FileCloud Server
Version 23.263
Upgrade FileCloud

13 October, 2026

Table of Contents

Upgrade using Update Tool (Windows Only) ... 3
Pre-upgrade: ... 3
STEP 1: Backup existing installation ... 3
STEP 2: Preparing for update ... 3
STEP 3: Update ... 4
Troubleshooting the Upgrade Tool ... 8
Disable MongoDB Authentication and IP Binding ... 10
Upgrade FileCloud on Linux ... 12
Upgrade FileCloud on Ubuntu ... 12
Upgrade FileCloud on RHEL ... 14
Backup FileCloud Before Upgrading ... 17
Upgrade using Admin Portal ... 18
Upgrade Steps ... 18
Updating Systems That Cannot Connect Outside ... 22
Upgrade Notes ... 24
Windows: Upgrading from 23.262 to the Latest Version ... 24
Windows: Upgrading from 23.261 to the Latest Version ... 26
Windows: Upgrading from 23.253 to the Latest Version ... 28
Windows: Upgrading from 23.252 to the Latest Version ... 31
Windows: Upgrading Versions <23.252 to the Latest Version ... 34
Linux: Upgrading from 23.262 to the Latest Version ... 45
Linux: Upgrading from 23.261 to the Latest Version ... 47
Linux: Upgrading from 23.253 to the Latest Version ... 50
Linux: Upgrading from 23.252 to the Latest Version ... 52
Linux: Upgrading from Versions <23.252 to the Latest Version ... 55

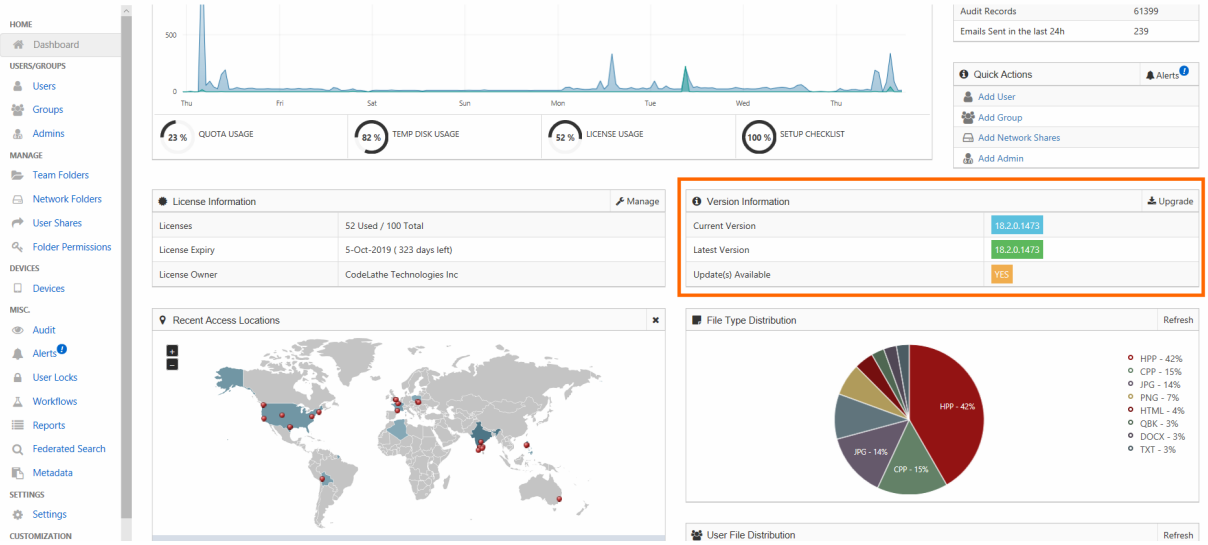
Administrators must keep FileCloud Server up-to-date with the latest version to take advantage of the new features, enhancements, and fixes for issues found in previous versions.

How do I know if an upgrade is available?

- FileCloud will always inform customers when a new upgrade is available.
- When you log on to the Admin Portal, the Admin Dashboard will also alert you to the fact that you can install an update.

Where is the notification on the Admin Dashboard?

The Version section is right next to the License section on the Dashboard.

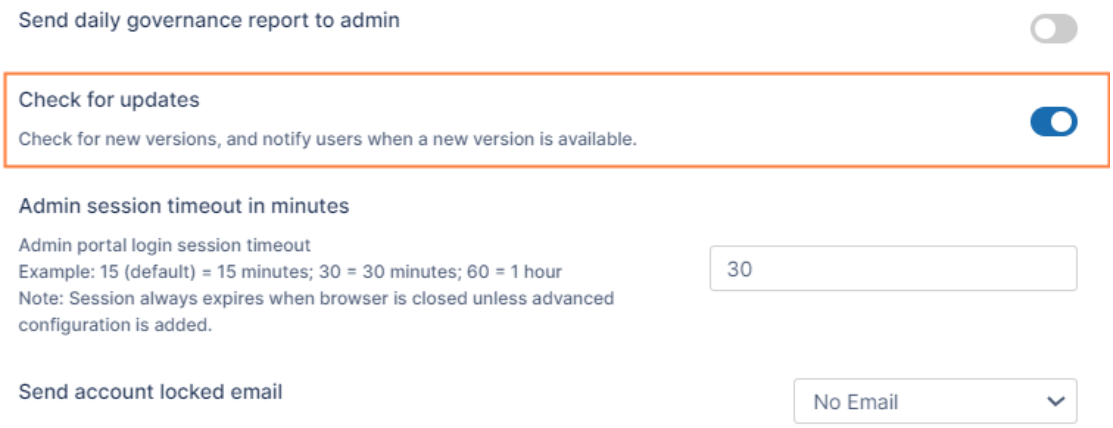


How do I enable the weekly email?

To check for updates on a weekly basis:

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

2. Scroll down to **Check for updates**, and enable it.



3. Click **Save**.

💡 To stop receiving the weekly email, disable this setting.

Remember to back up FileCloud before upgrading.

For instructions on upgrading from your current version of FileCloud, see Upgrade Notes .

To upgrade, see:

Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.
Check If the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:
C:\xampp\apache\conf\httpd.conf
C:\xampp\apache\conf\extra\httpd-filecloud.conf

Upgrade using Update Tool (Windows Only)

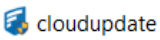
Pre-upgrade:

Please read the appropriate upgrade notes for the version you are upgrading from before proceeding with the following steps.

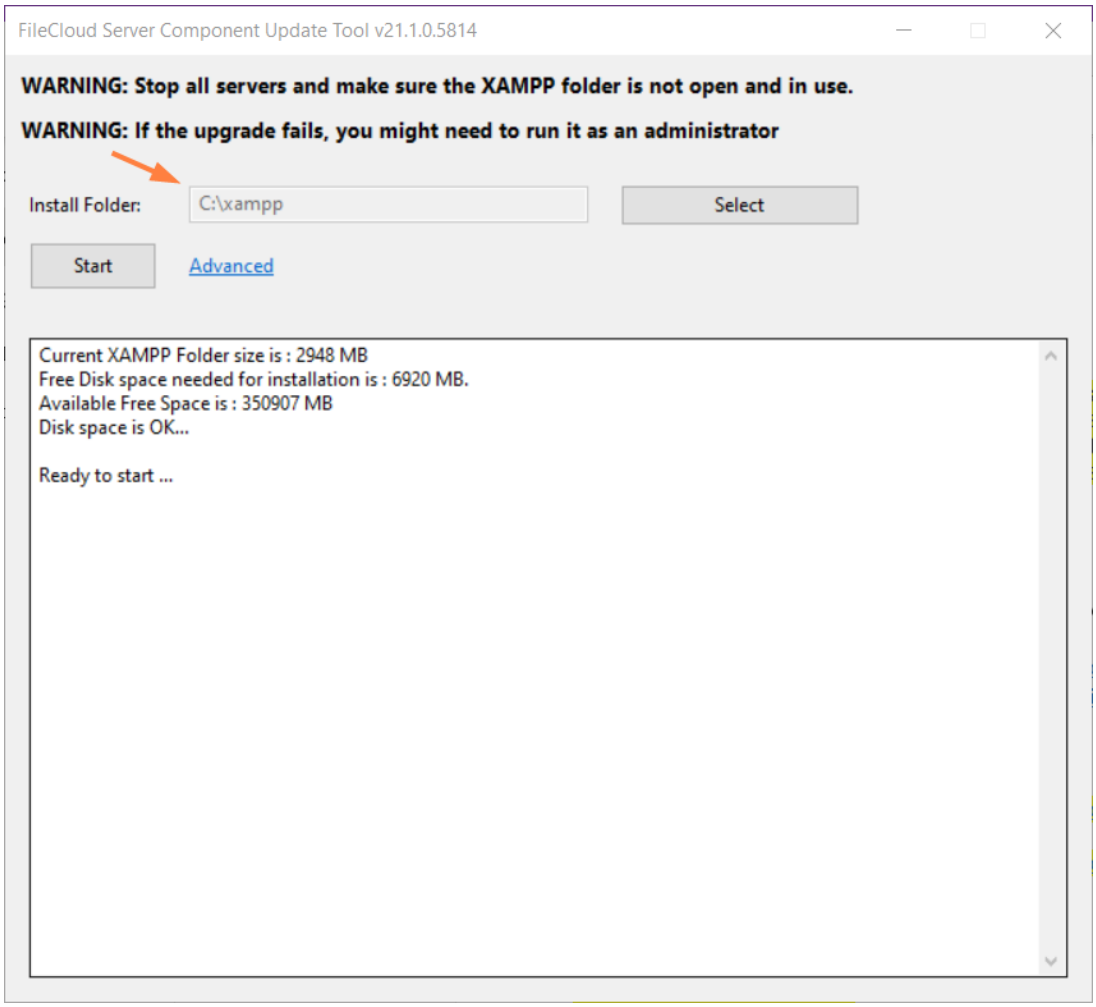
STEP 1: Backup existing installation

FileCloud installation environment	Backup steps
Windows OS and installation without backup tool	Windows manual backup

STEP 2: Preparing for update

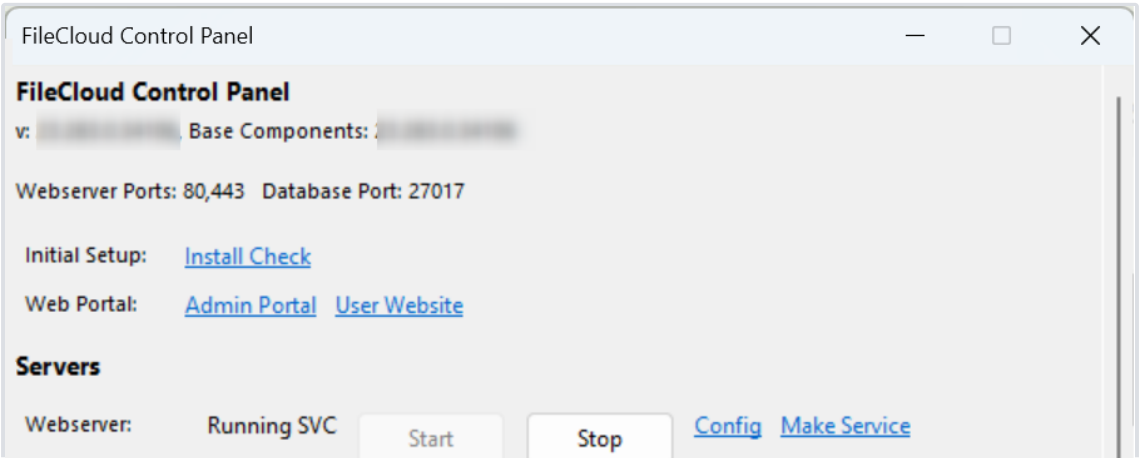
1. Download the latest FileCloud Windows Update Tool from https://patch.codelathe.com/tonidocloud/live/installer/cloudupdatetool.zip
   Note: It is essential that you download the latest version of the update tool; If you run an old version of the tool, you will re-install an old version of FileCloud.
2. Extract all files from cloudupdatetool.zip into a folder.
3. If your system allows downloading of files from internet, go to step 5. Otherwise, complete step 4 first.
4. Download the following files and copy them to the extracted folder (the cloudupdatetool folder)
   - FileCloud Windows Preupgrade Package from https://patch.codelathe.com/tonidocloud/live/installer/filecloudpreupgrade.zip
   - FileCloud Windows Preupgrade XML - Right-click and save the file https://patch.codelathe.com/tonidocloud/live/installer/filecloudpreupgrade.xml
   - FileCloud Windows Update Package from https://patch.codelathe.com/tonidocloud/live/installer/filecloudupdate.zip
   - FileCloud Windows Update XML - Right-click and save the file https://patch.codelathe.com/tonidocloud/live/installer/filecloudupdate.xml
5. Now, navigate to the cloudupdatetool folder and double click on
   

