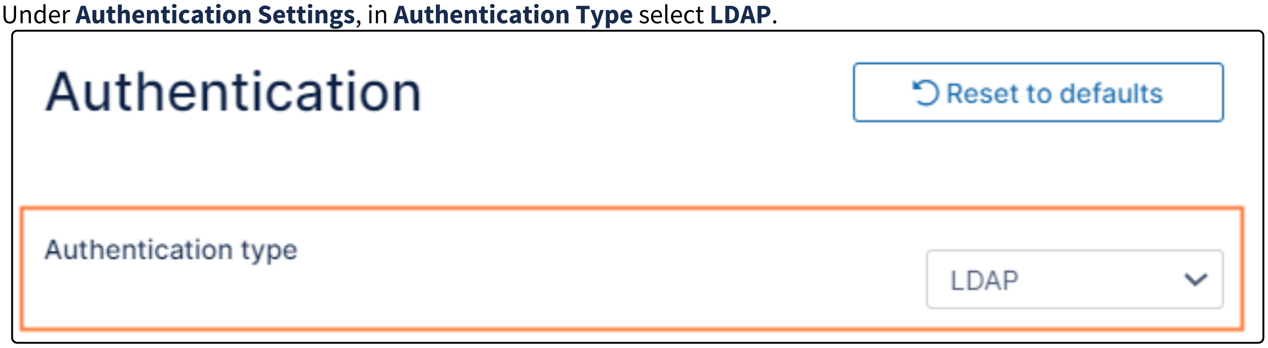
1. The LDAP service must be accessible from FileCloud (IP and Port must be accessible).
2. LDAP must support Simple Authentication Method (Anonymous or Name/Password Authentication Mechanism of Simple Bind).
3. LDAP users must have an email attribute.

- If LDAP Authentication is enabled, then Automatic User creation cannot be enabled (i.e, All user creation should be done in LDAP server)
- The LDAP user will count towards FileCloud License only after the user account logs into FileCloud

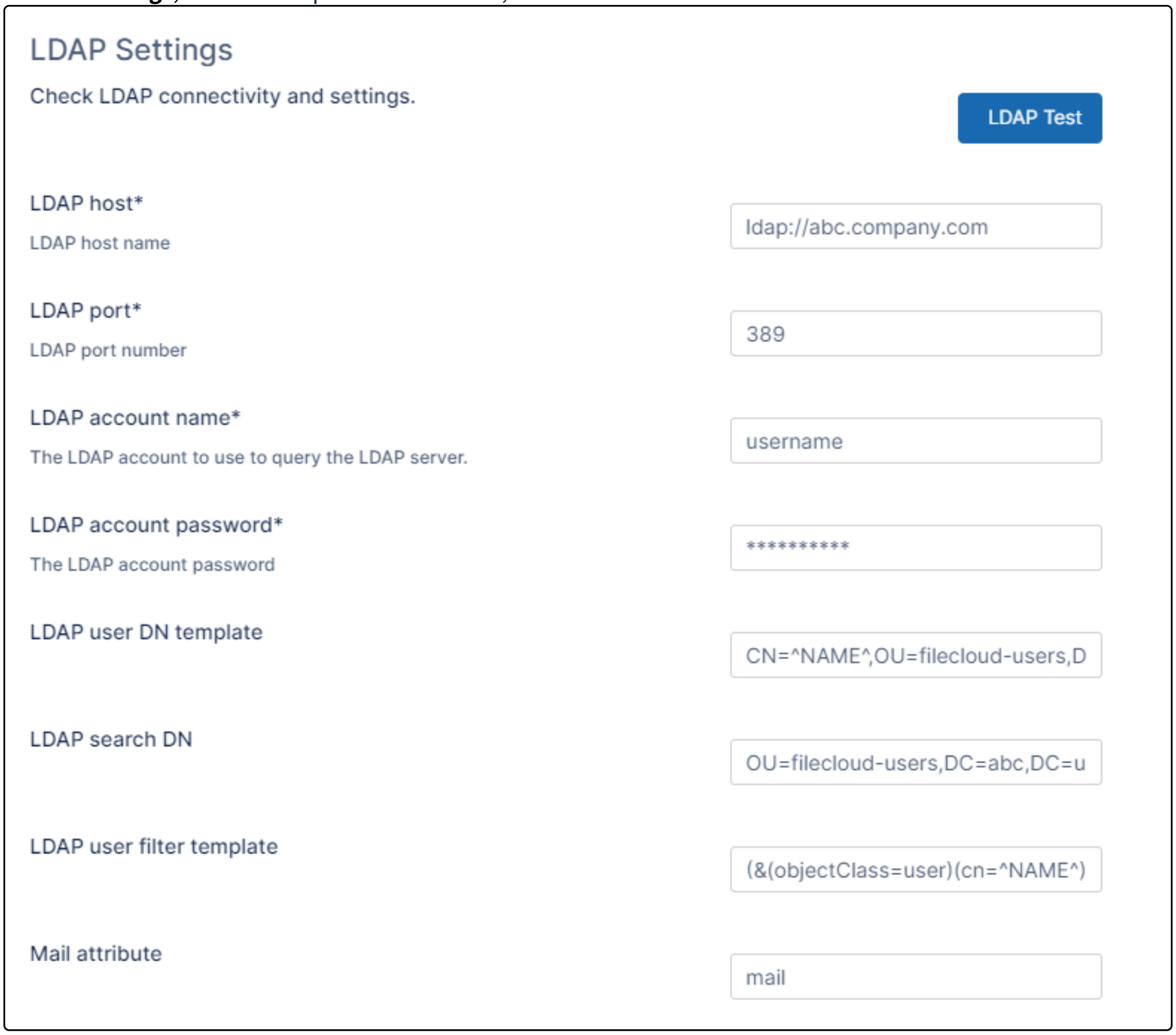
Enable LDAP Authentication

To enable LDAP Authentication in FileCloud:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** page opens.
2. Under **Authentication Settings**, in **Authentication Type** select **LDAP**.



3. In **LDAP Settings**, enter the required information, and then click **Save**.



Read a description of the LDAP Settings

LDAP Settings

SETTING	REQUIRED?	DESCRIPTION	Example
LDAP host	REQUIRED	The hostname or IP address where the LDAP server is running, including the protocol definition ldap://	`ldap://mycompany.com`
LDAP port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	389

SETTING	REQUIRED?	DESCRIPTION	Example
LDAP account name	REQUIRED	A valid LDAP login account required to perform queries	`<username>`
LDAP account password	REQUIRED	Password for the LDAP Account Name	`<password>`

LDAP User DN template	REQUIRED	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory.
		This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user.
		To use multiple OUs, set this equal to ^USE_USER_FULL_DN^
			Use the token ^NAME^ in place of user name:
			`cn=^NAME^,ou=someorg,dc=company,dc=com`
			
			`Multiple OU mode: ^USE_USER_FULL_DN^`

LDAP search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an *ou* encompassing all users, then the search DN would be pointing to that DN.	If all users are under the employees ou, then the search DN would be: `ou=employees,dc=company,dc=com`
LDAP user filter template	REQUIRED	**T**he filter to be used to identify a user entry record from results.	If the object class is inetOrgPerson, then you would use: `(&(objectClass=inetOrgPerson)(cn=^NAME^))`
Mail attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	`username_email_ID`

NOTE: For using with Zimbra, please use the following strings

```
User DN Template:
uid=^NAME^,ou=someou,dc=company,dc=com
```

LDAP Search DN
`ou=someou,dc=company,dc=com`

LDAP User Filter Template:
`(&(objectClass=zimbraAccount)(uid=^NAME^))`

NOTE: For using with JumpCloud, please use the following strings

User DN Template:
uid=^NAME^,ou=Users,o=xxxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com

`LDAP Search DN`

`ou=users,o=`**`xxxxxxxxxxxxxxxxxb42f7988db,`**`dc=jumpcloud,dc=com`

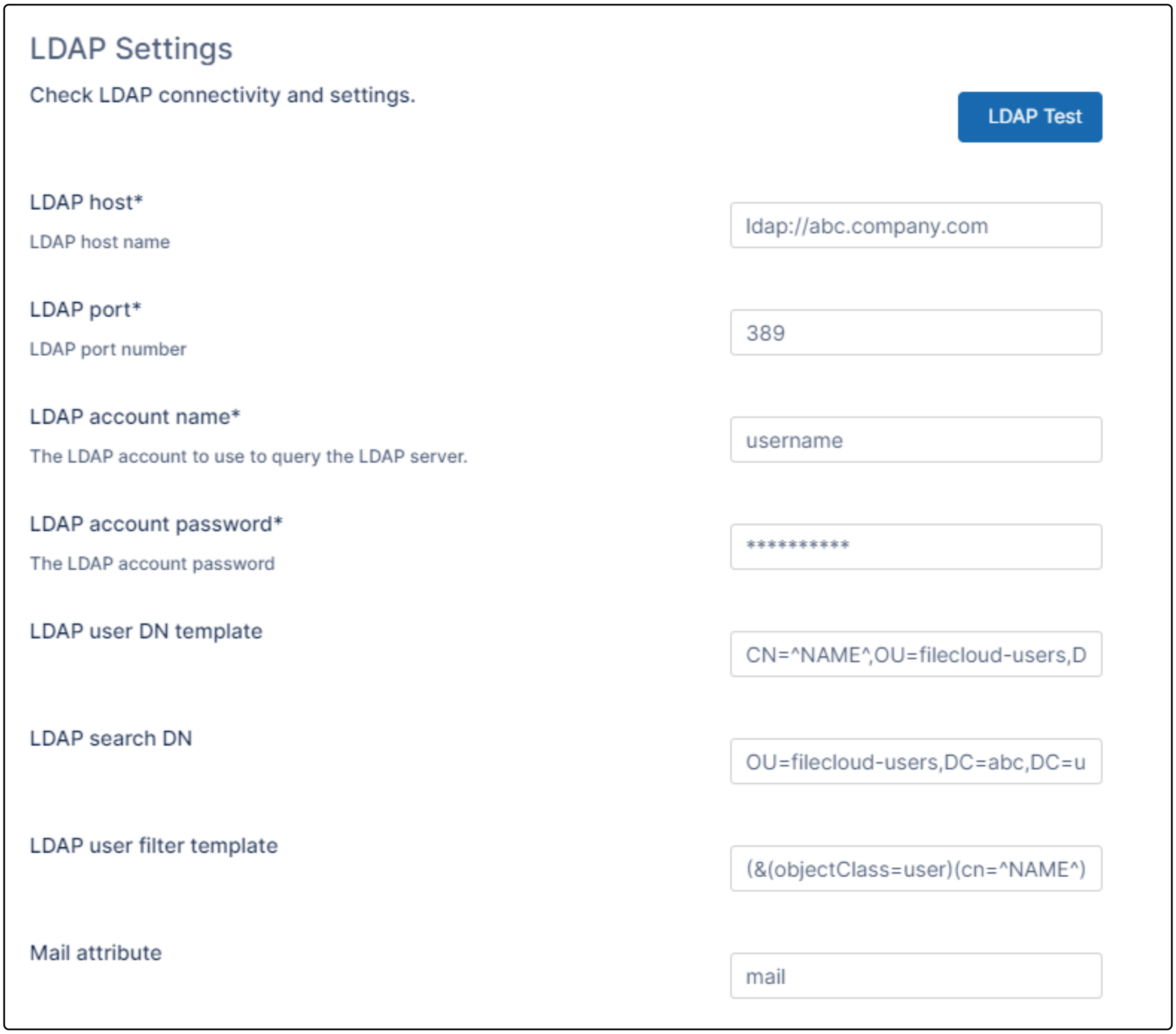
LDAP User Filter Template:
`(&(objectClass=inetOrgPerson)(uid=^NAME^))`

Use LDAP with TLS

If you are using an LDAP connection with TLS, then you must configure the LDAP fields using the following information:

SETTING	REQUIRED?	DESCRIPTION	TLS Example
LDAP host	REQUIRED	The hostname or IP address where the LDAP server is running	ldaps://*<your_server_hostname>*
LDAP port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	389
LDAP account name	REQUIRED	A valid LDAP login account required to perform queries	*<username>*
LDAP account password	REQUIRED	Password for the LDAP Account Name	<password>

SETTING	REQUIRED ?	DESCRIPTION	TLS Example
LDAP user DN template	REQUIRED	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory. This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user. `Use the token ^NAME^ in place of user name` Example : cn=^NAME^,ou=someorg,dc=company,dc=com To use multiple OUs, set this equal to ^USE_USER_FULL_DN^	cn=<username>,ou=<*abc*>,dc=<*company*>,dc=com Multiple OU mode: ^USE_USER_FULL_DN^
LDAP search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an *ou* encompassing all users, then the search DN would be pointing to that DN. For example, if all users are under the *employees* ou, then the search DN would be *ou=employees,dc=company,dc=com*	*ou=company-users,dc=company,dc=com*
LDAP user filter template	REQUIRED	**T**he filter to be used to identify a user entry record from results. For example, if the object class is inetOrgPerson, then you would use: `(&(objectClass=inetOrgPerson)(cn=^NAME^))`	(&(objectClass=*inetOrgPerson*)(cn=*^NAME^*))
Mail attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	*username_email_ID*



Two-Factor Authentication

Two-factor authentication (2FA) refers to the two-step verification process that is available in FileCloud and designed to provide an extra layer of security. With this function, in order to access FileCloud, the user is required to know not only the password and username but also an extra security code that is made available to them. The FileCloud administrator can enable two-factor authentication for the user portal, and also, separately, for the admin portal. This can be done regardless of the authentication type (default, AD, or LDAP).

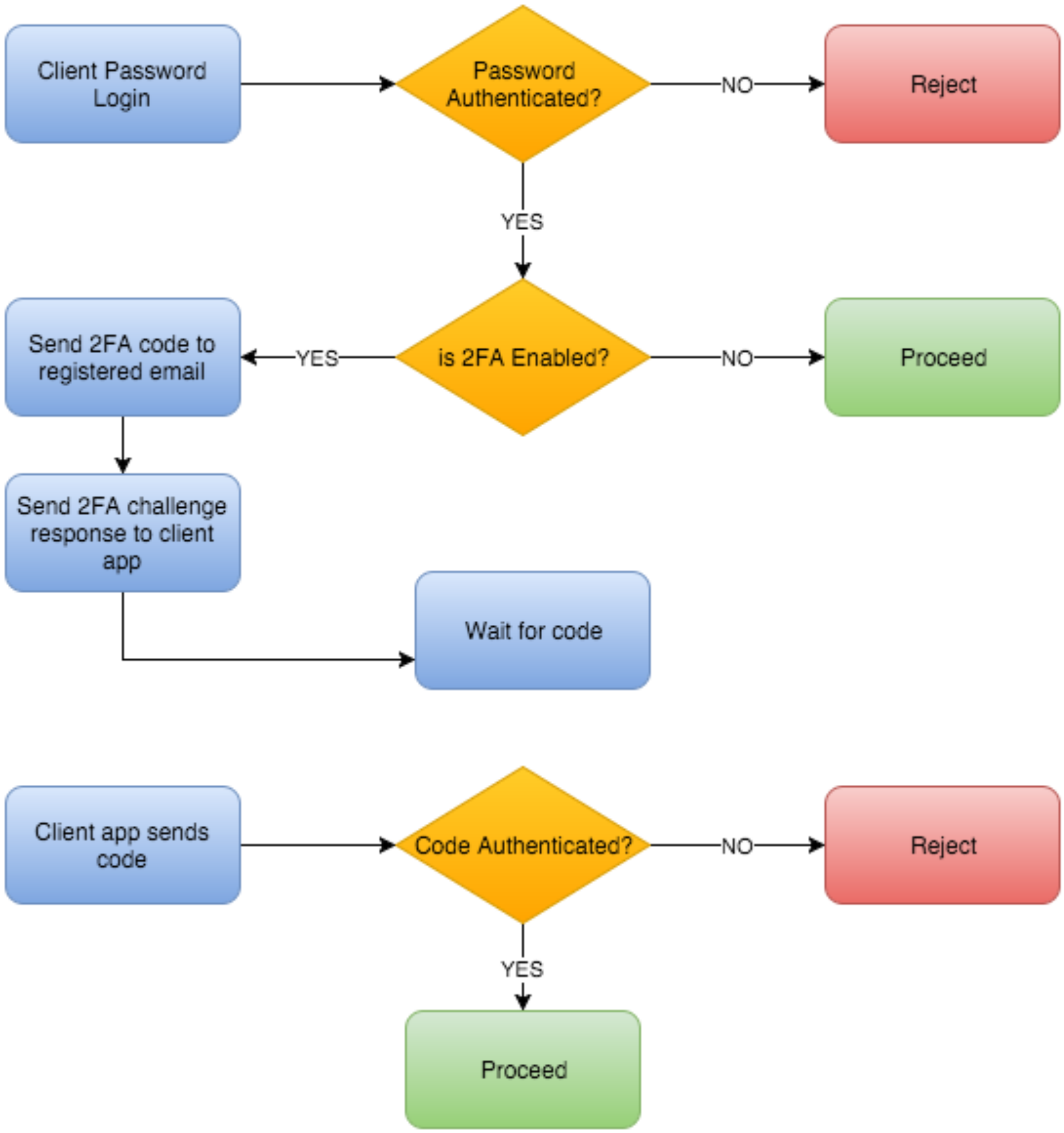
FileCloud supports the following modes to deliver 2FA codes:

- Email

- Google Authenticator TOTP Code
- DUO Security (user portal only)
- SMS OTP Security Code

Two-factor authentication using user's email address

The general flow is shown below



Two-factor authentication using TOTP (Google Authenticator or similar TOTP code generators)

These instructions are written using Google Authenticator as an example TOTP code generator, however, any TOTP apps such as Microsoft Authenticator or DUO mobile app, etc. can be used.

To set up 2FA with Google Authenticator:

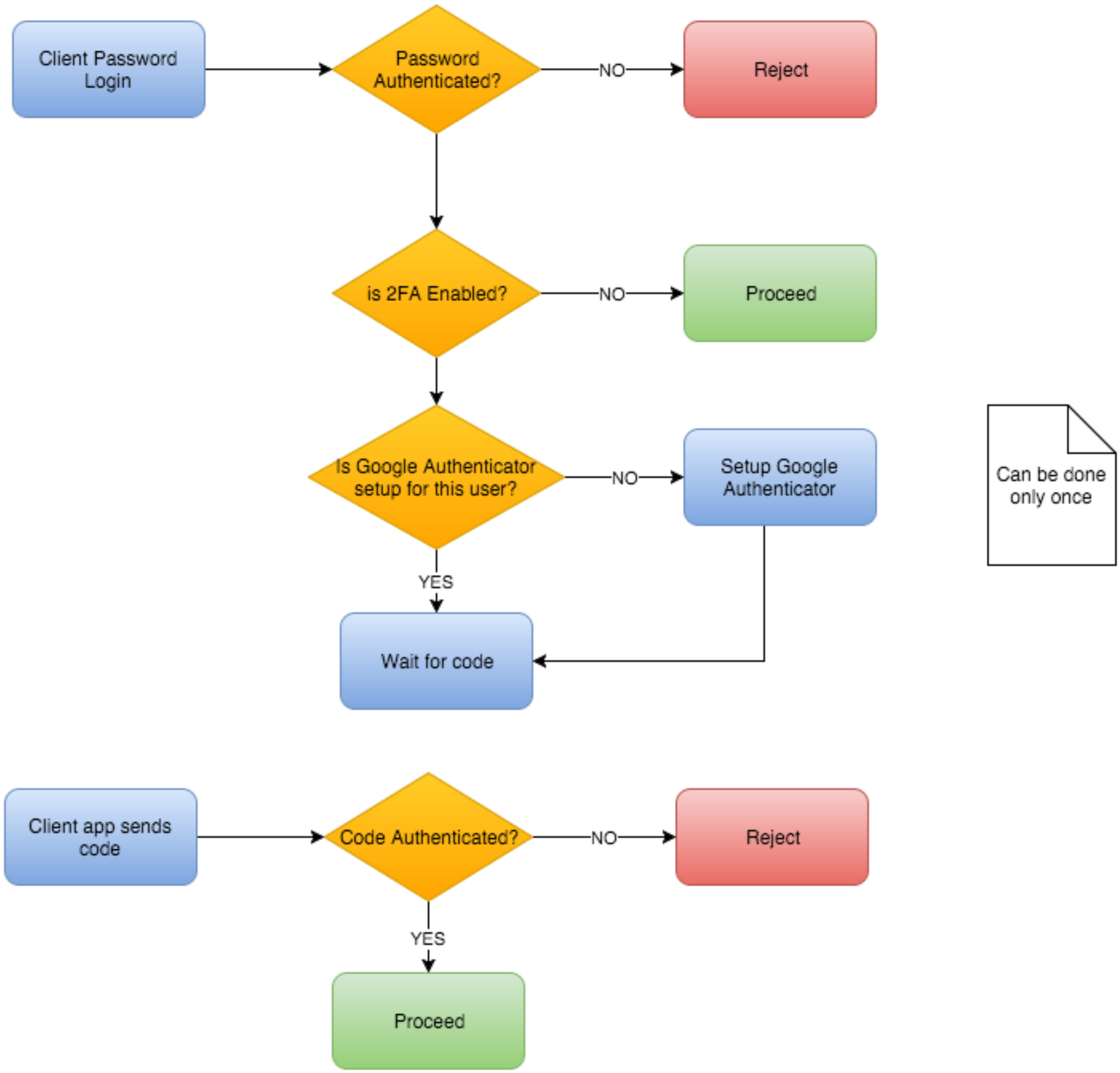
- In the FileCloud user portal, choose **TOTP (Authenticator App)** when configuring 2FA for the user portal. See Two-Factor Authentication for User Portal for help.
- In the FileCloud admin portal, choose **TOTP Authentication** when configuring 2FA for the admin portal. See Two-Factor Authentication for Admin Portal for help

When a user logs in for the first time, they are provided with an option to set up Google Authenticator. This involves entering a code or scanning a QR Code into the the Google Authenticator client. See Log in Using Two-Factor Authentication for more information.

Note that once Google Authenticator is set up using the user portal, other client devices can be used to connect to the FileCloud account.

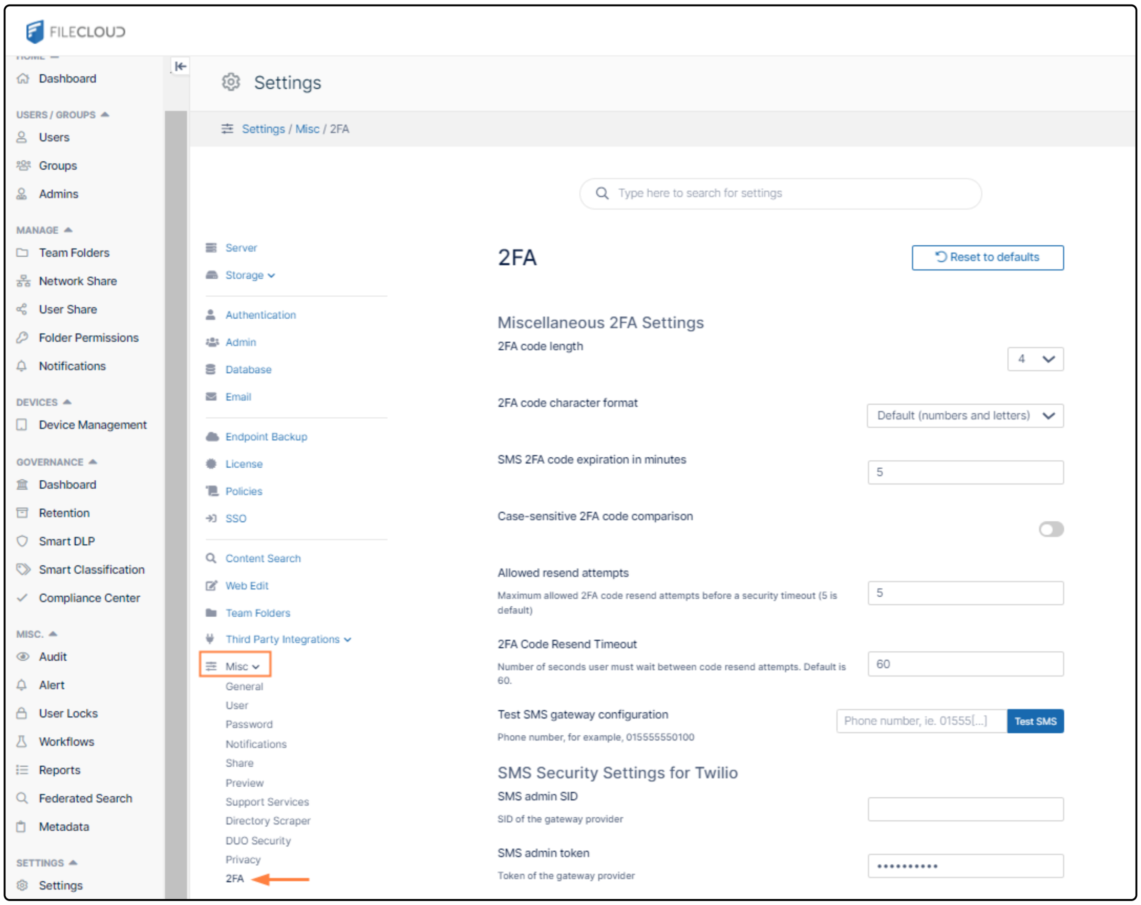
Once 2FA with Google Authenticator is set up for the first time, the user is no longer able to set it up again. Only the Administrator can clear the Google Authenticator setup.

The general flow is shown below

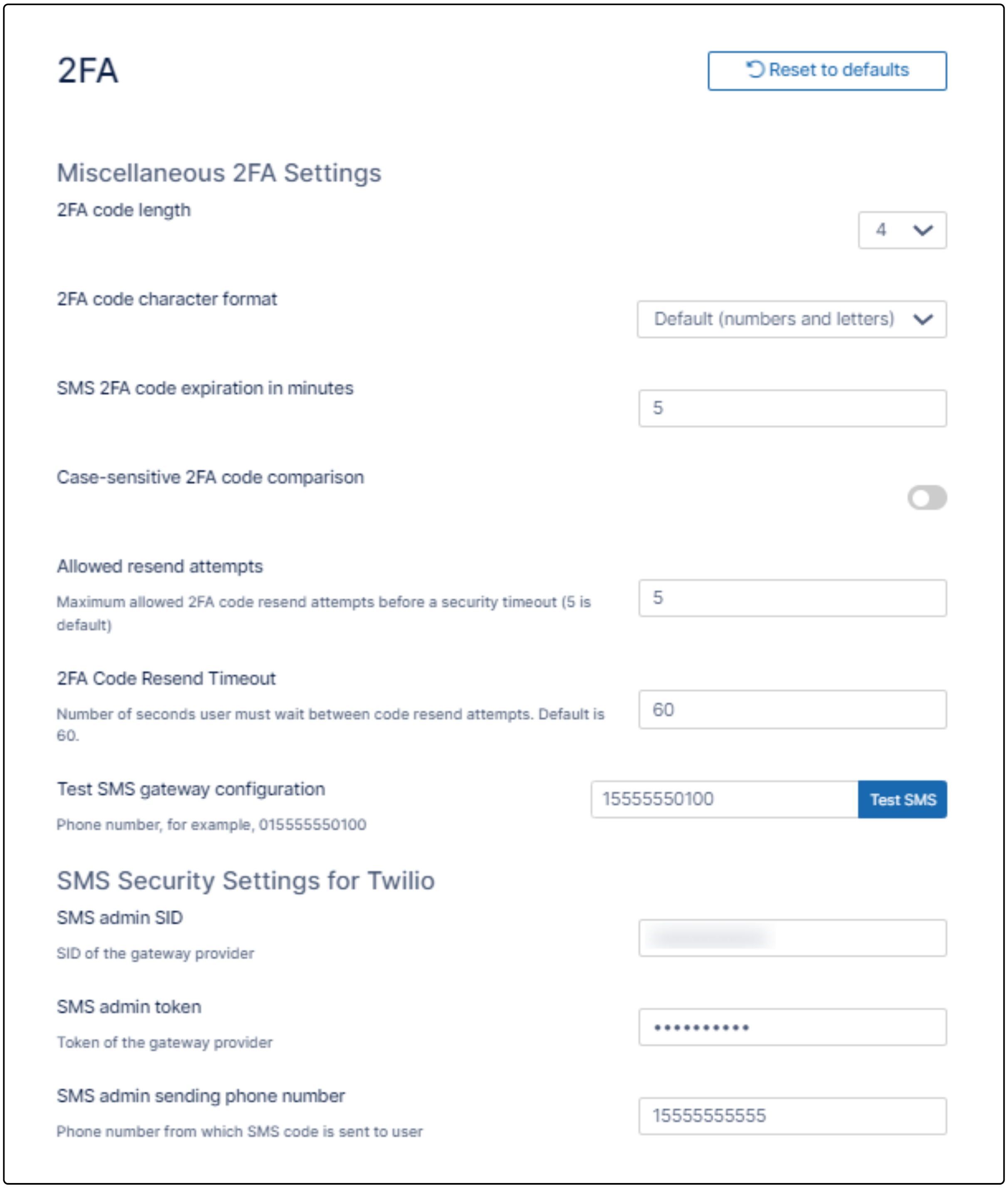


Two-factor authentication using SMS OTP (one-time password) Security Codes

FileCloud can be set up to use SMS security codes to perform 2FA. Currently, we have implemented Twilio as the default SMS Gateway Provider, although enterprise customers may add custom SMS providers and handlers to the system. In order to successfully use SMS security, admins must set up a Twilio account to receive the required security ID, authentication token and the phone number from which the codes will be sent.

1. Create a Twilio account.
   Follow instructions at https://www.twilio.com/docs/sms to obtain the required SID, Auth Token and create a phone number.
2. In the FileCloud admin portal, open the **2FA** settings page.
   To open the 2FA 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 **2FA**, as shown below.
   

   The **2FA** settings page opens.
3. Fill in the 2FA settings.



The settings **2FA code length** and **2FA code character format (2FA Code Dictionary)** are available beginning in FileCloud version 20.2.

2FA code length - The number of letters and digits in the 2FA code. Default is 4.

2FA code character format- Type of characters permitted in 2FA code. Options are:

- Numbers and letters (default)
- Numbers
- Letters
- Uppercase letters

SMS 2FA code expiration in minutes - How long, in minutes, the security code remains valid. Default is 10.

Case-sensitive 2FA code comparison - When checked, the code entered is case-sensitive.

Allowed resend attempts - Number of times the user may resend the code before logging in is timed out for the time set in **2FA Code Resend Timeout.**. Default is 5.

2FA Code Resend Timeout - Number of seconds between **Allowed resend attempts** that the user must wait before attempting to resend again. Default is 30.
For example, if **Allowed resend attempts** is 5, and **2FA Code Resend Timeout** is 30, a user can attempt to resend a code 5 times and then is forced to wait 30 seconds before being able to attempt to resend the code another 5 times. If those attempts fail, the user is forced to wait another 30 seconds, and so on.

Test SMS gateway configuration - Enter a secure known phone number, and save the settings. Click **Test SMS** to check if your SMS configuration is valid.

SMS admin SID - SID of gateway provider.

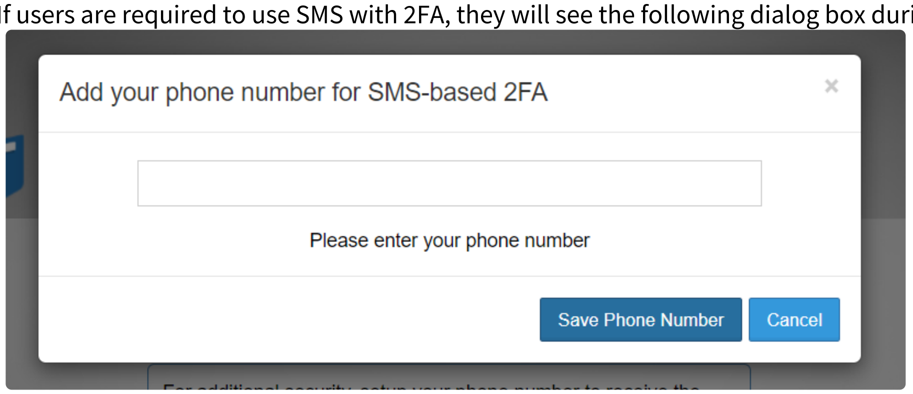
SMS admin token - Token of gateway provider.

SMS admin sending phone number - Phone number from which SMS code is sent to user.

Once the setup is complete, set up the policy for users and choose the appropriate SMS gateway provider, similarly to other 2FA methods.

> **Users are required to set up a phone number once the SMS 2FA Policy is enabled.** Once the phone number is set up, client devices can be used to connect to the FileCloud account. Set up the phone number via the web UI or through your admin.

If users are required to use SMS with 2FA, they will see the following dialog box during login after the policy is enabled:



Two factor authentication validity for Email based 2FA

> **2FA Code validity**: 10 minutes.
>
> For Web Apps, The 2FA validity period is tied to the Session Timeout
> For Client apps (iOS , Android App, Drive and Sync) the 2FA code will be required only on very first access and subsequent access will not require the code. If the record of that device is removed using "Remove Client Device Record" action, then subsequent access for that mobile device will require the 2FA code.

For instructions specific to the admin portal or the user portal, see:

- Two-Factor Authentication for User Portal
- Two-Factor Authentication for Admin Portal

Two-Factor Authentication for User Portal

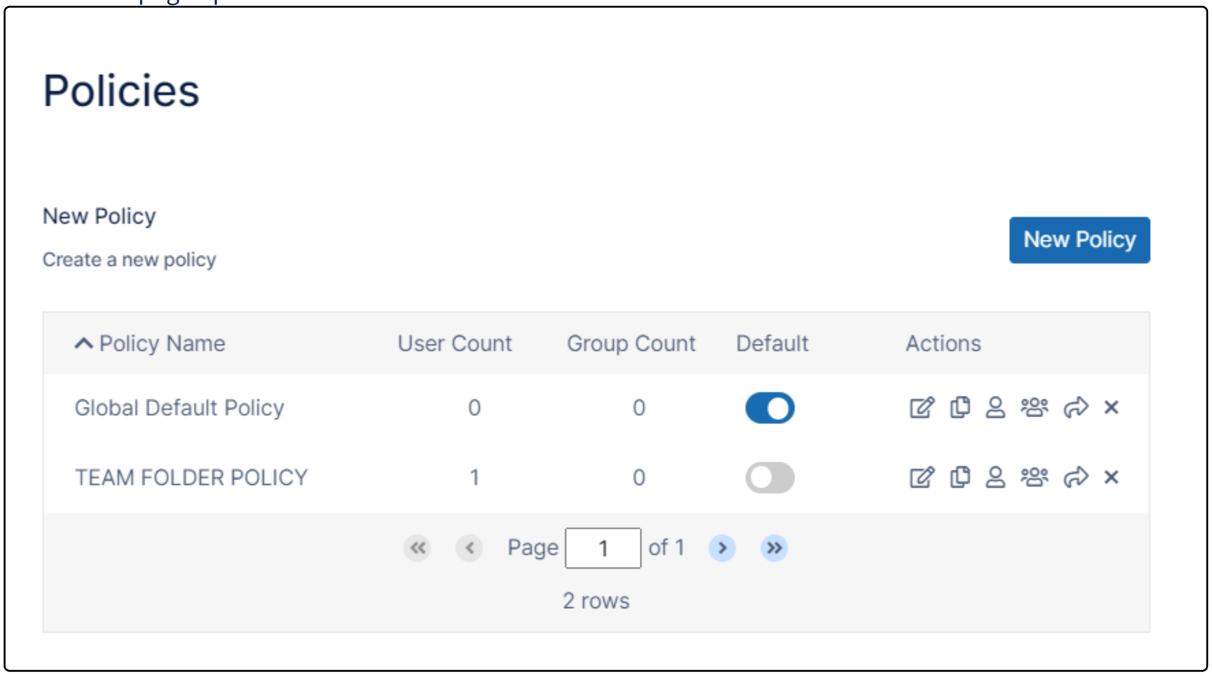
Enable two-factor authentication for user portal

To enable two-factor authentication for logging into the user portal:

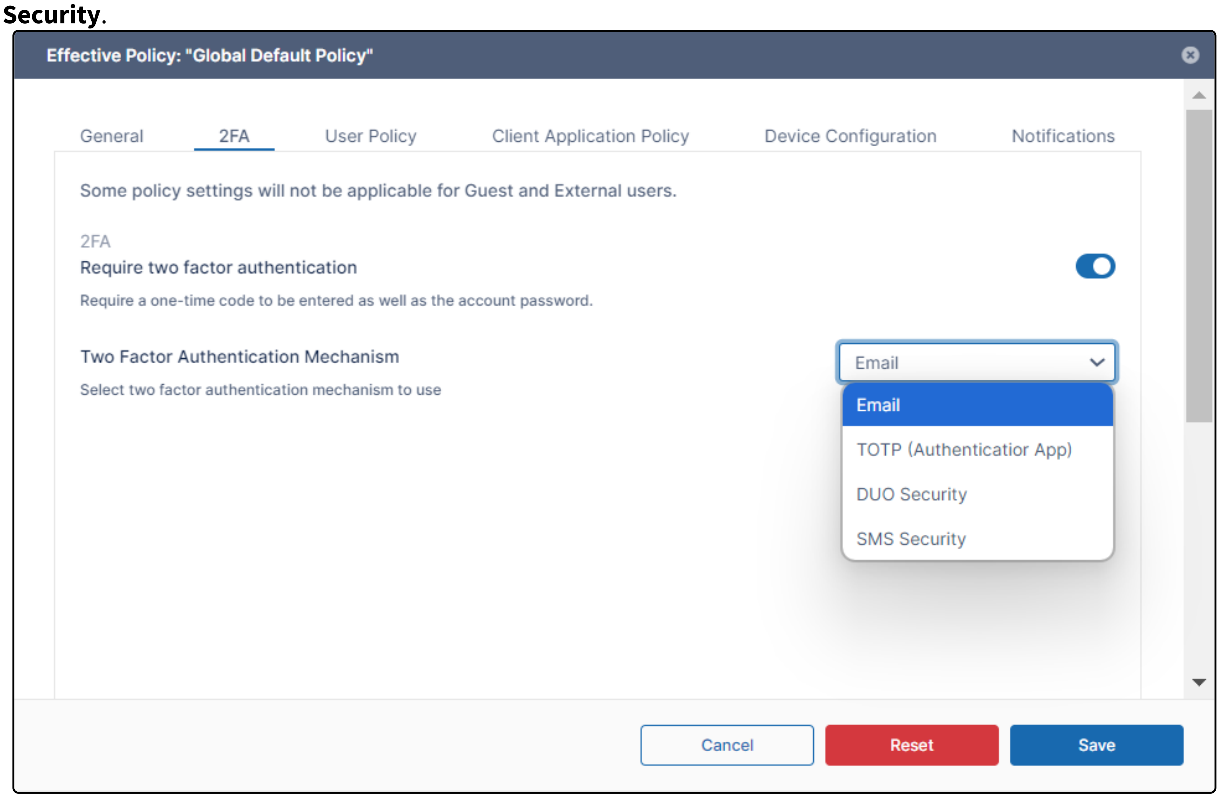
> If you are planning to enable DUO Security as the two-factor authentication mechanism, first set up FileCloud to use DUO Security Service (instructions below).

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

The **Policies** page opens.



2. Edit the policy assigned to the users who you want to use 2FA.
3. Click the **2FA** tab.
4. Under **2FA** heading, Change the **Enable Two Factor Authentication** drop down box to **Enabled**
5. In **Two Factor Authentication Mechanism** choose **Email, TOTP (Authenticator App), DUO Security** or **SMS Security**.

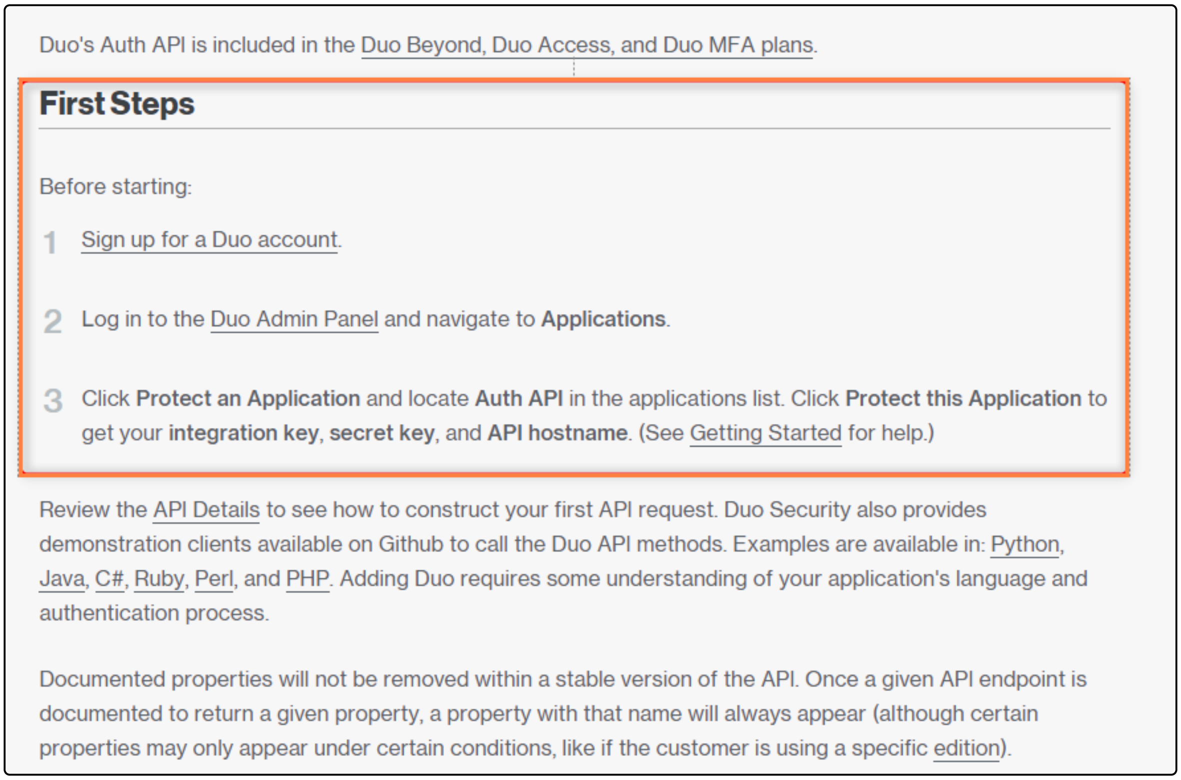


Two-factor authentication using DUO security

FileCloud can be set up to use DUO security service to perform 2FA. Note that DUO PUSH is not supported and requires code generated by DUO Mobile app to be entered to perform 2FA.

The following steps are required to set up 2FA using DUO.

1. ADD DUO Auth API
    - Follow instructions at https://duo.com/docs/authapi to get **integration key**, **secret key**, and **API hostname.**



Duo's Auth API is included in the Duo Beyond, Duo Access, and Duo MFA plans.

First Steps

Before starting:

1 Sign up for a Duo account.

2 Log in to the Duo Admin Panel and navigate to **Applications**.

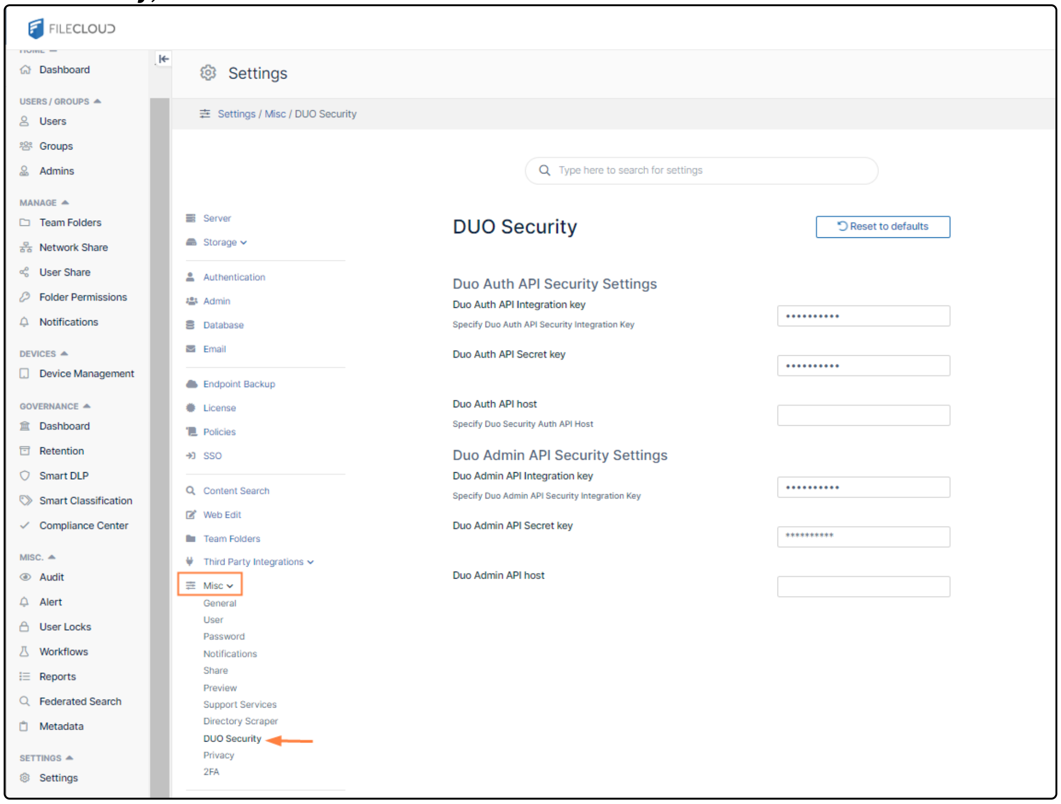
3 Click **Protect an Application** and locate **Auth API** in the applications list. Click **Protect this Application** to get your **integration key**, **secret key**, and **API hostname**. (See Getting Started for help.)

Review the API Details to see how to construct your first API request. Duo Security also provides demonstration clients available on Github to call the Duo API methods. Examples are available in: Python, Java, C#, Ruby, Perl, and PHP. Adding Duo requires some understanding of your application's language and authentication process.

Documented properties will not be removed within a stable version of the API. Once a given API endpoint is documented to return a given property, a property with that name will always appear (although certain properties may only appear under certain conditions, like if the customer is using a specific edition).

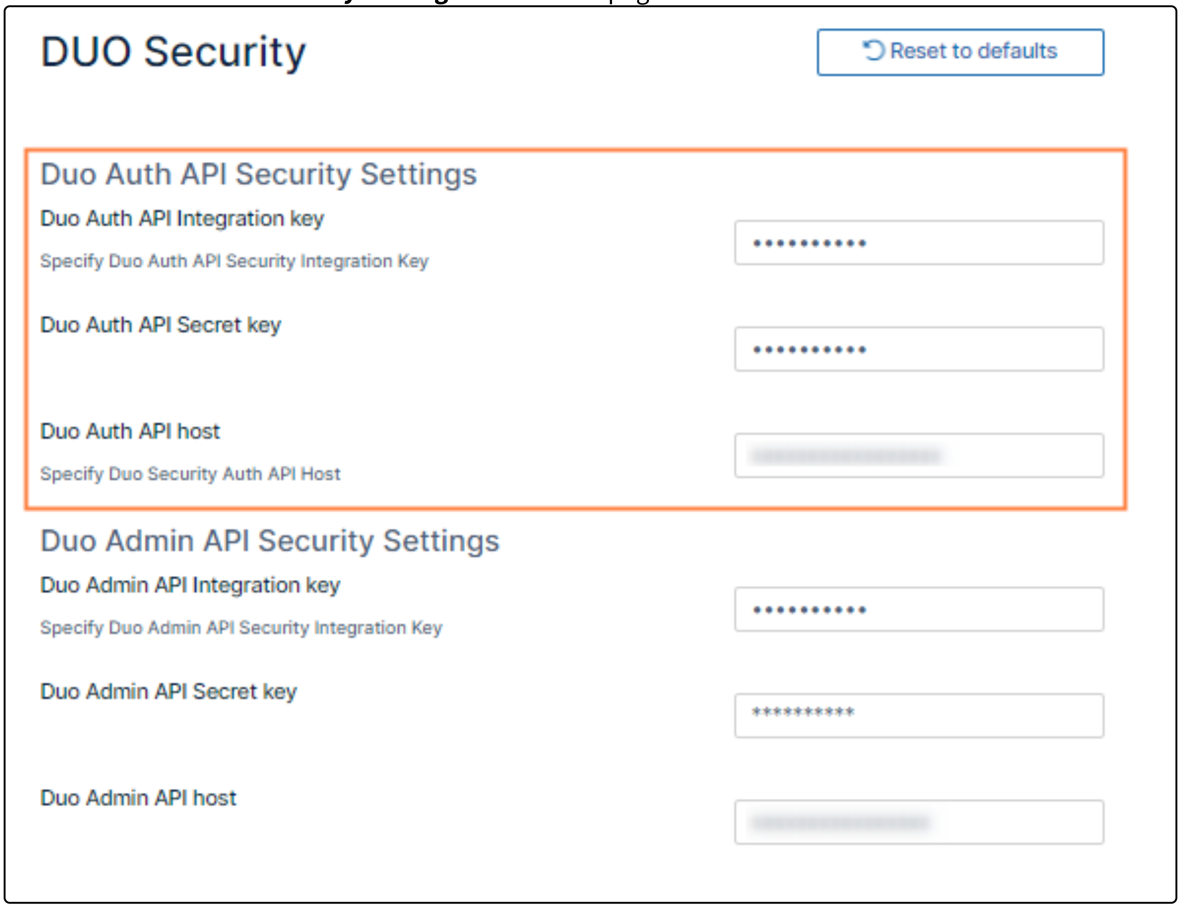
- In the FileCloud admin portal, open the **DUO Security** settings page.
  To go to the Duo Security settings page
    i. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

ii. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **DUO Security**, as shown below.



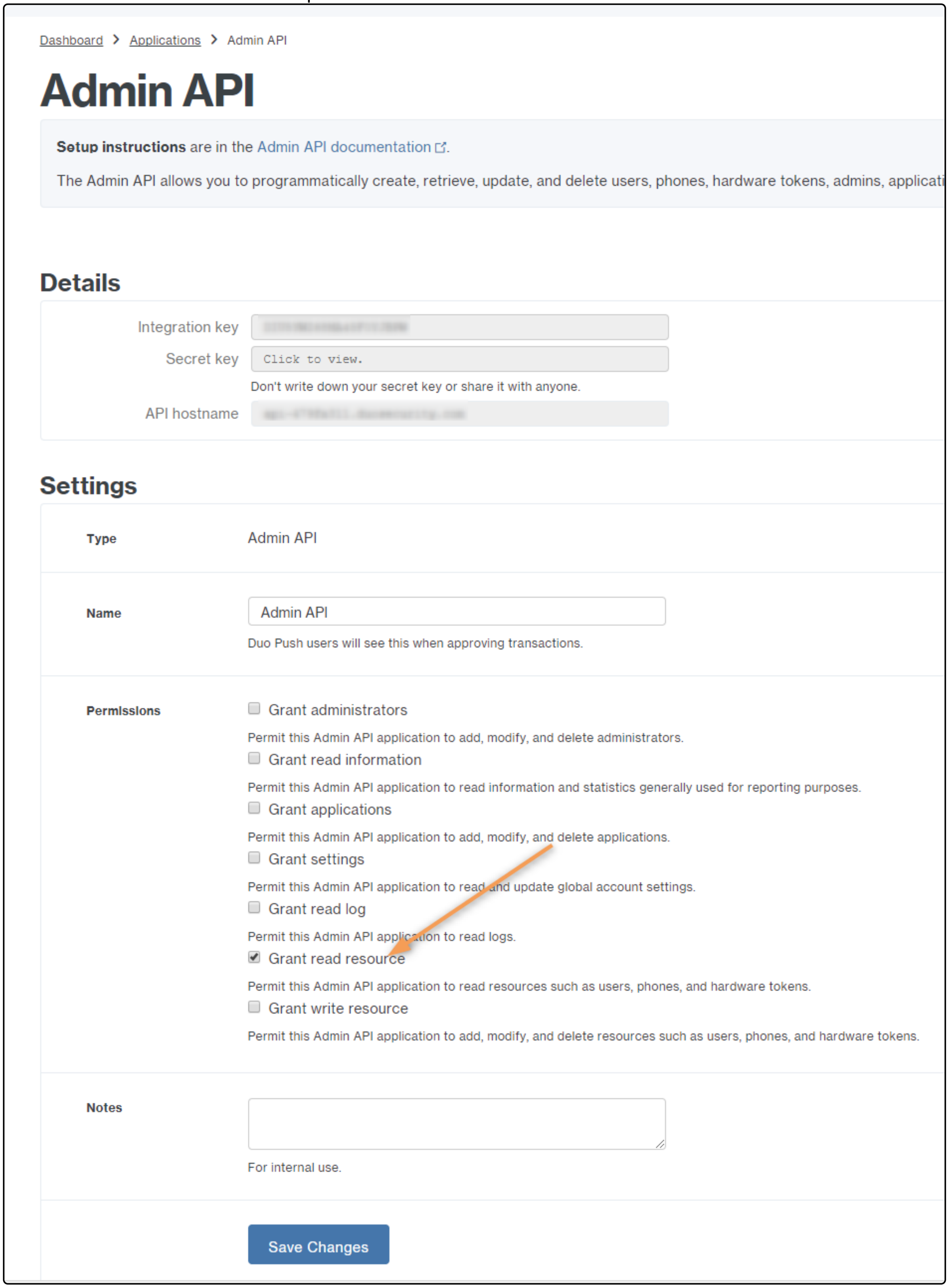
The **DUO Security** settings page opens.

- Fill in the **Duo Auth API Security Settings** fields on the page.



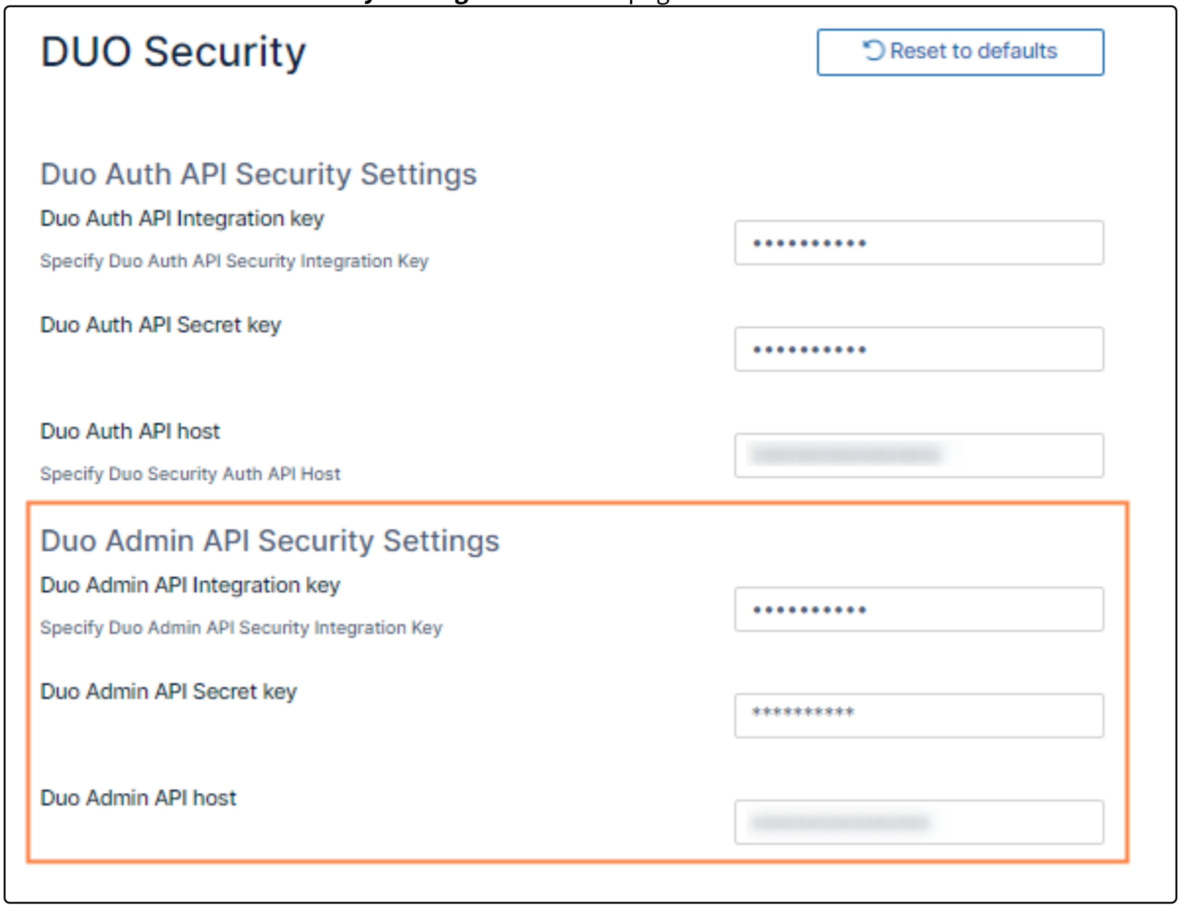
2. Add DUO Admin API
    - Follow instructions at https://duo.com/docs/adminapi to get values for **integration key**, **secret key**, and **API hostname**

- Ensure it has **Grant read resource** permission.



- In the FileCloud admin portal, go to the **DUO Security** settings page as shown in Step

- Fill in the **Duo Admin API Security Settings** fields on the page.



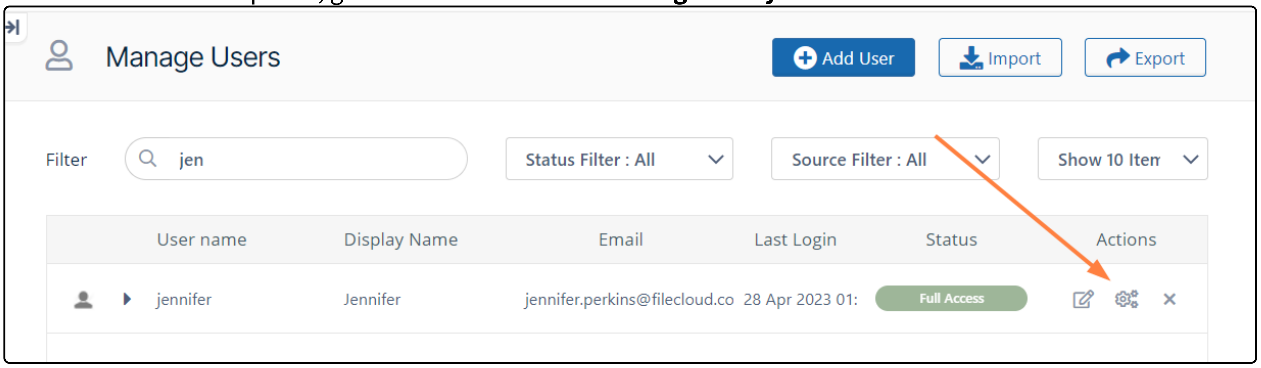
- Now follow the instructions above to enable 2FA and specify the 2FA mechanism as Duo Security.

  Note: When users who are enrolled in the Duo Admin Panel log in, they must use the text code from the default entry in their Duo App. When users who are not enrolled in the Duo Admin Panel attempt to log in, they are prompted to use a QR code scanner to enroll themselves, and then must use the text code from the entry they added in their Duo App. See Log in Using Two-Factor Authentication for more information.

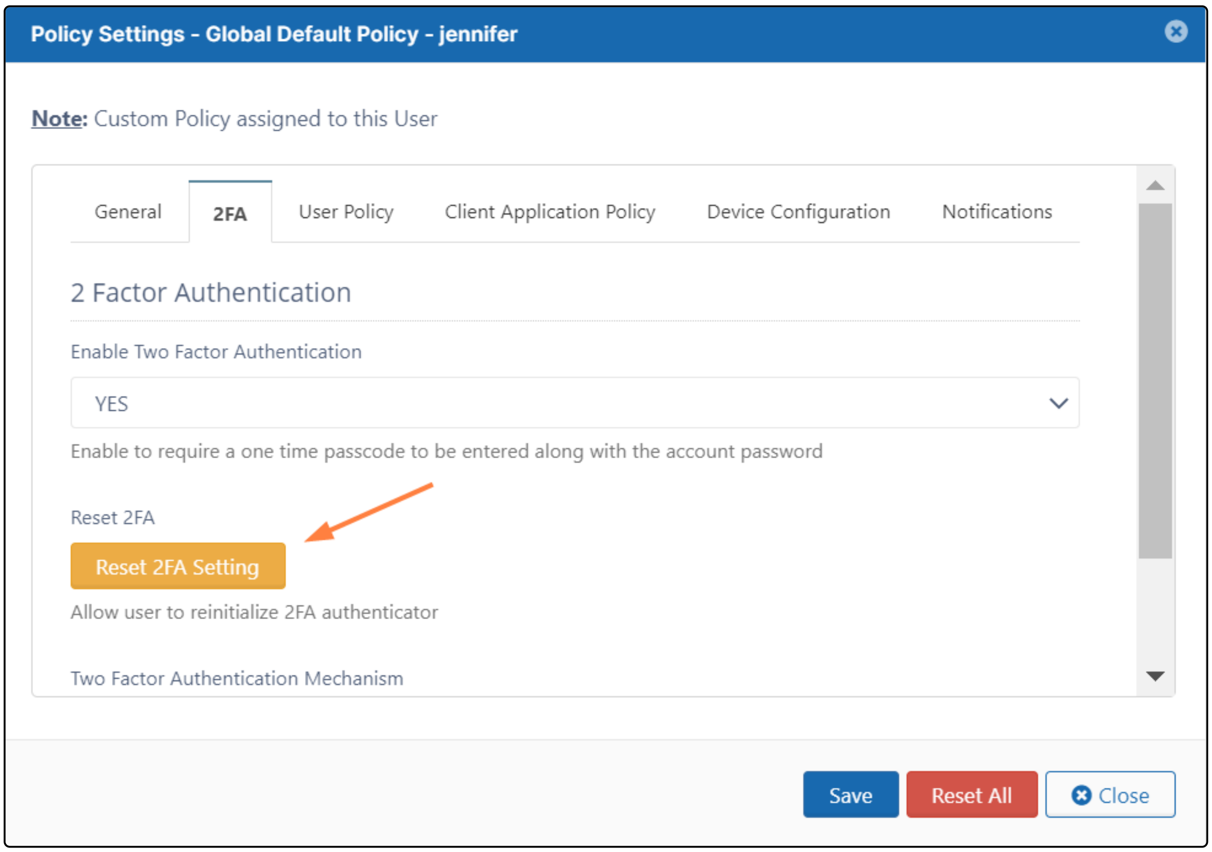
Reset TOTP or DUO settings for a user

When a user loses a TOTP (Google Auth) app enabled device or if they need to reset the code for any reason, you can reset the Google Authenticator setup for that user using the following steps.

1. In the FileCloud admin portal, go to **Users** and click the **Manage Policy** icon in the row for the user.



2. Click the **2FA** tab.
3. Click the **Reset 2FA Setting** to enable the user to reset their authenticator code.



After the secret is reset, the user is not required to redo the DUO 2FA setup on initial login as FileCloud will import access tokens from DUO automatically.
New devices can be registered from the DUO Admin Panel using the DUO Enrollment Email feature.

Two-Factor Authentication for Admin Portal

> ⚠ TOTP authentication for the admin portal is available beginning in FileCloud 23.242. TOTP authentication should work correctly with any authenticator app; however, the following apps have been tested and performed successfully: Google Authenticator, TOTP Authenticator, Duo Mobile, Microsoft Authenticator, Authy, Okta Verify, 2FA Authenticator (2FAS)

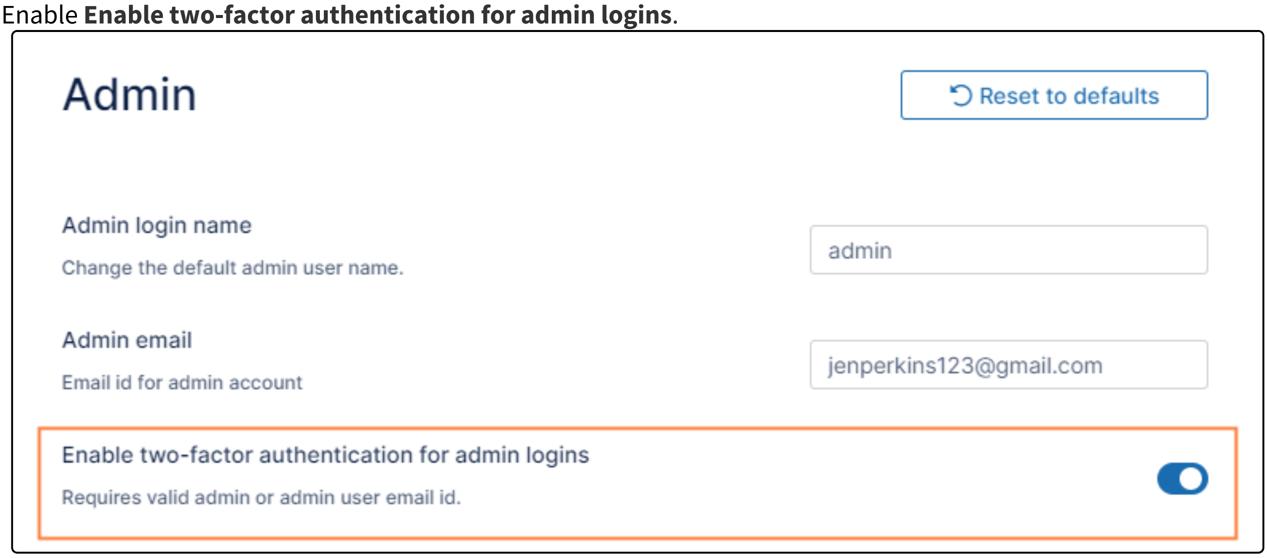
Support for two-factor authentication is available for admin portal login. Both the primary FileCloud admin and the superadmin (for multitenancy) can be set to require the additional code in order to access the admin portal.

Two-factor authentication for the admin portal supports authentication by email, SMS, and TOTP.

Enable two-factor authentication for admins

To enable 2FA for the first time an admin logs into the admin portal:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Admin**  .
   The **Admin** settings page opens.
2. Enable **Enable two-factor authentication for admin logins**.

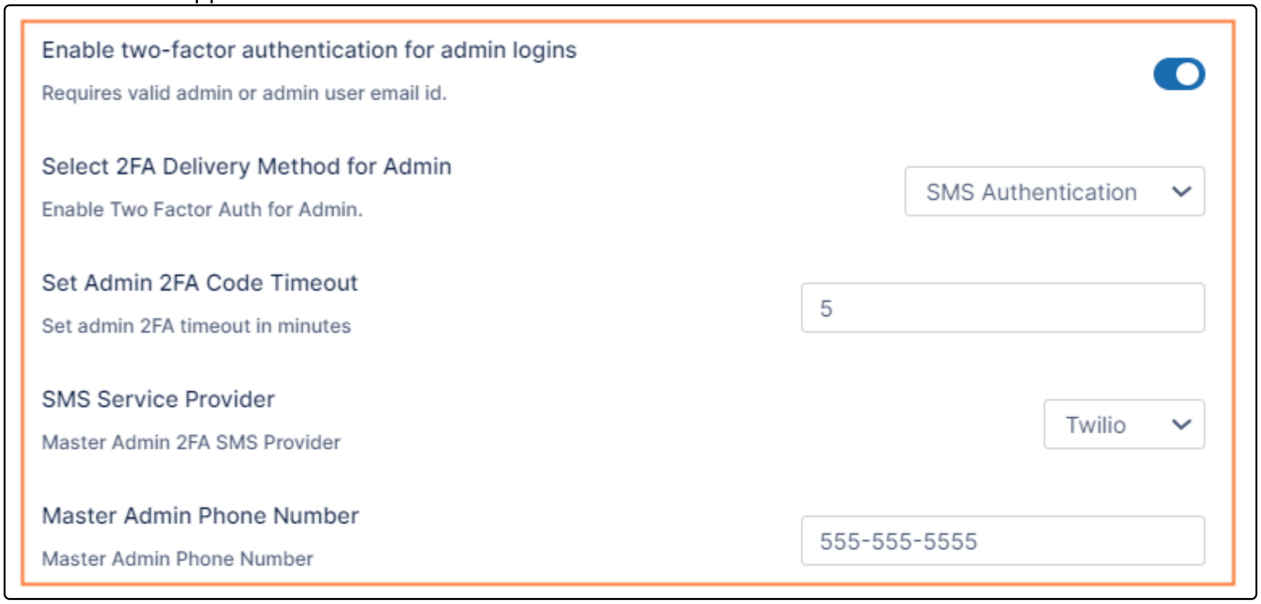


   2FA fields appear.

Setting 2FA delivery method to SMS

Note: Currently SMS authentication is effective for the primary admin, but not for promoted admins.

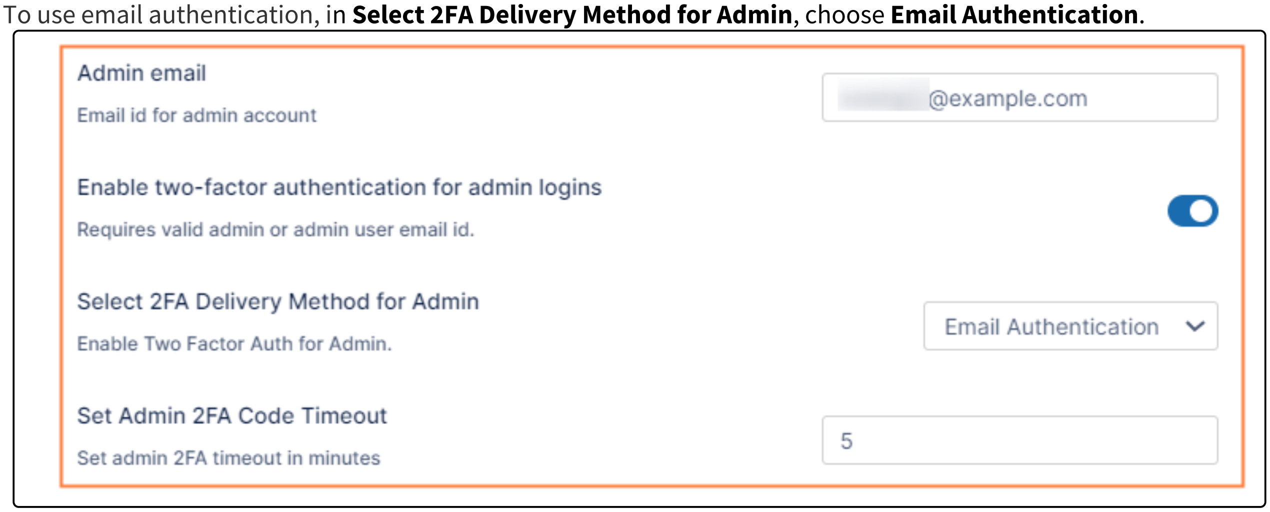
1. To use SMS authentication, In **Select 2FA Delivery Method for Admin**, choose **SMS Authentication**.
   Additional fields appear.



2. In **Set Admin 2FA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.
3. In **SMS Service Provider**, choose **Twilio** or **Custom**.
4. In **Master Admin Phone Number**, enter the admin's SMS phone number.
   An invalid master admin phone number will cause lockout - the portal will not be accessible when SMS Authentication is chosen.

Setting 2FA delivery method to email:

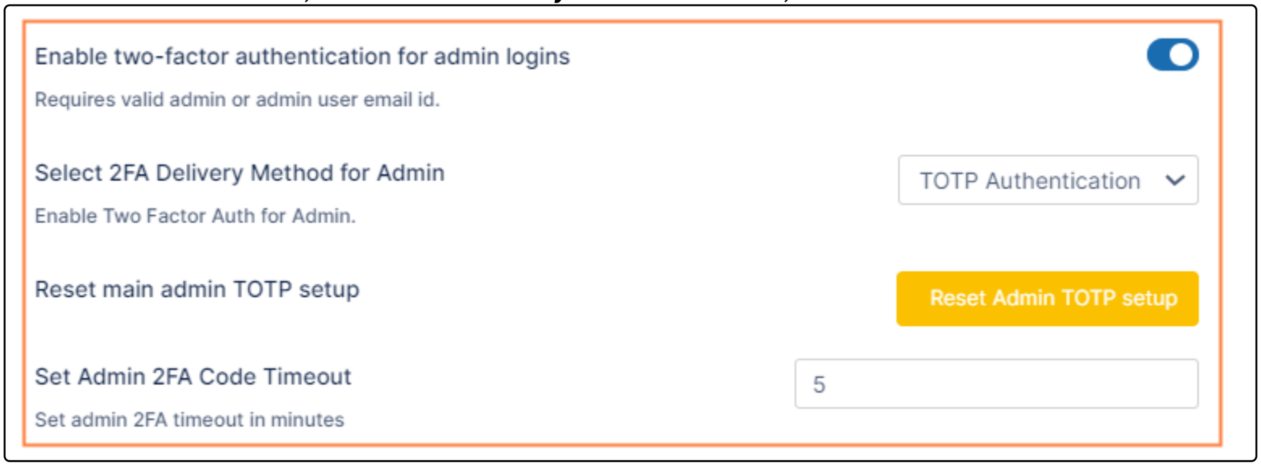
1. To use email authentication, in **Select 2FA Delivery Method for Admin**, choose **Email Authentication**.



2. Enter a valid email in the **Admin email** field above the **Enable Two Factor Authentication for Admin Logins** field.
3. In **Set Admin 2FA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.

Setting 2FA delivery method to TOTP

1. To use TOTP authentication, in **Select 2FA Delivery Method for Admin**, choose **TOTP Authentication**.

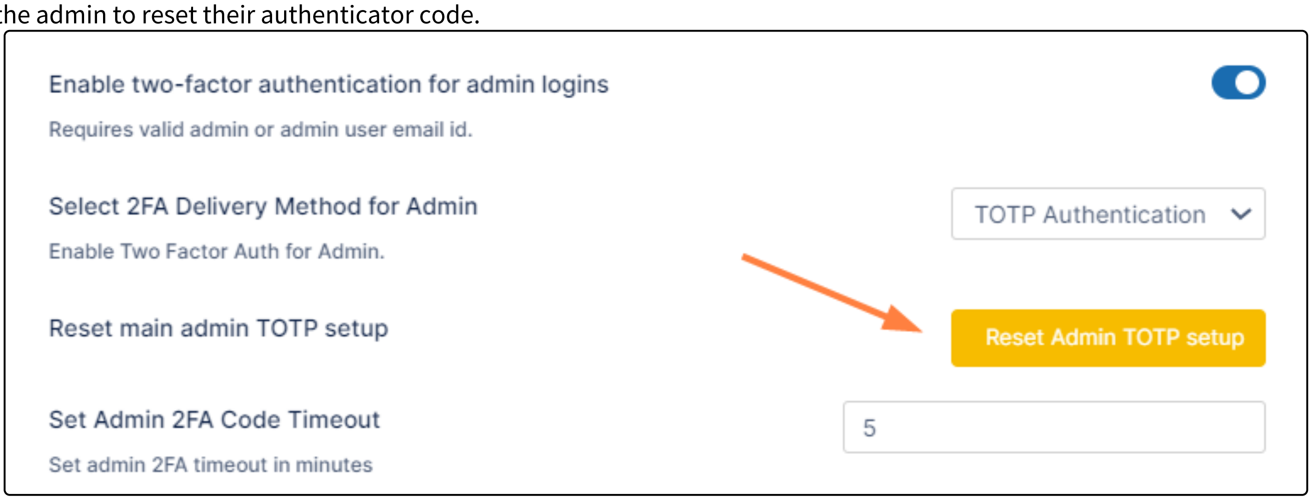


2. In **Set Admin 2FA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.
3. See Log in Using Two-Factor Authentication to set up Google Authenticator (or a similar authenticator app) to use for TOTP Authentication.

   Promoted admins use the method to log in to the admin portal that they use to log in to the user portal.

Reset TOTP settings for the primary admin

When you select TOTP Authentication for the 2FA delivery method, the setting **Reset Admin TOTP setup** appears below it. If the primary admin loses their TOTP-enabled device or needs to reset the TOTP authenticator code for another reason, a promoted admin with **Settings** read and update role privileges can click **Reset Admin TOTP setup** to enable the admin to reset their authenticator code.



Reset TOTP settings for promoted admins

Since promoted admins use their user login method rather than their admin login method to log into the admin portal, a promoted admin will only log in to the admin portal with TOTP if that is the method set for their user account, and therefore, to reset a promoted admin's TOTP authorization, use the method explained in Two-Factor Authentication for User Portal.

Single sign-on (SSO)

Single sign-on (SSO) is only available in some versions of FileCloud Online.

Single sign-on (SSO) is a user authentication process that permits a user to enter one name and password in order to access multiple applications.

FileCloud supports the following types of Single sign-on model.

- SAML Single Sign-On Support
- ADFS Single Sign-On Support
- NTLM Single Sign-On Support

SAML Single Sign-On Support

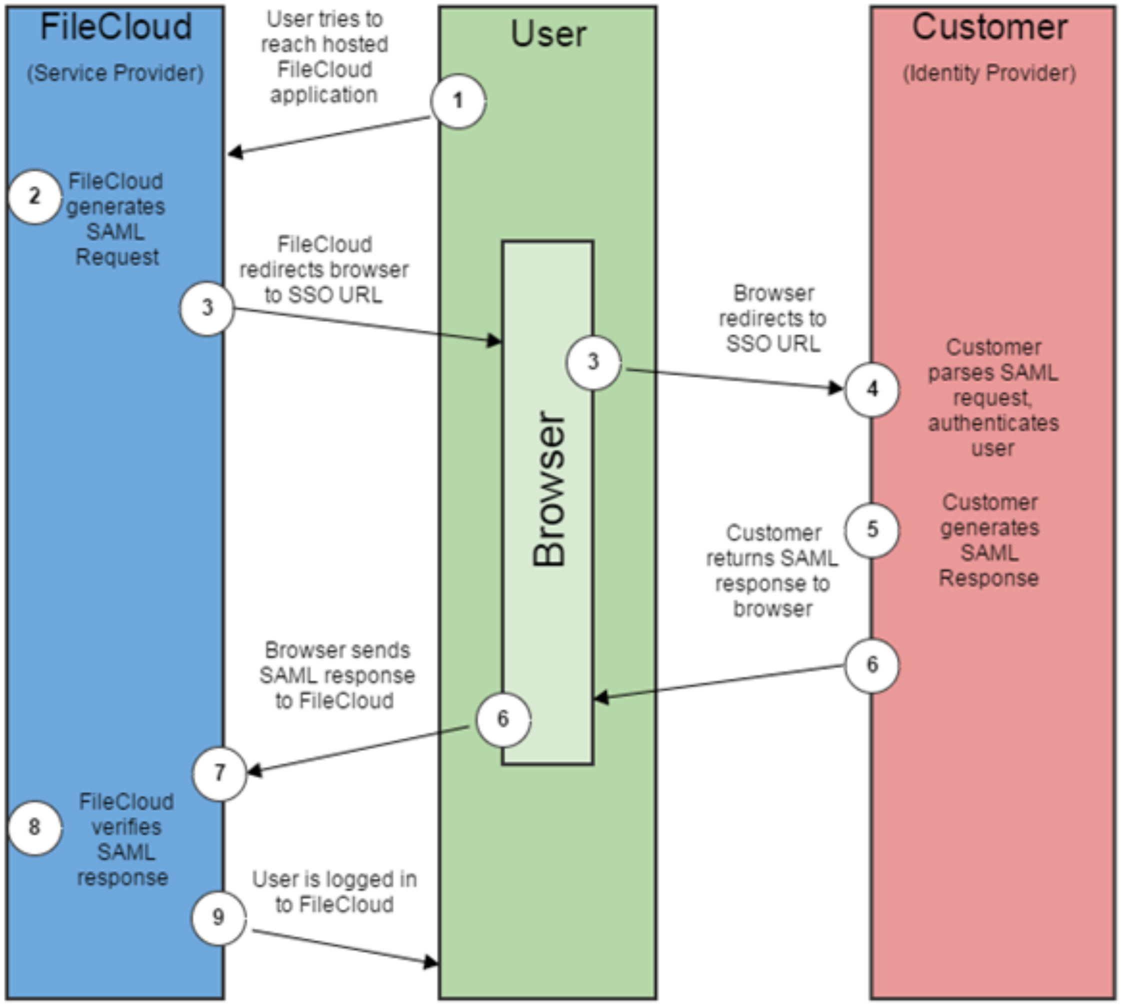
You can use SAML SSO to control the authorization and authentication of hosted user accounts that can access FileCloud Web based interface.

- SAML is an XML-based open standard data format for exchanging authentication and authorization data between parties.
- FileCloud supports SAML (Security Assertion Markup Language) based web browser Single Sign On (SSO) service
- FileCloud acts as a Service Provider (SP) while the Customer or Partner acts as the identity provider (IdP).
  FileCloud SAML SSO service is based on SAML v2.0 specifications.

SSO Login Diagram

SSO Login Diagram

The following process explains how the user logs into a hosted FileCloud application through customer-operated SAML based SSO service.



FileCloud SAML Transaction Steps

1. The user attempts to reach the hosted FileCloud application through the URL.
2. FileCloud generates a SAML authentication request. The SAML request is embedded into the URL for the customer's SSO Service.
3. FileCloud sends a redirect to the user's browser. The redirect URL includes the SAML authentication request and is submitted to customer's SSO Service.
4. The Customer's SSO Service authenticates the user based on valid login credentials.
5. The customer generates a valid SAML response and returns the information to the user's browser.
6. The customer SAML response is redirected to FileCloud.
7. The FileCloud authentication module verifies the SAML response.
8. If the user is successfully authenticated, the user will be successfully logged into FileCloud.

When the IdP successfully authenticates the user account, the FileCloud (SP) authentication module verifies that the user account exists in FileCloud.

If the user account does not exist in FileCloud, then a new user account is created and the user is logged into FileCloud.

SSO Configuration Steps

In order to successfully configure SAML SSO, the following steps must be followed.

1. Configure Apache Webserver

To configure Apache Webserver for SAML SSO, please Contact FileCloud Support.

2. Ensure the correct FileCloud URL is set and uses HTTPS

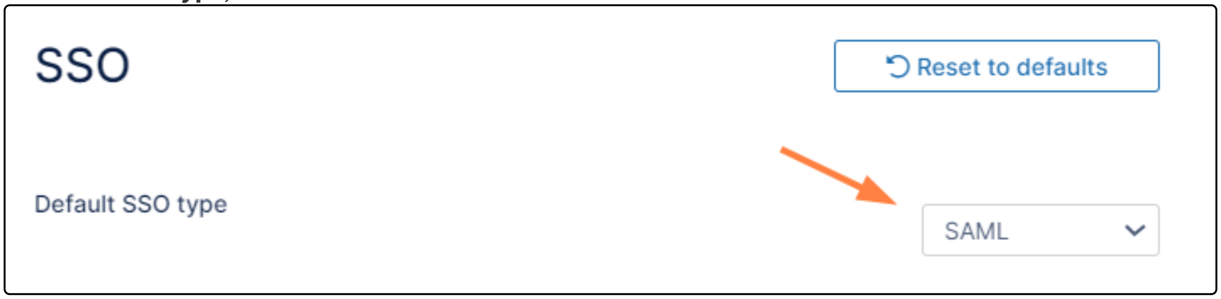
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Server**  .
   The **Server** settings page opens.
2. In the **Server URL** field, confirm that your URL begins with HTTPS.
3. Click **Check URL** to make sure your URL is valid.

3. Set SAML as the default single sign-on method in FileCloud

To set the SSO type in FileCloud:

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

2. In **Default SSO Type**, select **SAML**.

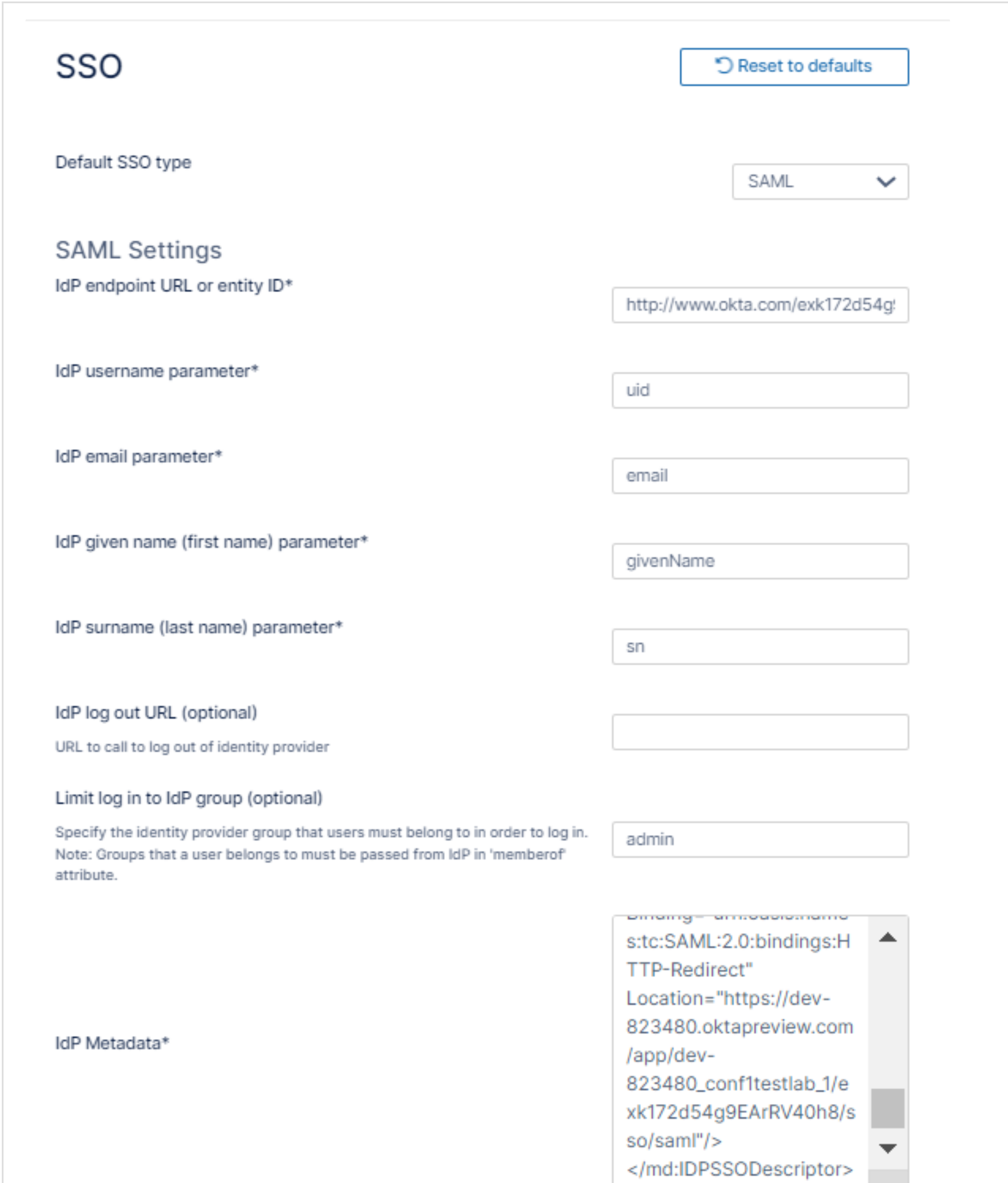


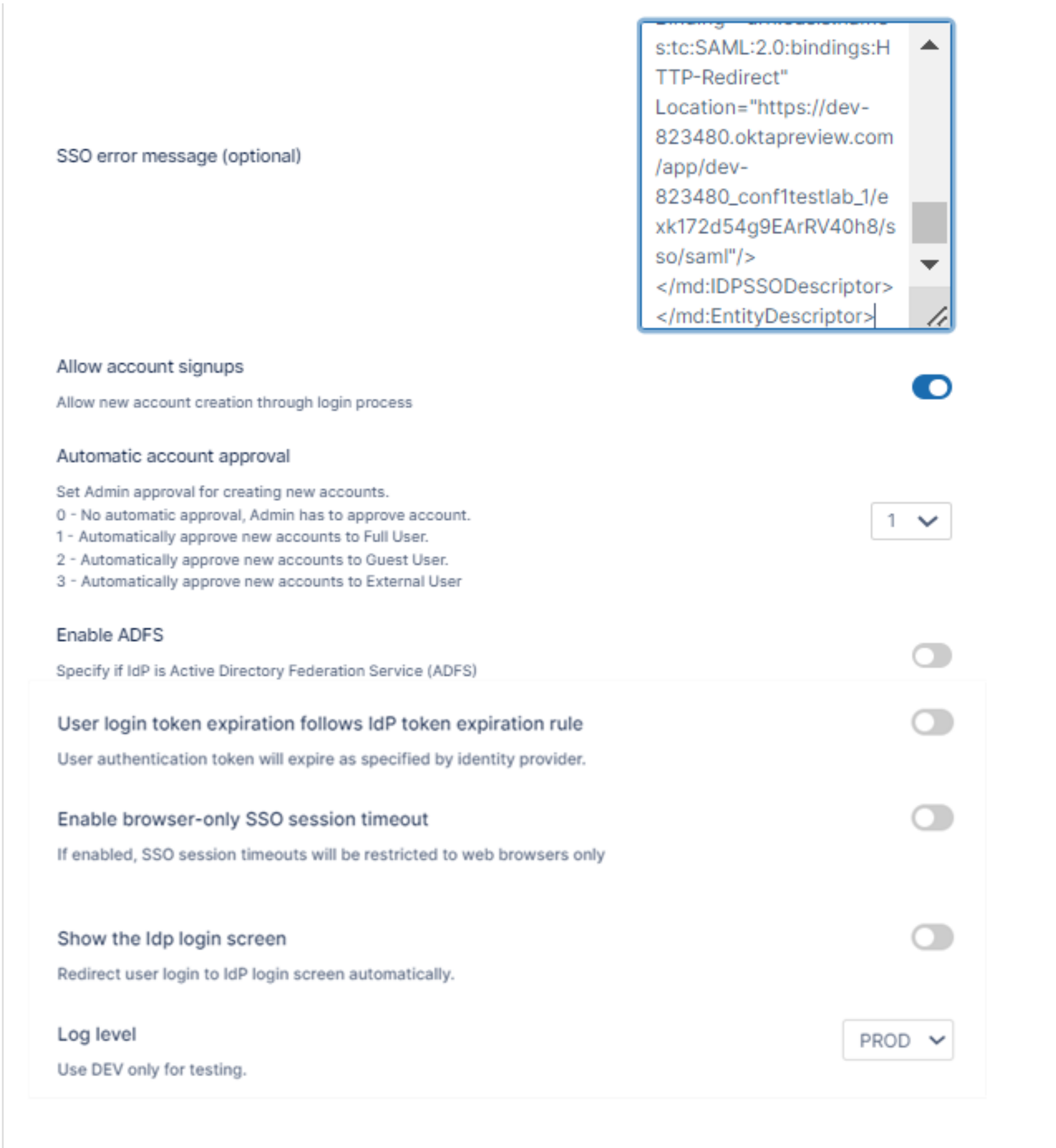
4. Configure IdP settings in FileCloud

Note: If you are using Active Directory Federation Services (ADFS) Support for authentication, see ADFS Single Sign-On Support.

To configure IdP settings in FileCloud:

1. In the FileCloud admin portal **SSO** settings page, fill in the settings under **SAML Settings**.


SSO
Reset to defaults
Default SSO type
SAML
SAML Settings
IdP endpoint URL or entity ID*
http://www.okta.com/exk172d54g
IdP username parameter*
uid
IdP email parameter*
email
IdP given name (first name) parameter*
givenName
IdP surname (last name) parameter*
sn
IdP log out URL (optional)
URL to call to log out of identity provider
Limit log in to IdP group (optional)
Specify the identity provider group that users must belong to in order to log in. Note: Groups that a user belongs to must be passed from IdP in 'memberof' attribute.
admin
IdP Metadata*
s:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://dev-823480.oktapreview.com/app/dev-823480_conf1testlab_1/exk172d54g9EArRV40h8/sso/saml"/>
</md:IDPSSODescriptor>



Use the following table to understand the IdP settings.

FileCloud Parameters	IdP Settings
IdP End Point URL	Identity Provider URL

FileCloud Parameters	IdP Settings
Idp Username Parameter	Identifies the Username (must be unique for each user) • Usually uid or agencyUID • Default value: uid **NOTE: The username must be unique**. If username sent by Idp is in email format, the email prefix will be used for username. The email prefix in this case must be unique.
IdP Email Parameter	Identifies the email of the user (must be unique) Default value: mail
IdP Given Name Parameter	Identifies the given name of the user Default value: givenName
IdP Surname Parameter	Identifies the surname of the user Default value: sn
IdP Log Out URL (Optional)	URL for logging out of IdP
Limit Logon to IdP Group	IdP Group Name • Specifying a group name means that a user can login through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group • The IdP must send this group name through the **memberof** parameter • The **memberof** parameter can include a comma separated value of all groups to which the user belongs
Show the IdP Logon Screen	Identifies which Logon screen the user will see: • FileCloud screen = not selected • IdP screen = selected
IdP Metadata	Identity Provider metadata in XML Format
SSO Error Message (Optional) Added in FileCloud 20.1	Custom error message that appears when a signin is invalid. Enter in HTML format.

FileCloud Parameters	IdP Settings
Allow Account Signups Added in FileCloud 20.1	When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.
Automatic Account Approval Added in FileCloud 20.1	This setting works with the **Allow Account Signups** setting to determine: • If the account created by the user is disabled until the administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. • Possible values are: 0 - No automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User
Enable ADFS	No
User login token expiration match Idp expiration	If enabled the user token expiration will be set based on Idp expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)
Enable Browser-Only SSO Session Timeout Added in FileCloud 23.232.1	If enabled, SSO session timeouts apply to browser sessions but not to client sessions.
Show the Idp Login Screen	If enabled, automatically redirect user to Idp log-in screen.
Log Level	Set the Log mode for the SAML Calls. Default Value: prod (Do not use DEV for production systems)

5. Register FileCloud as a Service Provider (SP) with the IdP

Use the following URL (Entity ID) to register FileCloud as an SP with IdP or ADFS. The URL below also provides the metadata of the FileCloud SP:

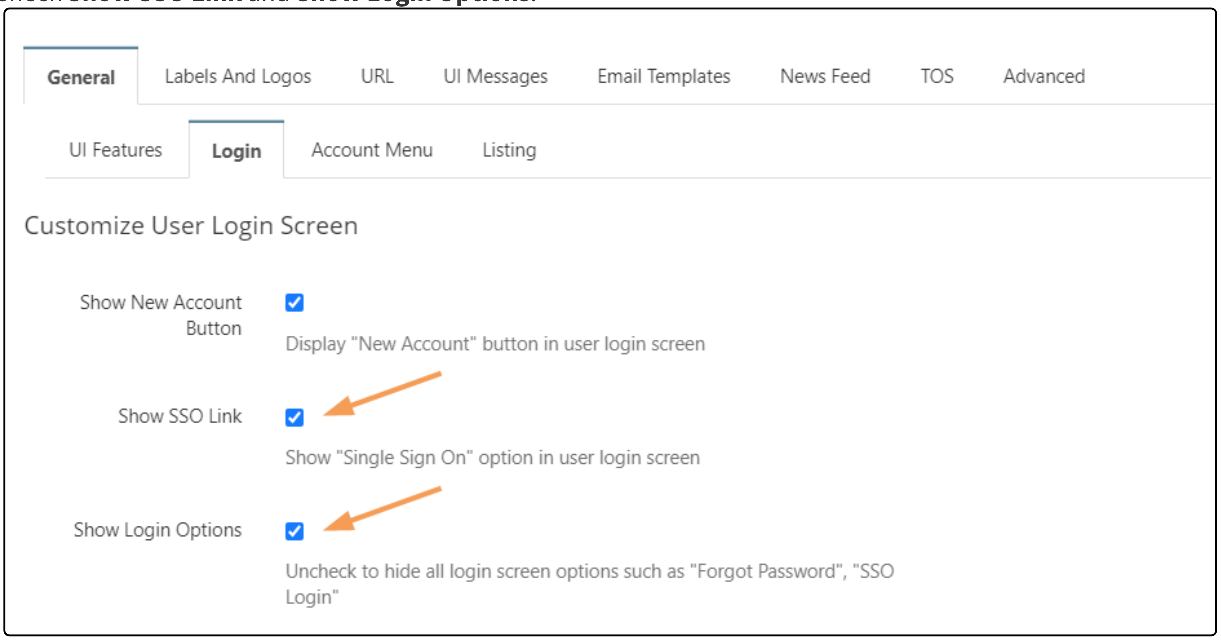
http://<Your Domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp

6. Enable the SSO link on the login page

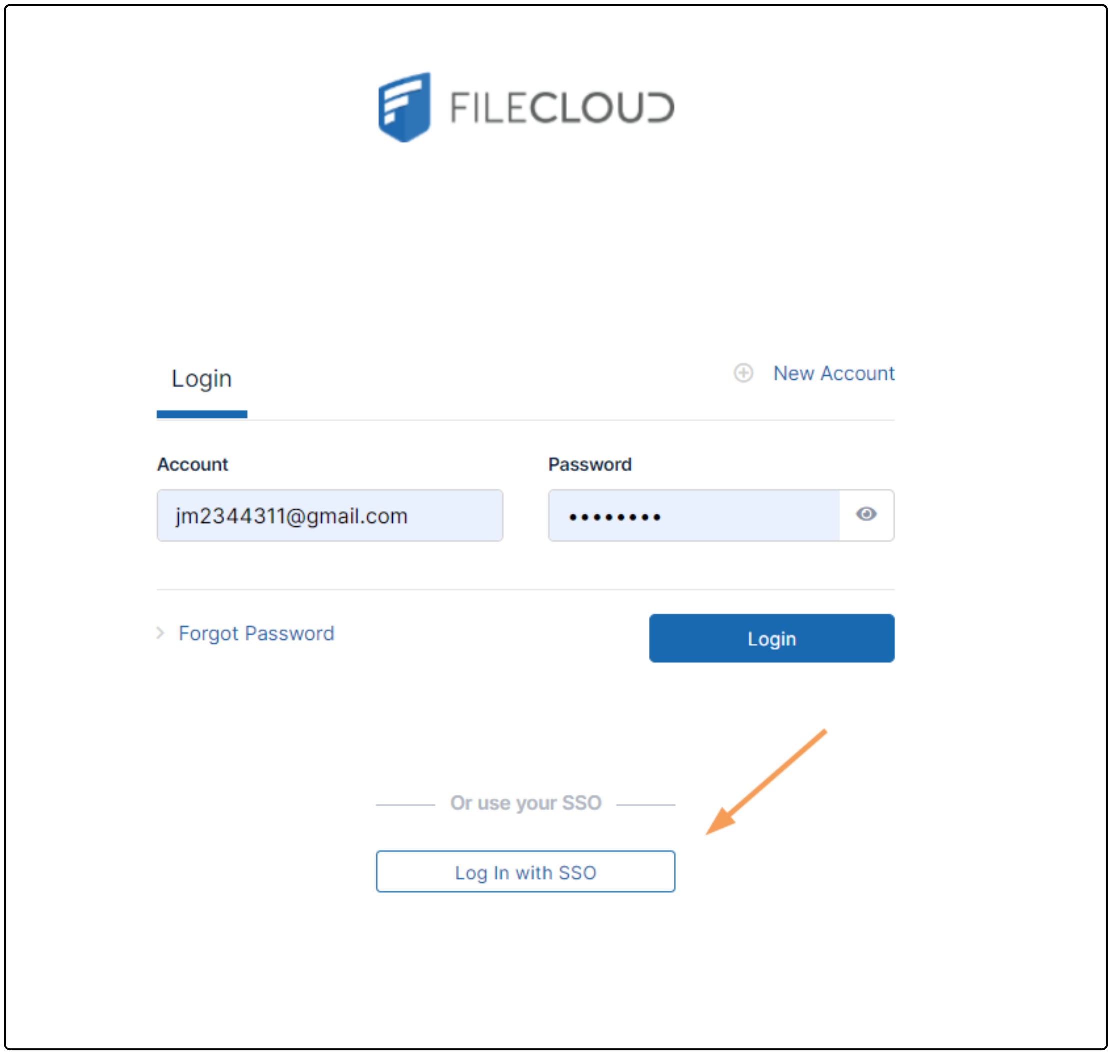
You can customize the user log-in screen to display the SSO log-in option along with the direct log-in option or to only display the SSO log-in.

To display the SSO log-in option along with the direct log-in option:

1. From the left navigation pane, click **Customization**.
2. Select the **General** tab, and then the **Login** sub-tab.
3. Check **Show SSO Link** and **Show Login Options**.



4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



On clicking the Single Sign-On link on the login page, the user is redirected to the SAML SSO Service web page.

To only display the SSO log-in the user portal or the admin portal, please Contact FileCloud Support.

Integrating with other applications

- Integrate Auth0 SSO with Filecloud
- Integrate Microsoft Entra ID with FileCloud
- Integrate Centrify with FileCloud
- Integrate CYBERARK with FileCloud
- Integrate JumpCloud with FileCloud
- Integrate Okta with FileCloud

- Integrate Google with FileCloud
- Integrate OneLogin with FileCloud
- Integrate ADSelfService Plus with FileCloud
- Integrate Ping Identity SSO with Filecloud
- Setting Up and Configuring Certificates when Upgrading SSO

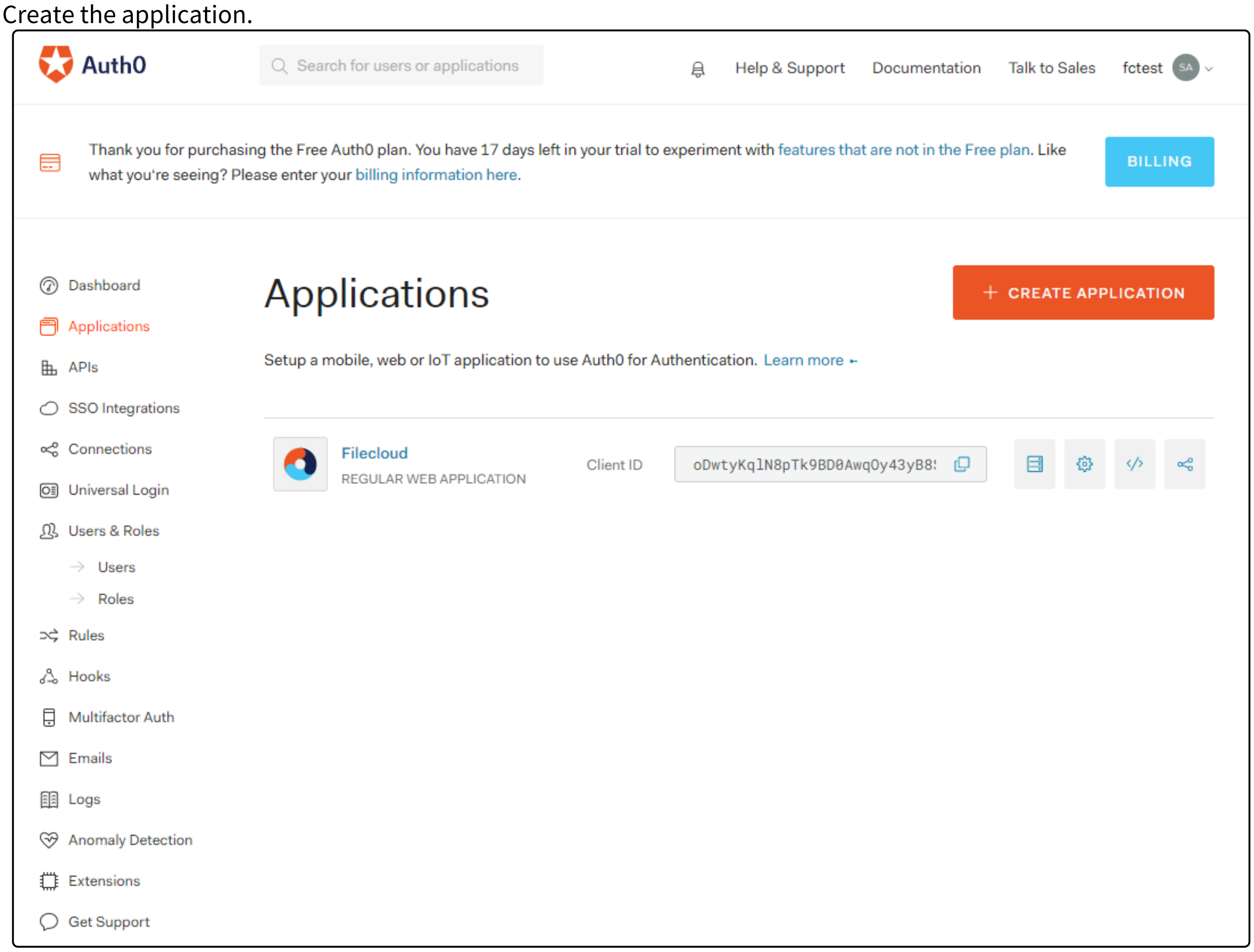
Integrate Auth0 SSO with Filecloud

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

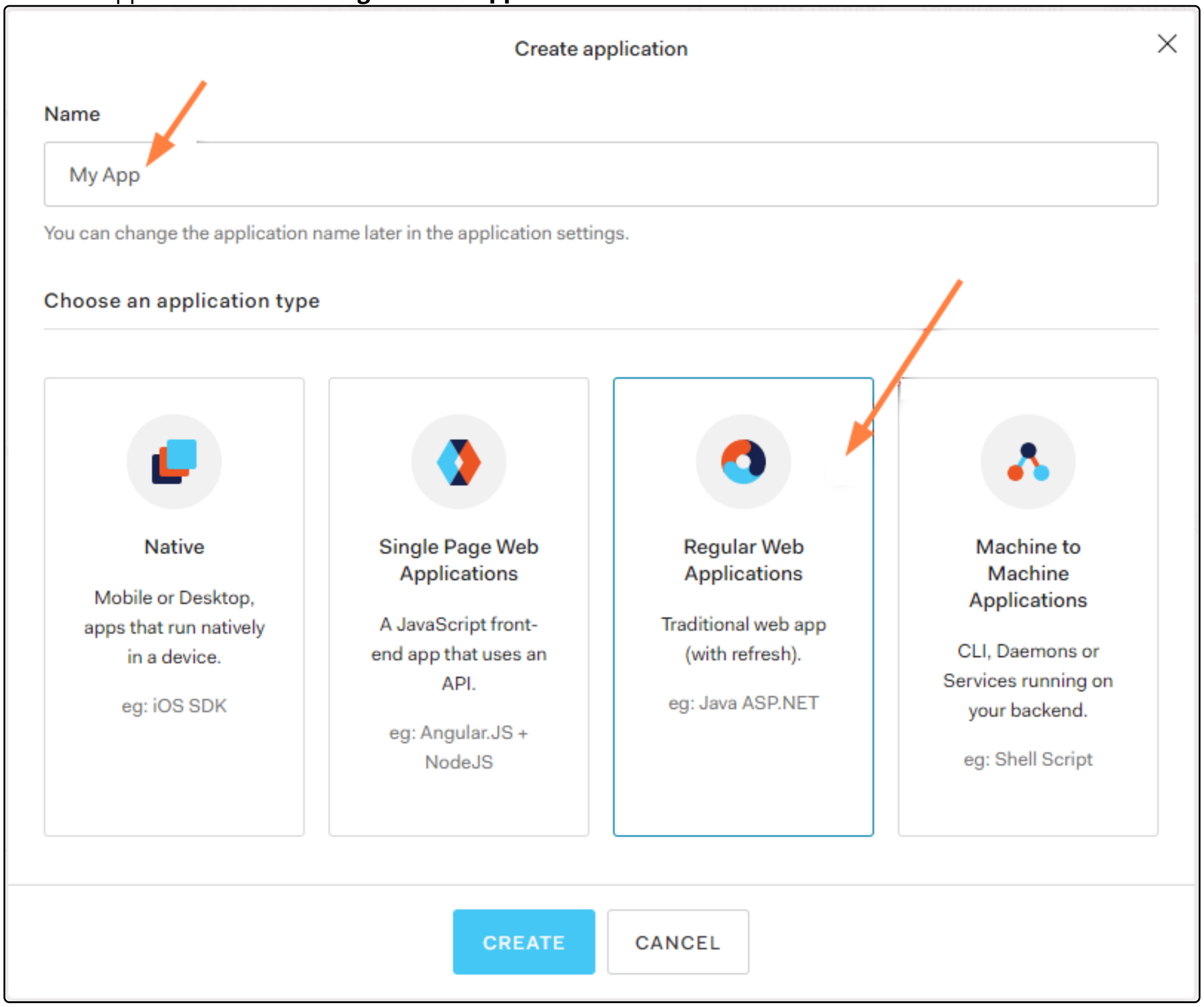
You can integrate Auth0 SSO with Filecloud using the SAML 2 protocol. Below are the steps to achieve this.

Configuration in Auth0 portal

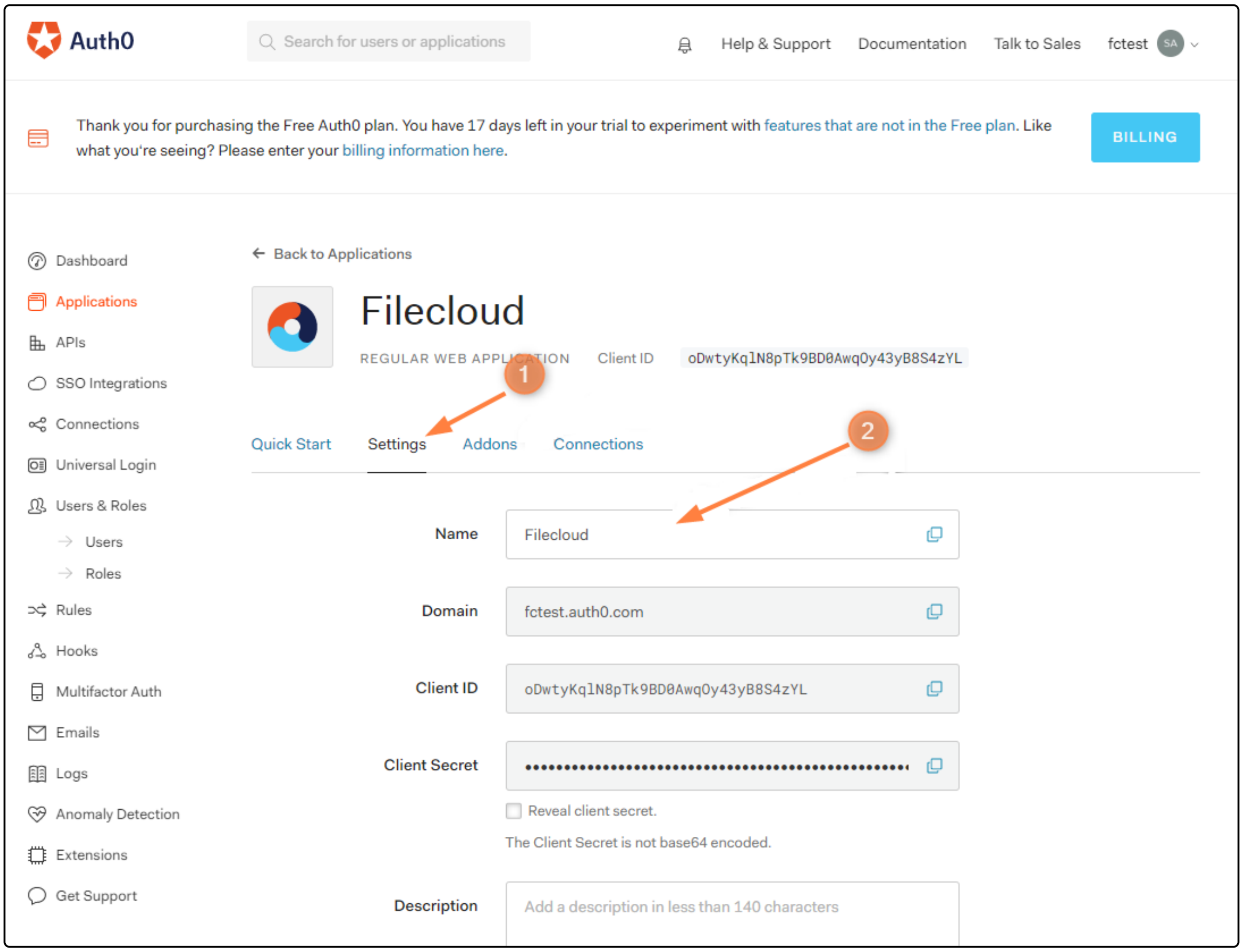
1. Log in to the Auth0 Dashboard and click the tab **Application** on the left panel.
2. Create the application.



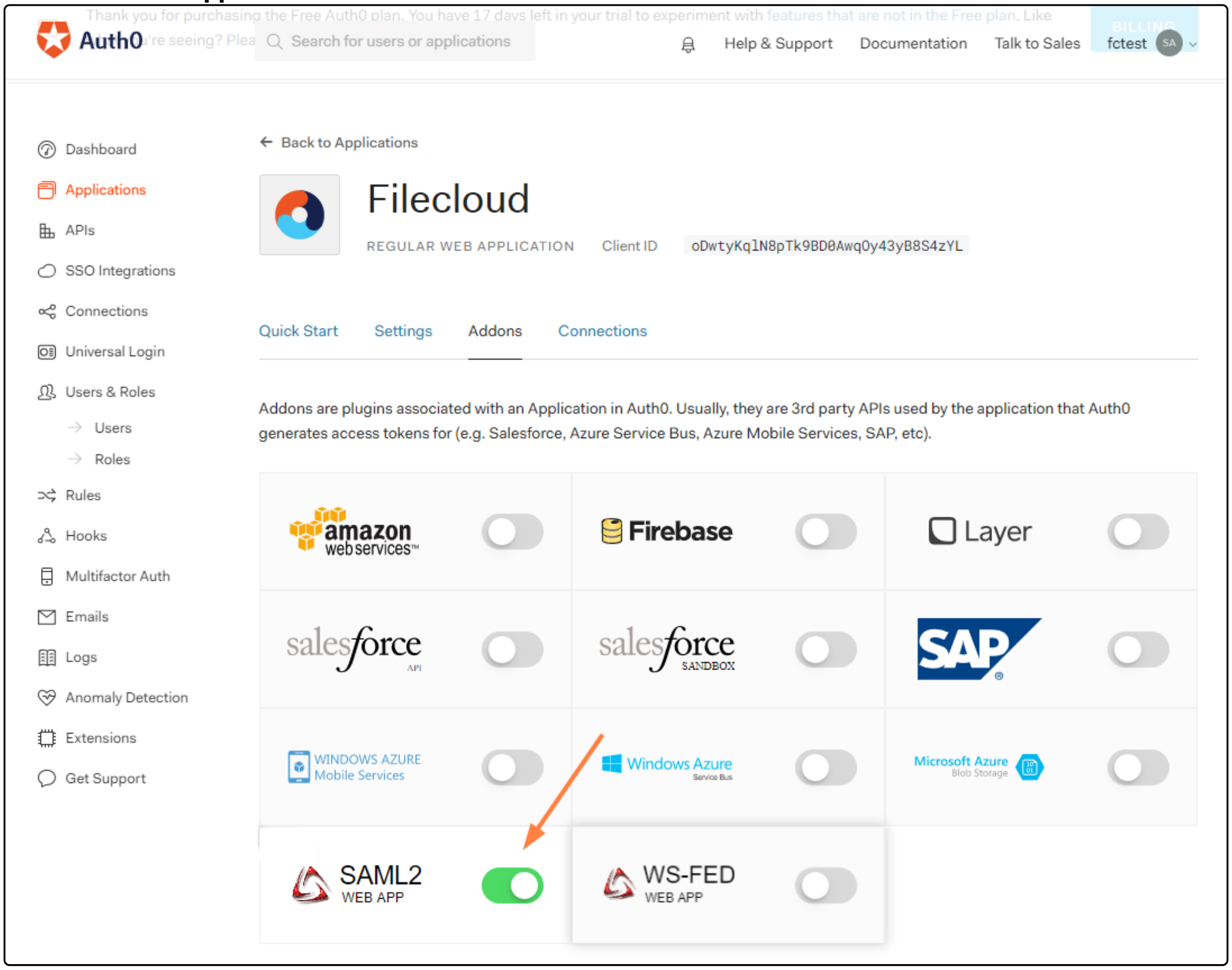
3. Name the application and click **Regular Web Applications**.



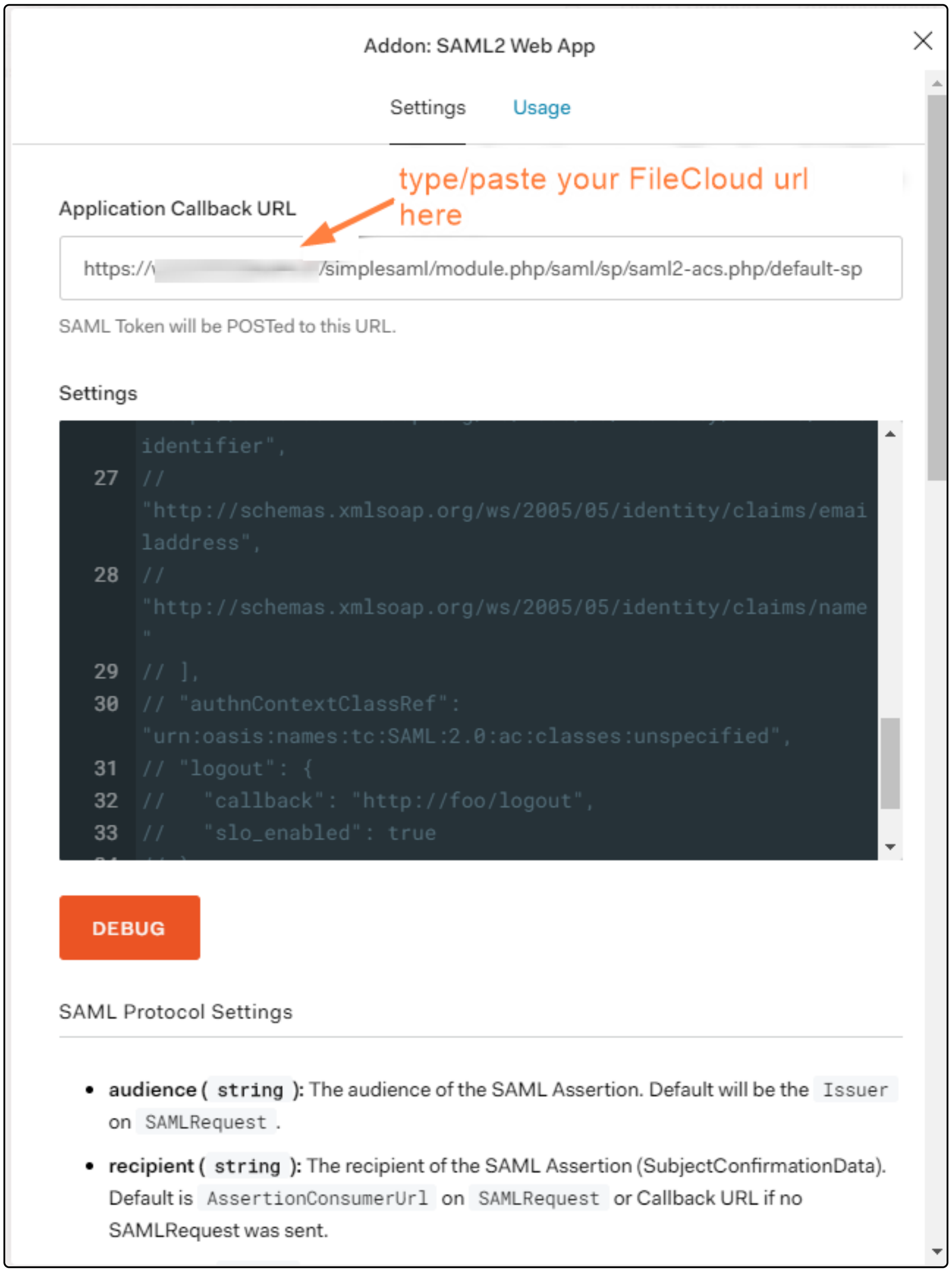
4. Click the created application again and go to the settings tab. Confirm that the application name is in the **Name** field and click **Addons**.



5. Click **SAML2 Web App**.

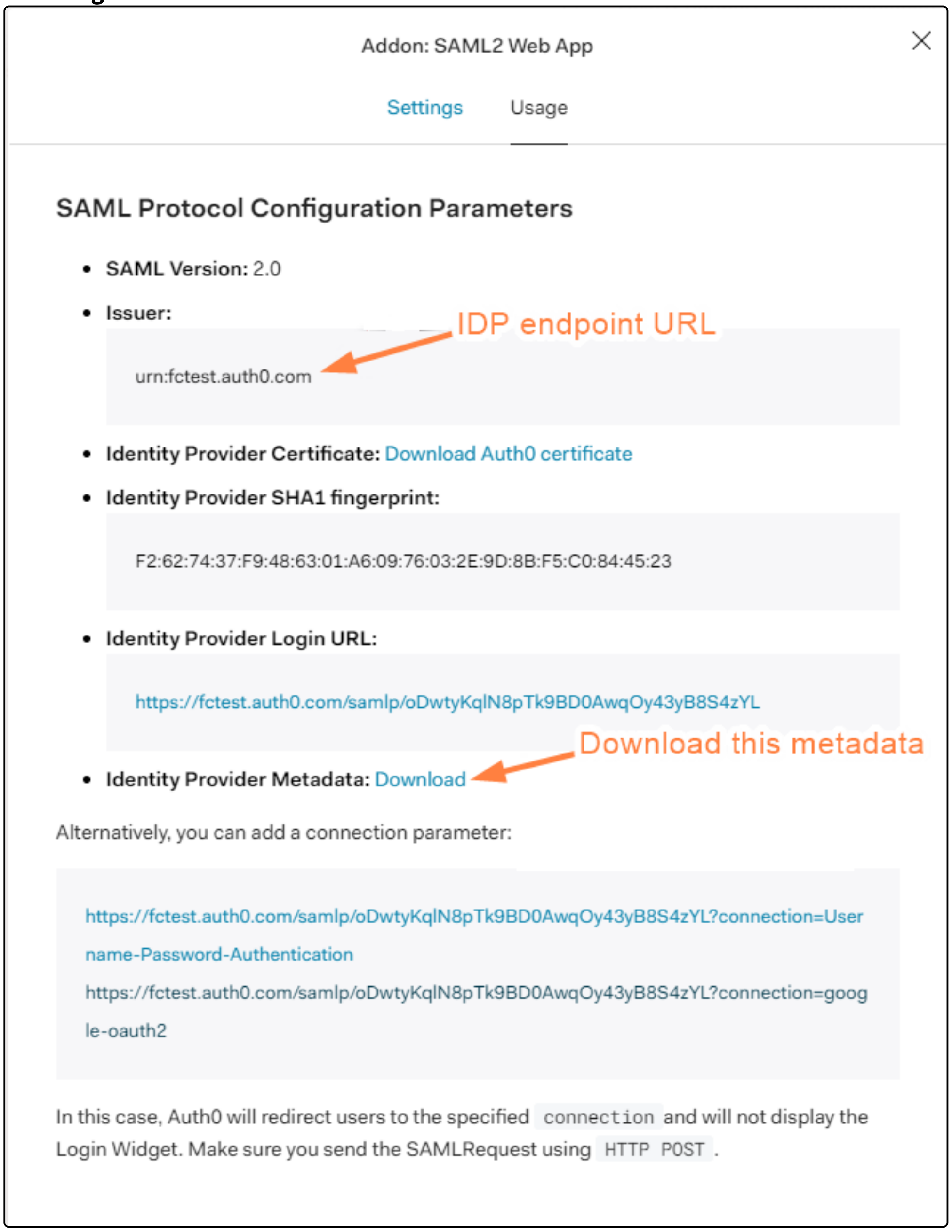


6. Enter your FileCloud URL in the **Application Callback URL**.
https://your_filecloud_url/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp



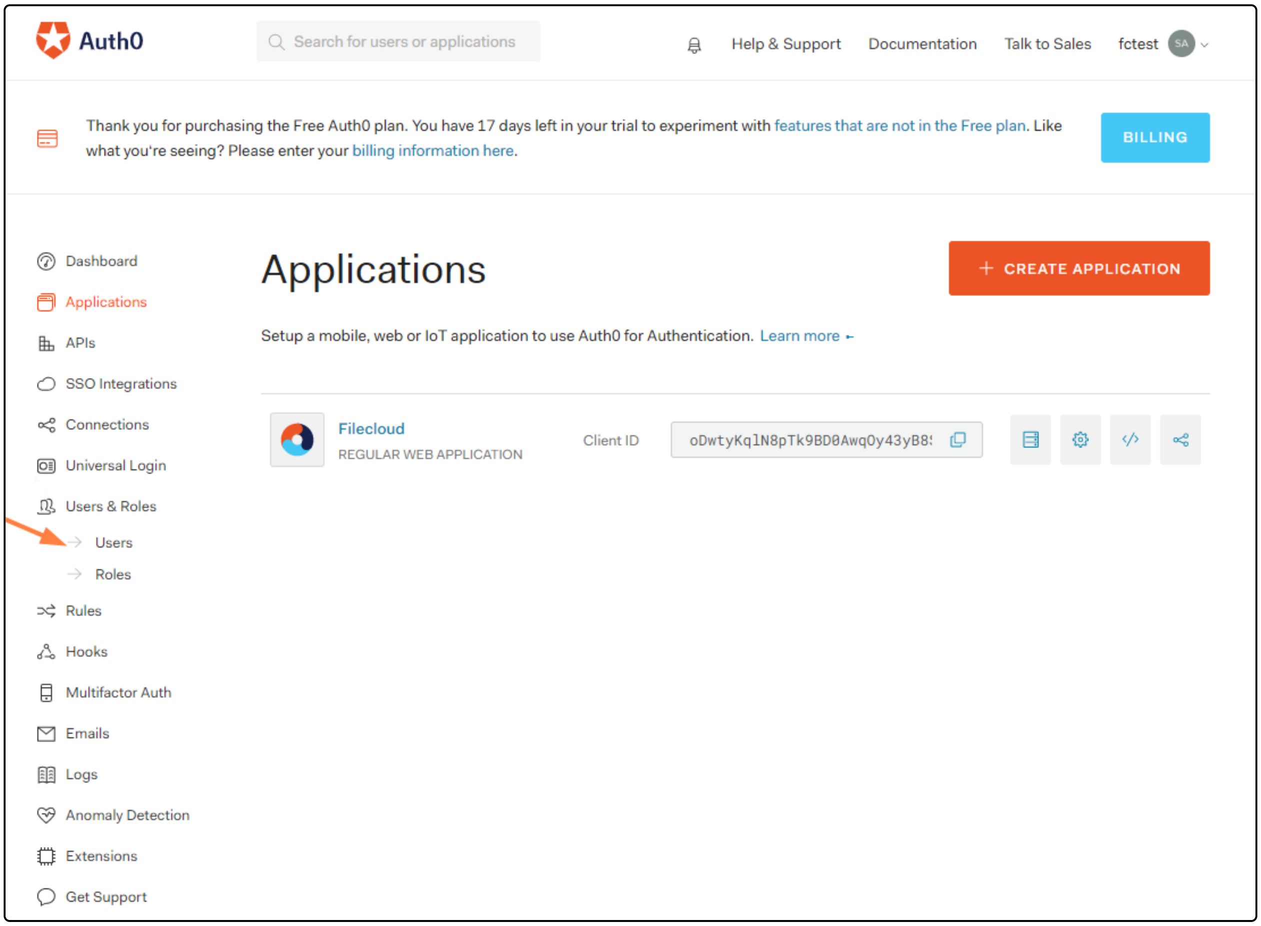
7. Scroll down and click **Enable**.

8. Click **Usage**.



9. Note down the value in the field **Issuer**.
10. Scroll down and download the metadata from **Identity Provider Metadata**.

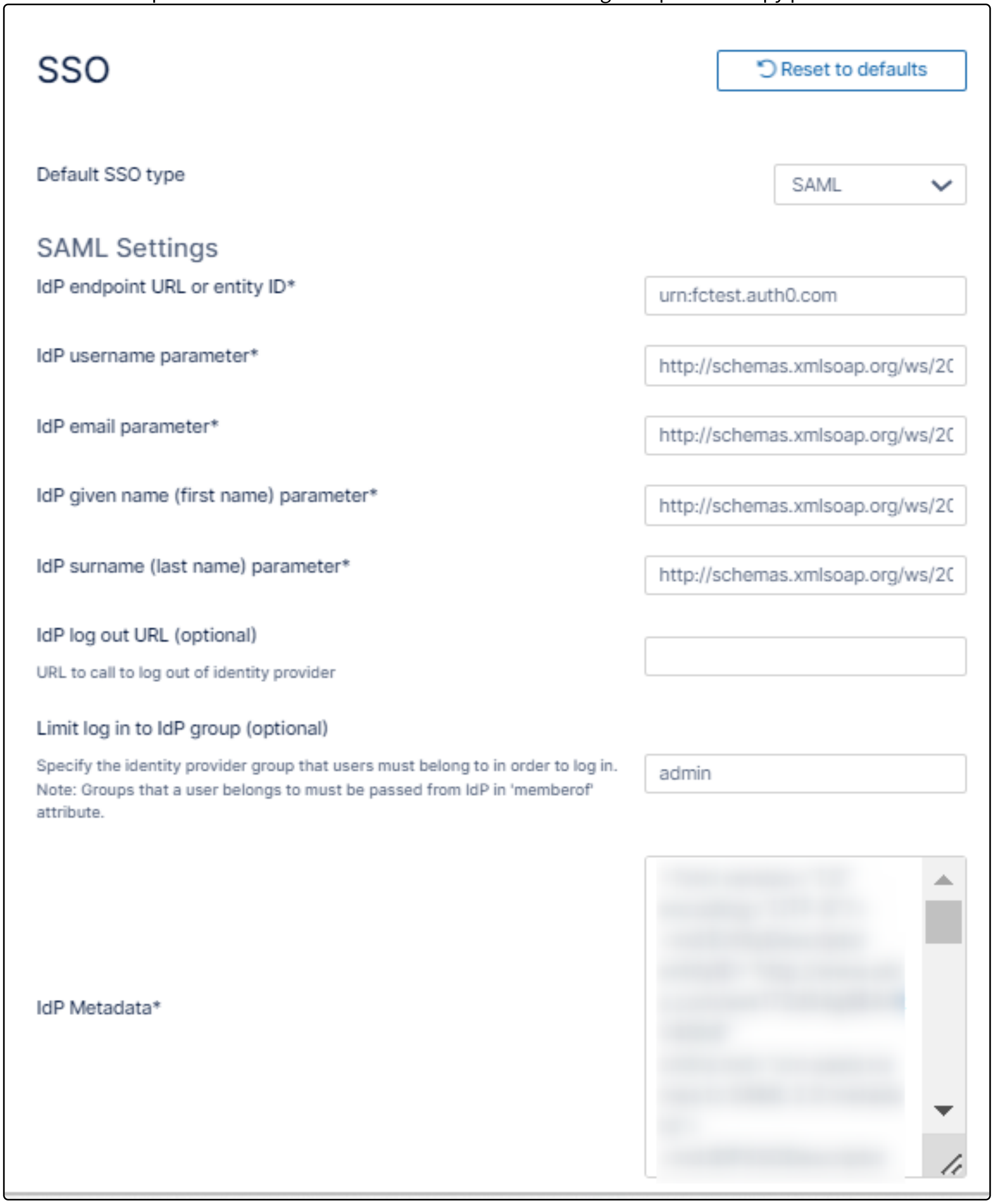
11. Go to **Users** in the Auth0 Dashboard and create the user.



Configuration in FileCloud admin portal

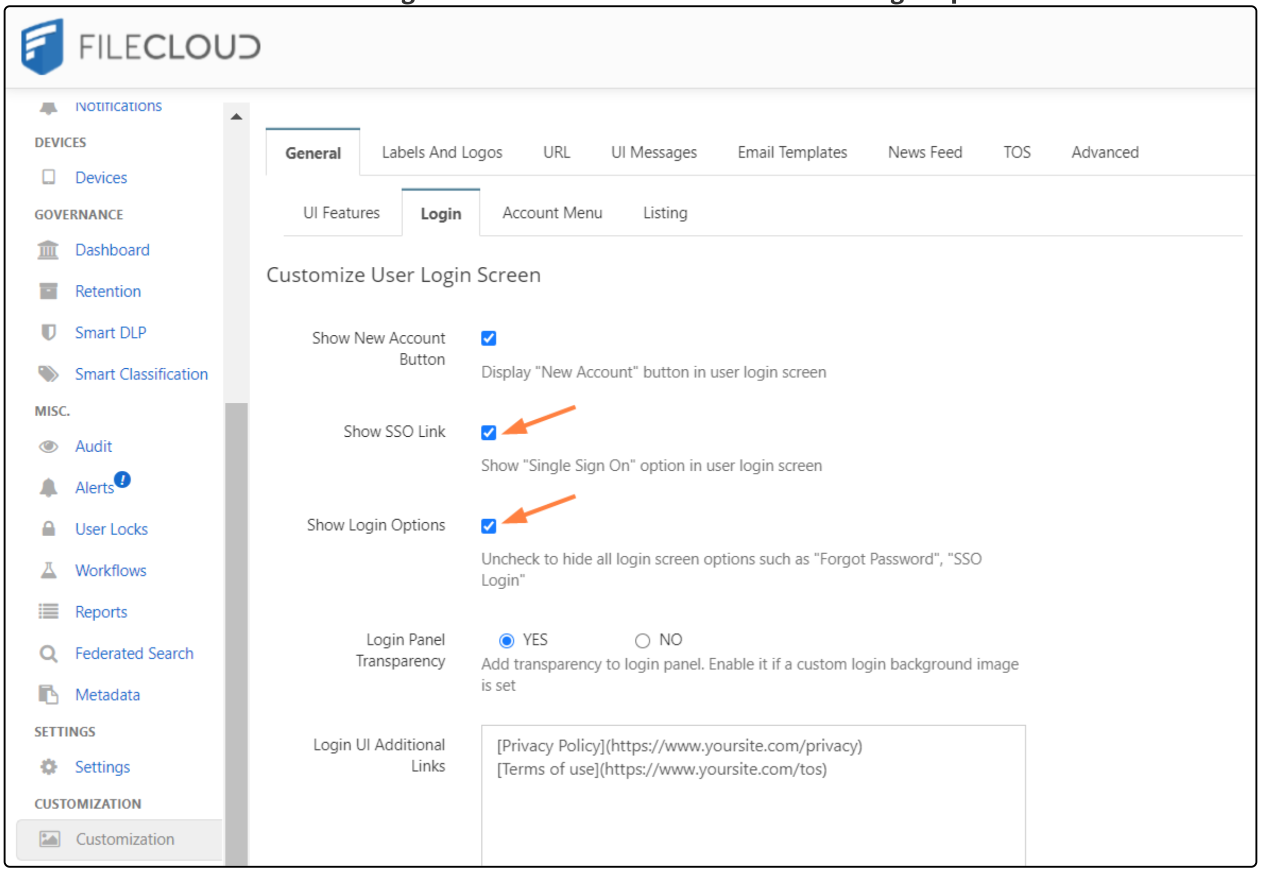
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. Enter the below details in the required fields
   - **IdP End Point URL**: Paste here the value we note down from **Issuer:** (step 9, above)
   - **IdP Username Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
   - **IdP Email Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
   - **IdP Given Name Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
   - **IdP Surname Parameter**: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

- **IdP Metadata**: Open the metadata file we have downloaded using notepad and copy paste value here.



