



FileCloud Online Version 23.232

Site Setup

Copyright Notice

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

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

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

Copyright Notice	2
Administrator Settings.....	9
Logging In	9
Resetting Admin Password	12
Changing the Default Login Name	17
Account Locked Alerts	18
Basic Settings	20
Basic Settings Checklist	20
Set the Language	22
Storage Settings.....	24
FileCloud Managed Storage	24
Enable Folder-Level Permissions	38
To enable users to set folder-level permissions:	38
Example scenarios	44
How a user sets folder permissions	51
Permission inheritance	53
Permission hierarchy	53
Set Granular Permissions on Team Folders.....	54
Team Folders.....	65
Configure the Team Folders Account.....	66
Seed and Organize Team Folder Data.....	75
Share the Team Folder and Set Permissions.....	79
Search for a Team Folder.....	83
Recover Deleted Files.....	84
View and Restore Previous Versions in Team Folders.....	86
User Settings	88
Create FileCloud Users.....	89

New Account Creation	102
Password Settings.....	133
Restrict Commonly Used Passwords	139
User Session Expiration	140
Changing the Storage Quota for Users	141
Enable WebDAV	146
Customize the User Login Screen	146
Limiting File Upload Size for Users	152
Remove the Export Secure Doc Option.....	154
Group Settings	156
What do you want to do?	156
Giving Users Group Management Permissions	163
Admin User and Role Settings	166
User Authentication Settings	173
Enabling Default Authentication	173
Active Directory Authentication	174
Single sign-on (SSO).....	194
LDAP Based Authentication.....	293
Oracle Identity Manager LDAP integration with FileCloud	301
Desktop Apps Code-Based Authentication.....	306
Document Settings	312
Enabling Watermarks On Previews	312
Import Files : Pre-seeding.....	315
Optimize PDF Preview.....	318
Managing File Extensions	320
Restricting File Names	323
Manage File Versioning	325
Configuring Zip Files and Zero Trust File Sharing	326
Share Settings	330
Configure Sharing Defaults.....	330

Set the Global Share Mode	340
Specify Sharing Expiration	342
Secure Shares.....	346
Email Settings	356
SMTP Configuration	360
Do Not Email Settings	364
Configuring System Generated Emails	366
Endpoint Backup Settings.....	367
What Do You Want To Do?	367
Automatic Database Backup	370
Setting Up Persona Backup Using Sync.....	372
Client Security Settings.....	376
Two Factor Authentication	376
Setting Client Application Policies	390
Using a Proxy Server	396
Online Web Editing.....	398
Web Editing with Google Apps	398
New Document Creation via Web Browser	408
Web Editing Text Files.....	411
Web Editing Markdown and Readme Files	411
Coauthoring Office Documents Using Web Edit	412
Disable Online Web Editing	413
Policies.....	414
Working with Policy Records	418
Notifications for File Changes	423
FAQ's	423
Changing notification settings	426
Example Setup: Fixed Notifications for Uploads and Deletions	434
Example Setup: User-enabled Notifications on Folders	437
The Misc. Tab Settings	444

General settings	444
User settings	446
Notifications settings	447
Other Misc. tab settings	448
Terms of Service	449
Enabling privacy settings and the Terms of Use checkbox.....	450
Showing TOS when users access public and password-protected shares	451
Terms of service settings	451
See if a user has accepted terms of service	452
Change the content of the Terms of Service.....	453
Set Search Location	455
Migrating data to FileCloud using Rclone	456
Requirements.....	456
Creating a FileCloud WebDav Configuration in Rclone	456
Testing your configuration and connectivity using Rclone.	459
Migrating (Move/Copy/Sync) Data from other solutions to FileCloud.	460
Things to consider when using Rclone to migrate your data to FileCloud.	460
Additional FileCloud Configurations.....	460

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.

i Beginning in FileCloud 20.1, the option for reverting to default values for all options in the Settings and Customization sections of the admin user interface is located in the [Settings > Reset tab](#). In earlier versions of FileCloud, the option appears in the upper-right corner of all Settings and Customization pages.

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Required	<p>Access the Admin Portal</p> <p>Admin Portal Dashboard</p> <p>Change the Admin Password</p> <p>Manage Account Approvals</p>	<p>Admin Settings video: Admin Settings</p> <p>Basic Settings video: Main Settings</p> <p>Manage Client Security Settings</p> <p>Configure Share Settings</p>	<p>Configure Team Folders video: Team Folders</p>	<p>Create FileCloud Users video: Creating Users</p> <p>Check User Access Level video: Managing Users</p> <p>Create User Policies video: Policy Overview video: Policy, General Tab video: Policy, User Policy Tab</p> <p>Create Groups video: Managing Groups</p> <p>Manage User Storage Quotas</p>
Recommended	<p>Configure Email Settings video: Email Settings</p>	<p>Set Client Application Policies video: Policy, Client Application Policy Tab</p>		<p>Manage User Authentication</p> <ul style="list-style-type: none"> • Configure Single Sign On video: SSO • Use LDAP Based Authentication video: LDAP Authentication • Active Directory Authentication video: AD Authentication <p>Set Up 2FA</p> <p>Configure Microsoft Office Integration Options</p>

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Provides a Better Experience	Add Customization and Branding			Enable MS Teams Integration Enable Salesforce Integration Set Up Notifications for File Changes Automate Business Workflows Enable Folder-Level Permissions Enable reCaptcha video: reCaptcha Integration
Advanced features	Set Up Compliance Checking <ul style="list-style-type: none"> • HIPAA • ITAR • GDPR • PDPL • NIST 	Set Up Data Governance		

See additional [Video Tutorials](#) for help setting up your site.

Administrator Settings

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

- [Logging In](#)
- [Resetting Admin Password](#)
- [Changing the Default Login Name](#)
- [Account Locked Alerts](#)

Logging In

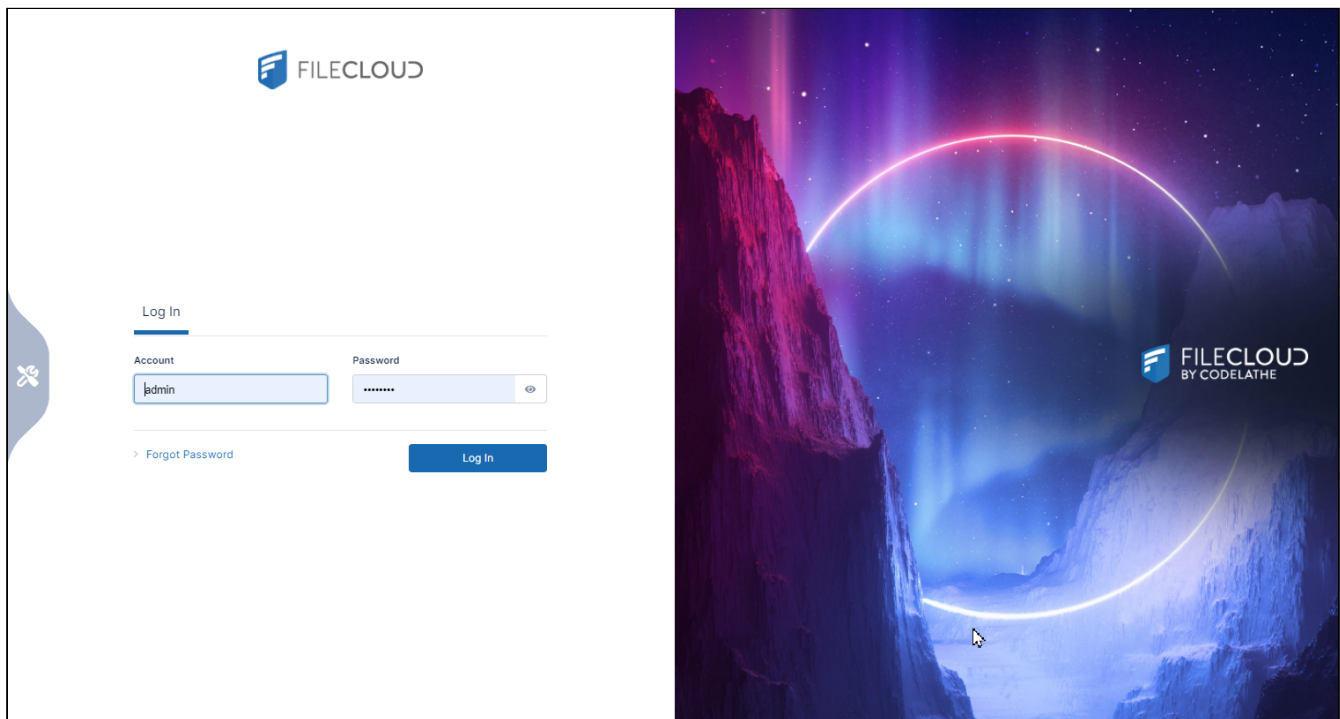
Log in using your admin account to perform administrative tasks.

Accessing the Admin Portal

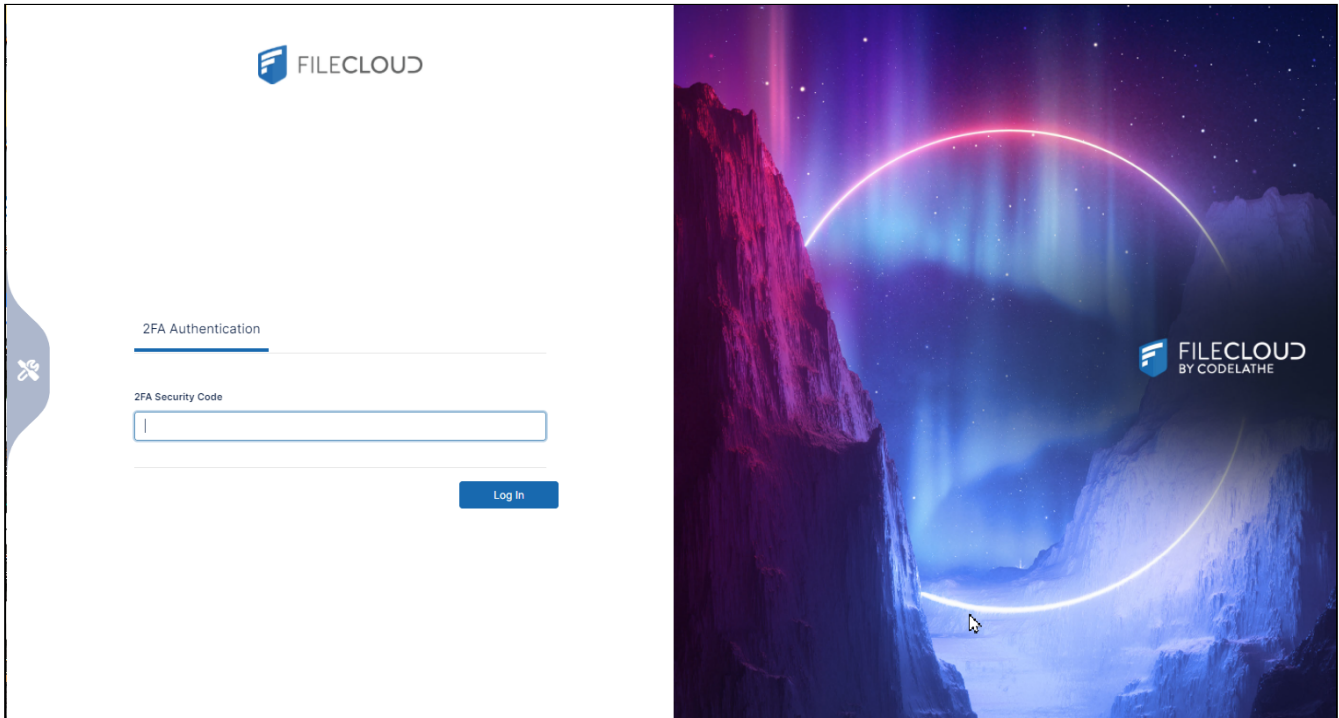
In a supported web browser, type in the URL to your Administrator dashboard. For example, <https://<yourteamname>.filecloudonline.com/admin>

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.



If [two factor authentication for administrators](#) is enabled, then you are required to provide a security code to continue.



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:


FileCloud Respects Your Privacy

FileCloud Respects Your Privacy

When you entrust your data to FileCloud, you remain the owner of the data.

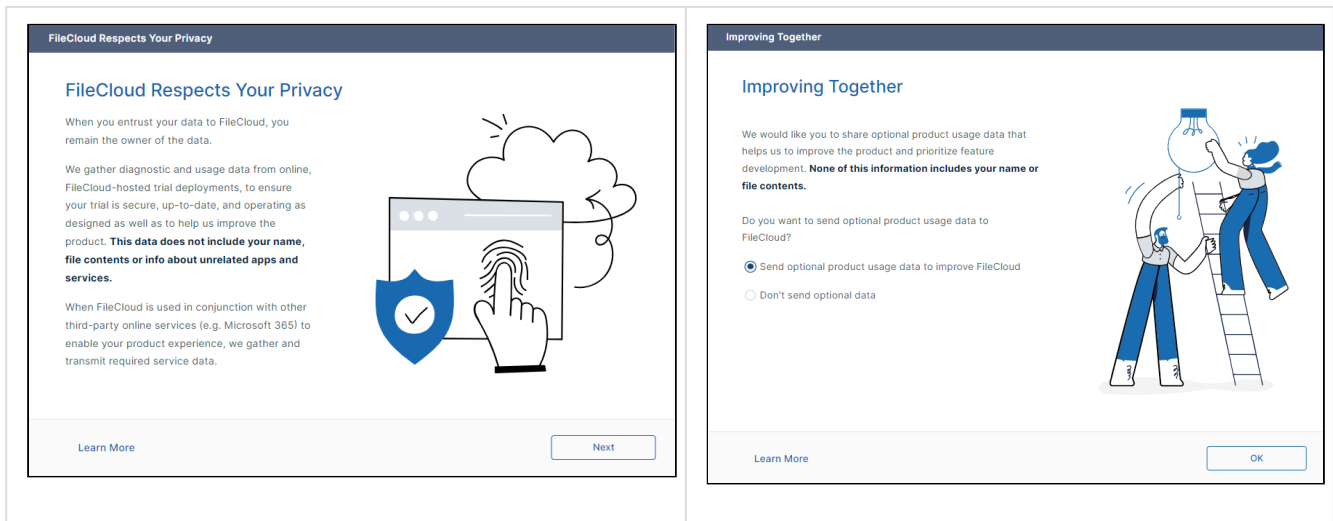
We gather diagnostic and usage data from online, FileCloud-hosted trial deployments, to ensure your trial is secure, up-to-date, and operating as designed as well as to help us improve the product. **This data does not include your name, file contents or info about unrelated apps and services.**

When FileCloud is used in conjunction with other third-party online services (e.g. Microsoft 365) to enable your product experience, we gather and transmit required service data.



[Learn More](#)

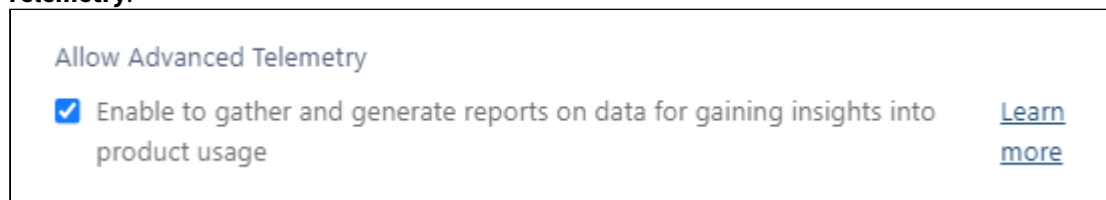
Once you convert from from an online trial license to an online product license, the first time you log in to the the admin portal a wizard opens with the following two screens:



To allow sending of optional product usage data to FileCloud, leave **Send optional product usage data to improve FileCloud** selected, and click **OK**.

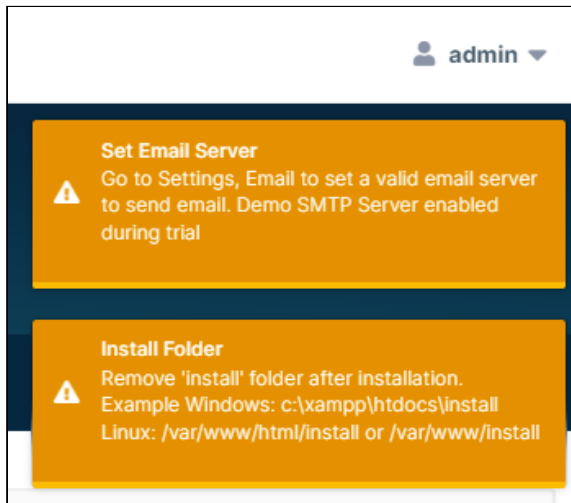
To prevent sending of optional product usage data to FileCloud, select **Don't send optional data**, and click **OK**.

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



Viewing and Clearing Checklist Notifications

Each time you log in, you are alerted of any system set-up recommendations that you skipped:



To avoid seeing the alerts again, correct the settings. To clear an alert for this session, click on it. To clear all alerts for this session, click Escape.

Customizing the Login Page

To customize the image on the admin login screen, see [Themes, Labels, and Logos](#).

Resetting Admin Password

i Starting with FileCloud 18.1, administrators can reset the admin password via the Web UI.

w 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

1. Click **Settings** in the navigation panel.
2. Click the **Admin** tab

3. Click **Reset Admin Password**.

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

Misc Reset

Admin Settings

Admin Login Name
Change the built-in admin user name

Admin Email
Email id for admin account.

Enable Two Factor Authentication For Admin Logins
Enable Two Factor Authentication for Admin user logins. Requires valid email id.

Reset Master Admin User Password
Reset Master Admin Password

Stats API Key
API Key for getting stats

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

Reset Master Admin Password

Current Master Admin Password

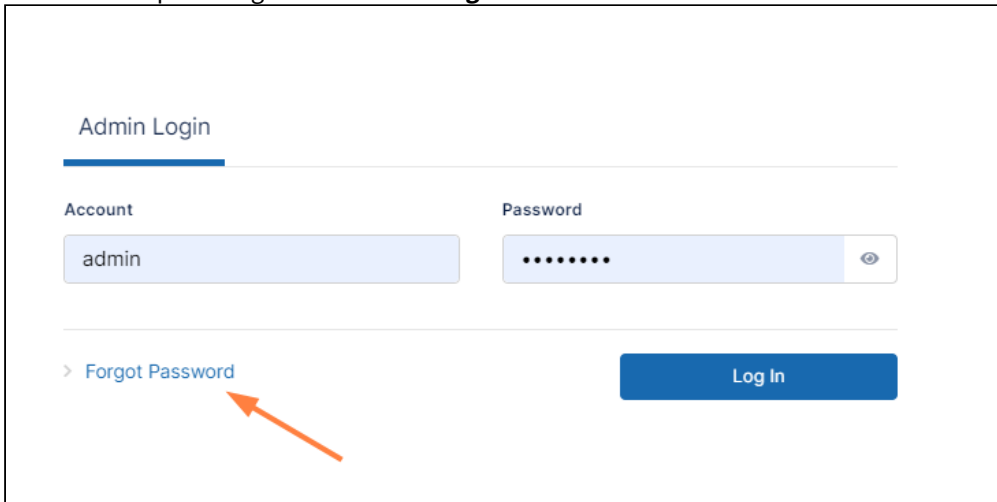
New Master Admin Password

Confirm New Master Admin Password

4. Enter the current and new password values, and click **Reset Password**.

Reset a forgotten admin password on the login screen

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

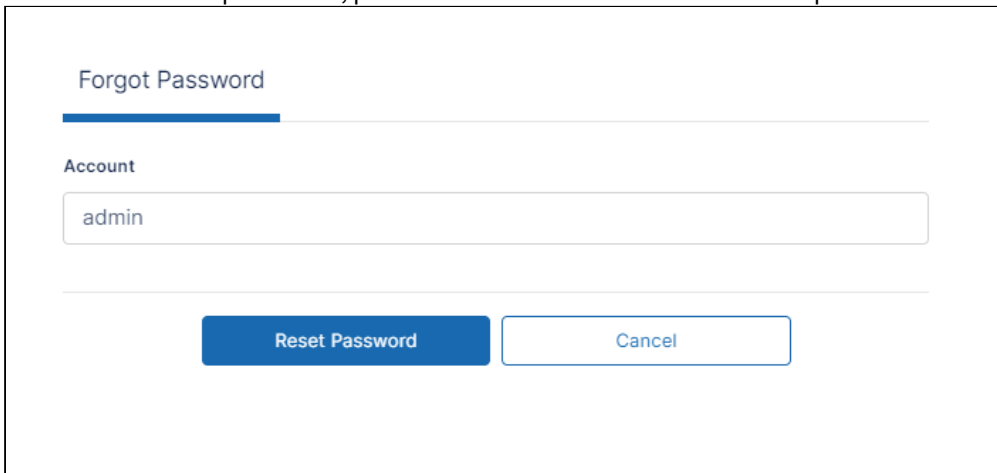


The screenshot shows the 'Admin Login' interface. At the top, the title 'Admin Login' is underlined. Below it are two input fields: 'Account' containing the text 'admin' and 'Password' containing a masked password (represented by dots). To the right of the password field is an eye icon for toggling visibility. Below the input fields, there is a blue button labeled 'Log In' and a link labeled '> Forgot Password'. An orange arrow points to the 'Forgot Password' link.

A dialog box prompts you to enter your user account.

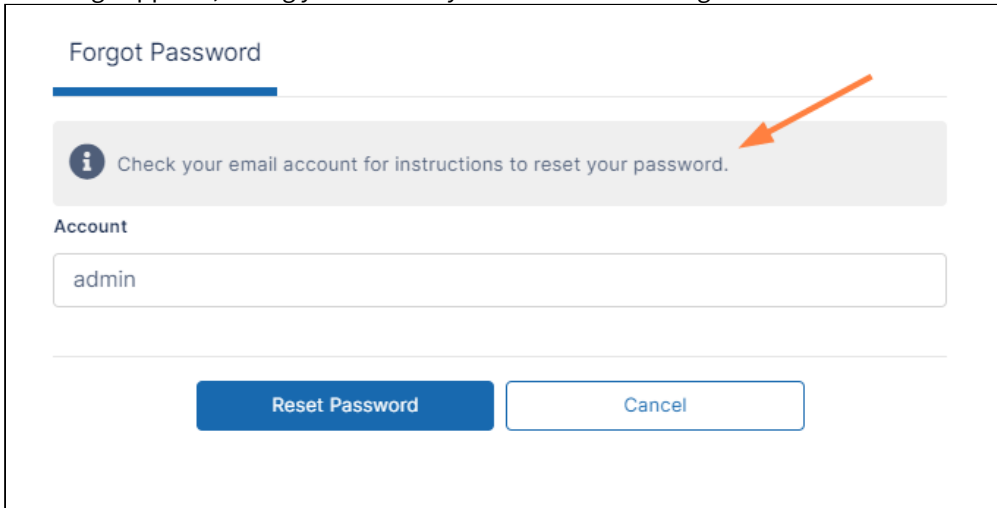
2. Enter your admin account name, and click **Reset Password**.

Note: To reset their passwords, promoted admin users must use the user portal.



The screenshot shows a 'Forgot Password' dialog box. The title 'Forgot Password' is underlined. Below it is an 'Account' input field containing the text 'admin'. At the bottom of the dialog, there are two buttons: a blue button labeled 'Reset Password' and a white button with a blue border labeled 'Cancel'.

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



Forgot Password

i Check your email account for instructions to reset your password.

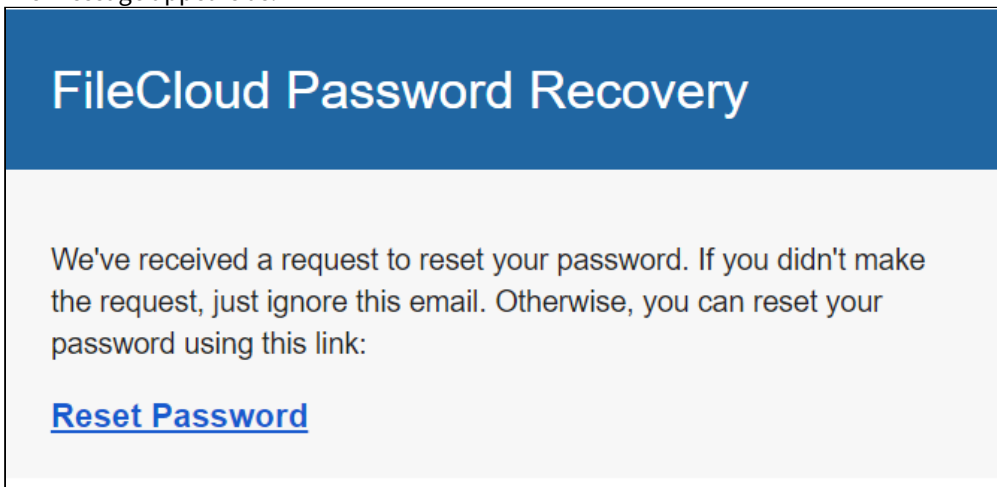
Account

admin

Reset Password Cancel

3. Find and open the message in your email.

The message appears as:



4. Click **Reset Password**.

The following dialog box opens:

The screenshot shows a dialog box titled "Reset your password" with the FileCloud logo. It contains two input fields: "Password" and "Confirm Password", both with masked text (*****). Below the fields are two buttons: "Reset Password" (highlighted in blue) and "Cancel". At the bottom, it says "Powered by FileCloud".

5. In **Password**, enter your new password. In **Confirm Password** enter it again.

6. Click **Reset Password**.

Your password is reset.

Reset the Admin Password from the SuperAdmin UI

Starting with the 17.3 version it is now possible to reset the Admin Password for each site directly from the SuperAdmin UI.

1. Log in to the admin portal with the Super Admin credentials
2. Navigate to **Site Settings**
3. Reset the Admin Password

For more information please visit the [Multi-Tenancy Settings Page](#).

Reset the Admin Password Using the FileCloud Control Panel

The password can also be reset to **password** using the FileCloud control panel.

FileCloud Control Panel
v: 20.3.2.13176, Base Components: 20.3.1.13094
Webserver Ports: 80,443 Database Port: 27017

Initial Setup: [Install Check](#)

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

Servers

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

Optional

FileCloud Helper:	Running SVC	Start	Stop	Install	Config
Memcache:	Running SVC	Start	Stop	Make Service	
Document Preview:	Running SVC	Start	Stop	Install	
Content Search:	Running SVC	Start	Stop	Install	

Miscellaneous

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

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

Technical Support

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

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. Log into the Administrator portal.

2. Select **Settings** in the left hand navigation menu.
3. Select **Admin** tab.

The screenshot shows the 'Admin Settings' page with the following fields and options:

- Admin Login Name:** Text box containing 'admin'. Below it: 'Change the built-in admin user name'.
- Admin Email:** Text box containing 'jessica@example.com'. Below it: 'Email id for admin account.'
- Enable Two Factor Authentication For Admin Logins:** A checkbox that is currently unchecked. Below it: 'Enable Two Factor Authentication for Admin user logins. Requires valid email id.'
- Reset Master Admin User Password:** A blue button labeled 'Reset Admin Password'. Below it: 'Reset Master Admin Password'.
- Stats API Key:** A text box containing masked characters (dots). Below it: 'API Key for getting stats'.

4. Change the value in **Admin Login Name** text box.
The name can only contain letters, numbers, spaces, hyphens, underscores and periods. It cannot be the same as the superadmin name.
5. 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:

The screenshot shows a login page with the following elements:

- Header:** "Login" on the left and "+ New Account" on the right.
- Error Message:** A red box with a warning icon containing the text: "Invalid Username or Password. Password is Case Sensitive. Your account has been locked due to 5 failed attempts. It will be unlocked after 5 minutes".
- Form Fields:**
 - Account:** A text input field containing "jennifer".
 - Password:** A password input field with masked characters (dots) and a toggle icon.
- Buttons:** A blue "Login" button at the bottom right.

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 admin portal, go to **Settings > Admin**.
2. Scroll down to the **Account Locked Alert** setting.

The screenshot shows the "Account Locked Alert" setting in the admin portal. It includes a dropdown menu with the following options:

- Account Locked Alert:** A dropdown menu currently set to "No Email".
- Account Locked Alert Email:** A section with three radio button options:
 - No Email - No Email Alert will be sent
 - Email User - Email Alert only for User
 - Email User and Admin - Email Alert for both User and Admin

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.

Basic Settings

 The ability to set the Date and Time format is available in FileCloud Server version 19.1 and later.

Administrators must configure the basic settings listed below.

Basic Settings Checklist

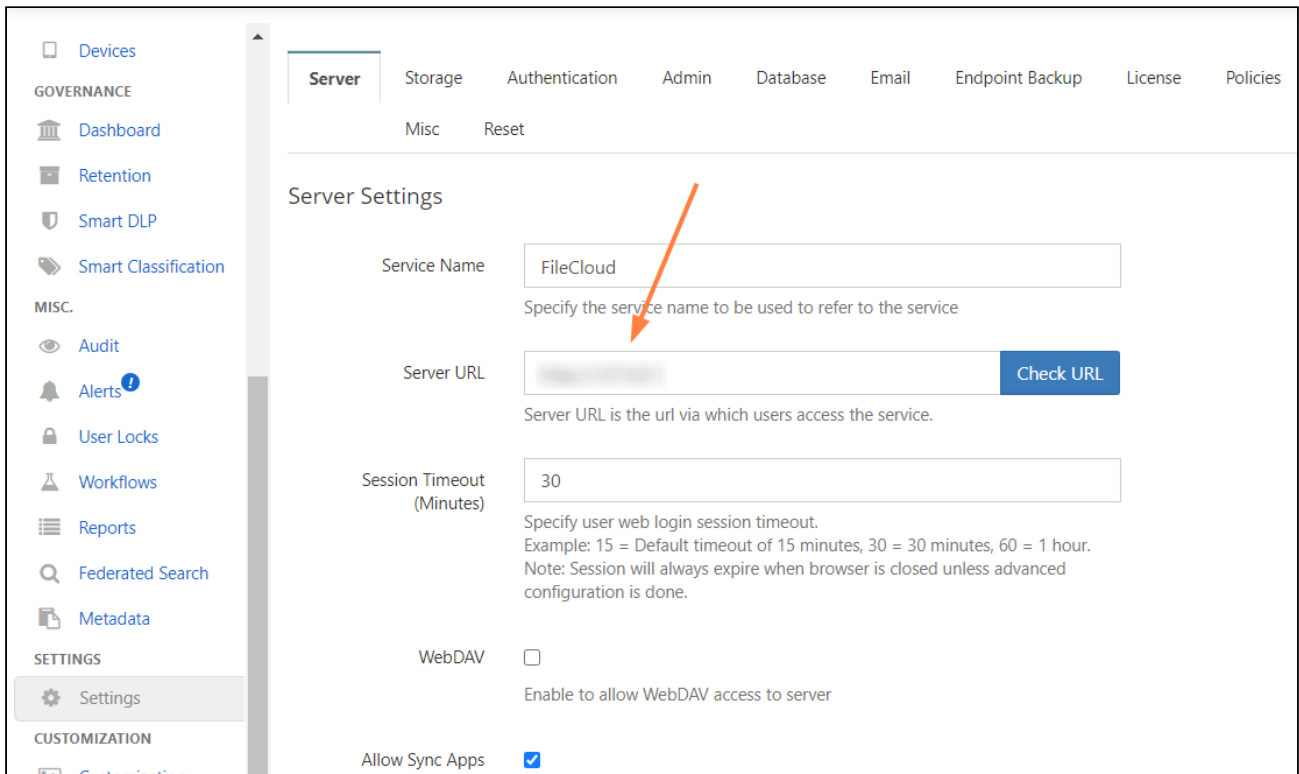
1. Access the Settings

To access the settings:

1. Open a browser and log into FileCloud *Admin Portal*.
2. In the left navigation panel, click **Settings**.
3. Click the **Server** tab, which is normally the default view.

2. Check the Server URL

It is very important that the **Server URL** is a valid externally accessible URL. This URL will be used for creating shares. Also if you are running multi-tenant setup, the URL is used for background cron job processing, so make sure the URL is accessible from the server running FileCloud.






The screenshot displays the FileCloud Admin Portal interface. On the left, a navigation menu is visible with categories: GOVERNANCE (Devices, Dashboard, Retention, Smart DLP, Smart Classification), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), and CUSTOMIZATION (Customization). The 'Settings' option is highlighted. The main content area shows the 'Server' tab selected, with sub-tabs for 'Storage', 'Authentication', 'Admin', 'Database', 'Email', 'Endpoint Backup', 'License', and 'Policies'. Below these are 'Misc' and 'Reset' options. The 'Server Settings' section contains the following fields and options:

- Service Name:** A text input field containing 'FileCloud'. Below it, a note reads: 'Specify the service name to be used to refer to the service'.
- Server URL:** A text input field with a blurred URL. To its right is a blue 'Check URL' button. Below it, a note reads: 'Server URL is the url via which users access the service.'
- Session Timeout (Minutes):** A text input field containing '30'. Below it, a note reads: 'Specify user web login session timeout. Example: 15 = Default timeout of 15 minutes, 30 = 30 minutes, 60 = 1 hour. Note: Session will always expire when browser is closed unless advanced configuration is done.'
- WebDAV:** A checkbox that is currently unchecked. Below it, a note reads: 'Enable to allow WebDAV access to server'.
- Allow Sync Apps:** A checkbox that is currently checked.

3. Configure the Remaining Settings

The following settings can be set on the *Manage Settings* screen on the *Server* tab, unless otherwise noted.

Settings Name	Description								
Service Name	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.								
Server URL	<p>This is your DNS entry registered with DNS service. example xyz.company.com . This is the URL by which users will access FileCloud service.</p> <p>It is also required that you make this server DNS name externally accessible via any firewall you might have.</p> <p>NOTE: Be sure to use the appropriate protocol prefix https:// or http:// . For production, it is highly recommended to use only https://</p>								
Session Timeout	<p>Number indicating the number of minutes the authentication is valid. If the browser is closed, the session will be logged out. To modify this behavior, see User Session Expiration.</p> <p>PLEASE NOTE: Session Timeout value is only applicable for Web browsers and not for other FileCloud clients such as Sync, Drive, Outlook Add-in etc as they store the login credentials.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>15 (default value)</td> <td>Session expires in 15 minutes (minimum session timeout), will always expire when browser session is closed.</td> </tr> <tr> <td>1</td> <td>Session Expires in 1 minute, will always expire when browser session is closed.</td> </tr> <tr> <td>60</td> <td>Session Expires in 1 hour, will always expire when browser session is closed.</td> </tr> </tbody> </table>	Value	Meaning	15 (default value)	Session expires in 15 minutes (minimum session timeout), will always expire when browser session is closed.	1	Session Expires in 1 minute, will always expire when browser session is closed.	60	Session Expires in 1 hour, will always expire when browser session is closed.
Value	Meaning								
15 (default value)	Session expires in 15 minutes (minimum session timeout), will always expire when browser session is closed.								
1	Session Expires in 1 minute, will always expire when browser session is closed.								
60	Session Expires in 1 hour, will always expire when browser session is closed.								
WebDAV	<p>You can enable this function to allow users to mount their FileCloud home folders as a Windows or Mac or Linux drives.</p> <p> Enable WebDAV support</p>								

Settings Name	Description
Allow Sync Apps	This switch can be disabled to block all Desktop Sync Apps from connecting to this server. Default value is "Enabled"
Default User Portal Language	Use this drop down to select the language that is used when a user logs on to the User Portal.  Set the Language
Default Admin Portal Language	Use this drop down to select the language that is used when an administrator logs on to the Admin Portal.  Set the Language

Set the Language

Introduction

FileCloud allows support for different languages and it is possible to control the language of the User portal as well as the Admin portal language.

1. Go to **Settings > Server**.
2. In the **Default User Portal Language** drop-down list, choose the user portal language.

3. In the **Default Admin Portal Language** drop-down list, choose the admin portal language.



The screenshot shows the 'Server Settings' page in FileCloud. The 'Default Admin Portal Language' dropdown is highlighted with a red box. The current selection is 'english'. Below it, the 'Default User Portal Language' is also set to 'english'. Other settings include Service Name (FileCloud), Server URL (http://127.0.0.1), Session Timeout (1440), WebDAV (disabled), Allow Sync Apps (checked), Allow Old Devices To Login (checked), and Log Level (PROD).

Setting	Value
Service Name	FileCloud
Server URL	http://127.0.0.1
Session Timeout (Minutes)	1440
WebDAV	<input type="checkbox"/>
Allow Sync Apps	<input checked="" type="checkbox"/>
Allow Old Devices To Login	<input checked="" type="checkbox"/>
Log Level	PROD
Default User Portal Language	english
Default Admin Portal Language	english

4. Click **Save**.
The new language appears in the user portal interface when the browser is refreshed.
The admin portal refreshes after you save and reloads with the new language.

Storage Settings

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

 <p>Managed Storage</p>	Setting up Managed Disk Storage
 <p>Protecting Your Storage</p>	Set Up Encryption for Managed Storage

FileCloud Managed Storage

Administrators can configure settings to control how users store data on FileCloud. This type of FileCloud storage is called **Managed Storage**, and it is displayed to the admin and users as the **My Files** folder.

Setting up Managed Storage

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

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

To set up Managed Storage:

1. Open a browser and log into the Admin portal.
2. On the left navigation panel, under Settings, click **Settings**.
3. Click the **Storage** tab.
4. Type the information into the fields as described below.

Setting	Description
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.
S3 Encryption	Appears when encryption is enabled in your system, and allows you to manage encryption. See Enabling S3 Storage Encryption .

Setting	Description
Disable My Files	If you are only using the "Network Folders" features of FileCloud and don't want to show "My Files", you can enable this checkbox. If there are existing data in "My Files" section, the data will no longer be accessible. Certain functions that depend on My Files will no longer be available.
User Storage Usage Calculation	When the user storage usage is reported, the shares used by the user can also be counted towards the quota. This can be changed by selecting the appropriate drop-down option.
Skip versioning for Files Greater Than	Any file larger than the specified value will not be versioned.
Email Users Nearing Storage Limit	If this option is enabled then automatic emails with notifications will be sent to users reaching their storage limit.
Percentage Threshold	Defines at what point the percentage of unused managed storage space is considered low. When unused storage is less than this value, an automatic email notification is sent to the admin. For example, if the value is set to 20, then the admin is notified if more than 80% of managed storage space is used.

5. Click **Save**.
6. Click the **Policies** tab.
7. For each policy that you want to change the default storage settings in:
 1. Click the edit button.
 2. Type the information into the fields as described below:
 3. Click **Save**.
 4. Assign the policy with relevant storage settings to each user.

Setting	Description
User Storage Quota	This is the storage quota that is provided for every user of FileCloud. Note that, this is only a quota and does not require physical storage until the user actually consumes the space. Setting this to 0 means each user has no storage quota limit. Changing this setting does not affect the existing user quota. <i>For example, if a user has 2 GB quota and if this setting is changed to 10 GB, it only affects newly created users after this point. To update the quota for an existing user, use the user details panel in Users section.</i>

Setting	Description
Store Deleted Files	Enable this setting if you wish to provide a way to keep deleted files in a Recycle Bin. When this option is enabled and a user deletes a file/folder, the deleted item gets moved into their personal deleted files area. Then the user can restore files from their recycle bin or empty the recycle bin completely. Note: Files in the recycle bin count towards a user's storage quota.
Automatically Empty Recycle Bin After Specified Days	Number of days after which Deleted Files is emptied automatically. Note that this recycle bin clearing happens at periodic intervals specified here and any files in any recycle bin are cleared. The default is 0 which means that the deleted files are not cleared automatically. Requires a Cron Job to be set up.
Do not store deleted files greater than	Any file larger than this setting is permanently deleted instead of getting moved into Deleted Files area.

Setting up Managed S3 Storage Encryption

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

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

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

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

What do you want to do?



[Enabling S3 Storage Encryption](#)



[Disabling S3 Storage Encryption](#)

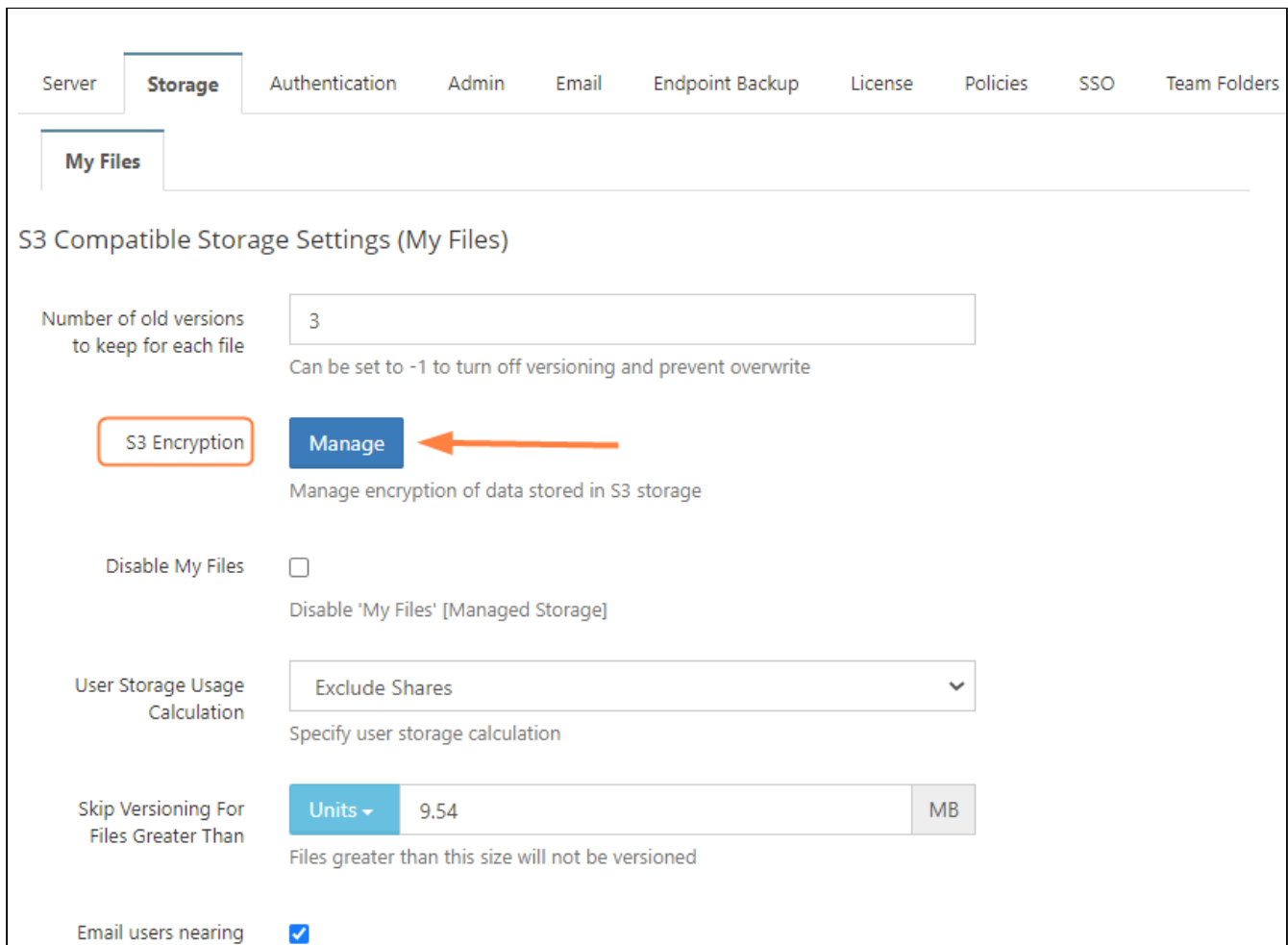


Read more about [Choosing S3 Encryption Type](#)

Enabling S3 Storage Encryption

In FileCloud Server version 19.1 and later, if a FIPS-enabled FileCloud license is installed, there is an option in the Admin Portal to enable FileCloud to run in FIPS mode.

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



The screenshot shows the 'Storage' settings page for 'My Files'. The 'S3 Encryption' section is highlighted with a red box, and a red arrow points to the 'Manage' button. The settings are as follows:

- Number of old versions to keep for each file:** 3. Can be set to -1 to turn off versioning and prevent overwrite.
- S3 Encryption:** Manage (highlighted with a red box and arrow). Manage encryption of data stored in S3 storage.
- Disable My Files:** Disable 'My Files' [Managed Storage].
- User Storage Usage Calculation:** Exclude Shares. Specify user storage calculation.
- Skip Versioning For Files Greater Than:** Units ▾ 9,54 MB. Files greater than this size will not be versioned.
- Email users nearing:**

Before you can set your S3 encryption options, S3 encryption must be configured in your system. If it 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:

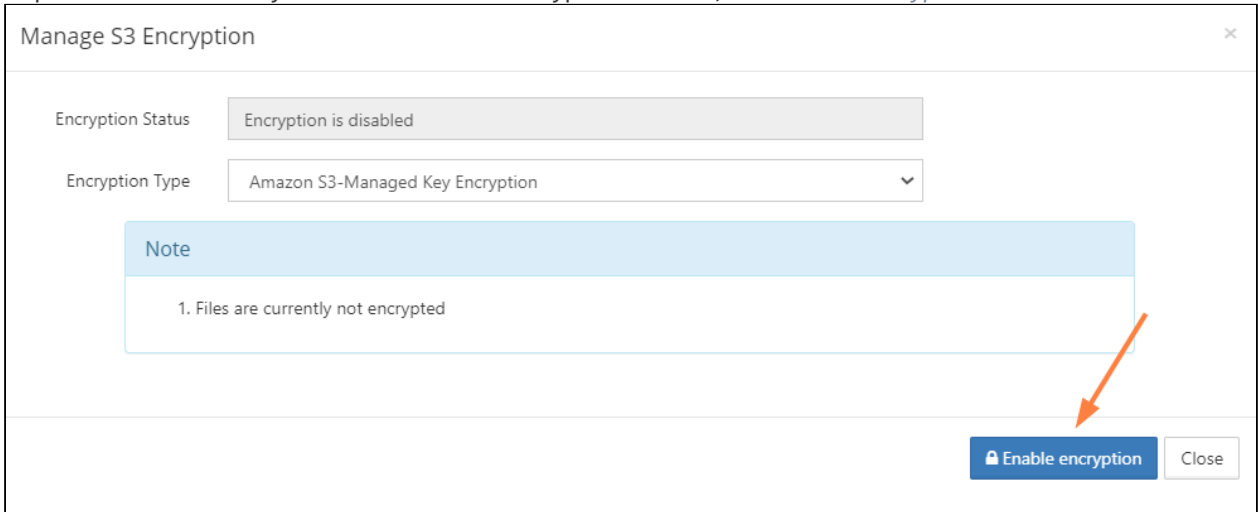
1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *SETTINGS*, select *Settings*.
3. On the *Manage Storage* screen, select the *Storage* tab and then the *My Files* sub-tab.
4. You will see a new option called *S3 Encryption*.
5. To open the *Manage S3 Encryption*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

The screenshot shows the 'S3 Compatible Storage Settings (My Files)' page in the FileCloud Admin Portal. The navigation tabs at the top are 'Server', 'Storage', 'Authentication', 'Admin', 'Email', 'Endpoint Backup', 'License', 'Policies', 'SSO', and 'Team Folders'. The 'Storage' tab is selected, and the 'My Files' sub-tab is active. The main content area is titled 'S3 Compatible Storage Settings (My Files)'. It contains several settings:

- Number of old versions to keep for each file:** A text input field containing '3'. Below it, a note says 'Can be set to -1 to turn off versioning and prevent overwrite'.
- S3 Encryption:** A section with a blue 'Manage' button. A red arrow points to this button. Below the button, it says 'Manage encryption of data stored in S3 storage'.
- Disable My Files:** A checkbox that is unchecked. Below it, it says 'Disable 'My Files' [Managed Storage]'.
- User Storage Usage Calculation:** A dropdown menu showing 'Exclude Shares'. Below it, it says 'Specify user storage calculation'.
- Skip Versioning For Files Greater Than:** A text input field containing '9.54' and a unit selector set to 'MB'. Below it, it says 'Files greater than this size will not be versioned'.
- Email users nearing:** A checkbox that is checked.

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

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

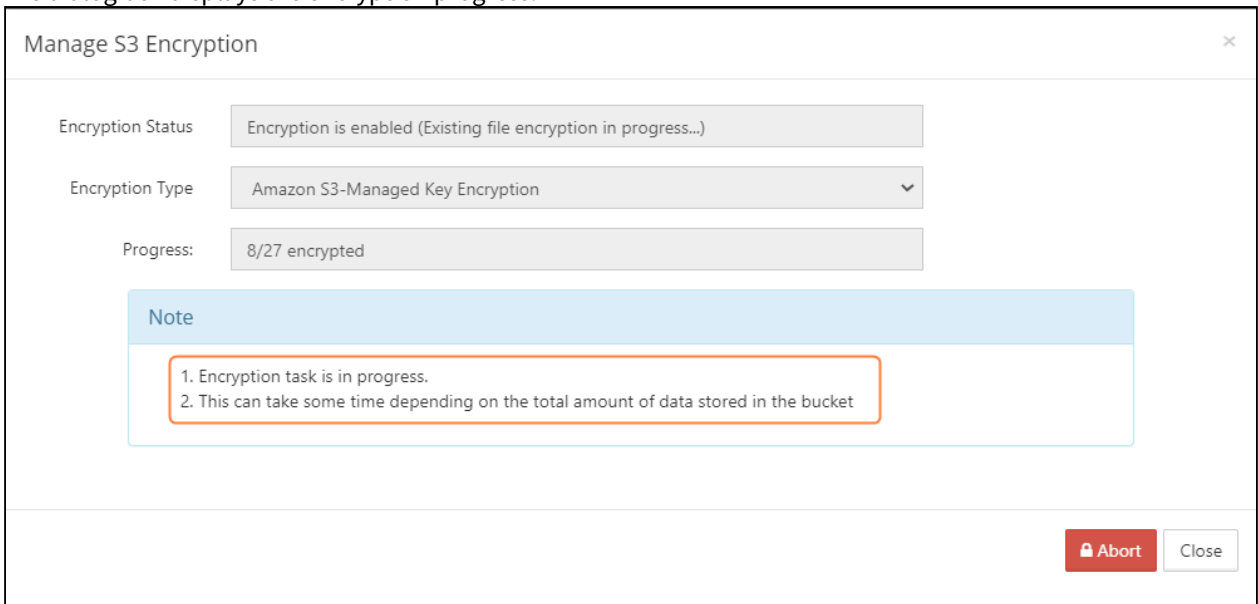


The screenshot shows a dialog box titled "Manage S3 Encryption" with a close button (X) in the top right corner. The "Encryption Status" field displays "Encryption is disabled". The "Encryption Type" dropdown menu is set to "Amazon S3-Managed Key Encryption". Below these fields is a "Note" box containing the text: "1. Files are currently not encrypted". At the bottom right, there are two buttons: "Enable encryption" (highlighted with an orange arrow) and "Close".

You are prompted to confirm encryption.

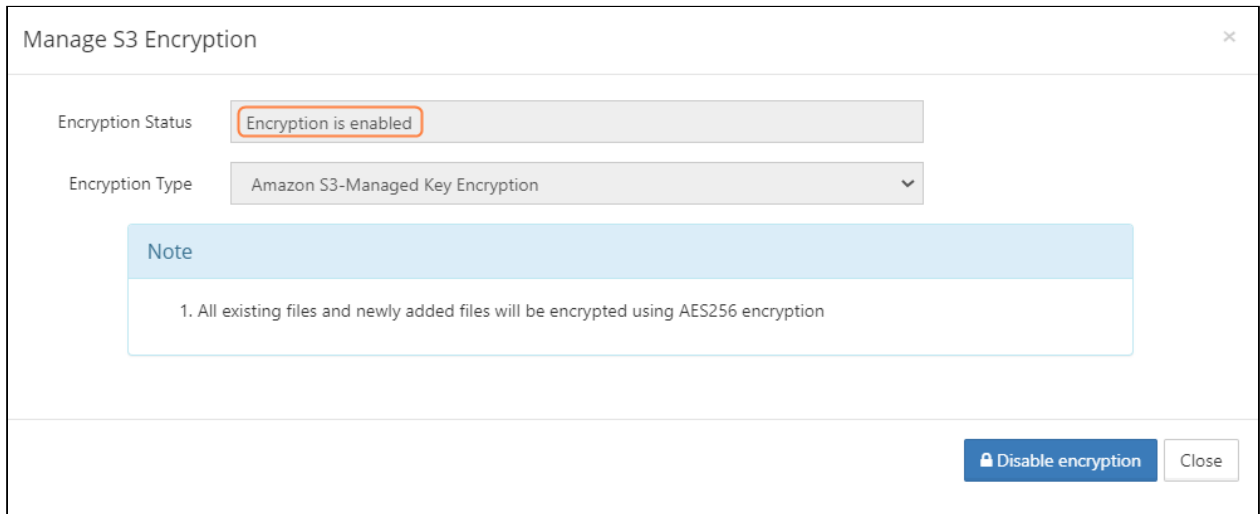
7. Click **OK**.

The dialog box displays the encryption progress.



The screenshot shows the same "Manage S3 Encryption" dialog box. The "Encryption Status" field now displays "Encryption is enabled (Existing file encryption in progress...)". The "Encryption Type" dropdown menu remains "Amazon S3-Managed Key Encryption". A new "Progress:" field shows "8/27 encrypted". The "Note" box contains two items: "1. Encryption task is in progress." and "2. This can take some time depending on the total amount of data stored in the bucket". At the bottom right, the buttons are "Abort" (highlighted with a red border) and "Close".

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

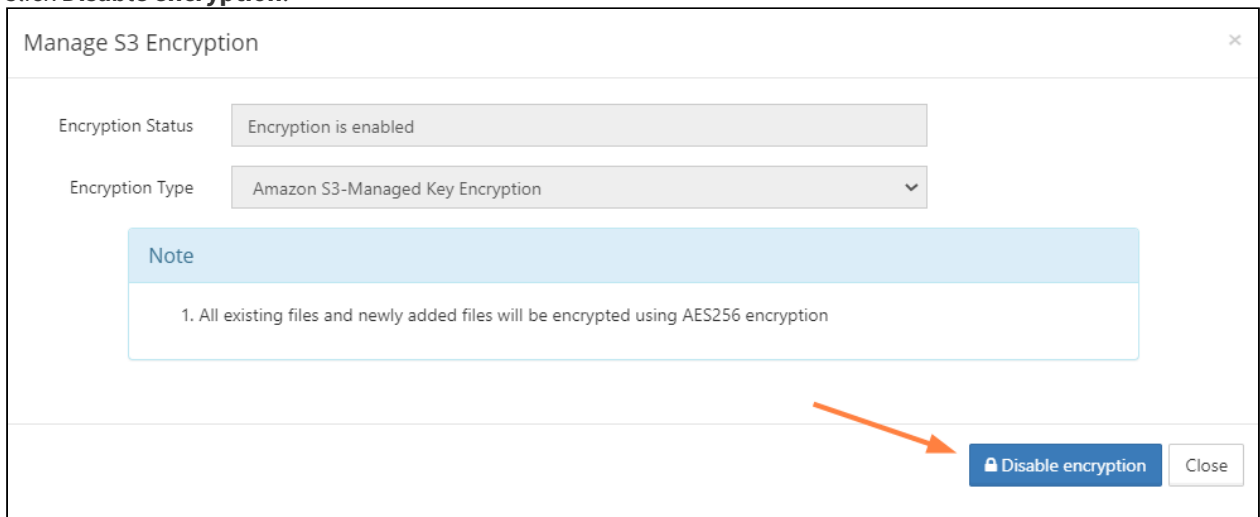


Disabling S3 Storage Encryption

Administrators can disable S3 storage encryption following the steps here.

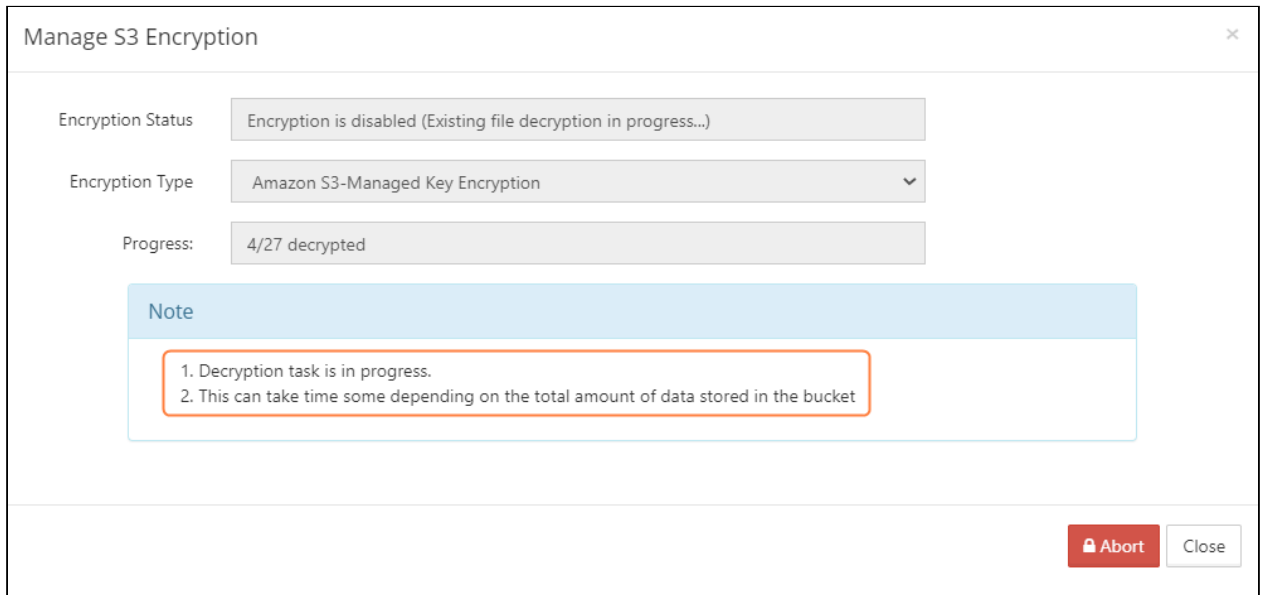
To disable S3 encryption:

1. Login into admin UI.
 2. Goto **Settings -> Storage**.
 3. Click **Manage**.
- The **Manage S3 Encryption** dialog box opens.
4. Click **Disable encryption**.

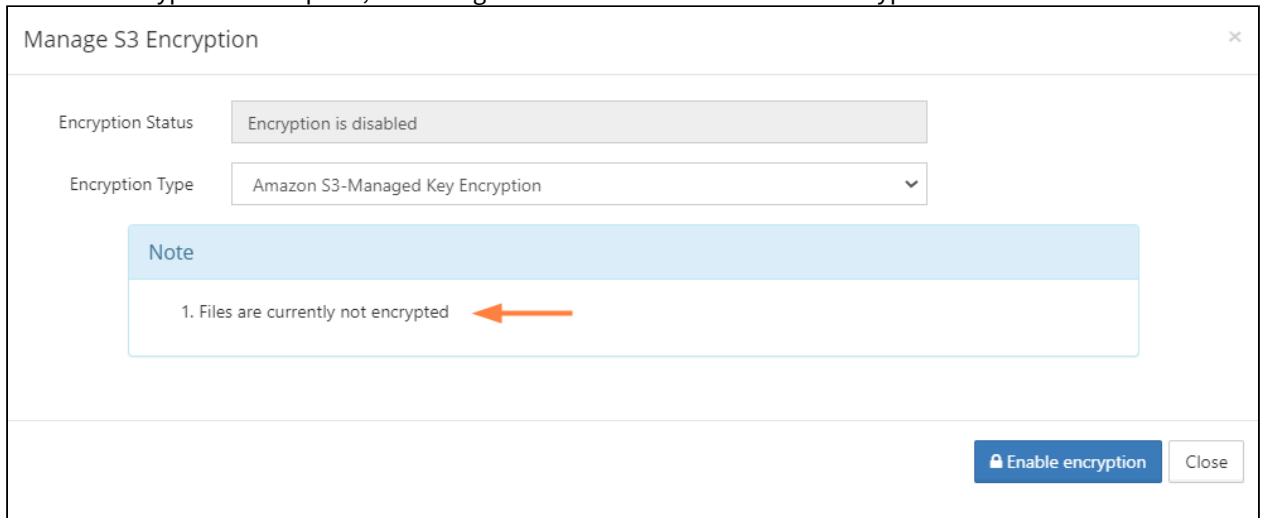


You are prompted to confirm disabling encryption.

5. Click **OK**.
- The **Manage S3 Encryption** dialog box displays decryption progress:



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



Choosing S3 Encryption Type

When you use S3 Storage Encryption:

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

FileCloud supports the following Server Side Encryption:

Encryption Type	Notes
Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)	All data is encrypted at rest using AES256 bit encryption. The data can only be accessed using the supplied key/secret credentials. The data will be accessible via S3 Console Note: Even though the encrypted data is accessible directly from the S3 console, do not access the data if it was created by FileCloud Managed storage, as doing so will cause data corruption to occur. In this case, the data should only be modified by FileCloud.
Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)	Similar to SSE-S3 but the key itself is managed using Amazon's KMS service. This allows management of specific keys and their permissions for encrypting the data. The data is still encrypted at rest and is accessible via S3 Console with appropriate credentials.
Server-Side Encryption with Customer-Provided Keys (SSE-C)	This is a new support available from FileCloud v15 on-wards. The data will be encrypted using customer supplied 32 bit encryption key. This option will have SLOWER performance due to restriction on how this data can be decrypted (Amazon server will NOT be able to decrypt the data and the data has to be first downloaded to FileCloud server and decrypted). The data will NOT be accessible via S3 console as well.

WARNINGS:

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

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

Manage the Recycle Bin Using Policies

Administrators can configure FileCloud to deal with the site's Recycle Bin through policies.

Why?

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

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

Do you want to store deleted files for recovery purposes?

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

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

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

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


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

This is configured by the setting called:

- *Automatically delete File from the Recycle Bin After Set Number of Days*

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

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

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

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

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

This is configured in the following setting:

- *Do Not Store Deleted Files Greater Than*

- Files less than this size are stored
- Files greater than this size are permanently deleted

You can specify the file size in the following ways:

- GB
- MB
- KB
- B

You can also restrict a user's ability to empty their own recycle bin.

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

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

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

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

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

The following three Recycle Bin settings exist in Policies:

Setting	Option	Description
<i>Store Deleted Files</i>	YES or NO	Move the file from it's location in My Files to the recycle bin when the user deletes it
<i>Automatically Delete Files from Recycle Bin After Set Number of Days</i>	Whole number	Number of days after a file was deleted that it will be automatically cleared from the recycle bin (and therefore, no longer be present in FileCloud). A value of 0 indicates that deleted files will not be cleared automatically. If they are not manually cleared from the recycle bin, they will remain available to be restored in FileCloud but will also use up available storage.
<i>Do Not Store Deleted Files Greater Than</i>	Any positive number of Units: <ul style="list-style-type: none"> • GB • MB • KB • B 	Files Greater than the specified size are permanently deleted. The number can contain decimals. For example: <ul style="list-style-type: none"> • 0.09765625 GB

Policy Settings - Global Default Policy ✕

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


Enables/disables privacy settings

Store Deleted Files NO ▾
Move file to recycle bin on delete action


Automatically Delete Files from Recycle Bin After Set Number of Days 0
Number of days once deleted files will be cleared. Value of 0 indicates that deleted files will not be cleared automatically.

Do Not Store Deleted Files Greater Than Units ▾ 0.09765625 GB
Files Greater than the specified size are permanently deleted.

Save
Reset
✕ Close


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

To configure the recycle bin policy:

1. Log into the *Admin Portal*.
2. From the left navigation pane, under SETTINGS, click *Settings*.
3. Click the *Policies* tab, select the *Global Default Policy*, and then click the *Edit policy* button ().
4. In the *Policy Settings* window, in *Store Deleted Files*, select *YES* or *NO*.
5. If you selected *NO*, to save your changes, click *Save* and to close the policy window click *Close*.
6. If you selected *YES*, in *Automatically delete File from the Recycle Bin After Set Number of Days*, to enable this option, type in a number. To disable this option, type in 0.
7. If you selected *YES*, in *Do Not Store Deleted Files Greater Than*, select the type of unit in *Units*, and then type in a number.
8. To save your changes, click *Save* and to close the policy window click *Close*.

Disable Managed Storage (MyFiles section)

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

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

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

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

4. Check **Disable My Files**.

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

My Files Network

My Files Storage Settings

Storage Path

Specify the location to store Cloud Files, this must be writable by Webserver.
 Example path on Windows : c:\clouddata
 Example path on Linux : /opt/cloud/data
Note: To change the storage location after it has been configured, move the contents from the old storage location to the new.

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

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

User Storage Usage Calculation
 Specify user storage calculation

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

Email users nearing storage limit

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

Restrict a User's Recycle Bin Options

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

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

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

By default, all users:

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

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

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

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

Policy Settings - Global Default Policy

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

General 2FA **User Policy** Client Application Policy Device Configuration Notifications

User Policy


Disable Invitations to New Users: NO
Do not allow user to send invitations to new users when shares are created.

Create account on new user shares: NO
Create accounts automatically when share invitations are sent to new users.

Enable Recyclebin Clear Feature: YES
Allow users to clear recyclebins.

Save Reset Close

To configure this option:

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

Enable Folder-Level Permissions

In many sharing scenarios, administrators are required to configure granular folder permissions. This feature provides a way to allow some actions on a parent, or top-level folder, while restricting those actions on a specific sub-folder.

Folder-Level Permissions Support	Folder-Level Permissions Do Not Support
<ul style="list-style-type: none"> ✔ Interaction with share permissions to apply the most restrictive permissions ✔ Allow or restrict access by specifying a user's email account ✔ Folders in Managed Storage ✔ Permissions can be set by the owner of the folder 	<ul style="list-style-type: none"> ✘ Folders in Network Storage ✘ Permissions set by a user other than the owner

To enable users to set folder-level permissions:

1. Enable Folder-Level Permissions

The screenshot displays the FileCloud Online administration interface. On the left is a navigation sidebar with categories: GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification, Compliance Center), MISC (Audit, Alert, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), CUSTOMIZATION (Customization), and SYSTEM (Checks). The main content area shows the 'Misc' settings page, with tabs for General, User, Password, Notifications, Share, Preview, Support Services, and Directory Scraper. Under the 'General' tab, there are sections for 'DUO Security', 'Privacy', and '2FA'. The 'General System Settings' section includes dropdown menus for 'Server Timezone' (America/New_York), 'Calendar Type' (Gregorian (English)), 'Date Format' (MMM dd, yyyy (Jan 15, 2019)), and 'Time Format' (h:mm A (2:20 PM)). Below these, there is a 'Default Web UI Version to show' dropdown set to 'UI 2.0'. At the bottom of the settings, the 'Apply Folder Level Security' checkbox is checked, with a blue checkmark and the text 'Allow folder level security settings to apply to share permissions'. An orange arrow points to this checkbox from the left sidebar.

To enable users to set folder-level permissions:

1. In the admin portal go to Settings > Misc > General.
2. Check the **Apply Folder Level Security** checkbox.
3. Click **Save**.

2. Use Policies to Allow Users to Set Folder Permissions

By default, users are not allowed to set folder-level permissions, as it can increase complexity of sharing and access rights.

However, administrators can allow this behavior by:

- Customizing the default global policy - which allows all users to set folder level permissions
- Creating a user-specific policy - which allows a specific user(s) to set folder level permissions (this can also be used for groups)

Customize the Default Global Policy

You do not have to create a new policy to allow all users to set folder-level permissions.

You can just edit the Global Default policy.

Policy Settings - Global Default Policy

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

Enable code based device authentication	NO	Enable code based device authentication
Require Admin Approval for Device Authentication	NO	Require admin approval for code based device authentication
Enforce Session Timeout for Devices	NO	Device timeout is enforced when code based authentication is used.
Allow Folder Level Security	NO	Allow users to set folder level security for granular permissions.

Save Reset Close

To grant all users the ability to set folder-level permissions:

1. Log into the admin portal.
2. In the left navigation pane, under **SETTINGS**, click **Settings**.
3. On the **Manage Settings** screen, select the **Policies** tab.
4. On the **Manage Policy** tab, click the **Global Default Policy** row, and then click the edit button ().

5. On the **Policy Settings- Global Default Policy** dialog, select the **User Policy** tab.
6. In **Allow Folder Level Security**, select **YES**.
7. Click **Save**.

Create a User-Specific Policy

You can either:


- Create a new policy granting folder-level permission access and then add specific users to it
- Create a policy for one specific user

The screenshot shows a dialog titled "Manage Policy Users : Allow Folder Perms". At the top, there is a search filter "Filter" with a magnifying glass icon and the text "Filter by name, email or notes". To the right of the filter is a "Status Filter : All" dropdown menu. Below the filter is a table with two columns: "Available Users" and "Status". The "Available Users" table has the following rows:


Available Users	Status
2 (2)	Limited Access
a (a)	Full Access
a_1 (a_1)	Full Access
a_1 (a_1)	Limited Access
ab (ab)	Full Access
alex (alex)	Full Access
Kara (Kara)	Full Access

At the bottom of the "Available Users" table is a pagination control showing "Page 1 of 10" and "94 rows". To the right of the "Available Users" table is an empty table with columns "Policy Users" and "Status". Between the two tables are two arrow buttons: a right-pointing arrow and a left-pointing arrow. At the bottom right of the dialog is a "Close" button. Three numbered callouts (1, 2, 3) are overlaid on the image: callout 1 points to the user "a_1 (a_1)" in the "Available Users" table; callout 2 points to the right-pointing arrow button; callout 3 points to the "Close" button.



To create a policy granting rights to set folder-level permissions:

1. Log into the admin portal.
2. In the left navigation pane, under **SETTINGS**, click **Settings**.
3. On the **Manage Settings** screen, select the **Policies** tab.
4. On the **Manage Policies** tab, click the **New policy** button.
5. In the **New policy** dialog, in **Policy Name**, type in Allow Folder Permissions or something similar, and then click **Create**.
6. On the **Policies** tab, in the **Manage Policy** section, click in the row of the policy you just created.
7. To configure the policy, click the edit policy icon ().
8. On the **Policy Settings** dialog, select the User Policy tab.
9. In **Allow Folder Level Security**, select **YES**.
10. Click **Save**.

To add one or more users to the policy:

1. On the **Policies** tab, in the **Manage Policy** section, click in the row of the policy you just created.
2. Click the manage users icon ().
3. On the **Manage Policy Users** dialog, in **Available Users**, select the user you want to grant folder-level permissions.
4. To add the user to this policy, click the right arrow.

5. Repeat steps 3 and 4 until you have added all the users you want.
6. To save your changes, click **Close**.

 These same steps can be used to add Groups to the policy by clicking on the manage groups icon ().

3. Check Effective Permissions

Administrators can check to see which permissions are actually granted for access to a folder.

- This is very useful when a user belongs to multiple groups or policies
- This check can also help you troubleshoot access issues
- This permissions check does not take into consideration any folder or file sharing permissions

When you check for effective permissions on a folder, you will be able to see if a user has one or more of the following Folder-Level Permissions:

Permission	Description
Read	<ul style="list-style-type: none"> • Allows Downloading Files • Allows Previewing Files
Write	<ul style="list-style-type: none"> • Allows uploading and modifying existing files • Allows creating files and folders • Allows renaming files and folders
Delete	<ul style="list-style-type: none"> • Allows deleting files and folders
Share	<ul style="list-style-type: none"> • Allows sharing files and folders
Manage	<ul style="list-style-type: none"> • Allow managing folder-level permissions for this folder

Manage Folder Level Security
✕

Folder: /sat1/Class 3

Security

Check Access

Effective Permissions



Check effective permissions for any user when this path is shared with them. Note: Share permissions are not considered here. If share permissions are more restrictive, those will be applied.

👤

Check

✔	Read access allowed
✔	Write access allowed
✔	Delete access allowed
✘	Share access not allowed
✘	Manage access not allowed

To check a user's effective permissions:

1. Log into the admin portal.
2. In the left navigation pane, under **MANAGE**, click **Folder Permissions**.
3. On the **Manage Folder Permissions** screen, click the row that contains the policy which allows folder-level permission.
4. Click the edit button ().
5. On the **Manage Folder Level Security** dialog, select the **Check Access** tab.
6. In the box next to the user icon (), type in the user's email id for their FileCloud Server account.
7. Click **Check**.

4. Test Setting Permissions on the User Portal

Once a user has the ability to set folder level permissions, after logging in to the User Portal, a security tab will be available for their folders.

The screenshot shows the FileCloud interface with the 'My Files' view. The left sidebar contains navigation options like 'All Files', 'My Files', 'Team Folders', 'Network Shares', 'Shared with Me', 'Recent Documents', 'Starred', 'Shared by Me', 'File Operations', 'Notice', and 'Deleted Files'. The main area displays a list of files and folders. The 'Public Documents' folder is selected, and the right-hand pane shows the 'Security' settings for this folder. The 'Security' pane includes a 'Manage Security' button, which is highlighted by an orange arrow.

Name	Modified	Size
Accounts	Oct 23, 2020 2:13 PM by you	
DI 19-20	Jun 08, 2020 1:00 PM by you	
Public Documents	Jun 15, 2020 10:04 AM by you	
QuickNotes	Nov 17, 2020 3:12 PM by you	
backups	Jul 24, 2020 4:08 PM by you	
2020-07-24_09h04_37.png	Jul 24, 2020 9:04 AM by you	27 KB
2020-11-04_09h53_35.png	Nov 04, 2020 9:53 AM by you	72 KB
AAAReceipt02272019.pdf	Feb 27, 2019 8:32 AM by you	108 KB

To test setting folder-level permissions, follow the steps in the User Guide for [Setting Permissions on a Folder](#).

Example scenarios

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

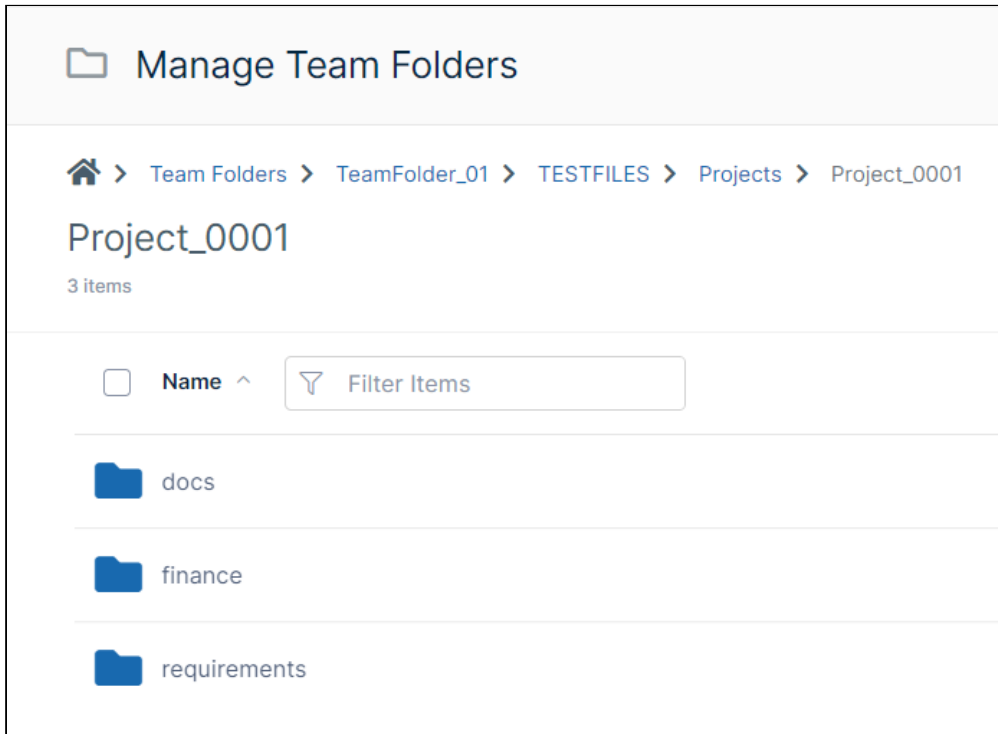
In this scenario, an administrator gives two groups access to a folder, but only gives one group access to one of its sub-folders.

Example of giving permissions to only specific users or groups

In this example, the folder **Projects** in the path **TeamFolder_01/TESTFILES** is only shared with the groups:

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

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



Example of giving permissions to only specific users or groups

To accomplish this, the administrator:

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

Share link for folder Projects ✕

Share Link

Modify Link 📄 🔗 ✉

Shared Folder
/team folder account/TeamFolder_01/TESTFILES/Projects

Share Options | Share History

Share Name: [Change](#)

Expires:

Upload Size Limit (MB):

Send Email Notifications:

Allow anyone with link
 Allow anyone with link and a password
 Allow selected users or groups

Sharing Permissions:

Group	View	Download	Upload	Share	Sync	Delete	Manage	
ProjectManagers	☑	☑	☑	☑	☐	☐	☐	✕
ProjectTeam	☑	☑	☑	☐	☐	☐	☐	✕

Example of giving permissions to only specific users or groups

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

The screenshot displays the FileCloud interface for managing team folders. The breadcrumb path is: Home > Team Folders > TeamFolder_01 > TESTFILES > Projects > Project_0001. The main view shows a folder named 'Project_0001' containing 3 items. A table lists the items:

Name	Modified	Size
docs	Jan 06, 2023 9:40 AM by team folder account	
finance		
requirements	Jan 06, 2023 9:40 AM by team folder account	

An orange arrow points to the 'Permissions' icon (a key) in the action menu for the 'finance' folder. A tooltip labeled 'Permissions' is visible above the icon.

Example of giving permissions to only specific users or groups

- a. Gives permission to the **ProjectManagers** group only.

Manage Folder Level Security
✕

Folder: /team folder account/TeamFolder_01/TESTFILES/Projects/Project_0001/finance

Security

Check Access

Permissions

Inherit Folder Level Security

Users

Groups

Add Group

Groups	Read	Write	Share	Delete	Manage	
ProjectManagers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ✕

Inherited Permissions

Users

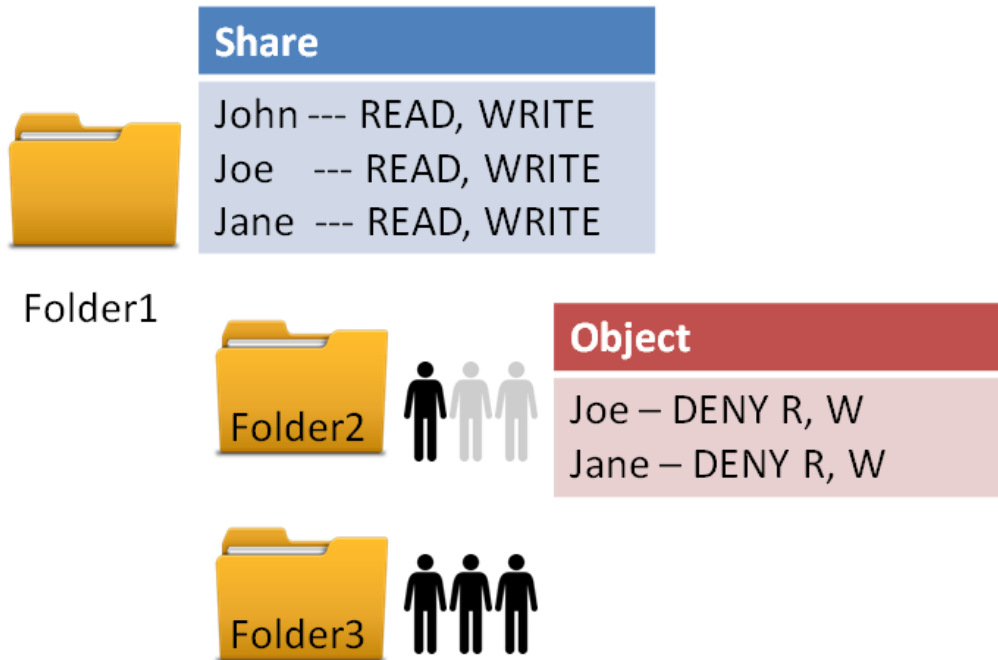
Groups

Users	Read	Write	Share	Delete	Manage
No entries					

OK

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 allow only John access to the subfolder, Folder2, but wants to give all three users access to the subfolder, Folder3.

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, Joe, and Jane

Example of a Sharing Scenario

To accomplish this, the administrator:

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

2. Creates folder-level security permissions for the two users who will not have access to Folder2.

- Joe- deny all access to Folder2
- Jane- deny all access to Folder2

When John, Joe, and Jane access the parent Folder1:

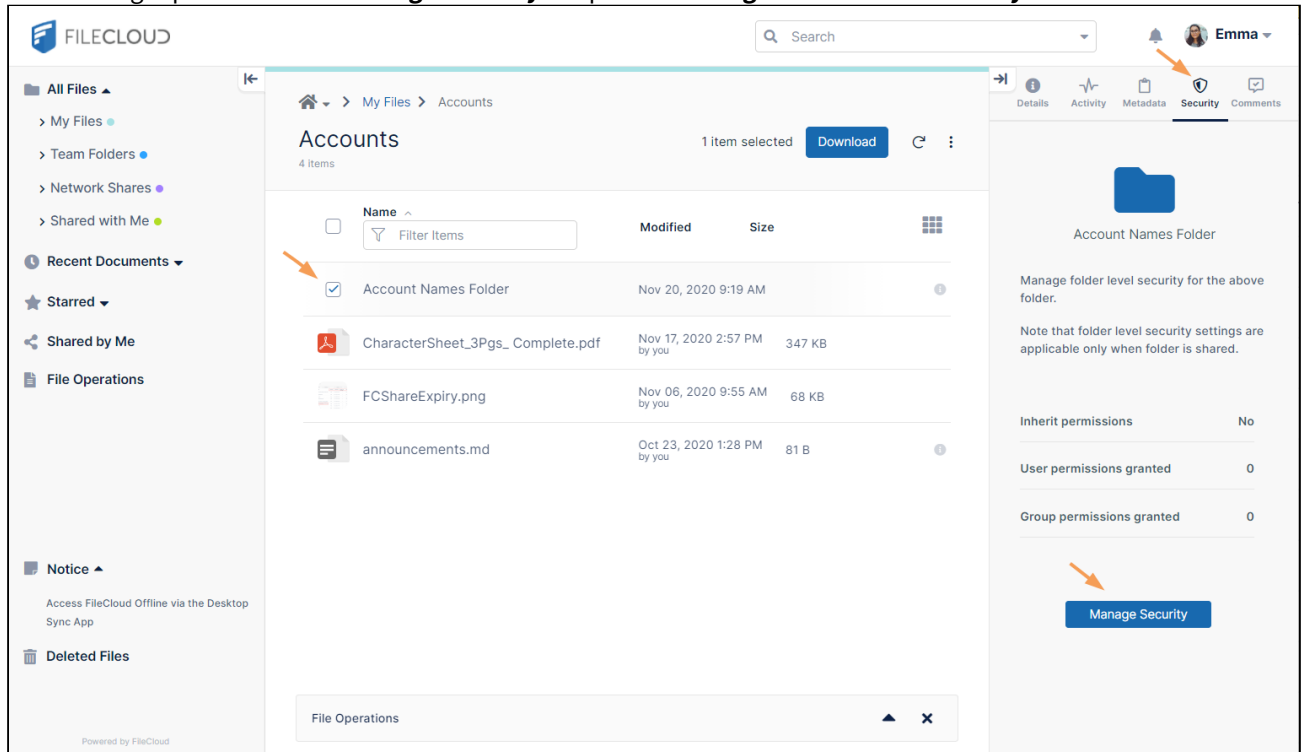
User	Folder1	Folder2	Folder3
John	✔ See it listed	✔ See it listed	✔ See it listed
	✔ Access its content	✔ Access its content	✔ Access its content

Example of a Sharing Scenario			
User	Folder1	Folder2	Folder3
Joe	<ul style="list-style-type: none"> ✓ See it listed ✓ Access its content 	<ul style="list-style-type: none"> ✗ See it listed ✗ Access its content 	<ul style="list-style-type: none"> ✓ See it listed ✓ Access its content
Jane	<ul style="list-style-type: none"> ✓ See it listed ✓ Access its content 	<ul style="list-style-type: none"> ✗ See it listed ✗ Access its content 	<ul style="list-style-type: none"> ✓ See it listed ✓ Access its content

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 and click **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:






Manage Folder Level Security ✕

Folder: /jenniferp/Accounts/Account Names Folder

Security

Check Access






Add User

Users	 Read	 Write	 Share	 Delete	 Manage	
gabrielle_95@example.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✕
jordan_95@example.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✕

Inherited Permissions

Users

Groups

Users	 Read	 Write	 Share	 Delete	 Manage	
gabrielle_95@example.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✕
jacob-87@example.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✕

OK

Permission	Description
Read	<ul style="list-style-type: none"> Allows Downloading Files Allows Previewing Files
Write	<ul style="list-style-type: none"> Allows uploading and modifying existing files Allows creating files and folders Allows renaming files and folders
Delete	<ul style="list-style-type: none"> Allows deleting files and folders

Permission	Description
Share	<ul style="list-style-type: none"> Allows sharing files and folders
Manage	<ul style="list-style-type: none"> Allow managing folder-level permissions for this folder

See [Set Permissions on Folders in the User Dashboard](#) for more information.



Permission inheritance

How Do Inherited Permissions Work?

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

- The child, or sub-folder has all of the same **permissions** as its parent folder
- The child, or sub-**folder** has all of the same **permissions** as its parent folder, plus additional **permissions**
- The child, or sub-**folder** has all of the same permissions as its parent, minus additional **permissions**
- The child, or 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 in this folder are exactly the same as the top level folder's permissions
 Don't Inherit Permissions	Permissions set in this folder don't inherit from any top level folder's permissions and are specific to only this folder

Permission hierarchy

In What Order Are Permissions Evaluated?

Folder-level permissions are evaluated in the following order:

- User's folder-level permissions for current folder (*if it exists*)
- Group's folder-level permissions for current folder (*if it exists*)
- Inherit permissions
 - If enabled, a search is continued along all parent paths until either:
 - user's folder level permission is set for any parent folder
 - group's folder level permission is set for any parent folder

 When a user belongs to multiple groups and each group has conflicting permissions, the effective permissions will be a composite of the permissions provided to each group.

For example: Jane belongs to Group1 and Group2.

- Group1 has Read permission on FolderA

- Group2 has Read and Write permissions on FolderA

Jane's effective permissions for FolderA are Read and Write.

Set Granular Permissions on Team Folders

Once a Team Folder is shared, all users with access to the share will see Team Folders in the navigation panel of the user portal and all FileCloud clients such as Sync, Drive, Outlook and the Office Add-In. These users' actions are limited by the **share** permissions. Additional limitations may be added in addition to the share permissions for specific users and groups in the form of **granular** permissions.

- Change **share** permissions on the Team Folder share to enable use of more granular permissions
- Use **granular** permissions on the Team Folder itself to restrict permissions to specific users and groups. These are applied in addition to the share permissions.

➔ For more information on folder **share** permissions, read about the [Private Share Permissions for Folders](#).

Enable granular folder level permissions

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Settings**.
3. On the **Settings** screen, click the **Misc** tab.
4. On the **General** sub-tab, select the checkbox **Apply Folder Level Security**.

The screenshot shows the FileCloud Online administration interface. The top navigation bar includes: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, and Policies. Below this, there are sub-navigation tabs: Third Party Integrations, ServerLink, Misc (highlighted), and Reset. Under the 'Misc' tab, there are several sub-sections: General (highlighted), User, Password, Notifications, Share, Preview, Support Services, and Directory Scraper. Below these are DUO Security, Privacy, and Two FA. The main content area is titled 'General System Settings' and contains the following settings:

- Server Timezone: America/Chicago (dropdown menu)
- Date Format: MMM dd, yyyy (Jan 15, 2019) (dropdown menu)
- Time Format: h:mm A (2:20 PM) (dropdown menu)
- Default Web UI Version to show: UI 2.0 (dropdown menu)
- Apply Folder Level Security: (checkbox with an orange arrow pointing to it)

Below the 'Apply Folder Level Security' checkbox, there is a note: 'Allow folder level security settings to apply to share permissions'.

Apply granular folder permissions to Team Folders:

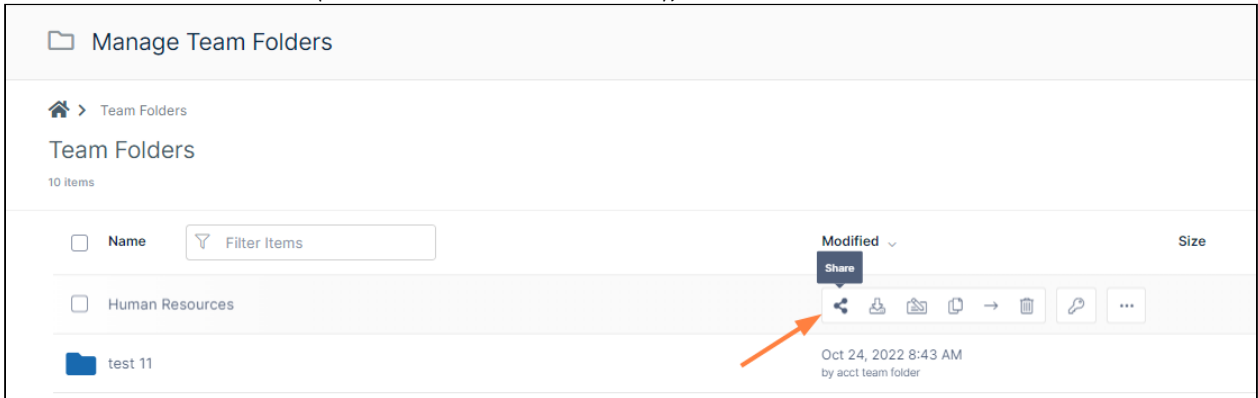
You can apply granular folder permissions to the top-level team folder or to its sub-folders.

Here, we will use a common scenario, in which a top-level team folder stores various sub-folders for the team. The entire team is given access to some of the sub-folders, 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 sub-folders that contain that information.

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

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

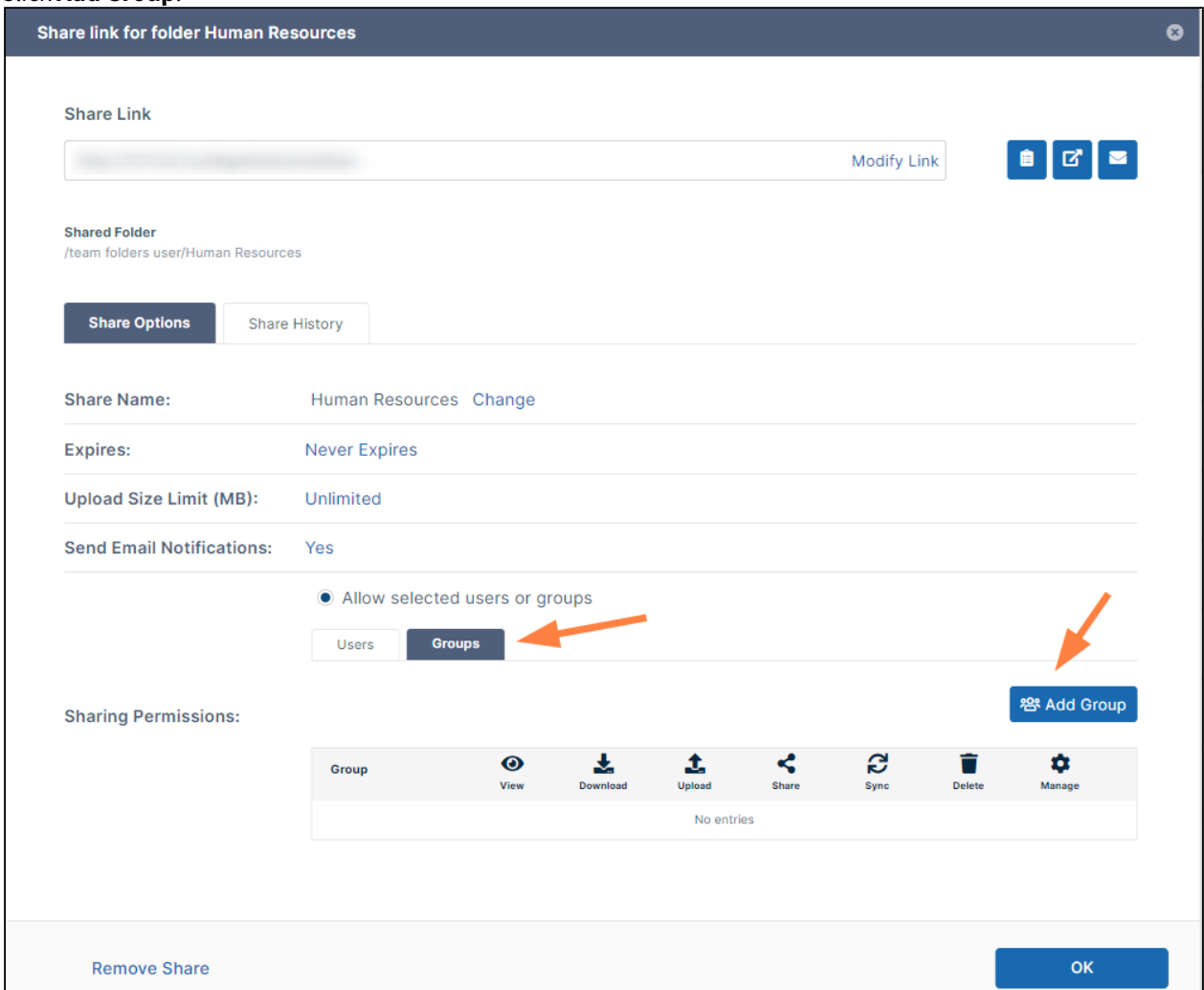
2. Hover over the Team Folder (in this case **Human Resources**), and click the share icon.



