FileCloud Server Version 23.232

Site Setup

Printed on 02/08/2024

Copyright Notice

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

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.

ⓘ 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.

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

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

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Recommended	Configure Email Settings video: Email Settings Restrict Access to the Admin Portal FileCloud Best Practices	Enable MongoDB Bind IP and Authentication Set Client Application Policies video: Policy, Client Application Policy Tab Configure Security Options		Manage User Authentication • Configure Single Sign On video: SSO • Use LDAP Based Authentication video: LDAP Authentication • Active Directory Authentication video: AD Authentication Set Up 2FA Configure Microsoft Office Integration Options Configure Online Web Editing video: Web Edit • Installing Office Online Server • Collabora Code • Google Docs Editing • OnlyOffice Editing Set Up Document Preview Set Up Content Search video: Content Search

Level of Priority	Administrator Settings	Server Settings	Storage Settings	User Access Settings
Provides a Better Experience	Add Customization and Branding Enable Antivirus Scanning video: AntiVirus Integration	Configure High Availability		Manage Document Settings 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 • 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

Log in using your admin account to perform administrative tasks.

Accessing the Admin Portal

In a supported web browser, open one of the following links depending on whether or not you are using an SSL connection.

ⓘ **Admin URLs**

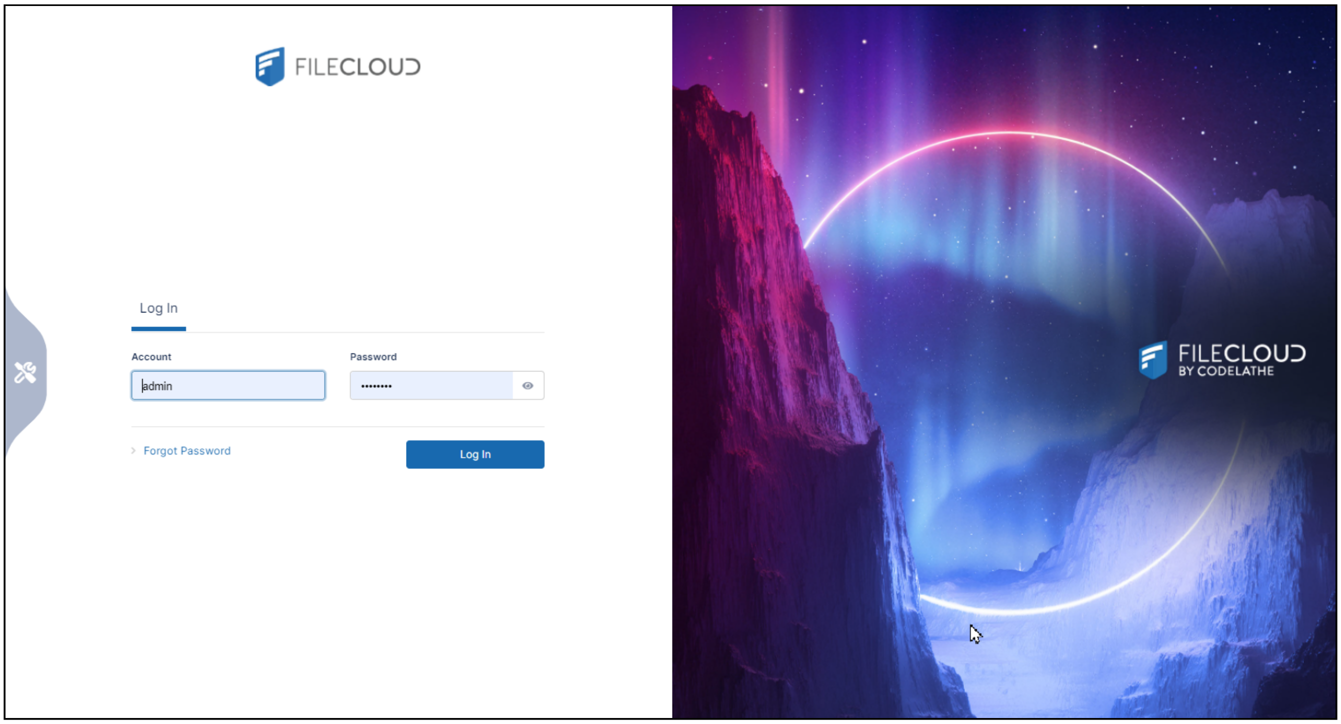
http://<your filecloud address or IP>/admin (or)
https://<your filecloud address or IP>/admin
this redirects to
http://<your filecloud address or IP>/ui/admin/index.html (or)
https://<your filecloud address or IP>/ui/admin/index.html

Using Default Credentials

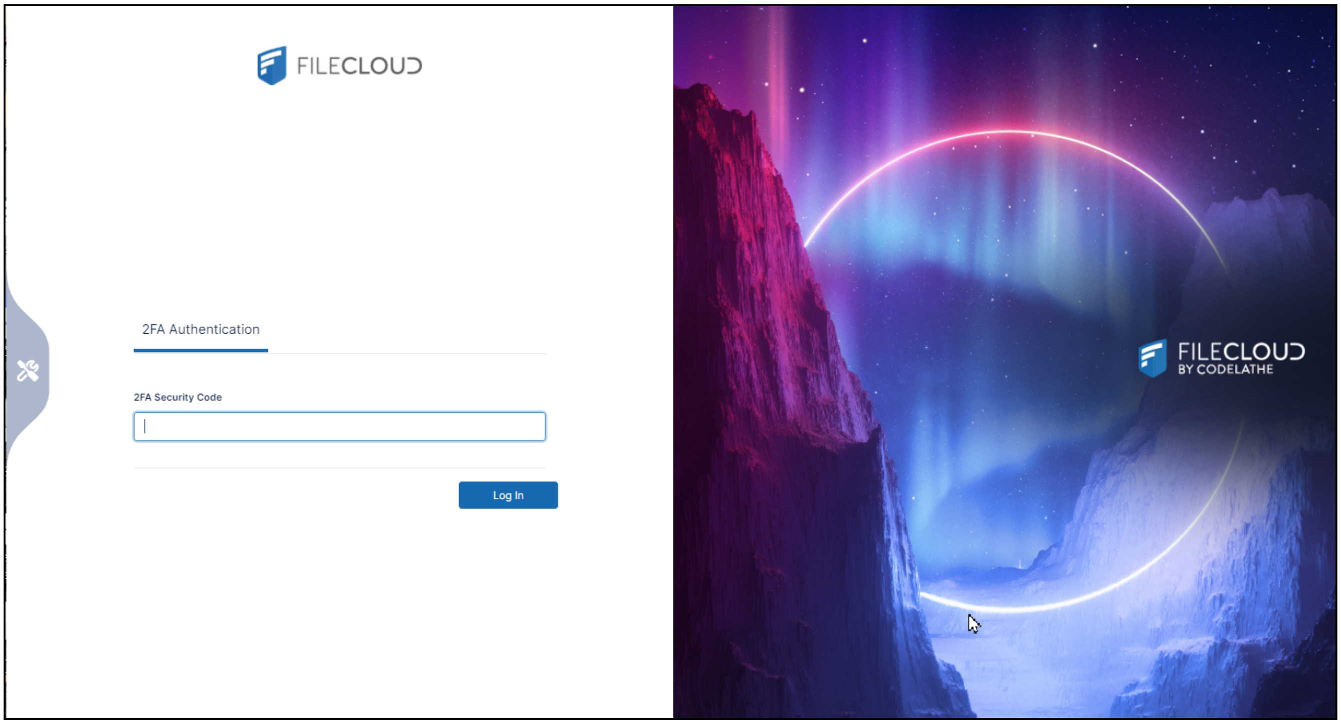
If your credentials were not changed during FileCloud installation, use the following information to log in to the admin UI.

Field	Default
Name	***admin***
Password	***password***

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.

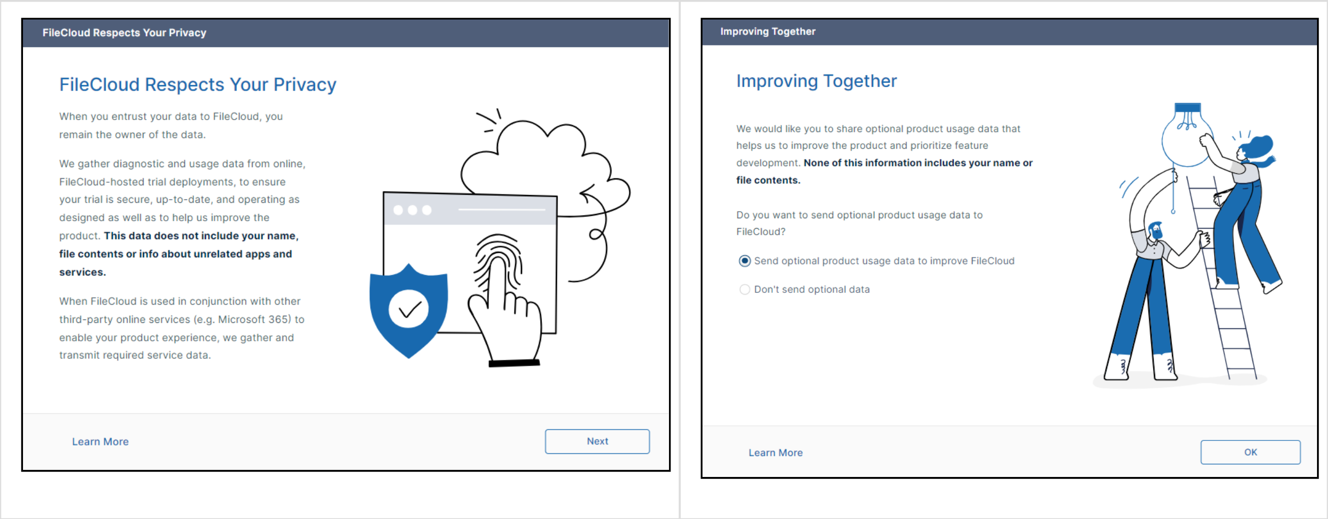


If two factor authentication for administrators is enabled, then you are required to provide a security code to continue.



Collection of usage data

If you are using a FileCloud Server with a trial or production license, the first time you log in to the admin portal, a wizard opens with the following two screens. These screens also appear the first time you log in to the admin portal after converting from a trial license to a production license.



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.

Improving Together

We would like you to share optional product usage data that helps us to improve the product and prioritize feature development. **None of this information includes your name or file contents.**

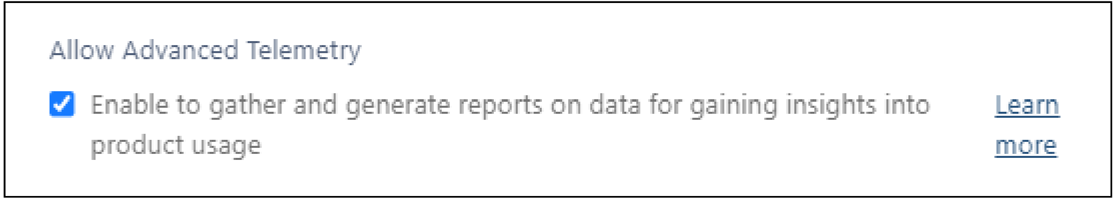
Do you want to send optional product usage data to FileCloud?

● Send optional product usage data to improve FileCloud

○ Don't send optional data

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**.

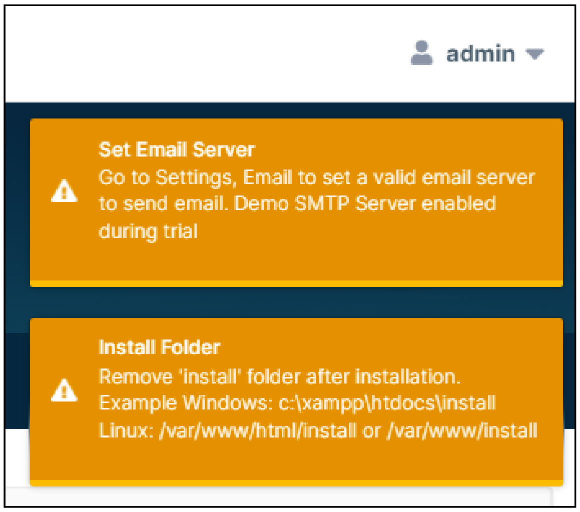
You can change the option at any time by going to **Settings > Server** and checking or unchecking **Allow Advanced Telemetry**.


Allow Advanced Telemetry

☑ Enable to gather and generate reports on data for gaining insights into product usage

Viewing and Clearing Checklist Notifications

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



Set Email Server
Go to Settings, Email to set a valid email server to send email. Demo SMTP Server enabled during trial

Install Folder
Remove 'install' folder after installation.
Example Windows: c:\xampp\htdocs\install
Linux: /var/www/html/install or /var/www/install

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

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

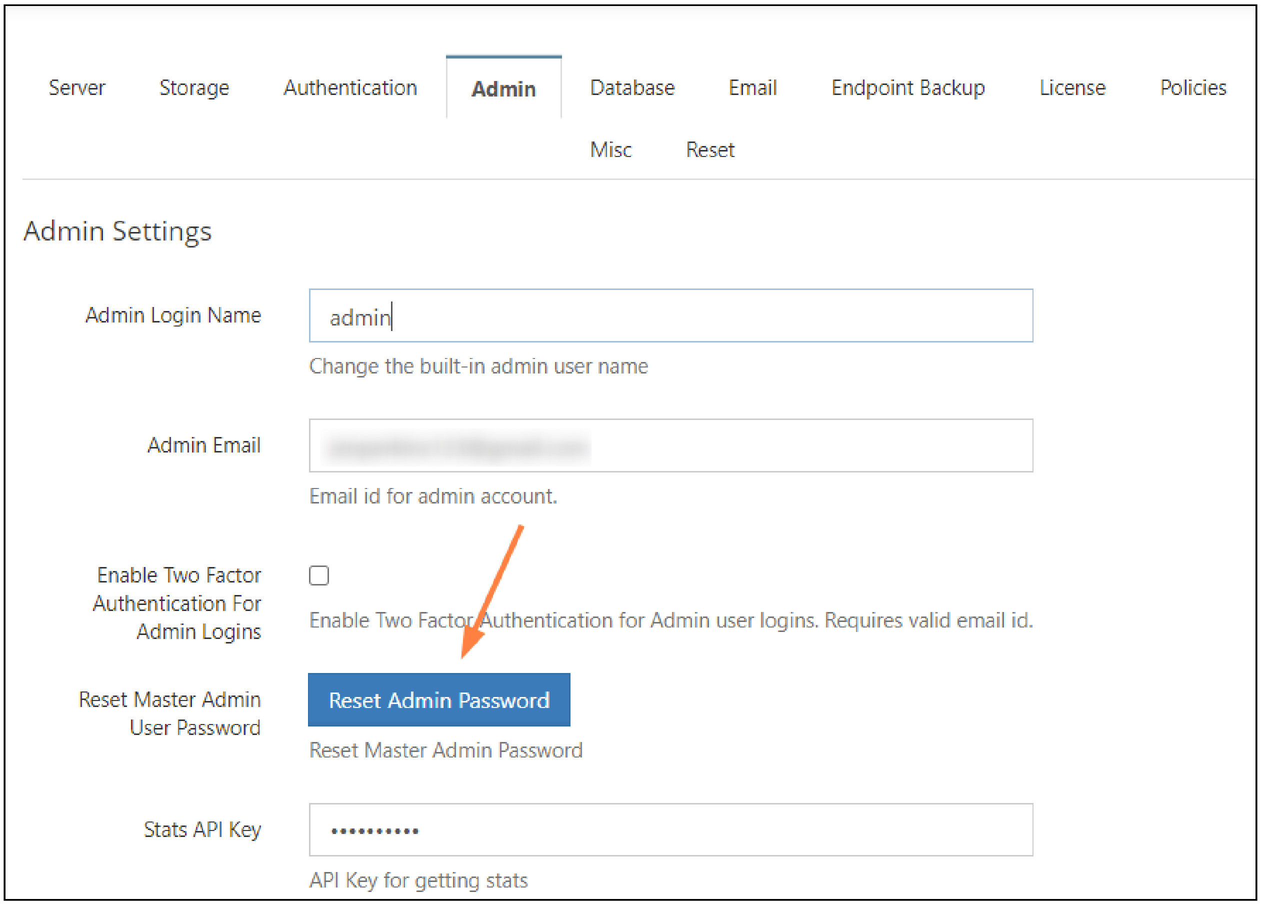
⚠ When Auth Type is set to AD or LDAP, the admin password cannot be changed using the procedure on this page, but must be changed in the AD or LDAP server by the AD or LDAP admin. See User Authentication Settings.

The FileCloud Admin can reset the Admin password from command line, in case the current password is forgotten. The reset password script also clears any admin login locks and disables two-factor authentication, if enabled.

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**.



Admin Settings

Admin Login Name: admin
Change the built-in admin user name

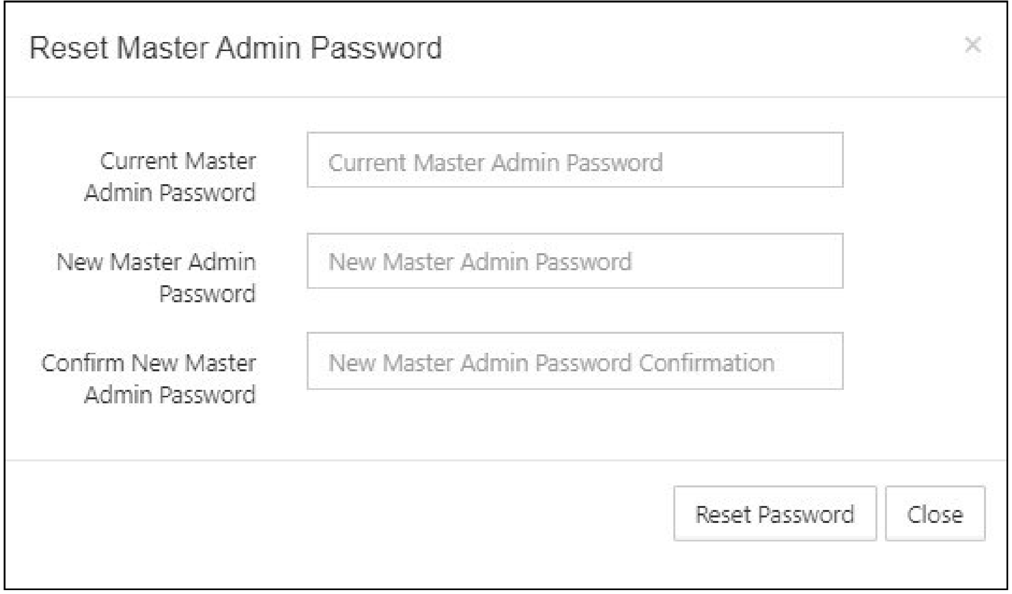
Admin Email: [redacted]
Email id for admin account.

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 Admin 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: Current Master Admin Password

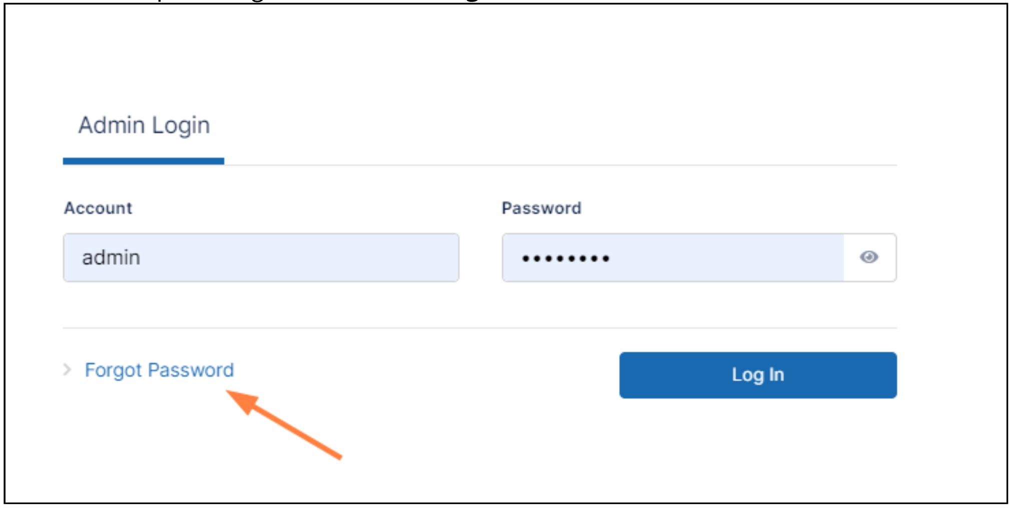
New Master Admin Password: New Master Admin Password

Confirm New Master Admin Password: New Master Admin Password Confirmation

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**.



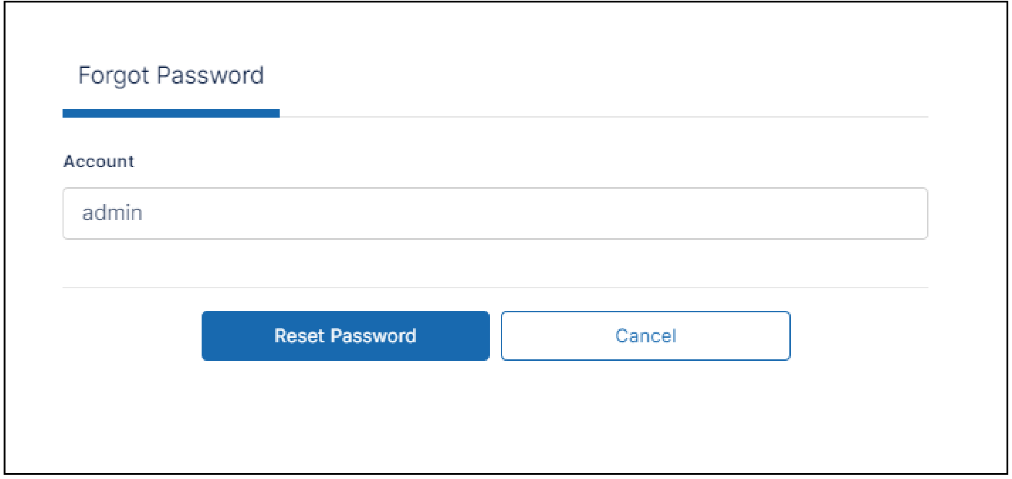
Admin Login

Account: admin

Password: •••••••••

A dialog box prompts you to enter your user account.

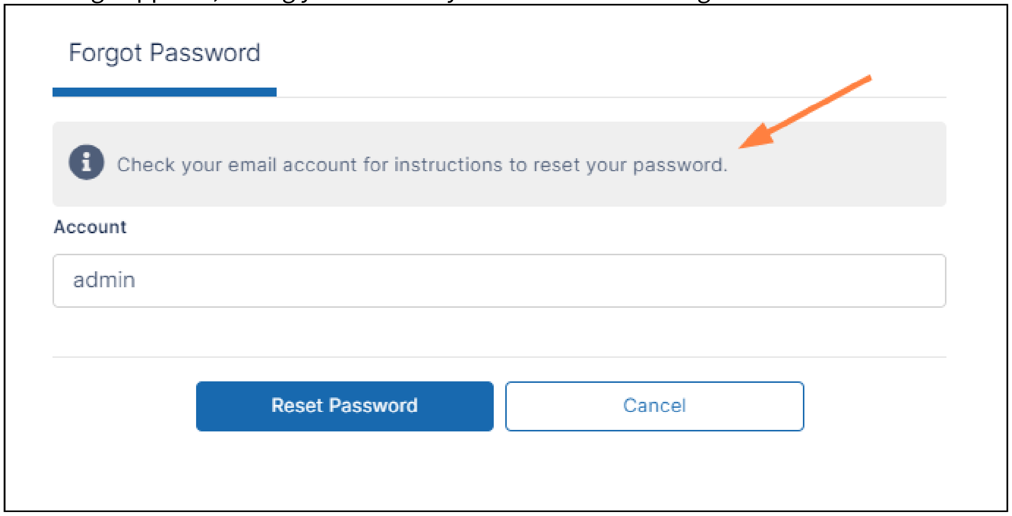
2. Enter your admin account name, and click **Reset Password**.
   Note: To reset their passwords, promoted admin users must use the user portal.



Forgot Password

Account: admin

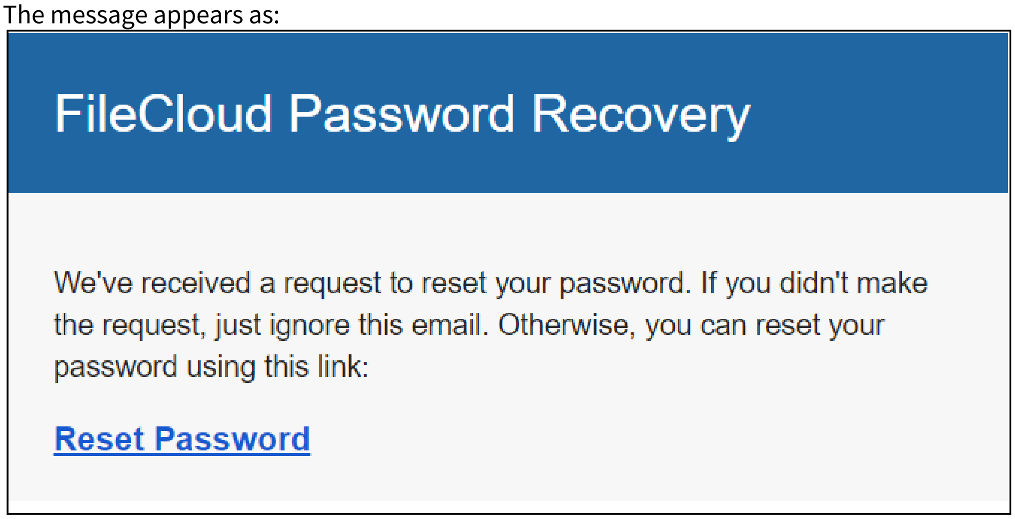
A message appears, telling you to check your email for a message.



Check your email account for instructions to reset your password.

Account: admin

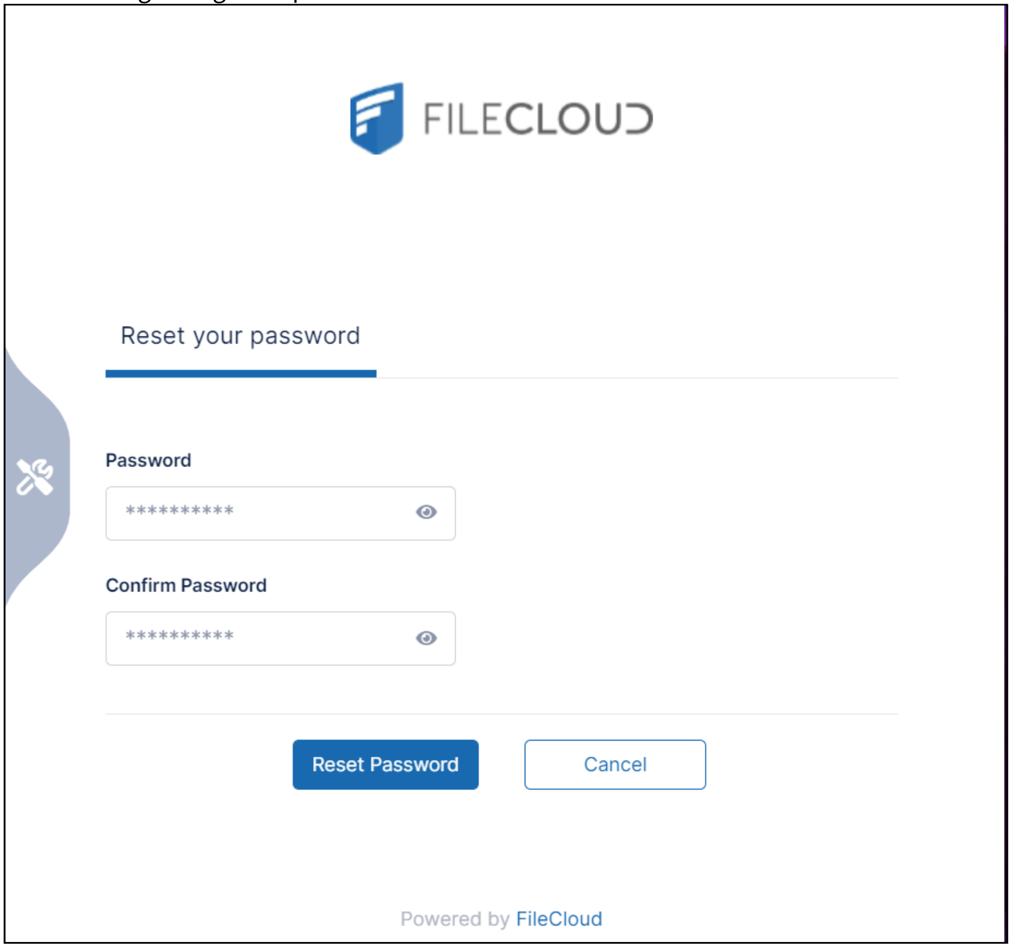
3. Find and open the message in your email.
   The message appears as:



FileCloud Password Recovery

We've received a request to reset your password. If you didn't make the request, just ignore this email. Otherwise, you can reset your password using this link:

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



Reset your password

Password

****

Confirm Password

****

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 in the Command Line Interface

1. In a command line enter:

   For Windows:

```
cd c:\xampp\htdocs\resources\backup
PATH=%PATH%;C:\xampp\php
```

   For Linux:

```
cd /var/www/html/resources/backup/
```

2. Then, for both Windows and Linux:
    - To reset the Admin password to **password**, enter:

      ```
      php resetadminpw.php
      ```

    - Beginning in FileCloud 20.2, you can reset the Admin password to a custom value. To reset the admin password to **he!@#%$%^)*el$AAo**, enter:

      ```
      php resetadminpw.php -p "he!@#%$%^)*el$AAo"
      ```

Displaying the new password in the system log

Prior to FileCloud Version 21.2, when the Admin password is reset, the new password is shown in the system logs.

From FileCloud Version 21.2 on, when the Admin password is reset, by default, the new password is not shown in the system logs. However, you may display the new password in the system logs by using the **-d** settings.

To display the new password in the system logs in FIleCloud Version 21.2 and after:

1. Follow Step 1, above, to navigate to the correct path for Windows or Linux.
2. Then, for both Windows and Linux, enter:

   ```
   php resetadminpw.php -d
   ```

Resetting the Admin password in multi-site setups

To reset password for another site, pass in the hostname using -h parameter in the command line interface.

```
php resetadminpw.php -h site2.xyz.com
```

Reset the Admin Password from the SuperAdmin UI

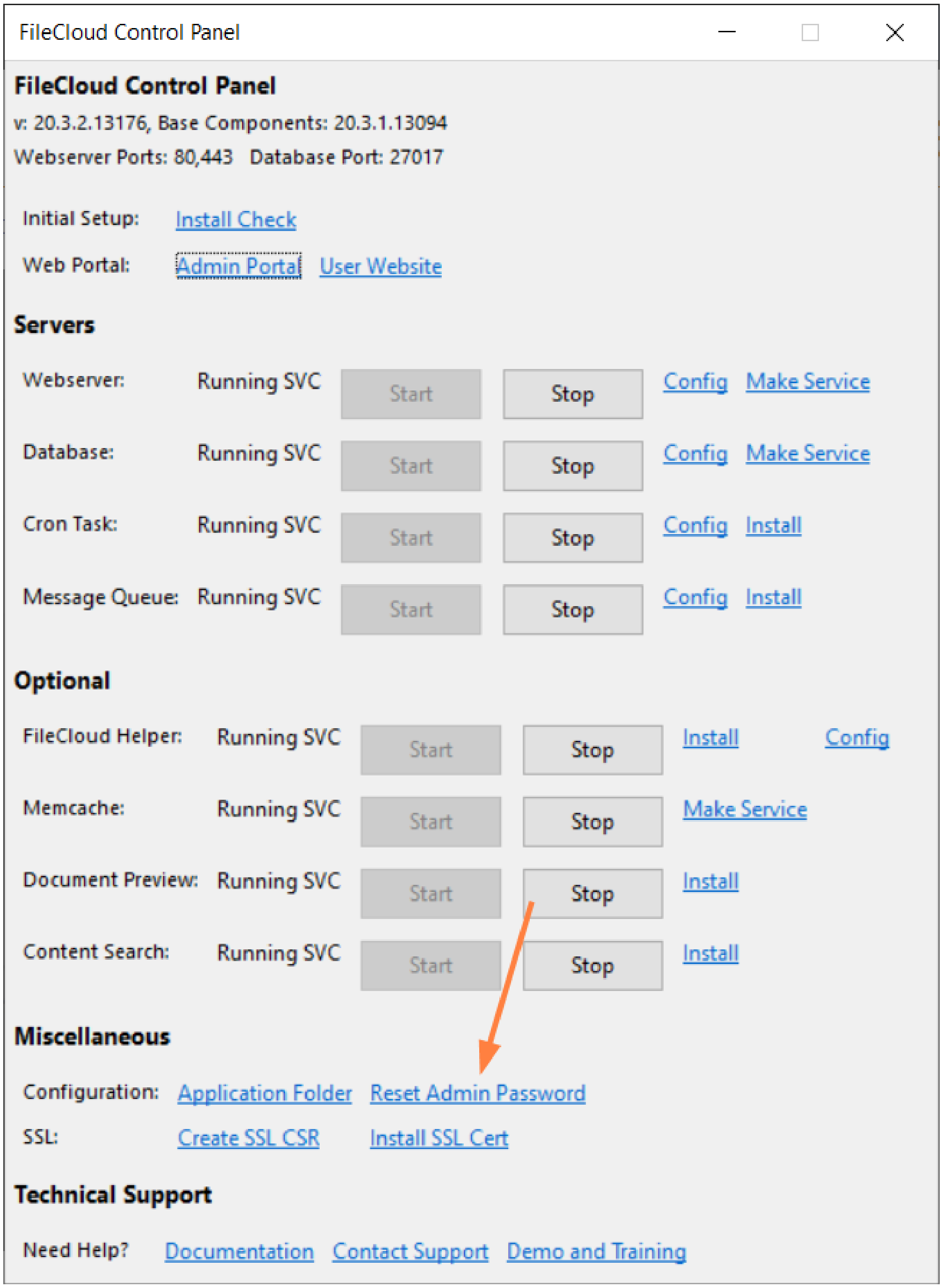
Starting with the 17.3 version it is now possible to reset the Admin Password for each site directly from the SuperAdmin UI.

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

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

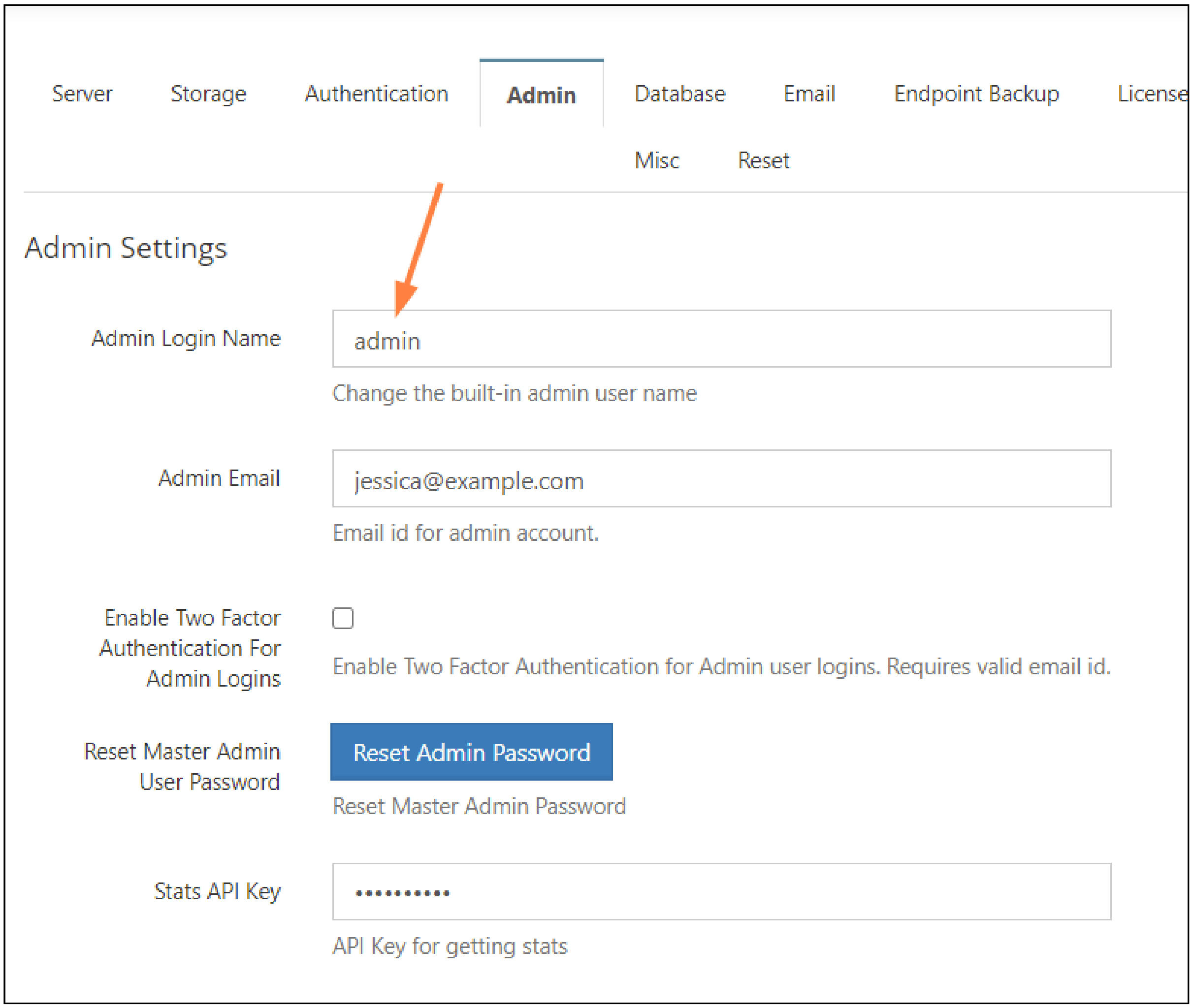
Need Help? Documentation Contact Support Demo and Training

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.



Admin Settings

Admin Login Name: admin
Change the built-in admin user name

Admin Email: jessica@example.com
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

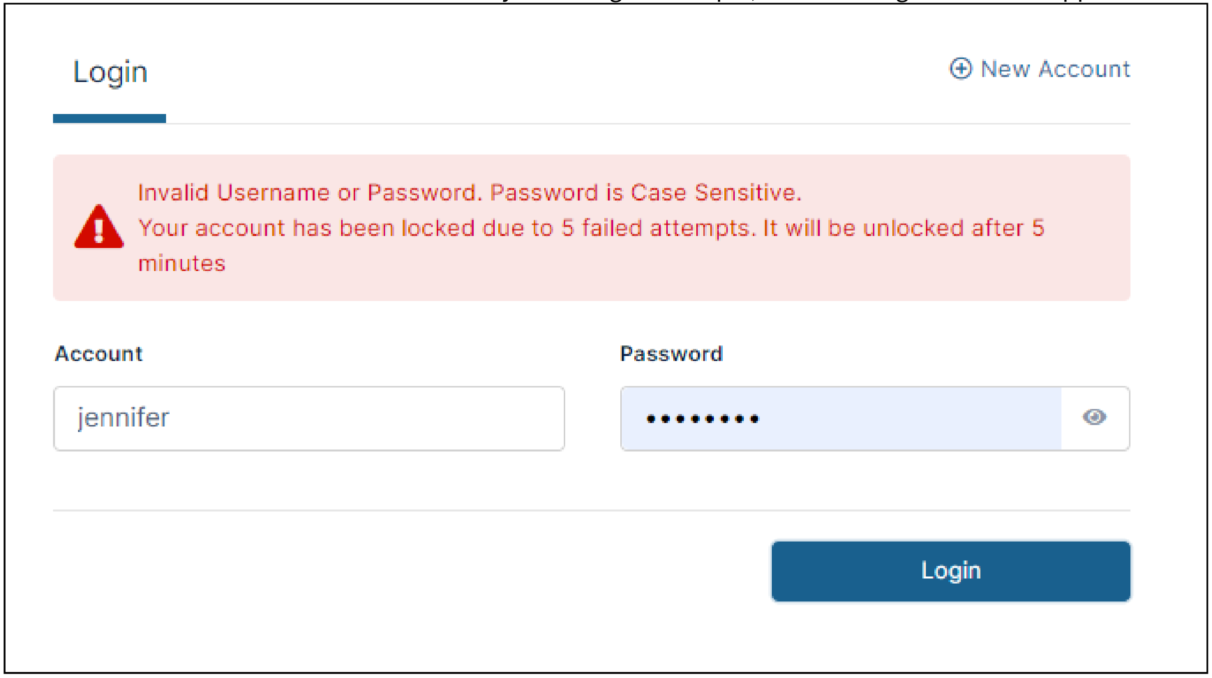
Stats API Key: ••••••••••
API Key for getting stats

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:



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

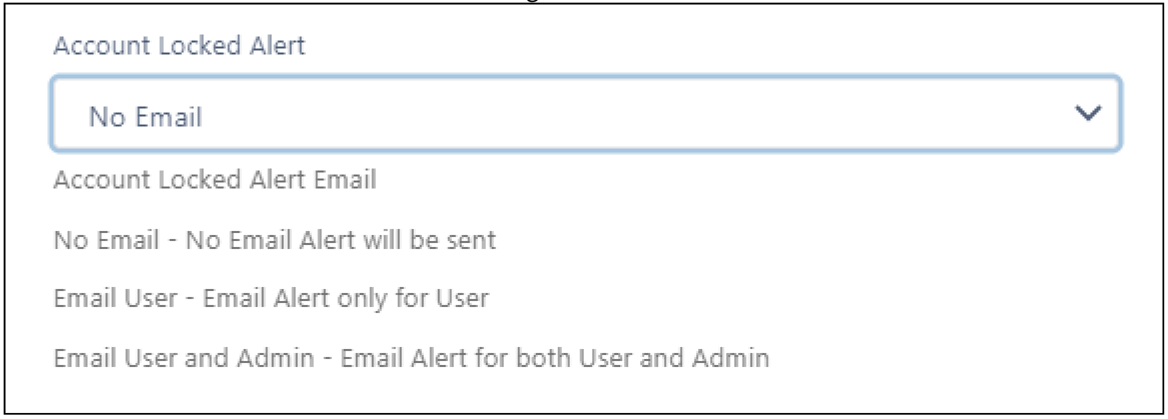
Account: jennifer

Password: •••••••••

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.

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

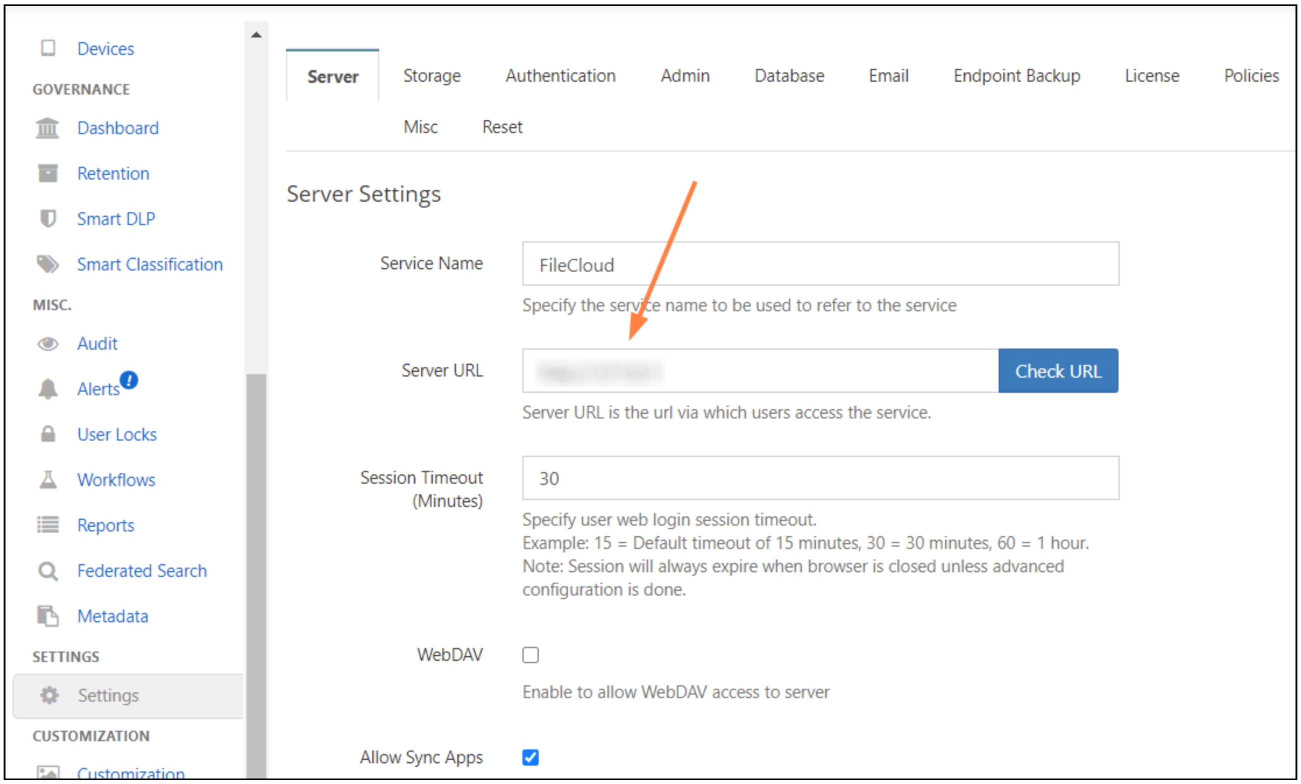
To access the settings:

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.



Server Settings

Service Name: FileCloud

Specify the service name to be used to refer to the service

Server URL: [redacted]

Server URL is the url via which users access the service.

Session Timeout (Minutes): 30

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 ☐

Enable to allow WebDAV access to server

Allow Sync Apps ☑

3. Configure the Remaining Settings

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

<table>
<tr><th>Settings Name</th><th>Description</th></tr>
<tr><td><b>Service Name</b></td><td>The name to be used when referring to your FileCloud service. This is used in email messages, in the zip filename for multiple downloads, and anywhere else your service is referred to by its name.</td></tr>
<tr><td><b>Server URL</b></td><td>This is your DNS entry registered with DNS service. example xyz.company.com . This is the URL by which users will access FileCloud service.
It is also required that you make this server DNS name externally accessible via any firewall you might have.
<b>NOTE: Be sure to use the appropriate protocol prefix https:// or http:// . For production, it is highly recommended to use only https://</b></td></tr>
<tr><td><b>Session Timeout</b></td><td>Number indicating the number of minutes the authentication is valid. If the browser is closed, the session will be logged out. Read this to change this behavior
<b>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.</b>
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<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>
</table>
</td></tr>
<tr><td><b>WebDAV</b></td><td>You can enable this function to allow users to mount their FileCloud home folders as a Windows or Mac or Linux drives.
➡ Enable WebDAV support</td></tr>
</table>

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"**
Allow Old Devices to Login	FileCloud supports Remote Client Management (RMC) of various clients. As of v4.5 onwards, All the FileCloud clients are RCM compliant. However, you can allow access using older FileCloud (non RMC compliant) clients by enabling this setting. ➡ Enable Remote Client Management (RMC)
Log Level	This setting is to control the logging level. **The default is "PROD"**. Changing the log level to "DEV" will generate more logging information and can have performance impact as well as take up more storage. Tech Support might change this value to help in troubleshooting any issues you might have.
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

4. Configure Cron Jobs

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

- Sending email notifications such as file change notification, share notification, etc.,
- Sending admin summary emails
- Perform recycle bin cleanup
- Delete expired shares
- Archiving old audit records

➡ Set Up a Cron Job

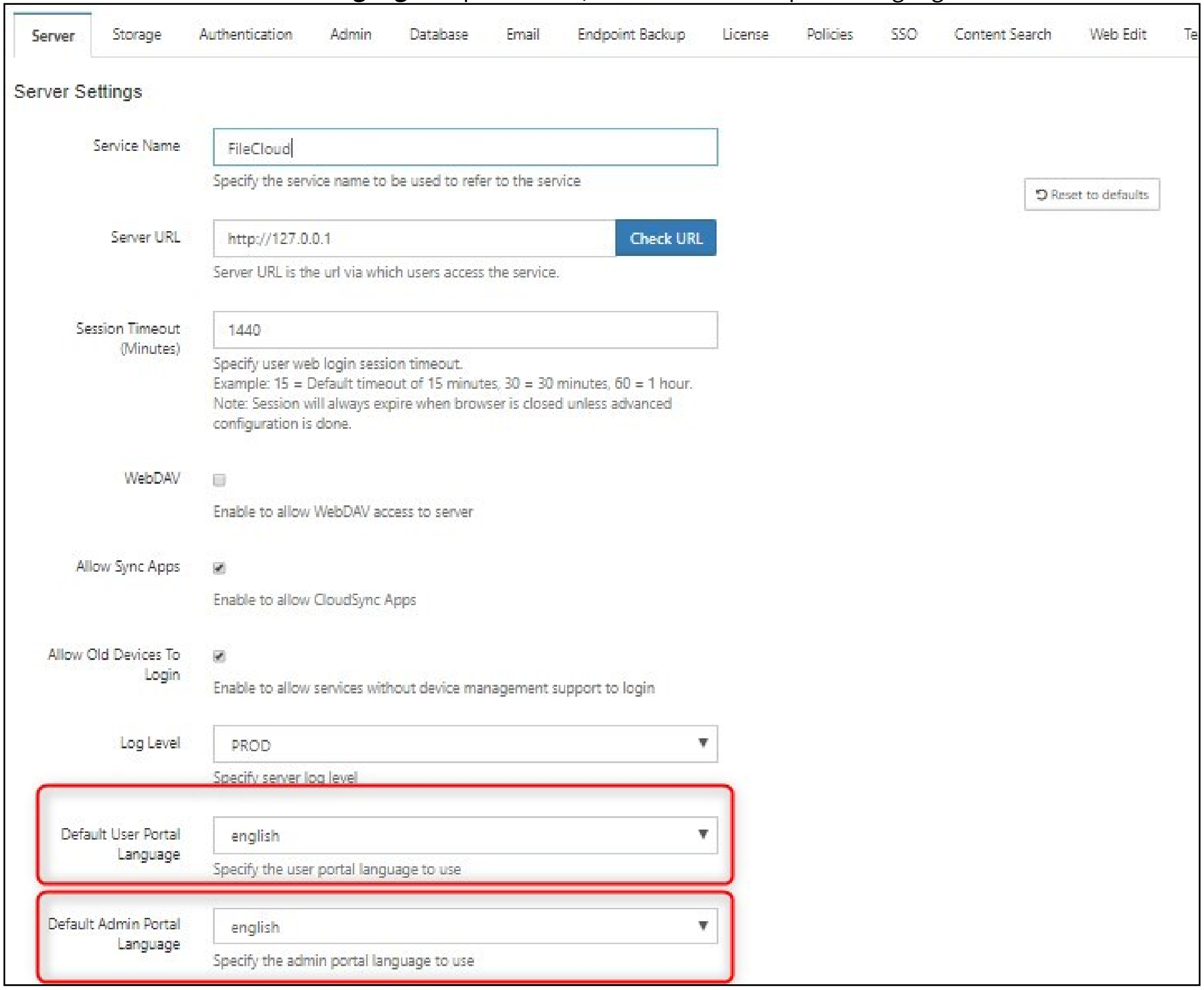
➡ Configure System-Generated Emails

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.



Server Settings

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

Server URL: http://127.0.0.1
Server URL is the url via which users access the service.

Session Timeout (Minutes): 1440
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: □
Enable to allow WebDAV access to server

Allow Sync Apps: ☑
Enable to allow CloudSync Apps

Allow Old Devices To Login: ☑
Enable to allow services without device management support to login

Log Level: PROD
Specify server log level

Default User Portal Language: english
Specify the user portal language to use

Default Admin Portal Language: english
Specify the admin portal language to use

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.

Setting Up a Cron Job or Scheduled Task

> ❗ If you are running a multi-tenant system with FileCloud, make sure all site URLs for each site are accessible from the local site. These are used by the task scheduler/Cron to run automated tasks for each site

Introduction

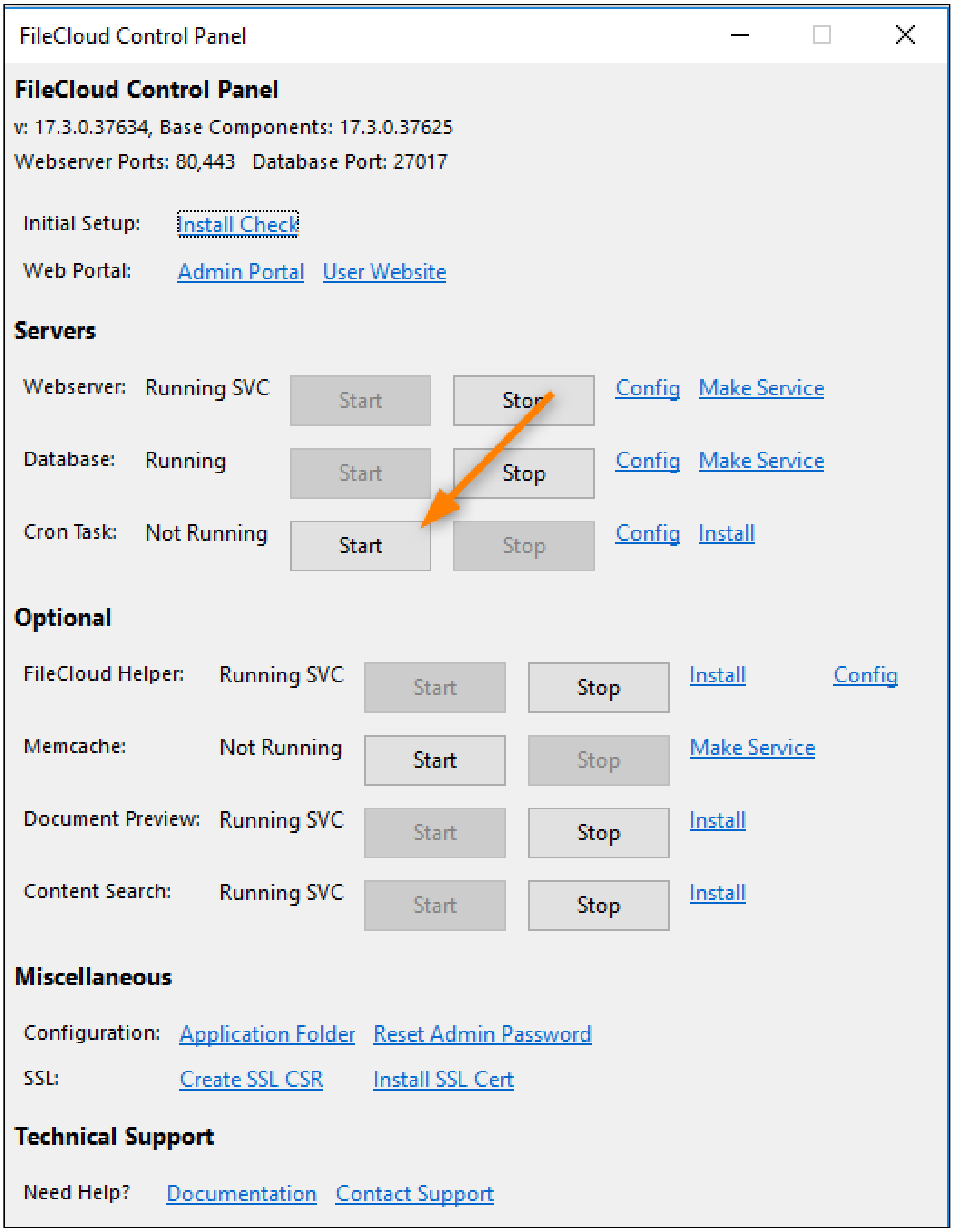
FileCloud needs a Cron job to perform certain ongoing maintenance tasks.
These tasks include:

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

Setup Cron Job in Windows

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

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



FileCloud Control Panel

FileCloud Control Panel

v: 17.3.0.37634, Base Components: 17.3.0.37625

Webserver Ports: 80,443   Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

Webserver: Running SVC

Database: Running

Cron Task: Not Running

Optional

FileCloud Helper: Running SVC

Memcache: Not Running

Document Preview: Running SVC

Content Search: Running SVC

Miscellaneous

Configuration: Application Folder Reset Admin Password

SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support

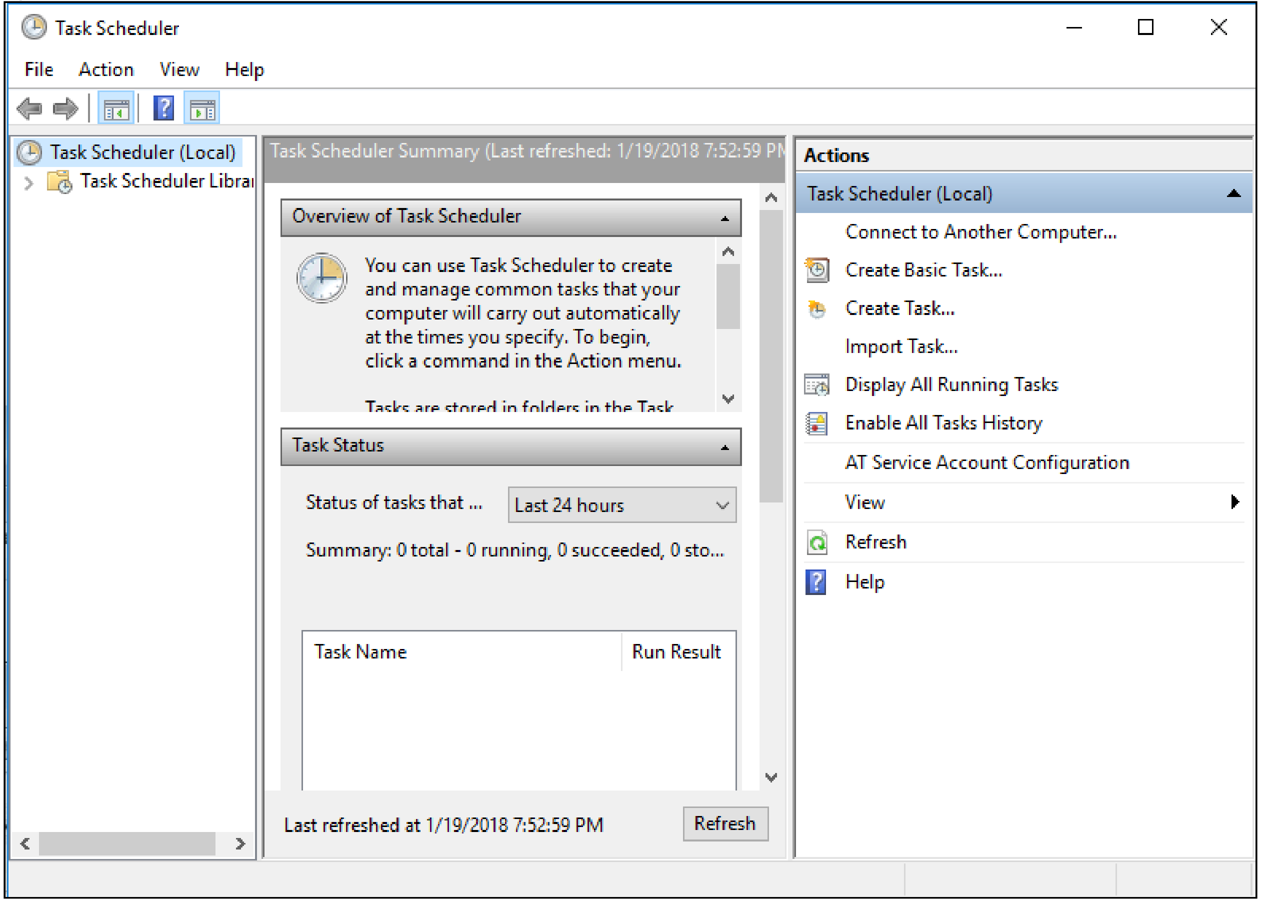
ⓘ Additional Settings for the Cron Task are available by editing the xampp\cron.ini file
[settings]
frequency=300 ---> Frequency of Cron in seconds (Default is every 5 mins)
timeout=600 ---> Time to wait for Cron to complete in seconds (Default is 10 mins)

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

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

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

2. Open Task Scheduler:



You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task

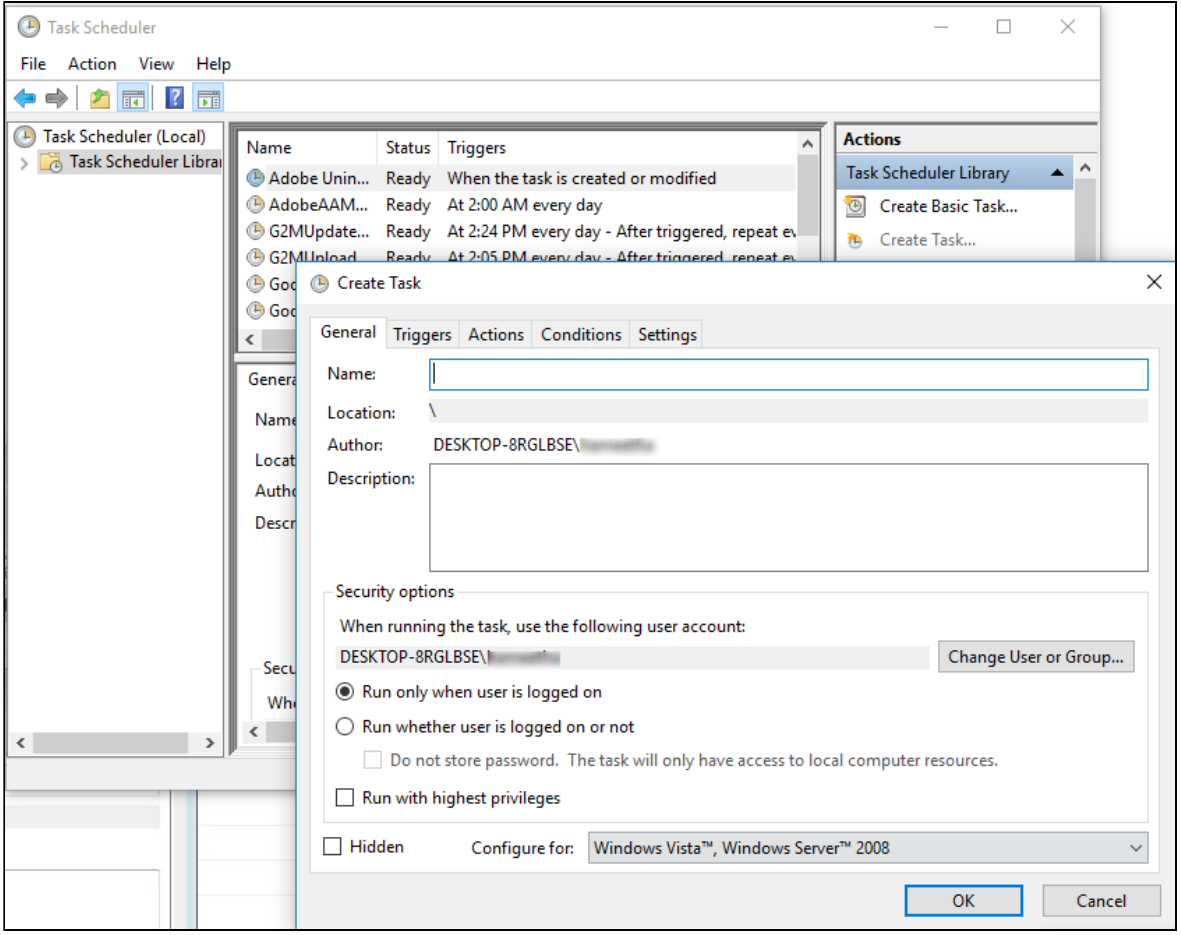
Status of tasks that ... Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 sto...

Last refreshed at 1/19/2018 7:52:59 PM

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

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



Name	Status	Triggers
Adobe Unin...	Ready	When the task is created or modified
AdobeAAM...	Ready	At 2:00 AM every day
G2MUpdate...	Ready	At 2:24 PM every day - After triggered, repeat ev
G2MUpload...	Ready	At 2:05 PM every day - After triggered, repeat ev

Name:

Location: \

Author: DESKTOP-8RGLBSE\[redacted]

Description:

Security options

When running the task, use the following user account:

DESKTOP-8RGLBSE\[redacted]

● Run only when user is logged on

○ Run whether user is logged on or not

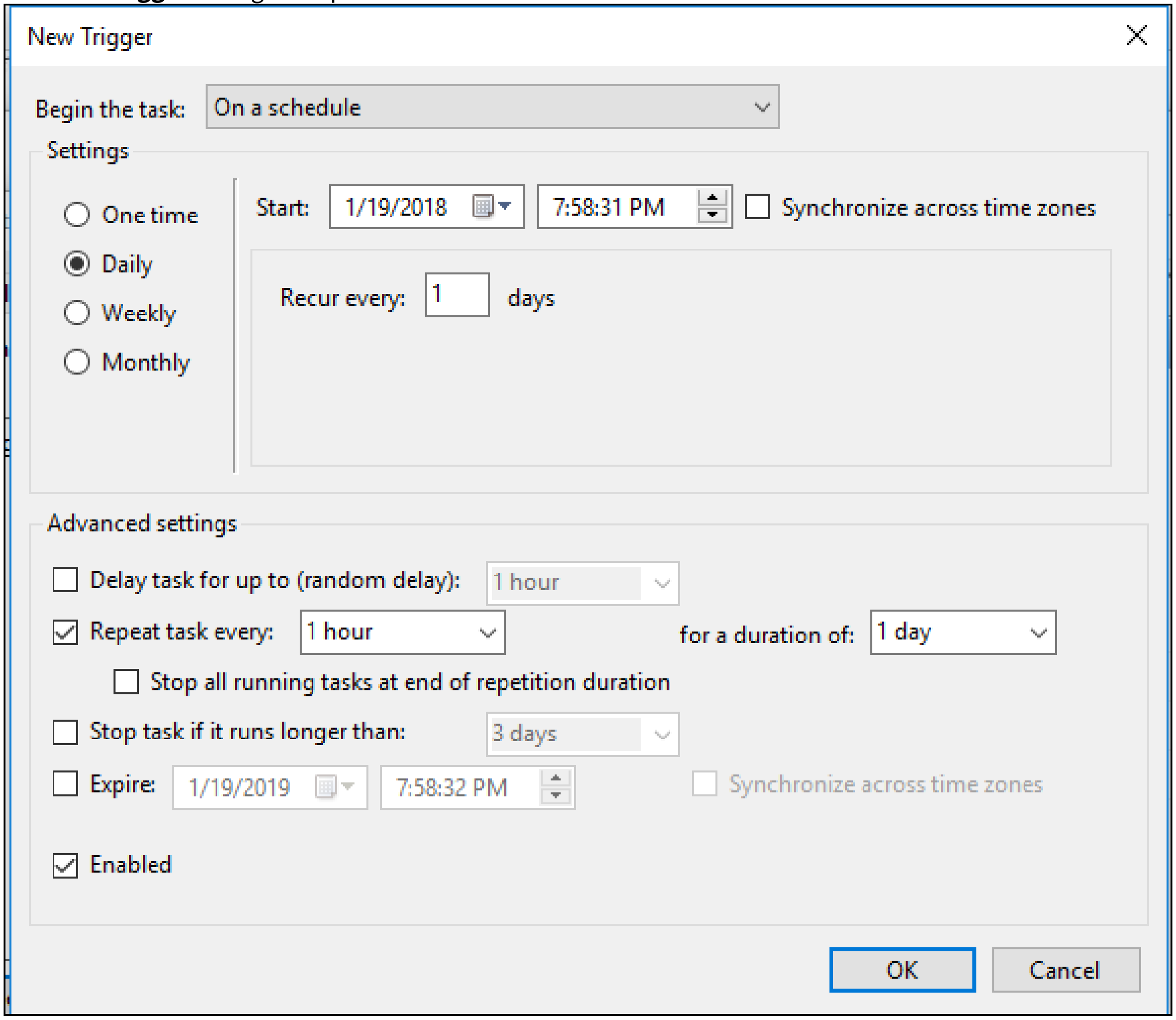
□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

5. On the **Triggers Tab:**

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



Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 1/19/2018 7:58:31 PM □ Synchronize across time zones

Recur every: 1 days

Advanced settings

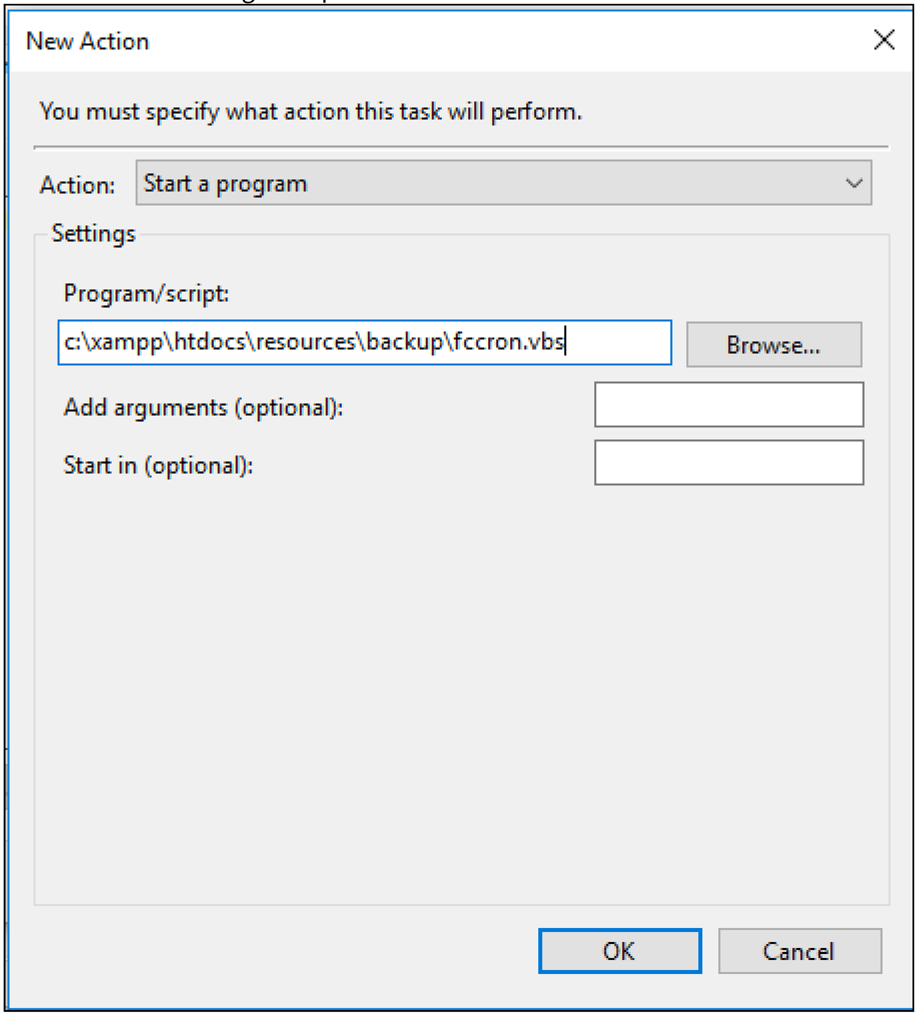
□ Delay task for up to (random delay): 1 hour
☑ Repeat task every: 1 hour for a duration of: 1 day
□ Stop all running tasks at end of repetition duration
□ Stop task if it runs longer than: 3 days
□ Expire: 1/19/2019 7:58:32 PM □ Synchronize across time zones

☑ Enabled

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

6. On the **Actions Tab:**

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



New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: c:\xampp\htdocs\resources\backup\fccron.vbs

Add arguments (optional):

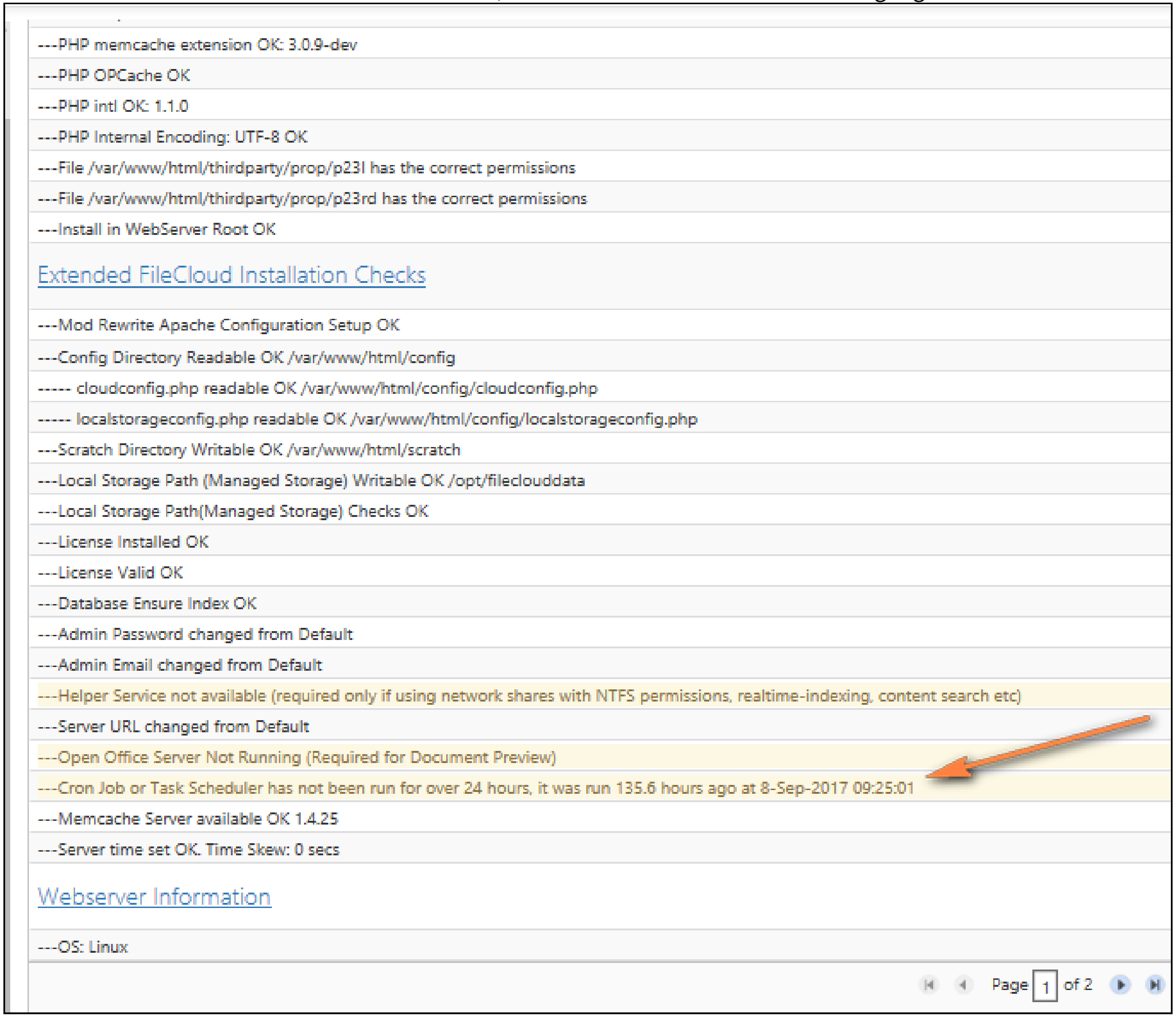
Start in (optional):

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

Verify the Cron Job is Running

1. Go to admin portal.

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



```
---PHP memcache extension OK: 3.0.9-dev
---PHP OPCache OK
---PHP intl OK: 1.1.0
---PHP Internal Encoding: UTF-8 OK
---File /var/www/html/thirdparty/prop/p23l has the correct permissions
---File /var/www/html/thirdparty/prop/p23rd has the correct permissions
---Install in WebServer Root OK
```

Extended FileCloud Installation Checks

```
---Mod Rewrite Apache Configuration Setup OK
---Config Directory Readable OK /var/www/html/config
----- cloudconfig.php readable OK /var/www/html/config/cloudconfig.php
----- localstorageconfig.php readable OK /var/www/html/config/localstorageconfig.php
---Scratch Directory Writable OK /var/www/html/scratch
---Local Storage Path (Managed Storage) Writable OK /opt/fileclouddata
---Local Storage Path(Managed Storage) Checks OK
---License Installed OK
---License Valid OK
---Database Ensure Index OK
---Admin Password changed from Default
---Admin Email changed from Default
---Helper Service not available (required only if using network shares with NTFS permissions, realtime-indexing, content search etc)
---Server URL changed from Default
---Open Office Server Not Running (Required for Document Preview)
---Cron Job or Task Scheduler has not been run for over 24 hours, it was run 135.6 hours ago at 8-Sep-2017 09:25:01
---Memcache Server available OK 1.4.25
---Server time set OK. Time Skew: 0 secs
```

Webserver Information

```
---OS: Linux
```

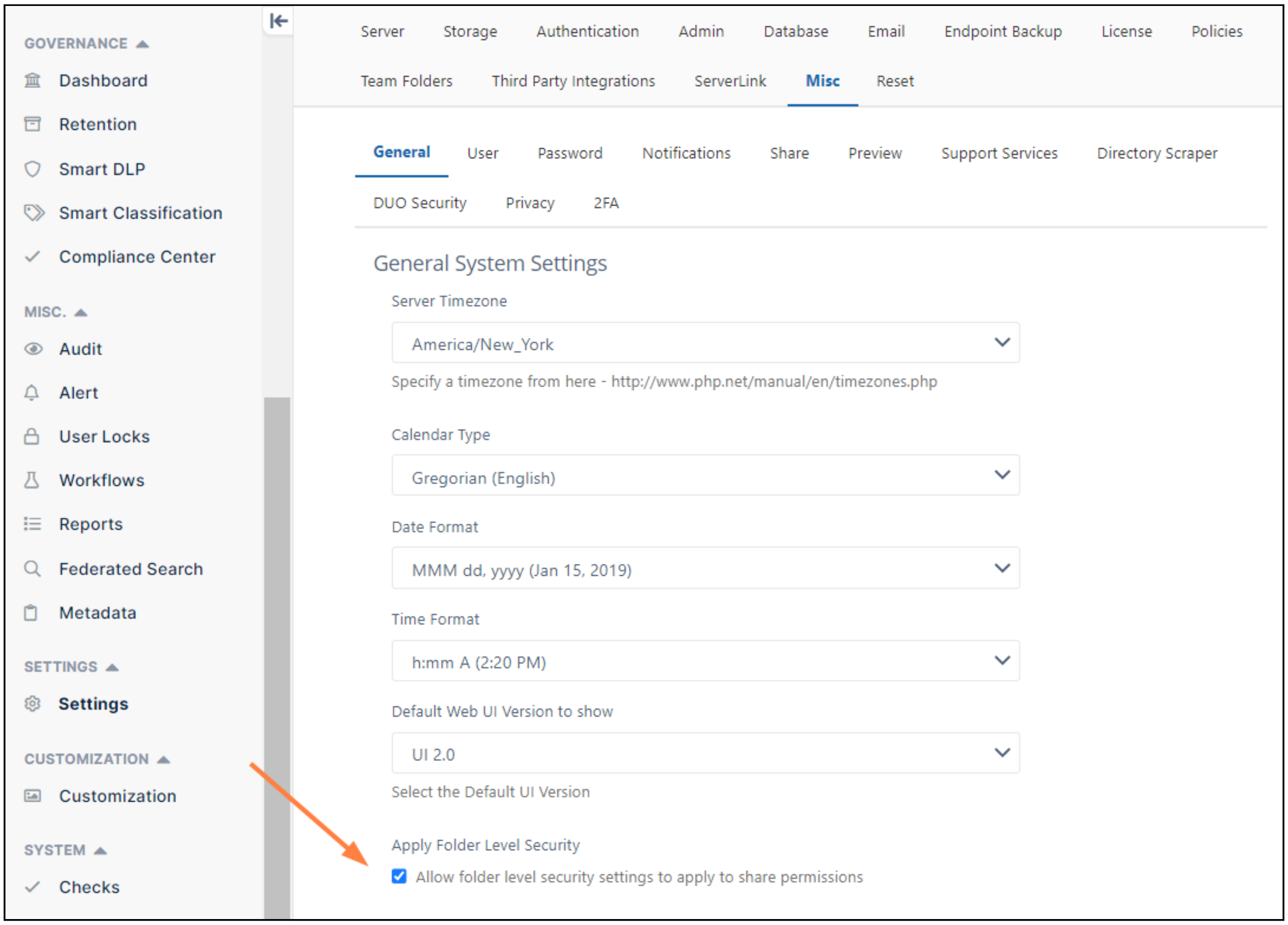
Enable Folder-Level Permissions

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**
✓ 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	✗ 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



General System Settings

Server Timezone: America/New_York

Specify a timezone from here - http://www.php.net/manual/en/timezones.php

Calendar Type: Gregorian (English)

Date Format: MMM dd, yyyy (Jan 15, 2019)

Time Format: h:mm A (2:20 PM)

Default Web UI Version to show: UI 2.0

Select the Default UI Version

Apply Folder Level Security

☑ Allow folder level security settings to apply to share permissions

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.

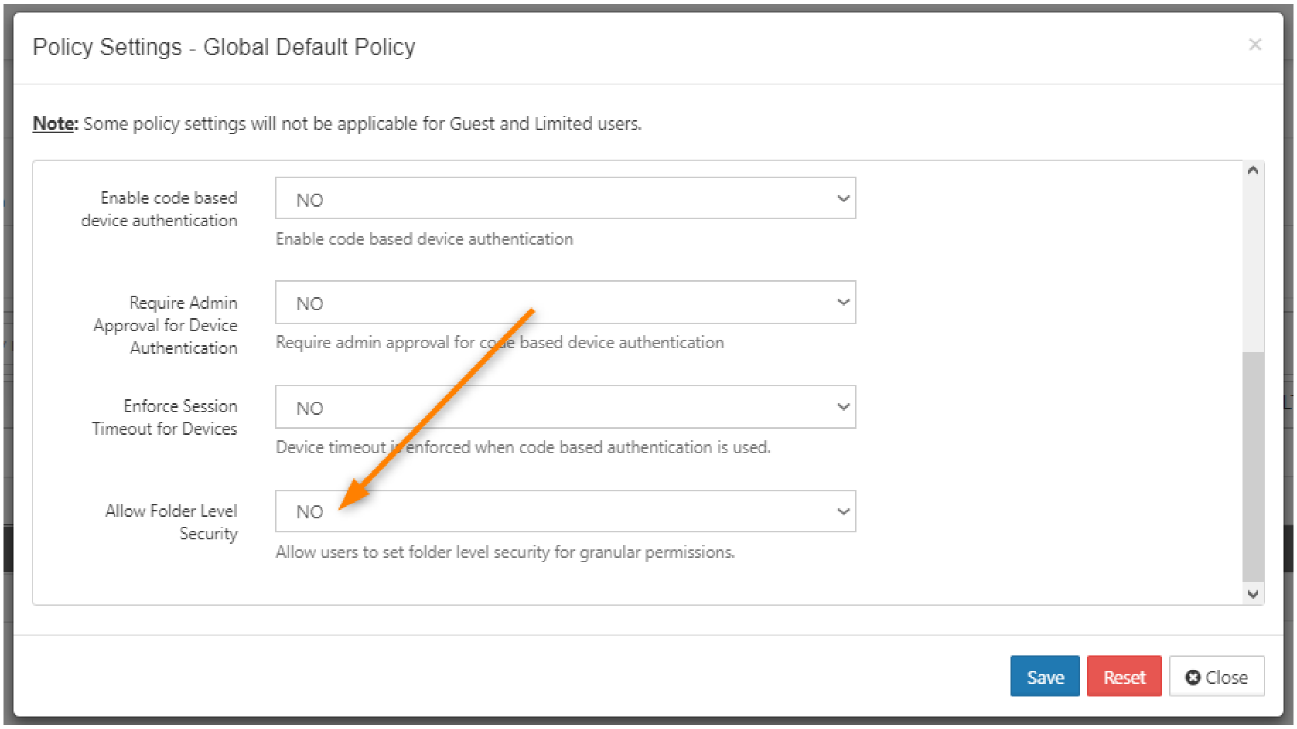
However, administrators can allow this behavior by:

- 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.

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

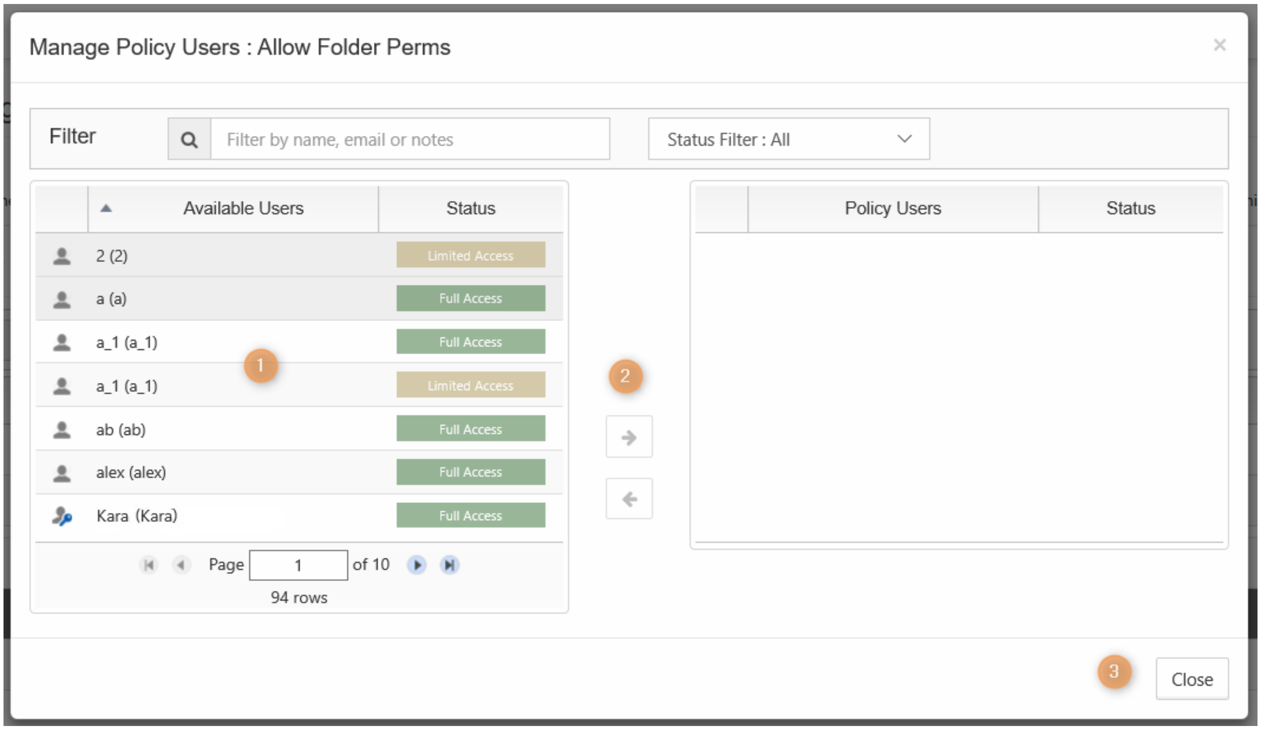
1. Log into the admin portal.
2. In the left navigation pane, under **SETTINGS**, click **Settings**.
3. On the **Manage Settings** screen, select the **Policies** tab.
4. On the **Manage Policy** tab, click the **Global Default Policy** row, and then click the edit button (✎).

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



Manage Policy Users : Allow Folder Perms

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

Page 1 of 10

94 rows

Policy Users	Status

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 (👥).

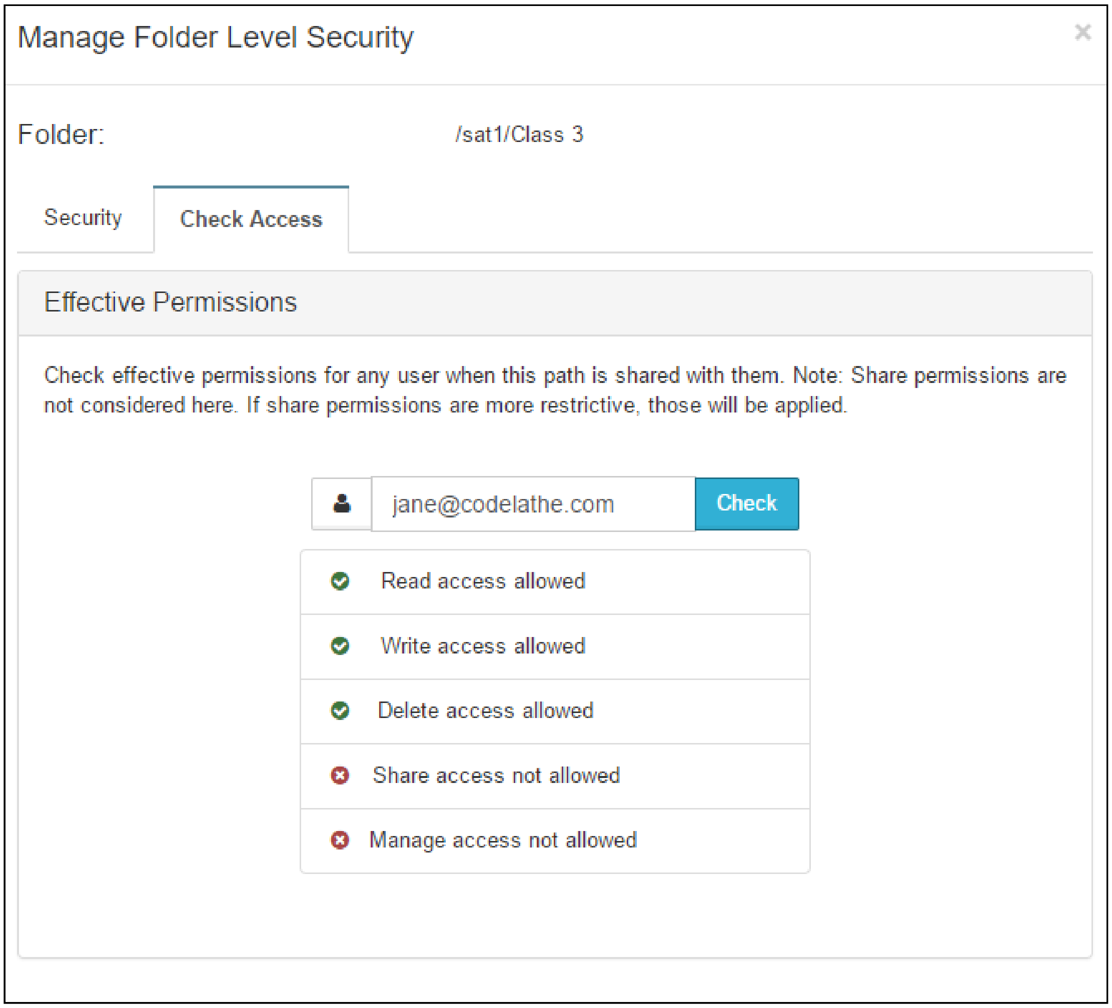
3. Check Effective Permissions

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



Manage Folder Level Security

Folder: /sat1/Class 3

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.

jane@codelathe.com

✓ Read access allowed

✓ Write access allowed

✓ Delete access allowed

☒ Share access not allowed

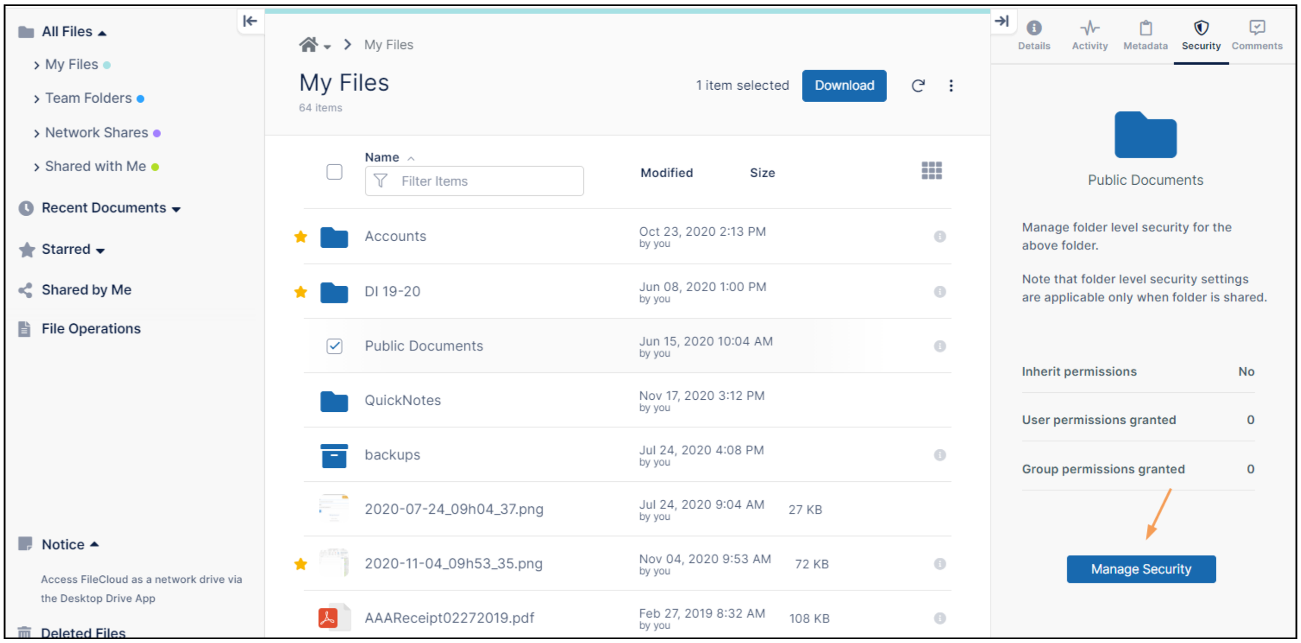
☒ Manage access not allowed

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.



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

Public Documents

Manage folder level security for the above folder.

Note that folder level security settings are applicable only when folder is shared.

Inherit permissions	No
User permissions granted	0
Group permissions granted	0

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

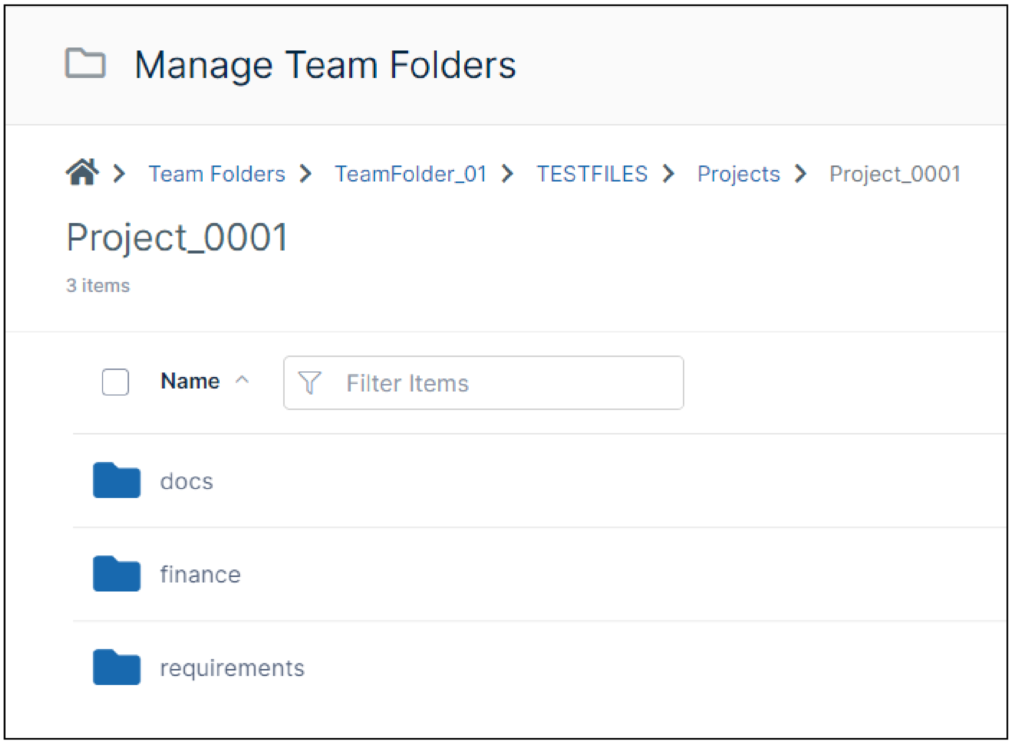
In this scenario, an administrator gives two groups access to a folder, but only gives one group access to one of its sub-folders.

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.**



Manage Team Folders

Team Folders > TeamFolder_01 > TESTFILES > Projects > Project_0001

Project_0001

3 items

□ Name ^ Filter Items

docs

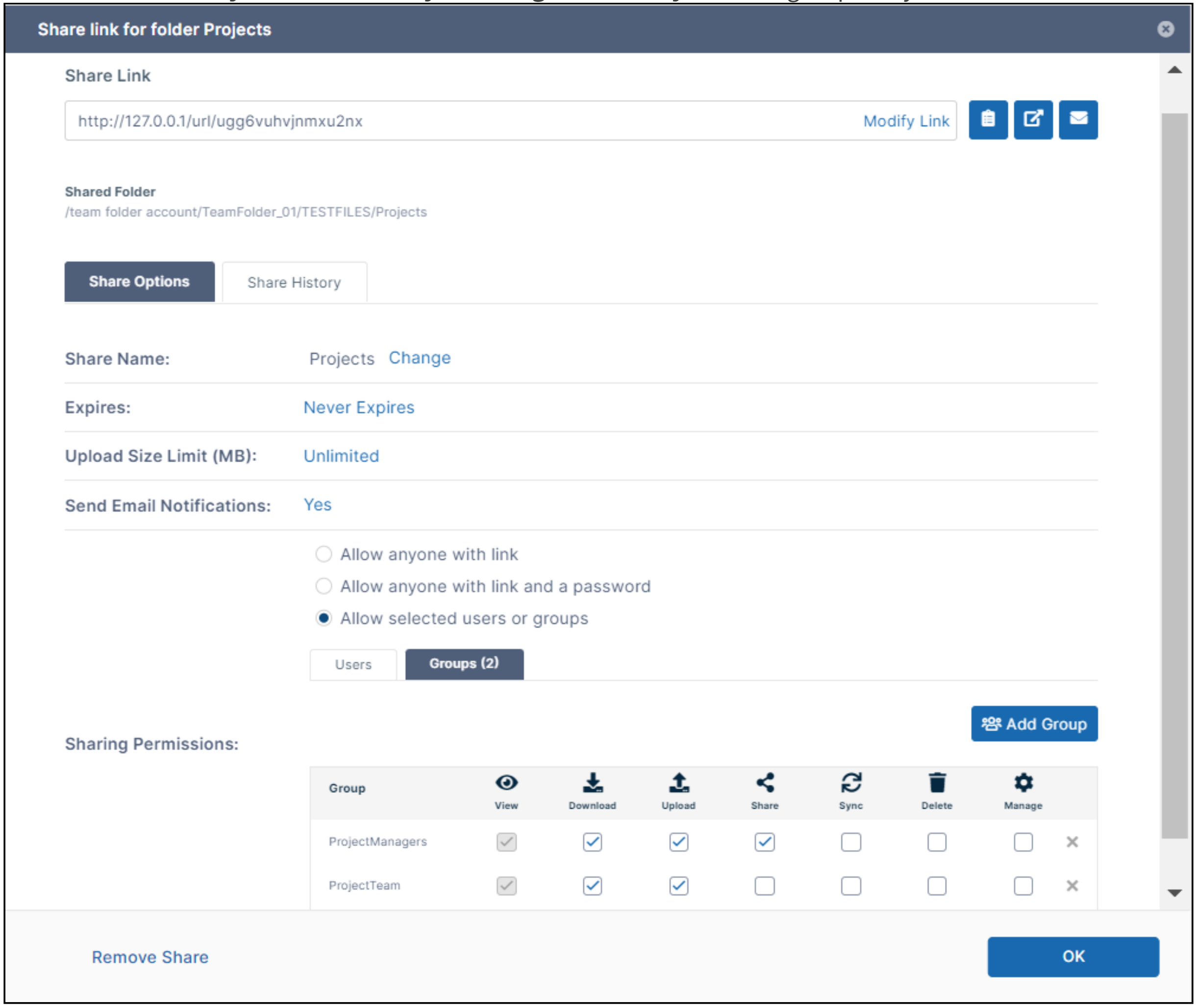
finance

requirements

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

http://127.0.0.1/url/ugg6vuhvjnmxu2nx Modify Link

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

Share Name: Projects Change

Expires: Never Expires

Upload Size Limit (MB): Unlimited

Send Email Notifications: Yes

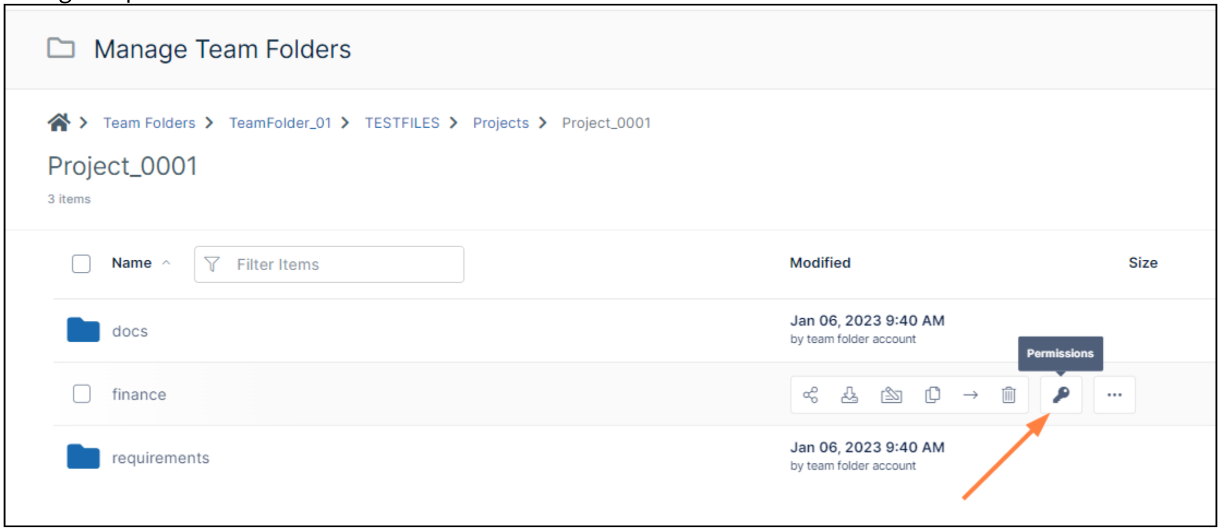
○ Allow anyone with link
○ Allow anyone with link and a password
● Allow selected users or groups

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:



Manage Team Folders

Team Folders > TeamFolder_01 > TESTFILES > Projects > Project_0001

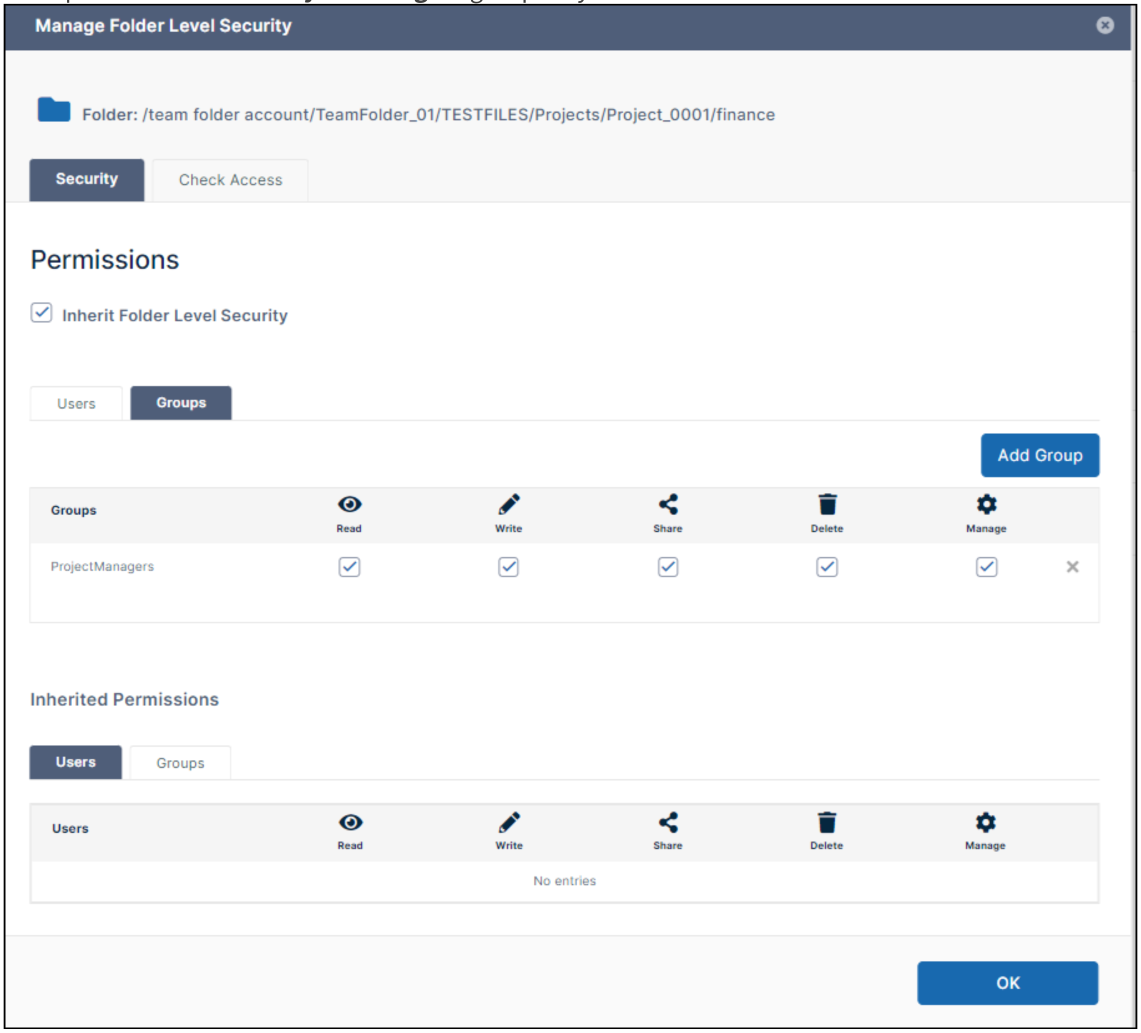
Project_0001

3 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	

Example of giving permissions to only specific users or groups

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



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

Permissions

☑ Inherit Folder Level Security

Groups	Read	Write	Share	Delete	Manage	
ProjectManagers	☑	☑	☑	☑	☑	✕

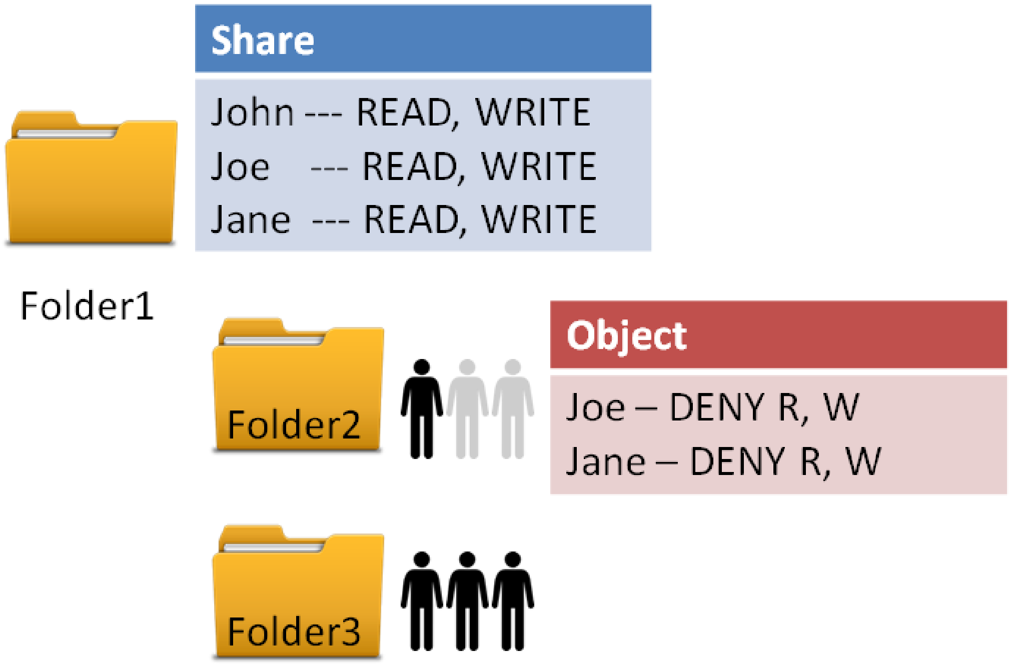
Inherited Permissions

Users	Read	Write	Share	Delete	Manage
No entries					

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.

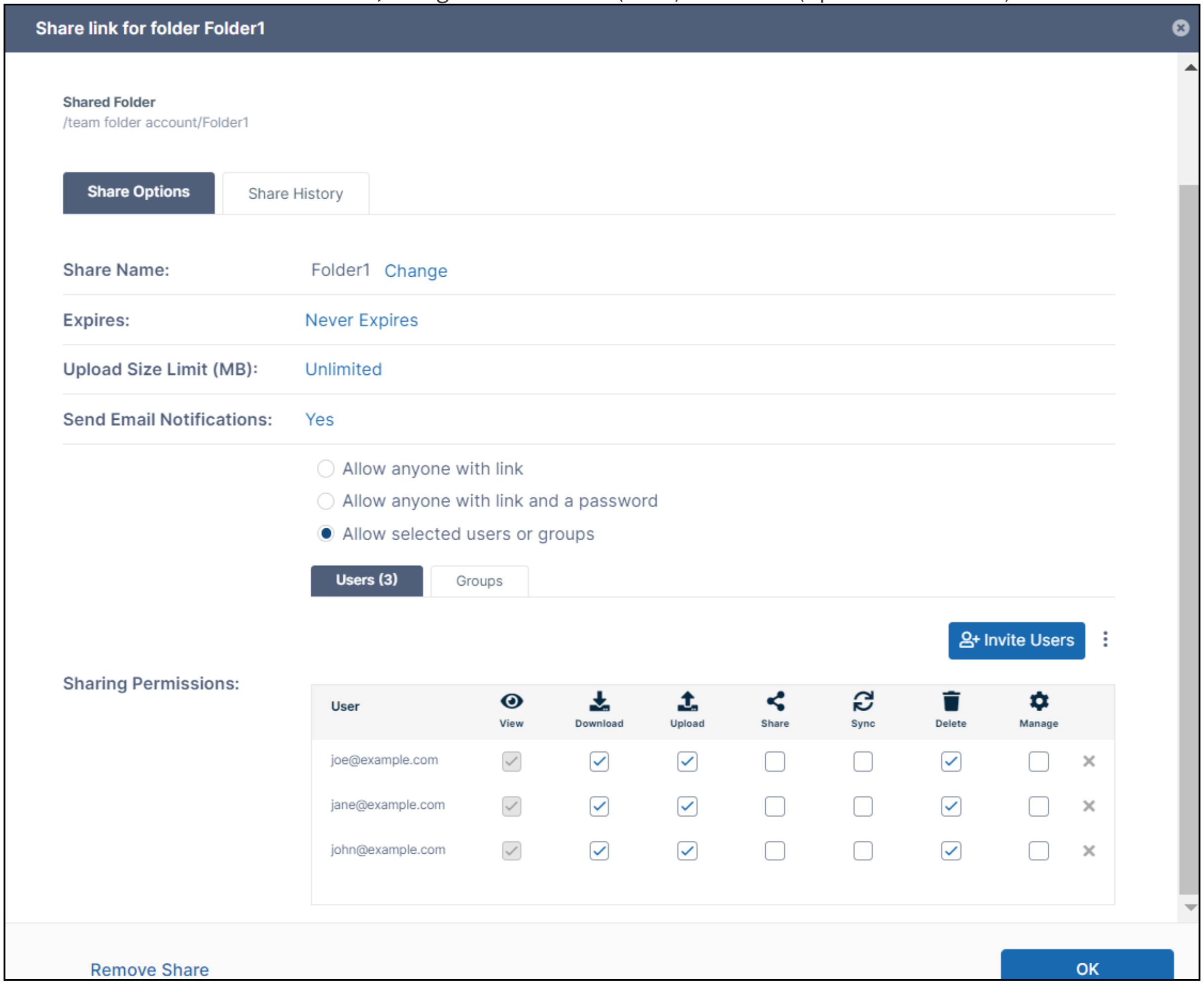
The administrator therefore wants the folder access to be the following:

- 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.



Share link for folder Folder1

Shared Folder
/team folder account/Folder1

Share Name: Folder1 Change

Expires: Never Expires

Upload Size Limit (MB): Unlimited

Send Email Notifications: Yes

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

Sharing Permissions:

User	View	Download	Upload	Share	Sync	Delete	Manage	
joe@example.com	☑	☑	☑	□	□	☑	□	×
jane@example.com	☑	☑	☑	□	□	☑	□	×
john@example.com	☑	☑	☑	□	□	☑	□	×

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 ✓ Access its content	✓ See it listed ✓ Access its content	✓ See it listed ✓ Access its content

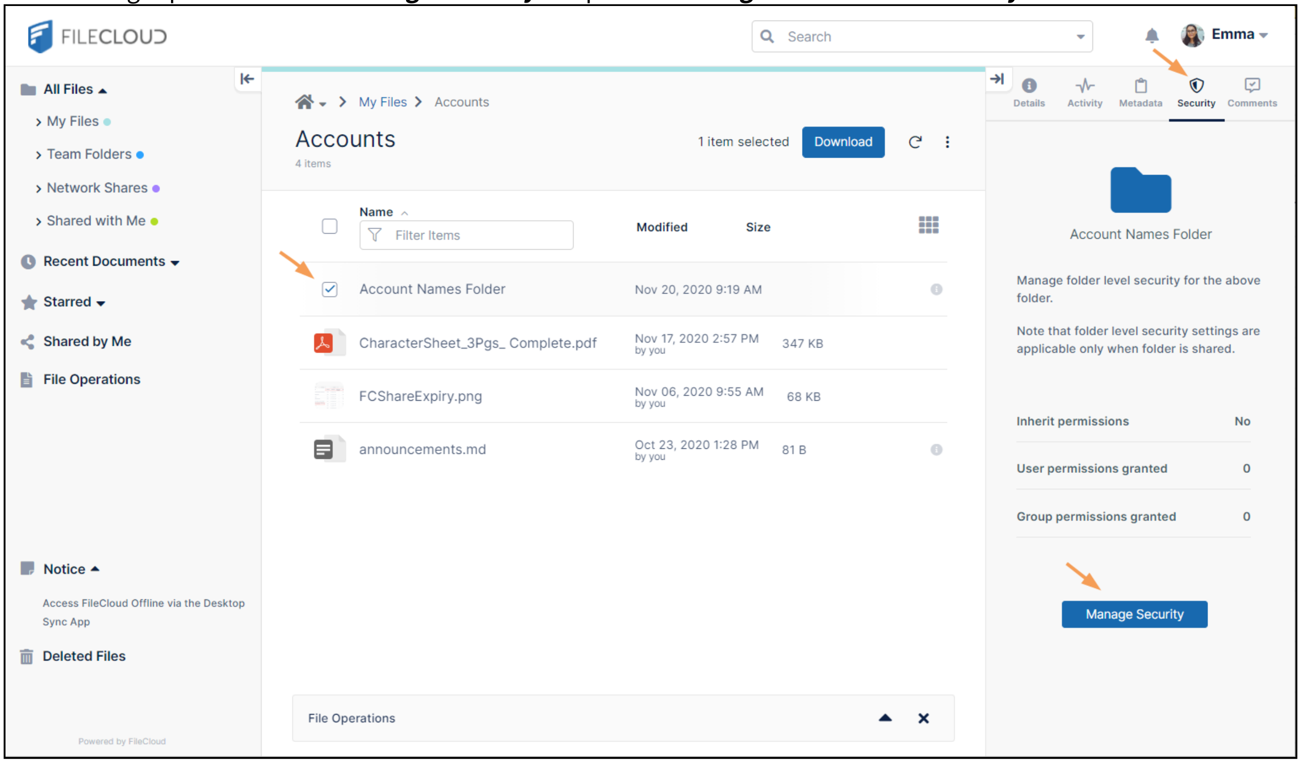
Example of a Sharing Scenario

User	Folder1	Folder2	Folder3
Joe	✓ See it listed ✓ Access its content	✗ See it listed ✗ Access its content	✓ See it listed ✓ Access its content
Jane	✓ See it listed ✓ Access its content	✗ See it listed ✗ Access its content	✓ See it listed ✓ Access its content

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.



☐ Name	Modified	Size
☑ Account Names Folder	Nov 20, 2020 9:19 AM	
CharacterSheet_3Pgs_ Complete.pdf	Nov 17, 2020 2:57 PM by you	347 KB
FCShareExpiry.png	Nov 06, 2020 9:55 AM by you	68 KB
announcements.md	Oct 23, 2020 1:28 PM by you	81 B

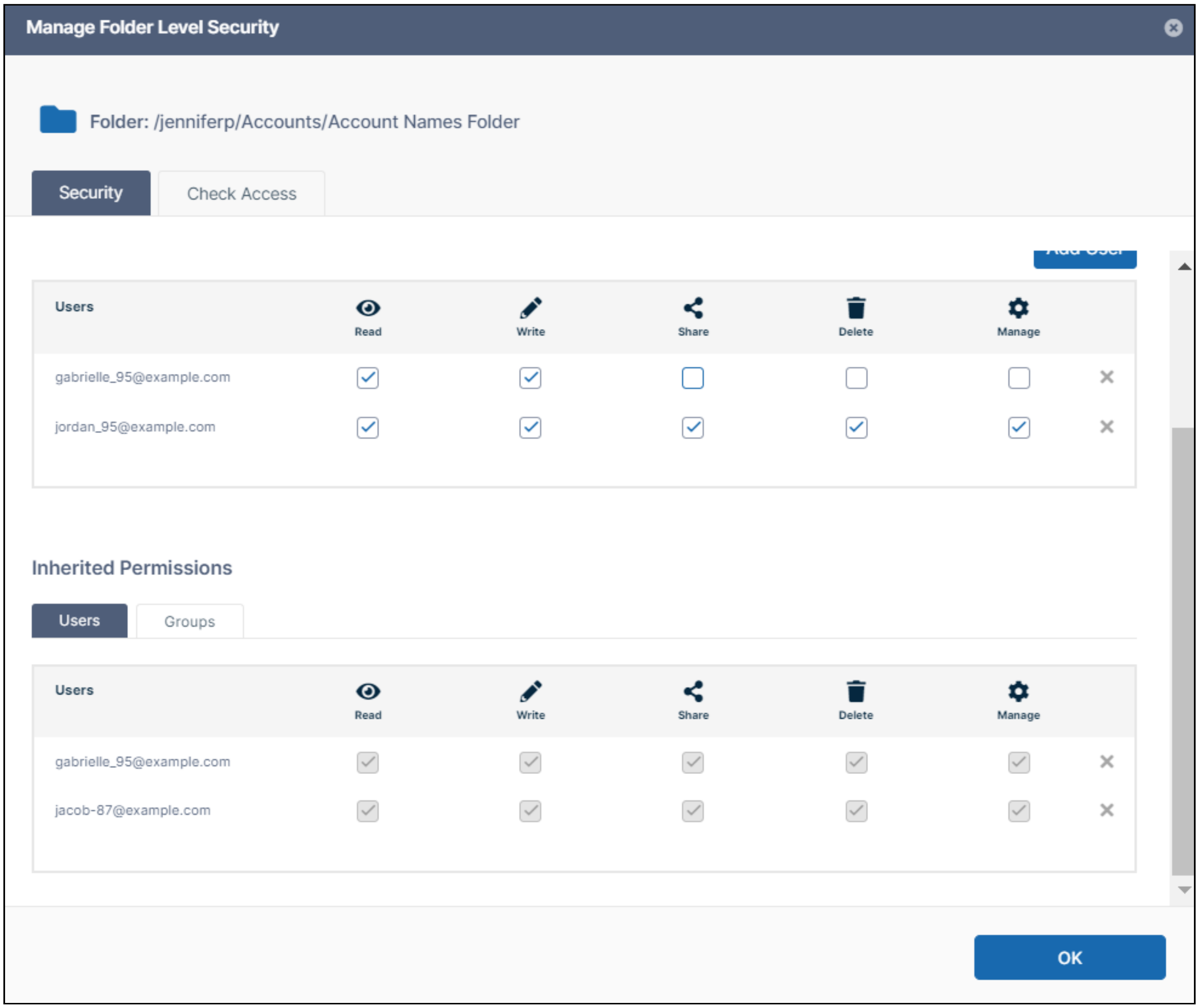
Account Names Folder

Manage folder level security for the above folder.

Note that folder level security settings are applicable only when folder is shared.

Inherit permissions	No
User permissions granted	0
Group permissions granted	0

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

Users	Read	Write	Share	Delete	Manage	
gabrielle_95@example.com	☑	☑	☐	☐	☐	✕
jordan_95@example.com	☑	☑	☑	☑	☑	✕

Inherited Permissions

Users	Read	Write	Share	Delete	Manage	
gabrielle_95@example.com	☑	☑	☑	☑	☑	✕
jacob-87@example.com	☑	☑	☑	☑	☑	✕

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

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

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

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 seperate 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:

1. User's folder-level permissions for current folder *(if it exists)*
2. Group's folder-level permissions for current folder *(if it exists)*
3. Inherit permissions
    a. 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

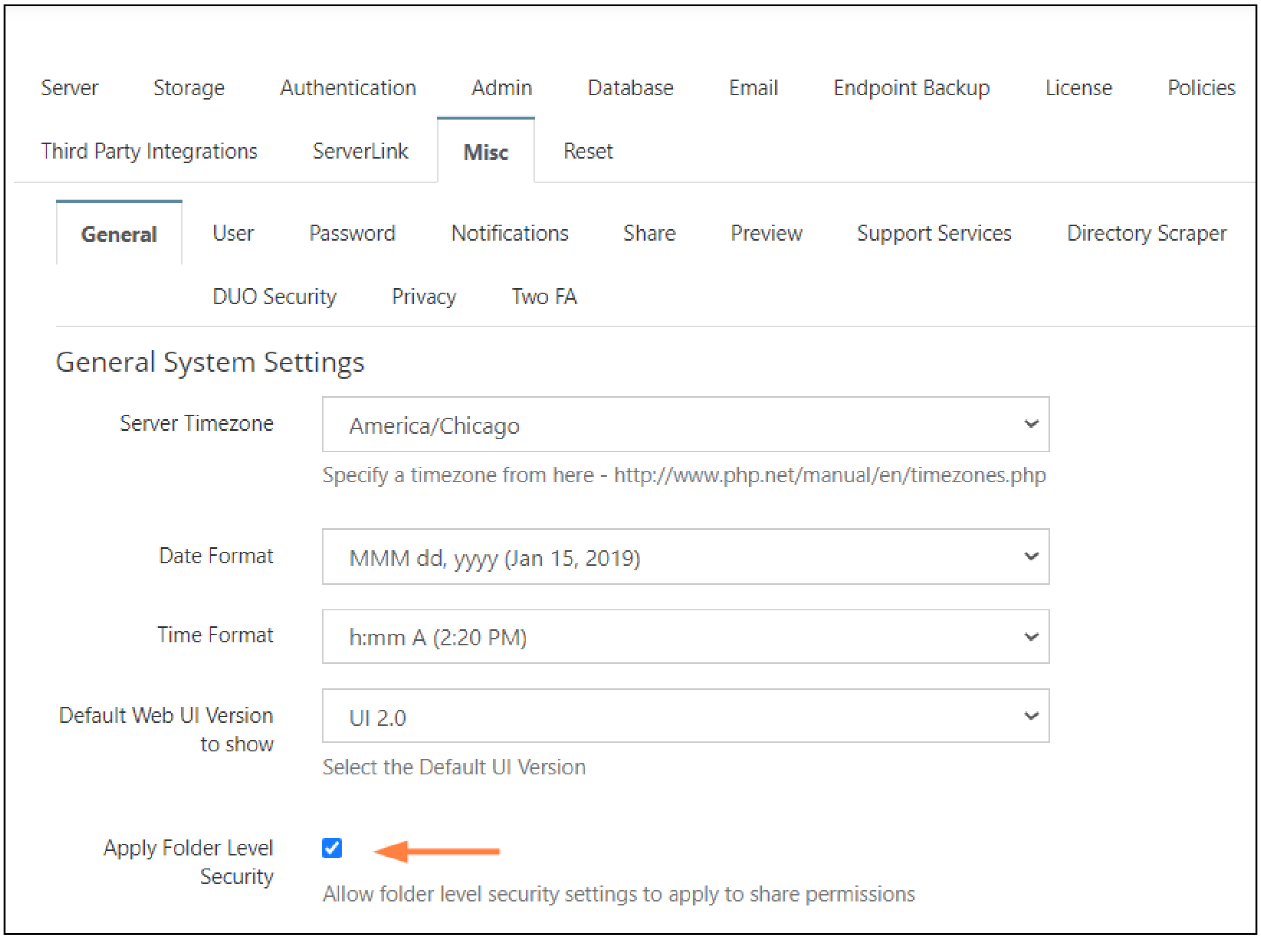
Once a Team Folder is shared, all users with access to the share will see Team Folders in the navigation panel of the user portal and all FileCloud clients such as Sync, Drive, Outlook and the Office Add-In. These users' actions are limited by the **share** permissions. Additional limitations may be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



General System Settings

Server Timezone: America/Chicago

Specify a timezone from here - http://www.php.net/manual/en/timezones.php

Date Format: MMM dd, yyyy (Jan 15, 2019)

Time Format: h:mm A (2:20 PM)

Default Web UI Version to show: UI 2.0

Select the Default UI Version

Apply Folder Level Security: ☑

Allow folder level security settings to apply to share permissions

Apply granular folder permissions to Team Folders:

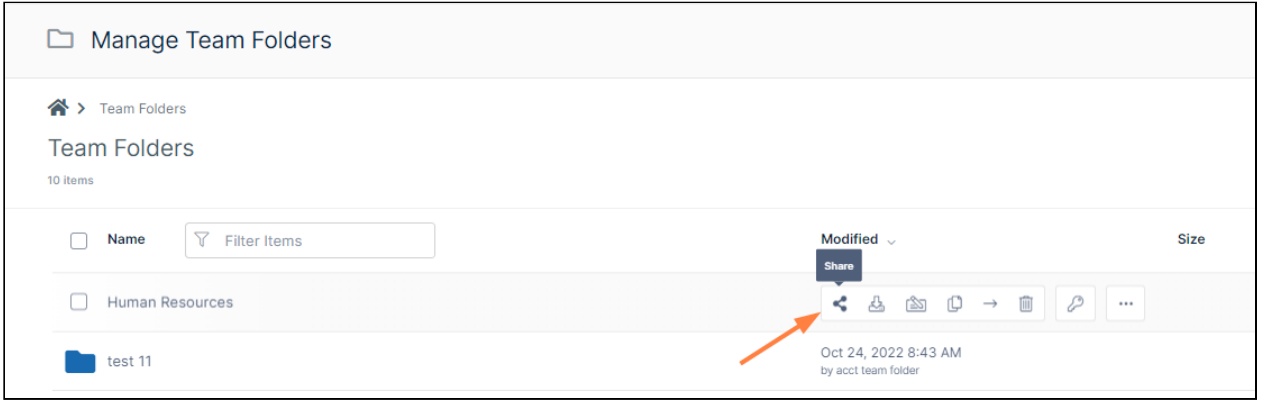
You can apply granular folder permissions to the top-level team folder or to its sub-folders.

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.



Manage Team Folders

Team Folders

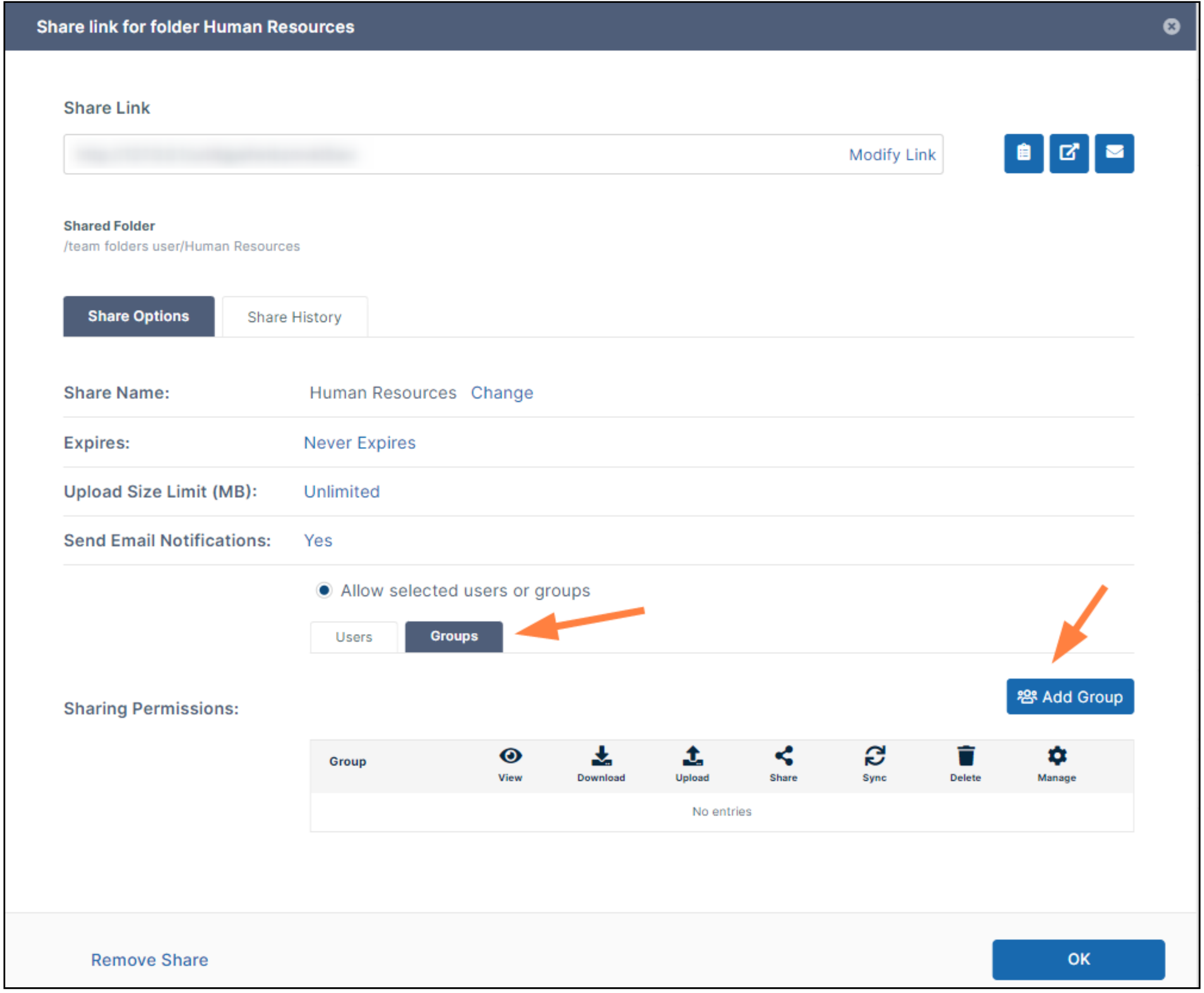
Team Folders

10 items

□	Name	Modified	Size
□	Human Resources		
	test 11	Oct 24, 2022 8:43 AM by acct team folder	

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**.



Share link for folder Human Resources

Share Link

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

Sharing Permissions:

Add Group

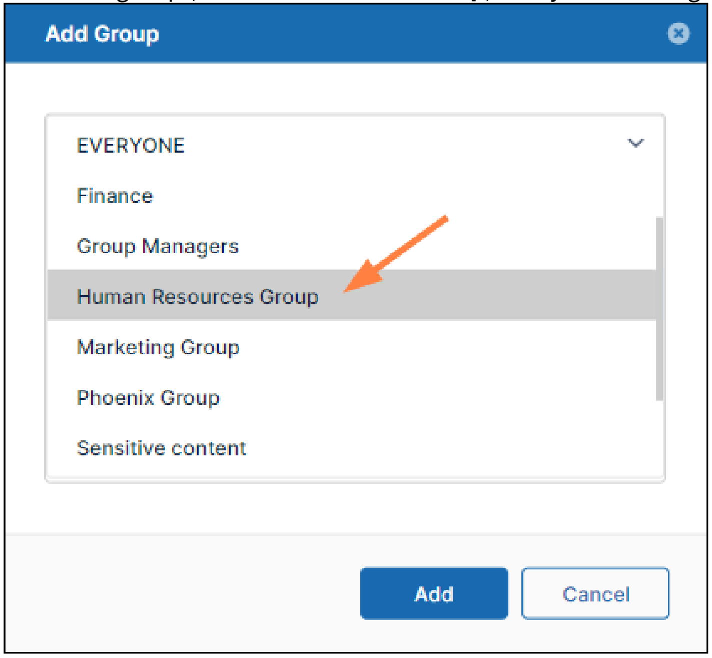
Group	View	Download	Upload	Share	Sync	Delete	Manage
No entries							

Remove Share

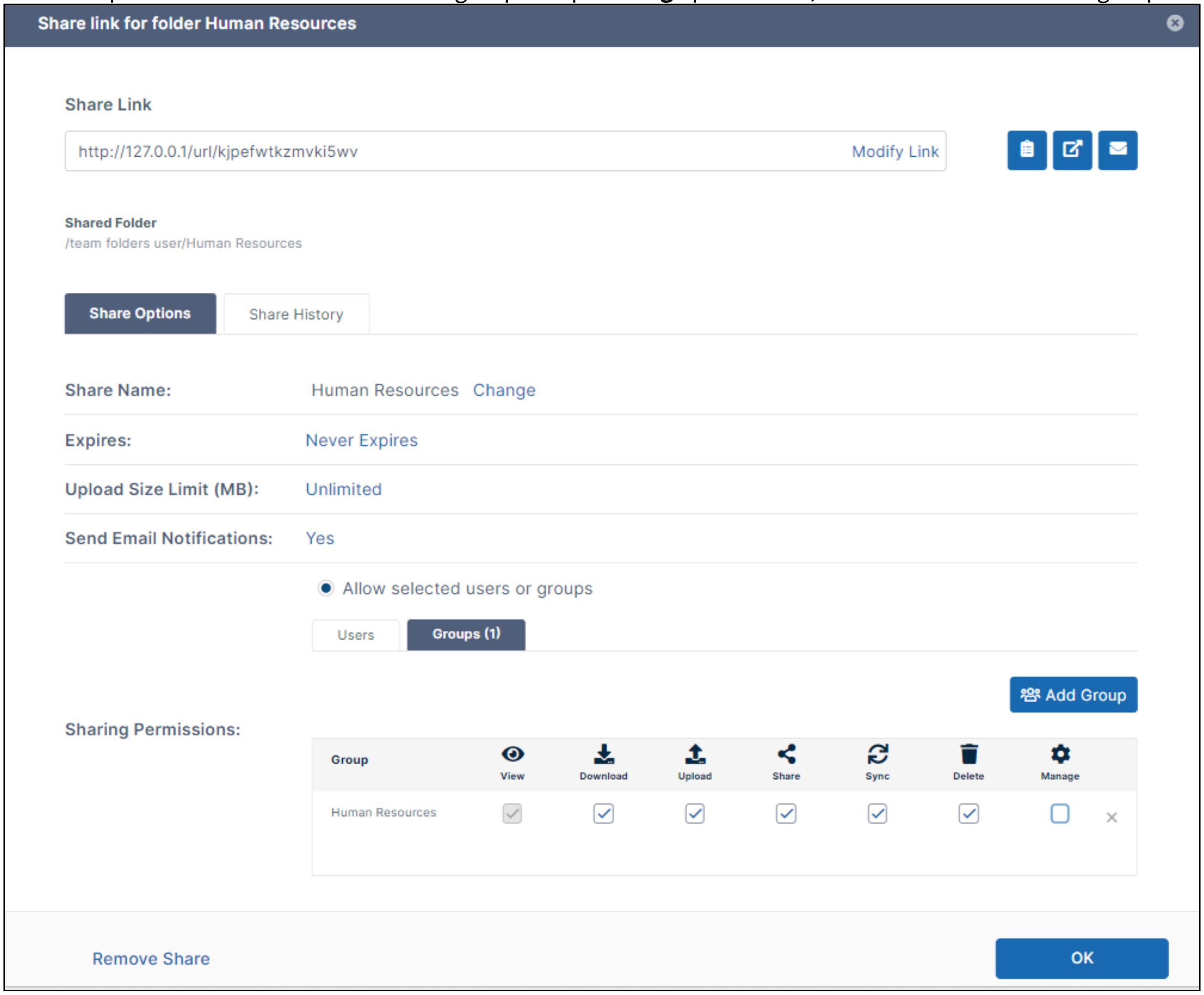
OK

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

http://127.0.0.1/url/kjpefwtkzmvki5wv

Shared Folder
/team folders user/Human Resources

Share Name: Human Resources

Expires: Never Expires

Upload Size Limit (MB): Unlimited

Send Email Notifications: Yes

● Allow selected users or groups

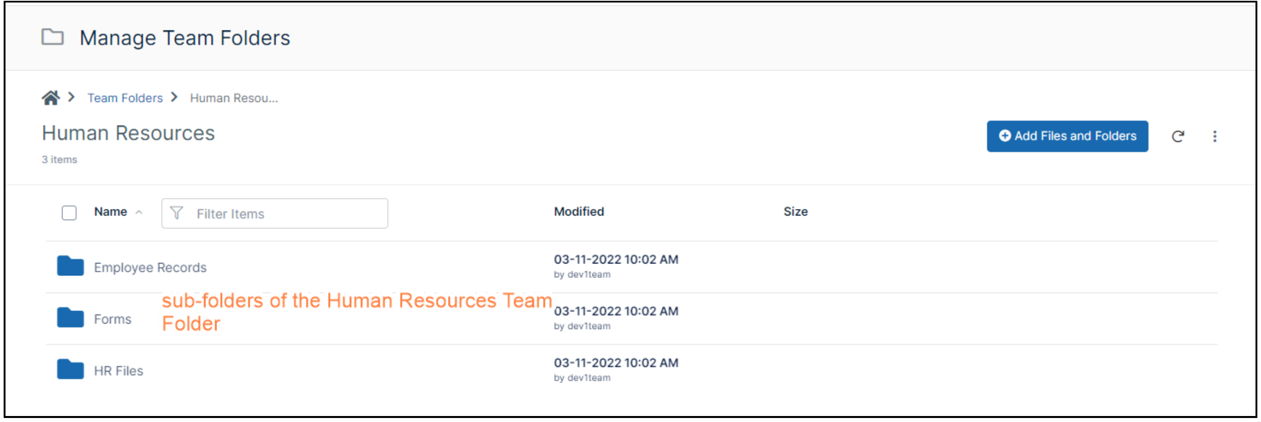
Sharing Permissions:

Group	View	Download	Upload	Share	Sync	Delete	Manage	
Human Resources	☑	☑	☑	☑	☑	☑	□	×

7. Close the dialog box.

Restrict permissions to specific users within the group

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



Manage Team Folders

Team Folders > Human Resou...

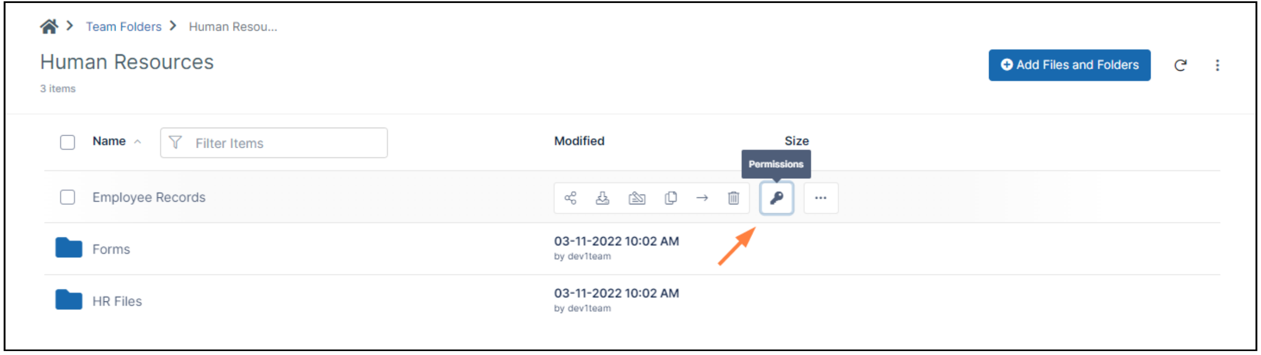
Human Resources

3 items

Name	Modified	Size
Employee Records	03-11-2022 10:02 AM by dev1team	
Forms	03-11-2022 10:02 AM by dev1team	
HR Files	03-11-2022 10:02 AM by dev1team	

sub-folders of the Human Resources Team Folder

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.



Team Folders > Human Resou...

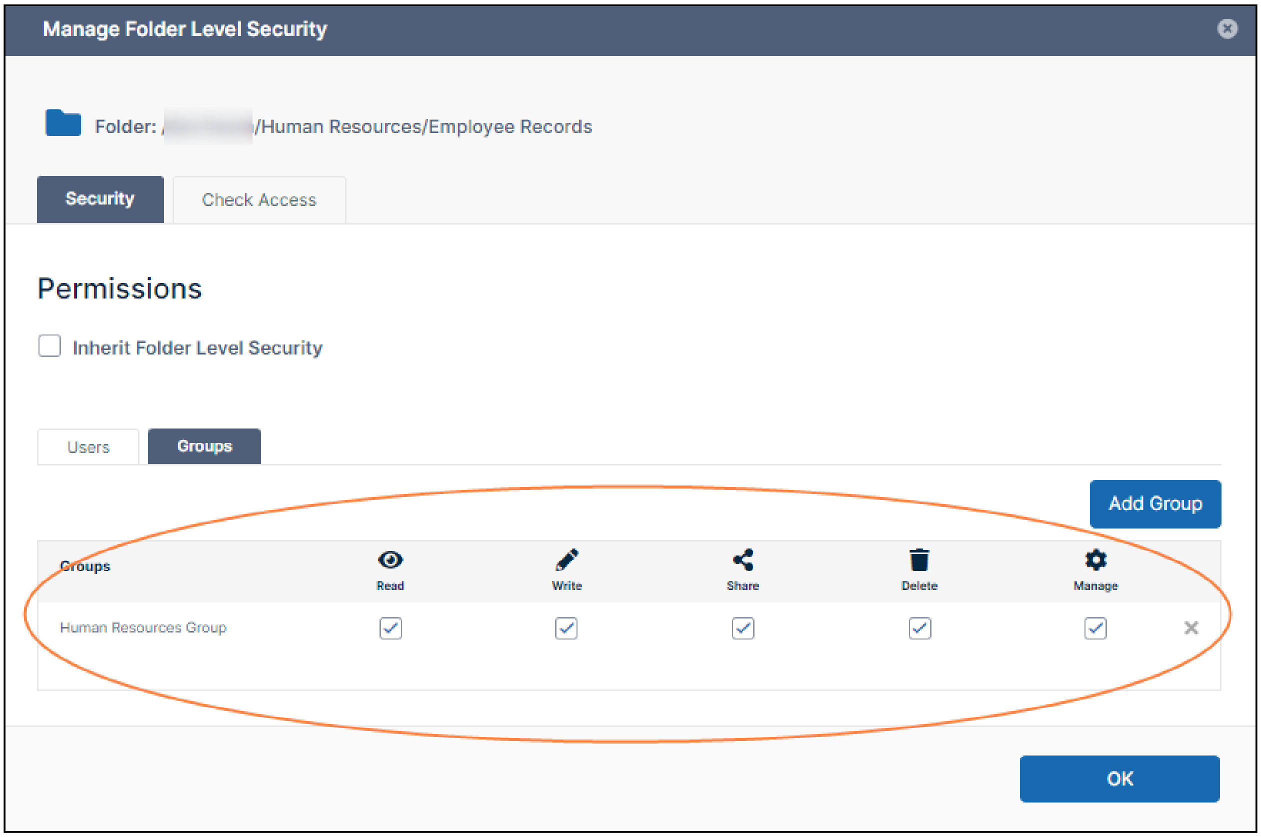
Human Resources

3 items

Name	Modified	Size
Employee Records		
Forms	03-11-2022 10:02 AM by dev1team	
HR Files	03-11-2022 10:02 AM by dev1team	

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.



Folder: /[redacted]/Human Resources/Employee Records

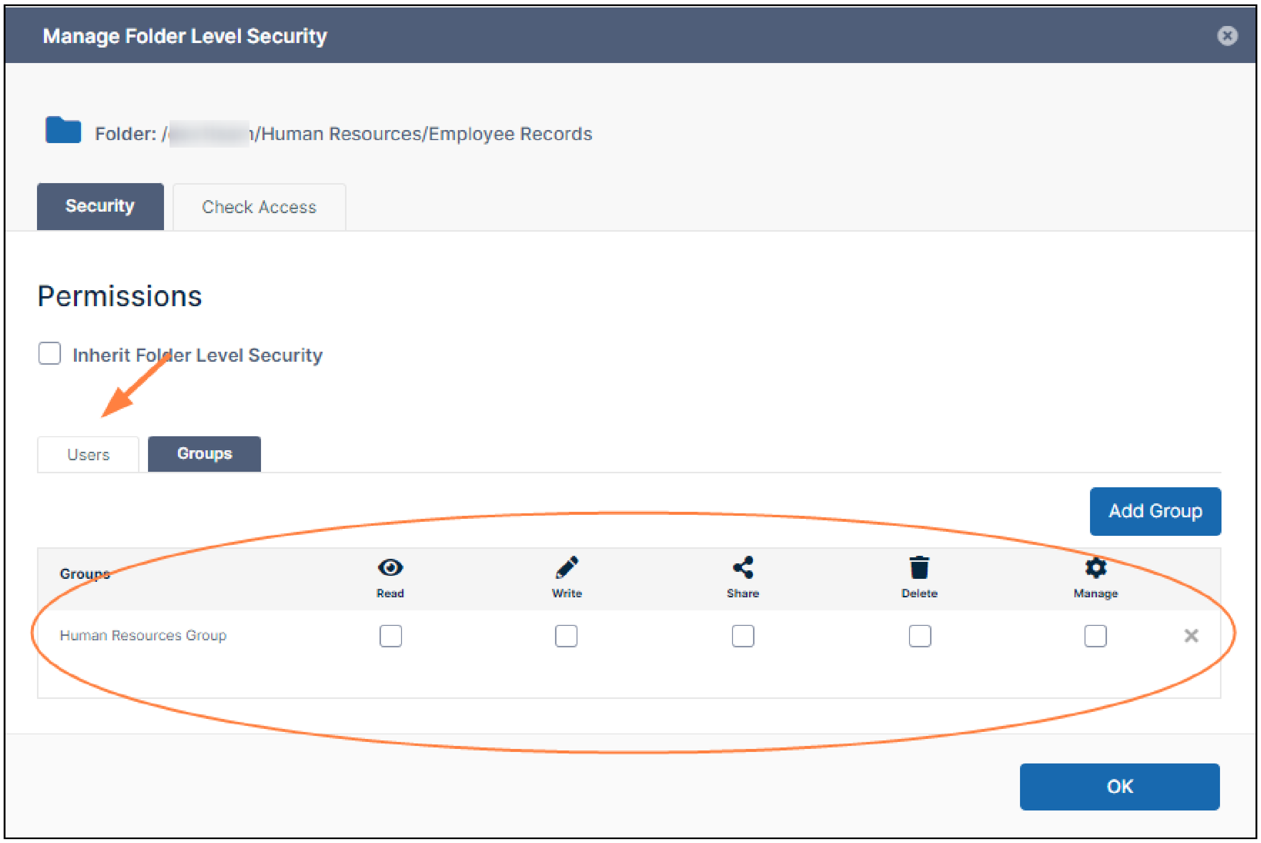
Permissions

☐ Inherit Folder Level Security

Groups	Read	Write	Share	Delete	Manage	
Human Resources Group	☑	☑	☑	☑	☑	×

5. 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

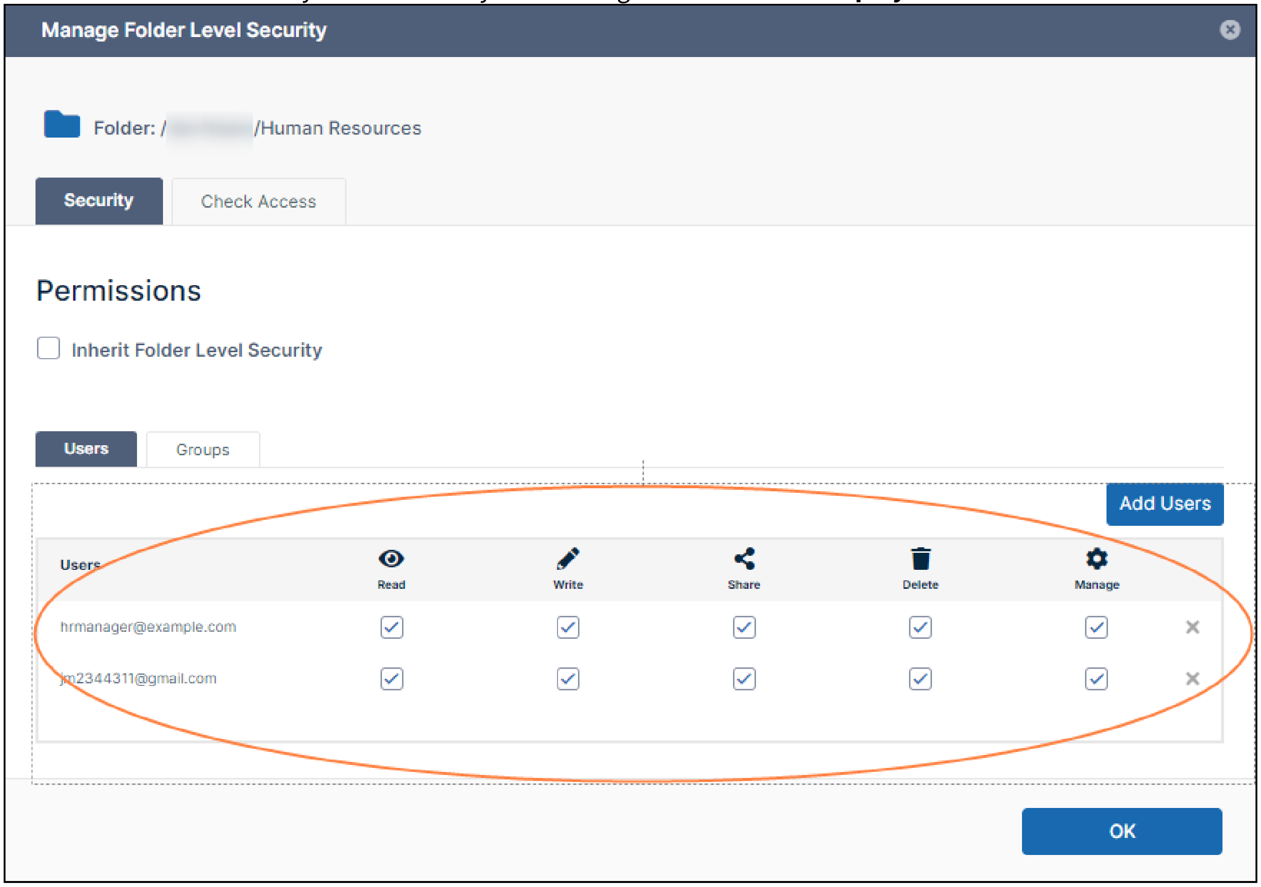
Folder: /[redacted]/Human Resources/Employee Records

Permissions

□ Inherit Folder Level Security

Groups	Read	Write	Share	Delete	Manage	
Human Resources Group	□	□	□	□	□	×

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



Manage Folder Level Security

Folder: /[redacted]/Human Resources

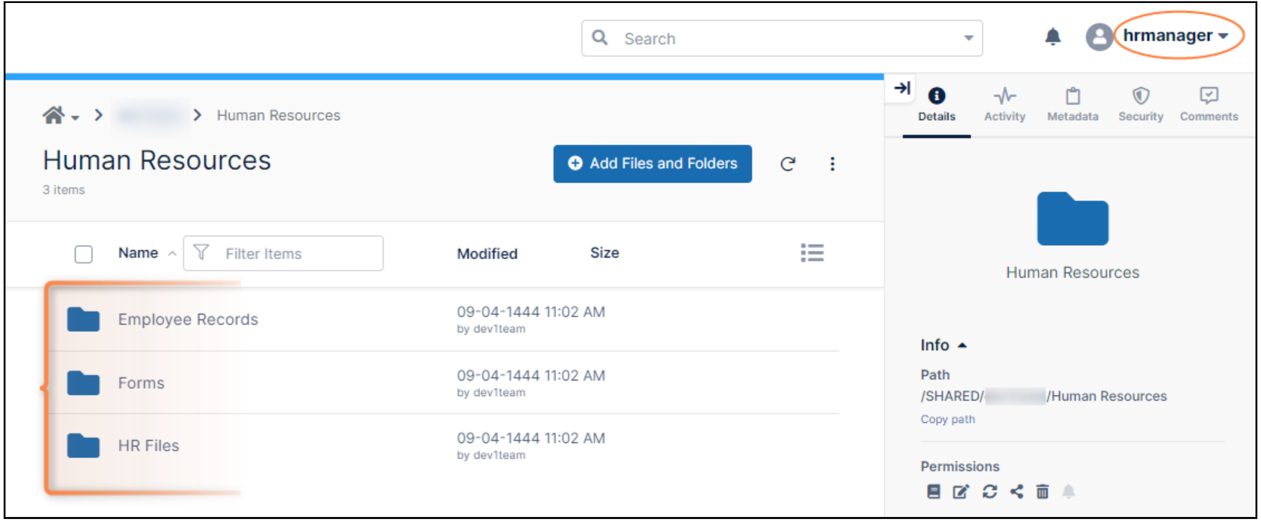
Permissions

□ Inherit Folder Level Security

Users	Read	Write	Share	Delete	Manage	
hrmanager@example.com	☑	☑	☑	☑	☑	×
jm2344311@gmail.com	☑	☑	☑	☑	☑	×

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**.



Human Resources

3 items

Name	Modified	Size
Employee Records	09-04-1444 11:02 AM by dev1team	
Forms	09-04-1444 11:02 AM by dev1team	
HR Files	09-04-1444 11:02 AM by dev1team	

Human Resources

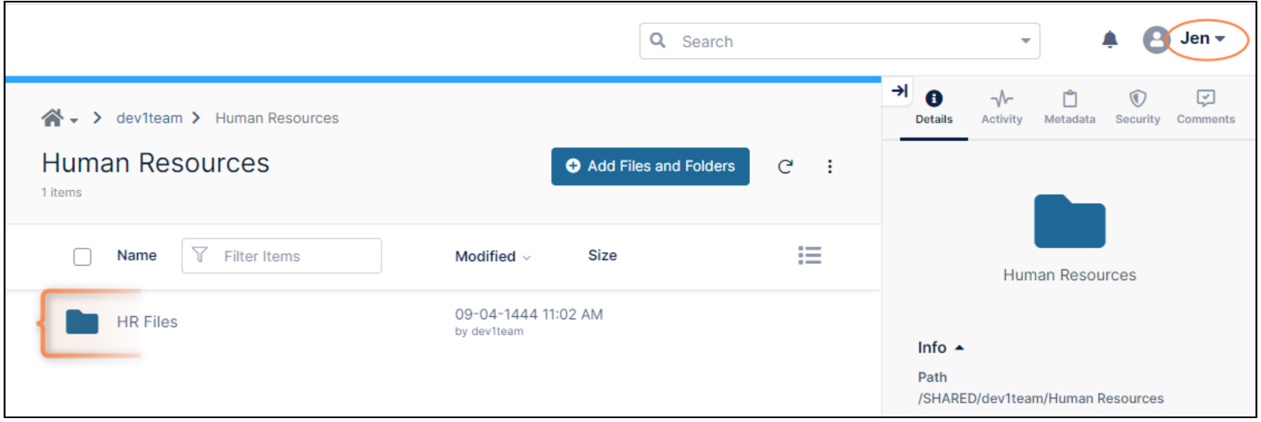
Info

Path

/SHARED/[redacted]/Human Resources

Permissions

When another member of the **Human Resources** group logs in, they see the **Human Resources** team folder, but only the **HR Files** sub-folder:



Human Resources

1 items

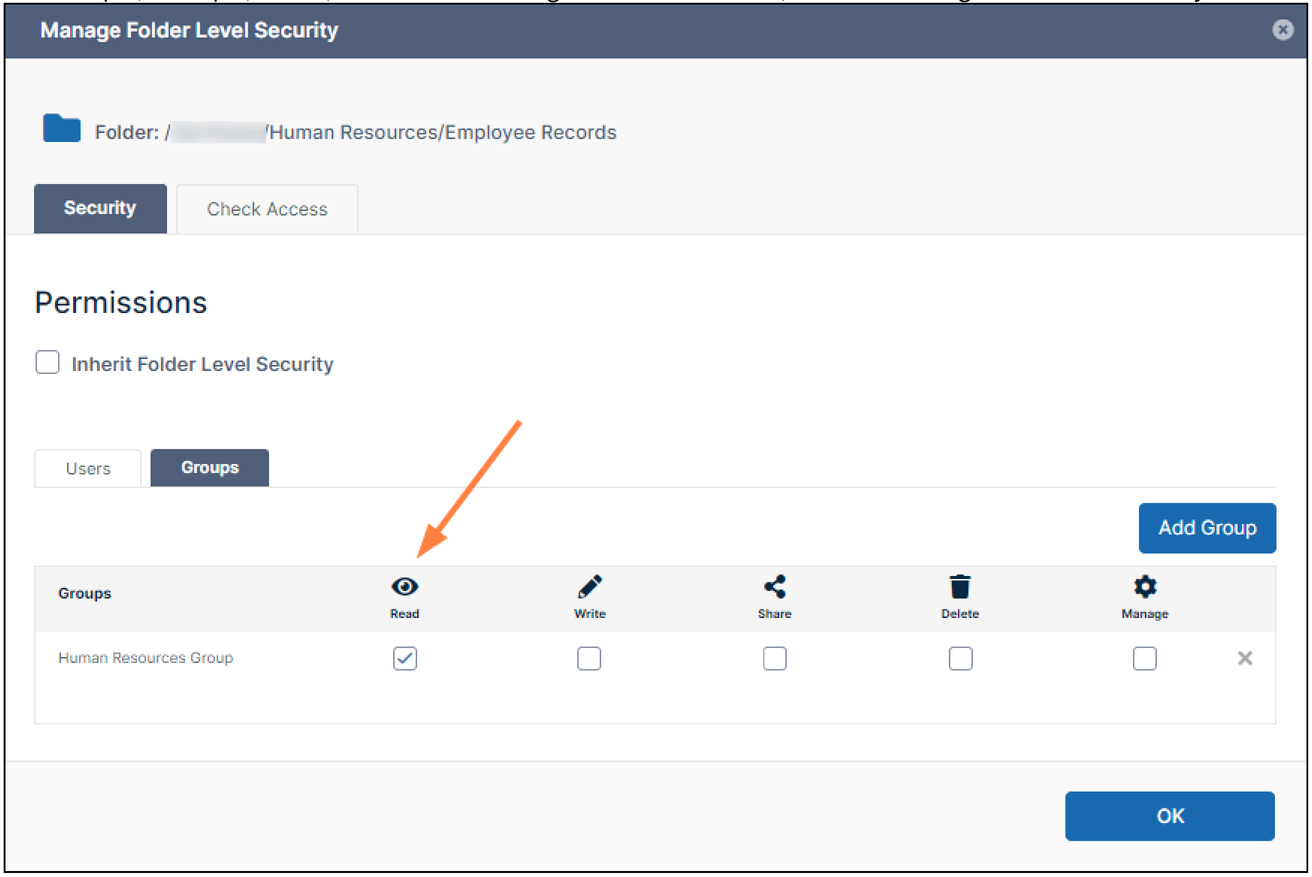
Name	Modified	Size
HR Files	09-04-1444 11:02 AM by dev1team	

Human Resources

Path
/SHARED/dev1team/Human Resources

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:



Manage Folder Level Security

Folder: /[redacted]/Human Resources/Employee Records

Permissions

□ Inherit Folder Level Security

Groups	Read	Write	Share	Delete	Manage	
Human Resources Group	☑	□	□	□	□	×

More Information:

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

Team Folders

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

Manage Team Folders	➡ Search for a Team Folder ➡ Recover Deleted Files ➡ View and Restore Previous Versions ➡ Promoting Existing User Account to Team Folders

Configure the Team Folders Account

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

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

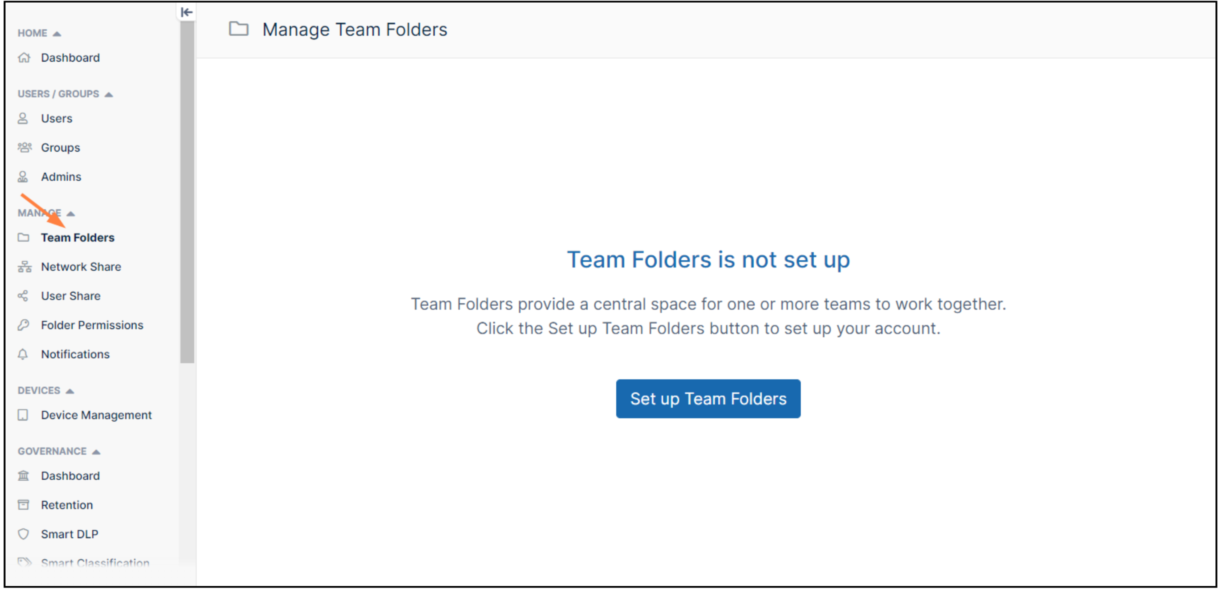
- FileCloud can create the account for you - you just need to choose the name you want to use.
- The Team Folder account is not counted towards your user license.
- FileCloud can also create an email account where it will send Team Folder notifications.
- The email address for Team Folder notifications 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.

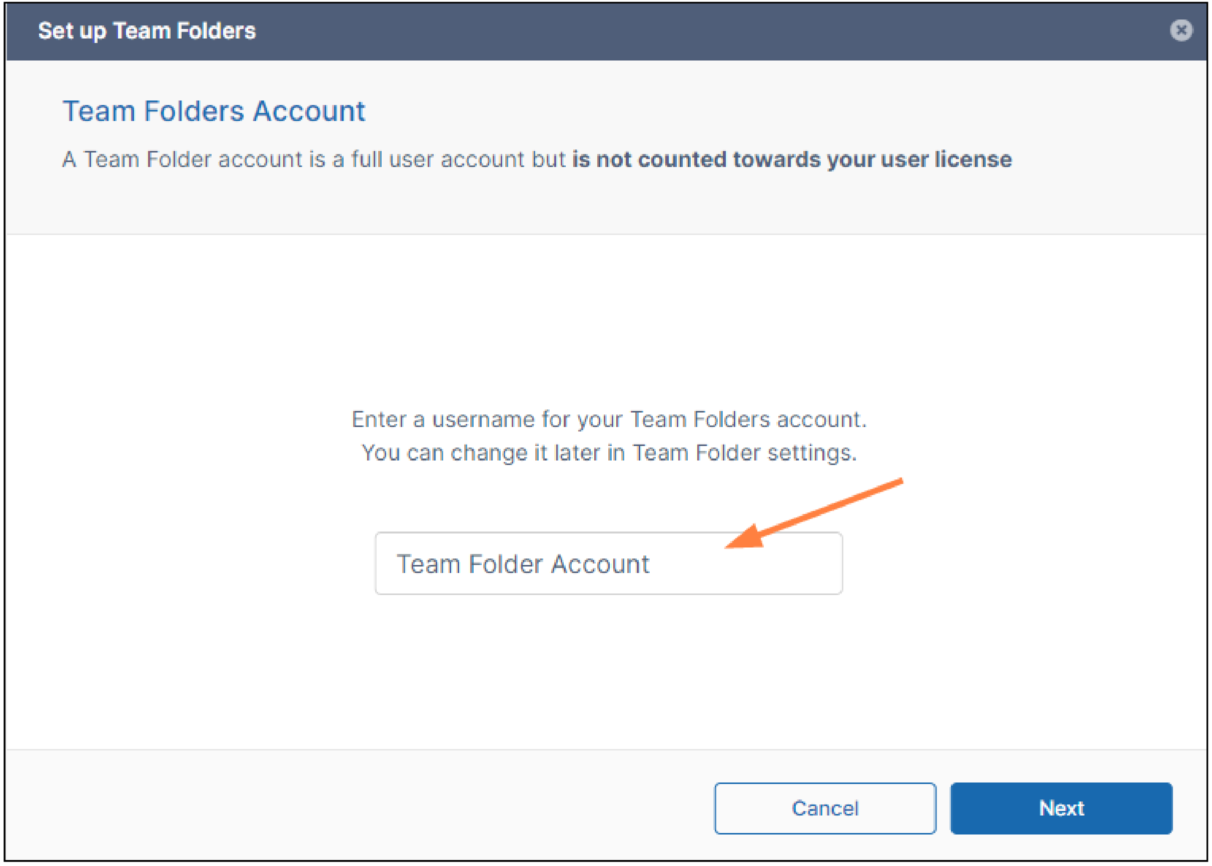


Team Folders is not set up

Team Folders provide a central space for one or more teams to work together.
Click the Set up Team Folders button to set up your account.

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**).



Team Folders Account

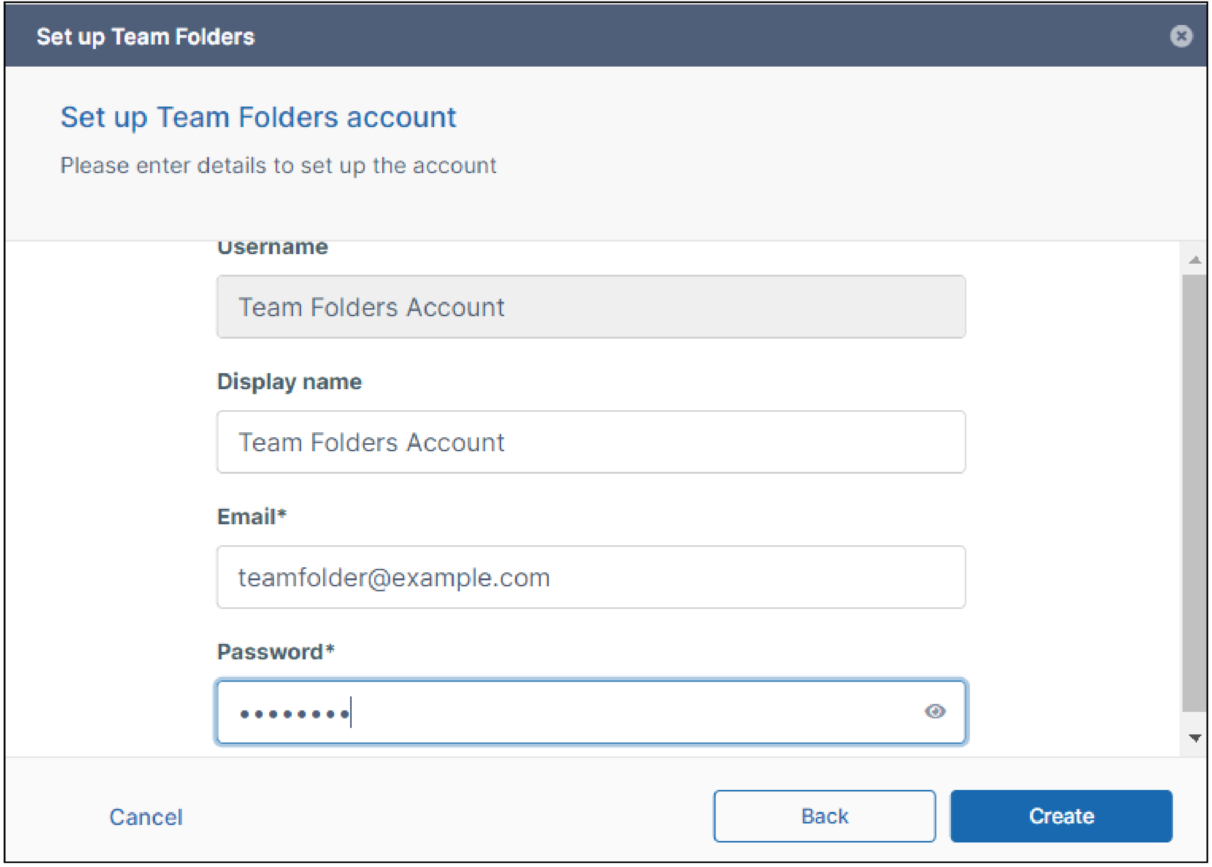
A Team Folder account is a full user account but **is not counted towards your user license**

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

Team Folder Account

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

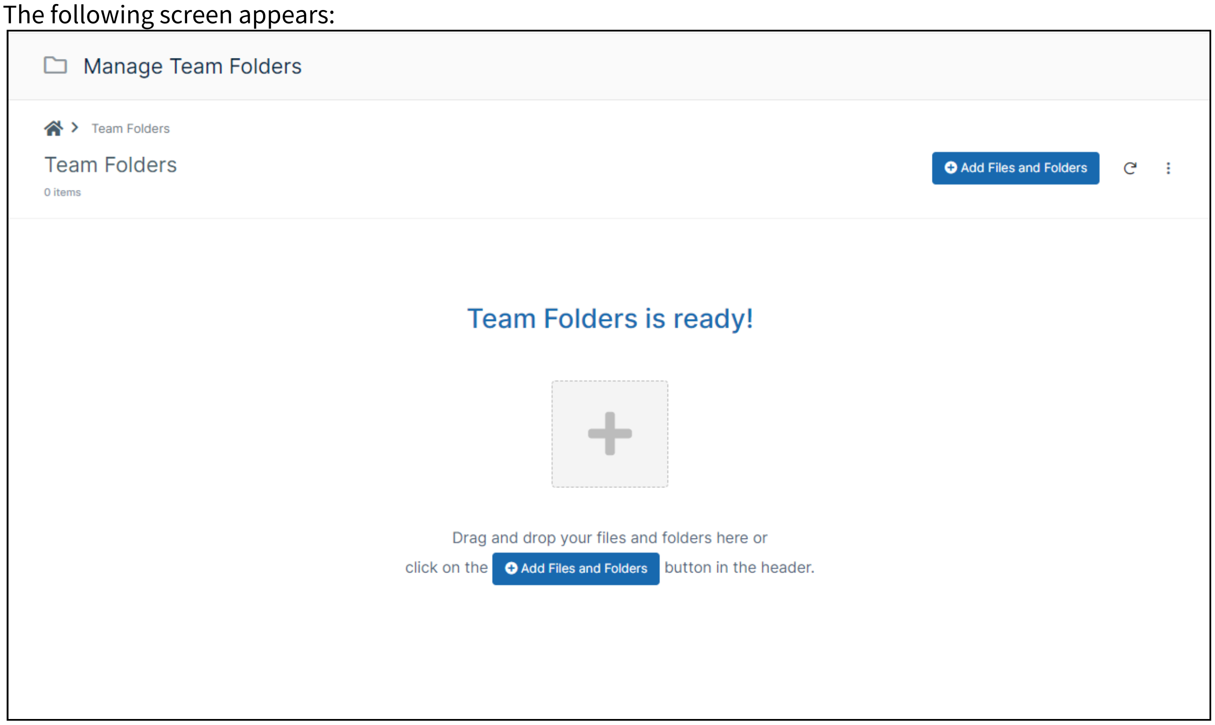
Username: Team Folders Account

Display name: Team Folders Account

Email*: teamfolder@example.com

Password*: ••••••••

The following screen appears:



Manage Team Folders

Team Folders

0 items

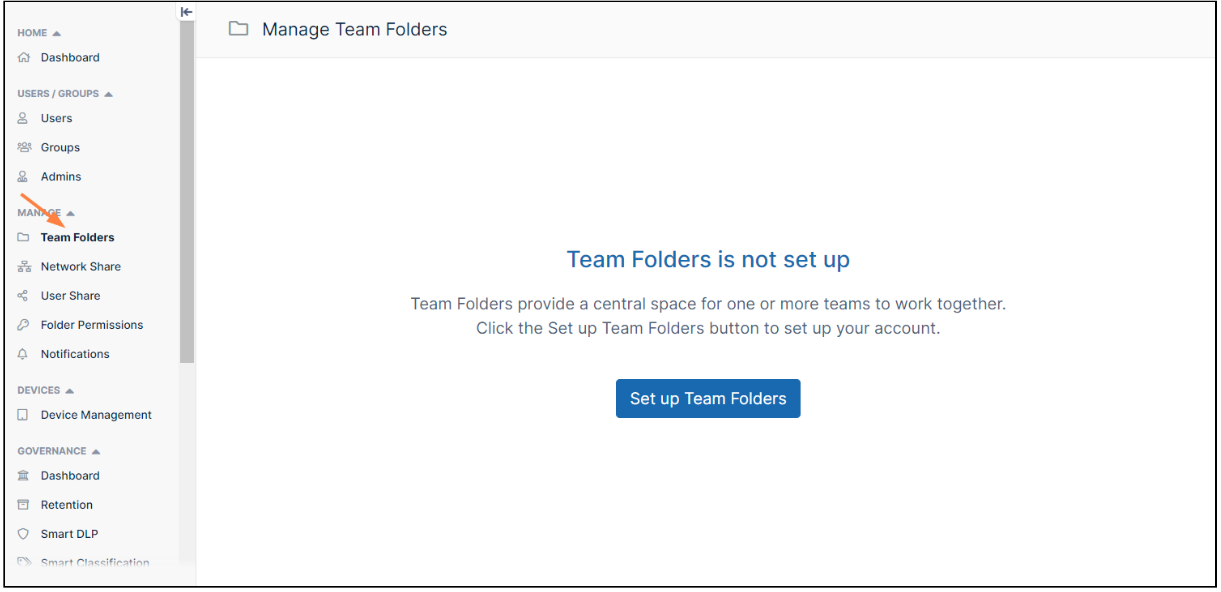
Team Folders is ready!

Drag and drop your files and folders here or click on the Add Files and Folders button in the header.

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

Convert an existing user account into the Team Folders account

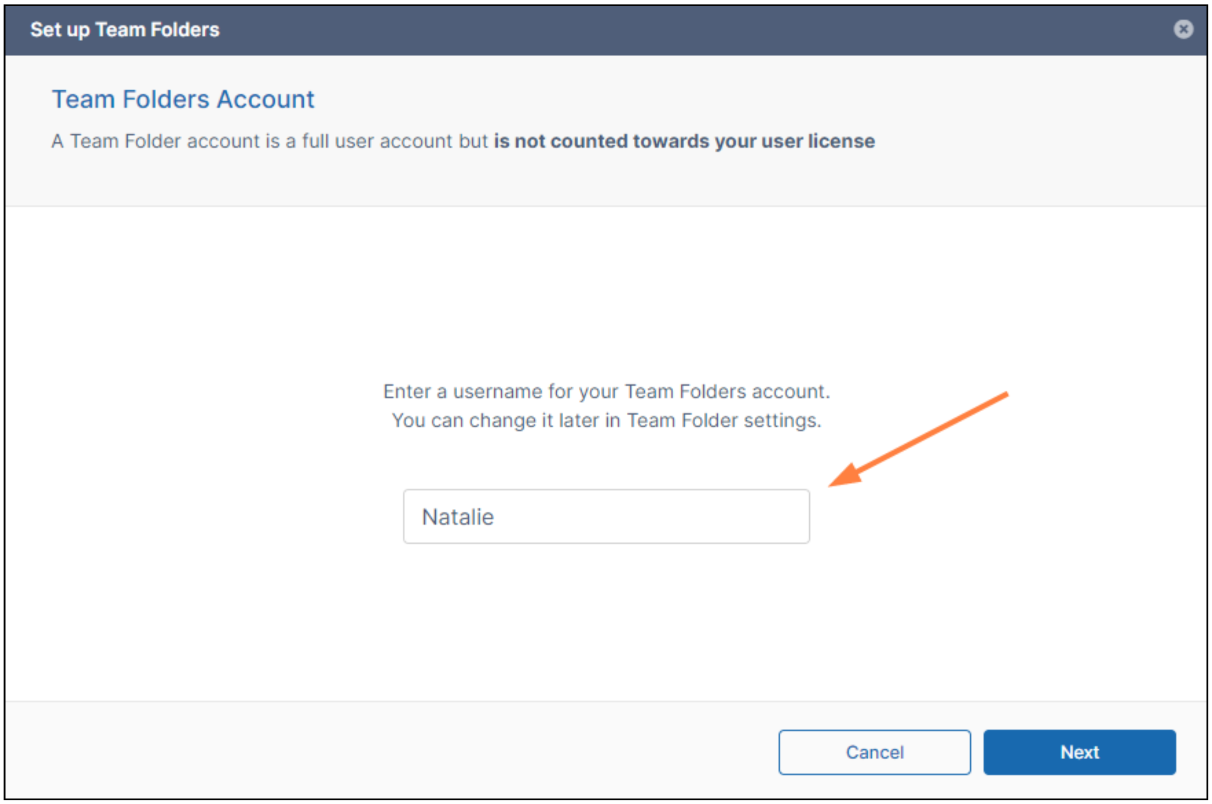
1. In the admin portal's navigation pane, click **Team Folders**.
   The screen tells you Team Folders is not set up, and it provides you with a **Set up Team Folders** button.



Team Folders is not set up

Team Folders provide a central space for one or more teams to work together.
Click the Set up Team Folders button to set up your account.

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



Set up Team Folders

Team Folders Account

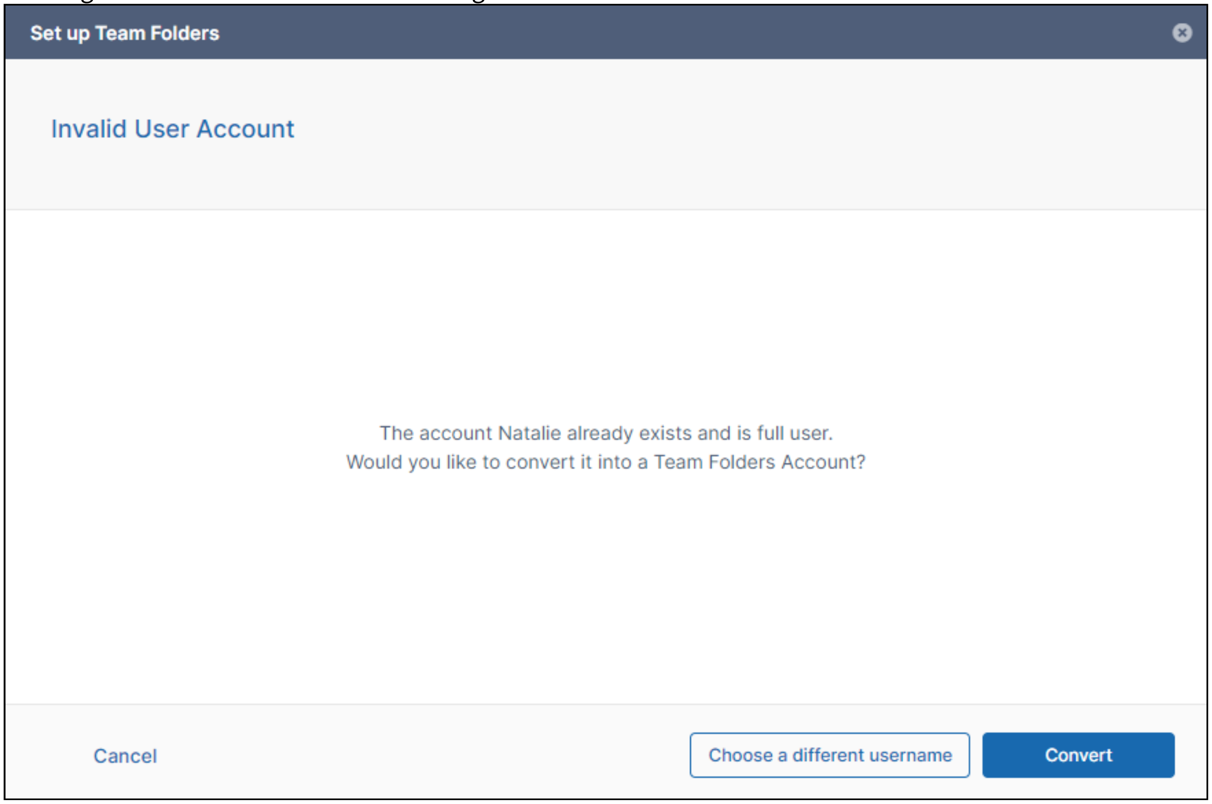
A Team Folder account is a full user account but **is not counted towards your user license**

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

Natalie

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:

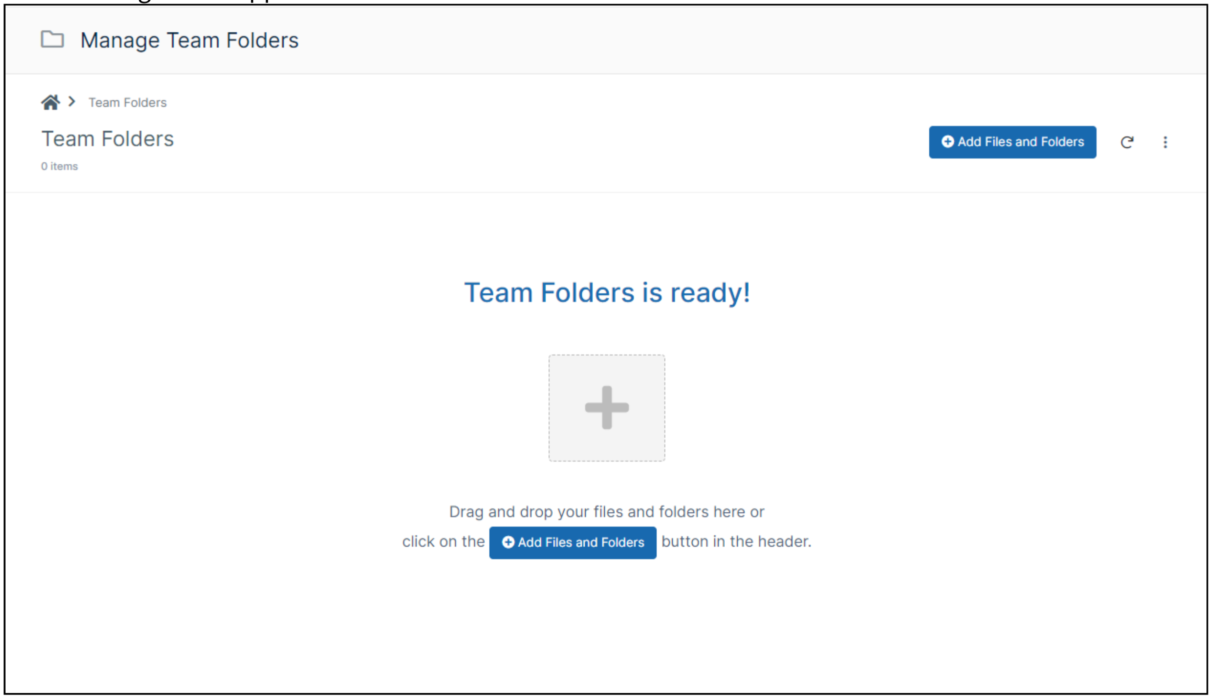


Set up Team Folders

Invalid User Account

The account Natalie already exists and is full user.
Would you like to convert it into a Team Folders Account?

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



Manage Team Folders

Team Folders

Team Folders

0 items

Team Folders is ready!

Drag and drop your files and folders here or click on the Add Files and Folders button in the header.