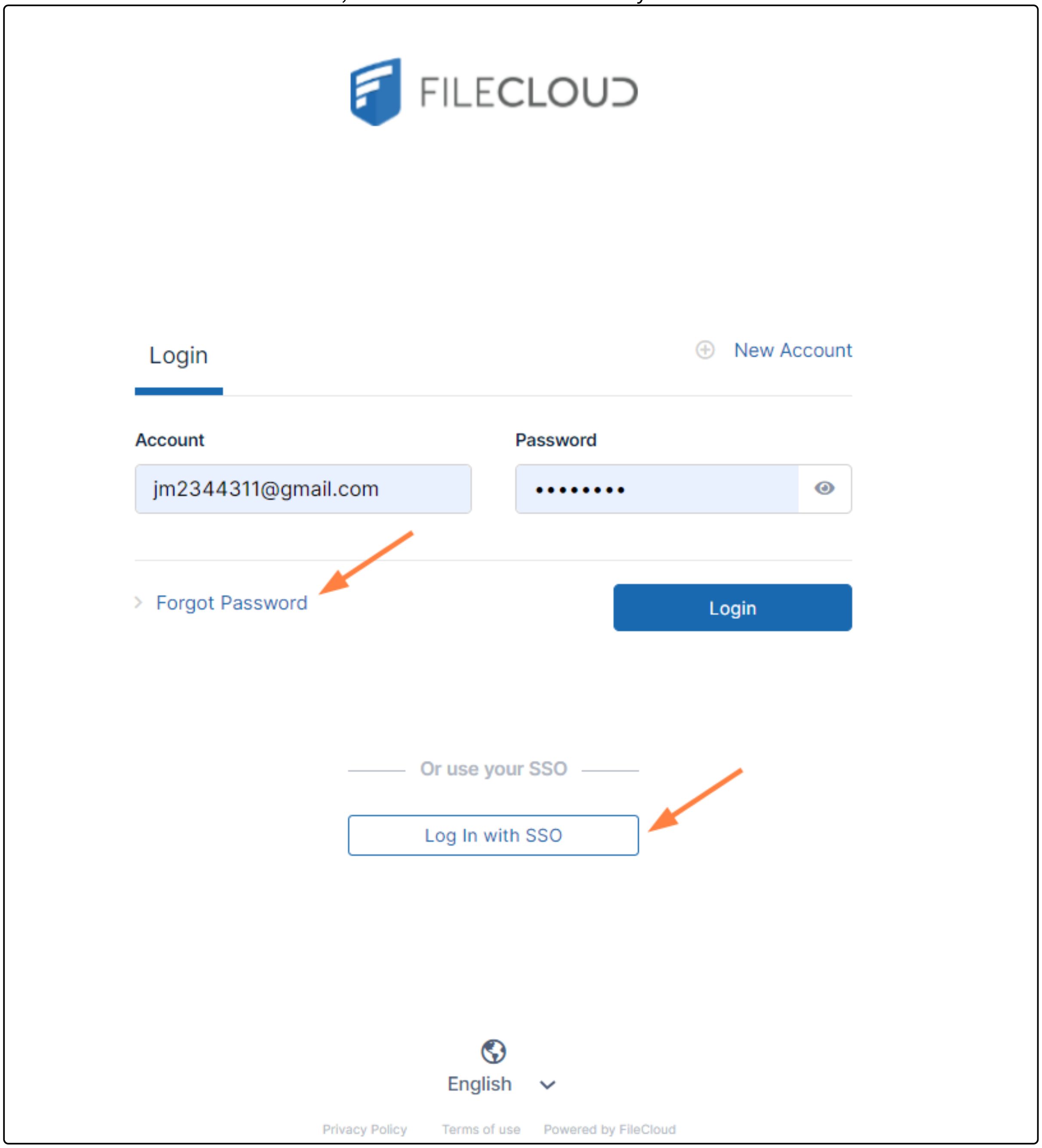
3. For help filling the remaining files on the page, see SAML Single Sign-On Support.
4. Click **Save**.

5. Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.



6. In the FileCloud user portal login page, click on the more option and access SSO. This will first redirect you to the Auth0 login page where you can authenticate as the user that you have created in Auth0.

If that user doesn't exist in FileCloud, it will be created automatically after successful authentication.



Integrate Microsoft Entra ID with FileCloud

Azure Active Directory is now Microsoft Entra ID.

Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

Note: Microsoft Entra ID can only be integrated if FileCloud has an SSL certificate in place, as Microsoft requires HTTPS URLs when configuring FileCloud in Entra ID.

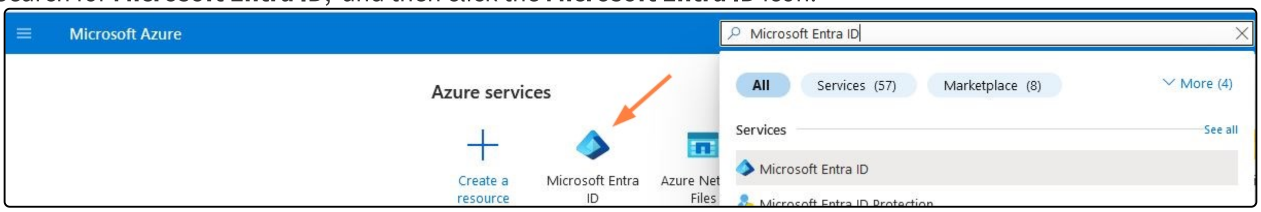
FileCloud can be integrated with Microsoft Entra ID.

- Microsoft Entra ID must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

To integrate Microsoft Entra ID with FileCloud:

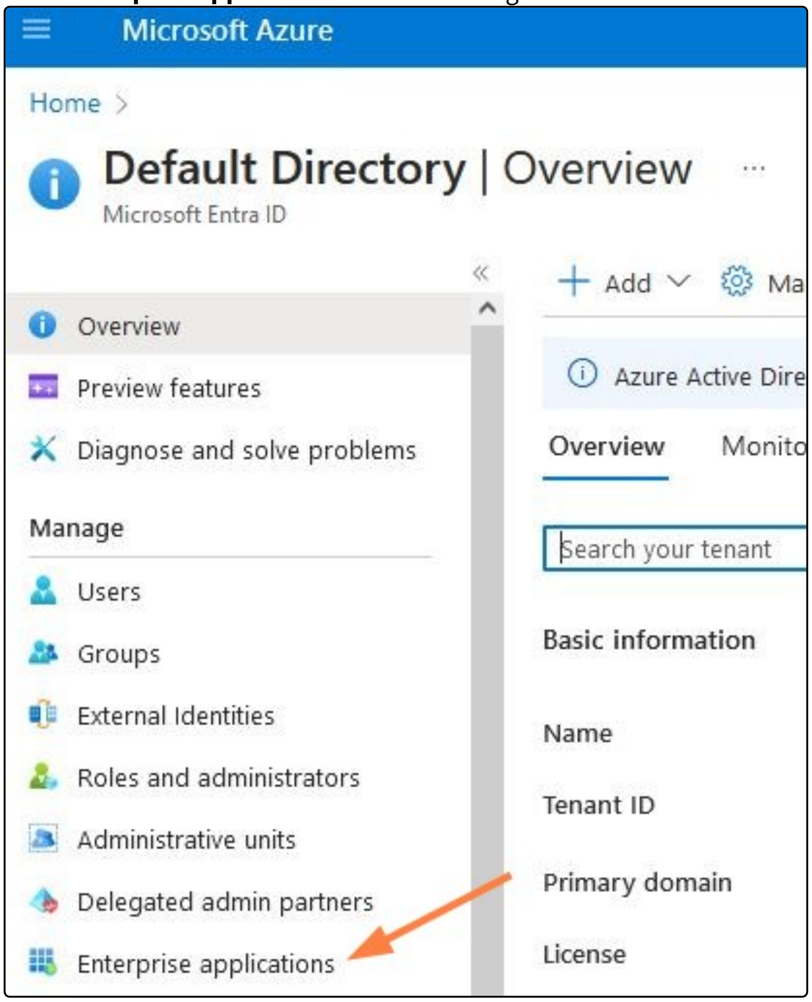
Log in to the Azure Portal (https://portal.azure.com).

1. Search for **Microsoft Entra ID**, and then click the **Microsoft Entra ID** icon.

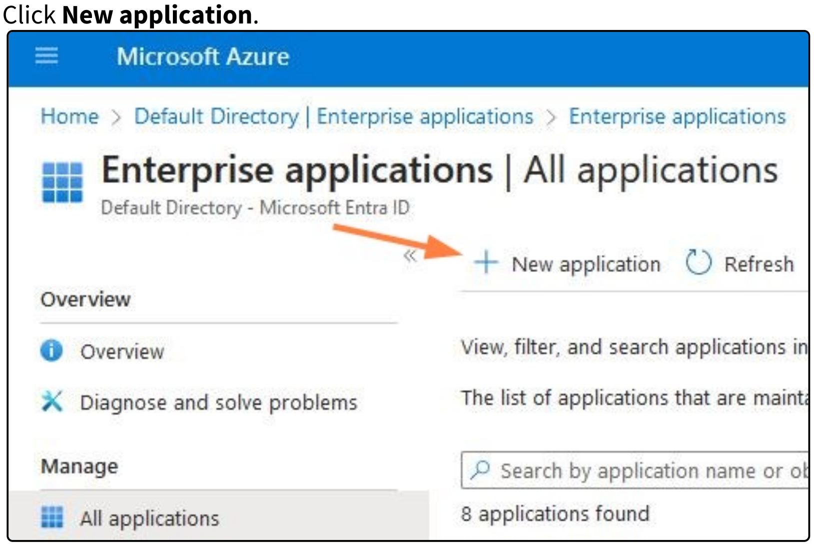


2. If you see a directory list, select the directory you want to integrate with FileCloud.

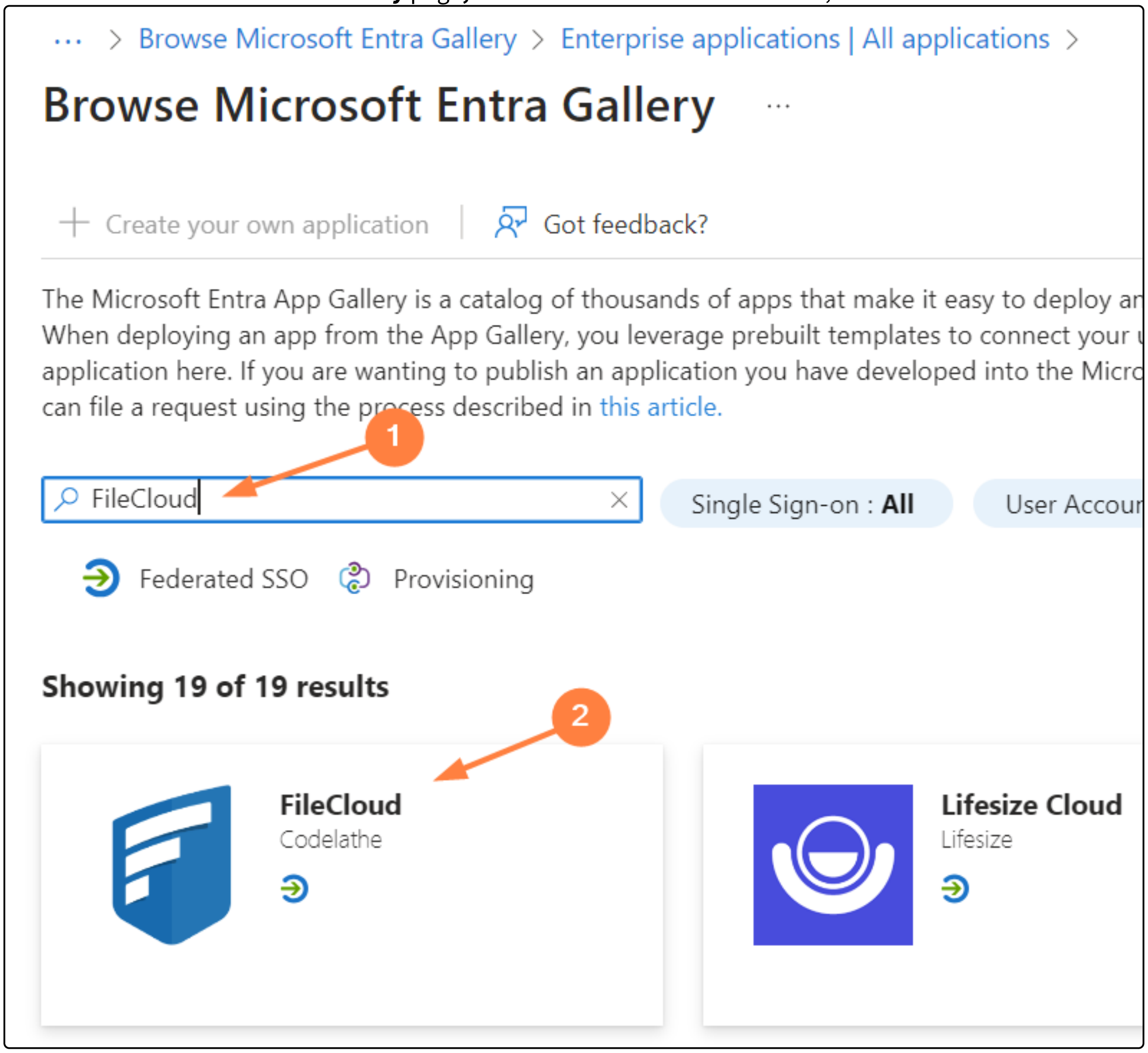
3. Select **Enterprise applications** in the left navigation menu.



4. Click **New application**.

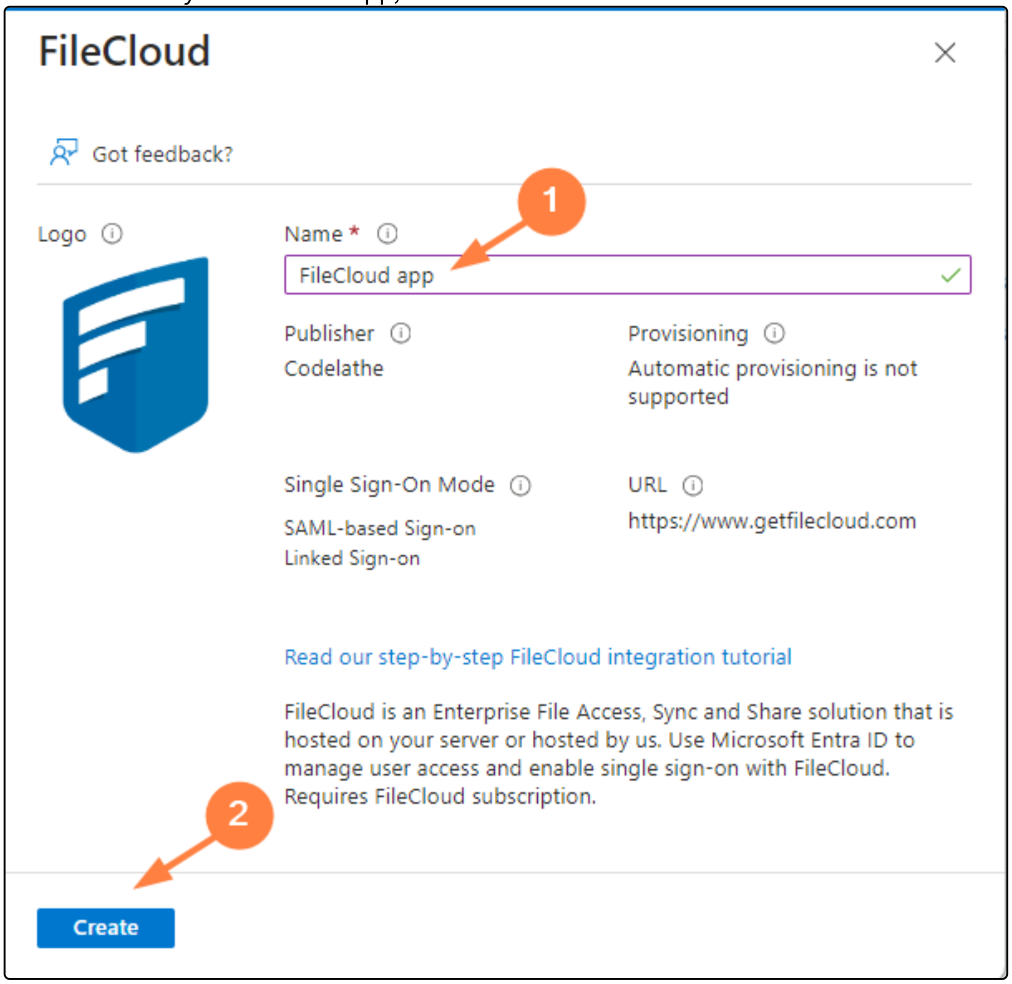


5. In the **Browse Microsoft Entra Gallery** page**,** enter **FileCloud** in the search box, and click the FileCloud icon.



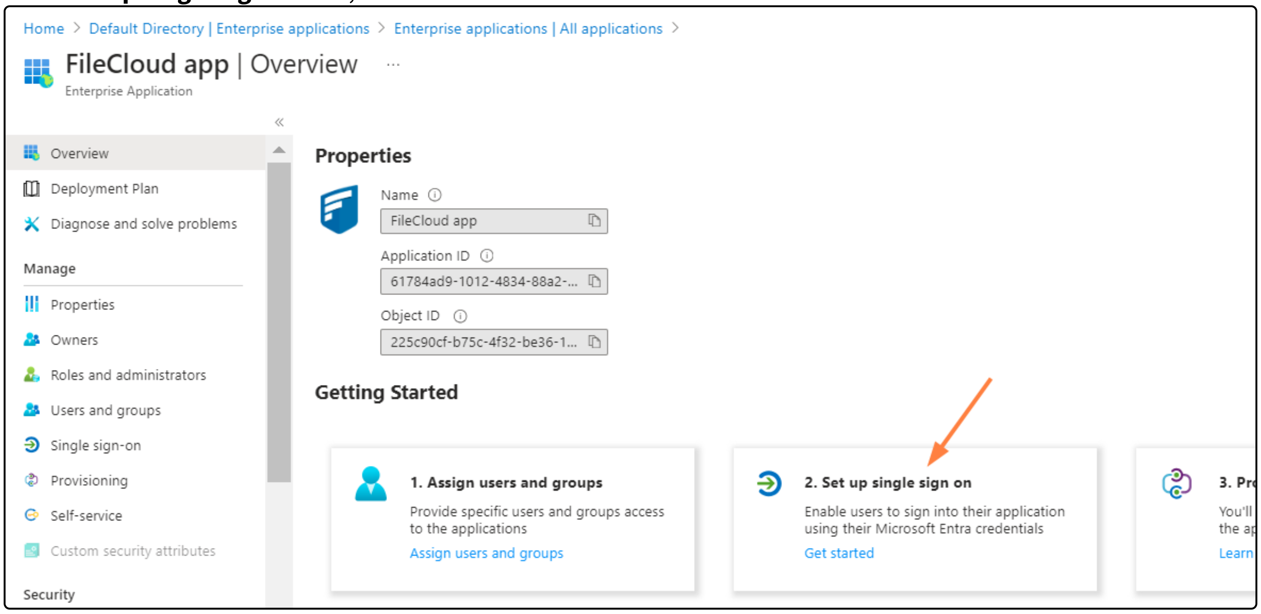
FileCloud information appears in the right panel.

6. Enter a name for your FileCloud app, and click **Create**.



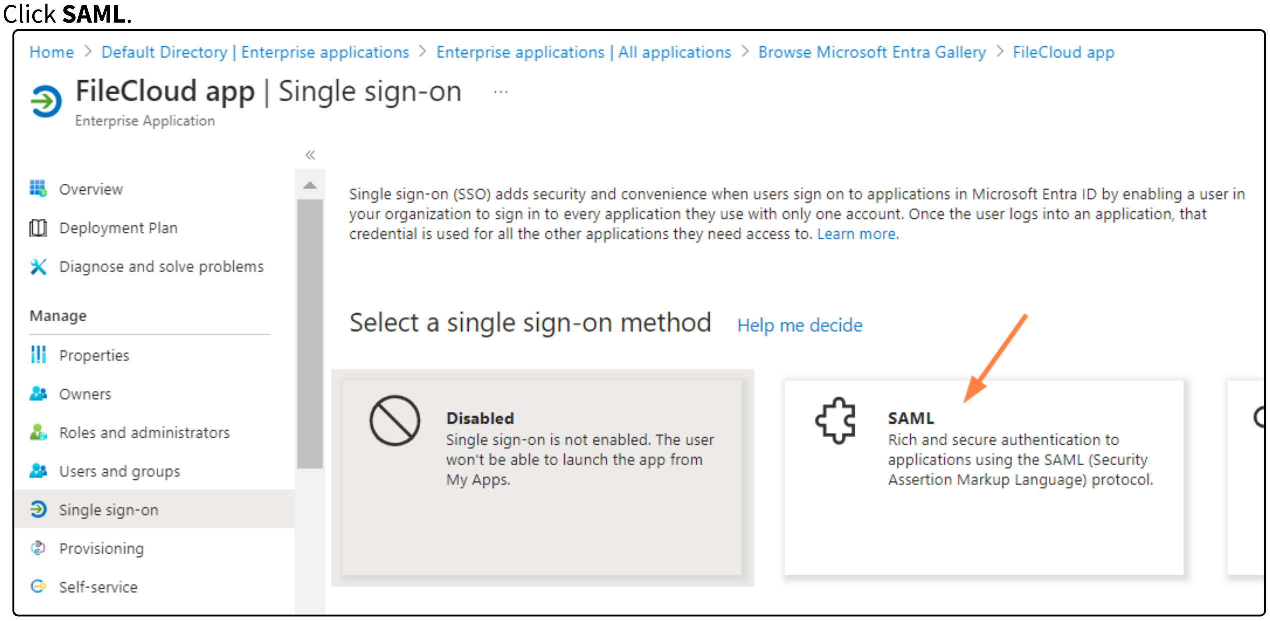
The **Overview** page for the new application opens.

7. In the **Set up single sign on** box, click **Get started**.



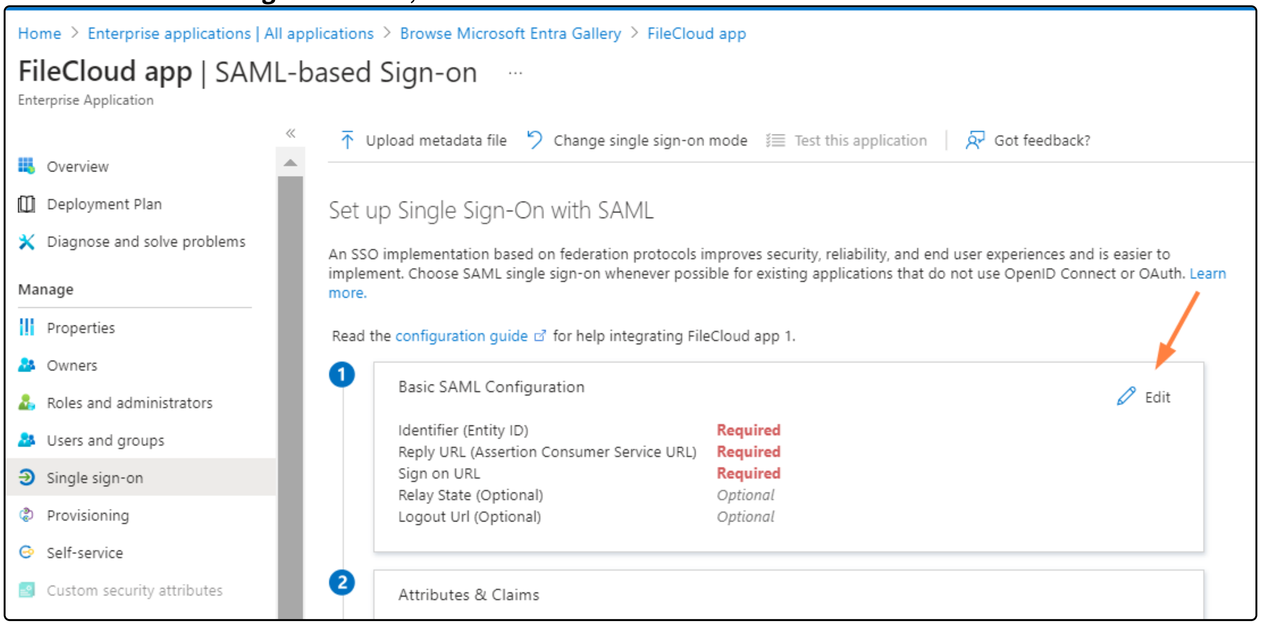
The **Single sign-on** screen opens.

8. Click **SAML**.

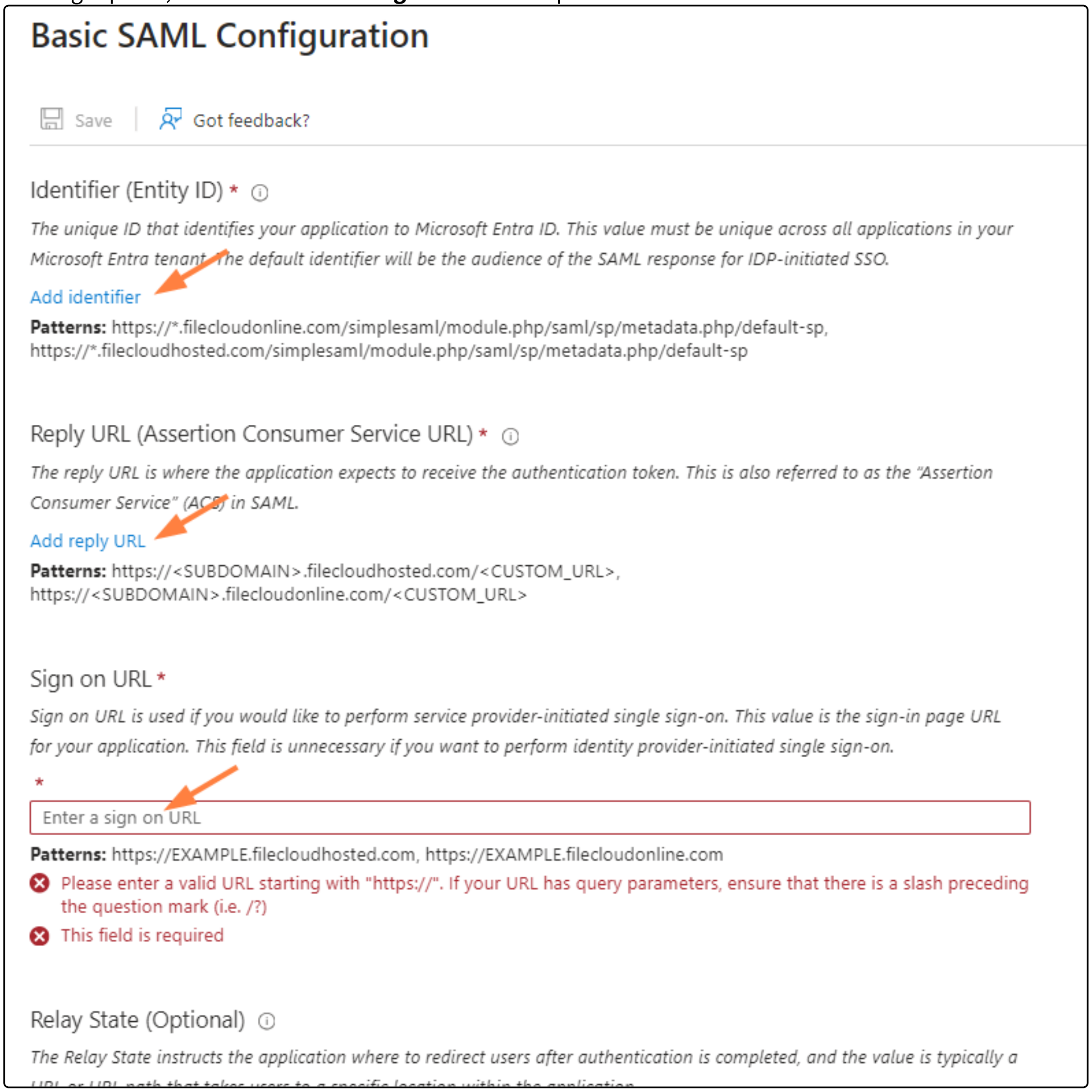


The **SAML-based Sign-on** screen opens.

9. In the **Basic SAML Configuration** box, click **Edit**.

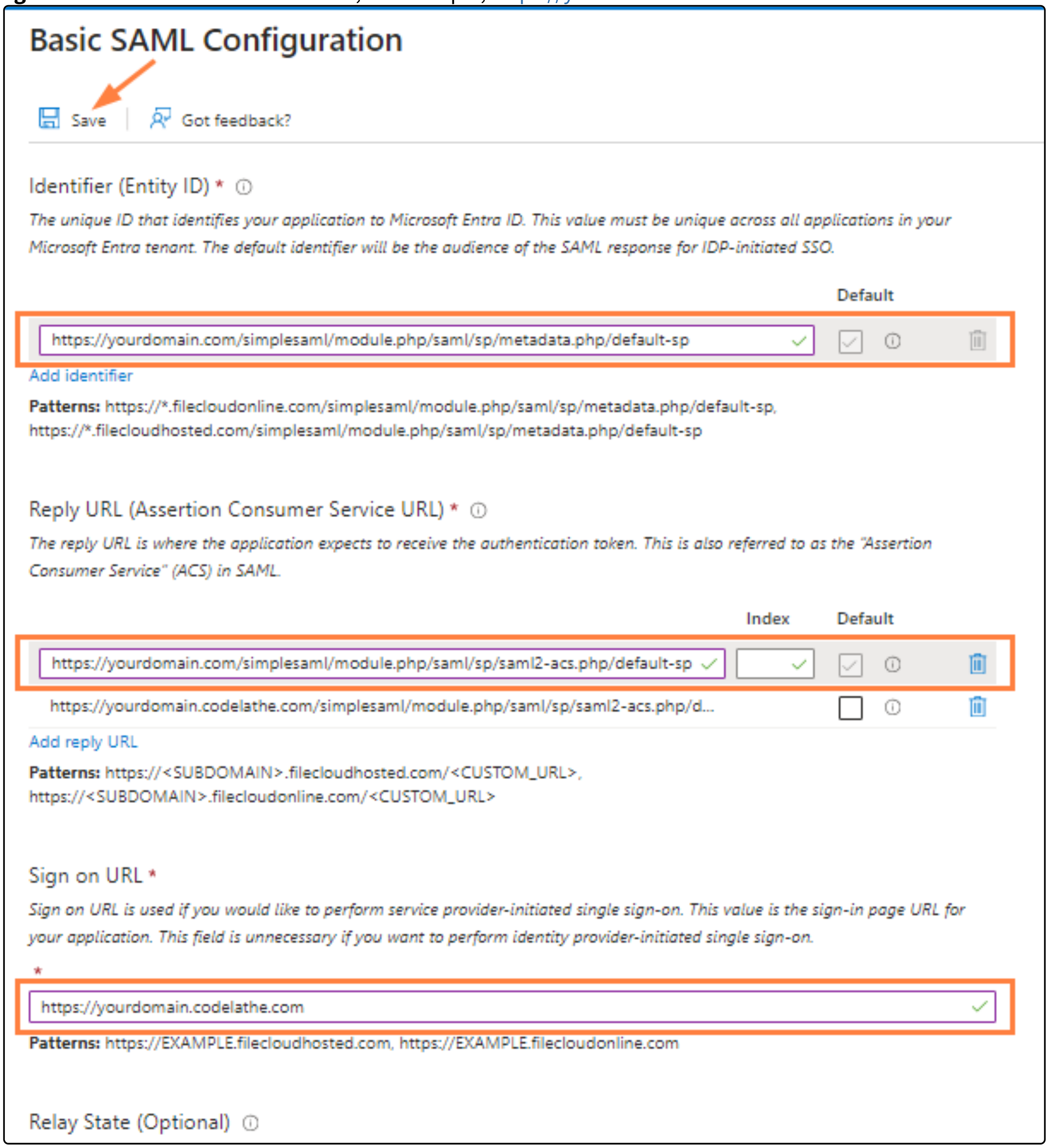


In the right panel, the **Basic SAML Configuration** form opens.



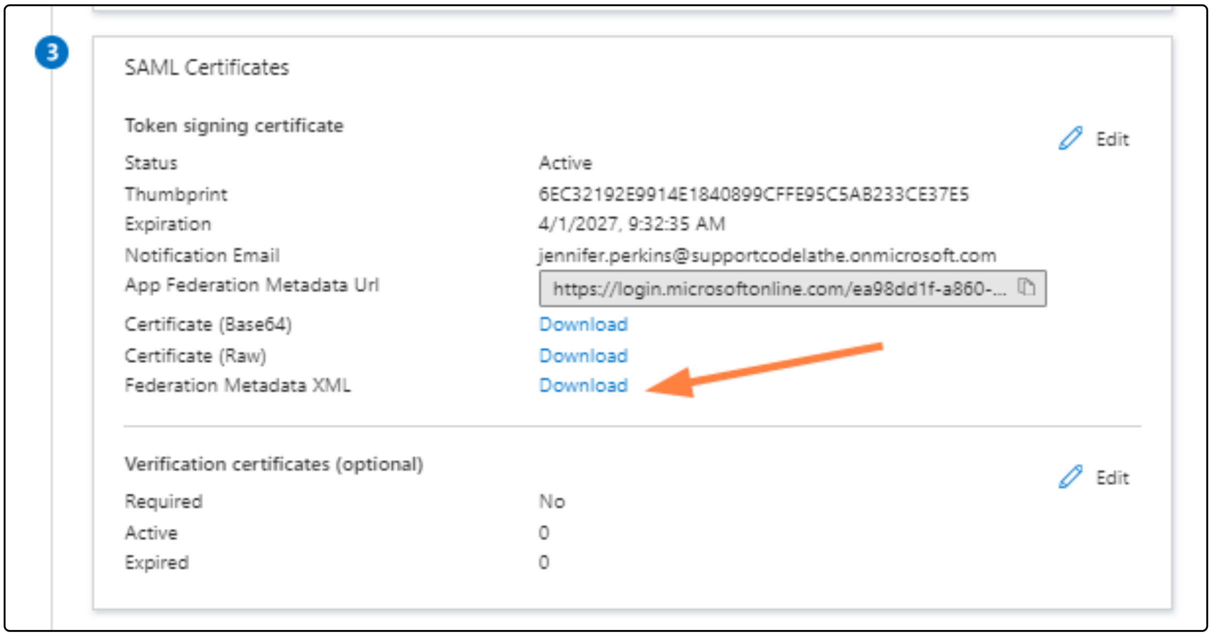
10. Enter the top three fields, **Identifier (Entity ID)**, **Reply URL**, and **Sign on URL** using your FileCloud domain, then click **Save**.
Identifier (Entity ID) - the FileCloud SSO endpoint, for example, https://yourdomain.com/simplesaml/module.php/saml/sp/metadata.php/default-sp
Reply URL - your FileCloud domain with the additional path indicated, https://yourdomain.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Sign on URL - Your FileCloud site URL, for example, https://yourdomain.com

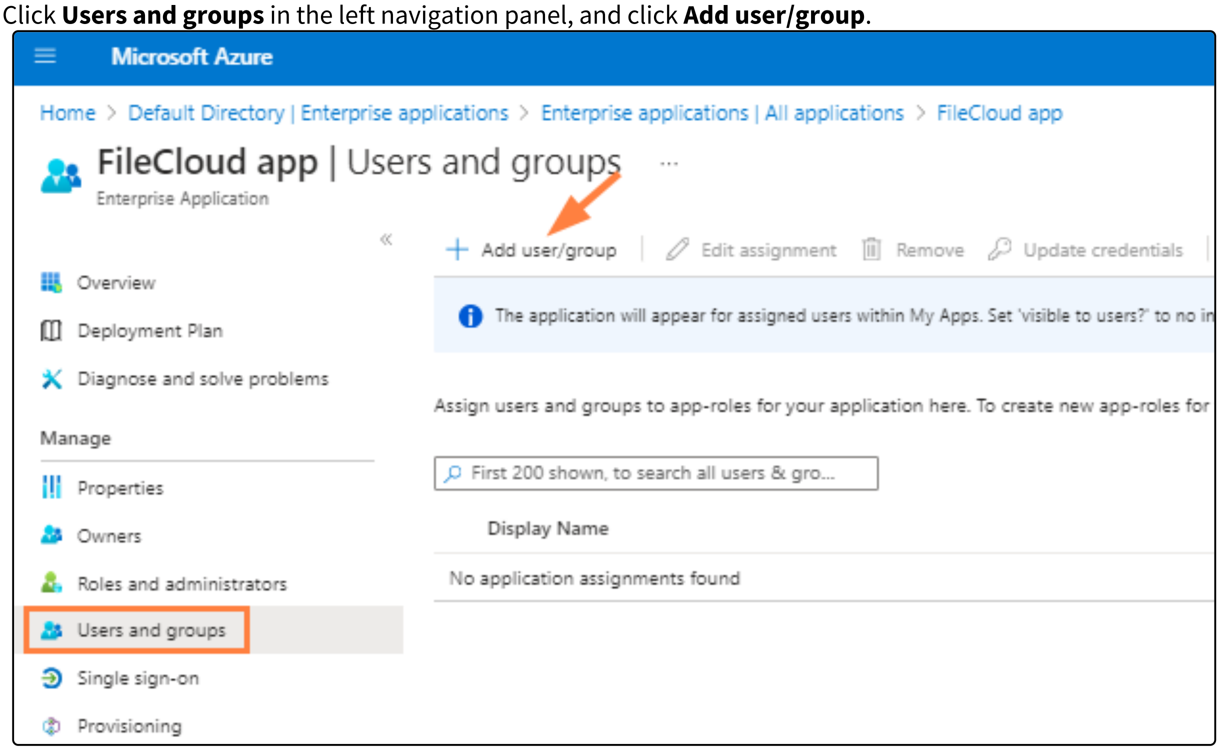


11. Close the panel and scroll down to the **SAML Certificates** box.

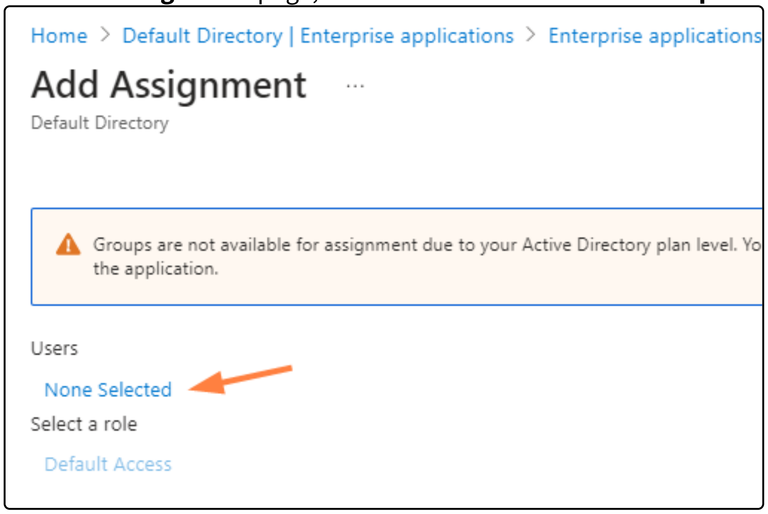
12. Download and save the **Federation Metadata XML**.



13. Click **Users and groups** in the left navigation panel, and click **Add user/group**.

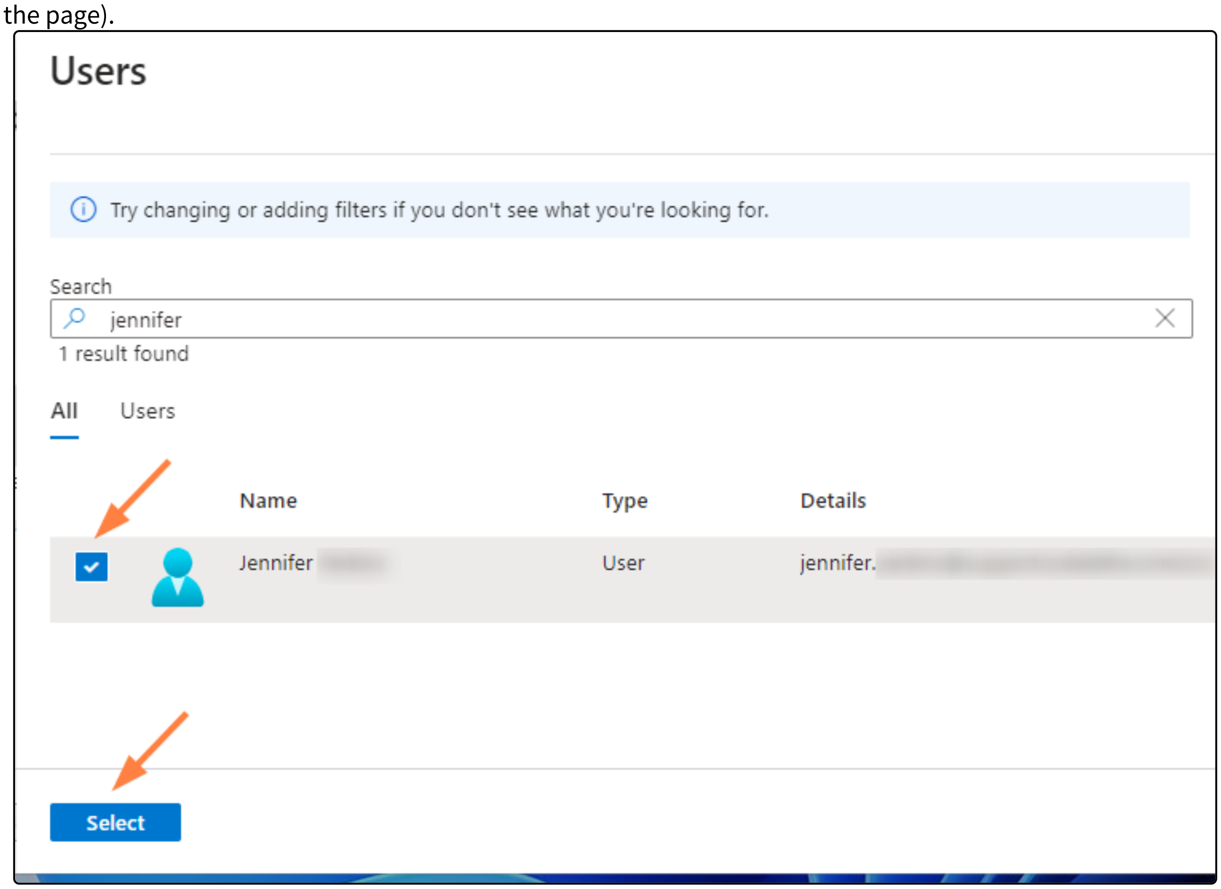


14. In the **Add Assignment** page, click the link under **Users** or **Groups** to add users and groups.

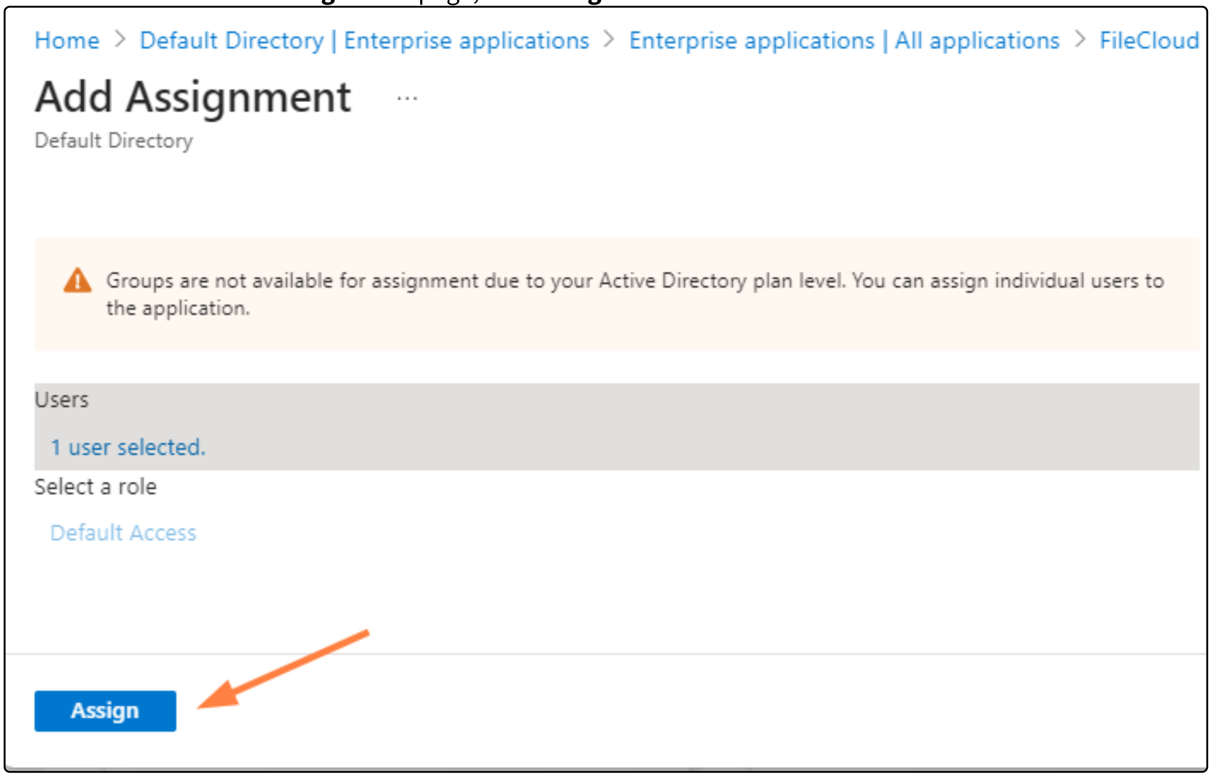


The **Users** or **Groups** page opens.

15. Search for and check the users or groups that you want to assign to the app, and choose **Select** (at the bottom of the page).



16. At the bottom of the **Add Assignment** page, click **Assign**.

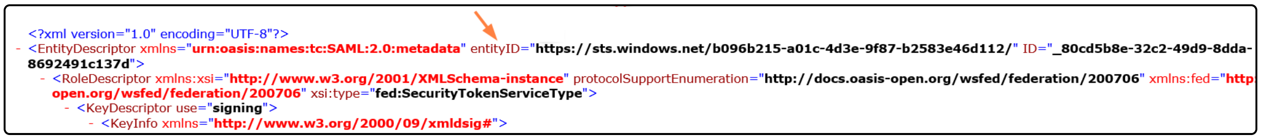


17. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
    The **SSO** settings page opens.
18. In the **Default SSO Type** drop-down list, choose **SAML**.
19. Enter the following details:

Settings	Value
Default SSO type	SAML
IdP endpoint URL or entity ID	From the metadata XML downloaded, copy the entity ID on the first line of the XML document.
IdP username parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
IdP email parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
IdP given name (first name) parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
IdP surname (last name) parameter	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Settings	Value
IdP Metadata	Copy the complete contents of the metadata XML downloaded.

To get the **IdP endpoint URL**, open your downloaded xml data and copy the **entityID** as shown in the screen shot below.



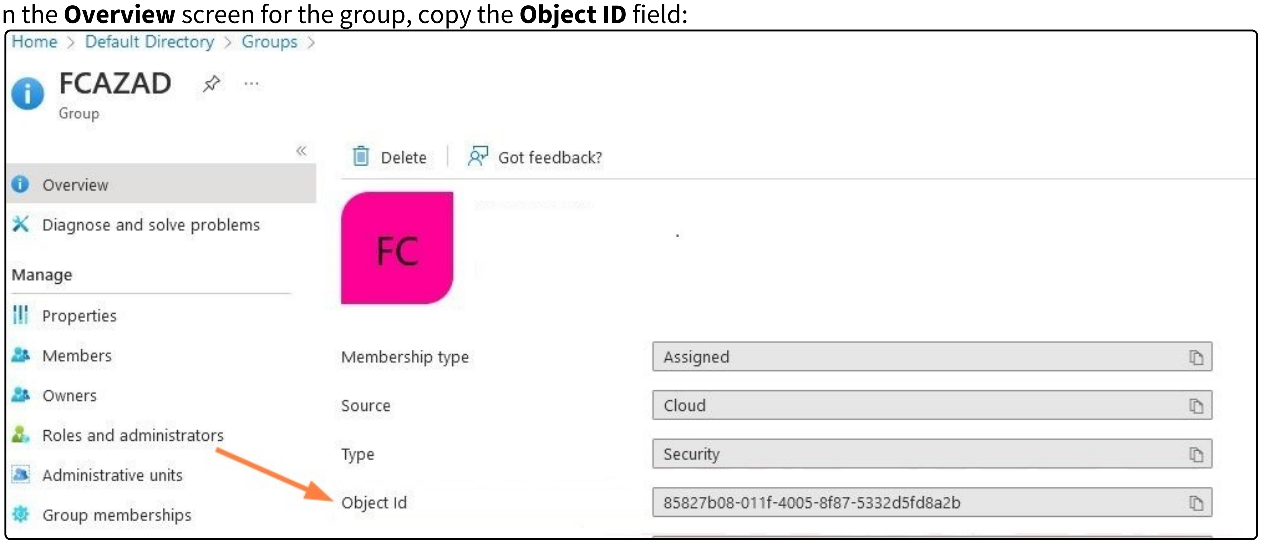
20. Save the above settings.
    This completes the Microsoft Entra ID SSO integration with FileCloud.

Troubleshooting failed SSO login for a member of an IdP group

An IdP group is a group of users in Microsoft Entra ID who are authorized to log in to FileCloud. When a user logs in to FileCloud with SSO using Entra ID, FileCloud automatically checks the login user's FileCloud group name to see if it is the same as the user's IdP group name. However, this fails because Entra ID can only send the **Group ID**, not the group name, to FileCloud. To fix this, add a custom claim parameter named **memberof** in Entra ID to send the group's **Object ID** (**Group ID**) to be compared with the field **Limit log in to IdP group** in FileCloud SSO settings. Since the two values are identical, the user is able to log in to FileCloud.

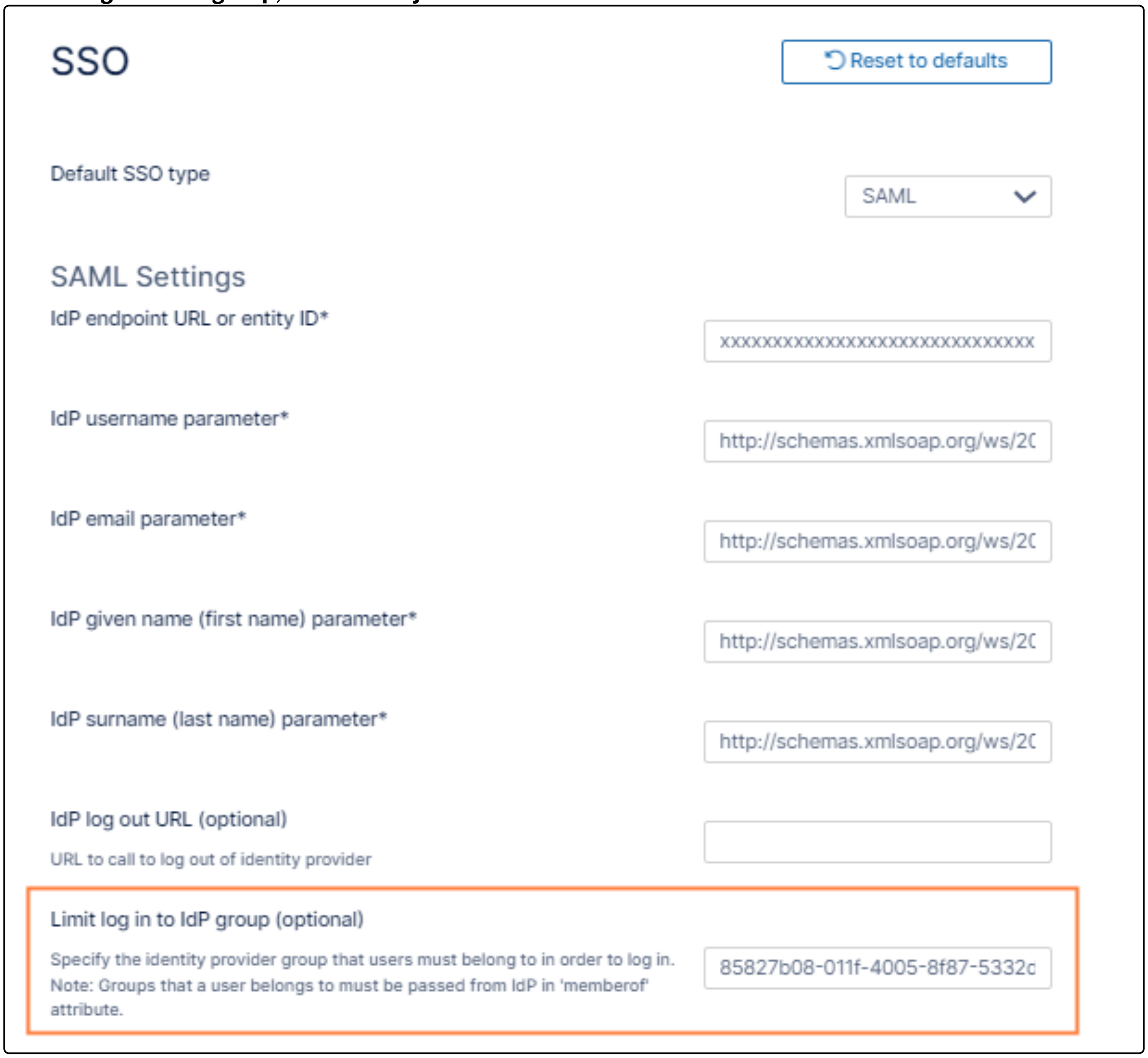
To get the group's **Object ID**, in Microsoft Entra ID:

1. Log in the the Azure portal, and in the navigation panel, click **Microsoft Entra ID**.
2. In the navigation panel, click **Groups**, and then click the **Group** to limit the login to.
3. In the **Overview** screen for the group, copy the **Object ID** field:



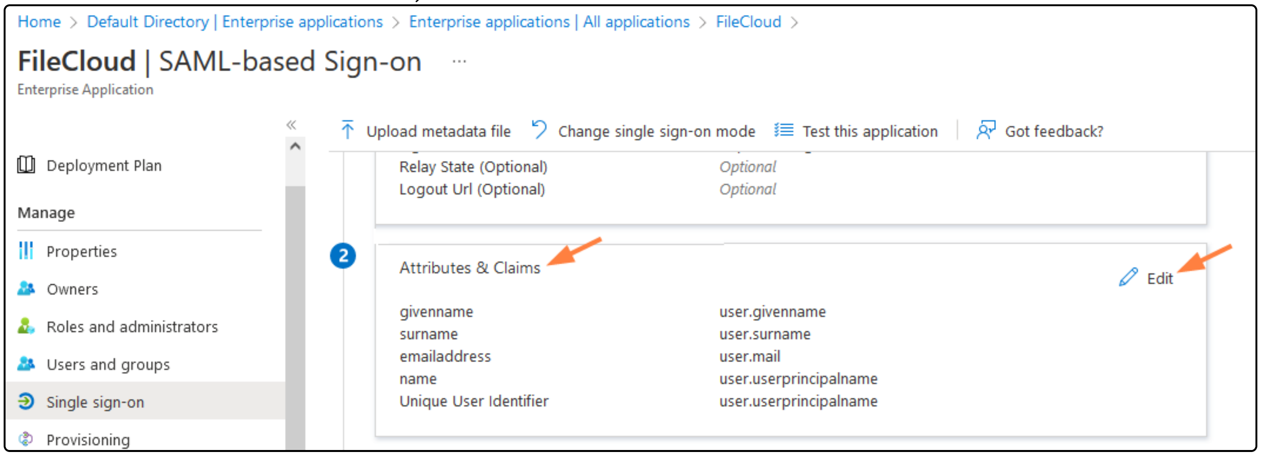
4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .

5. In **Limit log in to IdP group**, enter the **Object Id.**

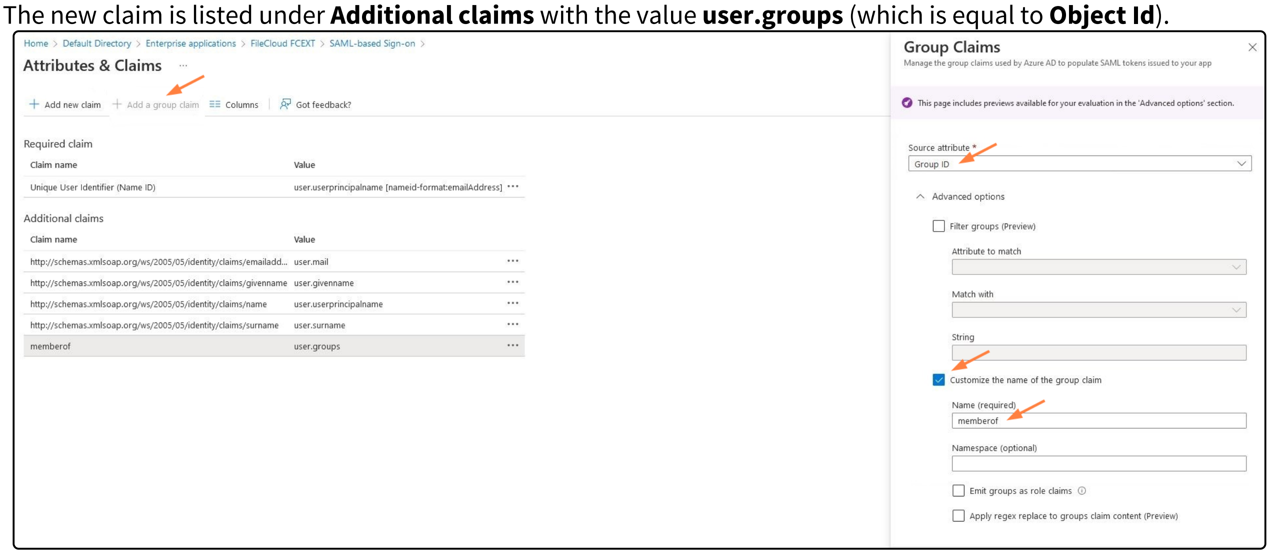


6. In Microsoft Entra ID, go to the **Enterprise Applications** screen, and choose the FileCloud application
7. In the navigation panel, click **Single sign-on**.

8. Scroll down to **Attributes and Claims**, and click **Edit**.



9. Click **Add a group claim.**
   A **Group Claims** form opens in the right panel.
10. In **Source attribute**, choose **Group ID**.
11. Check **Customize the name of the group claim**.
12. In **Name**, enter **memberof.**
13. Click **Save**.
    The new claim is listed under **Additional claims** with the value **user.groups** (which is equal to **Object Id**).



Now **memberof** will be sent to FileCloud with the value of the user group, and when FileCloud compares it with the **Idp Group**, the values match, so FileCloud will allow the login.

Integrate Centrify with FileCloud

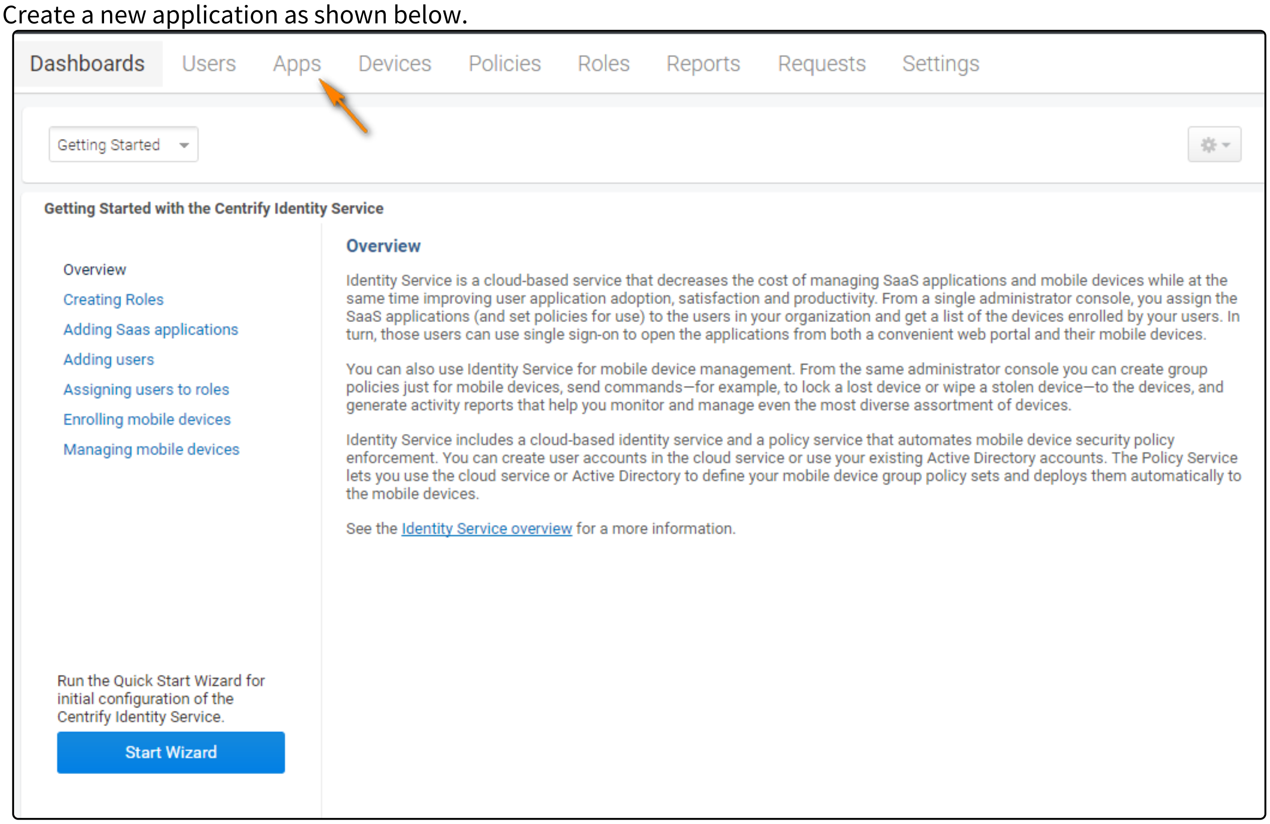
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

FileCloud can be integrated with Centrify. Centrify must be configured as an Identity Provider (IdP), and FileCloud will act as the Service Provider (SP).

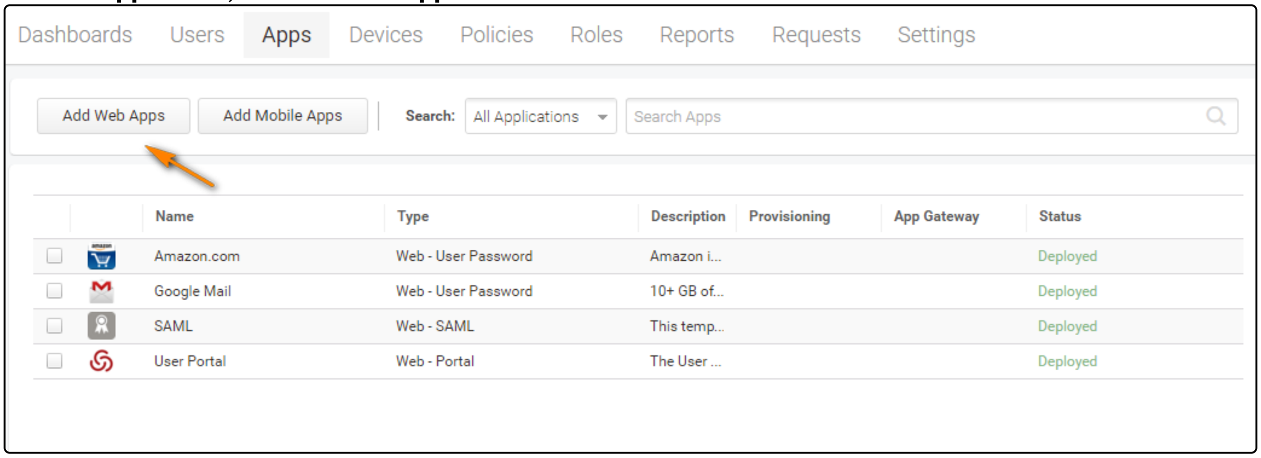
To configure FileCloud with Centrify:

PLEASE NOTE: Any reference to samldev.codelathe.com in this article should be replaced with your own FileCloud URL.

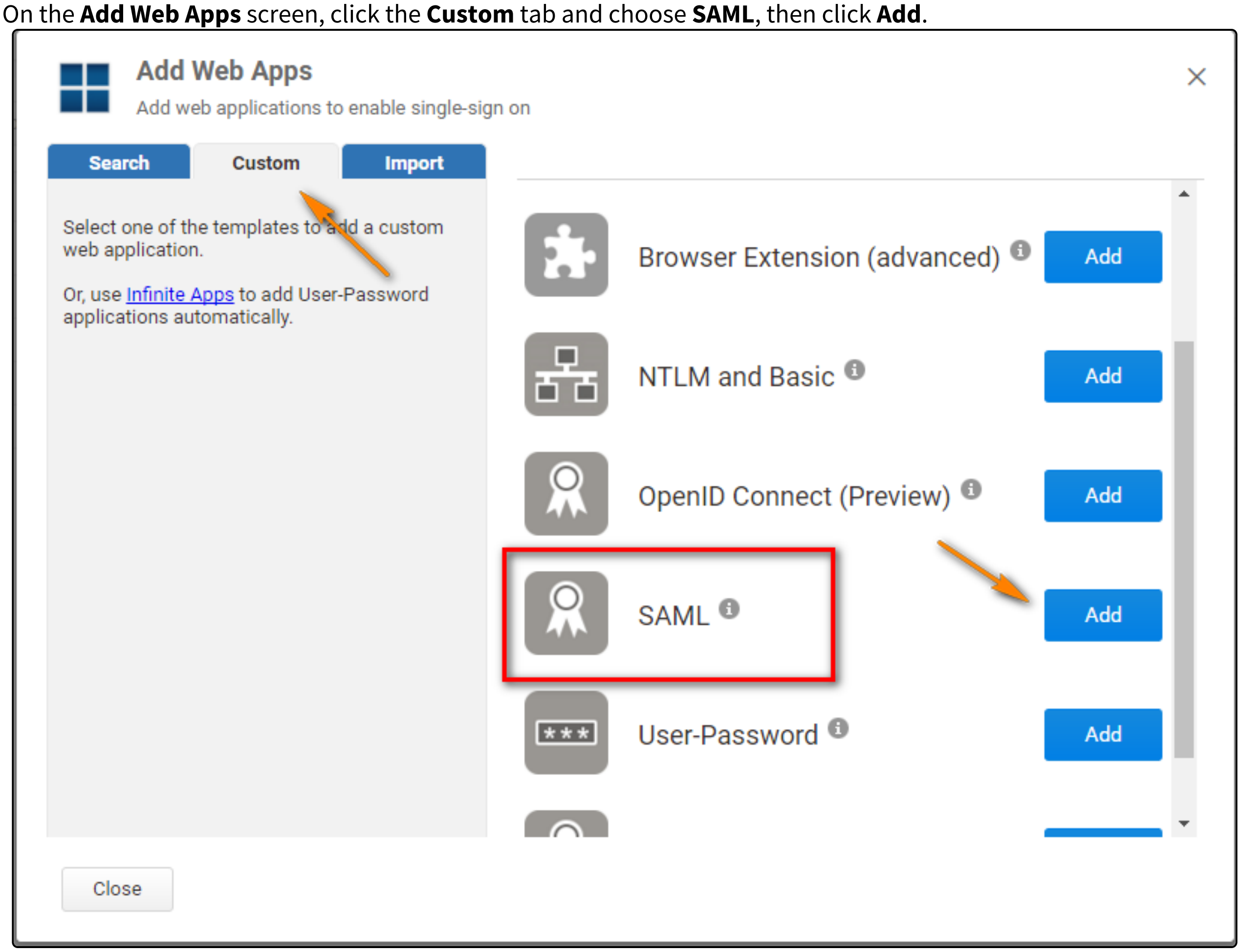
1. Log in to your Centrify issued URL.
2. After successful login to Centrify, go to the admin section and to the dashboard.
3. Create a new application as shown below.



4. From the **Apps** menu, click **Add Web Apps**.

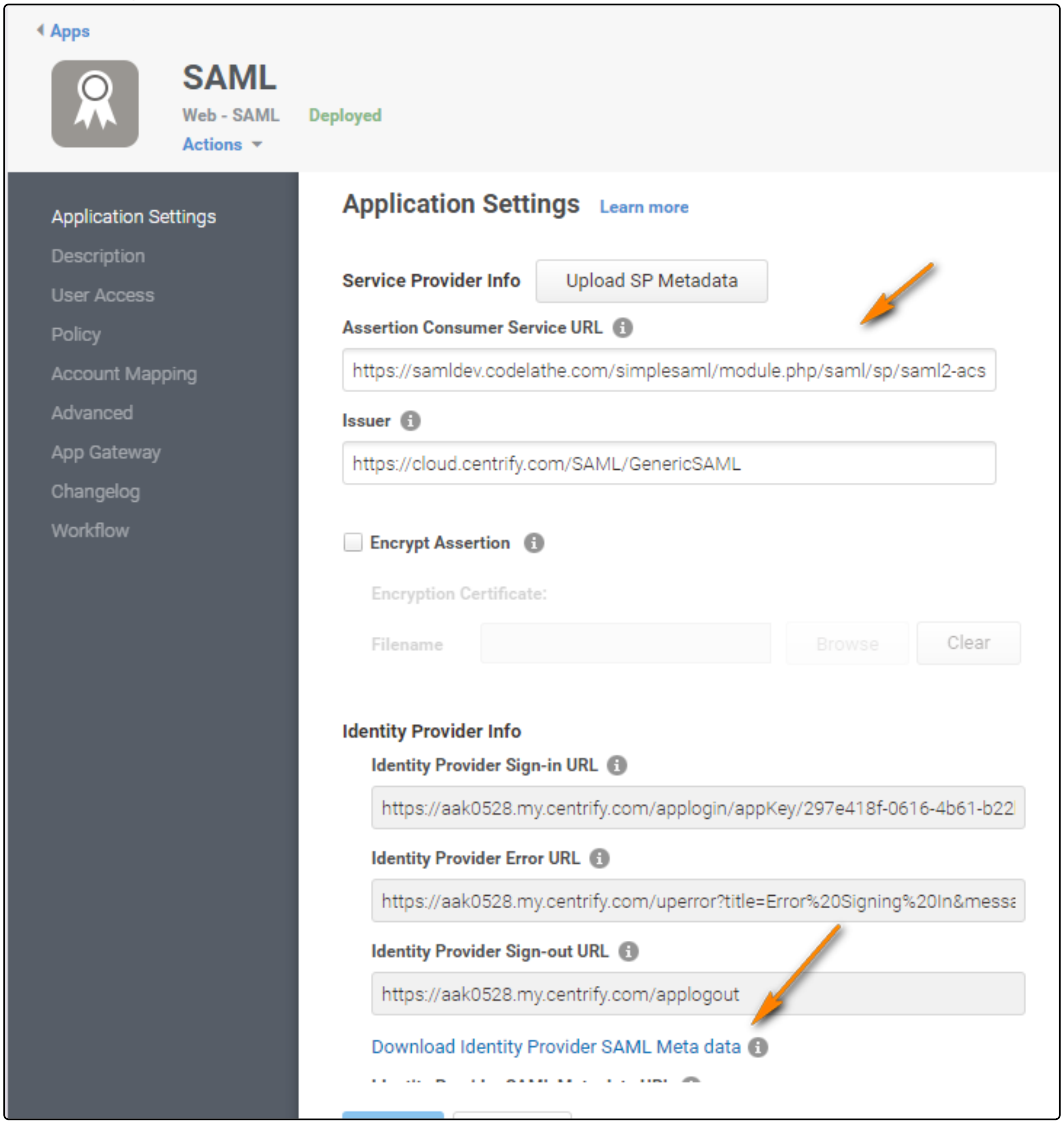


5. On the **Add Web Apps** screen, click the **Custom** tab and choose **SAML**, then click **Add**.



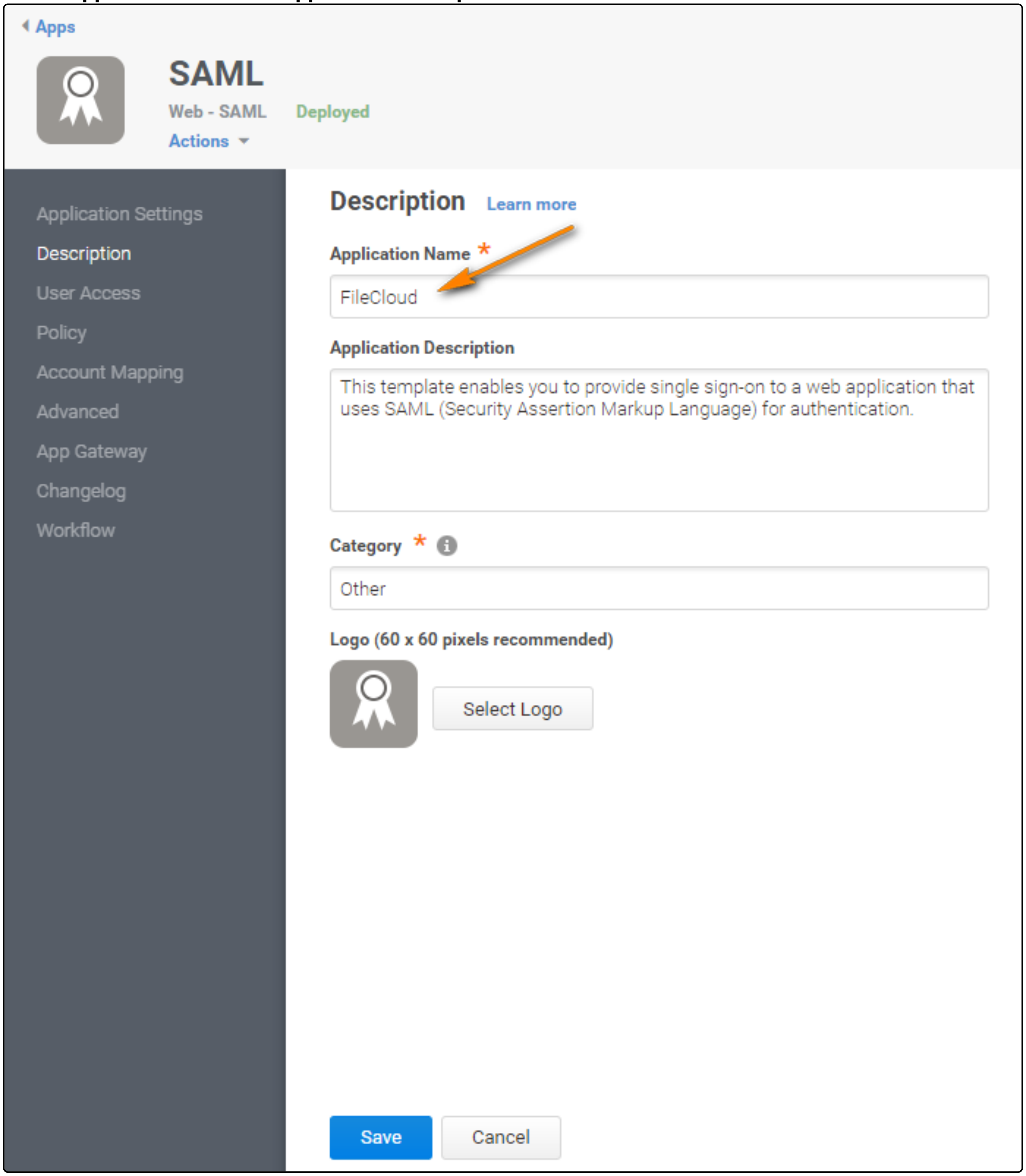
6. In the SAML Web App Screen, click **Application Settings** in the navigation panel.
7. In **Assertion Consumer Service URL** enter the FileCloud assertion URL **http://<your domain>/simplesaml/** module.php/saml/sp/saml2-acs.php/default-sp
8. Download the **Identity Provider SAML Metadata** as shown below. Get the details for configuring FileCloud on this screen in the FileCloud admin portal on the **Settings > SSO** tab.
    a. The Identity Provider Single Sign On URL must match the **Issuer** URL in the screenshot below.

b. The metadata downloaded from this screen must match the **IdP Metadata** in the FileCloud admin portal on the **Settings > SSO** tab.



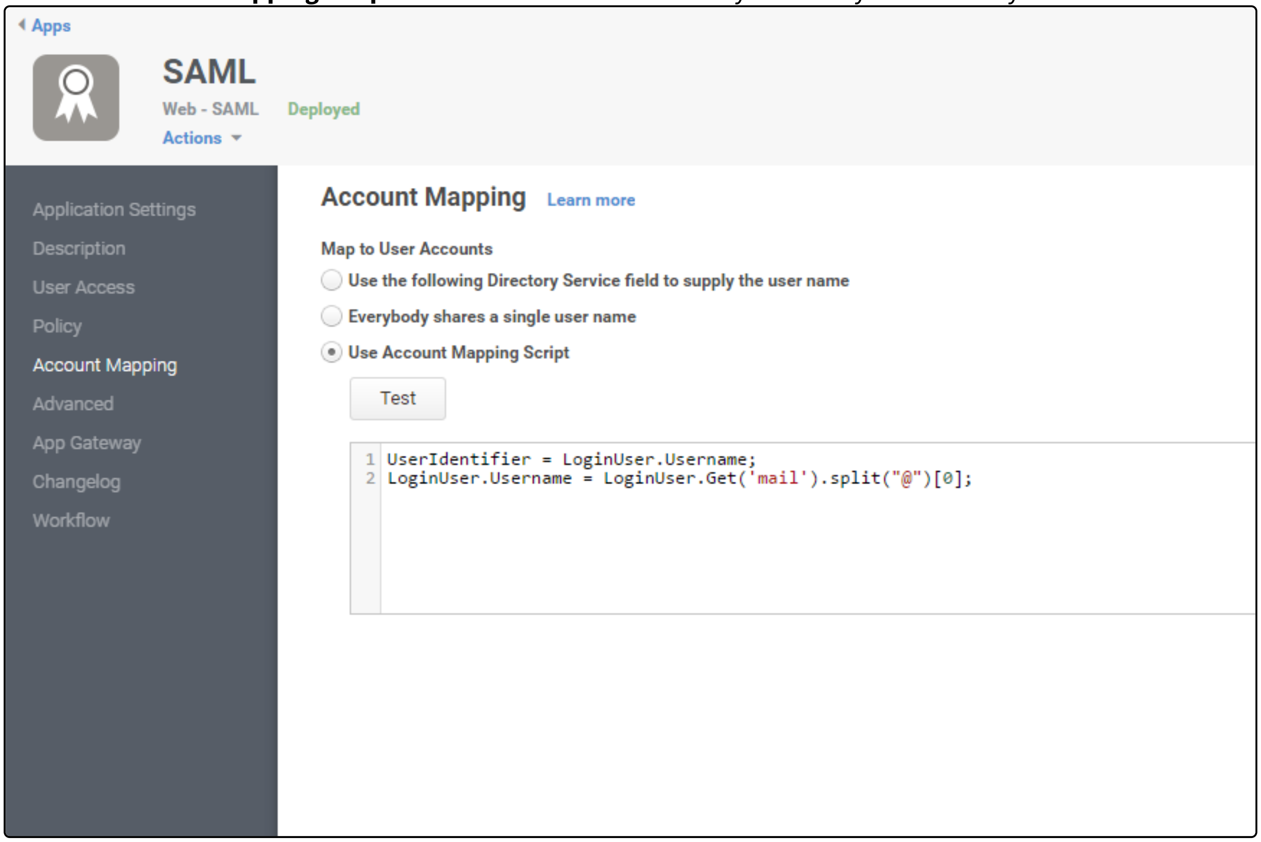
9. In the SAML Web App Screen, click **Description** in the navigation panel.

10. Add the **Application Name** and **Application Description**.

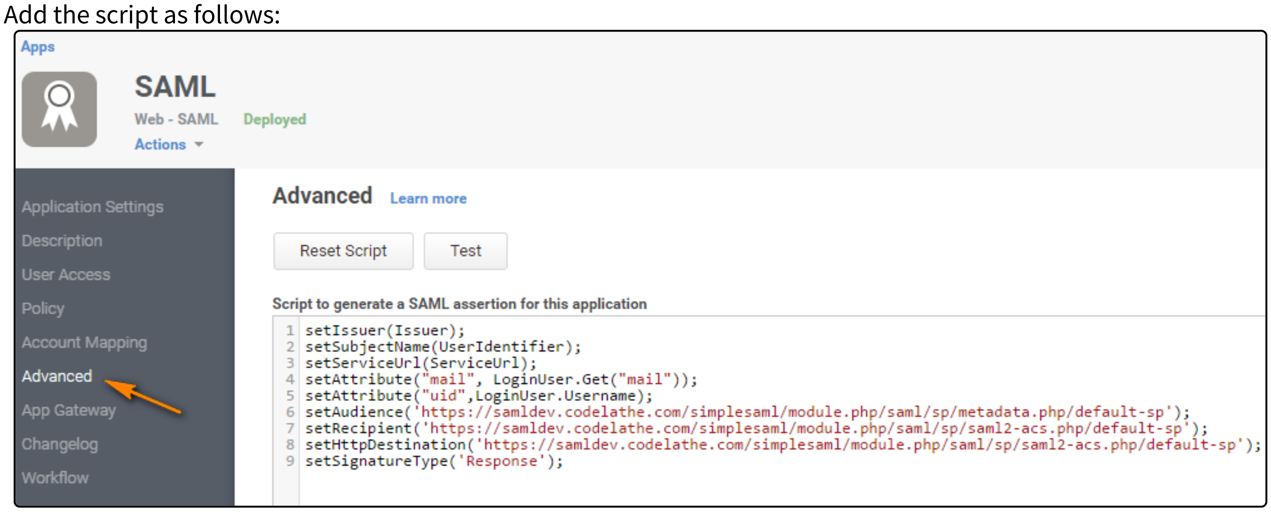


11. In the SAML Web App Screen, click **Account Mapping** in the navigation panel.

12. Select **Use Account Mapping Script** as shown below. This enables you to use your email as your username.

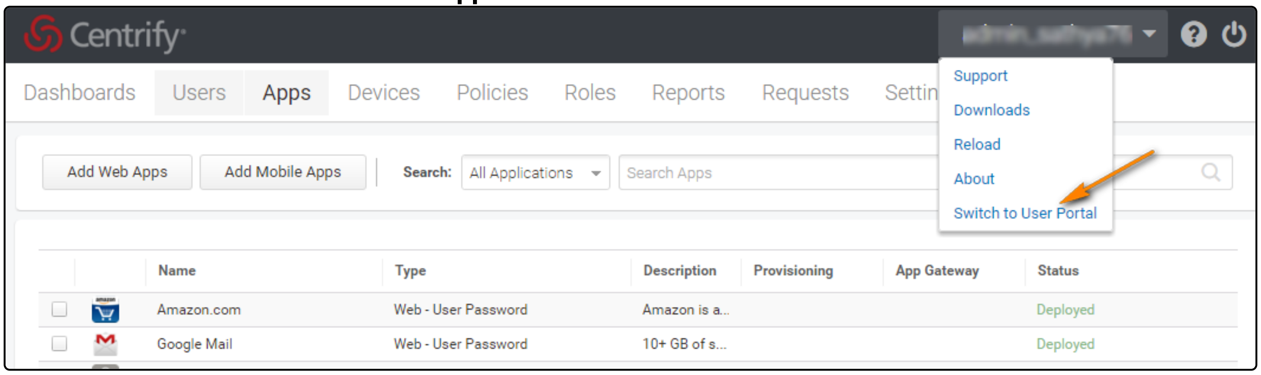


13. In the SAML Web App Screen, click **Advanced** in the navigation panel.
14. Add the script as follows:

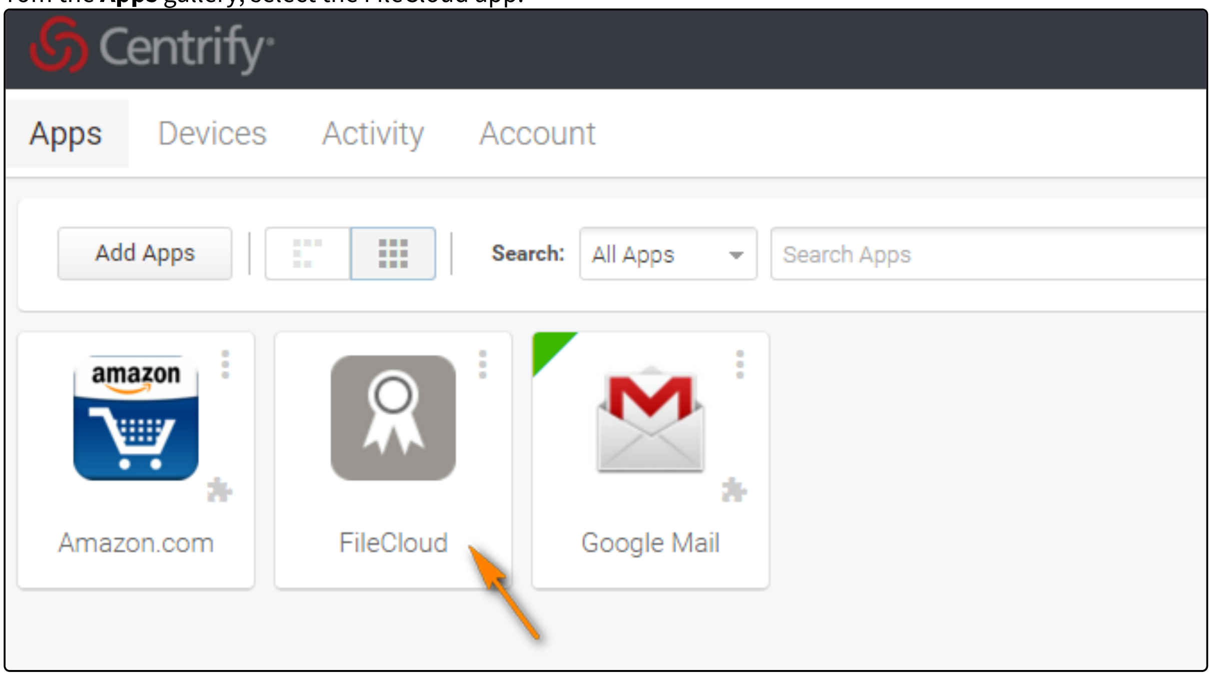


The configuration is now complete.

15. Choose **Switch to User Portal** and click **Apps**.



16. From the **Apps** gallery, select the FileCloud app.



From the FileCloud login screen, you can now select Single Sign-On to log in through Centrify.

Integrate CYBERARK with FileCloud

> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator, you can integrate CYBERARK SSO via SAML into FileCloud. Once integrated your users will be able to access FileCloud with their CYBERARK credentials.

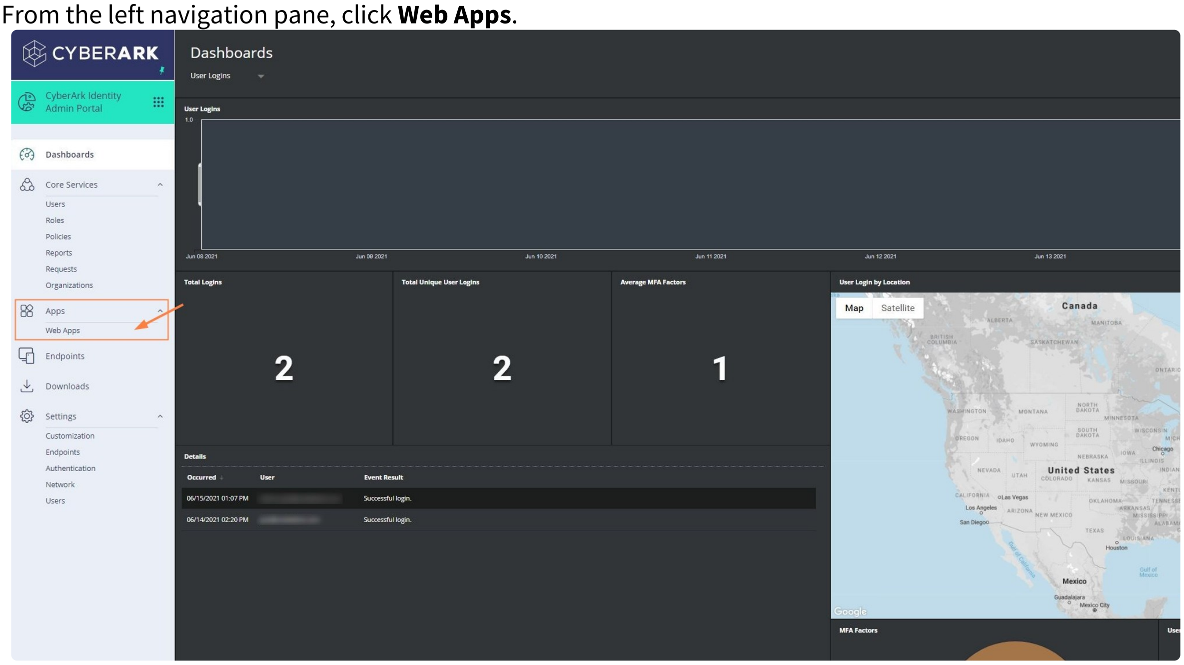
CYBERARK	CYBERARK is a cloud-based platform • Manage privileged accounts and credentials • Secure workforce and customer identities • Secure and manage access for applications and other non-human identities

In this integration scenario:

- CYBERARK must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

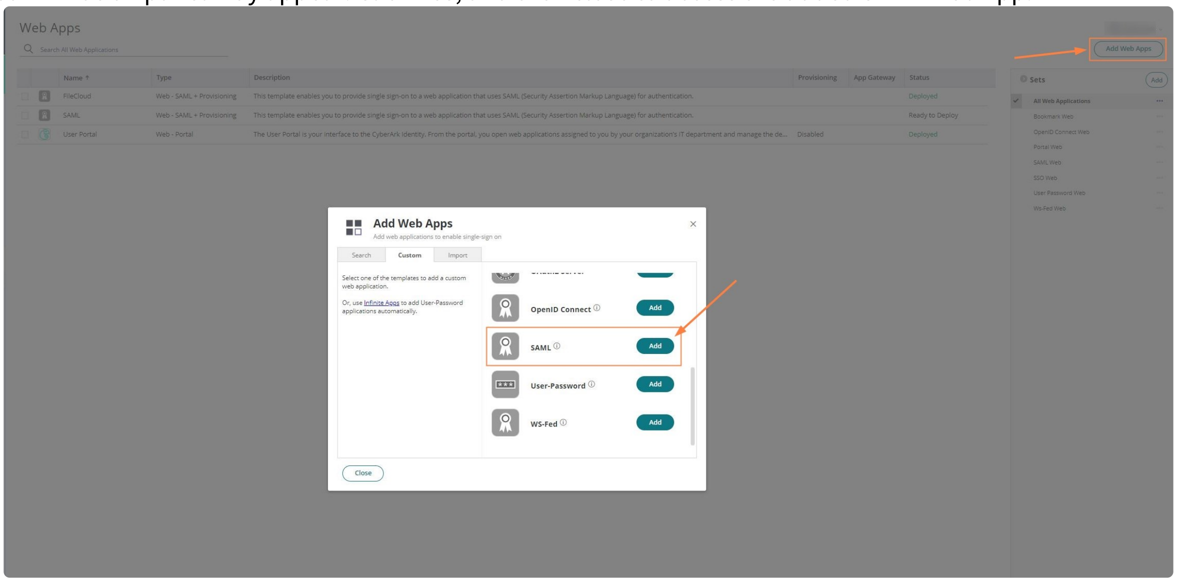
Configure FileCloud with CYBERARK

1. In CYBERARK, create a new web app.
    a. Open a browser and log in to your CYBERARK admin portal.
    b. From the left navigation pane, click **Web Apps**.

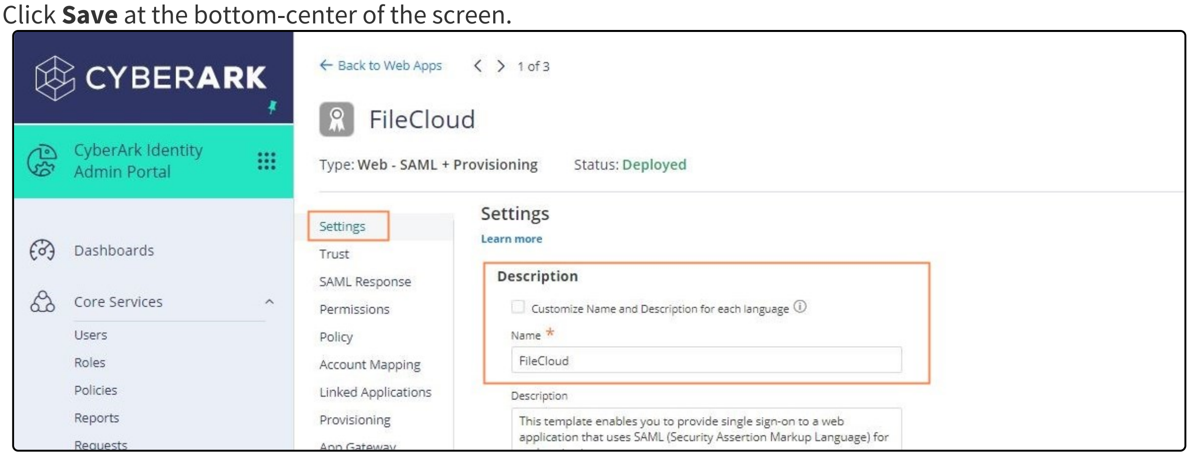


    c. On the Web Apps screen, in the top right corner, click **Add Web Apps**.

d. In the **Add Web Apps** popup, select the **Custom** tab and scroll down until you find **SAML**, and click **Add**. A confirmation panel may appear. Click **Yes**, and then close to access the added SAML Web App.

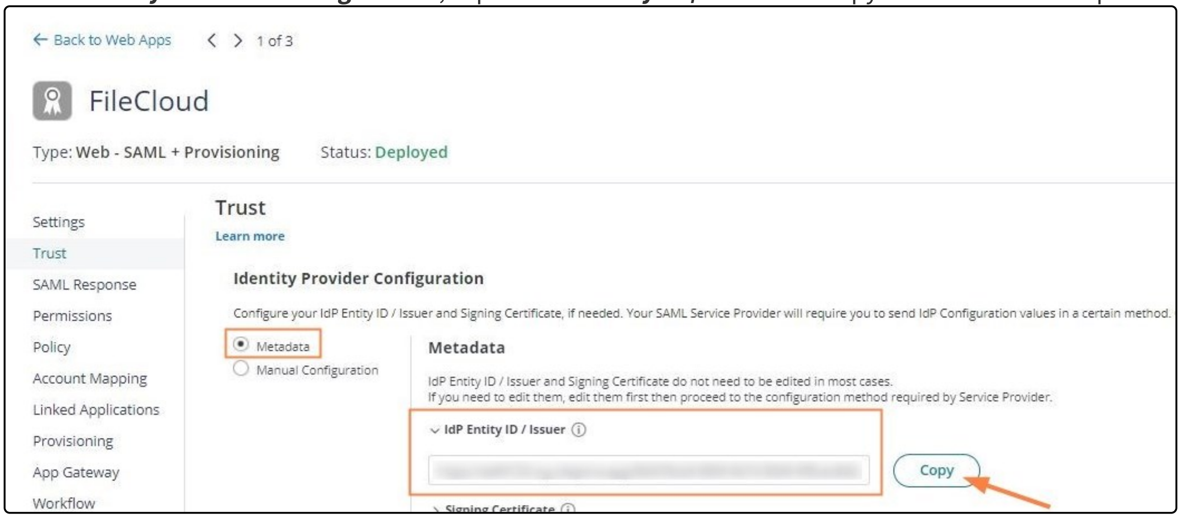


2. In CYBERARK, configure the added SAML Web App.
    a. Click **Settings** in the navigation panel. In **Description**, enter a meaningful name such as FileCloud SSO. Click **Save** at the bottom-center of the screen.

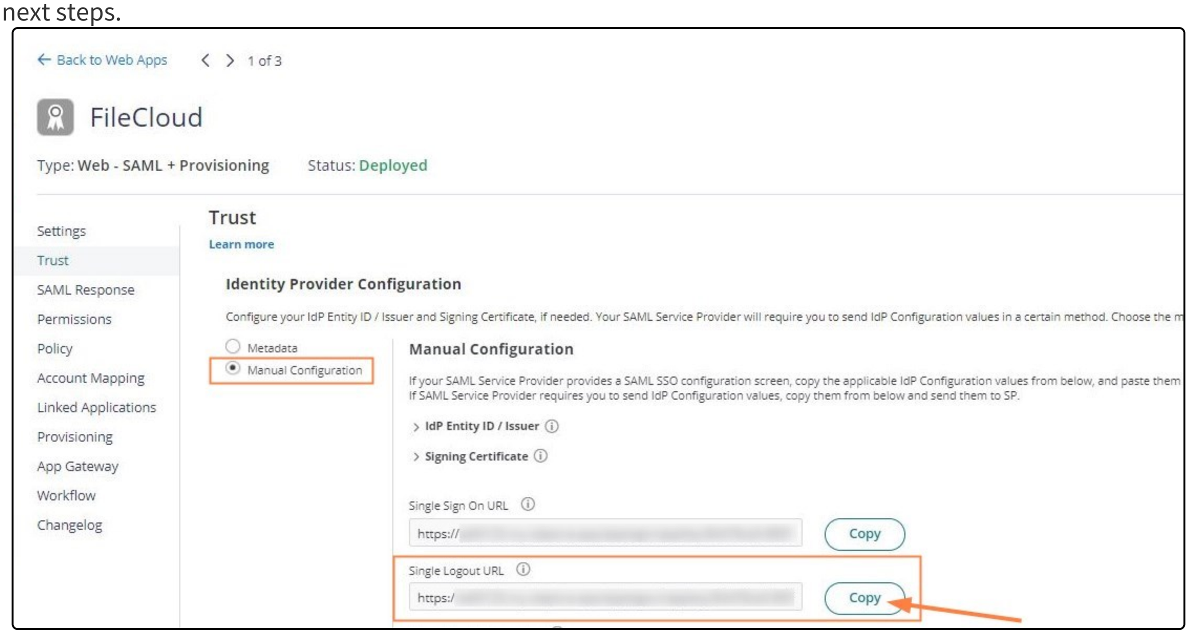


    b. Click **Trust** in the navigation panel, and download the metadata file.

c. Under **Identity Provider Configuration**, expand **IdP Entity ID /Issuer** and copy the URL into a notepad.



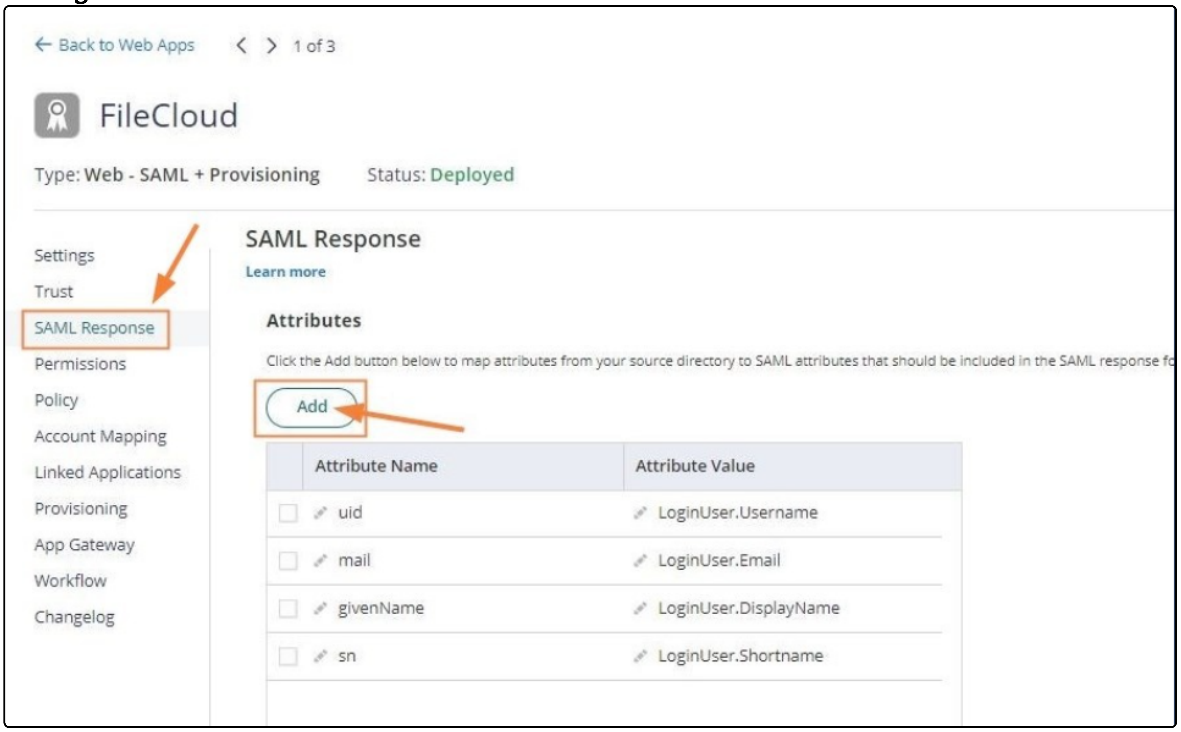
d. Select **Manual Configuration**, and copy the **Single Logout URL** into a notepad as it will be used in the next steps.



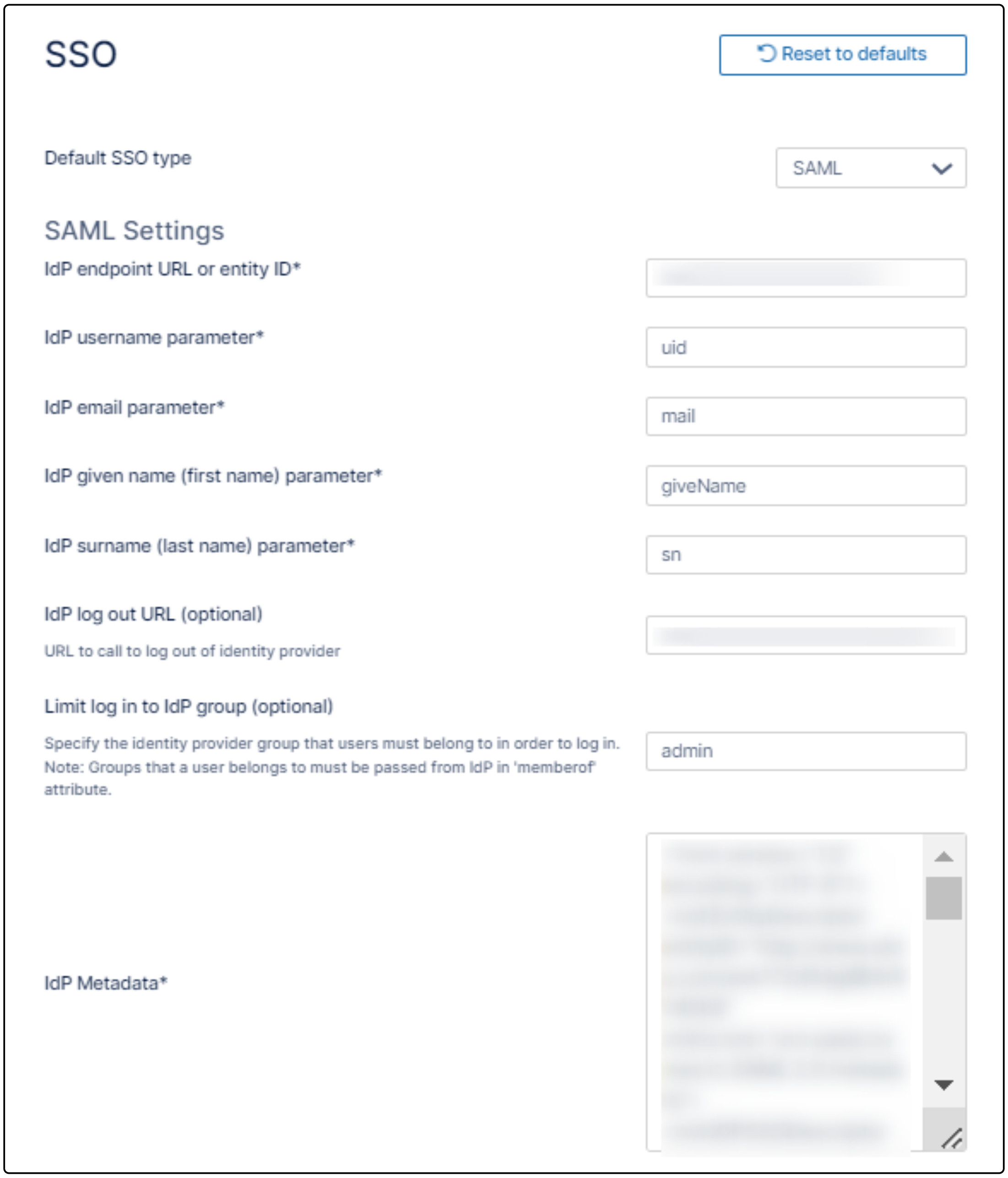
e. Access the **SAML Response** tab in the navigation panel, and add the following attribute values:

uid = LoginUser.Username
mail = LoginUser.Email
givenName = LoginUser.DisplayName

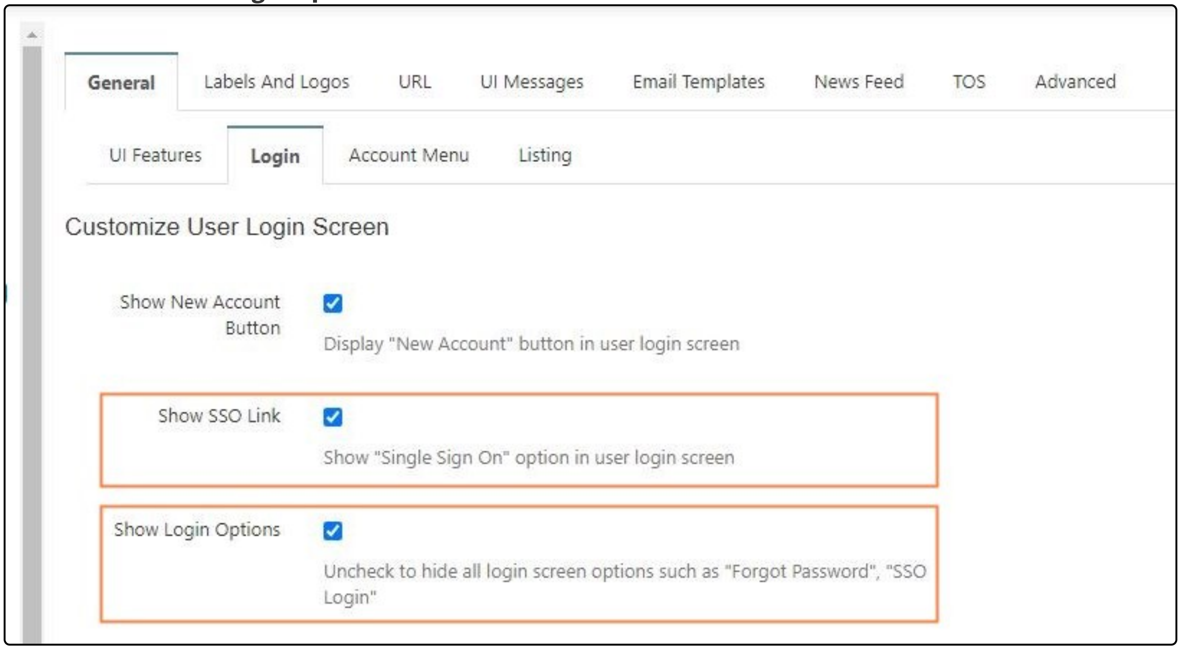
sn = LoginUser.Shortname



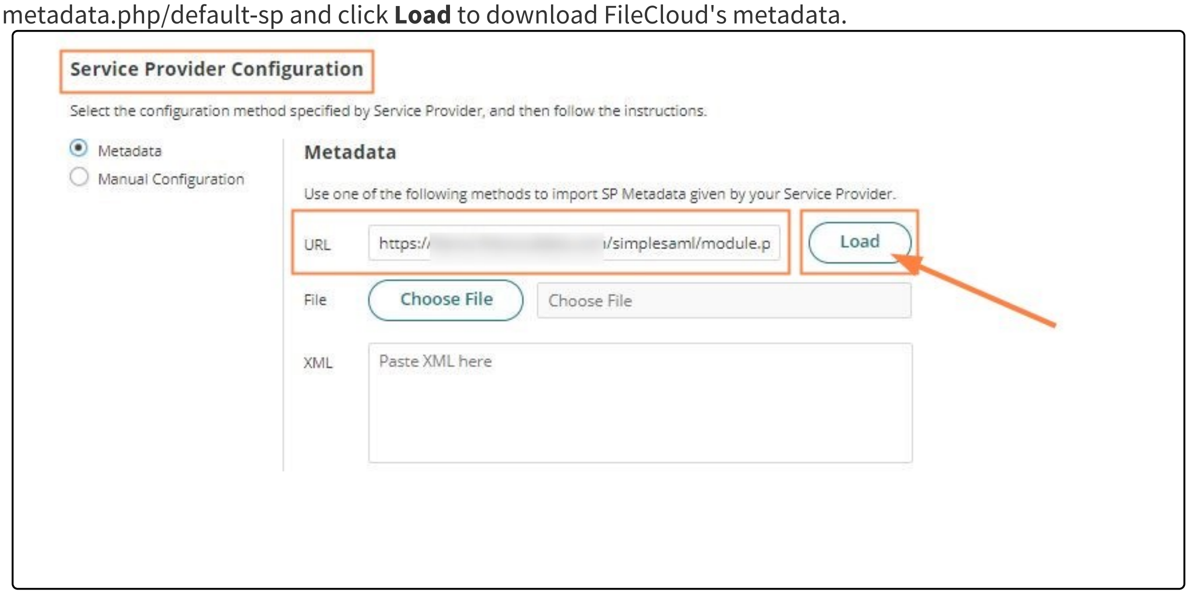
3. Export the metadata file into FileCloud and configure SSO.
   a. Configure Apache Webserver
   b. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
      i. Configure the following attributes:
      IdP Username Parameter = uid
      IdP Email Parameter = mail
      IdP Given Name Parameter = givenName
      IdP Surname Parameter = sn
      ii. Paste the **Single Logout URL** copied in step 2d into **IdP Log Out URL** (Optional)
      iii. Paste the **IdP Entity ID/Issuer URL** copied in step 2c into **Idp Endpoint URL or EntityID**
      iv. Open the metadata file downloaded in step 2b, and copy its content into **IdP Metadata**.
      v. Fill in the other settings on the page as shown in SAML Single Sign-On Support.
      vi. Click **Save**.


SSO
Reset to defaults
Default SSO type
SAML
SAML Settings
IdP endpoint URL or entity ID*
IdP username parameter*
uid
IdP email parameter*
mail
IdP given name (first name) parameter*
giveName
IdP surname (last name) parameter*
sn
IdP log out URL (optional)
URL to call to log out of identity provider
Limit log in to IdP group (optional)
Specify the identity provider group that users must belong to in order to log in.
Note: Groups that a user belongs to must be passed from IdP in 'memberof' attribute.
admin
IdP Metadata*

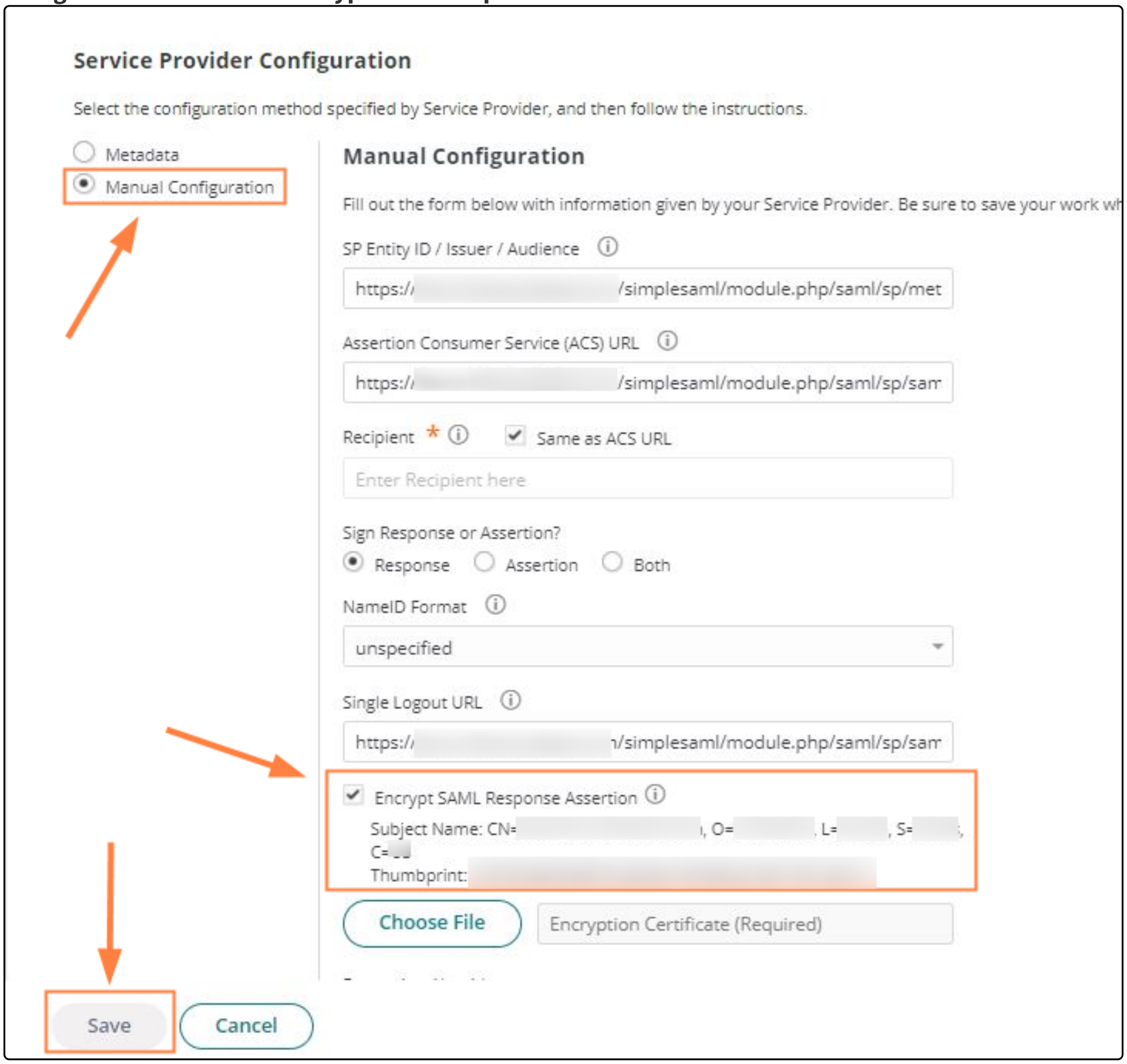
c. Enable SSO Login. In the FileCloud admin portal, go to **Customization > General > Login**. Enable **Show SSO Link** and **Show Login Options**.



4. Configure the service provider in CYBERARK.
   a. Click the **Trust** tab in the navigation panel for the Web App, and scroll down to **Service Provider Configuration**.
   b. In URL, add the following: https://YOUR-FILECLOUD-URL/simplesaml/module.php/saml/sp/metadata.php/default-sp and click **Load** to download FileCloud's metadata.

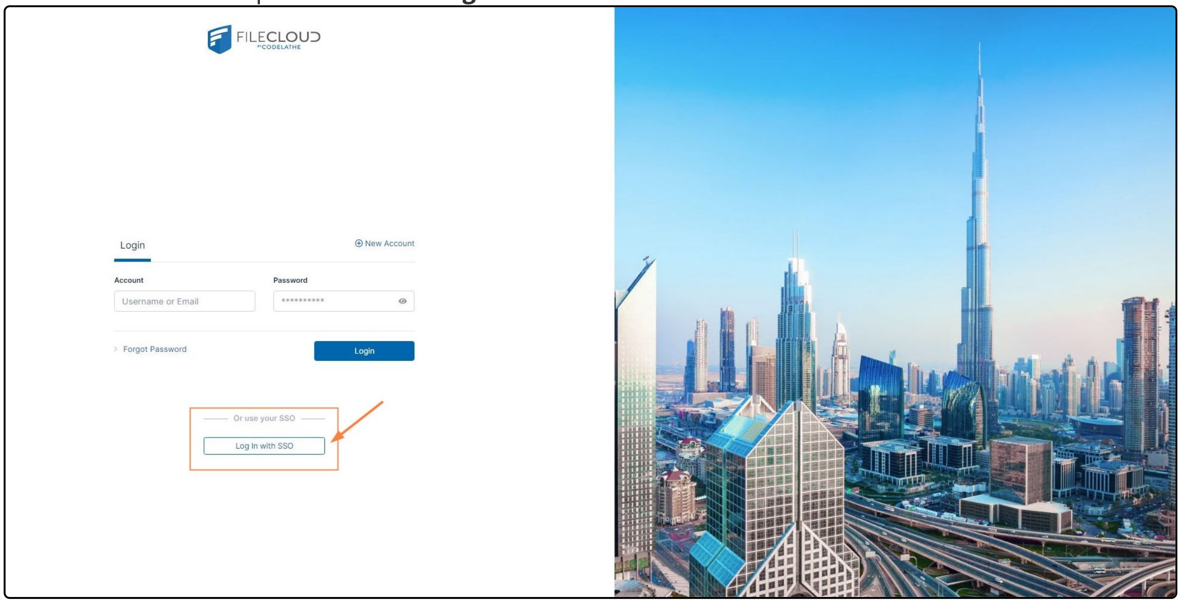


c. Once you have loaded FileCloud's metadata, change the settings from **Metadata** to **Manual Configuration** and disable **Encrypt SAML Response Assertion**. Click **Save**.

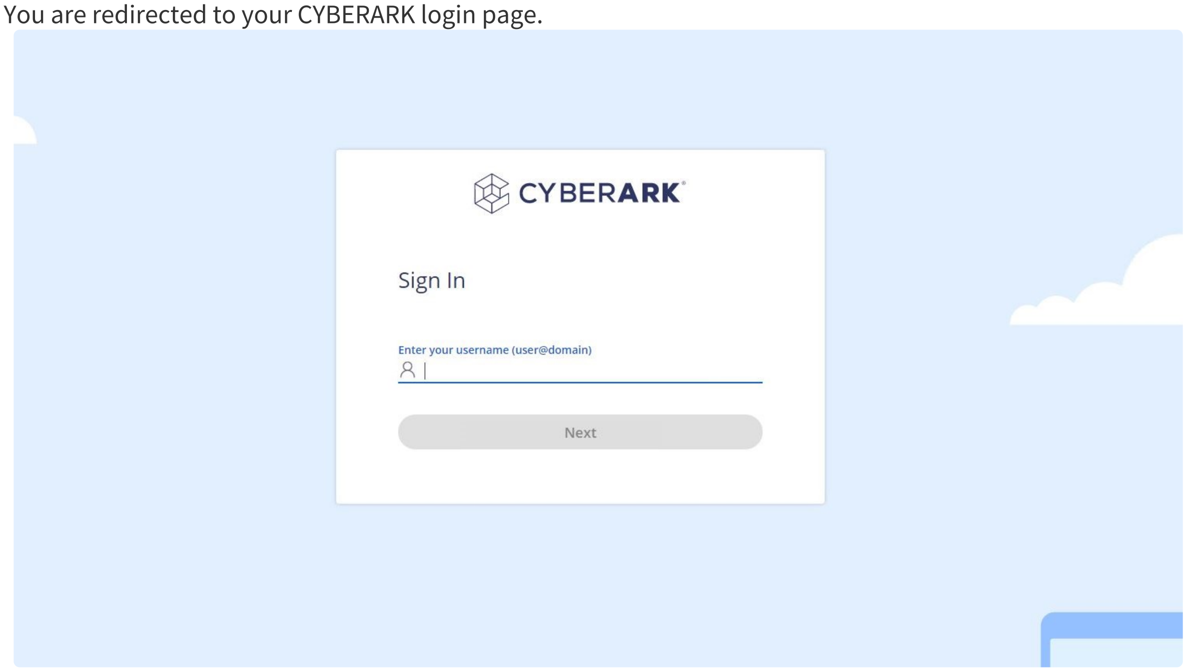


5. Complete CYBERARK SSO integration.

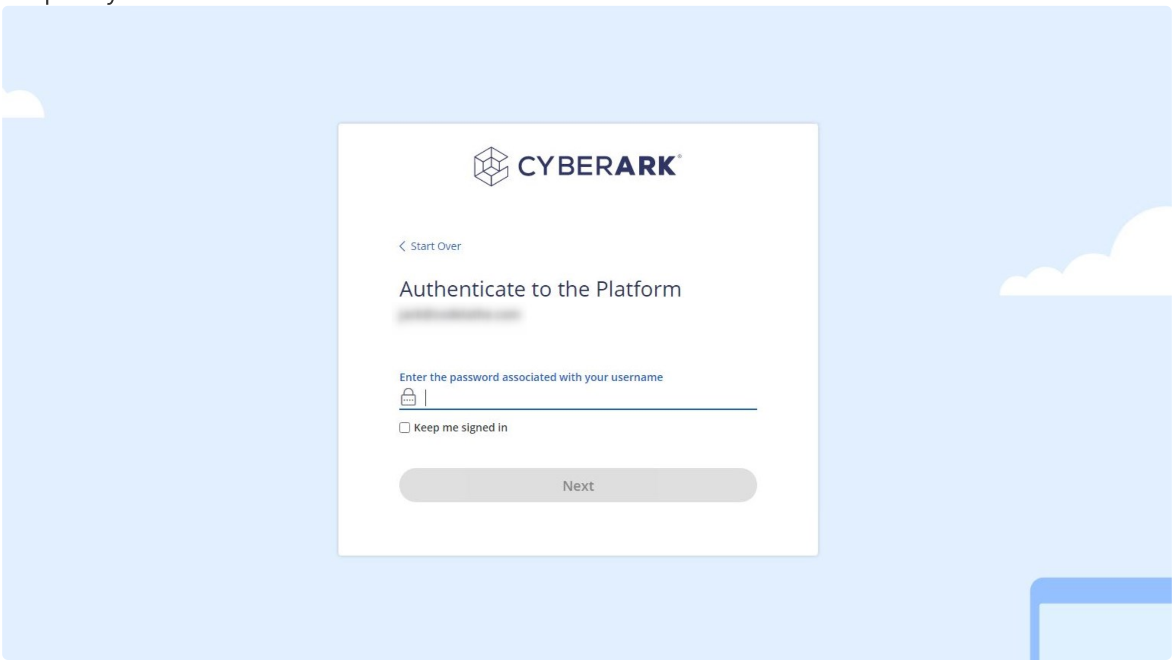
a. Access FileCloud's user portal and click **Login In with SSO**.



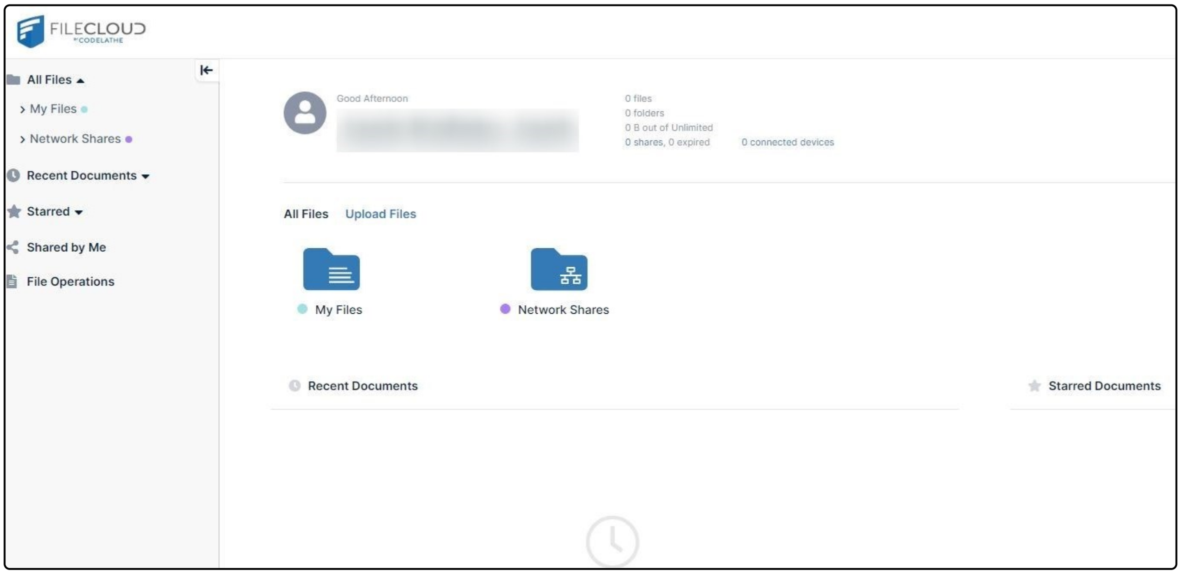
You are redirected to your CYBERARK login page.



b. Complete your user authentication.



You are redirected to FileCloud.



Now you can use single sign-on with CYBERARK from FileCloud.

Integrate JumpCloud with FileCloud

> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator you can integrate these two systems so that your JumpCloud users can access their FileCloud account without having to enter their credentials a second time.

JumpCloud Directory-as-a-Service	JumpCloud's is a cloud-based platform • It enables IT teams to securely manage user identities • It connects teams them to resources they need regardless of provider, protocol, vendor, or location

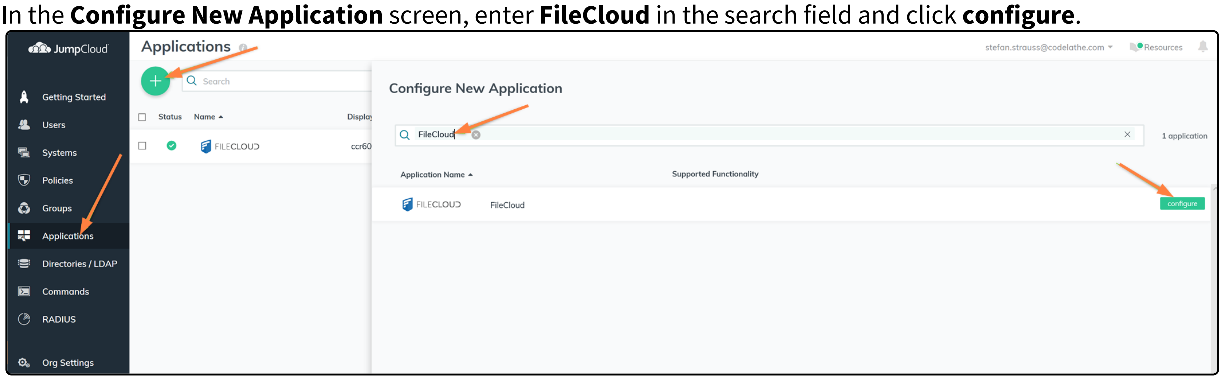
In this integration scenario:

- JumpCloud must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

Configure FileCloud with JumpCloud

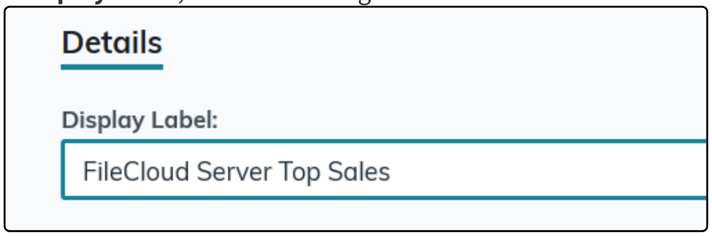
1. In JumpCloud, create a new application.

1. Open a browser and log in to your JumpCloud admin interface at https://console.jumpcloud.com/login.
2. From the left navigation pane, click **Applications**.
3. On the **Applications** screen, to add a new application, click the plus sign.
4. In the **Configure New Application** screen, enter **FileCloud** in the search field and click **configure**.

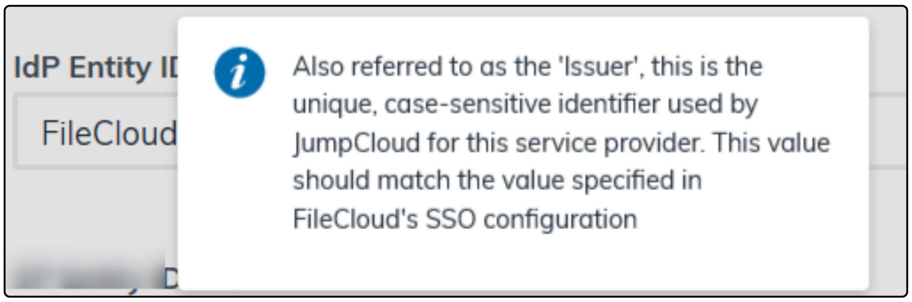


2. In JumpCloud, configure the FileCloud application

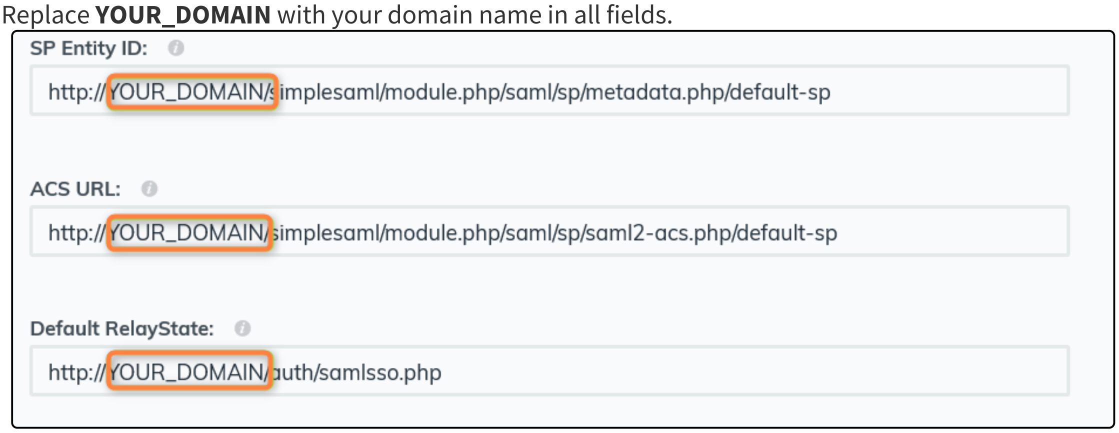
1. In **Display Label**, enter a meaningful name.



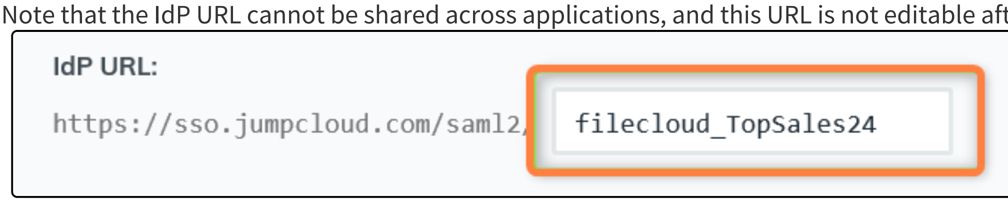
2. In **IDP Entity ID**, enter a unique, case-sensitive identifier to be used by JumpCloud for this FileCloud service provider.