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

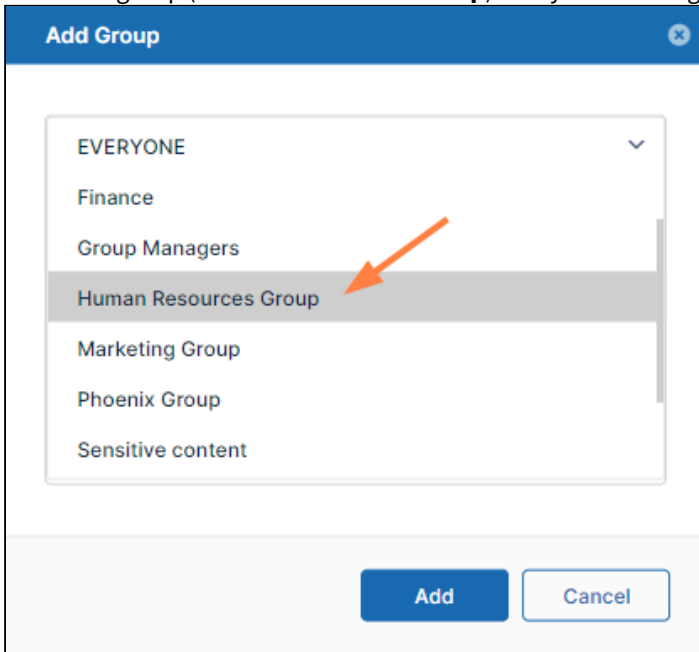
First give the entire **Human Resources Group** access to the **Human Resources** folder.

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.

Share link for folder Human Resources
✕

Share Link

http://127.0.0.1/url/kjpefwtkzmvki5wv
Modify Link

📄
🔗
✉️

Shared Folder
/team folders user/Human Resources

Share Options

Share History

Share Name: Human Resources Change

Expires: Never Expires

Upload Size Limit (MB): Unlimited

Send Email Notifications: Yes

Allow selected users or groups

Users

Groups (1)

+ Add Group

Sharing Permissions:

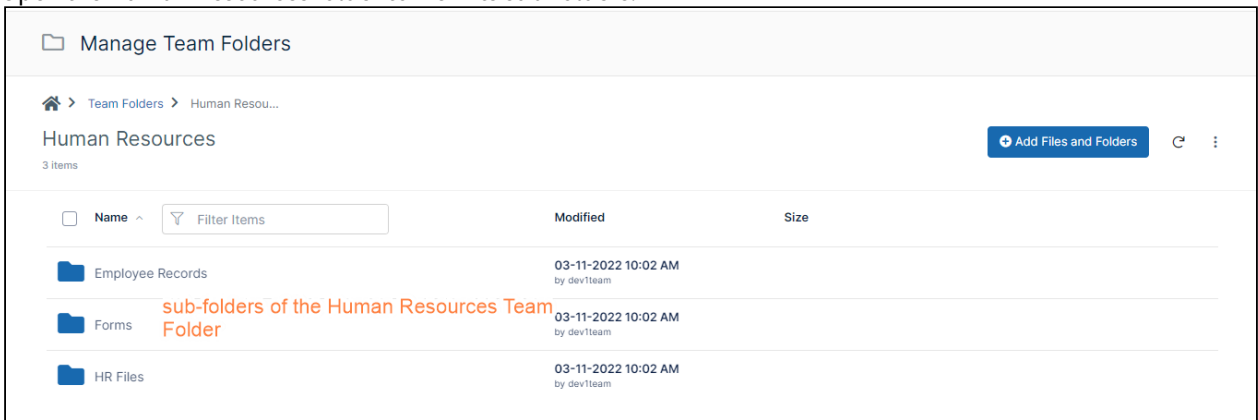
Group	View	Download	Upload	Share	Sync	Delete	Manage
Human Resources	☑️	☑️	☑️	☑️	☑️	☑️	☐ ✕

Remove Share
OK

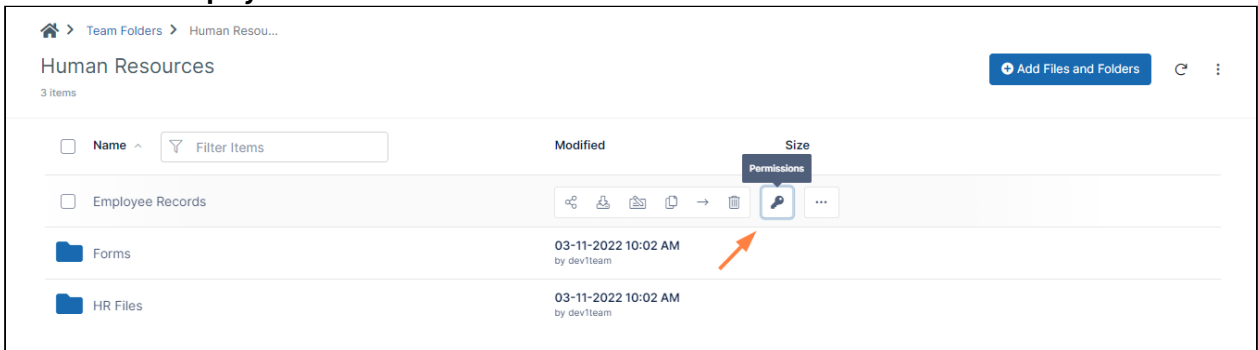
7. Close the dialog box.

Restrict permissions to specific users within the group

1. Open the Human Resources folder to view its sub-folders.



2. We want to give the users **HR Manager** and **Jessica** full access to the **Employee Records** and **Forms** sub-folders. We don't want to give the other members of the team any access to these sub-folders, 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** sub-folder.

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

Manage Folder Level Security

Folder: /Human Resources/Employee Records

Security Check Access

Permissions

Inherit Folder Level Security

Users Groups

Add Group

Groups	Read	Write	Share	Delete	Manage	
Human Resources Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

OK

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

6. Then click the **Users** tab.

Manage Folder Level Security

Folder: / /Human Resources/Employee Records

Security Check Access

Permissions

Inherit Folder Level Security

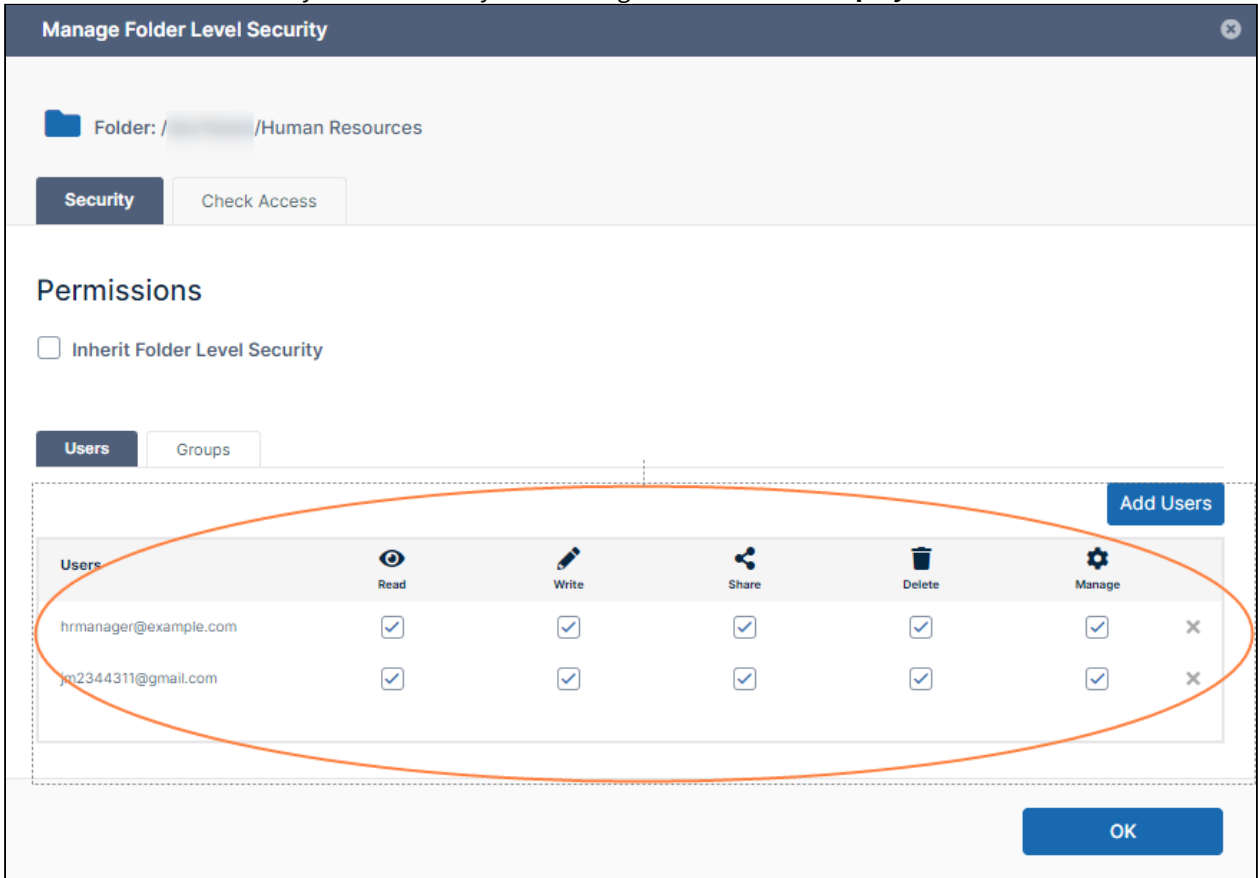
Users Groups

Add Group

Groups	Read	Write	Share	Delete	Manage
Human Resources Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

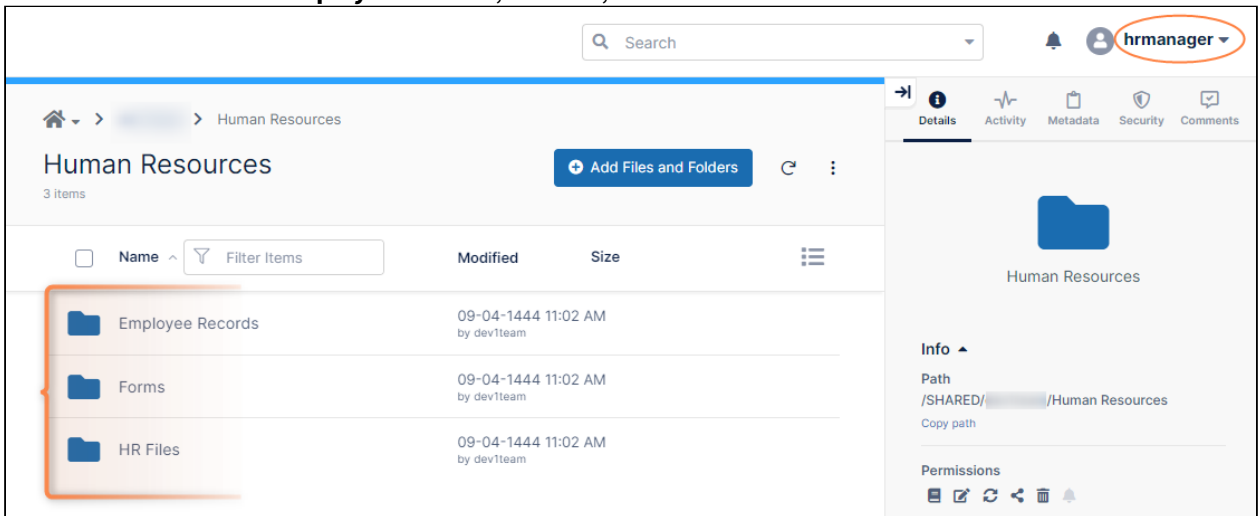
OK

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



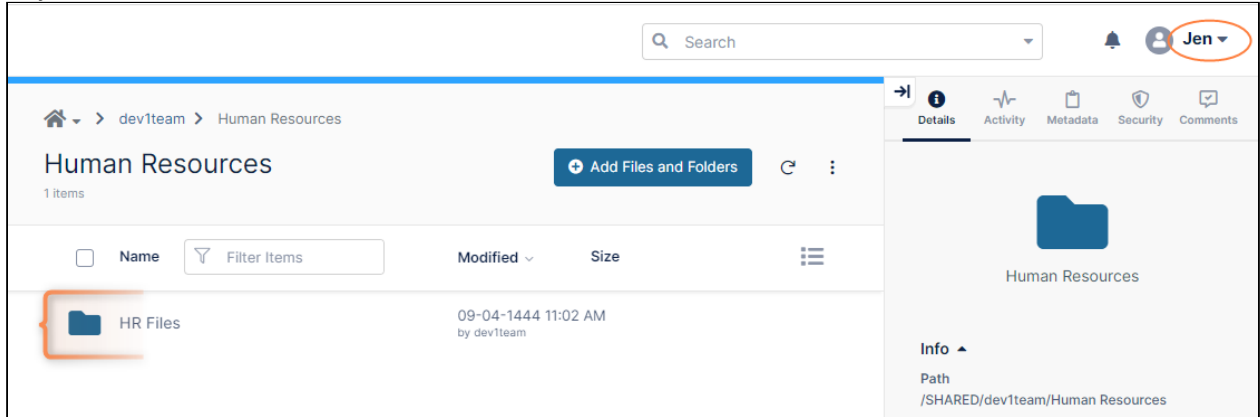
8. Repeat steps 3 through 8 for the **Forms** folder.

Now, when either **HR Manager** or **Jessica** logs in to the user portal, they see the **Human Resources** team folder and all of its sub-folders: **Employee Records**, **HR Files**, and **Forms**.



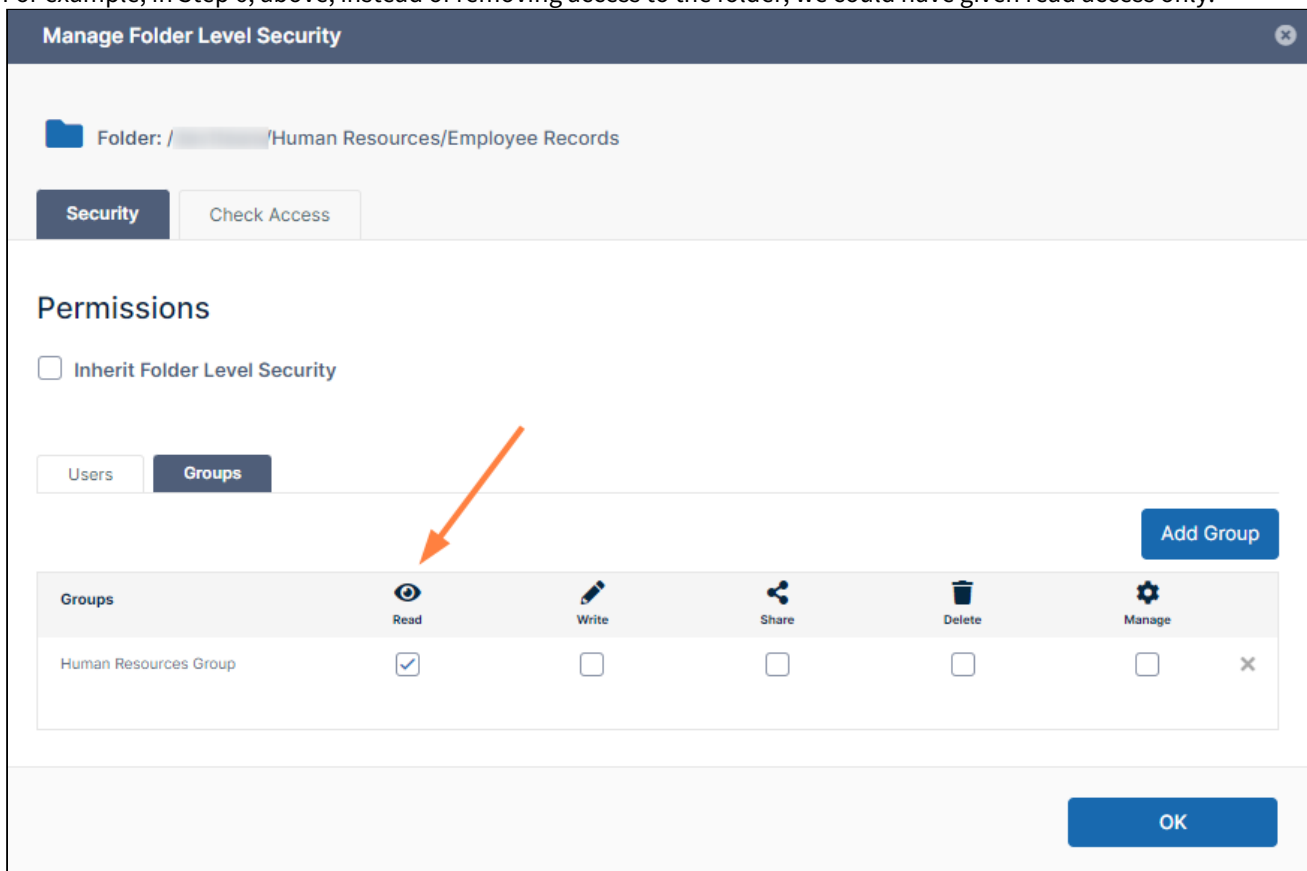
When another member of the **Human Resources** group logs in, they see the **Human Resources** team folder, but

only the **HR Files** sub-folder:



Set special permissions

In the above example, we hid some team folders from most of a group, but we also could have set special permissions. For example, in Step 6, above, instead of removing access to the folder, we could have given read access only:



More Information:

FileCloud Blogs

- [Using “Allow Manage” on FileCloud Team Folders](#)
- [User-Based Management of Team Folder Permissions](#)

Team Folders

- i** 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.
The ability to restore a previous version of a file in Team Folders is available in FileCloud version 18.2 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 \(Optional\)](#)

 <p>Manage Team Folders</p>	<ul style="list-style-type: none">  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 simply 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.

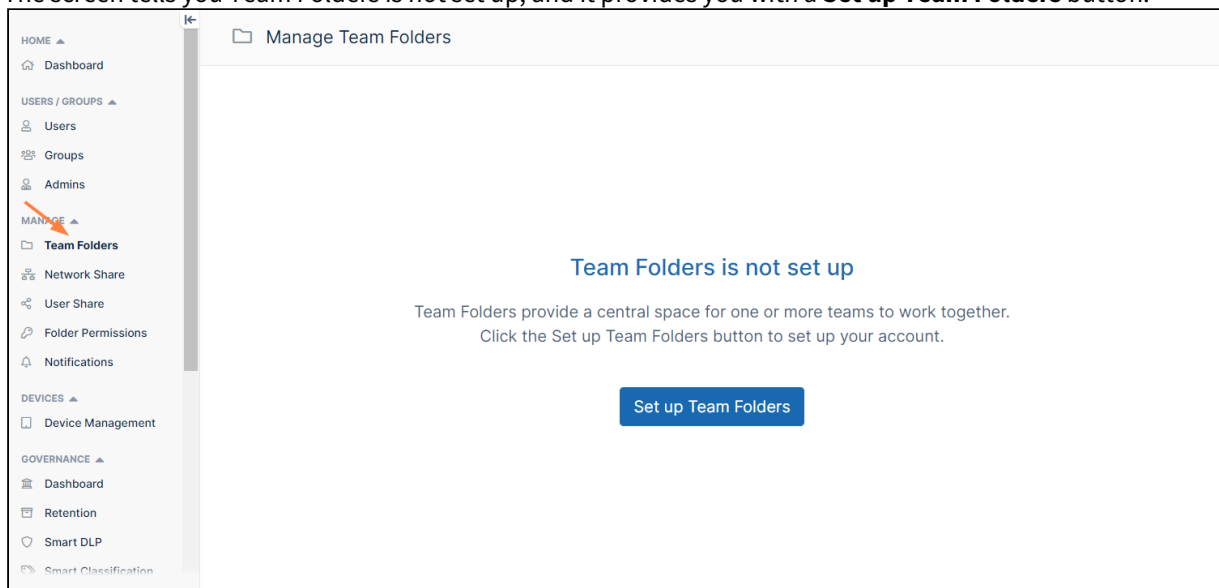
To allow FileCloud to create the Team Folders account

Choose one of the following options:

Create a new account through the Team Folders screen

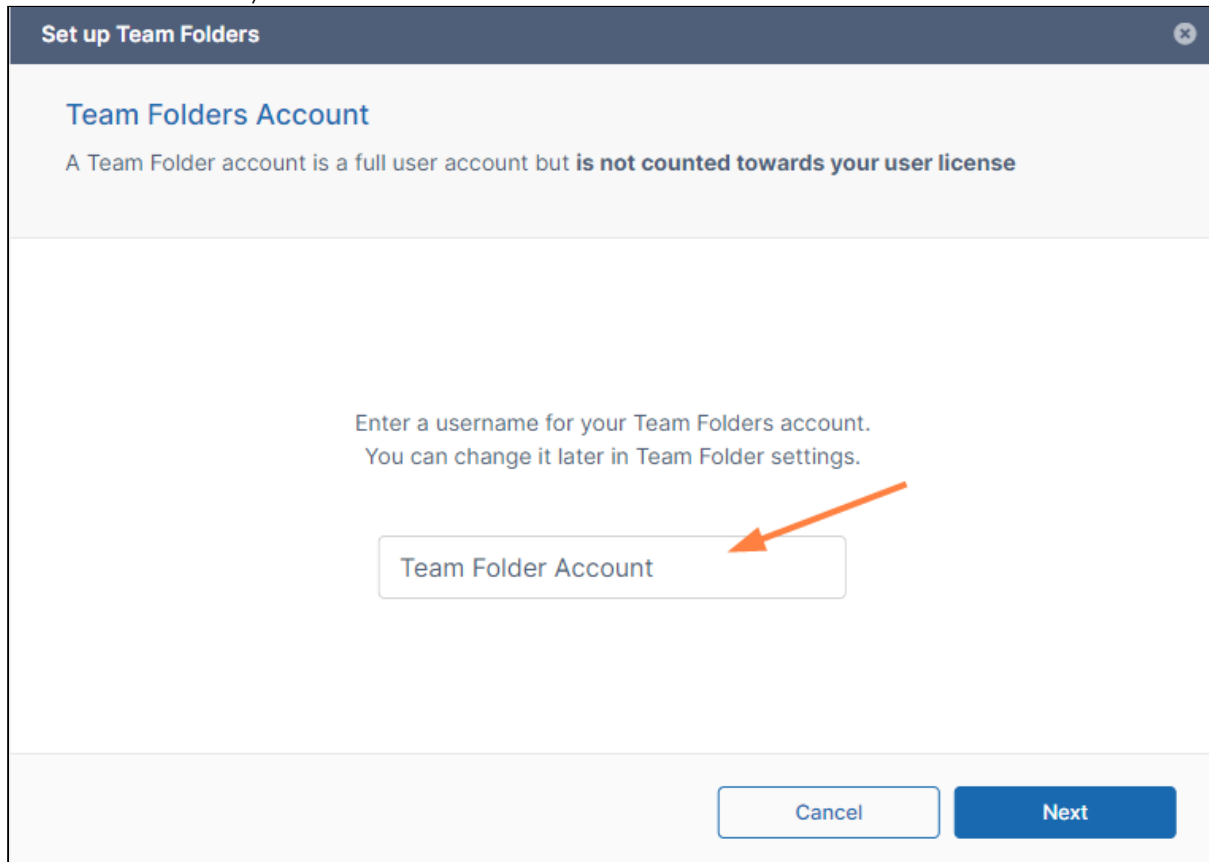
1. In the admin portal's navigation pane, click **Team Folders**.

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**).



Set up Team Folders

Team Folders Account

A Team Folder account is a full user account but **is not counted towards your user license**

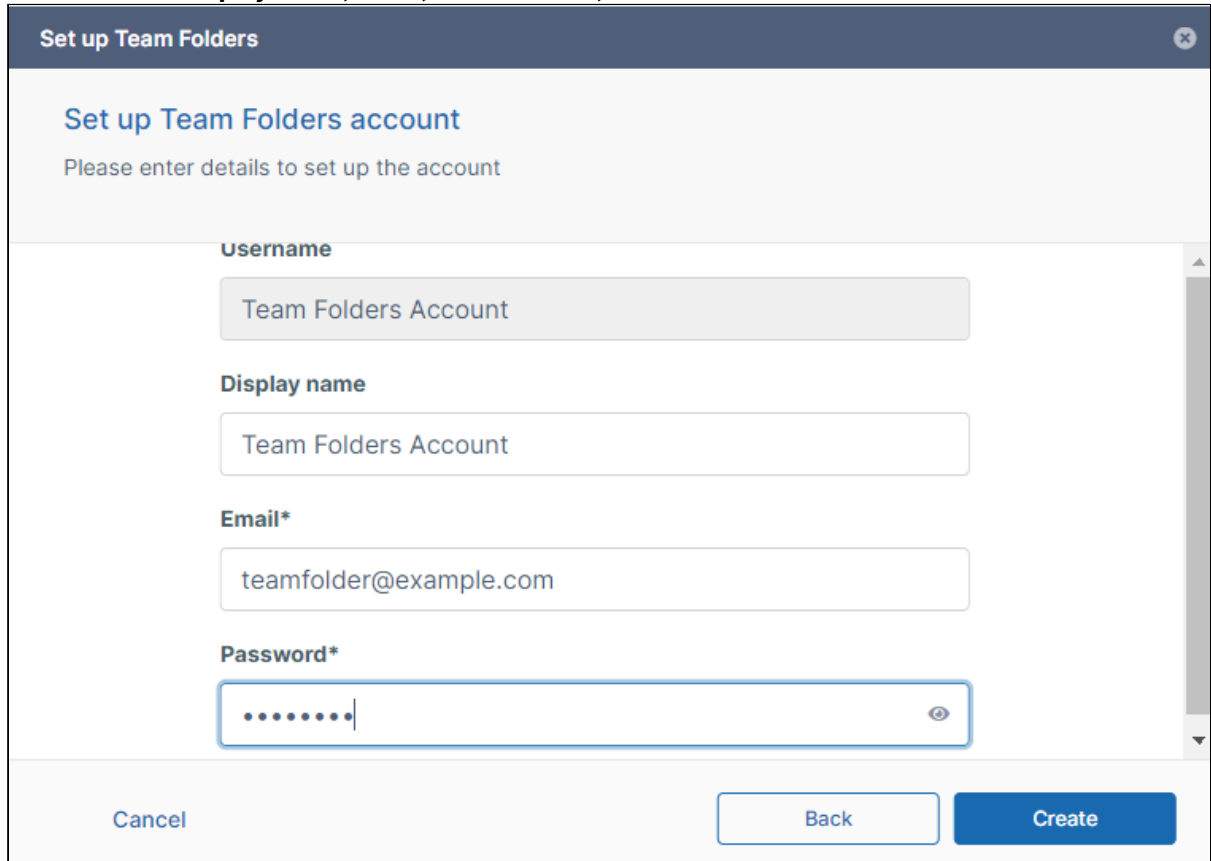
Enter a username for your Team Folders account.
You can change it later in Team Folder settings.

Team Folder Account

Cancel Next

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

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



Set up Team Folders

Set up Team Folders account
Please enter details to set up the account

Username
Team Folders Account

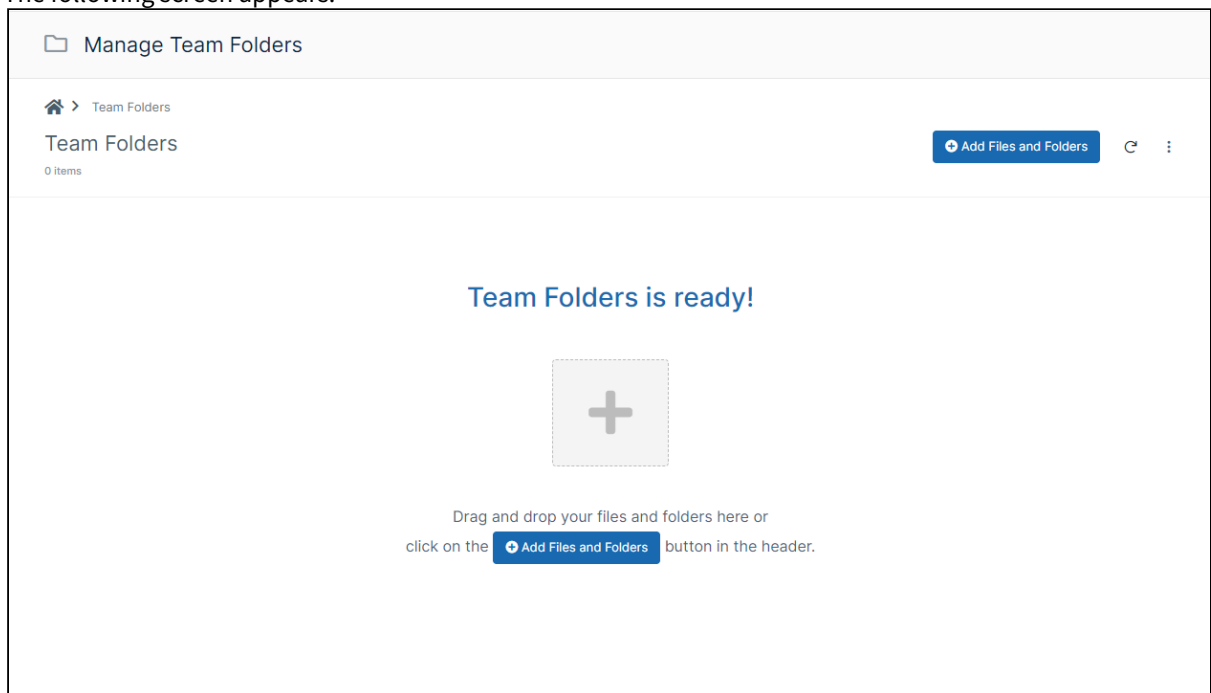
Display name
Team Folders Account

Email*
teamfolder@example.com

Password*
.....

Cancel Back Create

The following screen appears:

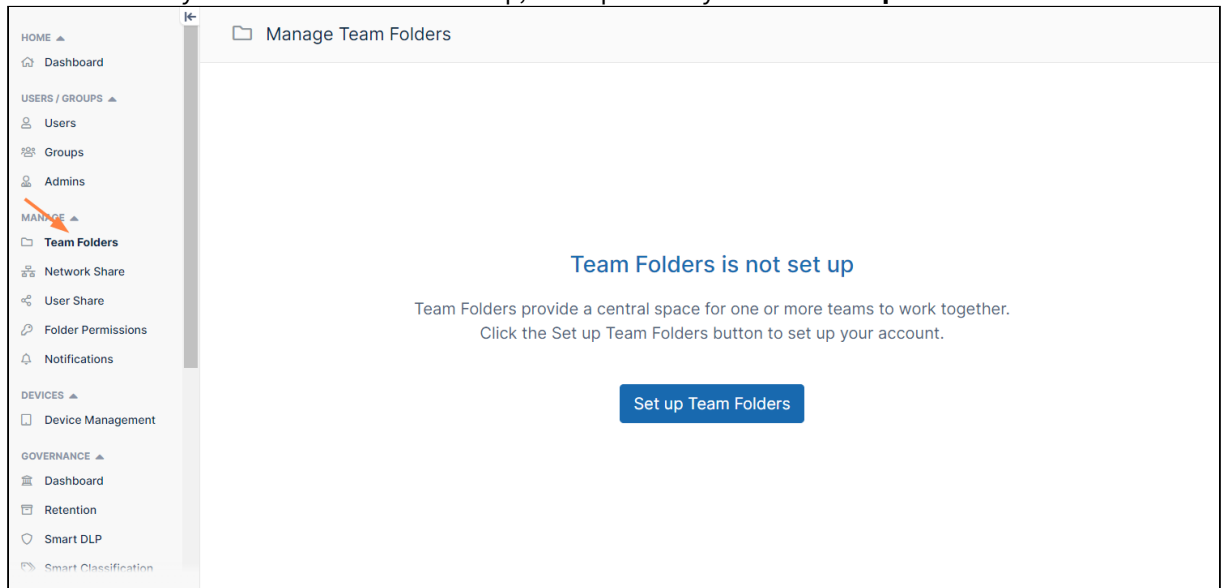


- Now you are ready to create your Team Folders and fill them with contents. You can proceed from where you are by dragging and dropping folders onto the page or by clicking **Add Files and Folders**. This is a good option if you do not already have a folder structure set up that you want to bring into 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

- 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.



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

Set up Team Folders

Team Folders Account

A Team Folder account is a full user account but **is not counted towards your user license**

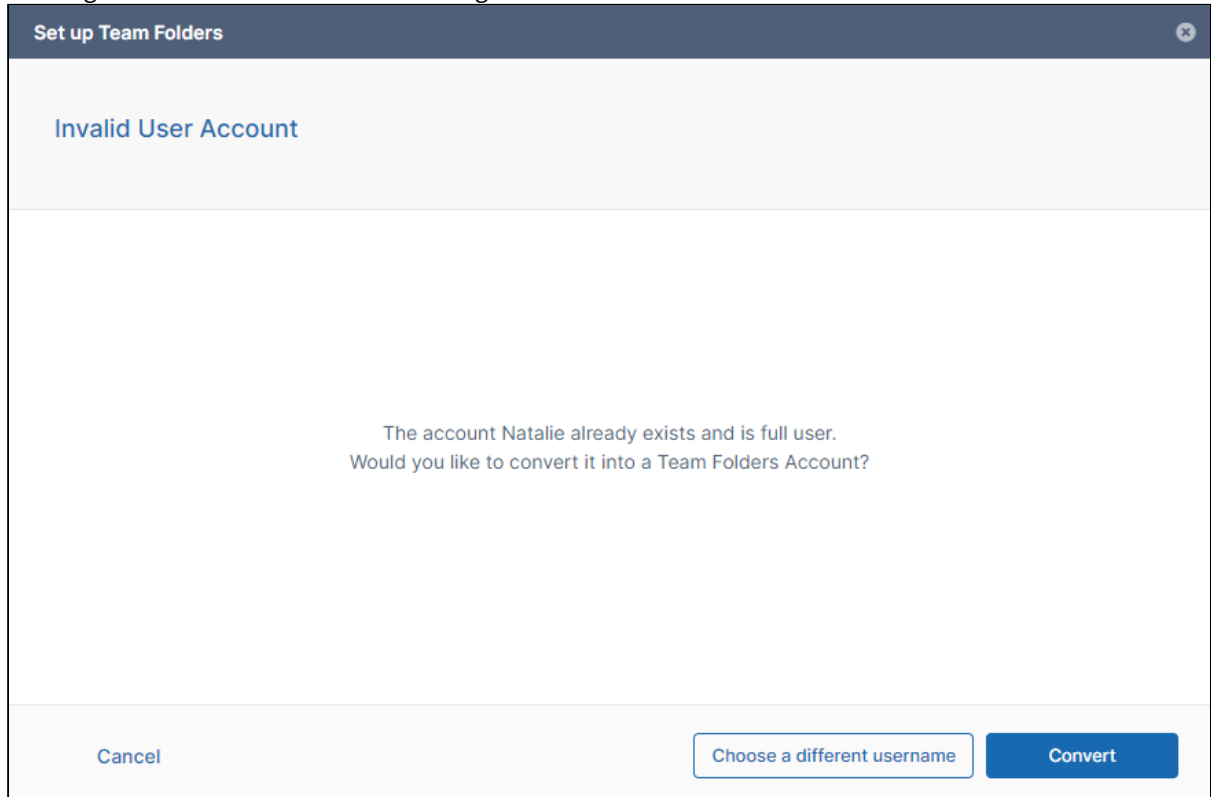
Enter a username for your Team Folders account.
You can change it later in Team Folder settings.

Cancel Next

4. Click **Next**.

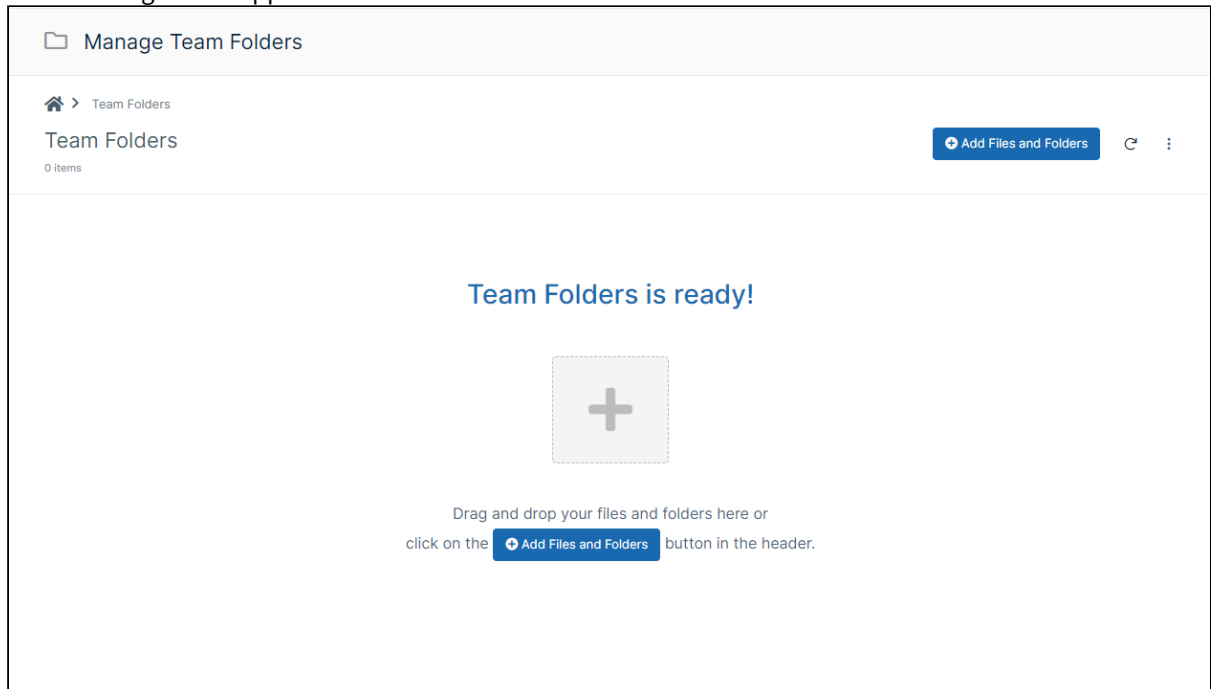
The next window of the wizard indicates that the username already exists, and gives you the option of

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

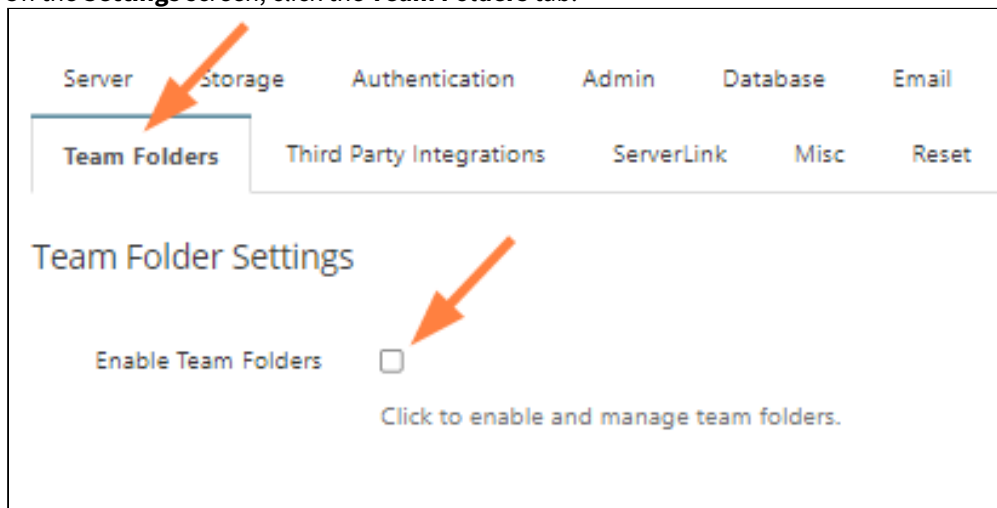
dropping folders onto the page or clicking **Add Files and Folders**. These are good options if you do not already have a folder structure set up that you want to bring into FileCloud as your Team Folders.

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 Settings > Team Folder tab

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

1. Open a browser and log in to the admin portal.
2. From the left navigation panel, click **Settings**.
3. On the **Settings** screen, click the **Team Folders** tab.



4. Click the **Enable Team Folders** checkbox.
The **Set up Team Folder Account** dialog box opens.
5. 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.

The screenshot shows the 'Set up Team Folder Account' dialog box. The 'Enter Team Folder Account Name' field contains the text 'Acct Team Folder', and an orange arrow points to it. There are 'Next' and 'Cancel' buttons at the bottom.

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

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

Set Team Folder Account
✕

User name *

Display Name ←

Password * ←


Email * ←

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.

Team Folder Account Details
✕


Name	team folder account	Total Quota	Unlimited
Email	teamfolder@codelathe.com	Used Quota	0 B
Last Login	--	Available Quota	0 B
TOS Date	Not Accepted	Used Storage	0 B




Manage Shares



Reset Password




Manage Notifications



Delete Account

Profile Image



Email

Secondary Email

Display Name


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.
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.
Account Locked	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: <ul style="list-style-type: none"> • 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 Settings > Team Folder tab

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. Ensure that all Sync apps connecting to your FileCloud site are running version 15.0 or later. Older versions do not sync Team Folders.
2. Open a browser and log in to the admin portal.
3. From the left navigation panel, click **Settings**.
4. On the **Settings** screen, click the **Team Folders** tab.
5. Click the **Enable Team Folders** checkbox.
6. 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.
7. On the **Set Team Folder Account** window, type in the existing **Password** and **Email** for the existing full user.
8. Click **Create**.
9. 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. The following steps must be followed to seed data using the Sync Client

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.

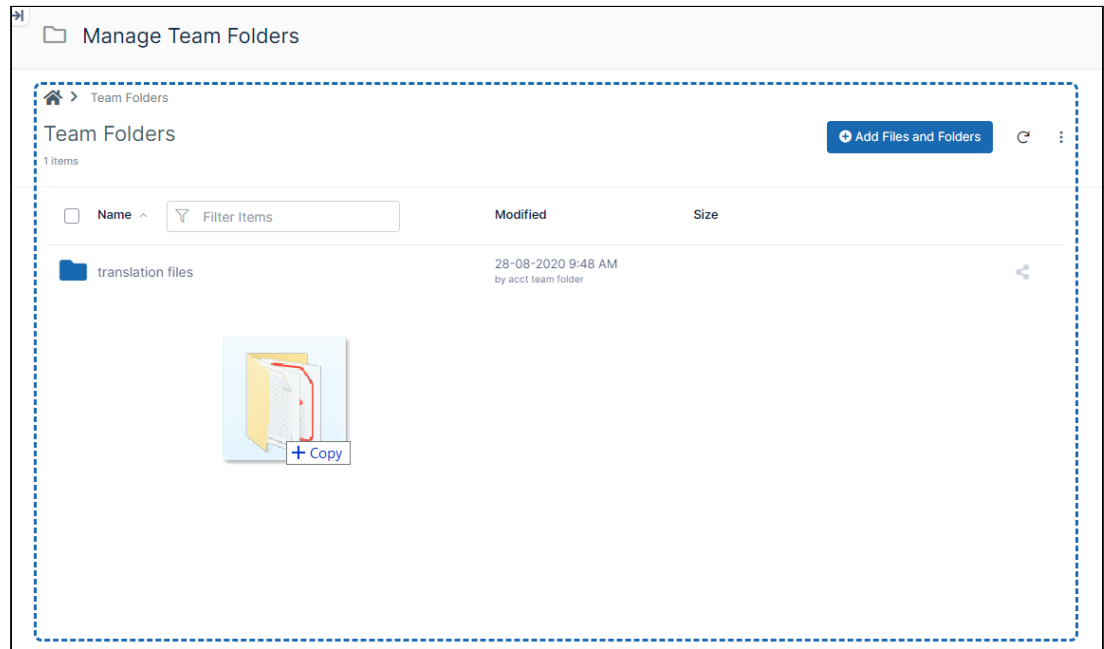
Now, log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Admin Portal

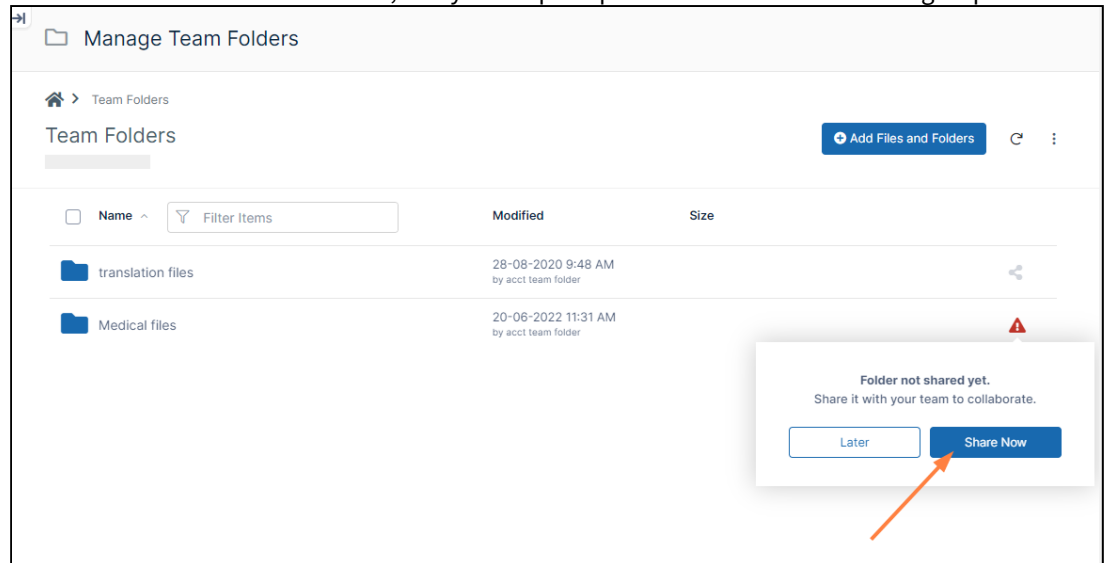
Go to the **Team Folders** page in the admin portal to create Team Folders and seed them with files.

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.



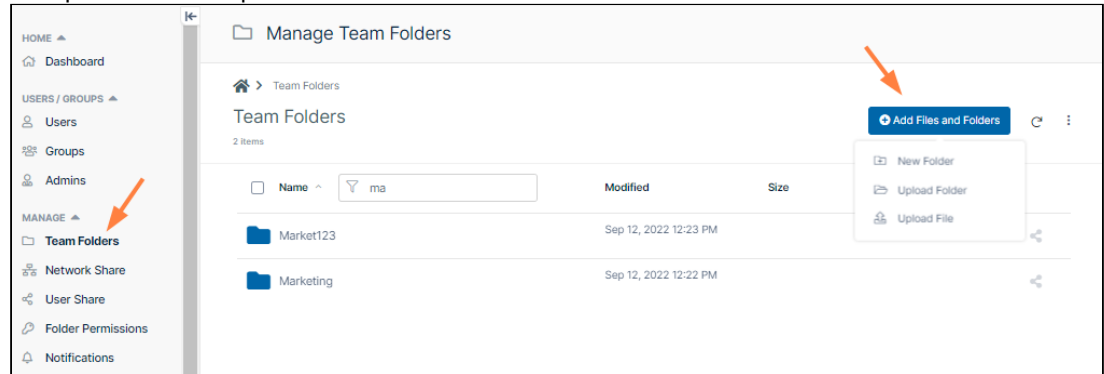
- b. The folder becomes a Team Folder, and you are prompted to share it with users or groups.



- 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

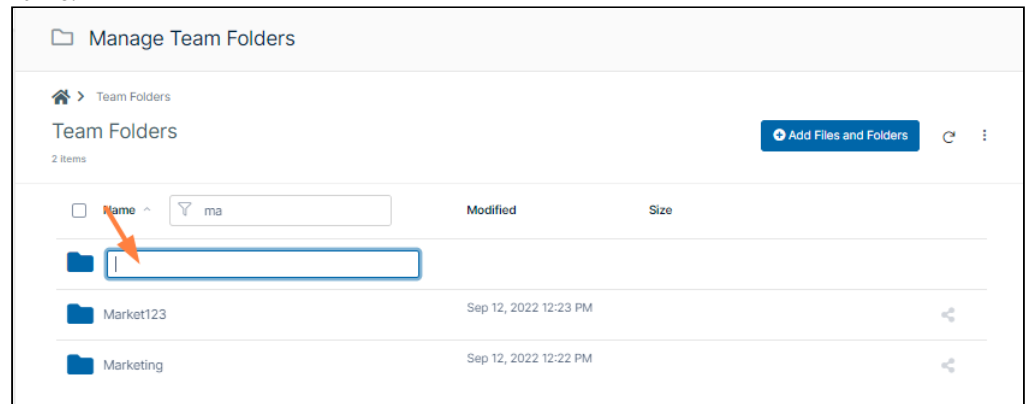
- a. Click the **Add Files and Folders** button.
A drop-down menu opens.



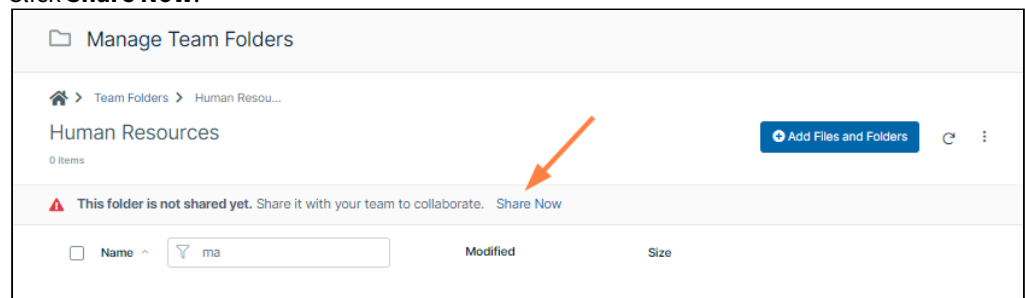
- b. Either choose **New Folder** to create a new Team Folder, or click **Upload Folder** to upload an existing folder (with or without contents) and make it a Team Folder.

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**.

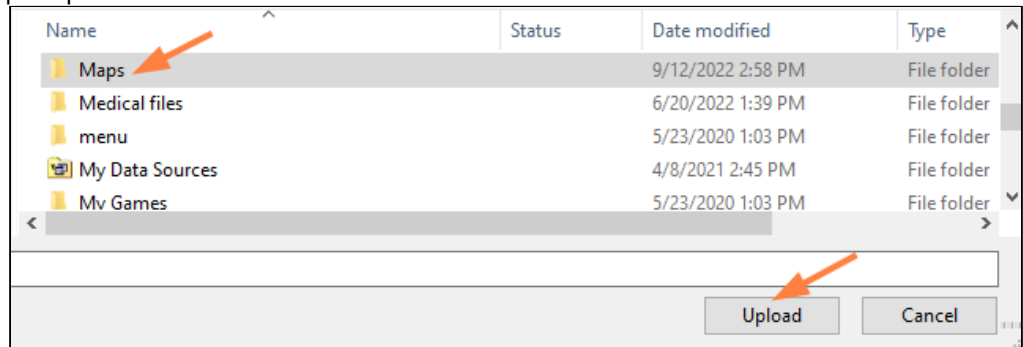


A share dialog box opens.

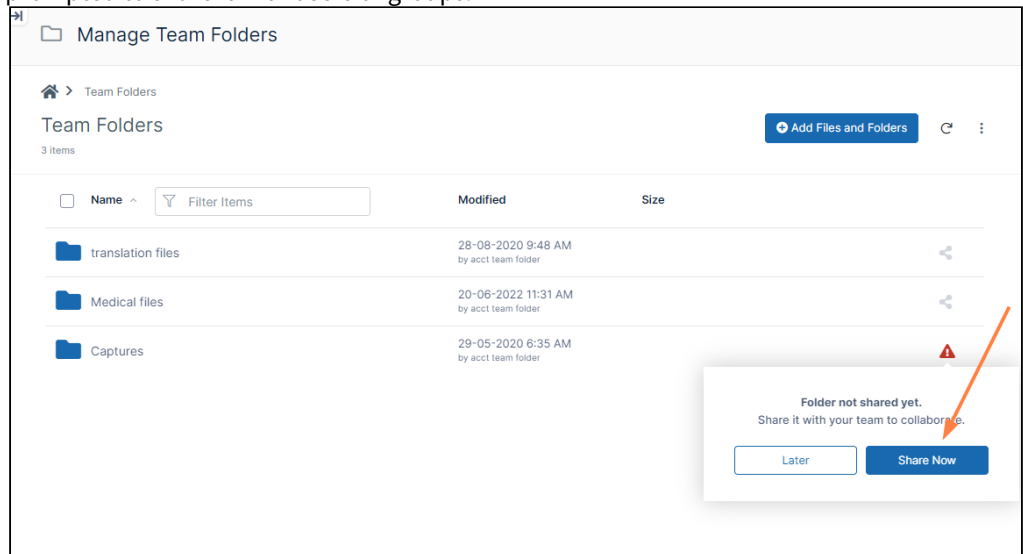
- To share the folder with users, see [Share the Team Folder and Set Permissions](#).
- To add contents to the folder, drag and drop them into the folder or click the **Add Files and Folder** button and select them from your file system.

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 23.1, by default, you can no longer share a top-level Team Folder publicly. To enable public sharing, please [Contact FileCloud Support](#).

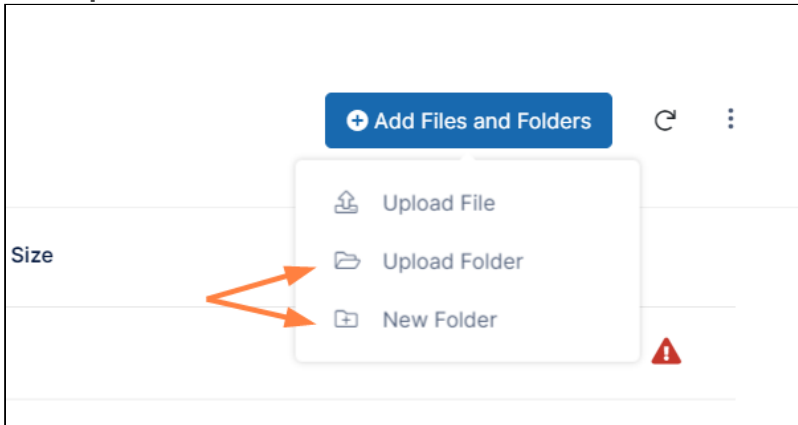
You must share Team Folders before users can access them.

- 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.
- From the admin portal, Team Folders can't be shared with external accounts; from the user portal, [full access accounts](#) can share Team Folders with external accounts.

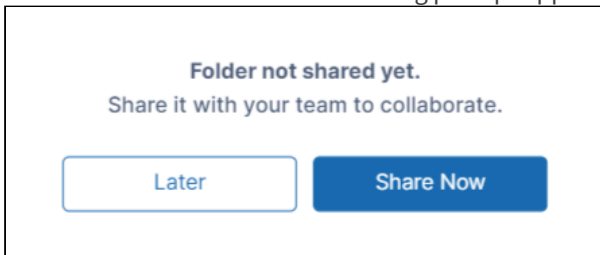
You can share a Team Folder when you add it or at a later time.

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**.

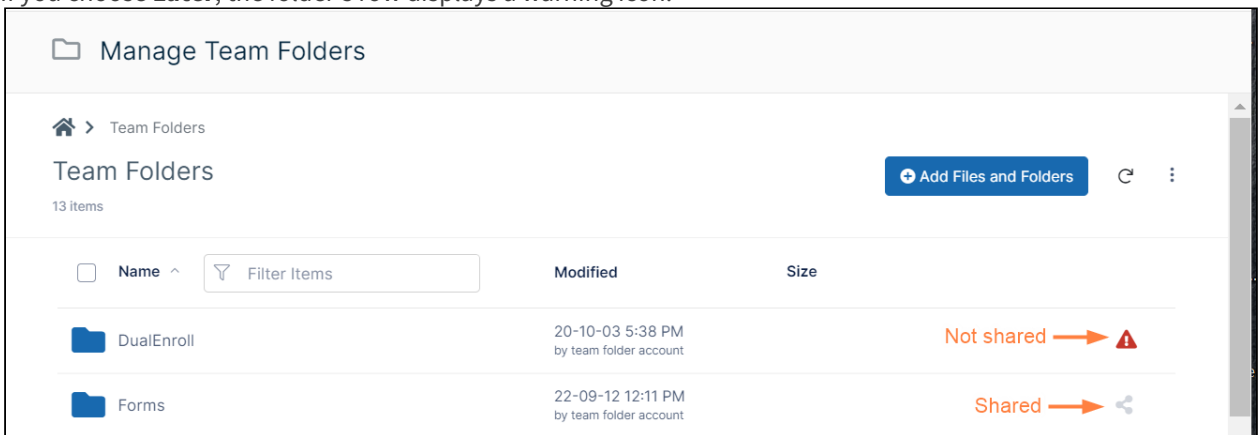


When the folder is added the following prompt appears:



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.



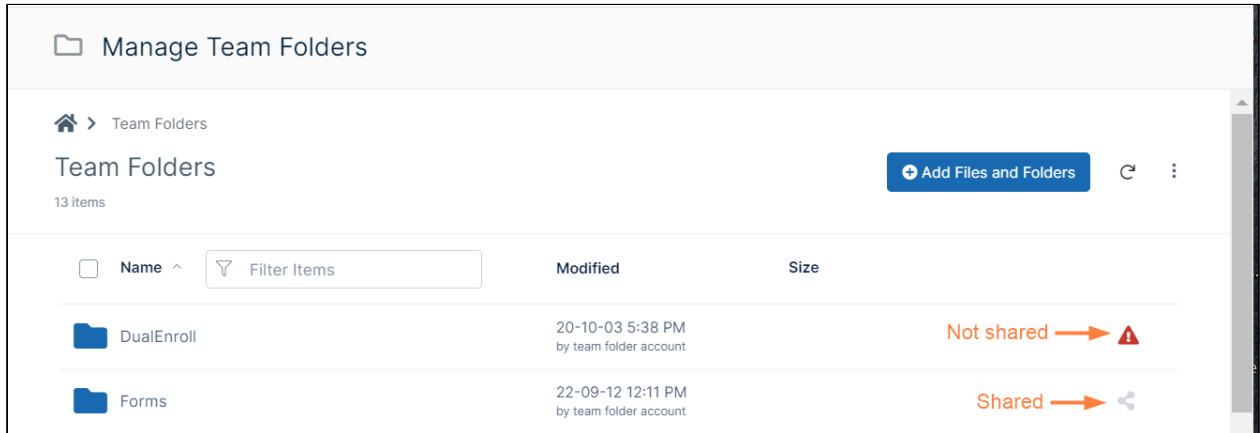
If you choose **Share Now** a **Share link for folder** dialog box opens.

4. To configure the share, see [To complete the Team Folder share](#), below.

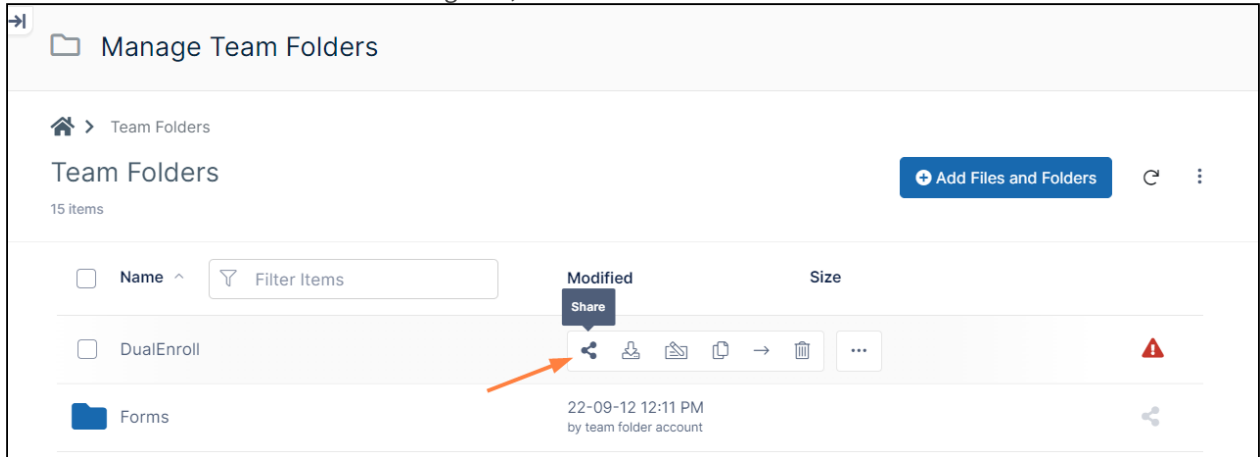
To share an existing Team Folder:

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

- 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.



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



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

- To configure the share, see [To complete the Team Folder share](#), below.

To complete the Team Folder share:

- 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.

Share link for folder DualEnroll
✕

Share Link

Modify Link

📄
🔗
✉️

Shared Folder
/team folders user/DualEnroll

Share Options

Share History

Share Name: For Review Change

Expires: Never Expires

Upload Size Limit (MB): Unlimited Limited Save

Send Email Notifications: Yes

Allow selected users or groups

Users

Groups (1)

👤 Add Group

Sharing Permissions:

Group	View	Download	Upload	Share	Sync	Delete	Manage
ProjectTeam	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> ✕

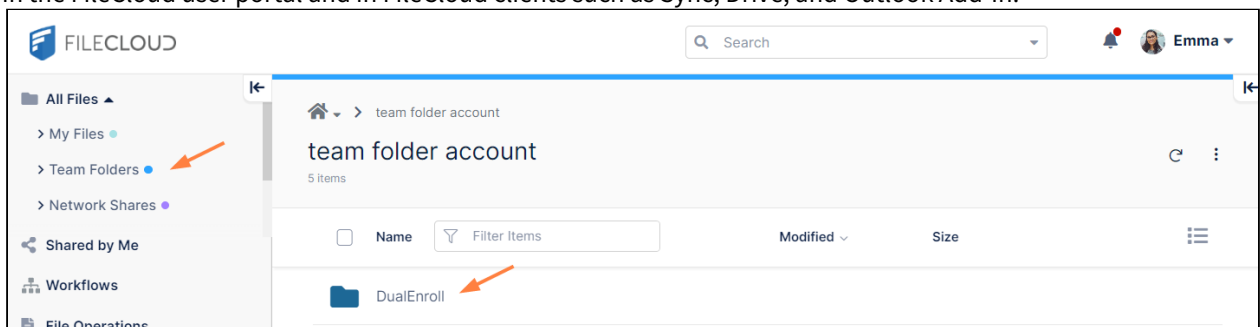
Remove Share
OK

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](#).

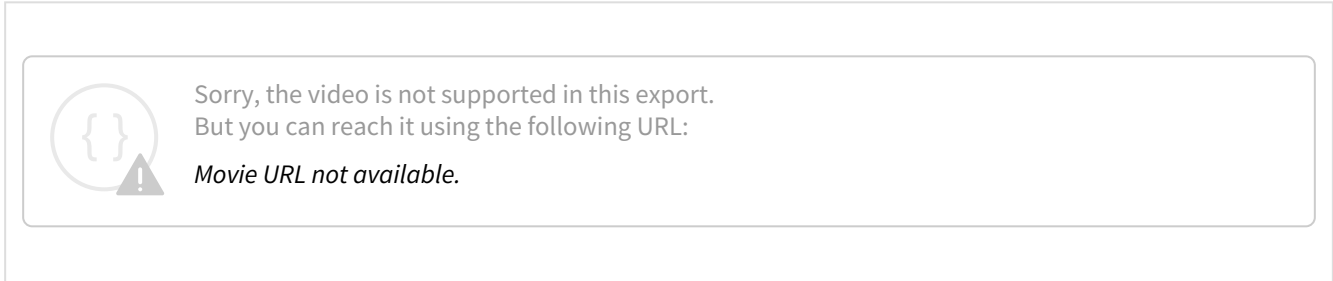
Note: You cannot share a top-level Team Folder publicly,

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.



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:



Search for a Team Folder

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

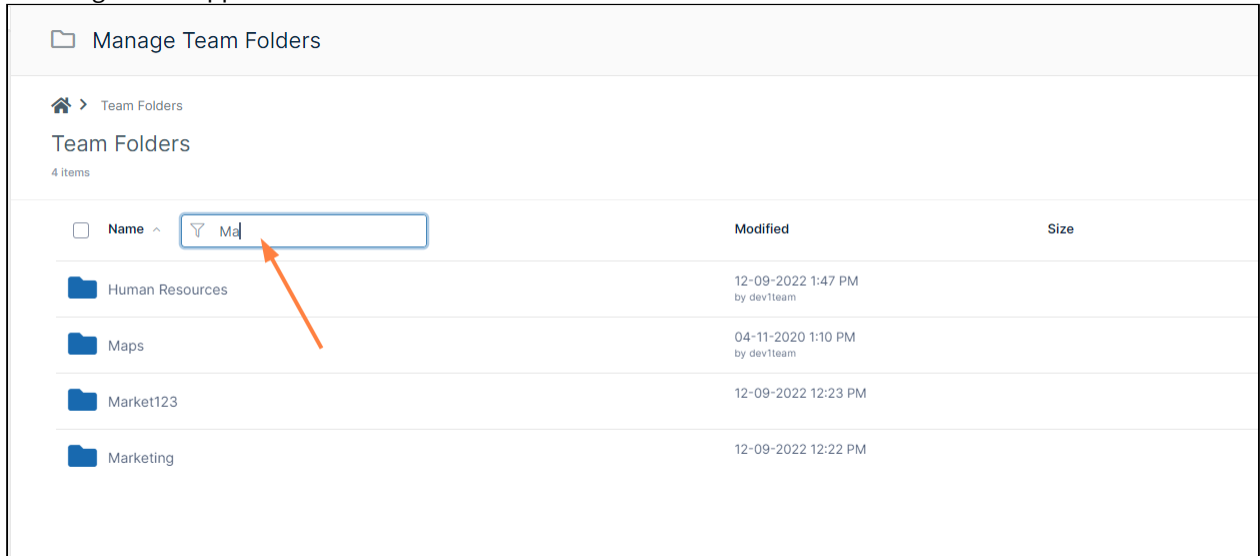
If you manage so many Team Folders that you have to look through multiple pages of folder listings to find a Team Folder, you can use the search box to find the folder you need quickly.

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

To search for a Team Folder:

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

Matching folders appear in the Team Folders list.



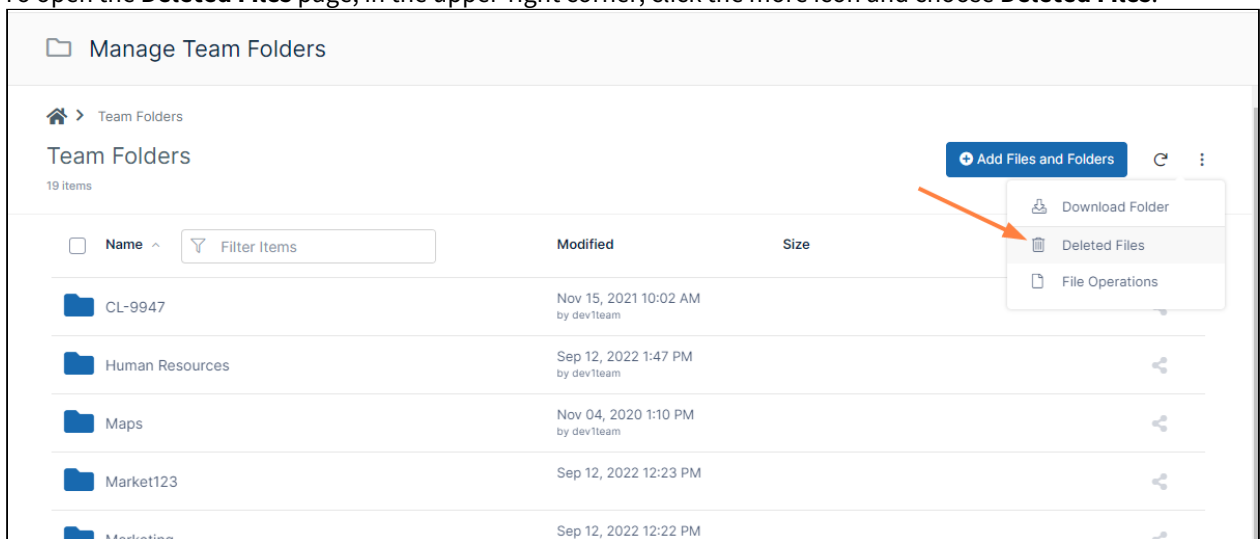
Recover Deleted Files

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

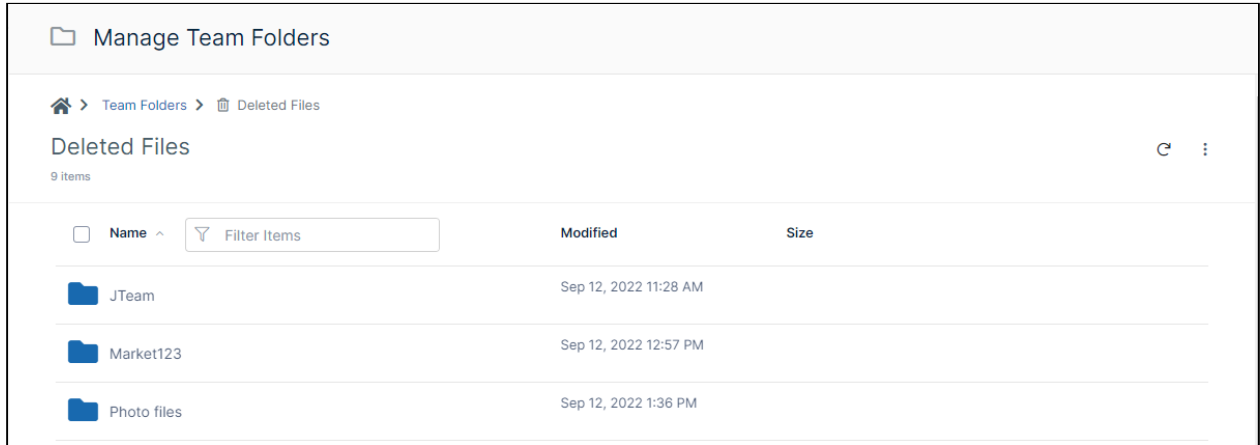
After you delete files and folders, they are placed in the Team Folder's recycle bin so that they can be recovered if deleted by mistake or are needed again at a later time.

To recover a deleted folder or file:

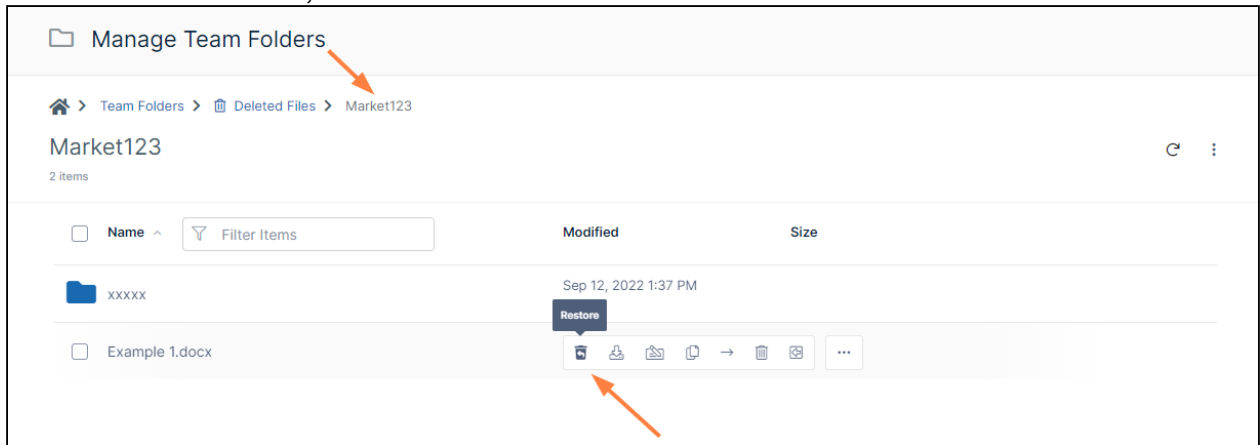
1. Open a browser and log in to the admin portal.
2. In the navigation panel, click **Team Folders**.
3. To open the **Deleted Files** page, in the upper-right corner, click the more icon and choose **Deleted Files**.



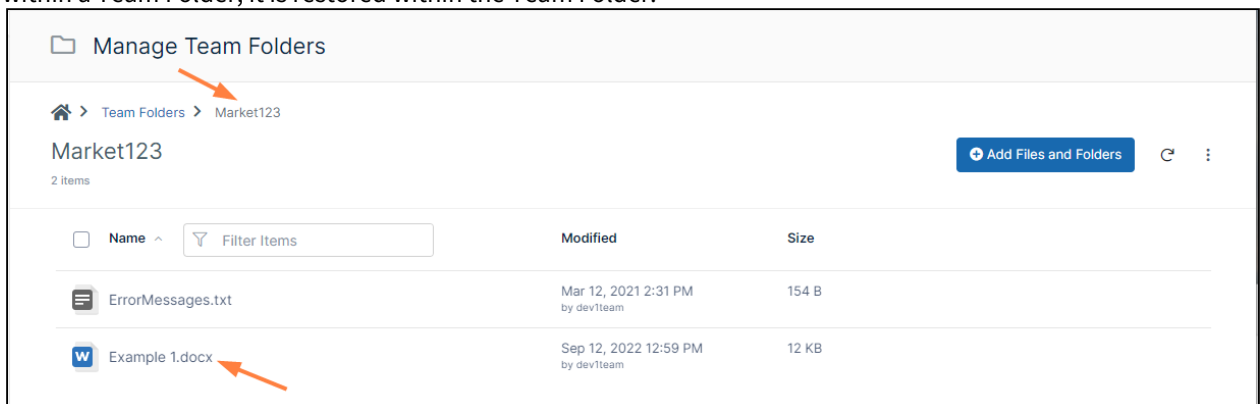
The **Deleted Files** screen opens. The top level of folders includes deleted team folders as well as non-deleted parent team folders of deleted files. For example, in the following screenshot, the **JTeam** and **Photo files** team folders are deleted team folders, but the **Market123** team folder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



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



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



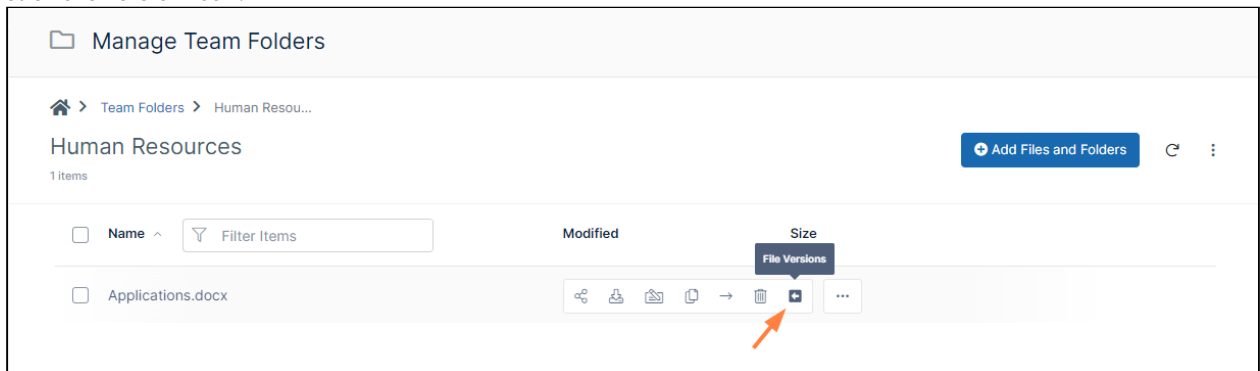
View and Restore Previous Versions in Team Folders

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

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

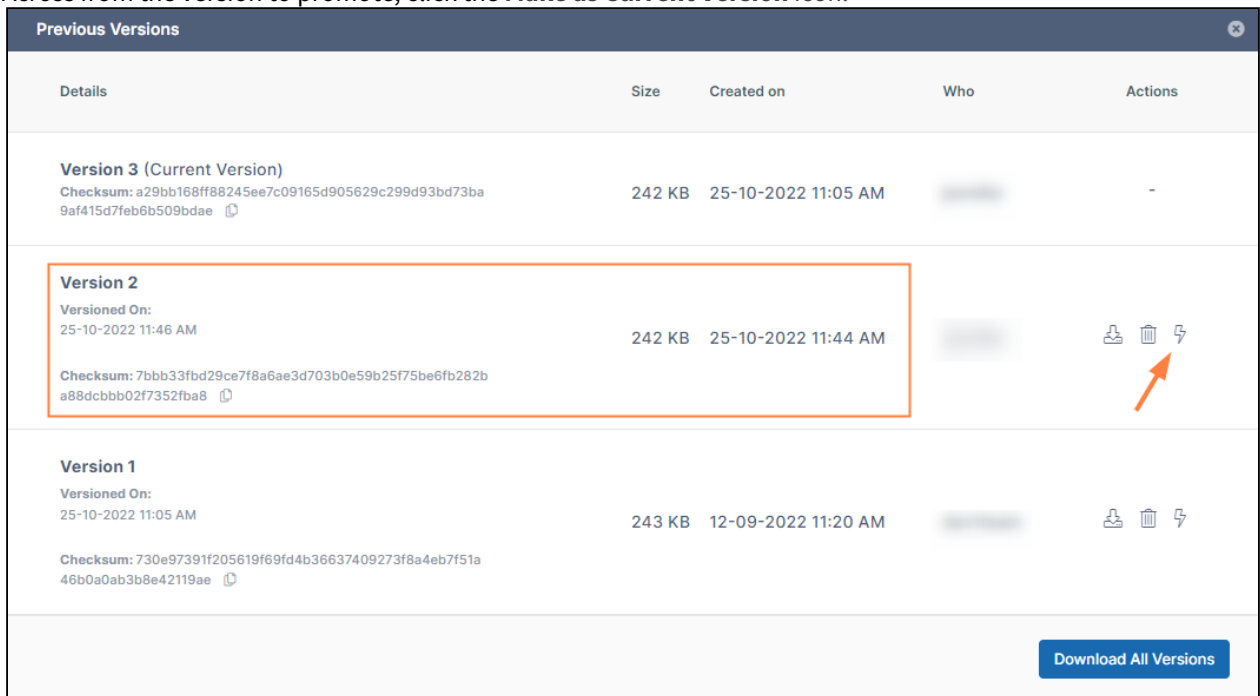
To restore a previous version of a file in Team Folders:

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

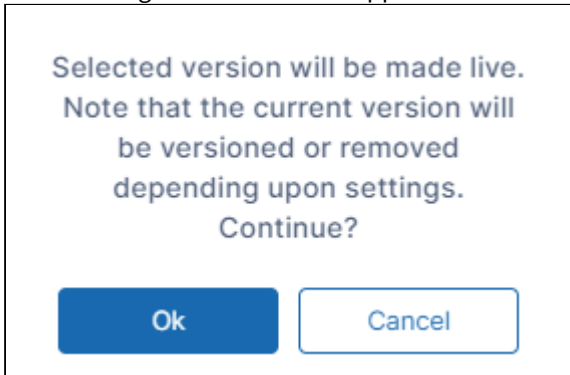


A list of the previous versions opens.

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



The following confirmation box appears:



6. Click **OK**.

The version that was made the current version now appears at the top, and the previous current version appears under it.

(Note that above, the 11:44 AM version was Version 2, but below, after it was made the current version, it is Version 3 at the top of the list.)

Previous Versions				
Details	Size	Created on	Who	Actions
Version 3 (Current Version) Checksum: 7bbb33fbd29ce7f8a6ae3d703b0e59b25f75be6fb282ba88dcbbb02f7352fba8	242 KB	25-10-2022 11:44 AM		-
Version 2 Versioned On: 25-10-2022 11:50 AM Checksum: a29bb168ff88245ee7c09165d905629c299d93bd73ba9af415d7feb6b509bdae	242 KB	25-10-2022 11:05 AM		
Version 1 Versioned On: 25-10-2022 11:05 AM Checksum: 730e97391f205619f69fd4b36637409273f8a4eb7f51a46b0a0ab3b8e42119ae	243 KB	12-09-2022 11:20 AM		

[Download All Versions](#)


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

To view and restore previous versions of files in the user portal, see [View Previous Versions Of Files](#)

User Settings

As an administrator, you can use your FileCloud Server site to provide a place for your users to store and share files.

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












 Administrators can not create a user with an account with a name of Admin or superadmin in FileCloud Server version 19.1 and later.

- In previous versions, an administrator could create a new user with an account name of **admin** or **superadmin**.
- However, when a user opens a browser and tries to log in to the *User Portal* with an account name of **admin**, the user gets an error that this is an invalid username.
- The user sees an error that says: *You are trying to login into user portal with admin account.*
CLFC-00035-00116

FileCloud Server has been modified to prevent an administrator in the *Admin Portal* from creating a user with the following names:

- **admin**
- **superadmin**

The administrator will receive an error that these names are not valid.


Add User Accounts	<ul style="list-style-type: none">  Create or Import New Accounts  Allow Users to Create Accounts
Configure User Authentication	<ul style="list-style-type: none">  User Authentication Settings  Enabling Default Authentication  Active Directory Authentication  Connecting to AD via SSL  Using Single Sign-On
Integrate with other User Directory Solutions	<ul style="list-style-type: none">  Integrate Azure AD with FileCloud  Integrate Centrify with FileCloud  Integrate Okta with FileCloud  Integrate OneLogin with FileCloud


Manage User Accounts	<ul style="list-style-type: none"> ➔ Migrate data after an account name change ➔ Changing the Storage Quota for Users ➔ Enable WebDAV ➔ 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.

 Administrators cannot create a user with an account name of `admin` or `superadmin` in FileCloud version 19.1 and later.

- In previous versions, an administrator could create a new user with an account name of `admin` or `superadmin`.
- However, when a user opened a browser and tried to log in to the user portal with an account name of `admin`, the user was unable to log in and saw the following invalid username error:
You are trying to login into user portal with admin account. CLFC-00035-00116

FileCloud has been modified to prevent an administrator from creating a user with the following names:

- `admin`
- `superadmin`

The administrator is sent an error that these names are not valid.


In this section

- [User Access Levels and User Types](#)
- [Manually Create a New User Account](#)
- [Video of Adding FileCloud Server User Account](#)
- [Bulk creation of User Accounts from a CSV File](#)
- [Import a user account from AD or LDAP Service](#)
- [Bulk Import User Accounts from AD Server](#)

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.	<p>The default Admin account is used to manage the FileCloud.</p> <p>The default admin user account is 'admin'. Other users can be marked as 'admins' and given limited set of permissions.</p> <p> Read more about Multiple Admins</p>
Full Access	Control over its own private cloud storage space in My Files.	<p>These user accounts can:</p> <ul style="list-style-type: none"> • 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.	<p>These user accounts:</p> <ul style="list-style-type: none"> • 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
External Access	Access to FileCloud only through a Web browser.	<p>These user accounts:</p> <ul style="list-style-type: none"> • 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
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

User Access Feature	Full Access	Guest Access	External Access
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	Only via shares created by users
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 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.

	User name	Display Name	Email	Last Login	Status	Actions
	aliah	Aliah	aliahp@example.com	25 Jul 2022 13:46	Full Access	
	brianna	Brianna	brianna@example.com	16 Feb 2022 14:31	Guest Access	
	briano	Brianna	briano@example.com	--	Disabled Access	

Manually Create a New User Account

i 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**.

The screenshot shows the 'Manage Users' interface. On the left, a navigation menu includes 'HOME', 'Dashboard', 'USERS/ROUPS' (with 'Users' selected), 'Groups', 'Admins', and 'MANAGE' (with 'Team Folders'). The main area is titled 'Manage Users' and features a search bar, filters, and a table of users. The 'Add User' button is highlighted with an orange arrow.

	User name	Display Name	Email	Last Login	Status	Actions
	aliah	Aliah	aliahp@example.com	25 Jul 2022 13:46	Full Access	[Edit] [Settings] [Delete]
	brianna	Brianna	brianna@example.com	16 Feb 2022 14:31	Guest Access	[Edit] [Settings] [Delete]
	briano	Brianna	briano@example.com	--	Disabled Access	[Edit] [Settings] [Delete]

4. Set the required account information.

Add User
✕

Authentication

Default Authentication ▼

Access Level

Full (Licensed Account with storage) ▼

User name *

Keira Walsh

Display Name

Keira

Password *

••••••

Email *

kwalsh@site.com

Send Email Notification

Include Password in Email

Create

Close


Settings	Description
Authentication	<p>Allows you to select the authentication type for granting access into the system.</p> <ul style="list-style-type: none"> • 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	<p>Allows you to select the user type. A user account with Full or Guest access counts as a license.</p>

Settings	Description
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 .
Display name	Name that appears on user interface
Password	Password for the user (Should adhere to password length and strength requirements for your organization)
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.


-  When you create multiple accounts at one time, all accounts will initially have the follow settings:
- Default Authentication
 - Status: [Guest Access](#) (user account type)
 - Email Verified: YES (allow users to immediately log in with their passwords)

As the Administrator, you can change the authentication and access level once the user account is created.

Format of CSV file for creating user

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

CSV import format	
UserName, EmailID, Password, DisplayName, Status, ExpirationDate, Groups, EmailVerified	
Field	Description
UserName	The user id.
EmailID	A unique email id to be associated with the user.
Password	Password for the user. Must follow password requirements (minimum length, etc.)
DisplayName (optional)	The name that appears in the user interface for the user. Default is same as UserName.
Status (optional)	The user's account type (access level). Options are Guest Full External . Default is Full.
ExpirationDate (optional)	The date the user account will expire. Default is none.
Groups (optional)	The group or groups the user belongs to. If there are multiple groups, separate them with the character. Default is none. Note: FileCloud can only recognize group names if you do not insert spaces between the group names and the characters: <ul style="list-style-type: none"> Valid: EVERYONE GROUP 1 GROUP 2 Invalid: EVERYONE 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.

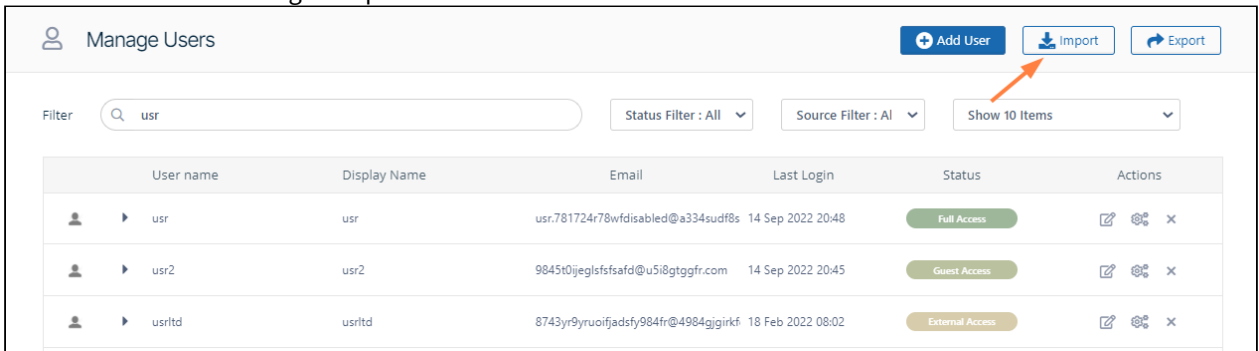
 Below is a sample csv file for import.

1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified
2	jessicam	jm2344311@example.com	password	Jessica	FULL		EVERYONE Human Resources Group	YES
3	david	dm898002@example.com	password	david	FULL		EVERYONE	YES
4	jaredtaylor978	jaredtaylor978@example.com	password	Jared	GUEST		EVERYONE Human Resources Group Marketing	YES
5	aliah	aliahp@example.com	password	Aliah	FULL		EVERYONE	YES
6	hr manager	hrmanager@example.com	password	HR Manager	FULL		EVERYONE	YES

Importing a CSV File

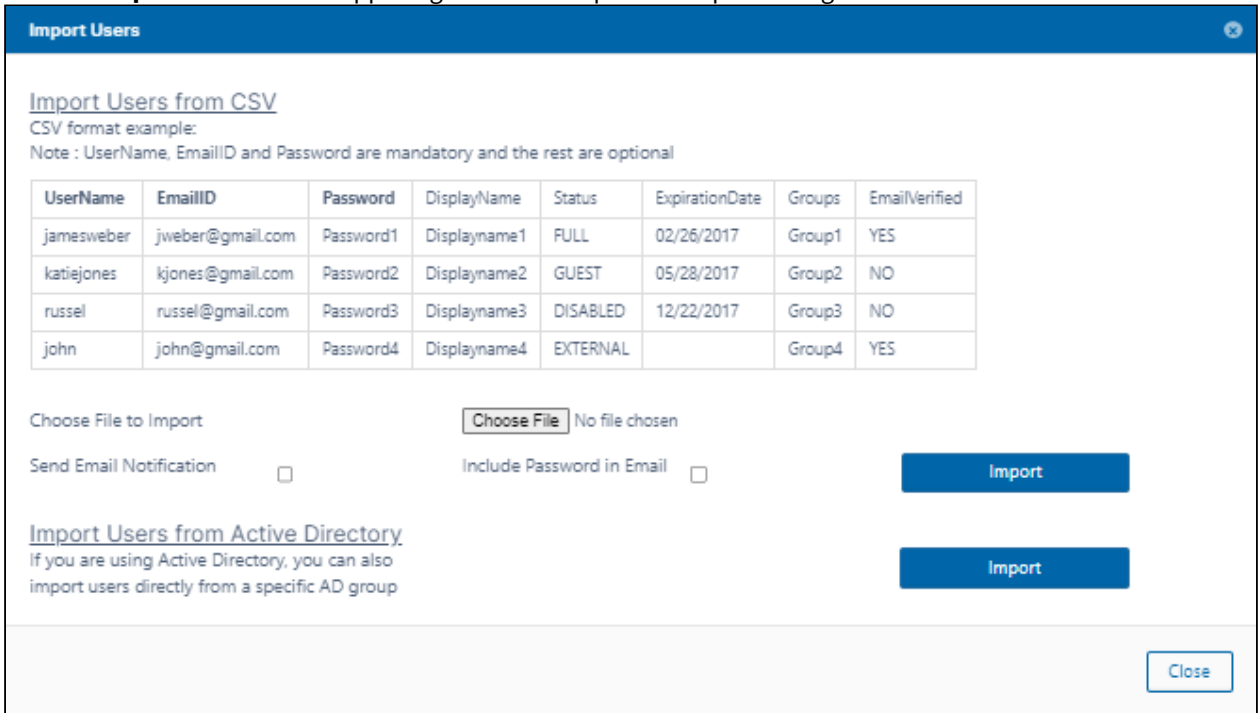
To import a CSV File:

1. Log on to the [Administration Portal](#)
2. Click **Users** in the left navigation panel.



The screenshot shows the 'Manage Users' interface. At the top right, there are three buttons: 'Add User', 'Import', and 'Export'. The 'Import' button is highlighted with an orange arrow. Below the buttons, there is a search filter with the text 'usr', a 'Status Filter' dropdown set to 'All', a 'Source Filter' dropdown set to 'All', and a 'Show 10 Items' dropdown. The main content area displays a table of users with columns for User name, Display Name, Email, Last Login, Status, and Actions. The table contains three rows of user data.

