

FileCloud Server Version 23.232 Installation Guide

Printed on 02/07/2024

Copyright Notice

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

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

FileCloud Phone: U.S: +1 (888) 571-6480 Fax: +1 (866) 824-9584 Email: support@filecloud.com

Table of Contents

Copyright Notice	2
Installation Steps	5
Installation	7
Direct Installation	7
Virtual Machine Installation	26
Microsoft Azure Installation	
Amazon Web Services (AWS) Installation	
Amazon GovCloud AWS Installation	
FileCloud Docker installation	
Oracle Cloud Installation	115
Post Installation	120
Delete the Installation Folder	
FAQs	
Verify Your Installation	
Install the FileCloud License	
Configure the Managed Storage Path	
Enable MongoDB Bind IP and Authentication	
SSL Configuration	
Changing a Default Port or Web Server Setting	
Installation Troubleshooting	191
FileCloud Server not starting on Windows	
Mod Rewrite Setup Check Fails during Install	
Mount a Share that FileCloud Can Access	195
FAQ's	
Mounting Scenarios	
Mount a CIFS Share on Linux for FileCloud	
Mount an NFS share on Linux for FileCloud	
Mount CIFS Shares from Windows Command Line	

Storage and Client Application Limits	200
Mounting CIFS and NFS Shares	202
How to Mount CIFS Shares from Windows Command Line	202
How to properly mount a CIFS share on Linux for FileCloud	202
How to properly mount a NFS share on Linux for FileCloud	204

Installation Steps

Use the following outline to understand how the installation process works.

💡 Make sure to read the Requirements and Storage and Client Application Limits first.

Step 1: Install FileCloud Software

- WINDOWS: Install FileCloud using the installer on Windows (Windows 64 bit) (or)
- LINUX (Ubuntu, RedHat)

• Other options

- Install FileCloud using the provided Virtual Machine (VMWare / VirtualBox etc)
- Manual install from scratch on Ubuntu or RedHat/Fedora
- Install FileCloud on Amazon AWS
- Install FileCloud on Amazon GovCloud AWS

After installation, if Apache will not start, see FileCloud not starting on Windows.

Step 2: Verify the FileCloud Installation

 Open the FileCloud Install page at http://<site>/install (typically http://127.0.0.1/install) and go through the BASIC and EXTENDED checks.

Note that some checks might fail, but you can resolve them later in the Admin Portal Settings.

Go to Verify Your Installation

Step 3: Log in to the Admin Portal

- Open the FileCloud Admin website at http://<site>/ui/admin/index.html
- Admin Username is admin, Admin Password is password
- Go to Extended Checks, Step 6

Step 4: Install Your License

Your FileCloud license is a document that provides legally binding guidelines on the use and distribution of your newly installed FileCloud software.

Go to Install the FileCloud License

Step 5: Set the Managed Storage Path

Set the storage path where FileCloud stores its all its files. This only applies if you are using Local Storage. P If you are going to use OpenStack or Amazon S3, then you don't need to set this path.

Go to Configure the Managed Storage Path



For more information, read:

About FileCloud for Administrators

About FileCloud for Users

Installation

Use the following links to install a new instance of FileCloud Server.

P Make sure to read the Requirements first.

- WINDOWS: Install FileCloud using the installer on Windows (Windows 64 bit) (or)
- LINUX: Installation of FileCloud on Linux Using the Repository

Installation Options

- Direct Installation
- Virtual Machine Installation
- Microsoft Azure Installation
- Amazon Web Services (AWS) Installation
- Amazon GovCloud AWS Installation
- FileCloud Docker installation
- Alibaba Cloud Installation
- Oracle Cloud Installation

Direct Installation

This section explains the procedure to install FileCloud in your system.

Select your system from the links below.

- Install FileCloud Server on Windows.
- FileCloud RPM Package Installation
- Installation of FileCloud on Linux
- Installation of FileCloud on Linux Using the Repository

Install Webserver as Service for Windows

By default, the Webserver that is shipped part of the FileCloud installation runs as a normal process. If the user running the application logs out the application will exit. To prevent this, you can run FileCloud Webserver as a service.

Install as a Service

Click on "Make Service" link in the Control Panel. It will be installed as a service. You can then click on "Start" to start the service.

FileCloud Control Panel					_		×	
FileCloud Control Panel v: 15.0.0.35818, Base Components: 15.0.0.35769 Webserver Ports: 80,443 Database Port: 27017								
Initial Setup: Install Check Web Portal: Admin Portal Servers	<u>User V</u>	<u>Vebsite</u>					ļ	
Webserver: Running SVC	S	tart	Sto	p	<u>Config</u>	<u>Make</u>	<u>Service</u>	
Database: Running	S	tart	Sto	p	<u>Config</u>	<u>Make</u>	Service	
Cron Task: Running SVC	S	tart	Sto	p	<u>Config</u>	<u>Install</u>		
Optional								
FileCloud Helper: Running S	VC	Star	t	St	ор	<u>Install</u>		
Memcache: Running		Star	t	St	ор	Make S	ervice	
Document Preview: Running S	VC	Star	t	St	ор	<u>Install</u>		
Content Search: Running S	VC	Star	t	St	ор	<u>Install</u>		
Miscellaneous								
Configuration: Application Fo	lder <u>F</u>	Reset Adm	in Passw	ord				
SSL: Create SSL CSF	3 1	nstall SSL (Cert					
Technical Support								
Need Help? Documentation	Cont	act Suppo	rt					

Note, if you are making existing network shares accessible to FileCloud, we suggest you modify the service "Log on" permissions to run as an user account with full privileges to the network share (See screenshot below).

FileCloud Server Version 23.232 Installation Guide

O , Services			_ [×
File Action View Help				
← ⇒	▶ ■ II IÞ			
Services (Local)	Apache2.4 Properties (Local Computer) 🛛 🗙			
Apache 2.4	General Log On Recovery Dependencies	Startup Type	Log On As	_
Stop the servic Restart the se Description: Apache/2.4.1(Log on as: Local System account Allow service to interact with desktop This account: CODELATHE\Administrator Browse Password: ••••••••••••••••••••••••••••••••••••	Automatic Manual Automatic Manual Manual Manual Disabled Manual Automatic Manual Automatic Manual Automatic Manual Disabled Manual Disabled Manual Automatic Automatic Automatic Automatic Automatic Automatic	CODELAT Local System Local System Local Service Local Service Local System Local System	
	OK Cancel Apply	Automatic (D Manual Manual Manual	Local Service Local Service Local System Local System	-
Extended (Standard /			

Alternate way to install as a service, open an administrator command prompt

i cd c:\xampp\apache\bin httpd.exe -k install

```
c:\xampp\apache\bin>httpd.exe -k install
Installing the Apache2.4 service
The Apache2.4 service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
c:\xampp\apache\bin>
```

Remove Apache Service

i cd c:\xampp\apache\bin httpd.exe -k uninstall

Install MongoDB as service in Windows

By default MongoDB in Windows runs as a process. If the user running the application logs out, the database process will exit. To prevent this, you can run the mongodb database as a service.

Install FileCloud

Before making MongoDB as a service, install FileCloud using the windows installer. By default FileCloud will be installed under C:\xampp. If you have manually installed FileCloud or installed FileCloud on a different path, update the paths accordingly in the next steps.

Make MongoDB run as Windows Service

FileCloud Control Panel					_		\times
FileCloud Control Panel v: 15.0.0.35818, Base Components: 15.0.0.35769 Webserver Ports: 80,443 Database Port: 27017							
Initial Setup: Install Check							
Web Portal: Admin Portal	User We	<u>ebsite</u>					
Servers							
Webserver: Running SVC	Sta	irt	Sto	р	<u>Config</u>	g <u>Make</u> s	Service
Database: Running	Sta	irt	Sto	р	<u>Confic</u>	<u>Make</u>	Service
Cron Task: Running SVC	Sta	ırt	Sto	р	<u>Confic</u>	<u>Install</u>	î
Optional							1
FileCloud Helper: Running S	VC	Sta	t	Sto	pp	<u>Install</u>	•
Memcache: Running		Sta	t	Sto	р	Make S	ervice
Document Preview: Running S	VC	Sta	t	Sto	р	<u>Install</u>	
Content Search: Running S	VC	Sta	t	Sto	p	<u>Install</u>	
Miscellaneous							
Configuration: Application Folder Reset Admin Password							
SSL: <u>Create SSL CSR</u> Install SSL Cert							
Technical Support							
Need Help? Documentation	<u>Conta</u>	ct Suppo	rt				

Alternate Installation Method Step 1: Create MongoDB Config File

Update a file called mongodb.conf under C:\xampp\mongodb\bin, and use absolute paths for the locations of **logpath** and **dbpath** to be absolute paths.

(i) It is important when running mongodb as a service that the dbpath and the logpath are provided as full paths instead of relative paths. ie c:\xampp\mongodb\bin\data

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
```

Here update values of logpath and dbpath if necessary.

Alternate Installation Method Step 2: Create MongoDB Service

To install MongoDB as a service, open a command prompt with administrator access (this is important), and run the following command.



Now the service will start automatically on machine reboots.

Remove MongoDB Service

Removing MongoDB Service

C:\xampp\mongodb\bin>mongod.exe --remove

FileCloud Watchdog Service

FileCloud Watchdog Service is an service for Windows that automatically monitors the availability of Apache Webserver and the MongoDB Databases and can restart them if they become unavailable or unresponsive.

FileCloud watchdog service is only available starting from v12.0
 FileCloud watchdog service monitors OpenOffice service starting from v13.0

Installation

- 1. Open a Windows Administrator Command Prompt
- 2. Navigate to c:\xampp folder (change it to the path XAMPP folder exists)
- 3. Run the following to register the service

cloudwatchdog.exe /registerService /displayName="FileCloud Watchdog Service"

4. Start the service

net start cloudwatchdog

Uninstall

- 1. Open a Windows Administrator Command Prompt
- 2. Navigate to c:\xampp folder (change it to the path XAMPP folder exists)
- 3. Run the following to register the service

net stop cloudwatchdog

4. Start the service

cloudwatchdog.exe /unregisterService

Default Configuration

To change parameters related to the watchdog, adjust the values in the cloudwatchdog.ini file in the xampp folder.

frequency (in seconds) controls how fast the watchdog checks the availability of services serverurl determines the URL to use to check availability

```
; Settings for FileCloud Watchdog
[settings]
frequency=60
serverurl=http://127.0.0.1
```

OpenOffice Configuration

To monitor the open office service, add the following entries to the ini file and adjust accordingly: Make sure the oowatchdogcheck.php and oowatchdogsample.txt files are present in the resources\backup folder.