3. Replace **YOUR_DOMAIN** with your domain name in all fields.

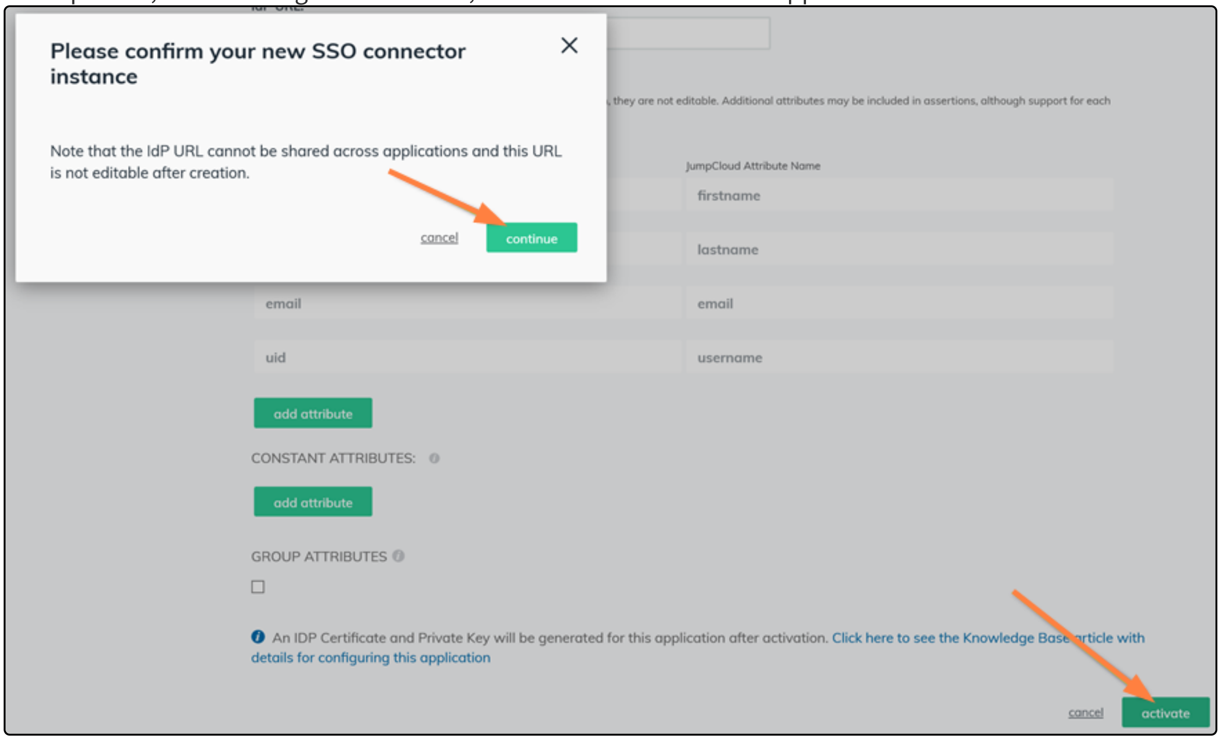


4. Enter a unique value for **IdP URL**.
   Note that the IdP URL cannot be shared across applications, and this URL is not editable after creation.

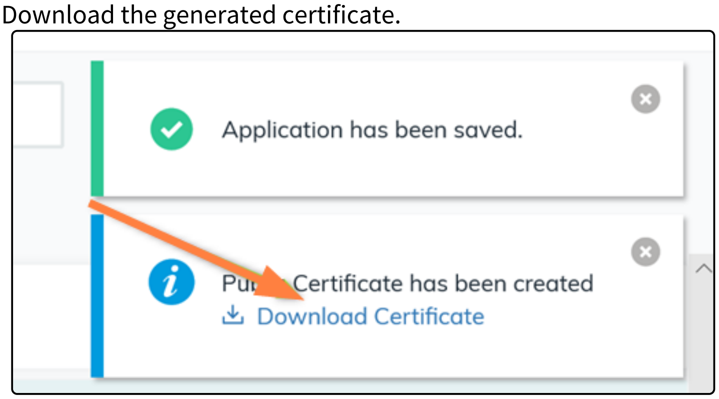


3. In JumpCloud, activate the new application and export metadata and certificate

1. In JumpCloud, on the configuration screen, save and activate the new application



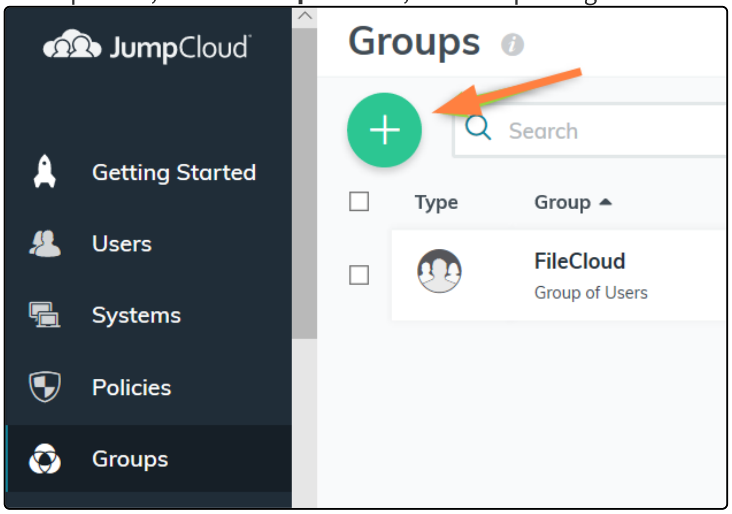
2. Download the generated certificate.



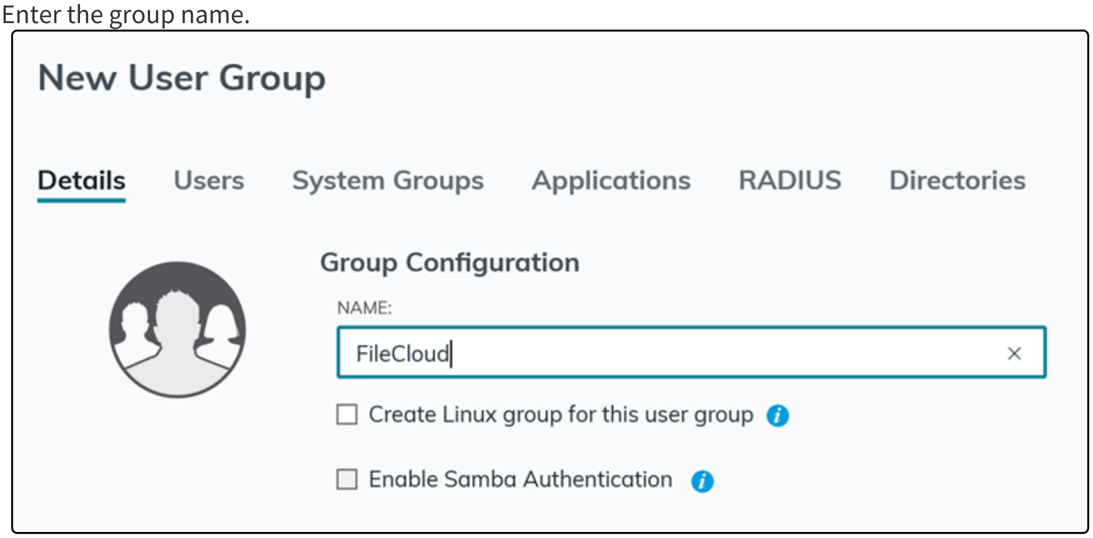
3. The **saml.crt** file must be copied into the correct location in the FileCloud root folder for your integration to work. Contact FileCloud support and request that your **saml.crt** file be copied into your Simple SAML certificate folder.

4. In JumpCloud, create a group and add users

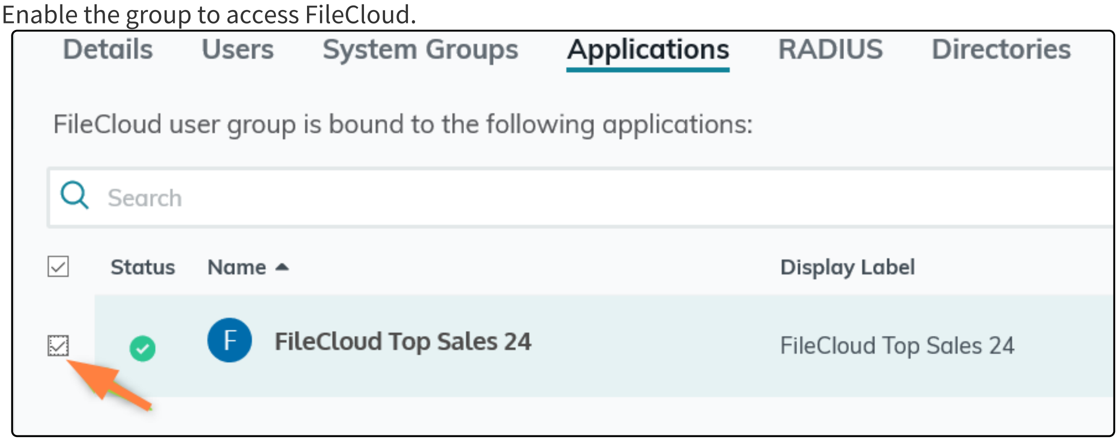
1. In JumpCloud, on the **Groups** screen, click the plus sign to add a new group.



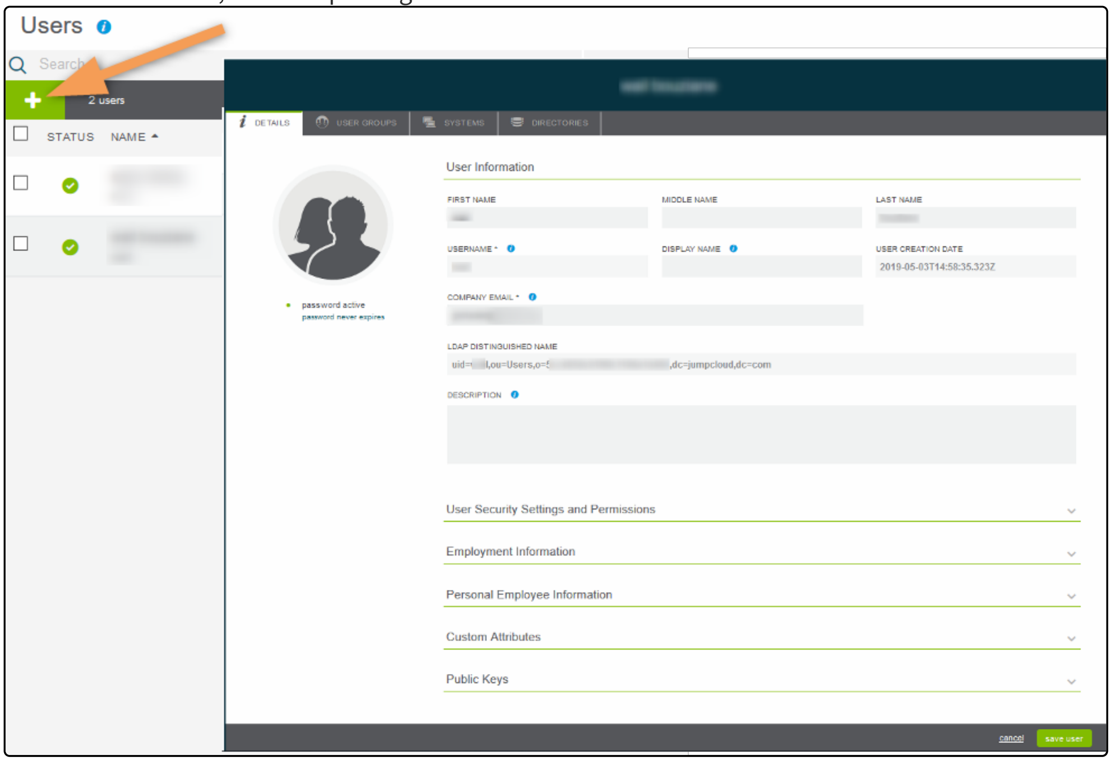
2. Enter the group name.



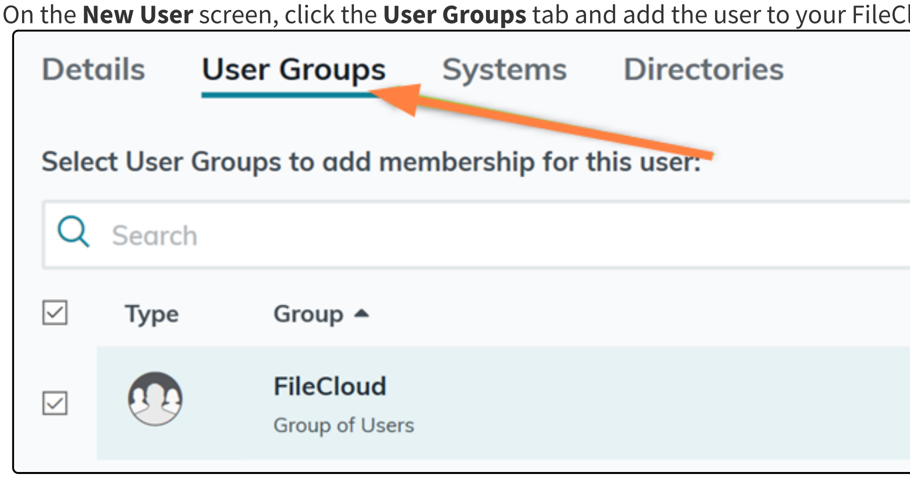
3. Enable the group to access FileCloud.



4. On the **Users** screen, click the plus sign to add a new user.



5. On the **New User** screen, click the **Details** tab and type in the user's information.
6. On the **New User** screen, click the **User Groups** tab and add the user to your FileCloud group.

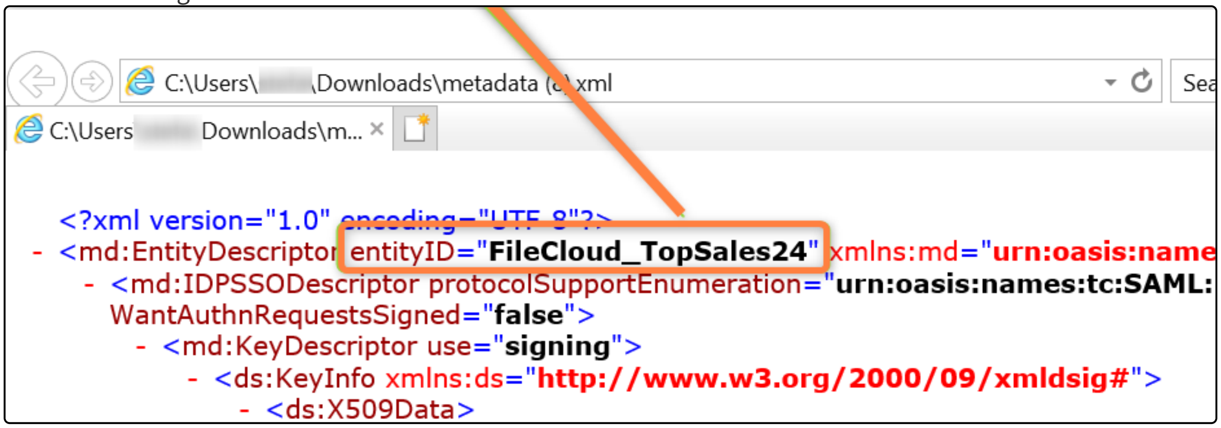


7. Click **Save User**.

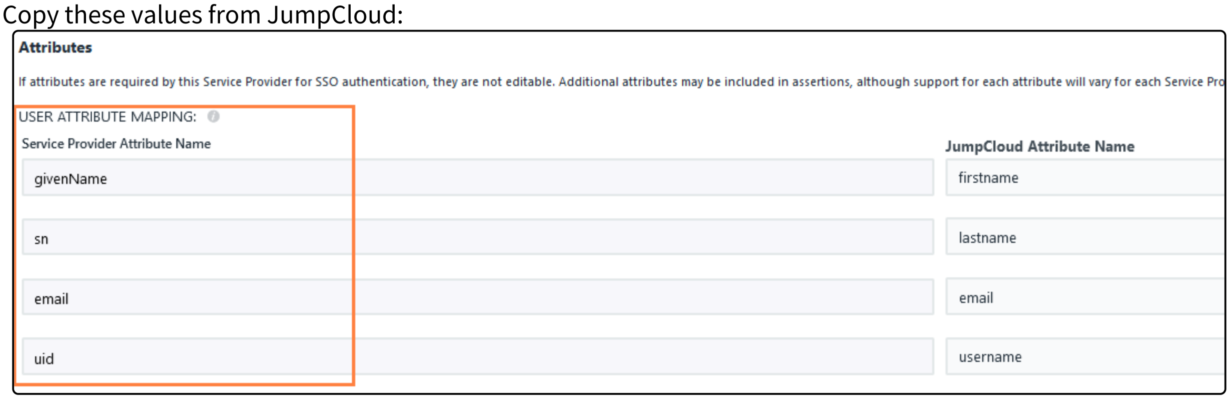
5. In FileCloud, configure the SSO settings.

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

2. In **Idp End Point URL**, type or paste in the same value as the **IdP Entity ID** that you entered into JumpCloud. The correct string can also be seen in the metadata xml file:

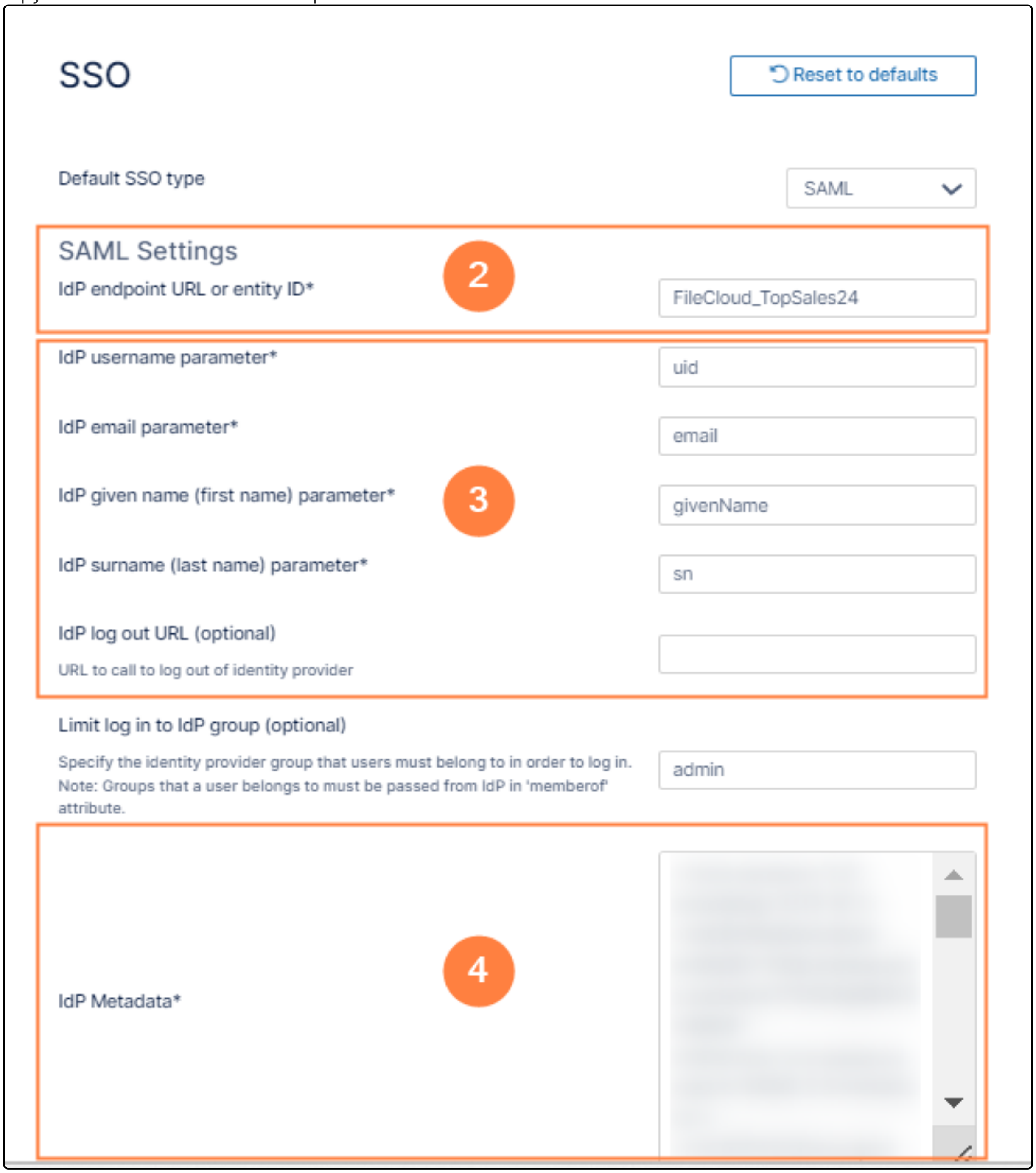


3. Input the **Service Provider Attribute Name** information from the JumpCloud configuration screen into the corresponding fields in the FileCloud **Settings > SSO** tab.
Copy these values from JumpCloud:



Enter them into the corresponding settings in FileCloud on the **Settings > SSO** tab.

4. On the server, open the XML file that contains the metadata you exported from JumpCloud.
   Copy the metadata in the file and paste it into the **IdP Metadata** field in FileCloud.



5. Fill in the other settings on the page as shown at SAML Single Sign-On Support.
6. Click **Save** and minimize the browser.

Now you can start using single sign-on with JumpCloud from FileCloud.

Integrate Okta with FileCloud

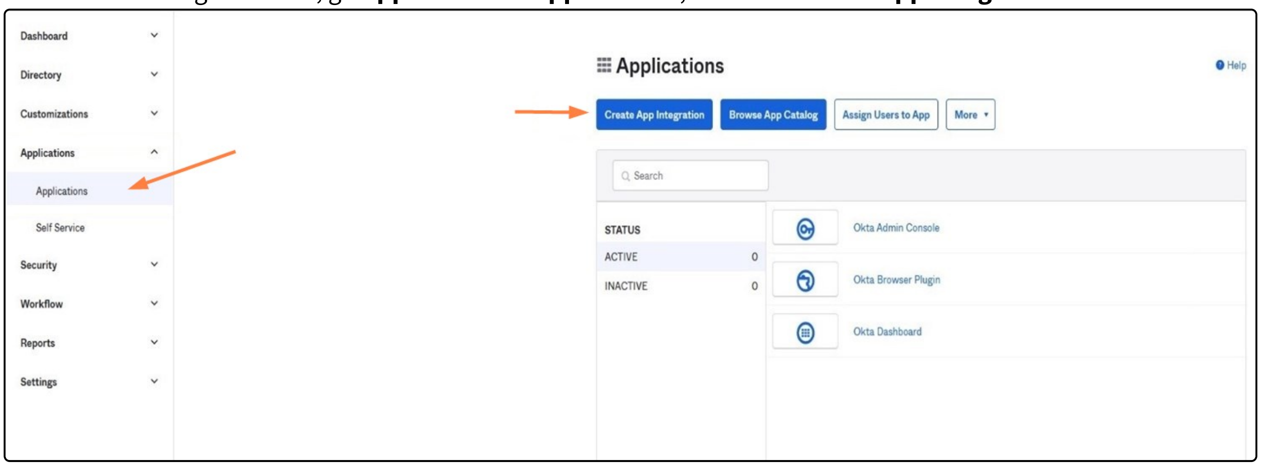
To integrate with the Okta browser plugin, please see Integrate with Okta using browser plugin.

> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

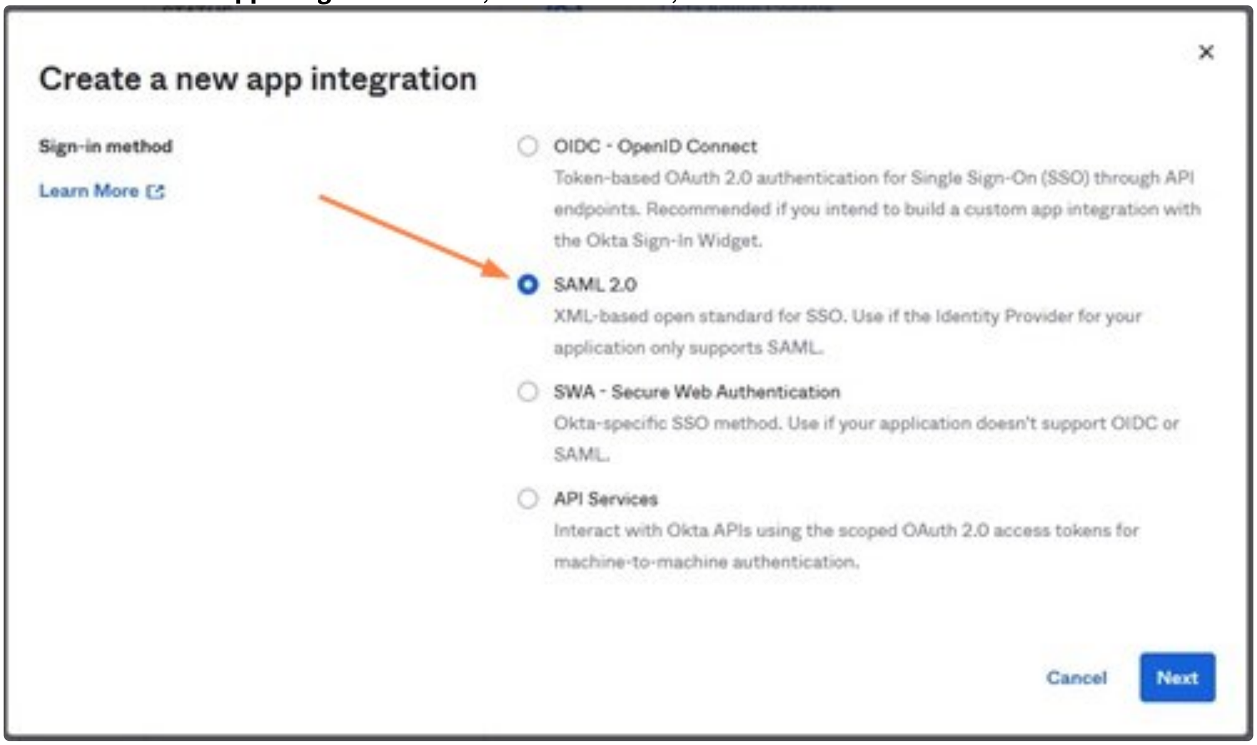
When FileCloud is integrated with Okta, Okta is configured as an Identity Provider (IdP) and FileCloud acts as the Service Provider (SP).

To configure FileCloud with Okta:

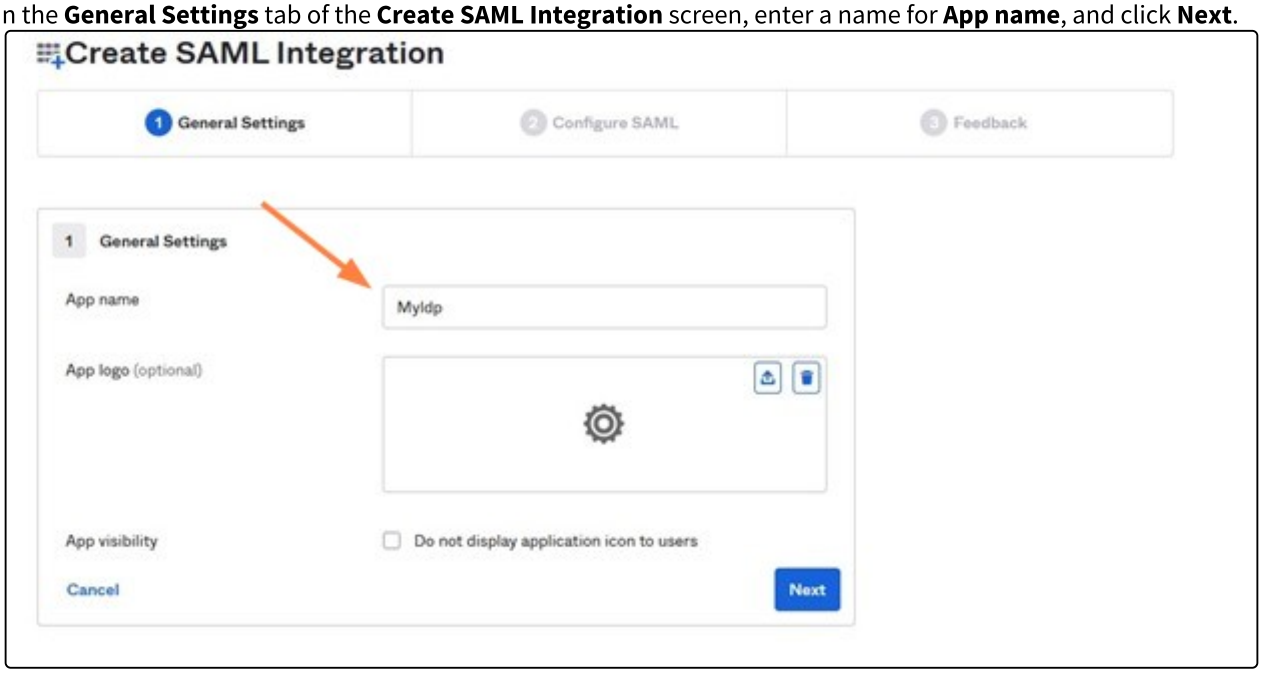
1. Log in to your Okta-issued URL, which has the format: https://yourdomain-admin.okta.com/admin/dashboard
2. After successful login to Okta, go **Applications > Applications**, and click **Create App Integration**.



3. In the **Create a new app integration** screen, select **SAML 2.0**, and click **Next**.

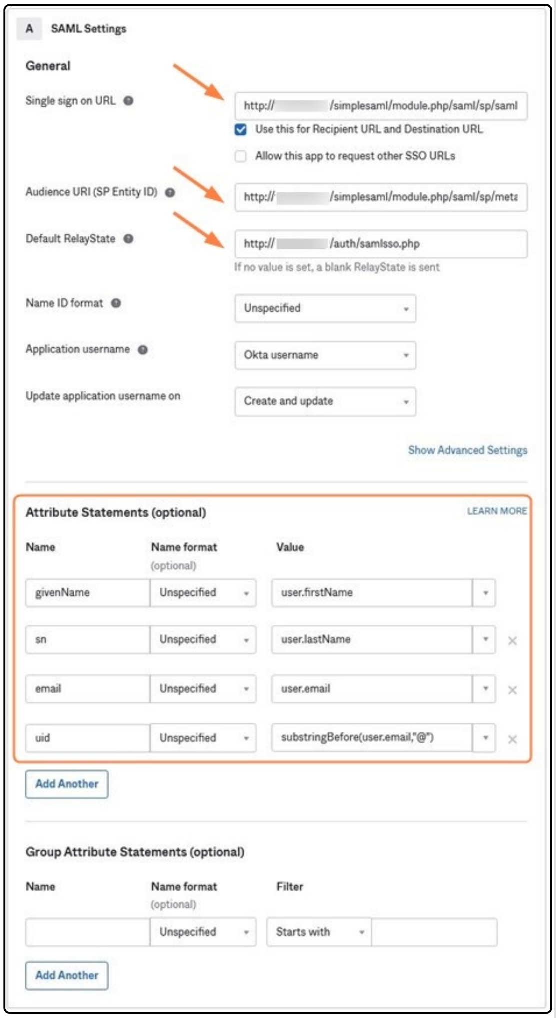


4. In the **General Settings** tab of the **Create SAML Integration** screen, enter a name for **App name**, and click **Next**.



5. In the **SAML Settings** screen, set the values as follows:
   - Set **Single sign on URL** to the FileCloud assertion URL **http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp**
   - Set **Audience URI (SP Entity ID)** to **http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp**
   - Set **Default Relay State** to **http://<your domain>/auth/samlsso.php**

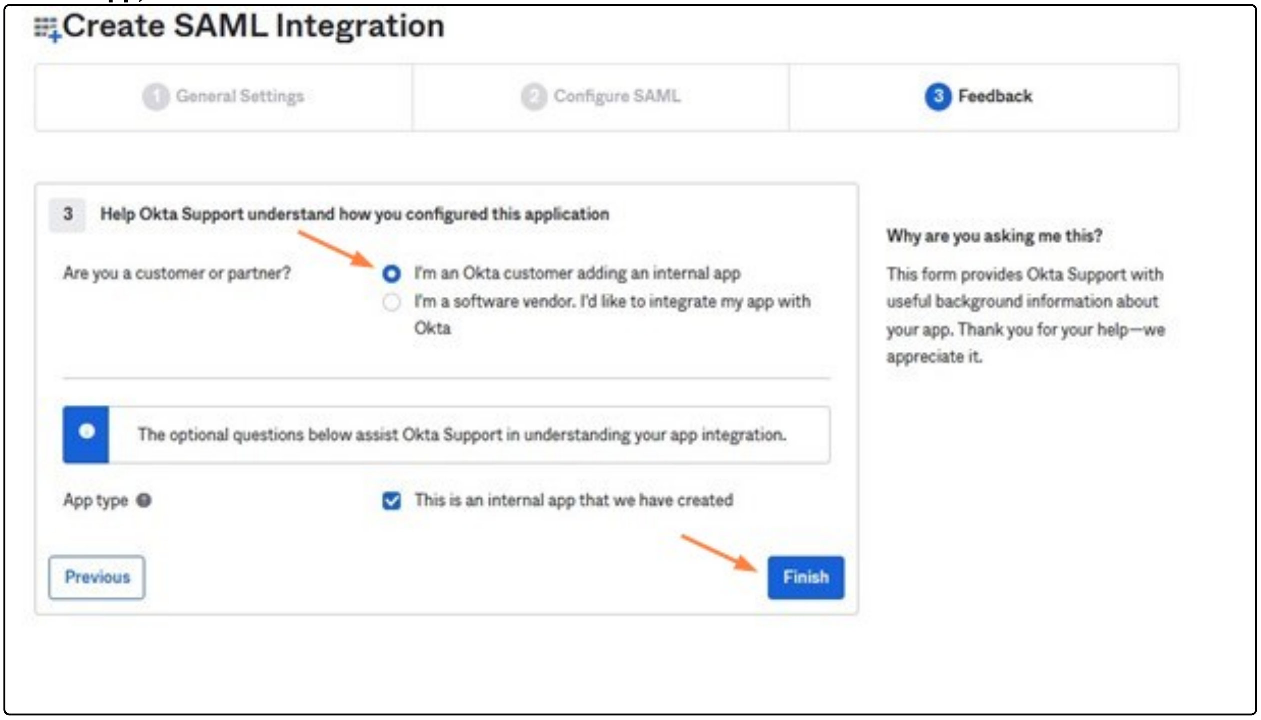
- Under **Attribute Statements**, the attribute names must match the names set in the FileCloud admin portal in **Settings > SSO** for **Idp Username Parameter**, **Idp Email Parameter**, **Idp Given Name Parameter**, and **IDP Surname Parameter**.
  Set the **Values** for the **Attribute Statements** to the values shown in the screenshot.

<table>
<tr><th>Okta</th><th>FileCloud</th></tr>
<tr><td>


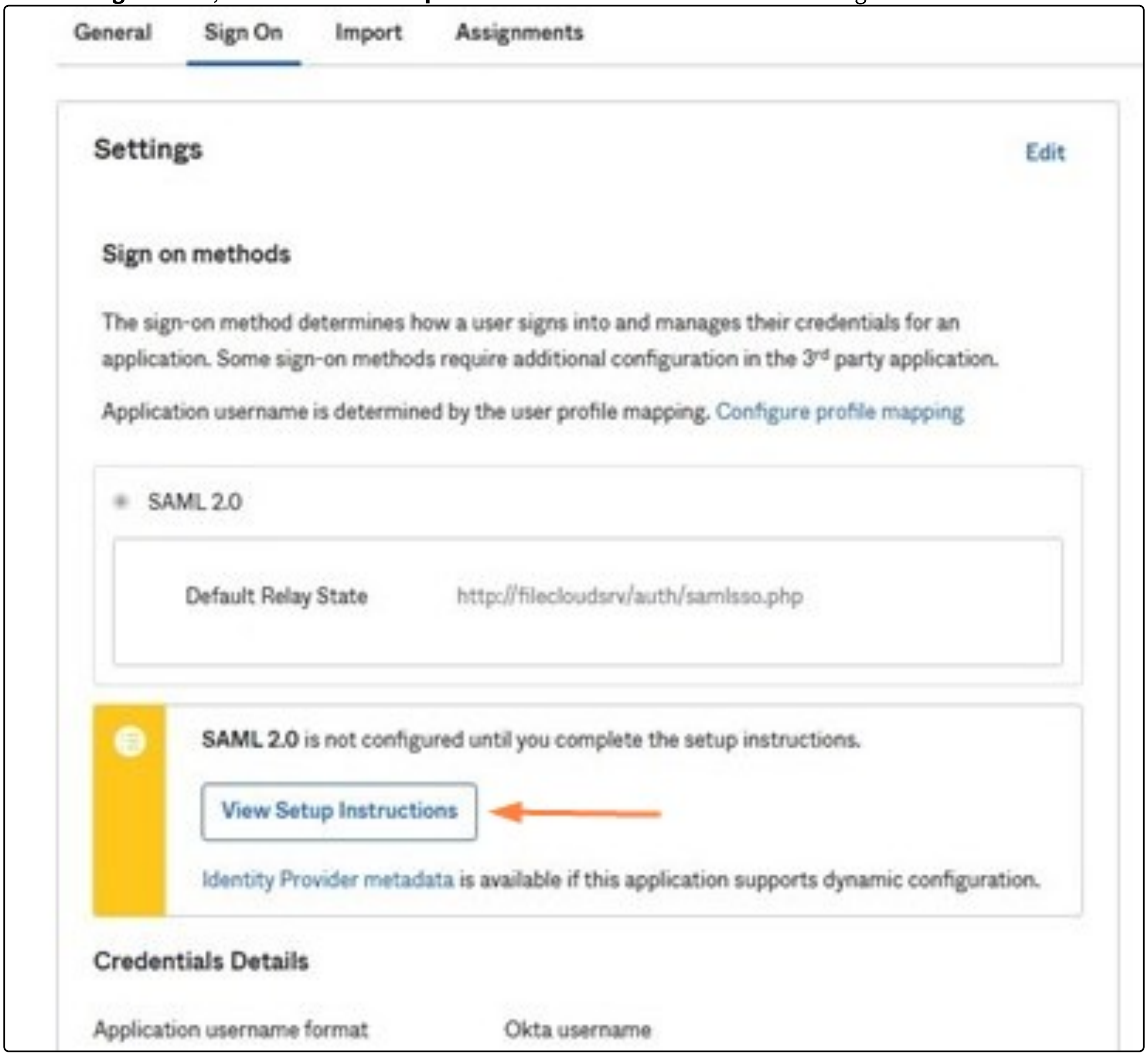
</td><td>


</td></tr>
</table>

6. Click the **Feedback** tab of the **Create SAML Integration** screen, then select **I'm an Okta customer adding an internal app**, and click **Finish**.



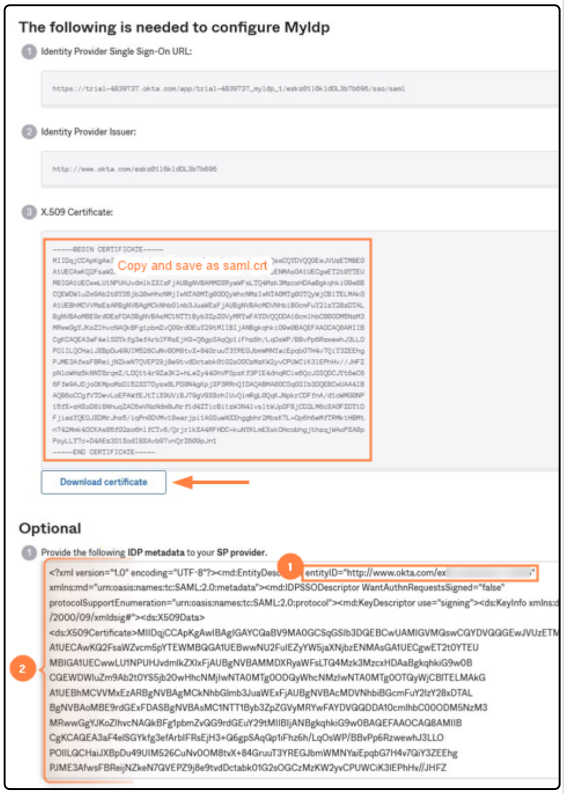
7. Go to the **Sign On** tab, and click **View Setup Instructions** to view FileCloud SSO configuration details .

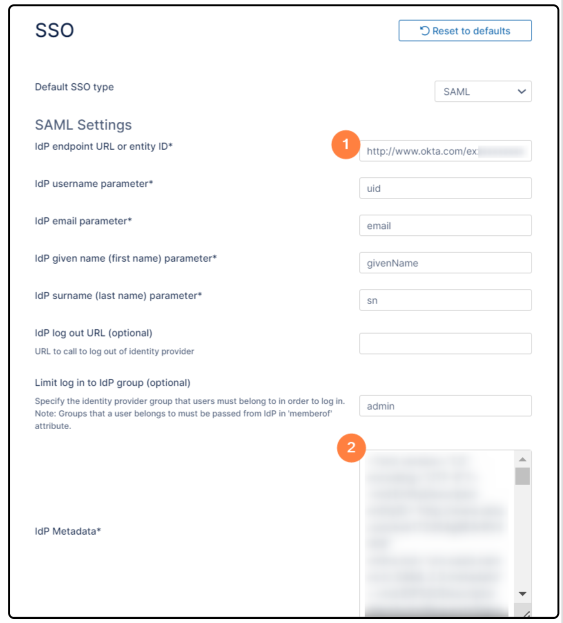


A screen with information similar to the first image in the table below opens.

8. Use the details in this screen to configure the settings in the FileCloud admin portal's **Settings > SSO** screen and to create a **saml.crt** file.
   a. Using the **IDP Metadata** text under **Optional**:
   (1) Copy the **entityID** field from the text box into **Idp Endpoint URL or EntityID** in FileCloud admin UI interface under **Settings > SSO**.
   (2) Confirm that the text in the **IDP Metadata** box is the same as the text in **Idp Metadata** in FileCloud admin UI interface under **Settings > SSO**.
   b. Click **Download certificate**, then copy the certificate file and rename it to **saml.crt**.

   The **saml.crt** file must be copied into the correct location in the FileCloud root folder for your integration to work. Contact FileCloud support and request that your **saml.crt** file be copied into your Simple SAML certificate folder.

<table>
<tr><th>Okta Setup Instructions</th><th>FileCloud SSO Settings</th></tr>
<tr><td>


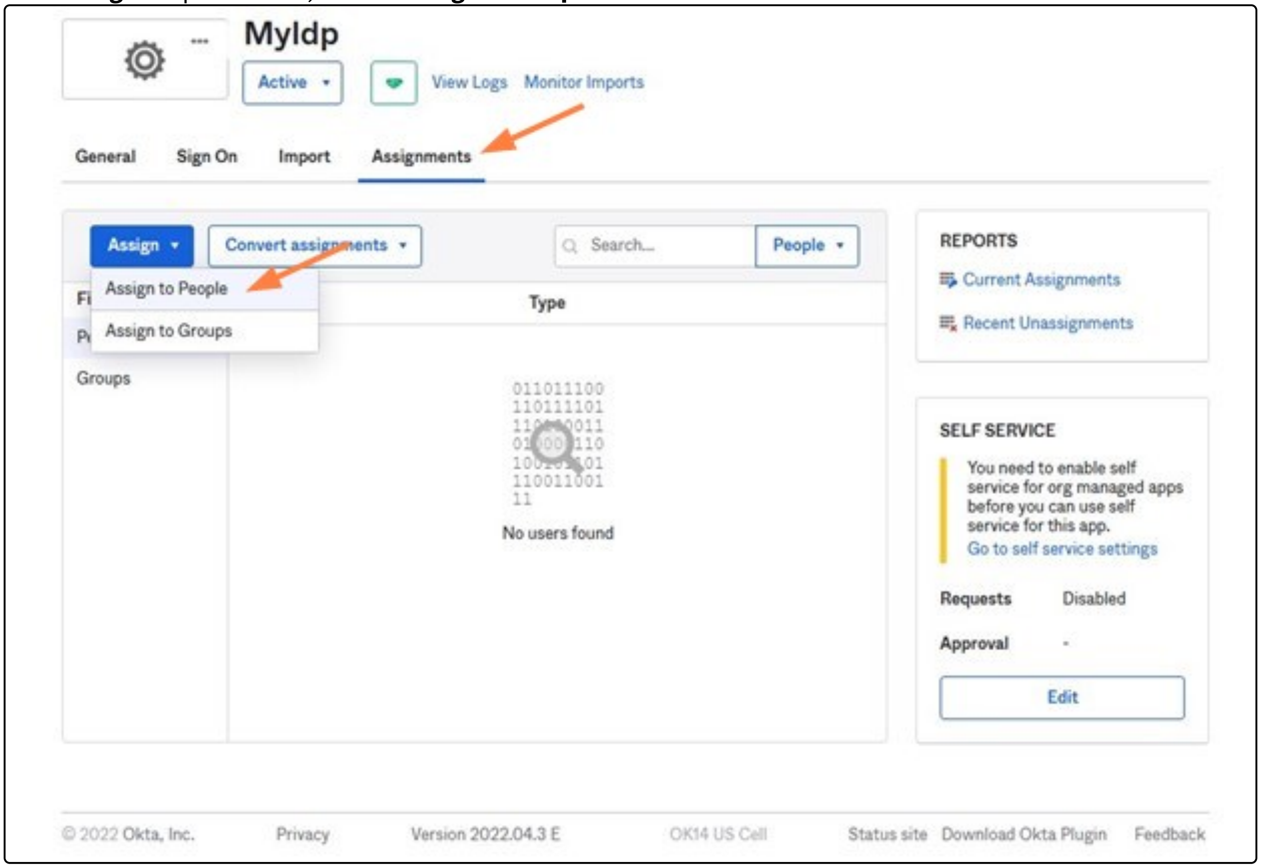
</td><td>


</td></tr>
</table>

Now assign the Okta FileCloud integration to users so they can log in with Okta.

9. Click the **Assignments** tab in Okta.

10. In the **Assign** drop-down list, choose **Assign to People**.



A list of users who have both Okta and FileCloud accounts opens.

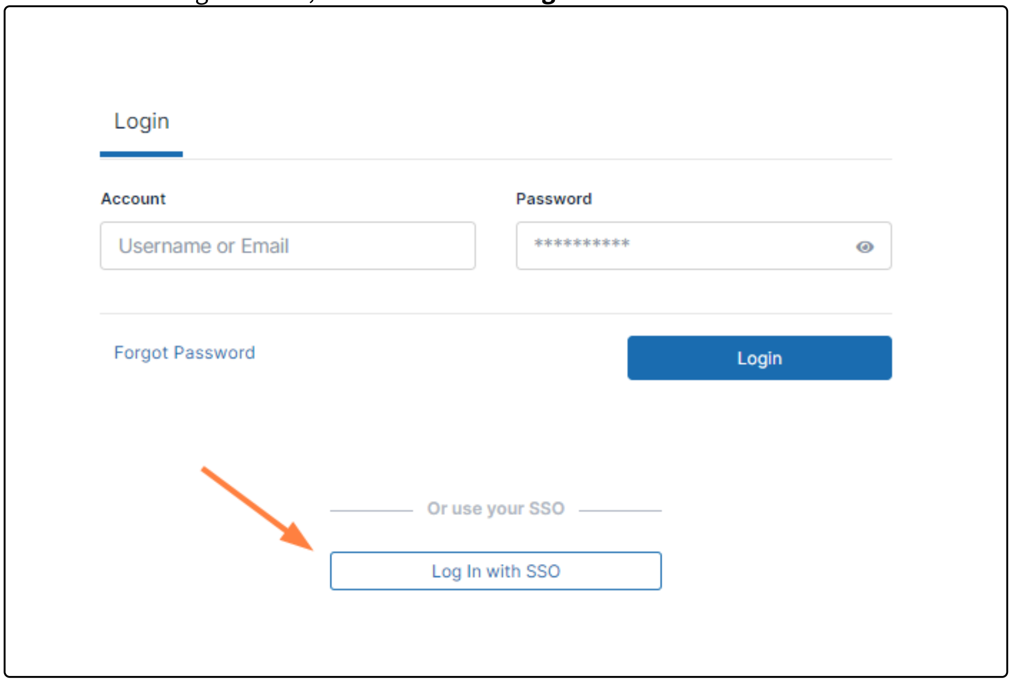
11. Select users from the list to allow them to sign in to FileCloud using Okta.

Once the application is created and FileCloud is configured you can start using single sign-on with Okta from FileCloud.

Log in to FileCloud using Single Sign-on with Okta

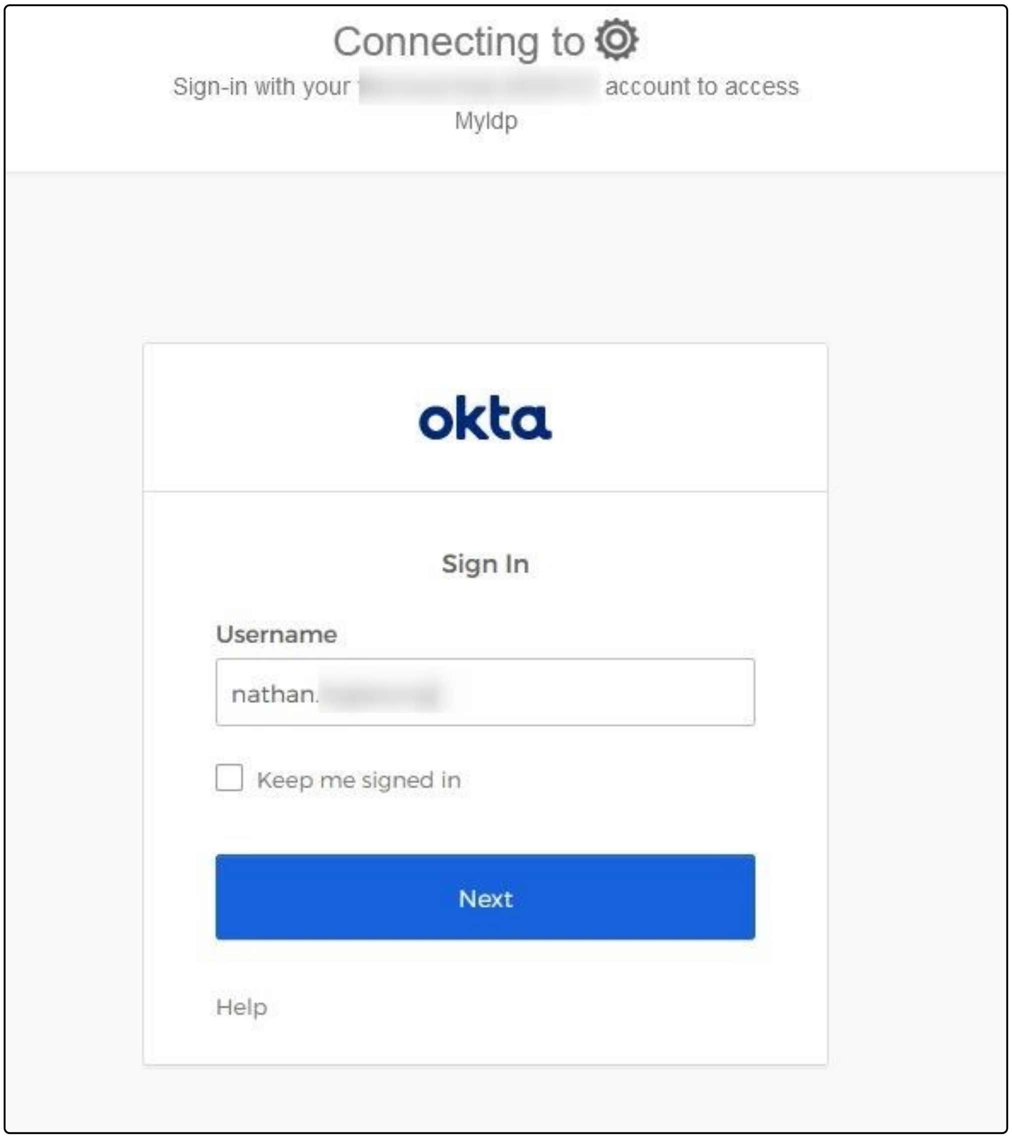
Users can sign in to the user portal or admin portal with SSO using Okta.

1. In the FileCloud login screen, the user chooses **Log in with SSO**.



If the user is already logged in to Okta, they are automatically logged in to FileCloud.

If the user not logged in to Okta, they are first redirected to the Okta sign in page, and after signing in to Okta, they are immediately redirected to FileCloud and logged in.



Integrate with Okta using browser plugin

> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

The Okta plugin for browsers works by storing FileCloud user credentials in a web application that you add to Okta. After a user chooses to log in with Okta, the credentials are entered in the FileCloud page and log in proceeds automatically.

The Okta plugin works with default FileCloud login, not SSO. Do not configure SSO settings in FileCloud.

Procedure:

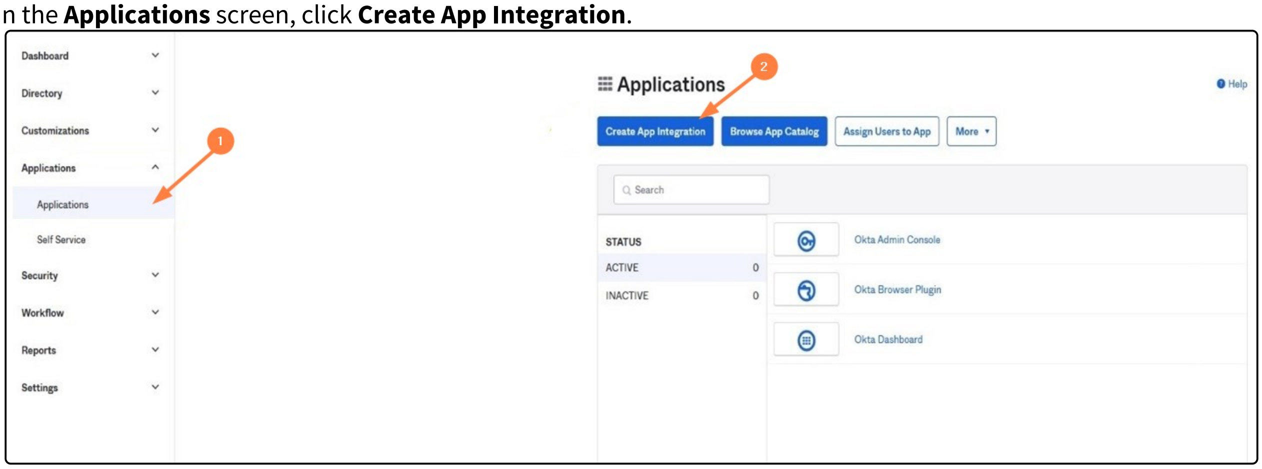
Note: You must have an Okta account before completing these steps.

1. Set up the FileCloud application in the Okta admin panel
2. Assign the FileCloud application to users
3. Install the plugin on the user browser.
4. User logs in to FileCloud using the plugin.

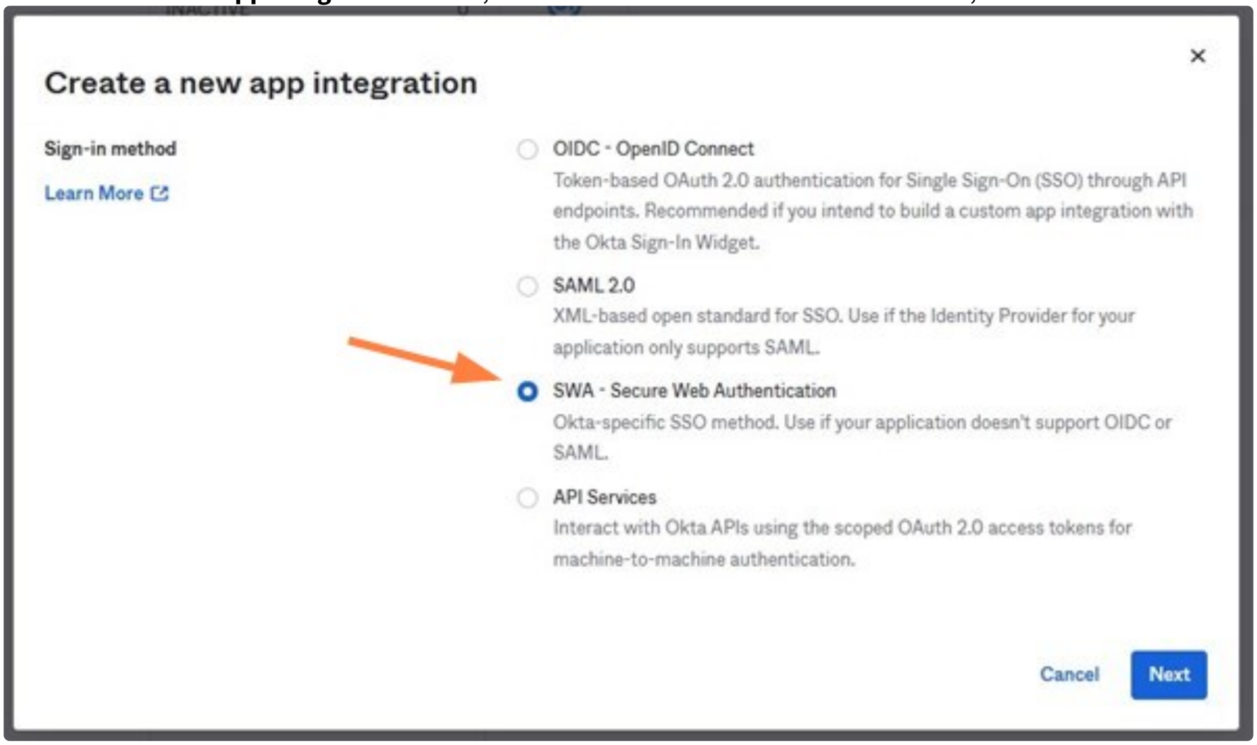
> The plugin supports different browsers. Setup and tests for this guide use Google Chrome.

Set up the FileCloud application in Okta admin panel

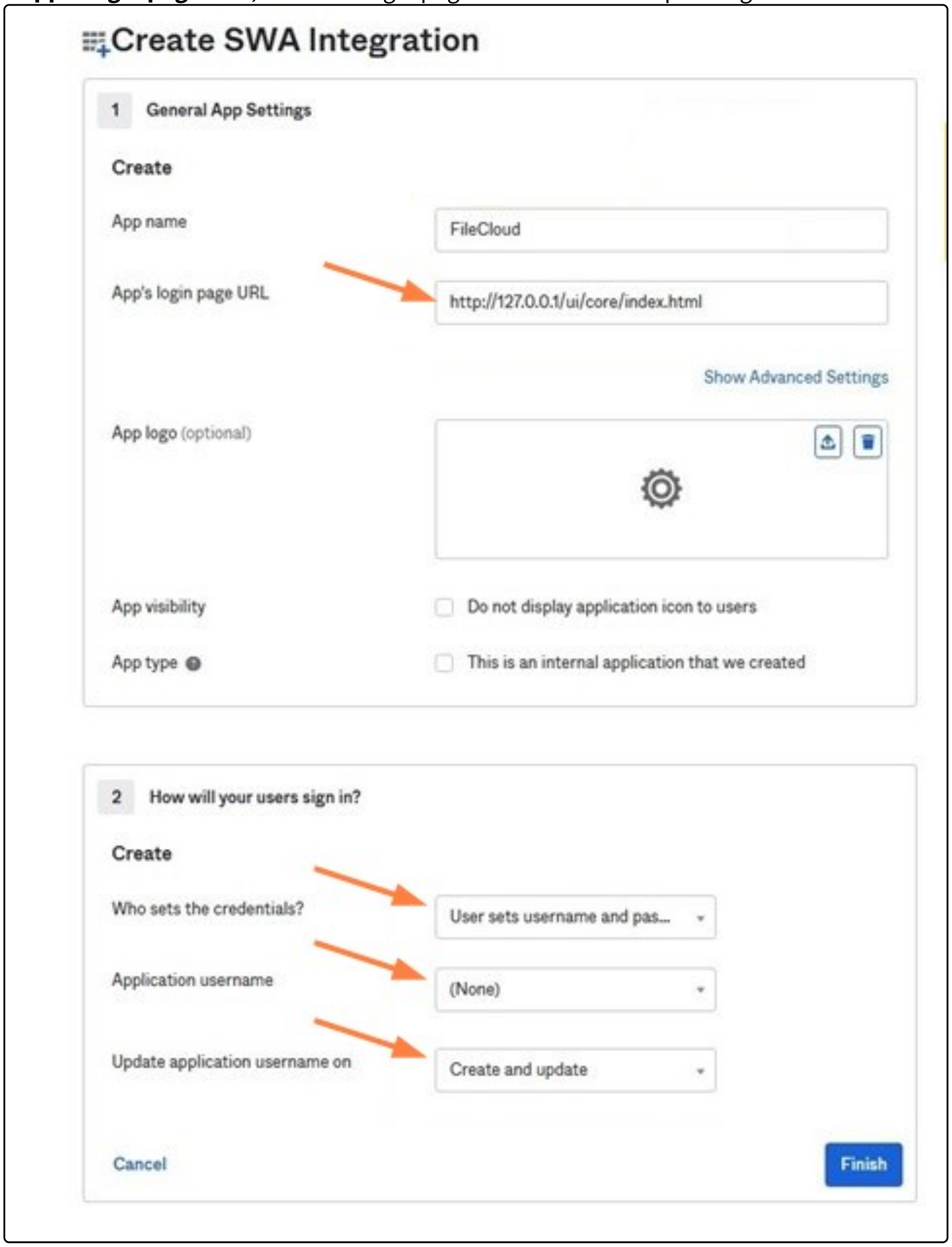
1. Log in as Admin in Okta.
2. In the navigation panel, click **Applications > Applications**.
3. In the **Applications** screen, click **Create App Integration**.



4. In the **Create a new app integration** screen, choose **SWA - Secure Web Authentication**, and click **Next**.



5. Fill in the **Create SWA Integration** screen as shown in the following screenshot, and click **Finish**.
   In **App's login page URL**, enter the login page URL for the corresponding FileCloud installation.

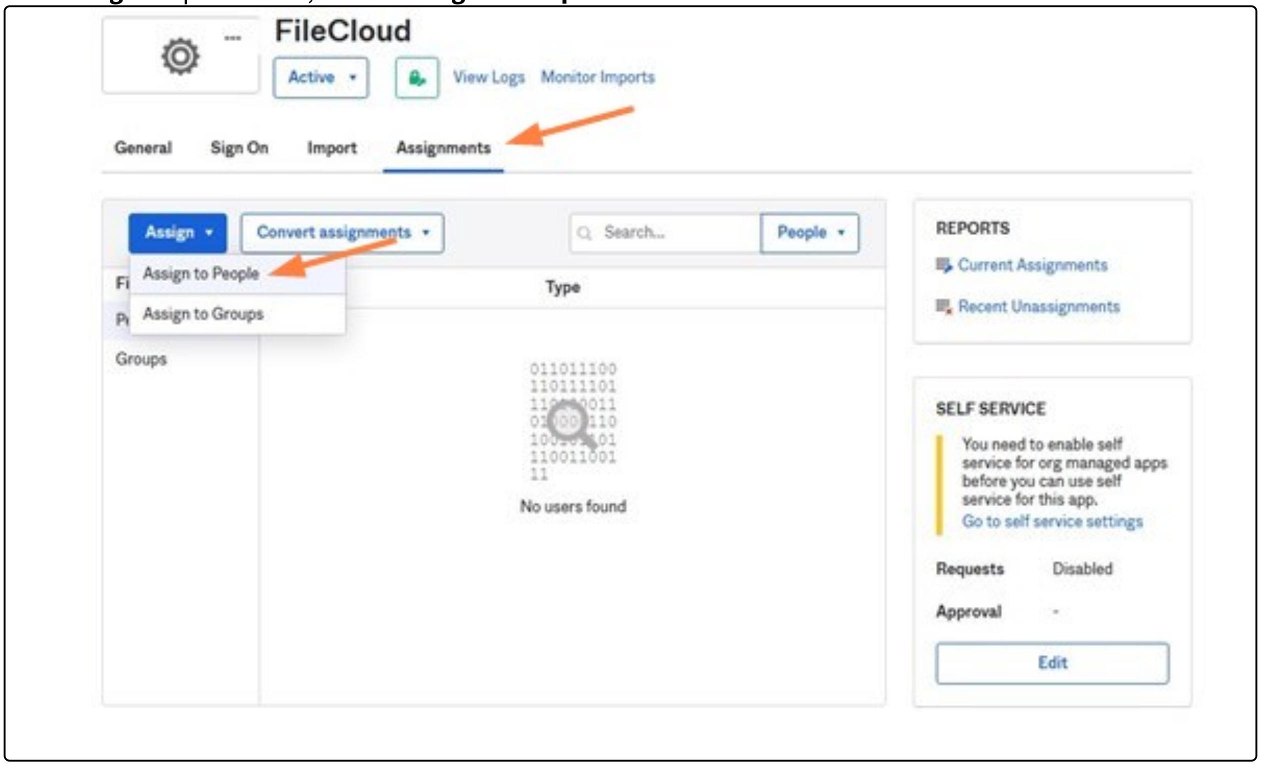


Assign application to users

Now assign the Okta FileCloud integration to users so they can log in with Okta.

1. Click the **Assignments** tab in Okta.

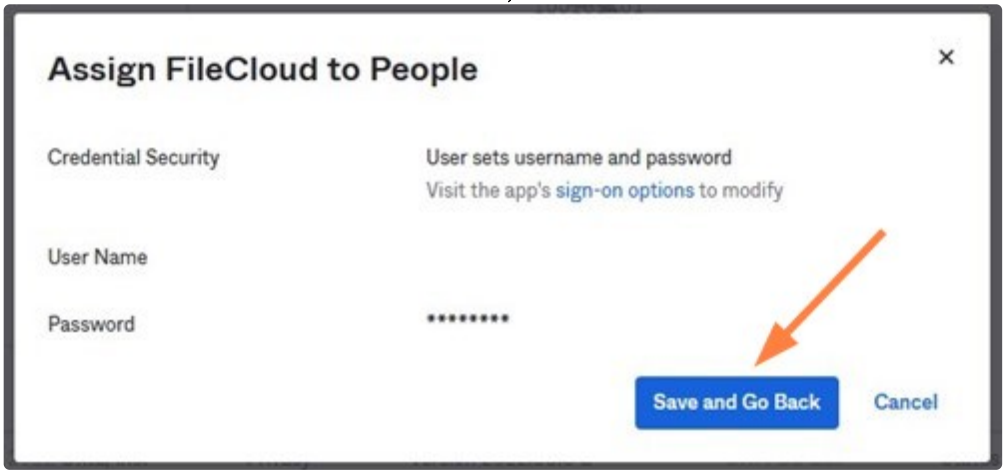
2. In the **Assign** drop-down list, choose **Assign to People**.



A list of users who have both Okta and FileCloud accounts opens.

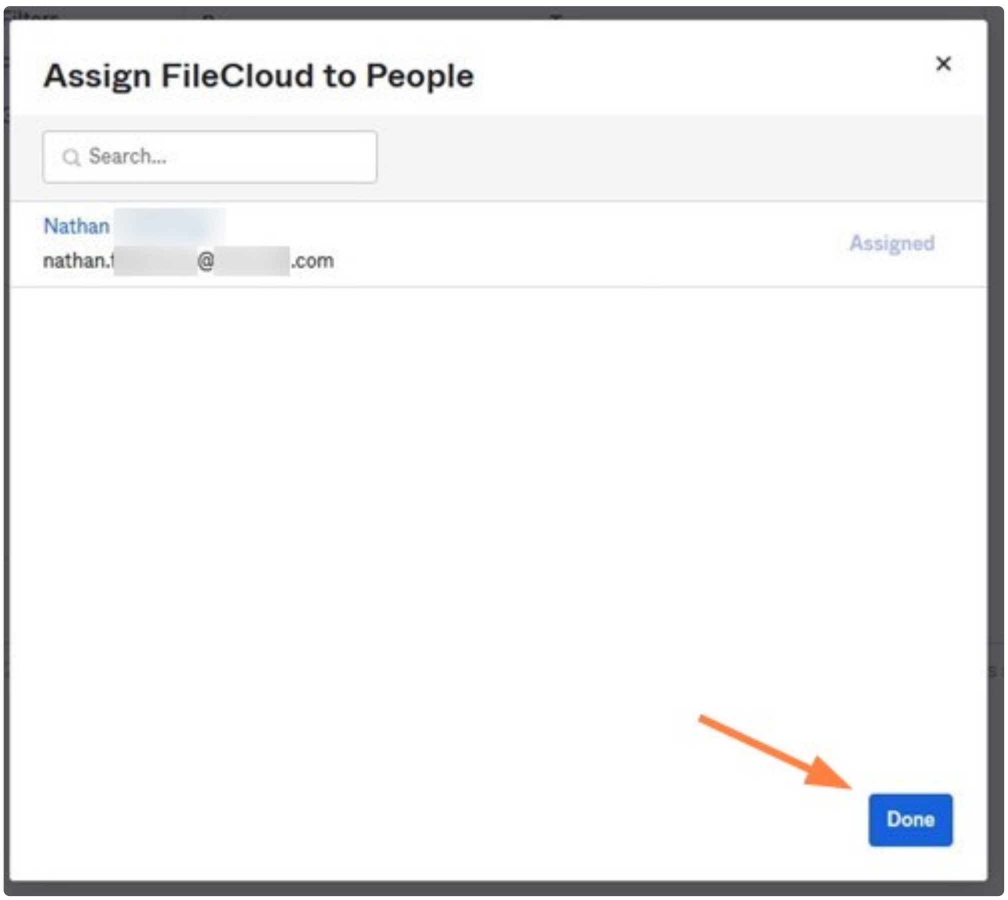
3. To allow users to sign in to FileCloud using Okta, click **Assign** in the row with their email.

4. Enter a **User Name** and **Password** for the user, then click **Save and Go Back**.



ck

5. Click **Done**.



6. Repeat this process for all users you want to assign to the integration.

Install the Plugin in the Browser

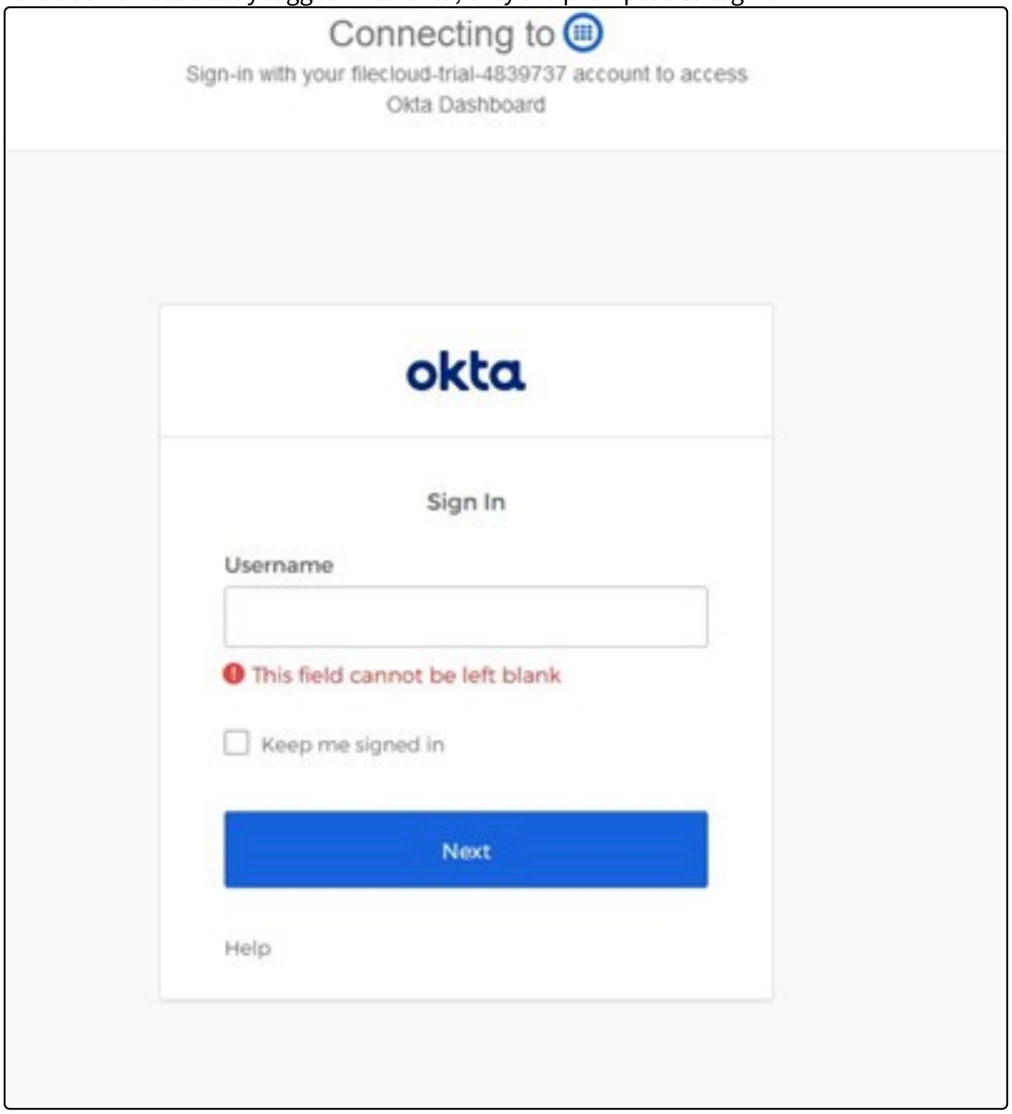
Information on plugin installation is available here:

https://help.Okta.com/en/prod/Content/Topics/Apps/Apps_Browser_Plugin.htm

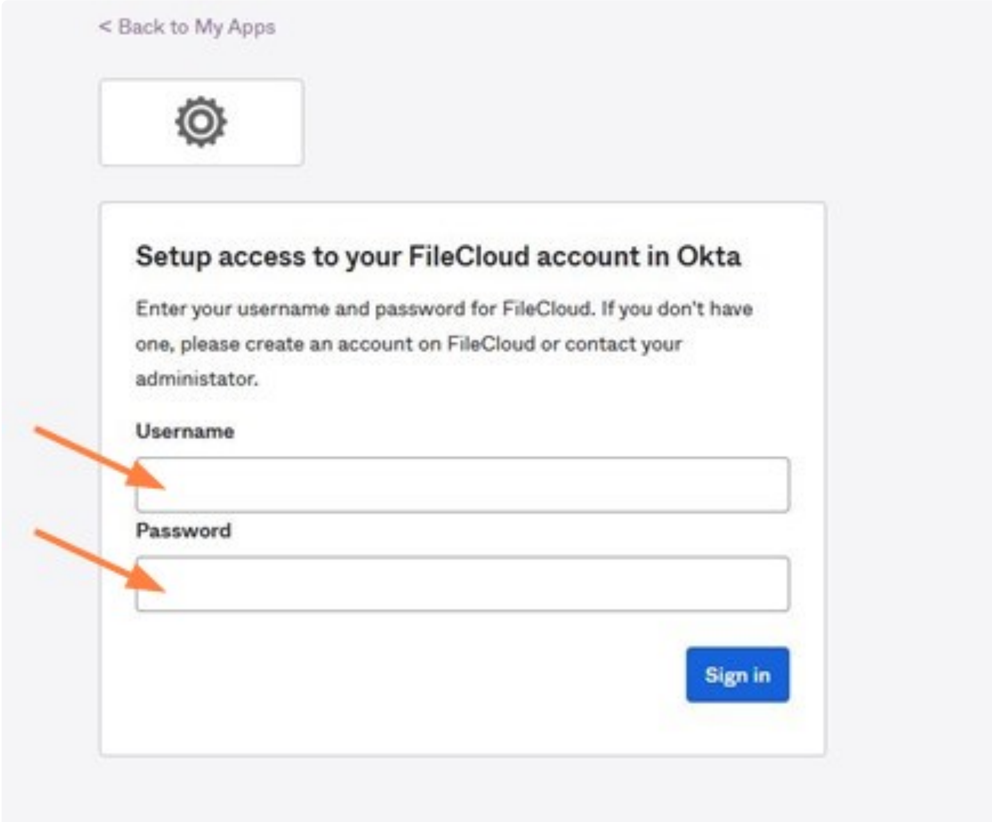
Users log in to FileCloud using the plugin

Users can sign in to the user portal or admin portal with SSO using the Okta plugin..

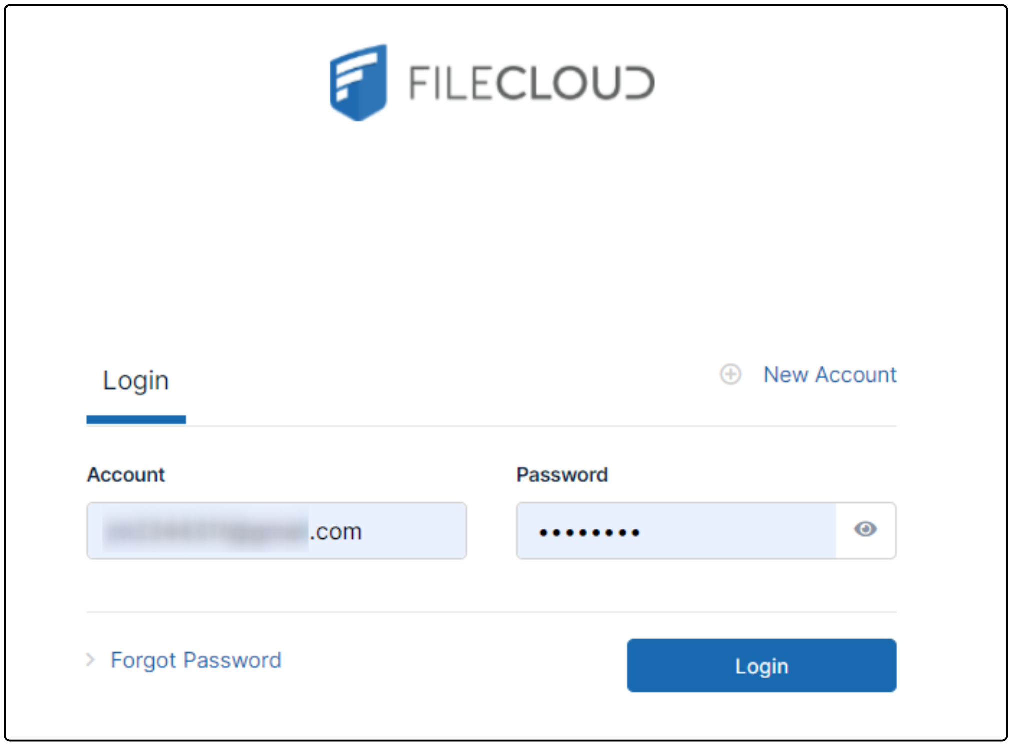
1. In a browser where the Okta Plugin is installed, the user clicks the Okta plugin icon, and selects the FileCloud application.
2. If the user is not already logged in to Okta, they are prompted to log in.



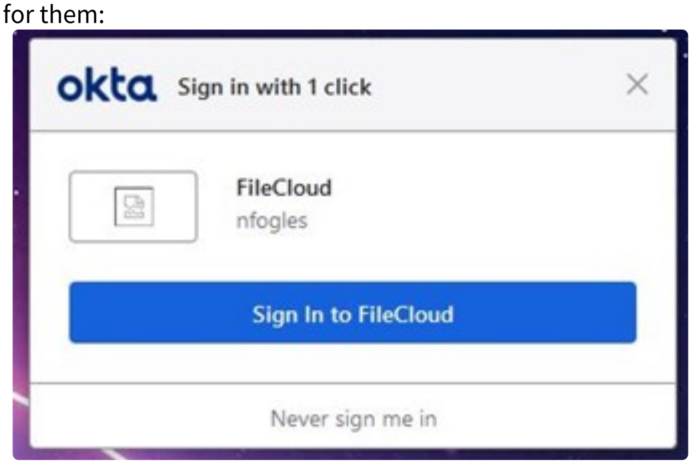
3. In the plugin **Setup access** dialog box, the user enters their FileCloud **Username** and **Password**. In the future, when they open the plugin, they will not be prompted to enter credentials again.



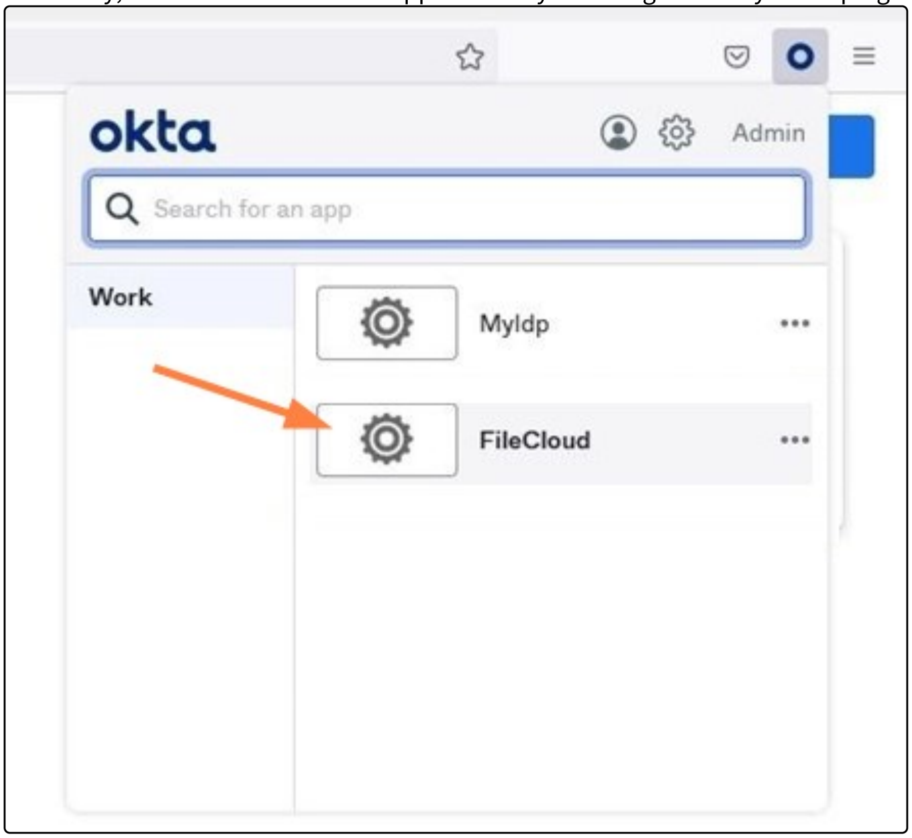
4. The browser redirects the user to the FileCloud login page in the Okta Admin Panel. The login screen with credentials filled in may appear first, and after a few seconds the FileCloud user portal should open (the user does not need to click **Login**).



Depending on the browser, when the user accesses the FileCloud login page again, the plugin may offer to log in for them:



Alternately, the user can access the application by choosing it directly in the plugin:



t

Integrate Google with FileCloud

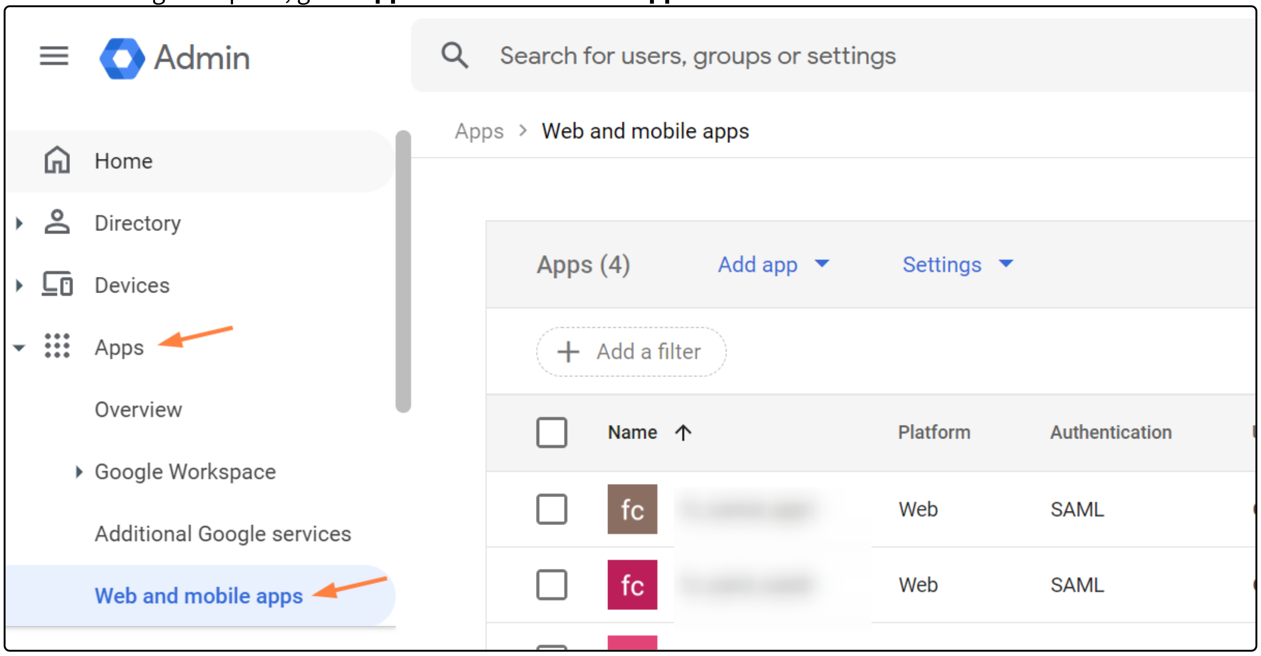
> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

As an administrator you can integrate Google and FileCloud so that your Google users can access their FileCloud account without having to enter their credentials a second time.

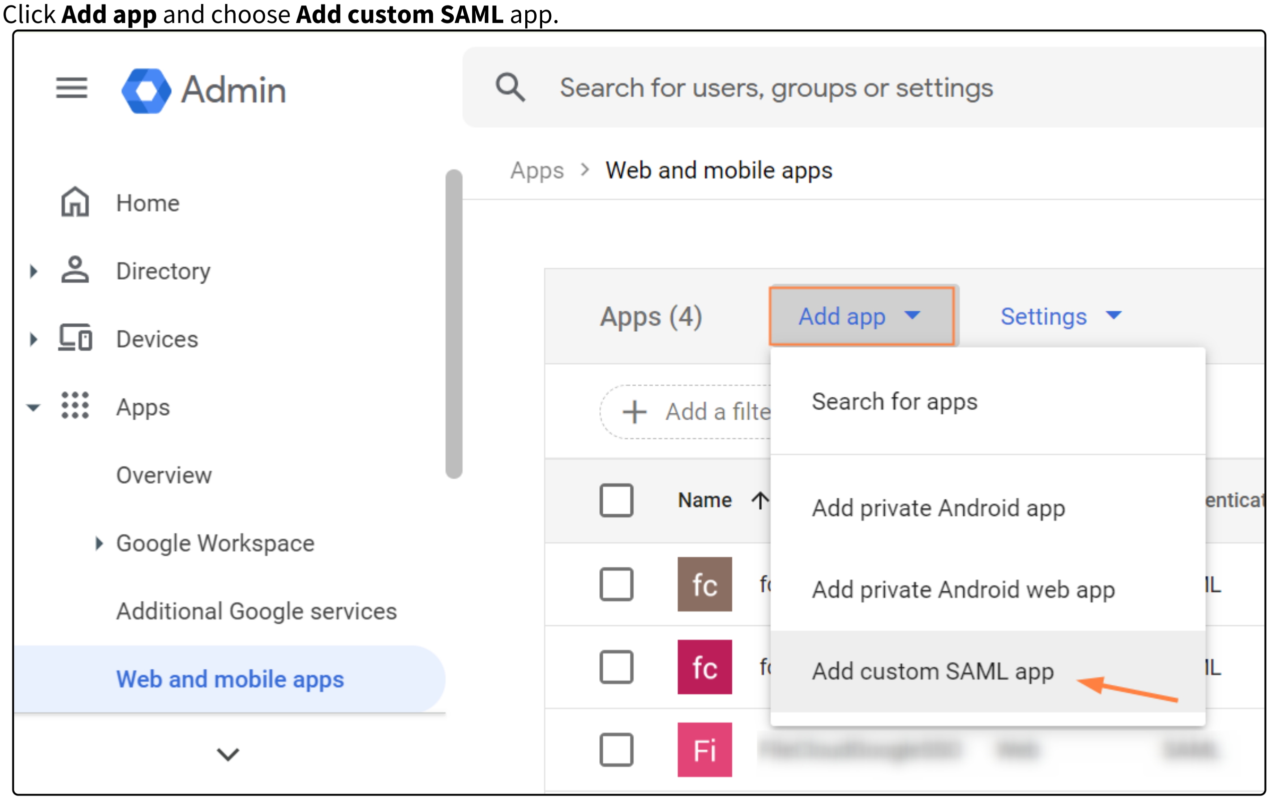
When FileCloud is integrated with Google, Google is configured as an Identity Provider (IdP) and FileCloud acts as the Service Provider (SP).

1. Log in to the Google Workspace Admin Center at admin.google.com.

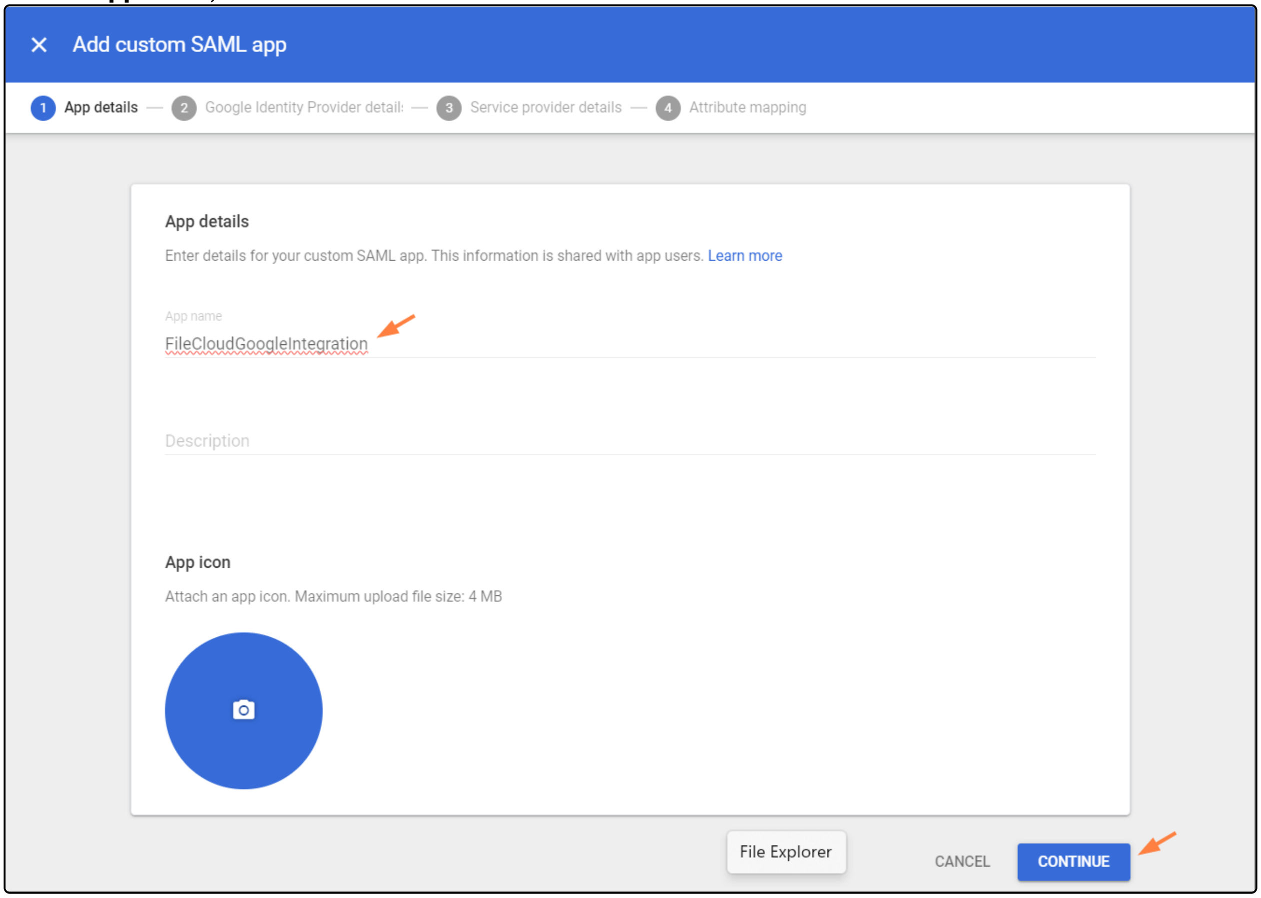
2. In the left navigation pane, go to **Apps > Web and mobile apps**.



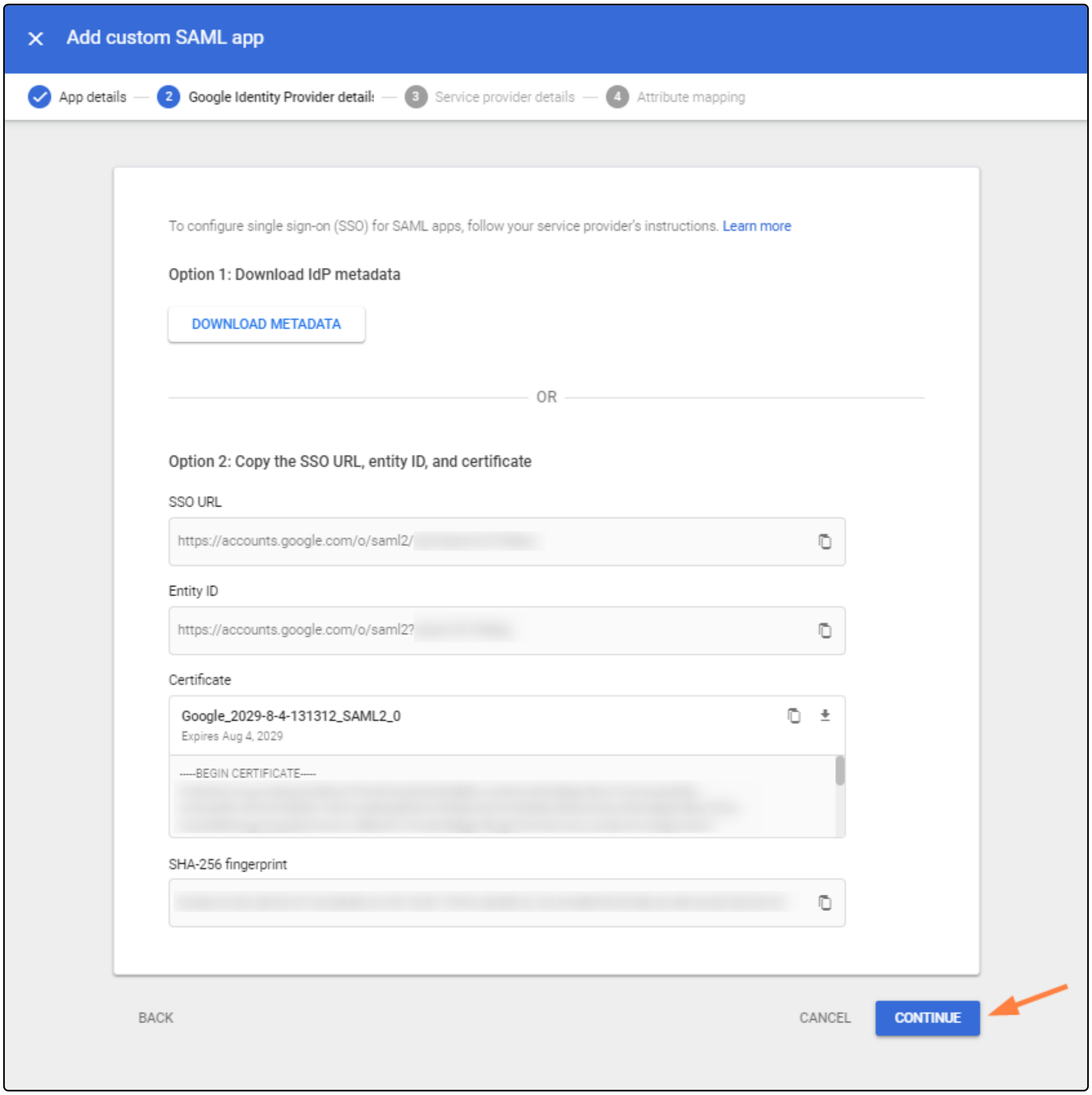
3. Click **Add app** and choose **Add custom SAML** app.



4. Enter an **App name**, and click **CONTINUE**.

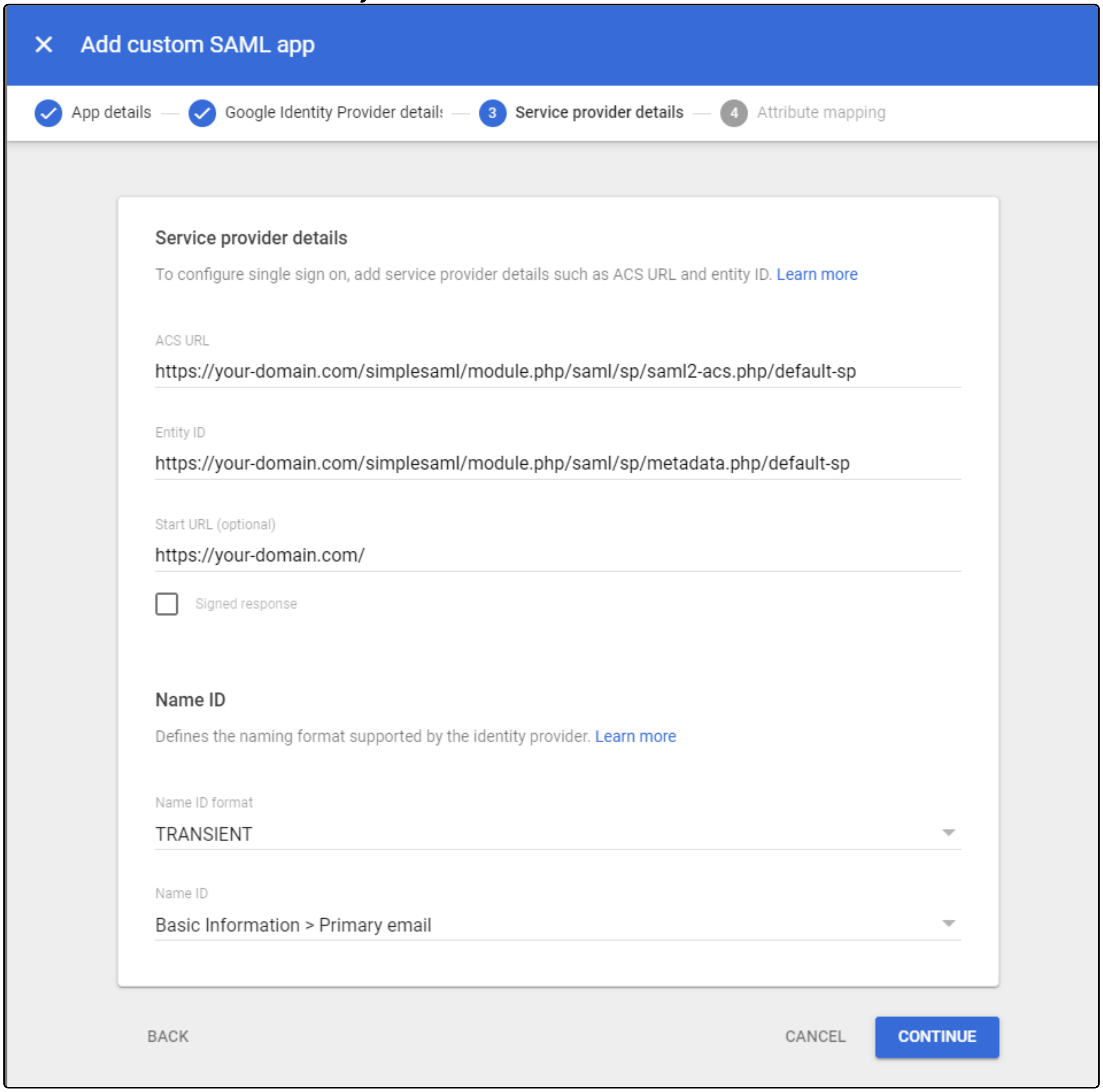


5. Click **CONTINUE**.

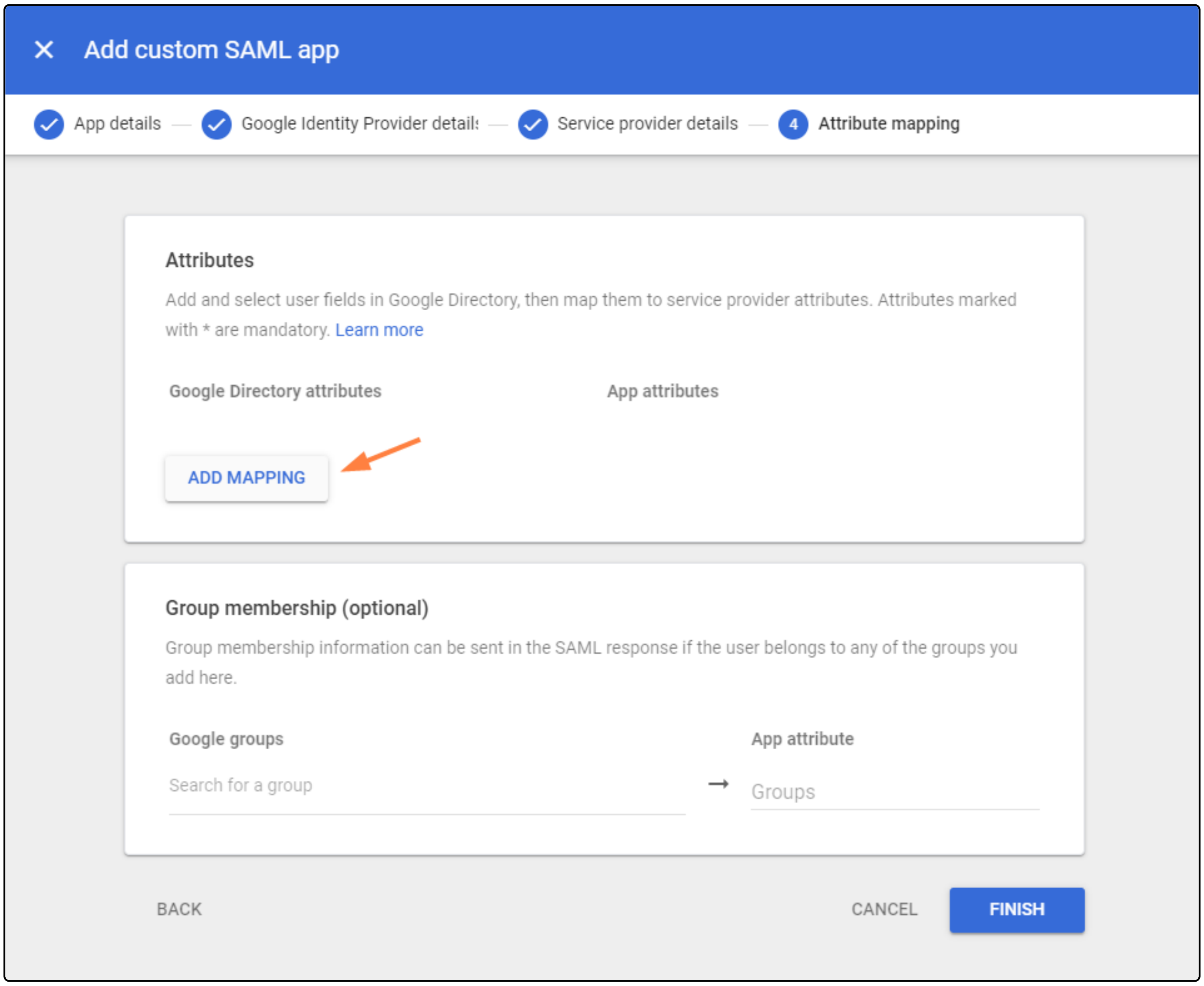


6. Fill in the fields as follows, replacing your-domain.com with your FileCloud domain. Click **CONTINUE**.
   ACS URL: https://your-domain/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
   Entity ID: https://your-domain/simplesaml/module.php/saml/sp/metadata.php/default-sp
   Start URL: https://your-domain/
   Name ID Format: **TRANSIENT**

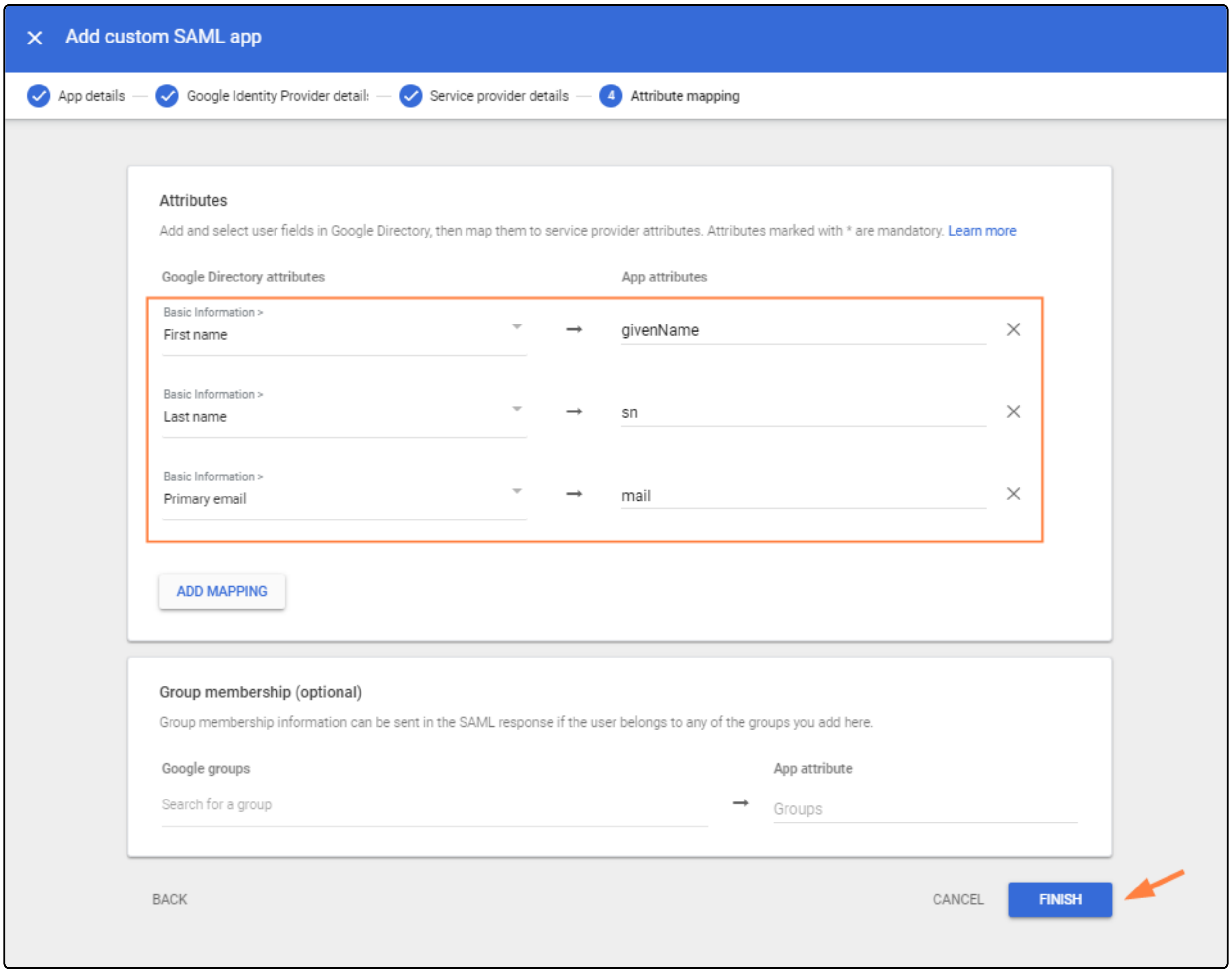
NameID: **Basic Information > Primary Email**



7. Click **ADD MAPPING**.

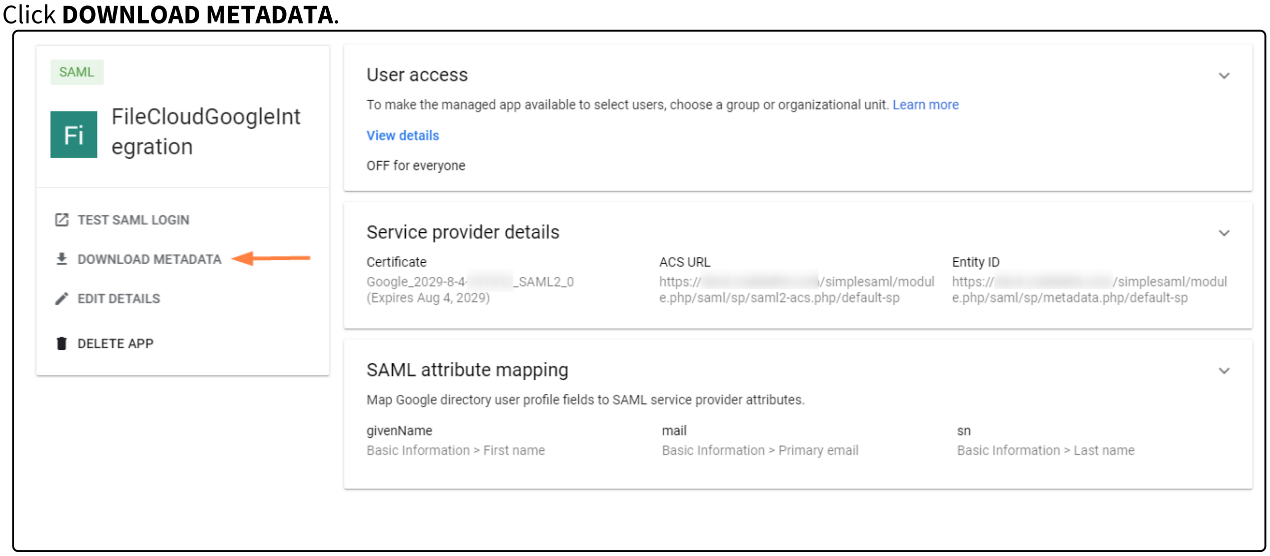


8. Choose the **Google Directory attributes** below, and add the specific values shown to **App attributes**. Then click **FINISH**.



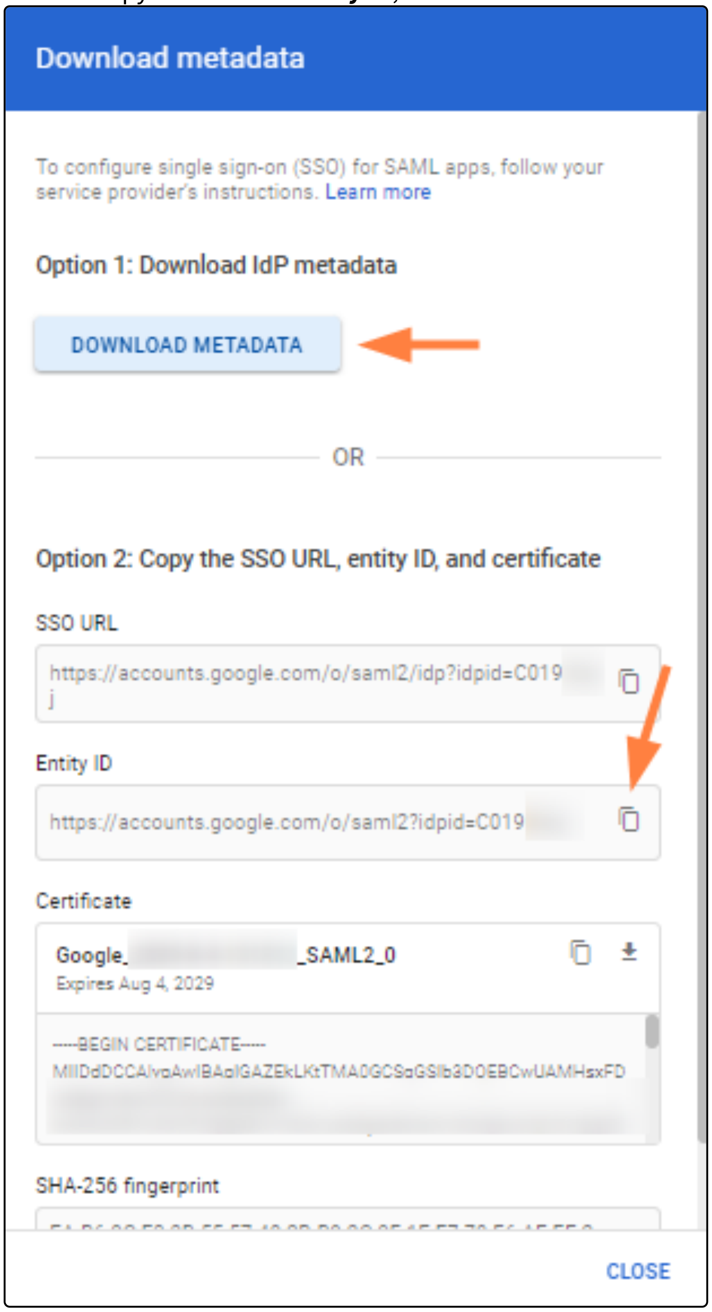
You should see a screen similar to the following.

9. Click **DOWNLOAD METADATA**.



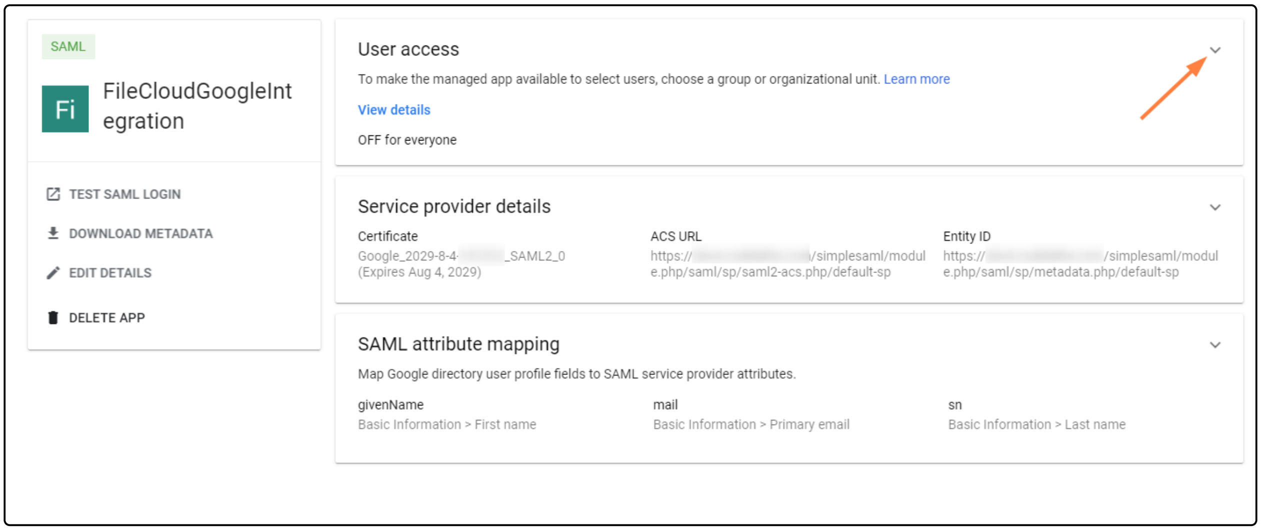
10. In the **Download metadata** popup, click **DOWNLOAD METADATA**.
    The file **GoogleIDPMetadata.xml** is automatically downloaded.

11. Click the copy icon next to **Entity ID**, and save it. You will need it to complete your configuration in FileCloud.

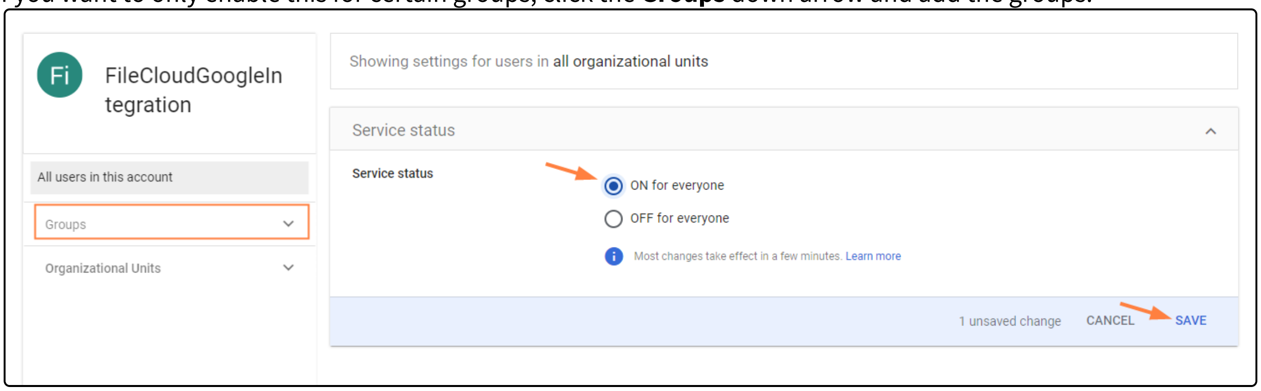


12. Click **CLOSE**.

13. Click the down arrow in the User access box.



14. Select **ON for everyone**.
    If you want to only enable this for certain groups, click the **Groups** down arrow and add the groups.

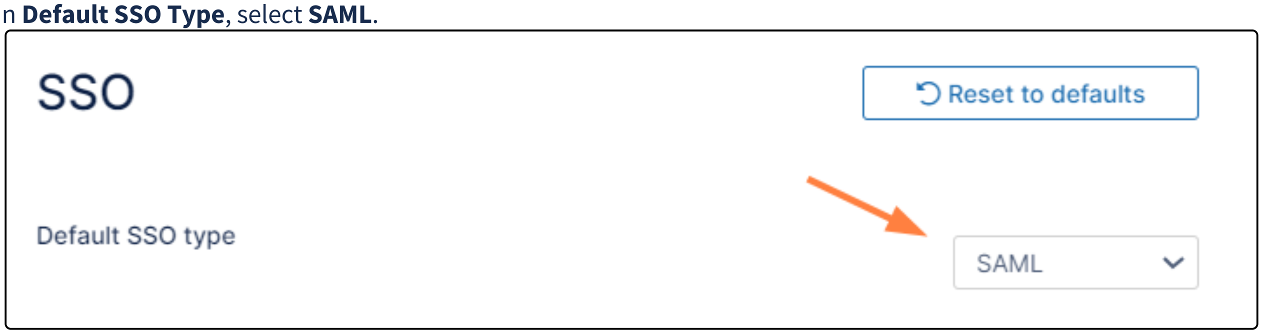


15. Click **SAVE.**

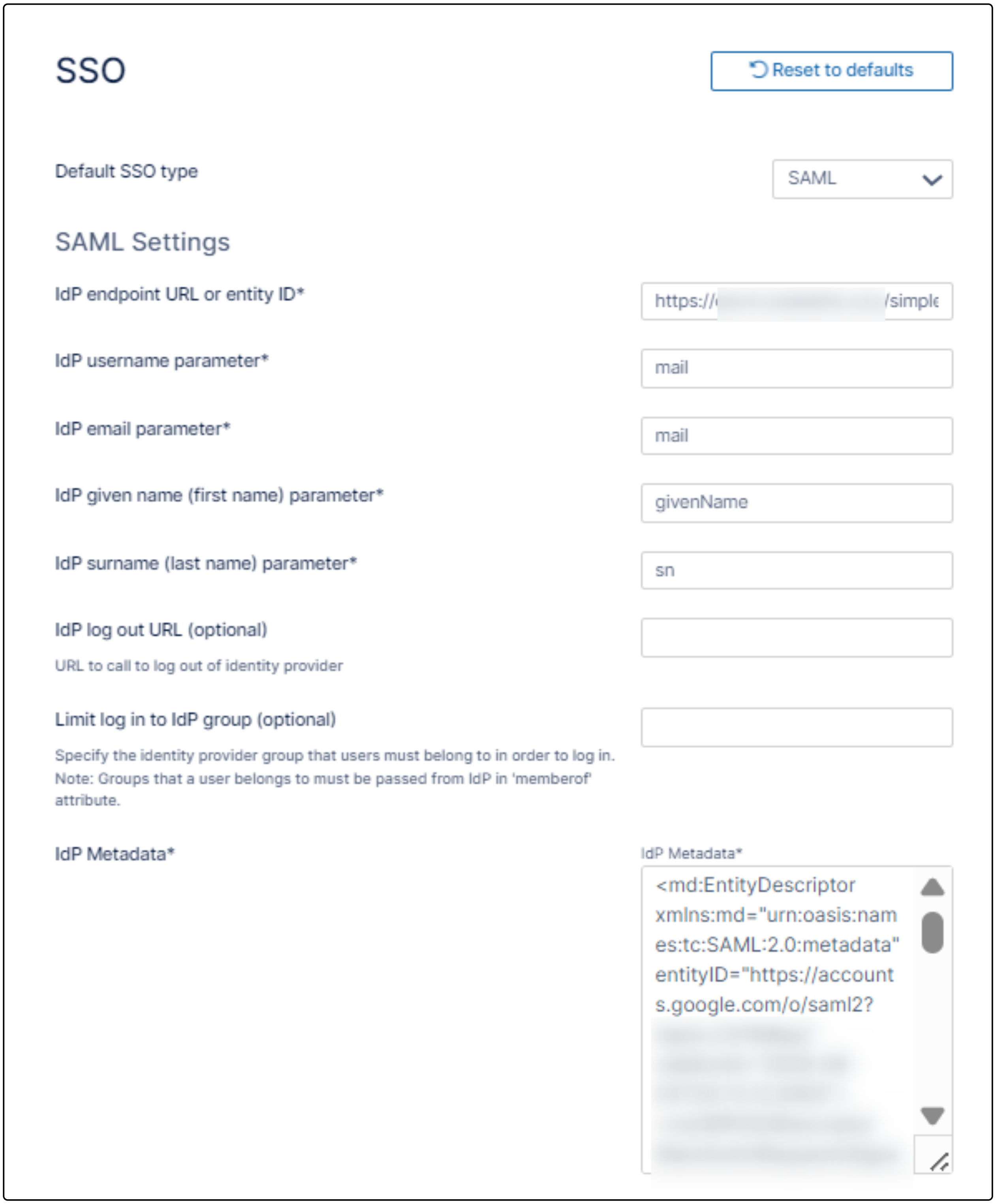
Configure Google SSO in the FileCloud admin portal

Now, add the values from your integration in the Google admin portal into the corresponding fields in FileCloud.

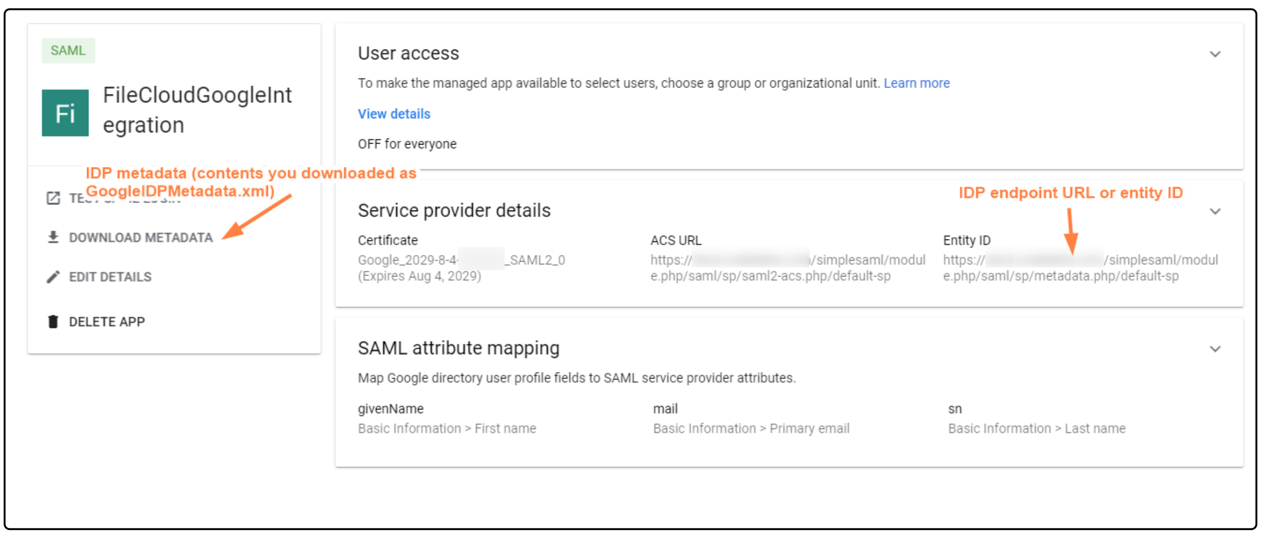
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. In **Default SSO Type**, select **SAML**.



3. Fill in the settings under **SAML Settings**. The table below the image shows what to enter in each required IdP value.



Setting	Value
IdP endpoint URL or entity ID	Enter the value of Entity ID from your Google/FileCloud app in the Google admin portal, See the image below.
IdP username parameter	mail
IdP email parameter	mail
IdP given name (first name) parameter	givenName
IdP surname (last name) parameter	sn
IdP log out URL	See SAML Single Sign-On Support
Limit log in to IdP group	See SAML Single Sign-On Support
IdP Metadata	Enter the content of the metadata file you downloaded from your Google/ FileCloud app in the Google admin portal. It should have been downloaded as GoogleIdPMetadata.xml.



4. For help filling the remaining settings on the page, see Step 4 on page SAML Single Sign-On Support.
5. To display the SSO option on the user login page, see Step 6 on page SAML Single Sign-On Support

Integrate OneLogin with FileCloud

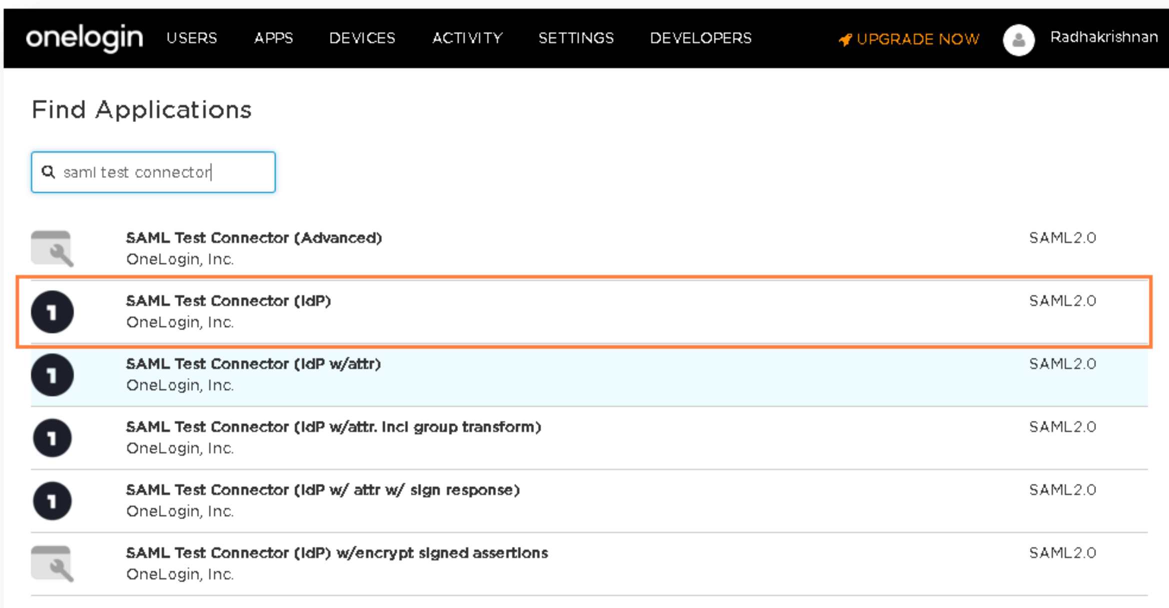
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

This article describes how to integrate OneLogin as an SSO provider with FileCloud.

Pre-requisite: The mcrypt module must be installed on FileCloud. In Windows, it should be installed by default. In Linux, if mcrypt is not installed, it must be installed

OneLogin: Create App Connector

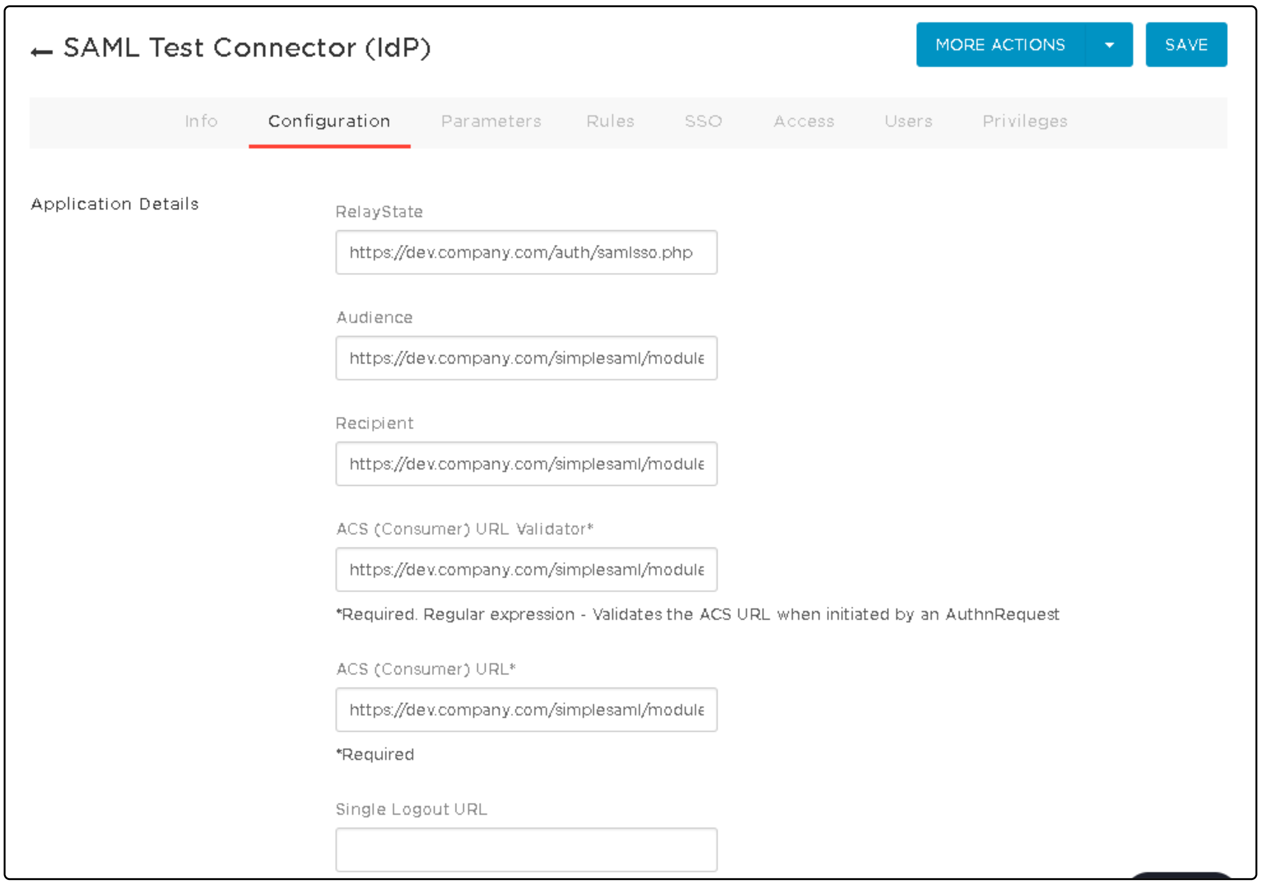
1. Login into the OneLogin web UI.
2. Click **Apps > Add Apps**.
3. Search for **SAML Test Connector** and select **SAML Test Connector (IdP)**.



4. In the add screen, enter a name for the connector. For example, something like **FileCloud Connector**.
5. Click **Save**.
6. Open the created connector and click the **Configuration** tab.
7. Fill the following values into the configuration tab. Replace **dev.company.com** with your FileCloud site.