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



The screenshot shows the 'Import Users' dialog box. The title bar says 'Import Users'. Below the title bar, there is a section titled 'Import Users from CSV' with a sub-section 'CSV format example:'. A note states: 'Note : UserName, EmailID and Password are mandatory and the rest are optional'. Below the note is a table showing the CSV format example with columns: UserName, EmailID, Password, DisplayName, Status, ExpirationDate, Groups, and EmailVerified. The table contains four rows of user data. Below the table, there is a 'Choose File to Import' section with a 'Choose File' button and the text 'No file chosen'. There are two checkboxes: 'Send Email Notification' (unchecked) and 'Include Password in Email' (unchecked). At the bottom right, there is a 'Close' button. There are also two 'Import' buttons, one for the CSV import and one for the Active Directory import.

4. Click **Choose File**, and select the CSV file containing the entries of users to be created.

- 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**.
- 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	Authentic	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

- Log on to [Administration Portal](#).
- Set up [AD configuration](#) or [LDAP configuration](#) depending on your requirements.
- Click **Users** on the left navigation panel.
- Click **Add User** button.
- Select **Active Directory** or **LDAP** as the authentication type.
- 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

Manage Users

Filter Status Filter Source Filter Show 10 Items

	User name	Display Name	Email	Last Login	Status	Actions
	aliah	Aliah	aliahp@example.com	25 Jul 2022 13:46	Full Access	
	brianna	Brianna	brianna@example.com	16 Feb 2022 14:31	Guest Access	
	briano	Brianna	briano@example.com	--	Disabled Access	

Add User

Authentication

Access Level

User name

Password

Email

Send Email Notification

Include Password in Email

Bulk Import User Accounts from AD Server

⚠ When importing user accounts from AD groups into FileCloud Server, some AD groups that cannot be imported are still listed.

- These AD groups are built-in to perform tasks.
- In the Windows Server operating system, there are several built-in accounts and security groups that are preconfigured with the appropriate rights and permissions to perform specific tasks.

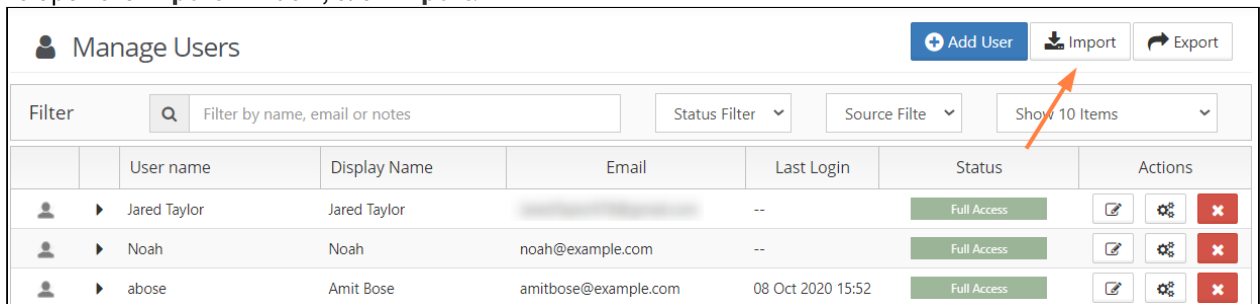
FileCloud Server version 19.1 and later has been modified to stop displaying built-in AD groups that cannot be imported.

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:

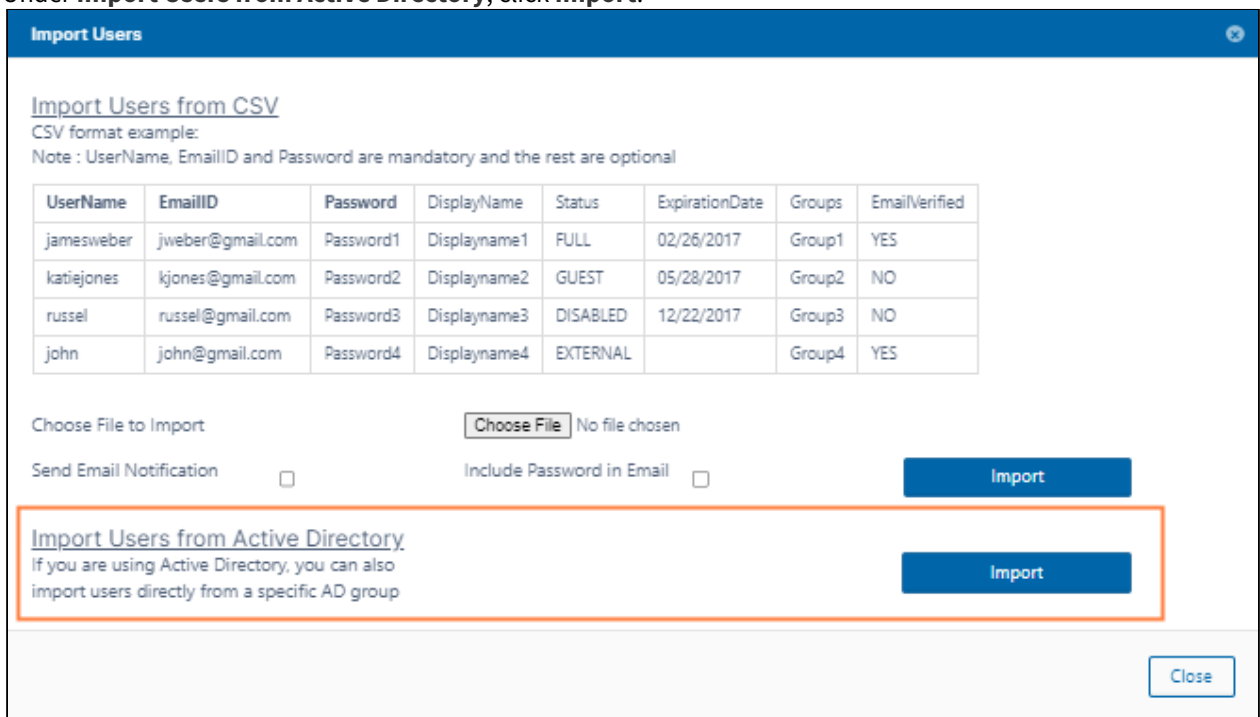
1. Open a browser and log on to Admin Portal.
2. Setup [AD configuration](#) or [LDAP configuration](#) depending on your requirements.
3. From the left navigation panel, under USERS/GROUPS, click **Users**.
4. To open the **Import** window, click **Import**.



The screenshot shows the 'Manage Users' interface. At the top right, there are three buttons: 'Add User', 'Import', and 'Export'. The 'Import' button is highlighted with a red arrow. Below the buttons is a search bar and several filters. The main part of the interface is a table with columns: User name, Display Name, Email, Last Login, Status, and Actions. The table contains three rows of user data.

	User name	Display Name	Email	Last Login	Status	Actions
	Jared Taylor	Jared Taylor	[REDACTED]	--	Full Access	
	Noah	Noah	noah@example.com	--	Full Access	
	abose	Amit Bose	amitbose@example.com	08 Oct 2020 15:52	Full Access	

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



The screenshot shows the 'Import Users' dialog box. It has a blue header with the title 'Import Users'. Below the header, there are two sections: 'Import Users from CSV' and 'Import Users from Active Directory'. The 'Import Users from Active Directory' section is highlighted with a red box. The 'Import' button in this section is also highlighted with a red box.

Import Users from CSV
 CSV format example:
 Note : UserName, EmailID and Password are mandatory and the rest are optional

UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified
jamesweber	jweber@gmail.com	Password1	Displayname1	FULL	02/26/2017	Group1	YES
katiejones	kjones@gmail.com	Password2	Displayname2	GUEST	05/28/2017	Group2	NO
russel	russel@gmail.com	Password3	Displayname3	DISABLED	12/22/2017	Group3	NO
john	john@gmail.com	Password4	Displayname4	EXTERNAL		Group4	YES

Choose File to Import No file chosen

Send Email Notification Include Password in Email

Import Users from Active Directory
 If you are using Active Directory, you can also import users directly from a specific AD group


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 approved, 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.

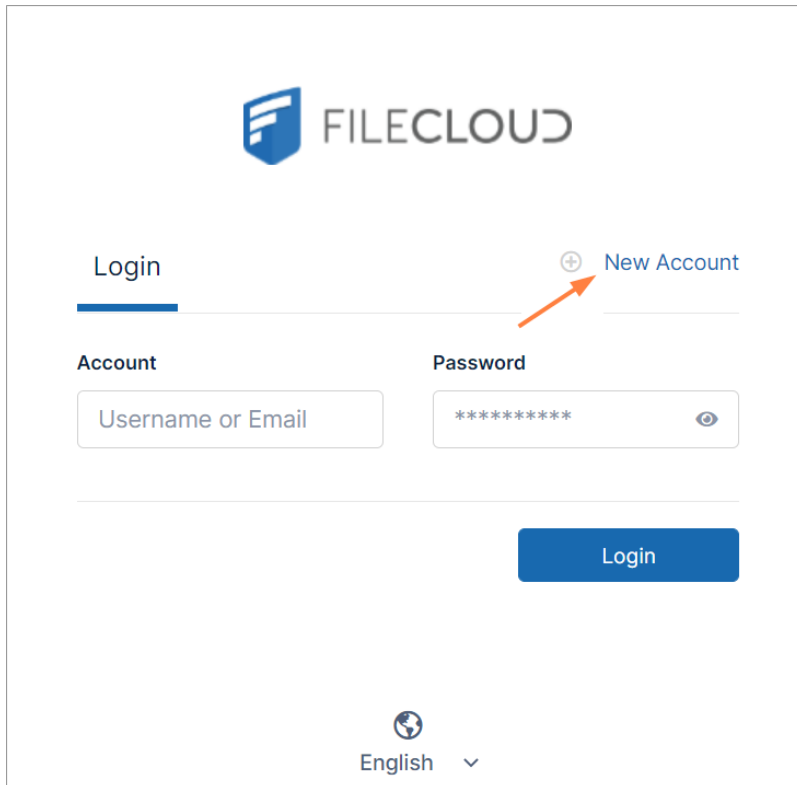
To use this option:

1. Open a browser and log on to the admin portal.
2. In the navigation panel, click **Groups**.
3. Select the **group** that you want to add users to, and then click the Edit Group () 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.



The screenshot shows the FileCloud login interface. At the top left is the FileCloud logo. Below it, the word "Login" is underlined. To the right of "Login" is a link labeled "New Account" with a plus sign icon, which is highlighted by an orange arrow. Below the "Login" link are two input fields: "Account" (containing "Username or Email") and "Password" (containing "*****" and an eye icon). A blue "Login" button is positioned below the password field. At the bottom center, there is a globe icon and the text "English" with a dropdown arrow.

Administrators can customize how new user accounts are created.

- i** 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 tab > Login tab	<p>ENABLED = Displays New Account button on User log-in page. opens a window for the user to type in new account information</p> <p>DISABLED = Hides New Account button on User log-in page.</p>	<p>This setting determines whether the New Account button appears on the User Portal Log-in page.</p> <p>If enabled, this setting works with two other settings to determine authentication and approval permissions:</p> <ul style="list-style-type: none"> • Allow Account Signups • Automatic Account Approval

Setting	Location	Options	Description
Allow Account Signups	Settings > Admin tab	<p>Specifies if a user can or cannot create a new FileCloud user account from the login-in page. by choosing:</p> <ul style="list-style-type: none"> • DEFAULT • TRUE • FALSE <p>Can Create an Account</p> <p>Prerequisite: <i>Show New Account Button</i> = Enabled</p> <p>DEFAULT = AD and LDAP users can create their own accounts</p> <ul style="list-style-type: none"> • Active Directory authentication allowed • LDAP authentication allowed • Local users (who are not using AD or LDAP authentication) cannot create their own accounts. 	<p>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 <i>Automatic Account Approval</i> settings.</p> <p>Do I choose DEFAULT or TRUE?</p> <p>DEFAULT</p> <ul style="list-style-type: none"> • 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, you can have the users create their own FileCloud account automatically on first login. In this scenario you would just tell your users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create that user's new FileCloud account. <p>Note: If you are not using AD or LDAP authentication, users cannot create their own accounts.</p> <p>TRUE</p> <ul style="list-style-type: none"> • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it. <p>Note: If you are using AD or LDAP authentication, users can create their own accounts.</p>

Setting	Location	Options	Description
		<p>TRUE = Local users can create their own accounts</p> <ul style="list-style-type: none"> • Local users (who are not using AD or LDAP authentication) can create their own accounts. • Active Directory authentication not allowed • LDAP authentication not allowed <p>Cannot Create an Account</p> <p>FALSE = No users can create their own accounts</p> <ul style="list-style-type: none"> • 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	Settings > Admin tab	<p>(Default) 0 = The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.</p> <p>1 = The new user account is automatically approved with FULL access.</p> <p>2 = The new user account is automatically approved with GUEST access.</p> <p>3 = The new user account is automatically approved with EXTERNAL access.</p>	<p> If the total number of licenses has been reached, share invitations to new users are blocked unless Automatic Account Approval is set to 3.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • New Account = ENABLED • Allow Account Signups = DEFAULT or TRUE <p>This setting works with the Allow Account Signups setting to determine:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> 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.</p>

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

Settings option, Admin tab

✘ Allow Account Signups = FALSE

✘ Automatic Account Approval = 0

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

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

⚠ 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, FileCloud Sync or FileCloud Drive.
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.

⚠ 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, FileCloud Sync or FileCloud Drive.
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.

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, FileCloud Sync or FileCloud Drive.
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 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.

<p>12. The user is required to verify the email account to complete the account creation process.</p>		<p>10. The user is required to verify the email account to complete the account creation process.</p>		<p>10. The user is required to verify the email account to complete the account creation process.</p>
<p>Settings option, Users tab</p> <ul style="list-style-type: none"> ✔ User Account Search Mode = <i>Exact Email with Implicit Account Invite</i> OR <i>Exact Email with Explicit Account Invite</i> <p>Settings option, Authentication tab</p> <ul style="list-style-type: none"> ✔ Authentication Type = DEFAULT <p>Customization settings, Login tab</p> <ul style="list-style-type: none"> ✔ New Account button = ENABLED <p>Settings option, Admin tab</p> <ul style="list-style-type: none"> ✔ Allow Account Signups = TRUE ✘ Automatic Account Approval = 0 		<p>Settings option, Users tab</p> <ul style="list-style-type: none"> ✔ User Account Search Mode = <i>Exact Email with Implicit Account Invite</i> OR <i>Exact Email with Explicit Account Invite</i> <p>Settings option, Authentication tab</p> <ul style="list-style-type: none"> ✔ Authentication Type = DEFAULT <p>Customization settings, Login tab</p> <ul style="list-style-type: none"> ✔ New Account button = ENABLED <p>Settings option, Admin tab</p> <ul style="list-style-type: none"> ✔ Allow Account Signups = TRUE ✔ Automatic Account Approval = 1, 2, 3, <p>Set the Create account on new user shares to true under policies.</p>		<p>Settings option, Authentication tab</p> <ul style="list-style-type: none"> ✔ Authentication Type = ACTIVE DIRECTORY or LDAP <p>Customization settings, Login tab</p> <ul style="list-style-type: none"> ✔ New Account button = ENABLED <p>Settings option, Admin tab</p> <ul style="list-style-type: none"> ✔ Allow Account Signups = DEFAULT ℹ Automatic Account Approval = 0, 1, 2, 3

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 their 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, FileCloud Sync or FileCloud Drive.
5. On the User Portal Login window, the user enters their AD or LDAP username and password.
6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.

Settings option, Authentication tab

- ✔ Authentication Type = ACTIVE DIRECTORY or LDAP

Customization settings, Login tab

- ✔ New Account button = ENABLED

Settings option, Admin tab

- ✔ Allow Account Signups = DEFAULT
- ✔ Automatic Account Approval = 1, 2

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](#)
- [Domain Limitations for External Users](#)

Account Approval

This feature is used to allow Automatic Account Creation by user on clicking the "New Account" button in user UI page.

The Admin can set this mode in the following ways at **Settings > Admin tab > Automatic Account Approval:**

Modes	Description
0 - No Automatic Approval, Admin has to approve account	Default. In this mode the account can be created by the user but cannot log in. It requires Admin approval for the user to access the account.

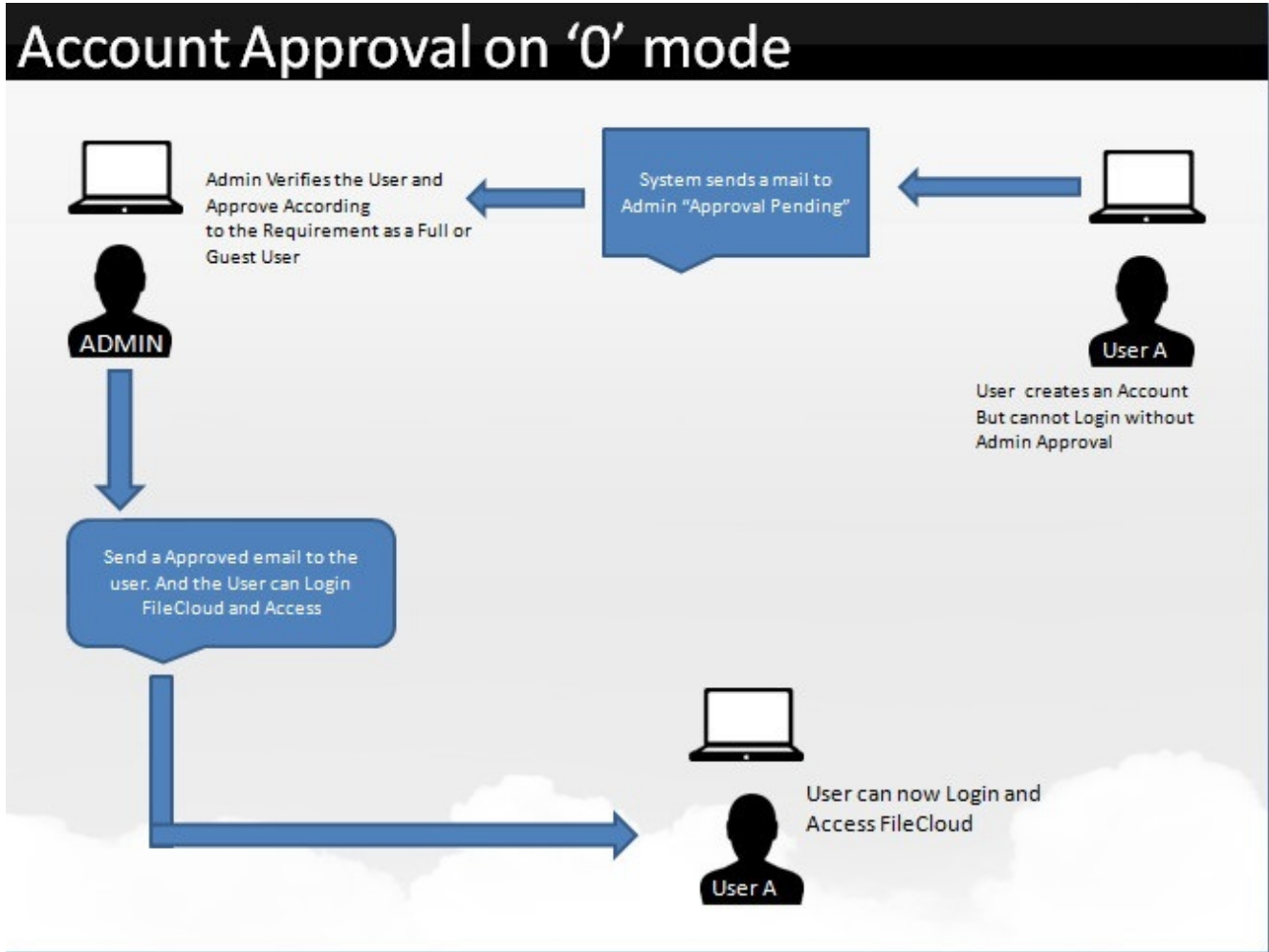
Modes	Description
1 - Automatically approved to Full User	This mode allows the user to Create Account and access FileCloud without waiting for Admin 's approval. This mode lets user create account as FULL USER Permission.
2 - Automatically approved to Guest User	This mode also allows the user to Create Account and access FileCloud without waiting for Admin 's approval. This mode lets user create account as GUEST USER Permission only. Later If the Admin wants the user to have Full User Permission It can be managed by the Admin.
3 - Automatically approved to External User	This mode also allows the user to Create account and access FileCloud without waiting for Admin approval. This mode lets user create account as External User only.

Account Approval on mode '0'

In this mode the user can Create an Account to access FileCloud but cannot Login . To Login it requires Admin's approval, so the system sends a Approval Pending Email to the Admin. Once Admin approves the user and sets the required Permission like Full User or Guest User. The user receives a email of Approval , and can Login and access FileCloud.

Note

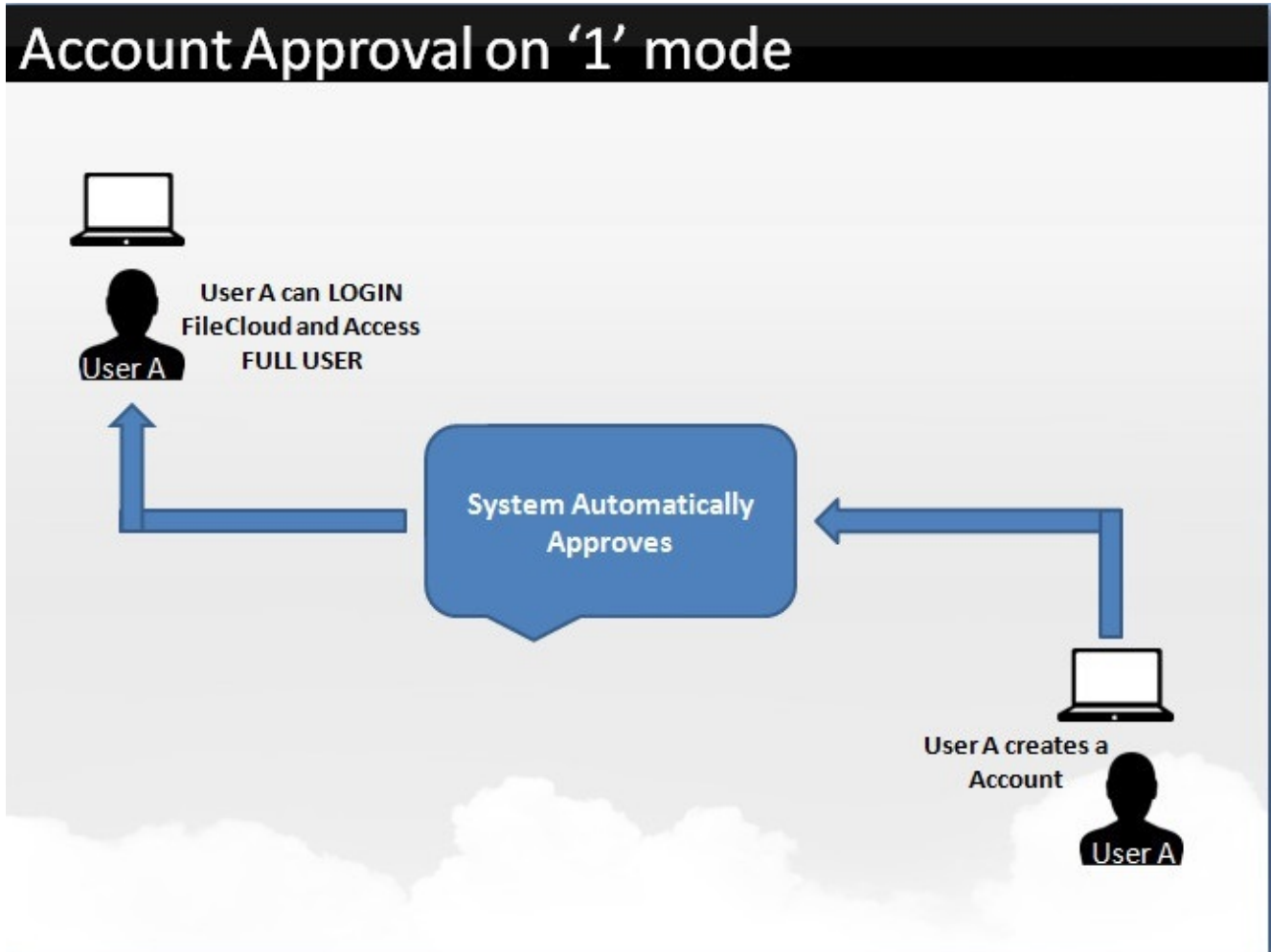
- Approval emails will be sent only if the option "Send Approval Pending Emails" is selected in the Admin UI -> Settings -> Admin.
- If "Send Approval Pending Emails" is unchecked, the account creation will not be notified. In this case, new accounts can get approved only when admin user logs in.
- If "Send Approval Pending Emails" is selected, the emails will be sent to mail id set at Admin UI -> Settings -> Email ->"Email Reply to Address"



Account Approval on mode '1'

In this mode, user can Create Account and can access FileCloud. User does not need to wait for approval. The system automatically approves and allows Login.

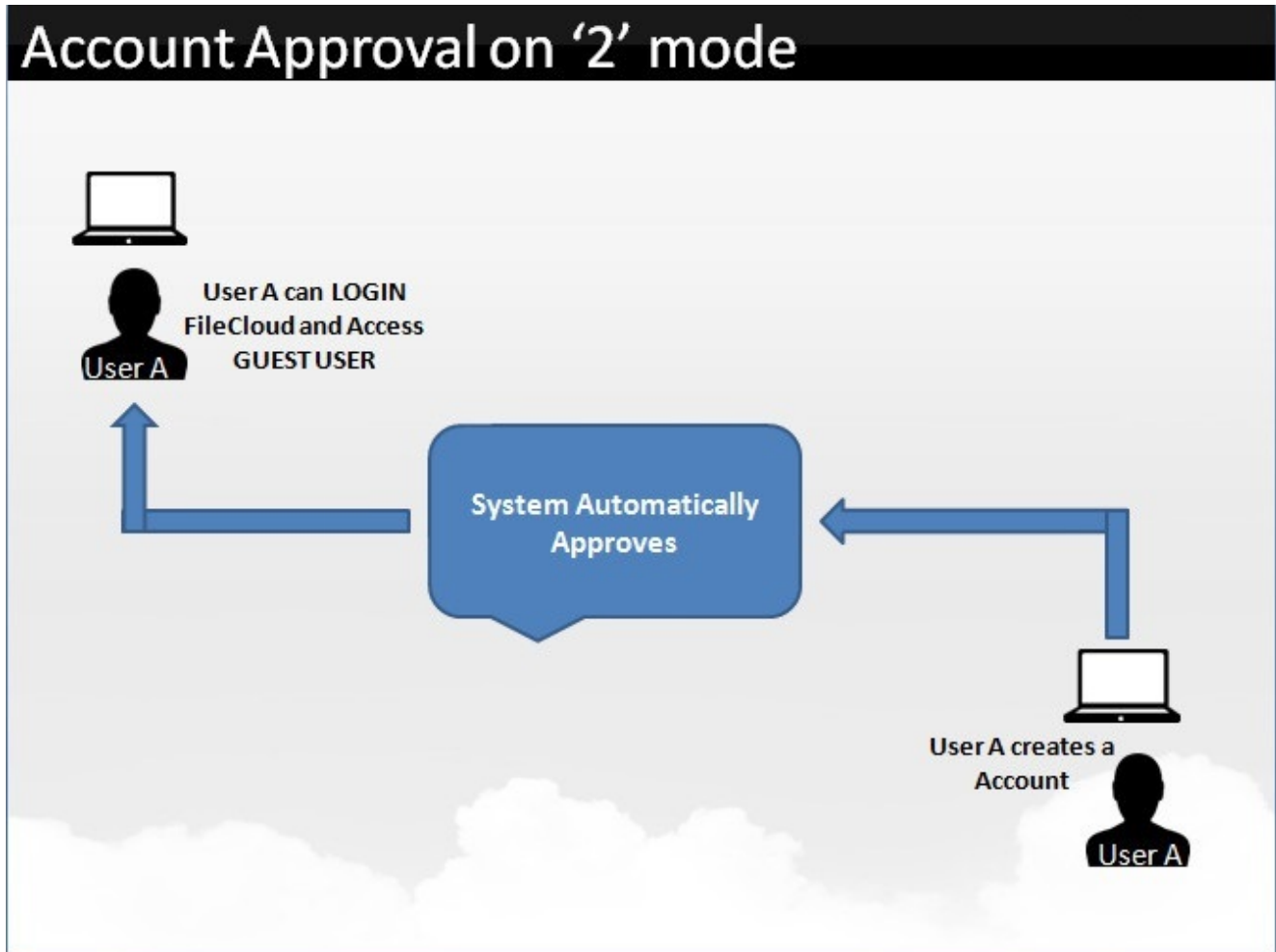
User is logged in the System as FULL USER in this mode.



Account Approval on mode '2'

In this mode, user can Create Account and can access FileCloud. User does not need to wait for approval. The system automatically approves and allows Login.

User is logged in the system as GUEST USER in this mode. To know more about Guest User check [User Access](#) page.



Account Approval on mode '3'

In this mode, user can Create Account and can access FileCloud. User does not need to wait for approval. The system automatically approves and allows Login.

User is logged in the system as EXTERNAL USER in this mode. To know more about External Users check [User Access Levels and User Types](#) page.

Allow AD or LDAP Users to Create a New Account

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

Administrators can customize how new user accounts are created.

In these scenarios you are allowing AD or LDAP users to create a new FileCloud user account in one of the following ways:



- 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 settings that you use to configure this scenario are described in Table1.

Table 1. The Settings

Setting	Options	Description
<i>New Account</i>	<p>ENABLED = opens a window for the user to type in new account information</p> <p>DISABLED = opens a window explaining that User Account Creation is not allowed</p>	<p>This setting determines the behavior of the New Account button on the User Portal Login page.</p> <p>If enabled, this setting works with two other settings to determine authentication and approval permissions:</p> <ul style="list-style-type: none"> • Allow Account Signups • Automatic Account Approval

Setting	Options	Description
<i>Allow Account Signups</i>	<p>Specifies if a user can or cannot create a new FileCloud user account by choosing:</p> <ul style="list-style-type: none"> • DEFAULT • TRUE • FALSE <p>Can Create an Account</p> <p>Prerequisite: <i>New Account</i> = Enabled</p> <p>DEFAULT = Local user authentication is allowed</p> <ul style="list-style-type: none"> • Active Directory authentication allowed • LDAP authentication allowed <p>TRUE = Local user can create their own account</p> <p>Cannot Create an Account</p> <p>FALSE = Local user cannot create their own account</p> <ul style="list-style-type: none"> • If the New Account button is enabled, and the user clicks it, they can fill out the fields on the form. However, when they try to submit the information they will get an error that new account creation is not allowed. 	<p>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 <i>Automatic Account Approval</i> settings.</p> <p>Do I choose DEFAULT or TRUE?</p> <p>DEFAULT</p> <ul style="list-style-type: none"> • If you are using AD or LDAP Authentication. • After you import AD or LDAP user accounts into FileCloud, tell your users to log in using their AD or LDAP credentials. <p>TRUE</p> <ul style="list-style-type: none"> • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it.

Setting	Options	Description
<i>Automatic Account Approval</i>	<p>(Default) 0 = The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.</p> <p>1 = The new user account is automatically approved with FULL access.</p> <p>2 = The new user account is automatically approved with GUEST access.</p> <p>3 = The new user account is automatically approved with EXTERNAL access.</p>	<p>Prerequisites:</p> <ul style="list-style-type: none"> • <i>New Account</i> = ENABLED • <i>Allow Account Signups</i> = DEFAULT or TRUE <p>This setting works with the <i>Allow Account Signups</i> setting to determine:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.</p>

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

<p>Admins want FileCloud to automatically create a new FileCloud account for their Active Directory or LDAP Users on First Login</p>	<p>Active Directory or LDAP Users create a new FileCloud account different from their AD or LDAP credentials</p> <p>The Admin can configure the approval process</p>
---------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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, FileCloud Sync or FileCloud Drive.
5. On the User Portal Login window, the user enters their AD or LDAP username and password.
6. FileCloud uses the AD or LDAP credentials to automatically create a FileCloud account for that user.

Settings option, Authentication tab

✔ Authentication Type = ACTIVE DIRECTORY or LDAP

Customization settings, Login tab

✔ New Account button = ENABLED

Settings option, Admin tab

✔ Allow Account Signups = DEFAULT

✔ Automatic Account Approval = 1, 2

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, FileCloud Sync or FileCloud Drive.
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 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 option, Authentication tab

✔ Authentication Type = ACTIVE DIRECTORY or LDAP

Customization settings, Login tab

✔ New Account button = ENABLED

Settings option, Admin tab

✔ Allow Account Signups = DEFAULT

❗ Automatic Account Approval = 0, 1, 2, 3

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

Table 3 Describes how each authentication mode impacts the users' ability to create a new account.

Table 3. Authentication Modes Comparison

	Default Authentication	AD	LDAP
Authentication	Performed by FileCloud Server	In AD Server	In LDAP Server
Allowing Users to 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
- The FileCloud version must be 4.0 or higher

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

1. Log in to the FileCloud Admin Portal.
2. In the left navigation panel, click **Settings**.
3. In the right panel, from the selection of tabs, click **Authentication**.
4. Under *Authentication Settings*, in *Authentication Type*, select **ACTIVE DIRECTORY** or **LDAP**.
5. To enable the New Account button, in the left navigation panel, click **Customization**, and then the **Login** tab.
6. **Next to New Account, select the checkbox if it is not already selected.**
7. To allow users to create an account, in the left navigation panel, click *Settings*, and then the *Admin* tab.
8. In *Allow Account Signups*, select **Default**.
9. To set an approval method, in *Automatic Account Approval*, choose one of the following values.

Value	Description
(Default) 0	The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.

Value	Description
1	The new user account is automatically approved with FULL access.
2	The new user account is automatically approved with GUEST access.
3	The new user account is automatically approved with EXTERNAL access.



The user is notified by email when:

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

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 these scenarios are described in Table1.




Table 1. The Settings

Setting	Options	Description
<i>New Account</i>	<p>ENABLED = opens a window for the user to type in new account information</p> <p>DISABLED = opens a window explaining that User Account Creation is not allowed</p>	<p>This setting determines the behavior of the New Account button on the User Portal Login page.</p> <p>If enabled, this setting works with two other settings to determine authentication and approval permissions:</p> <ul style="list-style-type: none"> • Allow Account Signups • Automatic Account Approval

Setting	Options	Description
<i>Allow Account Signups</i>	<p>Specifies if a user can or cannot create a new FileCloud user account by choosing:</p> <ul style="list-style-type: none"> • DEFAULT • TRUE • FALSE <p>Can Create an Account</p> <p>Prerequisite: <i>New Account</i> = Enabled</p> <p>DEFAULT = Local user authentication is allowed</p> <ul style="list-style-type: none"> • Active Directory authentication allowed • LDAP authentication allowed <p>TRUE = Local user can create their own account</p> <ul style="list-style-type: none"> • Active Directory authentication not allowed • LDAP authentication not allowed <p>Cannot Create an Account</p> <p>FALSE = Local user cannot create their own account</p> <ul style="list-style-type: none"> • If the New Account button is enabled, and the user clicks it, they can fill out the fields on the form. However, when they try to submit the information they will get an error that new account creation is not allowed. 	<p>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 <i>Automatic Account Approval</i> settings.</p> <p>Do I choose DEFAULT or TRUE?</p> <p>DEFAULT</p> <ul style="list-style-type: none"> • 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, you can have the users create their own FileCloud account automatically on first login. In this scenario you would just tell your users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create that user's new FileCloud account. <p>TRUE</p> <ul style="list-style-type: none"> • If you are NOT using AD or LDAP Authentication • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it.

Setting	Options	Description
<i>Automatic Account Approval</i>	<p>(Default) 0 = The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.</p> <p>1 = The new user account is automatically approved with FULL access.</p> <p>2 = The new user account is automatically approved with GUEST access.</p> <p>3 = The new user account is automatically approved with EXTERNAL access.</p>	<p>Prerequisites:</p> <ul style="list-style-type: none"> • <i>New Account</i> = ENABLED • <i>Allow Account Signups</i> = DEFAULT or TRUE <p>This setting works with the <i>Allow Account Signups</i> setting to determine:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.</p>

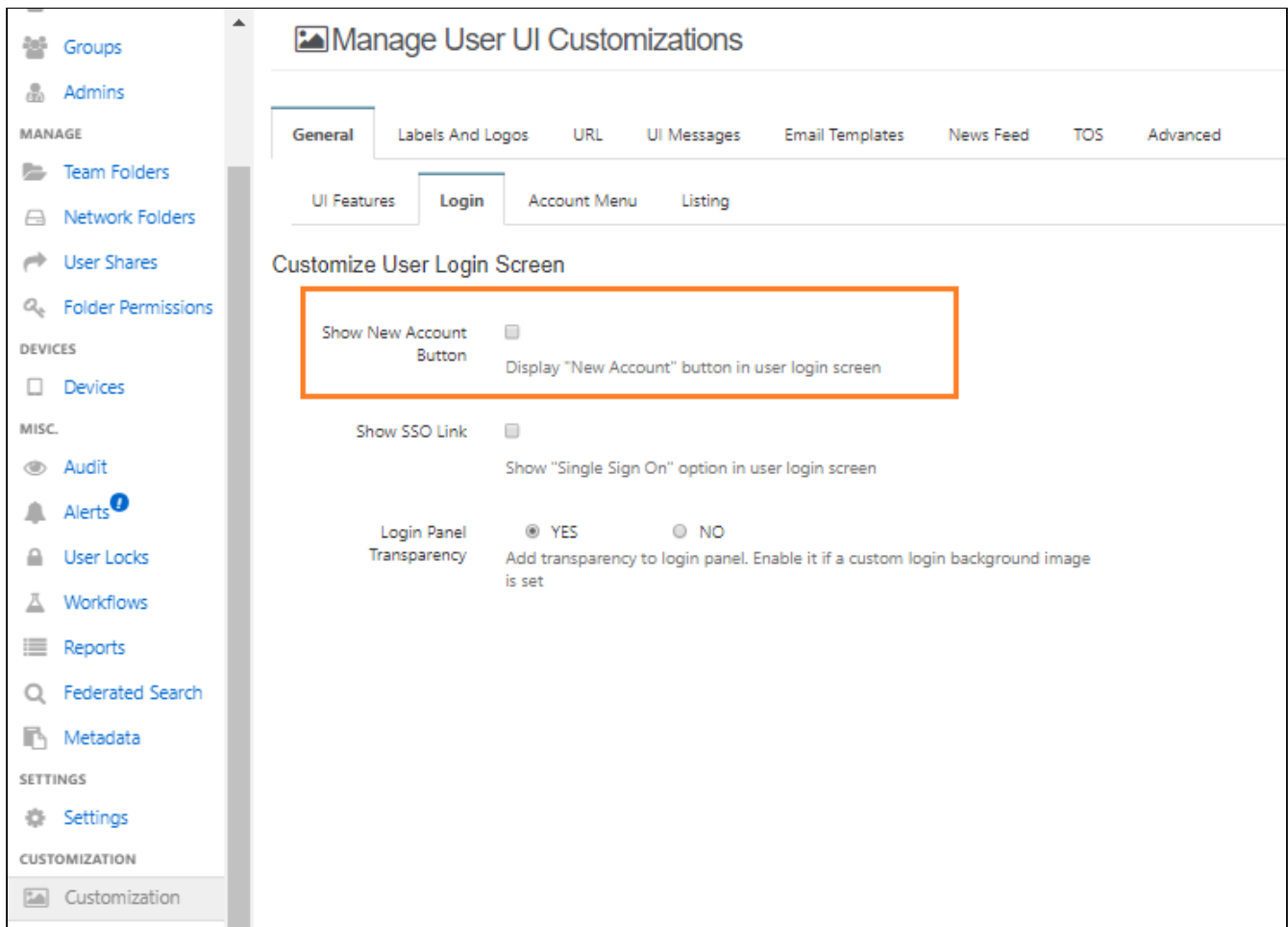
The scenario where only an administrator creates a new FileCloud account is described in Table 2.

Only an Admin can create User accounts
<ol style="list-style-type: none"> 1. The Administrator creates the account in the Admin Dashboard. 2. The User receives a Welcome email with the account credentials and User Portal URL.
<p>Customization settings, Login tab</p> <ul style="list-style-type: none">  New Account button = DISABLED <p>Settings option, Admin tab</p> <ul style="list-style-type: none">  Allow Account Signups = FALSE  Automatic Account Approval = 0

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. Next to **Show New Account Button**, make sure the checkbox is not selected.
5. 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.

In this scenario you are allowing users to create and approve their own accounts.

- An administrator sets a default level of access.
- Can be used when 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.
-  Allow user access/new account creation with an AD or LDAP account.

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

Table 1. The Settings

Setting	Options	Description
<i>New Account</i>	<p>ENABLED = opens a window for the user to type in new account information.</p> <p>DISABLED = opens a window explaining that User Account Creation is not allowed.</p>	<p>This setting determines the behavior of the New Account button on the User Portal Login page.</p> <p>If enabled, this setting works with two other settings to determine authentication and approval permissions:</p> <ul style="list-style-type: none"> • Allow Account Signups • Automatic Account Approval


Setting	Options	Description
<i>Allow Account Signups</i>	<p>Specifies if a user can or cannot create a new FileCloud user account by choosing:</p> <ul style="list-style-type: none"> • DEFAULT • TRUE • FALSE <p>Can Create an Account</p> <p>Prerequisite: <i>New Account</i> = Enabled</p> <p>DEFAULT = Local user authentication is allowed</p> <ul style="list-style-type: none"> • Active Directory authentication allowed • LDAP authentication allowed <p>TRUE = Local user can create their own account</p> <ul style="list-style-type: none"> • Active Directory authentication not allowed • LDAP authentication not allowed <p>Cannot Create an Account</p> <p>FALSE = Local user cannot create their own account</p> <ul style="list-style-type: none"> • If the New Account button is enabled, and the user clicks it, they can fill out the fields on the form. However, when they try to submit the information they will get an error that new account creation is not allowed. 	<p>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 <i>Automatic Account Approval</i> settings.</p> <p>Do I choose DEFAULT or TRUE?</p> <p>DEFAULT</p> <ul style="list-style-type: none"> • 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, you can have users create their own FileCloud account automatically on their first login. In this scenario, you would just tell your users to log in using their AD or LDAP credentials and on their first login FileCloud will automatically create that user's new FileCloud account. <p>TRUE</p> <ul style="list-style-type: none"> • If you are NOT using AD or LDAP Authentication. • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it.

Setting	Options	Description
<i>Automatic Account Approval</i>	<p>(Default) 0 = The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.</p> <p>1 = The new user account is automatically approved with FULL access.</p> <p>2 = The new user account is automatically approved with GUEST access.</p> <p>3 = The new user account is automatically approved with EXTERNAL access.</p>	<p>Prerequisites:</p> <ul style="list-style-type: none"> • <i>New Account</i> = ENABLED • <i>Allow Account Signups</i> = DEFAULT or TRUE <p>This setting works with the <i>Allow Account Signups</i> setting to determine:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> For larger organizations, it might not be practical to have the administrator approve every account created, so you can use the automatic account approval settings.</p>

The scenarios where a user can create a new FileCloud account are described in Table 2.

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, FileCloud Sync or FileCloud Drive.
5. On the user portal login window, the user clicks the New Account button.
6. The user enters details in the account creation fields.
7. The account is created and is granted access of a Full User, Guest User, or External User as set by the Administrator.
8. The user receives an account creation email using the email address provided during account creation.
9. The user is required to verify the email account to complete the account creation process.


Settings option, Users tab

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


Settings option, Authentication tab


 Authentication Type = *DEFAULT*

Customization settings, Login tab

 New Account button = *ENABLED*

Settings option, Admin tab

 Allow Account Signups = *TRUE*

 Automatic Account Approval = *1, 2, 3*

Set the Create account on new user shares to true under policies.

To configure these settings:

1. Log into the *Admin Portal*.
2. From the left navigation menu, click *Settings*.
3. Select the *Misc.* tab, and then click the *Users* sub-tab.
4. In *User Account Search Mode*, select *Exact Email Search with Explicit Account Invite* or *Exact Email Search with Implicit Account Invite*.
5. Click *Save*.
6. In the left menu panel, click *Customization*.
7. On the *General* tab, click the *Login* tab.
8. Select the *Show New Account Button* checkbox.
9. Click *Save*.
10. From the left navigation menu, click *Settings*.
11. In the right panel, click the *Admin* tab.

12. In the *Allow Account Signups* field, select *TRUE*.
13. Click *Save*.

The screenshot shows the 'Manage Settings' interface with the 'User' tab selected. Under 'User Settings', the 'User account search mode' dropdown menu is open, displaying four options. The second option, 'Exact Email Search With Implicit Account Invite', is highlighted in blue. Other options include 'Exact Email Search With Explicit Account Invite', 'Exact Name/Email Search', and 'Partial Name/Email Search'. Other settings visible include 'Import Files from Folder on User Creation' with a 'Check Path' button, 'Group Visibility' set to 'Show All Groups', and 'Send email to user to approve device' which is checked.

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 account but it is disabled until an Administrator approves it

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

Table 1. The Settings


Setting	Options	Description
<i>New Account</i>	<p>ENABLED = opens a window for the user to type in new account information</p> <p>DISABLED = opens a window explaining that User Account Creation is not allowed</p>	<p>This setting determines the behavior of the New Account button on the user log-in page.</p> <p>If enabled, this setting works with two other settings to determine authentication and approval permissions:</p> <ul style="list-style-type: none"> • Allow Account Signups • Automatic Account Approval
<i>Allow Account Signups</i>	<p>Specifies if a user can or cannot create a new FileCloud user account from the log-in page by choosing:</p> <ul style="list-style-type: none"> • DEFAULT • TRUE • FALSE <p>Can Create an Account</p> <p>Prerequisite: <i>New Account</i> = Enabled</p> <p>DEFAULT = Local user authentication is allowed</p> <ul style="list-style-type: none"> • Active Directory authentication allowed • LDAP authentication allowed <p>TRUE = Local user can create their own account</p> <ul style="list-style-type: none"> • Active Directory authentication not allowed • LDAP authentication not allowed <p>Cannot Create an Account</p> <p>FALSE = Local user cannot create their own account</p> <ul style="list-style-type: none"> • If the New Account button is enabled, and the user clicks it, they can fill out the fields on the form. However, when they try to submit the information they will get an error that new account creation is not allowed. 	<p>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 <i>Automatic Account Approval</i> settings.</p> <p>Do I choose DEFAULT or TRUE?</p> <p>DEFAULT</p> <ul style="list-style-type: none"> • 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, you can have the users create their own FileCloud account automatically on first login. In this scenario you would just tell your users to log in using their AD or LDAP credentials and on first login FileCloud will automatically create that user's new FileCloud account. <p>TRUE</p> <ul style="list-style-type: none"> • If you are NOT using AD or LDAP Authentication • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it.

Setting	Options	Description
<i>Automatic Account Approval</i>	<p>(Default) 0 = The account created by the user is DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.</p> <p>1 = The new user account is automatically approved with FULL access.</p> <p>2 = The new user account is automatically approved with GUEST access.</p> <p>3 = The new user account is automatically approved with EXTERNAL access.</p>	<p>Prerequisites:</p> <ul style="list-style-type: none"> • <i>New Account</i> = ENABLED • <i>Allow Account Signups</i> = DEFAULT or TRUE <p>This setting works with the <i>Allow Account Signups</i> setting to determine:</p> <ul style="list-style-type: none"> • 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. <p> 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.</p> <p> For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.</p>

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


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, FileCloud Sync or FileCloud Drive.
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 will be notified about the new account.
7. The Admin will approve the account.
8. The Admin will set the user account type to Full User or Guest User.
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 option, Authentication tab

 Authentication Type = DEFAULT

Customization settings, Login tab

 New Account button = ENABLED

Settings option, Admin tab


 Allow Account Signups = TRUE


 Automatic Account Approval = 0

To allow a user to create an account that is disabled by default, you will need to set the Allow Account Signups field. [Table 1](#) describes the options you can choose from.

This scenario allows the user to fill out the account information and the Administrator to approve it before the account be used to access the FileCloud site.

For this scenario, use the following settings:

 New Account button = ENABLED

 Allow Account Signups = FALSE

 Automatic Account Approval = 0

If you disable Account Signups, then the Automatic Approval setting can be left set to the default.

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. Next to **Show New Account Button**, make sure the checkbox is not selected.
5. In the left menu panel, click Settings.
6. In the right panel, click the **Admin** Tab.
7. In the Allow Account Signups field, select FALSE.

The screenshot shows the FileCloud 'Manage Settings' interface. The left sidebar contains navigation options like Groups, Admins, Team Folders, Network Folders, User Shares, Folder Permissions, Devices, Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata, Settings, Customization, Checks, and Upgrade. The main content area is titled 'Manage Settings' and has tabs for Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, and Policies. The 'Admin' tab is active, showing 'Admin Settings' with fields for Admin Login Name (admin), Admin Email, Enable Two Factor Authentication For Admin Logins (unchecked), Admin password, Re-Confirm Admin Password, Stats API Key (apipassword), and Allow Account Signups. The 'Allow Account Signups' dropdown menu is open, with 'FALSE' selected and highlighted in blue. An orange arrow points to this selection.



The user is notified by email when:

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

Domain Limitations for External Users

i 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

i 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.

The settings can be accessed by

1. Log into FileCloud [Administration Portal](#)
2. Click on **Settings** in the left navigation panel

3. Click on **Misc** tab
4. Click on **Password** tab
5. Change settings as needed
6. Click **Save**.

Server Storage Authentication Admin Database Email Endpoint Backup
Third Party Integrations **Misc** Reset

General User **Password** Notifications Share Preview Support Service:
Privacy 2FA

Password Settings

Minimum Password Length

Minimum acceptable length of Password

Enable Strong Passwords

- Enabling this will require the password to contain at least one uppercase, lowercase, number and a special character in the password

Disallow Commonly Used Passwords

- Enabling this checkbox will prevent users from using commonly used passwords for their user accounts

Incorrect Attempts Before Account Lockout

Number of times wrong password can be entered before an account is locked out. Value 0 implies account will not be locked out.

Account Lockout Length In Minutes

Number of minutes account will be locked out. Value 0 implies account will not be locked out.

Disallow User Login With Password

DEFAULT



Disallow Login with password on user accounts.

User Password Expires In Days

0

Number of days passwords are valid for user accounts. Value 0 implies passwords will not expire. Applicable only for default authentication. Expiry will apply only after passwords are changed.

New Accounts Must Change Password

New User accounts created will be forced to change password on login.

Skip password change on first login

Skip password change on first login for accounts created during share and new sign up.

Number of Previous Password that cannot be reused

Number of Previous Password that cannot be reused. Value 0 implies no restriction.

Reset password attempt interval

5

Interval (in minutes) between consecutive reset password attempts. Value 0 implies no restriction.

Send reset password email

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	<p>Enabling this will require the password to contain at least one uppercase, lowercase, number and a special character in the password. Checked by default.</p> <p>Applies only to local account and not to AD/LDAP account.</p>
Disallow Commonly Used Passwords	Prevents users from using commonly used passwords for their user accounts. Checked by default. For more information, see Restrict Commonly Used Passwords .
Incorrect attempts before account lockout	<p>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.</p> <p>A value of 0 means account lockout with wrong password is disabled.</p>
Account Lockout length in Minutes	<p>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.</p> <p>A value of 0 means lockout is disabled.</p>
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	<p>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.</p> <p>NOTE: Automatic email notifications are sent to the user 7 days and 1 day before the actual password expiry date.</p>

Type	Description
<p>New accounts must change password</p>	<p>When enabled, this setting forces new users to change their password on initial login, with the following exceptions:</p> <ul style="list-style-type: none"> • 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). <p>Default is disabled.</p>
<p>Skip password change on first login</p>	<p>Do not require password change on first login for accounts created during shared and new signups. Checked by default.</p>
<p>Number of previous passwords that cannot be reused</p>	<p>Specifies the number of previous passwords that cannot be reused when password is changed. A value of 0 indicates that there are no restrictions.</p>
<p>Reset password attempt interval</p>	<p>Interval in minutes between consecutive reset password attempts. Default is 5.</p> <p>0 indicates that there is no restriction.</p>
<p>Send reset password email</p>	<p>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 checked, email subject and email content fields appear.</p> <div data-bbox="732 1171 1463 1579" style="border: 1px solid black; padding: 5px;"> <p>Send reset password email</p> <p><input checked="" type="checkbox"/></p> <p>Email subject</p> <p><input type="text" value="Password Changed!"/></p> <p>Enter the text of the email below</p> <div style="border: 1px solid gray; height: 60px; width: 100%;"></div> </div> <p>Email subject is set to Password Changed! but may be changed. The note in Enter the text of the email below must be entered.</p> <p>Unchecked by default.</p>

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 admin portal, go to **Settings > Admin**.
2. Scroll down to the **Account Locked Alert** setting.

Account Locked Alert

No Email

Account Locked Alert Email

No Email - No Email Alert will be sent

Email User - Email Alert only for User

Email User and Admin - Email Alert for both User and Admin

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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then select the *Password* sub-tab.
4. Next to *Disallow Commonly Used Passwords*, select the checkbox.
5. 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

 In FileCloud version 19.3 and earlier session timeout was measured in days; in FileCloud version 20.1 and later, it is measured in minutes.

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. Go to **Settings > Policies**.
2. Open the policy for edit.
3. Click the **User Policy** tab.
4. In order to enable the **Enforce Session Timeout for Devices** setting, scroll down to the setting **Enable code based device authentication** and set it to **YES**.
Now **Enforce Session Timeout for Devices** is enabled.

5. Set **Enforce Session Timeout for All Devices** to **YES**.

Policy Settings - Global Default Policy

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

Enable code based device authentication
YES

Enable code based device authentication

Require Admin Approval for Device Authentication
NO

Require admin approval for code based device authentication

Enforce Session Timeout for Devices
YES

Device timeout is enforced. Users must log in again after session expires.

Save Reset All Close

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

i The ability to change the storage quota for users through Policies is available in FileCloud version 17.3 and later.

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 navigation pane, click **Settings** and click the **Policy** tab.
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.

✕
Policy Settings - Admin Users

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

Default Max Number of Downloads Allowed

Number of downloads allowed. Value 0 implies that the maximum number of downloads is unlimited.

User Storage Quota

Units ▾

2048

MB

Specify storage quota. 0 implies Unlimited Quota.

Enable Privacy Settings

NO
▾

Enables/disables privacy settings

Save
Reset

✕ Close

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

Manage Policy
+ New policy

Filter

Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	🔴	✎ 📄 👤 👥 🗑️
Global Default Policy	0	0	🟢	✎ 📄 👤 👥 🗑️
Admin Users	3	0	🔴	✎ 📄 👤 👥 🗑️

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 screenshot shows the 'Manage Policy Users : Admin Users' interface. It features a search filter with the text 'ie', and two dropdown menus labeled 'Status Fil' and 'Source Fil'. Below these are two main panels: 'Available Users' and 'Policy Users'. The 'Available Users' panel contains a table with two rows: 'gabrielled (Gaby)' with 'Full Access' status, and 'test_client_1 (test_client_1)' with 'Full Access' status. The 'Policy Users' panel is currently empty. Between the two panels, there are two buttons: a right-pointing arrow and a left-pointing arrow. An orange arrow points to the right-pointing arrow button. At the bottom right of the window, there is a 'Close' button. At the bottom left of the 'Available Users' panel, there is a pagination control showing 'Page 1 of 1' and '2 rows'.

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:

The screenshot shows a 'User Details' dialog box with the following information:

Name	gabrielled	Total Quota	2 GB
Email	gabrielle_95@example.com	Used Quota	0 B
Last Login	02 Feb 2021 15:03	Available Quota	2 GB
TOS Date	Not Accepted	Used Storage	0 B
Group			Manage

Below the user information is a toolbar with icons for: Manage Files, Manage Policy, Manage Shares, Mobile Devices, Reset Password, Send Email, Manage Notifications, Manage Backups, and Delete Account.

The Profile Image section shows a photo of a woman with 'Update' and 'Remove' buttons.

Access Level is set to 'Full' and Authentication is set to 'Default'.

At the bottom right are 'Save' and 'Close' buttons.

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.

Manage Policy					New policy
Filter <input type="text" value="Filter by policy name"/>					
Policy Name	User Count	Group Count	DEFAULT	Actions	
TEAM FOLDER POLICY	1	0	<input type="checkbox"/>		
Human Resources Policy	0	0	<input type="checkbox"/>		
Global Default Policy	0	0	<input checked="" type="checkbox"/>		

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.

Manage Policy Groups : Human Resources Policy ×

Available Groups

EVERYONE

Human Resources

Marketing

Policy Groups

→

←

Close

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

Policy Settings - Global Default Policy

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

Default Max Number of Downloads Allowed

0

Number of downloads allowed. Value 0 implies that the maximum number of downloads is unlimited.

User Storage Quota

Units ▾ 2 GB

Specify storage quota. 0 implies Unlimited Quota.


Enable Privacy Settings

YES ▾


Enables/disables privacy settings

Save Reset Close

To Increase the storage quota for all users:

1. In the left navigation pane, click **Settings**.
2. Click the **Policies** tab.
3. On the **Manage Policy** screen, click the edit button () for **Global Default Policy**.
4. In the **Policy Settings** dialog box, click the **General** tab.
5. On the **General** tab, enter the new value in **User Storage Quota**.
6. Click **Save**.

Enable WebDAV

-  FileCloud is preparing to deprecate WebDAV.
- Beginning with FileCloud 23.1, WebDAV can no longer be enabled or managed through the FileCloud admin portal.
 - At some time in 2024, WebDAV will no longer be available in FileCloud.

For help enabling or disabling WebDAV currently, please [Contact FileCloud Support](#).

Accessing storage using WebDAV

See [FileCloud WebDAV Access](#).

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.

FILECLOUD

Login [+ New Account](#)

Account Password

jessica

.....

Login

English

Powered by FileCloud

To customize the User Login screen

i 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**.

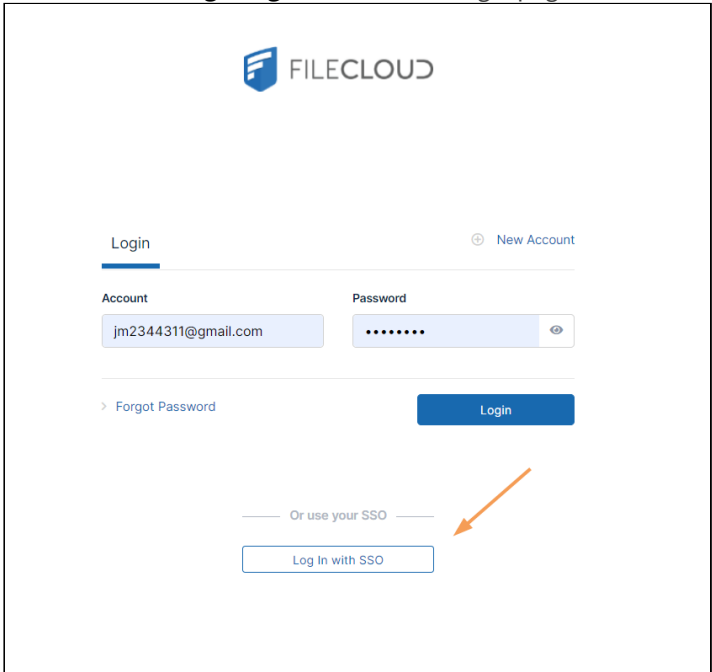
3. Select the **General** tab, and then the **Login** sub-tab.

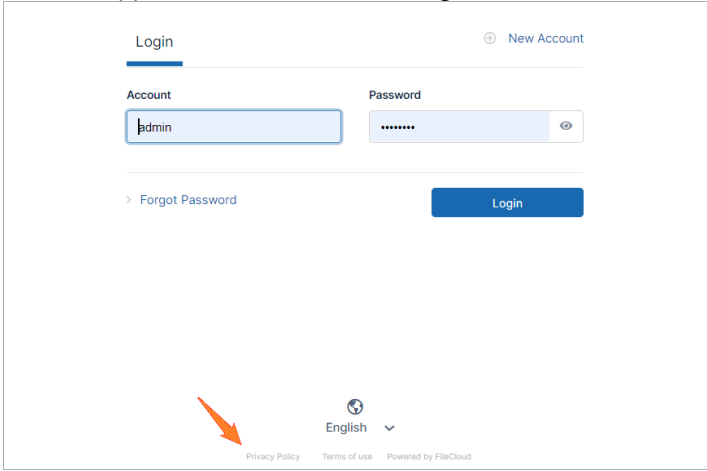
The screenshot displays the FileCloud Online settings interface. On the left is a navigation sidebar with categories: HOME (Dashboard), USERS/GROUPS (Users, Groups, Admins), MANAGE (Team Folders, Network Folders, User Shares, Folder Permissions, Notifications), DEVICES (Devices), GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), CUSTOMIZATION (Customization), and SYSTEM. The main content area is titled 'Customize User Login Screen' and has two tabs: 'General' (selected) and 'Login'. Under the 'Login' sub-tab, there are four settings:

- Show New Account Button:** A checkbox that is checked. Description: Display "New Account" button in user login screen.
- Show SSO Link:** A checkbox that is checked. Description: Show "Single Sign On" option in user login screen.
- Show Login Options:** A checkbox that is checked. Description: Uncheck to hide all login screen options such as "Forgot Password", "SSO Login".
- Login Panel Transparency:** Radio buttons for YES (selected) and NO. Description: Add transparency to login panel. Enable it if a custom login background image is set.

Below these settings are two text input fields:

- Login UI Additional Links:** A text area containing the text: [Privacy Policy](https://www.yoursite.com/privacy) and [Terms of use](https://www.yoursite.com/tos). Below the text area is a note: "Enter upto two additional links to be displayed in user login screen. Use the following format:" followed by a grey box showing the same text as an example.
- Phone Number Format Hint:** A text area containing the text: "Include + and country code with phone number." Below the text area is a note: "Message shown with phone number inputs regarding formatting".

Option	Description
Show New Account Button	<p>Displays New Account button in user log-in screen. Enabled by default.</p> <p>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.</p>
Show SSO Link	<p>Check to show Single Sign On link in the login page:</p> <div data-bbox="756 527 1463 1194" style="border: 1px solid black; padding: 10px; margin: 10px 0;">  <p>The screenshot shows the FileCloud login interface. At the top is the FileCloud logo. Below it, there are two tabs: 'Login' (active) and 'New Account'. Under the 'Login' tab, there are input fields for 'Account' (containing 'jm2344311@gmail.com') and 'Password' (masked with dots). Below these fields are links for 'Forgot Password' and a 'Login' button. At the bottom, there is a section 'Or use your SSO' with a 'Log In with SSO' button. An orange arrow points to this button.</p> </div> <p>Note: If this is checked, but Show Login Options is unchecked, Single Sign On link is not shown.</p> <p>💡 The functionality of this button is determined by how you configure Single Sign-On Access</p>
Show Login Options	<p>Uncheck to hide options in login screen such as Forgot Password and Single Sign On link even if Show SSO Link is checked.</p>
Login Panel Transparency	<p>Adds transparency to login panel.</p> <p>Set to:</p> <ul style="list-style-type: none"> • YES (default) • NO <p>💡 Enable this option if you are using a custom login background image.</p>

Option	Description
Login UI Additional Links	<p>Enter up to two additional links to be displayed in user login screen. Use the format:</p> <p>[Privacy Policy] (https://www.yoursite.com/privacy) [Terms of use] (https://www.yoursite.com/tos)</p> <p>The links appear at the bottom of the login screen:</p> 
Phone Number Format Hint	<p>Enter a hint to appear on screens where users can enter phone numbers. For example <i>Include + and country code when entering phone number.</i></p>

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 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**.

The screenshot shows a settings interface with a top navigation bar containing tabs: General, Labels And Logos, URL, UI Messages, Email Templates, News Feed, TOS, and Advanced. Below this is a sub-navigation bar with tabs: UI Features, Login, Account Menu, and Listing. The 'Login' tab is active. The main content area is titled 'Customize User Login Screen' and contains three settings:

- Show New Account Button** Display "New Account" button in user login screen
- Show SSO Link** Show "Single Sign On" option in user login screen
- Show Login Options** Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

Orange arrows in the original image point to the 'Show SSO Link' and 'Show Login Options' checkboxes.

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 admin portal, go to **Settings > Policies**, and click the edit icon for the policy that you want to modify.

2. Click the **User Policy** tab.

Policy Settings - Global Default Policy

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

General 2FA **User Policy** Client Application Policy Device Configuration Notifications

User Policy

Disable Invitations to New Users
NO

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

Create account on new user shares
NO

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

Enable code based device authentication

Save Reset Close

3. Scroll down to the **Max File Size Limit** setting.
4. Enter the maximum file size that can be uploaded.

Policy Settings - Global Default Policy

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

NO

Enables/disables mandatory workflow automation for shares

Max. File Size Limit

Units 3072 MB

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

Save Zip File Session Password

NO

Allow passwords to be saved inside encrypted zip files. Warning: Disabling the setting will require a password every time you access a file.

Save Reset Close

5. Click **Save**.

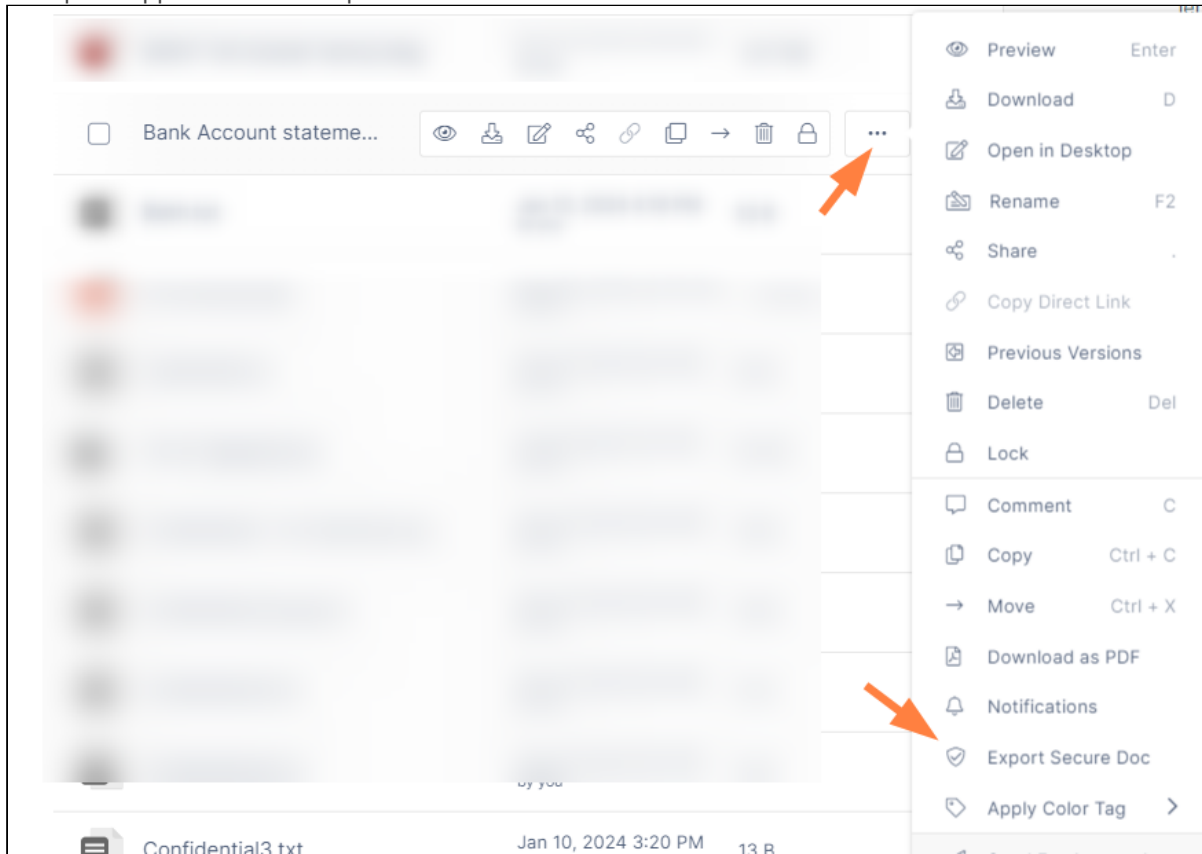
⚠ Max File Size Limit does not apply to Sync and Drive and other non-Web FileCloud clients.

For help applying **Max File Size Limit** to non-web FileCloud clients, please [Contact FileCloud Support](#).

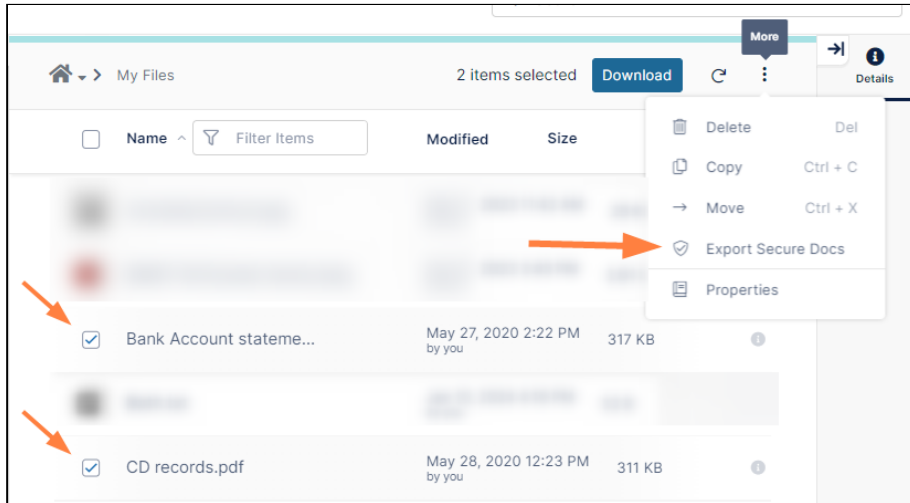
Remove the Export Secure Doc Option

If your FileCloud license includes DRM, any file of a type that is supported by DRM (**jpg, png, docx, pptx, and pdf**) has the **Export Secure Document** option enabled. When users choose this option, the downloaded file may only be viewed through the FileCloud Secure Viewer using an access key.

The option appears in the user portal either in the action menu for a file



or the action menu for multiple files:



By default, users may delete backup files. Beginning in FileCloud Version 21.1, you can disable user's ability to delete backup files..

To hide the Export Secure Docs option:

1. Open cloudconfig.php:
Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
Linux Location: /var/www/config/cloudconfig.php
2. Add:

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

3. To return to the default, change **true** to **false** or remove the setting.

Group Settings

Administrators can create groups of users in FileCloud Server. Creating groups allows [sharing of files and folders](#).

- ⚠** An automatic group called "EVERYONE" is created by default for every FileCloud installation. This is a special group that contains all active full users in the FileCloud system. Be sure to set a valid email address for the group in the [group details](#) OR [delete the group](#) if "EVERYONE" is not needed)
- External users are not included in the EVERYONE group.**

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.

Show me where to manage groups in the Admin Portal

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

The screenshot shows the 'Manage Groups' interface in the FileCloud Admin Portal. The left navigation menu has 'Groups' highlighted with a red arrow. The main content area displays a table of groups with the following data:

Group Name	Created On	Users in Group	Manage
Approvers	Oct 05, 2021 12:56 PM	2	Edit Delete
EVERYONE	Apr 26, 2021 11:59 AM	9	Edit Delete
Human Resources Group	Sep 22, 2021 9:28 AM	4	Edit Delete
Internal	Sep 21, 2021 4:58 PM	1	Edit Delete
Marketing	Sep 22, 2021 9:39 AM	1	Edit Delete

The **Everyone** group is included by FileCloud. It contains all [Full and Guest users](#).

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.

The screenshot shows the 'Manage Group' interface. At the top, there is a 'Group Name' field containing 'Approvers' and a 'Save' button. Below this are three tabs: 'Members', 'Admins', and 'Policies'. The 'Members' tab is selected. Under 'Members Management', there is a search bar labeled 'Search Users...' and a link 'Import Users from AD Group'. Below that, a section titled 'Users in Group (3 members in this group)' contains a 'Filter users' input field and an 'Export' link. A table lists three users with their names and email addresses, each with a 'Remove' button.

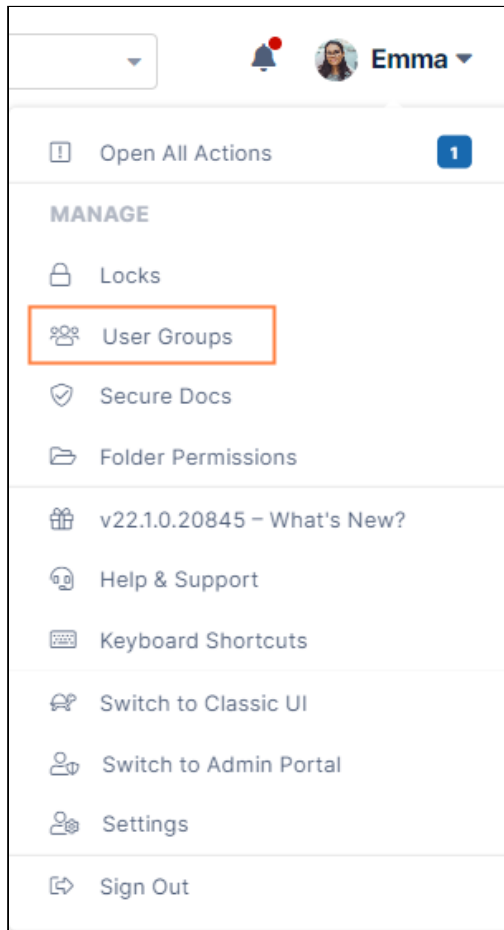
Users	
david dm898002@gmail.com	Remove
Jared jaredtaylor978@gmail.com	Remove
Jessica jm2344311@gmail.com	Remove

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.

Manage Group

Group Name: Save

Members **Admins** Policies

Group Admin Management

Q

jessicam
jm2344311@gmail.com Add

No Records Found

Close

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.

Manage Group

Group Name: Save

Members **Admins** Policies

Group Admin Management

Q

Group Admins	Can view users	Can add users	Can remove users
jessicam	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Remove

< Page 1 of 1 >

Close

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.

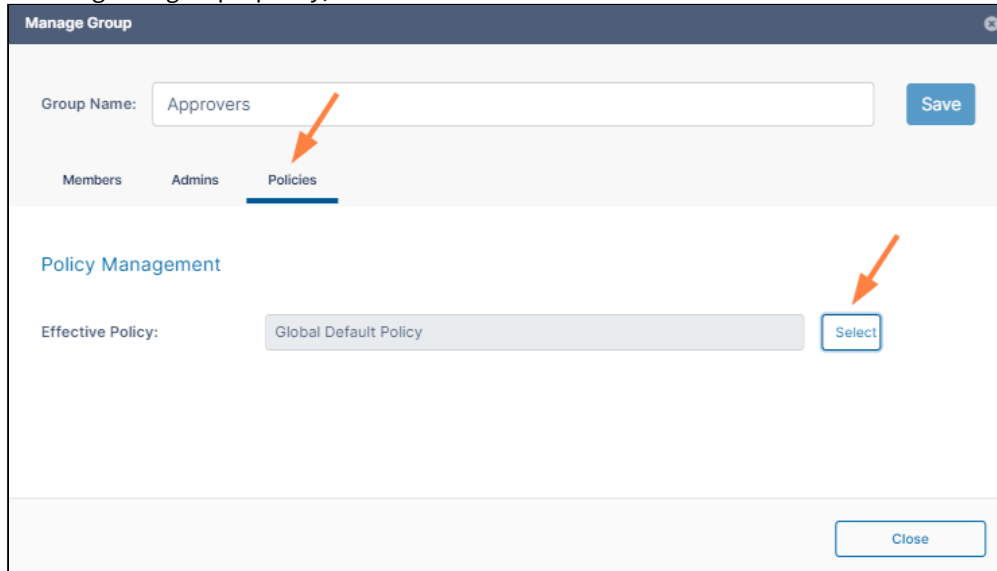
Change a Group's Policy

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

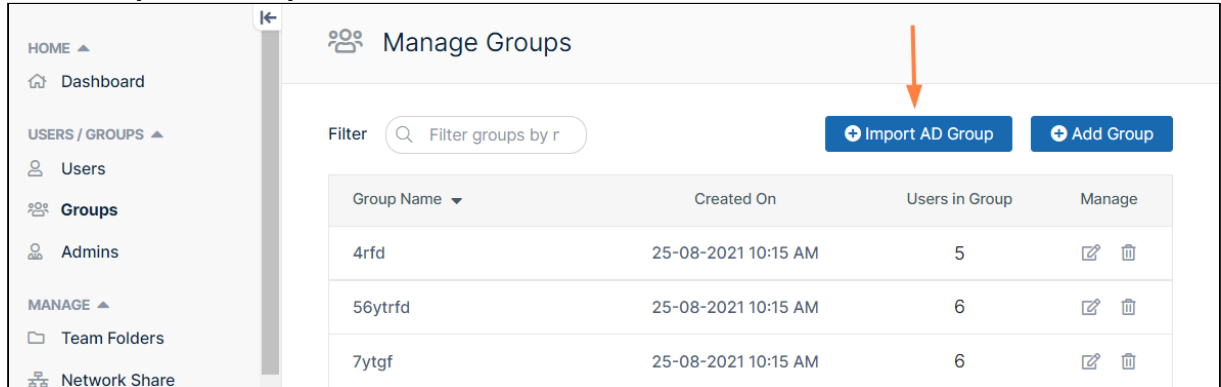
You can also import an existing AD group from an [Active Directory Server](#) connected to FileCloud.

- i** The ability to automatically remove users not in a group during AD group import is available in FileCloud version 18.2
- 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:

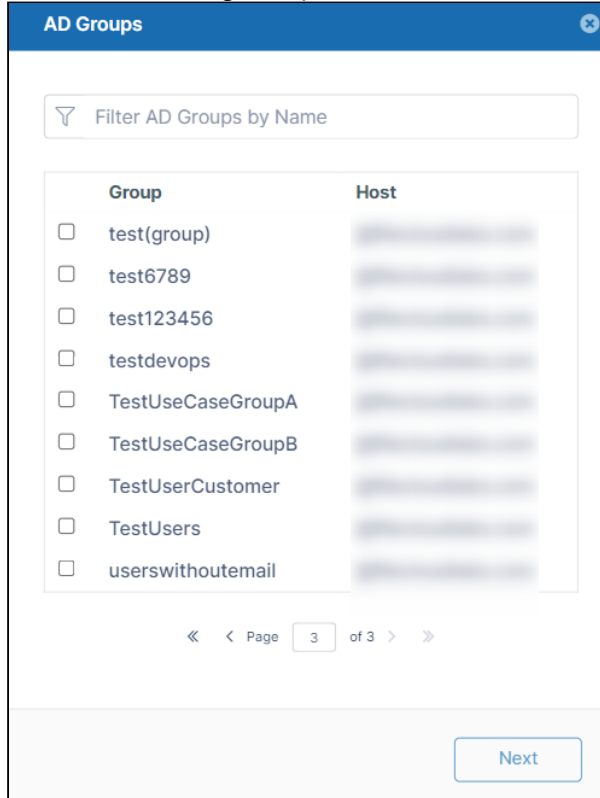
1. Open a browser and log in to the admin portal.
2. On the left control panel, click **Groups**.
3. Click the **Import AD Group** button.



The screenshot shows the 'Manage Groups' page in the FileCloud admin portal. On the left is a navigation menu with 'Groups' selected. The main area has a search filter and two buttons: 'Import AD Group' (highlighted with an orange arrow) and 'Add Group'. Below is a table of existing groups.

Group Name	Created On	Users in Group	Manage
4rfd	25-08-2021 10:15 AM	5	Edit Delete
56ytrfd	25-08-2021 10:15 AM	6	Edit Delete
7ytgf	25-08-2021 10:15 AM	6	Edit Delete

An **AD Groups** dialog box opens:



The 'AD Groups' dialog box is shown with a search filter 'Filter AD Groups by Name'. It contains a list of AD groups with checkboxes for selection. The 'Next' button is visible at the bottom right.

Group	Host
<input type="checkbox"/> test(group)	
<input type="checkbox"/> test6789	
<input type="checkbox"/> test123456	
<input type="checkbox"/> testdevops	
<input type="checkbox"/> TestUseCaseGroupA	
<input type="checkbox"/> TestUseCaseGroupB	
<input type="checkbox"/> TestUserCustomer	
<input type="checkbox"/> TestUsers	
<input type="checkbox"/> userswithoutemail	

Page 3 of 3

Next

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

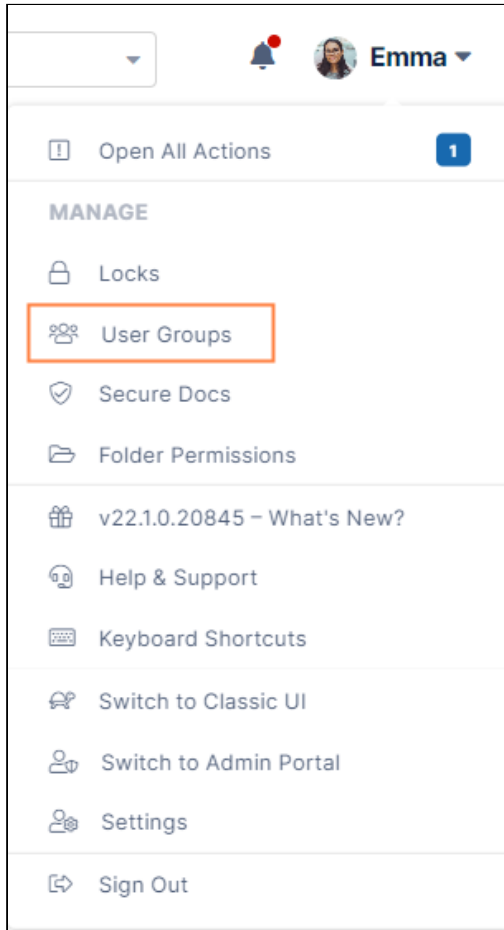
5. **Automatic Sync** is selected by default. Leave it selected to enable FileCloud to automatically add users to the FileCloud group that are added to the AD group. This sync is done every 24 hours.
 - The first time members from the AD group are imported as members of the FileCloud Group.
 - In the 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 if 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.

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. Go to **Settings > Policies**.
2. [Create a new policy](#) for user group management or edit an existing policy.
3. Edit the policy, and click the **User Policy** tab.

4. Scroll down to see the Group policy settings.
By default, each is set to **NO**.

Policy Settings - User Group Management ✕

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

Disable everyone group snaring

Allow New Group Creation	<input style="width: 100%; border: 1px solid #ccc;" type="text" value="NO"/>
<small>Allows users to create groups from user portal</small>	
Allow User Group Management (Add and Remove users)	<input style="width: 100%; border: 1px solid #ccc;" type="text" value="NO"/>
<small>Allows users to add or remove users from groups in user portal</small>	
Allow Group Deletion	<input style="width: 100%; border: 1px solid #ccc;" type="text" value="NO"/>
<small>Allows group removal from user portal</small>	
Disable Workflow Automation	<input style="width: 100%; border: 1px solid #ccc;" type="text" value="NO"/>
<small>Enables/disables workflow automation</small>	

5. Change the group settings that you want to enable for users with this policy.
- **Allow New Group Creation** - Allows the user to add new groups and manage members in the groups from the user portal.
 - **Allows User Group Management (Add and Remove Users)** - 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 set to **YES**, 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.

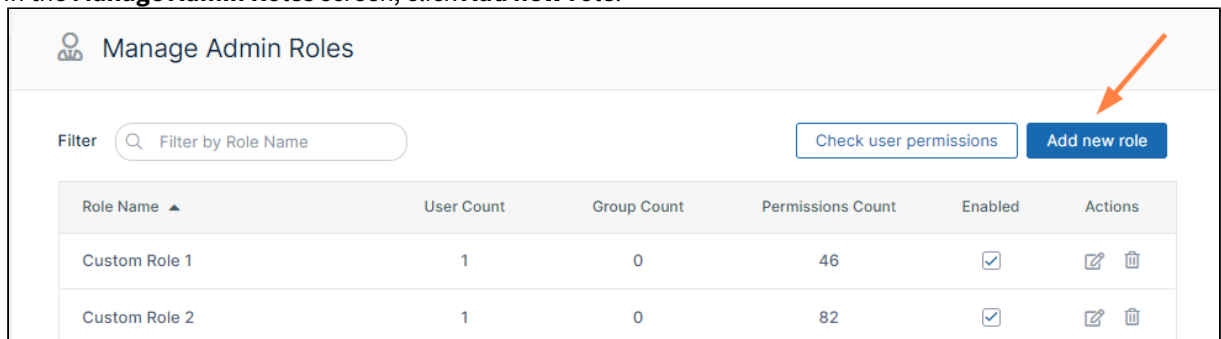
Admin User. User accounts that can access the FileCloud admin interface.

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

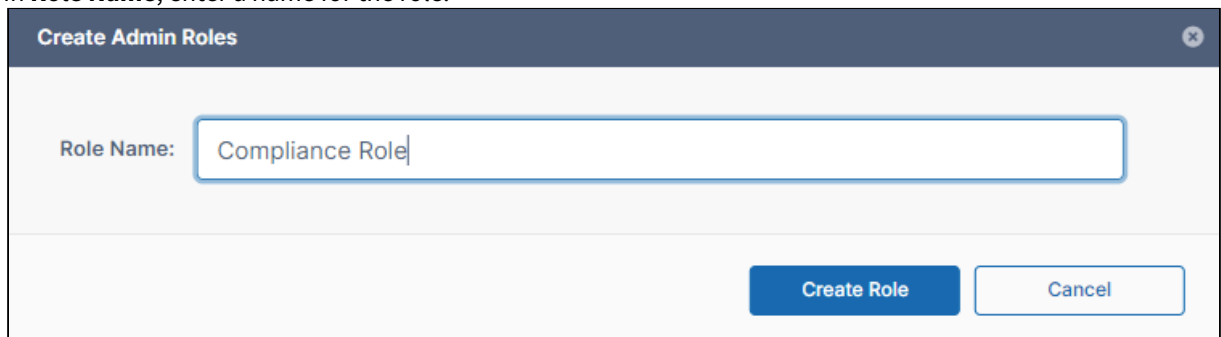
To create admin roles and add users to them:

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.

Manage Admin Roles ✕

Role Name: Enable

Permissions
Users
Groups
i

Permissions

Operation	Read	Create	Update	Delete
Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federated Search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

« < Page 1 of 4 > »

Remove Role
Close

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 an admin user.

The screenshot shows the 'Manage Admin Roles' window. At the top, the 'Role Name' is 'Compliance Role' and the 'Enable' toggle is turned on. Below this are three tabs: 'Permissions', 'Users' (which is selected), and 'Groups'. The 'Users' section is titled 'Users' and contains the heading 'Add Users to Role'. A search input field contains the text 'jm', with an orange arrow pointing to it. Below the search field, a dropdown menu shows a search result for 'jessicam' with the email 'jm2344311@gmail.com' and an 'Add' button. Below the dropdown is a 'Filter users...' input field. Further down, a user card for 'Gaby' is visible with a 'Remove' button. At the bottom of the window, there is a 'Remove Role' button on the left and a 'Close' button on the right.

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.

Manage Admin Roles

Role Name: Enable

Permissions Users **Groups**

Groups

Add Groups to Role

Human
Resources Group

Filter groups

No Records Found

10. Click **Close**.

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

Manage Admin Roles

Filter

Role Name ▲	User Count	Group Count	Permissions Count	Enabled	Actions
Compliance Role	2	1	29	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Custom Role 1	2	0	46	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Custom Role 2	1	0	82	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Login Screen Edits	1	0	4	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Security	0	0	0	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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, create, 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. <i>Note: The corresponding Folder Permission must be enabled to be able to perform a Team Folder operation.</i>
User Share	User Shares item on the admin interface is visible. Authorization to view, create, modify and delete User Shares.

Operation	Description
Users	Users menu item on the admin interface is visible. Authorization to view, create, modify and delete Users. Import New Users. Reset Password for Users.
Workflow	Workflow menu item on the admin interface is visible. Add, edit and delete workflows on FileCloud.

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

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 be 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 be 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

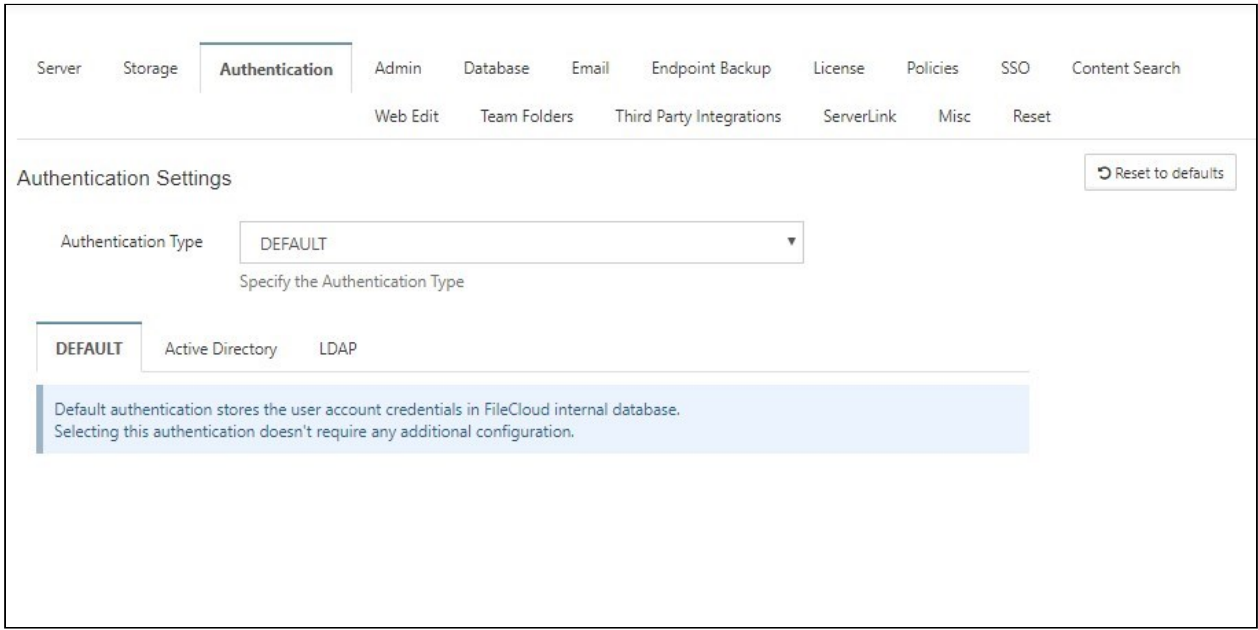
Initially, FileCloud is set to default authentication mode. User accounts created when this authentication type is configured have credentials stored and managed within FileCloud.

A user account that uses this type of authentication is also known as a local user.

-  As this authentication method is fully managed by FileCloud, there are no prerequisites.


To enable Default Authentication:

1. Log in to the FileCloud Admin Portal.
2. In the left navigation panel, click **Settings**.
3. In the right panel, from the selection of tabs, click **Authentication**.
4. Under *Authentication Settings*, in *Authentication Type*, select **DEFAULT**.



Active Directory Authentication

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

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

Note

The AD user will count towards FileCloud License only after:

- The user account logs into FileCloud
- If a user from AD is explicitly imported

Prerequisites

Required	Configuration Requirement	Notes
Active Directory service	Must be accessible from FileCloud	IP and Port must be accessible.