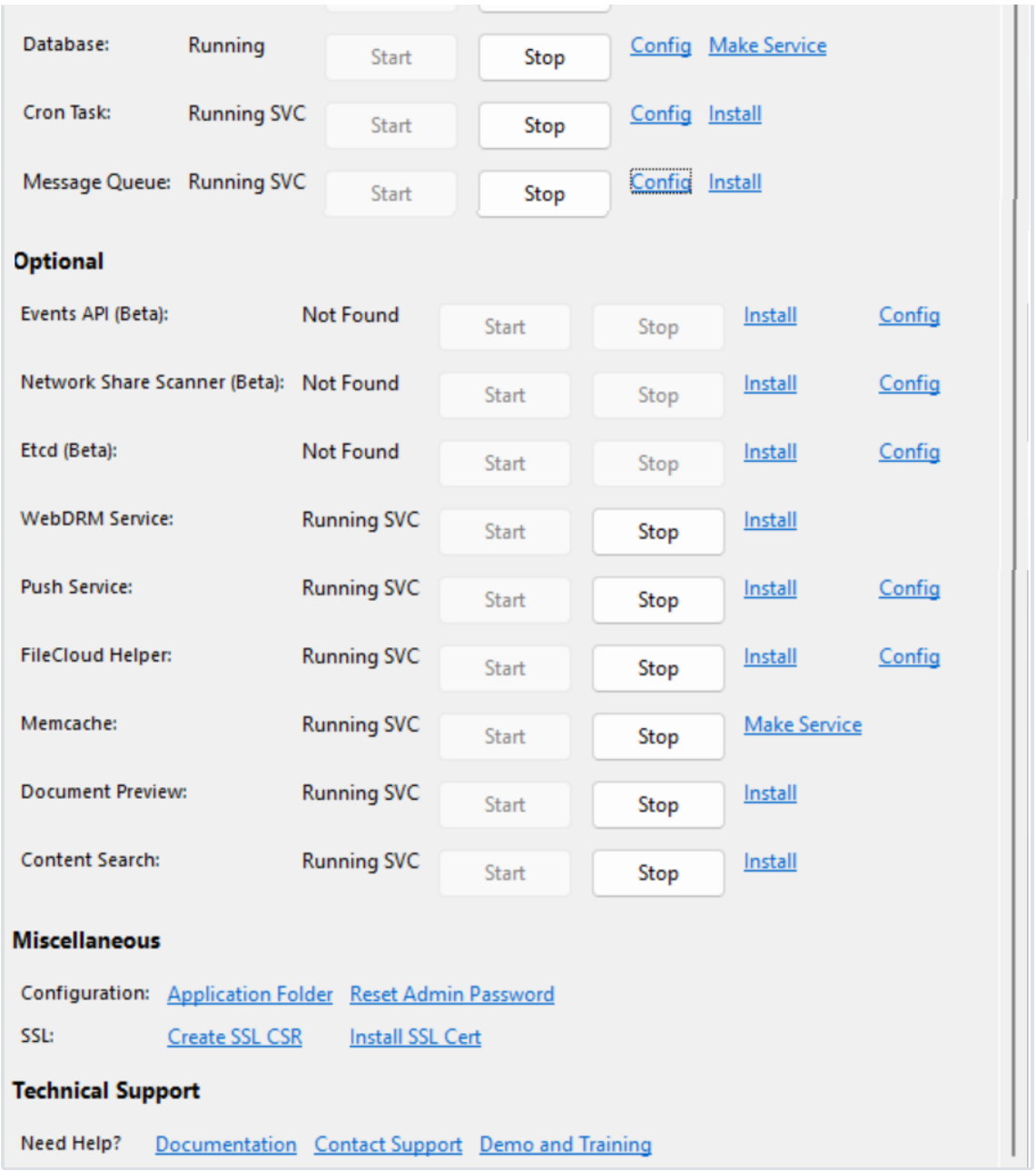
   (cloudupdate.exe). The following window opens:



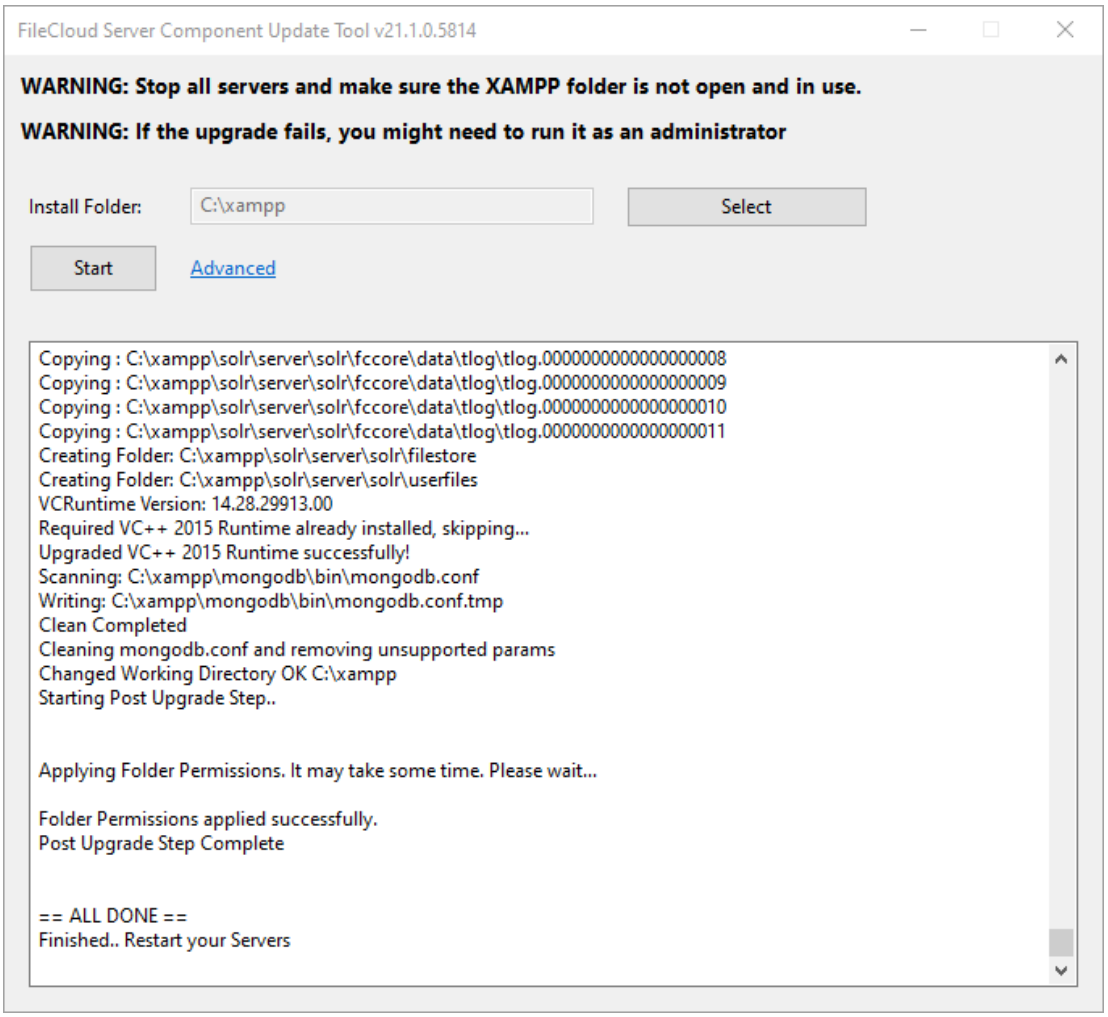
STEP 3: Update

1. Open the FileCloud Control Panel and confirm that each service you are using is running, and that your storage is in the READY state.





2. Ensure that **Install Folder** shows the location of your XAMPP folder. This location is auto-detected, but it may not be able to determine it correctly if there are multiple XAMPP folders. If it is not correct, select the correct XAMPP install folder.
3. Click **Start** on the Update Tool dialog box to begin the upgrade. (Repeat steps 1-3 for each of the nodes for HA system).
   The tool must be able to connect to the internet in order to download the update package. Please contact support@codelathe.com if you see any errors in this step.

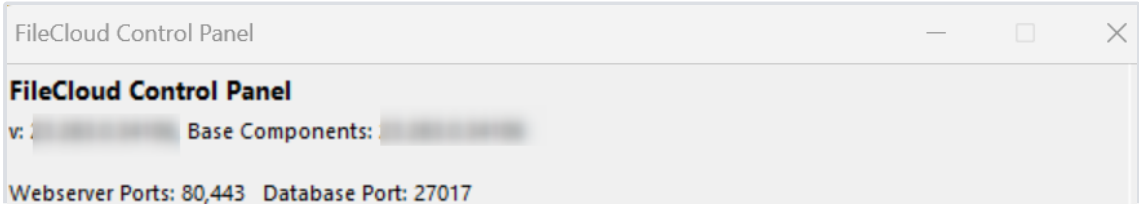


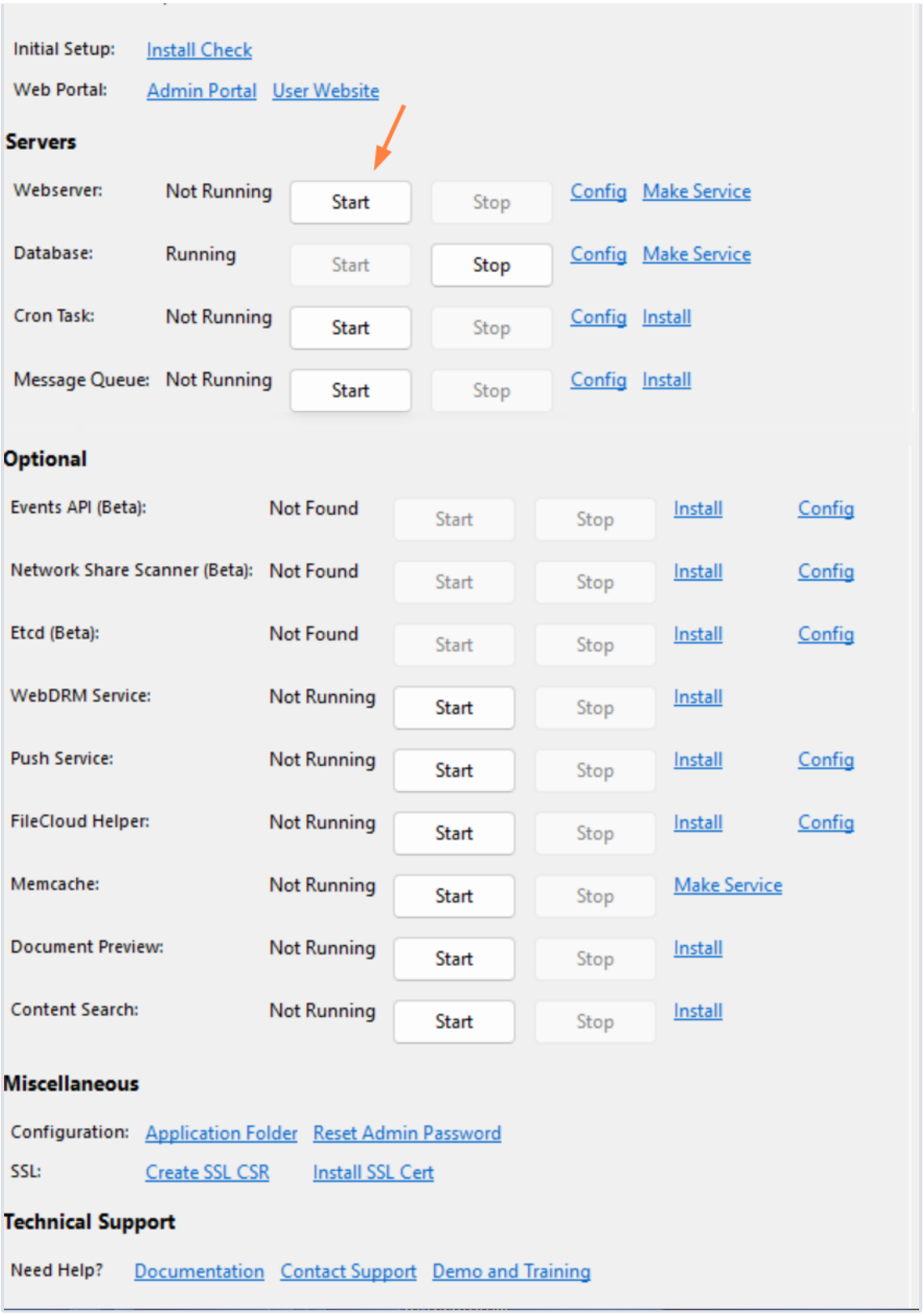
If you receive an error message, see Troubleshooting the Upgrade Tool.

4. If you are running multi-tenant FileCloud, make sure the database post upgrade script is run correctly.

```
cd c:\xampp\htdocs\resources\backup
c:\xampp\php\php.exe fcpostupgrade.php
```

5. After FileCloud is upgraded, the folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. Add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
6. Once the nodes are updated, start each of the nodes using the FileCloud Control Panel.





7. Message Queue is an important service and must be started after the upgrade.

> Message Queue must be installed. If you cannot click the **Start** button for **Message Queue**, it is not installed. Click **Install**, and once installation is complete, click **Start**.

8. Open the install URL http://<your domain>/install/index.php
9. Make sure basic checks are all OK.
10. Click on **Extended Checks**.
    In section 3 of **Extended Checks**, your new updates are shown with status and available actions.
11. If Apache is running as the Windows Logon account, then give the logon account write permission on the XAMPP folder.
12. When you initially log in to the admin portal after upgrade, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.
13. Beginning in FileCloud 20.1, to sign into the admin portal for multi-tenancy, you must sign in as the superadmin user and enter your password in encrypted format in the multi.php file.
    See Password encryption and logging in to a multi-tenant admin portal for instructions on encrypting your password.

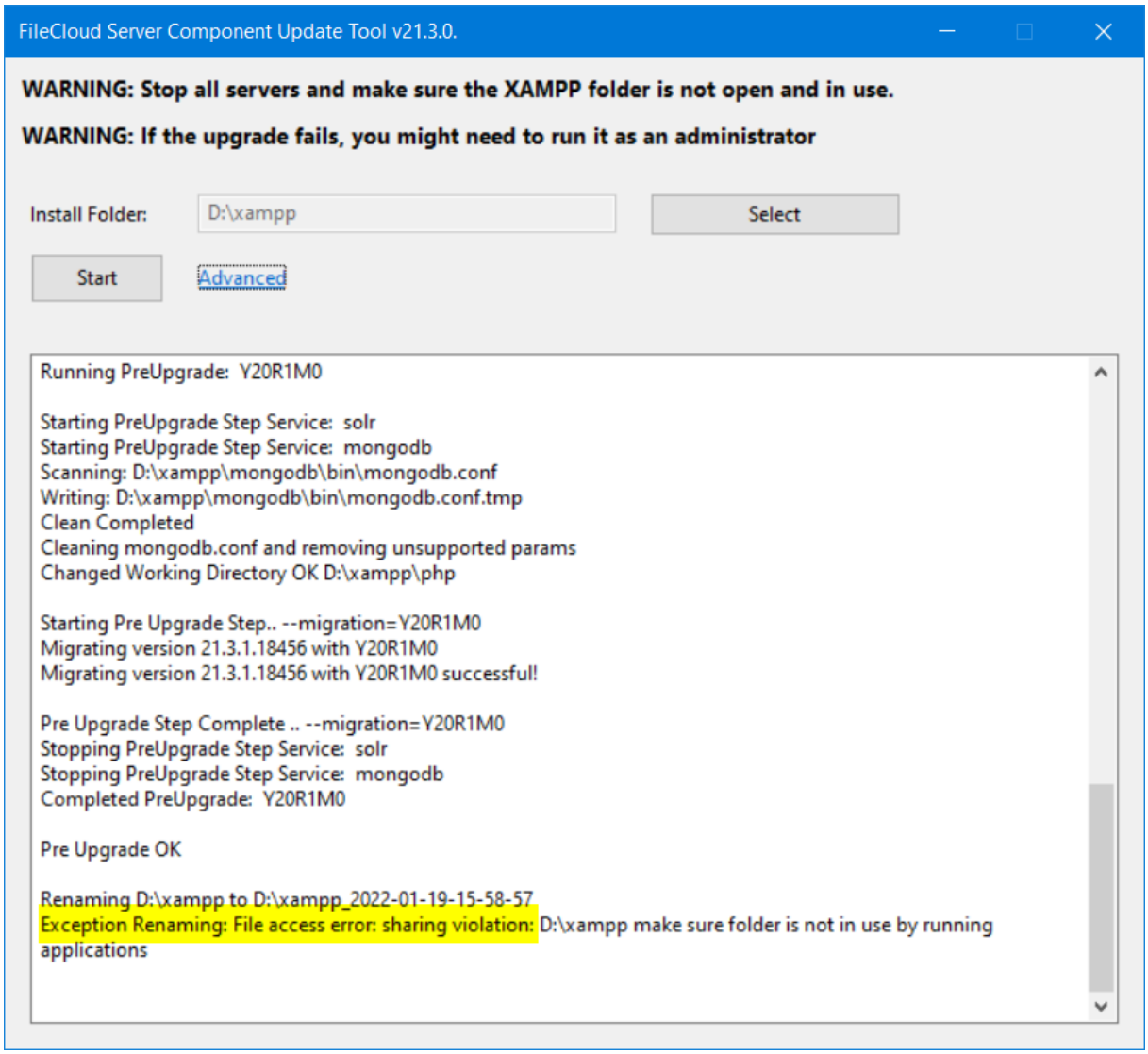
> **Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.**
> Check If the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:
> C:\xampp\apache\conf\httpd.conf
> C:\xampp\apache\conf\extra\httpd-filecloud.conf
> C:\xampp\apache\conf\extra\httpd-ssl.conf
> C:\xampp\cron.ini
> C:\xampp\htdocs\.htaccess
> C:\xampp\php\php.ini
> C:\xampp\htdocs\src\Scripts\config\default.json

