FileCloud Server 19.1 Release Notes

There is a NEW patch to correct issues found in FileCloud Server version 19.1

RELEASE 19.1.2	**Upgrading from version 19.1 or 19.1.1:**
For more information on what is included: ➡ Release Notes for 19.1.2	• Upgrades can be completed using the Admin portal Upgrading from any other version to 19.1.2: • A full system upgrade is required for all existing installations

19.1

Overview	Release Summary	Upgrade to 19.1
Release Date: April 5, 2019 Release Type: Major ➡ New Features ➡ Enhancements ➡ Issues Resolved ➡ Known Issues	CodeLathe customers get a huge boost in supporting financial regulations with FileCloud's new Governance features. The management dashboard and retention policy features have been designed to help regulators manage all digital content for legal, regulatory, compliance, and internal requirements. FileCloud allows regulators to manage content effectively - that means seeing what is occurring in a large installation with thousands of users on a day-to-day basis. CodeLathe knows that governance is also evolving, and as requirements change, our software is flexible enough to handle the new requirements. In addition to new features, FileCloud users will also notice how much faster FileCloud responds to your requests. This is due to improvements in background processing, allowing FileCloud to work more quickly when you are sharing files and storing data. Many other improvements have been completed to provide users with an even richer experience, especially to the Sync and Drive clients that synchronize data with FileCloud.	New installation: ➡ Installing FileCloud Server Upgrading from any version to 19.1: • **A full system upgrade is required** for all existing installations due to the following core change: a. More powerful background processing has been added to improve message queuing and the speed of FileCloud responses. ➡ Upgrading to 19.1

Module	Feature Name	Description
Governance	Governance Dashboard **HOME** 🏠 Dashboard **USERS/GROUPS** 👤 Users 👥 Groups 👥 Admins **MANAGE** 📁 Team Folders 💾 Network Folders ↪ User Shares 🔍 Folder Permissions **DEVICES** ▢ Devices **GOVERNANCE** 🔔 Dashboard 🗄 Retention	The Governance Dashboard allows an administrator to see all system alerts generated by retention policy violations or conflicts. For example: • Alerts informing about close policy expiry dates • Alerts informing about policy violation in certain conditions Administrators can manage alerts in the following ways:

Management Strategy	Dashboard Option	Description
Approve an alert	OK	The administrator is not going to take any action in response to the alert. This will not move the alert to the archived alerts list that can be viewed by the administrator at any point of time.
Acknowledge it is an issue	ACK	The administrator knows about this problem and wants to work on this issue later. This helps remove the alert from the incoming inbox for alerts and makes it easy for him to work to work on new issues.
Take action	Open	The administrator can resolve the issue, for example by deleting the file or adding a new policy

Governance	Retention Policies	Retention policies allow administrators to automate some of the processing related to protecting files and their folder groupings. This policy-based automation is designed to help secure digital content for compliance, but it can also enhance the management of digital content for other internal reasons.

Retention policies are created and attached to files and folders. These special policies allow you to define the conditions that enforce a set of restrictions on how each file or folder can be manipulated. For example, you can create a Retention Policy that disables a user's ability to delete or edit any of the files and folders named in the policy.

To resolve the issue of conflicting policies, FileCloud ranks retention policies by what best protects and retains the digital content.

Policy Type	Rank	Description
Admin Hold	1 • Outranks all other policies • Is outranked by no other policy	• Prevents any update or delete of digital content for an indefinite period of time • Admin Hold policies applied to folders can be removed • Admin policies applied to files can be removed
Legal Hold	2 • Outranks policies 3-5 • Is outranked by Admin Hold	• Freezes digital content to aid discovery or legal challenges • During a legal hold, file modifications are not allowed • Holds cannot be reversed once applied
Retention	3 • Outranks policies 4-5 • Is outranked by Admin and Legal Holds	• Identifies digital content to be kept around for an unlimited amount of time before being deleted or released • Retention policies cannot be reversed once applied
Archival	4 • Outranks policies 5 • Is outranked by Admin Hold • Is outranked by Legal Hold • Is outranked by Retention	• Moves and stores old organizational content, for example, to a more cost effective systems for long term • No Deletion is allowed until a specific time period is reached • After the specified time period is reached, content gets moved to a specific folder or location
Trash Retention	5 • Outranks no other policies • Is outranked by all other policies	• Controls if files can permanently be deleted completely off the FileCloud Server system • Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions

Administrators can read more about Retention Policies

Mobile Apps	New sharing option	For a better user experience, when an Android or iOS user opens a share link in a mobile browser, they will have the option to view this data inside the mobile app.
Backup Server	Backup Server now bundled in main installer	FileCloud backup server is an add-on to FileCloud Server. • Backup Server does not require its own license • An administrator has to first install FileCloud Server and then add backup server capability to it. • FileCloud backup server can backup only FileCloud server v11.0 or above. Backup Server is now bundled as part of the main installer, so there is no need for you to download it to install it. Administrators can read about FileCloud Backup Server Installation
Drive Clients	MSI Installer for Group Deployments	In previous versions, in an enterprise / SPLA / reseller environment, an administrator would have to individually install the Drive client on all computers or create their own script. Now, FileCloud provides a bundled MSI to install to multiple clients without encountering any prompts. This provides a scalable solution for an administrator to install the Drive client.

File Managem ent	Users can now view and manage email files	FileCloud has added a viewer for email files (.eml). Users can now open a browser, log on to the FileCloud User Portal, and upload an email file with an extension of .eml. When a user opens an email file in the User Portal, they can: • View the From, To, Subject and Body • View any file attachments • Forward that email to other email addresses ➡ Users can read more about how to Work with Email Files
File Managem ent	File Identity Tracking	A new built-in metadata set called Document Life Cycle contains a CheckSum attribute that provides a unique fingerprint for every file. • CheckSum: File SHA256 Fingerprint The SHA256 Fingerprint: • Is a unique text string generated by the SHA-1 hash algorithm. • It is a standard for the implementation of a secure hash algorithm. • It is a one-way hashing function that can be used to act as a *signature* of a sequence of bytes. While multiple files can have the same size and the same name, there is only one unique HASH for every file. • A new SHA256 fingerprint is generated every time a file is changed (uploaded, edited, renamed) • The CheckSum is shown for every file in the User Portal on the Metadata tab • You can use the hash to compare the integrity of the file downloads. This is a standard way to verify a file. This feature was added to help you know for sure, and be able to prove when a user has shared a specific restricted file. ➡ Administrators can read more about Built-In Metadata Sets
File Managem ent	New option for turning off versioning	Administrators can now configure FileCloud to prevent user from re-uploading a file: *Number of old versions to keep for each file* can be set to -1 • Turns off versioning and prevents overwrites

Scenario	FAIL or SUCCEED	Storage Type
• The *Number of old versions to keep for each file* is set to -1 • The user tries to upload another version	FAIL	• Managed • LAN-Based Network Folders • Managed S3
• The *Number of old versions to keep for each file* is set to any number greater than 0 • The maximum number of versions of the file stored has NOT been exceeded • The user tries to upload another version	SUCCEED	• Managed • LAN-Based Network Folders • Managed S3

Metadata	New built-in set for Image metadata	A new BUILT-IN metadata set is now automatically created for image files. The new Image Metadata set is based on the Exchangeable Image File Format (Exif). • Exif is a standard that records the important data on image files such as shutter speed, aperture, ISO Speed, lens type etc. • Exif requires that the image file be at least 12 bytes in order for the metadata to be applied. The Exif data provides valuable information to organize photographs, perform searches and provide vital information to photos stored in FileCloud. This set is provided to you so that you can allow users to store and search image attributes using metadata. Unlike the DEFAULT metadata set: • Built-In sets cannot be renamed • Built-In sets cannot be disabled • Built-In sets are not limited to paths • Built-In attributes cannot be edited or deleted • Built-In sets only allow Read access ➡ Administrators can read more about Built-In Metadata Sets

Metadata	New built-in set for Document Lifecycle	A new BUILT-IN metadata set is now automatically created for all files. It provides the following values (tags) extracted from the file. • Creation Date • Last Access • Last Modification • Check Sum: File SHA256 Fingerprint One of these attributes is a SHA256 Fingerprint. • This is a unique text string generated by the SHA-1 hash algorithm. • It is a standard for the implementation of a secure hash algorithm. • It is a one-way cryptographic function that can be used to act as a 'signature' of a sequence of bytes. • It is very unlikely that 2 different byte sequences would produce the same value (though not impossible) Unlike the DEFAULT metadata set: • Built-In sets cannot be renamed • Built-In sets cannot be disabled • Built-In sets are not limited to paths • Built-In attributes cannot be edited or deleted • Built-In sets only allow Read access ➡ Administrators can read more about Built-In Metadata Sets
Search	User Account Type Search Mode Added	Support for limiting user account searches to minimize the security risk of account hacking has previously been available in FileCloud by setting the *User Account Search Mode*. Now, to further limit a search of user accounts, a new option has been added that allows you to restrict the search results to a specific account access level. You can set the new *User Account Type Search Mode* to one of the following account types: • ALL • FULL • GUEST • LIMITED For example, if you want to allows users to see search matches only for FileCloud user accounts with Full Access when they are searching for a user to share a file or folder with, you can set this option to FULL. You can use both of these search modes 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. These settings can prevent users from searching for guests or limited users and can also help with GDPR compliance. ➡ Administrators can read more about Securing Shares by Limiting User Account Searches
Security	New ability to 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 Password* and if enabled it will prevent users from setting commonly used passwords for their user accounts. Places where the password will be checked: • Adding a new user (including an admin) • Updating the password (including admin) • Resetting the password (through forgot password email) • Importing users from CSV 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*.
Sync	Users can now log in to the Sync client using SSO	Sync users can now use single sign-on (SSO) to enter one name and password in order to access multiple applications. ➡ Administrators can read more about Desktop Apps Login support ➡ Users can read more about Log In to Sync Using SSO

User Portal	Able to tag groups in comments and notifications	A new feature has been added to allow users logged in to the User Portal to use @<group name> when adding a comment to a file. Adding this tag also notifies all the members of the group about the comment. This functionality was already present for tagging users.
		
		When a user opens a browser, logs in to the User Portal, browses to a file and clicks on it, in the right Details pane there is a section for comments.
		
		• After a user clicks Add Comment, a field appears for the user to type in their comment. If a user types the @ character, starting with the second character the user will see a pop-up list of not only all the users, but now also all groups that match the typed characters.
		• If the user selects a group from the list, the group is added to the comment
		• All tagged members of the group will be notified by email and notification pop-ups in small windows (toasts)
		• The administrator can configure if the user can mention any group or just the groups that he is part of.
		
		To configure the group tagging options:
		
		1. Open a browser and log on 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 *User* sub-tab.
		4. Next to *Group Visibility*, select one of the following options:
		   a. *Show all groups*
		   b. *Show groups user belongs to*
		5. Click *Save*.

Enhancements

Module	Feature Name	Description
Admin Portal	Display the number of members in a group	When an administrator opens a browser and logs in to the Admin Portal, in the left navigation pane, if they click on Groups, it will open the Manage Groups window. This windows displays information about all groups that exist, such as the name, when they were created, and what actions an administrator can perform. Now the Manage Groups windows includes a column called Users in Group which displays how many FileCloud accounts belong to the group.
Admin Portal	Set the File Change Notification Frequency in the Admin Portal	In previous versions, the File Change Frequency Notification could only be changed in the cron's running interval. Now this can be set in the Admin Portal using the following steps: 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. Scroll down to the bottom where there is a new field labelled *Email Notification Frequency*. 5. Change the value. 6. Save your changes.
Admin Portal	Ability to disable user account during import if the account is also disabled in Active Directory	As part of the Active Directory (AD) automatic synchronization that happens through cron, when a user account is disabled in AD, it is imported as a disabled account in FileCloud. To use this option: 1. Open a browser and log on to the *Admin Portal*. 2. On the left control panel, click **Groups**. 3. Select the **group** that you want to add users to, and then click the Edit Group ( ) icon. 4. On the *Group Details* screen, click *Manage Members*. 5. On the *Manage Group Members* screen, click *AD Group Import*. 6. Select the *Disable Users During Sync* option. 7. If there are users with disabled account in the AD group, they will be listed in the Admin Portal's *Manage Users* screen as having *Disabled Access*.

Admin Portal	New button to send the email on the same screen where you preview the edited email template	FileCloud provides you with various messages to send to a user when an action occurs. These messages can be customized, which means you are overriding the default messages that are provided with your FileCloud site after installation.
		Previously, you could preview the template but there was no way to send an email immediately to see how it looks in an email application. Now, when you preview an email template that you have just edited, there is a *Send Preview to Admin* button.
		To send an edited email template:
		1. Open a browser and log in to the Admin Portal. 2. From the left navigation panel, click **Customization**. 3. Click the **Email Templates** tab. 4. To change the mail subject and body, click the **Edit** button. 5. Make your changes, and then to save click *Submit*. 6. To confirm the changes, click **Preview**. 7. On the Preview dialog, click *Send Preview to Admin*. 8. The email with the template should be visible in admin's email account.
Admin Portal	New Installation Check	A new entry has been added to the system installation checks to ensure the Exif extension has been installed.

		• **The Exif extension is used** when uploading an image to generating a thumbnail. It is also used to extract information for the built-in metadata set for images.
		 • When Exif is disabled in PHP: A message appears in the logs saying that the Exif extension is disabled, up loaded images will not have a thumbnail, and the Image metadata set be empty.
		    • To disable: Open the php.inic file, comment out the exif extension, and restart the web server.
		 • When Exif is enabled in PHP: uploaded images will have a thumbnail and the Image metadata set will contain attributes for all image files.
		    • This is the default behavior.