```
; Settings for FileCloud Watchdog
[settings]
frequency=60
serverurl=http://127.0.0.1
ooservicename=ooservice
ooscriptpath=c:\xampp\htdocs\resources\backup\oowatchdogcheck.php
```

Troubleshooting

A log for FileCloud Watchdog Service is inside the XAMPP folder under the filename 'cloudwatchdog.log'

Windows Setup Wizard

The installation process on Windows includes the following steps:

- 1. Run the Setup Wizard
- 2. Use the FileCloud Control Panel to configure servers
- 3. Use the FileCloud Control Panel to configure optional components
- 4. Complete Post Installation Steps

Use these steps to install FileCloud on a Windows 64-bit system.

- During installation you will be asked to install the Microsoft Visual C++ Redistributable Package if it does not already exist.
- This installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ on a computer that does not have Visual C++ installed.

You can only install FileCloud on the root of the hard drive.

To install FileCloud directly:

- 1. Download the installer.
- 2. Locate the FileCloudSetup.exe file and run it.
- 3. On the Welcome screen, click Next.
- 4. In the select Installation drive box, verify that the root of the hard drive is listed, and then click Install. (For example, the location can either be c:\xampp, or d:\xampp etc).
- 5. If a dialog pops up during installation and asks you to install VC_redist.x64.exe, click Install.
- 6. After installation is complete, the FileCloud Control Panel opens.

Configuring Servers with the FileCloud Control Panel

The installation process on Windows includes the following steps:

- 1. Run the Setup Wizard
- 2. Use the FileCloud Control Panel to configure servers
- 3. Use the FileCloud Control Panel to configure optional components
- 4. Complete Post Installation Steps

When the Setup Wizard finishes successfully, the FileCloud Control Panel opens so that you can configure the servers that FileCloud requires to function.

FileCloud Control Panel		- 0	× The order you should start and configure these
FileCloud Control Pane			servers is:
v: 23.1.0.22590, Base Compo	nents: 23.1.0.22590		1 Make and Start the Database Service
Webserver Ports: 80,443 Da	tabase Port: 27017		2 Configure and Start the Message Queue
Initial Setup: Install Che	ck		3 Make and Start the Webserver
Web Portal: Admin Do	tal User Website		4 Configure and Start the Cron Task
Addition of the second se	USEI WEDSILE		4. configure and start the croit rusk
Servers			
Webserver: Running	SVC 3 Start	Stop Config Make Service	💡 By default the Database and Webserver run as a
Database: Running	Chard	Config Make Service	process.
	Start	Stop	If the user running the application logs out the
Cron Task: Running	SVC 4 Start	Stop Config Install	process will exit.
Message Queue: Running	SVC 2 Start	Stop Config Install	To prevent this, you can run these servers as a
Optional			service.
Push Service: Runni	ng SVC Start	Stop Install Confi	<u>.</u>
FileCloud Helper: Runni	ng SVC	Install Confi	a
	Start	Stop	
Memcache: Runni	ng SVC Start	Stop Make Service	
Document Preview: Runni	ng SVC Start	Stop Install	
	Start	Stop	
Content Search: Runni	ng SVC Start	Stop Install	
Miscellaneous			
Configuration: Application	n Folder Reset Admin	Password	
SSL: Create SSL	CSR Install SSL Cer	t	
Technical Support			
Need Help? Documents	tion Contact Support	Demo and Training	
<u>occumenta</u>	<u>contact support</u>		

Start the Database Server

FileCloud Server uses MongoDB as the database server.

MongoDB is a cross-platform document-oriented database program.

- Classified as a NoSQL database program because instead of storing information in tables, as with traditional relational databases, MongoDB stores structured information in JSON format with dynamic schemas
- This makes integrating information in applications much easier and faster
- For more details, visit the MongoDB web site

This software is installed by the FileCloud installation wizard, you only need to configure it and start it.

- A PHP-MongoDB driver is also installed with FileCloud Server to provide a minimal API for core driver functionality
- By default MongoDB in Windows runs as a process
- It is recommended that you run MongoDB as a service instead of a process

- If the user running the application logs out, the database process will exit. To prevent this, you should run the MongoDB database as a service.
- FileCloud requires MongoDB. You must make this service and start it running before moving on to the next step.

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

To make and start the Database service:

- 1. In the FileCloud Control Panel, in the Server section, for Database, click the Make Service link.
- 2. On the Service Installed OK window, click OK.
- 3. In the FileCloud Control Panel, in the Server section, for Database, click the Start button.
- 4. In the FileCloud Control Panel, in the Server section, for Database, next to Database, verify it says Running.

If the Database service doesn't start, then another process could be using that port. To check which program is using that port, you can follow the instructions here.

Start the Message Queue

A message queue is a form of service-to-service communication that is not concurrent.

- Message queues are used in serverless and microservices architectures.
- Messages are stored in the queue until they are processed and deleted.
- Each message is processed only once.
- Message queues can be used to separate heavyweight processing workloads
- Message queues can buffer work or process work in batches
- Message queues can smooth spiky workloads

FileCloud requires MongoDB. You must make this service and start it running before moving on to the next step.

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

To configure and start the Message Queue service:

- 1. In the FileCloud Control Panel, in the Server section, for Message Queue, click the Install link.
- 2. In the FileCloud Control Panel, in the Server section, for Message Queue, click the Start button.
- 3. On the Service Started OK window, click OK.
- 4. In the FileCloud Control Panel, in the Server section, for Message Queue, next to Database, verify it says Running.

When you make a change to the configuration file

Each time you make a change to the FileCloud configuration file (cloudconfig.php) you must restart the message queue (click **Stop**, and once the service stops, click **Start**).

Indicators that the message queue is not running or clearing

If the message queue is not running or clearing, when you log in to FileCloud or refresh it, you may see a message that there are a large number of items in the message queue or that the message queue has entries older than 7 days (or a custom number of days).

The **Serial Queue Count** alert appears when there are more than 10,000 items in the serial queue; the **Parallel Queue Count** alert appears when there are more than 100,000 items in the parallel queue.

6	Install Folder Remove 'install' folder after installation. Example Windows: c:\xampp\htdocs\install Linux: /var/www/html/install or /var/www/install
1 Week 1 Month 6 Months 2	GeoIP Data Go to Settings, Admin to enable GeoIP data generation and set GeoIP server URL (Optional)
	Serial Queue Count Number of items in serial queue has exceeded 10,000. Go to FileCloud control panel and ensure Message Queue service is running
	Audit Records 0

Serial Queue Count alert

Г

The Old Entries messages appear when one of the queues has message that are older than 7 days. To change the number of days triggering the message, please Contact FileCloud Support.



Old Entries alerts.

In either case, begin troubleshooting by confirming that the FileCloud control panel indicates that the Message Queue service has been started. If it has not been started, click **Start** (see the above image). It may take some time for the alert to disappear since the message queue must delete all previously processed messages before starting again.

Start the Webserver

FileCloud requires Apache Webserver. You must make this service and start it running before moving on to the next step.

FileCloud (v: 17.3.0.3765 Webserver Po	FileCloud Control Panel v: 17.3.0.37651, Base Components: 17.3.0.37625 Webserver Ports: 80,443 Database Port: 27017							
Initial Setup Web Portal: Servers	: <u>Install Check</u> Admin Portal	<u>User Website</u>						
Webserver:	Running SVC	Start	Stop	Config Make Service				
Database:	Running	Start	Stop	Config Make Service				
Cron Task:	Running SVC	Start	Stop	<u>Config</u> <u>Install</u>				

To make and start the Webserver service:

1. In the FileCloud Control Panel, for the Webserver, click the Make Service link.

- 2. On the Service Installed OK window, click OK.
- 3. In the FileCloud Control Panel, for the Webserver, click the Start button.
- 4. In the control panel, next to Webserver, verify it says Running SVC.

If the WebServer service doesn't start, then another process could be using that port. To check which program is using that port, you can follow the instructions here.

Install and Start the Cron Task

When the Setup Wizard finishes successfully, the FileCloud Control Panel opens so that you can complete the installation steps. During installation you will be warned that Cron Task is only needed if a FileCloud Scheduled Task is not already setup. However, Cron Task is required. if you try to run the Installation Check or log into the Admin Portal without installing Cron task and try to enable Team Folders, for example, the process will fail. Other components on the FileCloud server rely on the Cron Task as well, so this must be installed and started.

A	FileClo step.	oud requires th	ne Cron Task. '	You must Insta	Ill this se	rvice and star	t it running before moving on to the nex
FileO	loud Co	ntrol Panel					
v: 17.	3.0.37651,	Base Component	ts: 17.3.0.37625				
Webs	erver Port	s: 80,443 Databa	ase Port: 27017				
Initia	al Setup:	Install Check					
Web	Portal:	Admin Portal	User Website				
Serv	ers						
Web	server: R	Running SVC	Start	Stop	<u>Config</u>	<u>Make Service</u>	
Data	ibase: R	lunning	Start	Stop	Config	Make Service	
Cror	n Task: 🛛 🦷	Running SVC	Start	Stop	<u>Config</u>	<u>Install</u>	

To install and start the Cron Task service:

- 1. In the FileCloud Control Panel, for Cron Task, click the Install link.
- 2. On the Confirmation Installation window, click Yes.
- 3. On the Service Installed OK window, click OK.
- 4. In the FileCloud Control Panel, for Cron Task, click the Start button.
- 5. In the control panel, next to Cron Task, verify it says Running SVC.

Configuring Optional Components

The installation process on Windows includes the following steps:

- 1. Run the Setup Wizard
- 2. Use the FileCloud Control Panel to configure servers
- 3. Use the FileCloud Control Panel to configure optional components
- 4. Complete Post Installation Steps

Install Optional Components

After a successful installation check, the basic FileCloud service is ready.

Before running post-installation checks on everything that is installed, you can add any of the following optional services to include them in the post-installation verifications:

- WebDRM Service Runs the WebDRM server for digital rights management.
- Push Service Opens two-way connection for certain client-server processes to improve response time.
- FileCloud Helper Enables certain searches and NTFS checks on Network Folders.
- Memcache Improves performance when using Network Folders with NTFS permissions.
- Document Preview Enables previewing of document contents.
- **Content Search** Enables you to index and search the contents of files.

FileCloud Control Panel			– 🗆 X					
FileCloud Control Panel v: 23.232.0.24769, Base Components: 23.232.0.24769 Webserver Ports: 80,443 Database Port: 27017								
Initial Setup: Install Check								
Web Portal: <u>Admin Portal</u> User W	<u>/ebsite</u>							
Servers								
Webserver: Running SVC	Start	Stop	Config Make Service					
Database: Running	Start	Stop	Config Make Service					
Cron Task: Running SVC	Start	Stop	Config Install					
Message Queue: Running SVC	Start	Stop	Config Install					
Optional								
WebDRM Service: Running SVC	Start	Stop	<u>Install</u>					
Push Service: Running SVC	Start	Stop	Install Config					
FileCloud Helper: Running SVC	Start	Stop	Install Config					
Memcache: Running SVC	Start	Stop	Make Service					
Document Preview: Running SVC	Start	Stop	Install					
Content Search: Running SVC	Start	Stop	<u>Install</u>					
Miscellaneous								
Configuration: Application Folder Reset Admin Password								
SSL: Create SSL CSR Install SSL Cert								
Technical Support								
Need Help? Documentation Contact Support Demo and Training								

Because these components are optional, they can be added or removed at any time from the FileCloud Control Panel.

Install Content Search

Administrators can enable content search to provides users with the following features:

- Content search for file types such as txt, pdf, doc, docx, xls, xlsx, ppt, pptx
- Regex support for file/folder name searches

Content Search uses Solr, and Solr in turn uses Java.

A Before installing Content Search, you must install the correct Java Development Kit (JDK).

Installing Content Search

Install Helper, memcache, or doc preview

FileCloud Helper, Memcache, and Document preview do not require any pre-installation steps.

To install and start any of these optional services:

- 1. In the FileCloud Control Panel, click the Install or Make Service link next to the service.
- 2. On the Service Installed OK window, click OK.
- 3. In the FileCloud Control Panel, click the Start button for the service.
- 4. In the control panel, verify that **Running** or **Running SVC** appears next to the service.

Post-Installation Steps

The installation process on Windows includes the following steps:

- 1. Run the Setup Wizard
- 2. Use the FileCloud Control Panel to configure servers
- 3. Use the FileCloud Control Panel to configure optional components
- 4. Complete Post Installation Steps

Complete Post Installation Steps

At this point, the basic FileCloud service is ready to be tested. Before logging in to the Admin Portal, you should verify that are no port conflicts or issues with Apache, Mongo DB, or Cron Task. Unless these required services are running you will not be able to complete tasks in the Admin Portal. Therefore, use the following steps to verify that what you have is installed is running without issues.

To perform an post-installation checks:

- 1. In the FileCloud Control Panel, next to Webserver, verify it says Running SVC.
- 2. In the FileCloud Control Panel, next to Database, verify it says Running.
- 3. In the FileCloud Control Panel, next to Cron Task, verify it says Running SVC.
- 4. In the FileCloud Control Panel, next to Initial Setup, click Install Check.
- 5. If successful, you should see the Getting Started screen.
- 6. Follow the instructions in Post Installation to complete your cloud setup.



Installation of FileCloud on Linux Using the Repository

 Beginning in FileCloud 23.1, Linux installation and upgrades moved to a new repository system.
 The OS's we currently support are: Ubuntu 22.04 LTS RHEL 9.x

- If the Linux server is not in a isolated environment where regular users are prevented from using SSH login, we recommend enabling authentication for the MongoDB service to prevent unauthorized access through port forwarding.
- MongoDB 6.0 requires use of the AVX instruction set, which is available on select Intel and AMD processors. If your CPU doesn't have the AVX instruction set, MongoDB 6 will not run. To check whether your CPU has the instruction set, run: #lscpu | grep -i avx"

Note: FIPS 140-3 modules are still in review for Ubuntu 22.04 and RHEL 9. If you want to install FileCloud with FIPS, please wait until the OS vendors officially announce they are supporting FIPS. Ubuntu information RHEL information

Installation instructions for each operating system

Installation for Ubuntu 22.04 LTS

To install FileCloud on Ubuntu 22.04, complete the following steps:

Enter the following commands:

```
curl -fsSL https://pgp.mongodb.com/server-6.0.asc | sudo gpg -o /usr/share/keyrings/
mongodb-server-6.0.gpg --dearmor
curl -fsSL https://repo.filecloudlabs.com/static/pgp/filecloud.asc | sudo gpg -o /usr/
share/keyrings/filecloud.gpg --dearmor
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg ]
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 multiverse" | sudo tee /etc/
apt/sources.list.d/mongodb-org-6.0.list
echo "deb [ arch=amd64 signed-by=/usr/share/keyrings/filecloud.gpg ] https://
repo.filecloudlabs.com/apt/ubuntu jammy/filecloud/23.232 main" | sudo tee /etc/apt/
sources.list.d/filecloud.list
apt-get update -y
apt-get install apache2 mongodb-org pigz -y
```

```
apt install -y --no-install-recommends php8.2*
ACCEPT_EULA=Y apt-get install filecloud -y
```

Installation for RHEL 9

To install FileCloud on RHEL 9, complete the following steps:

Enter the following commands:

```
dnf module disable httpd -y
dnf module disable php -y
cat <<EOF > /etc/yum.repos.d/filecloud-23.232.repo
[filecloud-23.232]
name=FileCloud 23.232
baseurl=https://repo.filecloudlabs.com/yum/redhat/\$releasever/filecloud/23.232/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://repo.filecloudlabs.com/static/pgp/filecloud.asc
module_hotfixes=true
EOF
```