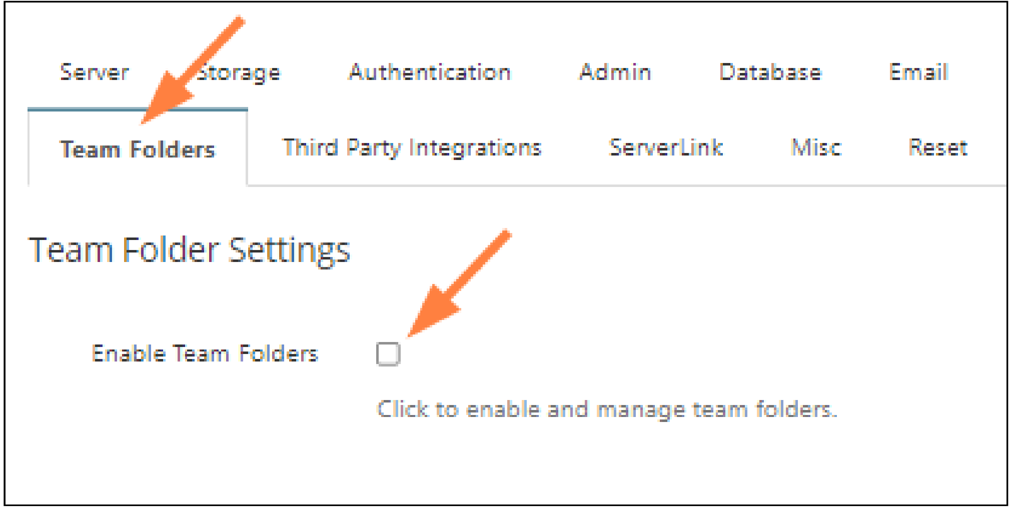
Now you are ready to create your Team Folders and fill them with contents. You can begin by dragging and dropping folders onto the page or clicking **Add Files and Folders**. These are good options if you do not already have a folder structure set up that you want to bring into FileCloud as your Team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

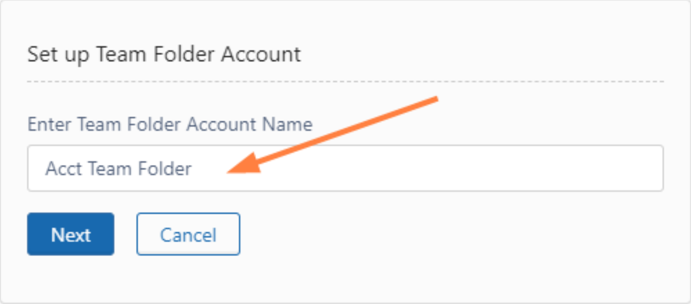


Team Folder Settings

Enable Team Folders □

Click to enable and manage team folders.

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.



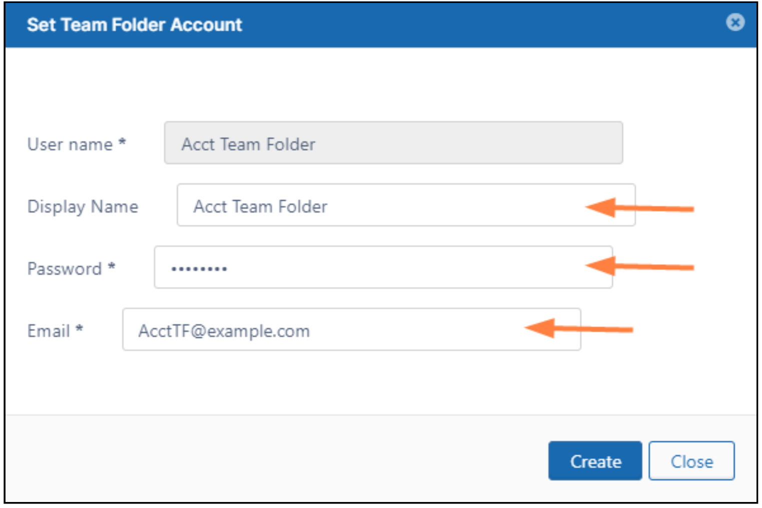
Set up Team Folder Account

Enter Team Folder Account Name

Acct Team Folder

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 * Acct Team Folder

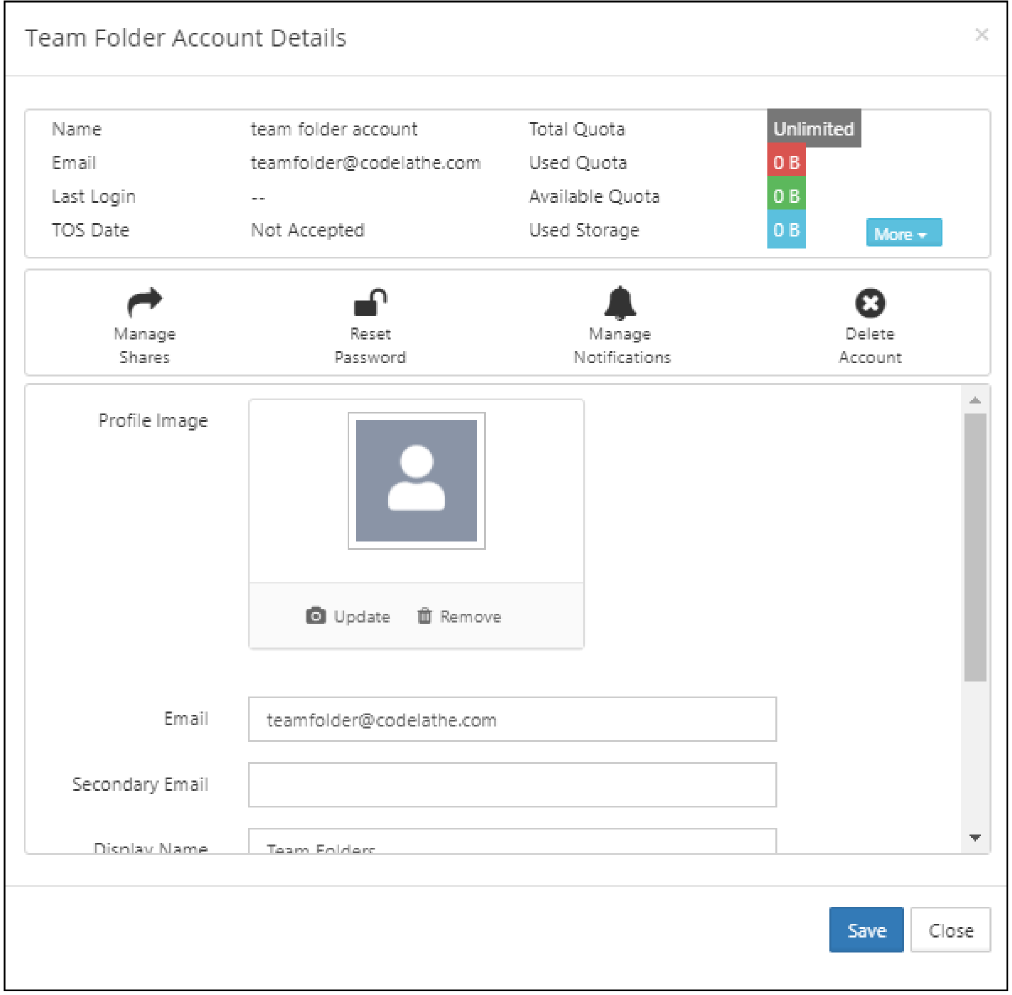
Display Name Acct Team Folder

Password * ••••••••

Email * AcctTF@example.com

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

Email teamfolder@codelathe.com

Secondary Email

Display Name Team Folders

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: • 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.

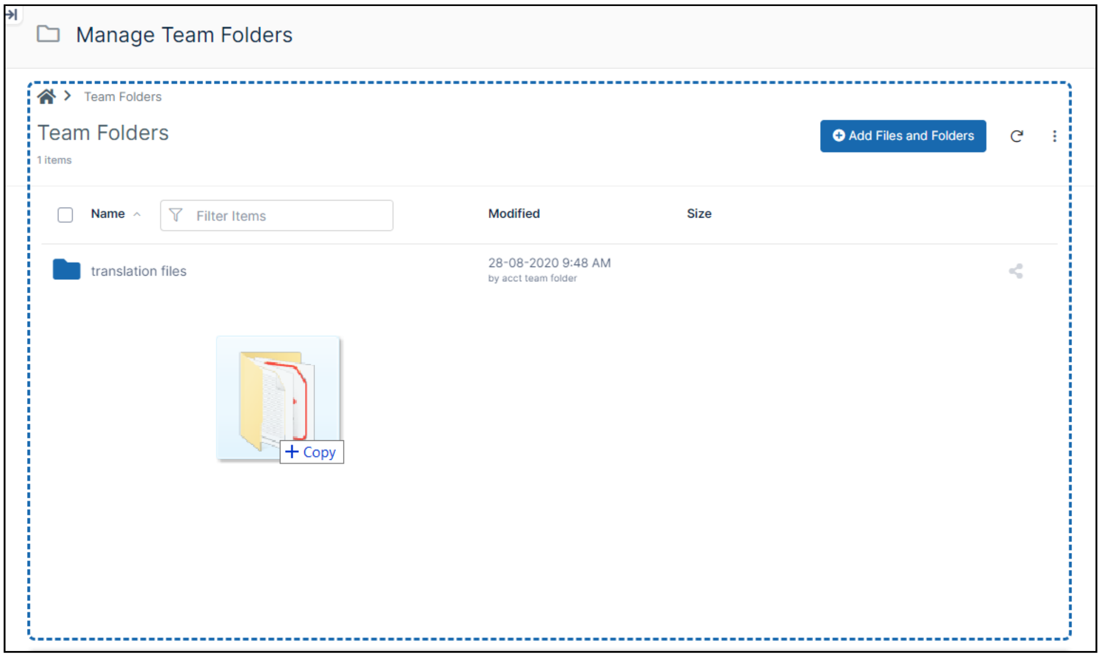
Now, log in to the admin interface and go to Team Folders to share them with users and groups and set up permissions.

Admin Portal

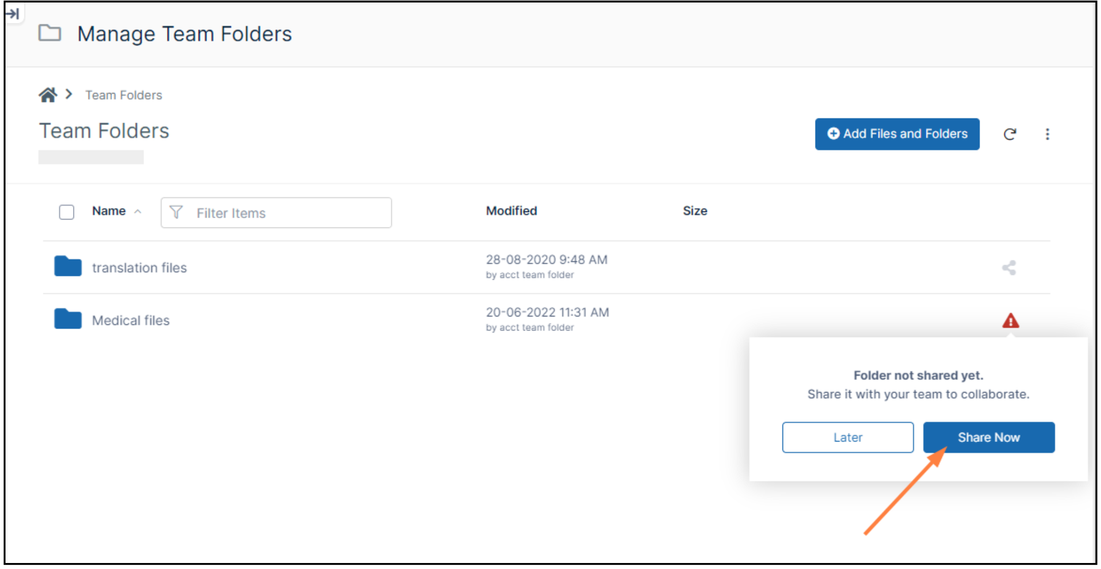
Go to the **Team Folders** page in the admin portal to create Team Folders and seed them with files.

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.

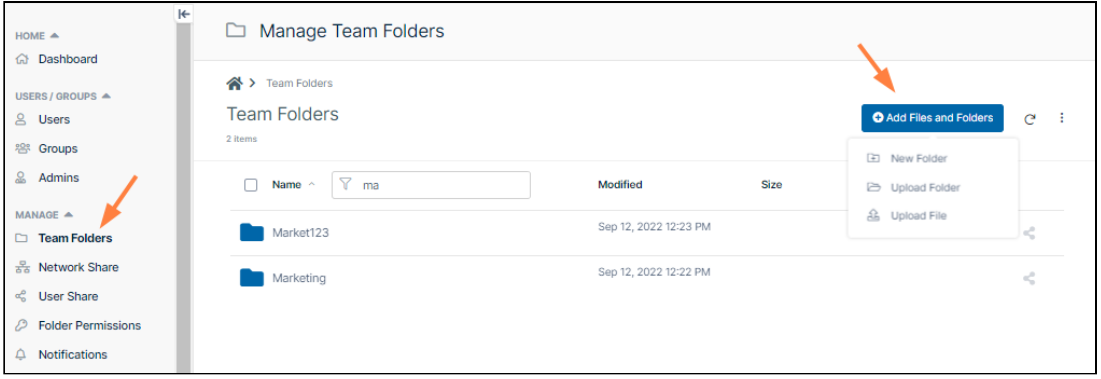


c. Click **Share Now** to share the Team Folder with users and/or groups.

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.

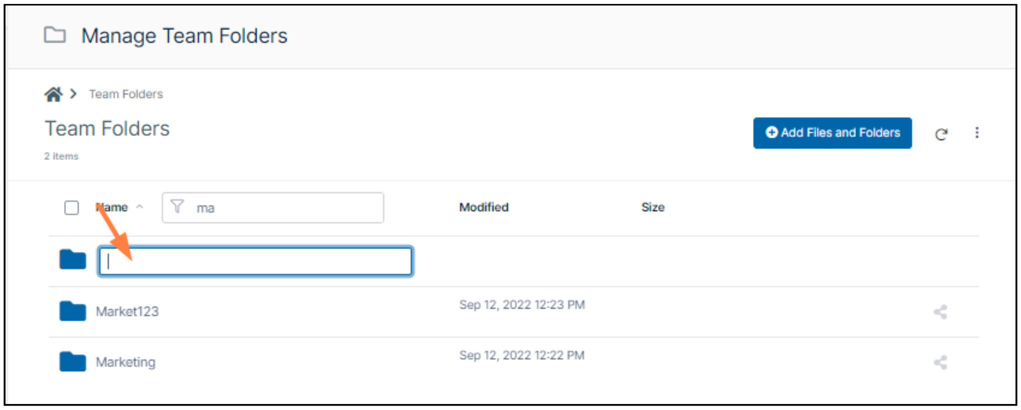
Add Team Folders by clicking the button

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

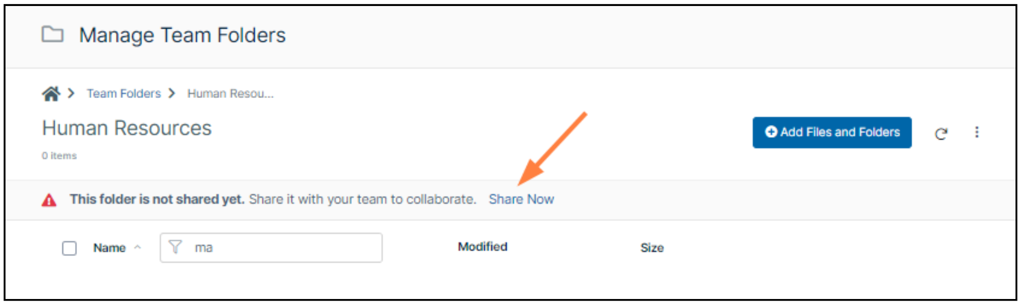


b. Either choose **New Folder** to create a new Team Folder, or click **Upload Folder** to upload an existing folder (with or without contents) and make it a Team Folder.
If you choose **New Folder:**

- 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**.

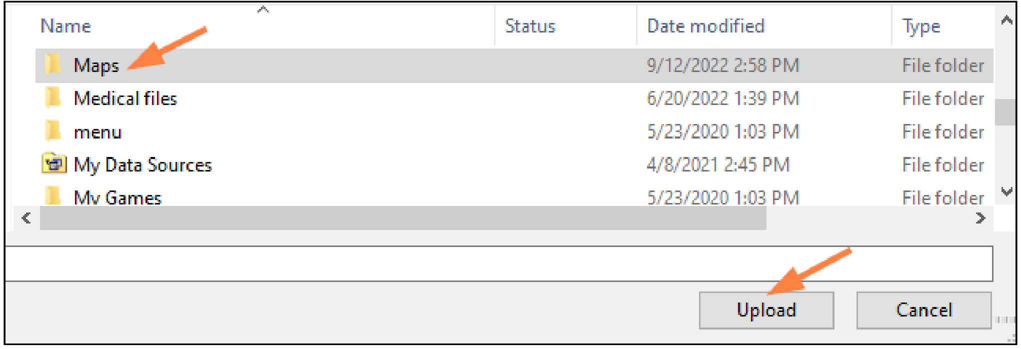


A share dialog box opens.

- 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.

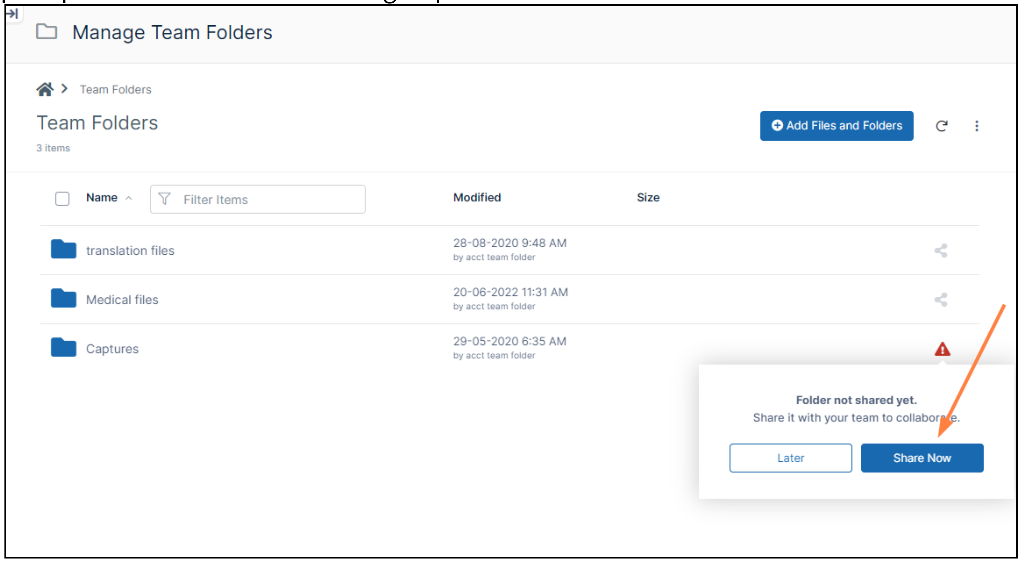
If you choose **Upload Folder**, your file explorer opens.

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



Name	Status	Date modified	Type
Maps		9/12/2022 2:58 PM	File folder
Medical files		6/20/2022 1:39 PM	File folder
menu		5/23/2020 1:03 PM	File folder
My Data Sources		4/8/2021 2:45 PM	File folder
My Games		5/23/2020 1:03 PM	File folder

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



Manage Team Folders

Team Folders

Team Folders

3 items

Name	Modified	Size
translation files	28-08-2020 9:48 AM by acct team folder	
Medical files	20-06-2022 11:31 AM by acct team folder	
Captures	29-05-2020 6:35 AM by acct team folder	

Folder not shared yet.

Share it with your team to collabor e.

- 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 change the default, see To enable public sharing of top-level Team Folders, below.

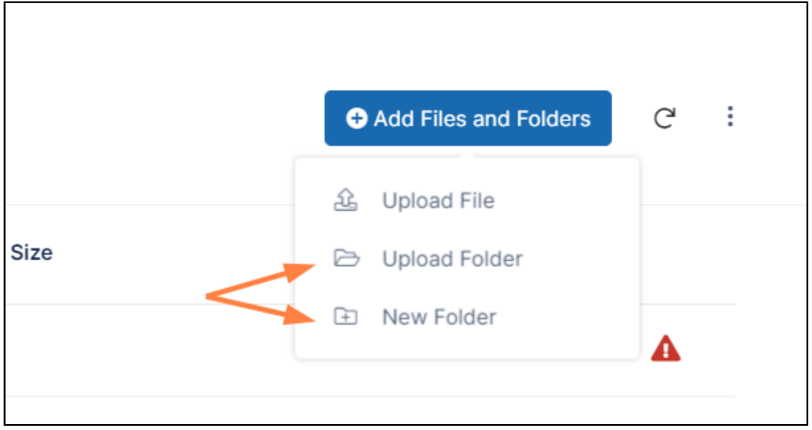
You must share Team Folders before users can access them.

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

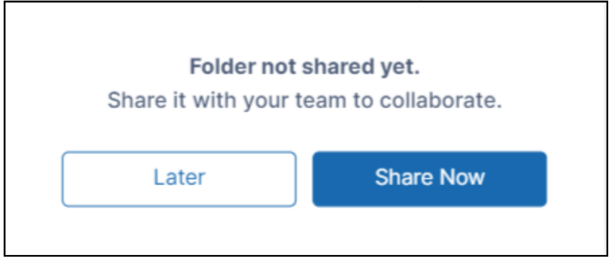
After setting up Team Folders, you can add and share them.

To share a new Team Folder when adding it:

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

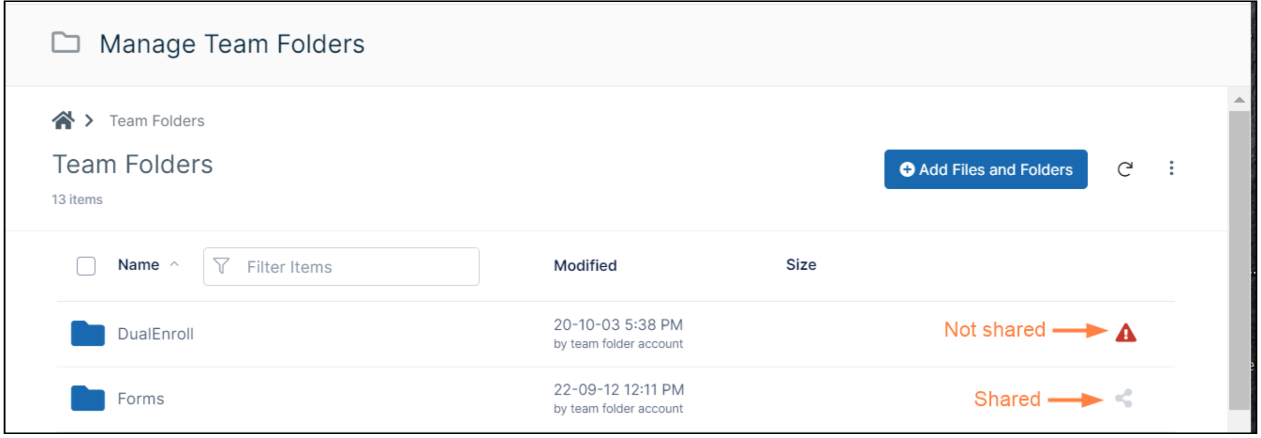


When the folder is added the following prompt appears:



Folder not shared yet.
Share it with your team to collaborate.

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.



Manage Team Folders

Team Folders > Team Folders

Team Folders
13 items

□	Name	Modified	Size	
	DualEnroll	20-10-03 5:38 PM by team folder account		Not shared
	Forms	22-09-12 12:11 PM by team folder account		Shared

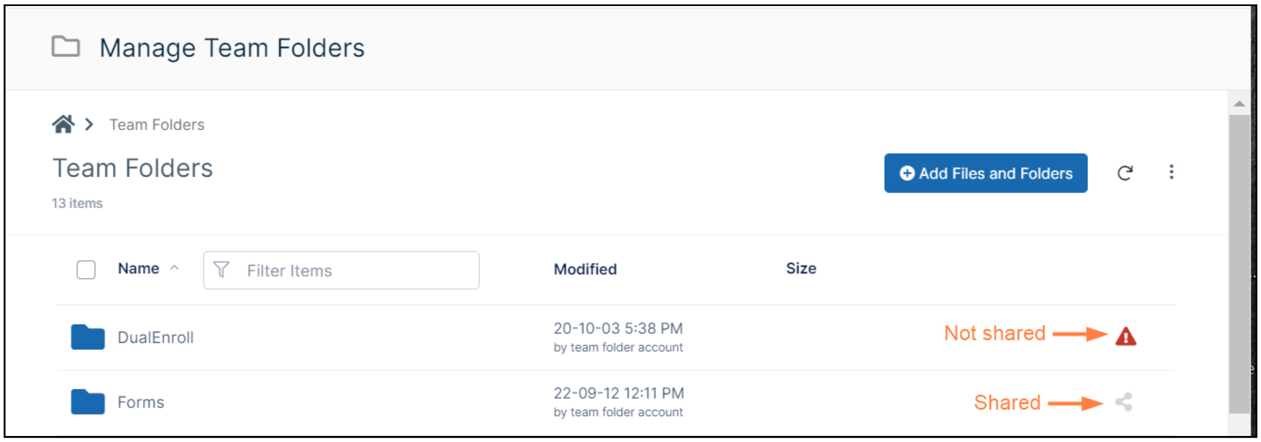
If you choose **Share Now** a **Share link for folder** dialog box opens.

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

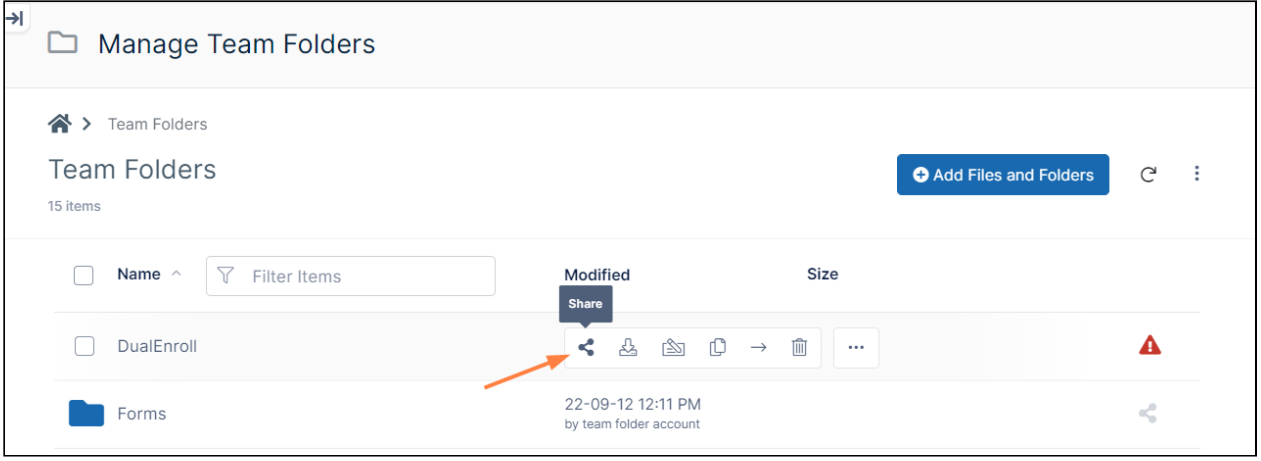
To share an existing Team Folder:

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

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



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

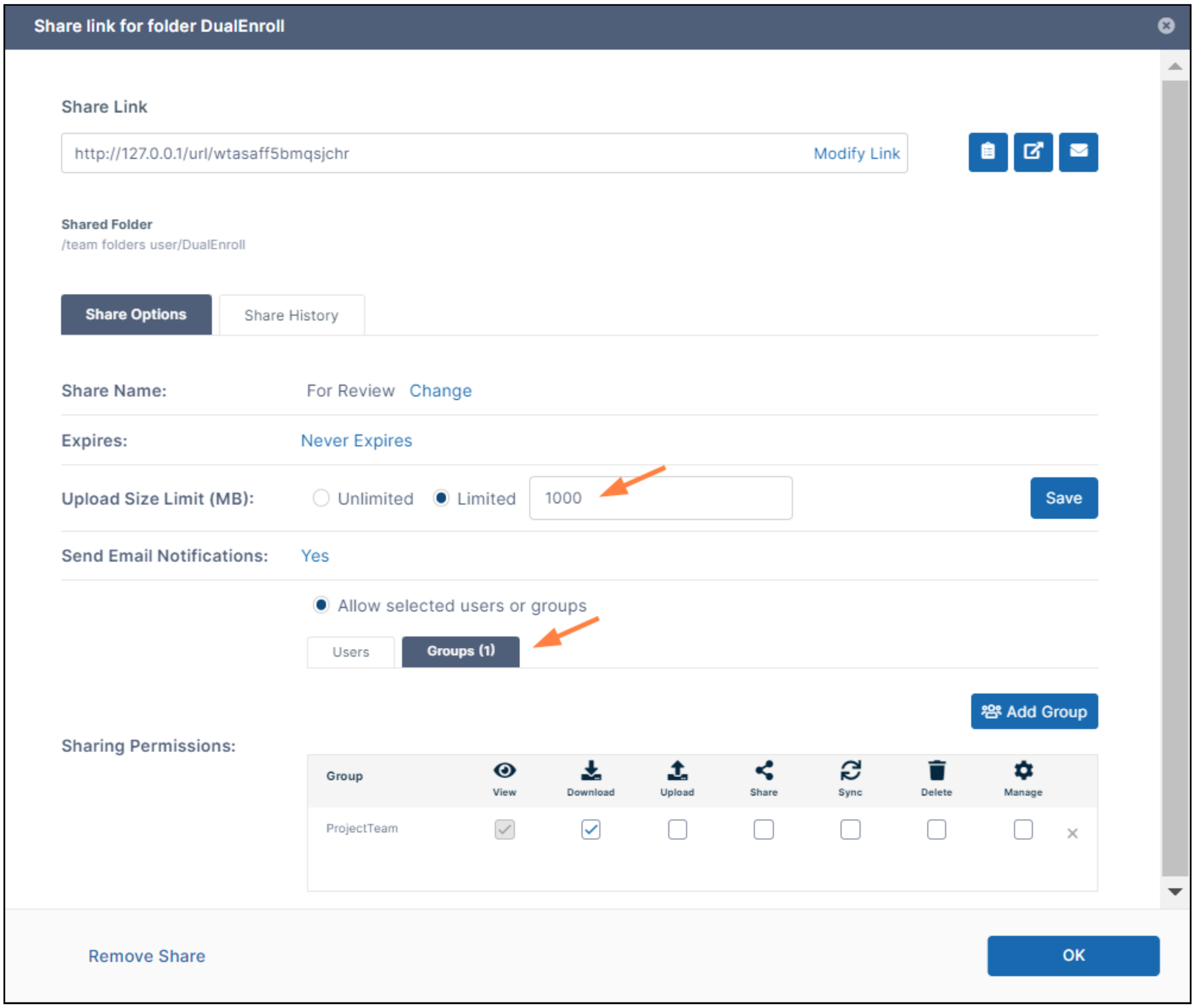


The **Share link for folder** dialog box opens.

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

To complete the Team Folder share:

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



Share link for folder DualEnroll

Share Link

http://127.0.0.1/url/wtasaff5bmqsjchr 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 1000 Save

Send Email Notifications: Yes

● Allow selected users or groups

Users | Groups (1)

Add Group

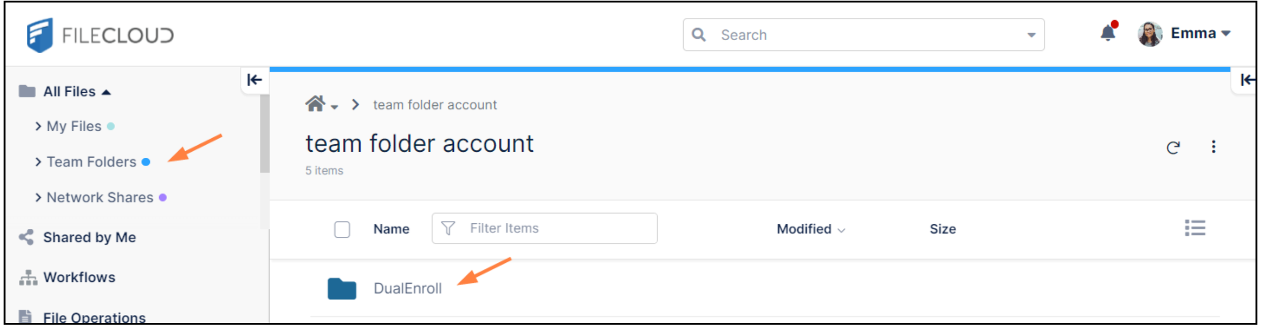
Sharing Permissions:

Group	View	Download	Upload	Share	Sync	Delete	Manage	
ProjectTeam	☑	☑	□	□	□	□	□	×

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.



team folder account
5 items

DualEnroll

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:

Sorry, the video is not supported in this export.
But you can reach it using the following URL:

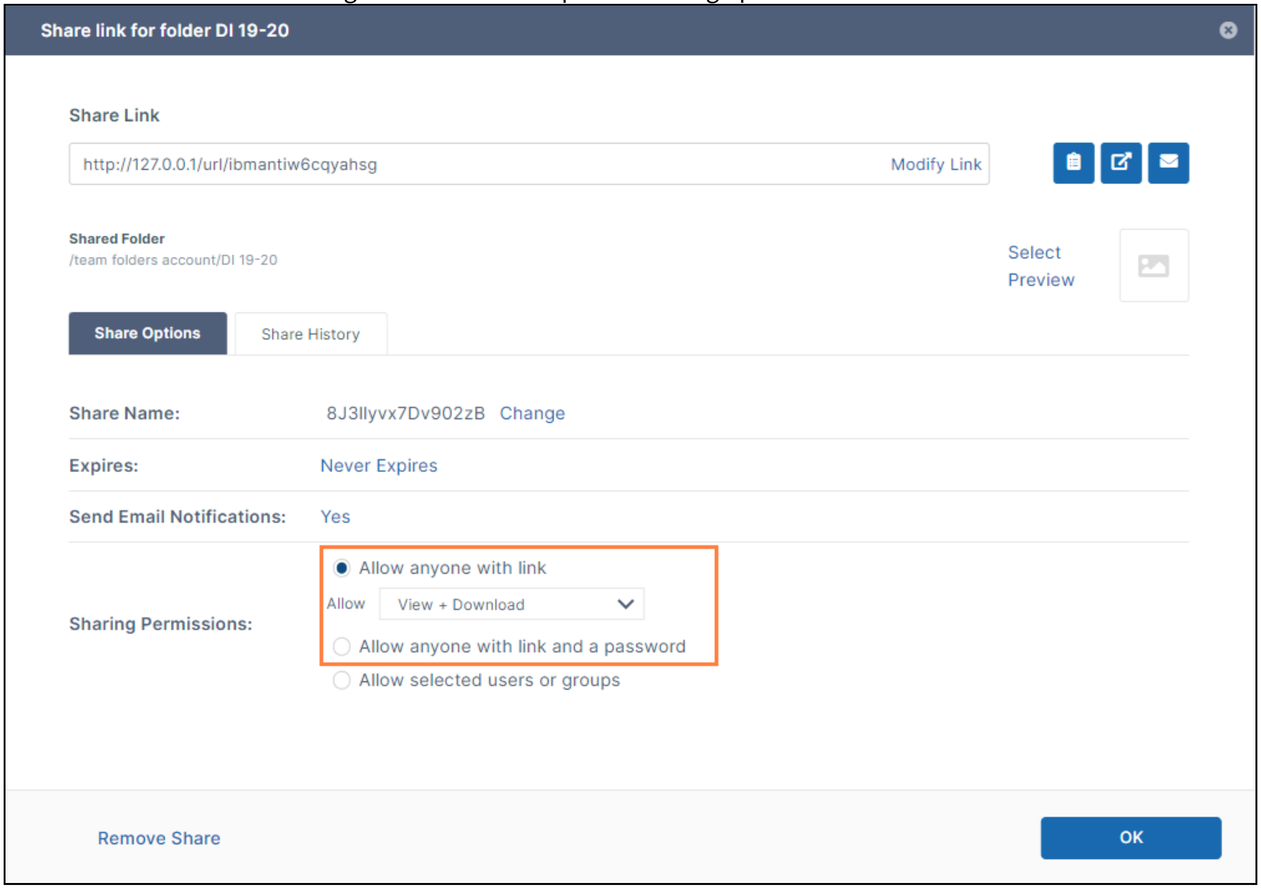
Movie URL not available.

To enable public sharing of top-level Team Folders

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

```
define('TONIDOCLOUD_ALLOW_PUBLIC_SHARE_TOP_LEVEL_TEAM_FOLDER', true);
```

The **Share link for folder** dialog box now includes public sharing options:



Share link for folder DI 19-20

Share Link

http://127.0.0.1/url/ibmantiw6cqyahsg Modify Link

Shared Folder
/team folders account/DI 19-20

Select
Preview

Share Options | Share History

Share Name: 8J3llyvx7Dv902zB Change

Expires: Never Expires

Send Email Notifications: Yes

Sharing Permissions:
● Allow anyone with link
Allow View + Download
○ Allow anyone with link and a password
○ Allow selected users or groups

Remove Share

OK

To return to disabling public sharing of top-level Team Folders:

- Change the value of the cloudconfig.php setting from **true** to **false**:

```
define('TONIDOCLOUD_ALLOW_PUBLIC_SHARE_TOP_LEVEL_TEAM_FOLDER', false);
```

Search for a Team Folder

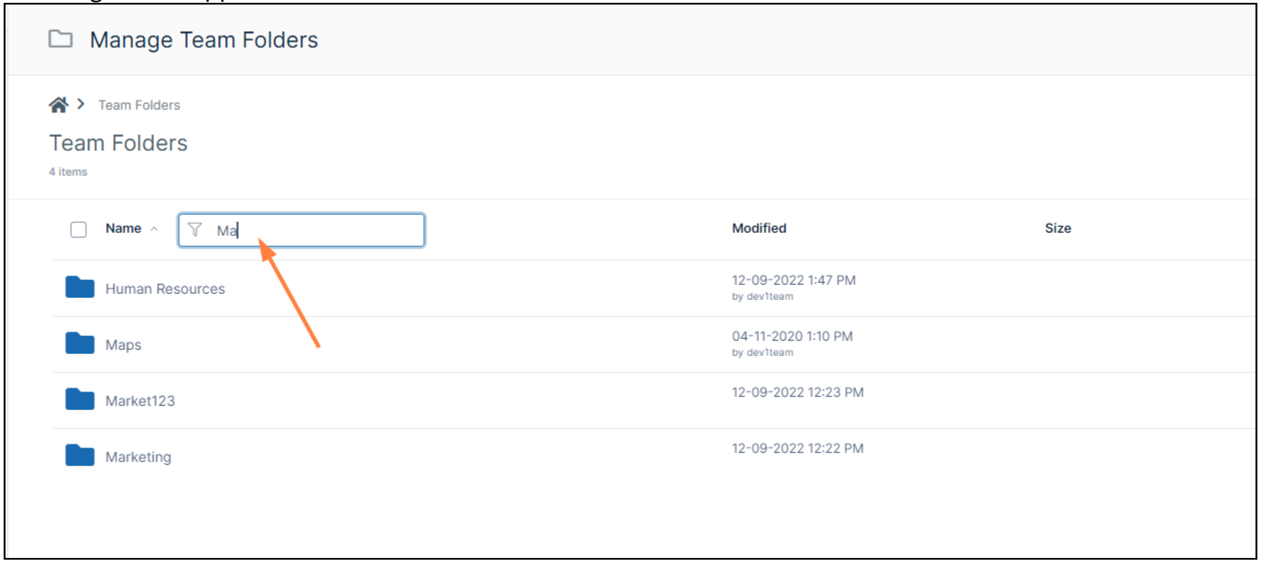
ⓘ The ability to search for a specific Team Folder is available in FileCloud Server version 19.1 and later.

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.



Name	Modified	Size
Human Resources	12-09-2022 1:47 PM by dev1team	
Maps	04-11-2020 1:10 PM by dev1team	
Market123	12-09-2022 12:23 PM	
Marketing	12-09-2022 12:22 PM	

Recover Deleted Files

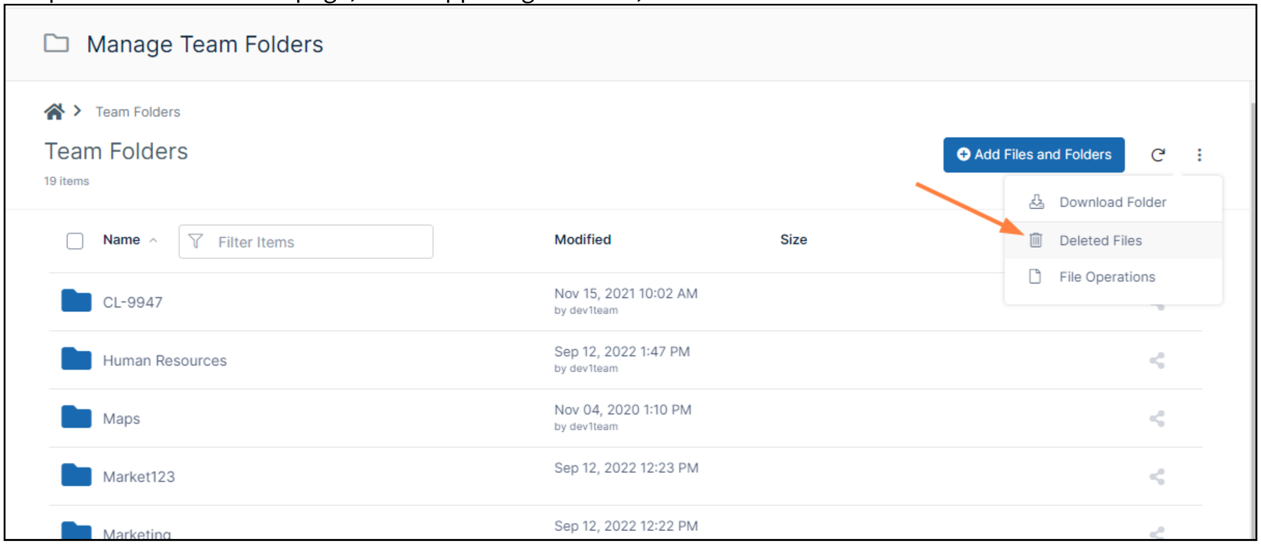
> The **Restore** button for deleted files and folders in Team Folders is available in FileCloud version 22.1 and later.
> The ability to recover deleted files and folders in a Team Folder is available in FileCloud version 17.3 and later.

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:

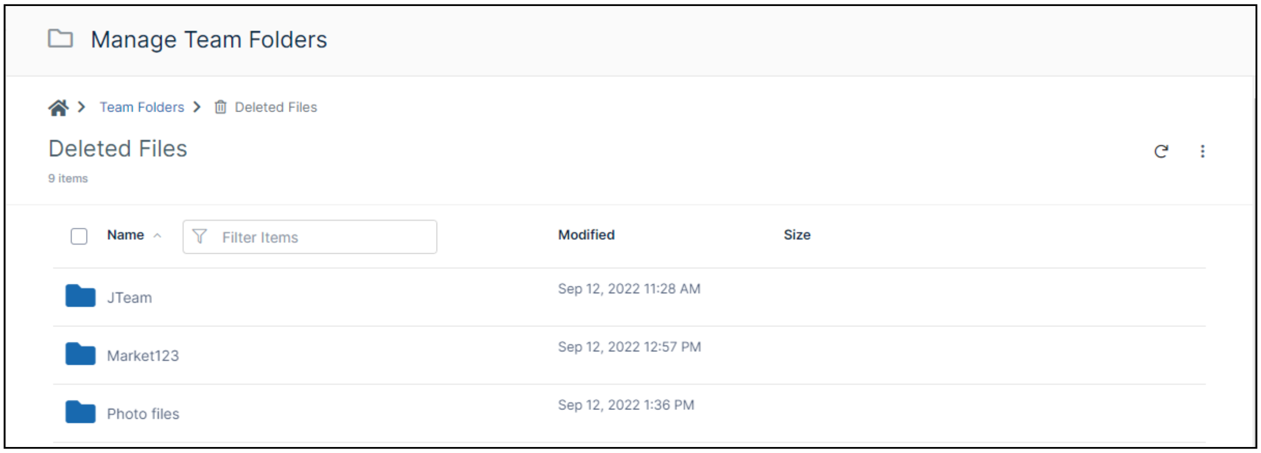
1. Open a browser and log in to the admin portal.
2. In the navigation panel, click **Team Folders**.

3. To open the **Deleted Files** page, in the upper-right corner, click the more icon and choose **Deleted Files**.



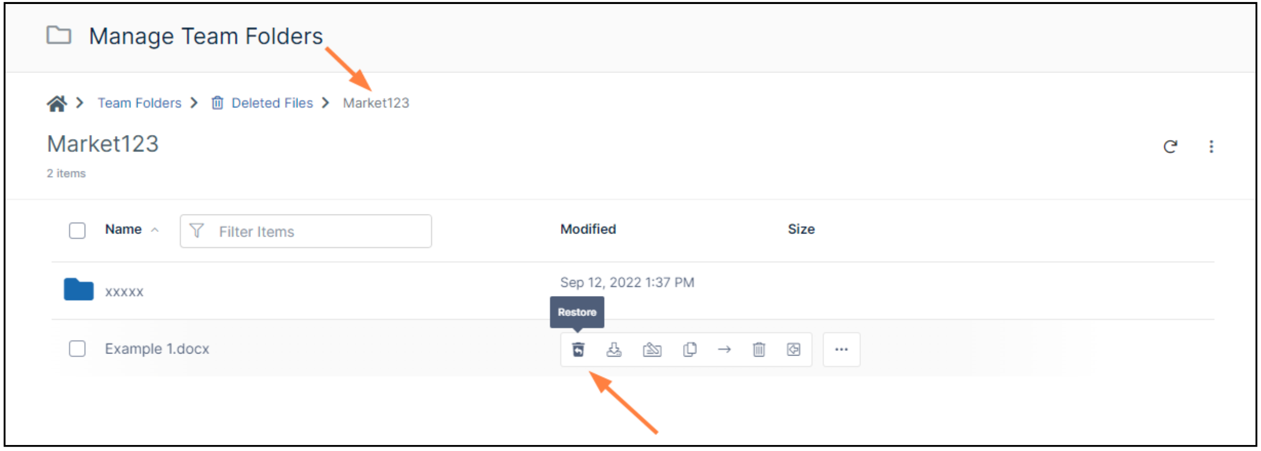
Name	Modified	Size
CL-9947	Nov 15, 2021 10:02 AM by dev1team	
Human Resources	Sep 12, 2022 1:47 PM by dev1team	
Maps	Nov 04, 2020 1:10 PM by dev1team	
Market123	Sep 12, 2022 12:23 PM	
Marketing	Sep 12, 2022 12:22 PM	

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.



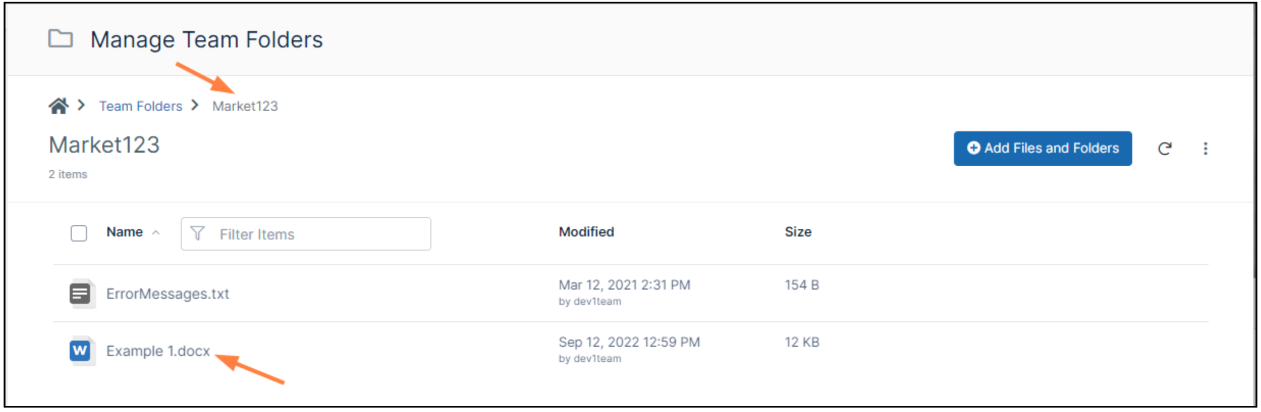
Name	Modified	Size
JTeam	Sep 12, 2022 11:28 AM	
Market123	Sep 12, 2022 12:57 PM	
Photo files	Sep 12, 2022 1:36 PM	

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



Name	Modified	Size
xxxxx	Sep 12, 2022 1:37 PM	
Example 1.docx		

6. 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.



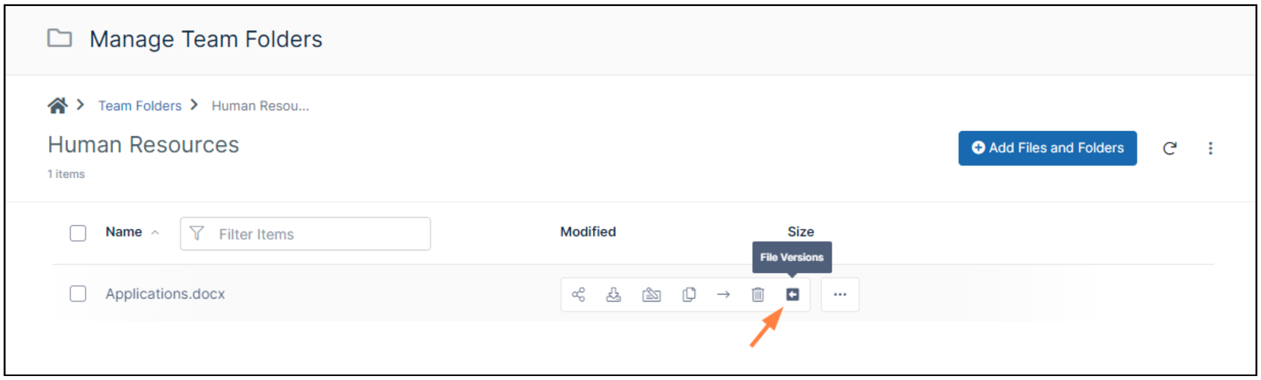
View and Restore Previous Versions in Team Folders

ⓘ 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.

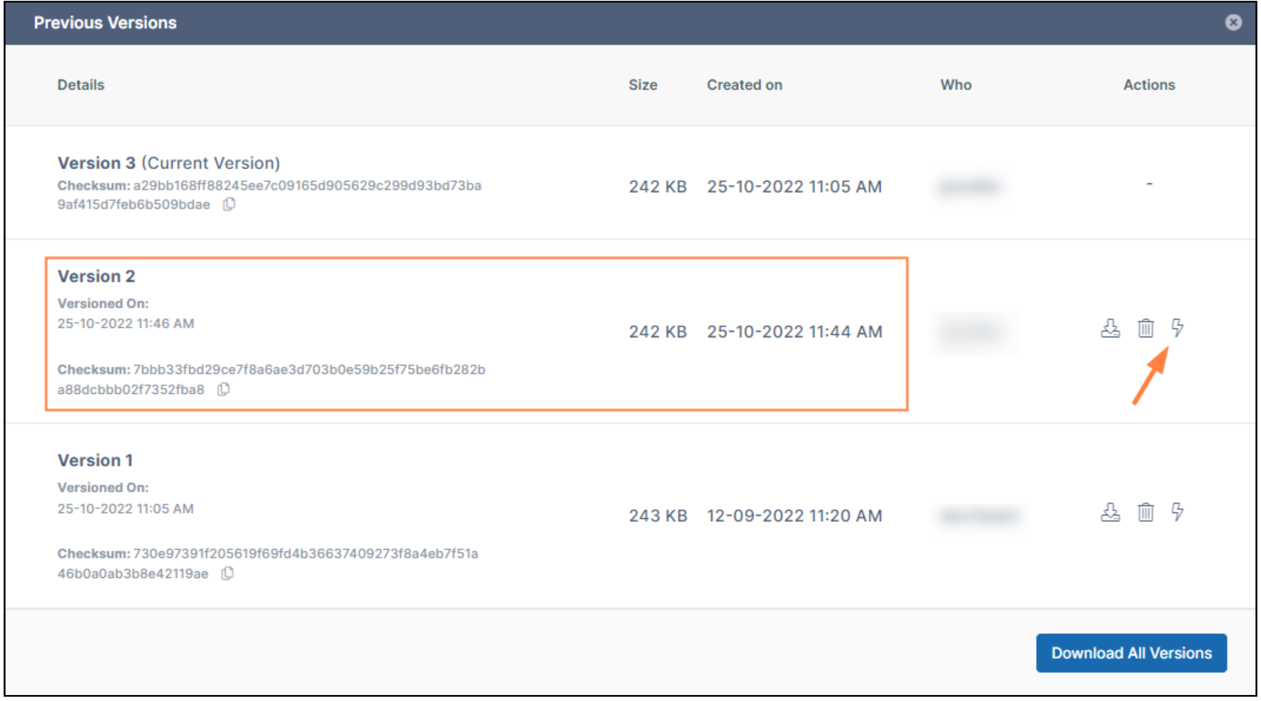
To restore a previous version of a file in Team Folders:

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.



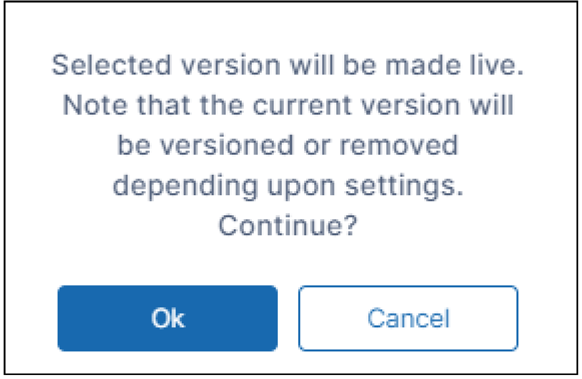
A list of the previous versions opens.

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



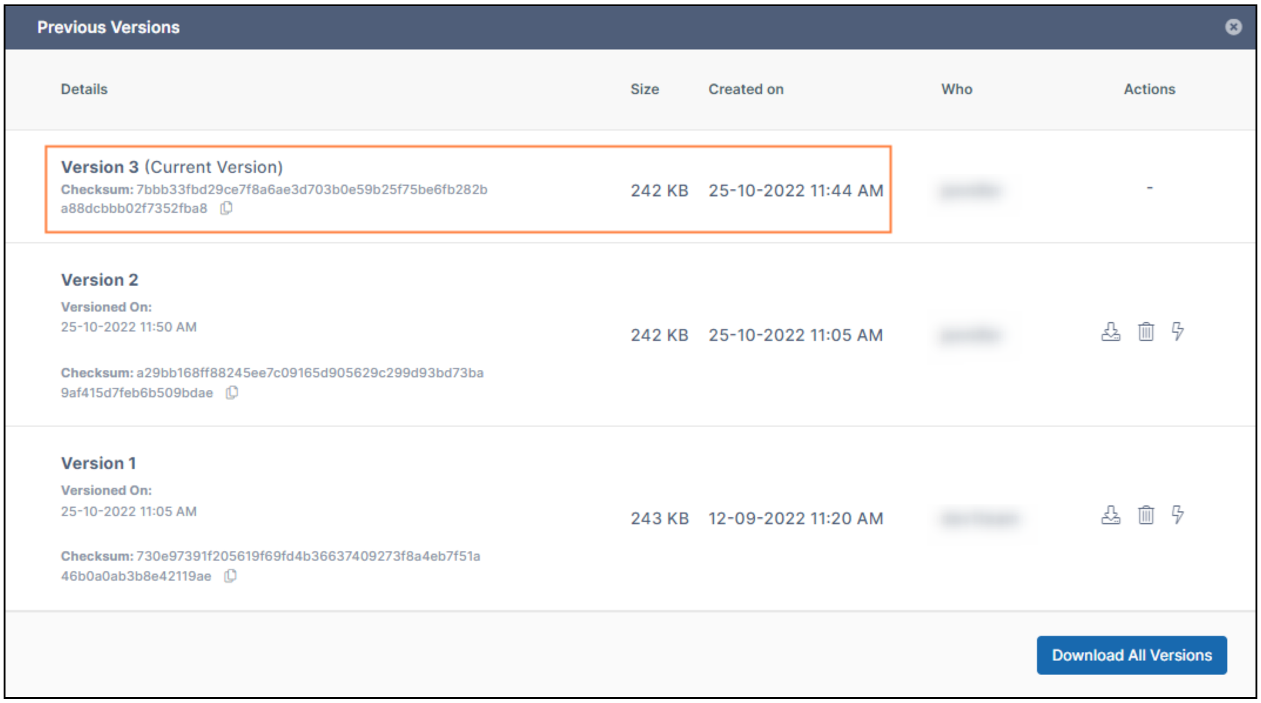
Details	Size	Created on	Who	Actions
Version 3 (Current Version) **Checksum:** a29bb168ff88245ee7c09165d905629c299d93bd73ba 9af415d7feb6b509bdae	242 KB	25-10-2022 11:05 AM	[redacted]	-
Version 2 **Versioned On:** 25-10-2022 11:46 AM **Checksum:** 7bbb33fbd29ce7f8a6ae3d703b0e59b25f75be6fb282b a88dcbbb02f7352fba8	242 KB	25-10-2022 11:44 AM	[redacted]	
Version 1 **Versioned On:** 25-10-2022 11:05 AM **Checksum:** 730e97391f205619f69fd4b36637409273f8a4eb7f51a 46b0a0ab3b8e42119ae	243 KB	12-09-2022 11:20 AM	[redacted]	

The following confirmation box appears:



Selected version will be made live. Note that the current version will be versioned or removed depending upon settings. Continue?

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:** 7bbb33fbd29ce7f8a6ae3d703b0e59b25f75be6fb282b a88dcbbb02f7352fba8	242 KB	25-10-2022 11:44 AM	[redacted]	-
Version 2 **Versioned On:** 25-10-2022 11:50 AM **Checksum:** a29bb168ff88245ee7c09165d905629c299d93bd73ba 9af415d7feb6b509bdae	242 KB	25-10-2022 11:05 AM	[redacted]	
Version 1 **Versioned On:** 25-10-2022 11:05 AM **Checksum:** 730e97391f205619f69fd4b36637409273f8a4eb7f51a 46b0a0ab3b8e42119ae	243 KB	12-09-2022 11:20 AM	[redacted]	

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	➡ Create or Import New Accounts ➡ Allow Users to Create Accounts
Configure User Authentication	➡ User Authentication Settings ➡ Enabling Default Authentication ➡ Active Directory Authentication ➡ Connecting to AD via SSL ➡ Using Single Sign-On
Integrate with other User Directory Solutions	➡ Integrate Azure AD with FileCloud ➡ Integrate Centrify with FileCloud ➡ Integrate Okta with FileCloud ➡ Integrate OneLogin with FileCloud

Manage User Accounts	➡ 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.	The default Admin account is used to manage the FileCloud. The default admin user account is 'admin'. Other users can be marked as 'admins' and given limited set of permissions. ➡ Read more about Multiple Admins
Full Access	Control over its own private cloud storage space in My Files.	These user accounts can: • store files in their own private cloud storage space • view and download files stored in their storage space • view and download files shared with them by other users
Guest Access	Restricted access to the FileCloud system.	These user accounts: • Do not have private cloud storage • Can only view/upload/download files shared to them by other user accounts • Can re-share content if they have permissions
External Access	Access to FileCloud only through a Web browser.	These user accounts: • Can only view/upload/download content shared with them • Do not count towards the user license limit • Cannot be authenticated via AD and can only be local user accounts • Have external linked email accounts and cannot use the same domain as the FileCloud URL • Can't be added directly to network shares via the admin portal • Can access content from network folders if they are shared

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

User Types Comparison

User Access Feature	Full Access	Guest Access	External Access
User Portal (Web Browser) Access	Permitted Fully functional	Permitted Not all functions available	Permitted Not all Functions Available
View shared files	Permitted	Permitted	Permitted
View Network Shares	Permitted	Permitted	**Only via shares created by users**
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**

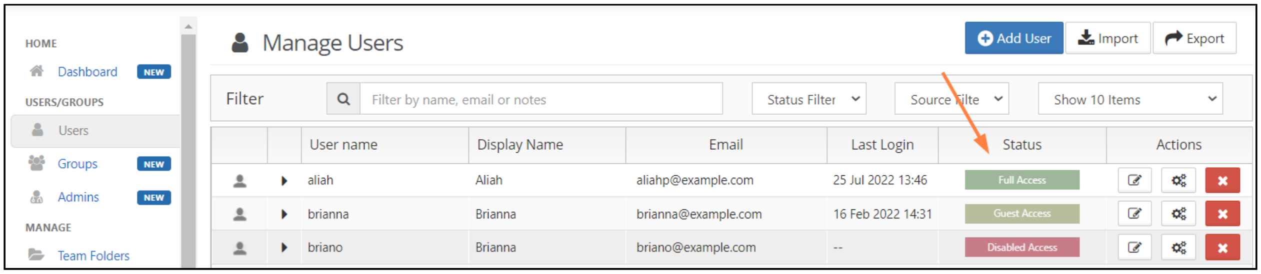
User Access Feature	Full Access	Guest Access	External Access
Group Membership	Can be member of any group	Can be member of any group	Can be member of any group except Everyone.
Admin Account	Can be Admin Account	Can be Admin Account	Cannot be an Admin Account
Team Folders	Permitted	Permitted	**Only via 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	

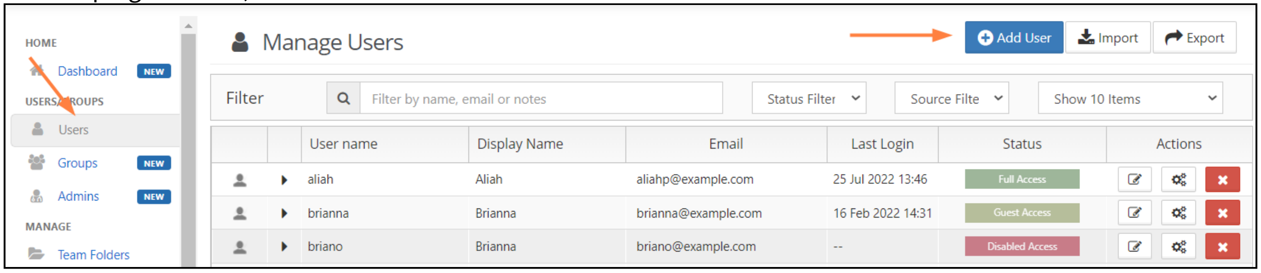
Manually Create a New User Account

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

An optional sample set of files can be preloaded for every user on creation.

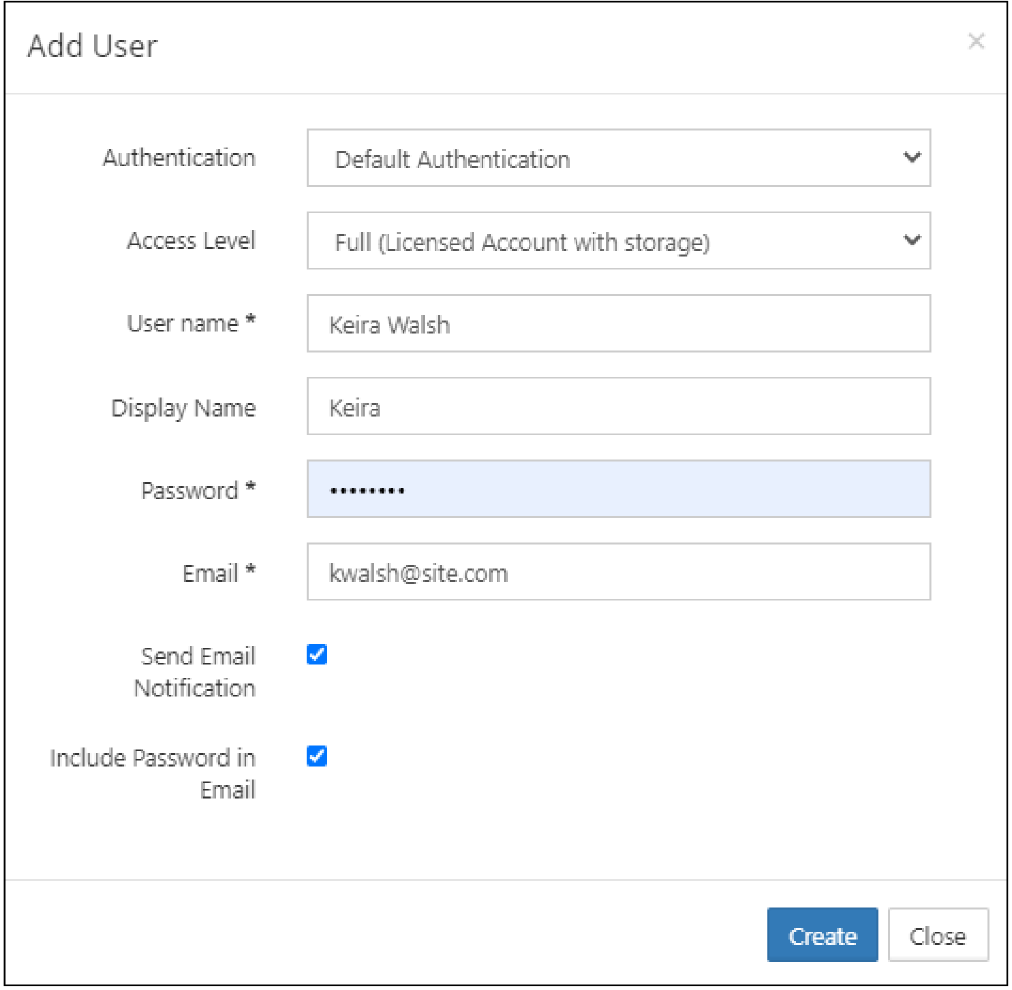
To create a FileCloud user with default authentication:

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



		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	

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	☑

Settings	Description
Authentication	Allows you to select the authentication type for granting access into the system. • Default Authentication - creates a local user account. User credentials are stored and authenticated within FileCloud. • LDAP or AD Authentication - creates an external user account. User credentials are stored and authenticated from an external LDAP or AD server.
Access Level	Allows you to select the user type. A user account with Full or Guest access counts as a license.

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

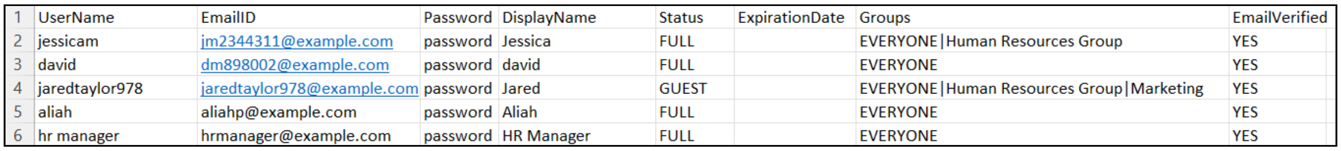
To import from a CSV, create a simple text file with the all the user account information. The format of the created file is explained below:

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: • 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.

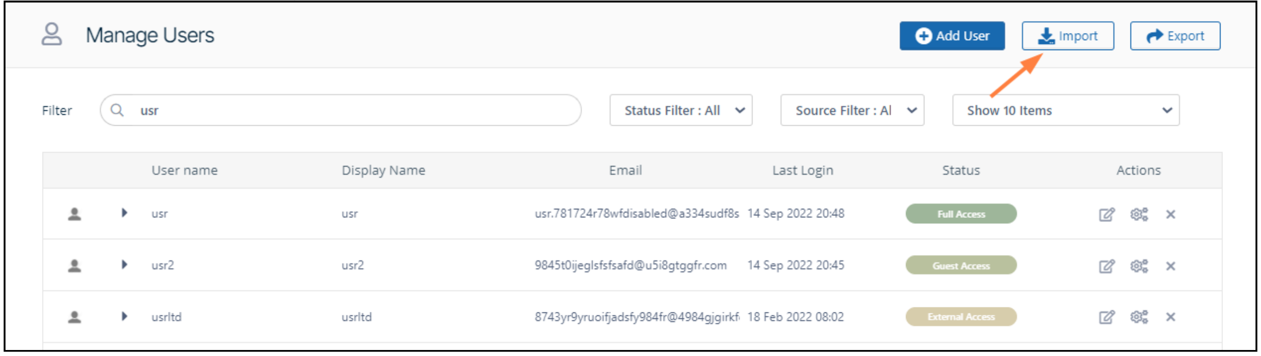


1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified
2	jessicam	jm2344311@example.com	password	Jessica	FULL		EVERYONE|Human Resources Group	YES
3	david	dm898002@example.com	password	david	FULL		EVERYONE	YES
4	jaredtaylor978	jaredtaylor978@example.com	password	Jared	GUEST		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

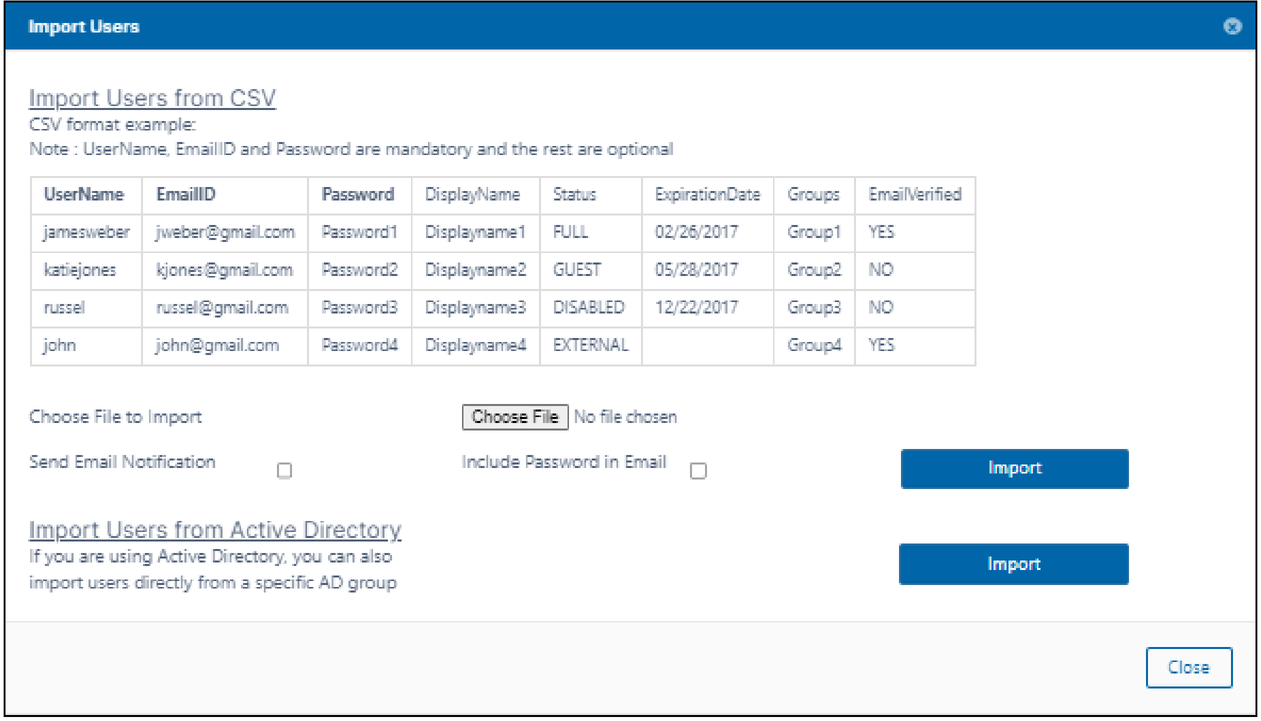
To import a CSV File:

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



User name	Display Name	Email	Last Login	Status	Actions
usr	usr	usr.781724r78wfdisabled@a334sudf8s	14 Sep 2022 20:48	Full Access	
usr2	usr2	9845t0ijeglsfsfsafd@u5i8gtggfr.com	14 Sep 2022 20:45	Guest Access	
usrltd	usrltd	8743yr9yruoifjadsfy984fr@4984gjgirkf	18 Feb 2022 08:02	External Access	

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



Import Users

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 Choose File No file chosen

Send Email Notification □ Include Password in Email □

Import Users from Active Directory

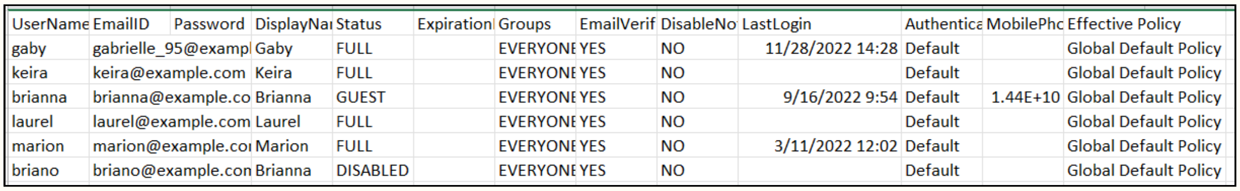
If you are using Active Directory, you can also import users directly from a specific AD group

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

5. To send a notification to each user imported, check **Send Email Notification**. (*Added in FileCloud 20.1)*
    - To include each user's password in the email, check **Include Password in Email**.
6. Click **Import.**
   When the process is complete, a report is generated indicating the status of each user account creation.

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

The fields exported are the same as the imported fields with the addition of the fields **DisableNotifications**, **LastLogin**, **Authentication Type**, **MobilePhone,** and **Effective Policy**.
Notice that the **Password** value is not exported.

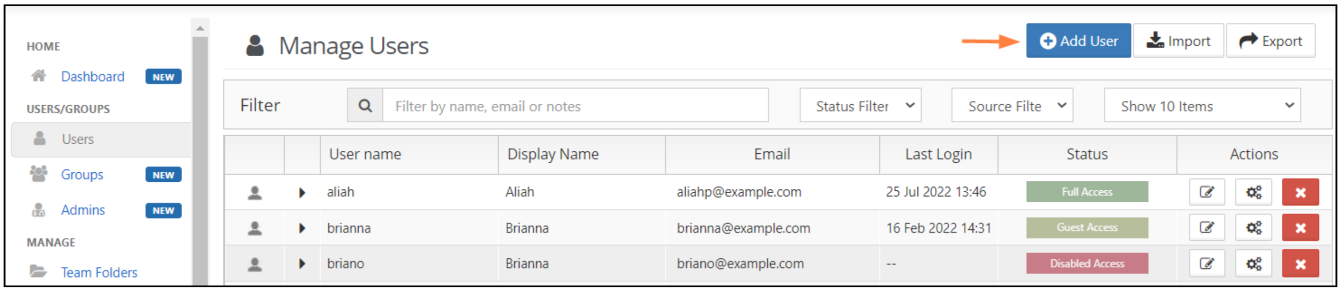


UserName	EmailID	Password	DisplayNa	Status	Expiration	Groups	EmailVerif	DisableNo	LastLogin	Authentica	MobilePhc	Effective Policy
gaby	gabrielle_95@exampl		Gaby	FULL		EVERYONE	YES	NO	11/28/2022 14:28	Default		Global Default Policy
keira	keira@example.com		Keira	FULL		EVERYONE	YES	NO		Default		Global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

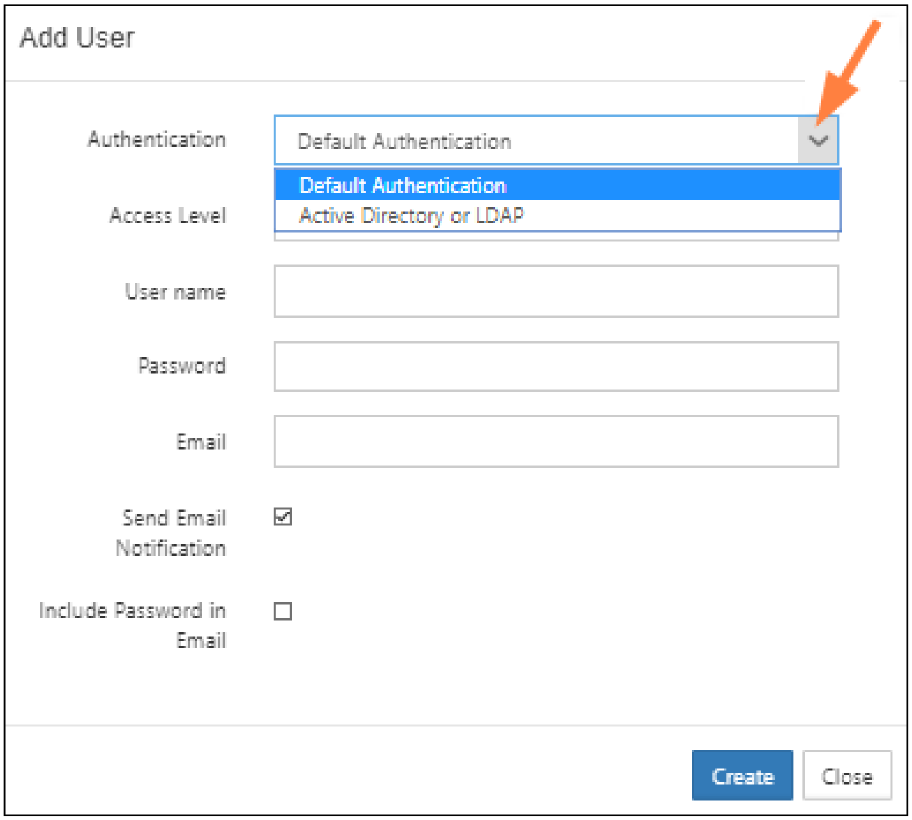
Import a user account from AD or LDAP Service

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

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



		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	Default 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.

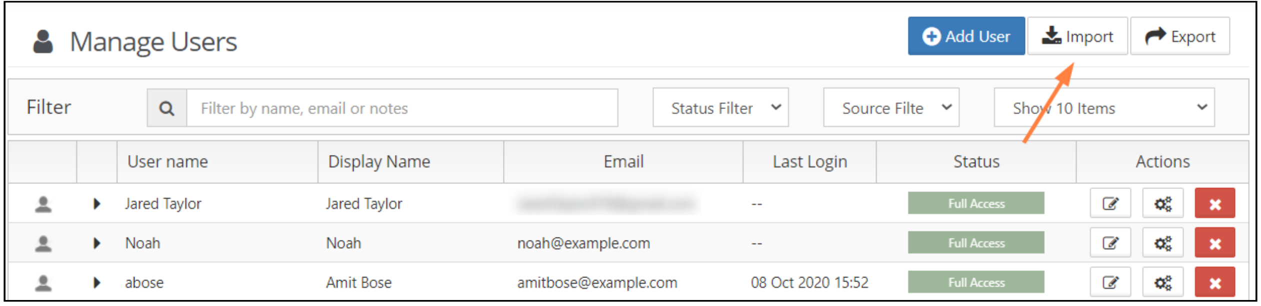
FileCloud Server version 19.1 and later has been modified to stop displaying built-in AD groups that cannot be imported.

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

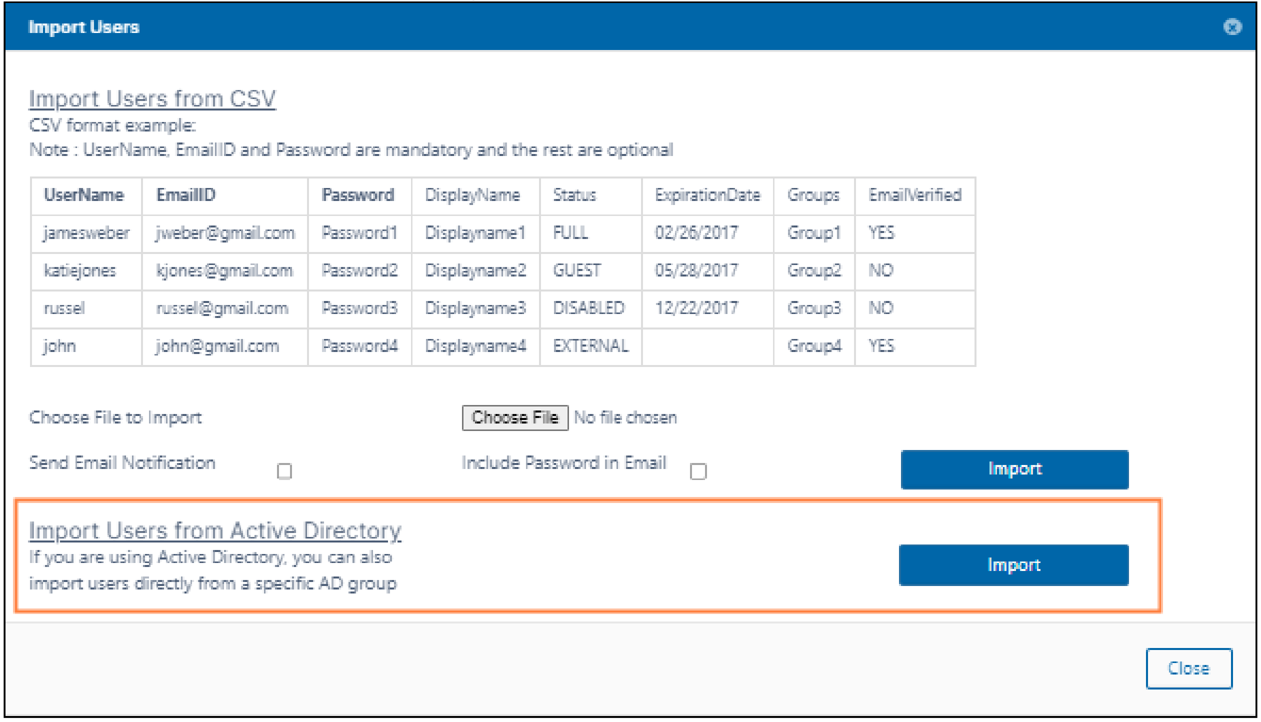
To import users from an AD server:

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**.



		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**.



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

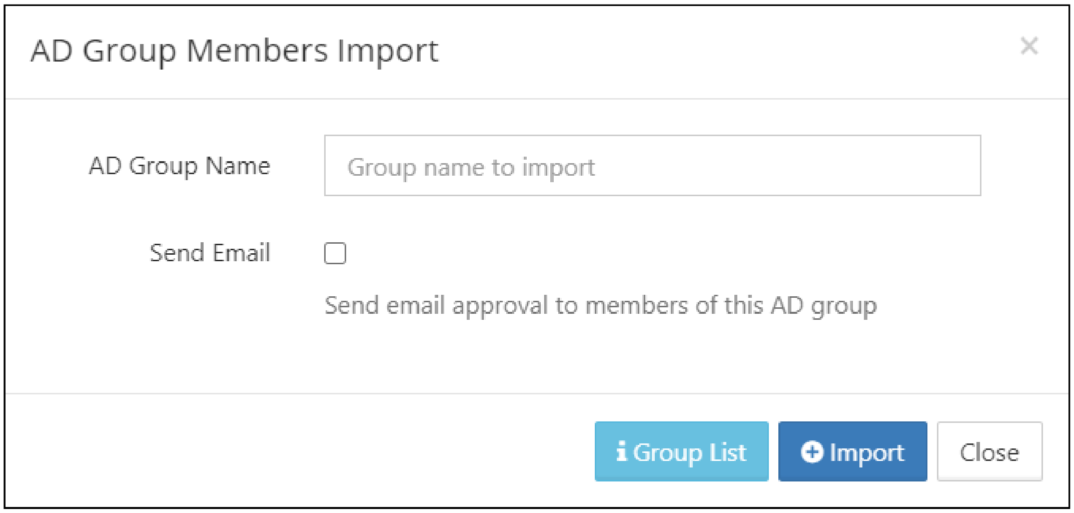
Choose File to Import Choose File No file chosen

Send Email Notification □ Include Password in Email □ Import

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.



AD Group Members Import

AD Group Name: Group name to import

Send Email □

Send email approval to members of this AD group

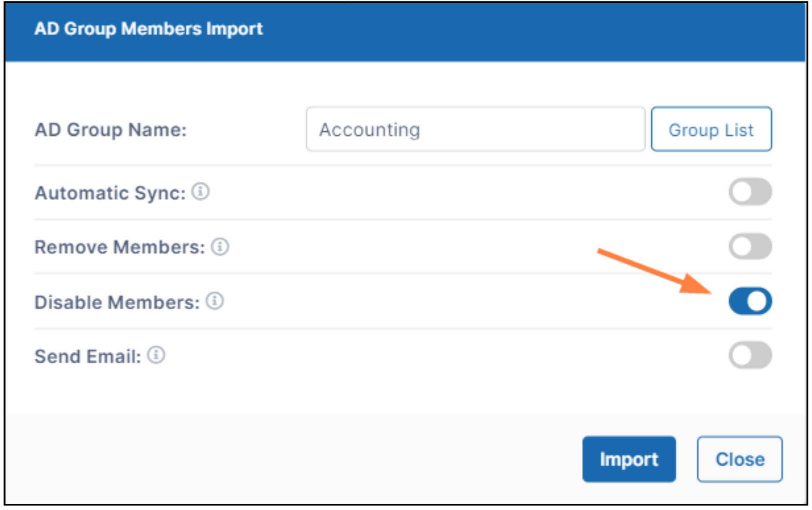
6. Type in the **AD Group Name**. A list of existing groups can also be viewed by clicking the **Group List** button.
7. To send an email to notify each user after their account is approve, check **Send Email**.
8. Click the **Import** button.

Import Disabled Users from Active Directory as Disabled

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

To use this option:

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



AD Group Members Import

AD Group Name: Accounting

Automatic Sync: ⓘ ○ (off)

Remove Members: ⓘ ○ (off)

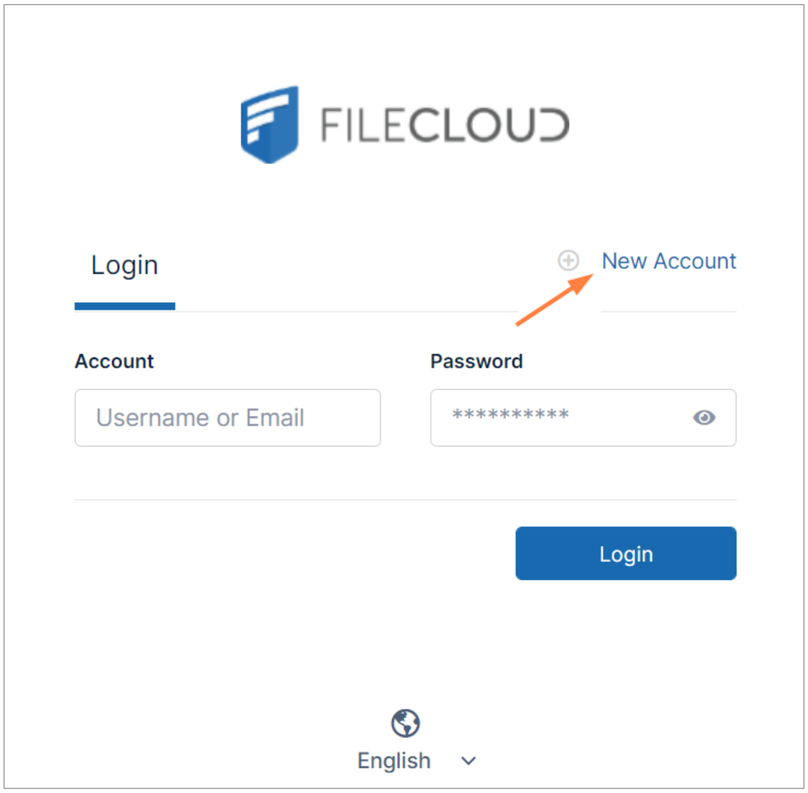
Disable Members: ⓘ ● (on)

Send Email: ⓘ ○ (off)

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

New Account Creation

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



Administrators can customize how new user accounts are created.

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

Who can create and approve accounts

New account settings

Table 1. The Settings

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

Setting	Location	Options	Description
Allow Account Signups	Settings > Admin tab	Specifies if a user can or cannot create a new FileCloud user account from the login-in page. by choosing: • DEFAULT • TRUE • FALSE **Can Create an Account** Prerequisite: *Show New Account Button* = Enabled DEFAULT = AD and LDAP users can create their own accounts • Active Directory authentication allowed • LDAP authentication allowed • Local users (who are not using AD or LDAP authentication) cannot create their own accounts.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the *Automatic Account Approval* settings. Do I choose DEFAULT or TRUE? **DEFAULT** • If you are using AD or LDAP authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, 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. **Note**: If you are not using AD or LDAP authentication, users cannot create their own accounts. **TRUE** • If you are NOT using AD or LDAP authentication • You want to allow your users to create their own user accounts. By default, the account is disabled until an Administrator approves it. **Note**: If you are using AD or LDAP authentication, users can create their own accounts.

Setting	Location	Options	Description
		TRUE = Local users can create their own accounts - Local users (who are not using AD or LDAP authentication) can create their own accounts. - Active Directory authentication not allowed - LDAP authentication not allowed **Cannot Create an Account** FALSE = No users can create their own accounts - If the New Account button is enabled, and the user clicks it, an error message indicates that new account creation is not allowed.	

Setting	Location	Options	Description
Automatic Account Approval	Settings > Admin tab	(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. 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.	💡 **If the total number of licenses has been reached, share invitations to new users are blocked unless Automatic Account Approval is set to 3.** Prerequisites: • **New Account** = ENABLED • **Allow Account Signups** = DEFAULT or TRUE This setting works with the **Allow Account Signups** setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and you can use the automatic account approval settings.

Scenarios

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

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

Table 2. Only an Admin Creates New Accounts

Only an Admin can create (or deny) User accounts
1. The administrator enables the account in the Admin Portal on the Users page by changing the user's status from *Disabled Access* to one of the enabled access statuses. 2. The user receives a Welcome email with the account credentials and User Portal URL. Note: An administrator denies approval by deleting a user account. In this case the user receives an email to inform them that the account has not been approved.
Customization settings, Login tab ❌ New Account button = DISABLED **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

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

⚠ This scenario does not work for AD and LDAP users. Refer to the specific scenarios and settings for AD and LDAP users. 1. The Administrator configures the User Search Mode. 2. The Administrator configures New Account Creation settings. 3. The Administrator provides the user with the URL for the User Portal OR an invitation to create a new account is sent when a user shares a folder or file. 4. The User accesses the user portal from a Web browser, mobile device, 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.

12. The user is required to verify the email account to complete the account creation process.		10. The user is required to verify the email account to complete the account creation process.		10. 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 = 0		**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.		**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 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.

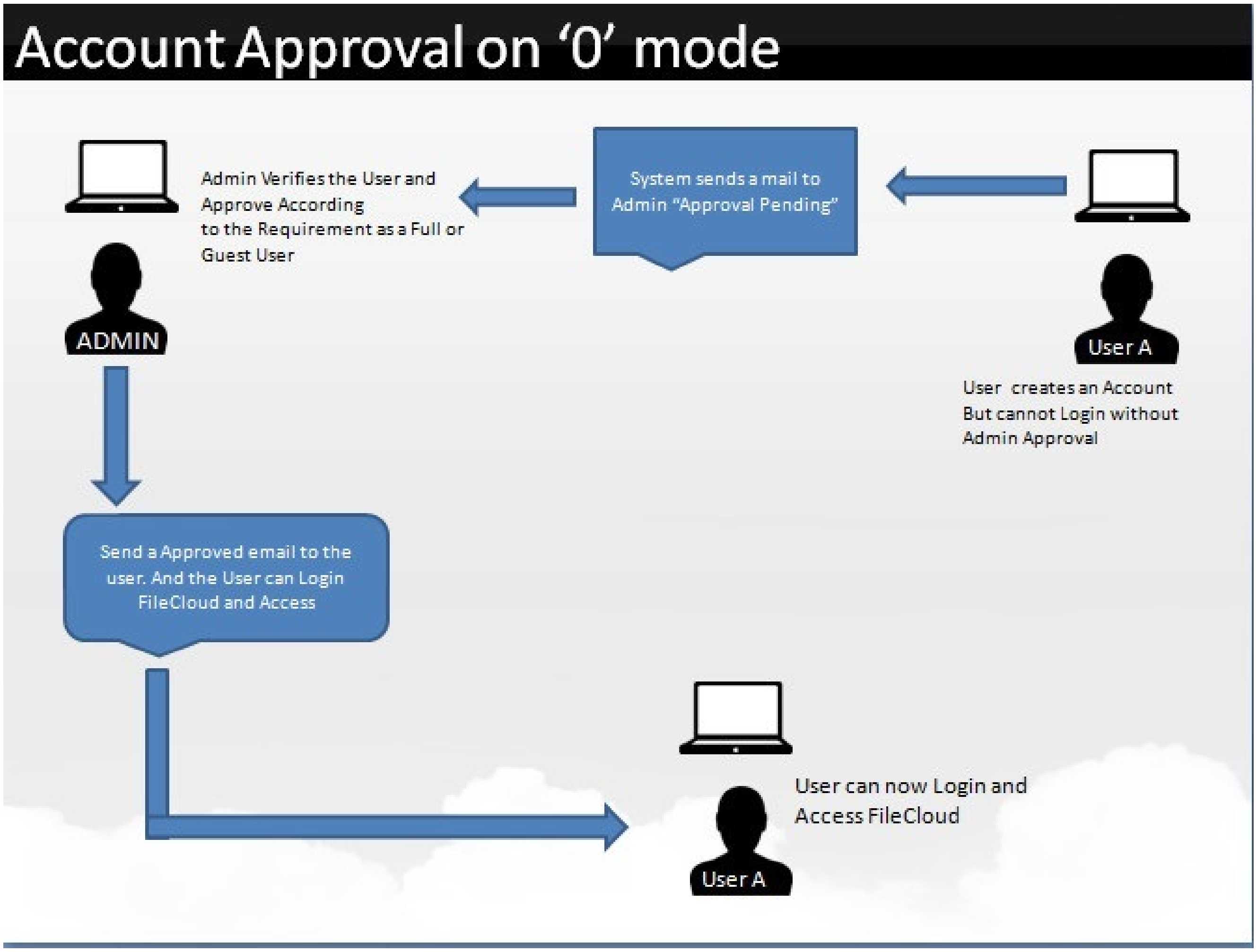
Modes	Description
1 - Automatically approved to Full User	This mode allows the user to Create Account and access FileCloud without waiting for Admin 's approval. This mode lets user create account as FULL USER Permission.
2 - Automatically approved to Guest User	This mode also allows the user to Create 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 '0' mode

Admin Verifies the User and Approve According to the Requirement as a Full or Guest User

System sends a mail to Admin "Approval Pending"

User creates an Account But cannot Login without Admin Approval

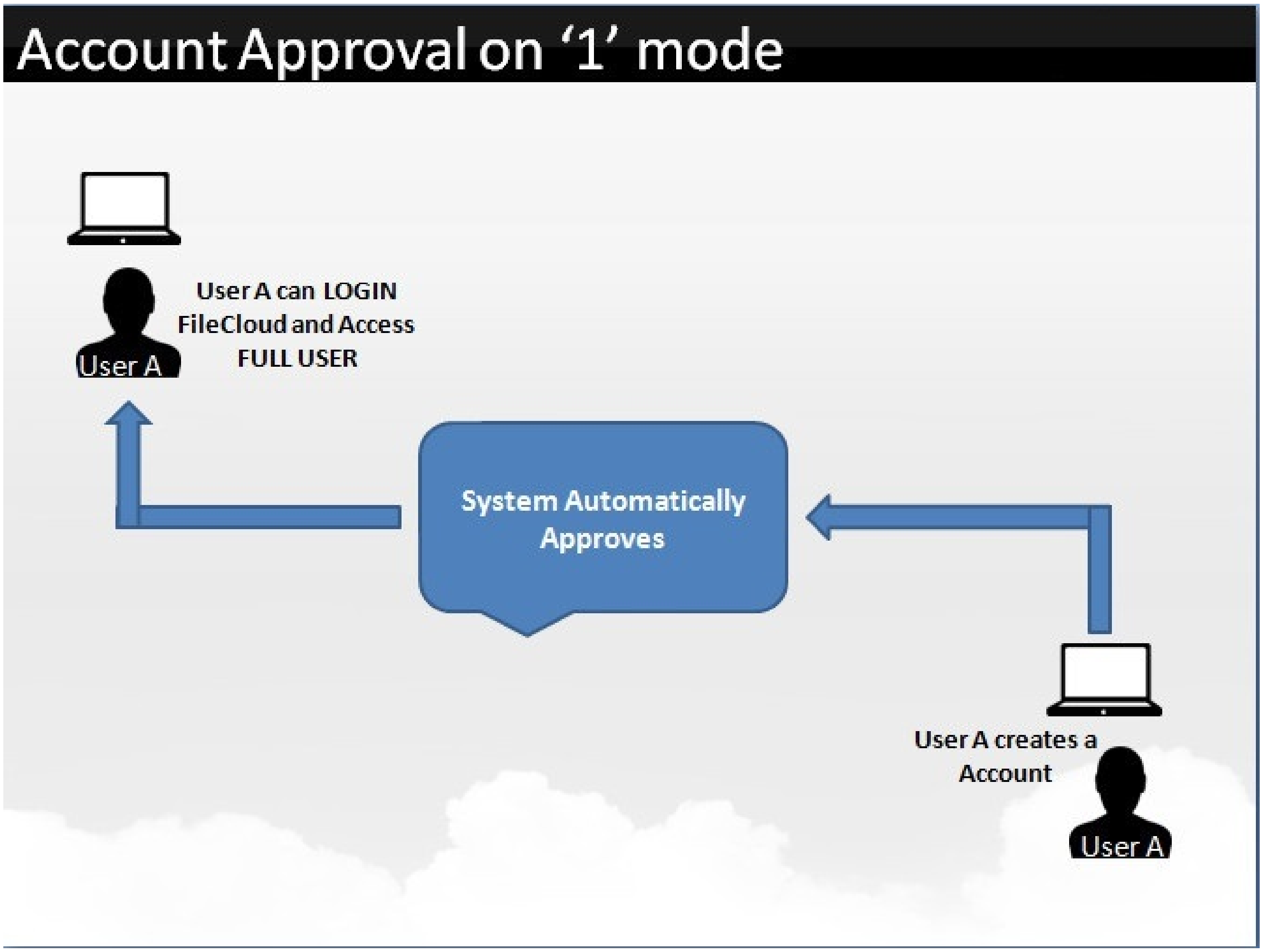
Send a Approved email to the user. And the User can Login FileCloud and Access

User can now Login and Access FileCloud

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.

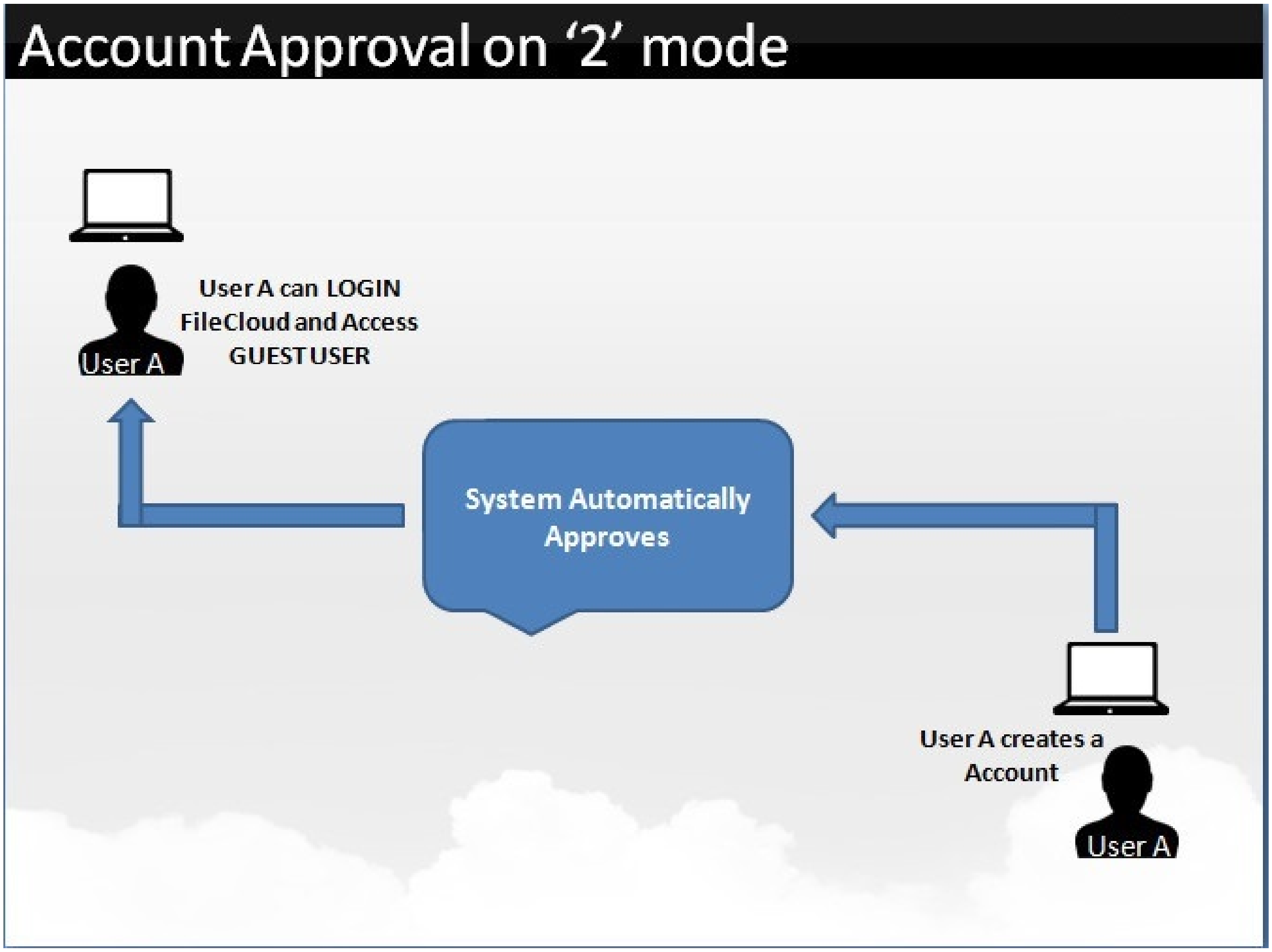
User is logged in the System as FULL USER in this mode.



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 '2' mode

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

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
New Account	ENABLED = opens a window for the user to type in new account information DISABLED = opens a window explaining that User Account Creation is not allowed	This setting determines the behavior of the New Account button on the User Portal Login page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • Allow Account Signups • Automatic Account Approval

Setting	Options	Description
Allow Account Signups	Specifies if a user can or cannot create an new FileCloud user account by choosing: - DEFAULT - TRUE - FALSE **Can Create an Account** Prerequisite: *New Account* = Enabled DEFAULT = Local user authentication is allowed - Active Directory authentication allowed - LDAP authentication allowed TRUE = Local user can create their own account **Cannot Create an Account** FALSE = Local user cannot create their own account - 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.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the *Automatic Account Approval* settings. Do I choose DEFAULT or TRUE? **DEFAULT** - 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. **TRUE** - 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
Automatic Account Approval	(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. 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.	Prerequisites: • *New Account* = ENABLED • *Allow Account Signups* = DEFAULT or TRUE This setting works with the *Allow Account Signups* setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.

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

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

1. The Administrator configures the Authentication Type as Active Directory or LDAP. 2. (Optional) The Administrator imports AD or LDAP user accounts into FileCloud. 3. The Administrator provides the user with the URL for the User Portal. 4. The User accesses the user portal from a Web browser, mobile device, 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.		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 = 1, 2		**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 ℹ 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 allows 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
New Account	ENABLED = opens a window for the user to type in new account information DISABLED = opens a window explaining that User Account Creation is not allowed	This setting determines the behavior of the New Account button on the User Portal Login page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • Allow Account Signups • Automatic Account Approval

Setting	Options	Description
Allow Account Signups	Specifies if a user can or cannot create an new FileCloud user account by choosing: • DEFAULT • TRUE • FALSE **Can Create an Account** Prerequisite: *New Account* = Enabled DEFAULT = Local user authentication is allowed • Active Directory authentication allowed • LDAP authentication allowed TRUE = Local user can create their own account • Active Directory authentication not allowed • LDAP authentication not allowed **Cannot Create an Account** FALSE = Local user cannot create their own account • 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.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the *Automatic Account Approval* settings. Do I choose DEFAULT or TRUE? **DEFAULT** • If you are using AD or LDAP Authentication. • You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, 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. **TRUE** • 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
Automatic Account Approval	(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. 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.	Prerequisites: • *New Account* = ENABLED • *Allow Account Signups* = DEFAULT or TRUE This setting works with the *Allow Account Signups* setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.

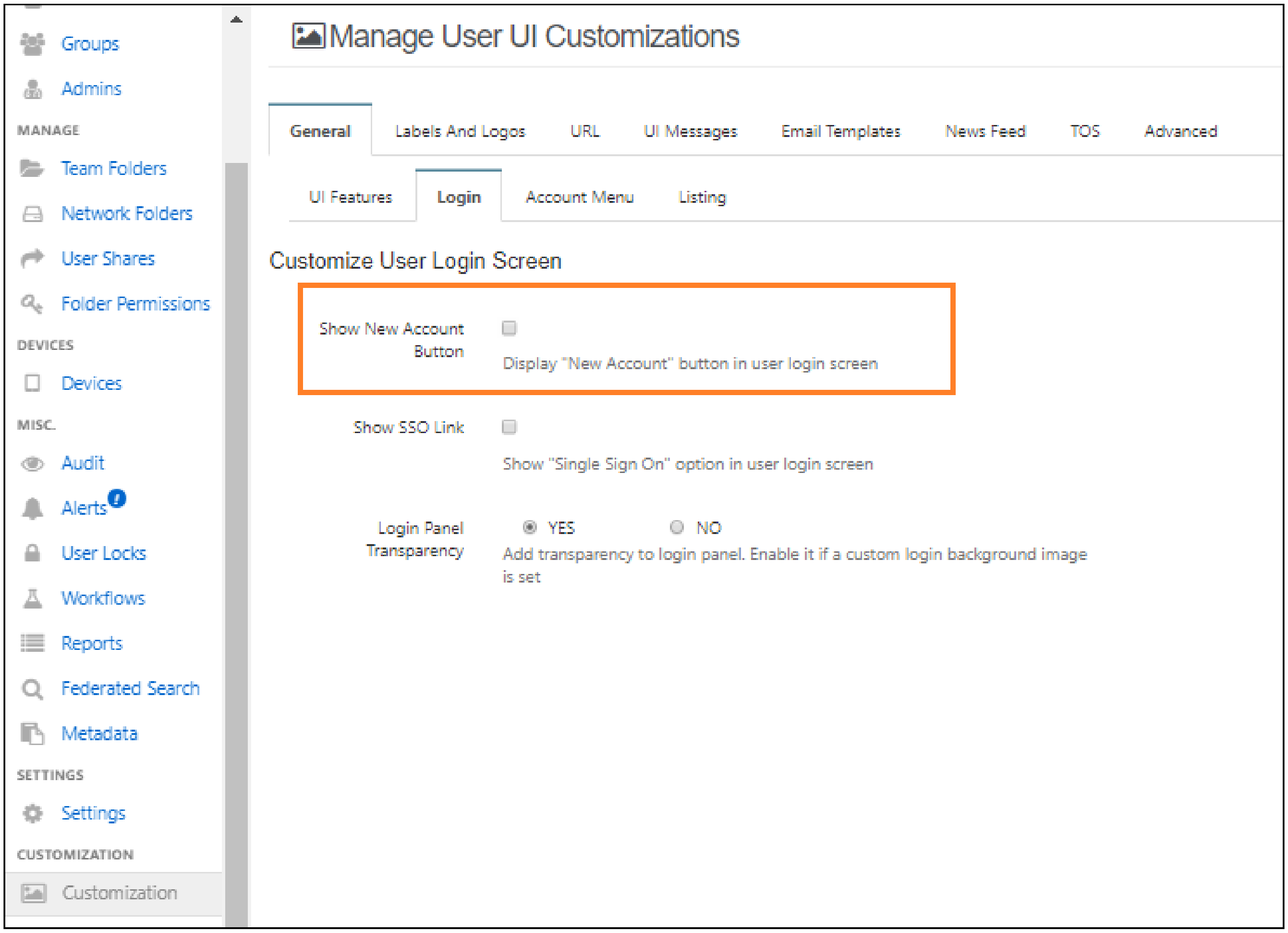
The scenario where only an administrator creates a new FileCloud account is described in Table 2.

Only an Admin can create User accounts
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.
Customization settings, Login tab ❌ New Account button = DISABLED **Settings option, Admin tab** ❌ 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.



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

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

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
New Account	ENABLED = opens a window for the user to type in new account information. DISABLED = opens a window explaining that User Account Creation is not allowed.	This setting determines the behavior of the New Account button on the User Portal Login page. If enabled, this setting works with two other settings to determine authentication and approval permissions: • Allow Account Signups • Automatic Account Approval

Setting	Options	Description
Allow Account Signups	Specifies if a user can or cannot create a new FileCloud user account by choosing: - DEFAULT - TRUE - FALSE **Can Create an Account** Prerequisite: *New Account* = Enabled DEFAULT = Local user authentication is allowed - Active Directory authentication allowed - LDAP authentication allowed TRUE = Local user can create their own account - Active Directory authentication not allowed - LDAP authentication not allowed **Cannot Create an Account** FALSE = Local user cannot create their own account - 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.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the *Automatic Account Approval* settings. Do I choose DEFAULT or TRUE? **DEFAULT** - If you are using AD or LDAP Authentication. - You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, 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. **TRUE** - 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
Automatic Account Approval	(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. 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.	Prerequisites: • *New Account* = ENABLED • *Allow Account Signups* = DEFAULT or TRUE This setting works with the *Allow Account Signups* setting to determine: • If the account created by the user is disabled until the Administrator approves it. • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created, so you can use the automatic account approval settings.

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*

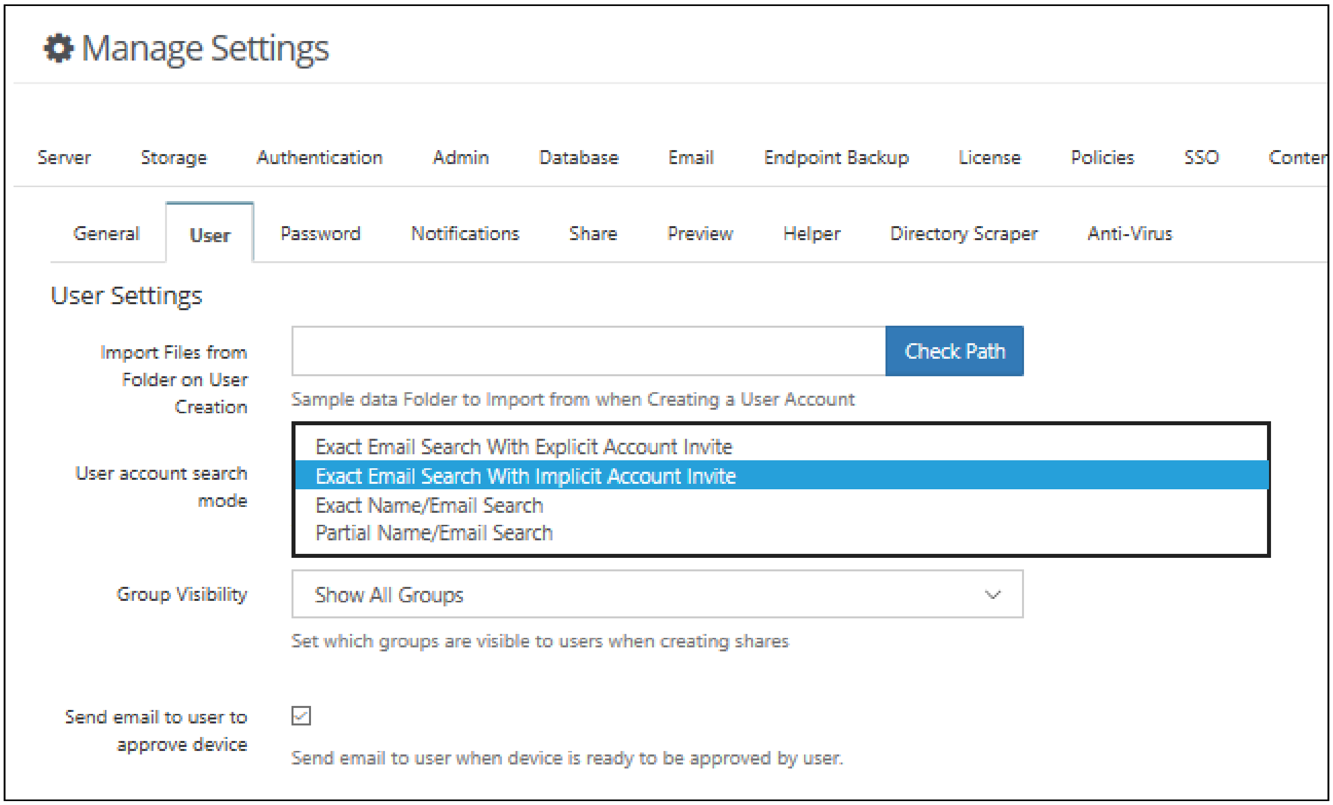
✓ Automatic Account Approval = *1, 2, 3*

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*.



User Settings

Import Files from Folder on User Creation

Sample data Folder to Import from when Creating a User Account

User account search mode

Exact Email Search With Explicit Account Invite
Exact Email Search With Implicit Account Invite
Exact Name/Email Search
Partial Name/Email Search

Group Visibility: Show All Groups

Set which groups are visible to users when creating shares

Send email to user to approve device ☑

Send email to user when device is ready to be approved by user.

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
New Account	ENABLED = opens a window for the user to type in new account information DISABLED = opens a window explaining that User Account Creation is not allowed	This setting determines the behavior of the New Account button on the user log-in page. If enabled, this setting works with two other settings to determine authentication and approval permissions: - Allow Account Signups - Automatic Account Approval
Allow Account Signups	Specifies if a user can or cannot create an new FileCloud user account from the log-in page by choosing: - DEFAULT - TRUE - FALSE **Can Create an Account** Prerequisite: *New Account* = Enabled DEFAULT = Local user authentication is allowed - Active Directory authentication allowed - LDAP authentication allowed TRUE = Local user can create their own account - Active Directory authentication not allowed - LDAP authentication not allowed **Cannot Create an Account** FALSE = Local user cannot create their own account - 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.	This setting controls if the user can create a new account. By default, the account is disabled until an administrator approves it. If you want the account to be automatically approved, use the *Automatic Account Approval* settings. Do I choose DEFAULT or TRUE? **DEFAULT** - If you are using AD or LDAP Authentication. - You want to allow your AD users to create their own FileCloud user accounts. After you import AD or LDAP user accounts into FileCloud, 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. **TRUE** - 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
Automatic Account Approval	(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. 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.	Prerequisites: • *New Account* = ENABLED • *Allow Account Signups* = DEFAULT or TRUE This setting works with the *Allow Account Signups* setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. 💡 For smaller organizations or high security sites, you can configure this option so that when a user creates a new account it is disabled until it is approved by the administrator. 💡 For larger organizations, it might not be practical to have the administrator approve every account created and so you can use the automatic account approval settings.

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

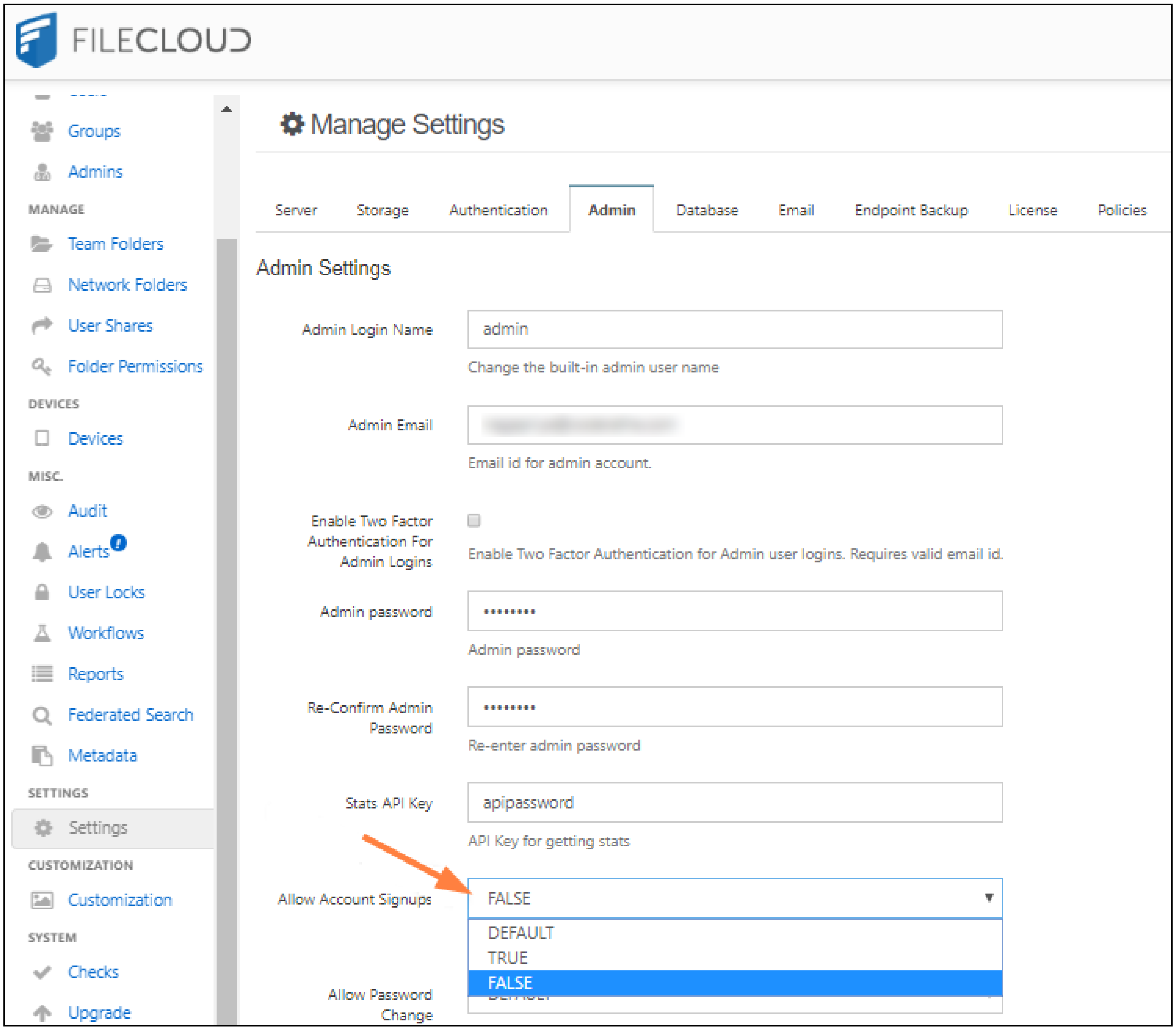
✗ Automatic Account Approval = 0

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.



Admin Settings

Admin Login Name: admin
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.

Admin password: ••••••••
Admin password

Re-Confirm Admin Password: ••••••••
Re-enter admin password

Stats API Key: apipassword
API Key for getting stats

Allow Account Signups: FALSE

Allow Password Change

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

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

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

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

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

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

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

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

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

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

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

Preload data for new accounts

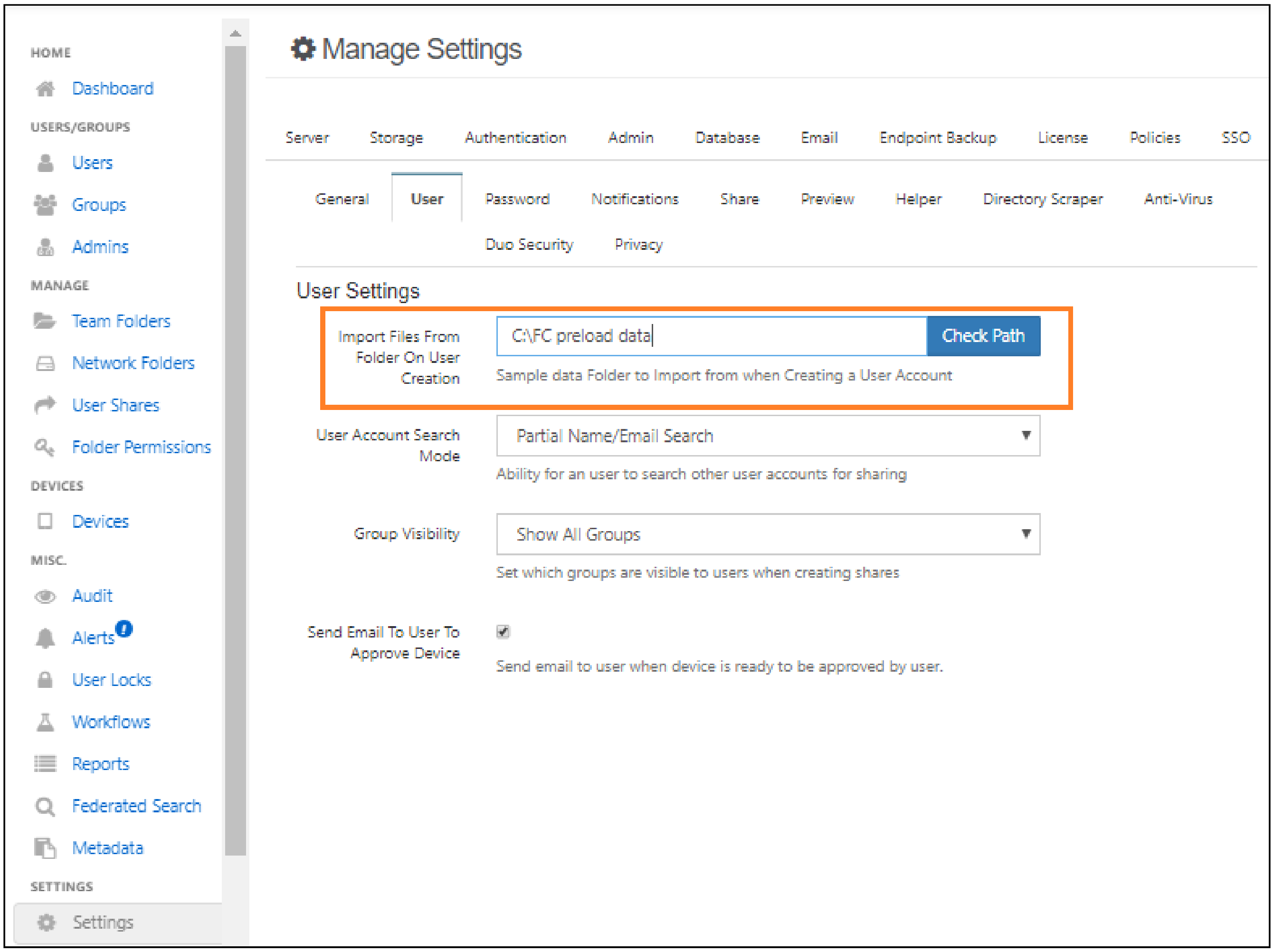
It is possible to preload user account with a set of sample files and folders. This could be useful to pre-populate a new user account with some help files etc.

Set up sample data folder when creating user account

This can be done using the following steps

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

3. Click on "**Misc**" tab
4. In "**User**" tab of "**Misc**" Settings, Enter the path containing the folder to preload in "**Import Files from Folder on User Creation**"
5. Click **Save**



User Settings

Import Files From Folder On User Creation: C:\FC preload data
Sample data Folder to Import from when Creating a User Account

User Account Search Mode: Partial Name/Email Search
Ability for an user to search other user accounts for sharing

Group Visibility: Show All Groups
Set which groups are visible to users when creating shares

Send Email To User To Approve Device: ☑
Send email to user when device is ready to be approved by user.

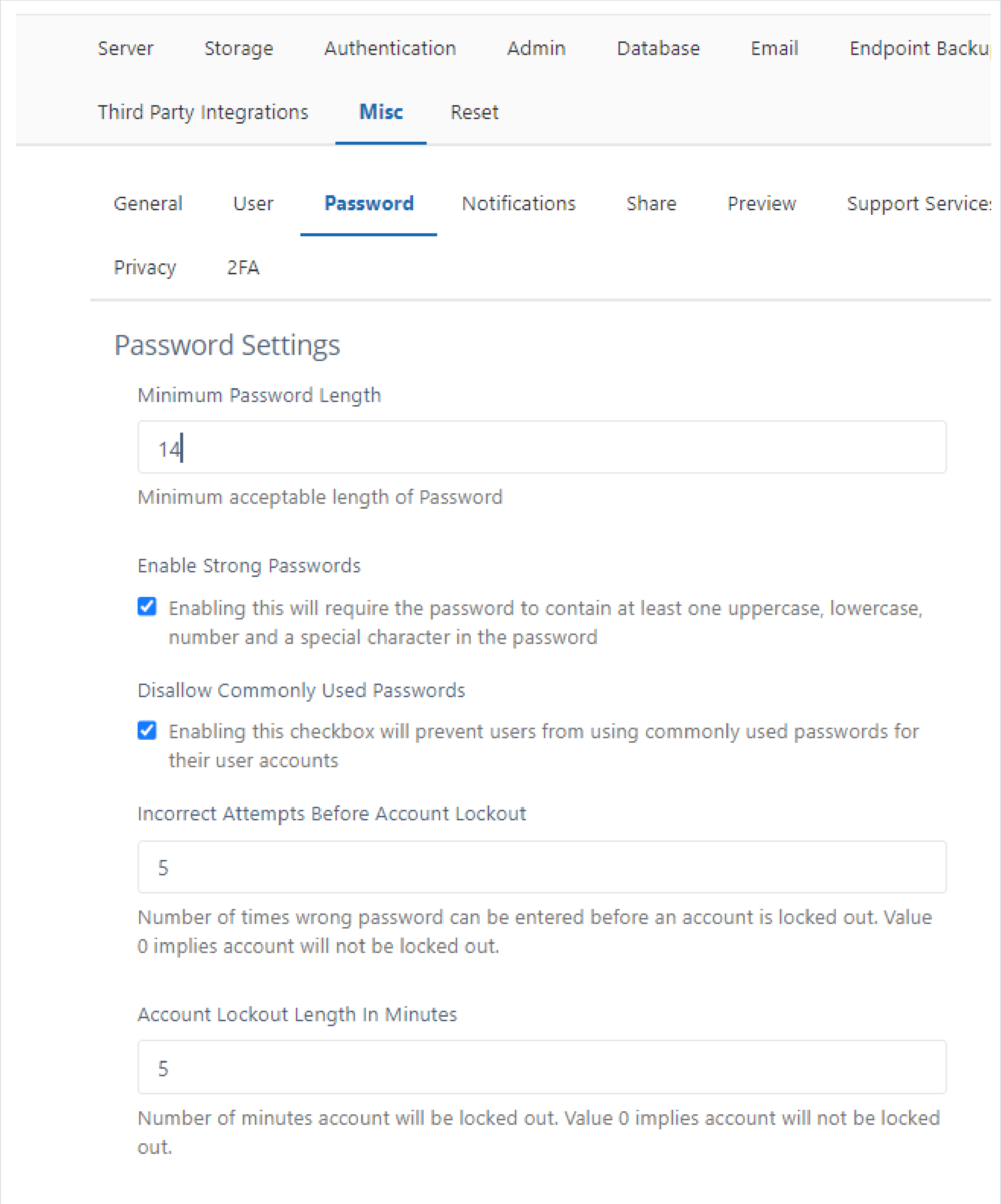
Password Settings

ⓘ 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**.



Password Settings

Minimum Password Length

14

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

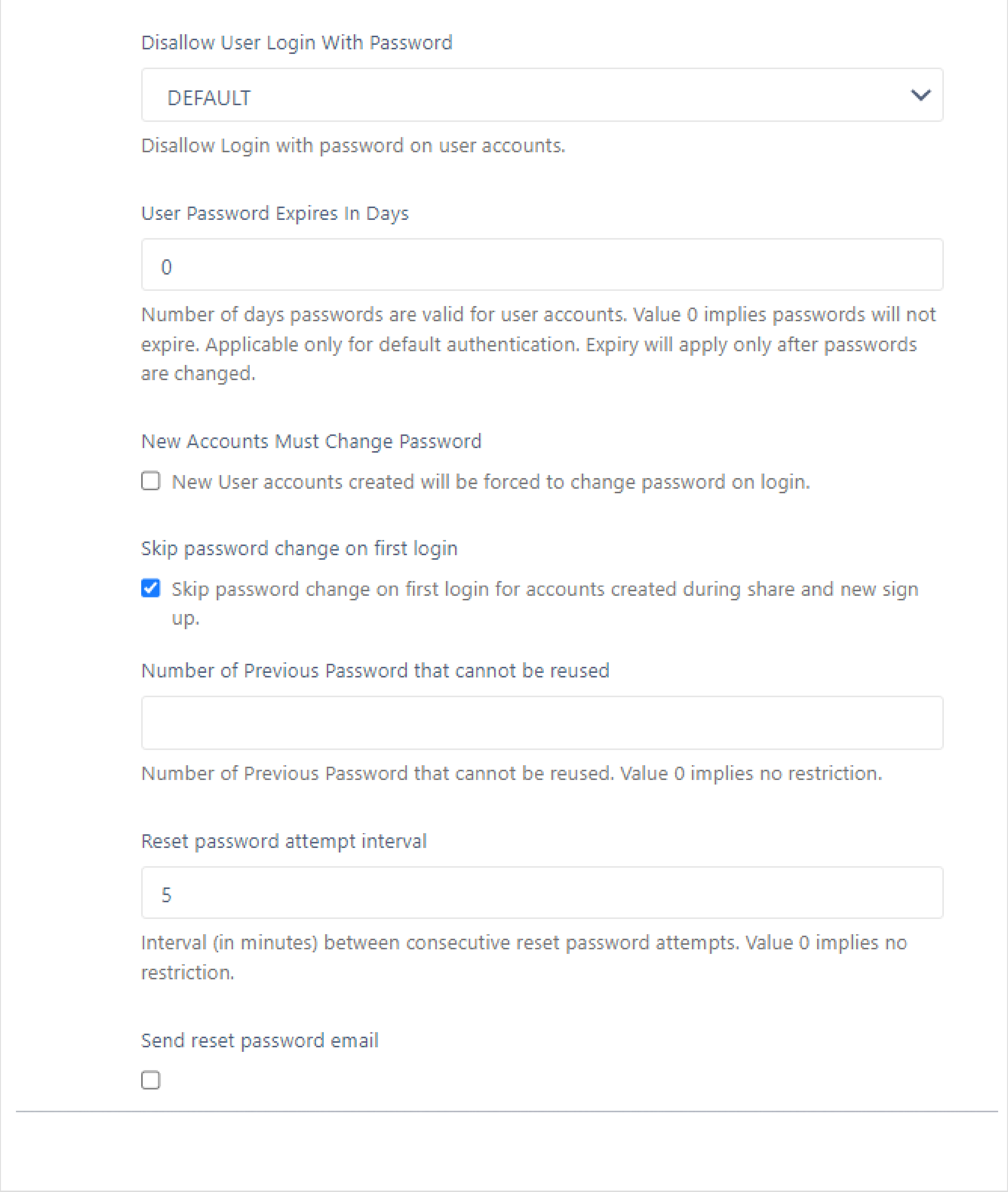
5

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

5

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

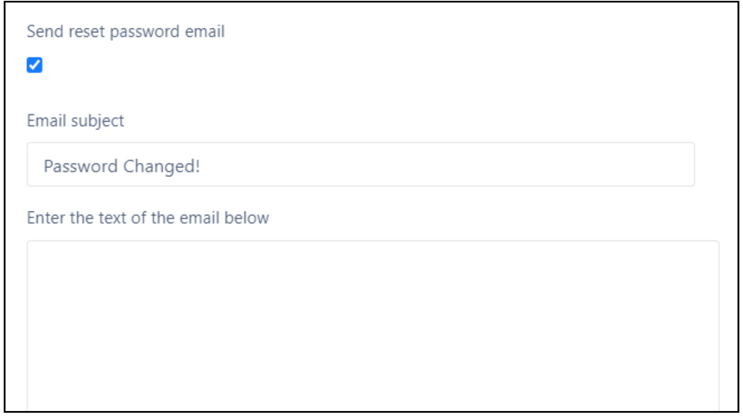
5

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

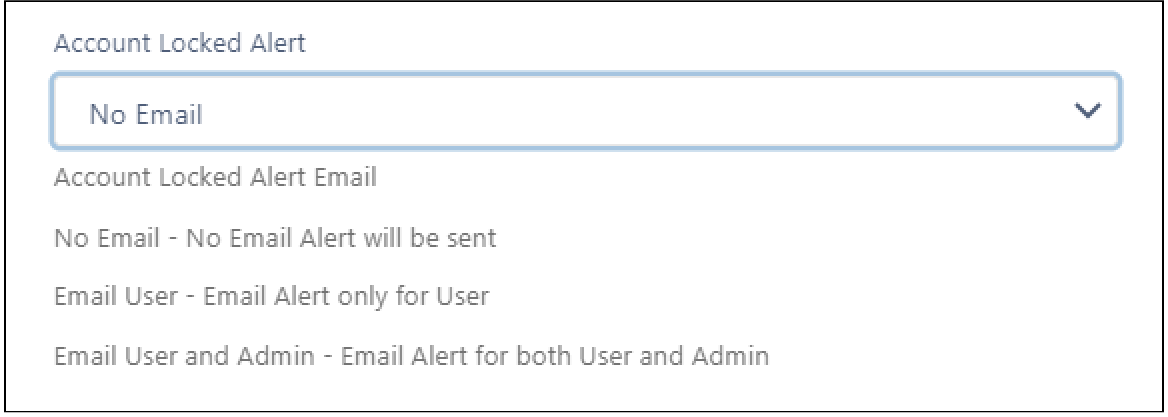
Type	Description
New accounts must change password	When enabled, this setting forces new users to change their password on initial login, with the following exceptions: • When the user creates the new account through a registration form (the user adds a password in the form). • When the user has an AD account (the user is automatically assigned an AD password). Default is disabled.
Skip password change on first login	Do not require password change on first login for accounts created during shared and new signups. Checked by default.
Number of previous passwords that cannot be reused	Specifies the number of previous passwords that cannot be reused when password is changed. A value of 0 indicates that there are no restrictions.
Reset password attempt interval	Interval in minutes between consecutive reset password attempts. Default is 5. 0 indicates that there is no restriction.
Send reset password email	Allows you to create an email that is automatically sent to a user when an admin resets the user's password. There is no default email; when this is checked, email subject and email content fields appear.  Send reset password email ☑ Email subject Password Changed! Enter the text of the email below **Email subject** is set to **Password Changed!** but may be changed. The note in **Enter the text of the email below** must be entered. Unchecked by default.

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.

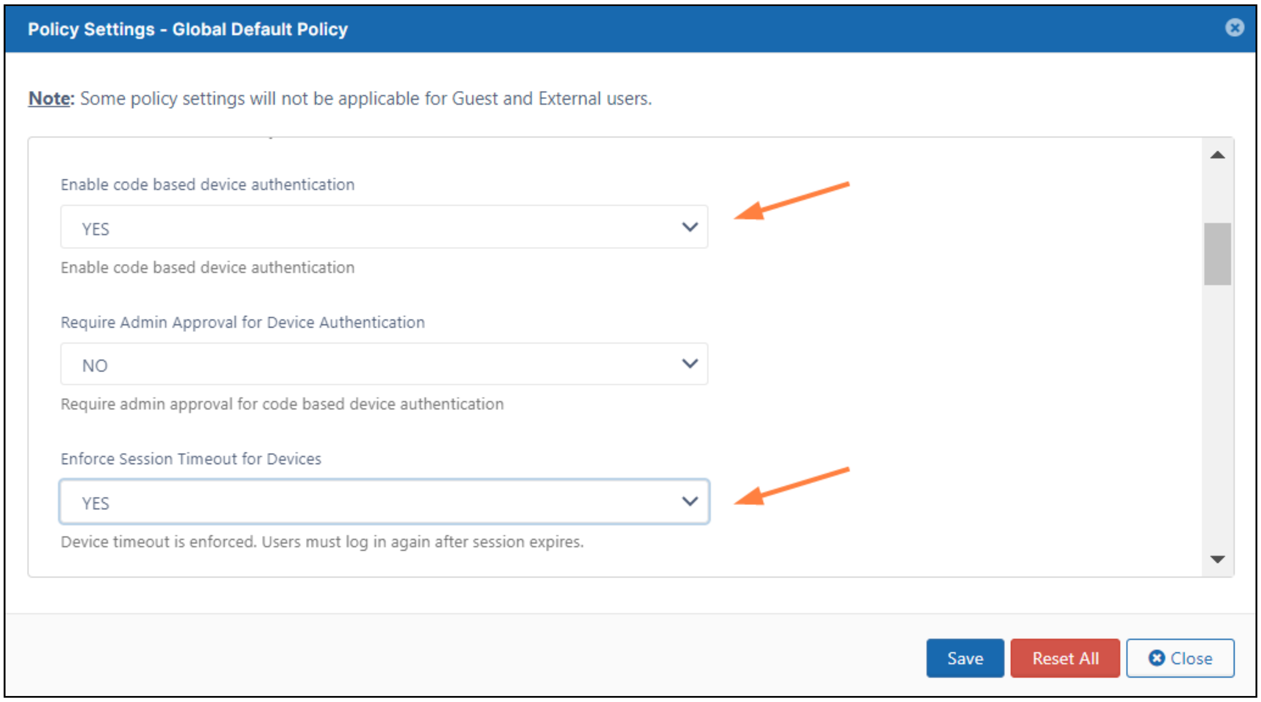
Enabling Session Expiration for all Devices

ⓘ 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.

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.

Disabling Session Expiry when Browser is closed

Session expiry time is valid until timeout setting expires or the browser is closed. If the browser is reopened, the user must log in again.

If session should be valid even when the browser is closed, set the following config parameter to extend the browser timeout setting. For correct behavior, set this value to be significantly larger than the session timeout value, for example, if the session timeout is 30 days, then set this configuration to 90 days.

define("TONIDOCLOUD_BROWSER_COOKIE_TIMEOUT", 86400); // time in seconds that browser remains logged in irrespective of whether browser is closed

Changing the Storage Quota for Users

> ⓘ 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.

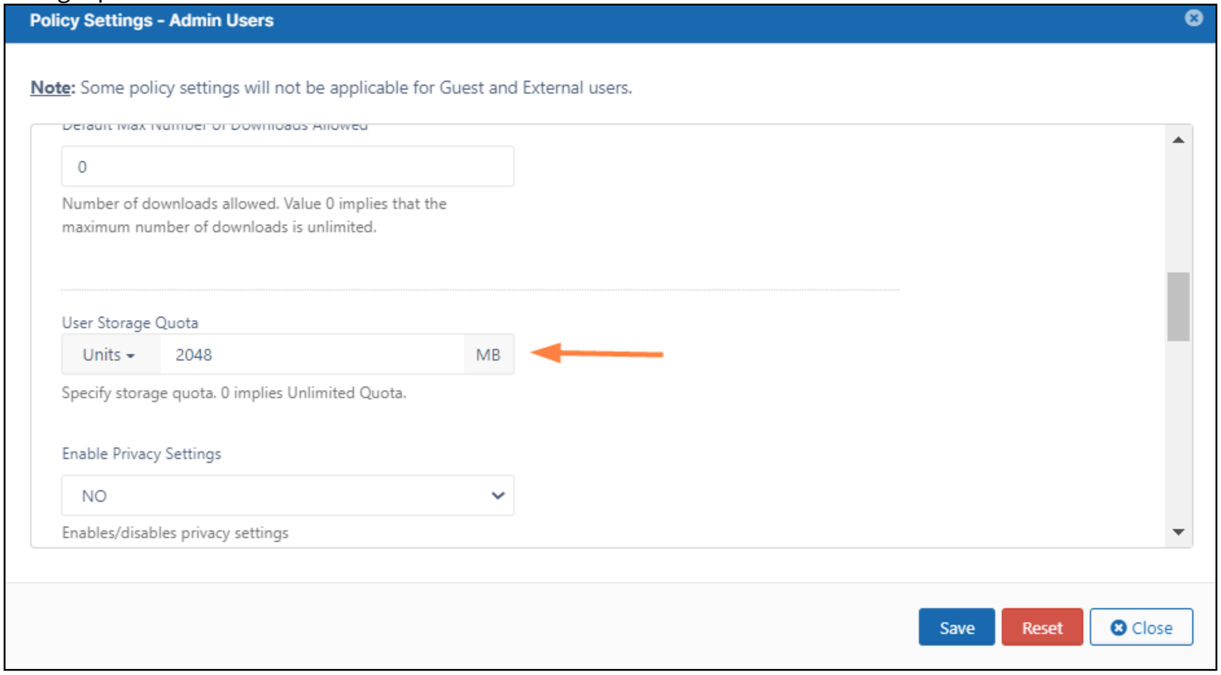
- Use the Global Default Policy to set a quota for all user accounts
- Use a custom policy to set a quota for a specific user or for a select group of users

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

0

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.

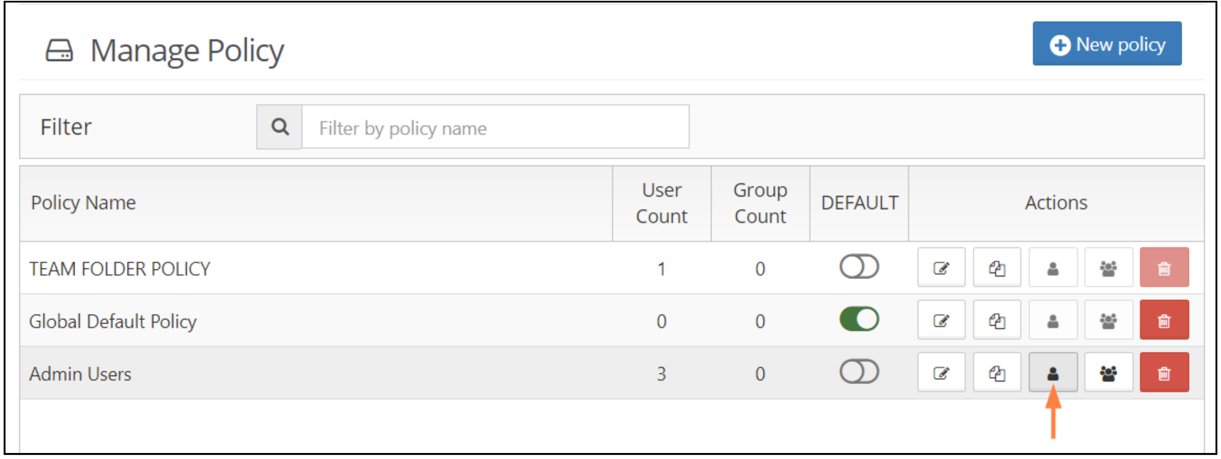
Enable Privacy Settings

NO

Enables/disables privacy settings

4. Click **Save**.

5. Click the user icon for the policy.



Manage Policy

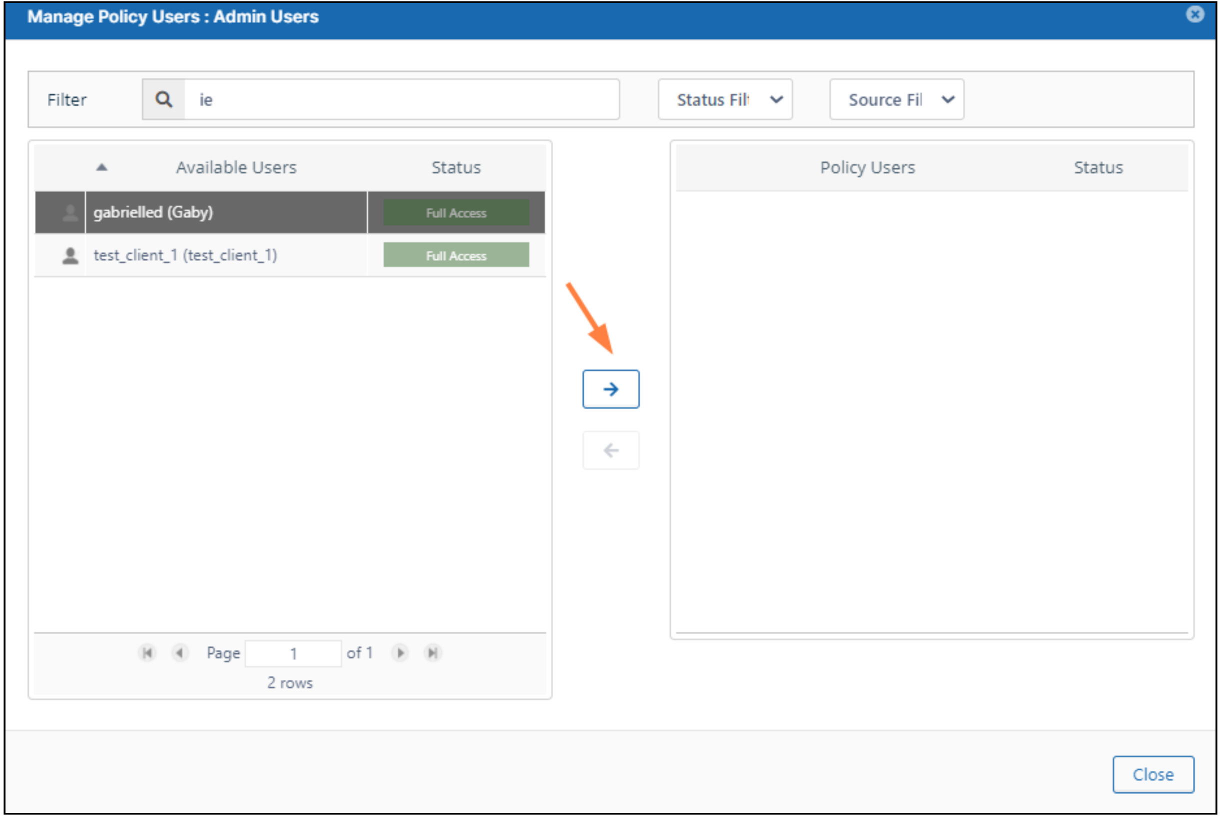
New policy

Filter | Filter by policy name

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.



Manage Policy Users : Admin Users

Filter | ie | Status Fil | Source Fil

Available Users	Status
gabrielled (Gaby)	Full Access
test_client_1 (test_client_1)	Full Access

Page 1 of 1

2 rows

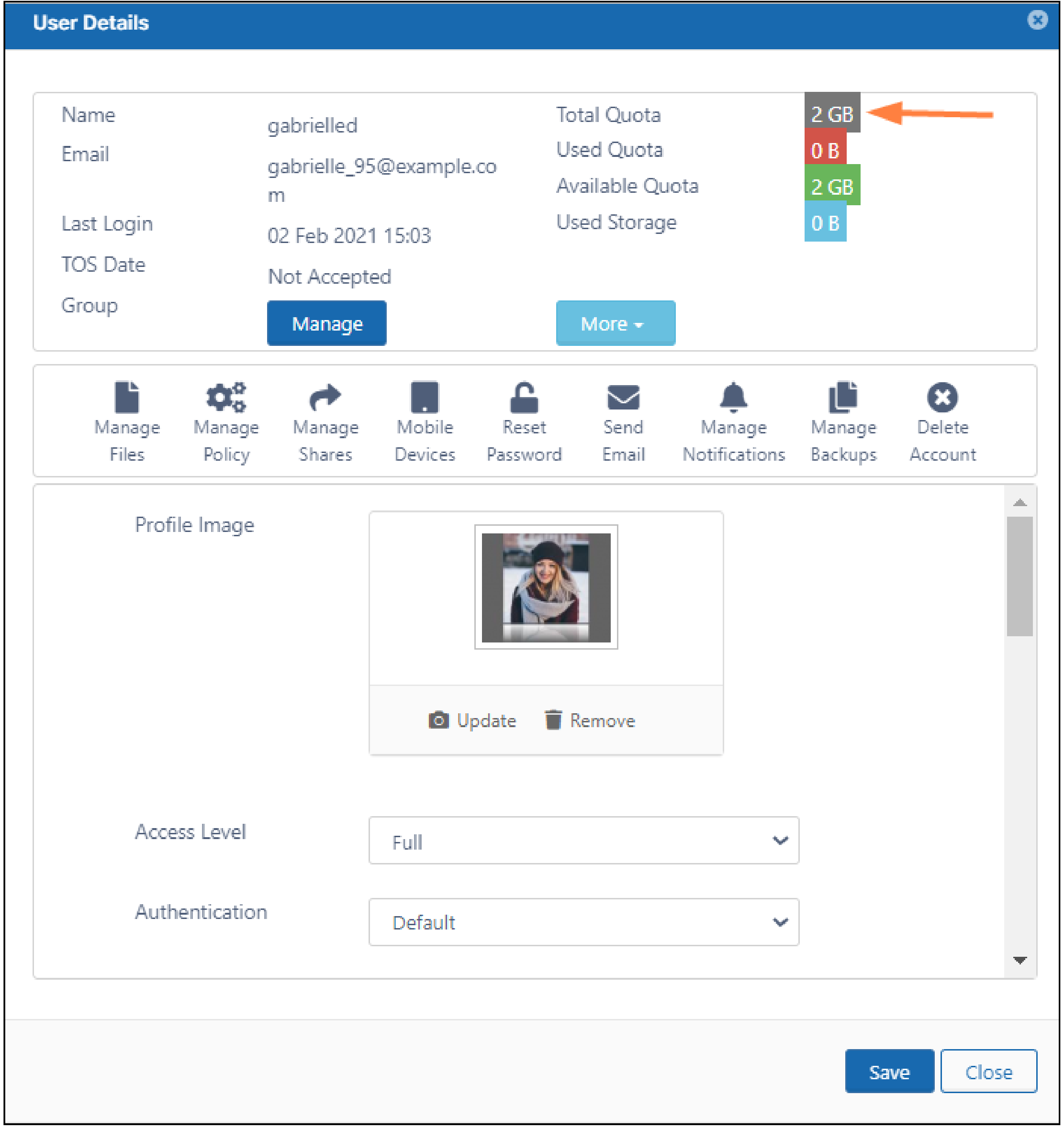
Policy Users	Status

Close

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:



User Details

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	More	

Access Level: Full

Authentication: Default

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.

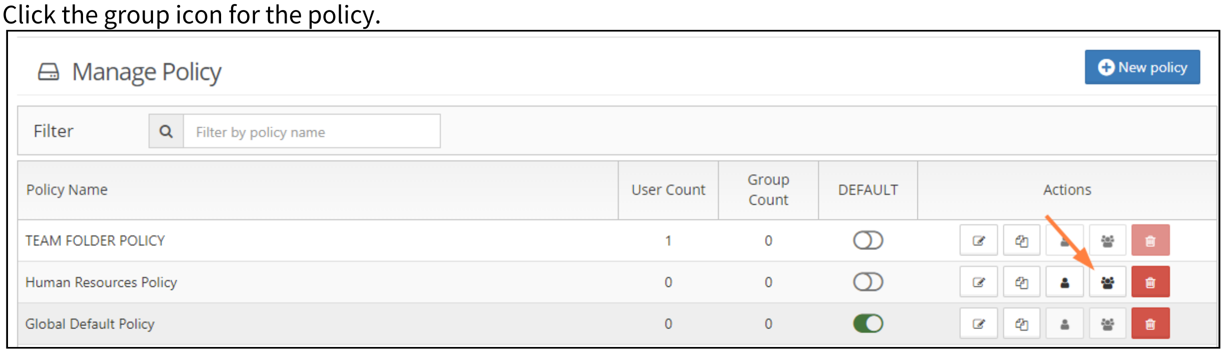
Create a Custom Policy to set the quota for a group of users

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.



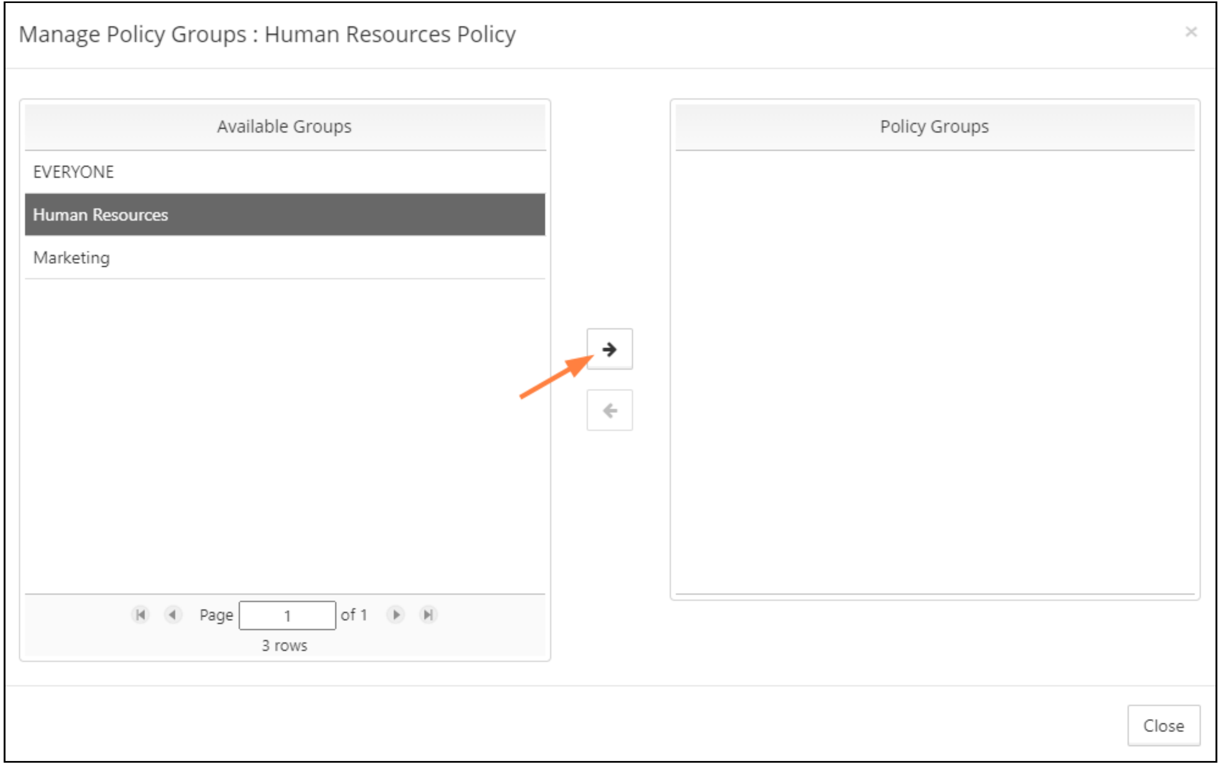
Manage Policy

Filter: Filter by policy name

Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	○	
Human Resources Policy	0	0	○	
Global Default Policy	0	0	●	

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

Page 1 of 1

3 rows

Policy Groups

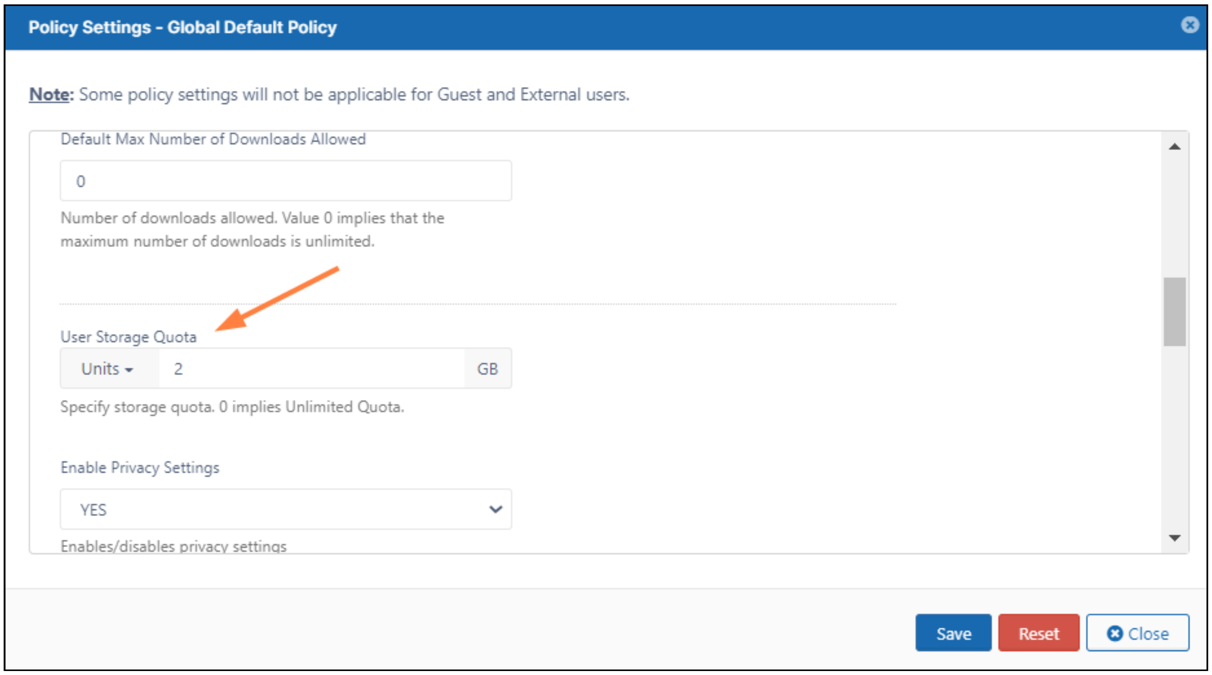
The new policy automatically becomes the group's effective policy.

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

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.

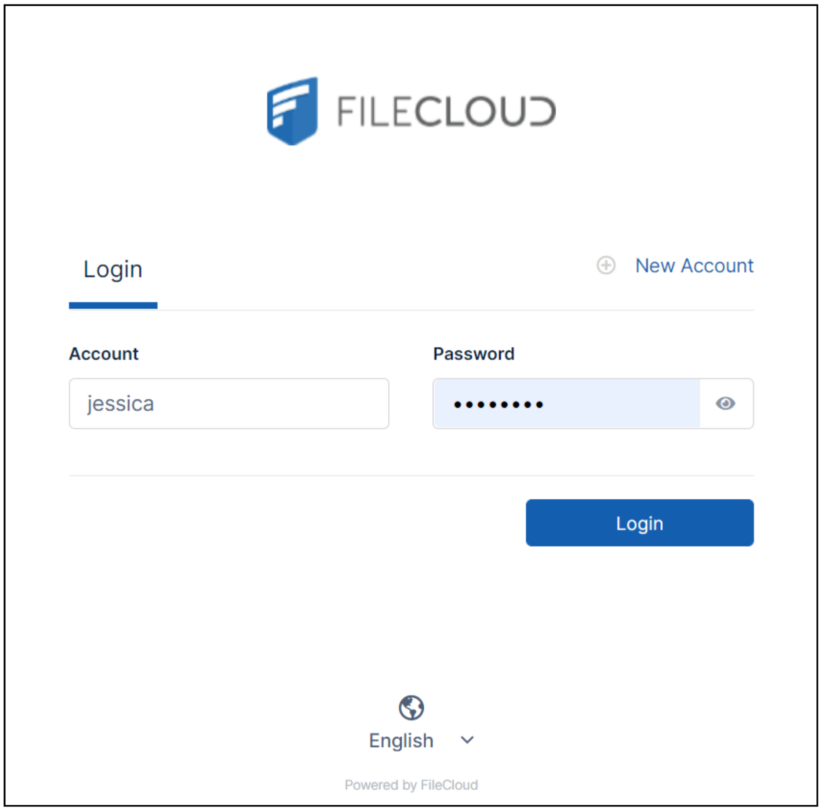
Currently, you may enable or disable WebDAV in your configuration file. For help, please Contact FileCloud Support.

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.

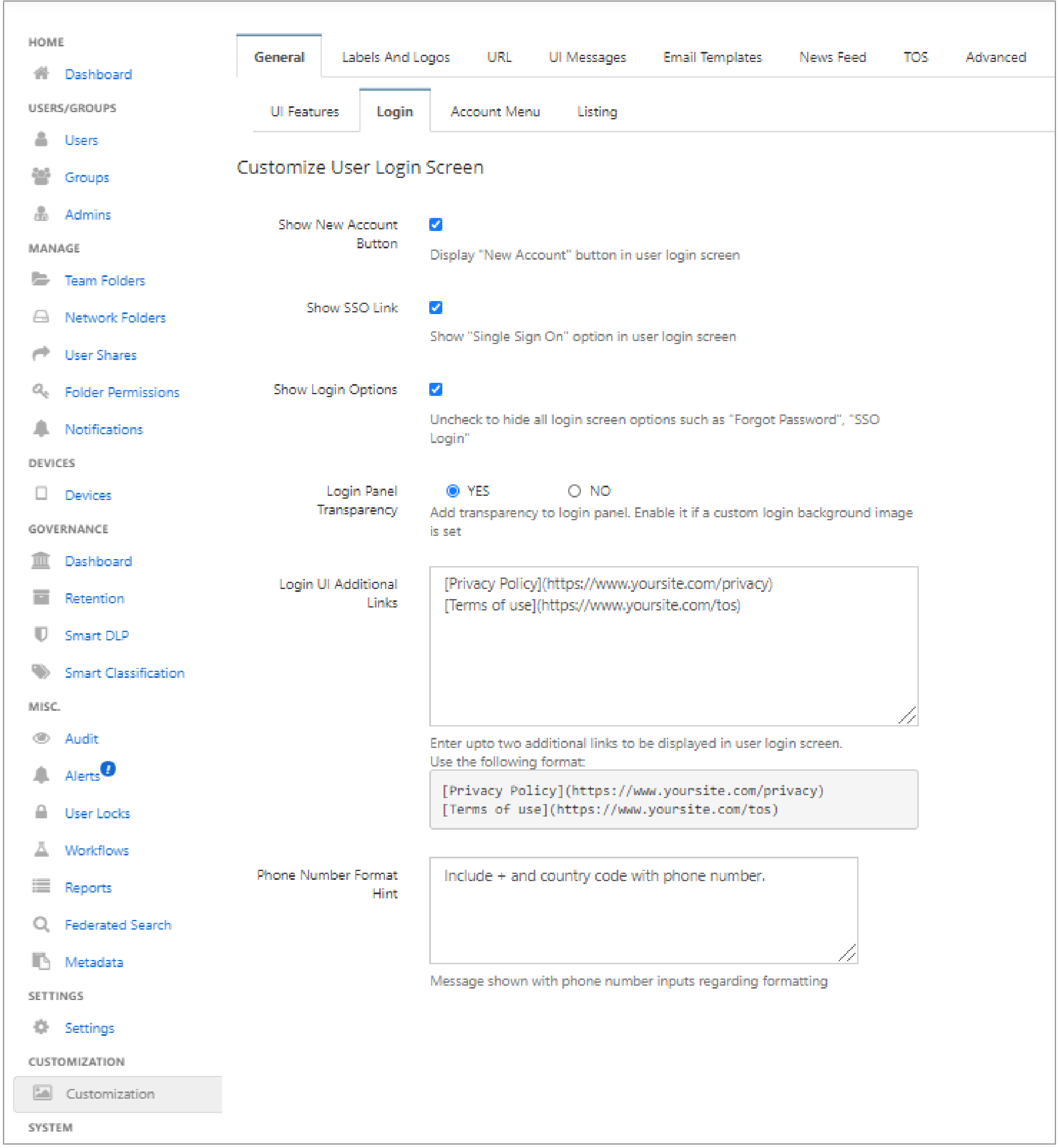


To customize the User Login screen

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

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

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



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

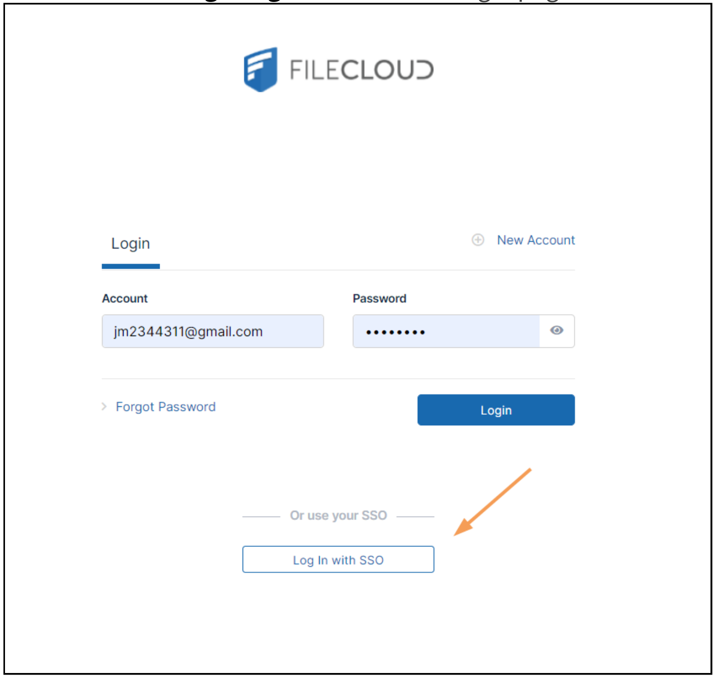
Login UI Additional Links
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/tos)

Enter upto two additional links to be displayed in user login screen.
Use the following format:

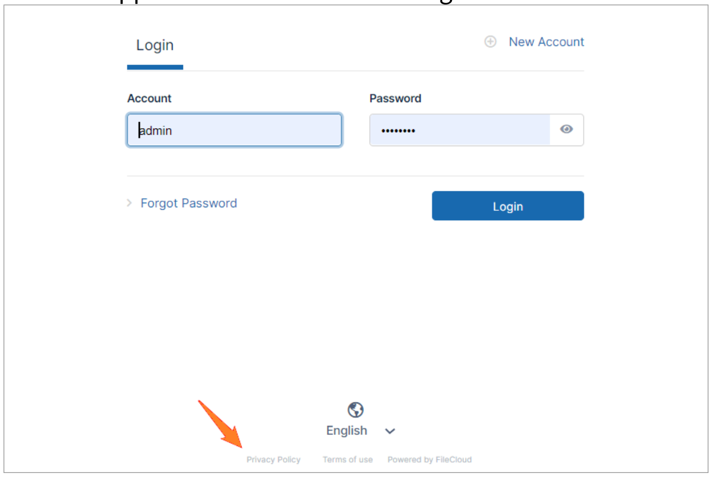
```
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/tos)
```

Phone Number Format Hint
Include + and country code with phone number.

Message shown with phone number inputs regarding formatting

Option	Description
Show New Account Button	Displays **New Account** button in user log-in screen. Enabled by default. The **New Account** button allows a user to create a new account for themselves, and depending on the configuration of Automatic Account Approval, have it automatically approved.
Show SSO Link	Check to show **Single Sign On** link in the login page:  FILECLOUD Login New Account Forgot Password Login Or use your SSO Log In with SSO Account: jm2344311@gmail.com Password: •••••••• **Note**: If this is checked, but **Show Login Options** is unchecked, **Single Sign On** link is not shown. 💡 The functionality of this button is determined by how you configure Single Sign-On Access
Show Login Options	Uncheck to hide options in login screen such as **Forgot Password** and **Single Sign On** link even if **Show SSO Link** is checked.
Login Panel Transparency	Adds transparency to login panel. Set to: • YES (default) • NO 💡 Enable this option if you are using a custom login background image.

Option	Description

Login UI Additional Links	Enter up to two additional links to be displayed in user login screen.
	Use the format:
	`[Privacy Policy](https://www.yoursite.com/privacy)`
	`[Terms of use](https://www.yoursite.com/tos)`
	The links appear at the bottom of the login screen:
	
	 Login
	New Account
	Account
	Password
	Forgot Password
	Login
	English
	Privacy Policy
	Terms of use
	Powered by FileCloud
	admin
	••••••••

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

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

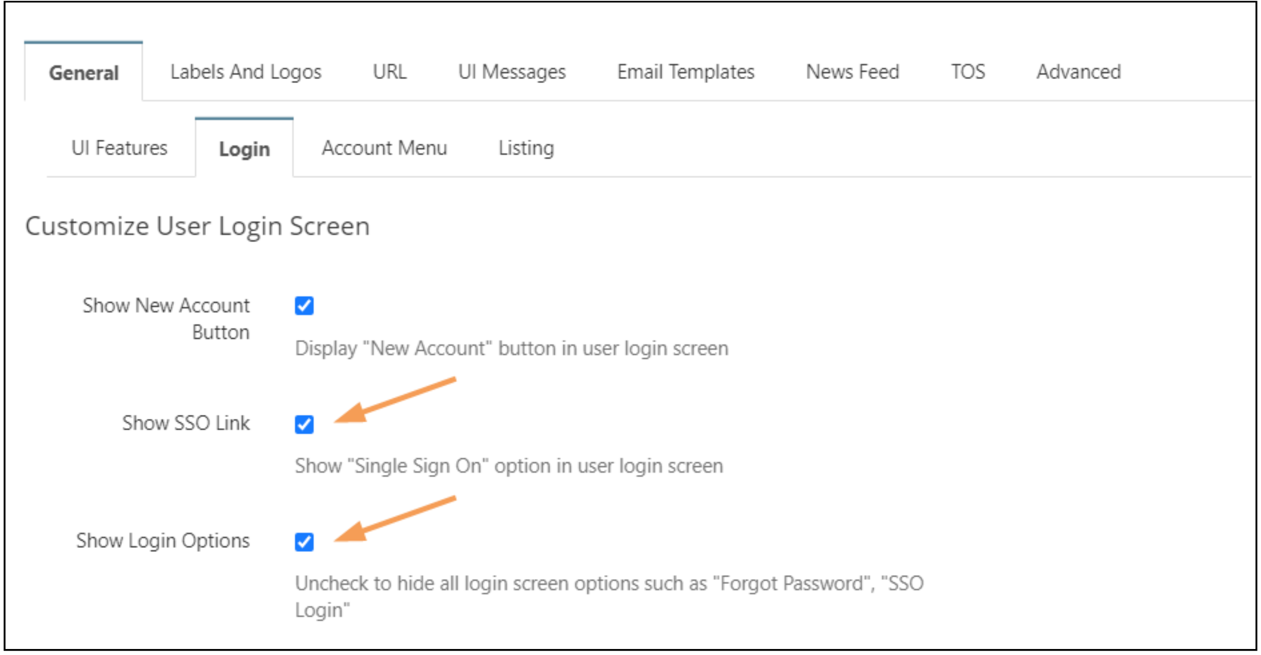
To customize for SSO log in

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



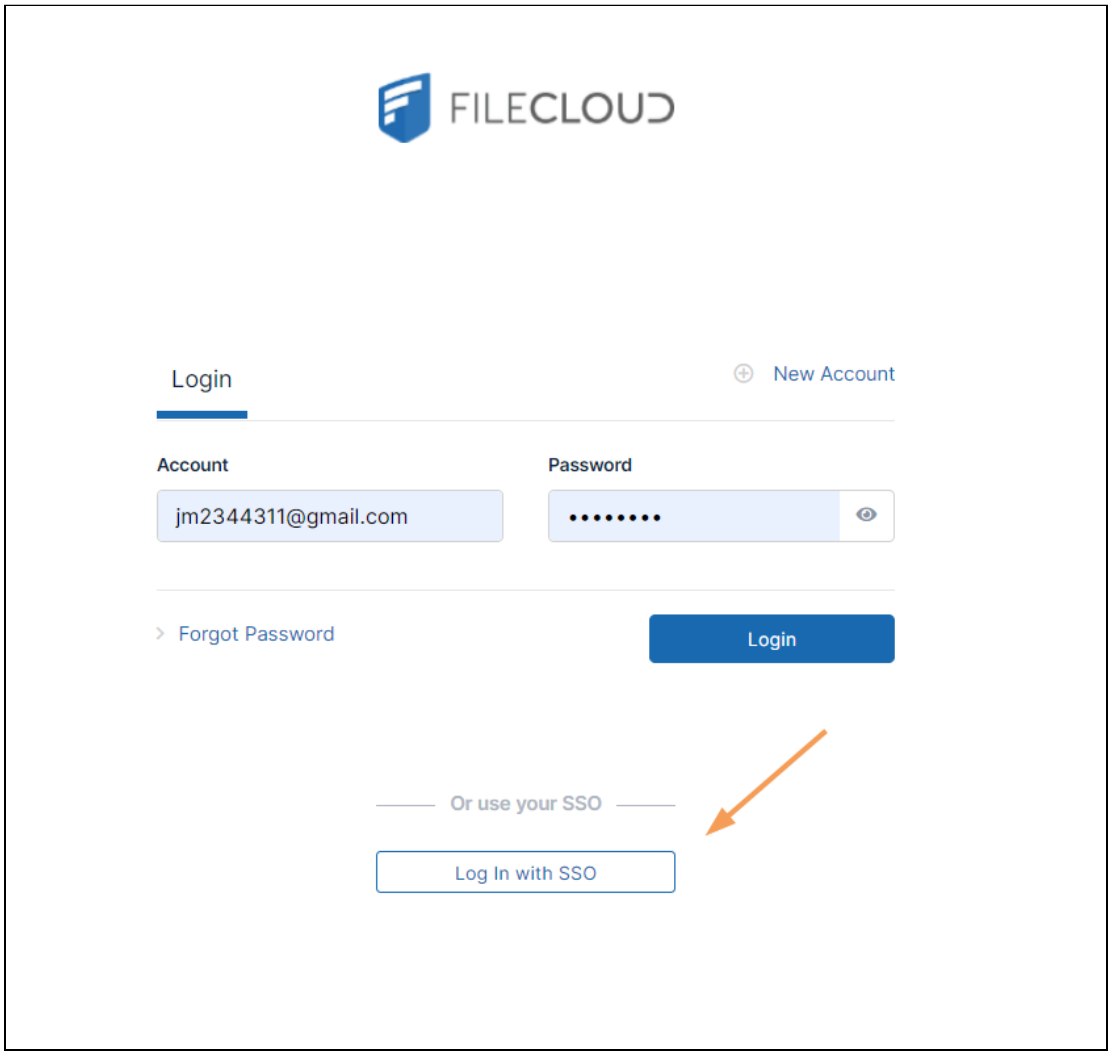
Customize User Login Screen

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"

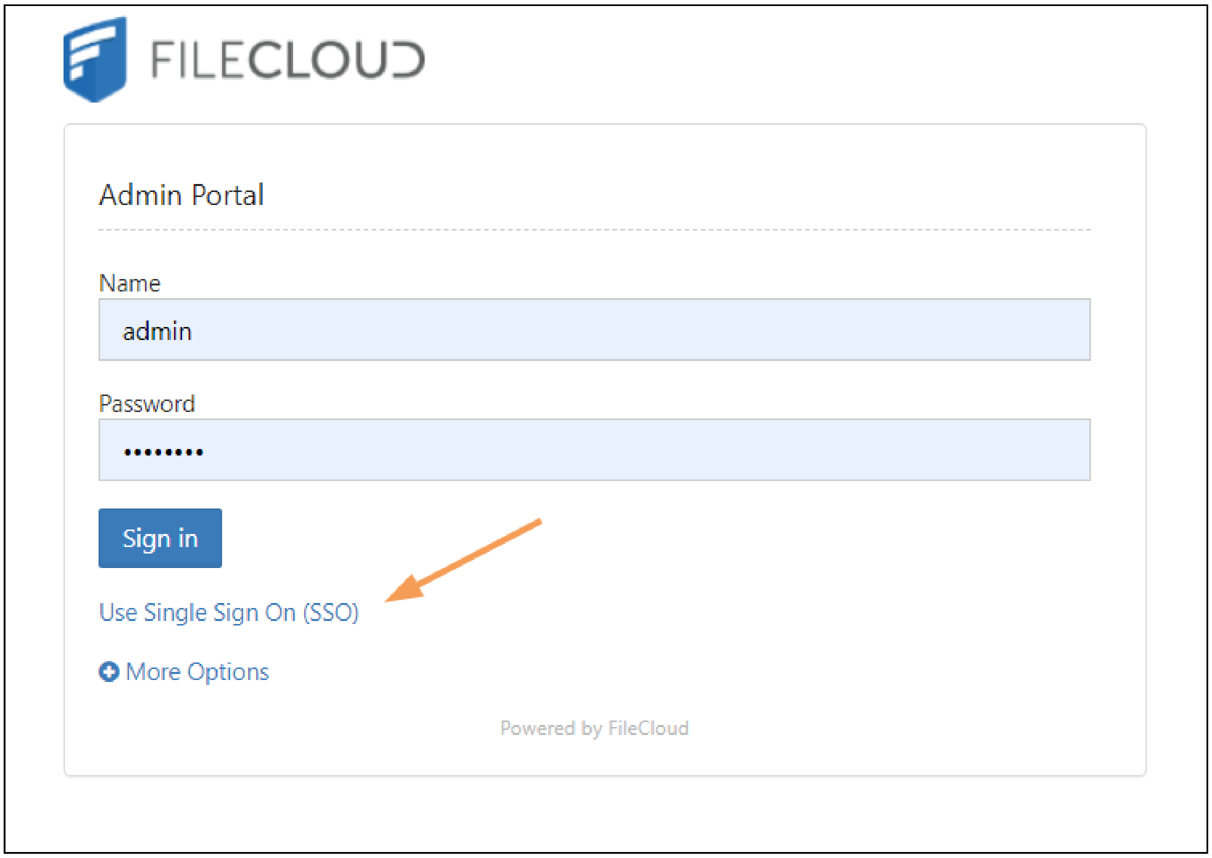
4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



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

The SSO log-in option in the admin portal:

Starting with FileCloud 13.0, FileCloud admin interface also supports Single Sign-On.



Default admin portal log-in screen

To only display the SSO log-in option:

In order to skip the FileCloud login page and send the user directly to the SAML SSO page you must add a setting to the cloudconfig.php file, as shown below. You can configure this option for the user portal login page and the admin portal login page.

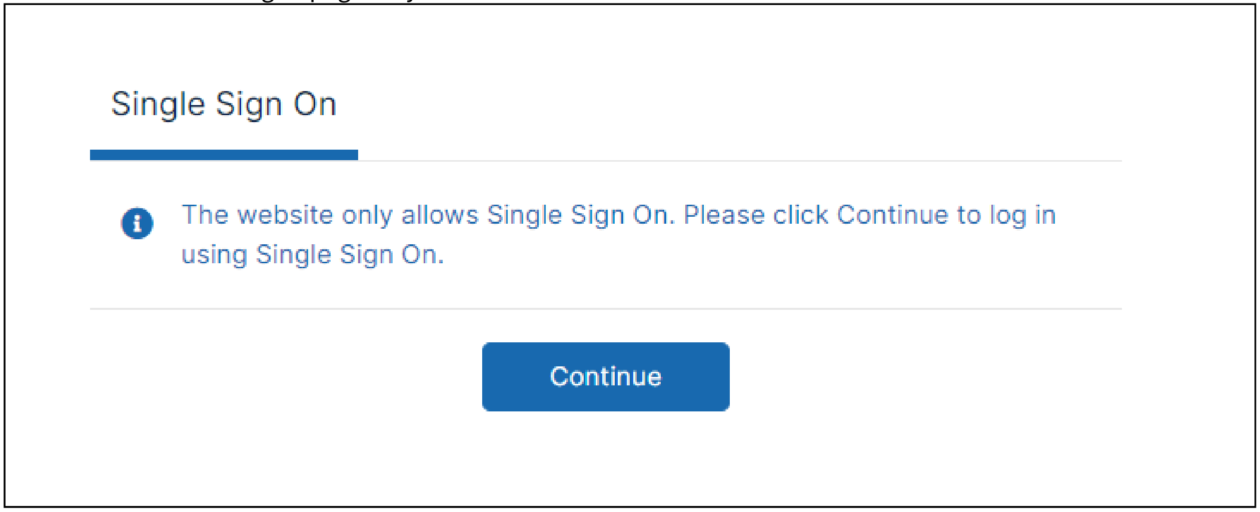
To only display the SSO log-in option in the user portal:
This configuration option is available starting with FileCloud Version 19.3, It supports skipping the login page when the user accesses FileCloud with a domain name or with a full URL.

1. In the admin portal, go to **Customization,** and select the **General** tab, and then the **Login** sub-tab.
2. Check **Show SSO Link** and **Show Login Options**, and save your changes.
3. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
4. To only display the SSO log-in option:

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

> An earlier version of this option is also effective in version of FileCloud prior to 19.3, but this redirect is only effective if the user specifies a domain name rather than a full URL. Instead of the above setting, use:
>
> ```
> define("TONIDOCLOUD_SSO_DIRECT", "1");
> ```

When users enter the log-in page they will see:



Single Sign On

The website only allows Single Sign On. Please click Continue to log in using Single Sign On.

To return to displaying other log-in options:

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

To display only SSO log-in in the admin portal:

Starting with Version 20.1, FileCloud supports skipping the login page when the admin accesses FileCloud with a domain name or with a full URL.

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To only display the SSO log-in option:

Enter:

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

An earlier version of this option is also effective in versions of FileCloud prior to 20.1, but this redirect is only effective if the user specifies a domain name rather than a full URL. Instead of the above setting, use:

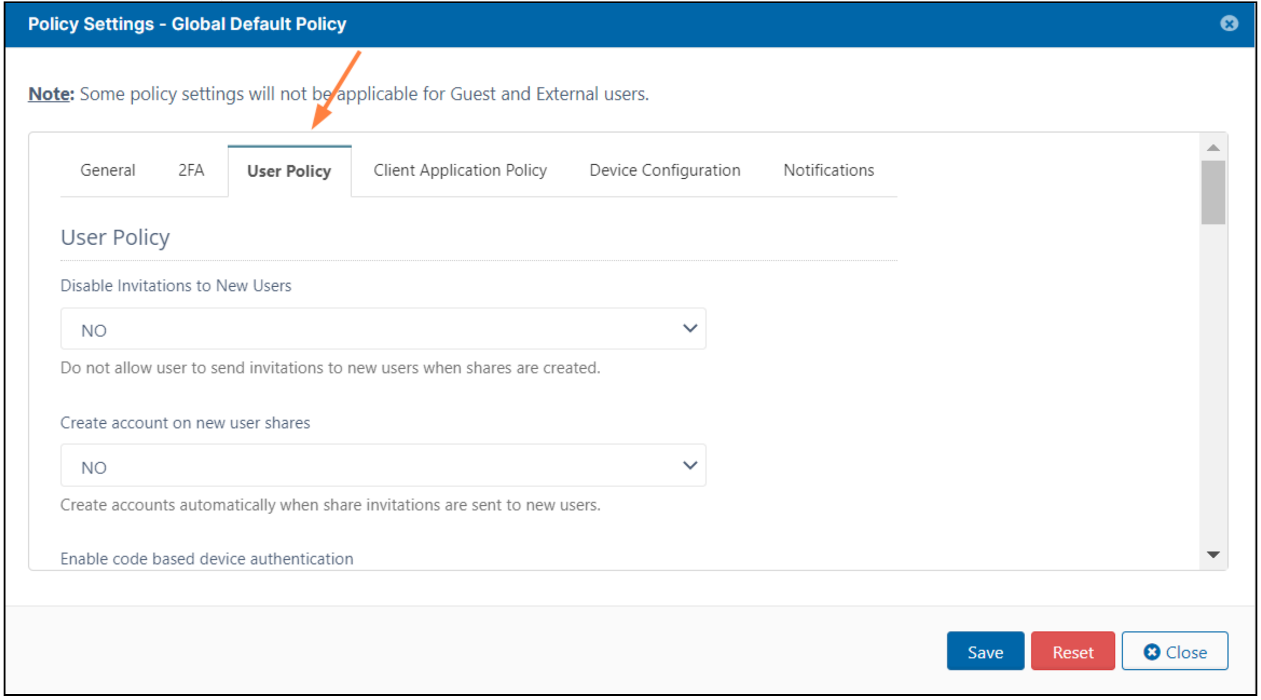
```
define("TONIDOCLOUD_SSO_DIRECT_ADMIN", "1");
```

Limiting File Upload Size for Users

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

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

1. In the 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.

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

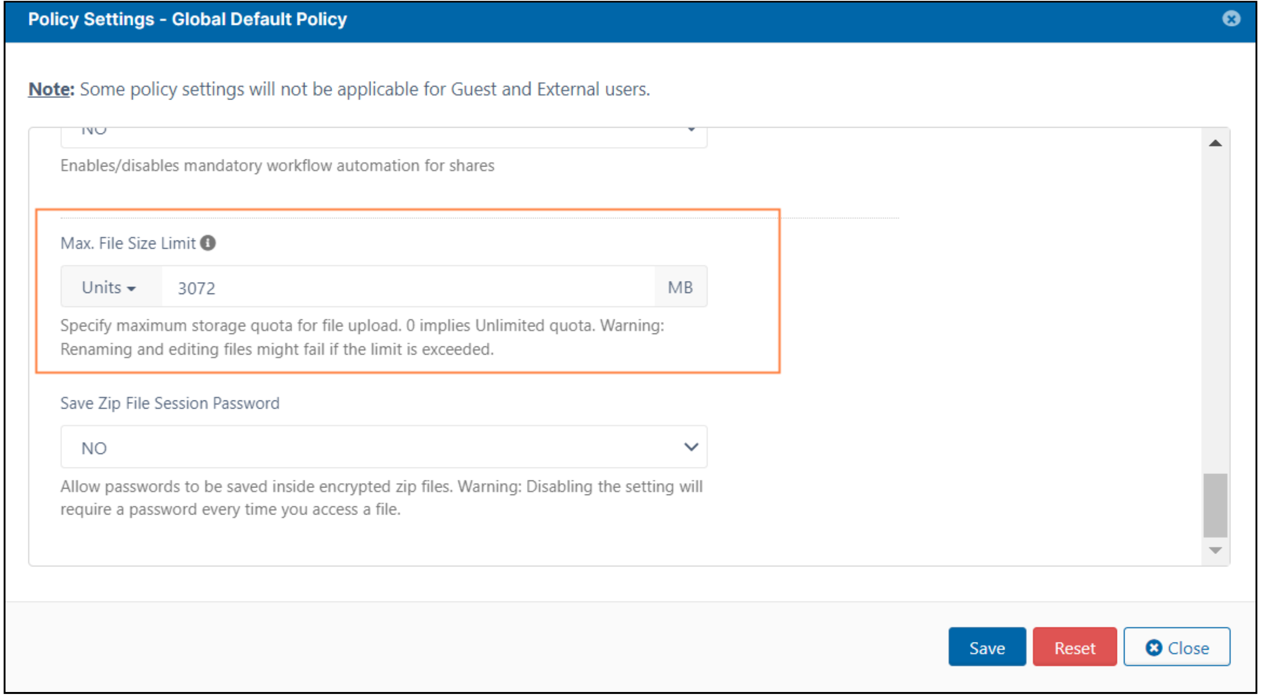
NO

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

Enable code based device authentication

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.