Admin Portal	High Availability health check display is more comprehensive	FileCloud servers can be configured for High Availability (HA) environment to improve service reliability and reduce downtime in your IT environment.
		The Admin Portal has been enhanced to display all information about the health of each node.
		• Administrators can run a system check and it will show one record for each node of the HA system, with data about its health • Cron will continue adding node information to the checks. • This data will help you determine node information such as code level and MQ status
Admin Portal	New search option to filter list of Team Folders	To manage team folders, an administrator opens a browser, logs in to the FileCloud Admin Portal, and from the left navigation panel, under MANAGE clicks TEAM FOLDERS.
		• In some cases, enterprises might see multiple pages of team folders. • To help you filter the Team Folder list, a new search box has been added to the Manage Team Folders page.
Admin Portal	In Admin Summary email, available Storage Quota for the Team Folder Account is shown	The Admin Summary email now displays the available storage quota for the Team Folder account.
		Administrators can read more about Team Folders
Admin Portal	New Admin Portal option enables FIPS mode	If a FIPS-enabled FileCloud license is installed, there is a new option in the Admin Portal to enable FileCloud to run in FIPS mode.
		• This option is disabled in the Admin Portal if a non-FIPS license is installed. • IF the FIPS mode is enabled, FileCloud will notify you if existing files are encrypted with older ciphers. If this is the case, the current encryption must be disabled before enabling FIPS mode. • After FIPS mode is re-enabled, you must re-encrypt existing files if you want encryption at rest.
		To test running in FIPS mode:
		1. Login into the following admin UI at: fipstest.filecloudlabs.com 2. Install a license with FIPS140 component. 3. Refresh the admin UI. 4. The admin UI should not switch to FIPS mode. 5. Open the following file for editing: cloudconfig.php 6. Add the following line:

		``
		define("TONIDOCLOUD_FIPS140_ENABLED", 1);
		``

		7. Refresh the admin UI.
		8. The admin UI should switch to FIPS mode.

Collabora	Support for features in newer versions of Collabora	Newer versions of Collabora support binary office documents such as doc, ppt, and xls.
		Now, when you configure a system with Collabora and upload some binary documents, you can edit them.
		➡ Administrators can read about Web Editing with Collabora Code
File Extensions	Allow only specific file types to be uploaded	In previous versions, to help prevent users from uploading malicious attachments and viewing them, you could create a list of file extensions you did not want to allow users to upload.
		If the list of disallowed file extensions grows too large, you may want to just list the file extensions you want to allow.
		Support for this ability to specify only the types of files users can upload has now been added.
		➡ Administrators can read more about Managing File Extensions
File Managem ent	New option to allow users to clear all files from recycle bin at once	An administrator can now use a checkbox to allow or restrict a user's ability to clear all files at once from their recycle bins.
		• Selected by default in *Global Default Policy* and newly created policies. When this option is checked for a policy, users belonging to that policy and logged in to the *User Portal* can click on *Folder Actions* and select *Clear Deleted Files*.
		• If this option is not selected by clearing the checkmark, users belonging to that policy and logged in to the *User Portal* can click on *Folder Actions* but will not see a *Clear Deleted Files* option.
		⚠ This policy doesn't block the delete operation! Users can still remove files from the recycle bin on a file-by-file basis.
		To configure this option:
		1. Open a browser and log in to the *Admin Portal*.
		2. From the left navigation pane, under *Settings*, click *Settings*.
		3. On the *Manage Settings* screen, select the *Policies* tab.
		4. On the *Manage Policies* screen, select the *Global Default Policy* to change this for all users, or select the policy you want to use.
		5. In the row of the policy, click the edit icon (🖊).
		6. In the *Policy Settings* window, select the *User Policy* tab.
		7. Scroll down until you see a checkbox labeled *Enable Recyclebin Clear Feature*.
File Sharing	Email notification of a file share updated	When FileCloud sends an email notification that a share invitation has been sent, it displays the following message:
		"FileCloud successfully sent your invitation"
		Per customer requests, the message has been updated to remove the FileCloud name from the message. It now displays:
		"Invitation sent successfully."
		➡ Administrators can read more about Configuring System-Generated Emails
File Sharing	New option to copy sharing link to clipboard	When a user opens a browser and logs in to the *User Portal*, if a file or folder already has an existing share link, when you right-click on it, you get the *Manage Share* option. For new shares, the *Manage Share* screen is available if you select *Advanced Options*.
		If you want to copy the link, previously you had to select the link manually and use the Ctrl+C keyboard combination. However, this method does not copy just link but also includes a paragraph before the link, so it has to be cleaned up before it can be used directly.
		Now, on the *Manage Share* screen, a *Copy to Clipboard* button has been added.
		This allows users to quickly have the link available to them at the click of a mouse button.
File Sharing	Automatically delete shared files on expiration	In previous versions, when a shared file or folder expired, only the share links were removed and anyone with the link to the share would not be able to access it although the files and folders still remain.
		Now the administrator has the option to have the files automatically moved to the Recycle Bin when the share expires.
		➡ Administrators can read more about Specifying Share Expiration

File Sharing	Admin can now prevent user from changing sharing defaults	In previous versions, in the Admin Portal after an administrator configured Sharing defaults, all the default values could still be overridden by the user when the share is created or modified. The default values that the administrator could configure and the user could overrride included: • Share Type • Share Expiry in Days • Max Share Upload Size FileCloud now includes a setting in the Admin Portal, in Settings, on the Share tab, called Disallow Default Share Setting Change. After an administrator selects this option, users cannot set any values other than the default values configured by the admin when creating and modifying shares. ➡ Administrators can read more about Configuring Sharing Defaults

File Sharing	Ability to disable Allow Manage share option for large Network shares	**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");`

Network Shares	Display network share files and folders with a dot in the name	An new option has been added that allows you to display files and folders that have a name starting with a (.) dot. • This option can be set for network shares. By default, if you: • Create a network share from a folder that has a name starting with a dot (.), for example, .SystemTest • Share it with another user • When the user browses to the share the folder will not be displayed and it will appear empty Similarly, if you: • Create a network share from a folder with a name that does not start with a dot (.), for example, AdminTest • Create files inside this folder that have a filename that starts with a dot (.), for example .Atest1, .ATest2 • Share it with another user • When the user browses to the share the folder will be displayed but the files inside will not and it will appear empty To display folders and files that start with a dot (.) : 1. Open the following file for editing: <code>cloudconfig.php</code> 2. Add the following line: <code>define("TONIDOCLOUD_SHOW_FILES_STARTWITH_DOT", 1);</code> 3. Refresh User Portal web page and the folders and files are now visible. ➡ Administrators can read more about Setting Up Network Folders
Recycle Bin	Recycle Bin configuration can now be set per user or group through policies	In previous versions, if an administrator wanted to configure how the recycle bin worked, they configured storage settings. These settings applied to all users and all items in Managed (My Files) and Network storage. Administrators can now configure options related to Recycle Bin behavior on a user or group level instead of only at a system-wide level for Managed storage. • The global configuration settings related to the recycle bin can now be configured only in policies. • This enhancement allows administrators to use different settings for different users and groups. • Administrators can still set global recycle bin policies using the Global Default Policy. • The recycle bin configuration settings for Network folders is still global and managed in the Admin Portal under the MANAGE section by selecting Network Folders. For example: In the Cherry Road Real Estate company, every user working in the Accounting office must retain their recycled items for 60 days, but everyone else can have their bins cleared in 30 days. You can now configure when the recycle bin is cleared differently for different groups and users. The following three Recycle Bin settings now exist in Policies:

Setting	Option	Description
Store Deleted Files	YES or NO	Move the file from it's location in My Files to the recycle bin when the user deletes it
Automatically Delete Files from Recycle Bin After Set Number of Days	Whole number	Number of days after the file was deleted that it will be cleared from the FileCloud System. A value of 0 indicates that deleted files will not be cleared automatically.
Do Not Store Deleted Files Greater Than	Any positive number of Units: • GB • MB • KB • B	Files Greater than the specified size are permanently deleted. The number can contain decimals. For example: • 0.09765625 GB

Remote Client Management	Disable remote management toggle	**Issue:** In the Sync client application, users can go into *Settings*, click on the *Advanced* tab, and select or de-select *Allow Remote Management* to allow or prevent administrators from managing their Sync app by setting options in the Admin Portal. In some cases, administrators want to disable this toggling.
		
		Resolution: Now an administrator can disable this option by adding a registry key called *allowcentralmgmtusermodify*.
		
		• When set to 0, the central management option is disabled and can no longer be changed by users.
		
		To add the registry key:
		
		1. Add a registry key under:
		
		`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\CodeLathe\FileCloud\DefaultCfg`
		
		2. Name the registry key:
		
		`allowcentralmgmtusermodify`
		
		3. Restart the computer.

Requirements	PHP Upgraded to 7.2	FileCloud Server uses PHP: Hypertext Preprocessor for it's Memory caching system. • The version of PHP was upgraded to version 7.2
Search	Solr updated to version 7.6.0	Solr enables content search in FileCloud for file types such as txt, pdf, doc, docx, xls, xlsx, ppt, pptx, as well as regular expressions. To include the improvments in the Solr version 7.6.0, the FileCloud installers have been updated to include this Solr version. As the Solr software is automatically included in FileCloud's Windows and Linux installers, the latest version will automatically be available. However, to make use of Solr, administrators are still required to install OpenJDK, which is an open source execution of the Java Standard Edition platform. For more information on the Solr 7.6.0 release, read the Apache Solr Release Notes Administrators can read about Setting Up Content Search
Security	New option to enable or disable the IP check	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. To configure this option: 1. Log into *Admin Portal*. 2. From the left navigation panel, select **SETTINGS** and then **Settings**. 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.
ServerSync	Disable syncing of specific folder sets	In previous versions, there was no way to disable the synchronization of one server folder without completely removing it. Two new ways have been added that allow you to specify that a folder should not be synchronized. • **Disable Sync button.** In *ServerSync*, on the *Settings* screen, select the *Folders* tab. If the folder is currently being synchronized, you will see a *Disable Sync* button. If the folder is not being synchronized, you will see an *Enable Sync* button. In the folder list, all disabled folders are greyed out. • **Device Configuration XML for Sync**. Use the Client Device configuration settings to remotely specify the Server Sync's behavior using XML policies. To disable the synchronization of a folder, add the *<limit_folder _count>* and *<limit_folder_X>* tags with the appropriate variables. Administrators can read more about Synchronizing Folders in ServerSync

ServerSync	One Way Sync Added	When a new folder is being added to the sync list, users can now choose a Remote to Local type of synchronization.

When a new folder is being added to the sync list, users can now choose a Remote to Local type of synchronization.

- This means that any changes made in the local folder are not uploaded to the server.
- If the same file is modified on both the server and locally, there will be no conflict file created. Instead, the local file will be overwritten with the server version of the file.
- If the file is deleted locally, it will be copied back from the server.

This feature is available only for new folders that are added.

- If you want to change the Sync type for existing folders, users have to delete the folder from the list and then add them back with the sync type required.

Administrators can also configure the sync type using RMC (Centralized Device Configuration).

ServerSync — New options to add proxy settings before user logs in.

In previous versions, there were no options for adding proxy settings in FileCloud Sync before logging in as a user. In previous versions, it was possible to add proxy setting only after logging in and accessing ServerSync's Advanced settings.

Proxy settings can now be provided in ServerSync in the following places:

- During user login from the settings dialog (Proxy settings entered here by the user are saved in the syncclientconfig.xml file.)
- Adding proxy settings as parameters in the syncclientconfig.xml manually

You can no longer add Proxy Settings after logging in and accessing Sync's Advanced Settings. These proxy setting fields have been removed.

To add proxy settings to the syncclientconfig.xml manually:

1. Open the *syncclientconfig.xml* file in one of the following locations:

OS	Location
Windows	%APPDATA%\FileCloudSync\syncclientconfig.xml
Mac OSX	{HomeDir}\FileCloudSync\syncclientconfig.xml
Linux	{HomeDir}\FileCloudSync\syncclientconfig.xml

2. Add the following entries replacing the sample values with the ones you want to use:

XML Code	Notes
```<rowentry> <name>httpprox yhost</name> <type>string< /type> <value>10. 1.0.1</value> </rowentry>```	Entry for the proxy host. - If ServerSync has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server address. - For example, if your proxy server is 10.1.0.1, it can be configured as shown.
```<rowentry> <name>httpprox yport</name> <type>string< /type> <value>8080< /value> </rowentry>```	Entry for the proxy port. - If ServerSync has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server port. - For example, if your proxy server listens at port 8080, it can be configured as shown.
```<rowentry> <name>httpprox yuser</name> <type>string< /type> <value>proxyus er</value> </rowentry>```	Entry for the user account. - If ServerSync has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server user. - For example, if your proxy server needs to authenticate with a user proxyuser, it can be configured as shown.
```<rowentry> <name>httpprox ypassword</name> <type>string< /type> <value>passw0rd </value> </rowentry>```	Entry for the account password. - If ServerSync has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server user. - For example, if your proxy server needs to authenticate with a password passw0rd (for configured proxy user), it can be configured as shown.