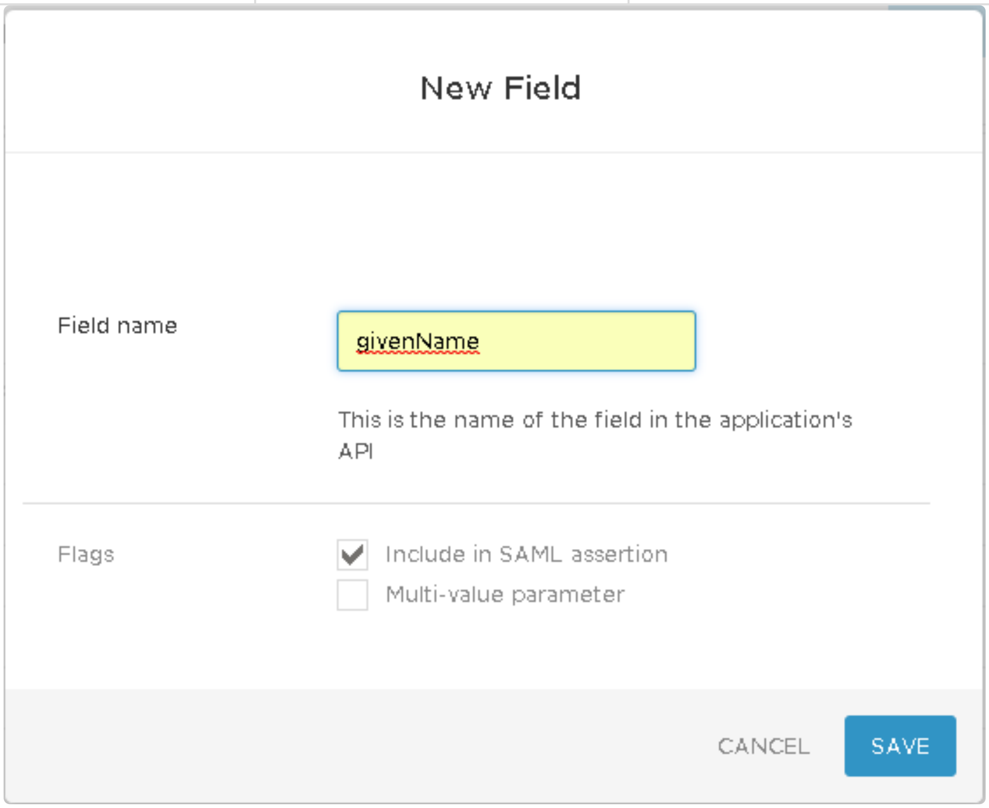
Configuration	Value
RelayState	https://**dev.company.com**/auth/samlsso.php

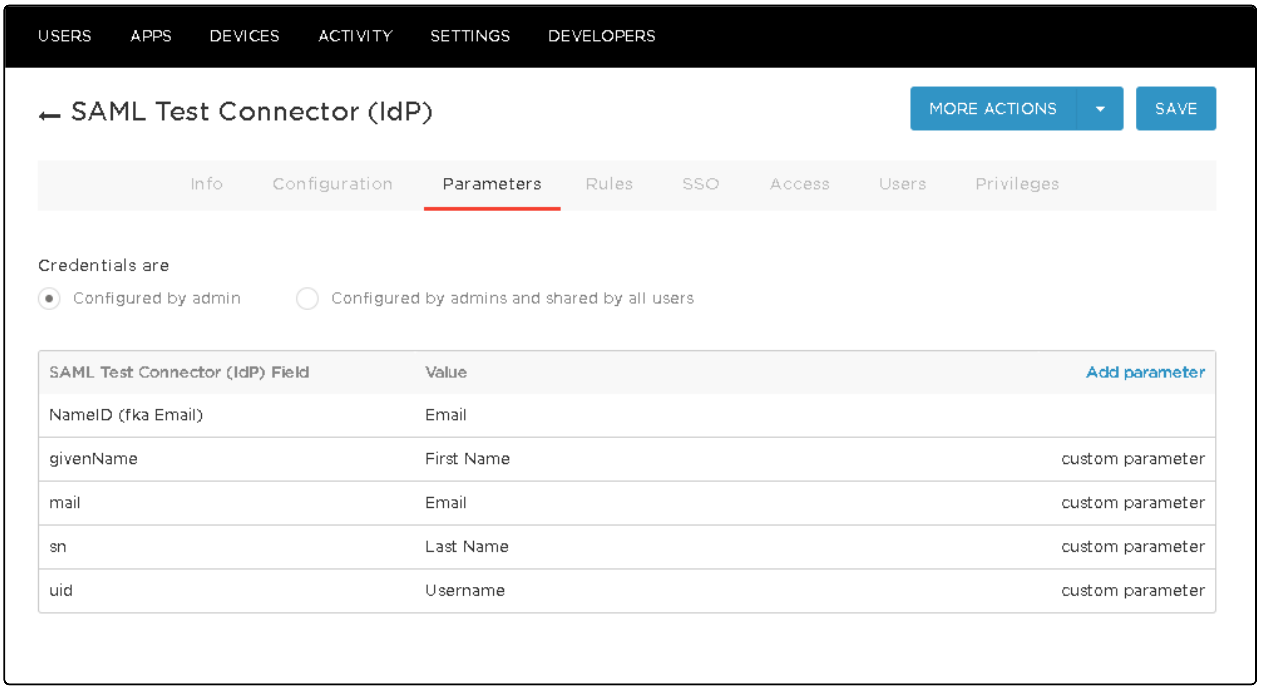
Configuration	Value
Audience	https://**dev.company.com**/simplesaml/module.php/saml/sp/metadata.php/default-sp
Recipient	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL Validator*	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL*	https://**dev.company.com**/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp



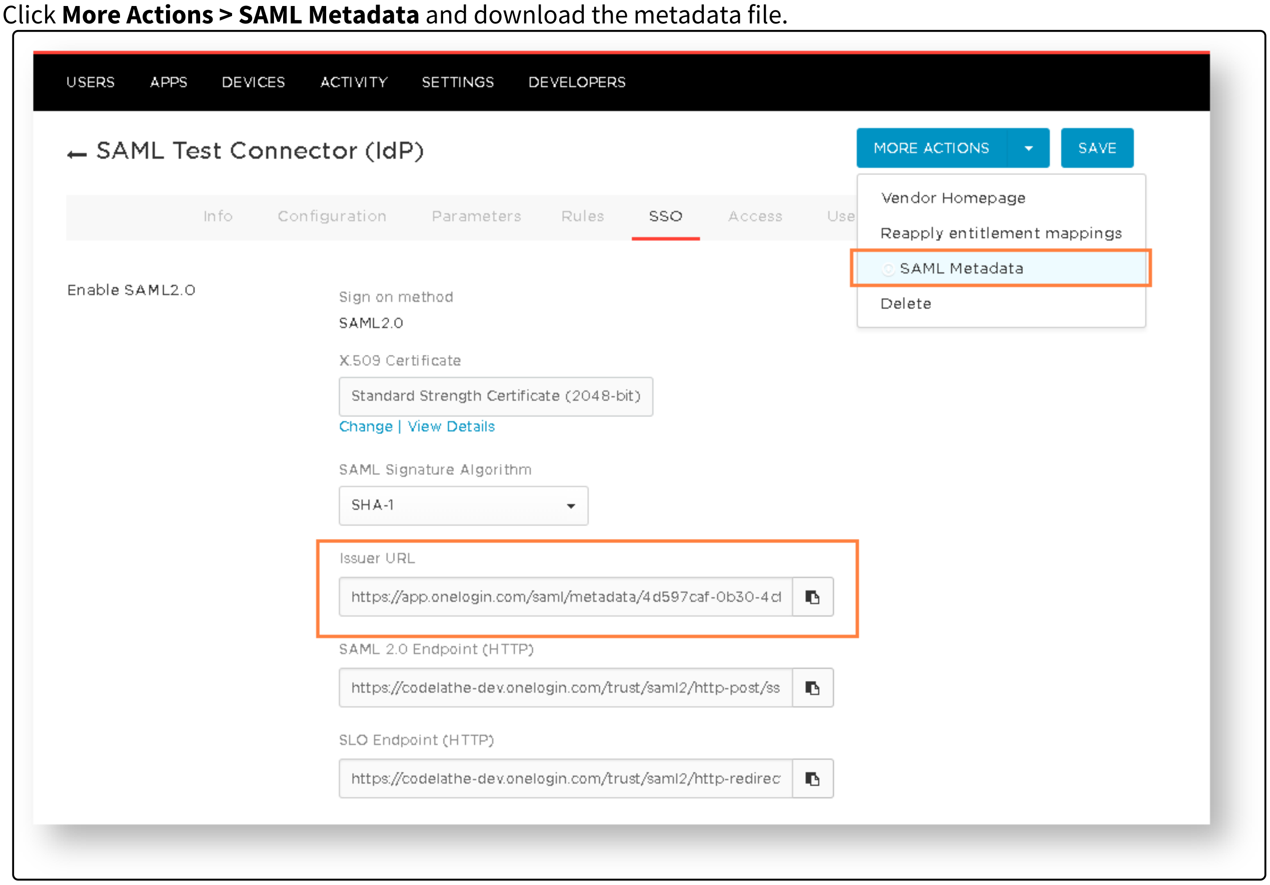
8. Once the configuration tab is completed, click the **Parameters** tab.
9. Add the following four parameters:

Field name	Flags	Value
givenName	Include in SAML assertion	First Name
mail	Include in SAML assertion	Email
sn	Include in SAML assertion	Last Name
uid	Include in SAML assertion	Username





10. Save these changes. Then click the **SSO** tab.
11. In the **SSO** tab, copy and save **Issuer URL**.
12. Click **More Actions > SAML Metadata** and download the metadata file.

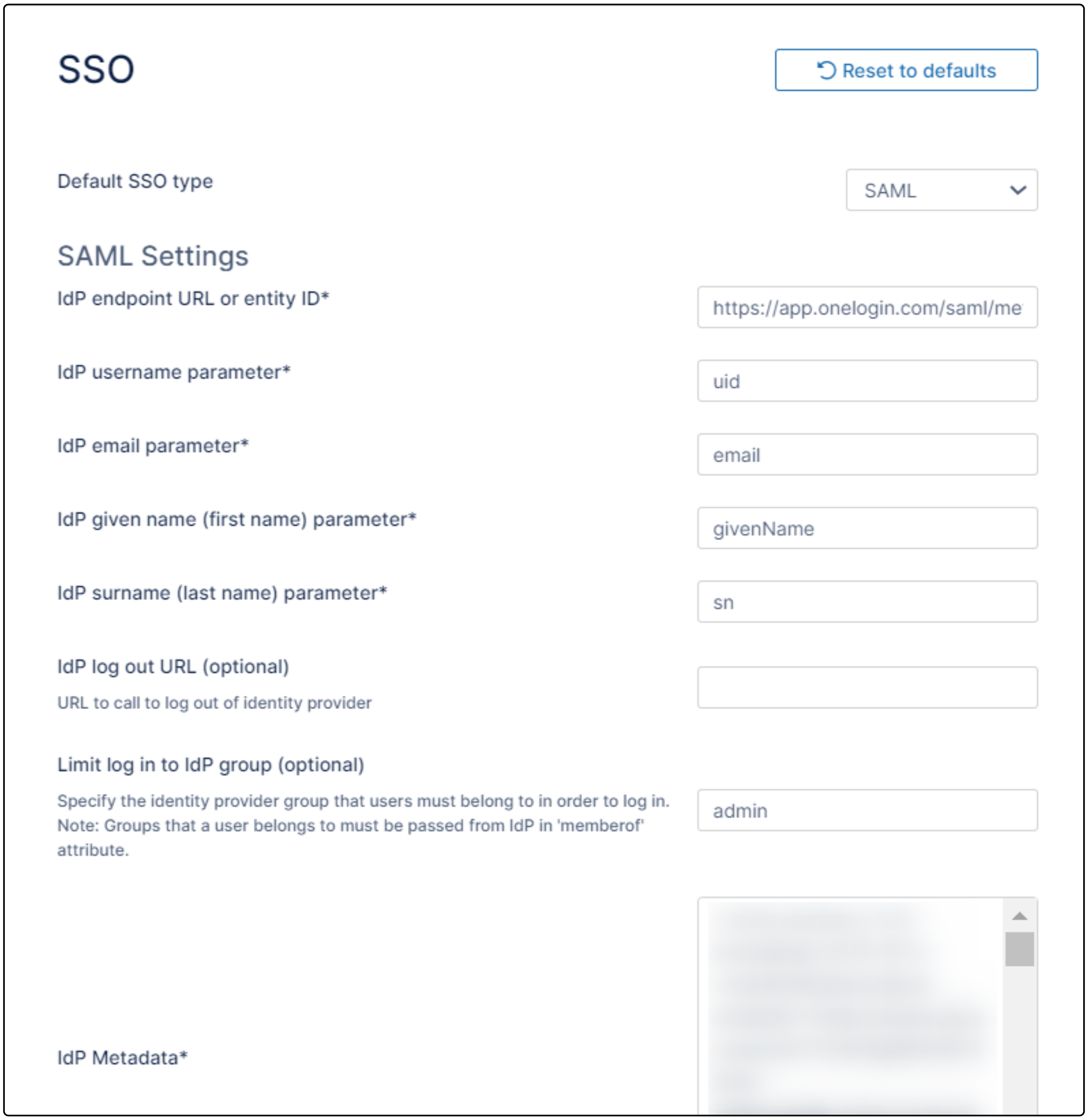


13. Finally, add users to the newly created FileCloud Connector either individually or as group.

Integrate FileCloud with OneLogin SSO

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. In **Default SSO Type** choose **SSO**.
3. Use the following table to fill in the SAML configuration.

SAML Settings	Value
IdP Endpoint URL	**Issuer URL** saved in the previous section from OneLogin SSO tab
IdP Username Parameter	uid
IdP Email Parameter	mail
IdP Given Parameter	givenName
IdP Surname Parameter	sn
IdP Metadata	Copy and the paste the contents of SAML metadata from OneLogin.



4. Save the changes.

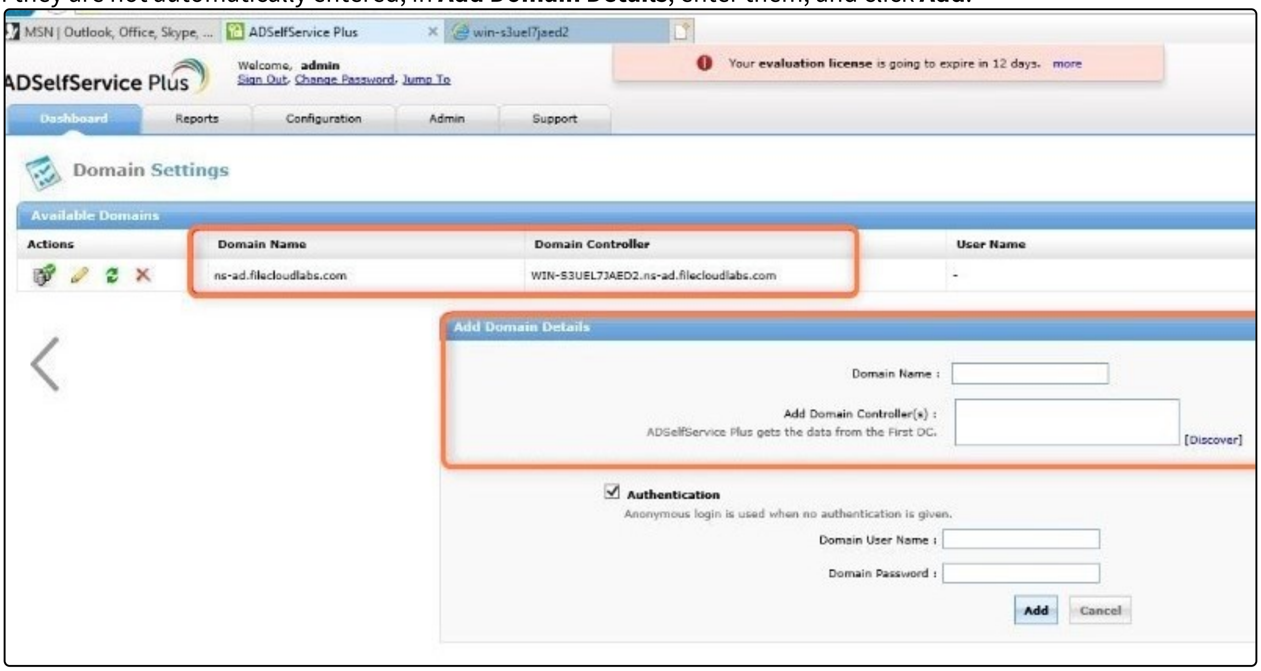
Integrate ADSelfService Plus with FileCloud

Integrate ADSelfService Plus with SimpleSAML SSO

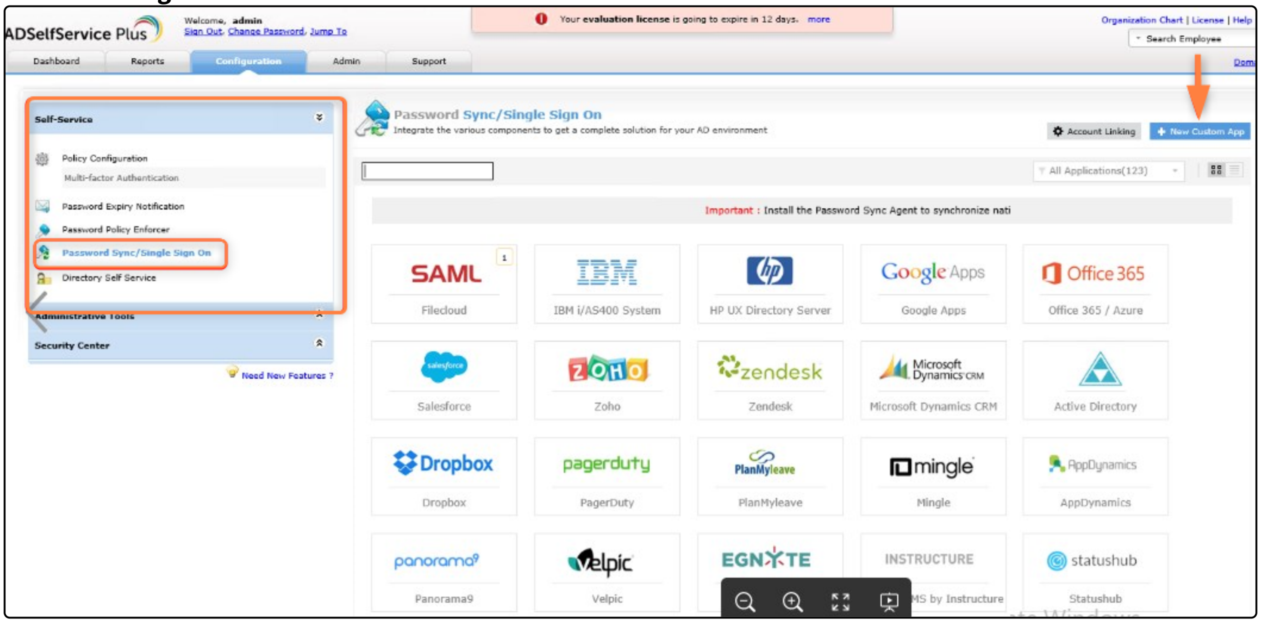
Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

Step 1: Install ADSelfService Plus and configure it to integrate with SimpleSAML SSO in FileCloud

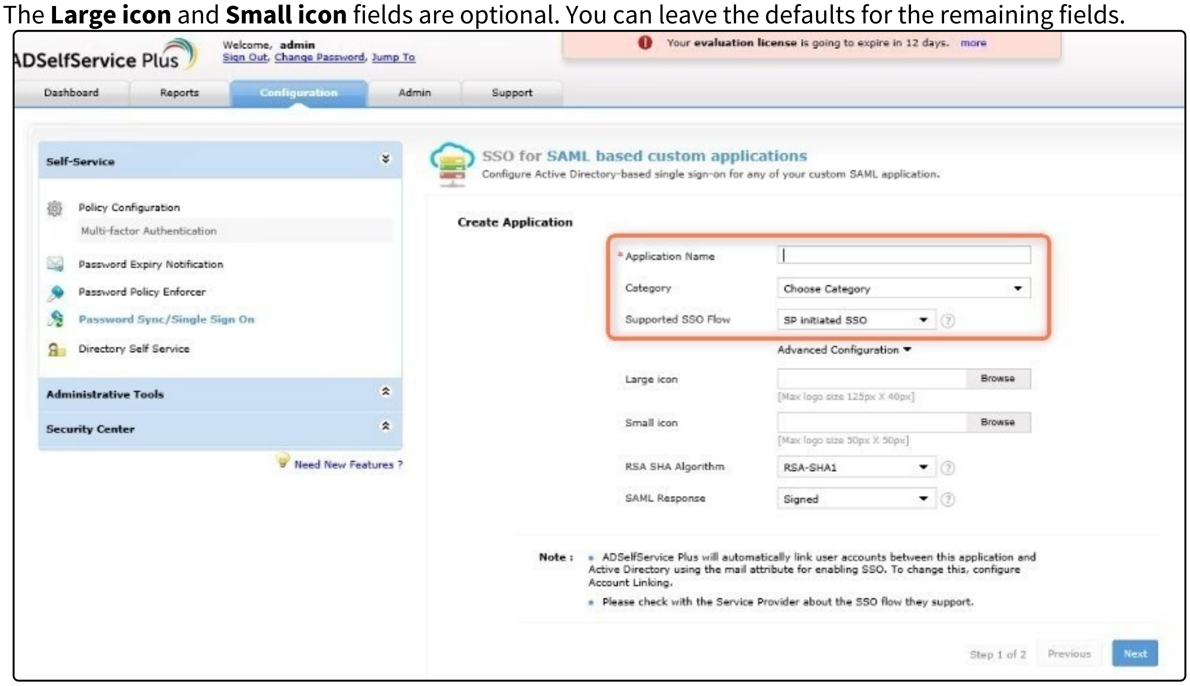
1. Install ADSelfService Plus.
2. Open the ADSelfService admin portal. Your URL should be similar to http://win-s3uexxjaed2:8888/authorization.do.
   The **Dashboard** tab should be selected, and the server name should be similar to: win-s3uexxjaed2
3. If AD is already installed, **Domain Name** and **Domain Controller** are automatically detected and entered for you. If they are not automatically entered, in **Add Domain Details**, enter them, and click **Add**.



4. Click the **Configuration** tab.



5. In the navigation bar, expand **Self-Service** and click **Password Sync/Single-Sign-On**.
6. Click **New Custom App**.
7. Fill in the following **Create Application** fields:
   a. In **Application Name** enter **FileCloud.**
   b. In **Category** drop-down list, choose any option.
   c. In the **Supported SSO flow** drop-down list,choose **SP initiated SSO.**
   The **Large icon** and **Small icon** fields are optional. You can leave the defaults for the remaining fields.



8. To go to the **SSO for SAML based custom applications/Configure Application** page, click **Next.**
9. Fill in the following **Configure Application** fields:
   a. In **Domain Name**, enter the domain name of your user's email address in AD.
   For example, if the email address is fc@test.com, enter test.com as the domain name.

b. In **Display Name** enter any name.
c. In **SAML Redirect URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/metadata.php/default-sp
d. In **ACS URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/saml2-acs.php/default-s

10. Click **Save**.
11. Click **Download SSO certificate** in the upper-right of the page.
    The **SSO/SAML Details** dialog box opens.

12. Click **Download Metadata file,** and save the metadata file (**metadata.xml**).

Step 2: In FileCloud, configure your SSO settings for ADSelfService Plus

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. In **Default SSO Type**, choose **SAML**.
3. Fill in the SAML settings:
   a. In **IDP Endpoint URL,**
      open the metadata.xml file you downloaded, and copy the URL after entityID. It should look similar to:
      entityID="http://yourFileclouddomainname:8888/iamapps/ssologin/custom_saml_10000/e6c2b84d31da852eac8e0f88ee5c4703b9974c2f
   b. In **IDP Username Parameter,** enter **mail.**
   c. In **IDP Email parameter** enter **mail**
   d. In **IDP Given Name Parameter** enter **givenName.**
   e. In **IDP Surname Parameter** enter **sn.**

f. In **IDP Metadata** paste the entire contents of the metadata.xml file.

> By default, ADSelfService Plus passes the **mail** attribute, and FileCloud creates the user from the username portion of the email address. For example, if the email is sam@fc.com, FileCloud creates an account with **sam** as the username.
> If you want to pass **userPrincipalName** as the parameter, contact the ADSelfService support team to make necessary changes in the database to pass that parameter. For example, to pass **userPrincipalName** instead of **mail**, ADSelfService must add the following entry to their database:
>
> ```
> "userPrincipalName":"uid"
> ```
>
> After they have added the entry, set **IDP Username Parameter** to **uid**.

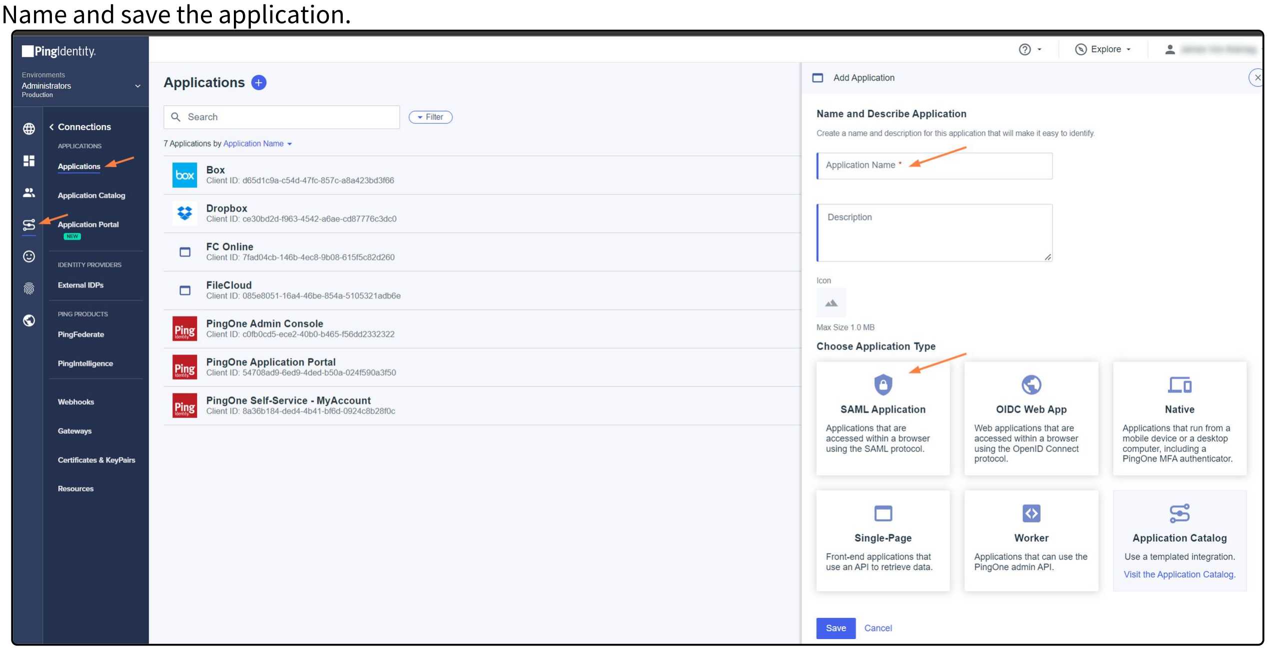
Integrate Ping Identity SSO with Filecloud

> Before completing the following procedures, configure Apache Web Server. See SSO Configuration Step 1 on the page SAML Single Sign-On Support for configuration instructions.

This article describes how to integrate PingOne as an SSO provider with FileCloud.

Configuration in Ping Identity portal

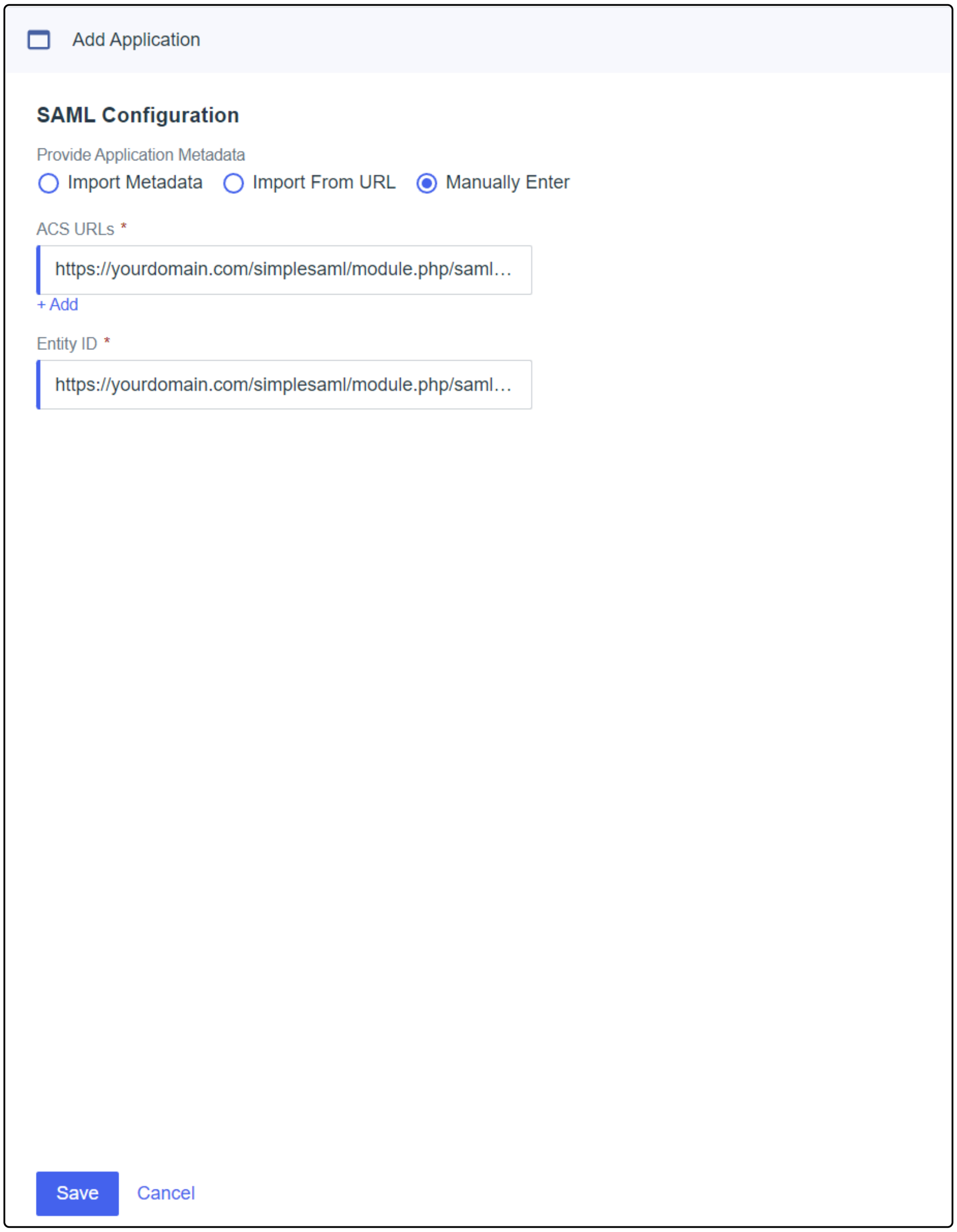
1. Log in to the Ping Identity dashboard, and click the **Connections** icon in the navigation panel.
2. Click **Applications**, then click the **+** button.
3. In the right panel, click **SAML Application**.
4. Name and save the application.



The **SAML Configuration** screen appears in the right panel.

5. Select **Manually Enter**, and fill in the fields as follows:
ACS URLs:
https://<your_filecloud_url>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

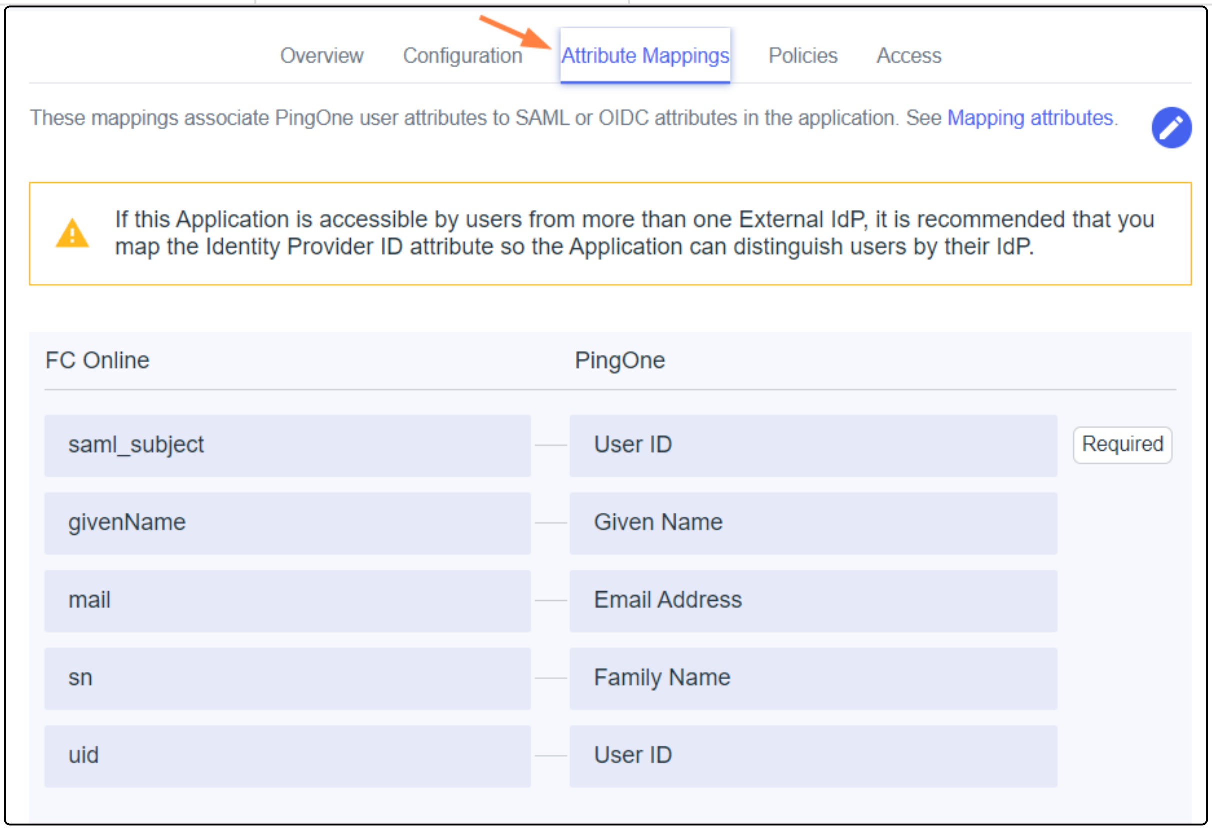
Entity ID:
https://<your_filecloud_url>/simplesaml/module.php/saml/sp/metadata.php/default-sp



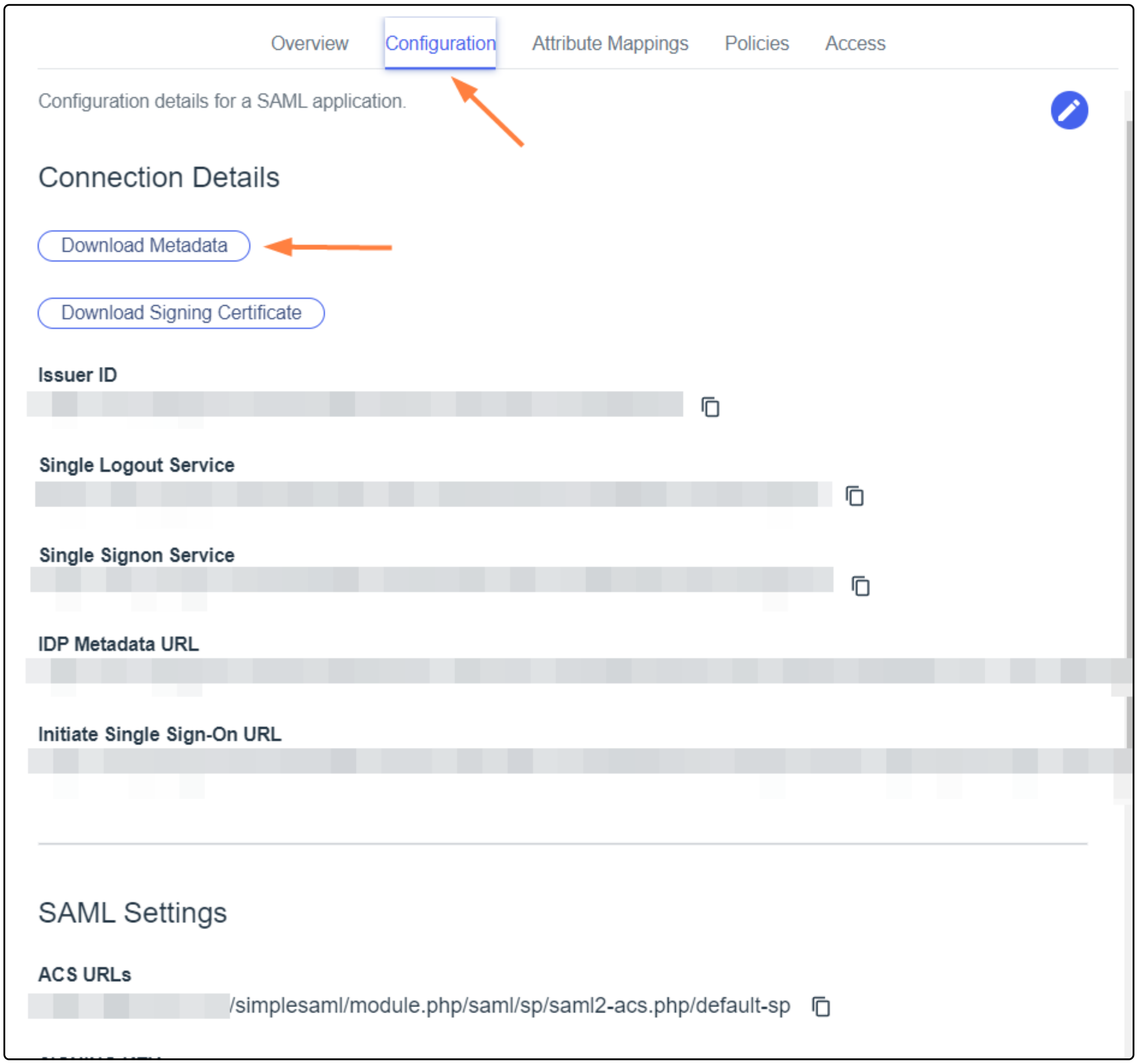
6. Click **Save**.
Several tabs appear in the right panel.

7. Select the **Attribute Mappings** tab, then click  , and add the following attributes:

Field name	Flags	Ping One Value
givenName	Include in SAML Assertion	Given Name
mail	Include in SAML Assertion	Email Address
sn	Include in SAML Assertion	Family Name
uid	Include in SAML Assertion	User ID



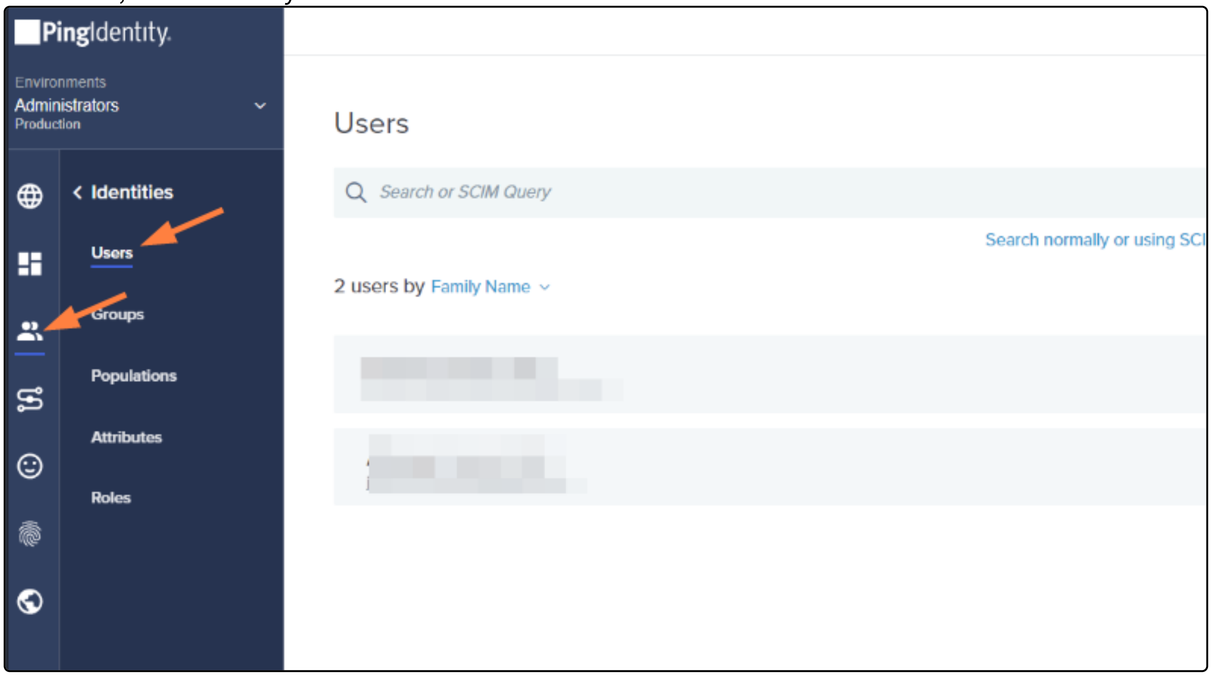
8. Click the **Configuration** tab.
9. To get a copy of the metadata file associated with the configuration, click **Download Metadata**. Save the file so you can enter its contents into the FileCloud admin portal.



Your application configuration is now complete.

10. Click the Identities icon in the Ping Identity navigation panel.

11. Click **Users**, and then add your users.

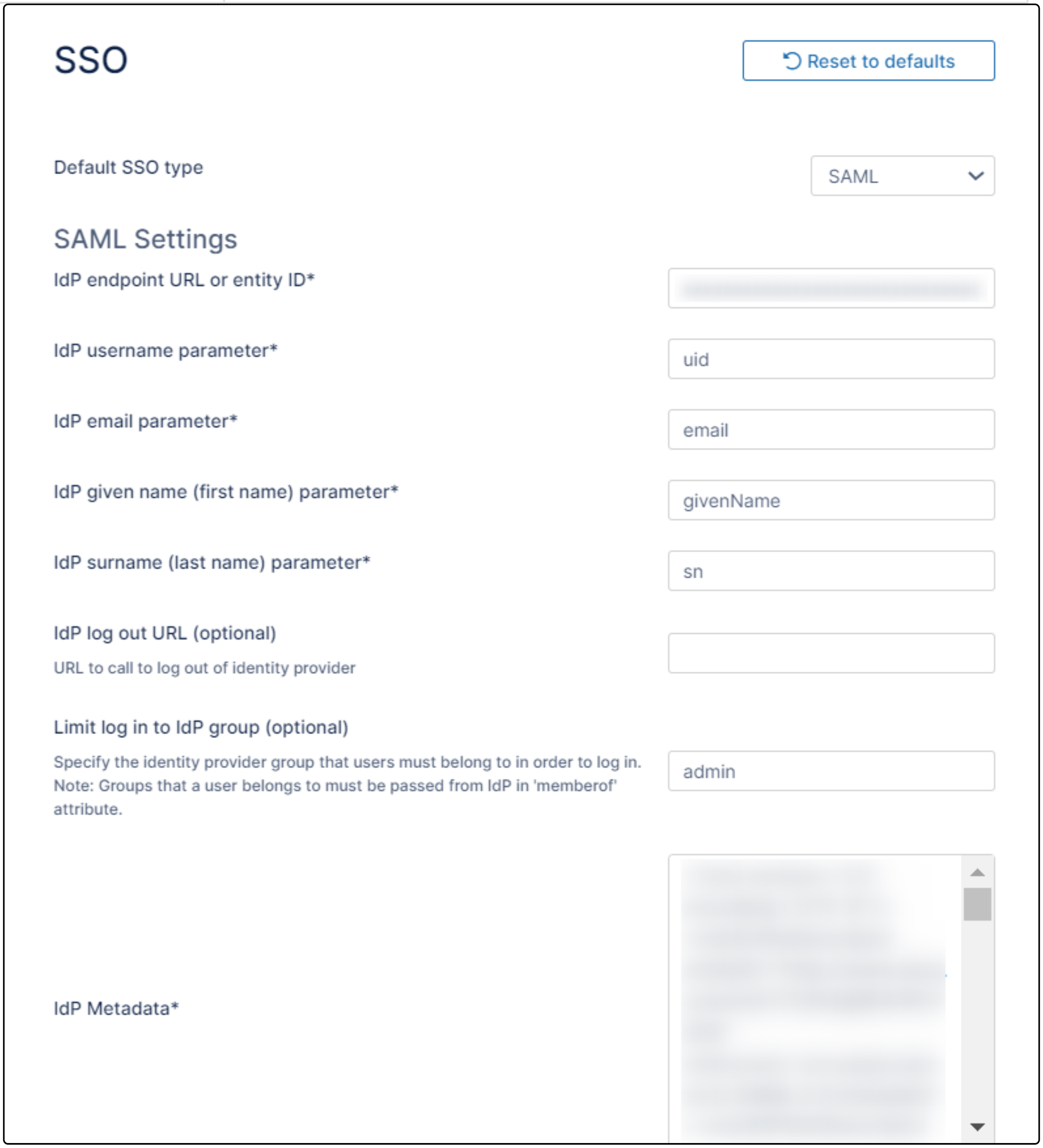


Configuration in Filecloud Admin portal

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. Enter the following information:

Field	**Value**
IdP End Point URL	Enter the value of **Issuer Id:** (Configuration tab → Issuer ID just below the "Download Metadata" button)
IdP Username Parameter	uid
IdP Email Parameter	mail
IdP Given Name Parameter	givenName
IdP Surname Parameter	sn

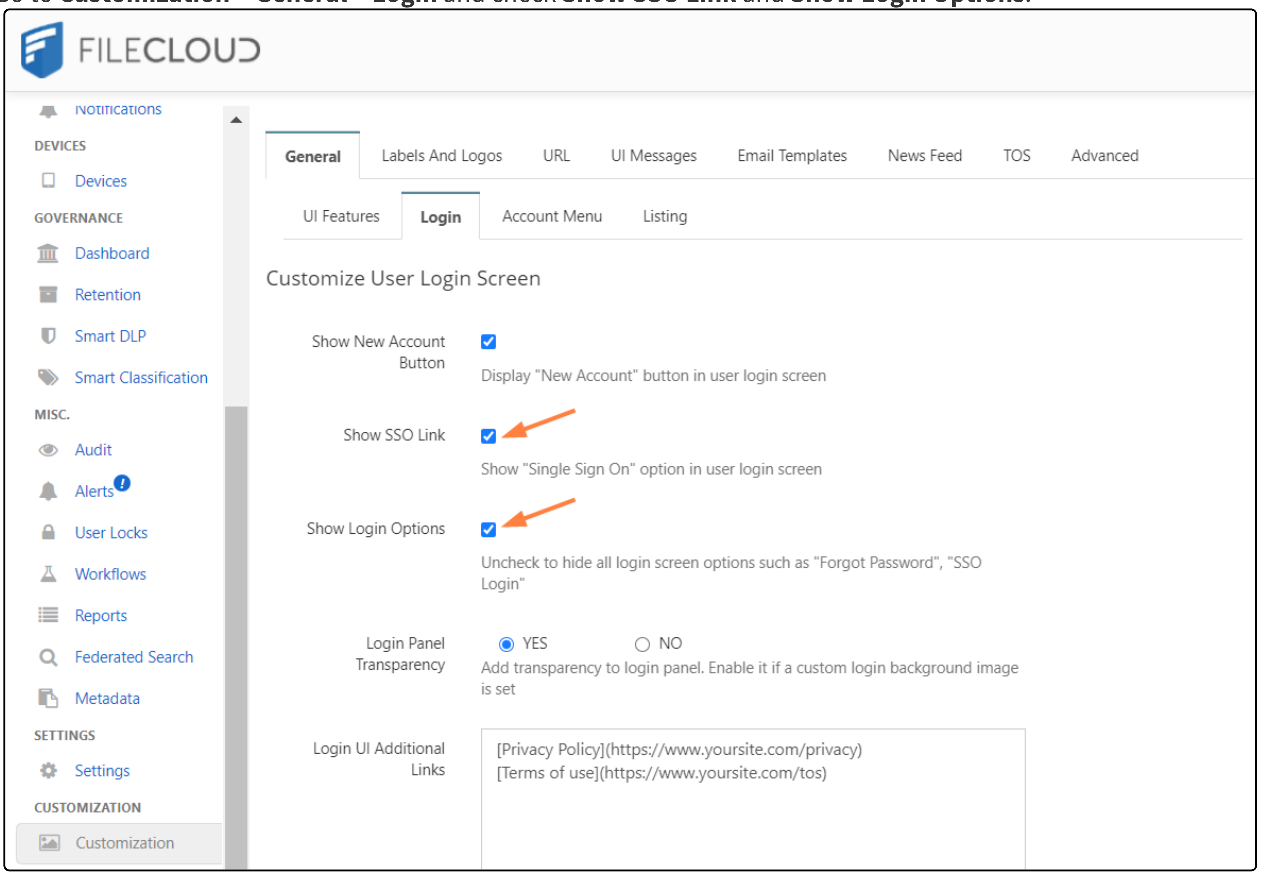
Field	Value
IdP Metadata	Copy the contents of the metadata file downloaded above paste them here.



3. If you want users to see the Ping Identity login after they click **Login with SSO**, scroll to the bottom of the screen and enable **Show the Idp Login Screen**.
   If you want users to be directly logged into FileCloud after they click **Login with SSO**, do not enable **Show the**

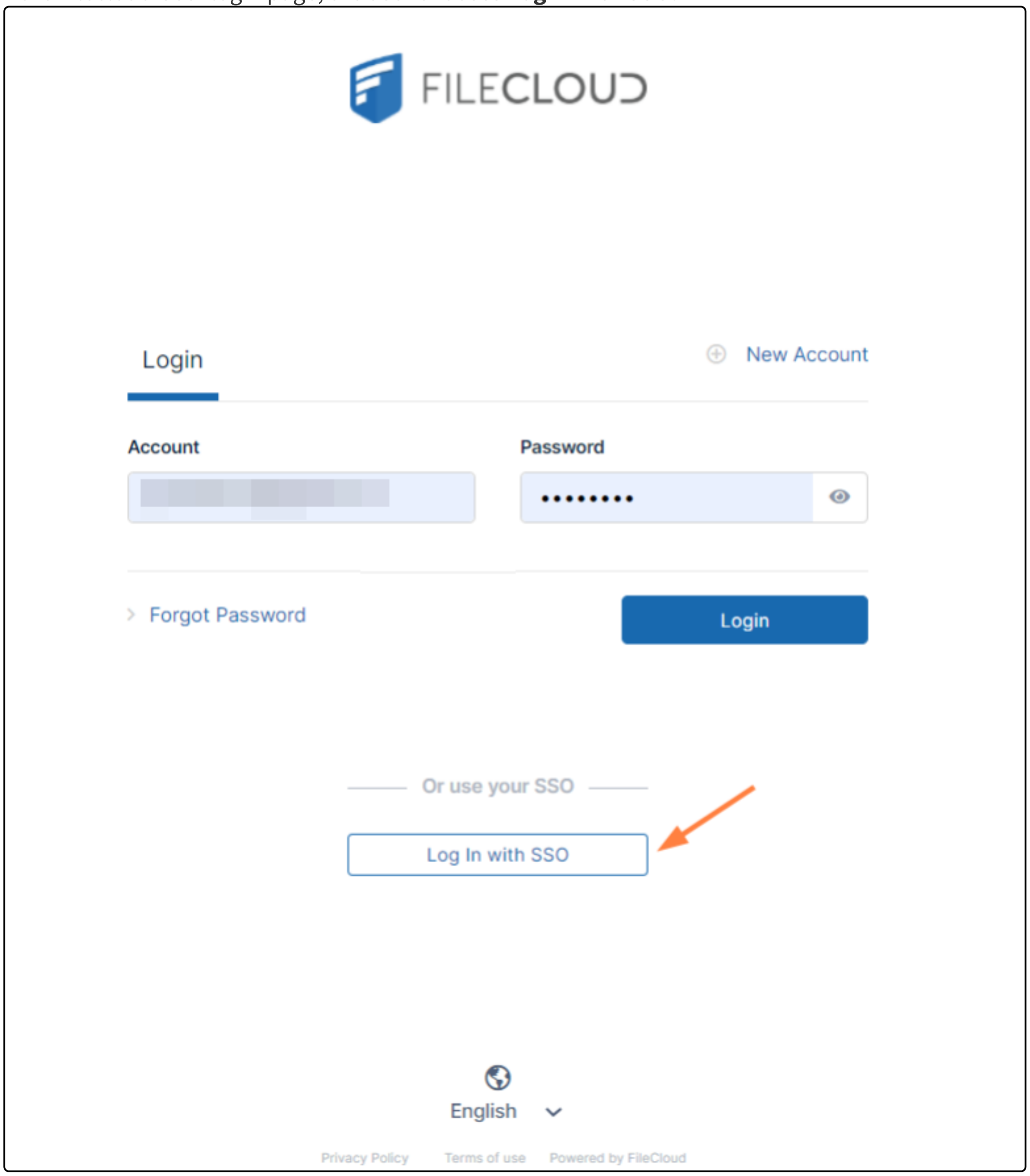
Idp Login Screen.

4. Fill in the other fields on the page as shown at SAML Single Sign-On Support.
5. Click **Save**.
6. Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.

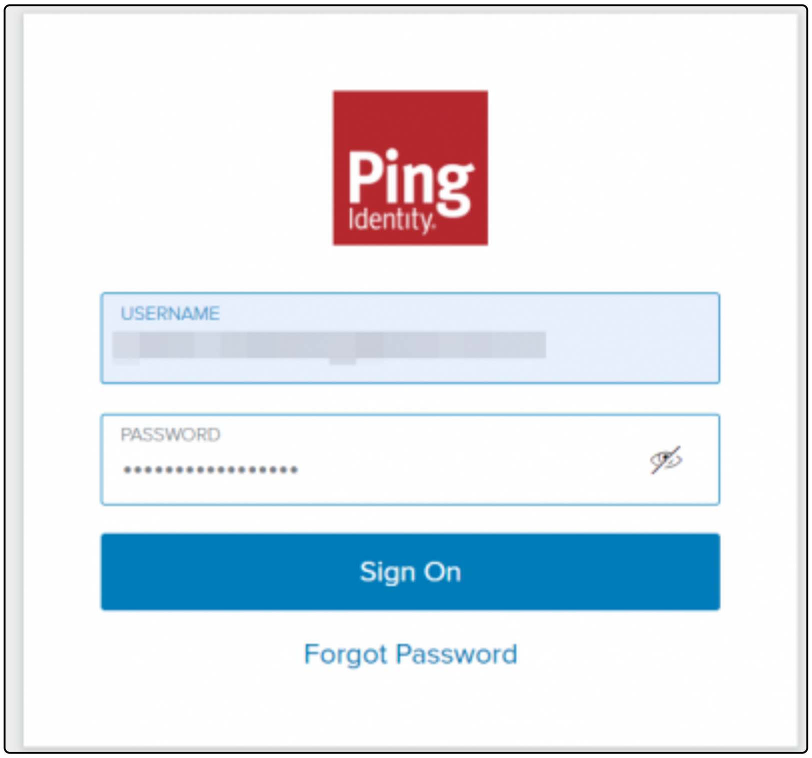


Log in to FileCloud using Single Sign-on with Ping Identity

1. In the Filecloud User login page, the user chooses **Login with SSO**.



If you have checked **Show the Idp Login Screen** in the FileCloud SSO settings, the user is redirected to the Ping Identity login screen, and must click **Sign On**.



Otherwise, the user is directly logged in to FileCloud.

Setting Up and Configuring Certificates when Upgrading SSO

When you upgrade SSO, please Contact FileCloud Support to avoid overwriting your current certificates with the default certificates sent with the library.

ADFS Single Sign-On Support

Introduction

FileCloud offers a SAML-based Single Sign-On (SSO) service that provides customers with full control over the authorization and authentication of hosted user accounts.

Using the SAML model, FileCloud acts as the **service provider** and also a **claims-aware application**. FileCloud customers that host FileCloud can authenticate against Active Directory Federation Services (ADFS) and log in to FileCloud.

FileCloud acts as a Service Provider (SP) while the ADFS server acts as the identity provider (IdP).

Active Directory Federation Services (ADFS) Support

When SAML SSO Type is selected and ADFS is enabled in FileCloud, FileCloud accepts claims in the form of ADFS security tokens from the Federation Service, and can use ADFS claims to support Single Sign-On (SSO) into FileCloud.

To specify the identity claims that are sent to the FileCloud refer to the IdP Configuration section below.

Prerequisites

- A Working ADFS implementation. This is beyond the scope of FileCloud. Please refer to articles available on the internet on setting up ADFS.
- FileCloud must be running on HTTPS using SSL. (Default self-signed SSLs that ship with FileCloud do not work). ADFS does not allow adding a relying party that is running on HTTP or self-signed SSL. For help setting up SSL in FileCloud, please Contact FileCloud Support.

FileCloud SSO Configuration Steps

In order to successfully configure SSO:

1. Configure Apache Webserver.
2. Set SAML as a the default single sign-on method in FileCloud and configure IdP settings.
3. Enable single sign-on link on the login page.
4. Register FileCloud as a service provider (SP) with IdP by adding FileCloud as a Relying Party Trust in ADFS.

Step 1: Apache Web Server Configuration

Follow the steps in SAML Single Sign-On Support to set up the Web Server configuration and enable SSO.

Step 2: Set SAML as the default SSO method and configure IdP/ADFS

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **SSO**  .
   The **SSO** page opens.
2. Set **Default SSO Type** to **SAML**.
3. Set the other fields as specified in the following table.

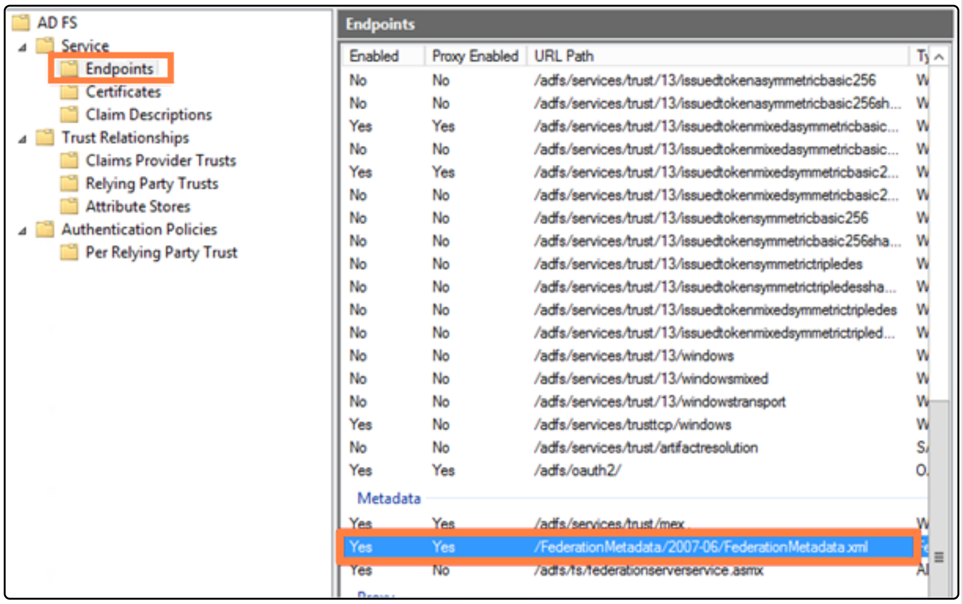
FileCloud Parameters	**ADFS as IdP** **Data can be obtained from Federation Metadata**	
Default SSO Type	For ADFS, select SAML	
IdP End Point URL	Identity Provider URL (Entity ID) e.g. http://yourADFSdomainName/adfs/services/trust	

IdP Username Parameter	Identifies the Username (must be unique for each user) Usually SAMAccountName or User Principal Name defined in claim rules. **NOTE: The username must be unique**. If username sent by Idp is in email format, the email prefix will be used for username. The email prefix in this case must be unique. value: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn or upn <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="UPN" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP Email Parameter	Identifies the email of the user (must be unique) http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or emailaddress <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="E-Mail Address" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP Given Name Parameter	Identifies the given name of the user. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname or givenname <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Given Name" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP Surname Parameter	Identifies the surname of the user http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname or surname <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Surname" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />	
IdP Log Out URL (Optional)	URL for logging out of IdP **Note:** For this setting to be effective, request that FileCloud Support add the corresponding setting to your FileCloud configuration.	

<table>
<tr>
<td>Limit Logon to IdP Group (Optional)</td>
<td>IdP Group Name

Specifying a group name means that a user can log in through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group
The IdP must send this group name through the memberof parameter
The memberof parameter can include a comma-separated list of all groups to which the user belongs

</td>
<td></td>
</tr>
<tr>
<td>IdP Metadata</td>
<td>Federation Metadata in xml format. Usually ADFS metadata is found at the URL Path below:
e.g.https://yourADFSDomain/federationmetadata/2007-06/federationmetadata.xml

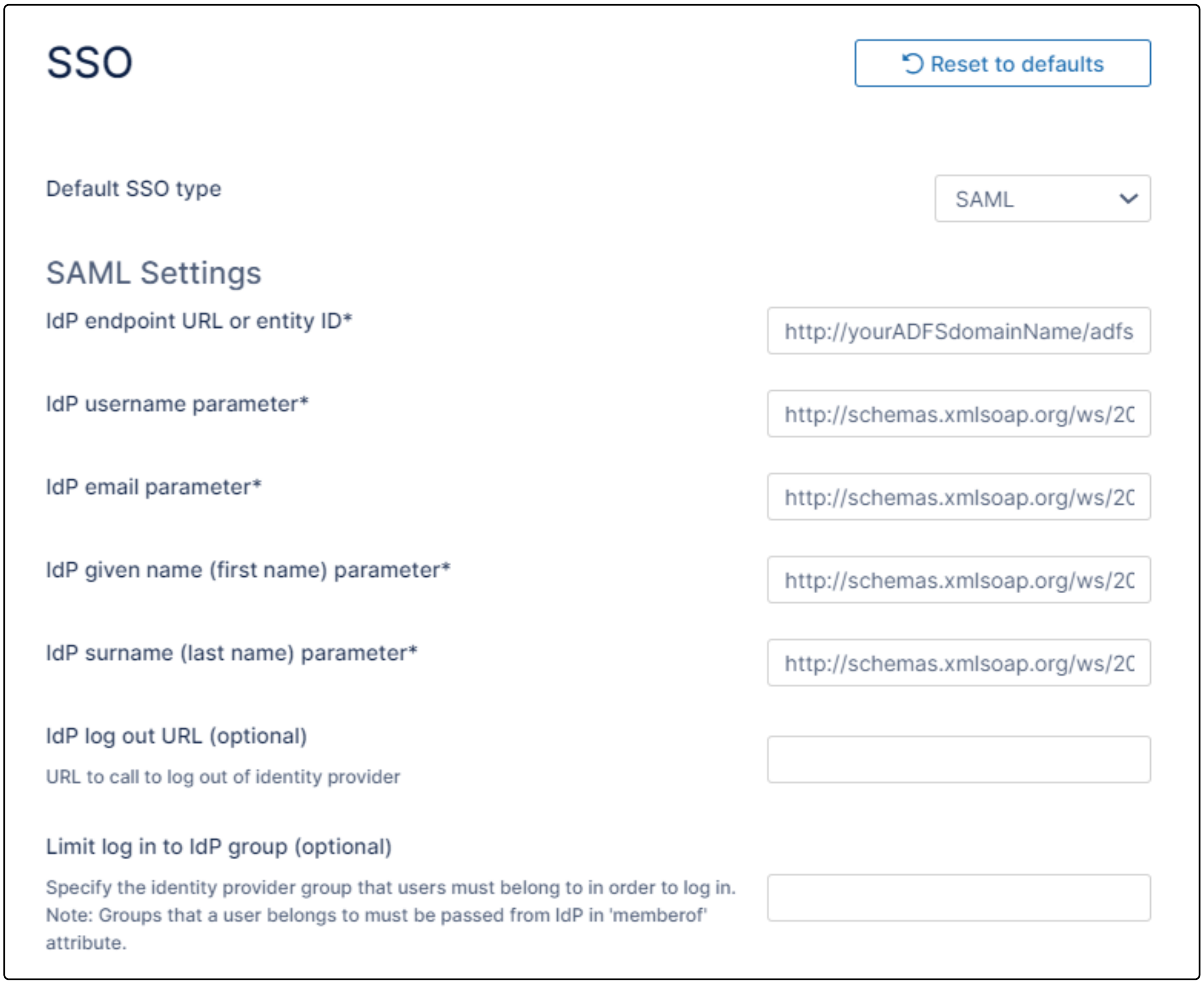


</td>
<td></td>
</tr>
<tr>
<td>SSO Error Message (Optional)

Added in FileCloud 20.1</td>
<td>Custom error message that appears when a signin is invalid. Enter in HTML format.</td>
<td></td>
</tr>
<tr>
<td>Allow Account Signups

Added in FileCloud 20.1</td>
<td>When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.</td>
<td></td>
</tr>
</table>

Automatic Account Approval Added in FileCloud 20.1	This setting works with the **Allow Account Signups** setting to determine: • If the account created by the user is disabled until the administrator approves it • If the account is approved with a specific level of access automatically without intervention from the administrator. • Possible values are: 0 - No Automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User	
Enable ADFS	Yes	
User login token expiration match Idp expiration	If enabled the user token expiration will be set based on ADFS expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)	
Enable Browser-Only SSO Session Timeout Added in FileCloud 23.232.1	If enabled, SSO session timeouts apply to browser sessions but not to client sessions.	
Show the IdP Login Screen	If enabled, automatically redirect user to IdP log-in screen.	
Log Level	Set the Log level for SAML calls. Default Value: PROD (Do not use DEV for production systems)	



Step 3: Enable SSO link on the login page

Follow the steps in SAML Single Sign-On Support (under SSO Configuration Steps, Step 6) to enable SSO sign-in on the user portal or admin portal.

Step 4: Register FileCloud as SP in IdP/ADFS

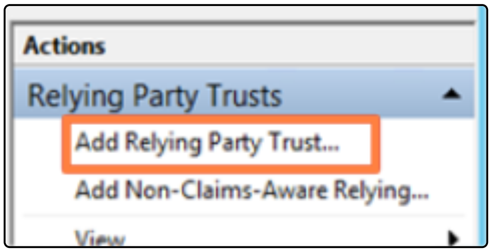
Registering FileCloud as SP in ADFS involves series of steps from adding FileCloud as a Relying Party Trust in ADFS to setting up Claim Rules for FileCloud in ADFS. Please follow the steps below to successfully register FileCloud in ADFS.

Before you proceed, you must be able to download the metadata of FileCloud from the following Entity ID URL. (Note HTTPS).

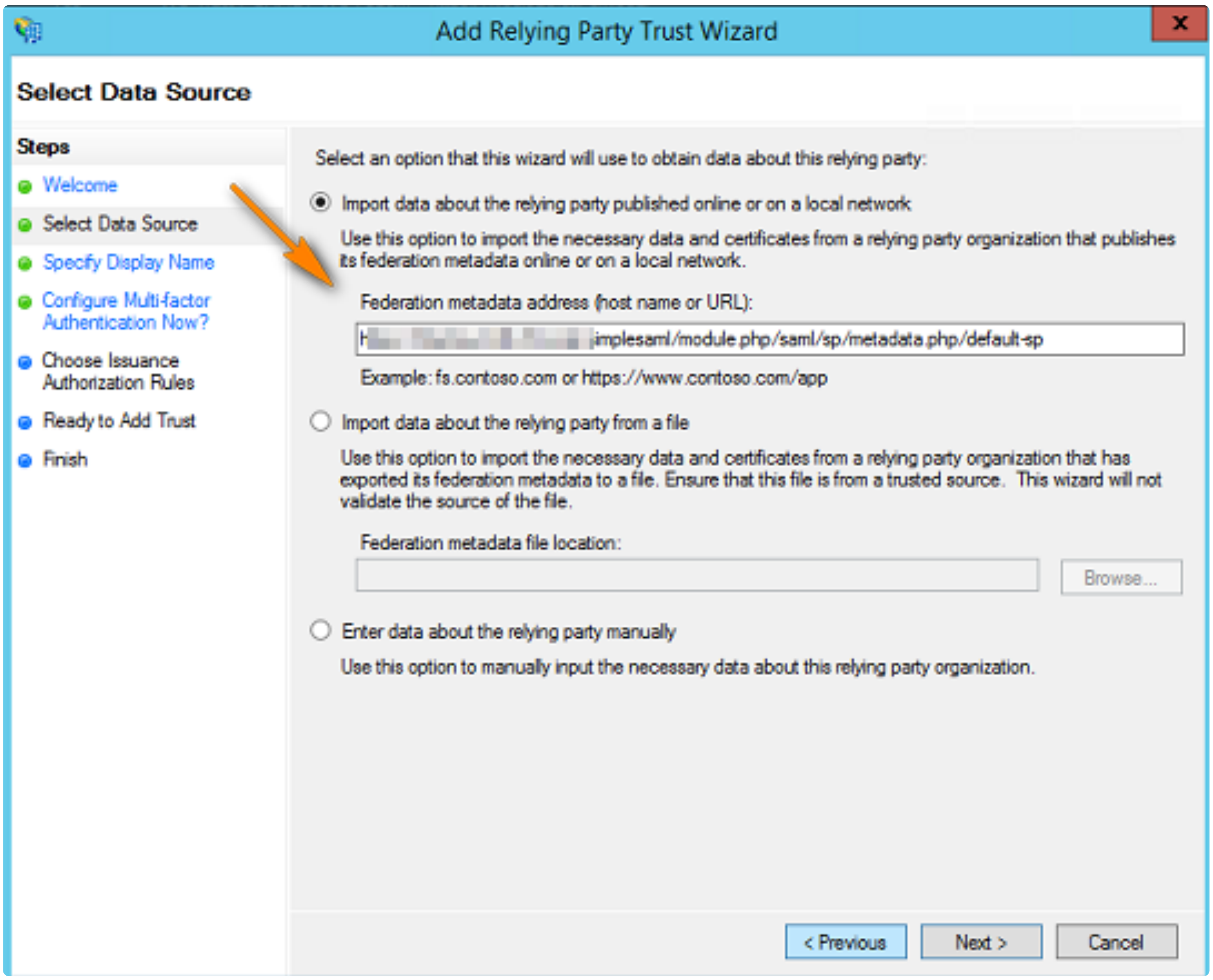
https://<Your Domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp

If you have trouble downloading the metadata from the above URL, please check if HTTPS is working and Steps 1, 2 and 3 above were completed successfully.

1. On your ADFS server, open the ADFS management console, expand **Trust Relationships** and select the **Relying Party Trust** node. In the **Actions** pane, click **Add Relying Party Trust**.



2. Click **Start**, then paste the **Entity ID URL** from above into the **Federation Metadata address** field and click **Next**.

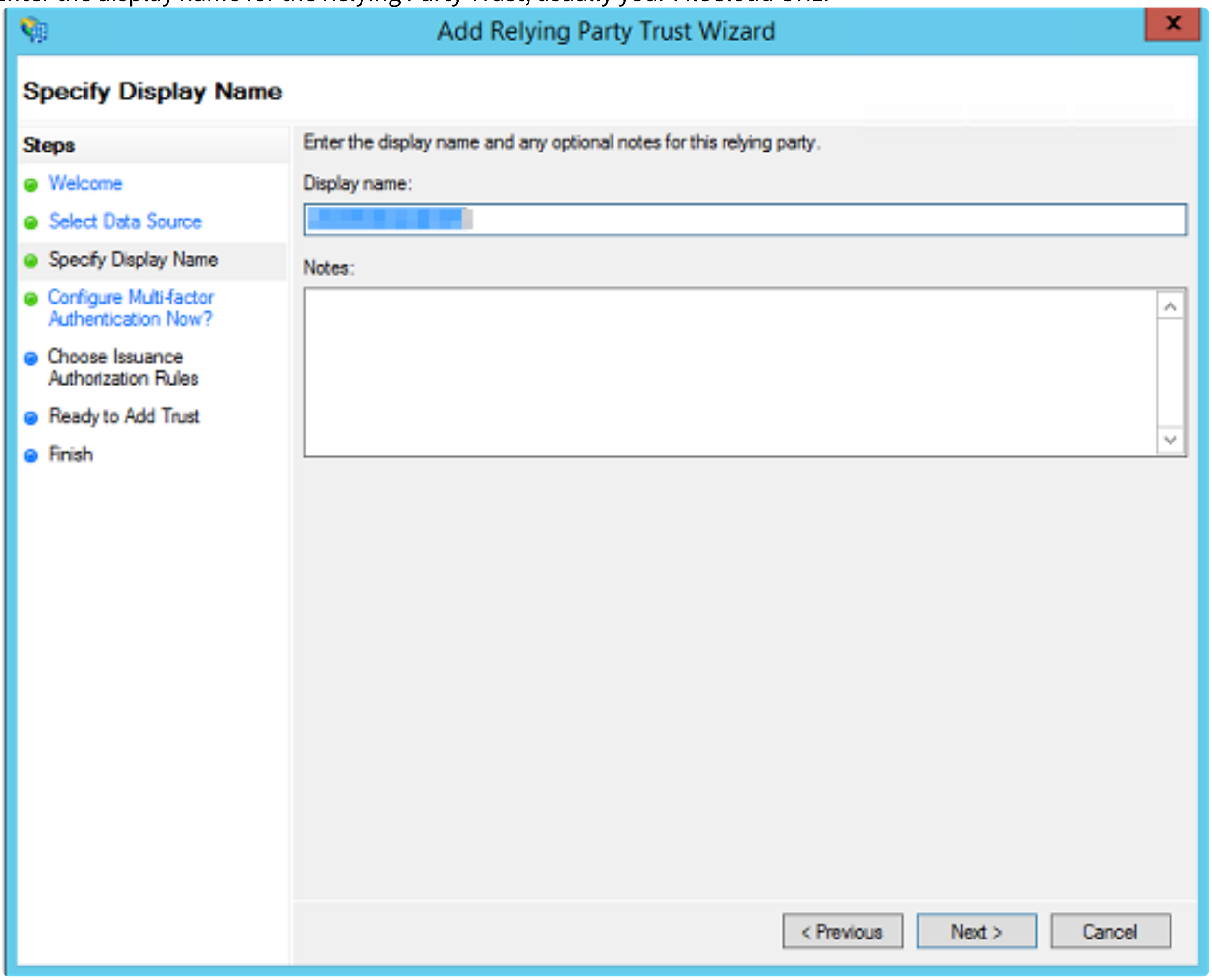


Note: You can do this manually by downloading your metadata file from http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp and importing it into ADFS by choosing **Import data about the**

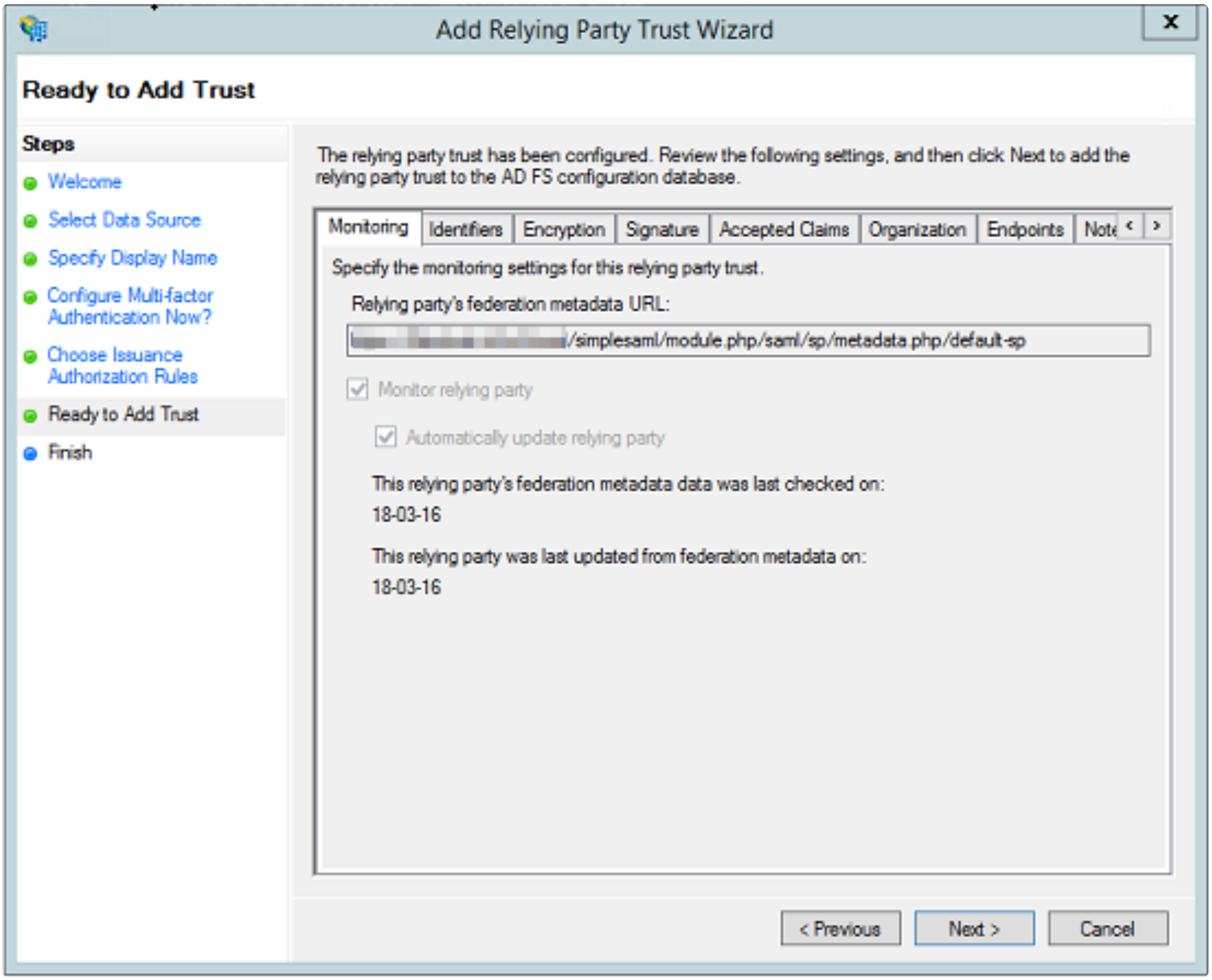
relying party from a file.

> Once you access the metadata URL you need to enter admin credentials to be able to download the metadata file. The username is **admin** and the password can be found in: **<FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php**

3. Accept the warning
4. Enter the display name for the Relying Party Trust, usually your FileCloud URL.

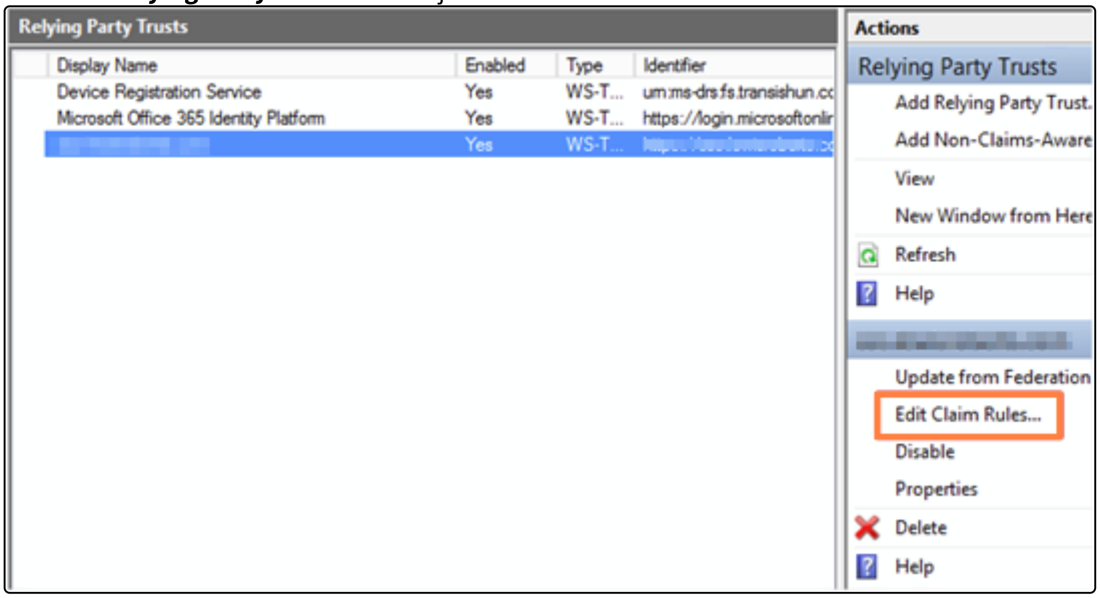


5. Click **Next** several times in the wizard until you reach the **Ready to Add Trust** page. Here, review the tabs. The **Encryption** and **Signature** tabs must have values associated with them.

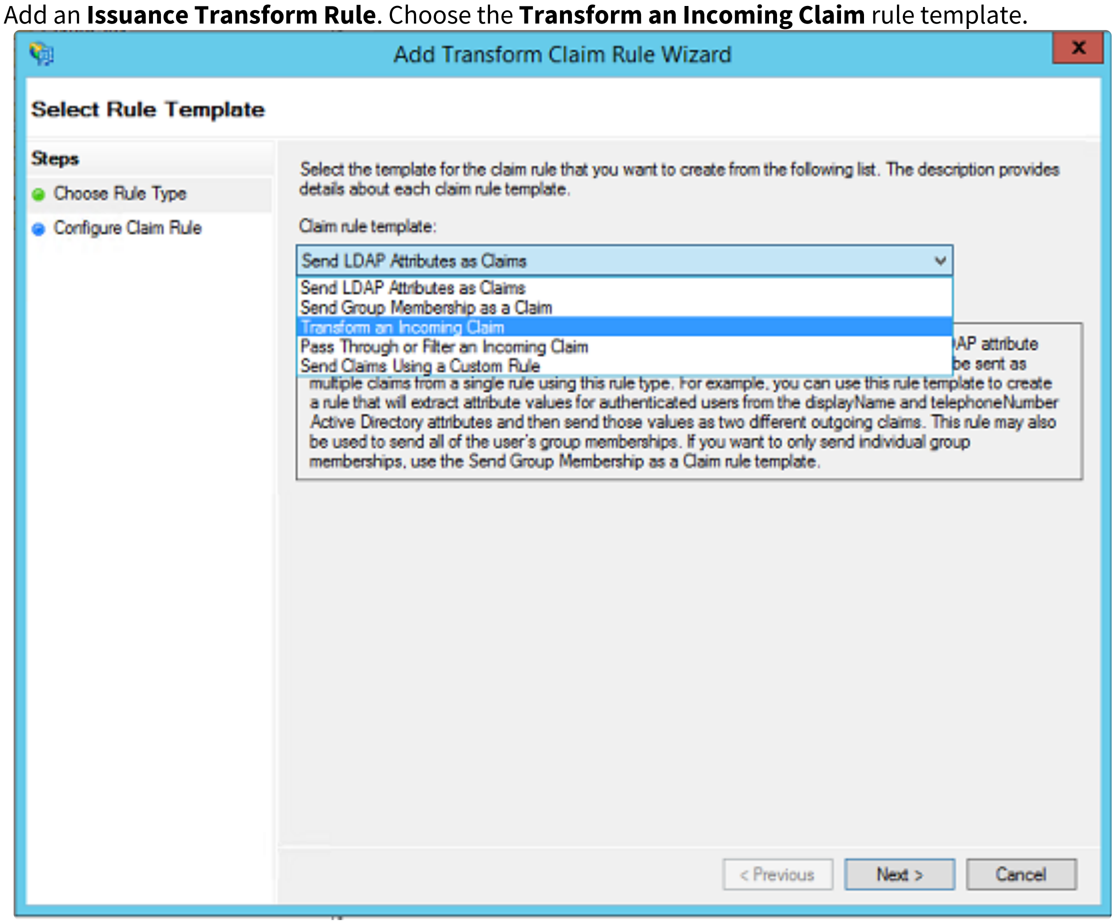


6. Click **Next**. The new **Relying Party Trust** is now added.

7. Select the **Relying Party Trust** we have just added and then click **Edit Claim Rules**.

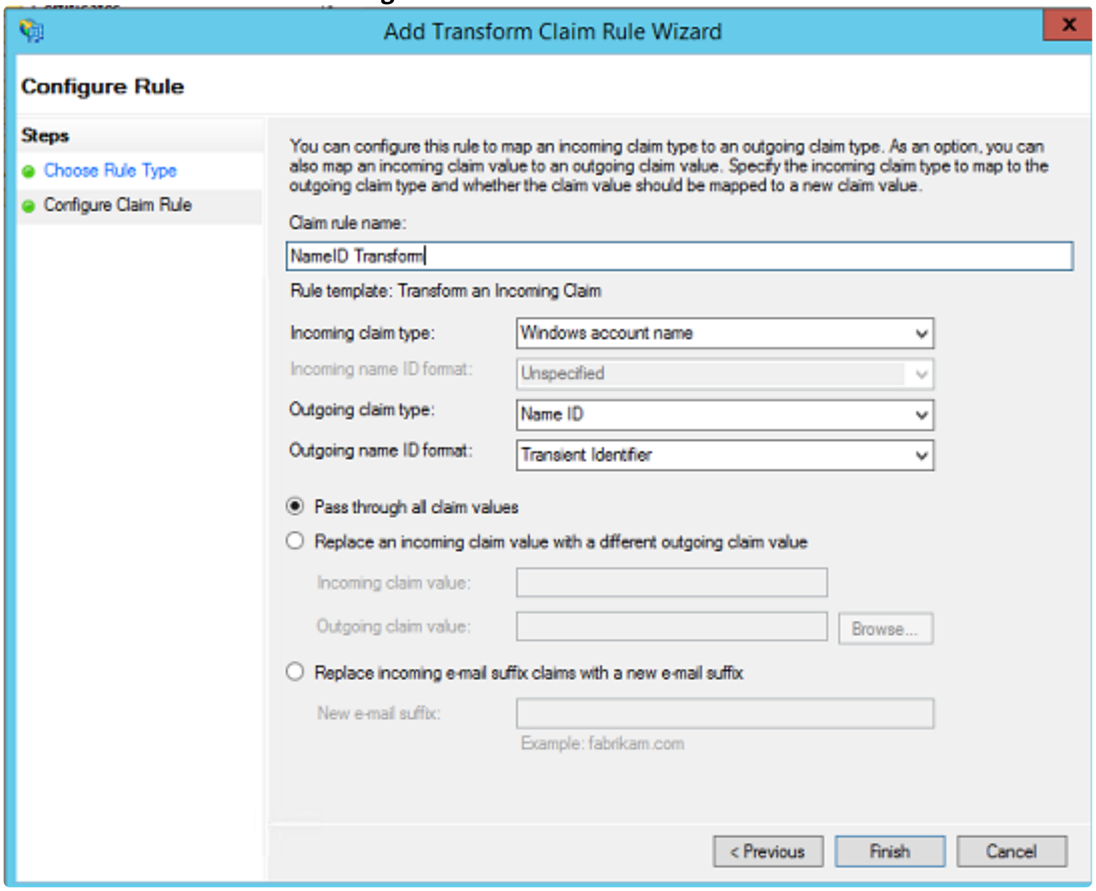


8. Add an **Issuance Transform Rule**. Choose the **Transform an Incoming Claim** rule template.

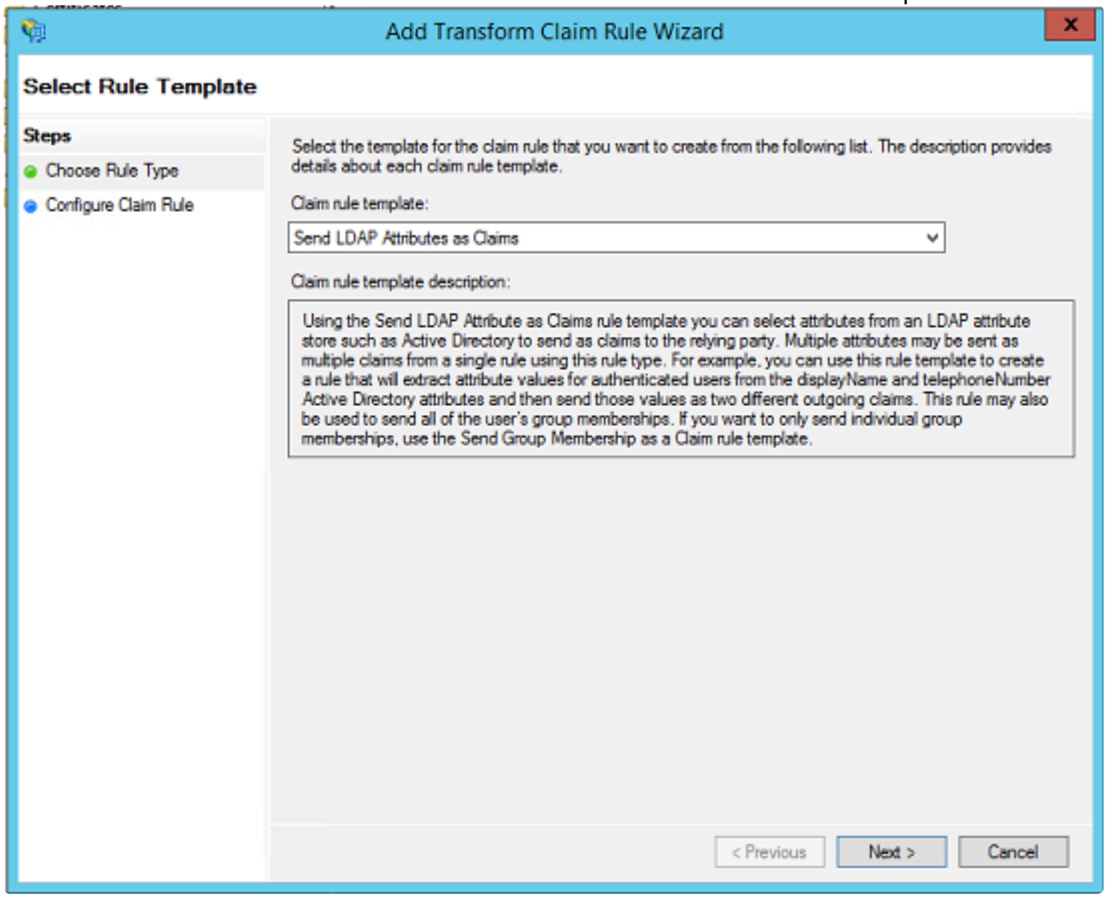


9. Give a **Claim rule name** (Name ID Transform - can be anything). Choose **Windows account name** as **Incoming claim type** and **Name ID** as **Outgoing claim type**. Choose **Transient Identifier** for **Outgoing name ID format**.

Select the radio button **Pass through all claim values.** Click **Finish** to add the claim rule.

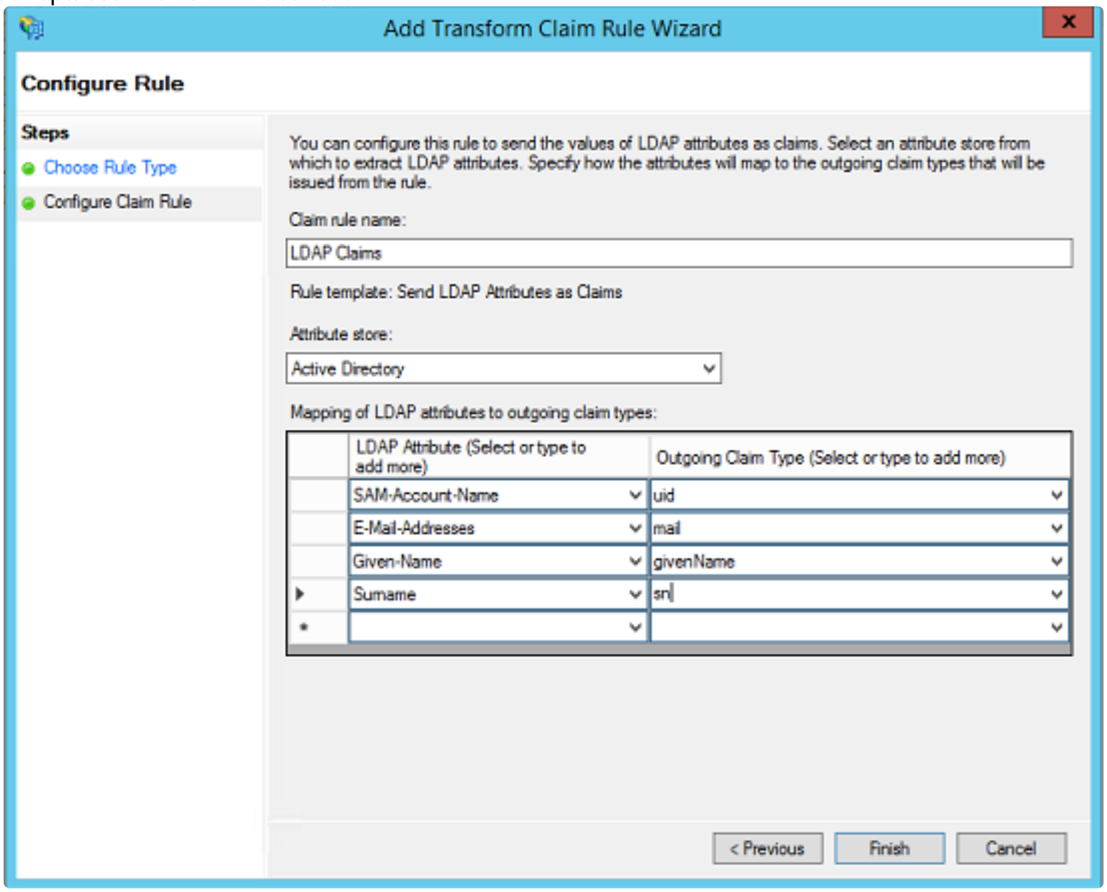


10. Add another issuance transform rule. Select **Send LDAP Attributes as Claims** template.

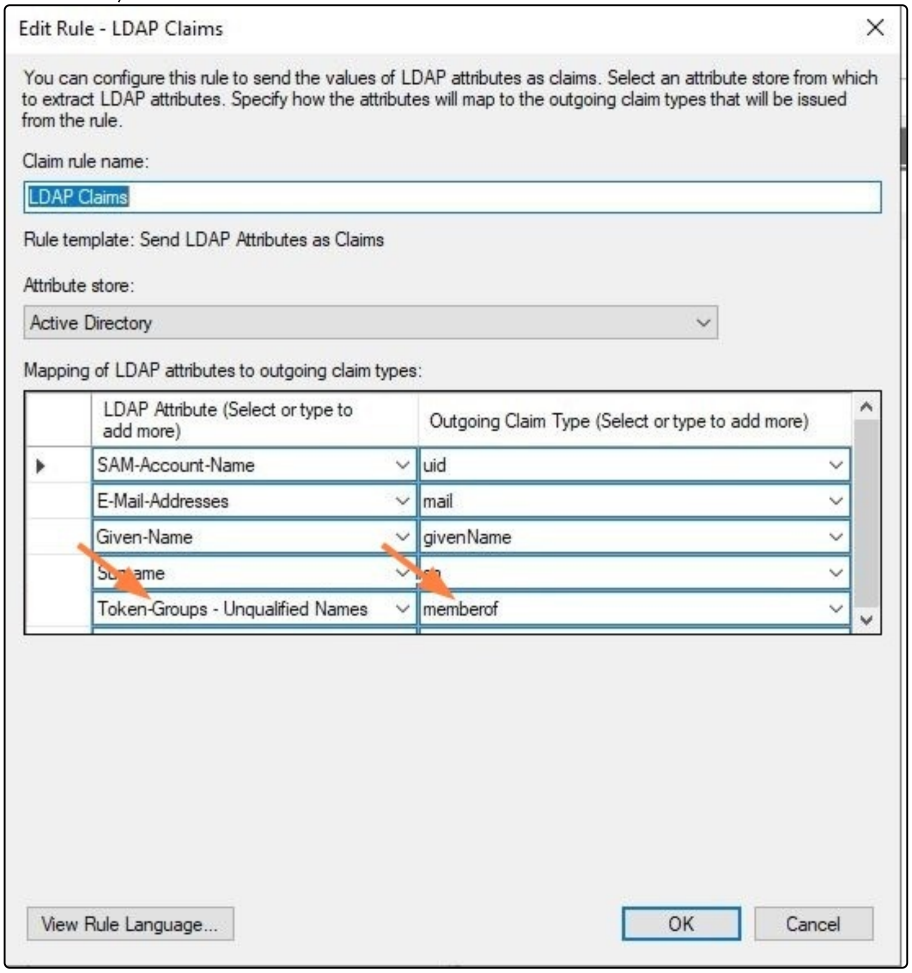


11. Fill in the rule fields:
   - Enter a **Claim rule name** (LDAP Claims - can be anything).
   - Select **Active Directory** as **Attribute store**.
   - Enter the mapping values of **LDAP Attributes** to **Outgoing Claim Types**. The outgoing claim type must match the names as specified in FileCloud SSO Settings UI Page (the screenshot below follows the FileCloud SSO Settings as documented above).

- For **Outgoing Claim Type, uid** and **mail** are required. **SAM-Account-Name** in the screenshot below can be replaced with **UPN** if desired.

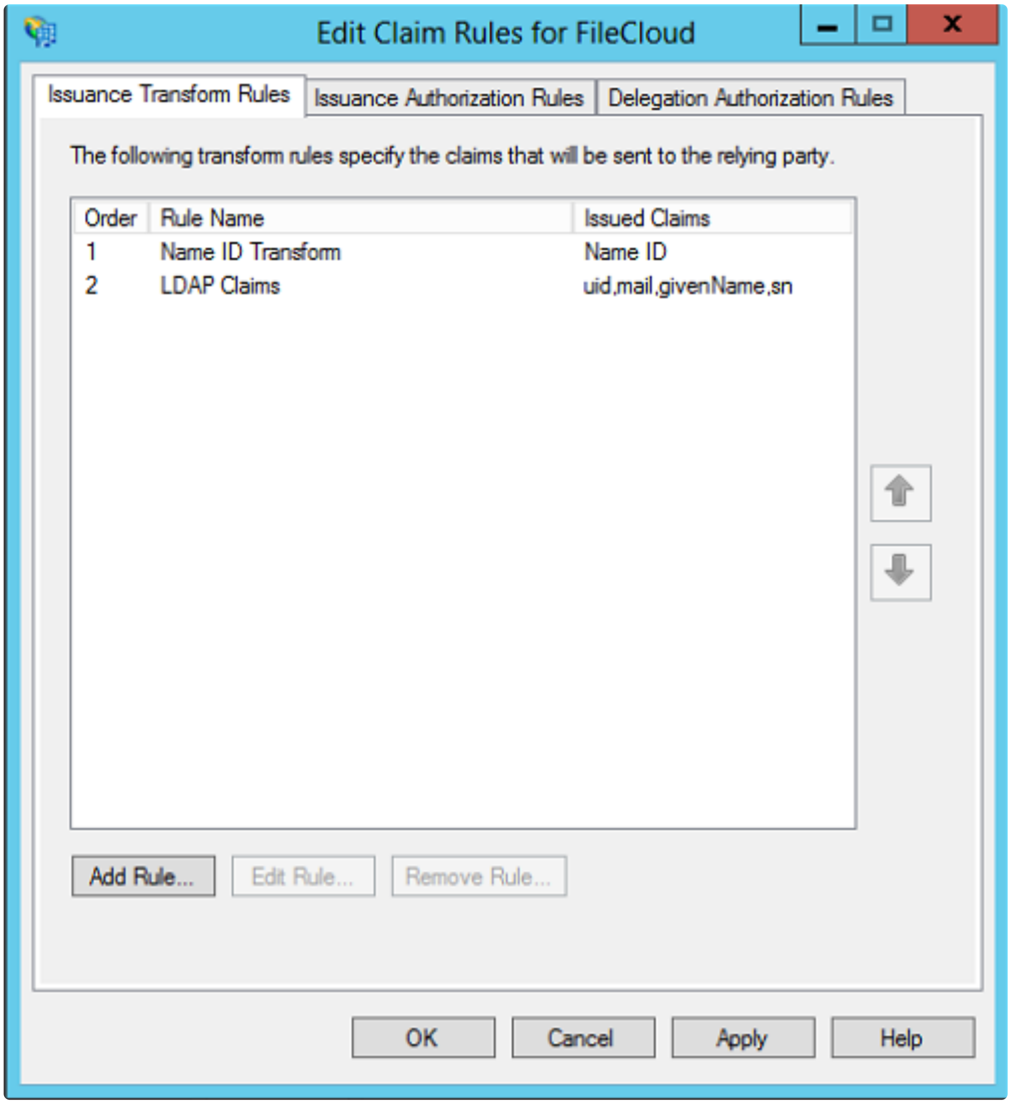


- For ADFS configuration, add an additional claim parameter (**Token-Groups - Unqualified Names > memberof**).



- Click **Finish** to add the rule.

12. Once configured, you should have two issuance transform rules (**Name ID Transform** and **LDAP Claims** if you followed the steps above). Click **Apply** and **Exit**.



This completes the ADFS configuration and FileCloud is added as a Relying Party Trust in the ADFS server. You can now test SSO from FileCloud by going to the FileCloud login page and clicking the Single Sign-On link as mentioned in Step 3, above.

NTLM Single Sign-On Support

FileCloud supports NTLM for User Login through SSO.

Prerequisites

For NTLM SSO to work, the FileCloud Server must be connected to the AD domain.

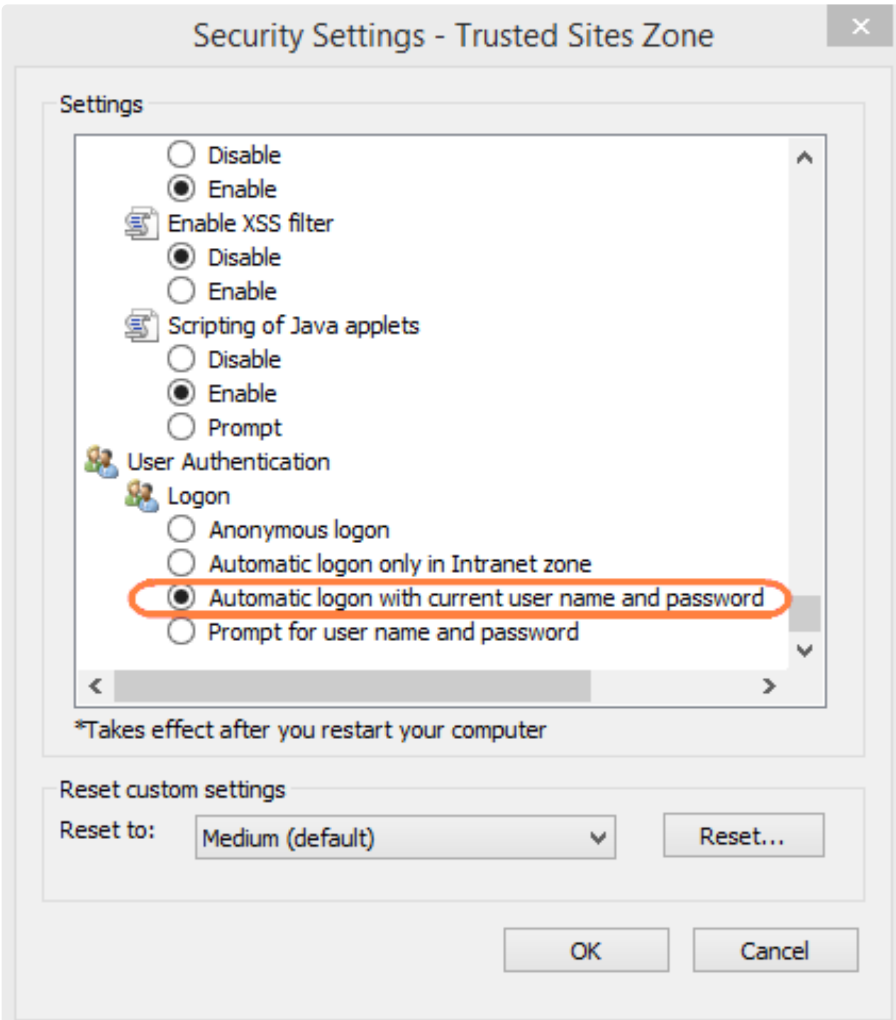
Web Server Settings

To configure your Web server for NTLM SSO, please Contact FileCloud Support.

Browser Settings to Enable Domain User SSO Login

For Internet Explorer and Google Chrome

1. Add the site URL to trusted site.
2. In the settings for trusted sites, enable user login to be sent, see screenshot below.



Troubleshooting

In some environments, additional code may be needed to complete authentication from the server.

After configuration, if you attempt to login with the AD username and password and are repeatedly prompted to enter your AD credentials instead of being transferred to the user portal:

1. Edit the file at c:\xampp\htdocs\.htaccess
2. Locate this section:

```
#--------------------------------------------------
# ADVANCED CUSTOMIZATION SECTION - END
#--------------------------------------------------

#Route all requests to our handler
RewriteRule   ^(.*)/?$ public/index.php [L]
```

3. Above the line:

```
#Route all requests to our handler
```

add the code:

```
RewriteRule ^auth/index\.php$ - [L]
```

Oracle Identity Manager LDAP integration with FileCloud

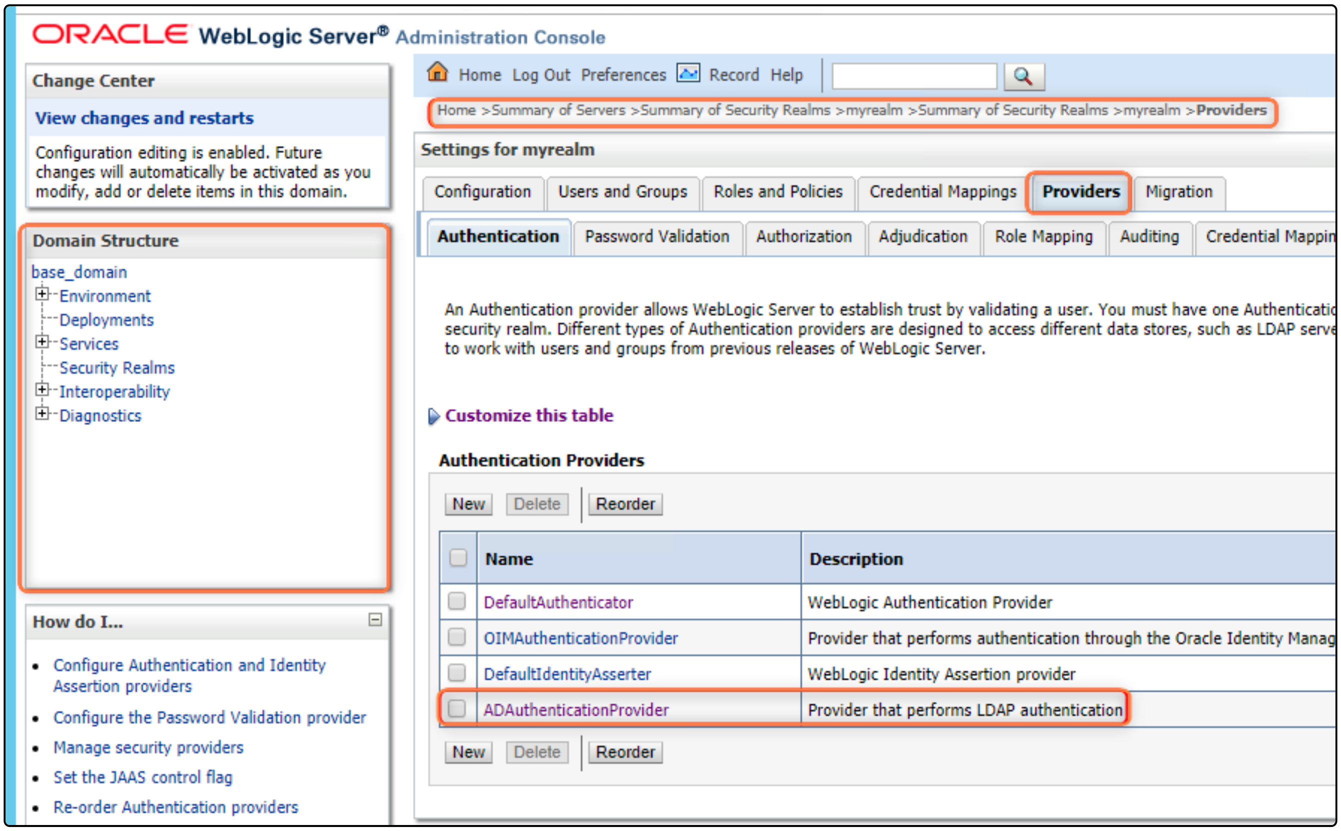
Oracle Identity Manager

Oracle Identity Management enables system administrators to integrate multiple Active Directories and control them from one location. To ensure a smooth configuration please ensure:

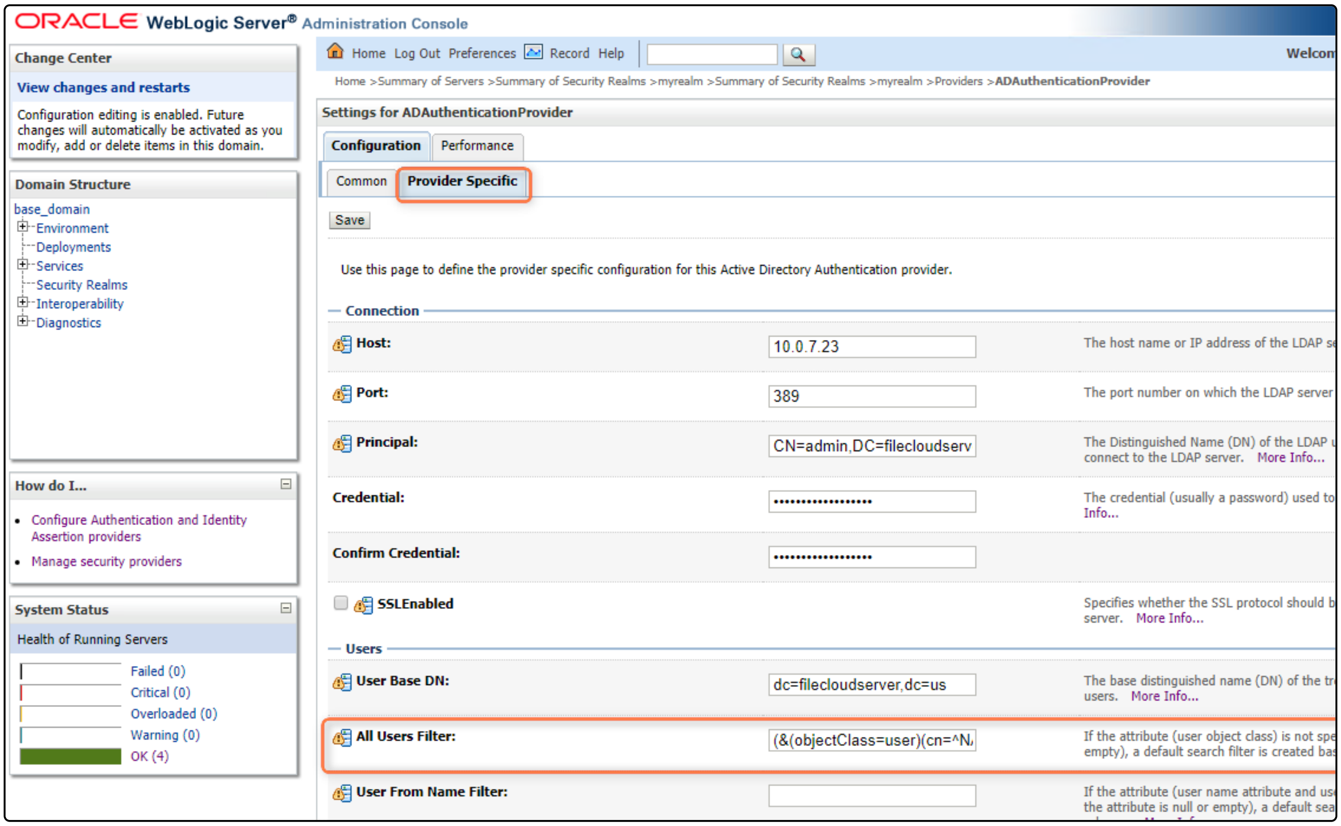
- The server that is hosting FileCloud is able to communicate to the server that is hosting OIM.
- You have access to the Admin user and are able to access WebLogic Admin server.
- Both server's firewalls accept the incoming connection.

Integrating OIM's LDAP with FileCloud

To successfully integrate OIM's LDAP with FileCloud, ensure that FileCloud is able to pull the corresponding attributes such as Name, Email, and password. To verify this, please review your connection settings under Oracle's WebLogic Admin Server under **Domain Structure> Services> Security Realms > [myrealm] > Providers**. Under **Providers > Authentication** select the authentication provider to use to connect to FileCloud via LDAP.

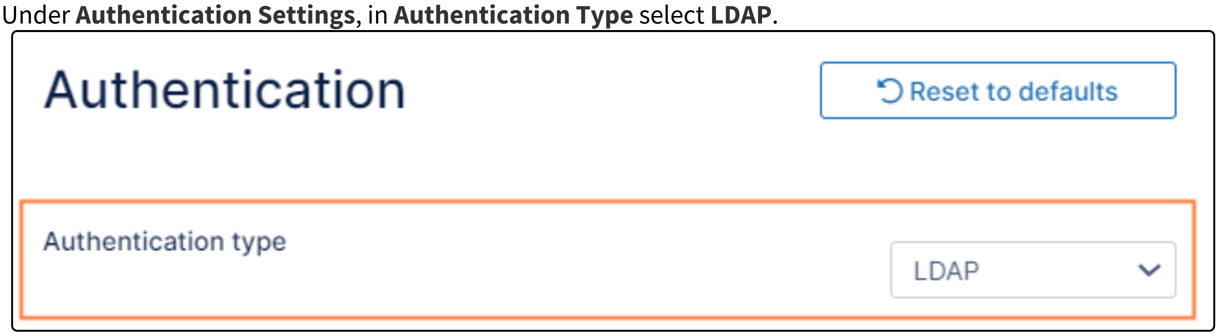


Click the authentication provider name to access its settings. Navigate to the **Provider Specific** tab. To enable FileCloud LDAP to pull the necessary attributes add the following ObjectClass string under **All Users Filter**.
(&(objectClass=user)(cn=^NAME^))
Then, fill out the other required fields based on your Active Directory configuration.



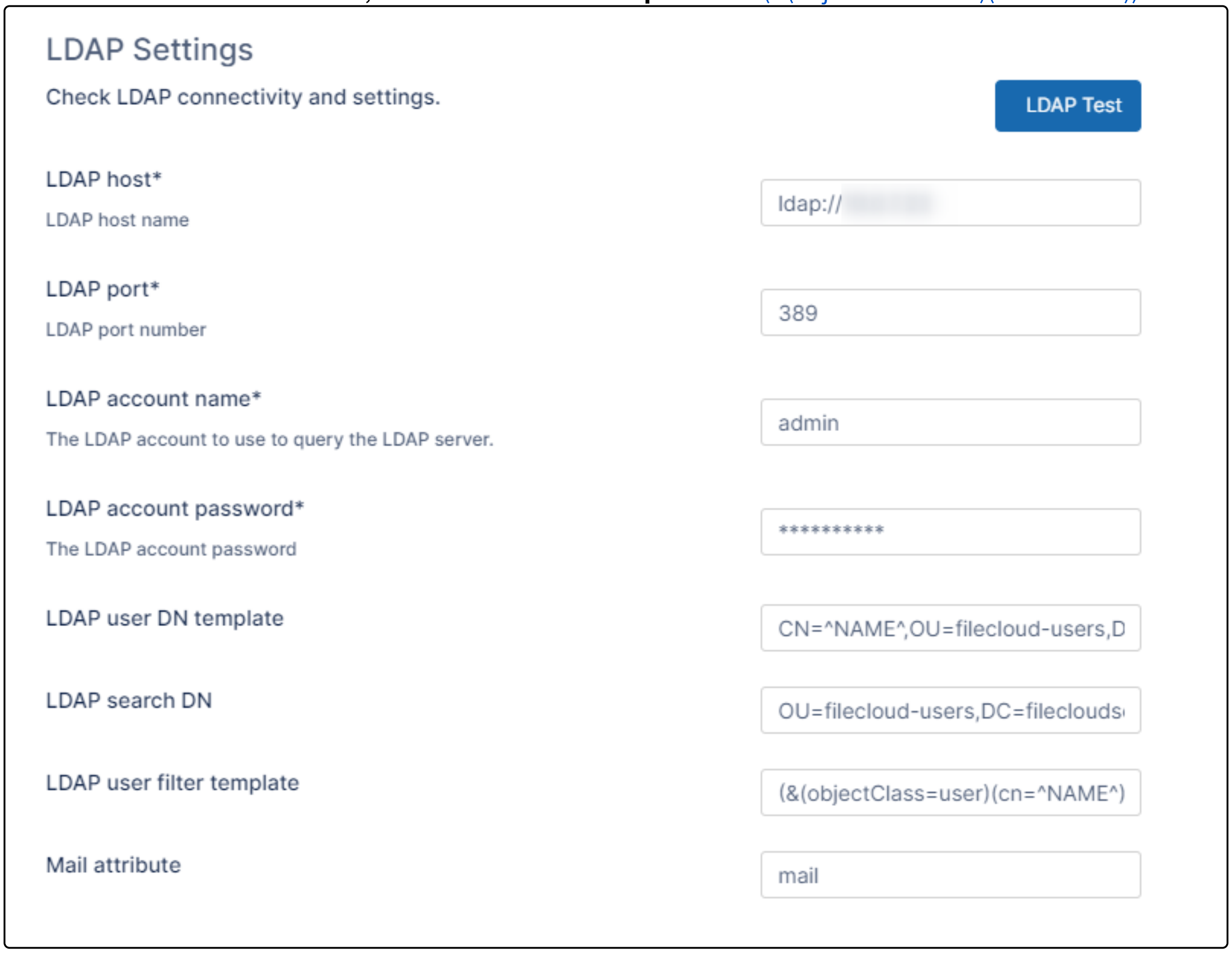
Once you have added the **ObjectClass** attribute on the WebLogic Server realm provider's configuration, access FileCloud's admin portal.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Authentication**  .
   The **Authentication** page opens.
2. Under **Authentication Settings**, in **Authentication Type** select **LDAP**.

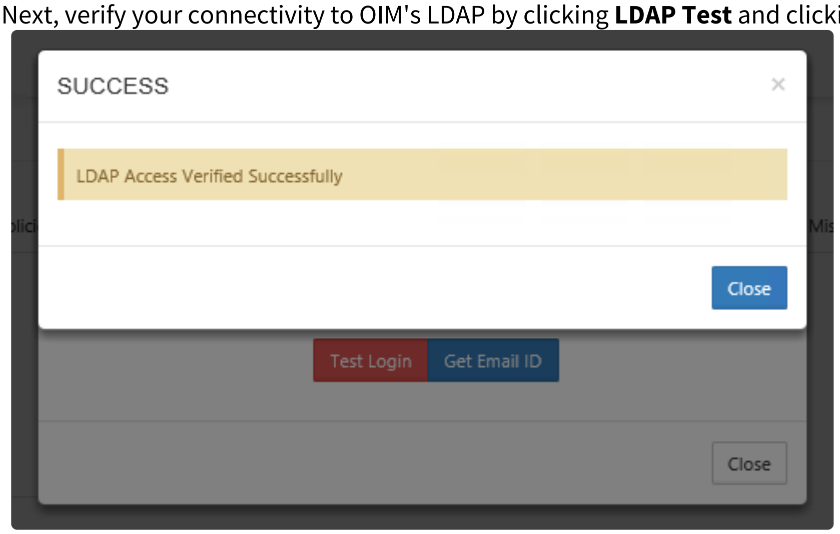


3. To successfully configure LDAP, see LDAP Based Authentication.

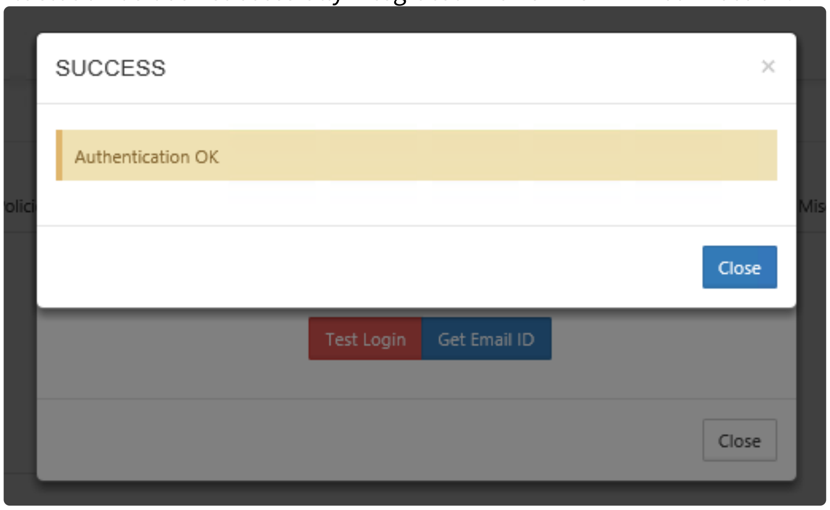
4. To ensure a successful connection, in **LDAP User Filter Template** add: (&(objectClass=user)(cn=^NAME^))

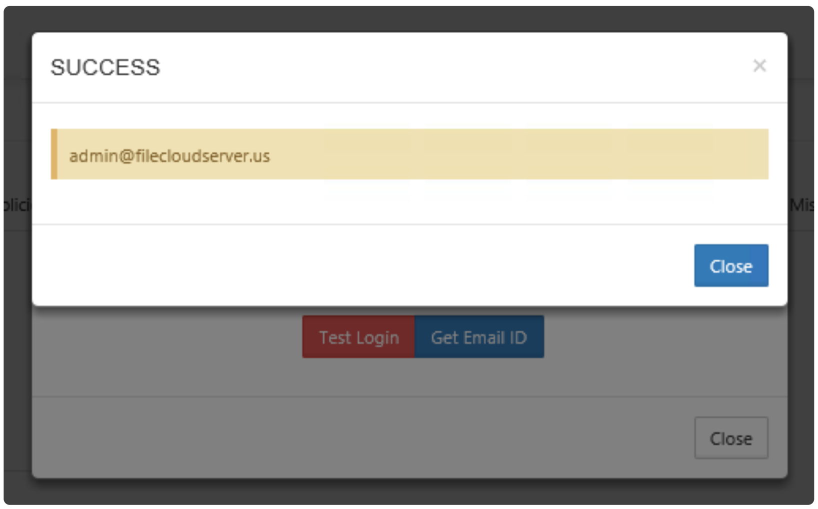


Next, verify your connectivity to OIM's LDAP by clicking **LDAP Test** and clicking **Validate LDAP Settings**.



If you obtain a successful confirmation message proceed to verify that FileCloud is able to login and obtain the email ID as seen on the screenshots below. Upon completion without any errors
FileCloud has been successfully integrated with OIM'S LDAP connection.





Desktop Apps Code-Based Authentication

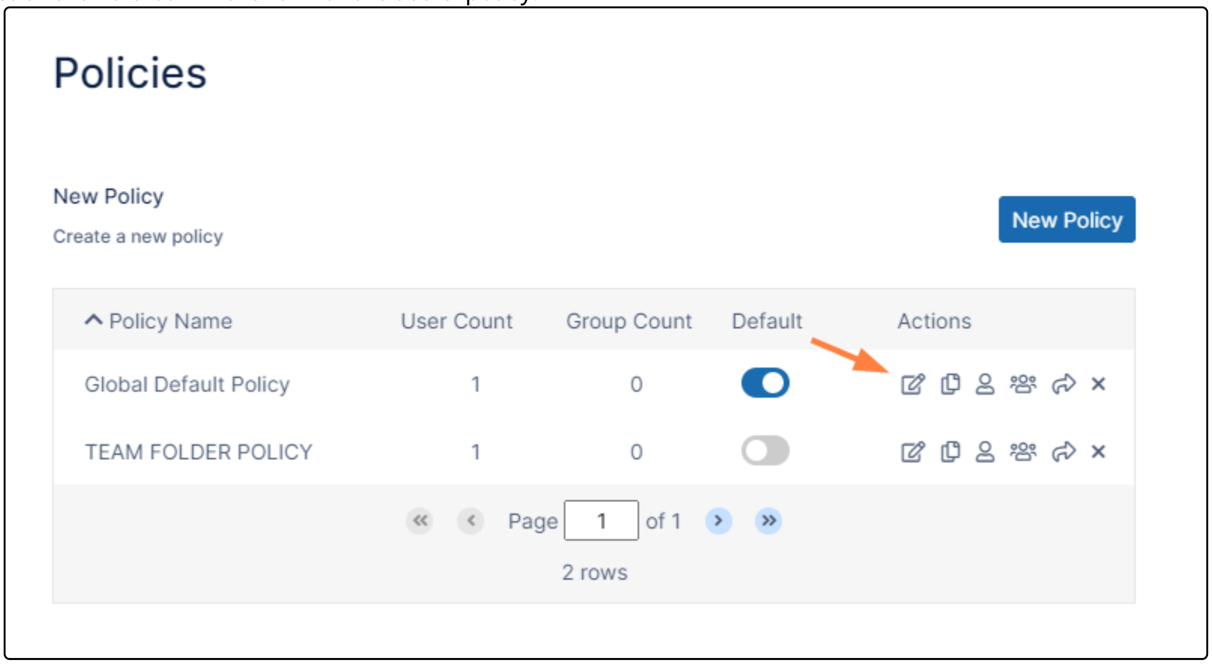
Code-based device authentication is set by policy. It requires users to request approval to log in to a desktop app or mobile app. When the request is approved, a code is created which the user must enter into the app to log in. Requests are approved in the user portal, but additional admin approvals may also be required.

Enabling code-based device authentication

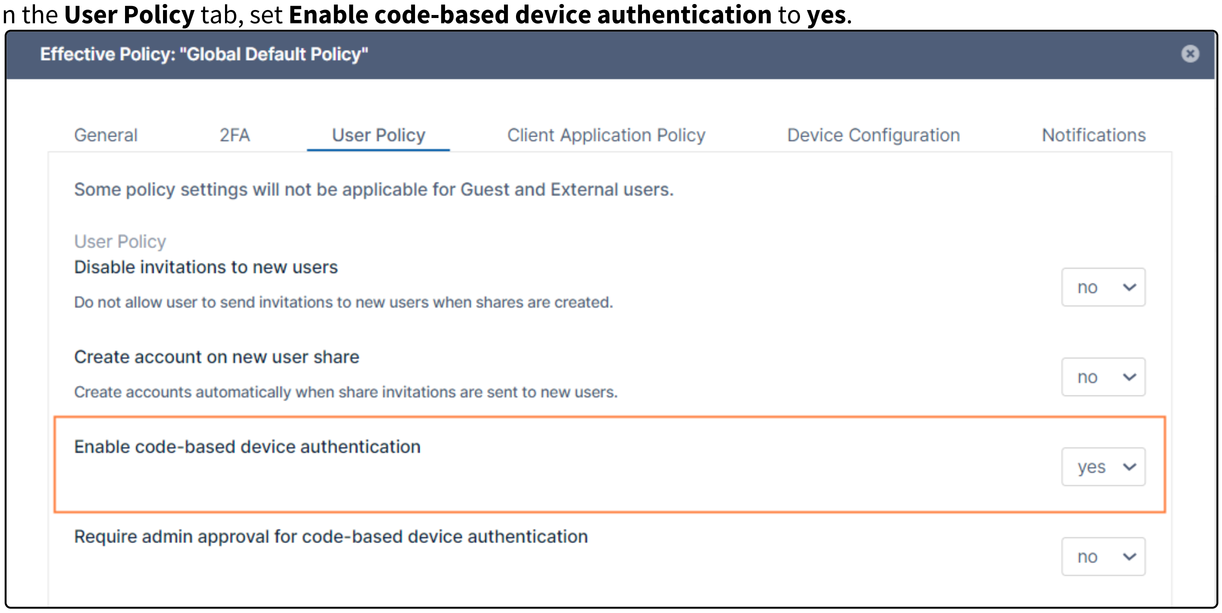
Enable Code based device authentication

To enable code-based device authentication:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



   The **Policy Settings** dialog box opens.
3. Click the **User Policy** tab.
4. In the **User Policy** tab, set **Enable code-based device authentication** to **yes**.



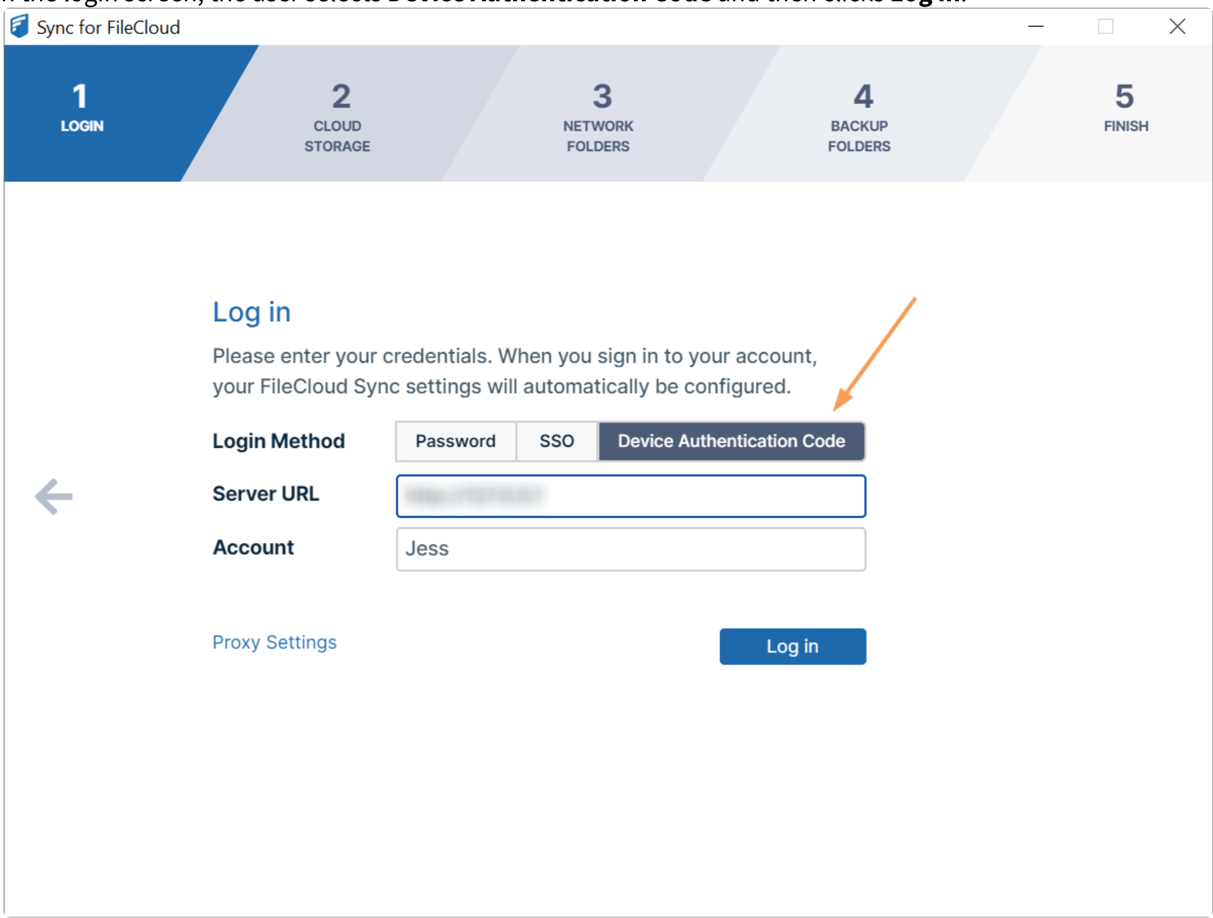
   Now, when a user logs in to a client app, an approval request appears in in the user portal. The user must approve the request to receive a code that is entered into the client app to successfully log in.
   How users log in with device authentication, below, shows how this process works.

How users log in with device authentication

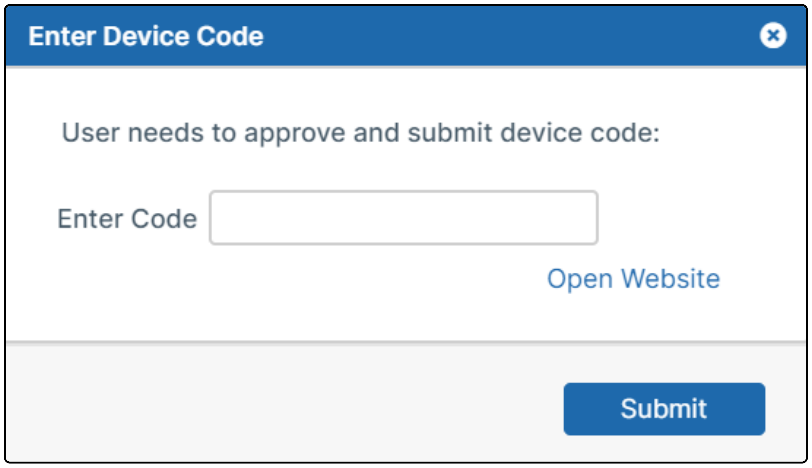
How users log in with device authentication to desktop apps

Once code based authentication is enabled, the user can follow these steps to log in via a desktop app.
The following example uses the Sync application, but the procedure is the same for all of the desktop applications and the mobile apps.

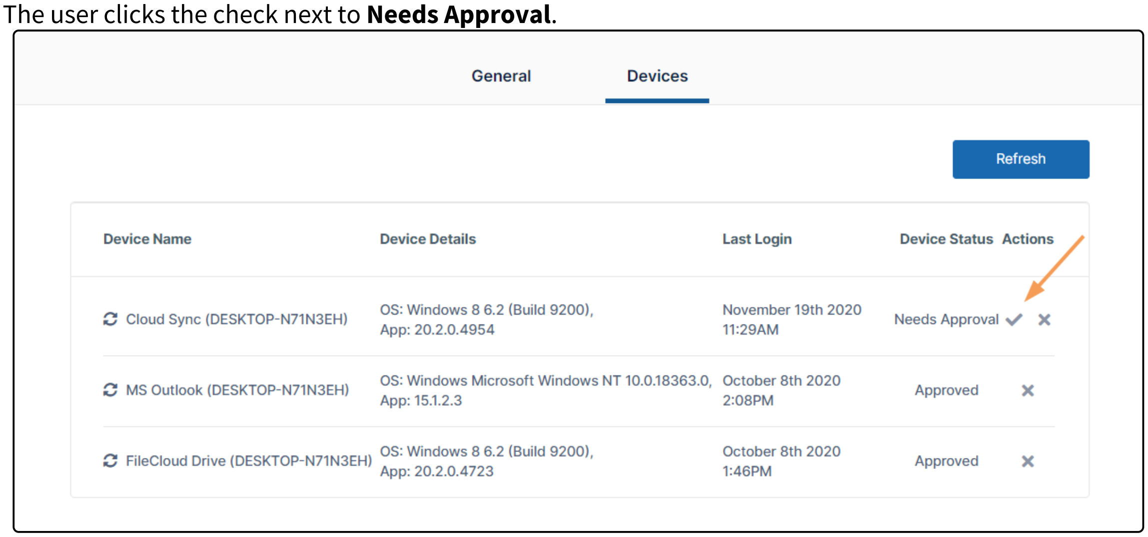
1. In the login screen, the user selects **Device Authentication Code** and then clicks **Log in**.