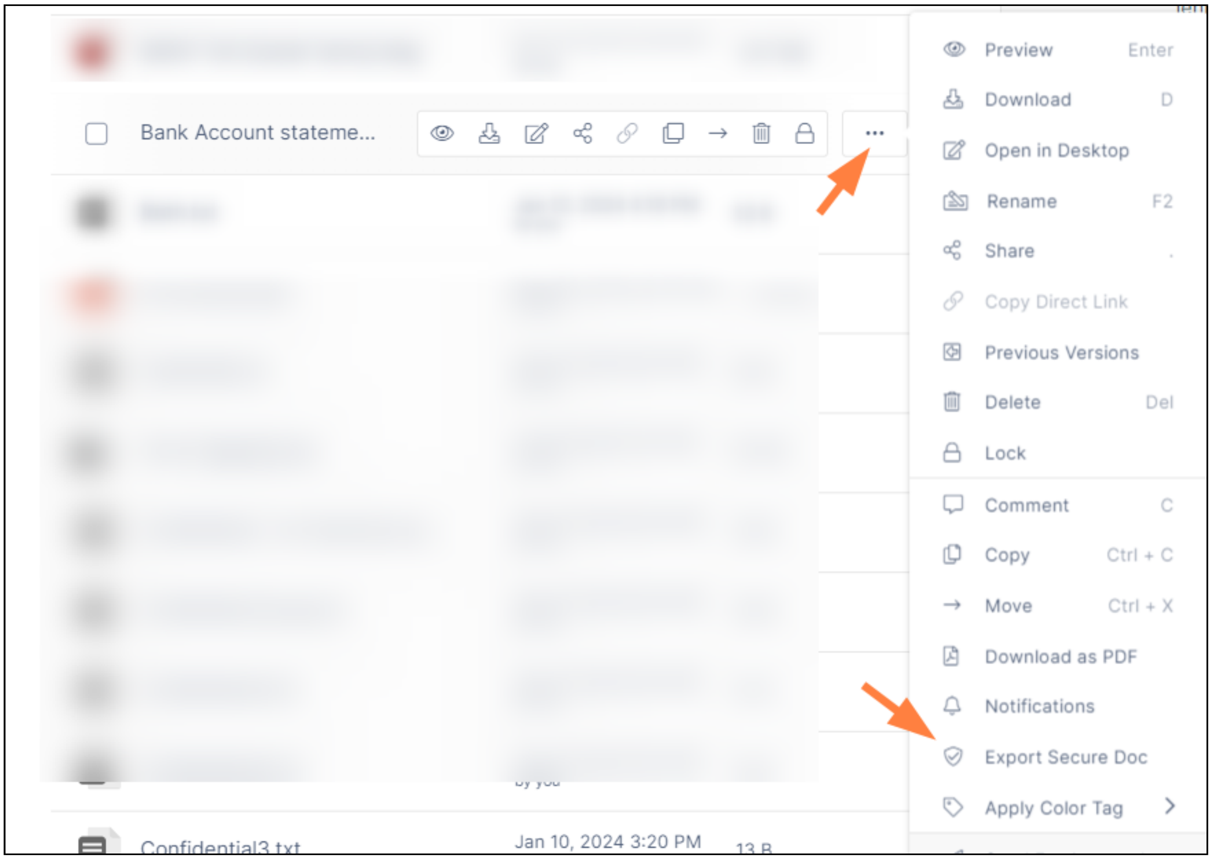
5. Click **Save**.

> **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.

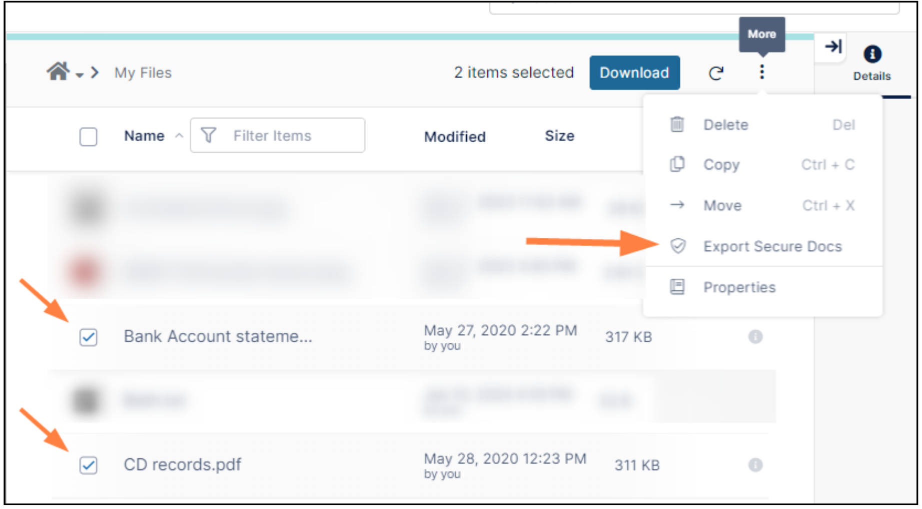
Remove the Export Secure Doc Option

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 setting network share access and 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

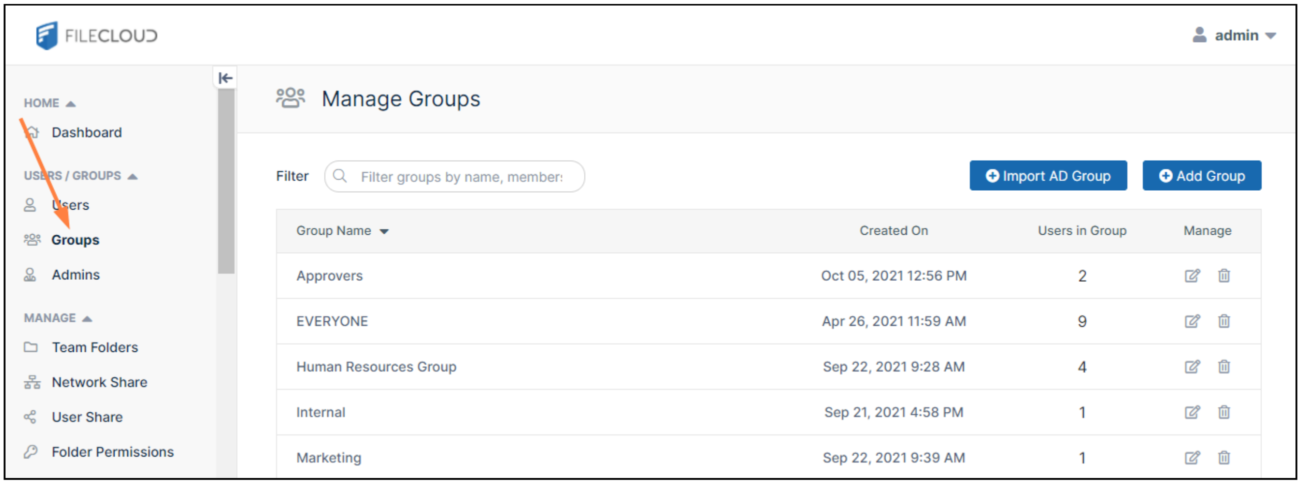
- **Group Name** - Name assigned by the Administrator
- **Group Members** - List of users that are part of the group
- **Group Admins** - (optional) Users with the ability to view users, add users, and/or remove users from the group.
- **Group Policy** - The policy that applies to all members of the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



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

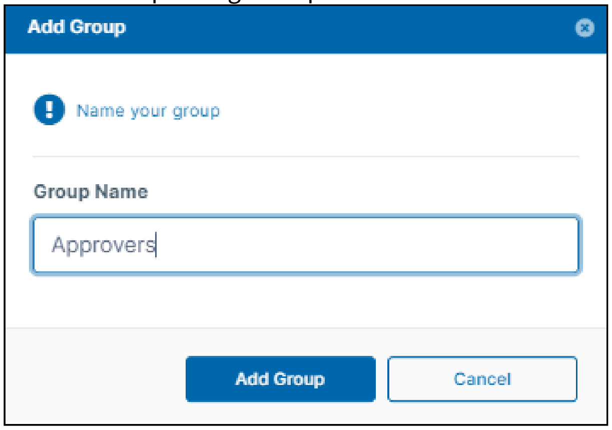
The **Everyone** group is included by FileCloud. It contains all Full and Guest users.

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.



Group Name: Approvers

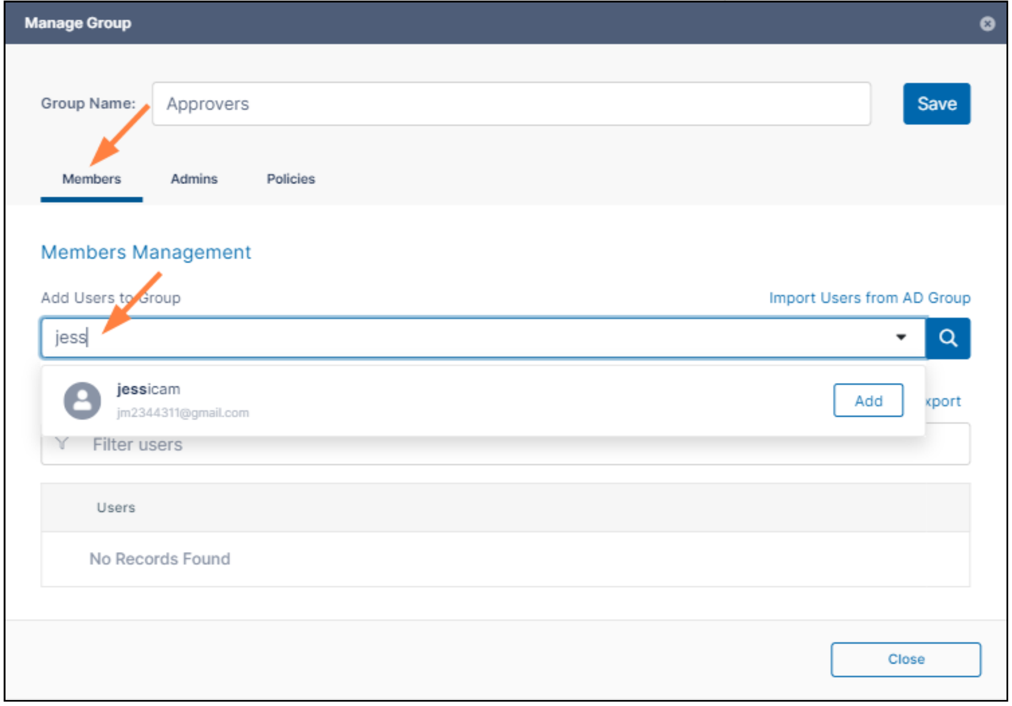
4. Click **Add Group**.
5. The group is added, and the **Manage Group** dialog box opens.

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**.



Group Name: Approvers

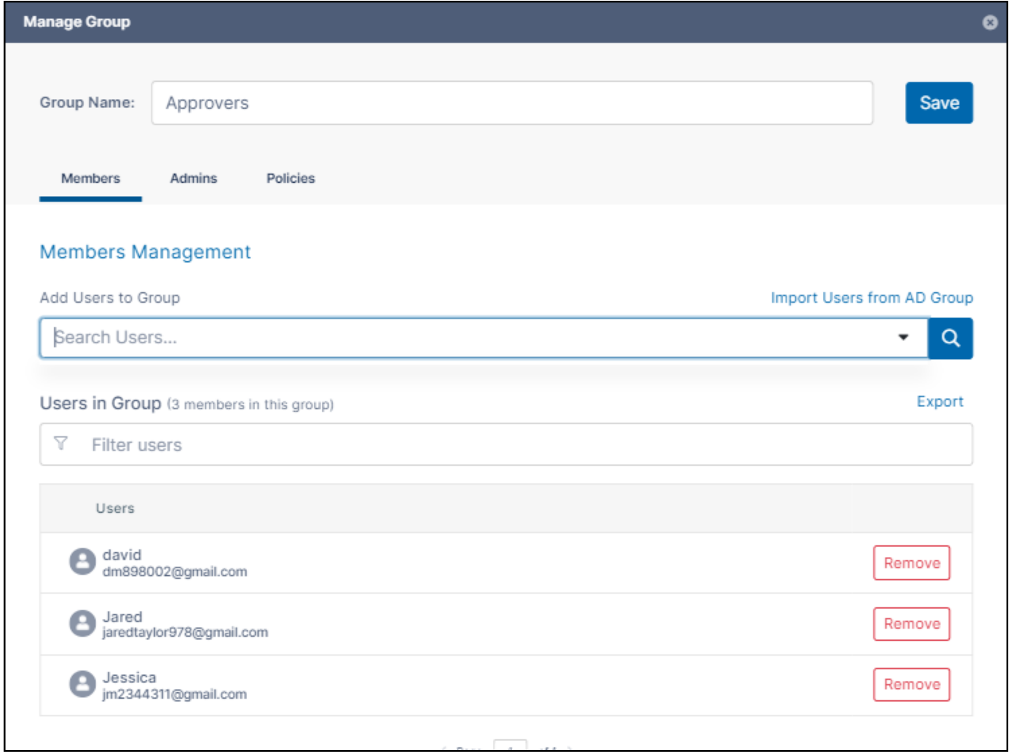
Add Users to Group: jess

jessicam
jm2344311@gmail.com

No Records Found

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

5. Add any number of users.



Manage Group

Group Name: Approvers

Members Management

Add Users to Group

Users in Group (3 members in this group)

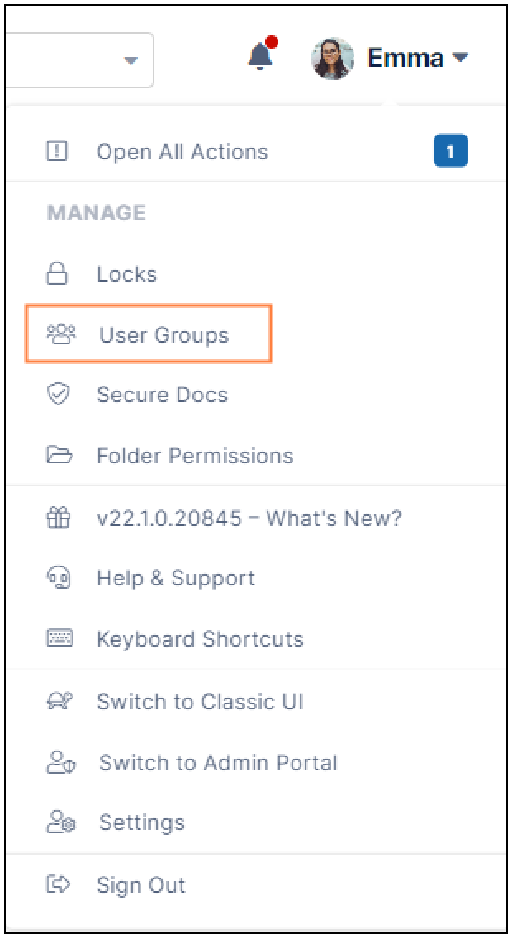
Users	
david dm898002@gmail.com	Remove
Jared jaredtaylor978@gmail.com	Remove
Jessica jm2344311@gmail.com	Remove

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

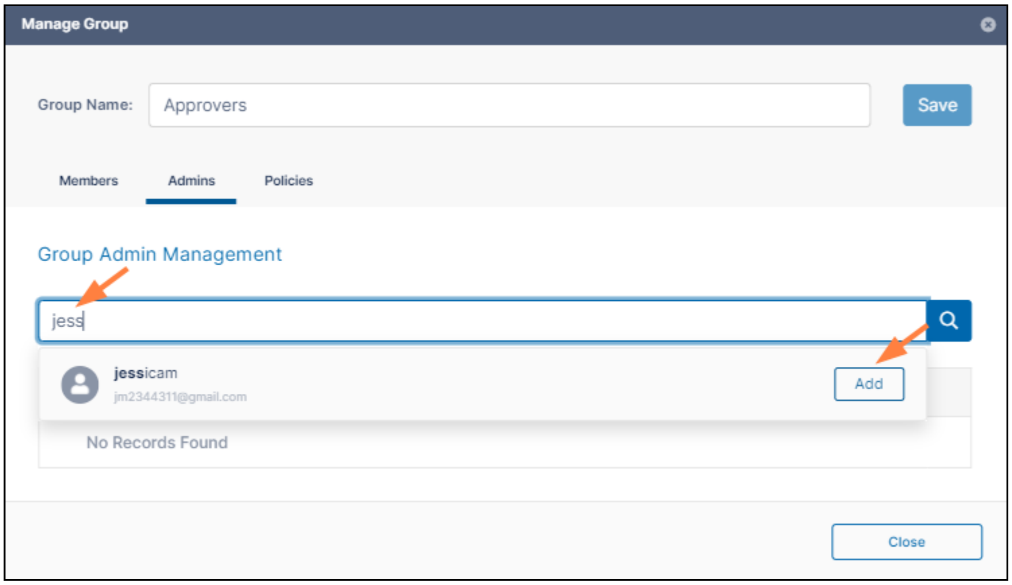
You can assign users to be admins of a group and give each group admin access to view, add, and/or remove users from the group.

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.



Group Name: Approvers

Save

Group Admin Management

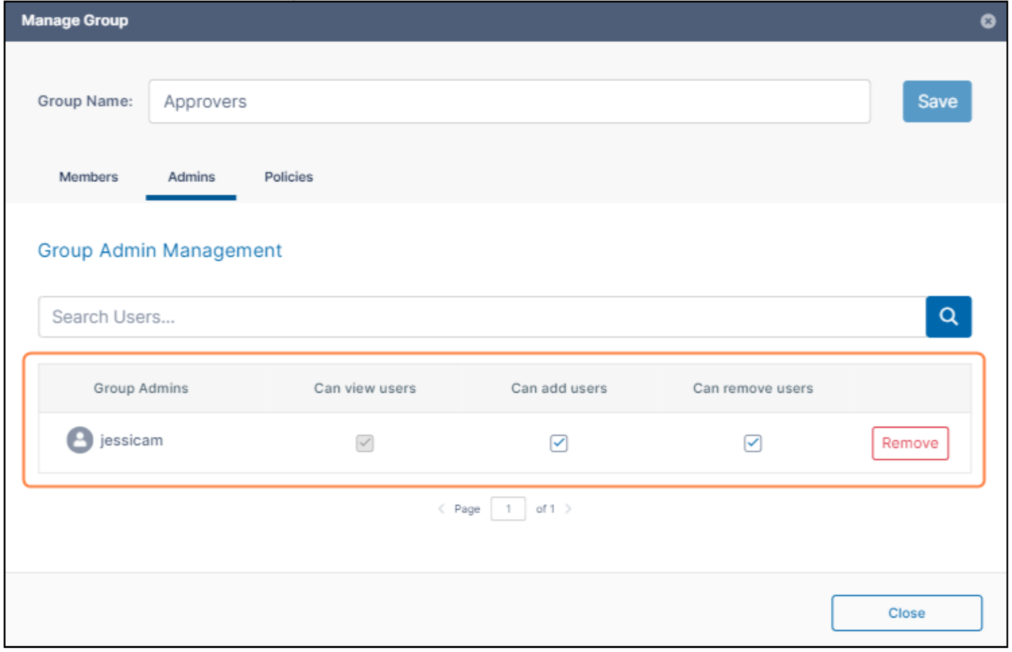
jess

jessicam
jm2344311@gmail.com

No Records Found

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.



Group Name: Approvers

Save

Group Admin Management

Search Users...

Group Admins	Can view users	Can add users	Can remove users	
jessicam	☑	☑	☑	Remove

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.

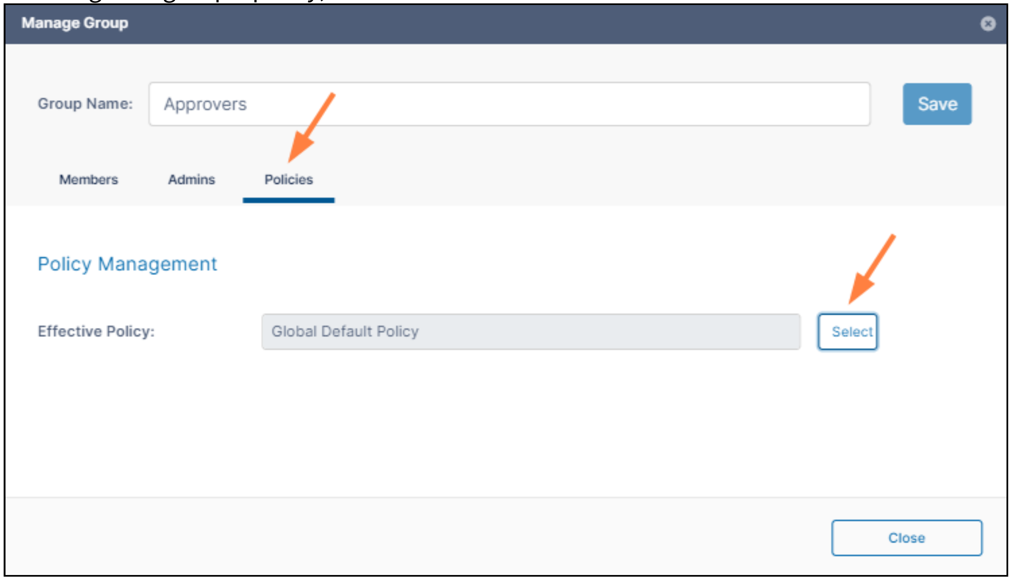
Change a Group's Policy

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

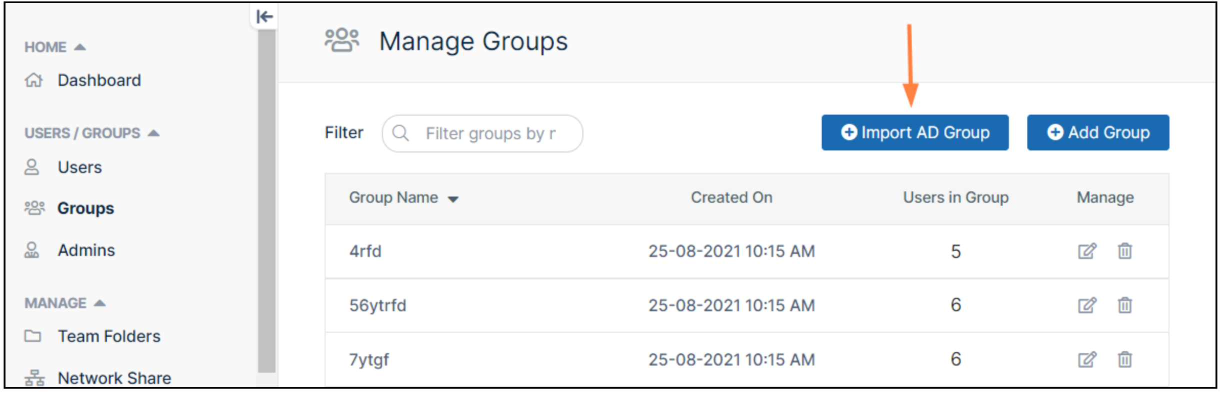
You can also import an existing AD group from an Active Directory Server connected to FileCloud.

> ⓘ 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.

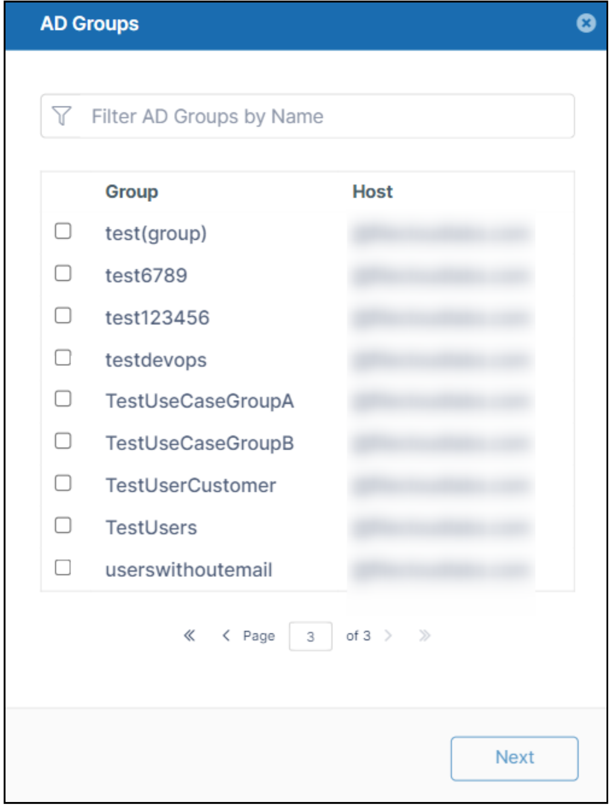
To add AD users to a FileCloud group:

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.



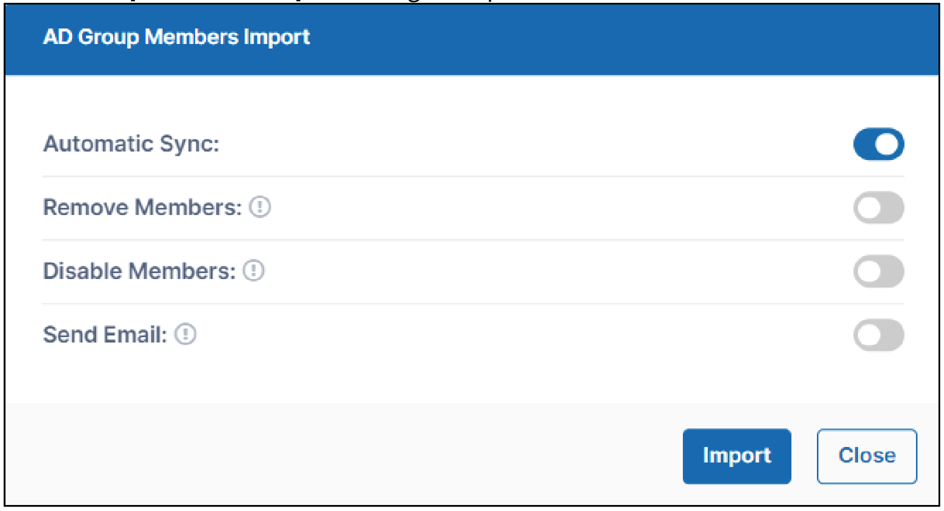
Group Name	Created On	Users in Group	Manage
4rfd	25-08-2021 10:15 AM	5	
56ytrfd	25-08-2021 10:15 AM	6	
7ytgf	25-08-2021 10:15 AM	6	

An **AD Groups** dialog box opens:



	Group	Host
☐	test(group)	[redacted]
☐	test6789	[redacted]
☐	test123456	[redacted]
☐	testdevops	[redacted]
☐	TestUseCaseGroupA	[redacted]
☐	TestUseCaseGroupB	[redacted]
☐	TestUserCustomer	[redacted]
☐	TestUsers	[redacted]
☐	userswithoutemail	[redacted]

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



AD Group Members Import

Automatic Sync: ●

Remove Members: ○

Disable Members: ○

Send Email: ○

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

To change the automatic sync interval:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the following line.
   Set the value to the interval in hours to sync FileCloud groups with AD groups. The minimum is 1.

```
define("TONIDOCLOUD_ADGROUPSYNC_INTVL", 2);
```

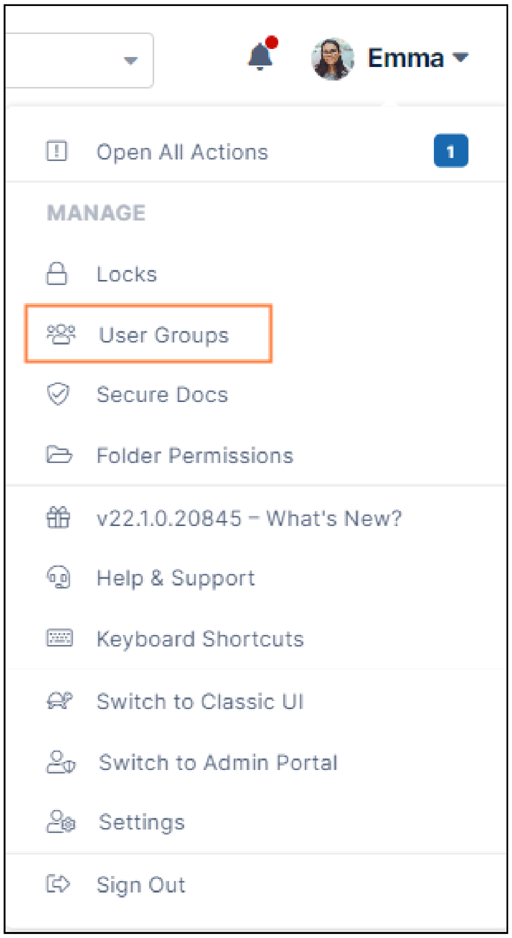
3. Restart the FileCloud message queue.

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:

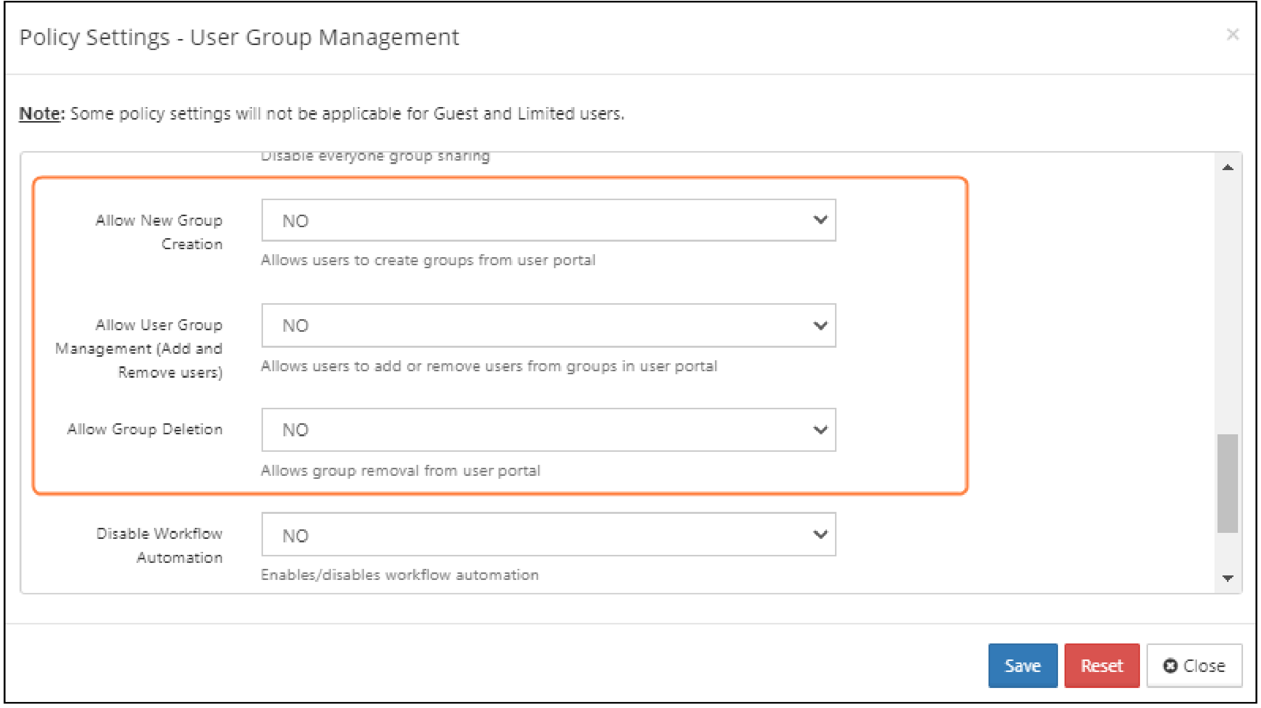


For more information on user management of groups, see User Groups.

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 sharing

Allow New Group Creation: NO
Allows users to create groups from user portal

Allow User Group Management (Add and Remove users): NO
Allows users to add or remove users from groups in user portal

Allow Group Deletion: NO
Allows group removal from user portal

Disable Workflow Automation: NO
Enables/disables workflow automation

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.

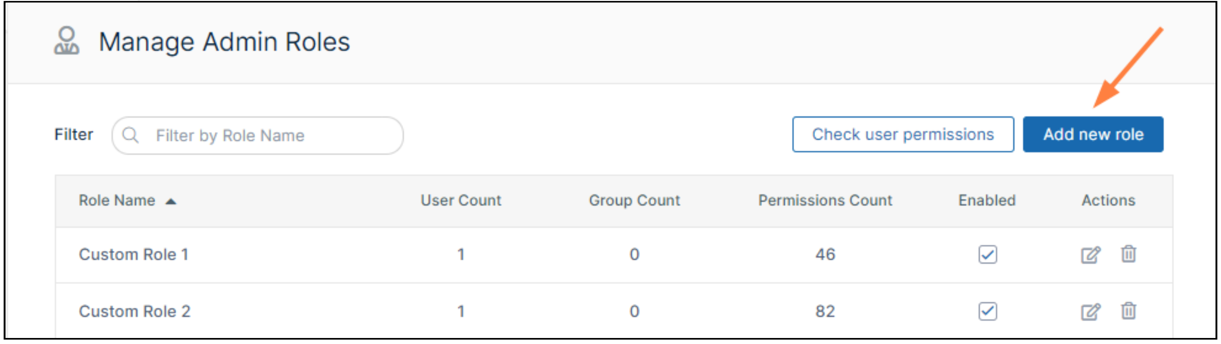
Admin User. User accounts that can access the FileCloud admin interface.

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:

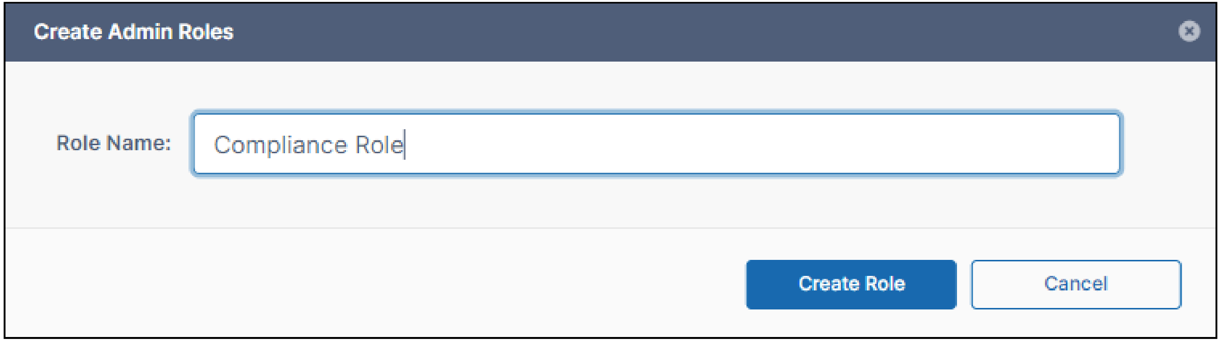
1. Click **Admins** in the navigation panel.
2. In the **Manage Admin Roles** screen, click **Add new role**.



Role Name ▲	User Count	Group Count	Permissions Count	Enabled	Actions
Custom Role 1	1	0	46	☑	✎ 🗑
Custom Role 2	1	0	82	☑	✎ 🗑

The **Create Admin Roles** dialog box opens.

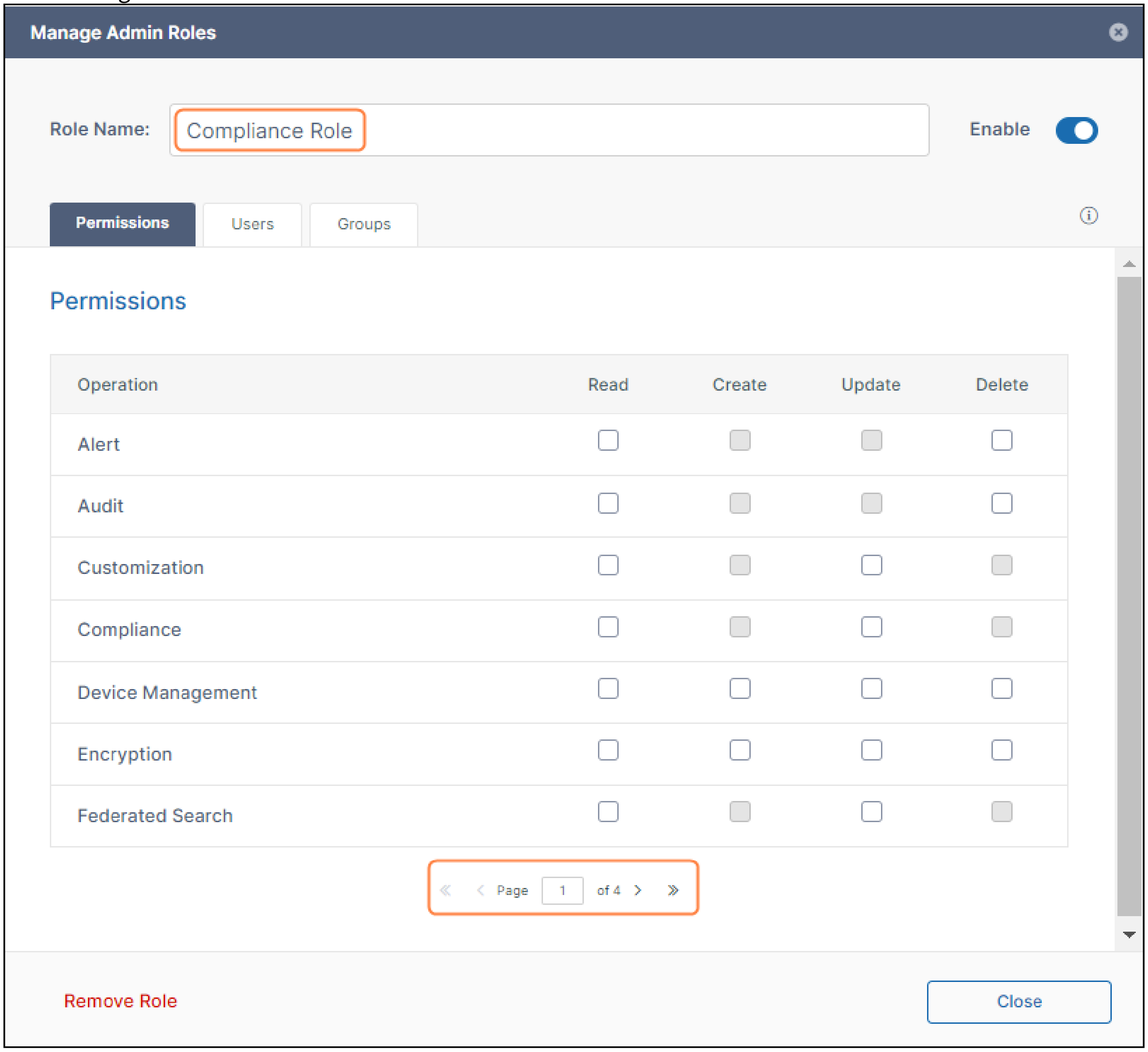
3. In **Role Name**, enter a name for the role.



Role Name: Compliance 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: Compliance Role

Enable

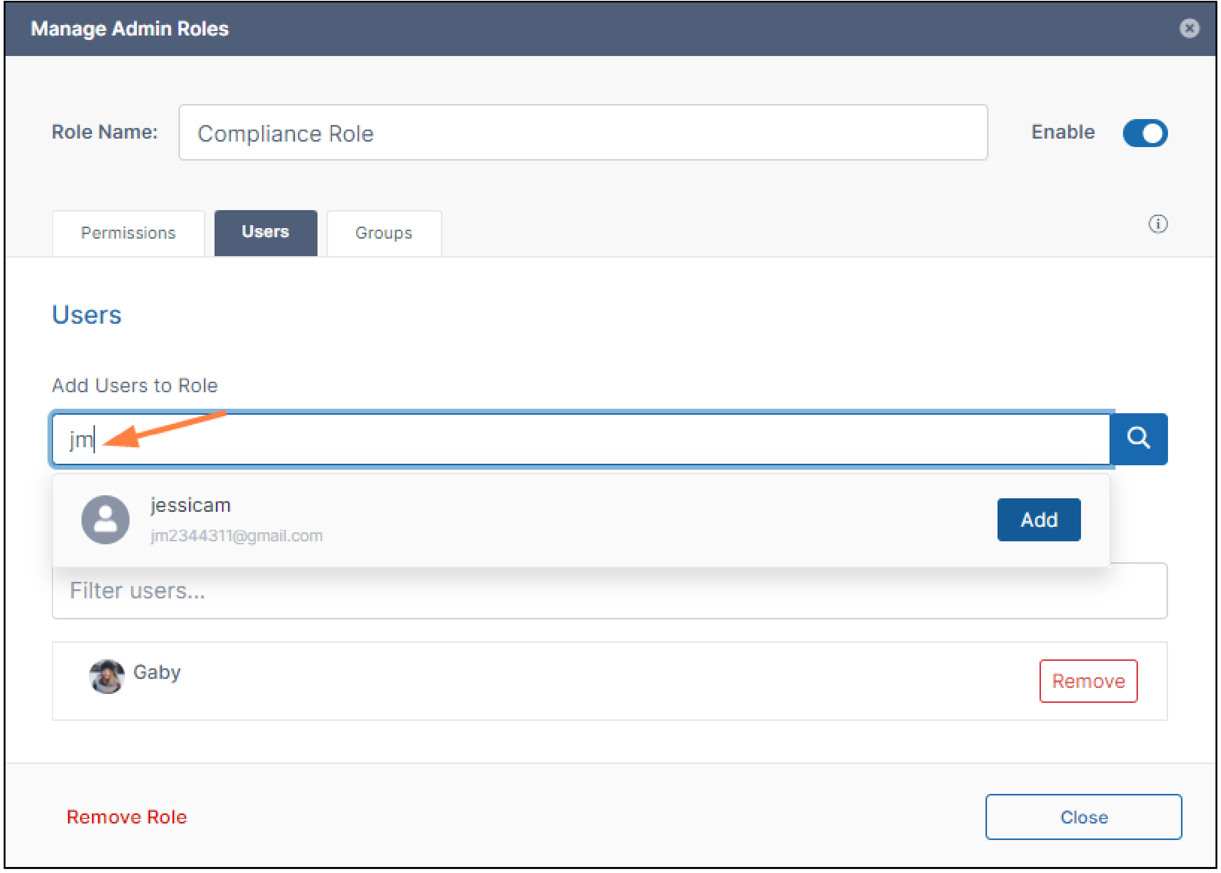
Permissions

Operation	Read	Create	Update	Delete
Alert	☐	☐	☐	☐
Audit	☐	☐	☐	☐
Customization	☐	☐	☐	☐
Compliance	☐	☐	☐	☐
Device Management	☐	☐	☐	☐
Encryption	☐	☐	☐	☐
Federated Search	☐	☐	☐	☐

Page 1 of 4

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

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



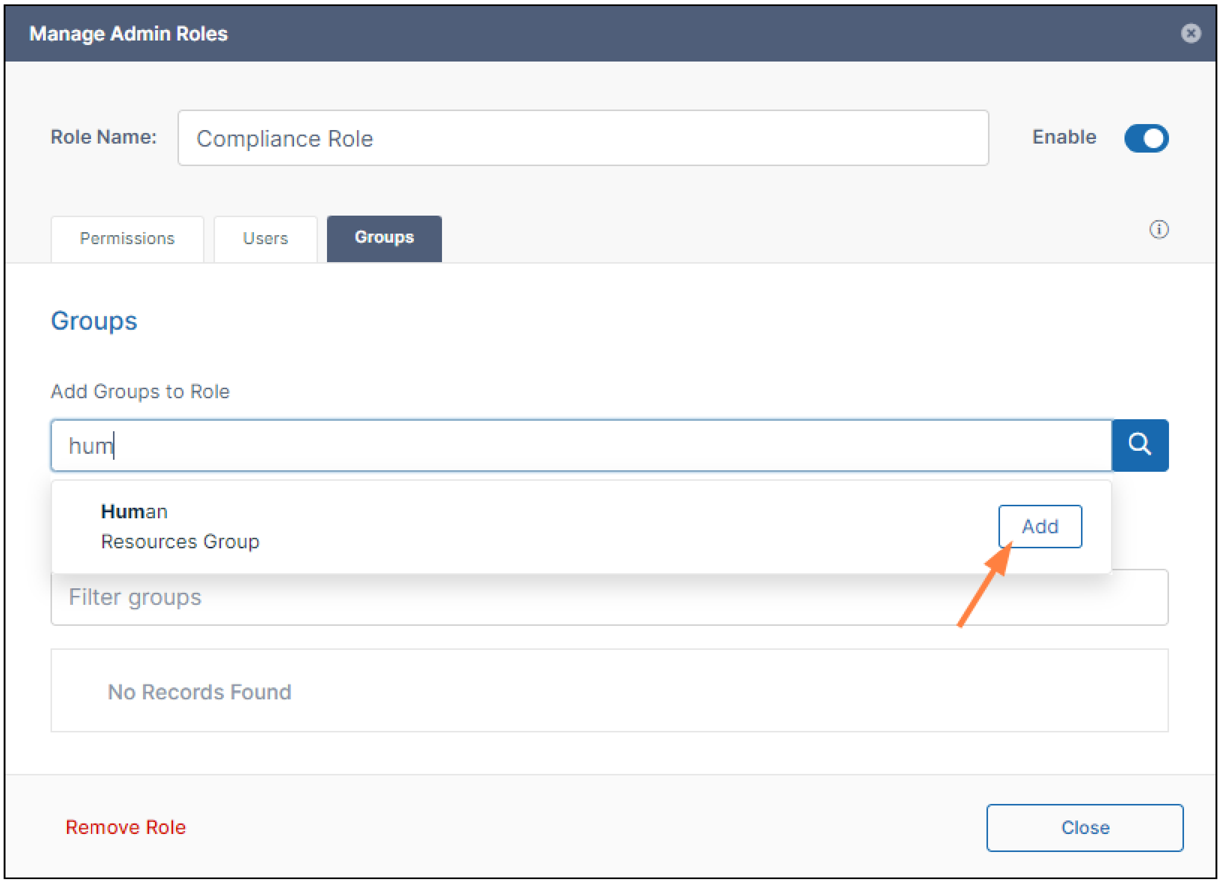
Manage Admin Roles

Role Name: Compliance Role

Enable

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: Compliance Role

Enable

Groups

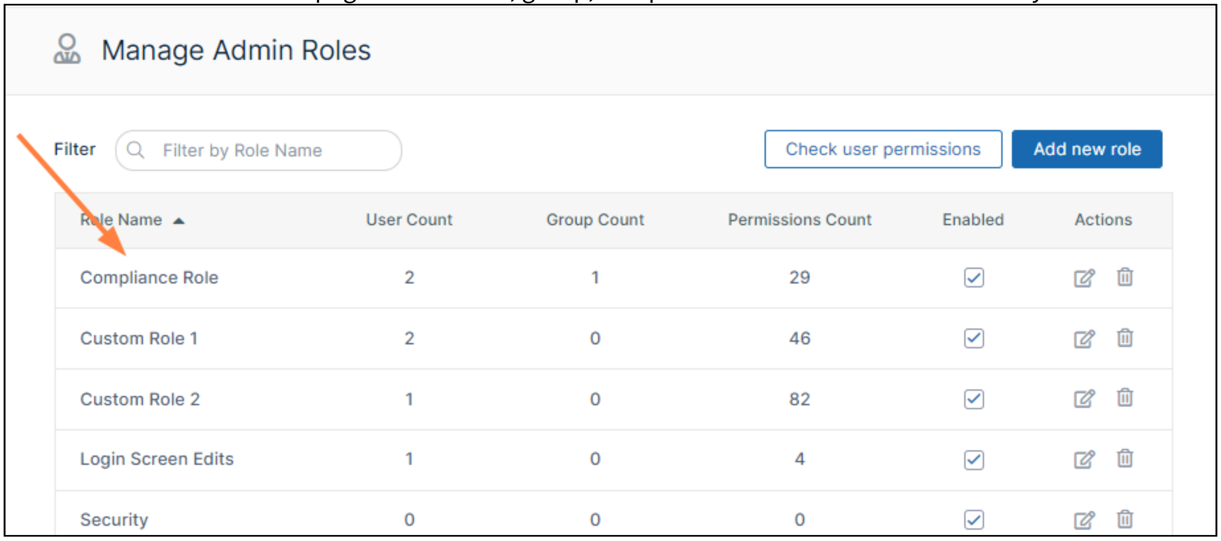
Add Groups to Role

hum

Human
Resources Group

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

Role Name ▲	User Count	Group Count	Permissions Count	Enabled	Actions
Compliance Role	2	1	29	☑	
Custom Role 1	2	0	46	☑	
Custom Role 2	1	0	82	☑	
Login Screen Edits	1	0	4	☑	
Security	0	0	0	☑	

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

Definitions of Permissions

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

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

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

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

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

2FA Settings for Promoted Admins

When a user is configured as an admin user, if 2FA is enabled for admins, by default, the 2FA delivery mode set for the user account (in the user's policy) is used for the Admin account. If the setting TONIDOCLOUD_2FA_ADMIN_FLOW_FOR_PROMOTED_ADMINS is enabled, the 2FA method set for administrators is used for the admin account.
To use the 2FA method set for administrators:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To use the 2FA method set for administrators, add the line:

```
define("TONIDOCLOUD_2FA_ADMI
N_FLOW_FOR_PROMOTED_ADMINS",
 true);
```

User Authentication Settings

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

FileCloud supports the following Authentication modes

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

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

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

⚠ **Note**

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

Enabling Default Authentication

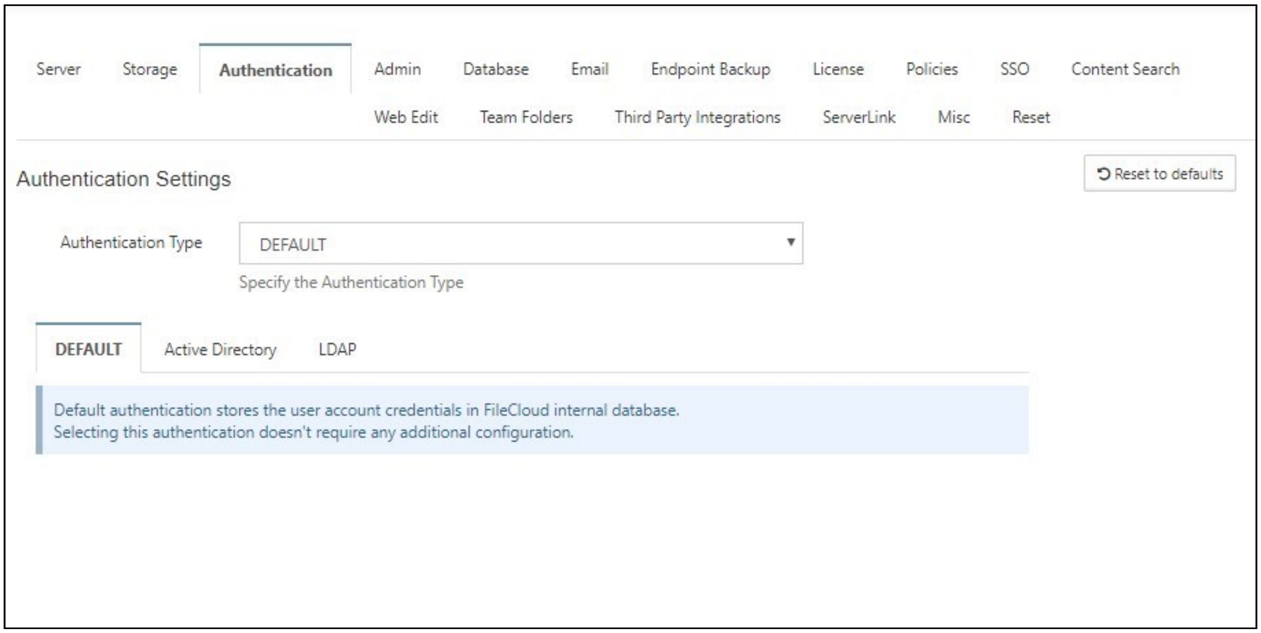
Initially, FileCloud is set to default authentication mode. User accounts created when this authentication type is configured have credentials stored and managed within FileCloud.

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.



Authentication Settings

Authentication Type: DEFAULT

Specify the Authentication Type

Default authentication stores the user account credentials in FileCloud internal database.
Selecting this authentication doesn't require any additional configuration.

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	

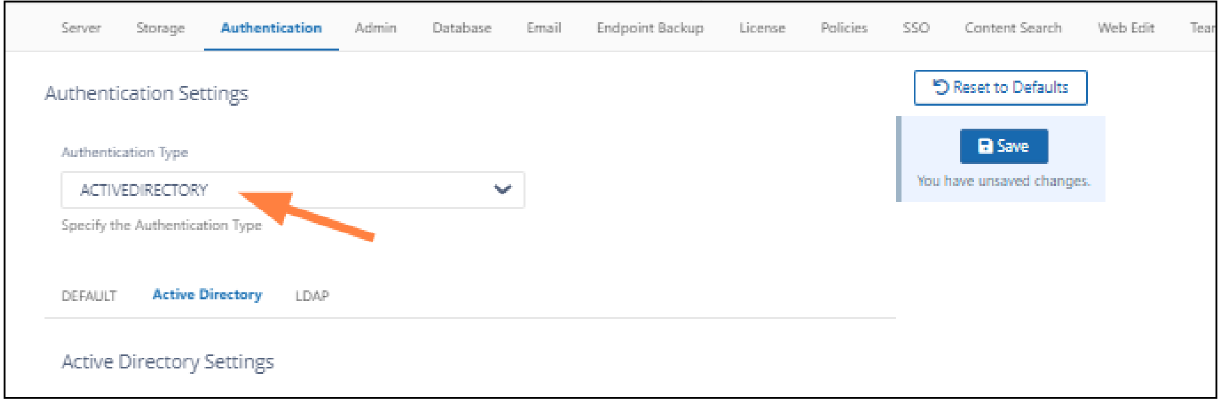
How To Enable AD Authentication

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.



Authentication Settings

Authentication Type: ACTIVEDIRECTORY

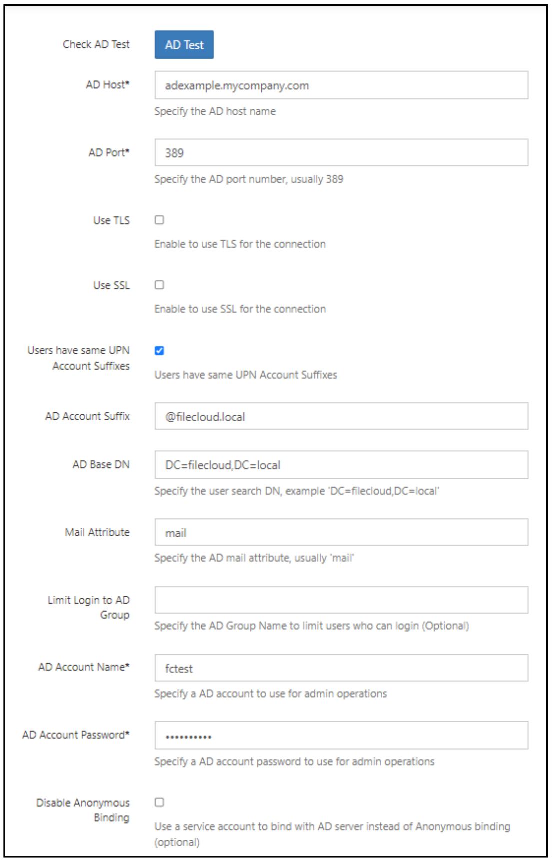
Specify the Authentication Type

Active Directory Settings

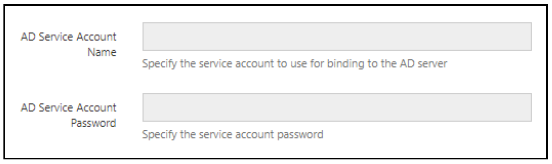
5. Enter the required information in the settings under **Active Directory Settings** (See **AD configuration parameters**, below) and then click **Save**.
   Note: The changed parameters must be saved before performing an AD test.

AD configuration parameters

To connect FileCloud with your AD environment, enter the correct connection parameters.



Check AD Test	AD Test	
AD Host*	adexample.mycompany.com	Specify the AD host name
AD Port*	389	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	@filecloud.local	
AD Base DN	DC=filecloud,DC=local	Specify the user search DN, example 'DC=filecloud,DC=local'
Mail Attribute	mail	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*	fctest	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.

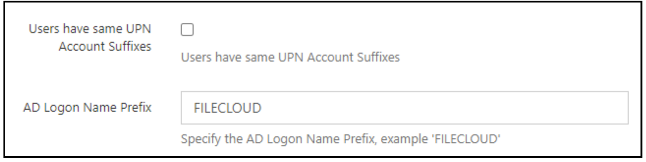
AD Port - Required. Enter **389** for non-SSL, or enter **636** for SSL.

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.

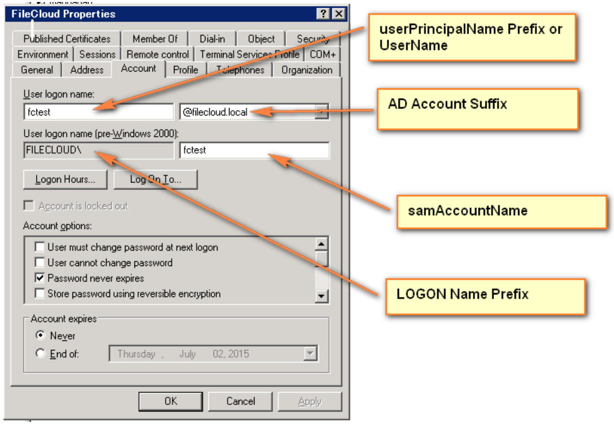
Users have the same UPN Account Suffixes
All of your AD users should have the same suffix or the same prefix.

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

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



User logon name: fctest @filecloud.local

User logon name (pre-Windows 2000): FILECLOUD\ fctest

□ Account is locked out

Account options:

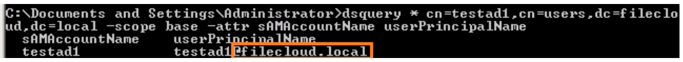
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Thursday , July 02, 2015

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.

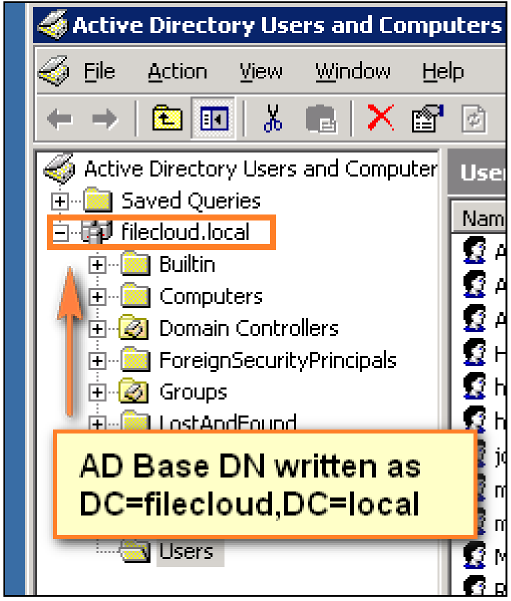
Instead of viewing the properties as shown above, you can get the account suffix by running the following query in the command line in the AD server:

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



```
C:\Documents and Settings\Administrator>dsquery * cn=testad1,cn=users,dc=fileclo
ud,dc=local -scope base -attr sAMAccountName userPrincipalName
  sAMAccountName    userPrincipalName
  testad1           testad1@filecloud.local
```

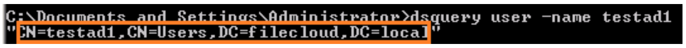
AD Base DN - Required. Do not enter value with quotes. The Base DN for your domain. Located in the extended attributes in **Active Directory Users and Computers MMC**:



AD Base DN written as DC=filecloud,DC=local

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 testad1
"CN=testad1,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.

	Limit Login to AD Group - Optional. To limit login to specific users, add them to a group and specify the group name here. (Typically this is left blank.) If you set this field, ensure that the account name specified in **AD Account Name** is part of the AD group. **AD Account Name** - Required. A valid account name is required here in order for FileCloud to query the AD server. This can be any account that can access the AD server, and is located in **User logon name** in the **FileCloud Properties** screenshot, above. **Notes:** Enter username, not email id in this field. This account must have an email address set in AD. **AD Account password** - A password for the AD account name. **Disable Anonymous Binding** - Optional. Enable this checkbox if your AD does not allow anonymous binding. Enabling this checkbox enables the **AD Service Account Name** and **AD Service Account Password text boxes**. **AD Service Account Name** - Optional. The service account name to use to bind with the AD server. **AD Service Account Password** - Optional. The service account password to use to bind with the AD server.

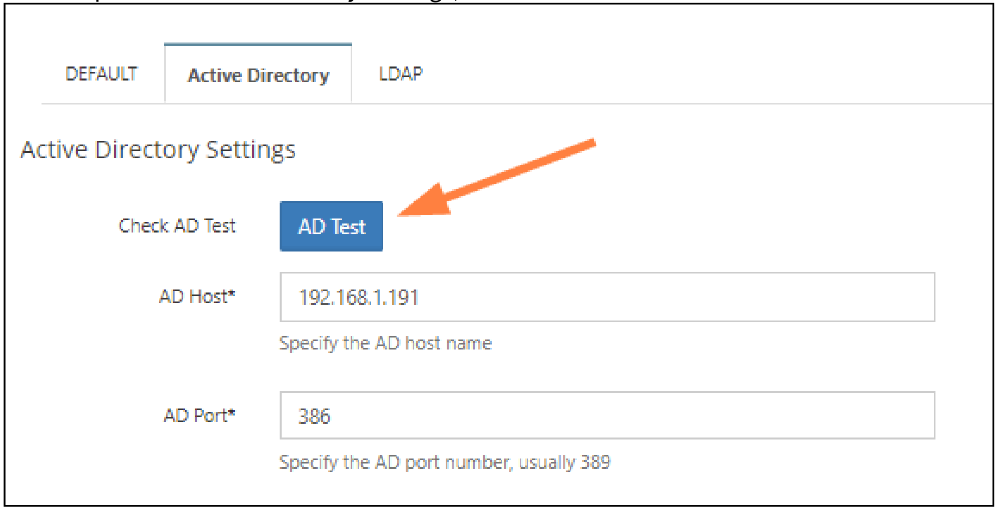
⚠ To connect to Active Directory over SSL, please follow the steps mentioned here.

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

Testing AD Connectivity

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

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



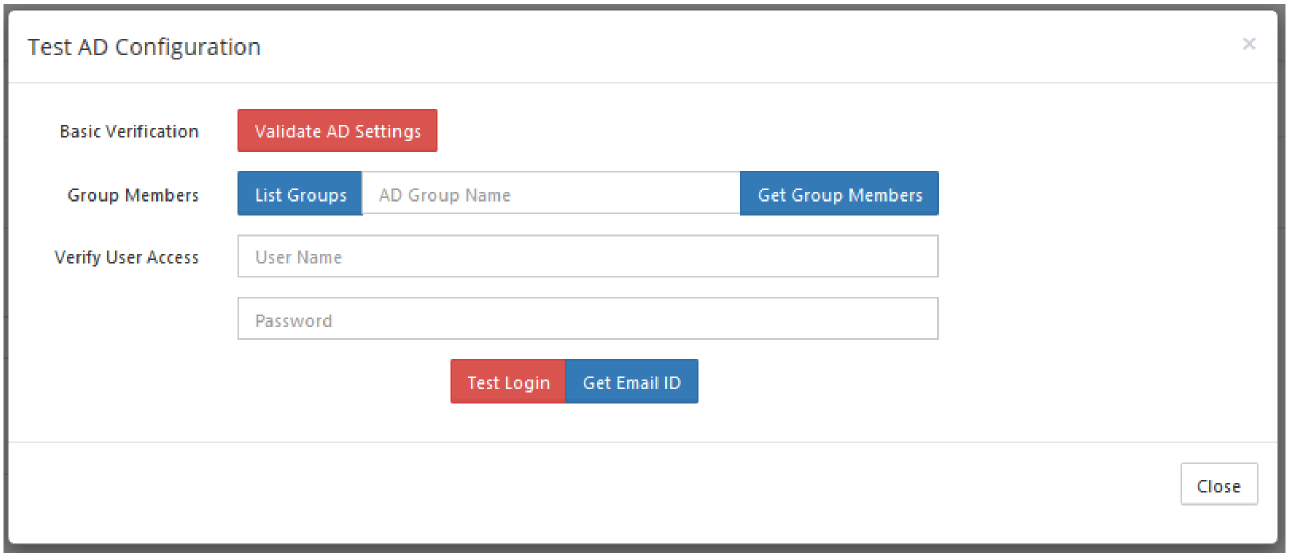
AD Host* 192.168.1.191

Specify the AD host name

AD Port* 386

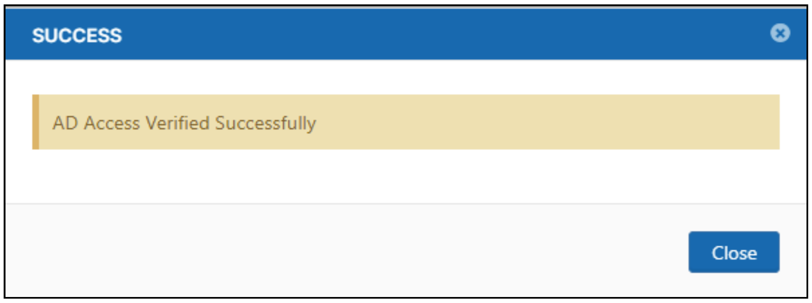
Specify the AD port number, usually 389

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



The following tests can be done.

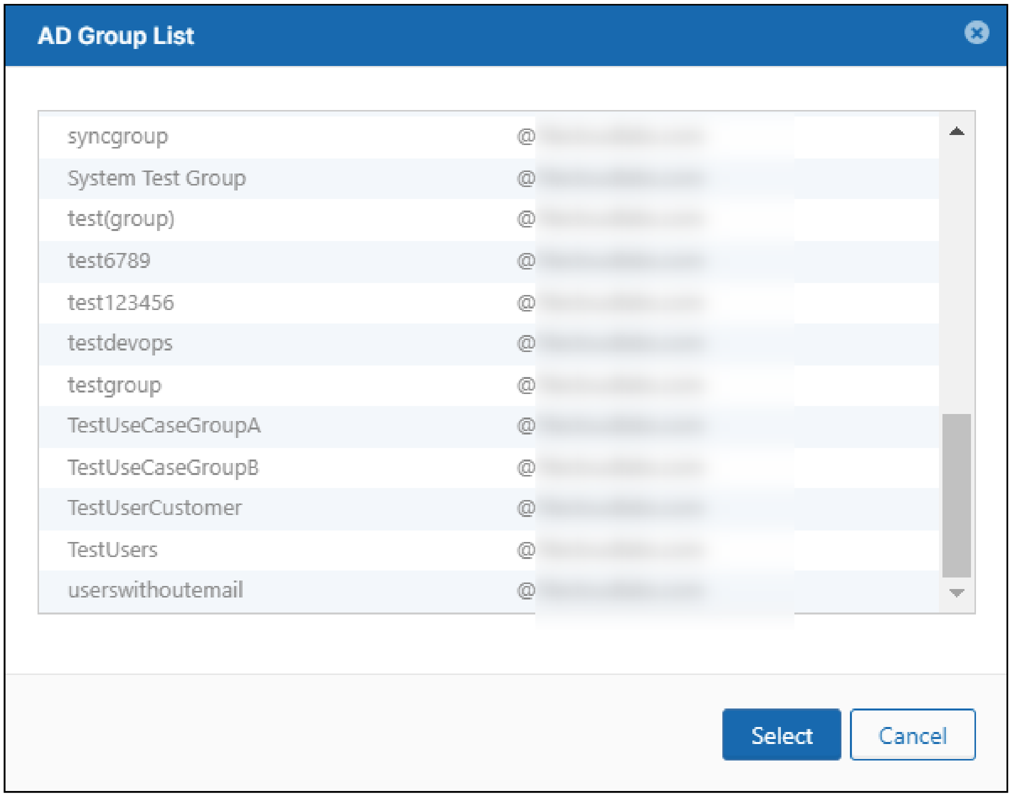
1. Validate AD settings.
   a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server. You should receive the response:



AD Access Verified Successfully

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

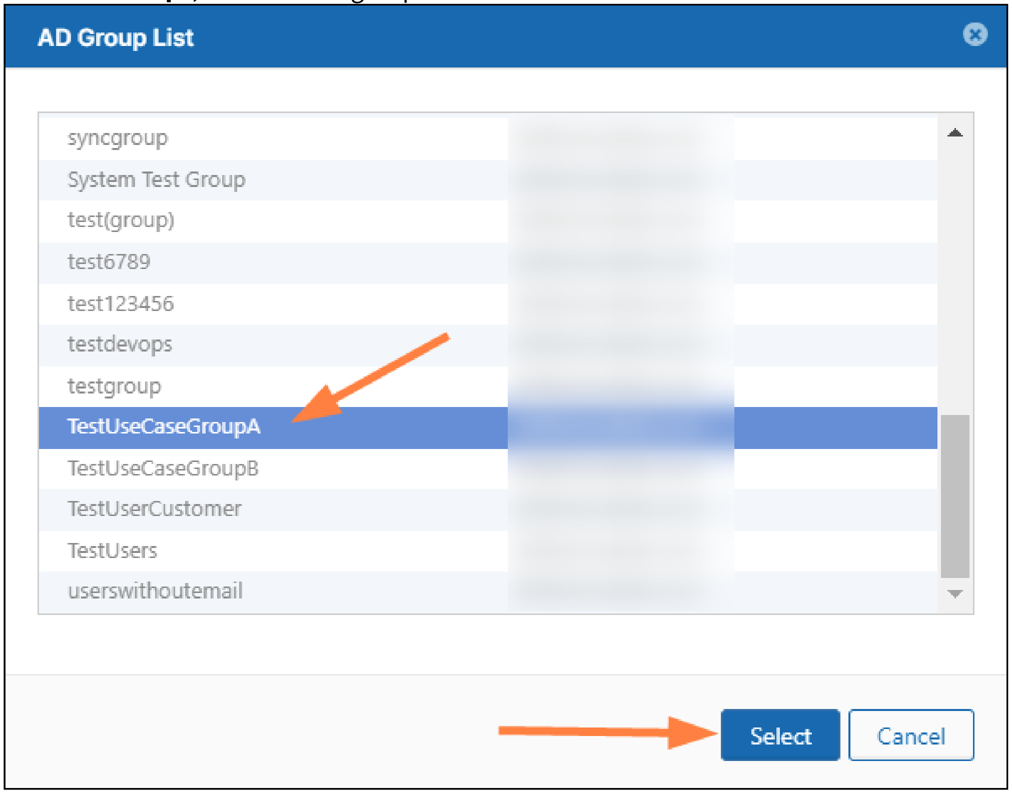
2. List Groups
    a. Once AD settings are validated, click **List Groups** to view the list of groups read from the server. You should see a list similar to:



syncgroup	@[redacted]
System Test Group	@[redacted]
test(group)	@[redacted]
test6789	@[redacted]
test123456	@[redacted]
testdevops	@[redacted]
testgroup	@[redacted]
TestUseCaseGroupA	@[redacted]
TestUseCaseGroupB	@[redacted]
TestUserCustomer	@[redacted]
TestUsers	@[redacted]
userswithoutemail	@[redacted]

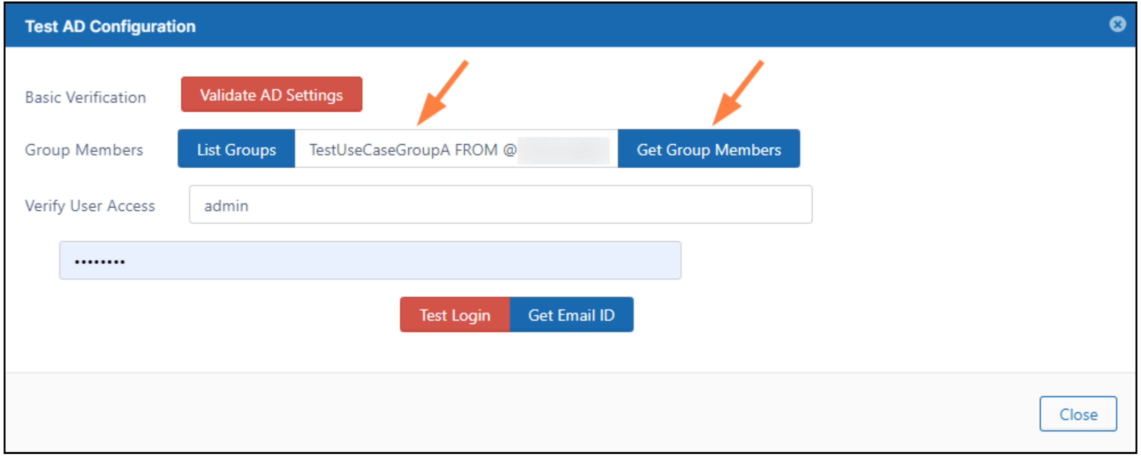
3. Get Group Member

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**.

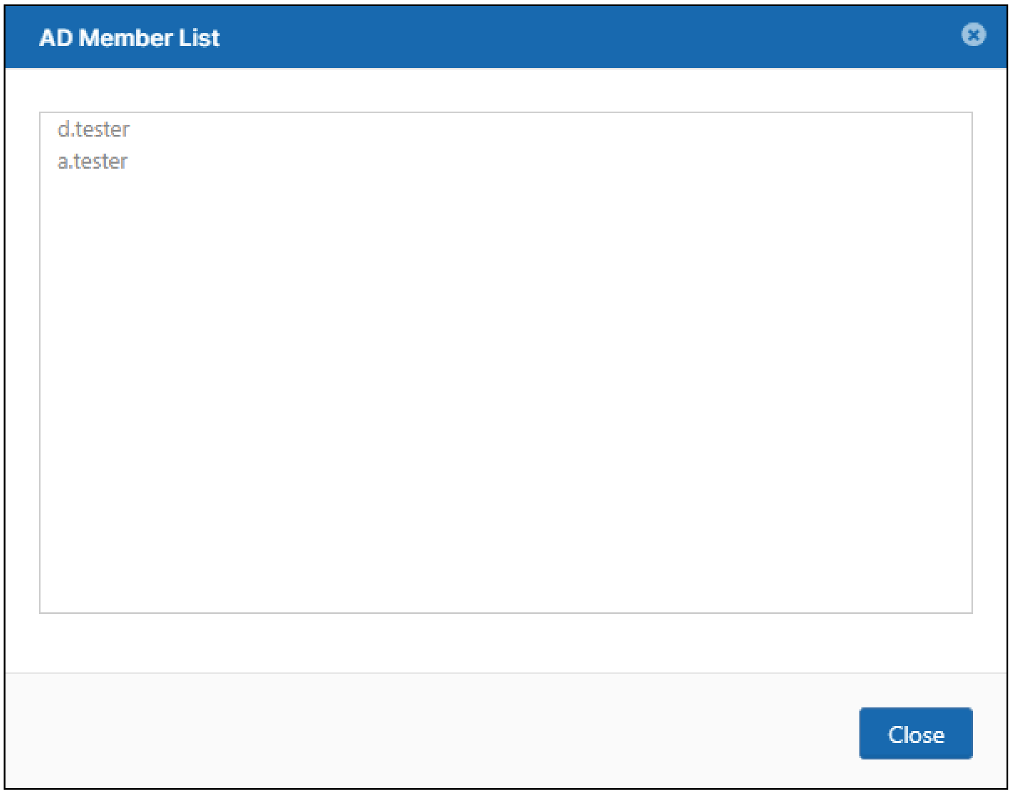


Group Members: TestUseCaseGroupA FROM @

Verify User Access: admin

••••••••

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



d.tester
a.tester

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

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

More Information:

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

Connecting to AD via SSL

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

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

> Before you can enable the use of SSL certificates in FileCloud Server, you must have completed the following steps:
> 1. Install and configure your Active Directory Server
> 2. Install an SSL certificate on your Active Directory Server

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 can I troubleshoot my AD/SSL connection?

If you have problems connecting after setting the above and non-SSL connections work OK, you might have to set this additional parameter.

1. Create a **ldap.conf** file.

   Windows Location should be c:\openldap\sysconf\ldap.conf
   Ubuntu Linux Location should be /etc/ldap/ldap.conf **Centos Linux Location** should be /etc/openldap/ldap.conf

2. This ldap.conf file should be

   ```
   #
   # LDAP Defaults
   #
   TLS_REQCERT never
   ```

3. Restart apache server.

How do I connect to AD using TLS?

Connecting to Active Directory over TLS

TLS

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

Some OS like Ubuntu 14.04, does TLS v1.2 negotiation by default. To disable this behavior, add the following line to WWWROOT/thirdparty/adLDAP.php

Disable TLS v1.2

```
if ($this->useSSL) {
putenv("LDAPTLS_CIPHER_SUITE=NORMAL:!VERS-TLS1.2");
$this->ldapConnection = ldap_connect("ldaps://" . $domainController, $this->adPort);
} else {
$this->ldapConnection = ldap_connect($domainController, $this->adPort);
}
```

Authenticating to Multiple AD servers

> ⓘ The ability for a single installation of FileCloud to authenticate against multiple Active Directory servers is available in FileCloud Server version 7.0 and later.

Although the latest versions of the Windows Server operating system handle large numbers of objects more efficiently, there are many reasons why organizations implement multidomain forests.

An example of this is a university.

- In the Faculty of Science, there are different departments or schools, such as the school of physics and the department of botany
- For political or organizational reasons it might have been decided that each department or school should have its own domain that is a part of the overall university forest
- Active Directory gives organizations the ability to create domain namespaces that meet their needs

To display more information, click on a topic.

Why would I use a multidomain AD structure?

The reasons for using multidomain AD structures can include but are not limited to:

- Historical domain structure. Some organizations have retained the forest structure that was established when the organization first adopted Active Directory.
- Organizational or political reasons. Some organizations are conglomerates, and they might be comprised of separate companies that share a common administrative and management core.
- Security reasons Domains. Some organizations need to create authentication and authorization boundaries. You can also use domains to partition administrative privileges so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it's possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

➡ For more information on using multidomain AD infrastructure, on the Microsoft Web site, read AD Directory Services Getting Started.

Enable multiple AD server authentication

To enable multiple AD server authentication, you have to configure settings in the following places:

- adconfig.php file
- Admin Dashboard

To enable multiple AD server authentication:

1. Open a browser and log in to the Admin Portal.
2. On the Admin Dashboard, from the left navigation panel, click Settings.
3. On the Manage Settings screen, click Authentication.
4. To enable the Active Directory Settings, under Authentication Settings, change the Authentication Type to ACTIVEDIRECTORY.

5. Select the Active Directory sub-tab, type in the required information, and then click Save.
6. Create a file called **adconfig.php** in one of the following locations, depending on your OS:

```
Windows Location
c:\xampp\htdocs\config\adconfig.php


Linux Location
/var/www/htdocs/config/adconfig.ph
```

7. Add the information for the other AD servers using the following example. ⚠ Do not add the same AD server detail that was already configured in Admin Dashboard.

```
<?php
/* Configuration values for ActiveDirectory Authentication */
// ... Multi-AD Server Support, set to 1 to enable additional AD servers
define("TONIDOCLOUD_MULTI_AD_ENABLE", 1);
//=============== SITE 1 ==============================
define("TONIDOCLOUD_AD_HOST_1", "ADSERVERHOST" ); // < ActiveDirectory Host
define("TONIDOCLOUD_AD_PORT_1", 389 ); // < ActiveDirectory port
define("TONIDOCLOUD_AD_ACCOUNTSUFFIX_1", "@mysite.internal"); // < User Login Name Suffix
//define("TONIDOCLOUD_AD_LOGONNAMEPREFIX_1","SST"); // use this if prefix is needed. Note use only prefix or suffix
define("TONIDOCLOUD_AD_BASEDN_1", "DC=mysite,DC=internal"); // < User Search DN
define("TONIDOCLOUD_AD_MAILATTRIBUTE_1", "mail"); // < Mail Attribute
define("TONIDOCLOUD_AD_LIMIT_GROUP_1", ""); // < If you want login users to be limited to a specific AD group
define("TONIDOCLOUD_AD_USETLS_1", false); //<< If you want to use TLS set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_USESSL_1", false); //<< If you want to use SSL set true, default is false, both SSL and TLS can't be true
define("TONIDOCLOUD_AD_ACCOUNTNAME_1", "Administrator"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ACCOUNTPASSWORD_1", "adminpassword"); // < Account Password for Admin Operations
define("TONIDOCLOUD_AD_USEADMINBINDING_1", "0"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ADMINACCOUNTNAME_1", ""); // < AD Service Account Username
define("TONIDOCLOUD_AD_ADMINACCOUNTPASSWORD_1", ""); // < AD Service Account Password
//=============== SITE 2 ==============================
define("TONIDOCLOUD_AD_HOST_2", "ADSERVERHOST2" ); // < ActiveDirectory Host
define("TONIDOCLOUD_AD_PORT_2", 389 ); // < ActiveDirectory port
define("TONIDOCLOUD_AD_ACCOUNTSUFFIX_2", "@mysite2.internal"); // < User Login Name Suffix
//define("TONIDOCLOUD_AD_LOGONNAMEPREFIX_1","SSK"); // use this if prefix is needed. Note use only prefix or suffix
define("TONIDOCLOUD_AD_BASEDN_2", "DC=mysite2,DC=internal"); // < User Search DN
define("TONIDOCLOUD_AD_MAILATTRIBUTE_2", "mail"); // < Mail Attribute
define("TONIDOCLOUD_AD_LIMIT_GROUP_2", ""); // < If you want login users to be limited to a specific AD group
define("TONIDOCLOUD_AD_USETLS_2", false); //<< If you want to use TLS set true, default is false, both SSL
```

```
and TLS can't be true
define("TONIDOCLOUD_AD_USESSL_2", false); //<< If you want to use SSL set true, default is false, both SSL
and TLS can't be true
define("TONIDOCLOUD_AD_ACCOUNTNAME_2", "Administrator"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ACCOUNTPASSWORD_2", "adminpassword"); // < Account Password for Admin
Operations
define("TONIDOCLOUD_AD_USEADMINBINDING_2", "0"); // < Account name for Admin Operations
define("TONIDOCLOUD_AD_ADMINACCOUNTNAME_2", ""); // < AD Service Account Username
define("TONIDOCLOUD_AD_ADMINACCOUNTPASSWORD_2", ""); // < AD Service Account Password
?>
```

Now additional users from these domains can also login into FileCloud.

> When connecting to multiple AD servers, there might be issues adding the same user account name from different domains into FileCloud. FileCloud requires unique usernames and will disallow adding another username from another domain if the name already exists.
> To handle this please add the following to cloudconfig.php. This will allow duplicate users to be added from other domains as long as the email address is unique. The users will have to login into the system using email address.
> define("TONIDOCLOUD_ALLOW_DUPUSERNAMES", 1);

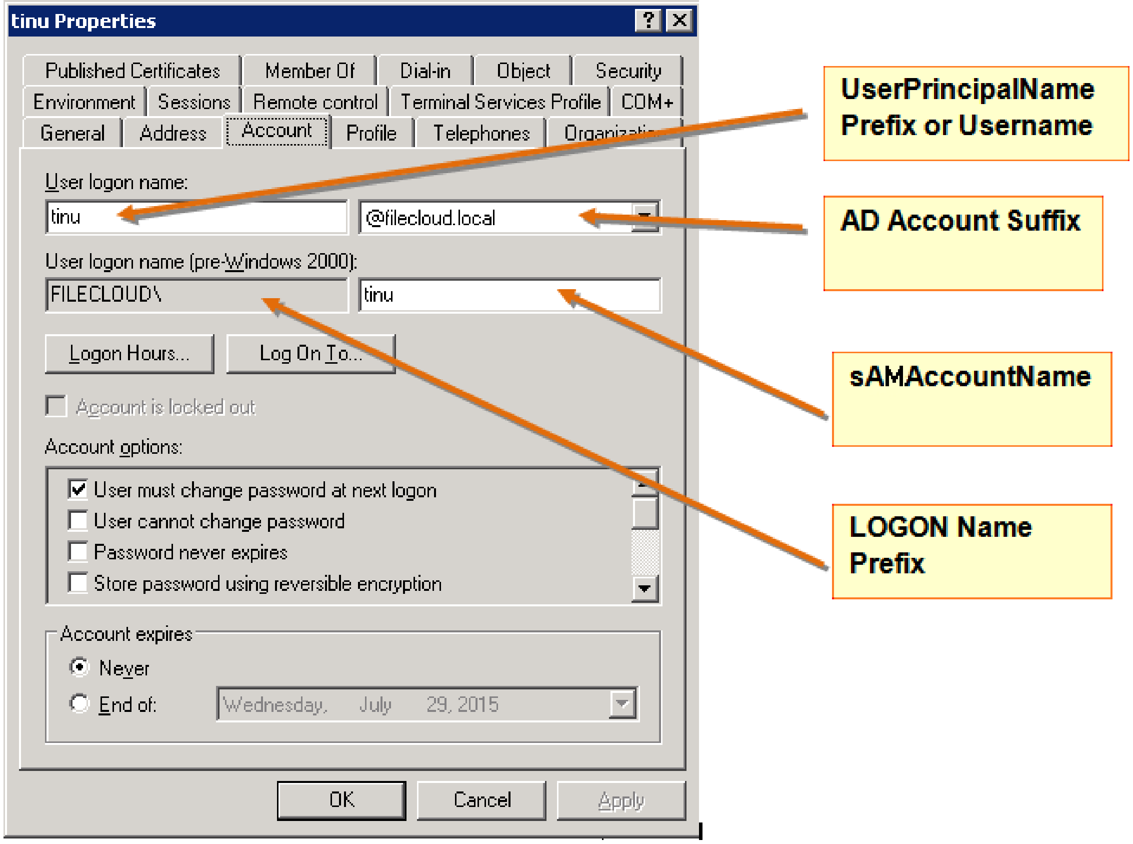
Mixed AD Domain Environments

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)



User logon name:
tinu @filecloud.local

User logon name (pre-Windows 2000):
FILECLOUD\ tinu

□ Account is locked out

Account options:

☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, July 29, 2015

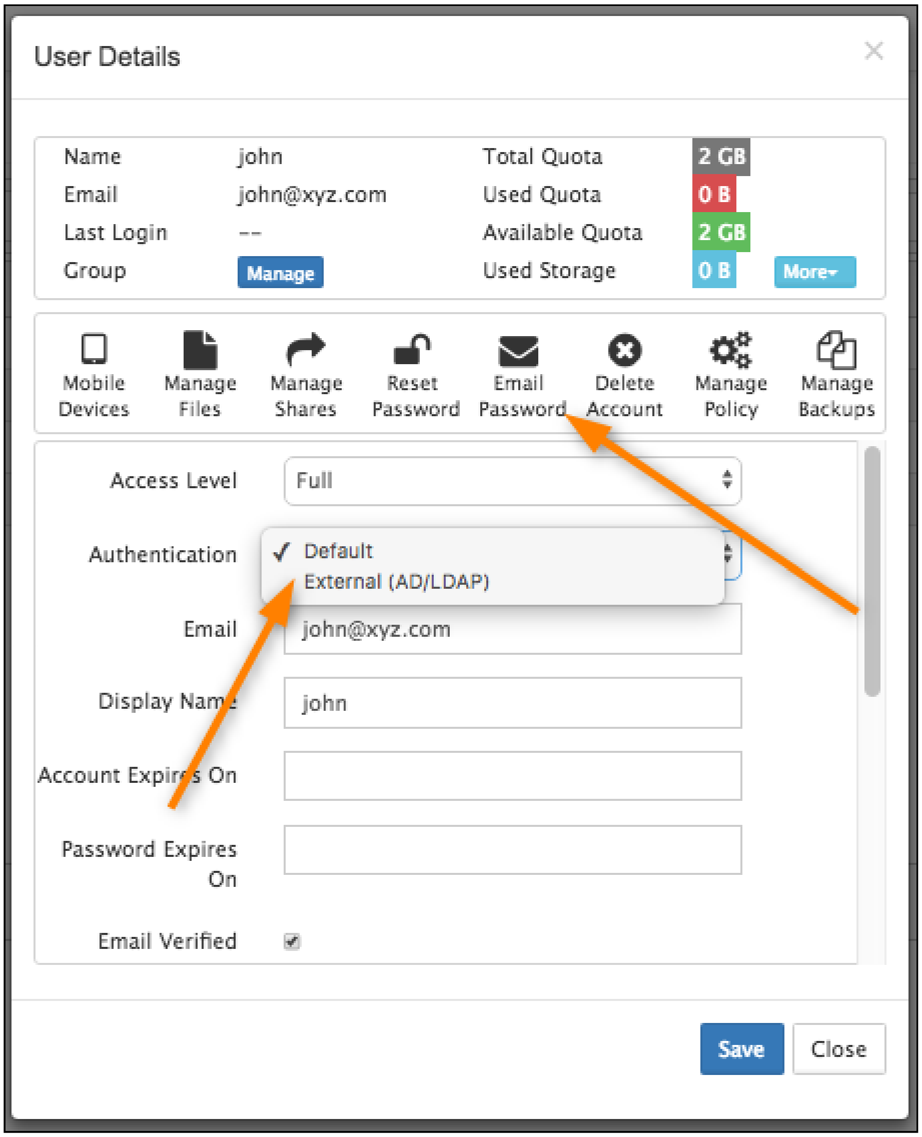
Users can login using either their email or sAMAccountName.

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 form 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

Access Level: Full

Authentication: ✓ Default

Email: john@xyz.com

Display Name: john

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:

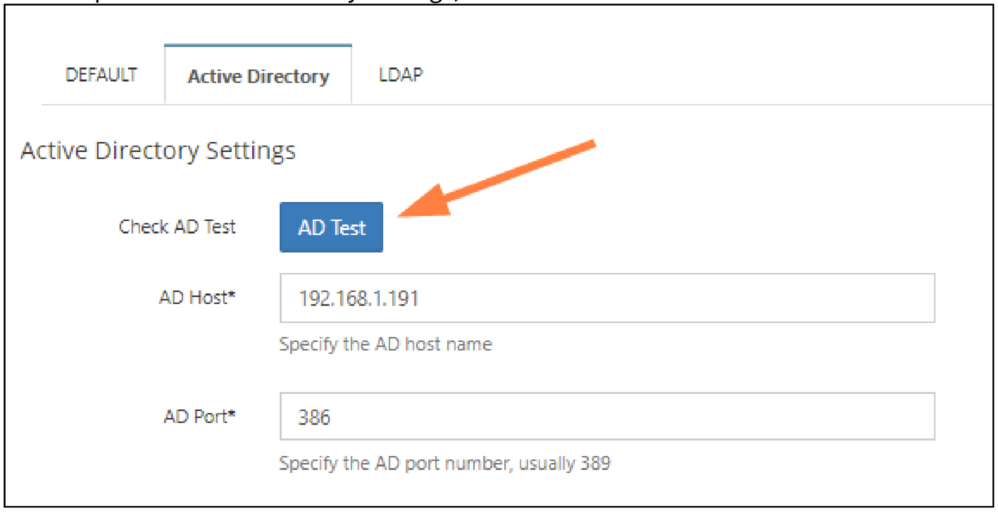
   ```
   telnet 192.168.1.191 389
   ```
3. Confirm that you have entered an account in **AD Account Name**. This account is used to query the AD server and must be present.
   If you have entered a value in **Limit Login to AD Group** (see below) the account you enter into **AD Account Name** must be 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.

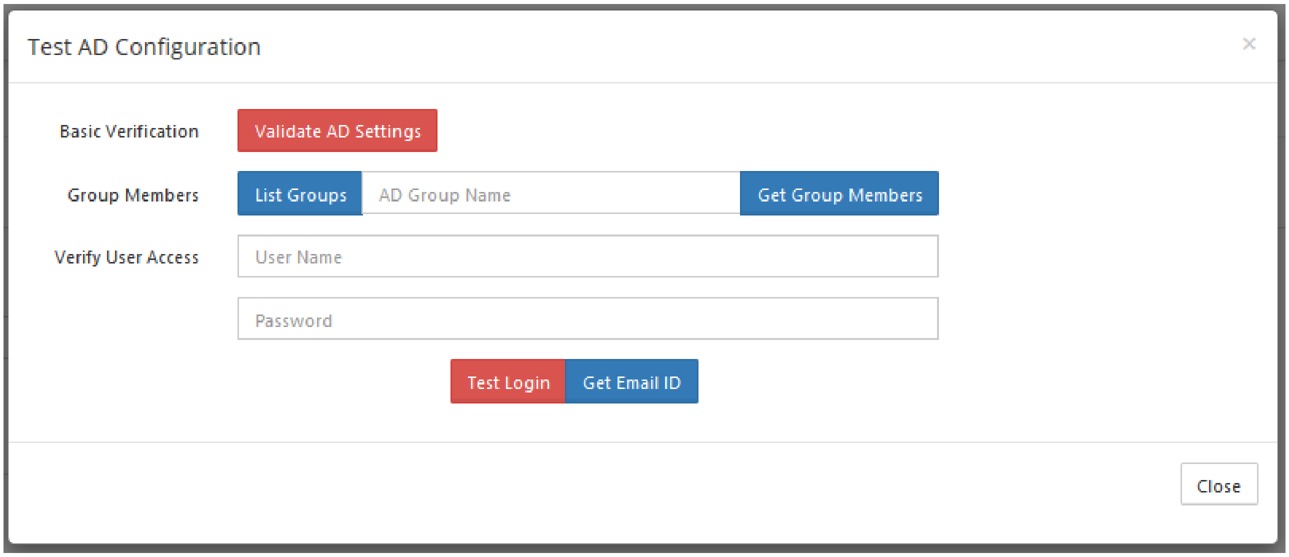
At the top of the Active Directory settings, click the **AD Test** button.



AD Host*: 192.168.1.191
Specify the AD host name

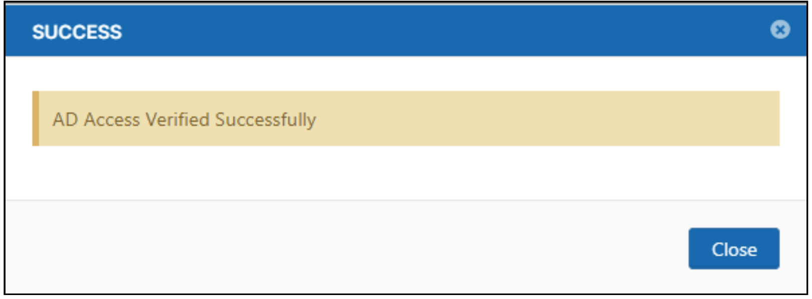
AD Port*: 386
Specify the AD port number, usually 389

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



The following tests can be done.

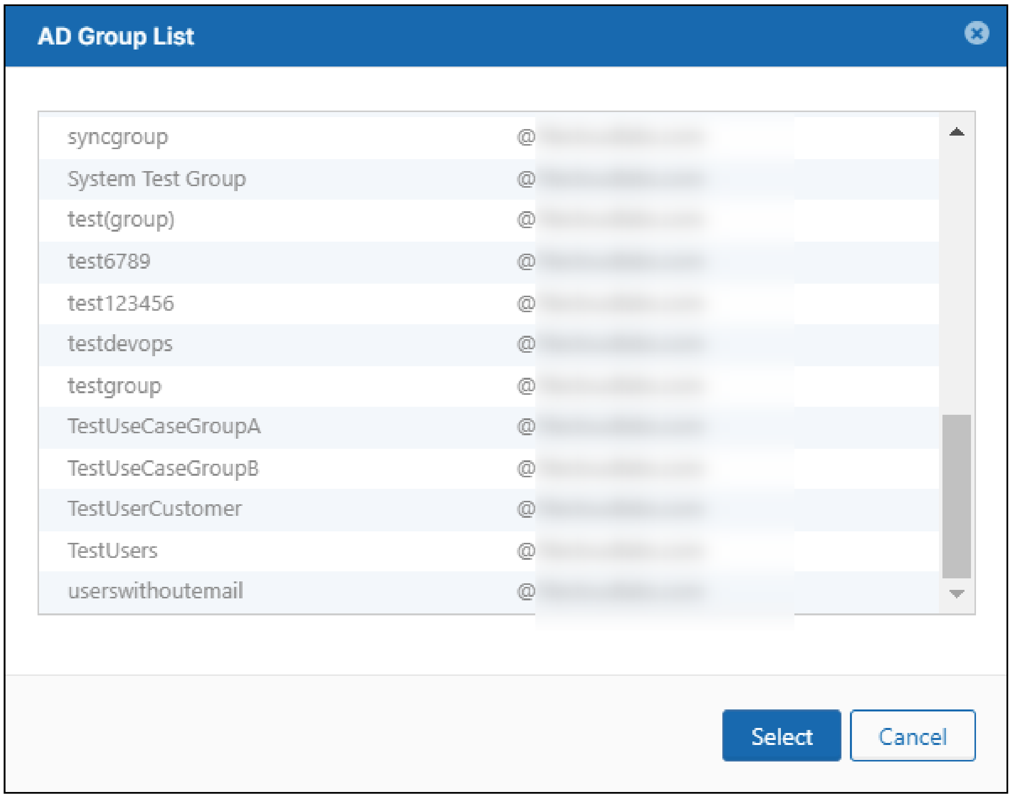
1. Validate AD settings.
    a. Click the **Validate AD Settings** button to perform basic connectivity tests with the AD server. You should receive the response:



AD Access Verified Successfully

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:

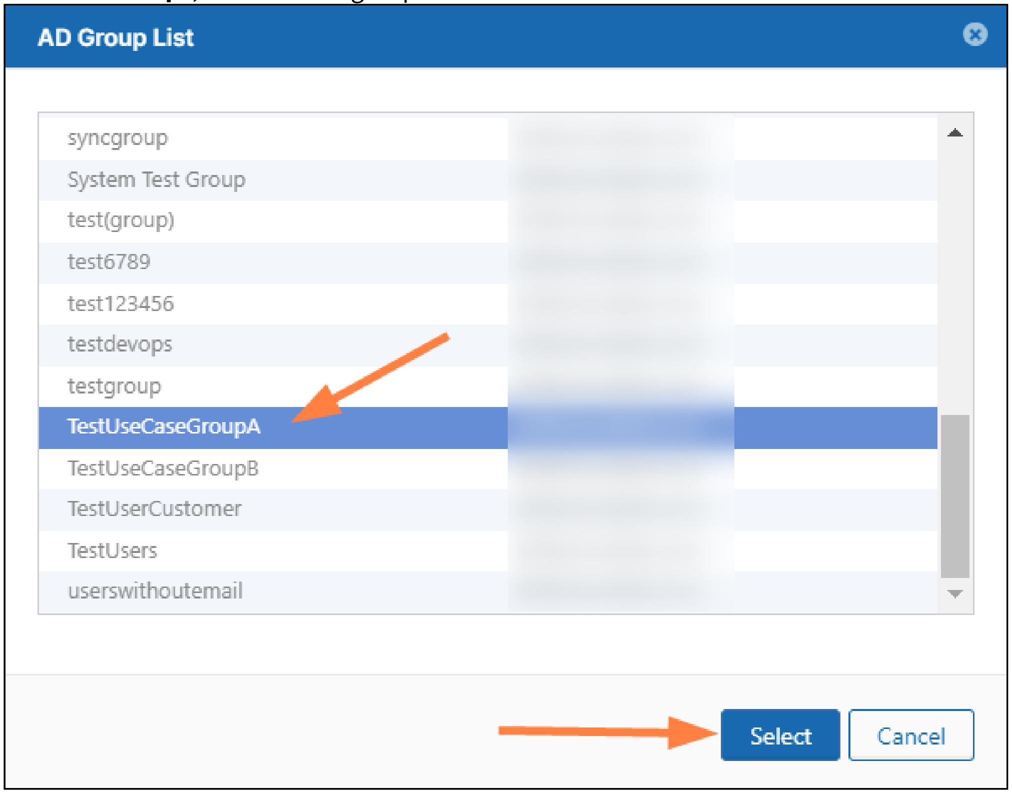


AD Group List

syncgroup	@[redacted]
System Test Group	@[redacted]
test(group)	@[redacted]
test6789	@[redacted]
test123456	@[redacted]
testdevops	@[redacted]
testgroup	@[redacted]
TestUseCaseGroupA	@[redacted]
TestUseCaseGroupB	@[redacted]
TestUserCustomer	@[redacted]
TestUsers	@[redacted]
userswithoutemail	@[redacted]

3. Get Group Member

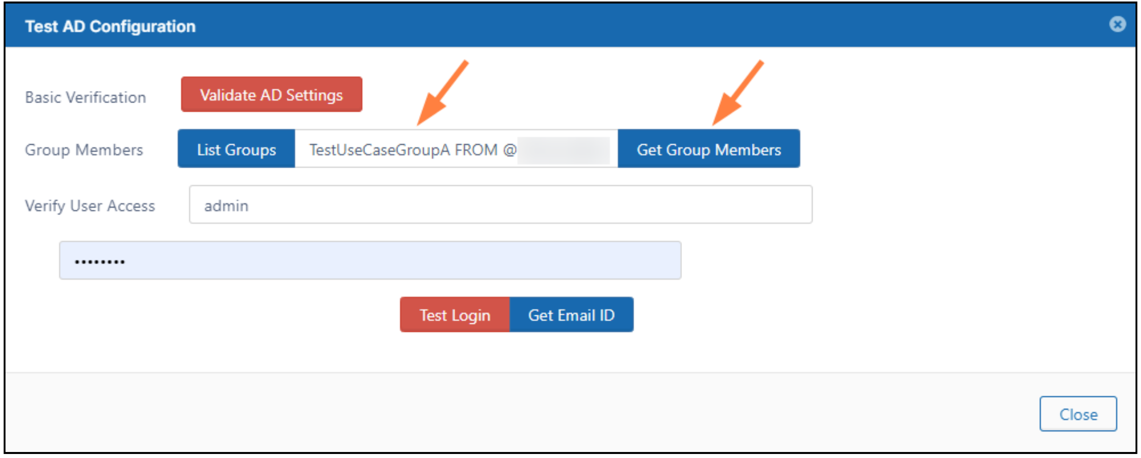
1. Click **List Groups**, then select a group and click **Select**.



- syncgroup
- System Test Group
- test(group)
- test6789
- test123456
- testdevops
- testgroup
- TestUseCaseGroupA
- TestUseCaseGroupB
- TestUserCustomer
- TestUsers
- userswithoutemail

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**.



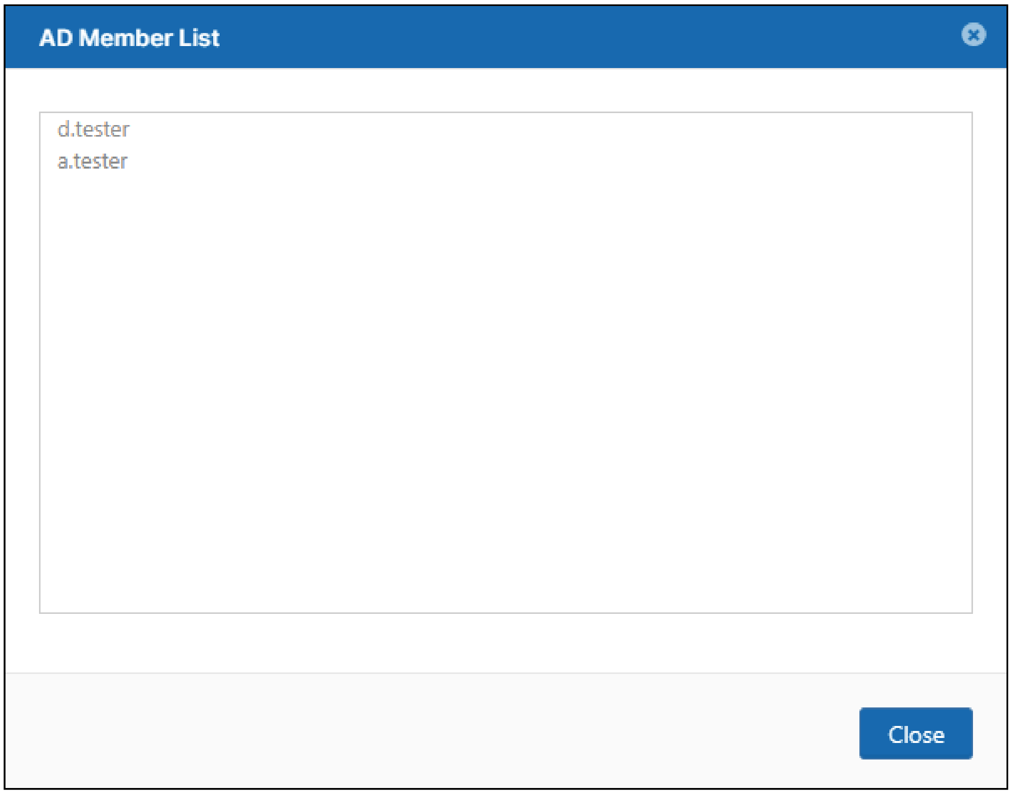
Basic Verification

Group Members: TestUseCaseGroupA FROM @

Verify User Access: admin

••••••••

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



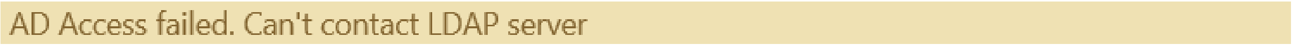
d.tester
a.tester

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.

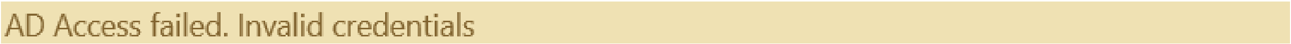
Here are some common AD connectivity error messages and their meanings:

Error messages



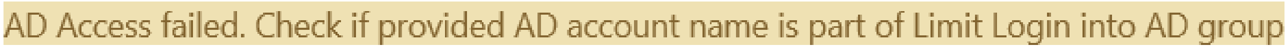
AD Access failed. Can't contact LDAP server

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 able to log in to FileCloud.
2. In **Limit Login to AD Group**, enter the name of the AD group.

Single sign-on (SSO)

Single sign-on (SSO) is a user authentication process that permits a user to enter one name and password in order to access multiple applications.

FileCloud supports the following types of Single sign-on model.

- SAML Single Sign-On Support
- ADFS Single Sign-On Support
- NTLM Single Sign-On Support

SAML Single Sign-On Support

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.

As of FIleCloud Version 19.3, you can override the default SSO port.
As of FileCloud Version 20.3.2, to achieve high availability, you can configure FileCloud to support multiple memcache servers.

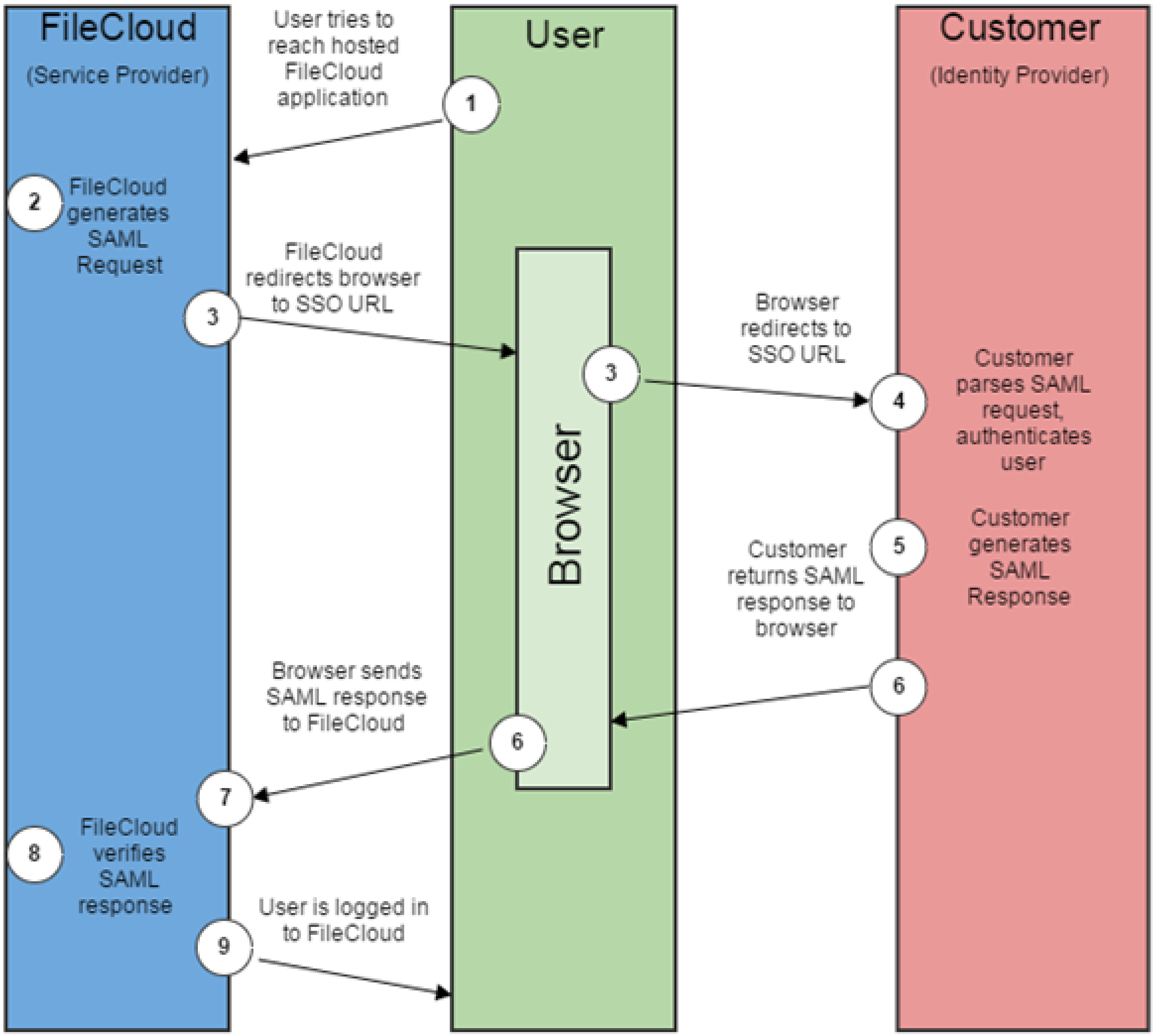
You can use SAML SSO to control the authorization and authentication of hosted user accounts that can access FileCloud Web based interface.

- SAML is an XML based open standard data format for exchanging authentication and authorization data between parties.
- FileCloud supports SAML (Security Assertion Markup Language) based web browser Single Sign On (SSO) service
- FileCloud acts as a Service Provider (SP) while the Customer or Partner acts as the identity provider (IdP). FileCloud SAML SSO service is based on SAML v2.0 specifications.

SSO Login Diagram

SSO transaction diagram

The following process explains how the user logs into a hosted FileCloud application through customer-operated SAML based SSO service.


FileCloud
(Service Provider)
User
Customer
(Identity Provider)
User tries to reach hosted FileCloud application
1
2
FileCloud generates SAML Request
FileCloud redirects browser to SSO URL
3
Browser
3
Browser redirects to SSO URL
4
Customer parses SAML request, authenticates user
5
Customer returns SAML response to browser
Customer generates SAML Response
6
Browser sends SAML response to FileCloud
6
7
8
FileCloud verifies SAML response
User is logged in to FileCloud
9

FileCloud SAML Transaction Steps

1. The user attempts to reach the hosted FileCloud application through the URL.
2. FileCloud generates a SAML authentication request. The SAML request is embedded into the URL for the customer’s SSO Service.
3. FileCloud sends a redirect to the user’s browser. The redirect URL includes the SAML authentication request and is submitted to customer’s SSO Service.
4. The Customer’s SSO Service authenticates the user based on valid login credentials.
5. The customer generates a valid SAML response and returns the information to the user’s browser.
6. The customer SAML response is redirected to FileCloud.
7. The FileCloud authentication module verifies the SAML response.
8. If the user is successfully authenticated, the user will be successfully logged into FileCloud.

When the IdP successfully authenticates the user account, 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

Configuring the Apache server requires you to add the Alias directive to the simplesaml.php configuration file.

Pre-requisite: The mcrypt module must be installed on the FileCloud Server.

- In Windows, it should be installed by default.
- In Linux, if mcrypt is not installed, it must be installed

To add the Alias directive:

Use the following table to understand the typical entries in Linux and windows.

You can change these settings if the FileCloud is installed under a different WEB ROOT Folder.

OS	Instructions

Windows	1. Navigate to the following directory
	`c:\xampp\apache\conf\extra`
	2. Open the following file for editing
	`httpd-filecloud.conf`
	3. Add the following line at the end of the file
	`Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/www"`
	4. Save the file.
	5. Open the FileCloud Control Panel.
	6. Use the control panel to stop and start the Webserver.

OS	Instructions

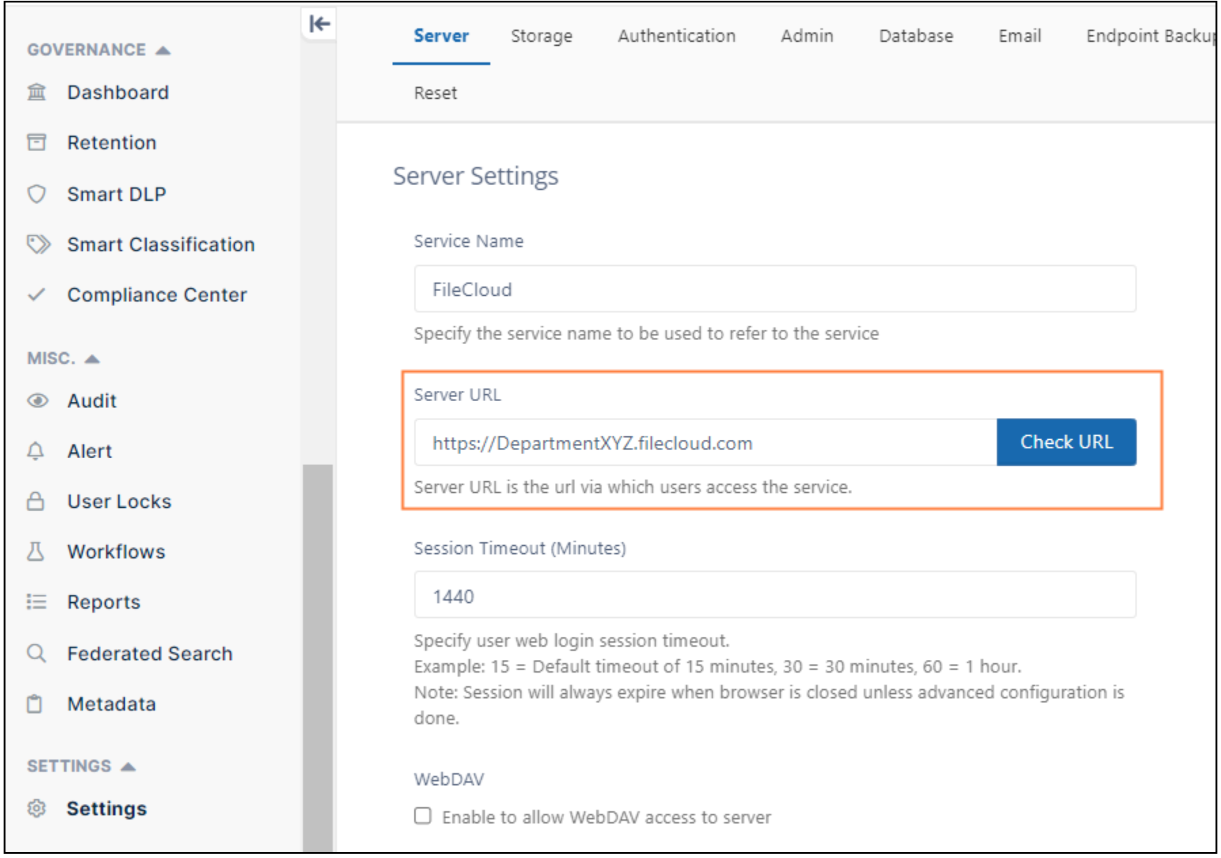
Linux	1. Go to the following directory:
	`/etc/apache2/sites-enabled/`
	2. Open the following file for editing:
	`000-default.conf`
	3. Add the following line within <VirtualHost *:80> for HTTP connection or <VirtualHost *.443> for HTTPS connection. You can place it under the line DocumentRoot /var/www/html.
	`Alias /simplesaml /var/www/html/thirdparty/simplesaml/www --→ (Ubuntu 16.04 and higher versions)`
	`Alias /simplesaml /var/www/thirdparty/simplesaml/www --→> (Ubuntu 14.04 and lower versions)`
	4. To restart the apache webserver, run the following command:
	`/etc/init.d/apache2 restart`

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.



Server Settings

Service Name

FileCloud

Specify the service name to be used to refer to the service

Server URL

https://DepartmentXYZ.filecloud.com Check URL

Server URL is the url via which users access the service.

Session Timeout (Minutes)

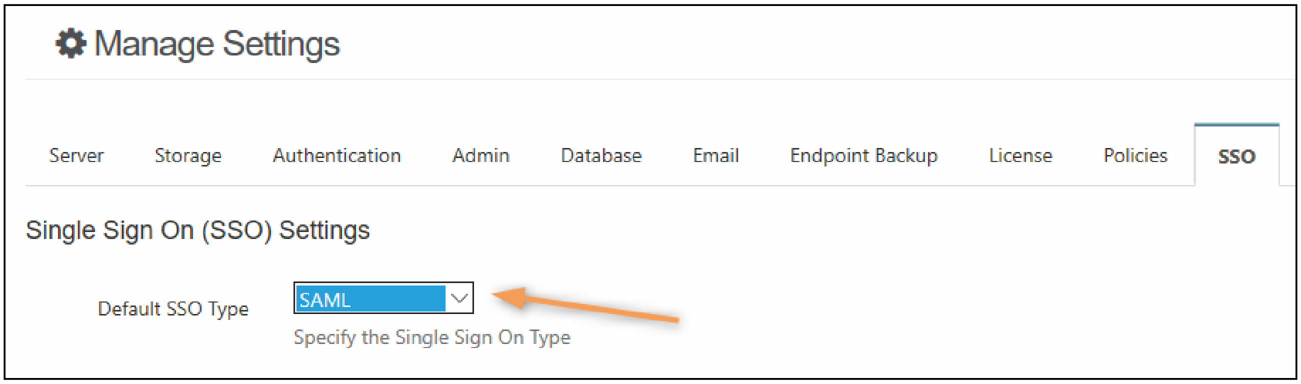
1440

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

☐ Enable to allow WebDAV access to server

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



Single Sign On (SSO) Settings

Default SSO Type SAML

Specify the Single Sign On Type

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.

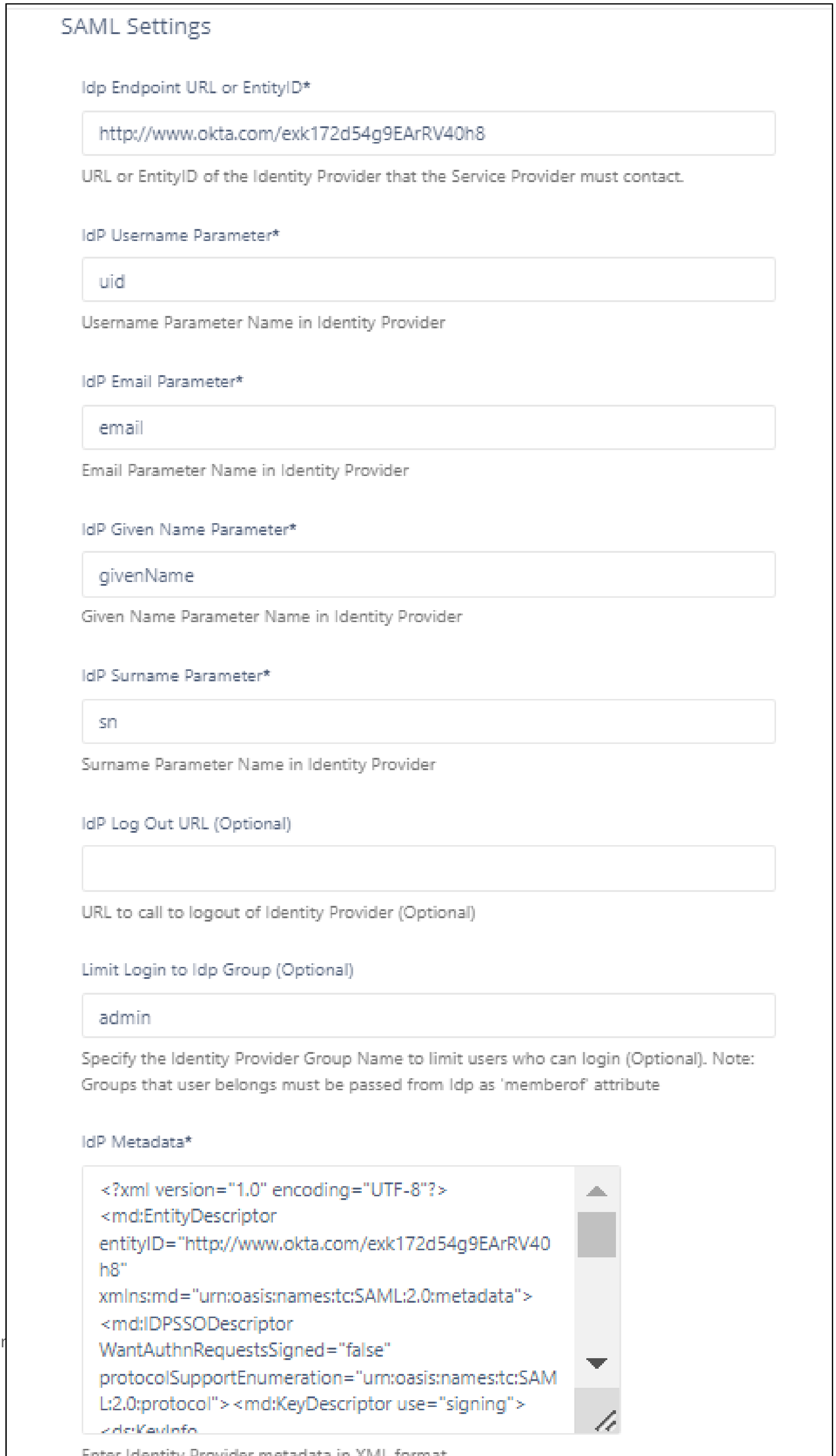
As a claims-aware application, FileCloud:

- 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*

http://www.okta.com/exk172d54g9EArRV40h8

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

IdP Username Parameter*

uid

Username Parameter Name in Identity Provider

IdP Email Parameter*

email

Email Parameter Name in Identity Provider

IdP Given Name Parameter*

givenName

Given Name Parameter Name in Identity Provider

IdP Surname Parameter*

sn

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)

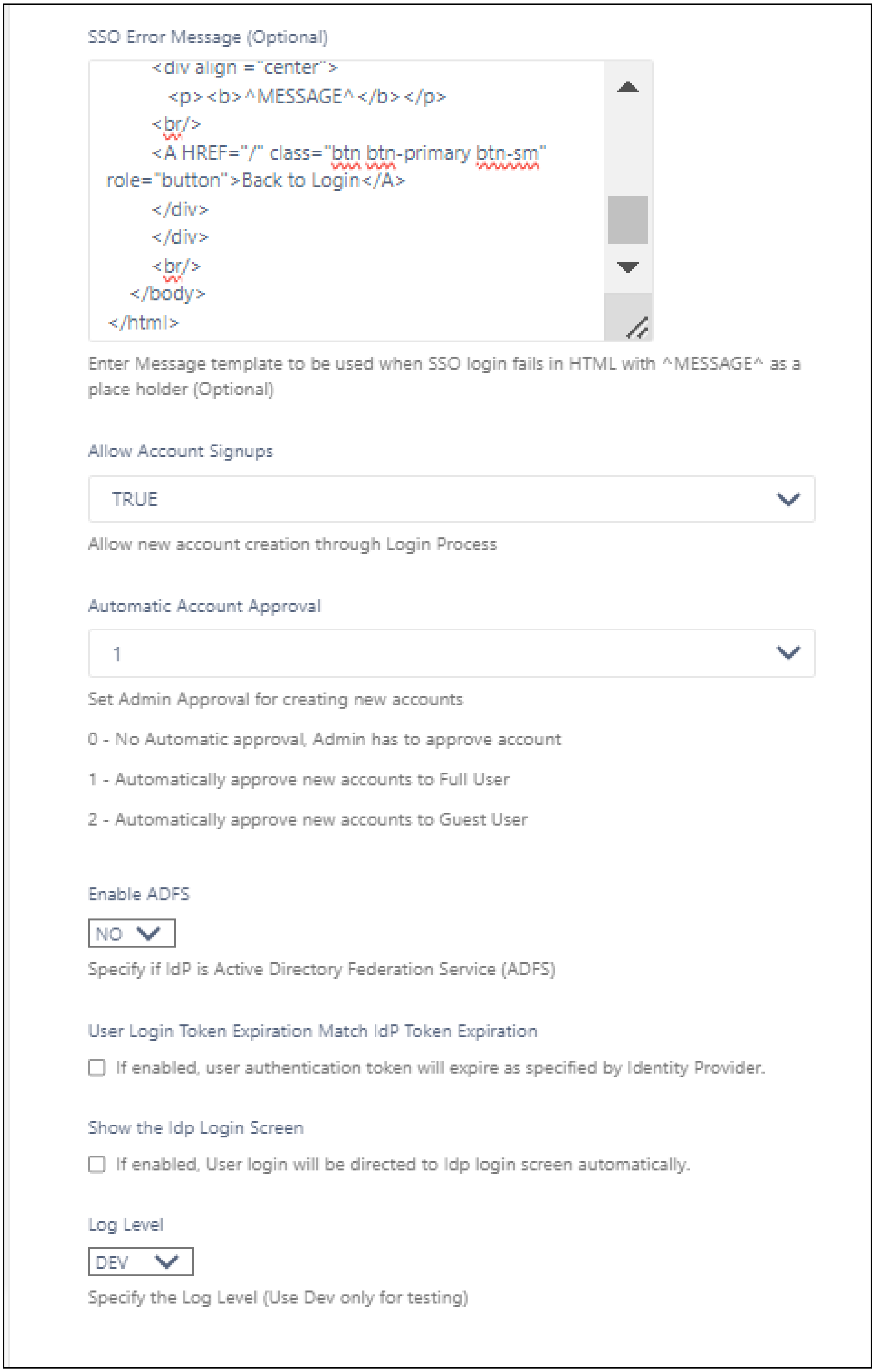
admin

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">
<ds: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.

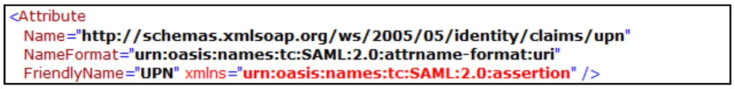
Log Level

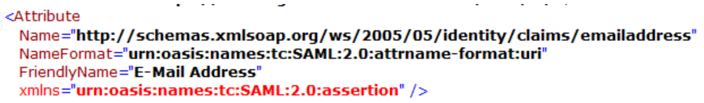
DEV

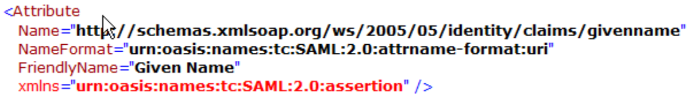
Specify the Log Level (Use Dev only for testing)

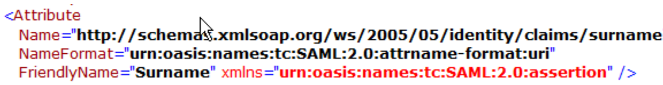
Use the following tables to understand the IdP settings.

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)
	• Usually uid or agencyUID
	• Default value: uid
	NOTE: The username must be unique. If username sent by Idp is in email format, the email prefix will be used for username. The email prefix in this case must be unique.
		Identifies the Username (must be unique for each user) Usually SAMAccountName or User Principal Name defined in claim rules.
		NOTE: The username must be unique. If username sent by Idp is in email format,
		the email prefix will be used for username. The email prefix in this case must be
		unique.
		value: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn or upn
		
		`<Attribute`
		`  Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"`
		`  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
		`  FriendlyName="UPN" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />`

IdP Email Parameter	Identifies the email of the user (must be unique)
	Default value: mail
		Identifies the email of the user (must be unique)
		http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress or emailaddress
		
		`<Attribute`
		`  Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"`
		`  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
		`  FriendlyName="E-Mail Address"`
		`  xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />`

IdP Given Name Parameter	Identifies the given name of the user
	Default value: givenName
		Identifies the given name of the user.
		http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname or givenname
		
		`<Attribute`
		`  Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"`
		`  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
		`  FriendlyName="Given Name"`
		`  xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />`

IdP Surname Parameter	Identifies the surname of the user
	Default value: sn
		Identifies the sur name of the user
		http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname or surname
		
		`<Attribute`
		`  Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"`
		`  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
		`  FriendlyName="Surname" xmlns="urn:oasis:names:tc:SAML:2.0:assertion" />`

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, you must also add a setting to the FileCloud config file: 1. Open the configuration file: Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php Linux: /var/www/config/cloudconfig.php 2. To make the **IdP Log Out URL** setting effective, add: `define("TONIDOCLOUD_SAML_SIGNED_LOGOUT", 1);`
Limit Logon to IdP Group (available in FileCloud Version 19.1 and higher)	IdP Group Name - Specifying a group name means that a user can login through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group - The IdP must send this group name through the *memberof* parameter - The *memberof* parameter can include a comma separated value of all groups to which the user belongs	IdP Group Name - Specifying a group name means that a user can login through SAML SSO only when the Identity Provider indicates that the user belongs to the specified IdP group - The IdP must send this group name through the *memberof* parameter - The *memberof* parameter can include a comma separated value of all groups to which the user belongs
Show the IdP Logon Screen	Identifies which Logon screen the user will see: - FileCloud screen = not selected - IdP screen = selected	Identifies which Logon screen the user will see: - FileCloud screen = not selected - IdP screen = selected
IdP Metadata	Identity Provider metadata in XML Format	Federation metadata in xml format

FileCloud Parameters	**IdP Settings**	**ADFS as IdP** **Data can be obtained from Federation Metadata**
SSO Error Message (Optional) Added in FileCloud 20.1	Custom error message that appears when a signin is invalid. Enter in HTML format. In a multiple IDP environment, this is the error message for the default IDP. To include a message specific to each IDP, include the parameter <MESSAGE>. See Integrating Multiple IDPs for help configuring multiple IDPs with error messages specific to each one..	Custom error message that appears when a signin is invalid. Enter in HTML format. In a multiple IDP environment, this is the error message for the default IDP. To include a message specific to each IDP, include the parameter <MESSAGE>. See Integrating Multiple IDPs for help configuring multiple IDPs and error messages specific to each one.
Allow Account Signups Added in FileCloud 20.1	When TRUE, during the login process, if the user account does not exists, a new FileCloud user account is created automatically.	When TRUE, during the login process, if the user account does not exists, a new FileCloud user account is created automatically.

FileCloud Parameters	**IdP Settings**	**ADFS as IdP** **Data can be obtained from Federation Metadata**
Automatic Account Approval Added in FileCloud 20.1	This setting works with the Allow Account Signups setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. • Possible values are: 0 - No Automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User See Integrating Multiple IDPs for help configuring multiple IDPs with automatic account approval settings specific to each one.	This setting works with the Allow Account Signups setting to determine: • If the account created by the user is disabled until the Administrator approves it • If the account is approved with a specific level of access automatically without intervention from the Administrator. • Possible values are: 0 - No Automatic approval, Admin has to approve account 1 - Automatically approve new accounts to Full User 2 - Automatically approve new accounts to Guest User 3 - Automatically approve new accounts to External User See Integrating Multiple IDPs for help configuring multiple IDPs with automatic account approval settings specific to each one.
Enable ADFS	No	Yes

FileCloud Parameters	**IdP Settings**	**ADFS as IdP** **Data can be obtained from Federation Metadata**
User login token expiration match Idp expiration	If enabled the user token expiration will be set based on Idp expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)	If enabled the user token expiration will be set based on ADFS expiration settings If not enabled user token expiration will be set based on FileCloud Session Timeout (FileCloud admin UI - Settings - Server - Session Timeout in Days) Default: No (Not enabled)
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	Set the Log mode for the SAML Calls. Default Value: prod (Do not use DEV for production systems)	Set the Log mode for the SAML Calls. Default Value: prod (Do not use DEV for production systems)

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

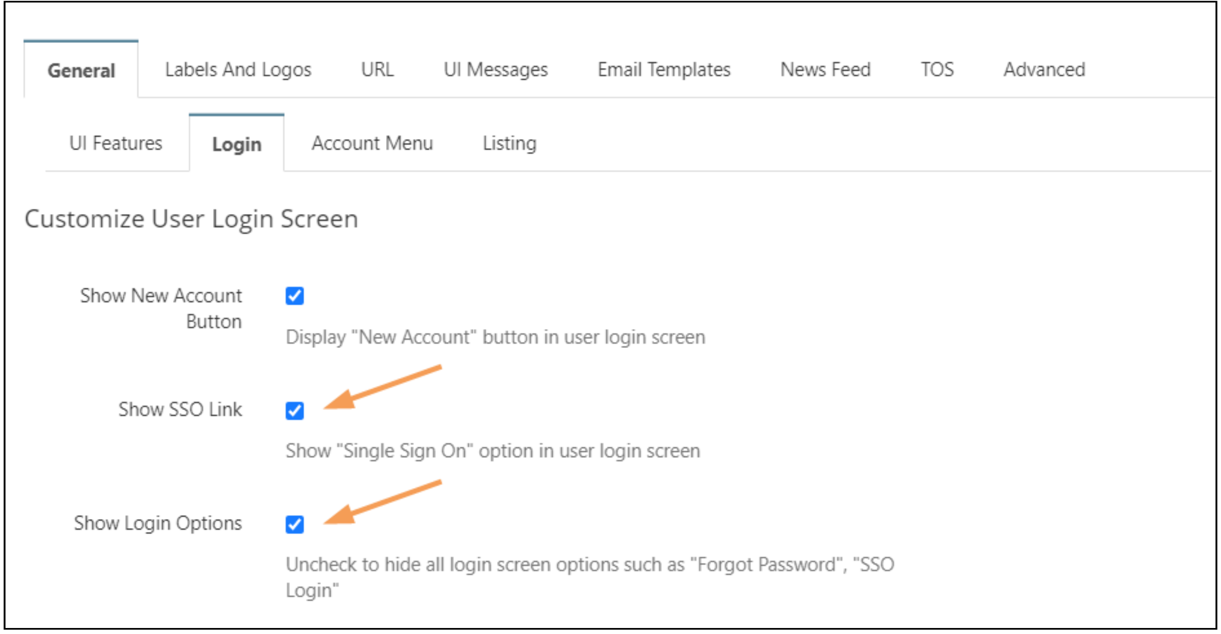
6. Enable Single Sign On Link on the login page.

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**.



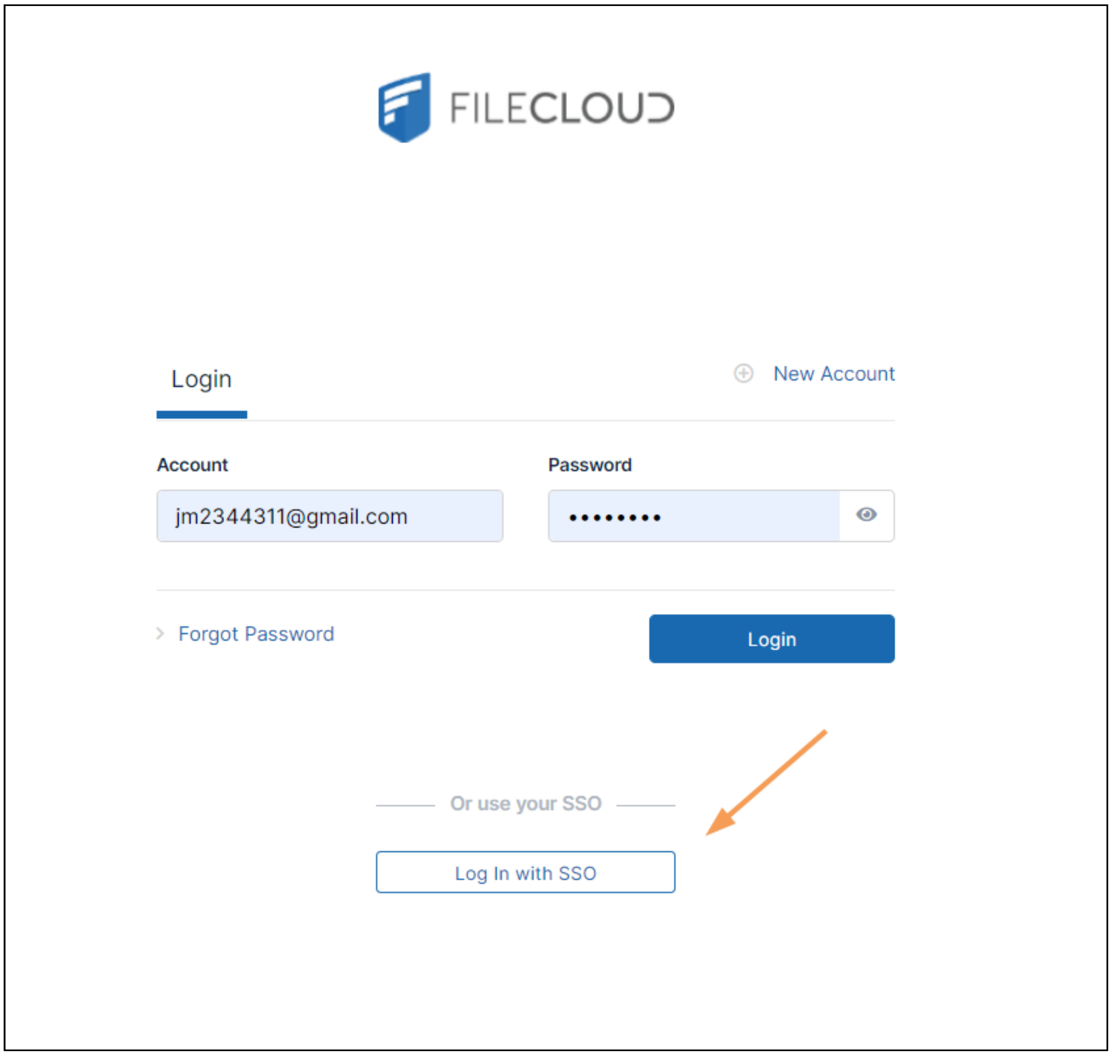
Customize User Login Screen

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"

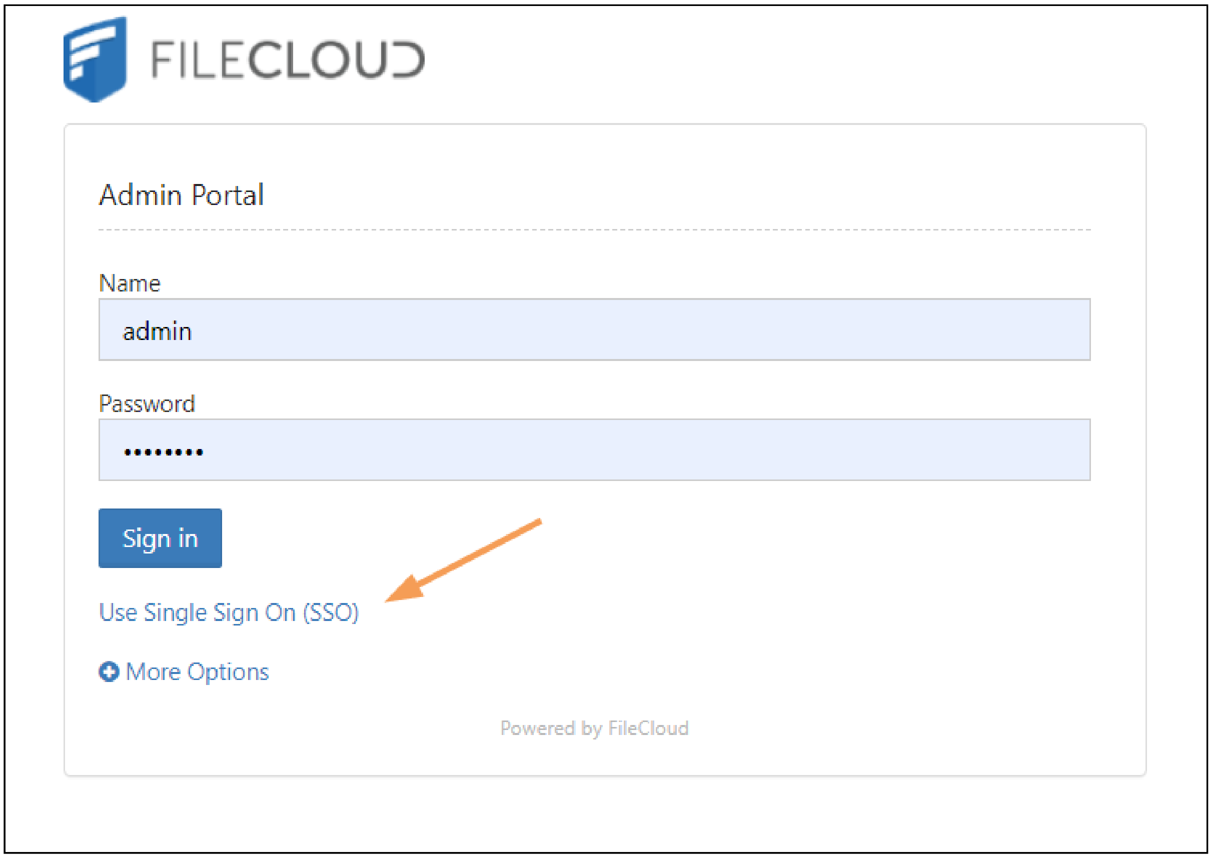
4. Save your changes.
   Now, when users access the user portal log-in page, they will see:



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

The SSO log-in option in the admin portal:

Starting with FileCloud 13.0, FileCloud admin interface also supports Single Sign-On.



Default admin portal log-in screen

To only display the SSO log-in option:

In order to skip the FileCloud login page and send the user directly to the SAML SSO page you must add a setting to the cloudconfig.php file, as shown below. You can configure this option for the user portal login page and the admin portal login page.

To only display the SSO log-in option in the user portal:
This configuration option is available starting with FileCloud Version 19.3, It supports skipping the login page when the user accesses FileCloud with a domain name or with a full URL.

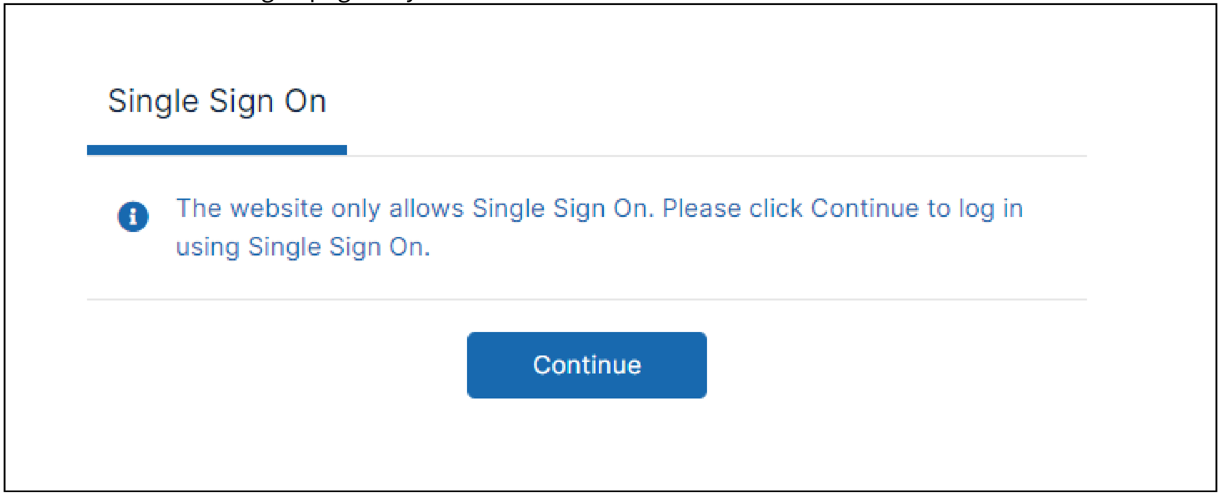
1. In the admin portal, go to **Customization,** and select the **General** tab, and then the **Login** sub-tab.
2. Check **Show SSO Link** and **Show Login Options**, and save your changes.
3. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
4. To only display the SSO log-in option:

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

ⓘ An earlier version of this option is also effective in version of FileCloud prior to 19.3, but this redirect is only effective if the user specifies a domain name rather than a full URL. Instead of the above setting, use:

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

When users enter the log-in page they will see:



Single Sign On

The website only allows Single Sign On. Please click Continue to log in using Single Sign On.

To return to displaying other log-in options:

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

To display only SSO log-in in the admin portal:

Starting with Version 20.1, FileCloud supports skipping the login page when the admin accesses FileCloud with a domain name or with a full URL.

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. To only display the SSO log-in option:

Enter:

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

An earlier version of this option is also effective in versions of FileCloud prior to 20.1, but this redirect is only effective if the user specifies a domain name rather than a full URL. Instead of the above setting, use:

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

7. Enable secure cookies for SimpleSAML

To enable secure cookies when using SimpleSAML to authenticate, proceed on the following.

1. Open the SimpleSAML configuration file:
   Windows: XAMPP DIRECTORY/htdocs/thirdparty\simplesaml\config\config.php
   Linux: /var/www/config/thirdparty/simplesaml/config/config.php

2. Change **session.cookie.secure** from **FALSE** to **TRUE**:

   ```
   'session.cookie.secure' => true,
   ```

3. (Optional) For better cookie security set the **session.cookie.samesite** attribute to **Strict** or **Lax** according to the environment's needs.
   If the FileCloud site is embedded in an external site, it may be necessary to leave this setting null or set it to **None** to enable cookie sharing with the external site.

   ```
   'session.cookie.samesite' => 'Strict',
   ```

8. Best Practices

Issue	Details

Avoid Open Redirect	FileCloud may be vulnerable to an open redirect when SSO is implemented.
	• An open redirect is an application vulnerability that takes a parameter and redirects the user to the supplied parameter value without any validation.
	This can be avoided by configuring the following setting:
	1. Navigate to the following directory:
	`<FileCloud WEB ROOT>/thirdparty/simplesaml/config`
	2. Open the following file for editing:
	`config.php`
	3. Add the following line:
	`'trusted.url.domains' => array()`

Restrict the Available Admin Login Resources	The FileCloud admin portal can possibly allow 2 administrative login interfaces: • One at admin API interface: /admin • One at simpleSAML admin resource: /simpleSAML. This can be avoided by changing the log level to "PROD" in SSO settings under settings in FileCloud admin interface. This will disable the SSO admin page under simpleSAML. The password to the SSO admin page under /simpleSAML can be changed under 'auth.adminpassword' key in <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php

9. Troubleshooting

Use the following table to read about issues that you may encounter and how to resolve them.

Issue	Solution
FileCloud is hosted behind a Proxy	When FileCloud is hosted behind a proxy server, SAML will not automatically work. Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/filecloudconfig.php Add Proxy Server Information here. Format is as follows user:password@yourproxyserverurl.com define("TONIDOCLOUD_SAML_PROXY", "ADD PROXY INFO HERE");
System Timezone Settings	After setting SAML log level to DEV. Log file will be created under <FileCloud WEB ROOT>/thirdparty/simplesaml/log/simplesamlphp.log SimpleSAML_Error_Exception: Error 2 - strftime(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. Solution: date.timezone setting must be set explicitly in php.ini
FileCloud is hosted behing a reverse proxy	When FileCloud is hosted behind a proxy server, SAML will not automatically work. Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php set the base url to 'baseurlpath' => 'http(s)://YOURFILECLOUDOMAIN/simplesaml/'
Debug page login	https://YOURFILECLOUDDOMAIN/simplesaml/module.php/core/frontpage_welcome.php

Issue	Solution
FileCloud in HA (High Availability) envrionment with multiple servers	In this scenario, SimpleSAML will most likely not work with default configuration and will require to run Memcache to manage the session. Go to <FileCloud WEB ROOT>/thirdparty/simplesaml/config/config.php set the store.type => memcache and set 'memcache_store.servers' => array(array(array('hostname' => 'localhost'),),), where 'localhost' must be replaced with IP of memcache server as appropriate.
Autofill Username or Email on the IDP screen when configured TONIDOCLOUD_SAML_DOMAINS_ALLOWED	When autofill will only work when username or email address is sent through POST from the FileCloud login page to IDP. Therefore, ensure that the IDP metadata accepts requests through only POST. For example, if the Idp Metadata contains the following 2 similar lines, remove the Redirect and only have the POST <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://mailinator-raja.okta.com/app/mailinatororg747392_myidp_1/exkgimvocj18Exx9g4x6/sso/saml"/> <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://mailinator-raja.okta.com/app/mailinatororg747392_myidp_1/exkgimvocj18Exx9g4x6/sso/saml"/>

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
- Integrating Multiple IDPs
- Integrate Ping Identity SSO with Filecloud
- Setting Up and Configuring Certificates when Upgrading SSO

Override the default SSO port

In FileCloud Versions 19.3 and higher, you can override the default SSO port.

To override the default port:

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

```
define("TONIDOCLOUD_SSO_FULLURL_OVERRIDE", "https://filecloud.test.com");
```

Use multiple memcache servers

In FileCloud Versions 20.3.2 and higher, you can use multiple memcache servers with SAML SSO to achieve high availability.

To use multiple memcache servers:

1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the following lines, including a hostname for each of the memcache servers.
   In this example, the IP addresses of the servers are 79.97.83.70 and 79.97.83.71.

```
function SSO_MEMCACHED_SERVERS() {
return [
[
['hostname' => '79.97.83.70'],
['hostname' => '79.97.83.71'],
],
];
}
```

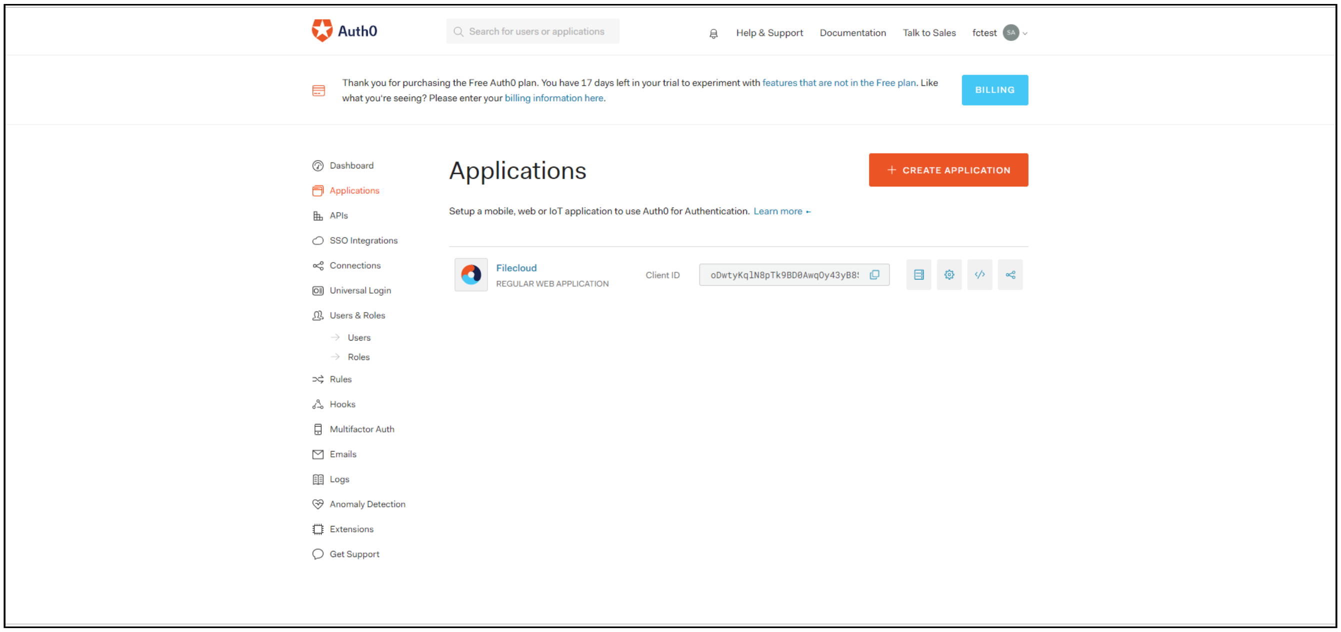
Integrate Auth0 SSO with Filecloud

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



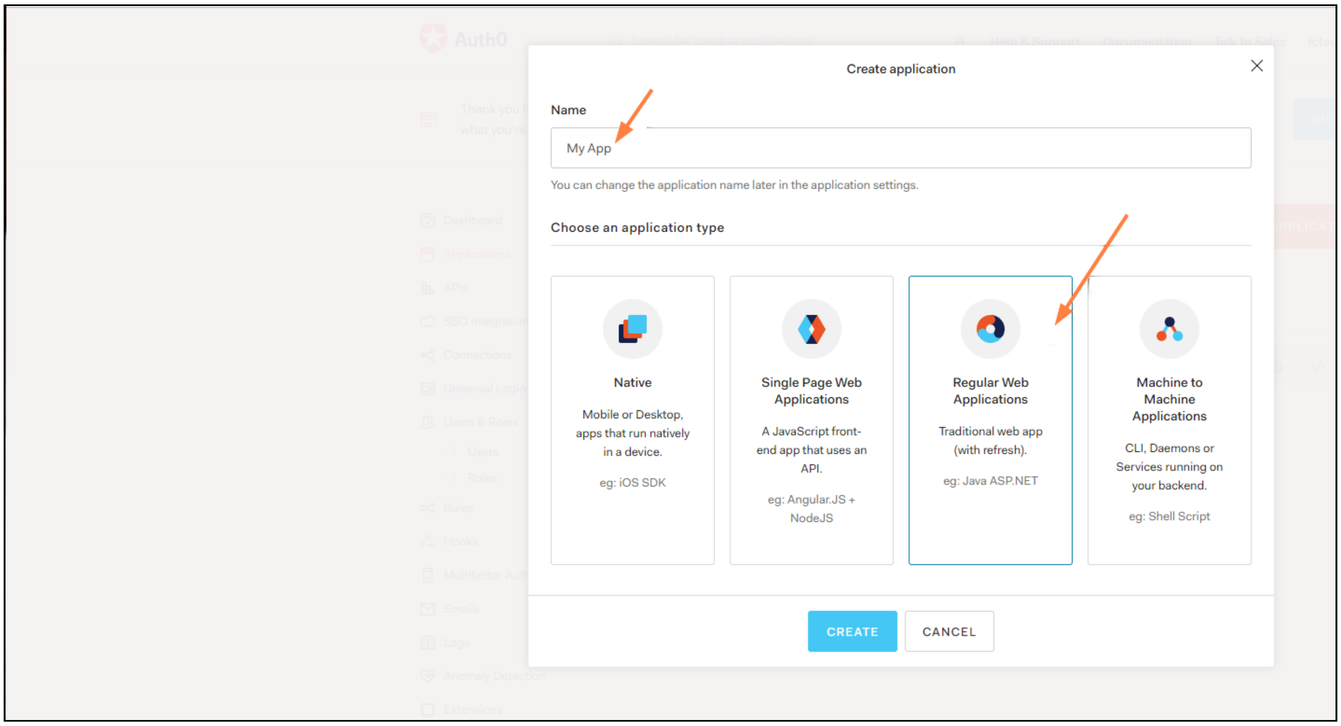
Thank you for purchasing the Free Auth0 plan. You have 17 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. Learn more

Filecloud
REGULAR WEB APPLICATION
Client ID oDwtyKq1N8pTk9BD0Awq0y43yB8!

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



Create application

Name

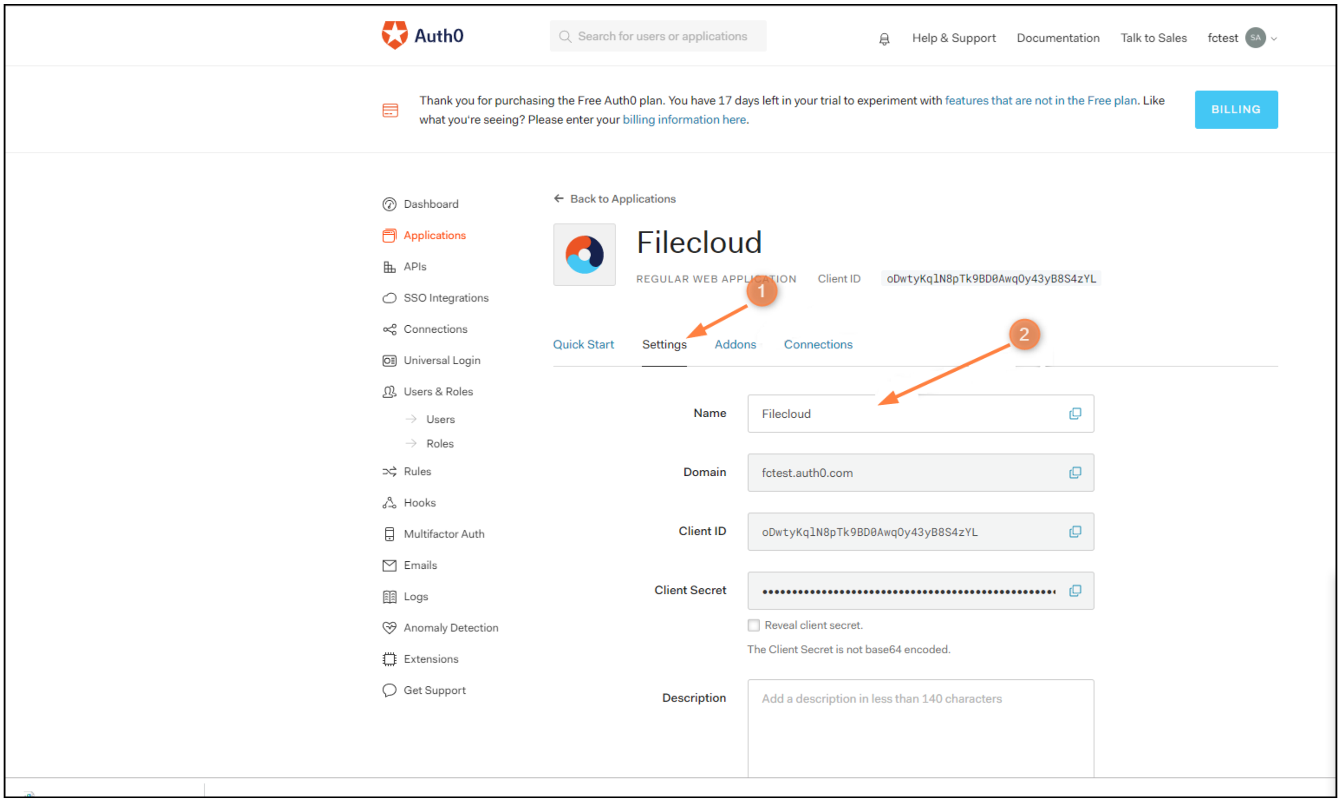
My App

You can change the application name later in the application settings.

Choose an application type

Native	Single Page Web Applications	Regular Web Applications	Machine to Machine Applications
Mobile or Desktop, apps that run natively in a device.	A JavaScript front-end app that uses an API.	Traditional web app (with refresh).	CLI, Daemons or Services running on your backend.
eg: iOS SDK	eg: Angular.JS + NodeJS	eg: Java ASP.NET	eg: Shell Script

- 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



Thank you for purchasing the Free Auth0 plan. You have 17 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Filecloud

REGULAR WEB APPLICATION   Client ID   oDwtyKqlN8pTk9BD0Awq0y43yB8S4zYL

Name: Filecloud

Domain: fctest.auth0.com

Client ID: oDwtyKqlN8pTk9BD0Awq0y43yB8S4zYL

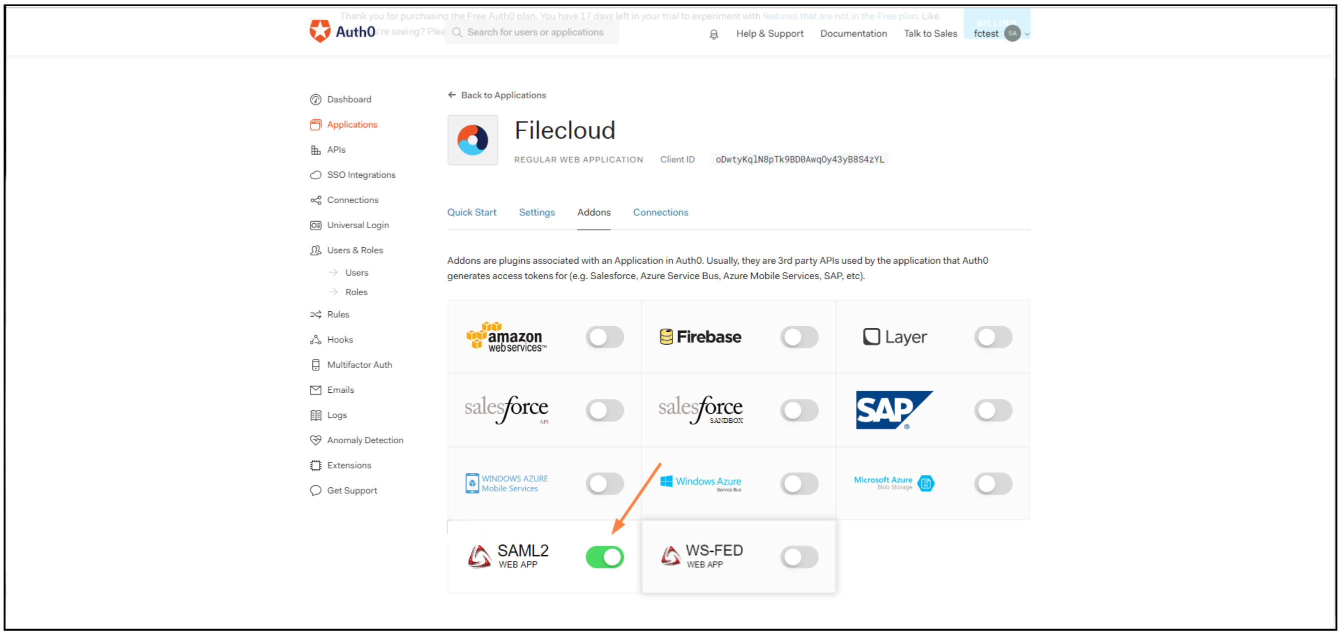
Client Secret: ••

□ Reveal client secret.

The Client Secret is not base64 encoded.

Description: Add a description in less than 140 characters

- Click on SAML2 (Web App)

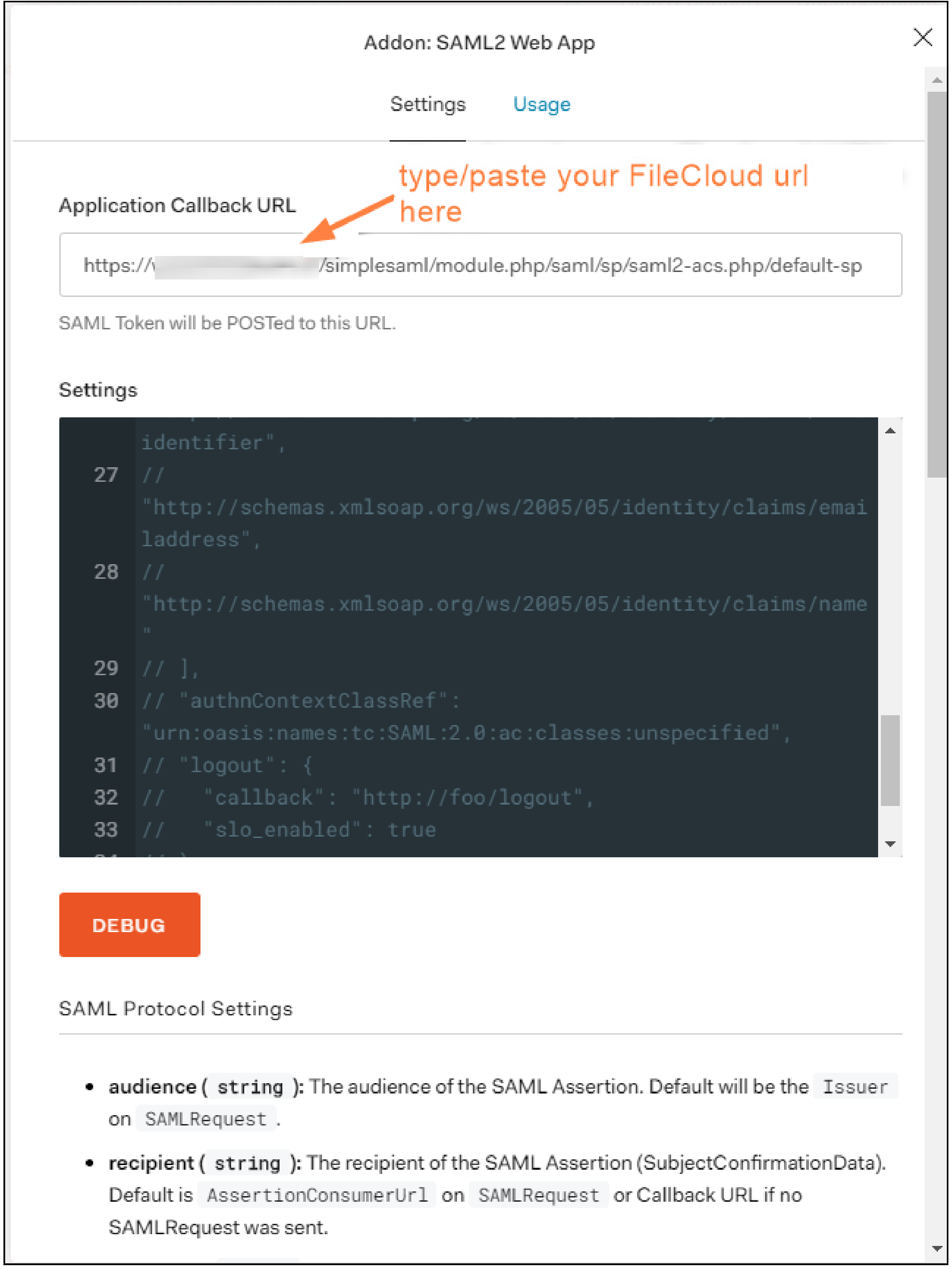


Filecloud

REGULAR WEB APPLICATION Client ID oDwtyKqlN8pTk9BD0AwqOy43yB8S4zYL

Addons are plugins associated with an Application in Auth0. Usually, they are 3rd party APIs used by the application that Auth0 generates access tokens for (e.g. Salesforce, Azure Service Bus, Azure Mobile Services, SAP, etc).

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



Application Callback URL

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

SAML Token will be POSTed to this URL.