Sharing	The Send Link via Email option for shared files and folders is now available in Sync and Drive	When Sync and Drive users right-click a file in File Browser and then select the option to share a FileCloud link, a Share Link window opens to provide the link. Previously, the option to send the share link in Email was not available. Now all Sync and Drive users have this option available to match what is available in the FileCloud User Portal.
Single Sign-On	Limit Single Sign-On (SSO) login to users in specific groups	You now have the ability to limit the use of SAML SSO to a group. • This means that a user can login through SAML SSO only when the Identity Provider indicates that the user belongs to the SAML SSO group • An Identity Provider is an infrastructure as a service (Iaas) entity that can communicate with FileCloud to provide a centralized SSO solution • This attribute is set through the *memberof* parameter • The *memberof* parameter can include a comma separated value of all groups to which the user belongs ➡ Administrators can read more about SAML Single Sign-On
Single Sign-On	Sync and Drive applications no longer require the user to re-authenticate every time when using SSO	After a FileCloud Drive or Sync user logs in to their FileCloud account without using SSO, their credentials are retained. • This means that if they restart the computer, Sync and Drive will automatically log users back into their FileCloud account. If an administrator sets up SSO authentication, when the user opens the Login screen, they can click the Login with SSO button and type in their username and password. • When using SSO, after logging in, their credentials were not retained. • If the user restarts the computer, Sync and Drive requires the user to re-enter their credentials every time. Now, the SSO credentials are retained just as they are for all other users. • A user with SSO credentials does not have to manually authenticate every time.
Sync and Drive Clients	New abilities for users when sharing files and folders including editing the Shared File/Folder field, restricting downloads, and g ranting permissions to Everyone	FileCloud client applications have been updated to include more features that are also available on the User Portal. Sync and Drive now include the following options for users when sharing a file or folder: • Edit the Shared File or Folder field • Restrict downloads (Not restricted by default) • Grant permissions to Everyone at once
Sync and Drive Clients	Open URL and Share Activity options now available in both Sync and Drive	FileCloud client applications have been updated to include more features that are also available on the User Portal. Sync and Drive now include the following options for users when sharing a file or folder: • Open URL • Share Activity (Windows Only)
Sync Client	Restrict specific file names from being uploaded	To help prevent users from uploading files with malicious names or to restrict users uploading personal files that are extremely large, an administrator can create a list of restricted file names in FileCloud Server. Sync has been updated to check with the *FileCloud Server* for a list of *Disallowed File Names* set by the administrator. The file that the user in the Sync Client is trying to upload is checked against this list. Only exact matches are blocked from being uploaded and the user is shown an error message. • If the administrator creates a list with an extension in the file name, then only the combination of name + extension will be restricted. ⚠ If you leave an empty space in your list, then Sync will ignore checking for restricted names. NOTE that this behavior is different than what happens when the User Portal encounters a restricted file list with a space. For example, if an administrator creates a list in *Disallowed File Names* that specifies: • "hello.xyz|hello" - only files which have names "hello.xyz" and "hello" are not uploaded. Every other file will be uploaded. ➡ Administrators can read more about Restricting File Names
Sync Client	Server URL Defaults to http://	In previous versions, during the initial setup of the Sync Client, the *Server URL* field would default to an unsecured hypertext transfer protocol URL (http://). To recommend the authentication of the user and for the protection, privacy, and integrity of the exchanged data, the server URL now defaults to an HTTPS URL (https://) which allows for a connection encrypted by Transport Layer Security Secure Sockets Layer. ➡ Users can read more about how to Start and Log In to Sync

Sync Client	Checking for locked files before uploading	Currently, when a user in the Sync client tries to upload a file that is open and locked, the user will see errors. This behaviour prevents uploading the file that is in use and shows the user errors. You now have the ability to prevent the upload of locked files without showing errors by setting a value for the *checklockedbeforeupload* parameter in the *syncclientconfig.xml* file. The file can be uploaded when the file is closed and no longer locked. 💡 This is especially useful when users have limited internet bandwidth because Sync does not even attempt to send the file to the server if the *checklockedbeforeupload* parameter is set. ➡️ Administrators can read more about XML Options for Sync
Sync Client	Managing Skipped Files	When synchronization occurs, some file types are not processed by the Sync client application. The Sync client now provides more support for managing skipped files. • The Activity log dropdown now has four categories that display the files that are ignored. • For My Files and the top-level folder (root of the Sync folder), the count and total size (MB/GB) of ignored files is also displayed. • You can also export a list of these files. ➡️ Sync users can read more about Reviewing Skipped Files

Sync Client	New options for restricting file types and setting an upload size limit during Sync backup	Two new options have been added to manage the content uploaded during Sync backup:
		
		• *backuprestrictions* - Allows you to specify the file types that should be ignored during Sync backup. (Multiple values can be specified by using "|" - for example "mp3|bat")
		• *backupsizelimit* - Allows you to specify the upload size limit during Sync backup. (Must be specified in MB)
		
		To enable these options:
		
		1. Open the *syncclientconfig.xml* file in one of the following locations:
		
		<table><tr><th>OS</th><th>Location</th></tr><tr><td>Windows</td><td>%APPDATA%\FileCloudSync\syncclientconfig.xml</td></tr><tr><td>MAC OSX</td><td>{HomeDir}\FileCloudSync\syncclientconfig.xml</td></tr><tr><td>Linux</td><td>{HomeDir}\FileCloudSync\syncclientconfig.xml</td></tr></table>
		2. Add any of the following entries, replacing the sample values with the ones you want to use:
		
		`<rowentry>`
		`  <name>backuprestrictions</name>`
		`  <type>string</type>`
		`  <value>mp3</value>`
		`</rowentry>`
		
		`<rowentry>`
		`  <name>backupsizelimit</name>`
		`  <type>double</type>`
		`  <value>2</value>`
		`</rowentry>`
		
		➡️ Administrators can read more about XML Options for Sync

Sync Client	Allow Sync to upload hidden files to the server	When Sync uploads files to FileCloud Server, you can now allow Sync to upload even hidden files.

Most commonly, hidden files and directories in the home directory contain settings or data that's accessed by that user's programs. They're not intended to be edited by the user, only the application. Hidden or dot files are not a security mechanism.

- In Windows: you can hide a file by right-clicking it, opening the *Properties* dialog, and then under the *Attributes* section, check the *Hidden* option and click *Apply*.
- In Linux: any file with a name that starts with a dot (.) is hidden. These files will not be displayed by default when listing the contents of a folder, however, you can use the *ls* command with options such as *(-a)* to view hidden files.

The list of file types, hidden or normal, that you want synchronized with the server can be specified using the following parameter:

- *allowedfilelist* - If a "*.*" is used, ALL hidden files will be uploaded.

To enable this option:

1. Open the *syncclientconfig.xml* file in one of the following locations:

OS	Location
Windows	%APPDATA%\FileCloudSync\syncclientconfig.xml
Mac OSX	{HomeDir}\FileCloudSync\syncclientconfig.xml
Linux	{HomeDir}\FileCloudSync\syncclientconfig.xml

2. Add any of the following entries, replacing the sample values with the ones you want to use:

```
<rowentry>
    <name>allowedfilelist</name>
    <type>string</type>
    <value>lnk|ini</value>
</rowentry>
```

Sync Client	New options to add proxy settings before user logs in.	In previous versions, there were no options for adding proxy settings in FileCloud Sync before logging in as a user. In previous versions, it was possible to add proxy setting only after logging in and accessing Sync's Advanced settings.

In previous versions, there were no options for adding proxy settings in FileCloud Sync before logging in as a user. In previous versions, it was possible to add proxy setting only after logging in and accessing Sync's Advanced settings.

Proxy settings can now be provided in Sync in the following places:

- During user login from the settings dialog (Proxy settings entered here by the user are saved in the syncclientconfig.xml file.)
- Adding proxy settings as parameters in the syncclientconfig.xml manually

You can no longer add Proxy Settings after logging in and accessing Sync's Advanced Settings. These proxy setting fields have been removed.

To add proxy settings to the syncclientconfig.xml manually:

1. Open the *syncclientconfig.xml* file in one of the following locations:

OS	Location
Windows	%APPDATA%\FileCloudSync\syncclientconfig.xml
Mac OSX	{HomeDir}\FileCloudSync\syncclientconfig.xml
Linux	{HomeDir}\FileCloudSync\syncclientconfig.xml

2. Add the following entries replacing the sample values with the ones you want to use:

XML Code	Notes

`<rowentry>`
`    <name>httpprox`
`yhost</name>`
`    <type>string<`
`/type>`
`    <value>10.`
`1.0.1</value>`
`</rowentry>`
	Entry for the proxy host.
	
	- If the FileCloud Sync client has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server address.
	- For example, if your proxy server is 10.1.0.1, it can be configured as shown.

`<rowentry>`
`    <name>httpprox`
`yport</name>`
`    <type>string<`
`/type>`
`    <value>8080<`
`/value>`
`</rowentry>`
	Entry for the proxy port.
	
	- If the FileCloud Sync client has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server port.
	- For example, if your proxy server listens at port 8080, it can be configured as shown.

`<rowentry>`
`    <name>httpprox`
`yuser</name>`
`    <type>string<`
`/type>`
`    <value>proxyus`
`er</value>`
`</rowentry>`
	Entry for the user account.
	
	- If the FileCloud Sync client has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server user.
	- For example, if your proxy server needs to authenticate with a user proxyuser, it can be configured as shown.

`<rowentry>`
`    <name>httpprox`
`ypassword</name>`
`    <type>string<`
`/type>`
`    <value>passw0rd`
`</value>`
`</rowentry>`
	Entry for the account password.
	
	- If the FileCloud Sync client has to use an HTTP Proxy server for outside connections, use this parameter to configure proxy server user.
	- For example, if your proxy server needs to authenticate with a password passw0rd (for configured proxy user), it can be configured as shown.

Time Formats	Time can now be set to a 24-hour format	In previous versions of FileCloud, an administrator could open a browser, log on to the Admin Portal, click **Settings**, **s**elect the *Misc* tab, then the *General* tab, and choose a Time Format option that displayed the time in AM or PM in the following ways:

In previous versions of FileCloud, an administrator could open a browser, log on to the Admin Portal, click **Settings**, **s**elect the *Misc* tab, then the *General* tab, and choose a Time Format option that displayed the time in AM or PM in the following ways:

- h:mm A (2:20 PM)
- h:mm:ss A (2:20:35 PM)

Now, FileCloud includes two new time format options that display times in a 24-hour format:

- HH:mm (14:20)
- HH:mm:ss (14:20:35)

The time set, as by the administrator on the Admin Portal, is displayed in the following places:

Component	Locations
Admin Portal	Any list displaying: - Users Last Login - Expiry - Groups Created On - File Lists - User Shares (created date) - Devices (last access) - Audit (created On) - Alerts (date) - User locks (expiration)
User Portal	Any list displaying: - Files - Activity - Comments - Shared Items - Share Activities - Search - Folder or File Details
FileCloud Clients	All displays listing time in: - FileCloud Mobile App - Sync File Browser - Drive File Browser

To set the Time Format:

1. Open a browser and log into FileCloud *Admin Portal*.
2. In the left navigation panel, click **Settings**.
3. Select the *Misc* tab.
4. Select the *General* tab.
5. Next to the *Time Format* label, choose an option.

User Management	When deleting a user, move their files instead of deleting	When a user account needs to be deleted, administrators can now we move the files to a different user instead of allowing the files to be deleted with the user account. Support for moving the files before a user deletion is currently only available through the command line.

When a user account needs to be deleted, administrators can now we move the files to a different user instead of allowing the files to be deleted with the user account. Support for moving the files before a user deletion is currently only available through the command line.

The command is available at:

```
WWWROOT/resources/tools/fileutils
```

Administrators can transfer files in a user account before deleting it using the following command:

```
php txfilesanddeleteaccount.php -h <host> -u <user> -p /destination
/path -o
```

Usage:
    [Required] -h <host> Site host name or 'default' for default site
    [Required] -u user account whose files are to be transferred before account delete
    [Required] -p path to which the user files are to be moved before deleting account
    [Optional] -o set this flag to overwrite and merge transferred file with destination

Examples:
a) Command to transfer files of user "richard" to path /tgtuser/holding of default site:

```
D:\work\gitrepo\cl-fc-server\server\resources\tools\fileutils>D:
\xampp\php\php.exe txfilesanddeleteaccount.php -h default -u richard -p
/tgtuser/holding
```

b) Command to transfer files of user "richard" to path /tgtuser/holding of default site, overwriting files/folders that may exists in the destination:

```
D:\work\gitrepo\cl-fc-server\server\resources\tools\fileutils>D:
\xampp\php\php.exe txfilesanddeleteaccount.php -h default -u richard -p
/tgtuser/holding -o
```

User Portal — Error messages indicate whether or not a user account is valid

In FileCloud Server version 19.1, the error message that a user sees when they provide invalid login information was changed to the following:

- Account doesn't exist error message: *"User does not exist or you reattempted with a wrong password."*
- Invalid password error message: *"Invalid Username or Password. Password is Case Sensitive."*

For security reasons, these error messages can be problematic since information is given about whether a user account exists or not.

Now, identical messages are given for invalid login attempts to help to prevent brute force attacks and provide less information for a potential attacker.

➡️ Administrators can read more about User Authentication Settings

User Portal — Added support for browser-based document preview

When a user opens a browser and logs in to the User Portal, if the administrator enables document preview, the user will see a preview of the document using the browser resources rather than server resources.