Troubleshooting the Upgrade Tool

Exception Renaming

Problem:
The upgrade tool returns the error **Exception Renaming: File access error: sharing violation D:\xampp**

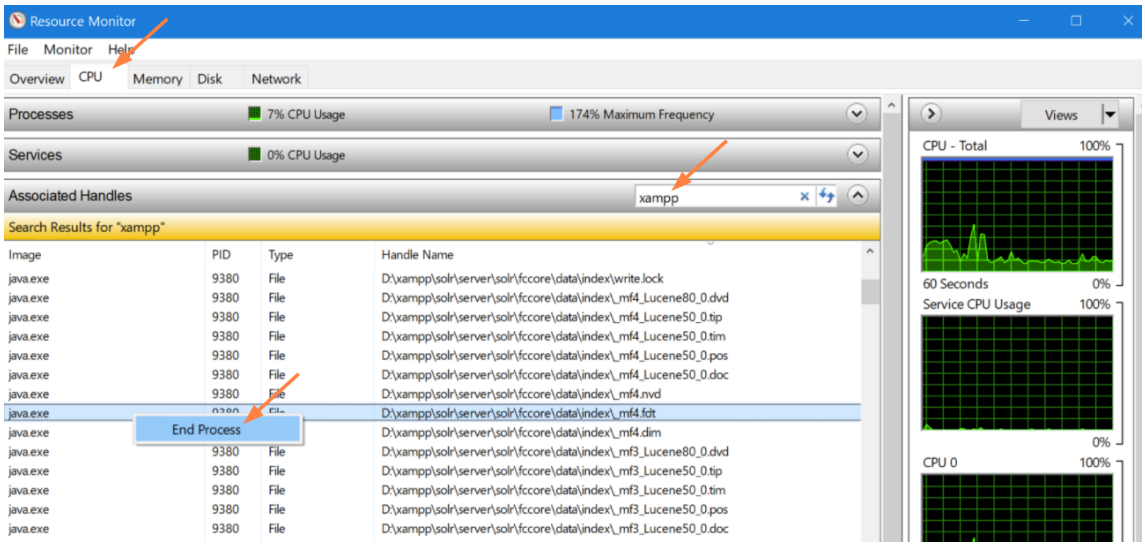
make sure folder is not in use by running applications as shown in the following screenshot:



Solution:

Use the Windows Resource Monitor to end the processes that are blocking the move:

1. Start the Resource Monitor by clicking **Win-R**, and then entering **resmon**.
2. Click the **CPU** tab.
3. Search for **xampp** in **Associated Handles**.
4. Right-click on each xampp process and choose **End Process**.



5. Click **Start** in the **Update Tool** interface again.

Disable MongoDB Authentication and IP Binding

If your system uses MongoDB authentication or custom IP binding, prior to using the FileCloud Update tool for Windows, MongoDB authentication and IP binding must be disabled.

To disable MongoDB authentication and IP binding:

1. Backup the MongoDB config file by running the command:

```
copy C:\xampp\mongodb\bin\mongodb.conf %TEMP%
```

2. In C:\xampp\mongodb\bin\mongodb.conf, disable authentication by adding **#** (a comment character) at the beginning of the line **auth = true**:

```
#auth = true
```

3. Also in C:\xampp\mongodb\bin\mnogodb.conf, disable IP binding by uncommenting **bind_ip_all** and commenting **bind_ip**:

```
#ip address
bind_ip_all = true
#bind_ip = 10.2.3.44
```

4. Restart MongoDB to activate the changes.

5. Test access using mongo shell.
   (If you are updating from a version of FileCloud prior to version 23.1, use **mongo** instead of **mongosh** in the following command:

```
cd C:\xampp\mongodb\bin
mongosh --quiet --eval "show dbs"
# you should see output similar to this:
admin                   148.00 KiB
config                  108.00 KiB
fcbackup                 20.00 KiB
fcbackup_duo             20.00 KiB
```

6. Update FileCloud using the Update Tool.
7. Re-enable IP binding and authentication and restart MongoDB.

Upgrade FileCloud on Linux

Upgrade FileCloud on Ubuntu

The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

Upgrade steps:

1. Prior to performing the following steps, review the upgrade notes that apply to the Linux version you are upgrading from.
   Upgrade Notes
2. Take server snapshots or back up your files. This will help restore the system to a working state if there are any unforeseen issues.
   (23.263a) FileCloud Backup and Restore - Linux Manual
3. Upgrade using the procedure below.

- During MongoDB upgrade, when you are prompted to replace the MongoDB configuration file, select 'N' (No) to keep your existing settings.
- When you are prompted to restart services during the upgrade, always restart the default one, which is marked with an asterisk (*).
- When you are prompted with a modified configuration file during PHP upgrade, choose "keep the local version currently installed" to retain your existing custom settings.

During upgrade, the default FileCloud MongoDB configuration file is saved as **mongo.conf.dist**. Please compare this file with your existing **mongo.conf** file and manually add any new configuration parameters introduced in the default configuration.

To upgrade to the latest release on Ubuntu 22.04 LTS:

```
apt clean cache
curl -fsSL https://pgp.mongodb.com/server-8.0.asc | sudo gpg -o /usr/share/keyrings/
mongodb-server-8.0.gpg --dearmor
```

```
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-8.0.gpg ]
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/8.0 multiverse" | sudo tee /etc/
apt/sources.list.d/mongodb-org-8.0.list
rm -rf /etc/apt/sources.list.d/mongodb-org-7.0.list

curl -fsSL https://repo.filecloudlabs.com/static/pgp/filecloud.asc | sudo gpg -o /usr/
share/keyrings/filecloud.gpg --dearmor
echo "deb [ arch=amd64 signed-by=/usr/share/keyrings/filecloud.gpg ] https://
repo.filecloudlabs.com/apt/ubuntu jammy/filecloud/23.263 main" | sudo tee /etc/apt/
sources.list.d/filecloud.list
```

After you enter the above line, you are prompted with:
File '/usr/share/keyrings/mongodb-server-8.0.gpg' exists. Overwrite? (y/N)

Enter **y** and continue entering the following code:

```
apt update -y
apt-mark unhold mongodb-org mongodb-org-database mongodb-org-server mongodb-org-mongos
mongodb-org-tools
apt install -y mongodb-org=8.0.29 mongodb-org-database=8.0.29 mongodb-org-server=8.0.29
 mongodb-org-mongos=8.0.29 mongodb-org-tools=8.0.29 --allow-downgrades
apt-mark hold mongodb-org mongodb-org-database mongodb-org-server mongodb-org-mongos
mongodb-org-tools
apt upgrade -y apache2 pigz
apt install -y php8.4 php8.4-bcmath php8.4-cli php8.4-igbinary php8.4-common
php8.4-curl php8.4-gd php8.4-gmp php8.4-imap php8.4-intl php8.4-ldap php8.4-mbstring
php8.4-memcache php8.4-memcached php8.4-mongodb php8.4-opcache php8.4-readline
php8.4-soap php8.4-xml php8.4-xsl php8.4-zip php8.4-sqlite3 php-json libapache2-mod-
security2
apt-get install nodejs=24.18.1-1nodesource1
ACCEPT_EULA=Y apt upgrade filecloud -y
a2dismod php8.2
a2dismod php8.3
service apache2 restart
```

To upgrade Solr to the latest release or apply the latest security patch

If you have Solr configured before you upgrade, also enter the following command.

```
filecloudcp -s
```

If your indexed Solr data was created using Solr version 7.x or older, a full re-index is required.

To upgrade Tesseract to the latest release

If you have Tessearct configured before you upgrade, also enter the following command.

```
filecloudcp -t
```

To upgrade LibreOffice to the latest release

If you have LibreOffice configured before you upgrade, also enter the following command.

```
filecloudcp --install-preview
```

Upgrade FileCloud on RHEL

Upgrade steps:

1. Prior to performing the following steps, review the upgrade notes that apply to the Linux version you are upgrading from.
   Upgrade Notes
2. Take server snapshots or back up your files. This will help restore the system to a working state if there are any unforeseen issues.
   (23.263a) FileCloud Backup and Restore - Linux Manual
3. Upgrade using the procedure below.

- During MongoDB upgrade, when you are prompted to replace the MongoDB configuration file, select 'N' (No) to keep your existing settings.
- When you are prompted to restart services during the upgrade, always restart the default one, which is marked with an asterisk (*).
- When you are prompted with a modified configuration file during PHP upgrade, choose "keep the local version currently installed" to retain your existing custom settings.

During upgrade, the default FileCloud MongoDB configuration file is saved as **mongo.conf.dist**. Please compare this file with your existing **mongo.conf** file and manually add any new configuration parameters introduced in the default configuration.

To upgrade to the latest release on RHEL9

```
yum clean all
curl -sL https://repo.filecloudlabs.com/static/fcp/apache_check | sudo bash -

dnf module disable httpd -y
dnf module disable php -y

rm -rf /etc/yum.repos.d/filecloud*
rm -rf /etc/yum.repos.d/mongodb-org*

cat <<EOF > /etc/yum.repos.d/mongodb-org-8.0.repo
[mongodb-org-8.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/\$releasever/mongodb-org/8.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-8.0.asc
EOF

cat <<EOF > /etc/yum.repos.d/filecloud-23.263.repo
[filecloud-23.263]
name=FileCloud 23.263
baseurl=https://repo.filecloudlabs.com/yum/redhat/\$releasever/filecloud/23.263/x86_64/
gpgcheck=1
priority=1
enabled=1
gpgkey=https://repo.filecloudlabs.com/static/pgp/filecloud.asc
module_hotfixes=true
EOF

yum update -y --allowerasing
yum install yum-utils -y
yum-config-manager --enable mongodb-org-8.0
yum upgrade mongodb-org mongodb-org-database mongodb-org-server mongodb-org-mongos
mongodb-org-tools -y
yum downgrade mongodb-org-8.0.29 mongodb-org-database-8.0.29 mongodb-org-server-8.0.29
 mongodb-org-mongos-8.0.29 mongodb-org-tools-8.0.29 -y

yum upgrade nodejs -y
yum upgrade openssl -y
ACCEPT_EULA=Y dnf upgrade --allowerasing filecloud -y
```

To upgrade Solr to the latest release or apply the latest security patch

If you have Solr configured before you upgrade, also enter the following command.

```
filecloudcp -s
```

If your indexed Solr data was created using Solr version 7.x or older, a full re-index is required.

To upgrade Tesseract to the latest release

If you have Tessearct configured before you upgrade, also enter the following command.

```
filecloudcp -t
```

To upgrade LibreOffice to the latest release

If you have LibreOffice configured before you upgrade, also enter the following command.

```
filecloudcp --install-preview
```

Backup FileCloud Before Upgrading

Before updating FileCloud, it is important to back up your data.

Linux manual backup

Windows manual backup

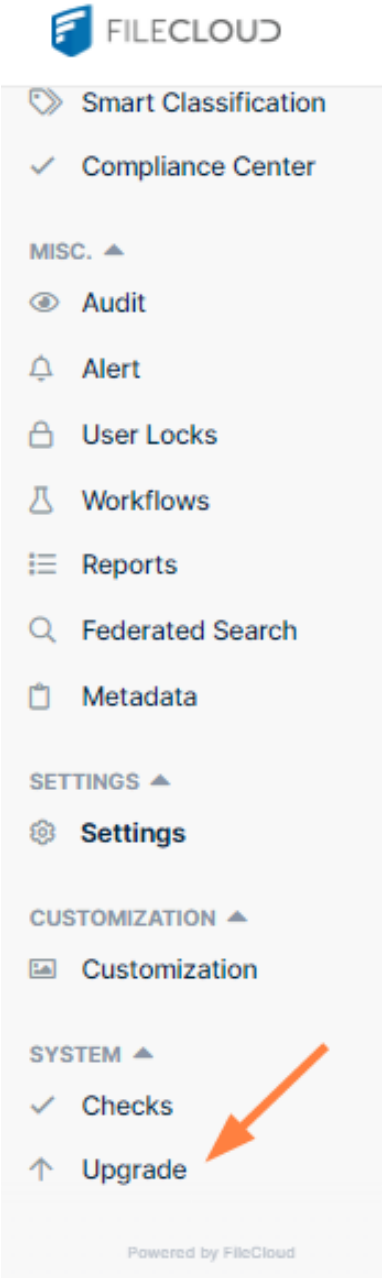
Upgrade using Admin Portal

Minor updates can be performed directly in the FileCloud Admin Portal by clicking the **Start Upgrade** button, as shown in the steps below. Check the release notes to see the minimum version for an update in the Admin portal.