Settings

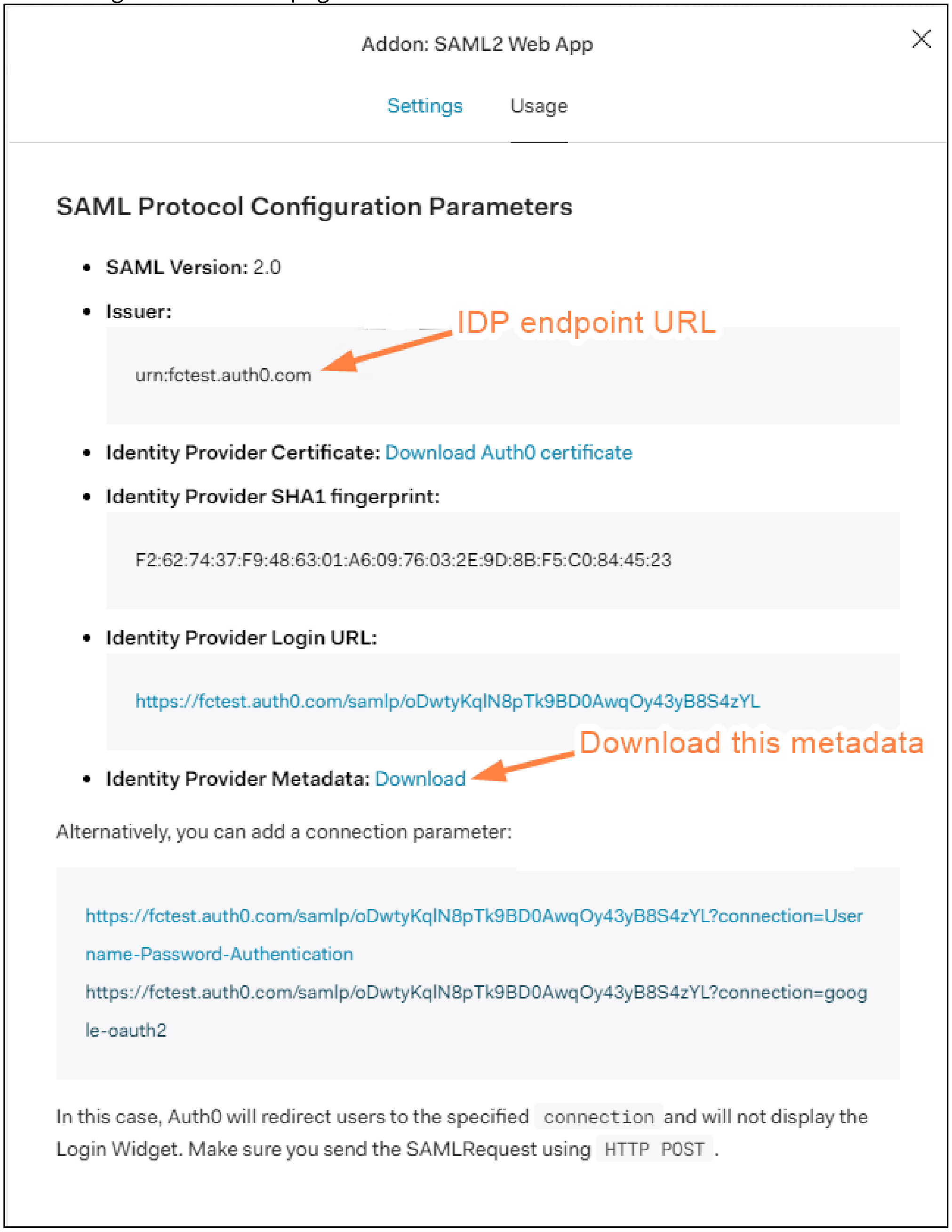
```
identifier",
//
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
//
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
// ],
// "authnContextClassRef":
"urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified",
// "logout": {
//   "callback": "http://foo/logout",
//   "slo_enabled":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

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.



SAML Protocol Configuration Parameters

- **SAML Version:** 2.0
- **Issuer:**

```
urn:fctest.auth0.com
```

- **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/oDwtyKqlN8pTk9BD0AwqOy43yB8S4zYL
```

- **Identity Provider Metadata:** Download

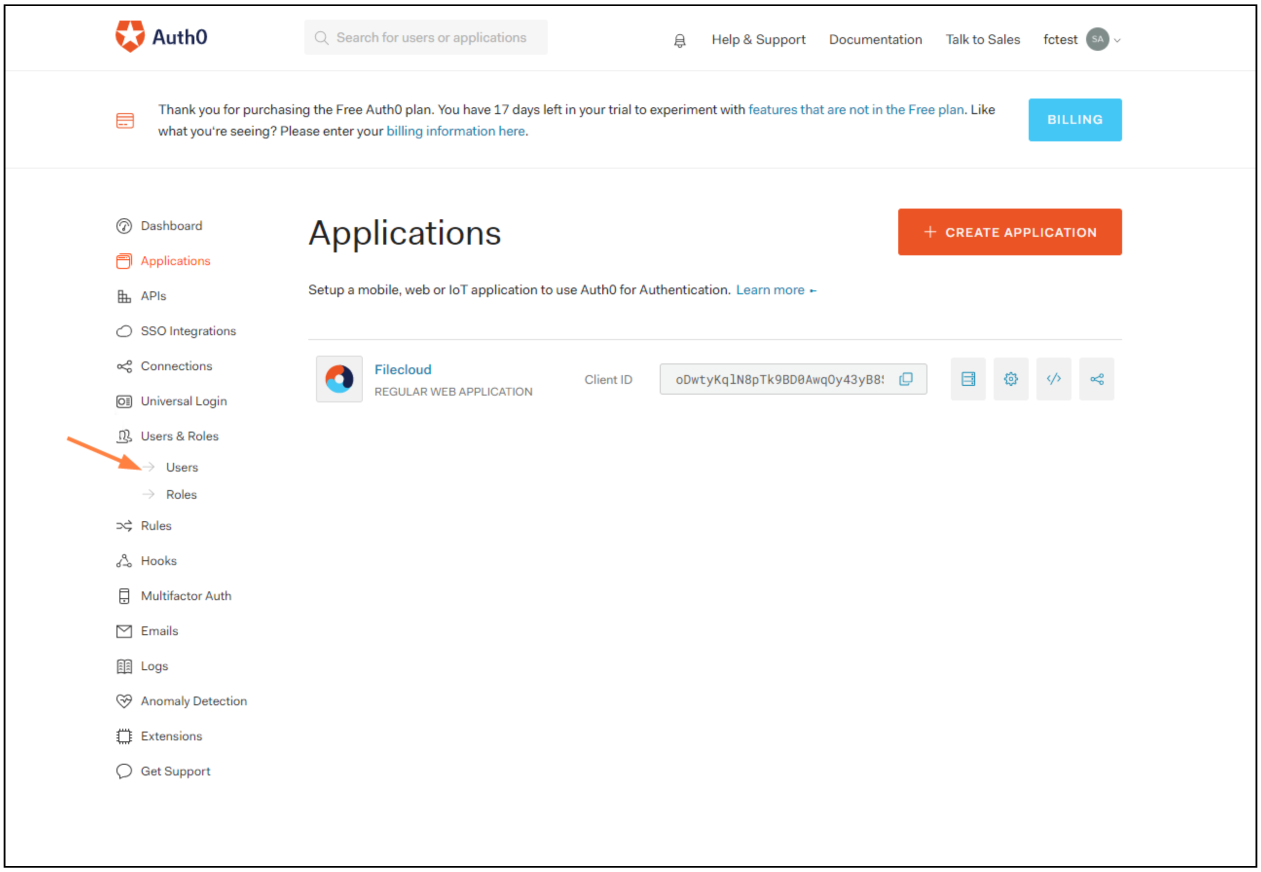
Alternatively, you can add a connection parameter:

```
https://fctest.auth0.com/samlp/oDwtyKqlN8pTk9BD0AwqOy43yB8S4zYL?connection=Username-Password-Authentication
https://fctest.auth0.com/samlp/oDwtyKqlN8pTk9BD0AwqOy43yB8S4zYL?connection=google-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.



Thank you for purchasing the Free Auth0 plan. You have 17 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here.

Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. Learn more ←

Filecloud
REGULAR WEB APPLICATION

Client ID oDwtyKqlN8pTk9BD0AwqOy43yB8!

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)

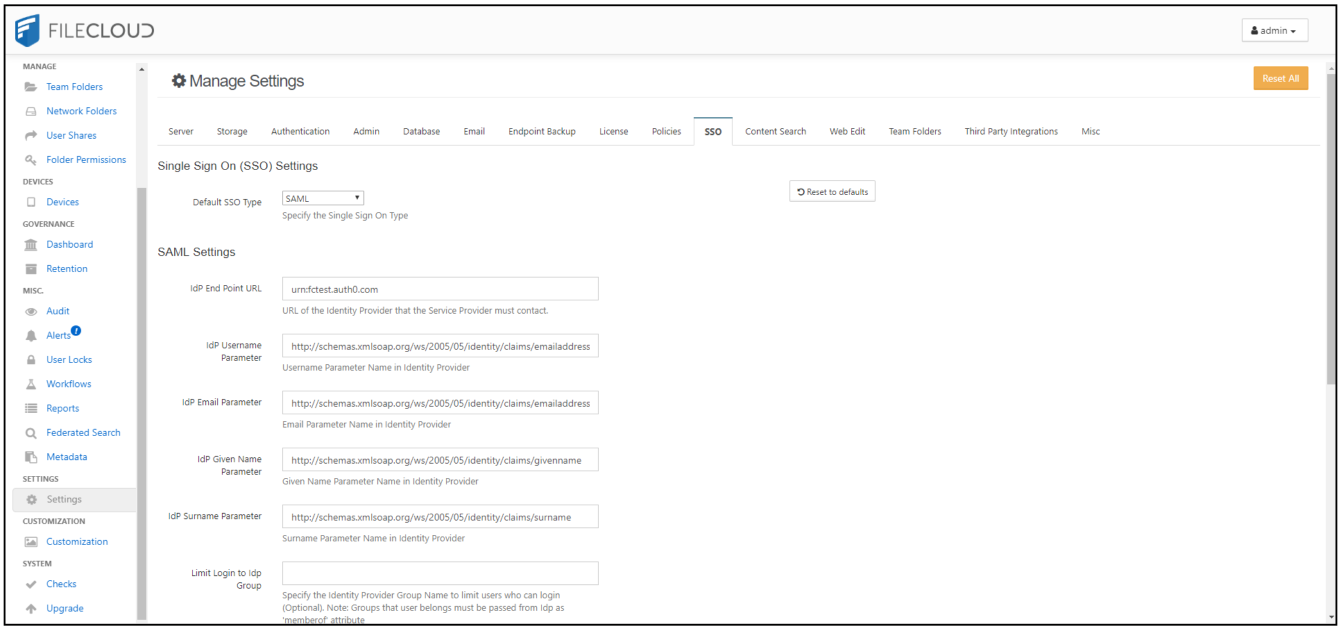
IdP Username Parameter : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

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.



Single Sign On (SSO) Settings

Default SSO Type: SAML
Specify the Single Sign On Type

SAML Settings

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

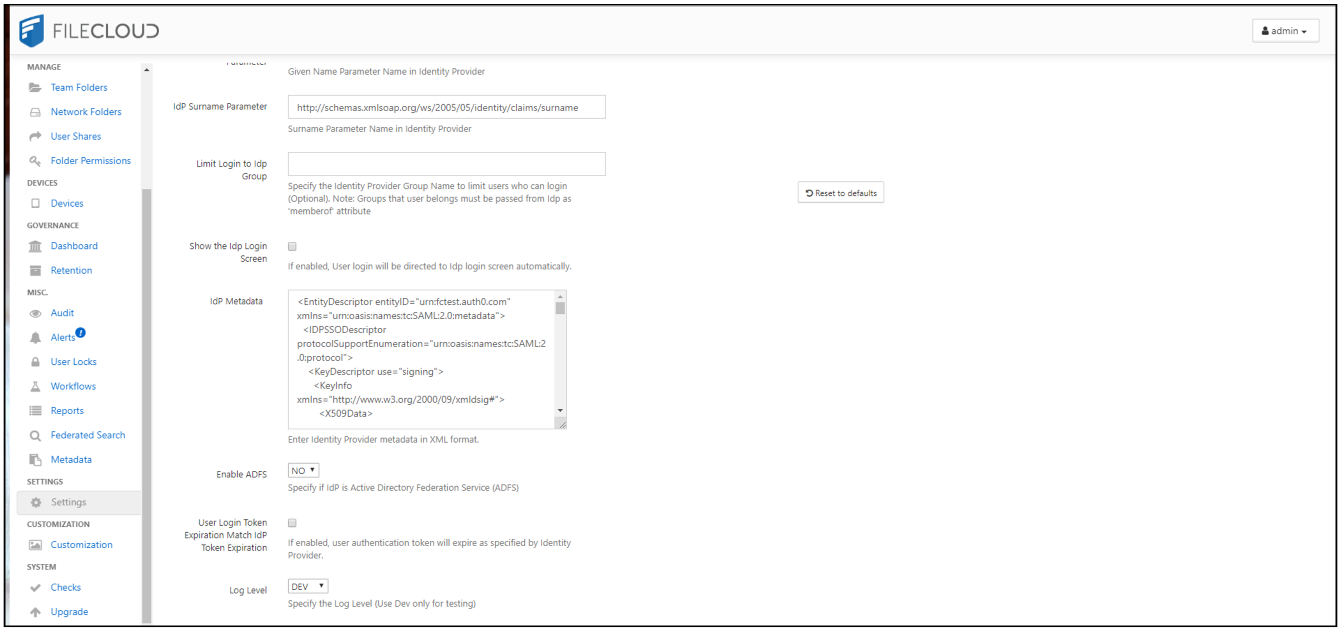
IdP Username Parameter: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Username Parameter Name in Identity Provider

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



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

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

IdP Metadata:

```
<EntityDescriptor entityID="urn:fctest.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>
```

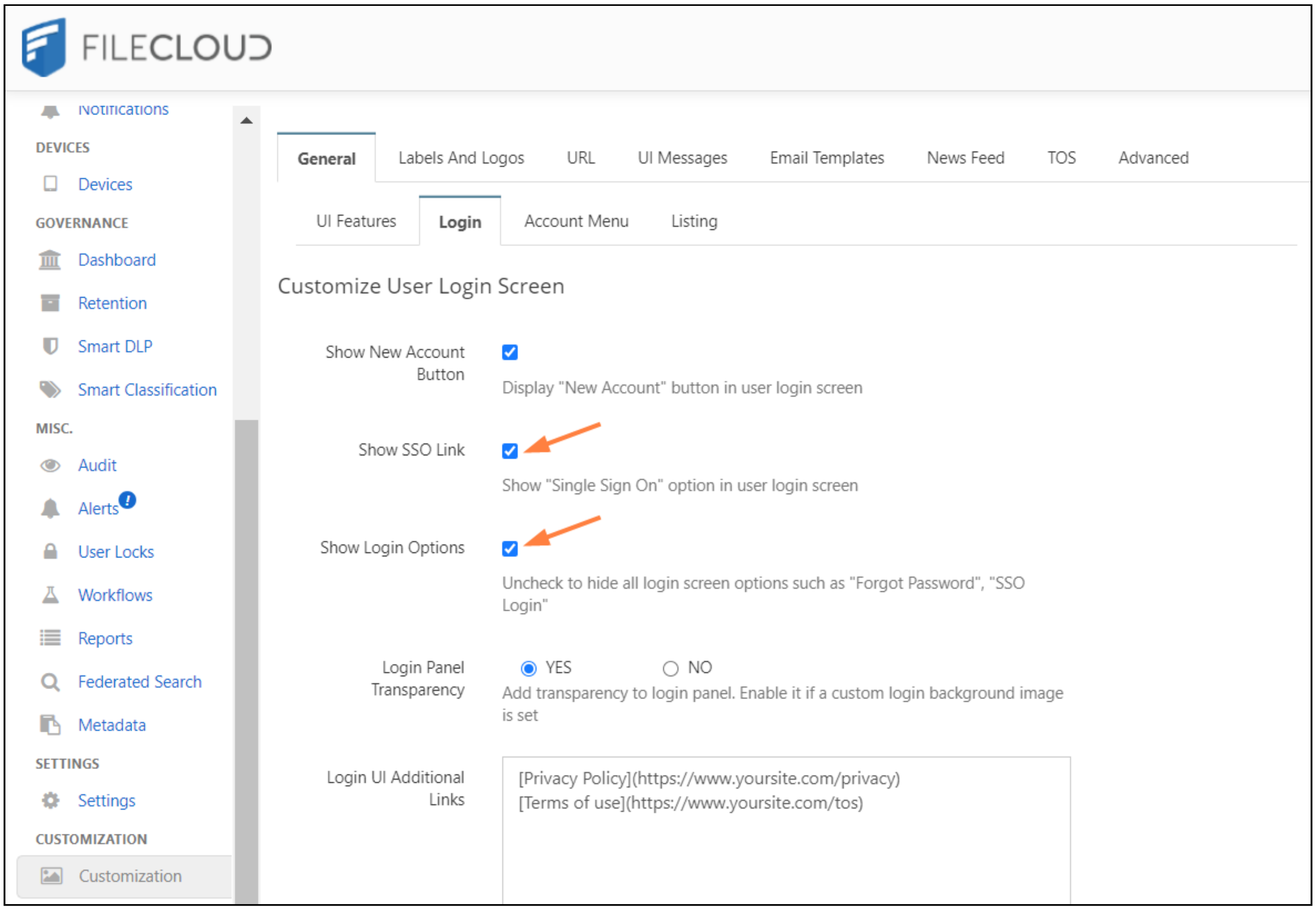
Enter Identity Provider metadata in XML format.

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**.



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

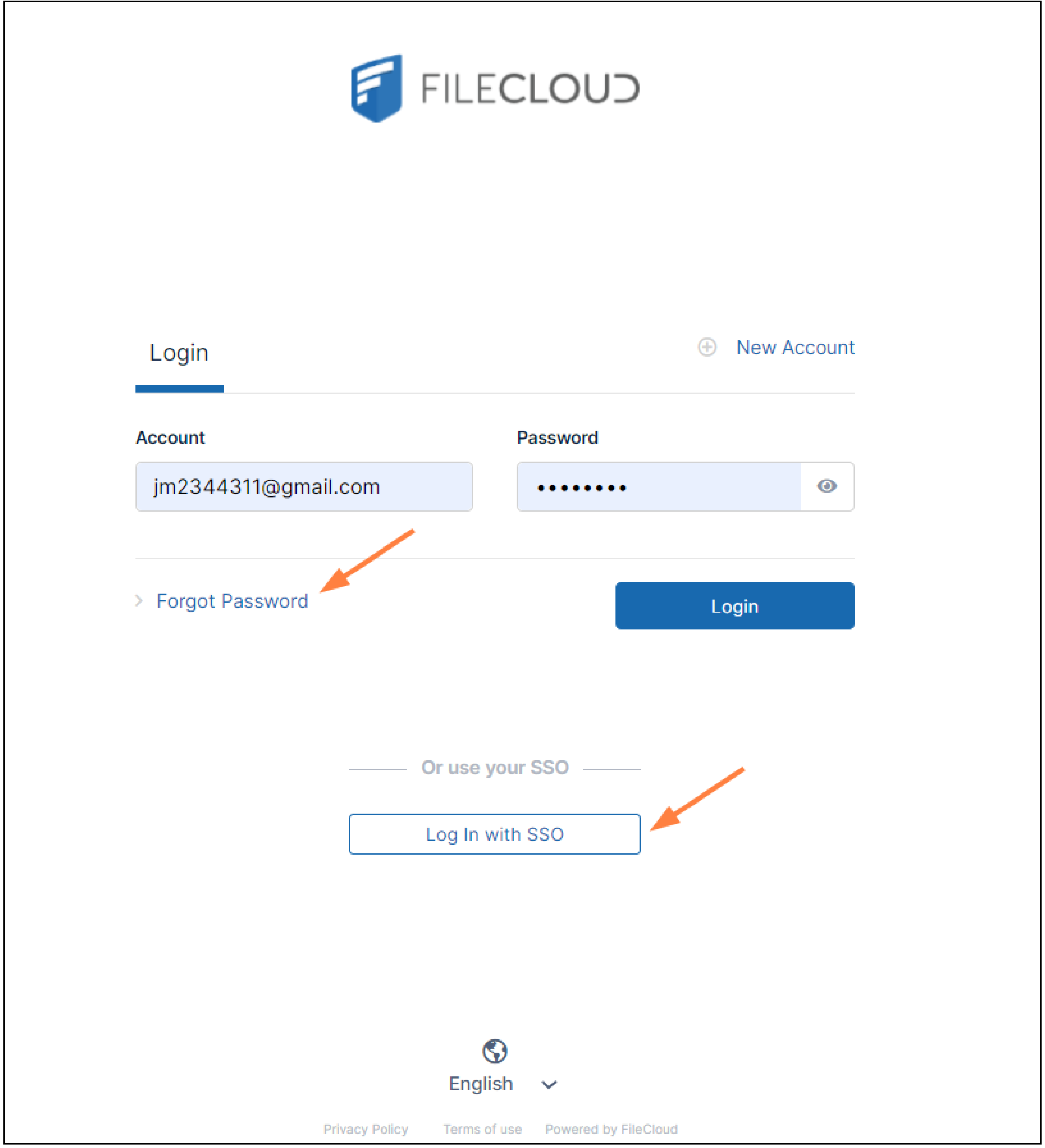
Show Login Options ☑
Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

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.



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.

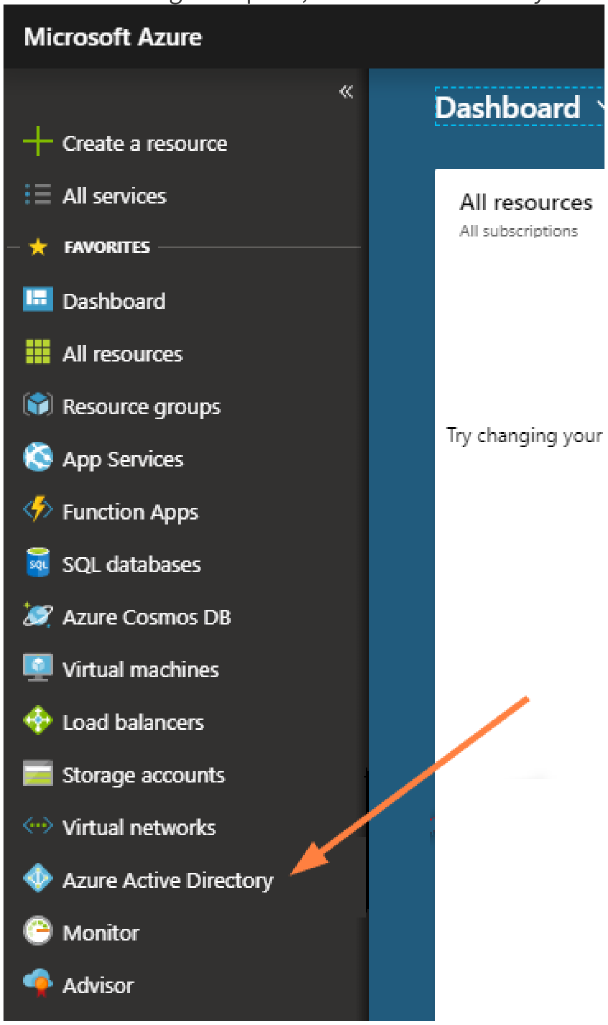
Note: Azure AD can only be integrated if FileCloud has an SSL certificate in place, as Microsoft requires HTTPS URLs when configuring FileCloud in Azure.

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)

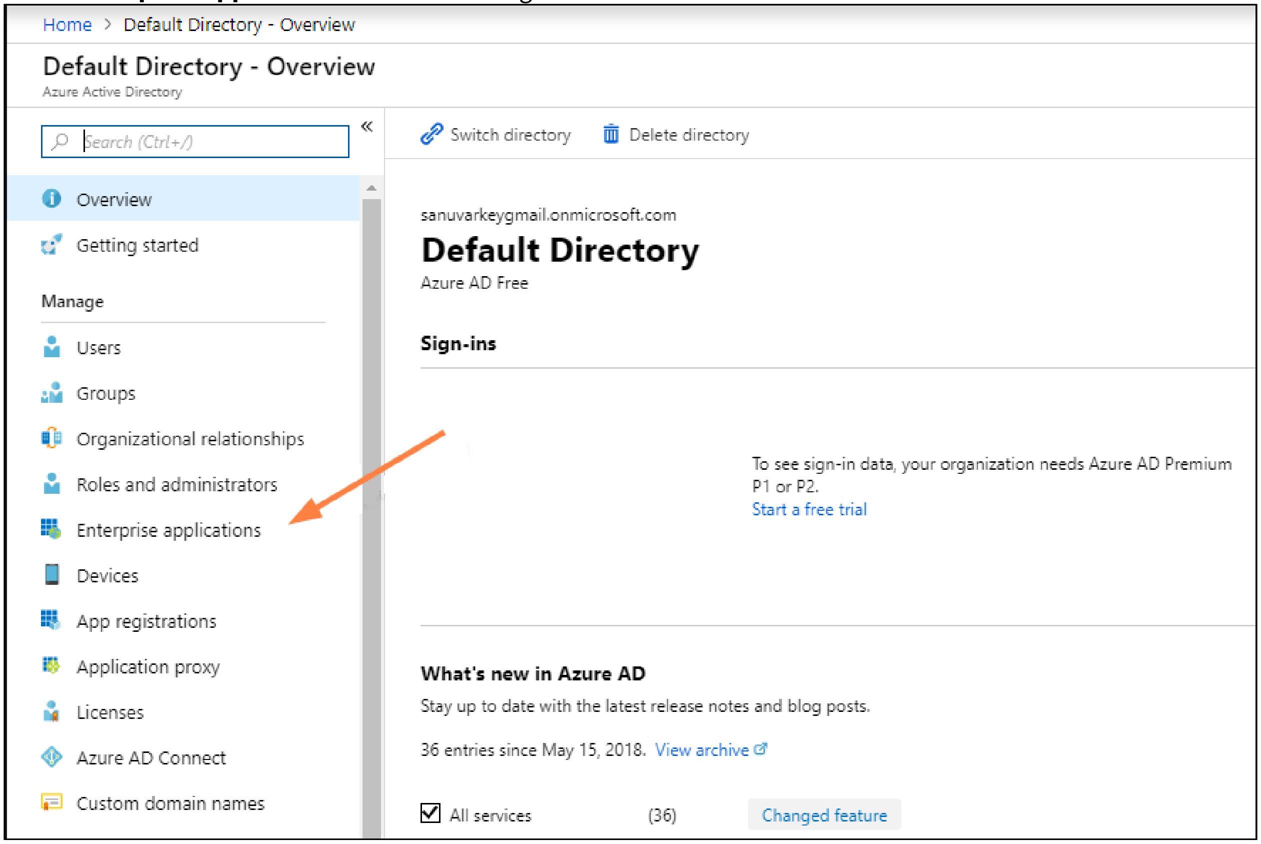
To integrate Azure AD with FileCloud:

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

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

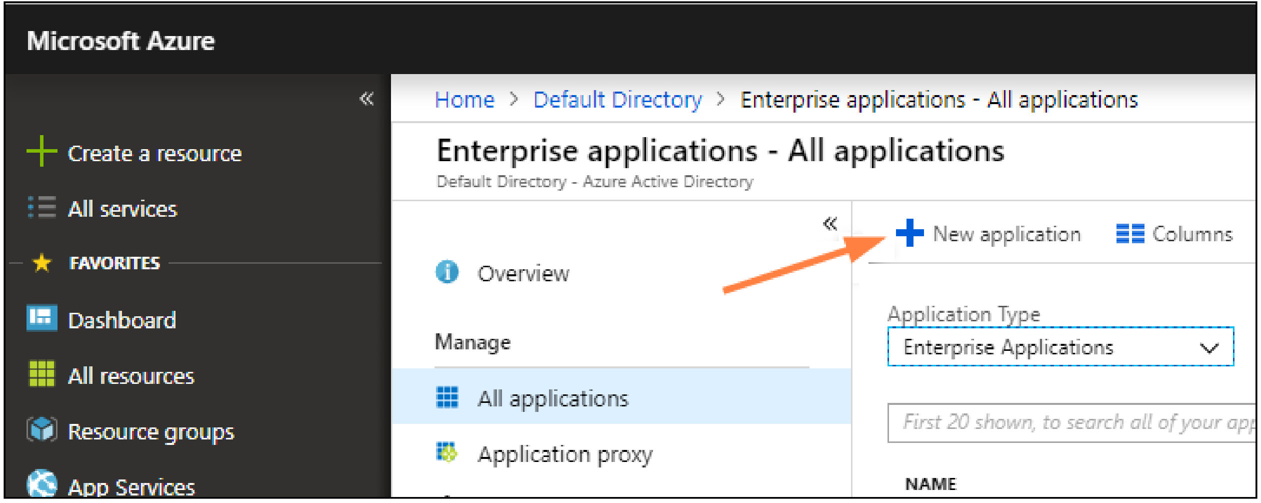
What's new in Azure AD

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**.



Home > Default Directory > Enterprise applications - All applications

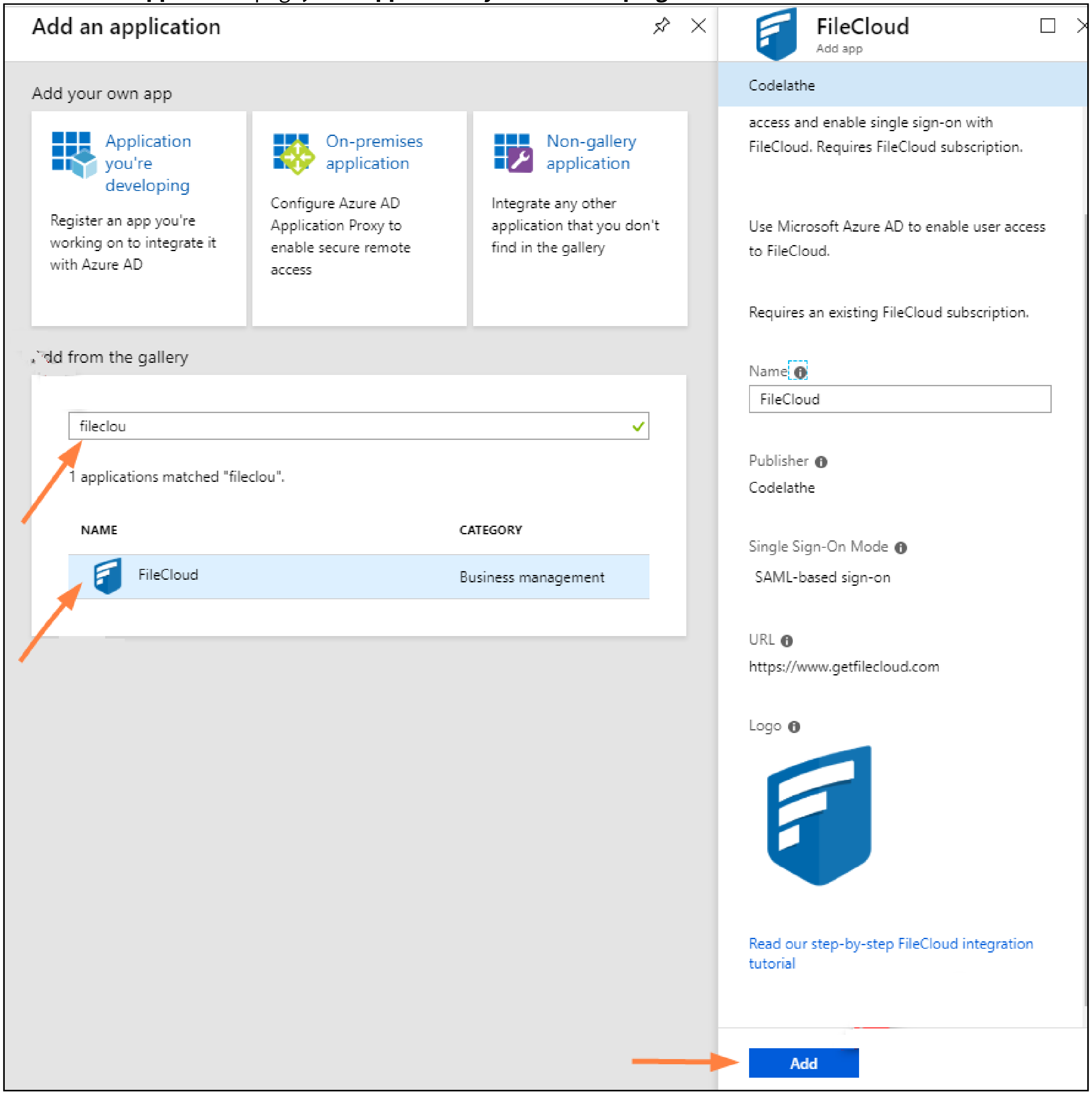
Enterprise applications - All applications
Default Directory - Azure Active Directory

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

fileclou

1 applications matched "fileclou".

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

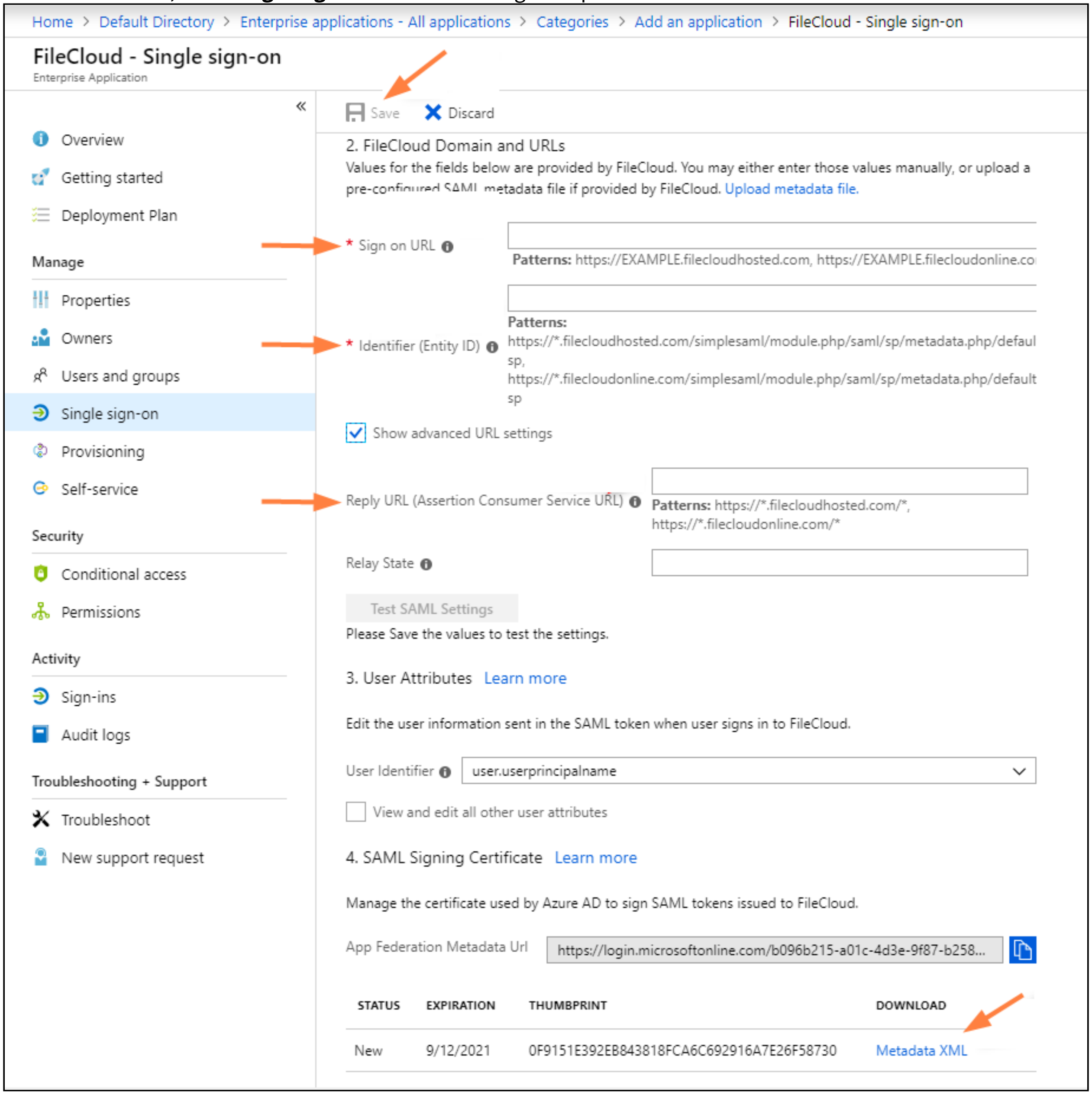
URL: https://www.getfilecloud.com

Logo

Read our step-by-step FileCloud integration tutorial

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

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.co

* 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

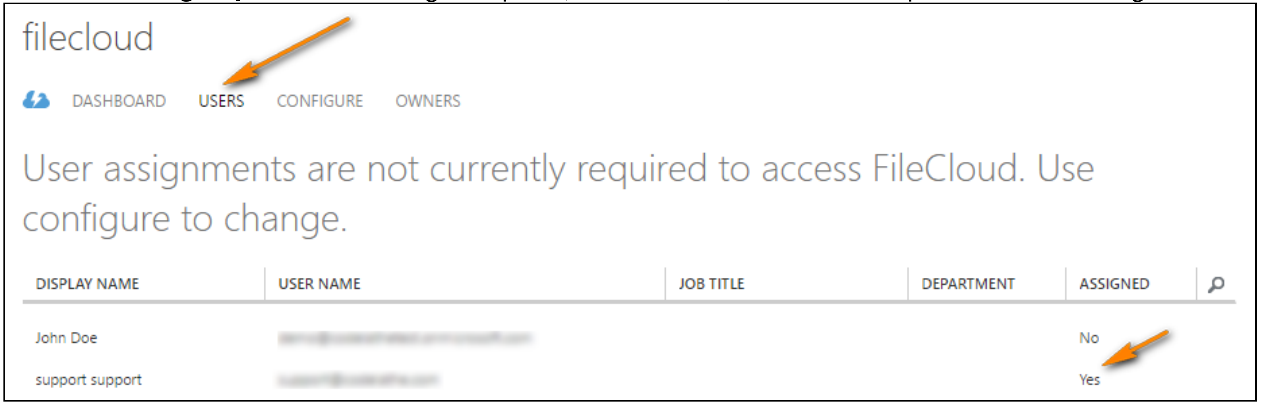
Manage the certificate used by Azure AD to sign SAML tokens issued to FileCloud.

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.



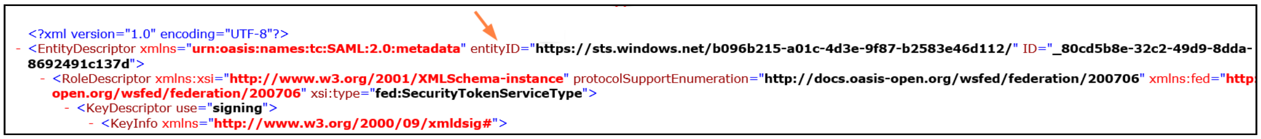
User assignments are not currently required to access FileCloud. Use configure to change.

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ASSIGNED
John Doe	[redacted]			No
support support	[redacted]			Yes

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 UR**L, 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#">
```

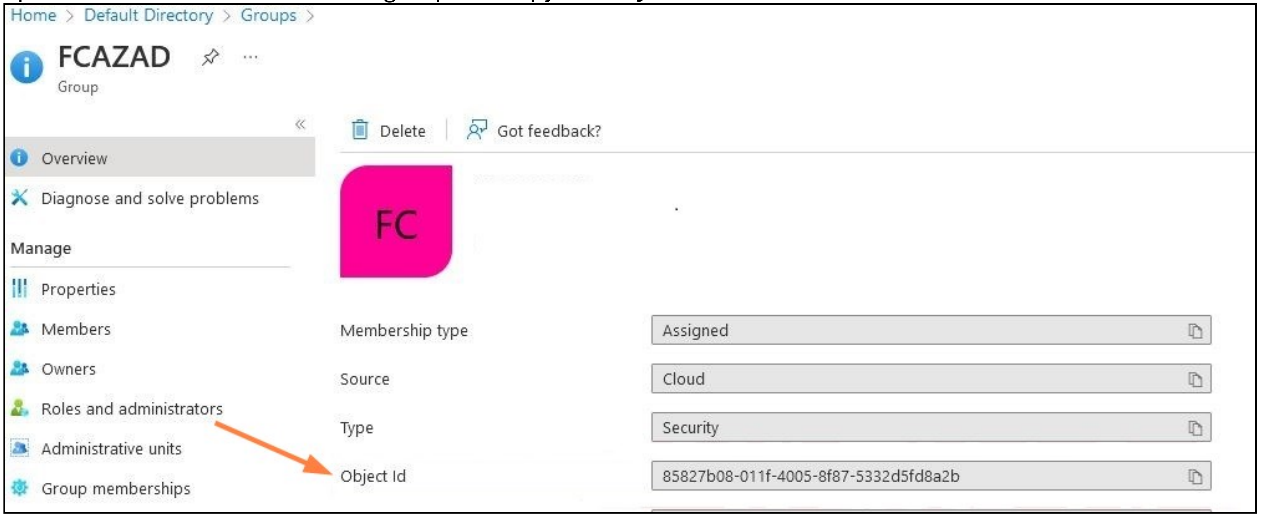
16. Save the above settings.
    This completes the Azure AD SSO integration with FileCloud.

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.

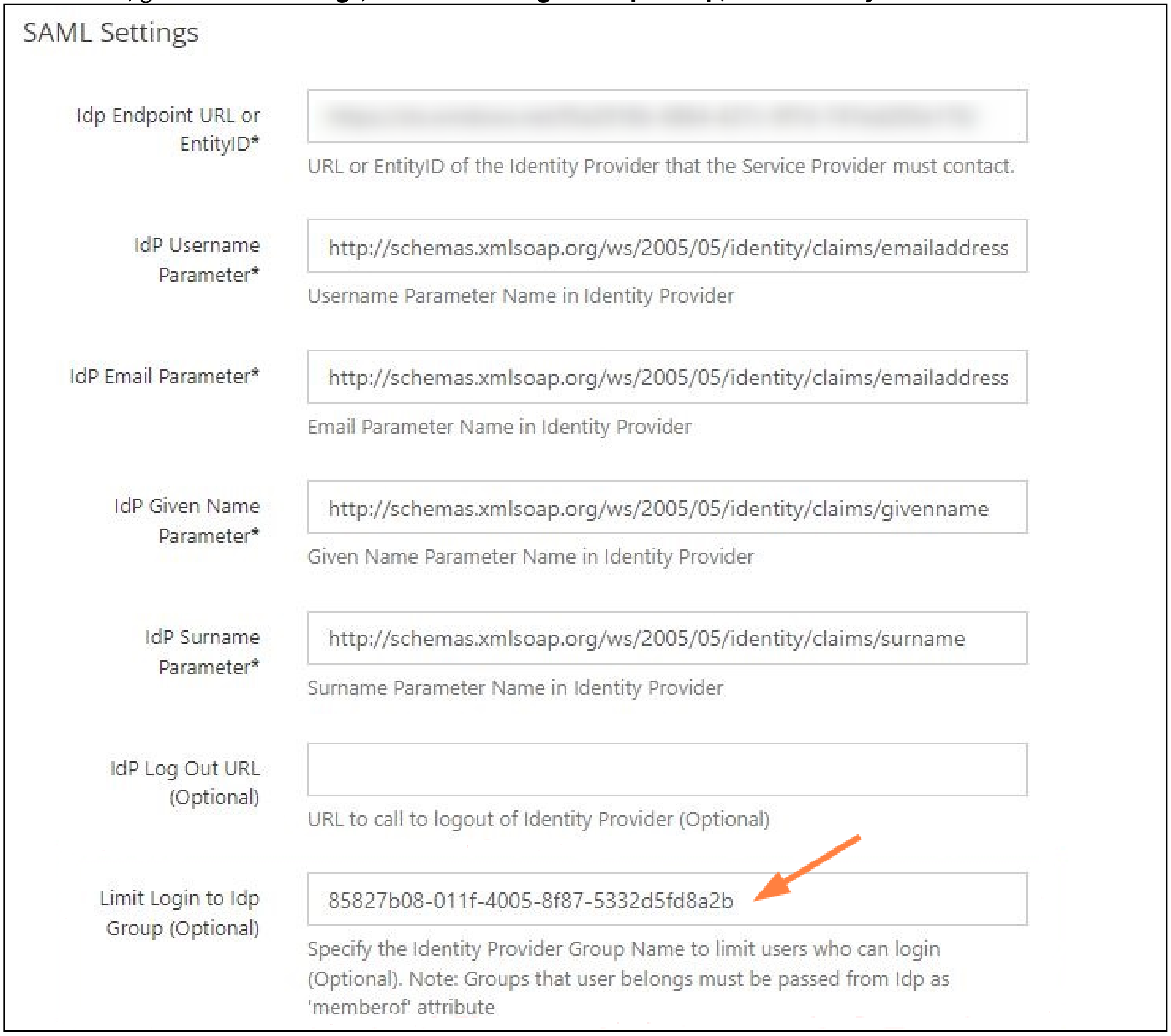
To get the group's **Object ID**, in Azure AD:

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:



Membership type: Assigned
Source: Cloud
Type: Security
Object Id: 85827b08-011f-4005-8f87-5332d5fd8a2b

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



SAML Settings

Idp Endpoint URL or EntityID*: [redacted]
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

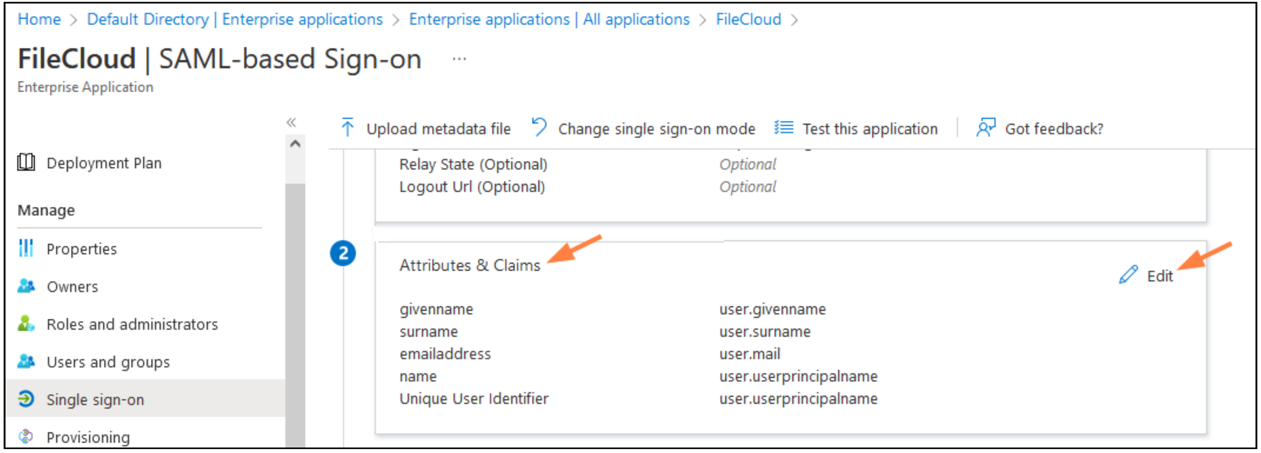
IdP Surname Parameter*: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Surname Parameter Name in Identity Provider

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**.

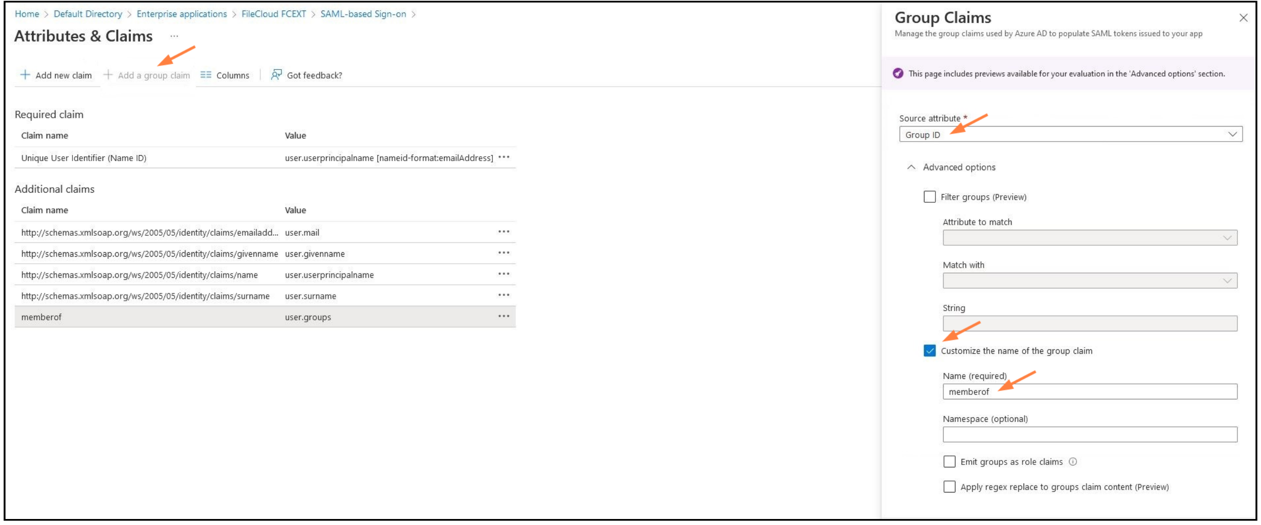


Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

Attributes & Claims

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
Got 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/emailadd...	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.

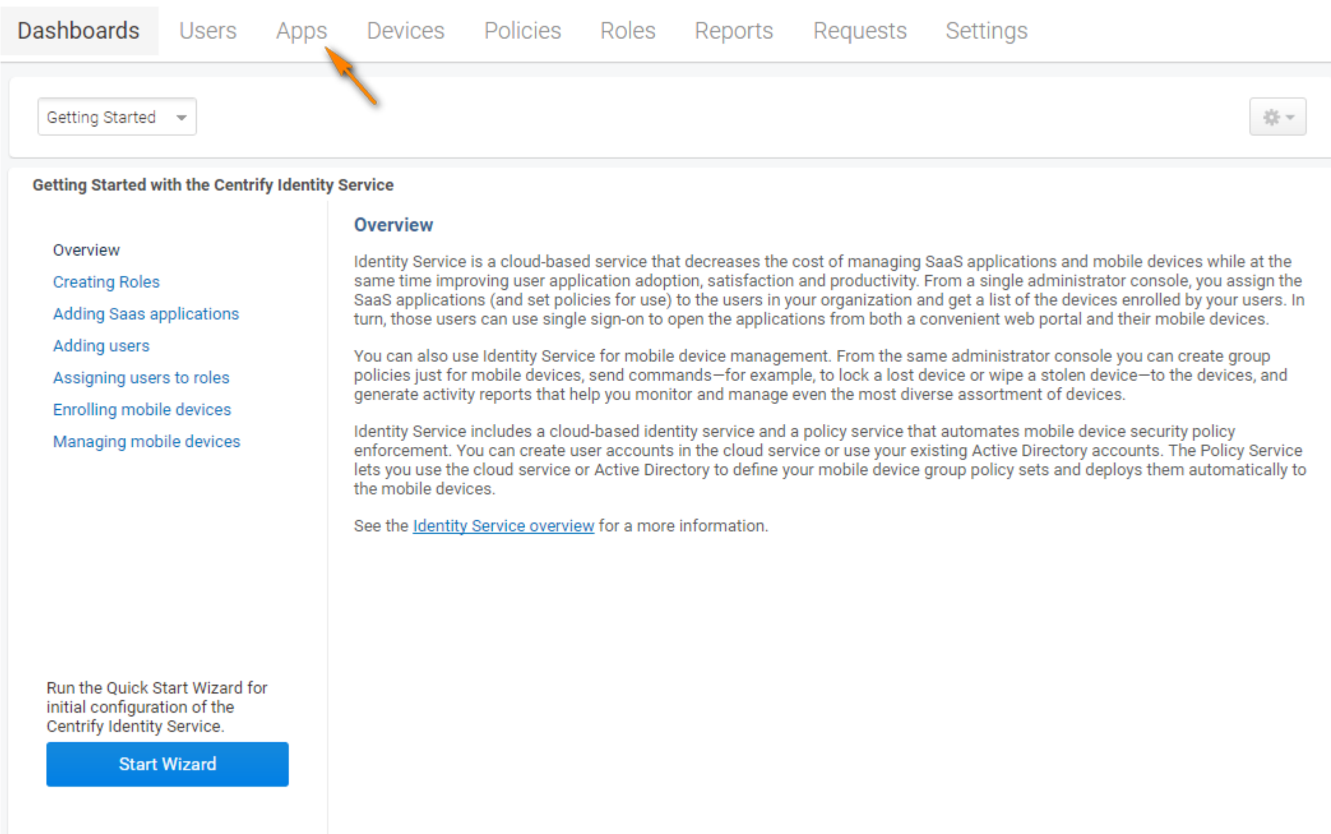
FileCloud can be integrated with Centrify. Centrify must be configured as an Identity Provider (IdP) and FileCloud will act as the Service Provider (SP). The following steps must be followed to configure FileCloud with Centrify.

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



Getting Started with the Centrify Identity Service

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.

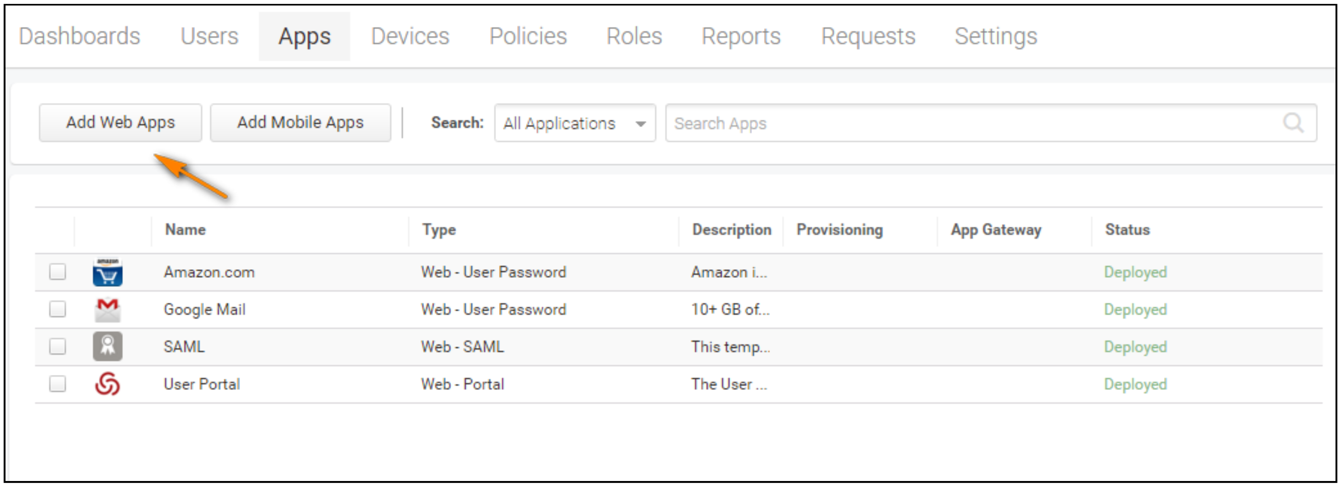
You can also use Identity Service for mobile device management. From the same administrator console you can create group policies just for mobile devices, send commands—for example, to lock a lost device or wipe a stolen device—to the devices, and generate activity reports that help you monitor and manage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

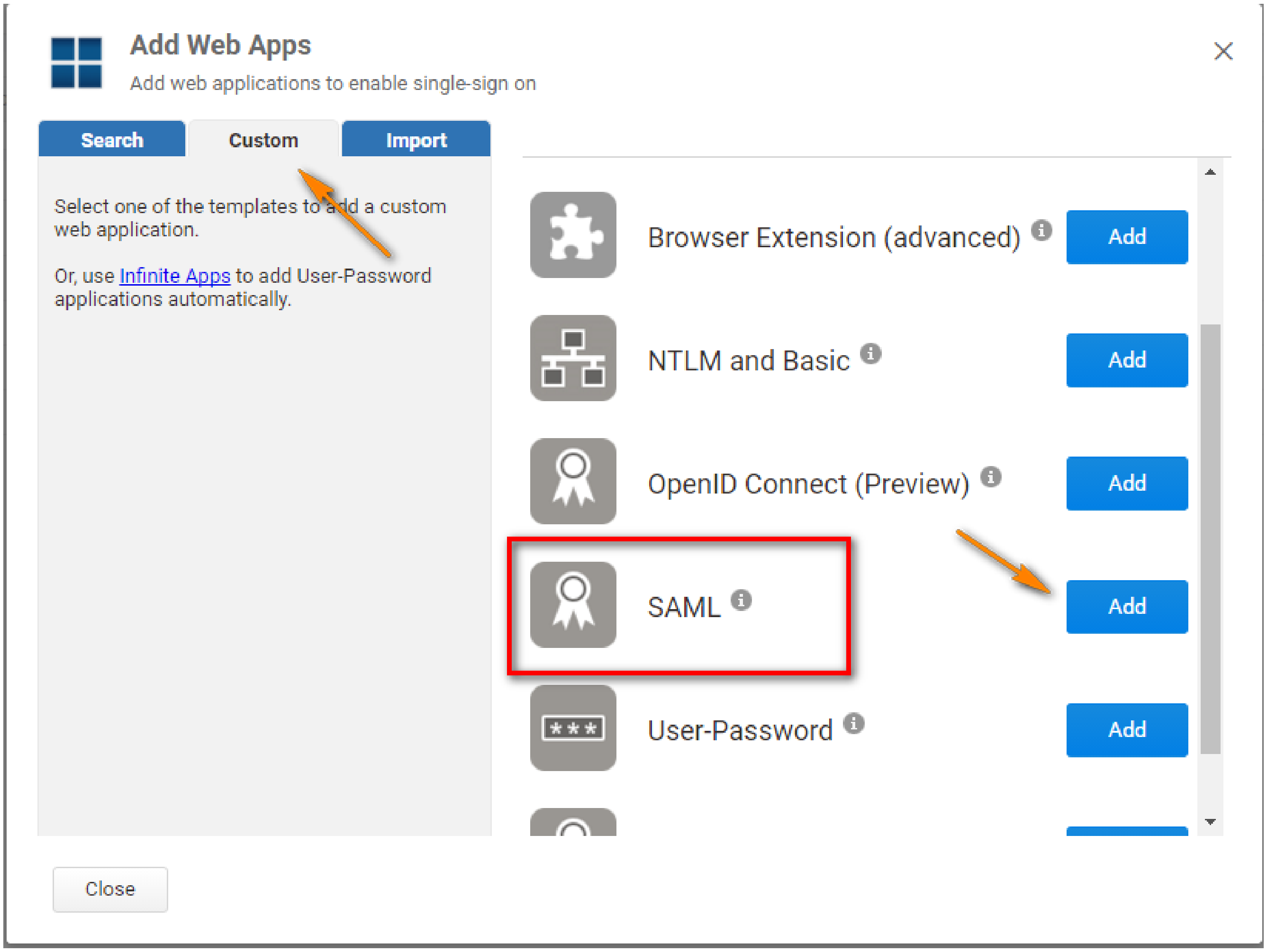
Run the Quick Start Wizard for initial configuration of the Centrify Identity Service.

From the Apps menu, Click Add Web Apps.



		Name	Type	Description	Provisioning	App Gateway	Status
□		Amazon.com	Web - User Password	Amazon i...			Deployed
□		Google Mail	Web - User Password	10+ GB of...			Deployed
□		SAML	Web - SAML	This temp...			Deployed
□		User Portal	Web - Portal	The User ...			Deployed

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



Add Web Apps

Add web applications to enable single-sign on

Select one of the templates to add a custom web application.

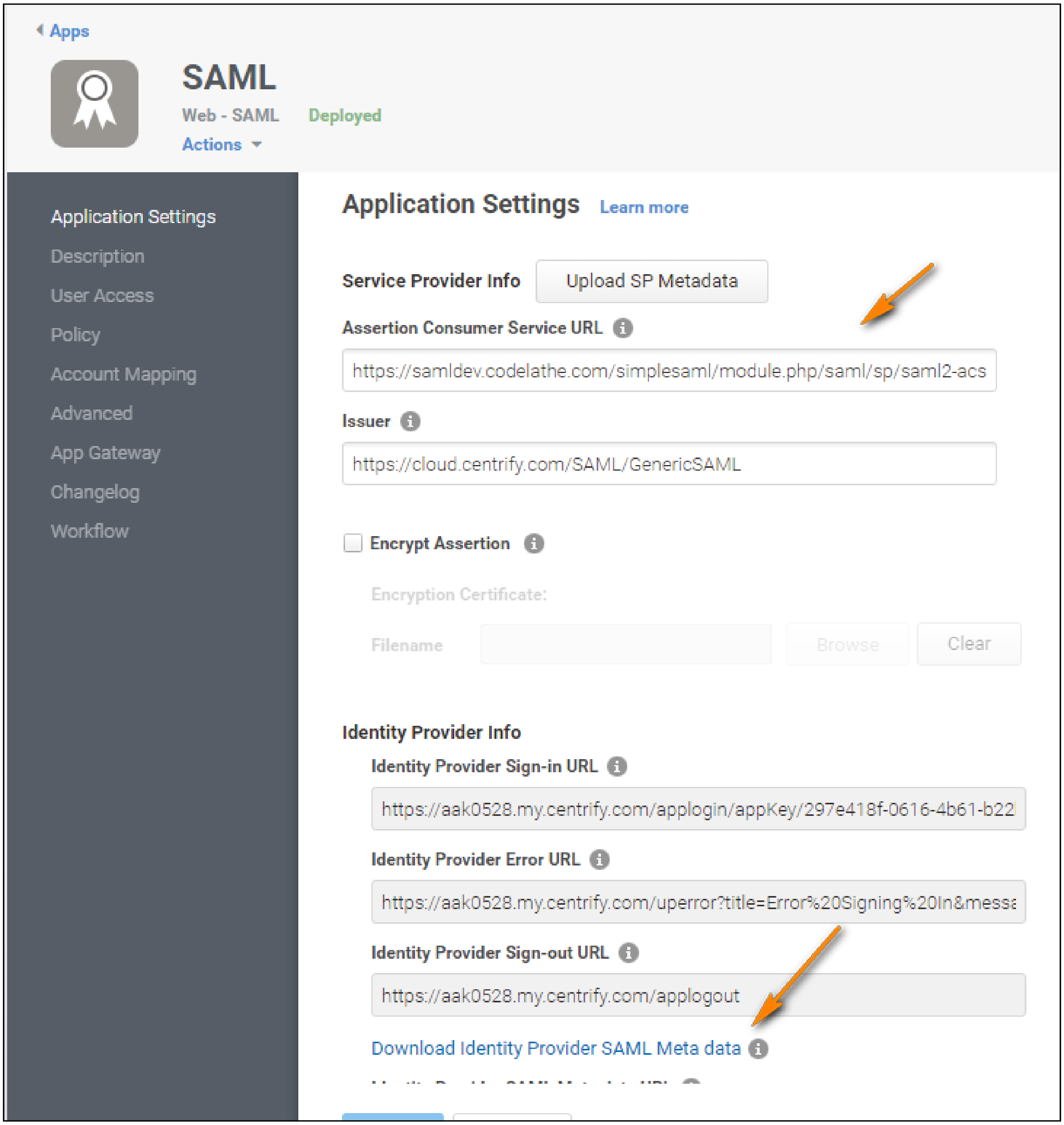
Or, use Infinite Apps to add User-Password applications automatically.

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.



Application Settings

Service Provider Info

Assertion Consumer Service URL: https://samldev.codelathe.com/simplesaml/module.php/saml/sp/saml2-acs

Issuer: https://cloud.centrify.com/SAML/GenericSAML

□ Encrypt Assertion

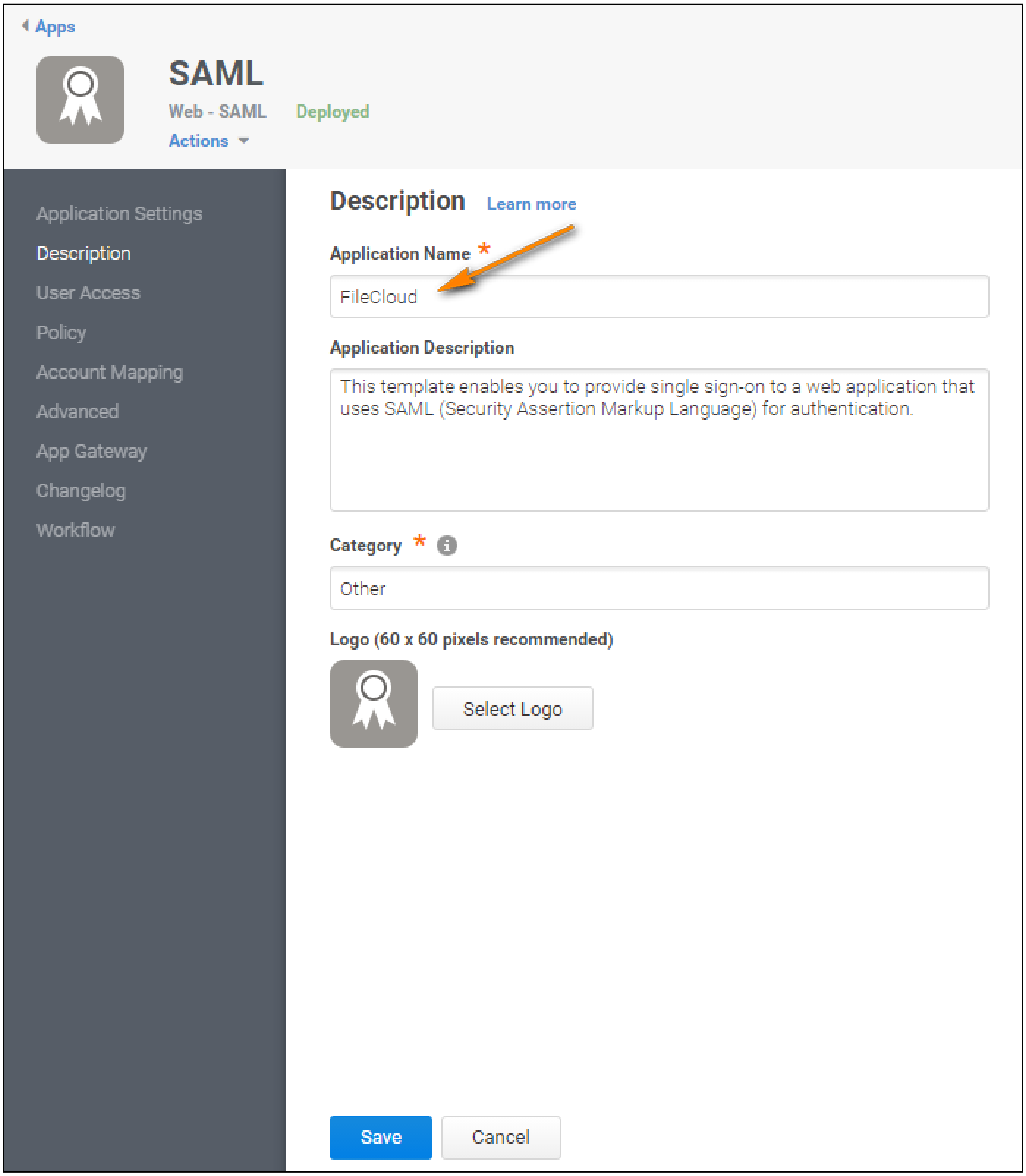
Identity Provider Info

Identity Provider Sign-in URL: https://aak0528.my.centrify.com/applogin/appKey/297e418f-0616-4b61-b22

Identity Provider Error URL: https://aak0528.my.centrify.com/uperror?title=Error%20Signing%20In&messa

Identity Provider Sign-out URL: https://aak0528.my.centrify.com/applogout

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



Application Name *

FileCloud

Application Description

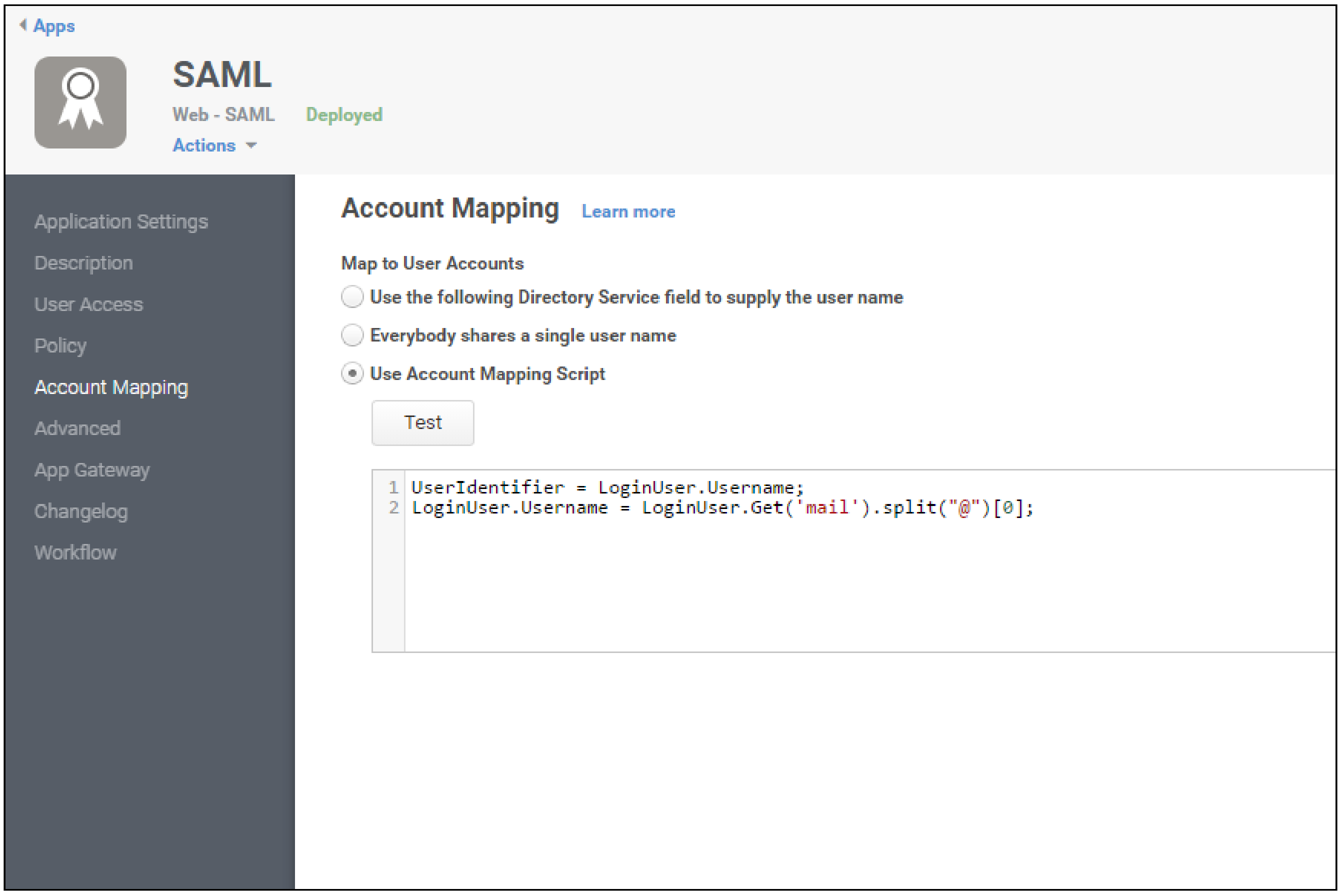
This template enables you to provide single sign-on to a web application that uses SAML (Security Assertion Markup Language) for authentication.

Category *

Other

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.



Map to User Accounts

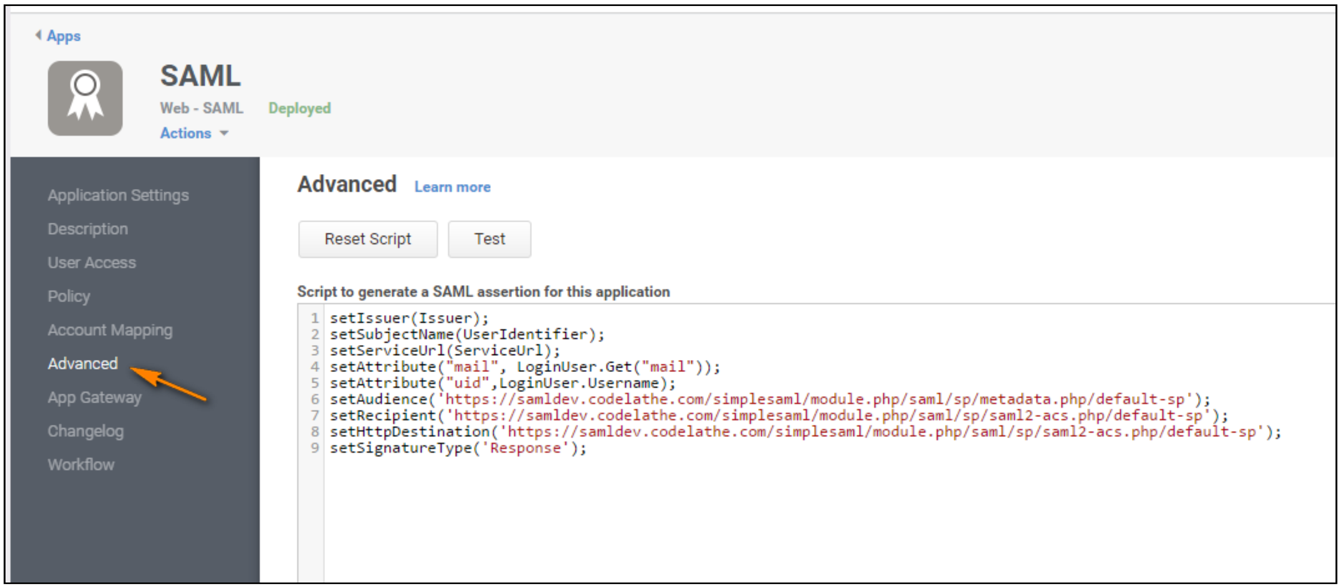
○ Use the following Directory Service field to supply the user name

○ Everybody shares a single user name

● Use Account Mapping Script

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

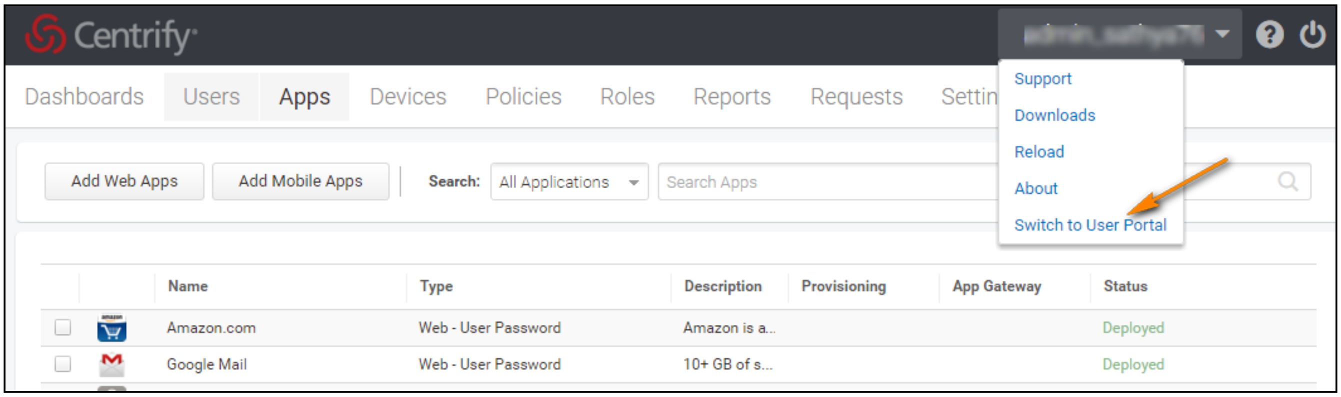
In the **Advanced** Link, add the script as follows:



Script to generate a SAML assertion for this application

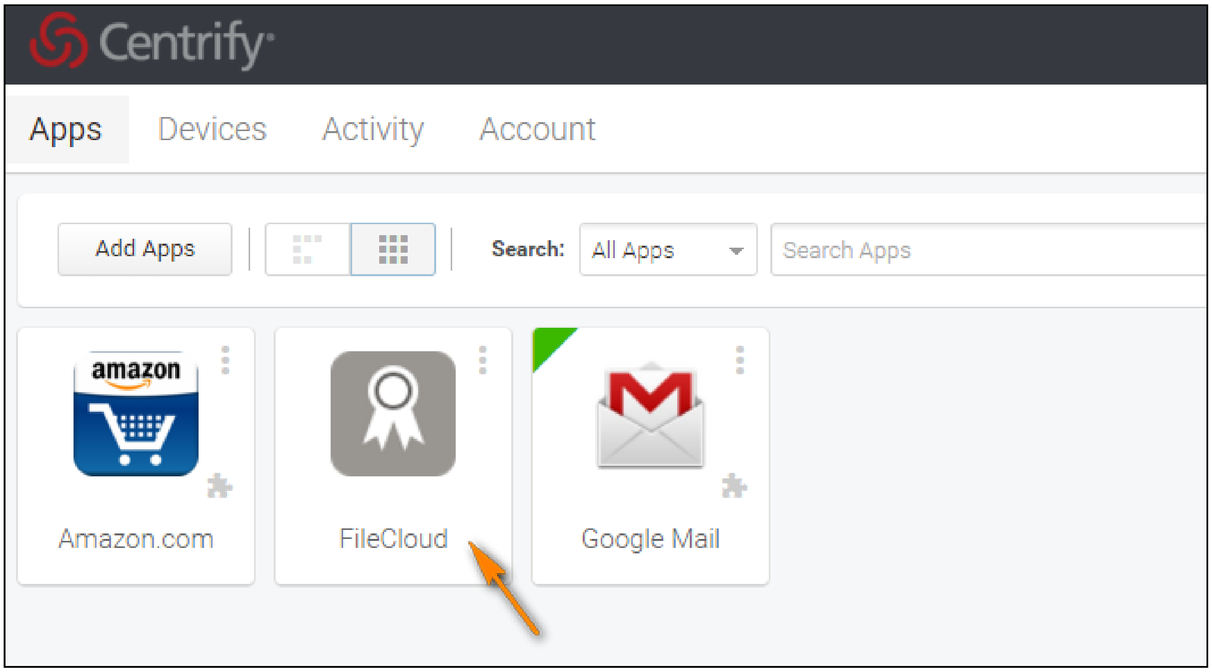
```
setIssuer(Issuer);
setSubjectName(UserIdentifier);
setServiceUrl(ServiceUrl);
setAttribute("mail", LoginUser.Get("mail"));
setAttribute("uid",LoginUser.Username);
setAudience('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/metadata.php/default-sp');
setRecipient('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp');
setHttpDestination('https://samldev.codelathe.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp');
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.



		Name	Type	Description	Provisioning	App Gateway	Status
□		Amazon.com	Web - User Password	Amazon is a...			Deployed
□		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.

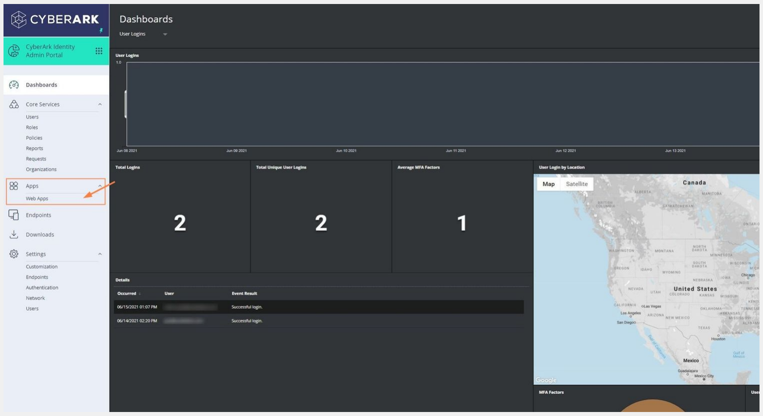
CYBERARK	CYBERARK is a cloud-based platform • Manage privileged accounts and credentials • Secure workforce and customer identities • Secure and manage access for applications and other non-human identities

In this integration scenario:

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

Configure FileCloud with CYBERARK

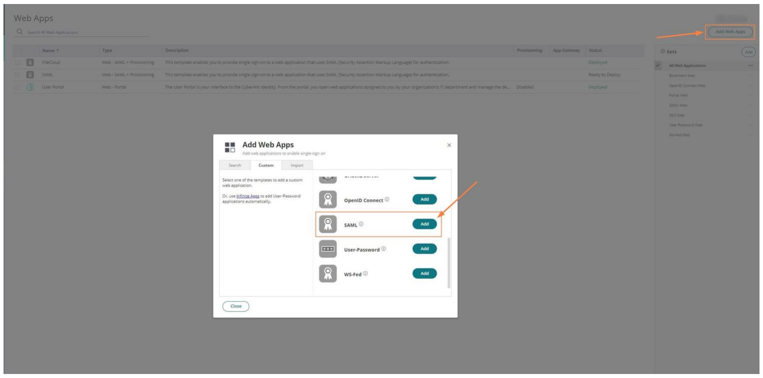
1. In CYBERARK, create a new Web App



1 Cyberark Dashboard

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

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

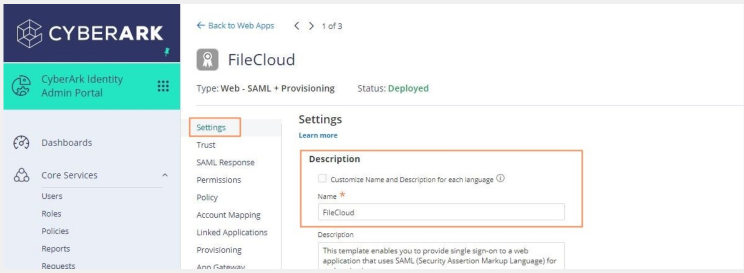


2 Add Web App window in CyberArk

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

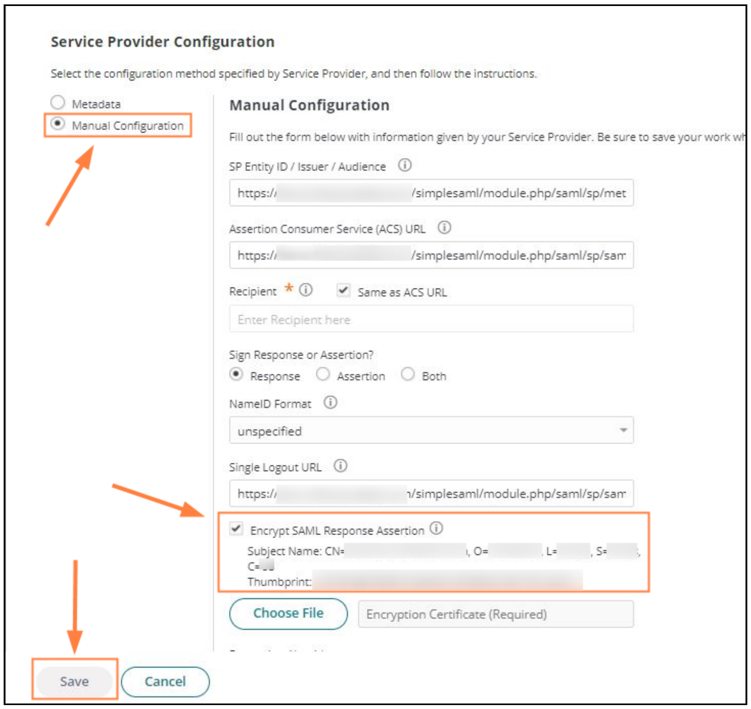
1d. Once the Add Web App popup panel appears, select the custom tab and scroll down until you find SAML and click Add, A confirmation panel might appear. Click Yes, and then close to access the added SAML Web App.

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 wh

SP Entity ID / Issuer / Audience ⓘ

https://[redacted]/simplesaml/module.php/saml/sp/met

Assertion Consumer Service (ACS) URL ⓘ

https://[redacted]/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://[redacted]/simplesaml/module.php/saml/sp/sam

☑ Encrypt SAML Response Assertion ⓘ

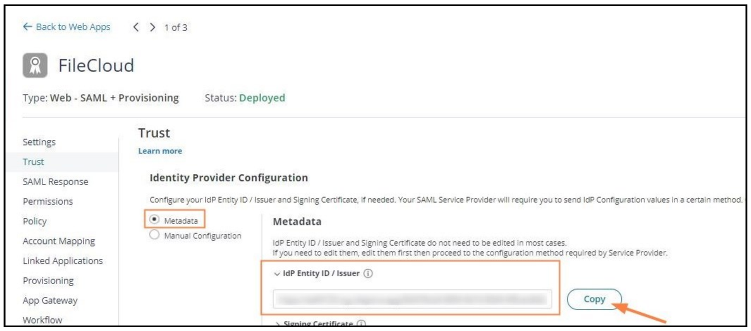
Subject Name: CN=[redacted], O=[redacted], L=[redacted], S=[redacted], C=[redacted]

Thumbprint: [redacted]

Encryption Certificate (Required)

4 In Trust in Cyberark, download metadata

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



Type: Web - SAML + Provisioning Status: Deployed

Trust

Identity Provider Configuration

Configure your IdP Entity ID / Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values in a certain method.

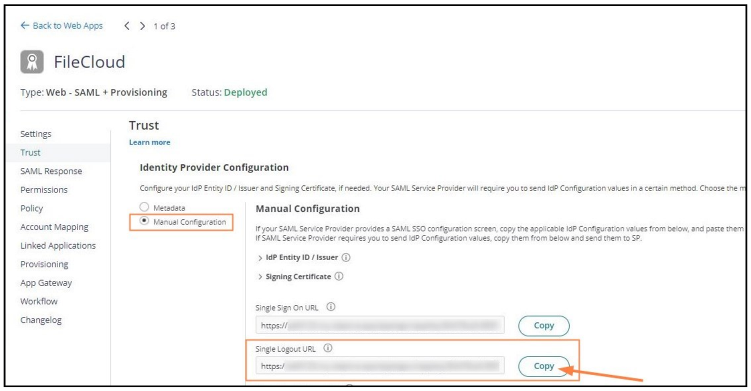
● Metadata
○ Manual Configuration

Metadata

IdP Entity ID / Issuer and Signing Certificate do not need to be edited in most cases.
If you need to edit them, edit them first then proceed to the configuration method required by Service Provider.

IdP Entity ID / Issuer: [redacted]

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



Type: Web - SAML + Provisioning Status: Deployed

Trust

Identity Provider Configuration

Configure your IdP Entity ID / Issuer and Signing Certificate, if needed. Your SAML Service Provider will require you to send IdP Configuration values in a certain method. Choose the m

○ Metadata
● Manual Configuration

Manual Configuration

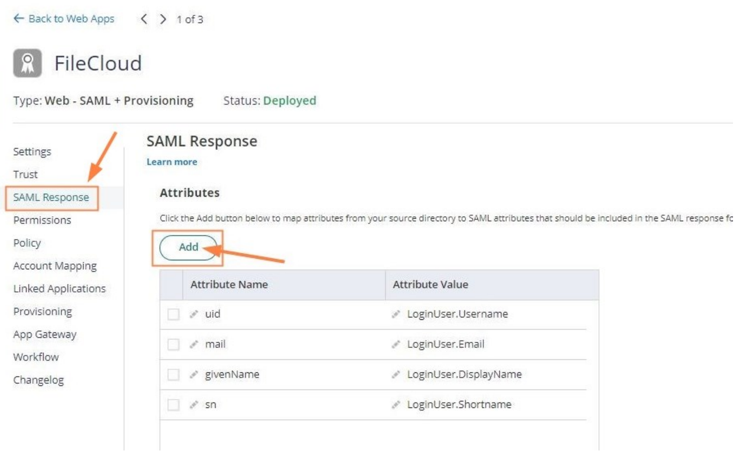
If your SAML Service Provider provides a SAML SSO configuration screen, copy the applicable IdP Configuration values from below, and paste them
If SAML Service Provider requires you to send IdP Configuration values, copy them from below and send them to SP.

Single Sign On URL: https://[redacted]

Single Logout URL: https:/[redacted]

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

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.



Type: Web - SAML + Provisioning Status: Deployed

SAML Response

Attributes

Click the Add button below to map attributes from your source directory to SAML attributes that should be included in the SAML response fc

Attribute Name	Attribute Value
uid	LoginUser.Username
mail	LoginUser.Email
givenName	LoginUser.DisplayName
sn	LoginUser.Shortname

7 In Web App SAML Response screen in Cyberark click Add

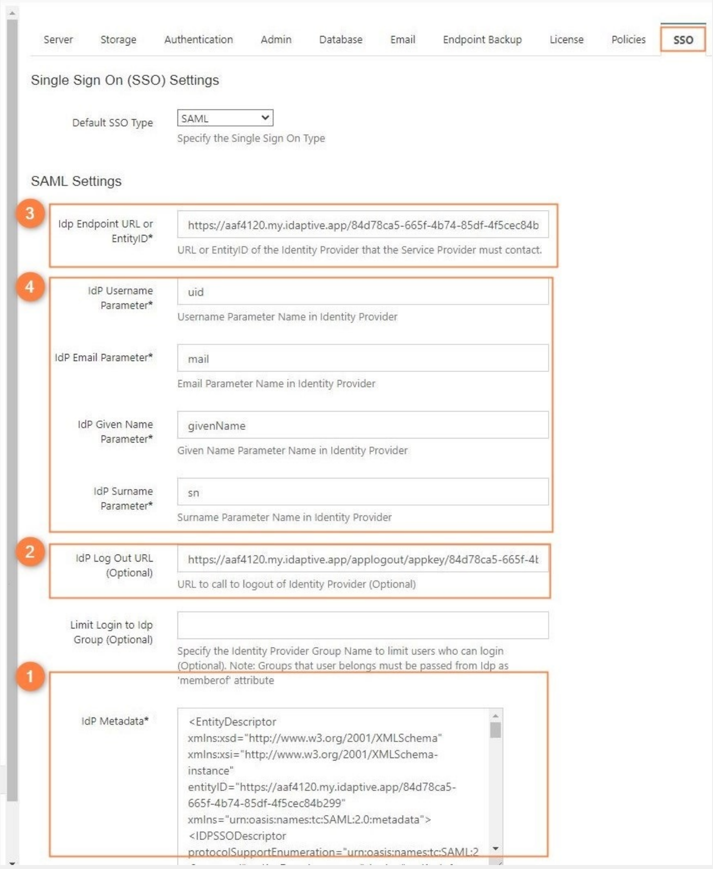
2D. Access the "SAML Response" tab in the navigation panel, and add the following attribute Values:

- **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



Single Sign On (SSO) Settings

Default SSO Type: SAML
Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*: https://aaf4120.my.idaptive.app/84d78ca5-665f-4b74-85df-4f5cec84b
URL or EntityID of the Identity Provider that the Service Provider must contact.

IdP Username Parameter*: uid
Username Parameter Name in Identity Provider

IdP Email Parameter*: mail
Email Parameter Name in Identity Provider

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

IdP Surname Parameter*: sn
Surname Parameter Name in Identity Provider

IdP Log Out URL (Optional): https://aaf4120.my.idaptive.app/applogout/appkey/84d78ca5-665f-4t
URL to call to logout of Identity Provider (Optional)

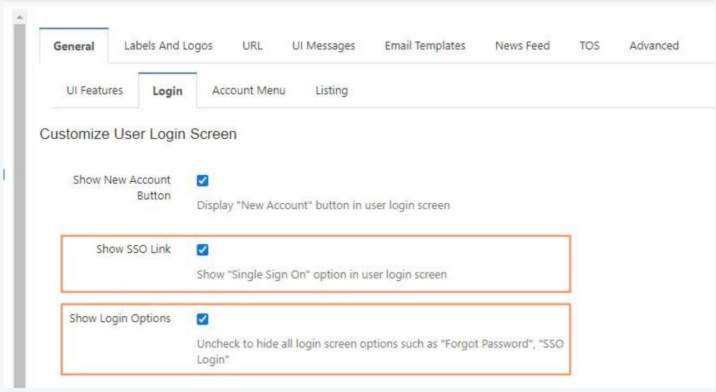
Limit Login to Idp Group (Optional):
Specify the Identity Provider Group Name to limit users who can login (Optional). Note: Groups that user belongs must be passed from Idp as 'memberof' attribute

IdP Metadata*:

```
<EntityDescriptor
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
entityID="https://aaf4120.my.idaptive.app/84d78ca5-
665f-4b74-85df-4f5cec84b299"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2
```

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.**



Customize User Login Screen

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

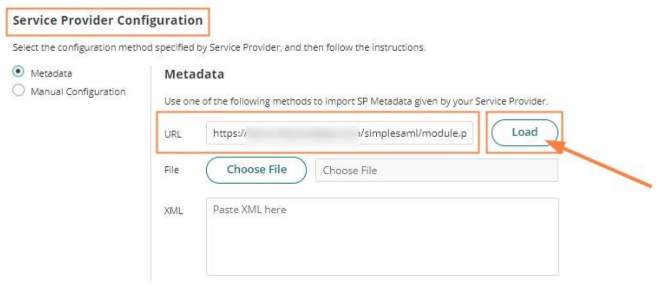
Show SSO Link ☑
Show "Single Sign On" option in user login screen

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

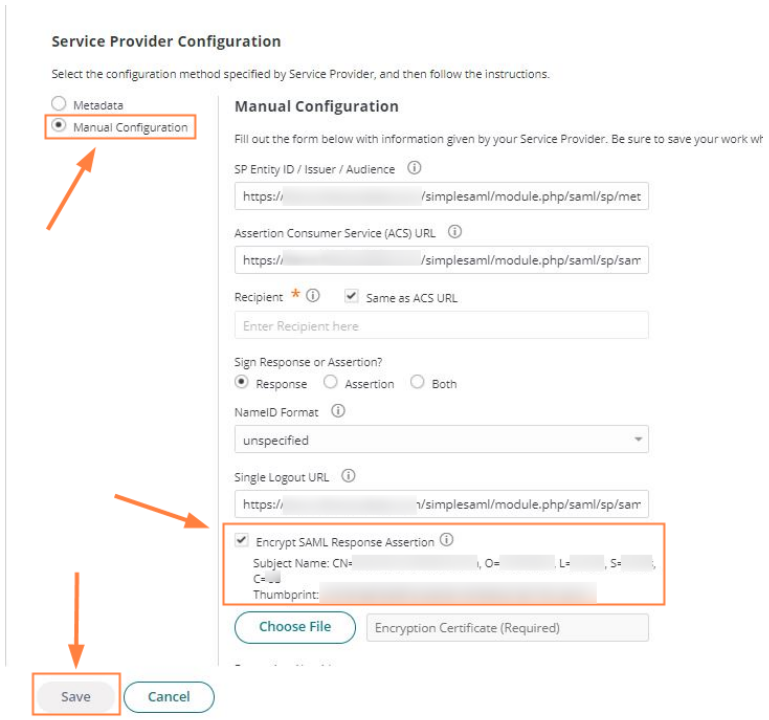
Use one of the following methods to import SP Metadata given by your Service Provider.

URL https://[redacted]/simplesaml/module.p Load

File Choose File Choose File

XML Paste XML here

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 wh

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

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

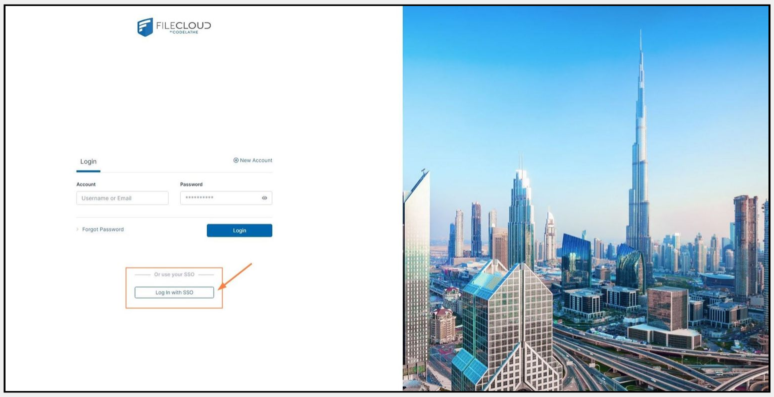
☑ Encrypt SAML Response Assertion ⓘ
Subject Name: CN=[redacted], O=[redacted] L=[redacted], S=[redacted],
C=[redacted]
Thumbprint: [redacted]

Choose File Encryption Certificate (Required)

Save Cancel

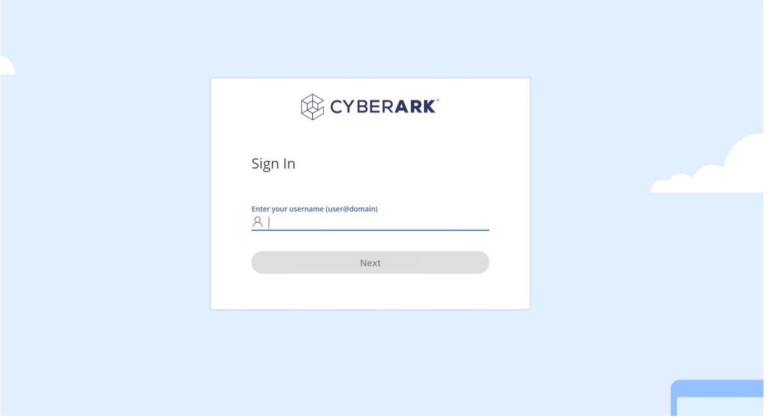
4b. Once you have loaded FileCloud's Metadatada, change the settings from Metadata to Manual Configuration and disable Encrypt SAML Response Assertion, Click Save.

5. CYBERARK SSO integration Completed

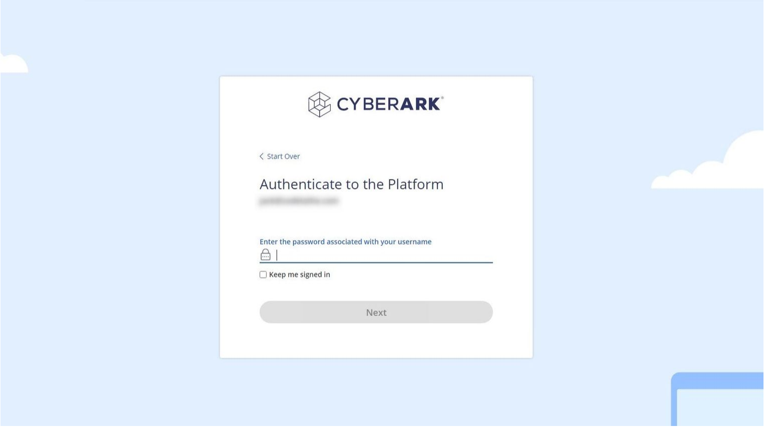


9 FileCloud User Portal, Login screen

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

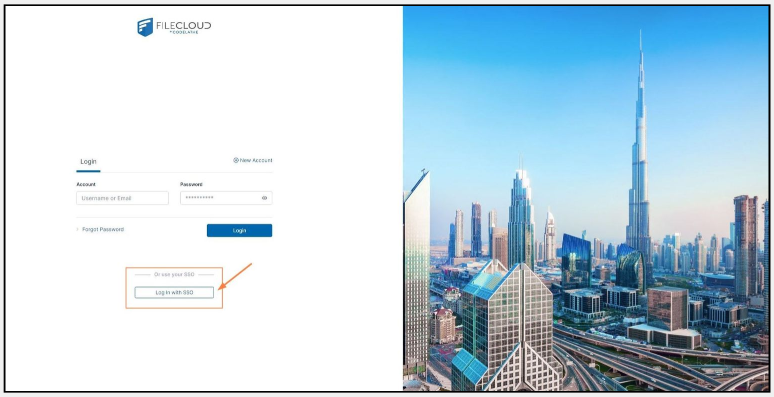
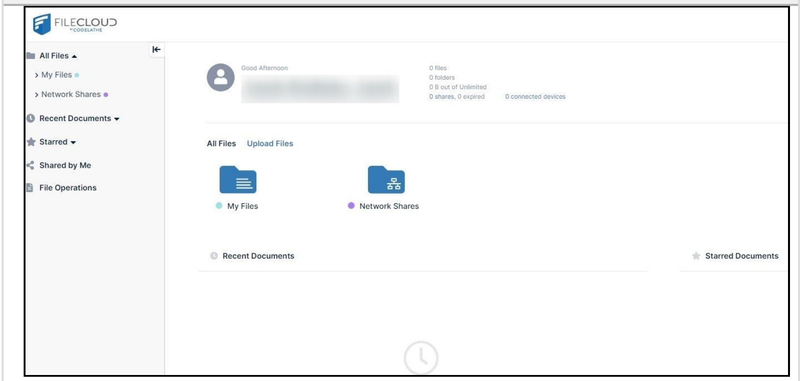


10 Cyberark Login page, username


CYBERARK
Start Over
Authenticate to the Platform
Enter the password associated with your username
Keep me signed in
Next

11 Cyberark Login page, password

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

 FILECLOUD Login New Account Account Password Username or Email Forgot Password Login Or use your SSO Log In with SSO **9 FileCloud User Portal, Login screen**	**5a. Access FileCloud's user portal and click Login In with SSO**
 FILECLOUD All Files My Files Network Shares Recent Documents Starred Shared by Me File Operations Good Afternoon [redacted] 0 files 0 folders 0 B out of Unlimited 0 shares, 0 expired 0 connected devices All Files Upload Files My Files Network Shares Recent Documents Starred Documents **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.

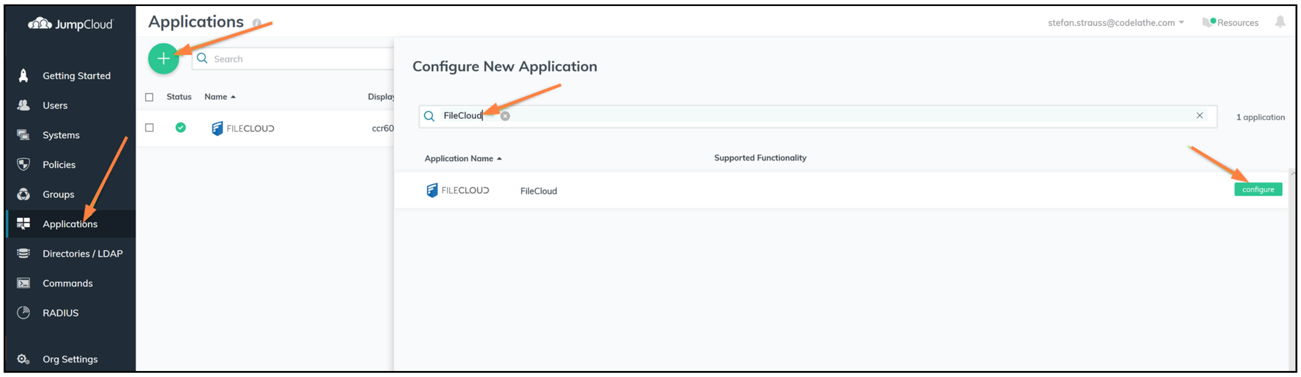
JumpCloud® Directory-as-a-Service®	JumpCloud's is a cloud-based platform • It enables IT teams to securely manage user identities • It connects teams them to resources they need regardless of provider, protocol, vendor, or location

In this integration scenario:

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

Configure FileCloud with JumpCloud

1. In JumpCloud, create a new Application.



FileCloud

FileCloud

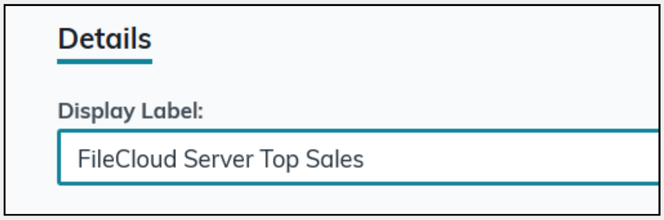
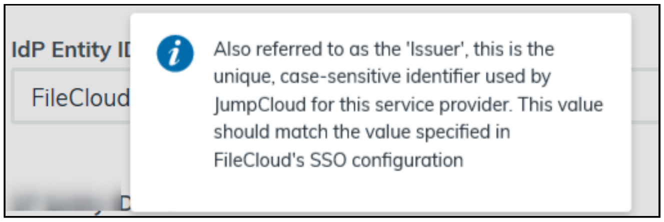
1a. Open a browser and log in to your JumpCloud admin URL by typing it in or clicking on this URL https://console.jumpcloud.com/login

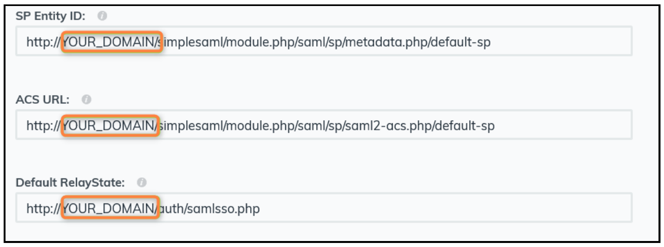
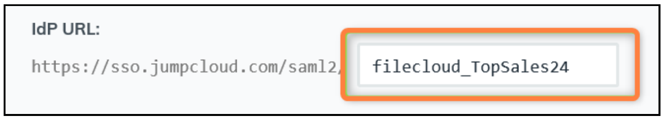
1b. From the left navigation pane, click APPLICATIONS.

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.

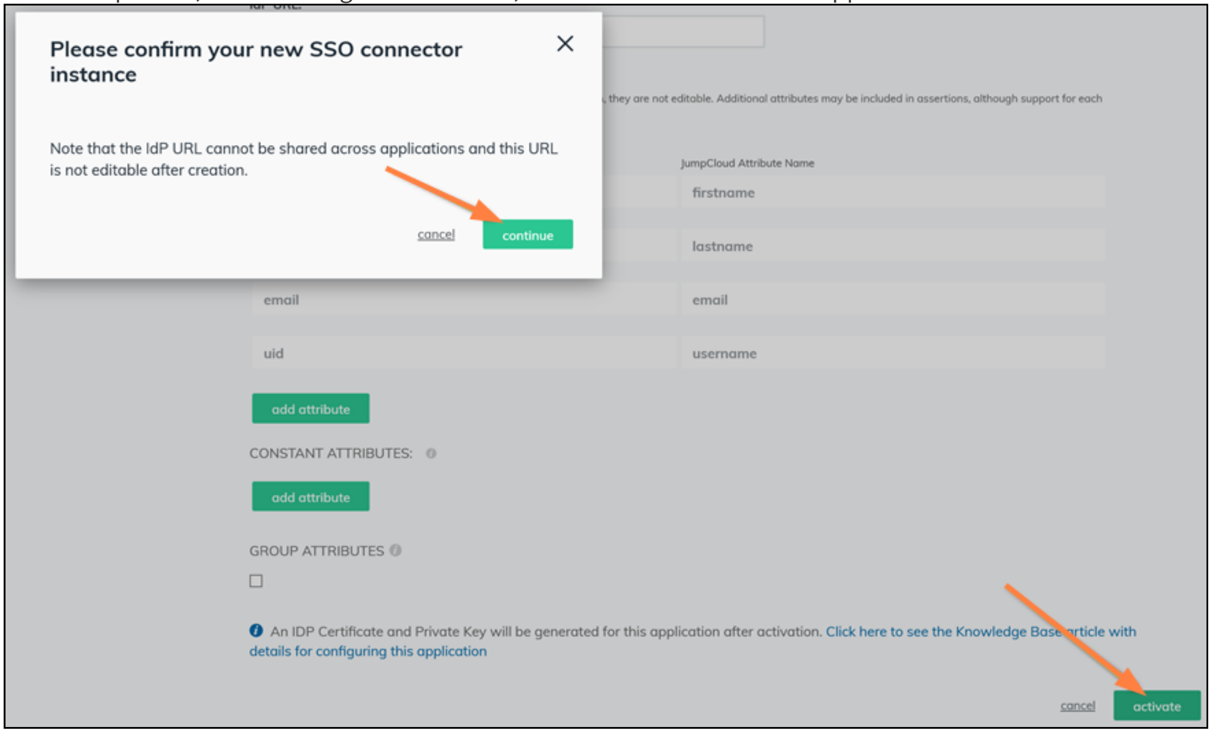
2. In JumpCloud, configure FileCloud Application

 Details Display Label: FileCloud Server Top Sales	**2a. In *Display Label*, enter a meaningful name.**
 IdP Entity ID FileCloud 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	**2b. In *IdP Entity ID*, enter an unique, case-sensitive identifier used by JumpCloud for this FileCloud service provider.**

 SP Entity ID: http://YOUR_DOMAIN/simplesaml/module.php/saml/sp/metadata.php/default-sp ACS URL: http://YOUR_DOMAIN/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp Default RelayState: http://YOUR_DOMAIN/auth/samlsso.php	**2c. Replace YOUR_DOMAIN with your domain name in all fields.**
 IdP URL: https://sso.jumpcloud.com/saml2/ filecloud_TopSales24	**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.**

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



Please confirm your new SSO connector instance

Note that the IdP URL cannot be shared across applications and this URL is not editable after creation.

they are not editable. Additional attributes may be included in assertions, although support for each

	JumpCloud Attribute Name
	firstname
	lastname
email	email
uid	username

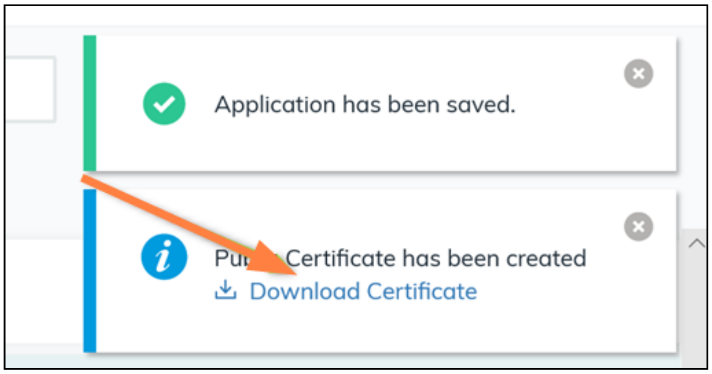
CONSTANT ATTRIBUTES:

GROUP ATTRIBUTES

□

An IDP Certificate and Private Key will be generated for this application after activation. Click here to see the Knowledge Base article with details for configuring this application

3b. Download the generated certificate.



Application has been saved.

Public Certificate has been created

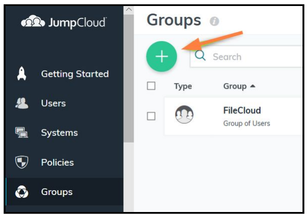
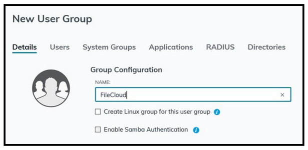
Download Certificate

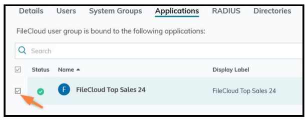
3c. Copy it into your Filecloud in the location for Linux or Windows:

Linux
`/var/www/html/thirdparty/simplesaml/cert/saml.crt`

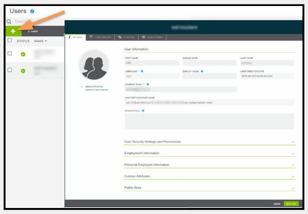
Windows
`C:\xampp\htdocs\thirdparty\simplesaml\cert\saml.crt`

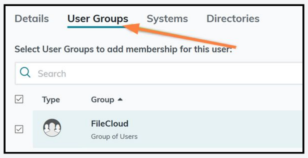
4. In JumpCloud, create a group and add users

 JumpCloud Groups Search Getting Started Users Systems Policies Groups Type Group FileCloud Group of Users	**4a. In JumpCloud, on the Groups screen, click the green button with the white plus sign to add a new group.**
 New User Group Details Users System Groups Applications RADIUS Directories Group Configuration NAME: FileCloud ☐ Create Linux group for this user group ☐ Enable Samba Authentication	**4b. In JumpCloud, enter the group name.**

<table>
<tr>
<td>

FileCloud user group is bound to the following applications:

☑ ✓ FileCloud Top Sales 24 — FileCloud Top Sales 24</td>
<td><b>4c. In JumpCloud, enable the group to access FileCloud.</b></td>
</tr>
<tr>
<td>
</td>
<td><b>4d. In JumpCloud, on the Users screen, click the green button with the white plus sign to add a new user.</b>

<b>4e. In JumpCloud, on the New User screen, select the Details tab and type in the user's information.</b></td>
</tr>
<tr>
<td>

Select User Groups to add membership for this user:

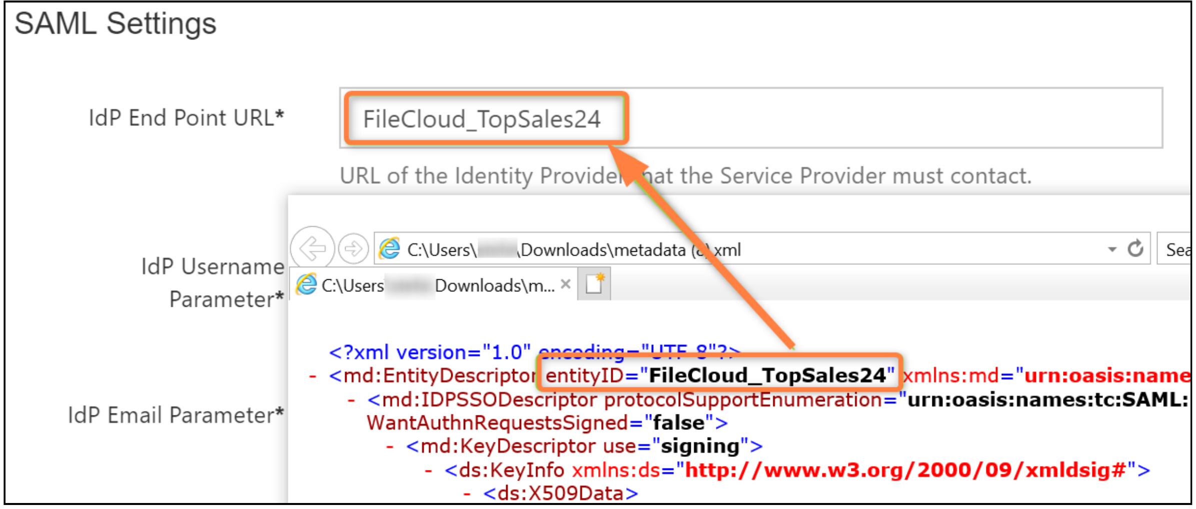
☑ FileCloud — Group of Users</td>
<td><b>4f. In JumpCloud, on the New User screen, select the User Groups tab and add the user to your FileCloud Group.</b>

<b>4g. In JumpCloud, on the New User screen, click the Save User button.</b></td>
</tr>
</table>

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* FileCloud_TopSales24

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

IdP Username Parameter*

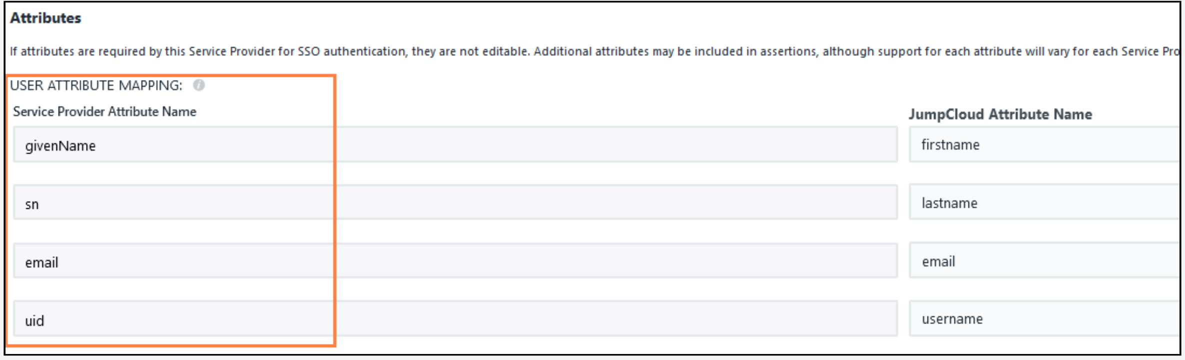
IdP Email Parameter*

C:\Users\[redacted]\Downloads\metadata (4).xml
Sea
C:\Users\[redacted]\Downloads\m...

```
  <?xml version="1.0" encoding="UTF-8"?>
- <md:EntityDescriptor entityID="FileCloud_TopSales24" xmlns:md="urn:oasis:name
  - <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:
    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:



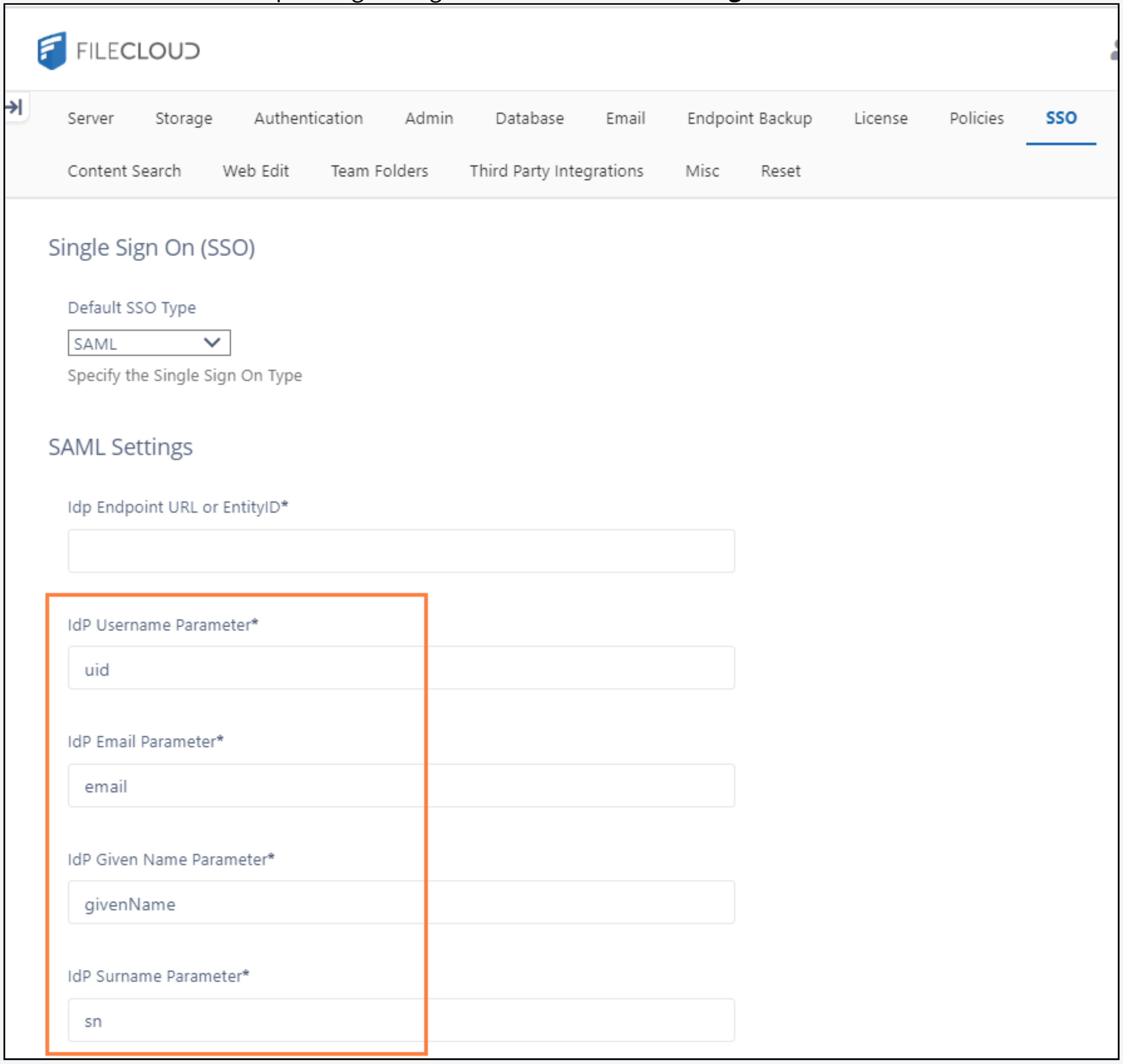
Attributes

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 Pro

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:



Single Sign On (SSO)

Default SSO Type

SAML

Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*

IdP Username Parameter*

uid

IdP Email Parameter*

email

IdP Given Name Parameter*

givenName

IdP Surname Parameter*

sn

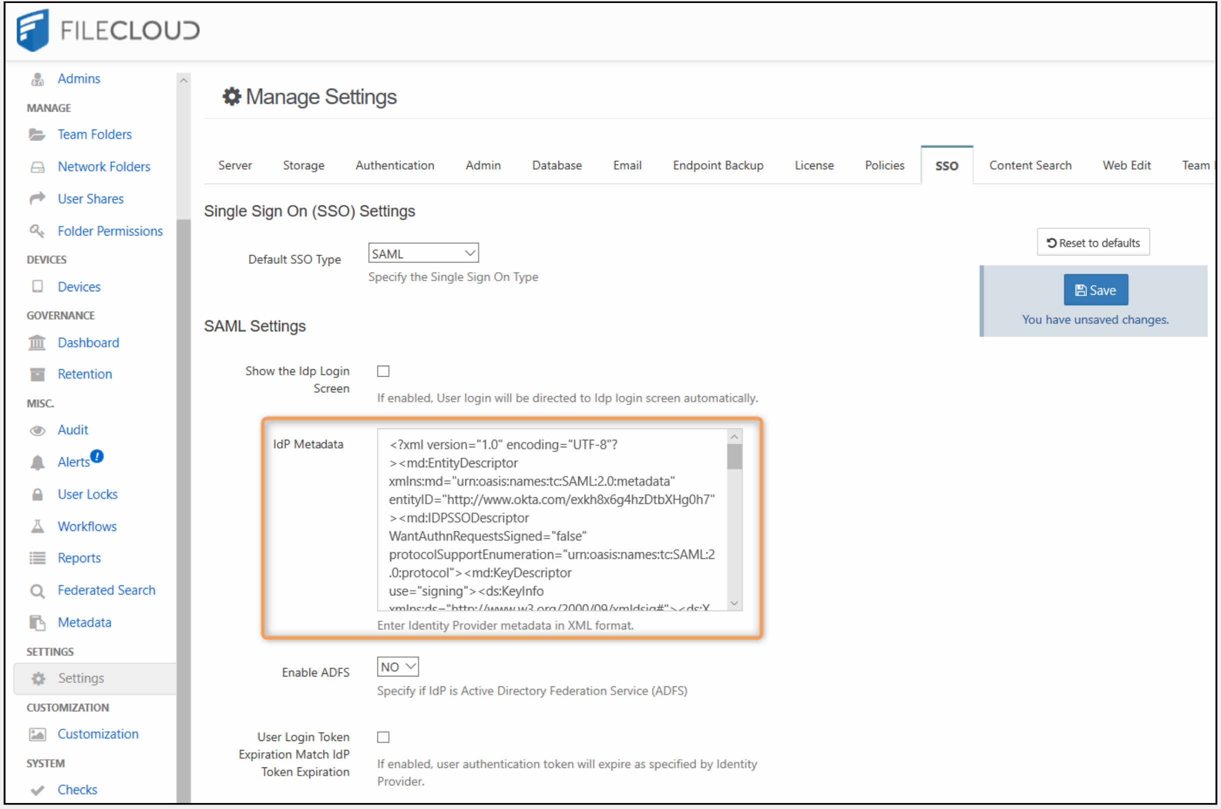
6. Click *Save* and minimize the browser.

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:

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. **Scroll down to the *Idp Meta Data field.***
5. **On the server, open the XML file that contains the metadata you exported from JumpCloud in step 3c.**
6. **Copy the metadata in the file and paste it into FileCloud on the *SSO* tab in the *IdP Metadata* field.**



Single Sign On (SSO) Settings

Default SSO Type: SAML
Specify the Single Sign On Type

SAML Settings

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

IdP Metadata:

```
<?xml version="1.0" encoding="UTF-8"?
><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exkh8x6g4hzDtbXHg0h7"
><md:IDPSSODescriptor
WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2
.0:protocol"><md:KeyDescriptor
use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X
```

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.

7. **Click *Save*.**

Now you can start using the Single Sign-On with JumpCloud from FileCloud!

Integrate Okta with FileCloud

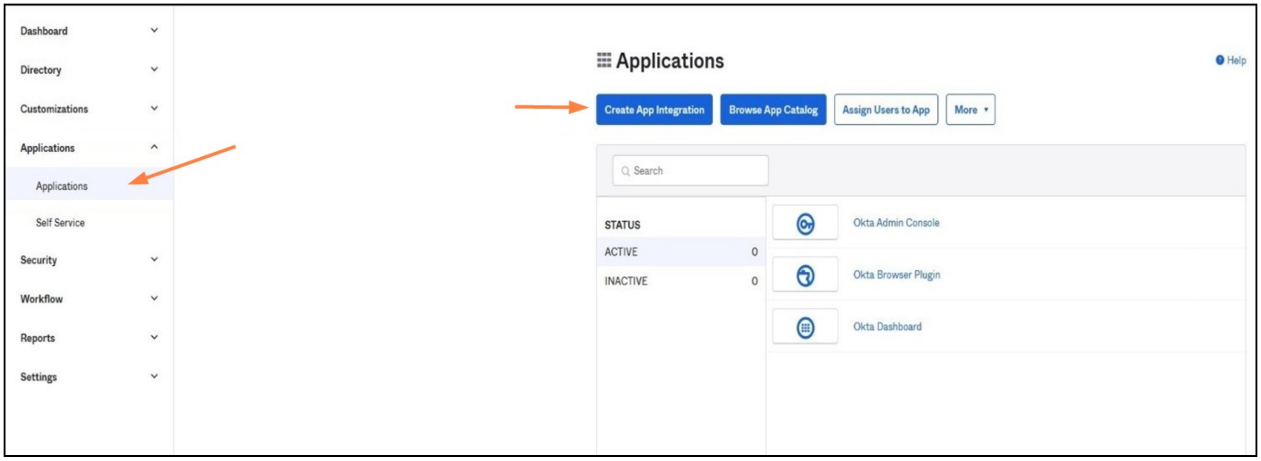
To integrate with the Okta browser plugin, please see Integrate with Okta using browser plugin.

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.

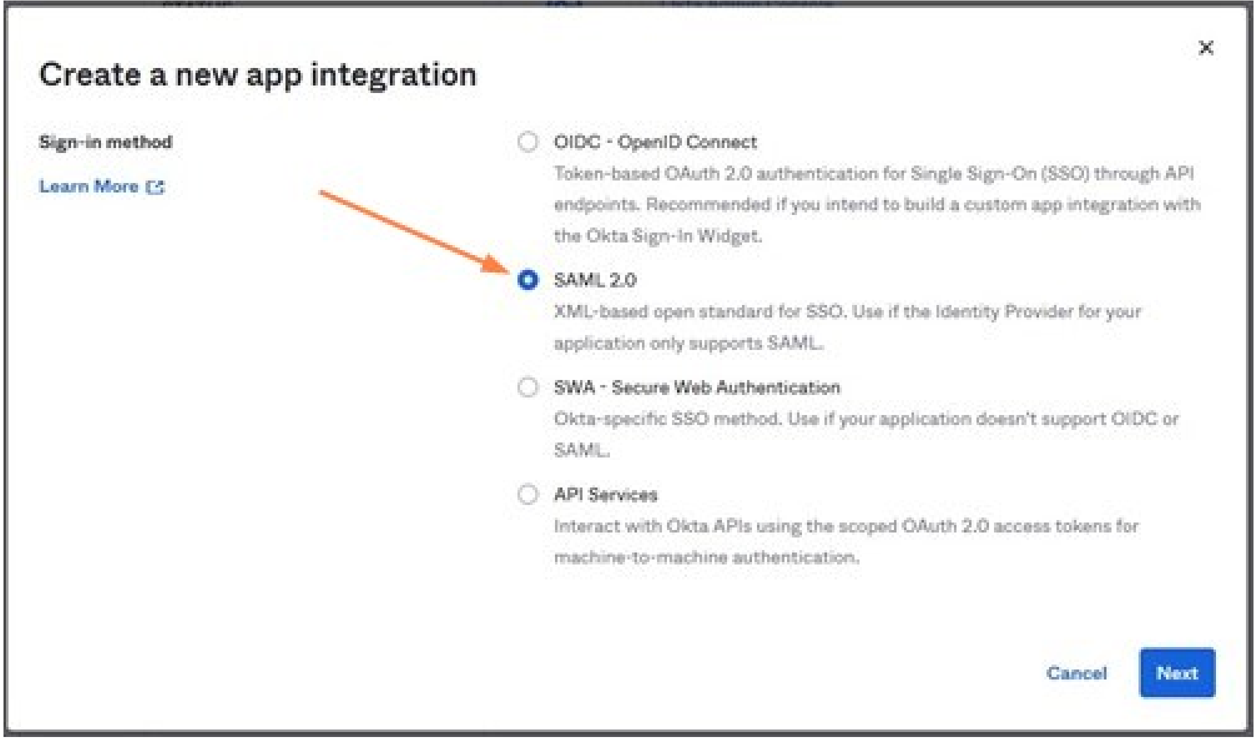
When FileCloud is integrated with Okta, Okta is configured as an Identity Provider (IdP) and FileCloud acts as the Service Provider (SP).

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

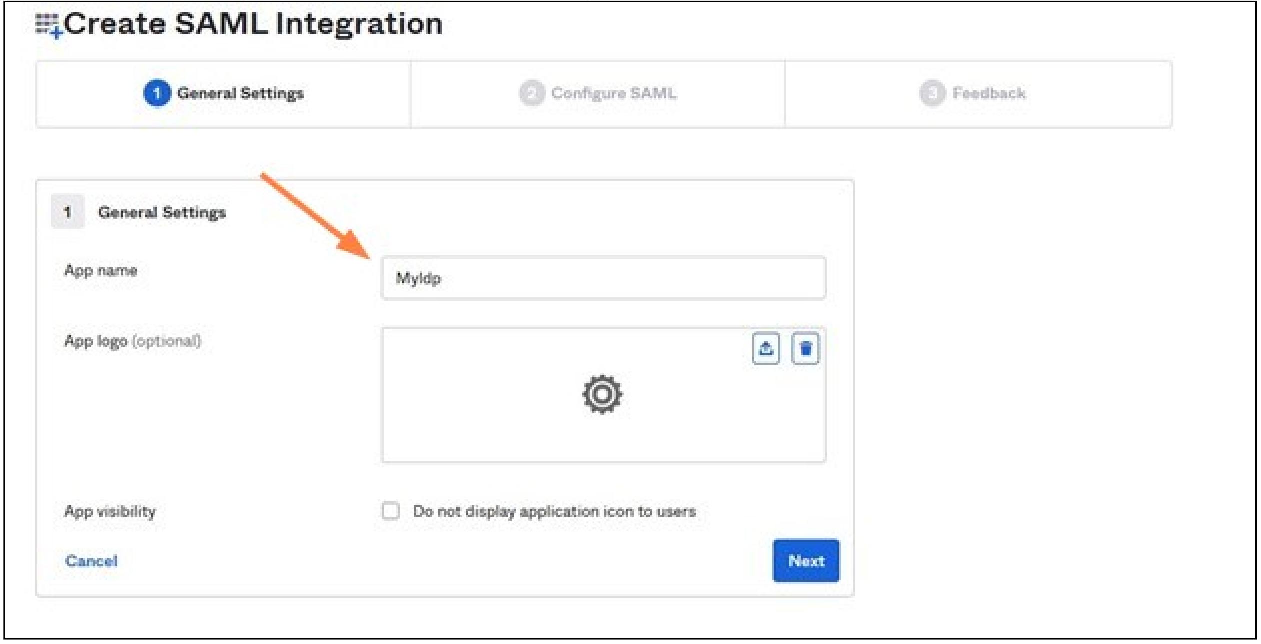
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● 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.

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

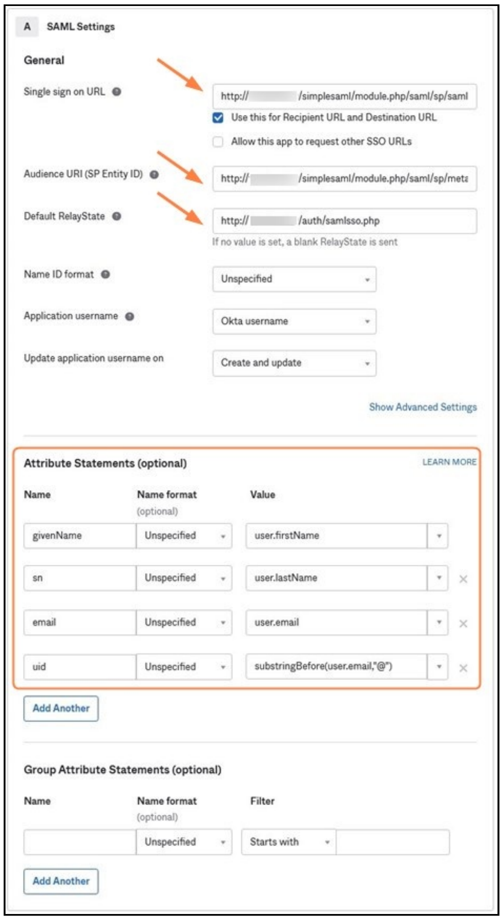
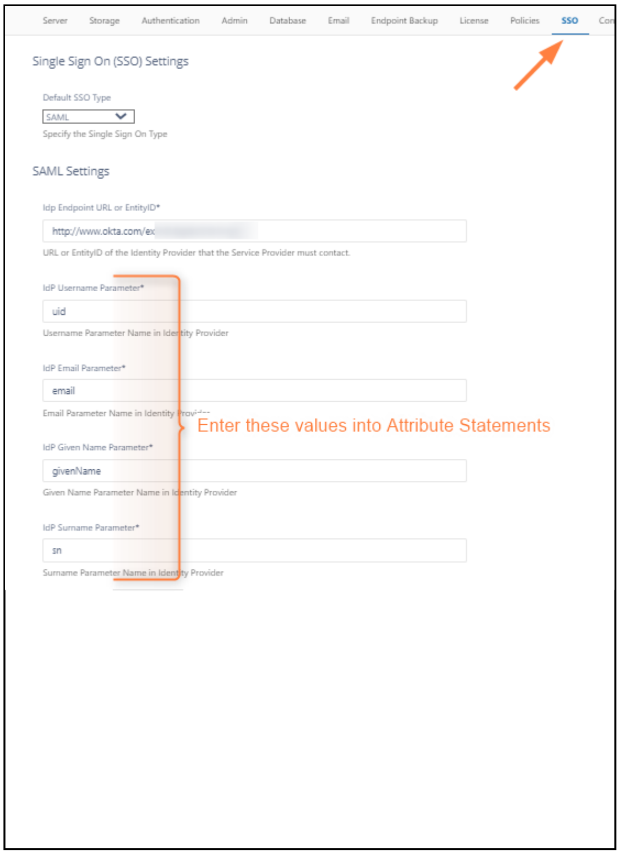
App name: MyIdp

App logo (optional)

App visibility: □ Do not display application icon to users

5. In the **SAML Settings** screen, set the values as follows:
    - Set **Single sign on URL** to the FileCloud assertion URL **http://<your domain>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp**
    - Set **Audience URI (SP Entity ID)** to **http://<your domain>/simplesaml/module.php/saml/sp/metadata.php/default-sp**
    - Set **Default Relay State** to **http://<your domain>/auth/samlsso.php**

- Under **Attribute Statements**, the attribute names must match the names set in the FileCloud admin portal in **Settings > SSO** for **Idp Username Parameter**, **Idp Email Parameter**, **Idp Given Name Parameter**, and **IDP Surname Parameter**.
  Set the **Values** for the **Attribute Statements** to the values shown in the screenshot.

Okta	**FileCloud**
	

A SAML Settings

General

Single sign on URL: http://[redacted]/simplesaml/module.php/saml/sp/saml

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): http://[redacted]/simplesaml/module.php/saml/sp/meta

Default RelayState: http://[redacted]/auth/samlsso.php

If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

Attribute Statements (optional)

Name	Name format (optional)	Value
givenName	Unspecified	user.firstName
sn	Unspecified	user.lastName
email	Unspecified	user.email
uid	Unspecified	substringBefore(user.email,"@")

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
	Unspecified	Starts with

Single Sign On (SSO) Settings

Default SSO Type: SAML

Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*: http://www.okta.com/ex[redacted]

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

IdP Username Parameter*: uid

Username Parameter Name in Identity Provider

IdP Email Parameter*: email

Email Parameter Name in Identity Provider

IdP Given Name Parameter*: givenName

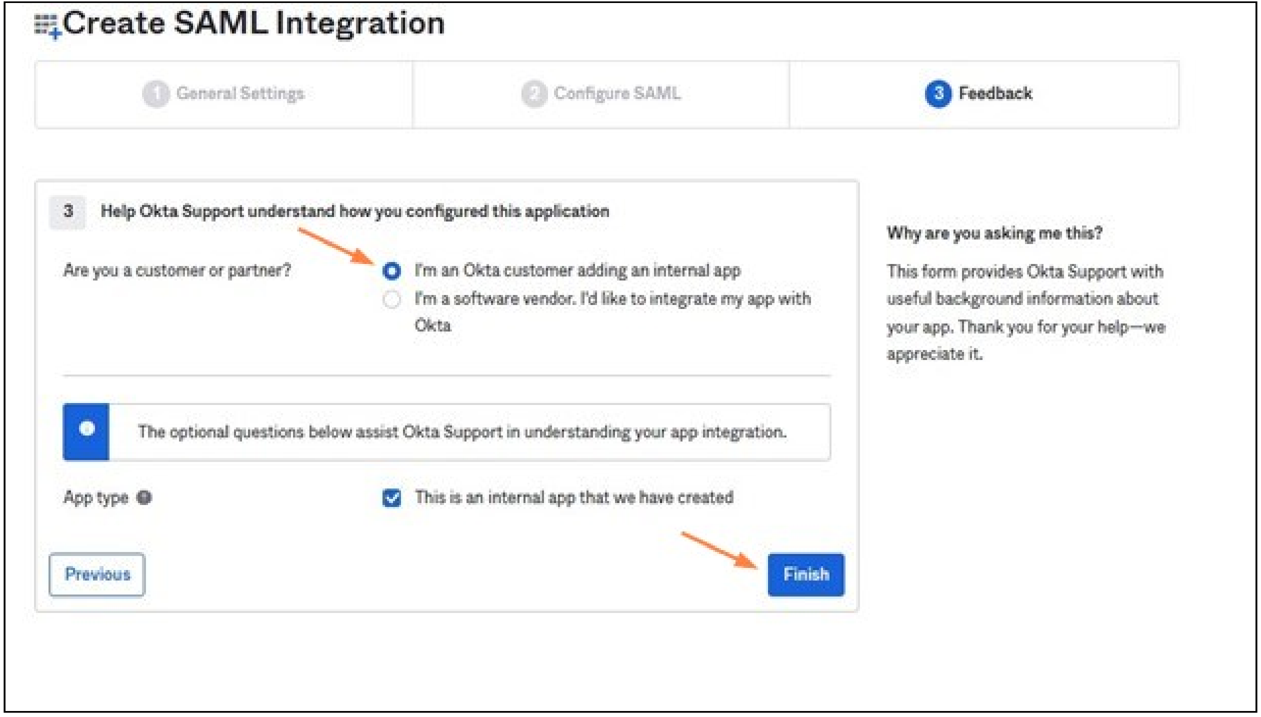
Given Name Parameter Name in Identity Provider

IdP Surname Parameter*: sn

Surname Parameter Name in Identity Provider

Enter these values into Attribute Statements

6. Click the **Feedback** tab of the **Create SAML Integration** screen, then select **I'm an Okta customer adding an internal app**, and click **Finish**.



Create SAML Integration

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

● I'm an Okta customer adding an internal app

○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

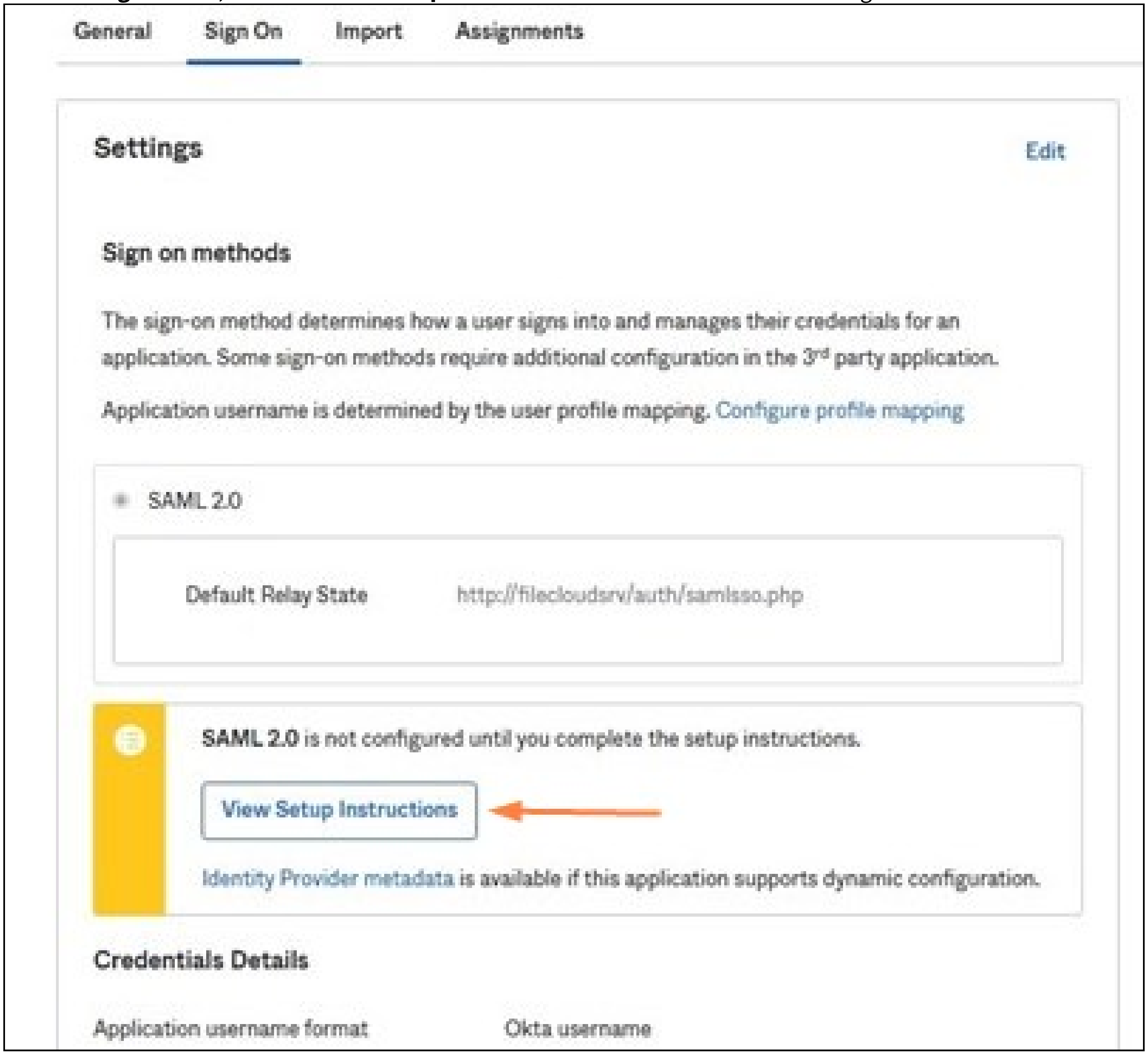
App type

☑ This is an internal app that we have created

Why are you asking me this?

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 .



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State http://filecloudsrv/auth/samlsso.php

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

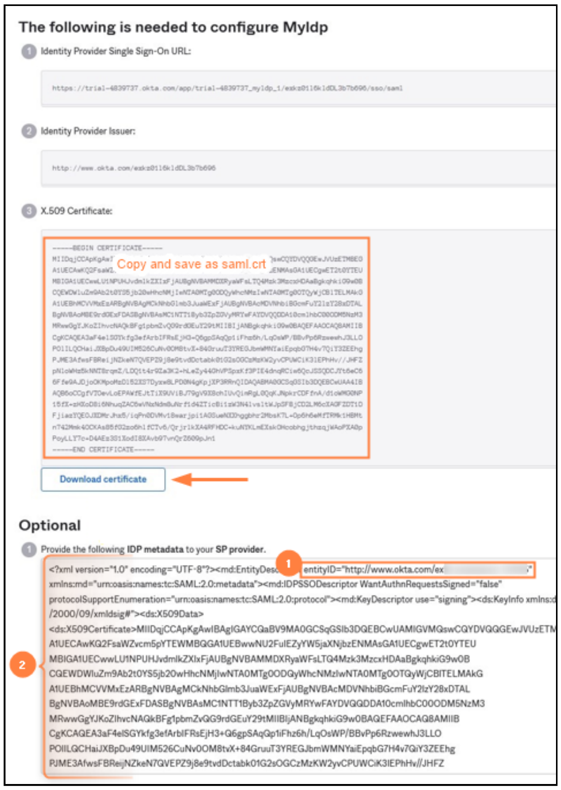
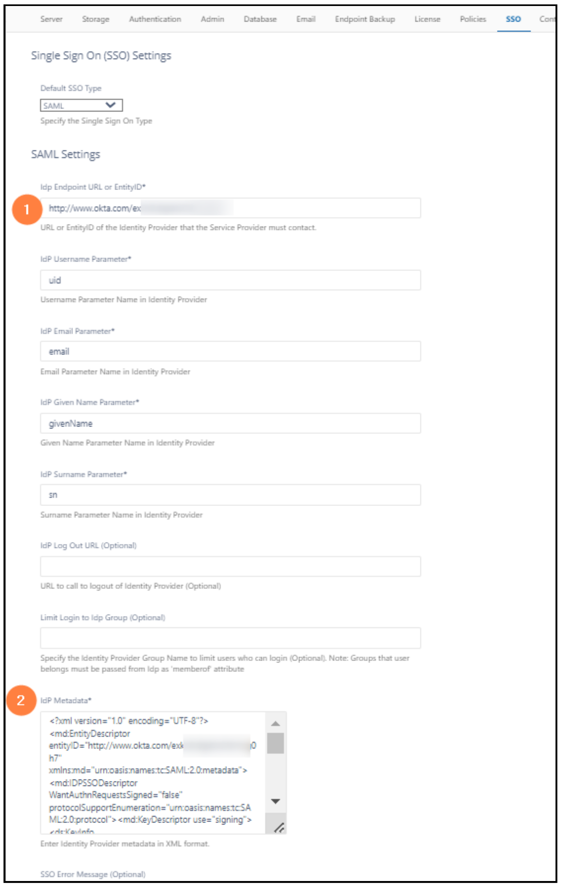
Credentials Details

Application username format Okta username

A screen with information similar to the first image in the table below opens.

8. Use the details in this screen to configure the settings in the FileCloud admin portal's **Settings > SSO** screen and to create a **saml.crt** file.
    a. Using the **IDP Metadata** text under **Optional**:
    (1) Copy the **entityID** field from the text box into **Idp Endpoint URL or EntityID** in FileCloud admin UI interface under **Settings > SSO**.
    (2) Confirm that the text in the **IDP Metadata** box is the same as the text in **Idp Metadata** in FileCloud admin UI interface under **Settings > SSO**.
    b. Click **Download certificate**, then copy the certificate file and rename it to **saml.crt**.

    Copy the **saml.crt** file in the FileCloud server in the following place **<FileCloud WEB ROOT>/thirdparty/simplesaml/cert**.

Okta Setup Instructions	FileCloud SSO Settings
	

The following is needed to configure MyIdp

1. Identity Provider Single Sign-On URL:

```
https://trial-4839737.okta.com/app/trial-4839737_myldp_1/exkz0116k1dDL3b7b696/sso/saml
```

2. Identity Provider Issuer:

```
http://www.okta.com/exkz0116k1dDL3b7b696
```

3. X.509 Certificate:

Copy and save as saml.crt

```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwI                                        QswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaW2                                        ENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTQ4Mzk3MzcxHDAaBgkqhkiG9w0B
CQEWDWluZm9Ab2t0YS5jb20wHhcNMjIwNTA0MTg0ODQyWhcNMzIwNTA0MTg0OTQyWjCBlTELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
BgNVBAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA10cmlhbC00ODM5NzM3
MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA3aF4elSGYkfg3efArbIFRsEjH3+Q6gpSAqQp1iFhz6h/LqOsWP/BBvPp6RzwewhJ3LLO
POIlLQCHaiJXBpDu49UIM526CuNv0OM8tvX+84GruuT3YREGJbmWMNYaiEpqbG7H4v7QiY3ZEEhg
PJME3AfwsFBReijNZkeN7QVEPZ9j8e9tvdDctabk01G2sOGCzMzKW2yvCPUWCiK3lEPhHv//JHFZ
pN1oWHz5kNNT8rqmZ/LDQ1t4r9Za3K2+hLeZy44GhVPSpxKf3PIE4dnqRCiw6QcJSSQDCJYt6eC6
6Ffe9AJDjoOKMpoMzD152XS7Dyxw8LPD0N4gKpjXP3RRnQIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
AQB6oCCgfV7OevLoEPAWfEJtTiX9UViBJ79gV9X8chIUvQimRgL0QqKJNpkrCDFfnA/d1oWMG0NP
15fX+zHXoD8i6NhuqZAC6wVNxNdm8uNrf1d4ZTicBi1zW3N4lvs1tWJpSF8jCD2LM6cXAGFZDT1D
FjiazYQEOJXDMrJhz5/iqPn0DVMv18warjpi1A0SueNXDhggbhr2MbsK7L+Op6h6eMfTRMk1HBMt
n742Mmk4OCKAs85f02zo6hlfCTv6/QrjrlkXA4RFHDC+kuNYKLmEXskOHcobhgjthzqjWAoPXA0p
PoyLLY7c+D4AEz3S1XodI8XAvb97vnQrZ609pJn1
-----END CERTIFICATE-----
```

Download certificate

Optional

1. Provide the following **IDP metadata** to your **SP provider.**

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDesc entityID="http://www.okta.com/ex[redacted]"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:d
/2000/09/xmldsig#"><ds:X509Data>
<ds:X509Certificate>MIIDqjCCApKgAwIBAgIGAYCQaBV9MA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETM
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXRyaWFsLTQ4Mzk3MzcxHDAaBgkqhkiG9w0B
CQEWDWluZm9Ab2t0YS5jb20wHhcNMjIwNTA0MTg0ODQyWhcNMzIwNTA0MTg0OTQyWjCBlTELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
BgNVBAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA10cmlhbC00ODM5NzM3
MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA3aF4elSGYkfg3efArbIFRsEjH3+Q6gpSAqQp1iFhz6h/LqOsWP/BBvPp6RzwewhJ3LLO
POIlLQCHaiJXBpDu49UIM526CuNv0OM8tvX+84GruuT3YREGJbmWMNYaiEpqbG7H4v7QiY3ZEEhg
PJME3AfwsFBReijNZkeN7QVEPZ9j8e9tvdDctabk01G2sOGCzMzKW2yvCPUWCiK3IEPhHv//JHFZ
```

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

Single Sign On (SSO) Settings

Default SSO Type: SAML

Specify the Single Sign On Type

SAML Settings

1 Idp Endpoint URL or EntityID*: http://www.okta.com/ex[redacted]

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

IdP Username Parameter*: uid

Username Parameter Name in Identity Provider

IdP Email Parameter*: email

Email Parameter Name in Identity Provider

IdP Given Name Parameter*: givenName

Given Name Parameter Name in Identity Provider

IdP Surname Parameter*: sn

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

2 IdP Metadata*:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor
entityID="http://www.okta.com/exk[redacted]0
h7"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<md:IDPSSODescriptor
WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SA
ML:2.0:protocol"><md:KeyDescriptor use="signing">
<ds:KeyInfo
```

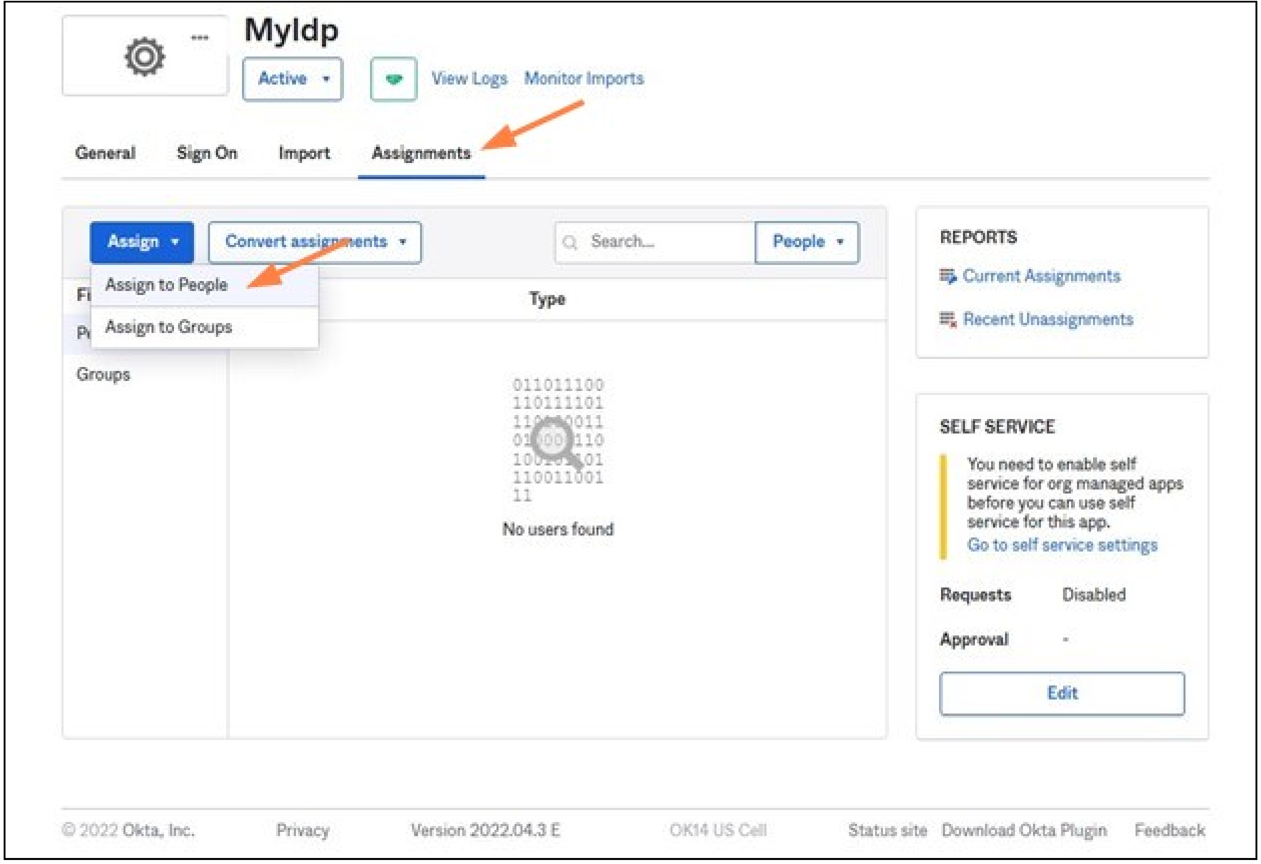
Enter Identity Provider metadata in XML format.

SSO Error Message (Optional)

Now assign the Okta FileCloud integration to users so they can log in with Okta.

9. Click the **Assignments** tab in Okta.

10. In the **Assign** drop-down list, choose **Assign to People**.



A list of users who have both Okta and FileCloud accounts opens.

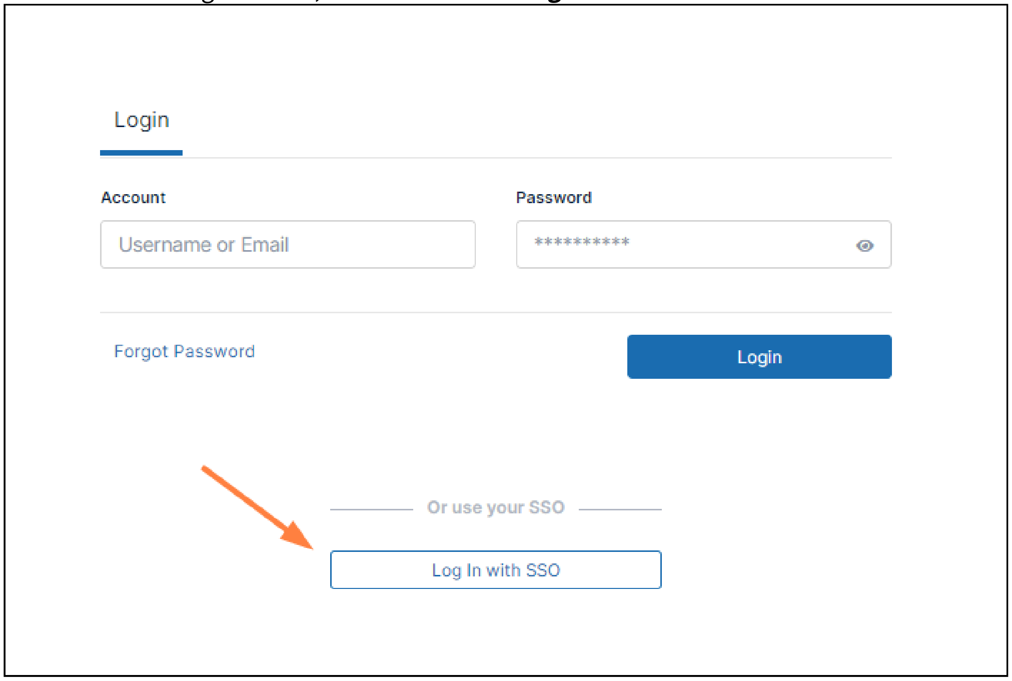
11. Select users from the list to allow them to sign in to FileCloud using Okta.

Once the application is created and FileCloud is configured you can start using single sign-on with Okta from FileCloud.

Log in to FileCloud using Single Sign-on with Okta

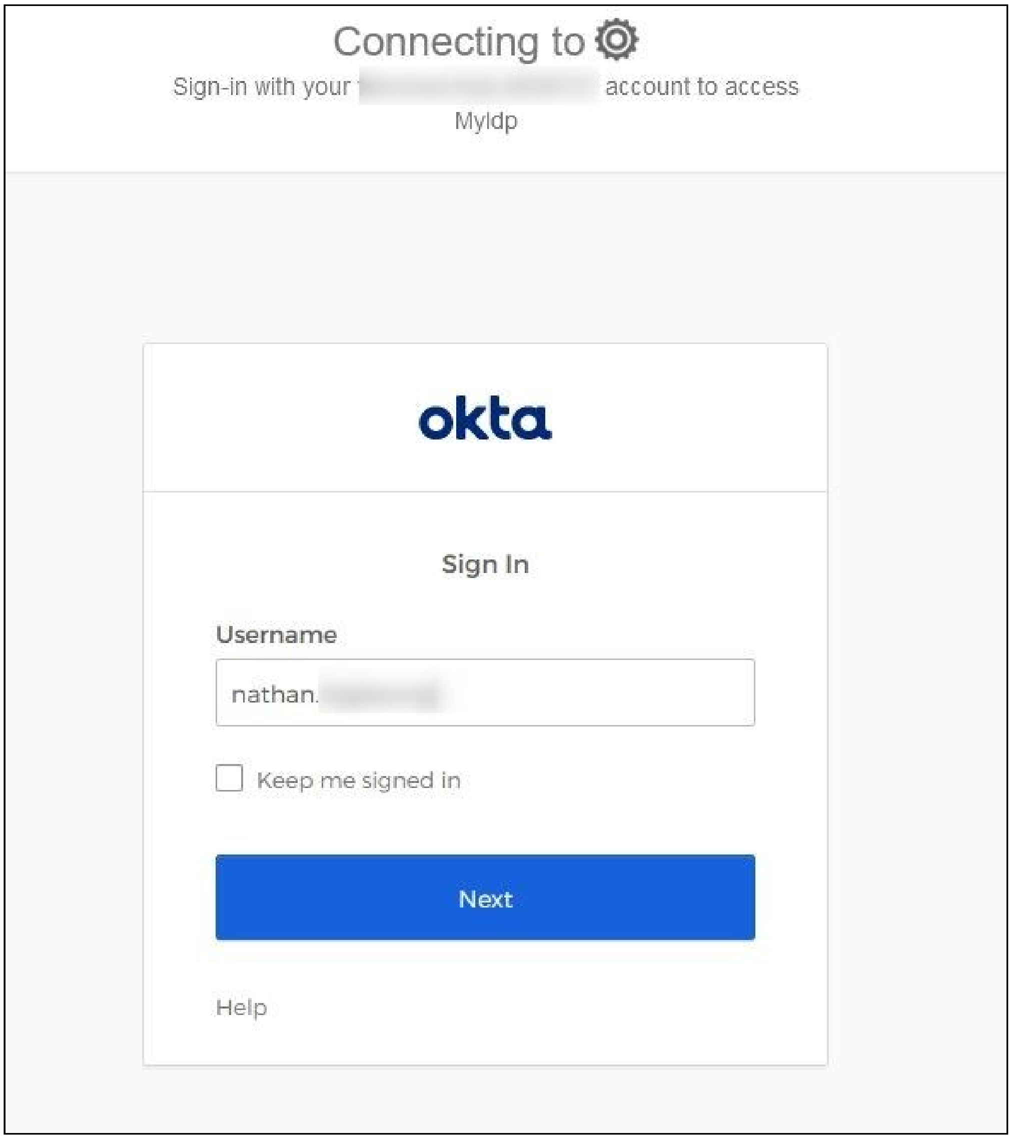
Users can sign in to the user portal or admin portal with SSO using Okta.

1. In the FileCloud login screen, the user chooses **Log in with SSO**.



If the user is already logged in to Okta, they are automatically logged in to FileCloud.

If the user not logged in to Okta, they are first redirected to the Okta sign in page, and after signing in to Okta, they are immediately redirected to FileCloud and logged in.



Connecting to ⚙

Sign-in with your [redacted] account to access MyIdp

okta

Sign In

Username

nathan.[redacted]

☐ Keep me signed in

Integrate with Okta using browser plugin

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

The Okta plugin for browsers works by storing FileCloud user credentials in a web application that you add to Okta. After a user chooses to log in with Okta, the credentials are entered in the FileCloud page and log in proceeds automatically.

The Okta plugin works with default FileCloud login, not SSO. Do not configure SSO settings in FileCloud. If the setting: define("TONIDOCLOUD_SSO_DIRECT_ONLY",1) appears in your cloudconfig.php file, remove or disable it.

Procedure:

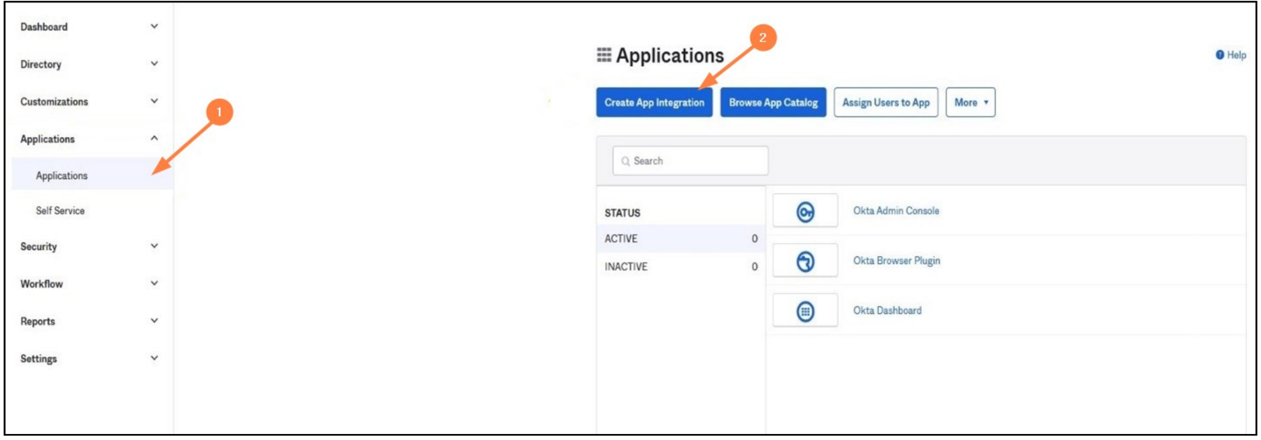
Note: You must have an Okta account before completing these steps.

1. Set up the FileCloud application in the Okta admin panel
2. Assign the FileCloud application to users
3. Install the plugin on the user browser.
4. User logs in to FileCloud using the plugin.

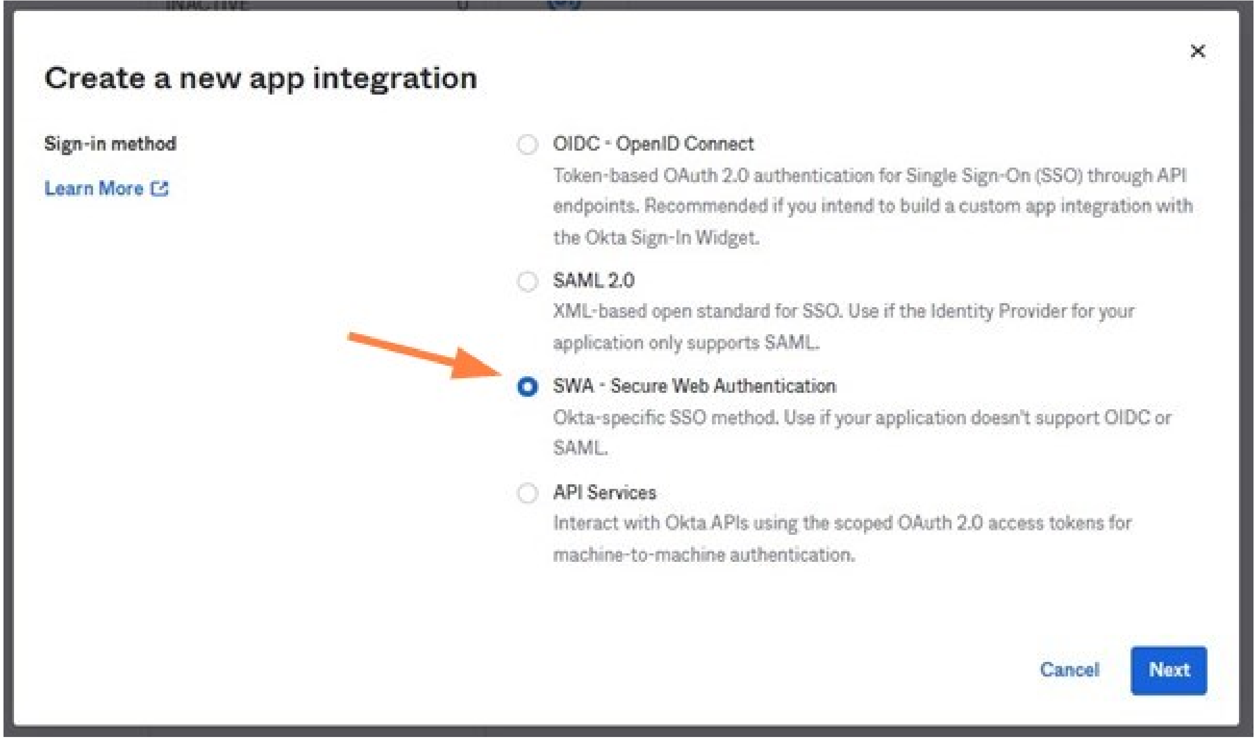
> ⓘ The plugin supports different browsers. Setup and tests for this guide use Google Chrome.

Set up the FileCloud application in Okta admin panel

1. Log in as Admin in Okta.
2. In the navigation panel, click **Applications > Applications**.
3. In the **Applications** screen, click **Create App Integration**.



4. In the **Create a new app integration** screen, choose **SWA - Secure Web Authentication**, and click **Next**.



Create a new app integration

Sign-in method

Learn More

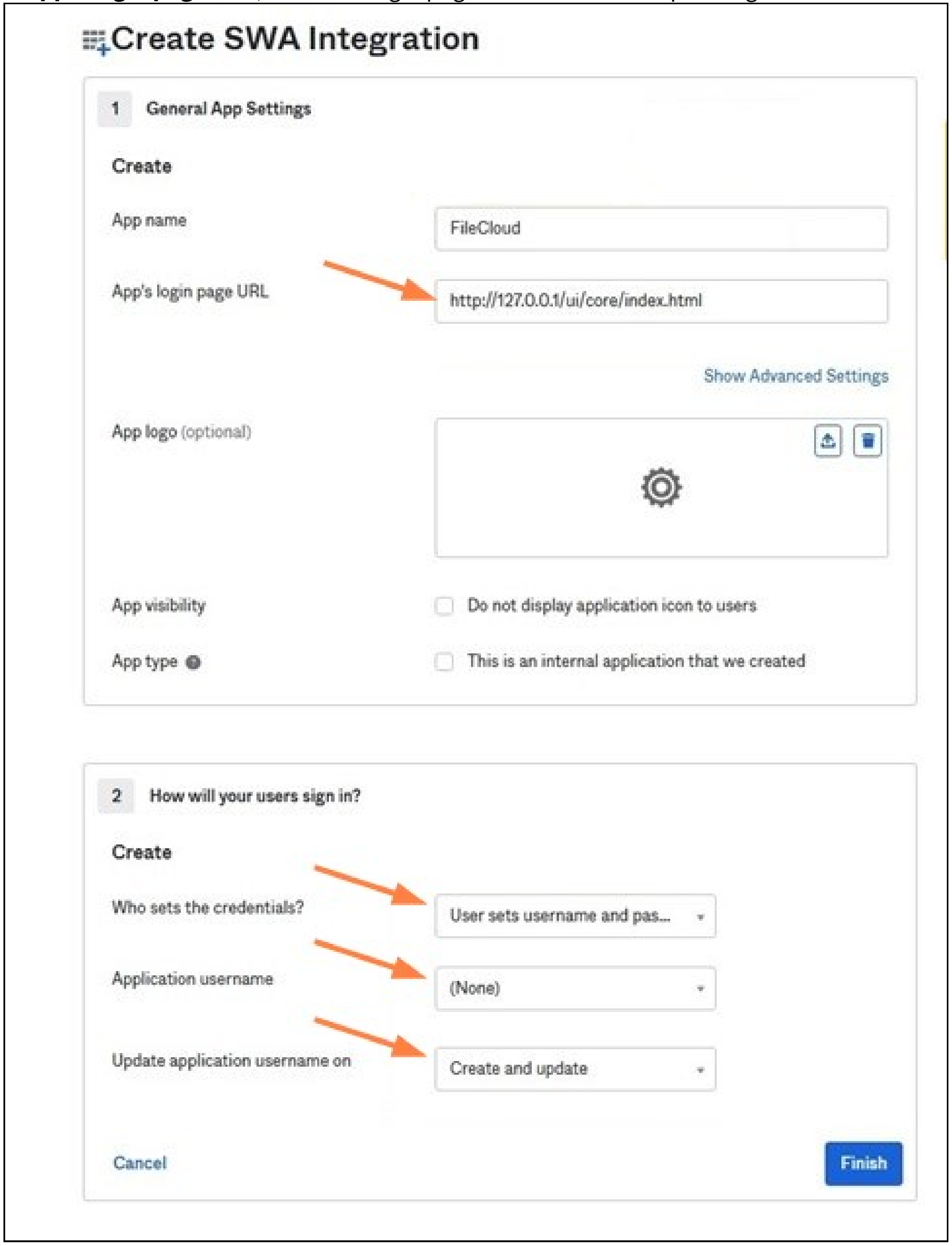
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ 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.

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)

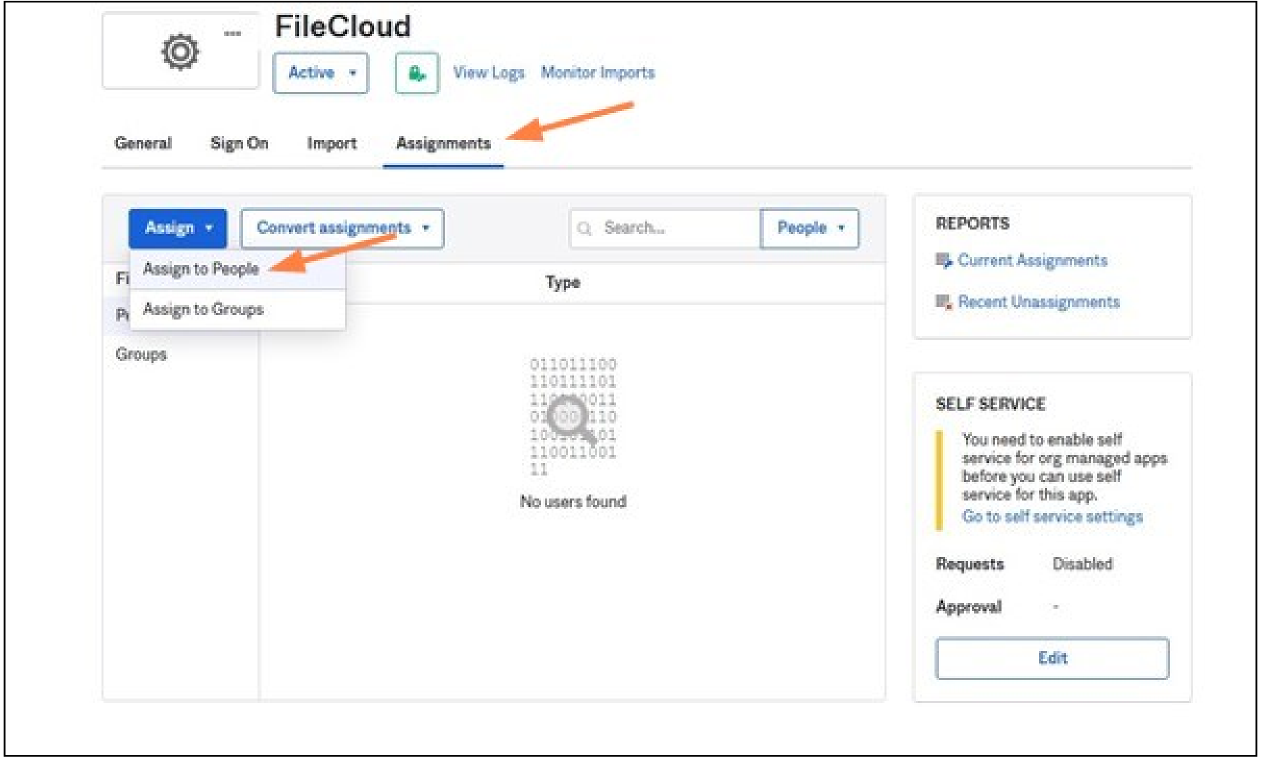
Update application username on: Create and update

Assign application to users

Now assign the Okta FileCloud integration to users so they can log in with Okta.

1. Click the **Assignments** tab in Okta.

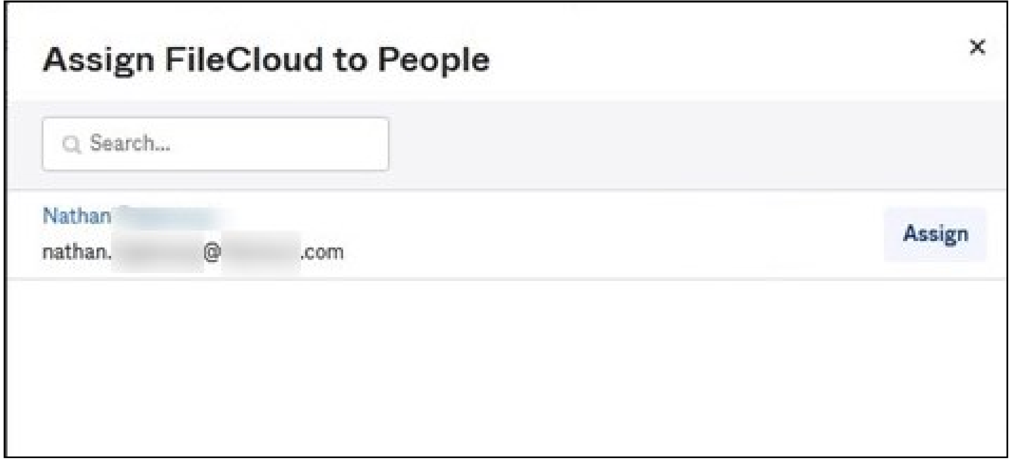
2. In the **Assign** drop-down list, choose **Assign to People**.



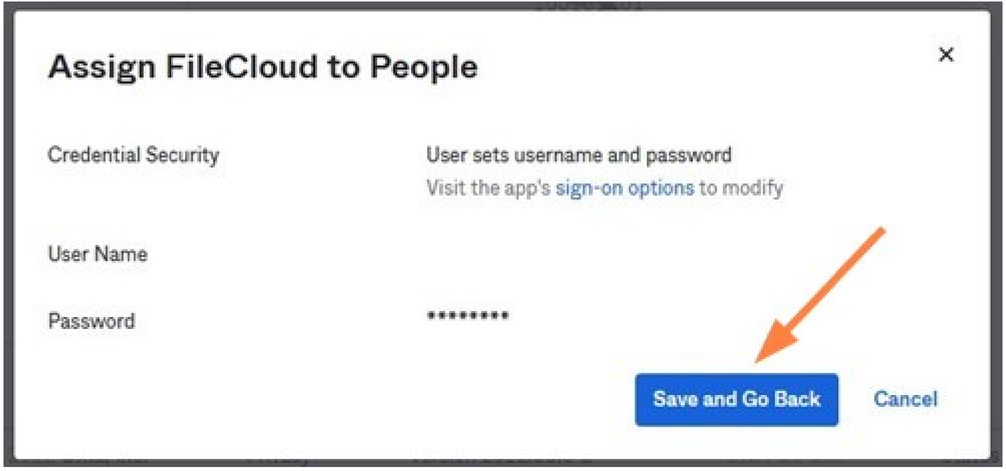
You need to enable self service for org managed apps before you can use self service for this app. Go to self service settings

A list of users who have both Okta and FileCloud accounts opens.

3. To allow users to sign in to FileCloud using Okta, click **Assign** in the row with their email.



4. Enter a **User Name** and **Password** for the user, then click **Save and Go Back**.



Assign FileCloud to People

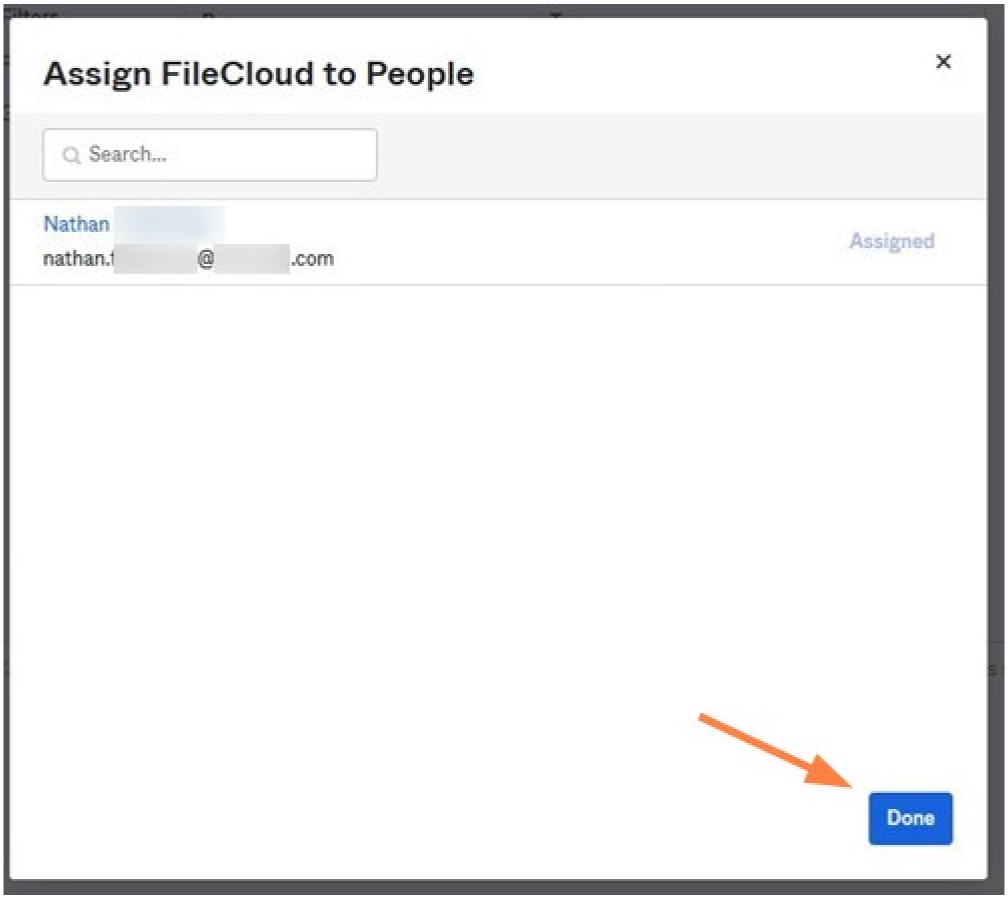
Credential Security: User sets username and password
Visit the app's sign-on options to modify

User Name

Password: *********

ck

5. Click **Done**.



Assign FileCloud to People

Search...

Nathan [redacted]
nathan.[redacted]@[redacted].com
Assigned

6. Repeat this process for all users you want to assign to the integration.

Install the Plugin in the Browser

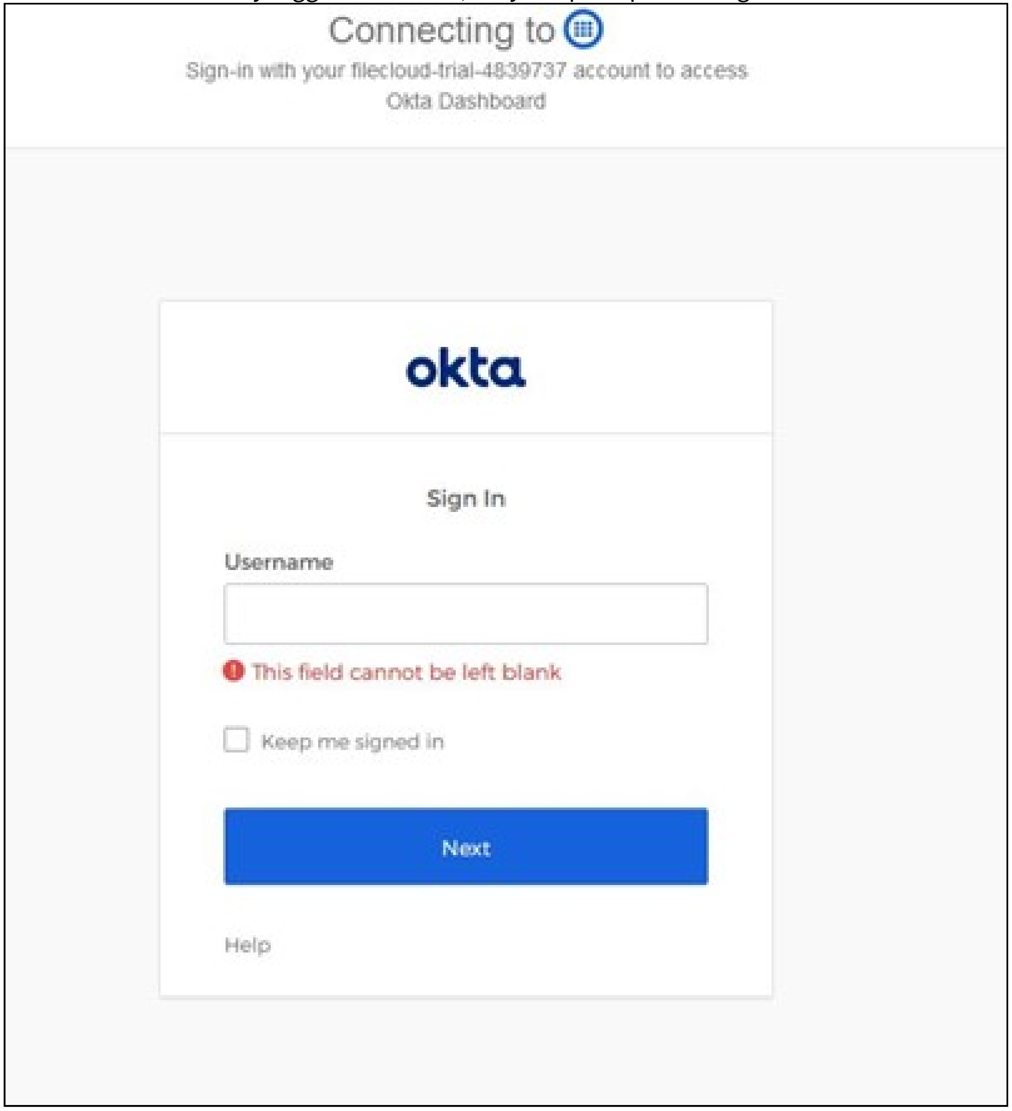
Information on plugin installation is available here:

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.

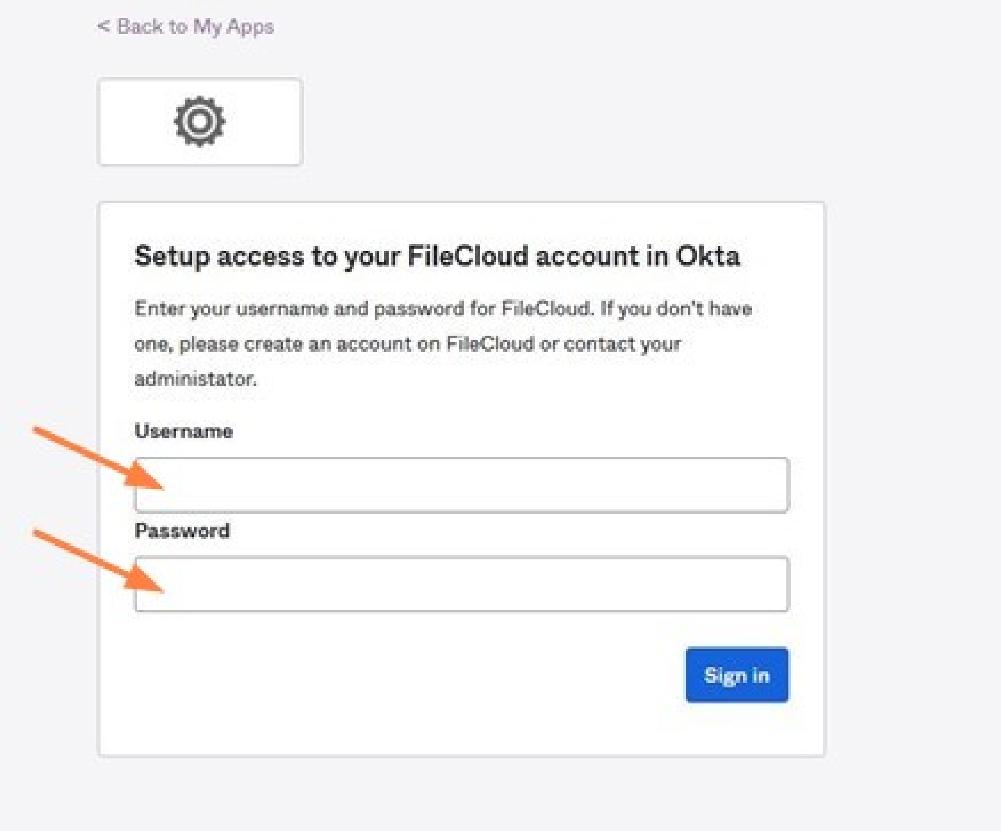


Connecting to

Sign-in with your filecloud-trial-4839737 account to access Okta Dashboard

This field cannot be left blank

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

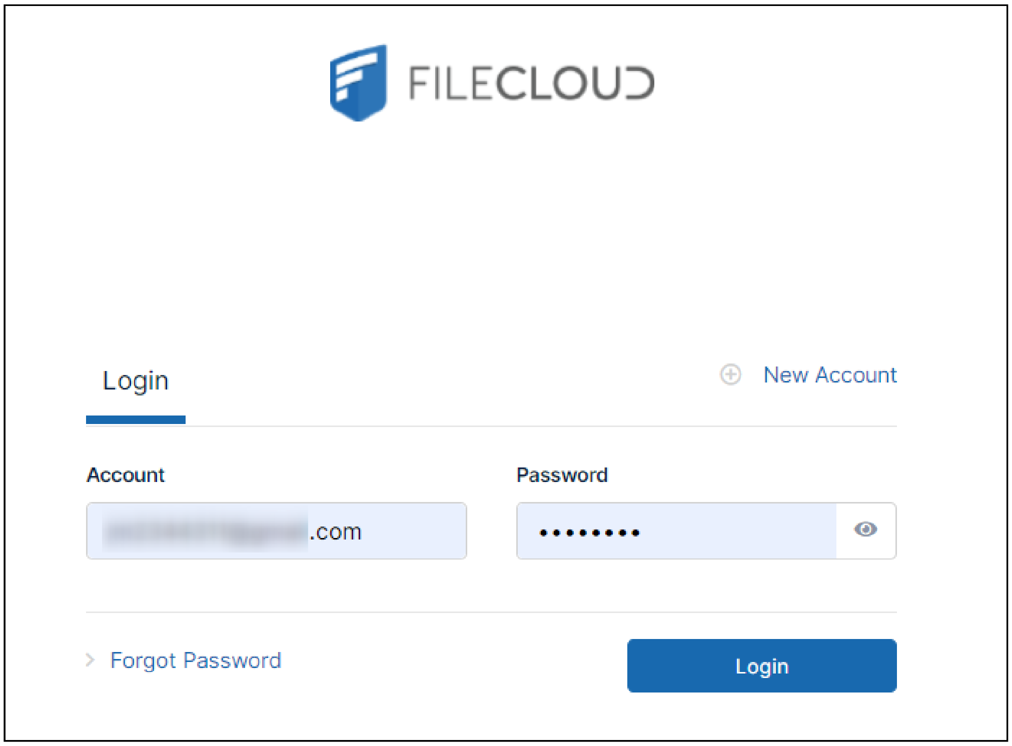
Setup access to your FileCloud account in Okta

Enter your username and password for FileCloud. If you don't have one, please create an account on FileCloud or contact your administator.

Username

Password

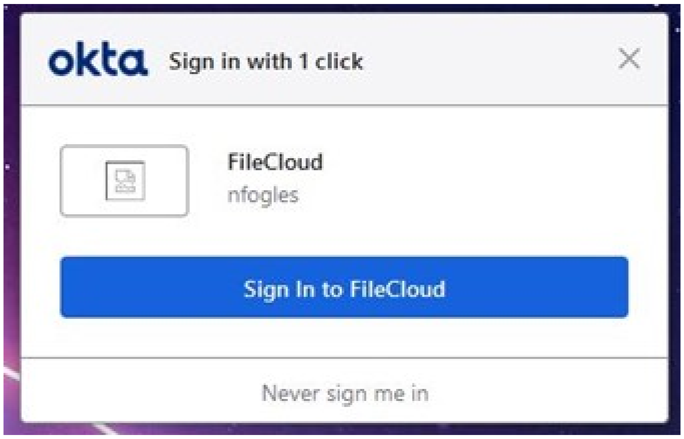
4. The browser redirects the user to the FileCloud login page in the Okta Admin Panel. The login screen with credentials filled in may appear first, and after a few seconds the FileCloud user portal should open (the user does not need to click **Login**).



Account: [redacted].com

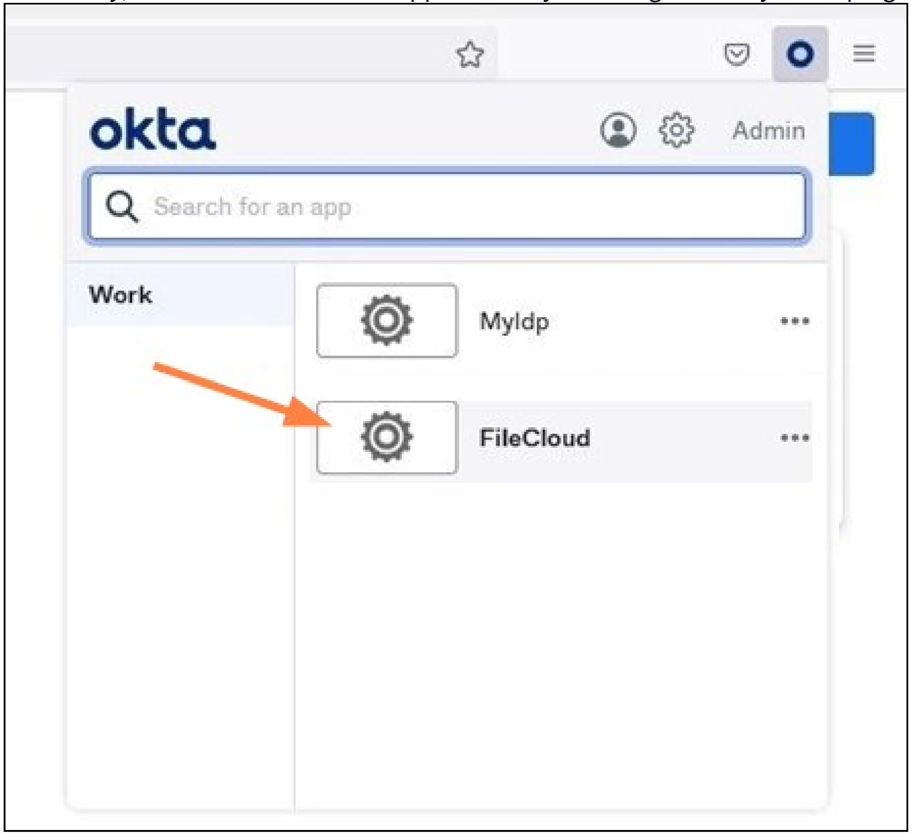
Password: ••••••••

Depending on the browser, when the user accesses the FileCloud login page again, the plugin may offer to log in for them:



FileCloud
nfogles

Alternately, the user can access the application by choosing it directly in the plugin:



t

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.

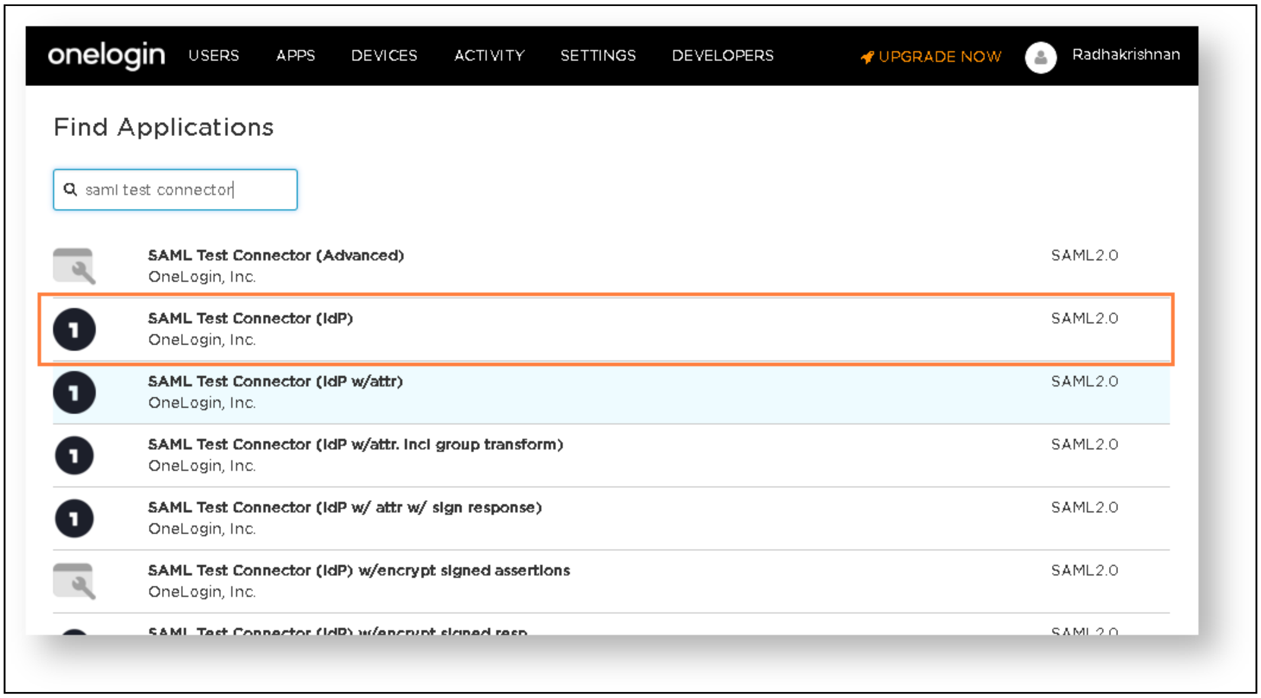
This article describes how to integrate OneLogin as an SSO provider with FileCloud.

⚠ **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

3. Search for "saml test connector" and select the sample connector named "SAML Test Connector (IdP)".



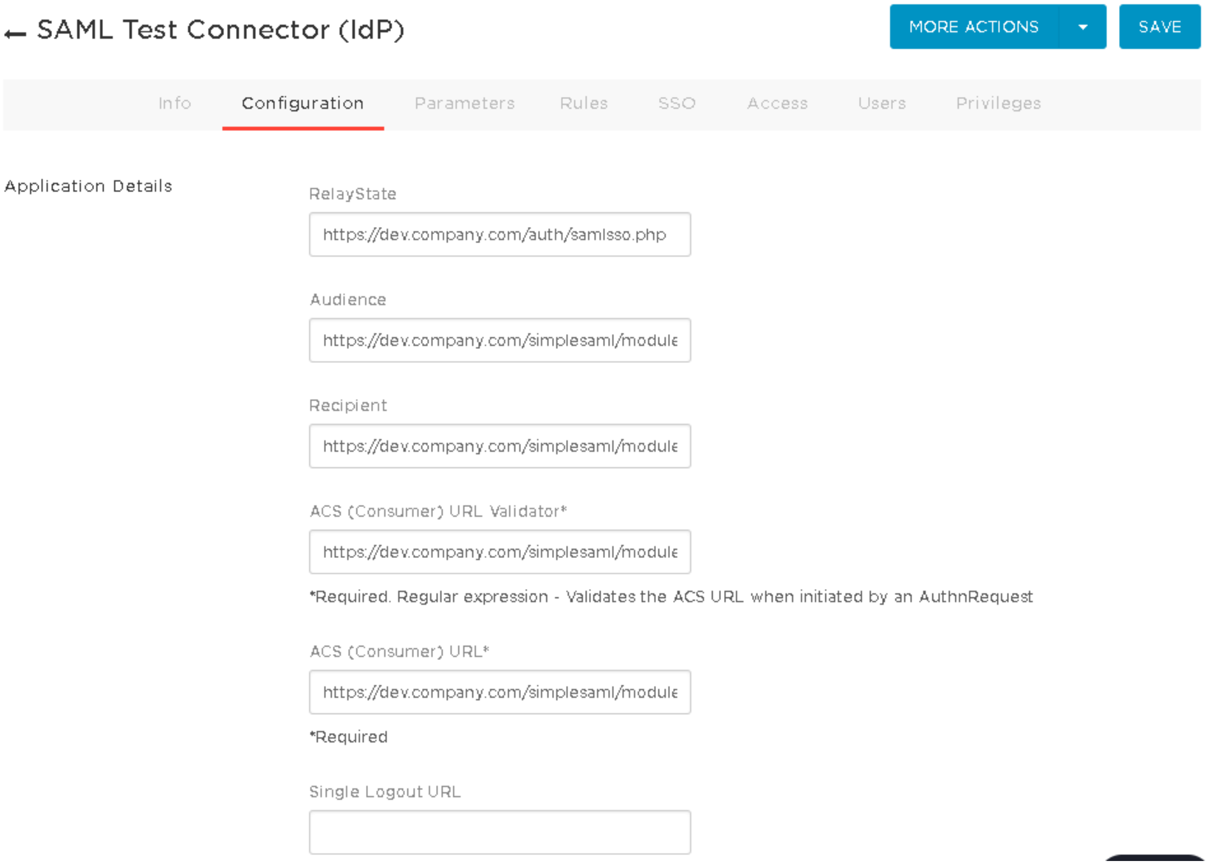
Find Applications

saml test connector

SAML Test Connector (Advanced) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP w/attr) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP w/attr. incl group transform) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP w/ attr w/ sign response) OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP) w/encrypt signed assertions OneLogin, Inc.	SAML2.0
SAML Test Connector (IdP) w/encrypt signed resp	SAML2.0

4. In the add screen, enter a name to the connector. For example, something like "FileCloud Connector". Click "Save".
5. Open the created connector and switch to "Configuration" tab.
6. 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/samlsso.php
Audience	https://dev.company.com/simplesaml/module.php/saml/sp/metadata.php/default-sp
Recipient	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL Validator*	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
ACS (Consumer) URL*	https://dev.company.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp



Application Details

RelayState: https://dev.company.com/auth/samlsso.php

Audience: https://dev.company.com/simplesaml/module

Recipient: https://dev.company.com/simplesaml/module

ACS (Consumer) URL Validator*: https://dev.company.com/simplesaml/module

*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest

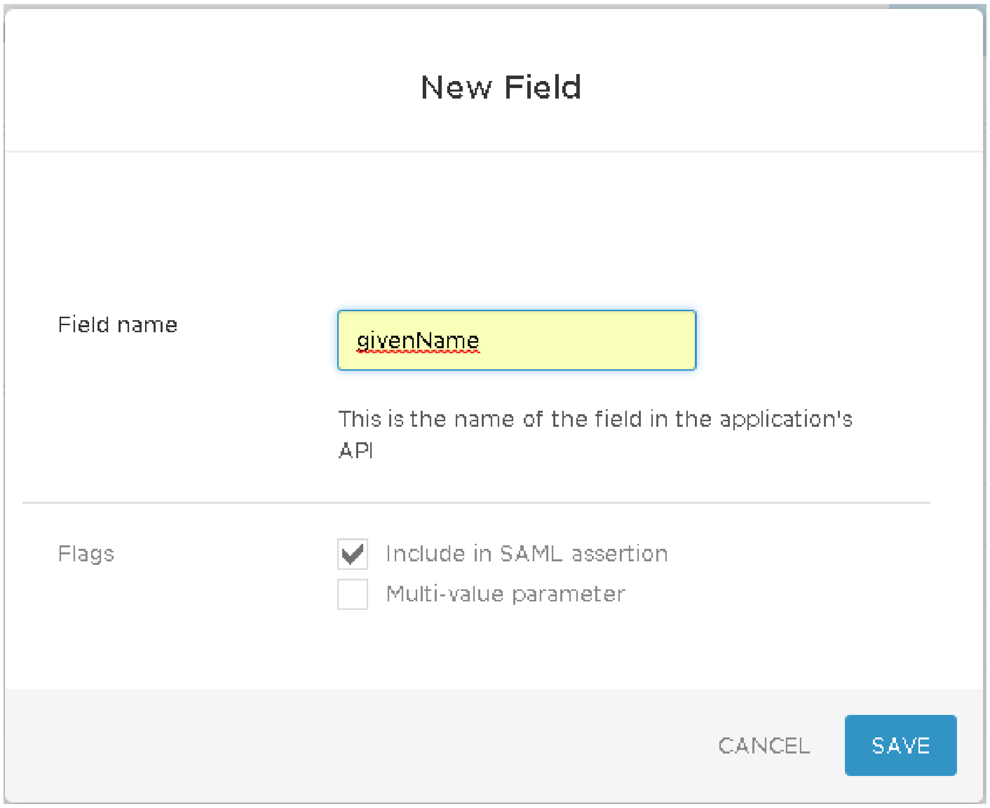
ACS (Consumer) URL*: https://dev.company.com/simplesaml/module

*Required

Single Logout URL:

7. Once the configuration tab is completed, switch to "Parameters" tab.
8. 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



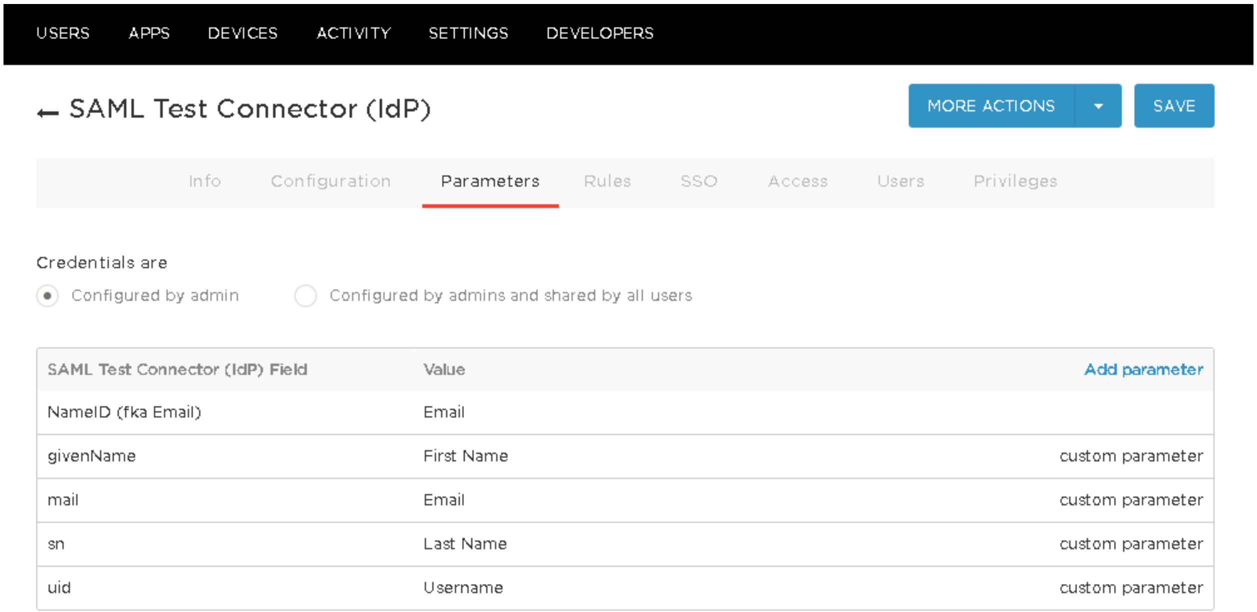
Field name: givenName

This is the name of the field in the application's API

Flags

☑ Include in SAML assertion

☐ Multi-value parameter



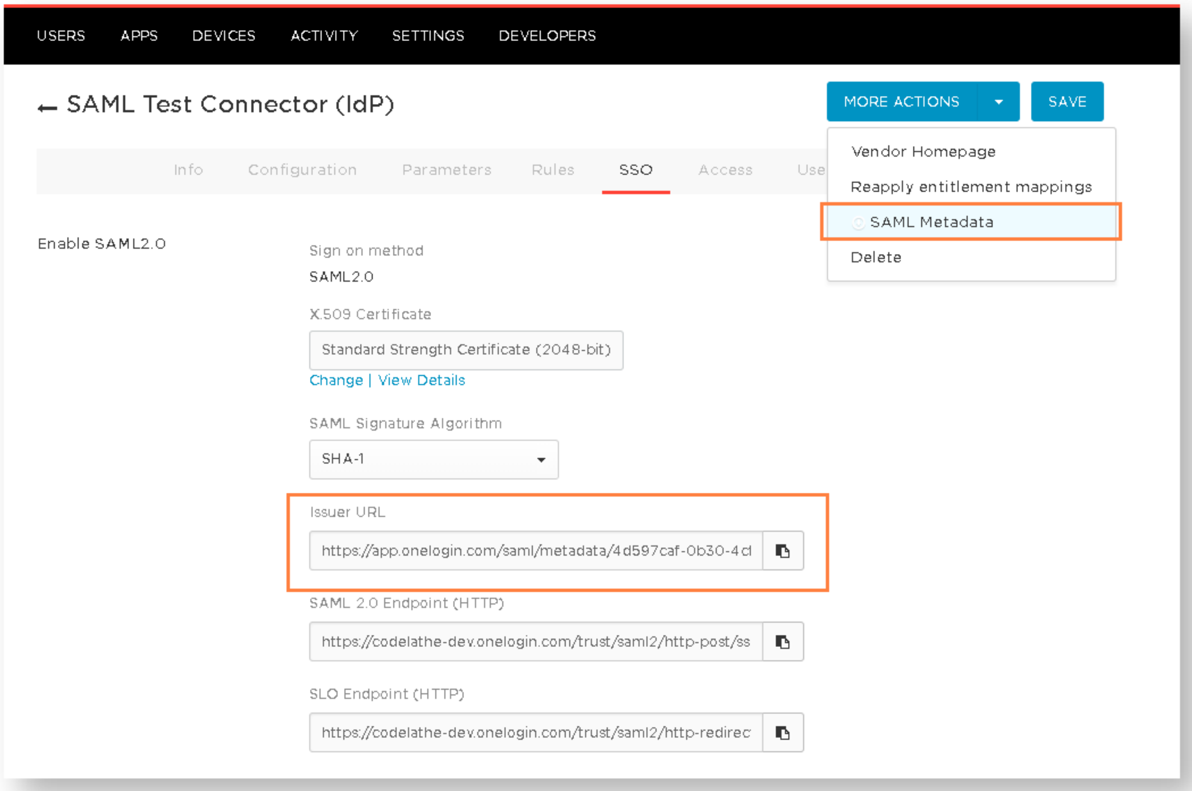
Credentials are

● 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".



Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)

SAML Signature Algorithm
SHA-1

Issuer URL
https://app.onelogin.com/saml/metadata/4d597caf-0b30-4d

SAML 2.0 Endpoint (HTTP)
https://codelathe-dev.onelogin.com/trust/saml2/http-post/ss

SLO Endpoint (HTTP)
https://codelathe-dev.onelogin.com/trust/saml2/http-redirec

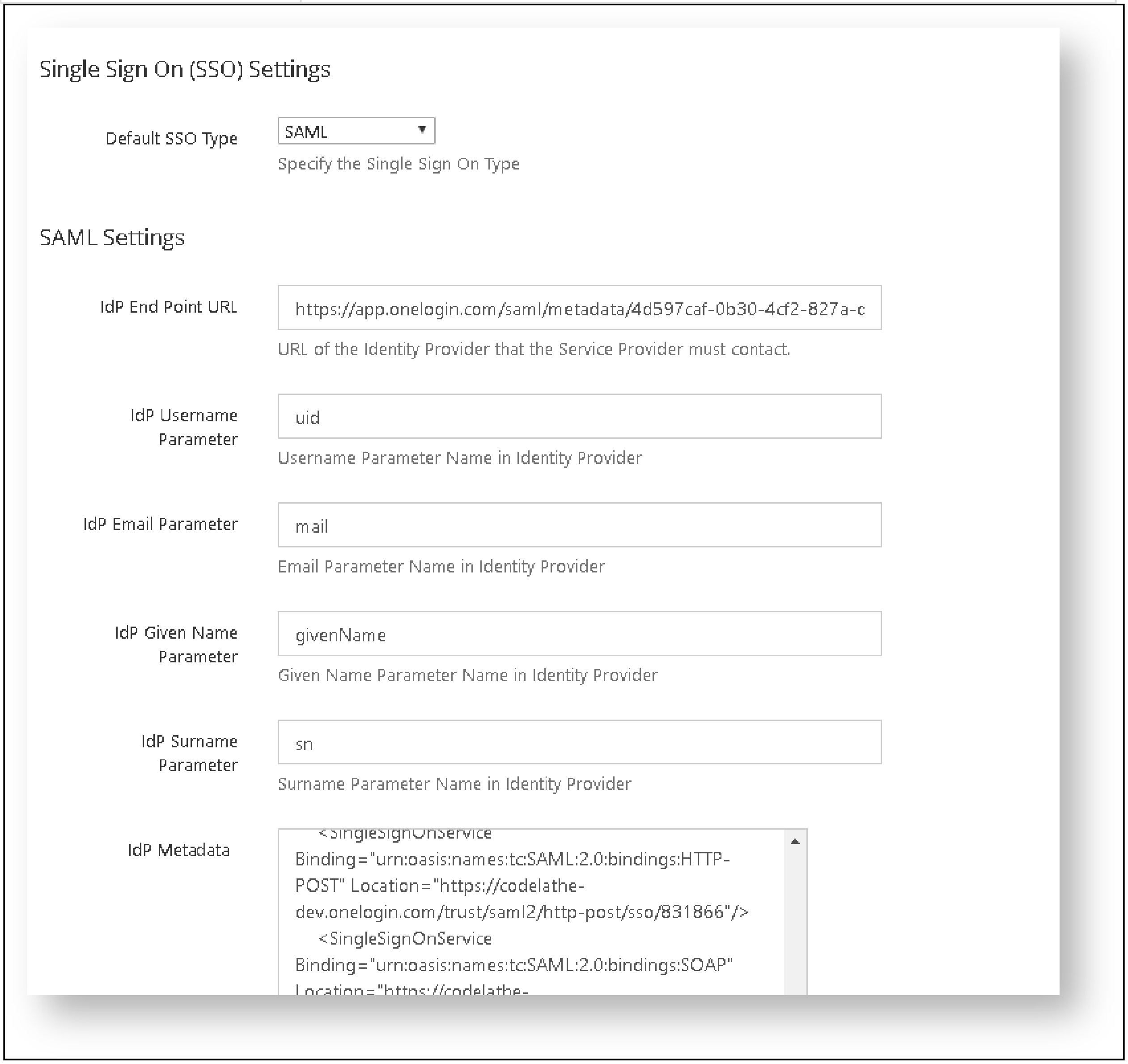
12. Finally, add users to the newly created "FileCloud Connector" either individually or as group.

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: SAML
Specify the Single Sign On Type

SAML Settings

IdP End Point URL: https://app.onelogin.com/saml/metadata/4d597caf-0b30-4cf2-827a-c
URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter: uid
Username Parameter Name in Identity Provider

IdP Email Parameter: mail
Email Parameter Name in Identity Provider

IdP Given Name Parameter: givenName
Given Name Parameter Name in Identity Provider

IdP Surname Parameter: sn
Surname Parameter Name in Identity Provider

IdP Metadata:

```
    <SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://codelathe-
dev.onelogin.com/trust/saml2/http-post/sso/831866"/>
    <SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://codelathe-
```

5. Save the changes

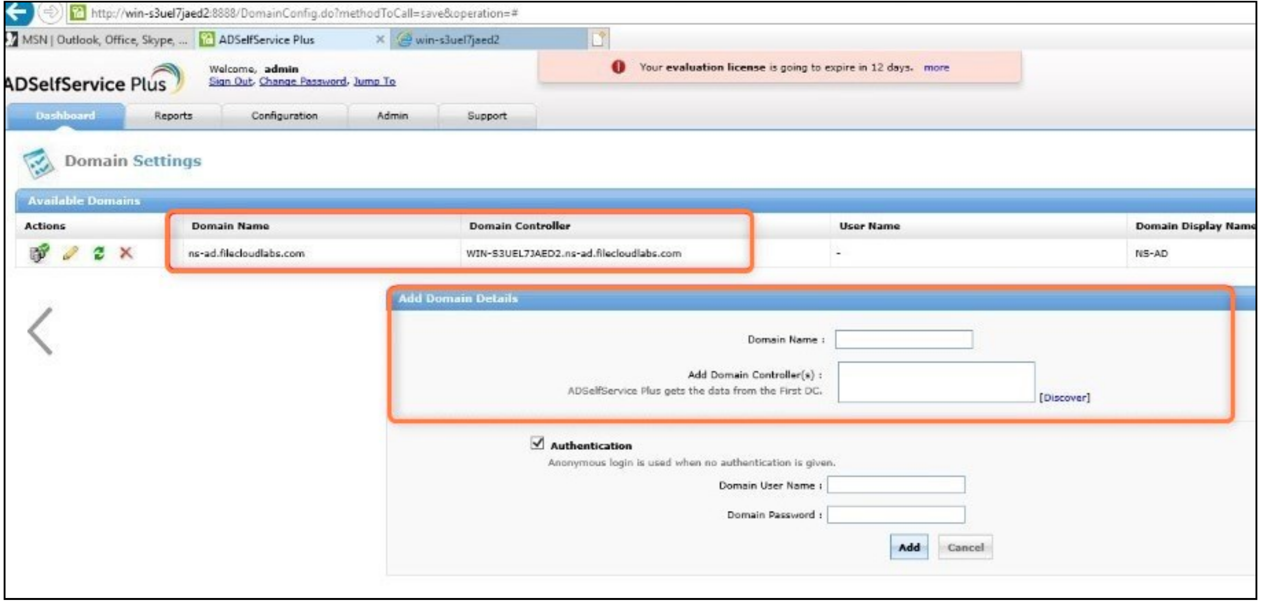
Integrate ADSelfService Plus with FileCloud

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**.



http://win-s3uel7jaed2:8888/DomainConfig.do?methodToCall=save&operation=#

Your evaluation license is going to expire in 12 days. more

Welcome, admin

Domain Settings

Available Domains

Actions	Domain Name	Domain Controller	User Name	Domain Display Name
	ns-ad.filecloudlabs.com	WIN-S3UEL7JAED2.ns-ad.filecloudlabs.com	-	NS-AD

Add Domain Details

Domain Name :

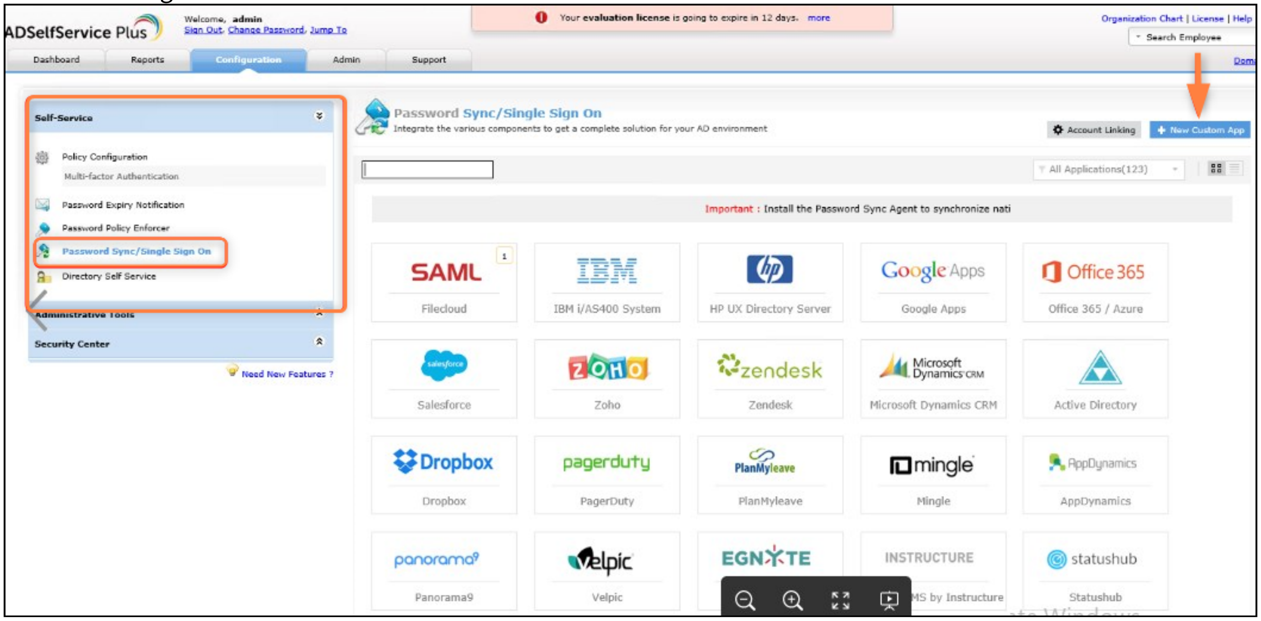
Add Domain Controller(s) :
ADSelfService Plus gets the data from the First DC.

☑ Authentication
Anonymous login is used when no authentication is given.

Domain User Name :

Domain Password :

4. Click the Configuration tab.



Your evaluation license is going to expire in 12 days. more

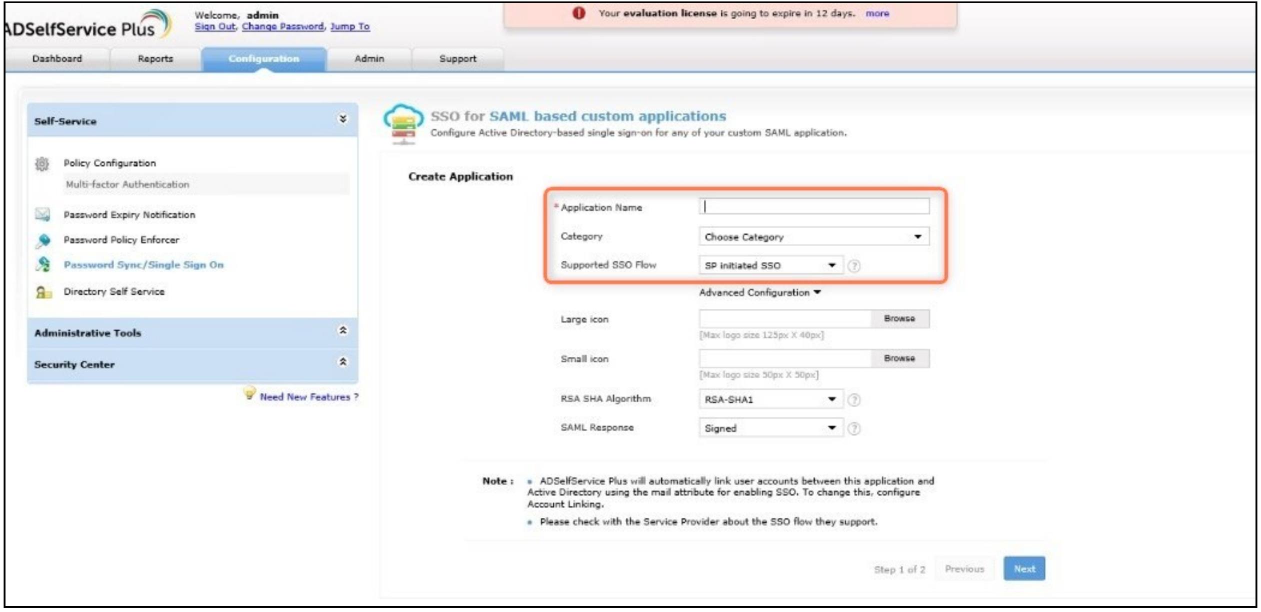
Welcome, admin

Password Sync/Single Sign On
Integrate the various components to get a complete solution for your AD environment

Important : Install the Password Sync Agent to synchronize nati

5. In the navigation bar, expand **Self-Service** and click **Password Sync/Single-Sign-On**.

6. Click **New Custom App**.



Your **evaluation license** is going to expire in 12 days. more

SSO for SAML based custom applications

Configure Active Directory-based single sign-on for any of your custom SAML application.

Create Application

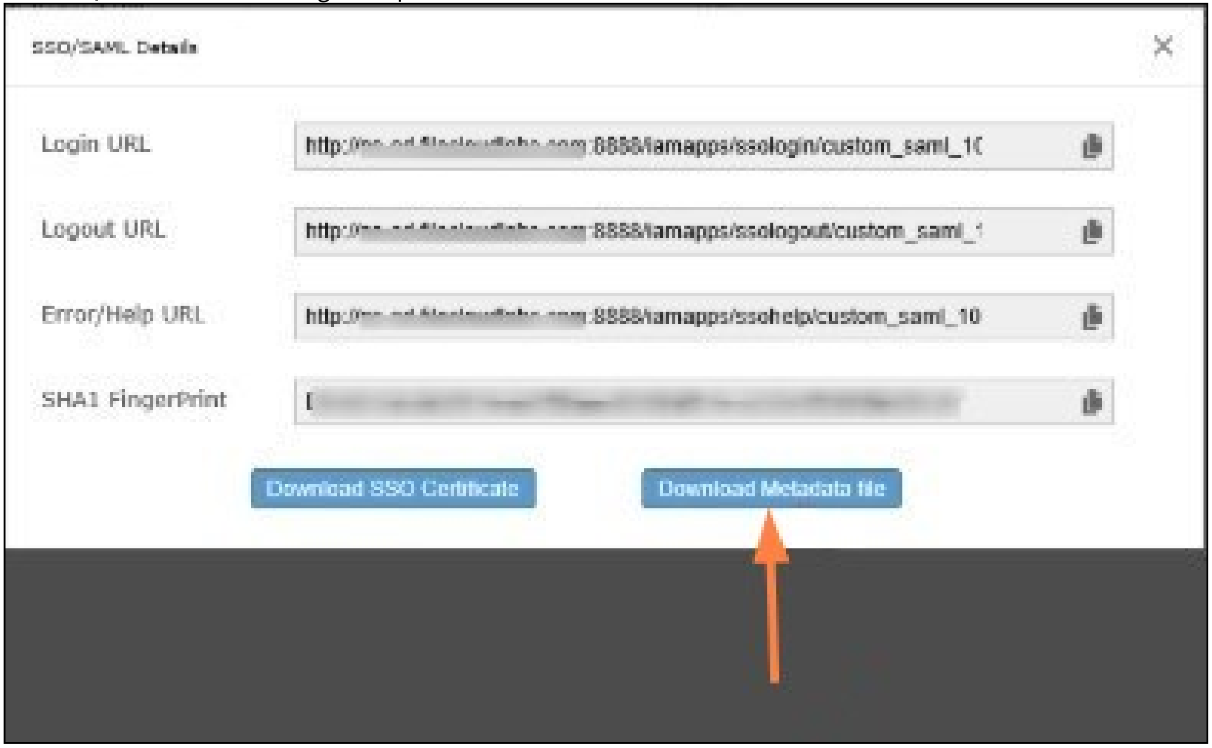
* Application Name:
Category: Choose Category
Supported SSO Flow: SP initiated SSO
Large icon: [Max logo size 125px X 40px]
Small icon: [Max logo size 50px X 50px]
RSA SHA Algorithm: RSA-SHA1
SAML Response: Signed

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

7. Fill in the following **Create Application** fields:
   a. In **Application Name** enter **FileCloud.**
   b. In **Category** drop-down list, choose any option.
   c. In the **Supported SSO flow** drop-down list,choose **SP initiated SSO.**
      The **Large icon** and **Small icon** fields are optional. You can leave the defaults for the remaining fields.
8. To go to the **SSO for SAML based custom applications/Configure Application** page, click **Next.**
9. Fill in the following **Configure Application** fields:
   a. In **Domain Name**, enter the domain name of your user’s email address in AD.
      For example, if the email address is fc@test.com, enter test.com as the domain name.
   b. In **Display Name** enter any name.
   c. In **SAML Redirect URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/metadata.php/default-sp
   d. In **ACS URL** enter https://yourFileclouddomainname/simplesaml/module.php/saml/sp/saml2-acs.php/default-s
10. Click **Save**.

11. Click **Download SSO certificate** in the upper-right of the page.
    The **SSO/SAML Details** dialog box opens.



Login URL: http://[redacted]:8888/iamapps/ssologin/custom_saml_1

Logout URL: http://[redacted]:8888/iamapps/ssologout/custom_saml_1

Error/Help URL: http://[redacted]:8888/iamapps/ssohelp/custom_saml_10

SHA1 FingerPrint: [redacted]

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.

> ⓘ 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**.

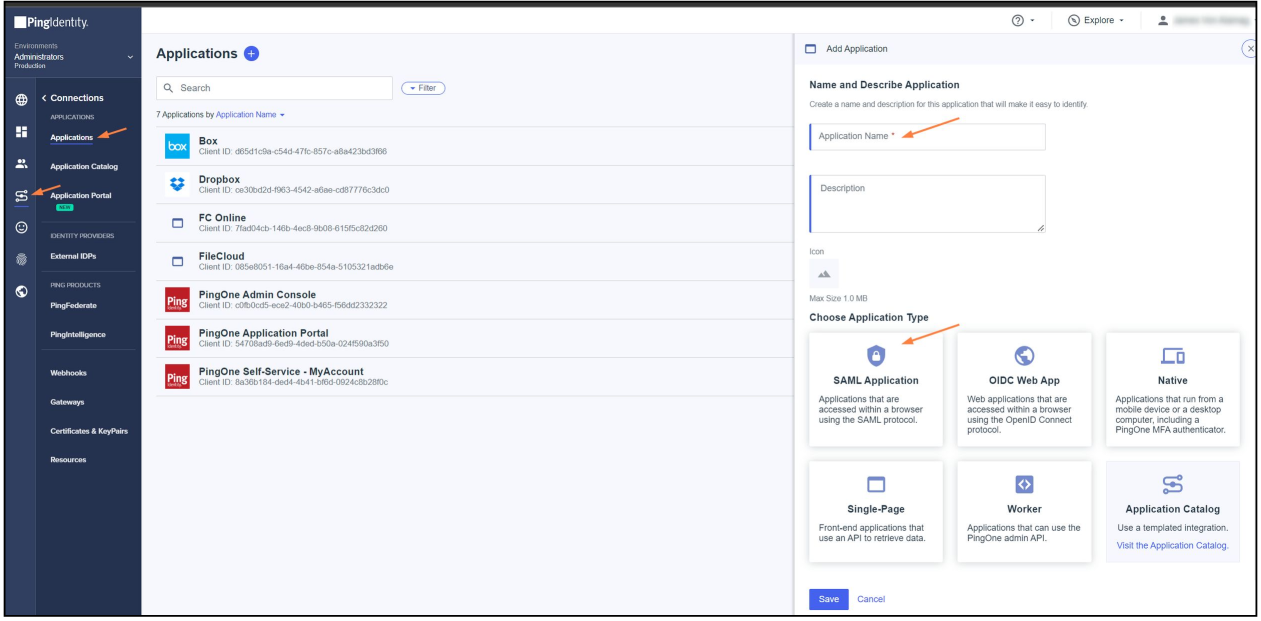
Integrate Ping Identity SSO with Filecloud

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.



7 Applications by Application Name

Box
Client ID: d65d1c9a-c54d-47fc-857c-a8a423bd3f66

Dropbox
Client ID: ce30bd2d-f963-4542-a6ae-cd87776c3dc0

FC Online
Client ID: 7fad04cb-146b-4ec8-9b08-615f5c82d260

FileCloud
Client ID: 085e8051-16a4-46be-854a-5105321adb6e

PingOne Admin Console
Client ID: c0fb0cd5-ece2-40b0-b465-f56dd2332322

PingOne Application Portal
Client ID: 54708ad9-6ed9-4ded-b50a-024f590a3f50

PingOne Self-Service - MyAccount
Client ID: 8a36b184-ded4-4b41-bf6d-0924c8b28f0c

Name and Describe Application

Create a name and description for this application that will make it easy to identify.

Application Name *

Description

Icon

Max Size 1.0 MB

Choose Application Type

SAML Application — Applications that are accessed within a browser using the SAML protocol.

OIDC Web App — Web applications that are accessed within a browser using the OpenID Connect protocol.

Native — Applications that run from a mobile device or a desktop computer, including a PingOne MFA authenticator.

Single-Page — Front-end applications that use an API to retrieve data.

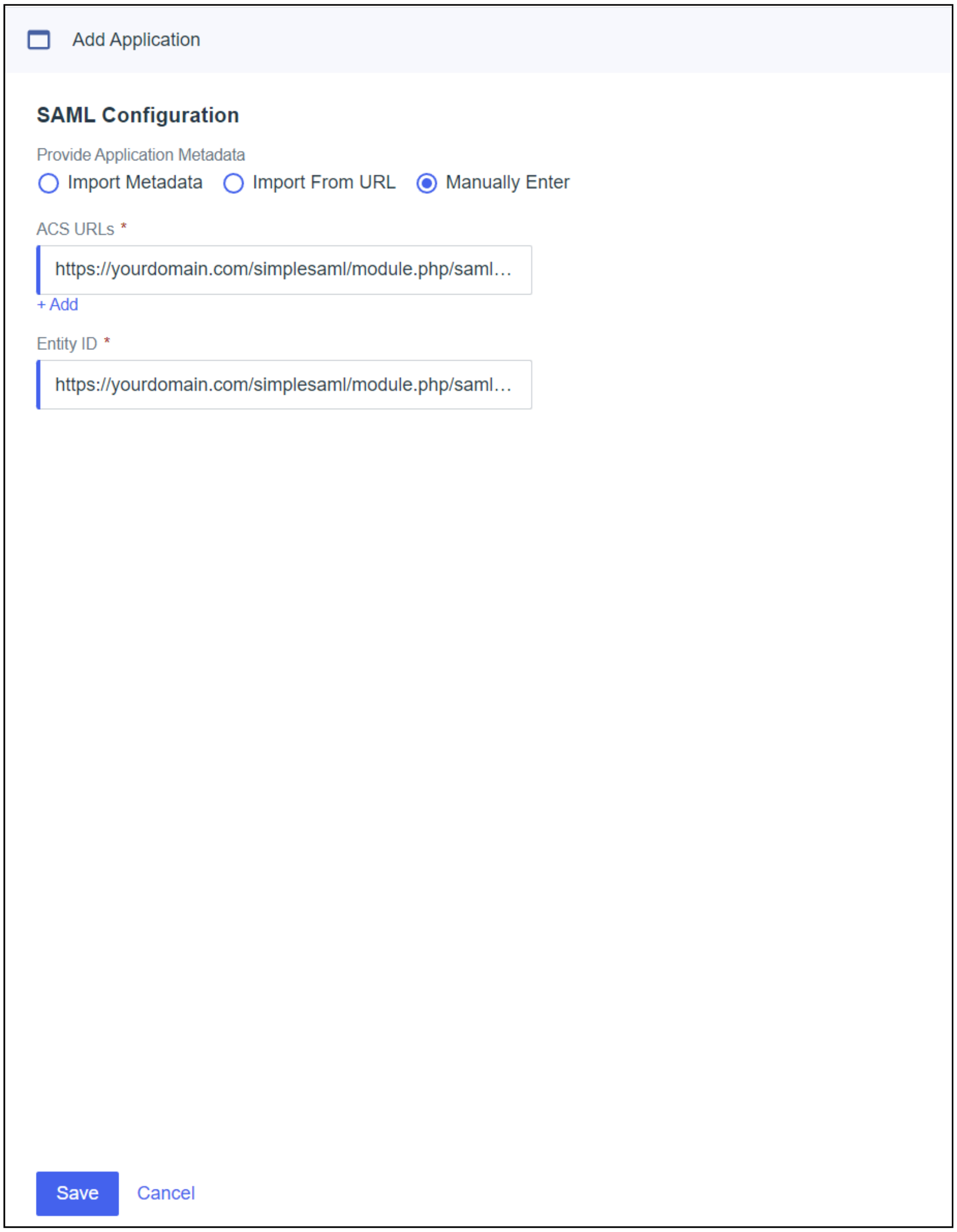
Worker — Applications that can use the PingOne admin API.

Application Catalog — Use a templated integration. Visit the Application Catalog.

The **SAML Configuration** screen appears in the right panel.

5. Select **Manually Enter**, and fill in the fields as follows:
   ACS URLs:
   https://<your_filecloud_url>/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Entity ID:
https://<your_filecloud_url>/simplesaml/module.php/saml/sp/metadata.php/default-sp



Add Application

SAML Configuration

Provide Application Metadata
○ Import Metadata ○ Import From URL ● Manually Enter

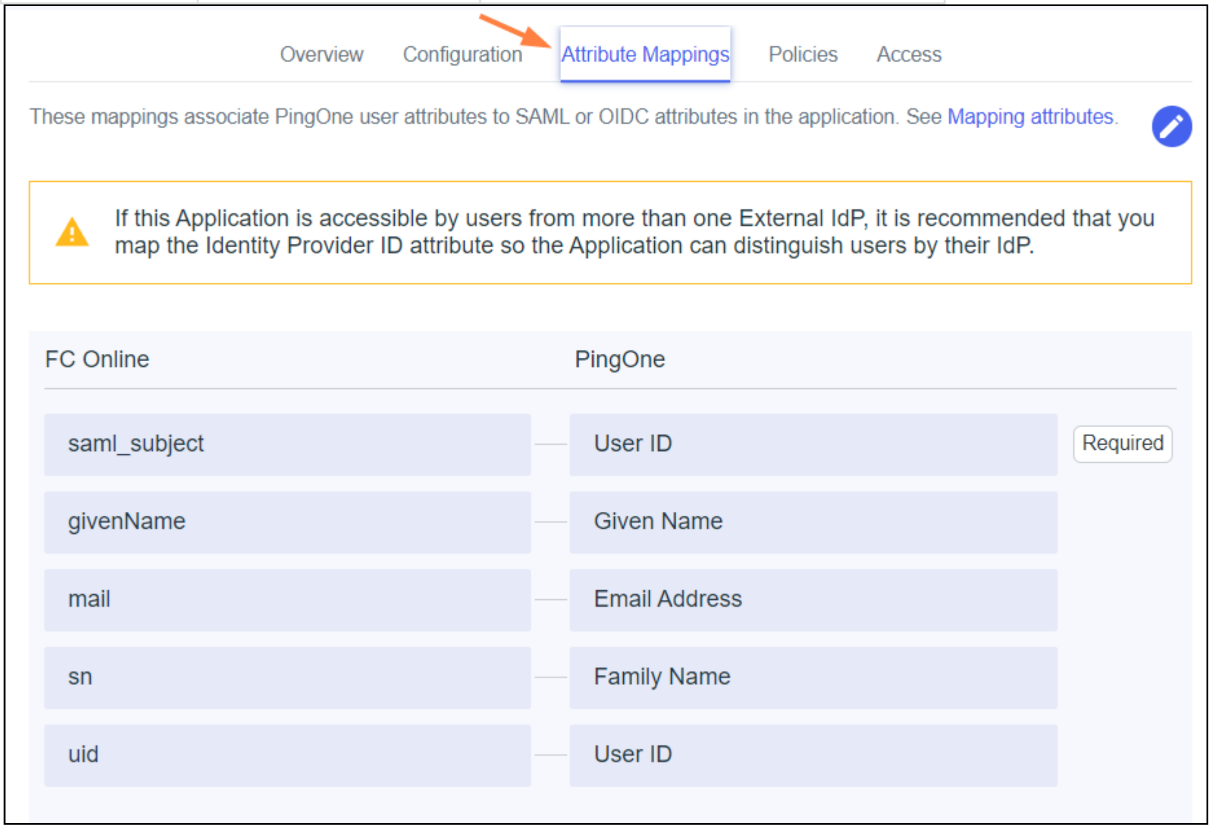
ACS URLs *
https://yourdomain.com/simplesaml/module.php/saml…

Entity ID *
https://yourdomain.com/simplesaml/module.php/saml…

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

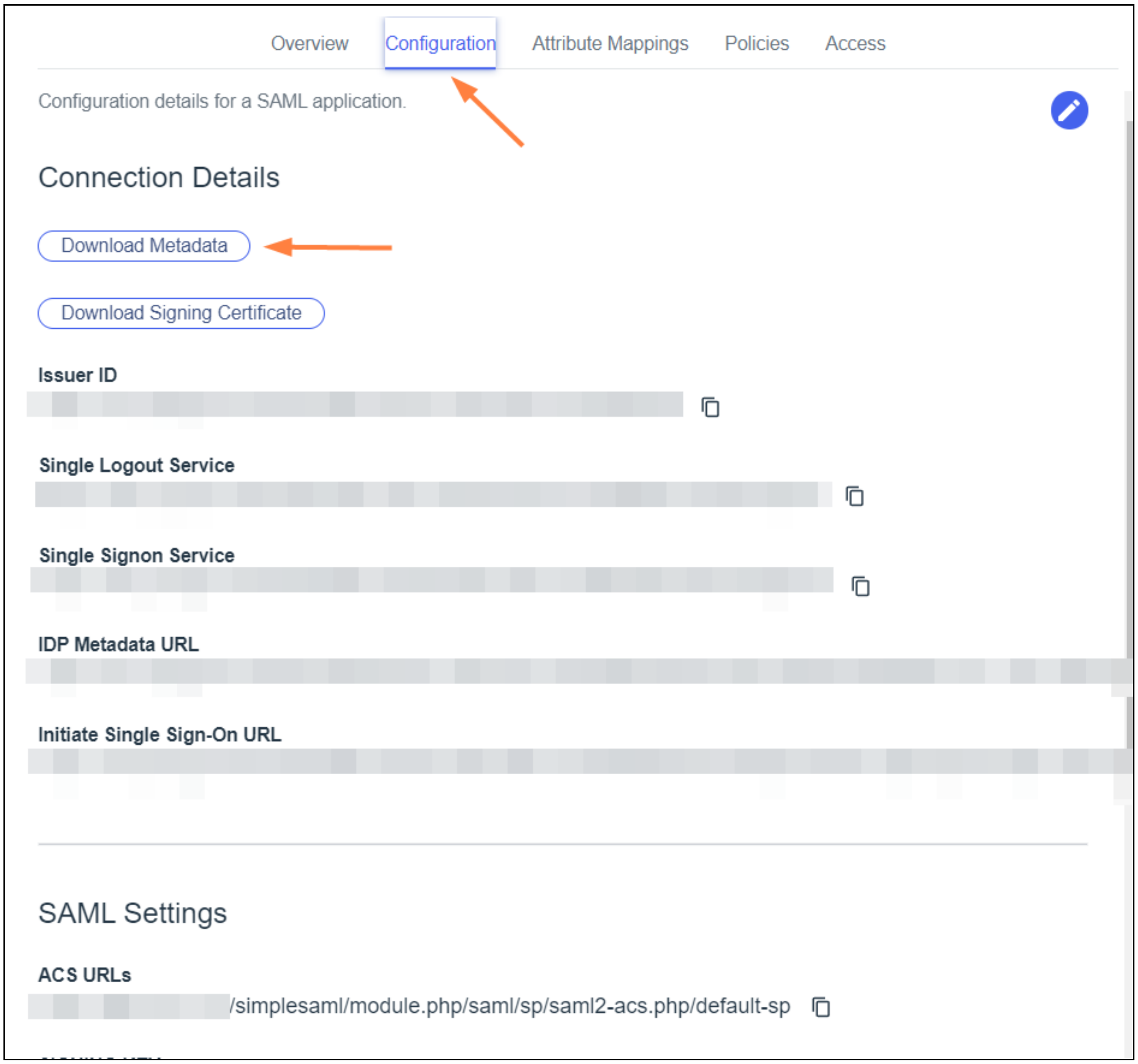


These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

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	

8. Click the **Configuration** tab.
9. To get a copy of the metadata file associated with the configuration, click **Download Metadata**. Save the file so you can enter its contents into the FileCloud admin portal.



Configuration details for a SAML application.

Connection Details

Issuer ID
[redacted]

Single Logout Service
[redacted]

Single Signon Service
[redacted]

IDP Metadata URL
[redacted]

Initiate Single Sign-On URL
[redacted]

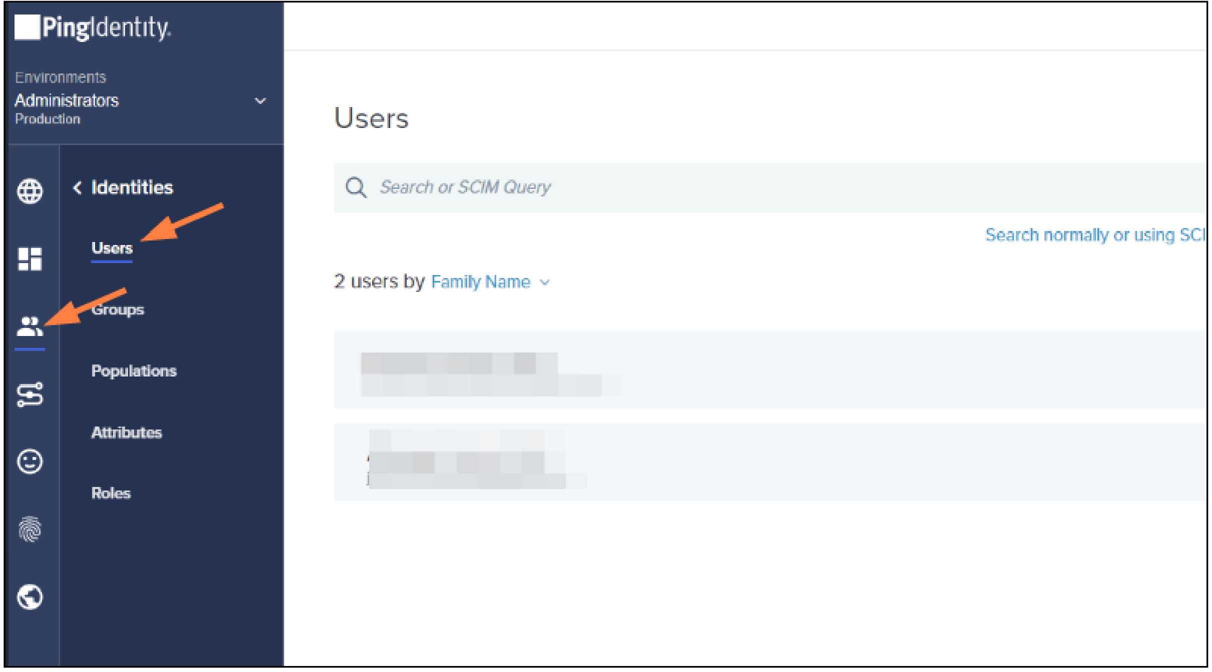
SAML Settings

ACS URLs
[redacted]/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Your application configuration is now complete.

10. Click the Identities icon in the Ping Identity navigation panel.

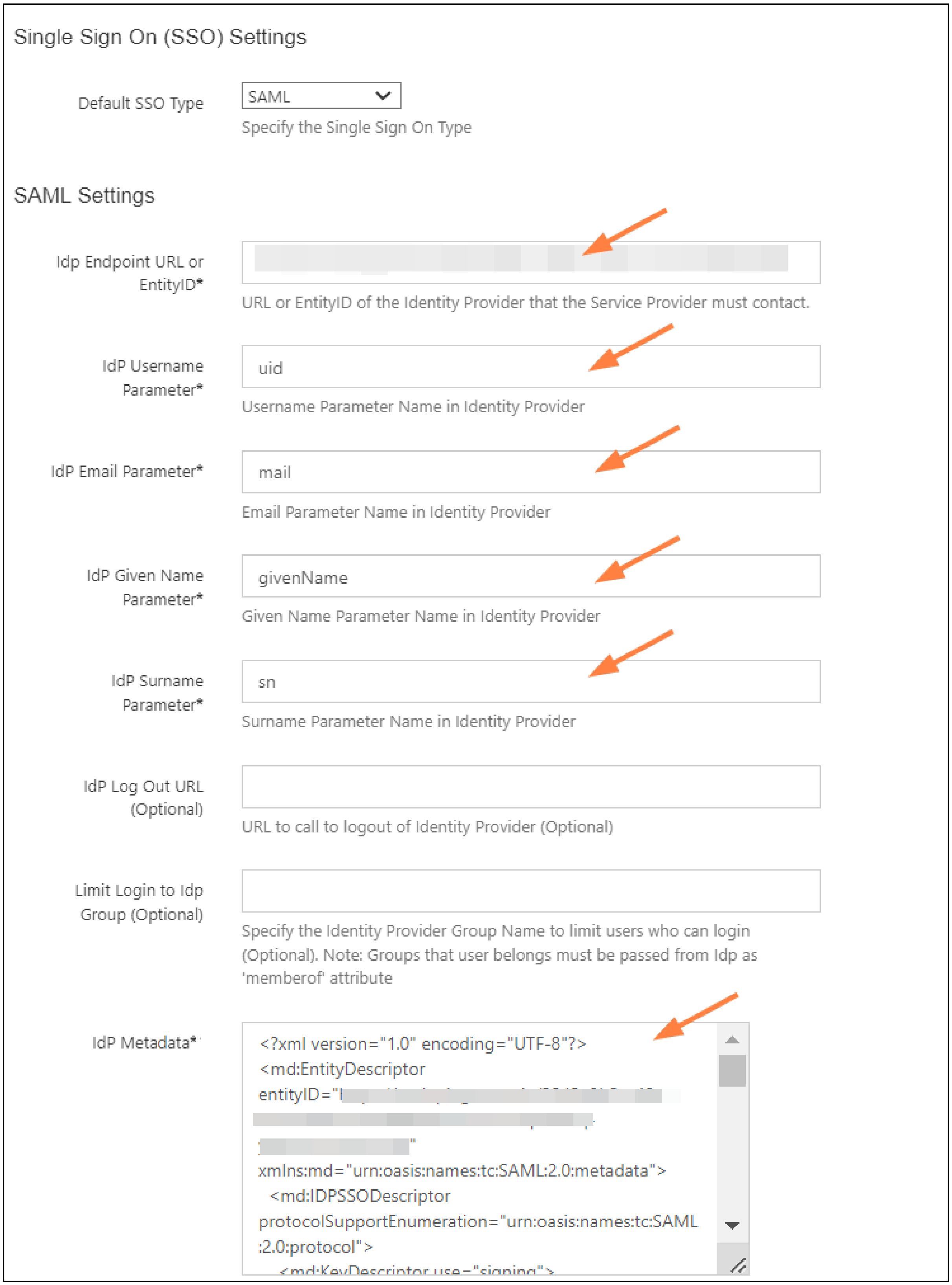
11. Click **Users**, and then add your users.



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: SAML

Specify the Single Sign On Type

SAML Settings

Idp Endpoint URL or EntityID*: [redacted]

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

IdP Username Parameter*: uid

Username Parameter Name in Identity Provider

IdP Email Parameter*: mail

Email Parameter Name in Identity Provider

IdP Given Name Parameter*: givenName

Given Name Parameter Name in Identity Provider

IdP Surname Parameter*: sn

Surname Parameter Name in Identity Provider

IdP Log Out URL (Optional):

URL to call to logout of Identity Provider (Optional)

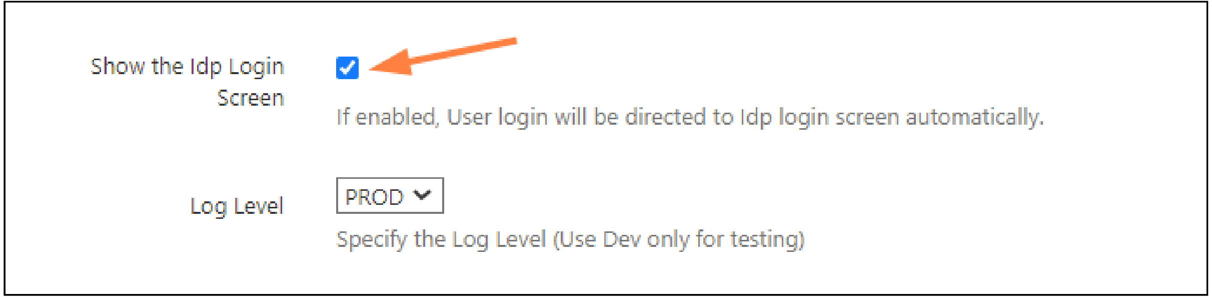
Limit Login to Idp Group (Optional):

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="[redacted]"
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">
```

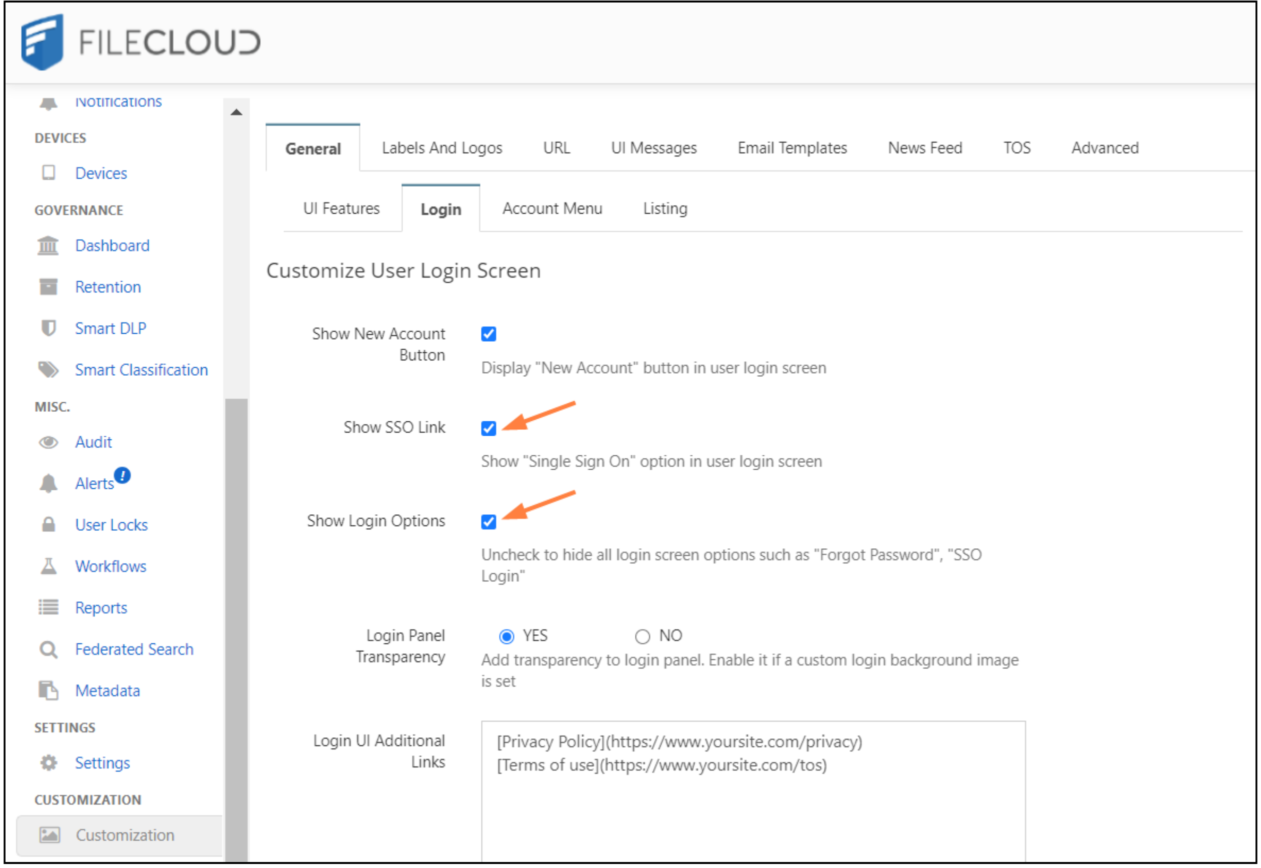
3. If you want users to see the Ping Identity login after they click **Login with SSO**, scroll to the bottom of the screen and check **Show the Idp Login Screen**.
   If you want users to be directly logged into FileCloud after they click **Login with SSO**, do not check **Show the Idp Login Screen**.



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

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

4. Click **Save**.
5. Go to **Customization > General > Login** and check **Show SSO Link** and **Show Login Options**.



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

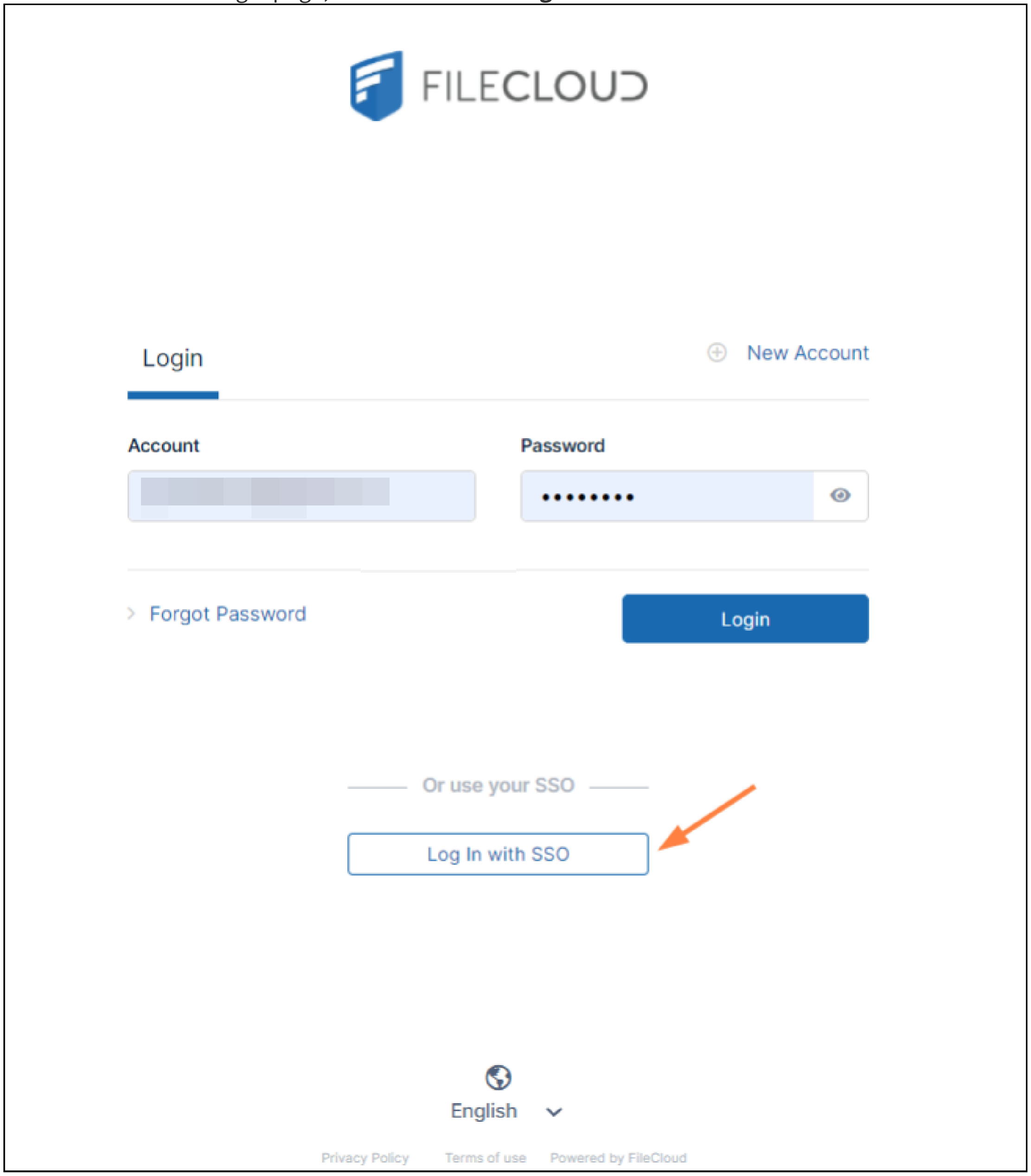
Show Login Options ☑
Uncheck to hide all login screen options such as "Forgot Password", "SSO Login"

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

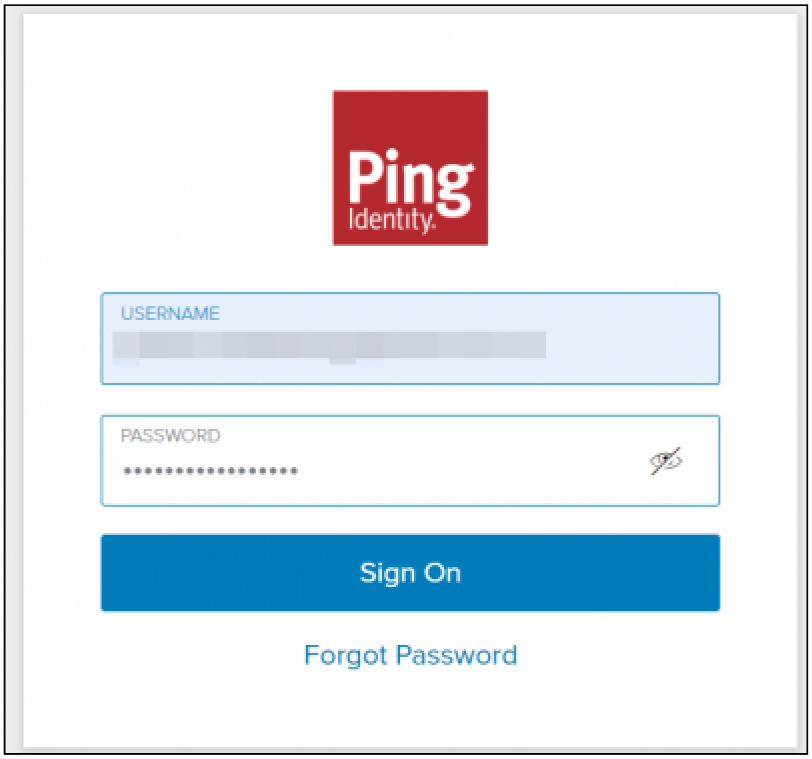
Login UI Additional Links
[Privacy Policy](https://www.yoursite.com/privacy)
[Terms of use](https://www.yoursite.com/tos)

Log in to FileCloud using Single Sign-on with Ping Identity

1. In the Filecloud User login page, the user chooses **Login with SSO**.



If you have checked **Show the Idp Login Screen** in the FileCloud SSO settings, the user is redirected to the Ping Identity login screen, and must click **Sign On**.



Otherwise, the user is directly logged in to FileCloud.

Setting Up and Configuring Certificates when Upgrading SSO

When you upgrade SSO, take the following steps to avoid overwriting your current certificates with the default certificates sent with the library.

For a non-multitenant set up with one Idp:

1. Create a folder named **samlcerts** in WWWROOT/resources/.
2. Copy the **saml.crt** and **saml.pem** files into the **samlcerts** folder.

For a non-multitenant or a multi-tenant set up with different Idp's:

1. Create a folder named **samlcerts** in WWWROOT/resources/ .
2. Create a folder with the same name as the site in WWWROOT/resources/samlcerts/<SITENAME>.
   For the default site, name the folder **default.** For other sites, give the folder the name of the site on the super admin user interface.
3. Calculate the sha1 of idp url using the following command:
   #echo -n "https://adfs.filecloudlabs.com/adfs/services/trust" | openssl sha1
   (stdin)= bea10f29becf8acab8d8d6e8b9b7ee52f35ada8a
4. Use the sha1 value from step 3 to create a new folder in WWWROOT/resources/samlcerts/<SITENAME>.
   For example, for the above case, create the folder: WWWROOT/resources/samlcerts/<SITENAME>/bea10f29becf8acab8d8d6e8b9b7ee52f35ada8a.
5. Place the **saml.pem** and **saml.crt** files into the folder created in step 4.

ADFS Single Sign-On Support

Introduction

FileCloud offers a SAML-based Single Sign-On (SSO) service that provides customers with full control over the authorization and authentication of hosted user accounts.

Using the SAML model, FileCloud acts as the **service provider** and also a **claims-aware application**. FileCloud customers that 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. You can follow the steps here to set up SSL in FileCloud.

FileCloud SSO Configuration Steps

In order to successfully configure SSO, the following steps must be followed.

1. Configure Apache Webserver
2. Set SAML as a 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.

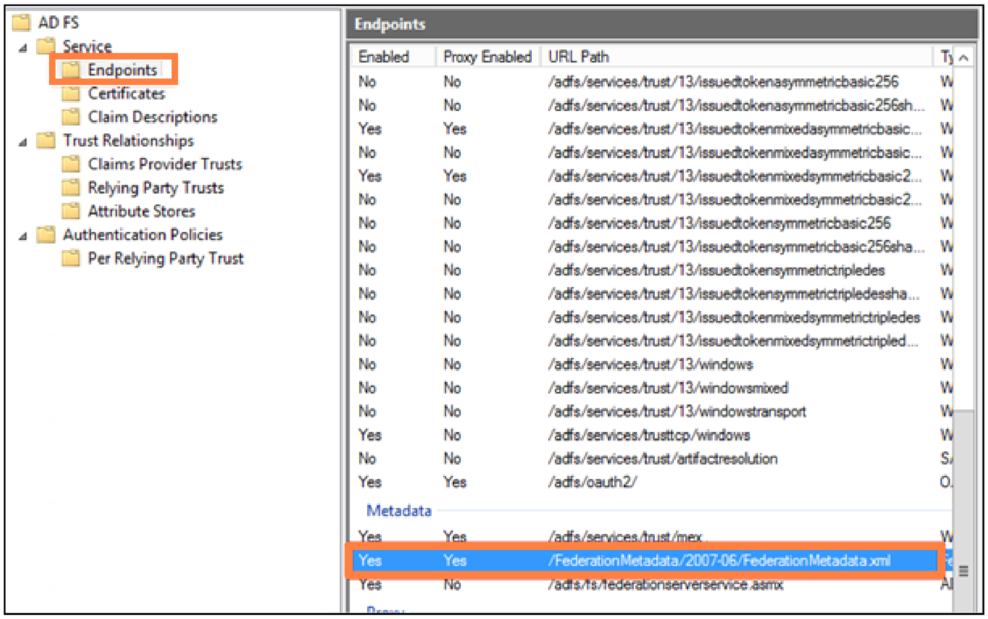
Step 1: Web Server Configuration

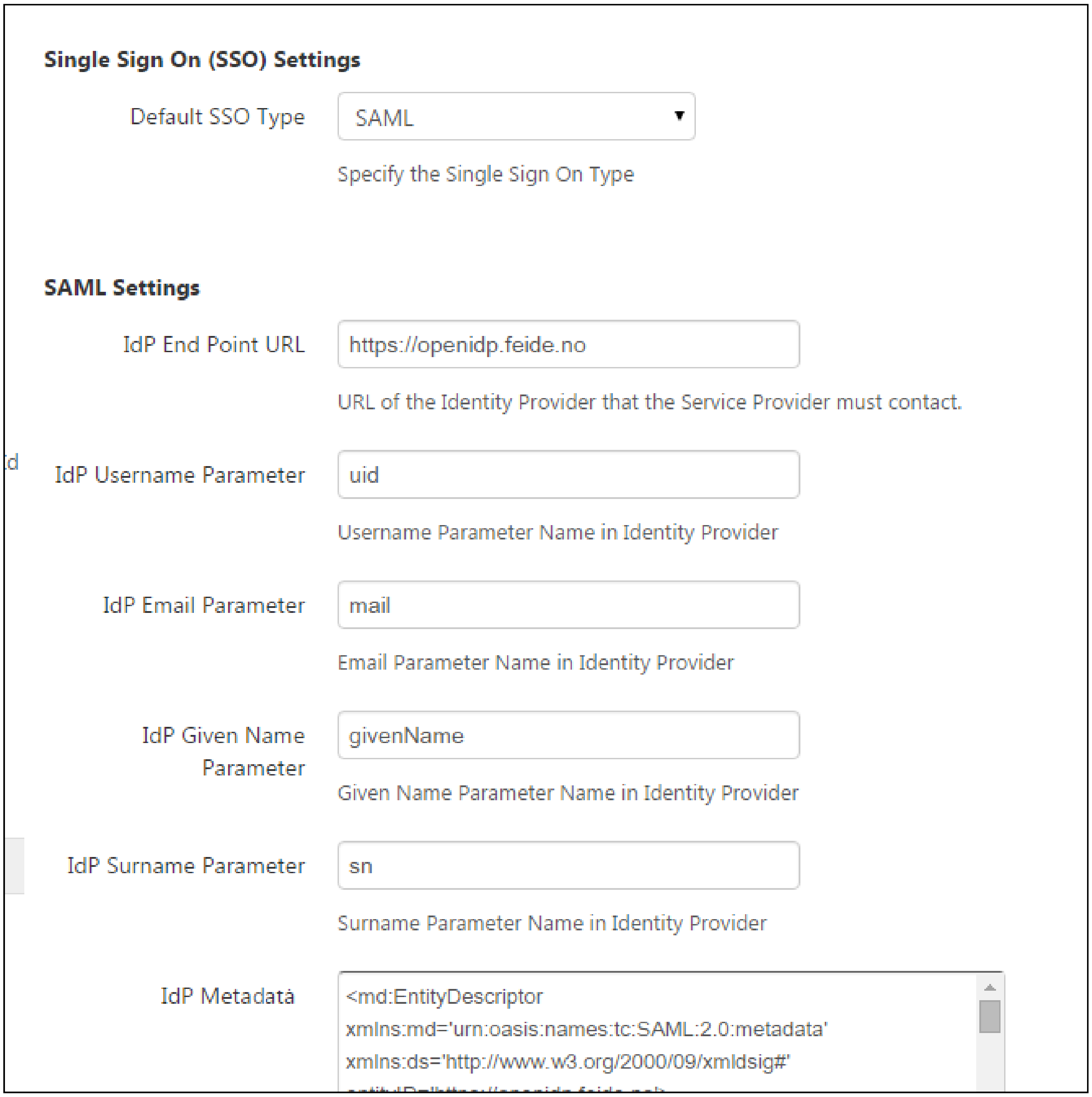
Follow the steps in SAML Single Sign-On Support to set up the Web Server configuration and enable SSO.

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
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

FileCloud Parameters	ADFS as IdP Data can be obtained from Federation Metadata
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  AD FS Service Endpoints Certificates Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies Per Relying Party Trust Endpoints Enabled / Proxy Enabled / URL Path / Ty 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/issuedtokensymmetrictripledes / W No / No / /adfs/services/trust/13/issuedtokensymmetrictripledessha... / W No / No / /adfs/services/trust/13/issuedtokenmixedsymmetrictripledes / W No / No / /adfs/services/trust/13/issuedtokenmixedsymmetrictripled... / 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 / F Yes / No / /adfs/ls/federationserverservice.asmx / A
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: SAML

Specify the Single Sign On Type

SAML Settings

IdP End Point URL: https://openidp.feide.no

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

IdP Username Parameter: uid

Username Parameter Name in Identity Provider

IdP Email Parameter: mail

Email Parameter Name in Identity Provider

IdP Given Name Parameter: givenName

Given Name Parameter Name in Identity Provider

IdP Surname Parameter: sn

Surname Parameter Name in Identity Provider

IdP Metadata:

```
<md:EntityDescriptor
xmlns:md='urn:oasis:names:tc:SAML:2.0:metadata'
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'
```

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.

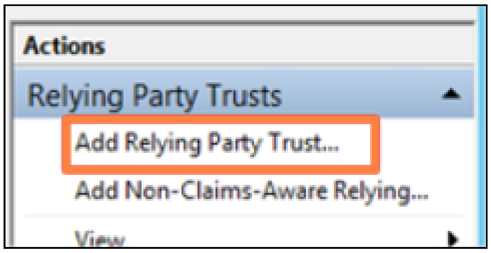
Step 4: Register FileCloud as SP in IdP/ADFS

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.

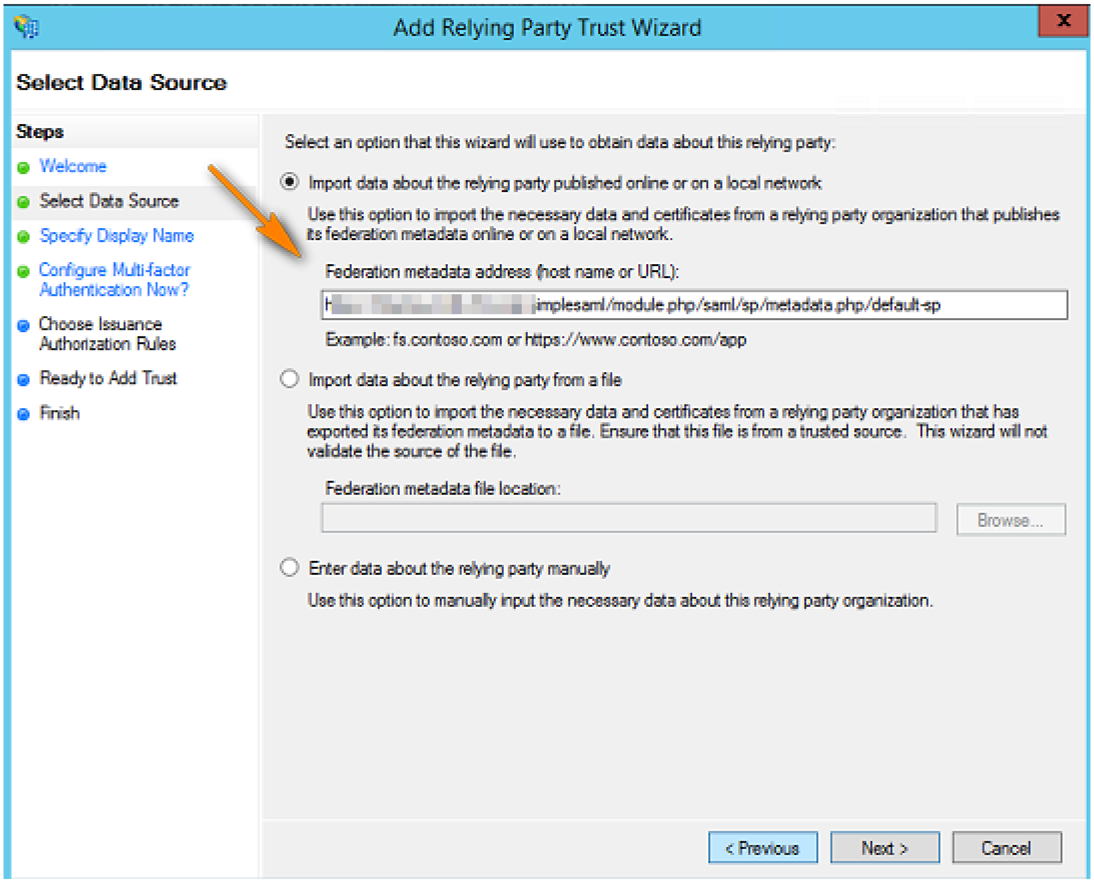
Before you proceed, you must be able to download the metadata of FileCloud from the following Entity ID URL. (Note HTTPS).

> 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 Truest 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.


Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Browse...
< Previous
Next >
Cancel

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

● Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

H[redacted]implesaml/module.php/saml/sp/metadata.php/default-sp

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

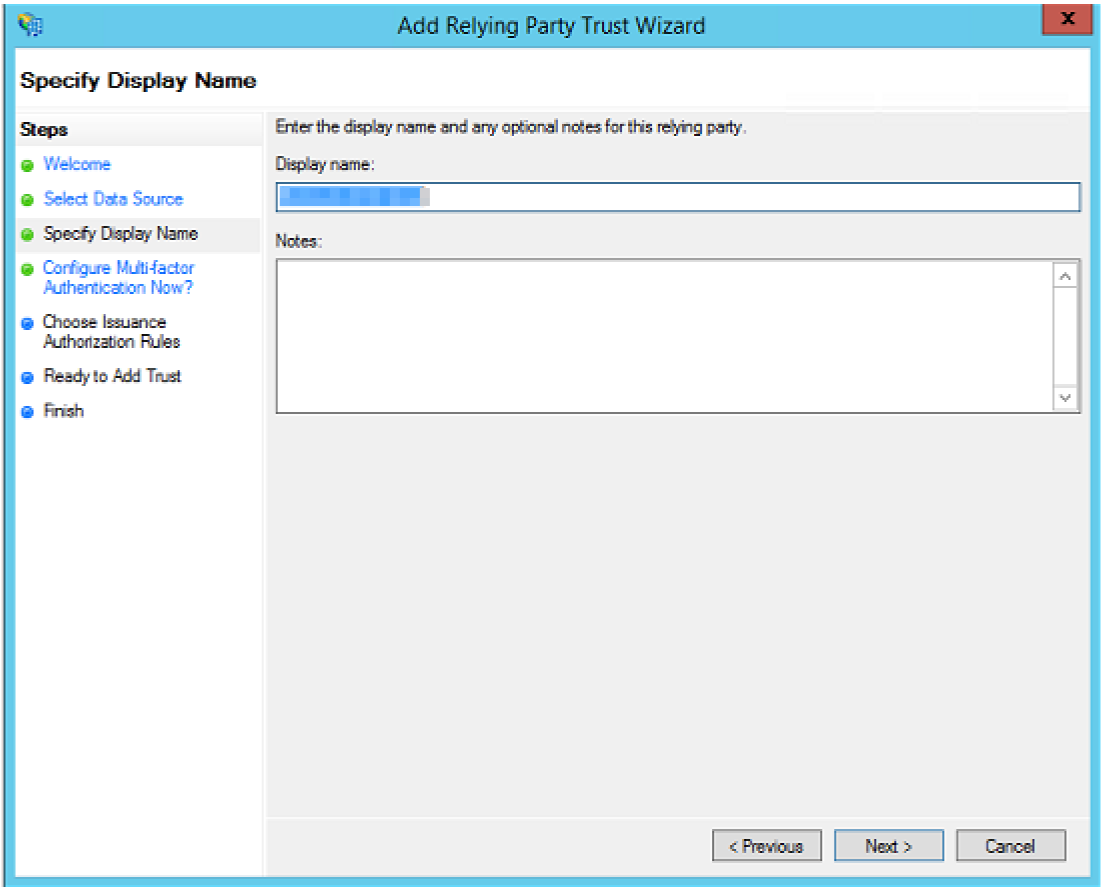
Use this option to manually input the necessary data about this relying party organization.

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"

> ⓘ 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.



Add Relying Party Trust Wizard

Specify Display Name

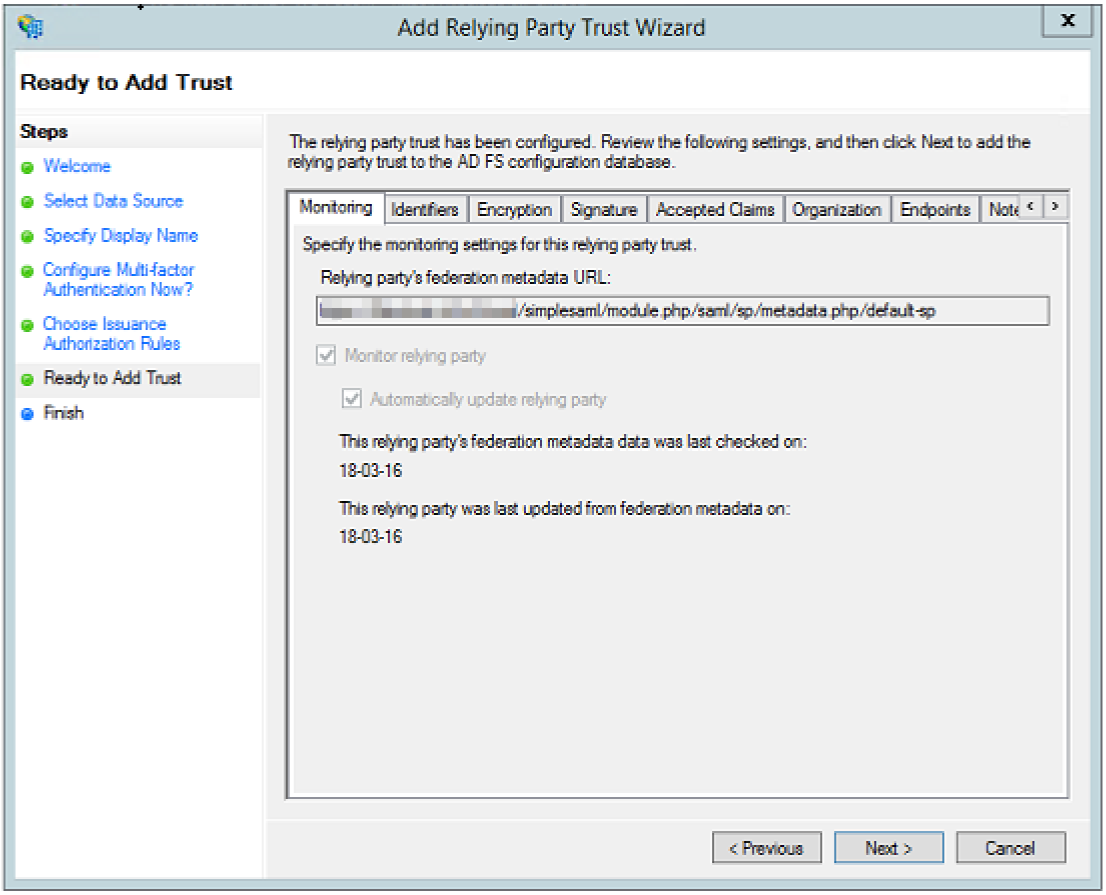
Steps
- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

Display name: [redacted]

Notes:

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.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

[redacted]/simplesaml/module.php/saml/sp/metadata.php/default-sp

☑ Monitor relying party

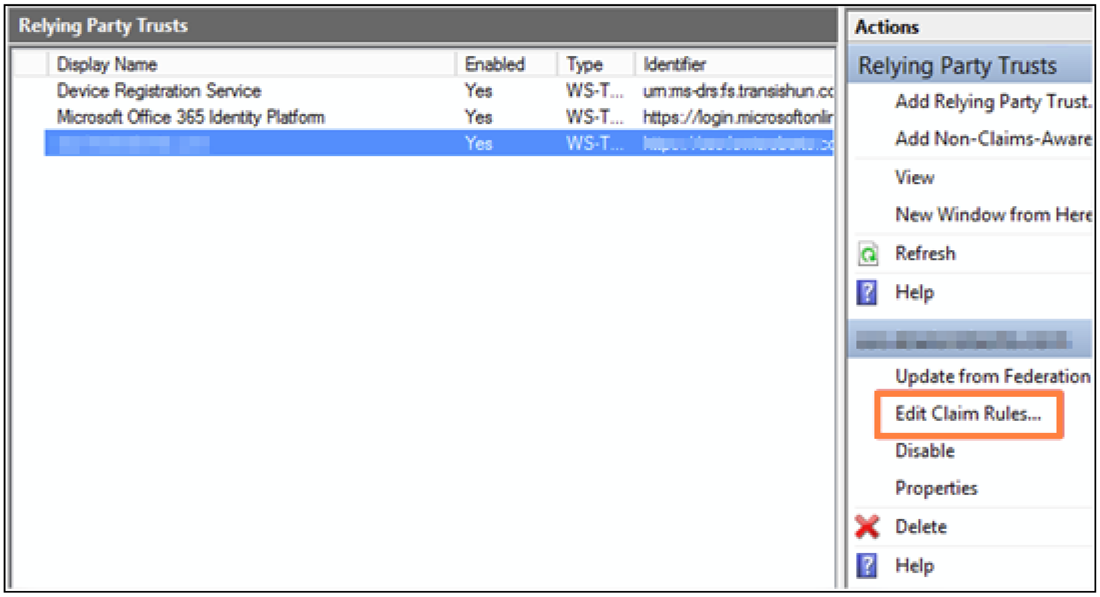
☑ Automatically update relying party

This relying party's federation metadata data was last checked on:
18-03-16

This relying party was last updated from federation metadata on:
18-03-16

6. Click Next and the new Relying Party Trust is now added.

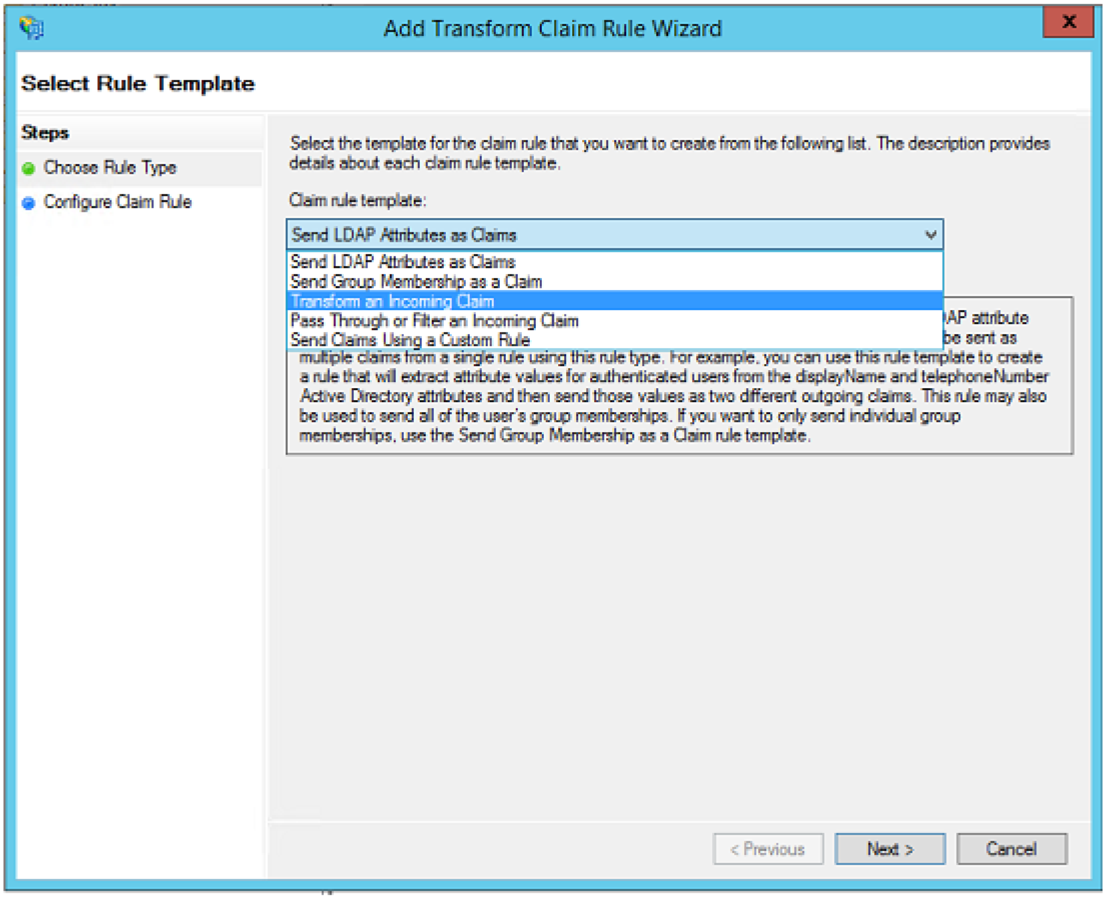
7. Select the Relying Party Trust we have just added and then click **Edit Claim Rules**.



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:fs.transishun.cc
Microsoft Office 365 Identity Platform	Yes	WS-T...	https://login.microsoftonlir
[redacted]	Yes	WS-T...	[redacted]

8. Add an **Issuance Transform Rule**. Choose the **Transform an Incoming Claim rule** Template.



Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

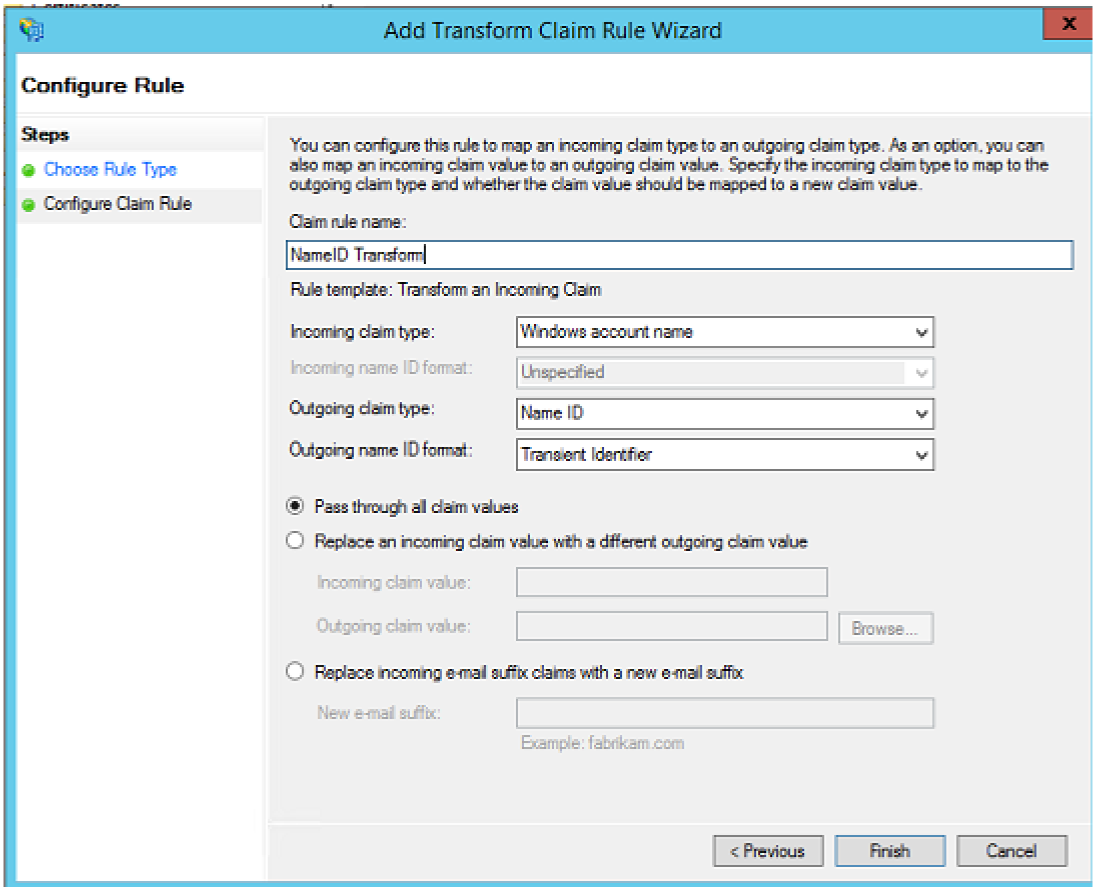
Claim rule template:

Send LDAP Attributes as Claims

Send LDAP Attributes as Claims
Send Group Membership as a Claim
Transform an Incoming Claim
Pass Through or Filter an Incoming Claim
Send Claims Using a Custom Rule

AP attribute be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a 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

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: NameID Transform

Rule template: Transform an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Transient Identifier

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

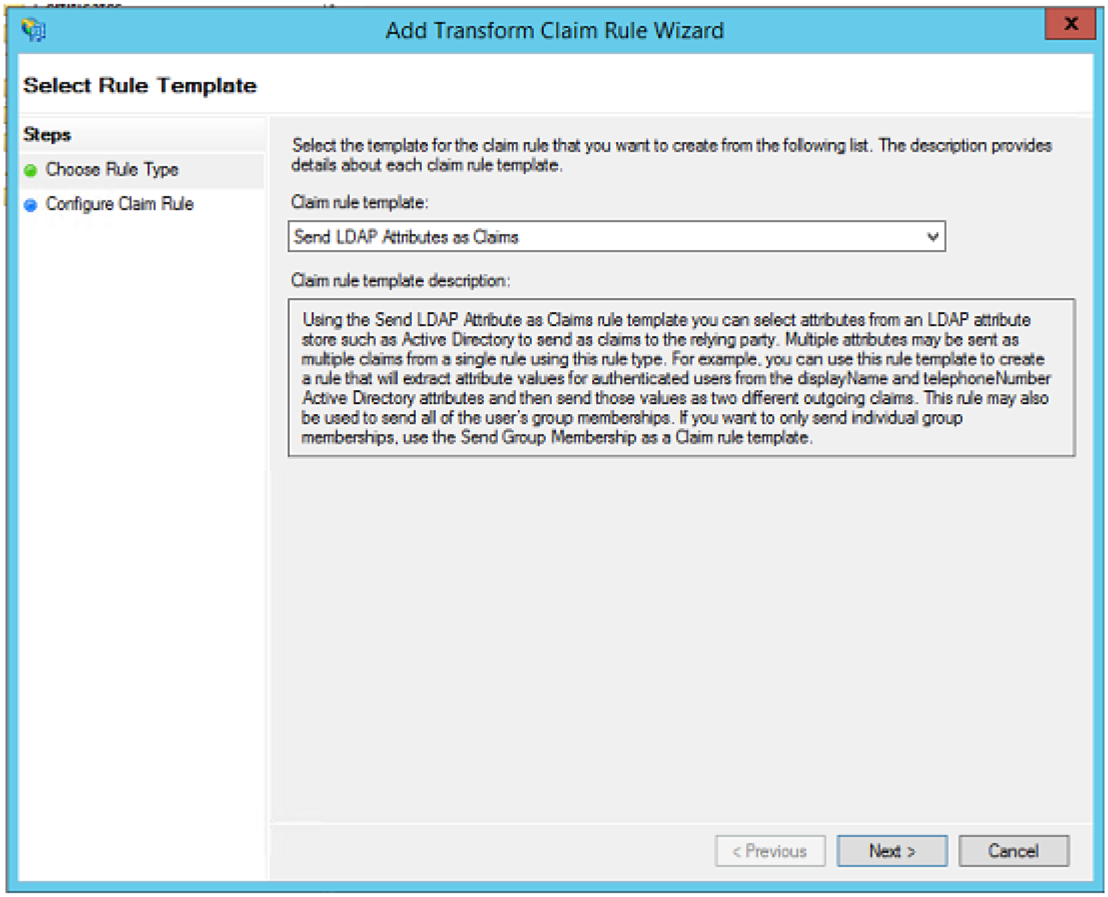
Outgoing claim value:

○ 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.



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

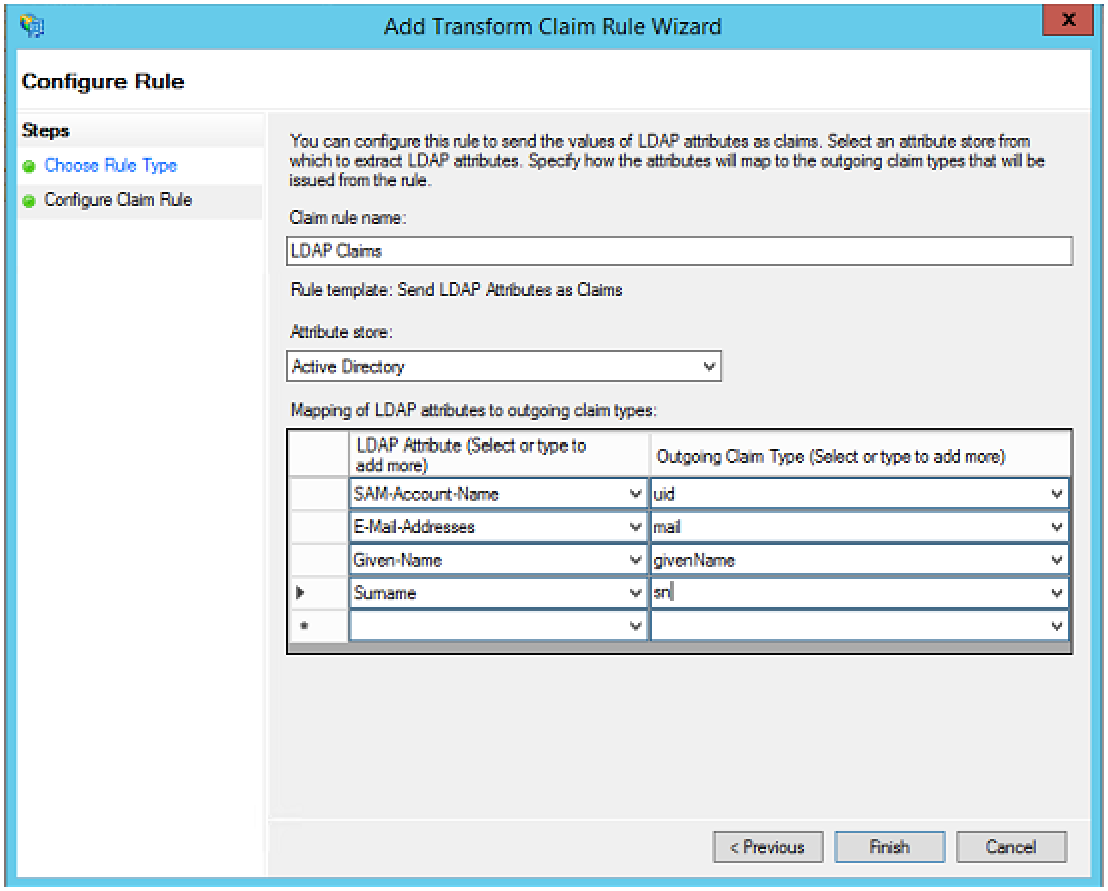
Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule 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

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

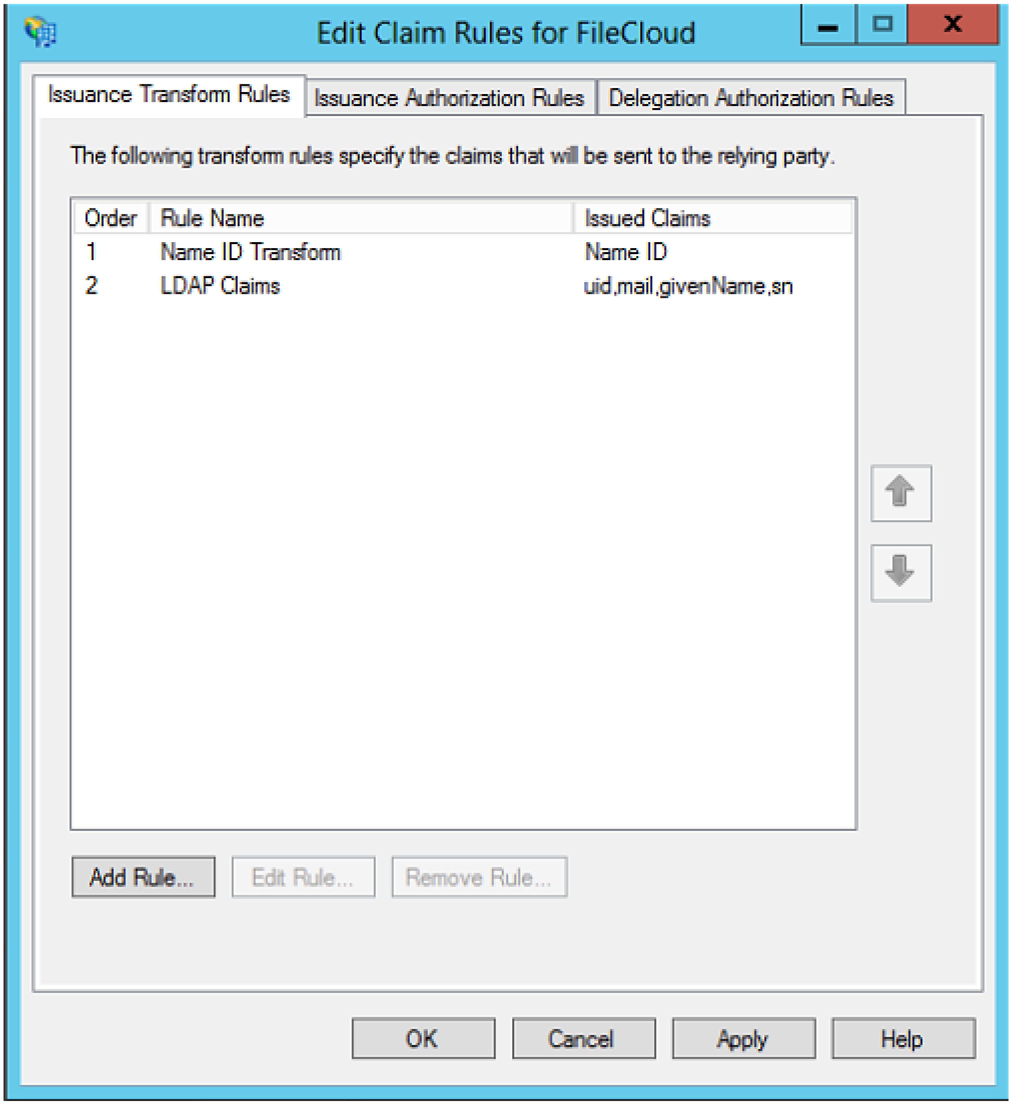
Rule template: Send LDAP Attributes as Claims

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
*		

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.


Edit Claim Rules for FileCloud
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Name ID Transform	Name ID
2	LDAP Claims	uid,mail,givenName,sn

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.

Troubleshooting

Please check the troubleshooting section from SAML Single Sign-On Support (under SSO Configuration Steps, Step 8) .

NTLM Single Sign-On Support

FileCloud supports NTLM for User Login through SSO.

Prerequisites

For NTLM SSO to work, the FileCloud Server must be connected to the AD domain.

Web Server Settings

1. Ensure the file "mod_authn_ntlm.so" exists in the c:\xampp\apache\modules folder
2. Edit the Webserver configuration file at c:\xampp\apache\conf\httpd.conf and add the following section.

```
<Location /auth >
  #AllowOverride None
  AuthName "Private location"
  AuthType SSPI
  NTLMAuth On
  NTLMAuthoritative On
  <RequireAll>
    <RequireAny>
      Require valid-user
      #require sspi-user EMEA\group_name
    </RequireAny>
    <RequireNone>
      Require user "ANONYMOUS LOGON"
      Require user "NT-AUTORITÄT\ANONYMOUS-ANMELDUNG"
    </RequireNone>
  </RequireAll>
  # use this to add the authenticated username to you header
  # so any backend system can fetch the current user
  # rewrite_module needs to be loaded then
  RewriteEngine On
  RewriteCond %{LA-U:REMOTE_USER} (.+)
  RewriteRule . - [E=RU:%1]
  RequestHeader set X_ISRW_PROXY_AUTH_USER %{RU}e
 </Location>
```

3. Ensure the module is loaded by ensuring the following line is enabled and not disabled.

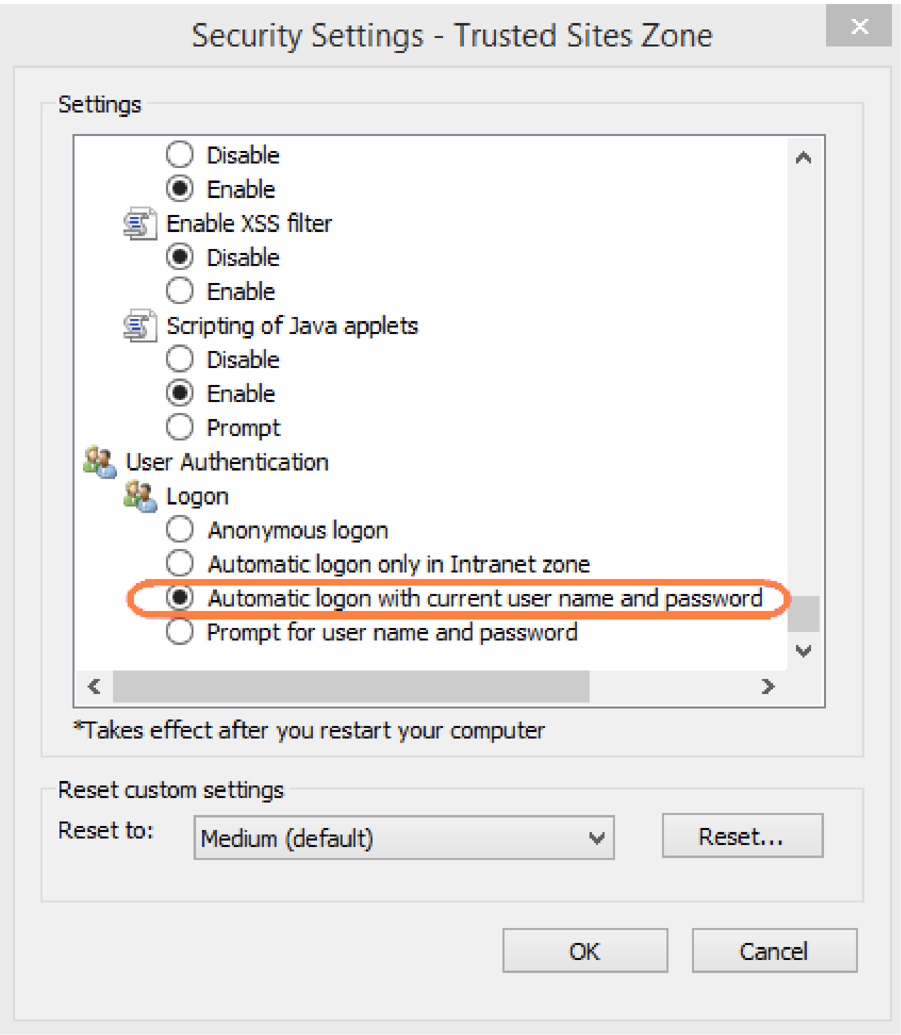
```
LoadModule auth_ntlm_module modules/mod_authn_ntlm.so
```

4. Ensure you have the "auth" folder available at WWWROOT
5. Restart Webserver
6. In your browser open http://<HOSTNAME>/auth URL, it will automatically login if everything works correctly. Make sure in your browser SSO has been enabled for the site.

Browser Settings to Enable Domain User SSO Login

For Internet Explorer and Google Chrome

1. Add the site URL to trusted site
2. In the settings for trusted sites, enable User login to be sent, see screenshot below



Security Settings - Trusted Sites Zone

Settings

○ Disable
● Enable
Enable XSS filter
● Disable
○ Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
○ Automatic logon only in Intranet zone
● Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium (default)

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

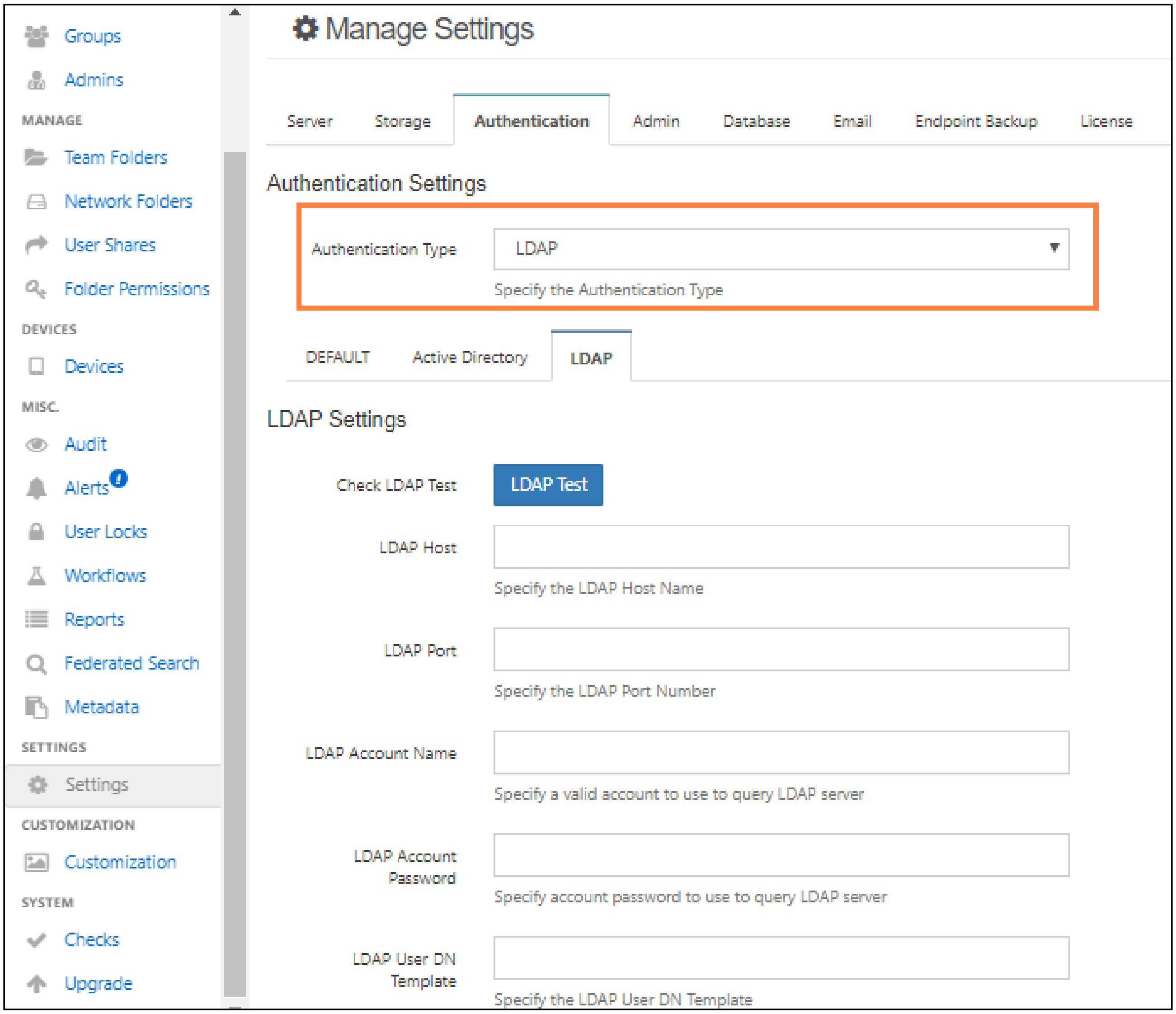
Enable LDAP Authentication

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 ...



Manage Settings

Authentication Settings

Authentication Type: LDAP
Specify the Authentication Type

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

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`

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

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

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

User DN Template:

uid=^NAME^,ou=someou,dc=company,dc=com

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

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

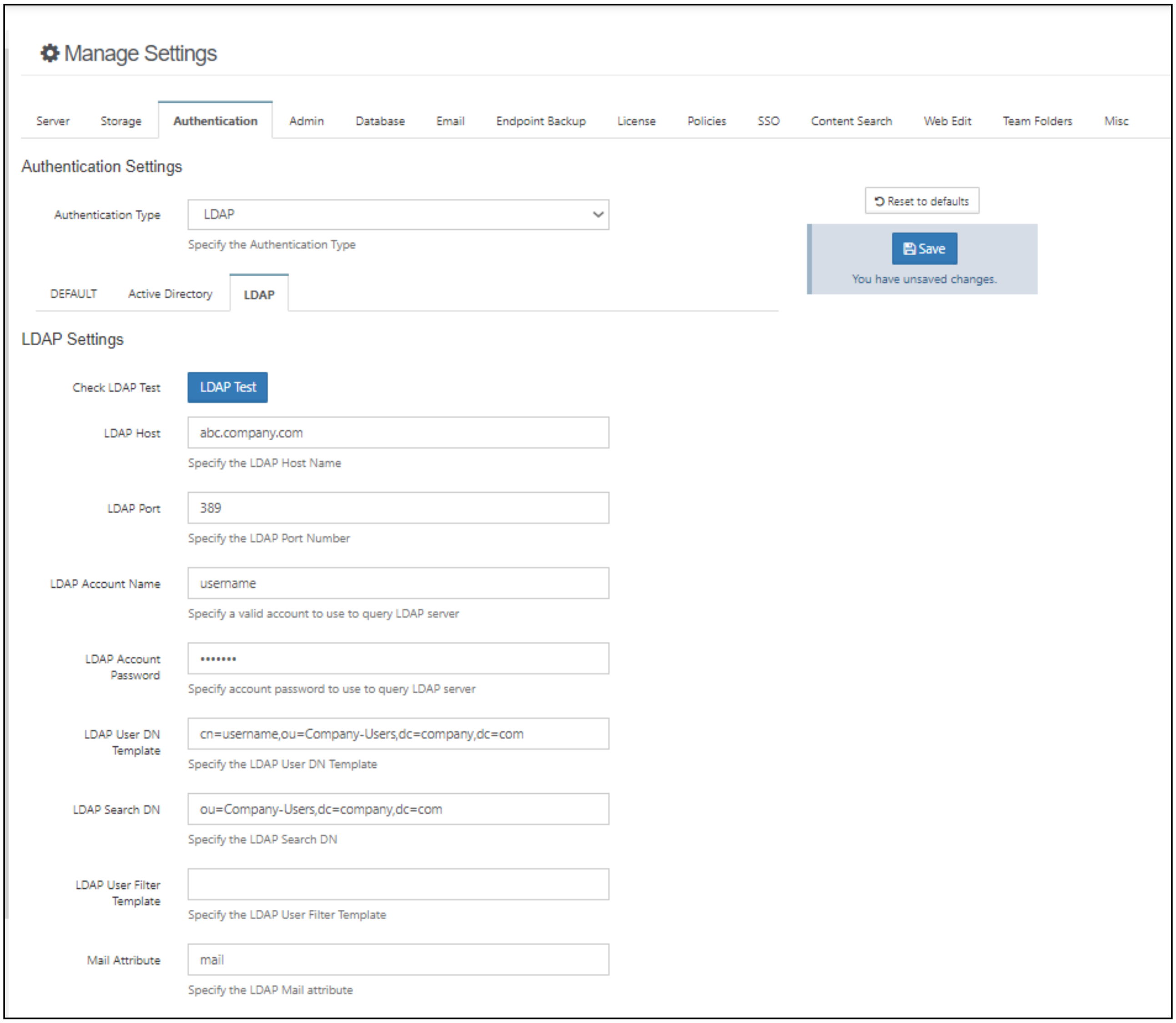
NOTE: For using with JumpCloud, please use the following strings

User DN Template:
uid=^NAME^,ou=Users,o=xxxxxxxxxxxxxxxxxb42f7988db,dc=jumpcloud,dc=com

LDAP Search DN

ou=users,o=**xxxxxxxxxxxxxxxxxb42f7988db,**dc=jumpcloud,dc=com

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



Authentication Settings

Authentication Type: LDAP
Specify the Authentication Type

LDAP Settings

Check 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

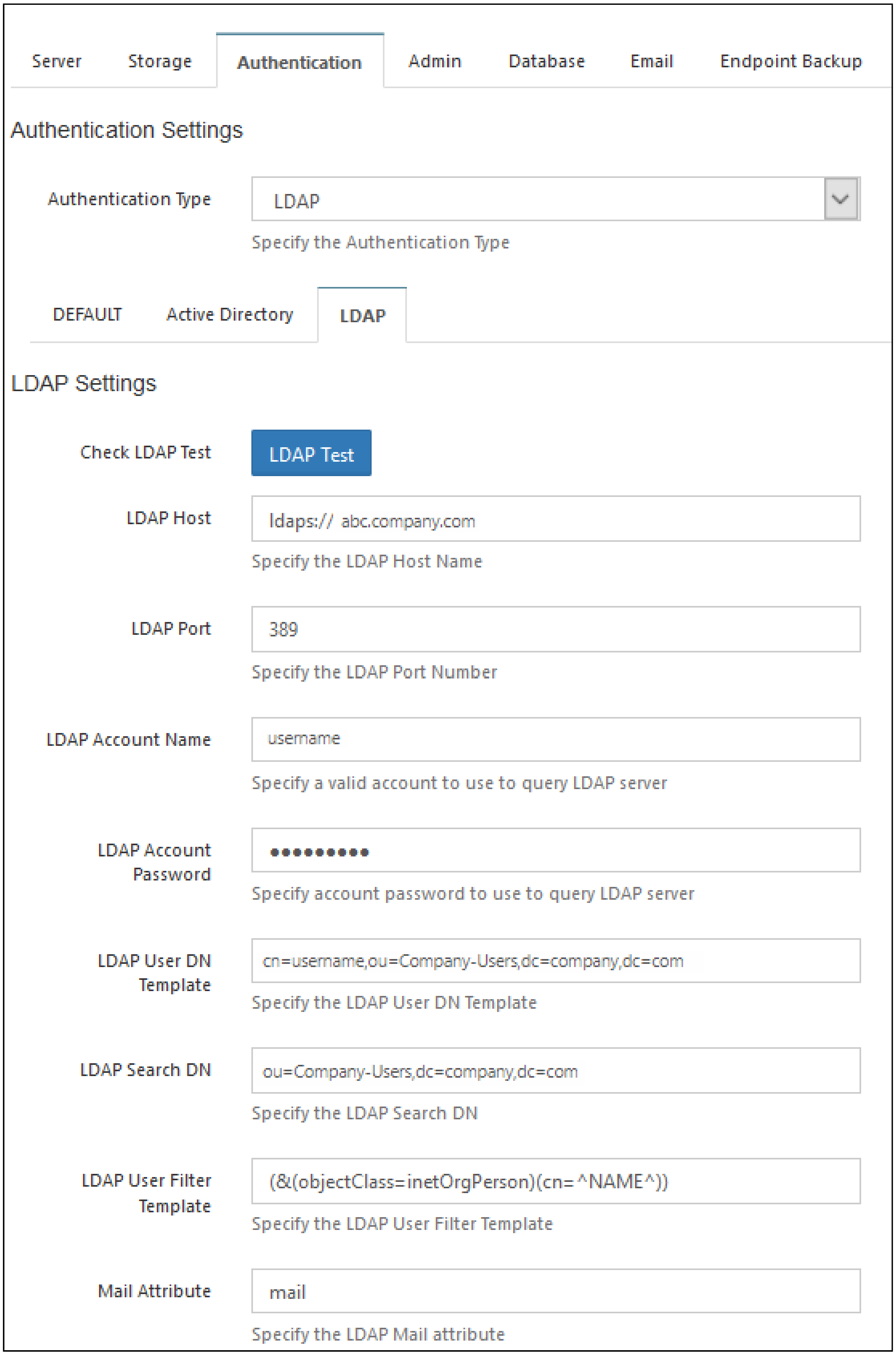
Use LDAP with TLS

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	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory. This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify a user. `Use the token ^NAME^ in place of user name` Example : cn=^NAME^,ou=someorg,dc=company,dc=com To use multiple OUs, set this equal to ^USE_USER_FULL_DN^	cn=<username>,ou=*<abc>*,dc=*<company>*,dc=com Multiple OU mode: ^USE_USER_FULL_DN^
LDAP Search DN	REQUIRED	The search DN (Specifies the set of resources to search for an user). If there is an *ou* encompassing all users, then the search DN would be pointing to that DN. For example, if all users are under the *employees* ou, then the search DN would be *ou=employees,dc=company,dc=com*	*ou=company-users,dc=company,dc=com*
LDAP User Filter Template	REQUIRED	**T**he filter to be used to identify a user entry record from results. For example, if the object class is inetOrgPerson, then you would use: `(&(objectClass=inetOrgPerson)(cn=^NAME^))`	(&(objectClass=*inetOrgPerson*)(cn=*^NAME^*))

SETTING	**REQUIRED ?**	**DESCRIPTION**	**TLS Example**
Mail Attribute	REQUIRED	In the FileCloud environment, every user requires an email ID. Specify the attribute name used in the LDAP's user record to refer to the email ID.	*username_email_ID*



Authentication Settings

Authentication Type: LDAP

Specify the Authentication Type

LDAP Settings

Check LDAP Test: LDAP Test

LDAP Host: ldaps:// 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: (&(objectClass=inetOrgPerson)(cn=^NAME^))

Specify the LDAP User Filter Template

Mail Attribute: mail

Specify the LDAP Mail attribute

➡ Authenticate to Multiple LDAP Servers

Authenticate to Multiple LDAP servers

ⓘ The ability for a single installation of FileCloud to authenticate against multiple LDAP servers is available in FileCloud Server version 18.2 and later.

You can use an LDAP directory server as a general-purpose data store in a wide variety of applications.

- As a directory server (more technically referred to as a Directory Server Agent, a Directory System Agent, or a DSA) LDAP is a type of network database that stores information represented as trees of entries
- An LDAP server database is different from a relational database, which uses tables comprised of rows and columns
- LDAP is designed to provide extremely fast read/query performance for a large scale of dataset
- Typically you want to store only a small piece of information for each entry
- The add/delete/update performance for LDAP is relatively slower compared with read/query because the assumption is that you don't want to update the data too often

Isn't LDAP a Protocol?

Strictly speaking, LDAP is a protocol - the Lightweight Directory Access Protocol. It is not a database or even a directory.

- LDAP, the Lightweight Directory Access Protocol, is a well-supported standards-based mechanism for interacting with directory servers
- It's often used for authentication and storing information about users, groups, and applications
- As a global directory service, LDAP was expected to hold hundreds of millions of entries and be managed by thousands of different organizations
- LDAP stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form
- An LDAP server is effectively a service model based on many cooperating servers known as DSAs (Directory System Agents)
- Queries are expected to outnumber updates by a very large factor

➡ For more information on using an LDAP infrastructure, on the LDAP Web site, Learn about LDAP.

Enable multiple LDAP server authentication

To enable multiple LDAP server authentication, you have to configure settings in the following places:

- ldapconfig.php file
- Admin Dashboard

To enable multiple AD server authentication:

1. Open a browser and log in to the *Admin Portal*.
2. On the *Admin Dashboard*, from the left navigation panel, click *Settings*.
3. On the *Manage Settings* screen, click *Authentication*.
4. To enable the LDAP Settings, under *Authentication Settings*, change the Authentication Type to *LDAP*.
5. Select the *LDAP* sub-tab, type in the required information, and then click *Save*.
6. Create a file called **ldapconfig.php** in one of the following locations, depending on your OS:

```
Windows Location
c:\xampp\htdocs\config\ldapconfig.php


Linux Location
/var/www/htdocs/config/ldapconfig.php
```

7. Add the information for the other LDAP servers using the following example. ⚠️ Do not add the same LDAP server detail that was already configured in Admin Dashboard.

```
<?php
/*
* Copyright(c) 2014 CodeLathe LLC. All rights Reserved.
* This file is part of FileCloud  http://www.filecloud.com
*/

// ... Multi-AD Server Support, set to 1 to enable additional AD servers
define("TONIDOCLOUD_MULTI_LDAP_ENABLE", 1);
//=============== SITE 1 ==============================
define("TONIDOCLOUD_LDAP_HOST_1", "ldap.mycompany.com" ); // < LDAP Server Host
define("TONIDOCLOUD_LDAP_PORT_1", 389 ); // < LDAP Server port
define("TONIDOCLOUD_LDAP_ACCOUNTNAME_1", "cn=admin,dc=mycompany,dc=com"); // < Account name for Admin Operations
define("TONIDOCLOUD_LDAP_ACCOUNTPASSWORD_1", "3lkjASdf9802"); // < Account Password for Admin Operations
define("TONIDOCLOUD_LDAP_USERDNTEMPLATE_1", "cn=^NAME^,ou=MyCompnay-Support,dc=mycompany,dc=com"); // < USer DN template
define("TONIDOCLOUD_LDAP_SEARCHDN_1", "ou=MyCompany-Support,dc=mycompany,dc=com"); // < USer DN template
define("TONIDOCLOUD_LDAP_USERFILTERTEMPLATE_1", "(&(objectClass=inetOrgPerson)(cn=^NAME^))"); // < USer DN template
define("TONIDOCLOUD_LDAP_MAILATTRIBUTE_1", "mail"); // < Mail Attribute

?>
```

Now additional users from these domains can also login into FileCloud.

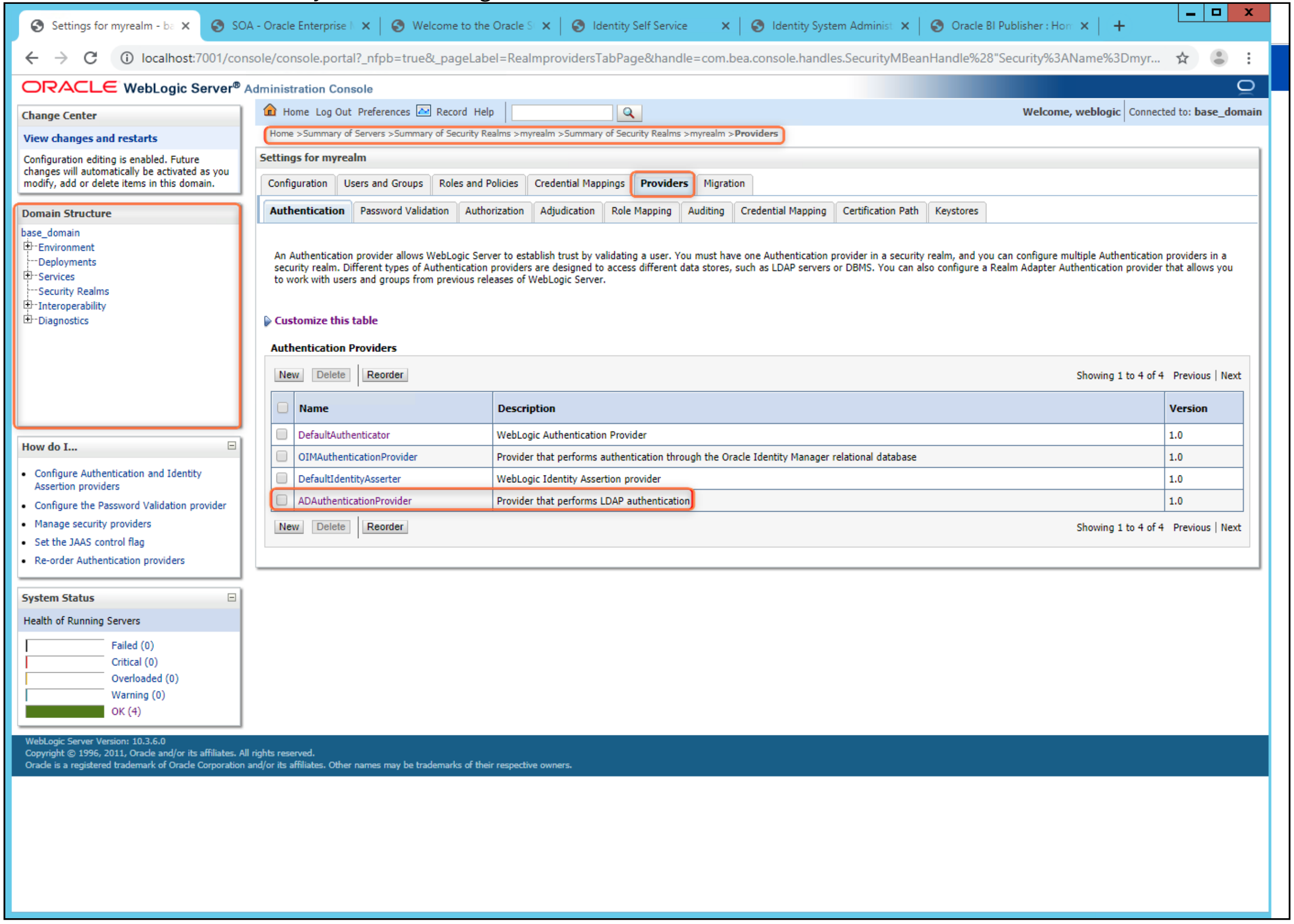
Oracle Identity Manager LDAP integration with FileCloud

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.


Settings for myrealm - ba
SOA - Oracle Enterprise
Welcome to the Oracle S
Identity Self Service
Identity System Administ
Oracle BI Publisher : Hon
localhost:7001/console/console.portal?_nfpb=true&_pageLabel=RealmprovidersTabPage&handle=com.bea.console.handles.SecurityMBeanHandle%28"Security%3AName%3Dmyr...
ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: base_domain
Home >Summary of Servers >Summary of Security Realms >myrealm >Summary of Security Realms >myrealm >Providers
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure Authentication and Identity Assertion providers
Configure the Password Validation provider
Manage security providers
Set the JAAS control flag
Re-order Authentication providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (4)
Settings for myrealm
Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration
Authentication
Password Validation
Authorization
Adjudication
Role Mapping
Auditing
Credential Mapping
Certification Path
Keystores
Customize this table
New
Delete
Reorder
Showing 1 to 4 of 4 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

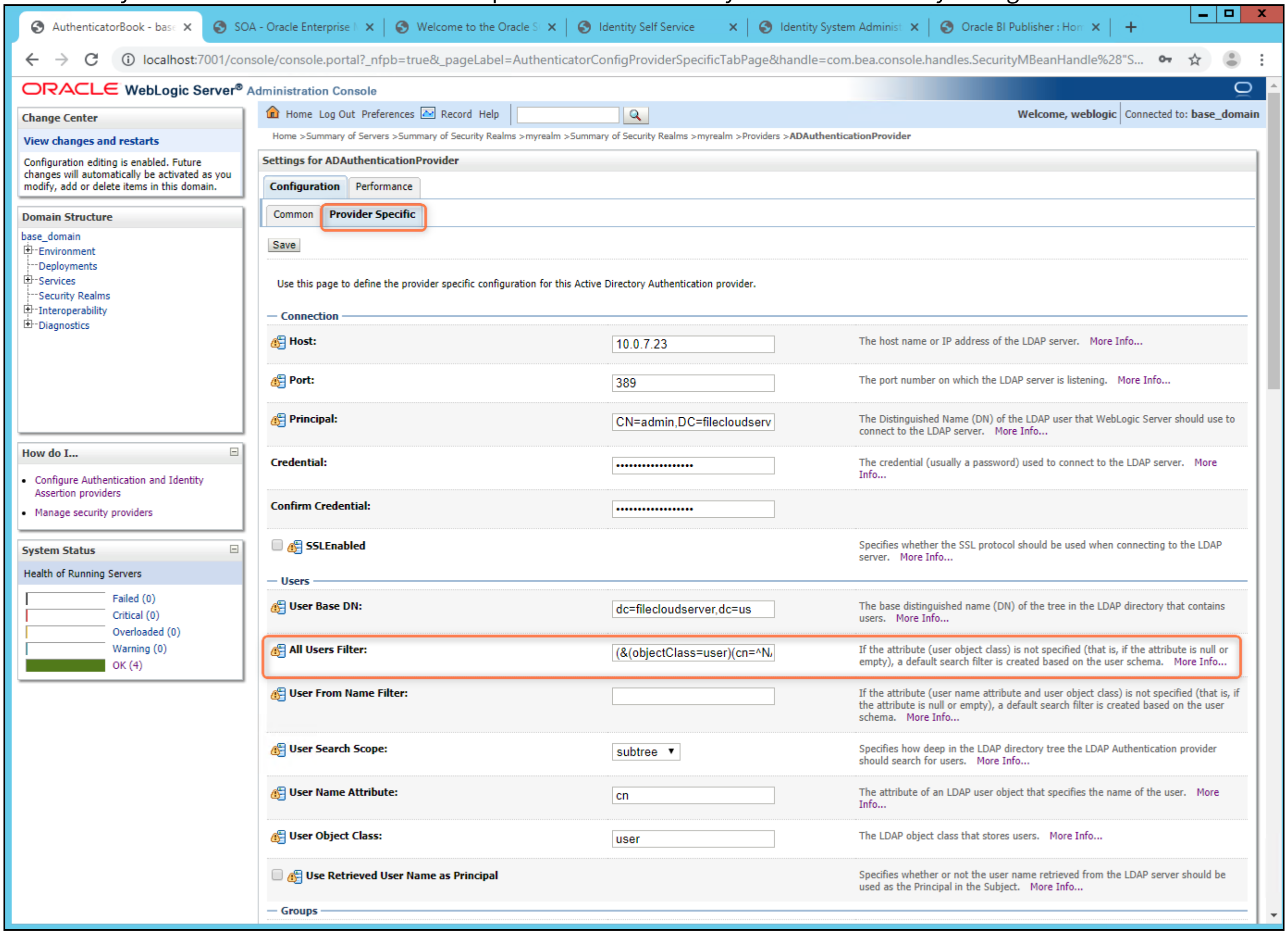
An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Authentication 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

WebLogic Server Version: 10.3.6.0
Copyright © 1996, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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.


AuthenticatorBook - base
SOA - Oracle Enterprise
Welcome to the Oracle S
Identity Self Service
Identity System Administ
Oracle BI Publisher : Hom
localhost:7001/console/console.portal?_nfpb=true&_pageLabel=AuthenticatorConfigProviderSpecificTabPage&handle=com.bea.console.handles.SecurityMBeanHandle%28"S...
ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: base_domain
Change Center
View changes and restarts
Domain Structure
base_domain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Configure Authentication and Identity Assertion providers
Manage security providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (4)
Configuration
Performance
Common
Provider Specific
Save

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Home >Summary of Servers >Summary of Security Realms >myrealm >Summary of Security Realms >myrealm >Providers >ADAuthenticationProvider

Settings for ADAuthenticationProvider

Use this page to define the provider specific configuration for this Active Directory Authentication provider.

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:	••••••••••••••••••	The credential (usually a password) used to connect to the LDAP server. More Info...
Confirm Credential:	••••••••••••••••••	
☐ SSLEnabled		Specifies whether the SSL protocol should be used when connecting to the LDAP server. More Info...

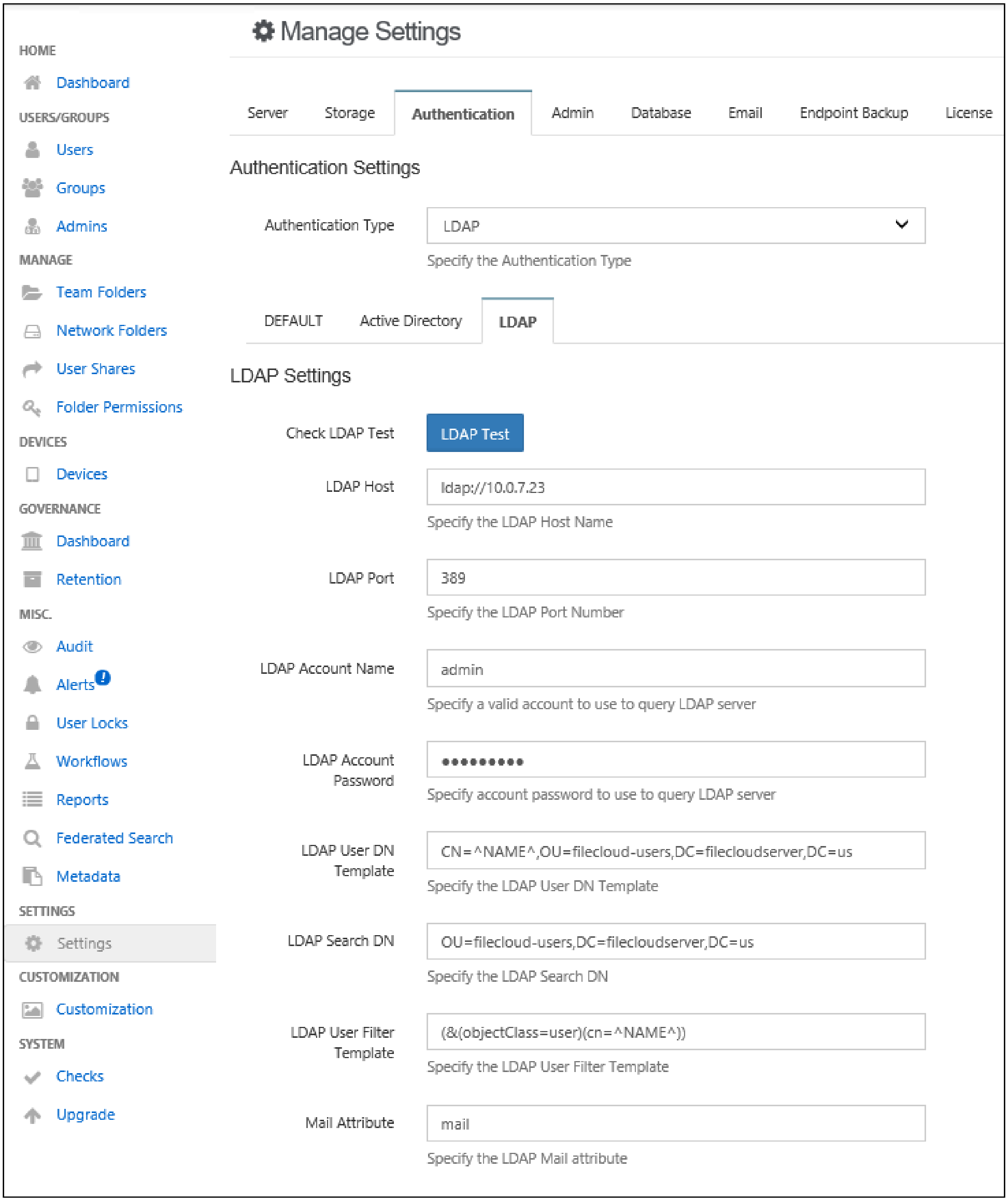
Users

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:		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

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^))



Manage Settings

Authentication Settings

Authentication Type: LDAP
Specify the Authentication Type

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

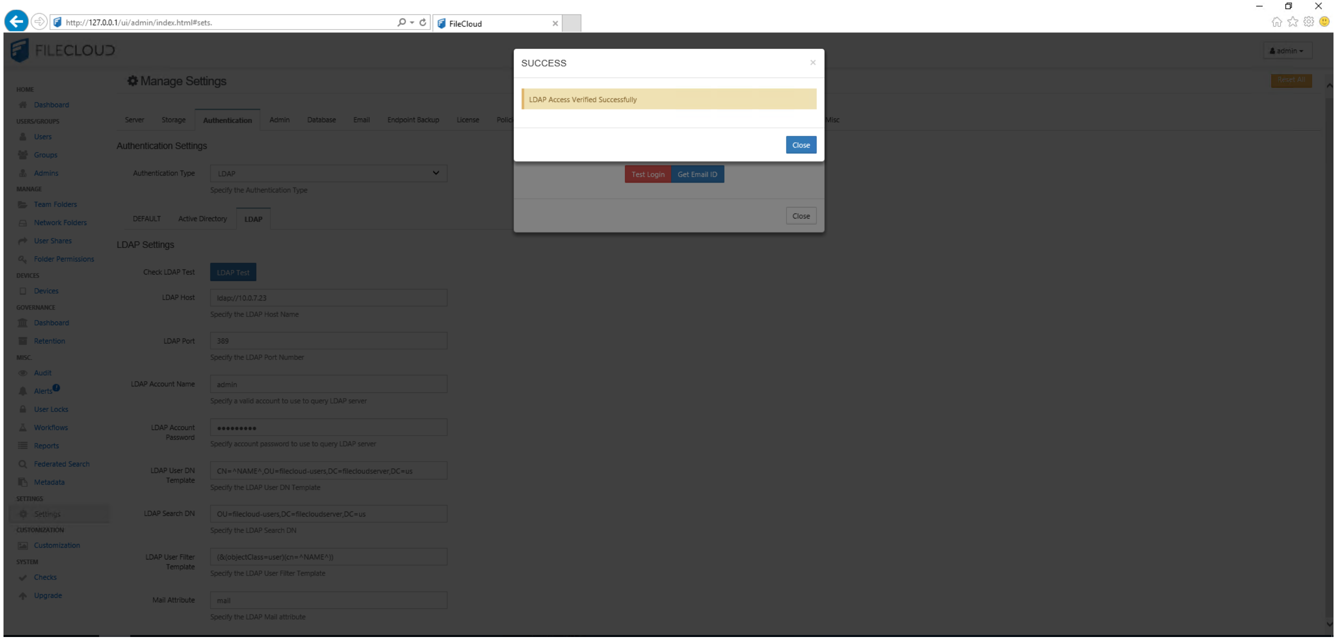
LDAP User DN Template: CN=^NAME^,OU=filecloud-users,DC=filecloudserver,DC=us
Specify the LDAP User DN Template

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.



SUCCESS

LDAP Access Verified Successfully

Authentication Settings

Authentication Type: LDAP
Specify the Authentication Type

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

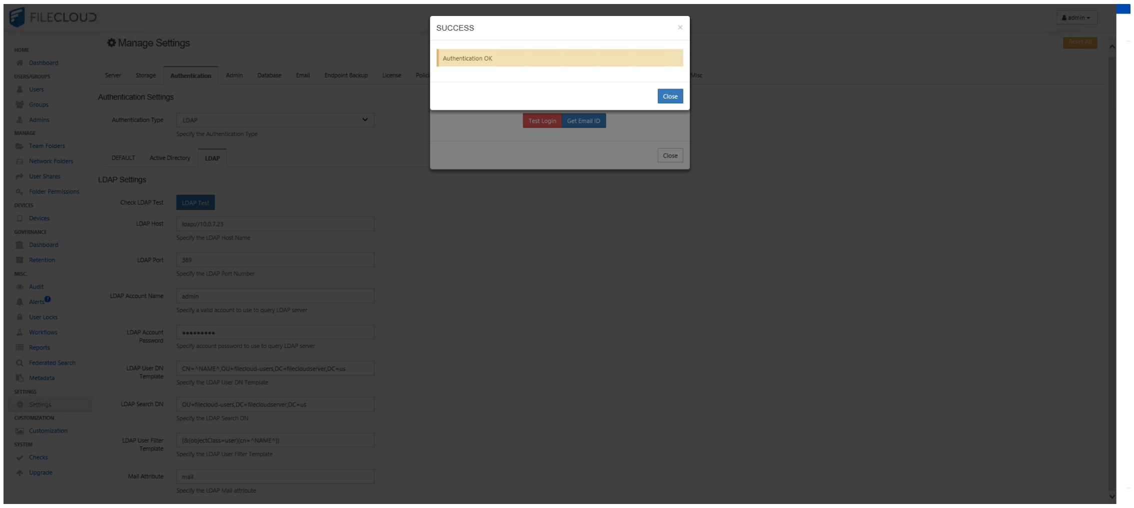
LDAP User DN Template: CN=^NAME^,OU=filecloud-users,DC=filecloudserver,DC=us
Specify the LDAP User DN Template

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

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.



SUCCESS

Authentication OK

Authentication Settings

Authentication Type: LDAP
Specify the Authentication Type

LDAP Settings

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

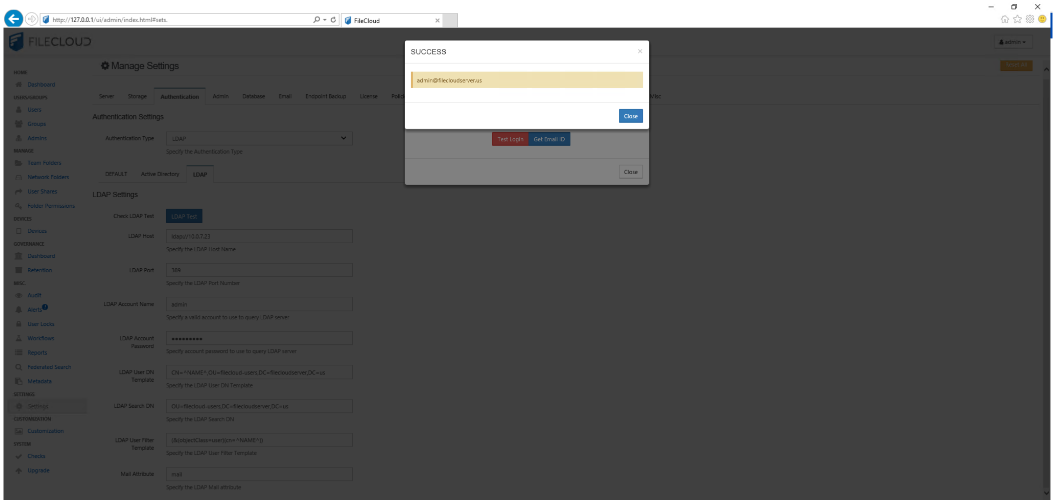
LDAP Account Password: ●●●●●●●●●
Specify account password to use to query LDAP server

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



SUCCESS

admin@filecloudserver.us

Authentication Type: LDAP

LDAP Host: ldap://10.0.7.23

LDAP Port: 389

LDAP Account Name: admin

LDAP Account Password: ●●●●●●●●●

LDAP User DN Template: CN=^NAME^,OU=filecloud-users,DC=filecloudserver,DC=us

LDAP Search DN: OU=filecloud-users,DC=filecloudserver,DC=us

LDAP User Filter Template: (&(objectClass=user)(cn=^NAME^))

Mail Attribute: mail

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.

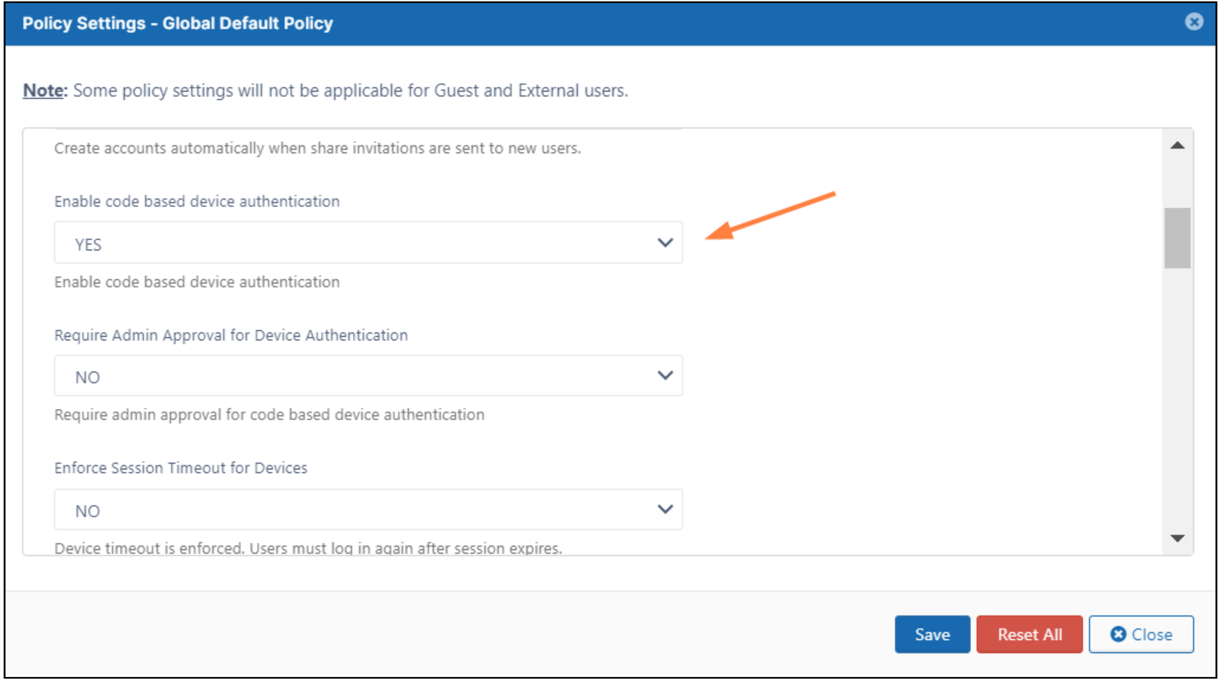
Enabling code-based device authentication

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.

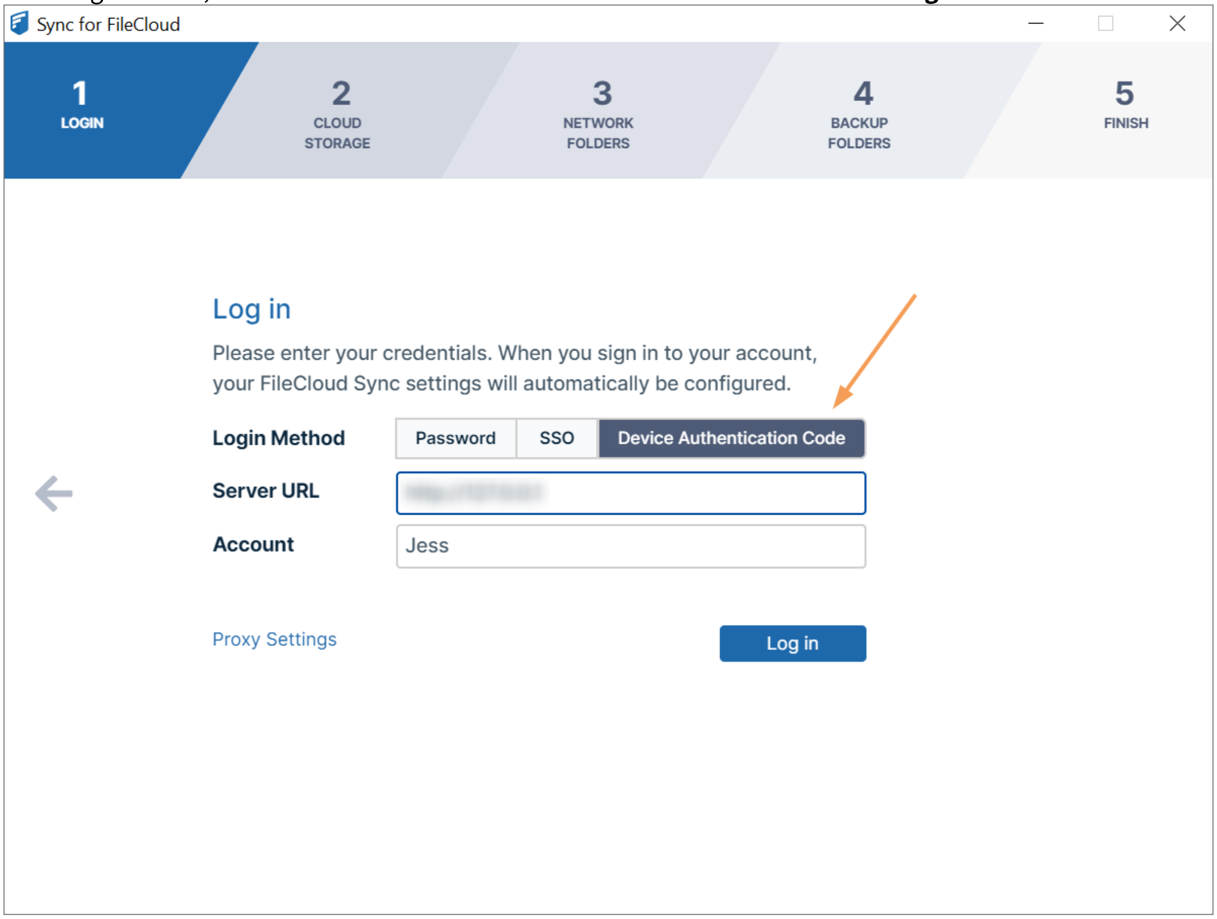
Now, when a user logs in to a client app, an approval request appears in in the user portal. The user must approve the request to receive a code that is entered into the client app to successfully log in.
How users log in with device authentication, below, shows how this process works.

How users log in with device authentication

How users log in with device authentication to desktop apps

Once code based authentication is enabled, the user can follow these steps to log in via a desktop app.
The following example uses the Sync application, but the procedure is the same for all of the desktop applications and the mobile apps.

1. In the login screen, the user selects **Device Authentication Code** and then clicks **Log in**.



Log in

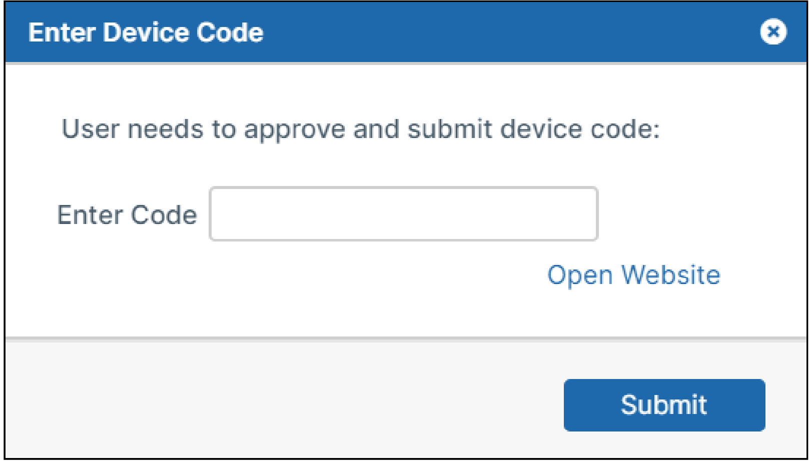
Please enter your credentials. When you sign in to your account, your FileCloud Sync settings will automatically be configured.

Login Method: Password | SSO | **Device Authentication Code**

Server URL: [redacted]

Account: Jess

The following dialog box opens.



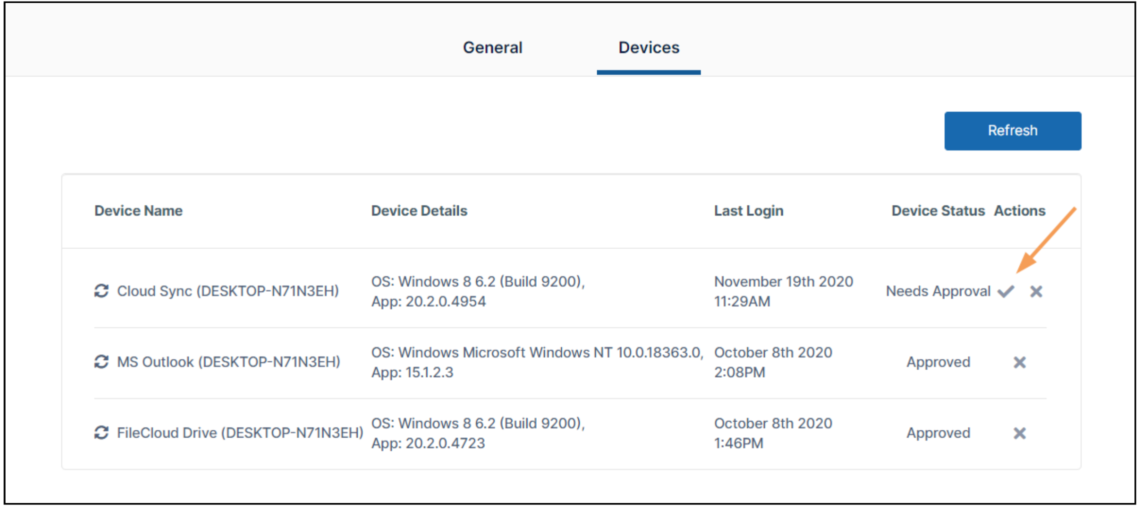
Enter Device Code

User needs to approve and submit device code:

Enter Code

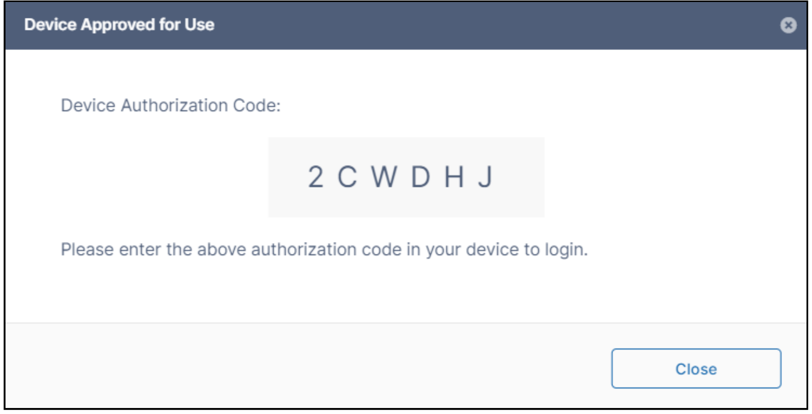
2. To get the device authorization code:
   a. The user logs in to the user portal, then clicks the arrow next to username and chooses **Settings**..
   b. In the **Settings** screen, the user click the **Devices** tab.

c. The user clicks the check next to **Needs Approval**.



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**:

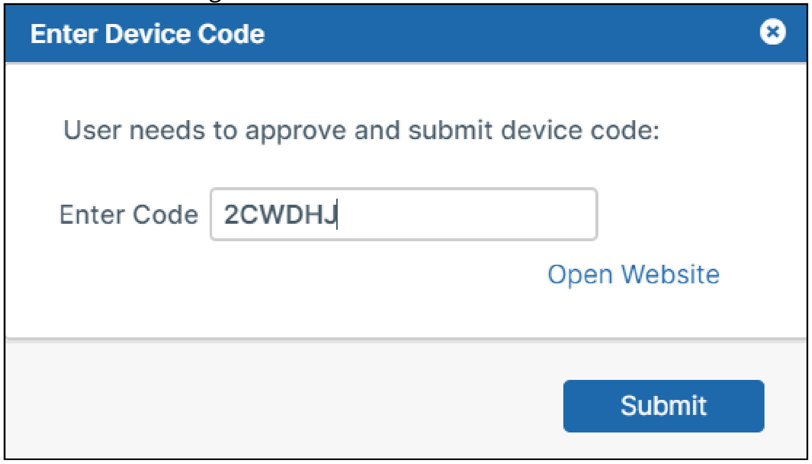


Device Authorization Code:

2 C W D H J

Please enter the above authorization code in your device to login.

3. The user copies the **Device Authorization Code** and pastes it into the **Enter Device Code** dialog box, then clicks **Submit** to log in.



User needs to approve and submit device code:

Enter Code 2CWDHJ

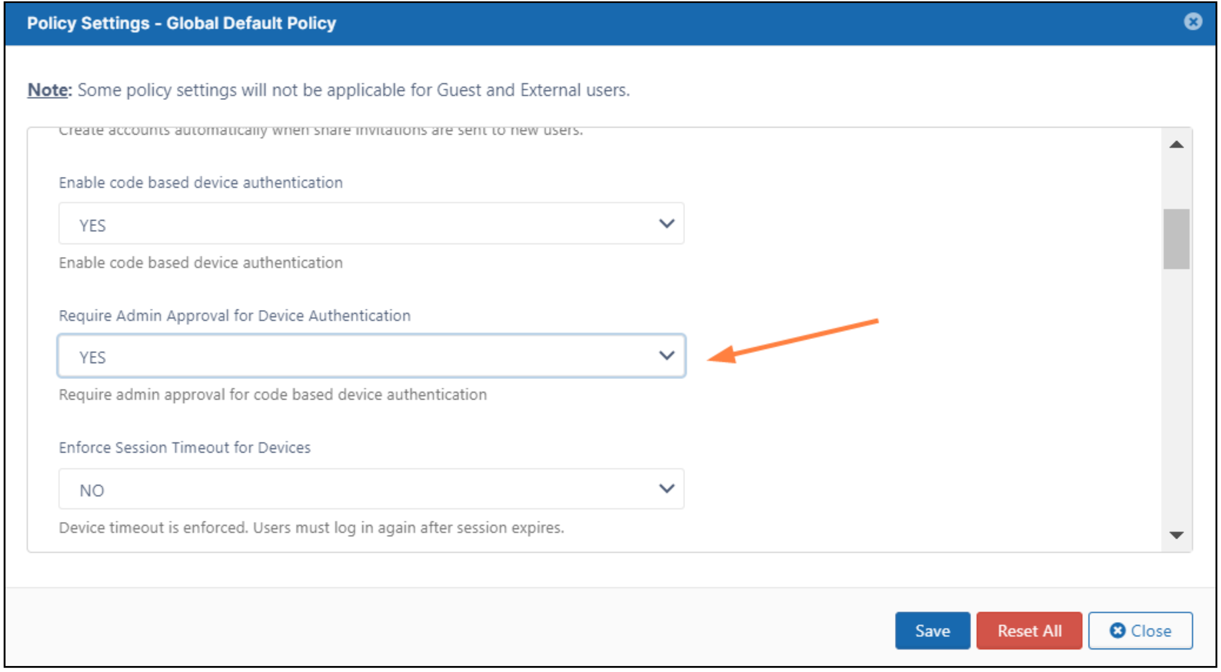
Requiring admin approval as well as user approval for devices

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

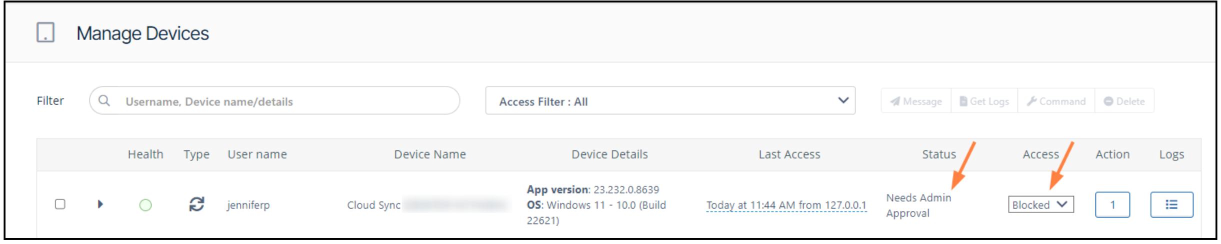
Require admin approval for code based device authentication

Enforce Session Timeout for Devices: NO

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

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**.



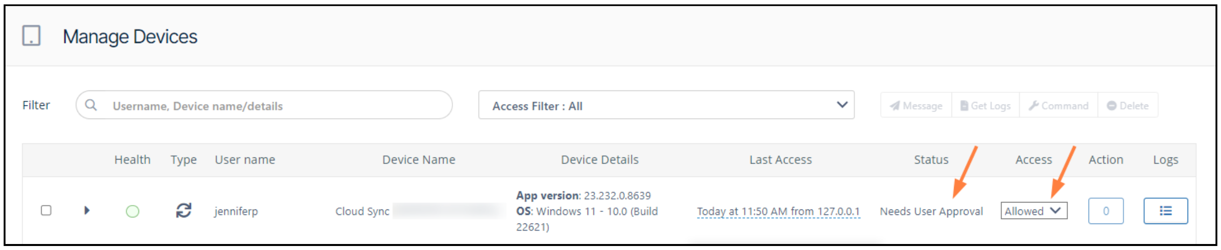
Manage Devices

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 [redacted]	**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	☰

2. In the **Access** column, change **Blocked** to **Allowed**.
   Now the **Status** column shows **Needs User Approval**, and the user must approve the client device (as shown above in **How users log in with device authentication**) and get an authorization code before log in can occur.



Manage Devices

Filter: Username, Device name/details | Access Filter : All | Message | Get Logs | Command | Delete

		Health	Type	User name	Device Name	Device Details	Last Access	Status	Access	Action	Logs
□	▸	○	⟳	jenniferp	Cloud Sync [redacted]	**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	☰

Enabling Basic Authentication

FileCloud supports enabling basic authentication for users through a policy setting.

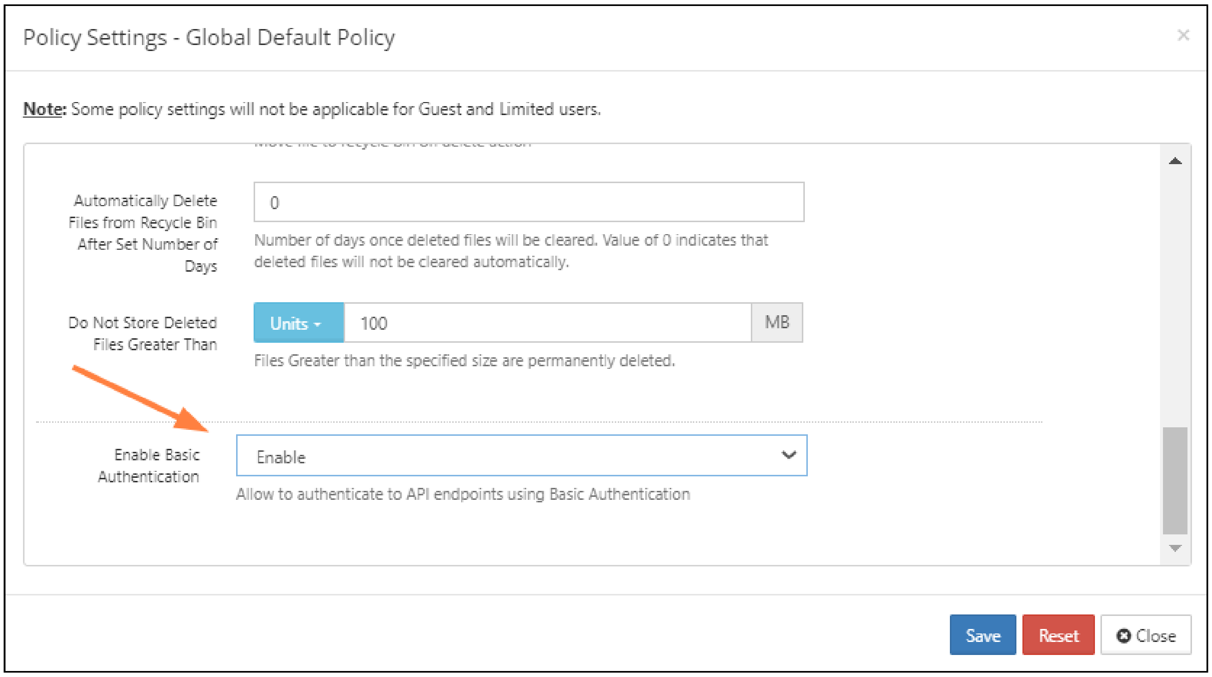
To enable basic authentication:

1. Add the setting for basic configuration to cloudconfig.php:
   a. Open cloudconfig.php.
      - Windows Location : C:\xampp\htdocs\config\cloudconfig.php
      - Linux Location : /var/www/html/config/cloudconfig.php
   b. Add the following and save:

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

2. In the Admin portal, navigate to **Settings > Policies**.
3. Open an existing policy for edit, or create a new policy and open it for edit.
4. Scroll to the bottom of the policy's **General** tab.

5. Set **Enable Basic Authentication** to **Enable**.



Policy Settings - Global Default Policy

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

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: 100 MB

Files Greater than the specified size are permanently deleted.

Enable Basic Authentication: Enable

Allow to authenticate to API endpoints using Basic Authentication

6. Click **Save**.
7. To enable specific users to use basic authentication, assign the policy to them.

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

⚠ 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.

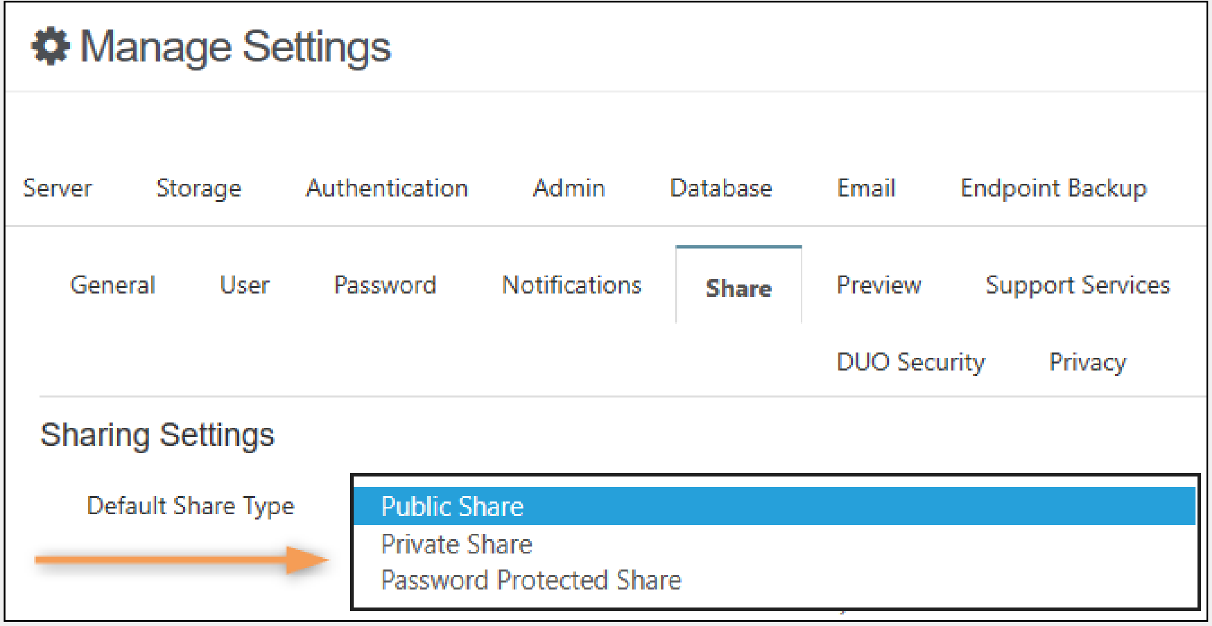
- Applicable only when *Global Share Mode* is set to Allow All Shares
- This type can be changed by the user unless *Disallow Default Share Settings Change* is set.

Public Share	Allows users to share with anyone who has the link to the share. • Does not require the user you want to share with to have a FileCloud account. • Share a file with everyone with or without restrictions. • Share a file with everyone and require a password.

Private Share	Allows users to share with anyone who has the link and can log in to a FileCloud account. • Does require the user you want to share with to have a FileCloud account. • Requires an invitation to be sent to someone to create a FileCloud account if they don't already have one. • Share a file with all FileCloud users with or without restrictions. • Share a file with specific FileCloud users with or without restrictions.
Password Protected Share	Forces users to create a password when sharing a file or folder. • Recipients of the share are given the password when they receive the link to the share. • The share can be public or private.

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.**



Sharing Settings

Default Share Type

Public Share
Private Share
Password Protected Share

5. **Click *Save*.**

› Set Expiration Days Default

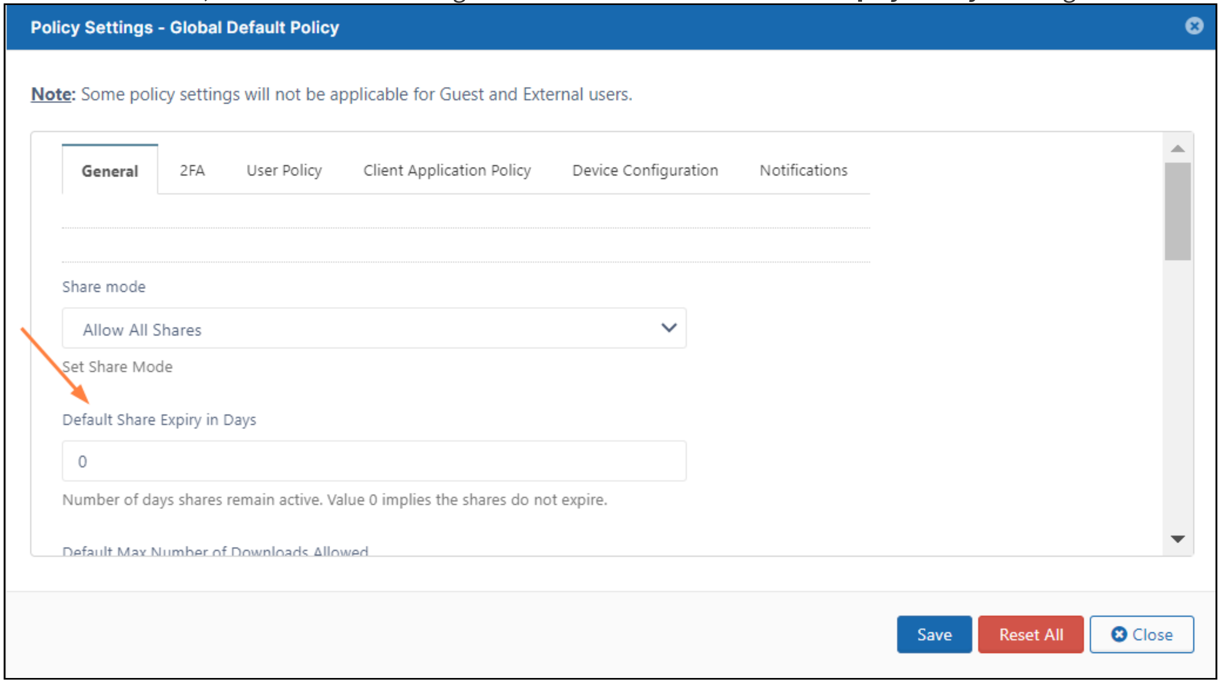
Administrators can allow users to share files and folders for as long as they exist, or you can set a suggested number of days that a share remains active by default.

- 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.

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

5. Click **Save**.
   The value is only changed for users who are using this policy.

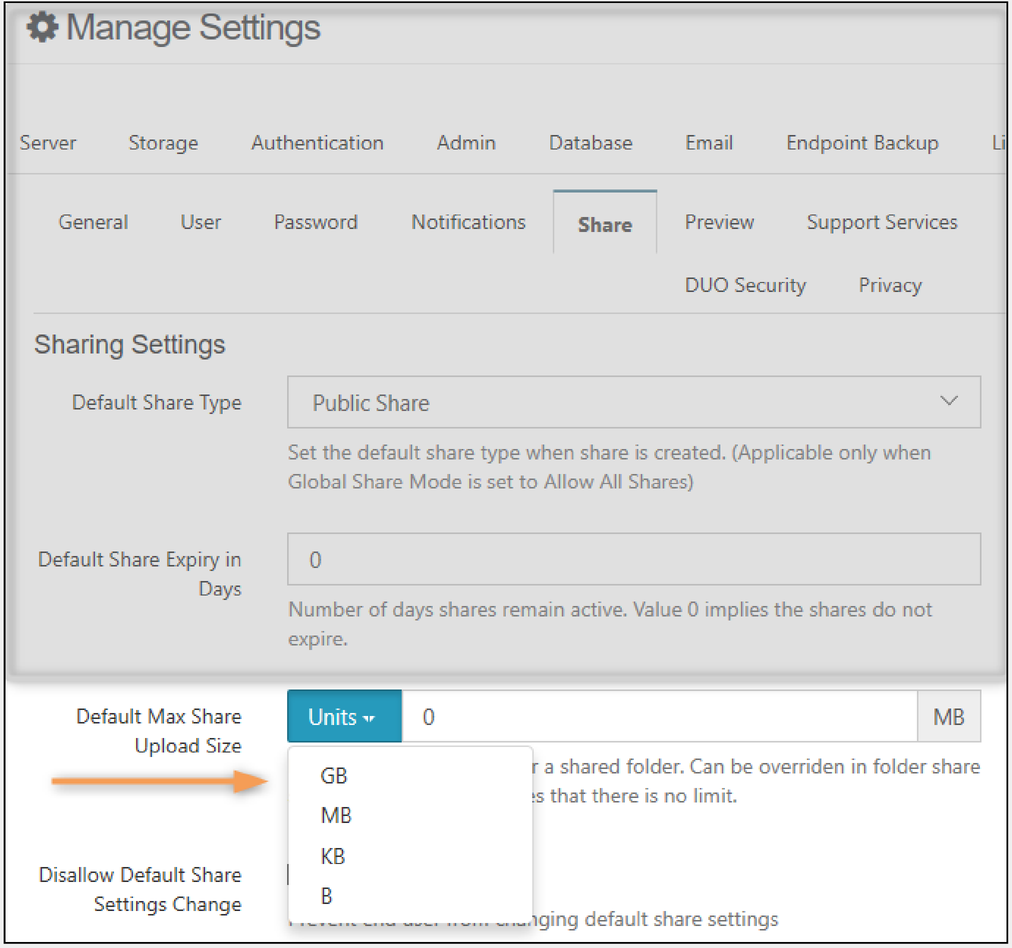
Default Max Share Upload Size

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.**



Sharing Settings

Default Share Type: Public Share

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

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Share Upload Size: 0 MB

r a shared folder. Can be overriden in folder share

s that there is no limit.

Disallow Default Share Settings Change

ging default share settings

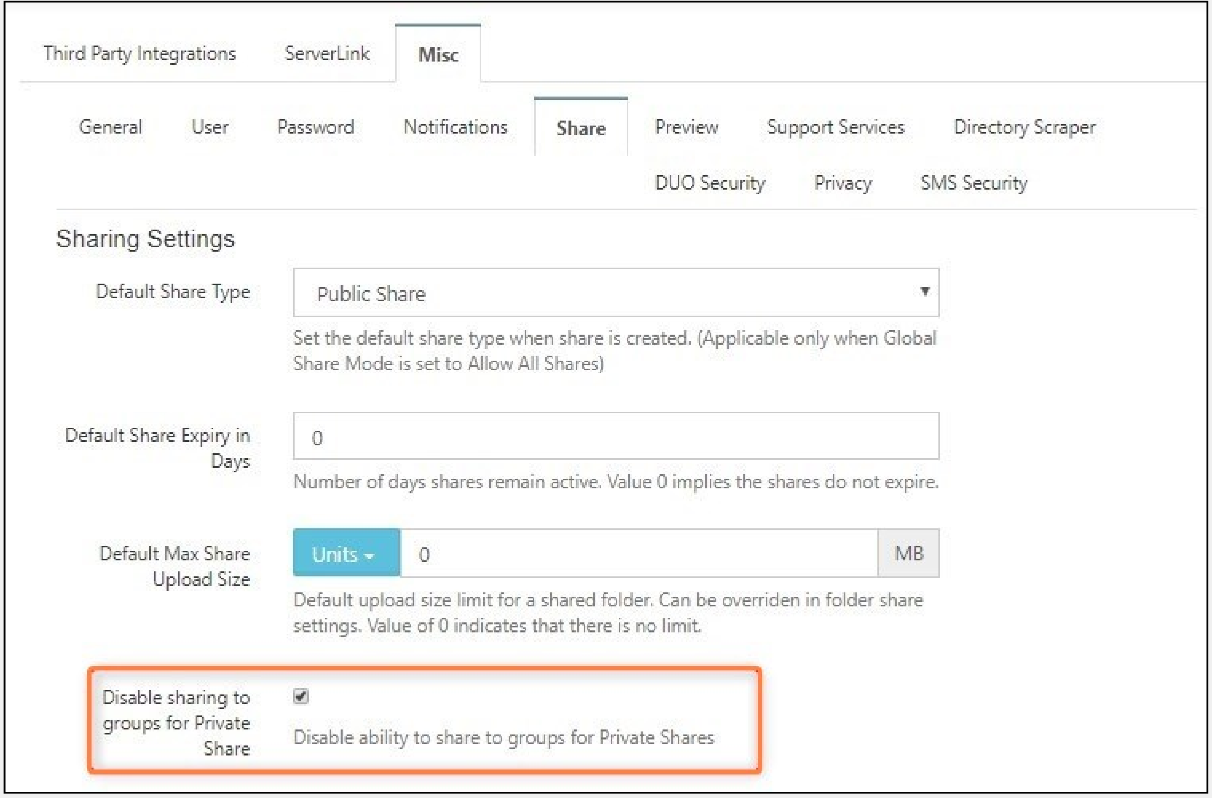
5. **Click *Save*.**

Disable Sharing to Groups for Private Share

You can check Disable 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*.**



Sharing Settings

Default Share Type: Public Share

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

Number of days shares remain active. Value 0 implies the shares do not expire.

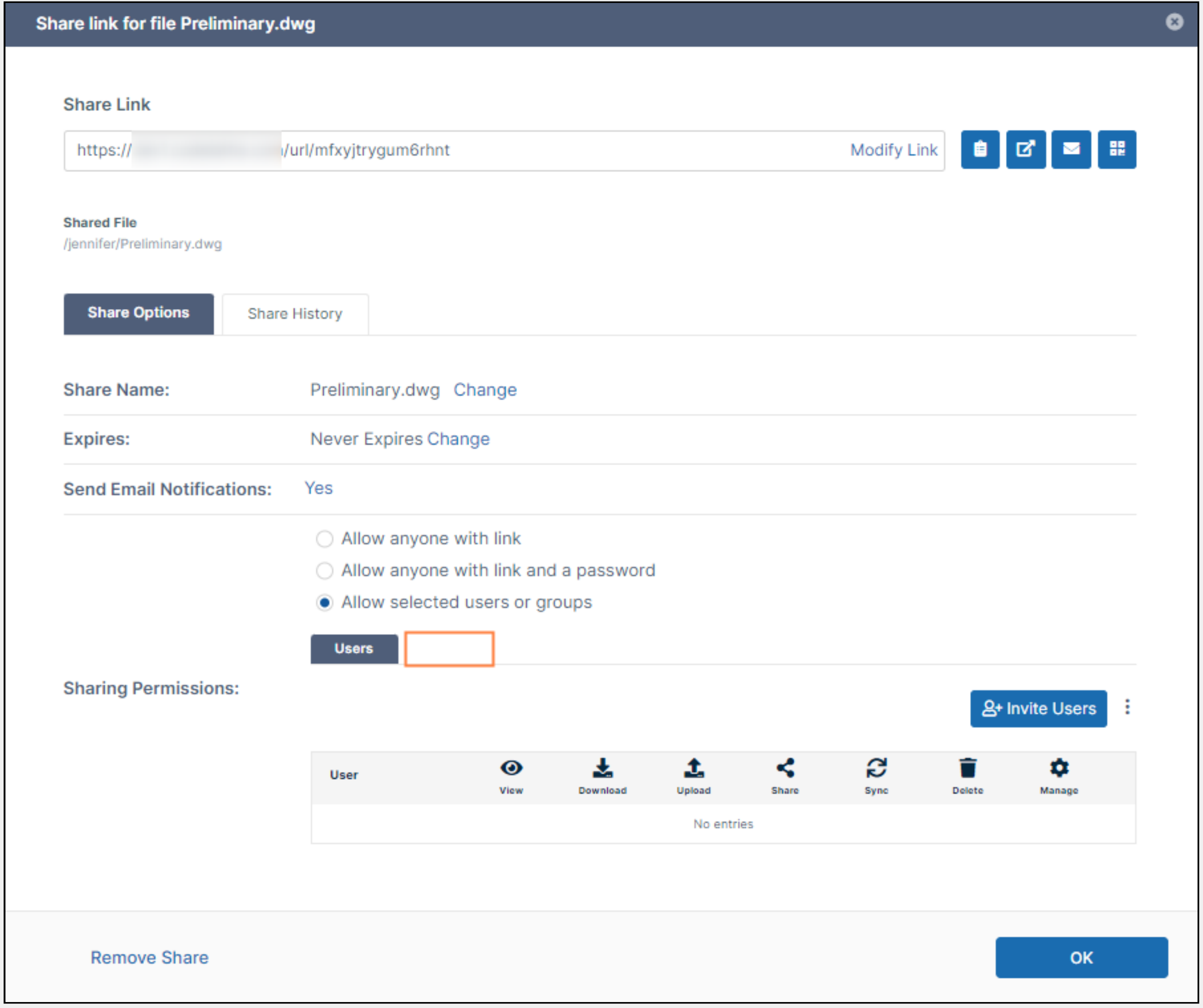
Default Max Share Upload Size: 0 MB

Default upload size limit for a shared folder. Can be overriden in folder share settings. Value of 0 indicates that there is no limit.

Disable sharing to groups for Private Share: ☑

Disable ability to share to groups for Private Shares

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

Shared File
/jennifer/Preliminary.dwg

Share Name: Preliminary.dwg

Expires: Never Expires

Send Email Notifications: Yes

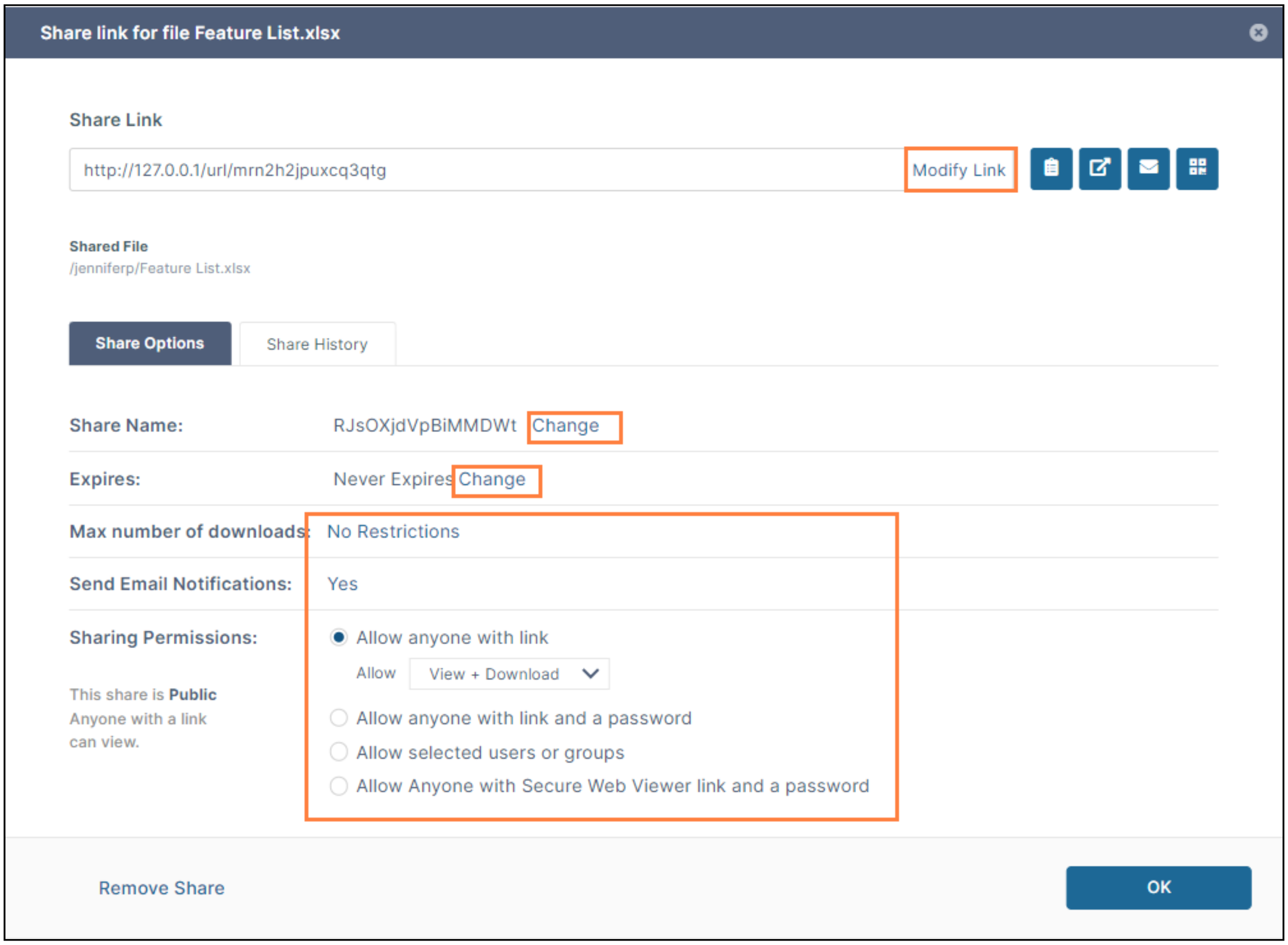
Sharing Permissions:

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

User	View	Download	Upload	Share	Sync	Delete	Manage
No entries							

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

http://127.0.0.1/url/mrn2h2jpuxcq3qtg

Shared File
/jenniferp/Feature List.xlsx

Share Name: RJsOXjdVpBiMMDWt

Expires: Never Expires

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 link
Allow View + Download

○ Allow anyone with link and a password

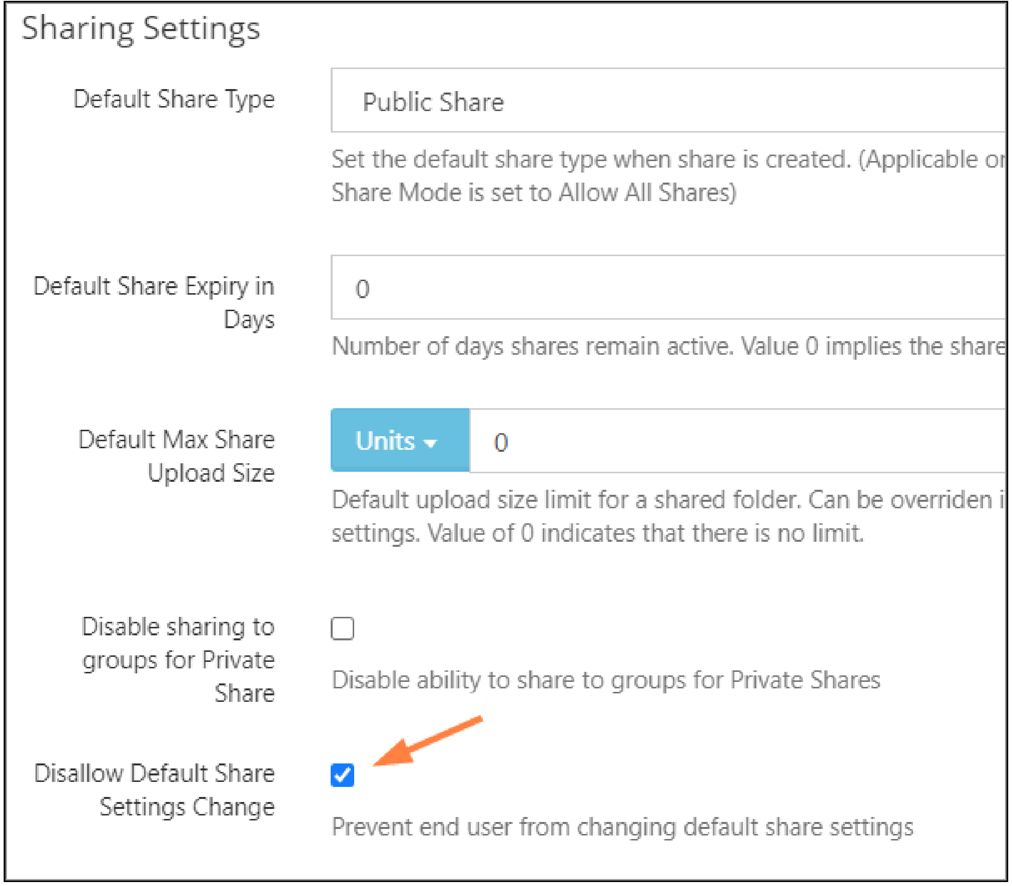
○ Allow selected users or groups

○ Allow Anyone with Secure Web Viewer link and a password

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 or
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

Default Max Share Upload Size: Units ▾ 0

Default upload size limit for a shared folder. Can be overriden i
settings. Value of 0 indicates that there is no limit.

Disable sharing to groups for Private Share: ☐

Disable ability to share to groups for Private Shares

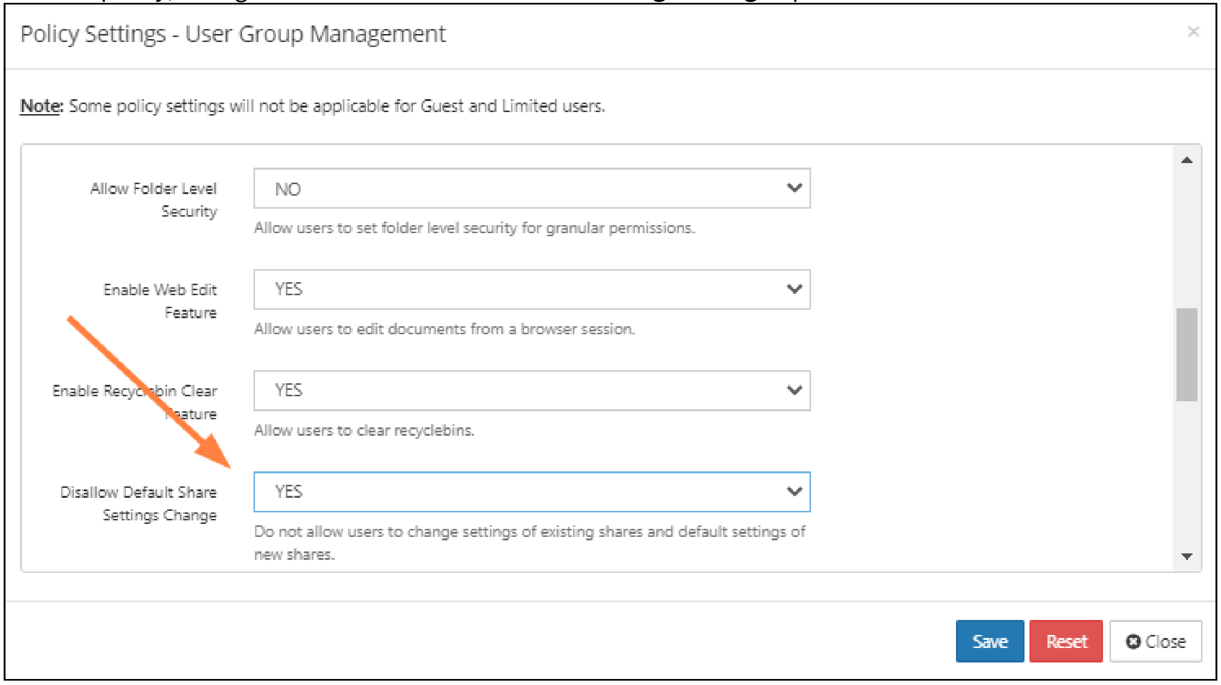
Disallow Default Share Settings Change: ☑

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.

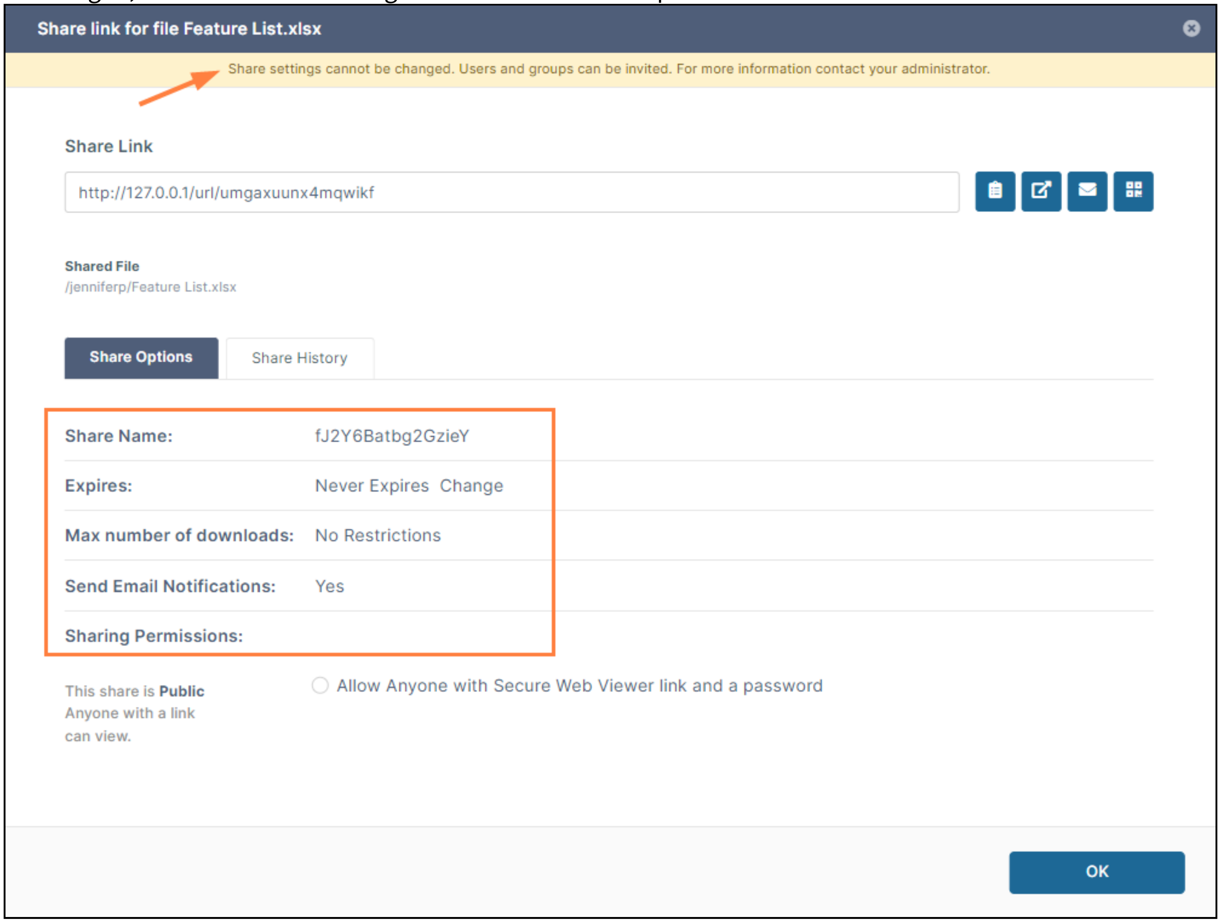
Allow Folder Level Security: NO
Allow users to set folder level security for granular permissions.

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.

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 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

Disable Manage Share Options

After a user opens a browser and logs in to the User Portal, they can share a folder privately.

- This share has the ability to be shared again by members.
- Share owners can also designate another user to manage those re-shares of the original shared folder by selecting the **Allow Manage option.**

If the folders being shared are in Network Folders, and there are a large number of shares and users working with Network Folders, displaying a list of shares may take too long or even timeout.

Now you can configure FileCloud to disable the **Allow Manage** option for shares in Network Folders to decrease the time it takes to display the list of shares.

- **TONIDOCLOUD_MANAGE_SHARE_ENABLE** is a new config that can be set to 0 to completely disable the **Allow Manage** sharing option for Network Folders.

To disable the Allow Manage option for Network Folders:

1. Open the following file for editing:

For Windows:

```
c:\xampp\htdocs\config\cloudconfig.php
```

For Linux:

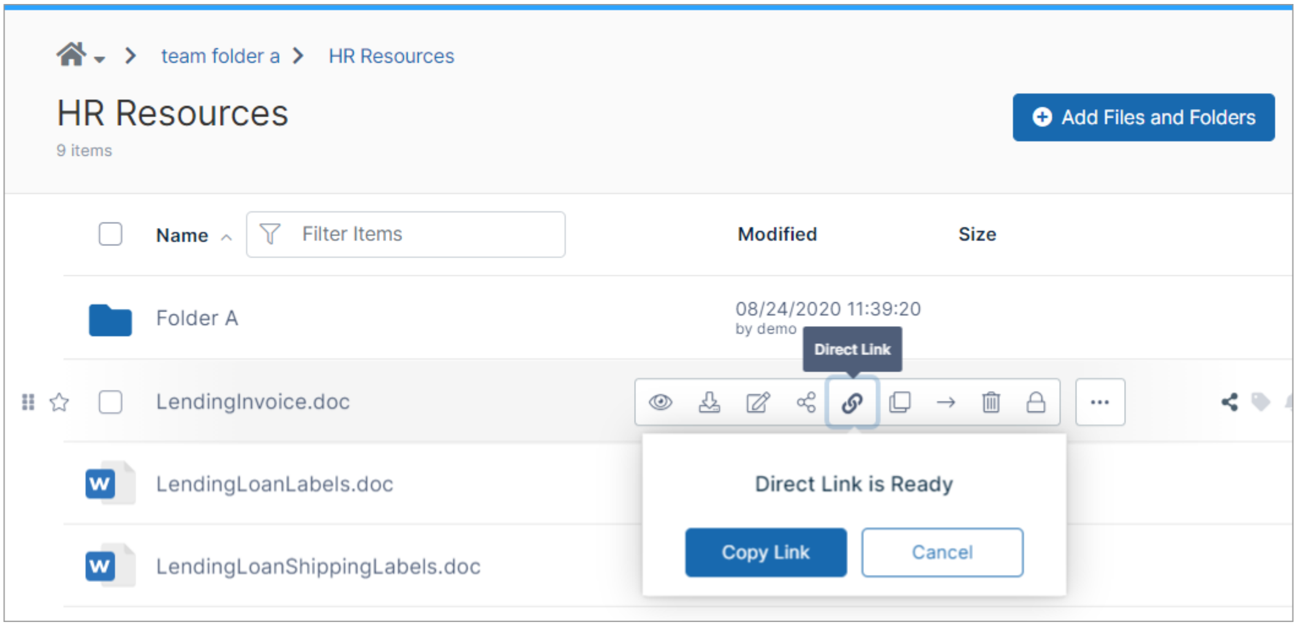
```
/var/www/html/config/cloudconfig.php
```

2. Add the following line:

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

Hide Direct Link option for shared files and folders

In the User portal, the **Direct Link** action is available when users select a file or folder in Team Folders or Shared with Me:



Beginning in FileCloud 20.2, you can configure FileCloud to hide the **Direct Link** action.

To hide the Direct Link action:

1. Open the following file for editing:
   For Windows:

```
XAMPP/htdocs/config/cloudconfig.php
```

For Linux:

```
/var/www/html/config/cloudconfig.php
```

2. Add the following line:

```
define('TONIDOCLOUD_HIDE_SHARE_DIRECTLINK_OPTION', 1);
```

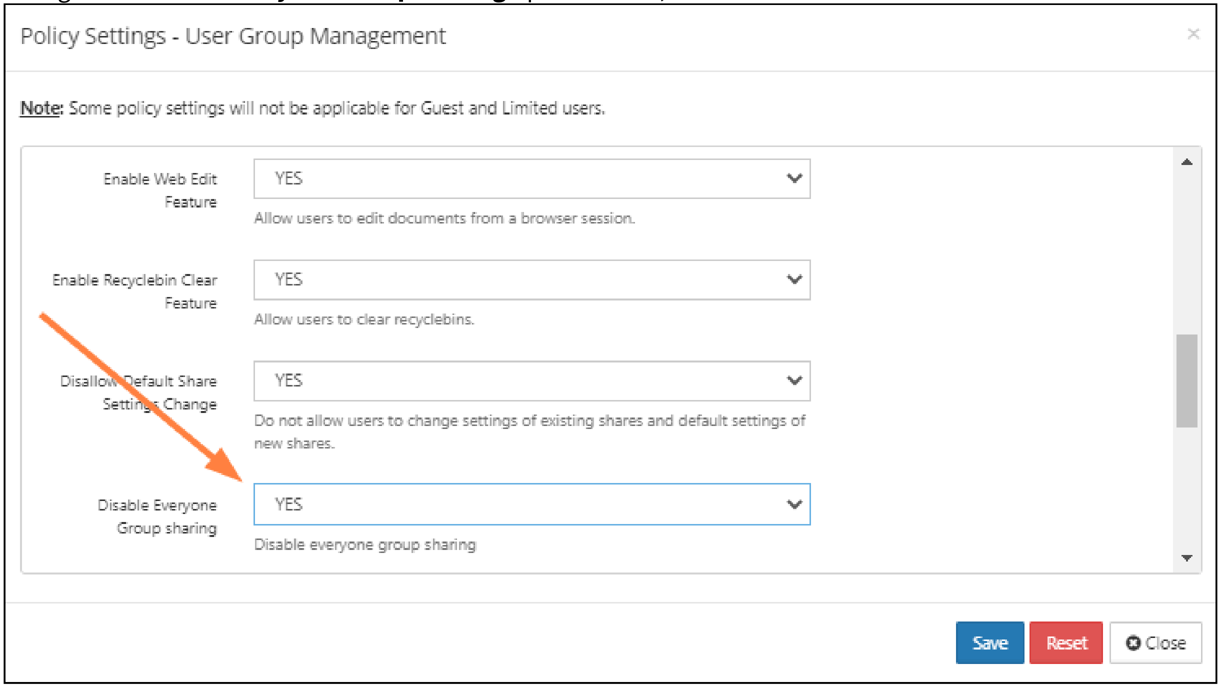
When a user selects a file or folder in Team Folders or Shared with Me, the direct link option no longer appears.

Disable sharing to the Everyone group

The Everyone group includes all of your active Full users. If you do not want to allow sharing of files or folders with all of your users at once, you can disable sharing to the Everyone group.

To disable sharing to the Everyone group:

1. 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

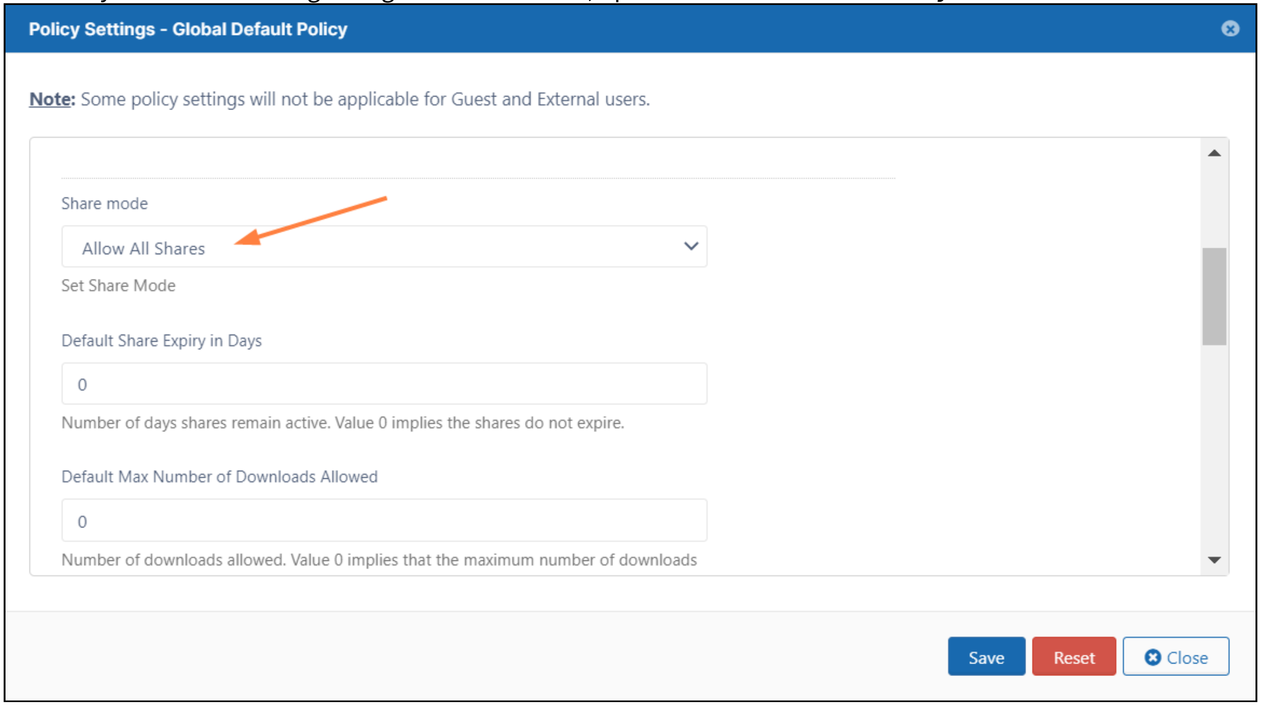
Now, when users select a group to share with, the **Everyone** group does not appear.

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: Allow All Shares

Set Share Mode

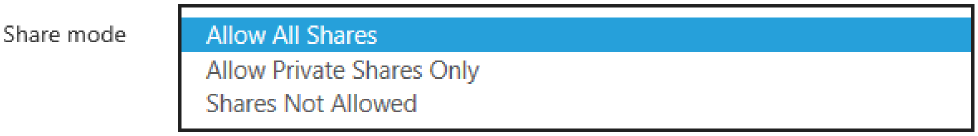
Default Share Expiry in Days: 0

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed: 0

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:



Option	Description
Allow All Shares	Allows users to share any file or folder with custom permissions. A file or folder can be shared with: • Anyone with access to the link (Public Share). *No FileCloud account required.* • Anyone with access to the link (Public Share) and a password. *No FileCloud account required.* • Another user in FileCloud (Private share). *FileCloud account required.* The shared files will show up in the "Shared with Me" folder.
Allow Private Shares Only	Allows users to share any file or folder with a user that has an existing FileCloud account. Sharing Privately requires: • The recipient(s) to be another user in FileCloud (Private share). *FileCloud account required.* The shared files will show up in the "Shared with Me" folder. • An invitation to be sent to someone to create a FileCloud account so that they can access a share. • Users to configure the share with or without restrictions.
Shares Not Allowed	Prevents users from sharing any file or folder. ⚠ If you choose this option, then no other Sharing settings that you configure will be in effect.

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	• 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	• Have FileCloud remove the URL links to shares automatically • Remove shared files automatically	Specify what happens when a shared file or folder is no longer accessible from the Share link • Expired URL links will be removed automatically on the next Cron run (In this case the files will not be affected.) • If you choose to remove files, they will be moved to the Recycle Bin on the next Cron run
Notifications	• Alert users with access to a share that it will expire soon • Specify the number of days before the share expires that you want to send the email notification	You can have FileCloud send email to everyone who has access to the shared file or folder

Set Expiration Period

Set Expiration Days Default

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.

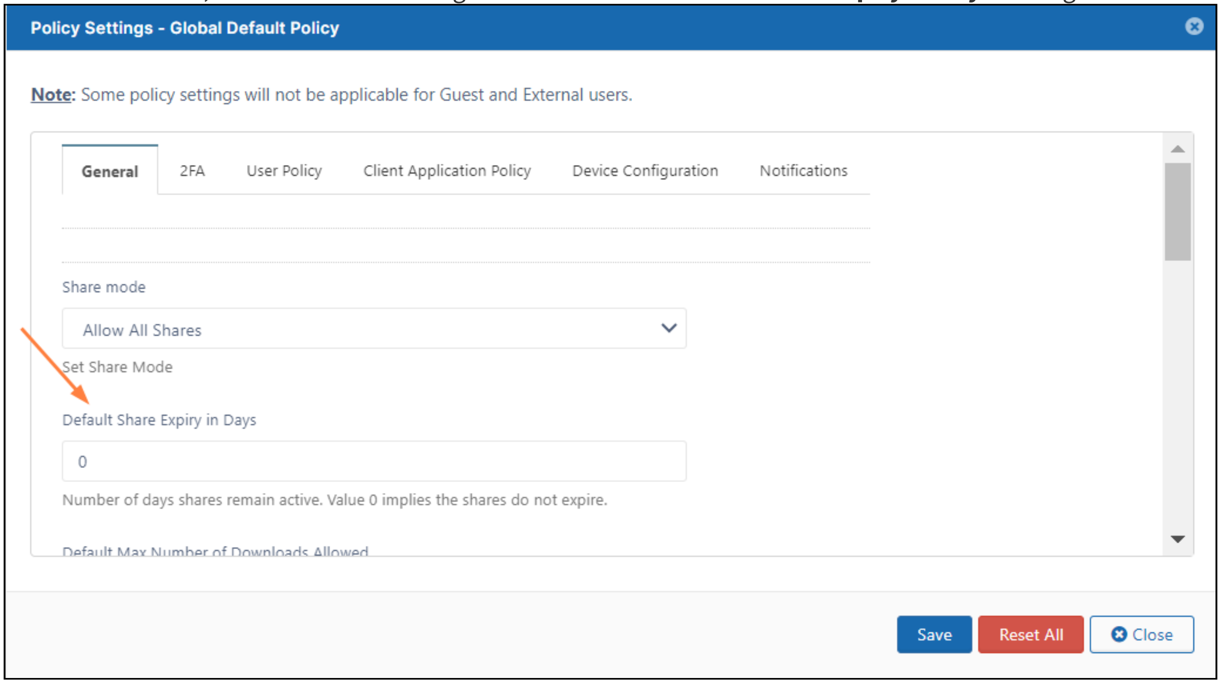
- Using a value of 0 means that unless changed by a user, shares do not expire.
- This setting can be changed by the user unless **Disallow Default Share Settings Change** is set in the **Settings > Misc > Share** tab.

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.

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

5. Click **Save**.
   The value is only changed for users who are using this policy.

Set Expiration Actions

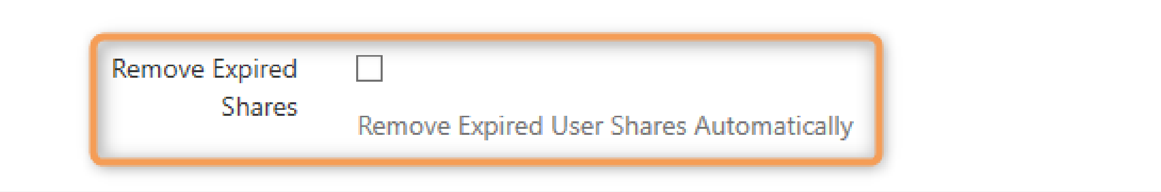
Remove Expired Shares

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:

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 *Removed Expired Shares*, select the checkbox.**



Remove Expired Shares □

Remove Expired User Shares Automatically

5. **Click *Save*.**

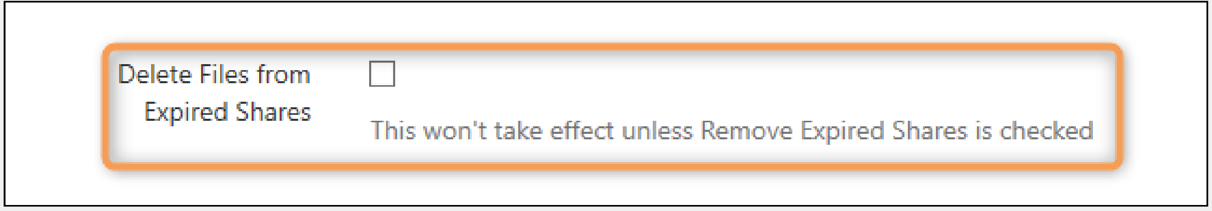
Remove Shared Files

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:

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 *Delete Files from Expired Shares*, select the checkbox.**



Delete Files from Expired Shares □

This won't take effect unless Remove Expired Shares is checked

5. **Click *Save*.**

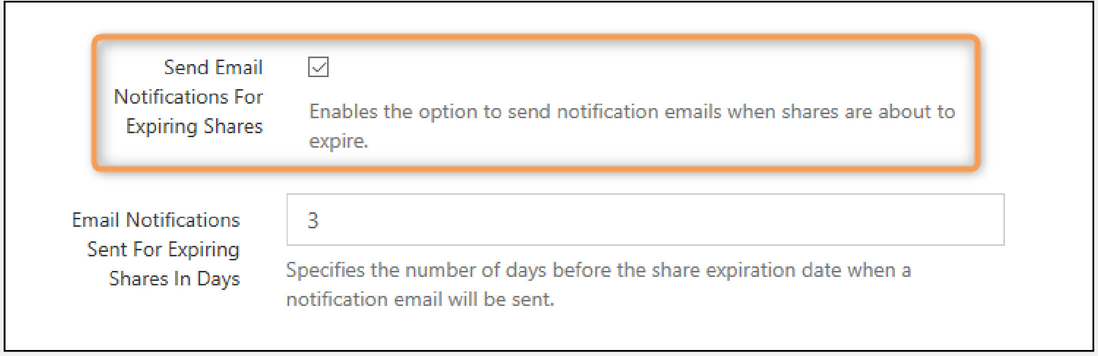
Send Expiration Notifications

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.**



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: 3

Specifies the number of days before the share expiration date when a notification email will be sent.

5. **Click *Save*.**

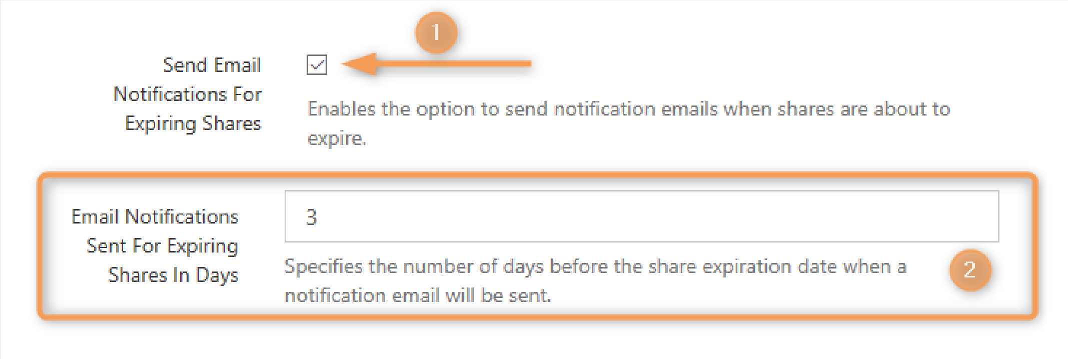
Specify Days to Expiration Email

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: 3
Specifies the number of days before the share expiration date when a notification email will be sent.

5. **Click *Save*.**

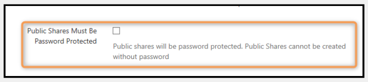
Secure Shares

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:

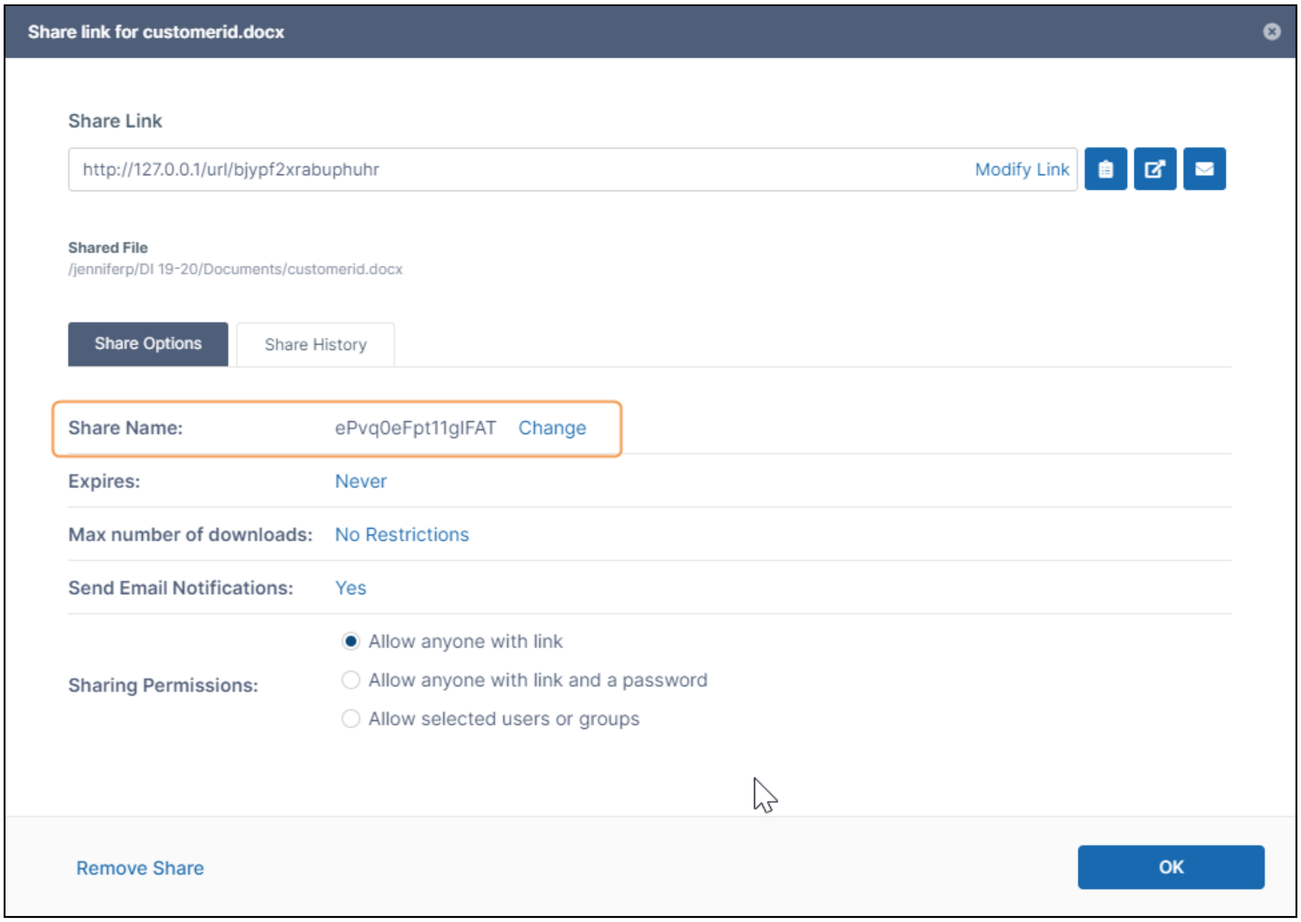
1. **Open a browser and log in to the *Admin Portal*.**
2. **From the left navigation pane, under *Settings*, select *Settings*.**
3. **Select the *Misc.* tab, and then the *Share* sub-tab.**
4. **Next to *Public Shares Must Be Password Protected*, select the checkbox.**
5. **Click *Save*.**

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

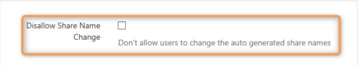
Share Link

http://127.0.0.1/url/bjypf2xrabuphuhr

Shared File
/jenniferp/DI 19-20/Documents/customerid.docx

Share Name:	ePvq0eFpt11gIFAT 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

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

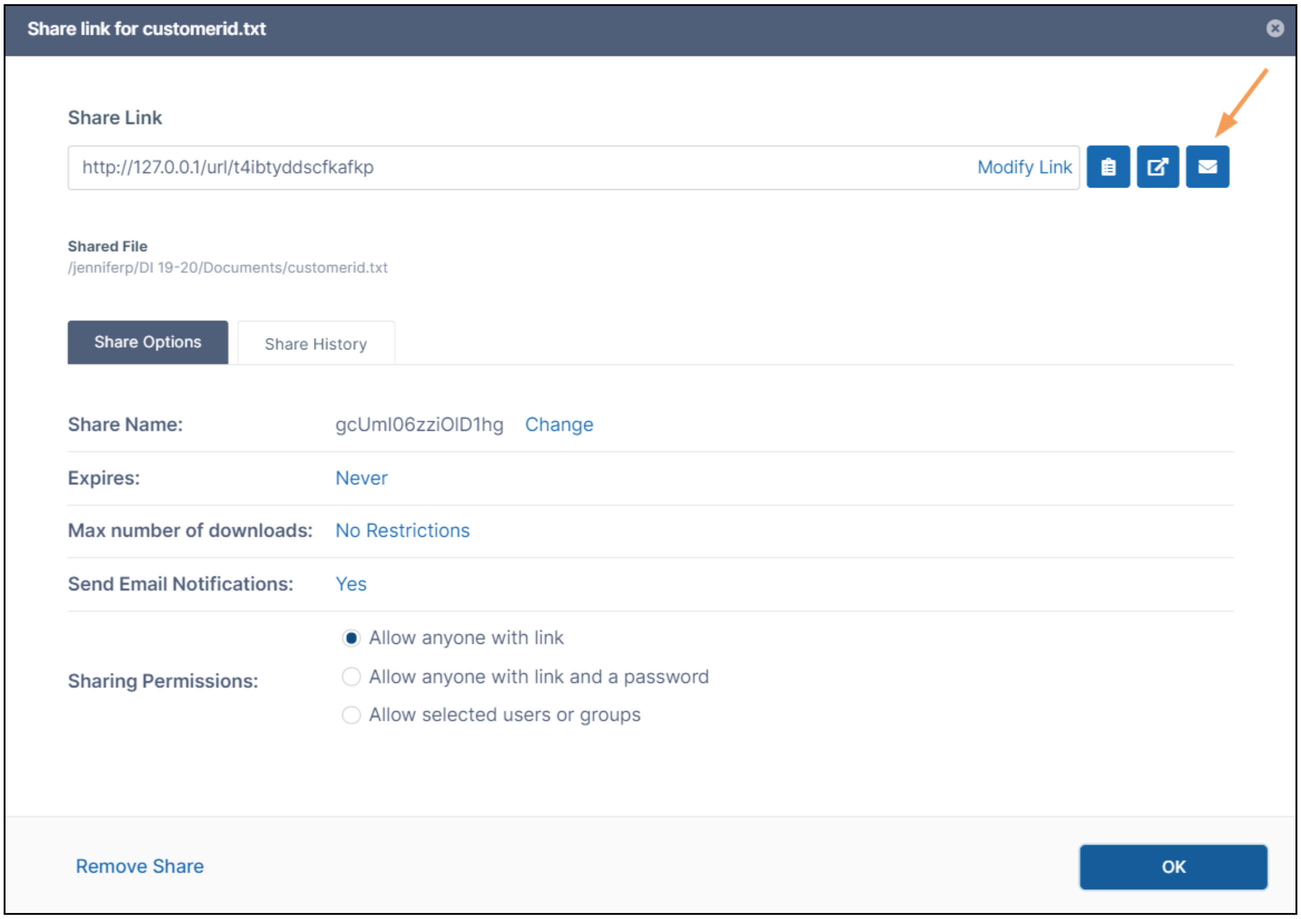
To prevent name changes for shares:

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

http://127.0.0.1/url/t4ibtyddscfkafkp

Shared File
/jenniferp/DI 19-20/Documents/customerid.txt

Share Name: gcUml06zziOlD1hg Change

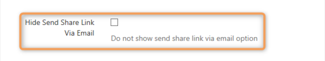
Expires: Never

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

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.

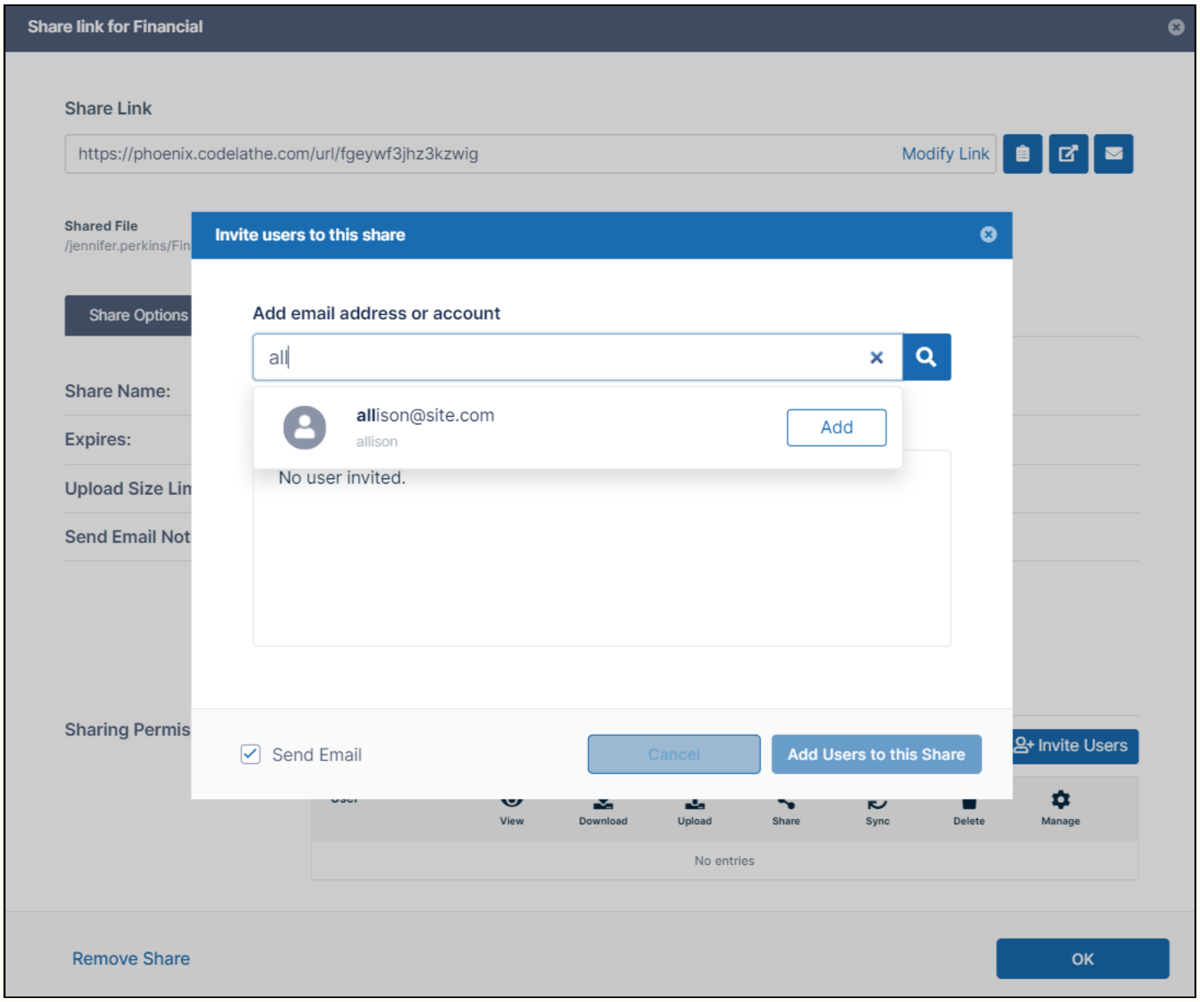
However, this is not desirable in certain cases and organizations, as the search results reveal user accounts that exist in the FileCloud system.

Therefore, FileCloud Server allows you to restrict user searches using two search modes:

User Account	User Account Type
• Exact Email Search With Explicit Account Invite • Exact Email Search With Implicit Account Invite • Exact Name/Email Search • Partial Name/Email Search	• ALL • FULL • GUEST • EXTERNAL
➡ How to Enable User Account Search Mode	➡ How to Enable User Account-Type Search Mode
NOTE: You can use both of these search limitations together to create a combination that meets your requirements. For example, you can set the *User Account Search Mode* to Partial Name/Email Search, and then use the *User Account Type* search mode to limit the results to only accounts with FULL access.	

⚠ **Note**

Using a search mode limits account searches for all the users in the FileCloud system.
These settings 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.

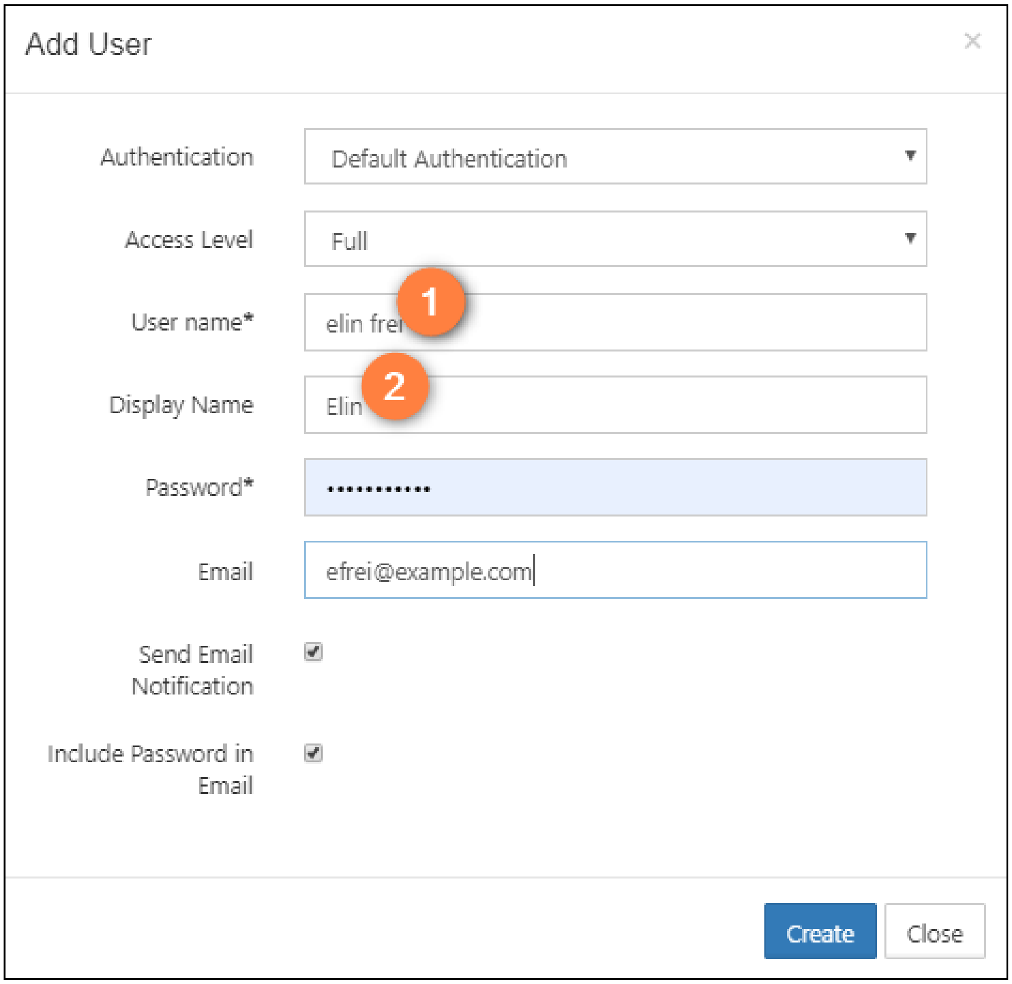


Use Display Name as well as User Account Name

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



Authentication: Default Authentication ▾

Access Level: Full ▾

User name*: elin frei

Display Name: Elin

Password*: ••••••••••••

Email: efrei@example.com

Send Email Notification: ☑

Include Password in Email: ☑

In the Admin Portal, when you create a user, you can set 2 different names.

1. User Name

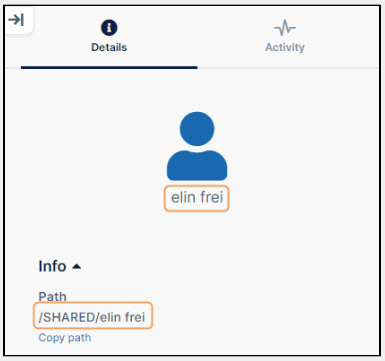
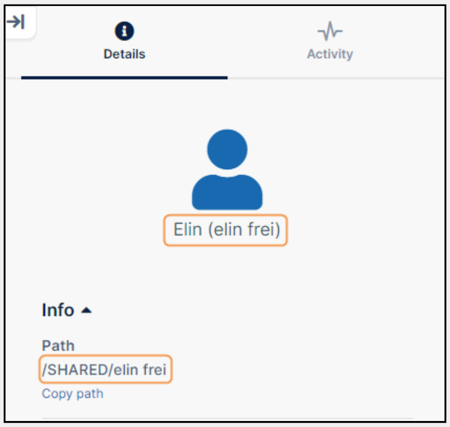
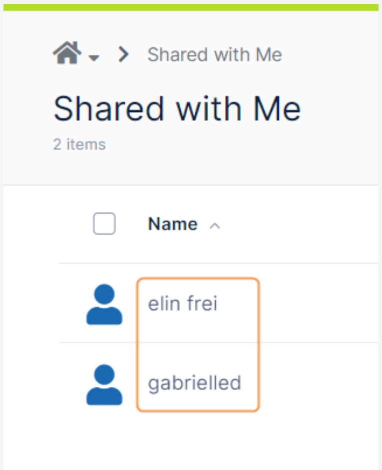
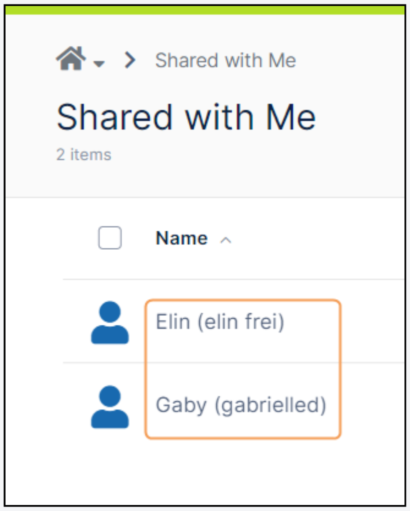
- In the User Portal, by default, FileCloud displays the User Name.
- It may not be clear to users who is sharing the file with them, especially if User Name includes only abbreviations and numbers.
- The User Name cannot be changed after the user has been created.

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	 Details Activity elin frei Info Path /SHARED/elin frei Copy path	 Details Activity Elin (elin frei) Info Path /SHARED/elin frei Copy path
Shared With Me list	 Shared with Me Shared with Me 2 items □ Name elin frei gabrielled	 Shared with Me Shared with Me 2 items □ Name Elin (elin frei) Gaby (gabrielled)

How to Change the Display of a User's Name in Sharing Details

Changing the display in sharing details requires you to edit the cloudconfig file and restart the server.

To change the default from User Name to Display Name in sharing details:

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

```
XAMPP DIRECTORY/htdocs/config/cloudconfig.php
```

For Linux

```
/var/www/config/cloudconfig.php
```

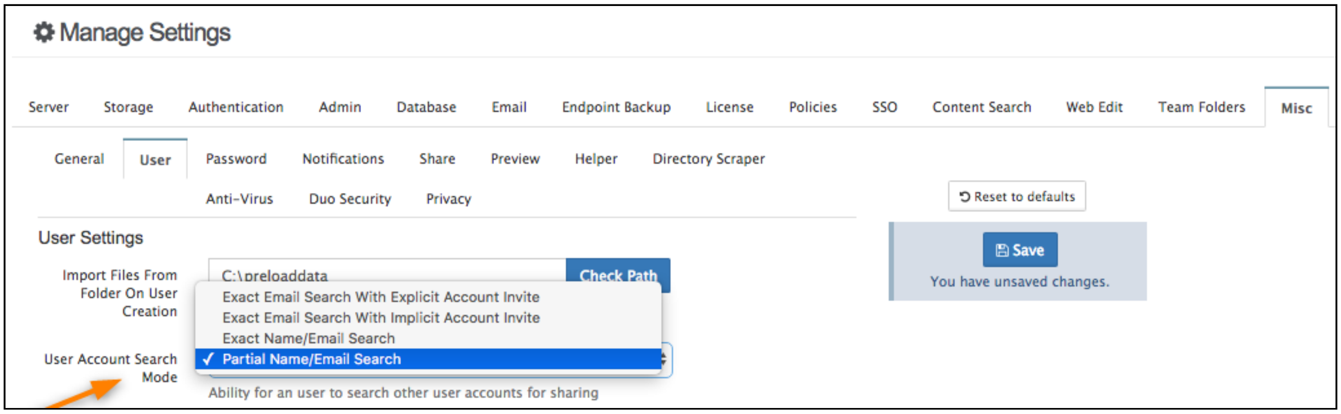
2. Add the following code to use the Display Name:

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

3. Save and close the file.
4. Restart the Apache server.

User Account Search Mode

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.



Import Files From Folder On User Creation: C:\preloaddata

User Account Search Mode:
- Exact Email Search With Explicit Account Invite
- Exact Email Search With Implicit Account Invite
- Exact Name/Email Search
- ✓ Partial Name/Email Search

Ability for an user to search other user accounts for sharing

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	• 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

Option	Example	When this search mode is set by admin, the following behavior will be seen during sharing by users:
Exact Email Search With Implicit Account Invite	JoeCarpenter@MyFileCloud.com	• Only email search is allowed • If the email doesn't exist in the system, then the system will send an invite to the entered email address without notifying the user • With this option, a user cannot figure out other users that exist in the system
Exact Name / Email Search	Joe Carpenter	• Both name and email search is allowed • No partial matches are allowed. • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the email doesn't exist in the system, the system will give the user option to invite the specified user
Partial Name / Email Search	Joe C	• Both name and email search is allowed • Partial matches are allowed • If the name doesn't exist in the system, the system will not give the user option to invite the specified user • If the searched email doesn't exist in the system, the system will give the user option to invite the specified user

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

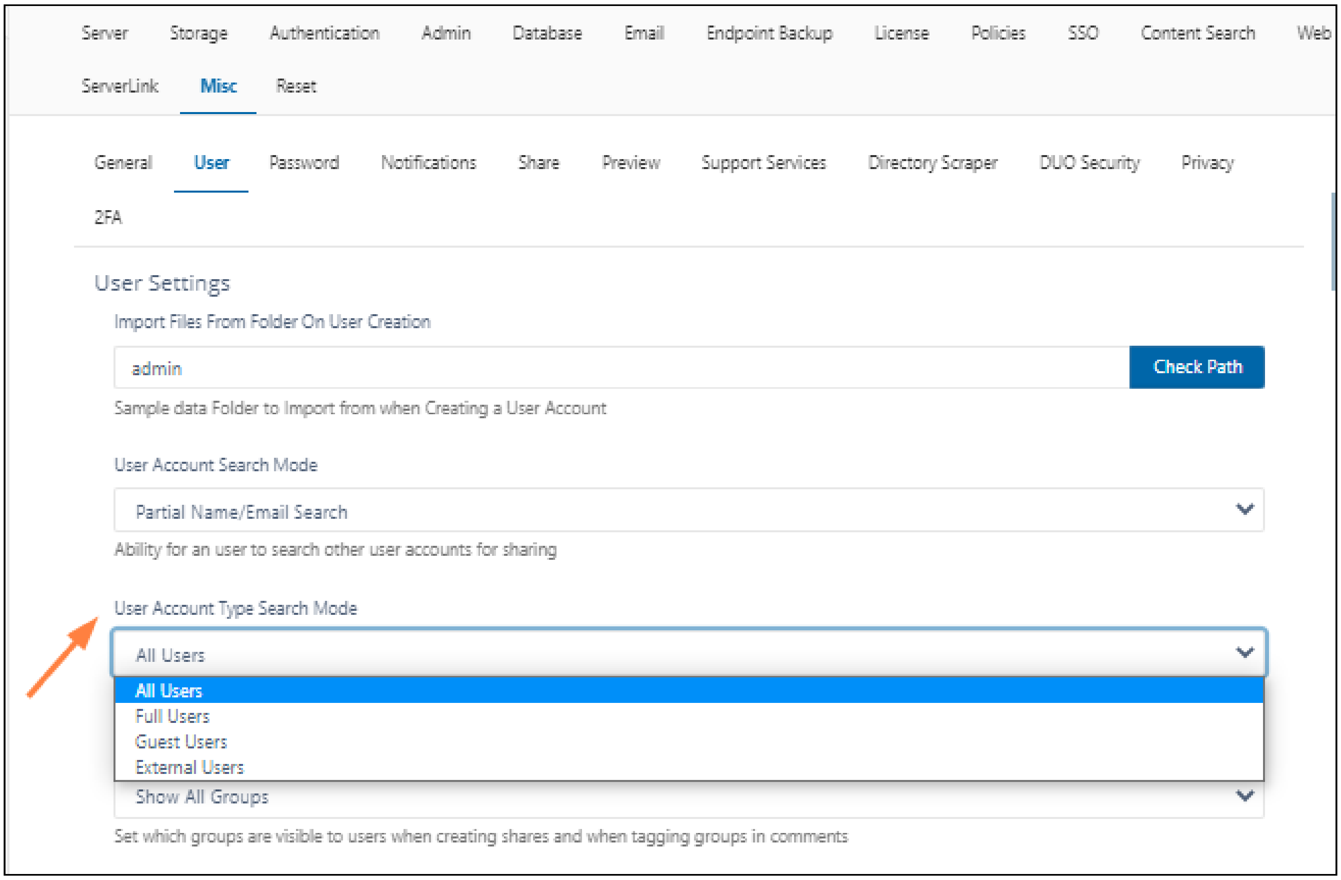
ⓘ The ability to limit searches of user accounts by account type to ALL, FULL, GUEST, or EXTERNAL is available in FileCloud version 19.1 and later.

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

User Account Type	Level of Access
FULL	An account with full access has its own private cloud storage space in the "My Files" area. These users can: • store files in their own private cloud storage space • view/download files stored in their storage space • view/download files shared with them by other user accounts
GUEST	An account with guest access level has restricted access to the FileCloud system. These user accounts do not have private cloud storage. These users can: • view/upload/download files shared to them by other user accounts • re-share content if they have permission
EXTERNAL	An account that can only be used to access the User Portal through a Web browser. External Accounts can: • view/upload/download content shared with them External Access accounts can only be local user accounts.

➡ For a complete list of features available to each account type, read User Account Types



User Settings

Import Files From Folder On User Creation

admin

Sample data Folder to Import from when Creating a User Account

User Account Search Mode

Partial Name/Email Search

Ability for an user to search other user accounts for sharing

User Account Type Search Mode

All Users

Show All Groups

Set which groups are visible to users when creating shares and when tagging groups in comments

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

ⓘ 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:

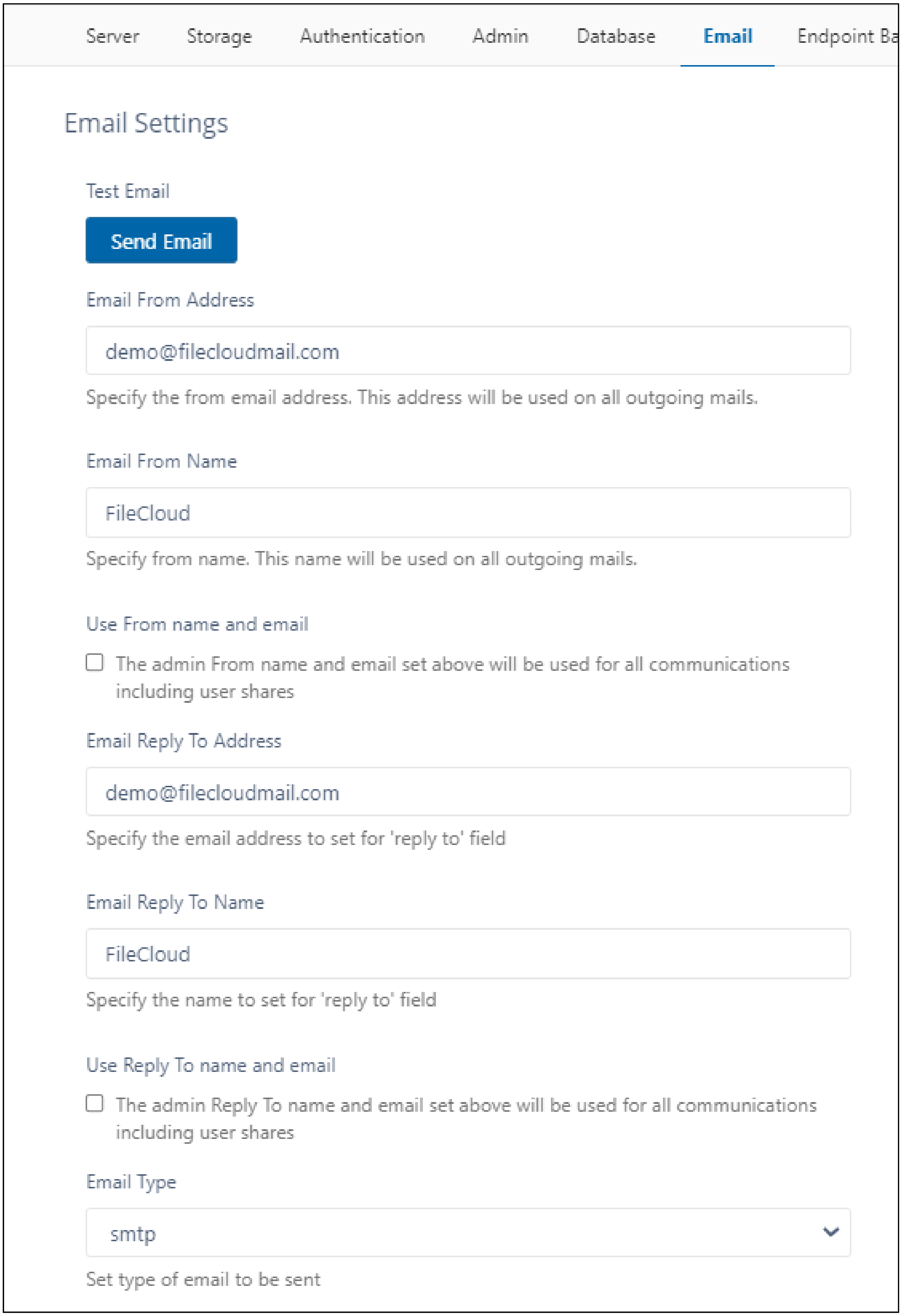
- share notifications
- file change notifications
- error notifications

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.



Email Settings

Test 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	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). ⓘ 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.
Email From Name	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).
Use From name and email	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.
Email Reply to Address	By default, **Email Reply To Address** is listed on emails if a reply to address does not exist (for example, when emails are sent by the system or by workflows).
Email Reply to Name	By default, **Email Reply To Name** is listed on emails when a recipient replies to an email without a reply to name (for example, when emails are sent from the system or by workflows).
Use Reply To name and email	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.
Email Type	Specify the email facility to be used. The type can be **SMTP**, **Mail** or **SendMail**. Note that **Mail** and **SendMail** use underlying OS's function (available only for Debian/Ubuntu installation). The recommended setting is **SMTP**.

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.

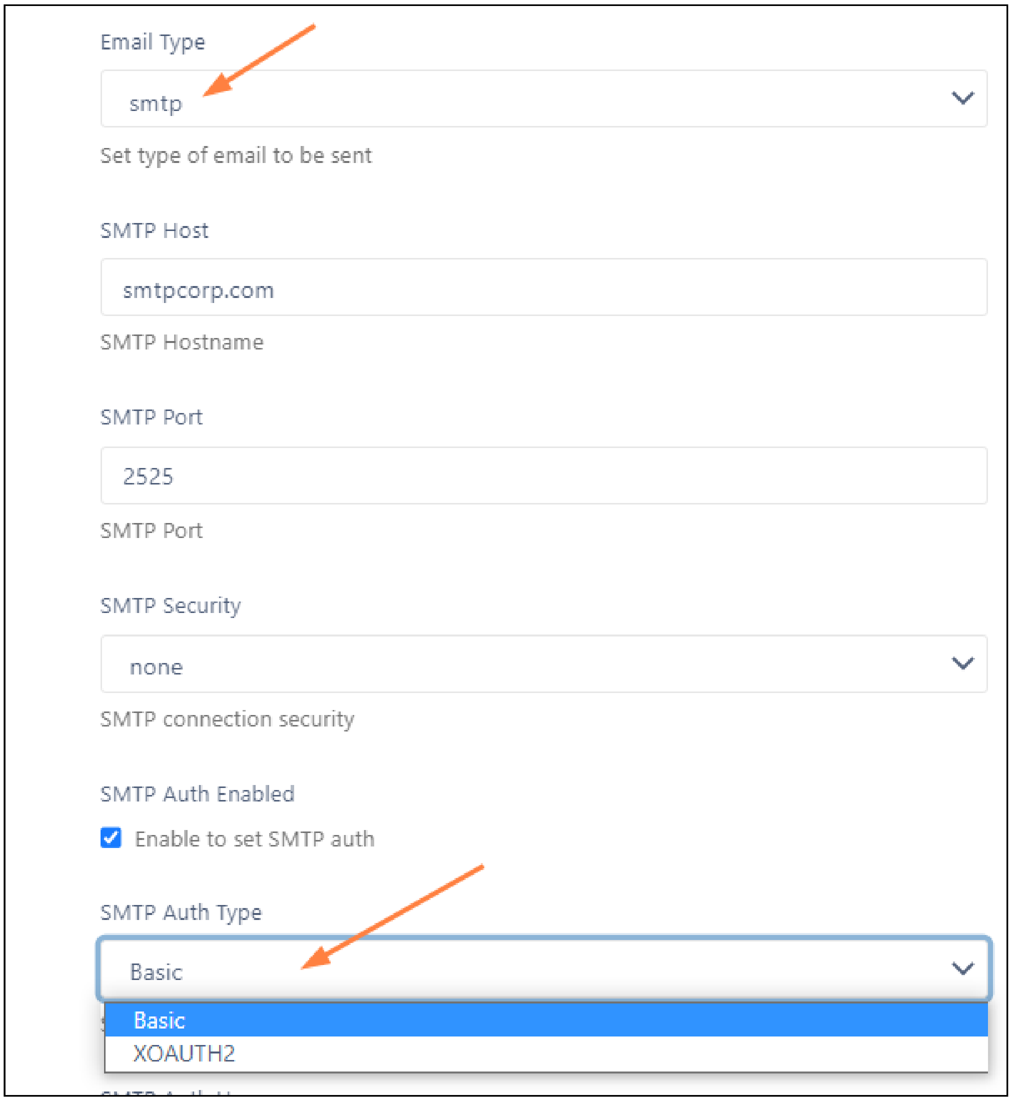
3. If you choose **SMTP** for **Email Type**, complete the following steps for filling in the SMTP fields. If you choose **Mail** or **SendMail** for **Email Type**, skip these steps, and go to Do Not Email Settings.

SMTP Configuration

Note: You must have an SMTP account to set up email using SMTP.

To configure SMTP in Email settings:

1. In **Email Type**, choose **SMTP**.
   The SMTP fields below it become enabled.



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

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	**SMTP Auth Type** may be **Basic** or **XOAUTH2**. The option you choose determines which additional SMTP fields follow. • **Basic** authentication requires the user to enter a username and password. It is supported by many email providers, but is being deprecated in Microsoft 365 in Exchange Online in early 2023. • **XOAUTH2** refers to OAuth 2.0 authentication, which uses temporary single-use tokens to provide a more secure method of verification. XOAUTH2 will now be used with Microsoft 365 for Exchange Online and is also the method used by a number of other providers.

If you choose **Basic** for **SMTP Auth Type**, enter values for the following fields:

Field	**Value to enter**
SMTP Auth User	Enter the authentication username.
SMTP Auth Password	Enter the password for SMTP Auth User.

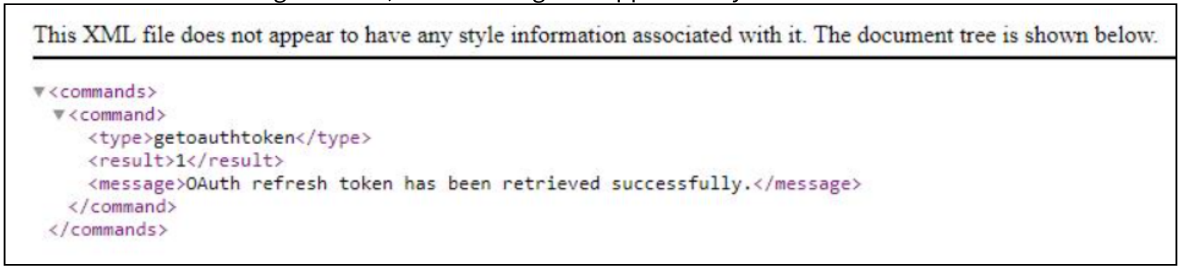
If you choose **XOAUTH2** for **SMTP Auth Type**:

a. 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.
b. 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.
c. Fill in the SMTP oAuth fields on the Email Settings page listed in the table below:

SMTP Auth User	Enter the authentication username ⓘ You must set **Email From Address** (described above under **General email setting configuration**) to the same value as **SMTP Auth User**. This is required for successful use of Azure as the authentication provider.

SMTP oAuth Provider	Choose the oAuth provider (authorization server). Currently, the only available option is **Azure**.
oAuth Client Secret	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.

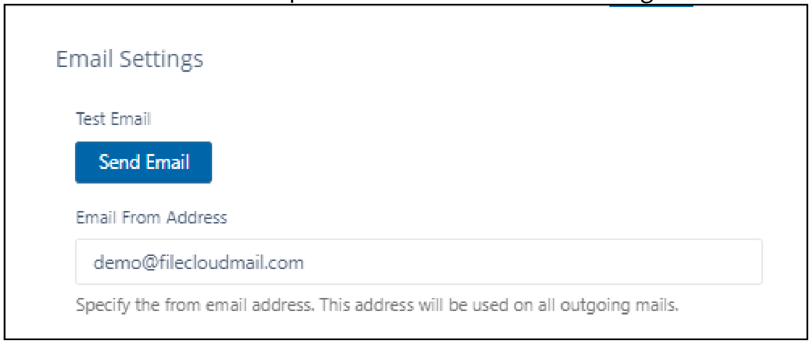
d. If your **SMTP Auth Type** is **XOAUTH2**, do the following:
After you have filled in the SMTP fields, click **Generate OAuth Token**.
If you are not logged in to your Microsoft authenticator app, you are prompted to log in so you can access Azure to generate the token.
Once the OAuth token is generated, 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.

```
▼<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

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.

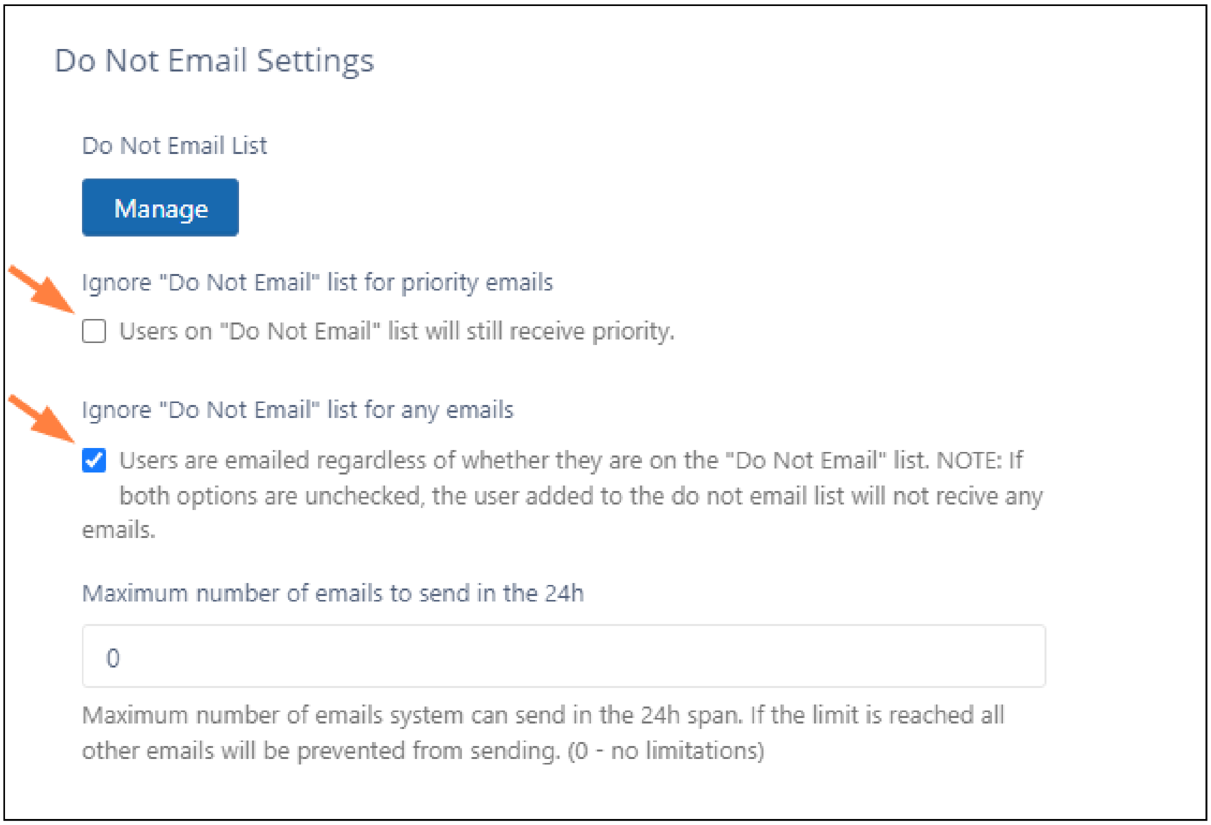
Do Not Email Settings

- 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

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 recive any emails.

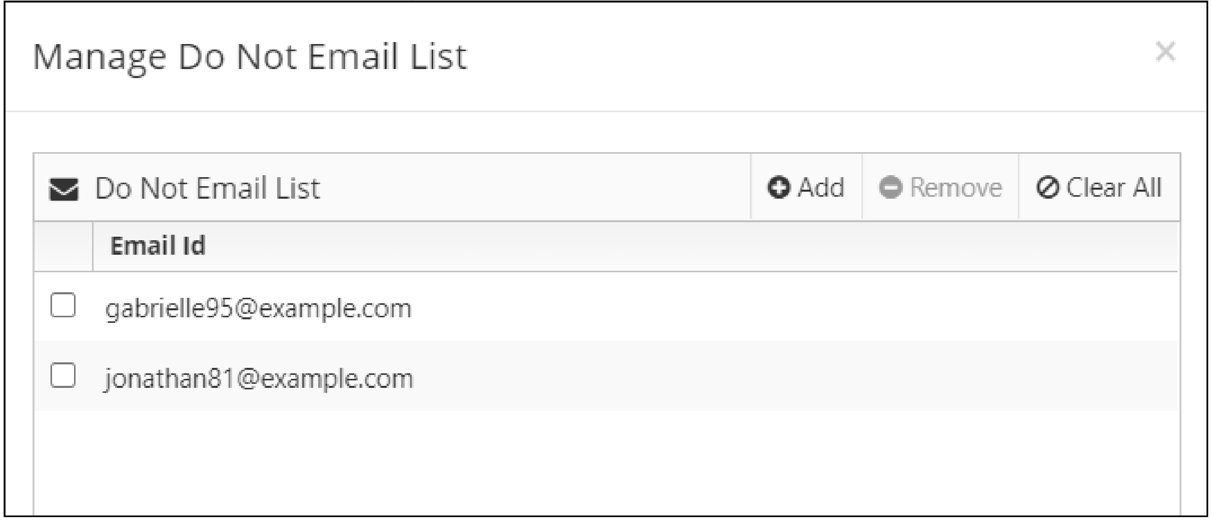
Maximum number of emails to send in the 24h

0

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:

1. Next to **Do Not Email List**, click **Manage**.
   The **Manage Do Not Email List** dialog box opens.



Manage Do Not Email List

	Email Id
☐	gabrielle95@example.com
☐	jonathan81@example.com

2. To add an email to the list, click **Add**, then enter and save an email address.
3. To remove an email from the list, check the box next to the email and click **Remove**.

Configuring System Generated Emails

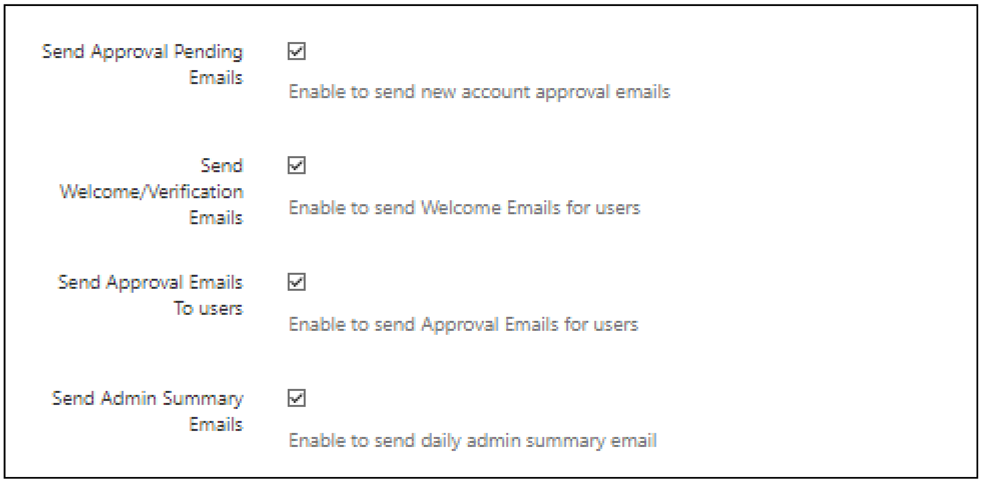
Controlling System Generated Automatic Emails

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 ☑ Enable to send new account approval emails

Send Welcome/Verification Emails ☑ Enable to send Welcome Emails for users

Send Approval Emails To users ☑ Enable to send Approval Emails for users

Send Admin Summary Emails ☑ Enable to send daily admin summary email

Change the frequency of Admin summary emails

By default, an Admin summary email is sent to the FileCloud Admin once per day. However, you can configure your system to send it weekly or monthly instead.

To change the frequency of Admin summary emails:

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

   ```
   define('TONIDOCLOUD_ADMIN_SUMMARY_EMAIL_FREQUENCY', 'DAILY');
   ```

3. Change the value of **DAILY** to **WEEKLY** or **MONTHLY**.

Endpoint Backup Settings

FileCloud lets you configure automatic backup settings for users' files and folders to ensure their data is secure.

Note: FileCloud supports backing up files and photos from different devices.

What Do You Want To Do?

Configure backup settings for all users

To configure the backed up settings for all users:

1. 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.

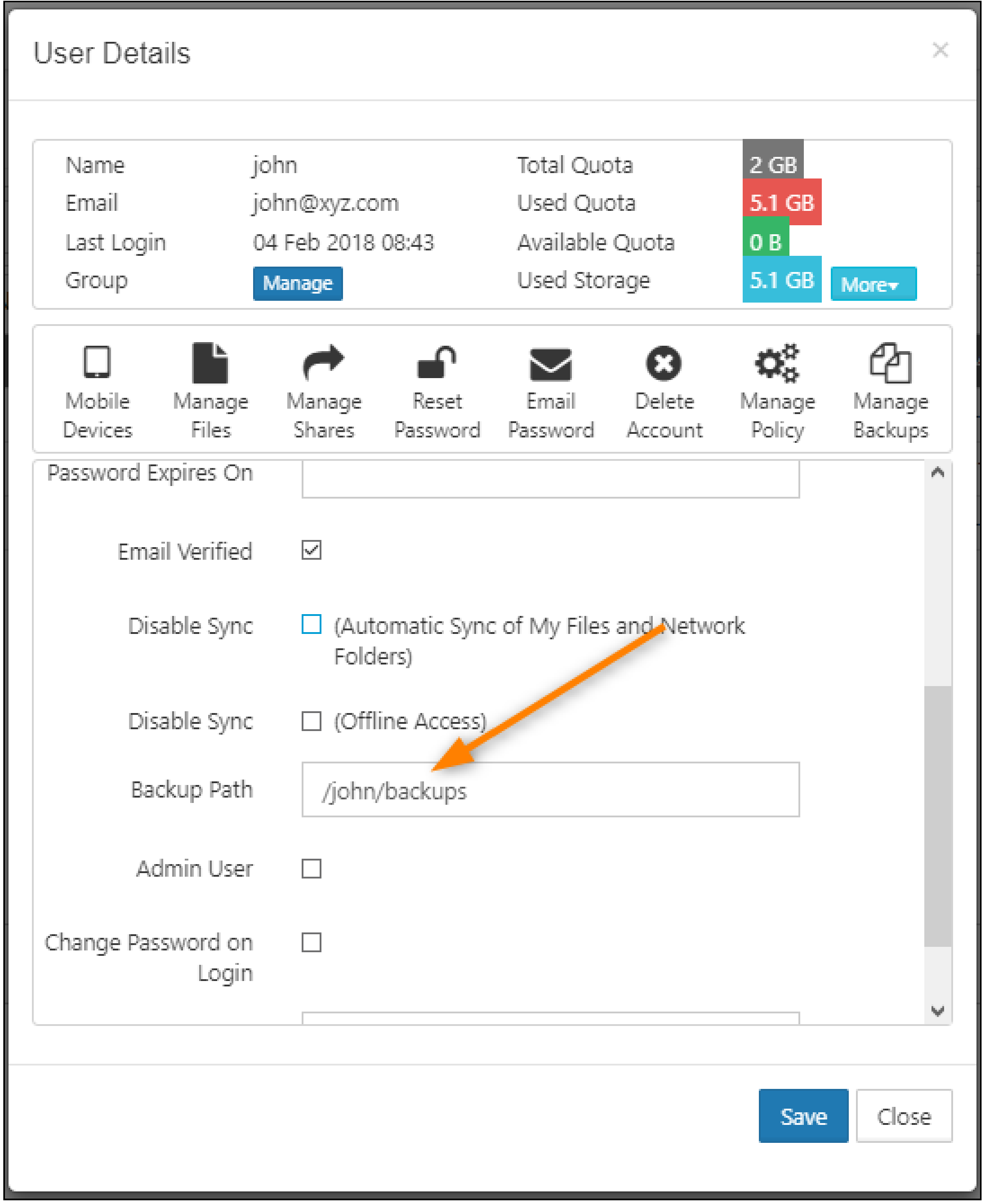
You must know the exact folder path you want to use.

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

Email john@xyz.com

Last Login 04 Feb 2018 08:43

Total Quota 2 GB

Used Quota 5.1 GB

Available Quota 0 B

Used Storage 5.1 GB

Password Expires On

Email Verified ☑

Disable Sync □ (Automatic Sync of My Files and Network Folders)

Disable Sync □ (Offline Access)

Backup Path /john/backups

Admin User □

Change Password on Login □

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
- Disabling Deletion of Backup Files

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.

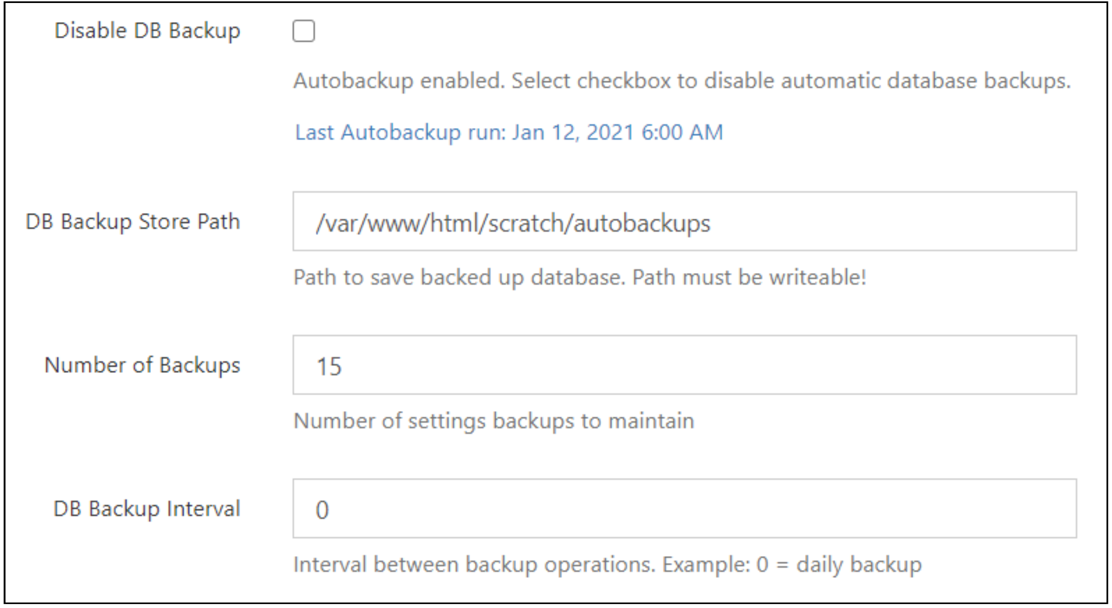
By default, automatic database backups are enabled with the following configuration:

- Daily backups are stored in the following directory: .../scratch/autobackups/
- Backups are maintained for the last 15 days before being overwritten with new backups

The auto backup function requires the Cron function to be working properly.
Cron is a requirement for FileCloud Server in general, so you should already have this service running.
If you have not done this yet, Set up Cron.

As an administrator, you can change the location where backups are stored, the number of backups to maintain, and the number of days between backups. Or, if you already have a back-up strategy, you can disable automatic backups.

Database Backup Options



Disable DB Backup □

Autobackup enabled. Select checkbox to disable automatic database backups.

Last Autobackup run: Jan 12, 2021 6:00 AM

DB Backup Store Path: /var/www/html/scratch/autobackups

Path to save backed up database. Path must be writeable!

Number of Backups: 15

Number of settings backups to maintain

DB Backup Interval: 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.

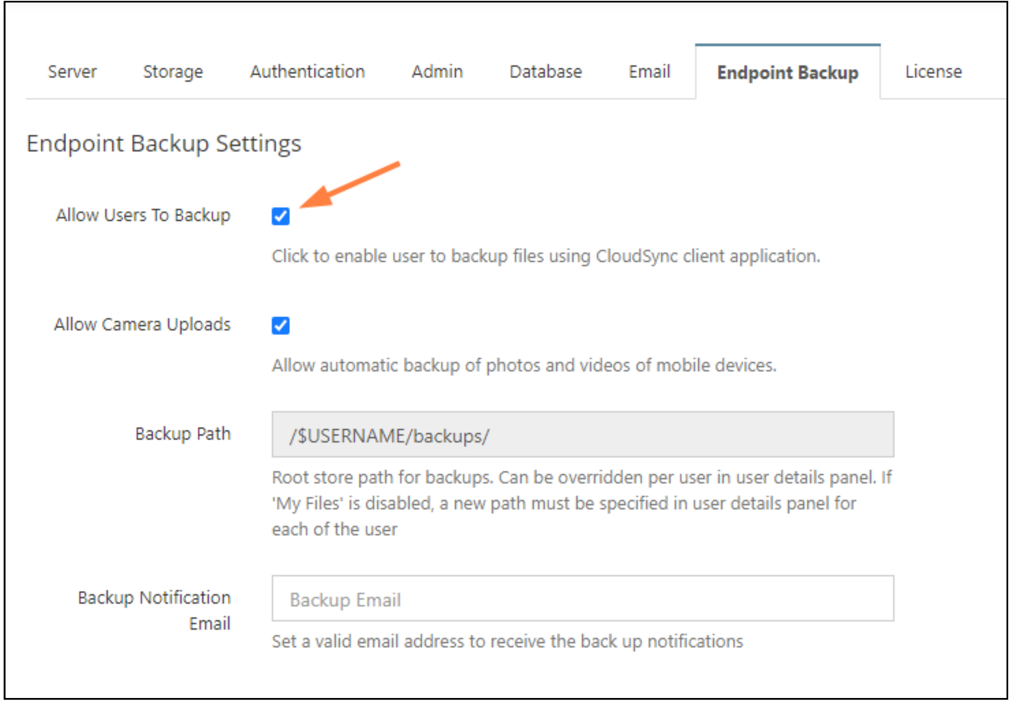
Steps:

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**.



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: /$USERNAME/backups/

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

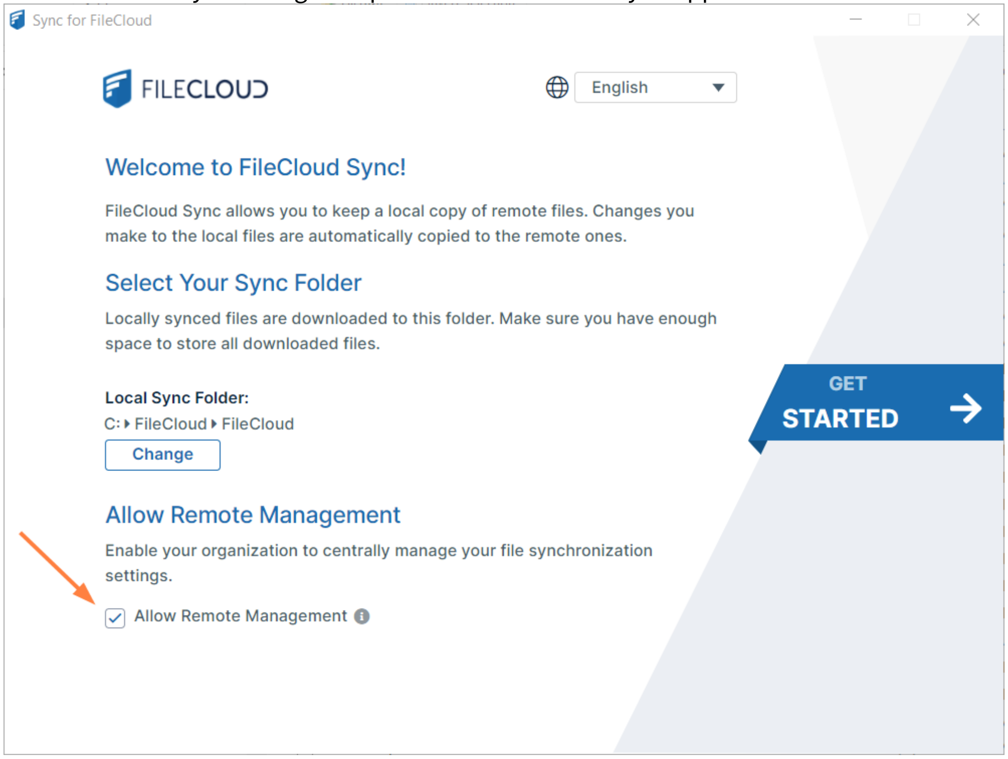
Backup Notification Email: Backup Email

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



Welcome to FileCloud Sync!

FileCloud Sync allows you to keep a local copy of remote files. Changes you make to the local files are automatically copied to the remote ones.

Select Your Sync Folder

Locally synced files are downloaded to this folder. Make sure you have enough space to store all downloaded files.

Local Sync Folder:
C: ▸ FileCloud ▸ FileCloud

Allow Remote Management

Enable your organization to centrally manage your file synchronization settings.

☑ Allow Remote Management

- On a Mass Deployment, an admin enabling remote management by setting the **allowcentralmgmt** parameter to **1**. This requires registry entries to be created before FileCloud Sync is initialized on the users' local machines.
  Note: If FileCloud Sync is initialized prior to the creation of registry keys in the users' local machines, the configuration to enable remote management will not take effect.

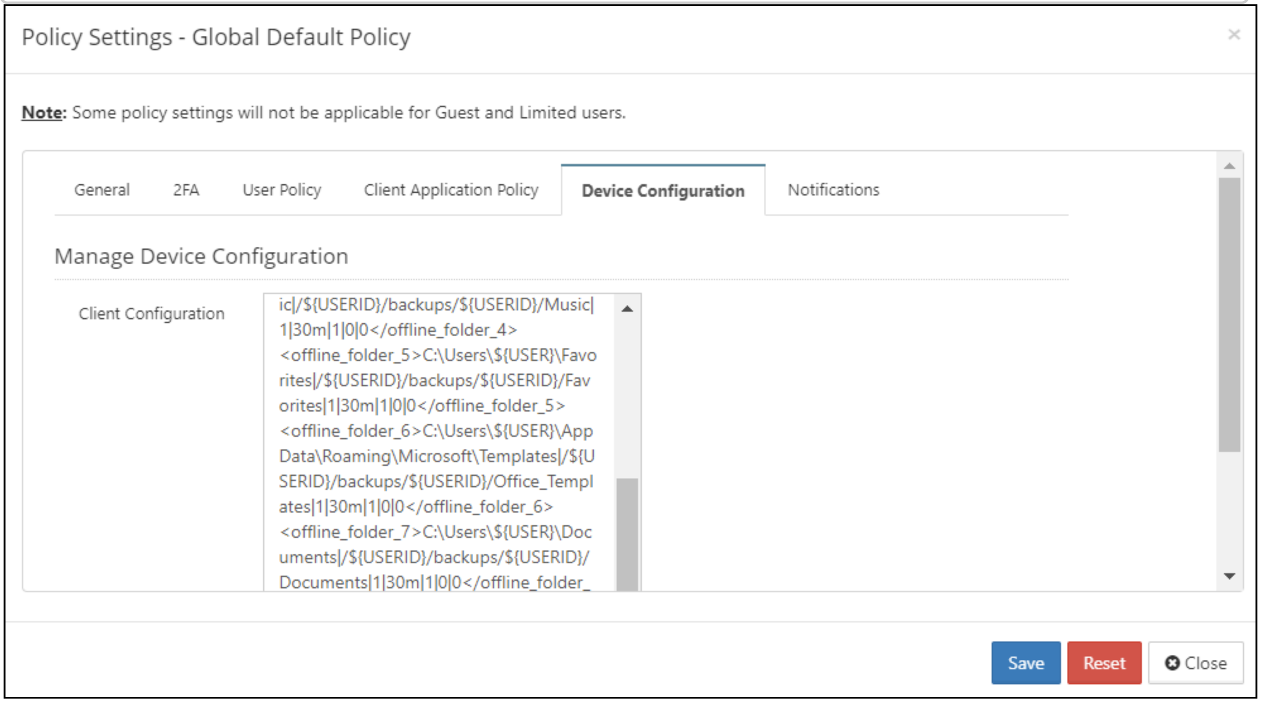
3) Set a default device configuration for Sync in the user's policy

Note: You must identify the local paths from the user’s computer to include in the Sync Backup before creating the device configuration XML. Refer to the Device Configuration XML documentation for Sync.

1. Log in to the admin portal.
2. Navigate to **Settings > Policies** and edit the users' policy.
3. Go to the **Device Configuration** tab and enter the configuration in XML format. Below is a sample script to use. The first parameter of the XML, **<offline_folder_1>**, is a local path in the user’s computer. The lines after it are the other local directories that must be included in the Sync Backup.

```
<xml>
<cloudsync>
<allowuserconfigforbackup>0</allowuserconfigforbackup>
<offline_folder_count>7</offline_folder_count>
<offline_folder_1>C:\Users\${USER}\AppData\Roaming\Microsoft\Outlook|/${USERID}/
backups/${USERID}/Outlook|1|30m|1|0|0</offline_folder_1>
```

```
<offline_folder_2>C:\Users\${USER}\Pictures|/${USERID}/backups/${USERID}/Pictures|
1|30m|1|0|0</offline_folder_2>
<offline_folder_3>C:\Users\${USER}\Desktop|/${USERID}/backups/${USERID}/Desktop|1|
30m|1|0|0</offline_folder_3>
<offline_folder_4>C:\Users\${USER}\Music|/${USERID}/backups/${USERID}/Music|1|30m|
1|0|0</offline_folder_4>
<offline_folder_5>C:\Users\${USER}\Favorites|/${USERID}/backups/${USERID}/
Favorites|1|30m|1|0|0</offline_folder_5>
<offline_folder_6>C:\Users\${USER}\AppData\Roaming\Microsoft\Templates|/${USERID}/
backups/${USERID}/Office_Templates|1|30m|1|0|0</offline_folder_6>
<offline_folder_7>C:\Users\${USER}\Documents|/${USERID}/backups/${USERID}/
Documents|1|30m|1|0|0</offline_folder_7>
</cloudsync>
</xml>
```



Policy Settings - Global Default Policy

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

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_
```

Disabling Deletion of Backup 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 prevent users from deleting backup files:

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

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

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

Client Security Settings

Two Factor Authentication

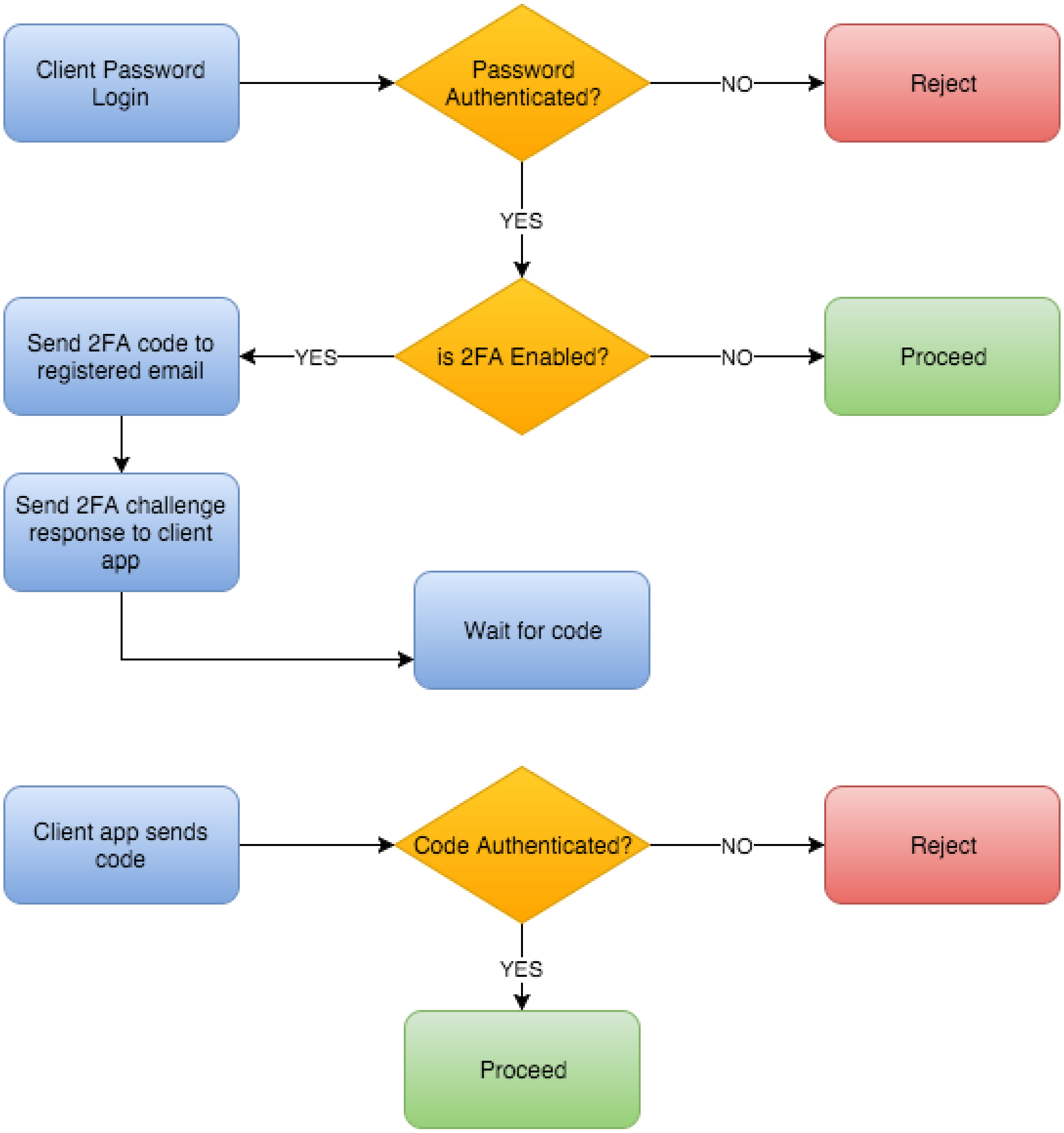
Two-factor authentication (2FA) refers to the two step verification process that is available in FileCloud and designed to provide an extra layer of security. With this function, in order to access FileCloud, the user is required to know not only the password and username but also an extra security code 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)

> 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.

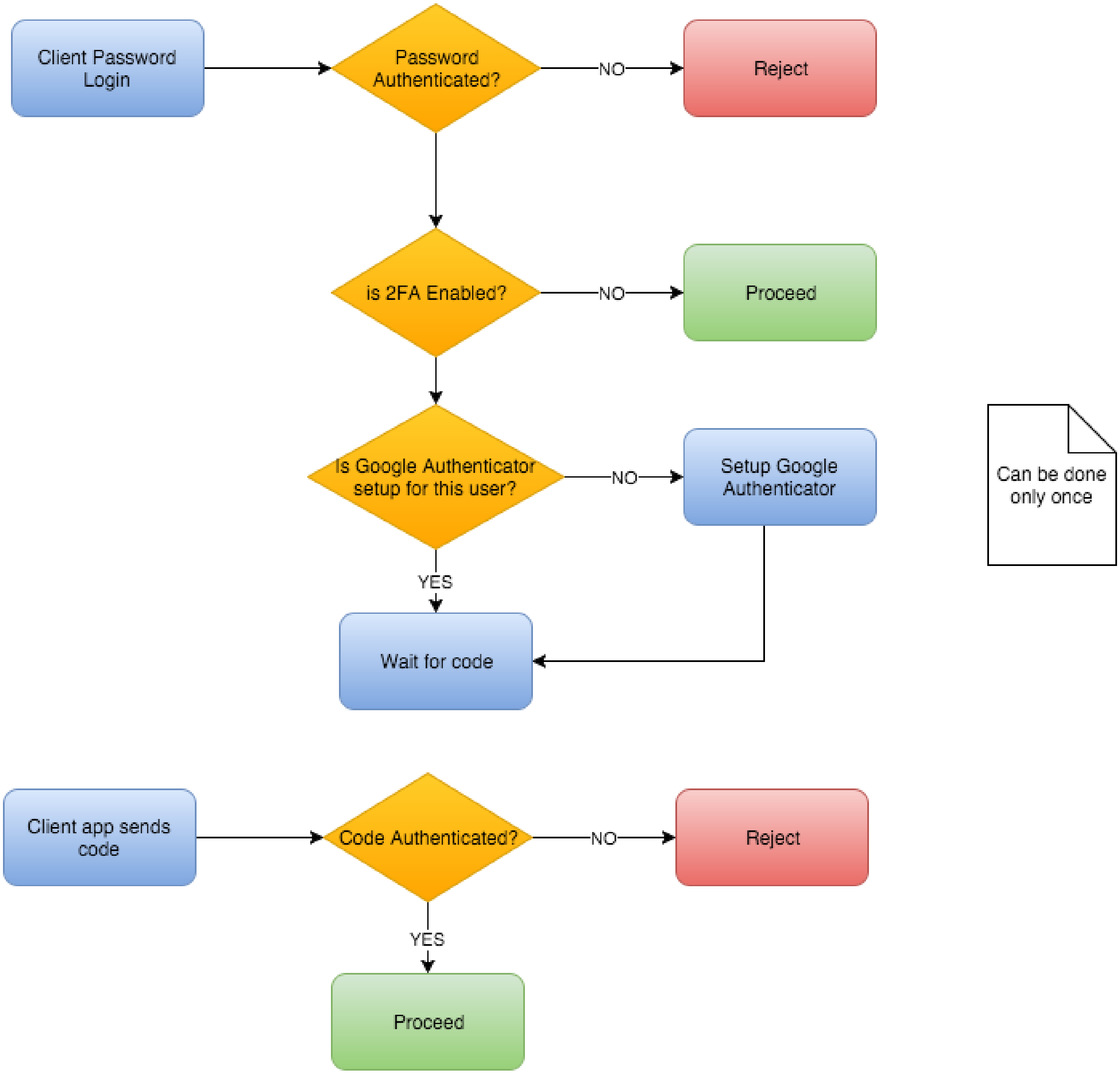
⚠ To set up 2FA with Google Authenticator, simply choose **TOTP (Authenticator App)** when configuring 2FA for the user portal. See Enable Two Factor Authentication for User Portal (Global setting), below, for help.
When the user logs in to the user portal for the first time, the user will be provided 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

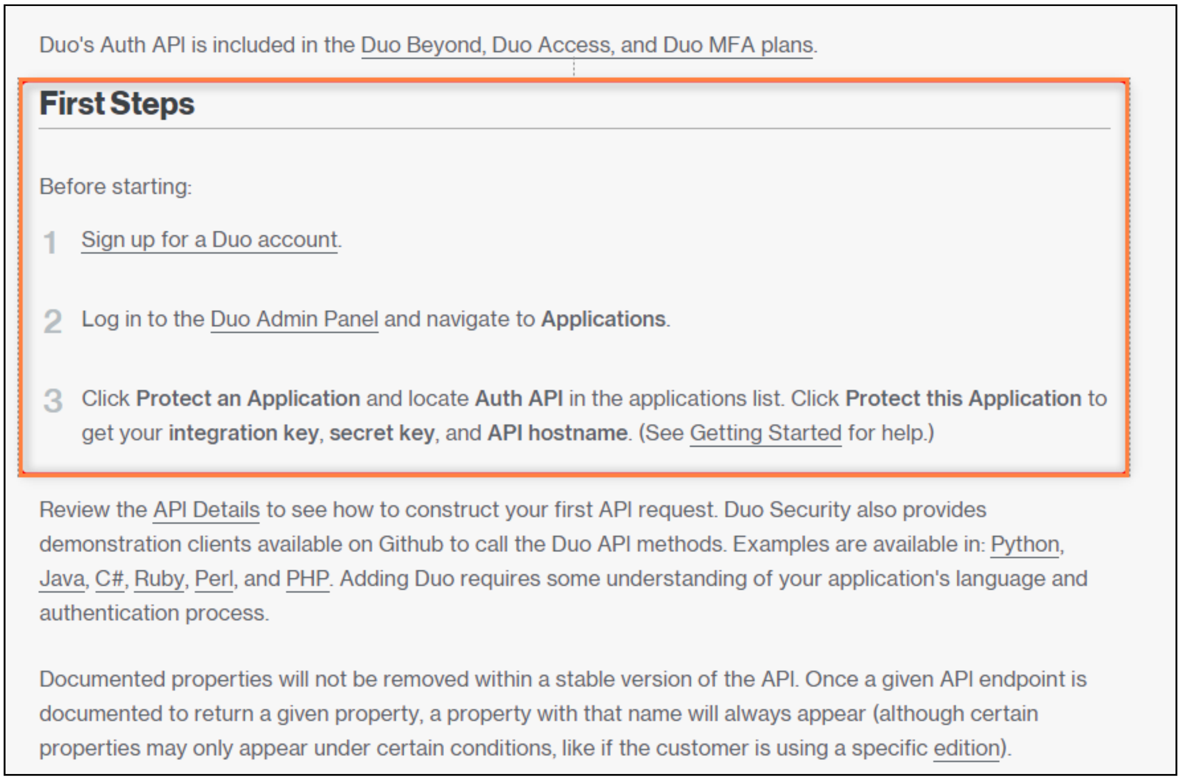


Two-factor authentication using DUO security

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

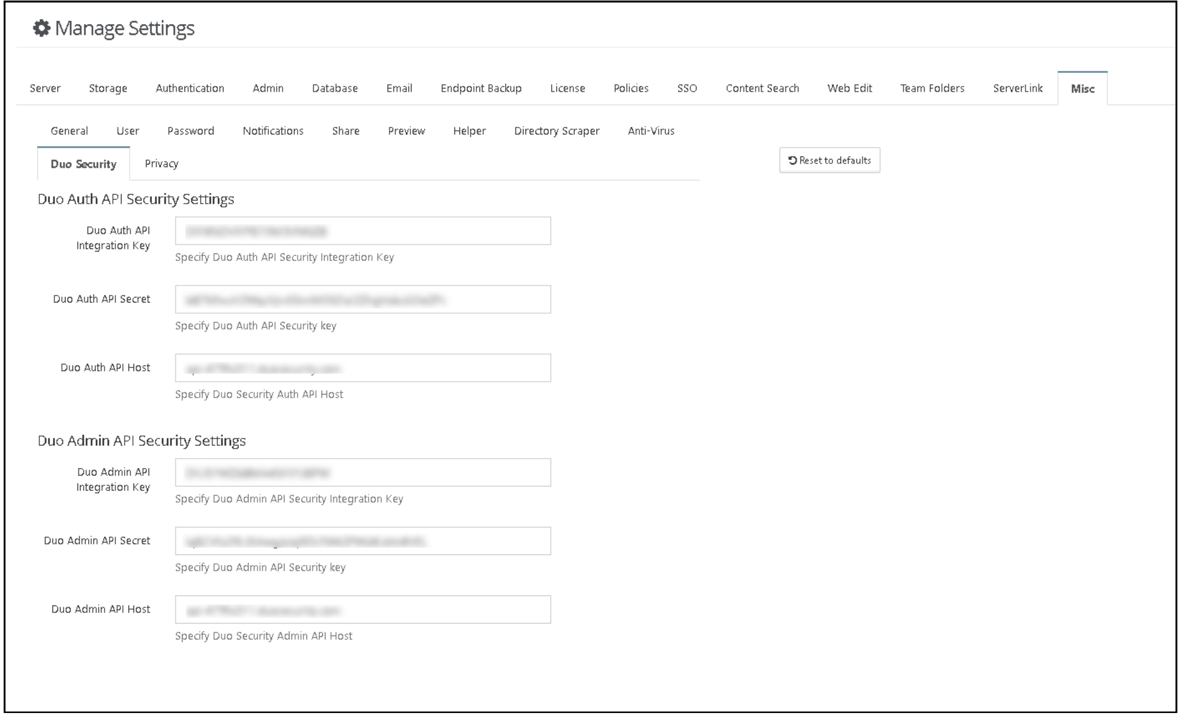
Before starting:

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.



Duo Auth API Security Settings

Duo Auth API Integration Key: [redacted]
Specify Duo Auth API Security Integration Key

Duo Auth API Secret: [redacted]
Specify Duo Auth API Security key

Duo Auth API Host: [redacted]
Specify Duo Security Auth API Host

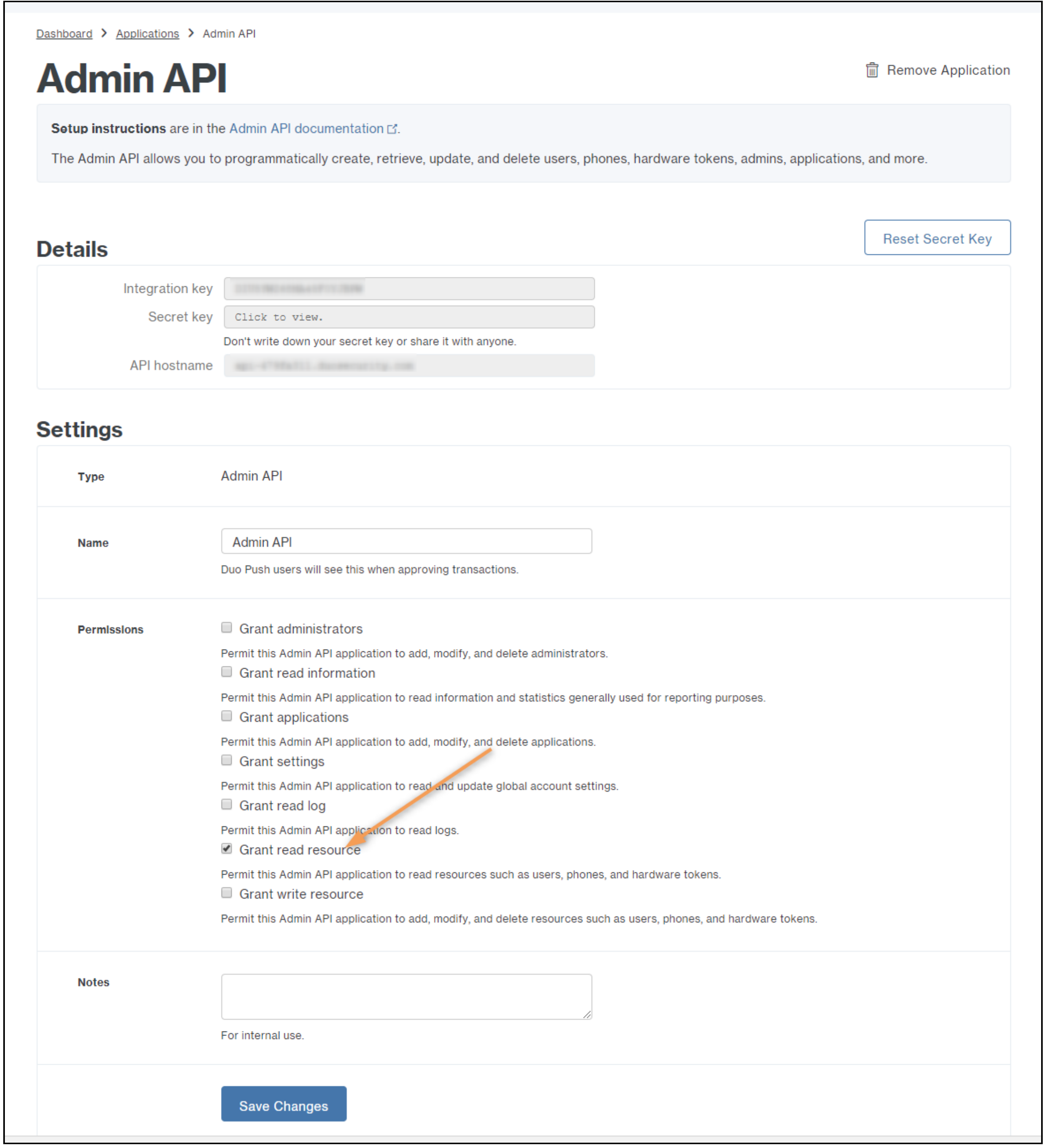
Duo Admin API Security Settings

Duo Admin API Integration Key: [redacted]
Specify Duo Admin API Security Integration Key

Duo Admin API Secret: [redacted]
Specify Duo Admin API Security key

Duo Admin API Host: [redacted]
Specify Duo Security Admin API Host

2. Add DUO Admin API
    - Follow instructions at https://duo.com/docs/adminapi to get values for **integration key**, **secret key**, and **API hostname**
    - Ensure it has **"Grant read resource"** permission.



Dashboard > Applications > Admin API

Admin API

Remove Application

Setup instructions are in the Admin API documentation.

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Reset Secret Key

Integration key: [redacted]

Secret key: Click to view.

Don't write down your secret key or share it with anyone.

API hostname: [redacted]

Settings

Type: Admin API

Name: Admin API

Duo Push users will see this when approving transactions.

Permissions

☐ Grant administrators

Permit this Admin API application to add, modify, and delete administrators.

☐ Grant read information

Permit this Admin API application to read information and statistics generally used for reporting purposes.

☐ Grant applications

Permit this Admin API application to add, modify, and delete applications.

☐ Grant settings

Permit this Admin API application to read and update global account settings.

☐ Grant read log

Permit this Admin API application to read logs.

☑ Grant read resource

Permit this Admin API application to read resources such as users, phones, and hardware tokens.

☐ Grant write resource

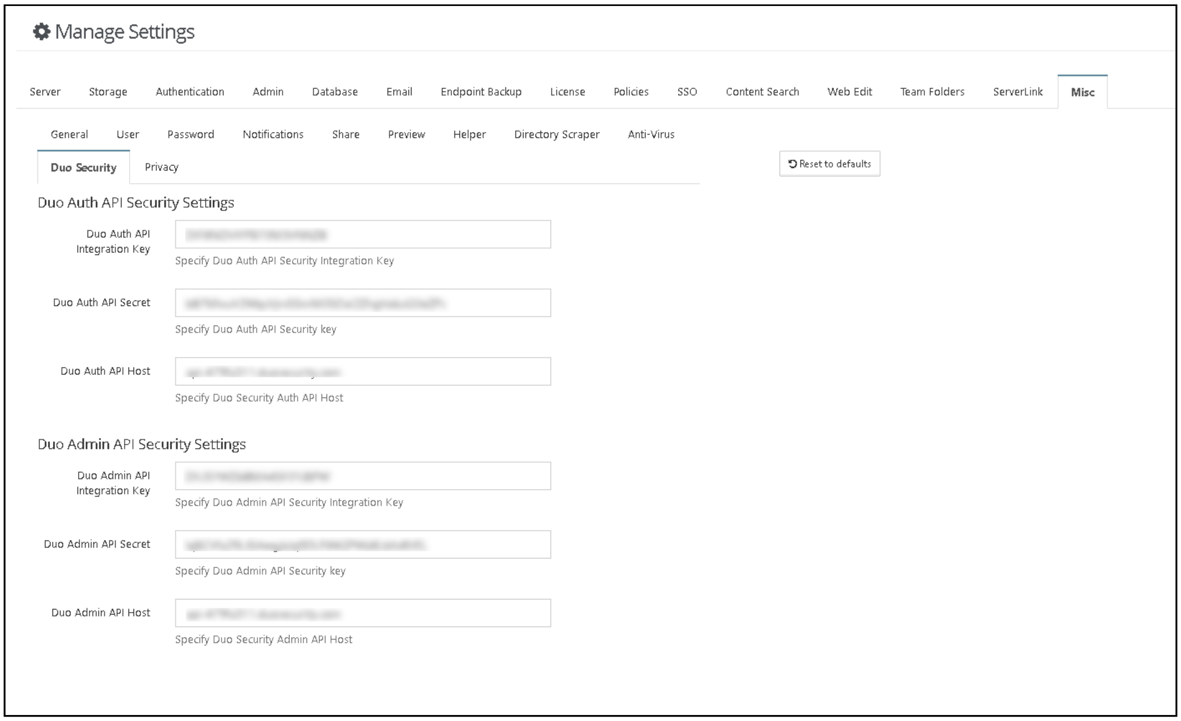
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

Notes

For internal use.

Save Changes

- In the Admin portal, enter the information in **Settings** > **Misc** > **Duo Security** under **Duo Admin API Security Settings**, and save.



Duo Auth API Security Settings

Duo Auth API Integration Key [redacted]
Specify Duo Auth API Security Integration Key

Duo Auth API Secret [redacted]
Specify Duo Auth API Security key

Duo Auth API Host [redacted]
Specify Duo Security Auth API Host

Duo Admin API Security Settings

Duo Admin API Integration Key [redacted]
Specify Duo Admin API Security Integration Key

Duo Admin API Secret [redacted]
Specify Duo Admin API Security key

Duo Admin API Host [redacted]
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.

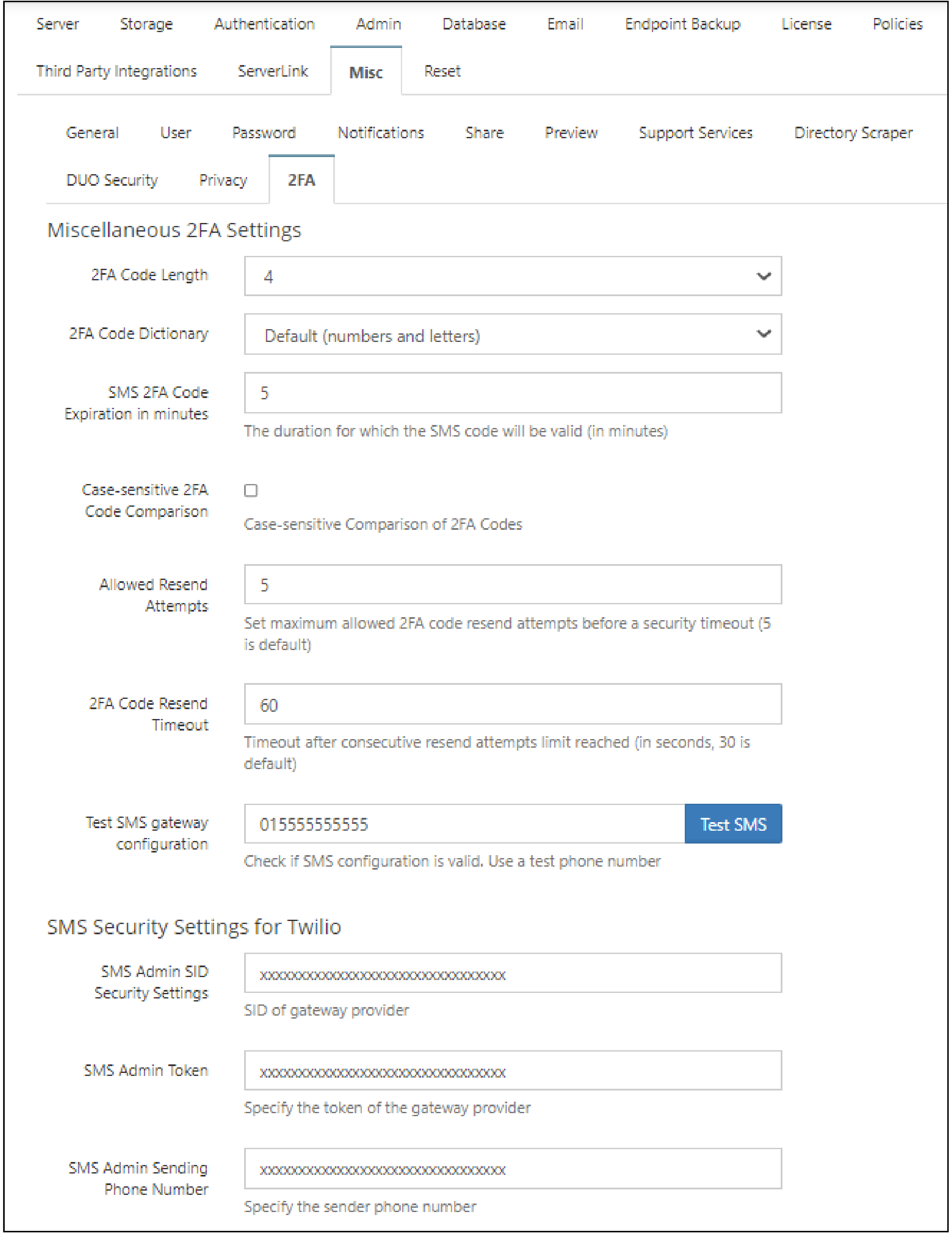
Sorry, the video is not supported in this export.
But you can reach it using the following URL:

Movie URL not available.

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**.



Miscellaneous 2FA Settings

2FA Code Length: 4

2FA Code Dictionary: Default (numbers and letters)

SMS 2FA Code Expiration in minutes: 5
The duration for which the SMS code will be valid (in minutes)

Case-sensitive 2FA Code Comparison: □
Case-sensitive Comparison of 2FA Codes

Allowed Resend Attempts: 5
Set maximum allowed 2FA code resend attempts before a security timeout (5 is default)

2FA Code Resend Timeout: 60
Timeout after consecutive resend attempts limit reached (in seconds, 30 is default)

Test SMS gateway configuration: 015555555555
Check if SMS configuration is valid. Use a test phone number

SMS Security Settings for Twilio

SMS Admin SID Security Settings: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
SID of gateway provider

SMS Admin Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Specify the token of the gateway provider

SMS Admin Sending Phone Number: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Specify the sender phone number

ⓘ 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:

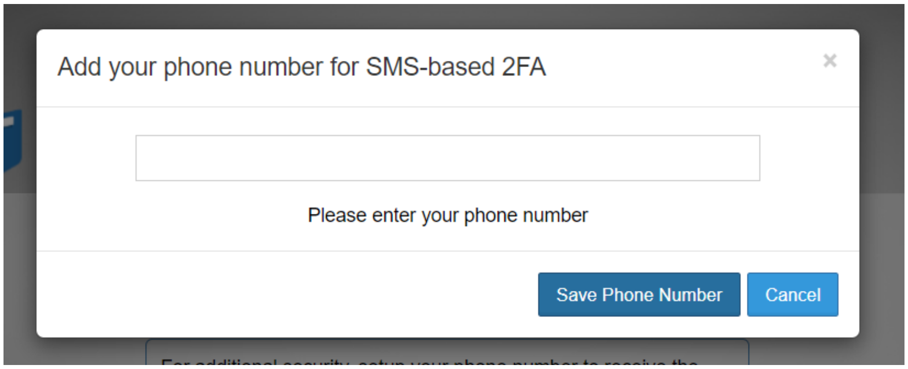
- Numbers and letters (default)
- Numbers
- Letters
- Uppercase letters

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.

ⓘ **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:



Add your phone number for SMS-based 2FA

Please enter your phone number

For additional security, setup your phone number to receive the

Enable Two-Factor Authentication using SMS OTP Security Codes for specific user agents

Starting with Version 19.3, FileCloud supports configuring two-factor authentication using SMS OTP for specific user agents. For example, you could apply this configuration to mobile clients only, or to FileCloud Drive, FileCloud Sync, and Microsoft Outlook only.

1. Complete the instructions above in Two Factor Authentication using SMS OTP Security Codes
2. Open cloudconfig.php at
    - Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
    - Linux: /var/www/config/cloudconfig.php
3. Add the following:

```
define("TONIDOCLOUD_TWOFA_REQUIRED_USERAGENT_LIST", "useragent1,useragent2, ... ");
```

4. Replace the *useragent* values with any number of user agents from the following list:
    - Web browser
    - Android
    - iOS
    - MS Outlook
    - MS Office
    - MS Office Online
    - Cloud Sync
    - Starting with Version 19.3 of FileCloud use: FileCloud Drive
      Prior to Version 19.3 of FileCloud use:
        FileCloudDrive or FileCloudDrive2
        FileCloud MacDrive or FileCloud MacDrive2
    - Any white labelled FileCloud Sync/Drive product name

For example:

```
define("TONIDOCLOUD_TWOFA_REQUIRED_USERAGENT_LIST", "Android,iOS");
```

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 **Polices** 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**.

Sorry, the video is not supported in this export.
But you can reach it using the following URL:

Movie URL not available.

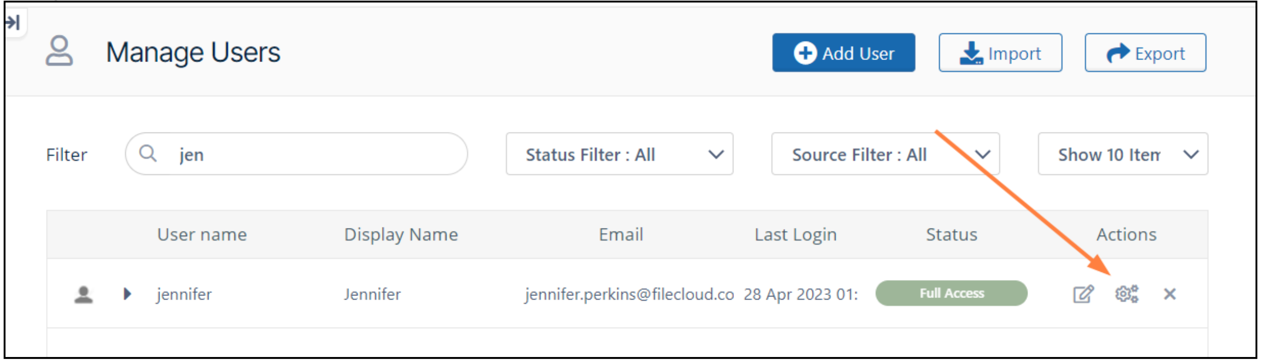
6. If you choose **SMS Security** and users are permitted to create accounts, add the following setting that enables users to add a phone number when creating a share with an external user:
   i. Open the configuration file:
      Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
      Linux: /var/www/config/cloudconfig.php
   ii. Add the line:

```
define ("TONIDOCLOUD_ENABLE_2FA_SMS_SHARE_INVITES", TRUE);
```

Reset TOTP or DUO settings for a user

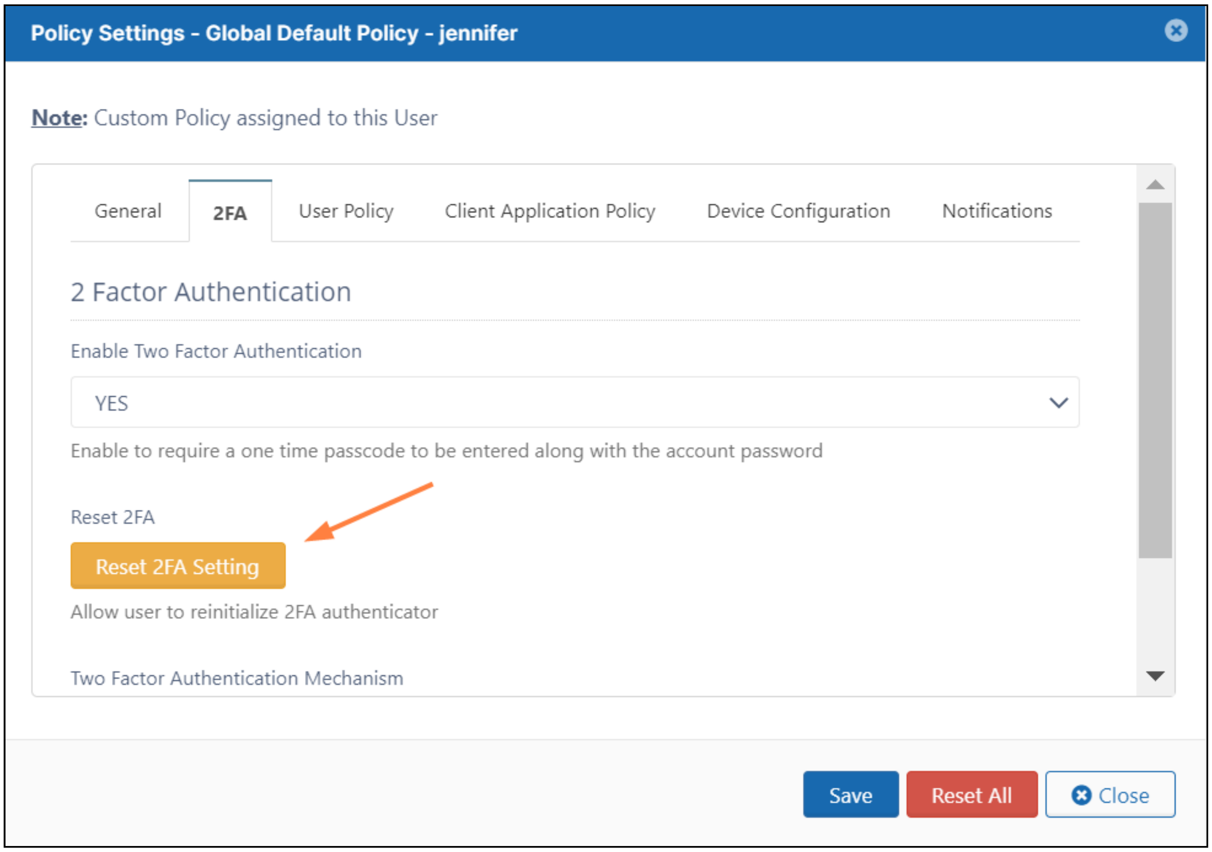
When a user loses a TOTP (Google Auth) app enabled device or if they need to reset the code for any reason, the Admin can reset the Google Authenticator setup for that user using the following steps

1. Login into the Admin portal
2. Navigate to **Users** and click the **Manage Policy** icon in the row for the user.



User name	Display Name	Email	Last Login	Status	Actions
jennifer	Jennifer	jennifer.perkins@filecloud.co	28 Apr 2023 01:	Full Access	

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

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

Allow user to reinitialize 2FA authenticator

Two Factor Authentication Mechanism

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

2FA Code validity: 10 minutes.

This can be changed by adding a key with a different timeout as shown (This key can be added <WEBROOT>/config/cloudconfig.php).
define ("TONIDOCLOUD_2FA_EMAIL_EXPIRATION_MINUTES", "5");
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.

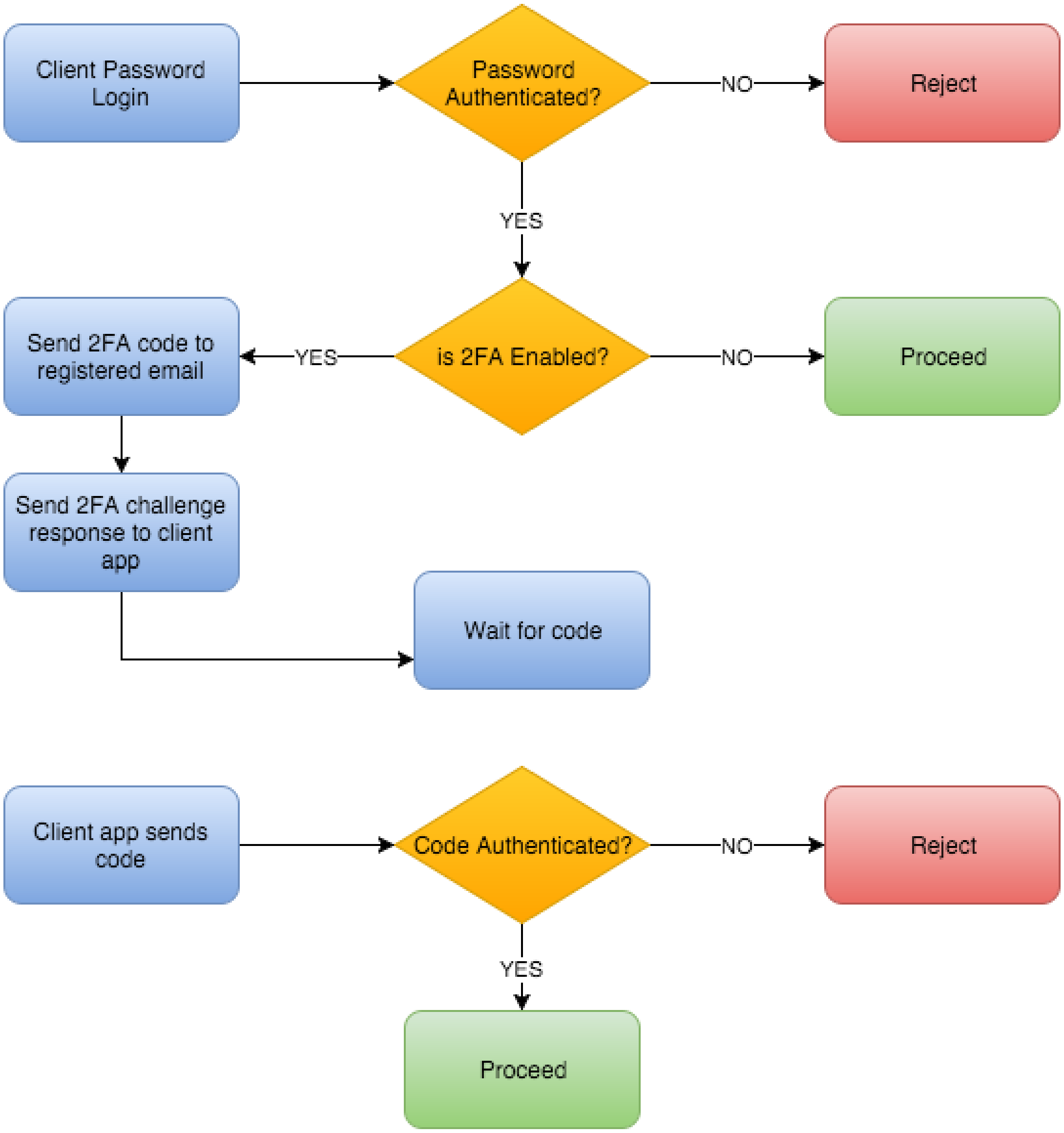
Two-Factor Authentication for Admin Portal

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.

> **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

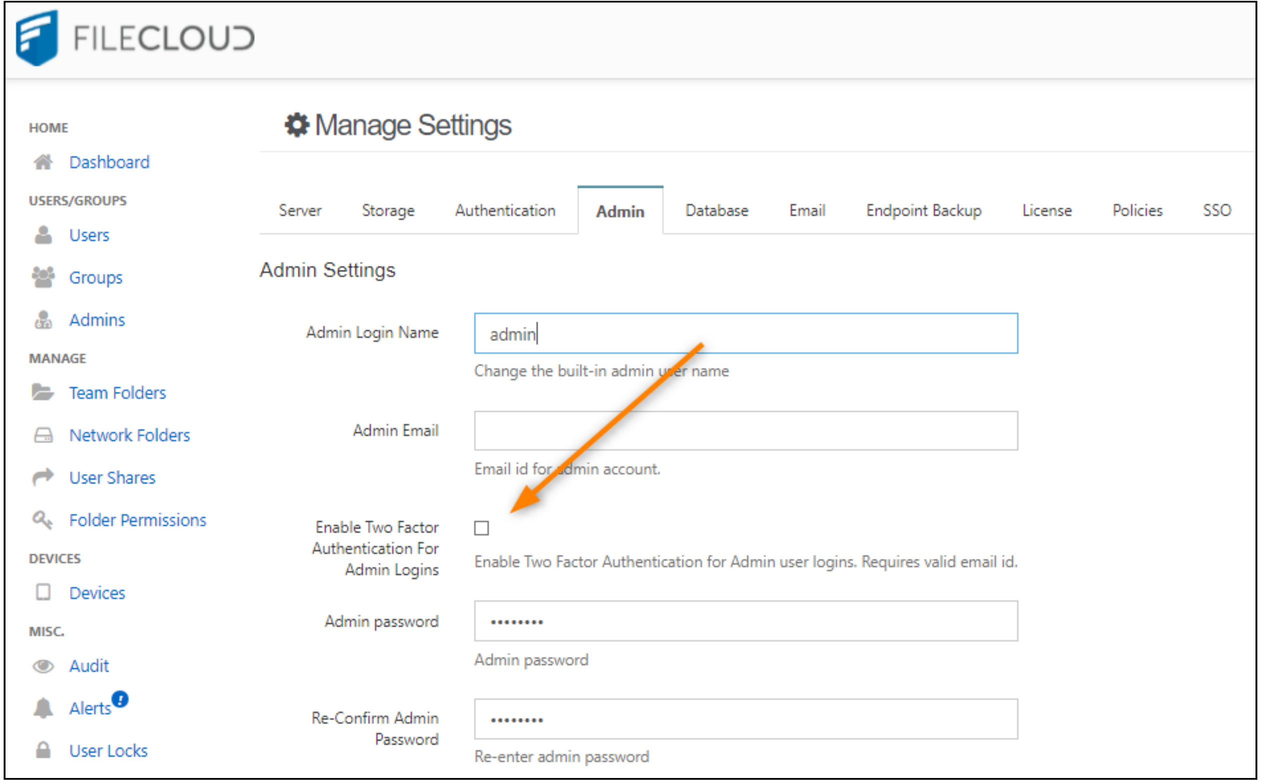


Enable Two Factor Authentication for Site Admin

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**.



Admin Settings

Admin Login Name: admin
Change the built-in admin user name

Admin Email:
Email id for admin account.

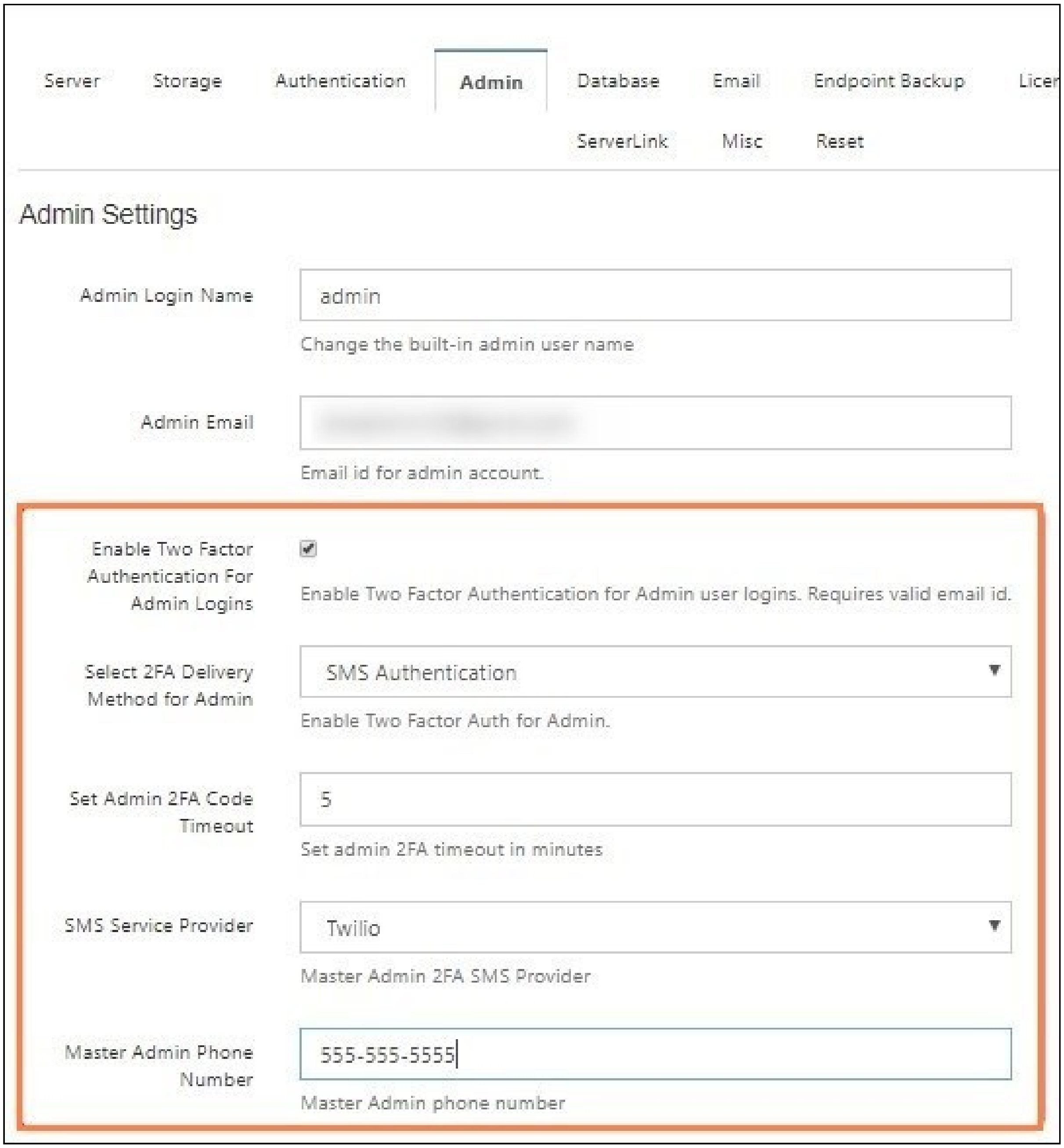
Enable Two Factor Authentication For Admin Logins: □
Enable Two Factor Authentication for Admin user logins. Requires valid email id.

Admin password: ••••••••
Admin password

Re-Confirm Admin Password: ••••••••
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.



Admin Settings

Admin Login Name: admin
Change the built-in admin user name

Admin Email: [redacted]
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: SMS Authentication ▼
Enable Two Factor Auth for Admin.

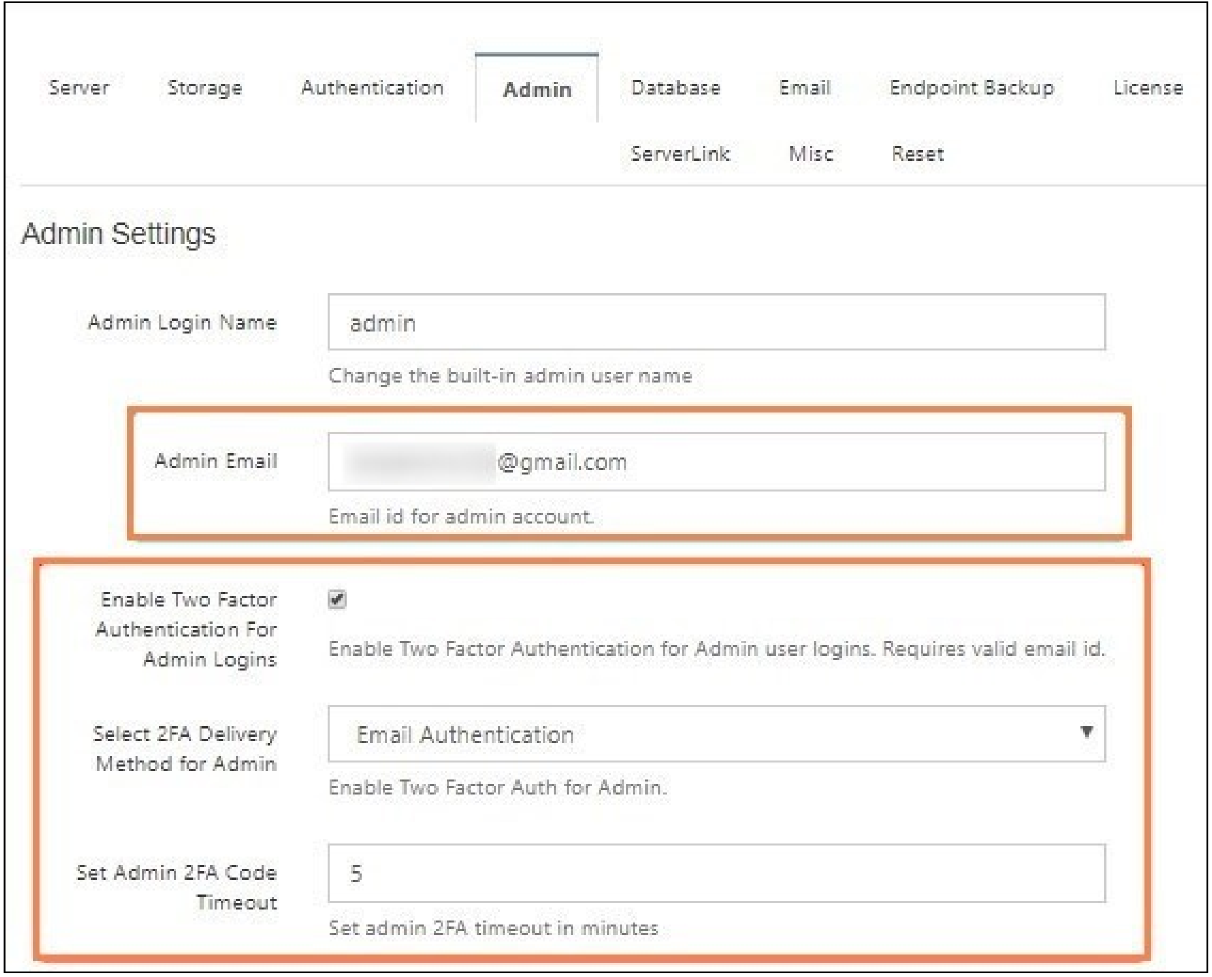
Set Admin 2FA Code Timeout: 5
Set admin 2FA timeout in minutes

SMS Service Provider: Twilio ▼
Master Admin 2FA SMS Provider

Master Admin Phone Number: 555-555-5555
Master Admin phone number

a. In **Set Admin 2FA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.
b. In **SMS Service Provider**, choose **Twilio** or **Custom**.
c. 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**..



Admin Settings

Admin Login Name: admin
Change the built-in admin user name

Admin Email: [redacted]@gmail.com
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: Email Authentication ▼
Enable Two Factor Auth for Admin.

Set Admin 2FA Code Timeout: 5
Set admin 2FA timeout in minutes

   a. Enter a valid email in the **Enable Two Factor Authentication for Admin Logins** field, above the Enable
   b. In **Set Admin 2FA Code Timeout,** set the time in minutes that you want the temporary log-in code to remain valid.

Enable Two-Factor Authentication for Super Admin for Multi-tenancy control panel access

From FileCloud v12 onwards, superadmin logins can be required to use 2FA to access the Multi-tenancy control panel.

Open "multi.php" (In ubuntu it is at /var/www/config/ and in Windows it is typically at c:\xampp\htdocs\config)

Add the lines:

```
define ("TONIDOCLOUD_SUPER_ADMIN_EMAIL_ID", "email@company.com");
define ("TONIDOCLOUD_ENABLE_SUPER_ADMIN_2FA","1");
```

In case the lines are commented "//", please remove the double slash symbol at the beginning of the line and save the changes.

Note that you need to provide valid email . If the email is invalid, then the Multi-tenancy control panel cannot be accessed.

Preventing an attacker from bypassing 2fa

Beginning in FileCloud 20.1, FileCloud only allows a user to set their phone number once. Once the phone number has been added, the user must contact their admin to change it. This prevents an attacker from obtaining a user name and password and then modifying the user's phone number to bypass two-factor authentication (2fa). It also prevents an attacker who has obtained the original phone number from restoring it to prevent the user from realizing there has been an attack.

To enable a user to only set their phone number once, the following setting appears in the config file:

```
define("TONIDOCLOUD_ENABLE_USER_SET2FASMS", 1);
```

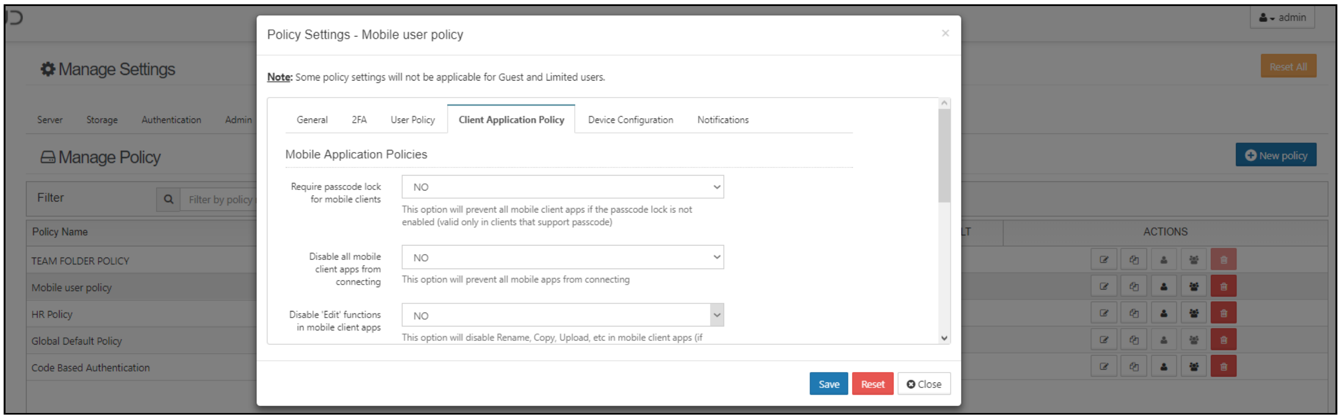
To require users to contact their admin to set their phone number initially and to change it,
set TONIDOCLOUD_ENABLE_USER_SET2FASMS to 0:

```
define("TONIDOCLOUD_ENABLE_USER_SET2FASMS", 0);
```

In addition, to prevent an attacker from gaining access with another user's token, if a token is invalid, the system clears it and requires the user to sign in again.

Setting Client Application Policies

FileCloud allows customizing the client application (Mobile clients, Sync Clients, Drive client) policies.



Policy Settings - Mobile user policy

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

Mobile Application Policies

Require passcode lock for mobile clients: NO
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: NO
This option will prevent all mobile apps from connecting

Disable 'Edit' functions in mobile client apps: NO
This option will disable Rename, Copy, Upload, etc in mobile client apps (if

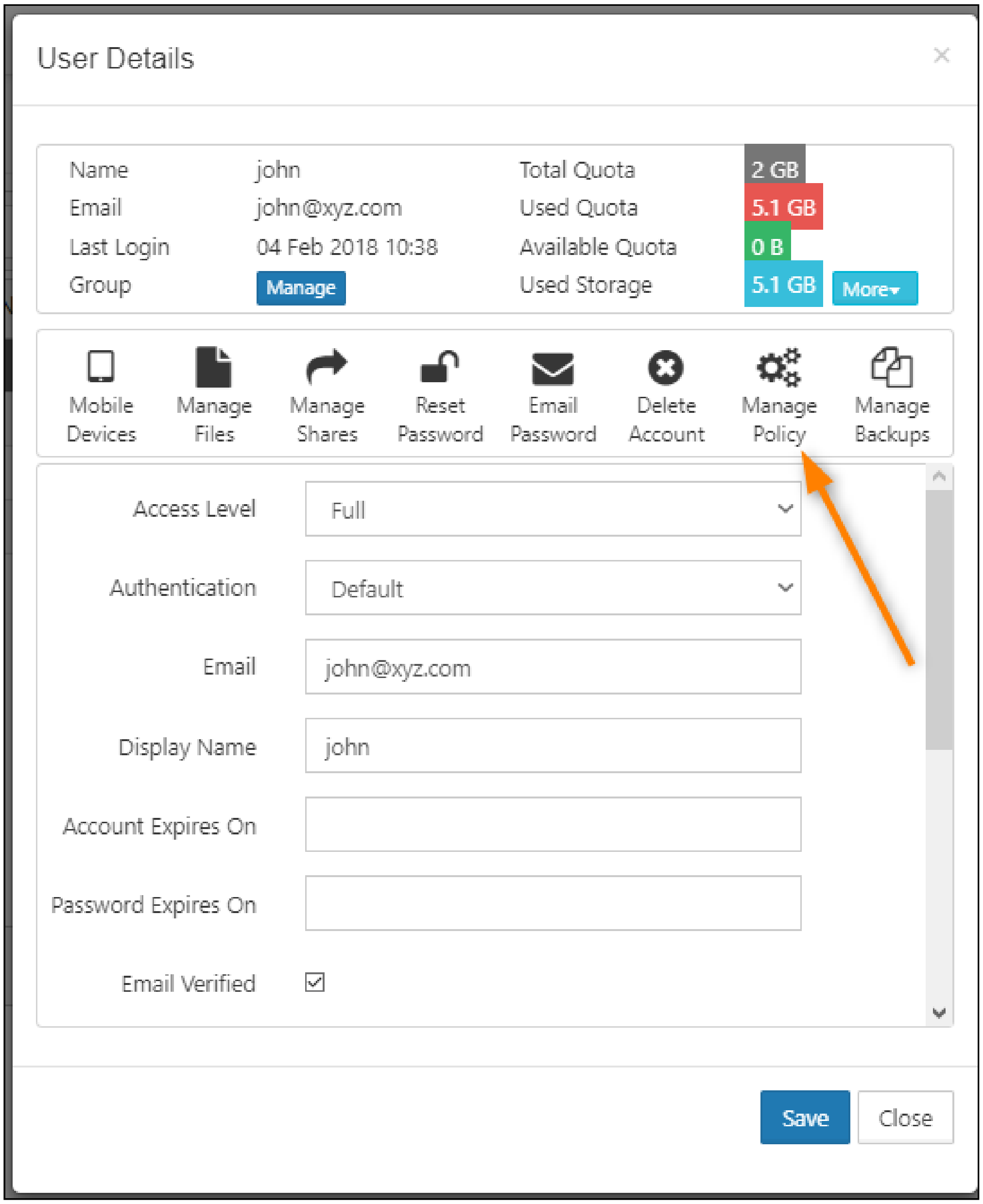
FileCloud allows setting global policies that will be applied to all users. But, these policies can be overridden for specific user.

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.
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,

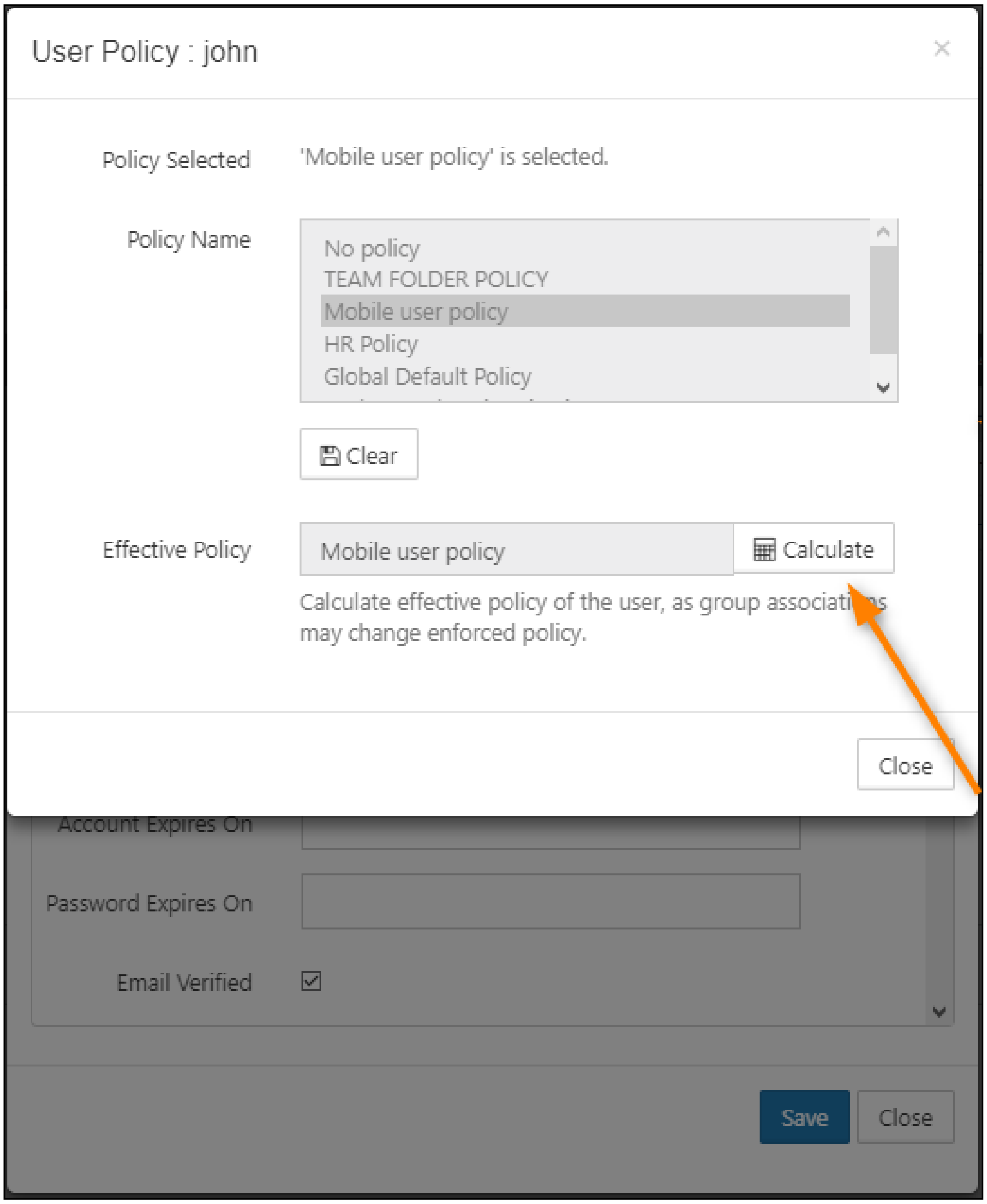
- Go to "**Users**" panel in Admin Portal
- Locate the user record (using Filter Users)
- Click on "**Edit**"
- Click on "**Manage Policy**"
- Change the appropriate policy to override



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

Access Level	Full
Authentication	Default
Email	john@xyz.com
Display Name	john
Account Expires On	
Password Expires On	
Email Verified	☑



User Policy : john

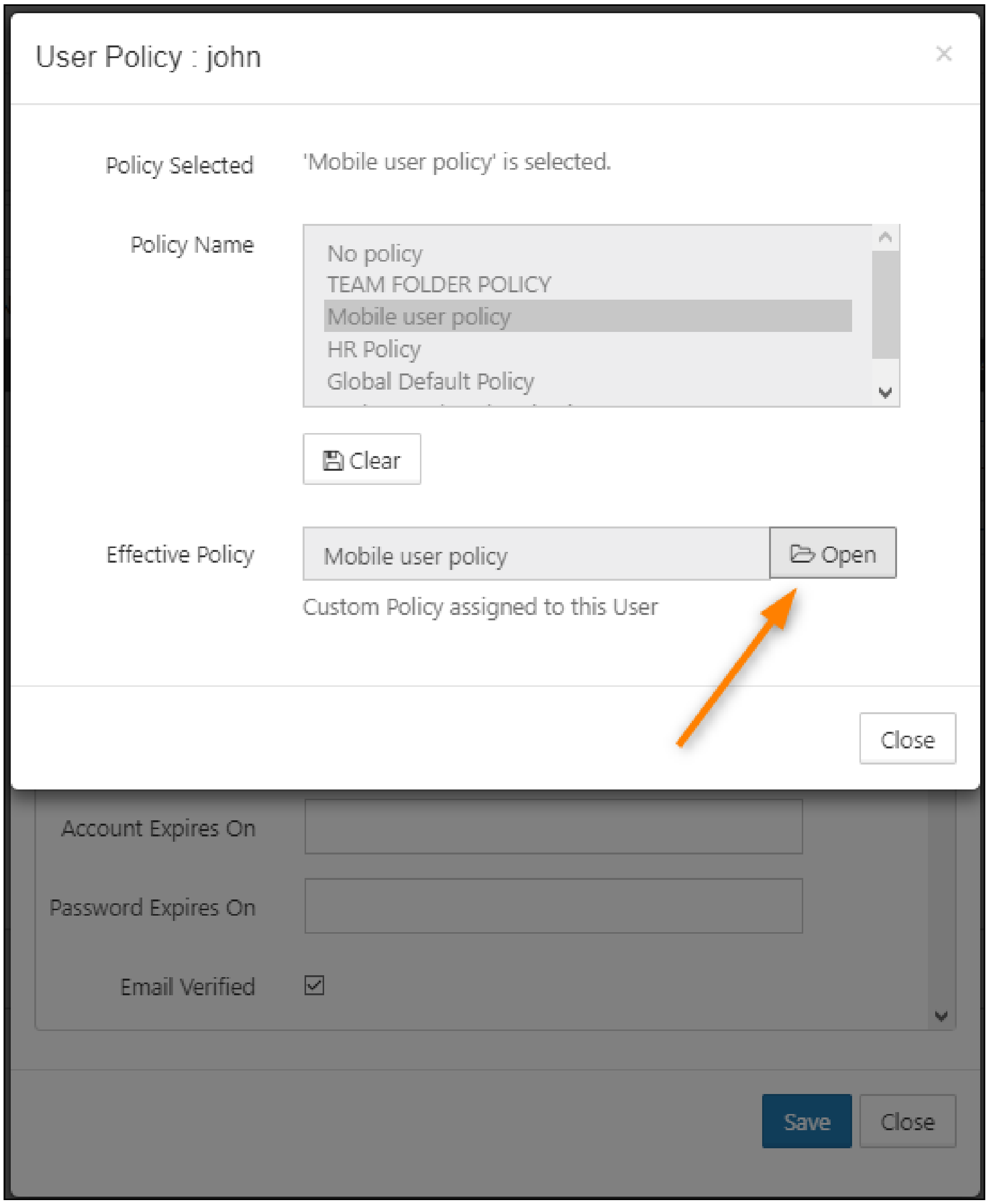
Policy Selected: 'Mobile user policy' is selected.

Policy Name:

- No policy
- TEAM FOLDER POLICY
- Mobile user policy
- HR Policy
- Global Default Policy

Effective Policy: Mobile user policy

Calculate effective policy of the user, as group associations may change enforced policy.



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

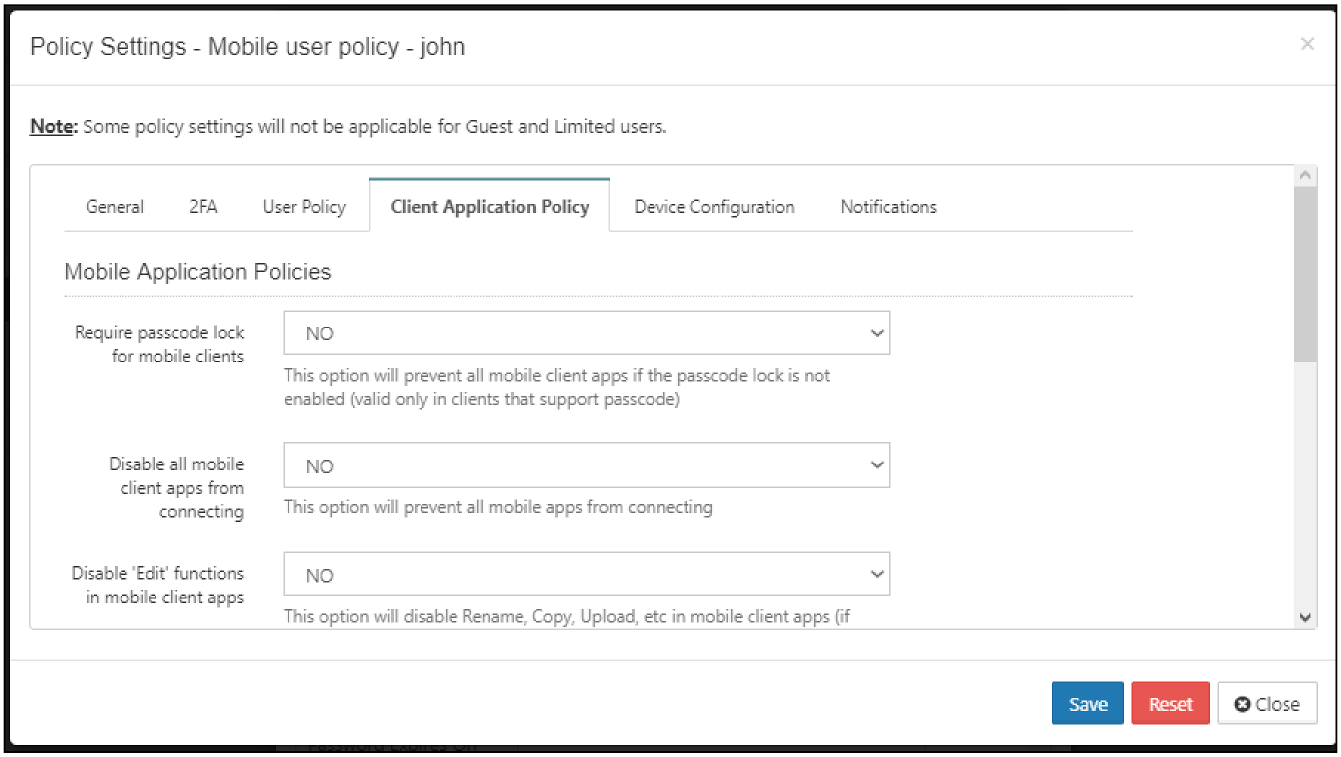
Effective Policy: Mobile user policy

Custom Policy assigned to this User

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.

Mobile Application Policies

Require passcode lock for mobile clients: NO

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: NO

This option will prevent all mobile apps from connecting

Disable 'Edit' functions in mobile client apps: NO

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?

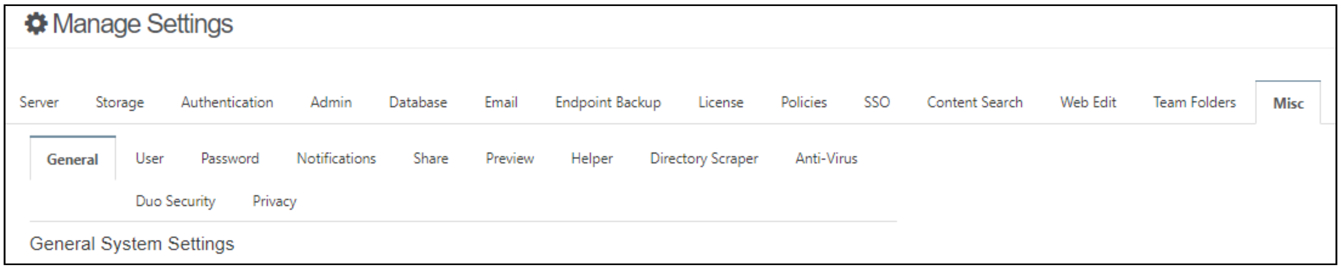
A proxy server is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers.

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.

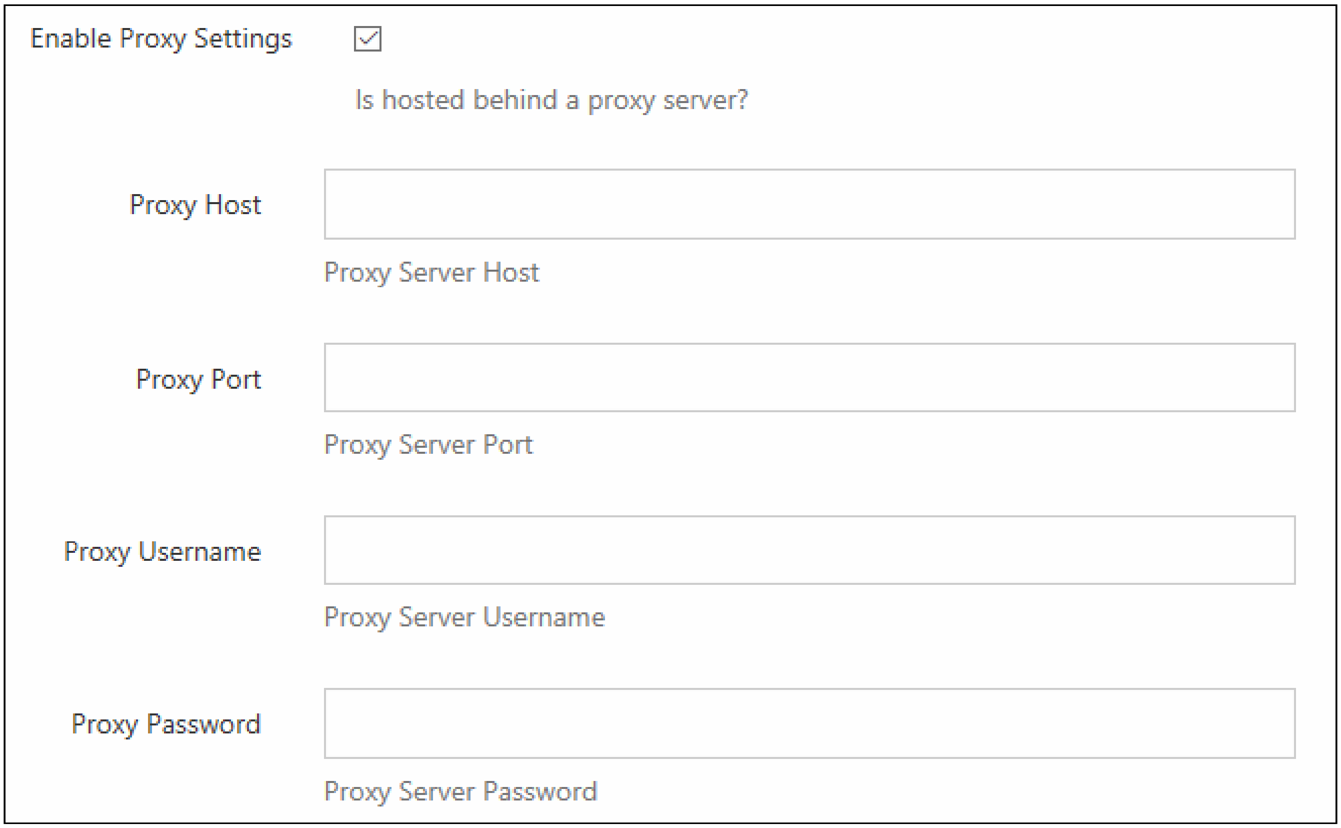
Figure 1. General System Settings



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


Enable Proxy Settings ☑
Is hosted behind a proxy server?

Proxy Host
Proxy Server Host

Proxy Port
Proxy Server Port

Proxy Username
Proxy Server Username

Proxy Password
Proxy Server Password

Improving Cookie Security

Defending your browser from CSRF attacks

To defend your browser from cross-site request forgery (CSRF) attacks , you can add a cookie same-site setting to FileCloud.

The cookie same-site value can be set to the following, as stated in the MDN Web Docs site at https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite:

- **Lax** - Cookies are not sent on normal cross-site subrequests (for example to load images or frames into a third party site), but are sent when a user is *navigating* to the origin site (i.e., when following a link).
- **Strict** - Cookies will only be sent in a first-party context and not be sent along with requests initiated by third-party websites.
- **None** - Cookies will be sent in all contexts, i.e. in responses to both first-party and cross-origin requests. If SameSite=None is set, the cookie Secure attribute must also be set (or the cookie will be blocked).
  To set the Secure attribute, see Adding httponly and secure flags, below.

For more information, see https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite.

To specify a cookie same-site value:

1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
   - To set the cookie same-site setting to strict, add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
     ```

   - To set the cookie same-site setting to lax (the default), add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Lax");
     ```

   - To set the cookie same-site setting to none, add:

     ```
     define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
     ```

Adding httponly and secure flags

You can take additional steps to make your cookies secure from external attacks by adding **httponly** and **secure flags** when sending cookies through HTTP headers.

What do httponly and secure flags do?

- A cookie can be accessed through http or through client-side Javascript. An **httponly flag** blocks access to a cookie from the client side (Javascript) by only allowing it to be accessed by http.
- Most sites are accessed by https, but some sites may also be accessed by http or some of their components may be sent through http. This leaves cookies vulnerable to being accessed over http. A **secure flag** prevents them from being accessed through http by only allowing them to be transmitted over https.

To configure FileCloud to always use the httponly and secure flags in HTTP headers:

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

```
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

Recommended and default settings

The recommended values for the cookie settings are the following:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "Strict");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

If you are using FileCloud 23.1 or later:

The above recommended settings are the same as your default settings.

If you are using a version of FileCloud prior to 23.1:

Your default settings are:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
define("TONIDOCLOUD_SECURE_COOKIE", 0);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 0);
```

You may copy the recommended settings, which are stored in cloudconfig-sample.php into cloudconfig.php to override the defaults.

Integration with MS Teams

If you have integrated your system with MS Teams, and login frequently redirects users back to the login page:

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

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

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.

ⓘ Using the WOPI protocol, online document editing is supported in FileCloud Server version 14.1 and later.

Administrators can configure online editing to allow FileCloud users to select any supported document and edit the document from within the User Portal.

- All the changes made by the user are saved in FileCloud automatically.
- Depending on the versioning settings in FileCloud, additional versions may be created.
- FileCloud uses the WOPI (Web Application Open Platform Interface) protocol to support online web editing.

Read more about the WOPI protocol to support document editing.

To use WOPI, you must install or have already available one of the following to provide the web editing capability:

- Microsoft Office Online
- Collabora Code
- OnlyOffice

Use the instructions from the following sections to install and configure online web editing.

- Microsoft Office Online Web Editing
- Web Editing With Collabora Code
- Web Editing with OnlyOffice
- 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
- Changing the locale in online Office documents

Microsoft Office Online Web Editing

Integration with Microsoft Office Online (Microsoft Office 365) is available in FileCloud Server version 17.3 and later.

You can integrate FileCloud with Microsoft Office Online to allow your users to edit documents in a browser. FileCloud uses the WOPI protocol for this integration.

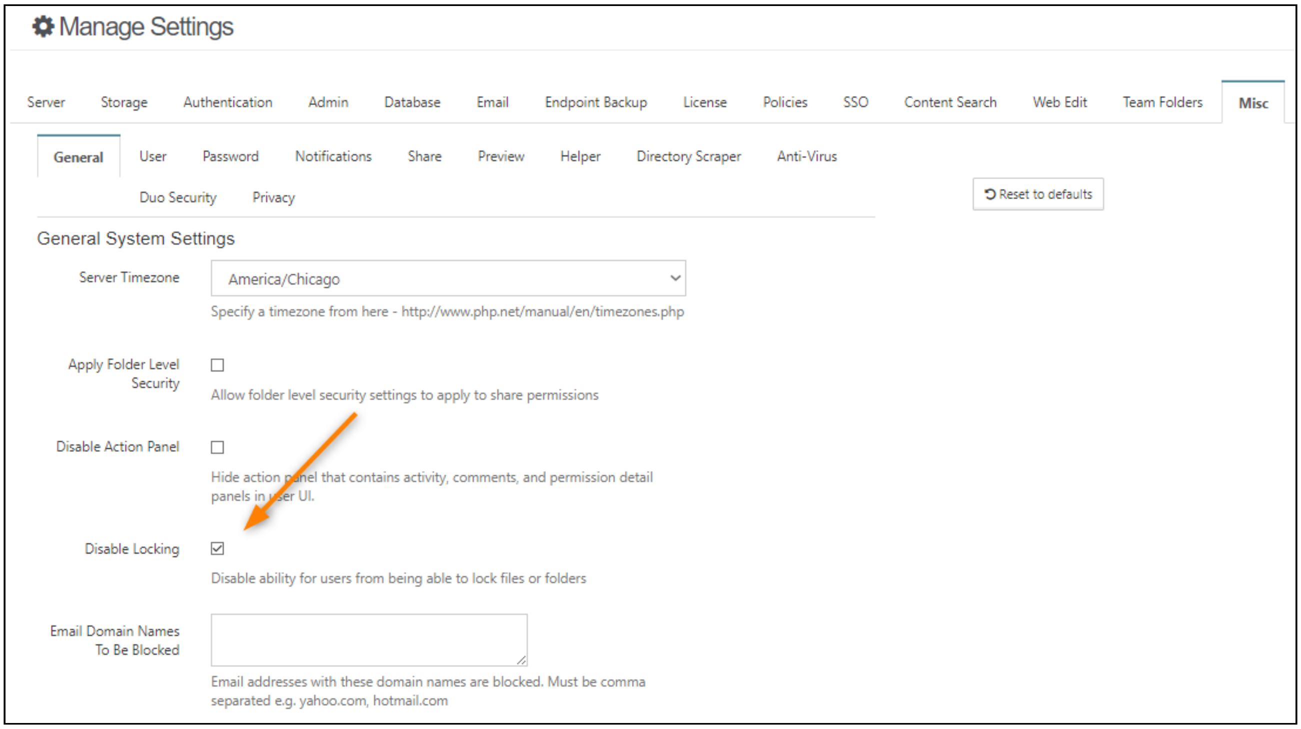
Administrators can configure Web Edit in the following ways:

FileCloud can integrate with your Microsoft-hosted Office online server to edit office documents.	➡ Microsoft Office Online for Cloud Web Editing
FileCloud can integrate with your on-premises Office online server installation to edit office documents.	➡ Microsoft Office Online Server Web Editing

Troubleshooting Office Web Editing

Document always opens in read-only mode

This issue can happen if admin has disabled "Locking" feature. To enable "Locking", navigate to admin UI → Settings → Misc tab and unselect "Disable Locking" checkbox.



General System Settings

Server Timezone: America/Chicago
Specify a timezone from here - http://www.php.net/manual/en/timezones.php

Apply Folder Level Security: □
Allow folder level security settings to apply to share permissions

Disable Action Panel: □
Hide action panel that contains activity, comments, and permission detail panels in user UI.

Disable Locking: ☑
Disable ability for users from being able to lock files or folders

Email Domain Names To Be Blocked:
Email addresses with these domain names are blocked. Must be comma separated e.g. yahoo.com, hotmail.com

Microsoft Office Online Cloud For Web Edit

FileCloud can integrate with your Microsoft-hosted Office online server to edit office documents.

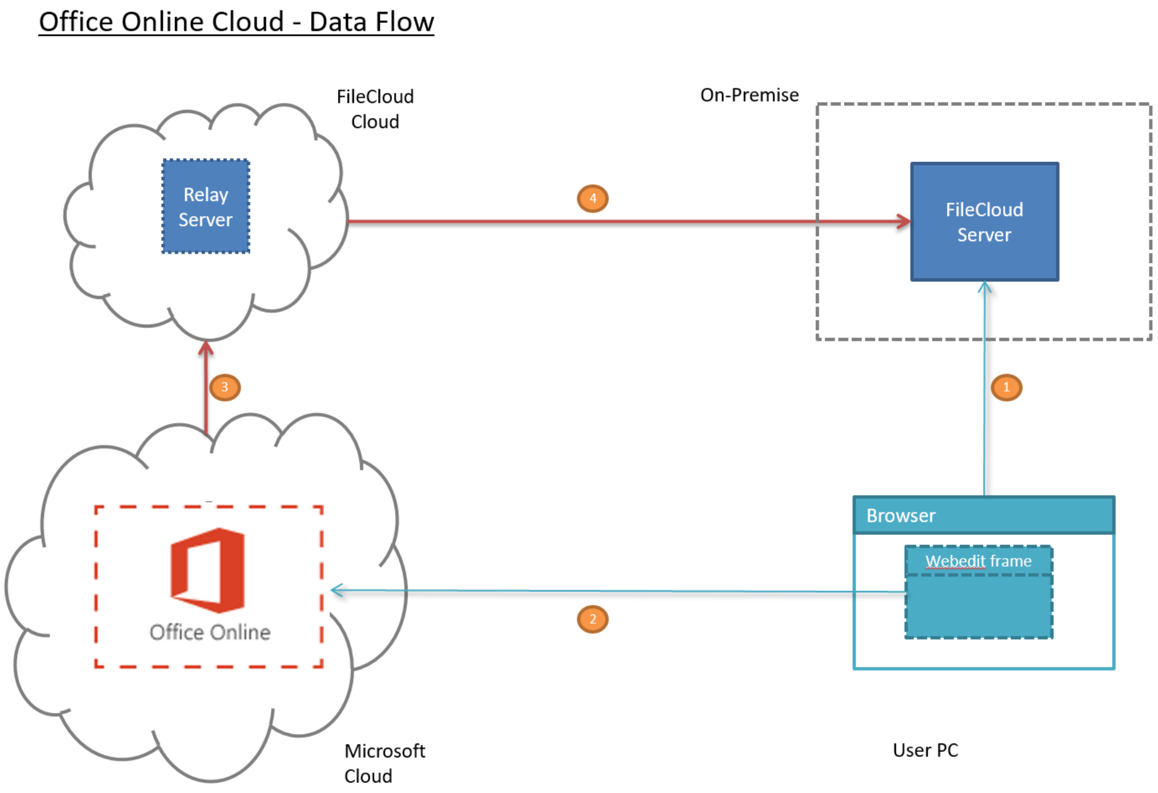
Tips

- Please note that for using this type of web editing, users should have an **Office365** account.
- When configuring Office365, please use the default 'admin' user to login into FileCloud admin UI. For security reasons, this configuration is not allowed as a normal user promoted as admin.
- Support for large file sizes may vary depending on the speed between FileCloud and the relay servers.

➡ Office 365 Office product page

Dataflow

Following diagram depicts the interaction between Microsoft Office Online cloud and an on-premises FileCloud server.



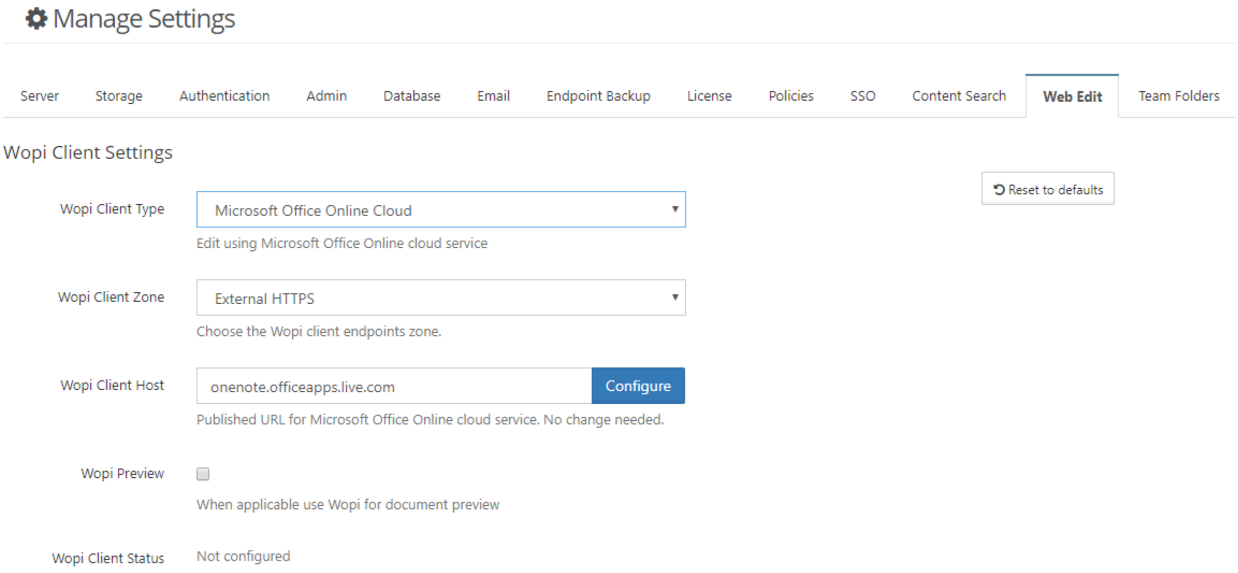
Steps:

1. User selects a document file in office online from FileCloud user UI. It loads a HTML page with embedded IFRAME pointing to the Microsoft Office Online cloud.
2. IFRAME loaded in the previous step loads the document specific application from the Microsoft cloud. This in turn instructs the Office Online cloud to load the document from FileCloud server.
3. Since Office Online cloud supports only pre-approved URLs it cannot load the document directly from FileCloud server. So the download request is forwarded to a relay server (hosted by FileCloud).

4. Relay server in turn forwards the request to FileCloud server and returns the response back. In summary, relay server serves as a bridge between Office Online cloud and FileCloud server making the communication back and forth work seamlessly.

Configuring FileCloud With Office Online Cloud

1. Login into FileCloud server admin UI(as the default 'admin' user), which needs to integrate with Office Online to offer web editing.
2. Navigate to Settings -> Web edit tab. Select "Microsoft Office Online Cloud" as Wopi Client Type. It automatically selects "External HTTPS" and pre-fills the "Wopi Client Host" to URL "onenote.officeapps.live.com".
   Click "Configure".



Wopi Client Settings

Wopi Client Type: Microsoft Office Online Cloud
Edit using Microsoft Office Online cloud service

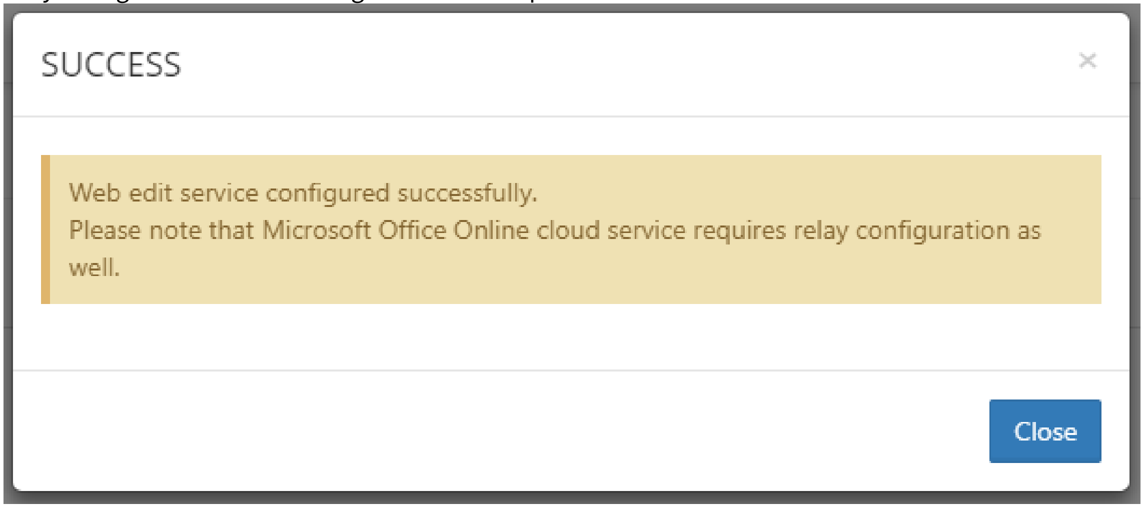
Wopi Client Zone: External HTTPS
Choose the Wopi client endpoints zone.

Wopi Client Host: onenote.officeapps.live.com
Published URL for Microsoft Office Online cloud service. No change needed.

Wopi Preview: □
When applicable use Wopi for document preview

Wopi Client Status: Not configured

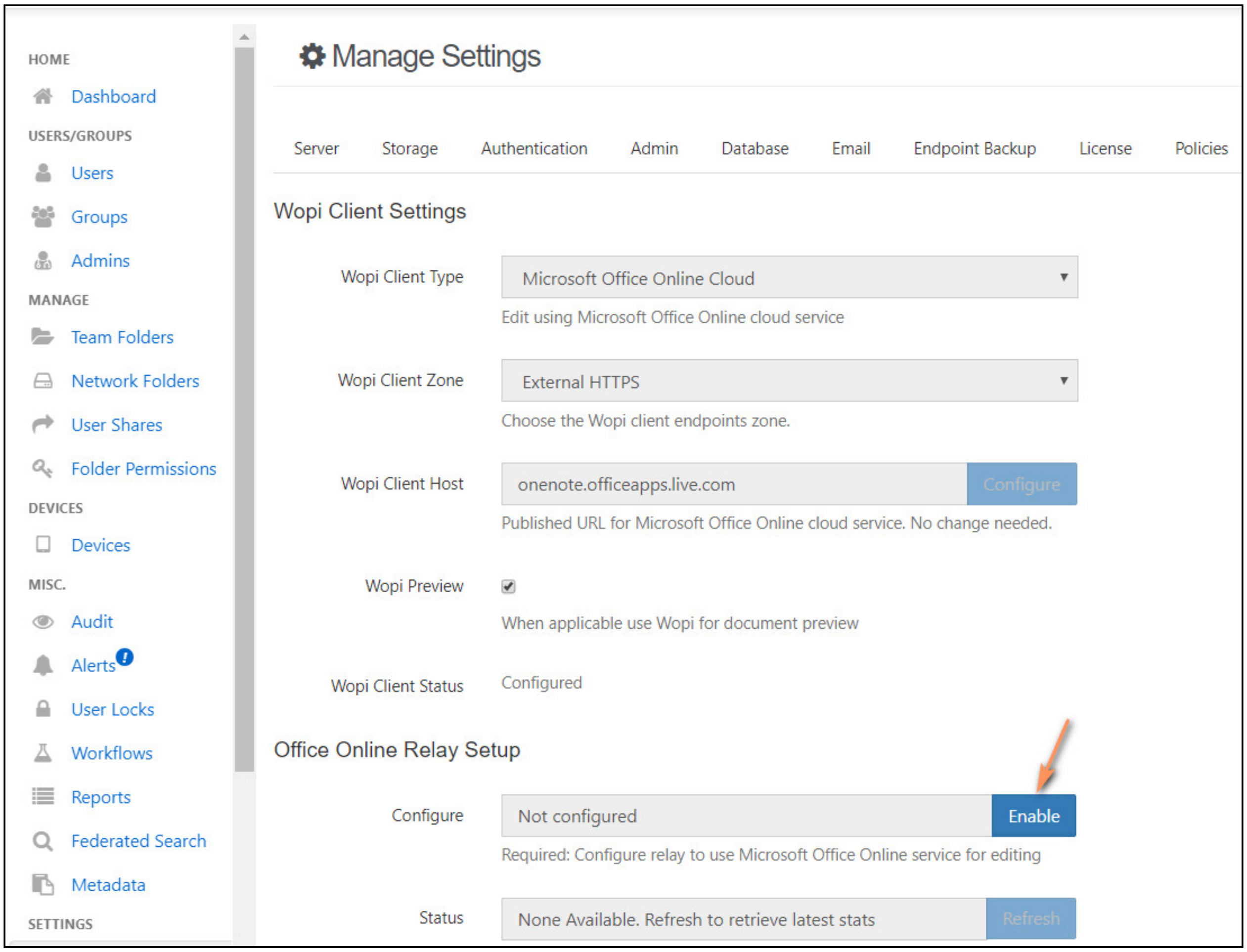
3. Upon successful configuration, the following screen should appear. This dialog notifies the user to enable the relay configuration for the configuration to complete.



SUCCESS

Web edit service configured successfully.
Please note that Microsoft Office Online cloud service requires relay configuration as well.

4. To enable relay, click on the "Enable" button on the "Office Online Relay Setup" section.



Manage Settings

Wopi Client Settings

Wopi Client Type: Microsoft Office Online Cloud
Edit using Microsoft Office Online cloud service

Wopi Client Zone: External HTTPS
Choose the Wopi client endpoints zone.

Wopi Client Host: onenote.officeapps.live.com
Published URL for Microsoft Office Online cloud service. No change needed.

Wopi Preview: ☑
When applicable use Wopi for document preview

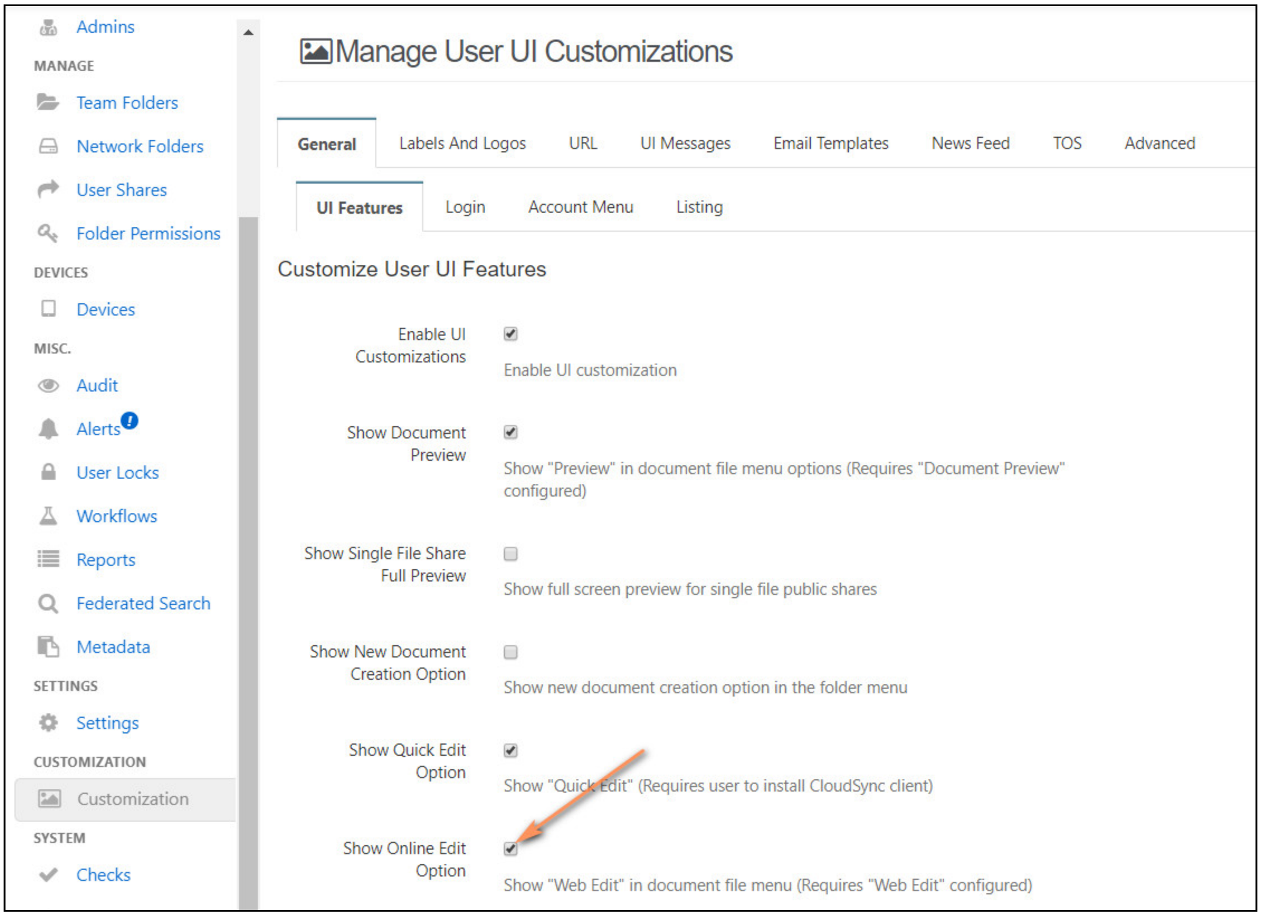
Wopi Client Status: Configured

Office Online Relay Setup

Configure: Not configured
Required: Configure relay to use Microsoft Office Online service for editing

Status: None Available. Refresh to retrieve latest stats

5. When WOPI edit over cloud is selected, it also switches to use WOPI for all document previews, since WOPI webeditor provides a more faithful reproduction of the document. Admins can disable this behaviour by unselecting "Wopi Preview" checkbox from the "Wopi Client Settings" screen.
6. Now that FileCloud server is configured with office online server, administrator might need to enable the web edit option for users.
   To enable web edit in user UI, navigate to Customizations -> General -> UI Features tab and check the option "Show Online Edit Option". Click "Save" button to save the changes.



Manage User UI Customizations

Customize User UI Features

Enable UI Customizations ☑ Enable UI customization

Show Document Preview ☑ Show "Preview" in document file menu options (Requires "Document Preview" configured)

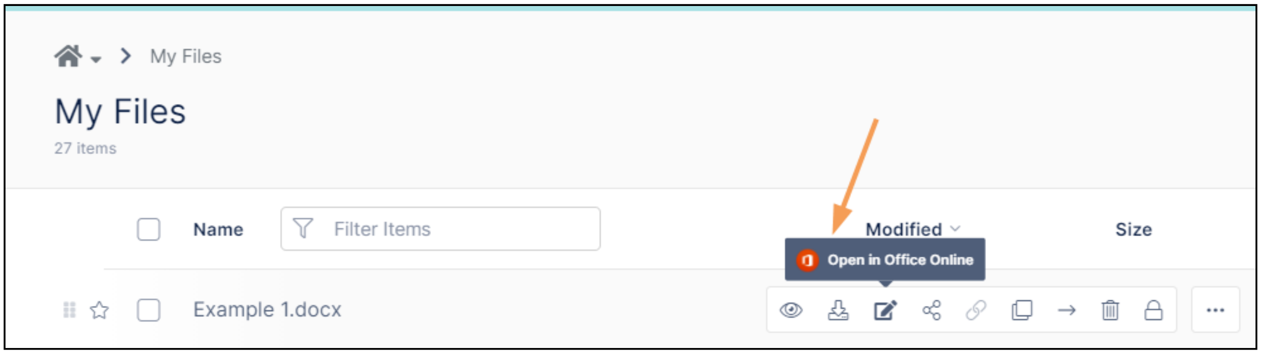
Show Single File Share Full Preview □ Show full screen preview for single file public shares

Show New Document Creation Option □ Show new document creation option in the folder menu

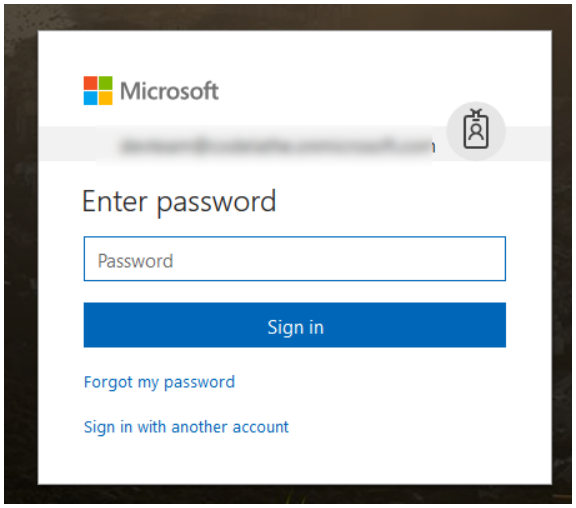
Show Quick Edit Option ☑ Show "Quick Edit" (Requires user to install CloudSync client)

Show Online Edit Option ☑ Show "Web Edit" in document file menu (Requires "Web Edit" configured)

7. Now login into user UI and hover over an editable Office document. Hover over the Web Edit icon, and ensure that you see the Office icon and the tooltip **Open in Office Online**.
8. Click the icon.
   The file is opened in the Office Online editor.



9. When the office online web editor application loads, it will prompt for "Office 365" account. Upon logging in the selected document will be loaded in the editor.



> ⓘ Depending the browser's cookie policies, after a user logs into their Microsoft account for WOPI edit, their FileCloud session could be closed. To avoid this problem, set TONIDOCLOUD_COOKIE_SAME_SITE_TYPE to Lax.

Microsoft Office Online Server For Web Edit

Introduction

FileCloud can integrate with an on-premises Office online server installation to edit office documents.

This section explains how to install office online server on a Windows 2012 server and configure FileCloud to use this installation for web editing.

- Installing Office Online Server on Windows 2012 R2 Server
- Configuring FileCloud To Use Office Online On-Premises Server For Web Edit

Installing Office Online Server on Windows 2012 R2 Server

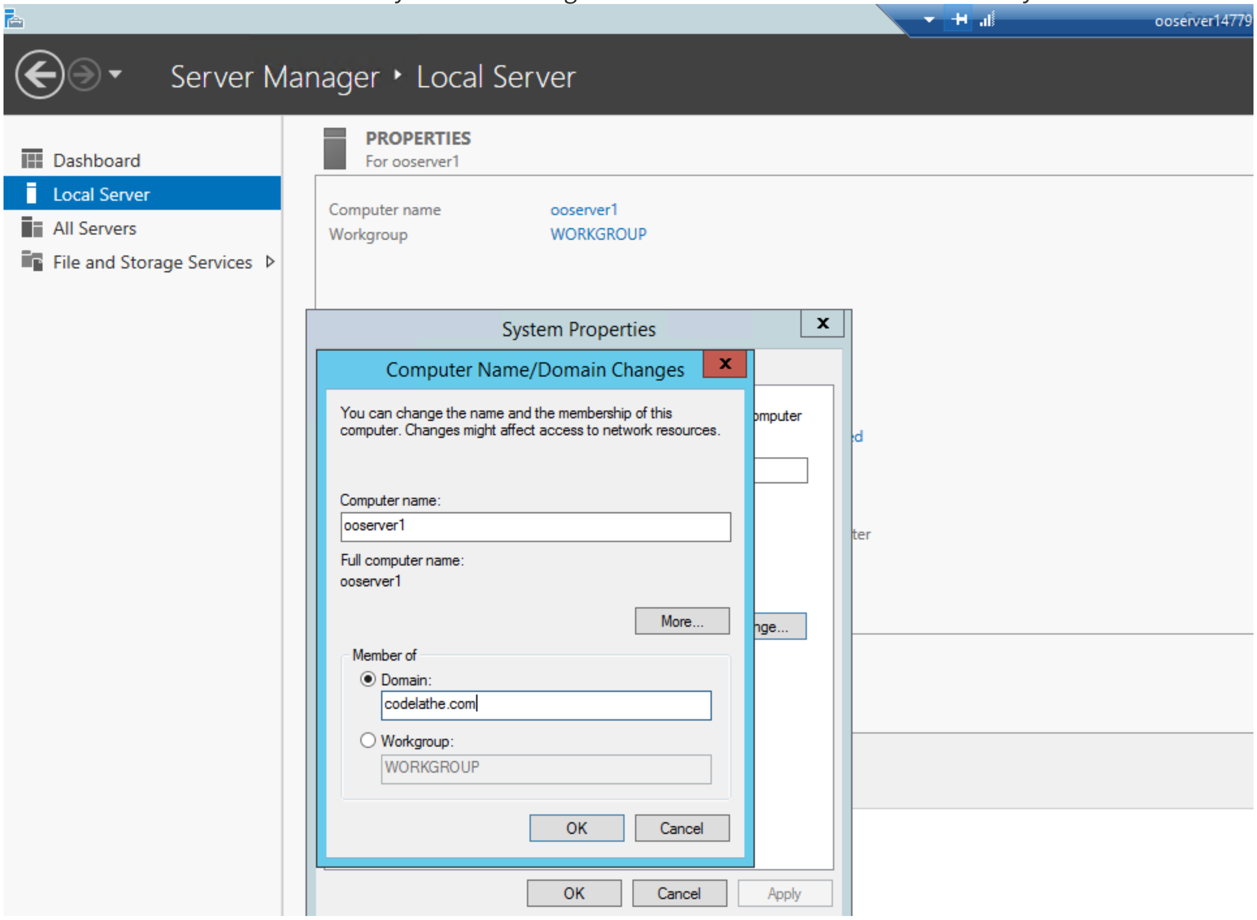
Introduction

FileCloud can integrate with an on-premises Office Online server installation to edit Office documents (word, excel and powerpoint) from a browser. The following guide explains how to install office online server on Windows 2012 server.

> It is recommended to install Office Online Server on its own Windows 2012 R2 server. Don't install it on Active Directory domain controller, sharepoint server or Exchange server. Also the windows server where you are installing the office online server has to be connected to an Active Directory domain.

First Steps

1. Connect the windows server where you be installing office online server to an active directory domain.



PROPERTIES
For ooserver1

Computer name ooserver1
Workgroup WORKGROUP

System Properties

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

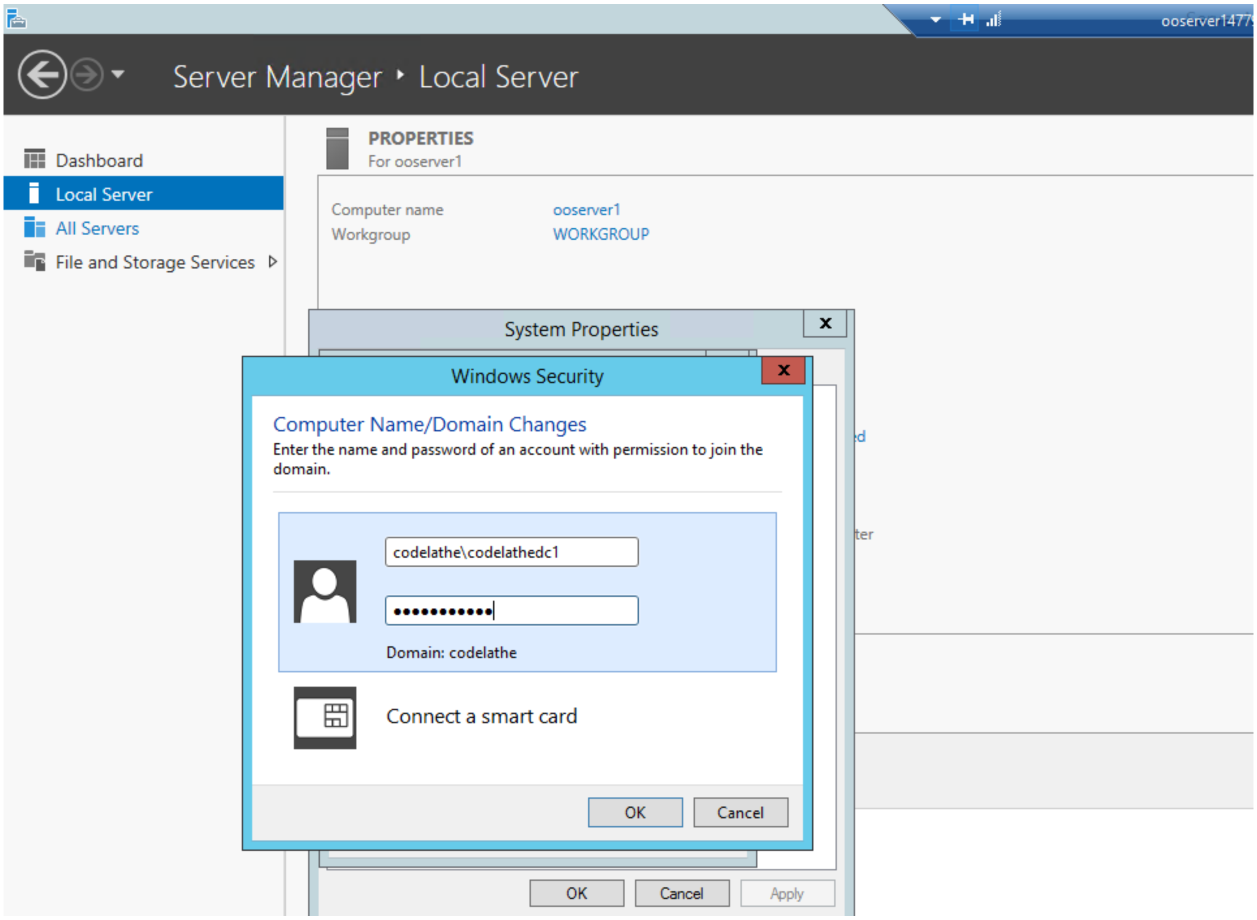
Computer name: ooserver1

Full computer name:
ooserver1

Member of

● Domain: codelathe.com

○ Workgroup: WORKGROUP



Computer name ooserver1
Workgroup WORKGROUP

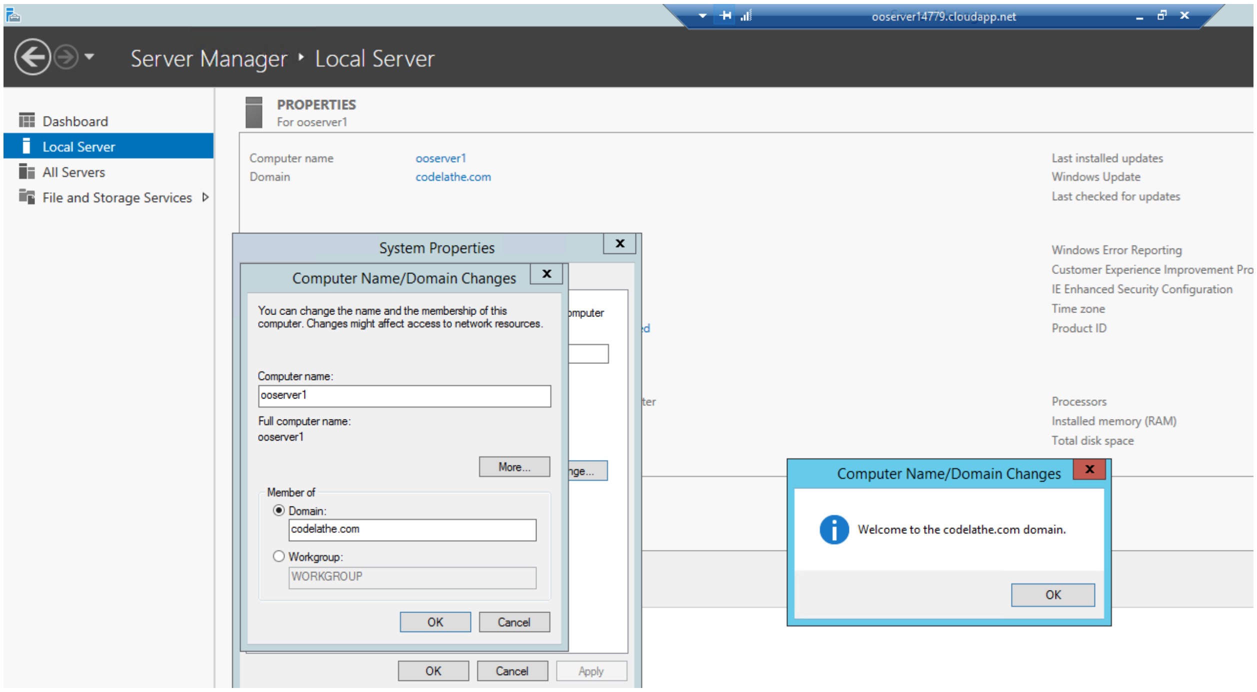
Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

codelathe\codelathedc1

•••••••••••

Domain: codelathe



Computer name ooserver1
Domain codelathe.com

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: ooserver1

Full computer name: ooserver1

More...

Member of

● Domain: codelathe.com

○ Workgroup: WORKGROUP

OK Cancel

Computer Name/Domain Changes

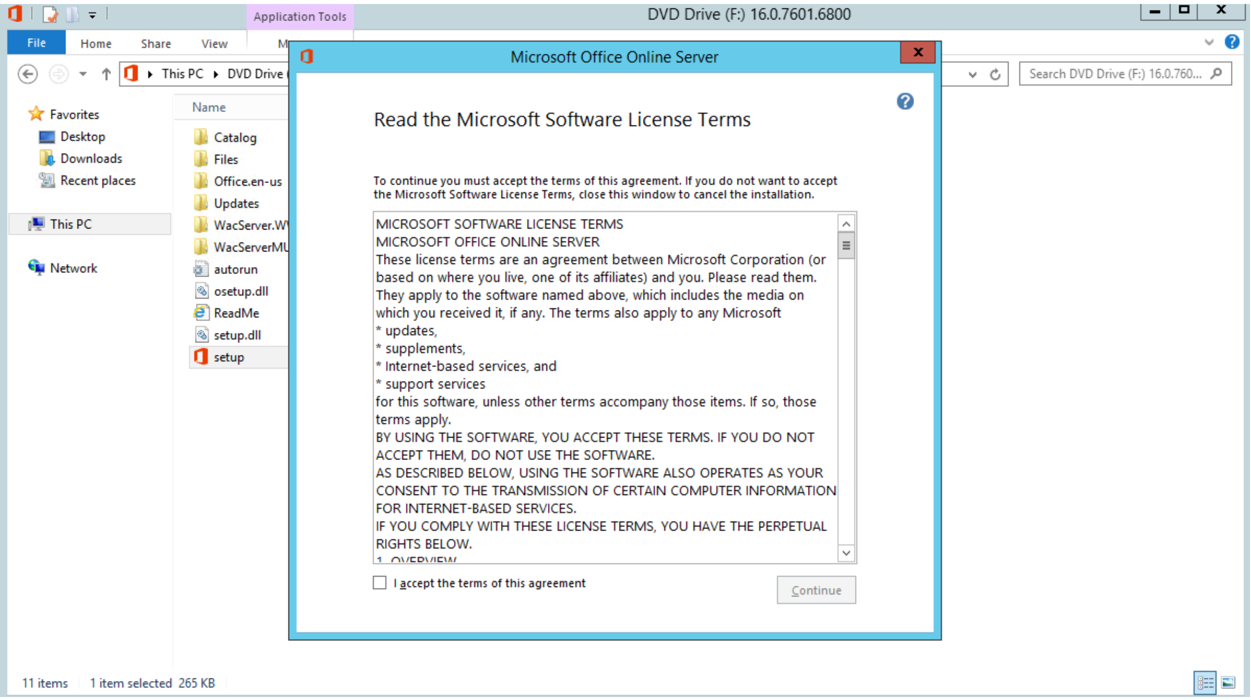
Welcome to the codelathe.com domain.

OK

2. Restart the server to apply the changes.
3. Install all available windows updates and restart the server if prompted.
4. Open the Windows PowerShell prompt as an administrator and run the following command to install the required roles and services. After the installation restart the server.