User Portal — HTML-formatting for better user experience and checkbox for I agree

An administrator can enable Privacy settings in the Admin Portal so that when a user logs in to the User Portal, they see a consent box. HTML-formatting has beed added to improve the display of the privacy warning. The user is now also required to click a button to continue, either:

- I Agree to open the User Portal
- Decline to close the browser window and end the login attempt

User Portal — Ability to hide the More Options button on the User Portal Login page

When a FileCloud user opens a browser and enters their credentials on the Login page to the *User Portal*, there is a button called *More Options* that allows users to access the *Forgot Password* option. Some enterprises who use Active Directory want to be able to hide this button and the *Forgot Password* option. By default, the *Show More Options* checkbox is selected. If you want you can clear this option to hide it from the User Portal *Login* screen.

To hide the More Options button:

1. Open a browser and log in to the *Admin Portal*.
2. From the left navigation pane, under *CUSTOMIZATION*, click *Customization*.
3. Select the *General* tab, and then the *Login* sub-tab.
4. Next to the *Show More Options* label, clear the checkbox.

| User Portal | Ability to hide the Web Edit button | 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*. |

Workflows	A new parameter added to Create a New User for filtering by account type	When an administrator opens a browser and logs in to the Admin Portal, they can create a workflow to automate what happens after a new user account is created. The workflow is created by selecting an IF condition, that when met, triggers a THEN action.

When creating the workflow, the administrator can select from the following parameters:

IF *Create a New User*

This tells FileCloud that if <u>ANY new user account</u> is created to trigger the THEN action.

Optional Parameters allow you to change *ANY new user to account* to an account that uses a specific authentication type:

- Active Directory *"auth_type" : {ACTIVEDIRECTORY}*
- Default *"auth_type" : {DEFAULT}*
- LDAP *"auth_type" : {ANY}*

⚠️ It is important to understand that the ANY condition will work for all users, and may overwrite actions from specific (*ACTIVEDIRECTORY, DEFAULT)* conditions.

THEN CLAUSE

This tells FileCloud what to do after a new user account is created. Options include:

- Run a report
- Notify the user that the account may be deactivated soon
- Disable user account
- Delete user account
- Change user status
- Generate an email report
- Notify user(s)

A new Optional Parameter has been added to allow you to specify which types of new user accounts should be acted upon. You can identify the accounts by *user_account_type* :

- Full Access *"user_account_type" : {USER_ACCOUNT_FULL_ACCESS}*
- Guest Access *"user_account_type" : {USER_ACCOUNT_GUEST_ACCESS}*
- LIMITED_ACCESS *"user_account_type" : {USER_ACCOUNT_LIMITED_ACCESS}*

For example, when you import new user accounts from Active Directory (AD) into FileCloud Server, 99% of the time they are set to FULL ACCESS. If you want to automate the process of notifying users that their AD account credentials now work on the FileCloud User Portal with full access, you can create a workflow with the following parameters:

IF *Create New User*

"auth_type" : {ACTIVEDIRECTORY}

THEN *Notify Users*

"user_account_type" : {USER_ACCOUNT_FULL_ACCESS}

In the example, this automation will <u>not be triggered</u> to notify a new user if the new account uses AD authentication but only has limited access. This allows you to handle the few special cases while letting the workflow automation handle the majority of common responses to new user account creation.

Workflows	Workflows now display activity, can be suspended and simulated	Administrators can use workflows to automate certain standard operations within FileCloud. Three new features have been added to the Manage Workflow screen to provide more details about how workflows are functioning and how they impact your FileCloud Server system. • Activity - All workflows now have the ability to show the Date of an event, and a Description of the event, such as file uploads, moves, and deletions. • Suspension - Suspending a workflow will prevent the workflow from automatically running at the next Cron job. This option retains the workflow if you want to manually run it. • Simulation - Use this option to display the list of users or files that a workflow will affect. The Simulate option is only available to workflows that are configured to run on demand and not to run automatically at scheduled times. Workflows now include the following options:

1. Run the workflow (once, on-demand)
2. Simulate the workflow
3. Edit the workflow
4. Enable or Disable the workflow
5. See the activity
6. Delete the workflow

To add a new workflow:

1. Open a browser and log into the Admin Portal.
2. On the left hand navigation panel, under MISC., click **Workflows**.

Issues Resolved

Module	Issue	Description
Active Directory	AD groups cannot be imported directly but are still listed	Issue: 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. Resolution: FileCloud Server has been modified to stop displaying built-in AD groups that cannot be imported.
Admin Portal	Users with Lowest Quota Remaining report not working	Issue: When an administrator logs on to the *Admin Portal*, the *Home* dashboard screen opens by default. At the bottom of the page is a section entitled *Users with Lowest Quota Remaining* which runs a report on FileCloud usage and displays the following information: • Percent Used • User name • File Count • Quota Used • Quota Assigned When the *Percent Used* grows larger than 999%, the pie chart and number that describe *Percent Used* are not correct. For example, if a user uploads a 10 MB file, and then the user's *Quota Assigned* is changed to 1 KB, the *Percent Used* column will show 999% instead of the correct 1000%. Resolution: The *Users with Lowest Quota Remaining* report was modified to calculate and display the correct value. Administrators can read more about using The Dashboard
Admin Portal	Dashboard reports for File Type Distribution and User File Distribution are not correct	Issue: When an administrator logs on to the *Admin Portal*, the *Home* dashboard screen opens by default. The dashboard contains reports for File Type Distribution and User File Distribution in the form of pie graphs. If there are no files stored on the FileCloud Server, the pie graph shows usage at 100% instead of 0%. Resolution: The dashboard has been updated so that if there are no files stored in FileCloud Server, then in the Admin Portal, on the Dashboard, File Type Distribution and User File Distribution shows usage at 0%. Administrators can read more about using The Dashboard

Admin Portal	In the Audit window, mouse over an IP and the map shows zoom tools but then they disappear	Issue: When an administrator logs on to the Admin Portal, the admin can click on Audit to open the Audit Logs window. In the results table, the admin can mouse over the IP address and a map will appear showing the location of the IP address. Tools for zooming also appear, however, when they are clicked on they disappear. Resolution: The Audit Logs window has been modified so that the map does not disappear when a user clicks inside the map. This allows the zoom tools to be used as expected. Administrators can read more about how to View Audit Logs
Admin Portal	Audit search does not work if a full email address is used	Issue: An administrator can display only audit logs entries for a specific user by typing in an email address in the Audit Log search box. To so this, an administrator opens a browser and logs in to the Admin Portal. From the left navigation panel, after the administrator clicks Audit, on the Audit Logs window, in the search box, the email address can be typed in. The results that the administrator will see depends on how the email address is typed in. For example:

Parameter		Filter	Display Shows
JoeC@MyCompany.com	✖	None applied	All audit log entries
JoeC@MyCompany.co	✖	None applied	All audit log entries
JoeC@MyCompany.c	✖	None applied	All audit log entries
JoeC@MyCompany	✔	Entries with	Only entries where User Name or Message includes "JoeC@MyCompany"

Resolution: The FileCloud Server Admin Portal has been modified so that on the Audit Logs window, any form of email address typed into the search box will limit the display of entries to those containing the search term used.

Administrators can read more about how to Filter Audit Log Views |
Admin Portal	Login to Admin Portal fails when SSO is enabled	Issue: An administrator can open a browser, log in to the Admin Portal, and set up SSO for an admin account. However, when logging in later with that account, the administrator will see errors and be unable to log in to the Admin Portal. Resolution: The FileCloud Server Admin Portal has been modified so that when SSO is set up for an admin account, the administrator will be able to log in to the Admin Portal with that account. Administrators can read more about Single Sign On
Admin Portal	Helper version displayed incorrectly	Issue: An administrator can create a network share with a path that uses XML special characters like the & symbol, enable Realtime indexing, and then start the FileCloud Helper Service. When the administrator checks the status of the Helper service, it will be displayed incorrectly. Resolution: FileCloud Server Admin Portal has been modified to display the correct version of the Helper Service that is running. Administrators can read more about the FileCloud Helper Service
Admin Portal	Helper service hangs when there is no database connection	Issue: When an administrator starts the FileCloud Helper service, if MongoDB is not running, then the Helper Service just hangs indefinitely. Resolution: The Helper Service has been modified so that when the administrator starts the Helper service, if MongoDB is not running, it will continue to retry to read the database until the database is available. Administrators can read more about the FileCloud Helper Service
Admin Portal	Audit logs export to CSV file has IP and HOW column headings reversed	Issue: An administrator can open a browser, log in to the Admin Portal, click Audit, and then export the Audit log entries to a CSV file. When the administrator opens the CSV file, the IP and HOW column headings are reversed. Resolution: FileCloud Server Admin Portal has been modified so that when Audit log entries are exported, the IP and HOW columns are not reversed.
Admin Portal	Hosted FileCloud should not allow admins to change the "FROM" address	Issue: In a hosted scenario, where the configuration is defined with ("TONIDOCLOUD_HOSTED_CLOUD",1); administrators can change the FROM address in the Settings screen on the Email tab. Resolution: FileCloud Server has been modified to prevent administrators from changing the email FROM address in a hosted environment in the following ways: • If key TONIDOCLOUD_HOSTED_CLOUD is set to 1, then the administrators is prevented from changing the FROM email. The administrator can save a change in the Admin Portal, but FileCloud will ignore the setting. • If key TONIDOCLOUD_FC_HOSTED_FROM_EMAIL isn't set, the FROM email will default to fchosted@filecloudmail.com.
Admin Portal	Administrator can create a user with an account name of Admin	Issue: When an administrator opens a browser and logs in to the Admin Portal, they can create a new user with an account name of admin. FileCloud Server allows the user account to be created. 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. It says: You are trying to login into user portal with admin account. CLFC-00035-00116 Resolution: 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.
Admin Portal	Auto backup for database not working for HA	Issue: By default, automatic database backups are enabled. This can be disabled in the Admin Portal, from the left navigation panel under SETTINGS, select the Settings tab, then the Misc. tab, and then the General sub-tab. On the General sub-tab, there is an option to select Disable DB Backup. However, in environments where High Availability architecture is being used, and the Disable DB backup option is NOT selected, the automatic back up is still not being performed during Cron runs. Resolution: FileCloud Server has been modified so that in environments where High Availability architecture is being used, and the Disable DB backup option is NOT selected, the automatic back up is performed during Cron runs.

Admin Portal	Removing the last user or group from folder permissions displays a *Bad Role* error	Issue: When an Administrator opens a browser and logs in to the Admin Portal, from the left navigation panel, under MANAGE, they can select Folder Permissions to set permissions on folders. If the administrator opens a folder that grants users or groups access to it, when the administrator removes the last user or group, an error message will display with a message of Bad Role or Bad Path. Resolution: FileCloud Server has been modified so that when the administrator removes the last user or group from a folder's permissions, no error is displayed.
Admin Portal	Super Admin And Admin login creates duplicate key entries	Issue: When a user logs in to the Admin Portal with an account called Admin or Super Admin duplicate key entries are created and after one of these accounts logs in, the other will not login or show errors. Resolution: FileCloud Server has been modified so that duplicate key entries are not created when an account called Admin or Super Admin logs in to the Admin Portal, allowing both accounts to be logged in.
DocConverter	Starting from FileCloud Control Panel overwrites existing DocConverter AppParameters registry value	Issue: Administrators can use a Java-based service called FileCloud Document Converter to enable thumbs and interface with LibreOffice for document preview generation. When an administrator logs on to the server running FileCloud, and from the Windows Start menu, selects *Open the FileCloud Control Panel*, they can then choose to start the DocConverter service. If the administrator then needs to run DocConverter on a different port the preview features will not work unless DocConverter is started manually from Windows Services. Resolution: The FileCloud Control Panel has been modified so that if DocConverter is started from the FileCloud Control Panel, and then DocConverter needs to be run on a different port, the preview features will work correctly. ➡ Administrators can read more about DocConverter
Document Preview	Document Preview installation fails	Issue: When an administrator logs on to the server running FileCloud, and from the Windows Start menu, selects *Open the FileCloud Control Panel*, they can click Document Preview Install service but it will display an error that it "Failed to install as service not found" even though the service is installed. If the administrator tries to start the service, the same error message is shown, and document preview does not work in the User Portal. Resolution: FileCloud Server has been modified so that when an administrator clicks Document Preview Install service it will not display an error, the service is installed, can be started, and is working in the User Portal. ➡ Administrators can read more about installing Document Preview
Document Preview	Document Preview becomes unresponsive for large files	Issue: When a user opens a browser and logs on to the User Portal, they can upload large files if there is no size restriction set by the administrator. For files larger than 10 MB, after the file is uploaded, if the user click the Preview button, the User Portal becomes unresponsive. Resolution: The User Portal has been modified to warn the user when the Preview button is clicked that the file is too large to preview. ➡ Users can read more about how to Preview a File
Drive Client	Uploading a file to a Read-Only folder shows an uploading message	Issue: In a shared folder, such as a Team Folder, the owner gives Read, Delete, Write, and Share permissions to all FileCloud users. Inside this folder, a user shares a sub-folder and gives Read-Only permissions. If a user connects to FileCloud using the Drive client, creates a file in the sub-folder with Read-Only permissions and tries to upload it, the user will see an error and then an uploading message, but the upload will not occur. Resolution: Now FileCloud Server tells the user that folder permissions do not allow the file to be uploaded. The file still exists in the folder where the user created it in the Drive local folder, but it is not available on the server or shown in the User Portal. ➡ Users can read more about Working with FileCloud Drive
Drive Client	The Activity tab does not show the time in the local time zone	Issue: By default, Drive shows on the Activity tab the time that actions occur in GMT instead of using the local time zone where the Drive client is being used. Resolution: Drive has been modified so that the Activity tab shows the time that actions occur in the local time zone where the Drive client is being used. ➡ Users can read more about Setting Up Drive for the First Time
Drive Client	In Windows, the registry data for DisplayName and version is not correct	Issue: On the computer where the Drive client is installed, if you use view the registry key for the FileCloud application, you will see the Name displayed as "DisplayName" instead of FileCloud. If you open the Windows Control Panel to uninstall or change the application, the version field is empty and does not display any information. Resolution: FileCloud Drive has been modified to write and display registry information correctly, both when viewing the registry key and when viewing information about the application in Control Panel. 💡 This issue has also been corrected for the FileCloud Sync client
Drive Client	A Windows users cannot save an image file from Photos to Drive	Issue: If a user opens the Drive client, then opens an image from Drive in the Windows Photos app, clicks *Save As* and types in a new file name, when the user clicks *Save*, they get an error. Resolution: The Drive client has been modified to allow users to save an image from the Photos Windows application to Drive without errors. ➡ Users can read more about using FileCloud Drive
Drive Client	Previous versions not displayed and options not available	Issue: In Drive, the different versions of a file are not displayed and users can not download, delete, or make live a particular version. Resolution: The Drive client application has been modified to provide options in the explorer to see the previous versions and download, delete or make a file live are available by right-clicking on the file and then selecting Properties and then Versions.
Drive Client (Mac OS)	Enabling options to run at startup and open a file browser window at startup do not work	Issue: If a Mac Drive user selects one of the following settings, they will not work. Also, the options should not include Windows for a Mac desktop. • Run at Windows Startup • Open Explorer Window in Startup Resolution: The Mac Drive client has been modified to run at startup and open file browser screen when the user enables these options. ➡ Users can read more about FileCloud MacDrive