Custom settings in configuration files that are replaced during upgrade are not reset in the new configuration files.
Check If the following files are replaced with newer versions during upgrade, and in the case that they are replaced, reconfigure any custom settings after upgrade:
C:\xampp\apache\conf\httpd.conf
C:\xampp\apache\conf\extra\httpd-filecloud.conf

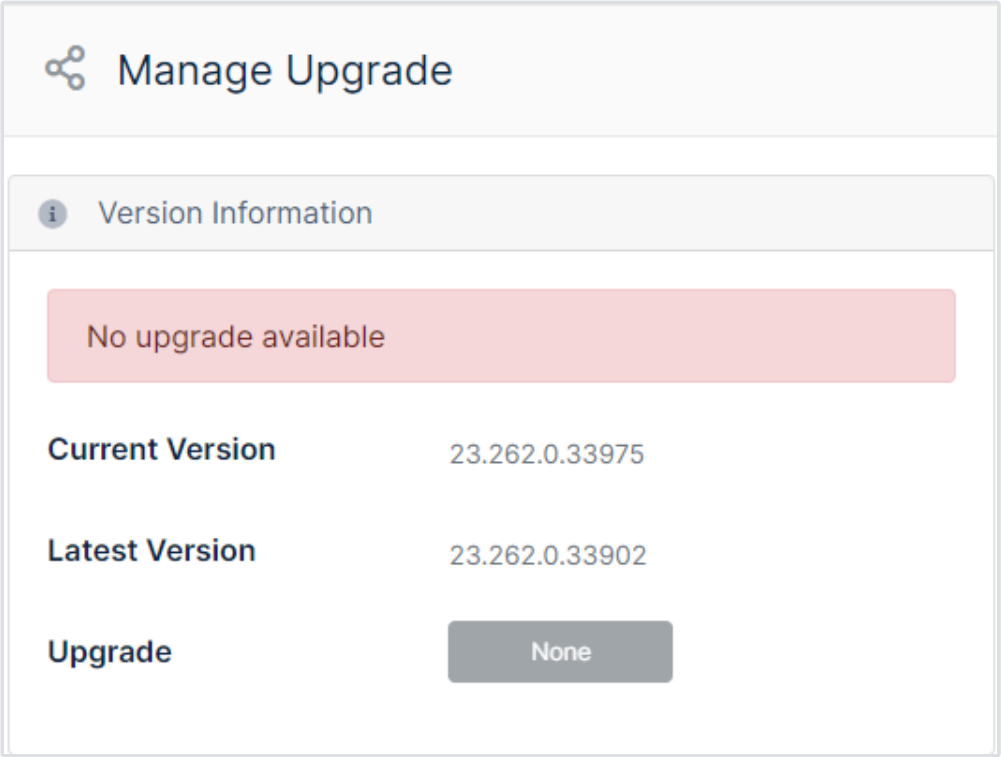
Upgrade Steps

1. Make a full backup or take a snapshot of the FileCloud server.
2. Login into the admin UI.
3. Click **Upgrade** at the bottom of the navigation panel.

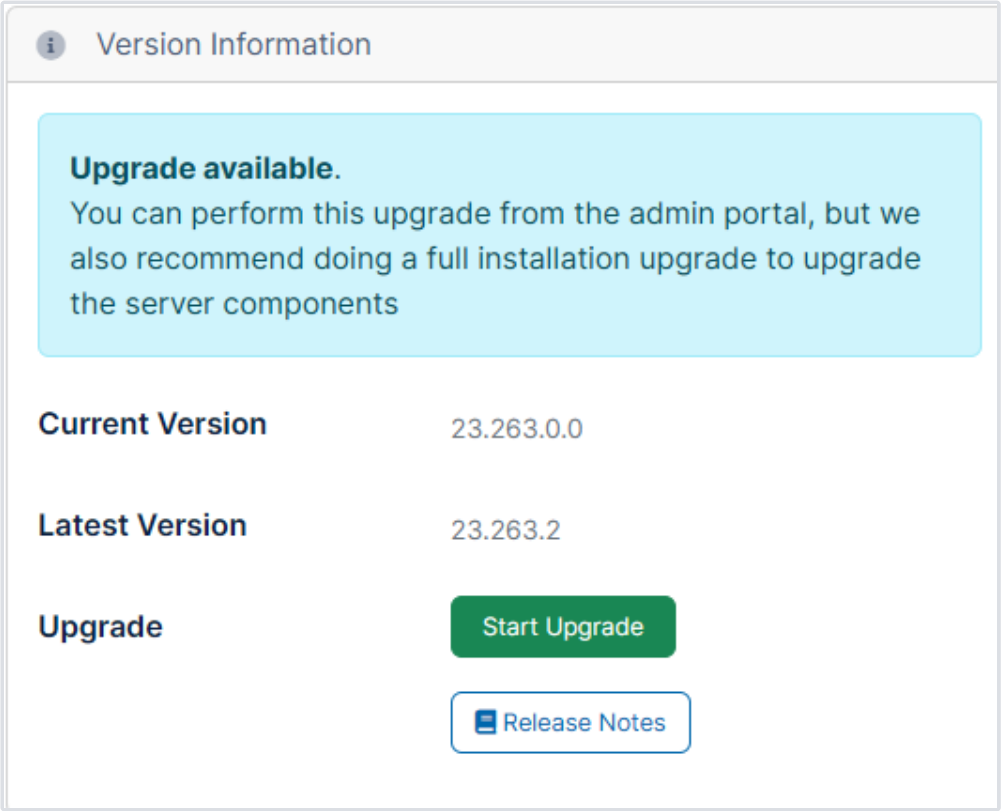


The Manage Upgrade window appears as follows if:

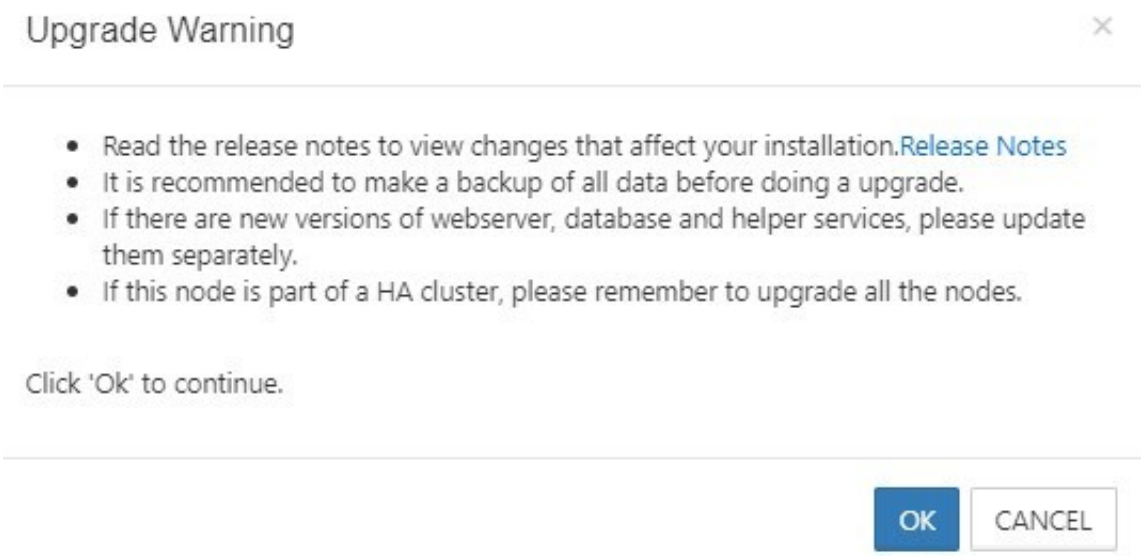
- No new upgrades are available
- Upgrades are not possible from the admin portal
- A license that does not allow upgrade to the latest version is installed



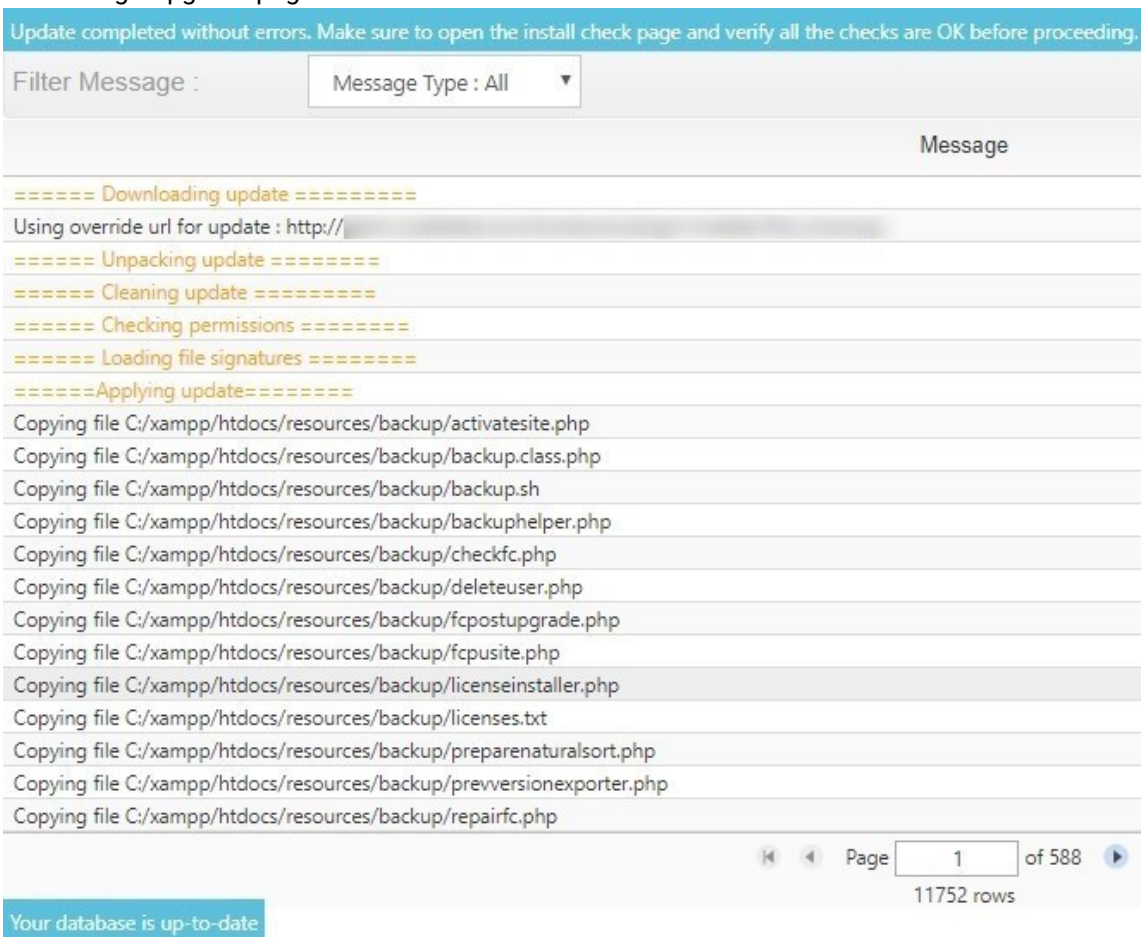
If there is an upgrade that can be installed from the admin portal and is permitted by the FileCloud license, the Manage Upgrade window appears as follows (the recommendation to do a full installation only appears if it applies).



4. If the Manage Upgrade window indicates that an upgrade is available, click **Start Upgrade**. The following window opens:



5. **Click OK.**
   The upgrade process begins. When it is complete, messages similar to the following appear on the Manage Upgrade page.



6. In the navigation bar, click Installation Checks directly above the Upgrade link and make sure that the installation is free of errors.
7. Refresh the browser UI (Ctrl + F5) to get the latest updated User Interface.

Updating Systems That Cannot Connect Outside

If your FileCloud server cannot connect to our update server to download the packages directly, you can download file_cloud.zip and file_cloud.xml to a local folder and update your installation using the local path.

1. Open the WWWROOT\config\cloudconfig.php file and edit the following entry:
   For Windows:
   If the files are located in c:\users\administrator\Downloads folder, then modify the url as follows:

```
define("TONIDOCLOUD_UPDATE_URL_OVERRIDE","file://C:\\Users\\Administrator\
\Downloads\\file_cloud.zip");
```

For Linux:
If the the files are located in /home/filecloudupdate/ (Apache should have permission for this folder), then modify the url as follows:

```
define("TONIDOCLOUD_UPDATE_URL_OVERRIDE","/home/filecloudupdate/file_cloud.zip");
```

2. Download the following packages and place them in the local folder specified in the TONIDOCLOUD_UPDATE_URL_OVERRIDE config:
   https://patch.codelathe.com/tonidocloud/live/installer/file_cloud.zip
   https://patch.codelathe.com/tonidocloud/live/installer/file_cloud.xml

Upgrade Notes

Windows: Upgrading from 23.262 to the Latest Version

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

1. As always, make a full backup of your existing installation before upgrading.
   Backup on Windows
2. If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
3. ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
   To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
4. If your system uses ServerLink, perform the following steps:
   a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
   b. Make backups of all nodes as needed.
   c. Stop the FileCloud ServerLink client service in secondary nodes.
   d. Upgrade the primary node first.
   e. Upgrade each secondary node after upgrading the primary node.
   f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

   Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

- If your system uses MongoDB authentication or a custom IP binding, follow the steps at Disable MongoDB Authentication and IP Binding.

Upgrade instructions

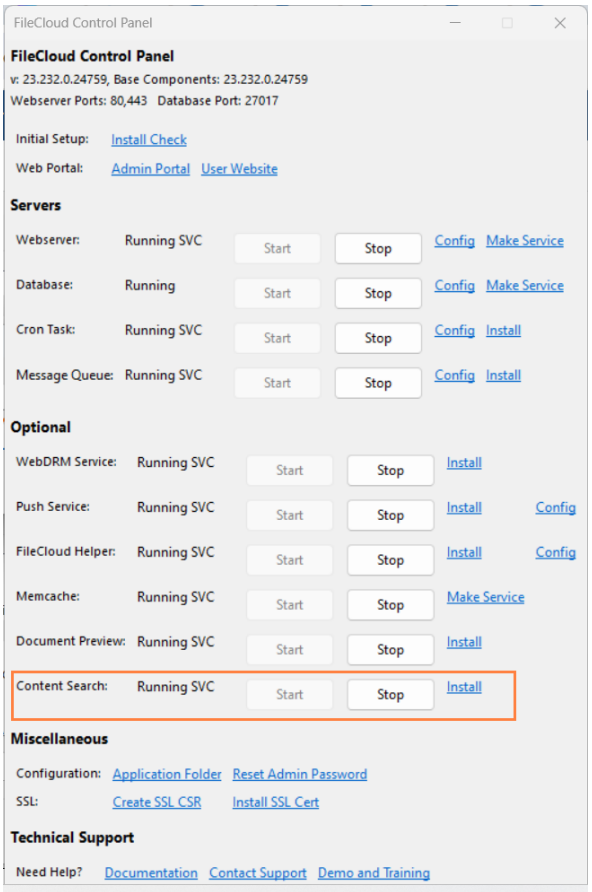
- The current version of the Windows Update Tool is 23.263.0.9354, which is effective for installing FileCloud Version 23.263.
- If you have a large installation, it is possible that your upgrade to version 23.263 may take longer than usual. This is due to pre-upgrade repair that is included with storage improvements and is to be expected.