```
cat <<EOF > /etc/yum.repos.d/mongodb-org-6.0.repo
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/\$releasever/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-6.0.asc
EOF
yum update -y --allowerasing
yum install yum-utils -y
yum-config-manager --enable filecloud-23.232
yum install mongodb-org -y
ACCEPT_EULA=Y yum install filecloud -y
```

Virtual Machine Installation

MongoDB 6 requires use of the AVX instruction set, which is available on select Intel and AMD processors. If your CPU doesn't have the AVX instruction set, MongoDB 6 will not run.

Virtual Machine Installation

FileCloud is provided as a Virtual Machine (in OVF format) so that it is easy to get started without doing any configuration or setup. The virtual machine also allows customers to quickly evaluate and try FileCloud in other non-Linux environments.

The FileCloud Virtual Machine has the following specifications :

Operating System	Ubuntu 22.04 LTS with Desktop
Disk Size	100 GB
RAM	8 GB

The following is the OS user login information

Username	cloud
Password	cloud

The following is the FileCloud Admin login information

Username	admin
Password	password

Installing Virtual Machine

- 1. Download the FileCloud OVF zip using the provided link.
- 2. Unzip the zip file with all the contents into your hard disk
- 3. See for VMWare Player Install Instructions
- 4. See for VirtualBox Install Instructions

Running the Virtual Machine

- 1. On startup, enter "cloud" as the password to login into the system.
- 2. After login, you will see the desktop with several icons.
- 3. Refer to shortcuts section for more details on the icons and how to use them.



National State (1997) State (19		-		×
Player 🗸 📔 🗶 🛄 🍓				«
Ubuntu Desktop	t,	€))	8:32 PN	v ¢⊱
6 6				
FileCloud Admin				
* 6				
FileCloud Install				
FileCloud Support				
cloudconfig.php				
filecloud				
CloudURLs				

Shortcuts

Here's the information on each shortcut and it's function.

ICON	Details
FileCloud	Opens the main FileCloud User Portal.

FileCloud Admin	Opens the FileCloud Admin Portal User name: admin Default Password: password
FileCloud Install	Opens the FileCloud Install Check Page
cloudconfig.php	Shortcut to the general cloud configuration file (cloudconfig.php).
FileCloud Support	Shortcut to the FileCloud support documentation.
CloudURLs	Click the icons to generate the URLs that can be used to access the FileCloud from outside the virtual image. Note: Depending on the network configuration, these links can be used to access FileCloud from anywhere on the local network (Bridged configuration) or from within the host (host-only or NAT configuration)
	Shortcut to the folder containing all cloud files.

VirtualBox

For **Virtual Box:** Click on File->Import Appliance and then select the "FileCloud - For VirtualBox.ovf" file, then hit "Next" and then "Import". The virtual machine will be imported and available to start.



		?	×
÷	Import Virtual Appliance		
	Appliance to import		
	VirtualBox currently supports importing appliances saved in Virtualization Format (OVF). To continue, select the file to ir	the Open nport below.	
	Expert Mode Next	Cance	el

♥ Please choose a virtual ap	in PC > Developeds > OVE > OVE			~ 7	Search OVE			×
Organize New folde	V O	Search OVF			?			
A Quick access	Name	Date modified	Туре	Size				
📃 Desktop 🛛 🖈	💗 FileCloud - For VirtualBox.ovf	8/25/2015 10:15 PM	Open Virtualizatio	6	КВ			
 Downloads p2p Dump FileCloud FileCloud Documents Documents logs OVF partners Scans OneDrive This PC 	¥ FileCloud.ovf	8/25/2015 10:15 PM	Open Virtualizatio	7	KB			
EOS_DIGITAL (E:) 🗸								
File na	ame: FileCloud - For VirtualBox.ovf			~	Open Virtual Open	ization Fo	ormat (*.c Cancel	• ~

		?	\times
 Import Virtual Appliance 			
Appliance settings			
These are the virtual machines co settings of the imported VirtualBo properties shown by double-clickin check boxes below.	ntained in the appliance a x machines. You can char ng on the items and disab	and the sugges nge many of the le others using	ted the
Description	Configuration		^
Virtual System 1			
🎲 Name	vm_1		
🗮 Guest OS Type	👺 Ubuntu (64-bi	it)	
CPU	1		
RAM	2048 MB		
💿 dvd			
USB Controller	\checkmark		~
Reinitialize the MAC address of	fall network cards		
Resto	ore Defaults Import	Cance	el

VMware ESXi

If you have issues starting up the Virtual Machine in your VMware ESXi 5.1 infrastructure: You might need to do the following.

- Open a console to ESXi host.
- Run this command to load the multiextend module

#vmkload_mod multiextent

• Convert the vmdk image, by going to the location of the virtual machine and then run the following command

#vmkfstools -i ./TonidoCloud-disk1.vmdk ./newdiskimage.vmdk -d zeroedthick

• Delete the original disk

#vmkfstools -U ./TonidoCloud-disk1.vmdk

• Rename the cloned disk to the original disk name

#vmkfstools -E ./newdiskimage.vmdk ./TonidoCloud-disk1.vmdk

• Unload the multiextent module

#vmkload_mod -u multiextent

For more information see http://kb.vmware.com/selfservice/microsites/search.do? language=en_US&cmd=displayKC&externalId=2036572

VMware Player

For **VMWare Player:** Click on "Open a Virtual Machine" and then select the TonidoCloud.ovf file and hit "Import". The virtual machine will be imported and be available to start.



1 vmwareplayer1.png

See Virtual Machine					
	nis PC > Downloads > OVF > OVF	~	ප Search OVF		Q
Organize 👻 New folde	er			III 🔹 🔲	?
A Quick access	Name	Date modified	Туре	Size	
🔜 Desktop 🛛 🖈	💗 FileCloud - For VirtualBox.ovf	8/25/2015 10:15 PM	Open Virtualizatio	6 KB	
👆 Downloads 🖈	🔰 FileCloud.ovf	8/25/2015 10:15 PM	Open Virtualizatio	7 KB	
p2p → 📌					
📙 Dump 🛛 🖈					
👸 FileCloud 🛛 🖈					
🍯 FileCloud 🛛 🖈					
🔮 Documents 🖈					
📰 Pictures 🖈					
logs					
OVF					
partners					
File n	ame: FileCloud.ovf		 All supported 	l files (*.vmx;*.vmc	\sim
			Open	Cancel	
		1			
Import Virtual Machine	×				
Store the new Virtu	ial Machine				
virtual machine.	nd local storage path for the new				
Name for the new side of		-			
Riane for the new virtual	machine:				
FileCloud					
Storage path for the new virtual machine:					
C:\Users\ Docum	nents\Virtual Machines\Fil Browse	_			
Help	Import Cancel				

Microsoft Azure Installation

FileCloud Virtual Machine is currently available via Azure Marketplace.

Using FileCloud VM on Azure, one can host their own file share sync and mobile access solution for their organization in less than 10 minutes. The FileCloud Virtual Machine is built on top of Windows Server 2016 Data Center Edition. FileCloud stores the metadata information in MongoDB which is already pre-configured in the FileCloud Virtual Machine. The actual files can be stored in the VM Disk or Azure Files depending on your requirement. We recommend to take periodic snapshots of your running instance for disaster recovery.

Steps To Launch FileCloud Virtual Machine on Azure

1. Login to https://portal.azure.com using your azure account. Upon successful login, go to Home>> Marketplace >> Everything. Search for FileCloud.

$\langle \rangle$		⊜ portal.azure.com C	
1	Vicrosoft Azure Installation - FileCloud - FileCloud Support	Everything - Microsoft Azure https://www.bing.co	om/cr?IG=6E2CBA91F54341D293244BCDE6DD0 +
Micro	osoft Azure	P Search resources, services, and docs ×) 🕐 🕀 devteam@codelathe
»			
+	Marketplace 🖈 🗙	Everything	* 🗆 ×
∷≡	My Saved List 🔍	Y Filter	
-*-	Everything		×
•••	Compute	Results	
	Networking	NAME PUBLISHER	CATEGORY
	Storage	FileCloud CodeLathe	Compute
٨	Web	FileCloud ServerLink CodeLathe	Compute
<i>«</i> >	Mobile		
8	Containers	FileCloud on Ubuntu Linux CodeLathe	Compute
2	Databases	FileCloud EFSS on Windows 2016 CodeLathe	Compute
Q	Analytics		
*	AI + Machine Learning		
-	Internet of Things		
<>	Integration		
•	Security	Related to your search 🗸	
<u>)</u>	Identity	GreatHorn GreatHorn	
-	Developer tools	<u>w</u>	
2. Select FileCloud and Click Create

$\langle \rangle$		🗎 portal.a	azure.com		Ċ 1
	Microsoft Azure Installation - FileCloud	- FileCloud Support			FileCloud - Microsoft Azure
Mic	rosoft Azure	${\cal P}$ Search resources, services, and ${\cal G}$		×Û	>_ 💱 🚱 🕐 🕞 devteam@codelathe
+	rerything			* ×	FileCloud CodeLathe
	Filter				Bring Your Own License enabled.
-*-	⊃ FileCloud			×	 File Sync and Sharing:FileCloud allows businesses to host the sync and mobile access, solution for their employees, partners
	esults				Infrastructure. FileCloud's effortless File synchronization across and Linux), smart phones and tablets (iOs, Android, Windows & powerful and secure solution
	VAME	PUBLISHER	CATEGORY		 Endpoint Backup and DLP:FileCloud provides secure, high pe platforms and devices (Computers and Smartphones) with unit carabilities. ElieCloud: unique carabilities to monitor, prevent
	🗃 FileCloud	CodeLathe	Compute		corporate data is protected across all your devices. Remote Blo in both mobile devices and computers.
%	DileCloud ServerLink	CodeLathe	Compute		 Custom Branding:FileCloud allows Businesses to customize th organization brand and it can be run under the business doma array of options to customize login page image, TOS and ema
2	FileCloud on Ubuntu Linux	CodeLathe	Compute		 Scalability and Redundancy:Leverage the highly-scalable, rel infrastructure to run your FileCloud.
2	FileCloud EFSS on Windows 2016	CodeLathe	Compute		 Microsoft Technology Integration:FileCloud is integrated wirdocuments on the browser. FileCloud can also be integrated wirdocuments for the browser. FileCloud can also be integrated wirdocuments file and the manager choose file.
					 Ose Cases. System administrators and in Managers choose nin client file sharing portal or use it as a cloud file server Industry Recognition:CodeLathe's FileCloud is named in Gart
*					Collaboration Platform and recognized by Network World as C Companies to Watch.
=					 Simple Pricing:FileCloud starter pack is 1000\$/year for 20 lice cost just 50\$ per user per year.
•	elated to your search 🗸				Select a deployment model 🚯 Resource Manager
()	GreatHorn				
-	GreatHorn				Create → Want to deploy programmatically? Get started →

3. Configure Basic Settings: Choose your Windows VM name, user name, password, subscription, resource group and the azure data center location. Once you complete the information click OK.

🗯 Sa	ifari File	Edit View H	istory Bookr	narks	Window Help		5 🦸 🕄 🍥 奈 🔽 72% 🗩 Mon 8:35	; PM Q 🌏 🖃
	$\langle \rangle$					portal.azure.com	Ċ	
		Microsoft Azure Ir	stallation - FileCl	oud - File	Cloud Support		Basics - Microsoft Azure	+
»	Home >	Marketolace > Everythin		Create virt	ual machine > Basics			CODELATHE
+	Create	virtual machine		×	Basics	□ ×	~	
:≡ -★-	1	Basics Configure basic setti) ngs		* Name filecloudazure	✓		
	2	Size Choose virtual machi	> ne size		Standard HDD * Username filecloudazure	~		
(*) (*)	3	Settings Configure optional fe	> atures		* Password			
<₽ 	4	Summary FileCloud	>		* Confirm password Subscription			
2					Microsoft Azure Sponsorship	~		
<u>₽</u> ♦					Create new Use existing IT	·		
=					* Location East US	~		
<>					Save money			
<u>e</u>				_	Save up to 49% with a license you	already own.		
					OK			

4. Choose Virtual Machine Size according to your needs. Here we are selecting D2_v3 (8 GB RAM, 50 GB Local SSD)

É	Safari	i File	Edit	View	History	Bookmarks	Windo	w Help	leeus	intere m			5	6	ا چ ا	79%	[4] Tu	ie 10:12 AM	Q	007
• •									0	portal.azure.co	m			Ċ						
	Micros	oft Azure	Installa	ation - FileC	loud - FileC	loud Support			Choose	e a size - Microsof	t Azu	re		About u	nmanaged (p	page blobs	s) and mana	ged disks stora	ige for Mi	ro +
IVII	» н	ome → M	arketpla			Cloud > Create	virtual mach	ine > Choose a si	ze	is, and does	-		. Ф.	´- ``		U	ሞያ		CODELA	тне 🔍
+		×		Choose Browse the av	a size vailable sizes	and their features														∎ ×
				Search				Compute type				Disk type				vCPUs				
		~						General purpos	se		~	All disk types			~	1	0			128
	_		RE	сомме 🖘	sku	↑џ түре		COMPUTE 🗘	VCPUS	1. GB RAM		DATA DISKS 👈	MAX IOP	s î↓	LOCAL SSD	↑↓ PRE	мим †.	ADDITION	tu Us	D/MON ∿
	ze	>	Av	ailable																
					D2_v3	Standa	ard	General purpose	2	8		4	4x500		50 GB	No			\$1	39.87
	es	>			D4_v3	Standa	ard	General purpose	4	16		8	8x500		100 GB	No			\$2	79.74
					D8_v3	Standa	ard	General purpose	8	32		16	16x500		200 GB	No			\$5	59.49
-		>			D16_v3	Standa	ard	General purpose	16	64		32	32x500		400 GB	No			\$1	118.98
8					D32_v3	Standa	ard	General purpose	32	128		32	32x500		800 GB	No			\$2	237.95
2					D64_v3	Standa	ard	General purpose	64	256		32	32x500		1600 GB	No			\$4	475.90
Q					D1_v2	Standa	ard	General purpose	1	3.5		4	4x500		50 GB	No			\$9	3.74
-					D2_v2	Standa	ard	General purpose	2	7		8	8x500		100 GB	No			\$1	87.49
					D3_v2	Standa	ard	General purpose	4	14		16	16x500		200 GB	No			\$3	74.98
<>					D4_v2	Standa	ard	General purpose	8	28		32	32x500		400 GB	No			\$7	49.95
•			F	Prices prese	nted are est	imates in your lo	ocal curren	cy that include Az	ure infrastr	ructure applicable	softv	vare costs, as well a	as any disc	ounts for	the subscri	ption and	location.			
<u>)</u>			-	Select		\														

5. Configure Storage and Network Settings as needed and Click OK.





6. Verify your offer details and click Create.

Note: FileCloud is offered under Bring your Own License Model. You can get FileCloud trial license by registering in our customer portal.

7. Azure will start provisioning your FileCloud Virtual Machine. Check the Notifications to see whether the deployment is complete.



8. Check the deployment is complete and make sure your FileCloud instance is running.



9. Connect to your FileCloud VM instance using RDP connection.



10. Right Click Windows Start Icon --> Launch File Explorer --> Go to C:\xampp and double click cloudcp (FileCloud Control Panel)

	· · · · ·		104.44.155.150 01				
board							
ER MANAGER							
	this local server						
👪 l ⊋ 🚯 = l			xampp				_ 🗆 X
File Home Share	View						v 🕐
🗲 💿 🕶 🕆 🚺 🕨 T	his PC → Local Disk (C:) → xampp →				<u></u>	Search xampp	Q
	Name	Date modified	Туре	Size			^
Deskton	🐌 mongodb	5/21/2015 12:51 AM	File folder				
Downloads	Dep php	5/21/2015 12:52 AM	File folder				
Recent places	🚡 sendmail	5/21/2015 12:52 AM	File folder				
A needed places	鷆 tmp	5/21/2015 12:52 AM	File folder				
1 This PC	🚳 apache_start	9/23/2014 7:39 PM	Windows Batch File	1 KB			
12	🚳 apache_stop	9/23/2014 7:39 PM	Windows Batch File	1 KB			
📬 Network	🚳 cloudcp 🥿	5/20/2015 6:20 PM	Application	3,253 KB			
*	Microsoft.V CRT.manifest	9/11/2009 3:01 PM	MANIFEST File	1 KB			
	🚳 msvcm90.dll	7/29/2008 7:24 PM	Application extens	220 KB			
	🗟 msvcp90.dll	7/29/2008 11:35 PM	Application extens	560 KB			
	🗟 msvcp100.dll	3/19/2010 1:45 AM	Application extens	412 KB			
	🚳 msvcr90.dll	7/29/2008 11:35 PM	Application extens	641 KB			
	🚳 msvcr100.dll	3/19/2010 1:45 AM	Application extens	753 KB			
	🚳 PocoCrypto.dll	2/8/2012 3:36 PM	Application extens	111 KB			=
	PocoFoundation.dll	2/8/2012 3:36 PM	Application extens	1,226 KB			
	NocoNet.dll	2/8/2012 3:36 PM	Application extens	737 KB			
	NocoNetSSL.dll	2/8/2012 3:36 PM	Application extens	209 KB			
	🚳 PocoUtil.dll	2/8/2012 3:36 PM	Application extens	329 KB			
	NocoXML.dll	2/8/2012 3:36 PM	Application extens	541 KB			
	🚳 PocoZip.dll	2/8/2012 3:36 PM	Application extens	211 KB			
	setup_xampp	9/23/2014 7:39 PM	Windows Batch File	1 KB			
	🚳 sync	4/26/2013 2:43 PM	lcon	345 KB			
	🚳 test_php	9/23/2014 7:39 PM	Windows Batch File	4 KB			
	🕞 uninstall	5/21/2015 12:53 AM	Application	395 KB			
	∰ vcredist_x86	4/26/2013 5:54 PM	Application	4,375 KB			\
							EE 🕥 🛛

11. Start the FileCloud web server and database server via the FileCloud Control Panel.

FileCloud Control Panel				_		×			
FileCloud Control Panel v: 17.3.0.37590, Base Components: 17.3.0.37590 Webserver Ports: 80,443 Database Port: 27017									
Initial Setup: Install Check Web Portal: Admin Portal User Website									
Servers									
Webserver: Not Running St.	art	Stop	<u>Config</u>	Make Serv	ice				
Database: Not Running St.	art	Stop	<u>Config</u>	Make Serv	ice				
Cron Task: Not Running St.	art	Stop	Config	<u>Install</u>					
Optional									
FileCloud Helper: Not Found	Start	St	op	<u>Install</u>	Co	onfig			
Memcache: Not Running	Start	St	op	Make Service					
Document Preview: Not Running	Start	St	op	Install					
Content Search: Not Found	Start	St	top	Install					
Miscellaneous									
Configuration: Application Folder Reset Admin Password									
SSL: Create SSL CSR Install SSL Cert									
Technical Support									
Need Help? Documentation Co	ntact Support								

12. Type http://<publicIP_of_FileCloudVM>/ui/admin/index.html to access the admin portal. Use "admin" as user name and the password is "password".

👫 fcazuretestvm - Microsoft 🗙 🍚 FileCloud	× +		
🗲 🕲 104.44.133.198/ui/admin/index.html			
Most Visited in Getting Started			
	Ĝ	្ឋិfile cloud	
	F	Admin Portal	
	Ň	Name Enter admin name	
	P	Password Enter password	
		Sign in	
		Powered by FileCloud	

13. Upon successful login, set the storage path for your files and install the trial license you have got from Microsoft Azure Installation.

Admin Attention Required ×								
Action Item	Description	^						
Storage Path Not Set	Storage Path							
	Specify the Location to Store Cloud Files, this must be writable by Webserver. Example path on Windows: Civelouddata Example path on Linux: /opt/cloud/data Check Path Apply	1						
Invalid License File	Upload your license via Install License	l						
Install Folder	Remove 'install' folder after installation Example Windows: c:\xampp\htdocs\install or Linux: /var/www/instal							
Set Admin Email	Go to Settings, Email to set a valid Email Reply-to Address							
Set Email Server	Go to Settings, Email to set a valid email server to send email. Demo SMTP Server enabled during trial	l						
GeolP Data	Go to Settings, Admin to enable GeoIP data generation and set GeoIP server URL (Optional)							
		~						
	S Clo	se						

14. You are set now. Follow the steps here (FileCloud Site Setup) to setup and customize FileCloud as per your organization requirements.

FileCloud Integration with Azure File Storage

Azure File storage offers file shares in the Azure Cloud using standard SAMBA protocol (SMB 3.0). FileCloud running on Azure VMs can mount the file shares created on Azure Files storage and use it as a main storage path for FileCloud. You can also use the same fileshare to store the MongoDB data files. Azure Files storage is built on the same technology as Blob, Table, and Queue storage. When you create the storage account in Azure portal you can choose what type of redundancy you would like to have (Local or geo-redundancy). By storing both files and the database db files in Azure Files Storage you will get the same scalability, durability, reliability and geo-redundancy of Azure storage infrastructure.

One can also easily scale FileCloud by running multiple app nodes while pointing to the same Azure Files Storage location for storing files and database data files.

We have tested FileCloud with Azure Files storage backend using few million files and the setup has worked great. This configuration gives the scalability and data redundancy without any complicated setup. If you have any questions please feel free to contact us at *support@filecloud.com*.

Step by Step Instructions to Integrate FileCloud with Azure File Storage

1. Create a storage account in Azure Portal and choose the storage account type (depending on your redundancy requirements). In this exercise, we have chosen a locally redundant storage account type. We recommend to choose the location same as where FileCloud VM is located.

FileCloud Server Version 23.232 Installation Guide

$_$ \square \times Create storage account	$_$ \square \times Choose storage account type $$_{\rm Browse the available plans and their features}$
* Name	P Premium Locally Re L Locally Redundant G Geo-Redundant
filecloudazurefiles	3 Local replicas 3 Local replicas 3 Local replicas
* Type	3 Geo-distributed replic
Standard-RAGRS	Page blob Elock and page blobs Elock and page blobs
	S000 Table Table
Diagnostics 🗊	(2) 99.9% I Queue Queue
Disabled Enabled	500 May IOPS per disk
Subscription	99.9% 91.9%
Microsoft Partner Network	
* Resource Group	19.71 2.40 STARTING COST PER 128GB DISK (STARTING COST PER 100GB (USD)
Select Existing	R Read-Access Geo-K Z Zone Redundant
	2 Cas distributed applie
Location	
	Queue
	Max IOPS per disk
	5LA 5LA
	V Read access to seco
	6.10 3.00 STARTING COST PER 100GB (USD) STARTING COST PER 100GB (USD)
Pin to dashboard	
Create	Select

2. Create a File Share under Storage Account as shown below. One can also choose the storage quota. Maximum storage for a File Share is 5120 GB.

FileCloud Server Version 23.232 Installation Guide

file deu dem vefiles	* _ 🗆 ×	Elle convice		_ 🗆 ×	File shares
Storage account		File service (filecloudazurefiles)			File service (filecloudazurefiles)
🔅 🛅 Settings Delete		Settings			+ Ö File share Refresh
Essentials ^	P & & <>	Essentials ^		Å	Search file shares by prefix
Resource group Type filectourdd Standard-RAGRS		Storage account filecloudazurefiles	File service endpoint https://filecloudazurefiles	file core windows	NAME MODIFIED
Status (primary, secondary) Available Available		Status (primary, secondary)	intport incore and a concerned		No file shares found.
Location (primary, secondary) Central US Fact US 2		Location (primary, secondary) Central US_East US_2			
Subscription name Microsoft Partner Network		Subscription name Microsoft Partner Network			
Subscription ID 509e66b9-5ec0-4e52-988f-aa4c5c37ccc3		Subscription ID 509e66b9-5ec0-4e52-988f-aa4c5c37ccc3			
	All settings 🔿			All settings $ ightarrow$	
Services	^			^	
Blobs Files	- m	File shares			
	TABLES QUEUES				
Marinaire		NAME	MODIFIED	QUOTA	
		No file shares found.			
i otal requests					
No available data.					
		Monitoring			
		Total requests			

	_ D ×		* _ 🗆 ×	_ 🗆 ×
File service File service (filecloudazurefiles)		File shares File service (filecloudazurefiles)		New file share File service (filecloudazurefiles)
Settings		U U File share Refresh		
Essentials ^	Å	Search file shares by prefix		* Name
Storage account filectoudazurefiles Status (primary, secondary) Available, Available Location (primary, secondary) Central US, East US 2 Subscription name Microsoft Partner Network Subscription ID 509e66b9-5ec0-4e52-988f-aa4c5c37ccc3	File service endpoint https://filecloudazurefiles.file.core.windows	NAME MODIFIED	QUOTA	Quota IIII IIIII IIIIIIIIIIIIIIIIIIIIIIIII
	All settings 🗸	~		
File shares				
NAME	MODIFIED QUOTA			
No file shares found.				
Total requests				Create

3. Create a local user in FileCloud VM with the same name as the storage account name that you have created in step 1. For password, please use the access key of Azure Files Storage.

	2			Com	puter Management			- 🗆	x
	File Action View Help								
	🗢 🔿 🙋 📰 🙆 🔒	▶ <u>:</u>							
	Computer Management (Local	Name	Full Name		Description		Actions		
	A System Tools ▶ ● Task Scheduler	🐙 filecloudcl 髪 filecloudde	filecloudcl		Built-in account for administering		Users		^
8 (Event Viewer Shared Folders 	🕵 Guest			Built-in account for guest access t	Y	More Action	IS	•
.2	▲ Local Users and Groups Isers		r		New User				
9.7	Groups		User name:	fileclouda	Azurefiles				
	Device Manager		Full name:	FlieCloud	i Storage Account Name	=			
	Windows Server Backup					_			
.3:	Disk Management Services and Applications		Password:	••	••••••	••			
8 1			Confirm password:	••	•••••	••			
			User must chan	nge passv	vord at next logon				
9-			Password never	er expires	SWOID .				
			Account is disat	bled					
						-			
			Help		Create Close				
	< III >								

FileCloud Server Version 23.232 Installation Guide

filecloudazurefiles Storage account Settings Delete	* _ ×	_ □ × ↑ Access keys filecloudazurefiles ℃ ℃ Regenera Key1 Key2
Essentials ^ Resource group Type filecloudcl Standard-RAG Status (primary, secondary) Available, Available Location (primary, secondary) Control US Fact US 2	▶ 22 89 <⊅ RS	STORAGE ACCOUNT NAME filecloudazurefiles
Subscription name Microsoft Partner Network Subscription ID 509e66b9-5ec0-4e52-988f-aa4c5c37ccc3	All settings →	KEY1 9wtq7tgVMEYkLzt5o6vuJ1weEil3S8kpf8W Factor KEY2 RoxX1ckiRd5zdWhicwNMvpozkd/V7RY6B
Services Blobs Files	TABLES QUEUES	Connection strings KEY1 DefaultEndpointsProtocol=https;Accountl
Monitoring Total requests		KEY2 DefaultEndpointsProtocol=https;AccountI
No available data.		

4. Make the local user created in step 3 as part of Administrators group.

1	Computer Management	_ 🗆 X
File Action View Help		
 Computer Management (Local System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Corport Users Groups Storage Windows Server Backur Disk Management Services and Applications 	Full Mease Filecloudazurefiles Properties X Select Groups X Select this object type: Object Types Groups Object Types From this location: [LecLOUDDEMO5 FILECLOUDDEMO5 Locations Enter the object names to select (examples): [FILECLOUDDEMO5\Administrators] Check Names Advanced Advanced OK Changes to a user's group membership are not effective until the next time the user logs on. OK Cancel Apply Help	Actions Users More Actions filecloudazurefiles More Actions

5. Run the Apache and MongoDB service using the local user account created in the previous step.

Note: We do this step for Apache and MongoDB to have the read, write access permissions to the file shares we created on Azure storage. By using the storage account name as a local user name and access key as the password, this local user will get complete access to the file shares.

🔍 Apache2.4	Apache/2.4	Running	Automatic .\filecloudcl
🔍 App Readiness	Gets apps re		Manual Local System
Application Experience	Processes a		Manual (Trig Local System
Application Identity	Determines		Manual (Trig Local Service
Application Information	Facilitates t	Running	Manual (Trig Local System
Application Layer Gateway	Provides su		Manual Local Service
Application Management	Processes in		Manual Local System
AppX Deployment Service (Provides inf		Manual Local System
Background Intelligent Tran	Transfers fil		Manual Local Suctors
Background Tasks Infrastru	Windows in	Running	Apache2.4 Properties (Local Computer)
Base Filtering Engine	The Base Fil	Running	
Certificate Propagation	Copies user	Running	General Log On Recovery Dependencies
CNG Key Isolation	The CNG ke	Running	Log on as:
COM+ Event System	Supports Sy	Running	O Local System account
COM+ System Application	Manages th		Local System account
Computer Browser	Maintains a		
Credential Manager	Provides se	Running	Select User X
Cryptographic Services	Provides thr	Running	
DCOM Server Process Laun	The DCOM	Running	Select this object type:
Device Association Service	Enables pair		User or Built-in security principal Object Types
🔍 Device Install Service	Enables a c		From this location:
Cevice Setup Manager	Enables the		
Client	Registers an	Running	Locations
Carling Service Diagnostic Policy Service	The Diagno	Running	Enter the object name to select (examples):
Diagnostic Service Host	The Diagno		FILECLOUDDEMO5\filecloudazurefiles Check Names
Diagnostic System Host	The Diagno		
Distributed Link Tracking Cl	Maintains li	Running	
Distributed Transaction Co	Coordinates	Running	
Client DNS Client	The DNS Cli	Running	Advanced OK Cancel
Encrypting File System (EFS)	Provides th		
Extensible Authentication P	The Extensi		
Sunction Discovery Provide	The FDPHO		
Runction Discovery Resourc	Publishes th		OK Cancel Apply
Group Policy Client	The service	Running	Automatic (T Eocal System
🔍 Health Key and Certificate	Provides X.5		Manual Local System

🍓 memcached	Fast Memor	Running	Automatic	Local System
Microsoft iSCSI Initiator Ser	Manages In		Manual	Local System
Microsoft Software Shadow	Manages so		Manual	Local System
Microsoft Storage Spaces S	Host service		Manual	Network Service
🔍 MongoDB	MongoDB S	Running	Automatic	.\filecloudcl
🔍 Multimedia Class Scheduler	Enables rela		Manual	Local System
Net.Tcp Port Sharing Service	Provides abi		Disabled	Local Service
🔍 Netlogon	Maintains a		Manual	Local System
Network Access Protection	The Networ		Manual	Natural Sanica
Network Connections	Manages o		Mon	IgoDB Properties (Local Computer)
Retwork Connectivity Assis	Provides Dir			Select Liser X
Service Network List Service	Identifies th	Running		
Network Location Awareness	Collects an	Running	Select this object	type:
Network Store Interface Ser	This service	Running	User or Built-in se	curity principal Object Types
OpenOffice Server		Running	Eram this leastion	
Coptimize drives	Helps the c			
Reformance Counter DLL	Enables rem		FILECLOODDEN	Locations
Reformance Logs & Alerts	Performanc	Running	Enter the object n	ame to select (<u>examples</u>):
😪 Plug and Play	Enables a c	Running	FILECLOUDDEM	105\filecloudazurefiles Check Names
Portable Device Enumerator	Enforces gr			
Ser Power	Manages p	Running		
Second Print Spooler	This service	Running		
Reprinter Extensions and Notif	This service		Advanced	OK Cancel
Problem Reports and Soluti	This service			
😪 RdAgent		Running		
Remote Access Auto Conne	Creates a co			
Remote Access Connection	Manages di			
🧟 Remote Desktop Configurat	Remote Des	Running		
Remote Desktop Services	Allows user	Running		
Remote Desktop Services U	Allows the r	Running		
🔍 Remote Procedure Call (RPC)	The RPCSS	Running		
🧟 Remote Procedure Call (RP	In Windows			
🧠 Remote Registry	Enables rem			Cancel Apply
Resultant Set of Policy Provi	Provides a n	l	Iviariuar	Locar System
Routing and Remote Access	Offers routi		Disabled	Local System
🔍 RPC Endpoint Mapper	Resolves RP	Running	Automatic	Network Service
Secondary Logon	Enables star		Manual	Local System

6. Copy the file share path of file share created in step 2 from the Azure Portal ("\ *filecloudazurefiles.file.core.windows.net\fileclouddata*")

FileCloud Server Version 23.232 Installation Guide



7. Set the share path("**filecloudazurefiles.file.core.windows.net****fileclouddata**") as Storage Path in Managed Storage Settings.

*	Dashboard	Server	Storage	Authentication	Admin	Database	Email	Endpoint Back	up	License	Policies
USER	S/GROUPS										
-	Users	My Files	My Files Network								
	Groups	My Files St	My Files Storage Settings								
8	Admins										
MAN	IAGE	S	Storage Path \\Filecloudazurefiles.file.core.windows\filecloudata × Check Path								
	Team Folders			Specify the loca	tion to store	Cloud Files, thi	s must be wr	itable by Webse	rver.		
	Network Folders			Example path or Example path or	n Windows : n Linux : /op	c:\clouddata t/cloud/data					
~	User Shares			contents from the	he old storage	e location after location to th	he new.	onngurea, move	rine		
a,	Folder Permissions										
DEVI	CES	versions	to keep for	3							
	Devices		each file	Number of versi	Number of versions to keep						
MISC			Encryption	Manage							
۲	Audit			Manage encount	tion						
	Alerts			manage energy							
	User Locks	Disa	ble My Files								
≞	Workflows			Disable 'My File	s' [Managed	Storage]					
	Reports	Default U	Jser Storage	Units+ 2					GB		
SETT	INGS		Quota	Default storage	quota for ne	w user. Can be	overriden in	user details. Thi	s		
•	Settings			does not affect	existing user						
CUST	OMIZATION	User Sto	orage Usage	Exclude Shar	ies.				\sim		
1	Customization	Calculation									
SYST	EM			specity user sto	rage calculat						
~	Checks	Store D	Deleted Files								

8. Open the C:\xampp\mongodb\bin\mongodb.conf file. Edit the dbpath to point to the file share path you created in Azure Files storage.

Note: Before editing the mongodb.conf file make sure you have stopped the database and the webserver from the FileCloud Control Panel.