Required	Configuration Requirement	Notes
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	Version must be 4.0 or later	

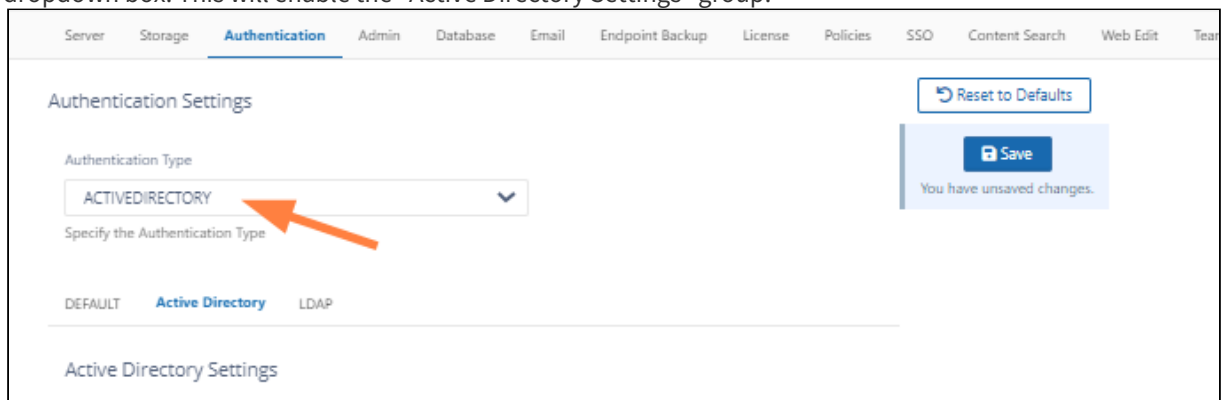
How To Enable AD Authentication

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

Enabling AD Authentication

To enabling AD authentication in FileCloud:

1. Log into the [FileCloud Administration Portal](#)
2. Click on **Settings** in the left navigation panel
3. Click on **Authentication** tab
4. Under **Authentication Settings**, change the Authentication Type to "ACTIVEDIRECTORY" using the dropdown box. This will enable the "Active Directory Settings" group.



The screenshot shows the 'Authentication Settings' page in the FileCloud Administration Portal. The 'Authentication Type' dropdown menu is set to 'ACTIVEDIRECTORY', with a red arrow pointing to it. The page also features a 'Reset to Defaults' button and a 'Save' button. A notification at the bottom right states 'You have unsaved changes.' Below the dropdown, there are tabs for 'DEFAULT', 'Active Directory', and 'LDAP'.

5. 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, enter the correct connection parameters.

Check AD Test **AD Test**

AD Host*
Specify the AD host name

AD Port*
Specify the AD port number, usually 389

Use TLS
Enable to use TLS for the connection

Use SSL
Enable to use SSL for the connection

Users have same UPN Account Suffixes
Users have same UPN Account Suffixes

AD Account Suffix

AD Base DN
Specify the user search DN, example 'DC=filecloud,DC=local'

Mail Attribute
Specify the AD mail attribute, usually 'mail'

Limit Login to AD Group
Specify the AD Group Name to limit users who can login (Optional)

AD Account Name*
Specify a AD account to use for admin operations

AD Account Password*
Specify a AD account password to use for admin operations

Disable Anonymous Binding
Use a service account to bind with AD server instead of Anonymous binding (optional)

AD Service Account Name
Specify the service account to use for binding to the AD server

AD Service Account Password
Specify the service account password

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 - Optional. Enable this checkbox if your AD server requires clients to use TLS to connect.

Use SSL - Optional. Enable this checkbox if your AD server requires clients to use SSL to connect.

NOTE: Additional change required.

Users have the same UPN Account Suffixes

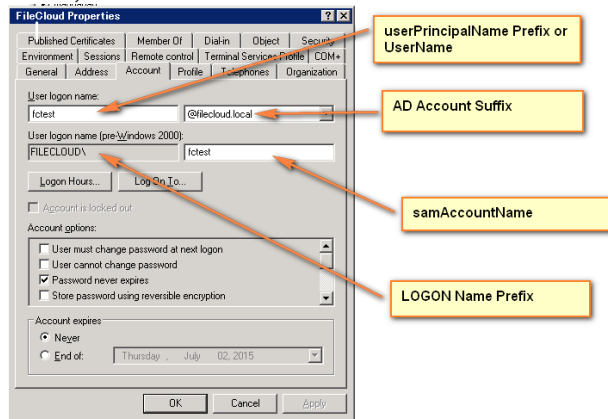
All of your AD users should have the same suffix or the same prefix.

- If your users have the same UPN suffixes: Enable this checkbox and enter the suffix in the next field, **AD Account Suffix**.
- Otherwise: Disable the checkbox. 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](#).

Users have same UPN Account Suffixes
Users have same UPN Account Suffixes

AD Logon Name Prefix
Specify the AD Logon Name Prefix, example 'FILECLOUD'

To find the **AD Logon Name Prefix** and the **AD Account Suffix**, refer to:



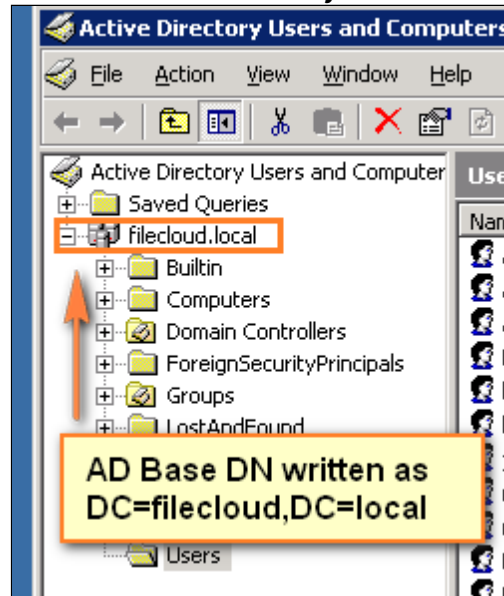
AD Account Suffix - The UPN suffix for your domain, the part after **User logon name** in the dropdown next to it in the above screenshot.

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
```

```
C:\Documents and Settings\Administrator>dsquery * cn=testadi,cn=users,dc=filecloud,dc=local -scope base -attr sAMAccountName userPrincipalName
sAMAccountName      userPrincipalName
testadi              testadi@filecloud.local
```

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>
```

```
C:\Documents and Settings\Administrator>dsquery user -name testadi
"CN=testadi,CN=Users,DC=filecloud,DC=local"
```

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.

	<p>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.</p> <p>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.</p> <p>Notes: Enter username, not email id in this field. This account must have an email address set in AD.</p> <p>AD Account password - A password for the AD account name.</p> <p>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.</p> <p>AD Service Account Name - Optional. The service account name to use to bind with the AD server.</p> <p>AD Service Account Password - Optional. The service account password to use to bind with the AD server.</p>

 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.

At the top of the Active Directory settings, click the **AD Test** button.

Active Directory Settings

Check AD Test **AD Test**

AD Host*
Specify the AD host name

AD Port*
Specify the AD port number, usually 389

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

Test AD Configuration

Basic Verification **Validate AD Settings**

Group Members **List Groups** **Get Group Members**

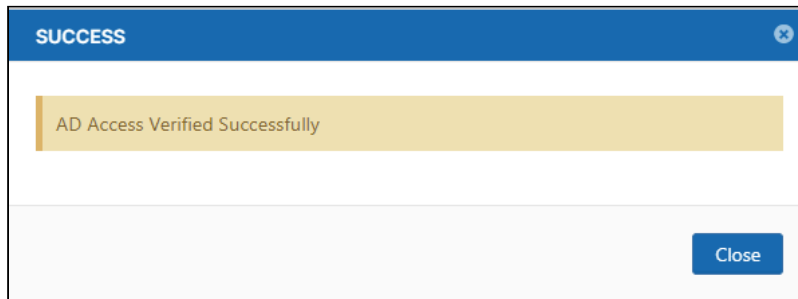
Verify User Access

Test Login **Get Email ID**

Close

The following tests can be done.

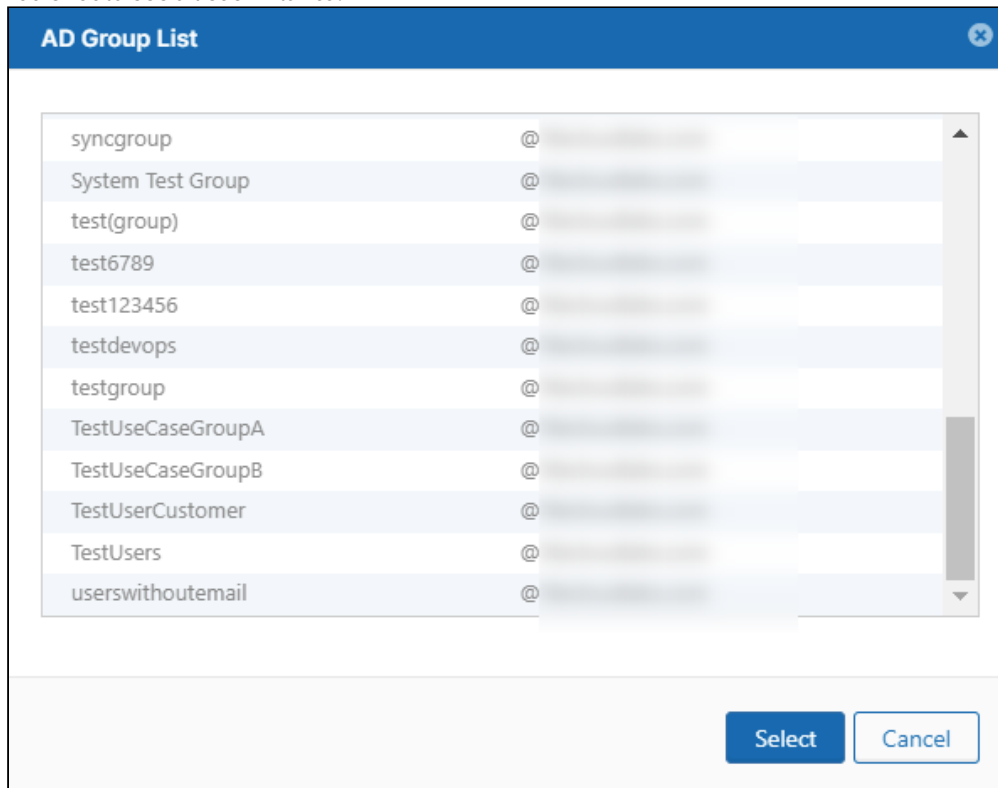
1. Validate AD settings.
 - a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server.
You should receive the response:



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

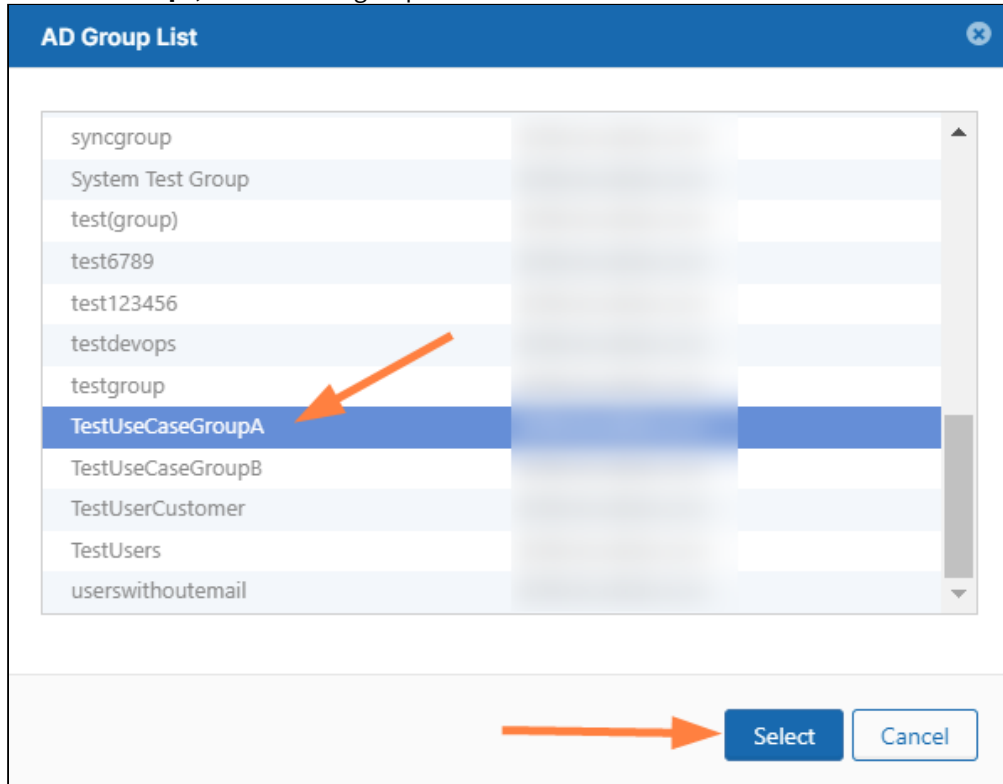
2. List Groups

- 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

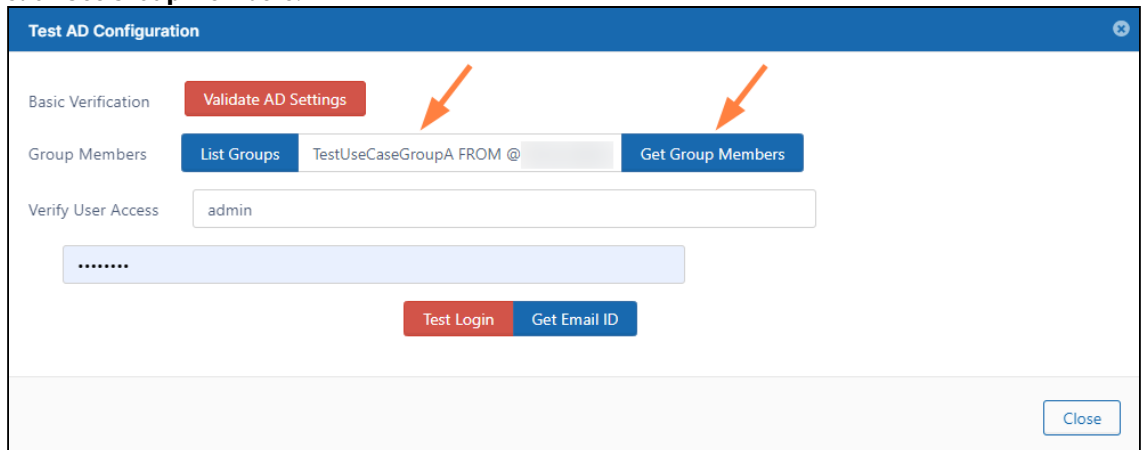
1. Click **List Groups**, then select a group and click **Select**.



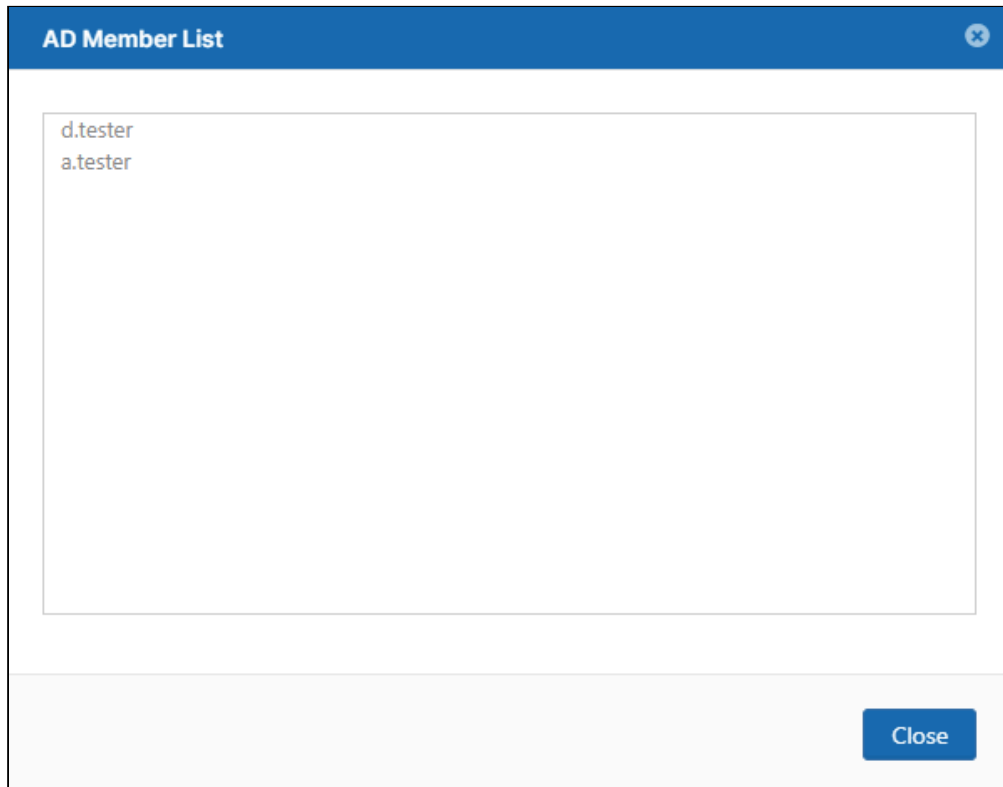
The Group name appears in the **Test AD Configuration** dialog box.

(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
<p>Active Directory Settings</p>	<p>Import Users to AD via PowerShell</p>

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

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

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

To enable the use of SSL Certificates in FileCloud Server:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation menu, under *Settings*, select the *Settings* tab.
3. On the *Settings* screen, select the *Authentication* tab.
4. On the *Authentication* tab, under *Authentication Settings*, select the *Active Directory* tab.
5. On the *Active Directory* tab, under *Active Directory Settings*, in *AD Port*, change the number to 636.
6. On the *Active Directory* tab, under *Active Directory Settings*, select the *Use SSL* check box.

7. Click *Save*.

How do I connect to AD using TLS?

Connecting to Active Directory over TLS

TLS

To use TLS, Port 389 should be used instead of the 636

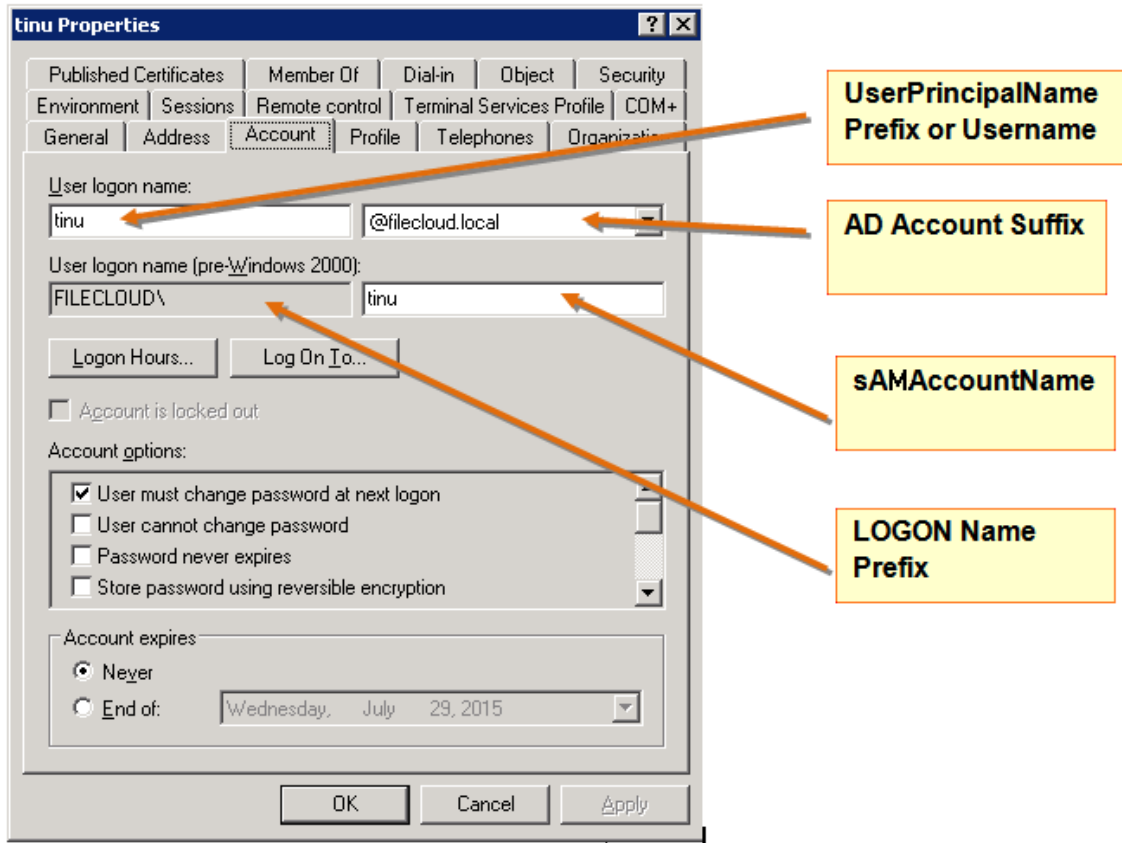
Mixed AD Domain Environments

In some AD environments, there could be multiple UPN domain suffixes setup 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 it causes problems identifying the user account correctly.

Therefore if you want FileCloud to authenticate using these kinds of environments, you need to setup the AD connection information slightly differently. In those 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, this is the prefix used in the non-editable part in the User Logon Name (Pre-Windows 2000)



Users can login 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 recognise this change. All the files the user owns still belong to the old account.


To migrate the account data to the new AD account, please follow these steps:


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


User Details ✕


Name	john	Total Quota	2 GB
Email	john@xyz.com	Used Quota	0 B
Last Login	--	Available Quota	2 GB
Group	Manage	Used Storage	0 B More~



 Mobile Devices



 Manage Files



 Manage Shares


 Reset Password


 Email Password


 Delete Account


 Manage Policy


 Manage Backups

Access Level:

Authentication:
External (AD/LDAP)

Email:

Display Name:

Account Expires On:

Password Expires On:

Email Verified:

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

4. Ask the user to log in via Web User Portal.

5. The user needs to use the new account/password (AD).

6. Reset the Sync App settings and enter the user's new domain credentials without removing the data. See [Sync Settings](#).

7. Log in to the Sync App with the new account credentials; don't remove the data from the computer.

8. 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 this 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. In **Settings > Authentication** on the **Active Directory** tab, 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.

At the top of the Active Directory settings, click the **AD Test** button.

The screenshot shows the 'Active Directory Settings' interface. At the top, there are three tabs: 'DEFAULT', 'Active Directory' (which is selected), and 'LDAP'. Below the tabs, the title 'Active Directory Settings' is displayed. On the left, there is a 'Check AD Test' checkbox. To its right is a blue 'AD Test' button, which is pointed to by an orange arrow. Below these are two input fields: 'AD Host*' with the value '192.168.1.191' and the instruction 'Specify the AD host name', and 'AD Port*' with the value '386' and the instruction 'Specify the AD port number, usually 389'.

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

Test AD Configuration [X]

Basic Verification **Validate AD Settings**

Group Members **List Groups** AD Group Name **Get Group Members**

Verify User Access User Name

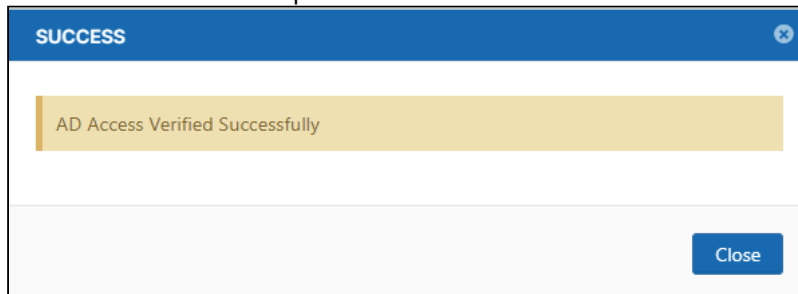
Password

Test Login **Get Email ID**

Close

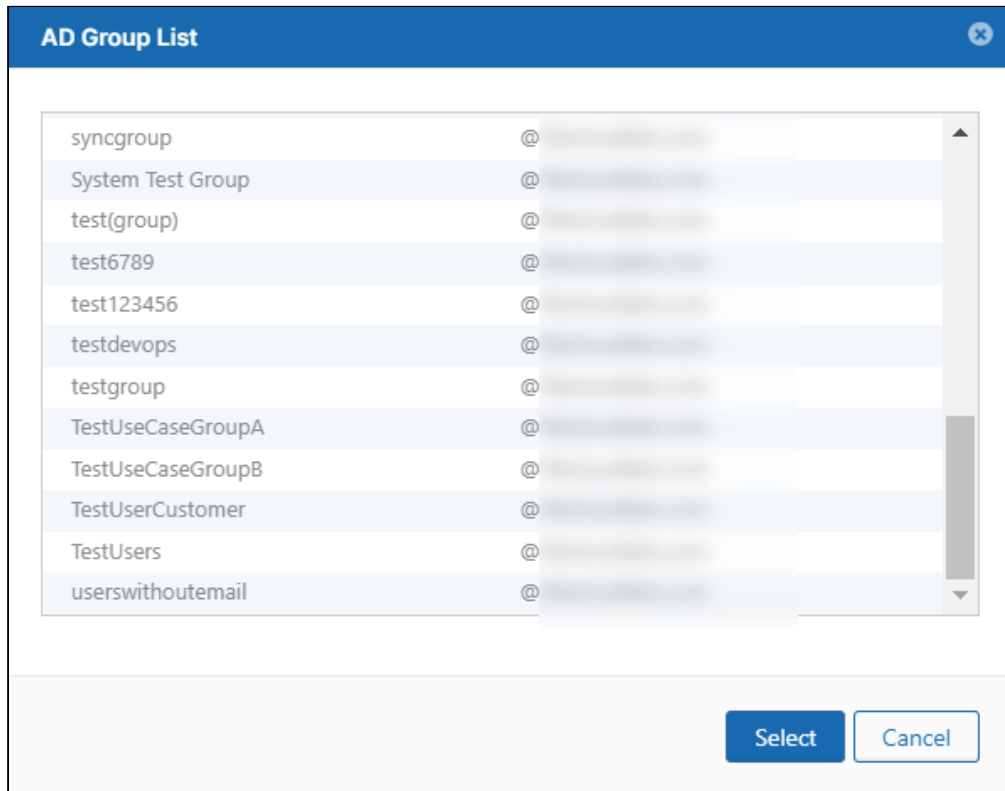
The following tests can be done.

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:



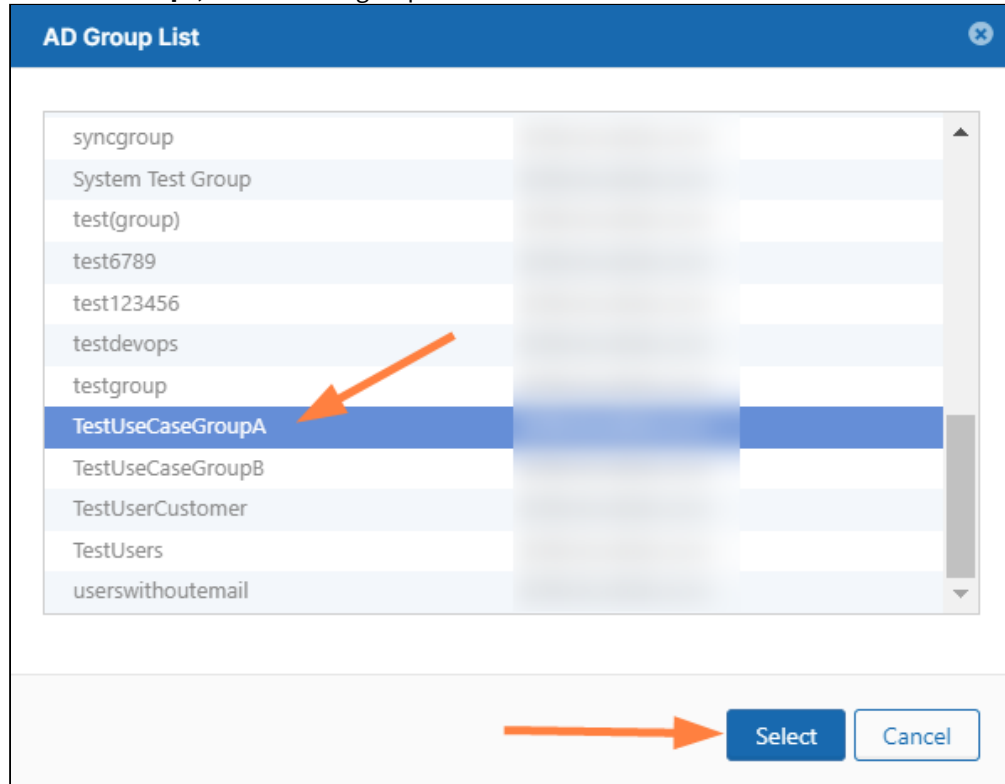
If the tests fail, then check your AD settings to ensure all the data is present and is accurate.

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

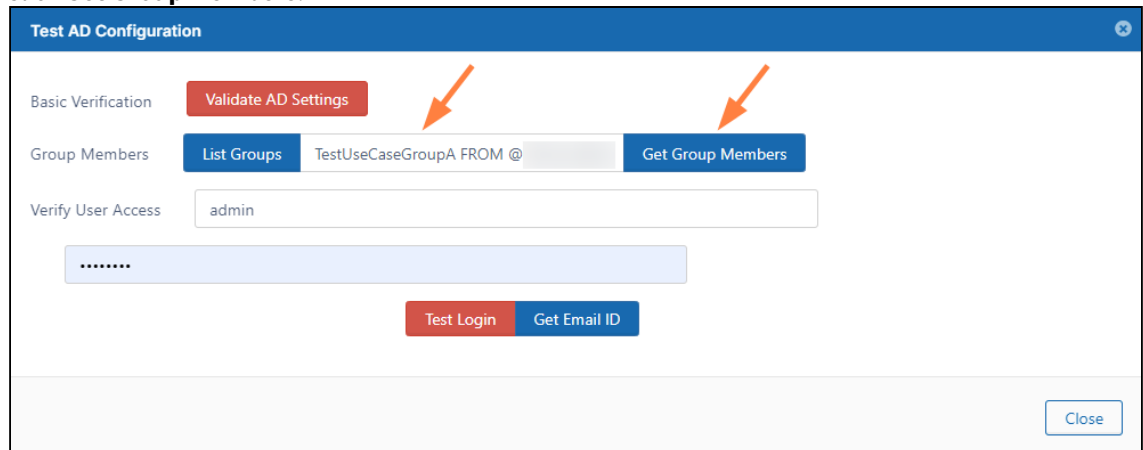
1. Click **List Groups**, then select a group and click **Select**.



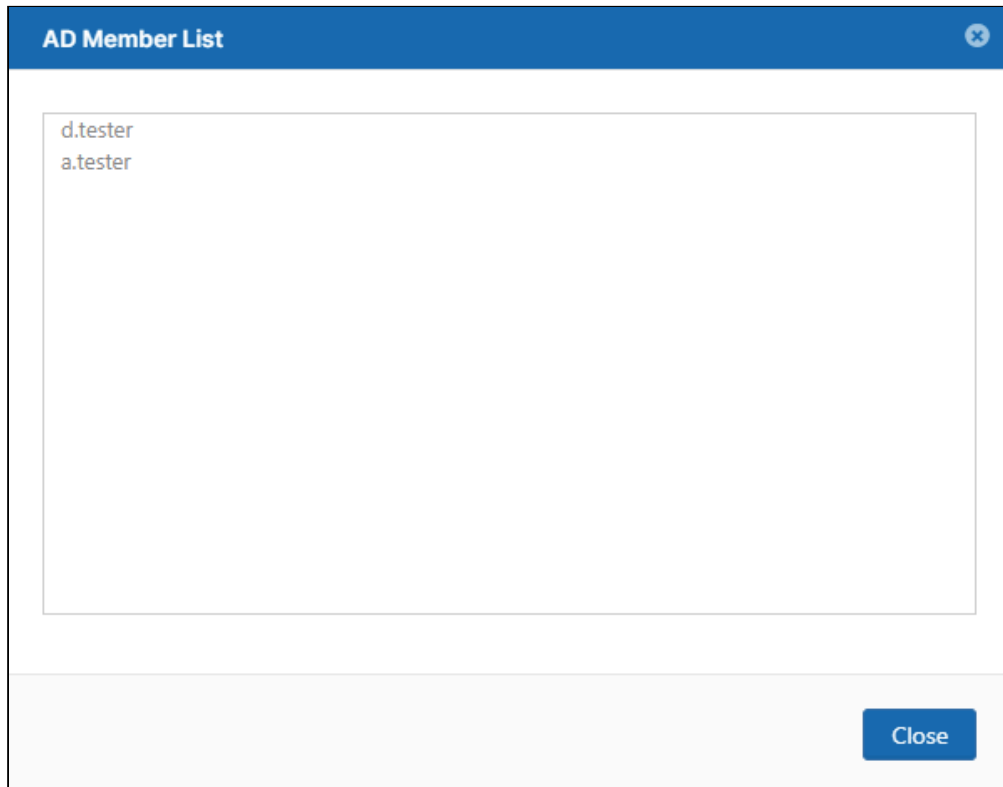
The Group name appears in the **Test AD Configuration** dialog box.

(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 Account Suffix**, 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 will not be able to log in to FileCloud.

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

Check if **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 admin portal, go to **Settings > Server** and 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 be able to log in to FileCloud.
2. In **Limit Login to AD Group**, enter the name of the AD group.

Single sign-on (SSO)

i 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

i Updates to SAML SSO

As of FileCloud Version 19.1, the ability to limit users to SSO by group is available.
As of FileCloud Version 19.2, FileCloud can detect an SSO email and automatically redirect the user to the corresponding IDP provider with prefilled login information for the user.

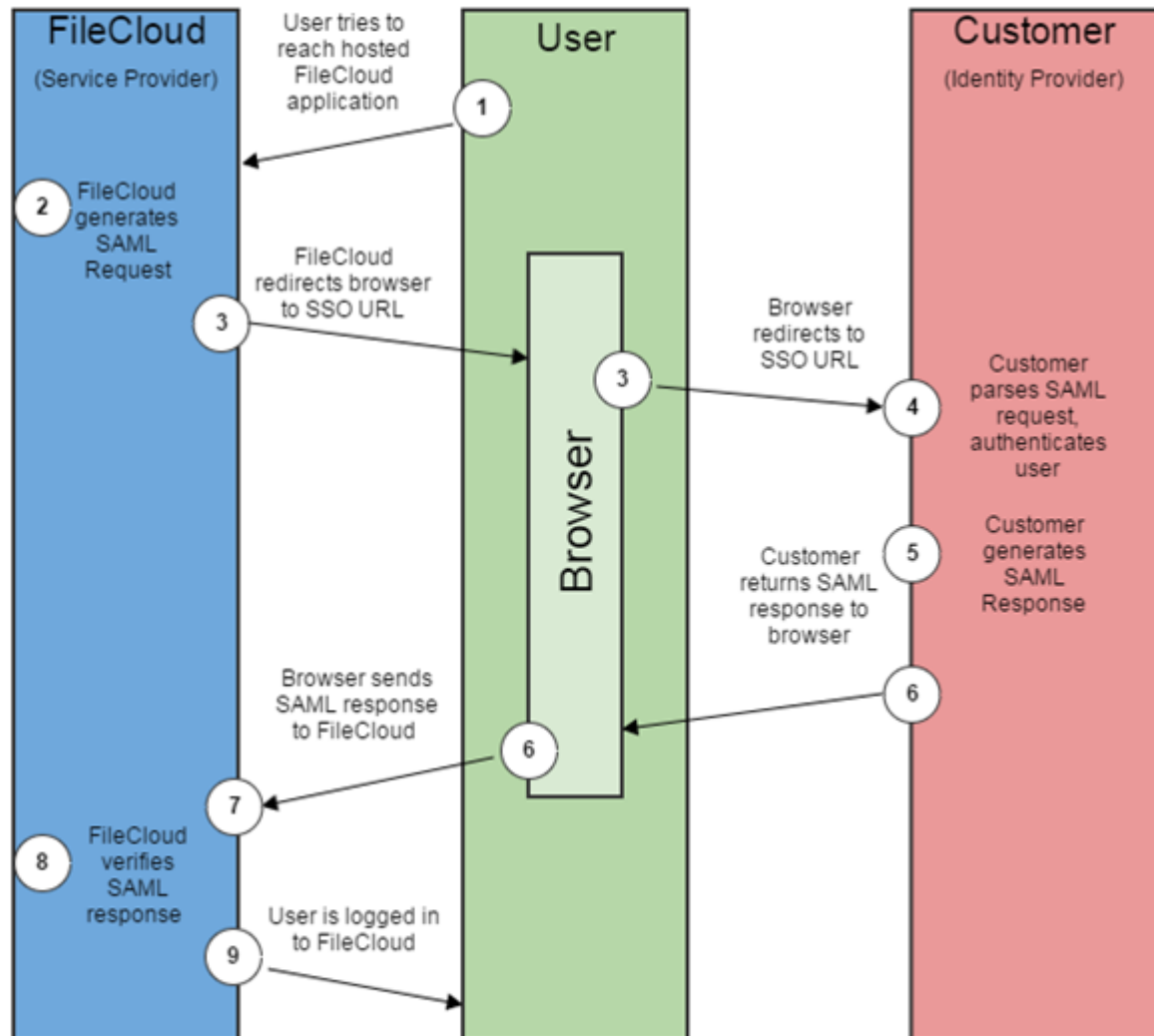
You can use SAML SSO to control the authorization and authentication of hosted user accounts that can access FileCloud Web based interface.

- 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 transaction 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.

- i** When the IdP successfully authenticates the user account, 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.

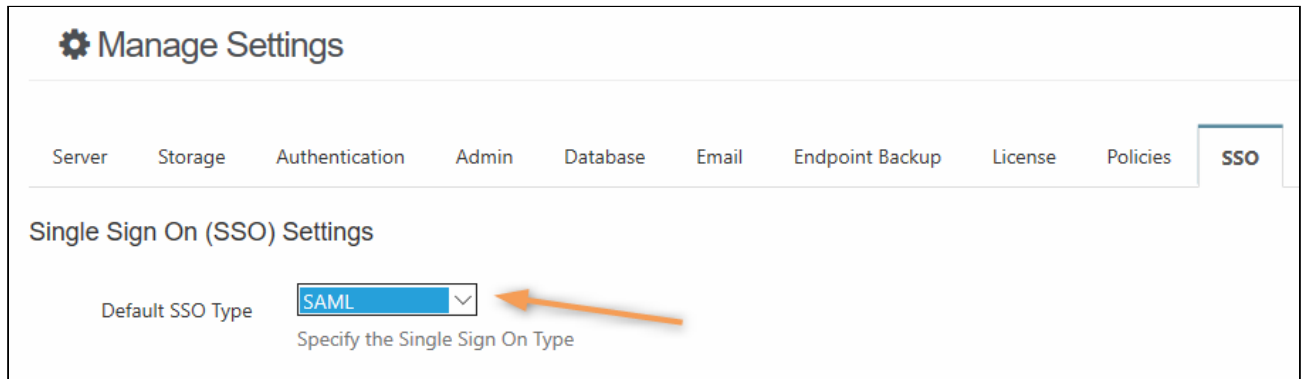
To ensure the correct FileCloud URL is set, and that it uses HTTPS:

1. In the admin portal, go to **Settings > Server**.
2. In the **Server URL** field, confirm that your URL begins with HTTPS.
3. Click **Check URL** to make sure your URL is valid.

The screenshot displays the 'Server Settings' page in the FileCloud admin portal. The left sidebar shows navigation options under 'GOVERNANCE', 'MISC.', and 'SETTINGS'. The main content area is titled 'Server' and includes a 'Reset' button. The 'Server Settings' section contains the following fields and options:

- Service Name:** A text input field containing 'FileCloud'.
- Server URL:** A text input field containing 'https://DepartmentXYZ.filecloud.com'. A blue 'Check URL' button is positioned to the right of the field. Below this field, a note reads: 'Server URL is the url via which users access the service.'
- Session Timeout (Minutes):** A text input field containing '1440'. Below this field, a note reads: 'Specify user web login session timeout. Example: 15 = Default timeout of 15 minutes, 30 = 30 minutes, 60 = 1 hour. Note: Session will always expire when browser is closed unless advanced configuration is done.'
- WebDAV:** A checkbox labeled 'Enable to allow WebDAV access to server', which is currently unchecked.

3. Set SAML as the default Single Sign On Method in FileCloud.



To set the SSO type in FileCloud:

1. Log into the FileCloud *admin portal*.
2. In the left navigation panel, click **Settings**.
3. **Select the SSO tab.**
4. **In Default SSO Type, select SAML.**

4. Configure IdP settings in FileCloud.

✔ Active Directory Federation Services (ADFS) Support

When SAML SSO Type is selected and ADFS is enabled in FileCloud:

- FileCloud will act as a Service Provider (SP)
- FileCloud also acts as a claims aware application.

As a claims-aware application, FileCloud:

- Accepts claims in the form of ADFS security tokens from Federation Service
- 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.

💡 When ADFS is used, the IdP (Identity Provider) in these instructions refers to Active Directory Federation Server.

To configure IdP settings in FileCloud:

1. Log into the FileCloud *admin portal*.
2. In the left navigation panel, click **Settings**.
3. **Select the SSO tab.**
4. **In Default SSO Type, verify it is set to SAML.**
5. Set other parameters according to your IdP settings.

SAML Settings

Idp Endpoint URL or EntityID*

URL or EntityID of the Identity Provider that the Service Provider must contact.

IdP Username Parameter*

Username Parameter Name in Identity Provider

IdP Email Parameter*

Email Parameter Name in Identity Provider

IdP Given Name Parameter*

Given Name Parameter Name in Identity Provider

IdP Surname Parameter*

Surname Parameter Name in Identity Provider

IdP Log Out URL (Optional)

URL to call to logout of Identity Provider (Optional)

Limit Login to Idp Group (Optional)

Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute

IdP Metadata*

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
entityID="http://www.okta.com/exk172d54g9EArRV40
h8"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<md:IDPSSODescriptor
WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAM
L:2.0:protocol"><md:KeyDescriptor use="signing">
<dc:KeyInfo
```

Enter Identity Provider metadata in XML format

SSO Error Message (Optional)

```

<div align = "center">
  <p><b>^MESSAGE^</b></p>
  <br/>
  <A HREF="/" class="btn btn-primary btn-sm"
  role="button">Back to Login</A>
</div>
</div>
<br/>
</body>
</html>

```

Enter Message template to be used when SSO login fails in HTML with ^MESSAGE^ as a place holder (Optional)

Allow Account Signups

TRUE

Allow new account creation through Login Process

Automatic Account Approval

1

Set Admin Approval for creating new accounts

- 0 - No Automatic approval, Admin has to approve account
- 1 - Automatically approve new accounts to Full User
- 2 - Automatically approve new accounts to Guest User

Enable ADFS

NO

Specify if IdP is Active Directory Federation Service (ADFS)

User Login Token Expiration Match IdP Token Expiration

If enabled, user authentication token will expire as specified by Identity Provider.

Show the Idp Login Screen

If enabled, User login will be directed to Idp login screen automatically.

Log Level

DEV

Specify the Log Level (Use Dev only for testing)

Use the following tables to understand the IdP settings.

FileCloud Parameters	IdP Settings	ADFS as IdP Data can be obtained from Federation Metadata
IdP End Point URL	Identity Provider 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) <ul style="list-style-type: none"> Usually uid or agencyUID Default value: uid <p>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.</p>	Identifies the Username (must be unique for each user) Usually SAMAccountName or User Principal Name defined in claim rules. <p>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.</p> <p>value: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn or upn</p> <pre data-bbox="743 877 1463 957" style="border: 1px solid black; padding: 5px;"> <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" /> </pre>
IdP Email Parameter	Identifies the email of the user (must be unique) Default value: mail	Identifies the email of the user (must be unique) http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or emailAddress <pre data-bbox="743 1144 1463 1241" style="border: 1px solid black; padding: 5px;"> <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" /> </pre>
IdP Given Name Parameter	Identifies the given name of the user Default value: givenName	Identifies the given name of the user. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname or givenname <pre data-bbox="743 1423 1463 1520" style="border: 1px solid black; padding: 5px;"> <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" /> </pre>
IdP Surname Parameter	Identifies the surname of the user Default value: sn	Identifies the sur name of the user http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname or surname <pre data-bbox="743 1703 1463 1778" style="border: 1px solid black; padding: 5px;"> <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" /> </pre>


FileCloud Parameters	IdP Settings	ADFS as IdP Data can be obtained from Federation Metadata
IdP Log Out URL (Optional)	URL for logging out of IdP	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.
Limit Logon to IdP Group (available in FileCloud Version 19.1 and higher)	<p>IdP Group Name</p> <ul style="list-style-type: none"> 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 <i>memberof</i> parameter The <i>memberof</i> parameter can include a comma separated value of all groups to which the user belongs 	<p>IdP Group Name</p> <ul style="list-style-type: none"> 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 <i>memberof</i> parameter The <i>memberof</i> parameter can include a comma separated value of all groups to which the user belongs
Show the IdP Logon Screen	<p>Identifies which Logon screen the user will see:</p> <ul style="list-style-type: none"> FileCloud screen = not selected IdP screen = selected 	<p>Identifies which Logon screen the user will see:</p> <ul style="list-style-type: none"> FileCloud screen = not selected IdP screen = selected
IdP Metadata	Identity Provider metadata in XML Format	Federation 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.	Custom error message that appears when a signin is invalid. Enter in HTML format.

FileCloud Parameters	IdP Settings	ADFS as IdP Data can be obtained from Federation Metadata
<p>Allow Account Signups</p> <p>Added in FileCloud 20.1</p>	<p>When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.</p>	<p>When TRUE, during the login process, if the user account does not exist, a new FileCloud user account is created automatically.</p>
<p>Automatic Account Approval</p> <p>Added in FileCloud 20.1</p>	<p>This setting works with the Allow Account Signups setting to determine:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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 	<p>This setting works with the Allow Account Signups setting to determine:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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
<p>Enable ADFS</p>	<p>No</p>	<p>Yes</p>

FileCloud Parameters	IdP Settings	ADFS as IdP Data can be obtained from Federation Metadata
User login token expiration match Idp expiration	<p>If enabled the user token expiration will be set based on Idp expiration settings</p> <p>If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days)</p> <p>Default: No (Not enabled)</p>	<p>If enabled the user token expiration will be set based on ADFS expiration settings</p> <p>If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days)</p> <p>Default: No (Not enabled)</p>
Show the Idp Login Screen	If enabled, automatically redirect user to Idp log-in screen.	If enabled, automatically redirect user to Idp log-in screen.
Log Level	<p>Set the Log mode for the SAML Calls.</p> <p>Default Value: prod (Do not use DEV for production systems)</p>	<p>Set the Log mode for the SAML Calls.</p> <p>Default Value: prod (Do not use DEV for production systems)</p>

5. Register the 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 Single Sign On 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**.

The screenshot shows the 'Login' configuration page. At the top, there are tabs for 'General', 'Labels And Logos', 'URL', 'UI Messages', 'Email Templates', 'News Feed', 'TOS', and 'Advanced'. Below these, there are sub-tabs for 'UI Features', 'Login', 'Account Menu', and 'Listing'. The 'Login' sub-tab is active, displaying the 'Customize User Login Screen' section. This section contains three settings, each with a checked checkbox and a description:

- Show New Account Button** (checked): Display "New Account" button in user login screen
- Show SSO Link** (checked): Show "Single Sign On" option in user login screen
- Show Login Options** (checked): Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

Two orange arrows point to the 'Show SSO Link' and 'Show Login Options' checkboxes, indicating they should be checked.

4. Save your changes.

Now, when users access the user portal log-in page, they will see:

FILECLOUD

Login [+ New Account](#)

Account

Password

> [Forgot Password](#)

Or use your SSO

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 in the user portal or the admin portal, please [Contact FileCloud Support](#).

Integrating with other applications

- [Integrate Auth0 SSO with Filecloud](#)
- [Integrate Azure AD with FileCloud](#)
- [Integrate Centrify with FileCloud](#)
- [Integrate CYBERARK with FileCloud](#)
- [Integrate JumpCloud with FileCloud](#)

- [Integrate Okta 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](#)

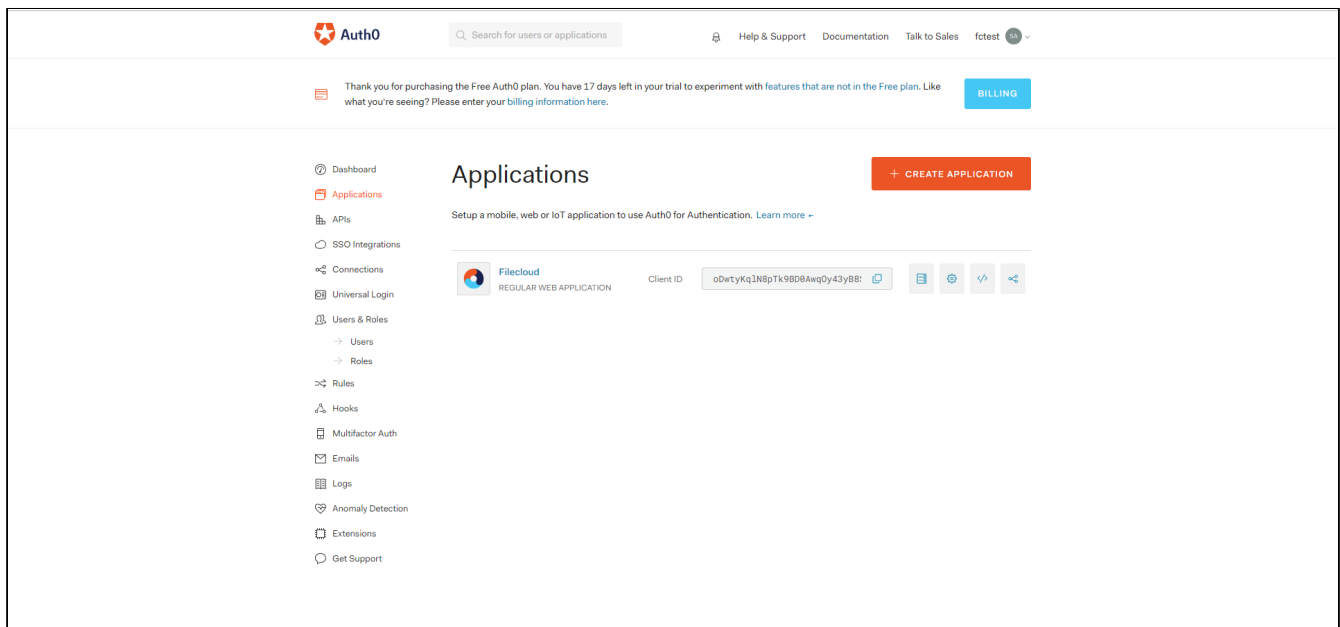
Integrate Auth0 SSO with Filecloud

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.

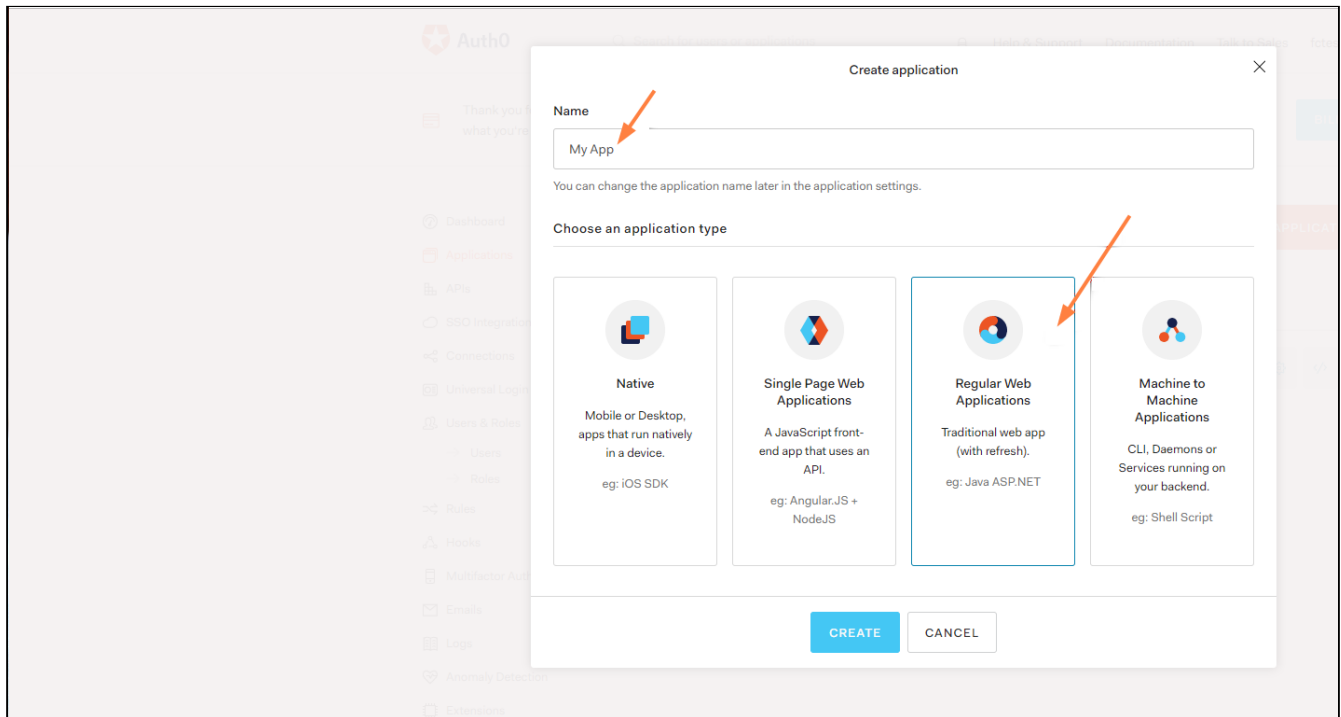
You can integrate Auth0 SSO with Filecloud using the SAML 2 protocol. Below are the steps to achieve this.

Configuration in Auth0 portal

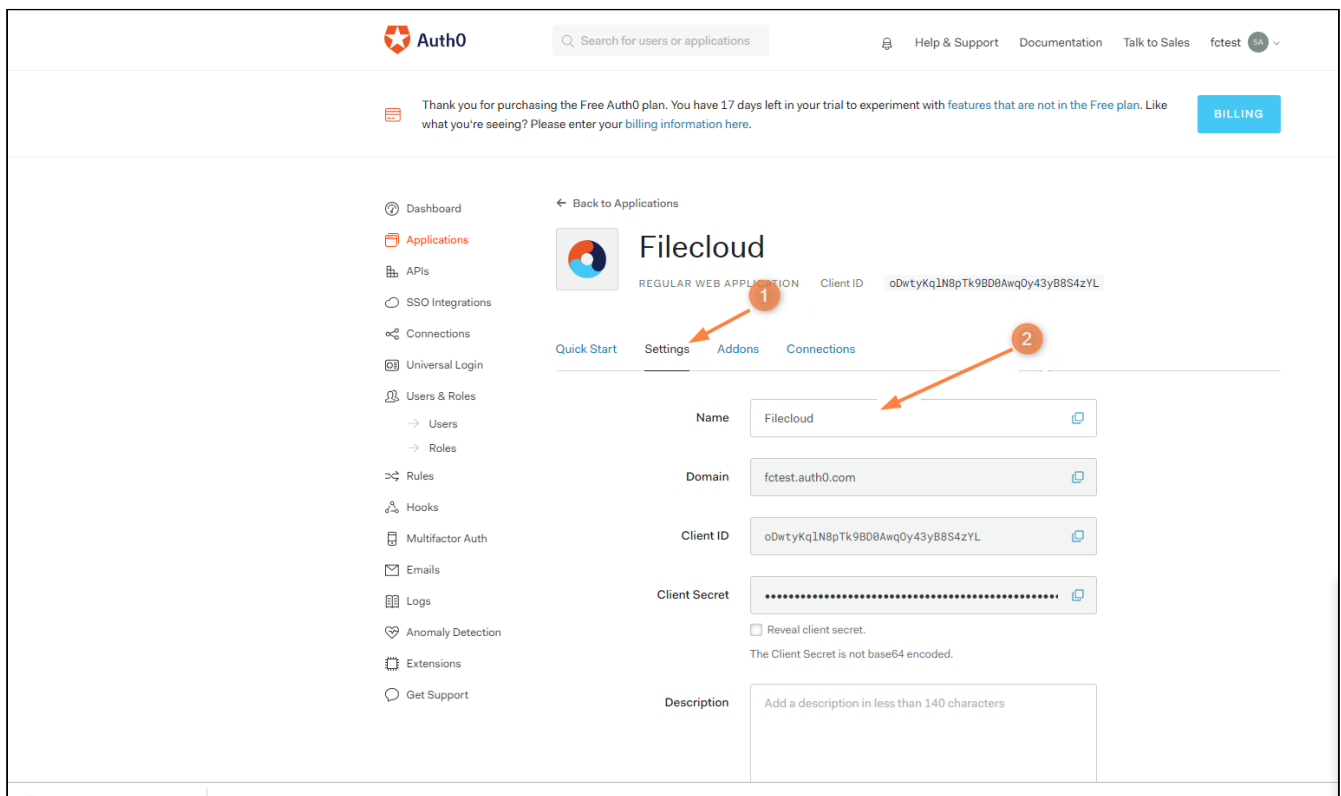
- Login to the Auth0 Dashboard and Click on the tab " Application " on the Left panel.
- Create application



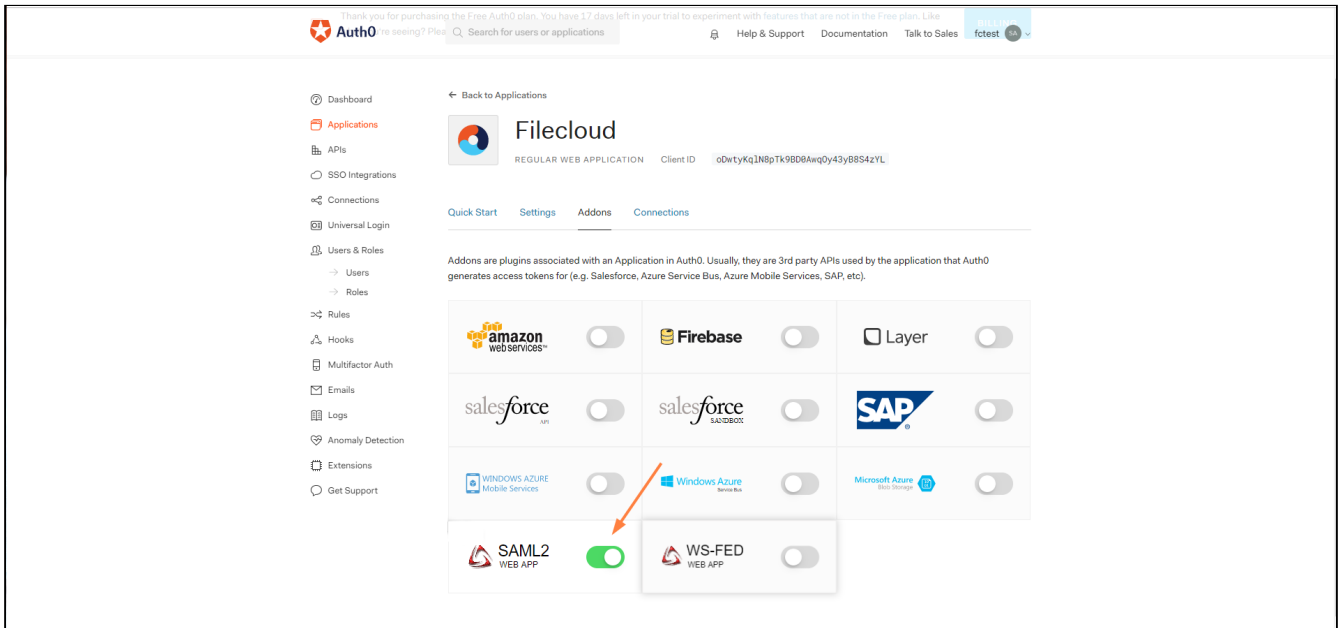
- Give the Application name as you wish and select Regular Web applications.



- Click on the created application again and go to the settings tab and confirm the application name in the " Name " field and Go to Addons



- Click on SAML2 (Web App)



- Enter the URL in the Field "Application Callback URL".
https://your_filecloud_url/simplesaml/module.php/saml/sp/saml2-accs.php/default-sp

Addon: SAML2 Web App

Settings Usage

Application Callback URL

type/paste your FileCloud url here

https://[redacted]/simplesaml/module.php/saml/sp/saml2-accs.php/default-sp

SAML Token will be POSTed to this URL.

Settings

```
27 //  
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",  
28 //  
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name",  
29 // ],  
30 // "authnContextClassRef":  
    "urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified",  
31 // "logout": {  
32 //   "callback": "http://foo/logout",  
33 //   "slo_enabled": true
```

DEBUG

SAML Protocol Settings

- **audience (string)**: The audience of the SAML Assertion. Default will be the Issuer on SAMLRequest .
- **recipient (string)**: The recipient of the SAML Assertion (SubjectConfirmationData). Default is AssertionConsumerUrl on SAMLRequest or Callback URL if no SAMLRequest was sent.

- Scroll down and click on "Enable"

- Go to "Usage" on the same page.

Addon: SAML2 Web App ✕

[Settings](#) [Usage](#)

SAML Protocol Configuration Parameters

- SAML Version: 2.0
- Issuer:

urn:fctest.auth0.com

IDP endpoint URL
- Identity Provider Certificate: [Download Auth0 certificate](#)
- Identity Provider SHA1 fingerprint:

F2:62:74:37:F9:48:63:01:A6:09:76:03:2E:9D:8B:F5:C0:84:45:23
- Identity Provider Login URL:

<https://fctest.auth0.com/samlp/oDwtyKqIN8pTk9BD0AwqOy43yB8S4zYL>
- Identity Provider Metadata: [Download](#) Download this metadata

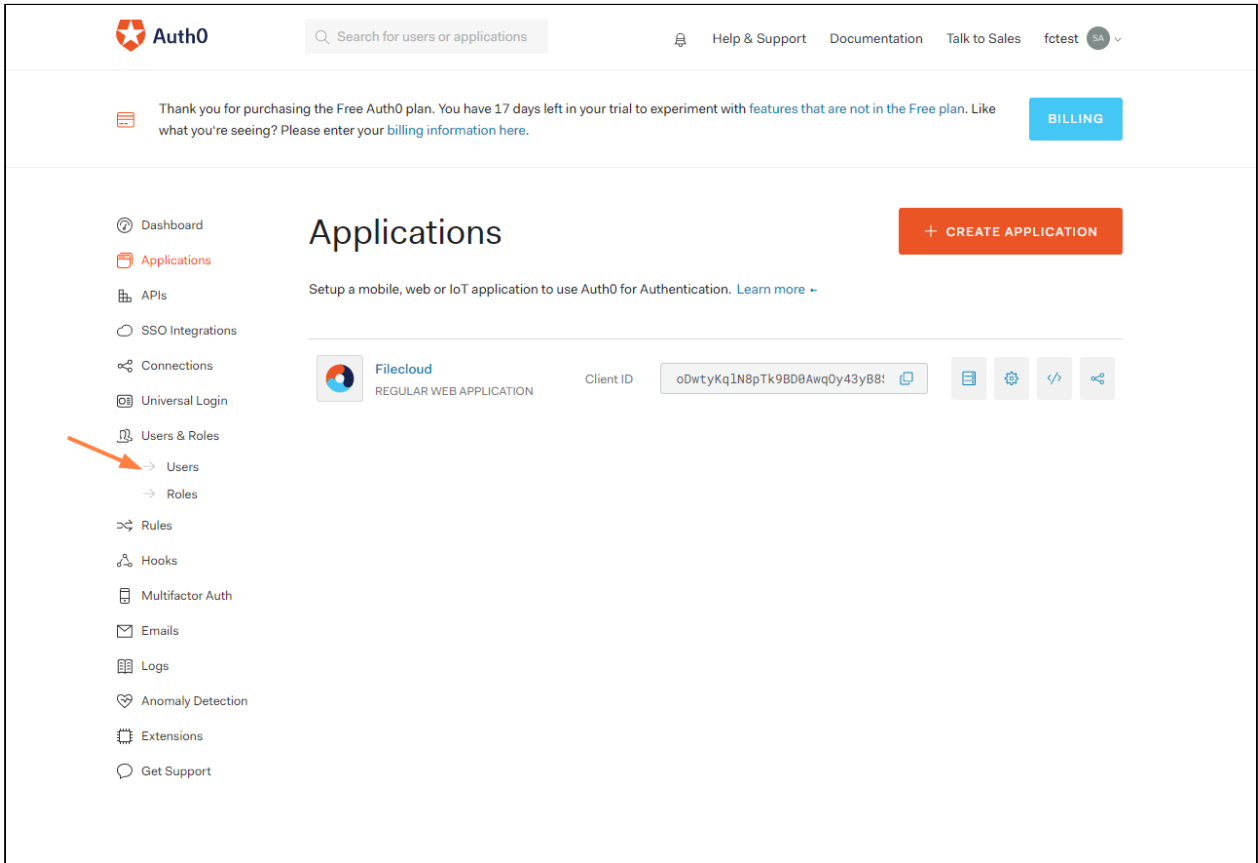
Alternatively, you can add a connection parameter:

```
https://fctest.auth0.com/samlp/oDwtyKqIN8pTk9BD0AwqOy43yB8S4zYL?connection=User
name-Password-Authentication
https://fctest.auth0.com/samlp/oDwtyKqIN8pTk9BD0AwqOy43yB8S4zYL?connection=goog
le-oauth2
```

In this case, Auth0 will redirect users to the specified `connection` and will not display the Login Widget. Make sure you send the SAMLRequest using `HTTP POST`.

- Note down the value in the field **Issuer**.
- Scroll down and download the metadata from **Identity Provider Metadata**:

- Go to Users in the Auth0 Dashboard and create user.



Configuration in Filecloud Admin portal

- Go to Admin portal → Settings → SSO
- Enter the below details in the required fields

IdP End Point URL: Paste here the value we note down from **Issuer**: (10th step in Auth0 configuration part)

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.

FILECLOUD admin

Manage Settings Reset All

Server Storage Authentication Admin Database Email Endpoint Backup License Policies **SSO** Content Search Web Edit Team Folders Third Party Integrations Misc

Single Sign On (SSO) Settings Reset to defaults

Default SSO Type: SAML
Specify the Single Sign On Type

SAML Settings

IdP End Point URL: urnfctest.auth0.com
URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Username Parameter Name in Identity Provider

IdP Email Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Email Parameter Name in Identity Provider

IdP Given Name Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Given Name Parameter Name in Identity Provider

IdP Surname Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Surname Parameter Name in Identity Provider

Limit Login to IdP Group:
Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute.

FILECLOUD admin

Given Name Parameter Name in Identity Provider

IdP Surname Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Surname Parameter Name in Identity Provider

Limit Login to IdP Group:
Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute. Reset to defaults

Show the IdP Login Screen:
If enabled, User login will be directed to IdP login screen automatically.

IdP Metadata:

```
<EntityDescriptor entityID="urnfctest.auth0.com"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" >
<IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
<KeyDescriptor use="signing" >
<KeyInfo
xmlns="http://www.w3.org/2000/09/xmldsig#" >
<X509Data >
```

Enter Identity Provider metadata in XML format.

Enable ADFS: NO
Specify if IdP is Active Directory Federation Service (ADFS)

User Login Token Expiration Match IdP Token Expiration:
If enabled, user authentication token will expire as specified by Identity Provider.

Log Level: DEV
Specify the Log Level (Use Dev only for testing)

- Click save
- Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.

FILECLOUD

NOTIFICATIONS

DEVICES

Devices

GOVERNANCE

Dashboard

Retention

Smart DLP

Smart Classification

MISC.

Audit

Alerts

User Locks

Workflows

Reports

Federated Search

Metadata

SETTINGS

Settings

CUSTOMIZATION

Customization

General Labels And Logos URL UI Messages Email Templates News Feed TOS Advanced

UI Features **Login** Account Menu Listing

Customize User Login Screen

Show New Account Button Display "New Account" button in user login screen

Show SSO Link Show "Single Sign On" option in user login screen

Show Login Options Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

Login Panel Transparency YES NO Add transparency to login panel. Enable it if a custom login background image is set

Login UI Additional Links
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/tos)

- In the Filecloud User login page Click on more option and access the SSO. This will first redirect you to Auth0 login page and you can authenticate as the user that you have created in the Auth0.

If that user doesn't exist in the Filecloud, it will be created automatically after the successful authentication.

The screenshot shows the FileCloud login interface. At the top center is the FileCloud logo. Below it, the page is divided into two main sections: 'Login' and 'New Account'. The 'Login' section contains two input fields: 'Account' (with the email 'jm2344311@gmail.com') and 'Password' (with masked characters). Below the 'Account' field is a link for '> Forgot Password'. To the right of the 'Account' and 'Password' fields is a blue 'Login' button. Below the login form, there is a section for SSO with the text 'Or use your SSO' and a 'Log In with SSO' button. At the bottom of the page, there is a language selector set to 'English' and links for 'Privacy Policy', 'Terms of use', and 'Powered by FileCloud'.

Integrate Azure AD with FileCloud

Before completing the following procedures, configure Apache Web Server. See [SSO Configuration Step 1](#) on the page [SAML Single Sign-On Support](#) for configuration instructions.

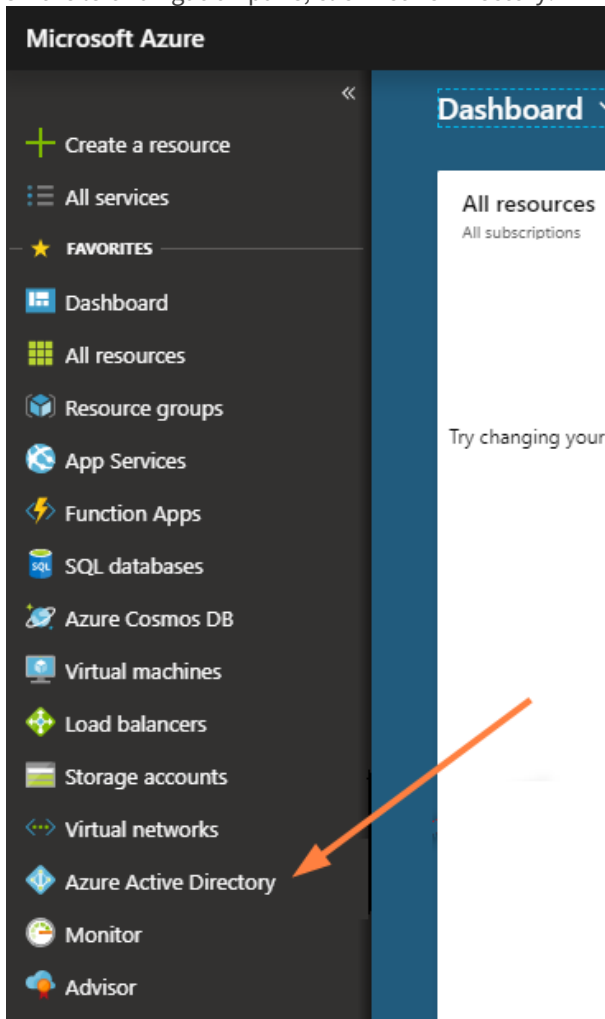
Note: Azure AD can only be integrated if FileCloud has an [SSL certificate](#) in place, as Microsoft requires HTTPS URLs when configuring FileCloud in Azure.

FileCloud can be integrated with Azure AD.

- The Azure AD must be configured as an Identity Provider (IdP)
- FileCloud will act as the Service Provider (SP)

To integrate Azure AD with FileCloud:

1. Login to Azure AD Portal (<https://portal.azure.com>).
2. On the left navigation pane, click Active Directory.



3. From the Directory list, select the directory for which you want to enable directory integration.

4. Select **Enterprise applications** on the left navigation menu.

Home > Default Directory - Overview

Default Directory - Overview

Azure Active Directory

Search (Ctrl+/)

Switch directory Delete directory

sanuvarkeygmail.onmicrosoft.com

Default Directory

Azure AD Free

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2. [Start a free trial](#)

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

36 entries since May 15, 2018. [View archive](#)

All services (36) [Changed feature](#)

5. Click **New application**.

Microsoft Azure

Home > Default Directory > Enterprise applications - All applications

Enterprise applications - All applications

Default Directory - Azure Active Directory

+ New application Columns

Overview

Manage

- All applications
- Application proxy

Application Type

Enterprise Applications

First 20 shown, to search all of your app

NAME

6. In the **Add an application** page, click **Application you're developing**.

Add an application

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Add from the gallery

filecloud ✓

1 applications matched "filecloud".

NAME	CATEGORY
FileCloud	Business management

FileCloud
Add app

Codelathe

access and enable single sign-on with FileCloud. Requires FileCloud subscription.

Use Microsoft Azure AD to enable user access to FileCloud.

Requires an existing FileCloud subscription.

Name

FileCloud

Publisher

Codelathe

Single Sign-On Mode

SAML-based sign-on

URL

https://www.getfilecloud.com

Logo

[Read our step-by-step FileCloud integration tutorial](#)

Add

7. Enter **FileCloud**, select the listing for **FileCloud**, and click **Add** in the right panel.

8. In the next screen, click **Single sign-on** in the left navigation panel.

Home > Default Directory > Enterprise applications - All applications > Categories > Add an application > FileCloud - Single sign-on

FileCloud - Single sign-on

Enterprise Application

« Save Discard

2. FileCloud Domain and URLs
Values for the fields below are provided by FileCloud. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by FileCloud. [Upload metadata file.](#)

* Sign on URL ⓘ
Patterns: <https://EXAMPLE.filecloudhosted.com>, <https://EXAMPLE.filecloudonline.com>

* Identifier (Entity ID) ⓘ
Patterns: https://*.filecloudhosted.com/simplesaml/module.php/saml/sp/metadata.php/default-sp, https://*.filecloudonline.com/simplesaml/module.php/saml/sp/metadata.php/default-sp

Show advanced URL settings

Reply URL (Assertion Consumer Service URL) ⓘ
Patterns: https://*.filecloudhosted.com/*, https://*.filecloudonline.com/*

Relay State ⓘ

Test SAML Settings
Please Save the values to test the settings.

3. User Attributes [Learn more](#)
Edit the user information sent in the SAML token when user signs in to FileCloud.

User Identifier ⓘ user.userprincipalname

View and edit all other user attributes

4. SAML Signing Certificate [Learn more](#)
Manage the certificate used by Azure AD to sign SAML tokens issued to FileCloud.

App Federation Metadata Url <https://login.microsoftonline.com/b096b215-a01c-4d3e-9f87-b258...>

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
New	9/12/2021	0F9151E392EB843818FCA6C692916A7E26F58730	Metadata XML

9. Enter the **Sign on URL**, **Identifier (Entity ID)**, and **Reply URL**.
Sign on URL is your FileCloud site URL, for example, <https://yourdomain.com>
Identifier (Entity ID) is the FileCloud SSO endpoint, for example, <https://yourdomain.com/simplesaml/module.php/saml/sp/metadata.php/default-sp>
10. Check **Show advanced URL settings**.
11. In **Reply URL**, and replace yourfileclouddomain.com with your FileCloud domain in the format: <https://yourfileclouddomain.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp>
12. Click **Save** in the top left of the screen.
13. From the bottom of the screen, click [Metadata XML](#) .
The metadata file is downloaded.

14. Click **Users and groups** in the left navigation panel, add the users, and make sure permissions are assigned.

15. Log in to your FileCloud Admin UI, and go to **Settings > SSO**, and enter the following details:

Settings	Value
Default SSO Type	SAML
Idp End Point URL	From the Metadata XML downloaded, copy the entity ID on the first line of the XML document.
Idp Username Parameter	Based on the IDP configurations these values may vary. Use the appropriate one of the following: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Idp Email Parameter	Based on the IDP configurations these values may vary. Use the appropriate one of the following: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
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	Copy the complete contents of the Metadata XML downloaded.

To get our **Idp End Point URL**, open your downloaded xml data and copy the **Entity ID** as shown in the screen shot below.

```
<?xml version="1.0" encoding="UTF-8"?>
- <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://sts.windows.net/b096b215-a01c-4d3e-9f87-b2583e46d112/" ID="_80cd5b8e-32c2-49d9-8dda-8692491c137d">
- <RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706" xmlns:fed="http://open.org/wsfed/federation/200706" xsi:type="fed:SecurityTokenServiceType">
- <KeyDescriptor use="signing">
- <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
```

16. Save the above settings.
This completes the Azure AD SSO integration with FileCloud.

Troubleshooting failed SSO login for a member of an AD limit group

For SAML SSO with an AD limit group, FileCloud checks the login user's FileCloud **Group name** to see if they are a member of the limit group. Azure AD can only send the **Group ID**, not the group name, to FileCloud, so login fails for a member of the limit group. To fix this, add a custom claim parameter named **memberof** in Azure AD that sends the group's **Object ID (Group ID)** in FileCloud SSO settings to limit the login to this specific group.


To get the group's **Object ID**, in Azure AD:

1. Log in the the Azure Portal Dashboard, and click **Azure Active Directory**.
2. Click **Groups**, and then click the **Group** to limit the login to.
3. Open the **Overview** screen for the group and copy the **Object ID** field:

The screenshot shows the Azure Portal interface for a group named 'FCAZAD'. The 'Overview' tab is selected, and the 'Object Id' field is highlighted with an orange arrow. The 'Object Id' field contains the value '85827b08-011f-4005-8f87-5332d5fd8a2b'. Other fields visible include 'Membership type' (Assigned), 'Source' (Cloud), and 'Type' (Security).

In FileCloud, go to **SAML Settings**, and in **Limit Login to Idp Group**, enter the **Object Id**.

SAML Settings

Idp Endpoint URL or EntityID*		URL or EntityID of the Identity Provider that the Service Provider must contact.
IdP Username Parameter*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Username Parameter Name in Identity Provider
IdP Email Parameter*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Email Parameter Name in Identity Provider
IdP Given Name Parameter*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Given Name Parameter Name in Identity Provider
IdP Surname Parameter*	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname Parameter Name in Identity Provider
IdP Log Out URL (Optional)		URL to call to logout of Identity Provider (Optional)
Limit Login to Idp Group (Optional)	85827b08-011f-4005-8f87-5332d5fd8a2b 	Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute

- 4.
5. Then, in Azure AD, go to the Enterprise Applications screen, and choose the FileCloud application
6. In the navigation panel, click **Single sign-on**.

7. Scroll down to Attributes and Claims, and click **Edit**.

Home > Default Directory | Enterprise applications > Enterprise applications | All applications > FileCloud >

FileCloud | SAML-based Sign-on

Enterprise Application

Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Relay State (Optional) *Optional*
Logout Url (Optional) *Optional*

Attributes & Claims Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

8. Click **Add a group claim**.
A **Group Claims** form opens in the right panel.
9. In **Source attribute**, choose **Group ID**.
10. Check **Customize the name of the group claim**.
11. In **Name**, enter **memberof**, and in **Value**, enter **user.groups** (which is equal to **Object Id**).

Home > Default Directory > Enterprise applications > FileCloud FCEXT > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim | Columns | Get feedback?

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format=emailAddress] ...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ...
memberof	user.groups ...

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

This page includes previews available for your evaluation in the 'Advanced options' section.

Source attribute *

Group ID

Advanced options

Filter groups (Preview)

Attribute to match

Match with

String

Customize the name of the group claim

Name (required)

memberof

Namespace (optional)

Emit groups as role claims

Apply regex replace to groups claim content (Preview)

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). The following steps must be followed to configure FileCloud with Centrify.

PLEASE NOTE: Any reference to [samldev.codelathe.com](#) in this article should be replaced with your own FileCloud URL.

Login to your Centrify issued URL.

After successful login to Centrify, go to the admin section and to the dashboard.

Create a new application as shown below

Navigation: Dashboards | Users | **Apps** | Devices | Policies | Roles | Reports | Requests | Settings

Getting Started ▾ ⚙️

Getting Started with the Centrify Identity Service

Overview

- [Creating Roles](#)
- [Adding Saas applications](#)
- [Adding users](#)
- [Assigning users to roles](#)
- [Enrolling mobile devices](#)
- [Managing mobile devices](#)

Run the Quick Start Wizard for initial configuration of the Centrify Identity Service.

[Start Wizard](#)

Overview

Identity Service is a cloud-based service that decreases the cost of managing SaaS applications and mobile devices while at the same time improving user application adoption, satisfaction and productivity. From a single administrator console, you assign the SaaS applications (and set policies for use) to the users in your organization and get a list of the devices enrolled by your users. In turn, those users can use single sign-on to open the applications from both a convenient web portal and their mobile devices.

You can also use Identity Service for mobile device management. From the same administrator console you can create group policies just for mobile devices, send commands—for example, to lock a lost device or wipe a stolen device—to the devices, and generate activity reports that help you monitor and manage even the most diverse assortment of devices.

Identity Service includes a cloud-based identity service and a policy service that automates mobile device security policy enforcement. You can create user accounts in the cloud service or use your existing Active Directory accounts. The Policy Service lets you use the cloud service or Active Directory to define your mobile device group policy sets and deploys them automatically to the mobile devices.

See the [Identity Service overview](#) for a more information.

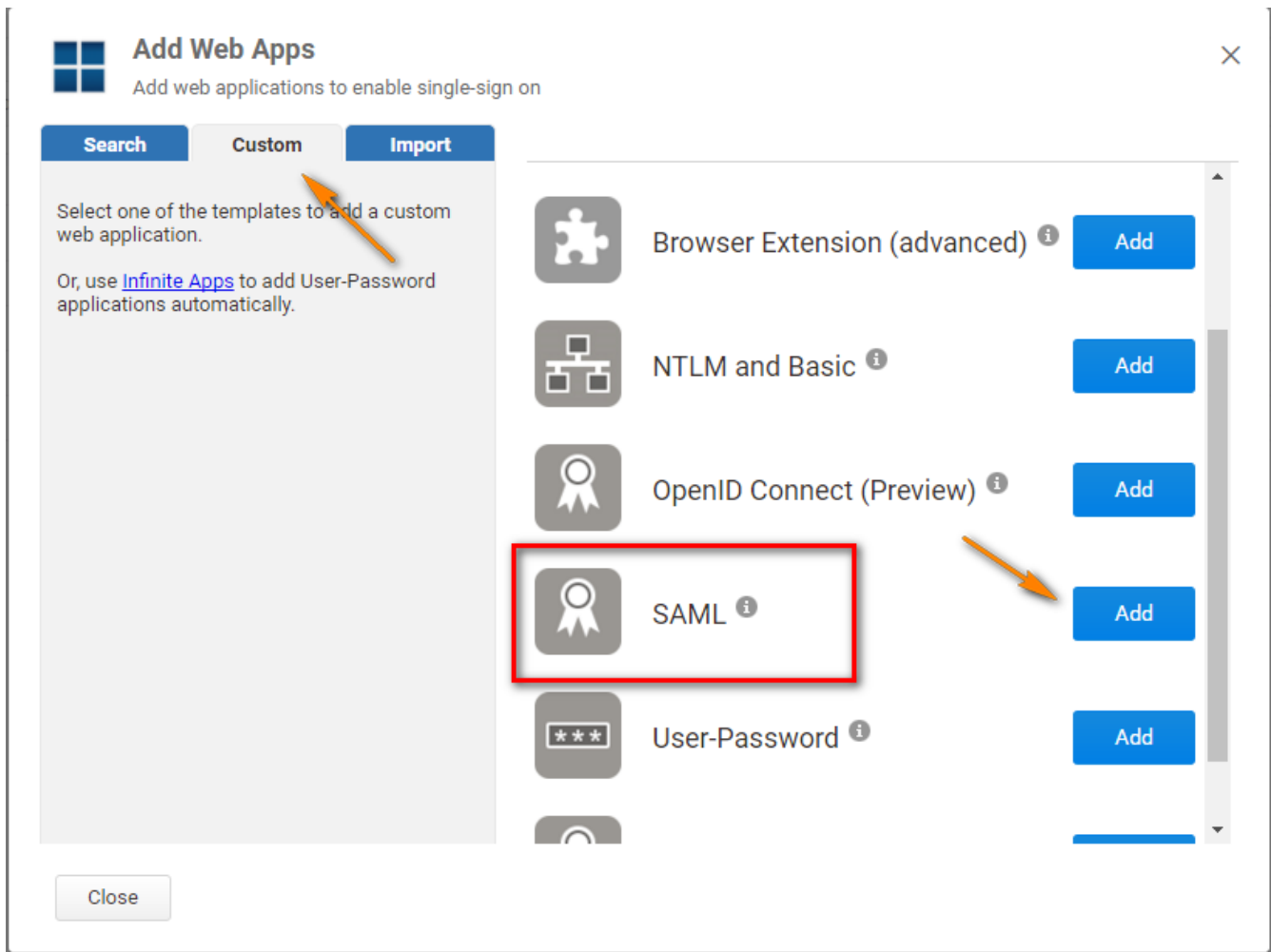
From the Apps menu, Click Add Web Apps.

Navigation: Dashboards | Users | **Apps** | Devices | Policies | Roles | Reports | Requests | Settings

Add Web Apps | Add Mobile Apps | Search: All Applications ▾ Search Apps 🔍

	Name	Type	Description	Provisioning	App Gateway	Status
<input type="checkbox"/>	Amazon.com	Web - User Password	Amazon i...			Deployed
<input type="checkbox"/>	Google Mail	Web - User Password	10+ GB of...			Deployed
<input type="checkbox"/>	SAML	Web - SAML	This temp...			Deployed
<input type="checkbox"/>	User Portal	Web - Portal	The User ...			Deployed

From the Add Web Apps, Click Custom Tab and Choose SAML and Click Add.



In the SAML Web App Screen, go to **Application Settings** Link the assertion consumer service URL is the FileCloud assertion URL <http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp>

Download the Idp Metadata as shown below on the screenshot and gGet the details to configure FileCloud from this screen under FileCloud Admin - Settings - SSO tab.

- a. The Identity Provider Single Sign On URL must match the Issuer URL in the screenshot below.
- b. The meta data downloaded from this screen must match the IdP meta data in FileCloud Admin Settings - SSO - Idp Metadata.

SAML
Web - SAML Deployed
Actions ▾

Application Settings
Description
User Access
Policy
Account Mapping
Advanced
App Gateway
Changelog
Workflow

Application Settings [Learn more](#)

Service Provider Info [Upload SP Metadata](#)

Assertion Consumer Service URL ⓘ

Issuer ⓘ

Encrypt Assertion ⓘ

Encryption Certificate:

Filename [Browse](#) [Clear](#)

Identity Provider Info

Identity Provider Sign-in URL ⓘ


Identity Provider Error URL ⓘ

Identity Provider Sign-out URL ⓘ

[Download Identity Provider SAML Meta data](#) ⓘ

In the **Description** link, add the application Name and Application Description as needed.

← Apps



SAML

Web - SAML Deployed

[Actions](#) ▾

- Application Settings
- Description
- User Access
- Policy
- Account Mapping
- Advanced
- App Gateway
- Changelog
- Workflow

Description [Learn more](#)


Application Name *

Application Description

This template enables you to provide single sign-on to a web application that uses SAML (Security Assertion Markup Language) for authentication.

Category * ⓘ

Logo (60 x 60 pixels recommended)



In the **Account Mapping** link, select Use Account Mapping Script as shown below. This will enable to use your email and get the username.

The screenshot shows the SAML application settings page. The left sidebar contains a navigation menu with the following items: Application Settings, Description, User Access, Policy, Account Mapping (highlighted), Advanced, App Gateway, Changelog, and Workflow. The main content area is titled "Account Mapping" and includes a "Learn more" link. Under the heading "Map to User Accounts", there are three radio button options: "Use the following Directory Service field to supply the user name", "Everybody shares a single user name", and "Use Account Mapping Script" (which is selected). Below these options is a "Test" button. A code editor displays the following script:

```
1 UserIdentifier = LoginUser.Username;  
2 LoginUser.Username = LoginUser.Get('mail').split("@")[0];
```

In the **Advanced** Link, add the script as follows:

SAML
Web - SAML Deployed
Actions ▾

Application Settings
Description
User Access
Policy
Account Mapping
Advanced
App Gateway
Changelog
Workflow

Advanced [Learn more](#)

Reset Script Test

Script to generate a SAML assertion for this application