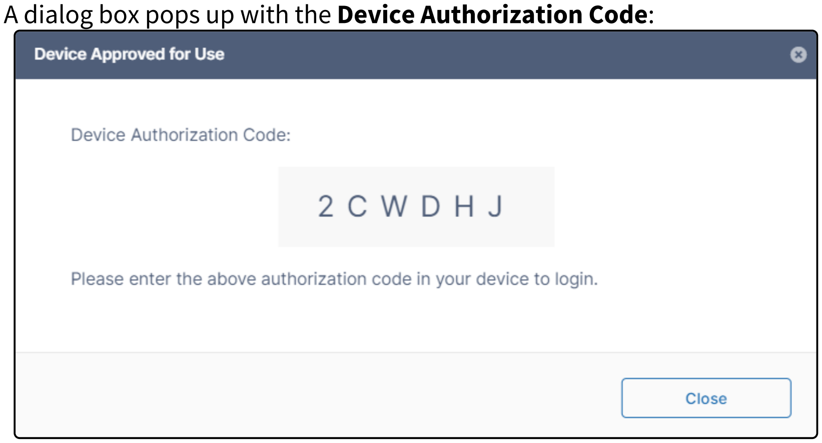
The following dialog box opens.



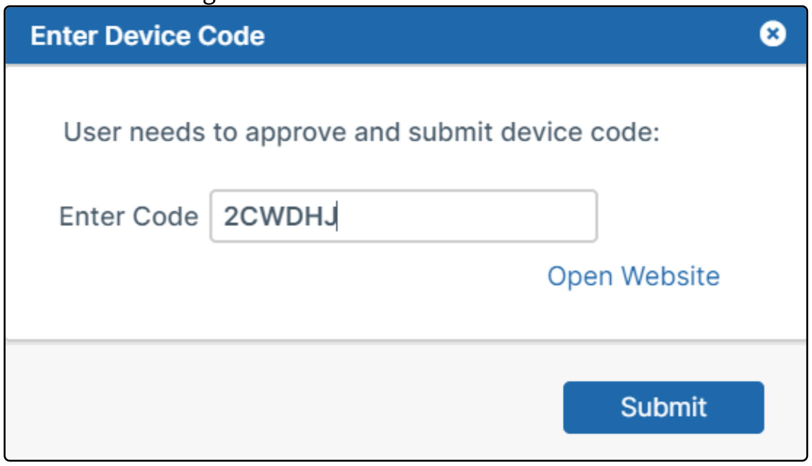
2. To get the device authorization code:
    a. The user logs in to the user portal, then clicks the arrow next to the username and chooses **Settings**..
    b. In the **Settings** screen, the user click the **Devices** tab.
    c. The user clicks the check next to **Needs Approval**.



A dialog box pops up with the **Device Authorization Code**:



3. The user copies the **Device Authorization Code** and pastes it into the **Enter Device Code** dialog box, then clicks **Submit** to log in.



Requiring admin approval as well as user approval for devices

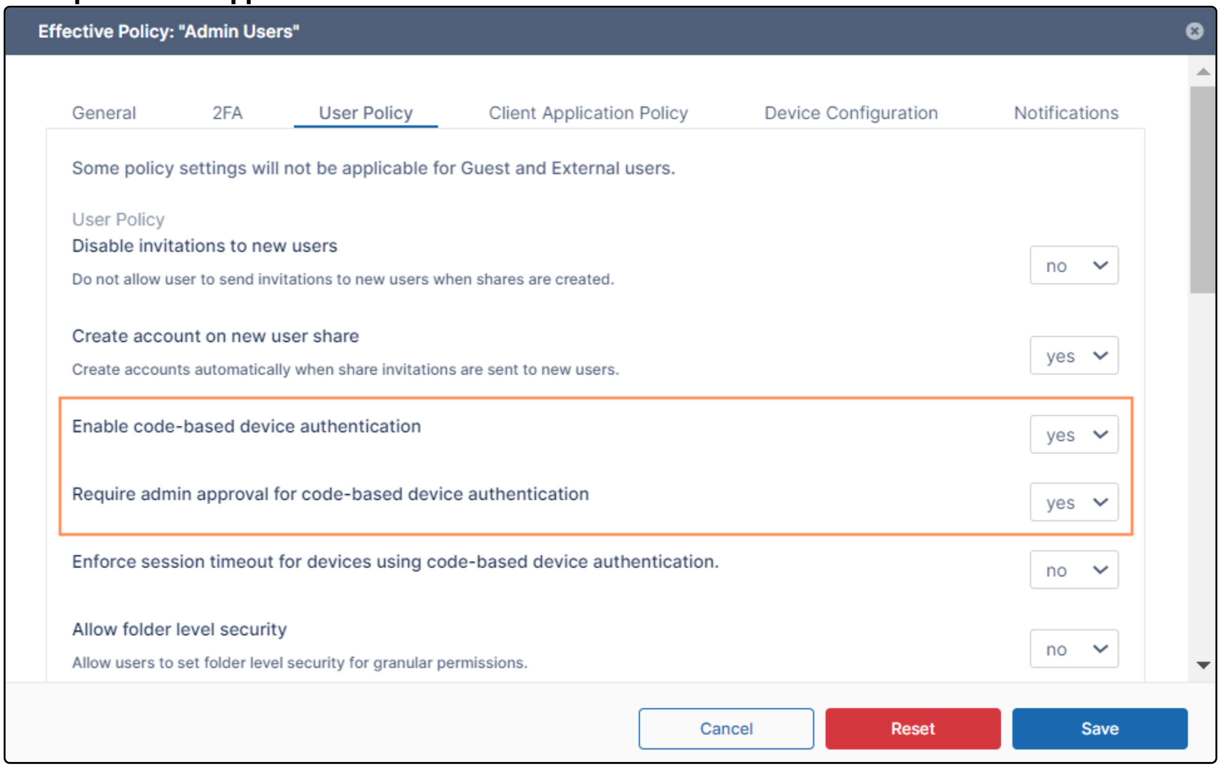
Requiring admin approval to log in with client devices

The **Enable code based device authentication** setting lets users log in to desktop apps using a device authorization code without admin approval. You can also can configure FileCloud to require logins to desktop apps to be approved by admins before being approved by users.

To require admin approval for device authentication:

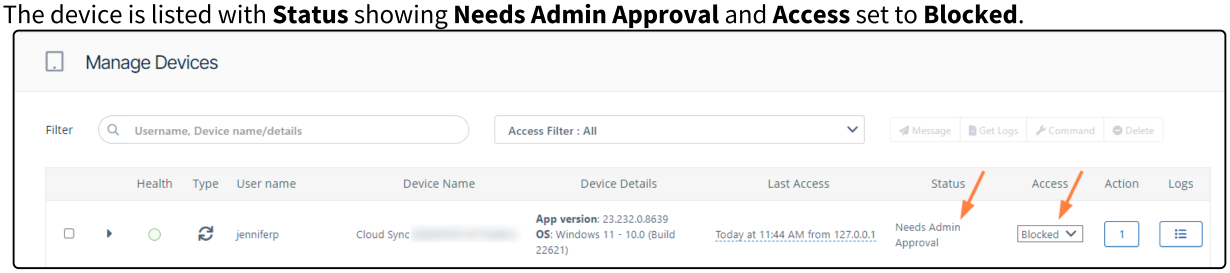
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Open a policy for edit.
3. In the **User Policy** tab, set **Enable code based device authentication** to **YES**.
   The **Require Admin Approval for Device Authentication** setting becomes enabled.

4. Set **Require Admin Approval for Device Authentication** to **YES.**

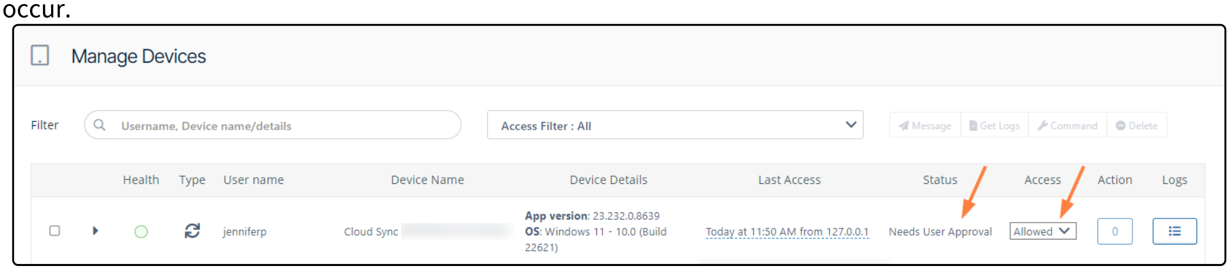


To approve a client device that has been sent to you for admin approval

1. Go to **Device Management** in the admin portal to view the listing for the device approval.
   The device is listed with **Status** showing **Needs Admin Approval** and **Access** set to **Blocked**.



2. In the **Access** column, change **Blocked** to **Allowed**.
   Now the **Status** column shows **Needs User Approval**, and the user must approve the client device (as shown above in **How users log in with device authentication**) and get an authorization code before log in can occur.



Share Settings

> The **Attach Share Password by Default for Public Shares** setting is available beginning in FileCloud 20.1.

File sharing allows users to provide public or private access to files stored in FileCloud Server with various levels of access privileges.

To control how users share files and folders in ways that are appropriate for your organization, administrators configure share settings.

Configure Sharing Defaults

> The field **Allow comments for external users** is available beginning in FileCloud 23.251.
>
> The fields **Public share default password length** and **Require complex public share passwords** are available beginning in FileCloud 23.242. Shares created with passwords prior to 23.242 maintain the passwords they were created with and are not required to comply with the new settings.

> Beginning with FileCloud 23.241, the **Default Share Type** is **Private Share**.
> Prior to FileCloud 23.241, the **Default Share Type** was **Public Share**.

When a user wants to share a file or folder, administrators can decide which options should be automatically selected.

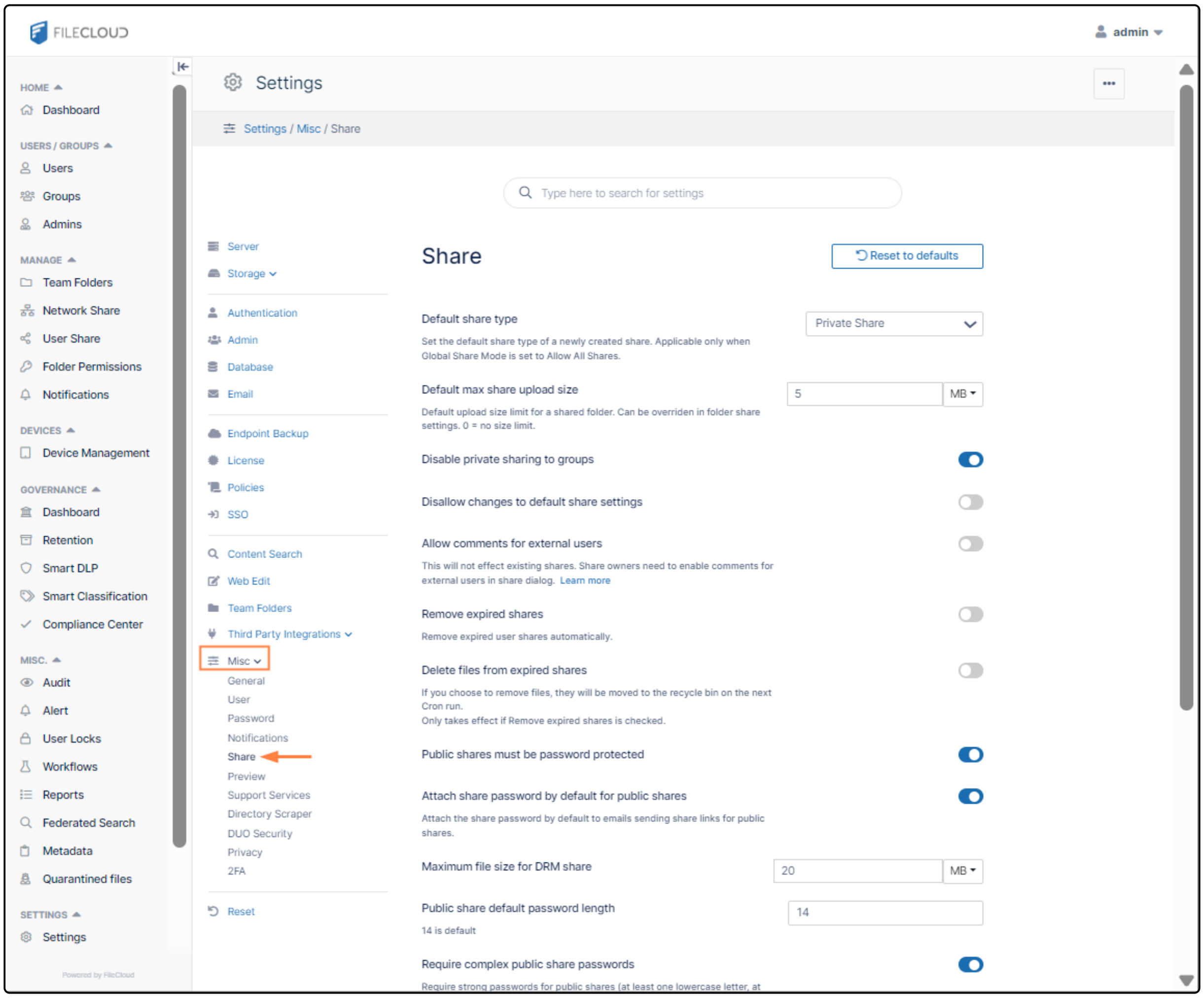
The settings are really just a recommendation and can be changed by the user, unless you disable the ability to change the defaults.

Most of the settings below are set the Share settings page.

To open the Share settings page:

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

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



The **Share** settings page opens.

Follow the procedures below to change the sharing defaults.

Default Share Type

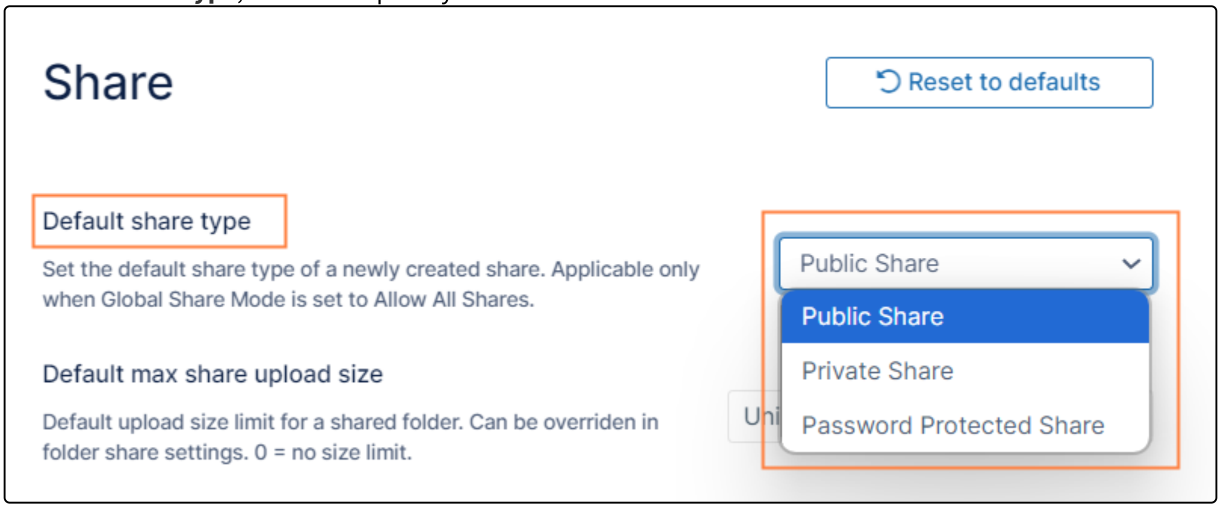
This option tells FileCloud Server what type of share to automatically select when a user shares a file or folder. By default it is set to **Private Share**, but you may change it.

- Applicable only when **Share Mode** is set to **Allow All Shares**.
- This type can be changed by the user unless **Disallow Default Share Settings Change** is set.

To change the Default Share Type:

1. Open the Share settings page.

2. In **Default share type**, select the option you want to use.



Public Share	Allows users to share with anyone who has the link to the share. • Does not require the user you want to share with to have a FileCloud account. • Share a file with everyone with or without restrictions. • Share a file with everyone and require a password.
Private Share (Default)	Allows users to share with anyone who has the link and can log in to a FileCloud account. • Does require the user you want to share with to have a FileCloud account. • Requires an invitation to be sent to someone to create a FileCloud account if they don't already have one. • Share a file with all FileCloud users with or without restrictions. • Share a file with specific FileCloud users with or without restrictions.
Password Protected Share	Forces users to create a password when sharing a file or folder. • Recipients of the share are given the password when they receive the link to the share. • The share can be public or private.

3. Click **Save**.

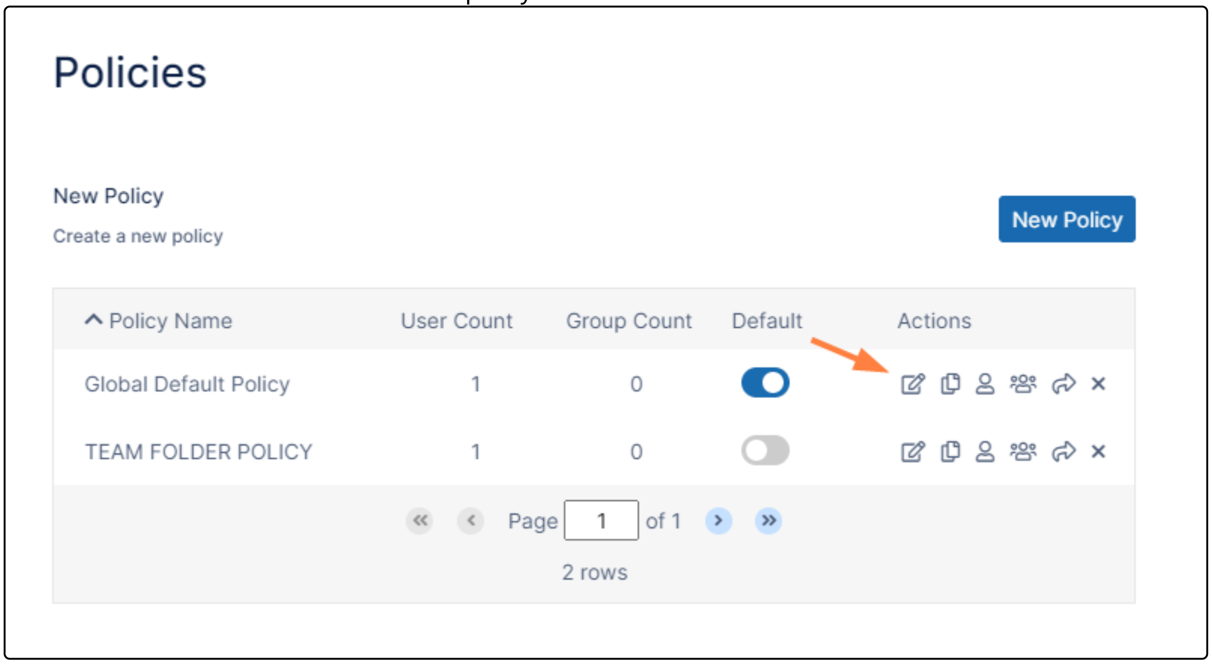
Set Expiration Days Default

You can allow users to share files and folders for as long as they exist, or you can set the number of days that a share remains active by default.

Note: This setting can be changed by the user unless **Disallow changes to default share settings** is set in the Share settings page.

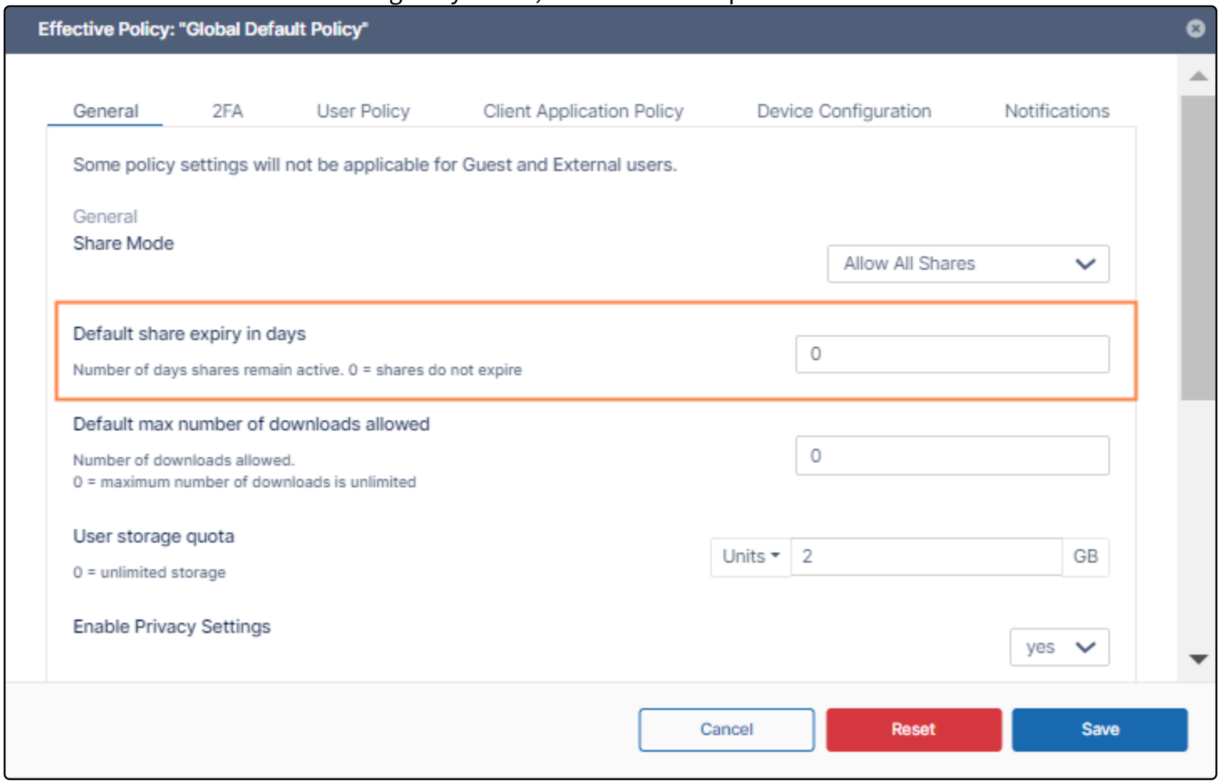
To set the Share Expiry default in a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



3. Click the **General** tab.

4. Change the value of the **Default Share Expiry in Days** setting.
   A value of **0** means that unless changed by a user, shares do not expire.



5. Click **Save**.
   The value is only changed for users who are using this policy.

Default Max Share Upload Size

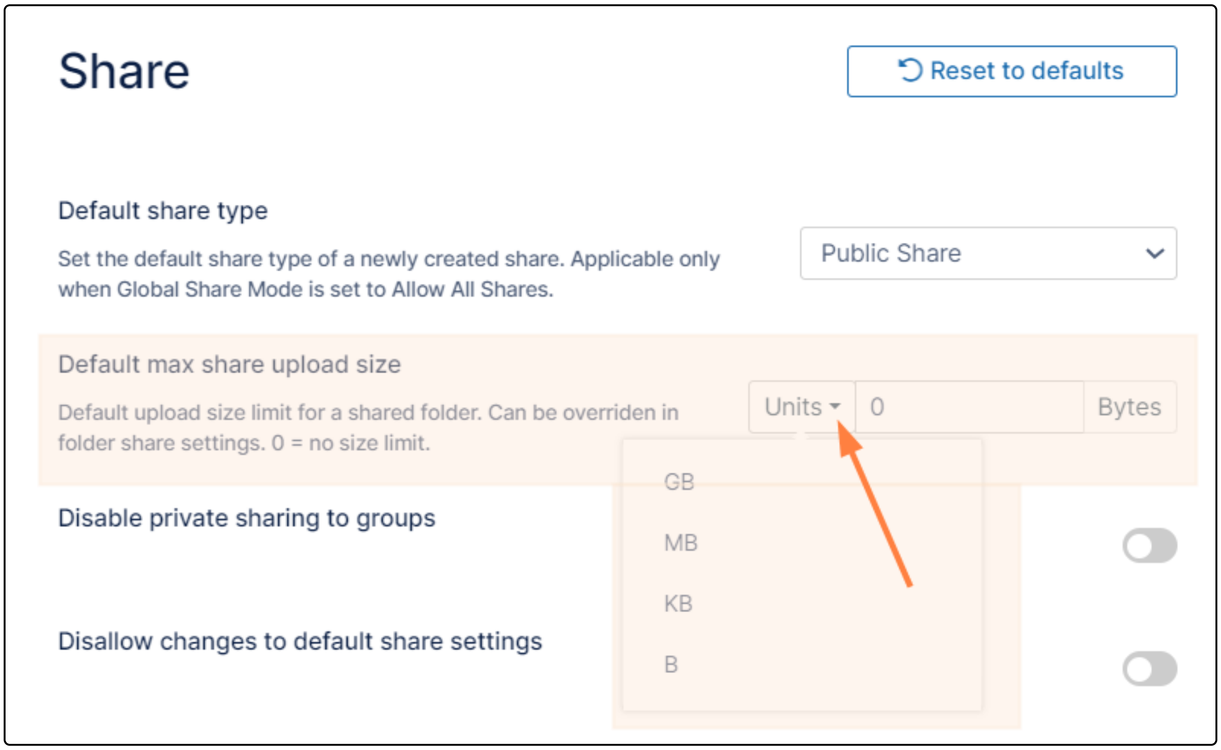
Administrators can allow users to upload files into a shared folder no matter how big it is, or you can set a suggested size limit.

- You can set a maximum size limit in any of the following units: **B**, **KB**, **MB**, **GB**.
- Using a value of **0** means that users can upload files into a shared folder no matter how big it is.
- This setting can be changed by the user in the shared folder settings.

To set the Max Upload size default for Shares:

1. Open the Share settings page.

2. In **Default max share upload size**, select a choice in **Units**, and then type in the file size limit you want to use.



3. Click **Save**.

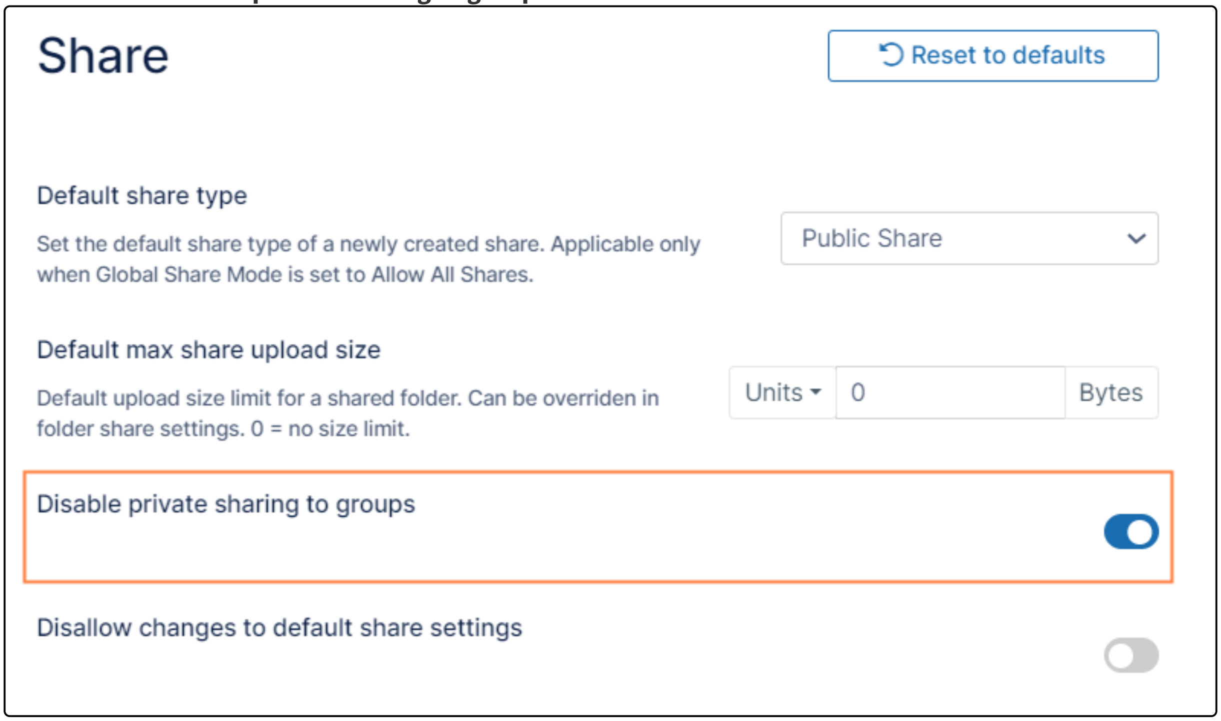
Disable Sharing to Groups for Private Share

You can check **Disable private sharing to groups** to hide the Group option when users or admins privately share a file or folder.

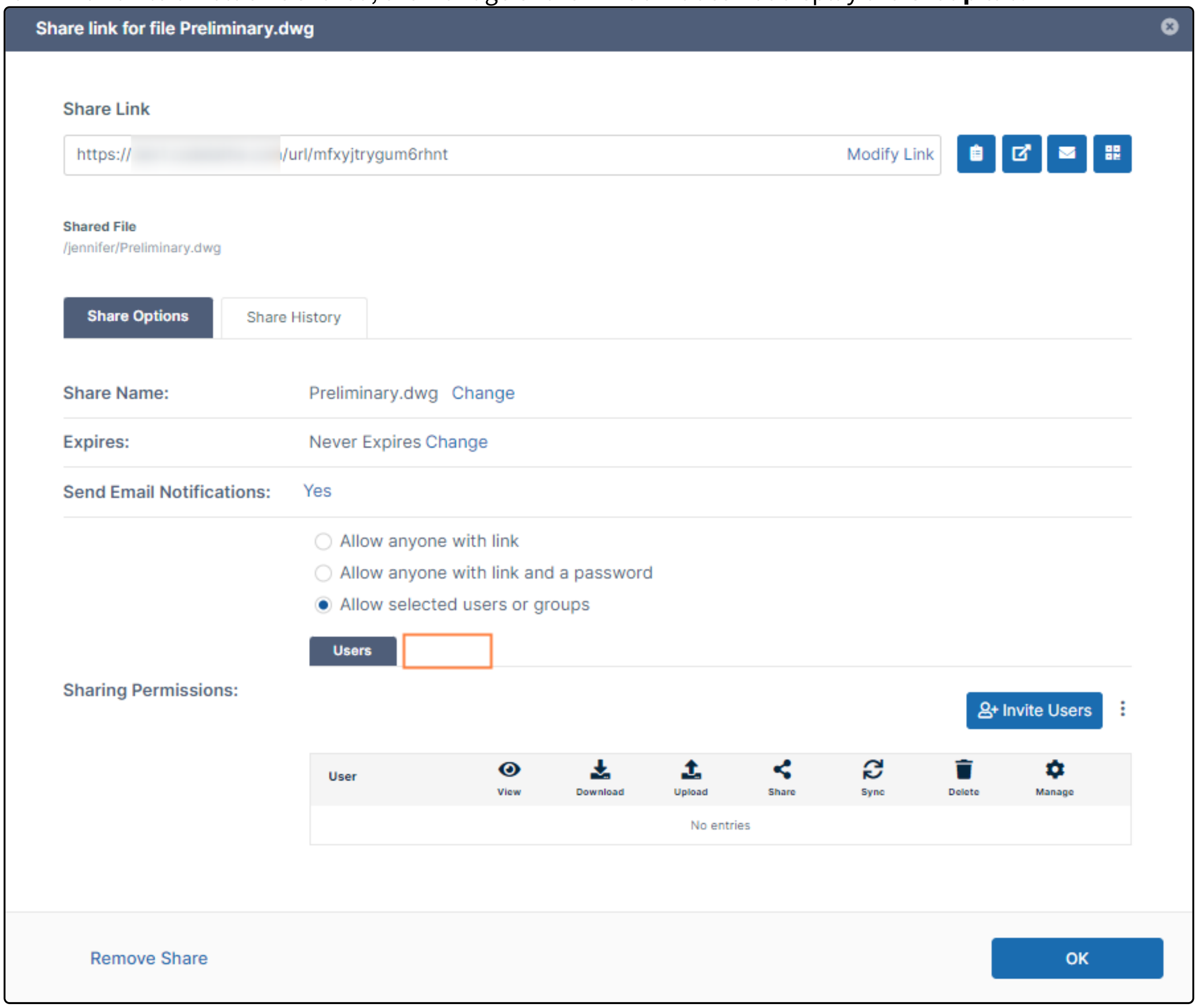
To disable users and admins from sharing to groups:

1. Open the Share settings page.

2. Scroll down to **Disable private sharing to groups** and enable it.



3. Click **Save**.
   Now when a file or folder is shared, the Manage Share window does not display the **Group** tab.



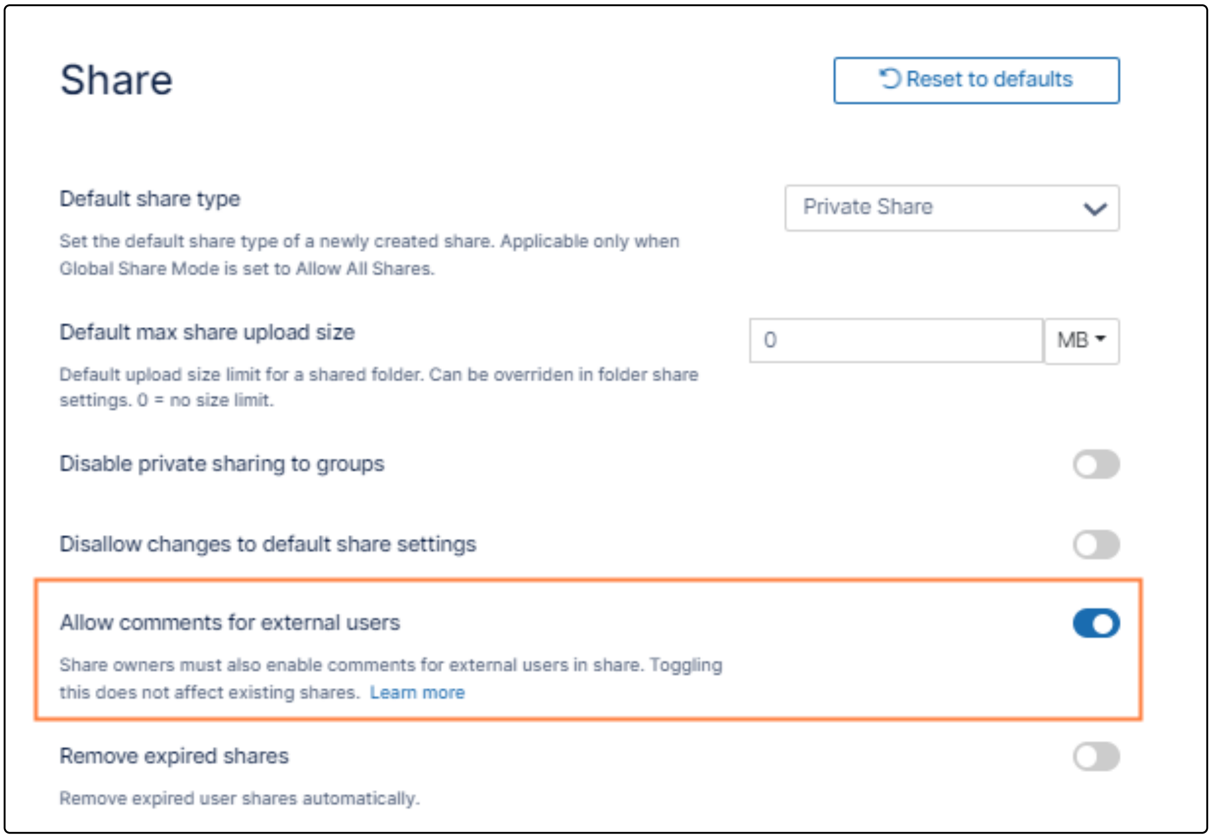
Allow External Users to Add Comments

By default, external users cannot add comments to shares. However, you can enable the **Allow comments for external users** setting to allow external users to add comments to private shares of files and folders. Note that for this setting to be effective, the share creator must also allow comments by external users and give the external user write access to the share.

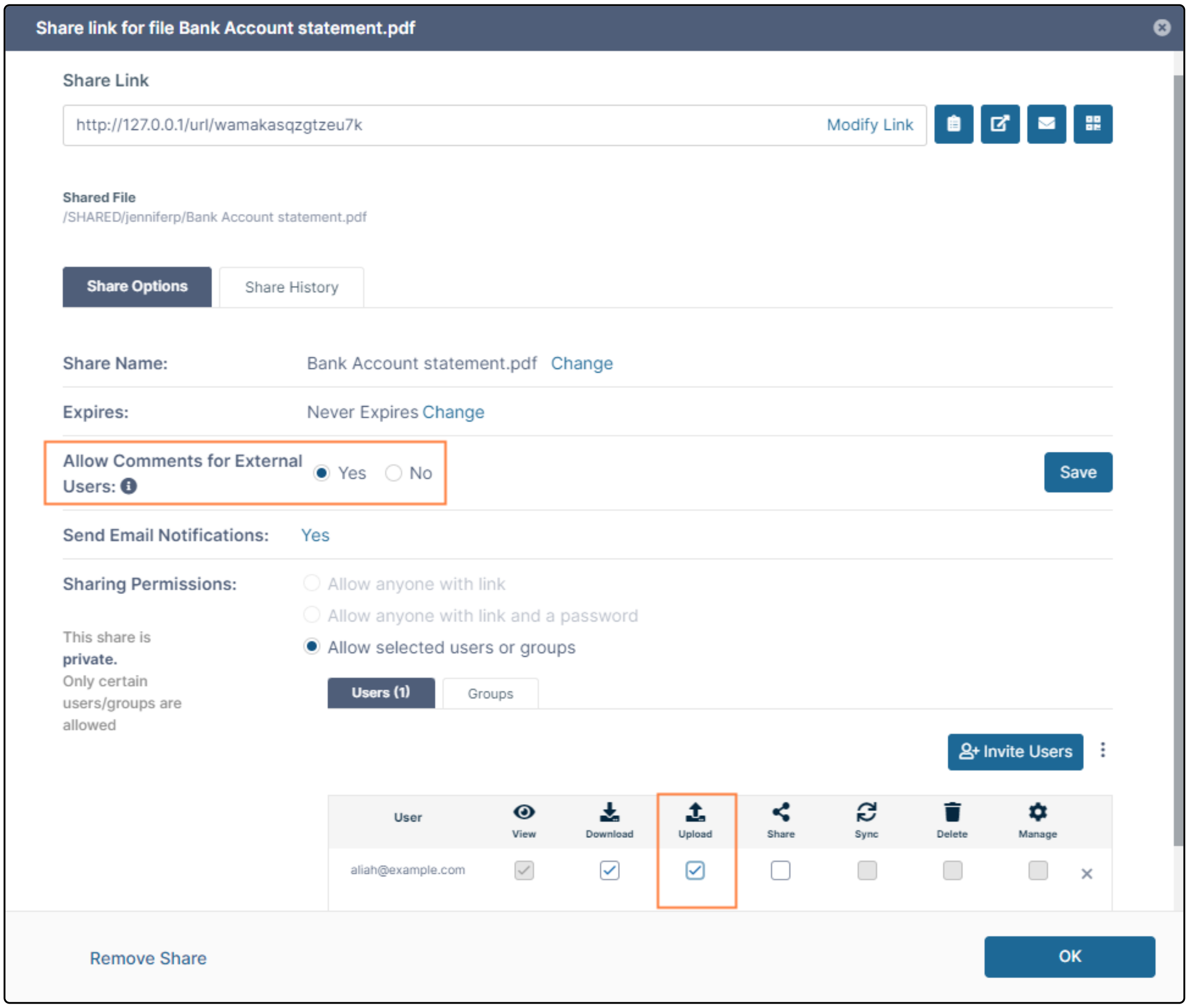
To allow external users to add comments:

1. Open the Share settings page.

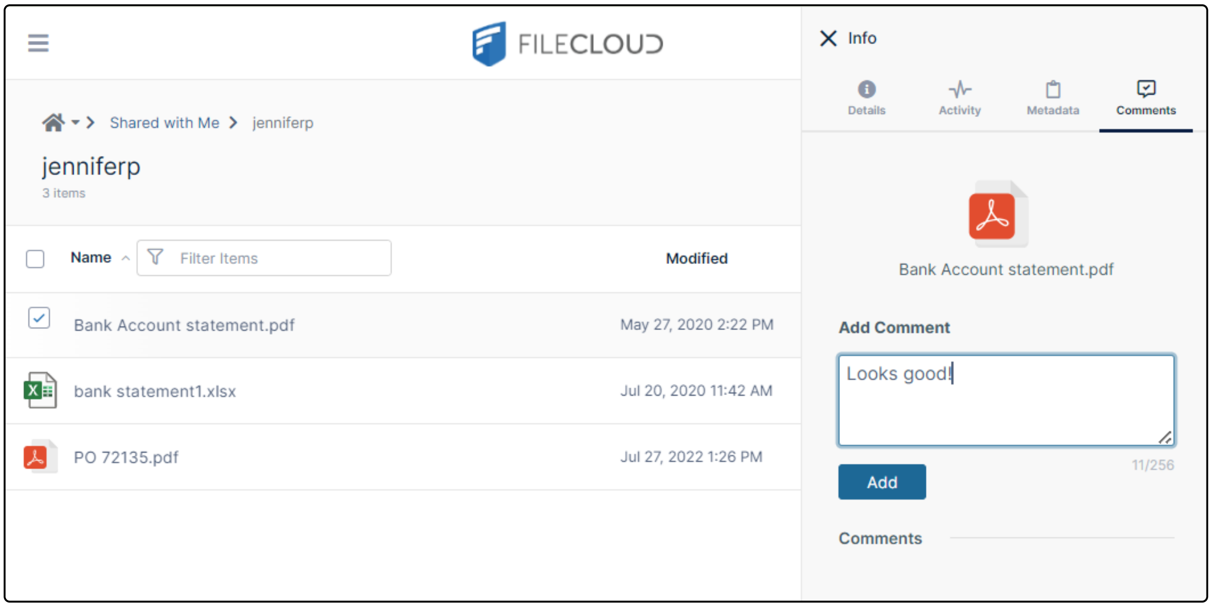
2. Scroll down to **Allow comments for external users** and enable it.



Now, if a share creator enables the option **Allow Comments for External Users** and gives the external user write (upload) access, as shown below . . .

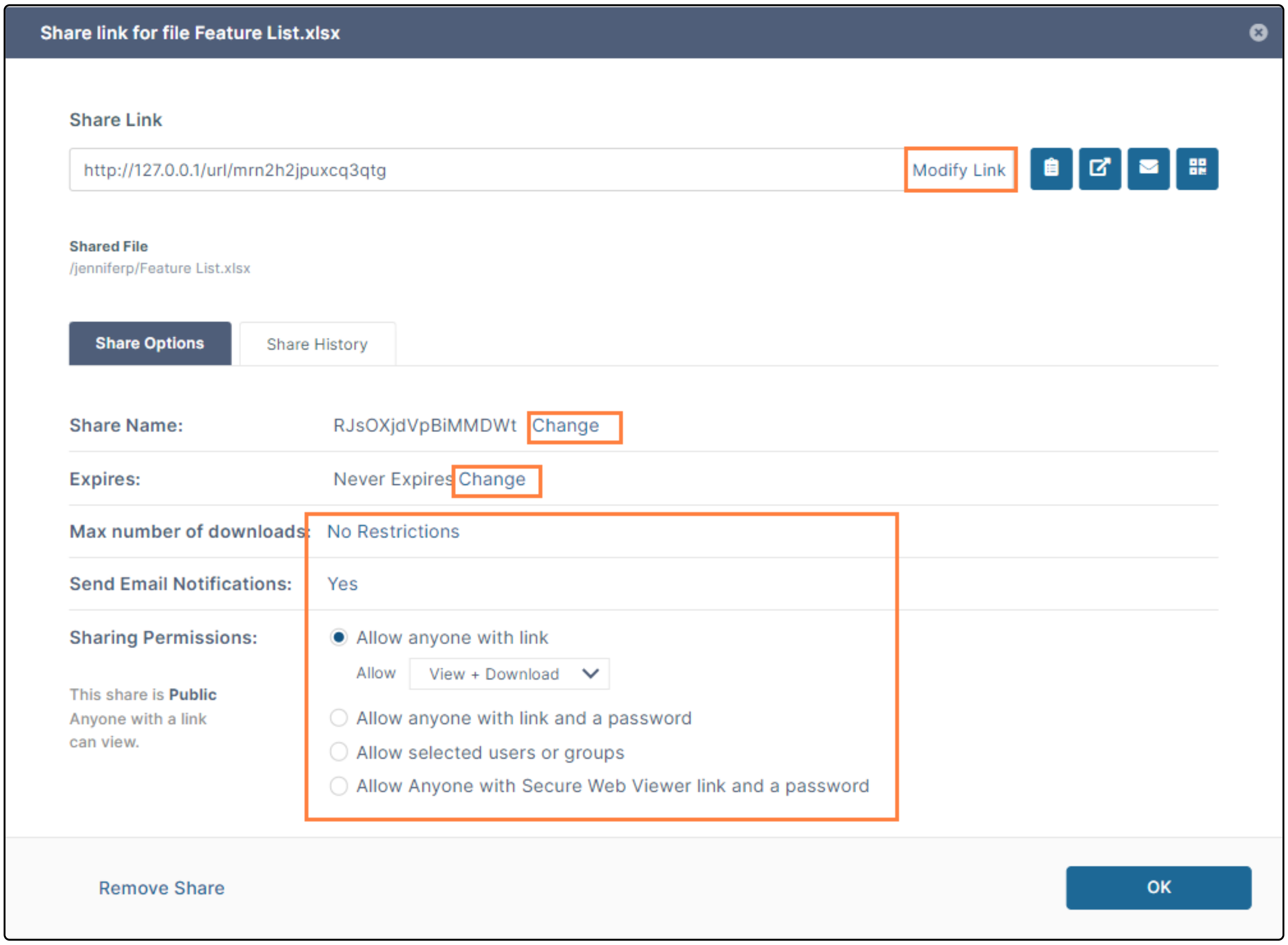


. . . the external user can select the share in the **Shared with Me** listing, click the Comments tab, and add a comment to the share:



Disallow/Allow Default Share Settings Change

The **Share link** dialog box appears with settings that the user can modify:

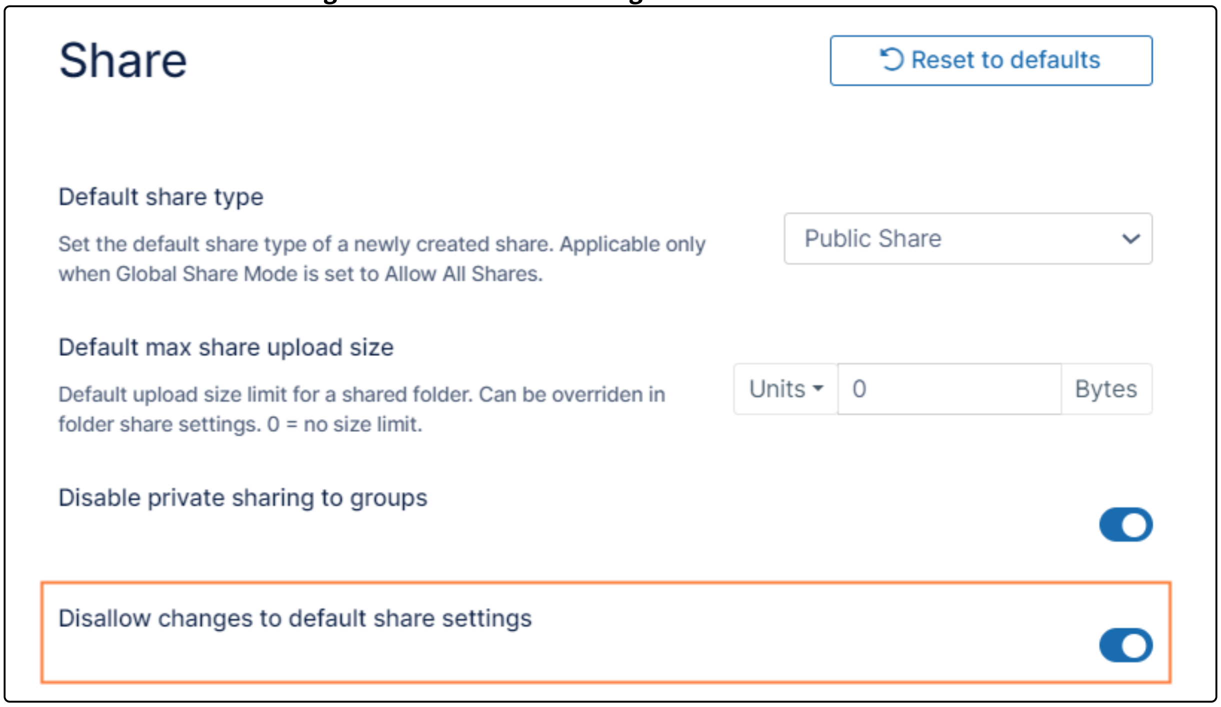


However, you can prevent users from changing these settings.

To require users to share files and folders with the default settings you have configured:

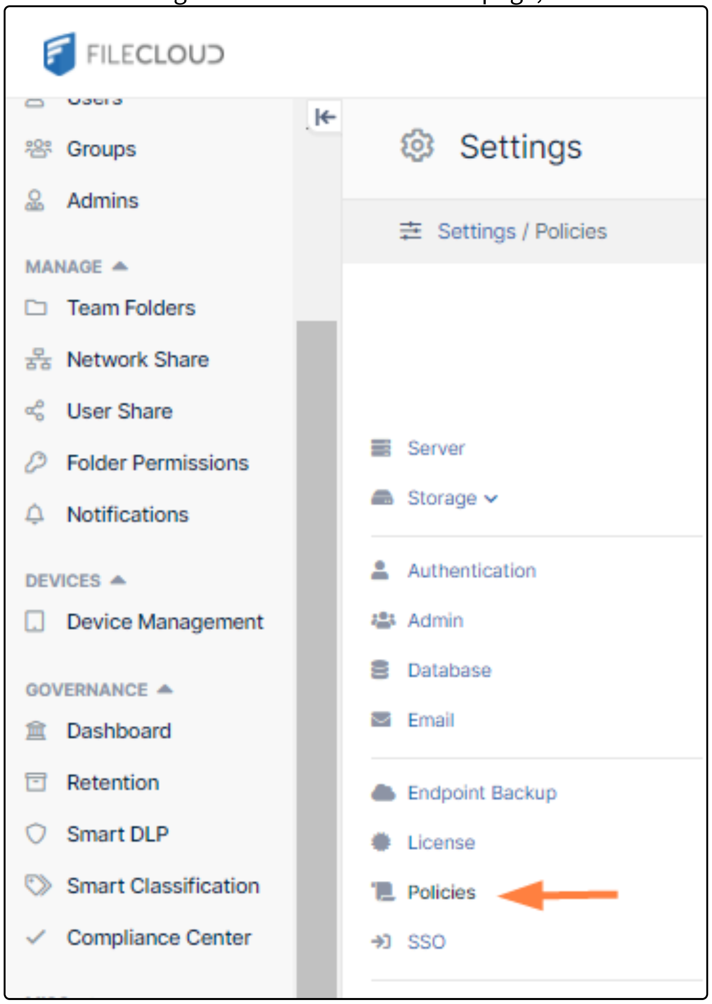
1. Open the Share settings page.

2. Scroll down to **Disallow changes to default share settings** and enable it**:**



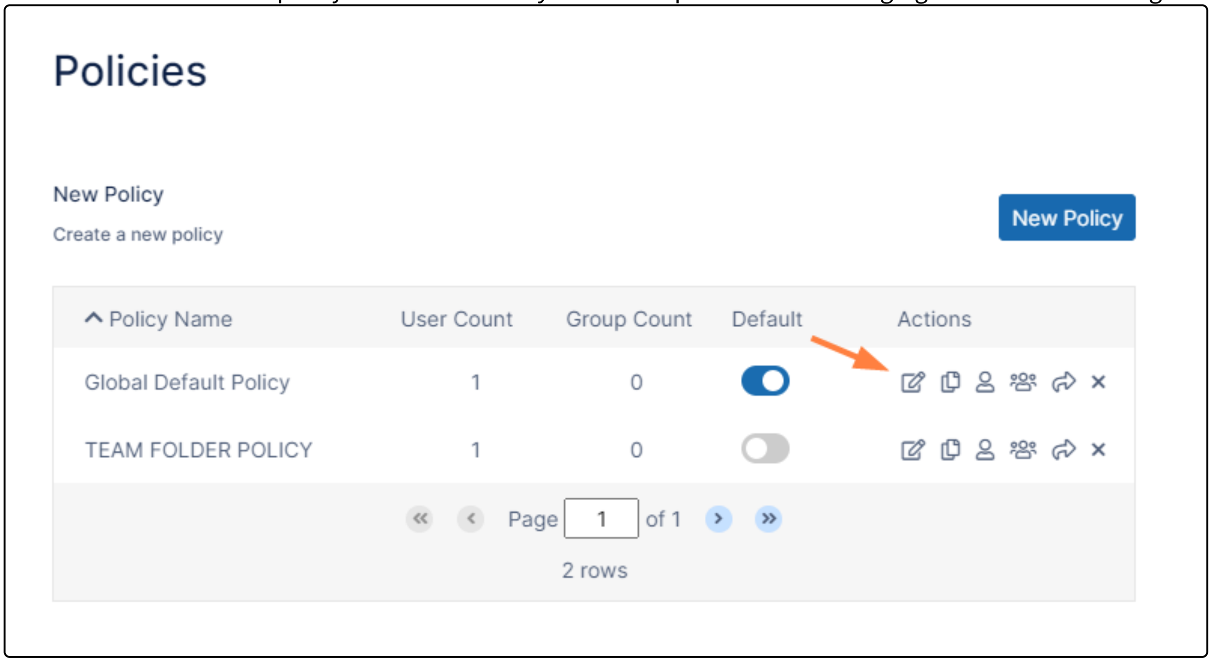
AND

3. In the inner navigation bar on the left of the page, click **Policies**

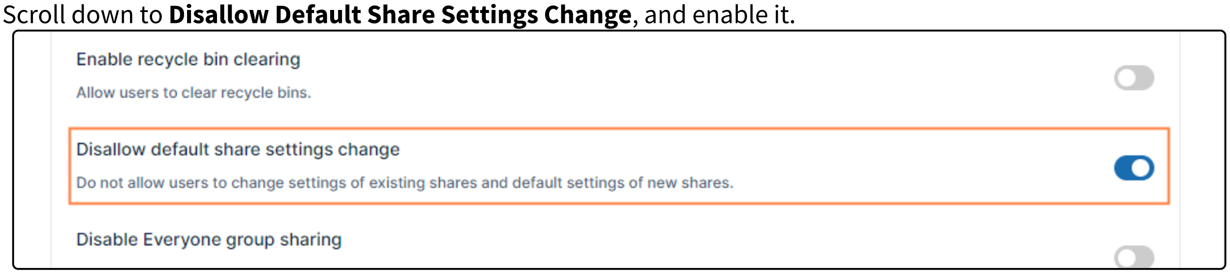


4. The **Policies** page opens.

5. Click the Edit icon for the policy of the users who you want to prevent from changing default share settings.

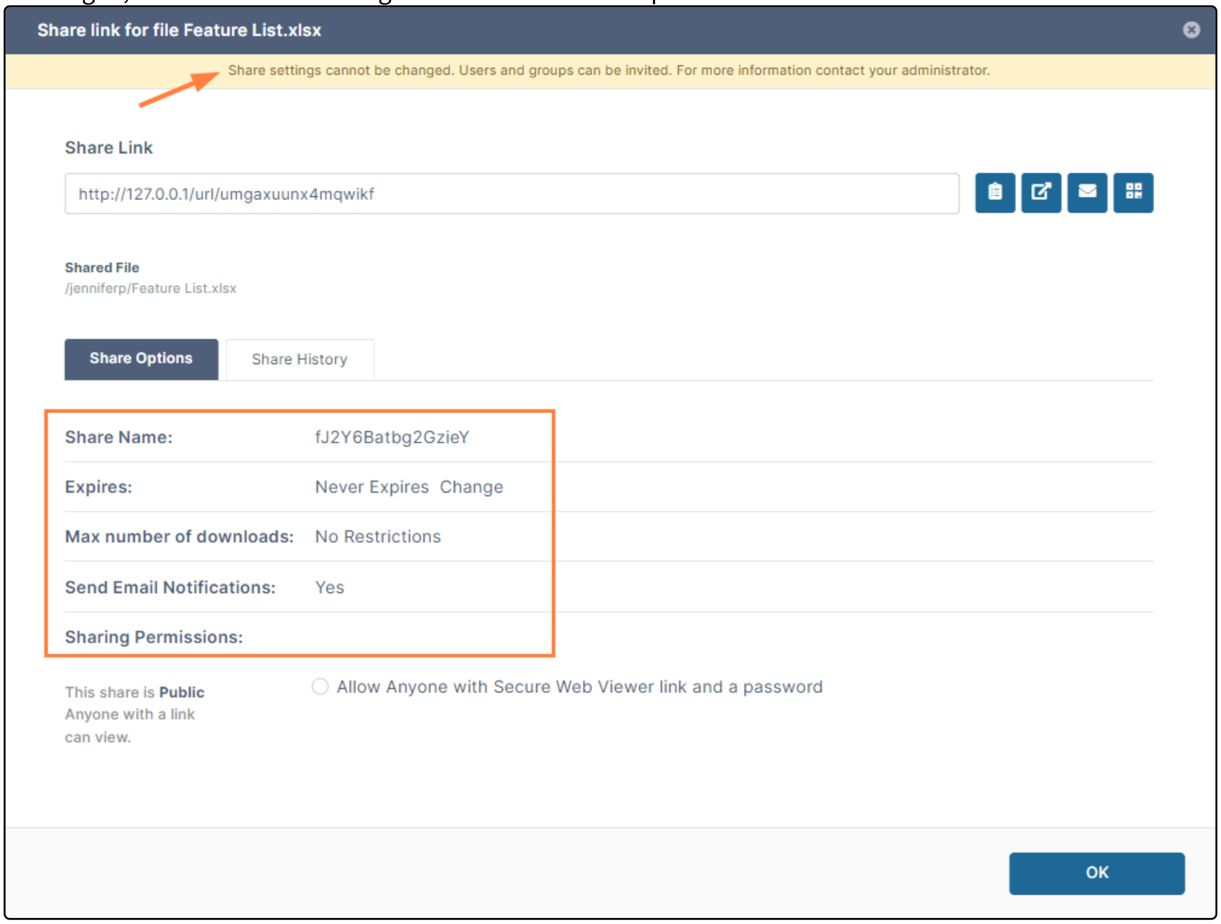


6. Click the **User Policy** tab.
7. Scroll down to **Disallow Default Share Settings Change**, and enable it.



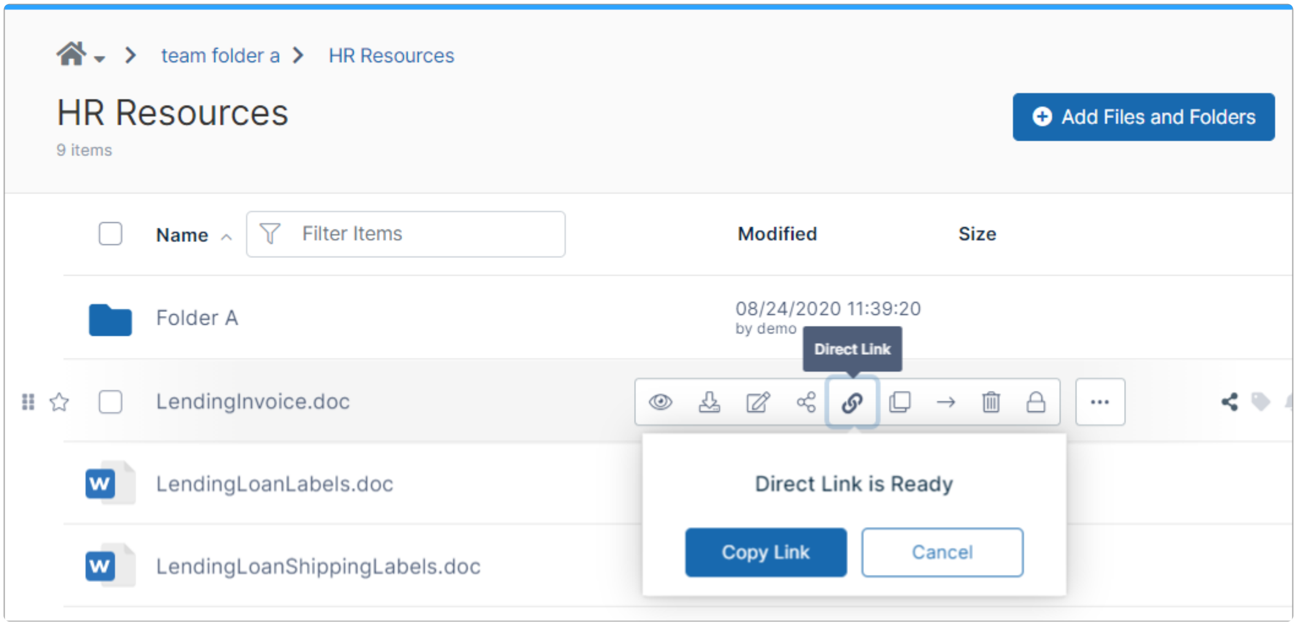
8. Repeat steps 5, 6, and 7 for the policies of all users who you want to prevent from changing default share settings.

   Now, for users with those policies, the **Share link** dialog box has a message at top that share settings cannot be changed, and there are no change buttons or clickable options:



Hide Direct Link option for shared files and folders

In the User portal, the **Direct Link** action is available when users select a file or folder in Team Folders or Shared with Me:



Beginning in FileCloud 20.2, FileCloud can be configured to hide the **Direct Link** action.

Please Contact FileCloud Support to hide the action.

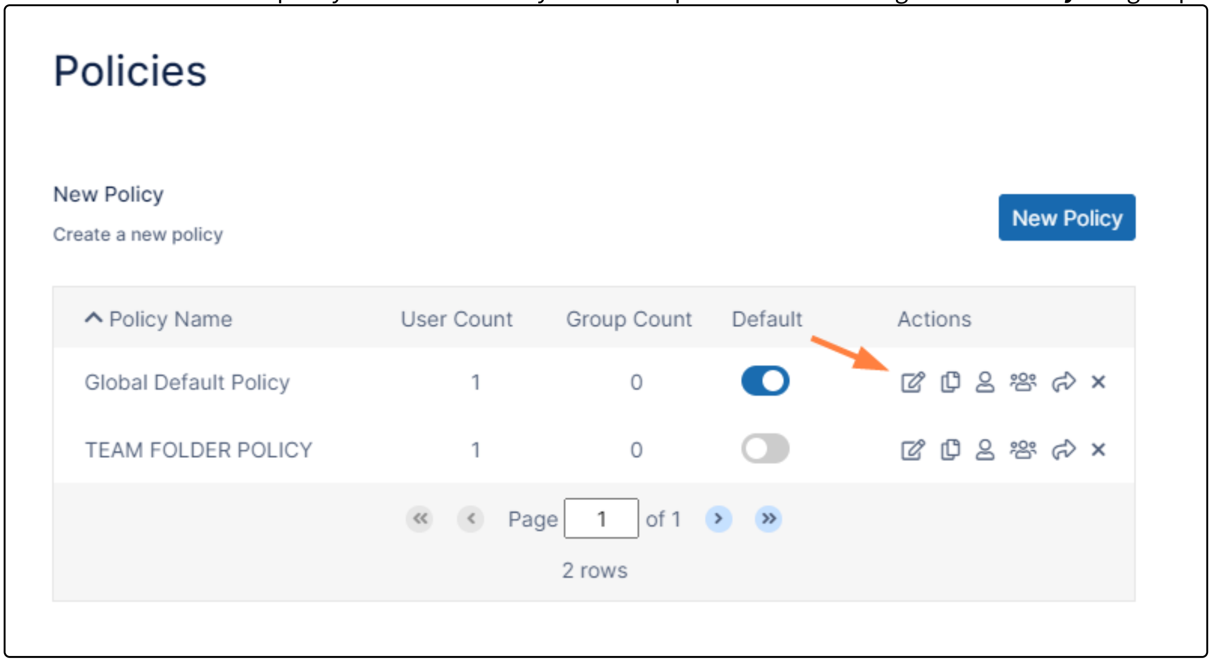
Disable sharing to the Everyone group

The **Everyone** group includes all of your active Full users. If you do not want to allow sharing of files or folders with all of your users at once, you can disable sharing to the **Everyone** group.

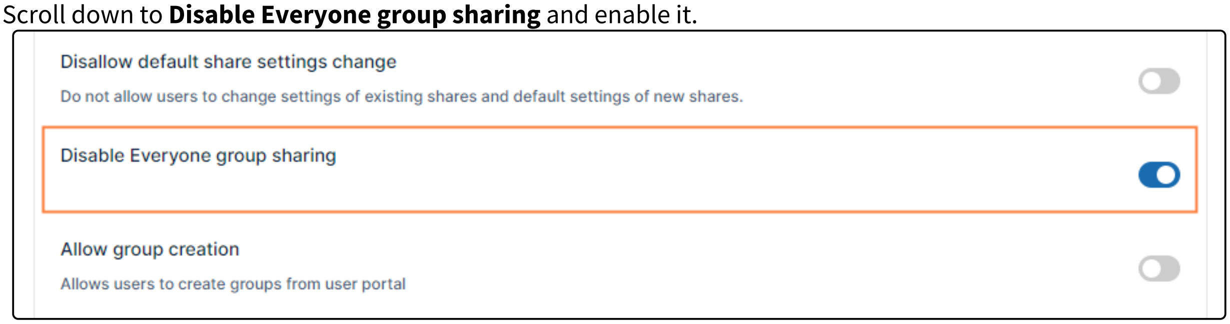
To disable sharing to the Everyone group:

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

2. Click the Edit icon for the policy of the users who you want to prevent from sharing with the **Everyone** group.



3. The **Policy Settings** dialog box opens.
4. Click the **User Policy** tab.
5. Scroll down to **Disable Everyone group sharing** and enable it.



6. Click **Save.**
7. Repeat steps 2 through 5 for the policies of all users who you want to prevent from sharing with the **Everyone** group.

   Now, when these users select a group to share with, the **Everyone** group does not appear.

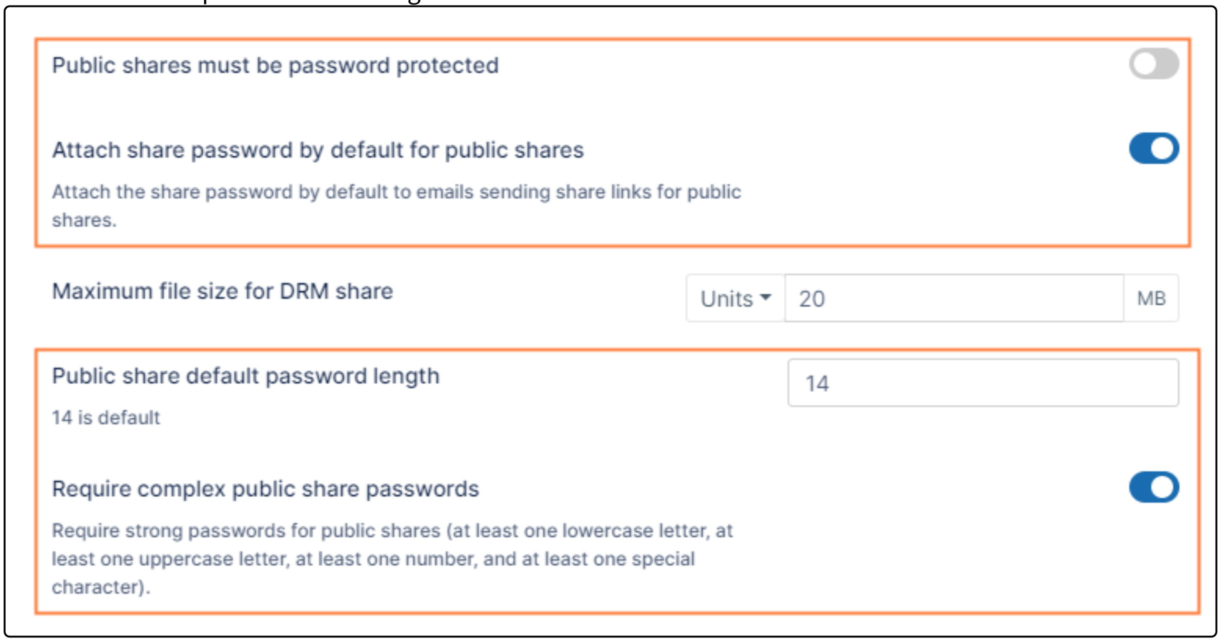
Default settings for public share passwords

There are several share settings that enable you to set defaults for public share passwords.

To access and configure the public share password settings:

1. Open the Share settings page.

2. Scroll down to the public share settings:



3. To require users to password protect public shares, enable **Public shares must be password protected**. The option **Allow anyone with link** is now unavailable when a user shares a file or folder.
4. When **Attach share password by default for public shares** is set to **enabled** (the default value), share passwords are included in share link emails sent from the share. Disable the setting to avoid including share passwords in the emails.
5. **Public share default password length** is **14**. Enter a new value to change the minimum length.
6. By default, **Require complex public share passwords** is enabled. This requires share passwords to have at least one lowercase letter, one uppercase letter, one number, and one special character. To allow users to enter any combination of characters, disable the setting.

To require users to accept FileCloud Terms of Service before accessing a public share or a password-protected share, see Terms of Service

Set the Share Mode

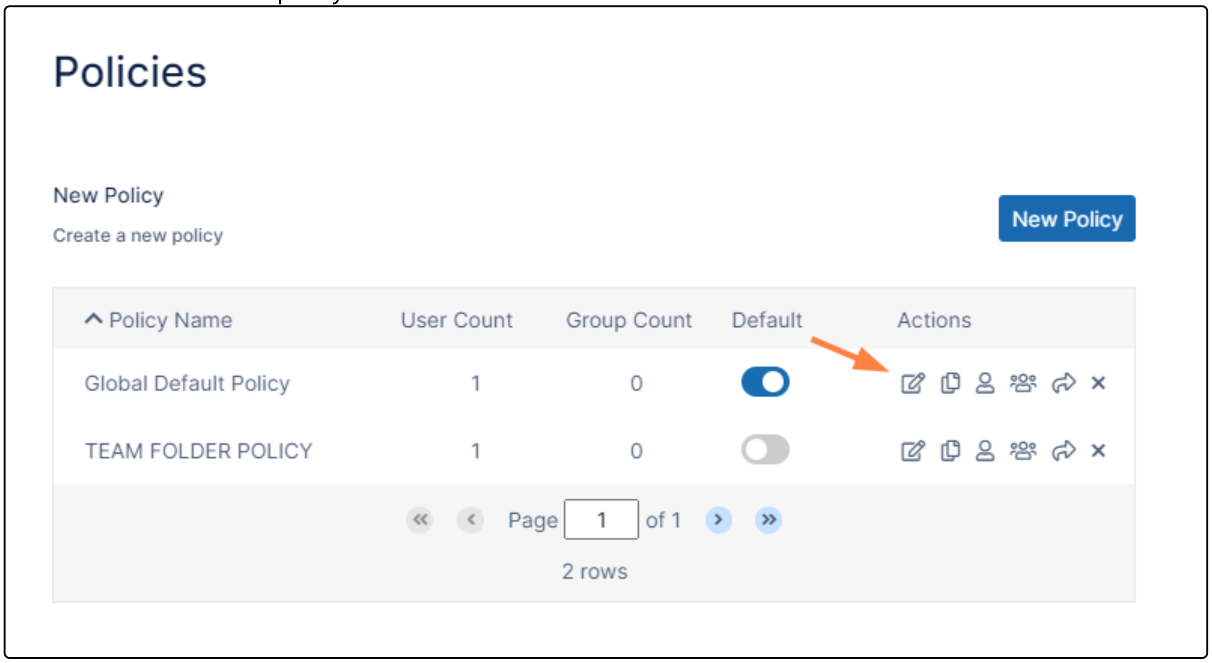
FileCloud allows administrators to manage file shares created by their users.

- You can choose to allow or restrict file sharing for accounts in FileCloud by setting the **Share Mode**.
- The **Share Mode** setting appears in policies on the **General** tab of a policy, and is set to **Allow All Shares** by default.

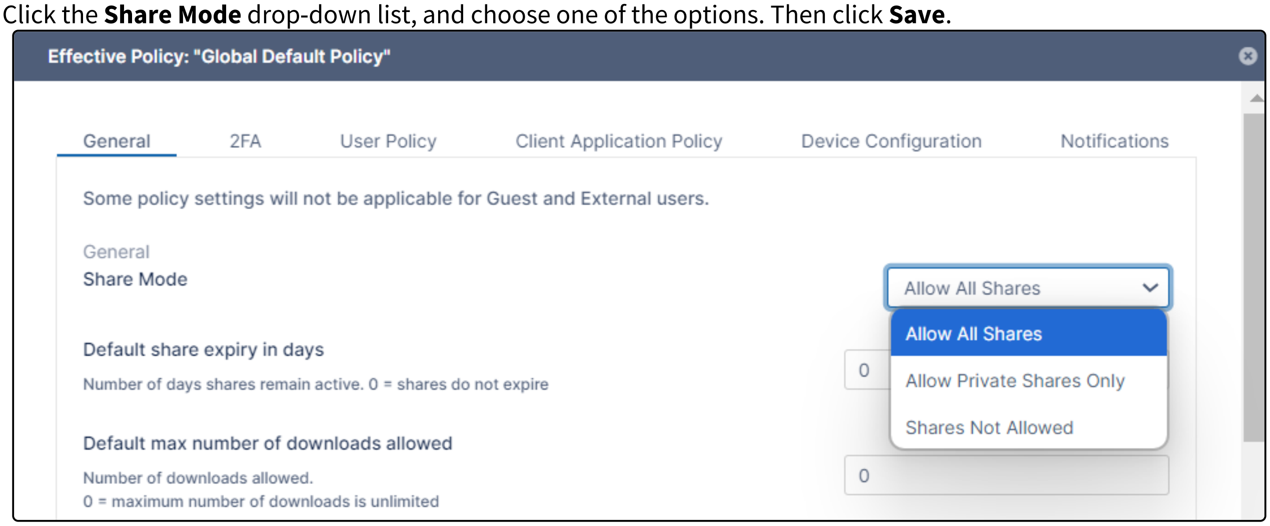
To manage the share mode for a set of users:

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

2. Click the Edit icon for the policy associated with the set of users.



3. Click the **General** tab.
4. Click the **Share Mode** drop-down list, and choose one of the options. Then click **Save**.



Option	Description
Allow All Shares	Allows users to share any file or folder with custom permissions. A file or folder can be shared with: • Anyone with access to the link (Public Share). **No FileCloud account required.** • Anyone with access to the link (Public Share) and a password. **No FileCloud account required.** • Another user in FileCloud (Private share). **FileCloud account required.** The shared files will show up in the **Shared with Me** folder.

Option	Description
Allow Private Shares Only	Allows users to share any file or folder with a user that has an existing FileCloud account. Sharing Privately requires: • The recipient(s) to be another user in FileCloud (Private share). **FileCloud account required.** The shared files will show up in the "Shared with Me" folder. • An invitation to be sent to someone to create a FileCloud account so that they can access a share. • Users to configure the share with or without restrictions.
Shares Not Allowed	Prevents users from sharing any file or folder. ⚠ If you choose this option, then no other sharing settings that you configure will be in effect.

Specify Sharing Expiration

Administrators can configure 3 main expiration features of a shared file or folder.

Feature	Options	Description
Number of days	• No expiration (0) • Expire in a certain number of days	Allow sharing to happen for a temporary time, or allow shares to exist as long as the file or folder exists.
Remove share links/shared files	• Remove the URL links to shares automatically • Remove shared files automatically	Specify what happens when a shared file or folder is no longer accessible from the Share link. • Expired URL links will be removed automatically on the next Cron run (In this case the files will not be affected.). • If you choose to remove files, they will be moved to the Recycle Bin on the next Cron run.
Notifications	• Alert users with access to a share that it will expire soon • Specify the number of days before the share expires that you want to send the email notification	You can have FileCloud send email to everyone who has access to the shared file or folder.

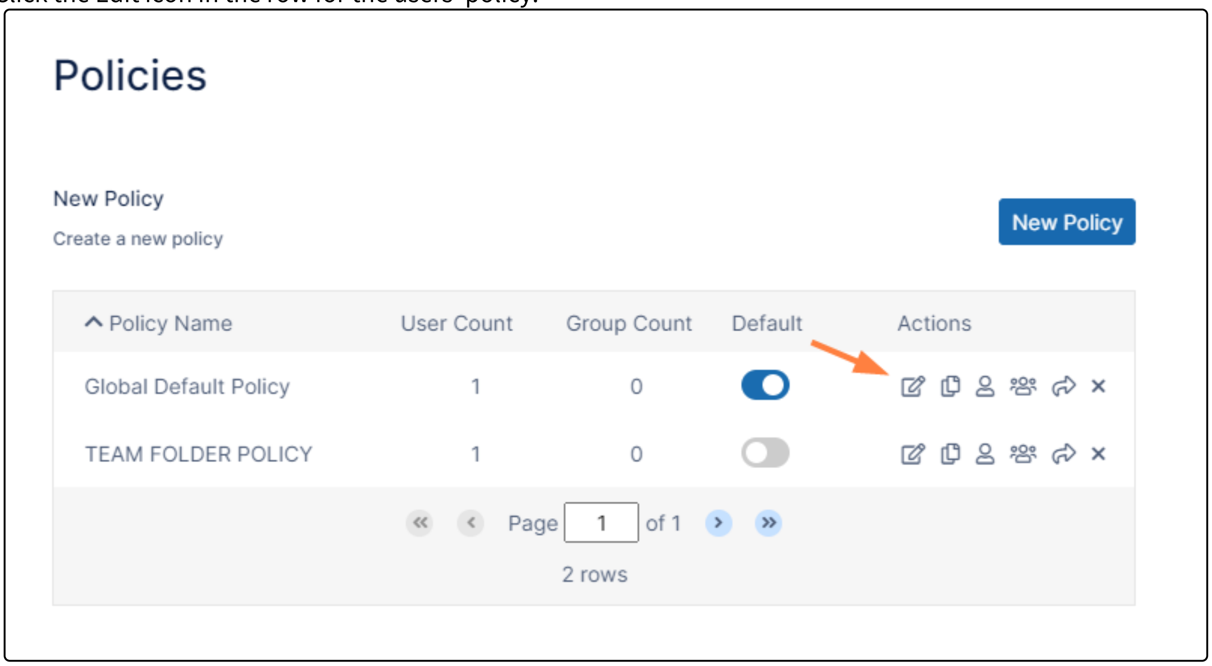
Set Expiration Period

Set Expiration Days Default

You can allow users to share files and folders for as long as they exist, or you can set the number of days that a share remains active by default.

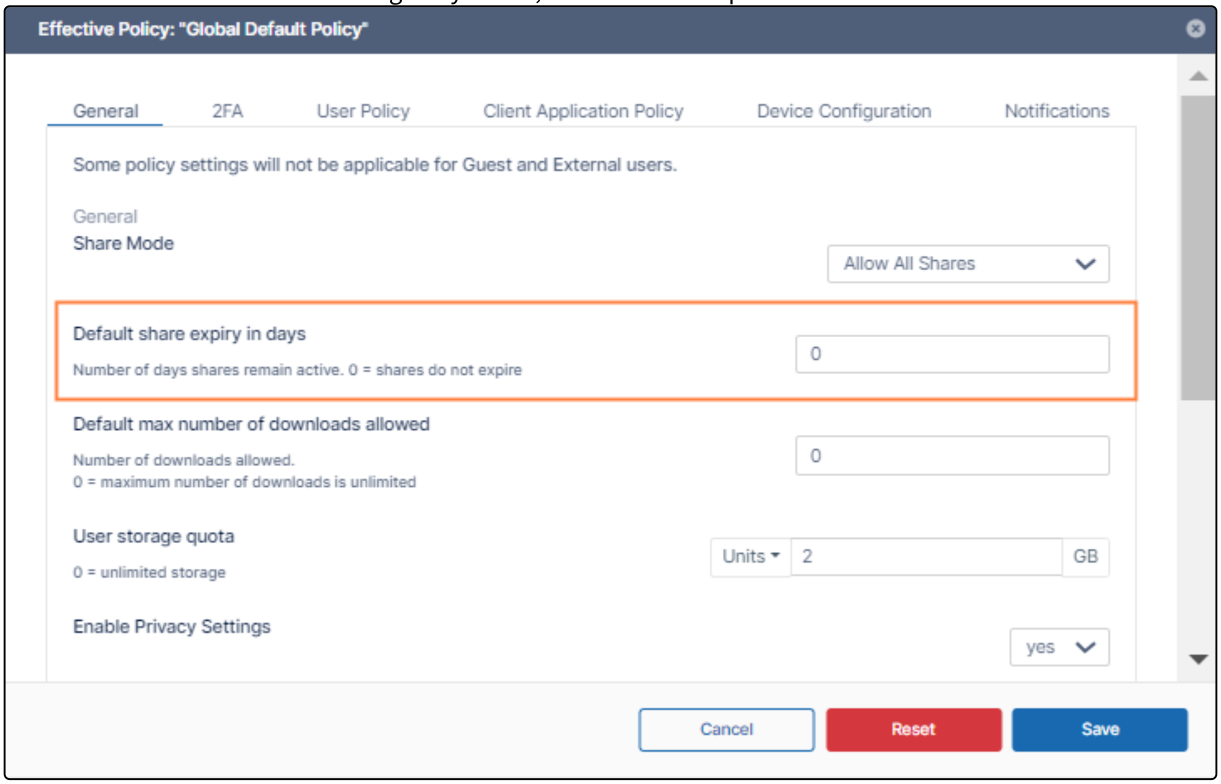
Note: This setting can be changed by the user unless **Disallow changes to default share settings** is set in the Share settings page.

To set the Share Expiry default in a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.


3. Click the **General** tab.

4. Change the value of the **Default Share Expiry in Days** setting.
   A value of **0** means that unless changed by a user, shares do not expire.



5. Click **Save**.
   The value is only changed for users who are using this policy.

Set Expiration Actions

Remove Expired Shares

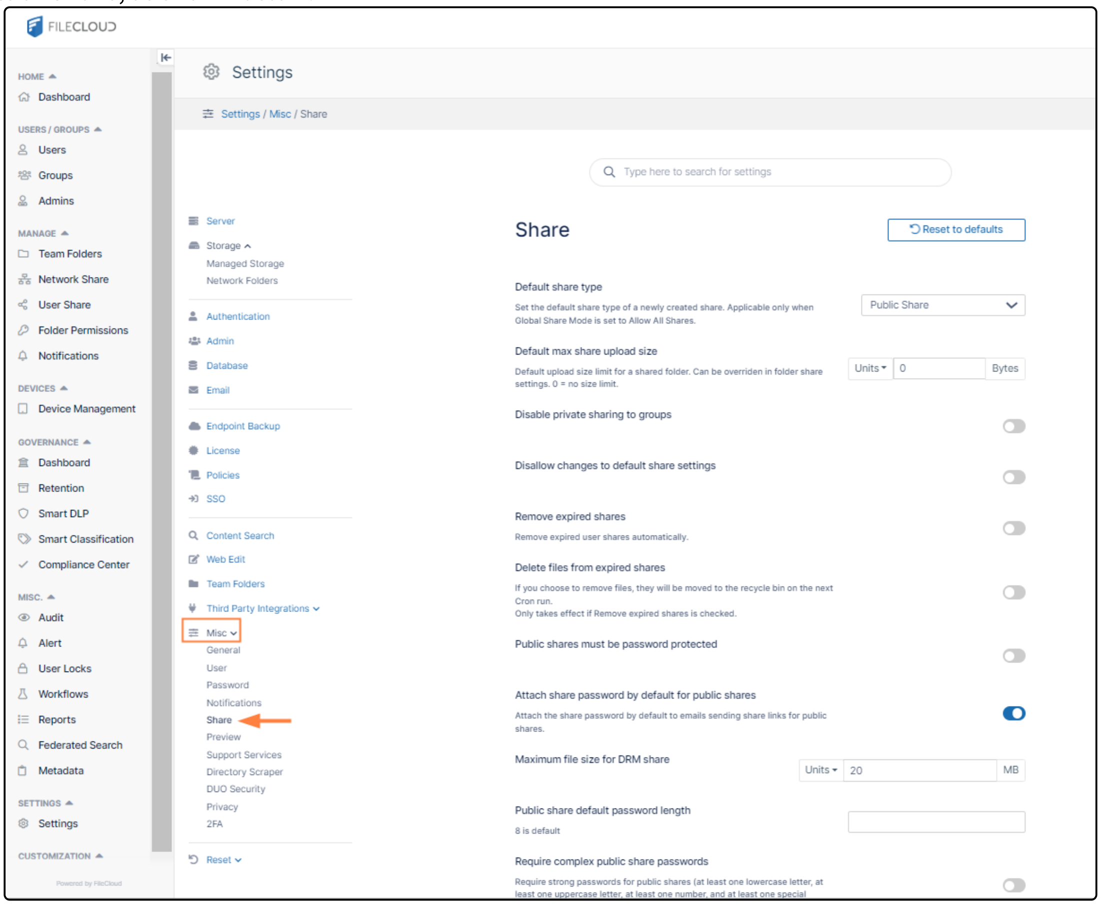
Expired URL links will be removed automatically on the next Cron run (In this case the files will not be affected.)

If you choose to remove files, they will be moved to the Recycle Bin on the next Cron run

To automatically remove expired links or expired files:

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

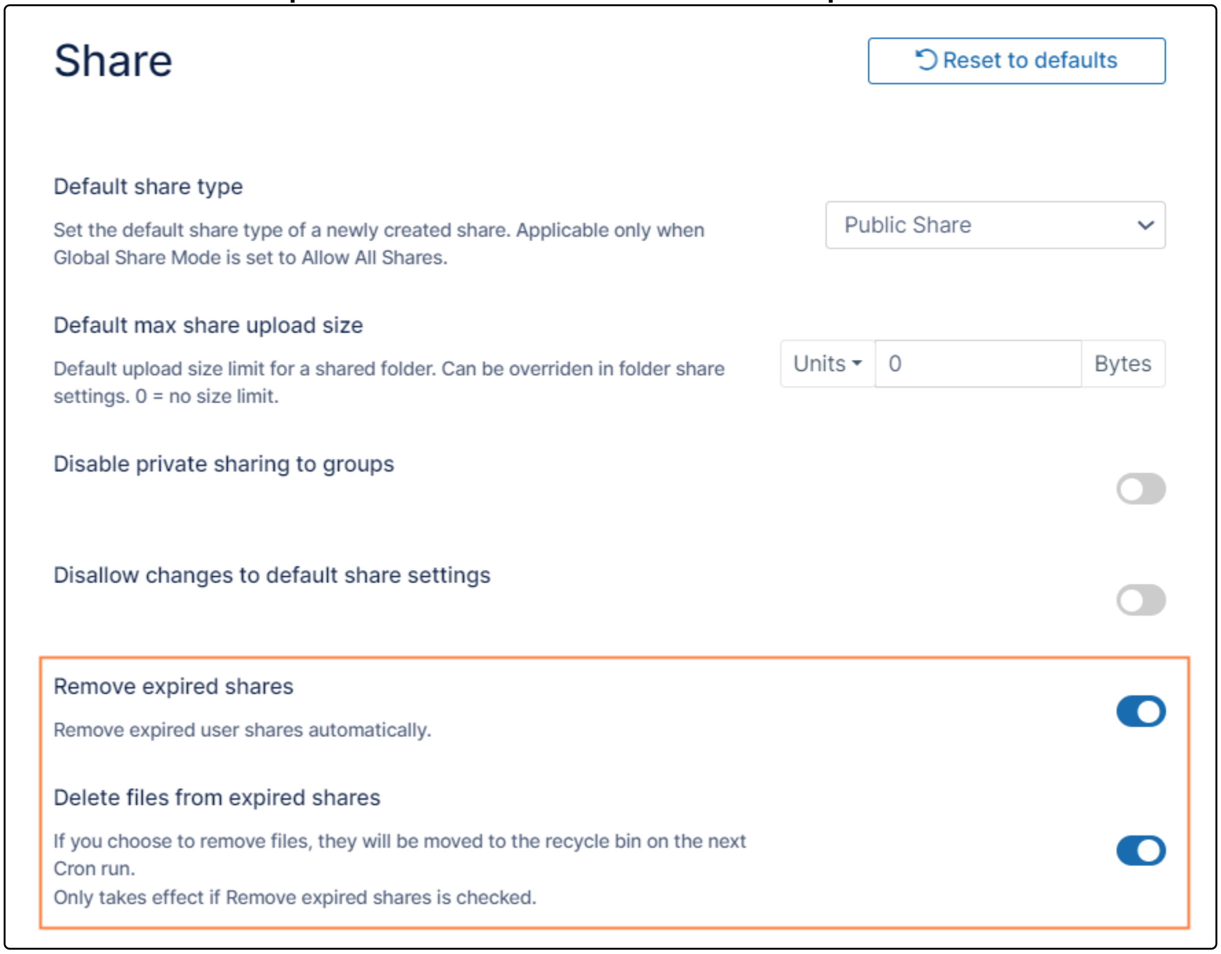
b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



The Share settings page opens.

2. Enable **Removed expired shares,**
   or
   enable both **Remove expired shares** and **Delete files from expired shares.**

Note: **Delete files from expired shares** is not effective unless **Removed expired shares** is also enabled.



3. Click **Save**.

Send Expiration Notifications

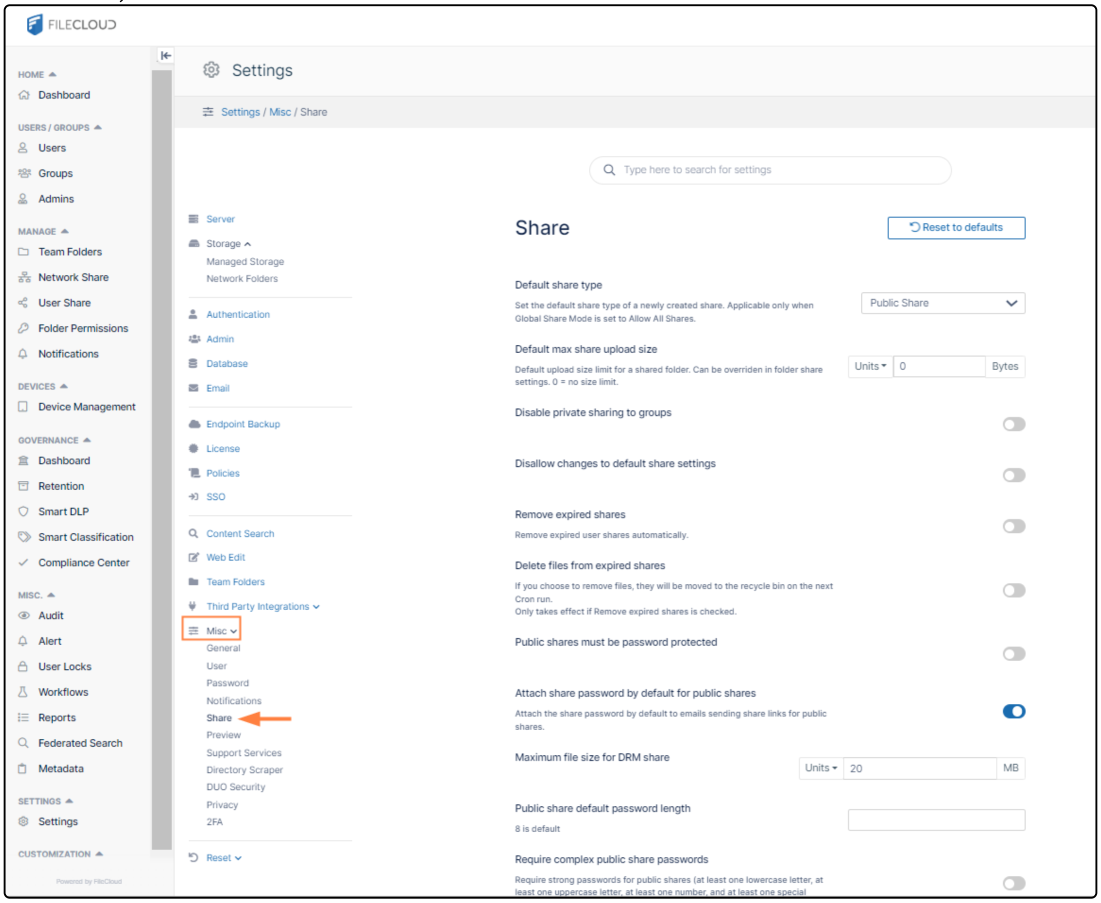
Alert share Users About Upcoming Expiration

You can have FileCloud send email to all of a share's recipients to notify them that the share will expire soon. You can also specify how many days before the share expires that the email notification is sent.

To send an email alert that a share will soon expire, and to specify the number of days before expiration the email is sent:

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

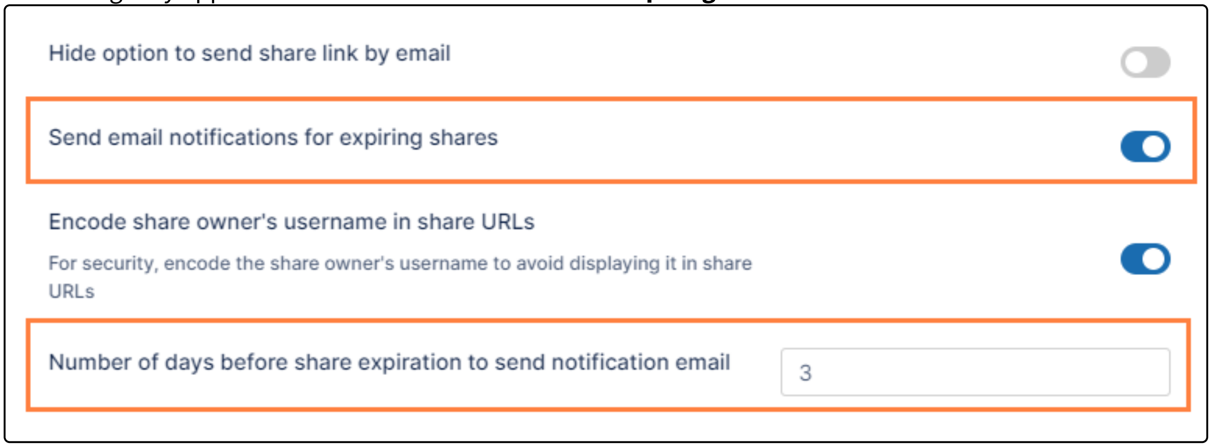
b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Share**, as shown below.



The Share settings page opens.

2. Scroll to the bottom of the page.
3. To send emails notifying share recipients that shares are expiring, enable **Send email notifications for expiring shares**.
   By default, the number of days before a share expires that an email is sent is **3**.
4. To change the number of days before a share expires that an email is sent, change the value in **Number of days before share expiration to send notification email**.

This setting only applies if **Send email notifications for expiring shares** is enabled.



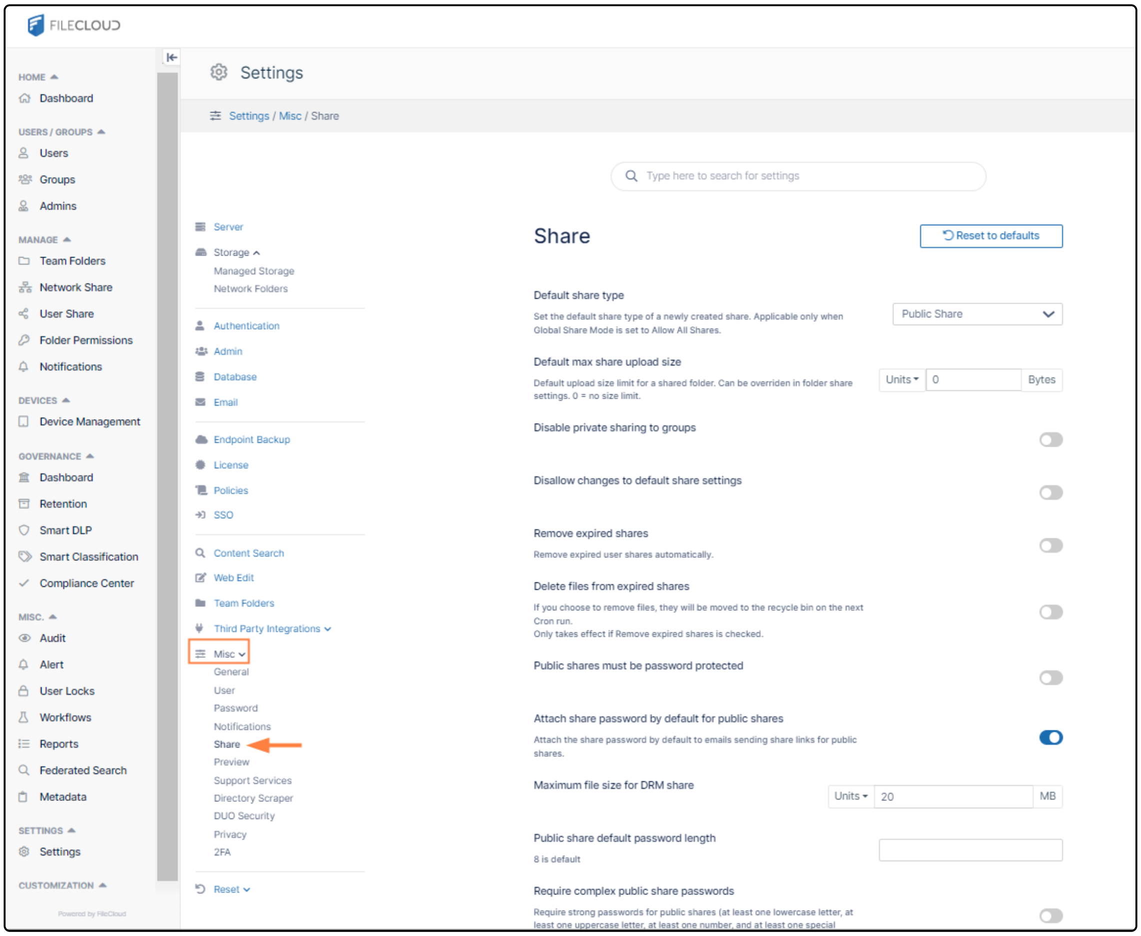
Secure Shares

Instead of just communicating the most secure sharing procedure to your users, administrators can configure special settings to ensure a more secure environment when users are sharing files.

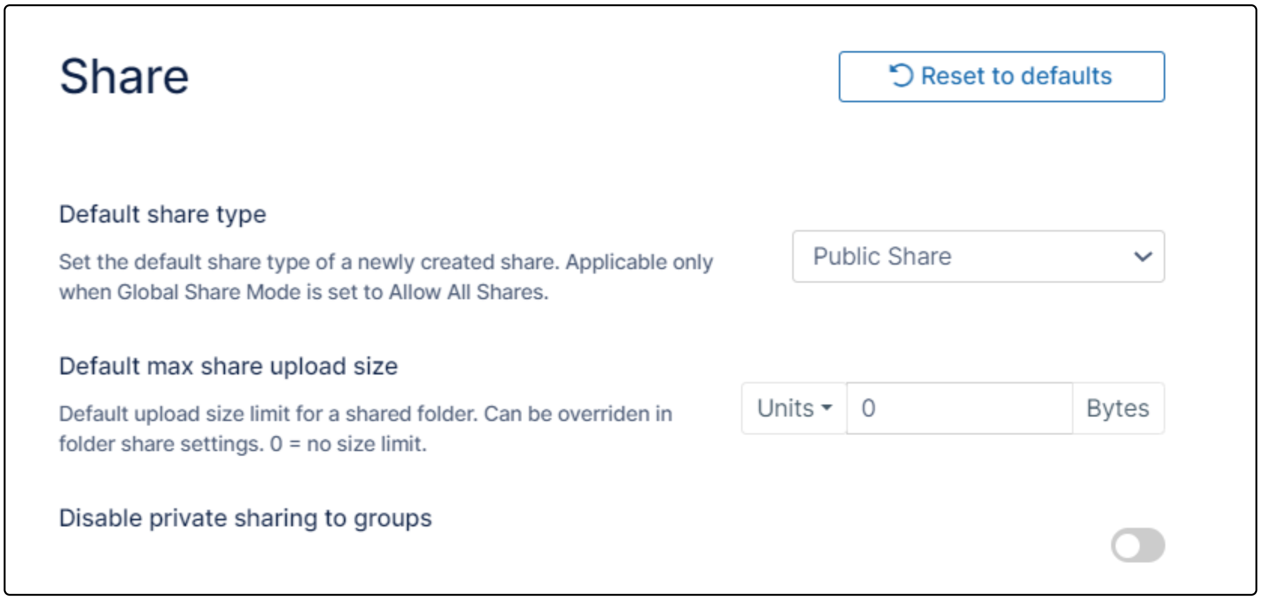
To password protect shares, prevent share name changes, or hide the option for sending share links by email:

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

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

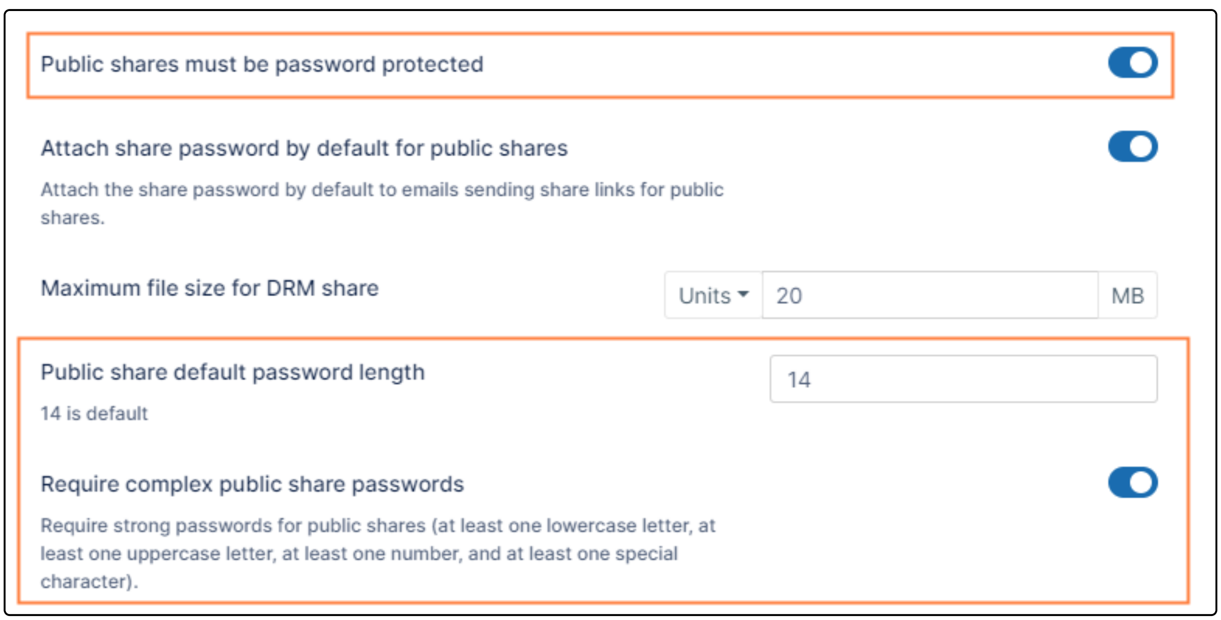


The **Share** settings page opens.



2. Configure any of the following secure share settings:
   Password Protect Shares and Require Complex Passwords

   Administrators can require users to create all public shares with a password for an extra layer of security. Users cannot disable the use of passwords when this is set.
   By default, FileCloud requires public share passwords of 14 characters in length that include at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character. Administrators may change these settings.



   To require strong password protection:

   a. In the **Share** settings page, scroll down to the password settings.
   b. Enable **Public shares must be password protected**.

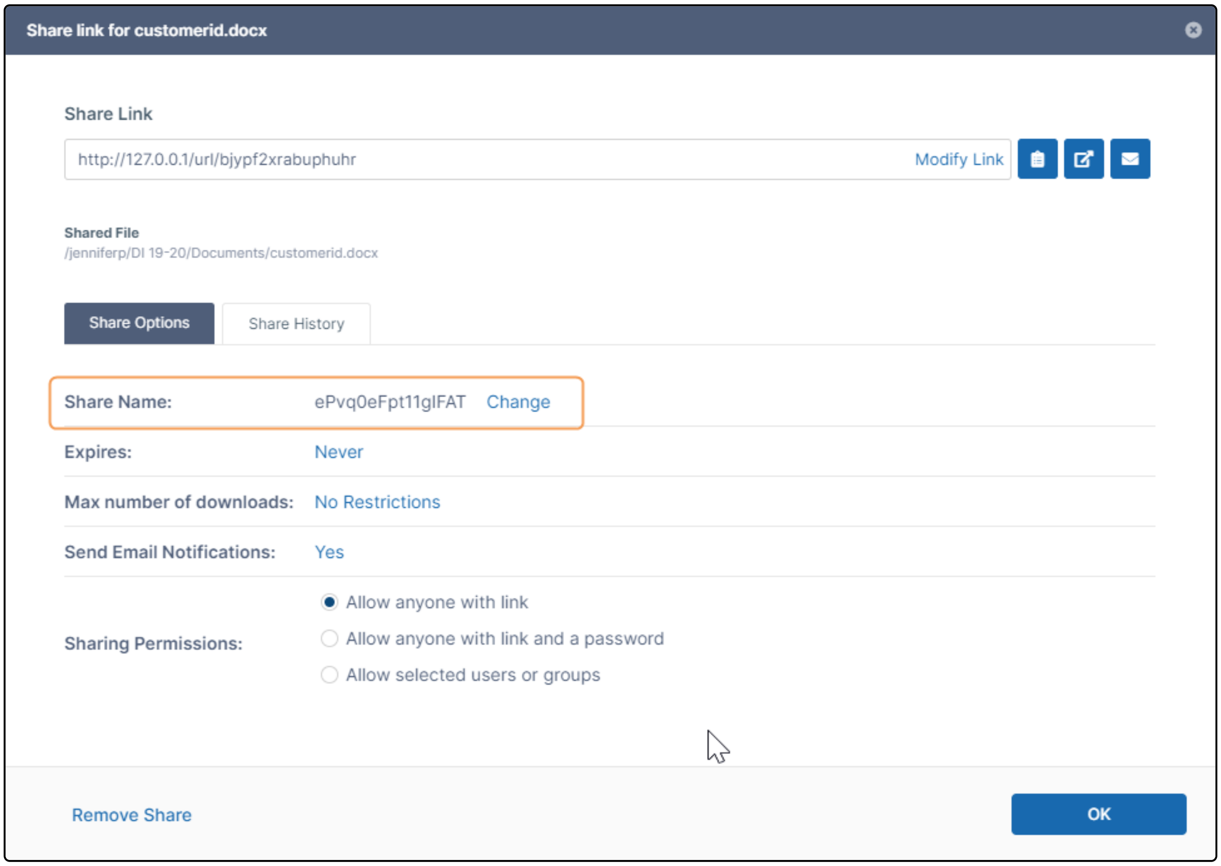
c. Leave **Public share default password length** at **14**, or change it to another number.
d. Leave **Require complex public share passwords** enabled.

Disallow Share Name Change

For security reasons, shares have a randomly generated name that is created by default.

- Randomly generated names are more difficult for attackers to guess.
- Randomly generated names do not expose user names or a description of the data.

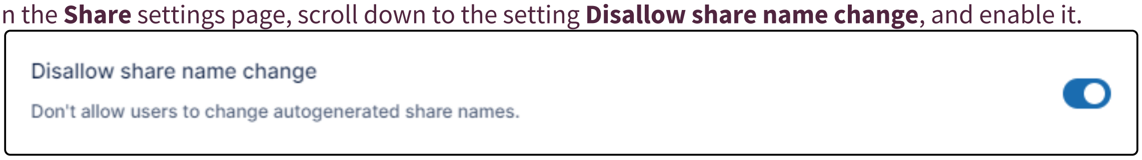
This is how the randomly generated name looks in the user portal when creating a share:



By default, users may change randomly generated share names to custom names. However, you may prevent users from changing share names.

To prevent users from changing randomly generated share names:

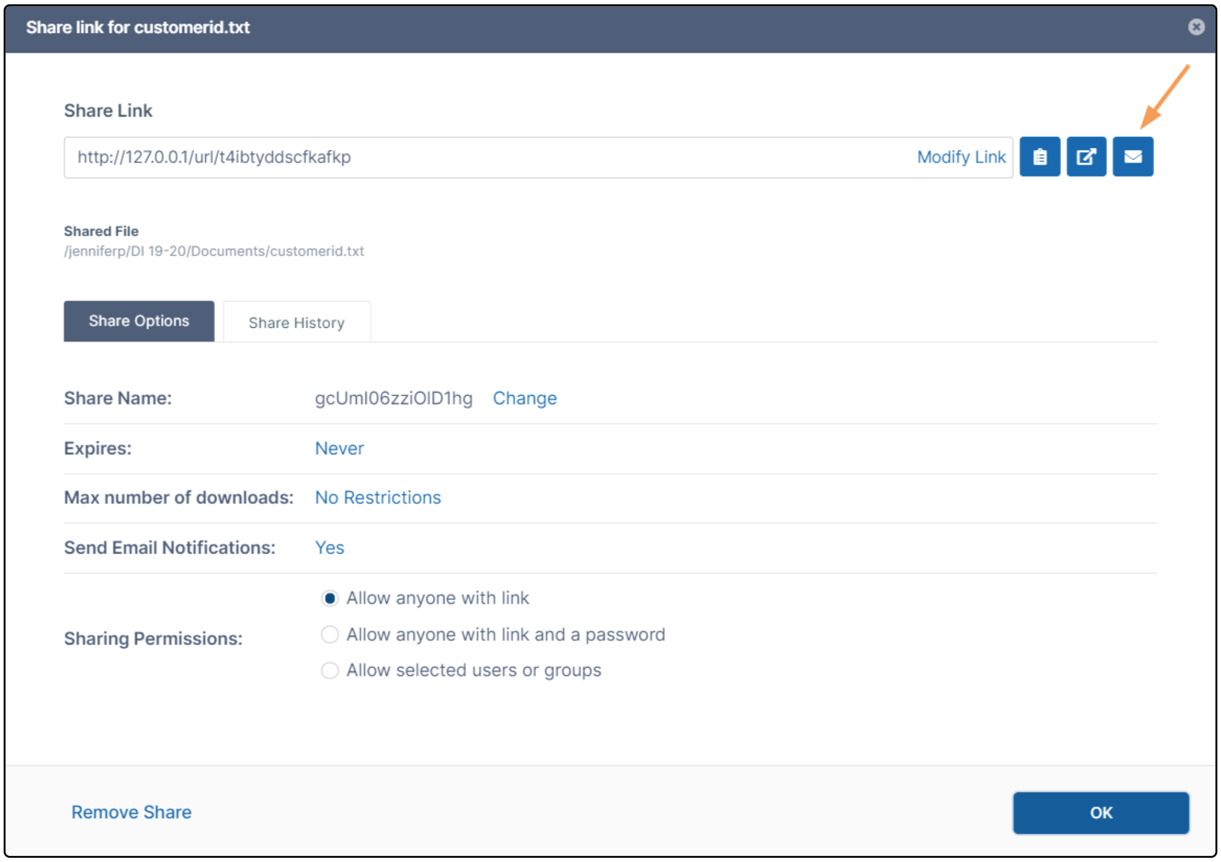
a. In the **Share** settings page, scroll down to the setting **Disallow share name change**, and enable it.



b. Click **Save**.

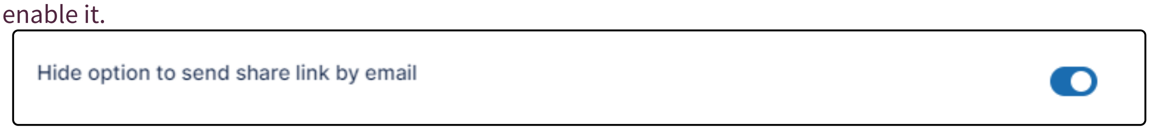
Hide Send Share Link Via Email

Users can send a share link by email by clicking the mail icon shown in the following image. To secure share links, you can hide the mail icon to make it unavailable to users.



To hide the option for sending a link to the share in email:

a. In the **Share** settings page, scroll down to the setting **Hide option to send share link by email**, and enable it.



b. Click **Save**.

To limit user account searches:

Limit User Account Searches

You can limit how users search for other user accounts.

By default, when user1 shares a file or folder with user2, user1 can search for user2's account by the user name or email id. The search results list both exact and partial matches.

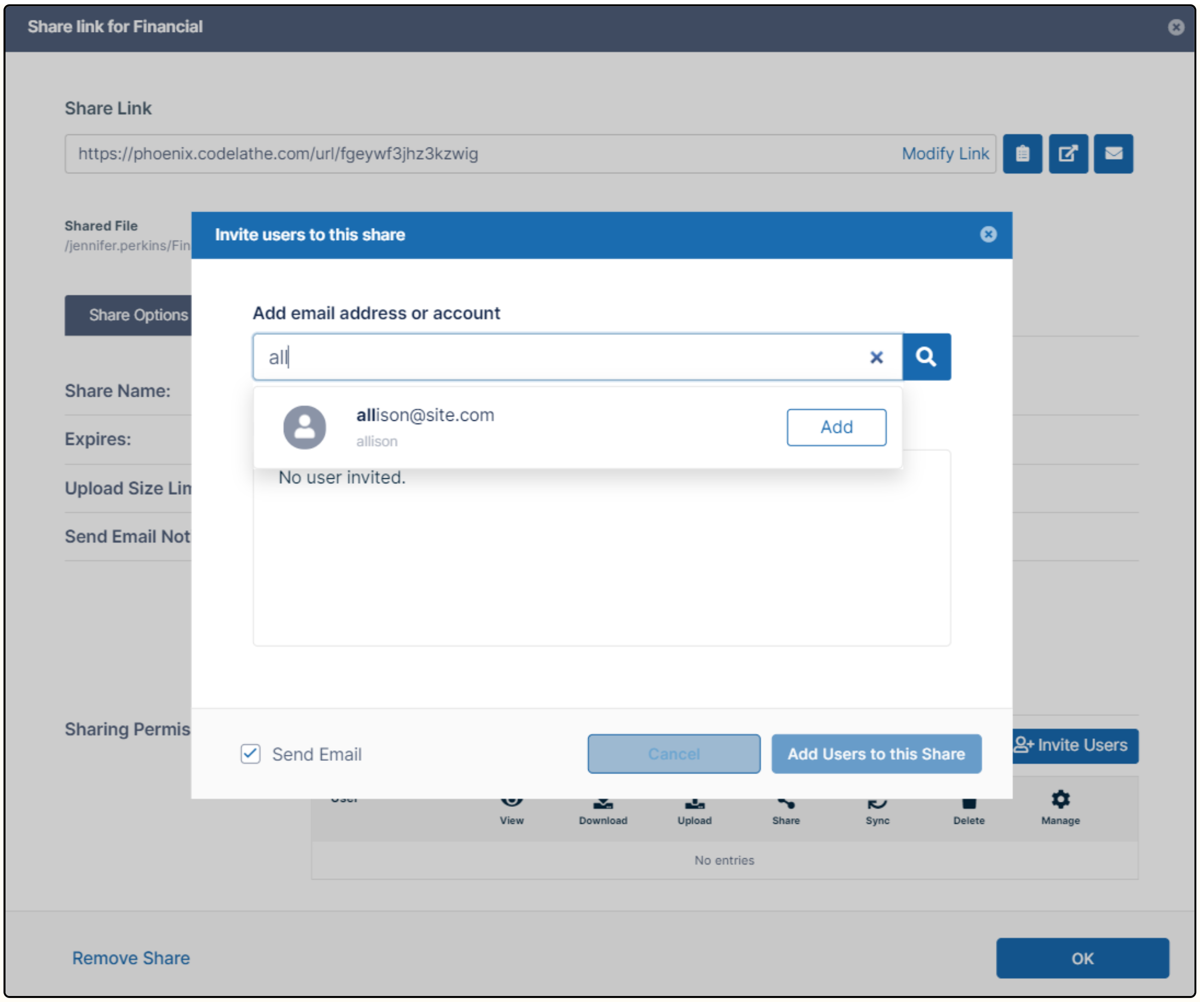
However, this is not desirable in certain cases and organizations, as the search results reveal user accounts that exist in the FileCloud system.

Therefore, FileCloud allows you to restrict user searches using two search modes:

User Account	User Account Type
• Exact Email Search With Explicit Account Invite • Exact Email Search With Implicit Account Invite • Exact Name/Email Search • Partial Name/Email Search	• ALL • FULL • GUEST • EXTERNAL
How to enable User Account Search Mode	How to enable User Search Account Type
NOTE: You can use these search limitations together. For example, you can set the **User Account Search Mode** to **Partial Name/Email Search**, and then use the **User Account Type** search mode to limit the results to only accounts with FULL access.	

Note

Using a search mode limits account searches for all the users in the FileCloud system.
These settings affect searches in shares for share recipients.



To make it clearer which user has shared a file:

Use Display Name as well as User Account Name

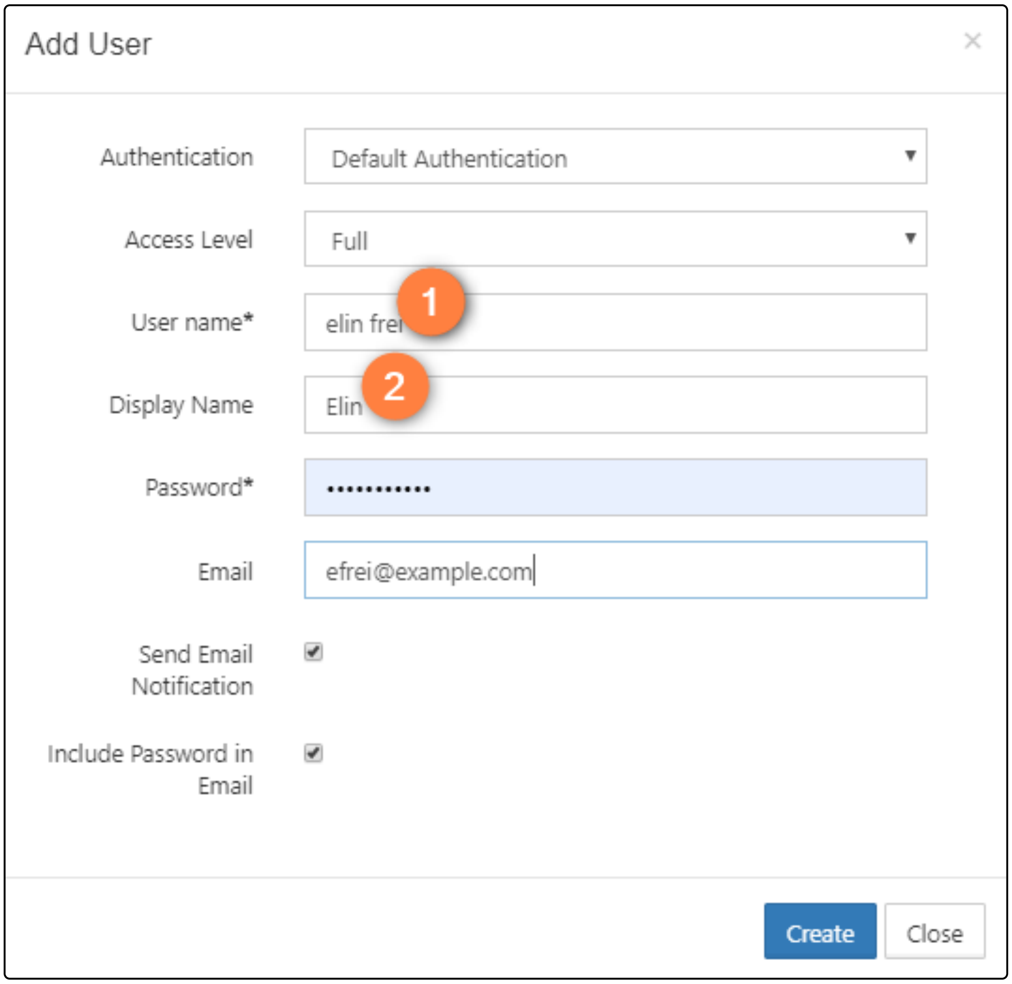
To make it clearer which user has shared a file, you can change how a user name is displayed in sharing details.

How user names are defined in FileCloud

In the admin portal, when you create a user, you set 2 different names.

1. **User name**
   - In the user portal, by default, FileCloud displays the **User name**.
   - It may not be clear to users who is sharing the file with them, especially if **User name** includes only abbreviations and numbers.
   - The **User name** cannot be changed after the user has been created.
2. **Display name**

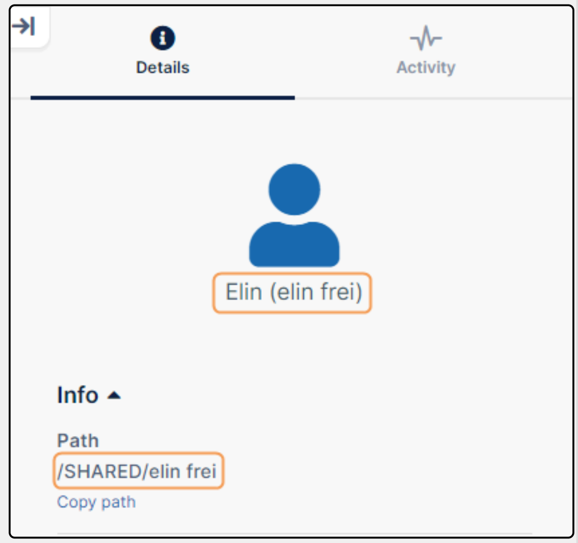
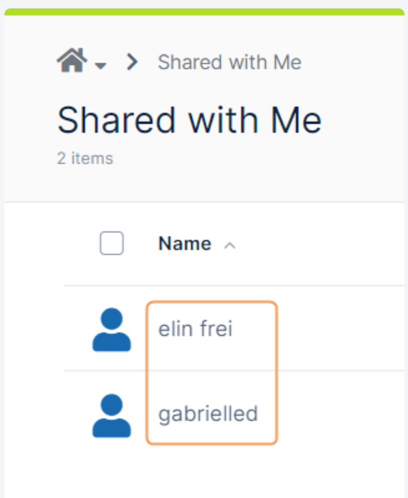
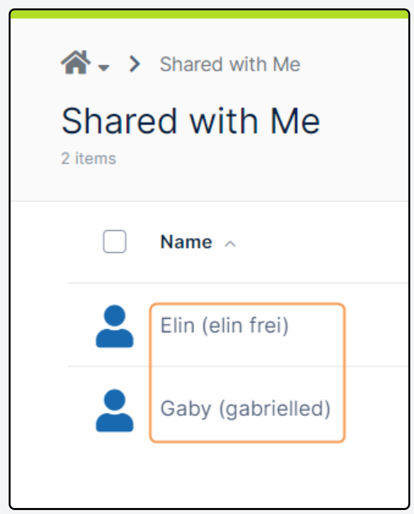
- You can have FileCloud use the **Display name** as well as the **User name** on the **Details** tab when showing the share information.
- Using the **Display name** makes it clearer to users who is sharing the file with them.
- The **Display name** can be changed after the user has been created.



Where Your Changes Appear

In the user portal, the user's name is displayed differently after you change the default display to include the **Display name**.

	BEFORE (User Name)	AFTER (Display Name and User Name)

Details Pane		
Shared With Me list		

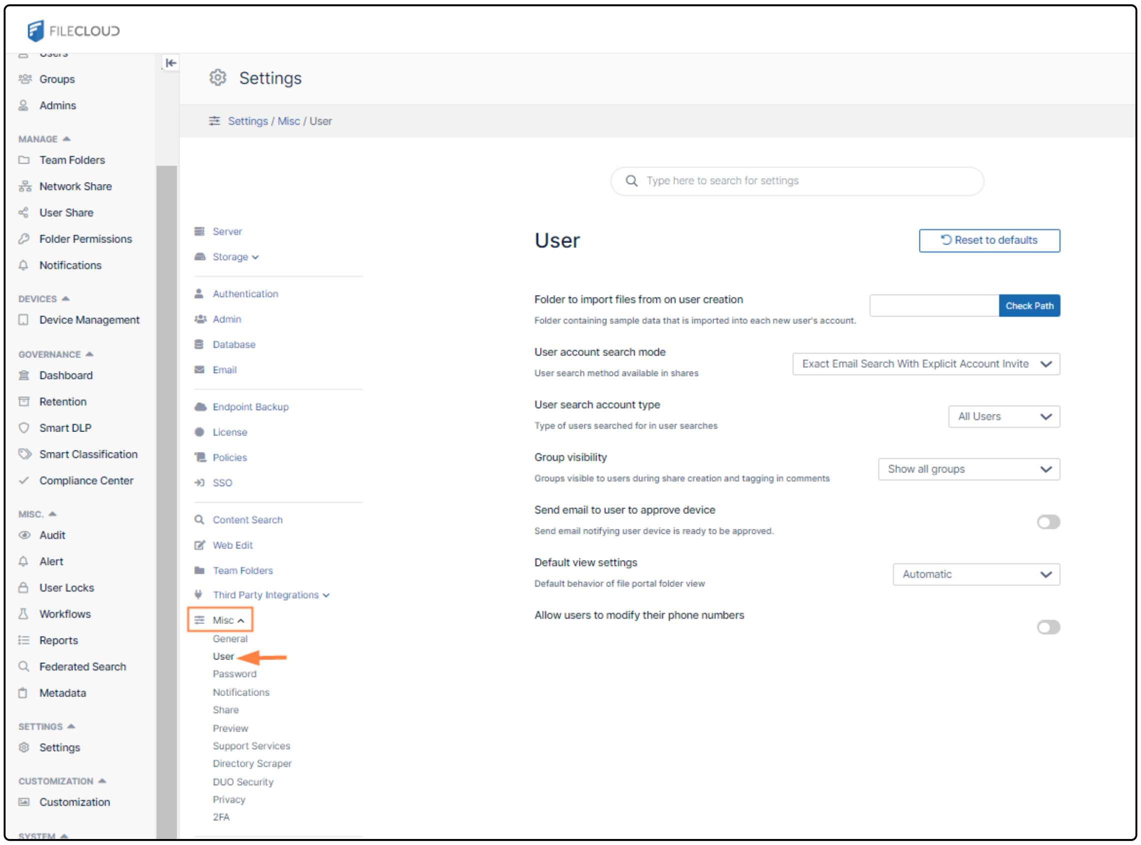
User Account Search Mode

For security reasons, you can restrict user searches so that your users have to know the exact email address of the person they want to add to a share or a workflow. Alternatively, you can set this option to allow users to search for another user with just a known partial email address.

To access the User Account Search Mode Settings:

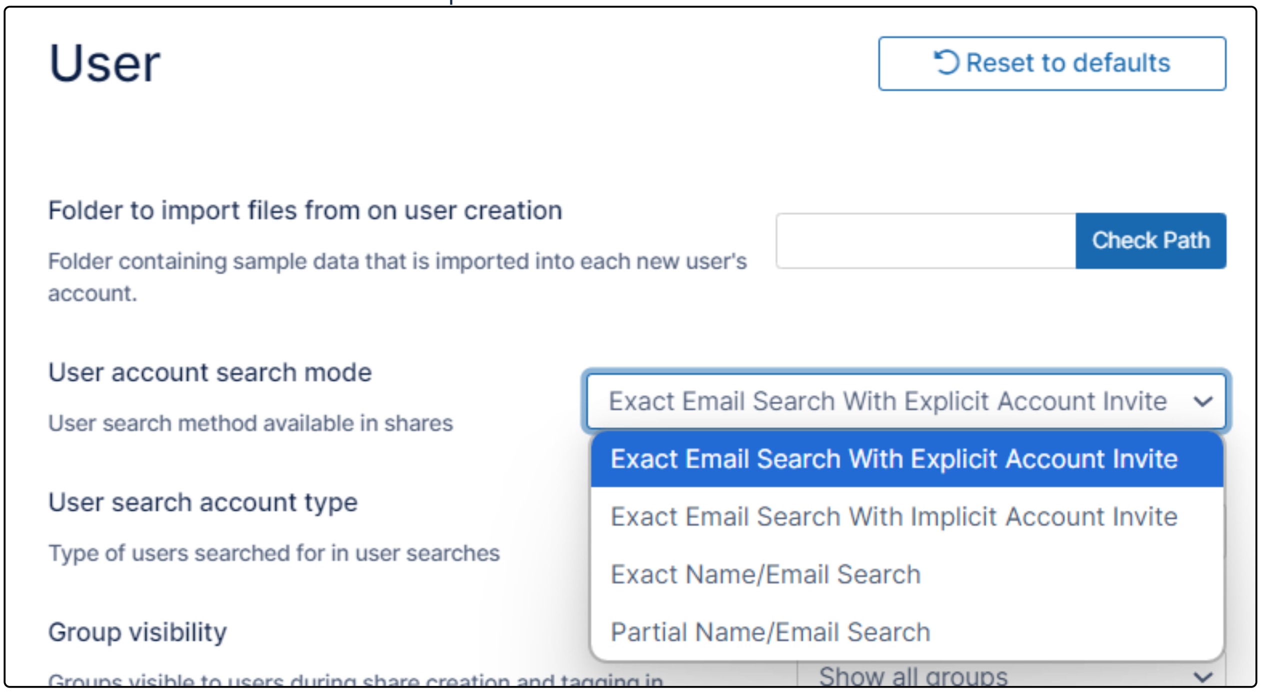
1. Open the **User** settings page.
   To open the User settings page:
      a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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



The **User** settings page opens.

2. Click the **User account search mode** drop-down list:



3. Choose a search mode, and click **Save**.

Search Mode	Example	When this search mode is set by admin, the following behavior will be seen during sharing by users:
Exact Email Search With Explicit Account Invite	JoeCarpenter@MyFileCloud.com	• Only email search is allowed • If the email doesn't exist in the system, an explicit invite option will be shown • With this option, a user may still figure out other users that exist in the system
Exact Email Search With Implicit Account Invite	JoeCarpenter@MyFileCloud.com	• Only email search is allowed • If the email doesn't exist in the system, then the system will send an invite to the entered email address without notifying the user • With this option, a user cannot figure out other users that exist in the system
Exact Name / Email Search	Joe Carpenter	• Both name and email search is allowed • No partial matches are allowed. • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the email doesn't exist in the system, the system will give the user option to invite the specified user

Search Mode	Example	When this search mode is set by admin, the following behavior will be seen during sharing by users:
Partial Name / Email Search	Joe C	• Both name and email search is allowed • Partial matches are allowed • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the searched email doesn't exist in the system, the system will give the user option to invite the specified user

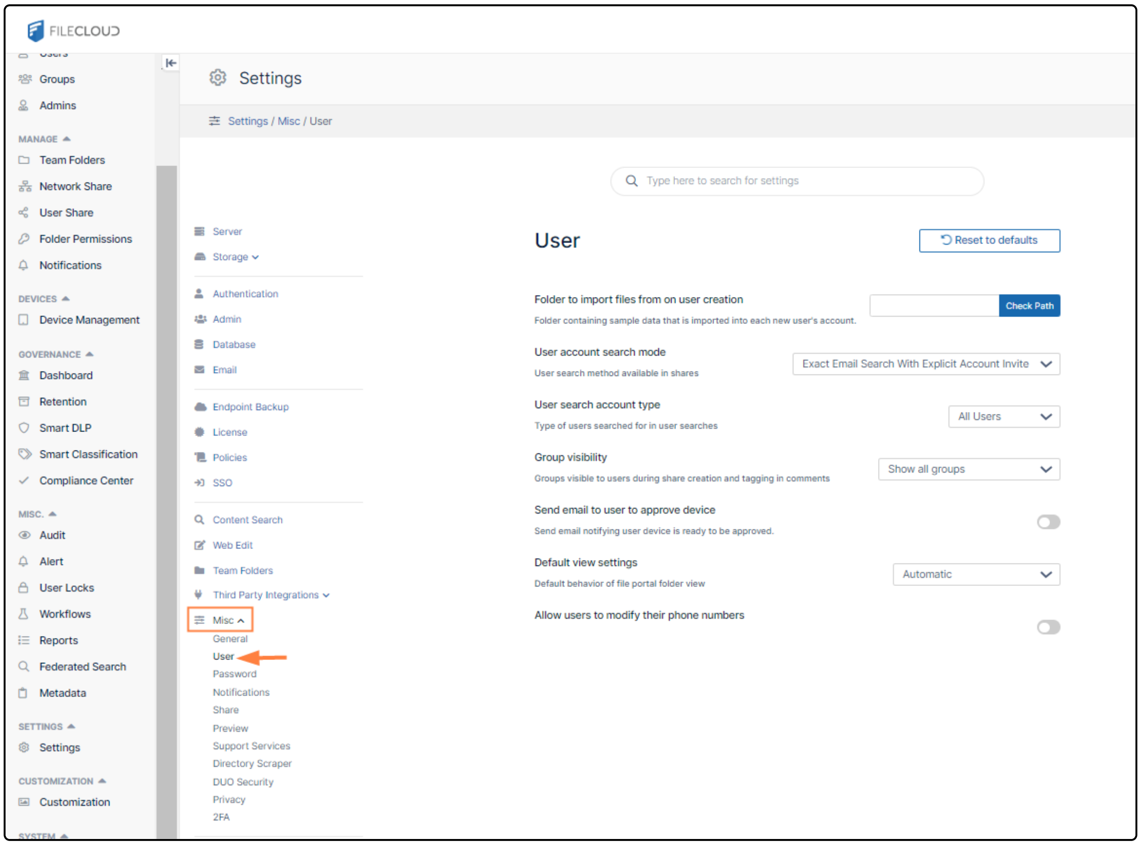
User Search Account Type

For security reasons, you can restrict user searches so that your users can only search for user accounts that are assigned a specific level of access.