```
# mongodb.conf
```

```
# Where to store the data.
dbpath=\\filecloudazurefiles.file.core.windows.net\fileclouddata
\mongodbdata
```

```
#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

9. Restart the Webserver and the Database from the FileCloud Control Panel. Now all your files and the database data files will be stored in Azure Files Storage.

FileCloud Control Panel – 🗖 🗙							
FileCloud Control Panel v: 14.0.0.34114, Base Components: 14.0.0.34114							
Initial Setup: Install Check Web Portal: Admin Portal User Website							
Servers							
Webserver Ports: 80,443 Database Port: 27017							
Webserver: Running Start Stop Config Make Service							
Database: Running Start Stop Config Make Service							
Cron Task: Running SVC Start Stop Config Install							
(Optional) Helper Service is needed for network folders (for indexing and NTFS permissions)							
FileCloud Helper: Running SVC Start Stop							
(Optional) Memcache Server is used for File Encryption and Performance Improvements							
Memcache: Running SVC Start Stop <u>Make Service</u>							
Configuration							
Application Folder Config Folder Create SSL CSR Install SSL Cert							
Technical Support							
Need Help? Documentation Contact Support							

Amazon Web Services (AWS) Installation

FileCloud Public AMI (Amazon Machine Image) is currently available in Amazon AWS Marketplace.

F

FileCloud

Version 21.1.1.15106 | Sold by CodeLathe

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using AWS infrastructure (EC2, EBS, S3) you can jumpstart your own branded, file storage solution in few minutes at a compelling price point . FileCloud client apps are available for all the desktop and... Linux/Unix, Ubuntu 18.04 - 64-bit Amazon Machine Image (AMI)

See FileCloud AMI here on AWS Marketplace.

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

How Does It Work?

The FileCloud AMI image is built on top of Ubuntu.

- FileCloud stores the meta data and file share information in MongoDB database which is already pre-configured in the FileCloud AMI.
- The actual files can be stored in EBS or S3.
- For scalability and redundancy, we recommend you use Amazon S3 for production.
- We also recommend to take periodic snapshots of your running instance for disaster recovery.

Best Practices for an organization of up to 100 users:

- Select a t2.medium, m3.medium, or m3.large instance
- Use Amazon EBS for FileCloud stack (FileCloud application, Apache Webserver, MongoDB Database)
- Use Amazon S3 for cloud storage to provide a scalable, redundant infrastructure to satisfy any business requirement



AWS Marketplace Launch a variety of popular software on AWS in minutes

What if I'm not using Ubuntu?

Apart from FileCloud AMI on Ubuntu, we have also pre-built AMIs (BYOL - Bring Your Own License) available on supported versions of Windows Server. Please see the AWS marketplace links below,

FileCloud Enterprise File Sharing and Sync (Windows Server 2016)

→ FileCloud for Windows Server 2012

We have also the following paid AMI's available on AWS Marketplace,

FileCloud Enterprise File Sharing and Sync (20 Users)

→ FileCloud Enterprise File Sharing and Sync - Windows 2012 R2 -(20 Users)

Launching the FileCloud AMI



An Amazon Machine Image (AMI) is a master image for the creation of virtual servers, known as Elastic Cloud (EC2 instances) in the Amazon Web Services (AWS) environment.

Machine images are like templates that are configured with:

- A root volume. This is an operating system and other software.
- Permissions. These settings constrain AMIs for instance launches to the appropriate AWS accounts.
- A block device mapping. This ensures that the correct volumes are attached to the launched instance.

These elements determine the user's operating environment.

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

To launch the FileCloud AMI:

1. Complete the Pre-requisites



An AWS account allows you to:

- Open the Amazon EC2 console
- Choose a launch instance
- Launch your instance

🕑 If you've already signed up for Amazon Web Services (AWS), you can start using Amazon EC2 immediately.

😢 If you haven't signed up for AWS yet, use the following link to get set up to use Amazon EC2.

Setting up with Amazon EC2

💡 You can read more about Amazon Elastic Compute Cloud on Amazon's site.

2. Choose an AMI

You can begin the process of launching a Linux instance by using the AWS Management Console.

To launch an instance:

- 1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
- 2. From the console dashboard, choose Launch Instance.
- 3. The Choose an Amazon Machine Image (AMI) page displays a list of basic configurations, called Amazon Machine Images (AMIs), that serve as templates for your instance.
- 4. In the Search bar, type in FileCloud.
- 5. Next to the latest version, click Select.

Figure 1. An example of FileCloud listings in AWS Marketplace. (This image does not necessarily show the latest version.)