```

1 setIssuer(Issuer);
2 setSubjectName(UserIdentifier);
3 setServiceUrl(ServiceUrl);
4 setAttribute("mail", LoginUser.Get("mail"));
5 setAttribute("uid", LoginUser.Username);
6 setAudience('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/metadata.php/default-sp');
7 setRecipient('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp');
8 setHttpDestination('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp');
9 setSignatureType('Response');
```

The Configuration is now complete. You can switch to the user portal and the FileCloud app that was added as shown in the screenshots below.

Centrify

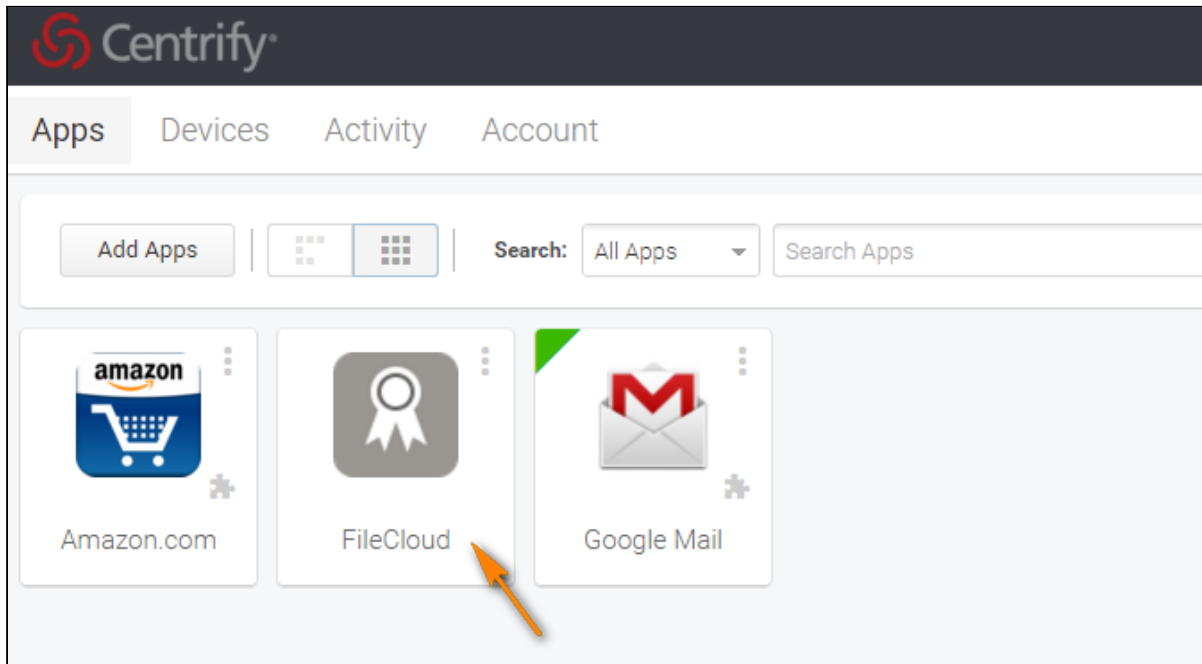
Dashboards Users **Apps** Devices Policies Roles Reports Requests Settings

Add Web Apps Add Mobile Apps Search: All Applications Search Apps

Support
Downloads
Reload
About
Switch to User Portal

	Name	Type	Description	Provisioning	App Gateway	Status
<input type="checkbox"/>	Amazon.com	Web - User Password	Amazon is a...			Deployed
<input type="checkbox"/>	Google Mail	Web - User Password	10+ GB of s...			Deployed

From the app gallery, select FileCloud.




Also, from the FileCloud login screen, you can select the Single Sign On to login 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 same CYBERARK credentials.

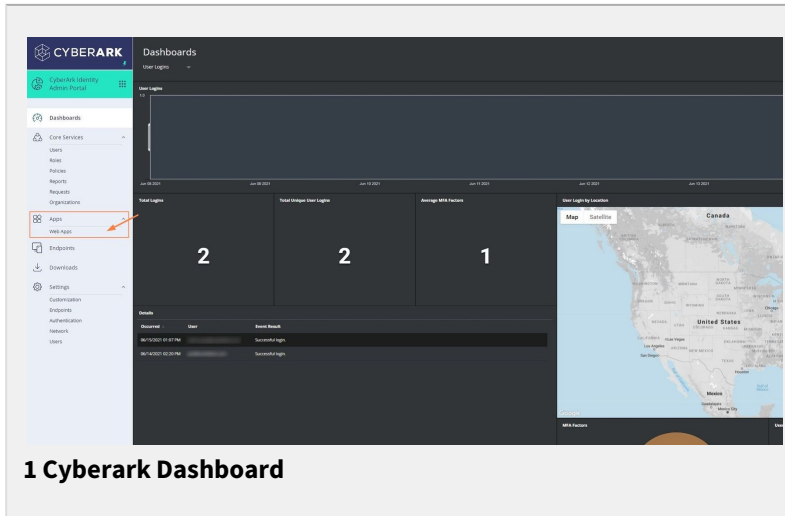
	<p>CYBERARK is a cloud-based platform</p> <ul style="list-style-type: none"> • Manage privileged accounts and credentials • Secure workforce and customer identities • Secure and manage access for applications and other non-human identities
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

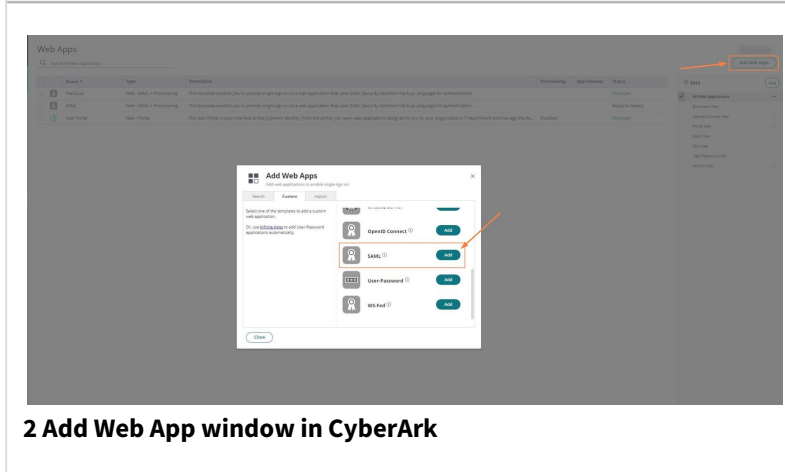
1. In CYBERARK, create a new Web App



1 Cyberark Dashboard

1a. Open a browser and log in to your CYBERARK admin portal

1b. From the left navigation pane, click Web Apps.

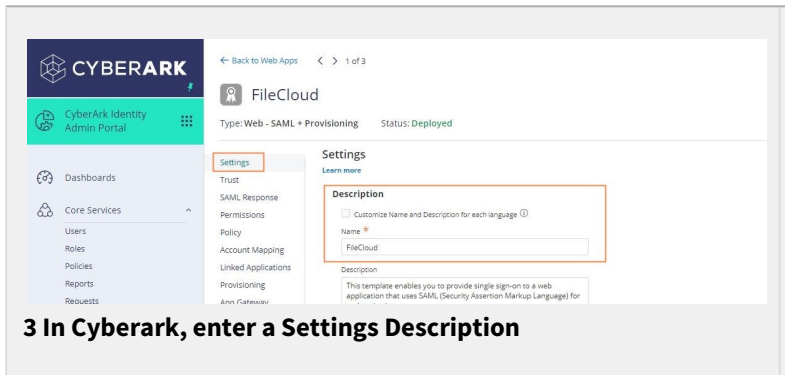


2 Add Web App window in CyberArk

1c. On the Web Applications panel, on the top right corner click, "Add Web App".

1d. Once the Add Web App popup panel appears, select the custom tab and scroll down until you find SAML and click Add, A confirmation panel might appear. Click Yes, and then close to access the added SAML Web App.

2. In CYBERARK configure the added SAML Web App



3 In Cyberark, enter a Settings Description

2a. Click Settings in the navigation panel. In Description, enter a meaningful name such as FileCloud SSO, and click Save at the bottom-center of the screen.

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata
 Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save your work w

SP Entity ID / Issuer / Audience ⓘ
https://.../simplesaml/module.php/saml/sp/met

Assertion Consumer Service (ACS) URL ⓘ
https://.../simplesaml/module.php/saml/sp/sam

Recipient * ⓘ Same as ACS URL
Enter Recipient here

Sign Response or Assertion?
 Response Assertion Both

NameID Format ⓘ
unspecified

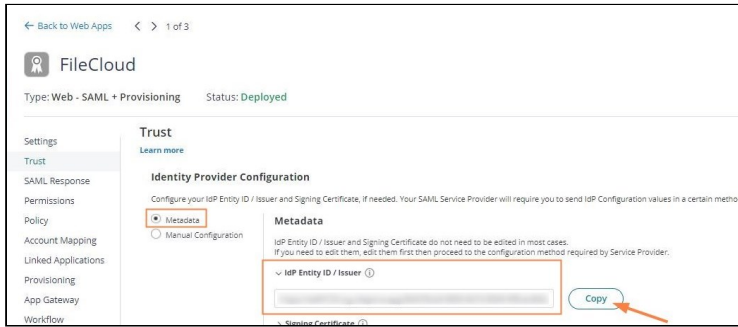
Single Logout URL ⓘ
https://.../simplesaml/module.php/saml/sp/sam

Encrypt SAML Response Assertion ⓘ
Subject Name: CN=..., O=..., L=..., S=...,
C=...
Thumbprint: ...

Encryption Certificate (Required)

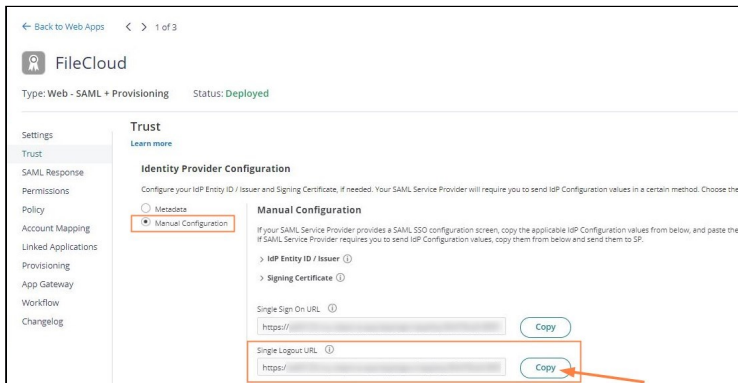
2b. Click Trust in the navigation panel, and download the metadata file.

4 In Trust in Cyberark, download metadata

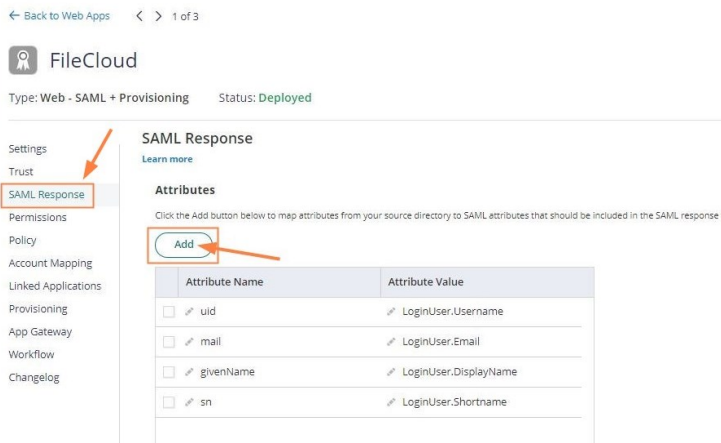


5 Web App Trust screen in Cyberark. Choose metadata and copy IDP Entity ID

2C. Within the Identity Provider Configuration, expand "IdP Entity ID / Issuer," and copy the URL into a notepad. Select Manual Configuration, and copy the Single Logout URL into a notepad as it will be used in the next steps.



6 In Web App Trust screen in Cyberark click Manual Configuration and copy Single Logout URL



7 In Web App SAML Response screen in Cyberark click Add

2D. 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

Click Save.

3. Export Metadata file into FileCloud and Configure SSO

FileCloud Single Sign-On requirements configuration.

3a. Configure Apache Webserver

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

Single Sign On (SSO) Settings

Default SSO Type: Specify the Single Sign On Type

SAML Settings

3 Idp Endpoint URL or EntityID* URL or EntityID of the Identity Provider that the Service Provider must contact.

4 IdP Username Parameter* Username Parameter Name in Identity Provider

IdP Email Parameter* Email Parameter Name in Identity Provider

IdP Given Name Parameter* Given Name Parameter Name in Identity Provider

IdP Surname Parameter* Surname Parameter Name in Identity Provider

2 IdP Log Out URL (Optional) URL to call to logout of Identity Provider (Optional)

Limit Login to Idp Group (Optional) Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute

1 IdP Metadata*

3b. Once you have completed the Apache configuration, access the FileCloud Admin Web portal > Settings> SSO and complete the following:

1. Open the metadata file downloaded in step 2b, and copy its content into IdP Metadata.
2. Paste the Single Logout URL copied in step 2c into IdP Log Out URL (Optional)
3. Paste the IdP Entity ID/Issuer URL copied in step 2c into Idp Endpoint URL or EntityID
4. Configure the following attributes:
 - IdP Username Parameter = uid
 - IdP Email Parameter = mail
 - IdP Given Name Parameter = givenName
 - IdP Surname Parameter = sn
5. Click Save.

General Labels And Logos URL UI Messages Email Templates News Feed TOS Advanced

UI Features **Login** Account Menu Listing

Customize User Login Screen

Show New Account Button Display "New Account" button in user login screen

Show SSO Link Show "Single Sign On" option in user login screen

Show Login Options Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

8 FileCloud Admin Portal Customization Login screen

3c. Enable SSO Login. Go to FileCloud Admin portal > Customization > General > Login. Enable Show SSO Link and "Show Login Options."

4. CYBERARK - Service Provider Configuration

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata
 Manual Configuration

Metadata

Use one of the following methods to import SP Metadata given by your Service Provider.

URL:

File:

XML:

4a. Click the Trust tab in the navigation panel for the Web App, and scroll down to Service Provider Configuration. 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,

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

Metadata
 Manual Configuration

Manual Configuration

Fill out the form below with information given by your Service Provider. Be sure to save your work w

SP Entity ID / Issuer / Audience

Assertion Consumer Service (ACS) URL

Recipient * Same as ACS URL

Sign Response or Assertion?
 Response Assertion Both

NameID Format

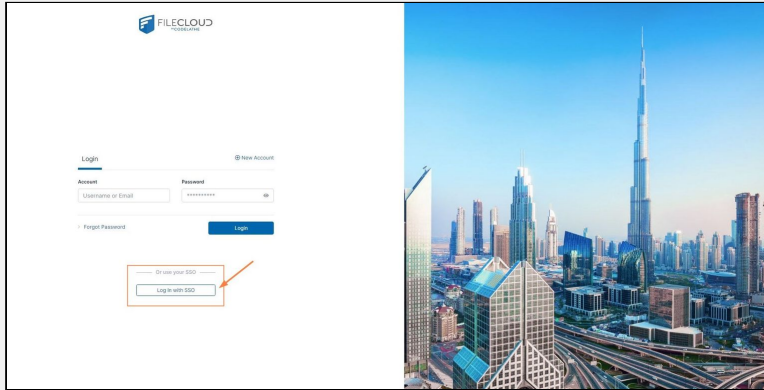
Single Logout URL

Encrypt SAML Response Assertion
Thumbprint:

Encryption Certificate (Required)

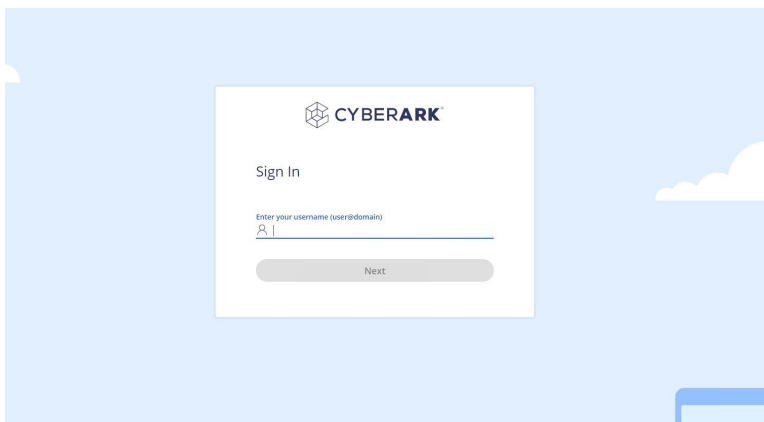
4b. Once you have loaded FileCloud's Metadata, change the settings from Metadata to Manual Configuration and disable Encrypt SAML Response Assertion, Click Save.

5. CYBERARK SSO integration Completed



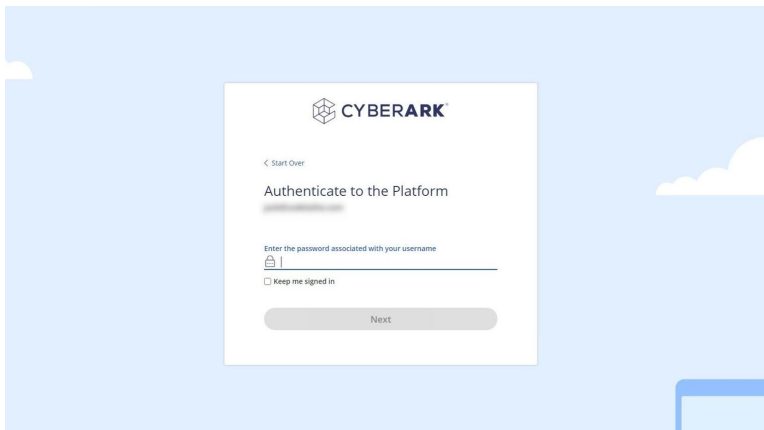
9 FileCloud User Portal, Login screen

5a. Access FileCloud's user portal and click Login In with SSO



10 Cyberark Login page, username

5b. You are redirected to your CYBERARK login page, After you complete your user authentication you are redirected to FileCloud.



11 Cyberark Login page, password

5a. Access FileCloud's user portal and click Login In with SSO

9 FileCloud User Portal, Login screen

12 FileCloud User Portal, home page

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's is a cloud-based platform

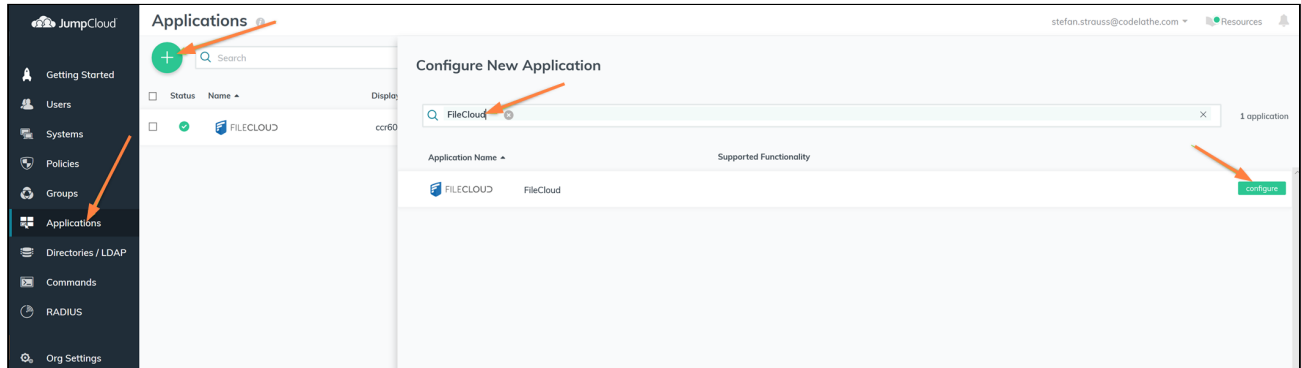
- It enables IT teams to securely manage user identities
- It connects teams them to resources they need regardless of provider, protocol, vendor, or location

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.



1a. Open a browser and log in to your JumpCloud admin URL by typing it in or clicking on this URL <https://console.jumpcloud.com/login>

1b. From the left navigation pane, click APPLICATIONS.

1c. On the Applications screen, to add a new application, click the plus sign.

1d. On the Configure New Application enter 'FileCloud' in the search field and press configure.

2. In JumpCloud, configure FileCloud Application

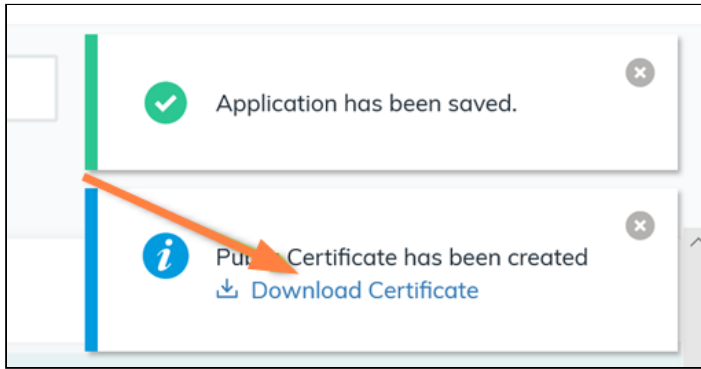
<p>Details</p> <p>Display Label:</p> <input type="text" value="FileCloud Server Top Sales"/>	<p>2a. In <i>Display Label</i>, enter a meaningful name.</p>
<p>IdP Entity ID</p> <p>FileCloud</p> <p>i Also referred to as the 'Issuer', this is the unique, case-sensitive identifier used by JumpCloud for this service provider. This value should match the value specified in FileCloud's SSO configuration</p>	<p>2b. In <i>IdP Entity ID</i>, enter an unique, case-sensitive identifier used by JumpCloud for this FileCloud service provider.</p>

<p>SP Entity ID: <input type="text" value="http://YOUR_DOMAIN/implesaml/module.php/saml/sp/metadata.php/default-sp"/></p> <p>ACS URL: <input type="text" value="http://YOUR_DOMAIN/implesaml/module.php/saml/sp/saml2-acis.php/default-sp"/></p> <p>Default RelayState: <input type="text" value="http://YOUR_DOMAIN/auth/samlssso.php"/></p>	<p>2c. Replace YOUR_DOMAIN with your domain name in all fields.</p>
<p>IdP URL: <input type="text" value="https://sso.jumpcloud.com/saml2/filecloud_TopSales24"/></p>	<p>2d. 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.</p>

3. In JumpCloud, activate the new application and export Metadata and certificate

3a. In JumpCloud, on the configuration screen, save and activate the new application

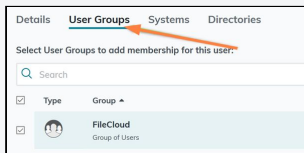
3b. Download the generated certificate.



3c. 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

	<p>4a. In JumpCloud, on the Groups screen, click the green button with the white plus sign to add a new group.</p>
	<p>4b. In JumpCloud, enter the group name.</p>
	<p>4c. In JumpCloud, enable the group to access FileCloud.</p>
	<p>4d. In JumpCloud, on the Users screen, click the green button with the white plus sign to add a new user.</p> <p>4e. In JumpCloud, on the New User screen, select the Details tab and type in the user's information.</p>



4f. In JumpCloud, on the New User screen, select the User Groups tab and add the user to your FileCloud Group.

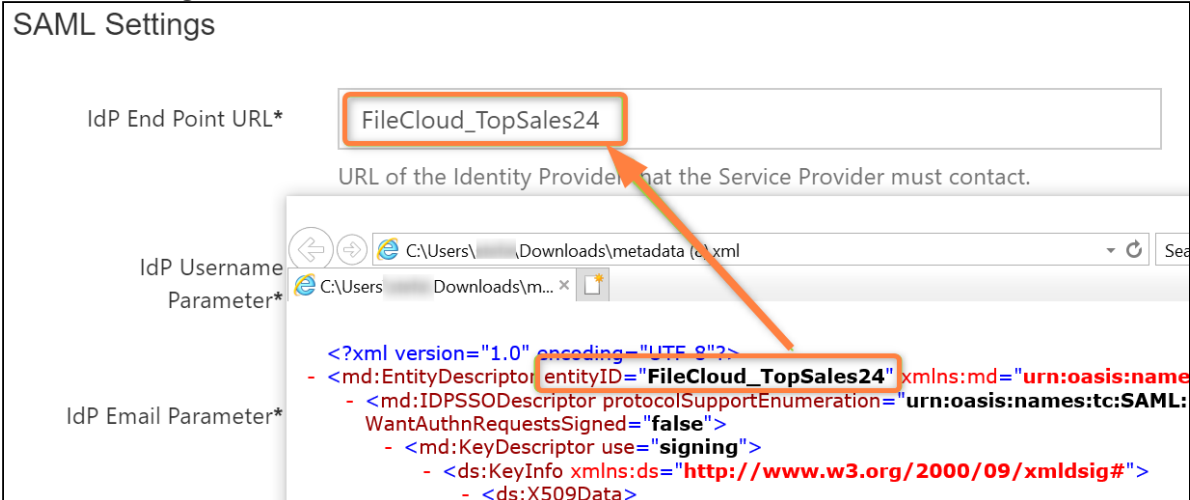
4g. In JumpCloud, on the New User screen, click the Save User button.

5. In FileCloud, configure the SSO settings.

To configure the FileCloud SSO settings:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *SETTINGS*, select *Settings*.
3. Select the *SSO* sub-tab.
4. In *IdP End Point URL*, type or paste in the SAME value as the *IdP Entity ID* entered in step 2b.

The correct string can also be seen in the metadata xml file:



SAML Settings

IdP End Point URL*

URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter*

IdP Email Parameter*

```
<?xml version="1.0" encoding="UTF-8"?>
- <md:EntityDescriptor entityID="FileCloud_TopSales24" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  - <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
    WantAuthnRequestsSigned="false">
    - <md:KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
```

5. 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:

Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider.

USER ATTRIBUTE MAPPING: ⓘ

Service Provider Attribute Name	JumpCloud Attribute Name
givenName	firstname
sn	lastname
email	email
uid	username

Enter them into the corresponding settings in FileCloud on the **Settings > SSO** tab:

FILECLOUD

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

Content Search Web Edit Team Folders Third Party Integrations Misc Reset

Single Sign On (SSO)

Default SSO Type

 Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*

IdP Username Parameter*

IdP Email Parameter*

IdP Given Name Parameter*

IdP Surname Parameter*

- Click *Save* and minimize the browser.

6. Copy JumpCloud metadata to FileCloud SSO Settings.

Use the metadata exported in Step 5 to configure the FileCloud SSO **Idp Meta Data** parameter.

To configure the FileCloud Idp Meta Data parameter:

- Open a browser and log in to the *Admin Portal*.
- From the left navigation pane, under *SETTINGS*, select *Settings*.
- Select the *SSO* sub-tab.
- Scroll down to the *Idp Meta Data* field.
- On the server, open the XML file that contains the metadata you exported from JumpCloud in step 3c.
- Copy the metadata in the file and paste it into FileCloud on the *SSO* tab in the *IdP Metadata* field.

The screenshot shows the FileCloud Admin Portal interface. The left sidebar contains navigation options like 'Admins', 'Team Folders', 'Network Folders', 'User Shares', 'Folder Permissions', 'DEVICES', 'GOVERNANCE', 'MISC.', 'SETTINGS', 'CUSTOMIZATION', and 'SYSTEM'. The main content area is titled 'Manage Settings' and has tabs for 'Server', 'Storage', 'Authentication', 'Admin', 'Database', 'Email', 'Endpoint Backup', 'License', 'Policies', 'SSO', 'Content Search', 'Web Edit', and 'Team'. The 'SSO' tab is active, showing 'Single Sign On (SSO) Settings'. The 'Default SSO Type' is set to 'SAML'. The 'SAML Settings' section includes a 'Show the Idp Login Screen' checkbox (unchecked) and an 'IdP Metadata' text area containing XML code. Below the text area is an 'Enable ADFS' dropdown set to 'NO' and a 'User Login Token Expiration Match IdP Token Expiration' checkbox (unchecked). A 'Save' button is visible on the right side of the page.

- Click *Save*.

Now you can start using the Single Sign-On with JumpCloud from FileCloud!

Integrate Okta with FileCloud

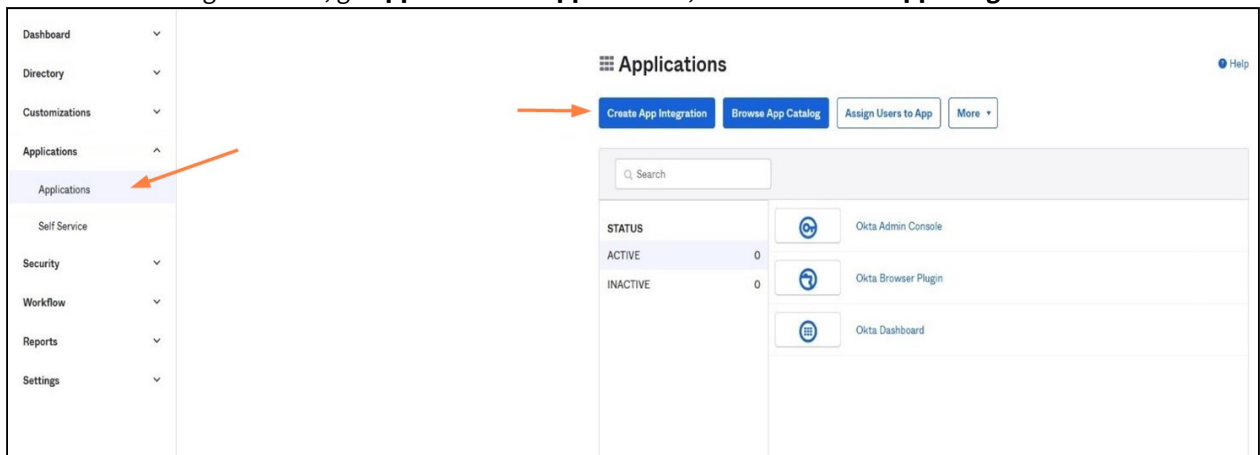
To integrate with the Okta browser plugin, please see [Integrate with Okta using browser plugin](#).

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**.

Create a new app integration

Sign-in method
[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel **Next**

4. In the **General Settings** tab of the **Create SAML Integration** screen, enter a name for **App name**, and click **Next**.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: Myldp





App logo (optional)

App visibility: Do not display application icon to users

Cancel **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/samlssso.php**

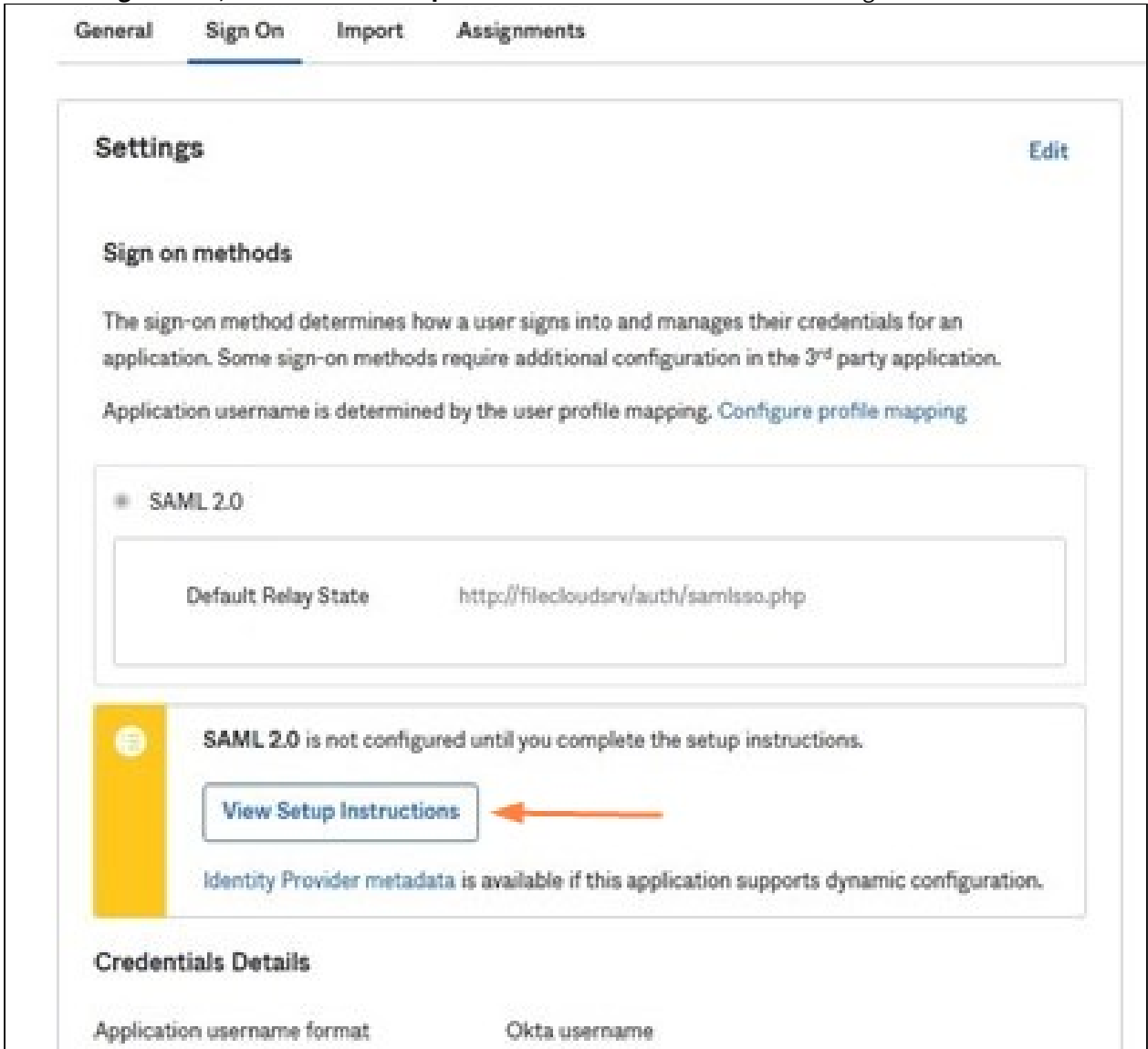
- Under **Attribute Statements**, the attribute names must match the names set in the FileCloud admin portal in **Settings > SSO** for **Idp Username Parameter**, **Idp Email Parameter**, **Idp Given Name Parameter**, and **IDP Surname Parameter**. Set the **Values** for the **Attribute Statements** to the values shown in the screenshot.

Okta	FileCloud																					
<div style="border: 1px solid #ccc; padding: 10px;"> <p>A SAML Settings</p> <p>General</p> <p>Single sign on URL  <input type="text" value="http://[redacted]/simplesaml/module.php/saml/sp/saml"/></p> <p><input checked="" type="checkbox"/> Use this for Recipient URL and Destination URL <input type="checkbox"/> Allow this app to request other SSO URLs</p> <p>Audience URI (SP Entity ID)  <input type="text" value="http://[redacted]/simplesaml/module.php/saml/sp/metadata"/></p> <p>Default RelayState  <input type="text" value="http://[redacted]/auth/samlso.php"/> <small>If no value is set, a blank RelayState is sent.</small></p> <p>Name ID format <input type="text" value="Unspecified"/></p> <p>Application username <input type="text" value="Okta username"/></p> <p>Update application username on <input type="text" value="Create and update"/></p> <p style="text-align: right;">Show Advanced Settings</p> <hr/> <p>Attribute Statements (optional) LEARN MORE</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Name format (optional)</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="givenName"/></td> <td><input type="text" value="Unspecified"/></td> <td><input type="text" value="user.firstName"/></td> </tr> <tr> <td><input type="text" value="sn"/></td> <td><input type="text" value="Unspecified"/></td> <td><input type="text" value="user.lastName"/></td> </tr> <tr> <td><input type="text" value="email"/></td> <td><input type="text" value="Unspecified"/></td> <td><input type="text" value="user.email"/></td> </tr> <tr> <td><input type="text" value="uid"/></td> <td><input type="text" value="Unspecified"/></td> <td><input type="text" value="substringBefore(user.email,'@')"/></td> </tr> </tbody> </table> <p><input type="button" value="Add Another"/></p> <hr/> <p>Group Attribute Statements (optional)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Name format (optional)</th> <th>Filter</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text" value="Unspecified"/></td> <td><input type="text" value="Starts with"/></td> </tr> </tbody> </table> <p><input type="button" value="Add Another"/></p> </div>	Name	Name format (optional)	Value	<input type="text" value="givenName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>	<input type="text" value="sn"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>	<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>	<input type="text" value="uid"/>	<input type="text" value="Unspecified"/>	<input type="text" value="substringBefore(user.email,'@')"/>	Name	Name format (optional)	Filter	<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>	<div style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: right;">Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO C...</p> <p>Single Sign On (SSO) Settings </p> <p>Default SSO Type <input type="text" value="SAML"/> Specify the Single Sign On Type</p> <p>SAML Settings</p> <p>Idp Endpoint URL or EntityID* <input type="text" value="http://www.okta.com/ex..."/> URL or EntityID of the Identity Provider that the Service Provider must contact.</p> <p>Idp Username Parameter* <input type="text" value="uid"/> Username Parameter Name in Identity Provider</p> <p>Idp Email Parameter* <input type="text" value="email"/> Email Parameter Name in Identity Provider</p> <p>Idp Given Name Parameter* <input type="text" value="givenName"/> Given Name Parameter Name in Identity Provider</p> <p>Idp Surname Parameter* <input type="text" value="sn"/> Surname Parameter Name in Identity Provider</p> <p style="text-align: center; color: orange;">Enter these values into Attribute Statements</p> </div>
Name	Name format (optional)	Value																				
<input type="text" value="givenName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>																				
<input type="text" value="sn"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>																				
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>																				
<input type="text" value="uid"/>	<input type="text" value="Unspecified"/>	<input type="text" value="substringBefore(user.email,'@')"/>																				
Name	Name format (optional)	Filter																				
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>																				

- Click the **Feedback** tab of the **Create SAML Integration** screen, then select **I'm an Okta customer adding an internal app**, and click **Finish**.

The screenshot shows the 'Create SAML Integration' screen with three tabs: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The 'Feedback' tab is active. The main content area is titled '3 Help Okta Support understand how you configured this application'. It contains a question 'Are you a customer or partner?' with two radio button options: 'I'm an Okta customer adding an internal app' (selected) and 'I'm a software vendor. I'd like to integrate my app with Okta'. Below this is a blue box with a white circle icon and the text 'The optional questions below assist Okta Support in understanding your app integration.' Underneath, there is an 'App type' section with a dropdown arrow and a checked checkbox for 'This is an internal app that we have created'. At the bottom left is a 'Previous' button and at the bottom right is a 'Finish' button. An orange arrow points from the 'Finish' button back to the 'Feedback' tab in the top navigation bar. To the right of the main form, there is a section titled 'Why are you asking me this?' with the text: 'This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.'

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.
- Using the **IDP Metadata** text under **Optional**:
 - Copy the **entityID** field from the text box into **Idp Endpoint URL or EntityID** in FileCloud admin UI interface under **Settings > SSO**.
 - 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**.
 - 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.

10. In the **Assign** drop-down list, choose **Assign to People**.

The screenshot shows the Okta MyIdp interface. At the top, there's a navigation bar with 'General', 'Sign On', 'Import', and 'Assignments' (highlighted). Below this, there's a section for 'Assignments' with a search bar and a 'People' dropdown. The 'Assign' dropdown menu is open, showing 'Assign to People' and 'Assign to Groups'. An orange arrow points to 'Assign to People'. The main content area shows a table with binary code and 'No users found'. The footer includes copyright information for Okta, Inc. and version details.

A list of users who have both Okta and FileCloud accounts opens.

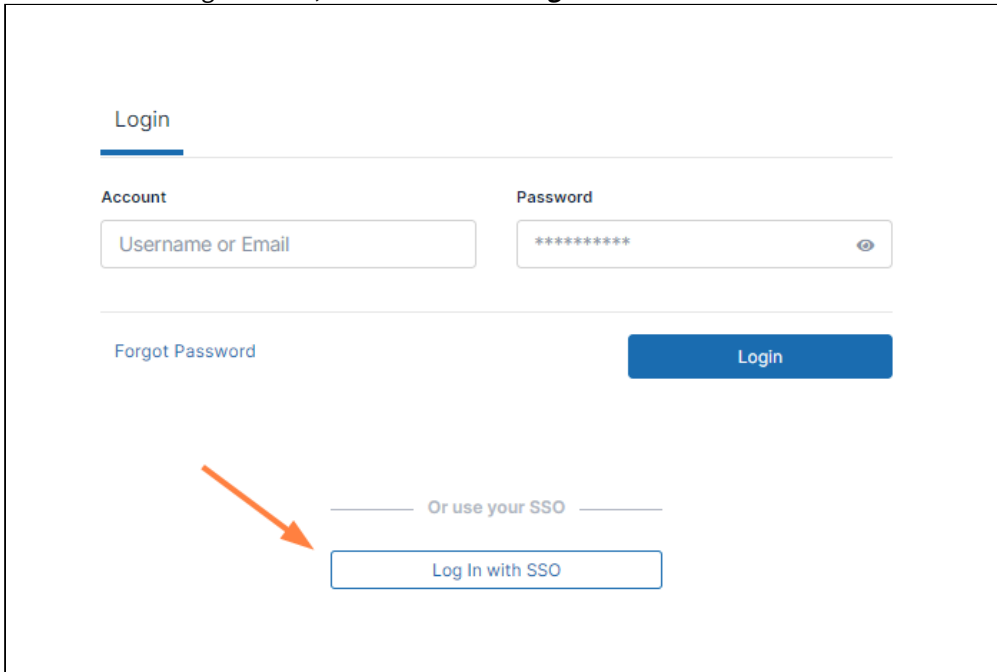
11. Select users from the list to allow them to sign in to FileCloud using Okta.

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**.




The screenshot displays the FileCloud login interface. At the top, the word "Login" is underlined. Below it, there are two input fields: "Account" with the placeholder "Username or Email" and "Password" with a masked password "*****" and a visibility toggle icon. A "Forgot Password" link is positioned to the left of a blue "Login" button. Below these elements, the text "Or use your SSO" is centered, with a blue "Log In with SSO" button underneath. An orange arrow points to this button.

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.

Connecting to 


Sign-in with your  account to access

MyIdp

okta

Sign In

Username

nathan. 

Keep me signed in

Next

Help

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:

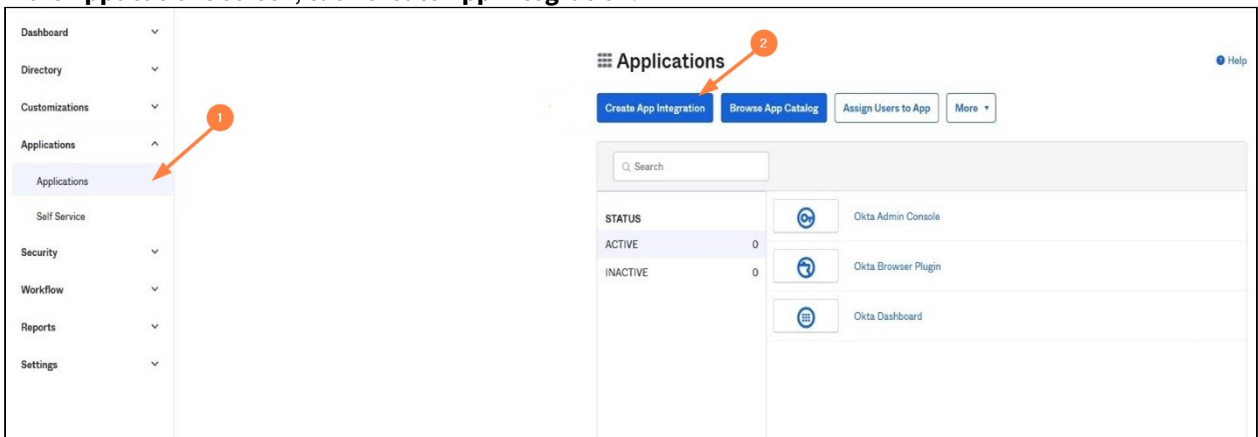
Note: You must have an Okta account before completing these steps.

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.

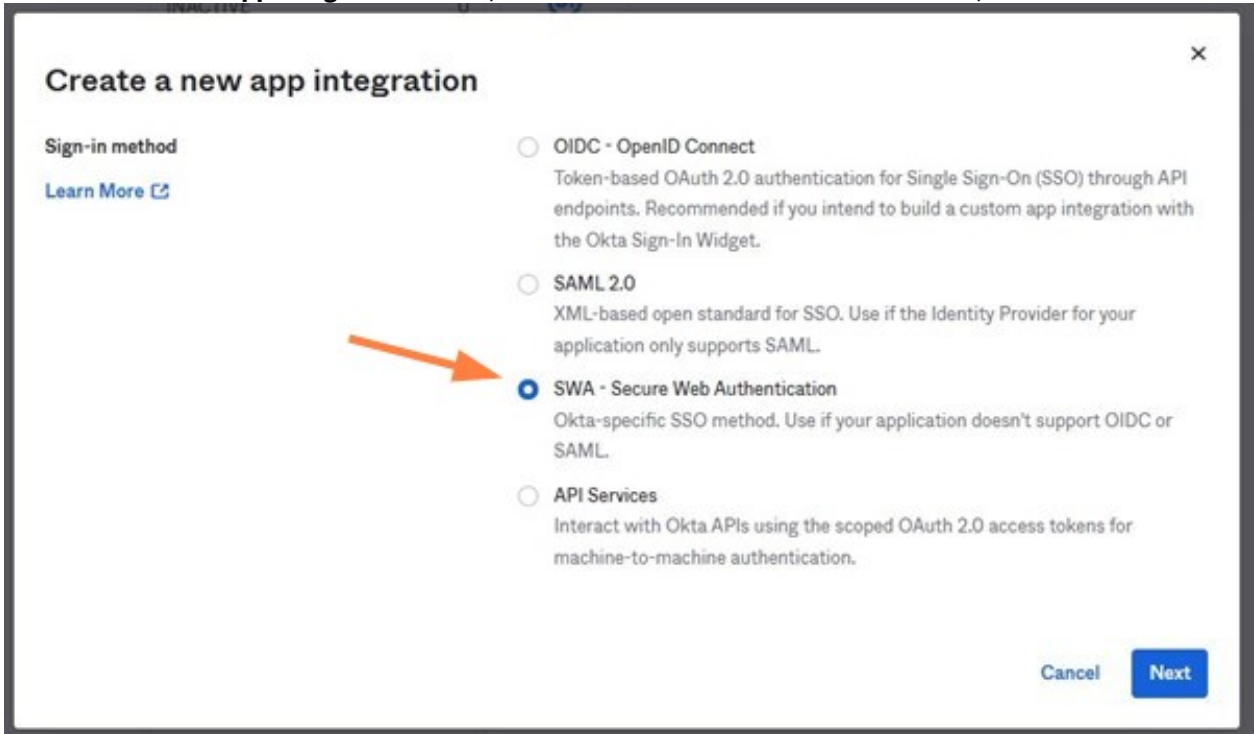
 The plugin supports different browsers. Setup and tests for this guide use Google Chrome.

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**.



Create a new app integration ✕

Sign-in method
[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel 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.


Create SWA Integration

1 General App Settings

Create

App name: FileCloud

App's login page URL: <http://127.0.0.1/ui/core/index.html>

App logo (optional): 

App visibility: Do not display application icon to users

App type: This is an internal application that we created

2 How will your users sign in?

Create

Who sets the credentials?: User sets username and pas...

Application username: (None)

Update application username on: Create and update

Cancel Finish

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.

- In the **Assign** drop-down list, choose **Assign to People**.

The screenshot shows the FileCloud interface. At the top, there's a navigation bar with 'General', 'Sign On', 'Import', and 'Assignments' (highlighted with an orange arrow). Below this, there's a section with 'Assign' and 'Convert assignments' buttons. The 'Assign' dropdown menu is open, showing 'Assign to People' (highlighted with an orange arrow) and 'Assign to Groups'. The main content area is a table with a 'Type' column containing binary code (011011100, 110111101, 110110011, 01100110, 10010101, 110011001, 11) and a 'No users found' message. The right sidebar contains 'REPORTS' (Current Assignments, Recent Unassignments) and 'SELF SERVICE' (You need to enable self service for org managed apps before you can use self service for this app. Go to self service settings, Requests: Disabled, Approval: -, Edit button).

A list of users who have both Okta and FileCloud accounts opens.

- To allow users to sign in to FileCloud using Okta, click **Assign** in the row with their email.

The screenshot shows a dialog box titled 'Assign FileCloud to People'. It has a search bar at the top. Below the search bar, there's a list of users. The first user is 'Nathan' with email 'nathan.@[redacted].com'. An 'Assign' button is visible next to the user's name.

4. Enter a **User Name** and **Password** for the user, then click **Save and Go Back**.

Assign FileCloud to People [X]

Credential Security User sets username and password
Visit the app's [sign-on options](#) to modify

User Name

Password

Save and Go Back Cancel

5. Click **Done**.

Assign FileCloud to People [X]

Q Search...

Nathan [redacted]
nathan.[redacted]@[redacted].com Assigned

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.


Connecting to 

Sign-in with your filecloud-trial-4839737 account to access
Okta Dashboard

okta

Sign In

Username

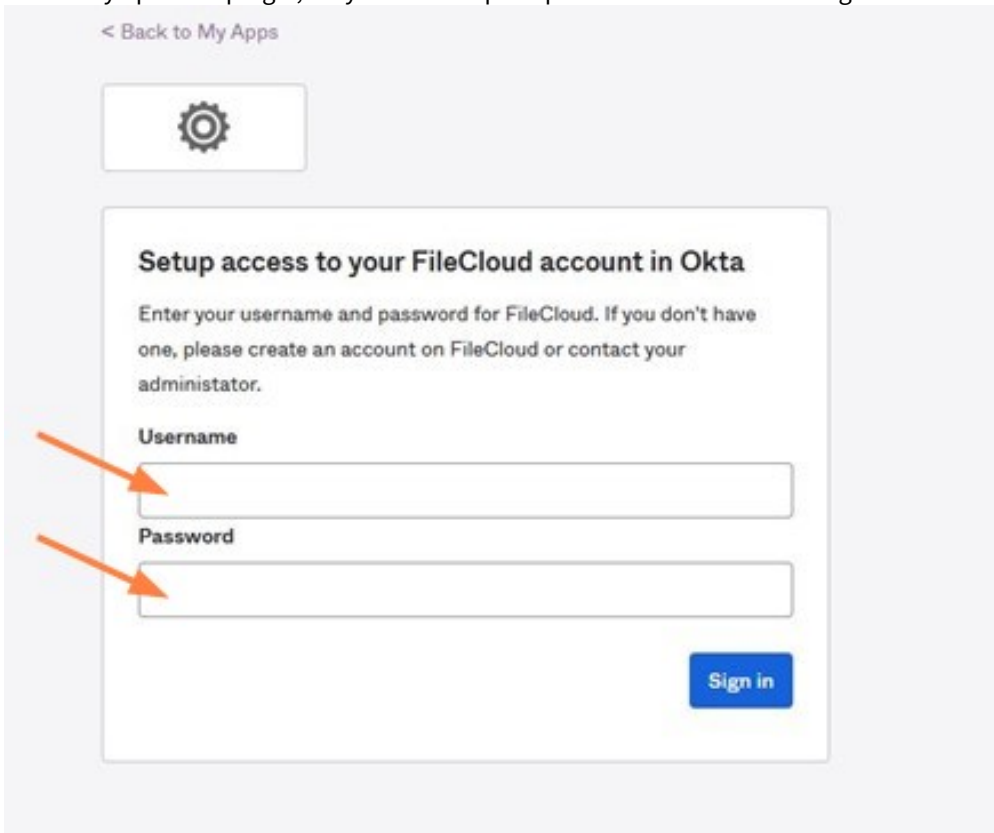
 This field cannot be left blank

Keep me signed in


Next

Help

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.



< Back to My Apps



Setup access to your FileCloud account in Okta

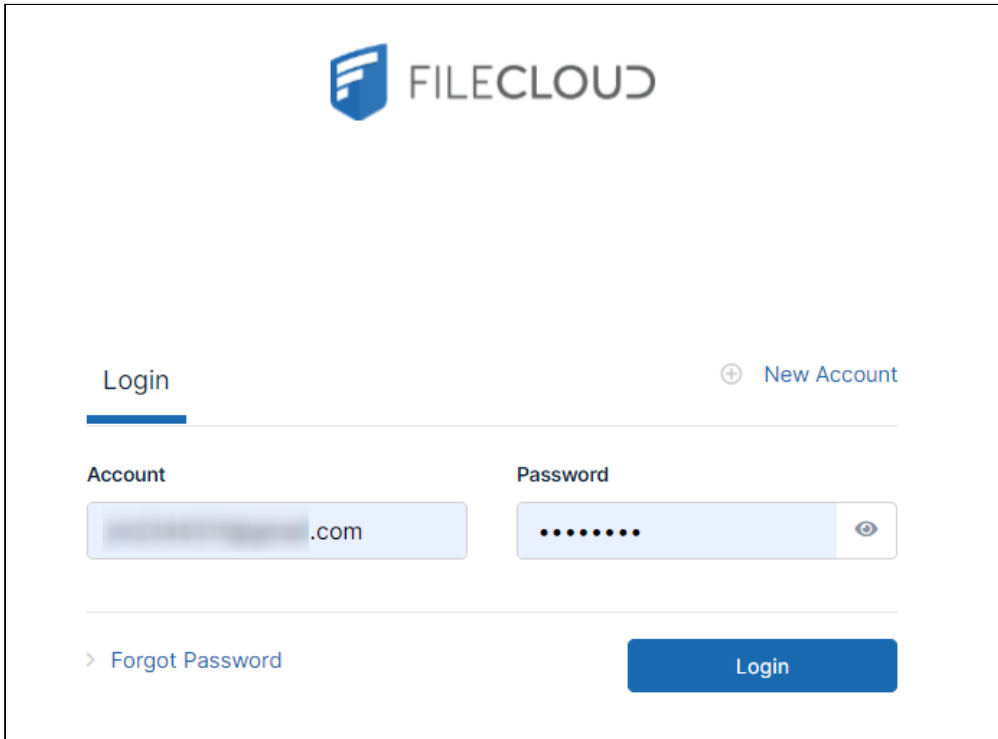
Enter your username and password for FileCloud. If you don't have one, please create an account on FileCloud or contact your administrator.

Username

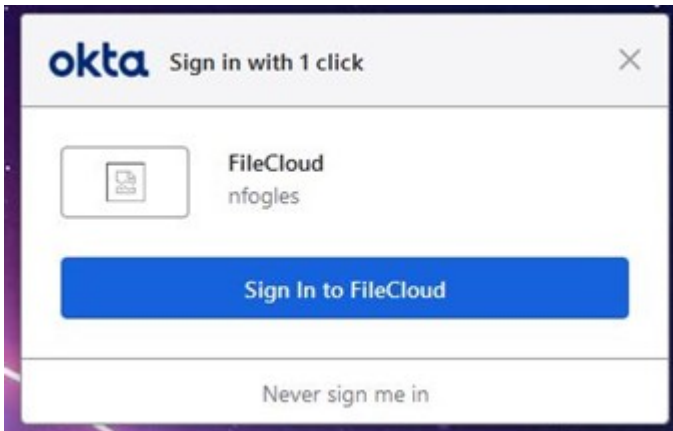
Password

Sign in

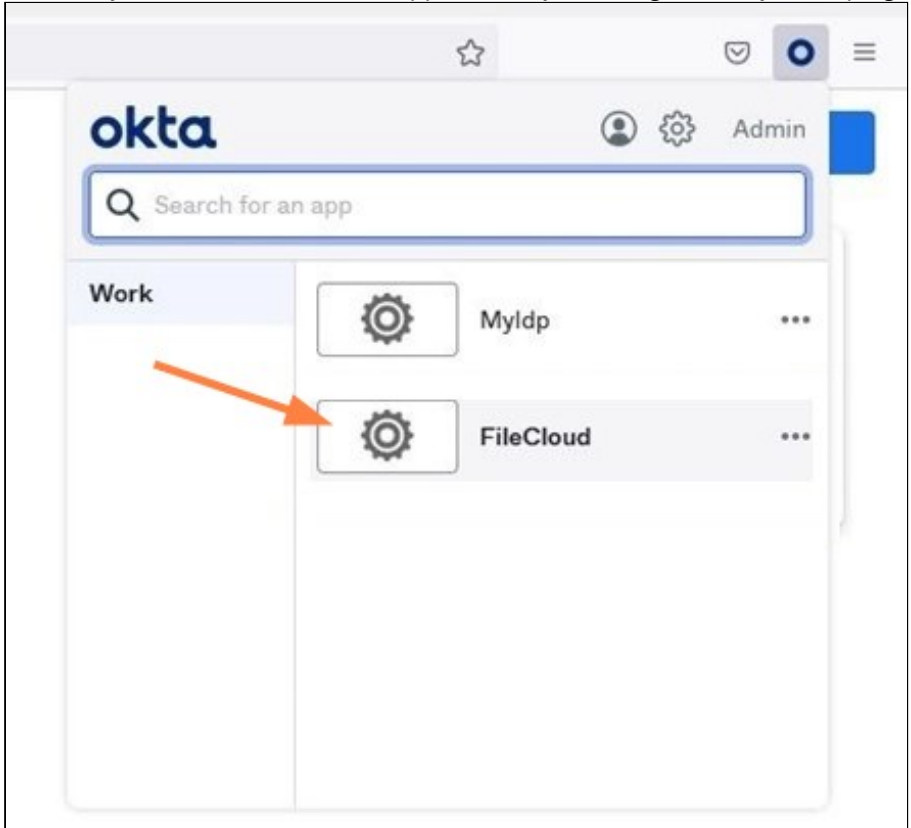
4. The browser redirects the user to the FileCloud login page in the Okta Admin Panel. The login screen with credentials filled in may appear first, and after a few seconds the FileCloud user portal should open (the user does not need to click **Login**).



Depending on the browser, when the user accesses the FileCloud login page again, the plugin may offer to log in for them:



Alternately, the user can access the application by choosing it directly in the plugin:



Integrate 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.

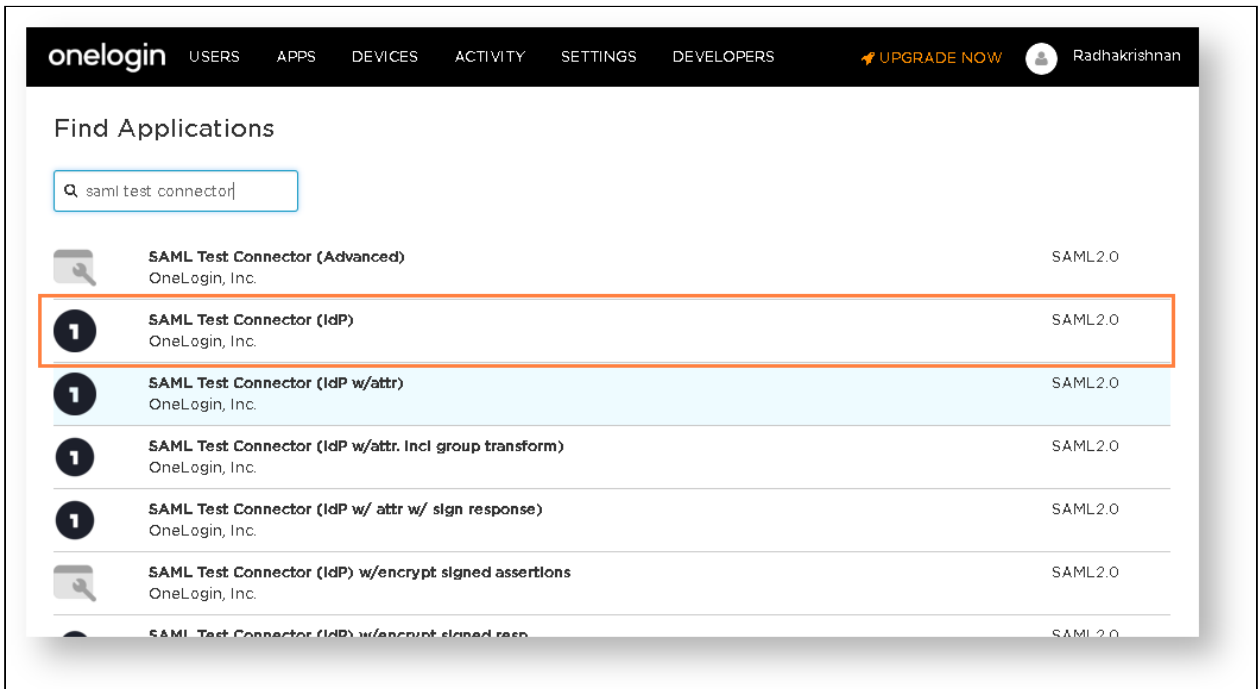
This article describes how to integrate OneLogin as an SSO provider with FileCloud.

⚠ Pre-requisite: 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 OneLogin web UI
2. Click on Apps → Add Apps

- Search for "saml test connector" and select the sample connector named "SAML Test Connector (IdP)".



- In the add screen, enter a name to the connector. For example, something like "FileCloud Connector". Click "Save".
- Open the created connector and switch to "Configuration" tab.
- Assuming your FileCloud URL is "https://dev.company.com", fill the following values in the configuration tab.

Configuration	Value
RelayState	https://dev.company.com/auth/samlso.php
Audience	https://dev.company.com/simplesaml/module.php/saml/sp/metadata.php/default-sp
Recipient	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL Validator*	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL*	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

← SAML Test Connector (IdP)

MORE ACTIONS ▾

SAVE

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Application Details

RelayState

Audience

Recipient

ACS (Consumer) URL Validator*

*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest

ACS (Consumer) URL*

*Required

Single Logout URL

- Once the configuration tab is completed, switch to "Parameters" tab.
- Add the following four parameters:

Field name	Flags	Value
givenName	Include in SAML accertion	First Name
mail	Include in SAML accertion	Email
sn	Include in SAML accertion	Last Name
uid	Include in SAML accertion	Username

New Field

Field name

This is the name of the field in the application's API

Flags

Include in SAML assertion

Multi-value parameter

CANCEL

USERS
APPS
DEVICES
ACTIVITY
SETTINGS
DEVELOPERS

← SAML Test Connector (IdP)

Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges

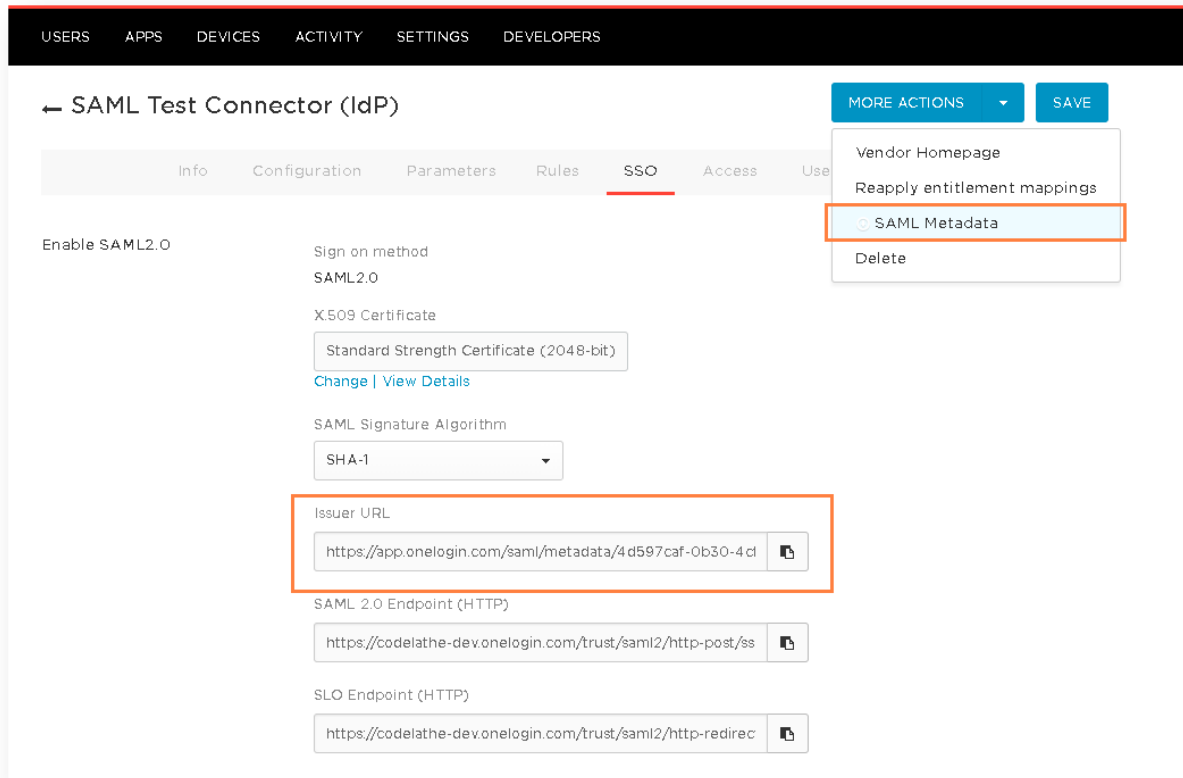
Credentials are

Configured by admin Configured by admins and shared by all users

SAML Test Connector (IdP) Field	Value	Add parameter
NameID (fka Email)	Email	
givenName	First Name	custom parameter
mail	Email	custom parameter
sn	Last Name	custom parameter
uid	Username	custom parameter

9. Save these changes. Once the save is complete, switch to SSO tab.
10. In the SSO tab, note "Issuer URL".

11. Download the metadata file from "More Actions" → "SAML Metadata".



12. Finally, add users to the newly created "FileCloud Connector" either individually or as group.

Integrate FileCloud with OneLogin SSO

1. Login into FileCloud admin UI.
2. Navigate to Settings → SSO tab.
3. Select default SSO type to be SSO.
4. Use the following table to fill the SAML configuration.

SAML Settings	Value
IdP Endpoint URL	" Issuer URL " noted in the previous section in OneLogin SSO tab
IdP Username Parameter	uid
IdP Email Parameter	mail
IdP Given Parameter	givenName
IdP Surname Parameter	sn

SAML Settings	Value
IdP Metadata	Copy and the paste the contents of SAML metadata from OneLogin web UI.

Single Sign On (SSO) Settings

Default SSO Type:
 Specify the Single Sign On Type

SAML Settings

IdP End Point URL:
 URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter:
 Username Parameter Name in Identity Provider

IdP Email Parameter:
 Email Parameter Name in Identity Provider

IdP Given Name Parameter:
 Given Name Parameter Name in Identity Provider

IdP Surname Parameter:
 Surname Parameter Name in Identity Provider

IdP Metadata:
 SAML metadata XML content.

5. Save the changes

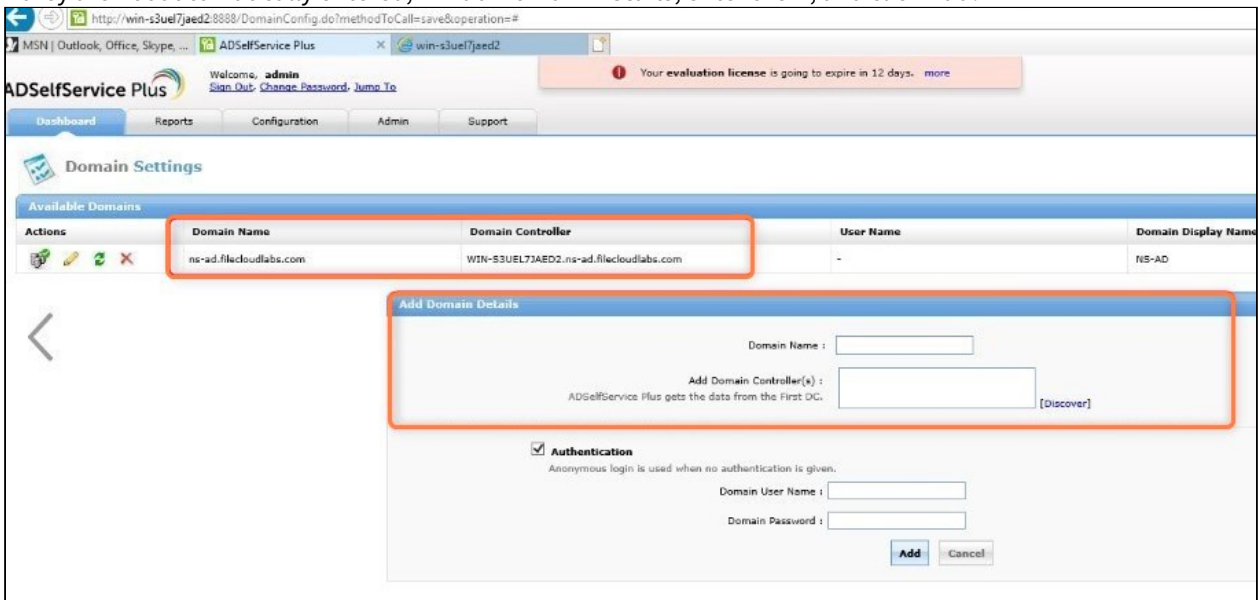
Integrate ADSelfService Plus with FileCloud

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.

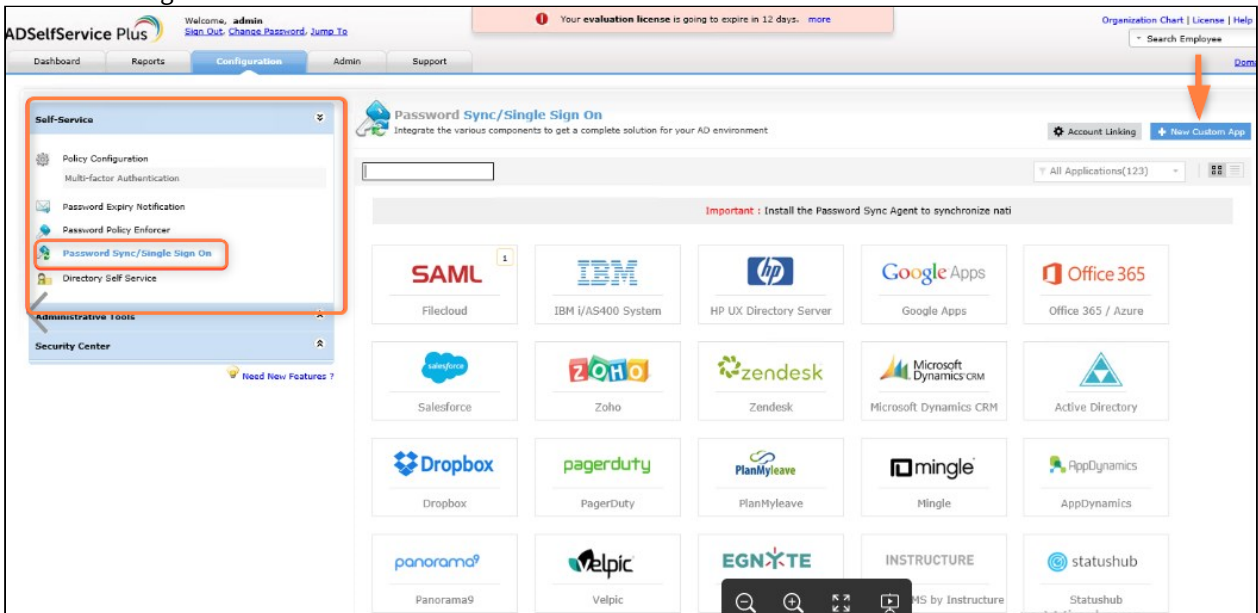
To integrate ADSelfService Plus with SimpleSAML SSO:

Step 1: Install ADSelfService Plus and Configure it to integrate with SimpleSAML SSO in FileCloud

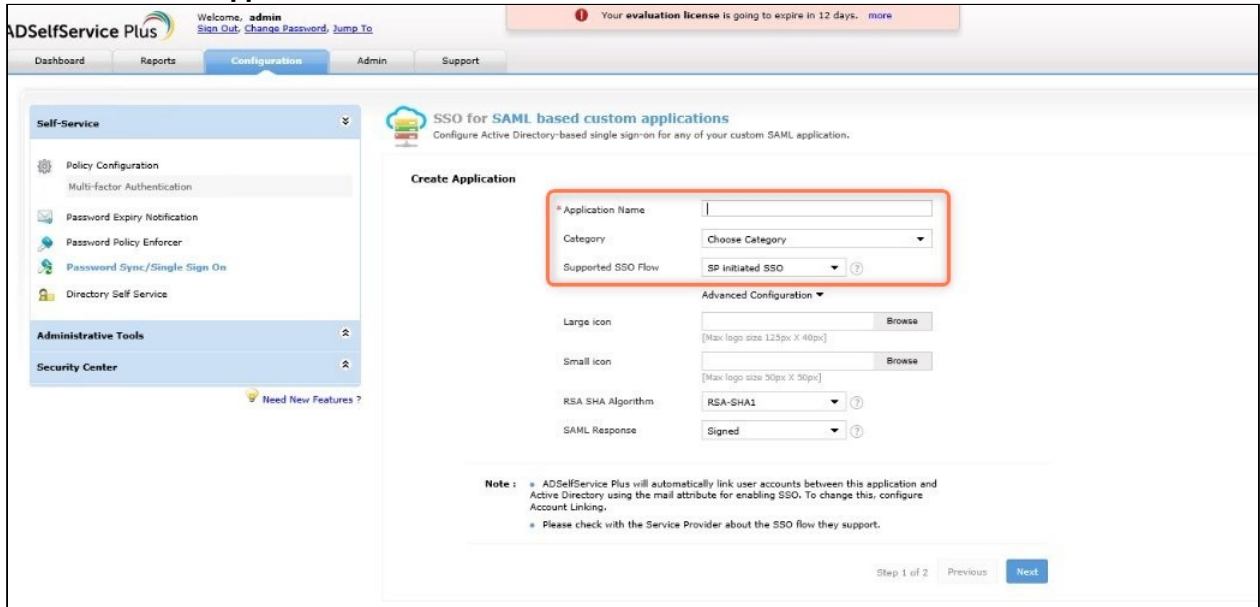
1. Install ADSelfService Plus.
2. Open the ADSelfService admin portal. Your URL should be similar to <http://win-s3uexxjaed2:8888/authorization.do>.
The Dashboard tab should be selected, and the server name should appear similar to: `win-s3uexxjaed2`
3. If AD is already installed, **Domain Name** and **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**.


Welcome, **admin**
[Sign Out](#), [Change Password](#), [Jump To](#)

Your evaluation license is going to expire in 12 days. [more](#)

Dashboard Reports **Configuration** Admin Support

Self-Service

- Policy Configuration
 - Multi-factor Authentication
- Password Expiry Notification
- Password Policy Enforcer
- Password Sync/Single Sign On
- Directory Self Service

Administrative Tools

Security Center

[Need New Features ?](#)

SSO for SAML based custom applications
 Configure Active Directory-based single sign-on for any of your custom SAML application.

Create Application

* Application Name

Category **Choose Category**

Supported SSO Flow **SP Initiated SSO**

Advanced Configuration

Large icon **Browse**
[Max logo size 125px X 40px]

Small icon **Browse**
[Max logo size 50px X 50px]

RSA SHA Algorithm **RSA-SHA1**

SAML Response **Signed**

Note :

- ADSelfService Plus will automatically link user accounts between this application and Active Directory using the mail attribute for enabling SSO. To change this, configure Account Linking.
- Please check with the Service Provider about the SSO flow they support.

Step 1 of 2 [Previous](#) [Next](#)

7. Fill in the following **Create Application** fields:

- In **Application Name** enter **FileCloud**.
- In **Category** drop-down list, choose any option.
- 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:

- 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.
- In **Display Name** enter any name.
- In **SAML Redirect URL** enter `https://yourFileclouddomainname/simplesaml/module.php/saml/sp/metadata.php/default-sp`
- 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. Log in to the FileCloud admin portal.
2. Navigate to Settings > SSO.
3. In **Default SSO Type**, choose **SAML**.
4. 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.

i 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**.

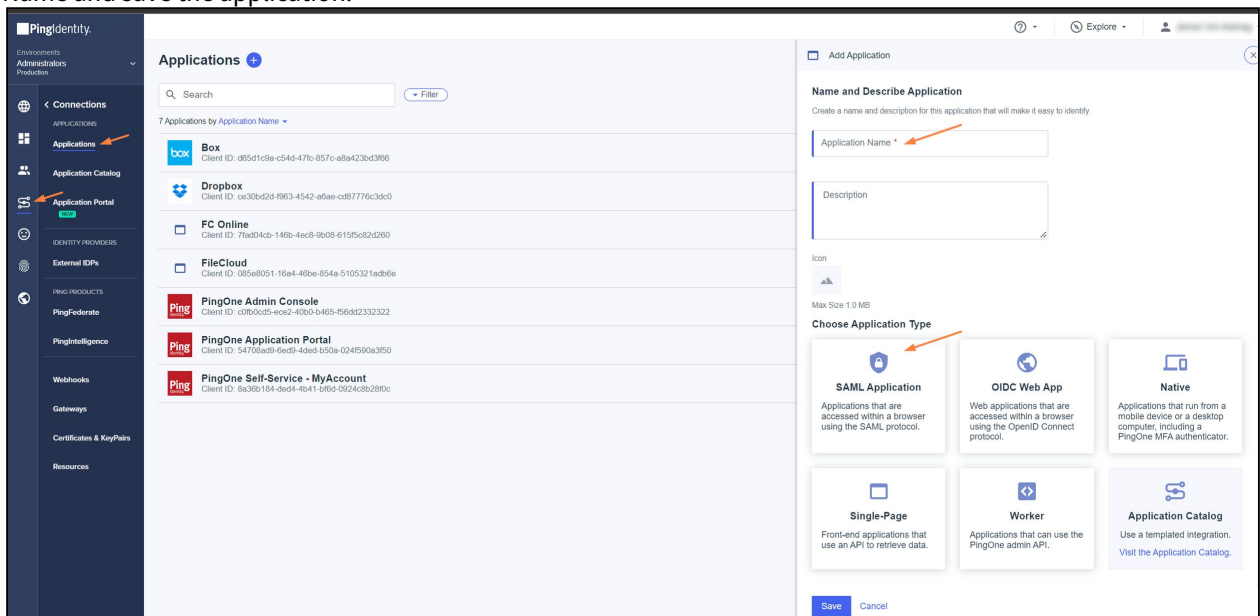
Integrate Ping Identity SSO with Filecloud

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-acis.php/default-sp

Entity ID:

https://<your_filecloud_url>/simplesaml/module.php/saml/sp/metadata.php/default-sp

Add Application

SAML Configuration

Provide Application Metadata

Import Metadata Import From URL Manually Enter


ACS URLs *

+ Add

Entity ID *

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

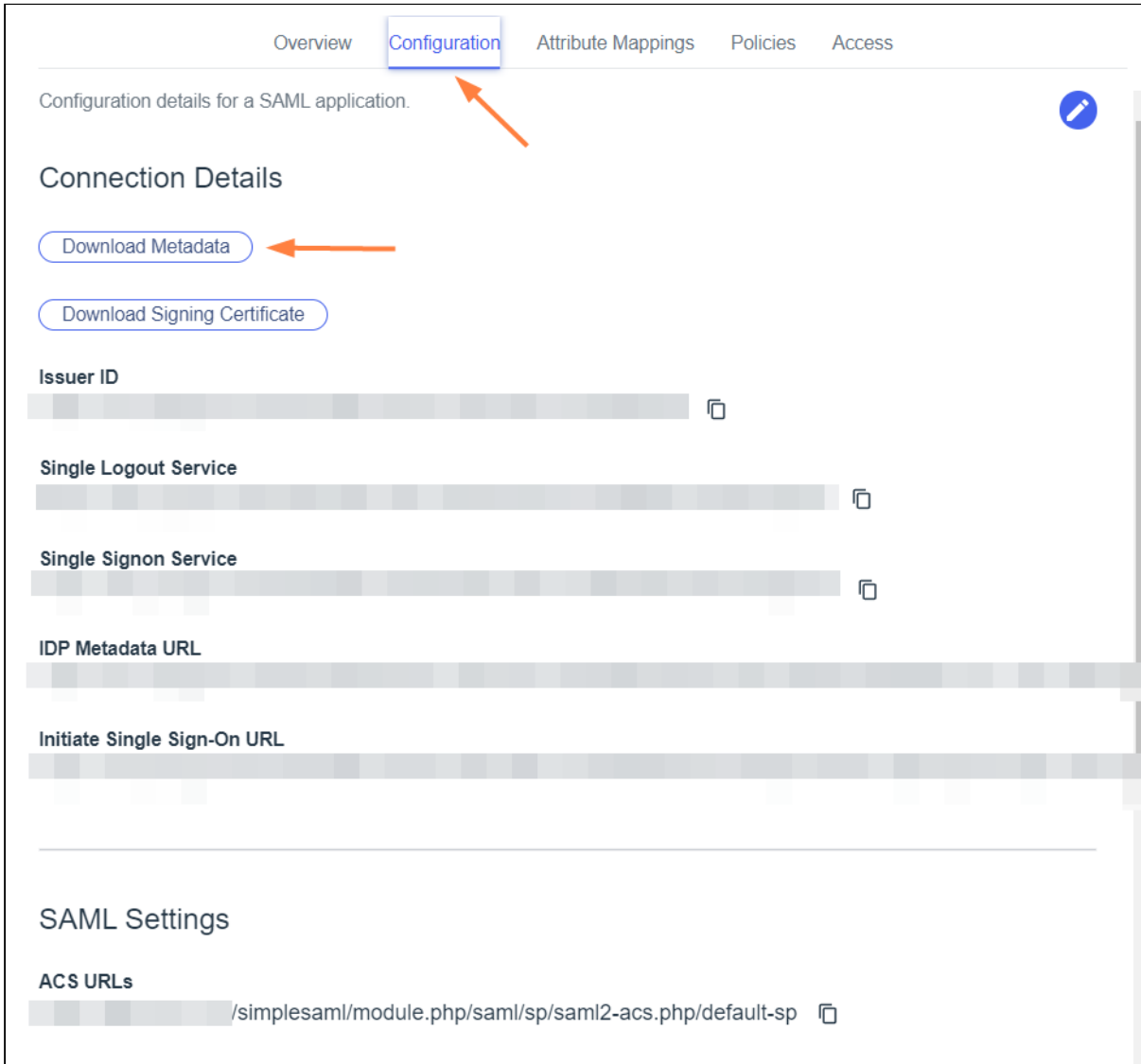
Overview Configuration **Attribute Mappings** Policies Access

These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See [Mapping attributes](#).

⚠ If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

FC Online	PingOne
saml_subject	User ID Required
givenName	Given Name
mail	Email Address
sn	Family Name
uid	User ID

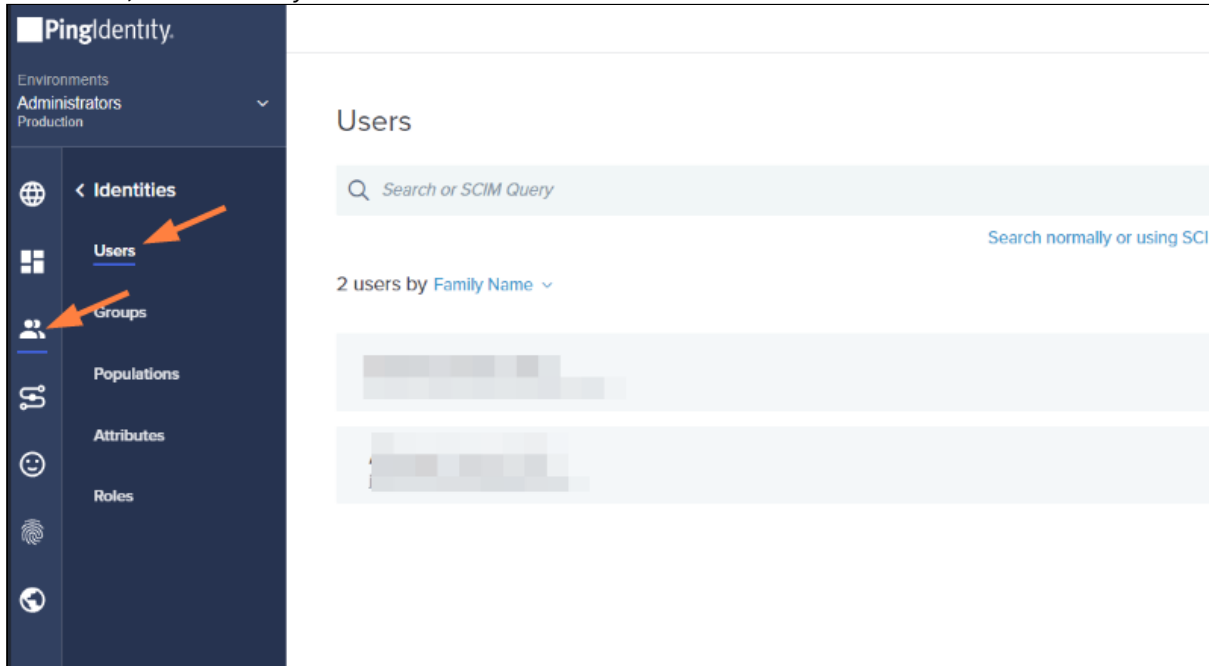
- Click the **Configuration** tab.
- To get a copy of the metadata file associated with the configuration, click **Download Metadata**. Save the file so you can enter its contents into the FileCloud admin portal.



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 admin portal, go to **Settings > SSO**.
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
IdP Metadata	Copy the contents of the metadata file downloaded above paste them here.

Single Sign On (SSO) Settings

Default SSO Type 
Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*
URL or EntityID of the Identity Provider that the Service Provider must contact.

IdP Username Parameter*
Username Parameter Name in Identity Provider

IdP Email Parameter*
Email Parameter Name in Identity Provider

IdP Given Name Parameter*
Given Name Parameter Name in Identity Provider

IdP Surname Parameter*
Surname Parameter Name in Identity Provider

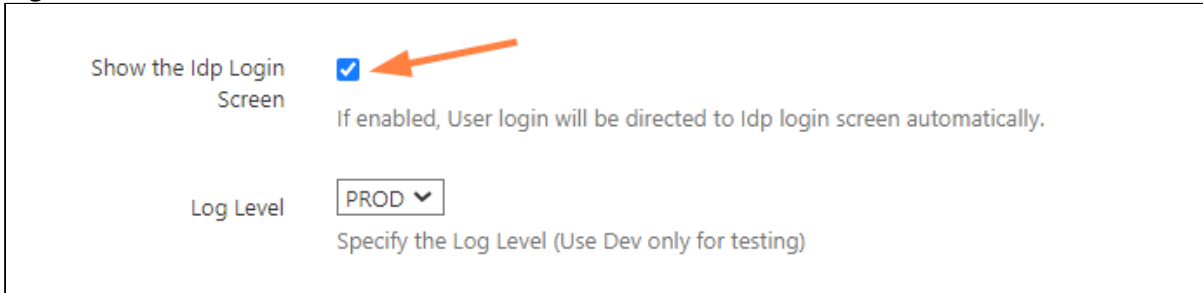
IdP Log Out URL (Optional)
URL to call to logout of Identity Provider (Optional)

Limit Login to Idp Group (Optional)
Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute

IdP Metadata*

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
entityID="l
"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML
:2.0:protocol">
    <md:KeyDescriptor use="signing">
```

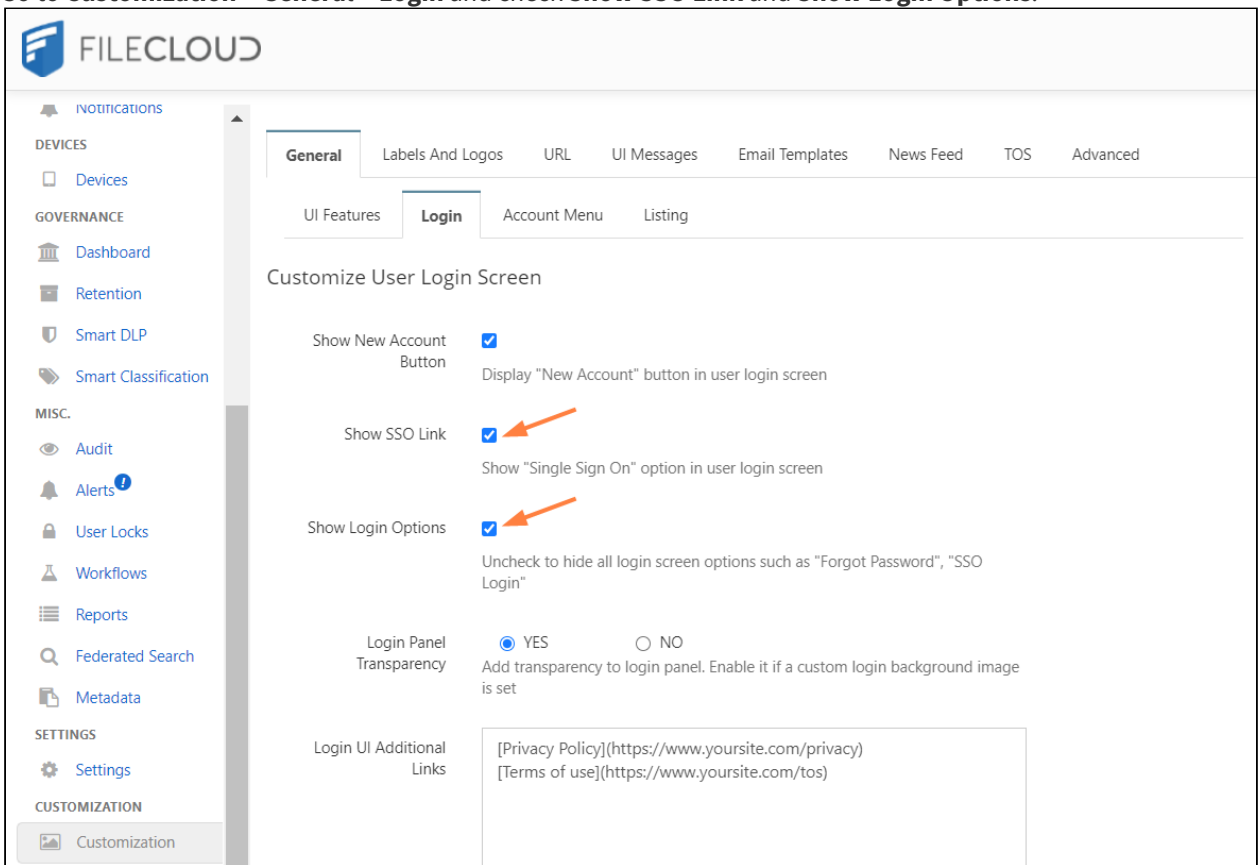

- If you want users to see the Ping Identity login after they click **Login with SSO**, scroll to the bottom of the screen and check **Show the Idp Login Screen**.
If you want users to be directly logged into FileCloud after they click **Login with SSO**, do not check **Show the Idp Login Screen**.



Show the Idp Login Screen **←**
If enabled, User login will be directed to Idp login screen automatically.

Log Level **▼**
Specify the Log Level (Use Dev only for testing)

- Click **Save**.
- Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.



FILECLOUD

NOTIFICATIONS

DEVICES

Devices

GOVERNANCE

Dashboard

Retention

Smart DLP

Smart Classification

MISC.

Audit

Alerts

User Locks

Workflows

Reports

Federated Search

Metadata

SETTINGS

Settings

CUSTOMIZATION

Customization

General Labels And Logos URL UI Messages Email Templates News Feed TOS Advanced

UI Features **Login** Account Menu Listing

Customize User Login Screen

Show New Account Button
Display "New Account" button in user login screen

Show SSO Link **←**
Show "Single Sign On" option in user login screen

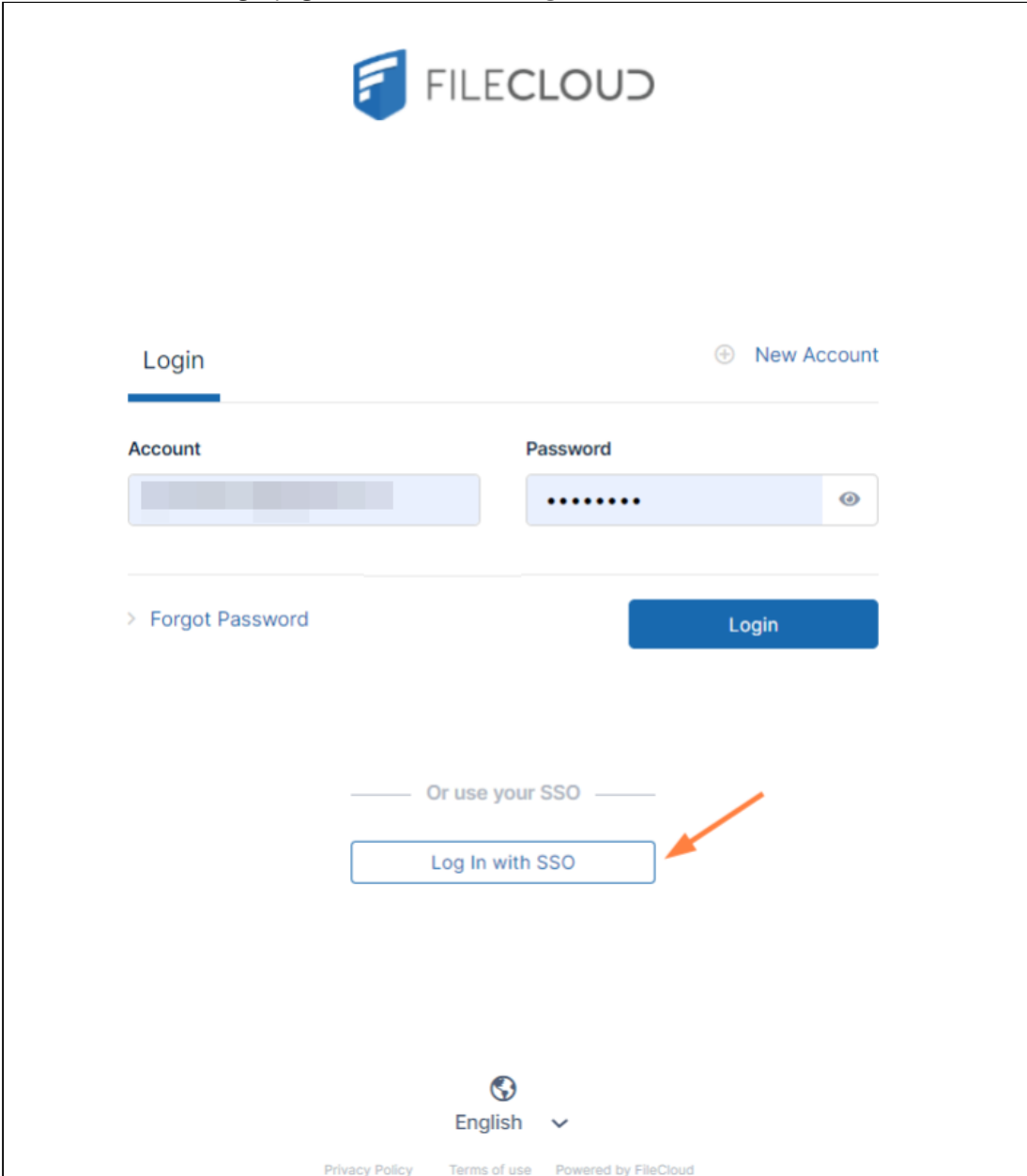
Show Login Options **←**
Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

Login Panel Transparency YES NO
Add transparency to login panel. Enable it if a custom login background image is set

Login UI Additional Links
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/tos)

Log in to FileCloud using Single Sign-on with Ping Identity

1. In the Filecloud User login page, the user chooses **Login with SSO**.



The screenshot displays the FileCloud login interface. At the top center is the FileCloud logo. Below it, the 'Login' tab is selected, with a 'New Account' link to the right. The form contains two input fields: 'Account' and 'Password'. Below the 'Account' field is a '> Forgot Password' link. A blue 'Login' button is positioned to the right of the 'Account' field. Below the 'Password' field is a 'Log In with SSO' button, which is highlighted with an orange arrow. Above this button is the text 'Or use your SSO'. At the bottom of the page, there is a language selector set to 'English' and a footer containing 'Privacy Policy', 'Terms of use', and 'Powered by FileCloud'.

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 hosts 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, the FileCloud will act as a Service Provider (SP) and also a claims aware application. As a claims-aware application, FileCloud accepts claims in the form of ADFS security tokens from 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.

When ADFS is used, the IdP (Identity Provider) in this document refers to Active Directory Federation Server. When ADFS successfully authenticates the user account, 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.

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 ships with FileCloud will 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, the following steps must be followed.

1. Configure Apache Webserver
2. Set SAML as the default Single Sign On Method in FileCloud Interface and Configure IdP settings in the FileCloud Admin Interface
3. Enable Single Sign On Link on the login page.
4. Register the FileCloud as a Service Provider (SP) with IdP by adding FileCloud as a Relying Party Trust in ADFS.