1. Before running the upgrade tool, confirm that each of your FileCloud services is **running** and that your storage is in a **READY** state.
2. Use the Windows Upgrade tool to do a full upgrade. (You cannot upgrade using the admin portal.)
   ⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, but prior to restarting each of the nodes in the FileCloud Control Panel, add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
   Upgrade using Update Tool (Windows Only)
3. For all upgrades, once upgrade is complete, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.

Post Upgrade

Upgrade Windows environments using Solr and Solr+OCR

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 17.
3. Set JAVA_HOME to the new version's path.
4. Log in to the FileCloud admin portal.
5. In the FileCloud Control Panel, and stop and restart Content Search.



FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Windows: Upgrading from 23.261 to the Latest Version

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

1. As always, make a full backup of your existing installation before upgrading.
   Backup on Windows
2. If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.

3. ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
   To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
4. If your system uses ServerLink, perform the following steps:
   a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
   b. Make backups of all nodes as needed.
   c. Stop the FileCloud ServerLink client service in secondary nodes.
   d. Upgrade the primary node first.
   e. Upgrade each secondary node after upgrading the primary node.
   f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

   Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

- If your system uses MongoDB authentication or a custom IP binding, follow the steps at Disable MongoDB Authentication and IP Binding.

Upgrade instructions

⚠️

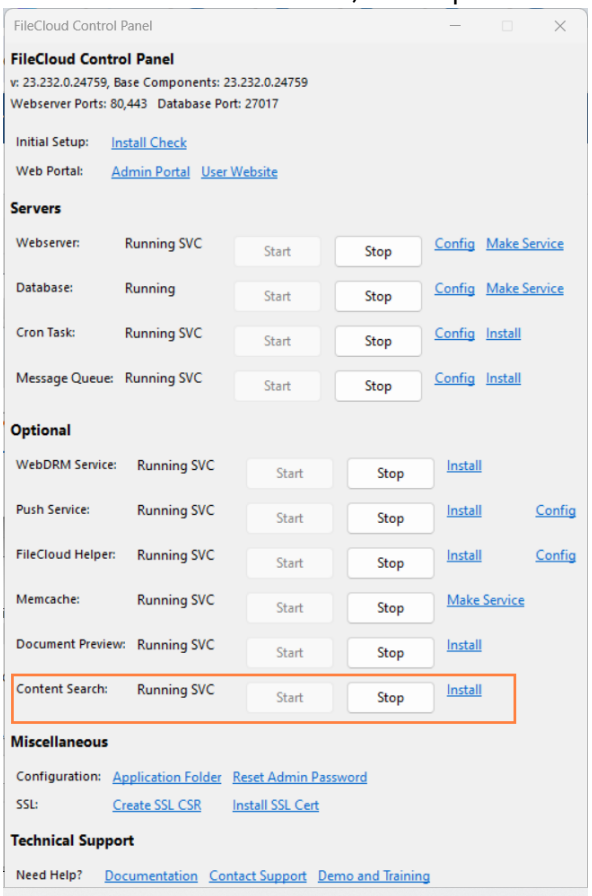
- The current version of the Windows Update Tool is 23.263.0.9354, which is effective for installing FileCloud Version 23.263.
- If you have a large installation, it is possible that your upgrade to version 23.263 may take longer than usual. This is due to pre-upgrade repair that is included with storage improvements and is to be expected.

1. Before running the upgrade tool, confirm that each of your FileCloud services is **running** and that your storage is in a **READY** state.
2. Use the Windows Upgrade tool to do a full upgrade. (You cannot upgrade using the admin portal.)
   ⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, but prior to restarting each of the nodes in the FileCloud Control Panel, add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
   Upgrade using Update Tool (Windows Only)
3. For all upgrades, once upgrade is complete, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.

Post Upgrade

Upgrade Windows environments using Solr and Solr+OCR

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 17.
3. Set JAVA_HOME to the new version's path.
4. Log in to the FileCloud admin portal.
5. In the FileCloud Control Panel, and stop and restart Content Search.



FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Windows: Upgrading from 23.253 to the Latest Version

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

1. As always, make a full backup of your existing installation before upgrading.
   Backup on Windows
2. If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
3. ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
   To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
4. If your system uses ServerLink, perform the following steps:
   a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
   b. Make backups of all nodes as needed.
   c. Stop the FileCloud ServerLink client service in secondary nodes.
   d. Upgrade the primary node first.
   e. Upgrade each secondary node after upgrading the primary node.
   f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

   Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

- If your system uses MongoDB authentication or a custom IP binding, follow the steps at Disable MongoDB Authentication and IP Binding.

Upgrade instructions

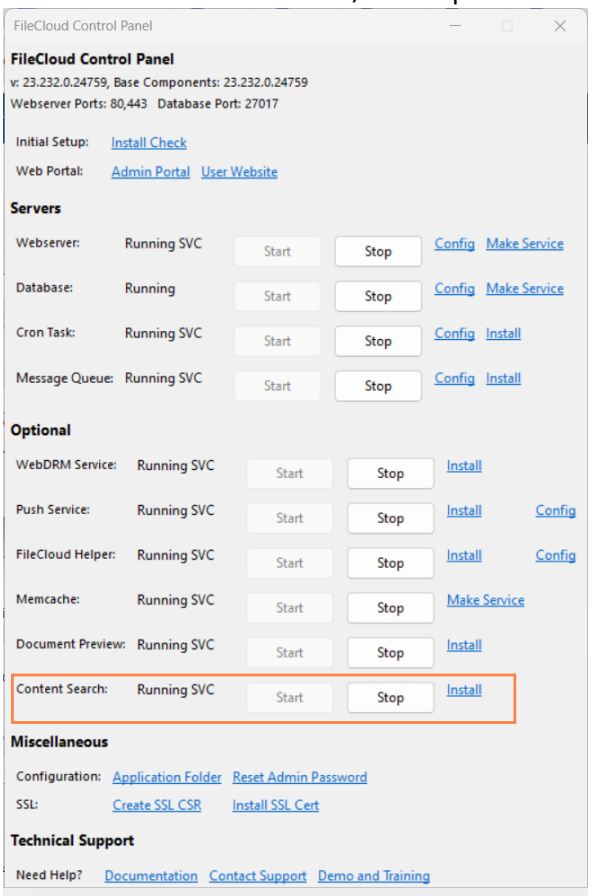
- The current version of the Windows Update Tool is 23.263.0.9354, which is effective for installing FileCloud Version 23.263.
- If you have a large installation, it is possible that your upgrade to version 23.263 may take longer than usual. This is due to pre-upgrade repair that is included with storage improvements and is to be expected.

1. Before running the upgrade tool, confirm that each of your FileCloud services is **running** and that your storage is in a **READY** state.
2. Begin using the Windows Upgrade tool to do a full upgrade.
   ⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, but prior to restarting each of the nodes in the FileCloud Control Panel, add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
   Upgrade using Update Tool (Windows Only).
3. For all upgrades, once upgrade is complete, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.

Post Upgrade

Upgrade Windows environments using Solr and Solr+OCR

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 17.
3. Set JAVA_HOME to the new version's path.
4. Log in to the FileCloud admin portal.
5. In the FileCloud Control Panel, and stop and restart Content Search.



FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Windows: Upgrading from 23.252 to the Latest Version

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

1. As always, make a full backup of your existing installation before upgrading.
   Backup on Windows
2. If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
3. ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
   To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
4. Beginning in FileCloud 23.253, by default, a more granular dynamic content security policy replaces the existing content security policy in the .htaccess file. If you are upgrading, to make this change effective, you must make a small change to the Content-Security-Policy header in the .htaccess file:
   - Open the .htaccess file.

     in Windows:
     C:\xampp\htdocs\.htaccess

     in Linux:
     /var/www/html/.htaccess
   - Find the line that begins:
     Header set Content-Security-Policy:
   - Change set to setifempty:
     Header setifempty Content-Security-Policy:

```
<IfModule mod_headers.c>
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header setifempty Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com *.skype.com *.autodesk.com; \
    frame-src 'self' blob: www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net *.autodesk.com; \
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com; \
    worker-src 'self' blob: *.autodesk.com"
```

5. If you have added custom rules to the .htaccess file, they will be overridden by the dynamic CSP feature. To solve this:
   Either:
   Disable the dynamic CSP feature with the setting **TONIDOCLOUD_DYNAMIC_CSP_ENABLED**.
   See (23.263a) Dynamic CSP in FileCloud.

   Or:
   Add the custom rules to the setting **TONIDOCLOUD_DYNAMIC_CSP_EXTEND**.

   To add the custom rules:
   a. On the FileCloud Server, open the cloudconfig file:
      In Windows:
      C:\xampp\htdocs\config\cloudconfig.php
      In Linux:
      /var/www/html/config/cloudconfig.php
   b. Add the setting in the format:

      ```
      define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND",directive:source,source;
      [directive:source,source;]);
      ```

      for example:

      ```
      define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND", "script-src:amazon.com;worker-
      src:amazon.com,google.com;");
      ```

6. If your system uses ServerLink, perform the following steps:
   a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
   b. Make backups of all nodes as needed.
   c. Stop the FileCloud ServerLink client service in secondary nodes.
   d. Upgrade the primary node first.
   e. Upgrade each secondary node after upgrading the primary node.

f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

- If your system uses MongoDB authentication or a custom IP binding, follow the steps at Disable MongoDB Authentication and IP Binding.

Upgrade instructions

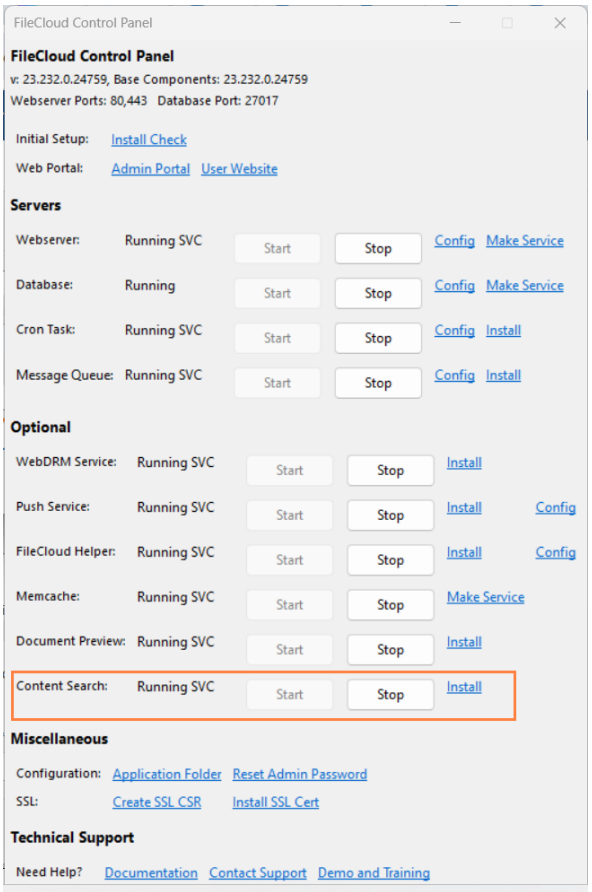
- The current version of the Windows Update Tool is 23.263.0.9354, which is effective for installing FileCloud Version 23.263.
- If you have a large installation, it is possible that your upgrade to version 23.263 may take longer than usual. This is due to pre-upgrade repair that is included with storage improvements and is to be expected.

1. Before running the upgrade tool, confirm that each of your FileCloud services is **running** and that your storage is in a **READY** state.
2. Use the Windows Upgrade tool to do a full upgrade. (You cannot upgrade using the admin portal.)
   ⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, but prior to restarting each of the nodes in the FileCloud Control Panel, add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
   Upgrade using Update Tool (Windows Only)
3. For all upgrades, once upgrade is complete, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.

Post Upgrade

Upgrade Windows environments using Solr and Solr+OCR

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 17.
3. Set JAVA_HOME to the new version's path.
4. Log in to the FileCloud admin portal.
5. In the FileCloud Control Panel, and stop and restart Content Search.



FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Windows: Upgrading Versions <23.252 to the Latest Version

If you are upgrading from version 23.252 or earlier use the following upgrade notes.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

- As always, make a full backup of your existing installation before upgrading.
  Backup FileCloud on Windows

- If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
- ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
  To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
- Please check all of the following conditions and see if any apply to the version you are updating from. For any that apply to you, take the specified step.
  - **If you are running a version of FileCloud below 23.242, and if you are running FileCloud in a high availability or multi-server environment**, verify that the MongoDB feature compatibility version is set to version 6. If not, set MongoDB feature compatibility to version 6 by following the instructions at https://www.mongodb.com/docs/manual/reference/command/setFeatureCompatibilityVersion/ or contacting FileCloud support.
  - **If your FileCloud installation uses admin portal user access restrictions,** follow the steps at Restricting Access To Admin UI Based On IP Addresses.
  - **If you are running a version of FileCloud below 23.1 and you have folder-level security enabled in Settings > Misc > General,** changes in functionality will significantly impact the way existing share behavior works when you upgrade.
    Please contact FileCloud Support before upgrading to avoid share and file access issues.
  - **If your system uses WebDAV**, please contact FileCloud Support before upgrading. Upgrading from a version prior to 23.241 to the current version completely disables WebDAV functionality.
  - **If your SSL certificate key is less than 2048 bits in length,** generate a new SSL certificate key of at least 2048 bits. For information, please Contact FileCloud Support (note that FileCloud support does not provide or generate certificates for customers).
  - **If you have enabled managed store encryption, and you have not yet changed your encryption from RC4, which has been deprecated, to AES256:**

    Follow the steps below this list under Windows: Upgrading Versions <23.252 to the Latest Version.
  - **If you are not running Windows Server 2019 or Windows Server 2022,** migrate your FileCloud site to one of these versions.
  - **If your Solr data with indexes was created using Solr version 7.x or older,** please do a full re-index.The version of Solr has been upgraded in FileCloud 23.232.
  - **If your system uses MongoDB authentication or custom IP binding**, follow the steps below this list at Windows: Upgrading Versions <23.252 to the Latest Version **.**
  - If you use an AD attribute other than **mail**, follow the steps below this list at Windows: Upgrading Versions <23.252 to the Latest Version .
  - **If you are using custom API services,** follow these steps below this list atWindows: Upgrading Versions <23.252 to the Latest Version**.**

- **If your system uses ServerLink,** follow these steps below this list at Windows: Upgrading Versions <23.252 to the Latest Version

Instructions for systems with custom rules in the file .htaccess

1. If you have added custom rules to the .htaccess file, they will be overridden by the dynamic CSP feature. To solve this:
   Either:
   Disable the dynamic CSP feature with the setting **TONIDOCLOUD_DYNAMIC_CSP_ENABLED**.
   See (23.263a) Dynamic CSP in FileCloud.
   Or:
   Add the custom rules to the setting **TONIDOCLOUD_DYNAMIC_CSP_EXTEND**.
   To add the custom rules:
   a. On the FileCloud Server, open the cloudconfig file:
      In Windows:
      C:\xampp\htdocs\config\cloudconfig.php
      In Linux:
      /var/www/html/config/cloudconfig.php
   b. Add the setting in the format:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND",directive:source,source;
[directive:source,source;]);
```

for example:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND", "script-src:amazon.com;worker-
src:amazon.com,google.com;");
```

Instructions for systems with managed storage encryption enabled

Instructions for systems with managed storage encryption enabled

If you have enabled managed store encryption, and you have not yet changed your encryption from RC4 to AES256:

You must change your storage encryption from RC4, which has been deprecated, to AES-256 prior to FileCloud upgrade. Your file key, a 183-character string used as a password for storage encryption, is stored in encrypted form in the FileCloud database. To change your file key encryption from RC4 to AES-256, use the following pre-upgrade instructions.