To access the User search account type setting:

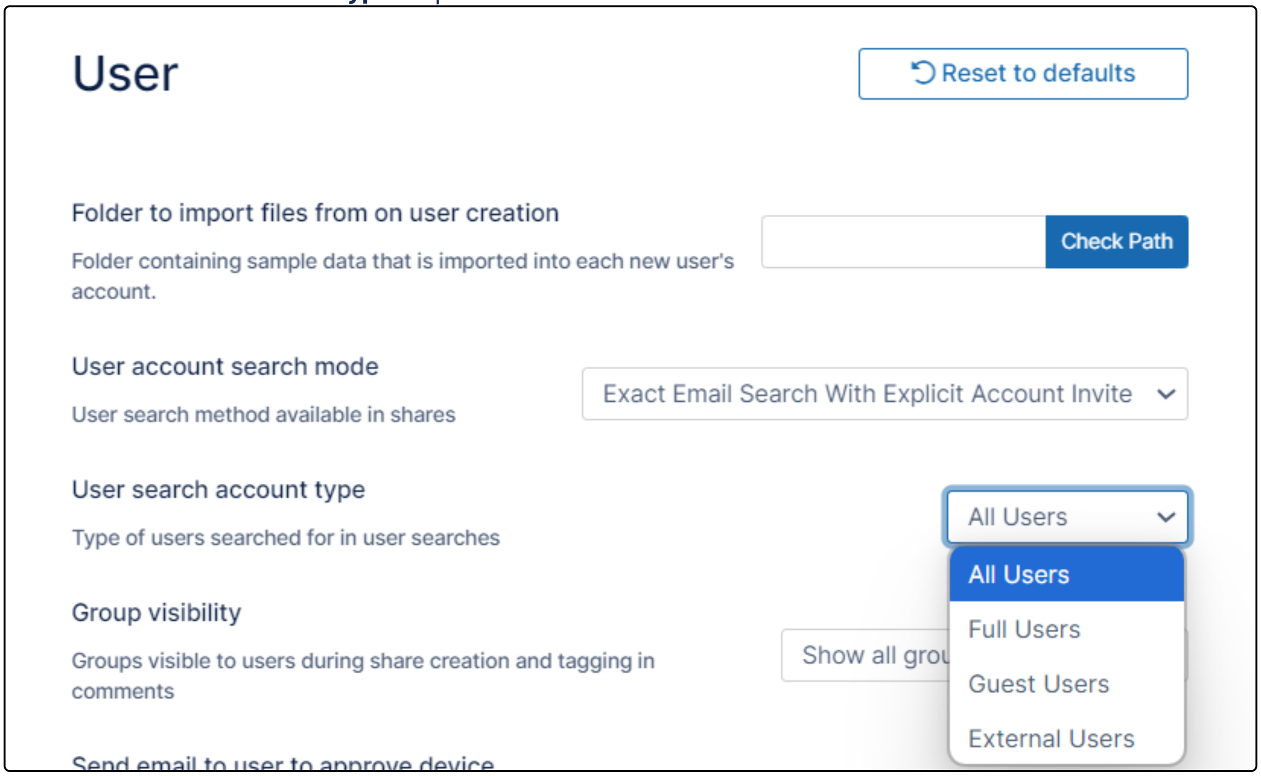
1. Open the **User** settings page.
   To open the User settings page:
      a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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



The **User** settings page opens.

2. Click the **User search account type** drop-down list:



3. Choose the account type to search on, and click **Save**.

User account type	Level of access
ALL	No restriction of account searches
FULL	An account with full access has its own private cloud storage space in the "My Files" area. These users can: • store files in their own private cloud storage space • view/download files stored in their storage space • view/download files shared with them by other user accounts
GUEST	An account with guest access level has restricted access to the FileCloud system. These user accounts do not have private cloud storage. These users can: • view/upload/download files shared to them by other user accounts • re-share content if they have permission

User account type	Level of access
EXTERNAL	An account that can only be used to access the User Portal through a Web browser. External Accounts can: • view/upload/download content shared with them External Access accounts can only be local user accounts.

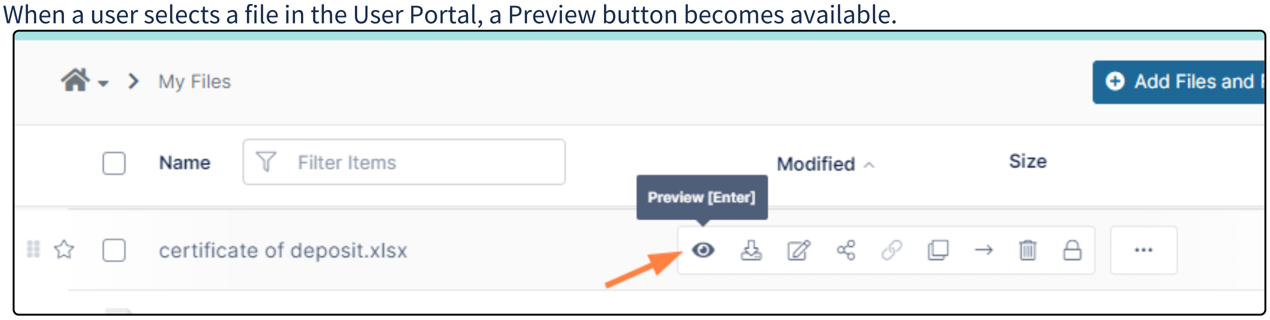
Document Settings

In this section:

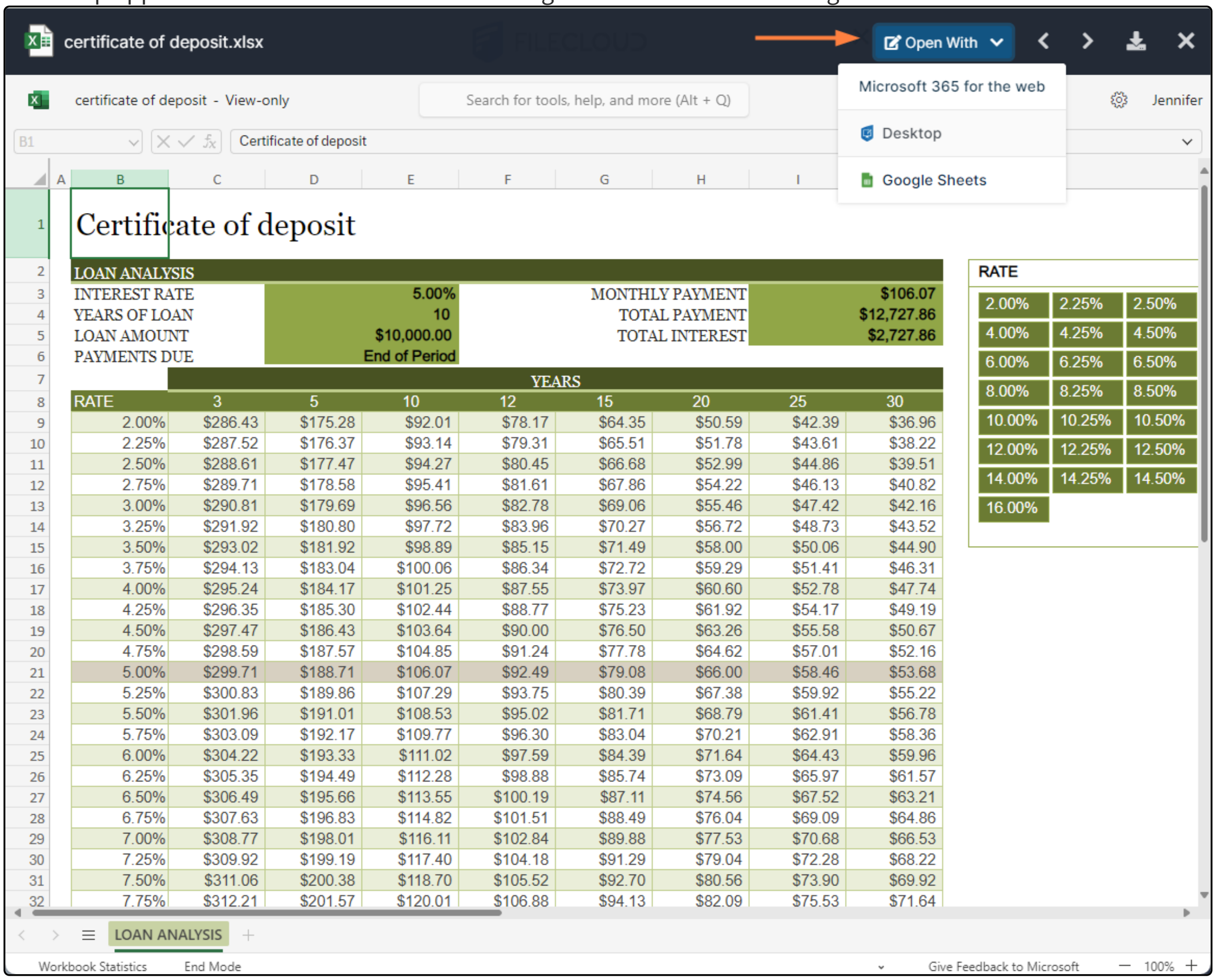
Setting Up Document Preview

When users preview supported file types directly in the User Portal through the web browser, they can see part of the file without having to install the application that created it.
This type of preview commonly uses the Quick JS Preview feature which enables previewing of DOCX, PPTX, XLSX, and PDF files when DocConverter is enabled. See LibreOffice Windows Instructions.

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



When the user clicks the **Preview** button, a separate window opens showing an image of the file.
Beginning in FileCloud 22.1, many of the previews can be edited with the same Web edit/Office Online and Edit in Desktop applications that are available for editing the file from the file listing.

2. 

Certificate of deposit

LOAN ANALYSIS			
INTEREST RATE	5.00%	MONTHLY PAYMENT	$106.07
YEARS OF LOAN	10	TOTAL PAYMENT	$12,727.86
LOAN AMOUNT	$10,000.00	TOTAL INTEREST	$2,727.86
PAYMENTS DUE	End of Period		

	YEARS							
RATE	3	5	10	12	15	20	25	30
2.00%	$286.43	$175.28	$92.01	$78.17	$64.35	$50.59	$42.39	$36.96
2.25%	$287.52	$176.37	$93.14	$79.31	$65.51	$51.78	$43.61	$38.22
2.50%	$288.61	$177.47	$94.27	$80.45	$66.68	$52.99	$44.86	$39.51
2.75%	$289.71	$178.58	$95.41	$81.61	$67.86	$54.22	$46.13	$40.82
3.00%	$290.81	$179.69	$96.56	$82.78	$69.06	$55.46	$47.42	$42.16
3.25%	$291.92	$180.80	$97.72	$83.96	$70.27	$56.72	$48.73	$43.52
3.50%	$293.02	$181.92	$98.89	$85.15	$71.49	$58.00	$50.06	$44.90
3.75%	$294.13	$183.04	$100.06	$86.34	$72.72	$59.29	$51.41	$46.31
4.00%	$295.24	$184.17	$101.25	$87.55	$73.97	$60.60	$52.78	$47.74
4.25%	$296.35	$185.30	$102.44	$88.77	$75.23	$61.92	$54.17	$49.19
4.50%	$297.47	$186.43	$103.64	$90.00	$76.50	$63.26	$55.58	$50.67
4.75%	$298.59	$187.57	$104.85	$91.24	$77.78	$64.62	$57.01	$52.16
5.00%	$299.71	$188.71	$106.07	$92.49	$79.08	$66.00	$58.46	$53.68
5.25%	$300.83	$189.86	$107.29	$93.75	$80.39	$67.38	$59.92	$55.22
5.50%	$301.96	$191.01	$108.53	$95.02	$81.71	$68.79	$61.41	$56.78
5.75%	$303.09	$192.17	$109.77	$96.30	$83.04	$70.21	$62.91	$58.36
6.00%	$304.22	$193.33	$111.02	$97.59	$84.39	$71.64	$64.43	$59.96
6.25%	$305.35	$194.49	$112.28	$98.88	$85.74	$73.09	$65.97	$61.57
6.50%	$306.49	$195.66	$113.55	$100.19	$87.11	$74.56	$67.52	$63.21
6.75%	$307.63	$196.83	$114.82	$101.51	$88.49	$76.04	$69.09	$64.86
7.00%	$308.77	$198.01	$116.11	$102.84	$89.88	$77.53	$70.68	$66.53
7.25%	$309.92	$199.19	$117.40	$104.18	$91.29	$79.04	$72.28	$68.22
7.50%	$311.06	$200.38	$118.70	$105.52	$92.70	$80.56	$73.90	$69.92
7.75%	$312.21	$201.57	$120.01	$106.88	$94.13	$82.09	$75.53	$71.64

RATE		
2.00%	2.25%	2.50%
4.00%	4.25%	4.50%
6.00%	6.25%	6.50%
8.00%	8.25%	8.50%
10.00%	10.25%	10.50%
12.00%	12.25%	12.50%
14.00%	14.25%	14.50%
16.00%		

To include watermarks on previewed documents, see Enabling Watermarks On Previews

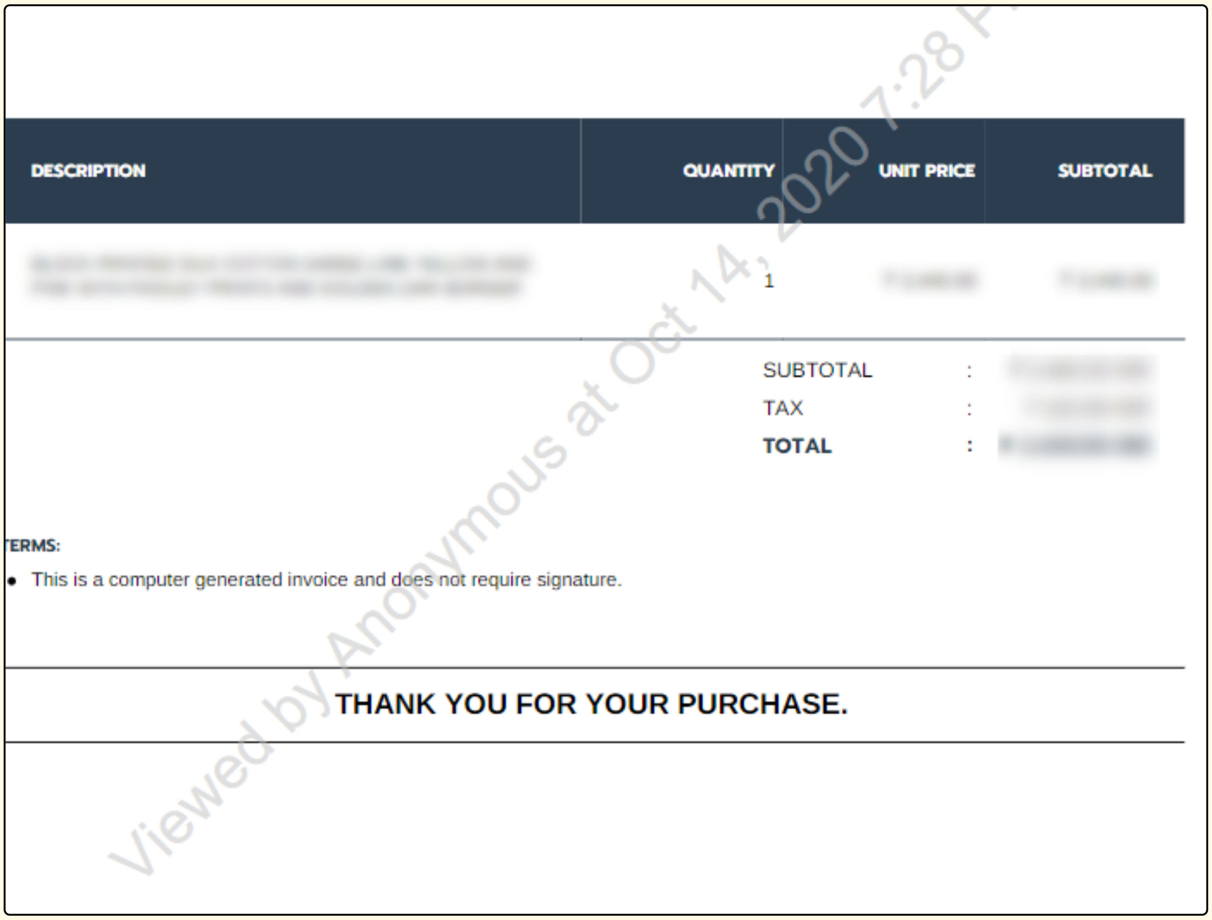
Enabling Watermarks On Previews

Administrators can add watermarks to all previews generated in FileCloud.

> The options of applying multiline watermarks and choosing a font size are available in FileCloud 23.251 and later.

> Password protected PDF previews are not showing watermarks. This is an issue with the third-party application used for previewing PDFs, and will be resolved when an update of the application becomes available.

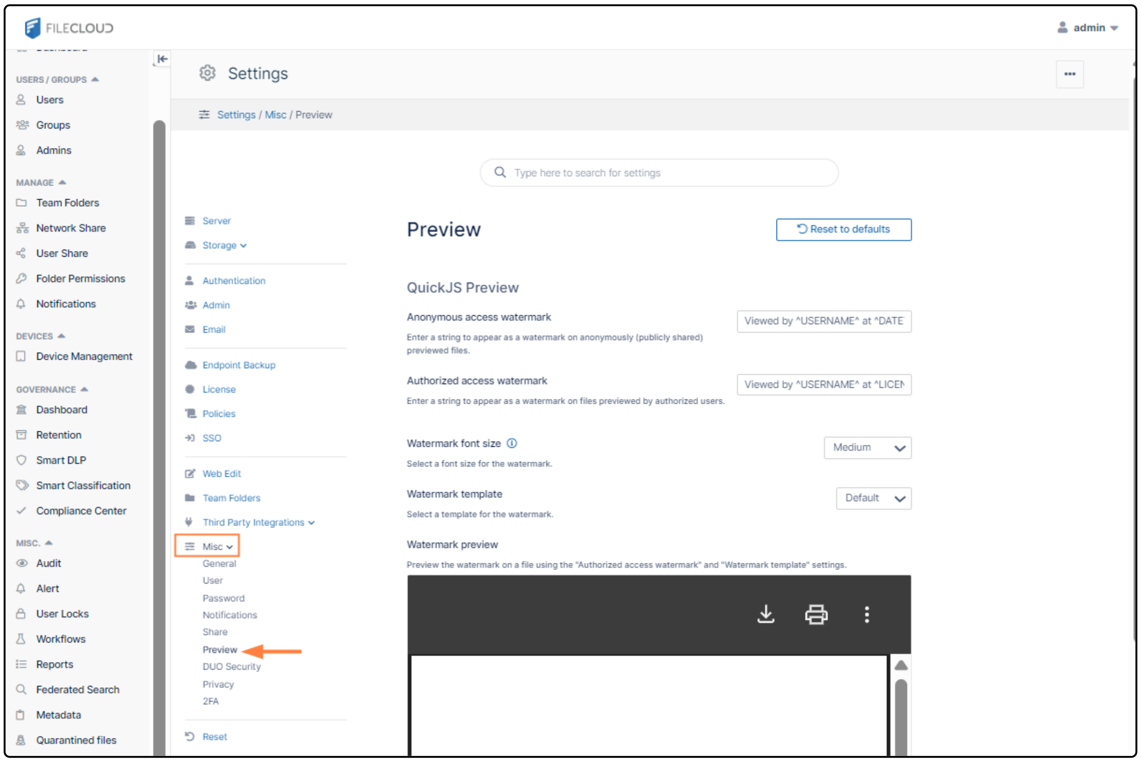
Example of a single line (default) watermark on a document preview in the admin and user portals.



To display watermarks for previews:

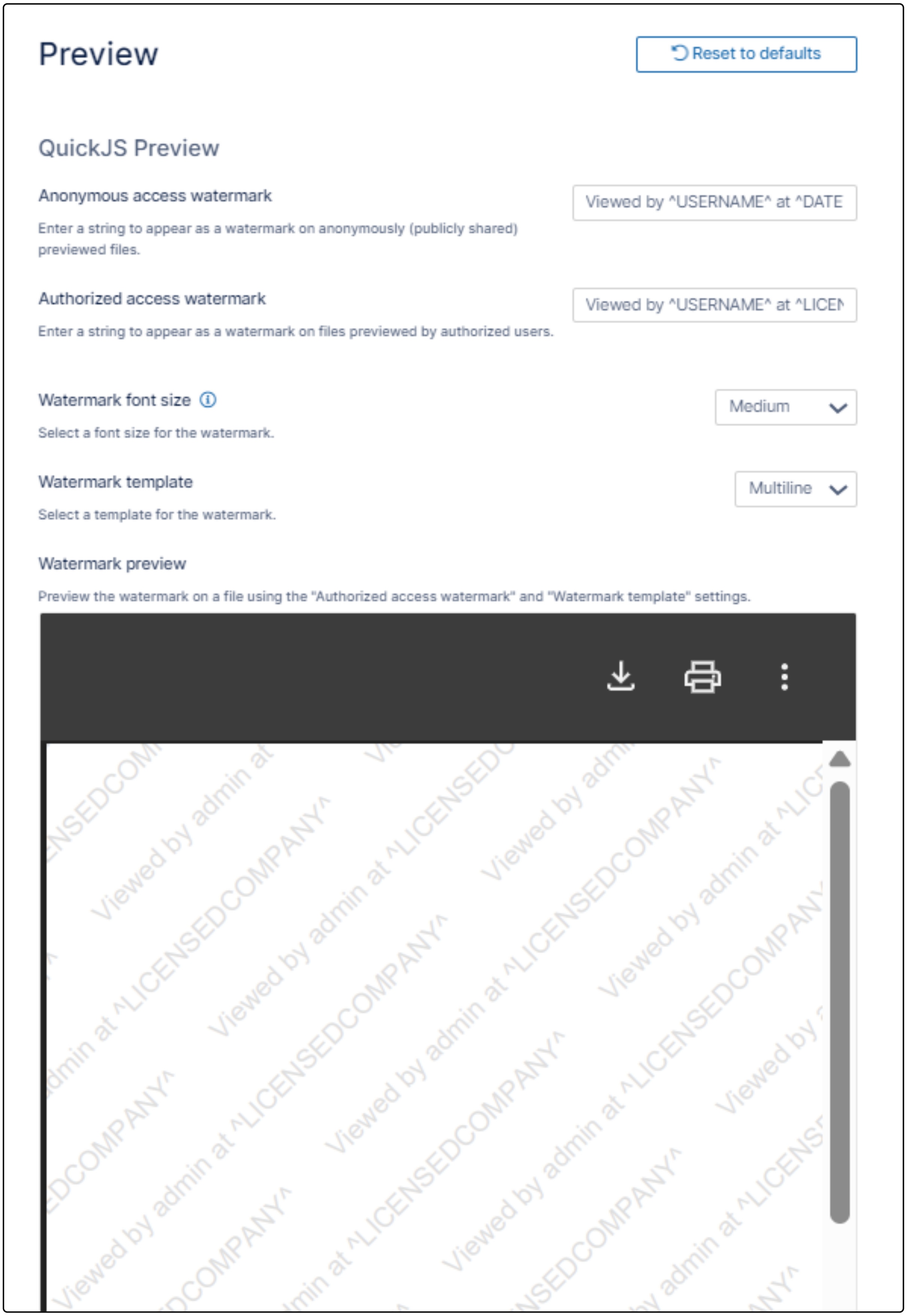
1. Open the Preview settings page.
   To open the Preview settings page
      a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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



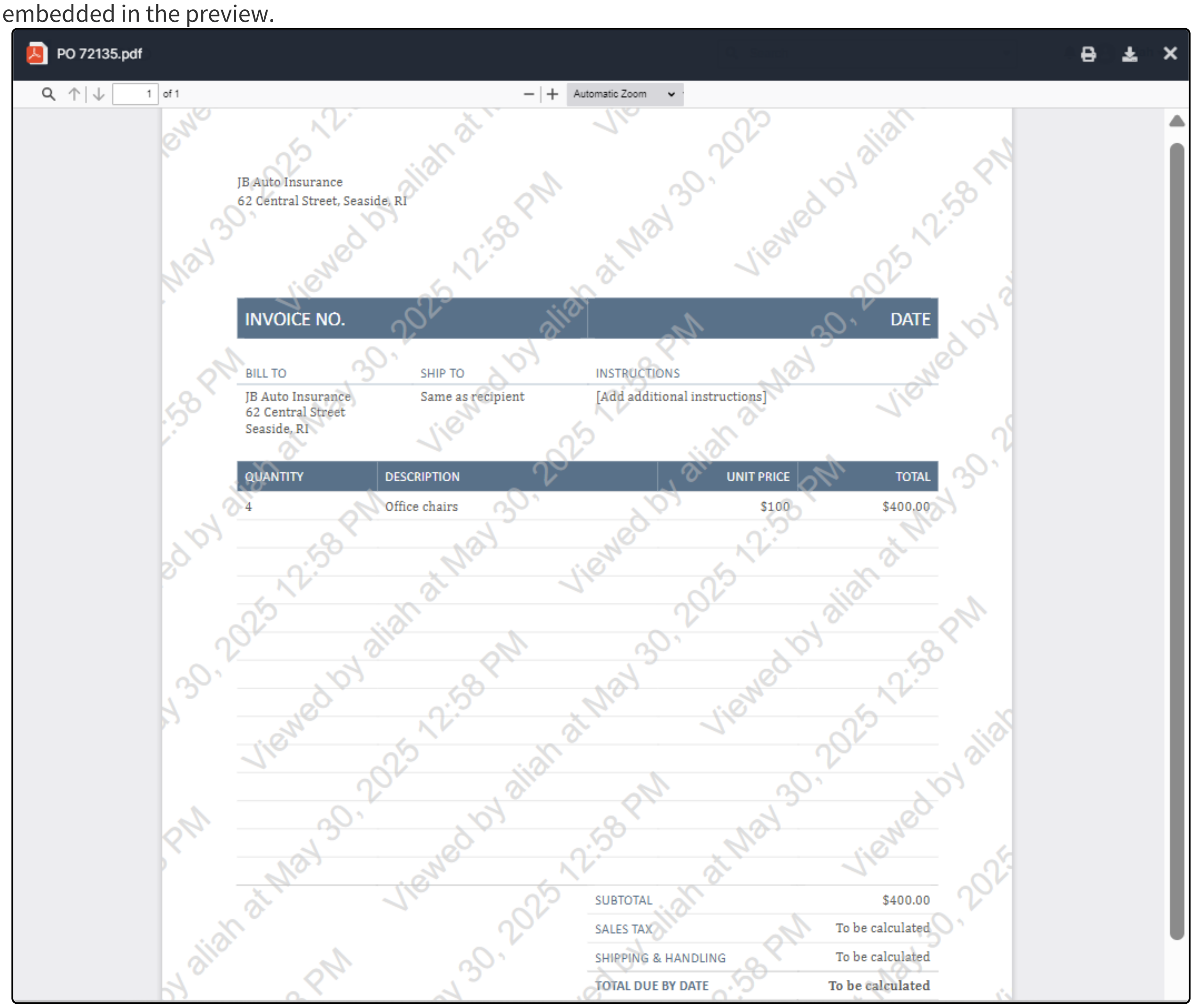
The **Preview** settings page opens.

2. In **Anonymous access watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by anonymous users. **Anonymous access watermarks** appear to unauthorized users (users viewing public shares).
3. In **Authorized access watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by authorized users.
4. In **Watermark font size**, choose a font size.
5. In **Watermark template**:
   - Leave **Default** if you want the watermark to appear in one line across each page of the document.
   - Choose **Multiline** if you want the watermark to appear repeatedly in multiple line across each page of the document.
   Watermark preview displays a sample of how your watermark would appear on previewed pages. You may change the settings before saving, and the preview will reflect your unsaved changes.


Preview
Reset to defaults
QuickJS Preview
Anonymous access watermark
Enter a string to appear as a watermark on anonymously (publicly shared) previewed files.
Viewed by ^USERNAME^ at ^DATE
Authorized access watermark
Enter a string to appear as a watermark on files previewed by authorized users.
Viewed by ^USERNAME^ at ^LICEN
Watermark font size
Select a font size for the watermark.
Medium
Watermark template
Select a template for the watermark.
Multiline
Watermark preview
Preview the watermark on a file using the "Authorized access watermark" and "Watermark template" settings.
Viewed by admin at ^LICENSEDCOMPANY^

Available parameters:
^USERNAME^ - The user who is viewing this file.
^SHARE_OWNER^ - The user who shared this file.
^FILE_OWNER^ - The file owner.
^OWNER^ - If this is a shared file, the user who shared this file. If this is not a shared file, the file owner.
^DATETIME^ - Date and time of preview.
^GEOIP_LOCATION^ - Geographic location of IP performing preview.
^LICENSED_COMPANY^ - The company listed on the current license.
^PREVIEW_ID^ - An encrypted ID that can be used in place of ^USERNAME^. The encrypted ID appears on the file preview. Admins can identify the user (and the device's IP address) by viewing the audit log for the preview action.

Now whenever a user previews a document, they see the watermark for anonymous or authorized access embedded in the preview.

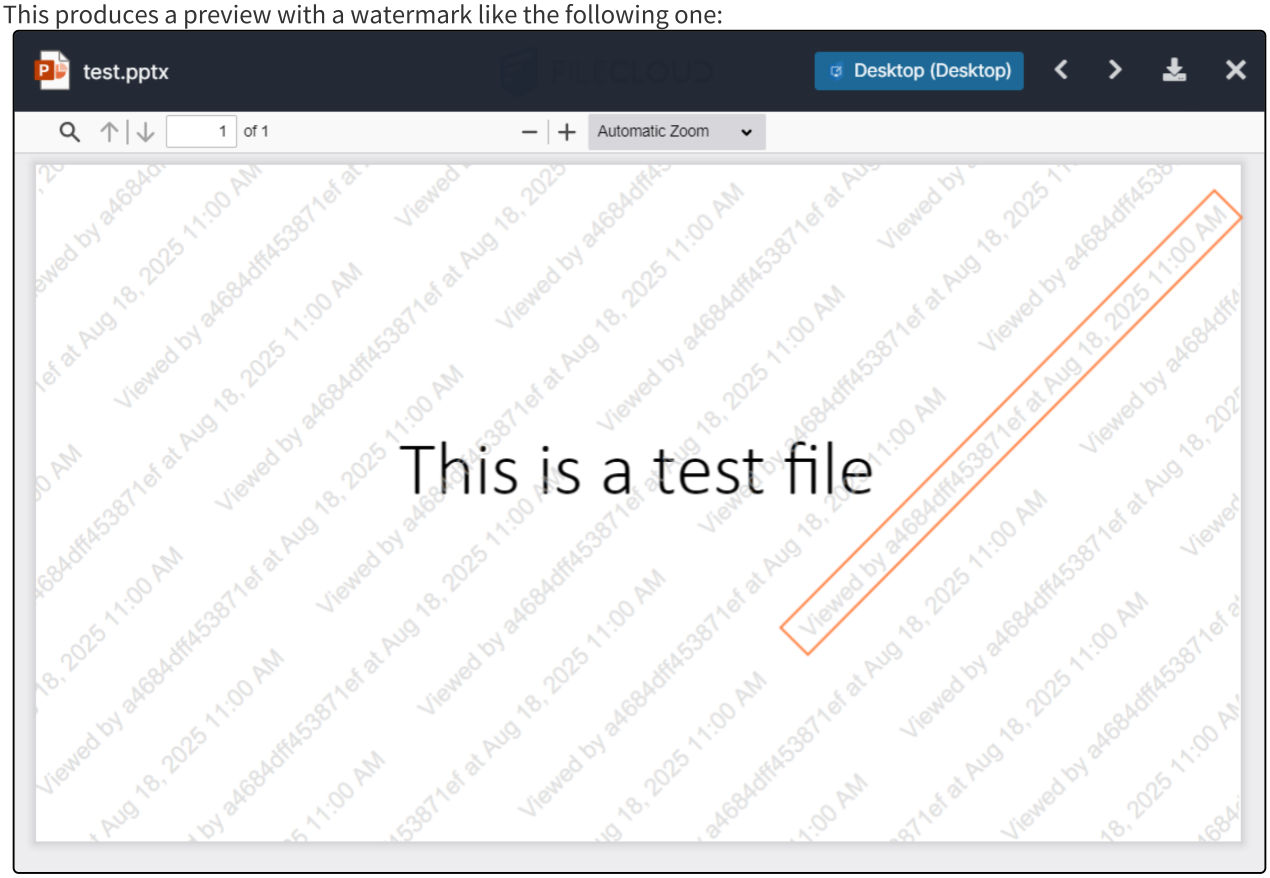


Displaying an encrypted User ID in the a watermark

To display an encrypted User ID instead of the actual User ID in a watermark:

1. In the Preview settings page, use the parameter **^PREVIEW_ID^** instead of **^USERNAME^** in the field **Anonymous access watermark** or **Authorized access watermark**:

This produces a preview with a watermark like the following one:



Note that if the user previews the file additional times, it will have different preview IDs each time.

2. To identify the user who previewed the file, go to the Audit Logs, and locate the log with the encrypted ID in the message. The message will identify the actual user who previewed the file, and, as with any audit log record, the IP address of the device where the action was performed.

User Name	Message	IP	Agent	Created On
tester	tester previewed file /tester/tester-sample/FCD.xlsx with watermark: Viewed by 3c8155ee13d9e5a7 at Aug 18, 2025 11:18 AM	139.162.50.236	Web browser	2025-Aug-18 11:18 AM

Import Files : Pre-seeding

Administrators can import files to managed storage configuration to prepare FileCloud for users.

⚠ NOTES:

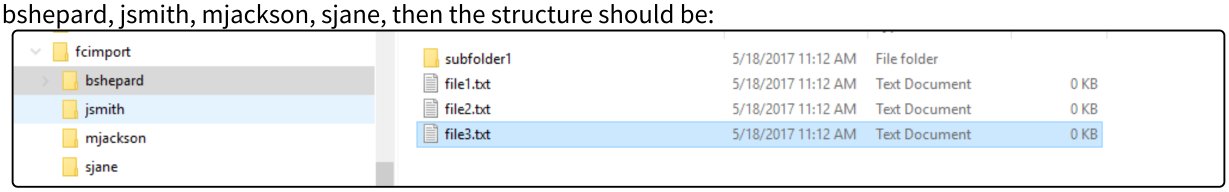
- During the seeding operation, the system is operating under a special mode and user access must not be allowed (though it is not prevented automatically).
- Therefore, ideally, seeding should be done during initial system setup.

Import Files into Local Managed Storage

Prerequisite:

In order for the data to be imported, the following conditions must be met.

1. The data must be in locally accessible disk. Ideally, the data must reside in the same drive as the managed storage (for example, if managed storage is in C:\fileclouddata, then the import data must also be in C: drive)
2. The data must be in following structure. <ImportPath><users><data>. For example, if you have four users, bshepard, jsmith, mjackson, sjane, then the structure should be:



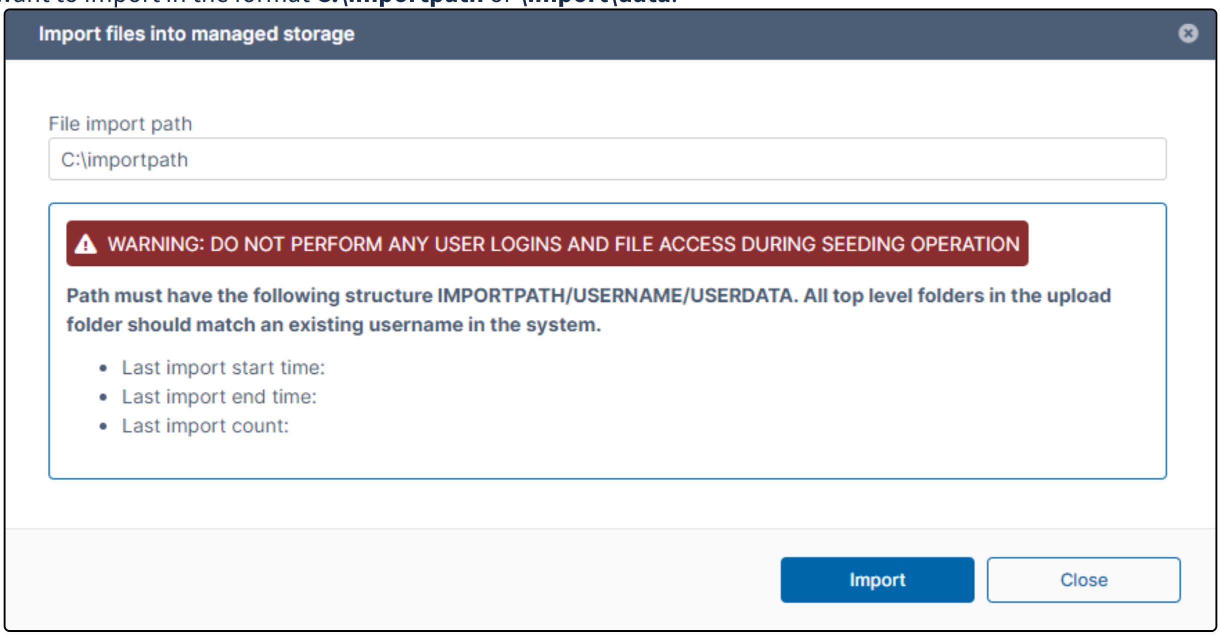
3. The users must already be created in the system (bshepard, jsmith, mjackson, sjane must already be valid full users in the system).
4. The users must have enough quota assigned to allow the data import.

To import files into local managed storage:

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

2. Scroll down to **Import Files**, and click the **Import Files** button.

3. On the **Import files into managed storage** dialog box, in **File Import Path**, type the location to the files you want to import in the format **C:\importpath** or **\import\data**.



4. Click **Import**.

Optimize PDF Preview

Administrators can configure FileCloud to show a preview of PDF files directly in the User Portal without forcing a user to download the file first.

This is configured when you Set Up Document Preview.

How users experience PDF previews

If you choose to allow previews of PDF files, you should be aware of what the user's experience will be on the user portal.

In some cases, viewing PDF files can take more time than expected.

The time it takes to generate a preview of a PDF depends on the how the file is created.

In general, a PDF can be categorized in to two main types:

- Native (quicker)
- Scanned (slower)

Why is a Native PDF quicker to preview?

Native

Information is saved as text when you save a file as PDF if you have created the file from the following sources:

- A word processing program such as Microsoft Word, Excel or PowerPoint
- A browser page printed to PDF
- A file saved directly from PDF generation software such as Nitro PDF, Adobe PDF, etc.

When information is saved as text, searching, copying, and other text-based operations on the PDF are quicker.

It also takes less time to generate a preview of a native PDF file than a scanned PDF file.

Scanned

When PDFs are created from scanning, there is no information about the content because the PDF file just serves as a container of images.

While this format is useful when the objective is to showcase graphics material, the rendering of this file can take a long time.

When a scanned PDF needs to be previewed in FileCloud:

1. The client's User Portal needs to check the entire PDF embedded text to allow search, copy or any other text based operations.
2. This text processing operation is done at the moment when the client's User Portal requests a preview.
3. The processing on the client-side portal can make the preview loading slow for general use.

If you have a scanned PDF file that has been created from one of the following sources, your best option is to convert the file to native PDF before uploading it to FileCloud:

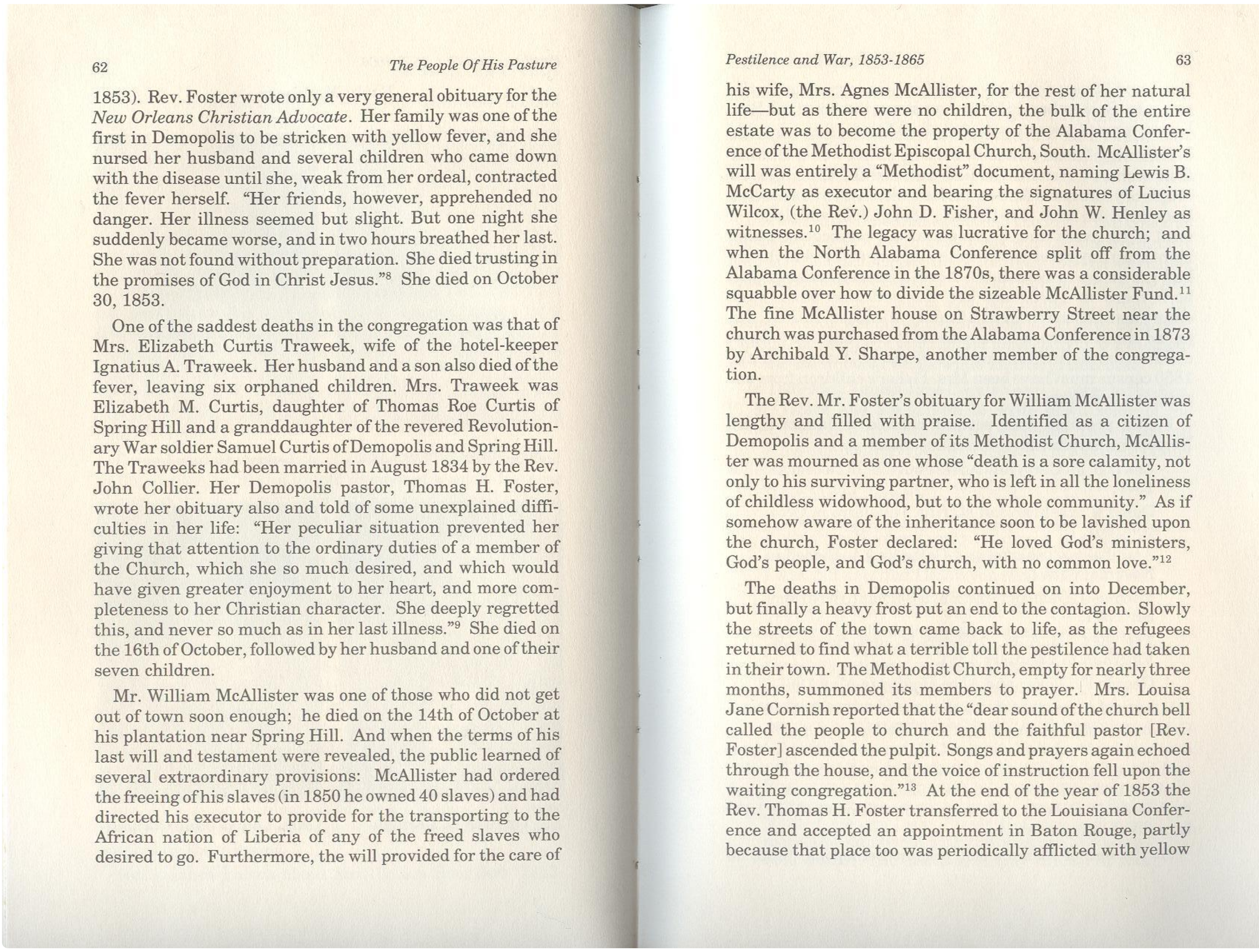
- Legal documents
- Insurance patient documents
- Blueprints and manuals

Optimizing files in this way allows a file to be opened with less processing time and generates a preview quicker.

How Do I Convert a Scanned PDF to Native?

There are several tools in the market you can use to convert scanned PDF files to native PDF files (OCR reading).

For example, if you have a scanned image similar to the following, you should convert it Native PDF:



62 *The People Of His Pasture*

1853). Rev. Foster wrote only a very general obituary for the *New Orleans Christian Advocate*. Her family was one of the first in Demopolis to be stricken with yellow fever, and she nursed her husband and several children who came down with the disease until she, weak from her ordeal, contracted the fever herself. "Her friends, however, apprehended no danger. Her illness seemed but slight. But one night she suddenly became worse, and in two hours breathed her last. She was not found without preparation. She died trusting in the promises of God in Christ Jesus."[8] She died on October 30, 1853.

One of the saddest deaths in the congregation was that of Mrs. Elizabeth Curtis Traweek, wife of the hotel-keeper Ignatius A. Traweek. Her husband and a son also died of the fever, leaving six orphaned children. Mrs. Traweek was Elizabeth M. Curtis, daughter of Thomas Roe Curtis of Spring Hill and a granddaughter of the revered Revolutionary War soldier Samuel Curtis of Demopolis and Spring Hill. The Traweeks had been married in August 1834 by the Rev. John Collier. Her Demopolis pastor, Thomas H. Foster, wrote her obituary also and told of some unexplained difficulties in her life: "Her peculiar situation prevented her giving that attention to the ordinary duties of a member of the Church, which she so much desired, and which would have given greater enjoyment to her heart, and more completeness to her Christian character. She deeply regretted this, and never so much as in her last illness."[9] She died on the 16th of October, followed by her husband and one of their seven children.

Mr. William McAllister was one of those who did not get out of town soon enough; he died on the 14th of October at his plantation near Spring Hill. And when the terms of his last will and testament were revealed, the public learned of several extraordinary provisions: McAllister had ordered the freeing of his slaves (in 1850 he owned 40 slaves) and had directed his executor to provide for the transporting to the African nation of Liberia of any of the freed slaves who desired to go. Furthermore, the will provided for the care of

Pestilence and War, 1853-1865 63

his wife, Mrs. Agnes McAllister, for the rest of her natural life—but as there were no children, the bulk of the entire estate was to become the property of the Alabama Conference of the Methodist Episcopal Church, South. McAllister's will was entirely a "Methodist" document, naming Lewis B. McCarty as executor and bearing the signatures of Lucius Wilcox, (the Rev.) John D. Fisher, and John W. Henley as witnesses.[10] The legacy was lucrative for the church; and when the North Alabama Conference split off from the Alabama Conference in the 1870s, there was a considerable squabble over how to divide the sizeable McAllister Fund.[11] The fine McAllister house on Strawberry Street near the church was purchased from the Alabama Conference in 1873 by Archibald Y. Sharpe, another member of the congregation.

The Rev. Mr. Foster's obituary for William McAllister was lengthy and filled with praise. Identified as a citizen of Demopolis and a member of its Methodist Church, McAllister was mourned as one whose "death is a sore calamity, not only to his surviving partner, who is left in all the loneliness of childless widowhood, but to the whole community." As if somehow aware of the inheritance soon to be lavished upon the church, Foster declared: "He loved God's ministers, God's people, and God's church, with no common love."[12]

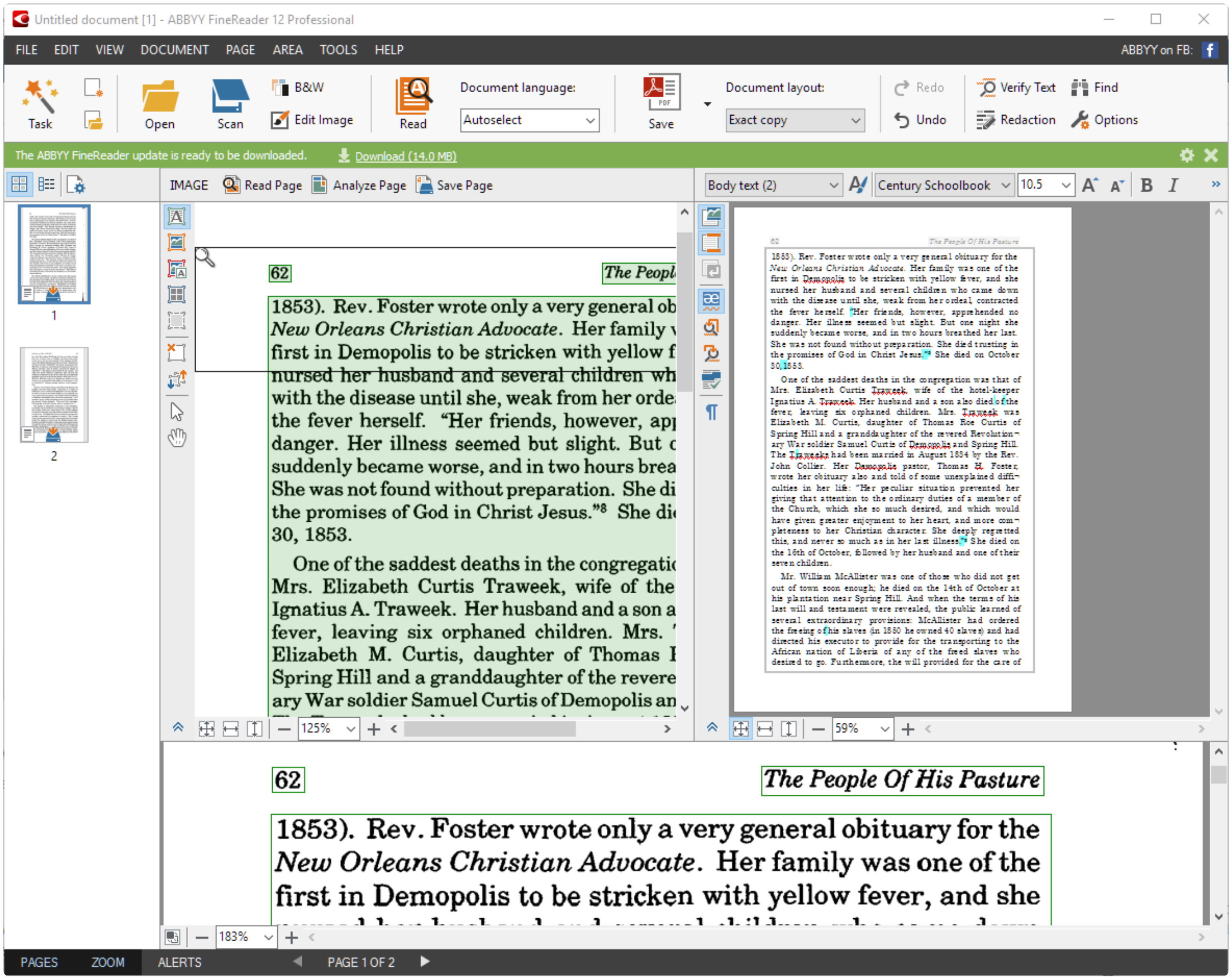
The deaths in Demopolis continued on into December, but finally a heavy frost put an end to the contagion. Slowly the streets of the town came back to life, as the refugees returned to find what a terrible toll the pestilence had taken in their town. The Methodist Church, empty for nearly three months, summoned its members to prayer. Mrs. Louisa Jane Cornish reported that the "dear sound of the church bell called the people to church and the faithful pastor [Rev. Foster] ascended the pulpit. Songs and prayers again echoed through the house, and the voice of instruction fell upon the waiting congregation."[13] At the end of the year of 1853 the Rev. Thomas H. Foster transferred to the Louisiana Conference and accepted an appointment in Baton Rouge, partly because that place too was periodically afflicted with yellow

In our example:

- this file is scanned and saved as a PDF named **Scanned_PDF.pdf**
- If we use this file as it is, the FileCloud Preview will take a longer than expected time to render this on the User Portal

For test purposes, CodeLathe has tested and recommends the following tool to optimize PDF files for generating a preview:

- ABBYY produces FineReader, an all-in-one OCR and PDF software application for increasing business productivity when working with documents.
- Using ABBYY Fine Reader software, you can open and convert this PDF file to a Native PDF file.



The use of ABBYY FineReader was used for explanation purposes only. Any other tool that can read a PDF file can be used to optimize the PDF files for web viewing.

Managing File Extensions

As of Version 23.232.1, FileCloud lists **php**, **php5**, **phar**, **phtml**, **php7**, and **htaccess** as disallowed file extensions. If you are using a version of FileCloud earlier than 23.232, you are advised to add any of these extensions that are not include by default onto the **Disallowed File** list.

For security reasons you may want to restrict uploading of files with specific extensions.

- You can either create a list of file extensions to restrict, or create a list of file extensions to allow.
- If you create an Allowed list of file extensions, then any settings in the Disallowed list will be ignored.
- These restrictions help to prevent users from uploading malicious attachments and viewing them.

- By default FileCloud restricts users from uploading any files with **php** extensions. This is to prevent any code injection.

In FileCloud's **Misc/General** settings you may specify allowed and disallowed file extensions.

Which list should I use? Allowed or Disallowed?

- If you know which file types you don't want to allow and this list is short, you can use the **Disallowed** setting.
- If you want to allow only a few file types to be uploaded, you can use the **Allowed** setting.
- If you create an **Allowed** list of file extensions, then any settings in the **Disallowed** list will be ignored.

What Do You Want to Do?

Allow File Extensions

If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.

- An empty space is defined as a delimiter character followed by no value.

Examples	Description	Impact on Uploading Files
`png | jpg |`	Allow files to be uploaded with an extension of: • png • jpg • *empty*	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group • Any file without an extension (for example, a file named *config*)
`png | jpg`	Allow files to be uploaded with an extension of: • png • jpg	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group

To allow extensions in the Admin Portal:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Scroll down until you see the **Allowed File Extensions** box.

3. In the **Allowed File Extensions** box, specify the allowed extensions, using the "|" character to separate each extension.

   Notes:

⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.

⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.

This list of extensions must use the following character as the delimiter:

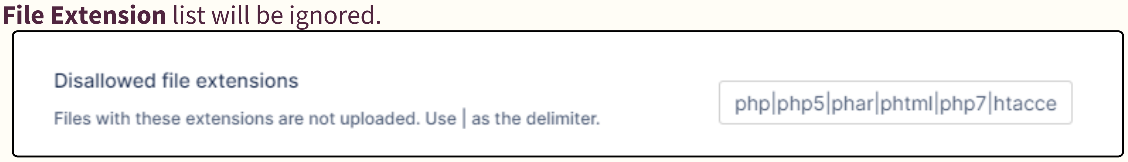
- '|'
- For example, to restrict the mp4 and mp3 extensions:
  `mp4|mp3`

Disallow File Extensions

To disallow extensions in the admin portal:

1. Log into admin portal.
2. From the left navigation panel, select **Settings.**
3. On the **Settings** screen, select the **Misc**. tab, and then the **General** tab.
4. Scroll down until you see the **Disallowed File Extensions** box.
5. In the **Disallowed File Extensions** box, add the additional restricted extensions.

⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.



This list of extensions must use the following character as the delimiter:

- '|'
- For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions:
  `php|php5|phar|phtml|php7|htaccess|mp3|mp4`

Restricting File Extensions

As an administrator, for security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud.

- This helps prevent users from uploading malicious attachments and viewing them.
- By default FileCloud will restrict files with php extensions. This is to prevent any code injection.

To manage extensions in the Admin Portal:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Scroll down until you see the **Disallowed File Extensions** box.
3. In the **Disallowed File Extensions** box, specify the restricted extensions.
   

   This list of extensions must use the following character as the delimiter:
   - '|'
   - For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions:
     `php|php5|phar|phtml|mp3|mp4`

Restricting File Names

For security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud Server. In this case, you may want to make sure that certain files are not available.

To restrict names of files that can be uploaded:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Add the file names to the **Disallowed file names** field.
   Separate multiple names with **|**.

Files matching or including any term entered are not uploaded. If you do not specify an extension, files matching or including the term and any extension are not uploaded.

To understand how to create a list of file names, use the examples below.

⚠ If you leave an empty space in your list:
- In the User Portal, all files are blocked from being uploaded.
- The Sync client does not check for restricted names.

⚠ If you add an extension to the file name, then only the combination of name + extension is restricted.

To manage file extensions ONLY, you can either create a list of file extensions to restrict, or create a list of file extensions to allow. See Manage File Extensions for instructions.

Example	Description	Impact on Uploading Files
`attack | threat.exe |`	Restrict any file from being uploaded if it contains any of the 3 strings in the file name: • attack • threat.exe • *empty*	The following files cannot be uploaded by users: • *attack*.* • *threat.exe • Any file The following files can be uploaded by users: • No files can be uploaded until the *empty delimiter* is removed.

Example	Description	Impact on Uploading Files
`attack | threat.exe`	Restrict any file from being uploaded if it contains any of the 2 strings in the file name: • attack • threat.exe	The following files cannot be uploaded by users: • *attack*.* • *threat.exe The following files can be uploaded by users: • Any file not containing *attack* • Any file not containing *threat.exe* • threat.* *(where * is NOT .exe)*

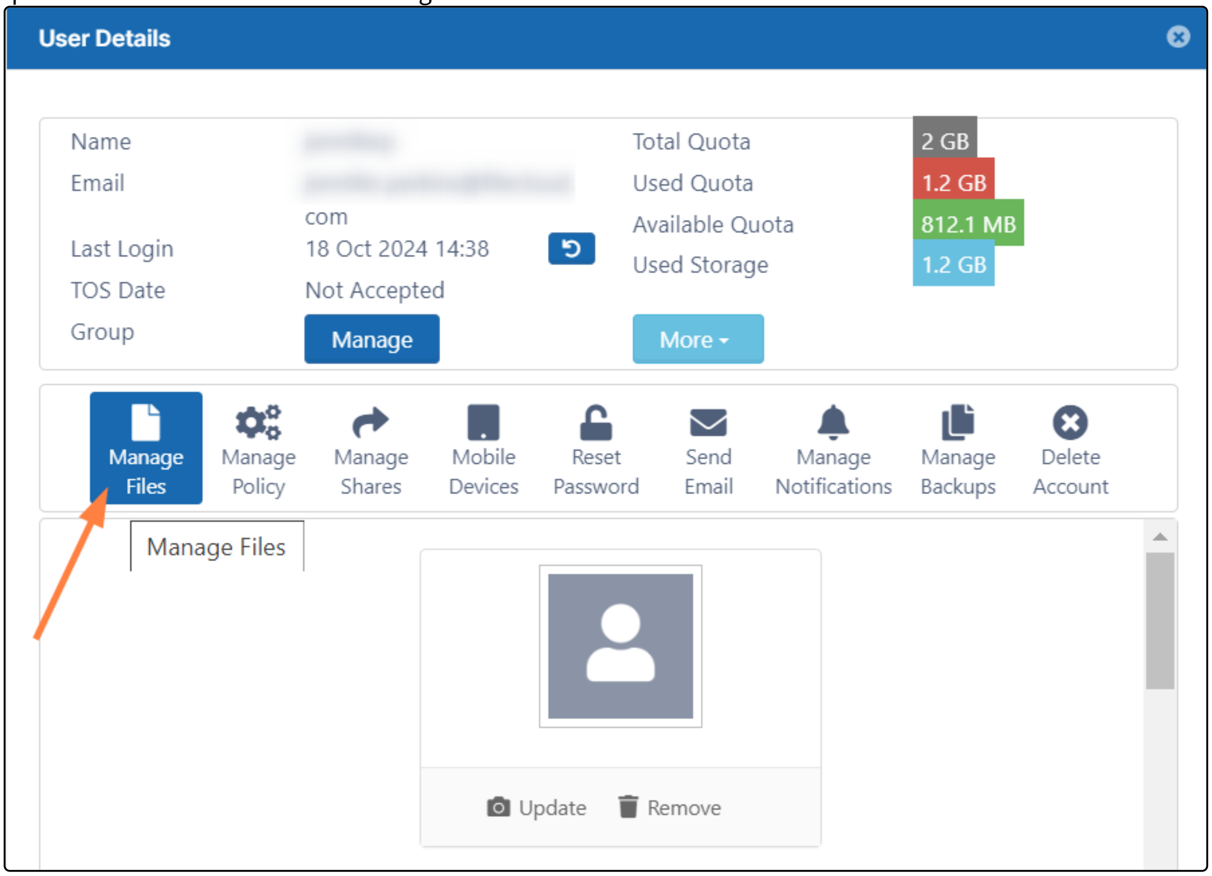
Manage File Versioning

You can allow a user to uploaded changes to a file and create another version of a file. This is called file versioning.

- This allows users to have an older version of the file on the site
- Users can download a previous version
- Users can remove previous versions to save space

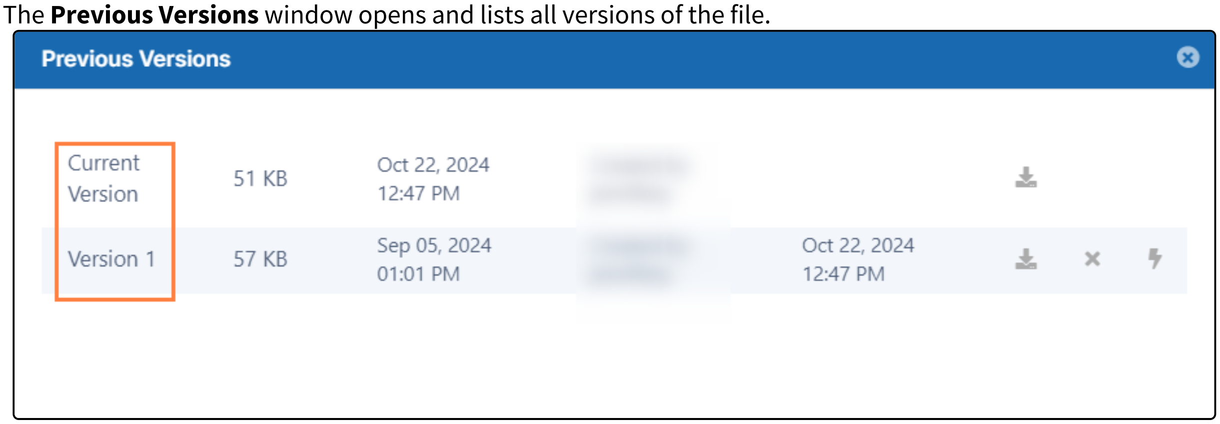
How do I know if there are previous versions of a user file?

1. Open the user's details and click Manage Files.



2. In the **Manage files** screen, navigate to a file and click its Versions icon  .

3. The **Previous Versions** window opens and lists all versions of the file.



If file versioning is causing issues, you can turn it off.

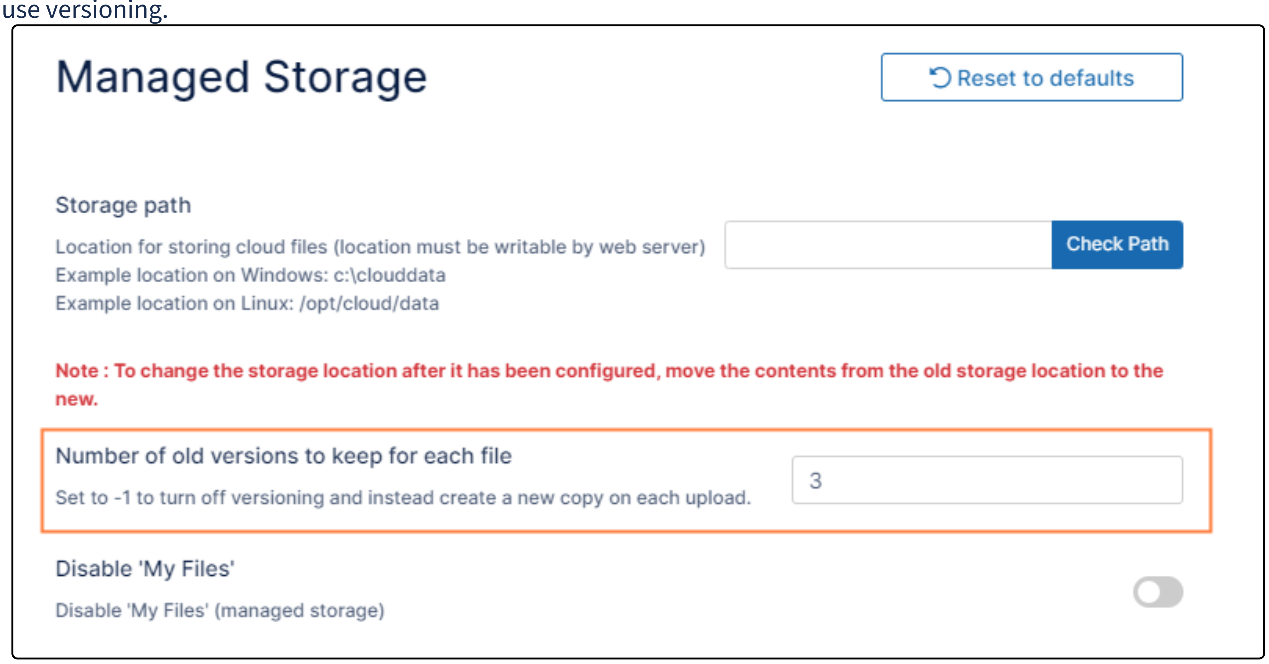
- File versioning can cause loss of data when a user accidentally overwrites a file with the same name.
- Users may be storing too many unnecessary versions of a file and are taking up too much space.

When you configure file versioning, use the following values:

Option	Setting	Result
Number of old versions to keep for each file	-1	The user tries to upload another version but the upload will FAIL
Number of old versions to keep for each file	any number greater than 0	When the user uploads a new version of a file, it is saved, and the latest <Number of old versions to keep for each file> versions are kept.

To manage file versioning:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage**  .
   The **Managed Storage settings** page opens by default.
2. In **Number of old versions to keep for each file** type in **-1** to turn versioning off or any number greater than **0** to use versioning.



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

Configuring Zip Files and Zero Trust File Sharing

Beginning with FileCloud 23.241, zip files are enabled by default. Prior to FileCloud 23.241, zip files were disabled by default.
Functionality for creating and working with content in zip files in My Files is available beginning with FileCloud 22.1.
Functionality for creating and working with content in zip files in Network Shares is available beginning with FileCloud 23.232.

If you use encrypted storage and have zip files enabled, FileCloud creates temporary unencrypted copies of the files when performing actions on them. These files are only present briefly; however, if you want to avoid having the unencrypted data on your system, contact FileCloud Support to disable zip files.

Users can create and upload zip files into their My Files and Network Shares folders, and then preview, download, add, and delete contents of these zip files.

When users create zip files within FileCloud, they may add a password to them to create them as encrypted Zero Trust folders The password (decryption key) must be entered by the user who created the zip file or anyone they share the file with to access it. Note that the decryption key is not stored in FileCloud or known by the FileCloud system, and therefore makes the file invulnerable to attacks where the system is compromised.

For information about how users add and work with zip files, see Working with Zip Files.

By default, after the password is entered the first time during a log-in session, it does not have to be entered again during that session, but a setting in policies enables you to require users to enter the password each time they access it during a session.

To disable or re-enable the zip file feature

By default, the zip file feature described above is enabled. Please Contact FileCloud Support to disable it, or re-enable it after it is disabled.

Zip File Settings

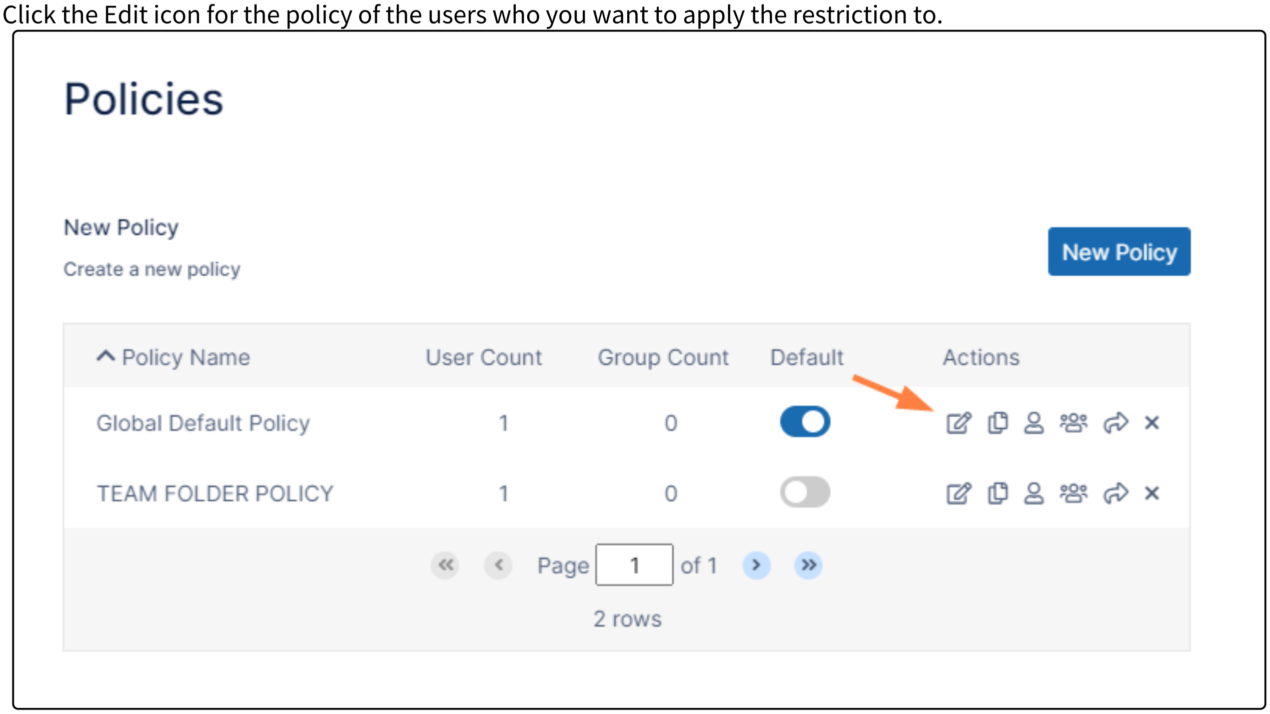
The following are default settings for zip files.

Setting	Default value
Encryption method	WinZip AES-256
Compression level	Normal

Setting	Default value
Compression method	Deflated
Fallback character set	None
Max zip file size	100 MB

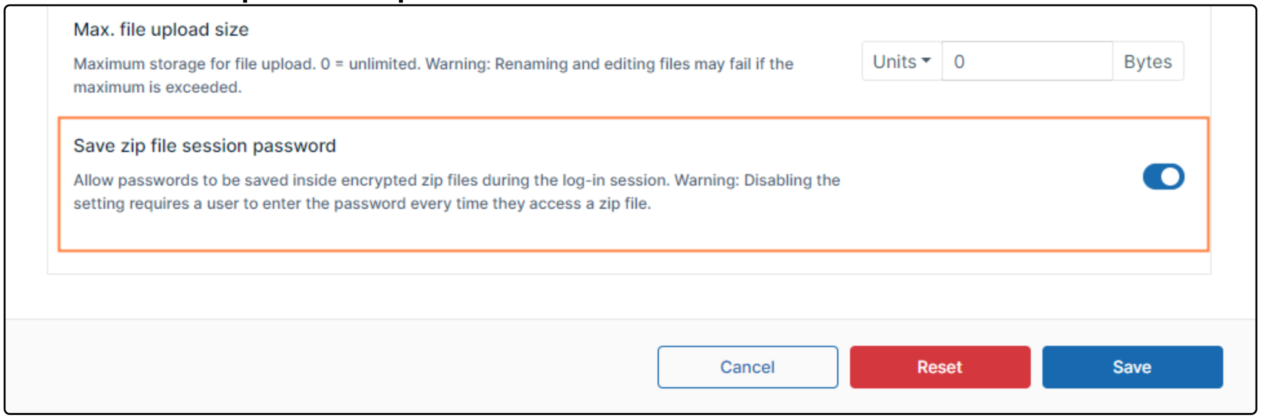
WinZip AES-256 encryption is not supported in Windows. If you are using Windows, Contact FileCloud Support to change your setting for the encryption method.

To require the password each time an encrypted zip file is accessed:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
2. Click the Edit icon for the policy of the users who you want to apply the restriction to.
   

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

5. Scroll down to **Save zip file session password** and enable it.



6. Click **Save**.
   Now, the users must enter the password each time they access the contents of the zip file.

Permissions in shared zip files

When a zip file is shared publicly, share users can view the contents of the zip file and download them. When a zip file is shared privately, the operations that share users can perform on its contents depends on their share permissions.

The following table shows what each share permission allows share users to do with the contents of a zip file

Permission	Description
View	Preview files and open folders in the zip file.
Download	Download files in the zip file and save them. Downloading folders in the zip file is not permitted.
Upload	Upload files into the zip file and delete files in the zip file.
Share	Share the zip file. Sharing of files and folders inside the zip file is not permitted.

Email Settings

Beginning with version 23.241.1, Azure XOAUTH XMTP with GCC High is supported.

Microsoft is replacing basic authentication with oAuth for emails sent using Office 365 in 2023. To address this change, beginning with version 22.1.1, FileCloud supports oAuth as an SMTP authentication method. To use SMTP oAuth with FileCloud, you must use Azure as an authorization provider.

FileCloud can send various messages to users via email, including:

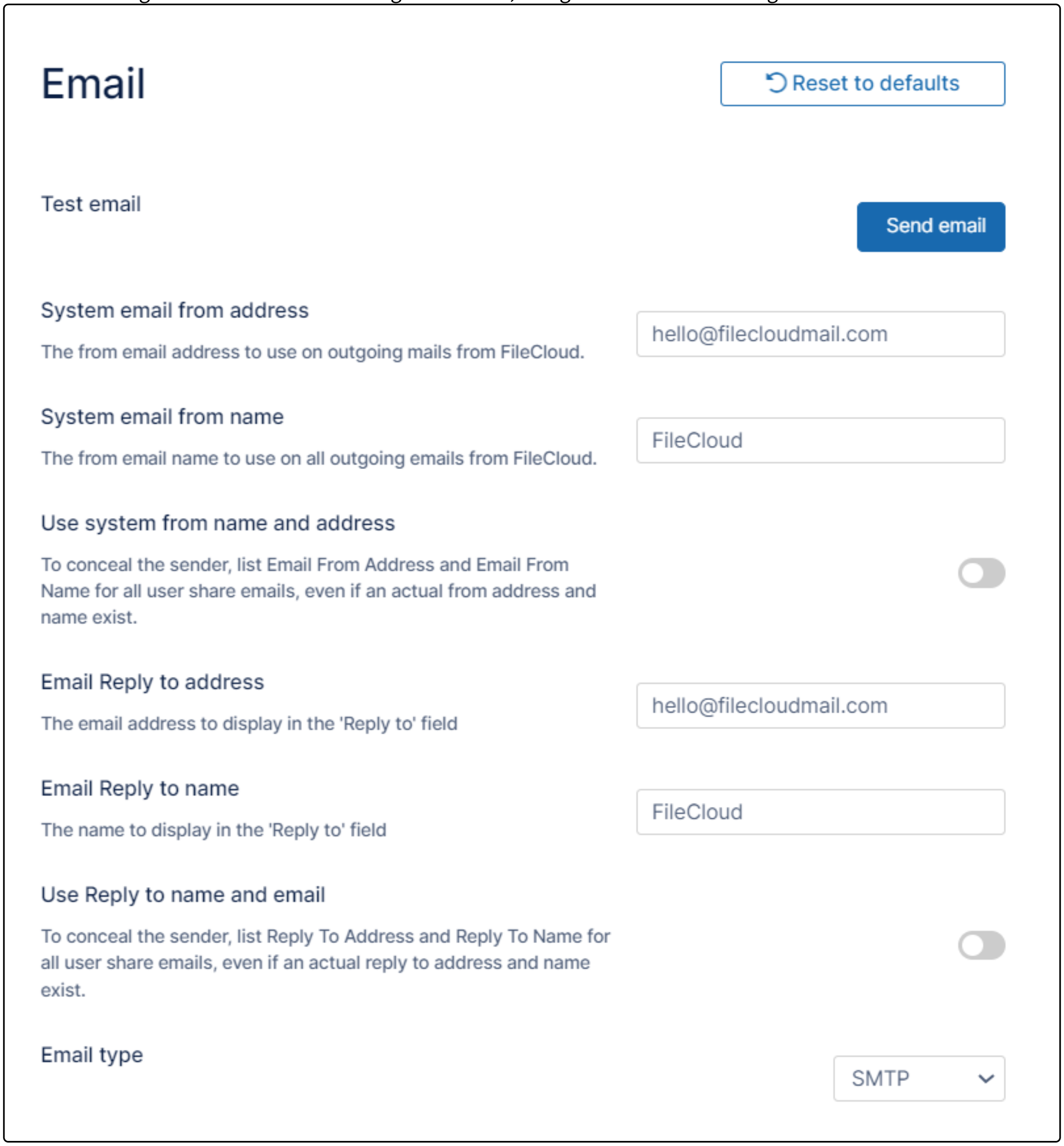
- share notifications
- file change notifications
- error notifications

For email to work smoothly with your system, configure the Email Settings below.

To configure email settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Email**  .
   The **Email** settings page opens.
   The general settings on the page begin with **System email from address** and go through **Email type**, as shown in the screenshot below.

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



General email setting information:

Setting	Description
System email from address	By default, **System email from address** is listed on emails if there is no email from address (for example, when emails are sent by the system or by workflows). ⚠ By default, admins cannot change the **System email from address**; it is set to fchosted@filecloudmail.com. If you want to change the **System email from address** or you want admin permission to change the **System email from address**, please Contact FileCloud Support. ℹ If you are using **SMTP** as your email type, and set **SMTP AUTH type** (listed below, under SMTP Configuration) to **XOAUTH2**, then set **System email from address** to the same value as **SMTP AUTH username**. This is required for successful use of Azure as the authentication provider.
System email from name	By default, **System email from name** is listed as the from display name from which email messages are sent to users. It is used if there is no email from name (for example, when emails are sent by the system or by workflows).
Use system from name and address	To conceal the sender, list the **System email from address** and **System email from name** for all user share emails, even if an actual from address and name exist.
Email Reply to address	By default, **Email Reply to address** is listed on emails if a reply to address does not exist (for example, when emails are sent by the system or by workflows).
Email Reply to name	By default, **Email Reply to name** is listed on emails when a recipient replies to an email without a reply to name (for example, when emails are sent from the system or by workflows).
Use Reply to name and address	To conceal the sender, list **Email Reply to address** and **Email Reply to name** for all user share emails, even if an actual reply to address and name exist.
Email type	Specify the email facility to be used. The type can be **SMTP**, **Mail** or **SendMail**. Note that **Mail** and **SendMail** use the underlying OS's function (and are available only for Debian/Ubuntu installation). The recommended setting is **SMTP**.

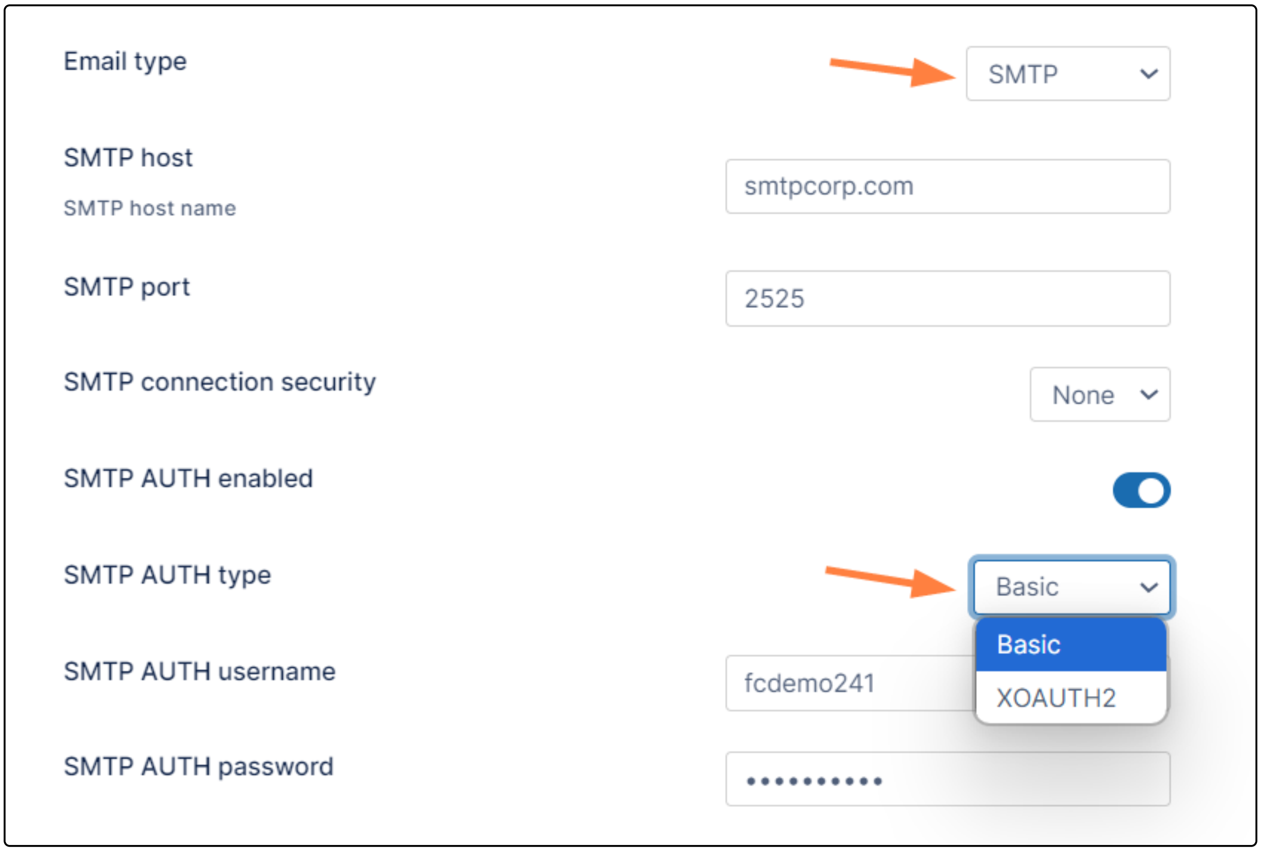
3. If you choose **SMTP** for **Email Type**, complete the following steps for filling in the SMTP fields. If you choose **Mail** or **SendMail** for **Email Type**, skip these steps, and go to Do Not Email Settings.

SMTP Configuration

Note: You must have an SMTP account to set up email using SMTP.

To configure SMTP in Email settings:

1. In **Email Type**, choose **SMTP**.
   The SMTP fields below it become enabled.



2. Fill in the SMTP fields according to the descriptions in the following tables.
   The value you choose for **SMTP Auth Type** determines which additional SMTP fields are displayed below.

Office 365 Settings
When using Office 365, SMTP settings must be set to the following values:

Setting	Recommended value
SMTP host	smtp.office365.com
SMTP port	587
SMTP connection security	TLS

Setting	Recommended value
SMTP AUTH username, SMTP AUTH password	Enter the sign in credentials of the hosted mailbox being used.

For more information about SMTP configuration for Office 365 accounts see the Microsoft Office Support Article.

SMTP Setting	Description
SMTP Host	SMTP Server to use for sending email
SMTP Port	The SMTP port to use to connect to SMTP Host (provided by your SMTP provider)
SMTP Security	If your SMTP provider uses SSL or TLS security then select the appropriate value.
SMTP AUTH enabled	If SMTP requires authentication, then check this to enable and enter the authentication settings.
SMTP AUTH type	**SMTP Auth Type** may be **Basic** or **XOAUTH2**. The option you choose determines which additional SMTP fields follow. • **Basic** authentication requires the user to enter a username and password. It is supported by many email providers, but is being deprecated in Microsoft 365 in Exchange Online in early 2023. • **XOAUTH2** refers to OAuth 2.0 authentication, which uses temporary single-use tokens to provide a more secure method of verification. XOAUTH2 will now be used with Microsoft 365 for Exchange Online and is also the method used by a number of other providers.

If you choose **Basic** for **SMTP Auth Type**, enter values for the following fields:

Field	Value to enter
SMTP AUTH username	The authentication username.
SMTP AUTH password	The password for SMTP AUTH username.

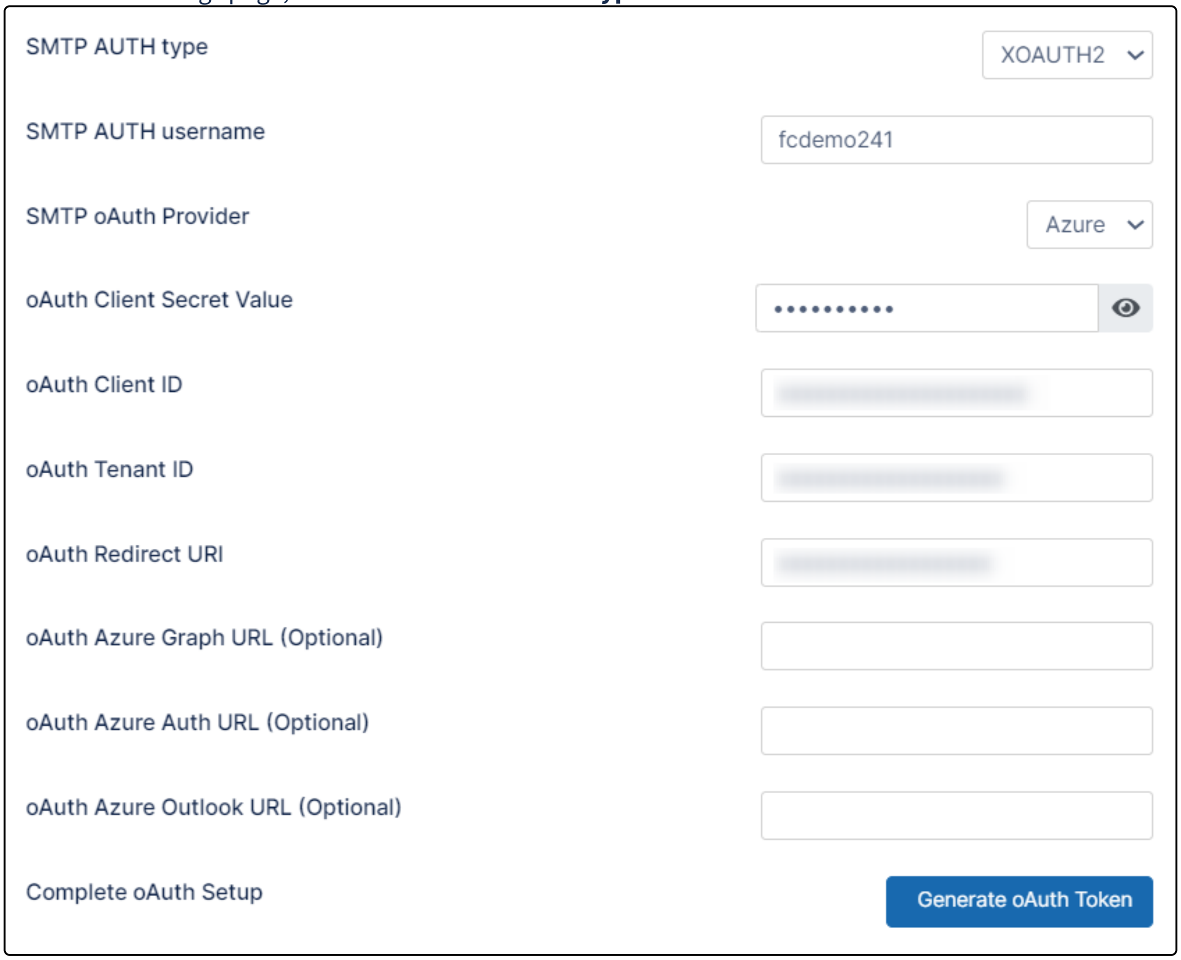
If you choose **XOAUTH2** for **SMTP Auth type**:

a. Review the following information.

> ⚠ XOAUTH2 token generation must be performed by the FileCloud master admin and not by a promoted admin user.
> To avoid configuration issues with Microsoft 365 XOAUTH2 setup due to Azure permissions settings, we recommend the following:
> **If you are able to use an Azure global admin as the SMTP AUTH username in FileCloud**:
>
> i. Use an Azure global admin account to create the FileCloud XOAUTH2 application.
> ii. Use the same Azure global admin account in the FileCloud email settings **System Email from address**, **Email Reply to address**, and **SMTP AUTH username**.
> iii. Use the Azure global admin account to grant permissions when generating the XOAUTH2 token.
>
> **If you are not able to use an Azure global admin as the SMTP AUTH username in FileCloud**:
>
> i. Use an Azure global admin account to create the FileCloud XOAUTH2 application.
> ii. Do not use the same Azure global admin account for the FileCloud email settings **System Email from address**, **Email Reply to address**, and **SMTP AUTH username**, but do set all three of these fields to a single email address.
> iii. Assign the email entered into **SMTP AUTH username** to the FileCloud XOAUTH2 application:
>   1. Log into **portal.azure.com** and go to **Microsoft Entra ID > App registrations**.
>   2. Click the FileCloud XOAUTH2 application, and in the navigation panel, click **Roles and administrators**.
>   3. Click **Cloud Application Administrator**, and then click **Add assignments** and assign the FileCloud **SMTP AUTH username** to the FileCloud XOAUTH2 application.
> iv. Use the **SMTP AUTH username** to grant permissions when generating the XOAUTH2 token.
>
> **If neither of the above options work, confirm that SMTP AUTH is enabled for the SMTP AUTH username and your Organization**:
> To check if SMTP AUTH is enabled for the **SMTP AUTH username**:
>
> i. Open Microsoft 365 admin center and go to **Users > Active Users** and check the **SMTP Auth User**.
> ii. In the right panel, click **Mail**, and then click **Manage Email** apps.
> iii. If **Authenticated SMTP** is not checked, check it.
>
> To check if SMTP AUTH is enabled for your **Organization**:
>
> i. Go to the Microsoft Exchange admin center and click **Settings**, then click **Mail flow.**
> ii. If **Turn Off SMTP Auth Protocol for your Organization** is not checked, check it and click **Save.**
>
> **If none of these options work, contact Microsoft Support for help.**

b. Go to the page Microsoft Azure and XOAUTH2 setup guide and follow the instructions under **Configure an OAuth2 app in Microsoft Azure** to register your oAuth application in portal.azure.com.

c. In the **Email** settings page, scroll down to **SMTP Auth type** and the **oAuth** fields.



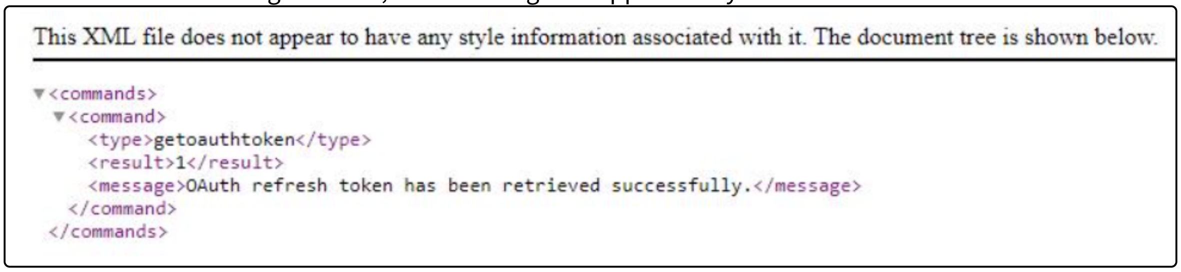
d. Fill in the SMTP oAuth fields on the Email Settings page listed in the table below:
For the fields **oAuth Client Secret Value**, **oAuth Client ID**, **oAuth Tenant ID**, and **oAuth Redirect URI** , retrieve the values from portal.azure.com after registering the oAuth application.

SMTP Auth User	Enter the authentication username You must set **Email From Address** (described above under **General email setting configuration**) to the same value as **SMTP Auth User**. This is required for successful use of Azure as the authentication provider.

SMTP oAuth Provider	Choose the oAuth provider (authorization server). Currently, the only available option is **Azure**.
oAuth Client Secret Value	The secret key your FileCloud system uses to get a temporary token from the authorization server.
oAuth Client ID	Application (client) ID from the SMTP provider application. This ID is used to get the temporary token from the authorization server.
oAuth Tenant ID	Directory (tenant) ID used to get the temporary token from the authorization server. (This field is applicable only when Azure is the provider; when other providers are added, it will not be required for them.)
oAuth Redirect URI	The location (appended with the parameter holding the token) where the authorization server should send the user after the token has been generated. The location specified should be your FileCloud domain. Use the format https://your-filecloud-domain.com/admin/getoauthtoken
oAuth Azure Graph URL oAuth Azure Auth URL oAuth Azure Outlook URL	If you are using Azure XOAUTH SMTP with GCC High, fill in these fields as follows:  If you are using Azure XOAUTH SMTP without GCC High, these settings default to the correct values for the non-GCC High setup, and it is not necessary to enter them. However, you may enter the correct values, which are: https://graph.microsoft.com https://login.microsoftonline.com https://outlook.office.com
Complete oAuth Setup	Click **Generate oAuth Token** so you can begin using email with oAuth.

e. If your **SMTP AUTH type** is **XOAUTH2**, do the following:
After you have filled in the SMTP fields, click **Generate OAuth Token**.
If you are not logged in to your Microsoft authenticator app, you are prompted to log in so you can access Azure to generate the token.

Once the OAuth token is generated, the following XML appears on your screen:



3. Click **Send email** at the top of the screen to test the settings.

If your setup is valid, the email is sent to the admin's email, and a success notification appears on your screen.

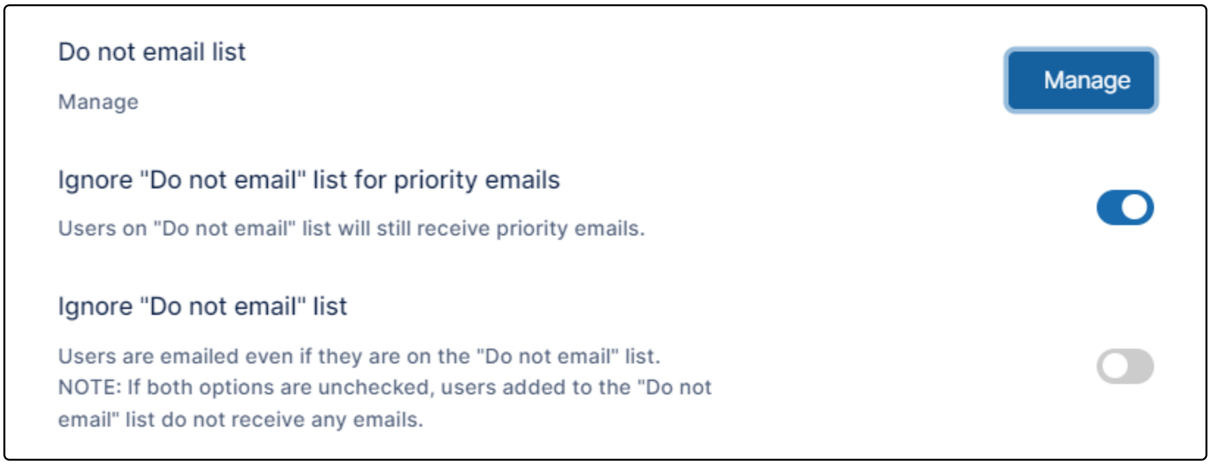
Do Not Email Settings

- Emails get added to the **Do not email** list when users click **unsubscribe** in the email body.
- Beginning with FileCloud version 20.3, admins can add or remove users from the **Do not email** list by clicking **Manage** beside **Do not email list**.
- Admins can specify the maximum number of emails that system can send in a 24 hour span.
- Users on the **Do not email** list do not receive any emails unless **Ignore "Do not email" list for priority emails** or **Ignore "Do not email" list** are checked**.**

To send emails to users on the Do not email list

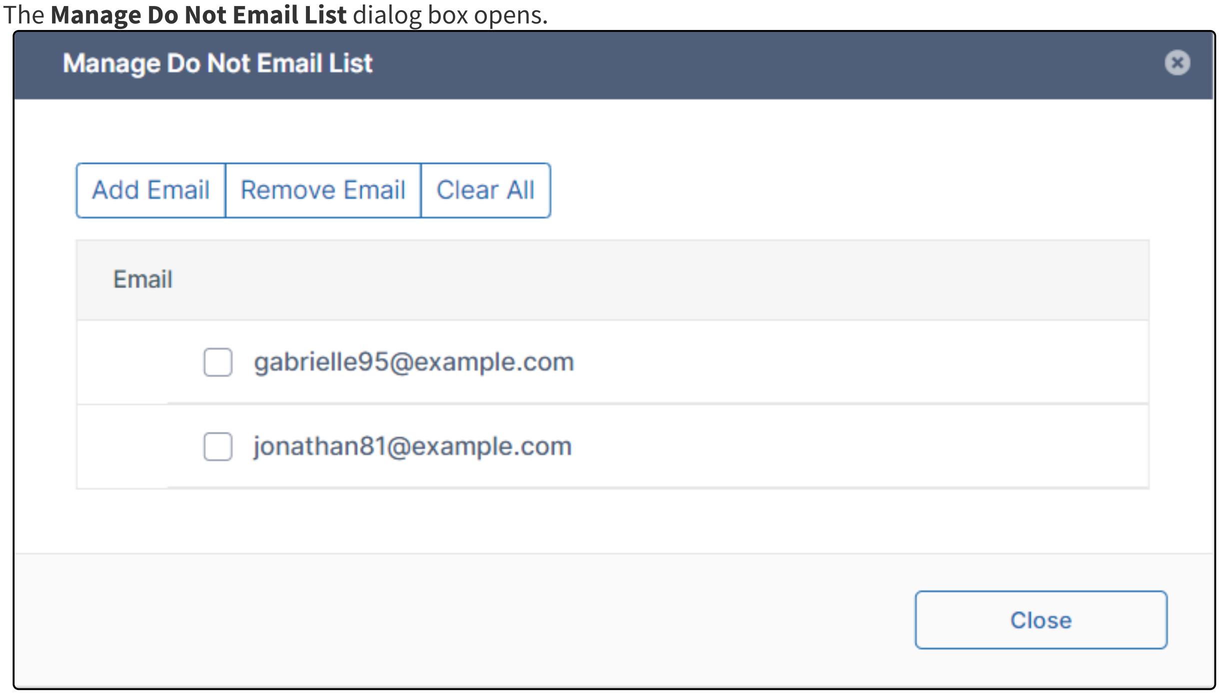
By default, users on the **Do not email** list do not receive any emails

- To allow users on the **Do not email** list to receive important emails like password recovery and 2FA, check the **Ignore "Do not email" list for priority emails** checkbox .
- To ignore the **Do not email** list and send all emails to users who are on the list., check the **Ignore "Do not email" list** checkbox.



To add or remove users from the Do Not Email list:

1. Next to **Do not email list**, click **Manage**.
   The **Manage Do Not Email List** dialog box opens.

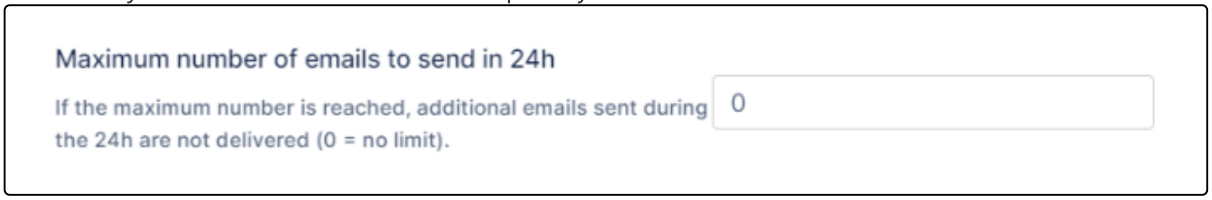


2. To add an email to the list, click **Add Email**, then enter and save an email address.
3. To remove an email from the list, check the box next to the email and click **Remove Email**.

To limit the number of emails sent to a user

If your users are receiving too many email notifications, you can limit the number of FileCloud system-generated emails sent to them in 24 hours.
In the field **Maximum number of emails to send in 24h** at the bottom of the **Email** settings page, enter the maximum

number of system emails to be sent each user per day.



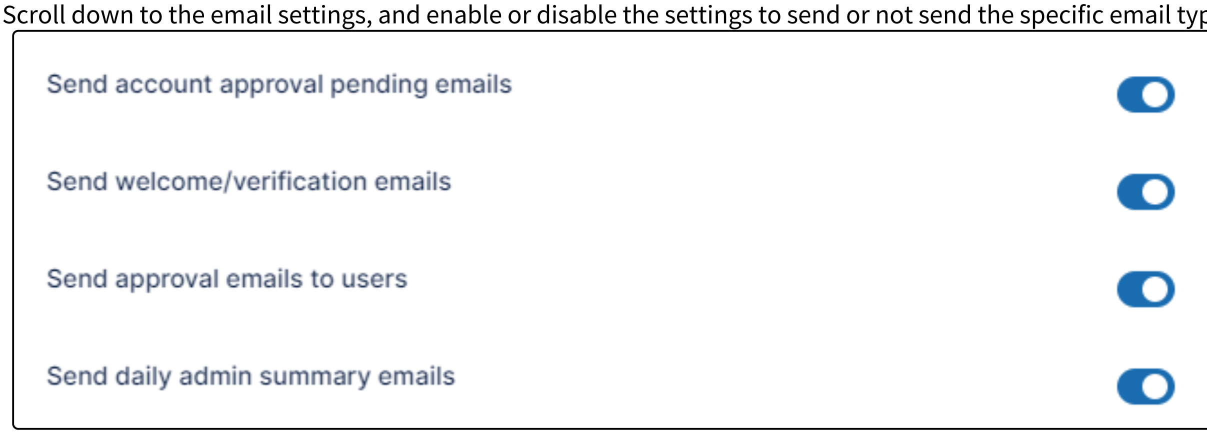
Configuring System Generated Emails

Controlling System Generated Automatic Emails

It is possible to control which emails are sent by the system.

To change the email settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Admin**  .
   The **Admin** settings page opens.
2. Scroll down to the email settings, and enable or disable the settings to send or not send the specific email types.



Send account approval pending emails	Send an approval pending email to the admin when a new user account is created and admin approval is required.
Send welcome/ verification emails	Send verification emails to users to verify their email addresses.
Send approval emails to users	Send account approval emails to users.
Send daily admin summary emails	Send daily system summary emails to the main admin account, This only works if a Cron Task or Windows Task Manager is setup.

3. Click **Save**.

Endpoint Backup Settings

FileCloud lets you configure automatic backup settings for users' files and folders to ensure their data is secure.

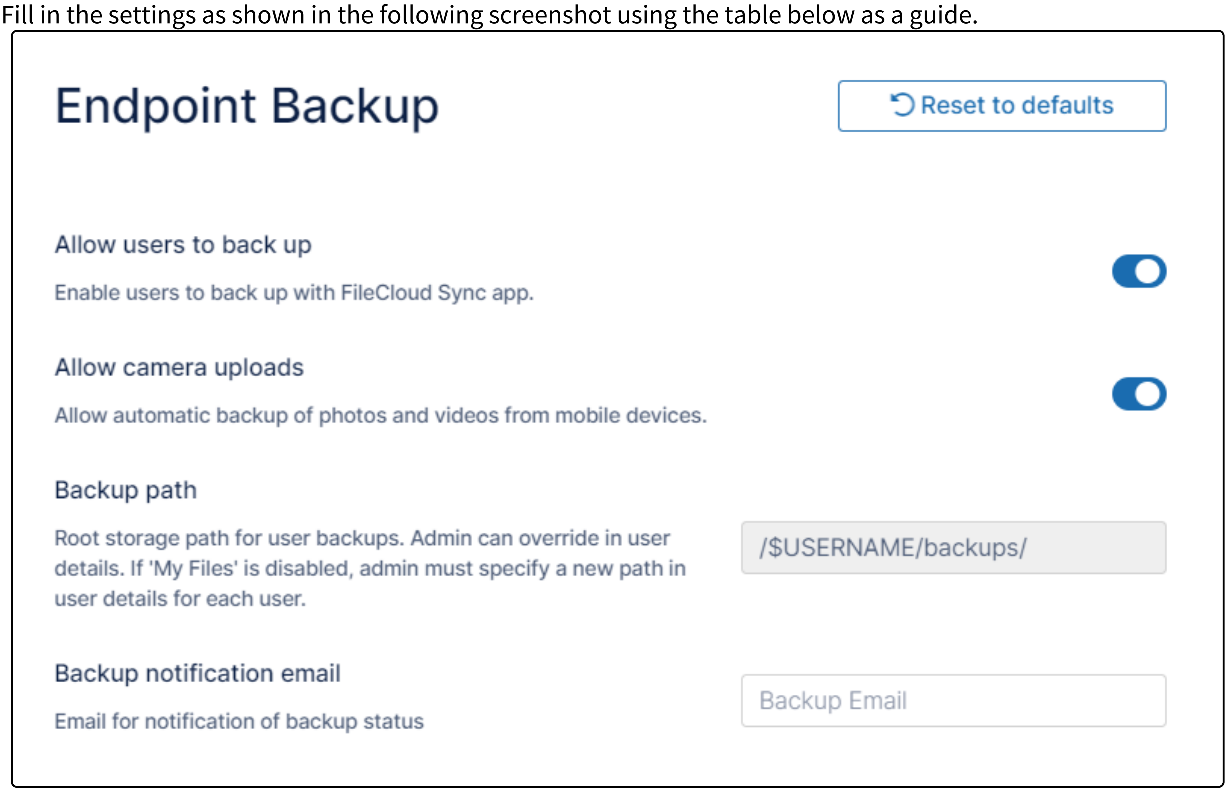
Note: FileCloud supports backing up files and photos from different devices.

What Do You Want To Do?

Configure backup settings for all users

To configure the backed up settings for all users:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Endpoint Backup** .
   The **Endpoint Backup** settings page opens.
2. Fill in the settings as shown in the following screenshot using the table below as a guide.



Settings Name	Description
Allow users to back up	Allow users to back up files and folders using the FileCloud Sync app. See Backing Up Files. This setting also enables you to configure Sync backup of specific files and folders for all users. See Globally Backing Up User Files and Folders.
Allow camera uploads	Allow mobile clients to automatically back up photos and videos to their FileCloud accounts. Turning off this setting prevents this server from being used to back up audio/video files. All camera uploads are stored in the user's backup folder. This location cannot be changed. For example, if the user name is jdoe, the camera uploads are stored in /jdoe/backups/<phone name>
Backup path	The location where automatically updated media and backup files are stored. This is a read-only field meant for display only. You can override this path for specific users to have them back up to a different location in the **User Details** screen (see below).
Backup notification email	An additional email ID to which Backup Complete notifications are sent.

Configure a specific user's backup folder

It is possible to set a different backup folder path for each user, overriding the default global path specified.

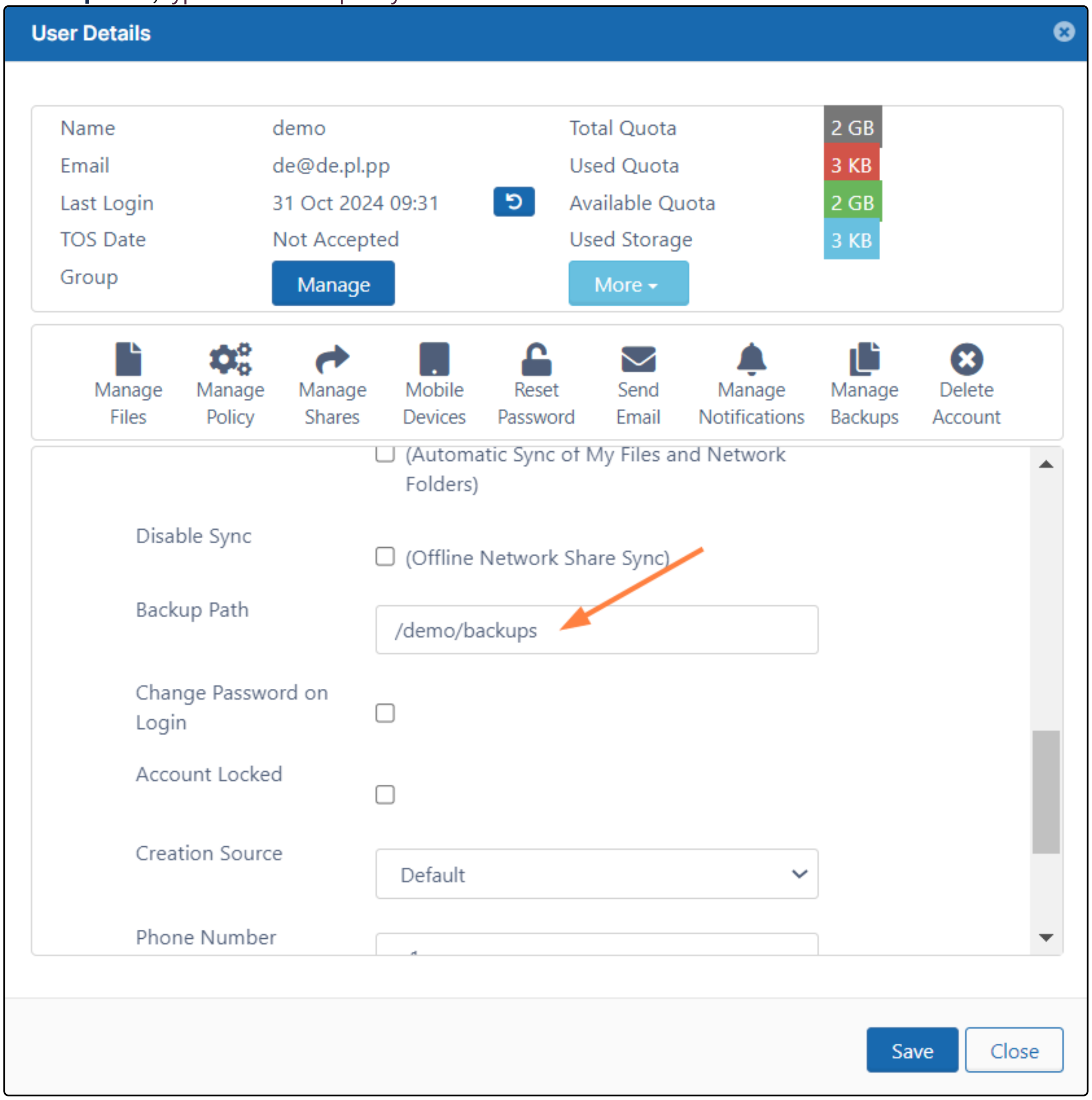
You must know the exact folder path you want to use.

For more information, see Identifying a FileCloud Specific Path.

To set the Backup Path for a user:

1. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Users**.
3. Click the **Edit** icon for the user whose path you want to change.
4. On the **User Details** screen, scroll down to the **Backup Path** field.

5. In **Backup Path**, type in the folder path you want to use.



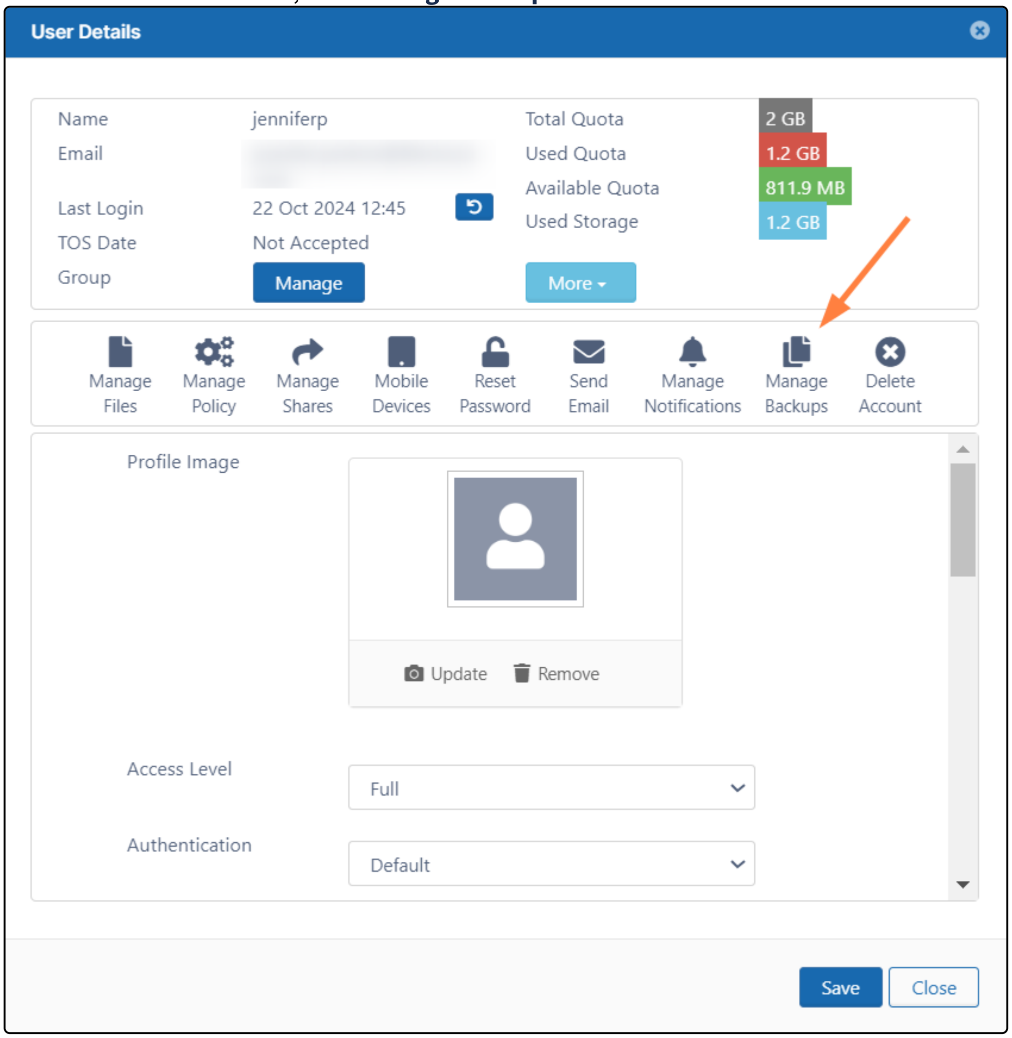
6. To save your changes, click **Save**.

View a user's backed-up files

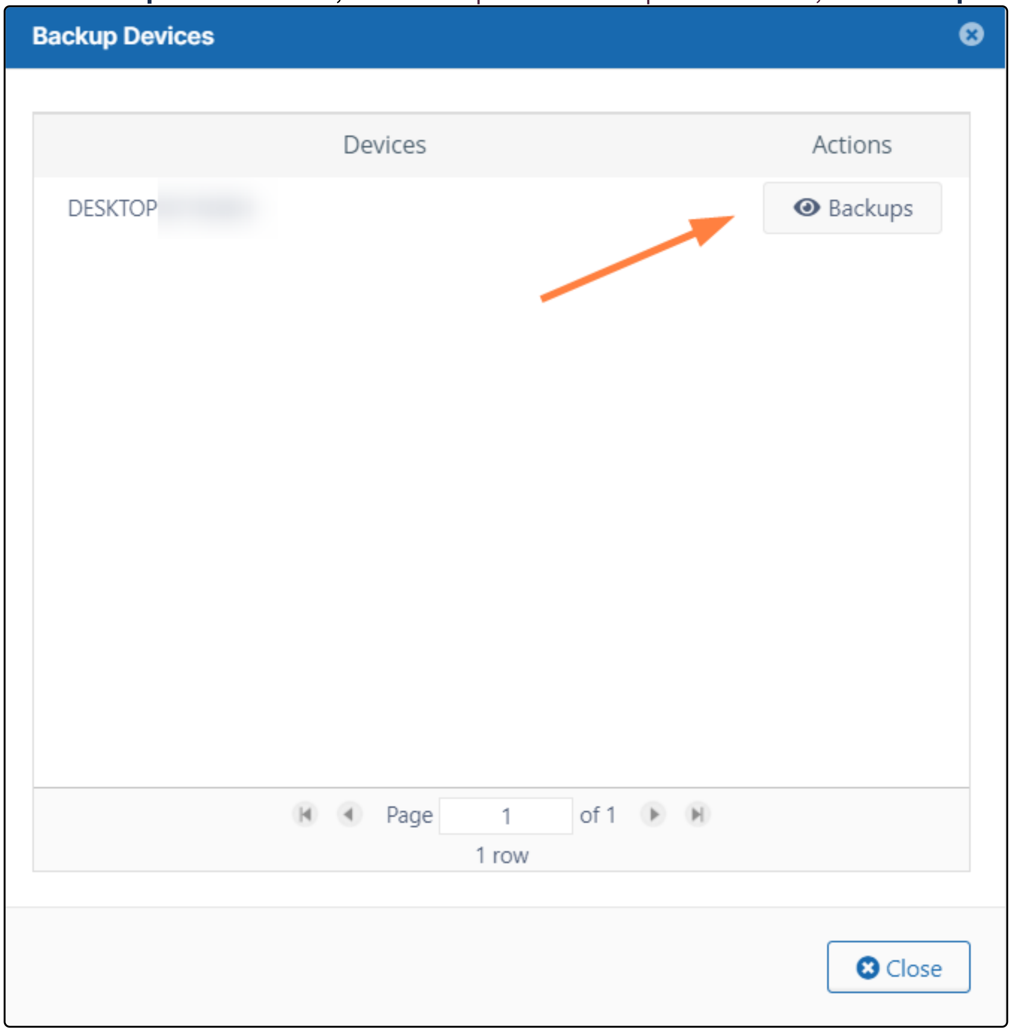
To view details of the backed up files for a specific user:

1. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Users**.
3. Click the **Edit** icon for the user whose path you want to change.

4. On the **User Details** screen, click **Manage Backups**.

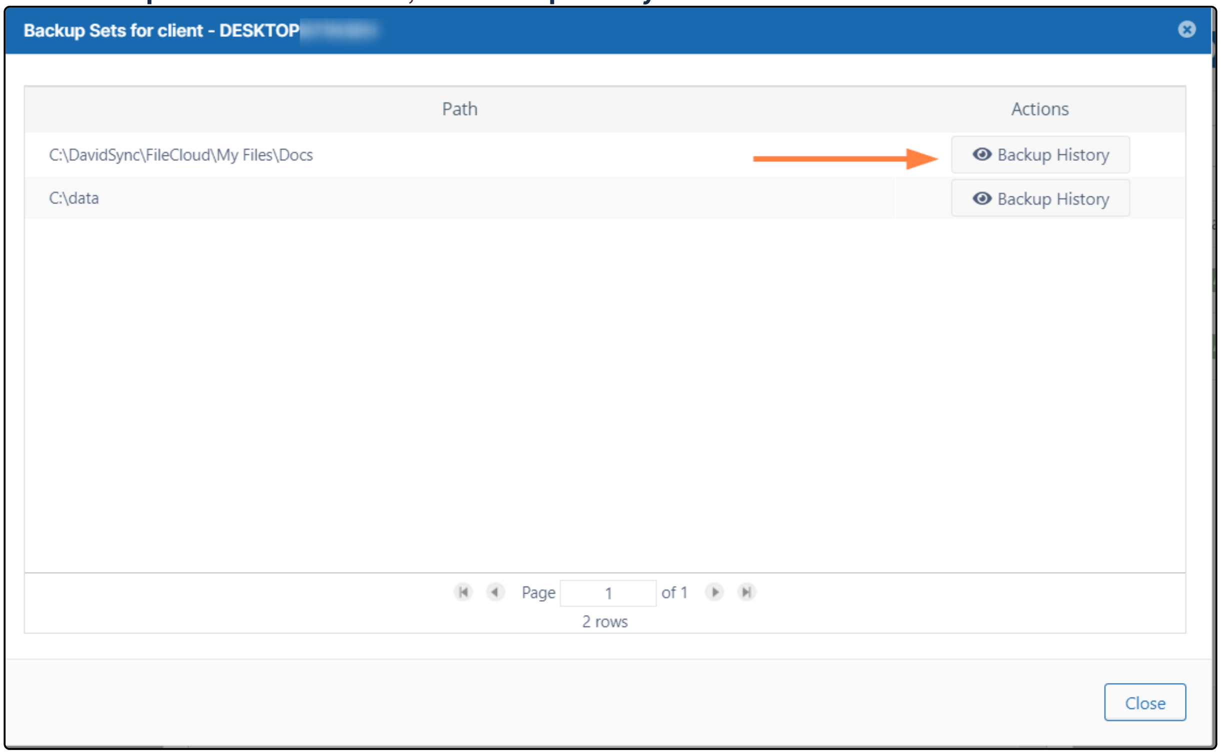


5. On the **Backup Devices** screen, to view the paths backed up from a device, click **Backups.**

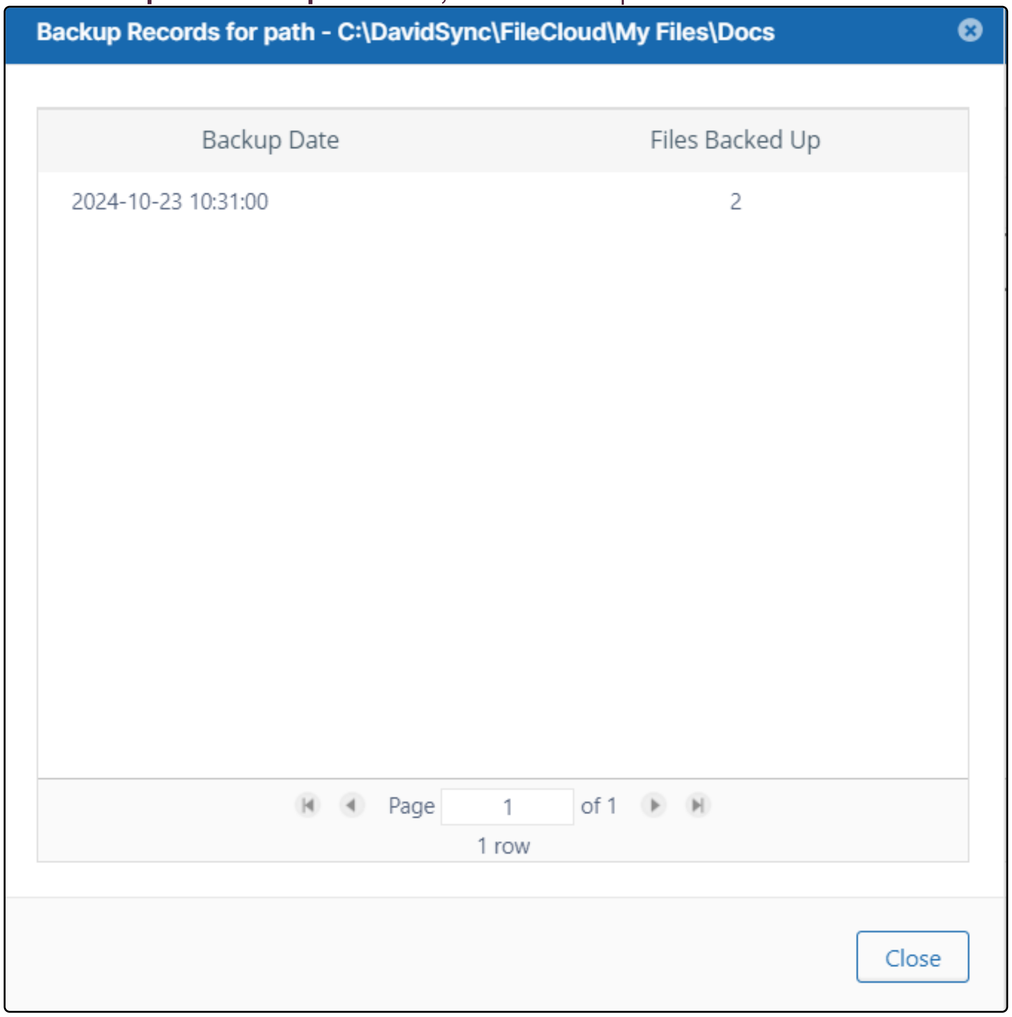


.

6. On the **Backup Sets for client** screen, click **Backup History** for a client.



7. On the **Backup Records for path** screen, view the backup dates and number of files backed up.



Also see:

- Automatic Database Backup
- Setting Up Persona Backup Using Sync

Automatic Database Backup

> In environments where high availability architecture is being used, automatic backups are performed during Cron runs.

By default, automatic database backups are enabled with the following configuration:

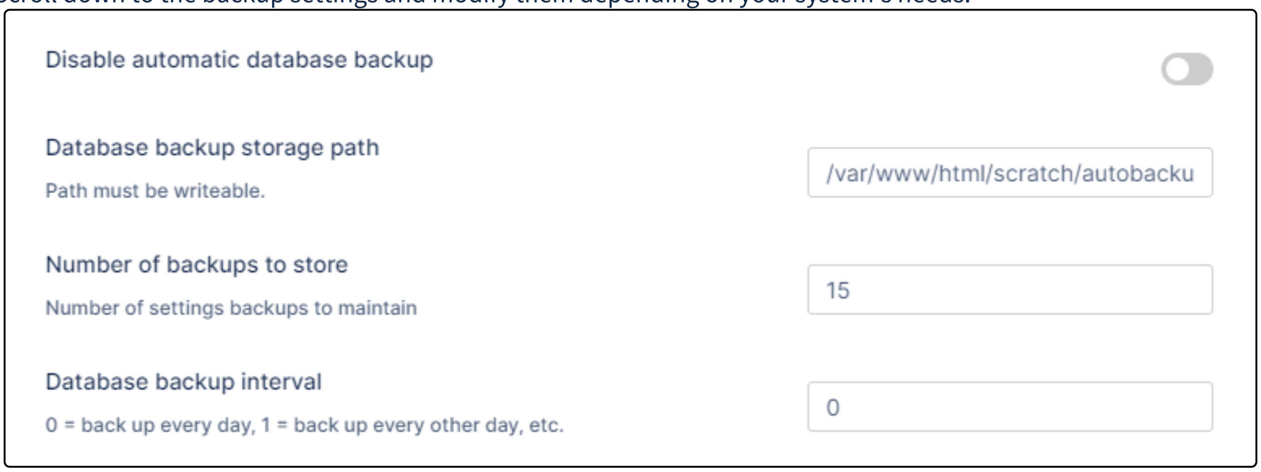
- Daily backups are stored in the following directory: .../scratch/autobackups/

- Backups are maintained for the last 15 days before being overwritten with new backups

As an administrator, you can change the location where backups are stored, the number of backups to maintain, and the number of days between backups. Or, if you already have a back-up strategy, you can disable automatic backups.

To configure automatic database backups:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Scroll down to the backup settings and modify them depending on your system's needs.

   Disable automatic database backup - Enable to prevent database back up during a Cron run. When disabled, automatic backup runs, and the last automatic backup run date is displayed.

   Database backup storage path - The path to the directory where backed-up database files are saved. You must use a path that is accessible to the FileCloud server, can have files saved to it, and has enough room for the backup files

   Number of backups to store -The number of days you want stored in a single backup file. By default, each backup file contains 15 days worth of data. If you want smaller files, you can lower this number. For example, if you type in 2 for **Number of backups to store**, the backup file will only contain 2 days worth of data. After those 2 days, the backup file is overwritten to store the next 2 days worth of data. This setting controls how far back you can recover data.

   Database backup Interval - The interval in days between each backup. The default is 0 which creates a daily backup of the number of days set in **Number of backups to store**.
3. Click **Save**.

Example

The Cherry Road Real Estate company needs to back up data from the last 30 days and wants the back-up refreshed every week. To do this, these are the settings they use:

- **Disable automatic database backup** = not selected
- **Database backup storage path** = /var/scratch/autobackups
- **Number of backups to store** = 30
- **Database backup Interval** = 7

Setting Up Persona Backup Using Sync

As an admin, you can use the FileCloud Sync app to set up a persona backup for all users of your FileCloud System. A persona backup saves individual settings and preferences for users across their FileCloud devices, making it easy for you to restore them.

To set up persona backup for users, open the policy used by them in the admin portal, and add device configuration code for Sync backup that includes the local paths that contain user specific configurations.

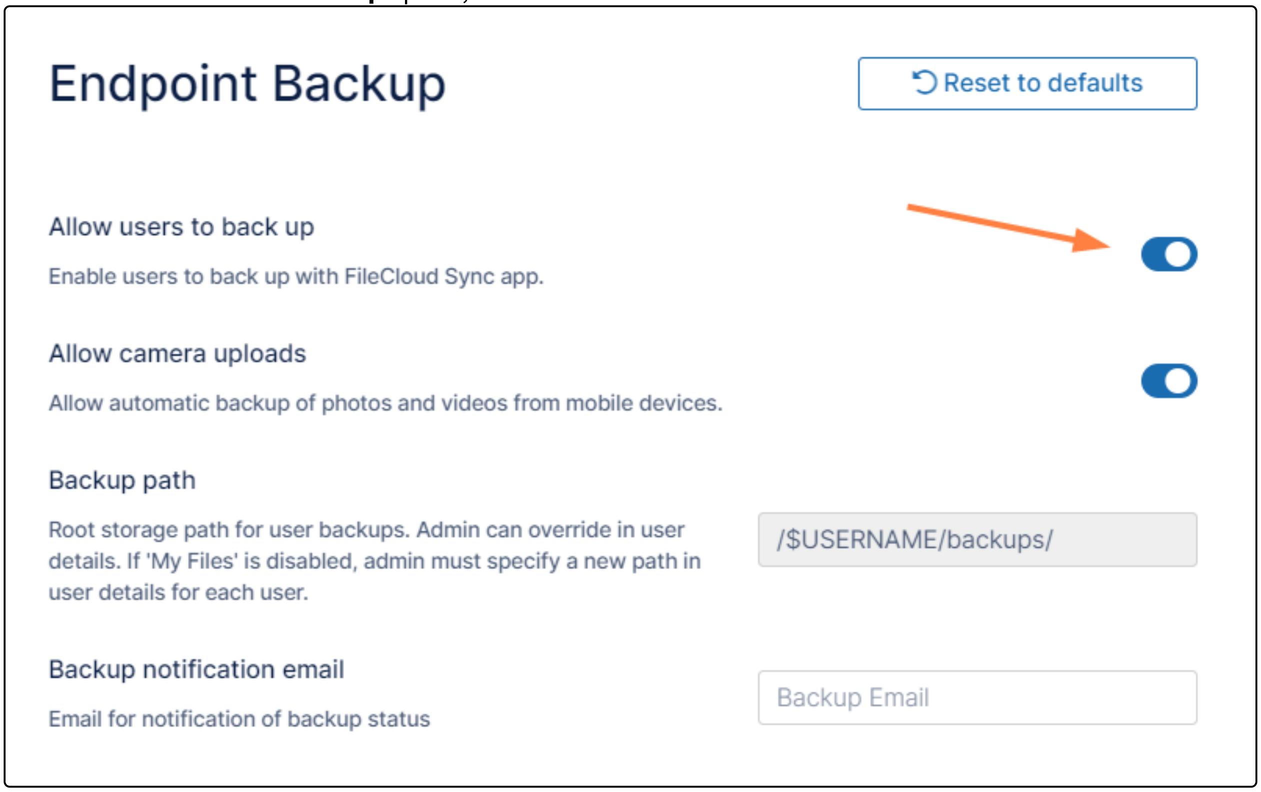
Steps:

1. Enable Endpoint Backup for FileCloud Sync from the Admin Portal.
2. Install FileCloud Sync on the users' computers, and enable Remote Management in Sync.
3. Set a default device configuration for Sync in the users' policy from the admin portal.

1) Enable Endpoint Backup for FileCloud Sync from the Admin Portal

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

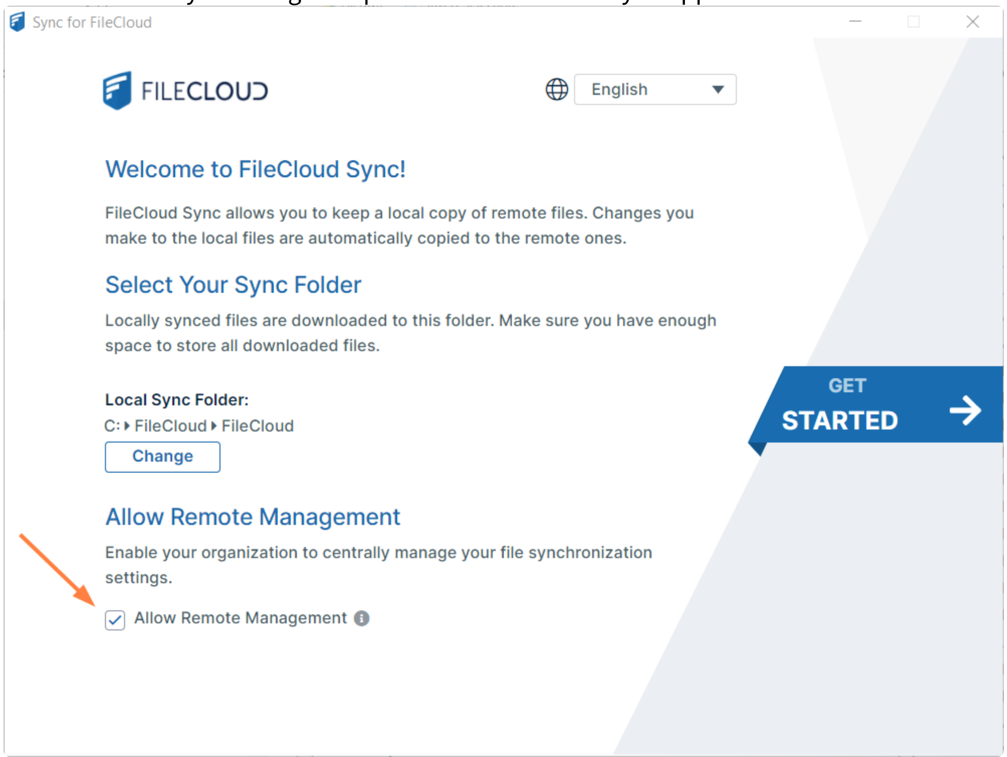
2. Enable the **Allow Users To Backup** option, and click **Save**.