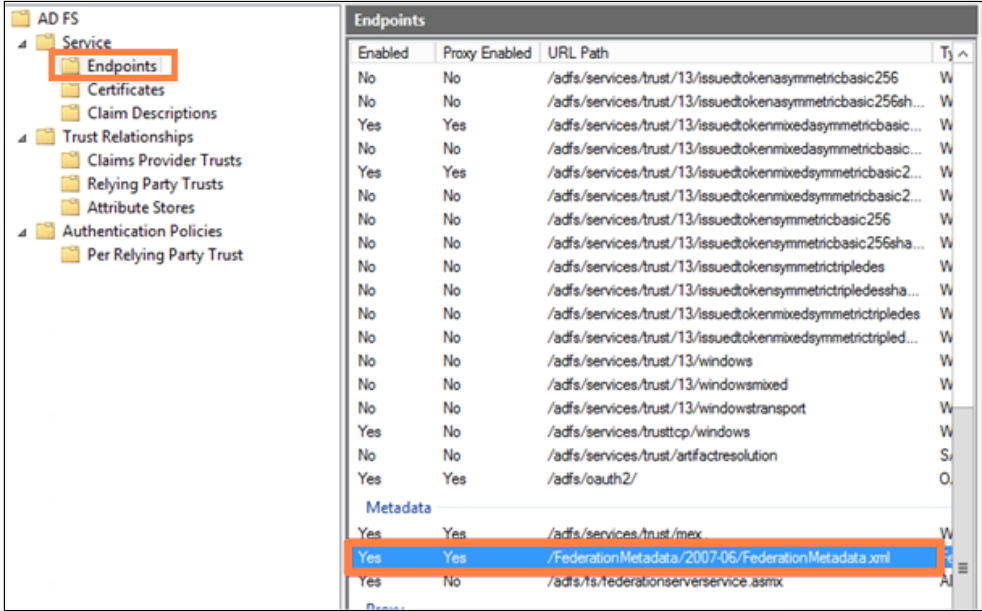
Step 1: Web Server Configuration

Follow the steps in [SAML Single Sign-On Support](#) to set up the Web Server configuration and enable SSO.

Step 2: IdP/ADFS Configuration

In the FileCloud Admin Interface – Settings => SSO => SSOType the default FileCloud SSO Type must be set to SAML. Other parameters must be set as per your IdP settings.

FileCloud Parameters	ADFS as IdP Data can be obtained from Federation Metadata
default SSO Type	For ADFS, select SAML

FileCloud Parameters	ADFS as IdP Data can be obtained from Federation Metadata																																																																																																																								
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. value: uid																																																																																																																								
IdP Email Parameter	Identifies the email of the user (must be unique) value: mail																																																																																																																								
IdP Given Name Parameter	Identifies the given name of the user. value: givenName																																																																																																																								
IdP Surname Parameter	Identifies the surname of the user Default value: sn																																																																																																																								
IdP Metadata	Federation Metadata in xml format. Usually ADFS metadata is found at the URL Path below: e.g. https://yourADFSDomain/federationmetadata/2007-06/federationmetadata.xml  <table border="1" data-bbox="485 1157 1461 1764"> <thead> <tr> <th colspan="5">Endpoints</th> </tr> <tr> <th>Enabled</th> <th>Proxy</th> <th>Enabled</th> <th>URL Path</th> <th>Type</th> </tr> </thead> <tbody> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenasymmetricbasic256</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...</td><td>W</td></tr> <tr><td>Yes</td><td>Yes</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...</td><td>W</td></tr> <tr><td>Yes</td><td>Yes</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokensymmetricbasic256</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokensymmetricbasic256sha...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokensymmetrictriplede...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokensymmetrictriplede...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/windows</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/windowsmixed</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/13/windowstransport</td><td>W</td></tr> <tr><td>Yes</td><td>No</td><td></td><td>/adfs/services/trusttcp/windows</td><td>W</td></tr> <tr><td>No</td><td>No</td><td></td><td>/adfs/services/trust/artifactresolution</td><td>S</td></tr> <tr><td>Yes</td><td>Yes</td><td></td><td>/adfs/oauth2/</td><td>O</td></tr> <tr><td colspan="5">Metadata</td></tr> <tr><td>Yes</td><td>Yes</td><td></td><td>/adfs/services/trust/mex</td><td>W</td></tr> <tr><td>Yes</td><td>Yes</td><td></td><td>/FederationMetadata/2007-06/FederationMetadata.xml</td><td>W</td></tr> <tr><td>Yes</td><td>No</td><td></td><td>/adfs/ls/federationserver/service.asmx</td><td>A</td></tr> </tbody> </table>	Endpoints					Enabled	Proxy	Enabled	URL Path	Type	No	No		/adfs/services/trust/13/issuedtokenasymmetricbasic256	W	No	No		/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	W	Yes	Yes		/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	W	No	No		/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	W	Yes	Yes		/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	W	No	No		/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	W	No	No		/adfs/services/trust/13/issuedtokensymmetricbasic256	W	No	No		/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	W	No	No		/adfs/services/trust/13/issuedtokensymmetrictriplede...	W	No	No		/adfs/services/trust/13/issuedtokensymmetrictriplede...	W	No	No		/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...	W	No	No		/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...	W	No	No		/adfs/services/trust/13/windows	W	No	No		/adfs/services/trust/13/windowsmixed	W	No	No		/adfs/services/trust/13/windowstransport	W	Yes	No		/adfs/services/trusttcp/windows	W	No	No		/adfs/services/trust/artifactresolution	S	Yes	Yes		/adfs/oauth2/	O	Metadata					Yes	Yes		/adfs/services/trust/mex	W	Yes	Yes		/FederationMetadata/2007-06/FederationMetadata.xml	W	Yes	No		/adfs/ls/federationserver/service.asmx	A
Endpoints																																																																																																																									
Enabled	Proxy	Enabled	URL Path	Type																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenasymmetricbasic256	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	W																																																																																																																					
Yes	Yes		/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	W																																																																																																																					
Yes	Yes		/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokensymmetricbasic256	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokensymmetrictriplede...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokensymmetrictriplede...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...	W																																																																																																																					
No	No		/adfs/services/trust/13/issuedtokenmixedsymmetrictriplede...	W																																																																																																																					
No	No		/adfs/services/trust/13/windows	W																																																																																																																					
No	No		/adfs/services/trust/13/windowsmixed	W																																																																																																																					
No	No		/adfs/services/trust/13/windowstransport	W																																																																																																																					
Yes	No		/adfs/services/trusttcp/windows	W																																																																																																																					
No	No		/adfs/services/trust/artifactresolution	S																																																																																																																					
Yes	Yes		/adfs/oauth2/	O																																																																																																																					
Metadata																																																																																																																									
Yes	Yes		/adfs/services/trust/mex	W																																																																																																																					
Yes	Yes		/FederationMetadata/2007-06/FederationMetadata.xml	W																																																																																																																					
Yes	No		/adfs/ls/federationserver/service.asmx	A																																																																																																																					

FileCloud Parameters	ADFS as IdP Data can be obtained from Federation Metadata
Enable ADFS	Yes
Log Mode	Set the Log Mode for the SAML Calls. Default Value: prod (Do not use DEV for production systems)

Single Sign On (SSO) Settings

Default SSO Type

Specify the Single Sign On Type

SAML Settings

IdP End Point URL

URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter

Username Parameter Name in Identity Provider

IdP Email Parameter

Email Parameter Name in Identity Provider

IdP Given Name Parameter

Given Name Parameter Name in Identity Provider

IdP Surname Parameter

Surname Parameter Name in Identity Provider

IdP Metadata

Step 3: Enable SSO link

Follow the steps in [SAML Single Sign-On Support](#) (under SSO Configuration Steps, Step 5) to enable SSO sign-in on the User or Admin Interface.

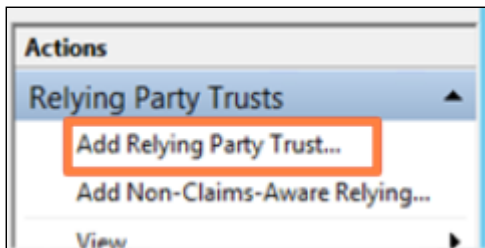
Step 4: Register FileCloud as SP in IdP/ADFS

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).

i <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 all the previous steps 1, 2 and 3 above were completed successfully.

1. On your ADFS server, open the ADFS management console, expand Trust Relationships and select Relying Party Trusts 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.

you can also do it manually by downloading your metadata file from <http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp> and import it into ADFS by choosing "import data about relying party from a file"

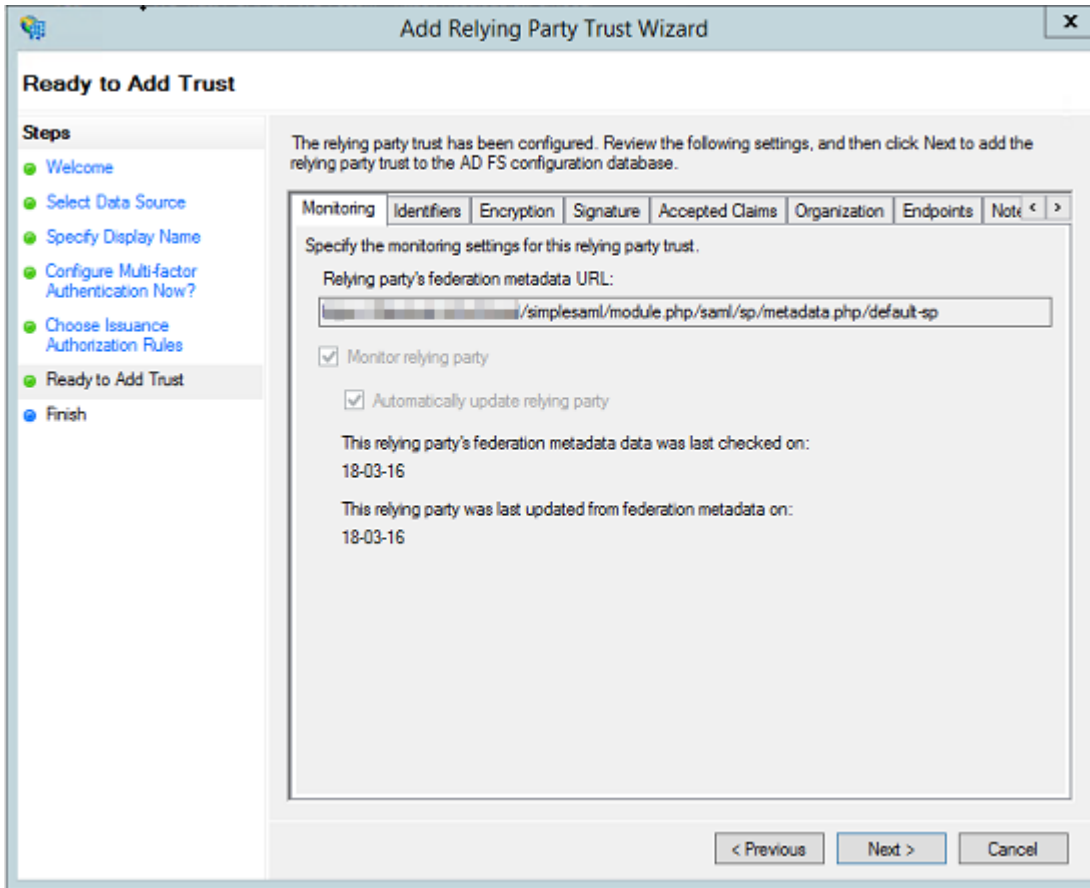
i once you access the metadata URL you need to enter admin credentials to be able to download the metadata file, the username is **admin** and password can be found in :
 <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php

3. Accept the Warning

4. Enter the display name for the Relying Party Trust, usually your FileCloud URL.

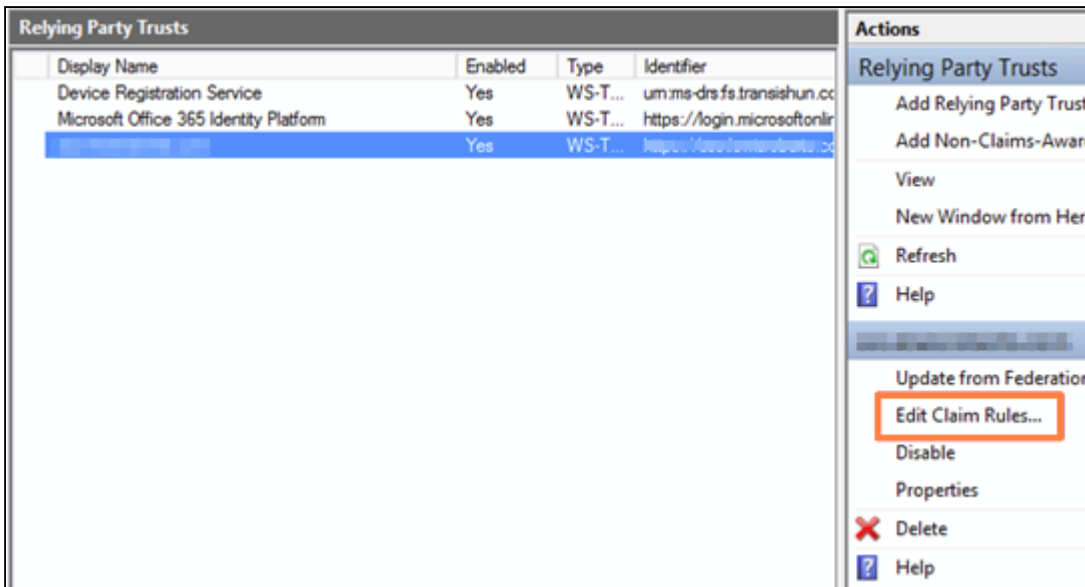
The screenshot shows a window titled "Add Relying Party Trust Wizard" with a close button in the top right corner. The main heading is "Specify Display Name". On the left, a "Steps" pane lists the following steps: Welcome, Select Data Source, Specify Display Name (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, there is a "Display name:" label followed by a text input field. Underneath is a "Notes:" label followed by a large text area with a vertical scrollbar. At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

5. Next Way through your Wizard until you reach **Ready to Add Trust** Page. Here, review the tabs. Encryption and Signature tabs must have values associated with them.

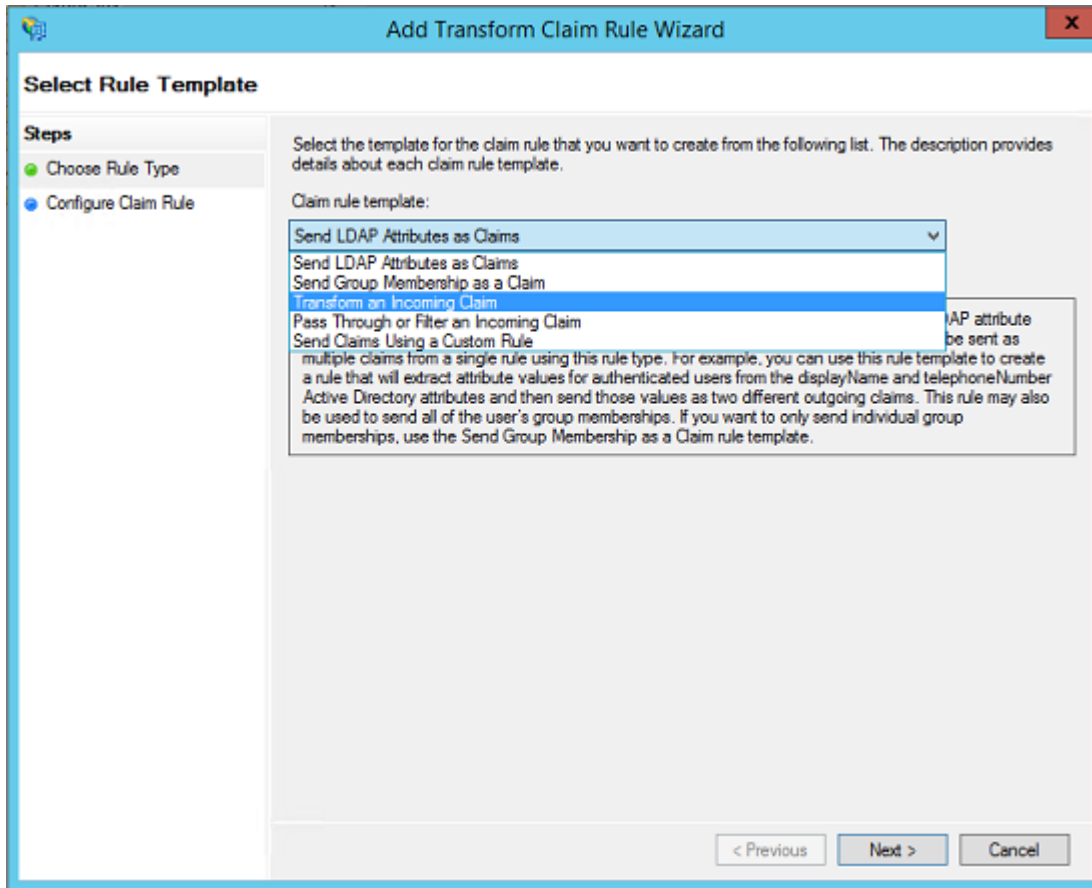


6. Click Next and the new Relying Party Trust is now added.

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.



8. Give a **Claim Rule Name** (Name ID Transform - can be anything). Enter **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.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

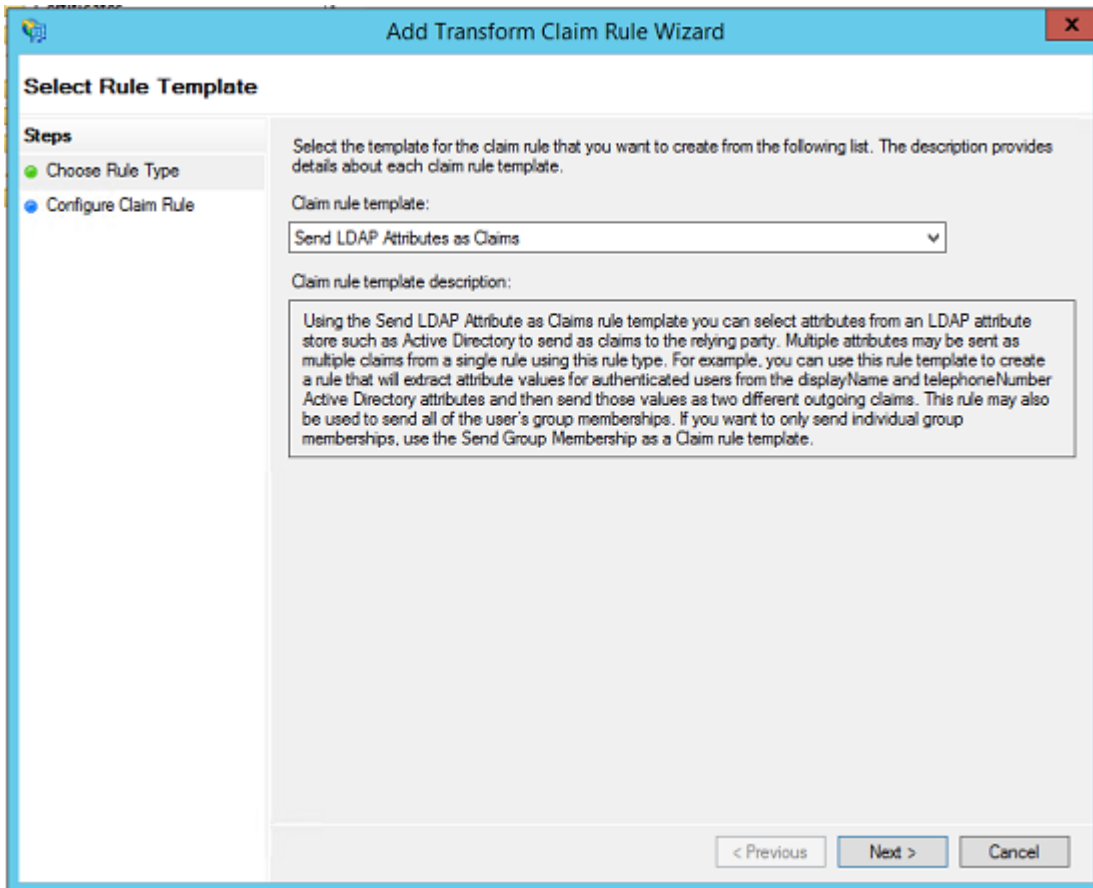
Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

Pass through all claim values
 Replace an incoming claim value with a different outgoing claim value
 Incoming claim value:
 Outgoing claim value:
 Replace incoming e-mail suffix claims with a new e-mail suffix
 New e-mail suffix:
 Example: fabrikam.com

9. Add **another Issuance Transform Rule**. Select **Send LDAPAttributes as Claims** template.



10. Enter a **name for Claim Rule** (LDAP Claims - can be anything). Select **Active Directory** as **Attribute Store**. Add the **Mapping of LDAP Attributes to outgoing claim types**. The outgoing claim type must match the names as specified in FileCloud SSO Settings UI Page (screenshot below follows the FileCloud SSO Settings as documented above). **Outgoing claim type of "uid" and "mail" is absolutely required**. SAM Account Name in the screenshot below can be replaced with UPN if desired. Click **Finish** to add the rule.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
LDAP Claims

Rule template: Send LDAP Attributes as Claims

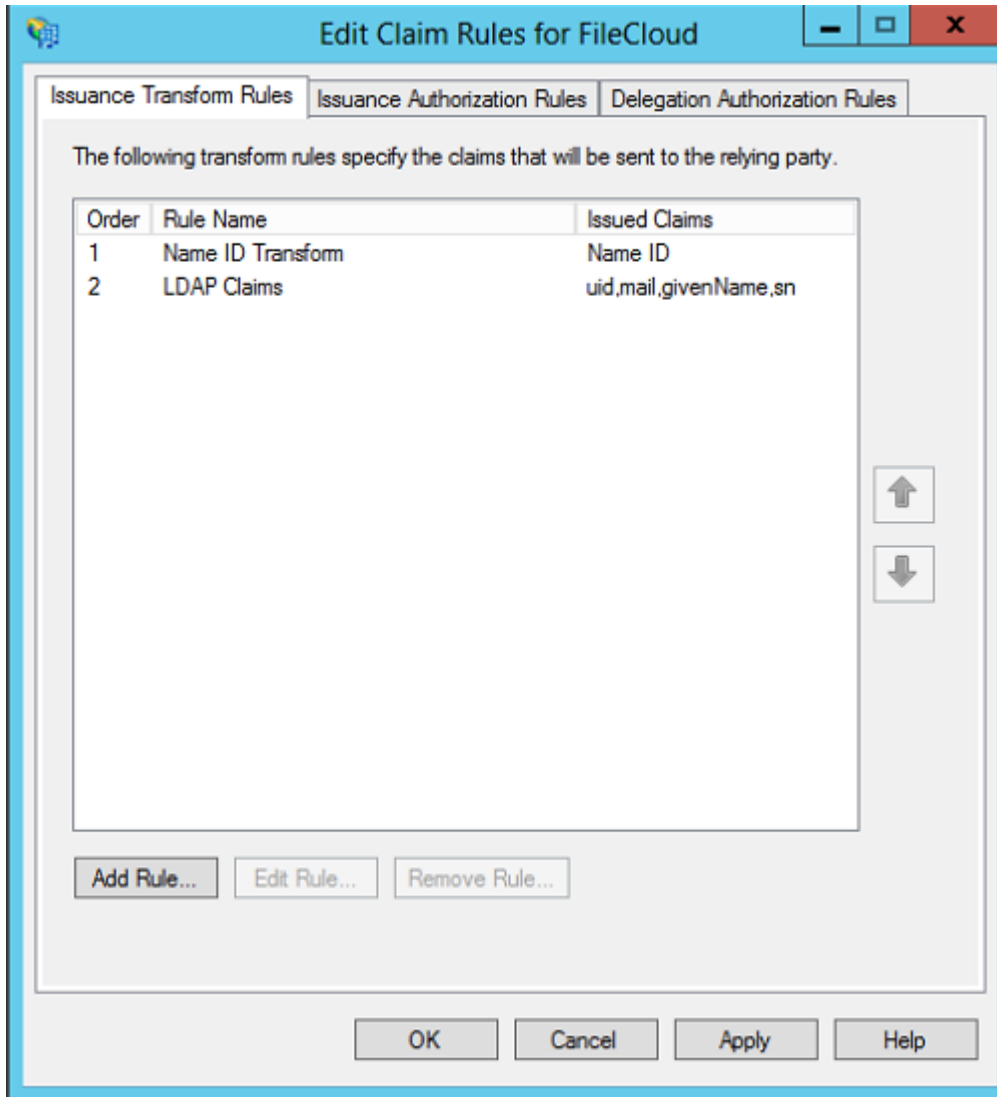
Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	uid
	E-Mail-Addresses	mail
	Given-Name	givenName
▶	Surname	sn
*		

< Previous Finish Cancel

11. Once Configured, you should have **two issuance transform rules**. (Screenshot below shows only one rule. However, you will have 2 rules (Name ID Transform and LDAP Claims if followed the steps above). Click Apply and Exit.



This completes the ADFS configuration and the FileCloud is added as a Relying Party Trust in ADFS server. You can now test the SSO from FileCloud by going to the FileCloud login page and clicking the Single Sign On link as mentioned in Step 3 of this documentation.

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.

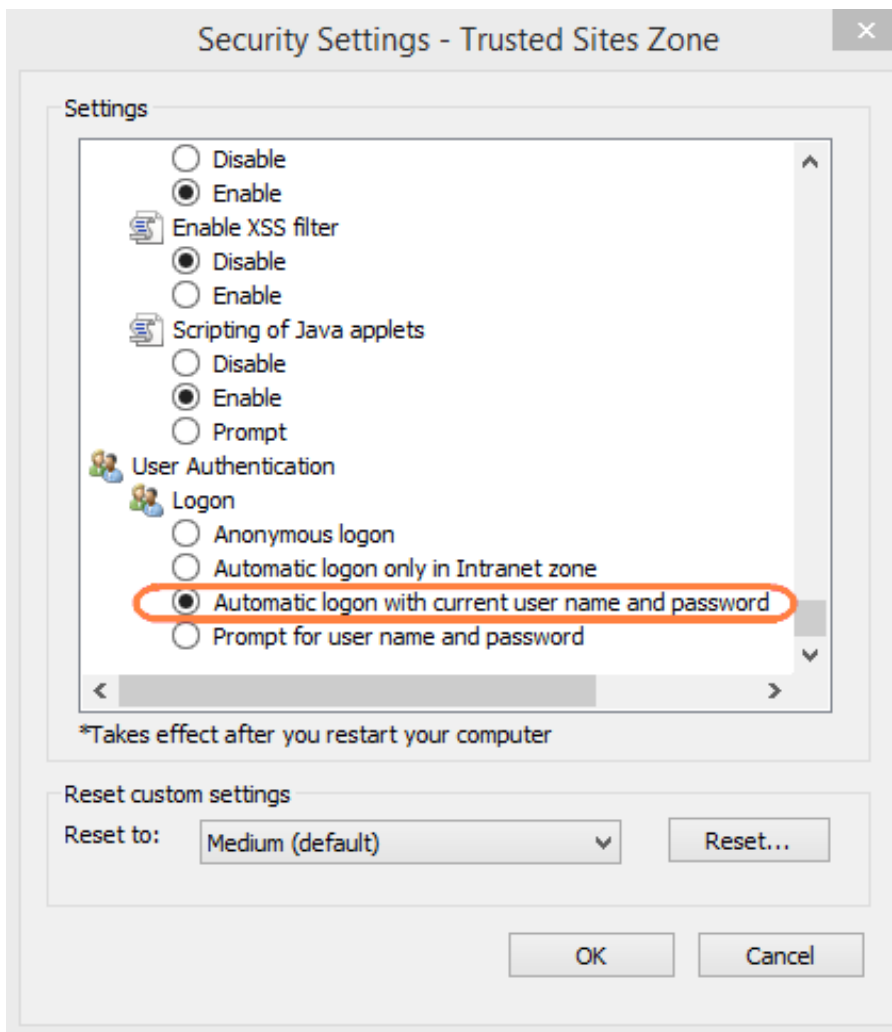
Web Server Settings

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



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.
4. The FileCloud version must be 4.0 or higher.

-  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

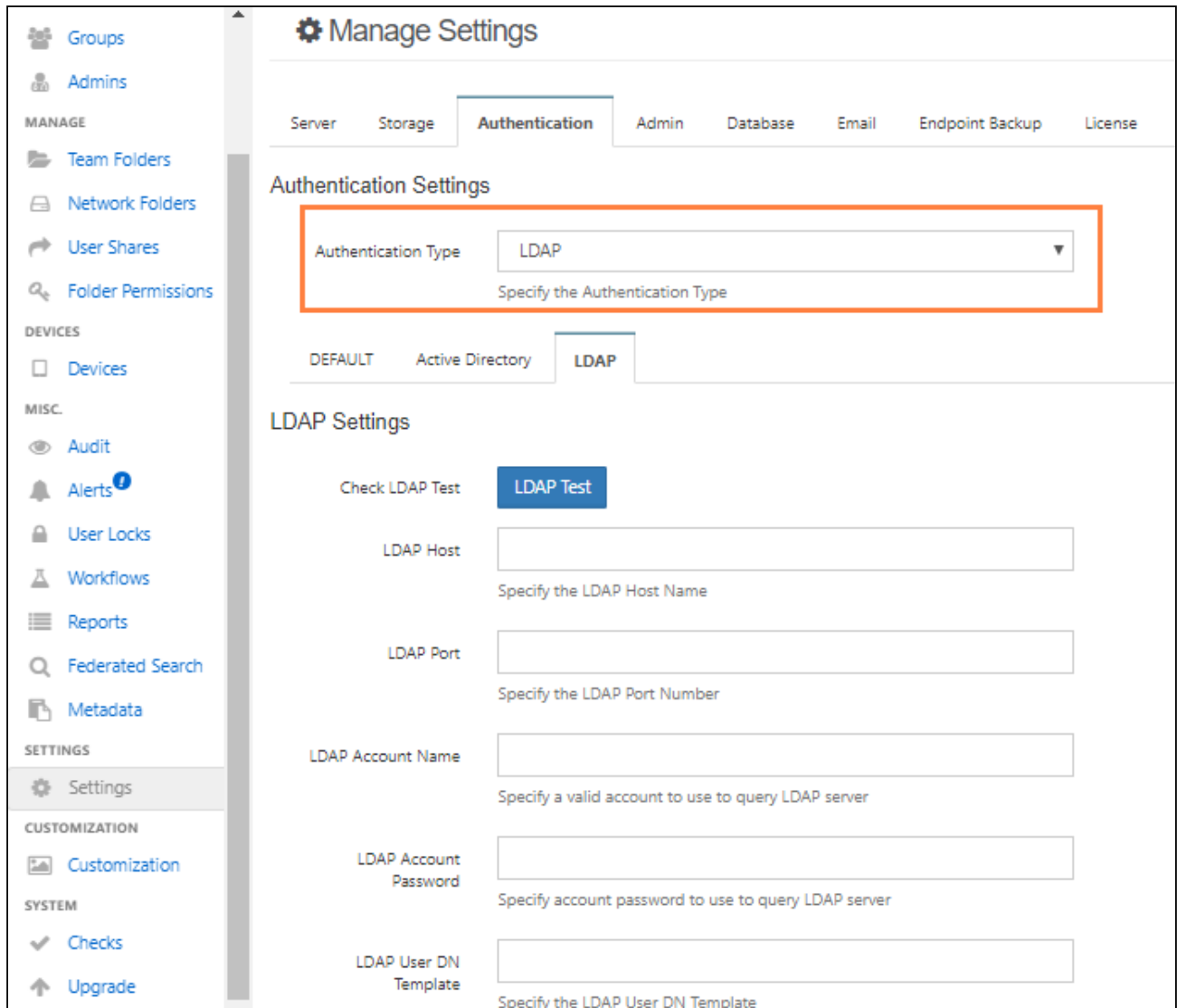
To enable LDAP Authentication in FileCloud:

1. Log into the FileCloud Admin Portal.

2. In the left navigation panel, click **Settings**.
3. In the right panel, from the list of tabs, click **Authentication**.
4. Under **Authentication Settings**, in **Authentication Type** select **LDAP**.
5. In LDAP Settings, enter the required information, and then click **Save**.

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

Show me the screen ...



The screenshot displays the 'Manage Settings' interface. On the left is a navigation sidebar with categories: MANAGE (Groups, Admins, Team Folders, Network Folders, User Shares, Folder Permissions), DEVICES (Devices), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), CUSTOMIZATION (Customization), and SYSTEM (Checks, Upgrade). The 'Settings' option is selected.

The main content area is titled 'Manage Settings' and has several tabs: Server, Storage, **Authentication**, Admin, Database, Email, Endpoint Backup, and License. The 'Authentication' tab is active.

Under 'Authentication Settings', the 'Authentication Type' dropdown menu is set to 'LDAP' and is highlighted with an orange border. Below it is the text 'Specify the Authentication Type'. There are also tabs for 'DEFAULT', 'Active Directory', and 'LDAP', with 'LDAP' being the selected tab.

The 'LDAP Settings' section includes the following fields:

- Check LDAP Test**: A blue button labeled 'LDAP Test'.
- LDAP Host**: A text input field with the placeholder 'Specify the LDAP Host Name'.
- LDAP Port**: A text input field with the placeholder 'Specify the LDAP Port Number'.
- LDAP Account Name**: A text input field with the placeholder 'Specify a valid account to use to query LDAP server'.
- LDAP Account Password**: A text input field with the placeholder 'Specify account password to use to query LDAP server'.
- LDAP User DN Template**: A text input field with the placeholder 'Specify the LDAP User DN Template'.

Read a description of the LDAP Settings

Once you have selected LDAP as your method of authentication, you must provide some additional information. Table 1 explains the required fields.

Table 1. LDAP Required Settings

SETTING	REQUIRED?	DESCRIPTION	Example
LDAP Host	REQUIRED	The hostname or IP address where the LDAP server is running	mycompany.com
LDAP Port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	389
LDAP Account Name	REQUIRED	A valid LDAP login account required to perform queries	<username>
LDAP Account Password	REQUIRED	Password for the LDAP Account Name	<password>
LDAP User DN Template	REQUIRED	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory. This is usually a combination of CN, OU, DC. Refer to your specific LDAP settings to uniquely identify a user. To use multiple OUs, set this equal to ^USE_USER_FULL_DN^	Use the token ^NAME^ in place of user name: cn=^NAME^,ou=someorg,dc=company,dc=com Multiple OU mode: ^USE_USER_FULL_DN^
LDAP Search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an <i>ou</i> 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	The filter to be used to identify a user entry record from results.	If the object class is inetOrgPerson, then you would use: (&(objectClass=inetOrgPerson)(cn=^NAME^))

SETTING	REQUIRED?	DESCRIPTION	Example
Mail Attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	username_email_ID

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

User DN Template:

uid=^NAME^,ou=someou,dc=company,dc=com

LDAP Search DN

ou=someou,dc=company,dc=com

LDAP User Filter Template:

(&(objectClass=zimbraAccount)(uid=^NAME^))

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

User DN Template:

uid=^NAME^,ou=Users,o=xxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com

LDAP Search DN

ou=users,o=xxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com

LDAP User Filter Template:

(&(objectClass=inetOrgPerson)(uid=^NAME^))

Manage Settings

Server
Storage
Authentication
Admin
Database
Email
Endpoint Backup
License
Policies
SSO
Content Search
Web Edit
Team Folders
Misc

Authentication Settings

Authentication Type LDAP ▼

Specify the Authentication Type

DEFAULT
Active Directory
LDAP

↻ Reset to defaults

Save

You have unsaved changes.

LDAP Settings

Check LDAP Test LDAP Test

LDAP Host abc.company.com

Specify the LDAP Host Name

LDAP Port 389

Specify the LDAP Port Number

LDAP Account Name username

Specify a valid account to use to query LDAP server

LDAP Account Password *****

Specify account password to use to query LDAP server

LDAP User DN Template cn=username,ou=Company-Users,dc=company,dc=com

Specify the LDAP User DN Template

LDAP Search DN ou=Company-Users,dc=company,dc=com

Specify the LDAP Search DN

LDAP User Filter Template

Specify the LDAP User Filter Template

Mail Attribute mail

Specify the LDAP Mail attribute

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>

SETTING	REQUIRED ?	DESCRIPTION	TLS Example
LDAP Port	REQUIRED	The port to be used to connect to LDAP server (typically 389)	389
LDAP Account Name	REQUIRED	A valid LDAP login account required to perform queries	<username>
LDAP Account Password	REQUIRED	Password for the LDAP Account Name	<password>
LDAP User DN Template	REQUIRED	<p>The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory.</p> <p>This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user.</p> <p>Use the token <code>^NAME^</code> in place of user name</p> <p>Example : <code>cn=^NAME^,ou=someorg,dc=company,dc=com</code></p> <p>To use multiple OUs, set this equal to <code>^USE_USER_FULL_DN^</code></p>	<code>cn=<username>,ou=<abc>,dc=<company>,dc=com</code> Multiple OU mode: <code>^USE_USER_FULL_DN^</code>
LDAP Search DN	REQUIRED	<p>The search DN (Specifies the set of resources to search for an user).</p> <p>If there is an <i>ou</i> encompassing all users, then the search DN would be pointing to that DN.</p> <p>For example, if all users are under the <i>employees</i> ou, then the search DN would be <code>ou=employees,dc=company,dc=com</code></p>	<code>ou=company-users,dc=company,dc=com</code>
LDAP User Filter Template	REQUIRED	<p>The filter to be used to identify a user entry record from results.</p> <p>For example, if the object class is <code>inetOrgPerson</code>, then you would use:</p> <code>(&(objectClass=inetOrgPerson)(cn=^NAME^))</code>	<code>(&(objectClass=inetOrgPerson)(cn=^NAME^))</code>

SETTING	REQUIRED ?	DESCRIPTION	TLS Example
Mail Attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	<i>username_email_ID</i>

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

Authentication Settings

Authentication Type: 

Specify the Authentication Type

DEFAULT
 Active Directory
 LDAP

LDAP Settings

Check LDAP Test:

LDAP Host:

Specify the LDAP Host Name

LDAP Port:

Specify the LDAP Port Number

LDAP Account Name:

Specify a valid account to use to query LDAP server

LDAP Account Password:

Specify account password to use to query LDAP server

LDAP User DN Template:

Specify the LDAP User DN Template

LDAP Search DN:

Specify the LDAP Search DN

LDAP User Filter Template:

Specify the LDAP User Filter Template

Mail Attribute:

Specify the LDAP Mail attribute

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 to follow the below notes:

- The server which is hosting FileCloud is able to communicate to the server which is hosting OIM.
- You have access to the Admin user and are able to access WebLogic Admin server.
- Both server's Firewall accept the incoming connection.

Integrating OIM's LDAP to FileCloud

To successfully integrate OIM's LDAP with FileCloud ensure that FileCloud is able to pull the corresponding attributes such as Name, Email, password and other. To verify this settings please review your connection settings under Oracles WebLogic Admin server > Domain Structure> Services> Security Realms >"myrealm" > Providers. Within the Providers select the Provider you will be using to connect to FileCloud via LDAP.

The screenshot shows the Oracle WebLogic Server Administration Console. The breadcrumb navigation is: Home > Summary of Servers > Summary of Security Realms > myrealm > Summary of Security Realms > myrealm > Providers. The 'Providers' tab is selected, and the 'Authentication' sub-tab is active. A table titled 'Authentication Providers' lists the following providers:

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
OIMAuthenticationProvider	Provider that performs authentication through the Oracle Identity Manager relational database	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
ADAuthenticationProvider	Provider that performs LDAP authentication	1.0

The 'ADAuthenticationProvider' row is highlighted with a red box. The console also shows a 'Domain Structure' tree on the left and a 'System Status' section at the bottom left indicating 4 OK servers.

Click on the Authentication provider to access its corresponding settings and Navigate to provider specific. In order for FileCloud LDAP to be able to pull all the need attributes add the following ObjectClass string under All User Filter.

`(&(objectClass=user)(cn=^NAME^))`

Once done you will need to fill out all other required fields based on your Active Directory configuration.

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for ADAuthenticationProvider" and is divided into "Configuration" and "Performance" tabs. The "Provider Specific" sub-tab is selected and highlighted with a red box. Below this, there is a "Save" button and a descriptive text: "Use this page to define the provider specific configuration for this Active Directory Authentication provider."

The configuration is organized into sections:

- Connection:**
 - Host:** 10.0.7.23 (The host name or IP address of the LDAP server. [More Info...](#))
 - Port:** 389 (The port number on which the LDAP server is listening. [More Info...](#))
 - Principal:** CN=admin.DC=filecloudserv (The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. [More Info...](#))
 - Credential:** [Redacted] (The credential (usually a password) used to connect to the LDAP server. [More Info...](#))
 - Confirm Credential:** [Redacted]
 - SSLEnabled** (Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#))
- Users:**
 - User Base DN:** dc=filecloudserver,dc=us (The base distinguished name (DN) of the tree in the LDAP directory that contains users. [More Info...](#))
 - All Users Filter:** (&(objectClass=user)(cn=^N) (If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. [More Info...](#))
 - User From Name Filter:** [Empty] (If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. [More Info...](#))
 - User Search Scope:** subtree (Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. [More Info...](#))
 - User Name Attribute:** cn (The attribute of an LDAP user object that specifies the name of the user. [More Info...](#))
 - User Object Class:** user (The LDAP object class that stores users. [More Info...](#))
 - Use Retrieved User Name as Principal** (Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. [More Info...](#))
- Groups:** [Empty]

On the left side of the console, there are several utility panels: "Change Center", "Domain Structure", "How do I...", "System Status", and "Health of Running Servers".

Once you have added the needed ObjectClass attribute on WebLogic Server realm provider's configuration, You will need to access FileCloud's Admin portal.

Within FileCloud's Admin portal go to Settings> Authentication and select LDAP from the Authentication type drop-down. To successfully configure LDAP please reference to the following [LINK](#). To ensure a successful connection under LDAP user filter template ensure to add the following:

`(&(objectClass=user)(cn=^NAME^))`

HOME

[Dashboard](#)

USERS/GROUPS

[Users](#)

[Groups](#)

[Admins](#)

MANAGE

[Team Folders](#)

[Network Folders](#)

[User Shares](#)

[Folder Permissions](#)

DEVICES

[Devices](#)

GOVERNANCE

[Dashboard](#)

[Retention](#)

MISC.

[Audit](#)

[Alerts 1](#)

[User Locks](#)

[Workflows](#)

[Reports](#)

[Federated Search](#)

[Metadata](#)

SETTINGS

[Settings](#)

CUSTOMIZATION

[Customization](#)

SYSTEM

[Checks](#)

[Upgrade](#)

Manage Settings

Server
Storage
Authentication
Admin
Database
Email
Endpoint Backup
License

Authentication Settings

Authentication Type LDAP

Specify the Authentication Type

DEFAULT
Active Directory
LDAP

LDAP Settings

Check LDAP Test LDAP Test

LDAP Host ldap://10.0.7.23

Specify the LDAP Host Name

LDAP Port 389

Specify the LDAP Port Number

LDAP Account Name admin

Specify a valid account to use to query LDAP server

LDAP Account Password ●●●●●●●●

Specify account password to use to query LDAP server

LDAP User DN Template CN=^NAME^,OU=filecloud-users,DC=filecloudserver,DC=us

Specify the LDAP User DN Template

LDAP Search DN OU=filecloud-users,DC=filecloudserver,DC=us

Specify the LDAP Search DN

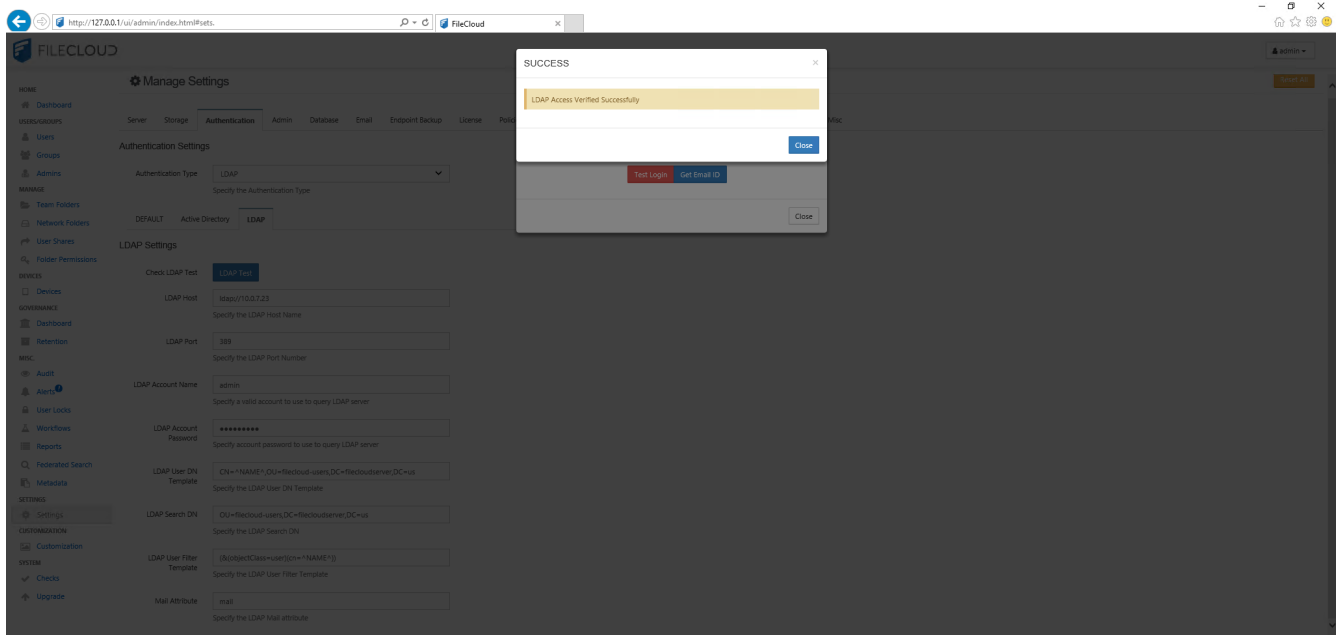
LDAP User Filter Template (&(objectClass=user)(cn=^NAME^))

Specify the LDAP User Filter Template

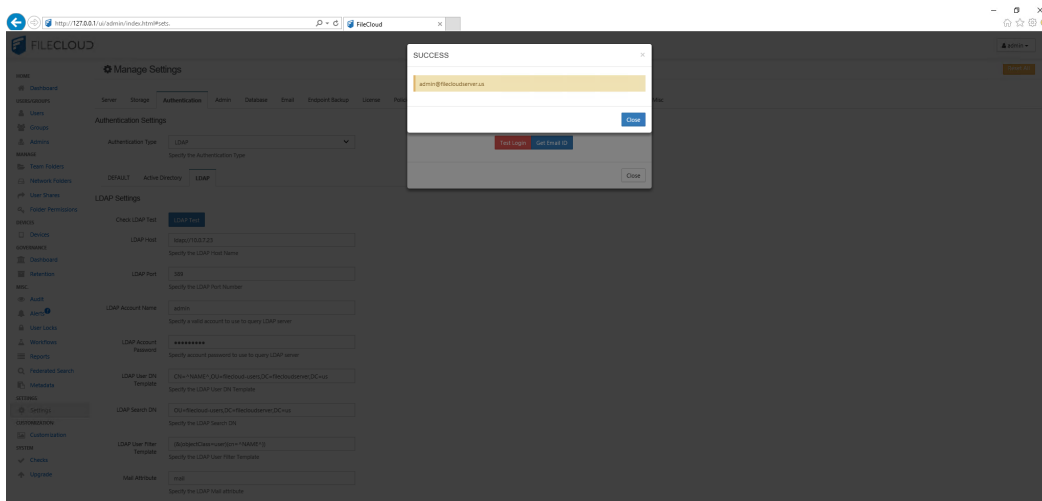
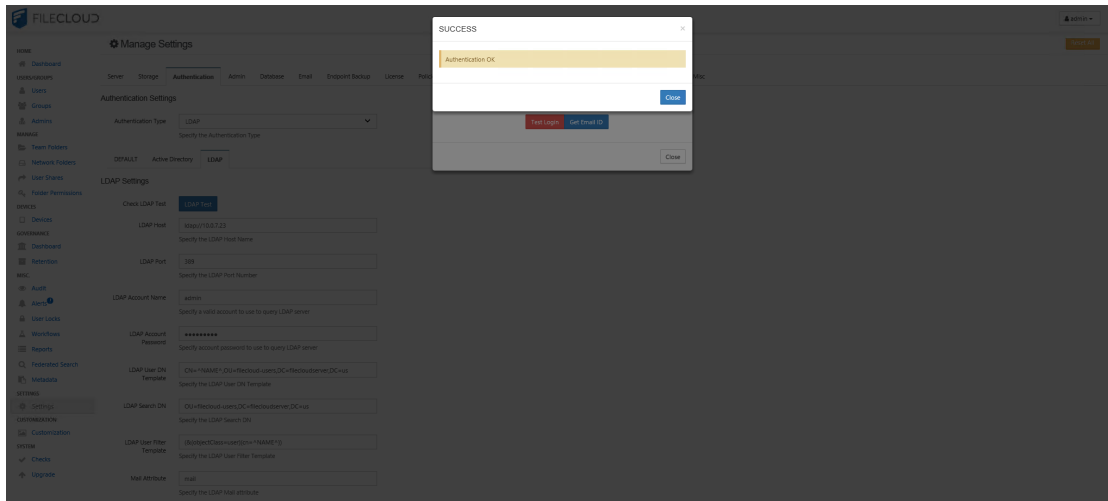
Mail Attribute mail

Specify the LDAP Mail attribute

Upon adding all the needed information you can verify your connectivity to OIM's LDAP by clicking on "LDAP TEST" and Click on Validate LDAP Settings.



If you obtain a successful confirmation message proceed on verifying if 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 admin portal, go to **Settings > Policies**.
2. On the **Manage Setting** screen, select the **Policies** tab.
3. Open a policy for edit.

4. In the **User Policy** tab, set **Enable code based device authentication** to **YES**.

✕
Policy Settings - Global Default Policy

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

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

Enable code based device authentication

YES
▼

Enable code based device authentication

Require Admin Approval for Device Authentication

NO
▼

Require admin approval for code based device authentication

Enforce Session Timeout for Devices

NO
▼

Device timeout is enforced. Users must log in again after session expires.

Save
Reset All

✕ Close

Now, when a user logs in to a client app, an approval request appears 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**.

Sync for FileCloud

1 LOGIN 2 CLOUD STORAGE 3 NETWORK FOLDERS 4 BACKUP FOLDERS 5 FINISH

Log in

Please enter your credentials. When you sign in to your account, your FileCloud Sync settings will automatically be configured.

Login Method Password SSO **Device Authentication Code**

Server URL

Account

Proxy Settings

The following dialog box opens.

Enter Device Code

User needs to approve and submit device code:

Enter Code

[Open Website](#)

2. To get the device authorization code:
 - a. The user logs in to the user portal, then clicks the arrow next to 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**.

General		Devices		
Refresh				
Device Name	Device Details	Last Login	Device Status	Actions
Cloud Sync (DESKTOP-N71N3EH)	OS: Windows 8 6.2 (Build 9200), App: 20.2.0.4954	November 19th 2020 11:29AM	Needs Approval ✓	
MS Outlook (DESKTOP-N71N3EH)	OS: Windows Microsoft Windows NT 10.0.18363.0, App: 15.1.2.3	October 8th 2020 2:08PM	Approved	
FileCloud Drive (DESKTOP-N71N3EH)	OS: Windows 8 6.2 (Build 9200), App: 20.2.0.4723	October 8th 2020 1:46PM	Approved	

- A dialog box pops up with the **Device Authorization Code**:

Device Approved for Use ✕

Device Authorization Code:

2 C W D H J

Please enter the above authorization code in your device to login.

[Close](#)

3. The user copies the **Device Authorization Code** and pastes it into the **Enter Device Code** dialog box, then clicks **Submit** to log in.

Enter Device Code ✕

User needs to approve and submit device code:

Enter Code

[Open Website](#)

[Submit](#)

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 admin portal, go to **Settings > Policies**.
2. On the Manage Setting screen, select the **Policies** tab.
3. Open a policy for edit.
4. In the **User Policy** tab, set **Enable code based device authentication** to **YES**.
The **Require Admin Approval for Device Authentication** setting becomes enabled.
5. Set **Require Admin Approval for Device Authentication** to **YES**.

Policy Settings - Global Default Policy

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

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

Enable code based device authentication
YES

Enable code based device authentication

Require Admin Approval for Device Authentication
YES

Require admin approval for code based device authentication

Enforce Session Timeout for Devices
NO

Device timeout is enforced. Users must log in again after session expires.

Save Reset All Close

To approve a client device that has been sent to you for admin approval

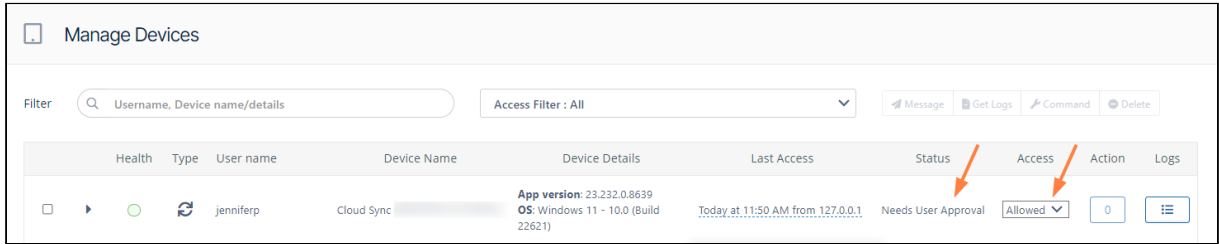
1. Go to **Device Management** in the admin portal to view the listing for the device approval.
The device is listed with **Status** showing **Needs Admin Approval** and **Access** set to **Blocked**.

Manage Devices

Filter: Username, Device name/details Access Filter: All

Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
🟢		jenniferp	Cloud Sync	App version: 23.232.0.8639 OS: Windows 11 - 10.0 (Build 22621)	Today at 11:44 AM from 127.0.0.1	Needs Admin Approval	Blocked	1	

- 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.



The screenshot shows the 'Manage Devices' interface. At the top, there is a search filter for 'Username, Device name/details' and an 'Access Filter' dropdown set to 'All'. Below the filter are buttons for 'Message', 'Get Logs', 'Command', and 'Delete'. The main area is a table with columns: Health, Type, User name, Device Name, Device Details, Last Access, Status, Access, Action, and Logs. A single device is listed with the following details:

Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
<input type="checkbox"/>		jenniferp	Cloud Sync	App version: 23.232.0.8639 OS: Windows 11 - 10.0 (Build 22621)	Today at 11:50 AM from 127.0.0.1	Needs User Approval	Allowed	0	

Two orange arrows point to the 'Needs User Approval' status and the 'Allowed' dropdown in the 'Access' column.

Document Settings

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

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

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

- [Enabling Watermarks On Previews](#)
- [Import Files : Pre-seeding](#)
- [Optimize PDF Preview](#)
- [Managing File Extensions](#)
- [Restricting File Names](#)
- [Manage File Versioning](#)
- [Configuring Zip Files and Zero Trust File Sharing](#)

Enabling Watermarks On Previews

Administrators can add watermarks to all previews generated in FileCloud.



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 watermark on a document preview in the Admin and User Portals.

DESCRIPTION	QUANTITY	UNIT PRICE	SUBTOTAL
[Blurred Description]	1	[Blurred Unit Price]	[Blurred Subtotal]
		SUBTOTAL	: [Blurred Subtotal]
		TAX	: [Blurred Tax]
		TOTAL	: [Blurred Total]
TERMS:			
<ul style="list-style-type: none"> This is a computer generated invoice and does not require signature. 			
THANK YOU FOR YOUR PURCHASE.			

13 Watermark on document preview**To display watermarks for previews:**

1. Open a browser and log in to the **Admin Portal**.
2. From the left navigation pane, click **Settings**.
3. On the **Manage Settings** screen, select the **Misc.** tab
4. Select the **Preview** sub-tab.
5. Next to **Anonymous Access Watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by anonymous users.
6. Next to **Authorized Access Watermark**, type in the text, including any of the parameters listed below, that you want embedded on previews by authorized users.

Available parameters:

^USERNAME^ - The user who is viewing this file.

^SHARE_OWNER^ - The user who shared this file.

^FILE_OWNER^ - The file owner.

^OWNER^ - If this is a shared file, the user who shared this file. If this is not a shared file, the file owner.

^DATETIME^ - Date and time of preview.

^GEOIP_LOCATION^ - Geographic location of IP performing preview.

^LICENSED_COMPANY^ - The company listed on the current license.

Server Storage Authentication Admin Email Endpoint Backup License Policies SSO

General User Password Notifications Share **Preview** DUO Security Privacy 2FA

Quick JS Preview

Document Preview Support

Anonymous Access Watermark

Viewed by ^USERNAME^ at ^DATETIME^

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

Authorized Access Watermark

Viewed by ^USERNAME^ at ^DATETIME^ at ^LICENSED_COMPANY^


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

Now whenever a user previews a document, they will see the watermark for anonymous or authorized access embedded in the preview.

DESCRIPTION	QUANTITY	UNIT PRICE	SUBTOTAL
	1		
		SUBTOTAL	:
		TAX	:
		TOTAL	:
TERMS:			
<ul style="list-style-type: none"> This is a computer generated invoice and does not require signature. 			
THANK YOU FOR YOUR PURCHASE.			

14 Preview doc showing watermark

Import Files : Pre-seeding

 The option to import or pre-seed user files into the system is available in FileCloud version 15 and later.

Administrators can import files to managed storage configuration to prepare FileCloud for users.

NOTES:

- During the seeding operation, the system is operating under a special mode and user access must not be allowed (though it is not prevented automatically).
- Therefore, ideally, seeding should be done during initial system setup.

[Show me where the option is...](#)

Go to **Settings > Misc > General**,

The screenshot shows the FileCloud settings interface. On the left is a navigation menu with sections: GOVERNANCE (Dashboard, Retention, Smart DLP, Smart Classification, Compliance Center), MISC. (Audit, Alert, User Locks, Workflows, Reports, Federated Search, Metadata), and SETTINGS (Settings). An orange arrow points to the 'Settings' option in the SETTINGS section. The main content area shows a breadcrumb trail: Server > Storage > Authentication > Admin > Email > Endpoint Backup > License. Below this, there are tabs for Team Folders, Third Party Integrations, Misc (highlighted with an orange arrow), and Reset. Under the Misc tab, there are sub-tabs: General (highlighted with an orange arrow), User, Password, Notifications, Share, Preview, and DUO Security. Below the sub-tabs, there are links for Privacy and 2FA. The main content area is titled 'General System Settings' and contains several configuration options: Server Timezone (America/Chicago), Calendar Type (Gregorian (English)), Date Format (MMM dd, yyyy (Jan 15, 2019)), Time Format (h:mm A (2:20 PM)), and Default Web UI Version to show.

and scroll down to the **Import** button:

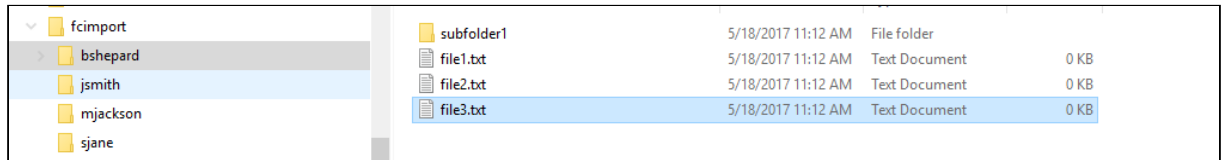
The screenshot shows the FileCloud settings interface, specifically the 'Import Files' section. The left navigation menu is visible, showing the 'Settings' option. The main content area shows a checkbox for 'Is hosted behind a proxy server?'. Below this is the 'Scheduled Tasks' section with a blue 'Run' button and the text 'Manually execute scheduled tasks which are normally run using cron'. The 'Import Files' section has a blue 'Import' button (highlighted with an orange arrow) and the text 'Import files into managed storage'. Below this is the 'Allowed File Extensions' section with a text input field and the text 'Specify file extensions that will be allowed for uploading (only files of those extensions)'.

Import Files into Local Managed Storage

Prerequisite:

In order for the data to be imported, the following conditions must be met

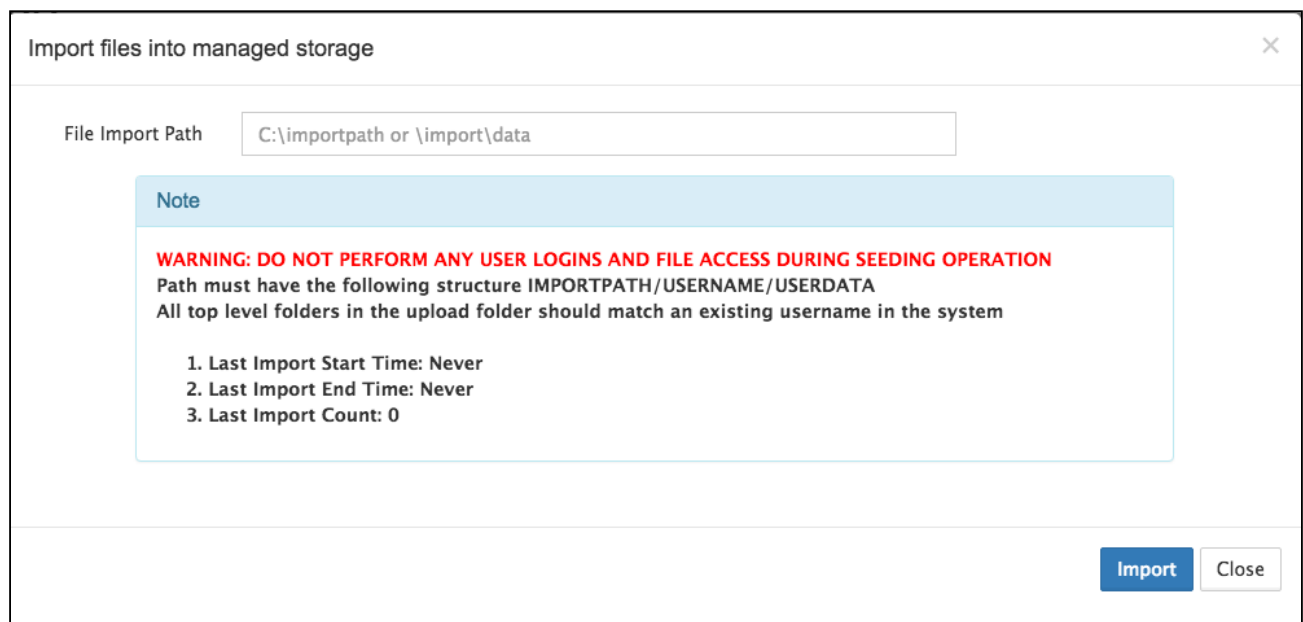
1. The data must be in locally accessible disk. Ideally, the data must reside in the same drive as the managed storage (say, Managed storage is in C:\fileclouddata, then the import data must also be in C: drive)
2. The data must be in following structure. <ImportPath><users><data>. For example, if you have four users, say, bshepard, jsmith, mjackson, sjane, then the structure should be as shown below



3. The users must already be created in the system (bshepard, jsmith, mjackson, sjane must already be a valid full user in the system)
4. The users must have enough quota assigned to allow the data import

To import files into local managed storage:


1. Open a browser and log in to the *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, click *Settings*.
3. On the *Manage Settings* window, click the *Misc.* tab, and then the *General* sub-tab.
4. On the *General* screen, next to *Import Files*, click the *Import* button.
5. On the *Import files into managed storage* dialog, in *File Import Path*, type the location to the files you want to import.
6. Click *Import*.



Optimize PDF Preview

Administrators can configure FileCloud to show a preview of PDF files directly in the User Portal without forcing a user to download the file first.

This is configured when you [Set Up Document Preview](#).

 If you choose to allow previews of PDF files, you should be aware of what the user's experience will be on the User Portal.

In some cases, viewing PDF files can take more time than expected.

The time it takes to generate a preview of a PDF depends on the how the file is created.

In general, a PDF can be categorized in to two main types:

- Native (quicker)
- Scanned (slower)

Why is a Native PDF quicker to preview?

Native

Information is saved as text when you save a file as PDF if you have created the file from the following sources:


- A word processing program such as Microsoft Word, Excel or PowerPoint
- A browser page printed to PDF
- A file saved directly from PDF generation software such as Nitro PDF, Adobe PDF, etc.

When information is saved as text, searching, copying, and other text-based operations on the PDF are quicker.

 It also takes less time to generate a preview of a native PDF file than a scanned PDF file.

Scanned

When PDFs are created from scanning, there is no information about the content because the PDF file just serves as a container of images.

 While this format is useful when the objective is to showcase graphics material, the rendering of this file can take a long time.

When a scanned PDF needs to be previewed in FileCloud:

1. The client's User Portal needs to check the entire PDF embedded text to allow search, copy or any other text based operations.
2. This text processing operation is done at the moment when the client's User Portal requests a preview.
3. The processing on the client-side portal can make the preview loading slow for general use.

If you have a scanned PDF file that has been created from one of the following sources, your best option is to convert the file to native PDF before uploading it to FileCloud:

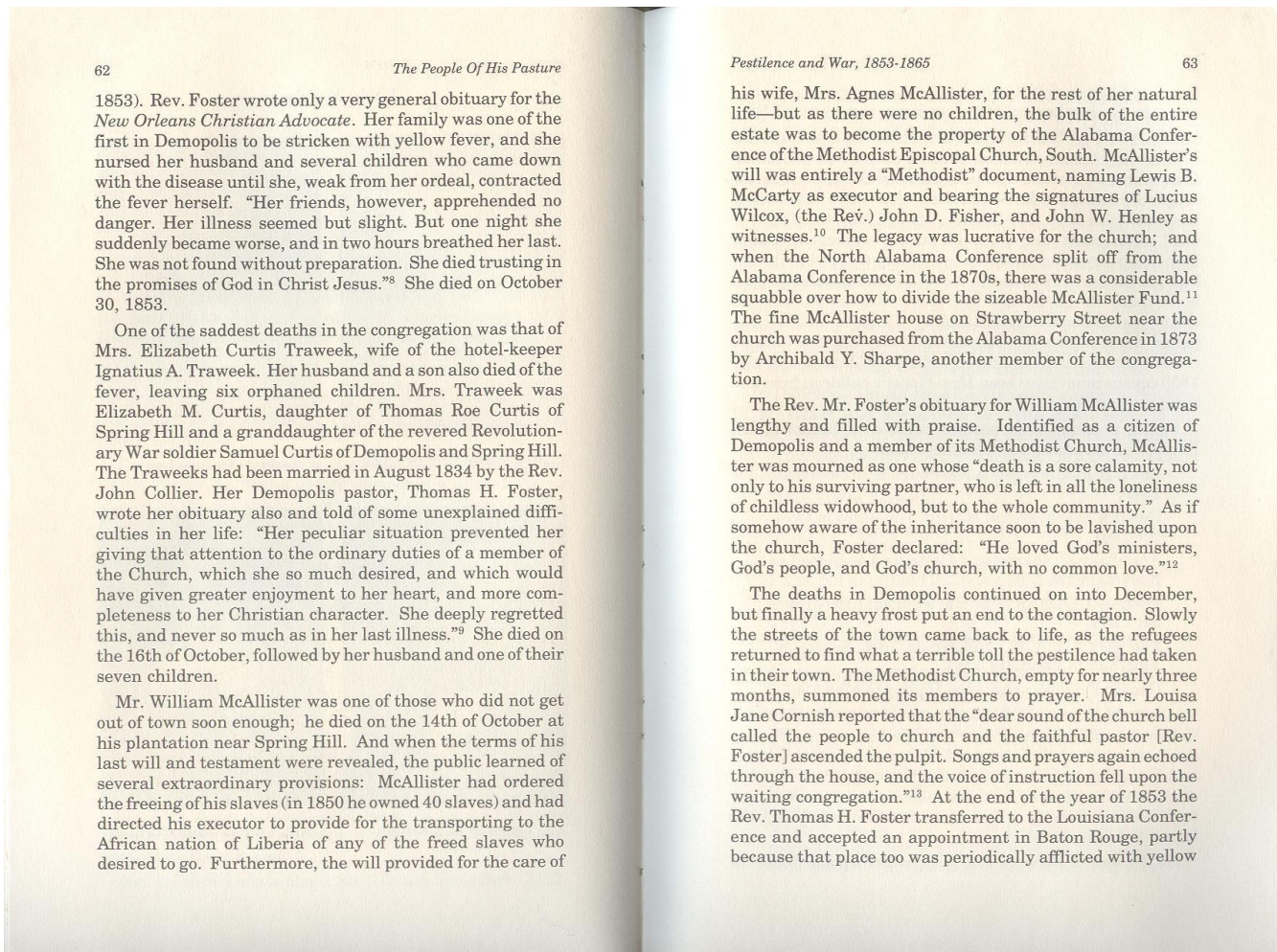
- Legal documents
- Insurance patient documents
- Blueprints and manuals

Optimizing files in this way allows a file to be opened with less processing time and generates a preview quicker.

How Do I Convert a Scanned PDF to Native?

There are several tools in the market you can use to convert scanned PDF files to native PDF files (OCR reading).

For example, if you have a scanned image similar to the following, you should convert it Native PDF:

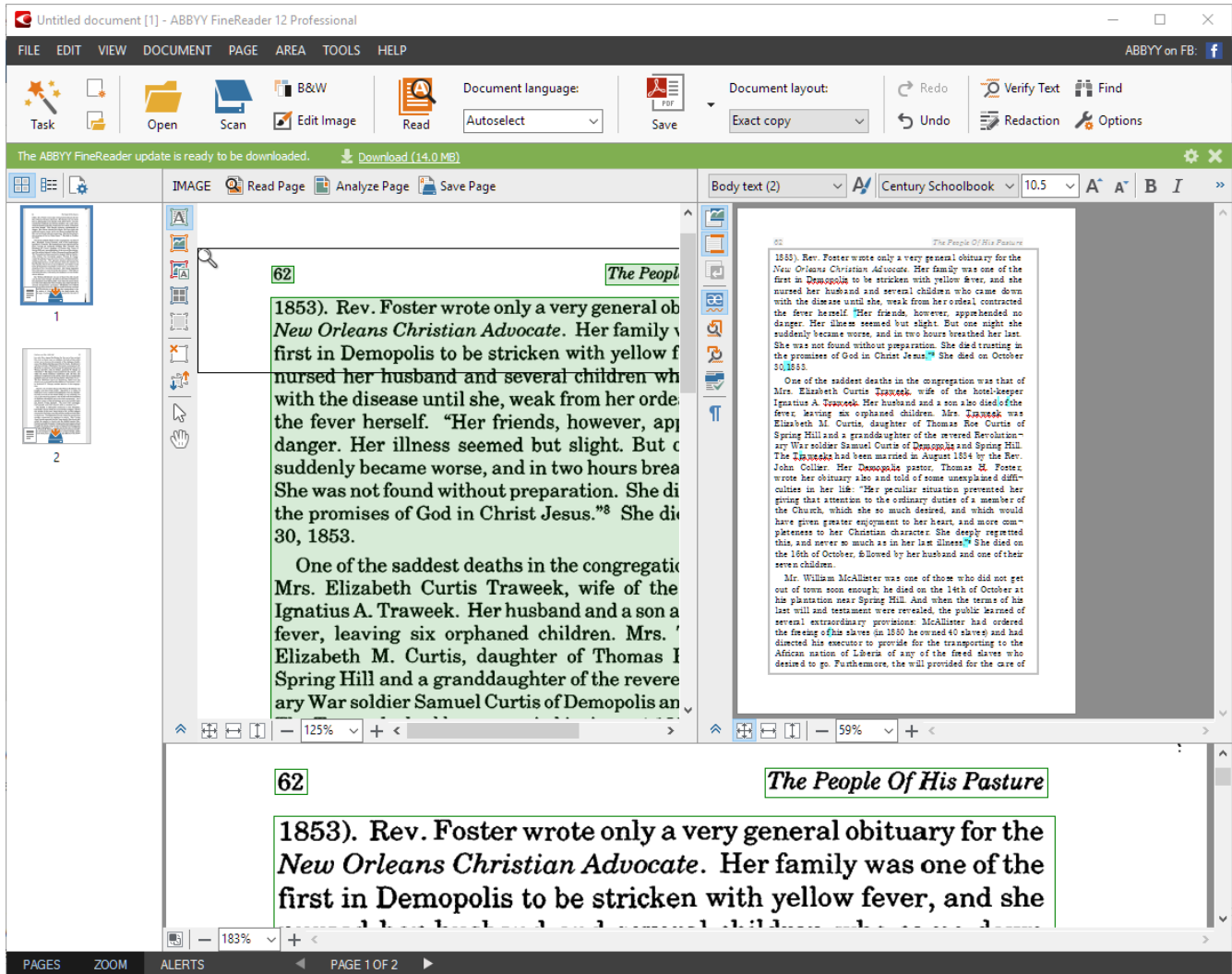


In our example:

- this file is scanned and saved as a PDF named *Scanned_PDF.pdf*
- If we use this file as it is, the FileCloud Preview will take a longer than expected time to render this on the User Portal

For test purposes, CodeLathe has tested and recommends the following tool to optimize PDF files for generating a preview:

- ABBYY produces [FineReader](#), an all-in-one OCR and PDF software application for increasing business productivity when working with documents.
- Using ABBYY Fine Reader software, you can open and convert this PDF file to a Native PDF file.



The use of ABBYY FineReader was used for explanation purposes only. Any other tool that can read a PDF file can be used to optimize the PDF files for web viewing.

Managing File Extensions

- You can prevent specific file extensions from being uploaded in FileCloud 10.0 and later.
- Existing files cannot be renamed to use a restricted file extension in FileCloud 17.3 and later.
- You can create a list of only the file extensions you want to allow to be uploaded in FileCloud 19.1 and later.

⚠ Prior to FileCloud Version 21.2, **Disallowed File Extensions** listed **php** and **php5** by default; from Version 21.2 on, it lists **php**, **php5**, **phar**, and **phtml**. If you are using a version of FileCloud earlier than 21.2, you are advised to add **phar** and **phtml** to the **Disallowed File** list. See [Advisory 2021-09 Upload of Potentially Unsafe File Types](#) for more information.

For security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud.

- You can either create a list of file extensions to restrict, or create a list of file extensions to allow.
- If you create an Allowed list of file extensions, then any settings in the Disallowed list will be ignored.
- These restrictions help to prevent users from uploading malicious attachments and viewing them.
- By default FileCloud restricts users from uploading any files with **php** extensions. This is to prevent any code injection.

Allowed File Extensions	<input type="text"/> Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use ' ' as the delimiter.
Disallowed File Extensions	<input type="text" value="php php5 phar phtml"/> Specify file extensions that will be prevented from uploading. Use ' ' as the delimiter.

Which list should I use? The Allowed or Disallowed?

- If you know which file types you don't want to allow and this list is short, you can use the **Disallowed** setting.
- If you want to allow only a few file types to be uploaded, you can use the **Allowed** setting.
- If you create an Allowed list of file extensions, then any settings in the Disallowed list will be ignored.

What Do You Want to Do?

Allow File Extensions

- ⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.
- An empty space is defined as a delimiter character followed by no value.

Examples	Description	Impact on Uploading Files
<code>png jpg </code>	Allow files to be uploaded with an extension of: <ul style="list-style-type: none"> png jpg <i>empty</i> 	Only the following files can be uploaded by users: <ul style="list-style-type: none"> Portable Network Graphics Joint Photographic Experts Group Any file without an extension (for example, a file named <i>config</i>)
<code>png jpg</code>	Allow files to be uploaded with an extension of: <ul style="list-style-type: none"> png jpg 	Only the following files can be uploaded by users: <ul style="list-style-type: none"> Portable Network Graphics Joint Photographic Experts Group

FileCloud Version	Method	Instructions	Notes
19.1	Admin Portal	<p>To manage extension in the Admin Portal:</p> <ol style="list-style-type: none"> Log into <i>Admin Portal</i>. From the left navigation panel, select Settings. On the Settings screen, select the Misc. tab, and then the General tab. Scroll down until you see the <i>Allowed File Extensions</i> box. In the <i>Allowed File Extensions</i> box, specify the allowed extensions, using the " " character to separate each extension. 	<p>⚠ If you add extensions to the Allowed File Extensions list, then any extensions in the Disallowed File Extension list will be ignored.</p> <p>⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.</p> <div data-bbox="857 1108 1461 1201" style="border: 1px solid black; padding: 5px;"> <p>Allowed File Extensions</p> <p>Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use ' ' as the delimiter.</p> </div> <p>This list of extensions must use the following character as the delimiter:</p> <ul style="list-style-type: none"> " " For example, to restrict the mp4 and mp3 extensions: mp4 mp3

Disallow File Extensions

To manage extensions in the Admin Portal:

- Log into Admin Portal.
- From the left navigation panel, select **Settings**.
- On the Settings screen, select the Misc. tab, and then the General tab.**
- Scroll down until you see the **Disallowed File Extensions** box.
- 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.

Disallowed File Extensions	<input type="text" value="php php5 phar phtml"/> <p>Specify file extensions that will be prevented from uploading. Use ' ' as the delimiter.</p>
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------

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 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. Log into Admin Portal.
2. From the left navigation panel, select **Settings**.
3. **On the Settings screen, select the Misc. tab, and then the General tab.**
4. Scroll down until you see the **Disallowed File Extensions** box.
5. In the **Disallowed File Extensions** box, specify the restricted extensions.

Disallowed File Extensions	<input type="text" value="php php5 phar phtml"/> <p>Specify file extensions that will be prevented from uploading. Use ' ' as the delimiter.</p>
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------

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

i You can create a list of file names that cannot be uploaded by users in FileCloud 19.1 and later.

For security reasons you may want to create a set of rules for the working environment where many users have access to a central resource, such as files and folders in FileCloud Server.

To restrict names of files that can be uploaded:

1. In the admin portal, go to **Settings > Misc > General**.
2. Add the file names to the **Disallowed File Names** field.
Separate multiple names with |.


Disallowed File Names

attack | threat.exe


Specify file names that will be prevented from uploading. Use '|' as the delimiter.



Files matching or including any term entered are not uploaded. If you do not specify an extension, files matching or including the term and any extension are not uploaded.

To understand how to create a list of file names, use the examples below.

-  **! If you leave an empty space in your list:**

 - In the User Portal, all files will be blocked from being uploaded.
 - In the Sync client, it will ignore checking for restricted names.

 If you add an extension to the file name, then only the combination of name + extension will be restricted.

-   To manage file extensions ONLY, you can either create a list of file extensions to restrict, or create a list of file extensions to allow. See [Manage File Extensions](#) for instructions.

Example	Description	Impact on Uploading Files
<div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> attack threat.exe </div>	Restrict any file from being uploaded if it contains any of the 3 strings in the file name: <ul style="list-style-type: none"> • attack • threat.exe • <i>empty</i> 	The following files cannot be uploaded by users: <ul style="list-style-type: none"> • *attack*.* • *threat.exe • Any file The following files can be uploaded by users: <ul style="list-style-type: none"> • No files can be uploaded until the <i>empty delimiter</i> is removed.

Example	Description	Impact on Uploading Files
<div style="border: 1px solid gray; padding: 5px; width: fit-content;"> attack threat.exe </div>	Restrict any file from being uploaded if it contains any of the 2 strings in the file name: <ul style="list-style-type: none"> • attack • threat.exe 	The following files cannot be uploaded by users: <ul style="list-style-type: none"> • *attack*.* • *threat.exe The following files can be uploaded by users: <ul style="list-style-type: none"> • Any file not containing <i>attack</i> • Any file not containing <i>threat.exe</i> • threat.* (<i>where * is NOT .exe</i>)

Manage File Versioning

You can allow a user to upload changes to a file and create another version of a file. This is called file versioning.

- This allows users to have an older version of the file on the site
- Users can download a previous version
- Users can remove previous versions to save space

How do I know if there are previous versions of a file?



Look for the Versions icon



Manage files for me ✕

/me ☰ ☆ 🗑️

← Up
🗑️ Deleted Files
📄 Copy
📁 Move
🗑️ Delete

		Name	Size	Modified	Actions
<input type="checkbox"/>	📁	Sub1		Sep 18, 2018 10:13 AM	📄 📁 ⚙️
<input type="checkbox"/>	📁	backups		Oct 26, 2018 11:13 AM	📄 📁 ⚙️
<input type="checkbox"/>	📄	059c1770e5e39c50d5efa5ced3b913d2--writing-process-writing-tips.jpg	107 KB	Jul 25, 2018 2:39 PM	📄 📁 ☰



If file versioning is causing issues, you can turn it off.

- File versioning can cause loss of data when a user accidentally overwrites a file with the same name

- Users may be storing too many unnecessary versions of a file and are taking up too much space

When you configure file versioning, you can use the following values:

Option	Setting	Result
<i>Number of old versions to keep for each file</i>	-1	The user tries to upload another version but the upload will FAIL
<i>Number of old versions to keep for each file</i>	any number greater than 0	When the user uploads a new version of a file, it is saved, and the latest <Number of old versions to keep for each file> versions are kept.

To manage file versioning:

1. Open a browser and log on to the *Admin Portal*.
2. From the left navigation menu, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, select the *Storage* tab, and then the *My Files* sub-tab.
4. On the *My Files* sub-tab, in *Number of old versions to keep for each file* type in -1 to turn versioning off or any number greater than 0 to use versioning.
5. To save your changes, click *Save*.

Configuring Zip Files and Zero Trust File Sharing

i Functionality for creating and working with content in zip files in My Files is available beginning with FileCloud 22.1. Functionality for creating and working with content in zip files in Network Shares is available beginning with FileCloud 23.232.

Users can create and upload zip files into their My Files and Network Shares folders, and then preview, download, add, and delete contents of these zip files.

When users create Zip files within FileCloud, they may add a password to them to create them as encrypted Zero Trust folders. The password (decryption key) must be entered by the user who created the zip file or anyone they share the file with to access it. Note that the decryption key is not stored in FileCloud or known by the FileCloud system, and therefore makes the file invulnerable to attacks where the system is compromised.

For information about how users add and work with zip files, see [Working with Zip Files](#).

By default, after the password is entered the first time during a log-in session, it does not have to be entered again during that session, but a setting in policies enables you to require users to enter the password each time they access it during a session.


To enable the zip file feature

By default, the zip file feature described above is disabled. Please [Contact FileCloud Support](#) to enable it.

Zip File Settings

The following are default settings for zip files.

Setting	Default value
Encryption method	WinZip AES-256
Compression level	Normal
Compression method	Deflated
Fallback character set	None
Max zip file size	100 MB

 WinZip AES-256 encryption is not supported 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 admin portal, go to **Settings > Policies**, and open the policy you want to change.

2. Click the **User Policy** tab:

Policy Settings - Global Default Policy

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

General 2FA **User Policy** Client Application Policy Device Configuration Notifications

User Policy

Disable Invitations to New Users
NO

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

Create account on new user shares
YES

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

Enable code based device authentication

Save Reset Close

3. Scroll down to the bottom of the tab.
By default **Save Zip File Session Password** is set to **Yes**. This enables users to enter the password once per login session to access the contents of the zip file.
4. Change the value of **Save Zip File Session Password** to **No**.

Policy Settings - Global Default Policy

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

NO

Enables/disables mandatory workflow automation for shares

Max. File Size Limit ⓘ

Units 0 MB

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

Save Zip File Session Password
NO

Allow passwords to be saved inside encrypted zip files. Warning: Disabling the setting will require a password every time you access a file.

Save Reset Close

5. Click **Save**.
Now users must enter the password each time they access the contents of the zip file.

Permissions in shared zip files

When a zip file is shared publicly, share users can view the contents of the zip file and download them. When a zip file is shared privately, the operations that share users can perform on its contents depends on their share permissions.

The following table shows what each share permission allows share users to do with the contents of a zip file

Permission	Description
View	Preview files and open folders in the zip file.
Download	Download files in the zip file and save them. Downloading folders in the zip file is not permitted.
Upload	Upload files into the zip file and delete files in the zip file.
Share	Share the zip file. Sharing of files and folders inside the zip file is not permitted.

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](#)
- [Set the Global Share Mode](#)
- [Specify Sharing Expiration](#)
- [Secure Shares](#)
 - [User Account Search Mode](#)
 - [User Account-Type Search Mode](#)

Configure Sharing Defaults

 In the User Portal, a user can click on the root folder, *My Files*, and select *Share*. This is a security threat and should not be allowed.

In FileCloud Server version 19.1 and later:

- in the User Portal, when a user clicks on the root folder, My Files, they no longer have the Sharing option.

When a user wants to share a file or folder, administrators can decide which options should be automatically selected.

These settings are really just a recommendation and can be changed by the user, unless you disable the ability to change the defaults.

Default Share Type

Setting this option tells FileCloud Server what type of share to automatically select when a user shares a file or folder.

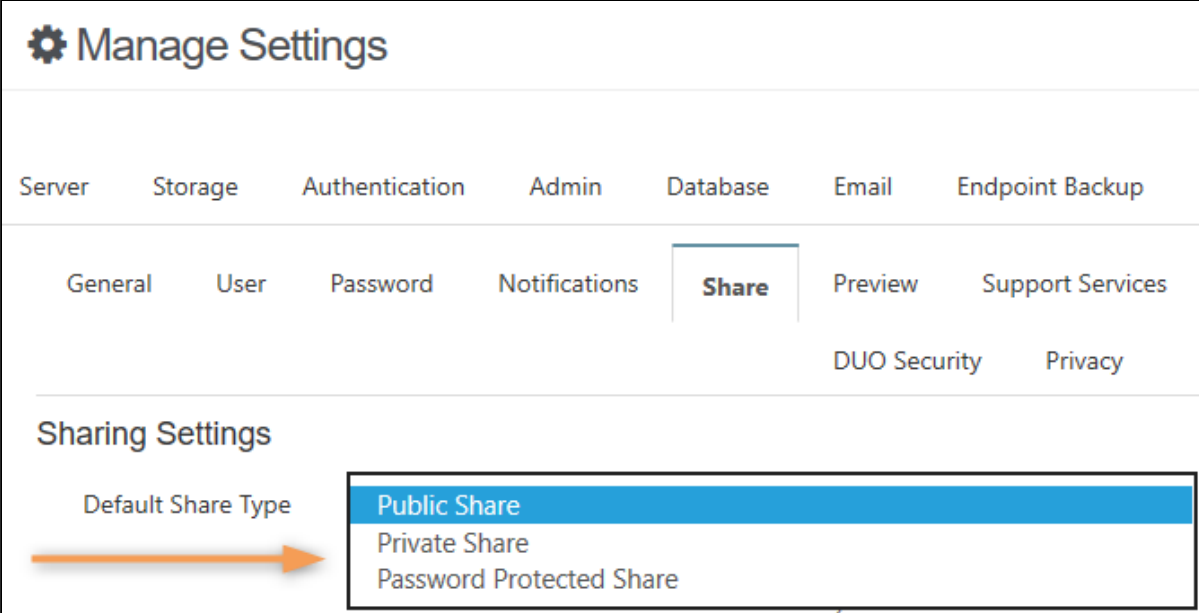
- Applicable only when *Global Share Mode* is set to **Allow All Shares**
- This type can be changed by the user unless *Disallow Default Share Settings Change* is set.

Public Share	<p>Allows users to share with anyone who has the link to the share.</p> <ul style="list-style-type: none"> • 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	<p>Allows users to share with anyone who has the link and can log in to a FileCloud account.</p> <ul style="list-style-type: none"> • 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	<p>Forces users to create a password when sharing a file or folder.</p> <ul style="list-style-type: none"> • Recipients of the share are given the password when they receive the link to the share. • The share can be public or private.

To set the Default Share Type:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Under *Sharing Settings*, in *Default Share Type*, select the option you want to use.



The screenshot shows the 'Manage Settings' interface. At the top, there is a gear icon and the text 'Manage Settings'. Below this is a horizontal navigation bar with tabs: Server, Storage, Authentication, Admin, Database, Email, and Endpoint Backup. Underneath, there is another set of tabs: General, User, Password, Notifications, Share (which is highlighted with a blue border), Preview, and Support Services. Below these are two more tabs: DUO Security and Privacy. The main content area is titled 'Sharing Settings'. Under this title, there is a label 'Default Share Type' with an orange arrow pointing to a dropdown menu. The dropdown menu is open and shows three options: 'Public Share' (highlighted in blue), 'Private Share', and 'Password Protected Share'.

5. Click *Save*.

> Set Expiration Days Default

Administrators can allow users to share files and folders for as long as they exist, or you can set a suggested number of days that a share remains active by default.

- Using a value of **0** means that unless changed by a user, shares do not expire.
- This setting can be changed by the user unless **Disallow Default Share Settings Change** is set in the **Settings > Misc > Share** tab.

Default share expiration days can be set for specific Users in a policy.

To set the Share Expiry default in a policy:

1. Open a browser and log in to the Admin Portal.
2. From the left navigation pane, click **Settings**, and then click the **Policies** tab.
3. Across from the policy that you want to edit, click the edit icon.
4. In the **General** tab, scroll down and change the value of the **Default Share Expiry in Days** setting.

Policy Settings - Global Default Policy

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

General | 2FA | User Policy | Client Application Policy | Device Configuration | Notifications

Share mode
Allow All Shares

Set Share Mode

Default Share Expiry in Days
0

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed

Save | Reset All | Close

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 a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Under *Sharing Settings*, in *Default Max Share Upload Size*, select the *Units*, and then type in the file size limit you want to use.

The screenshot shows the 'Manage Settings' interface with the 'Share' sub-tab selected. Under 'Sharing Settings', the 'Default Max Share Upload Size' field is set to '0' with units of 'MB'. An orange arrow points to the 'Units' dropdown menu, which is open and displays the following options: GB, MB, KB, and B. Below this field, there is a checkbox for 'Disallow Default Share Settings Change'.

5. Click *Save*.

Disable Sharing to Groups for Private Share

You can check Disallow sharing to groups for Private shares to hide the Group option when users share a file or folder.

To disable users from sharing to groups:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, click *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Under *Sharing Settings*, check *Disable sharing to groups for Private Share*.

The screenshot shows the 'Share' sub-tab under the 'Misc.' tab in the FileCloud Admin Portal. The 'Sharing Settings' section includes the following options:

- Default Share Type:** Public Share (dropdown menu). Description: Set the default share type when share is created. (Applicable only when Global Share Mode is set to Allow All Shares)
- Default Share Expiry in Days:** 0 (text input). Description: Number of days shares remain active. Value 0 implies the shares do not expire.
- Default Max Share Upload Size:** Units: MB, 0 (text input). Description: Default upload size limit for a shared folder. Can be overridden in folder share settings. Value of 0 indicates that there is no limit.
- Disable sharing to groups for Private Share:** . Description: Disable ability to share to groups for Private Shares.

The 'Disable sharing to groups for Private Share' checkbox is highlighted with a red box.

5. Click **Save**.

Now when the user shares a file or folder, the Manage Share window does not display the Group tab.

Share link for file Preliminary.dwg ✕

Share Link

https://[redacted]/url/mfxyjtrygum6rhnt
Modify Link

📄
🔗
✉
🗑

Shared File
/jennifer/Preliminary.dwg

Share Options

Share History

Share Name: Preliminary.dwg Change

Expires: Never Expires Change

Send Email Notifications: Yes

Allow anyone with link

Allow anyone with link and a password

Allow selected users or groups

Users

Sharing Permissions: 👤 Invite Users ⋮

User	View	Download	Upload	Share	Sync	Delete	Manage
No entries							





Remove Share

OK

Disallow/Allow Default Share Settings Change

The **Share link** dialog box appears with settings that the user can modify:

Share link for file Feature List.xlsx

Share Link
 [Modify Link](#)    

Shared File
/jenniferp/Feature List.xlsx


Share Options | Share History

Share Name: RJsOXjdVpBiMMDWt [Change](#)

Expires: Never Expires [Change](#)

Max number of downloads: No Restrictions

Send Email Notifications: Yes

Sharing Permissions:
 Allow anyone with link
Allow 

Allow anyone with link and a password
 Allow selected users or groups
 Allow Anyone with Secure Web Viewer link and a password

This share is **Public**
Anyone with a link can view.


[Remove Share](#) [OK](#)

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. Go to **Settings > Misc > Share** and check the **Disallow Default Share Settings Change** option:

Sharing Settings

Default Share Type	Public Share	Set the default share type when share is created. (Applicable only when Share Mode is set to Allow All Shares)
Default Share Expiry in Days	0	Number of days shares remain active. Value 0 implies the share never expires.
Default Max Share Upload Size	Units ▾ 0	Default upload size limit for a shared folder. Can be overridden in individual share settings. Value of 0 indicates that there is no limit.
Disable sharing to groups for Private Share	<input type="checkbox"/>	Disable ability to share to groups for Private Shares
Disallow Default Share Settings Change	<input checked="" type="checkbox"/> 	Prevent end user from changing default share settings

AND

2. Go to **Settings > Policies**, and edit the policies of users who you do not want to allow to change share settings.
3. Click the **User Policy** tab.