Q, FileCloud	× × ×	of 6 Products > >
Free tier eligible	FileCloud	Select
Free tier eligible	FileCloud ServerLink - Hybrid Enterprise File Sharing and Sync Solution ***** (0) 17.3.0.37658 Sold by CodeLathe Bring Your Own License + AWS usage fees Linux/Unix, Ubuntu Ubuntu 16.04 64-bit Amazon Machine Image (AMI) Updated: 3/18/18 FileCloud ServerLink is the most powerful hybrid file sharing, sync and backup solution for Enterprises. Using FileCloud ServerLink one can replicate the FileCloud site running More info	Select

3. Choose an Instance Type

When you launch an instance, the instance type that you specify determines the hardware of the host computer used for your instance.

Each instance type offers different capabilities, such as:

- compute
- memory

• storage capabilities

Instance types are grouped in instance families based on these capabilities.



Table 1. General Purpose Instance Types

Instance Family	Current Generation Instance Types
General Purpose	m5.large m5.xlarge m5.2xlarge m5.4xlarge m5.12xlarge m5.24xlarge m5d.large m5d.xlarge m5d.2xlarge m5d.4xlarge m5d.12xlarge m5d.24xlarge

Read Amazon's complete listing of Available Instance Types

CodeLathe recommends that you should select an instance type based on:

- Minimum requirement: m5.large
- For best performance: Select a type in the m series. For example: m5.xlarge

To choose the Amazon EC2 Instance type:

1. On the *Choose an Instance Type* page, you can select the hardware configuration of your instance.

4. Configure Instance Details

This step can change depending on the Instance Type you chose:

- T2 instances, such as t2.micro, must be launched into a VPC.
 - If your AWS account supports EC2-Classic and you do not have a VPC in the selected region, the launch wizard creates a VPC for you and you can continue to the next step.
 - Otherwise, the *Review and Launch* button is disabled and you must choose *Next: Configure Instance Details* and follow the directions to select a subnet.

Figure 2. Options for the next step after selecting an instance type.

	Family ~	Туре 🗸	vCPUs (i) 🔹	Memory (GiB) 👻	Instance Storage (GB)	EBS-Optimized Available (i)	Network Performance	IPv6 Support ·
0	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
					Cancel Prev	vious Review and Laund	ch Next: Configure Inst	ance Details

To configure instance details:

- If you selected an Instance Type of t2.medium or t3.medium, then you must enable T2/T3 unlimited. See Figure 3.
- 2. When you get to the Configure Security Group step, open up the port *80/443* for web access. See Figure 4.
- 3. You might need to open other ports such as 443 (HTTPS), depending on your business requirements.

Figure 3. Configure Instance Details

Network	(j)	vpc-2daa0148 (default)	٥	С	Create new VPC
Subnet	(j)	No preference (default subnet in any Availability Zone)	٥		Create new subnet
Auto-assign Public IP	()	Use subnet setting (Enable)	٥		
Placement group	(i)	Add instance to placement group.			
IAM role	(j)	None	٥	C	Create new IAM role
Shutdown behavior	(i)	Stop	٥		
Enable termination protection	(i)	Protect against accidental termination			
Monitoring	(i)	Enable CloudWatch detailed monitoring Additional charges apply.			
Tenancy	()	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	٥		
T2/T3 Unlimited	(i)	✓ Enable Additional charges may apply			
 Advanced Details 					

Figure 4. Configure Security Groups

🎁 Services 🕶 Edit 🗸			Help ¥
I. Choose AMI 2. Choose Instance Type 3.	Configure Instance 4. Add Storage 5. Tag Inst	ance 6. Configure Security Group 7. Review	
tep 6: Configure Security 6 security group is a set of firewall rules that con stance, add rules that allow unrestricted acces	Group Introl the traffic for your instance. On this page, y ss to the HTTP and HTTPS ports. You can creat	you can add rules to allow specific traffic to reach your instance. e a new security group or select from an existing one below. Lea	For example, if you want to set up a web server and allow internet traffic to reach your rn more about Amazon EC2 security groups.
Assign a security group:	Create a new security group		
	Select an existing security group		
Security group name:	launch-wizard-1		
Description:	launch-wizard-1 created 2014-08-25T15:10:00.0	22-04:00	
Type ()	Protocol (i)	Port Range (j)	Source (j)
SSH •	TCP	22	Anywhere - 0.0.0.0/0
HTTP -	TCP	80	Anywhere - 0.0.0.0/0
Warning Rules with source of 0.0.0.0/0 allow all	IP addresses to access your instance. We reco	mmend setting security group rules to allow access from known lf	P addresses only.
			Cancel Previous Review and Launc

You can read more about Amazon EC2 Security Groups.

To complete the Final Review and Launch, see the next step: Step 5: Launch the Instance

5. Launch the Instance

To launch an instance:

- 1. When you are ready, click *Review* and *Launch*
- 2. Next to your instance, select the acknowledgement check box, and then choose Launch Instance.
- 3. A confirmation page lets you know that your instance is launching.
- 4. Choose *View Instances* to close the confirmation page and return to the console.
- 5. On the *Instances* screen, you can view the status of the launch. It takes a short time for an instance to launch.
- 6. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name.
- 7. If the Public DNS (IPv4) column is hidden, choose Show/Hide Columns (the gear-shaped icon) in the top right corner of the page and then select Public DNS (IPv4).
- 8. It can take a few minutes for the instance to be ready so that you can connect to it.
- 9. Check that your instance has passed its status checks in the *Status Checks* column.
- 10. Note the Public DNS name to access your FileCloud site.

Figure 5. FileCloud Status in Your AWS dashboard.

🧊 Services 🗸	Edit 🗸								Venkat 🕶
EC2 Dashboard Events	Launch Instan	Connect	Actions V						
Tags	Filter: All inst	ances 👻 All instai	nce types 👻 🔍 S	earch Instances	:	×			
Reports Limits	Name	♀ - Instance ID ▲	Instance Type 🔹	Availability Zone -	Instance State 👻	Status Checks 👻	Alarm Status	Public DNS -	Public IP
INSTANCES		i-48a84f64	t2.micro	us-east-1a	running	🛣 Initializing	None 🍡	ec2-54-85-174-50.comp	54.85.174.50
Instances Spot Requests Reserved Instances									
 IMAGES AMIs Bundle Tasks 									
ELASTIC BLOCK STORE Volumes Snapshots									
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups	Instance: I-48	3a84f64 Public DN	IS: ec2-54-85-174-50	.compute-1.amazoi	naws.com	000			
Load Balancers Key Pairs Network Interfaces	Description	Status Checks	Monitoring Tags 48a84f64				Public DNS Public IP	ec2-54-85-174-50.compute	-1.amazonaws.com
AUTO SCALING Launch Configurations Auto Scaling Groups		Instance state 10 Instance type t2 Private DNS ip Private IPs 1		nal			Elastic IP Availability zone Security groups	us-east-1a	

2 Instance started with a public IP

6. Connect to the Instance

To connect to your instance:

- 1. Open a Web browser.
- 2. to access the FileCloud admin portal, type in the following URL:

http://<public_dns_name>/ui/admin/index.html

3. To login to the Admin Portal, use the following information:

Default Admin	admin
Default Password	Your amazon instance ID

• After logging in for the first time, you must change the admin password.

4. After logging in, you will see an Admin Attention window. Use this to install the FileCloud License.

P To receive a license you must register at the FileCloud license management portal.

7. Post-installation

After logging in to the Admin Portal, you will see an Admin Attention window. You will also see tags on the right side of the dashboard telling you about what needs to be done after installation.

Complete the following items after you are able to launch and connect to your instance:

V	Item			
	Remove the Installation Folder			
	The default FileCloud instance uses CodeLathe SMTP servers and accounts to send emails.			
	Change the SMTP servers and accounts to use your own servers for security purposes.			
	The admin email address is used in all the emails that sent out from the FileCloud System.			
	Change the admin email to your organization email address.			
	To show all the installed packages in this instance:			
	1. Open a Web browser			
	 Navigate to http://<public_dns_name>/install.</public_dns_name> Check the page and familiarize yourself with FileCloud components. 			
	The user name for the underlying Ubuntu OS is 'ubuntu'. Before launching the instance you will be required to create a key pair or you can use your existing key pair.			
	FileCloud recommends you use S3 for file storage instead of the EBS.			
	To understand how to setup S3 for FileCloud file storage, read Setting up FileCloud Managed S3 Storage			
	After you configure the FileCloud storage, follow the site setup instructions to setup the FileCloud site according to your requirements.			
	Take Periodic snapshots of your running instance for Disaster recovery and as an additional backup for FileCloud database and app.			
 The ability to install an Enterprise license with components (like Salesforce) is available in FileCloud Server version 18.2 and later. Your AMI image will automatically come with a standard or enterprise license. When you log in to the Admin Portal, you can automatically see the License type (BASE/ENTERPRISE) and also the total number of licenses on the dashboard. 				
	License Information			
	Licenses	52 Used / 100 Total		
	License Expiry	5-Oct-2019 (323 days left)		
	License Owner	CodeLathe Technologies Inc		

Need to seed data quickly into your new FileCloud installation?
 Seeding FileCloud for Amazon S3

FileCloud on AWS - User Deployment Guide

Introduction

Use AWS infrastructure (EC2, EBS, S3) to jumpstart your own branded, file storage solution in few minutes.

Use Cases

- File Sharing Portal- Use FileCloud to create your own own, branded file sharing, sync and mobile access, solution for your employees, customers and partners.
- File Sync Use FileCloud for effortless file synchronization across users computers, smart phones and tablets, so everyone can work together anywhere from any device
- Client Document Portal Use FileCloud to create a client document portal on AWS infrastructure to server your clients, customers and partners.
- Endpoint Backup and DLP Use FileCloud to securely backup your endpoint computing devices (PCs, Mobile Phones and Servers).
- Enterprise Data Protection and DLP: Use FileCloud's unique data leak prevention (monitor, prevent and fix) capabilities to protect your enterprise data across all your users devices (Computers, Mobile Phones/Tablets.
- File Server Enablement Use FileCloud's ServerSync to sync/backup you branch office windows files servers to FileCloud running on AWS to get low latency LAN access as well as remote access from anywhere.
- White Label Content Platform Use white label FileCloud Platform as part of your own product line to manage digital assets.

Overview of Typical Customer Deployment

FileCloud AMI's are available on the latest versions of Ubuntu and Windows. Depending on your requirements and familiarity, you can choose any operating systems supported by FileCloud. FileCloud stores the file, user and shares metadata in MongoDB (pre-installed in AMI) and actual files can be stored in a disk, AWS Elastic File System or AWS S3. For smaller deployments, disk is sufficient for file storage. For medium and large deployments, our recommendation is to use AWS S3 for file storage. The FileCloud AMI is also pre-configured for document preview and document indexing for full text search. It takes less than 30 minutes to configure the FileCloud AMI and get it running for production workload.

Prerequisites and Requirements

FileCloud AMI's are completely self contained. You don't need to install any additional software. Basic AWS skills are sufficient to deploy FileCloud on AWS. Simple deployments involve just EC2 and Disk (OR) EC2 and AWS S3. FileCloud AMI's are available as BYOL model. You need to register in our customer portal to get the trial license. Once you get the trial license you need to upload the license to your running EC2 instance. Since FileCloud AMI's are available on Ubuntu and Windows Server OS, you can choose the OS you are familiar with.



Architecture Diagrams





To access FileCloud, you only need port 80 (http) or 443 (https). We strongly recommend to use 443 and only allow SSL access. Depending on the underlying OS, you may need to open up port 22 (SSH access) and 3389 (Remote Desktop) for managing the FileCloud instance. Our recommended security practice is to specify the IP range for SSH and Remote Desktop instead of opening it for access from anywhere.

FileCloud secrets and keys are protected and managed in the FileCloud database. FileCloud supports encryption at Rest. To initialize encryption, administrator may supply an optional master password and start the initialization process. Once the initialization process is started, the following steps happen as part of the process:

- 1. An asymmetric key pair (private/public) known as "Master" key is generated with the optional master password.
- 2. A symmetric key known as "Plain File" key is generated.
- 3. The File key created in step 2 is encrypted using the Master private key resulting in an "Encrypted File" key.
- 4. All the existing uncrypted files (if they exist) in the FileCloud storage will be encrypted before the system will be ready for use. Look at the next section for more information on file encryption.

(i) Warning On Master Password

If an optional master password was specified, then administrator has to retain the password for future use. Without this password the encryption module cannot encrypt/decrypt files in the FileCloud storage.

Additional	details or	the keys:
------------	------------	-----------

Кеу	Key Details	User Input	Persistence	Remarks
Master public/ private key pair	 Asymmetric 4096 bits RSA sha512 digest 	Password (optional)	Both private and public keys are persisted.	 It is important to save the password (if one was provided).
Plain File Key	 Symmetric AES 128 bits 	None	Not persisted	 Plain file key will be used to encrypt/ decrypt all files using symmetric encryption. This key will not persisted but will be cached for performance. The cache will be valid for the lifetime of the FileCloud server process.

Кеу	Key Details	User Input	Persistence	Remarks
Encrypted File Key	 Encrypted using master public key 	None	Encrypted file key is persisted	 Decryption of the encrypted file key results in plain file key. Decryption of the encrypted file key will be done using the master private key and optional master password. Encrypted file key is decrypted every time FileCloud server is started. The plain key that is a result of decryption process is cached for the lifetime of the FileCloud server process. Restarting the server will need a fresh decryption.

If you are going to use S3 for Managed File storage, please see the security section given below to understand possible file encryption options available.

Planning Guidance

Security

When you deploy FileCloud you can use EBS for managed file storage or you can choose the S3. If you choose S3, Please use the following instructions to set up your S3 for FileCloud.

Setting up Amazon S3 Credentials

- 1. Log into Administration Portal
- 2. Navigate to Settings
- 3. Select "Storage" tab
- 4. Enter the S3 config information. Refer to the following table for more information about each setting
- 5. Click on Save S3 setting

Field	Description
S3 Key	This is your amazon authentication key (To get your access key, visit Amazon security portal) . For IAM user, it requires the IAM Policy for S3 Access given below.
Field	Description
---	--
S3 Secret	This is your amazon authentication secret (To get your access key, visit Amazon security portal). For IAM user, it requires the IAM Policy for S3 Access given below .
S3 Bucket Name	Provide a bucket name. The bucket should be new (in some circumstance, previously used bucket in FileCloud could be used).
	It is very important that the S3 bucket is never modified outside of the FileCloud subsystem.
S3 Storage Folder	Optional: All files will be stored inside this root storage folder (Will be created automatically).
S3 Region	Optional: Provide the region string. If the region is not provided, then US Standard region will be used. If you are planning to have your
	bucket in different region(say europe, south east) provide the correct region string. The strings should match the region string published by amazon.
	Note: For govcloud installs, you must use region string: us-gov- west-1
S3 End Point URL	Optional: This is the S3 endpoint. Use this if you are planning to use your own S3 endpoint (typically S3 compatible storage) or if it is a unpublished region.
	For using AWS end point, it must be the ones published at here
Note: The Amazon S3 Bucket shou Do not add/edit/modify files direct installation.	ld NEVER be modified outside of FileCloud subsystem tly using Amazon tools. Doing so will destabilize your FileCloud

ном	E	Manage Set	ettings						
*	Dashboard								
USER	S/GROUPS	Server Storage	Authentication Admin Database Email Endpoint Backup Licens						
2	Users								
쓥	Groups	My Files Network	k						
&	Admins	Amazon S3 Storage S	Settings (My Files)						
MAN	AGE								
	Team Folders	S3 Key							
	Network Folders		S3 account key						
e 🕈	User Shares	S3 Secret							
Q_{ϵ}	Folder Permissions	S3 Secret S3 Bucket Name	S3 account secret						
DEVI	CES								
	Devices	S3 Bucket Name	Leave empty to auto generate						
MISC			(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique						
۲	Audit		and cannot be changed once created.						
	Alerts	S3 Storage Folder	(Optional) Folder name to place the files						
	User Locks	S3 Secret S3 Bucket Name S3 Storage Folder S3 Region	(Optional) Folder name. If specified, a folder with this name will be created in the burket and files will be placed under it. Once configured this cannot be						
₫	Workflows		changed.						
	Reports	S3 Bucket Name S3 Storage Folder S3 Region	Ex: us-east-1						
Q	Federated Search		(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region						
ß	Metadata		string as published by Amazon and cannot be changed once the bucket is created						
SETT	INGS								
•	Settings	S3 End Point URL	Ex: https://s3.amazonaws.com						
CUST	OMIZATION	-	(Optional) AWS S3 end point. Leave it empty if using Amazon's S3 service. The region string will automatically select the correct Endpoint. End point cannot be						

IAM Policy for S3 Access

If you are going to use S3 for file storage, FileCloud requires S3 access in order to create bucket and manage it. The IAM user used to manage it must have the following permissions. This shows access to all buckets in your S3 console. You can restrict to specific bucket using the appropriate resource arn. Something like arn:aws:s3:::bucket_name

{

```
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
```

```
"s3:CreateBucket",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ]
}
```

}

Setting up S3 Encryption for FileCloud Managed Storage

S3 Managed Storage Encryption support to protect data at rest is available in Filecloud. The communication between FileCloud to AWS will use SSL encryption resulting in complete protection for data in transit. Once the S3 is set up correctly, a new field "S3 Encryption" will be available under Amazon S3 Storage Settings.