2) Install FileCloud Sync and enable Remote Management

For backup to take place using the device configuration set up in the policy, Remote Management must be enabled in the FileCloud Sync App. This can be done by either:

- The user manually enabling the option in the FileCloud Sync App



- On a Mass Deployment, an admin enabling remote management by setting the **allowcentralmgmt** parameter to **1**. This requires registry entries to be created before FileCloud Sync is initialized on the users' local machines.
  Note: If FileCloud Sync is initialized prior to the creation of registry keys in the users' local machines, the configuration to enable remote management will not take effect.

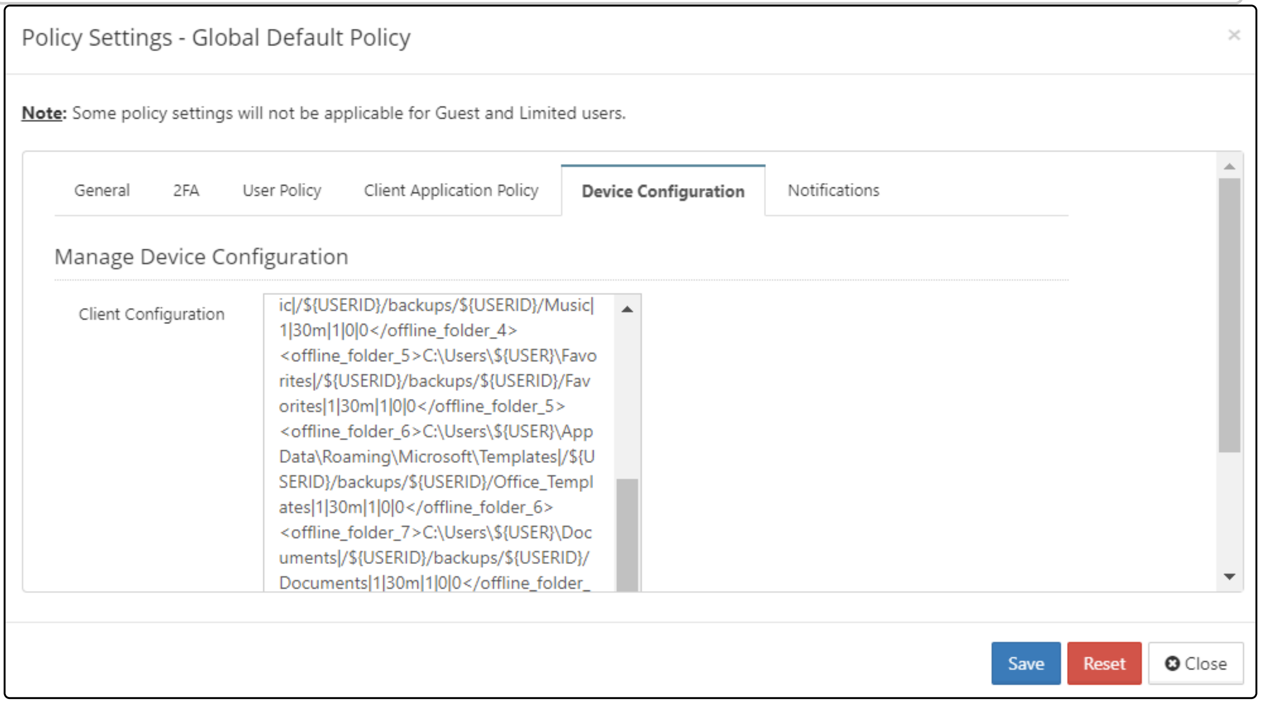
3) Set a default device configuration for Sync in the user's policy

Note: You must identify the local paths from the user's computer to include in the Sync Backup before creating the device configuration XML. Refer to the Device Configuration XML documentation for Sync.

1. Log in to the admin portal.
2. Navigate to **Settings > Policies** and edit the users' policy.
3. Go to the **Device Configuration** tab and enter the configuration in XML format. Below is a sample script to use. The first parameter of the XML, **<offline_folder_1>**, is a local path in the user's computer. The lines after it are the other local directories that must be included in the Sync Backup.

```
<xml>
<cloudsync>
<allowuserconfigforbackup>0</allowuserconfigforbackup>
<offline_folder_count>7</offline_folder_count>
<offline_folder_1>C:\Users\${USER}\AppData\Roaming\Microsoft\Outlook|/${USERID}/
backups/${USERID}/Outlook|1|30m|1|0|0</offline_folder_1>
<offline_folder_2>C:\Users\${USER}\Pictures|/${USERID}/backups/${USERID}/Pictures|
1|30m|1|0|0</offline_folder_2>
```

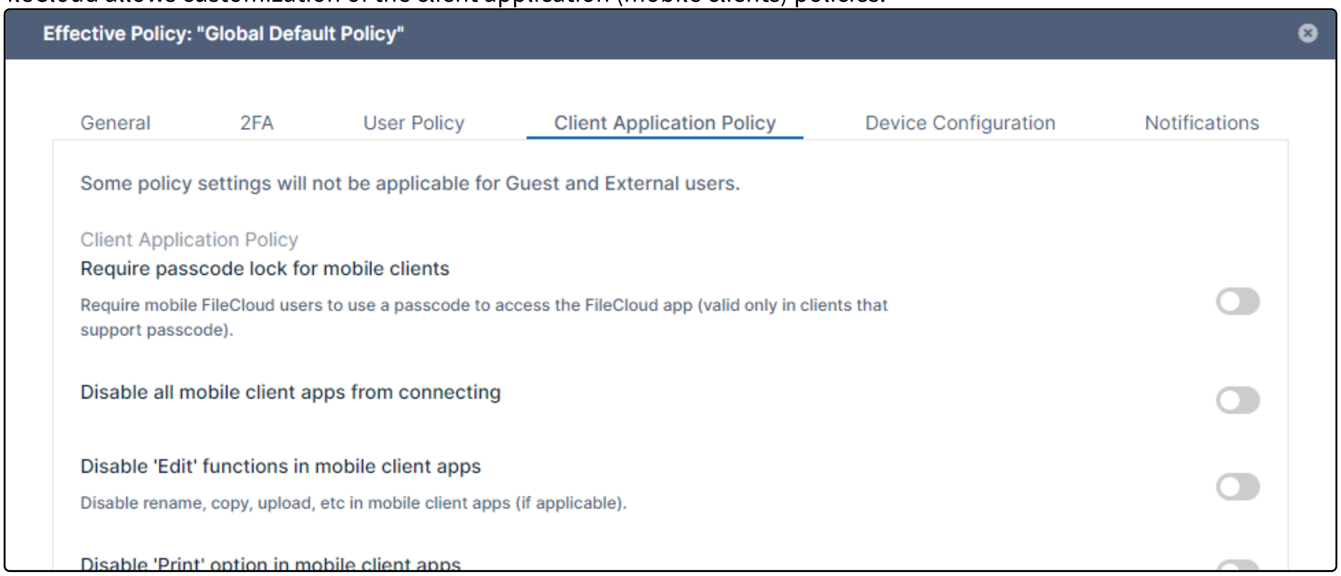
```
<offline_folder_3>C:\Users\${USER}\Desktop|/${USERID}/backups/${USERID}/Desktop|1|
30m|1|0|0</offline_folder_3>
<offline_folder_4>C:\Users\${USER}\Music|/${USERID}/backups/${USERID}/Music|1|30m|
1|0|0</offline_folder_4>
<offline_folder_5>C:\Users\${USER}\Favorites|/${USERID}/backups/${USERID}/
Favorites|1|30m|1|0|0</offline_folder_5>
<offline_folder_6>C:\Users\${USER}\AppData\Roaming\Microsoft\Templates|/${USERID}/
backups/${USERID}/Office_Templates|1|30m|1|0|0</offline_folder_6>
<offline_folder_7>C:\Users\${USER}\Documents|/${USERID}/backups/${USERID}/
Documents|1|30m|1|0|0</offline_folder_7>
</cloudsync>
</xml>
```



Client Security Settings

Setting Client Application Policies

FileCloud allows customization of the client application (mobile clients) policies.



Type	Description
Require Passcode lock for mobile clients	Force mobile clients to enable FileCloud app pincode. If the pincode is not enabled, the login is rejected with an appropriate message.
Disable all mobile client apps from connecting	Prevent login to FileCloud system using mobile client apps (users are allowed to login only via the web browser).
Disable edit functions in mobile client apps	Prevent delete, copy, and move operations from being performed from mobile client apps.
Disable "Print" option in mobile client apps	Prevent printing from mobile client apps (At this point only iOS app provides print function)
Disable "Download" option in mobile client apps	Prevent file downloads in mobile client apps.

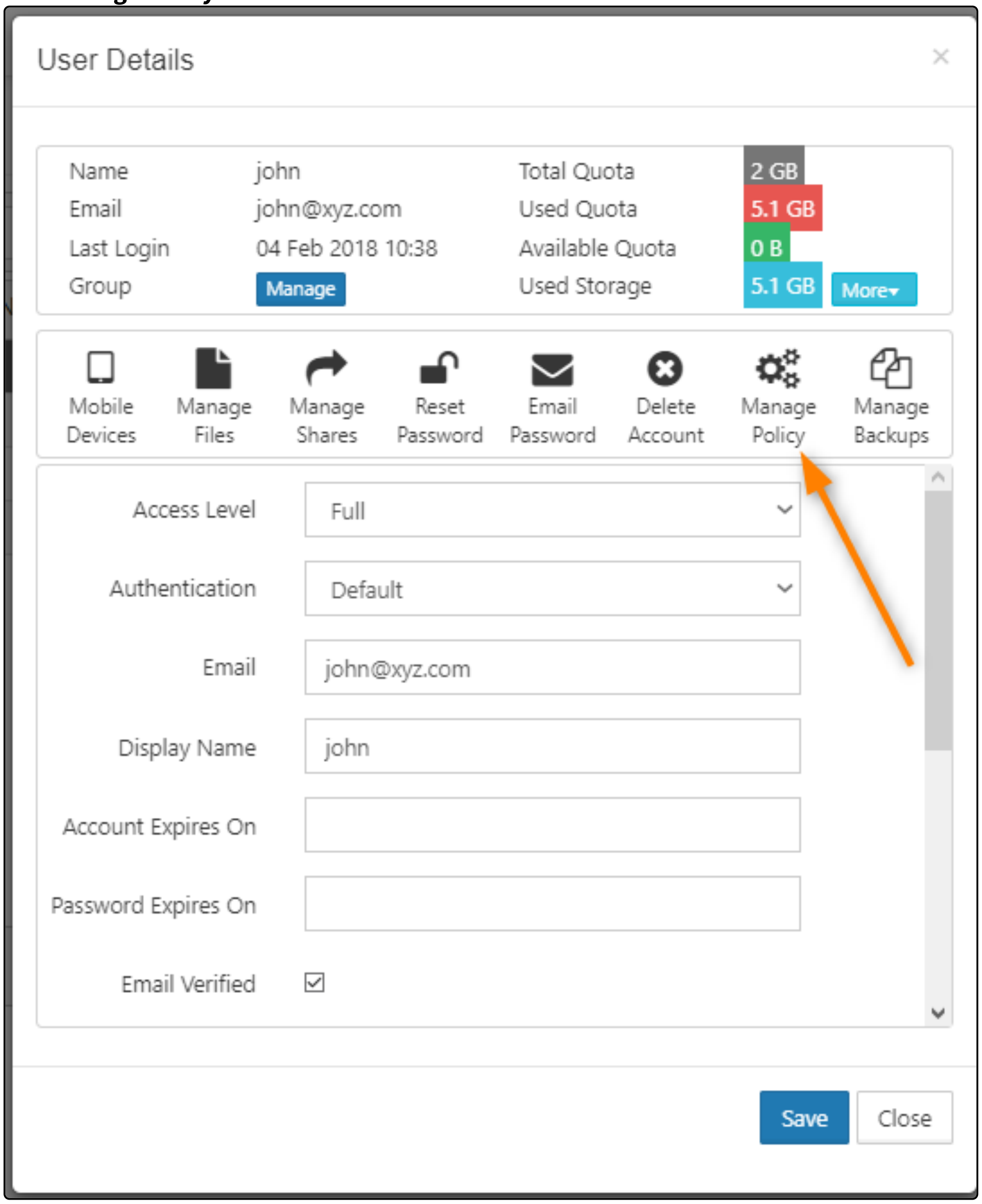
Type	Description
Disable "Open with" option in mobile client apps	Hide option to open a file in third party apps. NOTE: In Android, all files are opened in third party apps and this setting has no effect.
Disable "Share" options in mobile client apps	Hide file and folder sharing from mobile client apps.
Disable "Add to favorites" options in mobile client apps	Hide "Add to favorites" option from mobile client apps

You may override a policy when you are editing the user details for a specific user; however, the new policy settings apply to all users who are assigned that policy.

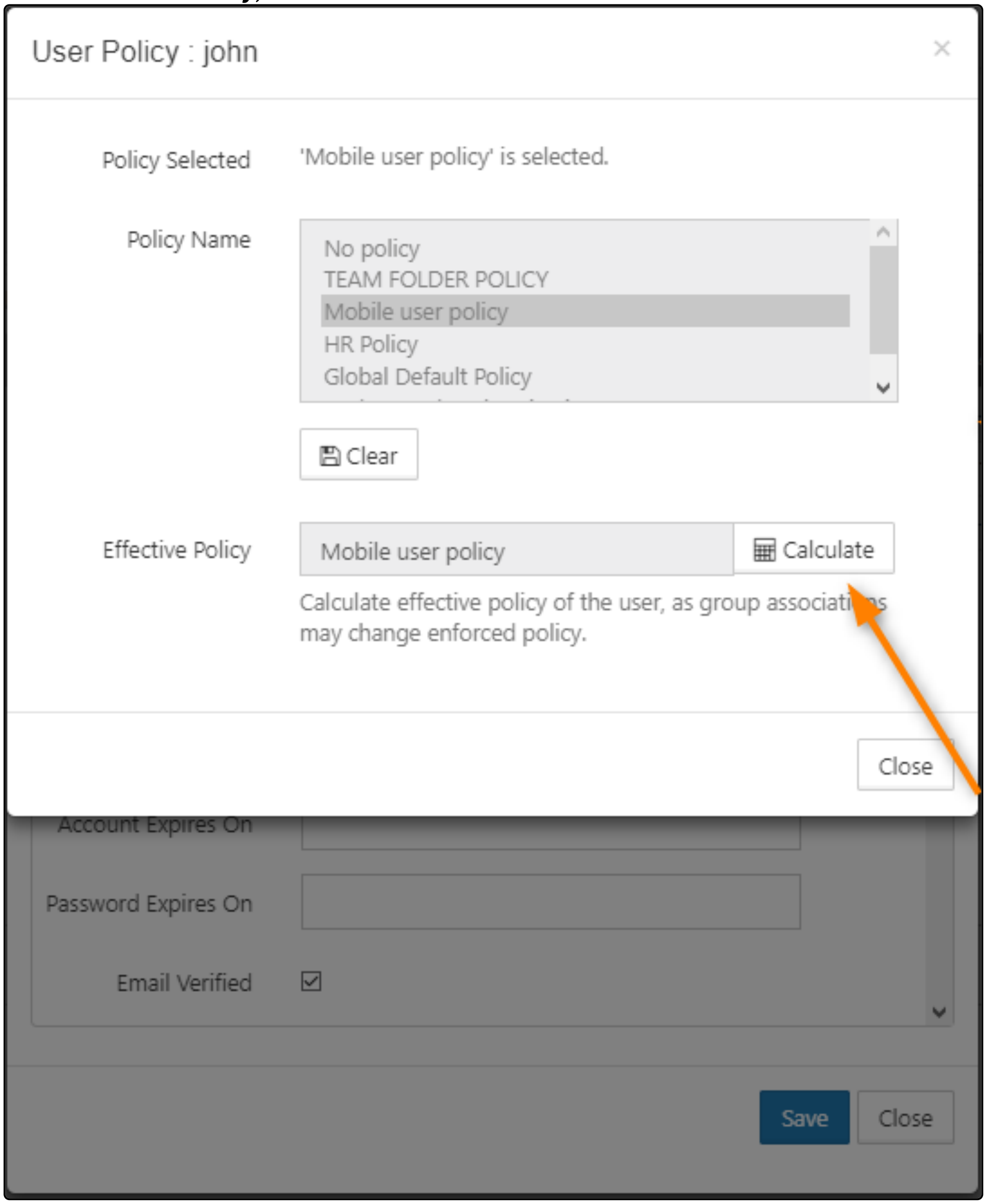
To change a policy through a user's details:

1. In the admin portal, go to **Users**.
2. Edit the user record.

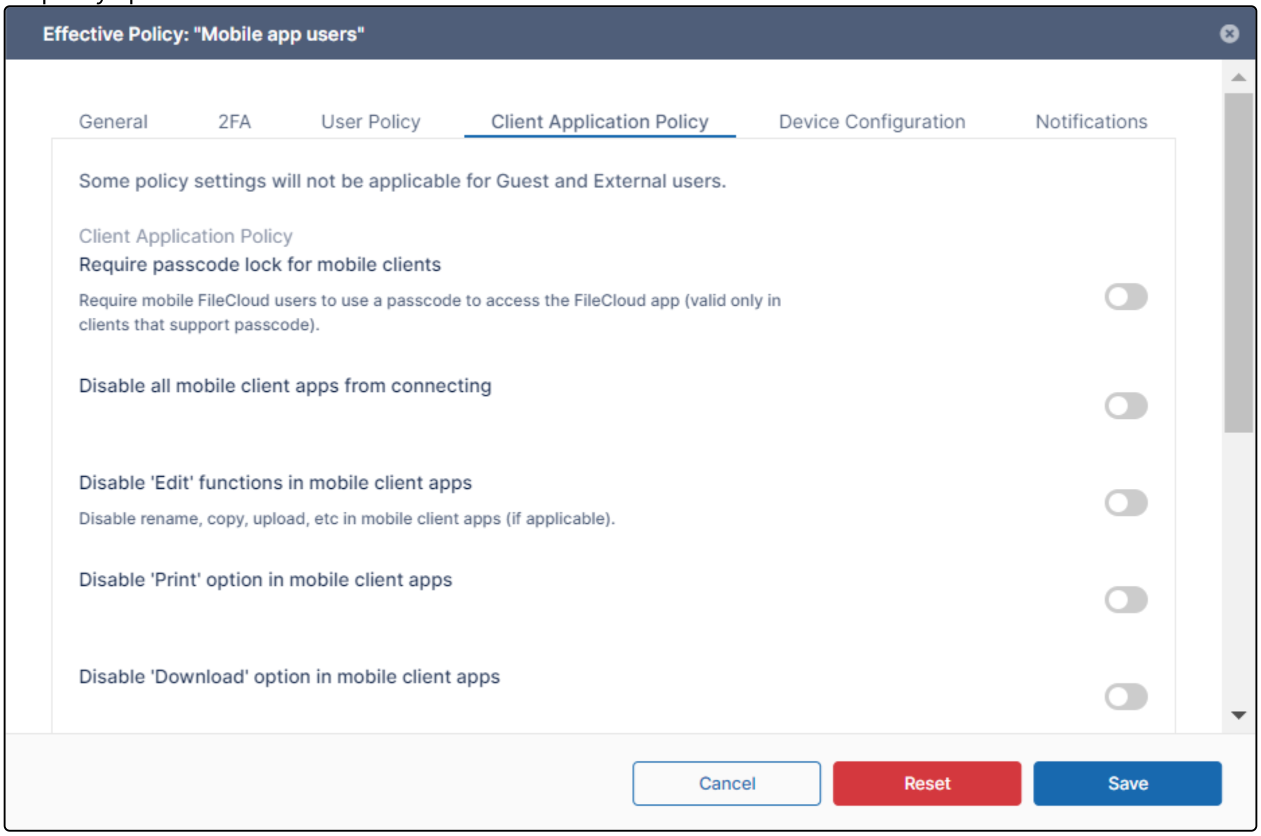
3. Click **Manage Policy.**



4. Next to **Effective Policy**, click **Calculate**.



5. Next to **Effective Policy**, click **Open**.
   The policy opens.



6. Change the settings and click **Save**.
   Note that the settings are changed for all users who belong to the policy.

Using a Proxy Server

As an Administrator, you can configure proxy network settings.

What is a proxy server?

A proxy server is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers.

1. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server.
2. The proxy server evaluates the request as a way to simplify and control its complexity.

Proxies are used to add structure and encapsulation to distributed systems.

Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and bypassing IP address blocking.

To configure proxy settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. Scroll down to **Enable Proxy Settings**, and enable it.
   Additional proxy settings appear.
3. Enter values for **Proxy host**, **Proxy port**, **Proxy user name**, and **Proxy password**.

4. Click **Save**.

Configuring OAuth for SCIM Integration

> Configuration of OAuth credentials that give external applications access to FileCloud resources is available beginning in FileCloud 23.252. SCIM is currently the only application that can gain access through this OAuth configuration, but in the future, additional applications may be added.
> FileCloud supports SCIM integration with Azure, Okta, and OneLogin, but most other SCIM IdPs should be able to connect to FileCloud using OAuth. Please contact your authentication service for support in configuring its integration with FileCloud.

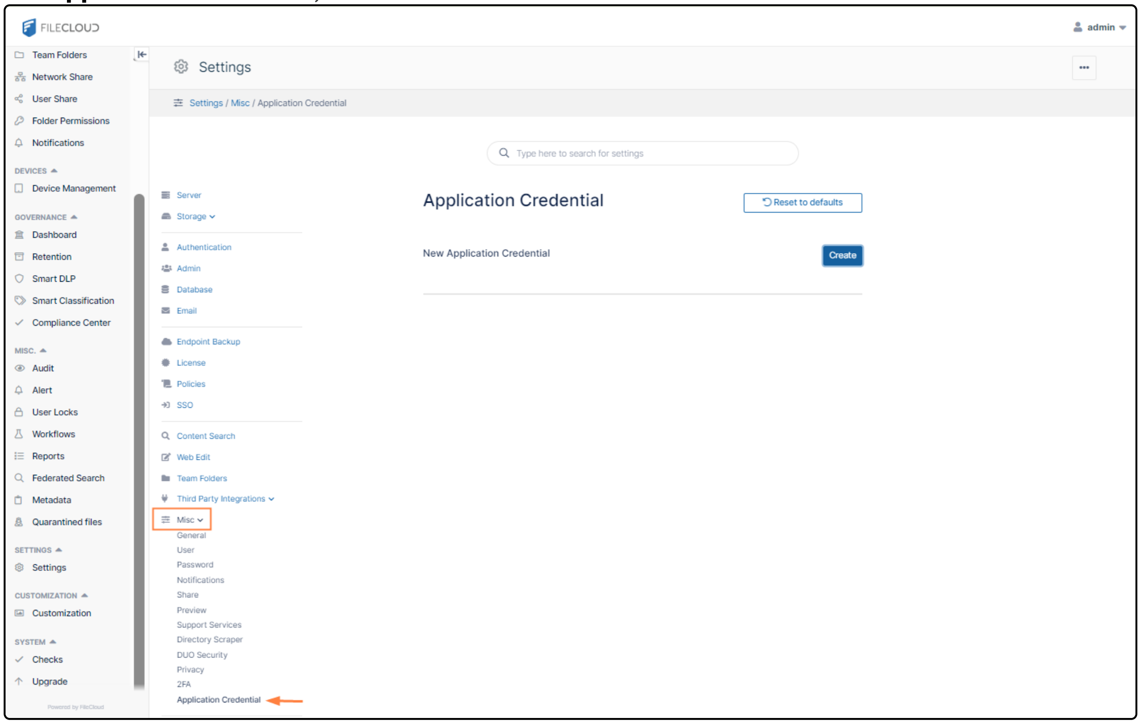
OAuth 2.0 authorization enables an application to securely access FileCloud resources without requiring a manual action or scheduled command to trigger the access request. OAuth 2.0 provides secure access by specifying scopes (permitted actions) associated with the access, and by creating unique tokens for accessing FileCloud. A token remains valid for an interval set in the configuration that may range from 1 hour to 5 years.

Currently, SCIM (System for Cross-domain Identity Management) is the only application that uses this OAuth configuration in FileCloud. SCIM is a protocol that enables you to update FileCloud user and group information by syncing it with changes made to user and group information in other applications. When SCIM detects a change in one of the apps, it uses OAuth 2.0 to gain access to FileCloud and update its user/group data.

To configure OAuth application credentials for SCIM in FileCloud:

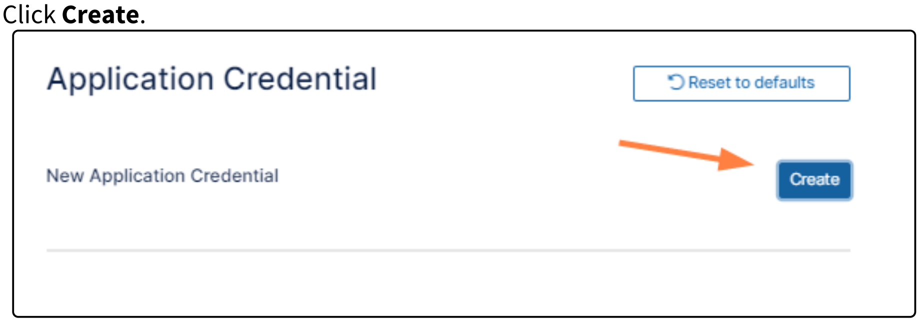
1. In the FileCloud admin portal, open the Application Credentials page.
   To go to the Application Credentials page:
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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



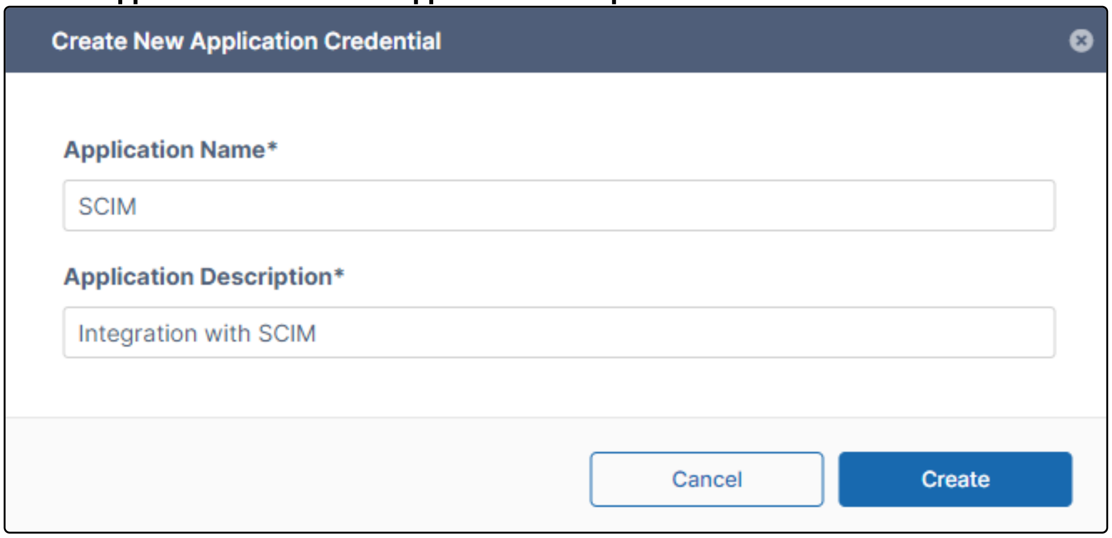
The Application Credentials page opens.

2. Click **Create**.

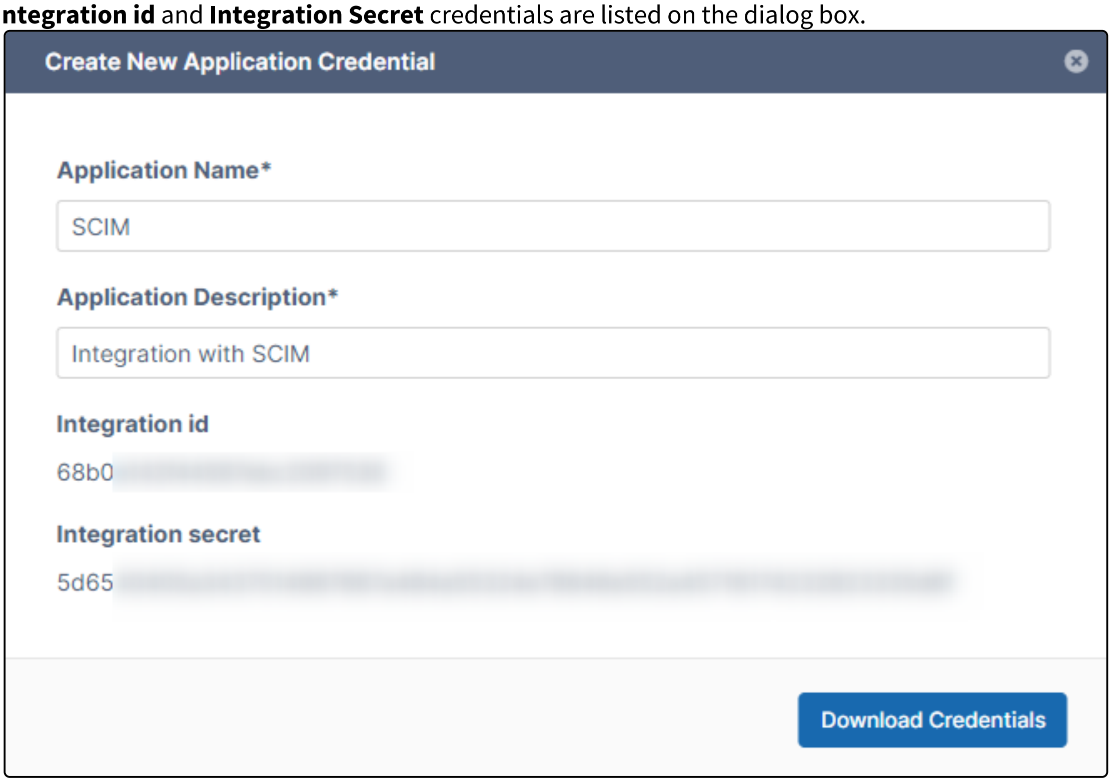


The **Create New Application Credential** dialog box opens.

3. Enter the **Application Name** and an **Application Description**.

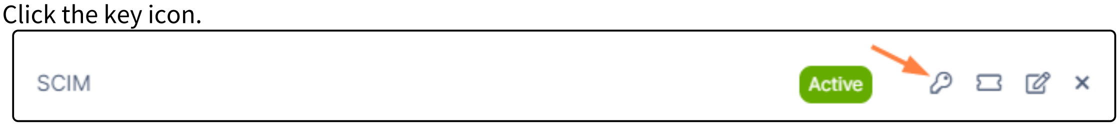


4. Click **Create**.
Integration id and **Integration Secret** credentials are listed on the dialog box.



The credentials will not be shown to you again, but you will be required to enter the **Integration secret** to create the token.

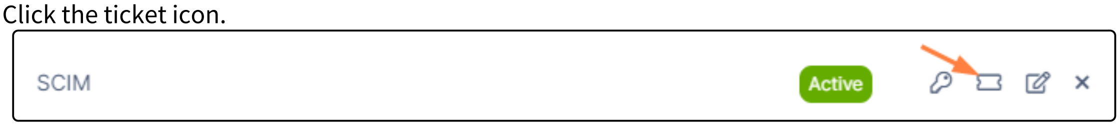
5. Click **Download Credentials** to save them in a file named **file credentials for [Application Name].txt**
The dialog box closes and the credential is now listed.
Click the key icon.



The **Manage Scopes** dialog box opens.

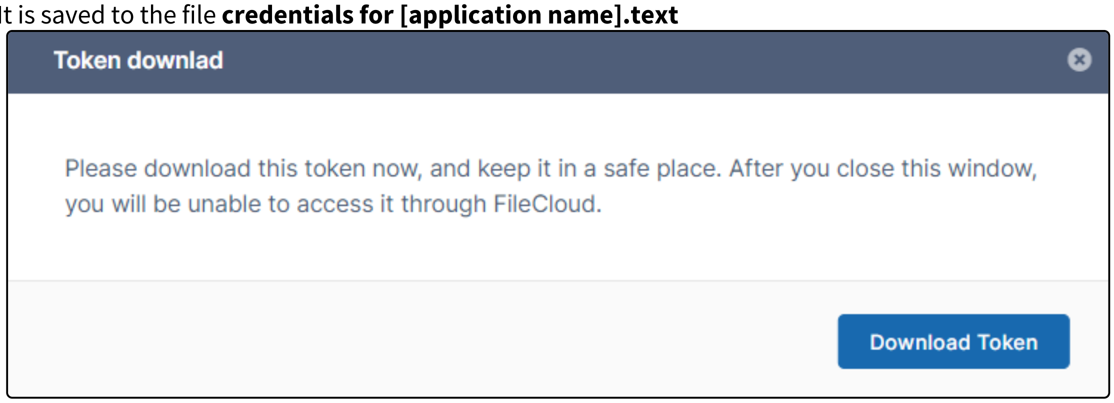
6. Enable **scim.read** to grant SCIM read permission to FileCloud's identity data, enable **scim.write** to grant SCIM create, update, and delete permissions to FileCloud's identity data, or enable both.

7. Click **Close**.
8. Click the ticket icon.

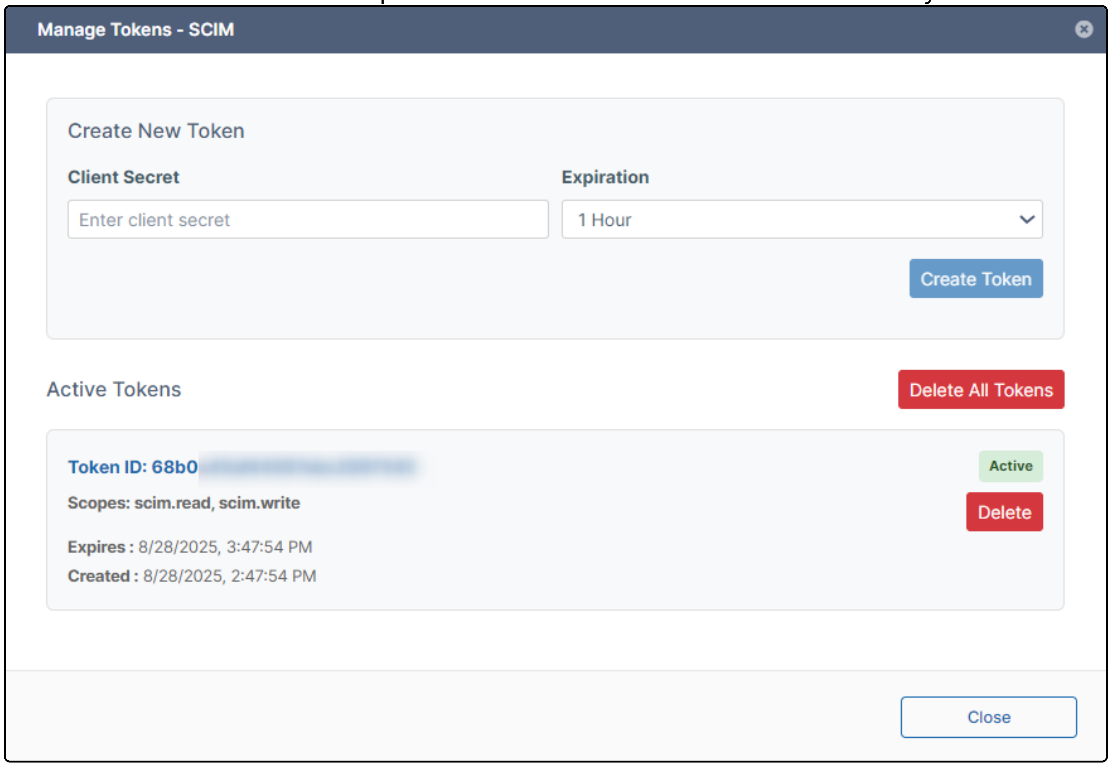


The **Manage Tokens** dialog box opens.

9. In **Client Secret** enter the **Integration secret** you saved above.
10. In **Expiration**, choose the interval that the token will remain usable. By default the interval is 1 hour.
11. Click **Create Token**.
You are prompted to save the token.
12. Click **Download Token**.
It is saved to the file **credentials for [application name].text**



The **Token ID** and its create and expire dates and times are shown. It is automatically made active.



13. Click **Close**.
    SCIM will now automatically update FileCloud with the connected apps' identity information.

Online Web Editing

Beginning in FileCloud 22.1, Office extensions .doc, .xls, and .ppt are no longer editable in Web Edit. In Desktop Edit, users may still edit .doc, .xls, and .ppt files.

If Web editing is enabled in your system, users can edit Office files, text files, markdown files (.md), HTML files, and log files without downloading them from FileCloud.

Users can edit supported Office file types in Office Online and edit the other file types listed above in FileCloud's built-in editors.

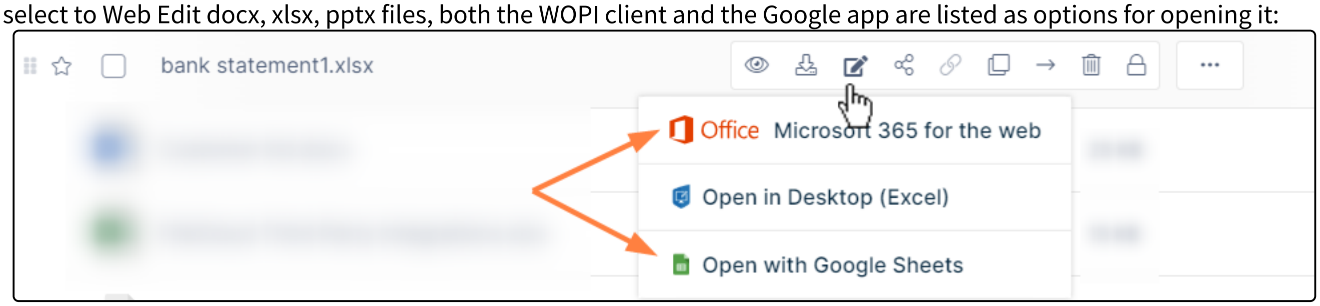
If Web editing is not available in your system, please Contact FileCloud Support.

To see how Web editing is done using Office Online, see Web Edit/Open in . . ..

- Web Editing with Google Apps
- New Document Creation via Web Browser
- Web Editing Text Files
- Web Editing Markdown and Readme Files
- Coauthoring Office Documents Using Web Edit
- Disable Online Web Editing

Web Editing with Google Apps

Beginning with FileCloud 21.3, you can integrate FileCloud with Google Apps to make an additional Web Edit option. Google Apps cannot replace your current WOPI client, but may be added as an additional option, so that when users select to Web Edit docx, xlsx, pptx files, both the WOPI client and the Google app are listed as options for opening it:



In FileCloud's mobile apps, files can be viewed but not edited in Google Apps.

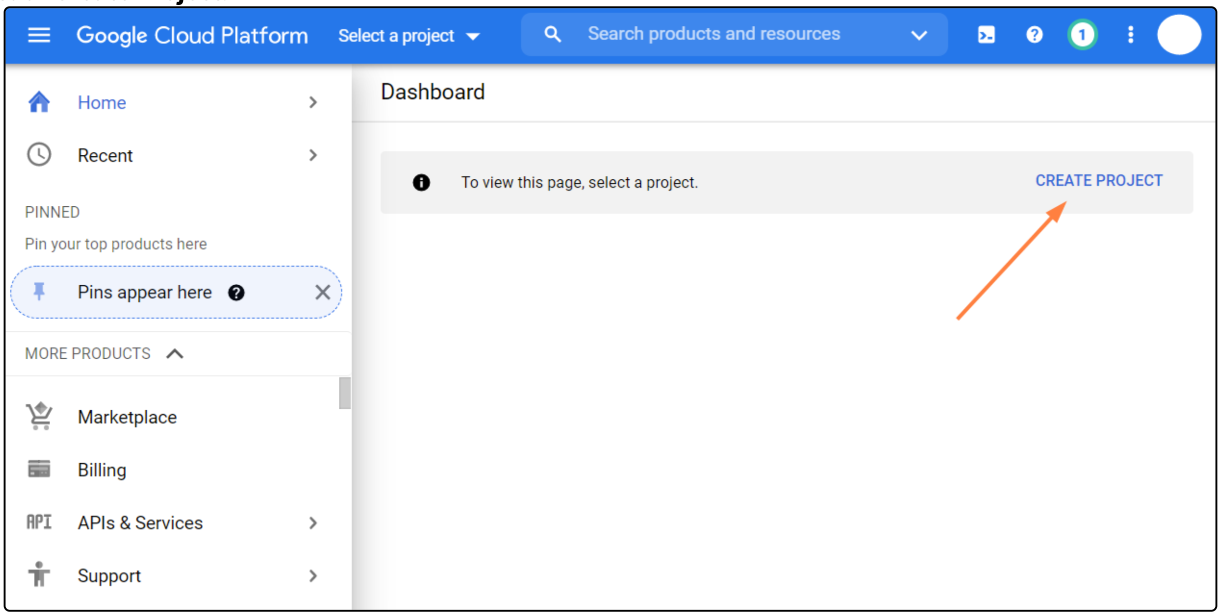
- Editing of some large files is not supported in Google Apps. See Files you can store in Google Drive for specific size limitations.
- To open a Google Apps editor in incognito windows, you may first have to grant Google Docs the correct permissions or unblock third party cookies.

To integrate with Google Apps:

Set up Google Apps - FileCloud integration in the Google Cloud platform:

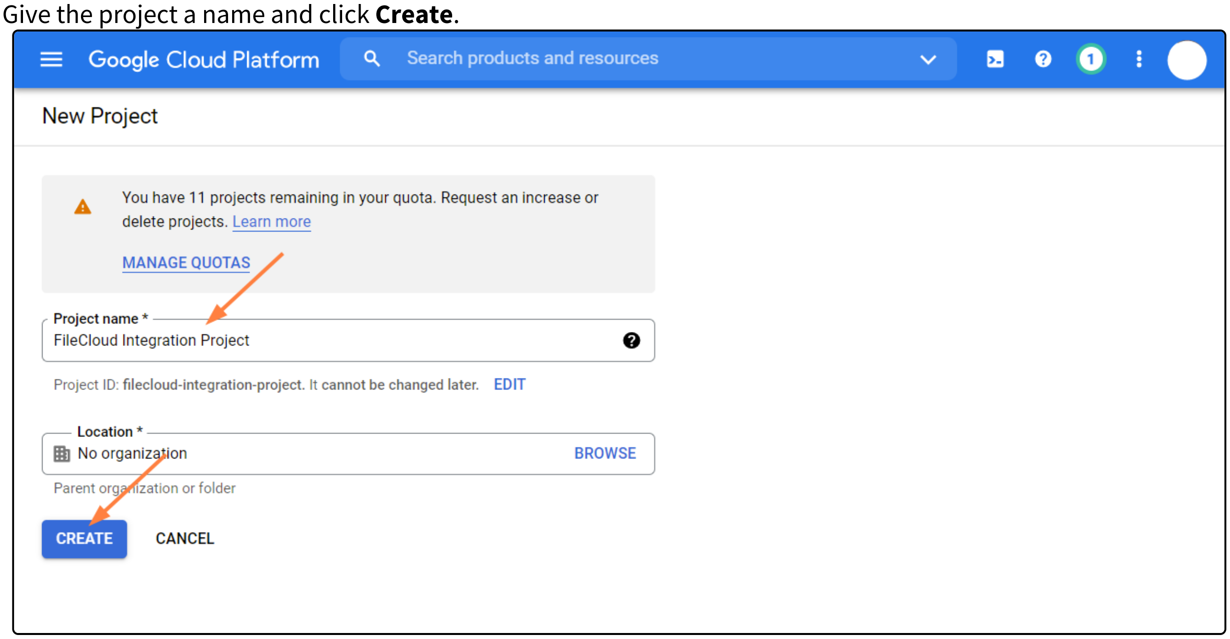
You must have a Google account that you can use to sign in to the Google Cloud Console in order to integrate your system with Google Apps.

1. Access the Google Cloud Console at https://console.cloud.google.com and sign in.
2. Go to **Home > Dashboard**.
3. Click **Create Project**.



A **New Project** screen opens.

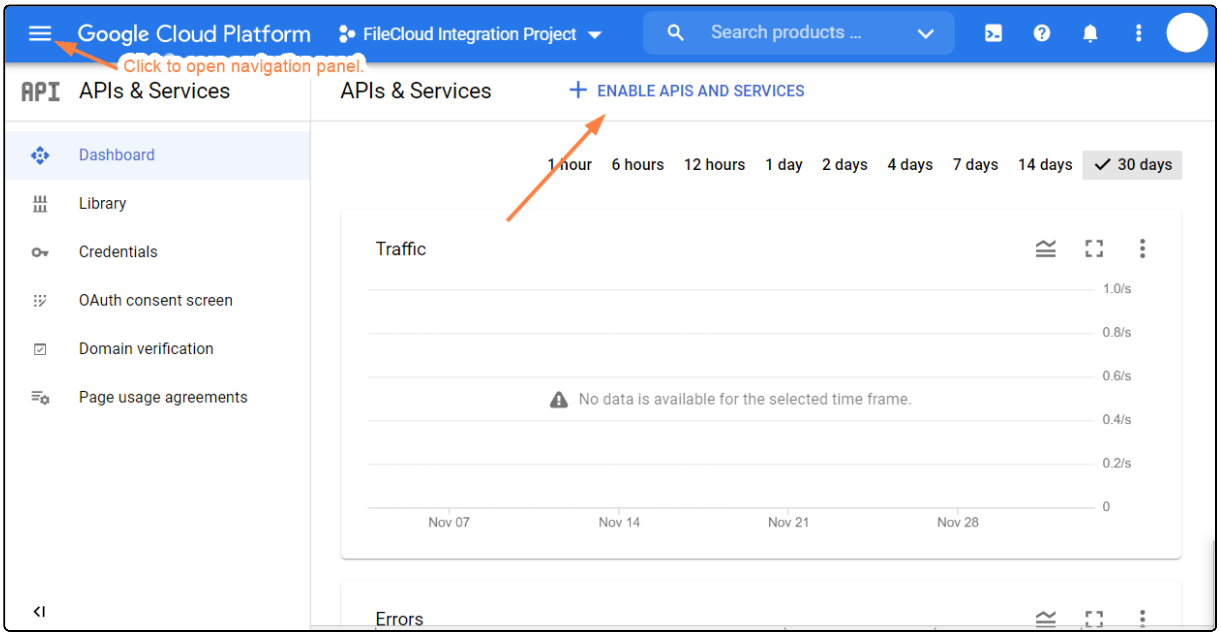
4. Give the project a name and click **Create**.



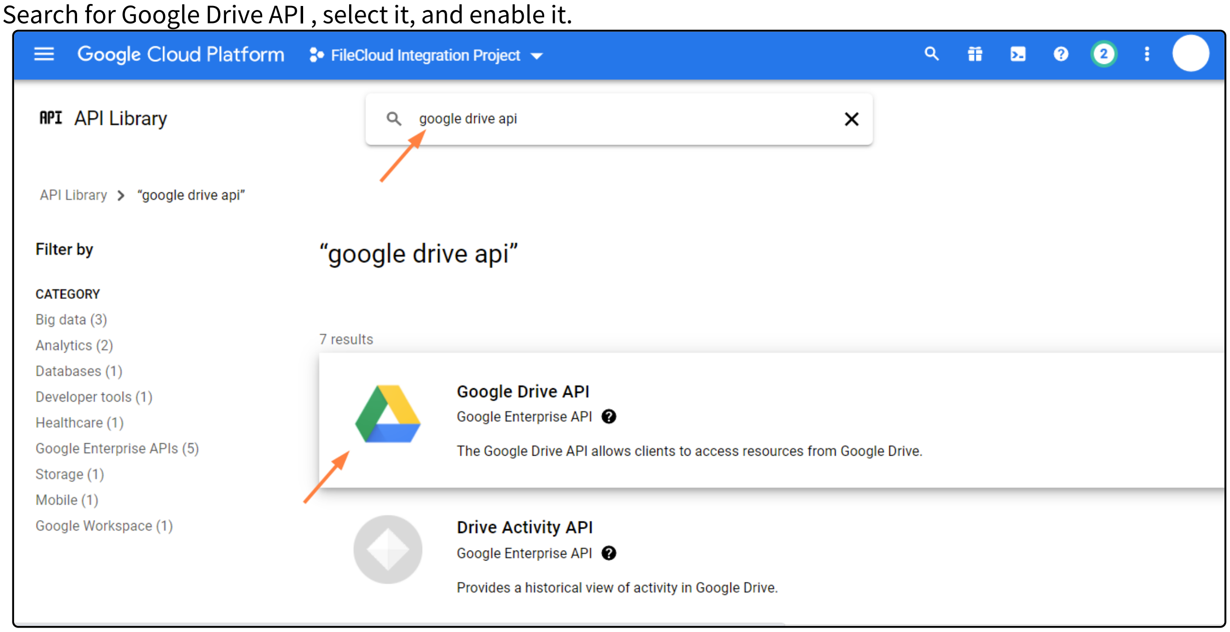
The project opens in the dashboard.

5. In the navigation panel, click **APIs & Services > Dashboard**.
(If the navigation panel is not visible, click the three bars in the upper-left corner of the screen to open it.)

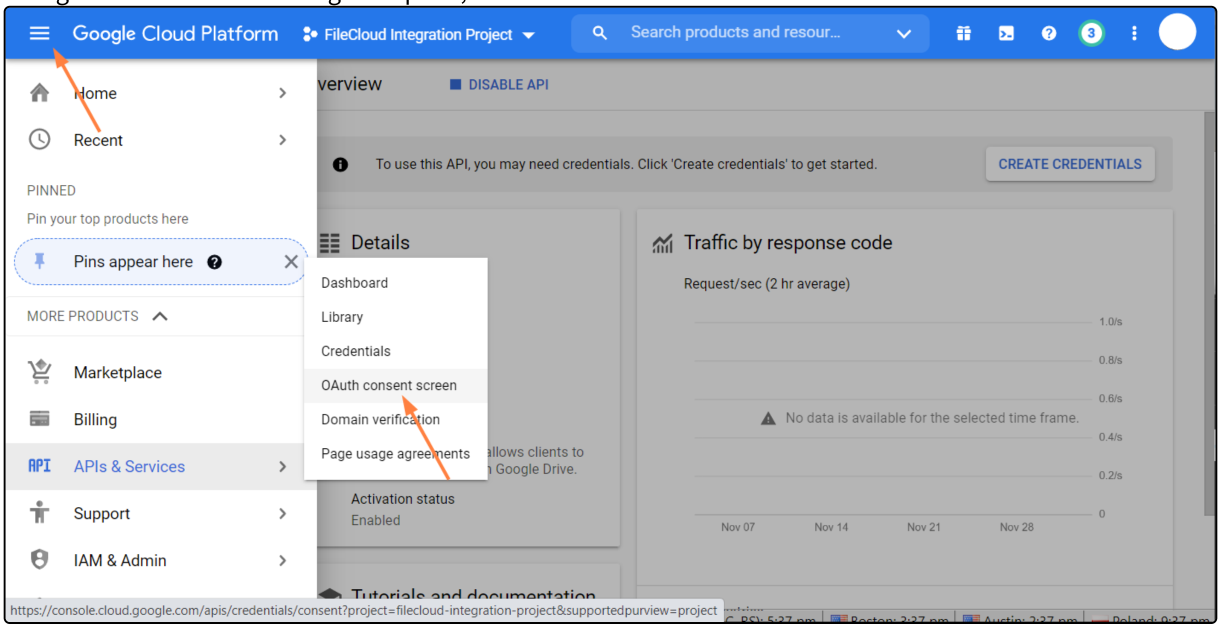
6. Click **Enable APIs and Services**.



7. Search for Google Drive API , select it, and enable it.

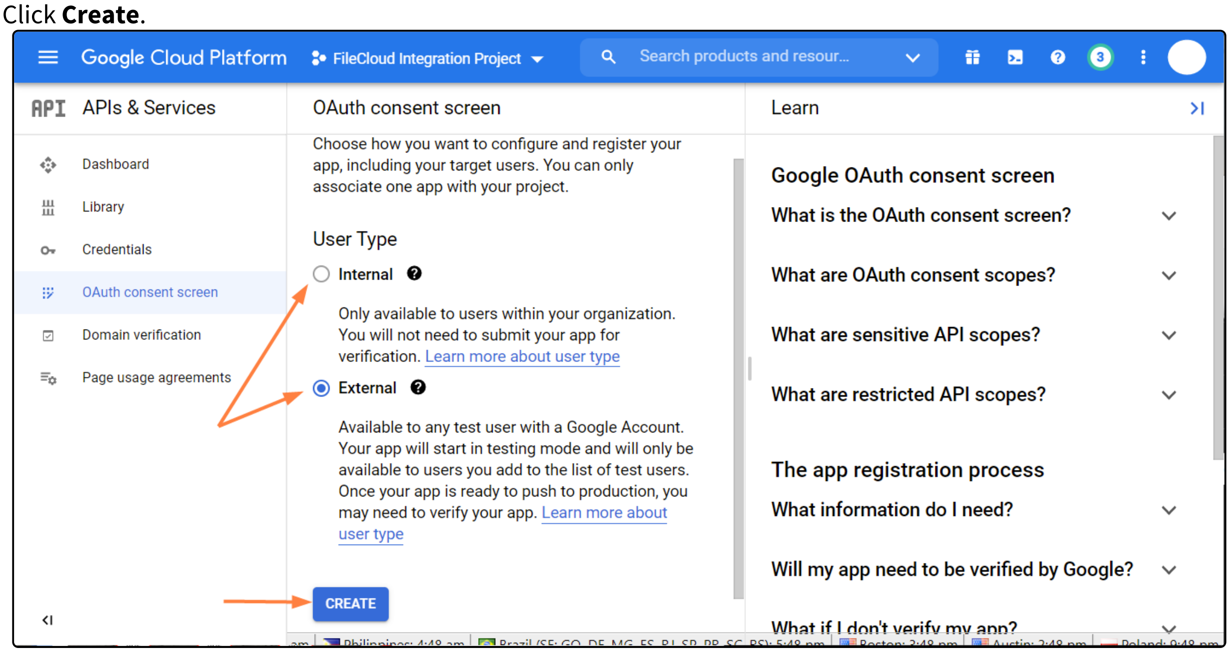


8. Then go back to the main navigation pane, and choose **APIs & Services > OAuth consent screen**.

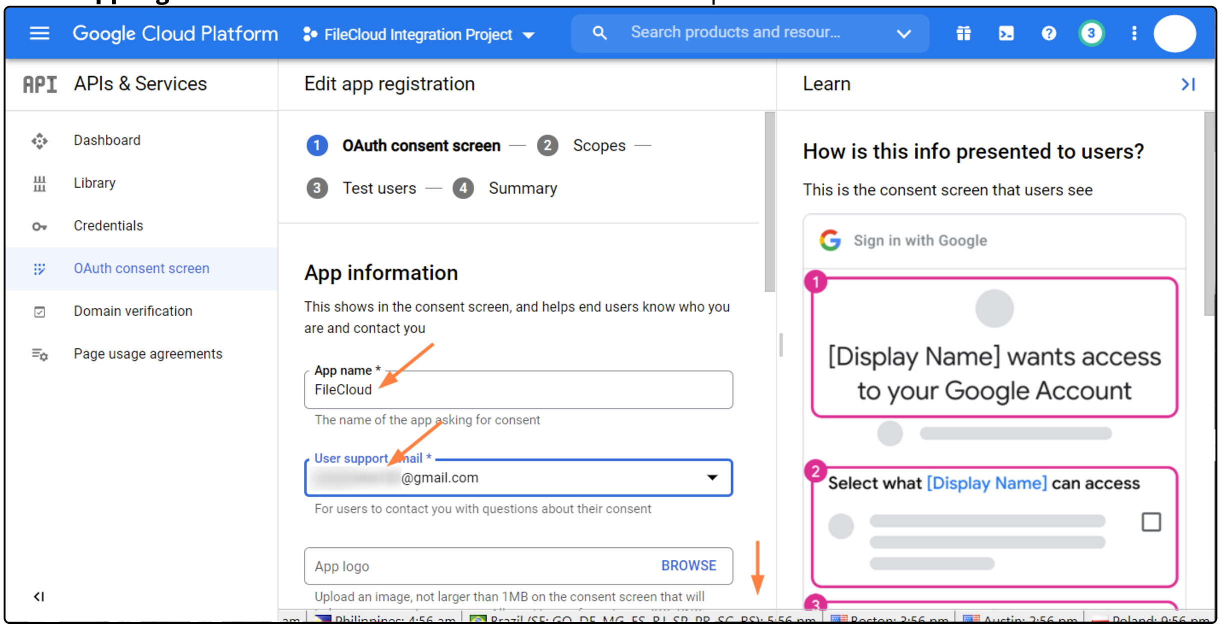


9. For **User Type**, choose **Internal** or **External** depending on the following guidelines:
   - **Internal** means the integration is limited to Google Workspace users within the organization (email domain). **External** allows any Google account.
   - Free google accounts only allow **External** users, because there is no Google Organization. Paid google accounts can use both, but **Internal** is only allowed if there's a Google Organization set up.
   - **External** requires the Google Project to be published into production status. It also may require the Google Project to be verified if it displays an icon or display name for the project on the OAuth consent screen.

10. Click **Create**.

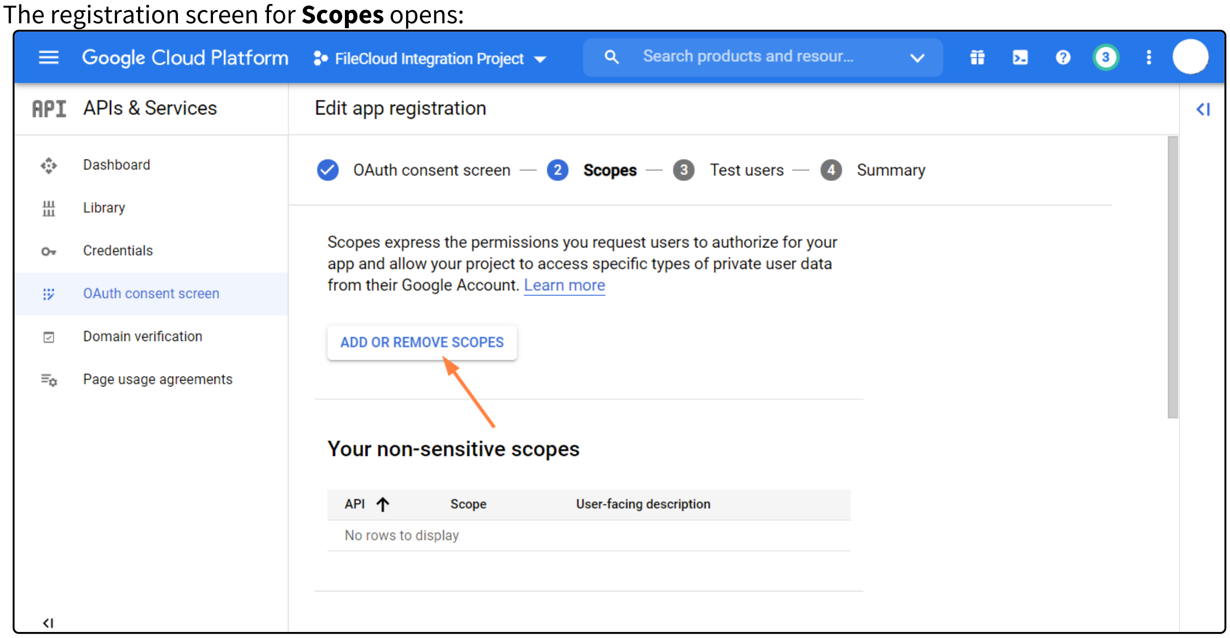


An **Edit app registration** screen for the **OAuth consent screen** opens.



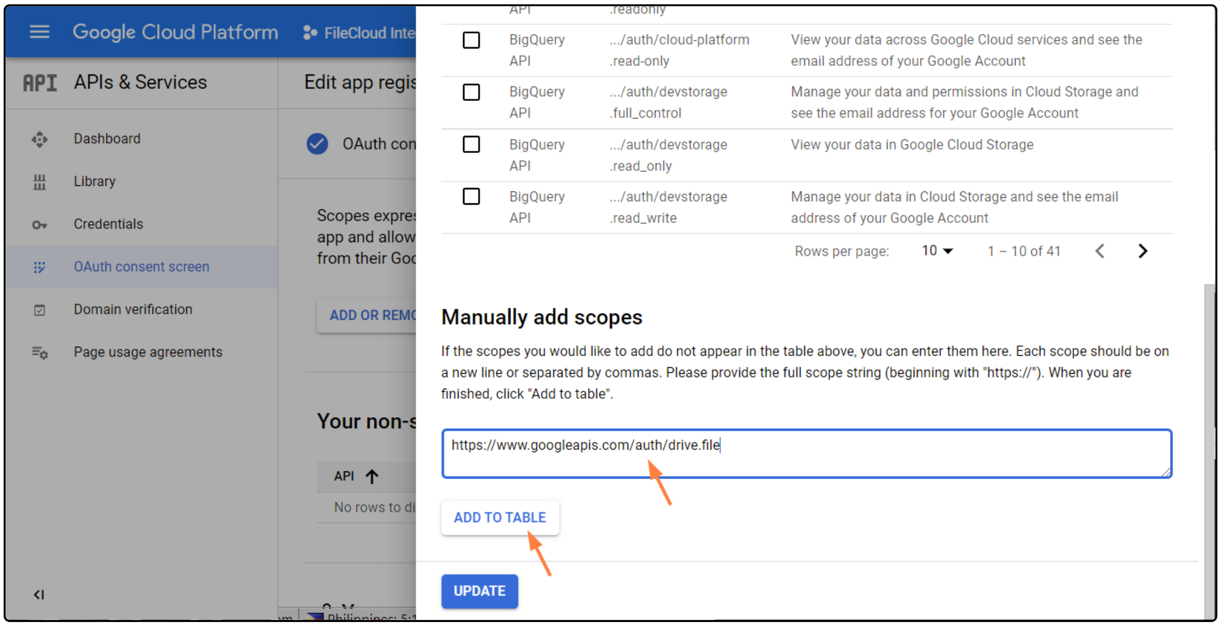
11. Fill in the required information, and then click **Save and Continue**.

The registration screen for **Scopes** opens:

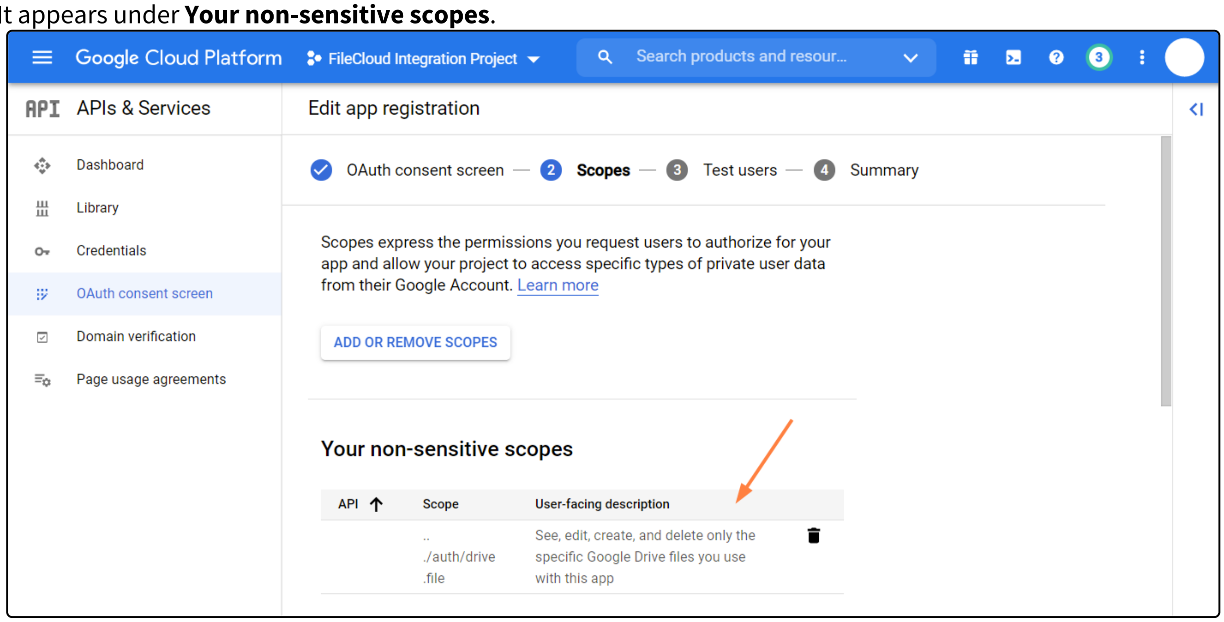


12. Click **Add or Remove Scopes**.
An **Update Selected Scopes** screen opens.

13. Scroll to the bottom of the screen and manually add https://www.googleapis.com/auth/drive.file. Then click **Add to Table**.

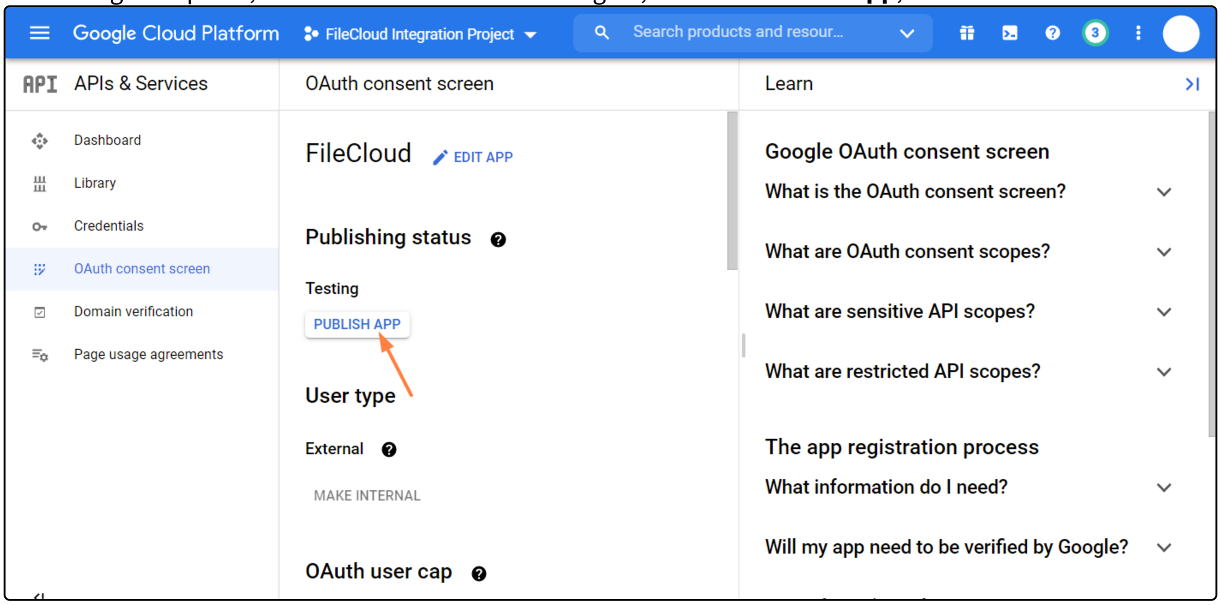


14. Check it in the table and click **Update**.
    It appears under **Your non-sensitive scopes**.

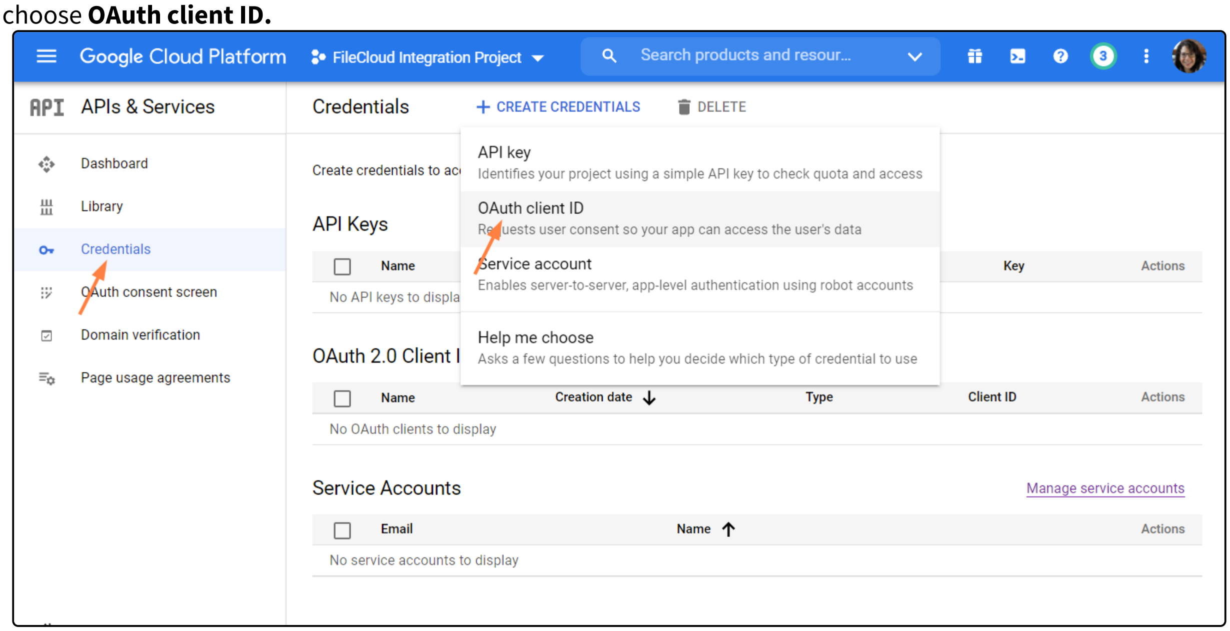


15. Scroll to the bottom of the screen and click **Save and Continue**.
16. In the **Test Users** screen, click **Save and Continue**.

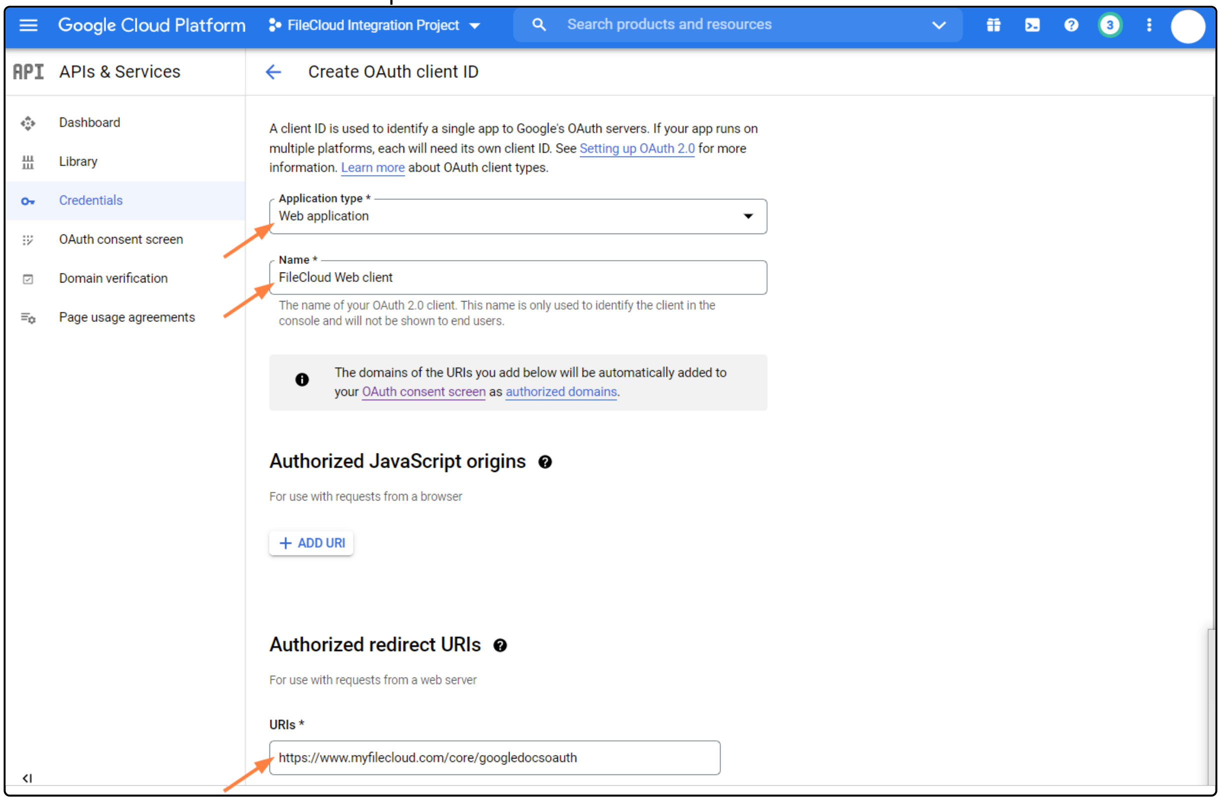
17. In the navigation panel, click **OAuth consent screen** again, and click **Publish App**, and then click **confirm**.



18. In the navigation panel, click **Credentials**, and in the **Credentials** screen, click **Create Credentials**, and choose **OAuth client ID.**

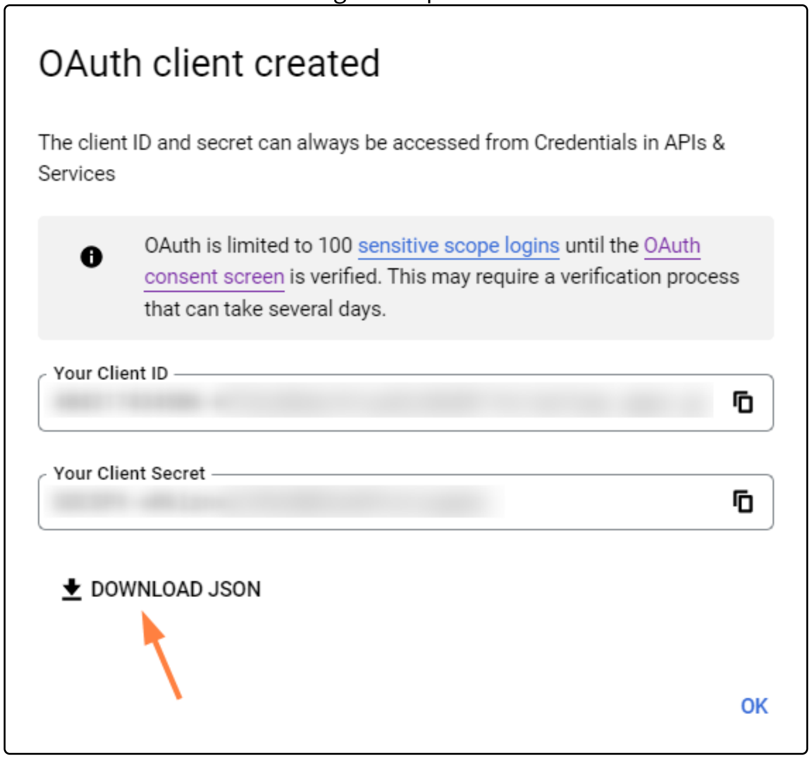


The Create OAuth Client ID screen opens.



19. In **Application type,** select **Web application**.
    In **Name**, enter any name.
    In **URIs** under **Authorized redirect URIs** enter your FileCloud URL appended with **/core/googledocsoauth**, for example, **https://www.myfilecloud.com/core/googledocsoauth**.

20. Click **Create**.
An OAuth client created message box opens:

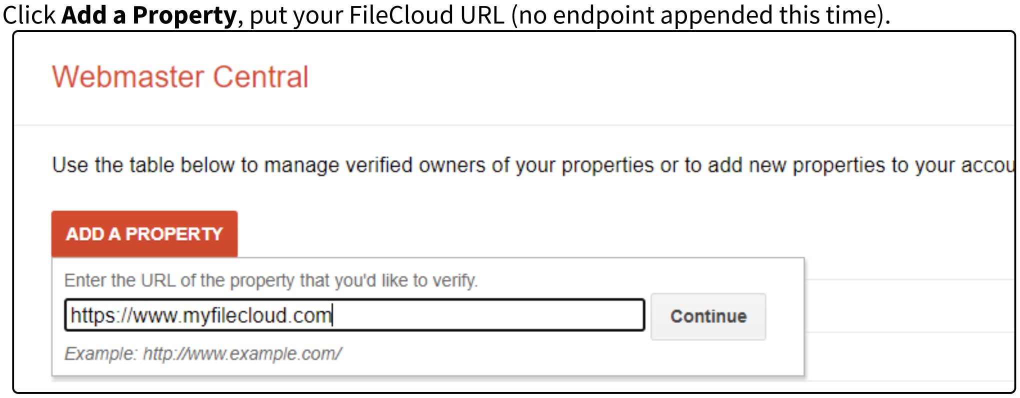


21. Click **Download JSON**, and download and save the JSON file.

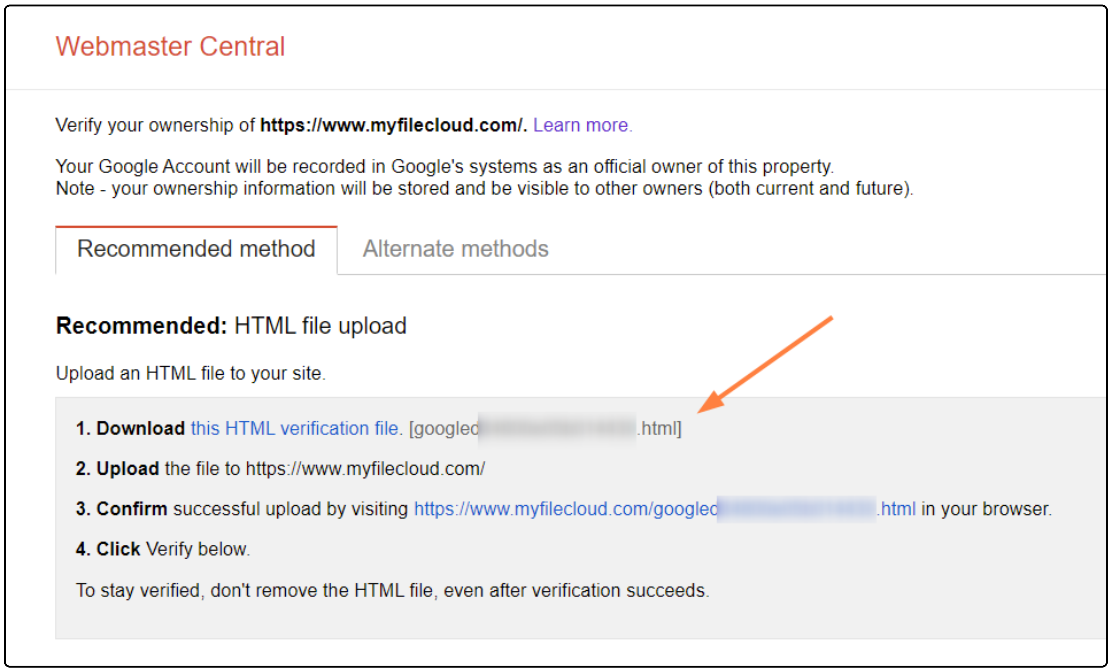
Configure Google Apps in FileCloud

Now we need set up Google Apps in FileCloud by adding the OAuth file and the HTML verification file.

1. Go to https://www.google.com/webmasters/verification/home
2. Click **Add a Property**, put your FileCloud URL (no endpoint appended this time).



3. Click **Continue**.



4. Download the HTML verification file.
5. Now open the FileCloud Admin UI and go to **Settings > Web Edit**, and scroll down to **Google Apps Access**.
    a. Check **Enable Google Apps**.
    b. For **Google OAuth Client ID**, click **Choose File** to select the JSON file you downloaded and saved in the previous procedure, and then click **Upload** to upload it.

c. For **Google's Domain Verification File**, click **Choose File** to select the HTML file that you just downloaded.

6. Now go back to the https://www.google.com/webmasters/verification page where you have just downloaded the HTML file.
   a. Confirm you are not a robot.
   b. Click **Verify**.

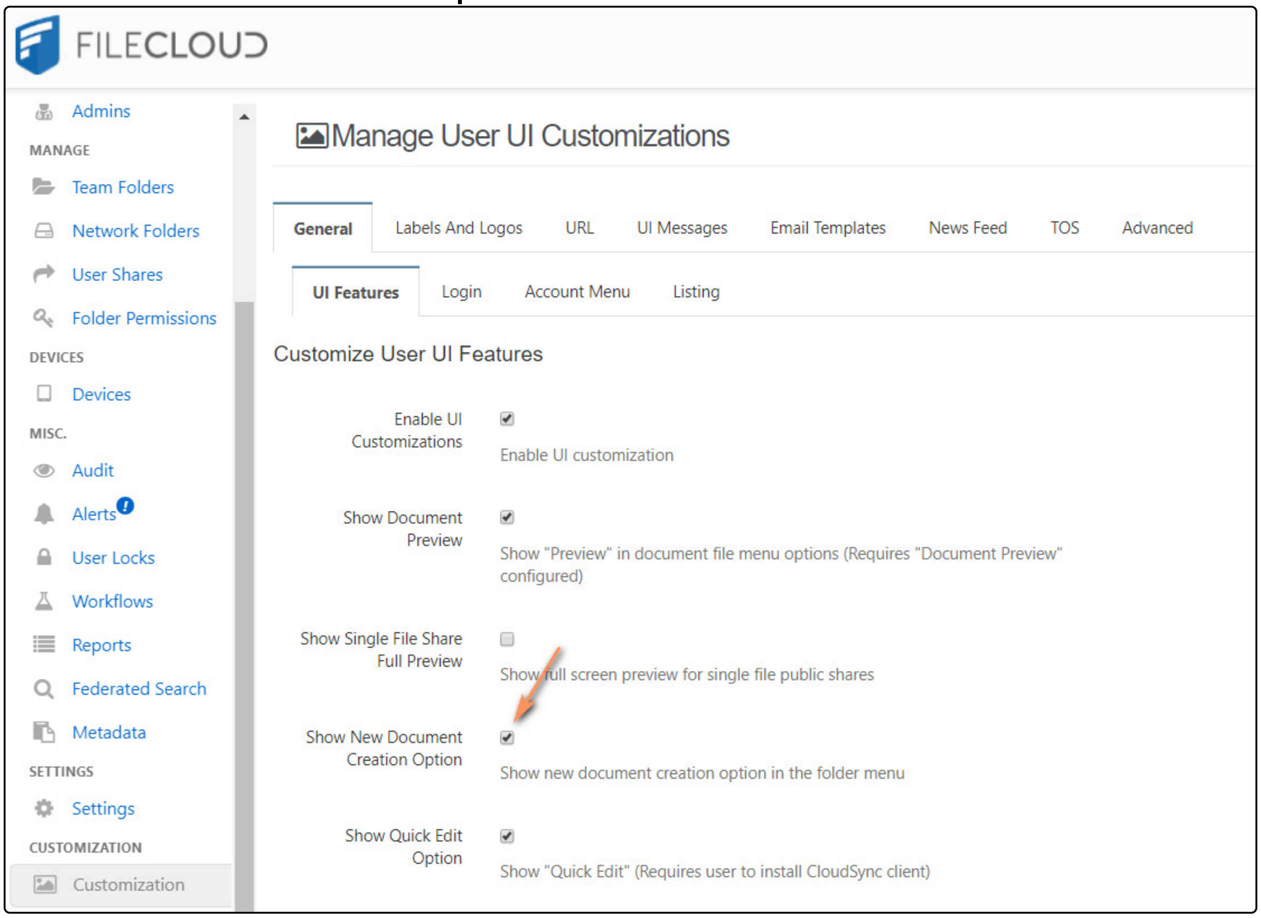
Your users can now view and use the **Open in Google [app]** option for docx, xlsx, and pptx files.

New Document Creation via Web Browser

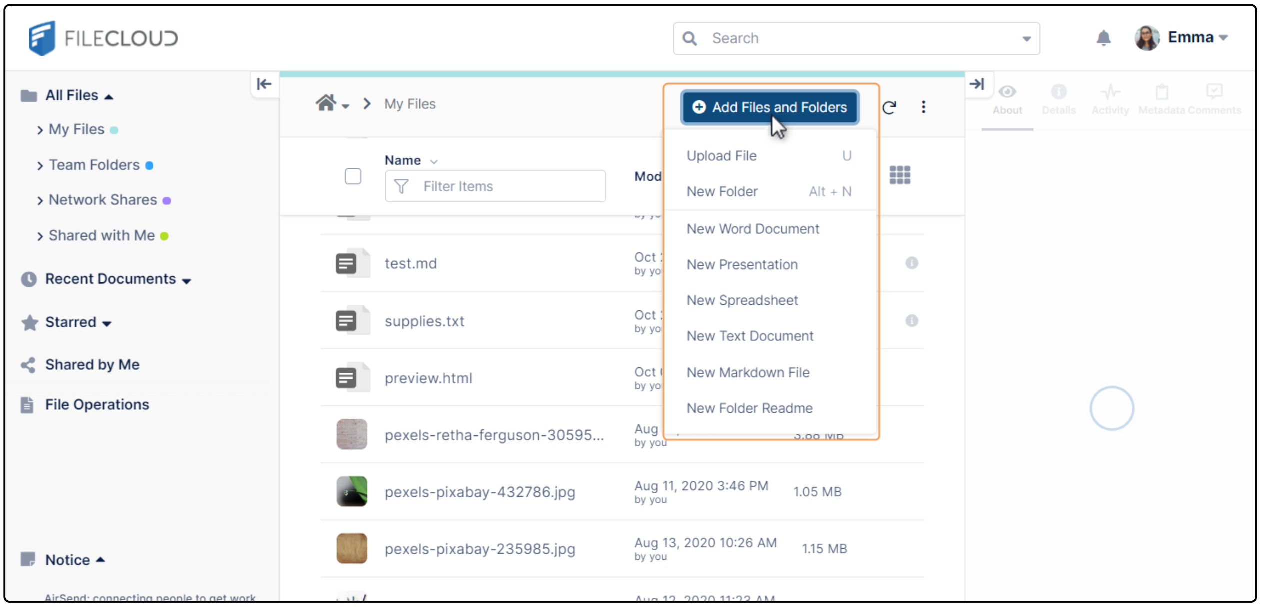
Once online editing is configured by the administrator, FileCloud users can log in to their portal and create new documents and edit them from within the web browser.

To enable new document creation

1. Enable **Show New Document Creation Option** in **Customization > General >UI Features**.

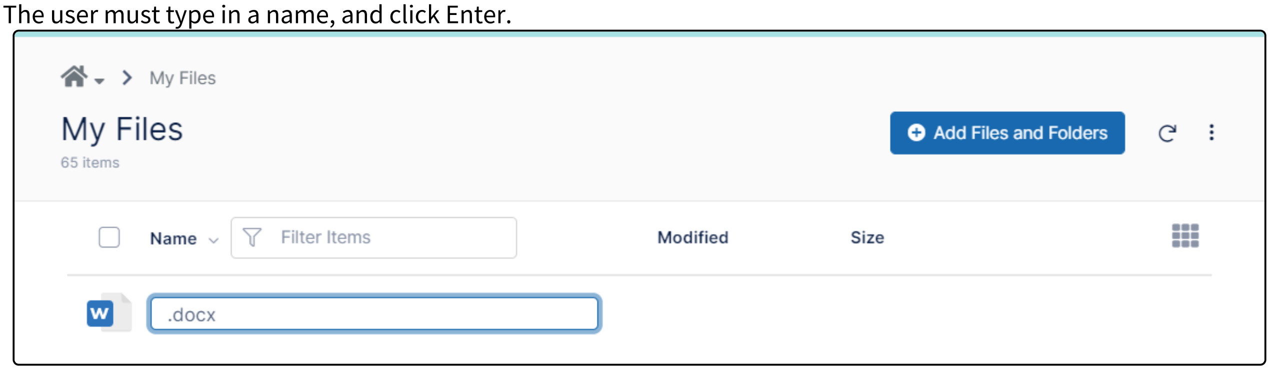


2. Now, in the user portal, users can click **Add Files and Folders** above the list of files. A drop-down list with options for creating new files or a new folder appears.



If the user chooses to create a file, the file appears at the top of the list of files and folders. The extension is already entered.

3. The user must type in a name, and click Enter.



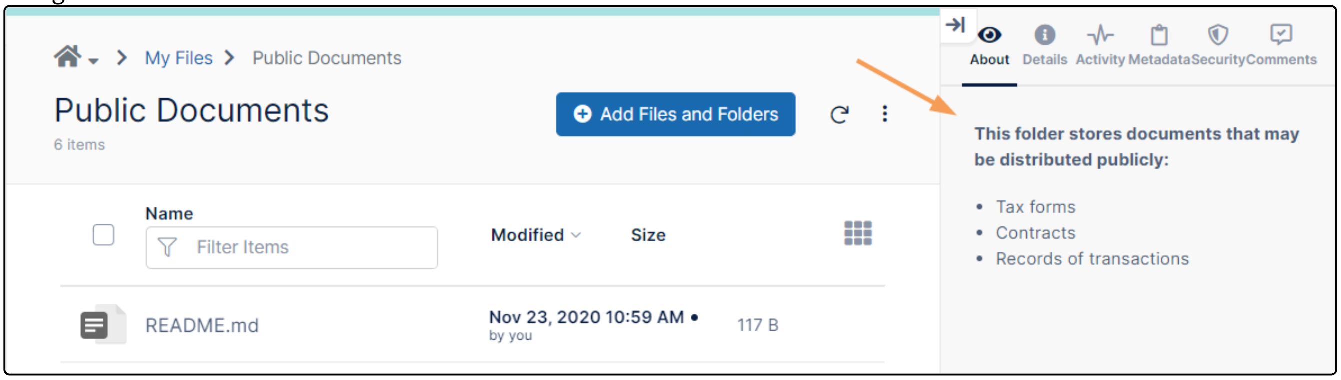
The document opens for edit.

Readme files

There can only be one readme file in a folder, and it is always named readme.md.

After a user creates the readme file, when they click **Add Files and Folders** and choose **New Folder Readme**, the existing readme is opened for edit.

When a user selects a folder that includes a readme file, the contents of the readme are displayed in the **About** panel to the right of the screen.



Web Editing Text Files

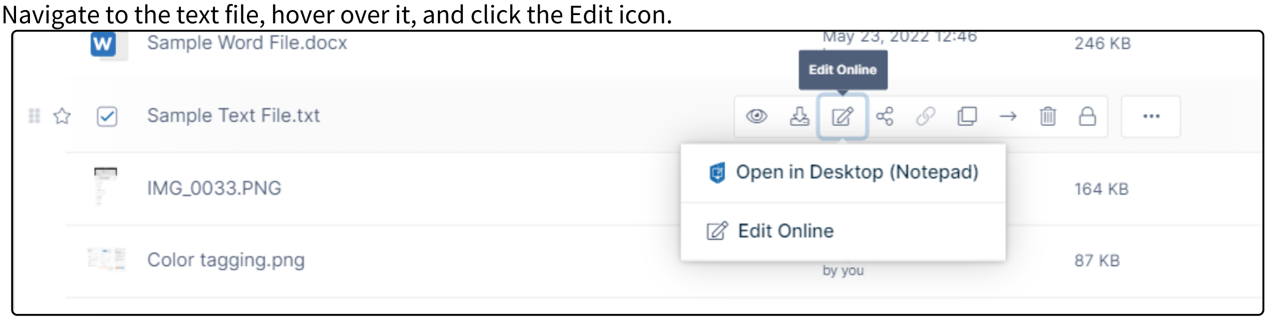
FileCloud supports editing text files from within a browser session. This support is enabled regardless of WOPI configuration, as editing of text files uses a built-in widget.

To create a new text file, see New Document Creation via Web Browser

Editing text files

To edit a text file:

1. Navigate to the text file, hover over it, and click the Edit icon.



2. Choose the edit option (there may be one or more).
   The file opens in the text editor you have chosen..
3. Edit and save the file.
   Note: You can also add and read comments about the file in the right panel.

Web Editing Markdown and Readme Files

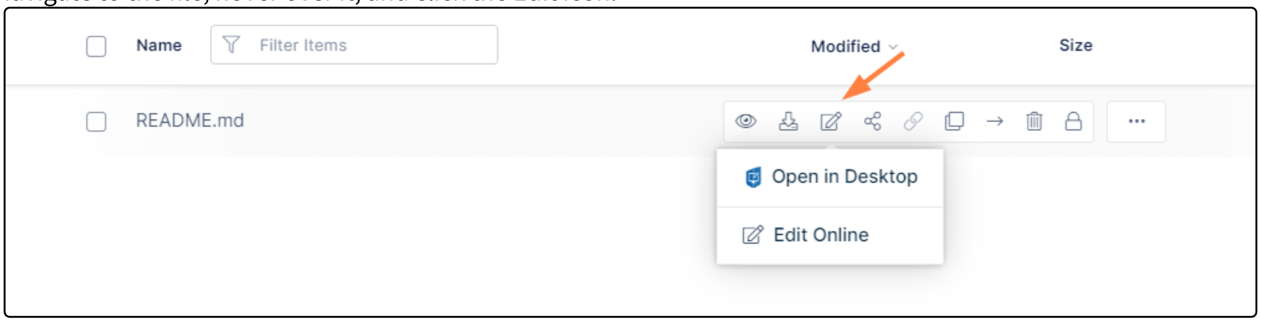
Starting with version 20.2, FileCloud supports editing markdown files from within a browser session. It also supports editing readme files, which are a form of markdown files and use the same types of editors.

To create a new markdown or readme file, see New Document Creation via Web Browser

Editing markdown and readme files

To edit a markdown or readme file:

1. Navigate to the file, hover over it, and click the Edit icon.



2. Choose the edit option (there may be one or more).
   The file opens in the text editor you have chosen..

> There can only be one readme file in a folder, and it is always named **readme.md**. After you create the file, it is displayed in the **About** section to the right of the page when you select the folder.

Coauthoring Office Documents Using Web Edit

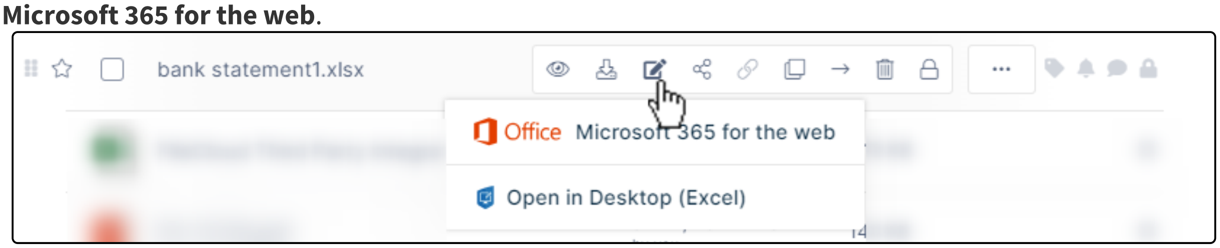
FileCloud supports coauthoring of Office document files from within a browser session.

Introduction

Coauthoring occurs when two users are editing the same document and can view each other's changes as they make them.

Only .docx, .xslx, and .pptx documents can be coauthored.

To open an Office file in web edit, hover over the file and click the **Web Edit** icon. In the drop-down list, choose **Microsoft 365 for the web**.



Coauthoring Flow

The following steps demonstrate the flow of coauthoring.

1. User A wants to coauthor a document with user B.
2. User A shares the folder containing the document to user B. The share should have view, download and upload permissions to user B.

3. User A opens the file in web edit.
4. User B opens the same file that was received via sharing in web edit.
5. Now both users can edit the document and they can see each other editing the file.
6. The web edit service will handle the coordination and will ensure saving both user changes.

Disable Online Web Editing

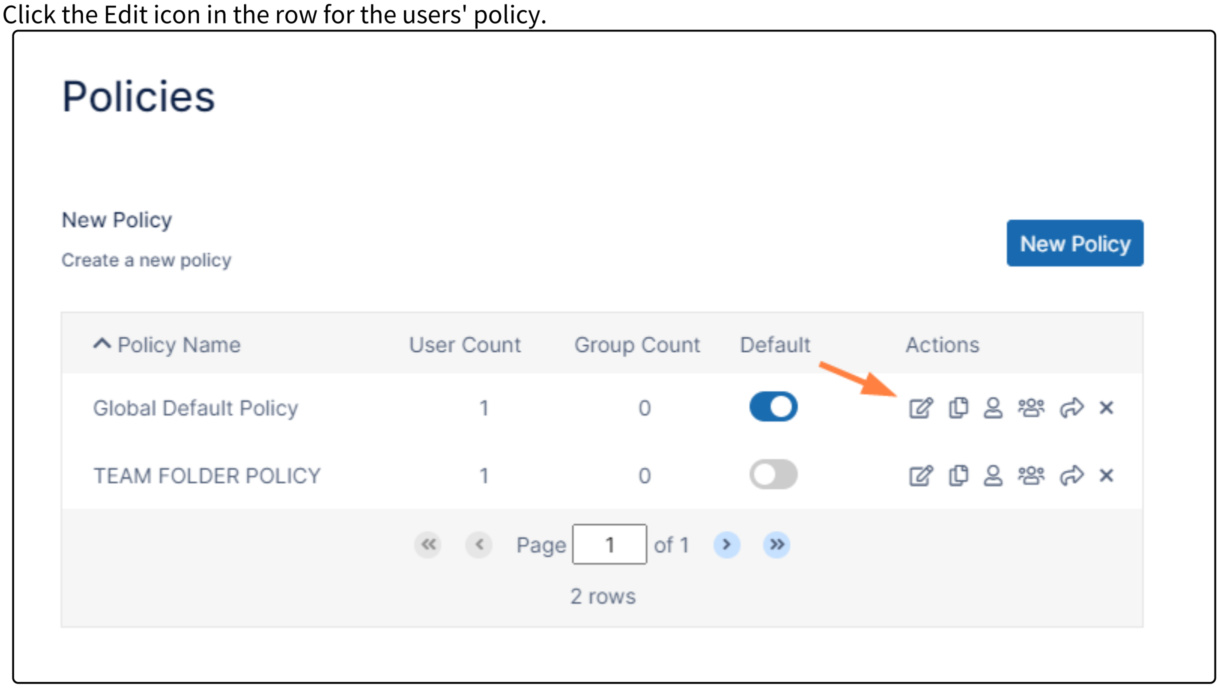
You can decide not to allow your users to edit documents in a browser.

After you configure online editing, FileCloud users can log in to the user portal, select any supported document and click a Web Edit button to edit the document from within the web browser. All the changes made by the user are saved in FileCloud automatically.

If you do not want to support this feature for certain users, the Web Edit button can be removed from the user portal through the users' policies.

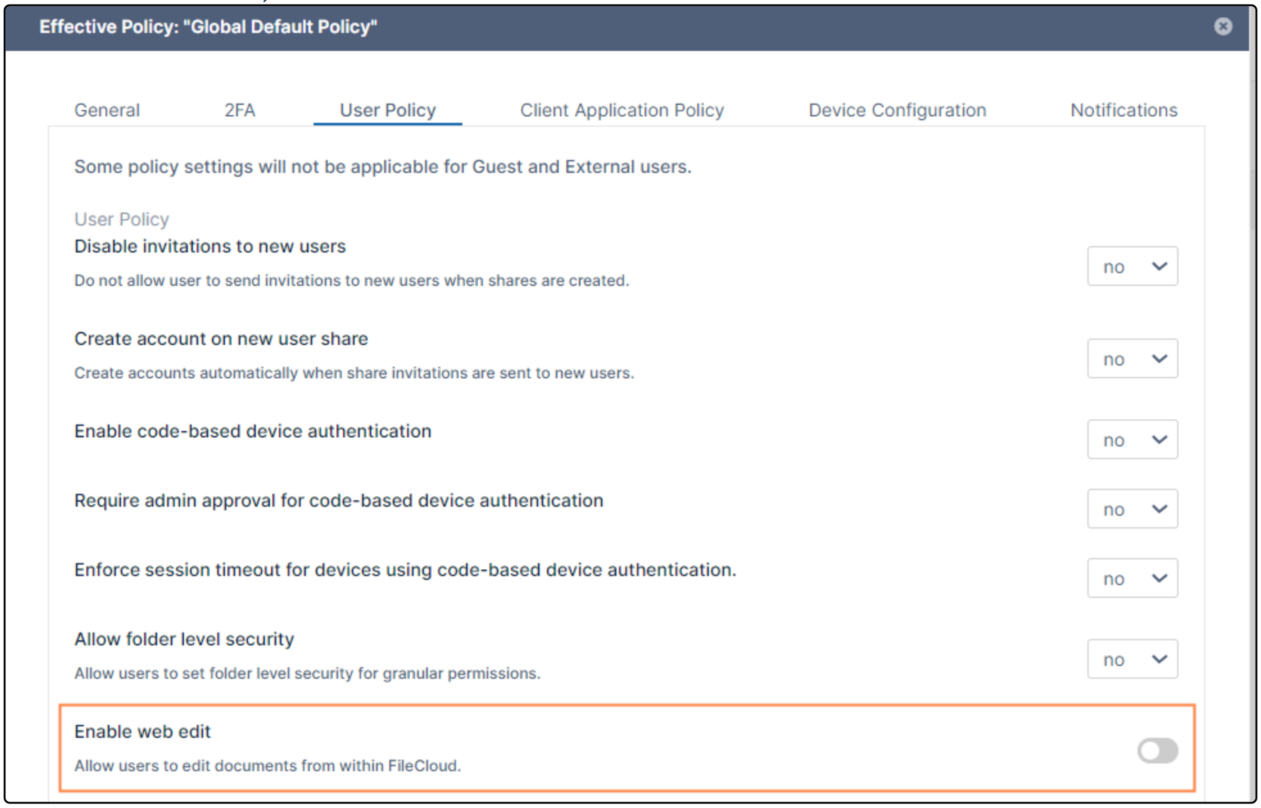
To hide the Web Edit button for the users associated with a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** settings page opens.
2. Click the Edit icon in the row for the users' policy.



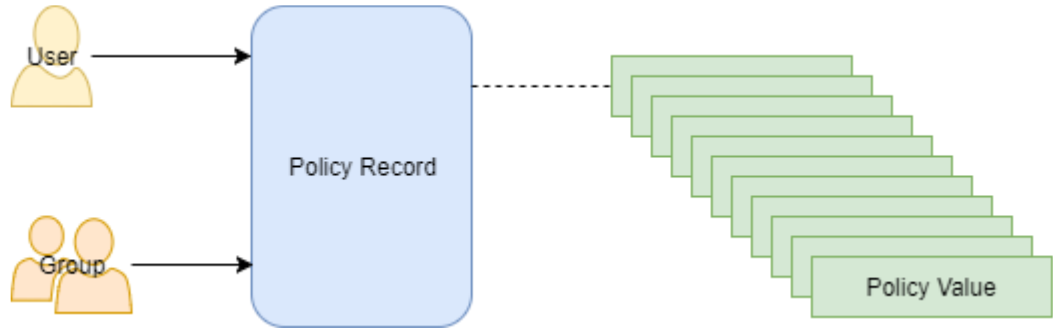
   The **Policy Settings** dialog box opens.
3. Click the **User Policy** tab.

4. Locate **Enable web edit**, and disable it.



5. Click **Save**.

Policies



You can manage users and groups easily using policies.

- Policies enable you to manage settings at the user or group level
- One policy record manages multiple policy settings
- The policy record can be associated with a user or group

To manage FileCloud policies, click **Settings** in the navigation pane, and then, on the **Settings** navigation page, click **Policies**  .

The policy values in Table 1 are managed in a policy record.

Table 1. Policy Values

General		
Share Mode	All (public and private)	
Default share expiry in days	0	
Default max number of downloads allowed	0	
User storage quota	2GB	
Enable Privacy Settings	NO	
Store deleted files in the recycle bin	NO	
Automatically delete files from recycle bin after set number days	0	
Do not store deleted files greater than	100 MB	
2FA		
Require two factor authentication	NO	
Two Factor Authentication Mechanism	Email	
User Policy		
Disable invitations to new users	NO	
Create account on new user share	NO	
Enable code-based device authentication	NO	

Require admin approval for code-based device authentication	NO (Only enabled if **Enabled Code Based Client Authentication** is set to YES.)	
Enforce session timeout for devices using code-based device authentication.	NO (Only enabled if **Enabled Code Based Client Authentication** is set to YES.)	
Allow folder level security	YES	
Enable web edit	YES	
Enable recycle bin clearing	YES	
Disallow default share settings change	NO	
Disable Send File For Approval	NO	
Disable Everyone group sharing	NO	
Allow group creation	NO	FileCloud 21.2
Allow group management (add and remove users)	NO	FileCloud 21.2
Allow group deletion	NO	FileCloud 21.2
Allow workflow automation sharing	NO	FileCloud 23.251
Disable workflow automation	NO	FileCloud 21.2
Require share approval workflow	NO	FileCloud 21.2
Selected Workflow (only appears if Require Share Approval Workflow is set to YES)	Select a Workflow	FileCloud 21.2
eSignature	YES	FileCloud 23.241.4

Max. file upload size	0	FileCloud 22.1
Save zip file session password	YES	FileCloud 22.1
Client Application Policy	**Default Value**	**Version Available**
Require passcode lock for mobile clients	NO	
Disable all mobile client apps from connecting	NO	
Disable 'Edit' functions in mobile client apps	NO	
Disable 'Print' option in mobile client apps	NO	
Disable 'Download' option in mobile client apps	NO	
Disable 'Open with' option in mobile client apps	NO	
Disable 'Share' options in mobile client apps	NO	
Disable 'Add to favorites' option in mobile client apps	NO	
Notifications		
Disable Notifications	NO	
Disable User Override	NO	
Disable Add notifications	NO	
Disable update notifications	NO	
Disable delete notifications	NO	
Disable Download notifications	NO	
Disable Preview notifications	NO	
Disable Lock/Unlock notifications	NO	

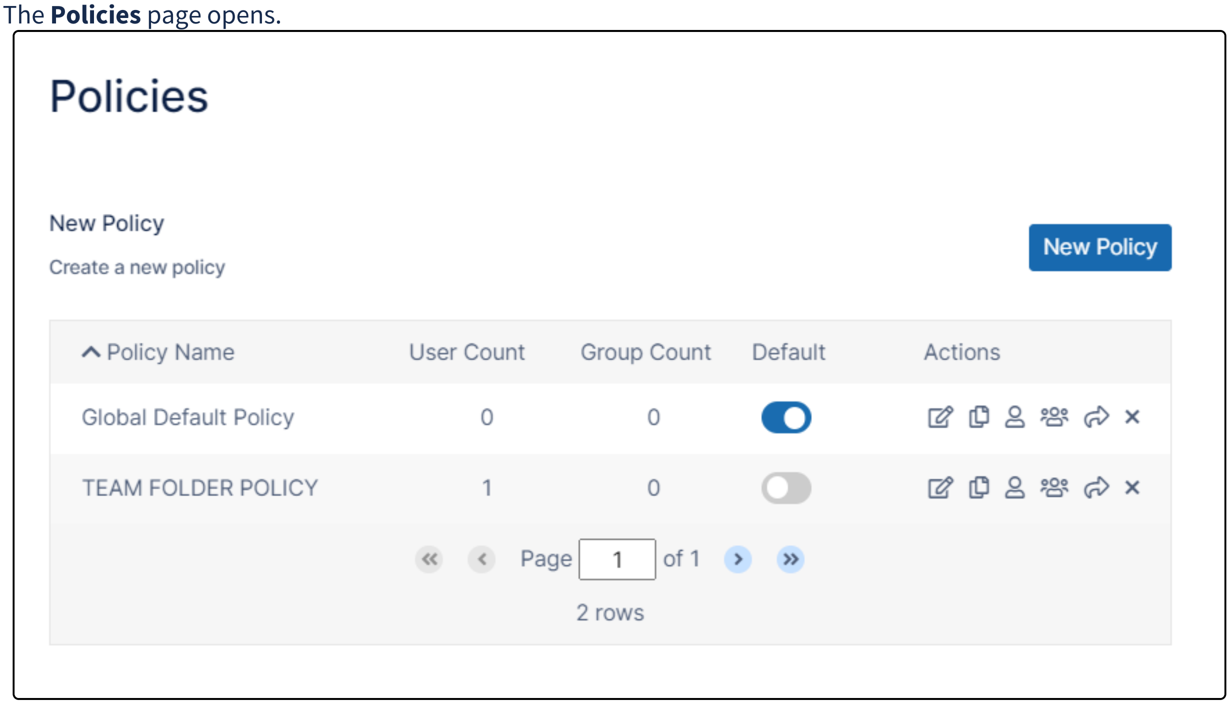
Disable Share notifications	NO	
Disable Rename notifications	NO	
Disable self notifications	NO	

Working with Policy Records

Accessing Policy Records

To access a policy record:

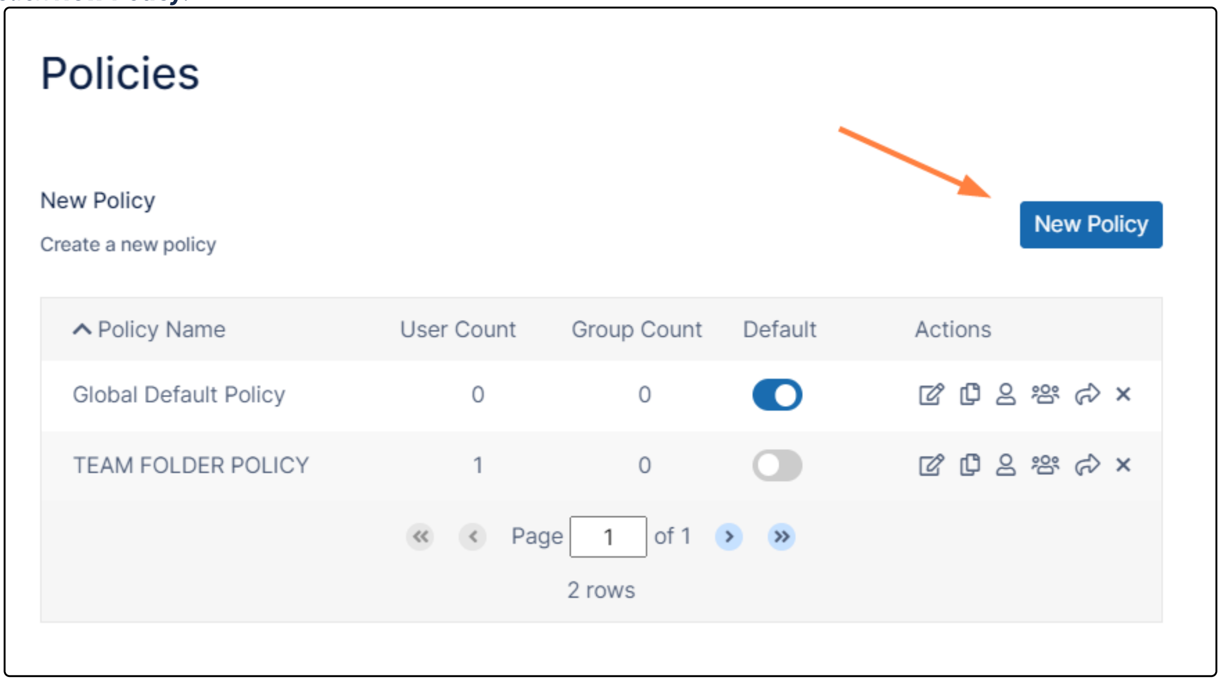
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
The **Policies** page opens.



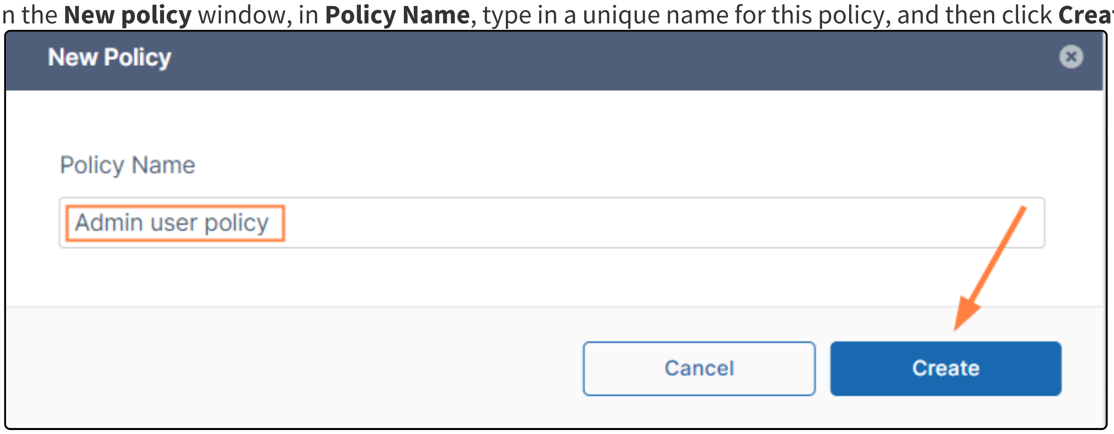
Creating a New policy Record

To create a policy:

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

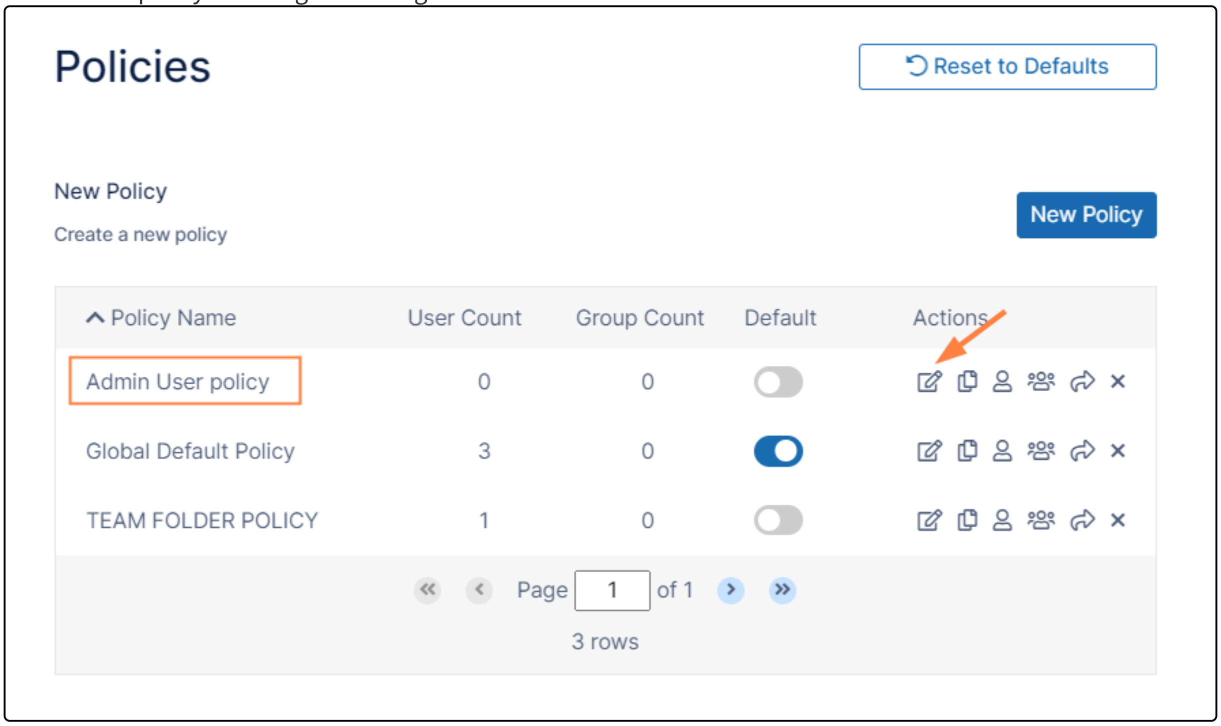


3. In the **New policy** window, in **Policy Name**, type in a unique name for this policy, and then click **Create**.



The policy is created and appears in the **Policies** list.

4. Edit the new policy to configure settings.

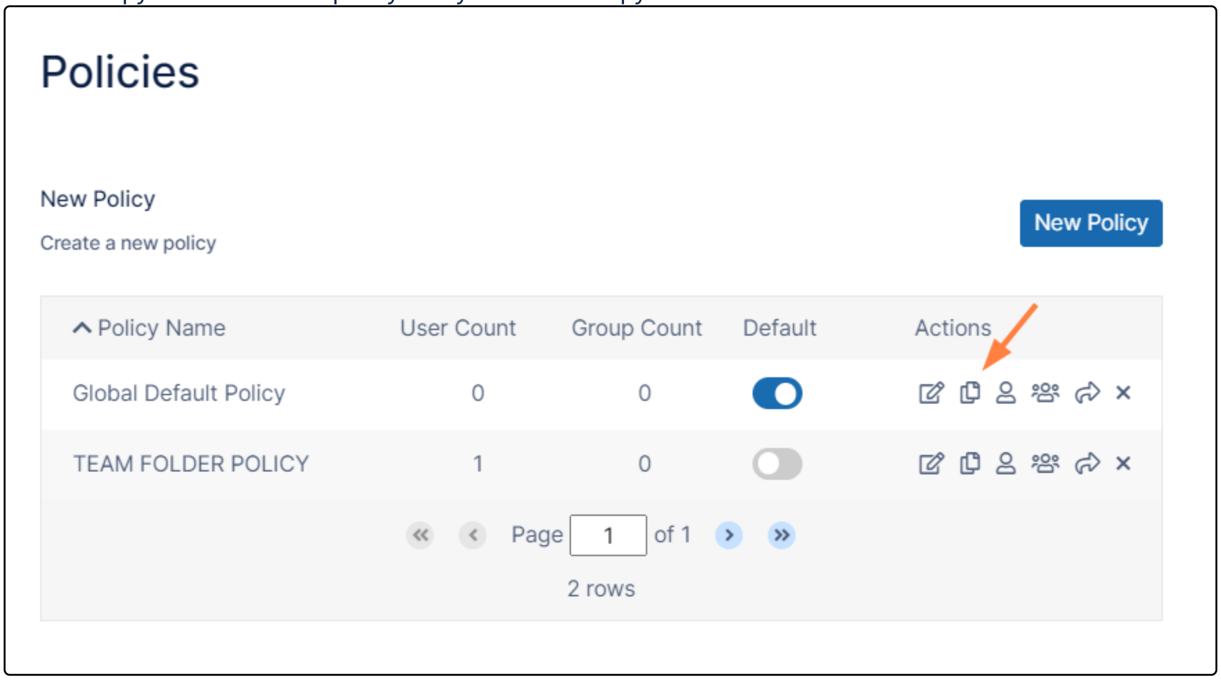


💡 Instead of creating a new policy, you have the option to copy an existing policy including changes you have made to its settings..

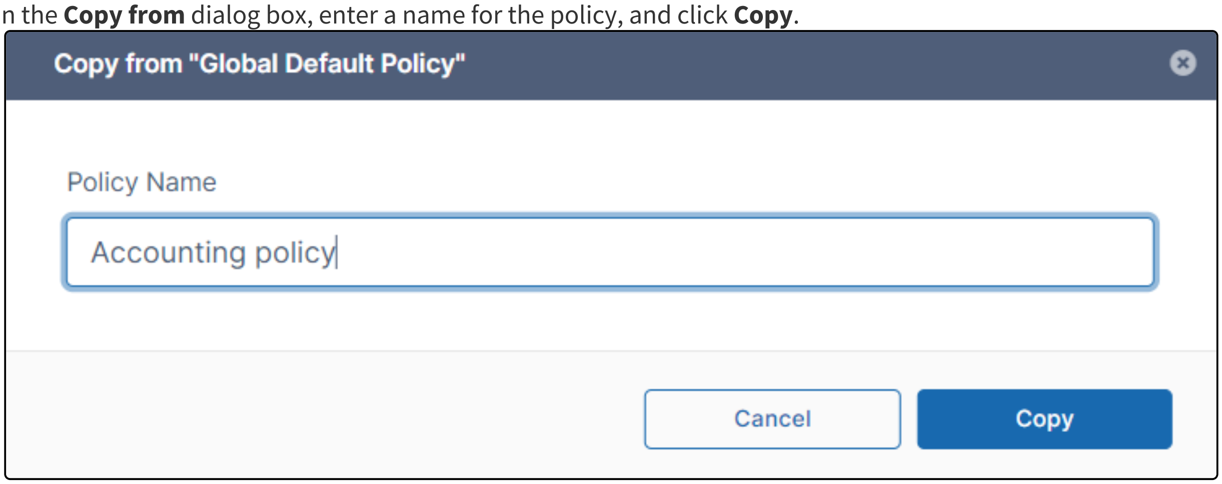
To copy a policy:

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

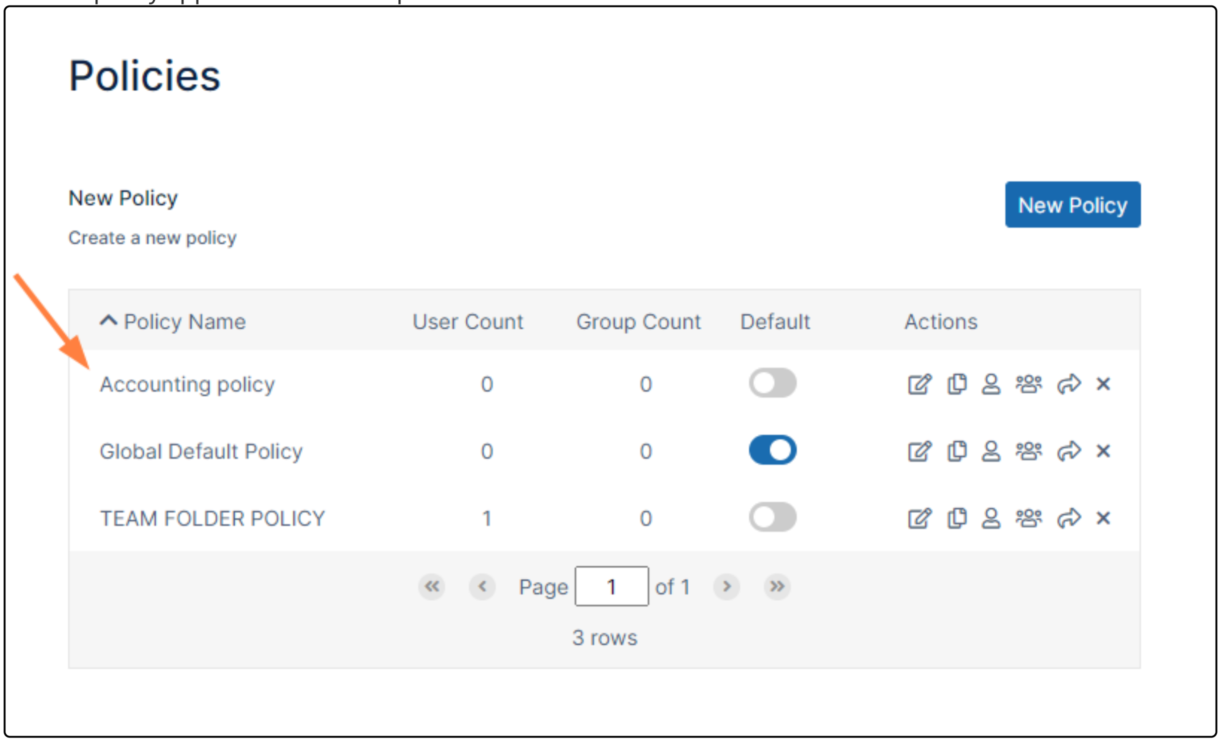
2. Click the copy icon next to the policy that you want to copy



In the **Copy from** dialog box, enter a name for the policy, and click **Copy**.



The new policy appears in the list of policies:



Managing Policy Users and Groups

A policy can be assigned to one ore more user or group.

To assign a user to a policy:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
2. Click the user icon next to the policy that you want to assign a user to.
3. Use the arrow to move the user to the **Policy Users** list box.
4. To save your changes, click **Close**.

To assign a group to a policy:

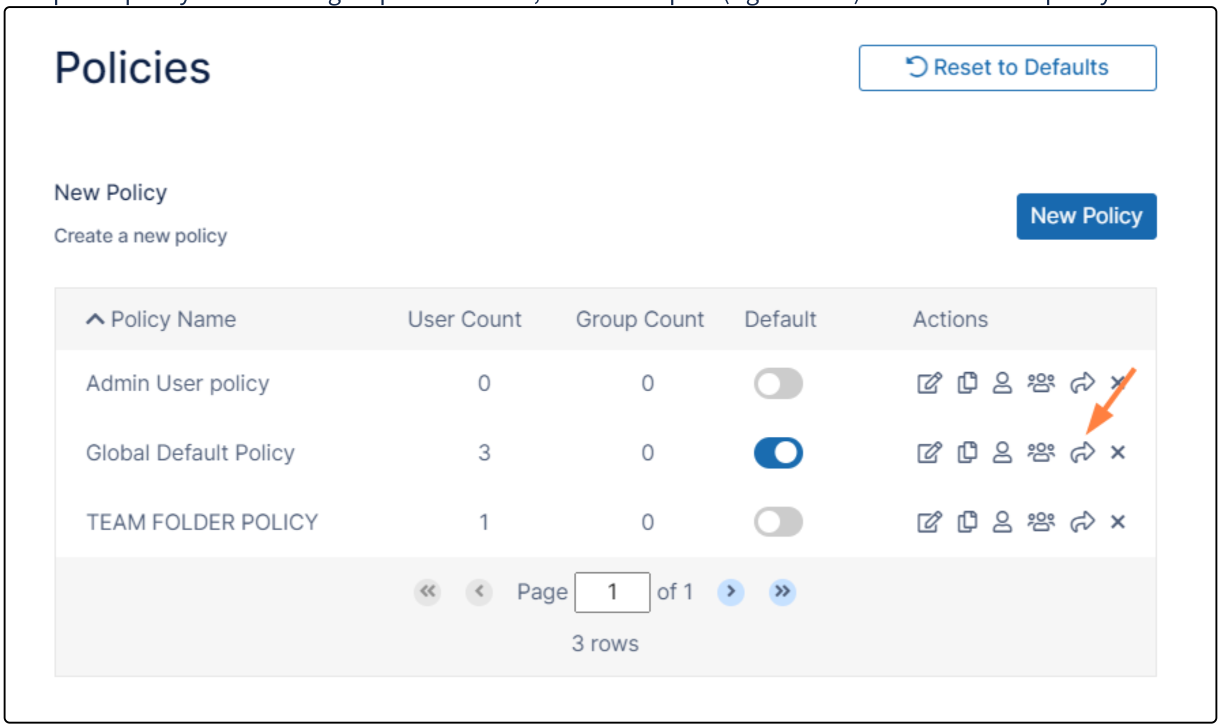
1. Log into the Admin Portal.
2. Click **Settings**.
3. On the **Policies** tab, to open the **Manage Policy Groups** window, click the groups icon.
4. In the **Manage Policy Groups** window, in **Available Groups**, select a group.
5. Use the arrows to move the group to the **Policy Groups** list box.
6. To save your changes, click **Close**.

Exporting a list of policy members

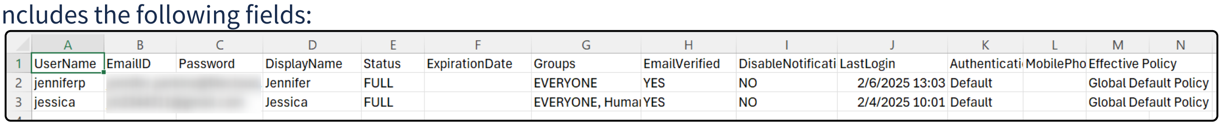
Beginning with FileCloud Version 21.3, you can see which users and groups are members of a policy by exporting them.

To export policy members:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
   The **Policies** page opens.
2. To export a policy's users and groups to a csv file, click the export (right arrow) icon next to the policy.



A csv file listing the individual users in the policy and users in groups in the policy is exported. The file includes the following fields:

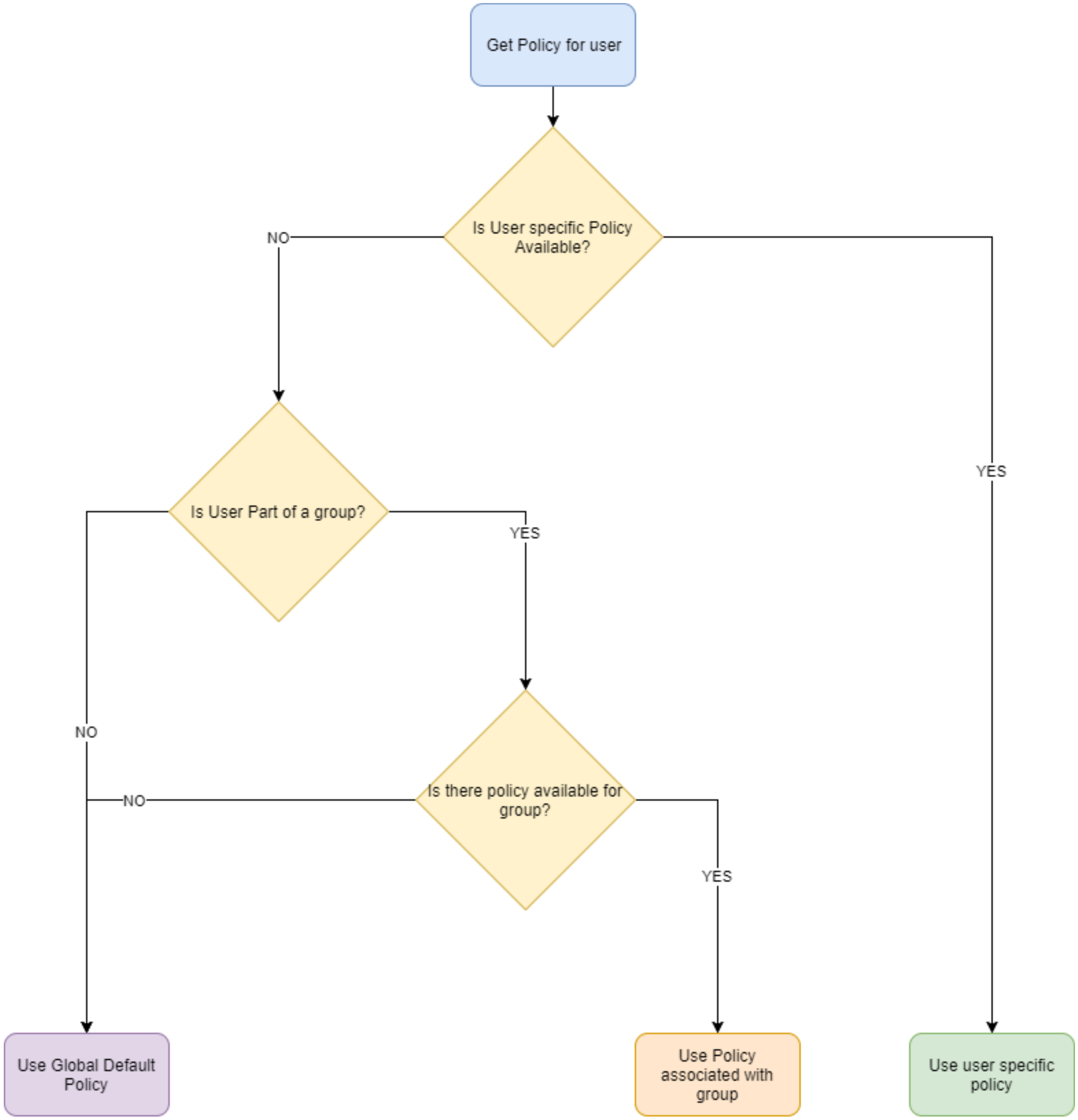


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotificati	LastLogin	Authenticati	MobilePho	Effective Policy	
2	jenniferp	[illegible]		Jennifer	FULL		EVERYONE	YES	NO	2/6/2025 13:03	Default		Global Default Policy	
3	jessica	[illegible]		Jessica	FULL		EVERYONE, Humai	YES	NO	2/4/2025 10:01	Default		Global Default Policy	

Manage the Recycle Bin Using Policies

Policy Calcuations Best Practices

An effective policy for a user is calculated on multiple factors



Policy Selection Scenarios

Case 1: User with no policy assigned : **Global Default Policy will be used**

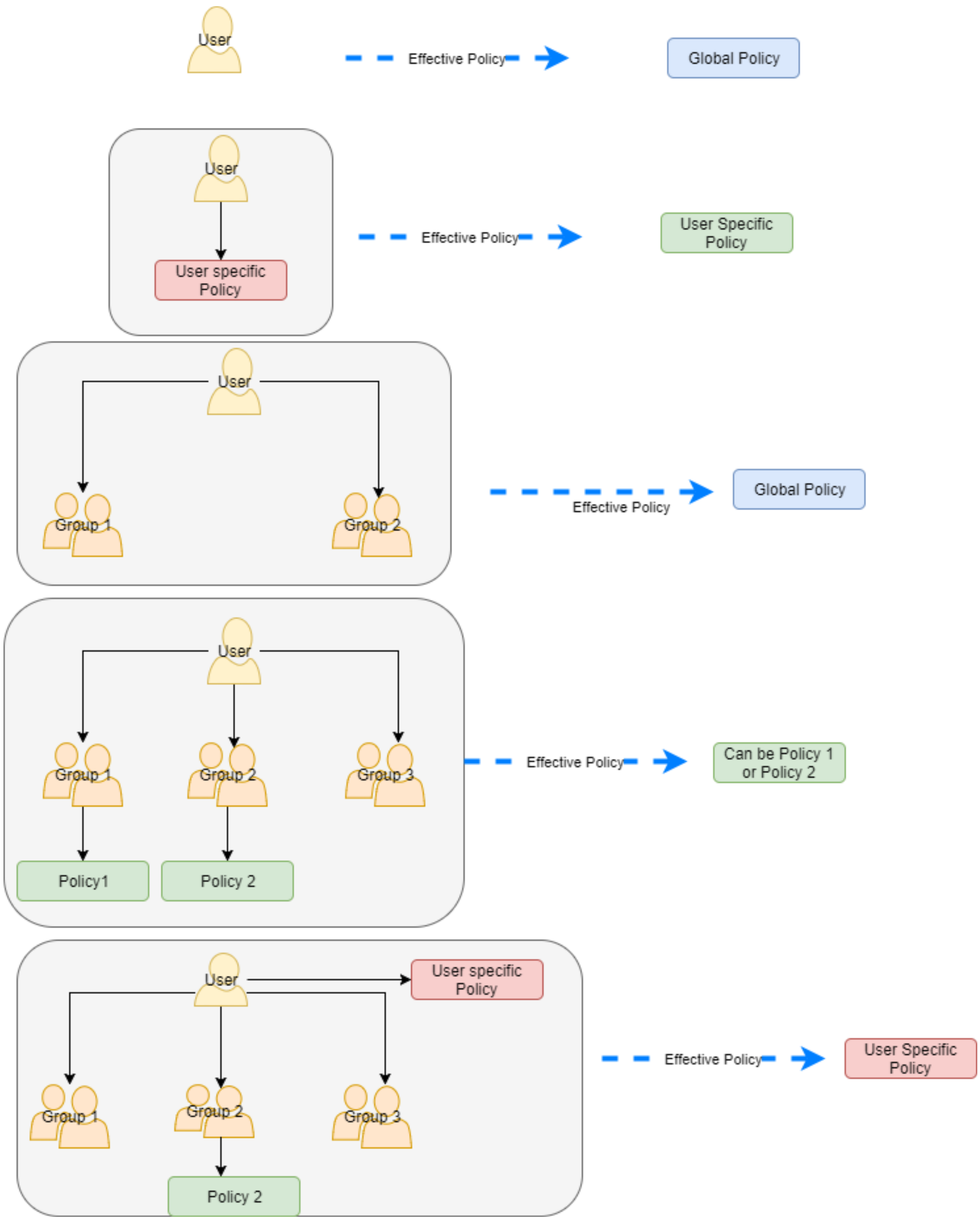
Case 2: User with specific policy assigned: **Assigned policy will be used**

Case 3: User is a member of multiple groups, No Policy is assigned to user or group: **Global Default Policy will be used**

Case 4: User is member of multiple groups and multiple groups have policies: **One of the group policies will be used (Randomly selected).**

Case 5: User is a member of multiple groups and has specific policy assigned and groups have their own policies: **User assigned policy will be used**

Selecting a Policy Scenario Flow Chart


User
Effective Policy
Global Policy
User
User specific Policy
Effective Policy
User Specific Policy
User
Group 1
Group 2
Effective Policy
Global Policy
User
Group 1
Group 2
Group 3
Policy1
Policy 2
Effective Policy
Can be Policy 1 or Policy 2
User
User specific Policy
Group 1
Group 2
Group 3
Policy 2
Effective Policy
User Specific Policy

Notifications for File Changes

FileCloud automatically sends you an email notification when:

- a file or folder is shared with you
- one of the following actions is performed (by you or another user) on a file or folder you have access to:
    - a file or folder is uploaded
    - a file or folder is downloaded
    - a file or folder is shared
    - a file or folder is deleted
    - a file or folder is renamed
    - a file is updated
    - a file is previewed in the browser or one of the mobile apps
    - a file or folder is locked

Administrators can set notifications at the global level and users can override them at the user level.