4. For each policy, change the **Disallow Default Share Settings Change** option to **Yes**.

Policy Settings - User Group Management ✕

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

Allow Folder Level Security	NO
Enable Web Edit Feature	YES
Enable Recyclebin Clear Feature	YES
Disallow Default Share Settings Change	YES

Save Reset Close

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:

Share link for file Feature List.xlsx

Share settings cannot be changed. Users and groups can be invited. For more information contact your administrator.

Share Link

http://127.0.0.1/url/umgaxuunx4mqwikf

Shared File

/jenniferp/Feature List.xlsx

Share Options Share History

Share Name:	fJ2Y6Batbg2GzieY
Expires:	Never Expires Change
Max number of downloads:	No Restrictions
Send Email Notifications:	Yes
Sharing Permissions:	

This share is **Public**
Anyone with a link can view.

Allow Anyone with Secure Web Viewer link and a password

OK

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. Go to **Settings > Policies**, and edit the policy.
2. Click the **User Policy** tab.

3. Change the **Disable Everyone Group sharing** option to **Yes**, and click **Save**.

Policy Settings - User Group Management

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

Enable Web Edit Feature	YES	Allow users to edit documents from a browser session.
Enable Recyclebin Clear Feature	YES	Allow users to clear recyclebins.
Disallow Default Share Settings Change	YES	Do not allow users to change settings of existing shares and default settings of new shares.
Disable Everyone Group sharing	YES	Disable everyone group sharing

Save Reset Close

Now, when users select a group to share with, the **Everyone** group does not appear.

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 Global Share Mode

FileCloud allows administrators to manage file shares created by their users at a global level.

- You can choose to allow or restrict file sharing for all accounts in FileCloud by setting the **Share Mode**.
- The **Share Mode** setting appears in **Settings > Policies** on the **General** tab of a policy, and is set to **Allow All Shares** by default. To manage the global share mode, open the **Global Default Policy**.

Policy Settings - Global Default Policy ✕

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

Share mode

Set Share Mode

Default Share Expiry in Days

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed

Number of downloads allowed. Value 0 implies that the maximum number of downloads

You can set the **Share Mode** to one of the following options:


Share mode

Allow All Shares


Allow Private Shares Only

Shares Not Allowed

Option	Description
Allow All Shares	<p>Allows users to share any file or folder with custom permissions.</p> <p>A file or folder can be shared with:</p> <ul style="list-style-type: none"> Anyone with access to the link (Public Share). <i>No FileCloud account required.</i> Anyone with access to the link (Public Share) and a password. <i>No FileCloud account required.</i> Another user in FileCloud (Private share). <i>FileCloud account required.</i> The shared files will show up in the "Shared with Me" folder.

Option	Description
Allow Private Shares Only	<p>Allows users to share any file or folder with a user that has an existing FileCloud account.</p> <p>Sharing Privately requires:</p> <ul style="list-style-type: none"> The recipient(s) to be another user in FileCloud (Private share). <i>FileCloud account required.</i> 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	<p>Prevents users from sharing any file or folder.</p> <p> If you choose this option, then no other Sharing settings that you configure will be in effect.</p>

To set the Share Mode:

1. Log into the **Admin Portal**.
2. Click **Settings**.
3. Click the **Policies** tab.
4. In the **Manage Policy** window, select the row with the **Global Default Policy**, and then click the edit icon .
5. Select the **General** tab, and then in **Share Mode**, choose the option you want to set for all FileCloud users.
6. Click **Save**.

Specify Sharing Expiration

Administrators can configure 3 main expiration features of a shared file or folder.

Feature	Options	Description
Date	<ul style="list-style-type: none"> No expiration (0) Expire in a number of days 	Allow sharing to happen for a temporary time, or allow shares to exist as long as the file or folder exists
Actions	<ul style="list-style-type: none"> Have FileCloud remove the URL links to shares automatically Remove shared files automatically 	<p>Specify what happens when a shared file or folder is no longer accessible from the Share link</p> <ul style="list-style-type: none"> 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

Feature	Options	Description
Notifications	<ul style="list-style-type: none"> 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

Administrators can allow users to share files and folders for as long as they exist, or you can set a suggested number of days that a share remains active by default.

- Using a value of **0** means that unless changed by a user, shares do not expire.
- This setting can be changed by the user unless **Disallow Default Share Settings Change** is set in the **Settings > Misc > Share** tab.

Default share expiration days can be set for specific Users in a policy.

To set the Share Expiry default in a policy:

1. Open a browser and log in to the Admin Portal.
2. From the left navigation pane, click **Settings**, and then click the **Policies** tab.
3. Across from the policy that you want to edit, click the edit icon.
4. In the **General** tab, scroll down and change the value of the **Default Share Expiry in Days** setting.

Policy Settings - Global Default Policy

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

General | 2FA | User Policy | Client Application Policy | Device Configuration | Notifications

Share mode
Allow All Shares

Set Share Mode

Default Share Expiry in Days
0

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed

Save | Reset All | Close

- Click **Save**.
The value is only changed for users who are using this policy.

Set Expiration Actions

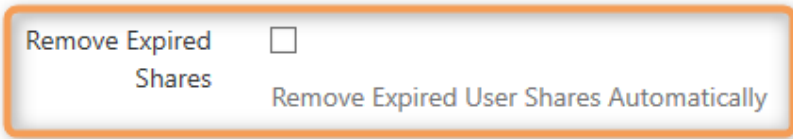
Remove Expired Shares

Administrators can specify that when a shared file or folder is no longer accessible, the share links are removed.

- Expired URL links will be removed automatically on the next Cron run
- The shared files will not be affected

To automatically have expired share links removed:

- Open a browser and log in to the *Admin Portal*.
- From the left navigation pane, under *Settings*, select *Settings*.
- Select the *Misc.* tab, and then the *Share* sub-tab.
- Under *Sharing Settings*, in *Removed Expired Shares*, select the checkbox.



Remove Expired Shares Remove Expired User Shares Automatically

- Click **Save**.

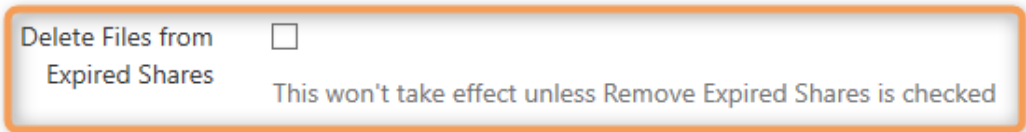
Remove Shared Files

Administrators can specify that when a shared file or folder is no longer accessible, the shared files are moved to the Recycle Bin automatically.

- Files in an expired share will be removed automatically on the next Cron run

To automatically have files in expired shares removed:

- Open a browser and log in to the *Admin Portal*.
- From the left navigation pane, under *Settings*, select *Settings*.
- Select the *Misc.* tab, and then the *Share* sub-tab.
- Under *Sharing Settings*, in *Delete Files from Expired Shares*, select the checkbox.



Delete Files from Expired Shares This won't take effect unless Remove Expired Shares is checked

- Click **Save**.

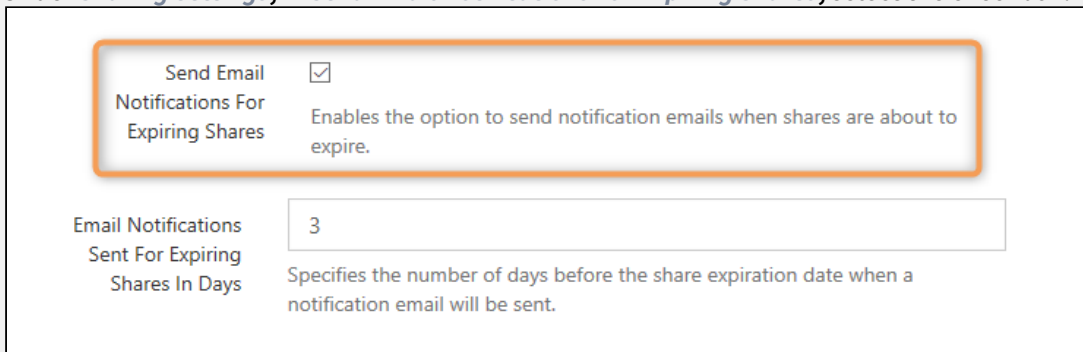
Send Expiration Notifications

Alert share Users About Upcoming Expiration

You can have FileCloud send email to everyone who has access to the shared file or folder that it will expire soon.

To send an email alert that a share will soon expire:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Under *Sharing Settings*, in *Send Email Notifications For Expiring Shares*, select the checkbox.



The screenshot shows a settings panel with two main sections. The first section, 'Send Email Notifications For Expiring Shares', has a checked checkbox and a description: 'Enables the option to send notification emails when shares are about to expire.' The second section, 'Email Notifications Sent For Expiring Shares In Days', has a text input field containing the number '3' and a description: 'Specifies the number of days before the share expiration date when a notification email will be sent.'

5. Click *Save*.

Specify Days to Expiration Email

Administrators can specify how many days before the share expires that an email notification is sent to users with access to the share.

- This option can only be set if you selected the option to *Send Email Notifications for Expiring Shares* first.

To send an email alert that a share will soon expire:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Under *Sharing Settings*, in *Email Notifications Sent For Expiring Shares in Days*, type the number of days you want to use.

Send Email Notifications For Expiring Shares Enables the option to send notification emails when shares are about to expire.

Email Notifications Sent For Expiring Shares In Days Specifies the number of days before the share expiration date when a notification email will be sent.

5. Click *Save*.

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.

Public Shares Must Be Password Protected

Administrators can require users to create all public shares with a password for an extra layer of security.

- Users will not be able to disable the use of passwords.
- This provides an extra layer of security for public shares.

Public Shares Must Be Password Protected Public shares will be password protected. Public Shares cannot be created without password

To require a password for shares:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Next to *Public Shares Must Be Password Protected*, select the checkbox.
5. Click *Save*.

Disallow Share Name Change

For security reasons, you may want shares to 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 which are commonly used in share names

This is how the randomly-generated name looks in the User Portal when creating a share:

Share link for customerid.docx

Share Link

http://127.0.0.1/url/bjyypf2xrabupuhr [Modify Link](#)   

Shared File

/jenniferp/DI 19-20/Documents/customerid.docx

Share Options | Share History

Share Name: ePvq0eFpt11glFAT [Change](#)

Expires: Never

Max number of downloads: No Restrictions

Send Email Notifications: Yes

Sharing Permissions:

Allow anyone with link

Allow anyone with link and a password

Allow selected users or groups

[Remove Share](#) [OK](#)

As an administrator, you can prevent users from changing the auto-generated share names for security purposes.

Disallow Share Name Change

Don't allow users to change the auto generated share names

To prevent name changes for shares:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Next to *Disallow Share Name Change*, select the checkbox.
5. Click *Save*.

Hide Send Share Link Via Email

To protect Share links, you can hide the option in the User Portal to send the share link in email.

This is where the user has the option to share a link to the file or folder in email on the User Portal:

Share link for customerid.txt
✕

Share Link

Modify Link

📄
🔗
✉️

Shared File
/jenniferp/DI 19-20/Documents/customerid.txt

Share Options

Share History

Share Name: gcUml06zziOID1hg [Change](#)

Expires: Never

Max number of downloads: No Restrictions

Send Email Notifications: Yes

Sharing Permissions:

Allow anyone with link

 Allow anyone with link and a password

 Allow selected users or groups

Remove Share

OK

As an administrator, you can disable the display of the email button to discourage users from sending the share link in email for security purposes.

Hide Send Share Link
Via Email

Do not show send share link via email option.

To hide the option for sending a link to the share in email:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. Select the *Misc.* tab, and then the *Share* sub-tab.
4. Next to *Hide Send Share Link Via Email*, select the checkbox.
5. Click *Save*.

Limit User Account Searches

- 📘 The ability to limit searches of user accounts by account type to ALL, FULL, GUEST, or EXTERNAL is available in FileCloud Server version 19.1 and later.



As an administrator, you can configure FileCloud to limit how users can search for other user accounts.

By default, when user1 shares a file or folder with user2, then user1 can search for user2's account by the user name or email-id.

- The search results list both exact and partial matches.

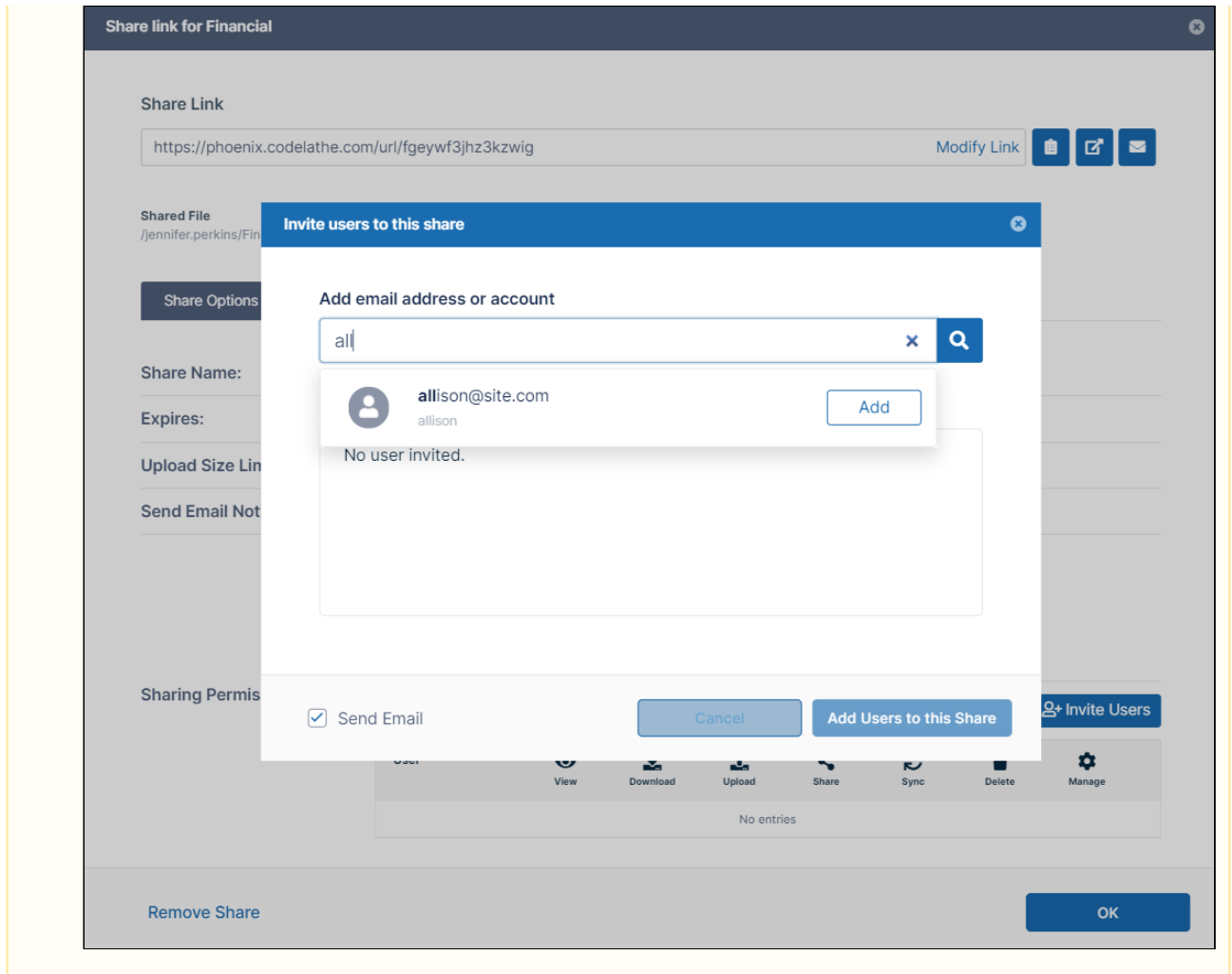
However, this is not desirable in certain cases and organizations, as the search results reveal user accounts that exist in the FileCloud system.

Therefore, FileCloud Server allows you to restrict user searches using two search modes:

User Account	User Account Type
<ul style="list-style-type: none"> • Exact Email Search With Explicit Account Invite • Exact Email Search With Implicit Account Invite • Exact Name/Email Search • Partial Name/Email Search 	<ul style="list-style-type: none"> • ALL • FULL • GUEST • EXTERNAL
<p> How to Enable User Account Search Mode</p>	<p> How to Enable User Account-Type Search Mode</p>
<p>NOTE: You can use both of these search limitations together to create a combination that meets your requirements.</p> <p>For example, you can set the <i>User Account Search Mode</i> to Partial Name/Email Search, and then use the <i>User Account Type</i> search mode to limit the results to only accounts with FULL access.</p>	

 **Note**

Using a search mode limits account searches for all the users in the FileCloud system. These settings are seen by a user when they want to share a file or folder with another specific user and need to find that user's email address.



Use Display Name as well as User Account Name

The ability to change how a name is displayed in Sharing details is available in FileCloud Server version 19.1 and later.

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

The screenshot shows the 'Add User' form with the following fields and values:

- Authentication: Default Authentication
- Access Level: Full
- User name*: elin frei (highlighted with a red circle containing the number 1)
- Display Name: Elin (highlighted with a red circle containing the number 2)
- Password*: [masked with dots]
- Email: efrei@example.com
- Send Email Notification:
- Include Password in Email:

At the bottom right of the form are two buttons: 'Create' and 'Close'.

In the Admin Portal, when you create a user, you can set 2 different names.

1. User Name



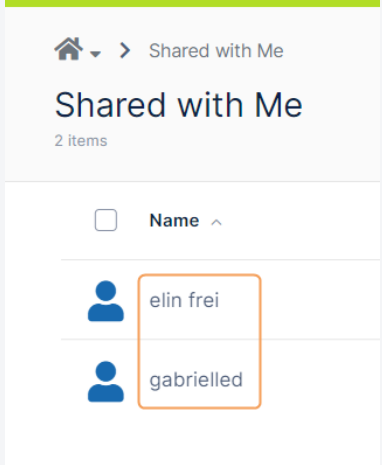
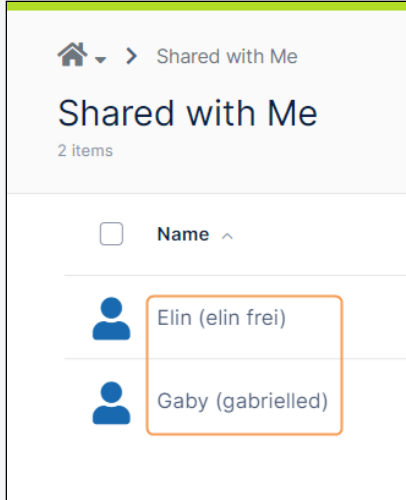
- In the User Portal, by default, FileCloud displays the User Name.
- It may not be clear to users who is sharing the file with them, especially if User Name includes only abbreviations and numbers.
- The User Name cannot be changed after the user has been created.

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.

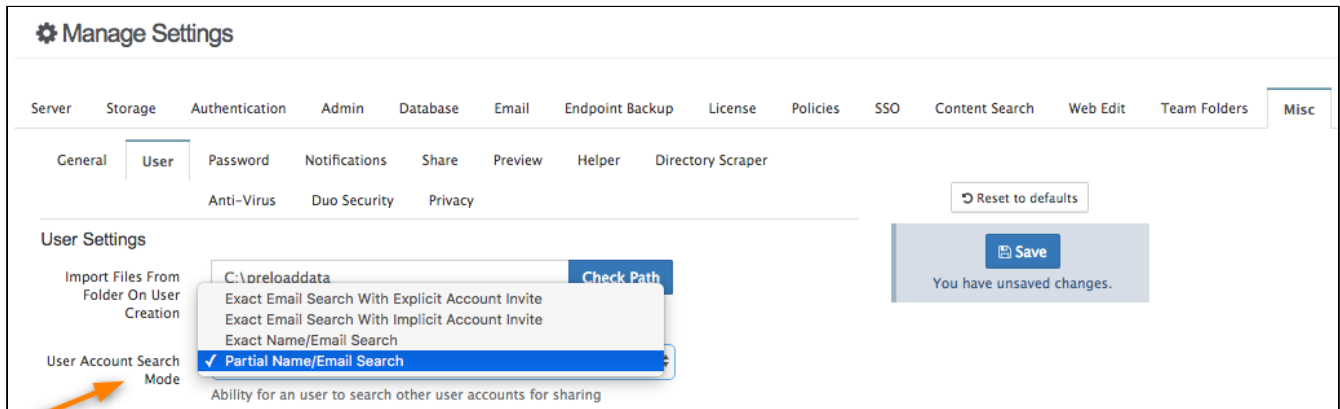
Where Your Changes Appear

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

As an administrator, 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. You can also set this option to allow users to search for another user with just a known partial email address.




Search Modes

Option	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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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
Partial Name / Email Search	Joe C	<ul style="list-style-type: none"> 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

To access the User Account Search Mode Settings:


1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, click *Settings*.
3. On the *Manage Setting Settings* screen, click the *Misc* tab, and then the *User* sub-tab.
4. Look in the *User Settings* section for the *User Account Search Mode* check box.

User Account-Type Search Mode

 The ability to limit searches of user accounts by account type to ALL, FULL, GUEST, or EXTERNAL is available in FileCloud version 19.1 and later.

As an administrator, 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.

User Account Type	Level of Access
ALL	No restriction of account searches
FULL	<p>An account with full access has its own private cloud storage space in the "My Files" area.</p> <p>These users can:</p> <ul style="list-style-type: none"> • 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	<p>An account with guest access level has restricted access to the FileCloud system.</p> <p>These user accounts do not have private cloud storage. These users can:</p> <ul style="list-style-type: none"> • view/upload/download files shared to them by other user accounts • re-share content if they have permission
EXTERNAL	<p>An account that can only be used to access the User Portal through a Web browser.</p> <p>External Accounts can:</p> <ul style="list-style-type: none"> • view/upload/download content shared with them <p>External Access accounts can only be local user accounts.</p>

 For a complete list of features available to each account type, read [User Account Types](#)

The screenshot shows the FileCloud Online Admin Portal settings page. The top navigation bar includes: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, Policies, SSO, Content Search, and Web. Below this, the 'Misc' tab is selected, and the 'User' sub-tab is active. The 'User Settings' section is visible, with the following options:

- Import Files From Folder On User Creation: A text input field containing 'admin' and a 'Check Path' button.
- Sample data Folder to Import from when Creating a User Account: A text input field.
- User Account Search Mode: A dropdown menu set to 'Partial Name/Email Search'.
- User Account Type Search Mode: A dropdown menu with options: All Users (selected), Full Users, Guest Users, External Users, and Show All Groups.

An orange arrow points to the 'User Account Type Search Mode' dropdown menu.

To access the User Account-Type Search Mode Setting:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, click *Settings*.
3. On the *Manage Setting Settings* screen, click the *Misc* tab, and then the *User* sub-tab.
4. Look in the *User Settings* section for the *User Account Type Search Mode* check box.

Email Settings

i 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 the following messages to users via email:

- share notifications
- file change notifications
- error notifications

In order for the email system to work, the FileCloud administrator must set up the mail configurations.

To configure email notifications:

1. In the admin portal, go to **Settings > Email**.
The general settings on the page begin with **Email From Address** and go through **Email Type**, as shown in the screenshot below.

2. Enter values for these settings; the table below the screenshot explains how each setting is used.

Server	Storage	Authentication	Admin	Database	Email	Endpoint Ba
--------	---------	----------------	-------	----------	--------------	-------------

Email Settings

Test Email

[Send Email](#)

Email From Address

demo@filecloudmail.com

Specify the from email address. This address will be used on all outgoing mails.

Email From Name

FileCloud

Specify from name. This name will be used on all outgoing mails.

Use From name and email

The admin From name and email set above will be used for all communications including user shares

Email Reply To Address

demo@filecloudmail.com

Specify the email address to set for 'reply to' field

Email Reply To Name

FileCloud

Specify the name to set for 'reply to' field

Use Reply To name and email

The admin Reply To name and email set above will be used for all communications including user shares

Email Type

smtp

Set type of email to be sent

General email setting information:

Setting	Description
Email From Address	<p>By default, 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).</p> <p>! By default, admins cannot change the Email From Address in FileCloud Server version 19.1 and later; it is set to fchosted@filecloudmail.com. If you want to change the Email From Address or you want admin permission to change the Email From Address, please Contact FileCloud Support.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>i If you are using SMTP as your email type, and set SMTP Auth Type (listed below, under SMTP Configuration) to XOAUTH2, then set Email From Address to the same value as SMTP Auth User. This is required for successful use of Azure as the authentication provider.</p> </div>
Email From Name	<p>By default, 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).</p>
Use From name and email	<p>To conceal the sender, list the Email From Address and Email From Name for all user share emails, even if an actual from address and name exist.</p>
Email Reply to Address	<p>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).</p>
Email Reply to Name	<p>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).</p>
Use Reply To name and email	<p>To conceal the sender, list Reply To Address and Reply To Name for all user share emails, even if an actual reply to address and name exist.</p>

Setting	Description
Email Type	<p>Specify the email facility to be used. The type can be SMTP, Mail or SendMail.</p> <p>Note that Mail and SendMail use underlying OS's function (available only for Debian/Ubuntu installation).</p> <p>The recommended setting is SMTP.</p>

Office 365 Settings

When using Office 365, SMTP settings must be set to the following values:

Setting	Recommended value
SMTP Host	smtp.office365.com
Port	587
SMTP Security	TLS
Username/email address and 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](#).

- 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:

- In **Email Type**, choose **SMTP**.
The SMTP fields below it become enabled.

Email Type

smtp

Set type of email to be sent

SMTP Host

smtpcorp.com

SMTP Hostname

SMTP Port

2525

SMTP Port

SMTP Security

none

SMTP connection security

SMTP Auth Enabled

Enable to set SMTP auth

SMTP Auth Type

Basic

Basic

XOAUTH2

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.

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 Setting	Description
SMTP Auth Enabled	If SMTP requires authentication, then check this to enable and enter the authentication settings.
SMTP Auth Type	<p>SMTP Auth Type may be Basic or XOAUTH2. The option you choose determines which additional SMTP fields follow.</p> <ul style="list-style-type: none"> • 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 User	Enter the authentication username.
SMTP Auth Password	Enter the password for SMTP Auth User.

If you choose **XOAUTH2** for **SMTP Auth Type**:

- 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.
- For the fields **oAuth Client Secret**, **oAuth Client ID**, **oAuth Tenant ID**, and **oAuth Redirect URI** listed in the table below, retrieve the values from [portal.azure.com](#) after registering the oAuth application.
- Fill in the SMTP oAuth fields on the Email Settings page listed in the table below:

SMTP Auth User	<p>Enter the authentication username</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> 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.</p> </div>
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SMTP oAuth Provider	Choose the oAuth provider (authorization server). Currently, the only available option is Azure .
oAuth Client Secret	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
Generate oAuth Token	Click to generate the oAuth token so you can begin using email with oAuth.

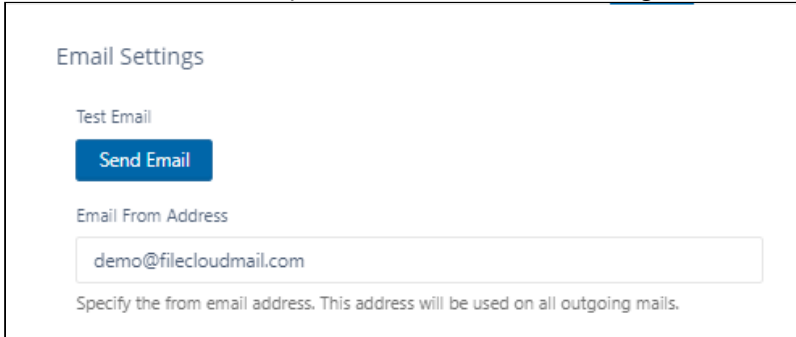
- d. If your **SMTP Auth Type** is **XOAUTH2**, do the following:
 After you have filled in the SMTP fields, click **Generate OAuth Token**.
 If you are not logged in to your Microsoft authenticator app, you are prompted to log in so you can access Azure to generate the token.
 Once the OAuth token is generated, the following XML appears on your screen:

```

This XML file does not appear to have any style information associated with it. The document tree is shown below.
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<commands>
  <command>
    <type>getoauthtoken</type>
    <result>1</result>
    <message>OAuth refresh token has been retrieved successfully.</message>
  </command>
</commands>

```

3. Click **Send Email** at the top of the screen to test the settings.



Email Settings

Test Email

Send Email

Email From Address

demo@filecloudmail.com

Specify the from email address. This address will be used on all outgoing mails.

The email should be sent to the admin's email, and a success notification should appear 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** in the **Do Not Email Settings** section.
- Beginning with FileCloud version 18.1 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 for any emails** 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 for any emails** checkbox.

Do Not Email Settings

Do Not Email List

[Manage](#)

Ignore "Do Not Email" list for priority emails
 Users on "Do Not Email" list will still receive priority.

Ignore "Do Not Email" list for any emails
 Users are emailed regardless of whether they are on the "Do Not Email" list. NOTE: If both options are unchecked, the user added to the do not email list will not receive any emails.

Maximum number of emails to send in the 24h

Maximum number of emails system can send in the 24h span. If the limit is reached all other emails will be prevented from sending. (0 - no limitations)

To add or remove users from the Do Not Email list:

- Next to **Do Not Email List**, click **Manage**.
The **Manage Do Not Email List** dialog box opens.

Manage Do Not Email List ×

Do Not Email List	+ Add	- Remove	⊘ Clear All
<input type="checkbox"/> Email Id			
<input type="checkbox"/> gabrielle95@example.com			
<input type="checkbox"/> jonathan81@example.com			

- To add an email to the list, click **Add**, then enter and save an email address.
- To remove an email from the list, check the box next to the email and click **Remove**.

Configuring System Generated Emails

Controlling System Generated Automatic Emails

It is possible to control which emails are sent by the system.

The settings can be accessed by

1. Log into FileCloud [Administration Portal](#)
2. Click on **Settings** in the left navigation panel
3. Click on **Admin** tab
4. Change settings as needed
5. Click **Save**.

Send Approval Pending Emails	This controls the option to send out an approval pending email to the admin when a new user account is created and admin approval is required
Send Welcome/Verification Emails	This controls whether verification emails are sent to users to verify their email addresses
Send Approval Emails to Users	This controls whether account approval emails are sent to users
Send Admin Summary Emails	This controls whether daily system summary emails are sent to the admin account, This only works if a Cron Task or Windows Task Manager is setup.

Send Approval Pending Emails	<input checked="" type="checkbox"/>	Enable to send new account approval emails
Send Welcome/Verification Emails	<input checked="" type="checkbox"/>	Enable to send Welcome Emails for users
Send Approval Emails To users	<input checked="" type="checkbox"/>	Enable to send Approval Emails for users
Send Admin Summary Emails	<input checked="" type="checkbox"/>	Enable to send daily admin summary email

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. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Settings**.
3. Click the **Endpoint Backup** tab.
4. Configure the settings according to the following descriptions:

Table 1. User backup settings in the admin portal

Settings Name	Description
Allow Users To Backup	This setting allows users to back up files and folders using the Cloud 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	This settings allows Mobile clients to back up photos and videos automatically to their FileCloud accounts. Turning off this setting prevents this server from being used to back up audio/video files. This path cannot be changed. All camera uploads are stored in the user's backup folder. For example, if the user name is jdoe, the camera uploads are stored in /jdoe/backups/<phone name> NOTE: This location cannot be synced
Backup Path	This is 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.
Backup Notification Email	This is 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 [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. In the **Manage Users** section, select the user whose backup path you want to set
4. Click the **Edit** icon .
5. On the **User Details** screen, scroll down to the **Backup Path** field.


6. In **Backup Path**, type in the folder path you want to use.


User Details
✕


Name	john	Total Quota	2 GB
Email	john@xyz.com	Used Quota	5.1 GB
Last Login	04 Feb 2018 08:43	Available Quota	0 B
Group	Manage	Used Storage	5.1 GB More



 Mobile Devices



 Manage Files



 Manage Shares


 Reset Password


 Email Password


 Delete Account


 Manage Policy


 Manage Backups

Password Expires On

Email Verified

Disable Sync (Automatic Sync of My Files and Network Folders)

Disable Sync (Offline Access)

Backup Path

Admin User

Change Password on Login


[Save](#)
[Close](#)

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

View a user's backed-up files

To view the backed up files for a specific user:

1. Log in to the FileCloud admin portal.
2. In the navigation panel, click **Users**.

3. In the **Manage Users** section, select the user whose backups you want to view.
4. Click the **Edit** icon .
5. On the **User Details** screen, click **Manage Backups**.
6. On the **Backup Devices** screen, to view the paths backed up from a device, select the device, and then click **View Backups**.
7. On the **Backup Devices** screen, to view the backup date and the number of files backed up, click **View Backup History**.

Also see:

- [Automatic Database Backup](#)
- [Setting Up Persona Backup Using Sync](#)

Automatic Database Backup

-  Filecloud will automatically backup databases starting in FileCloud Server version 17.3 and later.
-  In environments where High Availability architecture is being used, automatic backups are performed during Cron runs starting in FileCloud Server version 19.1 and later.

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.

Database Backup Options

Disable DB Backup	<input type="checkbox"/>
Autobackup enabled. Select checkbox to disable automatic database backups.	
Last Autobackup run: Jan 12, 2021 6:00 AM	
DB Backup Store Path	<input type="text" value="/var/www/html/scratch/autobackups"/>
Path to save backed up database. Path must be writeable!	
Number of Backups	<input type="text" value="15"/>
Number of settings backups to maintain	
DB Backup Interval	<input type="text" value="0"/>
Interval between backup operations. Example: 0 = daily backup	

- **Disable DB Backup** - When checked, FileCloud will not back-up databases during a Cron run. If autobackup is enabled, the last autobackup run date is shown.
- **DB Backup Store Path** - the path to a directory where you want to save the backed-up database files. 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** - this is 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 set this number to be lower. For example, if you type in 2 for **Number of Backups**, the backup file will only contain 2 days worth of data. Keep in mind that after those 2 days, the backup file will be overwritten to store the next 2 days worth of data. This setting controls how far back you can recover data.
- **DB Backup Interval** - this number is 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.

For 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 setting they would use:

- **Disable DB Backup** = *not selected*
- **DB Backup Store Path** = */var/scratch/autobackups*
- **Number of Backups** = 30
- **DB Backup Interval** = 7

To configure automatic database backups:

1. Open a browser and log in to the *Admin Portal*.
2. In the *Admin Portal*, from the left navigation panel under *SETTINGS*, select the *Settings* tab.
3. On the Manage Settings tab, select the *Misc.* tab, and then the *General* sub-tab.
4. On the *General* sub-tab, to disable backups, select *Disable DB Backup*.
5. On the *General* sub-tab, to create backups, clear the *Disable DB Backup* checkbox if it is selected.

6. On the *General* sub-tab, to configure backups, in *DB Backup Store Path*, type in the path to where you want the files stored.
7. If you are configuring backup settings, in *Number of Backups*, type in the number of days worth of data that you want stored in a single backup file.
8. If you are configuring backup settings, in *DB Backup Interval*, type in the number of days between a refresh of the backup file.
9. To save your settings, click *Save*.

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.

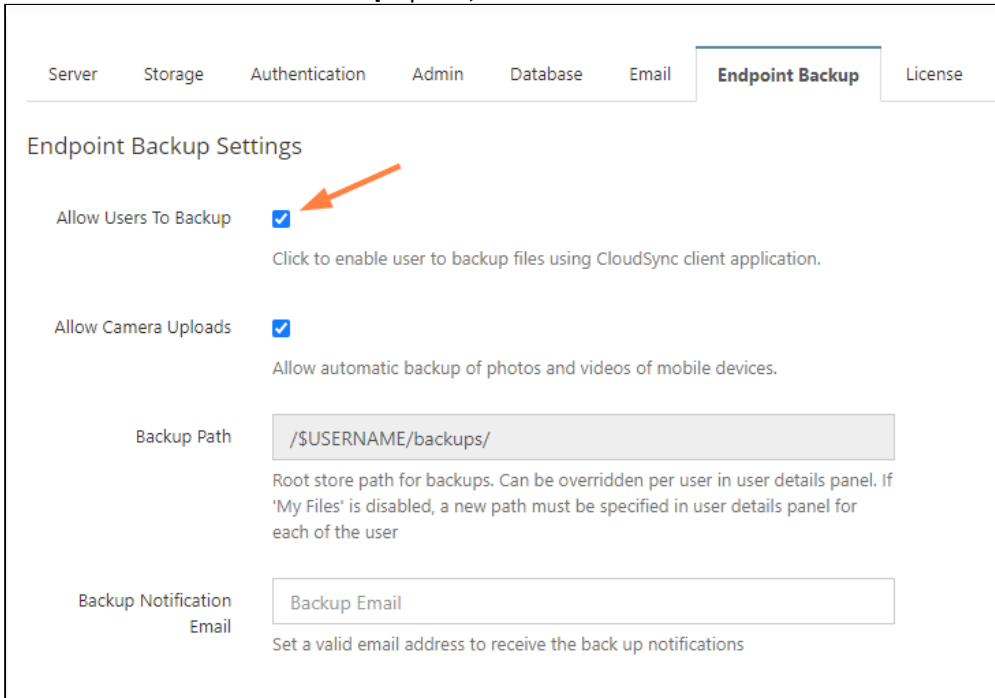
Steps:

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. Log in to the admin portal.
2. Navigate to **Settings > Endpoint Backup**.

3. Enable the **Allow Users To Backup** option, and click **Save**.



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

Endpoint Backup Settings

Allow Users To Backup 
Click to enable user to backup files using CloudSync client application.

Allow Camera Uploads
Allow automatic backup of photos and videos of mobile devices.

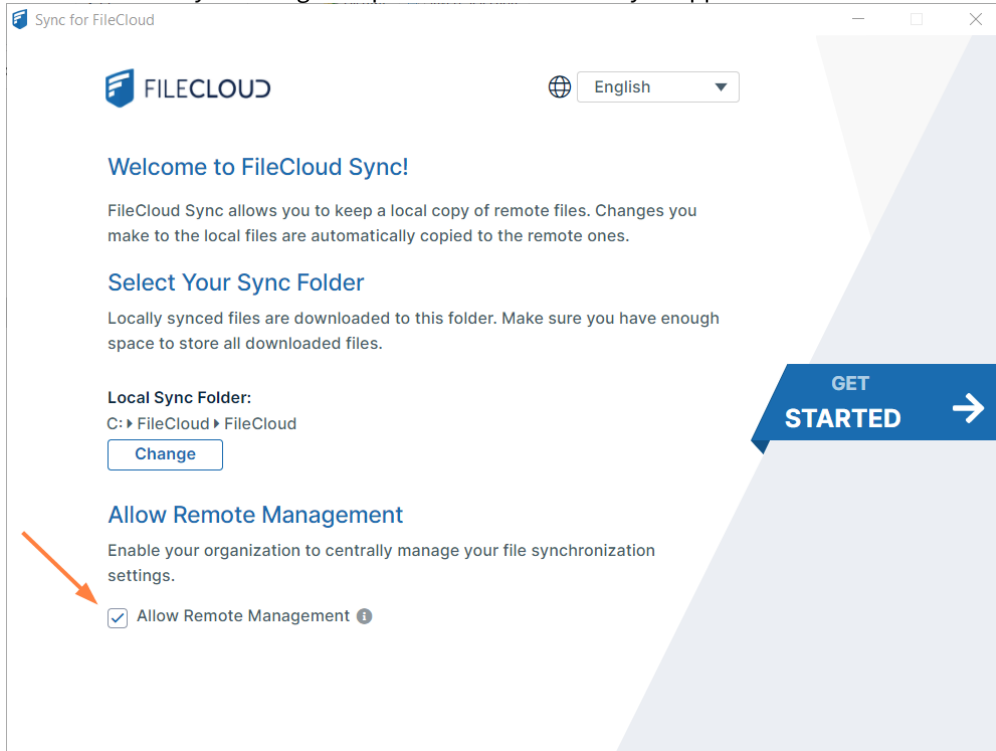
Backup Path
Root store path for backups. Can be overridden per user in user details panel. If 'My Files' is disabled, a new path must be specified in user details panel for each of the user

Backup Notification Email
Set a valid email address to receive the back up notifications

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.

- Log in to the admin portal.
- Navigate to **Settings > Policies** and edit the users' policy.
- 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>

```

Policy Settings - Global Default Policy ✕

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

General 2FA User Policy Client Application Policy Device Configuration Notifications

Manage Device Configuration

Client Configuration