FileCloud supports the following Server Side Encryption:

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

To manage S3 encryption,

- 1. Log into Administration Portal
- 2. Navigate to Settings
- 3. Select "Storage" tab
- 4. Click on "Manage" button in the S3 Encryption option

Depending on the status of encryption, you will see "Enable encryption" or "Disable encryption" button.

 Enabling encryption will attempt to encrypt all available data in the bucket as well as all new data will be encrypted. This can take some time depending on the amount of existing data in the bucket. Please modify encryption setting when there is minimal activity in FileCloud.
 Though, changing encryption can be done at any time, we recommend using off-peak hours to avoid any unexpected access issues

For Windows, If your xampp is installed in location other than c:\xampp, then add the following key in <your xampp folder>\htdocs\config\cloudconfig.php
 For example, if your xampp is in D:\xampp, then in file D:\xampp\htdocs\config\cloudconfig.php, add the following string (any location before the bottom "?>" line)
 define("PHPBIN_PATH","D:\\xampp\\php\\php.exe");

Manage S	3 Encryp	tion		×
Encryptio	An Status Encryption is disabled on Type Amazon S3-Managed Key Encryption \ddagger Note 1. Files are currently not encrypted			
Encrypti	on Type	Amazon S3-Managed Key Encryption \$)	
	Note			
	1. Fil	es are currently not encrypted	↓	
			€ Enable encryption	Close
				0.030

FileCloud Server Version 23.	232 Installation Guide
------------------------------	------------------------

Manage S	3 Encryp	tion		×
Encryption	n Status	Encryption is disabled		
Encryptic	on Type	Amazon KMS-Managed Key Encryption \$		
KMS SSI	E Key ID	OPTIONAL. Leave empty to use default KMS Key		
	Note			
	1. Fil	es are currently not encrypted		
			Enable encryption	Close

Manage S	3 Encryp	tion		×
Encryptio	n Status	Encryption is disabled		
Encrypti	on Type	Customer Supplied Key Encryption		
Encrypt	tion Key	32 character encryption key		
	Note			
	1. Fil	es are currently not encrypted		
			■ Enable encryption	Close

Costs

T2.Medium or T3.Medium is suffice to run FileCloud for 100 users. File Storage cost depends on the storage method you choose (EBS, EFS or S3) and amount of files you will be storing and the access pattern. Typical cost for 100 users and 10 TB storage comes around 2800-3250\$ per year.

Sizing

A T3.medium (Unlimited) can handle approximately 30-40 FileCloud calls per second which equates to approximately 100-200 users using FileCloud. Depending on number of users and thier access pattern, you can vertically (choose bigger instance) or horizontally (add more instances) can scale your deployment.

Deployment Guidance

Deployment Assets

FileCloud pre-built AMI's (Amazon Machine Image) are currently available in Amazon AWS Marketplace. We have prebuilt images for both Linux (Ubuntu) and Windows Server OS. You can choose the base OS as per your preference.

Steps to Launch FileCloud AMI

1. Login to AWS management console and Click EC2 (Virtual Servers in the Cloud)



2. Click Launch Instance



3. Search FileCloud AMI in AWS marketplace. Choose the latest version.

The version details in the screen shot is for reference purposes only. The latest version details may be different from the information shown.



4. Choose the desired Amazon EC2 Instance type. We recommend atleast t2.medium or t3.medium. **However, for best** performance, the "m" series is better. For example m3.medium. If you choose the t2 or t3 series, please enable T2/T3 unlimited when you configure the instance.

🗯 Safari File Edit View History Bookmar	ks Window Help	5 🯮 🍥 奈 🔽 86% 🔳	Sat 6:59 PM 🔍 🌏 🖃
		Ċ	0 1
Amazon Web Services AWS Installation - File	Cloud - FileCloud Support	EC2 Management Console	+

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

	Family ~	Туре 🗸	vCPUs (j) 👻	Memory (GiB) 👻	Instance Storage (GB)	EBS-Optimized Available (i)	Network Performance	IPv6 Support v
0	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
0	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
0	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
0	General purpose	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

🗨 Feedback 🔇 English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

				.amazon.com		Ċ			0 1
Amazon Web Services AWS	S Installation - FileCloud	- FileCloud Support				EC2 I	Management Console		
aws Services - R	esource Groups	~ *				Ф м	ladhan Kanagavel 👻	N. Virginia 👻	Support 👻
Choose AMI 2. Choose Instance Type	3. Configure Insta	nce 4. Add Storage	5. Add Tags	6. Configu	re Security Group	7. Review	٨		
ep 3: Configure Instan	ice Details								
Network	i vpc-2daa0	148 (default)		• C	Create new VP	°C			
Subnet	(i) No prefere	nce (default subnet in any	y Availability Zone)	٥	Create new su	Ibnet			
Auto-assign Public IP	(i) Use subner	setting (Enable)		٥					
Placement group	i Add ins	tance to placement g	roup.						
IAM role	None			• C	Create new IAM	VI role			
Shutdown behavior	(i) Stop			٥					
Enable termination protection	(i) Protect	against accidental ter	rmination						
Monitoring	Enable Additional	CloudWatch detailed charges apply.	monitoring						
Tenancy	i Shared - R	un a shared hardware inst	tance	٥					
	Additional	charges will apply for	dedicated tenam	cy.					
T2/T3 Unlimited	 (i)	charges manapply							
Advanced Details									
					Ca	ancel Prev	vious Review an	nd Launch	Next: Add Storag
				- 0000 - 0010	Web Con	the tre or ite	Mileten All debte seen	Difuseu D	Tormo of Lio

5. Configure the security group to open up the port 80/443 for web access.

🧊 Servi	ices 🗸 🛛 Edit 🗸								Venkat 🗸	N. Virginia 🕶	Help 🗙
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Tag Instance	6. Configure Security Gro	p 7. Review					
Step 6: Co A security group instance, add ru	onfigure Security is a set of firewall rules that les that allow unrestricted ad	Group control the traffic for cess to the HTTP and	your instance. On d HTTPS ports. Yo	this page, you ca ou can create a ne	in add rules to allow speci w security group or select	c traffic to reach from an existing	your instance. For example, if you wan one below. Learn more about Amazon	t to set up a web server a EC2 security groups.	and allow inte	ernet traffic to r	each your
	Assign a security grou	p: Oreate a new	security group								
		Select an exis	ting security grou	p							
	Security group name	launch-wizard-1									
	Description	: launch-wizard-1	created 2014-08-25	5T15:10:00.022-04:	DO						
Туре 🕕		Pro	i) iocol		Port	Range 🕕		Source (i)			
SSH	-	TCI	P		22			Anywhere • 0.0.0.0/0			⊗
HTTP	-	TC	P		80			Anywhere - 0.0.0/0			8
A Warnin Rules w	ng vith source of 0.0.0.0/0 allow	all IP addresses to a	ccess your instanc	ce. We recommen	d setting security group ru	ies to allow acces	ss from known IP addresses only.				
										ļ	
								Cancel	Previous	Review ar	nd Launch

() Note: You might need to open other ports such as 443 (HTTPS), depending on your business requirements.

6. Complete the Final Review and launch the instance.

	v Resou	rce Groups	~ %				φ.	O	hio 👻 Supp	ort 👻
oose AMI 2. Choose Insta	ance Type 3.	Configure Instanc	e 4. Add Storage 5.	Add Tags 6. Configure Security Group	7. Review					
7: Review Ins review your instance laur	tance La	unch J can go back to	edit changes for each se	tion. Click Launch to assign a key pair	to your instance and complete the launch p	process.				
Your instances may be You can also open ac	stances' sec be accessible fi dditional ports i	rom any IP addroin your security g	ecurity group, FC se ress. We recommend that group to facilitate access t	curity group, is open to the worl you update your security group rules to a o the application or service you're runnin	d. allow access from known IP addresses only g, e.g., HTTP (80) for web servers. Edit se	/. curity groups				
VI Details									E	dit AM
FileCloud v18. FileCloud v18.1:0 Root Device Type: el stance Type	.1.0.682_Ubuntu-16 0.682_Ubuntu-16 bs Virtualization	ntu-16.04 - am 5.04 type: hvm	il-08abc2fb9fb4361b3						Edit instan	ce type
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance				
t2.medium	Variable	2	4	EBS only	-	Low to Moderate				
curity Groups									Edit security	group
Security Group ID		Nam	e	Descr	iption					
-8f2e5ce6		FC sec	curity group	launch-v	vizard-1 created 2017-04-05T11:11:23.928-	-05:00	-			
I selected security grou	ips inbound ru	iles								
Type (j)		Protocol (j)		Port Range (i)	Source (j)	Description (i)				
HTTP		TCP		80	0.0.0.0/0					
HTTP		TCP		80	::/0					
224		TCP		22	0.0.0.0/0					
5511		700		443	0.0.0.0/0					
HTTPS		TCP								

7. You can see now your FileCloud is running in your AWS dashboard. Please note the Public DNS name to access your FileCloud.

🎁 Services 🗸															Venkat •	*
EC2 Dashboard Events	•	Launch Insta	nce	Connect	Actions V											_
Tags		Filter: All inst	tances	 All inst 	tance types 👻	Q, :	Search Instances		×							1
Reports Limits		Name	9-	Instance ID	 Instance Ty 	pe 👻	Availability Zone -	Instance State -	Stat	tus Checks 👻	Alarm Status	;	Public DNS	Ŧ	Public IP	
INSTANCES				i-48a84f64	t2.micro		us-east-1a	running	X	Initializing	None	7	ec2-54-85-174-50.con	ıp	54.85.174.50	
Instances Spot Requests Reserved Instances																
IMAGES																
AMIs Bundle Tasks																
ELASTIC BLOCK STORE																
Volumes Snapshots																
NETWORK & SECURITY																
Security Groups		•					III									
Placement Groups		Instance: i-4	8a84f64	Public	DNS: ec2-54-85	-174-50).compute-1.amazo	naws.com								
Load Balancers		Description	Stat	us Checks	Monitoring	Tags										
Network Interfaces			I	nstance ID	i-48a84f64						Public	DNS	ec2-54-85-174-50.co	npute	-1.amazonaws.com	
AUTO SCALING			Inst	ance state	running t2 micro						Publi	c IP	54.85.174.50			2
Launch Configurations			P	rivate DNS	ip-172-31-26-235	.ec2.inte	ernal				Availability z	one	us-east-1a			
Auto Scaling Groups				Private IPs	172.31.26.235						Security gro	oups	launch-wizard-1. vie	w rule	s	

8. Type 'http://<public_dns_name>/ui/admin/index.html' in your browser to access the FileCloud admin portal. If the Webpage fails to load, please verify port 80 is open as mentioned above in Step 5.

Default Admin	admin	
Default Password	Your amazon instance ID	
Note	Please change the admin password upon first login.	
@Enclosed x +		7 ×
(←) → C ²	html	<u>⊼</u> ≡
Admin Port	ttal	

Password Enter admin Sign in Use Single Sign On (SSO) O More Options

9. Once you logged into the admin portal, please install the FileCloud License. Please register at our license management portal (https://portal.getfilecloud.com/ui/user/index.html?mode=register) to get trial licenses.

🧃 FileCloud 🛛 🗙	+							-	٥	×
← → ♂ ☆	(i) ec2-18-218-216-29.us-east-2.compute.amazonaws.com/ui/	admin/index.html#dash.				•	·· 💟 🔂	± ⊪/	11 人	≡
FILECLOUD		Admin Attention Required		×		i	Install Folder Remove 'install' folder aff	er installation.		
номе	A Dashboard	Action Item	Description				Example Windows: c:\x /var/www/html/install or /	mpp\htdocs\insta var/www/install		
Dashboard USERS/GROUPS	II System Summary	Invalid License File	Upload your license via Ins	all License	Month 6 Months 2 Refresh	" i	Set Admin Email Go to Settings, Email to			
Groups	Hover over the graph for details	1	Install License		Cient Requests Served	(
MANAGE	0.5					1	Go to Settings, Server to			
Network Folders User Shares	0.4					4 i	Set Email Server Go to Settings, Email to email.	set a valid email :		
Qe Folder Permissions DEVICES DEVICES	0.2			S Close		Quick Ac	Demo SMTP Server ena	iled during trial	erts [®]	
Devices	0.0 Fri Sat	Sun M	on 1	ue Wed	Thu	Add Use	er oup			
 Audit Alerts¹ 	0 % QUOTA USAGE 0 8 Used 6 % TEMP DIS	K USAGE 65 KB Used 0 %	LICENSE USAGE	0 Used 12 % SETUP C	HECKLIST 2. Completed 17. Total	Add Ne	twork Shares min			
User Locks	License Information		🖌 Manage	Version Information						
Reports	Licenses	Not Installed		Current Version			18.1.0.682			
O Federated Search	License Expiry			Latest Version			18.1.0.682			
Metadata	License Owner			Update(s) Available			NO			
Settings	Recent Access Locations		×	File Type Distribution				R	tefresh	
CUSTOMIZATION CUSTOMIZATION SYSTEM			j.							
✓ Checks										

- 1. The user name for the underlying Ubuntu OS is 'ubuntu'. Before launching the instance you will be required to create a key pair or you can use your existing key pair.
- 2. If you go to 'http://<public_dns_name>/install', the page will show all the installed packages in this instance. Check the page and familiarize yourself with FileCloud components. Before going production move the install folder to somewhere else.
- 3. We recommend you to use S3 for file storage instead of the EBS. Please check the following section (Enabling Amazon S3 Storage) to know how to set up S3 for FileCloud file storage.
- 4. The default FileCloud instance uses our SMTP servers and accounts to send emails. Please change this to your SMTP server for security purposes.
- 5. Please change the admin email to your organization email address. This email address is used in all the emails that sent out from the FileCloud System

Enabling Amazon S3 Storage

warning

Do not change this once the installation is set up and data is already stored. This should only be set up for fresh installs.

When changing the storage type from local to amazons3, the file(s)/folder(s) that have been already stored in the local storage will not be automatically moved to was s3 storage.

In this case, adminstrator has to manually export file(s)/folder(s) from local storage before changing storage type and manually import them after changing storage type.

Be very careful when changing the storage path, If done improperly it could lead to data loss.

To enable Amazon s3 storage as the backend,

<u>Step 1:</u>

Edit the file "WWWROOT/config/cloudconfig.php" and change the line

define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");

to read as

define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");

<u>Step 2:</u>

Rename file "WWWROOT/config/amazons3storageconfig-sample.php" to "WWWROOT/config/ amazons3storageconfig.php"

Nothing needs to be added or edited in amazons3storageconfig.php

 In Windows WWWROOT is typically c:\xampp\htdocs and in Linux it is /var/www/html e using

Once you configured the FileCloud storage, Please follow the site setup instructions to set up the FileCloud site according to your requirements

Operational Guidance

Health Checkup

AWS offers excellent system, instance status checks and CloudWatch monitoring. Pay attention on CPU utilization, Network In/Out and Network Packet In/Out of your EC2 instance. Using CloudWatch monitoring scripts, you can also monitor memory, swap, and disk space utilization of your EC2 instance.

Apart from the standard AWS monitoring metrics, FileCloud also offers system alerts. FileCloud Alerts are available in FileCloud's Admin portal.

This page tracks all unhandled exceptions, system error messages generated in the FileCloud server. The number of alerts are shown in the Dashboard and the Alerts page will show detailed information about the various errors encountered.

Depending on the error, you might need to take steps to correct the problem. For example, if alerts indicate that system is frequently running out of memory, then system memory may need to be increased.

To view alerts:

- 1. Log into the Administration portal.
- 2. On the left navigation panel, click *Alerts*.