Drive Client	Large Excel files not uploading	Issue: When a user opens an Excel file from a Drive folder that is larger than 50 MB, after editing the file, changes will not be uploaded to FileCloud Server and errors are shown in the Microsoft Excel application. Resolution: The Drive client has been modified so that when a user opens an Excel file from a Drive folder that is larger than 50 MB, after editing the file: • If the user has Drive1 installed: Failure is expected because of long upload time. The Microsoft Excel application will show an error. Try splitting up the Excel file so that it is lass than 50MB, or upgrading to Drive2. • In the case Drive2, there should be no error and the file will be uploaded successfully. ➡ Users can read more about FileCloud Drive
Drive Client (Mac OS)	Mac Drive 2 does not open About and Help dialogs correctly	Issue: When a Mac Drive user selects the *Help* and *About* items from the Mac Drive 2 menu, nothing happens. Resolution: The Drive client has been modified so that when a user chooses *Help* and About from the menu the information is displayed. ➡ Users can read more about FileCloud MacDrive
Drive Client	Drive upgrades write over any custom configurations	Issue: When a user upgrades Drive, the config.xml file is overwritten and the custom configuration is lost. Resolution: The Drive client has been modified so that when a user upgrades it, the config.xml file is not overwritten if it already exists and any custom configuration is retained.
Drive Client	Drive should use the same date and time format as the server	Issue: An administrator can configure how times and dates are formatted on the server using the *Admin Portal*. These settings are used in the web-based *User Portal*, but are not used when a user views the *Activities* logs in the *Drive* client. Resolution: *Drive 1* and *Drive 2* have been modified so that the times and dates shown in the *Activities* logs use the formats as set in the FileCloud *Admin Portal*. ➡ Users can read more about Viewing FileCloud Drive Activity
Drive Client	Using Drive with SSO causes Search to fail	Issue: When a user opens Drive and logins in with Single Sign-On (SSO) credentials, the Drive user can go to the *System Tray*, right-click on the Drive icon, and select *Search*. When they click the Search option, Drive crashes. Resolution: The Drive client has been modified so that when the user selects the Search option, the Search box displays and Drive does not crash. ➡ Users can read more about Desktop Search Support
Drive Client	File or folder names containing a special character cannot be located	Issue: If a Drive user tries to browse to a file or folder that uses a special character in the name, the users sees an error message that the location cannot be found. 💡 File names cannot contain: ..\/:*?"<>| . , Resolution: Drive now alerts the user that files and folders using special characters in the names are not allowed.
Drive Client	Mounting Drive exposes it as a shared drive to entire network neighborhood	Issue: If a user is working in a network neighborhood with multiple other Windows computers, mounting Drive on one computer shows Drive as a network share to the other computers in network neighborhood. Resolution: Drive now allows a user to mount their share in a network neighborhood without exposing Drive as a network share to the other computers.
Drive2 Client	Network Folders with special characters or foreign-modifying characters not listed	Issue: If a Drive2 user browses Network Folders, any file or folder that uses a special character in the name, such as die Löwen or üben, is not listed. Resolution: Drive2 now displays Network files and folders using special characters in the names.
Drive2 Client	Logging in with SSO and renaming a file causes a crash	Issue: If a Drive2 user logs in with SSO credentials, browses to a file, and tries to rename it, the application will exit without any changes being made. Resolution: Drive2 now allows a user to rename a file without exiting the application when the user logs in with SSO credentials.
Drive Client (Mac Drive2)	File or folder name with special character disappears in Mac Drive 2, but exist on the server	Issue: If a Drive user on a Mac OS renames a file or folder and uses a special character, the name change is updated in the User Portal but the renamed file or folder will not be visible in the Mac Drive file browser. 💡 File names cannot contain: ..\/:*?"<>|" Resolution: Mac Drive 2 has been modified so that files and folders using special names will always appear in the file browser. ➡ Users can read more about Troubleshooting Drive Issues
Drive Client (Mac OS)	If FUSE is not installed, when a user opens MacDrive the error message is incomplete	Issue: If a MacDrive user uninstalls the required FUSE component, when the user tries to open MacDrive, they are shown an error message that "*blank* mount failed." Resolution: MacDrive have been modified so that if a user uninstalls the required FUSE component, when the user tries to open MacDrive, they are shown an error message telling them that FUSE must be installed in order to use MacDrive. ➡ Users can read more about How to install FileCloud MacDrive
FileCloud Helper Service	Helper has problems skipping folders	Issue: FileCloud Server may return exceptions instead of skipping folders during real-time indexing of Network folders for the specific paths. Resolution: Support for real-time indexing of Network folders has been added so that you can identify specific paths to skip. These paths will be matched as regexes (regular expressions) when indexing data. You must edit the realtimeconfig.ini and add a skipregex=REGEX line with regex expressions to the files or folders you want to skip. ➡ Administrators can read more about how to Exclude Folder Paths from Indexing

FileCloud Helper Service	Folder and File changes not updated	Issue: In FileCloud Server, when a network folder is set up for real-time sync, a file that has been indexed by Helper will always remain a file even if it has been changed to a folder and re-indexed. The same behavior occurs for folders changed to files. For example, in a network folder called World, there is a file called hello (no extensions). The World folder and the Hello file are indexed using Helper. After the administrator changes the hello file to a folder called hello and re-indexes the folder, when a Sync user tries synchronizing the hello folder, the user will encounter file errors and is unable to download the folder. Resolution: FileCloud's Helper tool has been modified so that when a network folder is set up for real-time sync, any file or folder that has been indexed by Helper and then changed will retain its new identity. This also allows a Sync user to synchronize the file and folders, and download them without encountering errors.
File Locking	Trying to access a locked file does not tell you who locked it	Issue: When a user opens the Drive or Sync client application, browses to a file and opens it for editing, if the file is locked, then the user will a message telling them that, but not who locked the file. Resolution: The Sync and Drive clients have been modified so that when a user browses to a file and opens it for editing, if the file is locked, then the user will a message telling them that it is locked and who locked the file. ➡ Users can read more about File Locking
File Management	Open files are unusable on upload	Issue: If a user is working on a file locally, and without closing the file tries to upload it, the file will be uploaded but unreadable. Resolution: FileCloud has been modified so that if a user is working on a file locally, and without closing the file tries to upload it, the file will be uploaded and readable. ➡ Users can read more about Uploading Items
File Management	Moving folders and files into a parent folder are blocked if any shared sub-folder is locked	Issue: For example, if Amy creates the following set of folders: AmyReports/Accounting/Receivables/2018. Then Amy shares her Accounting folder with Joe. If Joe locks the shared Accounting folder, then Amy cannot move an existing folder and it's contents into her AmyReports folder. She also cannot move any files into her AmyReports folder. Amy should be able to move files into this parent folder. Resolution: FileCloud Server has been modified so that if a sub-folder is locked, folders and files can still be moved into the parent folder. ➡ Users can read about Sharing Folders
File Management	On the Metadata panel, the creation date is not displayed correctly	Issue: For a file or folder, a user can view the Metadata Panel on the right-hand side of the dashboard, next to the Details and Activity panels. The Metadata panel will only appear when both the Activity and Metadata panel are enabled by an administrator. When a user opens a browser and logs in to the User Portal and views the metadata for a file or folder, the Creation Date is displayed as the current date instead of the date it was actually created. Resolution: FileCloud Server has been modified so that the Metadata Panel displays the correct Creation Date. ➡ Users can read more about Viewing Metadata
File Management	Metadata only captures 10 attributes	Issue: For a file or folder, a user can view the Metadata Panel on the right-hand side of the dashboard, next to the Details and Activity panels. The Metadata panel will only appear when both the Activity and Metadata panel are enabled by an administrator. If a file or folder contains 10 attributes and a user tries to add another, the attribute will not be added or saved. Resolution: FileCloud Server has been modified so that the Metadata Panel allows a user to add more than 10 metadata attributes. ➡ Users can read more about Adding Metadata
File Management	Copying a file or folder with existing metadata applies a new set of metadata	Issue: For a file or folder, a user can view and set metadata in the Metadata Panel on the right-hand side of the dashboard. If the user then copies that file or folder with existing metadata, after it is copied, a new set of metadata is applied instead of copying the existing metadata. Resolution: FileCloud Server has been modified so that when a user copies a file or folder with existing metadata, after it is copied, the existing metadata is copied also. ➡ Users can read more about Adding Metadata
File Management	Team Folder copy issue not showing error	Issue: When an administrator opens a browser and logs in to the Admin Portal, clicks Manage and then Team Folders, the administrator can view the folder structure. If Team Folders includes sub-folders, and the administrator tries to move a sub folder to the root directory where Team Folders exists, then FileCloud may encounter errors and never move the folder or notify the administrator. For example, if the Team Folders structure is: Team Folders/Team1/Team1_Reports, and the administrator tries to move Team1_Reports into the root directory containing Team Folders, then the Admin Portal will become unresponsive without completing the folder move. Resolution: FileCloud Server has been modified so that when an administrator tries to move a sub-folder to the root directory containing Team Folders, an error will inform the administrator that the move is not allowed. ➡ Administrators can read more about Team Folders
File Management	Permissions and locking in a folder structure not working as expected	Issue: In a folder structure where there are some folders that are shared and some that are locked, behavior is inconsistent with the permissions set. For example, 1. Amy creates the following set of folders with a file in the last sub-folder: AmyReports/Accounting/Receivables/MiningCorp.DOCX. 2. Then Amy shares her Accounting folder with Joe gives him write and delete permissions. 3. Then Amy locks the Receivables sub-folder. 4. Joe tries to remove the shared Accounting folder and is successful. This should not be allowed because Amy has locked the sub-folder Receivables. Also, in some cases the parent folder, AmyReports, can be deleted by Joe even though that folder has not been shared with him. Resolution: FileCloud Server has been modified so that if a folder structure permissions work as expected when some folders are locked and shared. ➡ Users can read about Private Share Permissions for Folders
File Management	Unable to download temporary files to Drive	Issue: When a Drive user opens a web browser and logs in to the User Portal, they can download files into a local Drive folder. If the file being downloaded is temporary file (.part, .partial, .crdownload), then FileCloud fails to download the file. Resolution: The FileCloud User Portal has been modified so any temporary files are handled and all files selected to be downloaded complete successfully.

| File Management | Automatically Empty Recycle Bin After Specified Days unexpected behavior | Issue: To configure the recycle bin settings, an administrator opens a browser and logs in to the *Admin Portal*. On the left navigation panel, under *Settings*, the administrator clicks on *Settings*, the *Storage* tab, and then in *Automatically Empty Recycle Bin After Specified Days*, the administrator types in 30 days. However, when a user deletes a file on the 29th day and it is placed in the recycle bin, this file is also deleted the next day, instead of being retained for 30 days from the date of deletion.

Resolution: When a user deletes a file, it is retained for the correct number of days as configured by the administrator.

➡️ Administrators can read more about [Setting Up Managed Disk Storage](#) |
|---|---|---|
| File Management | When a single folder has very large number of files, it cannot be deleted from the recycle bin | Issue: If you have a folder with a large number of files, more than 16 MB, and you delete this folder, it is moved to recycle bin. When they try to delete the folder or empty recycle bin, the request will fail.

Resolution: A new utility has been added to help an administrator empty the recycle bin when it contains a large folder that won't delete.

- The utility is at WWWROOT/fileutils/rmutil.php
- ⚠️ This tool can be used not only for emptying recycle bin, but also any folder path. Please use it with caution.
- Usage:
  [Required] -h <host> Site host name or 'default' for default site
  [Required] -u user account whose files are being removed from the recycle bin
  [Required] -p path to the user's recycle bin which you want to delete
  [Optional] -r remove files in the destination (For a test run, do not specify this option.)