```

ic|/${USERID}/backups/${USERID}/Music|
1|30m|1|0|0</offline_folder_4>
<offline_folder_5>C:\Users\${USER}\Favo
rites|/${USERID}/backups/${USERID}/Fav
orites|1|30m|1|0|0</offline_folder_5>
<offline_folder_6>C:\Users\${USER}\App
Data\Roaming\Microsoft\Templates|/${U
SERID}/backups/${USERID}/Office_Templ
ates|1|30m|1|0|0</offline_folder_6>
<offline_folder_7>C:\Users\${USER}\Doc
uments|/${USERID}/backups/${USERID}/
Documents|1|30m|1|0|0</offline_folder_

```

Save
Reset
Close

Client Security Settings

- [Two Factor Authentication](#)
- [Setting Client Application Policies](#)
- [Using a Proxy Server](#)

Two Factor Authentication

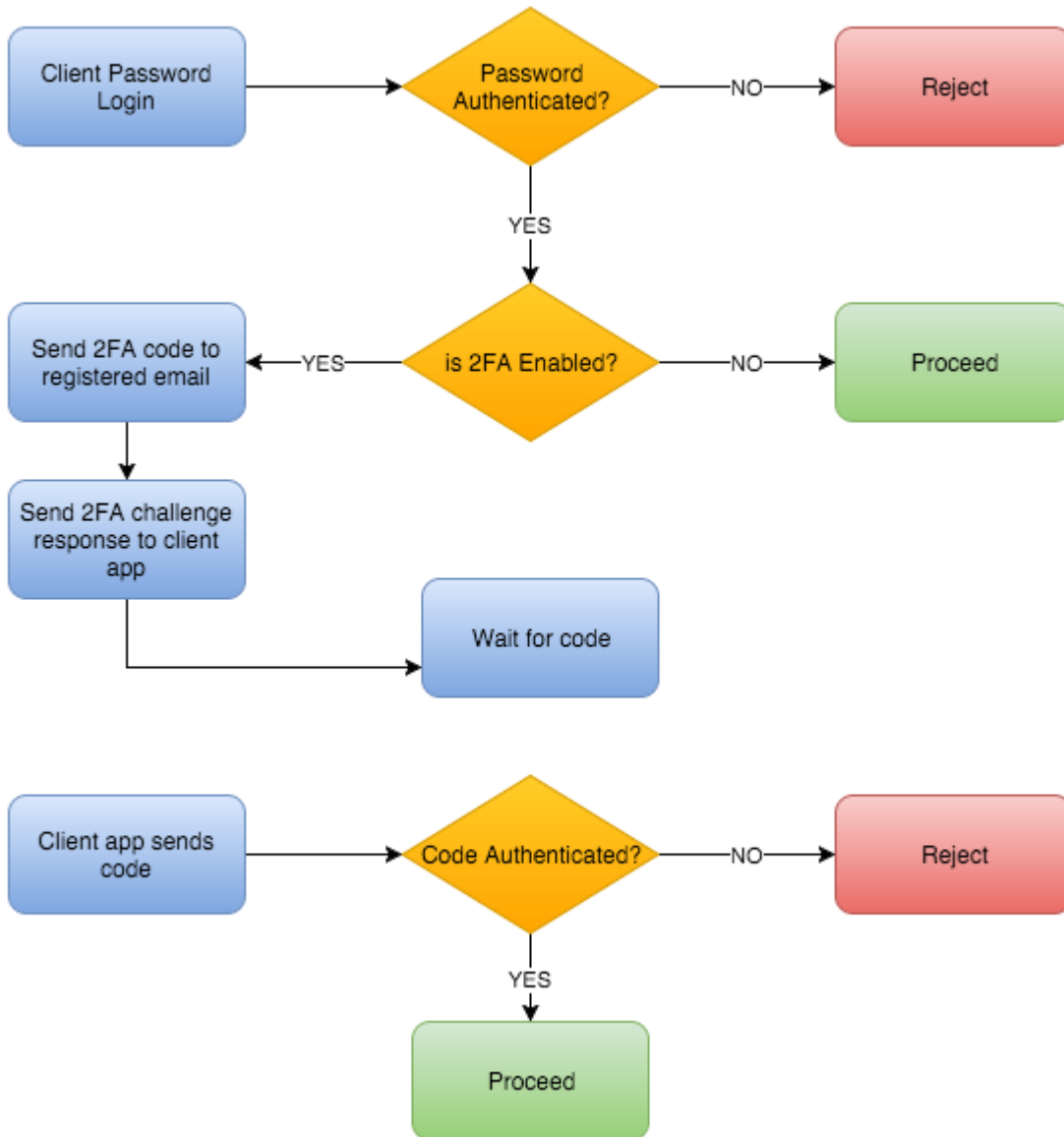
Two-factor authentication (2FA) refers to the two step verification process that is available in FileCloud and designed to provide an extra layer of security. With this function, in order to access FileCloud, the user is required to know not only the password and username but also an extra security code that is made available to them. The FileCloud administrator can enable two-factor authentication and require it for access to the user portal. This can be done regardless of the authentication type (default, AD, or LDAP).

FileCloud supports the following modes to deliver 2FA codes:

- Deliver code using user's registered email
- Google Authenticator TOTP Code
- DUO Security
- SMS OTP Security Code


Two-factor authentication into user portal using user's registered email address

The general flow is shown below




Two-factor authentication in user portal using TOTP (Google Authenticator or similar TOTP code generators)

i 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.

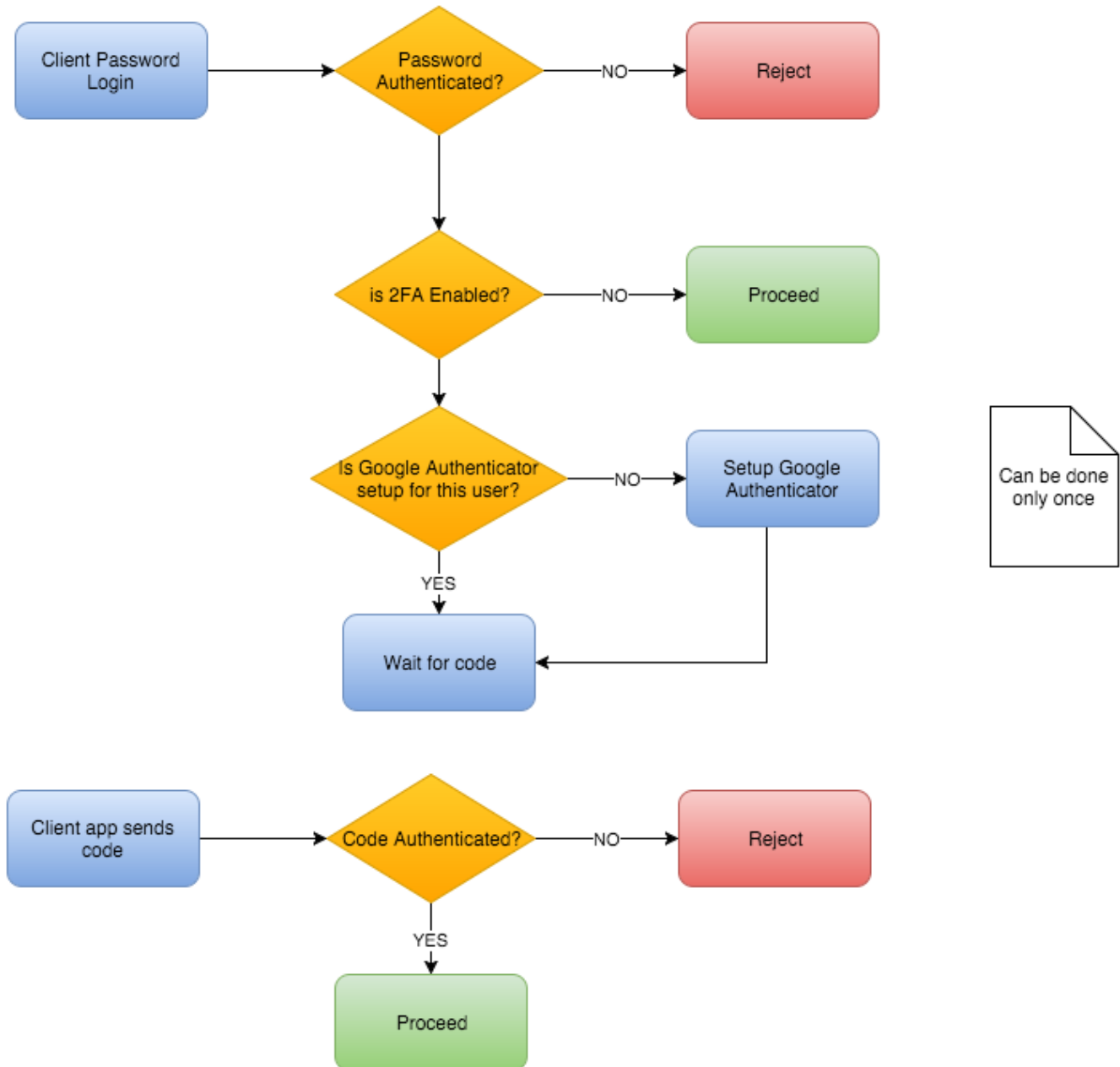
 To set up 2FA with Google Authenticator, simply choose **TOTP (Authenticator App)** when configuring 2FA for the user portal. See [Enable Two Factor Authentication for User Portal \(Global setting\)](#), below, for help. When the user logs in to the user portal for the first time, the user will be provided 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 will no longer be able to set it up again. Only the Administrator can clear the Google Authenticator setup.

Instead of Google Authenticator app, Microsoft or Duo Security apps can also be used to manage the TOTP code

The general flow is shown below



Two-factor authentication using DUO security

As of v17.3, FileCloud can be setup 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 setup 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, enter the information in **Settings > Misc > Duo Security** tab under **Duo Auth API Security Settings**, and save.

Manage Settings

Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO Content Search Web Edit Team Folders ServerLink Misc

General User Password Notifications Share Preview Helper Directory Scraper Anti-Virus

Duo Security Privacy [Reset to defaults](#)

Duo Auth API Security Settings

Duo Auth API Integration Key Specify Duo Auth API Security Integration Key

Duo Auth API Secret Specify Duo Auth API Security key

Duo Auth API Host Specify Duo Security Auth API Host

Duo Admin API Security Settings

Duo Admin API Integration Key Specify Duo Admin API Security Integration Key

Duo Admin API Secret Specify Duo Admin API Security key

Duo Admin API Host Specify Duo Security Admin API Host

Manage Settings

Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO Content Search Web Edit Team Folders ServerLink Misc

General User Password Notifications Share Preview Helper Directory Scraper Anti-Virus

Duo Security Privacy Reset to defaults

Duo Auth API Security Settings

Duo Auth API Integration Key
Specify Duo Auth API Security Integration Key

Duo Auth API Secret
Specify Duo Auth API Security key

Duo Auth API Host
Specify Duo Security Auth API Host

Duo Admin API Security Settings

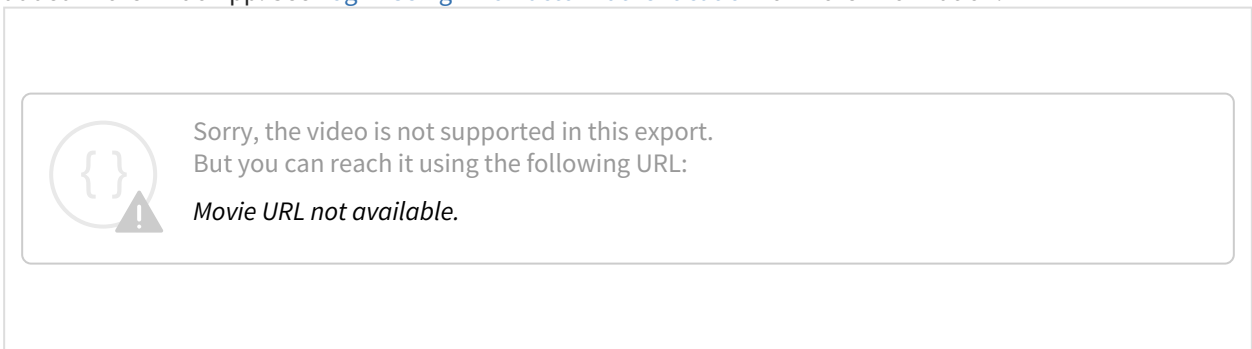
Duo Admin API Integration Key
Specify Duo Admin API Security Integration Key

Duo Admin API Secret
Specify Duo Admin API Security key

Duo Admin API Host
Specify Duo Security Admin API Host

3. Open the **Policies** tab and select the policy (Select the Global policy if 2FA needs to be the default)
 4. Open the **2FA** tab of the Policy.
 5. Select **"YES"** for **Enable Two Factor Authentication**
 6. Select **"DUO Security"** for **Two Factor Authentication Mechanism** and save the policy.
- Now, users are required to use 2FA to log in through the user portal.

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.



Two-factor authentication using SMS OTP (one-time password) Security Codes

As of v19.2, 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. Enter the information in **Settings > Misc > 2FA**.

Server	Storage	Authentication	Admin	Database	Email	Endpoint Backup	License	Policies
Third Party Integrations		ServerLink	Misc	Reset				
General		User	Password	Notifications	Share	Preview	Support Services	Directory Scraper
DUO Security		Privacy	2FA					

Miscellaneous 2FA Settings

2FA Code Length	<input type="text" value="4"/>
2FA Code Dictionary	<input type="text" value="Default (numbers and letters)"/>
SMS 2FA Code Expiration in minutes	<input type="text" value="5"/> <small>The duration for which the SMS code will be valid (in minutes)</small>
Case-sensitive 2FA Code Comparison	<input type="checkbox"/> <small>Case-sensitive Comparison of 2FA Codes</small>
Allowed Resend Attempts	<input type="text" value="5"/> <small>Set maximum allowed 2FA code resend attempts before a security timeout (5 is default)</small>
2FA Code Resend Timeout	<input type="text" value="60"/> <small>Timeout after consecutive resend attempts limit reached (in seconds, 30 is default)</small>
Test SMS gateway configuration	<input type="text" value="01555555555"/> <input type="button" value="Test SMS"/> <small>Check if SMS configuration is valid. Use a test phone number</small>

SMS Security Settings for Twilio

SMS Admin SID Security Settings	<input type="text" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/> <small>SID of gateway provider</small>
SMS Admin Token	<input type="text" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/> <small>Specify the token of the gateway provider</small>
SMS Admin Sending Phone Number	<input type="text" value="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"/> <small>Specify the sender phone number</small>

i The settings **2FA Code Length** and **2FA Code Directory** 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 Dictionary- 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 Security Settings - 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.

i **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.

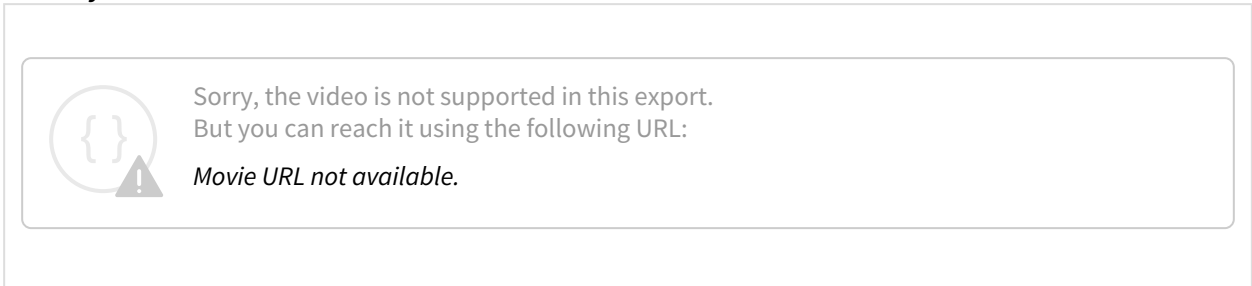
If users are required to use SMS with 2FA, they will see the following dialog box during login after the policy is enabled:

The screenshot shows a modal dialog box with the title "Add your phone number for SMS-based 2FA" and a close button (X) in the top right corner. Below the title is a text input field. Underneath the input field, the text "Please enter your phone number" is displayed. At the bottom of the dialog, there are two buttons: "Save Phone Number" and "Cancel".

Enable Two Factor Authentication for User Portal (Global setting)

Administrator can enable Two Factor Authentication using the following steps

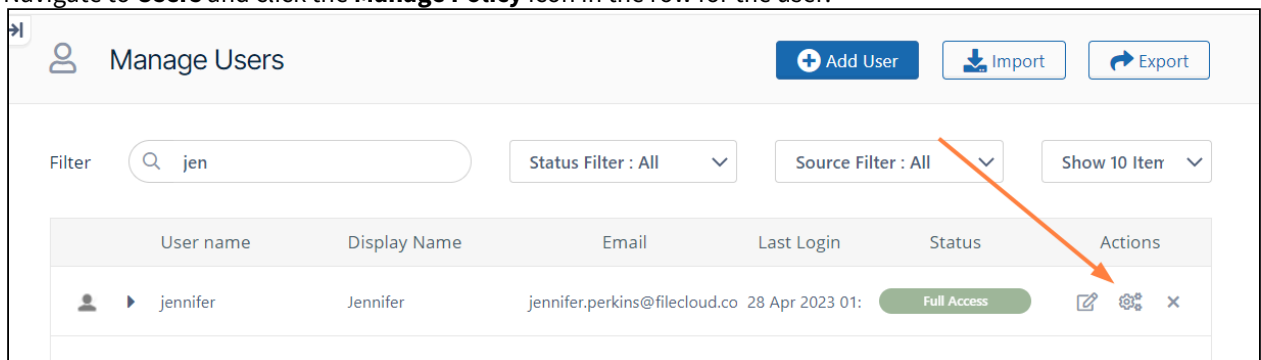
1. Log into the Administrator Portal
2. Navigate to "Settings"
3. Select **Policies** Tab
4. Under **2FA** heading, Change the **Enable Two Factor Authentication** drop down box to **Enabled**
5. In **Two Factor Authentication Mechanism** choose **Email, TOTP (Authenticator App), DUO Security** or **SMS Security**.



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, the Admin can reset the Google Authenticator setup for that user using the following steps

1. Login into the Admin portal
2. Navigate to **Users** and click the **Manage Policy** icon in the row for the user.



3. Click the **2FA** tab.
4. Click the **Reset 2FA Setting** to enable the user to reset their authenticator code.

Policy Settings - Global Default Policy - jennifer

Note: Custom Policy assigned to this User

General **2FA** User Policy Client Application Policy Device Configuration Notifications

2 Factor Authentication

Enable Two Factor Authentication

YES

Enable to require a one time passcode to be entered along with the account password

Reset 2FA

Reset 2FA Setting

Allow user to reinitialize 2FA authenticator

Two Factor Authentication Mechanism

Save Reset All Close

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 validity for Email based 2FA

i 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.

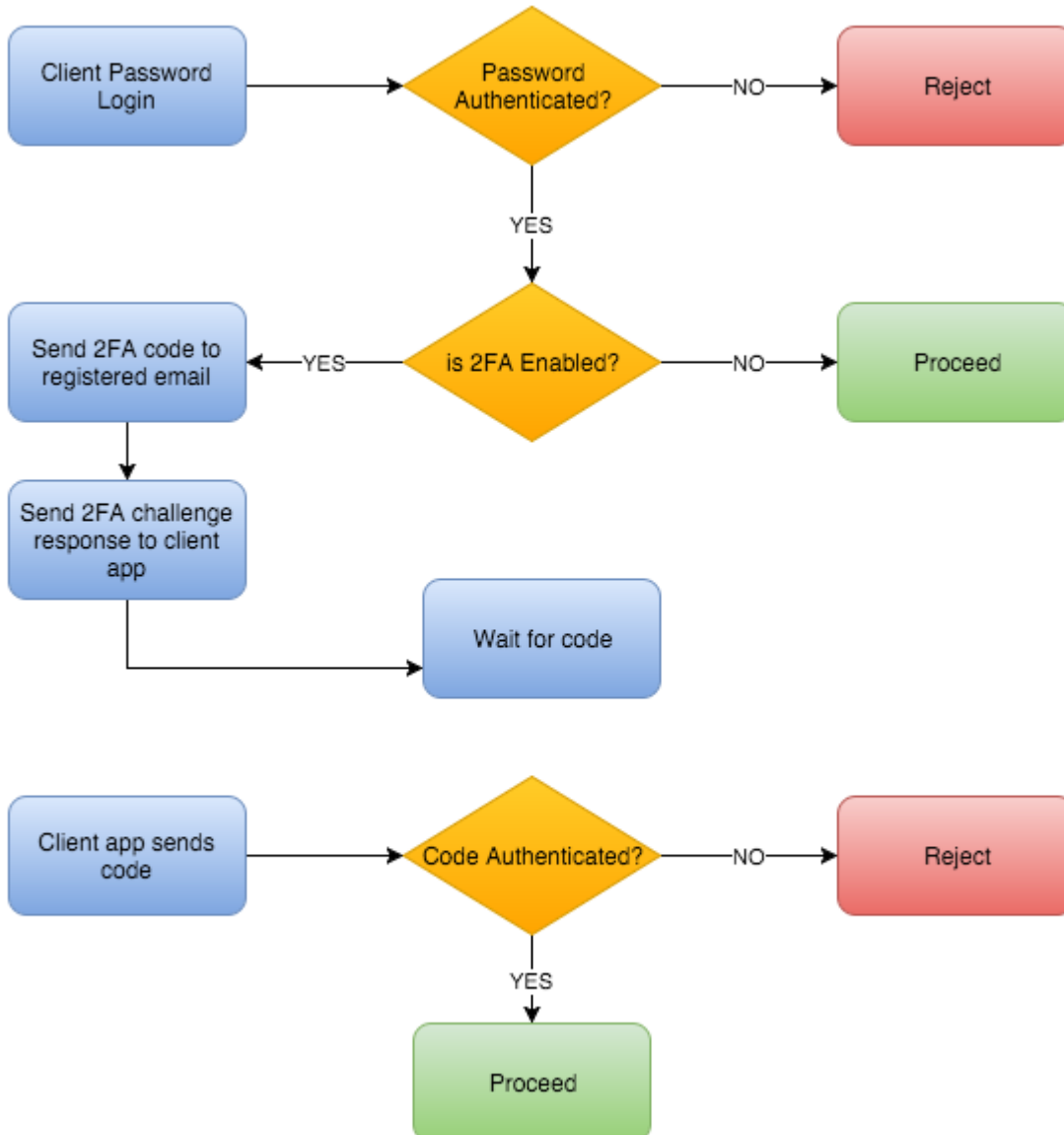
Two-Factor Authentication for Admin Portal

From v12 onwards, support for two factor authentication is available for Admin portal. Both site admin and super admin (for multi tenancy control panel) can be set to require additional code in order to access.

Two factor authentication for Admin supports only **Email based 2FA**. The code will be delivered to the email associated with the account.

i Since 19.2, the way admins set up 2FA has changed - the admin can now select code sendout methods using a drop down (Email or SMS). In order to upgrade without hassle, it is advised to disable admin 2FA before upgrading, and set it up again.

The flow is same as user 2FA flow as shown below



Enable Two Factor Authentication for Site Admin

A site admin is the admin account to log into the Administrator portal of a specific site. To enable 2FA for the first time, please follow the steps

1. Log into Admin portal
2. Navigate to "Settings"
3. Select "Admin" Tab
4. Check **Enable Two Factor Authentication for Admin Logins**.

The screenshot shows the FileCloud 'Manage Settings' interface. The 'Admin' tab is selected. The 'Admin Settings' section includes the following fields:

- Admin Login Name:** Input field containing 'admin'. Description: 'Change the built-in admin user name'.
- Admin Email:** Input field. Description: 'Email id for admin account.'
- Enable Two Factor Authentication For Admin Logins:** A checked checkbox. Description: 'Enable Two Factor Authentication for Admin user logins. Requires valid email id.' An orange arrow points to this checkbox.
- Admin password:** Password input field. Description: 'Admin password'.
- Re-Confirm Admin Password:** Password input field. Description: 'Re-enter admin password'.

2FA fields appear.

5. To use SMS authentication, In **Select 2FA Delivery Method for Admin**, choose **SMS Authentication**. Additional fields appear.

Server	Storage	Authentication	Admin	Database	Email	Endpoint Backup	Licen
				ServerLink	Misc	Reset	

Admin Settings

Admin Login Name:
Change the built-in admin user name

Admin Email:
Email id for admin account.

Enable Two Factor Authentication For Admin Logins:
Enable Two Factor Authentication for Admin user logins. Requires valid email id.

Select 2FA Delivery Method for Admin:
Enable Two Factor Auth for Admin.

Set Admin 2FA Code Timeout:
Set admin 2FA timeout in minutes

SMS Service Provider:
Master Admin 2FA SMS Provider

Master Admin Phone Number:
Master Admin phone number

- In **Set Admin 2FA Code Timeout**, set the time in minutes that you want the temporary log-in code to remain valid.
- In **SMS Service Provider**, choose **Twilio** or **Custom**.
- 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.

6. To use email authentication, in **Select 2FA Delivery Method for Admin**, choose **Email Authentication**..

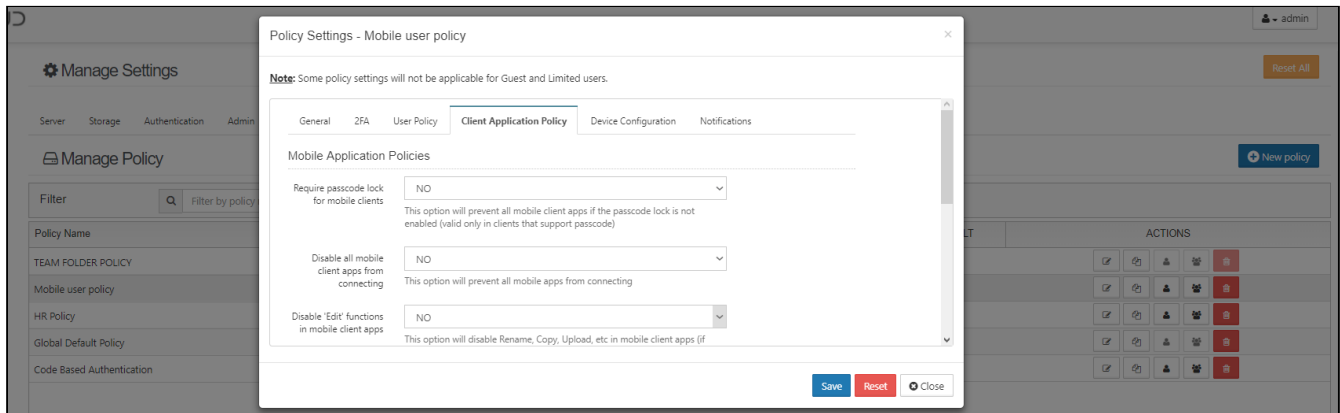
The screenshot shows the 'Admin Settings' page with the following configuration:

- Admin Login Name:** admin
- Admin Email:** [Redacted]@gmail.com
- Enable Two Factor Authentication For Admin Logins:**
- Select 2FA Delivery Method for Admin:** Email Authentication
- Set Admin 2FA Code Timeout:** 5

- Enter a valid email in the **Enable Two Factor Authentication for Admin Logins** field, above the Enable
- In **Set Admin 2FA Code Timeout**, set the time in minutes that you want the temporary log-in code to remain valid.

Setting Client Application Policies

FileCloud allows customizing the client application (Mobile clients, Sync Clients, Drive client) policies.



i FileCloud allows setting global policies that will be applied to all users. But, these policies can be overridden for specific user.

Type	Description
Require Passcode lock for mobile clients	Force mobile clients to enable FileCloud app pincode. If the pincode is not enabled, the login will be rejected with appropriate message
Disable all mobile client apps from connecting	This will prevent login into FileCloud system using mobile client apps (Users will be allowed to login only via the web browser)
Disable edit functions in mobile client apps	This will prevent delete, copy, move operations from being performed from mobile client apps
Disable "Print" option in mobile client apps	This will prevent printing from mobile client apps (At this point only iOS app provides print function)
Disable "Download" option in mobile client apps	This will prevent file download in mobile client apps
Disable "Open with" option in mobile client apps	This will hide option to open a file in third party apps. NOTE: In Android, all files are opened in third party apps and this setting will not affect Android client (otherwise, Android client will be completely useless)
Disable "Share" options in mobile client apps	This will hide file and folder sharing from mobile client apps.

Type	Description
Disable "Add to favorites" options in mobile client apps	This is will hide "Add to favorites" option from mobile client apps

Each of the following policies can be overridden for specific user.

To override the global policy,

- Go to "**Users**" panel in Admin Portal
- Locate the user record (using Filter Users)
- Click on "**Edit**"
- Click on "**Manage Policy**"
- Change the appropriate policy to override

User Details

Name	john	Total Quota	2 GB
Email	john@xyz.com	Used Quota	5.1 GB
Last Login	04 Feb 2018 10:38	Available Quota	0 B
Group	Manage	Used Storage	5.1 GB More

- Mobile Devices
- Manage Files
- Manage Shares
- Reset Password
- Email Password
- Delete Account
- Manage Policy
- Manage Backups

Access Level: Full

Authentication: Default

Email: john@xyz.com

Display Name: john

Account Expires On:

Password Expires On:

Email Verified:

[Save](#) [Close](#)

User Policy : john

Policy Selected 'Mobile user policy' is selected.

Policy Name

- No policy
- TEAM FOLDER POLICY
- Mobile user policy
- HR Policy
- Global Default Policy

Effective Policy

Mobile user policy

Calculate effective policy of the user, as group associations may change enforced policy.

Account Expires On

Password Expires On


Email Verified

User Policy : john


Policy Selected 'Mobile user policy' is selected.

Policy Name


- No policy
- TEAM FOLDER POLICY
- Mobile user policy
- HR Policy
- Global Default Policy

 Clear

Effective Policy

Mobile user policy  Open



Custom Policy assigned to this User

 Close

Account Expires On

Password Expires On

Email Verified

Policy Settings - Mobile user policy - john ×

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

General 2FA User Policy **Client Application Policy** Device Configuration Notifications

Mobile Application Policies

Require passcode lock for mobile clients ▼
 This option will prevent all mobile client apps if the passcode lock is not enabled (valid only in clients that support passcode)

Disable all mobile client apps from connecting ▼
 This option will prevent all mobile apps from connecting

Disable 'Edit' functions in mobile client apps ▼
 This option will disable Rename, Copy, Upload, etc in mobile client apps (if

Using a Proxy Server



As an Administrator, you can configure the settings of a proxy network by enabling proxy 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 may be used to bypass IP address blocking.

Figure 1. General System Settings

The screenshot shows the 'Manage Settings' interface. At the top, there is a gear icon and the text 'Manage Settings'. Below this is a horizontal navigation bar with tabs: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, Policies, SSO, Content Search, Web Edit, Team Folders, and Misc. The 'Misc' tab is currently selected. Underneath the 'Misc' tab, there is a sub-navigation bar with tabs: General, User, Password, Notifications, Share, Preview, Helper, Directory Scraper, and Anti-Virus. The 'General' sub-tab is selected. Below the sub-navigation bar, the text 'General System Settings' is visible.

To configure proxy settings:

1. Log in to the FileCloud Admin portal.
2. On the left *Home* panel, select *Settings*.
3. In the *Manage Settings* section, select the *Misc* tab.
4. From the *Misc* tabs, select *General*.
5. In General System Settings, next to *Enable Proxy Settings*, select the checkbox.
6. In *Proxy Host*, type in the hostname or FQDN of the proxy server in your environment, for example, *<myproxyserver>*
7. In *Proxy Port*, type in the network port on which to communicate with the proxy server. For example, *<8080>*.
8. Many proxy servers require a user to authenticate. In *Proxy Username*, type in the username for the proxy server account.
9. In *Proxy Password*, type in the password for the proxy server account.
10. To save your changes, on the right side of the window, click *Save*.

Figure 2. Proxy Server Settings

The screenshot shows the 'Proxy Server Settings' configuration form. At the top, there is a checkbox labeled 'Enable Proxy Settings' which is checked. Below this is a question: 'Is hosted behind a proxy server?'. There are four input fields, each with a label on the left and a descriptive label below the input field:

- Proxy Host**: Input field for the proxy server hostname or FQDN. Below the field is the label 'Proxy Server Host'.
- Proxy Port**: Input field for the proxy server network port. Below the field is the label 'Proxy Server Port'.
- Proxy Username**: Input field for the proxy server account username. Below the field is the label 'Proxy Server Username'.
- Proxy Password**: Input field for the proxy server account password. Below the field is the label 'Proxy Server Password'.

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.

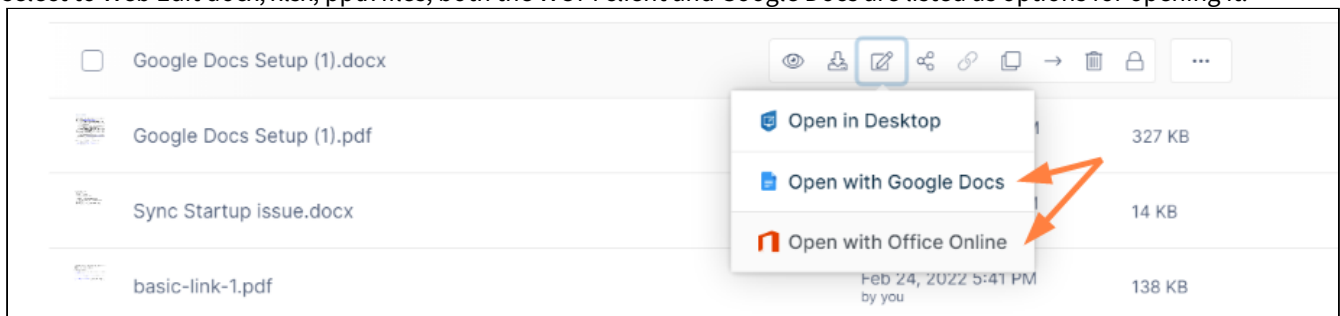
If Web editing is not available in your system, please [Contact FileCloud Support](#).

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 Google Docs are listed as options for opening it:



i In FileCloud's mobile apps, files can be viewed but not edited in Google Apps.

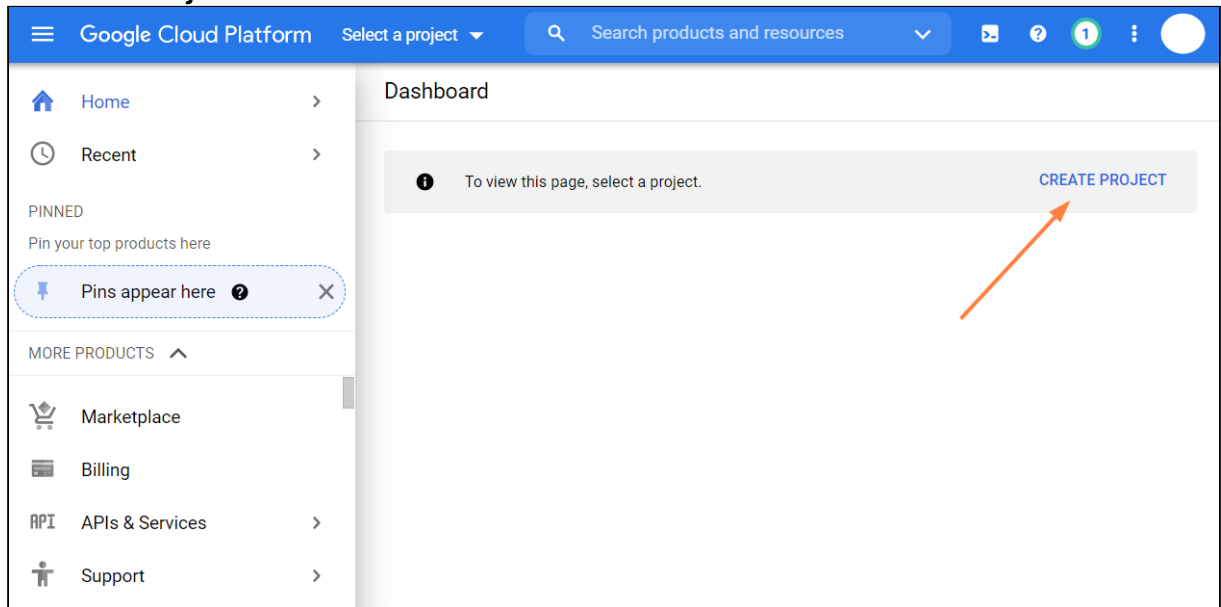
- **!** Editing of some large files is not supported in Google Apps. See [Files you can store in Google Drive](#) for specific size limitations.
- To open a Google Apps editor in incognito windows, you may first have to grant Google Docs the correct permissions or unblock third party cookies.

To integrate with Google Apps:

Set up Google Apps - FileCloud integration in the Google Cloud platform:

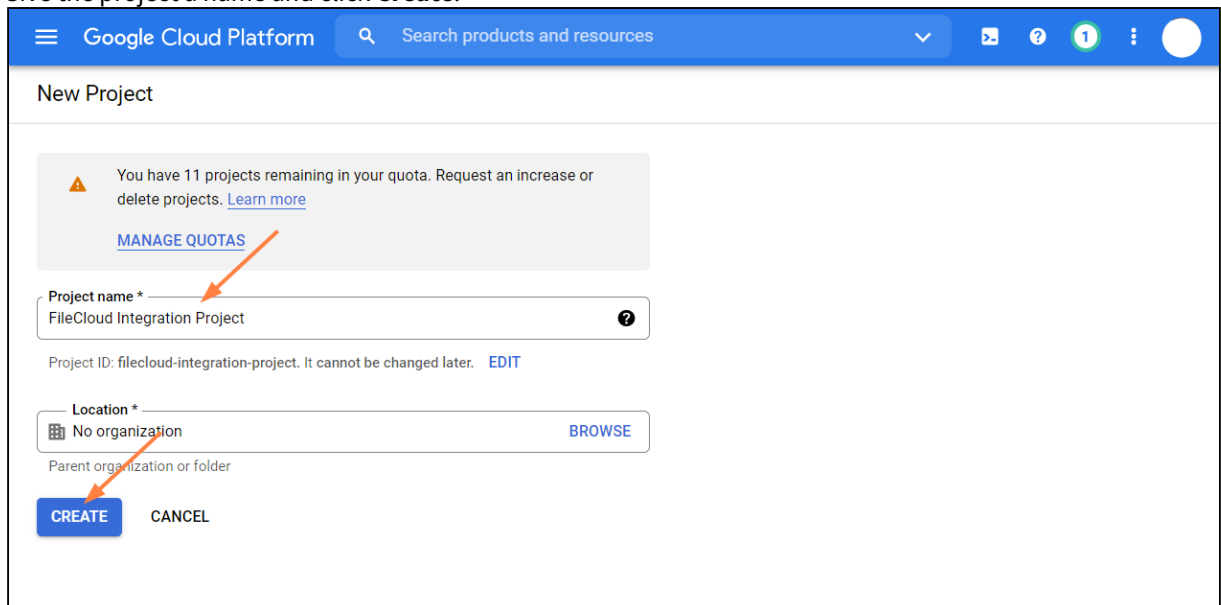
You must have a Google account that you can use to sign in to the Google Cloud Console in order to integrate your system with Google Apps.

1. Access the Google Cloud Console at <https://console.cloud.google.com> and sign in.
2. Go to **Home > Dashboard**.
3. Click **Create Project**.



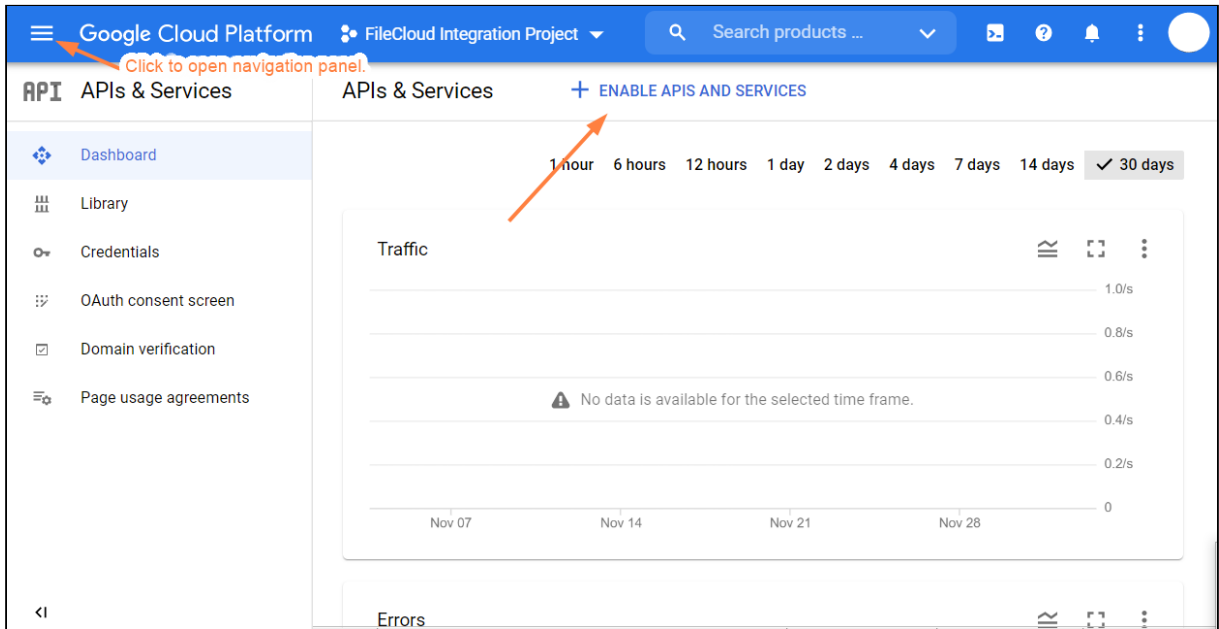
A **New Project** screen opens.

4. Give the project a name and click **Create**.

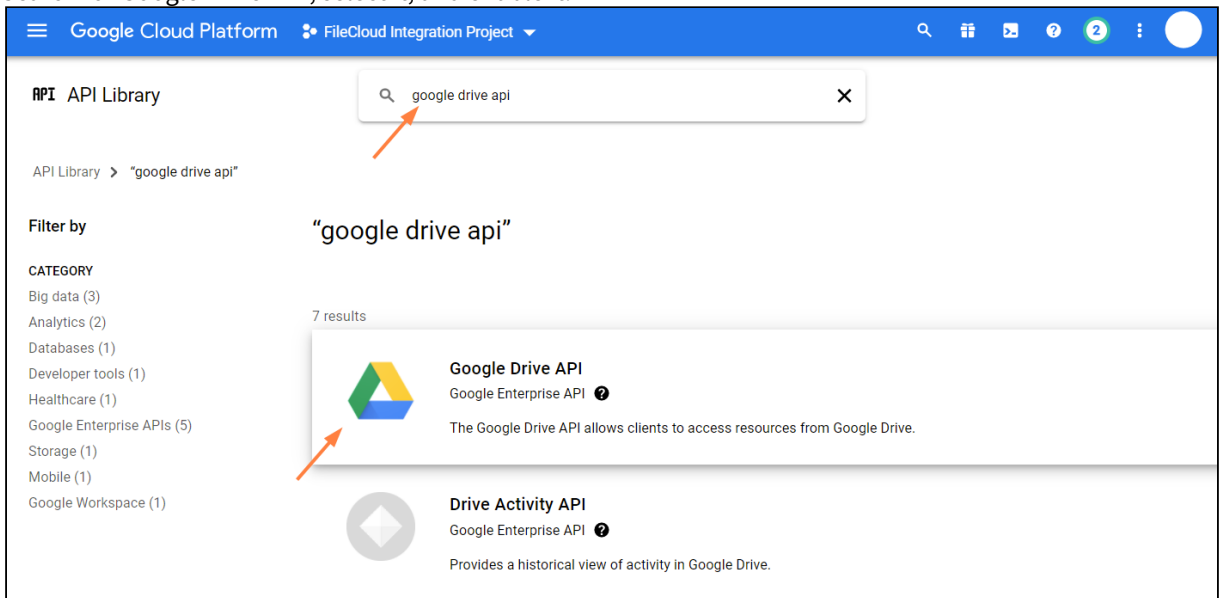


The project opens in the dashboard.

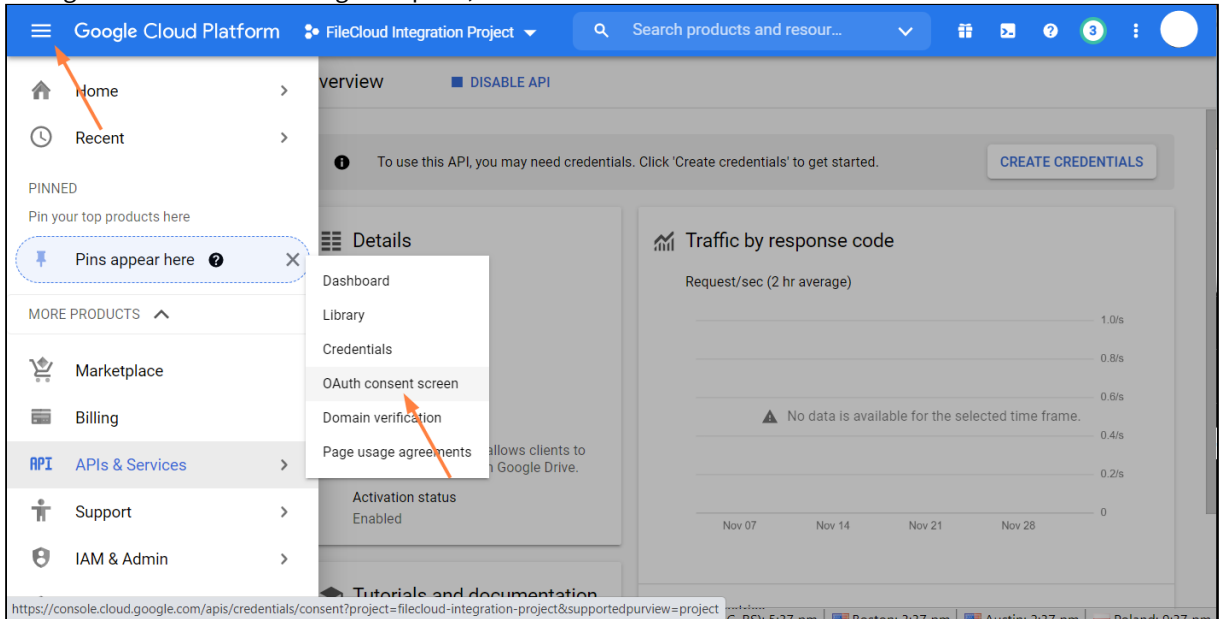
- In the navigation panel, click **APIs & Services > Dashboard**.
(If the navigation panel is not visible, click the three bars in the upper-left corner of the screen to open it.)
- Click **Enable APIs and Services**.



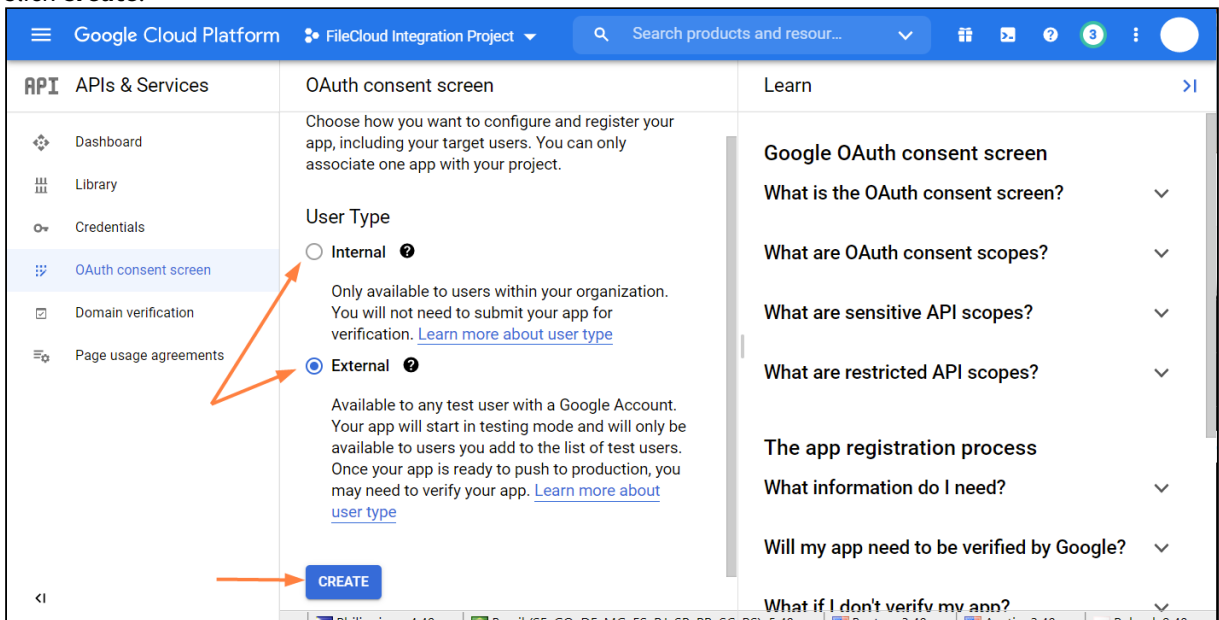
- Search for Google Drive API , select it, and enable it.



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.

- Fill in the required information, and then click **Save and Continue**.

The registration screen for **Scopes** opens:

- Click **Add or Remove Scopes**.
An **Update Selected Scopes** screen opens.
- Scroll to the bottom of the screen and manually add <https://www.googleapis.com/auth/drive.file>. Then click **Add to Table**.

API | .readonly

<input type="checkbox"/>	BigQuery API	.../auth/cloud-platform .read-only	View your data across Google Cloud services and see the email address of your Google Account
<input type="checkbox"/>	BigQuery API	.../auth/devstorage .read-only	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
<input type="checkbox"/>	BigQuery API	.../auth/devstorage .full_control	View your data in Google Cloud Storage
<input type="checkbox"/>	BigQuery API	.../auth/devstorage .read_only	Manage your data in Cloud Storage and see the email address of your Google Account
<input type="checkbox"/>	BigQuery API	.../auth/devstorage .read_write	Manage your data in Cloud Storage and see the email address of your Google Account

Rows per page: 10 | 1 - 10 of 41 | < >

Manually add scopes

If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with 'https://'). When you are finished, click "Add to table".

14. Check it in the table and click **Update**.
It appears under **Your non-sensitive scopes**.

API | APIs & Services | Edit app registration

OAuth consent screen — 2 Scopes — 3 Test users — 4 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

Your non-sensitive scopes

API ↑	Scope	User-facing description	
..	..	See, edit, create, and delete only the specific Google Drive files you use with this app	<input type="button" value="Delete"/>
..	./auth/drive	See, edit, create, and delete only the specific Google Drive files you use with this app	<input type="button" value="Delete"/>
..	.file	See, edit, create, and delete only the specific Google Drive files you use with this app	<input type="button" value="Delete"/>

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**.

The screenshot shows the Google Cloud Platform console for the 'FileCloud Integration Project'. The left navigation panel has 'OAuth consent screen' selected. The main content area shows the 'FileCloud' app details, including 'Publishing status', 'Testing' (with a 'PUBLISH APP' button highlighted by a red arrow), 'User type' (set to 'External'), and 'OAuth user cap'. A 'Learn' sidebar on the right contains various help links related to OAuth consent screens.

18. In the navigation panel, click **Credentials**, and in the **Credentials** screen, click **Create Credentials**, and choose **OAuth client ID**.

The screenshot shows the Google Cloud Platform console for the 'FileCloud Integration Project'. The left navigation panel has 'Credentials' selected. The main content area shows the 'Credentials' screen with a '+ CREATE CREDENTIALS' button and a 'DELETE' button. A dropdown menu is open, showing options: 'API key', 'OAuth client ID' (selected with a red arrow), 'Service account', and 'Help me choose'. Below the dropdown, there are sections for 'API Keys', 'OAuth 2.0 Client IDs', and 'Service Accounts', each with a table of existing credentials.

The Create OAuth Client ID screen opens.

Google Cloud Platform | FileCloud Integration Project | Search products and resources

API APIs & Services | Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
FileCloud Web client

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins

For use with requests from a browser

+ ADD URI

Authorized redirect URIs

For use with requests from a web server

URIs *

https://www.myfilecloud.com/core/googledocsoauth

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:


OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is verified. This may require a verification process that can take several days.

Your Client ID

Your Client Secret

 **DOWNLOAD JSON**

[OK](#)

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).

Webmaster Central

Use the table below to manage verified owners of your properties or to add new properties to your account

ADD A PROPERTY

Enter the URL of the property that you'd like to verify.

Example: <http://www.example.com/>

3. Click **Continue**.

Webmaster Central

Verify your ownership of <https://www.myfilecloud.com/>. [Learn more](#).

Your Google Account will be recorded in Google's systems as an official owner of this property.
Note - your ownership information will be stored and be visible to other owners (both current and future).

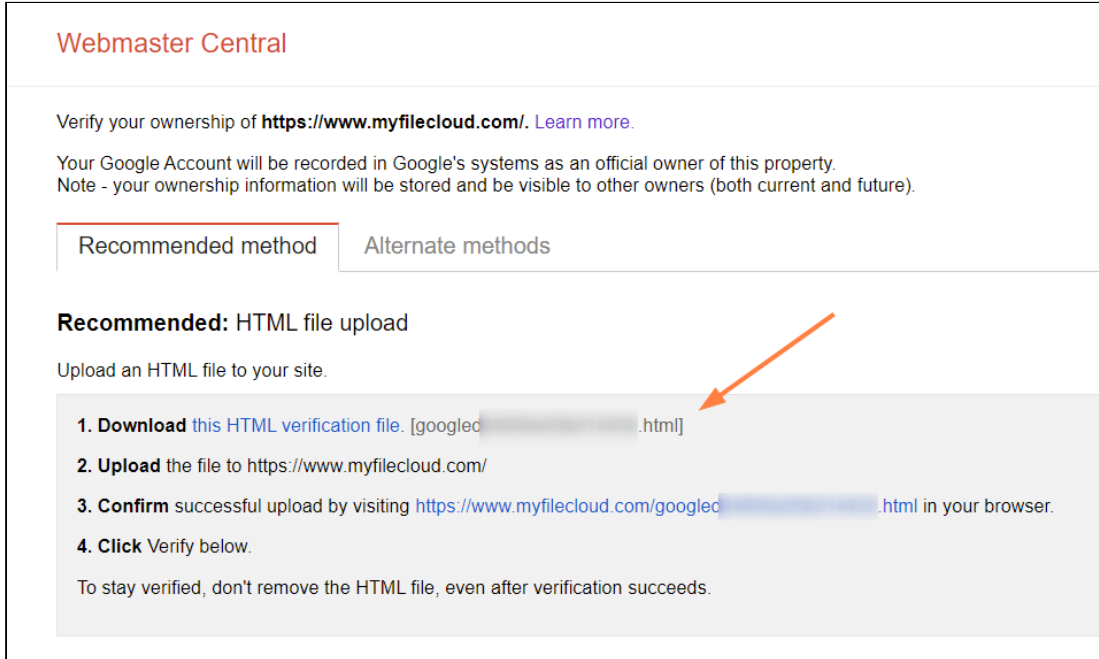
Recommended method Alternate methods

Recommended: HTML file upload

Upload an HTML file to your site.

1. Download [this HTML verification file](#). [googled[redacted].html]
2. Upload the file to <https://www.myfilecloud.com/>
3. Confirm successful upload by visiting [https://www.myfilecloud.com/googled\[redacted\].html](https://www.myfilecloud.com/googled[redacted].html) in your browser.
4. Click Verify below.

To stay verified, don't remove the HTML file, even after verification succeeds.



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.

Google Apps Access

Enable Google Apps

Click to edit documents using Google Docs/Sheets/Slides

Google Server Idle Session Timeout

Enter idle session expiry time (in minutes from 5 to 1440) in which the edit will be considered finished

Google OAuth Client ID

Upload OAuth Client ID (.json)

client_secre...ent.com.json

Upload the client secret JSON file to be used to access Google Docs via the OAuth method

Google's Domain Verification File

Upload Google's Domain Verification File (.html)

google4f3c...e19747.html

Upload HTML file to be used to verify your domain

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

Introduction

Starting in v17.x, FileCloud supports creating new documents 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.

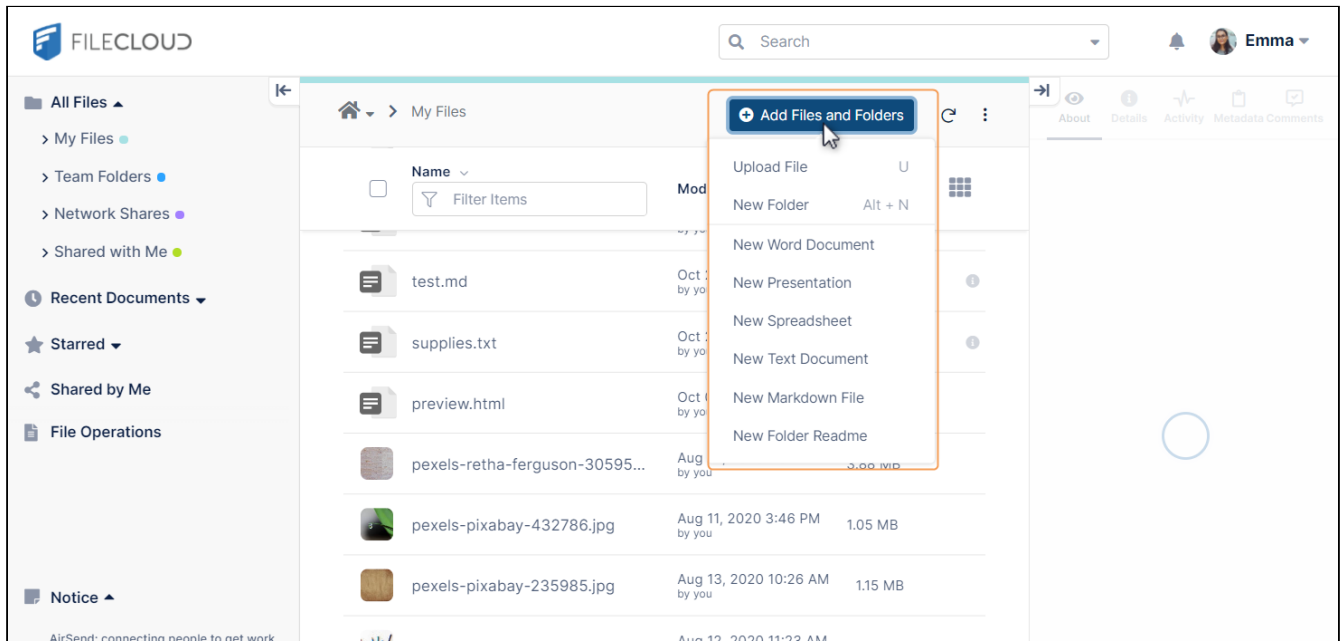
To enable new document creation

- Enable **Show New Document Creation Option** in **Customization > General > UI Features**.

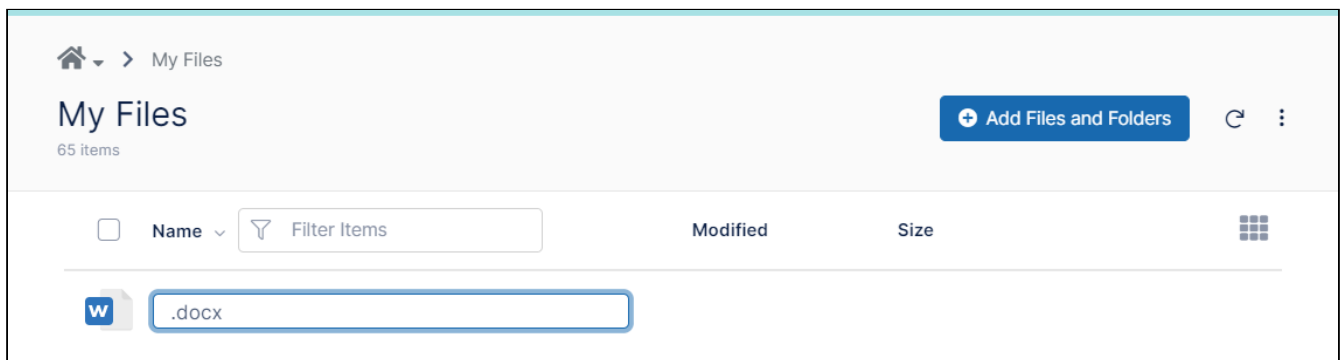
The screenshot shows the FileCloud administration interface. The left sidebar contains navigation menus for Admins, MANAGE (Team Folders, Network Folders, User Shares, Folder Permissions), DEVICES (Devices), MISC. (Audit, Alerts, User Locks, Workflows, Reports, Federated Search, Metadata), SETTINGS (Settings), and CUSTOMIZATION (Customization). The main content area is titled 'Manage User UI Customizations' and has several tabs: General, Labels And Logos, URL, UI Messages, Email Templates, News Feed, TOS, and Advanced. Under the 'General' tab, there are sub-tabs for 'UI Features', Login, Account Menu, and Listing. The 'UI Features' sub-tab is active, showing a list of features to customize. The 'Show New Document Creation Option' feature is checked, and an orange arrow points to its checkbox.

Feature	Enabled	Description
Enable UI Customizations	<input checked="" type="checkbox"/>	Enable UI customization
Show Document Preview	<input checked="" type="checkbox"/>	Show "Preview" in document file menu options (Requires "Document Preview" configured)
Show Single File Share Full Preview	<input type="checkbox"/>	Show full screen preview for single file public shares
Show New Document Creation Option	<input checked="" type="checkbox"/>	Show new document creation option in the folder menu
Show Quick Edit Option	<input checked="" type="checkbox"/>	Show "Quick Edit" (Requires user to install CloudSync client)

Now, in 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 user's cursor is placed in the name. The extension is already entered. The user must type in a name, and click Enter. The document opens for edit.

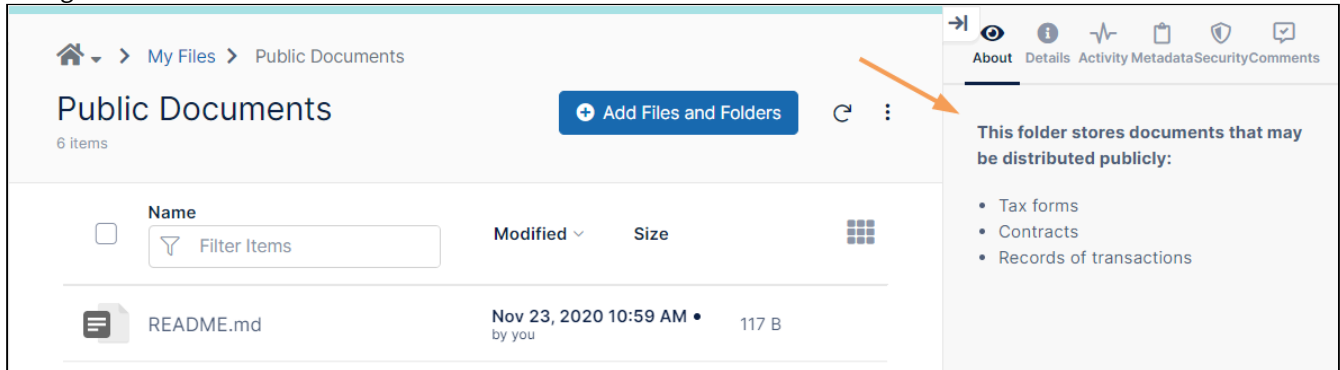


Readme files

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

Introduction

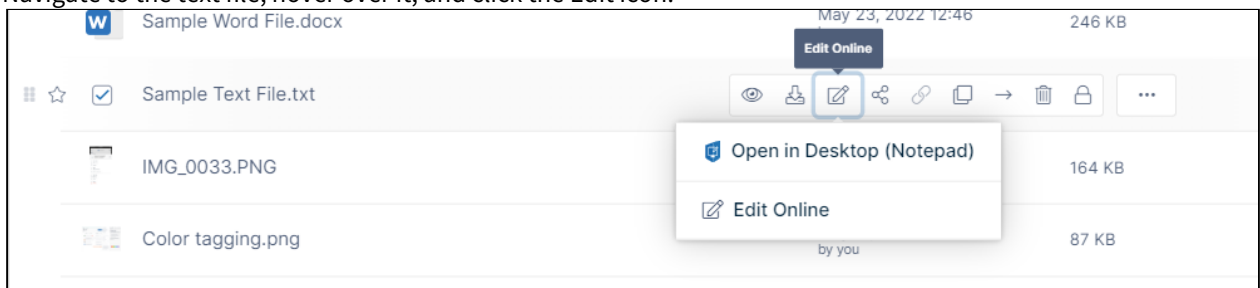
Starting with v17.x, FileCloud supports editing text files from within a browser session. This support is enabled irrespective of WOPI configuration, as editing of text files uses a built-in widget.

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

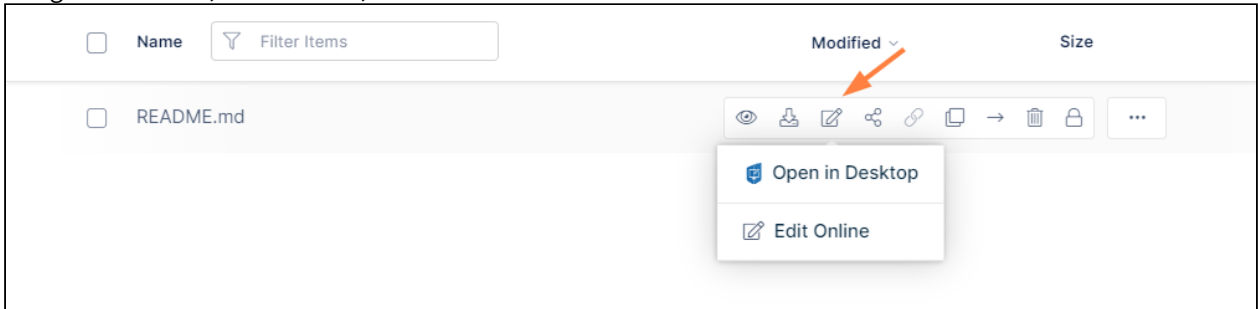
Starting with version 20.2, FileCloud supports editing markdown files from within a browser session. It also supports editing readme files, which are a form of markdown files and use the same types of editors.

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..

i 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

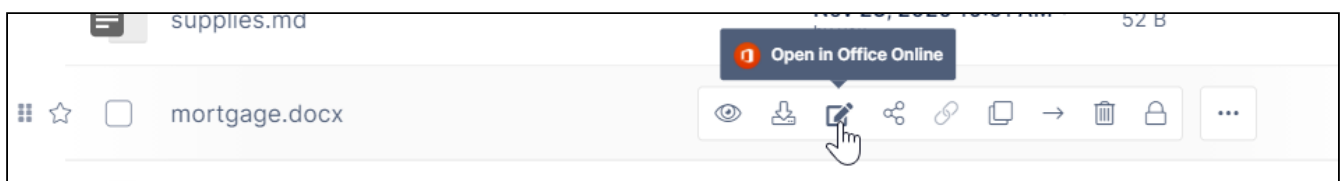
Beginning with v17.x, FileCloud supports coauthoring of Office document files from within a browser session.

Introduction

Coauthoring occurs when two users are editing the same document and can view each other's changes as they make them.

Only .docx, .xlsx, and .pptx documents can be coauthored.

To open an Office file in web edit, hover over the file and click the **Web Edit** icon. Since you are editing an Office document, the tooltip displays **Open in Office Online** rather than **Web edit**.



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

The ability to hide the Web Edit button is available in FileCloud Server version 19.1 and later.


You can decide not to allow your users to edit documents in a browser.

After an administrator configures online editing, FileCloud users can login 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 gets saved in FileCloud automatically.


If an administrator does not want to support this feature, the Web Edit button can now be removed from the User Portal for:

- a single user - in the user's policy
- a group of users - in the group's policy
- all users - in the *Global Default Policy*


To hide the Web Edit button for a single user:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *USERS/GROUPS*, select *Users*.
3. On the *Manage Users* screen, in the row of the user you want to modify, click the *Manage Policies* () button.
4. On the *Policy Settings* dialog, select the *User Policy* tab.
5. Next to the *Enable Web Edit Feature* label, select *NO*.
6. Click *Save*.

To hide the Web Edit button for a group:

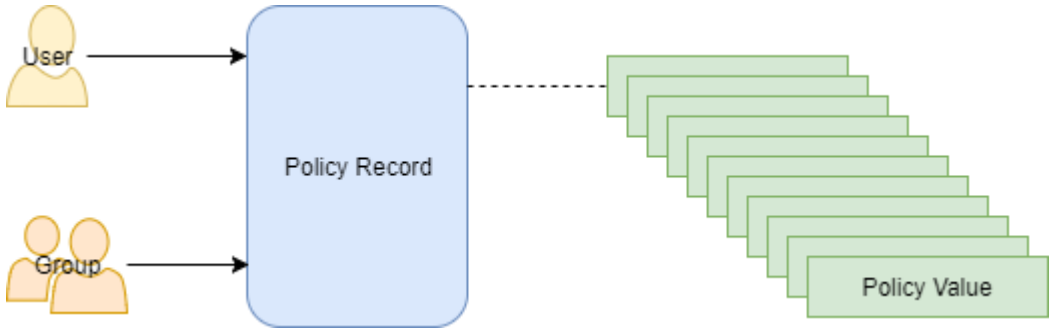
1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *USERS/GROUPS*, select *Groups*.
3. On the *Manage Groups* screen, in the row of the group you want to modify, click the *Manage Policies* () button.
4. On the *Policy Settings* dialog, select the *User Policy* tab.
5. Next to the *Enable Web Edit Feature* label, select *NO*.
6. Click *Save*.

To hide the Web Edit button for all users:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, in the row of the *Global Default Policy*, click the *Edit* () button.
4. On the *Policy Settings* dialog, select the *User Policy* tab.
5. Next to the *Enable Web Edit Feature* label, select *NO*.
6. Click *Save*.

Policies

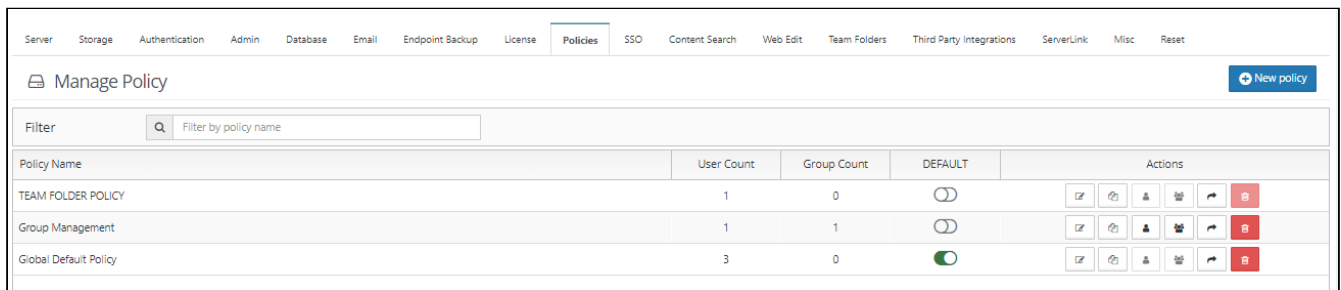
i Policies are available in FileCloud 17.3 and later.



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 click the **Policies** tab.



The policy values in Table 1 are managed in a policy record.

Table 1. Policy Values

Client Application Policy	Default Value	Version Available
Mobile Application Policies		
Require Passcode for Mobile Apps	NO	
Disable Mobile Apps from Connecting	NO	
Disable "Edit" Option in Mobile Apps	NO	

Client Application Policy	Default Value	Version Available
Disable Printing in Mobile Apps	NO	
Disable Downloads in Mobile Apps	NO	
Disable "Open With" in Mobile Apps	NO	
Disable Sharing in Mobile Apps	NO	
Disable "Add to Favorite" in Mobile Apps	NO	
Disable Configuration Changes in Clients	NO	
Apply Configuration in Client		
2FA		
Enable 2FA	NO	
2FA Delivery Mode	Email	
Notifications		
Disable All Notifications	NO	
Disable User Override of Notification Settings	NO	
Disable Add Notification	NO	
Disable Update Notification	NO	
Disable Delete Notification	NO	
Disable Download Notification	NO	
Disable Preview Notification	NO	
Disable Lock/Unlock Notification	NO	

Client Application Policy	Default Value	Version Available
Disable Share Notification	NO	
Disable Rename Notification	NO	
Disable Self Notification	NO	
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	NO	
Automatically Delete Files from Recycle Bin After Set Number of Days	0	
Do Not Store Deleted Files Greater Than	100 MB	
User Policy		
Disable User Invites	NO	
Create Account on New User Shares	NO	
Enable Code Based Client Authentication	NO	

Client Application Policy	Default Value	Version Available
Admin Approval Required for Code Based Authentication	NO (Only enabled if Enabled Code Based Client Authentication is set to YES.)	
Enforce Session Timeout for Devices	NO (Only enabled if Enabled Code Based Client Authentication is set to YES.)	
Allow Folder Level Security	YES	
Enable Web Edit Feature	YES	
Enable Recycle Bin Clear Feature	YES	
Disallow Default Share Settings Change	NO	
Disable Everyone Group Sharing	NO	
Allow New Group Creation	NO	FileCloud 21.2
Allow User Group Management (Add and Remove users)	NO	FileCloud 21.2
Allow Group Deletion	NO	FileCloud 21.2
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
Max File Size Limit	0	FileCloud 22.1
Save Zip File Session Password	YES	FileCloud 22.1

Working with Policy Records


Accessing Policy Records


To access a policy record:

1. Log into the Admin Portal.
2. Click *Settings*.
3. Click the *Policies* tab.


Creating a New policy Record

To create a policy:

1. Log into the *Admin Portal*.
2. Click *Settings*.
3. Click the *Policies* tab, and then click the *New policy* button.
4. In the *New policy* window, in *Policy Name*, type in a unique identifier for this policy, and then click *Create*.
5. On the *Policies* tab, in the *Manage Policy* section, select the policy you just created.
6. To configure the policy, click the *edit policy* icon  .

 Instead of creating a new policy, you have the option to copy an existing policy.


To copy a policy:

1. Log into the Admin Portal.
2. Click *Settings*.
3. Click the *Policies* tab.
4. In the *Manage Policy* section, select the policy you want to copy.
5. To copy the policy, click the copy policy icon  .

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. Log into the Admin Portal.
2. Click *Settings*.
3. On the *Policies* tab, to open the *Manage Policy Users* window, click the users icon .
4. In the *Manage Policy Users* window, in *Available Users*, select a user.

5. Use the arrow to move the user to the *Policy Users* list box.
6. To save your changes, click *Close*.

To assign a group to a policy:

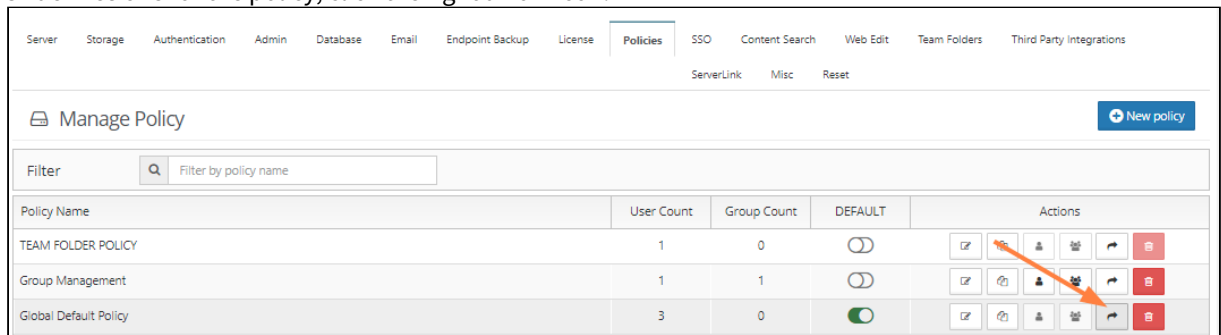
1. Log into the Admin Portal.
2. Click *Settings*.
3. On the *Policies* tab, to open the *Manage Policy Groups* window, click the groups icon .
4. In the *Manage Policy Groups* window, in *Available Groups*, select a group.
5. Use the arrows to move the group to the *Policy Groups* list box.
6. To save 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. Go to **Settings > Policies**.
2. Under **Actions** for the policy, click the right arrow icon.



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:

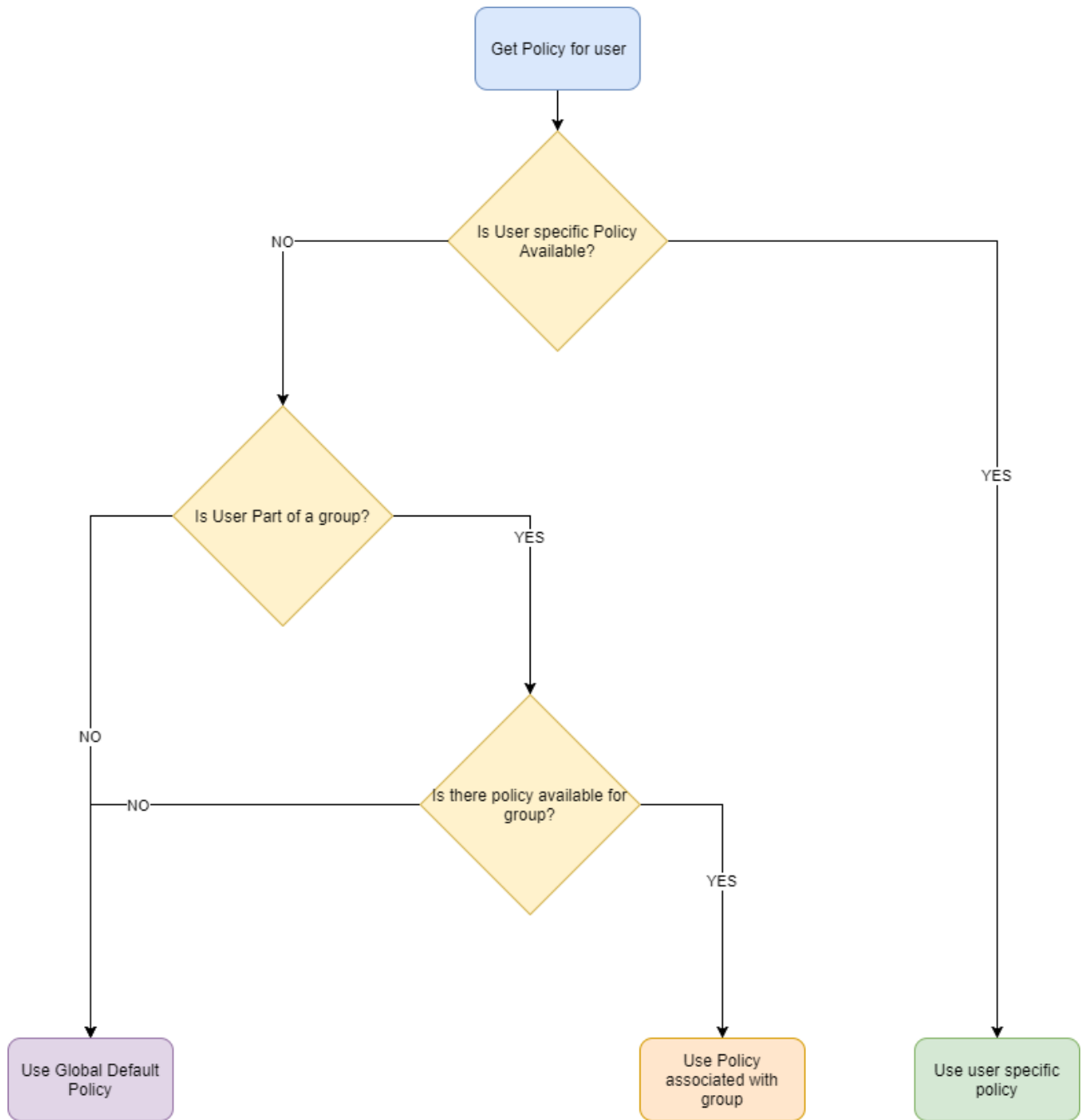
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotifications	LastLogin	Authentication Type	MobilePhone	Effective Policy	
2	david	dm898002@gmail.co	david	FULL			EVERYON	YES	NO	10/4/2021 15:16	Default		Group Management	
3	jaredtaylor9	jaredtaylor978@gmail	Jared	FULL			EVERYON	YES	NO	10/18/2021 12:36	Default		Global Default Policy	
4	jessicam	jm2344311@gmail.cc	Jessica	FULL			EVERYON	YES	NO	2/10/2022 14:08	Default		Global Default Policy	
5														

 **Manage the Recycle Bin Using Policies**

Policy Calculations Best Practices

An effective policy for a user is calculated on multiple factors as shown in Figure 2.

Figure 2. Effective Policy Calculation Flow Chart



Policy Selection Scenarios

Case 1: User with no policy assigned : **Global Default Policy will be used**

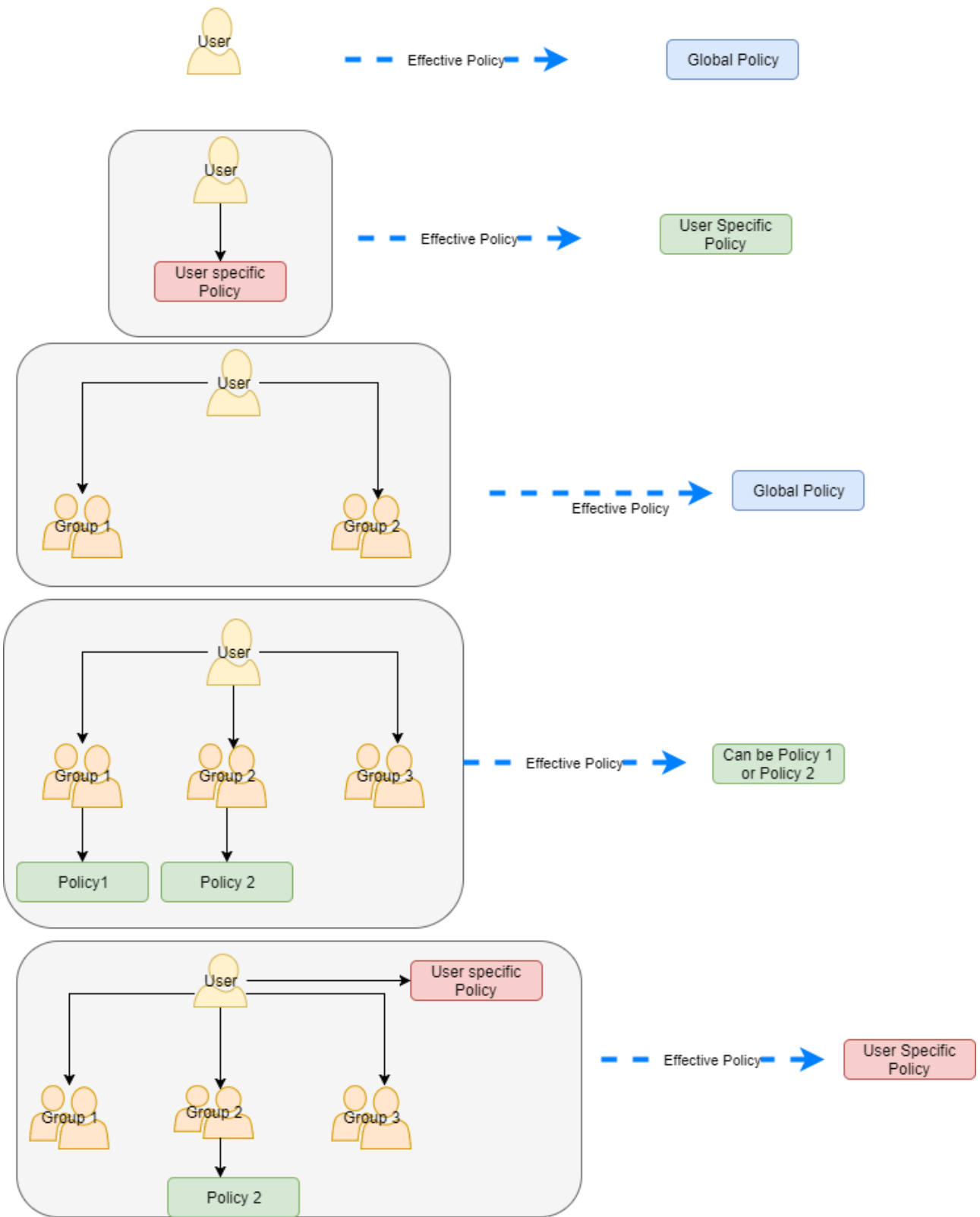
Case 2: User with specific policy assigned: **Assigned policy will be used**

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 policy 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**

Figure 3. Selecting a Policy Scenario Flow Chart



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 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 **Settings > Policies** or in **Settings > Misc > Notifications**.

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.

When were digest notifications last generated

You can now see when the cron job that generates digest notifications was last run.

 This option is only available in FileCloud Server version 19.1 and later.

Server	Storage	Authentication	Admin	Database	Email	Endpoint Backup
Third Party Integrations		Misc	Reset			
General	User	Password	Notifications	Share	Preview	Support Services

Notification Settings

Enable File Change Notifications

Enable Notifications on File Change

Enable Email File Change Notifications

Enable to send Email Notifications on File Change

Disable Notifications for External Accounts

Disable notifications for external user accounts

Enable Share Notification

Default Setting to enable or disable notifications for a share

Enable new version email notification

Enable new version email notification. It will be sent to admin once a week.

Number Of Days After Which Notifications Are Not Sent

Do not send email notifications for actions that occurred before the set number of days.

Email Notification Frequency

How many minutes before the system sends another email notification.

Last run was on 2022-09-16 13:20:02

To see when digest notifications were last generated:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. On the *Manage Settings* screen, select the *Misc*. tab, and then the *Notifications* tab.
4. Look under the field labeled *Email Notification Frequency*.

Changing notification settings

Global notification settings

Enable or Disable ALL Notifications

The screenshot shows the 'Misc' tab in the FileCloud Admin portal. The 'Notifications' sub-tab is selected. Two settings are highlighted with orange boxes:

- Enable File Change Notifications** (checked): Enable Notifications on File Change
- Enable Email File Change Notifications** (checked): Enable to send Email Notifications on File Change

To enable file change notifications:

1. Open a browser and log on to the *Admin* portal.
2. From the left navigation panel, click *Settings*.
3. On the *Manage Settings* screen, click the *Misc* tab, and then the *Notifications* sub-tab.
4. To display notifications of file changes on the user portal, check *Enable File Change Notifications*.
5. 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.
6. Click *Save*.

i 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. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. On the *Manage Settings* screen, select the *Misc.* tab, and then the *Notifications* tab.
4. Find the a field labeled *Email Notification Frequency*.

The screenshot shows the Admin Portal interface. At the top, there are navigation tabs: Server, Storage, Authentication, Admin, Database, Email, and Endpoint Backup. Below these, there are sub-tabs: Third Party Integrations, **Misc**, and Reset. Under the **Misc** tab, there are further sub-tabs: General, User, Password, **Notifications**, Share, Preview, and Support Services. The **Notifications** sub-tab is active, showing the following settings:

- Enable File Change Notifications
 - Enable Notifications on File Change
- Enable Email File Change Notifications
 - Enable to send Email Notifications on File Change
- Disable Notifications for External Accounts
 - Disable notifications for external user accounts
- Enable Share Notification
 - Default Setting to enable or disable notifications for a share
- Enable new version email notification
 - Enable new version email notification. It will be sent to admin once a week.
- Number Of Days After Which Notifications Are Not Sent
 - Input field: 7
 - Do not send email notifications for actions that occurred before the set number of days.
- Email Notification Frequency** (highlighted with an orange box)
 - Input field: 15
 - How many minutes before the system sends another email notification.
 - Last run was on 2022-09-16 13:20:02

5. Change the value.
6. 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 not send email notifications that were created a specified number of days ago (by default, 7 days). This prevents the system from sending notifications that remained in the email queue for a number of days and may have messages that are no longer relevant or accurate.

To prevent sending notifications after a specific number of days:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *Settings*, select *Settings*.
3. On the *Manage Settings* screen, select the *Misc.* tab, and then the *Notifications* tab.
4. In the *Number of Days After which Notifications Are Not Sent*, type in a number.
Enter 0 to disable notifications.

Server Storage Authentication Admin Database Email Endpoint Backup

Third Party Integrations **Misc** Reset

General User Password **Notifications** Share Preview Support Services

Notification Settings

Enable File Change Notifications
 Enable Notifications on File Change

Enable Email File Change Notifications
 Enable to send Email Notifications on File Change

Disable Notifications for External Accounts
 Disable notifications for external user accounts

Enable Share Notification
 Default Setting to enable or disable notifications for a share

Enable new version email notification
 Enable new version email notification. It will be sent to admin once a week.

Number Of Days After Which Notifications Are Not Sent

 Do not send email notifications for actions that occurred before the set number of days.

Email Notification Frequency

 How many minutes before the system sends another email notification.
 Last run was on 2022-09-16 13:20:02

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

The screenshot shows the Admin Portal interface. At the top, there are navigation tabs: Server, Storage, Authentication, Admin, Database, Email, and Endpoint Backup. Below these, there are sub-tabs: Third Party Integrations, Misc (selected), and Reset. Under the Misc tab, there are further sub-tabs: General, User, Password, Notifications (selected), Share, Preview, and Support Services. The main content area is titled 'Notification Settings' and contains several options:

- Enable File Change Notifications: Enable Notifications on File Change
- Enable Email File Change Notifications: Enable to send Email Notifications on File Change
- Disable Notifications for External Accounts: Disable notifications for external user accounts** (This section is highlighted with a red box in the image)
- Enable Share Notification: Default Setting to enable or disable notifications for a share
- Enable new version email notification: Enable new version email notification. It will be sent to admin once a week.
- Number Of Days After Which Notifications Are Not Sent: Do not send email notifications for actions that occurred before the set number of days.
- Email Notification Frequency: How many minutes before the system sends another email notification. Last run was on 2022-09-16 13:20:02

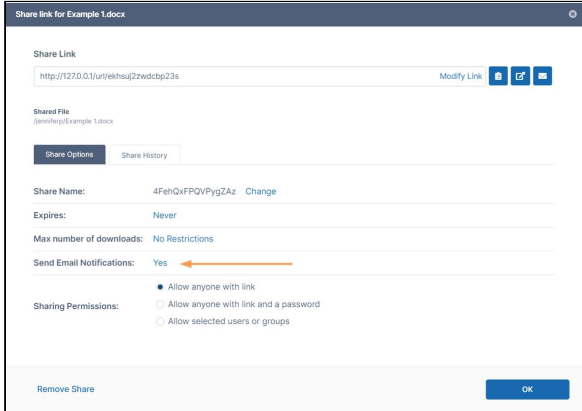
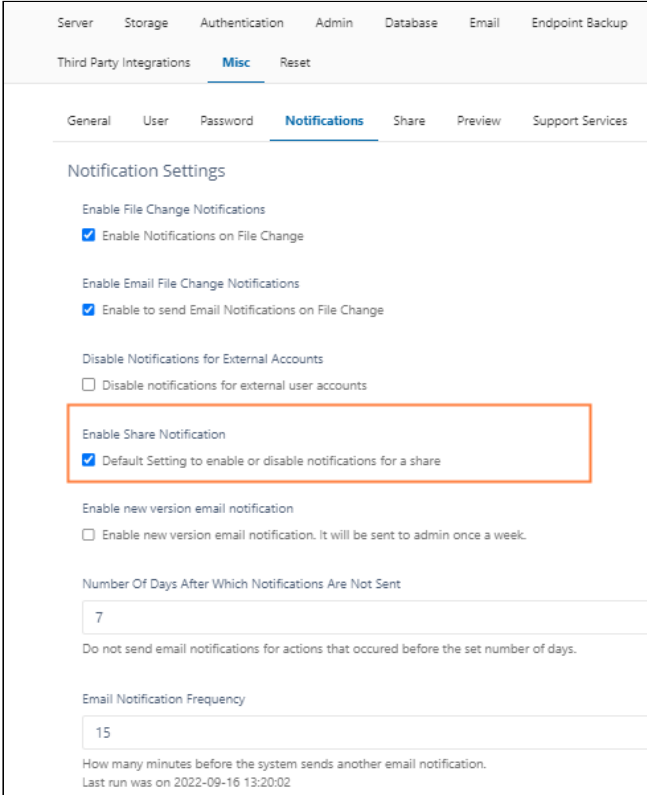
2. From the left navigation pane, under *Settings*, select *Settings*.
3. On the *Manage Settings* screen, select the *Misc.* tab, and then the *Notifications* tab.
4. To stop sending notifications, select the *Disable Notifications for External Accounts* checkbox.
5. Save your changes

Sharing Notifications

When a File or Folder is shared, the owner can allow or restrict file change notifications for all users that have access to that share.

- Enabling this setting sends an email notification when a file is opened or downloaded for a public share.
- 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
	
<p>To share a file with everyone without restrictions:</p> <ol style="list-style-type: none"> 1. Open a browser and log in to the <i>User Portal</i>. 2. In the <i>User Portal</i>, click <i>My Files</i>. 3. Hover over the file you want to share. 4. Click the <i>Share</i> icon. 5. On the <i>Share Link for File</i> dialog box, click <i>Share Options</i> 6. In <i>Share Options</i>, set <i>Send Email Notifications</i> to YES. 	<p>To enable File Change Notifications for Shares:</p> <ol style="list-style-type: none"> 1. Log in to the <i>Admin Portal</i>. 2. From the left navigation pane, select <i>Settings</i>. 3. Select <i>Misc.> Notifications</i>. 4. Select <i>Enable Share Notification</i>. 5. Click <i>Save</i>.

Policy notification settings

User and Group Notifications

The ability to enable or disable notifications through policies is available in FileCloud Server version 17.3 and later. Notification settings can be set for a specific policy and that policy can be applied at group or user level.

- For example, notifications can be enabled for all users in the Global Default Policy.
- Notifications can also be disabled for a specific user or group by defining a policy and disabling the notification.

Administrators can configure how notifications will work by using the following settings. Note that unless **Disable User Override** is checked, users can override all of these settings except for **Disable Notifications**.

Policy Settings - Global Default Policy

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

General
2FA
User Policy
Client Application Policy
Device Configuration
Notifications

Manage File Change Notifications

Disable Notifications

Disable all notifications

Disable User Override

Do not allow notification setting override by user. This is applicable only when Disable Notifications option above is not selected.

Disable Add Notifications NO ▼

Do not send notifications when new file is added to a shared folder.

Disable Update Notifications NO ▼

Do not send notifications when a shared file is updated.

Disable Delete Notifications NO ▼

Do not send notifications when a shared file is deleted.

Disable Download Notifications NO ▼

Do not send notifications when a shared file is downloaded.

Disable Preview Notifications NO ▼

Do not send notifications when a shared file is previewed.

Disable Lock/Unlock Notifications	NO	Do not send notifications when a shared file is locked or unlocked.
Disable Share Notifications	NO	Do not send notifications when a shared file is shared.
Disable Rename Notifications	NO	Do not send notifications when a shared file is renamed.
Disable Self Notifications	NO	Do not send notifications to the user when action is done by the same user.

Save

Reset

Close

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.

To customize notifications in a policy:

1. Open a browser and log on to the *Admin* portal.
2. From the left navigation panel, under *SETTINGS*, click *Settings*.
3. On the *Manage Settings* screen, click the *Policies* tab.
4. On the *Policies* screen, click the row of the policy you want to customize.
5. On the Manage Policy dialog box, select the Notifications tab.
6. In the Manage File Change Notifications section, set the options as you want to use them.
7. 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:

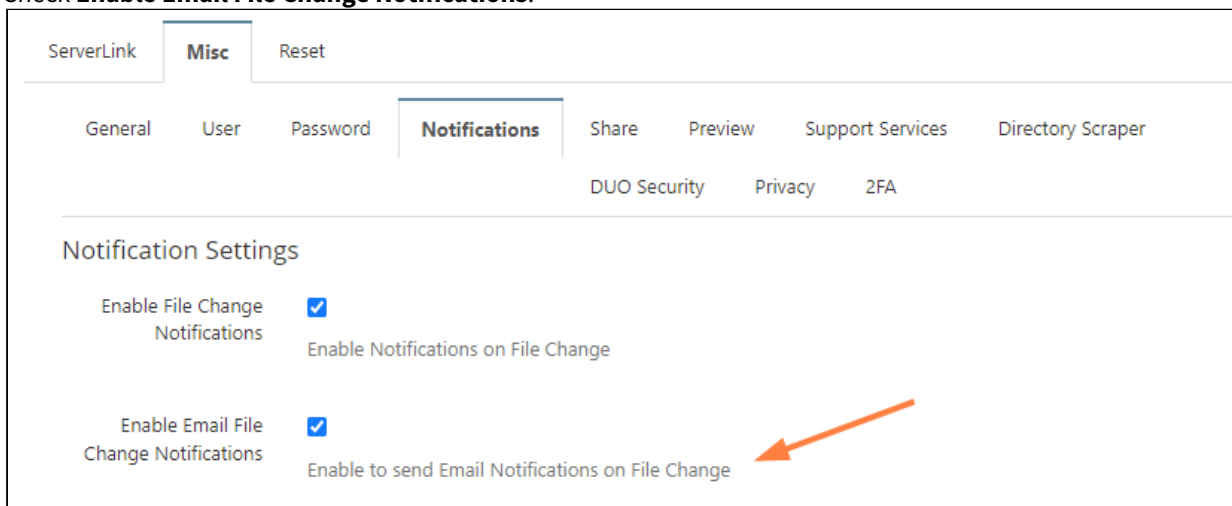
- new help requests are uploaded so they can begin processing them
- existing help requests are deleted in case they have begun addressing them.

To prevent accidental changes to these notifications, you do not allow users to change the notification settings.

To configure these settings

These are the steps you (the admin) use to set up the notifications according to these requirements:

1. To enable email notifications globally, in the FileCloud admin portal, go to **Settings > Misc > Notifications**.
2. Make sure **Enable File Change Notifications** is checked; if it is not checked, **Enable Email File Notifications** is not available.
3. Check **Enable Email File Change Notifications**.



4. To set up the update and delete notifications for support personnel, go to **Settings > Policies**.
5. Edit the policy assigned to support personnel.
6. Click the **Notifications** tab.


7. Uncheck **Disable Notifications**, and check **Disable User Override**.


Policy Settings - Support Policy

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

General 2FA User Policy Client Application Policy Device Configuration **Notifications**

Manage File Change Notifications

Disable Notifications 
Do not send notifications when a shared file is changed.

Disable User Override 
Do not allow notification setting override by user. This is applicable only when Disable Notifications option above is not selected.

Disable Add Notifications
Do not send notifications when new file is added to a shared folder.


Save Reset Close

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 **No**. Change the other **Disable Notification** settings to **Yes**.


Policy Settings - Support Policy

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

Disable Add Notifications
Do not send notifications when new file is added to a shared folder.

Disable Update Notifications 
Do not send notifications when a shared file is updated.

Disable Delete Notifications
Do not send notifications when a shared file is deleted.

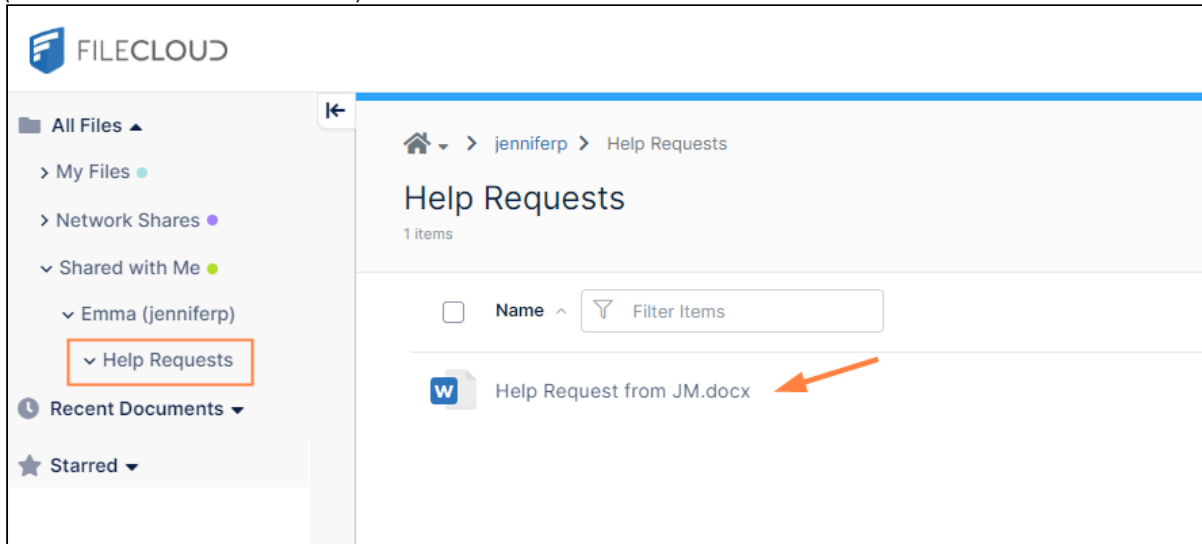
Disable Download Notifications 
Do not send notifications when a shared file is downloaded.

Save Reset Close

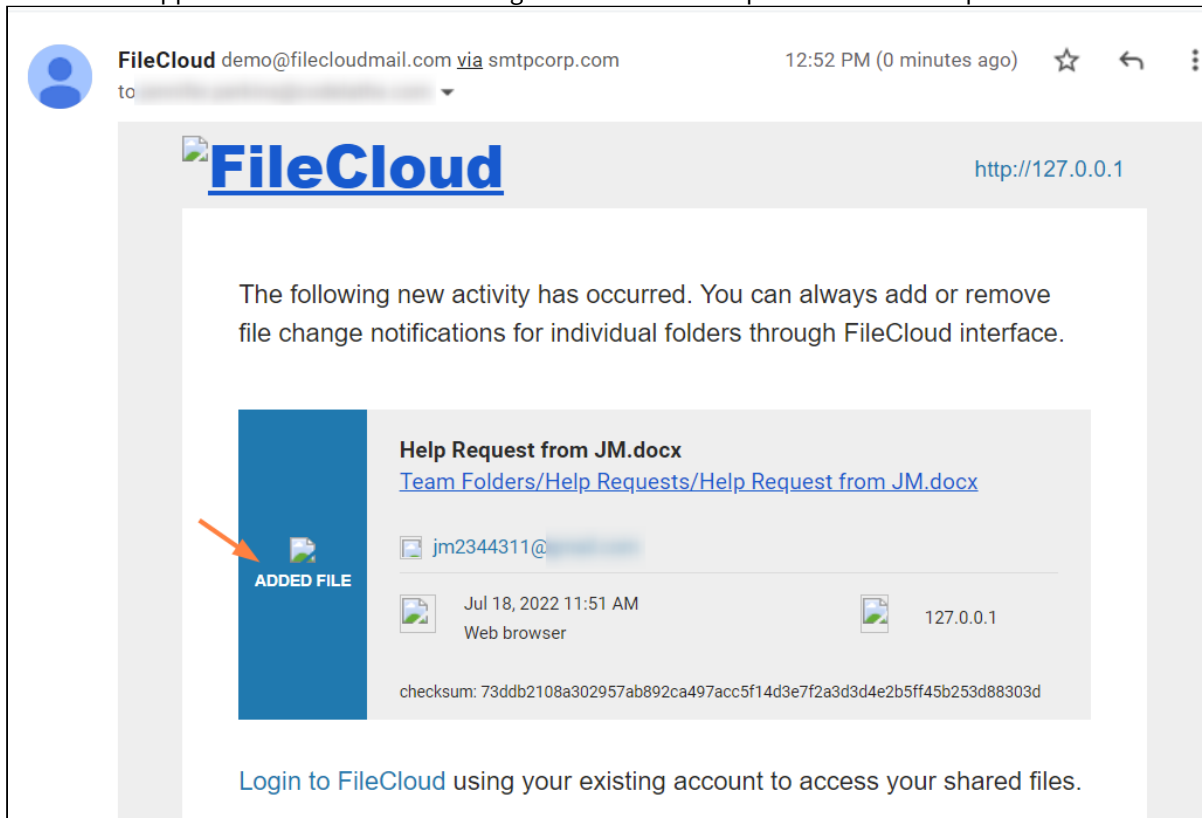
9. Save your changes.

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**) . . .

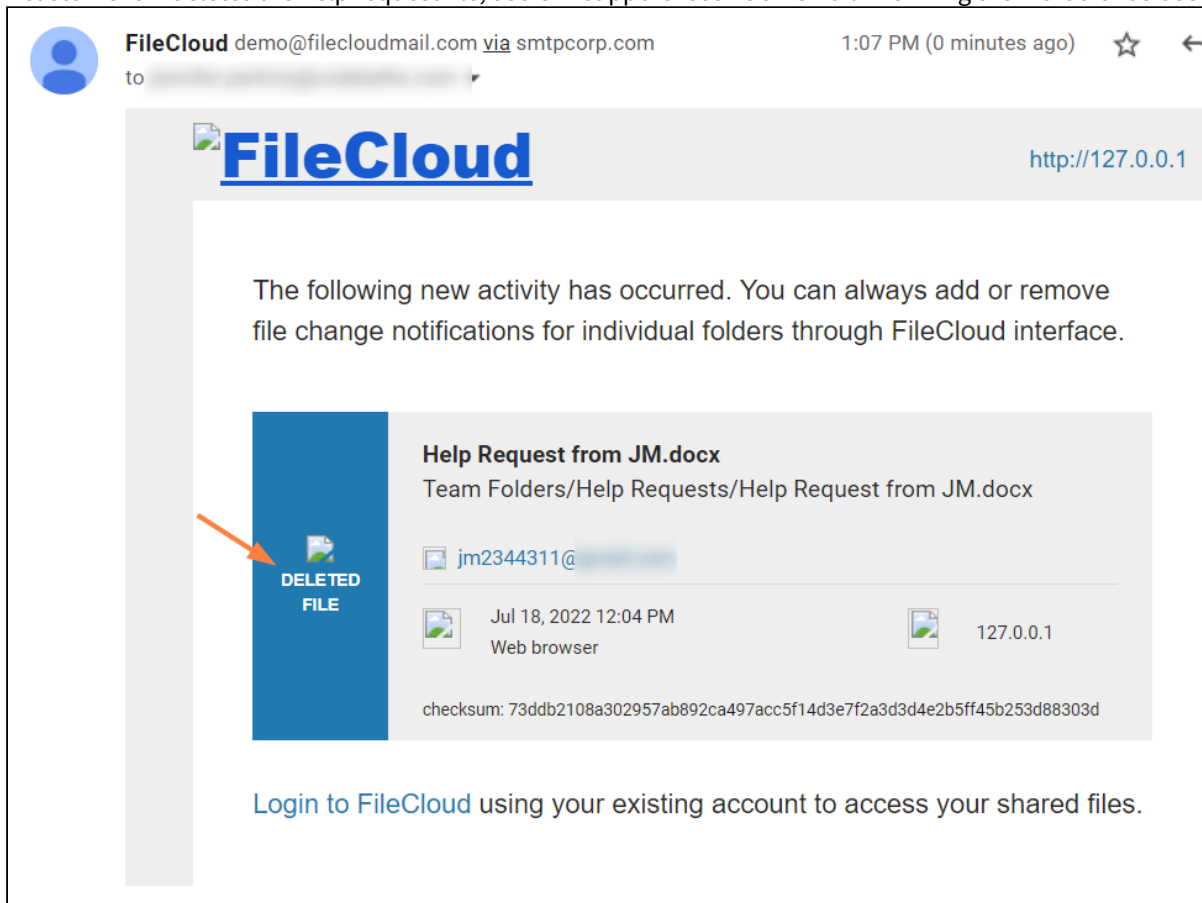


. . . users in support receive an email informing them that a new request file has been uploaded:



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.

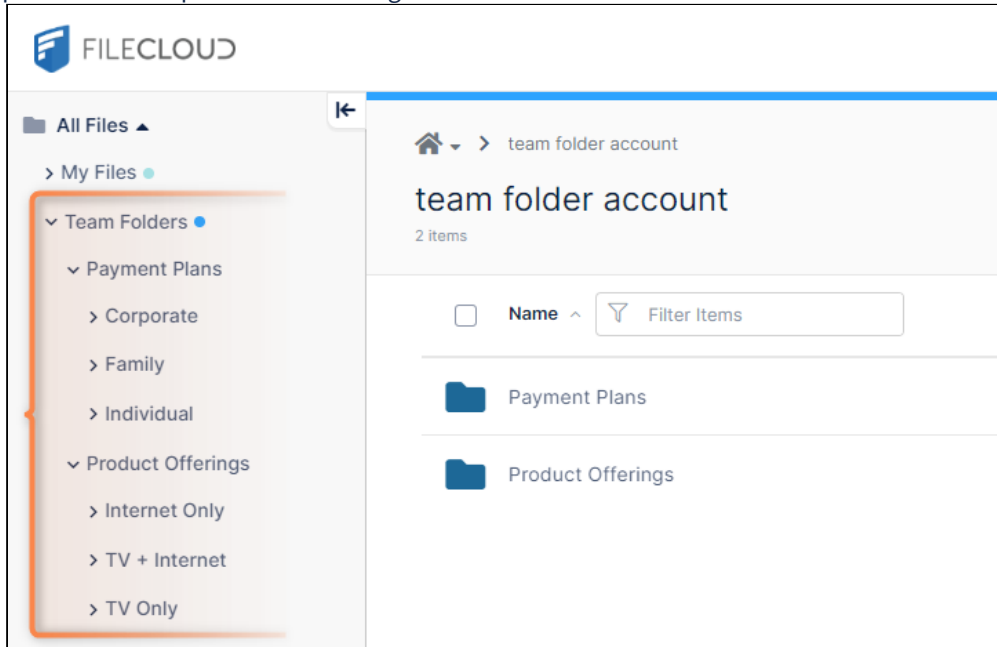
The company has three product offering categories:

- **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 representative 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.

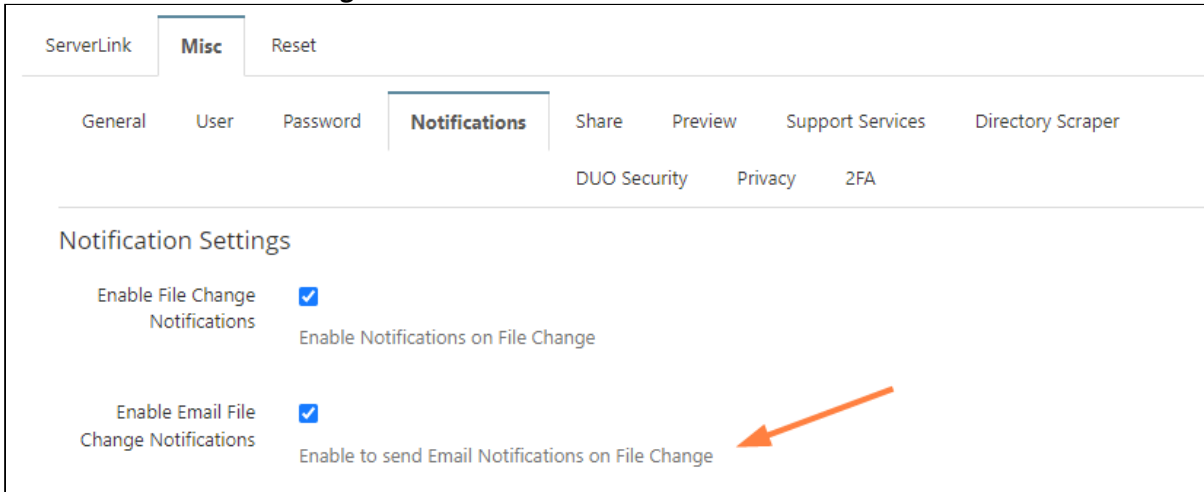
Therefore, as the FileCloud admin, you want each sales rep to be able to customize their file change notifications depending on which campaigns or pricing plans they are currently working with, so they know immediately when these product offerings and prices change. In addition, you want to give sales 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, in the FileCloud admin portal, go to **Settings > Misc > Notifications**.
2. Make sure **Enable File Change Notifications** is checked; if it is not checked, **Enable Email File Notifications** will not be available.

3. Check **Enable Email File Change Notifications**.


ServerLink **Misc** Reset

General User Password **Notifications** Share Preview Support Services Directory Scraper

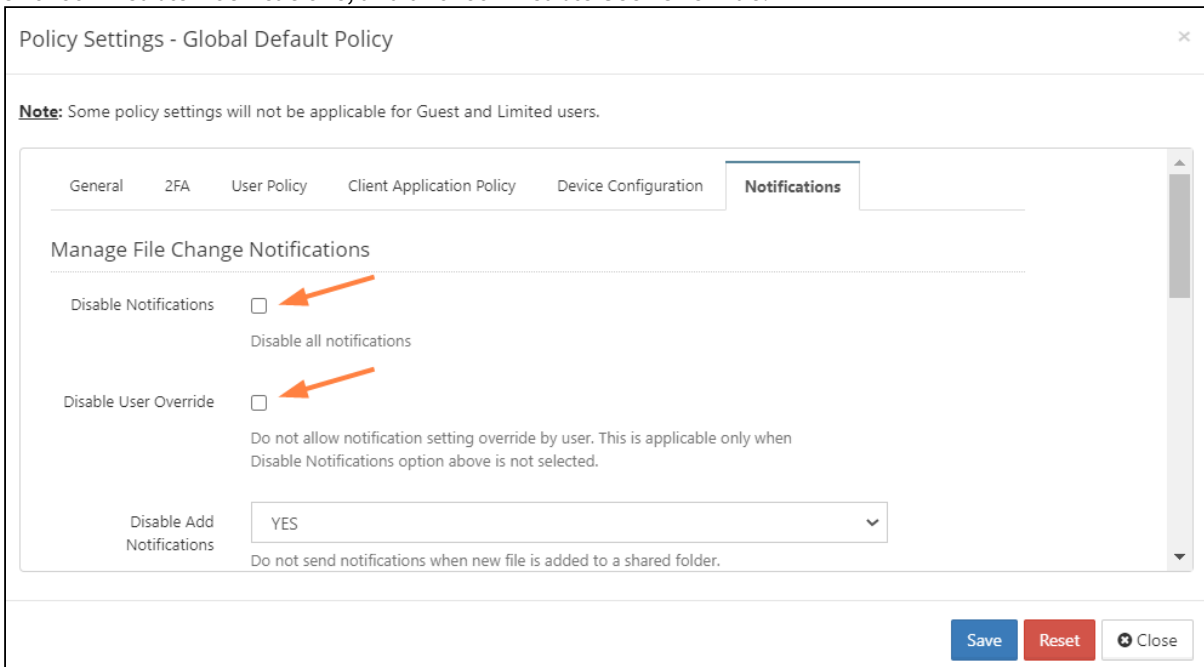
DUO Security Privacy 2FA

Notification Settings

Enable File Change Notifications Enable Notifications on File Change

Enable Email File Change Notifications Enable to send Email Notifications on File Change

4. To disable all notifications by default but allow sales reps to enable them, go to **Settings > Policies**.
5. Edit the policy assigned to the sales reps.
6. Click the **Notifications** tab.
7. Uncheck **Disable Notifications**, and uncheck **Disable User Override**.



Policy Settings - Global Default Policy

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

General 2FA User Policy Client Application Policy Device Configuration **Notifications**

Manage File Change Notifications

Disable Notifications Disable all notifications

Disable User Override Do not allow notification setting override by user. This is applicable only when Disable Notifications option above is not selected.






Disable Add Notifications YES Do not send notifications when new file is added to a shared folder.

Save Reset Close

8. Scroll down so that you can view the individual **Disable Notifications** settings, and change all of the **Disable Notification** settings to **Yes**.

Policy Settings - Global Default Policy ✕

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

Disable Add Notifications	YES 	Do not send notifications when new file is added to a shared folder.
Disable Update Notifications	YES 	Do not send notifications when a shared file is updated.
Disable Delete Notifications	YES 	Do not send notifications when a shared file is deleted.
Disable Download Notifications	YES 	Do not send notifications when a shared file is downloaded.
Disable Preview	YES 	

Save Reset Close

9. Save your changes.

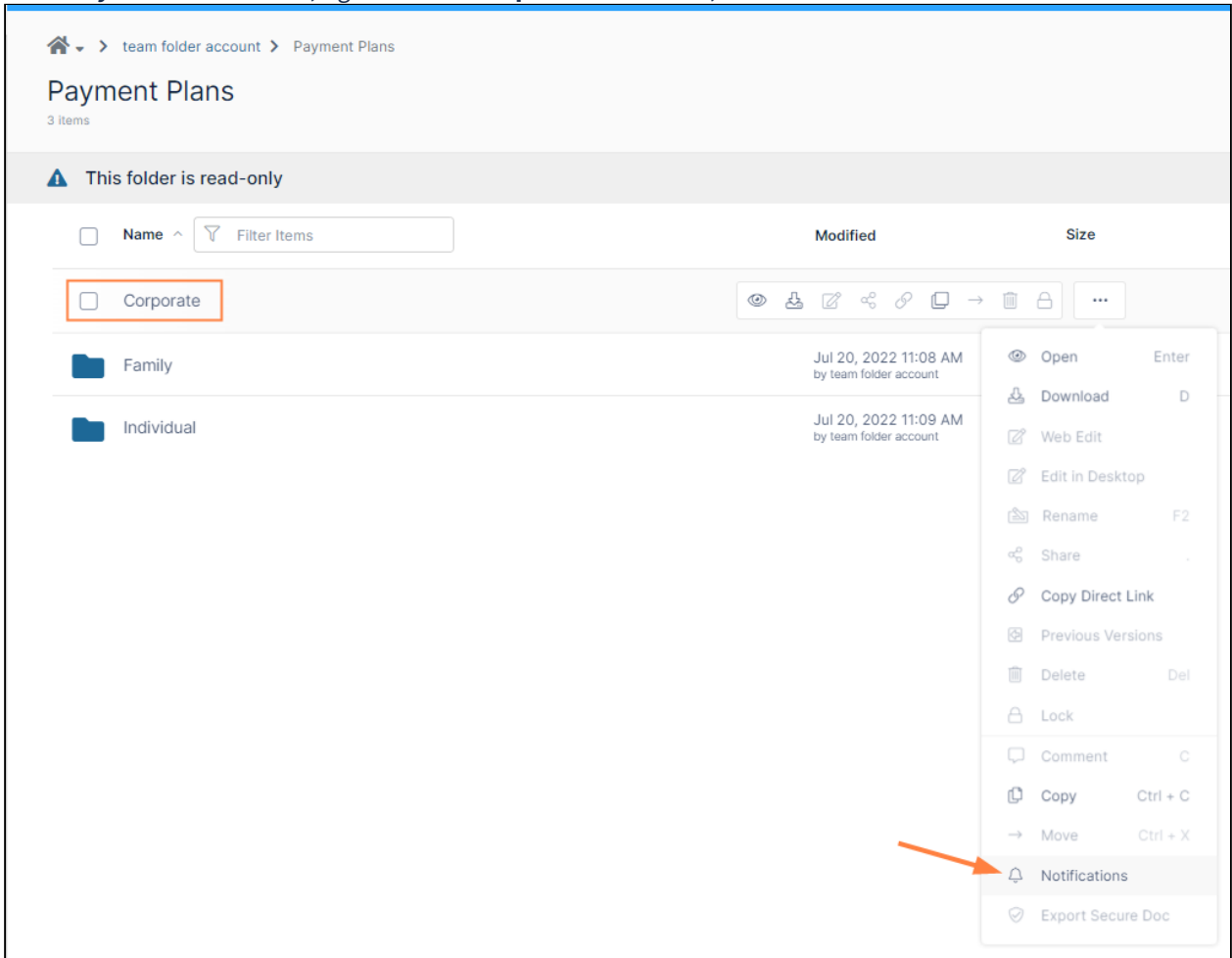
How a Sales Rep sets up notifications about information particular to their clients:

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.

- In the **Payment Plans** folder, right click the **Corporate** sub-folder, and choose **Notifications**.



Notifications settings for the **Corporate** Team Folder open.

- Select **Use my own notification settings**.
- Check the actions that you want to be notified about in the folder (for example **Upload, Delete, Rename, and Update**).

Notification Settings for /SHARED/team folder account/Payment Plans/Corporate

Use default notification settings
 Use my own notification settings

Send Notifications

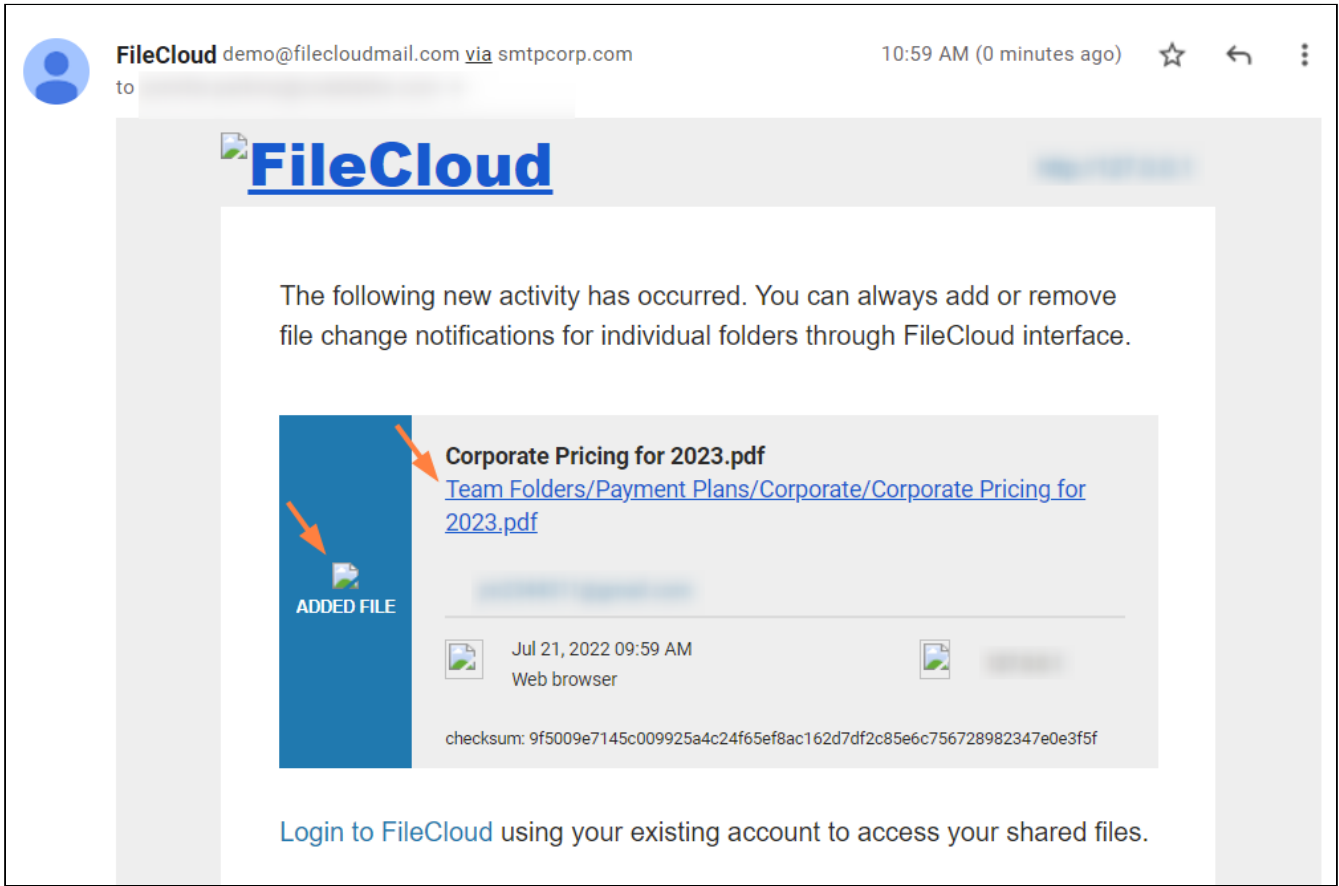
Send Notifications on:

<input checked="" type="checkbox"/> Upload When a file or folder is added	<input checked="" type="checkbox"/> Update When a file is modified
<input type="checkbox"/> Download When a file or folder is downloaded	<input type="checkbox"/> Preview When a file is viewed in the browser or in the mobile app
<input type="checkbox"/> Share When a file or folder is shared with someone	<input type="checkbox"/> Lock/Unlock When a file or folder is locked or unlocked
<input checked="" type="checkbox"/> Delete When a file or folder is deleted	<input type="checkbox"/> Self Notifications When an action is performed by me
<input checked="" type="checkbox"/> Rename When a file or folder is renamed	

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.

The Misc. Tab Settings

There are many ways to configure a FileCloud Server to work with your unique environment. The Misc. tab contains settings that can be configured if you need to change the default values.

To access the Misc. tab:

1. In the Admin Portal, from the left navigation panel, click **Settings**.
2. Select the **Misc.** tab.

General settings

Setting	Tab	Description	Version Added
Server Timezone	General	Sets the time zone for the server	
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: <ul style="list-style-type: none"> • 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	

Setting	Tab	Description	Version Added
Disable Action 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 action is checked.	
Disable Activities for External Users	General	Hides Activities panel if the user is a External user. Check by default.	
Disable Metadata Panel	General	Hides metadata panel and disables metadata search option in User Portal	
Disable Locking	General	Disables supports for File and Folder Locking. See Locking section for more information on Locking functionality .	
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 be blocked	General	Enter the comma separated email domain names that has to be blocked.	
Enable Proxy settings	General	Change the settings of a proxy network if needed.	
Scheduled Tasks	General	Manually execute cron tasks as needed	
Import Files	General	Import files to Managed storage	
Allowed File Extensions	General	Specify file extensions that are allowed for uploading. 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.	
Disable DB backup	General	Disables automatic database backup	

Setting	Tab	Description	Version Added
DB backup store path	General	Specify a writable path to store backed up database.	
Number of Backups	General	Number of backups to maintain.	
DB Backup Interval	General	Interval between backup process. 0 = daily backup.	
Disable Content Classification	General	Do not allow content classification.	

User settings

Setting	Tab	Description
User account search mode	User	See: Securing Shares by Limiting User Account Searches
User account type search mode	User	Restrict user searches so that your users can only search for users in certain account types. See User Account-Type Search Mode .
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	Select the checkbox to send email to user when a new device is ready for approvedi

Setting	Tab	Description
Default Grid View Settings	User	<p>Select how files appear to users by default. (See: Viewing Files by List or Grid).</p> <p>The options are: (size varies depending on screen resolution)</p> <ul style="list-style-type: none"> • 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 set phone numbers	User	Select to 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	Notification s	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	Notification s	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 Email Notifications for External Users	Notification s	When this option is enabled no share notifications will be sent to the external user.
Enable Share Notification	Notification s	<p>When this option is enabled share notifications will be set to NO by default.</p> <p>The "Email FileChange Notifications" will be set to NO in Manage Share → advanced options.</p>
Enable New Version Email Notification	Notification s	When checked, emails about new versions of FileCloud are sent to the administrator once a week.

Setting	Tab	Description
Number of Days After which Notifications are not sent	Notifications	Do not sent notifications for actions that occurred before the set number of days
Email Notification Frequency	Notifications	How frequently, in minutes, email notifications are sent.

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

i 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.

The screenshot shows the FileCloud registration interface. At the top is the FileCloud logo. Below it, the 'New Account' section is active, with a 'Login' link. The form contains four input fields: 'Email' (placeholder: 'Enter email id'), 'Account Name' (placeholder: 'Enter username'), 'Password' (placeholder: 'Enter password'), and 'Repeat Password' (placeholder: 'Re-enter password'). Below the password fields is a checked checkbox labeled 'I agree to Terms of Use' with a 'Help' link to its right. At the bottom of the form are 'Create' and 'Cancel' buttons. An orange arrow points to the 'I agree to Terms of Use' checkbox. At the very bottom, there is a globe icon and the text 'English' with a dropdown arrow.

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. From the left navigation panel, click **Settings**.
2. Click the **Policies** tab.

Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	<input type="checkbox"/>	
Global Default Policy	1	0	<input checked="" type="checkbox"/>	

3. Edit the policy that includes the users whose privacy settings you want to modify.
4. On the **Policy Settings** screen, on the **General** tab, in **Enable Privacy Settings**, select **YES**.

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

General | 2FA | User Policy | Client Application Policy | Device Configuration | Notifications

Share mode: Allow All Shares (Set Share Mode)

User Storage Quota: Units 1024 MB (Specify storage quota. 0 implies Unlimited Quota)

Enable Privacy Settings: YES (Enables/disables privacy settings)

Save | Reset | Close

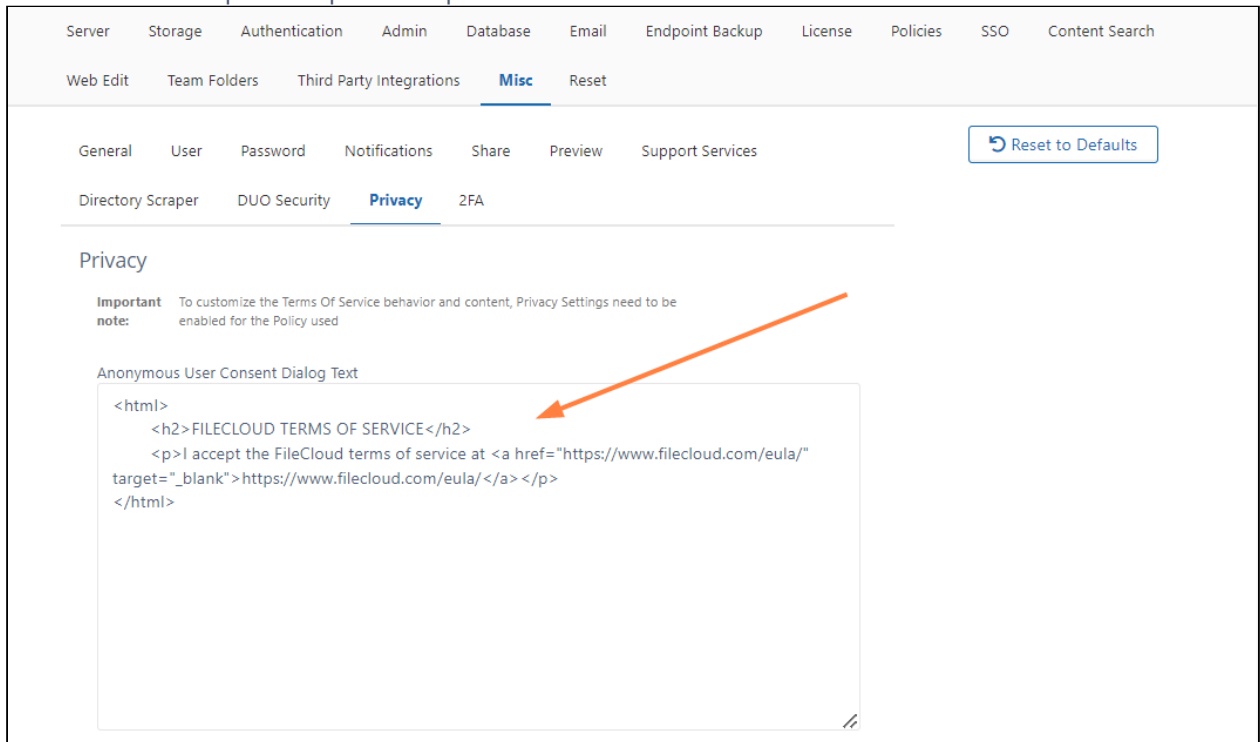
5. Click **Save**.

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 into 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.
2. Go to **Settings > Misc > Privacy**.
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:



The screenshot shows the FileCloud settings interface. The top navigation bar includes: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License, Policies, SSO, Content Search. Below this is a secondary navigation bar with: Web Edit, Team Folders, Third Party Integrations, **Misc**, Reset. The main content area has tabs for: General, User, Password, Notifications, Share, Preview, Support Services, and a 'Reset to Defaults' button. Underneath are more tabs: Directory Scraper, DUO Security, **Privacy**, 2FA. The 'Privacy' section is active, showing an 'Important note' and a text area for 'Anonymous User Consent Dialog Text'. An orange arrow points to the HTML code in this text area.

```
<html>
  <h2>FILECLOUD TERMS OF SERVICE</h2>
  <p>I accept the FileCloud terms of service at <a href="https://www.filecloud.com/eula/"
target="_blank">https://www.filecloud.com/eula/</a></p>
</html>
```

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

i In versions of FileCloud prior to version 20.2, the fields **Globally Reset User's 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. Go to **Settings > Misc** and click the **Privacy** tab.
2. Scroll down to the following settings:

Globally Reset User's TOS Consent	<input type="button" value="Reset TOS Consent for all users"/>
	Reset Terms of Service globally
Force users to accept TOS when changed	<input type="text" value="NO"/>
	Force users to accept TOS when changed
Show TOS for every login	<input type="checkbox"/>
	Show TOS every time a user logs in

3. 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**.
4. By default, **Force users to accept TOS when changed** is set to **NO**.
To require users to accept changed terms of service before logging in (to the user portal only), choose **YES**.
5. By default, **Show TOS for every login** is disabled.
To require users to accept the TOS every time they log in, check **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.
6. 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.


User Details ✕


Name	abose	Total Quota	1000 MB
Email	amitbose@example.com	Used Quota	0 B
Last Login	--	Available Quota	1000 MB
TOS Date	Not Accepted	Used Storage	0 B More ▾
Group	Manage		



 Mobile Devices



 Manage Files



 Manage Shares


 Reset Password



 Email Password




 Delete Account


 Manage Policy


 Manage Backups

Profile Image



 Update
 Remove

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**.

General Labels And Logos URL UI Messages Email Templates News Feed **TOS** Custom Header Custom Footer

Advanced

Terms of Service [Reset to Defaults](#)

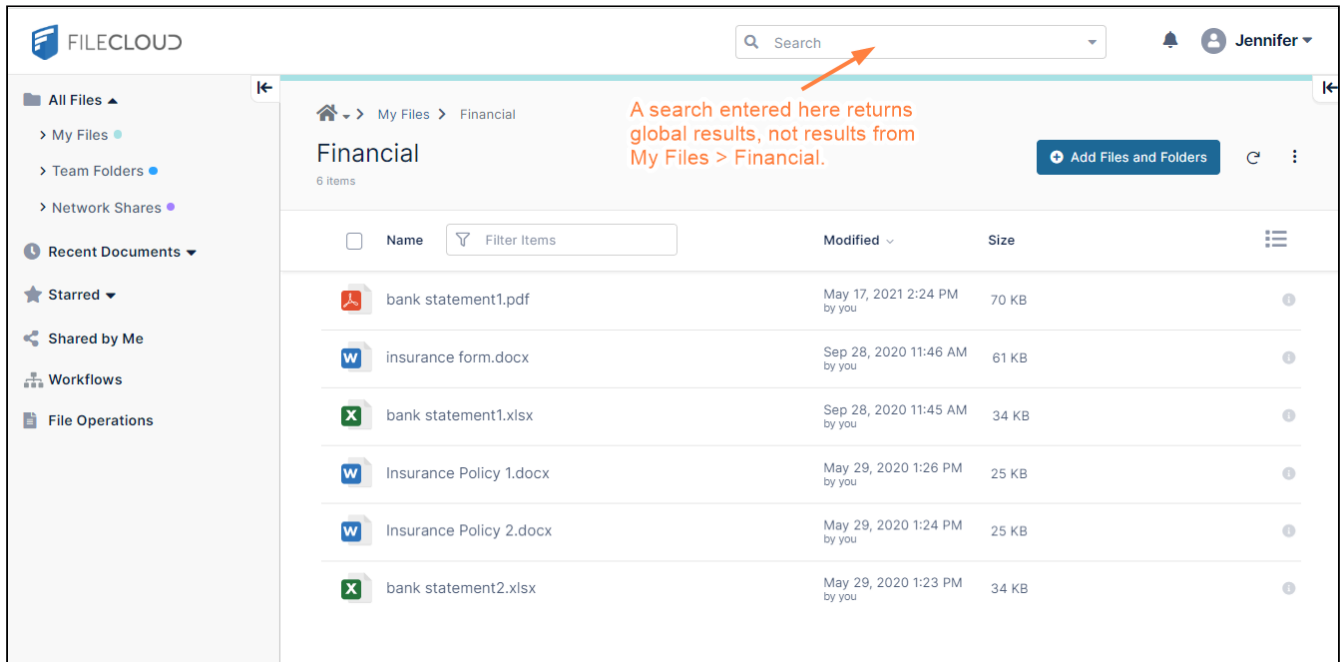
```
<html>
  <h2>FILECLOUD TERMS OF SERVICE</h2>
  <p>The latest version of TOS is available at <a
href= "https://www.filecloud.com/eula/"
target= "_blank">https://www.filecloud.com/eula/</a></p>
</html>
```

Note: This text is not shown when users open a public or password-protected share; instead the text in **Anonymous User Consent Dialog Text** in **Settings > Misc > Privacy**, if it is entered, is shown.

4. Click **Save**

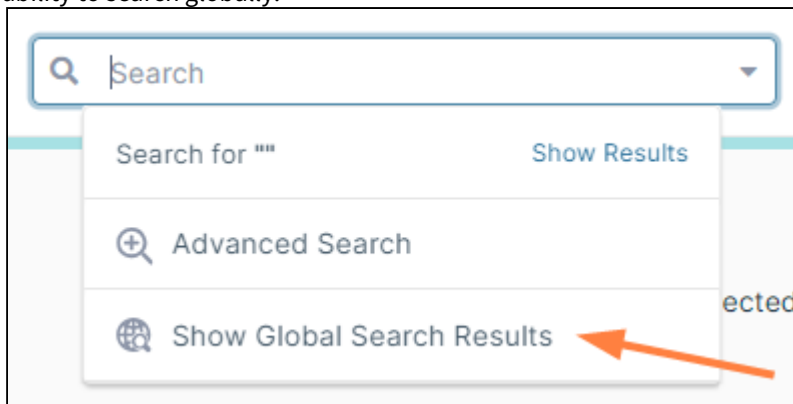
Set Search Location

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](#).

Migrating data to FileCloud using Rclone

-  FileCloud is preparing to deprecate WebDAV.
- Beginning with FileCloud 23.1, WebDAV can no longer be enabled or managed through the FileCloud admin portal.
 - At some time in 2024, WebDAV will no longer be available in FileCloud.


For help enabling or disabling WebDAV currently, please [Contact FileCloud Support](#).

Rclone is a command-line program that manages files in cloud storage. It is a feature-rich alternative to cloud vendors' web storage interfaces. For more information on Rclone please visit their website by accessing the following <https://rclone.org/>.

Requirements

Complete the following requirements before using Rclone with FileCloud.

1. [Download Rclone](#)
2. [Enable WebDav protocol in FileCloud](#).
3. [Configure Rclone](#)

-  FileCloud does not provide support for Rclone, which is third-party software. If you need assistance with your Rclone configuration or setup please contact Rclone directly at <https://rclone.org/contact/>. For assistance setting up WebDav or user permissions in FileCloud please contact FileCloud support at support@codeatthe.com.

Creating a FileCloud WebDav Configuration in Rclone

Once you have completed the above requirements, create your FileCloud configuration profile in Rclone.

1. Extract the .zip file download from the [Rclone website](#), and access its content via command prompt or terminal window using Visual Studio Code.
2. Enter **rclone config**

```
C:\rclone>rclone config
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> |
```

- From the menu options enter **n** to create a new remote profile and enter **FileCloud**, and click enter.

```
C:\rclone>rclone config
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> FileCloud
```

- From the list of types of storage, enter **webdav**, and click enter.

```
34 / Webdav
   \ "webdav"
35 / Yandex Disk
   \ "yandex"
36 / http Connection
   \ "http"
37 / premiumize.me
   \ "premiumizeme"
38 / seafile
   \ "seafile"
Storage> webdav
```

- Once processing is completed you are prompted to enter your FileCloud URL. You must include **/webddav** at the end as mentioned in our [WebDAV documentation](#), for example: **HTTP://** or **HTTPS://YOUR-FILECLOUD-URL/webdav/**

```
URL of http host to connect to
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / Connect to example.com
   \ "https://example.com"
url> https://[REDACTED].com/webdav/
```

- After you enter your FileCloud URL, you are prompted to enter the name of the WebDav site or software you are using.
Enter **FileCloud** and click enter.
- Now you are prompted to enter your FileCloud user name and password.
In this example we are using a user named **rclone**.

```

url> https://demo.filecloudlabs.com/webdav/
Name of the Webdav site/service/software you are using
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / Nextcloud
   \ "nextcloud"
 2 / Owncloud
   \ "owncloud"
 3 / Sharepoint
   \ "sharepoint"
 4 / Other site/service or software
   \ "other"
vendor> FileCloud
User name
Enter a string value. Press Enter for the default ("").
user> rclone
Password.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank (default)
y/g/n> y
Enter the password:
password:
Confirm the password:
password:

```

8. You are prompted to enter the bearer token.
Click enter to leave the value blank and continue.
9. Next, you are asked if you would like to edit the advanced configuration.
Click enter to answer **No**.

```

Bearer token instead of user/pass (eg a Macaroon)
Enter a string value. Press Enter for the default ("").
bearer_token>
Edit advanced config? (y/n)
y) Yes
n) No (default)
y/n>
Remote config

```

10. Once processing is completed, Rclone displays a summary of your configuration that should look similar the following.

```
[FileCloud]
type = webdav
url = https://[REDACTED]/webdav/
vendor = FileCloud
user = rclone
pass = *** ENCRYPTED ***
-----
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d> y
Current remotes:

Name                Type
====                ====
FileCloud           webdav

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> [ ]
```

11. Enter **y** to continue.
Rclone displays your FileCloud profile.
12. Enter **q** to exit the configuration.

Testing your configuration and connectivity using Rclone.

Once you have created your profile you can use the command below to confirm that it is configured correctly. For more details on available commands, go to <https://rclone.org/commands/>.

rclone ls remote:path

This command displays all FileCloud files based on the configuration profile created.

```
C:\rclone>rclone ls FileCloud:"/My Files/"
 9722 Book (1).xlsx
 72037464 FileCloudDrive2eSetup.exe
 6960504 FileCloudServerSyncSetup64.exe
 617689064 FileCloudSetup.exe
 22622208 FileCloudSyncSetup.exe
 7945 Sales Report.xlsx
 78516 download.pdf
```

Migrating (Move/Copy/Sync) Data from other solutions to FileCloud.

To [copy](#), [move](#), or [sync](#) data directly from other providers into FileCloud, create corresponding profiles within your Rclone configuration file.

For more details click on the hyperlink of each corresponding solution below.

- copy data from [s3](#) to **FileCloud**
- copy data from [OwnCloud](#) to **FileCloud**
- copy data from [Box](#) to **FileCloud**
- copy data from [OneDrive](#) to **FileCloud**
- copy data from [Dropbox](#) to **FileCloud**

Things to consider when using Rclone to migrate your data to FileCloud.

- FileCloud does not have any control over the bandwidth speed of your host machine. Rclone fully depends on the machine's /host bandwidth where it is being executed to copy, move, or sync your data.
- FileCloud does not control any bandwidth restriction or limitation when copying, syncing, or moving your data from another provider to FileCloud using Rclone.
- To view the progress of your data transfer when using rclone simple add **--progress** at the end of the command.
- FileCloud does not limit the amount or size of data (files or folders) you transfer. However, prior to starting your migration make sure you have enough storage space available in your FileCloud Server to avoid any issues.

Additional FileCloud Configurations

- By default when using WebDav, FileCloud has a single file maximum upload size limitation of 524288000 bytes. You can increase this parameter by accessing :

Windows: **C:\xampp\htdocs\.htaccess**

Linux: **/var/www/html**

and modifying the following parameters. It is also recommended that you increase the `max_execution_time`.

```
php_value post_max_size 500M
php_value upload_max_filesize 500M
php_value max_execution_time 60
```

Once you have applied the changes, restart Apache and retry your upload. In the example below, notice that once the change is applied Rclone is able to upload a 6GB file into FileCloud.

```
C:\Users\... \rclone-v1.52.2-windows-amd64\rclone-v1.52.2-windows-amd64>rclone copy "C:\Users\... \Desktop\6GB.zip" webdav:"/My Files/" --progress --log-level=DEBUG --log-file=xyz.log
Transferred:      6.001G / 6.001 GBytes, 100%, 53.987 MBytes/s, ETA 0s
Transferred:      1 / 1, 100%
Elapsed time:     1m53.8s
```