The following view shows errors detected by FileCloud. The alerts are categorized as Informational, Warning, Critical and Fatal. Always pay attention to critical and fatal errors. FileCloud administrators also get periodic Administrator Summary emails that will show the number of alerts.

			🗎 dev1.co	delathe.com	Ċ		
FileClou	d on AWS - User Deployment Guid	e - FileCloud - FileCloud	Support		FileCloud	I	+
							🛔 admin 🗸
HOME	Alerts				h	t	0
USERS/GROUPS	Filter Varnin	ıg	\$		Remove	Clear All	
Lusers	Date	Severity	Description				ACTIONS
Groups	2018-Jun-13 11:33 AM	Warning	Desynced set definitions found	in the metadata_values collection			i
Admins MANAGE	2018-Jun-13 12:15 AM	Warning	Desynced set definitions found	in the metadata_values collection			1
Team Folders	2018-Jun-13 12:05 AM	Warning	Desynced set definitions found	in the metadata_values collection			i.
Network Folders	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	1
🔿 User Shares	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	1
Q Folder Permissions	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	1
DEVICES	C 2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	i .
Devices	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	1 - C
MISC.	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	i
④ Audit	2018-May-30 09:52 AM	Warning	Failed Upload for My Files: Disl	Usage Size Limit Exceeded for hameetha Usage:	2822031520 Limit:	1073741824	i.
Alerts 1							
User Locks				H 4 Page 1 of 100 • H			
A Workflows				10001043			
Reports							
Q Federated Search							
🗈 Metadata							
SETTINGS							
Settings							
CUSTOMIZATION							
Ungrade							
-i- opqrade							

Backup and Recovery

FileCloud supports unlimited file versioning and to recycle bin. You can configure this options by logging in to FileCloud admin portal. This provides protection from accidental deletes by users.

In addition to that, please take periodic snapshots of your running instance for disaster recovery and as an additional backup for FileCloud database and app. If you are not taking snapshots of your running instance, atleast make sure you are backing up the mongodb database to a disk or S3 using AWS CLI. As long as we have the FileCloud database, we can recover the FileCloud application from instance/service failure.

The following instruction will backup the mongodb to a designated s3 bucket (You can also make it as a cron job so that it runs periodically),

cd /var/lib/mongodb
aws s3 sync . s3://my-bucket/fileclouddbbackup/

In case of instance failure, Please start a new FileCloud AMI and and follow the instructions below to bring the instance up and running.

1. Before making any changes, stop mongodb service

```
service mongod stop
```

2. Copy the backup database files back to /var/lib/mongodb from the s3 bucket

```
cd /var/lib/mongodb
aws s3 sync s3://my-bucket/fileclouddbbackup/ .
```

3. Finally start the mongodb service using following command.

service mongod start

Routine Maintenance

We release 2 or 3 major releases every year. Routine maintenance requires you keep your FileCloud system updated to the latest version.

Generally, new FileCloud release availability will be notified in two ways:

- 1. By subscribing to the FileCloud Mailing List
- 2. By seeing the version update available in the FileCloud Admin Dashboard.



FileCloud offers in-place system updates. Please follow the instructions to update FileCloud from the admin portal.

1. Login into the admin UI. Select "Upgrade" from the left-side navigation panel.



- 2. In the upgrade screen, click on "Click here to upgrade" button.
- 3. If there are no new updates available, no additional actions required.
- 4. If there are any new updates available, a popup will be shown with new update information.

G filecloud		Upgrade Warning ×	
A Dashboard	Manage Upgrade	Read the release notes to view changes that affect your installation.Release Notes	
Users/groups	Version information	 It is recommended to make a backup of all data before doing a upgrade. If there are new versions of webserver, database and helper services, please update 	
Groups	Current Version 14.0.0.34030	them separately. If this node is part of a HA cluster, please remember to upgrade all the nodes. 	
a Admins	Latest Version 14.0.0.34030	Click 'Ok' to continue.	
MANAGE			
A Network Folders	Upgrade Start Upgrade		
🥐 User Shares	Release Notes	OK Cancel	
Q Folder Permissions			
DEVICES			
Devices			
MISC.			

- 5. Click on the "Click here to Upgrade" button to start the upgrade process.
- 6. The upgrade process will check for perform the upgrade and a report will be generated after the update process is completed

file cloud	
A Dashboard	Manage Upgrade
USERS/GROUPS	
👗 Users	Version information
🚰 Groups	Current Version 14.0.0.34030
admins Admins	Latest Version 14.0.0.34030
MANAGE	
Network Folders	Upgrade Start Upgrade
Iser Shares	Release Notes
🔍 Folder Permissions	
DEVICES	
	Update completed without errors. Make sure to open the install check page and verify all the checks are OK before proceeding.
MISC.	Filter Message : Message Type : All 🗸
Audit	Message
Alerts	===== Downloading update =======
A Liser Locks	Using override un for update : http://patch.codelathe.com/tonidocloud/qa/installer/file_cloud.zip
	===== Unpacking update =======
A Workflows	===== Cleaning update =======
Reports	===== Checking permissions =======
SETTINGS	===== Backup server detected. Downloading =======
A Settings	===== Unpacking backupserver zip======
ige occurigo	===== Loading file signatures =======
CUSTOMIZATION	=====Applying update======
Customization	Copying the Cysamppintaocs/resources/backup/activatesite.pnp
SYSTEM	Copying meamppimouc_resources/backup/backup.class.pnp
 Checks 	Conving Tile Cytampp model/resources/bekup/bekup/sit
	Copying the Cysampp model resources becopy becopy responses on the company of the Cysamp model and the Cysamp model and the company of the Cysamp model and the cysamp model a
T Upgrade	En and the second process of the second second process and the second seco

- 7. Once the upgrade is completed, you will be redirected to the install verification page at http://site/install
- 8. Once it is verified that the checks are complete, refresh the browser UI (Ctrl + F5) to get the latest updated User Interface.

Emergency Maintenance

If the EC2 instance where you are running FileCloud is degraded, You have two options:

- 1. Take the snapshot of EBS disk and start an instance from the snapshot.
- (or)
 2. If option 1 is not feasible, please start a new FileCloud AMI and copy the backed up FileCloud Database files to / var/lib/mongodb (Linux) or c:\xampp\mongodb\bin\data (Windows). Then start the mongod service.

Support

Please send an email to support@filecloud.com to receive technical support.

- We answer all support questions within one business day and most within a couple of hours
- If your question or issue cannot be resolved via email, our support team will connect remotely via screen sharing software to troubleshoot and fix the problem on your server

Support Costs

Your annual FileCloud subscription includes a basic support plan, software updates, and security updates. For pricing of advanced support plans, please contact our sales team.

Accessibility

Reference Materials

FileCloud Site Setup Guide - FileCloud Site Setup Guide FileCloud End User Guide - FileCloud End User Guides FileCloud API Getting Started Guide - FileCloud Developer Guide

Seeding FileCloud for Amazon S3

These instructions should be used only for new installations (or, as shown in the last procedure, for migrating from FileCloud Server to FileCloud Online).

These instructions will not work if you are seeding a system with ServerLink enabled. Contact support.

Initially, when FileCloud is ready for production purposes, you may need to pre-populate the server with files and folders for FileCloud users.

- FileCloud is bundled with a tool to pre-load files and folders before you grant users access.
- These instructions explain how to use the FileCloud Server tool for seeding data into your deployment.

How To Seed Data

1. Enable MongoDB

To use the seeding tool, MongoDB should be enabled and running in PHP CLI mode.

- This may require you to edit the PHP.ini file.
- In Windows, the MongoDB module is already enabled by default.
- If MongoDB is not enabled for PHP CLI mode, the tool will fail.

Enable MongoDB:

In Linux enter:

```
[root@cnfc php.d]# php -m | grep mongodb
mongodb
[root@cnfc php.d]#
```

In Windows enter:

```
C:\Windows\system32>C:\xampp\php.exe -m | findstr mongodb
```

C:\Windows\system32>

If you do not get the above results, please Contact FileCloud Support.

2. Use the seed command

1. In a command line enter: For Windows:

cd c:\xampp\htdocs\resources\tools\seeding
PATH=%PATH%;C:\xampp\php

For Linux:

```
cd /var/www/html/resources/tools/seeding
```

Then, for both Windows and Linux, enter:

```
php seed.php -h <hostname>] -p <from path> -i -d <storagepath> -m <s3inipath> -u
<user> -r
```

Parameters:

[required] -h <host> Site host name or 'default' for default site.

[required] -p <from path> Source path from which files are seeded.

[optional] -i Seed files. Set this flag to seed files.

[optional] -d <storagepath> Seed files from source path specified with -p to this existing storage path.

[optional] -m <s3inipath> Path to migrate.ini. This ini file will be used to migrate existing local storage to S3 storage.

[optional] -u <user> User whose files are to be imported. File with the user name should exist in the source path. Applicable only with -i.

[optional] -r Reset existing database. This will reset the databases, so use it with caution.

() The seed command deletes the source files after uploading. This is designed to improve the speed of seeding.

Seeding Scenarios

Seed files for multiple users without resetting databases

To seed files for multiple users at the same time, prepare a top directory(source path) with separate folders for each user to be seeded with data. Under the user specific folder place files/folders to be seeded for that user. Run the following command to seed all the users from the prepared source path.

Linux seeding files/folders for multiple users - Default site

```
php seed.php -h default -p /tmp/seedfolder -i
```

The following code shows how to export files for user 'jdoe' from site site21.hostedcloud.com to directory 'cloudexport'.

Windows seeding files/folders for multiple users - Default site

```
php seed.php -h default -p C:\temp\seedfolder -i
```

(i) Note

- If user account exists, seeded files/folders will be imported to those accounts
- If user accounts doesn't exist, user accounts will be created before seeding.

Seed files for multiple users resetting databases

To seed files for multiple users at the same time, prepare a top directory(source path) with separate folders for each user to be seeded with data. Under the user specific folder place files/folders to be seeded for that user. Run the following command to delete all the existing data and seed from the prepared source path.

Linux resetting and seeding files/folders for multiple users - Default site

```
php seed.php -h default -p /tmp/seedfolder -i -r
```

Windows resetting and seeding files/folders for multiple users - Default site

```
php seed.php -h default -p C:\temp\seedfolder -i -r
```

(i) Note

- All the existing user accounts and its associated data will be deleted before the seeding.
- New user accounts will be created before seeding. Default username and password will be used (i.e password → password)

Seed files for a single user

Windows seeding files/folders for single user - Default site

```
php seed.php -h default -p C:\temp\seedfolder -u jdoe -i
```

(i) Note

- Data will be seeded for a single user.
- In this case, command expects a folder **jdoe** to exist under the source path.

Seed files into an existing path

To seed files into an existing FileCloud storage path, prepare a top directory(source path) with a single folder under which files/folders to be seeded are placed.

Run the following command to seed the single folder and its contents to an existing FileCloud storage path.

Linux seeding files/folders into an existing storage path - Default site

```
php seed.php -h default -p /tmp/seedfolder -d /jdoe/march
```

Windows seeding files/folders into an existing storage path - Default site

php seed.php -h default -p C:\temp\seedfolder -d /jdoe/march

(i) Note

 In this case, the command imports a single folder under the source path into the FileCloud storage path /jdoe/march. All contents of seedfolder are copied to /jdoe/march, but the folder seedfolder is not copied.

Migrate local storage to S3 storage

The seeding tool can also migrate files from local storage to S3 storage. When the tool is run in this mode, it does the following steps:

- 1. Checks if AWS CLI is installed on the system running the tool
- 2. Checks if a valid migration ini file is specified. Look below for the file format.
- 3. <u>Important</u>: Deletes the existing S3 storage database. If the site was never configured for S3 before, then this should not be an issue.
- 4. Creates a new S3 storage database and imports the data from local storage database converting it into S3 storage database format on the fly.
- 5. Creates multiple AWS CLI commands to upload data from the local storage to the S3 bucket. The details of this transfer are generated using the specified ini file.
- 6. Executes the AWS CLI commands prepared in the previous step.

Run the following command to migrate from local storage to S3 storage

Linux migrating from local storage to S3 storage

php seed.php -h default -m /tmp/migrates3.ini

Windows migrating from local storage to S3 storage

php seed.php -h default -m C:\temp\migrates3.ini

S3 migration ini file

```
aws_storage_bucket = "company.bucket"
aws_storage_folderprefix = "site1"
aws_access_key_id = "AKIAT4YDRDUSR0863KJJ"
```

```
aws_secret_access_key = "stPwbS3Y1KrZGUkVbNcYJx+8S/ZZKFR00jUdG9e9"
aws_region = "us-east-1"
```

Migrate from FileCloud Server to FileCloud Online

If you are migrating to FileCloud Online, the full set of databases has to be exported along with migration. This can be achieved with the following commands.

Linux migrating from local storage to S3 storage

```
php seed.php -h default -m /tmp/migrates3.ini -e /tmp/dbexport
```

Windows migrating from local storage to S3 storage

```
php seed.php -hdefault -mC:\temp\migrates3.ini -e C:\temp\dbexport
```

Contact FileCloud Support for help with this procedure.

Amazon GovCloud AWS Installation

Prerequisite: One needs to have Amazon AWS GovCloud account to use the GovCloud infrastructure. If you are a federal, state govt agency or a US business working with government contracts, you can get AWS GovCloud account from Amazon. You can apply for an Amazon Govcloud account here (https://aws.amazon.com/govcloud-us/contact/). Once your account is approved, you can start using the AWS GovCloud infrastructure. Note that the Amazon GovCloud admin console as well as the account is different from your regular AWS account. Not all aws services are available under AWS GovCloud. The AWS GovCloud (US) Region allows customers to adhere to: US International Traffic in Arms Regulations (ITAR), Federal Risk and Authorization Management Program (FedRAMP), and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Levels 2, 4, and 5.

FileCloud Public AMI (Amazon Machine Image) is currently available in Amazon AWS GovCloud. Using FileCloud's AMI, government agencies can host their own, secure file share sync and mobile access solution for their organization is less than 10 minutes. The FileCloud AMI image is built on top of Ubuntu 16.04 OS. FileCloud stores the metadata and file share information in MongoDB Database which is already configured in the FileCloud AMI. The actual files can be stored in EBS or S3. For scalability and redundancy, we recommend to use S3 for production. We also recommend that you take periodic snapshots of your running instance for disaster recovery.

For a 100 users organization, a t2.medium or m3.medium or m3.large instance is good enough. Using Amazon EBS for FileCloud stack (FileCloud application, Apache Web Server, MongoDB Database) and Amazon S3 for cloud storage provides a scalable, redundant infrastructure that will satisfy any stringent business and federal security requirements. Since you only pay for the FileCloud licenses (\$40/user/year) and Amazon infrastructure the cost savings are very significant compared to any other public cloud file sharing app like Dropbox or Box.net.

In a normal usage scenario, we expect FileCloud + AWS Infrastructure will cost \$60/user/year compared to \$240/user/ year for Dropbox or Box.net. In addition, with FileCloud you have complete control over the app, branding, domain naming and access permissions. Using FileCloud + AWS, one can approximately save over \$18,000 (assumption 100 users) when compared to Dropbox for business or Box.net.

Steps to Launch FileCloud AMI on GovCloud

1. Login to your aws govcloud admin console using your account, username and password

webservices™	
Account:	youraccount
User Name:	accountname
Password:	
	I have an MFA Token (more info)
	Sign In
	English -
Terms o	r <u>f Use Privacy Policy</u> © 1996-2015, Amazon Web Services, Inc. or its affiliates.