To run the utility:

1. **Open a command line prompt.**
2. **Use the following code to navigate to the directory containing the utility**

```
C:\xampp\htdocs\resources\tools\fileutils
```

3. **Use the following command to delete files and folders under the path /user1/recyclebin/ (replace the smple parameters with your own data)**

```
C:\xampp\php\php.exe rmutil.php -h default -u jdoe -p /jdoe/recyclebin/ -r
``` |
| File Sharing | Upload file size limit can be set to a negative value | Issue: When a user shares a folder in the User Portal, they can set an *Upload Size Limit* in MB to be a negative number, such as -23 MB.

Resolution: The *Upload Size Limit* field has been changed to allow only whole interger values.

- The smallest possible upload limit is 1 MB
- If a negative number is typed in, it will be replaced with 0, disabling the *Upload Size Limit* functionality

➡️ Users can read more about [Sharing Folders](#) |
| File Sharing | Admin disables locking system-wide but locks still show up | Issue: After an Admin logs on to *Admin Portal*, from the left navigation pane, they can click *Settings*, then the *Misc.* tab, and then the *General* sub-tab. Under *General System Settings*, the admin can select the checkbox next to *Disable Locking* to remove the option from the User Portal so that no FileCloud user can set a lock on a file or folder. However, after checking the *Disable* option, the lock information continues to be displayed in the User Portal.

Resolution: FileCloud Server has been modified to remove all lock information when the *Disable* option is selected. This means that files will have to be locked again after Locking is enabled again.

➡️ Administrators can read more about [Managing User Locks](#) |
| File Sharing | Export of the shared items list does not work when the Filter contains text | Issue: When an administrator opens a browser and logs on to the *Admin Portal*, from the left navigation panel they can click *User Shares*. If the admin types anything into the *Filter* text box, and then clicks *Export*, nothing happens.

Resolution: The FileCloud *Admin Portal* has been modified so that on the *User Shares* screen, when text is typed into the *Filter* text box, only those relevant records will be exported. If nothing is typed into the *Filter* text box, then all records are exported.

➡️ Administrators can read more about [Managing User Shares](#) |
| File Sharing | Unable to share parent team folder directly to users | Issue: Team folders have the ability to be shared again by members and you can also designate another user to manage those re-shares of your original shared file. To do this, an administrator opens a browser and logs in to the Admin Portal. From the left navigation panel, the administrator clicks Team Folders, and then for the Team Folder that needs to be shares, the Manage button is clicked. On the Configure the share settings window, in the Share Permissions panel, add the user or groups you want to give sharing permissions, and then select the following level of permissions: Allow View, Allow Download, Allow Upload, Allow Share. The administrator must also, in the Misc. section, select the edit icon and then select Allow Manage. However, when this procedure is followed for Team Folders, the permission is not available to the user even though it has been granted by the administrator.

Resolution: FileCloud Server has been modified to grant the share permissions to the user for a Team Folder once the permission are set by the administrator.

➡️ Administrators can read more about how to [Share the Team Folder and Set Permissions](#) |
| File Sharing | Full path to shared items leaked | Issue: For example, if Amy creates a new folder called TaxForms in the path AmyReports/Accounting/Receivables/2018, then the full path is AmyReports/Accounting/Receivables/2018/TaxForms. When Amy shares the TaxForms folder with Joe, when Joe tries to perform actions such as copy, move, delete, lock, or rename, any messages Joe receives about these actions contains the full original path, AmyReports/Accounting/Receivables/2018/TaxForms and thereby leaks information to the shared user.

Resolution: FileCloud Server has been modified so that when a folder is shared, the original path is not displayed to the user(s) it is shared with.

➡️ Users can read more about how to [Share a Folder Privately](#) |

File Sharing	Sharing with a newly invited FileCloud user provides an incorrect share URL	Issue: When the *Drive* or *Sync* user opens the *User Portal*, and right-clicks on any file and selects *Share FileCloud Link*, they can invite a user without a FileCloud account to create one and access the shared file. In the email window that opens displaying the *Share URL*, the localhost is shown instead of the configured Server URL, and the user receiving the invite cannot access the shared file. Resolution: FileCloud Sync has been modified so the URL to the shared file is correct. ➡ Users can read more about Managing Files in Sync's File Explorer
File Sharing	Share Name not updated in Sync and Drive Clients	Issue: When a *Sync* or *Drive* user goes to the *System Tray*, right-clicks on the FileCloud icon, and selects *File Browser*, they can find a file to share. For new shares, when they right-click on the file and select *Share FileCloud Link*, they can click *Advanced* to change the name of the share, which is randomly generated by default. However, when the user clicks *Update*, the *Share Name* reverts back to the randomly-generated original name. This also occurs when a file is already shared, and the user accesses the Advanced Sharing dialog. Resolution: FileCloud *Sync* and *Drive* clients have been modified to save the *Share Name* set by the user. ➡ Users can read more about Sharing Files and Folders
File Sharing	Manage re-shares is not working as expected	Issue: A user can open a browser and log in to the User Portal, click on a folder, and share it. If the folder owner also gives permission to another user to manage the share by selecting *Allow Manage*, the user who is given this permission should be able to remove permissions and users from the share but is not able to. Resolution: For a shared folder, a user who is given the *Allow Manage* permission is able to remove permissions and users from the share. ➡ Users can read more about how to Allow Members to Manage Re-Shares
File Sharing	Root user folder should not be shared	Issue: 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. Resolution: FileCloud Server has been modified so that in the User Portal, when a user clicks on the root folder, My Files, they do not have the Sharing option.
File Sharing	FileCloud fails to create a direct link to Network folders	Issue: When a user in the User Portal, in Sync, or in Drive right-clicks on a Network folder and selects the option to Create a Direct FileCloud Link, FileCloud returns the following error message: "Failed. Direct Link can be created only for private shared folders." Resolution: FileCloud Server has been modified so that when a user right-clicks on a Network folder and selects the option to Create a Direct FileCloud Link it is created successfully.
File Sharing	Show warning when root folder is shared	Issue: When a user opens a browser and logs in to the User Portal, on the Home dashboard that is shown by default the user sees a list of the files they have access to, including the root folder (My Files). If the user shares the root folder, the User Portal does not show them a warning or any indication that the root level user folder is being shared. Resolution: FileCloud Server has been modified so that the user can see if the root folder is being shared and the user will also see a warning if the root folder is not being shared yet and the user shares it.
File Sharing	Share permission for a single file different between User Portal and Drive	Issue: When a user opens a browser and logs in to the User Portal, they can share a file or folder with the following 3 permission options: • View • Download • Share When a user opens the Drive client application, they can share a file or folder with the following 5 permission options: • View • Download • Sync • Write • Share This discrepancy causes issues when a file or folder has been shared from Drive with permissions that are not available to view or update on the User Portal. Resolution: The Drive client application has been modified to use the same three permissions that are set in the User Portal: View, Download, and Share.
Log Files	When a large file is uploaded, server log files are not being updated	Issue: When a user logs in to the User Portal and uploads a large file that is more than 25 MB, and the file does not already exist, the audit logs do not record this event. Resolution: FileCloud Server has been modified to record the upload of files larger than 25 MB in the server audit logs. ➡ Administrators can read more about how to View Audit Logs
Log Files	Improved Scratch Log Management	Issue: Administrators can set the Logging Level to development (DEV) mode for troubleshooting issues. In DEV mode, a comprehensive amount of trace data is generated, so the amount of log files and their size can become large. Setting the Log Level to DEV may also slow down the speed of FileCloud Server responses. Resolution: The server log files in the scratch folder are now automatically compressed into a zip folder. This new auto-archive process is completed by Cron. As soon as a log file is 30 days old, it is compressed and added to the archive. After the file is archived, the original file is deleted to free up space. This archival process happens automatically and does not require you to configure any special settings ➡ Administrators can read more about Debug Log File Locations

Policies	Adding a new user to an existing policy removes the original users	Issue: When an administrator opens a browser and logs in to the Admin Portal, from the left navigation panel, under USERS/GROUPS they can select Users, and then on the Manage Users screen, click a user and then the Manage User Policy (⚙) button. If the administrator adds this user to an existing policy, all original policy members will be removed from the policy and this newly added user will be the only member in the policy. For example, an administrator clicks SETTINGS from the left navigation panel, then clicks Settings, and then on the Policies tab. On the Manage Policies screen, the administrator creates a User Policy called LargestSQ and sets the User Storage Quota to 50 MB. Only users who are members in this policy have this amount of storage. After saving this policy, the administrator clicks the Manage Policy Users (👤) button, and adds only 3 employees: AmyR, JosephC, and SamS. Later, the administrator needs to add one more user, MichaelJ to the LargestSQ policy. If the administrator opens a browser, logs in to the Admin Portal, under USERS/GROUPS selects Users, and then on the Manage Users screen, clicks MichaelJ and then the Manage User Policy (⚙) button, the admin can add MichaelJ to the LargestSQ policy. However, AmyR, JosephC, and SamS are removed from the policy. MichaelJ will be the only member in the LargestSQ policy. Resolution: FileCloud Server has been modified so that when a user is added to an existing policy through the Manage Users screen, any other users who were already members of the policy are not removed.
Secure Sockets Layer	Private key corrupted when CSR is generated through FileCloud Control Panel (Windows)	Issue: To use SSL, an administrator creates a CSR and private key in the FileCloud Control Panel. With these, the administrator uses a third-party to create a Certificate. When the certificate is installed using the FileCloud Control Panel, the Apache server will not start up because the certificate is not accepted. Resolution: FileCloud Server has been modified to accept the SSL certificate when installed by the FileCloud Control Panel. ➡ Administrators can read more about how to Install a certificate using the FileCloud Control Panel
ServerSync	In some cases NTFS permissions are not retained	Issue: In Server Sync an administrator can set NTFS permissions on a parent folder, like adding an extra user account. When new files are added on the remote FileCloud server and then downloaded to a local folder, the newly added files do not have the correct parent permissions that were previously set. Resolution: Server Sync has been modified so that any NTFS permissions are correctly retained. ➡ Administrators can read more about FileCloud Server Sync
ServerSync	'Save Log File' does not work	Issue: When an administrator wants to check the logs, from the system tray icon they can right-click ServerSync, and then select Settings. On the Home screen, they can click Help to see the "Save Log File" option. However, after selecting a file name and location and clicking Save, a message says the file is saved but when the administrator browses to the folder location it's not there. If the administrator goes to Recent Documents the file is displayed but it is empty. Resolution: ServerSync has been modified so that when the administrator wants to save the logs to a file, clicking on 'Save Log File' creates the file. ➡ Administrators can read more about Troubleshooting ServerSync
ServerSync	Detect condition when disk is unavailable	Issue: If the top level local folder is missing due to the network being unavailable, ServerSync deletes the local copy. When the top level folder does become available, synchronization will remove the top level folder on the remote server as well. Resolution: ServerSync has been modified so that if a top level local folder is missing due to the network being unavailable, ServerSync will not delete any files.
ServerSync	ServerSync service and windows gui running together	Issue: If the ServerSync regular non-service application (Windows GUI) is running, the service can also run at the same time and they can get in the way of each other's operations. Resolution: If the ServerSync regular non-service application (Windows GUI) is running, the service won't also run at the same time. To run the service, the user must first exit the ServerSync Windows application.

ServerSync	Folder Change approval dialog doesn't provide enough details	Issue: In ServerSync, when the percentage of changes to folders exceeds 10%, a dialog pops up asking the administrator for approval. The 10% is a default number and can be changed through the config file.
		
		• If Yes is clicked: all the changes made locally are pushed to the server
		• If No is clicked: all the folder sets that were present are completely removed. The user has to then manually add all of them back. There are also no details in that pop-up as to which folders were changed locally.
		
		Resolution: ServerSync has been modified so that the pop-up dialog now lists the folders which have been modified. Now there are now 2 checkboxes for each folder - Sync and Revert.
		
		• Sync synchronizes all changes to the server
		• Revert resets only that specific folder. This means:
		  • If a file is deleted locally, it will be copied to the local destination again from the server
		  • If a file is modified, a conflict file appears and administrator must select the server version so that server version can be copied

ServerSync	Previous versions not displayed and options not available	Issue: In ServerSync, the different versions of a file are not displayed and users can not download, delete, or make live a particular version. Resolution: The ServerSync application has been modified to provide options in the File Browser to see the previous versions and download, delete or make a file live are available by right-clicking on the file and then selecting Properties and then Versions.
ServerSync	Errors do not provide a numerical error code	Issue: In ServerSync, when a user encounters an error, the error message does not include a numerical code for easier troubleshooting. Resolution: The ServerSync application has been modified to provide a numerical code when a user encounters an error.