If you are not using managed storage encryption, you do not have to perform this process.

To change your storage encryption from RC4 to AES-256:

To view the correct version of the admin portal in the following procedure, either empty your browser cache or view in incognito mode.
To empty your browser cache, go to development mode, click refresh, and then choose **Empty cache and hard reload**.

1. If you are running FileCloud versions 22.1 through 23.232.x, skip this step, and go to step 2.
   If you are running a version of FileCloud less than 22.1:
   a. Upgrade FileCloud to 23.232.1.
   b. Activate encrypted storage for your site (or each of your sites) by providing a password or recovery key.
      For help activating encrypted storage, see: Activating Password Protected Storage Encryption - FileCloud Docs - Server.
      To learn more about setting up encryption in FileCloud see Setting up Managed Storage Encryption - FileCloud Docs - Server.
2. (**Begin here for FileCloud Versions 22.1 through 23.232.x**)
   Ensure that encrypted storage is activated for your site (or each site you are running in a multitenant environment) by confirming that Memcache is running on your FileCloud server and that each of your sites has the raw file key stored in the Memcache service.
3. Ensure that any other FileCloud services you use are running.
4. Take a snapshot of your production server before running the pre-upgrade tool.
   If possible, further safeguard your data by initially performing this pre-upgrade in a staging environment.
5. Run the pre-upgrade tool:
   - For Windows systems: Run upgrade as you would using the instructions on page Upgrade using Update Tool (Windows Only).
6. When the pre-upgrade is successfully completed, manually activate storage encryption for your site (or each of your sites in a multi-tenant environment).
   a. During this step, you may optionally enter a new encryption password to encrypt the RAW key stored in AES-256 instead of RC4 (however, the same password may be used).

Troubleshooting encryption pre-upgrades

PROBLEM:
The pre-upgrade tool returns a STOP result.
This may happen when the Memcache service is turned off or if a site with encrypted storage is inactive, and potentially leads to loss of the raw file key from Memcache and deactivation of encrypted storage.
SOLUTION:
Run the Memcache service to ensure that storage encryption is activated, then run the pre-upgrade tool again.

PROBLEM:
Wrong File Key for Multi-Tenant Environments. For multi-tenant environments, the pre-upgrade tool might retrieve the wrong File Key for sites, leading to data loss.

SOLUTION:
Ensure storage encryption is activated by running the Memcache service. If the wrong File Key is retrieved for multi-tenant environments, decrypt the data, disable encryption, perform the upgrade, and then re-enable encryption.

PROBLEM:
One inactive website with encrypted storage blocks upgrades on all other websites.
SOLUTION:
Decrypt and disable encryption, then perform a site database backup, and remove the unused site.

PROBLEM:
Service Provider Licensing Agreement (SPLA) admin lacks options to enable inactive encrypted storage.
SOLUTION:
Ensure you have access to the storage system in SPLA admin settings.

If you are upgrading to the latest FileCloud version and you are using a custom mongodb.conf

If you are upgrading to the latest FileCloud version and you are using a custom mongodb.conf

If you are running mongoDB as a service in Windows and updating from a version of FileCloud earlier than 23.242 to the latest version, and you are replacing the provided mongodb.conf with a custom one, it is important that you remove the **journal=true** setting which is no longer supported.

To remove the command:

1. Open C:\\xampp\mongodb\mongodb.conf.

2. Delete the lines that are highlighted in the image below and save the file.

Mongodb configuration file

```
# mongodb.conf

# Where to store the data.
dbpath=C:\xampp\mongodb\bin\data

#where to log
logpath=C:\xampp\mongodb\bin\log\mongodb.log

#append log
logappend=true

#ip address
bind_ip = 127.0.0.1
port = 27017

# Enable journaling, http://www.mongodb.org/display/DOCS/Journaling
journal=true

# Don't show mongodb http interface
nohttpinterface=true

# Enable mongodb rest interface
rest=false

#quiet mode
quiet=true
```

If you are upgrading to the latest version and you are using custom API services

If you are upgrading to the latest version and you are using custom API services

If you are using custom API services, the services may be logged out after the session timeout time (15 minutes by default). To prevent this from happening, in your custom API code, in requests to the FileCloud API, change your user-agent header to contain the string "FileCloud API". This is a one-time change only required when you upgrade from a version prior to 23.242 to the latest version.
Examples:
In PHP script, change:

```
// Set the custom User-Agent header
curl_setopt($ch, CURLOPT_HTTPHEADER, [
    "User-Agent: CustomUserAgent/1.0"
]);
```

to:

```
// Set the custom User-Agent header
curl_setopt($ch, CURLOPT_HTTPHEADER, [
    "User-Agent: FileCloud API"
]);
```

In CLI, change:

```
curl -X GET https://filecloud-domain.com/core/getfilelist -H "User-Agent:
CustomUserAgent/1.0"
```

to:

```
curl -X GET https://filecloud-domain.com/core/getfilelist -H "User-Agent: FileCloud
API"
```

Upgrading systems that use ServerLink

Upgrading systems that use ServerLink

To upgrade systems running ServerLink, the following steps should be taken:

1. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
2. Make backups of all nodes as needed.
3. Stop the FileCloud ServerLink client service in secondary nodes.
4. Upgrade the primary node first.
5. Upgrade each secondary node after upgrading the primary node.
6. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Correcting the AD mail attribute

Correcting the AD mail attribute

Prior to version 23.241, FileCloud always used the AD attribute **mail** to authenticate AD users, even if the **AD mail attribute** field in FileCloud specified a different attribute.

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

Upgrade instructions

- The current version of the Windows Update Tool is 23.263.0.9354, which is effective for installing FileCloud Version 23.263.
- If you have a large installation, it is possible that your upgrade to version 23.263 may take longer than usual. This is due to pre-upgrade repair that is included with storage improvements and is to be expected.

1. When you are upgrading to the latest version, leave all FileCloud services in the control panel running.
2. If you are upgrading from FileCloud 23.241, in addition to confirming that each of your FileCloud services is running, make sure that your storage is in a **READY** state.
3. Use the upgrade tool to do a full upgrade.
   ⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, but prior to restarting each of the nodes in the FileCloud Control Panel, add the folder `C:\xampp\htdocs\scratch\tmp` to avoid any issues.
   Upgrade using Update Tool (Windows Only)
4. For all upgrades, once upgrade is complete, refresh the browser using CTRL-F5 to clear any prior setup information from the cache.

Post Upgrade

1. If you are running in a high availability or multi-server environment manually set the MongoDB feature compatibility version to version 7. Use the instructions at https://www.mongodb.com/docs/manual/reference/command/setFeatureCompatibilityVersion/ or contact FileCloud support.
2. Beginning with version 23.252, a new group, **Externals**, automatically includes all External users, and the **Everyone** group does not include External users. External users who were include in the Everyone group in earlier versions of FileCloud are no longer included in it.

   The **Externals** group functions to prevent External users from having the same share, folder, and policy access as users in the Everyone group.

Previously created DLP rules that denied access to the Everyone group will now deny access to both the Everyone and Externals groups. Previously created DLP rules that allowed access to the Everyone group will continue to allow access to the Everyone group and not to the Externals group.

If your use cases require that external users have the same access to files and folders as other users, you can give the Externals group the same permissions as the Everyone group by running the tool **assignexternalsgroup.php**. See Assign the Externals Group the Same File Access as the Everyone Group for help.

3. Beginning in FileCloud 23.253, by default, a more granular dynamic content security policy replaces the existing content security policy in the .htaccess file. If you are upgrading, to make this change effective, you must make a small change to the Content-Security-Policy header in the .htaccess file:
   - Open the .htaccess file.
     C:\xampp\htdocs\.htaccess
   - Find the line that begins:
     Header set Content-Security-Policy:
   - Change set to setifempty:
     Header setifempty Content-Security-Policy:

```
<IfModule mod_headers.c>
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header setifempty Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com *.skype.com *.autodesk.com; \
    frame-src 'self' blob: www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net *.autodesk.com; \
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com; \
    worker-src 'self' blob: *.autodesk.com"
```

4. If you plan to update to the new FileCloud Outlook Add-in, see Windows: Upgrading Versions <23.252 to the Latest Version .
5. If you are upgrading FileCloud from a version below 23.241 and your system uses SSO, follow the instructions below in Windows: Upgrading Versions <23.252 to the Latest Version
   This is necessary because Version 23.241.x of FileCloud dropped support for Shibboleth 1.3 and SAML 1.1, and updated SimpleSAML to version 2.x.
6. If you are upgrading from a version prior to 23.1 and upgrading to a system running with MongoDB replica set or standalone MongoDB, follow the steps in Windows: Upgrading Versions <23.252 to the Latest Version
7. If you are using Solr, follow the steps below under https://filecloudddocs.atlassian.net/wiki/spaces/FH/pages/edit-v2/114556973#Upgrade-Windows-environments-using-Solr-and-Solr%2BOCR .
8. Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Upgrade instructions for the FileCloud 23.242 Outlook Add-in

Upgrade instructions for the FileCloud 23.242 Outlook Add-in

If you are upgrading FileCloud, and you plan to use the updated FileCloud Outlook Add-in, if you have previously modified the default values for **Access-Control-Allow-origin** or **Access-Control-Allow-Credentials**, they may not be set to the values required to run the FileCloud Outlook Add-in. After updating the Outlook Add-in, open .htaccess and make sure these settings have the values indicated below.

To check/replace the htaccess settings:

1. Open the .htacess file:
   `Windows:  C:\xampp\htdocs\.htaccess`
2. If the following commands are missing or are present, but set to different values, set them as follows:

```
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
```

Configuring SSO after updating from a version older than 23.241

Configuring SSO after updating from a version older than 23.241

SimpleSAML update

Version 23.241.x of FileCloud has updated SimpleSAML to version 2.x. If your FileCloud build uses SSO, please take the following steps to replace your old configuration files with new ones; otherwise, SSO will not work correctly in your system.

1. Go to your SimpleSAML config directory.
   Windows: **C:xampp\htdocs\thirdparty\simplesaml\config**
   Linux: **/var/www/html/thirdparty/simplesaml/config**
2. Rename:
   config.php to **config.php.bak**
   authsources.php to **authsources.php.bak**
3. Then rename:
   config.php-[date] to **config.php**
   authsources.php-[date] to **authsources.php**
4. Copy any modifications you made to the original **config.php** (now **config.php.bak**) to the current **config.php**
5. Copy any modifications you made to the original **authsources.php** (now **authsoruces.php.bak**) to the current **authsources.php**

Alias directive modification

The Alias directive has been modified in 23.241. If you have it written as:

```
Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/thirdparty/www"
```

change it to:

```
Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/public"
```

for more information, see SSO Configuration Steps, Step 1. Configure Apache Webserver.

FC Push Service Configuration

FC Push Service Configuration

In FileCloud version 23.1, a Push service was added to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload, share). If you are upgrading from a version prior to 23.1, upgrading to the latest version on systems running with MongoDB replica set or standalone MongoDB require the push service **env** file to be updated based on the MongoDB configuration.

To configure the Push service in Windows:

1. Open the file **xampp\pushservice\.env** for edit.
2. Update the MongoDB connection string to:

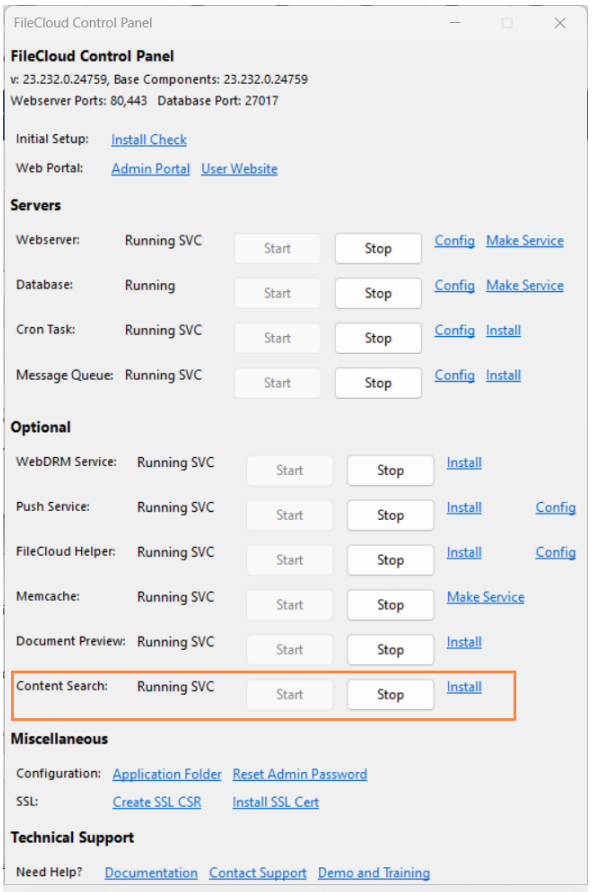
   ```
   FCPS_DB_DSN=mongodb://dbuser:passw0rd1@ dbserver01, dbserver02, dbserver03:27017
   ```

3. Restart the Push service in the FileCloud control panel.

Upgrade Windows environments using Solr and Solr+OCR

Upgrade Windows environments using Solr and Solr+OCR

1. Upgrade FileCloud
2. Upgrade OpenJDK to version 17.
3. Set JAVA_HOME to the new version's path.
4. Log in to the FileCloud admin portal.
5. In the FileCloud Control Panel, and stop and restart Content Search.