```
Add-WindowsFeature Web-Server,Web-Mgmt-Tools,Web-Mgmt-Console,Web-WebServer,Web-Common-Http,Web-Default-Doc,Web-Static-Content,Web-Performance,Web-Stat-Compression,Web-Dyn-Compression,Web-Security,Web-Filtering,Web-Windows-Auth,Web-App-Dev,Web-Net-Ext45,Web-Asp-Net45,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Includes,InkandHandwritingServices,NET-Framework-Features,NET-Framework-Core,NET-HTTP-Activation,NET-Non-HTTP-Activ,NET-WCF-HTTP-Activation45
```

5. Download Office Online Server from the Volume License Service Center. Go to the location where you downloaded Office Online Server and run setup.exe.

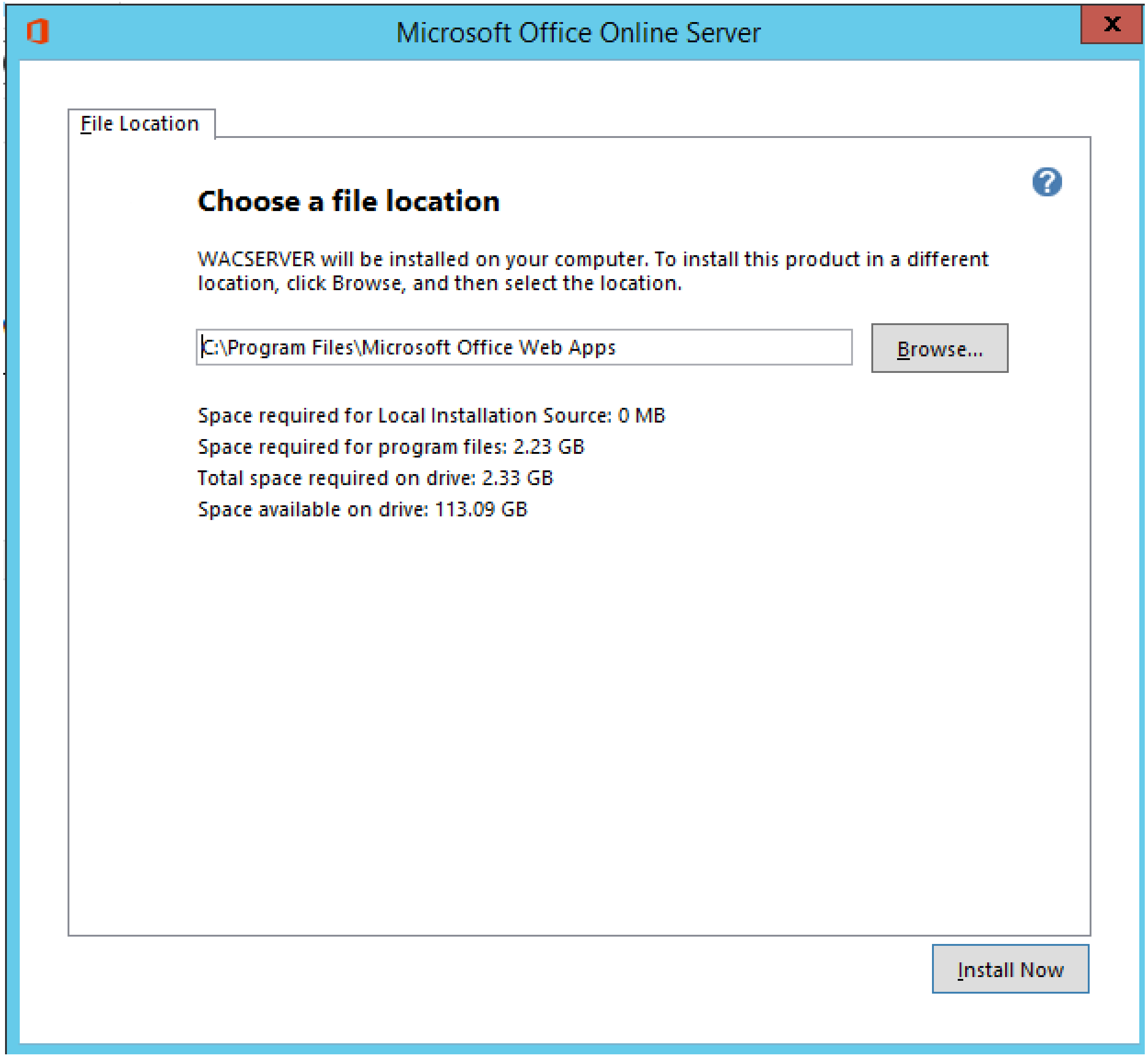


Read the Microsoft Software License Terms

To continue you must accept the terms of this agreement. If you do not want to accept the Microsoft Software License Terms, close this window to cancel the installation.

MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT OFFICE ONLINE SERVER
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
* updates,
* supplements,
* Internet-based services, and
* support services
for this software, unless other terms accompany those items. If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.
AS DESCRIBED BELOW, USING THE SOFTWARE ALSO OPERATES AS YOUR CONSENT TO THE TRANSMISSION OF CERTAIN COMPUTER INFORMATION FOR INTERNET-BASED SERVICES.
IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE PERPETUAL RIGHTS BELOW.
1. OVERVIEW

☐ I accept the terms of this agreement

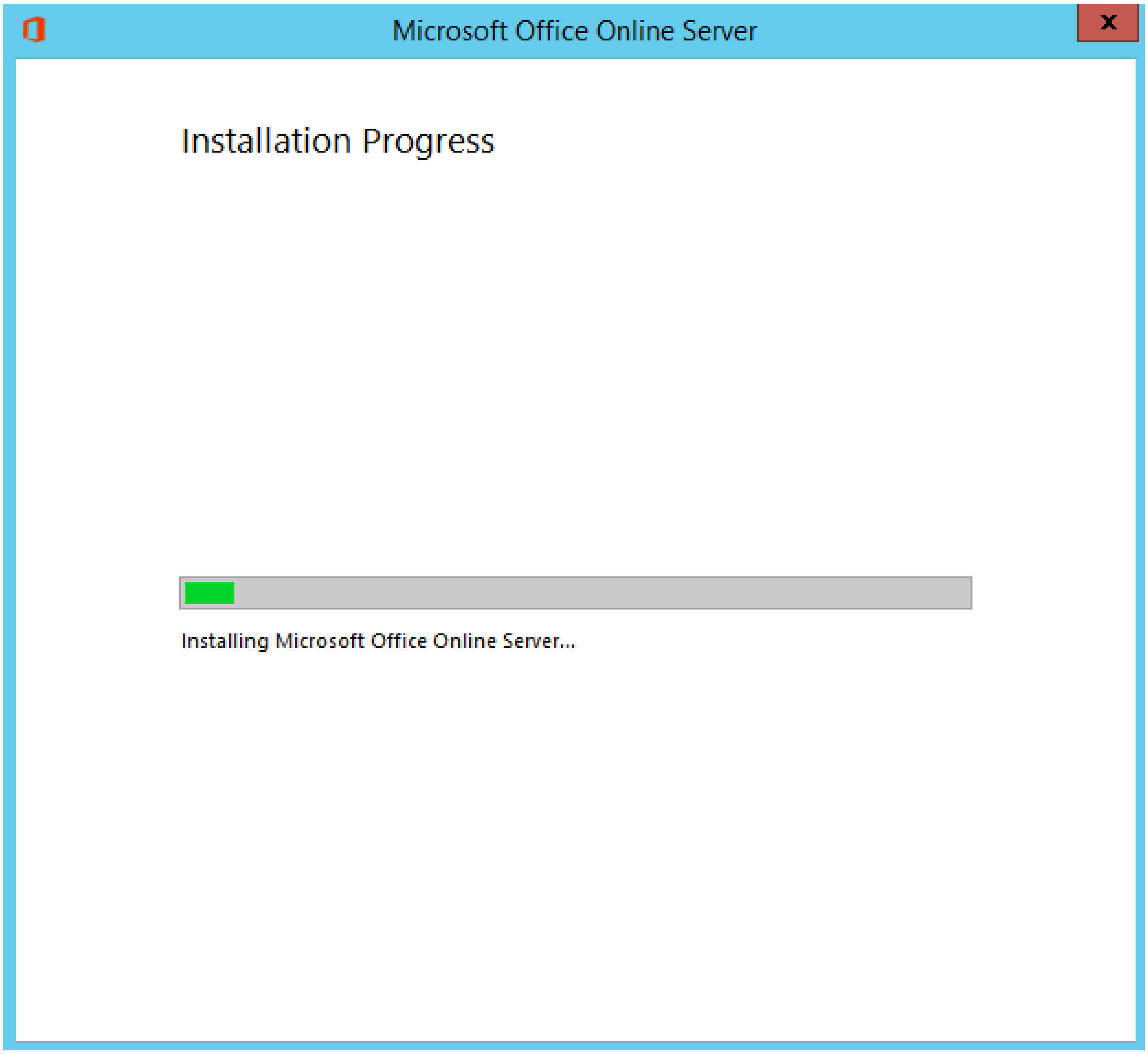


Choose a file location

WACSERVER will be installed on your computer. To install this product in a different location, click Browse, and then select the location.

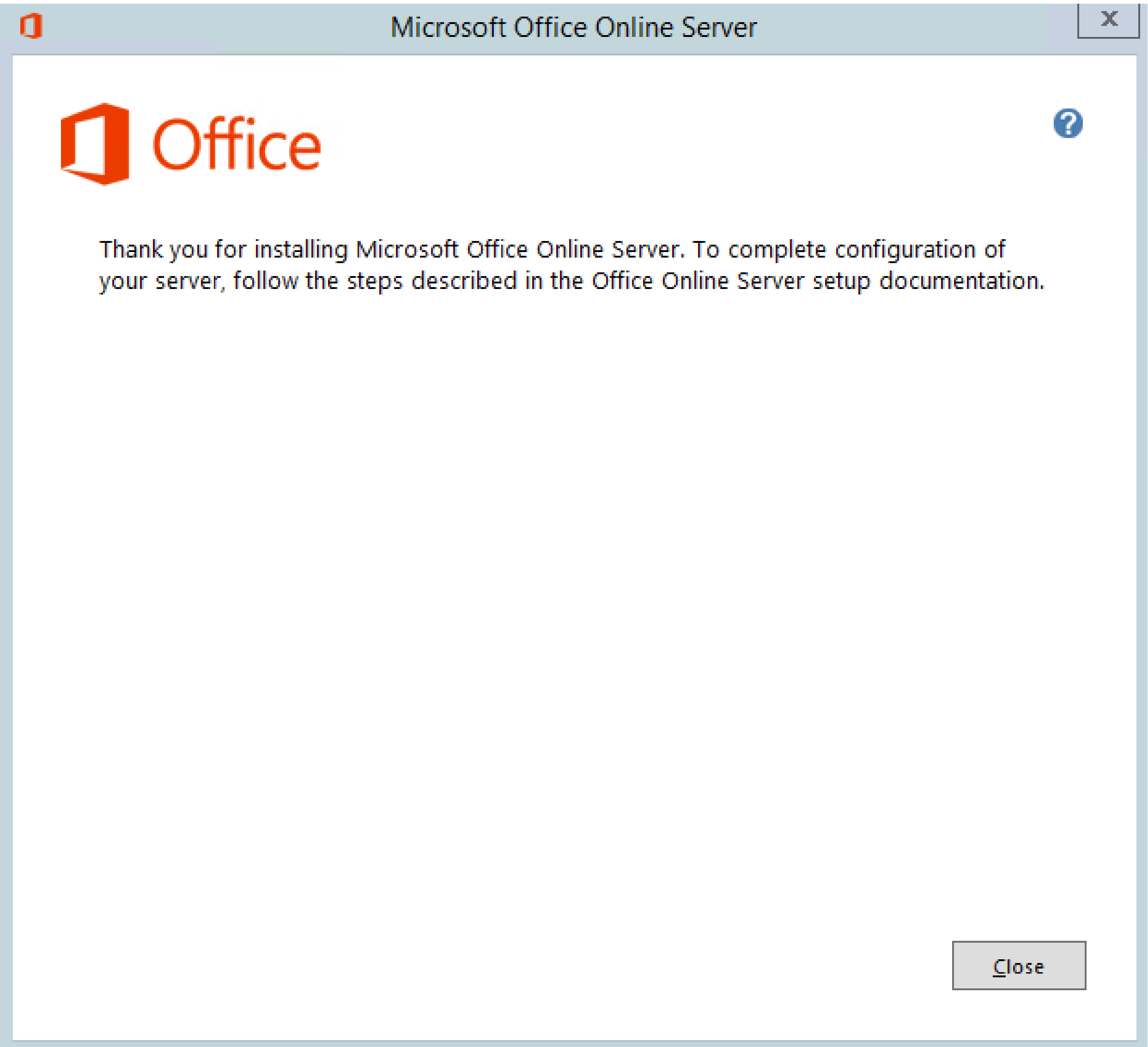
C:\Program Files\Microsoft Office Web Apps

Space required for Local Installation Source: 0 MB
Space required for program files: 2.23 GB
Total space required on drive: 2.33 GB
Space available on drive: 113.09 GB



Installation Progress

Installing Microsoft Office Online Server...



Thank you for installing Microsoft Office Online Server. To complete configuration of your server, follow the steps described in the Office Online Server setup documentation.

6. Open the Windows PowerShell prompt as an administrator and run the following command to Import the OfficeWebApps powershell module.

```
import-module “C:\Program Files\Microsoft Office Web
Apps\AdminModule\OfficeWebApps\OfficeWebApps.psd1”
```

ⓘ Note: Windows powershell for Office Online Server provide offers powershell cmdlets to create and manage Office Web Apps. You can find complete reference document here: https://technet.microsoft.com/en-us/library/jj219436.aspx

Deploy as single-server Office Online Server farm that uses HTTP

1. Open the Windows PowerShell prompt as an administrator and run the **New-OfficeWebAppsFarm** command to create a new Office Online Server farm that consists of a single server, as shown in the following example. This example creates an Office Online Server farm on the local server that has editing enabled as well as http access.

   > ⓘ You need to login as the Domain Administrator to run the New-OfficeWebAppsFarm cmdlet. Local administrator account is not sufficient. Make sure you replace the URL with your domain names.

   ```
   New-OfficeWebAppsFarm -InternalUrl "http://ooserver.internal.contoso.com"
   -ExternalUrl "http://oos.contoso.com" -AllowHttp -EditingEnabled
   ```

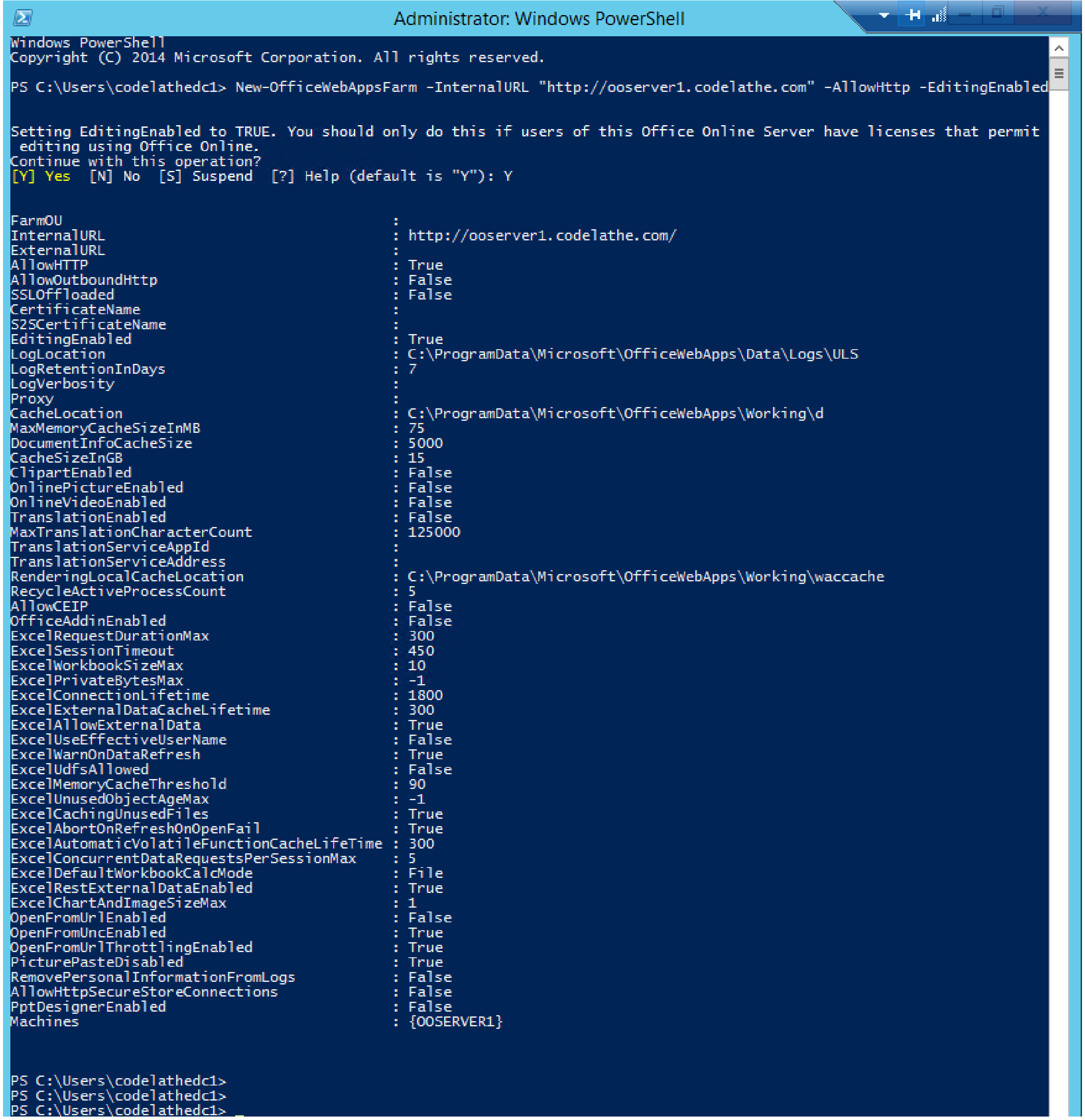
   Parameters

   - **–InternalURL** is the name of the server that runs Office Online Server
   - **–ExternalURL** Specifies the URL that clients use to access the Office Online Server from the Internet
   - **–AllowHttp** configures the farm to use HTTP.
   - **–EditingEnabled** enables editing in Office Online Server when used with FileCloud.

   Additional parameters that configure translation services, proxy servers, ClipArt support, and Online Viewers are described in New-OfficeWebAppsFarm.

2. Verify that Office Online Server Farm was created successfully. After the farm is created, details about the farm are displayed in the Windows PowerShell prompt like given below. To verify that Office Online Server is installed and configured correctly, use a web browser to access the Office Online Server discovery URL, as shown in the following example. The discovery URL is the *InternalUrl* parameter you specified when you configured your Office Online Server farm, followed by **/hosting/discovery**, for example: http://oos.yourdomain.com/hosting/

discovery



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\codelathedc1> New-OfficeWebAppsFarm -InternalURL "http://ooserver1.codelathe.com" -AllowHttp -EditingEnabled


Setting EditingEnabled to TRUE. You should only do this if users of this Office Online Server have licenses that permit
 editing using Office Online.
Continue with this operation?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


FarmOU                                      :
InternalURL                                 : http://ooserver1.codelathe.com/
ExternalURL                                 :
AllowHTTP                                   : True
AllowOutboundHttp                           : False
SSLOffloaded                                : False
CertificateName                             :
S2SCertificateName                          :
EditingEnabled                              : True
LogLocation                                 : C:\ProgramData\Microsoft\OfficeWebApps\Data\Logs\ULS
LogRetentionInDays                          : 7
LogVerbosity                                :
Proxy                                       :
CacheLocation                               : C:\ProgramData\Microsoft\OfficeWebApps\Working\d
MaxMemoryCacheSizeInMB                      : 75
DocumentInfoCacheSize                       : 5000
CacheSizeInGB                               : 15
ClipartEnabled                              : False
OnlinePictureEnabled                        : False
OnlineVideoEnabled                          : False
TranslationEnabled                          : False
MaxTranslationCharacterCount                : 125000
TranslationServiceAppId                     :
TranslationServiceAddress                   :
RenderingLocalCacheLocation                 : C:\ProgramData\Microsoft\OfficeWebApps\Working\waccache
RecycleActiveProcessCount                   : 5
AllowCEIP                                   : False
OfficeAddinEnabled                          : False
ExcelRequestDurationMax                     : 300
ExcelSessionTimeout                         : 450
ExcelWorkbookSizeMax                        : 10
ExcelPrivateBytesMax                        : -1
ExcelConnectionLifetime                     : 1800
ExcelExternalDataCacheLifetime              : 300
ExcelAllowExternalData                      : True
ExcelUseEffectiveUserName                   : False
ExcelWarnOnDataRefresh                      : True
ExcelUdfsAllowed                            : False
ExcelMemoryCacheThreshold                   : 90
ExcelUnusedObjectAgeMax                     : -1
ExcelCachingUnusedFiles                     : True
ExcelAbortOnRefreshOnOpenFail               : True
ExcelAutomaticVolatileFunctionCacheLifeTime : 300
ExcelConcurrentDataRequestsPerSessionMax    : 5
ExcelDefaultWorkbookCalcMode                : File
ExcelRestExternalDataEnabled                : True
ExcelChartAndImageSizeMax                   : 1
OpenFromUrlEnabled                          : False
OpenFromUncEnabled                          : True
OpenFromUrlThrottlingEnabled                : True
PicturePasteDisabled                        : True
RemovePersonalInformationFromLogs           : False
AllowHttpSecureStoreConnections             : False
PptDesignerEnabled                          : False
Machines                                    : {OOSERVER1}


PS C:\Users\codelathedc1>
PS C:\Users\codelathedc1>
PS C:\Users\codelathedc1> _
```

Deploy as single-server Office Online Server farm that uses HTTPS

1. Obtain and import an SSL certificate with the fully qualified domain name(s) (FQDN) of the Office Online Server server. You only need to configure one FQDN on the certificate. For example, oos.contoso.com. If you have different internal and external FQDNs, you'll need to configure both FQDNs on the certificate. For example, oos.internal.contoso.com and oos.contoso.com.

2. Configure DNS records to point the FQDN(s) on the certificate to your Office Online Server server. If you have different DNS servers for internal and external users, you'll need to configure the appropriate FQDN on each server.
3. Open Windows PowerShell and run the following commands. When you run the commands, replace the example FQDNs and certificate friendly name with your own.
 Same internal and external FQD

```
New-OfficeWebAppsFarm -InternalURL "https://oos.contoso.com" -ExternalURL
"https://oos.contoso.com" -CertificateName "OfficeOnlineCertificate"
```

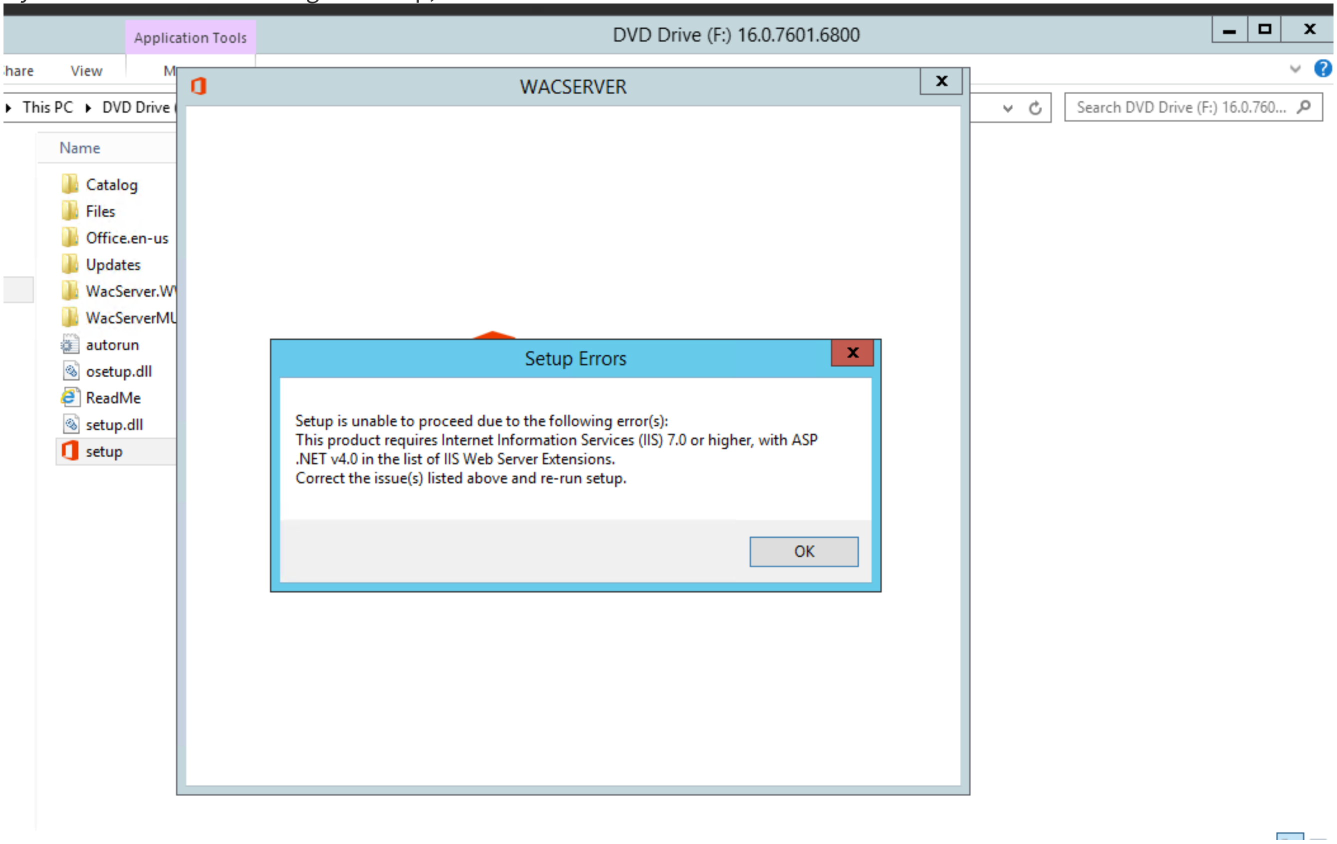
Different internal and external FQDNs

```
New-OfficeWebAppsFarm -InternalURL "https://oos.internal.contoso.com" -ExternalURL
"https://oos.contoso.com" -CertificateName "OfficeOnlineCertificate"
```

It is possible to use the wildcard ssl certificate. You need to import the ssl certificate to you certificate store.

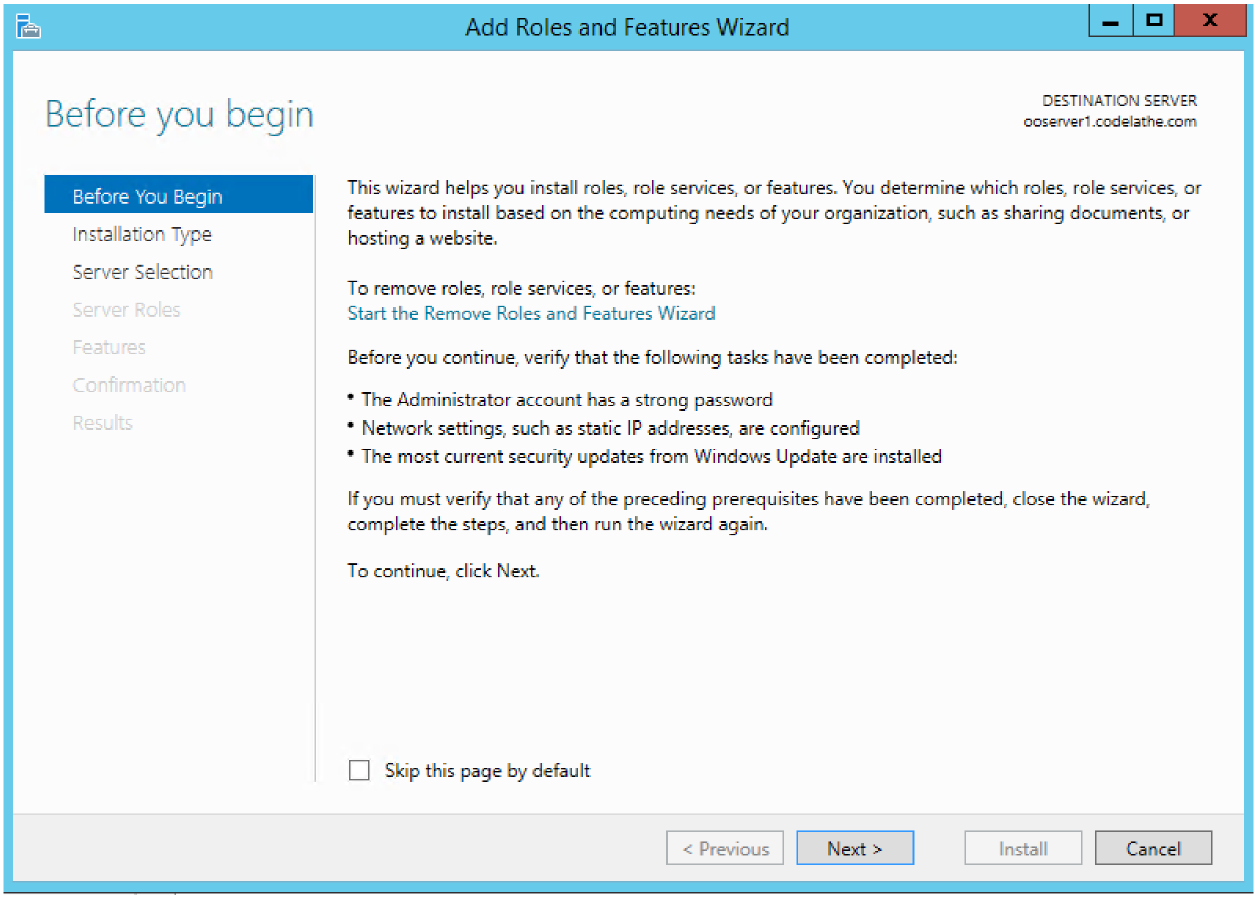
Troubleshooting Tips

If you receive an error during the setup, You need to enable web server role and ASP.NET 45



Setup is unable to proceed due to the following error(s):
This product requires Internet Information Services (IIS) 7.0 or higher, with ASP .NET v4.0 in the list of IIS Web Server Extensions.
Correct the issue(s) listed above and re-run setup.

- Start Add Roles, Features Wizard from Server Manager --> Manage --> Add Roles and Features. Enable IIS Web Server Role and ASP.Net Feature. Confirm the selections and install.



Before you begin

DESTINATION SERVER
ooserver1.codelathe.com

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

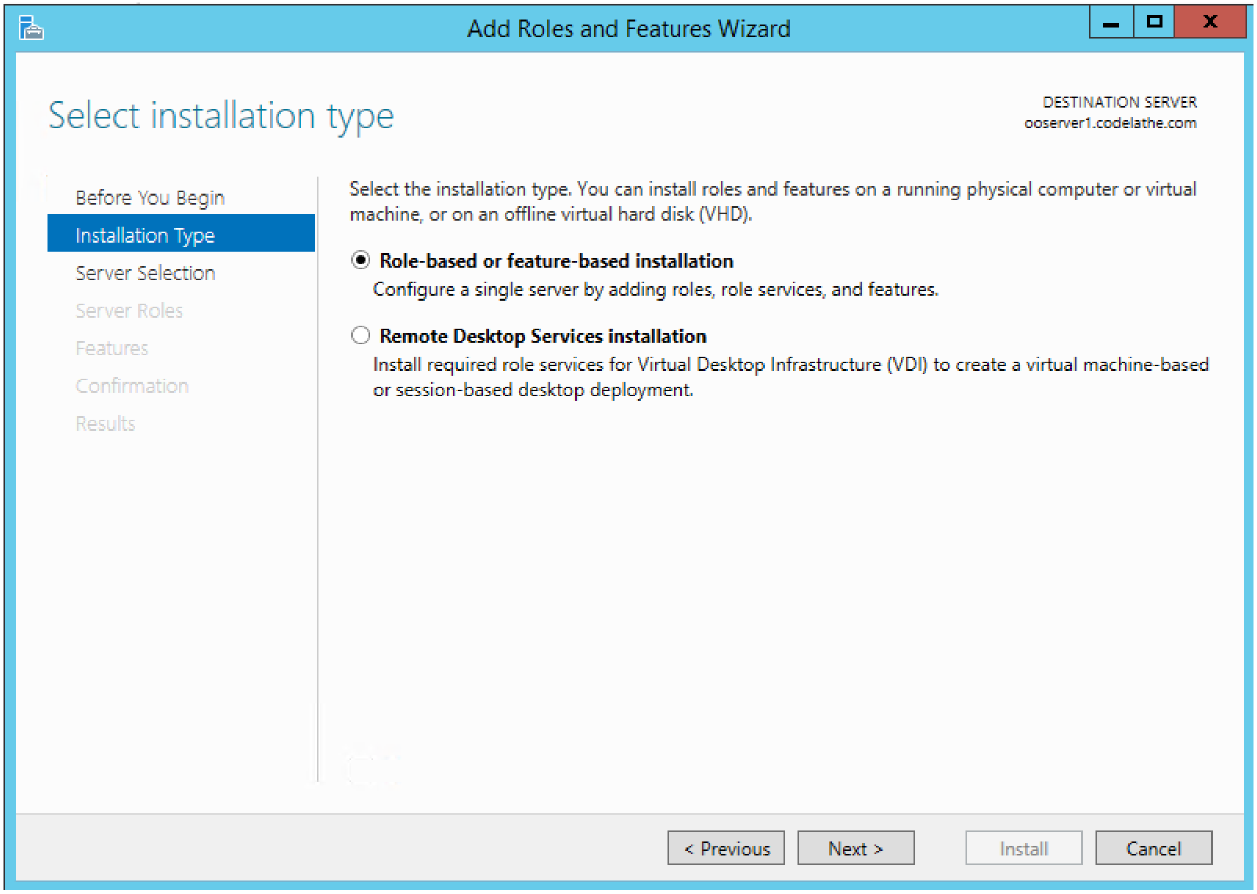
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default



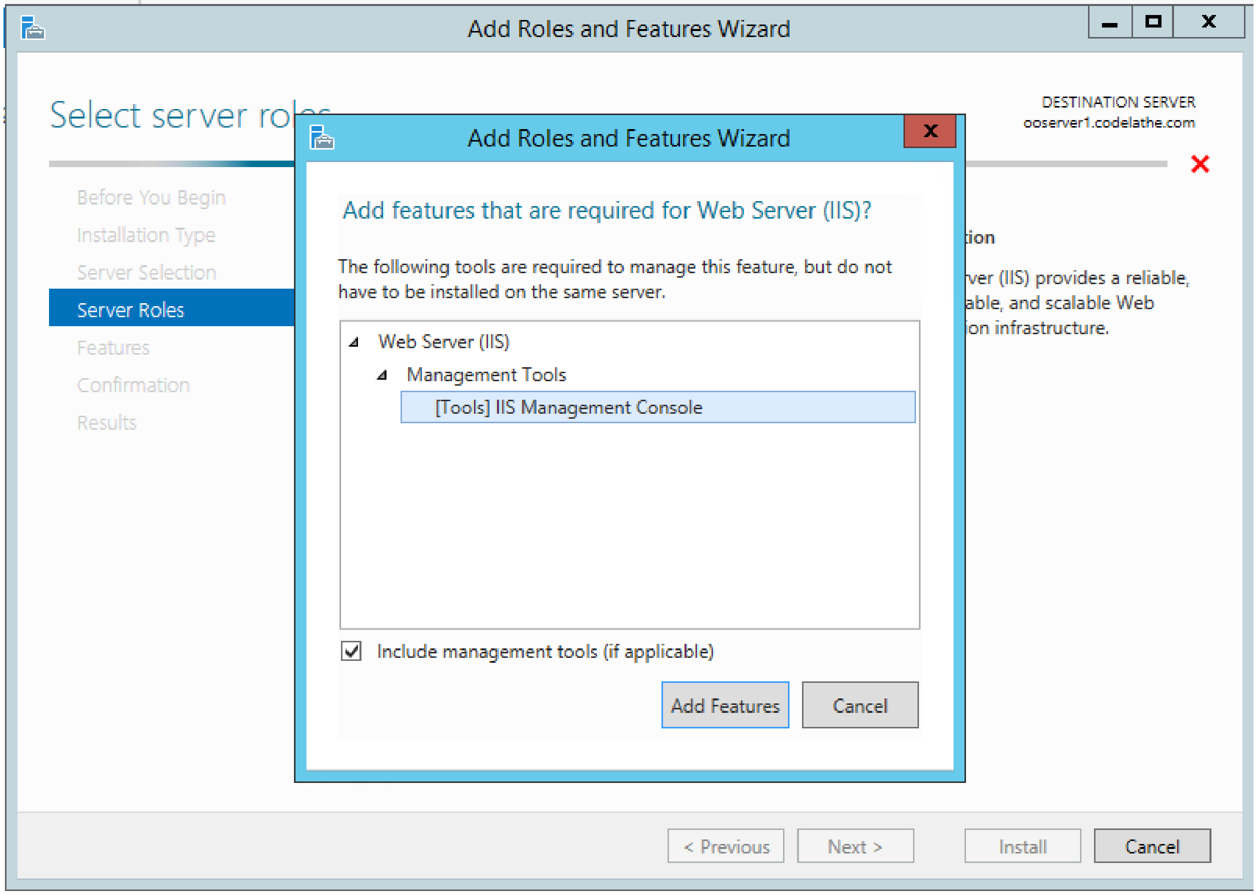
Select installation type

DESTINATION SERVER
ooserver1.codelathe.com

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.



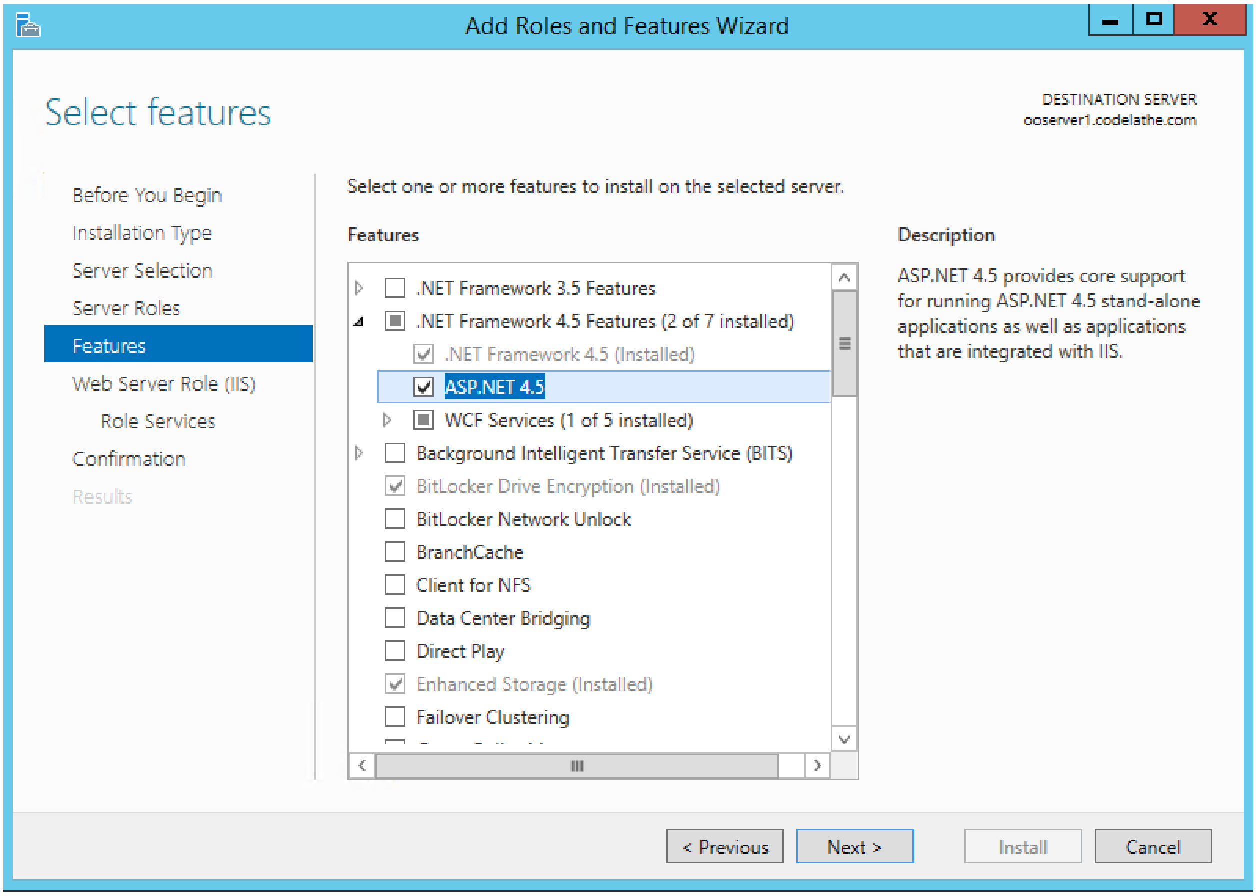
Add Roles and Features Wizard

Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)



Select features

DESTINATION SERVER
ooserver1.codelathe.com

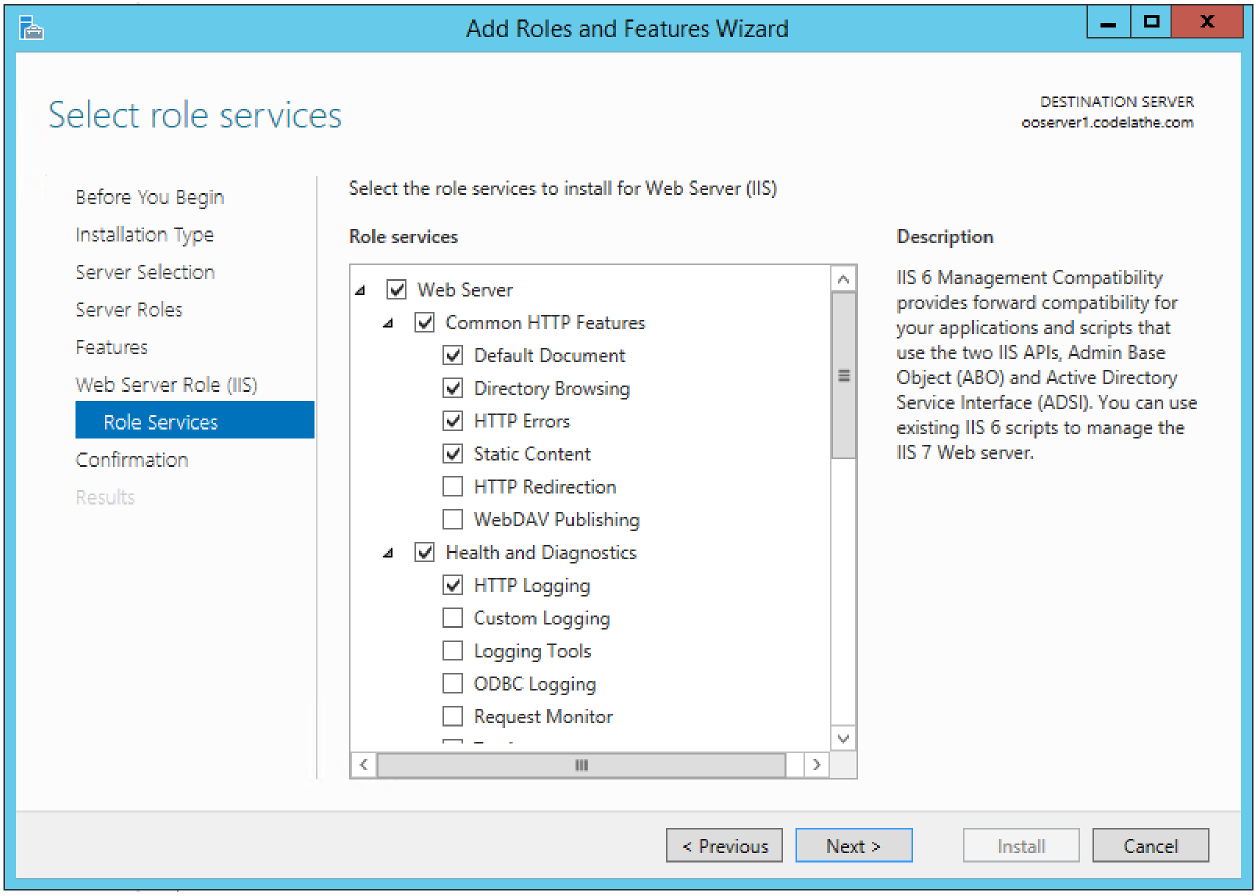
Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5
  - ▣ WCF Services (1 of 5 installed)
- □ Background Intelligent Transfer Service (BITS)
- ☑ BitLocker Drive Encryption (Installed)
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- ☑ Enhanced Storage (Installed)
- □ Failover Clustering

Description

ASP.NET 4.5 provides core support for running ASP.NET 4.5 stand-alone applications as well as applications that are integrated with IIS.



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
ooserver1.codelathe.com

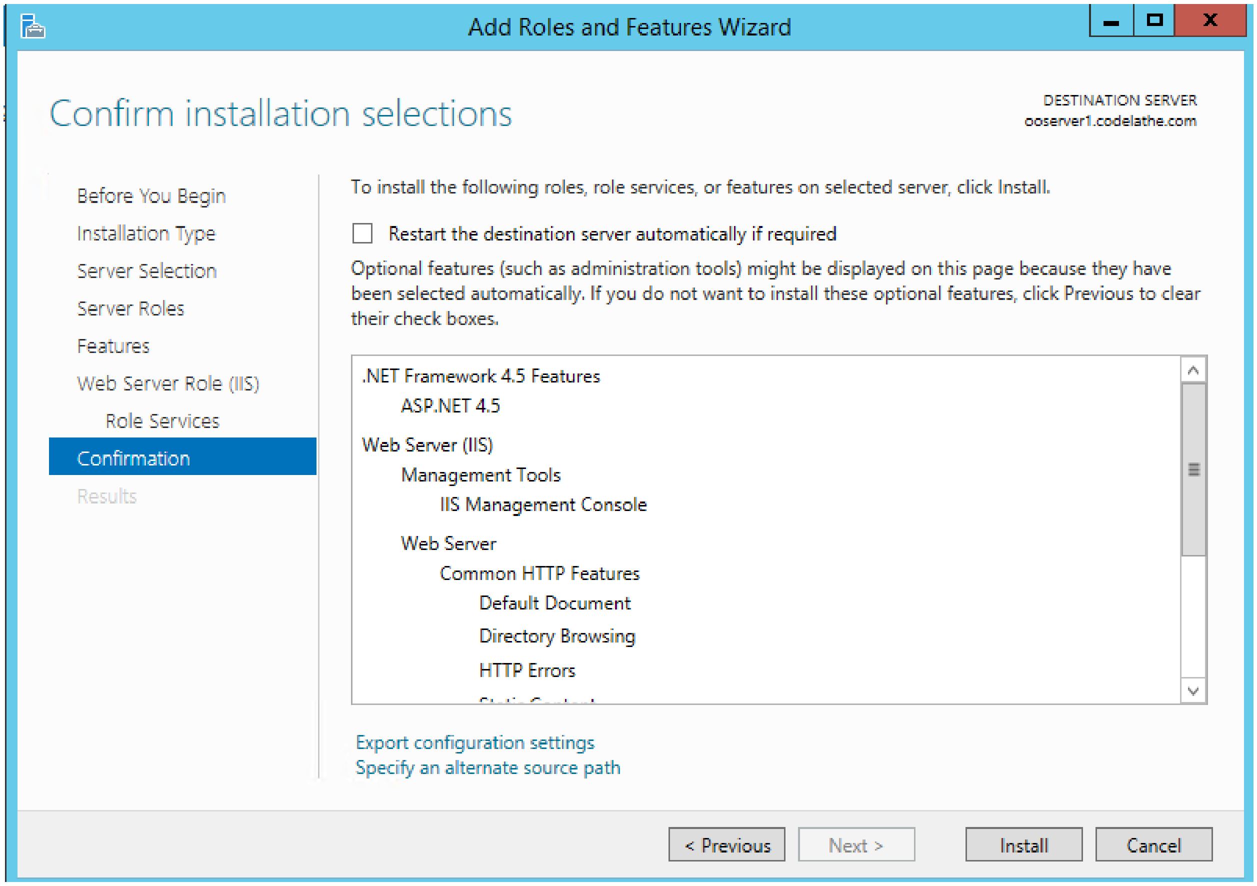
Select the role services to install for Web Server (IIS)

Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - □ Logging Tools
    - □ ODBC Logging
    - □ Request Monitor

Description

IIS 6 Management Compatibility provides forward compatibility for your applications and scripts that use the two IIS APIs, Admin Base Object (ABO) and Active Directory Service Interface (ADSI). You can use existing IIS 6 scripts to manage the IIS 7 Web server.



To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
.NET Framework 4.5 Features
    ASP.NET 4.5
Web Server (IIS)
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
```

Configuring FileCloud To Use Office Online On-Premises Server For Web Edit

Introduction

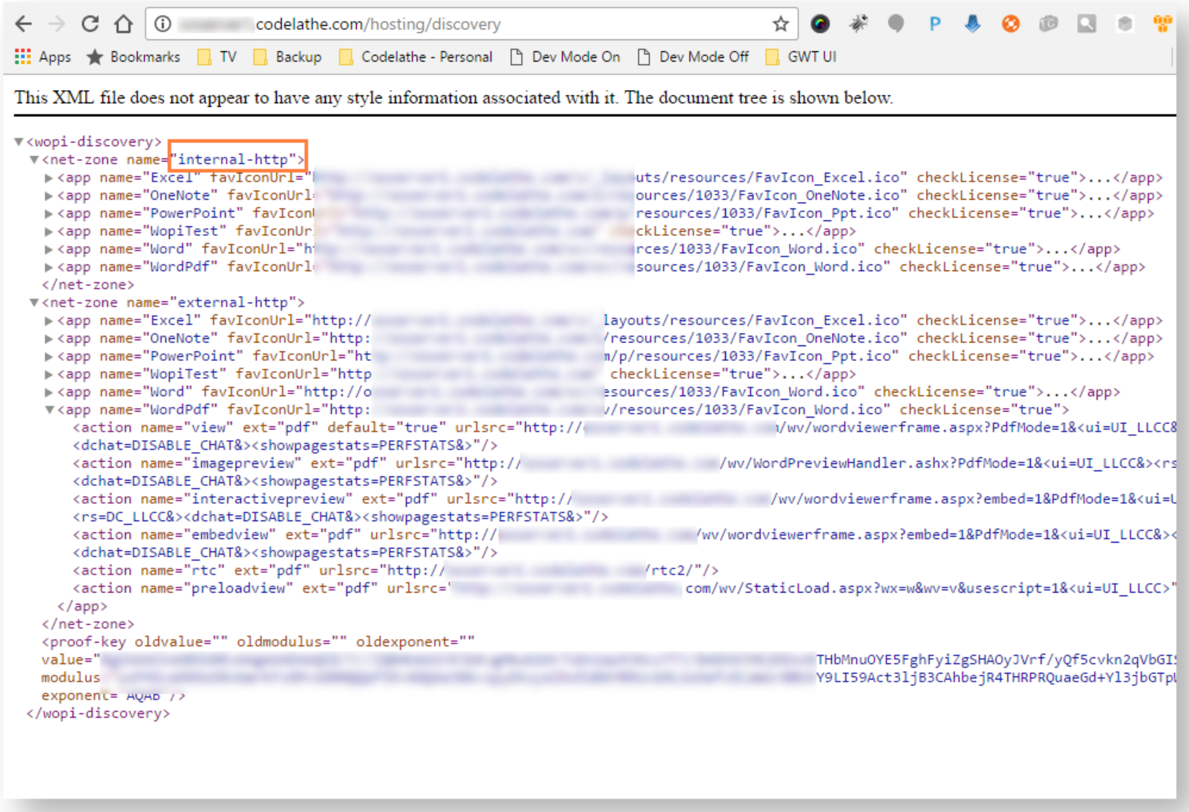
FileCloud supports web based document editing using Microsoft Office Online. FileCloud uses the WOPI protocol to connect to Office Online for web based editing.
This document assumes that the administrator has already installed an Office Online server.

Configuration Tips

- When configuring FileCloud with Office Online on-premises server, please use the default 'admin' user to login into FileCloud admin UI. For security reasons, this configuration is not allowed as a normal user promoted as admin.

Configuring FileCloud With Office Online

1. Navigate to the URL http[s]://IPAddressOfYourOfficeOnlineServer/hosting/discover using a browser. This is the page that contains all the information of various editors supported by Office Online server.
2. From the resulting page, note zone of editors to be used by FileCloud. The selection depends on the requirement of where the web edit feature will be used. In our case, we will choose "internal-http", as we want to offer web-editing only to internal users.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

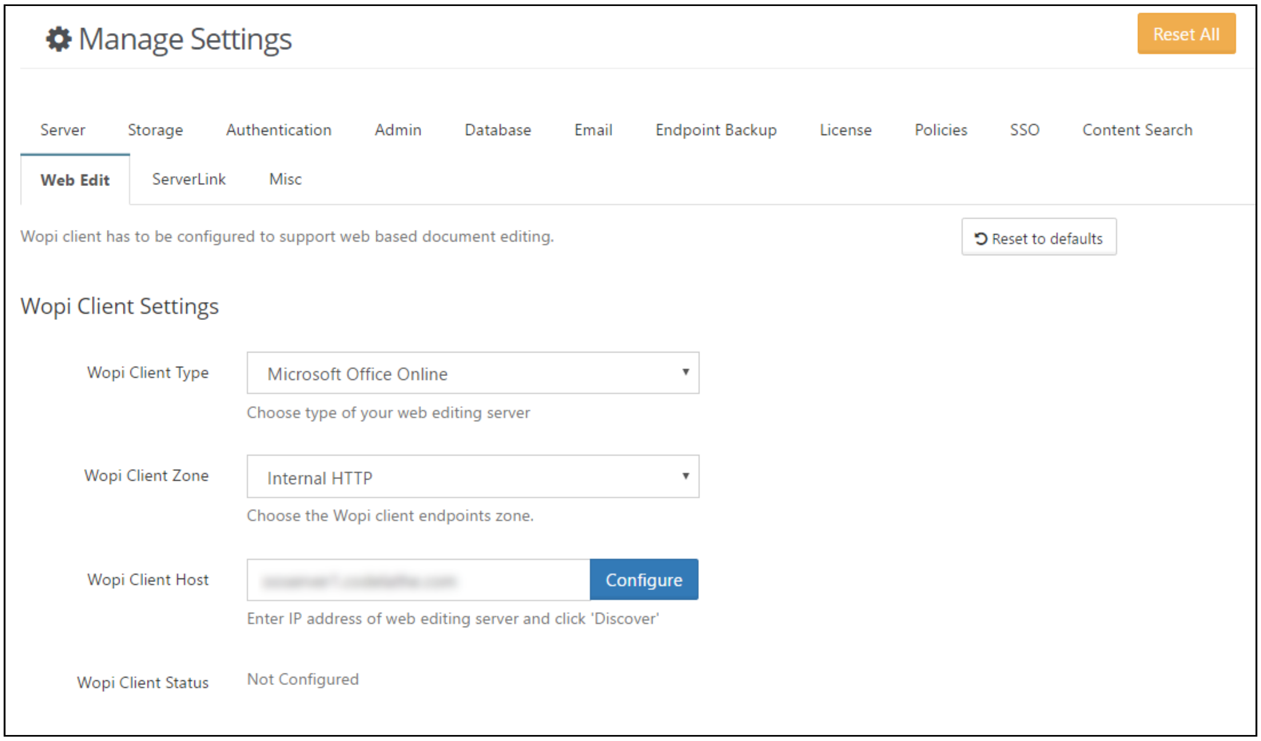
```
▼<wopi-discovery>
 ▼<net-zone name="internal-http">
   ▶<app name="Excel" favIconUrl="[redacted]uts/resources/FavIcon_Excel.ico" checkLicense="true">...</app>
   ▶<app name="OneNote" favIconUrl[redacted]ources/1033/FavIcon_OneNote.ico" checkLicense="true">...</app>
   ▶<app name="PowerPoint" favIcon[redacted]resources/1033/FavIcon_Ppt.ico" checkLicense="true">...</app>
   ▶<app name="WopiTest" favIconUr[redacted]ckLicense="true">...</app>
   ▶<app name="Word" favIconUrl="h[redacted]rces/1033/FavIcon_Word.ico" checkLicense="true">...</app>
   ▶<app name="WordPdf" favIconUrl[redacted]sources/1033/FavIcon_Word.ico" checkLicense="true">...</app>
  </net-zone>
 ▼<net-zone name="external-http">
   ▶<app name="Excel" favIconUrl="http://[redacted]layouts/resources/FavIcon_Excel.ico" checkLicense="true">...</app>
   ▶<app name="OneNote" favIconUrl="http:[redacted]/resources/1033/FavIcon_OneNote.ico" checkLicense="true">...</app>
   ▶<app name="PowerPoint" favIconUrl="ht[redacted]n/p/resources/1033/FavIcon_Ppt.ico" checkLicense="true">...</app>
   ▶<app name="WopiTest" favIconUrl="http[redacted] checkLicense="true">...</app>
   ▶<app name="Word" favIconUrl="http://o[redacted]esources/1033/FavIcon_Word.ico" checkLicense="true">...</app>
   ▼<app name="WordPdf" favIconUrl="http:[redacted]/resources/1033/FavIcon_Word.ico" checkLicense="true">
      <action name="view" ext="pdf" default="true" urlsrc="http://[redacted]/wv/wordviewerframe.aspx?PdfMode=1&<ui=UI_LLCC&
      <dchat=DISABLE_CHAT&><showpagestats=PERFSTATS&>"/>
      <action name="imagepreview" ext="pdf" urlsrc="http://[redacted]/wv/WordPreviewHandler.ashx?PdfMode=1&<ui=UI_LLCC&><rs
      <dchat=DISABLE_CHAT&><showpagestats=PERFSTATS&>"/>
      <action name="interactivepreview" ext="pdf" urlsrc="http://[redacted]/wv/wordviewerframe.aspx?embed=1&PdfMode=1&<ui=U
      <rs=DC_LLCC&><dchat=DISABLE_CHAT&><showpagestats=PERFSTATS&>"/>
      <action name="embedview" ext="pdf" urlsrc="http://[redacted]/wv/wordviewerframe.aspx?embed=1&PdfMode=1&<ui=UI_LLCC&><
      <dchat=DISABLE_CHAT&><showpagestats=PERFSTATS&>"/>
      <action name="rtc" ext="pdf" urlsrc="http://[redacted]/rtc2/"/>
      <action name="preloadview" ext="pdf" urlsrc='[redacted] com/wv/StaticLoad.aspx?wx=w&wv=v&usescript=1&<ui=UI_LLCC>"
    </app>
  </net-zone>
  <proof-key oldvalue="" oldmodulus="" oldexponent=""
  value="[redacted]THbMnuOYE5FghFyiZgSHAOyJVrf/yQf5cvkn2qVbGI
  modulus[redacted]Y9LI59Act3ljB3CAhbejR4THRPRQuaeGd+Yl3jbGTp
  exponent= AQAB />
</wopi-discovery>
```

3. Ensure that the Office online server has access to the FileCloud server (To verify: navigate to FileCloud user login page from office online server).
4. Add the Office Online server to the Content Security policy in the .htaccess file.
   a. Open the .htacess file:
      Windows: C:\xampp\htdocs\.htaccess
      Linux: /var/www/html/.htaccess
   b. Find the line: **Header set Content-Security-Policy**, and add your Office Online server url without http or https, for example o**os.company.com** to the url's listed for **default-src**, **script-src**, **frame-src**, and **img-src**:

```
Header set Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com
*.core.windows.net oos.company.com www.google.com
http://127.0.0.1:34320/v1/fileassociations; style-src 'unsafe-inline' 'self';script-src 'unsafe-
inline' 'unsafe-eval' 'self' www.google.com oos.company.com www.gstatic.com
teams.microsoft.com *.teams.microsoft.com *.skype.com;frame-src 'self' www.google.com
oos.company.com *.live.com docs.google.com accounts.google.com; font-src 'self' data:;img-
src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com
*.core.windows.net oos.company.com *.office.net; frame-ancestors 'self'
teams.microsoft.com *.teams.microsoft.com *.skype.com;
```

   c. Save your changes.

5. Now login into FileCloud server admin UI(as the default 'admin' user), which needs to integrate with Office Online to offer web editing.
6. Navigate to Settings -> Web edit tab. Select "Microsoft Office Online" as Wopi Client Type, "Internal HTTP" as Wopi Client Zone (select other option as required), IP address/URL for office online server as Wopi client host. On entering the details click on configured.



Wopi client has to be configured to support web based document editing.

Wopi Client Settings

Wopi Client Type: Microsoft Office Online

Choose type of your web editing server

Wopi Client Zone: Internal HTTP

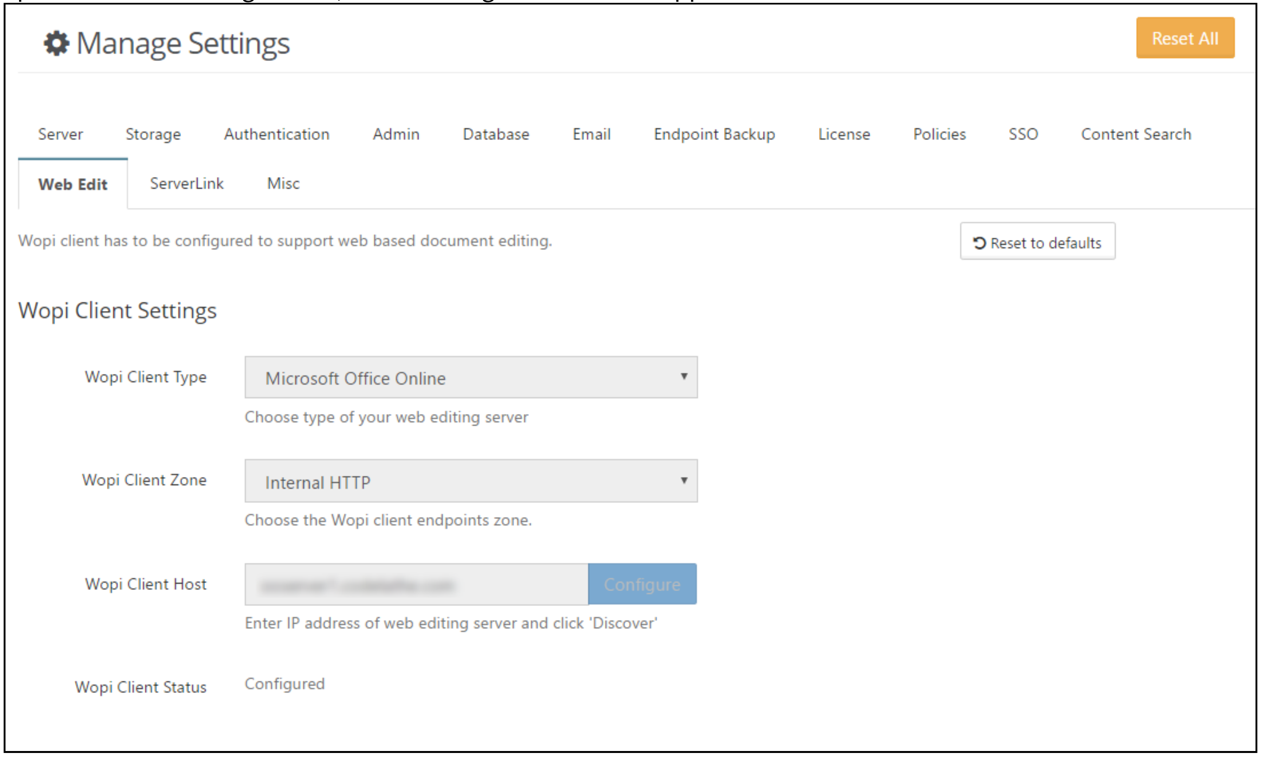
Choose the Wopi client endpoints zone.

Wopi Client Host: [redacted]

Enter IP address of web editing server and click 'Discover'

Wopi Client Status: Not Configured

7. Upon successful configuration, the following screen should appear.



Wopi client has to be configured to support web based document editing.

Wopi Client Settings

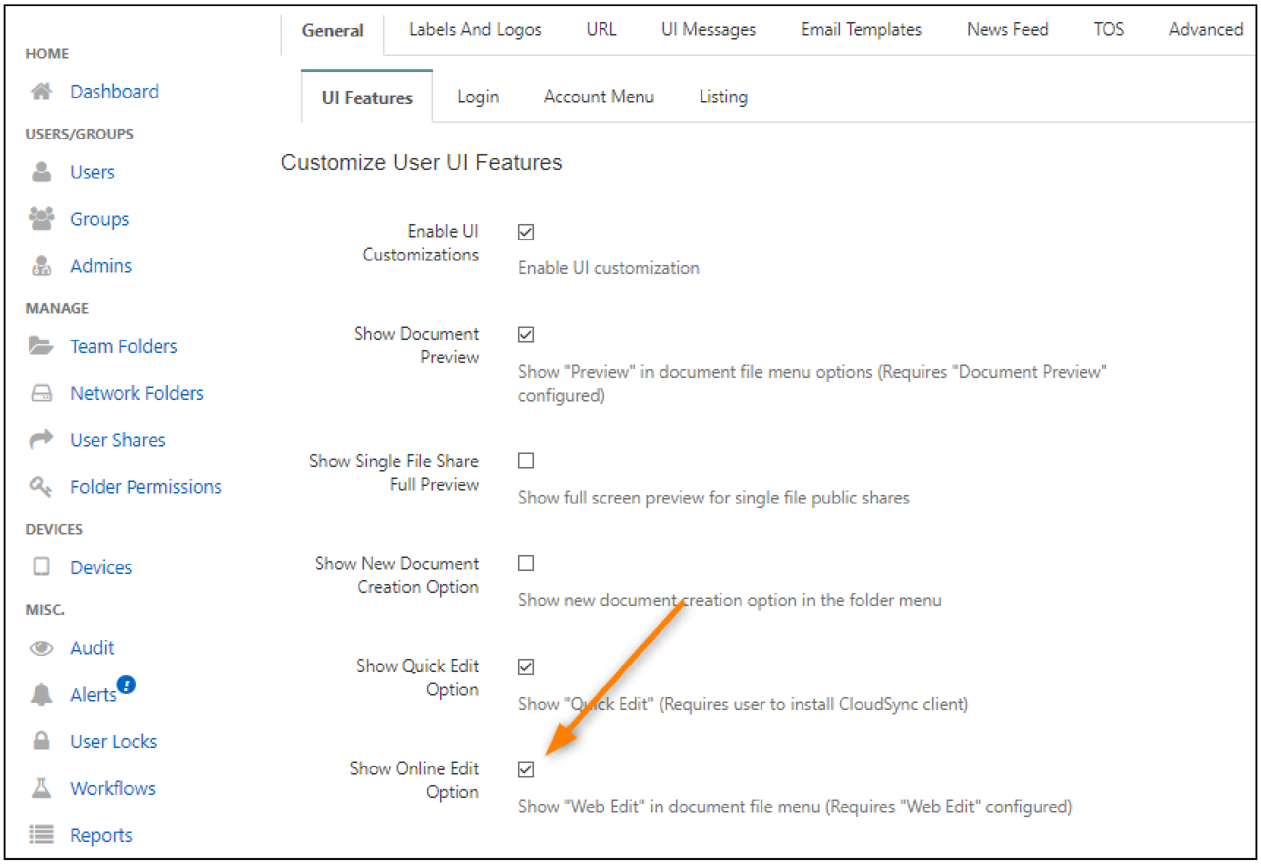
Wopi Client Type: Microsoft Office Online
Choose type of your web editing server

Wopi Client Zone: Internal HTTP
Choose the Wopi client endpoints zone.

Wopi Client Host: [redacted]
Enter IP address of web editing server and click 'Discover'

Wopi Client Status: Configured

8. Now that FileCloud server is configured with office online server, administrator might need to enable the web edit option for users.
   To enable web edit in user UI, navigate to Customizations -> General -> UI Features tab and check the option "Show Online Edit Option". Click "Save" button to save the changes.



Customize User UI Features

Enable UI Customizations ☑ Enable UI customization

Show Document Preview ☑ Show "Preview" in document file menu options (Requires "Document Preview" configured)

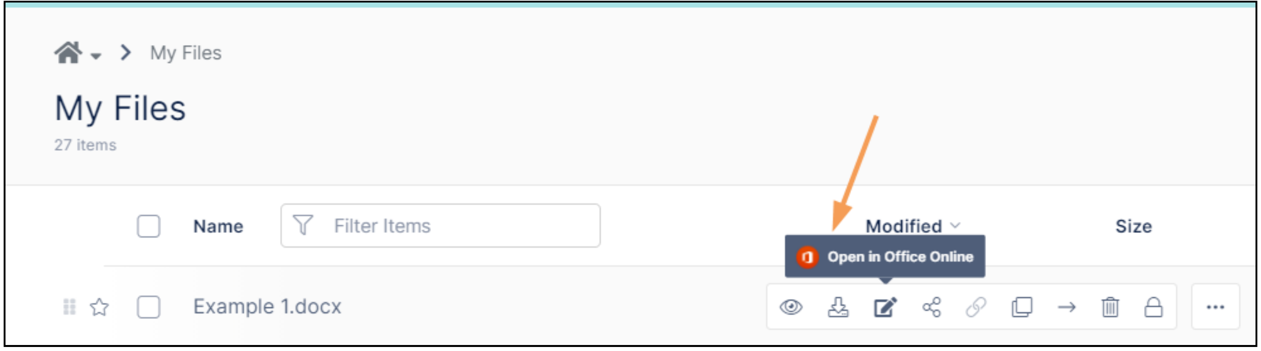
Show Single File Share Full Preview □ Show full screen preview for single file public shares

Show New Document Creation Option □ Show new document creation option in the folder menu

Show Quick Edit Option ☑ Show "Quick Edit" (Requires user to install CloudSync client)

Show Online Edit Option ☑ Show "Web Edit" in document file menu (Requires "Web Edit" configured)

9. Now login into the user UI and hover over an editable Office document. Hover over the Web Edit icon, and ensure that you see the Office icon and the tooltip **Open in Office Online**.



10. Click the icon and confirm that the document opens in its Office Online editor.

Web Editing With Collabora Code

This section explains how to configure FileCloud to use Collabora Code for web editing.

Prerequisites

- The Collabora server must be installed. For help, see Collabora's Installation Guide.
- Reverse Proxy must be set up for the Collabora URL. For help, see Collabora's Installation Guide, Proxy Settings.

In this section

Configuring FileCloud To Use Collabora CODE For Web Edit

Introduction

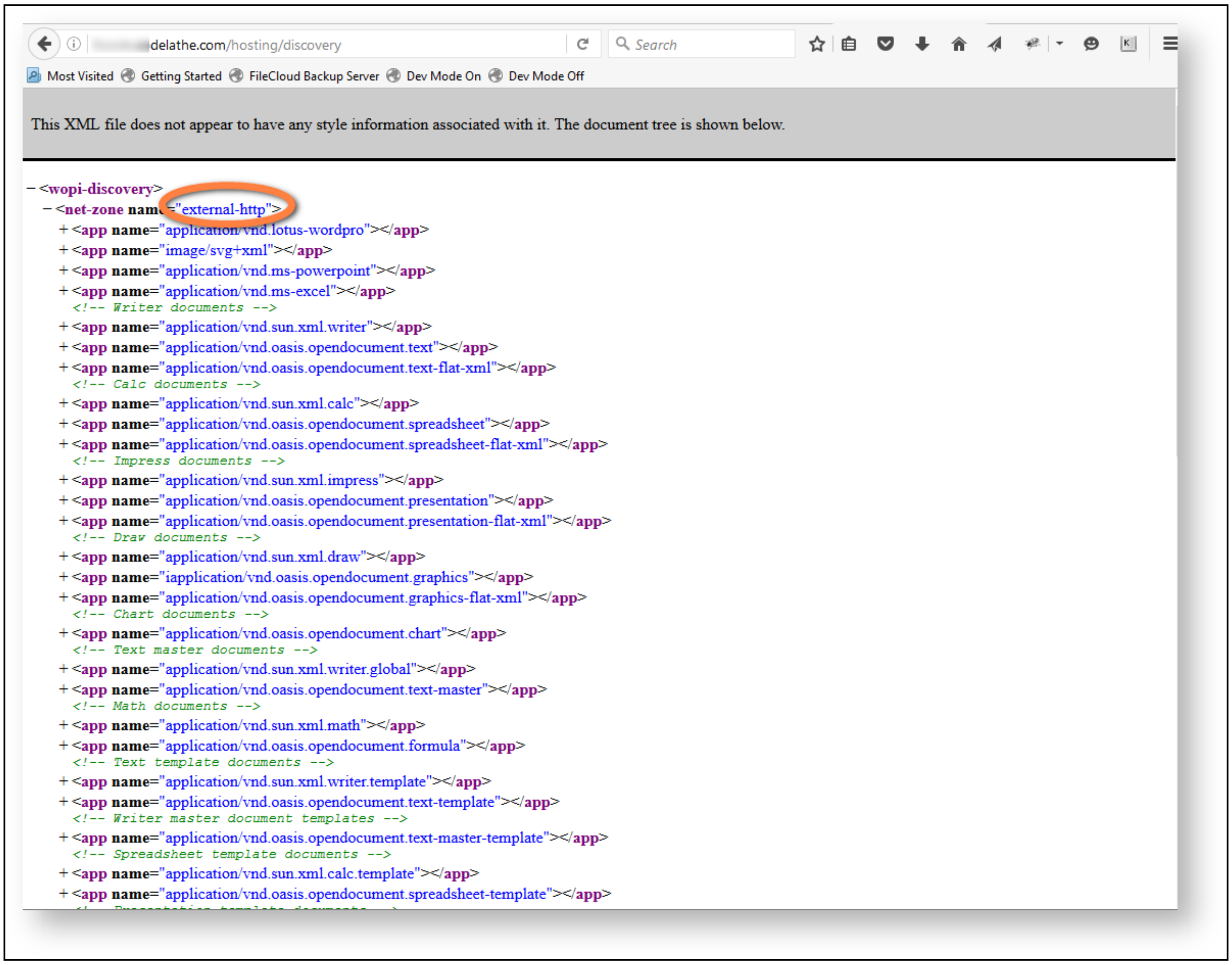
Document Web Edit support is available in FileCloud starting from FileCloud 14.0. FileCloud supports web based document editing using Collabora CODE. FileCloud uses the WOPI protocol to connect to office online for web based editing.

> ⓘ This document assumes that the administrator has already installed Collabora CODE completely and ready for use.
> For Collabora CODE installation, refer to the official Collabora documentation at:
> https://sdk.collaboraonline.com/docs/installation/CODE_Docker_image.html
> https://sdk.collaboraonline.com/docs/installation/Proxy_settings.html#reverse-proxy-with-apache-2-webserver

> **Configuration Tips**
>
> - When configuring FileCloud with Collabora CODE, please use the default 'admin' user to login into FileCloud admin UI. For security reasons, this configuration is not allowed as a normal user promoted as admin.

Configuring FileCloud With Collabora CODE

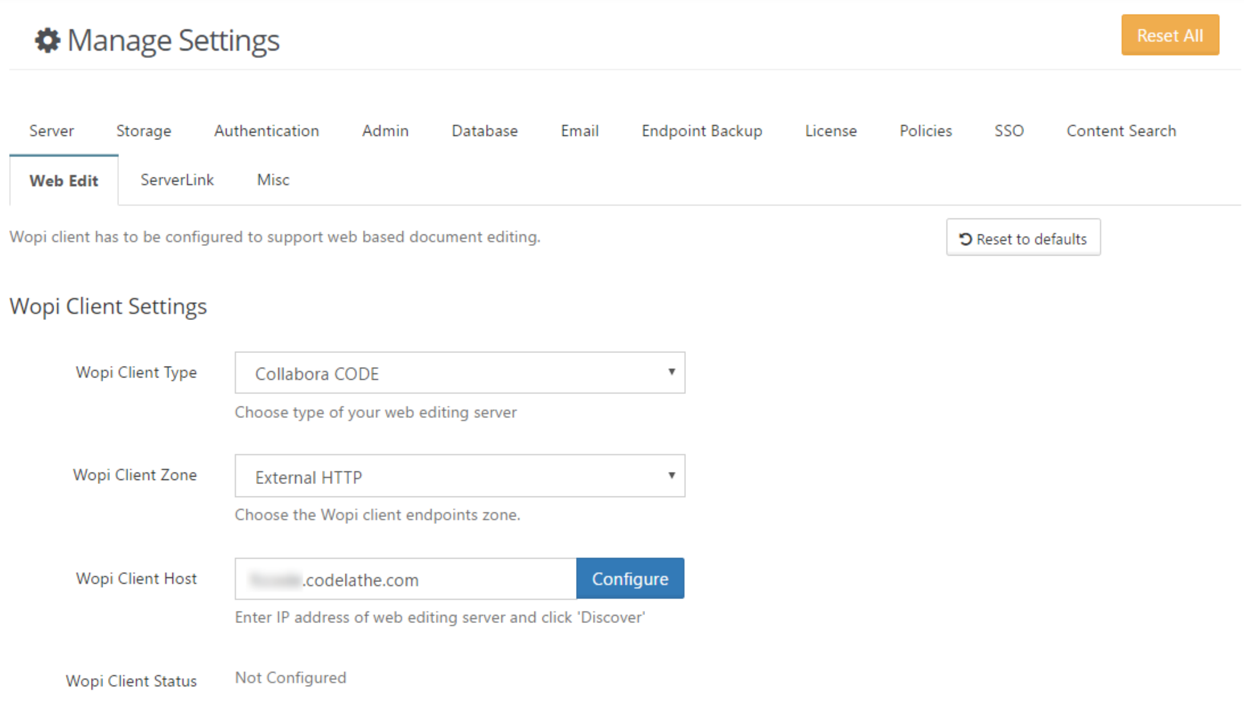
1. Navigate to the URL http[s]://IPAddressOfYourCODEServer/hosting/discovery using a browser. This is the page that contains all the information of various editors supported by CODE server.
2. From the resulting page, note zone of editors to be used by FileCloud. The selection depends on the requirement of where the web edit feature will be used. In our case, we will choose "external-http", as we want to offer web-editing to external users.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
– <wopi-discovery>
  – <net-zone name="external-http">
    + <app name="application/vnd.lotus-wordpro"></app>
    + <app name="image/svg+xml"></app>
    + <app name="application/vnd.ms-powerpoint"></app>
    + <app name="application/vnd.ms-excel"></app>
      <!-- Writer documents -->
    + <app name="application/vnd.sun.xml.writer"></app>
    + <app name="application/vnd.oasis.opendocument.text"></app>
    + <app name="application/vnd.oasis.opendocument.text-flat-xml"></app>
      <!-- Calc documents -->
    + <app name="application/vnd.sun.xml.calc"></app>
    + <app name="application/vnd.oasis.opendocument.spreadsheet"></app>
    + <app name="application/vnd.oasis.opendocument.spreadsheet-flat-xml"></app>
      <!-- Impress documents -->
    + <app name="application/vnd.sun.xml.impress"></app>
    + <app name="application/vnd.oasis.opendocument.presentation"></app>
    + <app name="application/vnd.oasis.opendocument.presentation-flat-xml"></app>
      <!-- Draw documents -->
    + <app name="application/vnd.sun.xml.draw"></app>
    + <app name="iapplication/vnd.oasis.opendocument.graphics"></app>
    + <app name="application/vnd.oasis.opendocument.graphics-flat-xml"></app>
      <!-- Chart documents -->
    + <app name="application/vnd.oasis.opendocument.chart"></app>
      <!-- Text master documents -->
    + <app name="application/vnd.sun.xml.writer.global"></app>
    + <app name="application/vnd.oasis.opendocument.text-master"></app>
      <!-- Math documents -->
    + <app name="application/vnd.sun.xml.math"></app>
    + <app name="application/vnd.oasis.opendocument.formula"></app>
      <!-- Text template documents -->
    + <app name="application/vnd.sun.xml.writer.template"></app>
    + <app name="application/vnd.oasis.opendocument.text-template"></app>
      <!-- Writer master document templates -->
    + <app name="application/vnd.oasis.opendocument.text-master-template"></app>
      <!-- Spreadsheet template documents -->
    + <app name="application/vnd.sun.xml.calc.template"></app>
    + <app name="application/vnd.oasis.opendocument.spreadsheet-template"></app>
      <!-- Presentation template documents -->
```

3. Ensure that the CODE server has access to the FileCloud server (To verify: navigate to FileCloud user login page from code server).
4. Now login into FileCloud server admin UI(as the default 'admin' user), which needs to integrate with CODE for web editing.
5. Navigate to Settings -> Web edit tab. Select "Collabora CODE" as Wopi Client Type, "External HTTP" as Wopi Client Zone (select other option as required), IP address/URL for office online server as Wopi client host.
   On entering the details click on configured.



Wopi client has to be configured to support web based document editing.

Wopi Client Settings

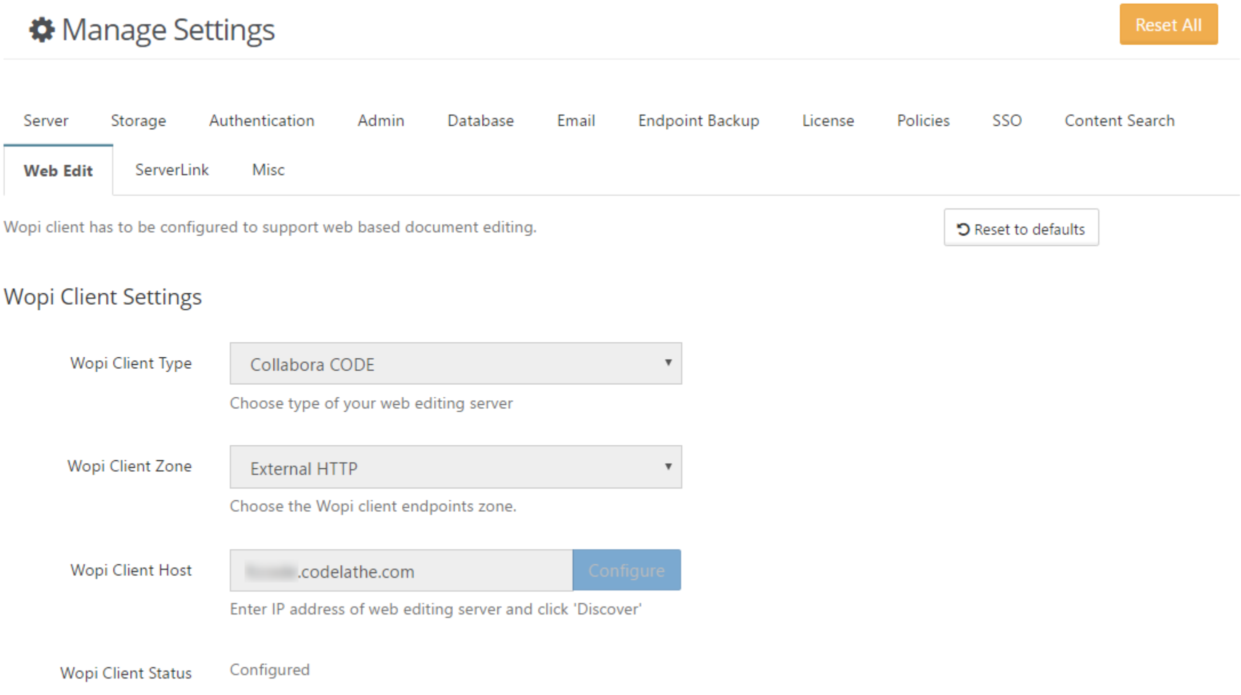
Wopi Client Type: Collabora CODE
Choose type of your web editing server

Wopi Client Zone: External HTTP
Choose the Wopi client endpoints zone.

Wopi Client Host: [redacted].codelathe.com
Enter IP address of web editing server and click 'Discover'

Wopi Client Status: Not Configured

6. Upon successful configuration, the following screen should appear.



Wopi client has to be configured to support web based document editing.

Wopi Client Settings

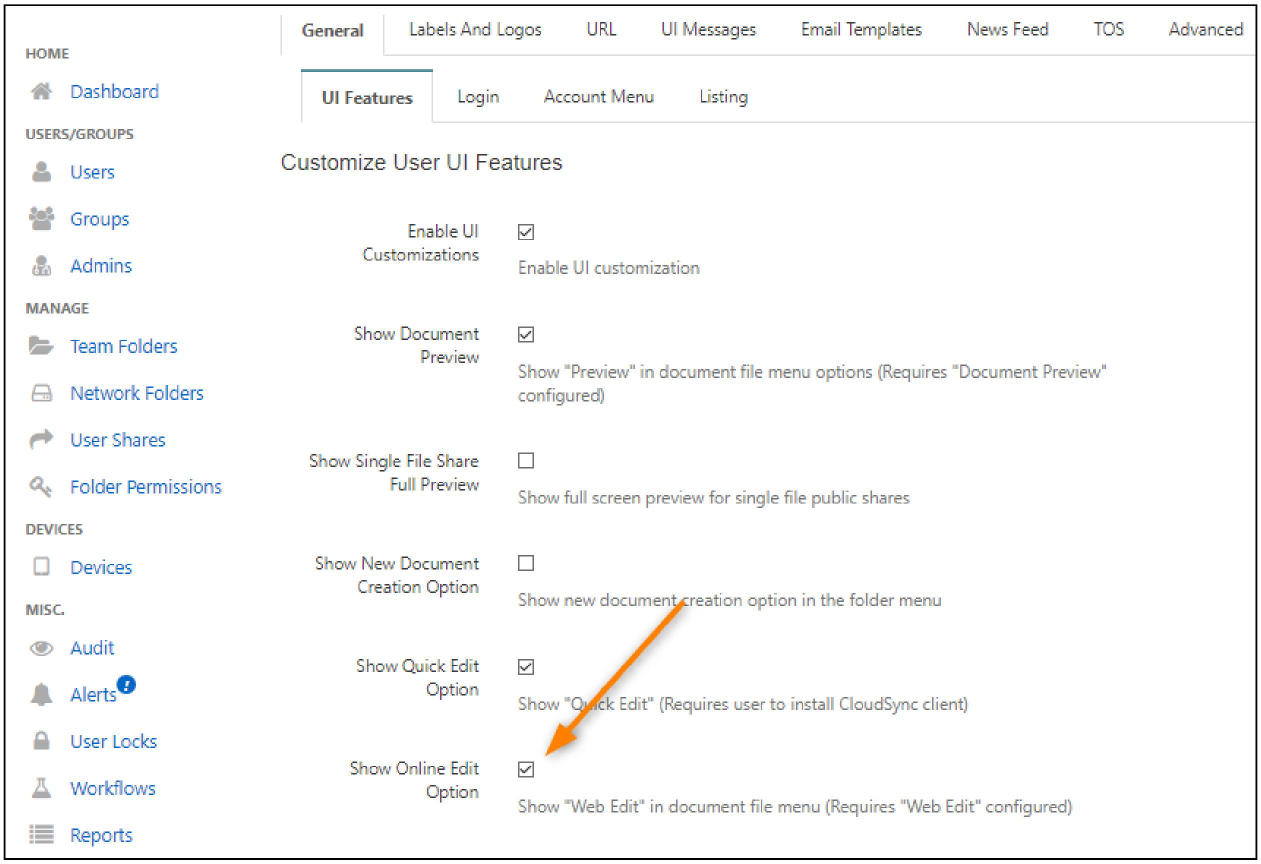
Wopi Client Type: Collabora CODE
Choose type of your web editing server

Wopi Client Zone: External HTTP
Choose the Wopi client endpoints zone.

Wopi Client Host: [redacted].codelathe.com
Enter IP address of web editing server and click 'Discover'

Wopi Client Status: Configured

7. Now that FileCloud server is configured with office online server, administrator might need to enable the web edit option for users.
   To enable web edit in user UI, navigate to Customizations -> General -> UI Features tab and check the option "Show Online Edit Option". Click "Save" button to save the changes.



Customize User UI Features

Enable UI Customizations ☑ Enable UI customization

Show Document Preview ☑ Show "Preview" in document file menu options (Requires "Document Preview" configured)

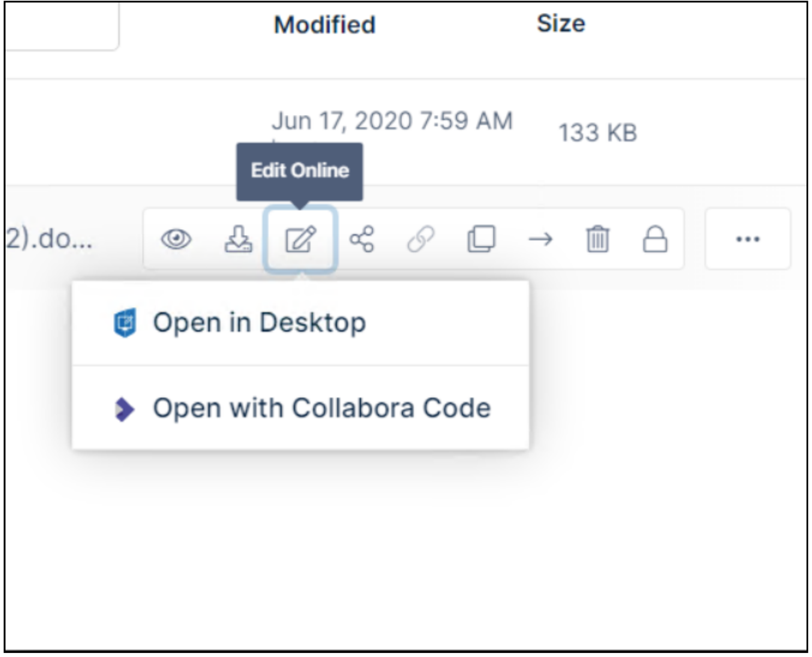
Show Single File Share Full Preview □ Show full screen preview for single file public shares

Show New Document Creation Option □ Show new document creation option in the folder menu

Show Quick Edit Option ☑ Show "Quick Edit" (Requires user to install CloudSync client)

Show Online Edit Option ☑ Show "Web Edit" in document file menu (Requires "Web Edit" configured)

8. Now log in to the user portal, hover over a document and click the **Web Edit** icon. Ensure the selected document opens in the code web editor.



Configuring FileCloud to use Collabora CODE for File Creation

Starting in FileCloud 19.3, web-based file creation using Collabora CODE is supported.

To configure FileCloud to use Collabora Code for file creation:

1. Configure FileCloud to use Collabora CODE according to the instructions in Configuring FileCloud To Use Collabora CODE For Web Edit.
2. Create a folder for storing templates such as *C:\documenttemplates.*
3. In the folder, create empty Office templates, each having the filename *template*, for example, *template.docx, template.pptx, template.xlsx.*
4. In **C:\xampp\htdocs\config\cloudconfig.php** add the following line:
   define("WOPI_CLIENT_TEMPLATE_DIR", "C:\documenttemplates");
   You can now create files that match the template types you have added.

Web Editing with OnlyOffice

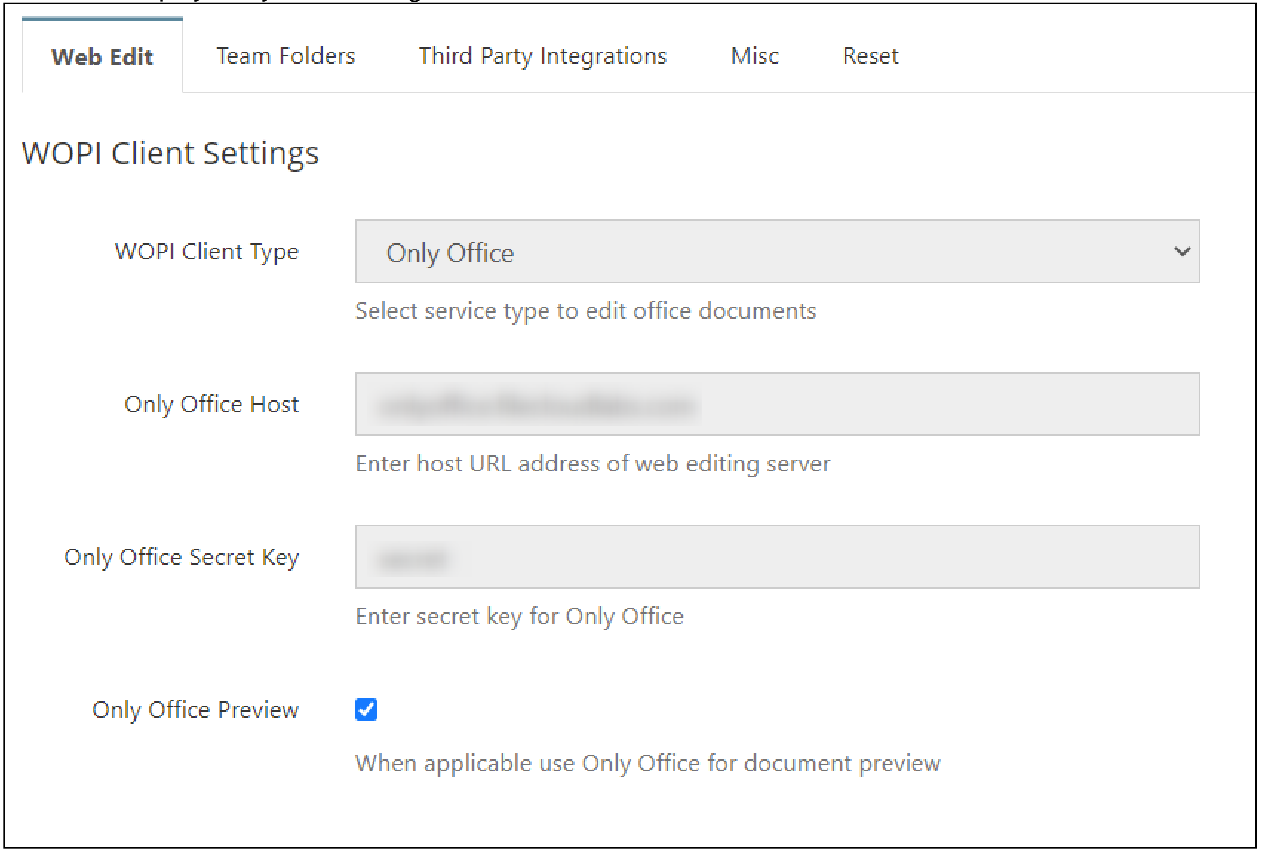
⚠ For OnlyOffice integration to be effective, the OnlyOffice URL must be accessible over HTTPS with a valid SSL certificate and chain certificate.

FileCloud supports web based document editing using OnlyOffice. The following procedures assume you have already installed OnlyOffice.

Configuring FileCloud with OnlyOffice

1. Open In the FileCloud Admin portal, go to **Settings > Web Edit**.

2. In **WOPI Client Type**, choose **Only Office**.
   The screen displays OnlyOffice settings.



WOPI Client Settings

WOPI Client Type: Only Office

Select service type to edit office documents

Only Office Host: [redacted]

Enter host URL address of web editing server

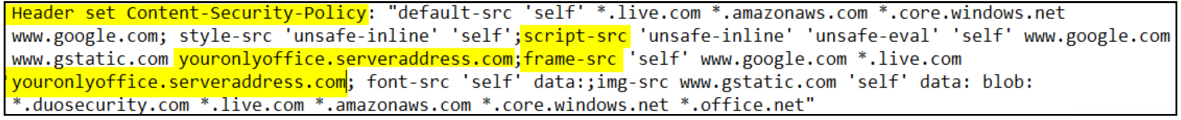
Only Office Secret Key: [redacted]

Enter secret key for Only Office

Only Office Preview: ☑

When applicable use Only Office for document preview

3. Enter the **Only Office Host** and **Only Office Secret Key.**
4. To preview as well as edit supported file types in OnlyOffice, check **Only Office Preview**.
5. Click **Save**.
6. Add the OnlyOffice Server to the Content Security Policy in the .htaccess file.
   a. Open the .htacess file:
      Windows: C:\xampp\htdocs\.htaccess
      Linux: /var/www/html/.htaccess
   b. Find the line: **Header set Content-Security-Policy**, and add your url without http or https, for example **youronlyoffice.serveraddress.com** to the url's listed for **script-src** and **frame-src**:

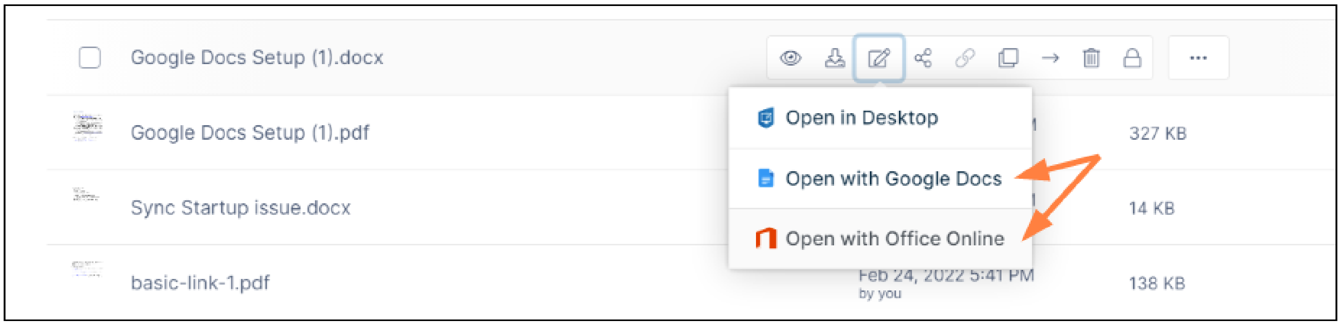


```
Header set Content-Security-Policy: "default-src 'self' *.live.com *.amazonaws.com *.core.windows.net
www.google.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com
www.gstatic.com youronlyoffice.serveraddress.com;frame-src 'self' www.google.com *.live.com
youronlyoffice.serveraddress.com; font-src 'self' data:;img-src www.gstatic.com 'self' data: blob:
*.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net"
```

   c. Save your changes.
      Now users can Web edit with OnlyOffice.

Web Editing with Google Apps

Beginning with FileCloud 21.3, you can integrate FileCloud with Google Apps to make an additional Web Edit option. Google Apps cannot replace your current WOPI client, but may be added as an additional option, so that when users select to Web Edit docx, xlsx, pptx files, both the WOPI client and Google Docs are listed as options for opening it:



In FileCloud's mobile apps, files can be viewed but not edited in Google Apps.

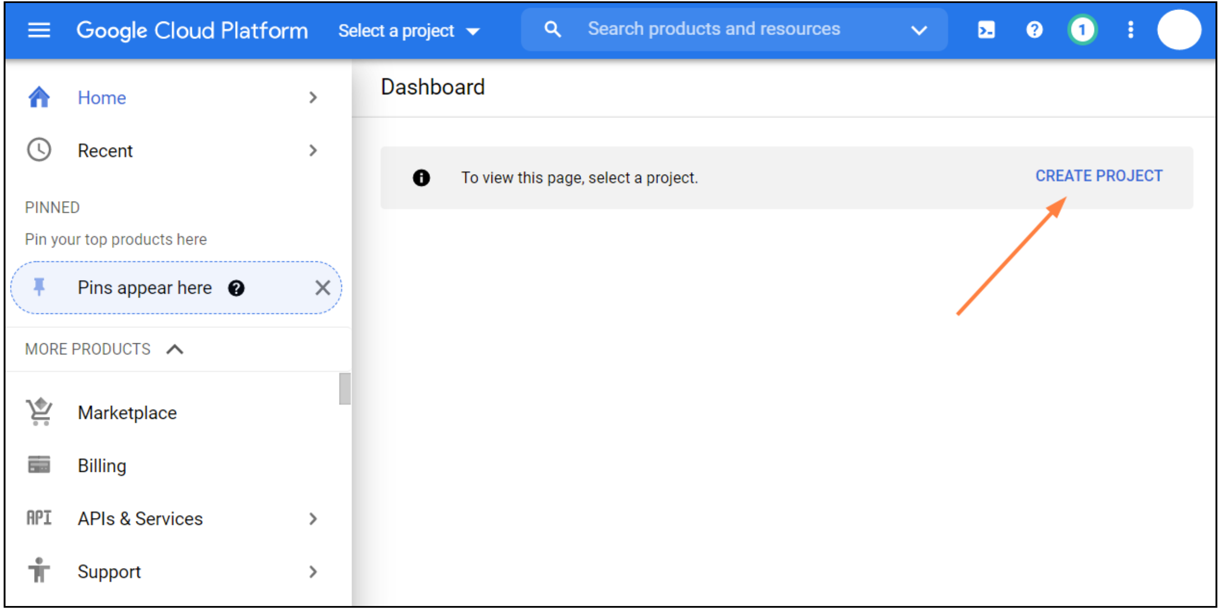
- Editing of some large files is not supported in Google Apps. See Files you can store in Google Drive for specific size limitations.
- To open a Google Apps editor in incognito windows, you may first have to grant Google Docs the correct permissions or unblock third party cookies.

To integrate with Google Apps:

Set up Google Apps - FileCloud integration in the Google Cloud platform:

You must have a Google account that you can use to sign in to the Google Cloud Console in order to integrate your system with Google Apps.

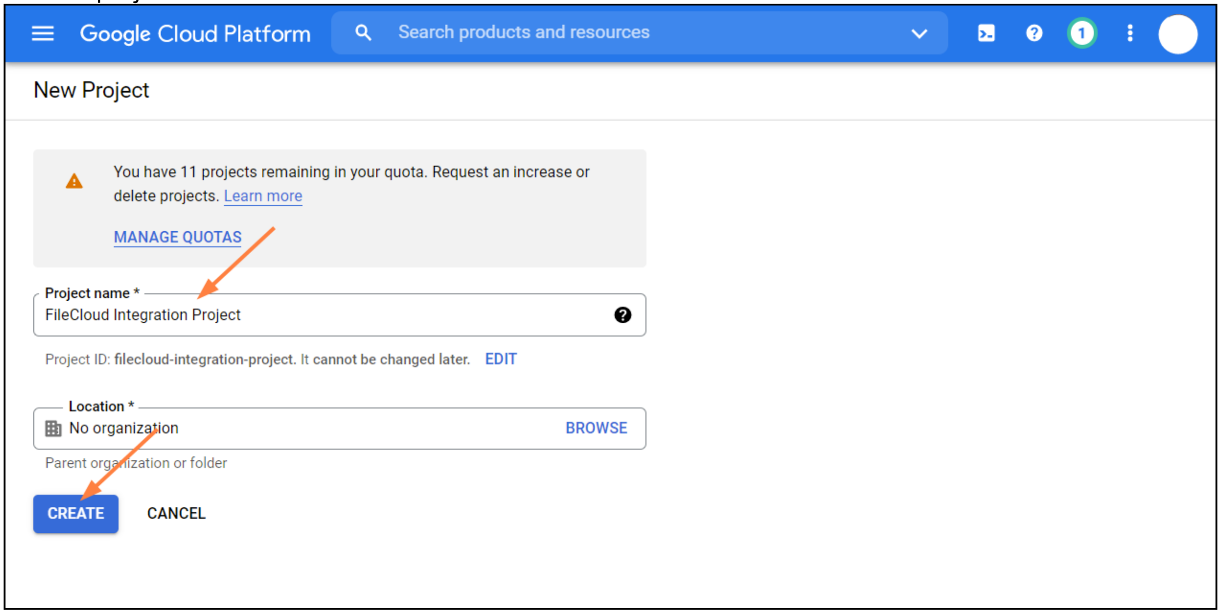
1. Access the Google Cloud Console at https://console.cloud.google.com and sign in.
2. Go to **Home > Dashboard**.
3. Click **Create Project**.



To view this page, select a project.

A **New Project** screen opens.

4. Give the project a name and click **Create**.



You have 11 projects remaining in your quota. Request an increase or delete projects. Learn more

Project name * FileCloud Integration Project

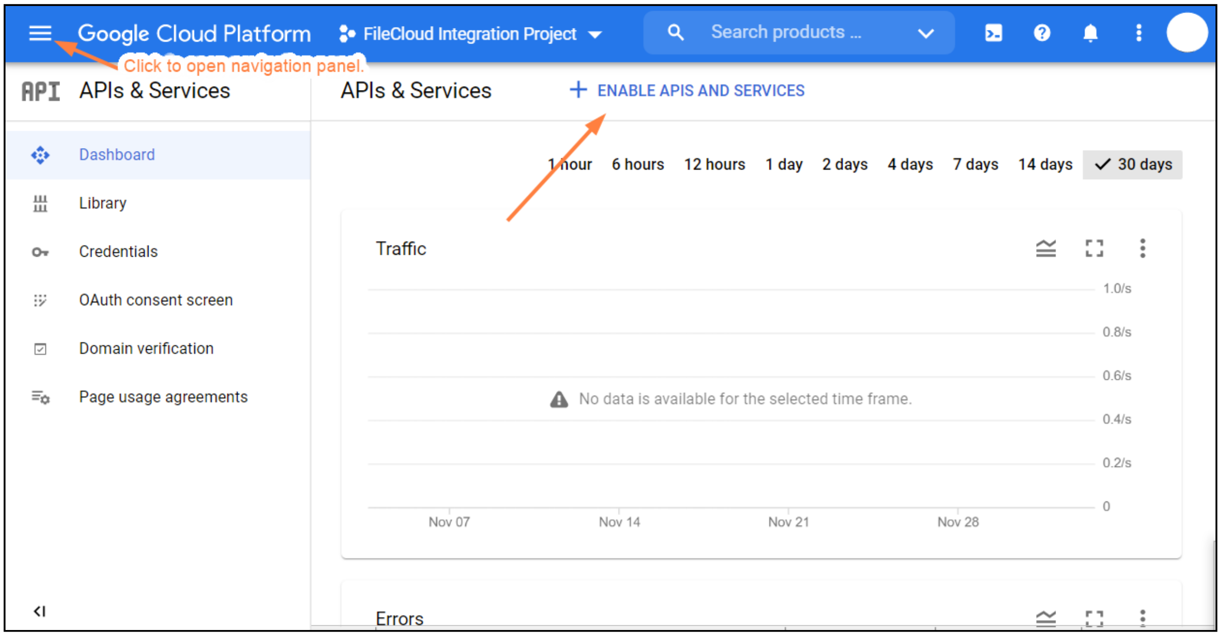
Project ID: filecloud-integration-project. It cannot be changed later.

Location * No organization

Parent organization or folder

The project opens in the dashboard.

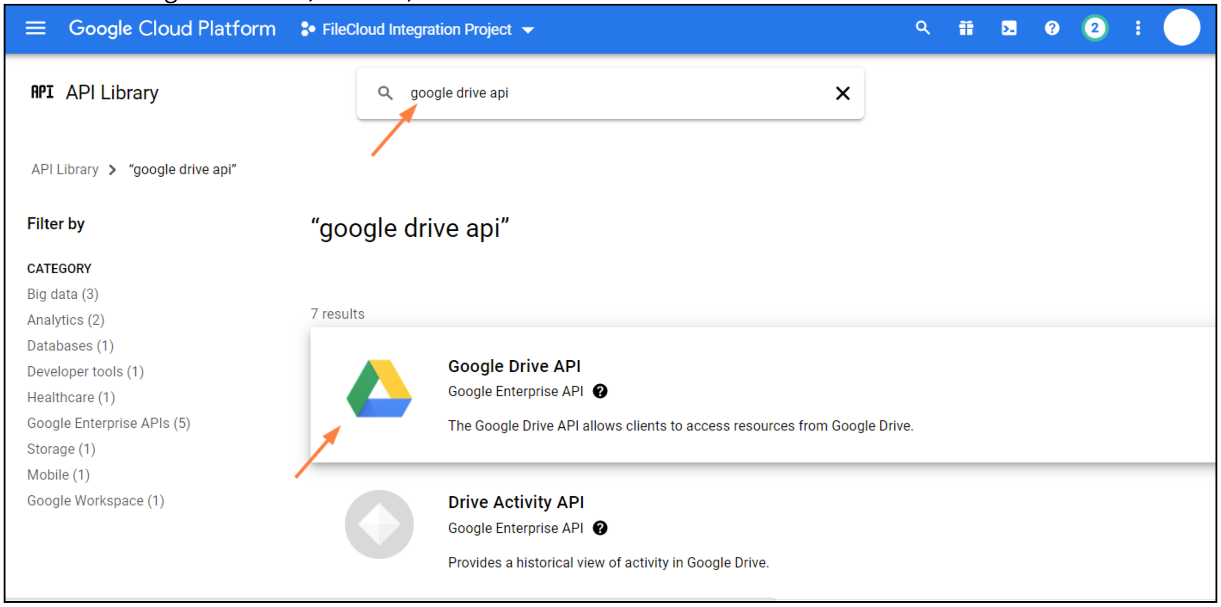
5. In the navigation panel, click **APIs & Services > Dashboard**.
(If the navigation panel is not visible, click the three bars in the upper-left corner of the screen to open it.)
6. Click **Enable APIs and Services**.



Click to open navigation panel.

No data is available for the selected time frame.

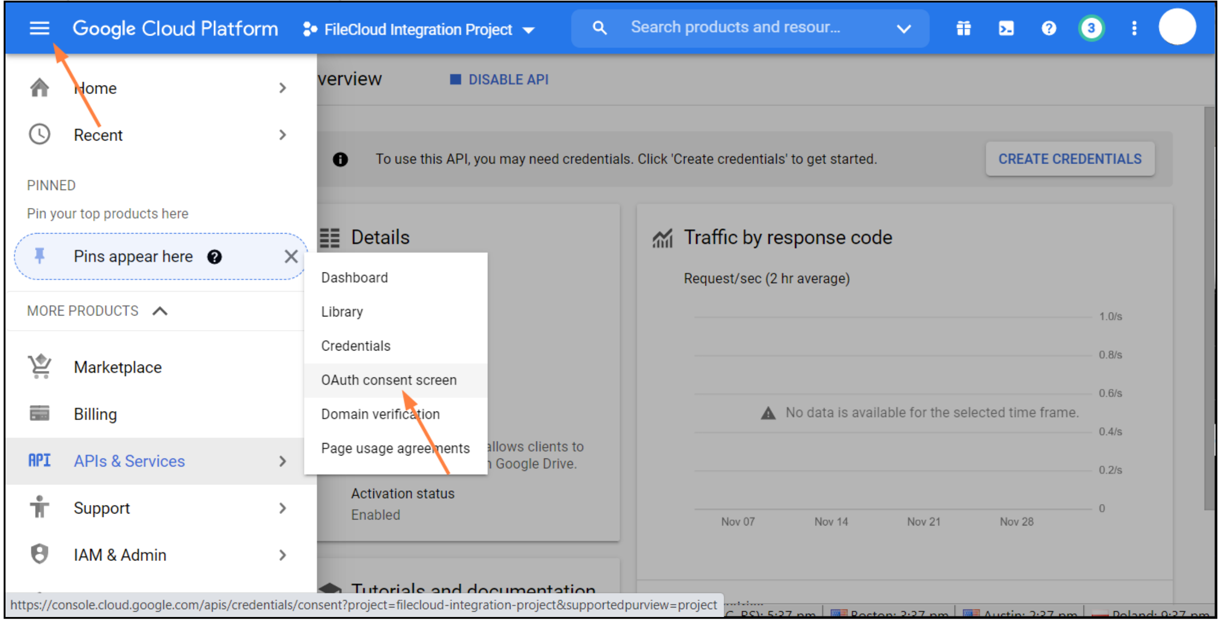
7. Search for Google Drive API , select it, and enable it.



The Google Drive API allows clients to access resources from Google Drive.

Provides a historical view of activity in Google Drive.

8. Then go back to the main navigation pane, and choose **APIs & Services > OAuth consent screen**.



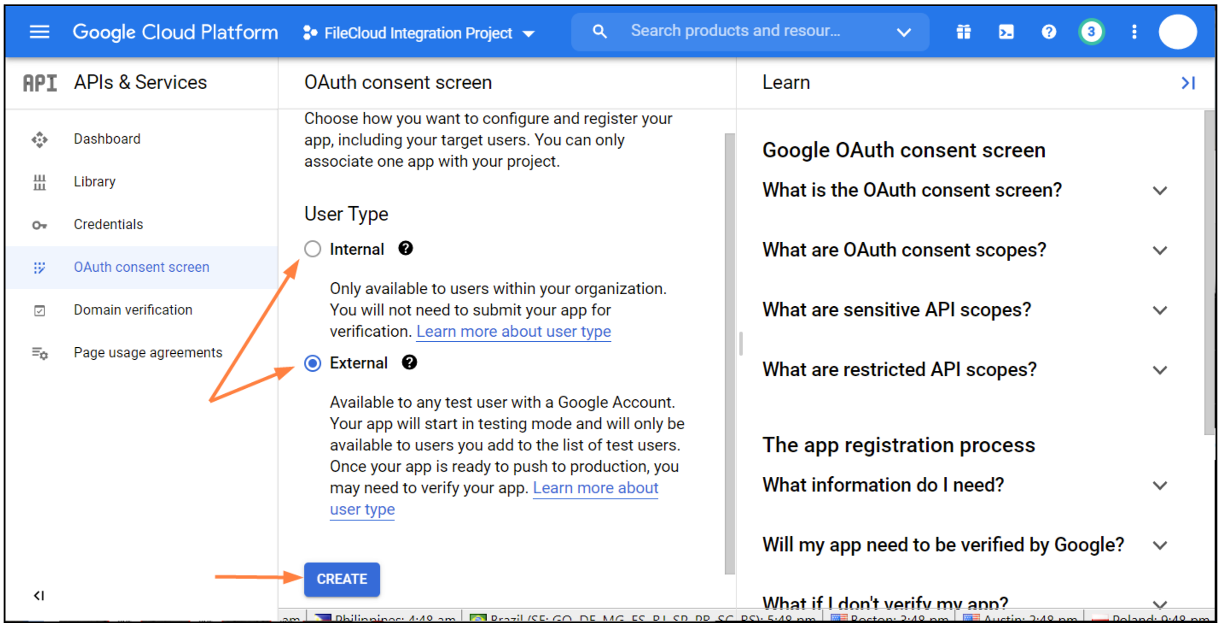
To use this API, you may need credentials. Click 'Create credentials' to get started.

No data is available for the selected time frame.

https://console.cloud.google.com/apis/credentials/consent?project=filecloud-integration-project&supportedpurview=project

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**.


Google Cloud Platform
FileCloud Integration Project
Search products and resour...
APIs & Services
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Learn
Google OAuth consent screen
What is the OAuth consent screen?
What are OAuth consent scopes?
What are sensitive API scopes?
What are restricted API scopes?
The app registration process
What information do I need?
Will my app need to be verified by Google?
What if I don't verify my app?
CREATE

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

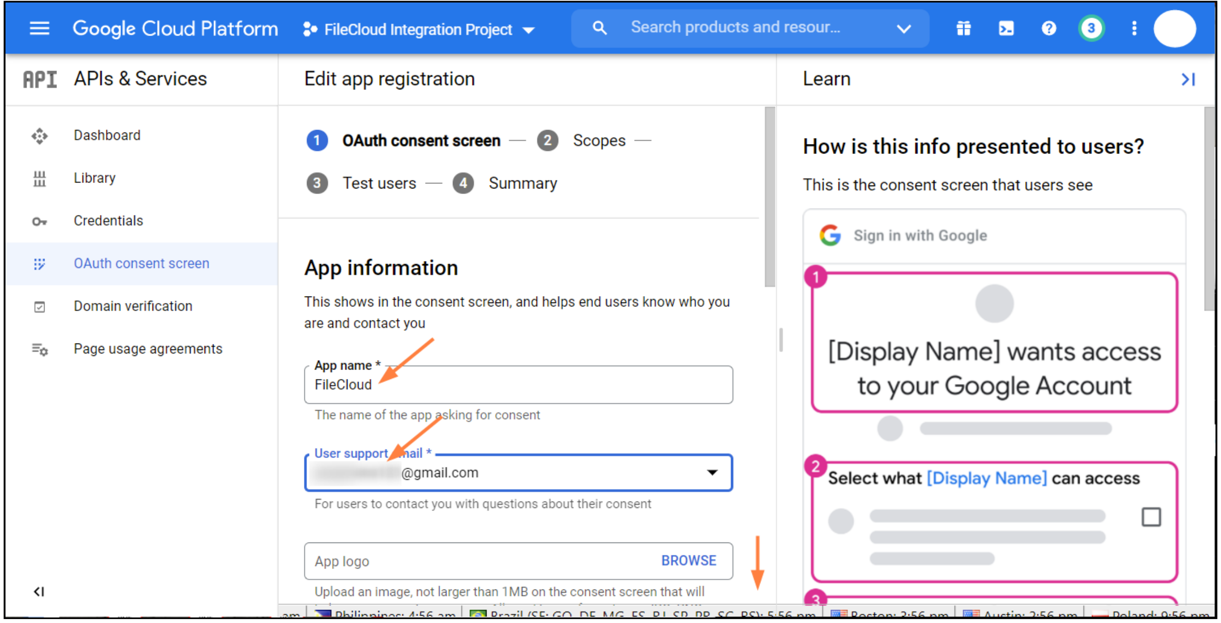
○ Internal

Only available to users within your organization. You will not need to submit your app for verification. Learn more about user type

● External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type

An **Edit app registration** screen for the **OAuth consent screen** opens.



Edit app registration

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *: FileCloud

The name of the app asking for consent

User support email *: [redacted]@gmail.com

For users to contact you with questions about their consent

App logo

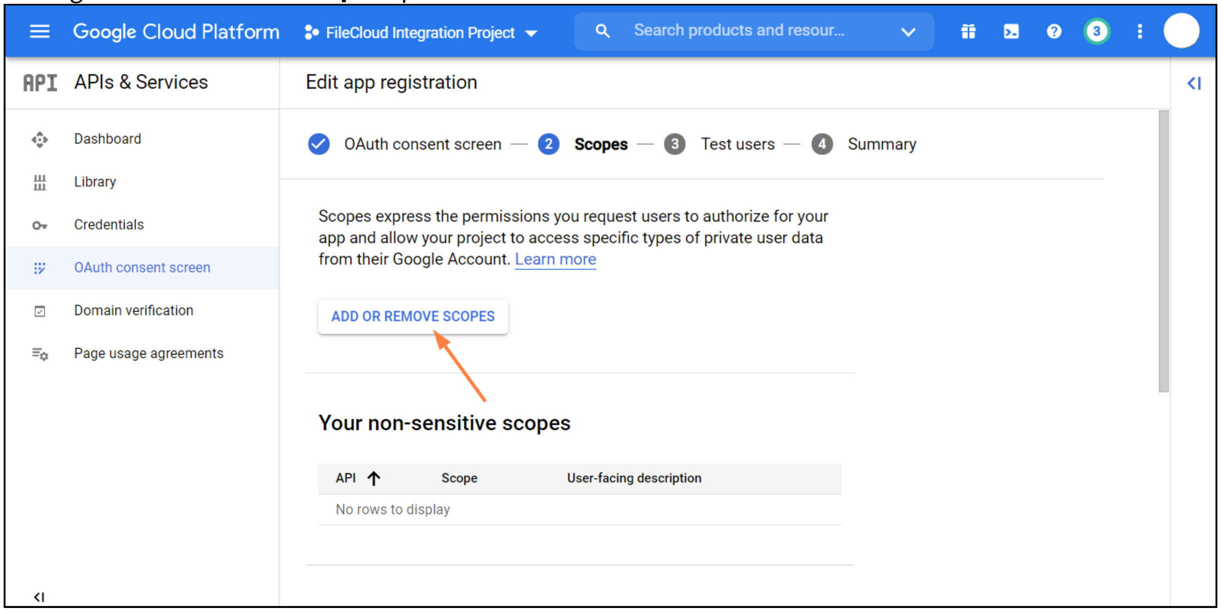
Upload an image, not larger than 1MB on the consent screen that will

How is this info presented to users?

This is the consent screen that users see

11. Fill in the required information, and then click **Save and Continue**.

The registration screen for **Scopes** opens:

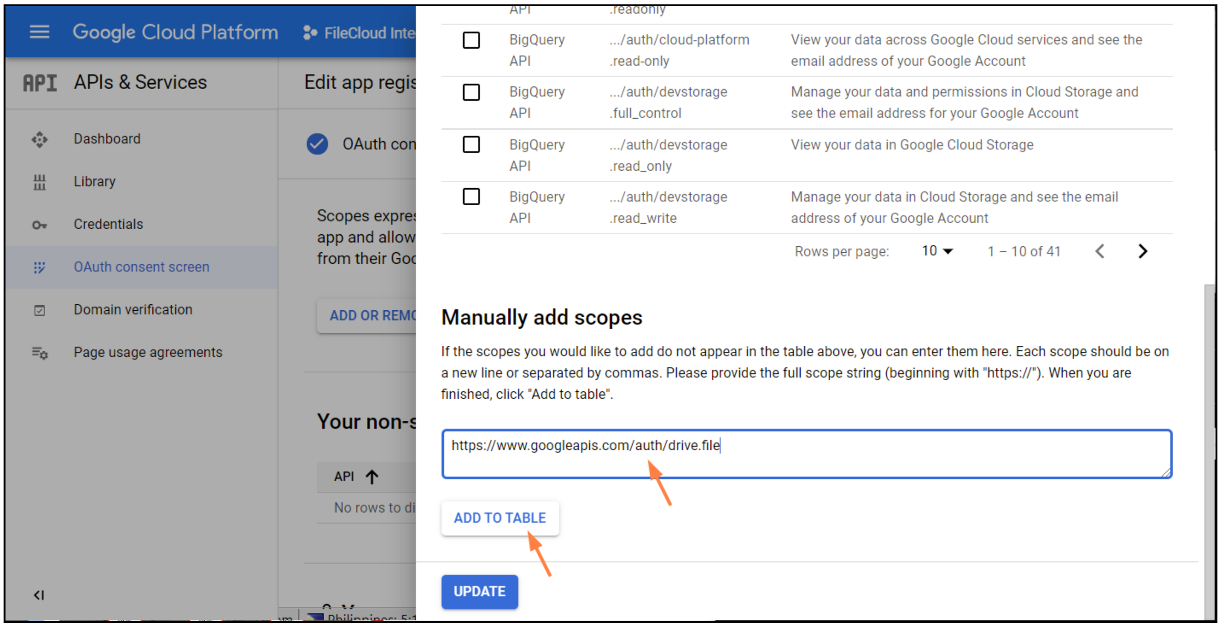


Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. Learn more

Your non-sensitive scopes

API	Scope	User-facing description
No rows to display		

12. Click **Add or Remove Scopes**.
    An **Update Selected Scopes** screen opens.
13. Scroll to the bottom of the screen and manually add https://www.googleapis.com/auth/drive.file. Then click **Add to Table**.



	API	.readonly	
☐	BigQuery API	.../auth/cloud-platform .read-only	View your data across Google Cloud services and see the email address of your Google Account
☐	BigQuery API	.../auth/devstorage .full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
☐	BigQuery API	.../auth/devstorage .read_only	View your data in Google Cloud Storage
☐	BigQuery API	.../auth/devstorage .read_write	Manage your data in Cloud Storage and see the email address of your Google Account

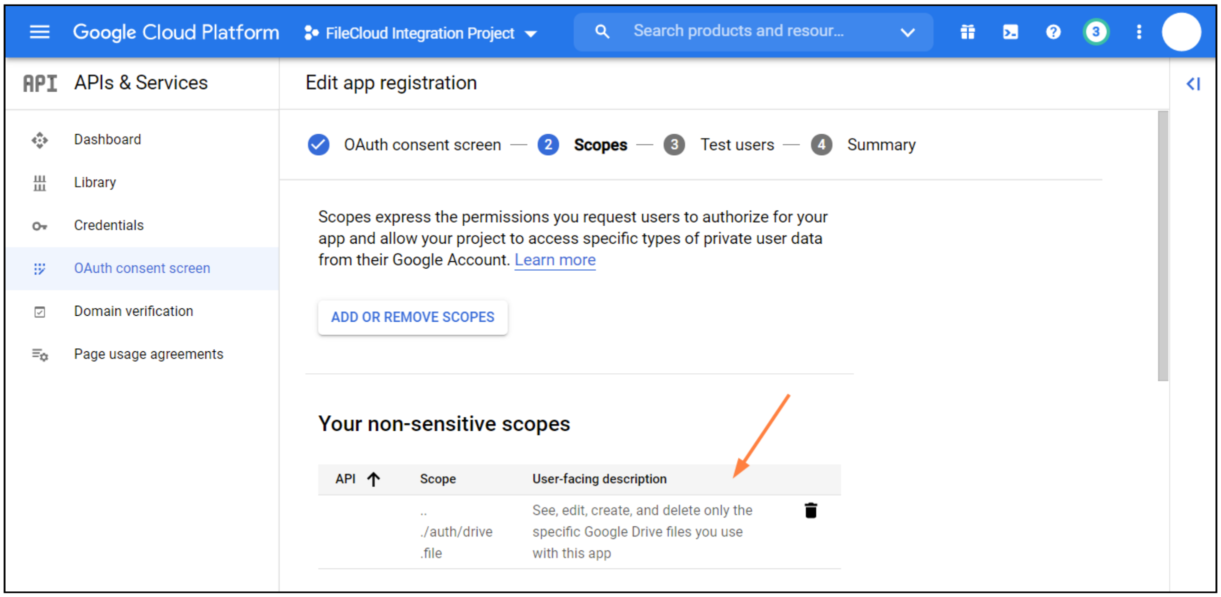
Rows per page: 10 1 – 10 of 41

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".

https://www.googleapis.com/auth/drive.file

14. Check it in the table and click **Update**.
    It appears under **Your non-sensitive scopes**.

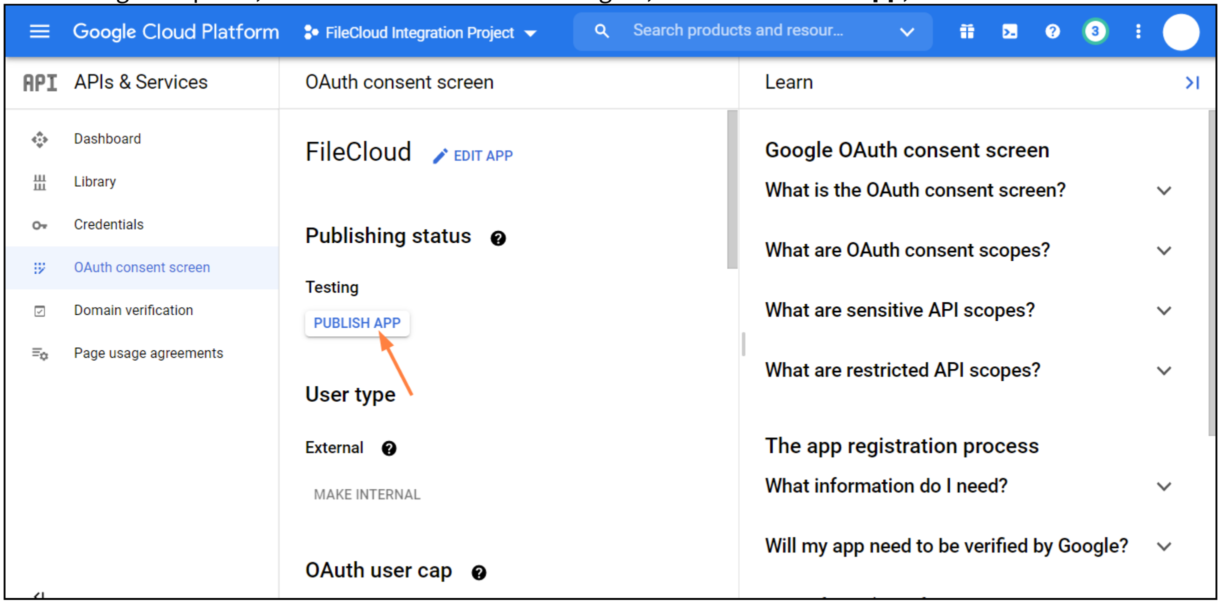


Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. Learn more

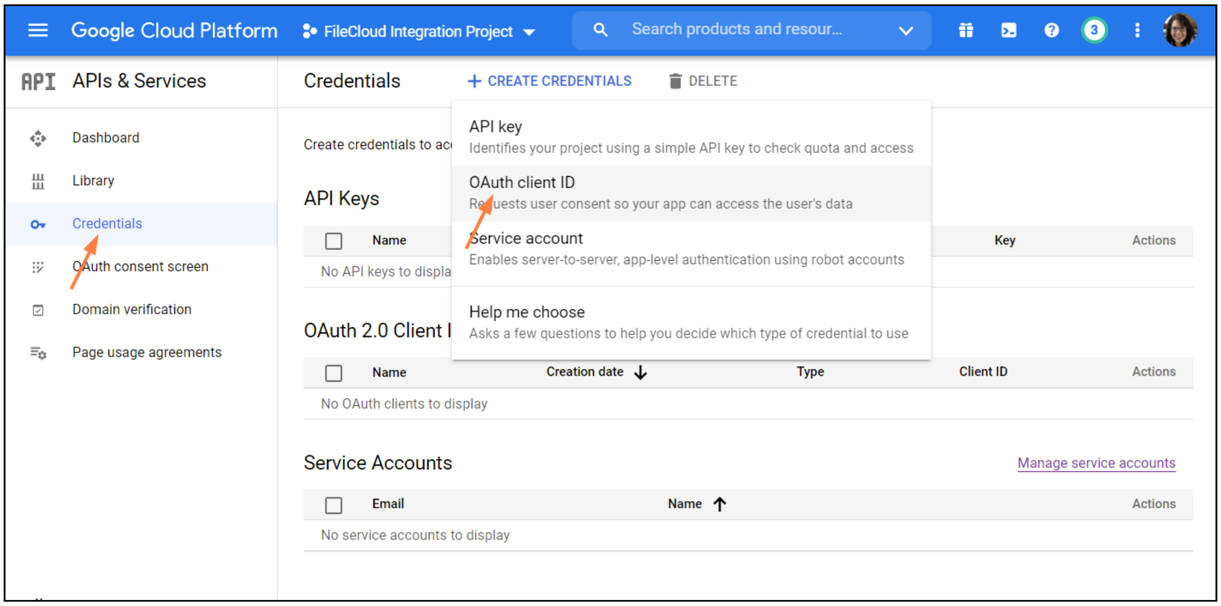
Your non-sensitive scopes

API ↑	Scope	User-facing description
	../auth/drive.file	See, edit, create, and delete only the specific Google Drive files you use with this app

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**.


Google Cloud Platform
FileCloud Integration Project
Search products and resour...
API APIs & Services
OAuth consent screen
Learn
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
FileCloud
EDIT APP
Publishing status
Testing
PUBLISH APP
User type
External
MAKE INTERNAL
OAuth user cap
Google OAuth consent screen
What is the OAuth consent screen?
What are OAuth consent scopes?
What are sensitive API scopes?
What are restricted API scopes?
The app registration process
What information do I need?
Will my app need to be verified by Google?

18. In the navigation panel, click **Credentials**, and in the **Credentials** screen, click **Create Credentials**, and choose **OAuth client ID.**



Create credentials to ac

API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

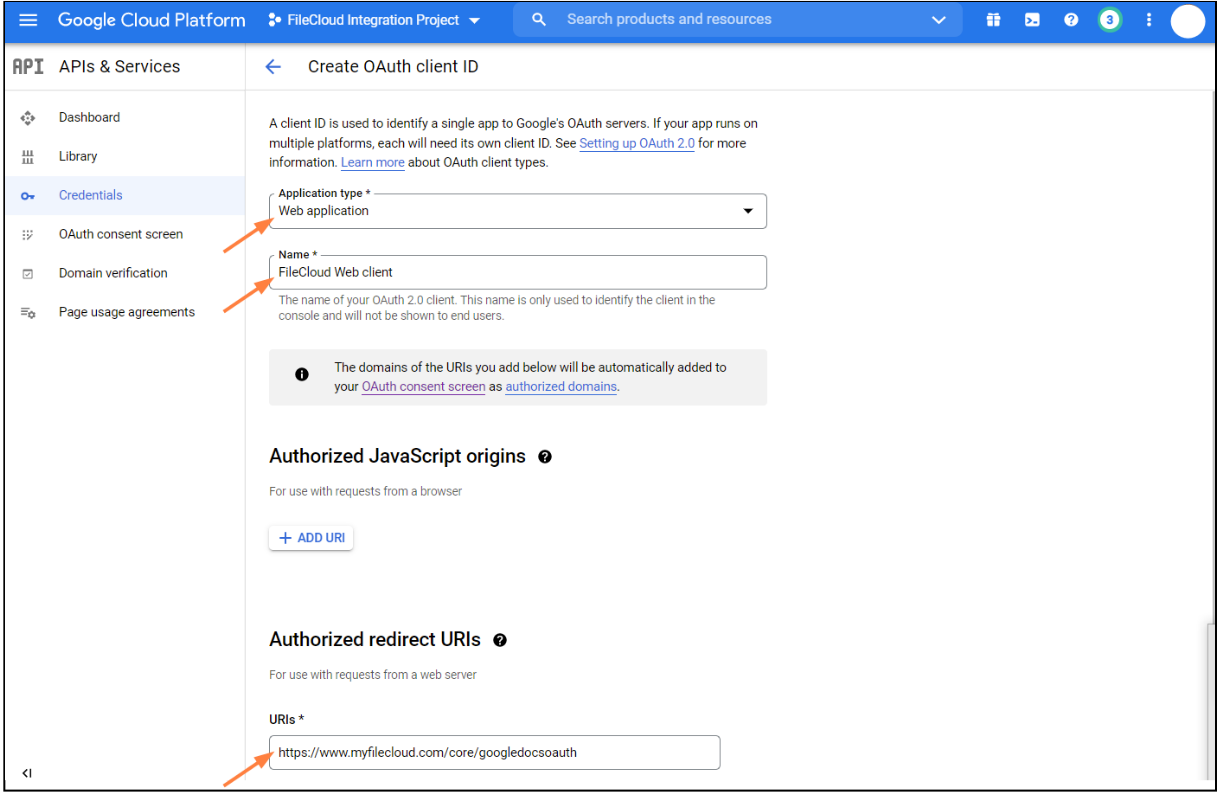
Help me choose
Asks a few questions to help you decide which type of credential to use

No API keys to displa

No OAuth clients to display

No service accounts to display

The Create OAuth Client ID screen opens.



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

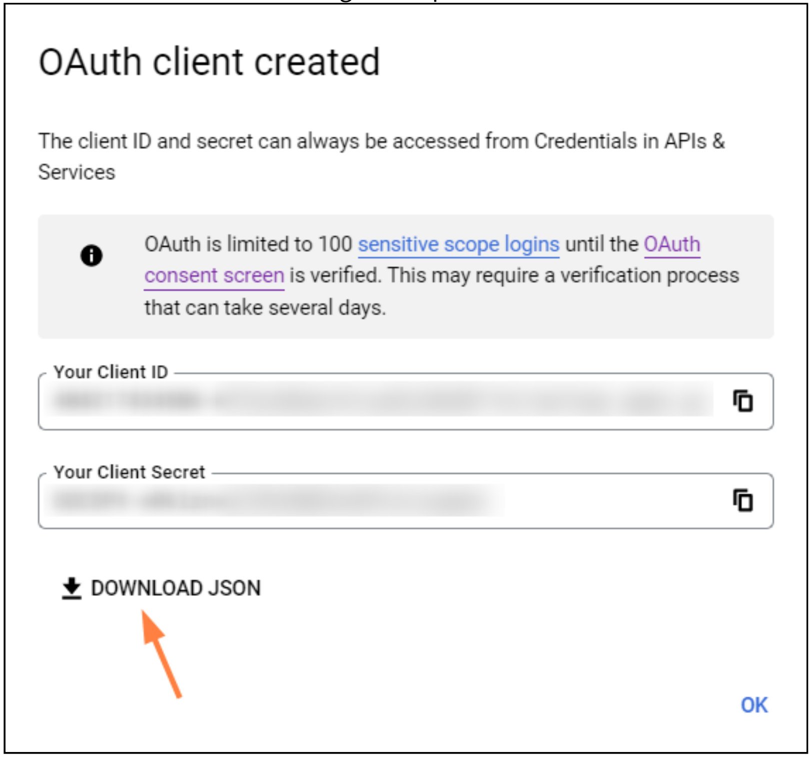
Authorized redirect URIs

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

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

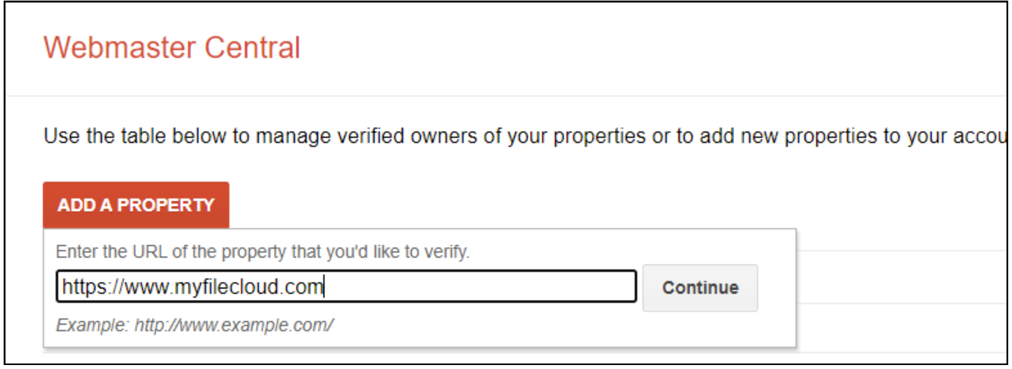
Your Client Secret

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

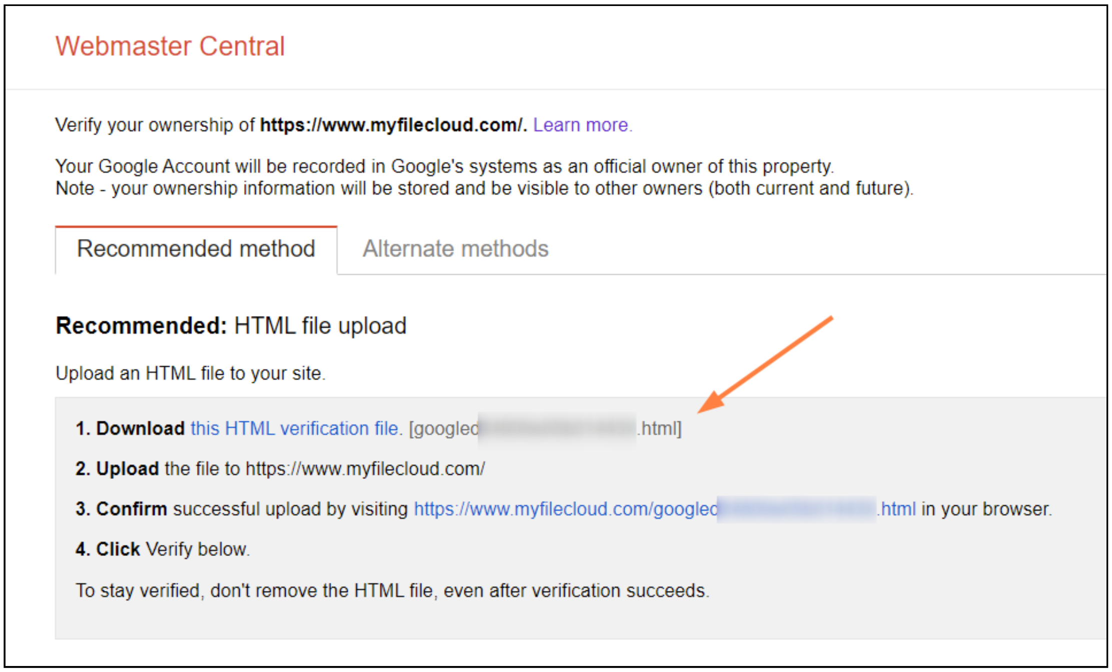
Use the table below to manage verified owners of your properties or to add new properties to your accou

Enter the URL of the property that you'd like to verify.

https://www.myfilecloud.com

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: HTML file upload

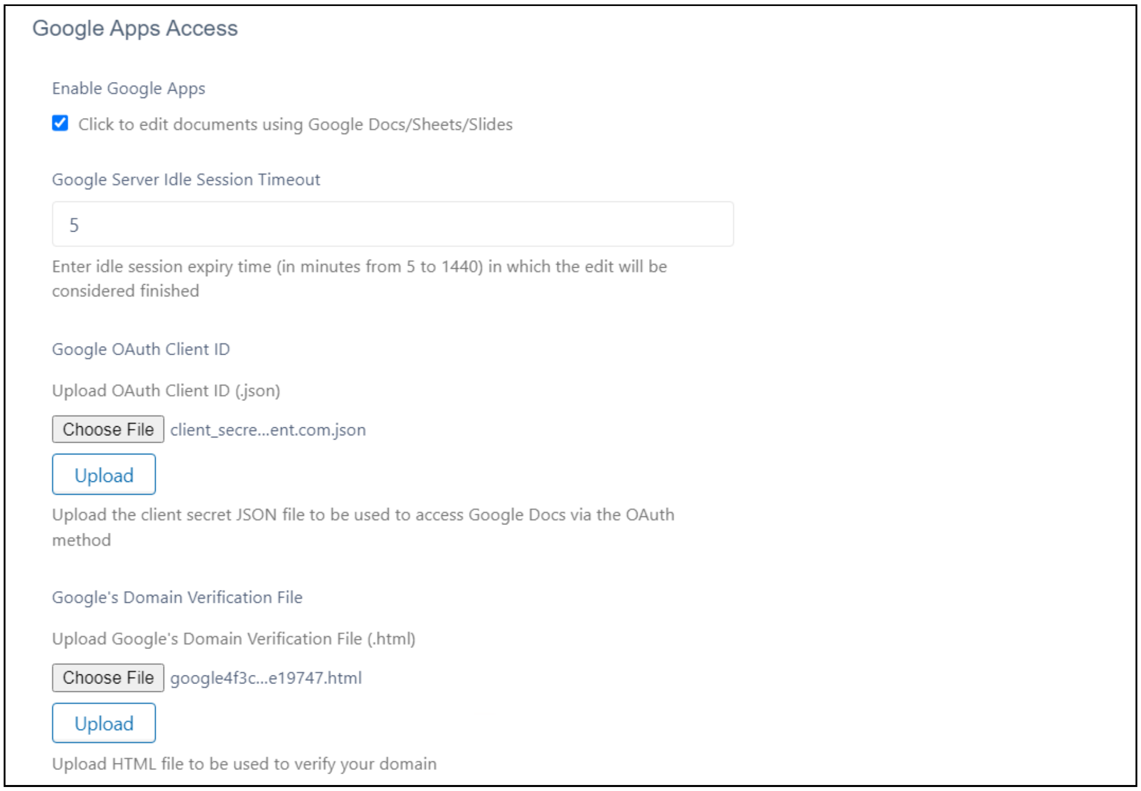
Upload an HTML file to your site.

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 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

5

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)

Choose File client_secre...ent.com.json

Upload

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)

Choose File google4f3c...e19747.html

Upload

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.

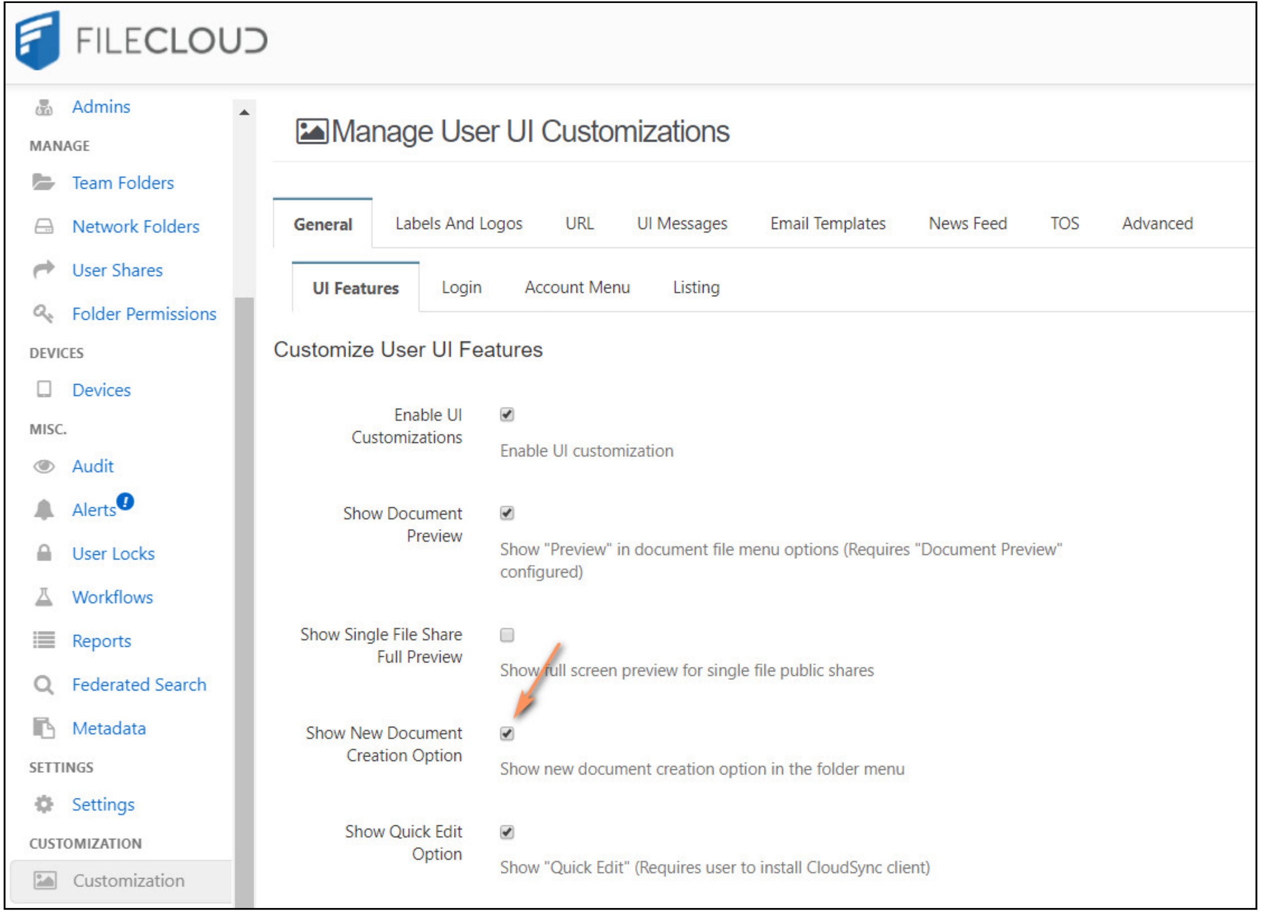
New Document Creation via Web Browser

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**.



Manage User UI Customizations

Customize User UI Features

Enable UI Customizations ☑ Enable UI customization

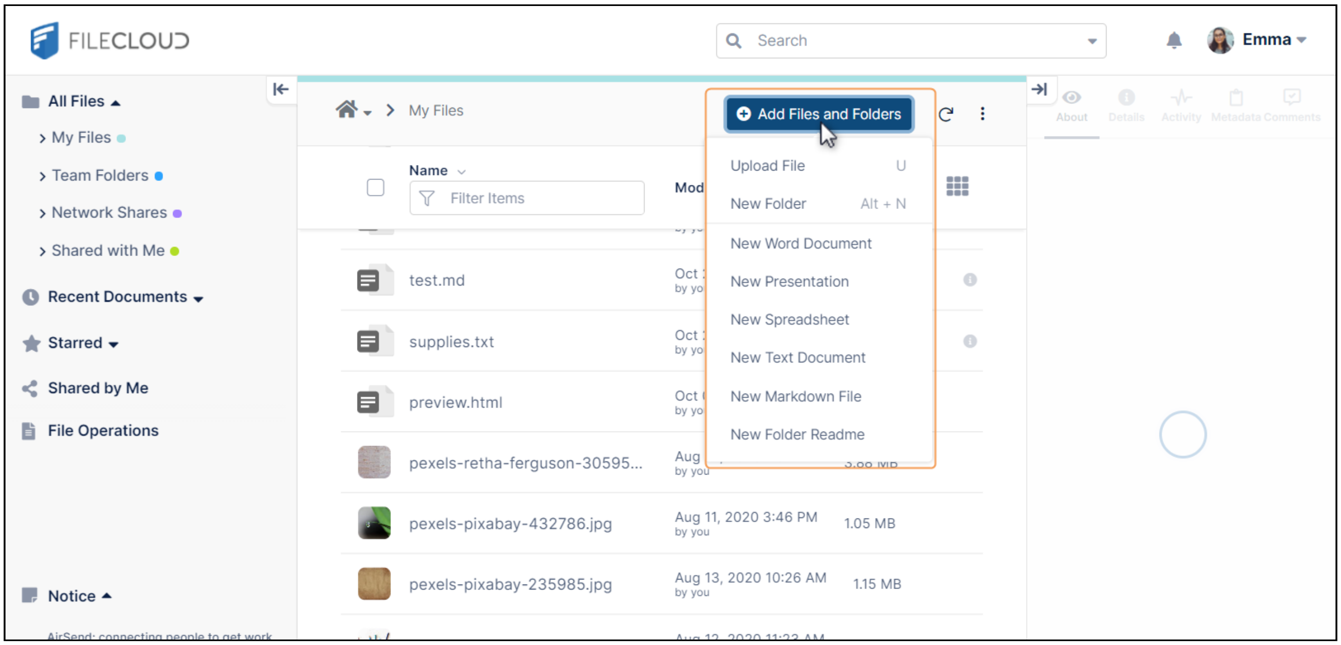
Show Document Preview ☑ Show "Preview" in document file menu options (Requires "Document Preview" configured)

Show Single File Share Full Preview ☐ Show full screen preview for single file public shares

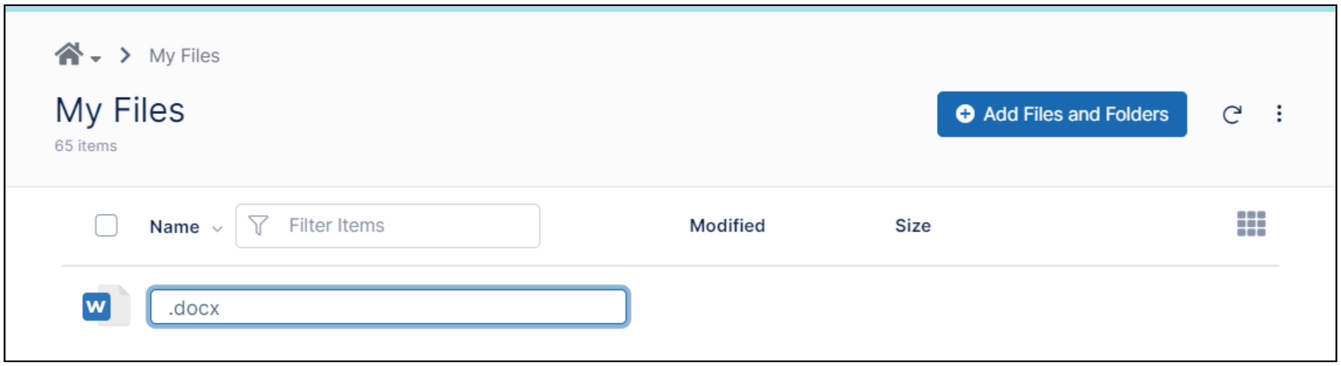
Show New Document Creation Option ☑ Show new document creation option in the folder menu

Show Quick Edit Option ☑ 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.

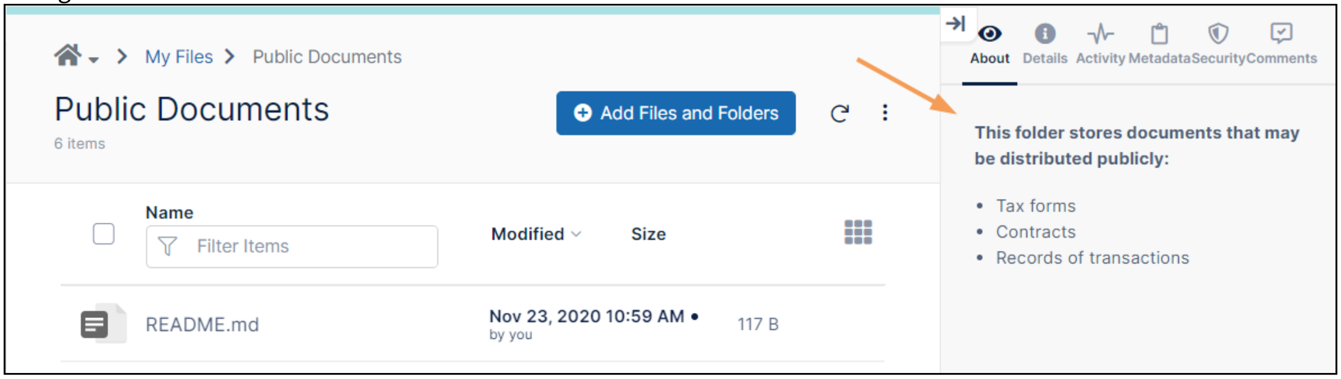


Readme files

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.



This folder stores documents that may be distributed publicly:

- Tax forms
- Contracts
- Records of transactions

Web Editing Text Files

Introduction

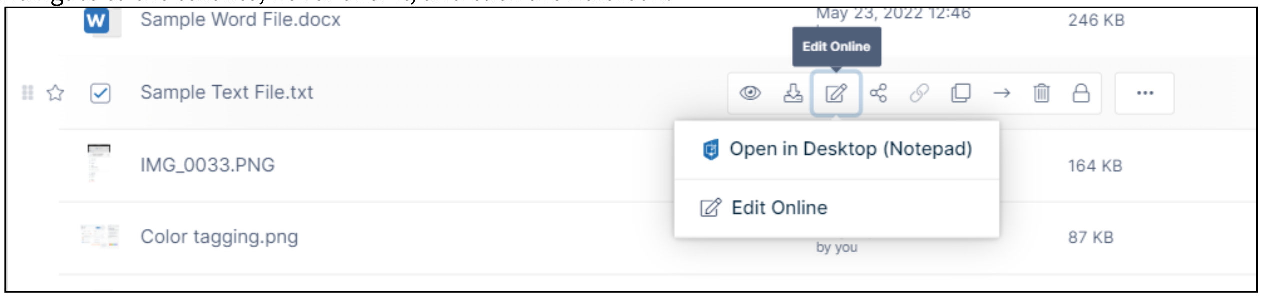
Starting with v17.x, FileCloud supports editing text files from within a browser session. This support is enabled irrespective of WOPI configuration, as editing of text files uses a built-in widget.

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

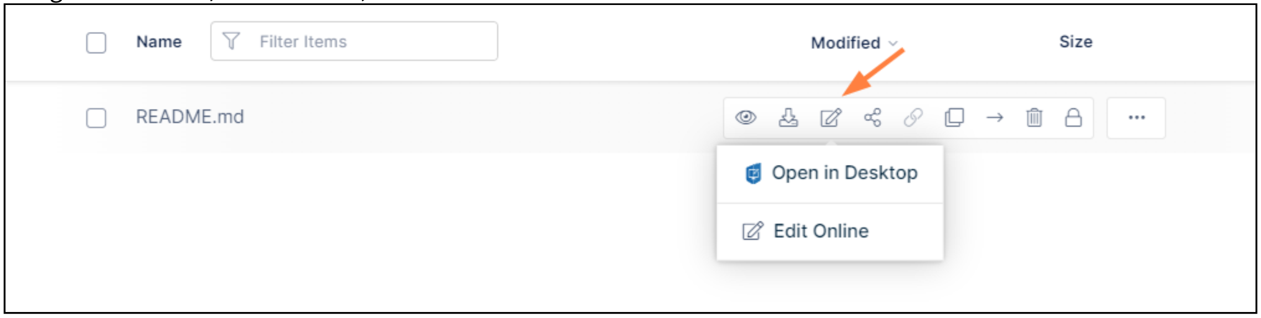
Starting with version 20.2, FileCloud supports editing markdown files from within a browser session. It also supports editing readme files, which are a form of markdown files and use the same types of editors.

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..

> ⓘ 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

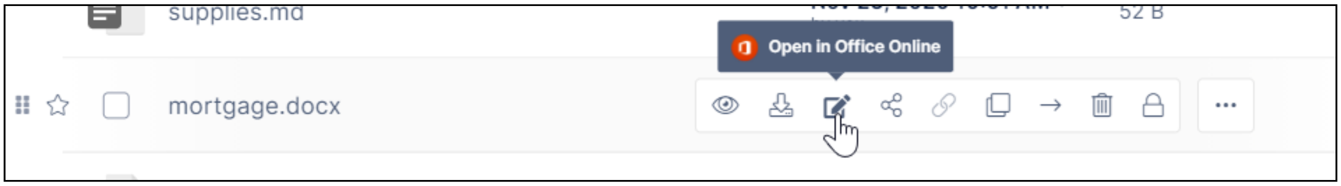
Beginning with v17.x, FileCloud supports coauthoring of Office document files from within a browser session.

Introduction

Coauthoring occurs when two users are editing the same document and can view each other's changes as they make them.

Only .docx, .xslx, and .pptx documents can be coauthored.

To open an Office file in web edit, hover over the file and click the **Web Edit** icon. 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*.

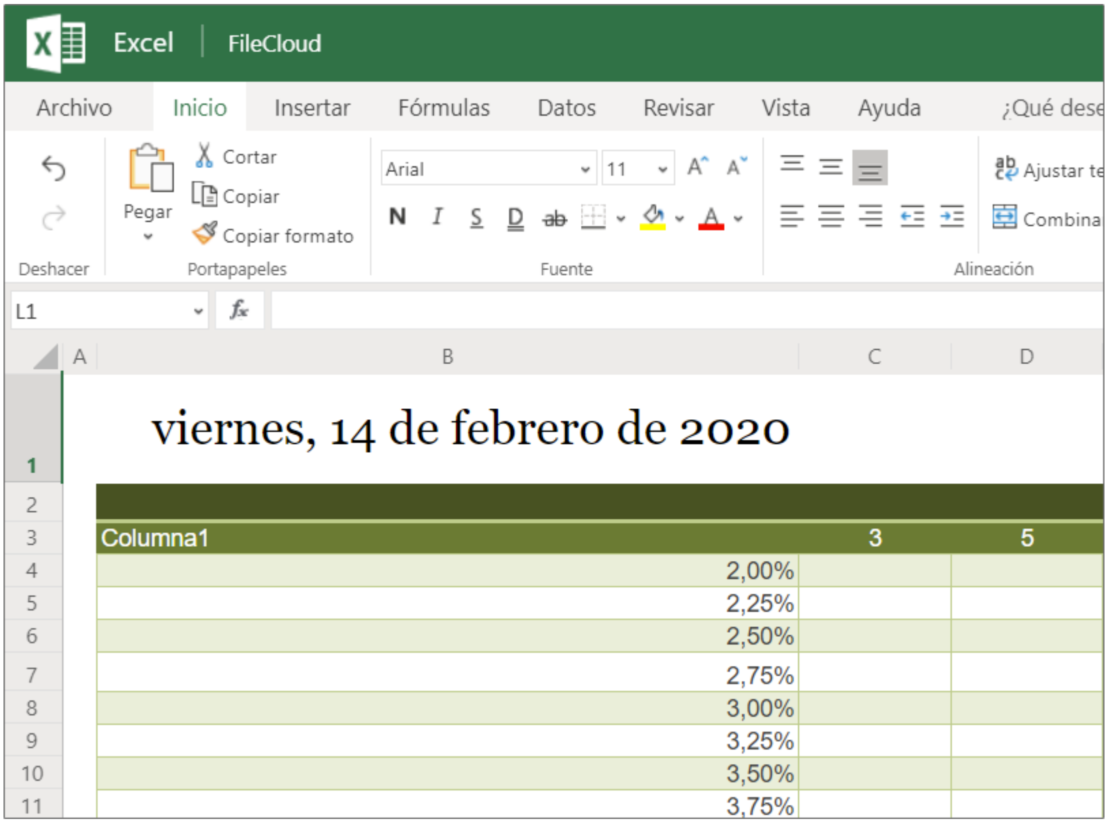
Changing the locale in online Office documents

If you want online Office documents to open in a different locale than the default (en-US), you must change the locale in WOPI.

1. Choose any of the WOPI locales included in https://wopi.readthedocs.io/en/latest/faq/languages.html.
2. Change the WOPI locale:
    a. Open the configuration file:
       Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
       Linux: /var/www/config/cloudconfig.php
    b. Add the line following line, changing *en-US* to the new locale:

```
define("WOPI_CLIENT_LOCALEID", "en-US");
```

Now when you open a FileCloud document in Office online, the labels appear in the new locale, and if you add locale-sensitive features, like dates, they appear in the correct format. For example, the WOPI locale for the following document opened in FileCloud is es-ES:

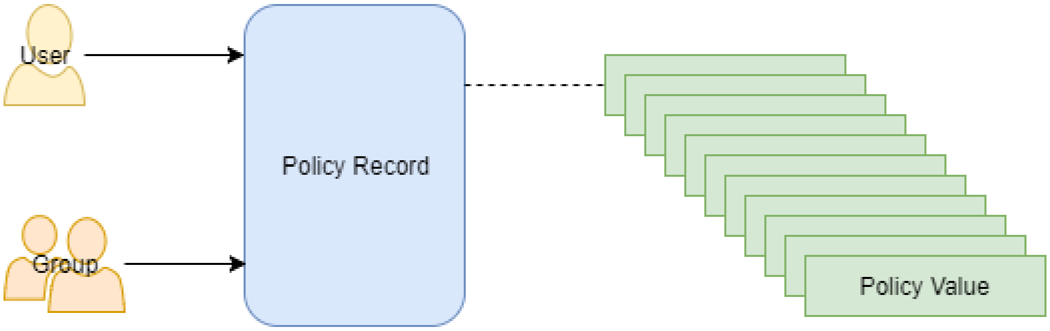


viernes, 14 de febrero de 2020

	A	B	C	D
1		viernes, 14 de febrero de 2020		
2				
3		Columna1	3	5
4		2,00%		
5		2,25%		
6		2,50%		
7		2,75%		
8		3,00%		
9		3,25%		
10		3,50%		
11		3,75%		

Policies

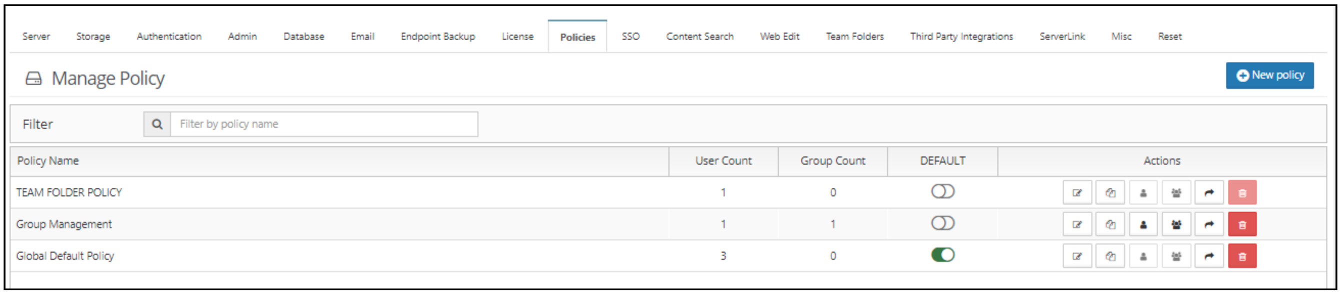
ⓘ Policies are available in FileCloud 17.3 and later.



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.



Manage Policy

Filter: Filter by policy name

Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	○	
Group Management	1	1	○	
Global Default Policy	3	0	●	

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	
Enable Basic Authentication (appears if enabled, see Enabling Basic Authentication)	Disable	
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:

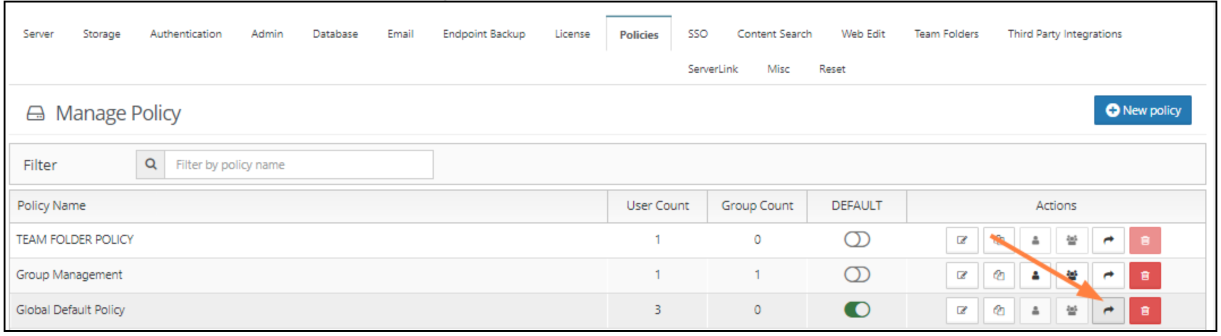
1. Log into the Admin Portal.
2. Click *Settings*.
3. On the *Policies* tab, to open the *Manage Policy Groups* window, click the groups icon 👥.
4. In the *Manage Policy Groups* window, in *Available Groups*, select a group.
5. Use the arrows to move the group to the *Policy Groups* list box.
6. To save 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.