Sharing	Share URL rename option is missing in the client applications Sync and Drive	Issue: Filecloud automatically generates a unique and difficult-to-guess short link to shared files and folder. Users can edit the short link to be more recognizable. This option is available when the user opens a browser and logs in to the User Portal. On the Home dashboard, they can click My Files, select the shared file to update, and then click Manage Share. On the Manage Share dialog box, at the top, there is a button that can be clicked to customize the share link. This option is not available in the Drive and Sync client applications. Resolution: FileCloud client applications, Drive and Sync, have been modified to include the option to customize the share URL link from the Advanced Share dialog.
Sync & Drive	Error in .DMG scripts causes installation to fail	Issue: When using Bash scripting to download the Sync and Drive clients from Filecloud Server to mount the DMG files and copy the .app file to applications folder, the clients do not install properly and warn the user that the applications are incomplete or damaged. Resolution: The DMG scripts have been modified to allow users to download Sync and Drive installation files, copy them to the Applications folder, and successfully install Sync and Drive.
Sync (Mac OS)	In the Mac OS, the Sync Settings screen is opening in the background	Issue: For Mac users, when opening the Settings window, it always open in the background. This can confuse users because they click and it appears as if nothing happens, although the window does open in the background. This issue is seen with other windows besides Settings. Resolution: The Sync client has been modified so that the opening and closing of windows does not occur in the background. Now the Sync client windows appear in front of other open windows. Users can read more about Sync Settings
Sync Client (Mac OS)	In the Mac OS, file browser and Settings windows have issues	Issue: When a user is working in the File Browser and also has the Settings window open, if the user closes the File Browser, the Settings window will also close. Also, sometimes if a user opens the File Browser and then later clicks Settings from the menu, it will show the File Browser in front of the Settings window. Resolution: The Sync client has been modified so that if both the File Browser and Settings windows are open, closing one will not close the other. Sync has also been modified so that the Settings window behaves as expected. Users can read more about Using the Sync Client
Sync Client (Mac OS)	The dock icons stays after the file browser is closed	Issue: When a Sync user on a Mac OS opens the File Browser, a dock icon is shown. However, this icon remains even after the user closes the File Browser. Resolution: The Sync client has been modified so that the dock icon never appears to a Sync user. Users can read more about Browsing Sync Files
Sync Client (Mac OS)	Duplicate instances should not be allowed	Issue: After installing FileCloud Sync on Mac, a user can open a duplicate instance on Terminal using the Open command. Using this command allows a duplicate instance to run. Resolution: The Sync client for Mac OS users has been modified to not allows a duplicate instance to be started from the Open command and the user is warned that Sync is already running. Users can read more about how to Start and Log In to Sync
Sync Client	Special characters not displayed correctly in the Properties tab	Issue: After opening the Sync client and logging in to FileCloud, Sync users can open the File Browser and right-click on a file to see the properties. If the file name contains special characters, they may appear differently in the Properties tab than they do in the File Browser. Resolution: The Sync client has been modified so that the name of the file appears the same in the Properties tab as it does in the File Browser. Users can read more about Managing Files in File Explorer
Sync Client	Users can't see the overlay icons in the local Sync folder	Issue: In the Sync folder, the icons indicating the status of files and folders are not visible. The only way to make them visible was to **manually change the registry entries** related to icons overlay by adding spaces to the beginning of the entries. Resolution: The registry entries related to icons overlay have been updated so that icon overlays are automatically seen and no manual changes need to be made by users. Administrators can read more about FileCloud Sync Icon Overlays
Sync Client	Sync overlay icons are low resolution and difficult to enlarge to see	Issue: The Sync overlay icons appear with a jagged boundary and blurry effect when the extra large icons view is selected. Resolution: The Sync client has been modified so that overlay icons displays without jagged boundaries and blurriness even when the extra large icons view is selected. Administrators can read more about FileCloud Sync Icon Overlays
Sync Client	User sees errors when using email address as login name	Issue: Users will see errors when logging in to FileCloud Server from the Sync client if: • Two-Factor Authentication (2FA) is enabled • The user types in their address for the User Account name Resolution: FileCloud Sync has been updated to log users in correctly when 2FA is enabled and a user's email address is used for login credentials. Administrators can read more about Two Factor Authentication

Sync Client	Displays of the schedule for when Bandwidth Rate Limits are in effect show inconsistent behavior	Issue: Users can limit the max amount of bandwidth that Sync can use to reduce the impact on your network and day to day operations. When setting bandwidth limits, users can set a limit that is enforced only during a specific interval of time. When setting time intervals, users may see the following inconsistent behavior: • **On the Mac Sync client**: when the time is saved as PM, for example 10 PM, after re-opening the dialog, the time is displayed in AM, for example as 10 AM. • **On the Windows Sync client**: the day of the week shows up incorrectly sometimes Resolution: The Mac and Windows Sync clients have been modified to show the day and times correctly when the user sets the schedule for *Bandwidth Rate Limits*. ➡ Users can read more about how to **Limit Sync Bandwidth Rates**
Sync Client	Changing http to https resets the sync app	Issue: In Sync and ServerSync, you can change the URL from *http* to a secured protocol of *https*. This action resets the Sync app as if the server URL is different. Resolution: The Sync and ServerSync apps have been modified so that changing the same URL to the FileCloud Server from *http* to *https* does not reset the application. ➡ Users can read more about how to **Start and Log In to Sync**
Sync Client	Adding a selective sync backup path already set on the server does not create the backup or warn the user	Issue: When a user selects a backup path (that an administrator has already configured) for Selective Sync, it does not sync that folder or warn the user. For example: The administrator sets the backup folder for the FileCloud user Joe Carpenter: 1. The administrator logs in to the FileCloud Admin portal, selects *Users*, and in the *Manage Users* section, selects Joe Carpenter. 2. The administrator clicks the *Edit User* icon, and in *Backup Path*, the admin types in the folder path where all of Joe's files will be kept, */Accounting/JoeCarpenter/Ledgers*. On the user side, Joe Carpenter tries to setup a Selective Sync folder: 1. Joe opens *Sync,* and on the *Home* screen clicks *Settings*. 2. In the *Selective Sync* section, Joe clicks *Edit*. 3. On the *Selective Sync* tab, Joe clicks *Add Folder*. 4. Joe selects */Accounting/JoeCarpenter/Ledgers* 5. Joe clicks *Save* but no syncing happens for that folder. Resolution: Sync has been modified so that the user is warned that the backup location is already configured in the server backup folder path and that the user cannot add that path for Selective syncing.
Sync Client	Download to Sync folder option in File Browser is not working	Issue: When a user opens the Sync *File Browser*, finds a file/folder to download (that has not been synchronized before), right-clicks and chooses *Download to Sync Folder,* Sync does not create the folder or download the files. Resolution: The Sync client application has been modified to create a new folder in the File Browser (if it does not already exist) when a user wants to download a file/folder. ➡ Users can read more about **Managing Files In Sync's File Browser**
Sync Client	Downloading a large number of files to Sync causes delays	Issue: If the Sync application is configured to have *Network* folders or *Backup* folders with millions of files, then when the Sync user goes to the System Tray to use the right-click menu, there is a delay. Resolution: The Sync client has been modified so that even when Sync is configured with a large number of *Network* or *Backup* folders, there is no delay when trying to access the right-click menu. ➡ Users can read more about **Managing Files in Sync**
Sync Client	Cannot download folder from the File Browser	Issue: When a Sync user opens the *File Browser*, right-clicks a folder and selects *View in FileCloud* site, they can check the folder contents on the server. To download all of the files in this folder, the user can right-click the folder and then chooses the *Download* option. When this action is performed, the folder is created locally but the folder contents are not downloaded. Resolution: The Sync client has been modified so that all folder contents are downloaded. ➡ Users can read more about **Downloading Items from the FileCloud Site**
Sync Client	Option links change colors used when although the link is not a URL	Issue: When a *Sync* user clicks on an option such as *Open Folder*, *Open Website*, or *File Browser*, the text changes color when clicked, as if they are browser URLs when they are not. Resolution: The Sync client has been modified so the options do not change color after being clicked.
Sync Client	Files shown in incorrect order	Issue: When a *Sync* client opens the *Search* dialog to search for files, the results are listed by date, but in ascending order instead of descending order. Resolution: The *Sync* client has been modified so that files in the *Search* results are listed by date in descending order.
Sync Client	An unlimited storage quota shows as 0MB available	Issue: When a *Sync* user goes to the *System Tray* and right-clicks the FileCloud icon, they can select *Settings*. This option opens a window which shows, by default, the *Home* screen. On the *Home* screen the user can see how much of their storage quota is available. If an administrator has set the storage quota to *unlimited* on the server, Sync will show *0 MB* available in error. This same issue is also seen in ServerSync. Resolution: The *Sync* and *ServerSync* applications have been modified to show an unlimited storage quota as *Unlimited Storage*.
Sync Client	Recent log panel in Sync Settings entries show a downloads completes and then fails	Issue: When a *Sync* user views their files on the *User Portal*, they can share and edit a file or folder. If the file or folder cannot be downloaded during synchronization, such as a locked file with read not allowed permissions, then in the *Sync* application, on the *Home* screen in the *Recent Log*, it will show the file as being downloaded, completed and then failed. This behavior also occurs in *ServerSync*. Resolution: The Sync and ServerSync applications have been modified so that in the log entries, *Completed* is only displayed when an item is successfully downloaded or uploaded. If the item could not be synchronized, the user will see a message that *Upload failed* or *Download failed* along with the file or folder name.

Sync Client	When MyFiles is disabled, the Move to FileCloud option still displays	**Issue:** When an administrator disables *MyFiles* in the *Admin Portal*, whenever a *Sync* user right-clicks on a file or folder that is outside of FileCloud, they can select the *Move to FileCloud* option although nothing will happen. **Resolution:** When an administrator disables *MyFiles* in the *Admin Portal*, if a *Sync* user right-clicks on a file or folder that is outside of FileCloud, they will not have the *Move to FileCloud* option. ➡ Administrators can read about [Disabling Managed Storage](#)
Sync Client	Recent Logs does not display delete related information	**Issue:** When a file on the server is deleted, in the Sync client, the *Recent Log* activity doesn't display the path information. **Resolution:** The *Recent Logs* activity has been modified to now show: • Deleted Remote File Object : <file/folder name> - when the file or folder is deleted remotely • Deleted Local File Object: <file/folder name> - when locally synced file/folder is deleted
Sync Client	Users cannot modify selective sync, network and backup folders	**Issue:** Users are prevented from adding or changing the following folders: selective sync folders, network folders and backup folders when RMC (Centralized Device Configuration) is set up by the administrator. **Resolution:** The Sync client has been modified so that users can modify the selective sync folders, network folders and backup folders when allowed by remote management XML policies. The administrator must set the XML attribute for the folder-type they want Sync users to modify by using the following attributes: *allowuserconfigforbackup*, *allowuserconfigfornwfolders*, *allowuserconfigforlimitsync*. ➡ Administrators can read more about [Device Configuration XML for Sync](#)
Sync Client	Sync notifications for failed backup not being sent	**Issue:** FileCloud Sync backup notifications work only when when the backup is successful. When a backup fails, no notification is sent. Also, any notifications that do get sent are sent only to the Sync user and not to the administrator. **Resolution:** FileCloud Sync and FileCloud Server have been modified so that if a backup fails, notification is sent to the Sync user and the FileCloud administrator. Also, all Sync notifications are now sent to both the Sync user and the FileCloud administrator.
Sync Client	Errors shown when custom logo is used without a profile	**Issue:** When administrators use their own PNG files on the server to customize the logo, if the PNG file doesn't have a profile, then Sync users will see an error when the image is rendered for display. **Resolution:** The errors caused by the use of a custom PNG file without a profile are no longer displayed.
Sync Client	Image less than 200x50 set as logo is stretched	**Issue:** An administrator can select an image to use as a custom logo on FileCloud Server. If the image size is less than 200x50, it will appear as expected in the Admin and User portals, but it will appear stretched in the Sync client application. **Resolution:** The FileCloud Sync client application has been modified to display any custom images the same way they appear in the Admin and User portals.
Sync Client	During file transfer, if Network folder is added, Sync becomes unresponsive	**Issue:** When Sync is uploading or downloading files, if a new network folder is added, Sync will become unresponsive and will stop uploading or downloading files. **Resolution:** The FileCloud Sync client application has been modified to continue uploading and downloading files if a real-time or non-realtime network folder is added during transfer.
Sync Client	Every locked shared folder that cannot be synchronized displays a notification	**Issue:** When a shared folder with sync permission is locked, a notification displays for every failed download. So if there are 100 files that cannot be synchronized, Sync displays 100 notifications to the user. **Resolution:** The FileCloud Sync client application has been modified to display a failure notification ONLY once every sync cycle. The failure message now informs users: *Failed to download file(s); check the Activity Log for details.*
Sync Client	File or folder names containing a special character cannot be located	**Issue:** If a Sync user tries to browse to a file or folder that uses a special character in the name, the users sees an error message that the location cannot be found. 💡 File names cannot contain: ..\/:*?"<>| . , **Resolution:** Sync now alerts the user that files and folders using special characters in the names are not allowed.
Sync Client	When a large number of remote files are being deleted, the status shows as Idle	**Issue:** After a Sync user deletes a large number of files that were in their *Sync* folder, when the user goes to the System Tray and right-clicks on the FileCloud Sync icon, they can choose Show Syncing Status to see if all the files have been deleted. However, the status only shows *Idle*. **Resolution:** The FileCloud Sync client application has been modified to show the progress of the deletion, such as showing the name of the file that is currently being deleted.
Sync Client	Sync file mismatch error leaves part files in folder	**Issue:** File mismatch errors need to delete .part files that are left over in the sync folder when a file cannot be downloaded. **Resolution:** The FileCloud Sync client application has been modified so that it will not leave part files in the folder if file download fails.
S3 Storage	Temporary files are not cleaned up	**Issue:** In High Availability (HA) installations such as S3 Amazon Storage, a key can be used to override the location of a common temporary folder. For example: <table><tr><th>KEY</th><th>VALUE</th><th>DESCRIPTION</th></tr><tr><td>TONIDOCLOUD_NODE_COMMON_TEMP_FOLDER</td><td>"/somepath/location"</td><td>In HA installs, the temp folder must be in a commonly accessible location. This key must be set in each of the HA nodes.</td></tr></table> This key is not typically used however it may be needed in specific circumstances. After this key is set, any old files placed in this folder should be removed but are not. **Resolution:** FileCloud Server has been modified so that the old files are removed after waiting for 24 hours or deleting the global run in global keystores. ➡ Administrators can read more about [Setting Up Managed S3 Storage](#)