Linux: Upgrading from 23.262 to the Latest Version

> The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

> Prior to upgrade, confirm that your SSL certificate and your SSL private key are in the correct directory:
> Ubuntu: /etc/apache2/ssl
> RHEL: /etc/httpd/ssl
> See Install an SSL Certificate on Linux.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

- As always, make a full backup of your existing installation before upgrading.
  Backup on Linux
- If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
- ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
  To perform the necessary prerequisites and access troubleshooting information, please review:
  FileCloud Storage Upgrade Guide 10-1-2026.pdf .
- If you initially installed FileCloud before version 23.242
  AND
  You have not upgraded to FileCloud version 23.261.1 or 23.261.2
  You must change your MongoDB Feature Compatibility Version from 6.0 to 7.0 by running the applicable command below, or MongoDB will not start.

  If MongoDB authentication is not enabled:

  ```
  mongosh --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

  If MongoDB authentication is enabled:
  (Replace PASSWORD with your MongoDB admin password)

  ```
  mongosh -u admin -p 'PASSWORD' --authenticationDatabase admin \
    --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

  After you run one of the above commands, verify that the current Feature Compatibility Version is 7.0 by running the following command and checking the value it returns:

  ```
  mongosh --quiet --eval
  'db.adminCommand({getParameter:1,featureCompatibilityVersion:1})'
  ```

- If you are using native LDAP for authentication and using non-TLS connections set the LDAP Host value to ldap://hostname. Older FileCloud versions supported host value without the protocol definition ldap://
- If your system uses ServerLink, follow these steps:
  a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
  b. Make backups of all nodes as needed.
  c. Stop the FileCloud ServerLink client service in secondary nodes.
  d. Upgrade the primary node first.
  e. Upgrade each secondary node after upgrading the primary node.
  f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Upgrade instructions

- Upgrade using the steps at Upgrade FileCloud on Linux .

Post-upgrade

Add ../scratch/tmp folder

⚠️ The folder ../scratch/tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, add the folder **/var/www/html/scratch/tmp** to avoid any issues.

FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Linux: Upgrading from 23.261 to the Latest Version

> The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

> Prior to upgrade, confirm that your SSL certificate and your SSL private key are in the correct directory:
> Ubuntu: /etc/apache2/ssl
> RHEL: /etc/httpd/ssl
> See Install an SSL Certificate on Linux.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

- As always, make a full backup of your existing installation before upgrading.
  Backup on Linux
- If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
- ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
  To perform the necessary prerequisites and access troubleshooting information, please review:
  FileCloud Storage Upgrade Guide 10-1-2026.pdf .
- If you initially installed FileCloud before version 23.242
  AND
  You have not upgraded to FileCloud version 23.261.1 or 23.261.2
  You must change your MongoDB Feature Compatibility Version from 6.0 to 7.0 by running the applicable command below, or MongoDB will not start.

  If MongoDB authentication is not enabled:

  ```
  mongosh --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

  If MongoDB authentication is enabled:
  (Replace PASSWORD with your MongoDB admin password)

  ```
  mongosh -u admin -p 'PASSWORD' --authenticationDatabase admin \
    --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

After you run one of the above commands, verify that the current Feature Compatibility Version is 7.0 by running the following command and checking the value it returns:

```
mongosh --quiet --eval
'db.adminCommand({getParameter:1,featureCompatibilityVersion:1})'
```

- If you are using native LDAP for authentication and using non-TLS connections set the LDAP Host value to ldap://hostname. Older FileCloud versions supported host value without the protocol definition ldap://
- If your system uses ServerLink, follow these steps:
  a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
  b. Make backups of all nodes as needed.
  c. Stop the FileCloud ServerLink client service in secondary nodes.
  d. Upgrade the primary node first.
  e. Upgrade each secondary node after upgrading the primary node.
  f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Upgrade instructions

- Upgrade using the steps at Upgrade FileCloud on Linux .

Post-upgrade

Add ../scratch/tmp folder

⚠️ The folder ../scratch/tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, add the folder **/var/www/html/scratch/tmp** to avoid any issues.

FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Linux: Upgrading from 23.253 to the Latest Version

The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

Prior to upgrade, confirm that your SSL certificate and your SSL private key are in the correct directory:
Ubuntu: /etc/apache2/ssl
RHEL: /etc/httpd/ssl
See Install an SSL Certificate on Linux.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

- As always, make a full backup of your existing installation before upgrading.
  Backup on Linux
- If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
- ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
  To perform the necessary prerequisites and access troubleshooting information, please review:
  FileCloud Storage Upgrade Guide 10-1-2026.pdf .
- If you initially installed FileCloud before version 23.242
  AND
  You have not upgraded to FileCloud version 23.261.1 or 23.261.2
  You must change your MongoDB Feature Compatibility Version from 6.0 to 7.0 by running the applicable command below, or MongoDB will not start.

  If MongoDB authentication is not enabled:

  ```
  mongosh --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

If MongoDB authentication is enabled:
(Replace PASSWORD with your MongoDB admin password)

```
mongosh -u admin -p 'PASSWORD' --authenticationDatabase admin \
  --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
```

After you run one of the above commands, verify that the current Feature Compatibility Version is 7.0 by running the following command and checking the value it returns:

```
mongosh --quiet --eval
'db.adminCommand({getParameter:1,featureCompatibilityVersion:1})'
```

- If you are using native LDAP for authentication and using non-TLS connections set the LDAP Host value to ldap://hostname. Older FileCloud versions supported host value without the protocol definition ldap://
- If your system uses ServerLink, follow these steps:
  a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
  b. Make backups of all nodes as needed.
  c. Stop the FileCloud ServerLink client service in secondary nodes.
  d. Upgrade the primary node first.
  e. Upgrade each secondary node after upgrading the primary node.
  f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Upgrade instructions

- Upgrade using the steps at Upgrade FileCloud on Linux .

Post-upgrade

Add ../scratch/tmp folder

⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, add the folder **/var/www/html/scratch/tmp** to avoid any issues.

FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Linux: Upgrading from 23.252 to the Latest Version

> The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

> Prior to upgrade, confirm that your SSL certificate and your SSL private key are in the correct directory:
> Ubuntu: /etc/apache2/ssl
> RHEL: /etc/httpd/ssl
> See Install an SSL Certificate on Linux.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

1. As always, make a full backup of your existing installation before upgrading.
   Backup on Linux
2. If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.
3. ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
   To perform the necessary prerequisites and access troubleshooting information, please review:
   FileCloud Storage Upgrade Guide 10-1-2026.pdf .
4. If you initially installed FileCloud before version 23.242
   AND
   You have not upgraded to FileCloud version 23.261.1 or 23.261.2
   You must change your MongoDB Feature Compatibility Version from 6.0 to 7.0 by running the applicable command below, or MongoDB will not start.

   If MongoDB authentication is not enabled:

```
mongosh --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
```

If MongoDB authentication is enabled:
(Replace PASSWORD with your MongoDB admin password)

```
mongosh -u admin -p 'PASSWORD' --authenticationDatabase admin \
  --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
```

After you run one of the above commands, verify that the current Feature Compatibility Version is 7.0 by running the following command and checking the value it returns:

```
mongosh --quiet --eval
'db.adminCommand({getParameter:1,featureCompatibilityVersion:1})'
```

5. If you are using native LDAP for authentication and using non-TLS connections set the LDAP Host value to ldap://hostname. Older FileCloud versions supported host value without the protocol definition ldap://
6. Beginning in FileCloud 23.253, by default, a more granular dynamic content security policy replaces the existing content security policy in the .htaccess file. If you are upgrading, to make this change effective, you must make a small change to the Content-Security-Policy header in the .htaccess file:
   - Open the .htaccess file.

     in Windows:
     C:\xampp\htdocs\.htaccess

     in Linux:
     /var/www/html/.htaccess
   - Find the line that begins:
     Header set Content-Security-Policy:
   - Change set to setifempty:
     Header setifempty Content-Security-Policy:

```
<IfModule mod_headers.c>
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header setifempty Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com *.skype.com *.autodesk.com; \
    frame-src 'self' blob: www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net *.autodesk.com; \
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com; \
    worker-src 'self' blob: *.autodesk.com"
```

7. If you have added custom rules to the .htaccess file, they will be overridden by the dynamic CSP feature. To solve this:
   Either:
   Disable the dynamic CSP feature with the setting **TONIDOCLOUD_DYNAMIC_CSP_ENABLED**.
   See (23.263a) Dynamic CSP in FileCloud.
   Or:
   Add the custom rules to the setting **TONIDOCLOUD_DYNAMIC_CSP_EXTEND**.
   To add the custom rules:
   a. On the FileCloud Server, open the cloudconfig file:
      In Windows:
      C:\xampp\htdocs\config\cloudconfig.php
      In Linux:
      /var/www/html/config/cloudconfig.php
   b. Add the setting in the format:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND",directive:source,source;
[directive:source,source;]);
```

      for example:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND", "script-src:amazon.com;worker-
src:amazon.com,google.com;");
```

8. If your system uses ServerLink, follow these steps:
   a. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
   b. Make backups of all nodes as needed.
   c. Stop the FileCloud ServerLink client service in secondary nodes.
   d. Upgrade the primary node first.
   e. Upgrade each secondary node after upgrading the primary node.
   f. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Upgrade instructions

- Upgrade using the steps at Upgrade FileCloud on Linux.

Post-upgrade

Add ../scratch/tmp folder

⚠️ The folder ..\scratch\tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, add the folder **/var/www/html/scratch/tmp** to avoid any issues.

FileCloud iOS mobile users

Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Linux: Upgrading from Versions <23.252 to the Latest Version

If you are upgrading from version 23.241 or earlier use the following upgrade notes.

> The current version of FileCloud is FIPS 140-3 compliant when running in FIPS mode on Ubuntu Pro 22.04.

> Prior to upgrade, confirm that your SSL certificate and your SSL private key are in the correct directory:
> Ubuntu: /etc/apache2/ssl
> RHEL: /etc/httpd/ssl
> See Install an SSL Certificate on Linux.

If you are running FileCloud in a high availability environment, to upgrade to the latest version, please Contact FileCloud Support.

FileCloud Support can help you upgrade or can provide a PDF with instructions if you would like to perform the upgrade without assistance.

Pre-upgrade

- As always, make a full backup of your existing installation before upgrading.
  Backup FileCloud on Linux
- If you are running in a high-availability environment with separate MongoDB servers, upgrade to MongoDB version 8 if you have not upgraded already. Please Contact FileCloud Support if you need more information.

- ⚠️ When users upgrade from FileCloud version 23.262 or earlier to versions 23.263 and later, the upgrade process restructures storage in FileCloud. It is particularly important that you back up MongoDB prior to this upgrade. Due to changes in the way FileCloud stores folders, redundant values and inconsistent records are permanently removed from the storage database.
  To perform the necessary prerequisites and access troubleshooting information, please review: FileCloud Storage Upgrade Guide 10-1-2026.pdf .
- If you initially installed FileCloud before version 23.242
  AND
  You have not upgraded to FileCloud version 23.261.1 or 23.261.2
  You must change your MongoDB Feature Compatibility Version from 6.0 to 7.0 by running the applicable command below, or MongoDB will not start.

  If MongoDB authentication is not enabled:

  ```
  mongosh --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

  If MongoDB authentication is enabled:
  (Replace PASSWORD with your MongoDB admin password)

  ```
  mongosh -u admin -p 'PASSWORD' --authenticationDatabase admin \
    --eval 'db.adminCommand({setFeatureCompatibilityVersion: "7.0"})'
  ```

  After you run one of the above commands, verify that the current Feature Compatibility Version is 7.0 by running the following command and checking the value it returns:

  ```
  mongosh --quiet --eval
  'db.adminCommand({getParameter:1,featureCompatibilityVersion:1})'
  ```

- Please check all of the following conditions and see if any apply to the version you are updating from. For any that apply to you, take the specified step.
  - **If you are running FileCloud in a high availability or multi-server environment**, verify that the MongoDB feature compatibility version is set to version 6. If not, set MongoDB feature compatibility to version 6 by following the instructions at https://www.mongodb.com/docs/manual/reference/command/setFeatureCompatibilityVersion/ or contacting FileCloud support.
  - **If your installation of FileCloud uses admin portal user access restrictions,** please see Restricting Access To Admin UI Based On IP Addresses for updated instructions.
  - **If you are running a version below 23.1 and have granular folder permissions set,** please contact FileCloud Support before upgrading to avoid share and file access issues.

Changes in functionality will significantly impact the way existing share behavior works when you upgrade.

- **If your system uses WebDAV, please contact FileCloud Support before upgrading.** Upgrading to the current version completely disables WebDAV functionality.
- **If your SSL certificate key is less than 2048 bits in length, generate a new SSL certificate key of at least 2048 bits.** For information, please Contact FileCloud Support (note that FileCloud support does not provide or generate certificates for customers).
- **If you have enabled managed store encryption, and you have not yet changed your encryption from RC4, which has been deprecated, to AES256:**

  Follow the steps below under Linux: Upgrading from Versions <23.252 to the Latest Version
- **If you are using Ubuntu 18.04/20.04, CentOS 7/RHEL 7 and RHEL 8,** please migrate to Ubuntu 22.04 LTS or RHEL 9.
- **If you are updating from a version prior to 23.241, to enable access to FileCloud, redownload and reinstall your license.** See Install the FileCloud License for help.
- **If you are using native LDAP for authentication and using non-TLS connections,** set the LDAP Host value to ldap://hostname. Older FileCloud versions supported host value without the protocol definition ldap://
- **Upgrade to the latest supported Version of MongoDB Version 7.**
  If your CPU does not have the AVX instruction set, MongoDB 7 (and MongoDB 6) will not run.
  To check whether your CPU has the instruction set, run:
  #lscpu | grep -i avx"

If you do not have the AVX instruction set, install one of the select Intel and AMD processors.