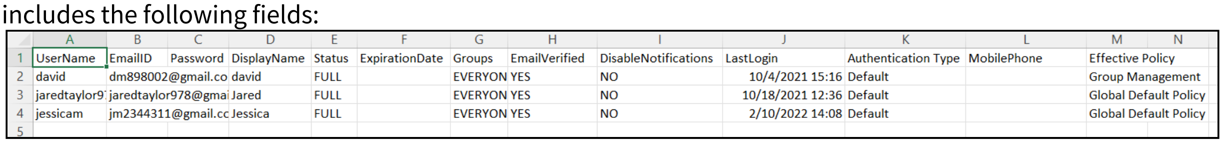
To export policy members:

1. Go to **Settings** > **Policies**.
2. Under **Actions** for the policy, click the right arrow icon.



Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	○	
Group Management	1	1	○	
Global Default Policy	3	0	●	

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:



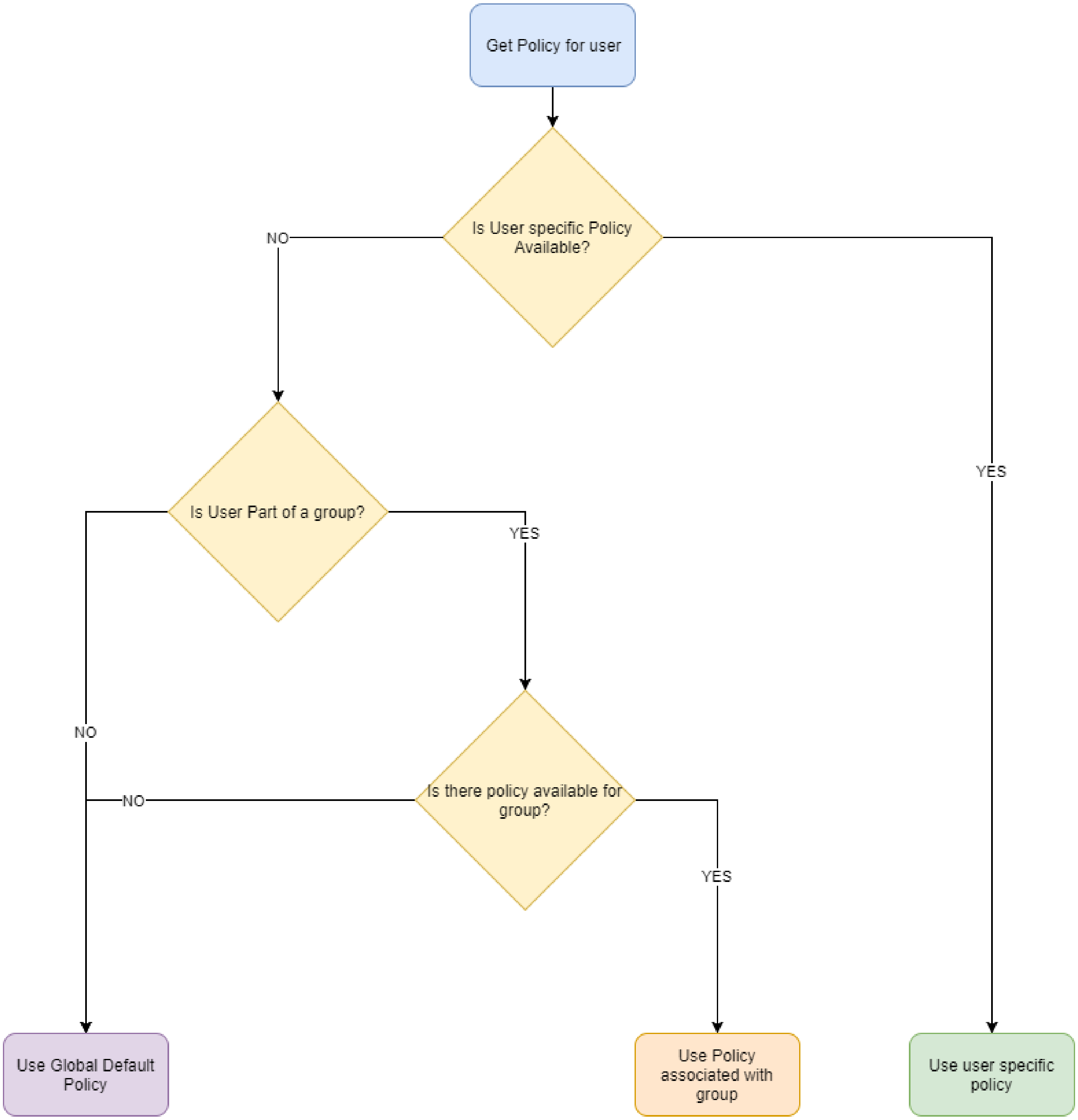
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	UserName	EmailID	Password	DisplayName	Status	ExpirationDate	Groups	EmailVerified	DisableNotifications	LastLogin	Authentication Type	MobilePhone	Effective Policy	
2	david	dm898002@gmail.co		david	FULL		EVERYON	YES	NO	10/4/2021 15:16	Default		Group Management	
3	jaredtaylor9	jaredtaylor978@gmai		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 Calcuations 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


Get Policy for user
Is User specific Policy Available?
NO
YES
Is User Part of a group?
YES
NO
Is there policy available for group?
NO
YES
Use Global Default Policy
Use Policy associated with group
Use user specific policy

Policy Selection Scenarios

Case 1: User with no policy assigned : **Global Default Policy will be used**

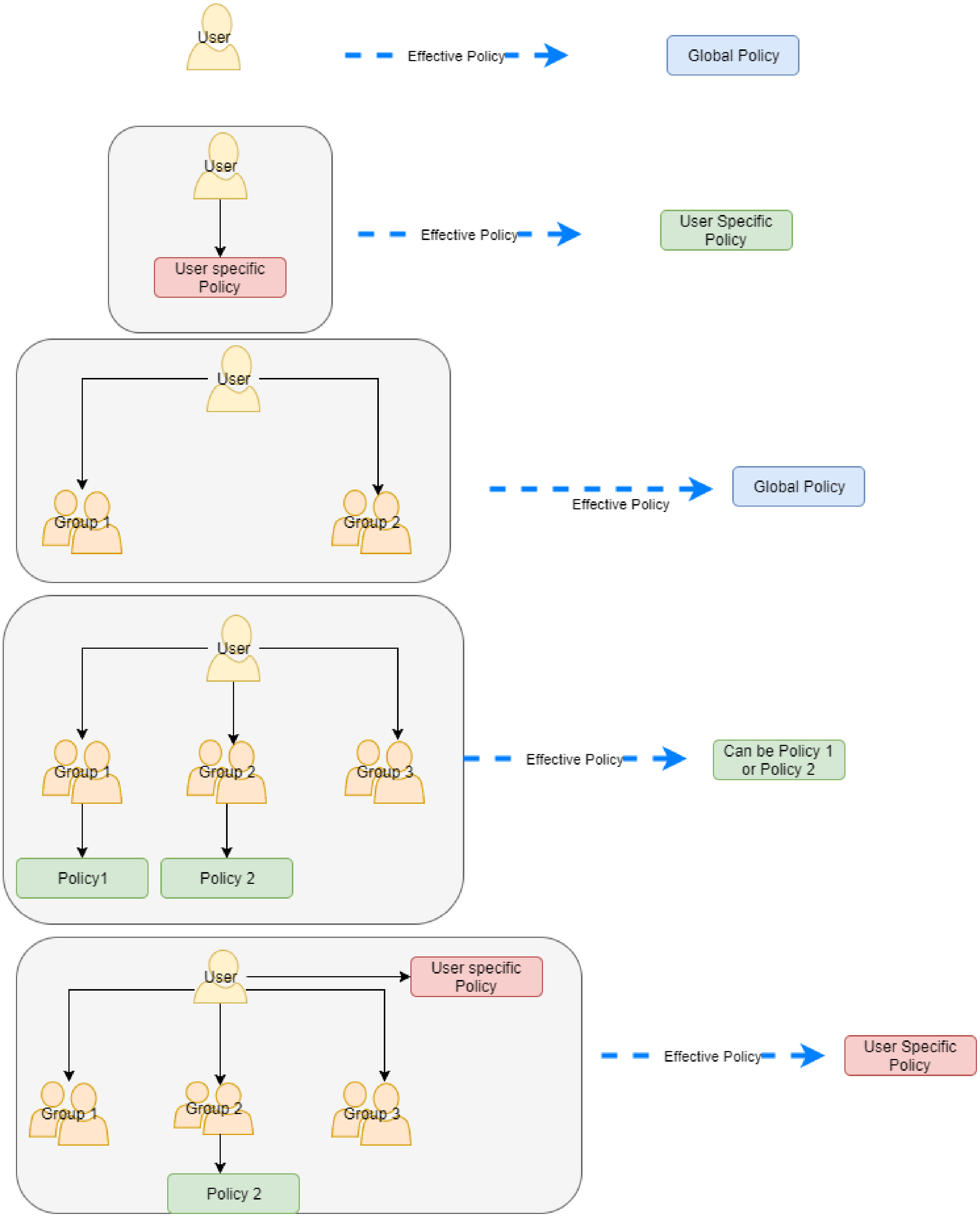
Case 2: User with specific policy assigned: **Assigned policy will be used**

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


User
Effective Policy
Global Policy
User
User specific Policy
Effective Policy
User Specific Policy
User
Group 1
Group 2
Effective Policy
Global Policy
User
Group 1
Group 2
Group 3
Policy1
Policy 2
Effective Policy
Can be Policy 1 or Policy 2
User
User specific Policy
Group 1
Group 2
Group 3
Policy 2
Effective Policy
User Specific Policy

Notifications for File Changes

FileCloud automatically sends you an email notification when:

- a file or folder is shared with you
- one of the following actions is performed (by you or another user) on a file or folder you have access to:
  - a file or folder is uploaded
  - a file or folder is downloaded
  - a file or folder is shared
  - a file or folder is deleted
  - a file or folder is renamed
  - a file is updated
  - a file is previewed in the browser or one of the mobile apps
  - a file or folder is locked

Administrators can set notifications at the global level and users can override them at the user level.

FAQ's

How Do Notifications Work?

By default, when users make any of the changes listed above to their own files or folders, FileCloud sends them a notification. When a user makes any of the changes listed above to shared files or folders, all users that the file or folder has been shared with receive a notification.

All file change notifications are consolidated and emails are are sent by FileCloud at regular notification frequencies (15 minutes, 1 hour, 1 day etc) as set by your FileCloud administrator as part of the Cron Job Setting.

Why is the User Not Getting a Notification?

If you have enabled file and folder change notifications and a user is not receiving a notification, it may be because:

- the file change was made directly on the LAN

- 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

This applies to both My Files and Network Folders.

For network folders, when files are changed directly on the LAN, FileCloud does not have any knowledge of file changes and will not send a notification.

Is the Notification Blocked in Another Place?

File change notifications can be blocked for a specific action in any of the following places:

- Global settings
- Policy settings
- Share settings
- Network folder settings,
- File or folder settings
- NTFS Permissions
- Account settings for external users

If a user is not receiving a notification, check to see if that file action is disabled at any level.

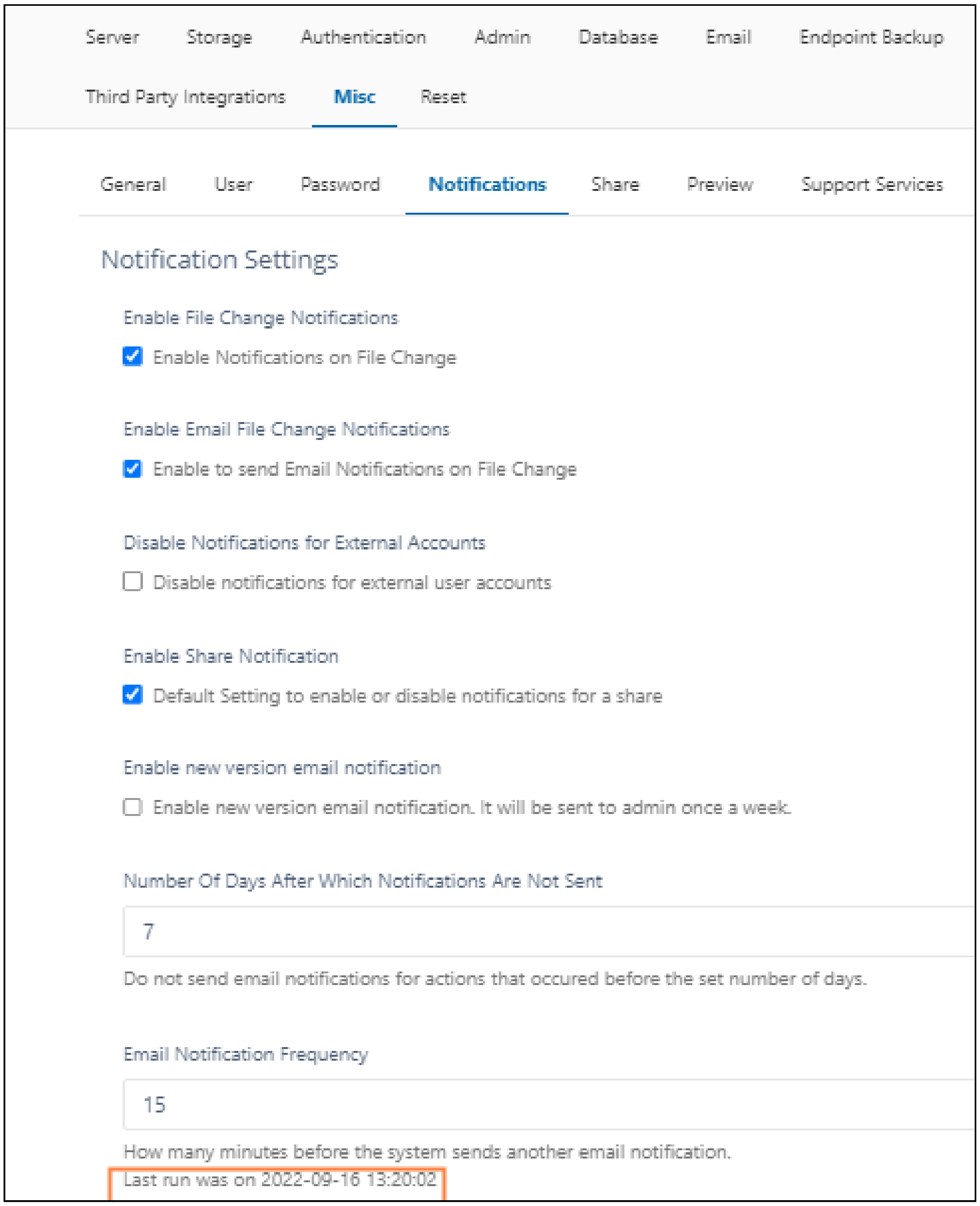
Are you using a trial account?

Trial accounts have notification limits. If you are using a trial account and have been able to send notifications previously, the notification limit may have been reached.

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.



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

7

Do not send email notifications for actions that occured before the set number of days.

Email Notification Frequency

15

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 the time when digest emails are sent

By default, FileCloud uses the following schedule for sending daily and weekly digest emails:

- Weekly digest emails are sent on Fridays at 8 am.
- Daily digest emails are sent at 9 am.

However, beginning with FileCloud Version 20.1, you can override these times by adding settings to the cloudconfig.php file.

1. Open cloudconfig.php in
   - Windows: xampp/htdocs/config
   - Linux: /var/www/config

2. To set:
   a. The day of the week that weekly digests are sent, add the setting:

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

   enter 0 - 6, where  0 = Sunday and 6 = Saturday
   ```

   b. The hour of the day that weekly digests are sent, add the setting:

   ```
   define("TONIDOCLOUD_WEEKLY_DIGEST_HOUR", 8);

   enter 0 - 23, where 0 = 12:00 am and  23 = 11:00 pm
   ```

   c. The hour of the day that daily digests are sent, add the setting:

   ```
   define("TONIDOCLOUD_DAILY_DIGEST_HOUR", 9);

   enter 0 - 23, where 0 = 12:00 am and  23 = 11:00 pm
   ```

Notes: These settings do not affect other settings for notifications. If Email notification frequencies are set to run every 60 minutes, these emails are sent as well as the daily and weekly digests.

Digests are processed by cron, so if you schedule a mailing at 9, but the cron process is scheduled to run at 9.30, the emails are sent at 9:30.

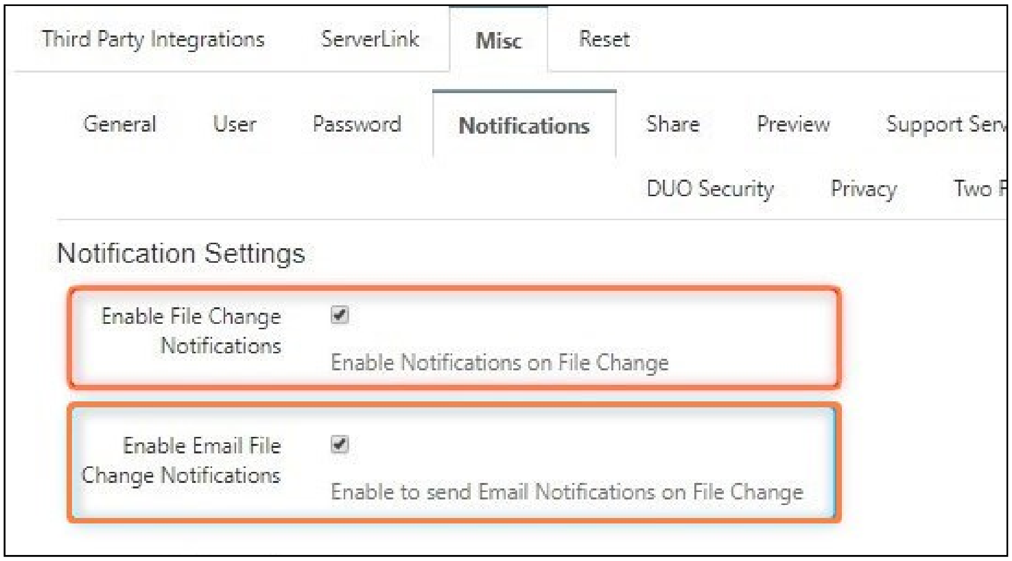
Changing notification settings

Global notification settings

Enable or Disable ALL Notifications

Prerequisites

1. Cron jobs must be setup. See Steps at Setting Up a Cron Job or Scheduled Task



Notification Settings

Enable File Change Notifications ☑ Enable Notifications on File Change

Enable Email File Change Notifications ☑ 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***.

ⓘ 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

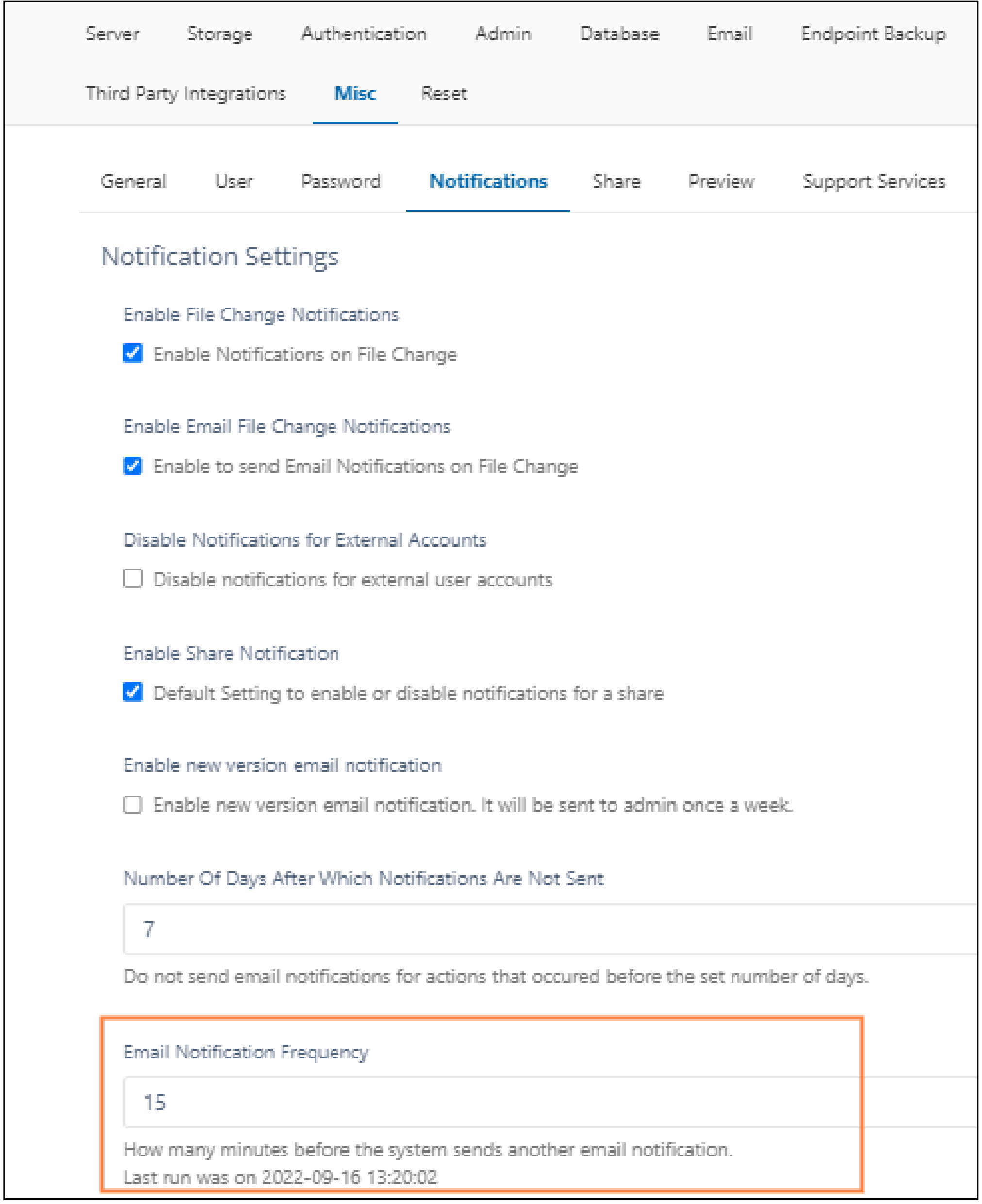
You can set the file change notification frequency level in the Admin portal, and users can override this and set their own frequency in the User portal.

- 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.*



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

7

Do not send email notifications for actions that occured before the set number of days.

Email Notification Frequency

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.

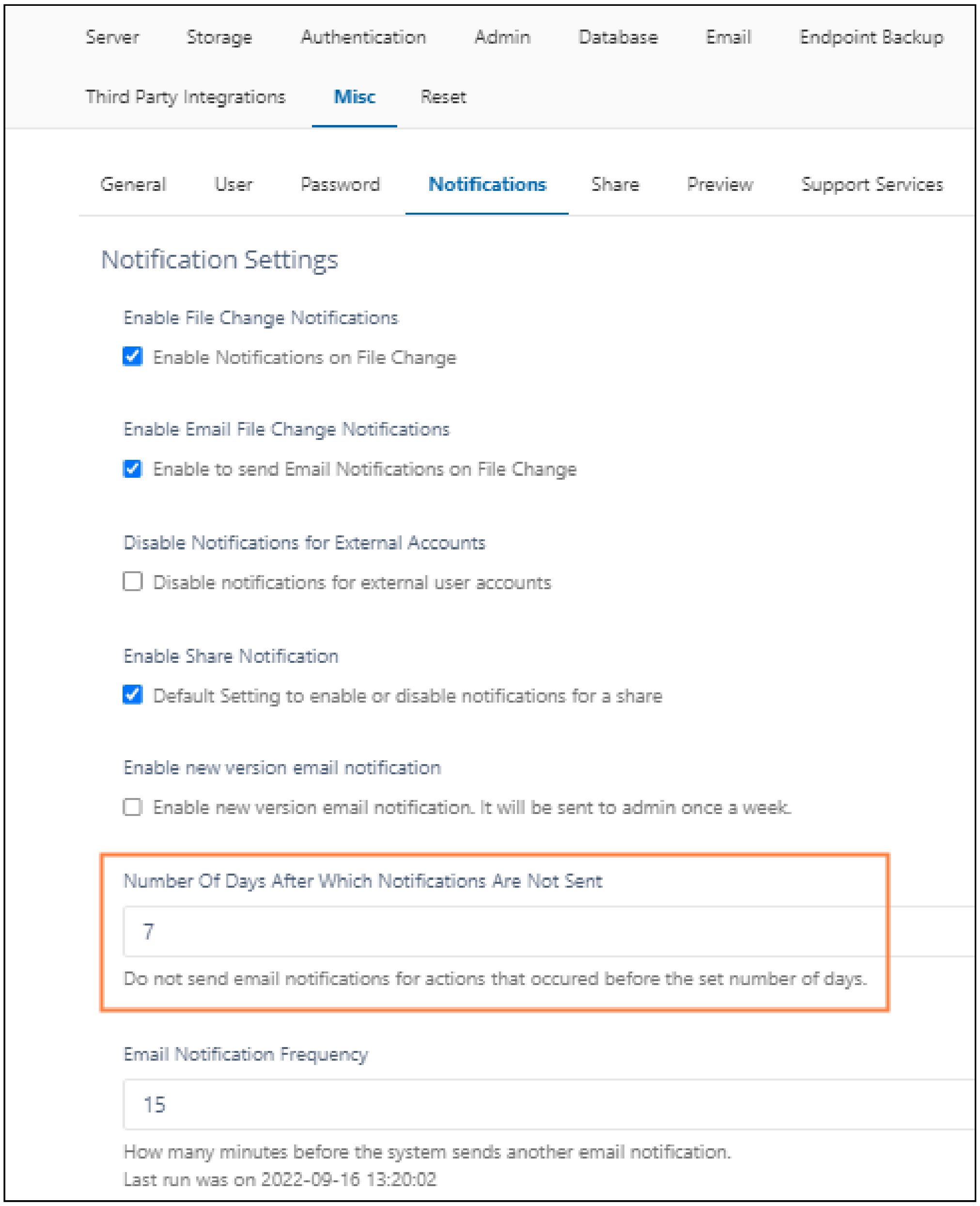
Do not send outdated email notifications

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.



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

7

Do not send email notifications for actions that occured before the set number of days.

Email Notification Frequency

15

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.

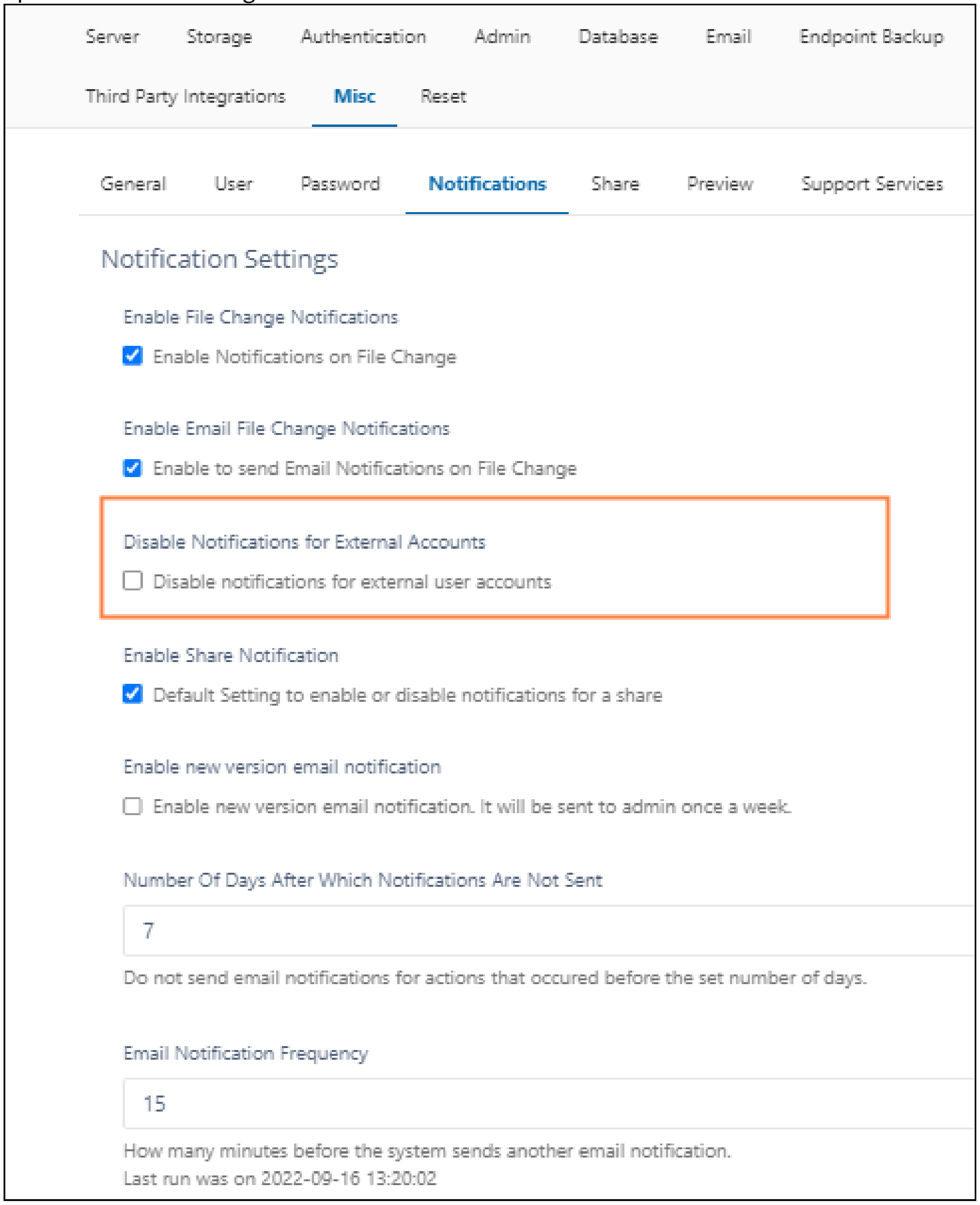
These user accounts:

- 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*.



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

7

Do not send email notifications for actions that occured before the set number of days.

Email Notification Frequency

15

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

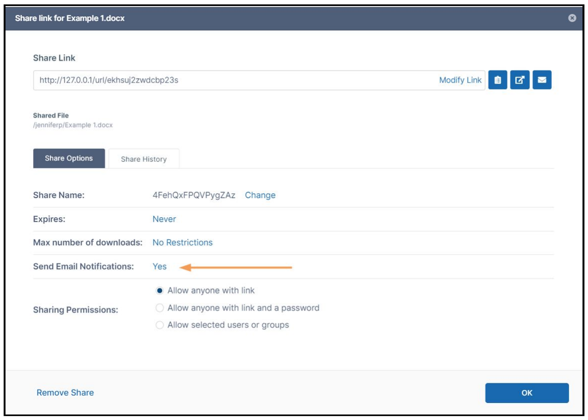
Sharing Notifications

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



Share link for Example 1.docx

Share Link

http://127.0.0.1/url/ekhsuj2zwdcbp23s

Shared File
/jenniferp/Example 1.docx

Share Name: 4FehQxFPQVPygZAz Change

Expires: Never

Max number of downloads: No Restrictions

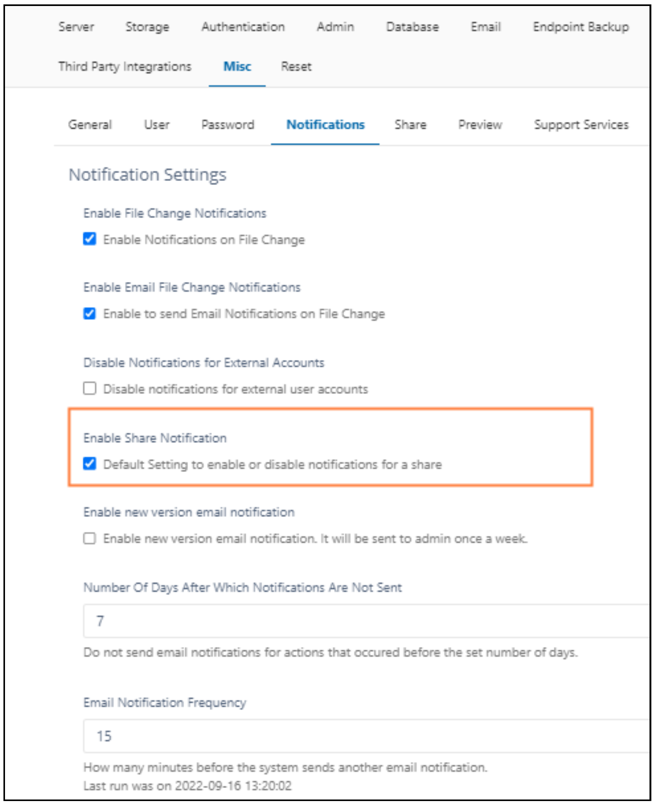
Send Email Notifications: Yes

Sharing Permissions:
● Allow anyone with link
○ Allow anyone with link and a password
○ Allow selected users or groups

To share a file with everyone without restrictions:

1. Open a browser and log in to the User Portal.
2. In the *User Portal*, click *My Files*.
3. Hover over the file you want to share.
4. Click the *Share* icon.
5. On the *Share Link for File* dialog box, click *Share Options*
6. In *Share Options*, set *Send Email Notifications* to YES.

Admin Portal



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
7
Do not send email notifications for actions that occured before the set number of days.

Email Notification Frequency
15
How many minutes before the system sends another email notification.
Last run was on 2022-09-16 13:20:02

To enable File Change Notifications for Shares:

1. Log in to the *Admin Portal*.
2. From the left navigation pane, select *Settings*.
3. Select *Misc.*> *Notifications*.
4. Select *Enable Share Notification*.
5. Click *Save*.

Policy notification settings

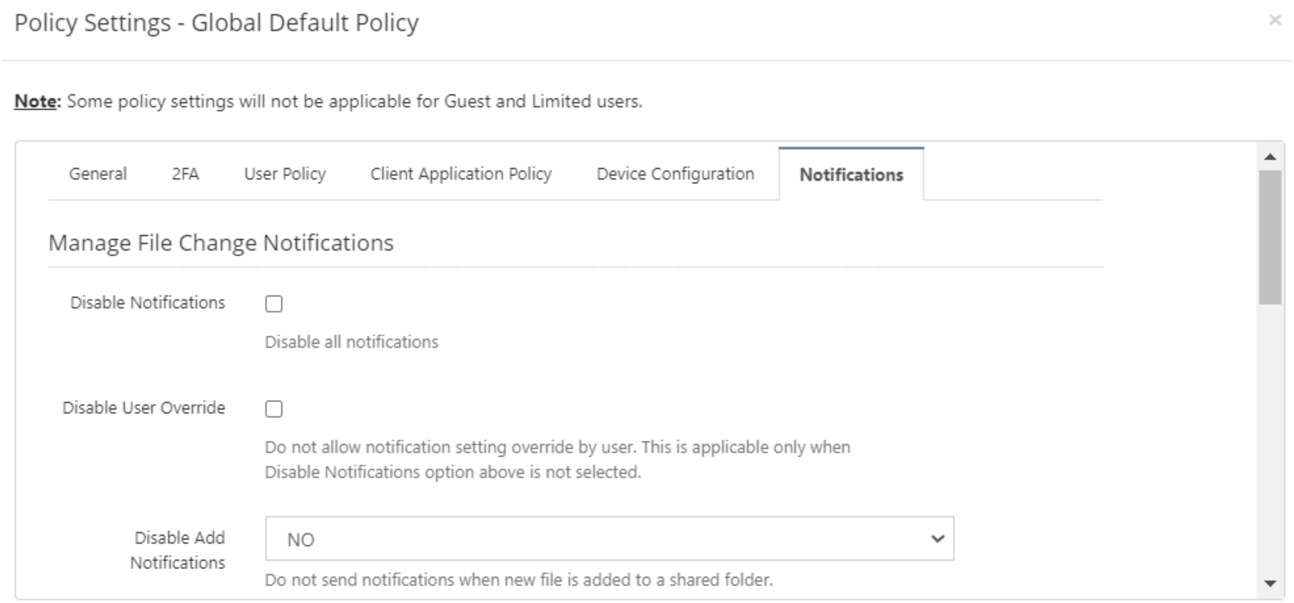
User and Group Notifications

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

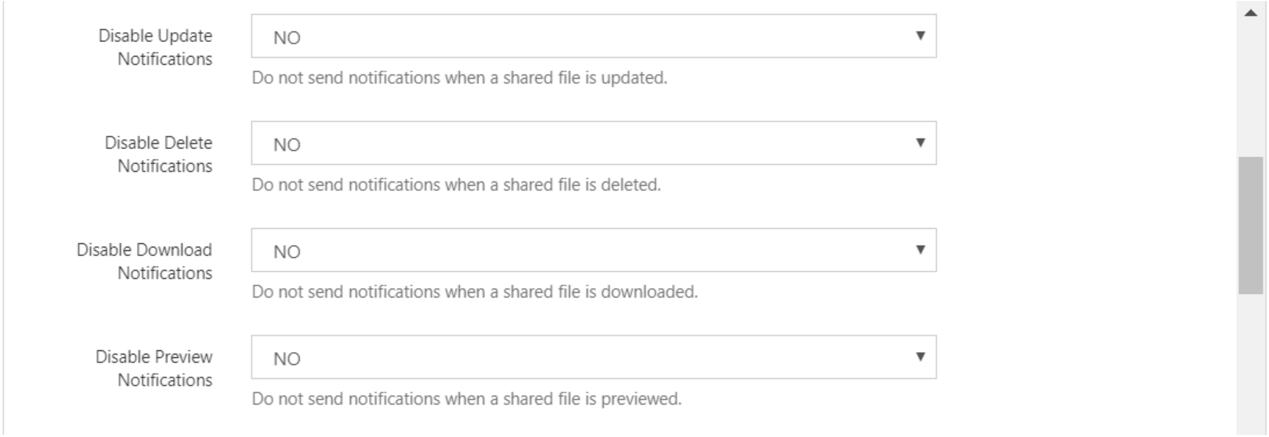
Note: Some policy settings will not be applicable for Guest and Limited users.

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.

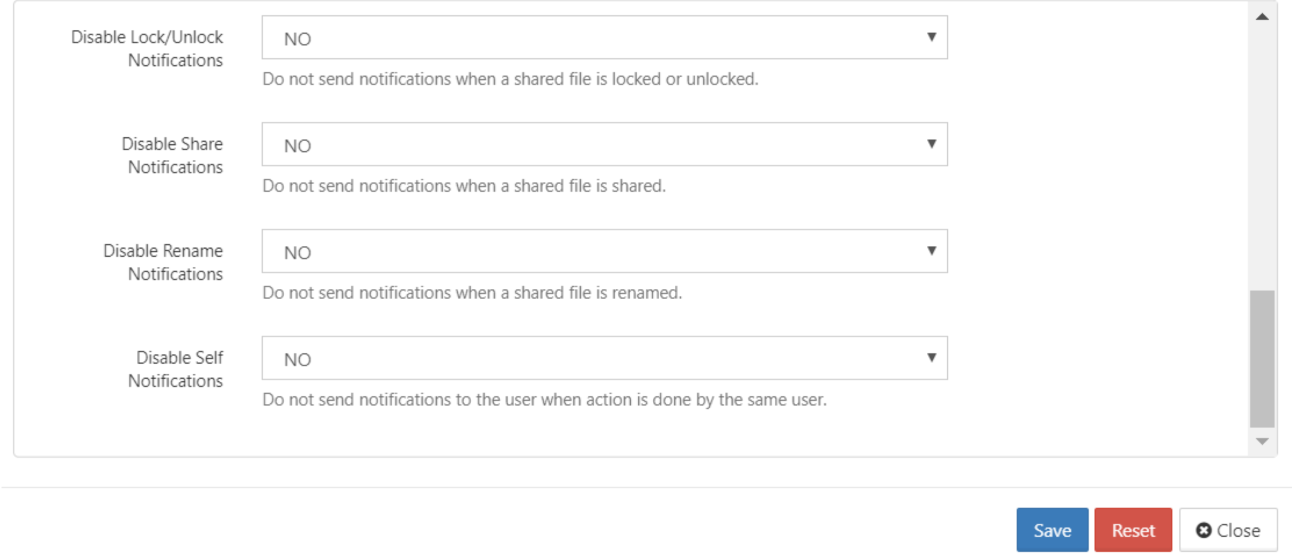


Disable Update Notifications: NO
Do not send notifications when a shared file is updated.

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.

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:

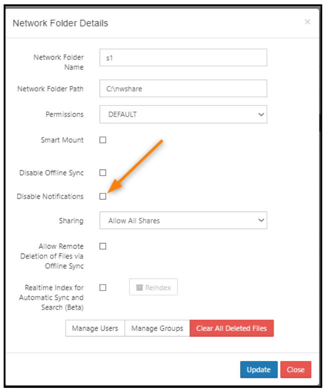
1. Open a browser and log on to the *Admin* portal.
2. From the left navigation panel, under *SETTINGS*, click ***Settings***.
3. On the *Manage Settings* screen, click the ***Policies*** tab.
4. On the *Policies* screen, click the row of the policy you want to customize.
5. On the Manage Policy dialog 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*.

Network Folder Notifications

Network Folder Notifications

Administrators can disable notifications for specific network folders.

Users can override these settings by setting custom notifications for a file or folder paths.



Network Folder Name: s1
Network Folder Path: C:\nwshare
Permissions: DEFAULT
Smart Mount □
Disable Offline Sync □
Disable Notifications □
Sharing: Allow All Shares
Allow Remote Deletion of Files via Offline Sync □
Realtime Index for Automatic Sync and Search (Beta) □

To enable File Change Notifications for Network Folders:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *MANAGE*, select *Network Folders*.
3. On the *Manage Network Folders* screen, select a folder that you change the notification setting for.
4. Click the *Edit Network Folder* (✎) button.
5. On the *Network Folder Details* screen, to enable notifications, clear the *Disable Notifications* checkbox.
6. To save your changes, click *Update*.

NTFS Folders

Many organizations have Windows-based Network Folders that are shared with employees.

- The permissions on these Network Folders are managed using NTFS rights setup for various users and groups (usually from Active Directory).
- FileCloud can use the same NTFS permissions on the Network Folders for user authorization and access to these resources.

For more information, read about Network Folders with NTFS Permissions

💡 By default, file change notifications are disabled for Network folders with NTFS Permissions.

- To enable notifications, you will need to edit a configuration file
- By default, configuration files for FileCloud installation will be under WEBROOT/config

Setting	Option	Description
TONIDOCLOUD_NOTIFICATION_ENABLE_NTFS	0	**Disable notifications for NTFS folders**
TONIDOCLOUD_NOTIFICATION_ENABLE_NTFS	1	**Allow notifications for NTFS folders**

To configure file change notifications for Network folders with NTFS Permissions:

1. Navigate to the following directory:

```
WEBROOT/config
```

2. Open the following file for editing:

```
cloudconfig.php
```

3. Add the following line, using **1 to allow notifications and 0 to disable notifications for NTFS Folders.**

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

Also see:

Customize notifications in user settings

Example Setup: Fixed Notifications for Uploads and Deletions

In this example, a company shares FileCloud support folders with customers so the customers can upload help requests that are then viewed by Support. The customers are also permitted to delete requests that no longer have to be addressed.

As the admin you must set up email notifications that inform Support staff when:

- new help requests are uploaded so they can begin processing them
- existing help requests are deleted in case they have begun addressing them.

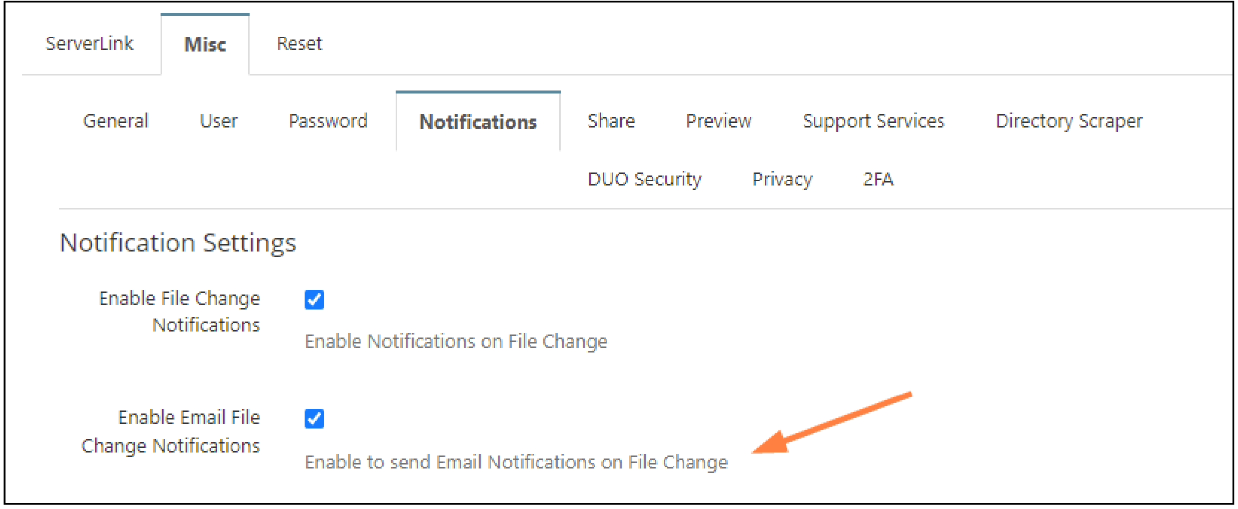
To prevent accidental changes to these notifications, you do not allow users to change the notification settings.

To configure these settings

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**.

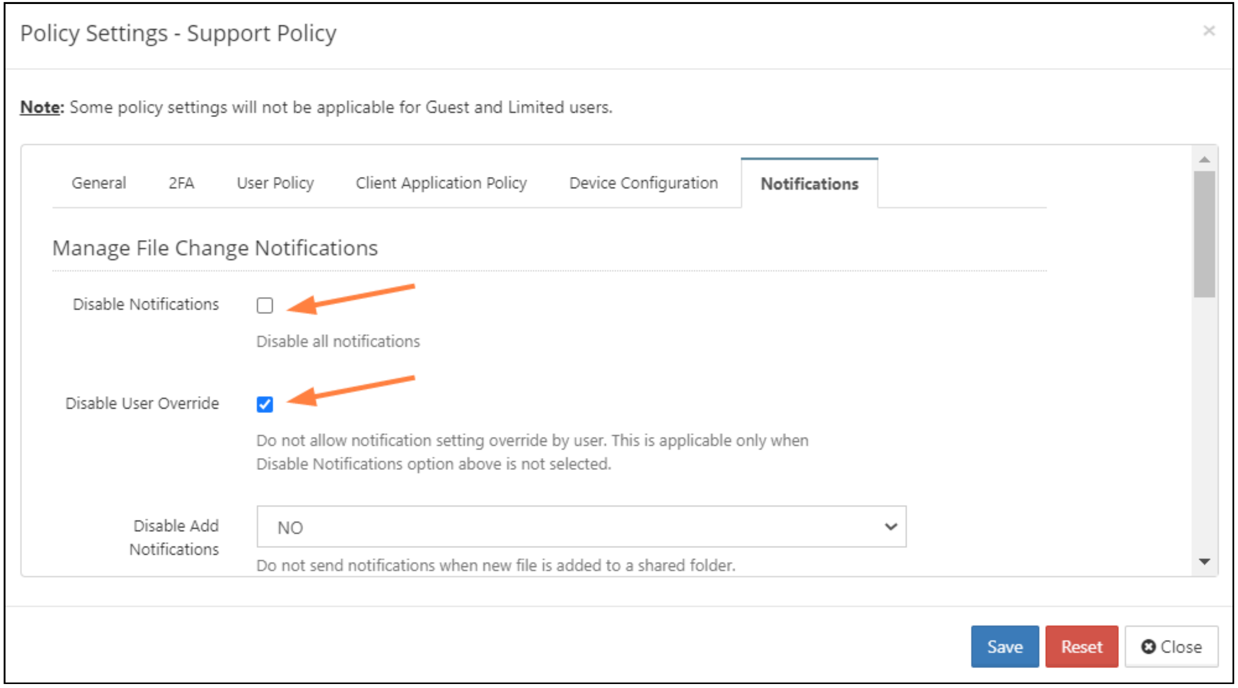


Notification Settings

Enable File Change Notifications ☑
Enable Notifications on File Change

Enable Email File Change Notifications ☑
Enable to send Email Notifications on File Change

4. To 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.

Manage File Change Notifications

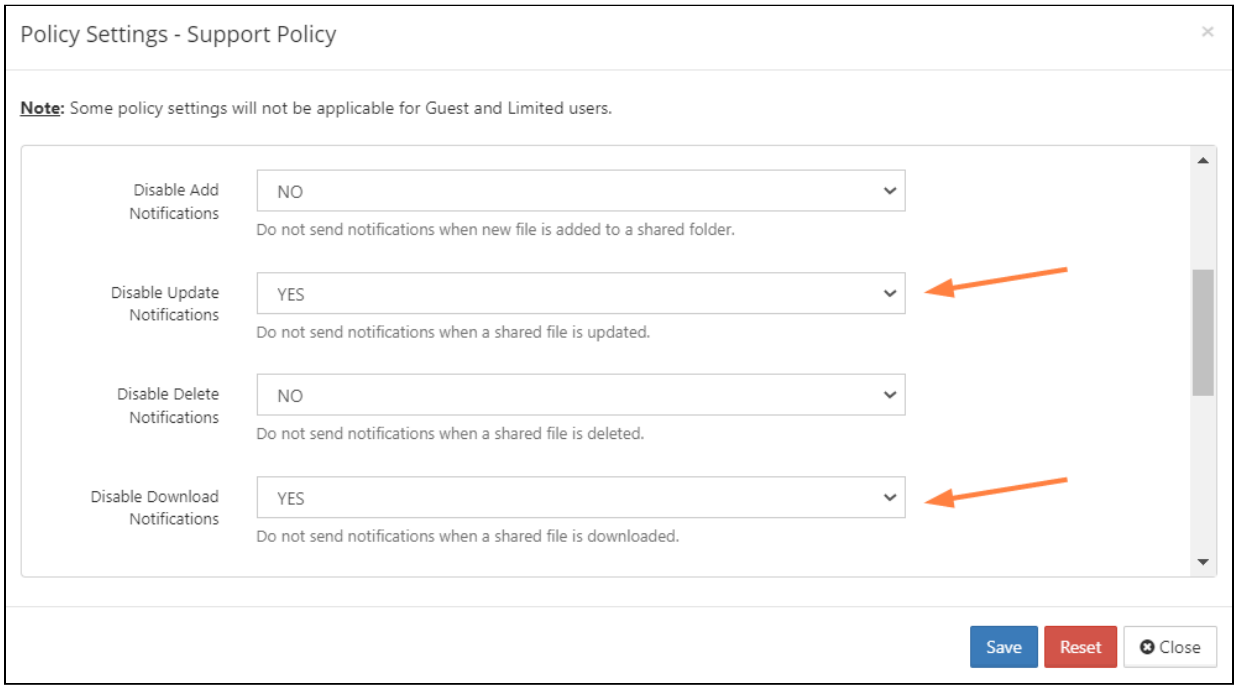
Disable Notifications ☐
Disable all notifications

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.

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: NO
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.

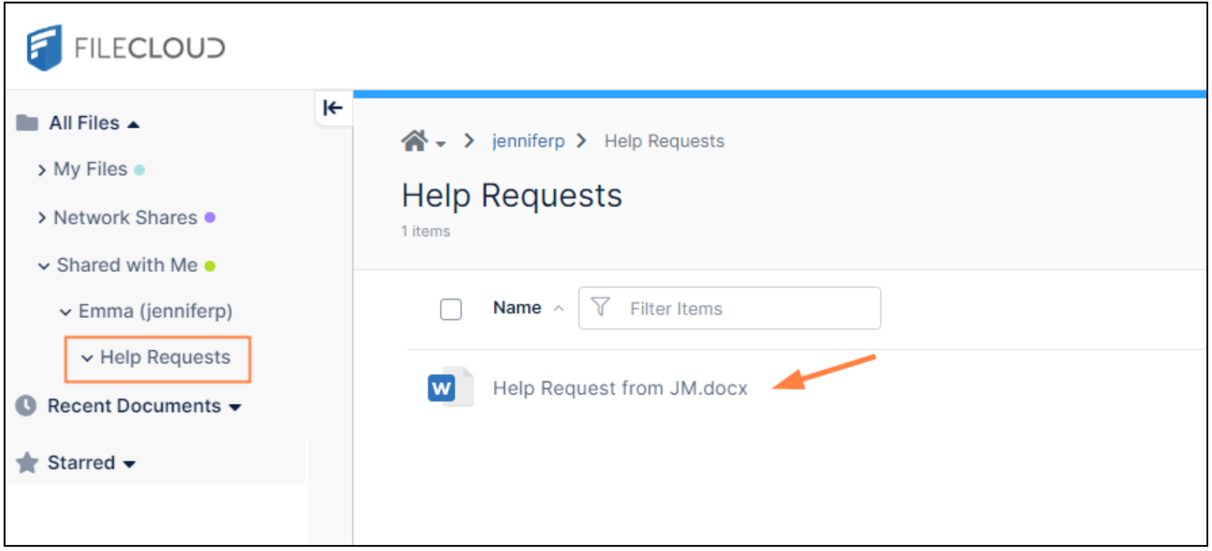
Disable Delete Notifications: NO
Do not send notifications when a shared file is deleted.

Disable Download Notifications: YES
Do not send notifications when a shared file is downloaded.

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**) . . .

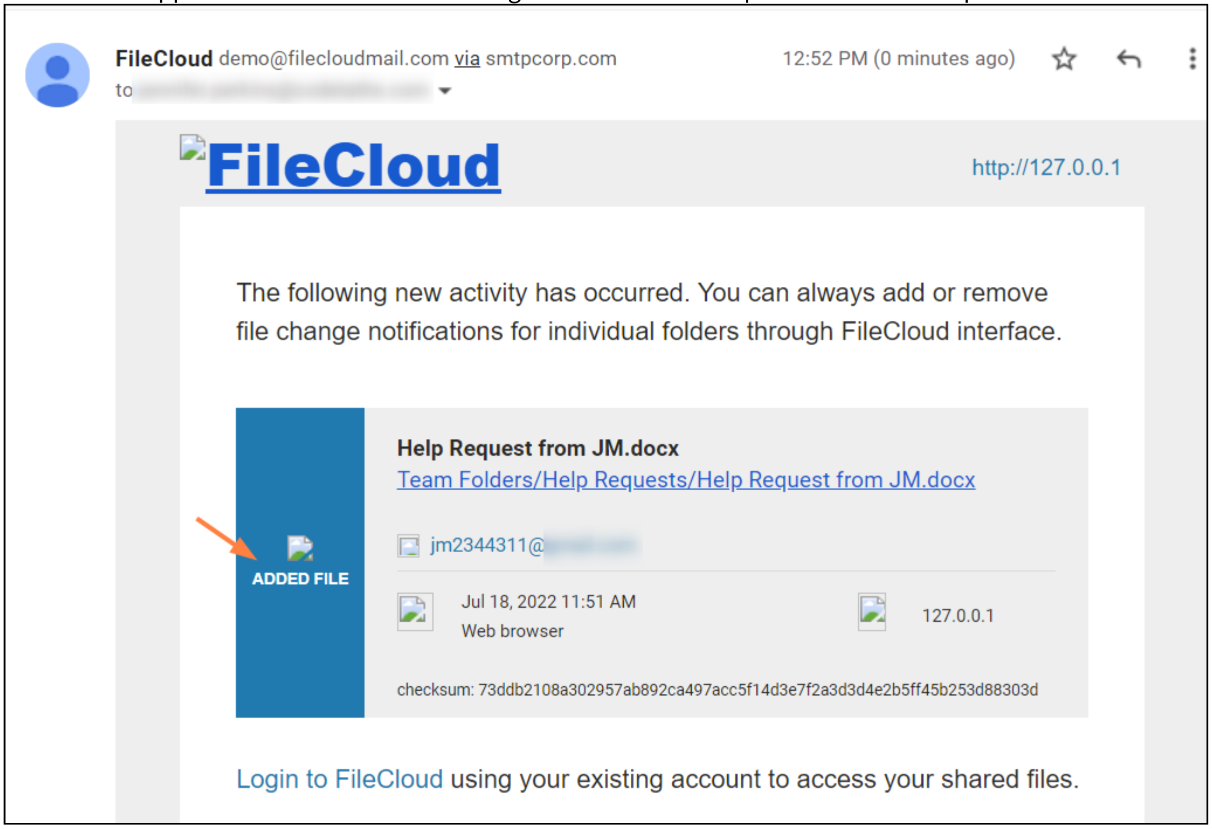


Help Requests

1 items

Help Request from JM.docx

. . . users in support receive an email informing them that a new request file has been uploaded:



FileCloud demo@filecloudmail.com via smtpcorp.com 12:52 PM (0 minutes ago)

to [redacted]

FileCloud http://127.0.0.1

The following new activity has occurred. You can always add or remove file change notifications for individual folders through FileCloud interface.

ADDED FILE

Help Request from JM.docx

Team Folders/Help Requests/Help Request from JM.docx

jm2344311@[redacted]

Jul 18, 2022 11:51 AM
Web browser

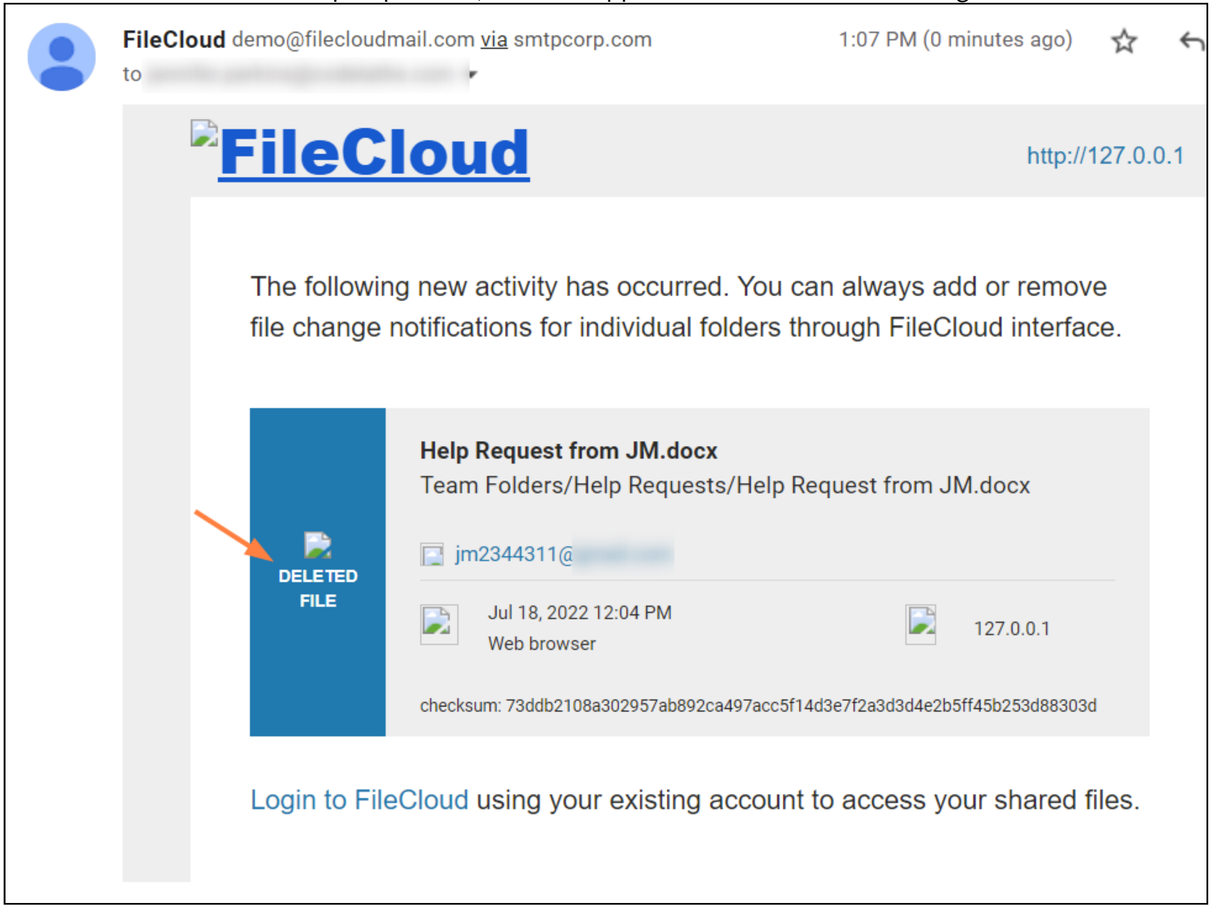
127.0.0.1

checksum: 73ddb2108a302957ab892ca497acc5f14d3e7f2a3d3d4e2b5ff45b253d88303d

Login to FileCloud using your existing account to access your shared files.

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:



FileCloud demo@filecloudmail.com via smtpcorp.com 1:07 PM (0 minutes ago)

to [redacted]

FileCloud http://127.0.0.1

The following new activity has occurred. You can always add or remove file change notifications for individual folders through FileCloud interface.

DELETED FILE

Help Request from JM.docx
Team Folders/Help Requests/Help Request from JM.docx

jm2344311@[redacted]

Jul 18, 2022 12:04 PM
Web browser

127.0.0.1

checksum: 73ddb2108a302957ab892ca497acc5f14d3e7f2a3d3d4e2b5ff45b253d88303d

Login to FileCloud using your existing account to access your shared files.

Example Setup: User-enabled Notifications on Folders

In this example, a telecommunications company uses FileCloud to share Team Folders that hold the latest product and pricing information with everyone in its sales department.

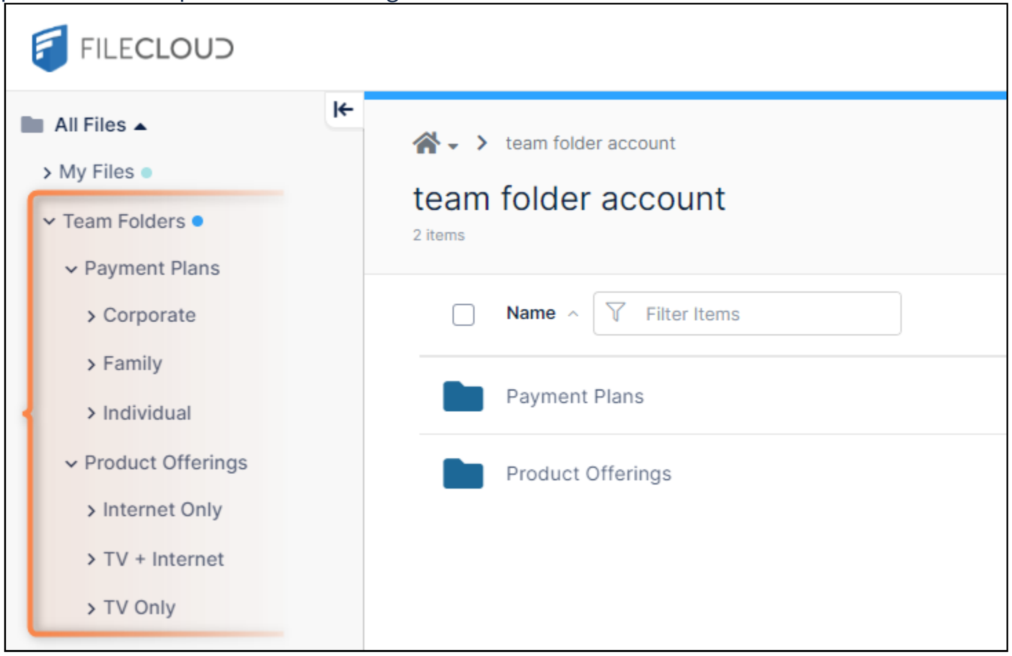
The company has three product offering categories:

- **Internet Only**
- **TV Only**
- **Internet + TV**

and it has three pricing plans:

- **Corporate**
- **Family**
- **Individual**

The company has a Team Folder with information that is available to all sales reps on each product offering and pricing plan. All sales reps see the following under Team Folders:



Each sales representatives works with a specific payment plan and product offering and only needs notifications about the product and pricing plans they work with, and do not want to receive updates about other offerings.

Therefore, as the FileCloud admin, you want each sales rep to be able to customize their file change notifications depending on which campaigns or pricing plans they are currently working with, so they know immediately when these product offerings and prices change. In addition, you want to give sales reps the opportunity to eliminate notifications about information they are not interested in.

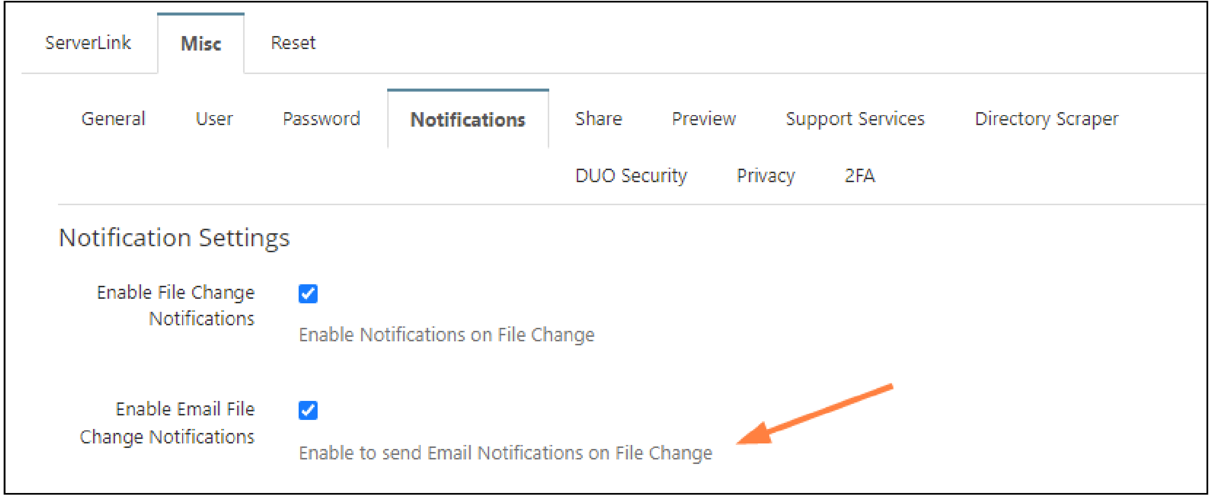
After you configure these capabilities, each sales rep must log in to the user portal and choose the paths of the Team Folders that pertain to them and add notifications to them.

To configure these settings

These are the steps you (the admin) use to set up the notifications according to these requirements:

1. To enable email notifications globally, 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**.

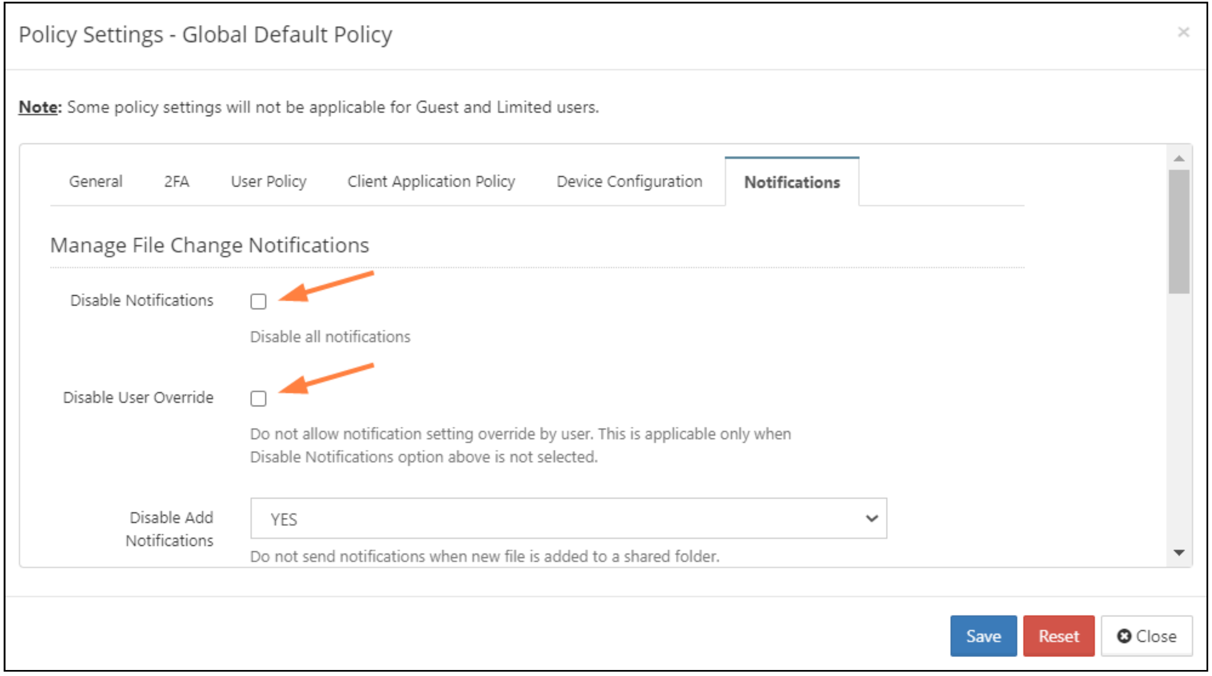


Notification Settings

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.

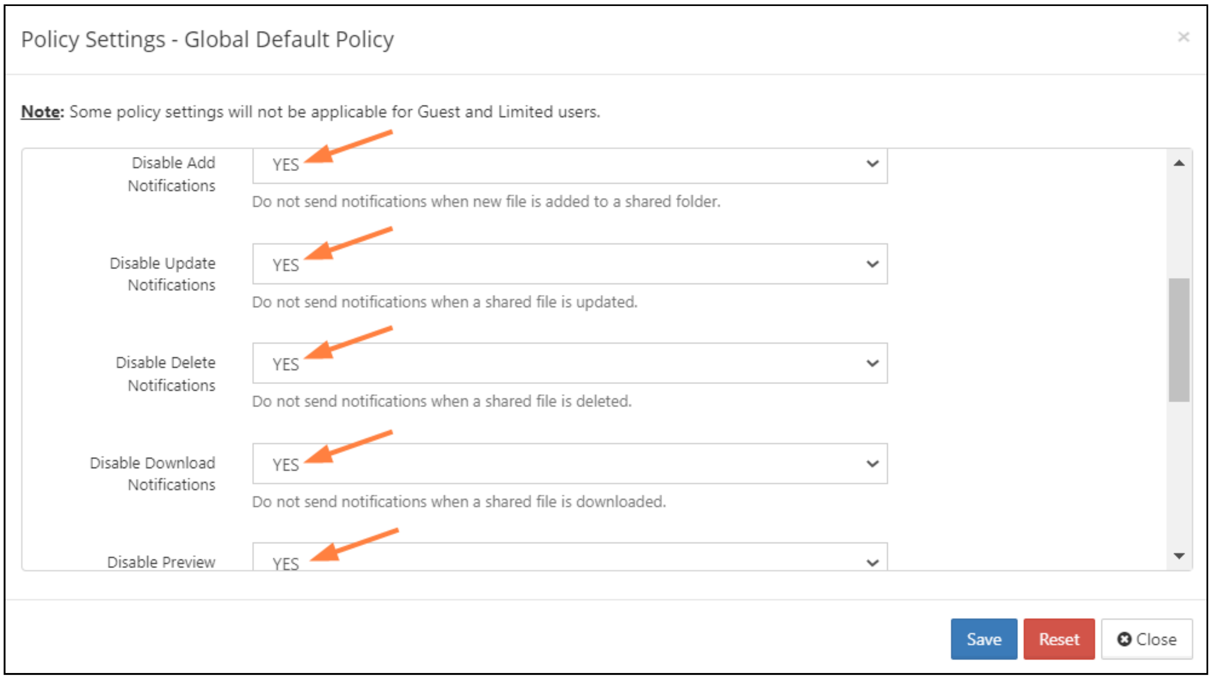
Manage File Change Notifications

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.

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

9. Save your changes.

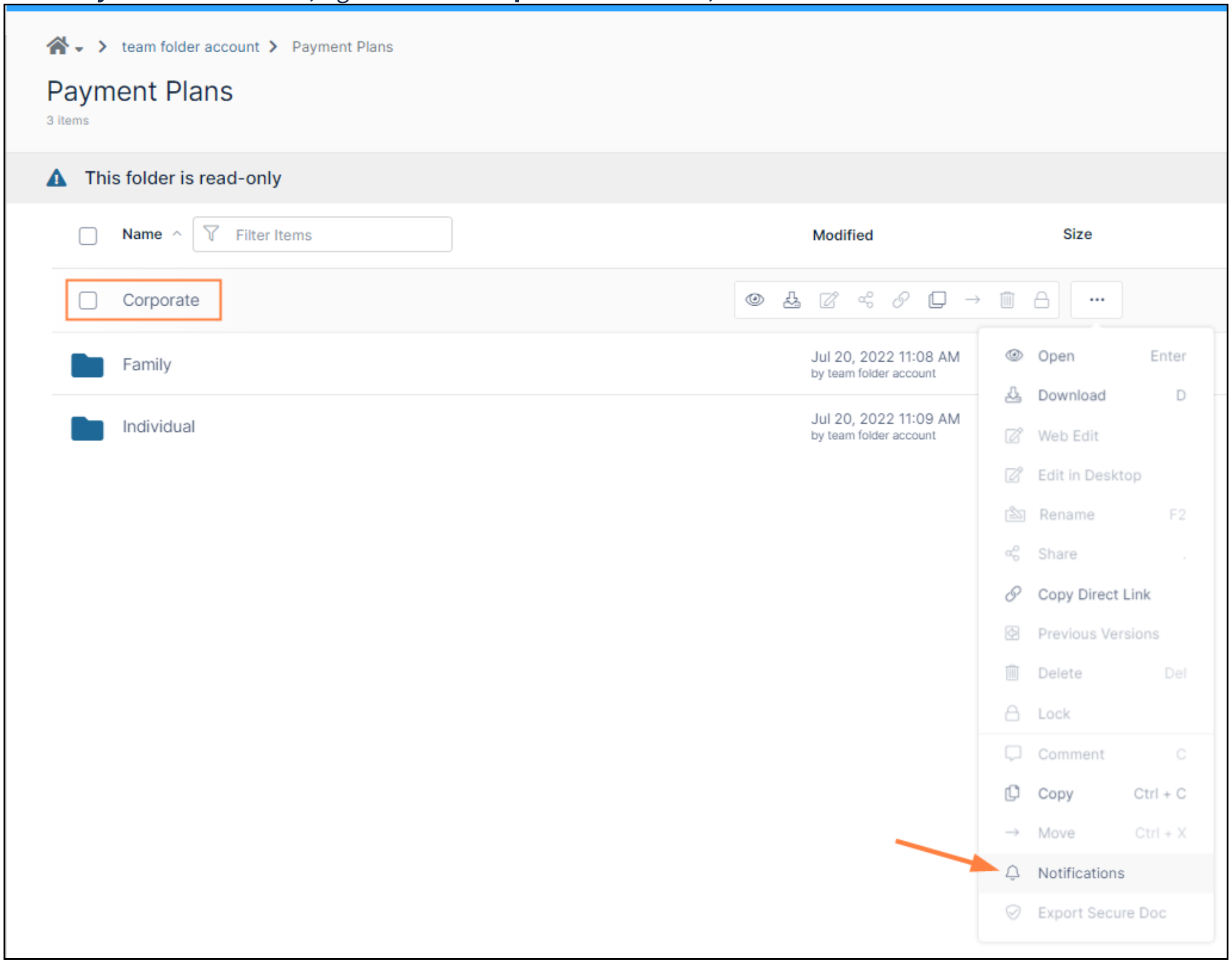
How a Sales Rep sets up notifications about information particular to their clients:

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:

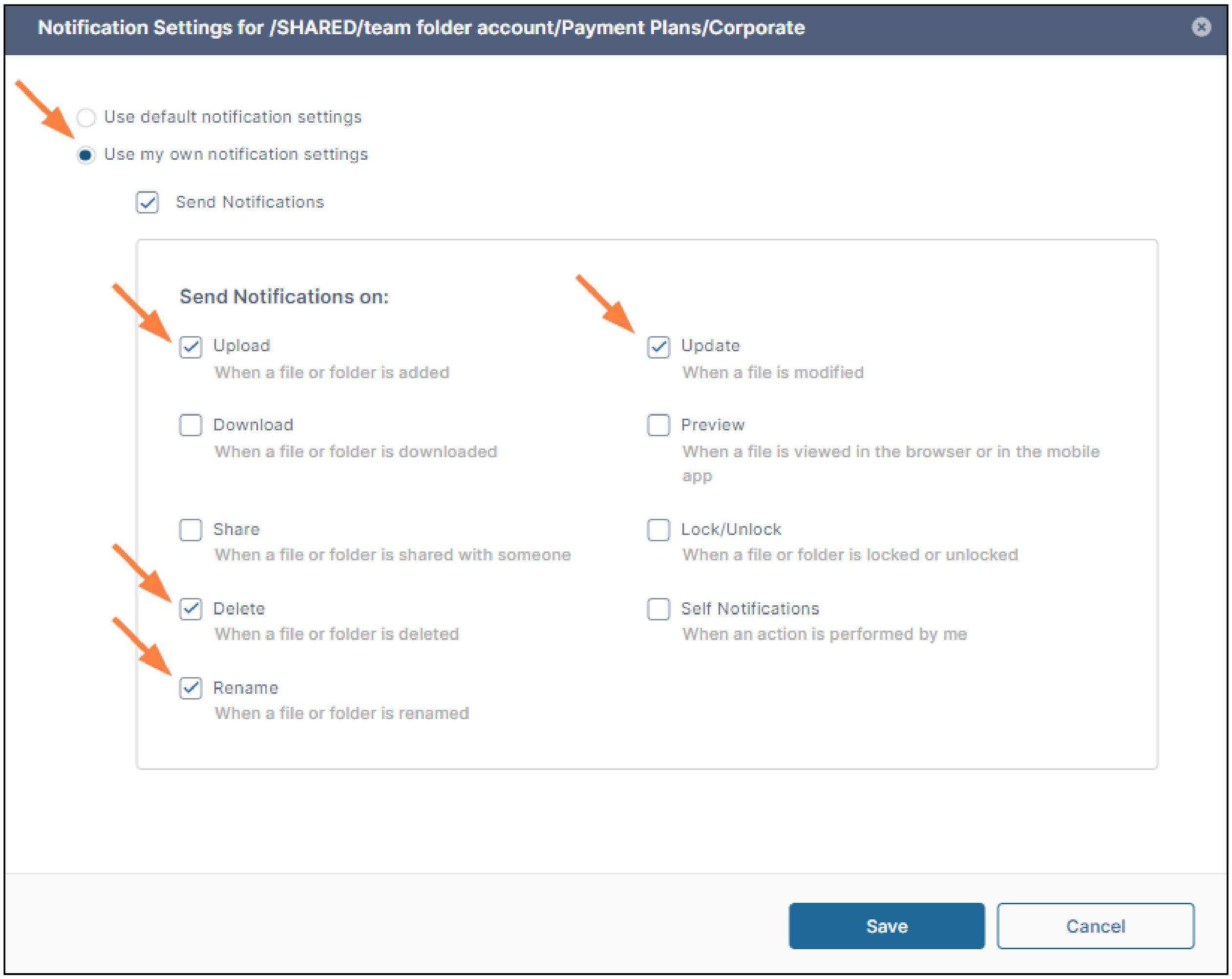
1. Log in to the user portal and go to Team Folders.

2. In the **Payment Plans** folder, right click the **Corporate** sub-folder, and choose **Notifications**.



Notifications settings for the **Corporate** Team Folder open.

3. Select **Use my own notification settings**.
4. Check the actions that you want to be notified about in the folder (for example **Upload**, **Delete**, **Rename**, and **Update**).



Notification Settings for /SHARED/team folder account/Payment Plans/Corporate

○ Use default notification settings

● Use my own notification settings

☑ Send Notifications

Send Notifications on:

☑ Upload
When a file or folder is added

☑ Update
When a file is modified

□ Download
When a file or folder is downloaded

□ Preview
When a file is viewed in the browser or in the mobile app

□ Share
When a file or folder is shared with someone

□ Lock/Unlock
When a file or folder is locked or unlocked

☑ Delete
When a file or folder is deleted

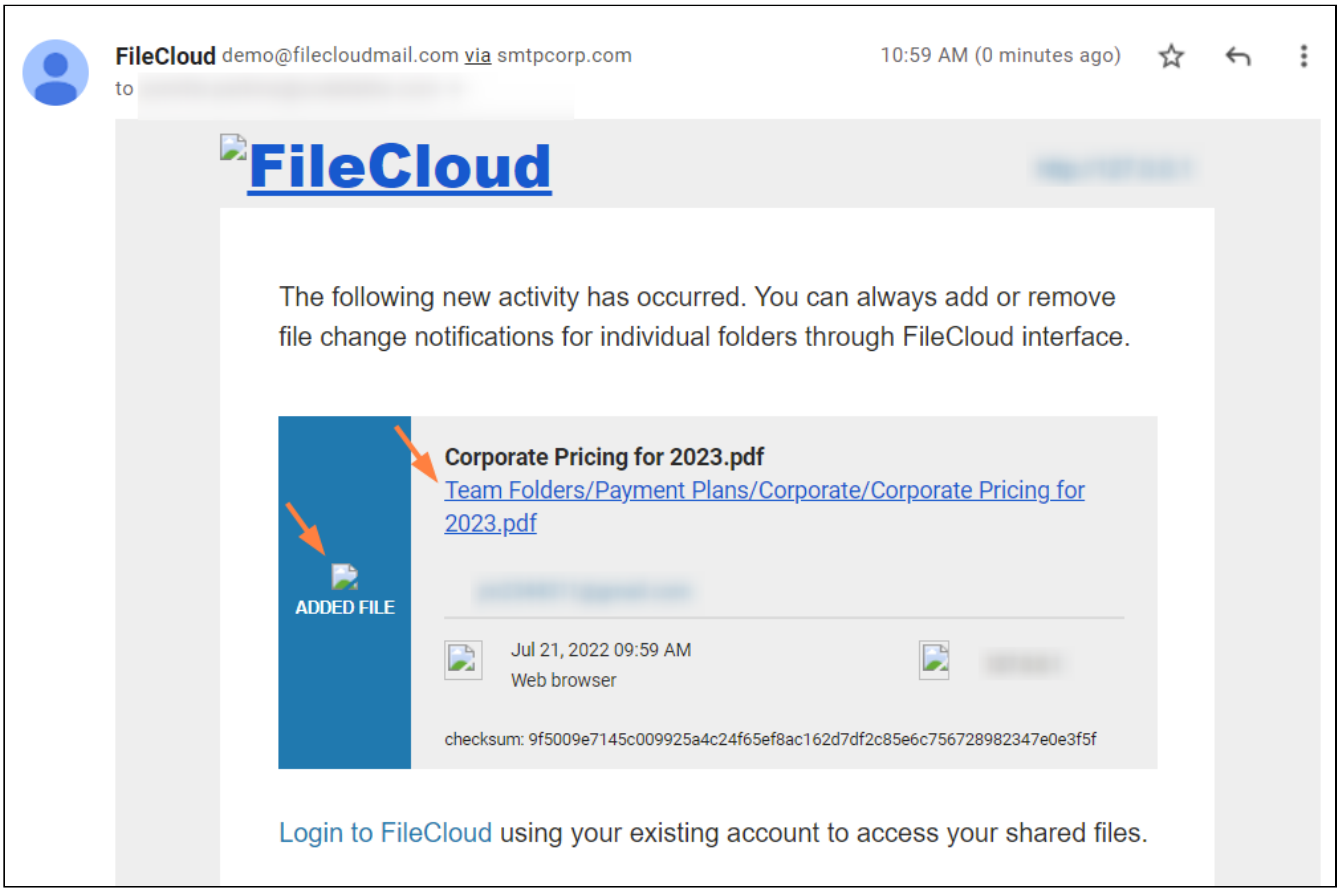
□ Self Notifications
When an action is performed by me

☑ 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:



FileCloud demo@filecloudmail.com via smtpcorp.com 10:59 AM (0 minutes ago)

to [redacted]

FileCloud [redacted]

The following new activity has occurred. You can always add or remove file change notifications for individual folders through FileCloud interface.

ADDED FILE

Corporate Pricing for 2023.pdf

Team Folders/Payment Plans/Corporate/Corporate Pricing for 2023.pdf

[redacted]

Jul 21, 2022 09:59 AM
Web browser

[redacted]

checksum: 9f5009e7145c009925a4c24f65ef8ac162d7df2c85e6c756728982347e0e3f5f

Login to FileCloud using your existing account to access your shared files.

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: • **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.	
Enable WebSocket	General	Enable WebSocket in order to run the Push service or other client/server communications.	FileCloud 23.232

User settings

Setting	Tab	Description
Import Files from Folder on User Creation	User	See: Preload data for new accounts
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 approval

Setting	Tab	Description
Default Grid View Settings	User	Select how files appear to users by default. (See: Viewing Files by List or Grid). The options are: (size varies depending on screen resolution) • **Automatic** - The default. Initially, **Automatic** is List view. Once the view is changed by the admin or by the user, **Automatic** is the user's most recent view. • **Large Thumbnails** - Grid of thumbnails that are approximately 400 by 400 pixels. • **Medium Thumbnails** - Grid of thumbnails that are approximately 280 by 280 pixels. • **Small Thumbnails** - Grid of thumbnails that are approximately 200 by 200 pixels. • **List View**
Allow users to set phone numbers	User	Select to allow users to change their phone numbers in the user portal Settings screen.

Notifications settings

Setting	Tab	Description
Enable File Change Notifications	Notifications	When checked, enables recent activity notifications to appear on the user portal when files are created, updated, deleted and downloaded on a shared folder. Checked by default.
Enable Email File Change Notifications	Notifications	When checked, enables the system to send Email notifications when files are created, updated, deleted and downloaded on a shared folder. Enable File Change Notifications must be checked for this setting to be enabled. Checked by default.
Disable Email Notifications for External Users	Notifications	When this option is enabled no share notifications will be sent to the external user.
Enable Share Notification	Notifications	When this option is enabled share notifications will be set to NO by default. The "Email FileChange Notifications" will be set to NO in Manage Share → advanced options.
Enable New Version Email Notification	Notifications	When checked, emails about new versions of FileCloud are sent to the administrator once a week.

Setting	Tab	Description
Number of Days After which Notifications are not sent	Notification s	Do not sent notifications for actions that occurred before the set number of days
Email Notification Frequency	Notification s	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 document preview settings, see Document Preview and Enabling Document Converter and Thumbs.

For support service settings, see Improve Helper Performance.

For directory scraper, see Enabling Directory Scraping.

For DUO security settings, see Two Factor Authentication.

For privacy settings, see Terms of Service and Anonymizing User Data,

For 2fa settings, see Two Factor Authentication

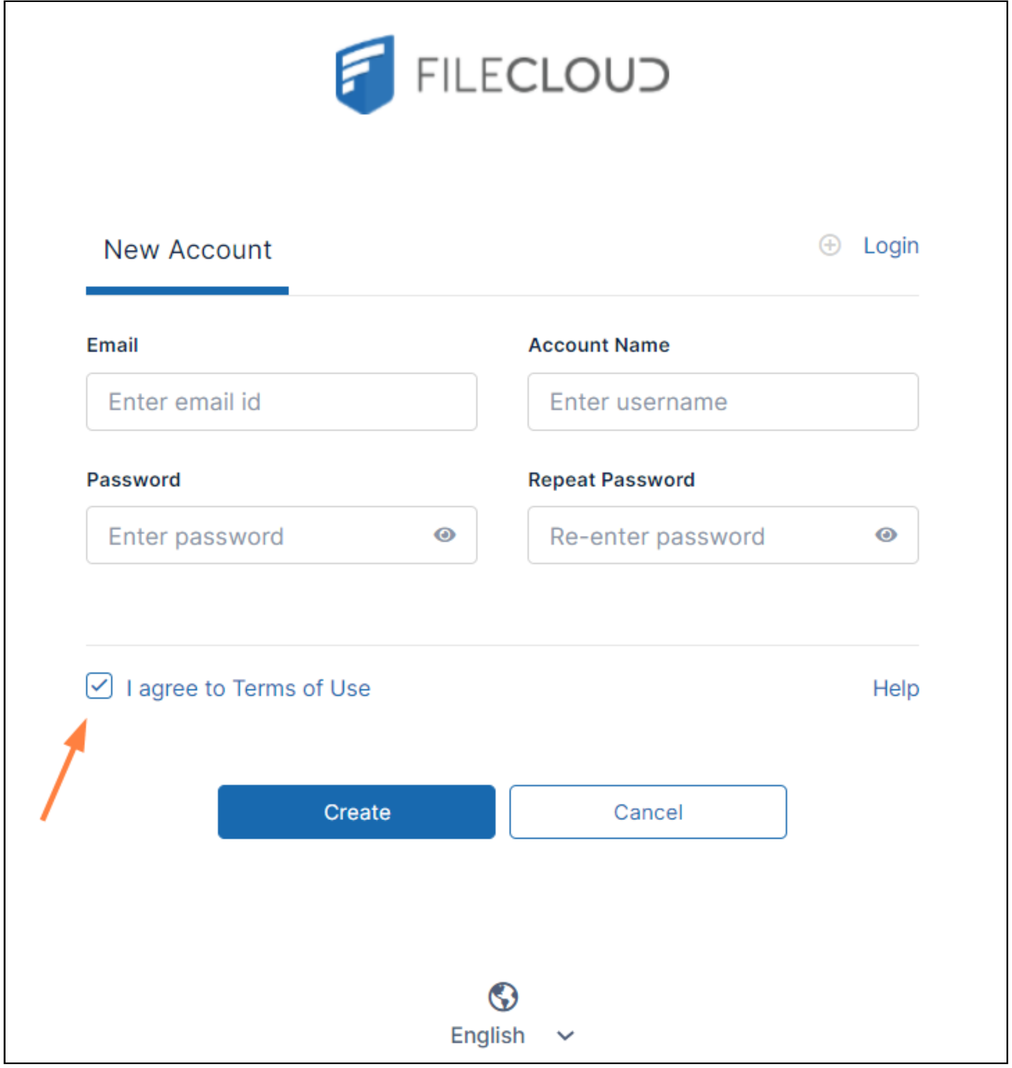
Terms of Service

ⓘ Beginning with FileCloud Version 21.3, when **Enable Privacy Settings** is set to **YES** in their user policies, admin users are required to accept terms of service the first time they log into the admin portal.

⚠ Beginning with FileCloud Version 22.232, the default link to FileCloud terms of service has changed to https://www.filecloud.com/eula/. The link will only be changed automatically on new installations of FileCloud. Although the previous link will automatically redirect users to the new page, if you are upgrading FileCloud to version 23.232 or using an earlier version, we recommend that you change the link in **Customization > TOS** to https://www.filecloud.com/eula/

By default, FileCloud requires users to accept terms of service (TOS) when:

- they initially create an account
- the content of terms of service changes.



FILECLOUD

New Account

Login

Email: Enter email id

Account Name: Enter username

Password: Enter password

Repeat Password: Re-enter password

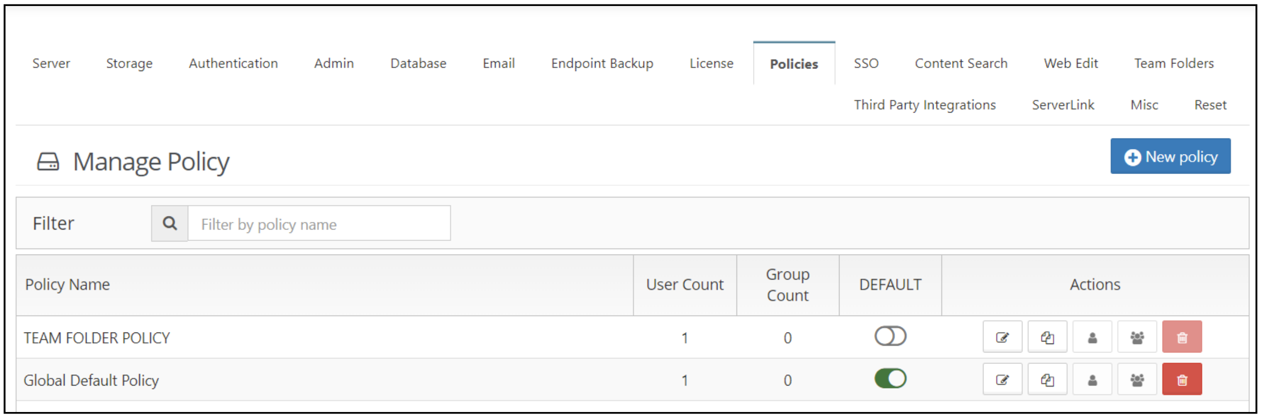
☑ I agree to Terms of Use

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:

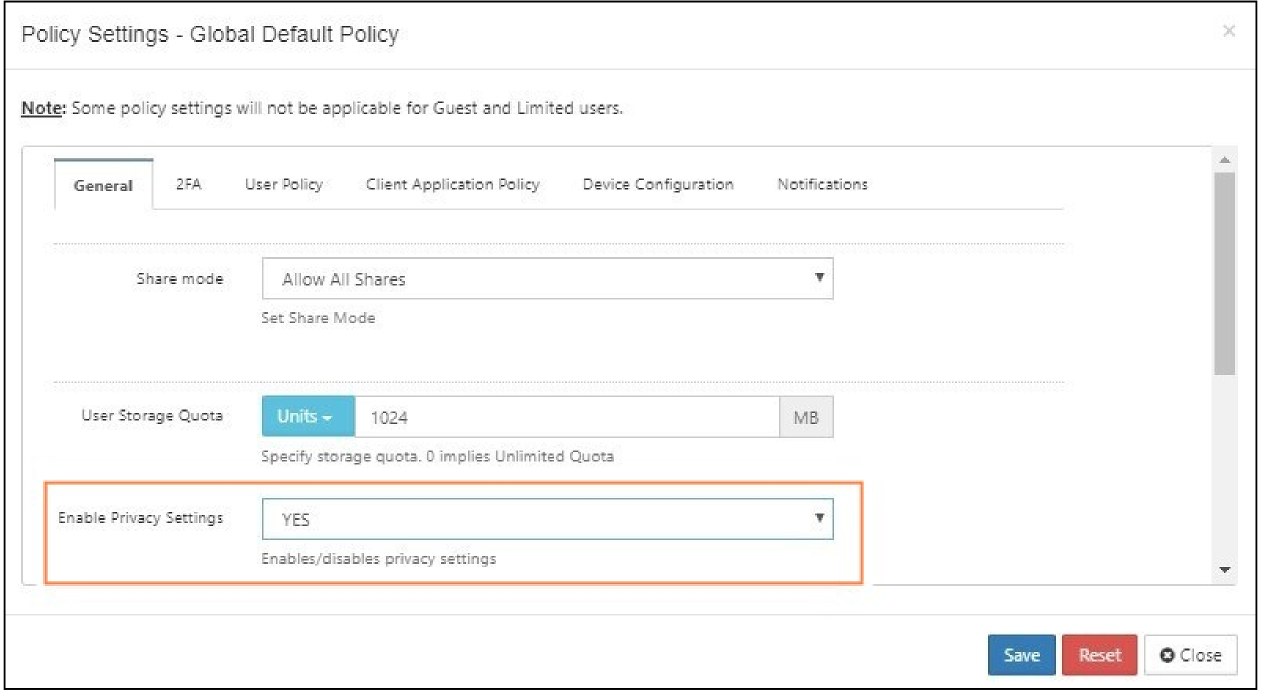
1. From the left navigation panel, click **Settings**.
2. Click the **Policies** tab.



Manage Policy

Policy Name	User Count	Group Count	DEFAULT	Actions
TEAM FOLDER POLICY	1	0	○	
Global Default Policy	1	0	●	

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**.



Policy Settings - Global Default Policy

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

Share mode: Allow All Shares
Set Share Mode

User Storage Quota: 1024 MB
Specify storage quota. 0 implies Unlimited Quota

Enable Privacy Settings: YES
Enables/disables privacy settings

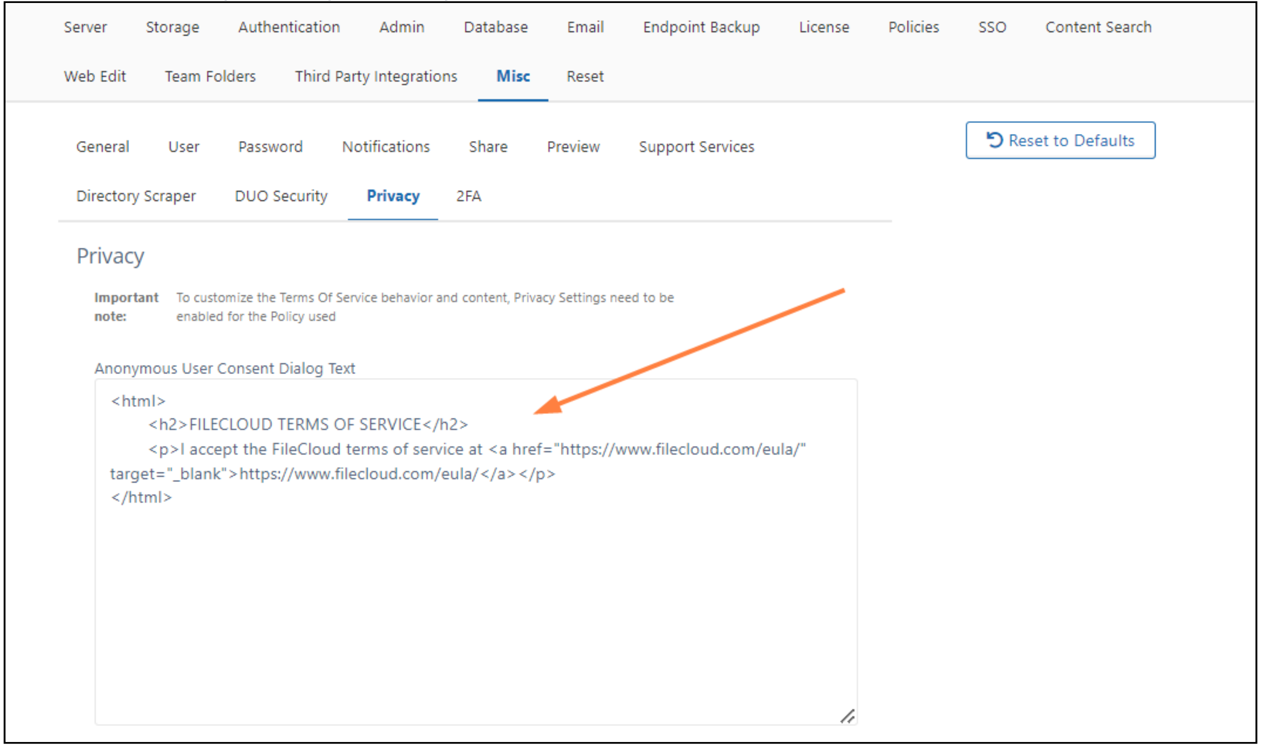
5. Click **Save**.

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:



Privacy

Important note: To customize the Terms Of Service behavior and content, Privacy Settings need to be enabled for the Policy used

Anonymous User Consent Dialog Text

```
<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

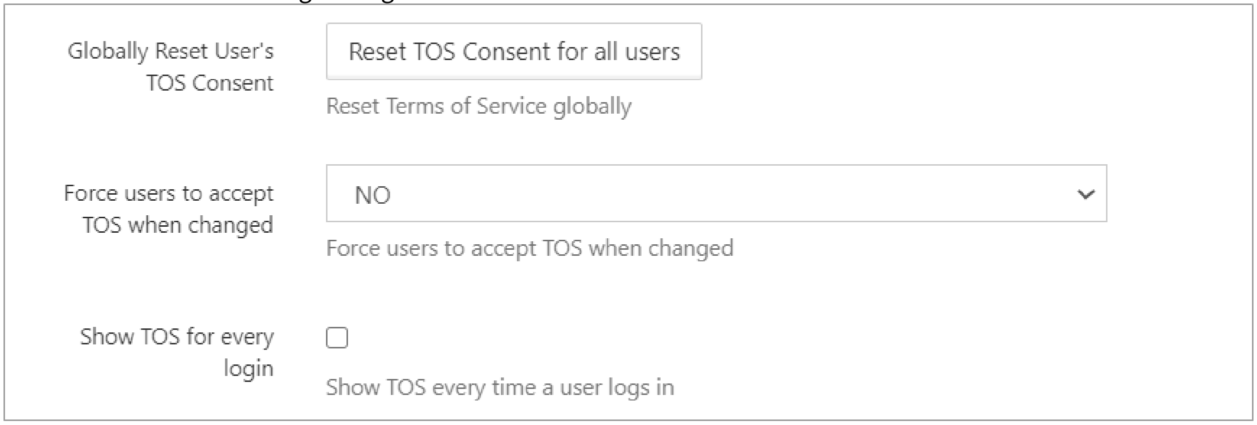
Administrators are able to configure the following terms of service settings:

- 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

> 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: Reset TOS Consent for all users
Reset Terms of Service globally

Force users to accept TOS when changed: NO
Force users to accept TOS when changed

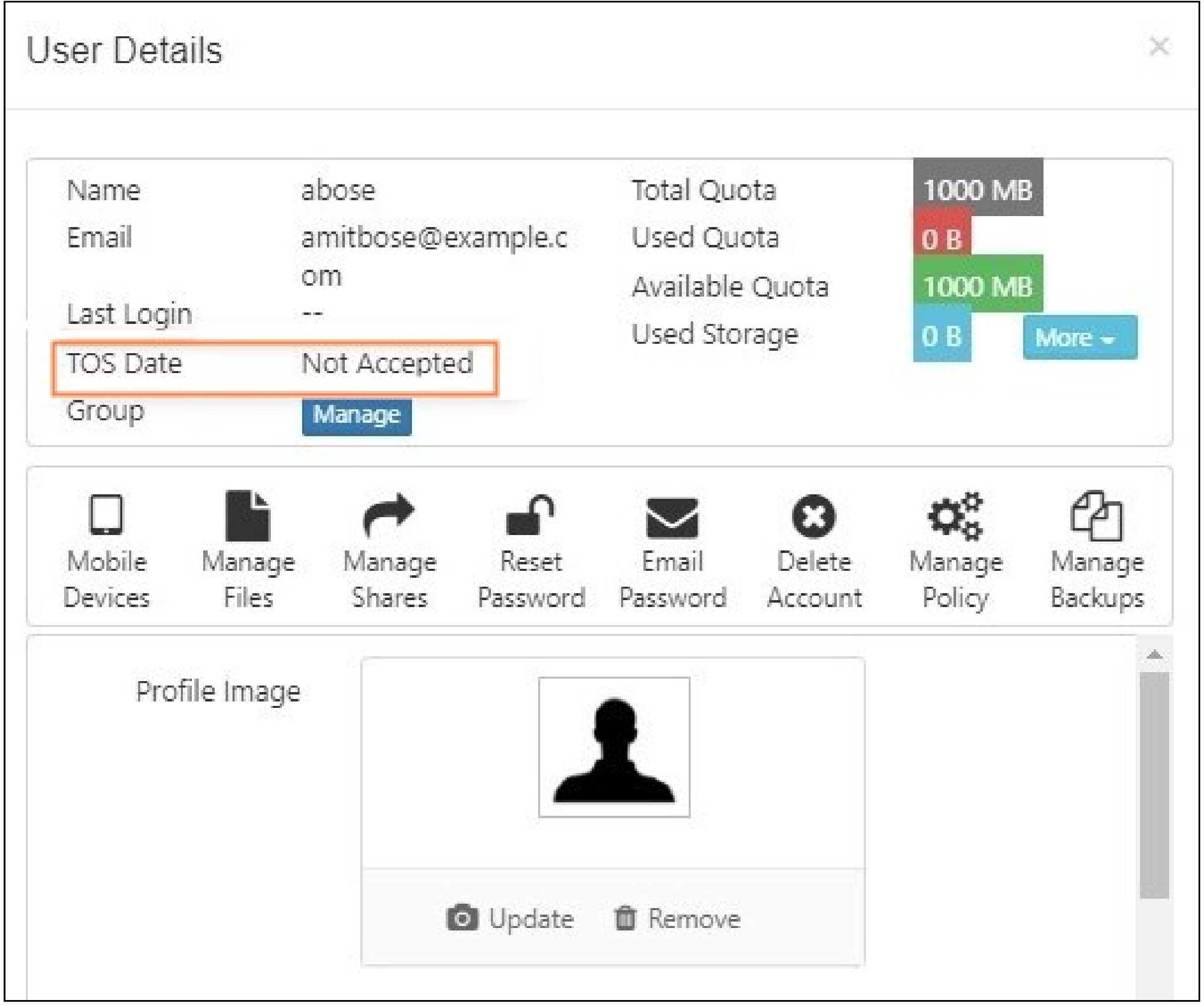
Show TOS for every login: □
Show TOS every time a user logs in

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

Email amitbose@example.com

Last Login --

TOS Date Not Accepted

Group Manage

Total Quota 1000 MB

Used Quota 0 B

Available Quota 1000 MB

Used Storage 0 B

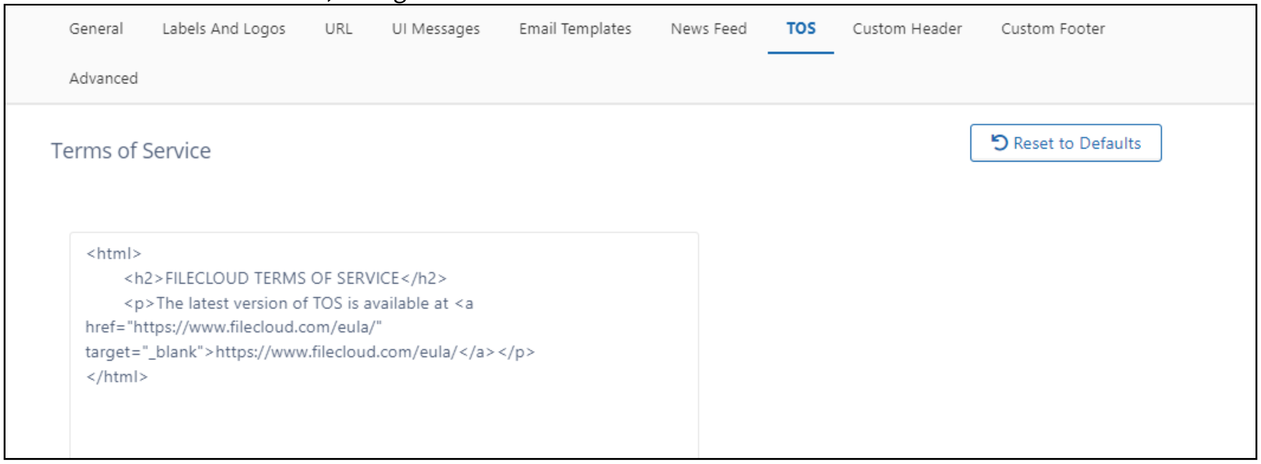
Profile Image

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**.



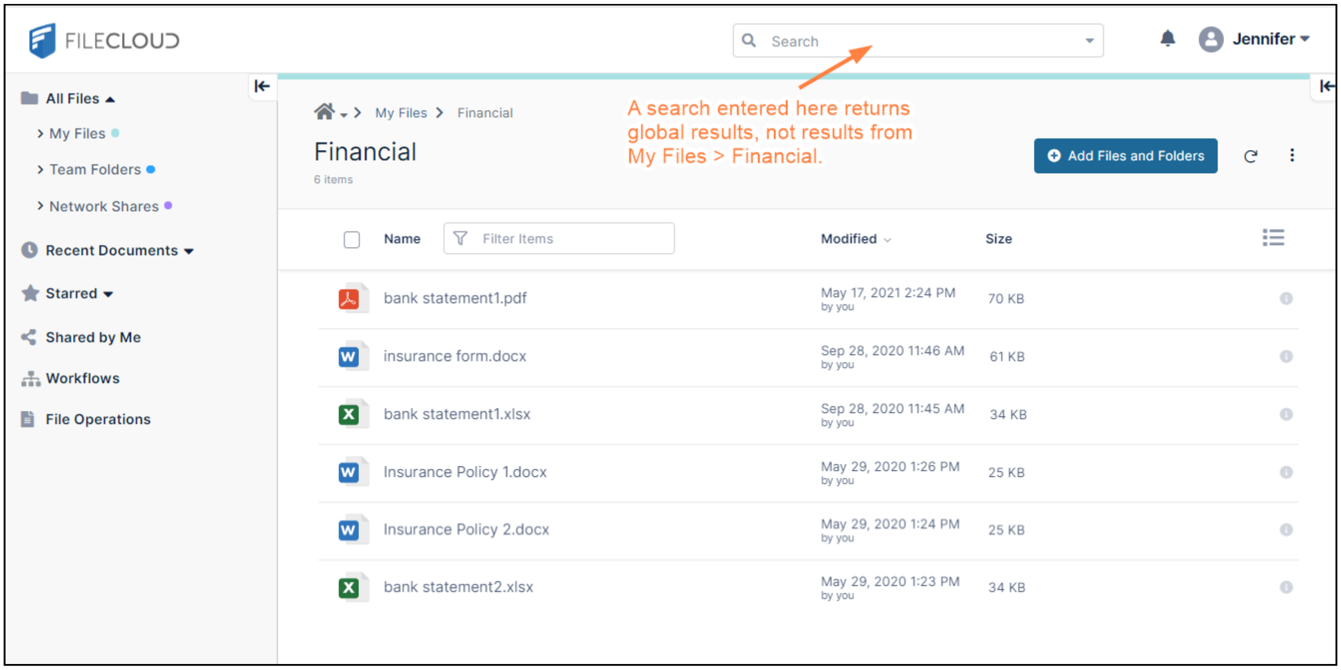
```
<html>
      <h2>FILECLOUD TERMS OF SERVICE</h2>
      <p>The latest version of TOS is available at <a
href="https://www.filecloud.com/eula/"
target="_blank">https://www.filecloud.com/eula/</a></p>
</html>
```

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

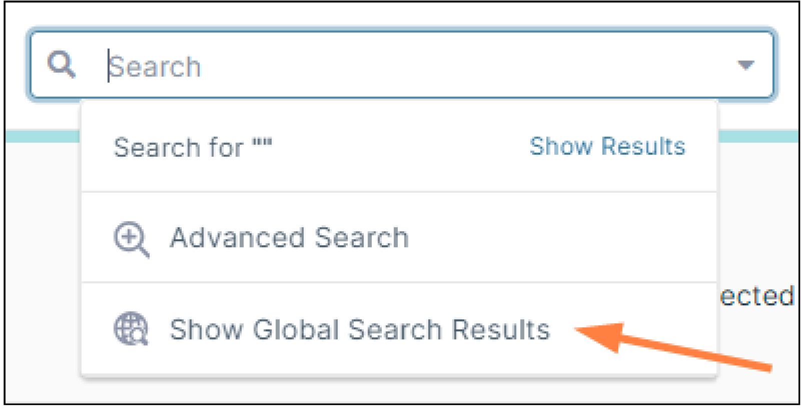
By default, basic searches from the user portal header's search bar are performed globally, regardless of where the user has navigated in the folders shown in the main part of the screen.



A search entered here returns global results, not results from My Files > Financial.

Name	Modified	Size
bank statement1.pdf	May 17, 2021 2:24 PM by you	70 KB
insurance form.docx	Sep 28, 2020 11:46 AM by you	61 KB
bank statement1.xlsx	Sep 28, 2020 11:45 AM by you	34 KB
Insurance Policy 1.docx	May 29, 2020 1:26 PM by you	25 KB
Insurance Policy 2.docx	May 29, 2020 1:24 PM by you	25 KB
bank statement2.xlsx	May 29, 2020 1:23 PM by you	34 KB

A setting is available for changing the default search location to the current path shown in the user portal. In the above screen, if the setting were turned on, searches would begin at the **My Files/Financial** folder.
The setting adds the option **Show Global Search Results** when users click in the Search bar so users still have the ability to search globally:



To set the search to begin from the current path but include the global search option:

1. Open cloudconfig.php at
   - Windows: XAMPP DIRECTORY\htdocs\config\cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Add the setting:

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

To return to a global search only:

1. Change the value of **TONIDOCLOUD_START_SEARCHES_ON_CURRENT_NAVIGATION_LOCATION** from **true** to **false**.

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

Migrating 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.

Currently, you may enable or disable WebDAV in your configuration file. For help, 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.

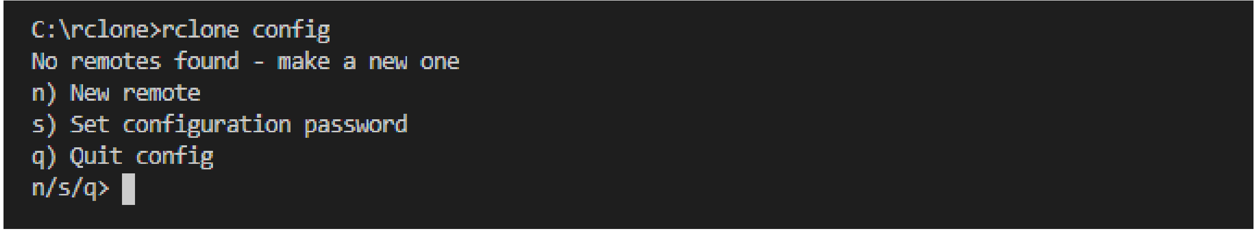
1. Download Rclone
2. Enable WebDav protocol in FileCloud.
3. Configure Rclone

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@codelathe.com.

Creating a FileCloud WebDav Configuration in Rclone

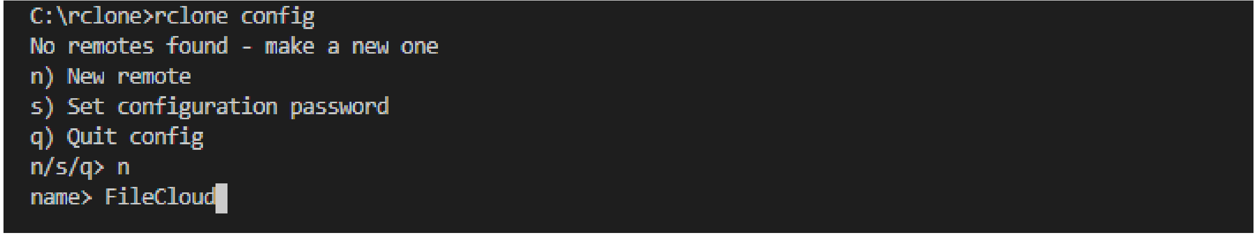
Once you have completed the above requirements, create your FileCloud configuration profile in Rclone.

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**



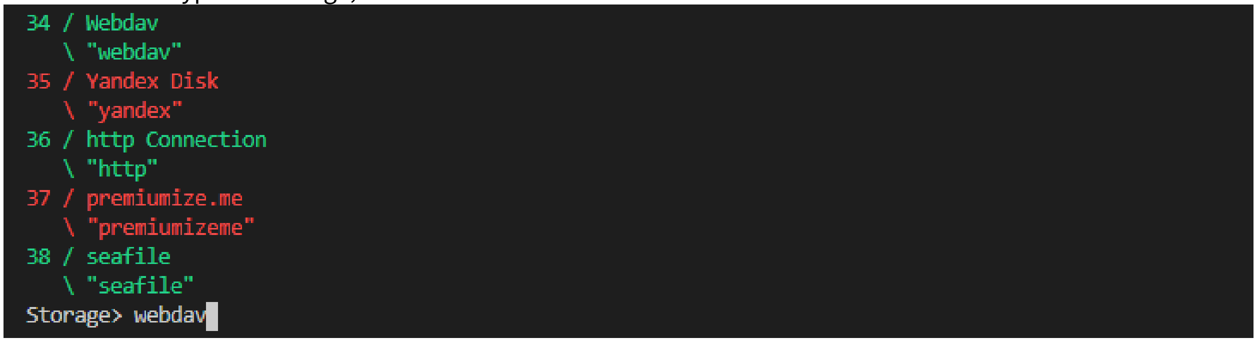
```
C:\rclone>rclone config
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q>
```

3. From the menu options enter **n** to create a new remote profile and enter **FileCloud**, and click enter.



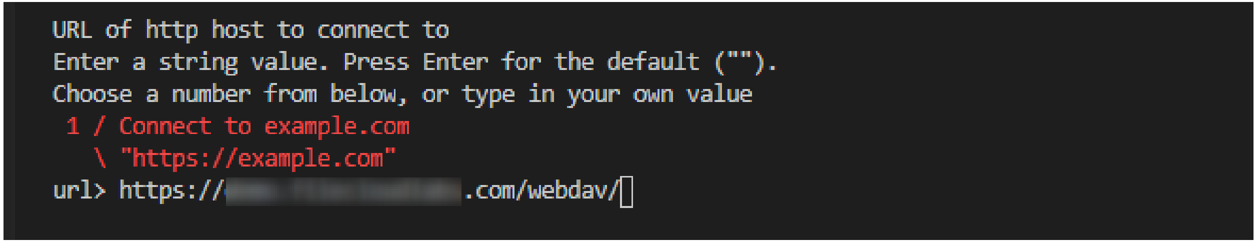
```
C:\rclone>rclone config
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> FileCloud
```

4. From the list of types of storage, enter **webdav.** and click enter.



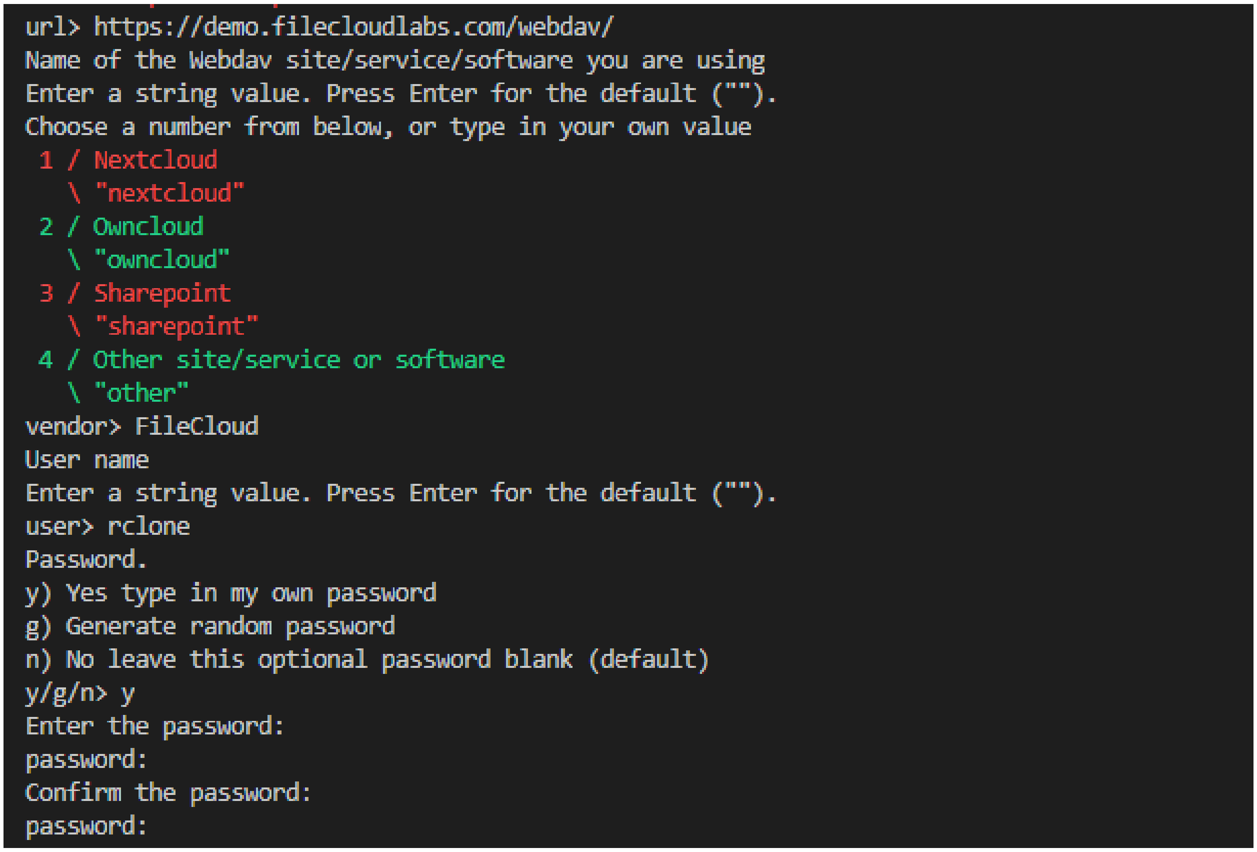
```
34 / Webdav
   \ "webdav"
35 / Yandex Disk
   \ "yandex"
36 / http Connection
   \ "http"
37 / premiumize.me
   \ "premiumizeme"
38 / seafile
   \ "seafile"
Storage> webdav
```

5. 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/**



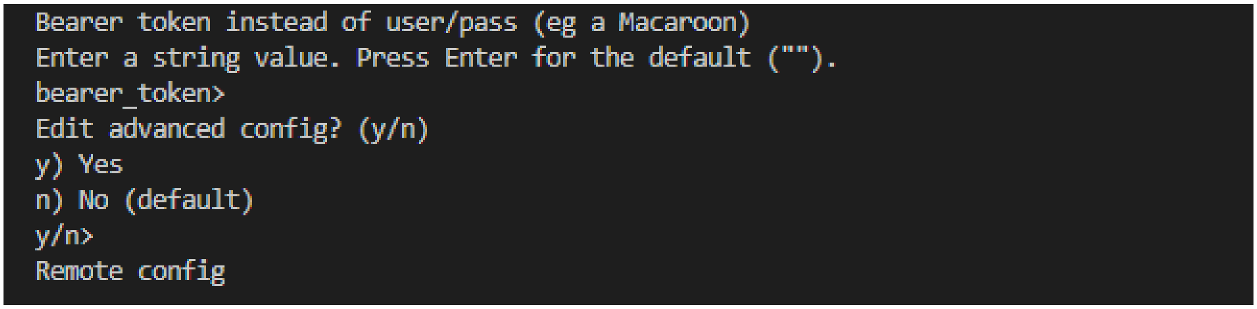
```
URL of http host to connect to
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / Connect to example.com
   \ "https://example.com"
url> https://[redacted].com/webdav/
```

6. 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.
7. Now you are prompted to enter your FileCloud user name and password.
   In this example we are using a user named **rclone**.



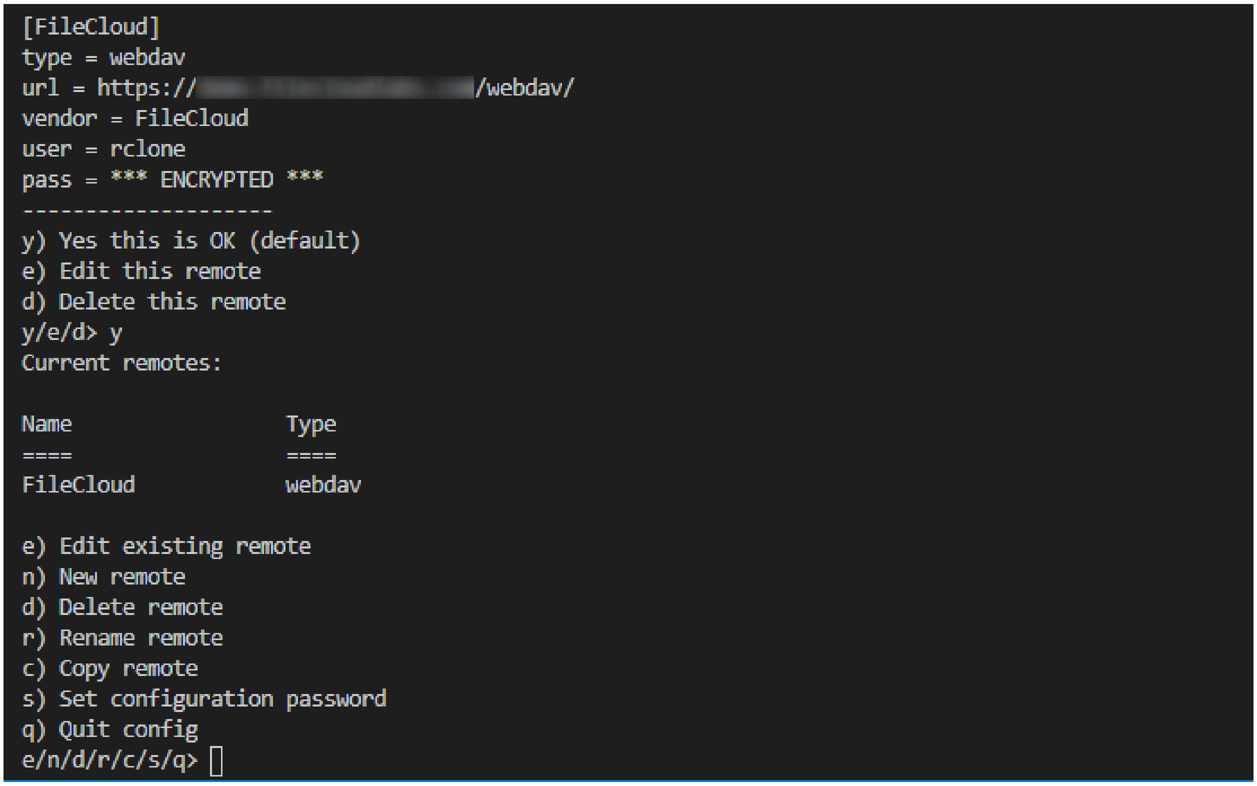
```
url> https://demo.filecloudlabs.com/webdav/
Name of the Webdav site/service/software you are using
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / Nextcloud
   \ "nextcloud"
 2 / Owncloud
   \ "owncloud"
 3 / Sharepoint
   \ "sharepoint"
 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.



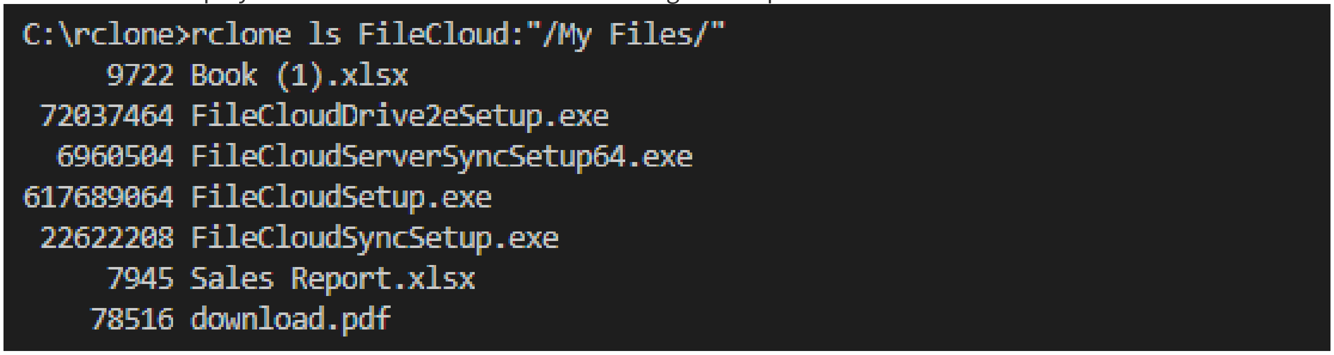
```
[FileCloud]
type = webdav
url = https://[redacted]/webdav/
vendor = FileCloud
user = rclone
pass = *** ENCRYPTED ***
--------------------
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
y/e/d> y
Current remotes:

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 creatied 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

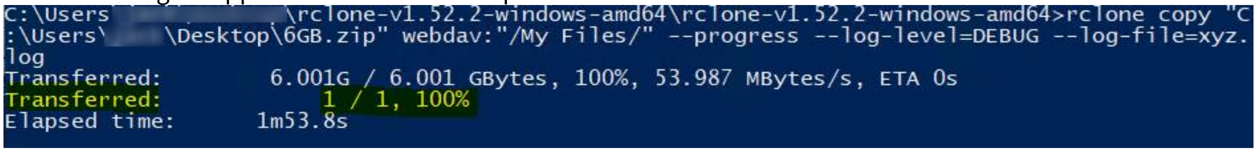
- By default when using WebDav, FileCloud has a single file maximum upload size limitation of 524288000 bytes. You can increase this parameter by accessing :

  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[redacted]\rclone-v1.52.2-windows-amd64\rclone-v1.52.2-windows-amd64>rclone copy "C
:\Users\[redacted]\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
```

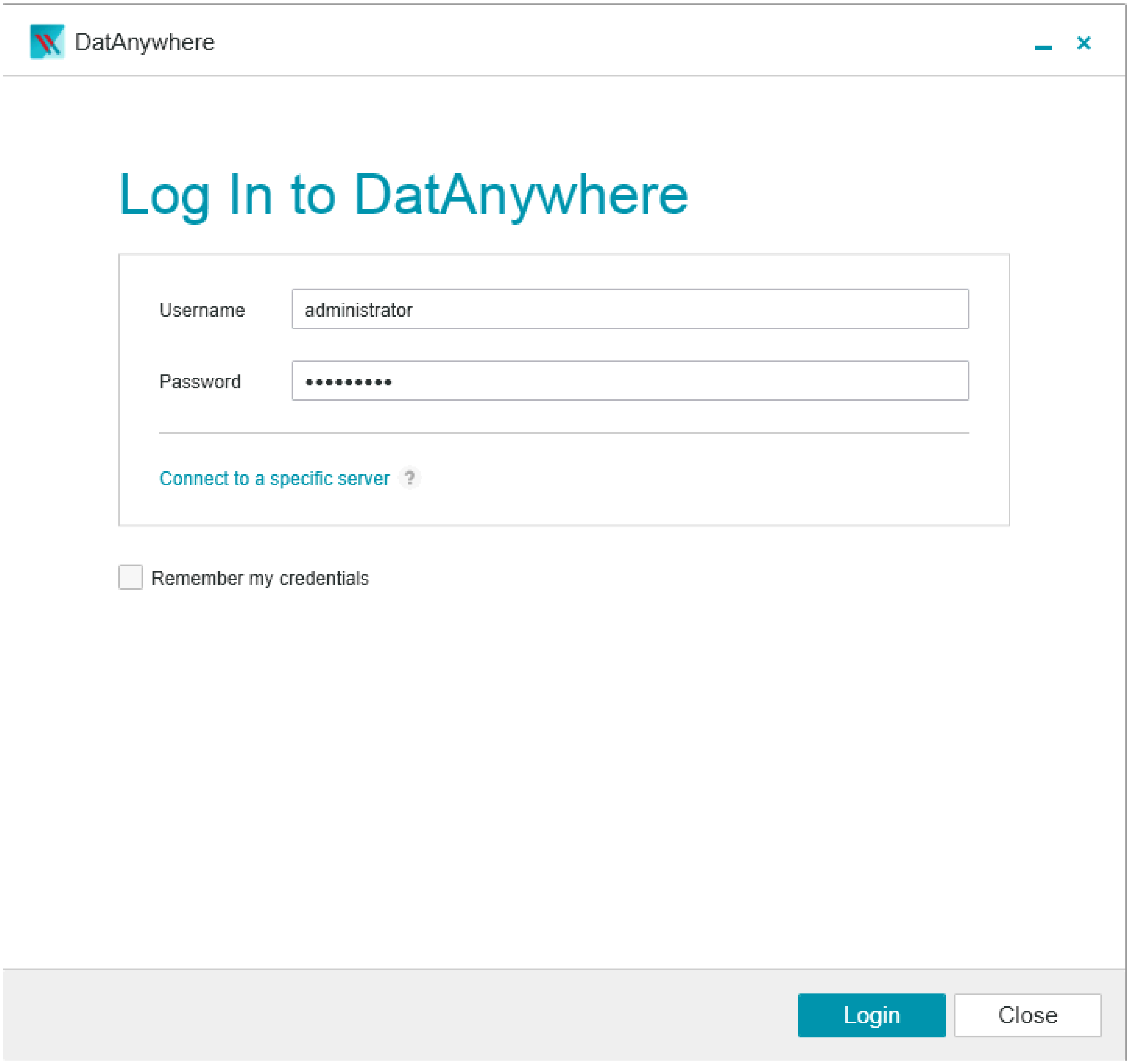
Migrating your data from Varonis DatAnywhere to FileCloud

Varonis Datanywhere will enter End of Life (EOL) in February 2020. What does this mean for existing users of Datanywhere? This means no further product development and a limited support from Varonis. It is a suitable time to look for an alternate product which offers more security and support. There may be multiple EFSS solutions similar to Varonis Datanywhere but, FileCloud is the only solution which offers all Datanywhere features and much more. For instance, FileCloud is also an on-premise solution just like Varonis Datanywhere, FileCloud can also be used on Windows Server like Datanywhere allowing use of Windows based network folders and preserve NTFS permissions. FileCloud integrates with Active Directly Credentials so, there is no need to recreate them.
The below guide will assist you towards migrating your data from DatAnywhere to FileCloud in just a few easy steps!

Download your files and folder from DatAnywhere

1) To download your files from Varonis DatAnywhere can be done from the Web-client / Web Portal or from Varonis DatAnywhere desktop client which is available for both Mac and Windows.
Once you download and install the desktop client you can login using your Varonis DatAnywhere credentials.

Note: The first time you login to Varonis DatAnywhere client you might be asked to enter your server URL. To obtain such information please contact your system Administrator,



Log In to DatAnywhere

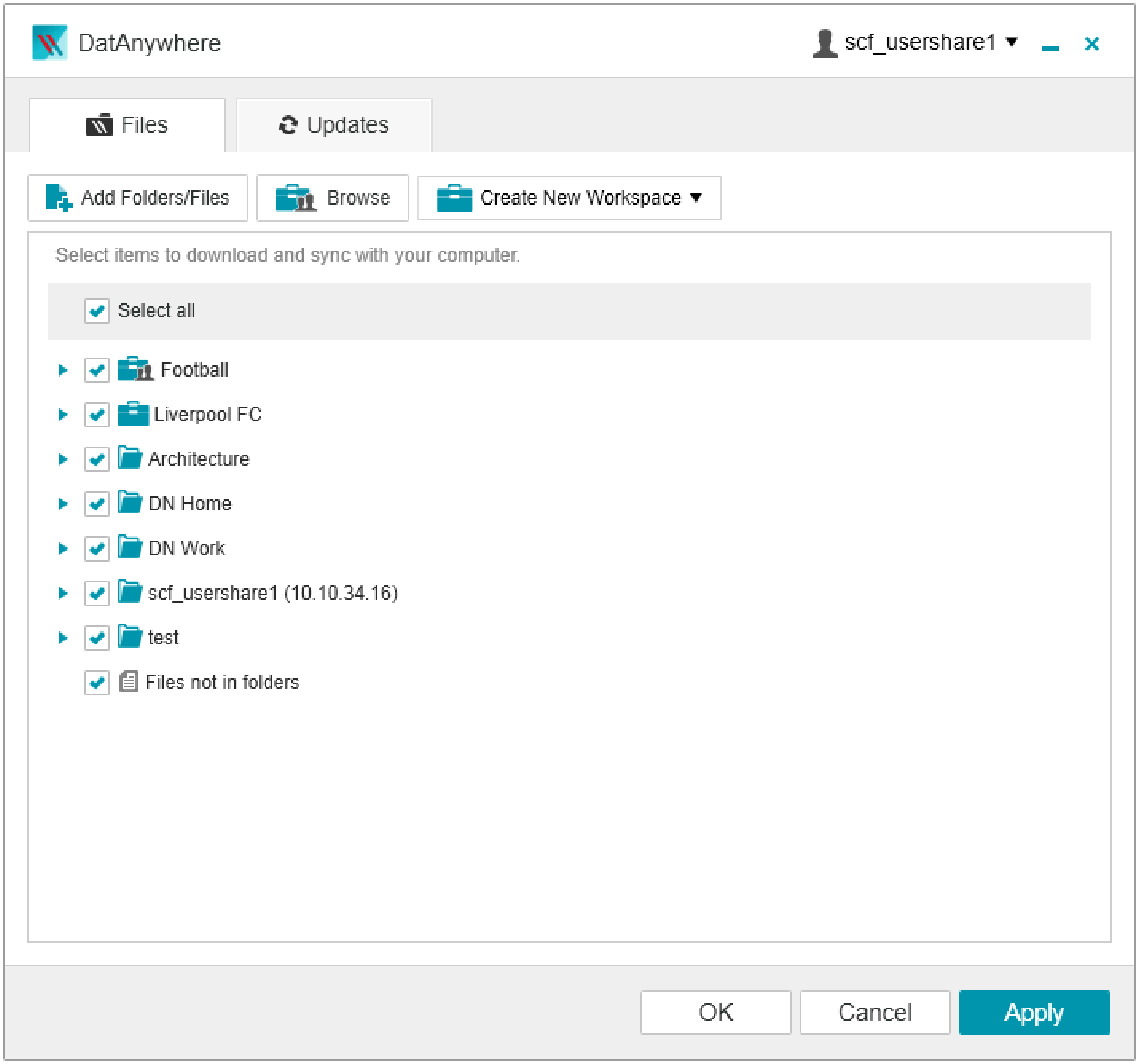
Username administrator

Password ••••••••••

□ Remember my credentials

2) Once you have logged in to Varonis DatAnywhere client from your Windows or Mac computer you can select which folders you would like to be sync'ed to your local desktop/computer.
When a specific item is synced, the selected item and all its parent folders are created in your DatAnywhere folder. You can also sync individual files in case you do not wish to download all the folders content.

Upon selecting the files and folders you wish to sync, you can proceed on clicking "Apply"



Select items to download and sync with your computer.

☑ Select all

☑ Football

☑ Liverpool FC

☑ Architecture

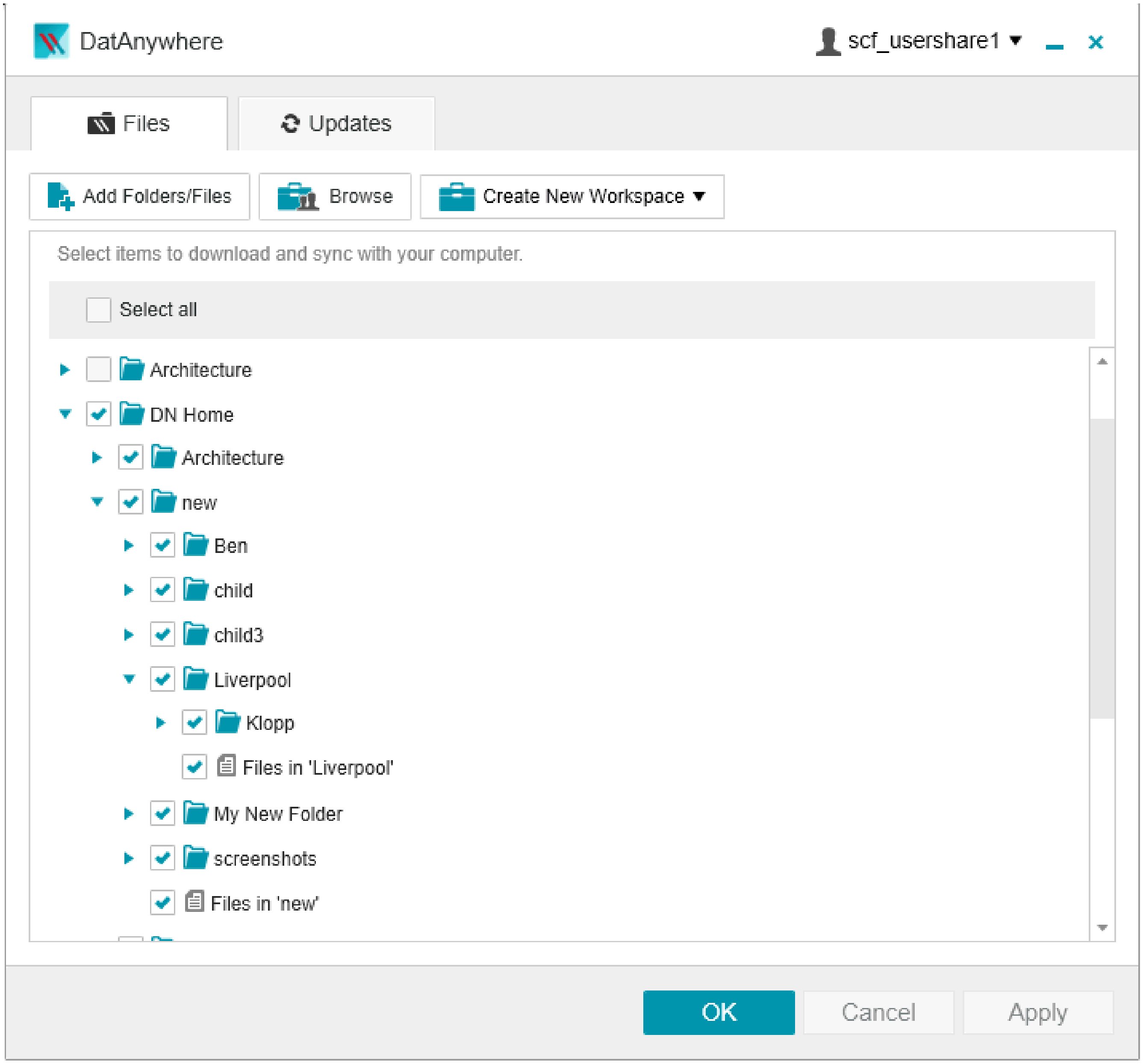
☑ DN Home

☑ DN Work

☑ scf_usershare1 (10.10.34.16)

☑ test

☑ Files not in folders



Select items to download and sync with your computer.

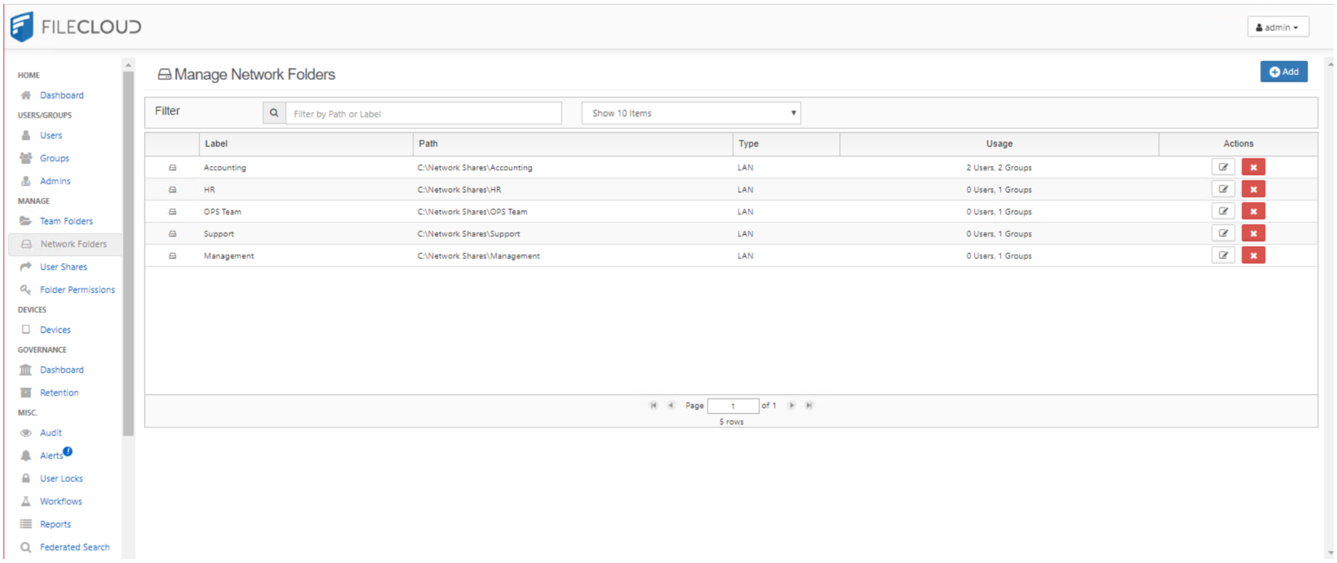
□ Select all

- □ Architecture
- ☑ DN Home
  - ☑ Architecture
  - ☑ new
    - ☑ Ben
    - ☑ child
    - ☑ child3
    - ☑ Liverpool
      - ☑ Klopp
      - ☑ Files in 'Liverpool'
    - ☑ My New Folder
    - ☑ screenshots
    - ☑ Files in 'new'

3) Once your files have completed the Sync/Download process you can access them on your Windows explorer or Mac Finder under the folder DatAnywhere.

Integrate your Network shares with FileCloud!

An easy alternative to migrate to FileCloud is to simply integrate your current Network shares to FileCloud.
To accomplish this please see Create a LAN-Based Network Folder.
Once done your users will simply access FileCloud using our desktop clients or from their Web browser to obtain immediate access to all their data!



Manage Network Folders

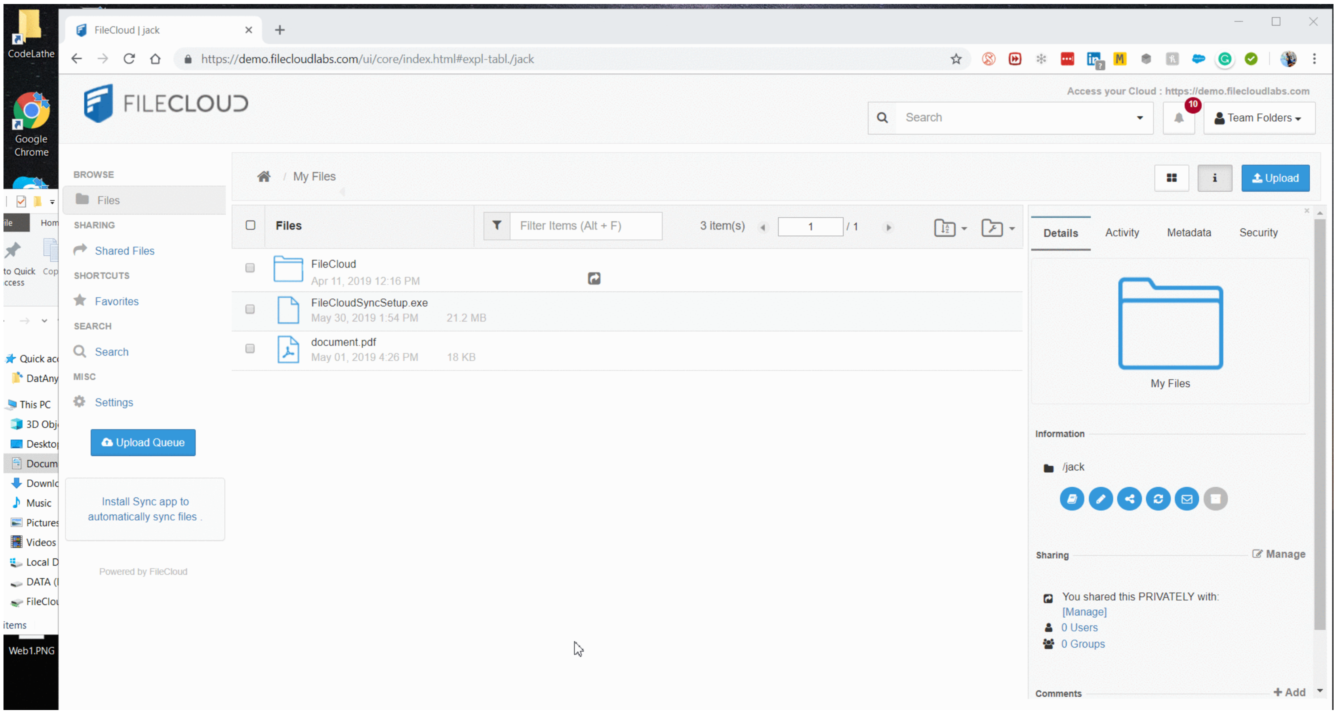
	Label	Path	Type	Usage	Actions
	Accounting	C:\Network Shares\Accounting	LAN	2 Users, 2 Groups	
	HR	C:\Network Shares\HR	LAN	0 Users, 1 Groups	
	OPS Team	C:\Network Shares\OPS Team	LAN	0 Users, 1 Groups	
	Support	C:\Network Shares\Support	LAN	0 Users, 1 Groups	
	Management	C:\Network Shares\Management	LAN	0 Users, 1 Groups	

5 rows

Migrating your files and folder to FileCloud

Users can upload files by either one of the two methods.

- You can navigate to any folder and click on the "Upload Icon" and select files to upload. You can select multiple files.
- You can also drag and drop files from your desktop into the FileCloud Web Browser window to upload the file.

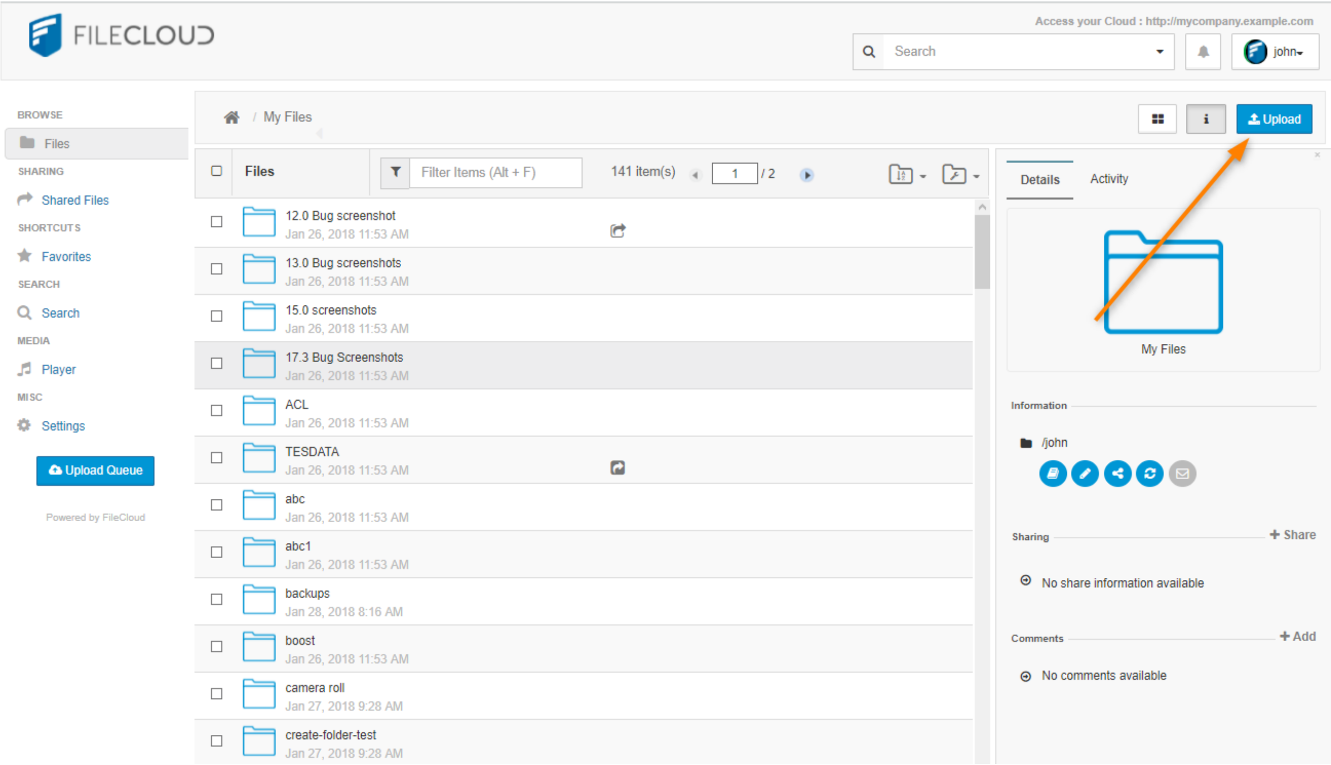


FileCloud
Apr 11, 2019 12:16 PM

FileCloudSyncSetup.exe
May 30, 2019 1:54 PM 21.2 MB

document.pdf
May 01, 2019 4:26 PM 18 KB

You shared this PRIVATELY with:
[Manage]
0 Users
0 Groups



12.0 Bug screenshot
Jan 26, 2018 11:53 AM

13.0 Bug screenshots
Jan 26, 2018 11:53 AM

15.0 screenshots
Jan 26, 2018 11:53 AM

17.3 Bug Screenshots
Jan 26, 2018 11:53 AM

ACL
Jan 26, 2018 11:53 AM

TESDATA
Jan 26, 2018 11:53 AM

abc
Jan 26, 2018 11:53 AM

abc1
Jan 26, 2018 11:53 AM

backups
Jan 28, 2018 8:16 AM

boost
Jan 26, 2018 11:53 AM

camera roll
Jan 27, 2018 9:28 AM

create-folder-test
Jan 27, 2018 9:28 AM

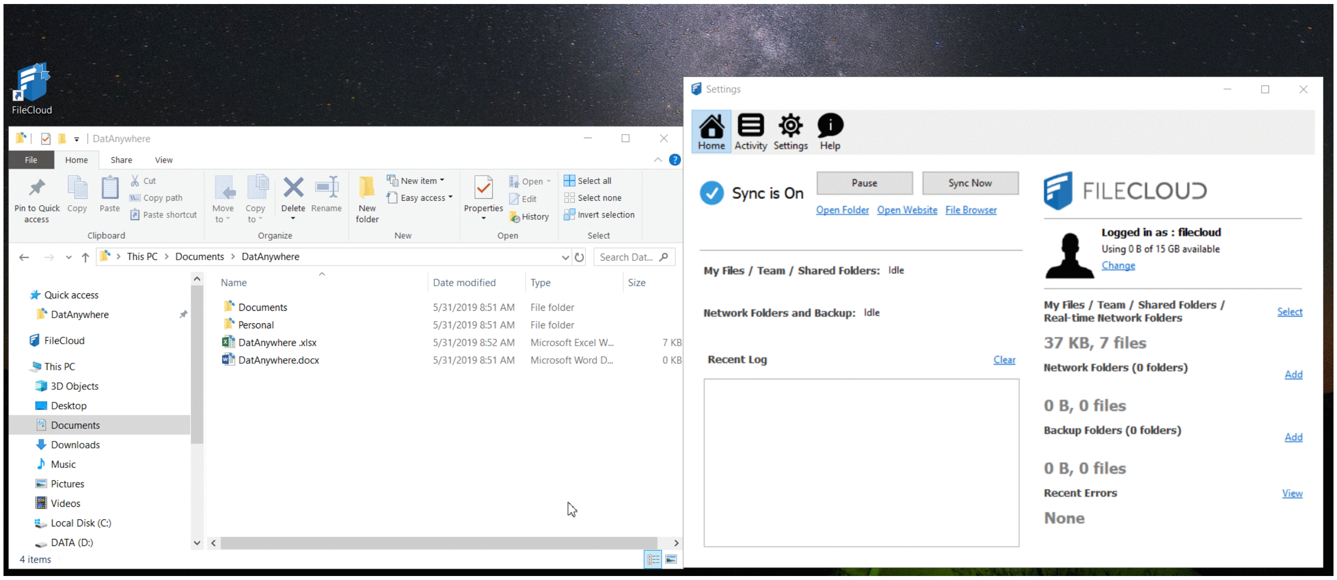
No share information available

No comments available

Migrating your DataAnywhere files and folders using FileCloud's Sync Client

FileCloud offers a variaty of desktop clients to simplfy the way you interact with your files and folders. When migrating your files and folder from Varonis DatAnywhere to FileCloud we recommend that you use our FileCloud Sync client. FileCloud Sync will securely upload your data to FileCloud in just 3 easy steps.
1) Download FileCloud Sync using the following LINK.
2) Install FileCloud Sync on your computer
3) Login to FileCloud Sync and Open FileCloud's Sync folder.
4) Select and Drag your files/ folders from Varonis DatAnywhere folder into FileCloud's Folder as seen below.

Once done FileCloud Sync will upload your data to FileCloud!



Name	Date modified	Type	Size
Documents	5/31/2019 8:51 AM	File folder	
Personal	5/31/2019 8:51 AM	File folder	
DatAnywhere .xlsx	5/31/2019 8:52 AM	Microsoft Excel W...	7 KB
DatAnywhere.docx	5/31/2019 8:51 AM	Microsoft Word D...	0 KB

Sync is On

My Files / Team / Shared Folders: Idle

Network Folders and Backup: Idle

Recent Log

Logged in as : filecloud
Using 0 B of 15 GB available

My Files / Team / Shared Folders / Real-time Network Folders
37 KB, 7 files

Network Folders (0 folders)
0 B, 0 files

Backup Folders (0 folders)
0 B, 0 files

Recent Errors
None

FileCloud Support

If you need assistance to migrate your data please feel free to contact our support team at support@filecloud.com. Please do keep in mind that FileCloud's support team will not be able to assist you in downloading your data from Varonis DatAnywhere.
If you need assistance to download your data from Varonis DatAnywhere we kindly ask that you contact your system Administrator for further assistance.

FileCloud Best Practices

In this section:

FileCloud Blogs

- FileCloud Best Practices: How to Use Private Shares and External User Accounts

Deployment

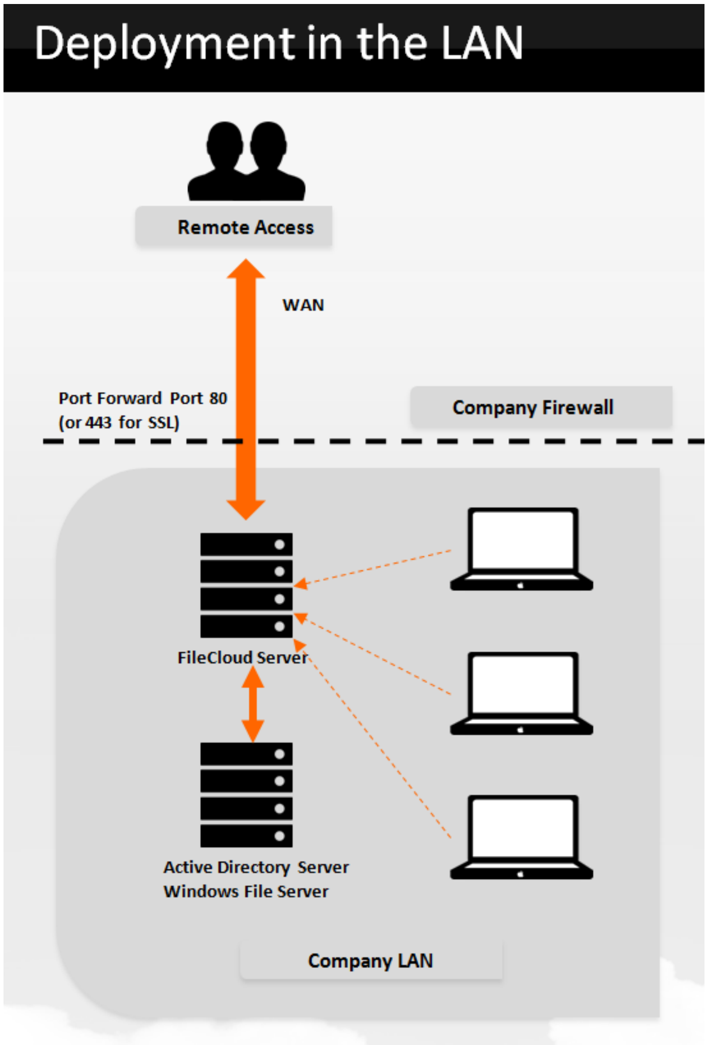
FileCloud Deployment Scenarios

FileCloud can be deployed in several configurations, but we discuss the two most common and recommended ways.

> As a best practice, ensure that your outgoing firewall rules are enforced.

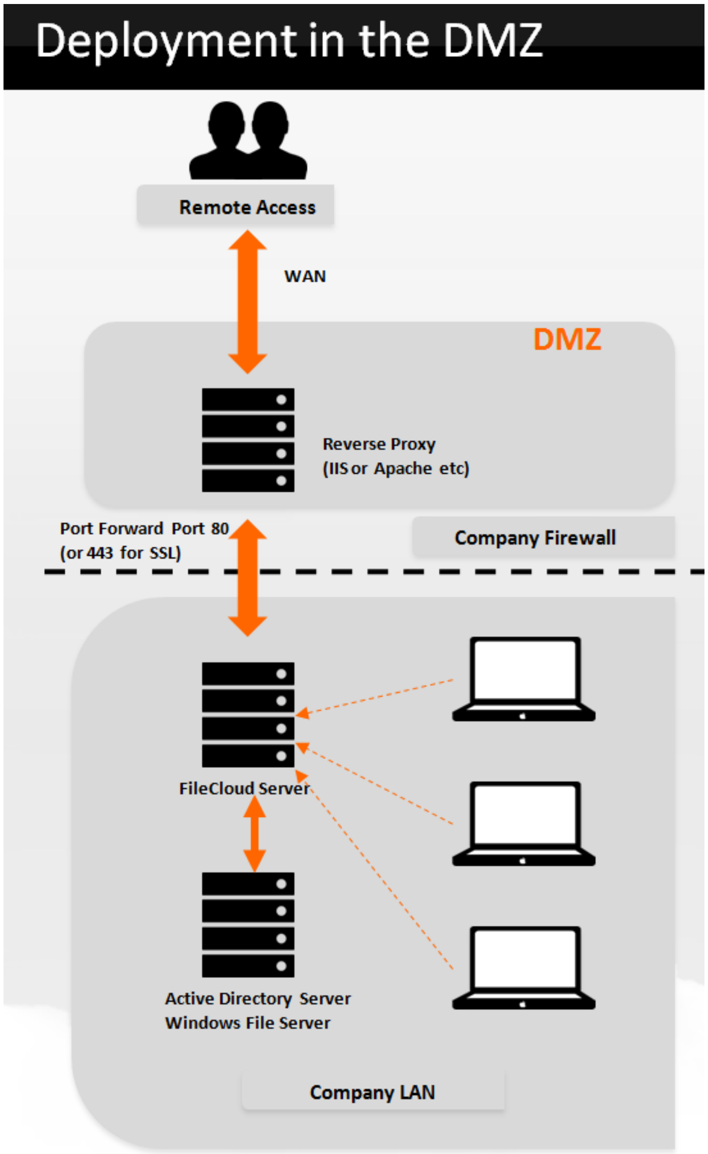
Deployment in the LAN

In this scenario, FileCloud server is deployed directly in the LAN along side the file servers and Windows Active Directory servers. The port 80 or port 443 is then opened and forwarded to the server running FileCloud.



Deployment in the DMZ

In some networks, it might not be possible or desired to open the firewall port directly to a machine on the LAN, in this case, a server running a HTTP reverse proxy (Microsoft IIS, NGINX or Apache and others) in the DMZ outside the LAN can forward HTTP requests to the actual FileCloud server in the LAN.



Performance

Introduction

- Consider using PHP 5.6 and above with OpCache enabled for improved performance
- Enabling Local Storage File Encryption will affect performance. Consider not using encryption unless absolutely required.
- Use SSD disks for storage for running the Server. It will have significant performance boost.
- Having a large number of CPU cores will help with scaling when there are a lot of incoming requests

Optimizing Mongo Database Performance

- For large databases, MongoDB might require a lot of RAM, so ensure your server running MongoDB has enough RAM.
- Consider using SSD storage to store MongoDB databases
- Consider moving MongoDB to a separate server outside of the webserver node. This might improve performance.

Improving Upload Speeds

There are many factors that can affect upload speeds.

- Your internet connection bandwidth speed
- Where the storage is location (local to the filecloud server or on the network). Local is faster.
- Type of storage (SSD vs Hard Disk) . SSD is fastest.

Improving File Synchronization Speeds

- Use FileCloud 11.0 or later for multi-threaded file uploads and downloads
- Use realtime sync for optimum sync performance
- Offline sync of large network folders will be slow and might severely impact server performance when there are lots of users using the system.

Restricting Access To Admin UI Based On IP Addresses

Introduction

Administrators would like to restrict access to admin web UI only for intranet IP addresses or even only when accessed from their PC. Follow these steps, to restrict admin UI access for certain IP addresses.

Steps

1. Stop Apache Server.
2. Edit the following file, based on the OS on which FileCloud server is installed (adjust these paths for your environment).

Operating System	**Typical Configuration File Location**
Windows	C:\xampp\apache\conf\extra\httpd-filecloud.conf
Ubuntu	/etc/apache2/sites-enabled/000-default.conf
RHEL	/etc/httpd/conf/httpd.conf

3. Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration.

```
<Location /ui/admin2>
          Order deny,allow
          deny from all
          allow from 192.168.
          allow from 33.201.24.69
</Location>
```

4. Restart apache, after making this change. Now admin UI will be accessible only from subnet 192.168.x.x and IP 33.201.24.69.

> Old installations which use **http(s)://<your filecloud address>/ui/admin** to restrict access should change this to **http(s)://<your filecloud address>/ui/admin2** and restart Apache for changes to take effect

Restricting Access To User UI Based On IP Addresses

Introduction

Administrators might like to restrict access to user web UI only for intranet IP addresses. If this is the case, please follow these steps to restrict user UI access to certain IP addresses.

Steps

1. Stop Apache Server.
2. Edit the following file, based on the OS on which FileCloud server is installed (adjust these paths for your environment).

Operating System	Typical Configuration File Location
Windows	C:\xampp\apache\conf\httpd.conf
Linux	/etc/apache2/sites-enabled/000-default.conf

3. Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration.

```
<Location /ui/core>
          Order deny,allow
          deny from all
          allow from 192.168.
```

```
                allow from 33.201.24.69

        </Location>
```

4. Restart apache, after making this change. Now admin UI will be accessible only from subnet 192.168.x.x and IP 33.201.24.69.

Add the following lines to the configuration. In Windows, lines can be added to the end of the file. On Linux, lines needs to be added inside the VirtualHost configuration for blocking client apps also

```
        <Location />

                Order deny,allow

                deny from all

                allow from 192.168.

                allow from 33.201.24.69

        </Location>

Restart apache, after making this change. Now filecloud will be accessible
only from subnet 192.168.x.x and IP 33.201.24.69
```

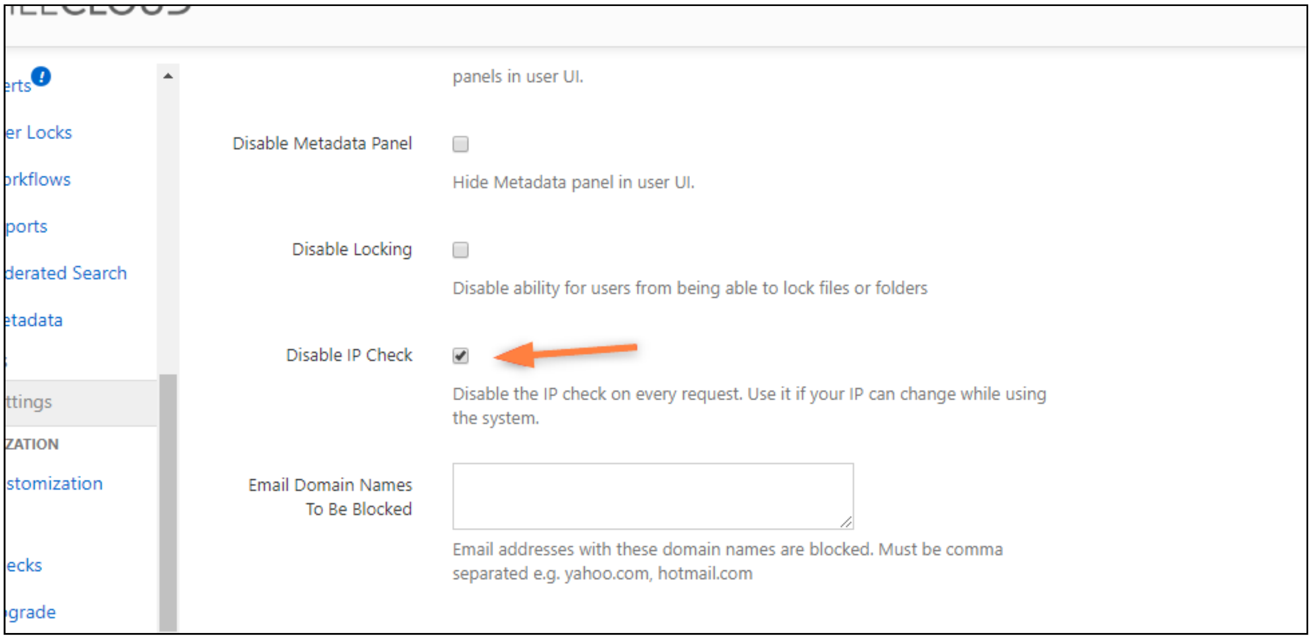
Manage IP Checks

In FileCloud Server, the IP address used when an administrator or user requests data is checked against the IP stored on the session.

- This means that the session is invalidated if the user IP address changes (the user is automatically logged out).
- For some environments, the IP address change is common and expected.

Now there is a checkbox labeled *Disable IP Check* that allows an administrator to control this behavior.

- Select the checkbox to disable the IP check on every request. This allows you to avoid IP comparison on cookies.
- The use of this option is only recommended if your IP address can change while using the system.



panels in user UI.

Disable Metadata Panel □
Hide Metadata panel in user UI.

Disable Locking □
Disable ability for users from being able to lock files or folders

Disable IP Check ☑
Disable the IP check on every request. Use it if your IP can change while using the system.

Email Domain Names To Be Blocked
Email addresses with these domain names are blocked. Must be comma separated e.g. yahoo.com, hotmail.com

To configure this option:

1. Log into *Admin Portal*.
2. From the left navigation panel, select ***SETTINGS*** **and then** ***Misc*** **and then** **General.**
3. **On the** ***Settings*** **screen, select the** ***Misc.*** **tab, and then the** ***General*** **sub-**tab.
4. Next to *Disable IP Check*, select or clear the checkbox.

Changing default config and log directory for FileCloud

Introduction

Out of the box, FileCloud has the configuration and log directories under the WEBROOT. This document discusses how to move these directories to different location.

Changing Config Directory

By default configuration files for FileCloud installation will be under WEBROOT/config. To change this directory, move the WEBROOT/config directory to the new location and then update the WEBROOT/localconfig.php file to notify this change to FileCloud.

Change from: define("TONIDOCLOUD_CONFIG_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."config"); // < VALID config directory path, needs to be read/write by www-data
To:
For Linux: define("TONIDOCLOUD_CONFIG_PATH", "/home/tonidocloud/config"); // < VALID config directory path, needs to be read/write by www-data
For Windows: define("TONIDOCLOUD_CONFIG_PATH", "c:\\tonidocloud\\config"); // < VALID config directory path, needs to be read/write by webserver

Note: As the comment says, the new path should have read/write permissions for the user account that is used to run apache. For instance, www-data in Linux.

Changing Log Directory

By default FileCloud log files will be placed under WEBROOT/scratch. To change this directory, update the WEBROOT/localconfig.php file to notify the new log path to FileCloud.

Change from: define("TONIDOCLOUD_SCRATCH_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."scratch"); // < VALID scratch directory path, needs to be writable by www-data
To:
For Linux: define("TONIDOCLOUD_SCRATCH_PATH", "/home/somenewpath/scratch"); // < VALID directory path, with read-write permission for www-data user
For windows: define("TONIDOCLOUD_SCRATCH_PATH", "c:\\somenewpath\\scratch"); // < VALID config directory path, with read-write permission for the webserver.

Note: As the comment says, the new path should have write permissions for the user account that is used to run apache. For instance, www-data in Linux.

Disable CONNECT Method in HTTP

Introduction

Some security vulnerability scanners might report that your Apache server is vulnerable because CONNECT method is being allowed. For example, a scanner might report:

- CONNECT Method Allowed in HTTP Server Or HTTP Proxy Server Vulnerability
- The HTTP server or the HTTP proxy server accepts the "CONNECT" method.

Following section explains how to disable the CONNECT method on your installation.

Disabling CONNECT Method

There is no inherent vulnerability with the CONNECT method but you should not leave it enabled since it would allow Apache httpd to be used a proxy. This should only be enabled if you intent for Apache httpd to be used as a proxy.

In case of errors like CONNECT Method Allowed in HTTP Server Or HTTP Proxy Server Vulnerability; you will need to disable the connect method in HTTP.

To disable connect method in HTTP, please make the changes in .htaccess file.

Generally, the file location for linux is /var/www/html/.htaccess and for Windows is C:\xampp\htdocs\.htaccess

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^CONNECT
RewriteRule .* - [R=405,L]
```

The above code will redirect any connect method to 405 method not allowed, which will automatically rejects any connect request with no acknowledgement.

Enforcing TLS 1.2 and TLS 1.3 and Strong Ciphers

Introduction

FileCloud can be configured to use stronger SSL Protocol (TLSv1.2 and 1.3 only) instead of the default protocols. This article shows how to configure FileCloud server and clients to make use of the TLSv1.2 and TLSv1.3 protocols.

Server Configuration

1. In order to enable TLS 1.2 or TLS 1.3 , please edit the httpd configuration file.

OS	Remarks
Windows	Configuration file is located at XAMPPROOT\apache\conf\extra\httpd-ssl.conf For example, if you have installed xampp in c:\, then it will be C:\xampp\apache\conf\extra\http-ssl-conf
Ubuntu	/etc/apache2/sites-enabled/000-default.conf If you use a non-default site, please use appropriate configuration file.

2. Locate the SSLCipherSuite key and change it to
   SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
3. Locate the SSLProtocol key and change it to
   SSLProtocol -all +TLSv1.3 +TLSv1.2
4. This is the highest level of security possible.

Security: Changing a Default Port or Web Server Setting

The ports and Web servers used by FileCloud are normally set during installation. After installation is completed, if you need to, you can change the default listening ports and Web servers.

By default, FileCloud uses these 3 ports:

- **80 (web server)**
- **443 (web server)**
- **27017 (database)**

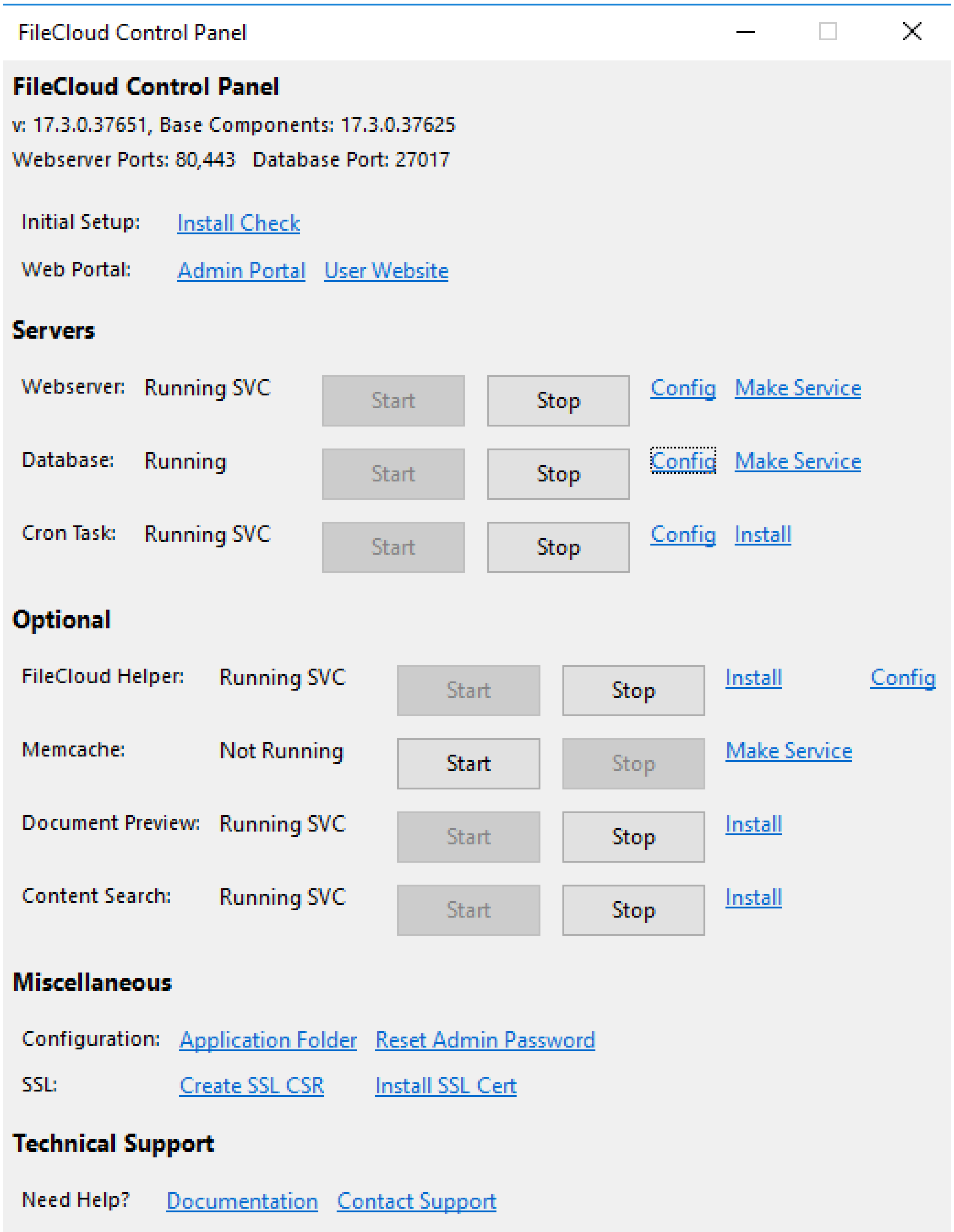
If other programs are using these ports, the FileCloud server will not start up properly.

You might want to change the port numbers or Web servers in some of the following scenarios:

- You need to disable anything that uses port 80 and 443
- You want Apache to run on non standard ports or servers or use firewall rules
- You need to use IIS on standard ports

💡 It is also recommended to disable HTTP port on the FileCloud server.

To change the ports, you will need to open the FileCloud Control Panel.



FileCloud Control Panel

FileCloud Control Panel

v: 17.3.0.37651, Base Components: 17.3.0.37625

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

Webserver: Running SVC Start Stop Config Make Service

Database: Running Start Stop Config Make Service

Cron Task: Running SVC Start Stop Config Install

Optional

FileCloud Helper: Running SVC Start Stop Install Config

Memcache: Not Running Start Stop Make Service

Document Preview: Running SVC Start Stop Install

Content Search: Running SVC Start Stop Install

Miscellaneous

Configuration: Application Folder Reset Admin Password

SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support

To change a port or Web server setting:

1. On the server, from the *Windows Start* menu, select the *FileCloud Control Panel*, or double-click the *xampp/ cloudcp.exe* file.
2. In the Servers section, for Webserver, click Stop.
3. Change the Port configuration according to HTTPS Best Practices for FileCloud.
4. To start the Webserver, click Start next to Webserver.
5. In the Servers section, for Database, click Stop, then Config.
6. Make your changes, save them, and next to Database, click Start.

7. If you have changed the default Web server, open localconfig.php at:
   Windows Location: XAMPP DIRECTORY/htdocs/config/localconfig.php
   Linux Location: /var/www/config/localconfig.php
   and add the following, replacing n.n.n.n with the correct IP address.

```
define("TONIDOCLOUD_APACHE_BIND_IP", "n.n.n.n");
```

.

Security: HTTPS Best Practices for FileCloud

FileCloud recommends that you run all servers in a production environment only on:

- HTTPS (SSL)
- Port 443

This ensures that all communications between clients and FileCloud are completely encrypted.

💡 To access these secured sites, users will have to type in:

https://<SITENAME>

Best Practice	**Reason**	**Steps**
Disable the existing HTTP port.	So that FileCloud can be accessed only securely via HTTPS. Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security) Therefore removing the HTTP port completely is the best option. ➡ If you must use a redirect, Configure HTTP SSL Redirects.	To Disable HTTP (port 80) for Windows: 1. Open the webserver config file for editing: `c:\xampp\apache\conf\httpd.conf` and 2. Comment out the line with Listen 80. 3. Save and close the file. 4. Restart the server. To Disable HTTP (port 80) for Linux: 1. Open the webserver config file for editing: `/etc/apache2/ports.conf` 2. Comment out the line with Listen 80. 3. Save and close the file. 4. Restart the server.

Best Practice	Reason	Steps
Verify your certificates are valid.	If you have an invalid SSL configuration, your users would receive various errors on the browser, and iPhone/iPad apps **cannot preview Office documents**.	You can check the validity of the SSL certificate by testing your install against a SSL certificate checker like https://www.sslshopper.com/ssl-checker.html Provide your FileCloud URL and it will report any potential problems your SSL installation might have. These tools should report no errors for your FileCloud to function properly in SSL mode.

Best Practice	Reason	Steps

Change the default listening port (80).	If you have are conflicts with other ports.	For Windows:
		1. Open the following file for editing: `c:\xampp\apache\conf\httpd.conf`
		2. Locate the following two lines: `Listen 80`
		`ServerName localhost:80`
		3. Change these lines to the following: `Listen your_new_port`
		`ServerName localhost:your_new_port`
		4. Save and close the file.
		For Linux:
		1. Open the following file for editing: `/etc/apache2/ports.conf`
		2. Locate the following line: `Listen 80`
		3. Change it to `Listen Your_new_port`
		4. Open the following file for editing: `/etc/apache2/sites-enabled/000-default.conf`
		5. Locate the following line `<VirtualHost *:80>`
		6. Change it to `<virtualHost _default:your_new_port>`
		7. Save and close the file.

Best Practice	Reason	Steps
Change the default HTTPS port (443).	If you have are conflicts with other ports.	For Windows: 1. Open the following file for editing: `c:\xampp\apache\conf\extra\httpd-ssl.conf` 2. Locate the following line `Listen 443` 3. Change it to `Listen your_new_port` 4. Locate the following line `<VirtualHost _default_:443` 5. Change it to `<VirtualHost _default_:your_new_port>` 6. Save and close the file. For Linux: 1. Open the following file for editing: `/etc/apache2/ports.conf` 2. Locate the following lines `<IfModule mod_ssl.c>Listen 443</IfModule>` 3. Change it to `<IfModule mod_ssl.c>Listen Your_New_Port</IfModule>` 4. Open the following file for editing: `/etc/apache2/sites-available/default-ssl` 5. Locate the following line: `<VirtualHost _default_:443>` 6. Change it to `<VirtualHost _default_:your_new_port>` 7. Save and close the file.

Best Practice	Reason	Steps

Disable server information in headers.	To prevent the Web application from disclosing the server name and server version in the response header.	1. Open the Apache configuration file:
		Ubuntu location: /etc/apache2/apache2.conf
		CentOS location: /etc/httpd/conf/httpd.conf
		Windows location: C:\xampp\apache\conf\httpd.conf
		2. Add the following:
		`ServerSignature Off`
		`ServerTokens Prod`
		3. Restart the Apache server.

HTTP To HTTPS Redirects

It is recommended that you configure FileCloud Server so that it can be accessed securely only via HTTPS.

Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security).

Therefore removing the HTTP port completely is the best option.

If you must use a redirect, add the following lines:

```
<VirtualHost *:80>
 RewriteEngine On
 RewriteCond %{HTTPS} off
 RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
 </VirtualHost>
```

- In Windows, the above lines should we added to file c:\xampp\apache\conf\extra\httpd-vhosts.conf. Restart the apache server.
  Also make sure the following line is uncommented in the file C:\xampp\apache\conf\httpd.conf.

  ```
  # Virtual hosts
  Include conf/extra/httpd-vhosts.conf
  ```

- In Linux, the above lines should be added to the /etc/apache.d/sites-enabled/000-default.conf file. If you already have a VirtualHost directive, add only the lines starting with "Rewrite". Restart the apache server.

Also see: Configure HTTP SSL Redirects

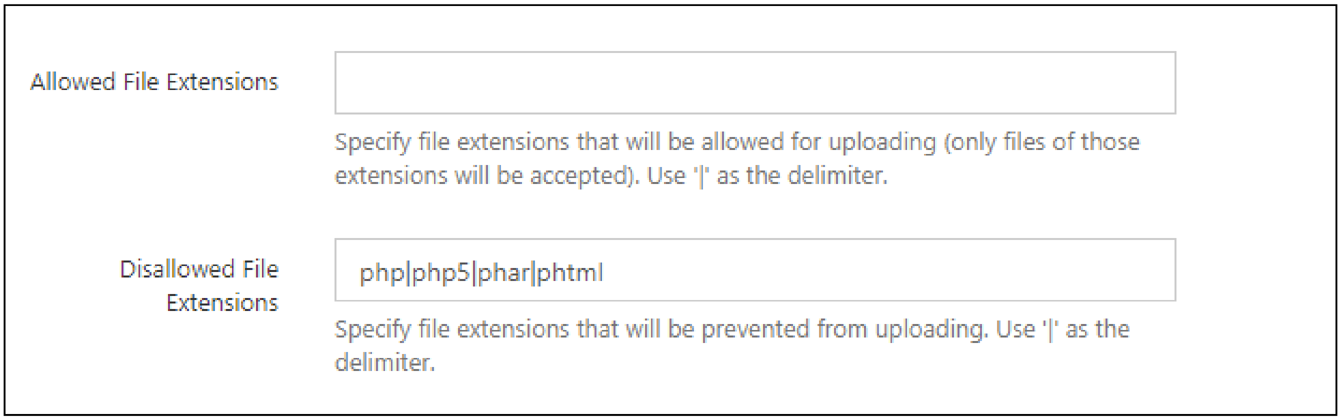
Security: Managing File Extensions

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

Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use '|' as the delimiter.

Disallowed File Extensions: 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.

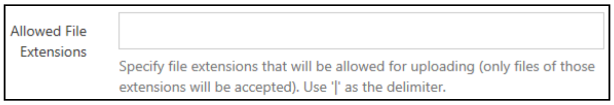
What Do You Want to Do?

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.

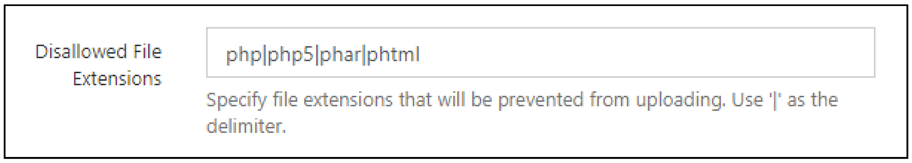
- An empty space is defined as a delimiter character followed by no value.

Examples	Description	Impact on Uploading Files
`png | jpg |`	Allow files to be uploaded with an extension of: • png • jpg • *empty*	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group • Any file without an extension (for example, a file named *config*)
`png | jpg`	Allow files to be uploaded with an extension of: • png • jpg	Only the following files can be uploaded by users: • Portable Network Graphics • Joint Photographic Experts Group

FileCloud Version	Method	Instructions	Notes
19.1	Admin Portal	To manage extension 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 *Allowed File Extensions* box. 5. In the *Allowed File Extensions* box, specify the allowed extensions, using the "|" character to separate each extension.	⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored. ⚠ If you leave an empty space in your list, then you will allow files that don't have an extension to be uploaded.  Allowed File Extensions Specify file extensions that will be allowed for uploading (only files of those extensions will be accepted). Use '|' as the delimiter. This list of extensions must use the following character as the delimiter: • '|' • For example, to restrict the mp4 and mp3 extensions: mp4 | mp3

Disallow File Extensions

<table>
<tr><th>FileCloud Version</th><th>Method</th><th>Instructions</th></tr>
<tr><td>Earlier than 17.3</td><td>Direct Coding</td><td>To add file extension restrictions:
1. Open the following file
WWWROOT\config\cloudconfig.php
2. Add the following code
define("TONIDOCLOUD_DISALLOWED_RESTRICTIONS", "php|php5|phar|phtml");
To remove all file extension restrictions:
1. Open the following file
WWWROOT\config\cloudconfig.php
2. Edit the code to match this:
define("TONIDOCLOUD_DISALLOWED_RESTRICTIONS", "");
Note:
This list of extensions must use the following character as the delimiter:
• '|'
• For example, to restrict php extensions: php|php5|phar|phtml</td></tr>
</table>

FileCloud Version	Method	Instructions
17.3 and later	Admin Portal Direct Coding	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, add the additional restricted extensions. **Notes:** ⚠ If you add extensions to the **Allowed File Extensions** list, then any extensions in the **Disallowed File Extension** list will be ignored.  Disallowed File Extensions: php|php5|phar|phtml Specify file extensions that will be prevented from uploading. Use '|' as the delimiter. This list of extensions must use the following character as the delimiter: - '|' - For example, to add restrictions for mp3 and mp4 to the list of disallowed extensions: `php|php5|phar|phtml|mp3|mp4`