FAQ's

How Do Notifications Work?

By default, when users make any of the changes listed above to their own files or folders, FileCloud sends them a notification. When a user makes any of the changes listed above to shared files or folders, all users that the file or folder has been shared with receive a notification.

All file change notifications are consolidated and emails are are sent by FileCloud at regular notification frequencies (15 minutes, 1 hour, 1 day etc) as set by your FileCloud administrator as part of the Cron Job Setting.

Why is the User Not Getting a Notification?

If you have enabled file and folder change notifications and a user is not receiving a notification, it may be because:

- that specific file change was blocked in the Admin user interface in Policy settings or in Notifications settings.

Where was the change made?

To receive a notification, actions must occur in one of the following places:

- The FileCloud Admin Portal
- The FileCloud User Portal
- The FileCloud Sync client
- The FileCloud Drive client
- The FileCloud Mobile App

Is the Notification Blocked in Another Place?

File change notifications can be blocked for a specific action in any of the following places:

- Global settings
- Policy settings
- Share settings
- File or folder settings

- Account settings for external users

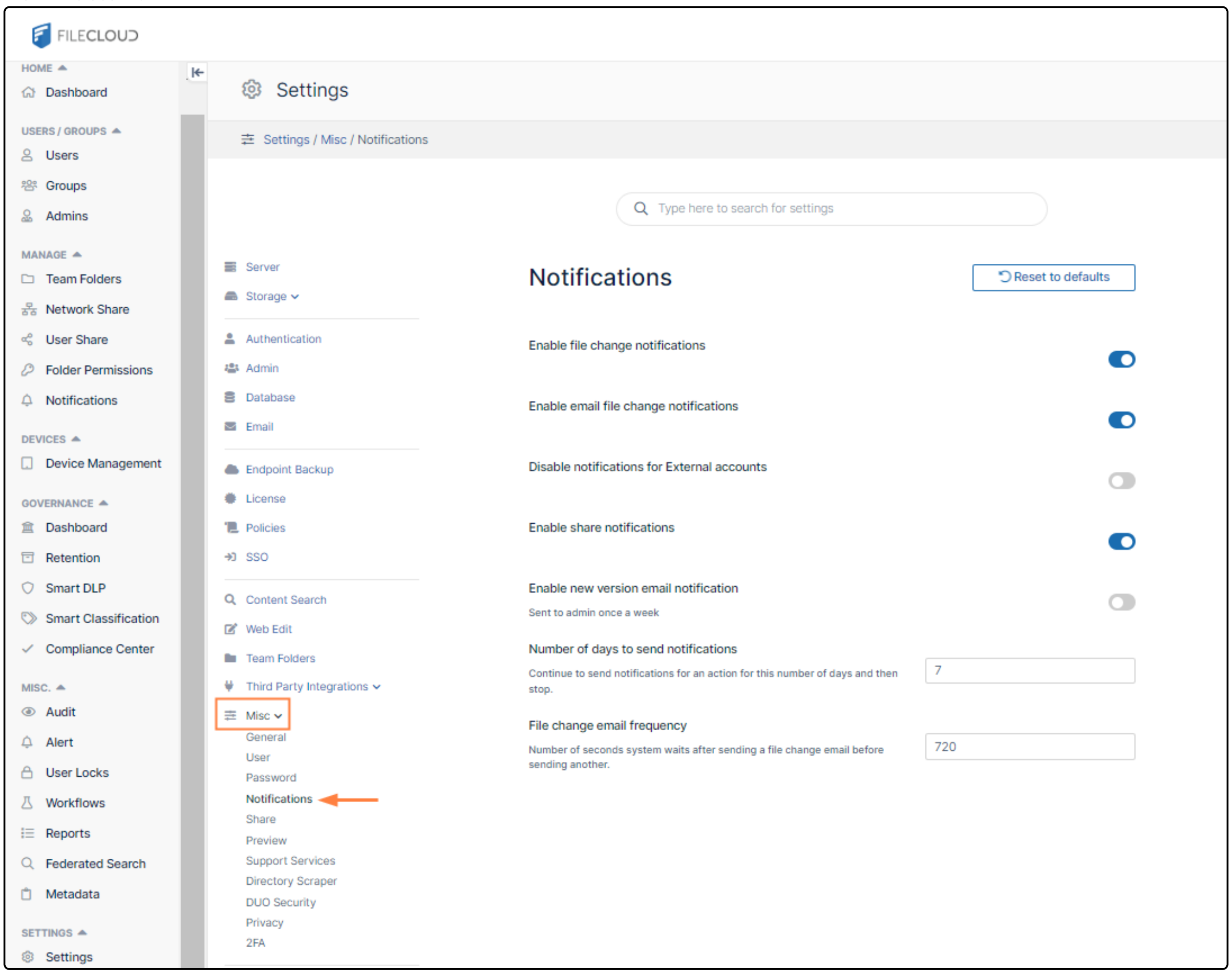
If a user is not receiving a notification, check to see if that file action is disabled at any level.

Are you using a trial account?

Trial accounts have notification limits. If you are using a trial account and have been able to send notifications previously, the notification limit may have been reached.

How to access notification settings in the admin portal

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

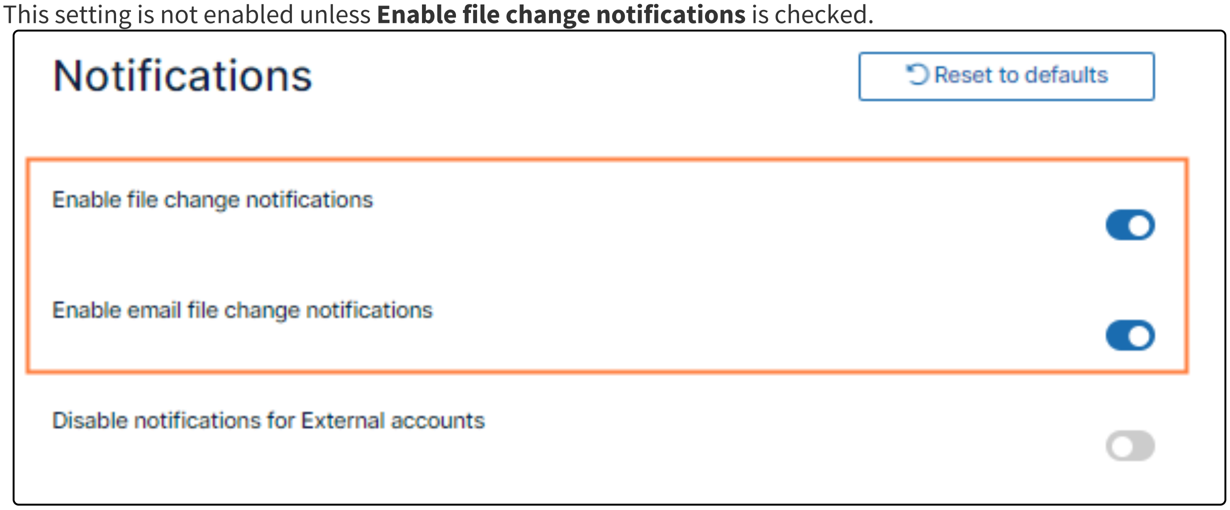


Changing notification settings

Global notification settings

Enable or Disable ALL Notifications

To enable file change notifications:

1. Access the **Notifications** settings page.
2. To display notifications of file changes on the user portal, check **Enable file change notifications**.
3. To send email notifications of file changes to users, also check **Enable email file change notifications**.
   This setting is not enabled unless **Enable file change notifications** is checked.
   

4. Click **Save**.

> Beginning with FileCloud 20.1, if **Enable file change notifications is unchecked**, users cannot override the admin notification settings.

Set the Frequency for ALL Notifications

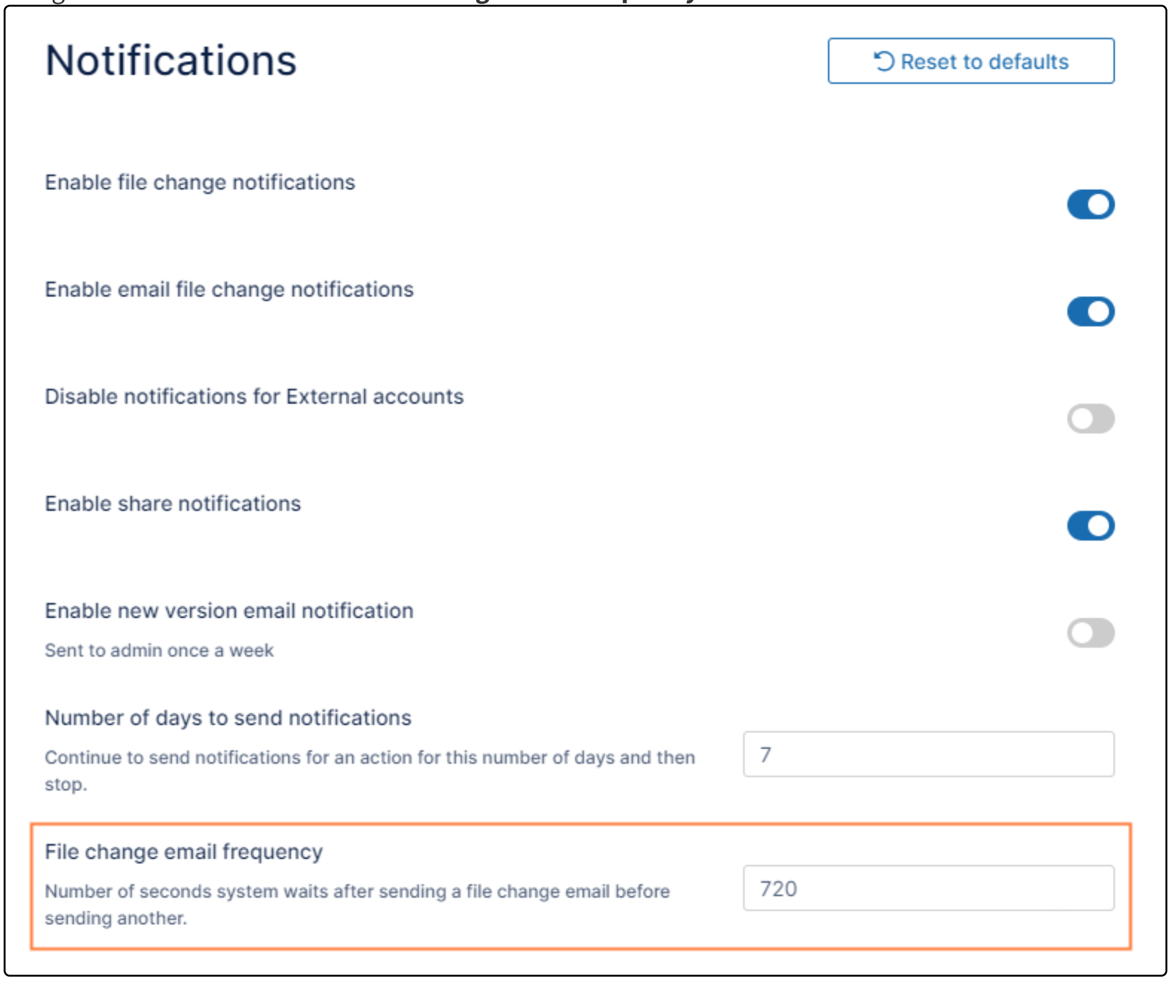
Increase the Frequency of Notifications

You can set the file change notification frequency level in the Admin portal, and users can override this and set their own frequency in the User portal.

- This option is only available in FileCloud Server version 19.1 and later.
- In previous versions, the File Change Frequency Notification could only be changed in cron's running interval.

To set file change notification frequency in the admin portal:

1. Access the **Notifications** settings page.
   The default file change email frequency is 720 seconds (12 minutes).
2. Change the number of seconds in **File change email frequency**.



3. Change the value.
4. Save your changes.

To see how users can set their own notification frequency, see the help topic Notifications.

Do not send outdated email notifications

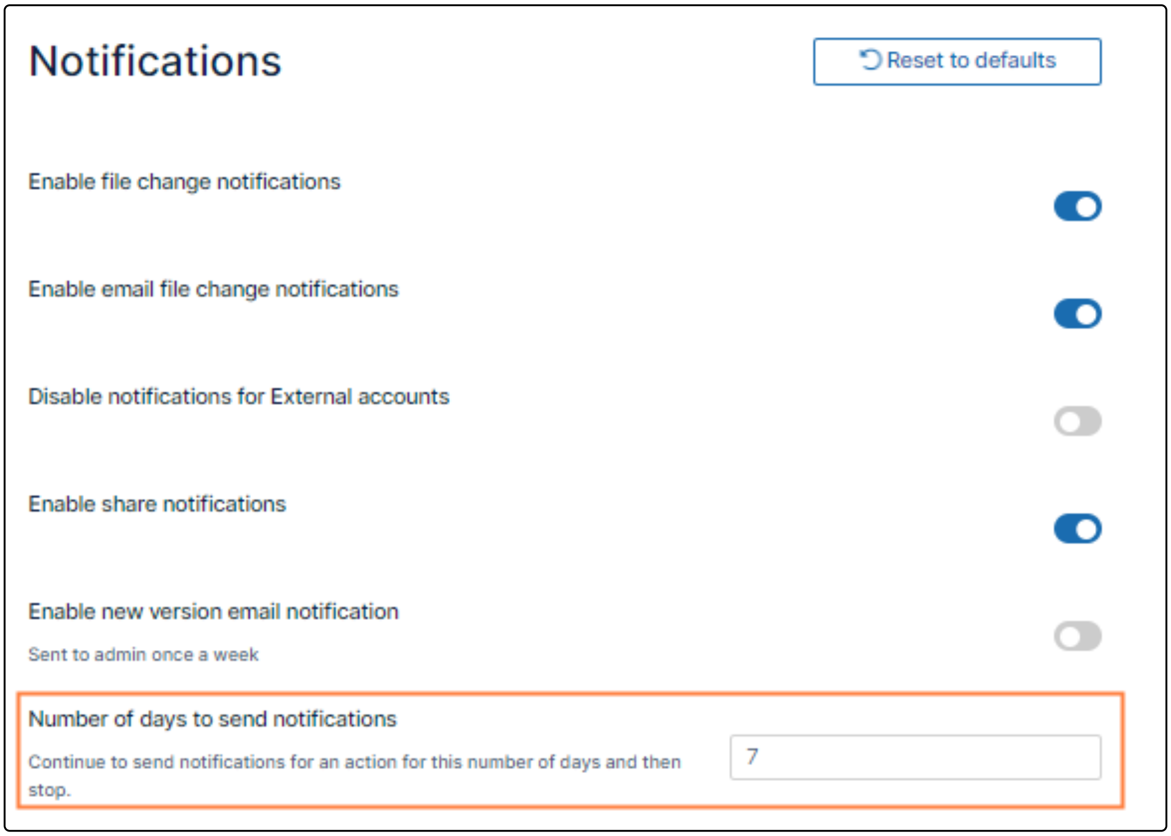
Do not send notifications that were created a number of days ago

You can configure FileCloud Server to stop sending email notifications for an action after a specified number of days (by default, 7 days). This prevents the system from sending notifications that are no longer relevant.

To prevent sending notifications after a specific number of days:

1. Access the **Notifications** settings page.

2. In **Number of days to send notifications**, type in a number.
   Enter **0** to disable notifications.



3. Save your changes.

External User Account Notifications

User accounts with external access can manage FileCloud content only through a Web browser.

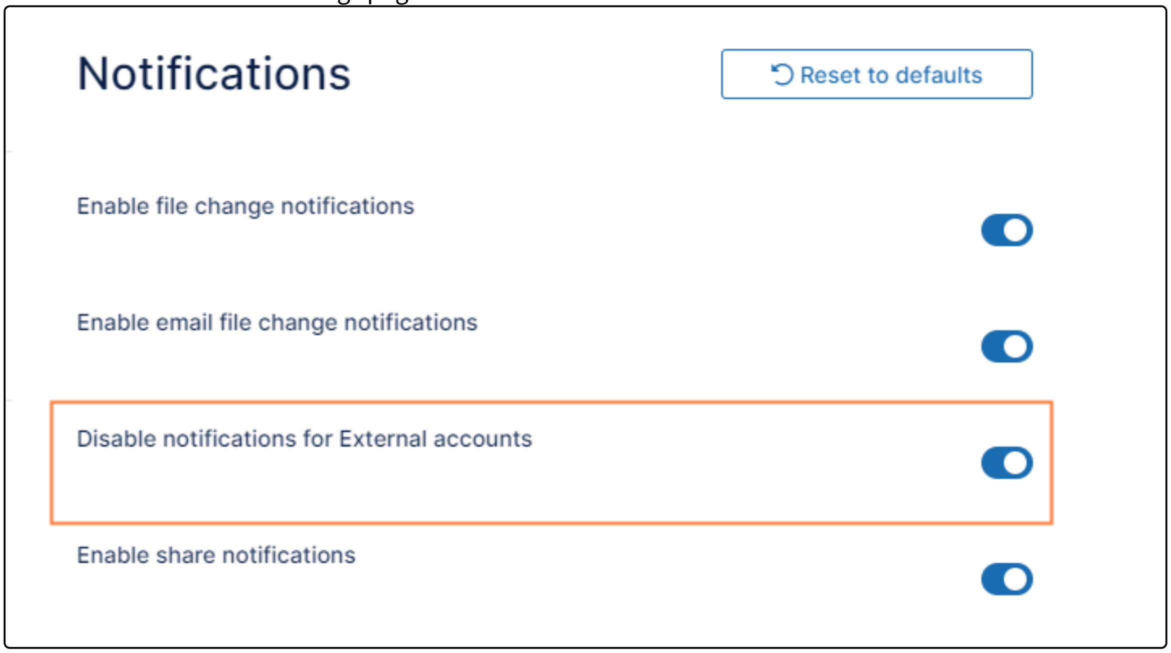
These user accounts:

- Can only view/upload/download to content shared with them
- Do not count towards the user license limit
- Cannot be authenticated via AD and can only be local user account
- Linked email accounts cannot use the same domain specified in the FileCloud URL
- Can't be added directly to network shares via the Admin Portal
- Can access content from network folders if they are shared

If you have users with external access to content, you may want to avoid confusion that may occur when an email is sent about content that users with external accounts cannot access.

To set the file change notification frequency for external accounts:

1. Access the **Notifications** settings page.

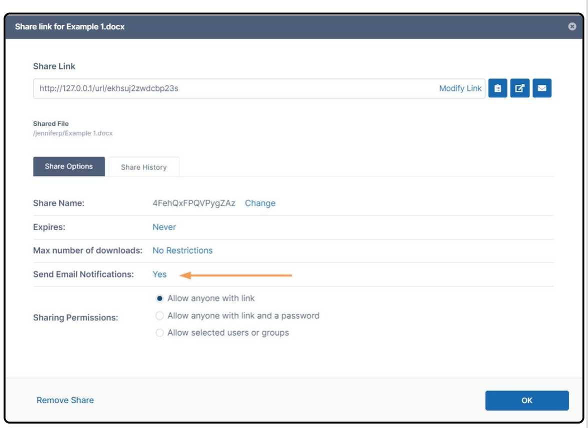
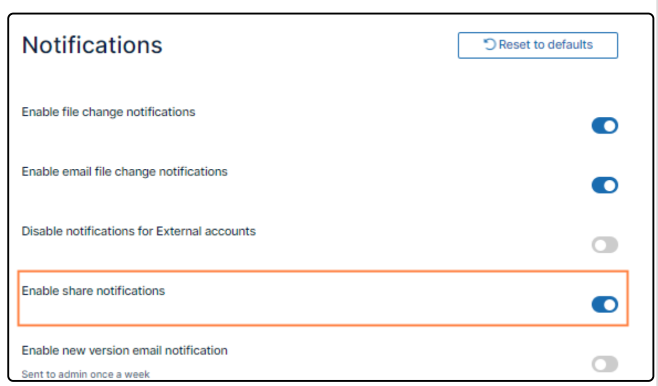


2. To stop sending notifications, locate the setting **Disable notifications for External accounts** and enable it.
3. Click **Save**.

Sharing Notifications

When a File or Folder is shared, the owner can allow or restrict sending file change notifications to all users that have access to that share.

- Enabling this setting sends an email notification when a publicly shared file is opened or downloaded.
- Notifications can be enabled or disabled by the user in the User Portal
- Notifications can also be enabled or disabled by the admin in the Admin Portal.
- The user can override these settings by setting custom notifications for a file or folder path.

User Portal	Admin Portal
	

User Portal	Admin Portal
To share a file with everyone without restrictions: 1. Open a browser and log in to the user portal. 2. Click My Files. 3. Hover over the file you want to share. 4. Click the share icon. 5. On the Share Link for File dialog box, click **Share Options**. 6. In **Share Options**, set **Send Email Notifications** to **Yes**.	**To enable file change notifications for shares:** 1. Log in to the admin portal. 2. Access the Notifications settings page. 3. Enable **Enable share notification**. 4. Click **Save**.

Customize notification settings for individual users and groups

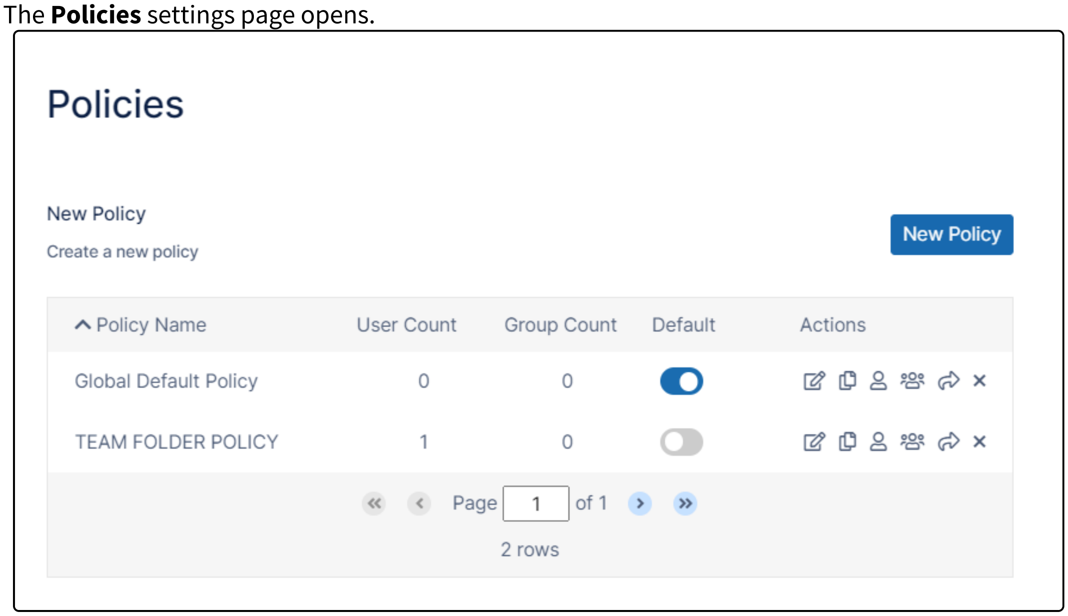
User and Group Notifications

You can customize notifications for specific users or groups by customizing the notifications settings on their policies.

For example, notifications can be disabled for a specific user or group by disabling notifications in their policy.

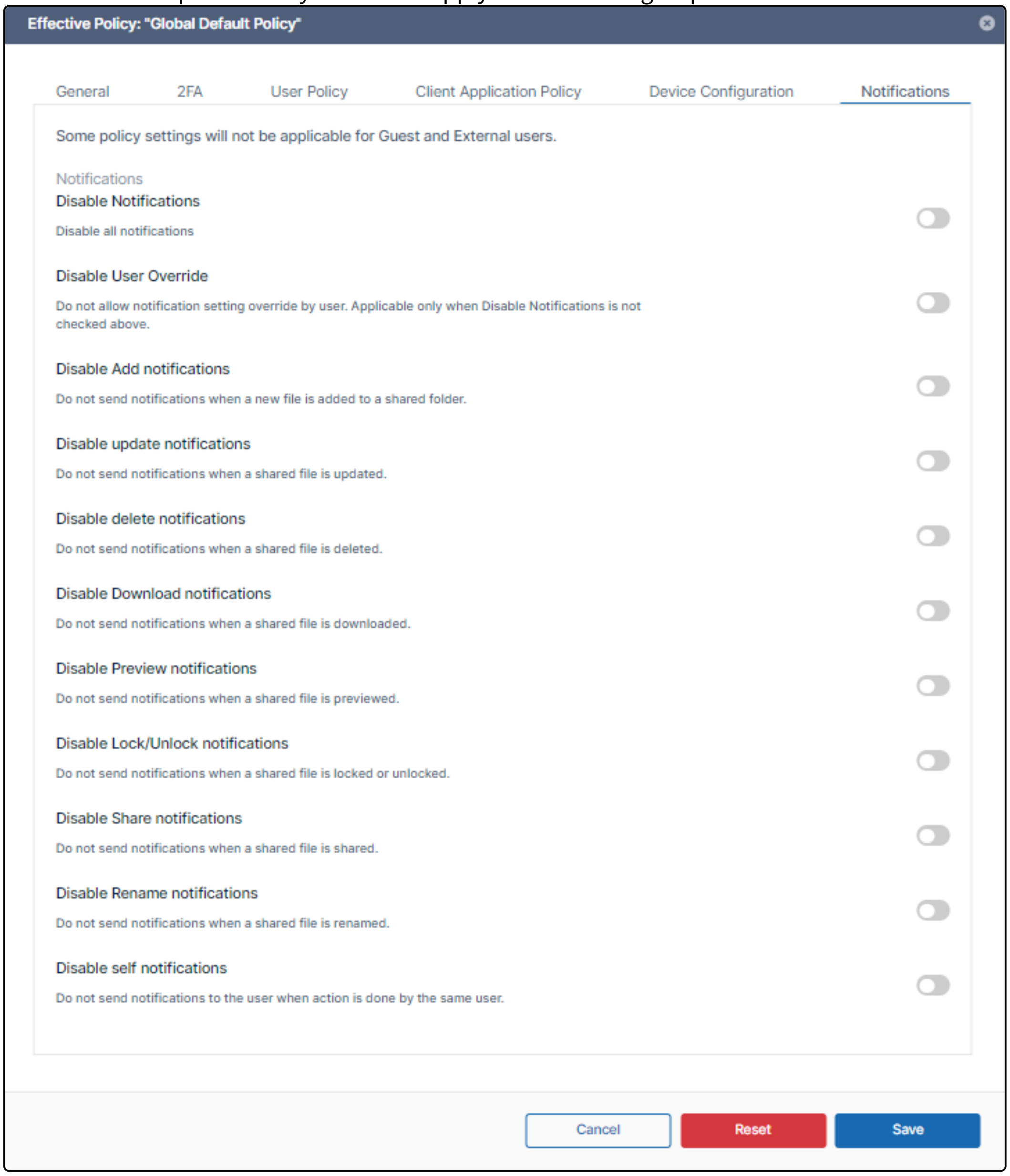
Note that unless **Disable User Override** is checked, users can override all of these settings except for **Disable Notifications**.

To customize notifications through a policy:

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

2. Edit the policy assigned to the user or group.

3. Click the **Notifications** tab.
4. Turn on disable options that you want to apply to the user or group.



Disable Notifications - When checked, disable all notifications. This setting cannot be overridden.
Disable User Override - When checked, disable user override of these settings. Applicable only when the above setting, **Disable Notifications**, is not checked.
Disable Add notifications - Do not send notifications when a new file is added to a shared folder.
Disable update notifications - When YES, do not send notifications when a shared file is updated.
Disable delete notifications - When YES, do not send notifications when a shared file is deleted.
Disable Download notifications - When YES, do not send notifications when a shared file is downloaded.

Disable Preview notifications - When YES, do not send notifications when a shared file is previewed.
Disable Lock/Unlock notifications - When YES, do not send notifications when a shared file is locked or unlocked.
Disable Share notifications - When YES, do not send notifications when a shared file is shared.
Disable Rename notifications - When YES, do not send notifications when a shared file is renamed.
Disable self notifications - When YES, do not send notifications to a user when any of these actions are done to a file or folder (shared or not shared) owned by the user.

5. Click **Save**.

Also see:

Customize notifications in user settings

Example Setup: Fixed Notifications for Uploads and Deletions

In this example, a company shares FileCloud support folders with customers so the customers can upload help requests that are then viewed by Support. The customers are also permitted to delete requests that no longer have to be addressed.

As the admin you must set up email notifications that inform Support staff when:

- new help requests are uploaded so they can begin processing them
- existing help requests are deleted in case they have begun addressing them.

To prevent accidental changes to these notifications, you do not allow users to change the notification settings.

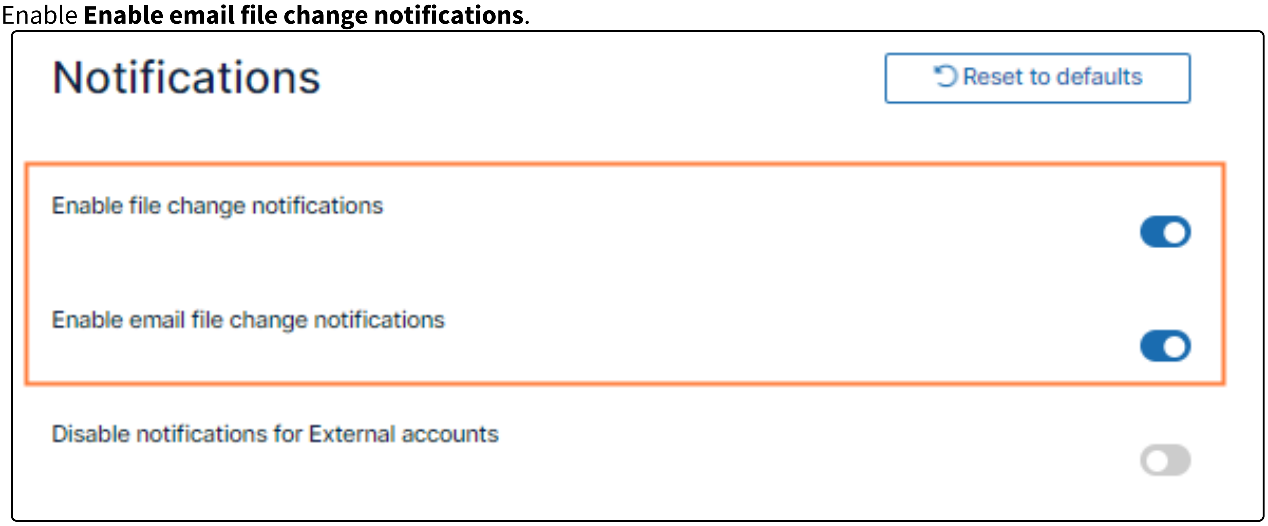
To configure these settings**:**

1. To enable email notifications globally, open the Notifications settings page.
   To open the Notification settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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

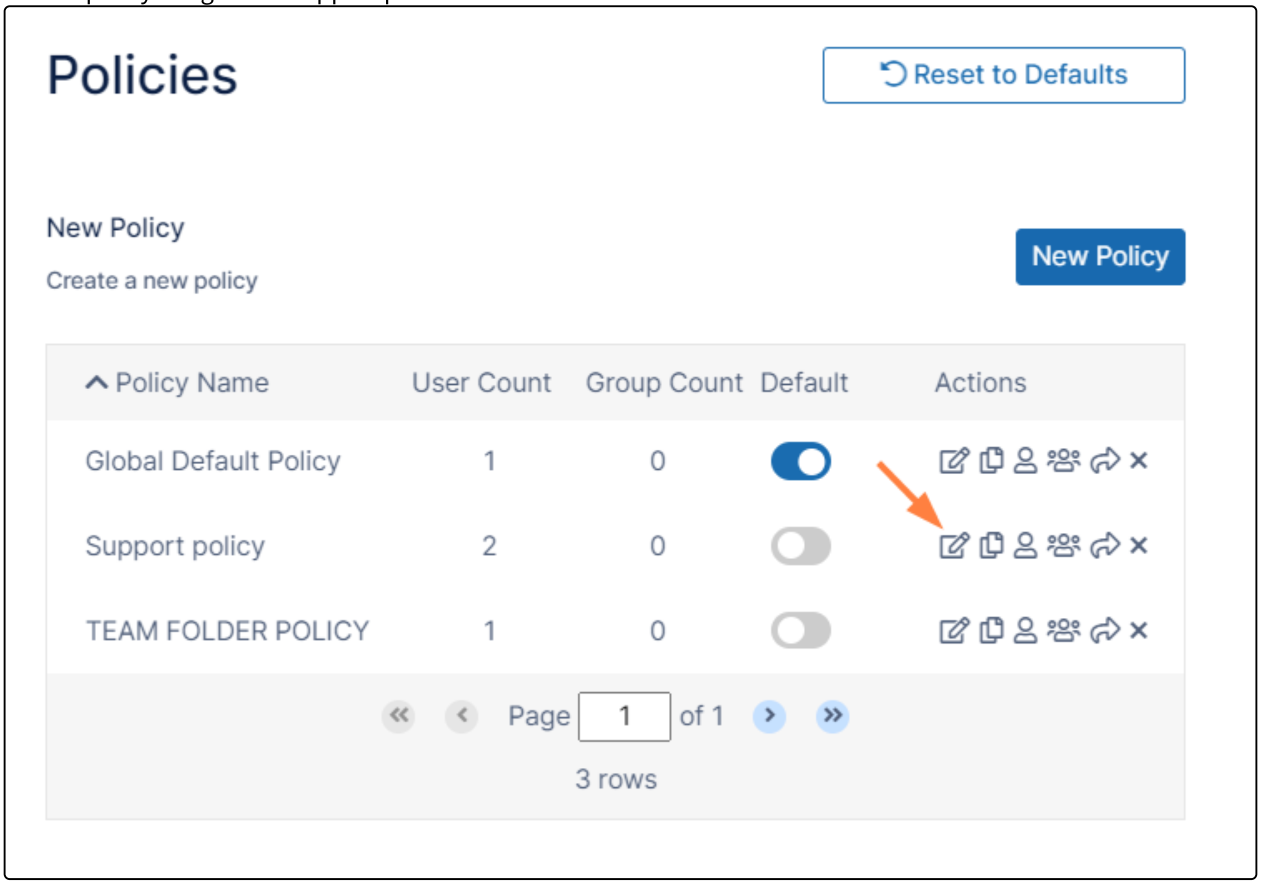
The **Notifications** settings page opens.

2. Make sure **Enable file change notifications** is enabled. if it is not enabled, **Enable email file change notifications** is not available.
3. Enable **Enable email file change notifications**.

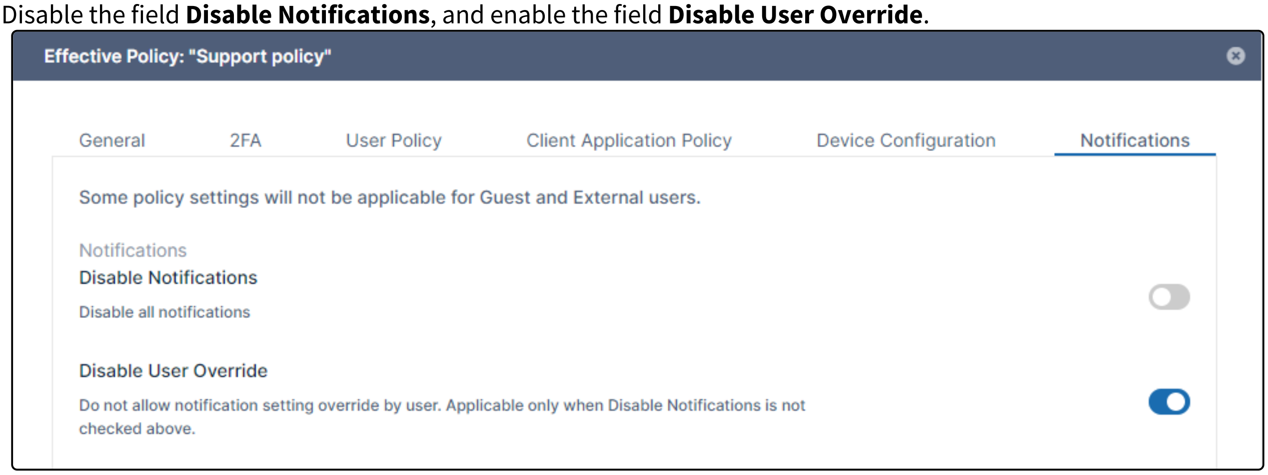


4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
The **Policies** settings page opens.

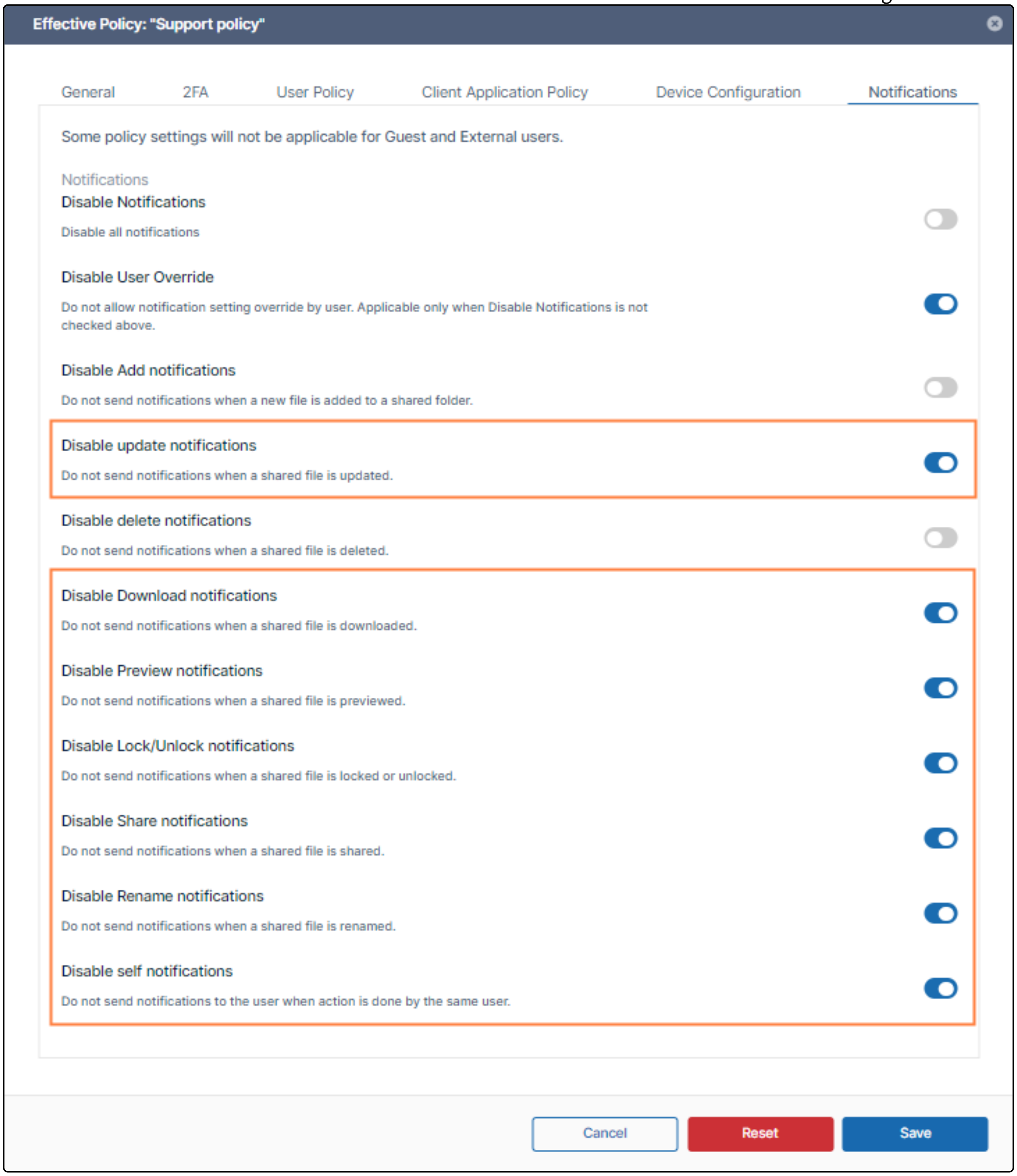
5. Edit the policy assigned to support personnel.



6. Click the **Notifications** tab.
7. Disable the field **Disable Notifications**, and enable the field **Disable User Override**.



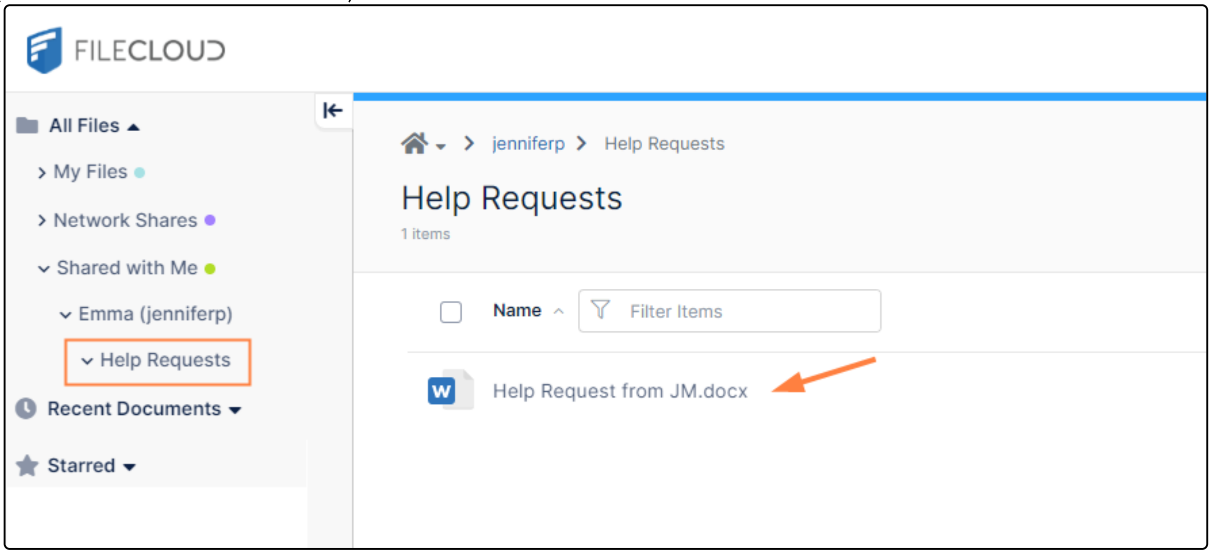
8. Scroll down so that you can view the individual **Disable Notifications** settings, and only leave **Disable Add Notifications** and **Disable Delete Notifications** set to off. Set the other **Disable Notification** settings to on.



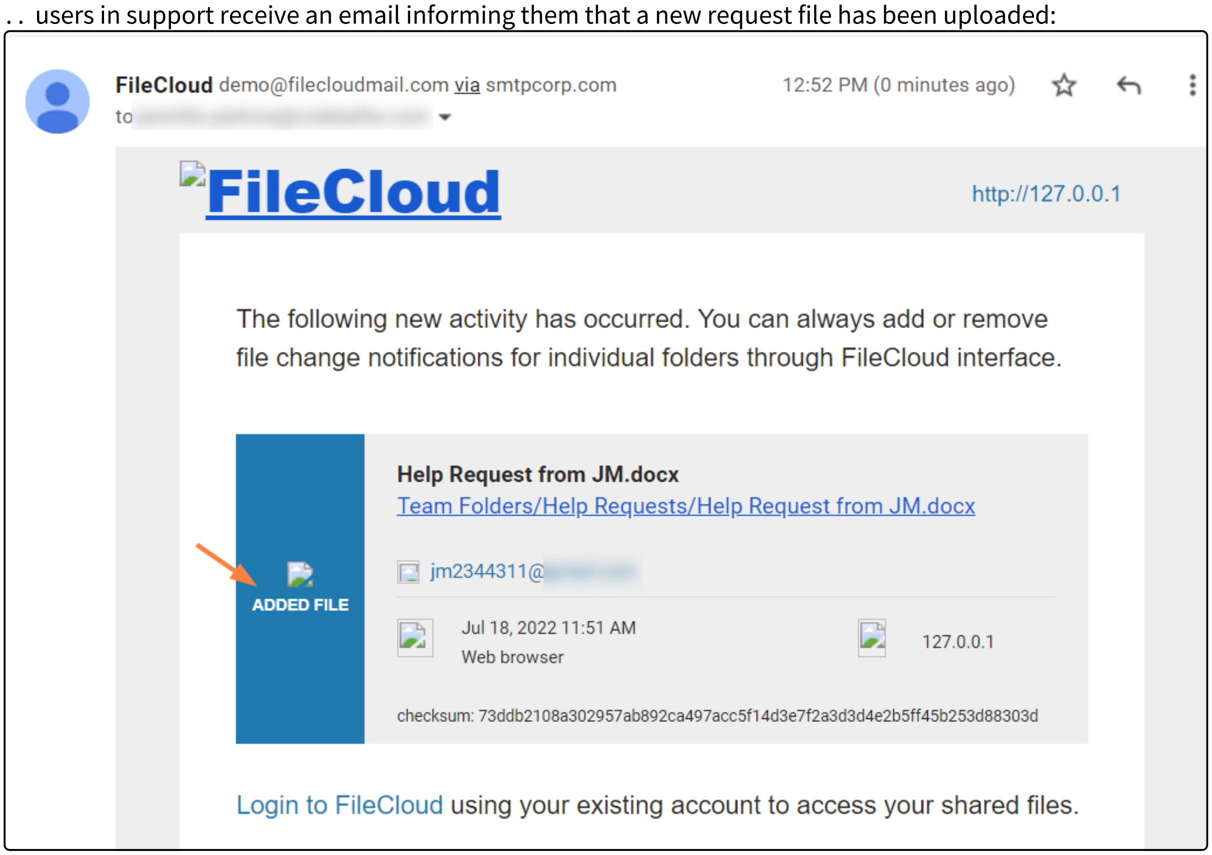
9. Save your changes.

When a customer uploads a help request

Now, when customer JM uploads a help request to the **User Help Requests** folder which has been shared with them (the folder is in **Shared with Me**) . . .

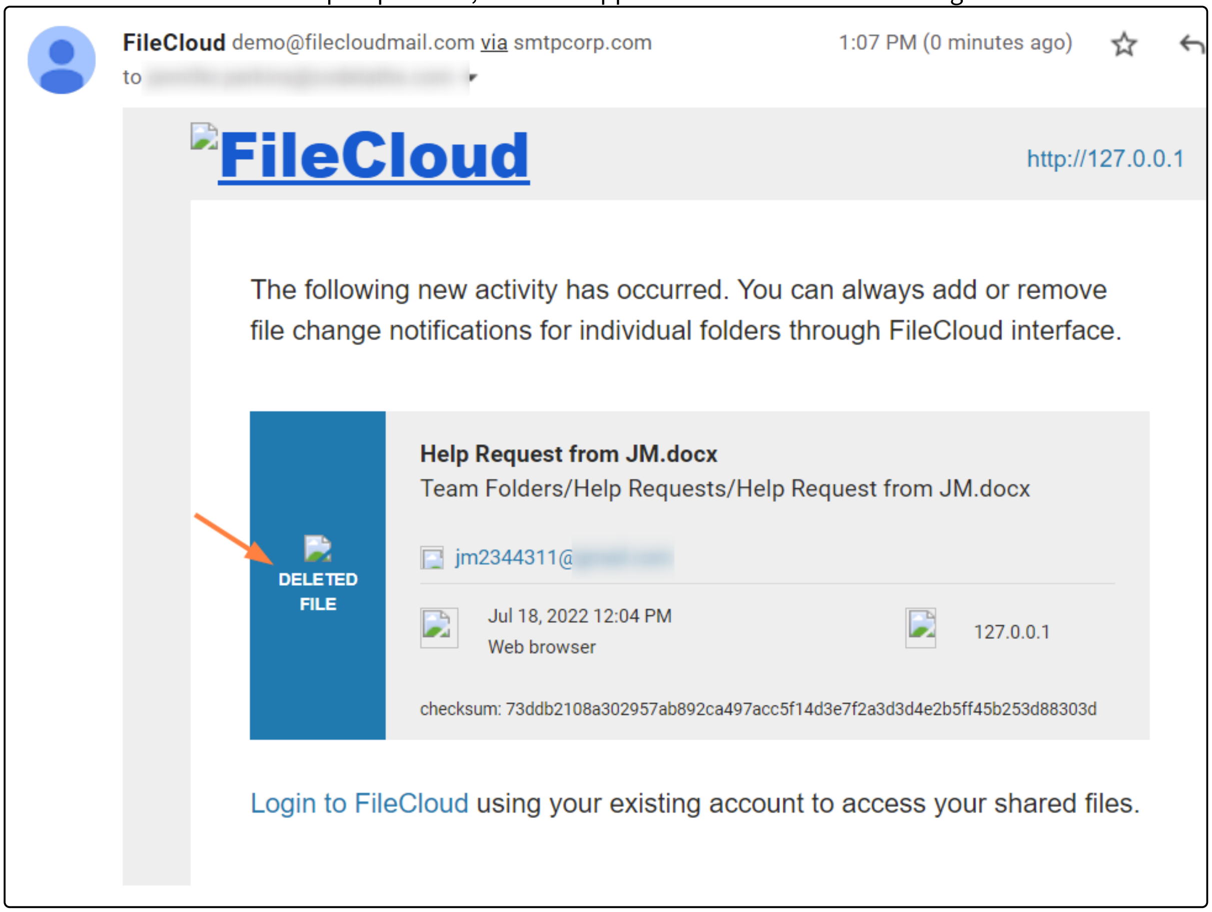


. . . users in support receive an email informing them that a new request file has been uploaded:



When a customer deletes a help request:

If customer JM deletes the help request file, users in support receive an email informing them that it has been deleted:



Example Setup: User-enabled Notifications on Folders

In this example, a telecommunications company uses FileCloud to share Team Folders that hold the latest product and pricing information with everyone in its sales department.

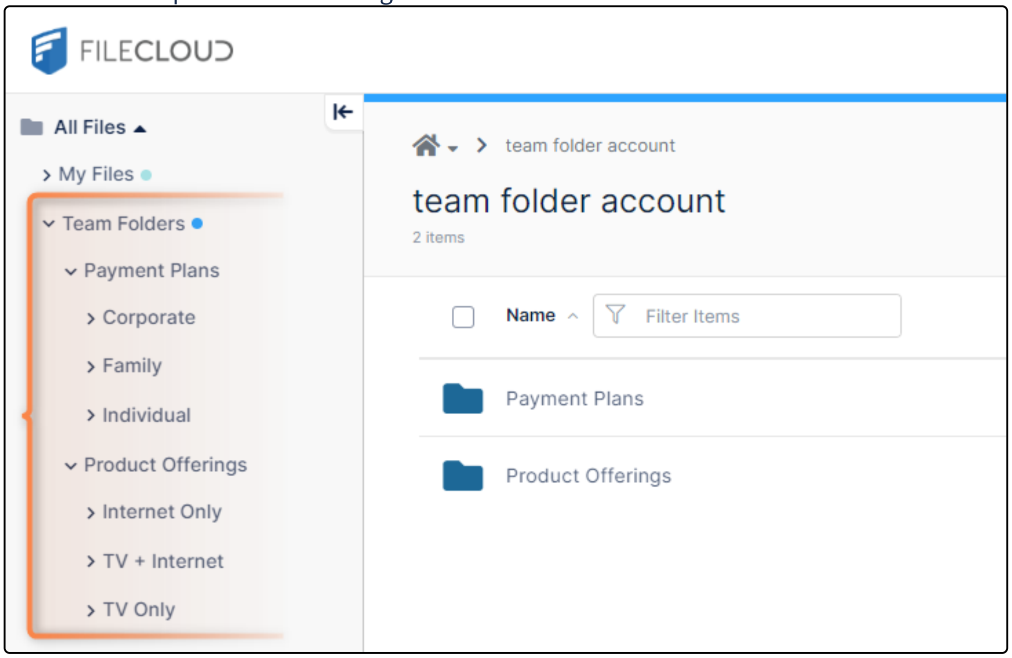
The company has three product offering categories:

- **Internet Only**
- **TV Only**
- **Internet + TV**

and it has three pricing plans:

- **Corporate**
- **Family**
- **Individual**

The company has a Team Folder with information that is available to all sales reps on each product offering and pricing plan. All sales reps see the following under Team Folders:



Each sales representatives works with a specific payment plan and product offering and only needs notifications about the product and pricing plans they work with, and do not want to receive updates about other offerings.

Therefore, as the FileCloud admin, you want each sales rep to be able to customize their file change notifications depending on which campaigns or pricing plans they are currently working with, so they know immediately when these product offerings and prices change. In addition, you want to give sales reps the opportunity to eliminate notifications about information they are not interested in.

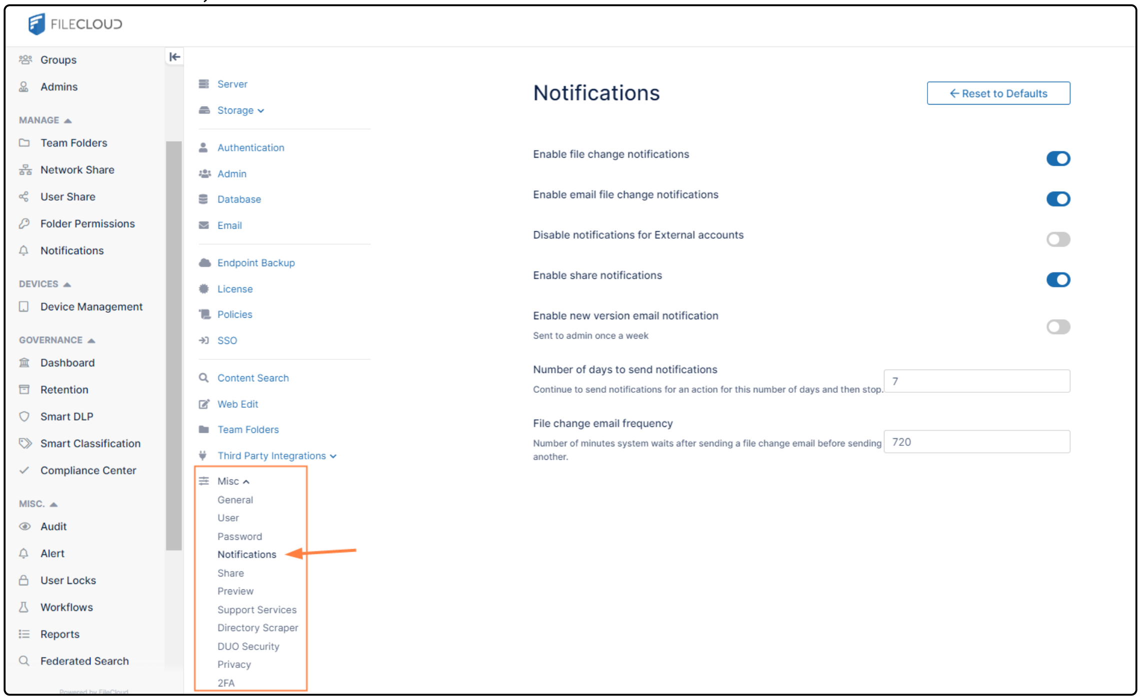
After you configure these capabilities, each sales rep must log in to the user portal and choose the paths of the Team Folders that pertain to them and add notifications to them.

To configure these settings

These are the steps you (the admin) use to set up the notifications according to these requirements:

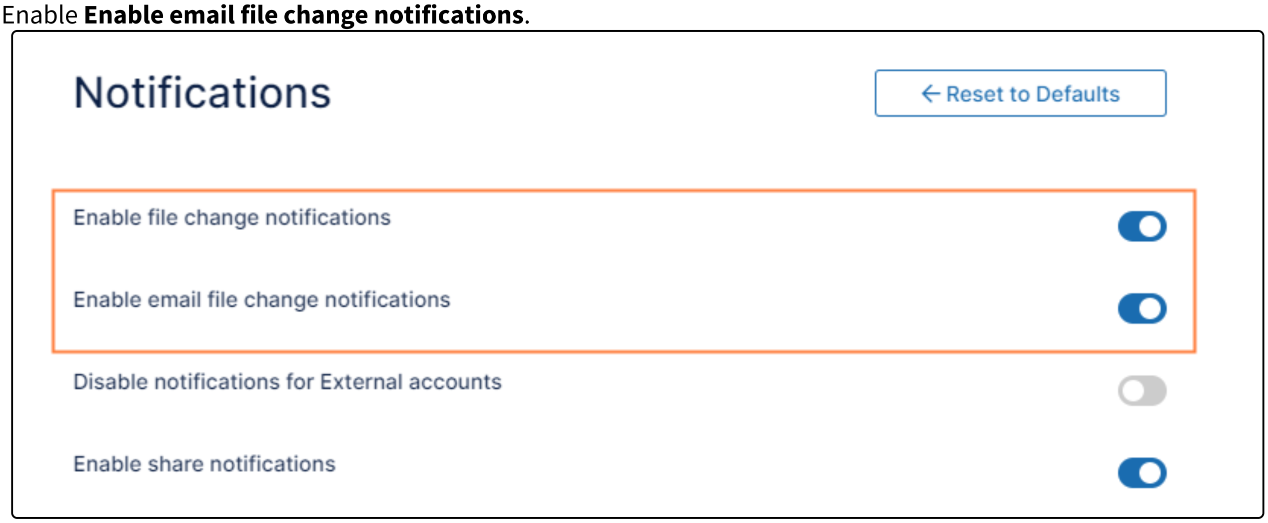
1. To enable email notifications globally, open the Notifications settings page.
   To open the Notification settings page
      a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .

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



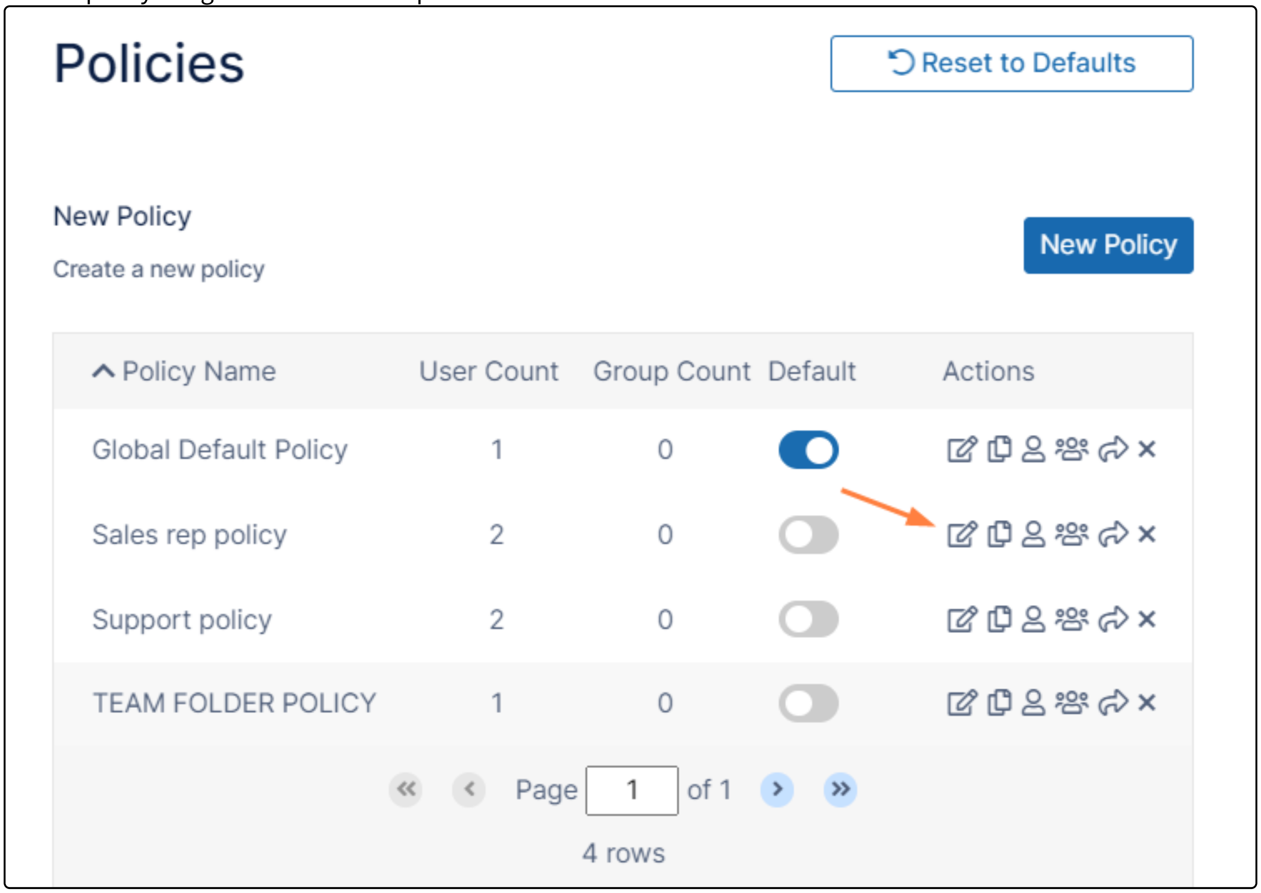
The **Notifications** settings page opens.

2. Make sure **Enable file change notifications** is enabled. if it is not enabled, **Enable email file change notifications** is not available.
3. Enable **Enable email file change notifications**.

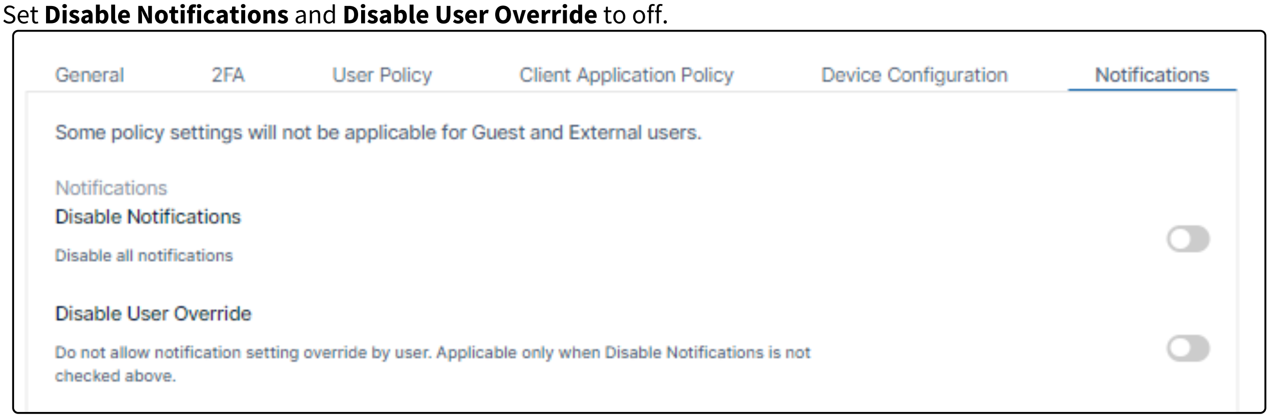


4. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies**  .
The **Policies** settings page opens.

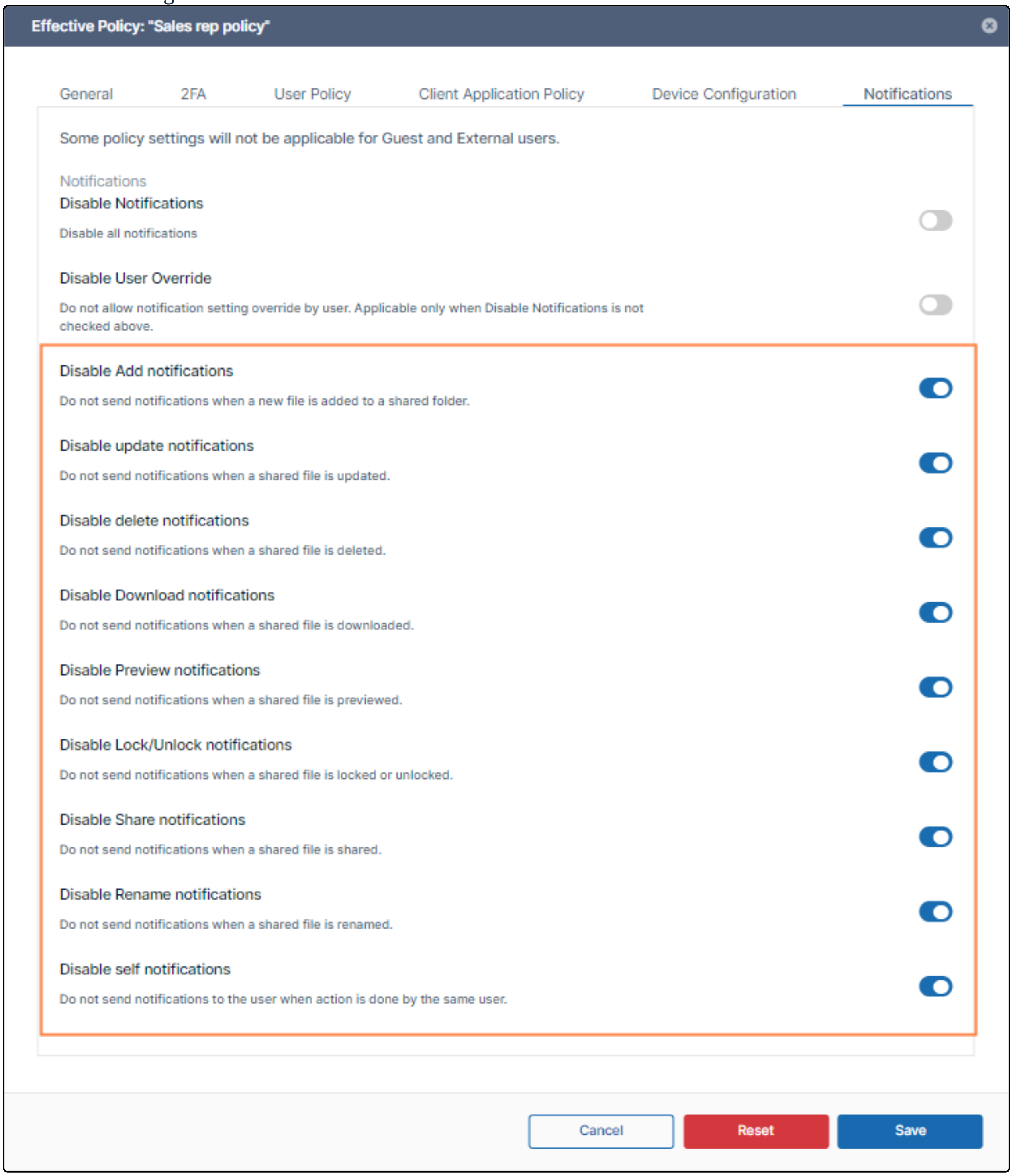
5. Edit the policy assigned to the sales reps.



6. Set **Disable Notifications** and **Disable User Override** to off.



7. Scroll down so that you can view the individual **Disable Notifications** settings, and set all of the **Disable Notification** settings to on.



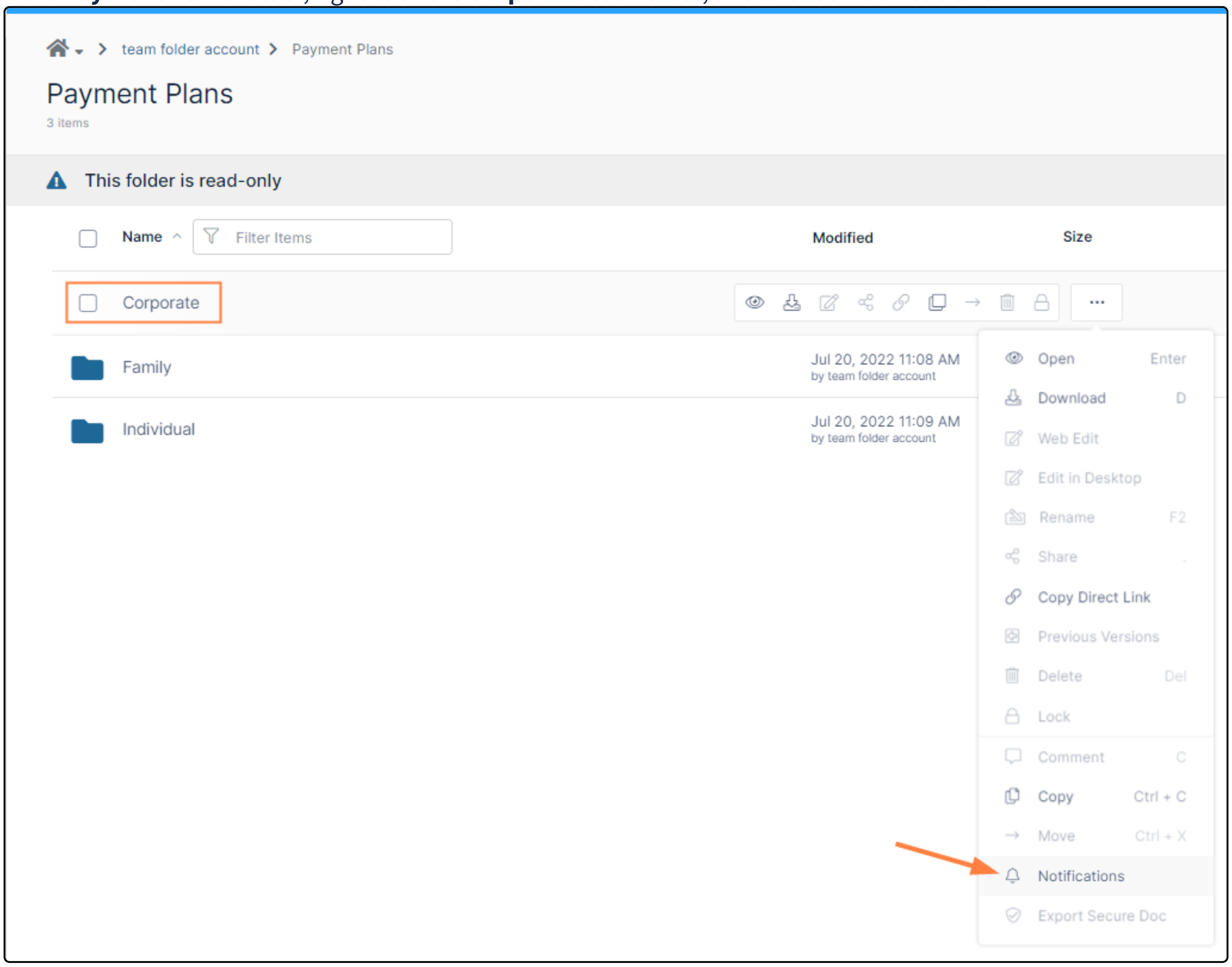
8. Save your changes.

How a Sales Rep sets up notifications about information particular to their clients:

In this example, the sales rep only works with corporate customers who purchase internet only.

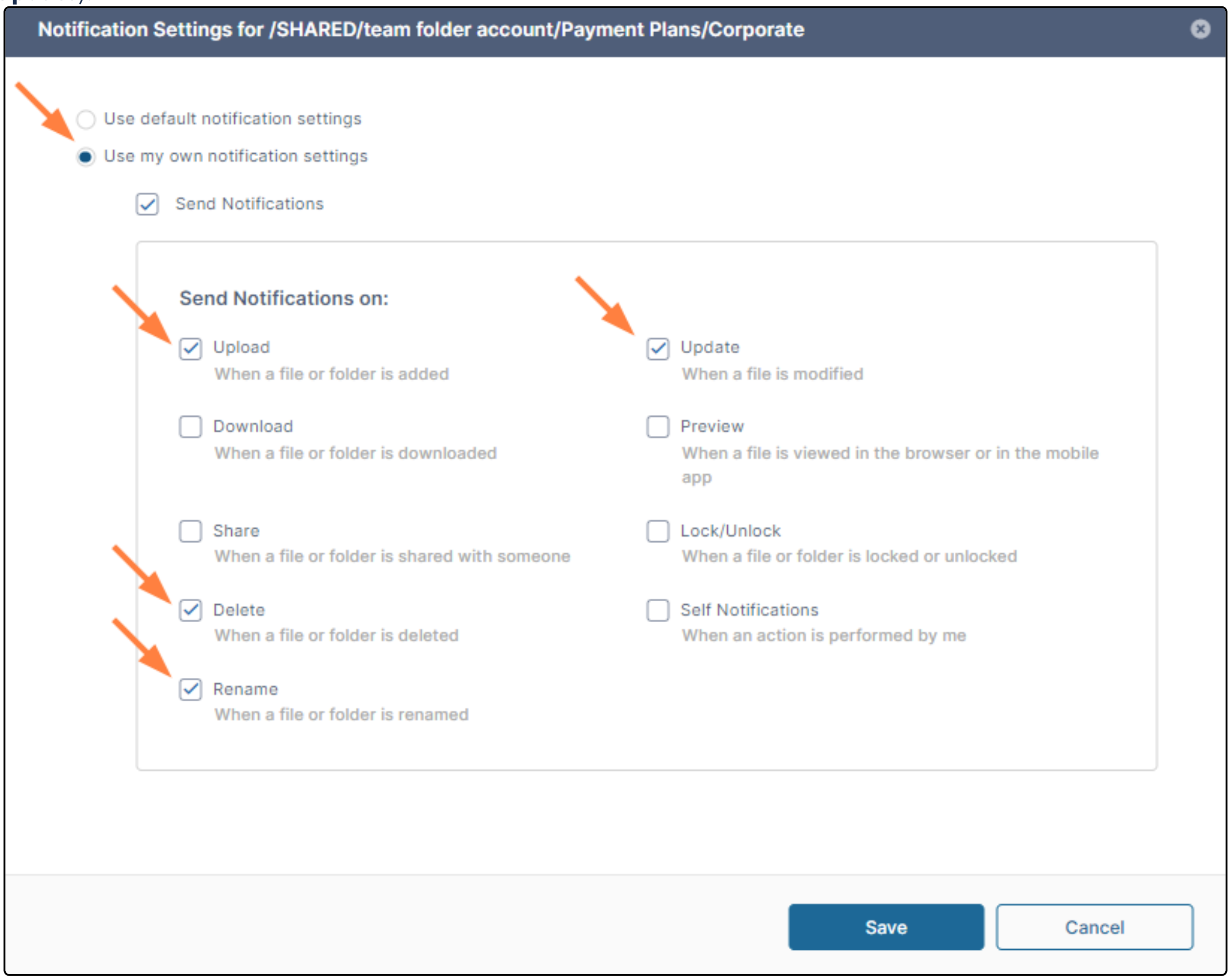
Instructions for the sales rep to configure notifications for just the Corporate and Internet Only Team Folders:

1. Log in to the user portal and go to Team Folders.
2. In the **Payment Plans** folder, right click the **Corporate** sub-folder, and choose **Notifications**.



   Notifications settings for the **Corporate** Team Folder open.
3. Select **Use my own notification settings**.

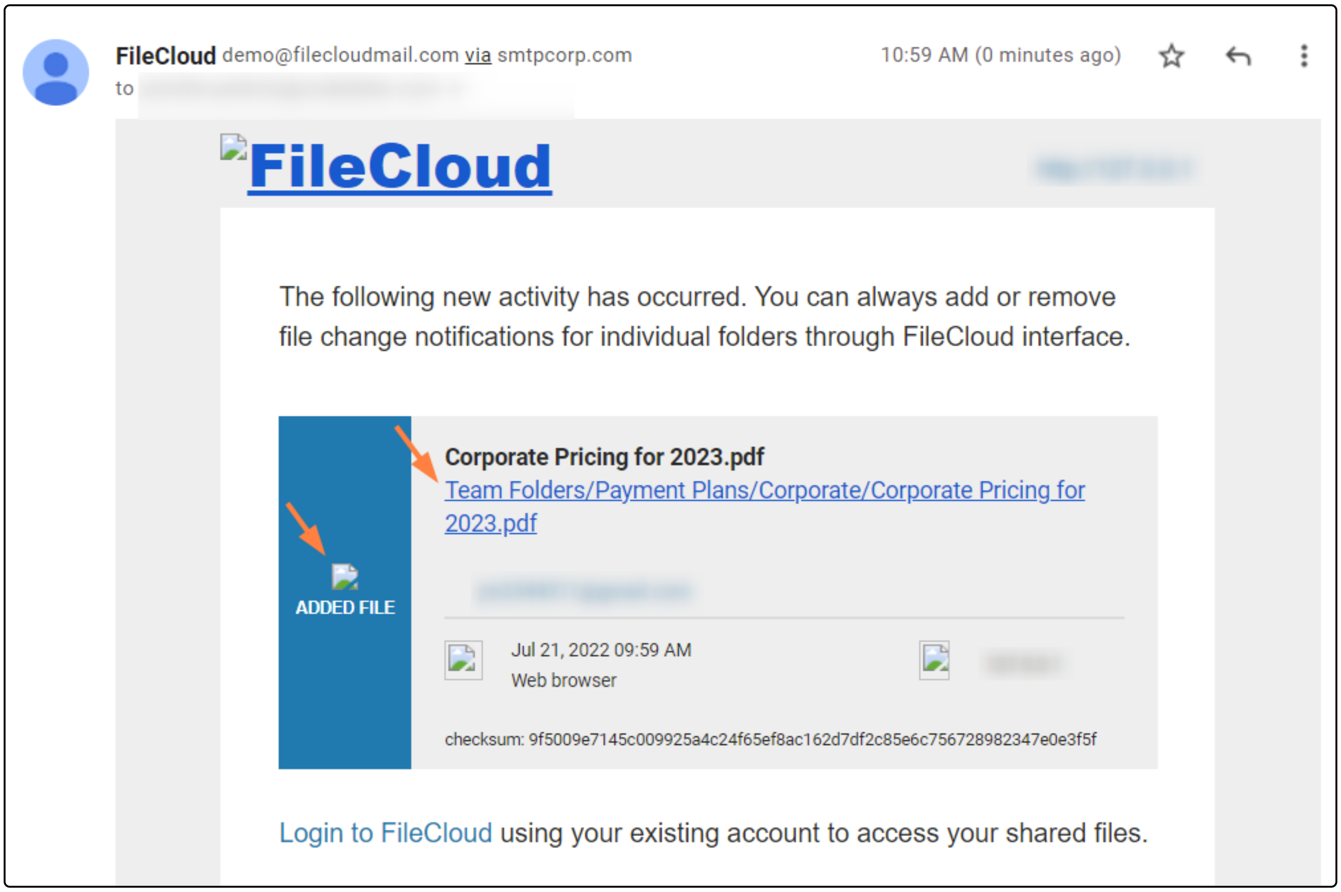
4. Check the actions that you want to be notified about in the folder (for example **Upload**, **Delete**, **Rename**, and **Update**).



5. Click **Save**.
6. Navigate to the **Product Offerings/Internet Only** folder, and repeat steps 2 through 5, above, to set notifications for the folder.

When content is changed in one of the folders:

If content is added to the **Corporate** or **Internet Only** Team Folder, the sales rep who set up notifications for those folders receives an email similar to the following:



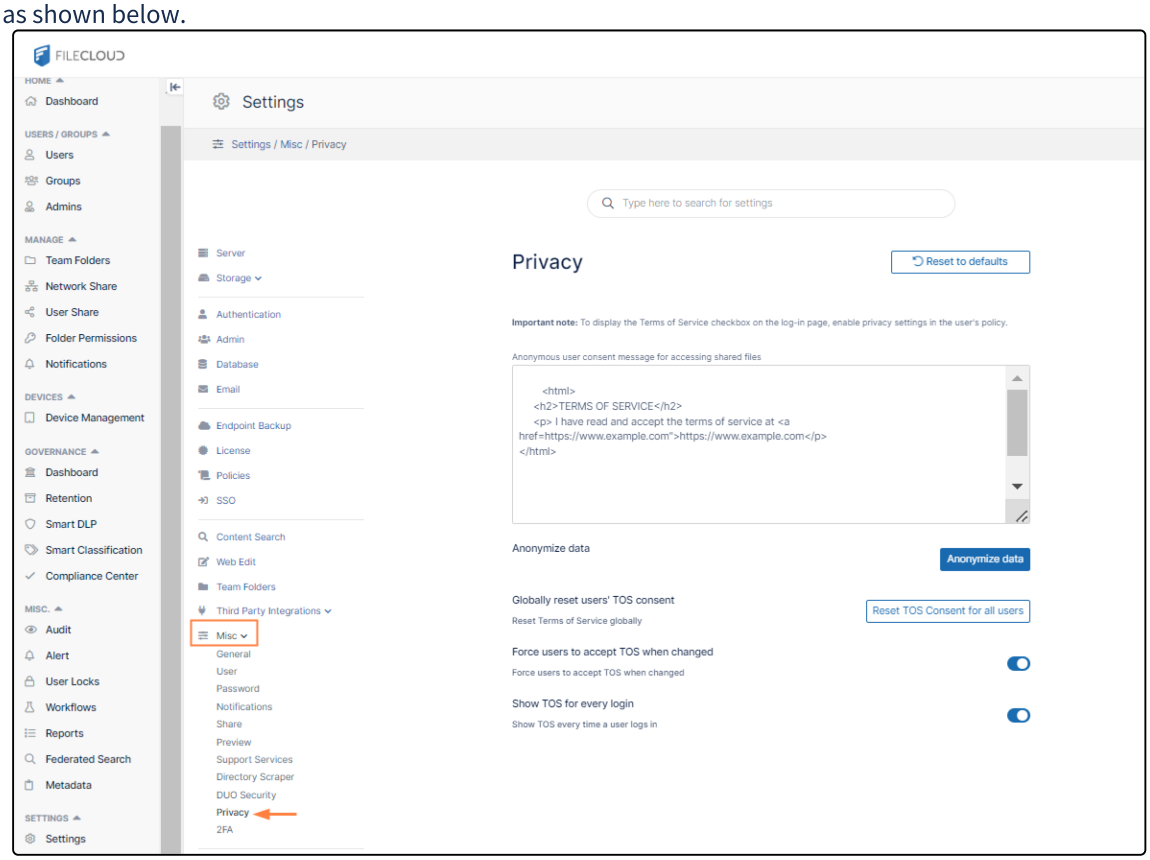
If content is modified in any of the other Team Folders, the sales rep does not receive notifications about them.

Anonymizing User Data

You can search for and replace specific names, emails, and IP addresses with a non-traceable ID in the activity logs.
This action cannot be undone.
The process does not make activity outside this FileCloud instance anonymous. This includes any backup system, web site logs, or database server logs. You must search and remove references from those separately.

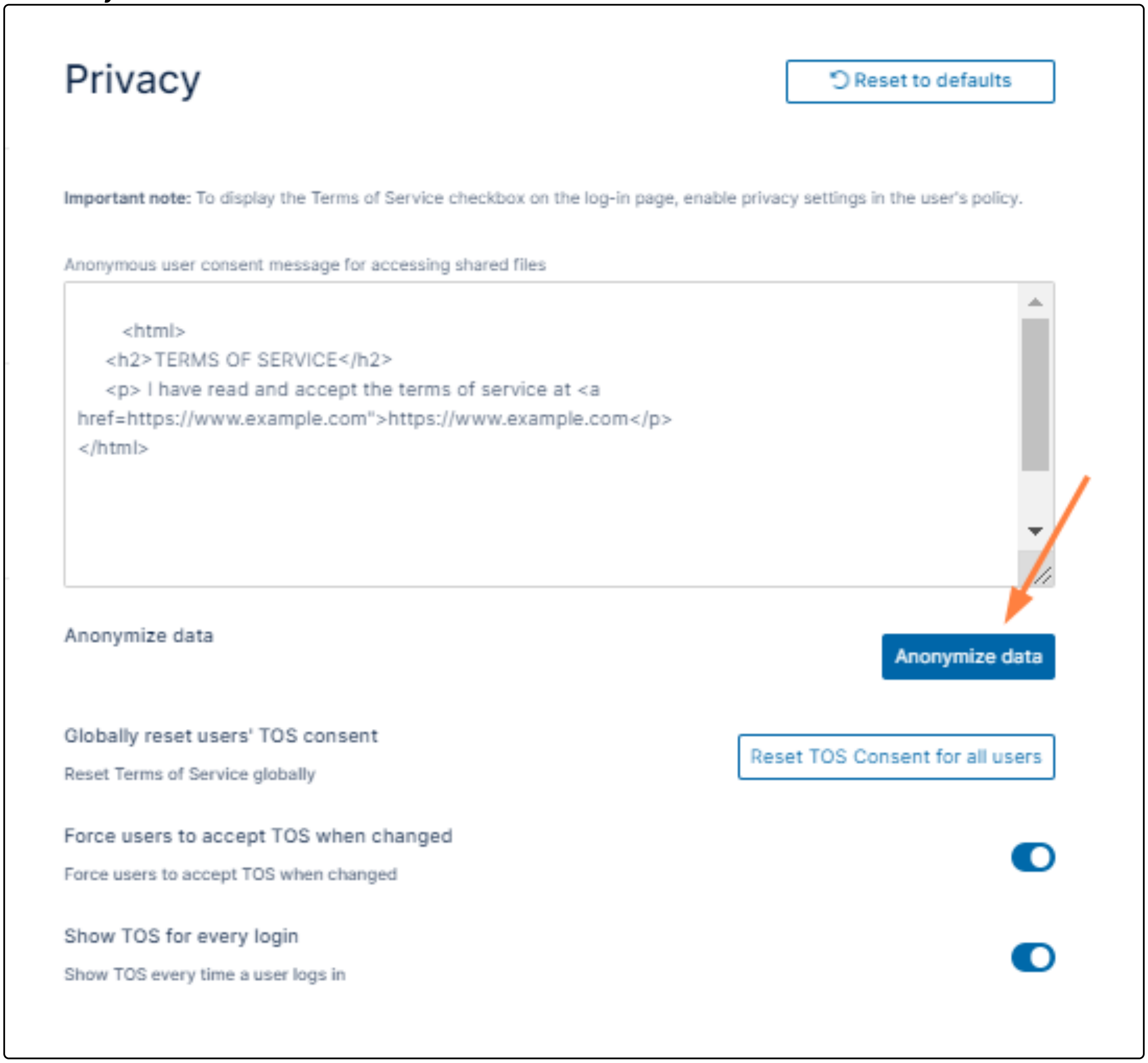
To anonymize user data:

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



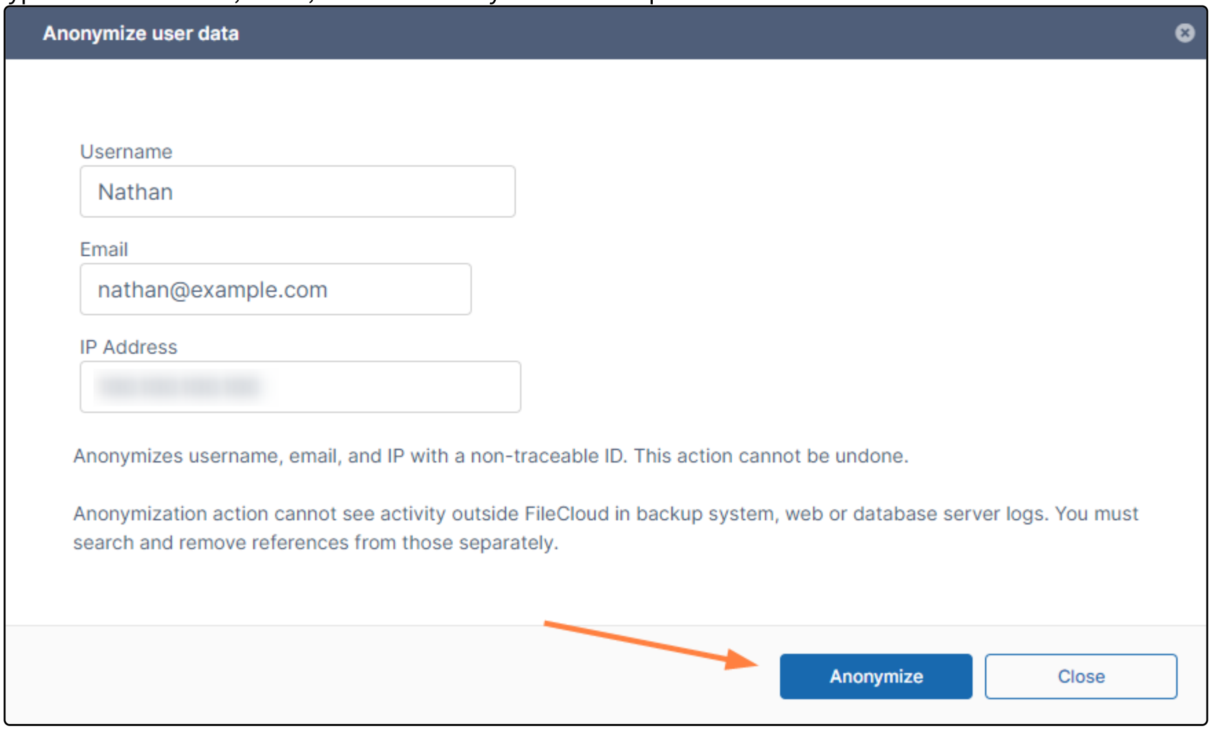
   The Privacy settings page opens.

2. Click **Anonymize data**.



The Anonymize user data dialog box opens.

3. Type in the username, email, and IP address you want to replace with a non-traceable ID.



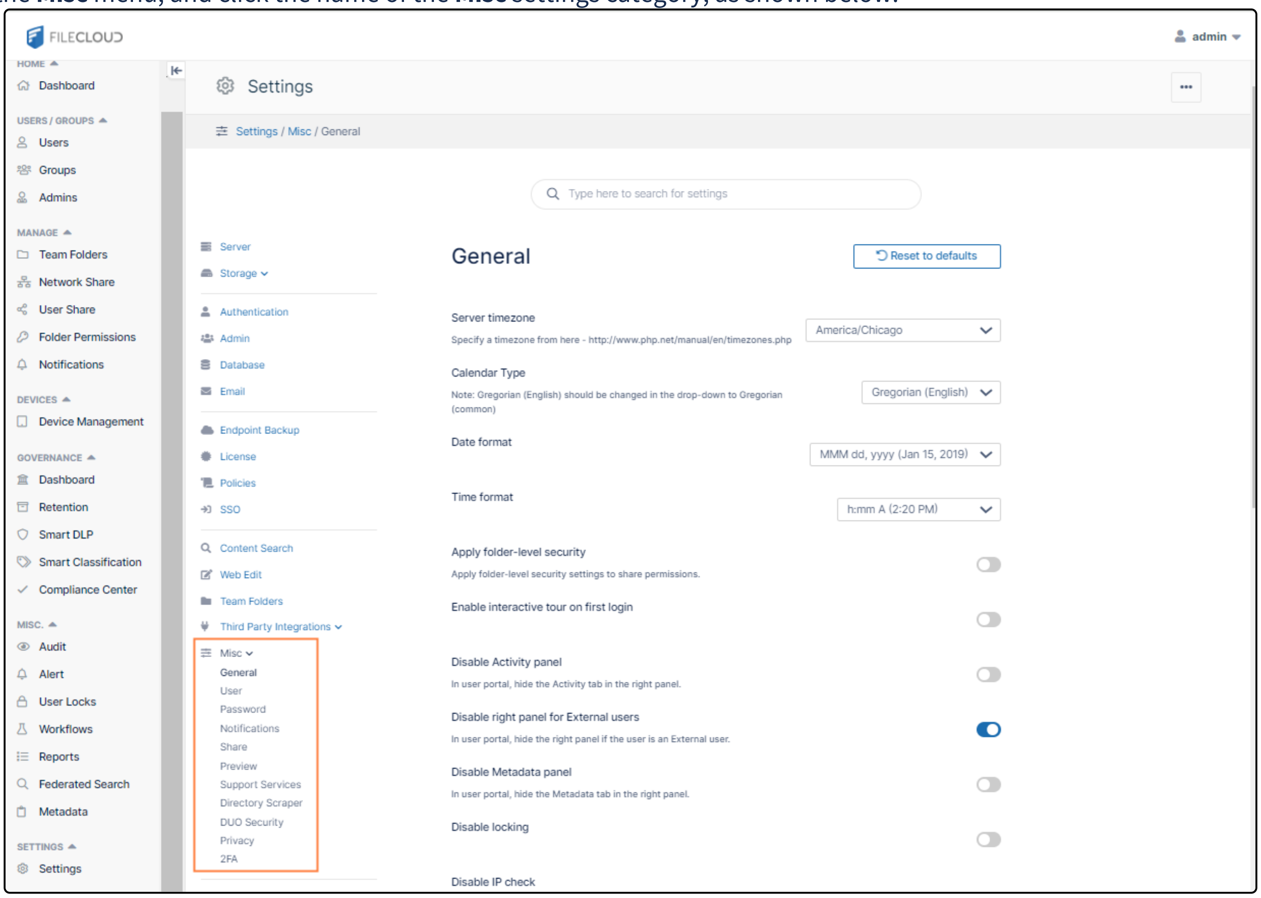
4. Click **Anonymize**.

Misc Settings

There are many ways to configure a FileCloud Server to work with your unique environment. Misc settings include many options for you to change default values.

To access the Misc settings:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .
   By default, **General** settings are opened.
2. To access other pages of **Misc** settings, in the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click the name of the **Misc** settings category, as shown below.



General settings

Setting	Tab	Description	Version Added
Server timezone	General	Sets the time zone for the server	

Setting	Tab	Description	Version Added
Calendar Type	General	Choose the format of the choices that appear in the following **Date format** and **Time format** drop-down lists. The **Calendar Type** chosen is used for dates in the user portal as well as the Drive client. It is not used in the admin portal. Options: • **Gregorian** (English, default)) - Show Western formats. • **Hijri** (Islamic) - Show Arabic formats.	FileCloud 22.1
Date format	General	Choose one of the options in the drop-down list. The options shown depend on whether **Gregorian** or **Hijri** is selected in the **Calendar Type** field. The **Date format** chosen is used for dates in the user portal as well as the Drive client. It is not used in the admin portal.	
Time format	General	Choose one of the options in the drop-down list. The options shown depend on whether **Gregorian** or **Hijri** is selected in the **Calendar Type** field. The **Time format** chosen is used in the user portal as well as the Drive client. It is not used in the admin portal.	
Apply folder-level security	General	Allow folder level security permissions to share.	
Enable interactive tour on first login	General	Displays interactive tour to users the first time they log in to the FileCloud user portal.	
Disable Activity panel	General	This setting hides the right panel that displays activities, comments, permissions and other details in the user interface. Note that activity records are not generated when this is enabled..	
Disable right panel for External users	General	Hides right panel if the user is a External user. Check by default.	
Disable Metadata panel	General	Hides metadata panel and disables metadata search option in user portal.	

Setting	Tab	Description	Version Added
Disable locking	General	Disables supports for file and folder locking. See File Locking for more information about locking files and folders.	
Disable IP check	General	Disables IP check on every request. Use if it is valid for IP addresses to change while users are using the system to avoid unwanted session termination.	
Email domain names to block	General	Enter the comma separated email domain names to block.	
Enable proxy settings	General	Enter the settings of a proxy network if needed.	
Scheduled tasks	General	Manually execute cron tasks.	
Import files	General	Import files to managed storage,	
Allowed file extensions	General	Specify file extensions that are allowed to be uploaded. Leave this empty to allow all file extensions except any specified in **Disallowed file extensions**.	
Disallowed file extensions	General	Specify file extensions that cannot be uploaded.	
Disallowed file names	General	Specify file names that cannot be uploaded.	
Check for double file extension	General	Include additional checks for double extensions to increase security.	
Forbidden Network Folder paths	General	Network Folder paths that are prohibited from being used	
Disable automatic database backup	General	Disables automatic database backup	
Database backup store path	General	Specify a writable path to store backed up database.	

Setting	Tab	Description	Version Added
Number of backups to store	General	Number of backups to maintain.	
Database backup Interval	General	Interval between backup process. 0 = daily backup.	
Disable content classification	General	Do not allow content classification.	
Enable WebDRM	General	Enable use of the Secure Web Viewer option.	

User settings

Setting	Tab	Description
User account search mode	User	See: Securing Shares by Limiting User Account Searches
User search account type	User	Restrict user searches so that your users can only search for users in certain account types. See User Search Account Type.
Group visibility	User	Control what groups are listed to a user when a private share is created by that user. By default, all user groups are shown, you can change that to only show groups that the user actually belongs to. This can prevent sharing of files inadvertently to large groups.
Send email to user to approve device	User	Send email to users when a new device is ready for approval.

Setting	Tab	Description
Default view settings	User	Select how files appear to users by default. (See: Viewing Files by List or Grid). The options are: (size varies depending on screen resolution) • **Automatic** - The default. Initially, **Automatic** is List view. Once the view is changed by the admin or by the user, **Automatic** is the user's most recent view. • **Large Thumbnails** - Grid of thumbnails that are approximately 400 by 400 pixels. • **Medium Thumbnails** - Grid of thumbnails that are approximately 280 by 280 pixels. • **Small Thumbnails** - Grid of thumbnails that are approximately 200 by 200 pixels. • **List View**
Allow users to modify their phone numbers	User	Allow full and external users to change their phone numbers in the user portal Settings screen.

Notifications settings

Setting	Tab	Description
Enable file change notifications	Notifications	When checked, enables recent activity notifications to appear on the user portal when files are created, updated, deleted and downloaded on a shared folder. Checked by default.
Enable email file change notifications	Notifications	When checked, enables the system to send Email notifications when files are created, updated, deleted and downloaded on a shared folder. Enable File Change Notifications must be checked for this setting to be enabled. Checked by default.
Disable notifications for External accounts	Notifications	When this option is enabled no share notifications will be sent to the external user.
Enable share notification	Notifications	When this option is enabled share notifications will be set to NO by default. The "Email FileChange Notifications" will be set to NO in Manage Share → advanced options.
Enable new version email notification	Notifications	When checked, emails about new versions of FileCloud are sent to the administrator once a week.

Setting	Tab	Description
Number of days to send notifications	Notifications	Send notifications for actions for the specified number of days
File change email frequency	Notifications	How frequently, in minutes, email notifications are sent. Beginning in FileCloud 23.241, the default frequency is 720 minutes (12 hours).

Other Misc. tab settings

For password settings, see Password Settings

For share settings, see Share Settings

For DUO security settings, see Two-Factor Authentication.

For privacy settings, see Terms of Service and Anonymizing User Data,

For 2fa settings, see Two-Factor Authentication

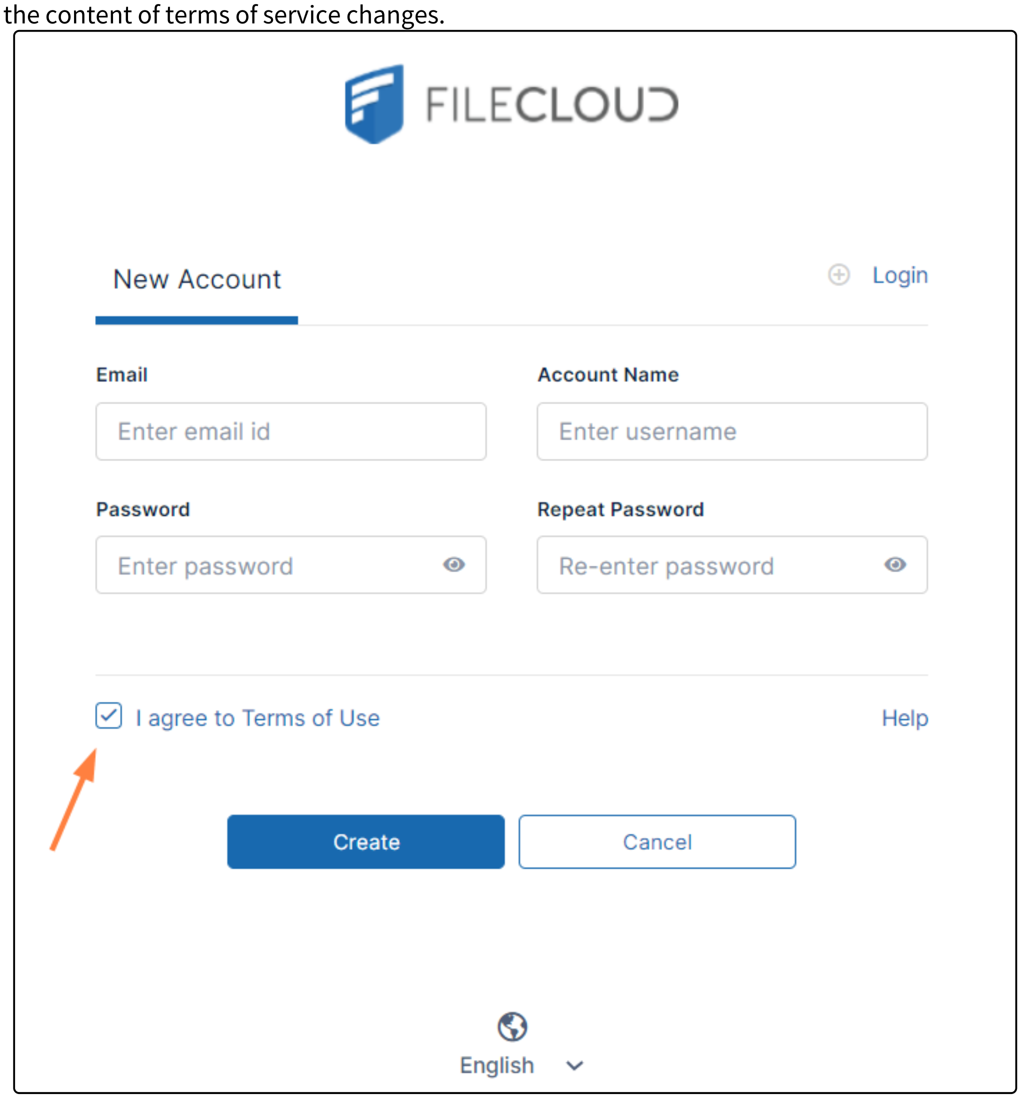
Terms of Service

Beginning with FileCloud Version 21.3, when **Enable Privacy Settings** is set to **yes** in their user policies, admin users are required to accept terms of service the first time they log into the admin portal.

Beginning with FileCloud Version 22.232, the default link to FileCloud terms of service has changed to https://www.filecloud.com/eula/. The link will only be changed automatically on new installations of FileCloud. Although the previous link will automatically redirect users to the new page, if you are upgrading FileCloud to version 23.232 or using an earlier version, we recommend that you change the link in **Customization > TOS** to https://www.filecloud.com/eula/

By default, FileCloud requires users to accept terms of service (TOS) when:

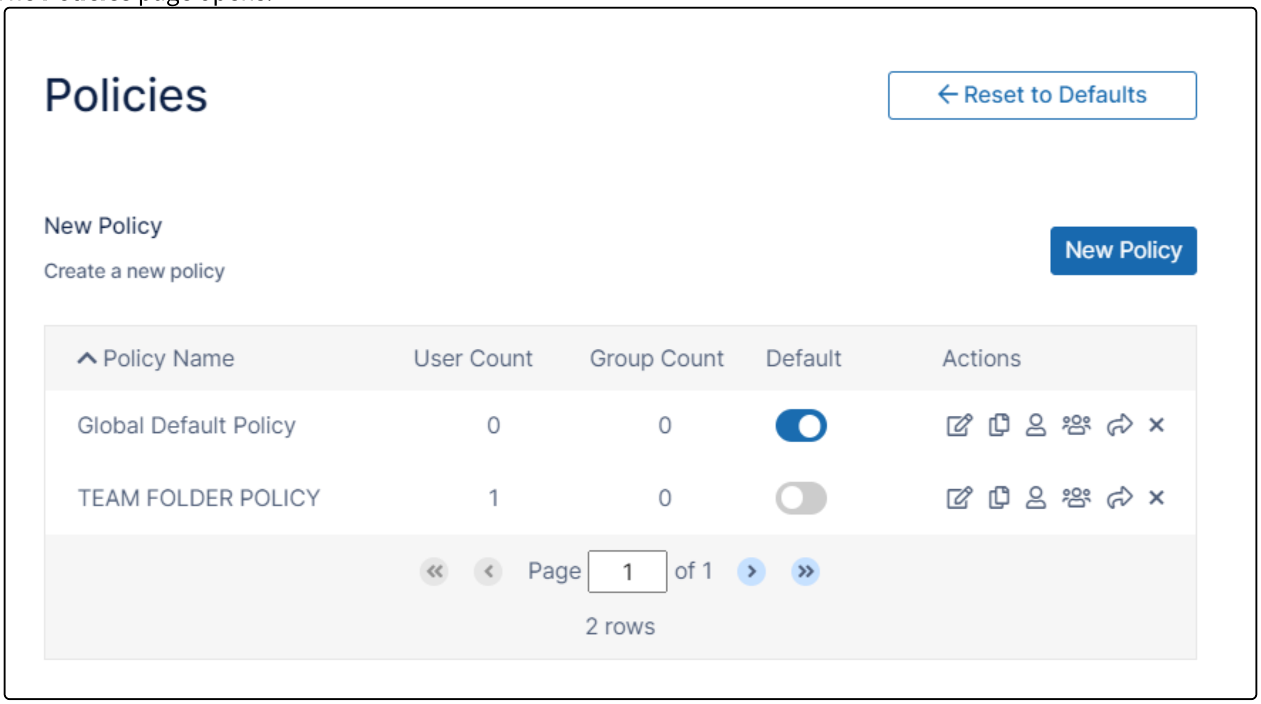
- they initially create an account
- the content of terms of service changes.



Enabling privacy settings and the Terms of Use checkbox

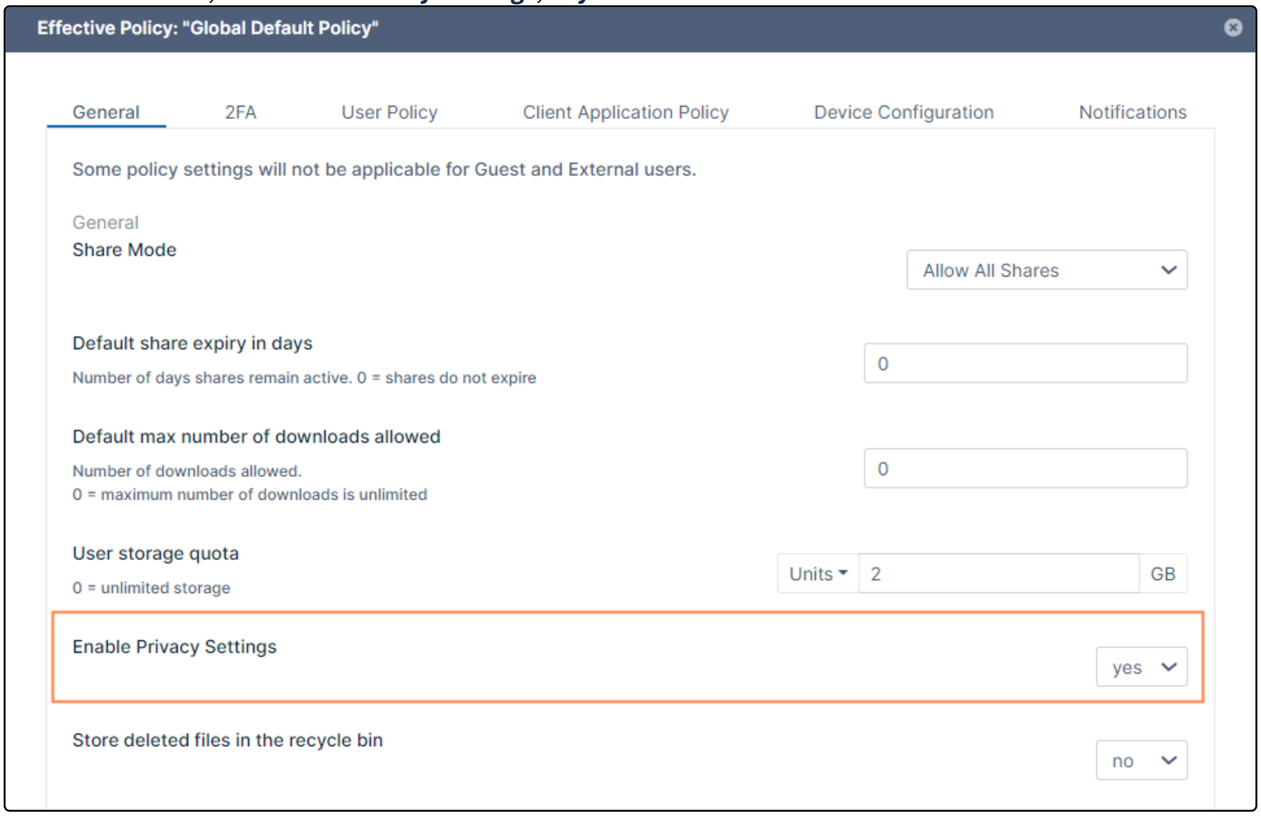
To display the **Terms of Use** checkbox on the log-in page, you must enable privacy settings. **Enable Privacy Settings** is set to **no** by default.

To enable privacy settings:

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

2. Edit the policy of the users whose privacy settings you want to modify.

3. On the **General** tab, set **Enable Privacy Settings**, to **yes**.



4. Click **Save**.

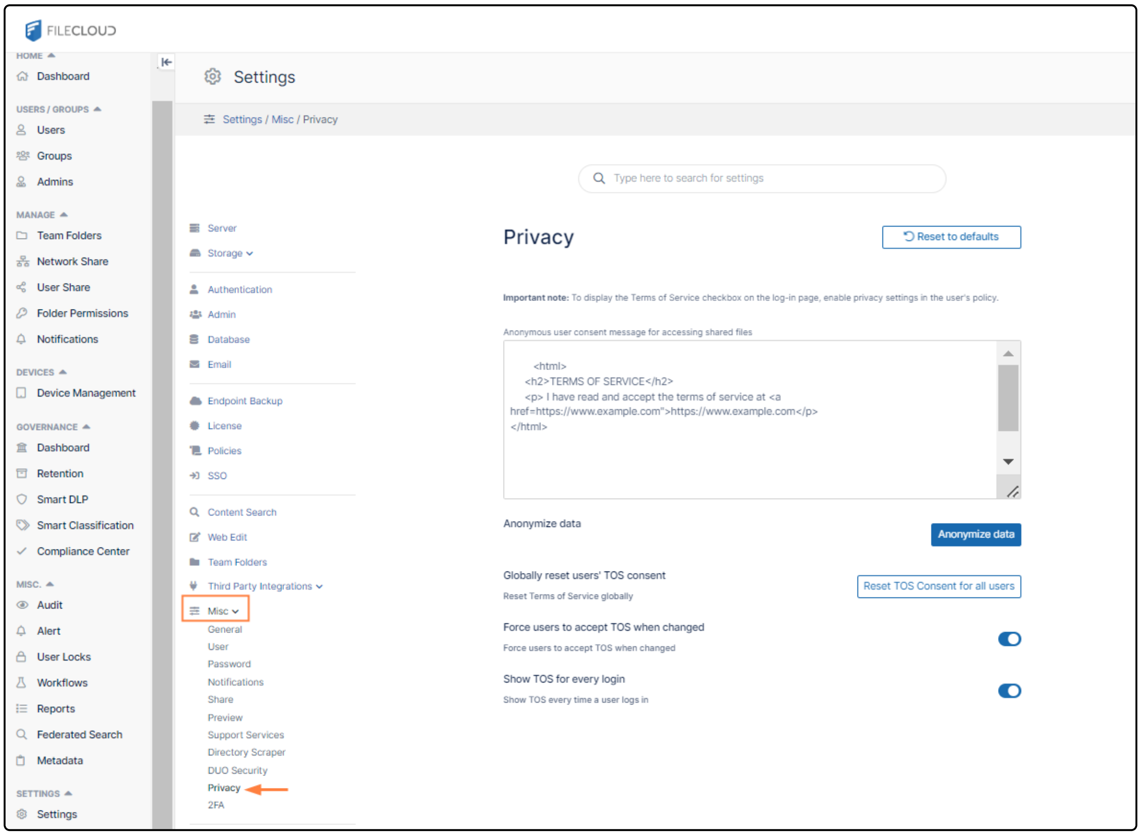
Showing TOS when users access public and password-protected shares

If **Enable Privacy Settings** in the General tab of a user's policy is set to **yes**, you can require users who log in to public and password-protected shares to accept FileCloud terms of service by adding text to the **Anonymous User Consent Dialog Text** field.

To require that a user accept of terms of service to access public and password-protected shares:

1. Set **Enable Privacy Settings** to **Yes** in the General tab of the user's policy as shown in the above procedure.
2. Open the **Privacy** settings page.
   To go to the Privacy settings page
      a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc**  .

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



The **Privacy** settings page opens.

3. Add the content that you want to appear with the **Accept Terms of Service** button when users attempt to access the link for a public or password-protected share:

4. Click **Save**.
   Note: If you do not enter text here, the **Accept Terms of Service** button is not shown when users enter the link for a public or password-protected share, and the share is opened directly.

Terms of service settings

Administrators are able to configure the following terms of service settings:

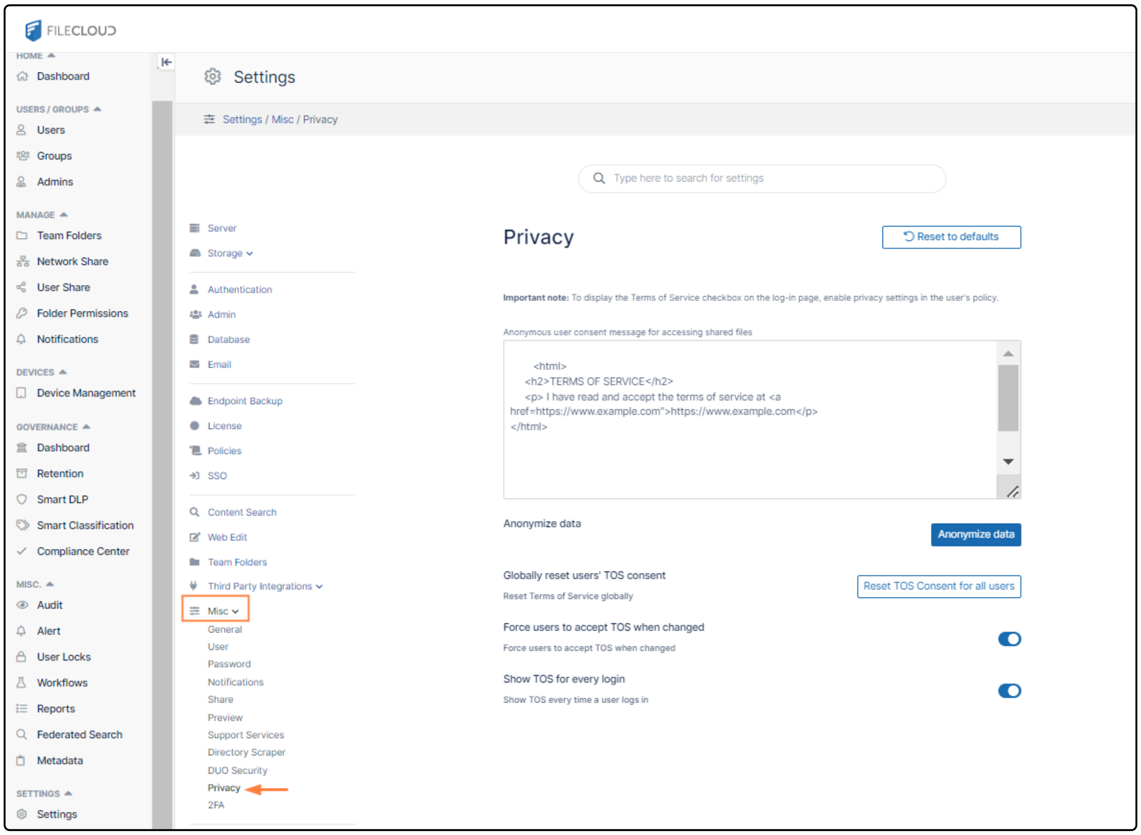
- Enable/disable whether users must re-accept terms of service when the content changes
- Enable/disable whether users must accept terms of service each time they log in to FileCloud
- Globally reset all users' terms of service consent

> In versions of FileCloud prior to version 20.2,
> the fields **Globally reset users' TOS consent**, **Force users to accept TOS when changed**, and **Show TOS for every login** appear in the **Customization > TOS** tab. Now these fields appear in the **Settings > Misc > Privacy** tab.

To configure terms of service settings:

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

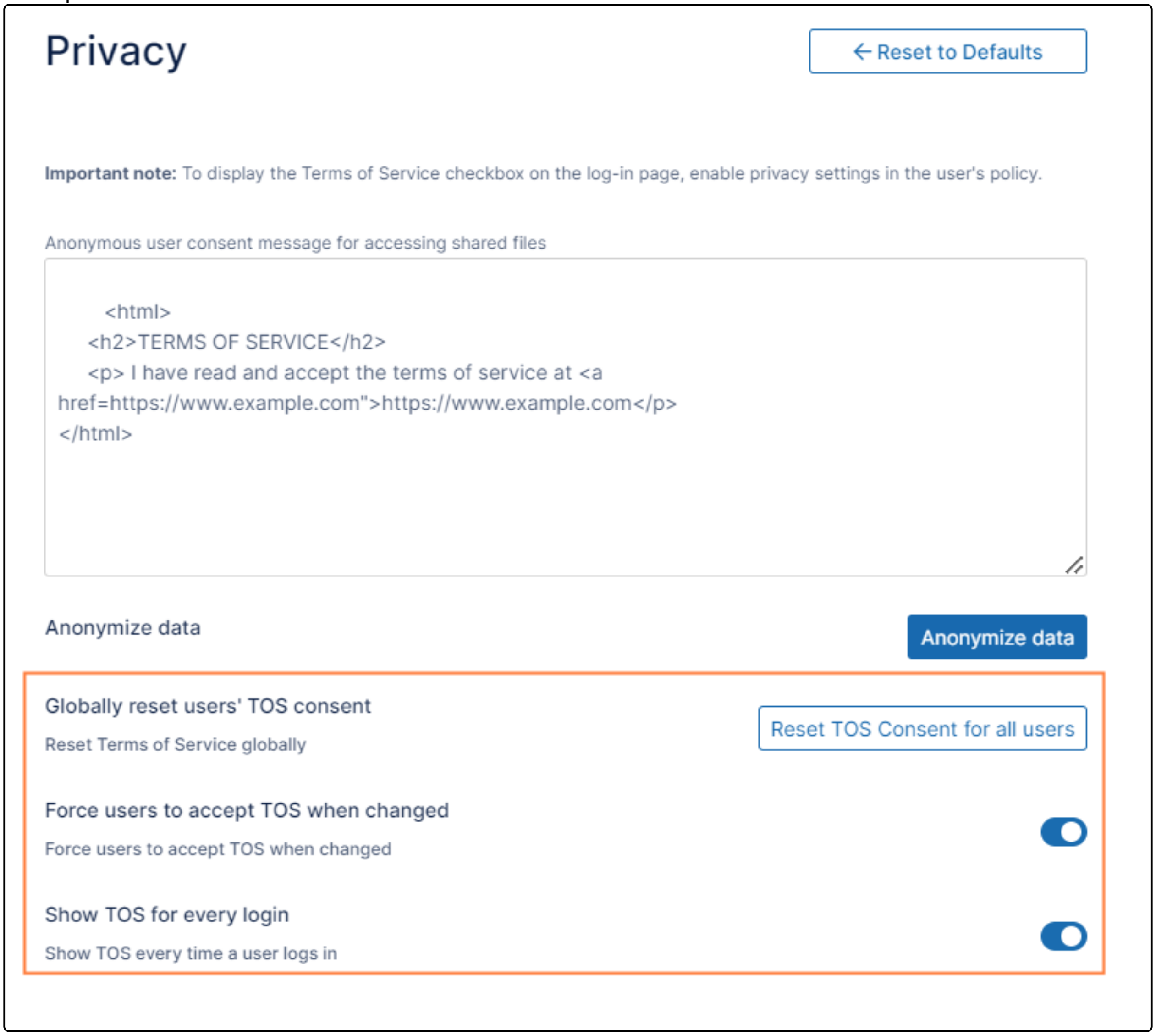
b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Privacy**, as shown below.



The **Privacy** settings page opens.

2. To globally reset TOS consent so that all users are required to re-accept the terms of service when they log in (to the user portal only), click **Reset TOS Consent for all users**
3. By default, **Force users to accept TOS when changed** is disabled.
   To require users to accept changed terms of service before logging in (to the user portal only), enable **Force users to accept TOS when changed**.
4. By default, **Show TOS for every login** is disabled.
   To require users to accept the TOS every time they log in, enable **Show TOS for every login**.
   This feature applies to all users when they sign in to the user portal and to admin users when they sign in to the

admin portal.

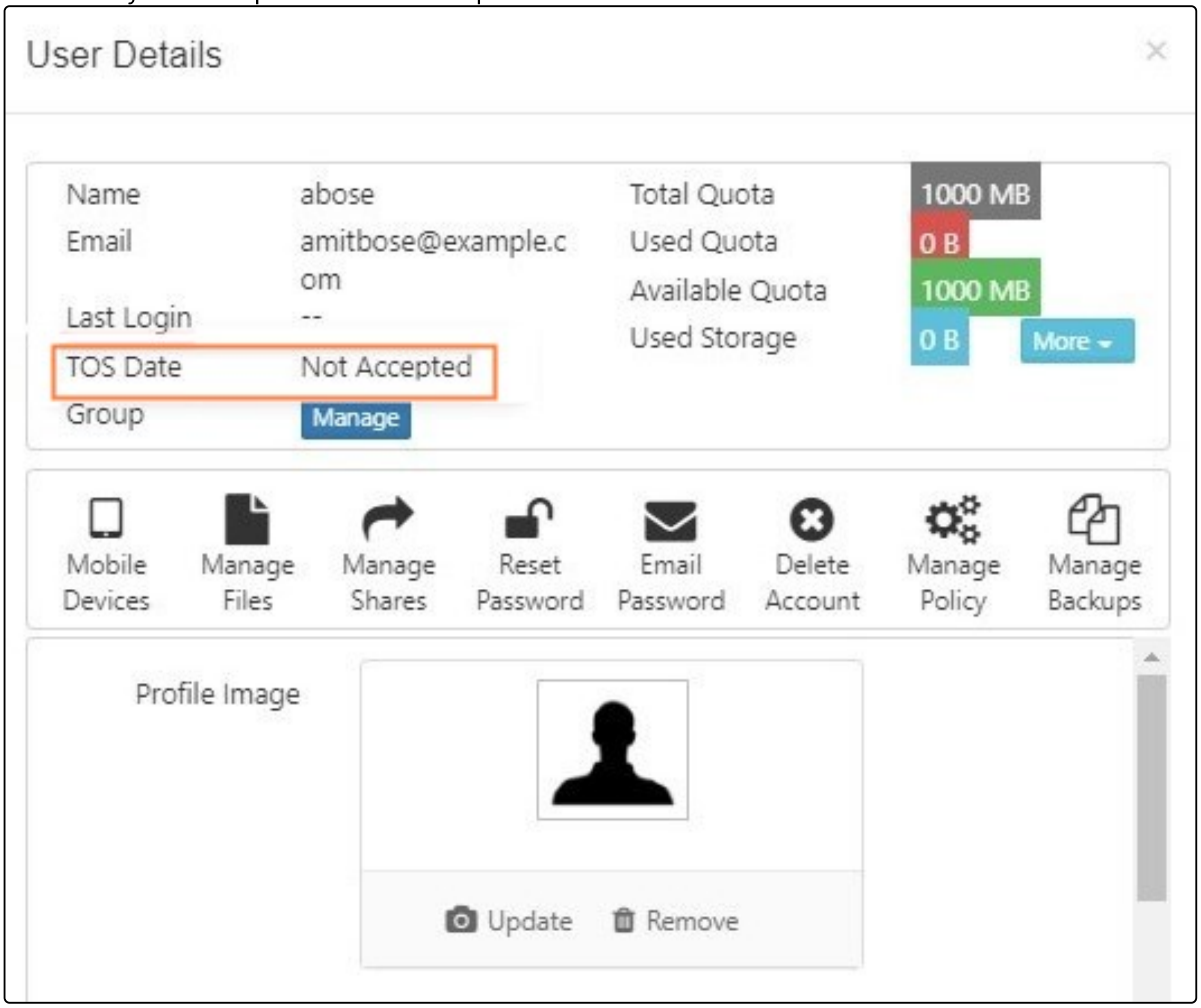


5. Click **Save**.

See if a user has accepted terms of service

Administrators can view the user details for a user to see if they have accepted the latest terms of service. **TOS Date** either displays the date that the user accepted the terms of service or displays **Not Accepted.**
Note: TOS Date only shows if admin users have accepted the latest terms of service for the user portal; it does not show

whether they have accepted it in the admin portal.

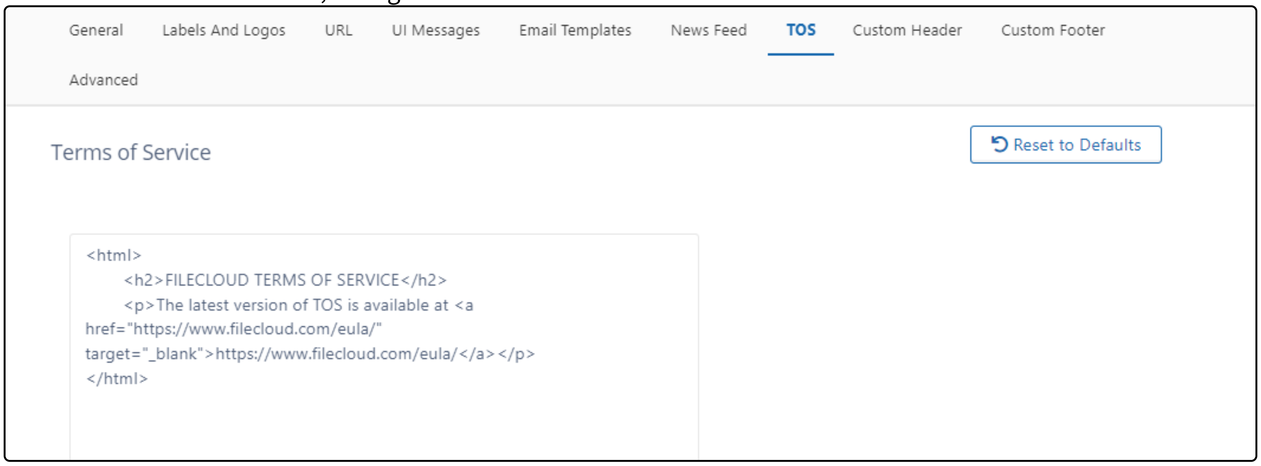


Change the content of the Terms of Service

To change the content of the Terms of Service:

1. Click **Customization** in the left navigation panel.
2. Click the **TOS** tab

3. To enter new terms of service, change the HTML code in **Terms of Service**.

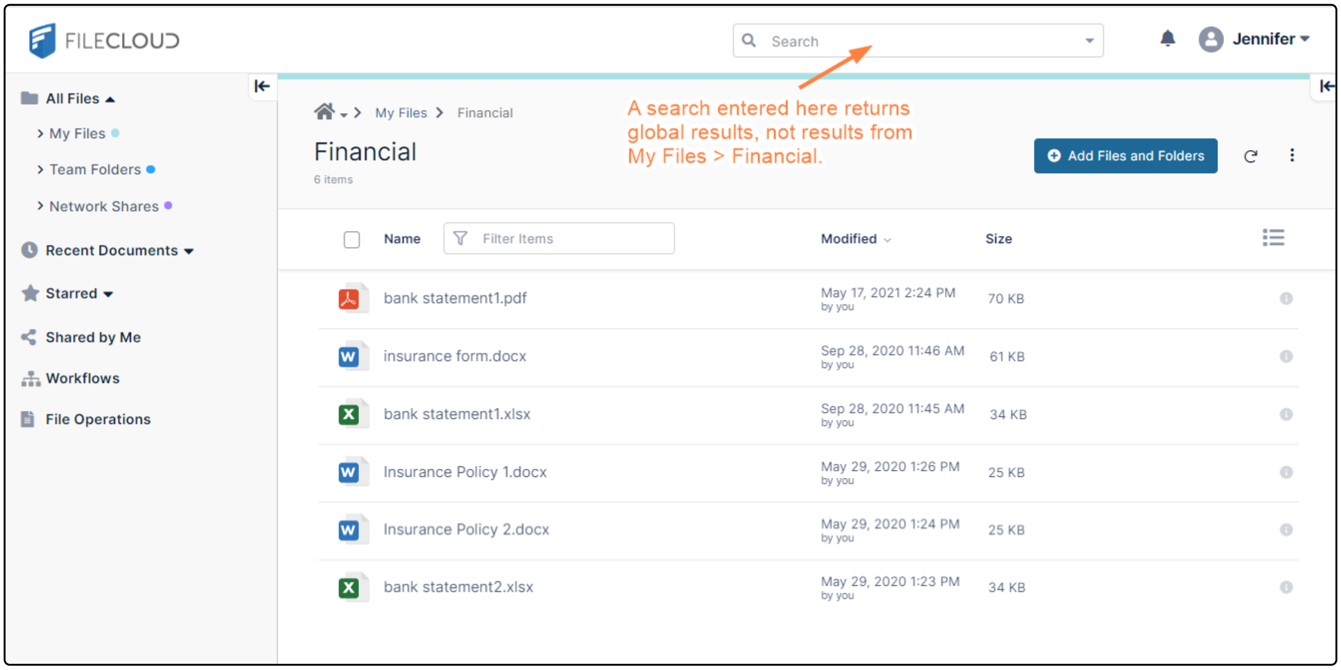


Note: This text is not shown when users open a public or password-protected share; instead the text in **Anonymous user consent message for accessing shared files** in **Privacy settings** page, if it is entered, is shown.

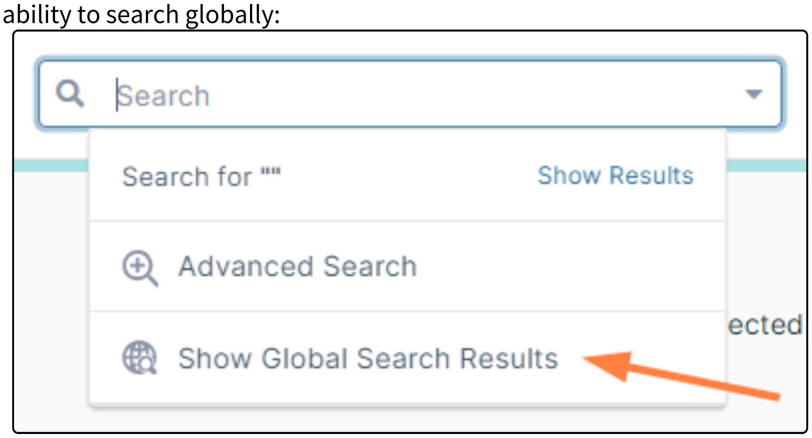
4. Click **Save**.

Set Search Location

By default, basic searches from the user portal header's search bar are performed globally, regardless of where the user has navigated in the folders shown in the main part of the screen.



A setting is available for changing the default search location to the current path shown in the user portal. In the above screen, if the setting were turned on, searches would begin at the **My Files/Financial** folder.
The setting adds the option **Show Global Search Results** when users click in the Search bar so users still have the ability to search globally:



To set the search to begin from the current path but include the global search option, please Contact FileCloud Support.