S3 Storage	Creating a new network share creates multiple shares	Issue: Administrators can integrate Amazon's AWS S3 buckets with FileCloud Server to allow users access to this data inside FileCloud Server portals and clients. To do this, an administrator opens a browser and logs in to the *Admin Portal*. On the left navigation panel, the administrator can select *Network Folders*, and on the *Manage Network Folders* window, clicks *Add*. After specifying all the required information and clicking *Finish*, in the *Manage Network Folders* window, the administrator will see the new network share was created multiple times. Resolution: FileCloud Server was modified so that after an administrator adds an S3 network share, in the *Manage Network Folders* window, the administrator will see the new network share was created only once. ➡ Administrators can read more about Creating a Network Folder Based on an Amazon S3 Bucket
Team Folders	Users not given explicit permission to manage Team Folders inherit it	Issue: When an administrator opens a browser and logs in to the *Admin Portal*, they can share a folder inside *Team Folders*. In the following case, a user inherits a permission they are not explicitly granted: 1. An administrator privately shares a folder in *Team Folders* called Accounts Receivable with a AmyR and grants all permissions <u>except</u> *Allow Manage*. 2. AmyR logs in to the *User Portal*, navigates to *Team Folders*, and then the Accounts Receivable folder. She notices that she can read and write to the folder but doesn't have any right to manage it. 3. The administrator, in the *Admin Portal*, now shares the Accounts Receivable Team Folder with JosephC and grants all permissions <u>including</u> *Allow Manage*. 4. AmyR logs back in to the *User Portal*, navigates to *Team Folders*, and then the Accounts Receivable folder. She notices that now she has rights to manage the Accounts Receivable Team Folder. The expected behavior is that only JosephC can manage the Accounts Receivable Team Folder. Resolution: FileCloud Server has been modified so that only the user given explicit right to *Allow Manage* for a Team Folder actually has that permission, and no other users who also have access to the share can manage it.
User Accounts	Account is getting locked after resetting password from AD	Issue: If an administrator changes a user's password on the Active Directory (AD) server, then when that user logs in to FileCloud, the user's account is locked and the user sees the following message: *We have temporarily locked your CloudFiles account because we detected unsuccessful login attempts from this account. The last unsuccessful login was attempted from Cloud Sync. Your account will be locked for 5 minute(s). Please wait for 5 minute(s) before you attempt to login again. If you have not attempted to login recently and you have received this email, please contact your FileCloud Administrator. However, you can use Forgot Password on the Login Screen to reset your password. We are sorry for the inconvenience, but your security is our top priority.* Resolution: FileCloud Server has been modified so that if a FileCloud user's password is changed in AD, FileCloud recognizes the new AD password as correct and the user's account is not locked. ➡ Administrators can read more about Active Directory Authentication
User Portal	Cannot upload empty folder in the User Portal	Issue: When a user opens a browser and logs in to the User Portal, if the user tries to drag and drop an empty folder from the local computer into FileCloud, it will not upload the folder. Drag and drop only works if there is at least one file in the folder. Resolution: The User Portal has been modified so that when a user opens a browser and logs in to the User Portal, if an empty folder is dragged and dropped from the local computer into FileCloud, it will upload the folder. ➡ Users can read more about Uploading Items
User Portal	Logging in with an incorrect password shows the wrong error message	Issue: When a user opens a browser and tries to log in to the *User Portal* with an incorrect password, they are shown an error stating that they have *Failed to Log Back into the System* instead of an error that the password does not match the user account specified. Resolution: The *User Portal* has been modified so that when a user opens a browser and logs in to the User Portal, if they provide an incorrect password they are shown an error message telling them that the password is not correct.
User Portal	Change the default Sharing display from User Name to Display Name	Issue: In the User Portal, by default FileCloud displays the user name. For security reasons, this may not be desired because it exposes the user's account name. • It may not be clear to users who is sharing the file with them, especially if User Name includes only abbreviations and numbers (ie. are generated automatically). • Also, the User Name cannot be changed after the user has been created. Resolution: FileCloud now allows you to set a configuration variable that will make the system use the Display Name on the Details tab and Shared with Me list when showing the share information. ➡ Administrators can read more about how to Secure Shares
User Portal	Using Network Shares with Smart Mount causes Activity to display all users' activity	Issue: When using Network Shares with Smart Mount, when a user opens a browser, logs in to the User Portal, and reviews the right-side panel called Activity, they should see only the actions completed by their user account. Instead, the user can see the actions for all user accounts in the FileCloud system. Resolution: The FileCloud Server User Portal has been modified so that when Network Shares with Smart Mount, a user logged in to the User Portal see only the actions completed by their user account.
User Portal	When a user explicitly locks a file, users trying to preview the file will see an error with no explanation	Issue: When a user opens a browser, logs in to the User Portal, and browses to a file, the user can explicitly lock the file. When this is done, if another user tries to preview the file on the User Portal, the other user only sees a 404 error with no reason as to why it cannot be edited. Resolution: The FileCloud Server User Portal has been modified so that when a file is locked by one user, if the other user attempts to preview it on the User Portal, they see the following message: *<filename> edit is blocked by <user name>*
User Portal	Searching with Results "Limit 50" and "All" sometimes don't work as expected	Issue: When the user opens a browser and logs in to the *User Portal*, they can click on *Search*. In the *Search* window, they can enter a term to search for and then click the down arrow for *Advanced Search* options. In the *Advanced Search* dropdown, the user can set *Results Count* to *Limit 50* or *All*. If the user selects *Limit 50*, searches for a string, and then in *Advanced Search* changes *Results Count* to *All*, only 50 results will still show even though there are more results. Clearing all settings and starting the Search over again will show all results. Resolution: The FileCloud Server User Portal has been modified so that it the user searches and set *Results Count* to *Limit 50 ,* then only 50 results will show, and if the user changes *Results Count* to *All,* then all results will show.

User Portal	SAML login error page needs more details	Issue: When a user opens a browser and logs in to the User Portal, if they click Login with SSO, and an error is encountered, the user is only shown a page with the following information:

```
SAML Curl Request Failed. HTTP code:0.
Curl ERR: [Curl Error no 0]SAML Curl Request Failed.
HTTP code 0. Curl ERR: [Curl Error no 0]
```

This information does not help the user understand what to do next.

Resolution: The FileCloud Server User Portal has been modified so that when login issues occur with SSO on the User Portal, the user sees the following message and understands what to do next:

Single Sign-on Login

Failed to login automatically via SAML Single Sign-on (SSO).
Please return to the main login page and login normally.

The following additional information was returned as well:
SAML Authentication Failed

Go Back to Login

Workflows	After running a workflow, no activity is displayed	Issue: After an administrator opens a browser and logs into the Admin Portal, they can see a list of workflows they have created by clicking on Workflows. On the Manage Workflows screen, there is a column called Last Check. If there is a date in this column, then the workflow has been run and the administrator can see the activity by clicking on the Workflow Activity button. When the Workflow Activity screen opens, the table that should list events is empty even though the workflow has been run.

Resolution: The Workflow Activity screen has been modified to display the events related to a workflow that has been run.

Administrators can read more about Workflows

Workflows	Workflow to delete old files in recycle bin produces errors	Issue: After an administrator creates a new workflow to delete old files in the recycle bin, it shows errors for Invalid Path.

Resolution: FileCloud Server has been modified so that when a workflow needs to delete old files in the recycle bin it will complete without errors.

Administrators can read more about Workflows

Workflows	Workflows that move a file from one folder to another folder encounter errors	Issue: When an administrator sets up a workflow that moves any file added to a folder to another folder, when the workflow is triggered the administrator will see errors and the move is not completed.

Resolution: FileCloud Server has been modified so that when a workflow is created to move files, the workflow completes without errors and the files are moved.

Administrators can read more about Workflows

Workflows	Disabling a workflow does not stop it from running automatically	Issue: When an administrator opens a browser and logs in to the *Admin Portal*, they can create workflows to automate standard operations. However, when the automation is no longer needed, and the administrator goes to the left hand navigation panel, and under *MISC.*, clicks **Workflows** , and clears the *Enabled* **option, the workflow still runs at the next scheduled cron job**.

Resolution: FileCloud Server has been modified so that when the administrator clears the *Enabled* option, the workflow no longer runs automatically.

Known Issues

File Sharing	Comments disappear from a file when it is renamed	Issue: When a user logs in to the User Portal and creates a file, they can add comments about the file. If the user renames the file, the comments are not immediately displayed.

Cause: This is expected behavior due to the event queue process.

After renaming a file with comments, the process that binds the comments to the new file name is deferred for background processing.

- The comments reappear in the properly renamed file after running the cron job.
- If the user renames the file and then re-renames it back to the original name, the comments reappear. This is because a cron job is not necessary to re-bind the comments to a new file name.

Workaround: To see the comments immediately after renaming a file. the cron job must run at it's scheduled time or run manually.

Managing Files and Folders	Expected behavior when moving a folder to a target folder that is being deleted	**Issue:** For example, if Joe is moving the Accounts folder to the Business Expense folder, and while the move is in-progress, Amy deletes the Business Expense folder. In this case, when the move has completed, the Business Expense folder is moved to the Recycle bin with the Accounts folder inside it. **Cause:** This is the expected behavior: • If the folder move is started before deleting the target parent folder: The final result is that the parent folder now only exists in the recycle bin. The parent folder will contain the folder being moved. • If the folder move is started after deleting the parent folder: The final result is that the move will fail. The parent folder exists in recycle bin but will not contain the folder that the user was trying to move. **Workaround:** Configure your environment around this expected behavior: • Check the recycle bin for your folders. • Configure permissions on the parent folder to restrict deletions
Managing Files and Folders	Apparent file count mismatch between User Portal and Windows Explorer	**Issue:** There is a difference in the way FileCloud and Windows calculate disk usage. • When a FileCloud user opens a browser and logs in to the *User Portal*, from the left navigation panel they can click *Settings* to see their *Disk Usage*. This number includes the total number of live files plus the space used to store thumbnail views for the files. • When the same user opens *Windows Explorer* and views the *Properties* for the FileCloud folder where those same files are downloaded so that a local copy is available, the *Size on Disk* number appears to be smaller than the *Disk Usage Total* shown on the *User Portal*. **Cause:** The *Disk Storage Total* on the *User Portal* includes both the number of live files plus the space used to store thumbnail views for the files. The *Windows Explorer Properties* dialog only includes live files. Those numbers should be very close. However, because of the way Windows counts file size there may be minor variations. **Workaround:** When comparing disk usage size, in the *User Portal*, check the *Disk Storage Live Files* number against the *Windows Explorer Properties Size on Disk* number.
Storage	AmazonS3 does not load thumb nails	**Issue:** AmazonS3 backend configuration does not load thumb nails for images, although Document Converter is running without issues. **Workaround:** Verify the following are working correctly: To provide document thumbnail features to your users, you must configure the following tool: • Document Converter - This feature provides thumbnail images and requires OpenJDK. ➡ **FileCloud Document Converter** ⚑ If you are still having issues, try removing the security header from .htaccess file.

Storage	Text editor doesn't work for AmazonS3 share object storage	**Issue:** Documents stored in AmazonS3 share object storage cannot be edited using a text editor. Workaround: 1. Change the Header set in the Content-Security-Policy 2. Use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket. ### Change the Content-Security-Policy Content Security Policy (CSP) is an HTTP header that allows site operators control over where resources can be loaded from on their site. - The use of this header is the best method to prevent cross-site scripting (XSS) vulnerabilities. To change the Header set in CSP: 1. Open a command-line prompt. 2. Type in the following code (or copy and paste): ``` Content-Security-Policy: "default-src 'self' *.live.com s3.amazonaws.com; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval' 'self';font-src 'self' data:;img-src 'self' data ``` ### Add a CORS Policy To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket. A CORS configuration is an XML document that defines rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information. For more information about CORS, see Cross-Origin Resource Sharing (CORS) in the Amazon Simple Storage Service Developer Guide. To allow the use of a text editor: The CORS configuration is an XML file. The text that you type in the editor must be valid XML. 1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/. 2. In the Bucket name list, choose the name of the bucket that you want to create a bucket policy for. 3. Choose Permissions, and then choose CORS configuration. 4. In the CORS configuration editor text box, type or copy and paste the following CORS configuration: ``` <CORSConfiguration> <CORSRule> <AllowedOrigin>*</AllowedOrigin> <AllowedMethod>GET</AllowedMethod> <AllowedHeader>*</AllowedHeader> <MaxAgeSeconds>3000</MaxAgeSeconds> </CORSRule> </CORSConfiguration> ``` 5. Click Save.
Sync Client	Error behavior for the root folder	**Issue:** Filecloud Sync does not show an error every time a user copies and then pastes a file or folder into the parent folder. In FileCloud Drive, the same action displays an error that the parent folder is Read-Only. The user can be confused when no error is shown in FileCloud Sync but is shown in Drive. Cause: In FileCloud Sync, these errors are shown only every 3 hours. - The user will see the following message: *Skipping top level files or folders that are not inside a sync-able folder* - The message is displayed in the *Activity* log and also as a pop-up notification - Only the name of the very first folder or file that cannot be synchronized is displayed in the *Activity* log and pop-up (Instead of every file and folder name)