- **If your system uses custom API services,** follow the instructions below this list under Linux: Upgrading from Versions <23.252 to the Latest Version
- **If your system uses ServerLink,** follow the instructions below this list under Linux: Upgrading from Versions <23.252 to the Latest Version
- **If you use an AD attribute other than mail,** follow the steps below this list underLinux: Upgrading from Versions <23.252 to the Latest Version .

Instructions for systems with custom rules in the file .htaccess

1. If you have added custom rules to the .htaccess file, they will be overridden by the dynamic CSP feature. To solve this:
   Either:
   Disable the dynamic CSP feature with the setting **TONIDOCLOUD_DYNAMIC_CSP_ENABLED**.
   See (23.263a) Dynamic CSP in FileCloud.

   Or:
   Add the custom rules to the setting **TONIDOCLOUD_DYNAMIC_CSP_EXTEND**.

   To add the custom rules:

   a. On the FileCloud Server, open the cloudconfig file:

In Windows:
C:\xampp\htdocs\config\cloudconfig.php

In Linux:

/var/www/html/config/cloudconfig.php

b. Add the setting in the format:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND",directive:source,source;
[directive:source,source;]);
```

for example:

```
define("TONIDOCLOUD_DYNAMIC_CSP_EXTEND", "script-src:amazon.com;worker-
src:amazon.com,google.com;");
```

Instructions for systems with managed storage encryption enabled

Instructions for systems with managed storage encryption enabled

If you have enabled managed store encryption, and you have not yet changed your encryption from RC4 to AES256:

You must change your storage encryption from RC4, which has been deprecated, to AES-256 prior to FileCloud upgrade. Your file key, a 183-character string used as a password for storage encryption, is stored in encrypted form in the FileCloud database. To change your file key encryption from RC4 to AES-256, use the following pre-upgrade instructions.

If you are not using managed storage encryption, you do not have to perform this process.

To change your storage encryption from RC4 to AES-256:

To view the correct version of the admin portal in the following procedure, either empty your browser cache or view in incognito mode.
To empty your browser cache, go to development mode, click refresh, and then choose **Empty cache and hard reload**.

If your system is running in Linux and you are migrating to a new FileCloud server from FileCloud 22.1, go to the section Migrating FileCloud 22.1 with local encryption storage to Ubuntu 22.04 and RHEL 9, below.

1. If you are running FileCloud versions 22.1 through 23.232.x, skip this step, and go to step 2.
   If you are running a version of FileCloud less than 22.1:
   a. Upgrade FileCloud to 23.232.1.

   b. Activate encrypted storage for your site (or each of your sites) by providing a password or recovery key.
      For help activating encrypted storage, see: Activating Password Protected Storage Encryption - FileCloud Docs - Server.
      To learn more about setting up encryption in FileCloud see Setting up Managed Storage Encryption - FileCloud Docs - Server.

2. (**Begin here for FileCloud Versions 22.1 through 23.232.x**)
   Ensure that encrypted storage is activated for your site (or each site you are running in a multitenant environment) by confirming that Memcache is running on your FileCloud server and that each of your sites has the raw file key stored in the Memcache service.
3. Ensure that any other FileCloud services you use are running.
4. Take a snapshot of your production server before running the pre-upgrade tool.
   If possible, further safeguard your data by initially performing this pre-upgrade in a staging environment.
5. Run the pre-upgrade tool:
   - For Linux systems:
     Download the latest version of **filecloudcp** by running this command:

     ```
     curl --location 'repo.filecloudlabs.com/static/fcp/filecloudcp' -o /usr/bin/filecloudcp
     ```

     Set the correct permissions for the file by running:

     ```
     chmod 755 /usr/bin/filecloudcp
     ```

     Start the pre-upgrade tool by running:

     ```
     filecloudcp -fpm
     ```

6. When the pre-upgrade is successfully completed, manually activate storage encryption for your site (or each of your sites in a multi-tenant environment).
   a. During this step, you may optionally enter a new encryption password to encrypt the RAW key stored in AES-256 instead of RC4 (however, the same password may be used).

Troubleshooting encryption pre-upgrades

PROBLEM:
The pre-upgrade tool returns a STOP result.
This may happen when the Memcache service is turned off or if a site with encrypted storage is inactive, and potentially leads to loss of the raw file key from Memcache and deactivation of encrypted

storage.
SOLUTION:
Run the Memcache service to ensure that storage encryption is activated, then run the pre-upgrade tool again.

PROBLEM:
Wrong File Key for Multi-Tenant Environments. For multi-tenant environments, the pre-upgrade tool might retrieve the wrong File Key for sites, leading to data loss.
SOLUTION:
Ensure storage encryption is activated by running the Memcache service. If the wrong File Key is retrieved for multi-tenant environments, decrypt the data, disable encryption, perform the upgrade, and then re-enable encryption.

PROBLEM:
One inactive website with encrypted storage blocks upgrades on all other websites.
SOLUTION:
Decrypt and disable encryption, then perform a site database backup, and remove the unused site.

PROBLEM:
Service Provider Licensing Agreement (SPLA) admin lacks options to enable inactive encrypted storage.
SOLUTION:
Ensure you have access to the storage system in SPLA admin settings.

Migrating FileCloud 22.1 with managed storage and encryption enabled to Ubuntu 22.04 or RHEL 9

Follow one of the options to migrate FileCloud 22.1 to an updated operating system and to upgrade it to the current version.

Option 1: For customers running with or without FIPS mode: (recommended option):
Note: Customers who are using encrypted Managed Storage and running FileCloud on RHEL9 in FIPS-enabled mode should not upgrade to FileCloud versions 23.242 and 23.251.

1. Decrypt the files in FileCloud 22.1
2. Install one of the supported operating systems (Ubuntu 22.04 or RHEL 9).
3. Install FileCloud on Linux on the newly installed operating system.
4. Migrate FileCloud to the newly installed operating system.
5. Encrypt the data in FileCloud.

Option 2: For customers running without FIPS mode:
This method does not require decryption.

1. Perform a FileCloud upgrade to FileCloud 23.232.1, which requires OS upgrades to Ubuntu 22.04 or RHEL 9.x. For this procedure, please Contact FileCloud Support.
2. Follow the upgrade instructions on page Upgrade FileCloud on Linux.
   Please note that FileCloud Support cannot resolve OS upgrade problems.

If you are upgrading to the latest version and you are using custom API services

If you are upgrading to the latest version and you are using custom API services

If you are using custom API services, the services may be logged out after the session timeout time (15 minutes by default). To prevent this from happening, in your custom API code, in requests to the FileCloud API, change your user-agent header to contain the string "FileCloud API". This is a one-time change only required when you upgrade from a version prior to 23.242 to the latest version.
Examples:
In PHP script, change:

```
// Set the custom User-Agent header
curl_setopt($ch, CURLOPT_HTTPHEADER, [
    "User-Agent: CustomUserAgent/1.0"
]);
```

to:

```
// Set the custom User-Agent header
curl_setopt($ch, CURLOPT_HTTPHEADER, [
    "User-Agent: FileCloud API"
]);
```

In CLI, change:

```
curl -X GET https://filecloud-domain.com/core/getfilelist -H "User-Agent:
CustomUserAgent/1.0"
```

to:

```
curl -X GET https://filecloud-domain.com/core/getfilelist -H "User-Agent: FileCloud
API"
```

Upgrading systems that use ServerLink

Upgrading systems that use ServerLink

To upgrade systems running ServerLink, the following steps should be taken:

1. Before upgrade, ensure all ServerLink nodes are fully synced and are at the same state.
2. Make backups of all nodes as needed.
3. Stop the FileCloud ServerLink client service in secondary nodes.
4. Upgrade the primary node first.
5. Upgrade each secondary node after upgrading the primary node.
6. Start the FileCloud ServerLink client service in secondary nodes. (In HA setups, client service must run only in one of the servers from each secondary node.)

Note: All connected ServerLink nodes, both primary and secondary, must be upgraded to the same FileCloud version before enabling access to the site again.

Correcting the AD mail attribute

Correcting the AD mail attribute

Prior to version 23.241, FileCloud always used the AD attribute **mail** to authenticate AD users, even if the **AD mail attribute** field in FileCloud specified a different attribute.

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

Upgrade instructions

Upgrading FileCloud from 23.232.x and higher to the latest version

To upgrade FileCloud from 23.232.x and higher to the latest version in Linux see Upgrade FileCloud on Linux .

Upgrading FileCloud from 22.1 to Ubuntu 22.04 and RHEL 9

You can either re-install FileCloud or upgrade both FileCloud and your operating system.

Option 1: Install one of the supported operating systems, then Install the latest version of FileCloud on the newly installed operating system, and then migrate FileCloud to the newly installed operating system. This is the recommended option.

Option 2: Perform a FileCloud upgrade which requires OS upgrades to Ubuntu 22.04 or RHEL 9.x, For this procedure, please Contact FileCloud Support.
Please note that FileCloud Support cannot resolve OS upgrade problems.

Upgrading FileCloud from versions lower than 22.1

If you are upgrading from a version of FileCloud lower than 22.1 or from an operating system below Ubuntu 22.04 LTS or RHEL 9, please install one of the supported operating systems, then Install the

latest version of FileCloud on the newly installed operating system, and then migrate FileCloud to the newly installed operating system.

Post Upgrade

1. The folder ../scratch/tmp is not recreated in FileCloud, causing the system to fail to save necessary short-term data. After FileCloud is upgraded, add the folder **/var/www/html/scratch/tmp** to avoid any issues.
2. If you are running in a high availability or multi-server environment manually set the MongoDB feature compatibility version to version 7. Use the instructions at https://www.mongodb.com/docs/manual/reference/command/setFeatureCompatibilityVersion/ or contact FileCloud support.
3. Beginning with version 23.252, a new group, **Externals**, automatically includes all External users, and the **Everyone** group does not include External users. External users who were include in the Everyone group in earlier versions of FileCloud are no longer included in it.

   The **Externals** group functions to prevent External users from having the same share, folder, and policy access as users in the Everyone group.

   Previously created DLP rules that denied access to the Everyone group will now deny access to both the Everyone and Externals groups. Previously created DLP rules that allowed access to the Everyone group will continue to allow access to the Everyone group and not to the Externals group.

   If your use cases require that external users have the same access to files and folders as other users, you can give the Externals group the same permissions as the Everyone group by running the tool **assignexternalsgroup.php**. See Assign the Externals Group the Same File Access as the Everyone Group for help.
4. Beginning in FileCloud 23.253, by default, a more granular dynamic content security policy replaces the existing content security policy in the .htaccess file. If you are upgrading, to make this change effective, you must make a small change to the Content-Security-Policy header in the .htaccess file:
   - Open the .htaccess file.

     in Windows:
     C:\xampp\htdocs\.htaccess

     in Linux:
     /var/www/html/.htaccess
   - Find the line that begins:
     Header set Content-Security-Policy:
   - Change set to setifempty:
     Header setifempty Content-Security-Policy:

```
<IfModule mod_headers.c>
Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
Header set Access-Control-Allow-Credentials true
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header setifempty Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    connect-src 'self' *.amazonaws.com *.core.windows.net blob: data: http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com *.skype.com *.autodesk.com; \
    frame-src 'self' blob: www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net *.autodesk.com; \
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com; \
    worker-src 'self' blob: *.autodesk.com"
```

5. If you are upgrading FileCloud from a version below 23.241 and your system uses SSO, follow the instructions below in Linux: Upgrading from Versions <23.252 to the Latest Version
   This is necessary because Version 23.241.x of FileCloud dropped support for Shibboleth 1.3 and SAML 1.1, and updated SimpleSAML to version 2.x.
6. If you plan to update to the new FileCloud Outlook Add-in, follow the instructions below inLinux: Upgrading from Versions <23.252 to the Latest Version
7. If you are upgrading from a version prior to 23.1 or upgrading on a system running with MongoDB replica set or standalone MongoDB follow the instructions below in Linux: Upgrading from Versions <23.252 to the Latest Version .
8. Beginning with FileCloud Server version 23.261, iOS users must be on iOS 16+ and app version 23.261+.

Configuring SSO after updating from a version older than 23.241

Configuring SSO after updating from a version older than 23.241

SimpleSAML update

Version 23.241.x of FileCloud has updated SimpleSAML to version 2.x. If your FileCloud build uses SSO, please take the following steps to replace your old configuration files with new ones; otherwise, SSO will not work correctly in your system.

1. Go to your SimpleSAML config directory.
   Linux: **/var/www/html/thirdparty/simplesaml/config**
2. Rename:
   config.php to **config.php.bak**
   authsources.php to **authsources.php.bak**
3. Then rename:
   config.php-[date] to **config.php**
   authsources.php-[date] to **authsources.php**
4. Copy any modifications you made to the original **config.php** (now **config.php.bak**) to the current **config.php**
5. Copy any modifications you made to the original **authsources.php** (now **authsoruces.php.bak**) to the current **authsources.php**

Alias directive modification

The Alias directive has been modified in 23.241. If you have it written as:

```
Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/thirdparty/www"
```

change it to:

```
Alias /simplesaml "/xampp/htdocs/thirdparty/simplesaml/public"
```

for more information, see SSO Configuration Steps, Step 1. Configure Apache Webserver.

Upgrade instructions for the FileCloud 23.242 Outlook Add-in

Upgrade instructions for the FileCloud 23.242 Outlook Add-in

If you are upgrading FileCloud, and you plan to use the updated FileCloud Outlook Add-in, if you have previously modified the default values for **Access-Control-Allow-origin** or **Access-Control-Allow-Credentials**, they may not be set to the values required to run the FileCloud Outlook Add-in. After updating the Outlook Add-in, open .htaccess and make sure these settings have the values indicated below.

To check/replace the htaccess settings:

1. Open the .htacess file:
   `/var/www/html/.htaccess`
2. If the following commands are missing or are present, but set to different values, set them as follows:

   ```
   Header always set Access-Control-Allow-Origin https://ffol.filecloud.com
   Header set Access-Control-Allow-Credentials true
   ```

FC Push Service Configuration

FC Push Service Configuration

In FileCloud version 23.1, a Push service was added to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload, share). If you are upgrading from a version prior to 23.1, upgrading to the latest version on systems running with MongoDB replica set or standalone MongoDB require the push service **env** file to be updated based on the MongoDB configuration.

To configure the Push service in Linux:

1. Open and edit the .env file from path: **/opt/fcpushservice/**

```
vi /opt/fcpushservice/.envsystemctl restart fcpushservice
```

2. Update the MongoDB connection string:

```
FCPS_DB_DSN=mongodb://dbuser:passw0rd1@dbserver01,dbserver02,dbserver03:27017
```

3. Restart the **fcpushservice**.

```
systemctl restart fcpushservice
```