2. Click EC2 (Virtual Servers in the Cloud)

🎁 Services 🕶 Edit 👻		
Amazon Web Services		
Compute & Networking	Database	Analytics
Virtual Servers in the Cloud	DynamoDB Predictable and Scalable NoSQL Data Store	EMR Managed Hadoop Framework
Isolated Cloud Resources	RDS MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora	Application Services
Storage & Content Delivery	ElastiCache In-Memory Cache	NS SNS Push Notification Service
S3 Scalable Storage in the Cloud	Redshift Managed Petabyte-Scale Data Warehouse Service	es SQS Message Queue Service
Glacier Archive Storage in the Cloud	Deployment & Management	Workflow Service for Coordinating Application Components
	CloudFormation Templated AWS Resource Creation	
	User Activity and Change Tracking	
	CloudWatch Resource and Application Monitoring	
	Identity & Access Management Access Control and Key Management	
	Trusted Advisor AWS Cloud Optimization Expert	

3. Click Launch Instance



4. Search FileCloud AMI in AWS marketplace



and choose Continue

	File	eCloud							
	FileCloud	Pricing Details	~						
	FlieCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using	Bring Your Own License (BYOL)							
	AWS infrastructure (EC2, EBS, S3) one can jumpstart their own branded, file storage solution in	Hourly Fees							
	few minutes at a compelling price point. FileCloud	Instance Type	Software	EC2	Total				
Free tier eligible	client apps are available for all the desktop and	R3 Eight Extra Large	\$0.00	\$3.192	\$3.192/hr				
	iOS	M3 Extra Large	\$0.00	\$0.336	\$0.336/hr				
	More info	R4 16 Extra Large	\$0.00	\$5.107	\$5.107/hr				
	View Additional Details in AWS Marketplace	M4 Extra Large	\$0.00	\$0.252	\$0.252/hr				
Product Details		T2 Large	\$0.00	\$0.109	\$0.109/hr				
r roddor botano		C4 Double Extra Large	\$0.00	\$0.479	\$0.479/hr				
Sold by	CodeLathe	R3 Double Extra Large	\$0.00	\$0.798	\$0.798/hr				
Customer Rating	$\star \star \star \star \star \star (4)$	High Storage Eight Extra Large	\$0.00	\$5.52	\$5.52/hr				
Latest Version	17.3.0.37658	T2 Double Extra Large	\$0.00	\$0.435	\$0.435/hr				
Base Operating System	Linux/Unix, Ubuntu 16.04	T2 Extra Large	\$0.00	\$0.218	\$0.218/hr				
Delivery Method	64-bit Amazon Machine Image (AMI)	High I/O Extra Large	\$0.00	\$1.023	\$1.023/hr				
License Agreement	End User License Agreement	C4 Eight Extra Large	\$0.00	\$1.915	\$1.915/hr				
On Marketplace Since	9/1//14	M4 Quadrupie Extra Large	\$0.00	\$1.008	\$1.008/nr				
AWS Services Required	EC2, S3	12 Medium	\$0.00	\$0.054	\$0.054/nr				
Highlights		GPU Compute Extra Large	\$0.00 \$0.00	\$1.00 \$0.12	\$1.00/nr \$0.12/br				
 File Sharing -Allows busine 	esses to create their own, branded file sharing, sync	T2 Small	\$0.00	\$0.027	\$0.027/hr				
			+0.00						
					Cancel	Continue			

5. Choose the desired Amazon EC2 Instance type. We recommend at least t2.medium. However, m3 series (like m3.medium) would be better. t2 series begin to throttle resources after sustained usage.

FileCloud Server Version 23.232 Installation Guide

tep 2: C	Choose an Instance	e Type ECUs, 2 vCPUs, 2.5 GHz, Ir	itel Xeon Family, 4 GiB memo	ory, EBS only)			
	Family	- Туре -	vCPUs (j) -	Memory (GiB) -	Instance Storage (GB) (j) •	EBS-Optimized Available (i) 🔹	Network Performance (j)
)	Micro instances	t1.micro	1	0.613	EBS only	-	Very Low
	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate

6. Configure the instance details as per your requirement.

1. Choose AMI 2. Choose Instant	e Type 3. (Configure Instance	4. Add Storage	5. Tag Instance	6. Conf	igure Security Group	7. Review				
Step 3: Configure In: Configure the instance to suit your	stance E	Details s. You can launch r	nultiple instances	from the same AMI	reques	t Spot Instances to 1	take advantage	of the lower pricing	j, assign an acce	ss managemer	t role to the instance, and n
Number of insta	nces (j	1									
Net	work (j	vpc-d65943b4	(172.31.0.0/16) (default)	- C	Create new VPC					
Si	bnet (j	No preference	(default subnet in	n any Availability Zo	r 🕶	Create new subn	et				
Auto-assign Pub	lic IP 🕧	Use subnet se	tting (Enable)		•						
IAN	role (j	None			- C	Create new IAM r	ole				
Shutdown beh	avior (j	Stop			•						
Enable termination prote	ction (j	Protect agai	nst accidental terr	mination							
Monit	oring (j)	Enable Clou	dWatch detailed r ges apply.	nonitoring							
Ter	ancy (j	Shared tenand Additional char	y (multi-tenant ha ges will apply for (rdware) dedicated tenancy.	•						
Advanced Details											
									Cancel	Previous	Review and Launch

7. Select the desired storage. EBS storage is used to store the file meta and application data in the mongodb database. Depending on your implementation, actual files can be stored either in EBS or amazon S3.

🧊 Serv	ices 🗸 Edit 🗸								
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Tag Instance	6. Configure Securit	y Group	p 7. Review	1	
Step 4: Ac Your instance wi edit the settings storage options i	dd Storage II be launched with the follo of the root volume. You ca in Amazon EC2.	owing storage device se In also attach additional	ttings. You can att EBS volumes afte	ach additional EBS r launching an inst	volumes and insta ance, but not insta	ince st	tore volumes ore volumes.	to your instance, or Learn more about	
Volume Type	(i) Device (i)	Snapshot (j)	Size (GiB) (j)	Volume Type	(i)		IOPS (j)	Delete on Termination (i	Encrypted (i)
Root	/dev/sda1	snap-b01dfbf1	100	General Purpos	e SSD (GP2)	~	300 / 3000		Not Encrypted
Add New Volu	ime								

8. Configure Security Groups. If you need a external HTTP/HTTPS access you need to open port 80 and 443.

1. Choose AMI	2. Choose Instance Type	3. Configure Instance 4. Ad	d Storage 5. Tag Instance	6. Configure Security Group	7. Review	
Step 6: Co A security group instance, add rul	is a set of firewall rules that les that allow unrestricted a Assign a security grou	y Group t control the traffic for your ins ccess to the HTTP and HTTP: p: © Create a new security © Select an existing se	stance. On this page, you ca S ports. You can create a ne / group curity group	an add rules to allow specific f w security group or select fro	traffic to reach your instance. Foi m an existing one below. Learn	example, if you want to set up a web ser more about Amazon EC2 security groups
Security	y Group ID	Name		Description		
sg-e3d53	3786	default		default VPC securi	ty group	
sg-fcd53	799	FC_Default(ssh,http	,https)	launch-wizard-1 cre	eated 2015-04-19T13:25:02.400	-04:00
sg-5357t	ba36	launch-wizard-1		launch-wizard-1 cre	eated 2015-05-07T07:34:50.695	-04:00
	6		22200	000		
	for sg-icass/ss (selection	ea security groups: sg-rcaa		-	·- 0	
туре 🕕		Protocol		Pol	rt Range 🕕	source ()
SSH		TCP		22		0.0.0/0
HTTP		TCP		80		0.0.0.0/0
HTTPS		TCP		443	}	0.0.0.0/0
						Cano

9. Complete the review and launch instance

aws	Services 🗸	Edit 🗸								
1. Choose AMI	2. Choose Instance	Type 3. C	Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review			
Step 7: Re Please review ye	eview Instar our instance launch	ICE LAU details. You d	nch can go back to ed	it changes for each s	section. Click L	aunch to assign a key pair to	your instance and comple	te the launch proce	255.	
A Imp You You	prove your insta r instances may be a can also open addit	nces' secu accessible fro ional ports in	urity. Your sec om any IP address n your security gro	s. We recommend th bup to facilitate acces	Cloud-17-3- at you update ss to the applic	0-37658-AutogenByAV your security group rules to a cation or service you're runni	VSMP-, is open to the allow access from known IF ag, e.g., HTTP (80) for web	e world. Paddresses only. servers. Edit securi	ity groups	
 AMI Deta 	ails									
F	FileCloud [Copied ami-032f753 Root Device Type: ebs	3e43230c4e t	from us-east-2] File ype: hvm	2Cloud_17.3.0.37658_U	Jbuntu16.04					
	Hourly Software Fe Software charges v By launching this pr End User License A	ees: \$0.00 pe /ill begin onc roduct, you w .greement	er hour on t2.medi e you launch this vill be subscribed	ium instance (Additic AMI and continue ur to this software and	onal taxes may itil you termina agree that you	apply.) ite the instance. r use of this software is subj	ect to the pricing terms and	d the seller's		
 Instance 	Туре									
Instance	e Type E	CUs	vCPUs	Memory (GiB)	Instan	ce Storage (GB)	EBS-Optimized Availa	ble	Network Performance	
t2.mediu	m Va	ariable	2	4	EBS or	ıly	-		Low to Moderate	
 Security 	Groups									
Security g Descriptio	roup name n	FileCloud- This secur	17-3-0-37658-Aut ity group was ger	ogenByAWSMP- nerated by AWS Mark	etplace and is	based on recommended set	tings for FileCloud version	17.3.0.37658 provid	ded by CodeLathe	
Type ())		Protocol (i)		Port Rang	ge ()	Source (i)		Description (j)	
SSH			ТСР		22		0.0.0.0/0			_
HTTP			ТСР		80		0.0.0.0/0			
Custom	TCP Rule		TCP		443		0.0.0/0			
Instance	Details									
 Storage 										
▶ Tads										

10. You can see now your FileCloud is running in your AWS dashboard. Please note the Public DNS name to access your FileCloud.

FileCloud Server Version 23.232 Installation Guide

🎁 Services 🗸	Edit 🗸	
EC2 Dashboard	Launch Instance Connect Actions *	
Tags	Q Filter by tags and attributes or search by keyword	
Limits	Name Instance ID Instance Type Availability Zone Instance State Status Checks Instance State Instance ID Instance ID	4
	i-c5f758e0 t2.micro us-gov-west-1b 🥥 terminated	1
Reserved Instances	i-33f95616 t2.micro us-gov-west-1b 🥥 terminated	1
	i-1bfa553e t2.micro us-gov-west-1b 🥥 terminated	N
IMAGES AMIs	i-20918b02 t2.medium us-gov-west-1a 🥥 running 🔮 2/2 checks	1
Bundle Tasks ELASTIC BLOCK STORE Snapshots NETWORK & SECURITY		
Security Groups	۲. (III)	_
Elastic IPs Placement Groups	Instance: i-20918b02 Public DNS: ec2-96-127-69-148.us-gov-west-1.compute.amazonaws.com	
Load Balancers	Description Status Checks Monitoring Tags	
Network Interfaces	Instance ID i-20918b02 Instance state running	
AUTO SCALING	Instance type t2.medium	

11. Type 'http://<public_dns_name>/ui/admin/index.html' in your browser to access the FileCloud admin portal.

Default Admin	admin
Default Password	Your amazon instance ID
Note	Please change the admin password upon first login.

ec2-52-61-48-102.us-gov-west-1.compute.amazonaws.com/ui/admin/index.html		
	FILECLOUD	
	Admin Portal	
	Name Enter admin name	
	Password	
	Enter admin password	
	Sign in	
	Use Single Sign On (SSO)	
	Powered by FileCloud	

12. Once you logged into the admin portal, please install the FileCloud License.

Please register at our license management portal (https://portal.getfilecloud.com/ui/user/index.html? mode=register) to get trial licenses.

	Í	Admin Attentio	on Required		×	
		Action Item	Description		i i i	
		Invalid License File	Upload your license via Install License		1 W	Veek 1 Month 6 Months 2 Refresh Client Requests Served
		Invalid Server URL	Go to Settings, Server to set a valid Server	URL		
		Install Folder	Remove 'install' folder after installation. Example Windows: c:\xampp\htdocs\instal or /var/www/install	l Linux: /var/www/html/install		
		Set Admin	Go to Settings, Email to set a valid Email R	eply-to Address		
Sat	Sup		Mon Lue	S Clos	se	
6 % TEMP DISK USAG	E	52 KB Used 85 GB Remaining	0 % LICENSE USAGE	0 Used 12	% SETUP CHECKLIST	2 Completed 17 Total
			🖋 Manage	Version Information		
	Not Installed			Current Version		
				Latest Version		
				Update(s) Available		
			×	File Type Distribution	n	

- 1. The user name for the underlying Ubuntu OS is 'ubuntu'. Before launching the instance you will be required to create a key pair or you can use your existing key pair.
- 2. If you go to 'http://<public_dns_name>/install', the page will show all the installed packages in this instance. Check the page and familiarize yourself with FileCloud components. Before going production move the install folder (/var/www/html/install) to somewhere else.
- 3. We recommend you to use S3 for file storage instead of the EBS. Please check this page (Setting up FileCloud Managed S3 Storage) to know how to setup S3 for FileCloud file storage.
- 4. Take Periodic snapshots of your running instance for Disaster recovery and as an additional backup for FileCloud database and app.

FAQ

What is AWS GovCloud (US?

AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS

GovCloud (US) framework adheres to U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMPSM) requirements.

What is the Federal Risk and Authorization Management Program (FedRAMP)?

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. For more info check FedRAMP website (http://www.fedramp.gov/).

What is ITAR Regulations?

International Traffic in Arms Regulations (ITAR) The regulations control the export and import of defense-related articles and services on the United States Munitions List (USML).

More Information:

FileCloud Blogs	
Choose the Right File Sharing Solution for ITAR Compliance	

FileCloud Online GovCloud Verification Guide

FileCloud is the leading self-hosted, file sharing, sync, and mobile access solution for government agencies and public sector organizations. With the addition of FileCloud on Amazon Web Services (AWS) GovCloud, government organizations can now deploy a secure file sharing and sync solution that can meet the most stringent data security requirements used by the government.

How to obtain your IP and Hosting

In order to verify that your FileCloud Online is hosted in GovCloud, you can execute the following steps:

1) In your windows or Linux computer, open the command prompt. **Windows**: Windows logo/Search Icon> type CMD> hit Enter.



Linux: Press. Ctrl + Alt + T.This will launch the Terminal.

@u	buntu: ~		
 @ubuntu:~\$			

2) Modify the following command accordingly and copy and paste it in the terminal/command prompt and hit enter.
 Once the IP appears (example [52.11.222.333]), cancel the command by using Ctrl + C at the same time.
 Windows: ping GOVCHECK.filecloudonline.com
 Linux: ping GOVCHECK.filecloudonline.com


NOTE: Change GOVCHECK to your FileCloud's URL name or team name before running the command.

3) Once you have obtained the IP address of your FileCloud you can do a traceroute to verify where your FileCloud is being hosted. This takes about 20 seconds. Once the initial address appears, press **Ctrl + C** at the same time to cancel. **Windows**: tracert 52.11.222.333

Linux: traceroute 52.11.222.333



NOTE: Before running the command, change the IP address on the example provided with the IP obtained from step 2.

Interpreting the Result



FileCloud Docker installation

Docker images are mainly created for trialing/testing the product and are not optimized for production servers.

Installing Docker

1. Install **docker-compose** in your Docker server:

```
apt-get install docker-compose
```

2. Download **docker-compose.yml** using the below command:

wget https://patch.codelathe.com/tonidocloud/live/scripts/fc/docker-compose.yml

3. Pull the four FileCloud images:

docker-compose pull

4. Start the containers:

```
docker-compose up -d filecloud.server filecloud.mongodb filecloud.preview
filecloud.solr
(Do not change these names.)
If you do not want to start the optional containers filecloud.solr and
filelcoud.preview, remove filecloud.solr and filecloud.preview from the command.
```

Now you can access the FileCloud admin portal at http://<hostip>/ui/admin/index.html. The user name is admin and the password is password. You can access the FileCloud user portal at http://<hostip>/ui/core/ index.html.

Setting up LibreOffice preview

Filecloud has two preview methods:

- Built-in web preview
- LibreOffice preview

To use LibreOffice

- 1. Start the filecloud.preview container.
- 2. In the Admin portal, go to Settings > Misc > Preview.
 - a. In Office Location, enter /usr/lib/libreoffice/program
 - b. Check Enable Document Converter.



Confguring Solr

- 1. To configure Solr, start the filecloud.solr container.
- 2. Enter the Solr container shell:

```
docker exec -it filecloud.solr bash
```

3. Copy the skeleton:

```
cp -R /var/www/html/thirdparty/overrides/solarium/Solarium/fcskel/* /var/solr/
data/fccore/
```

- 4. Go to Admin portal > Settings > Content search.
 - a. Click Configure.
 - b. To start indexing, click the green Index button.

(i) By default, FileCloud uses host mount volumes for the Database and Filecloud storage folder.

Upgrading the Docker Image from Version 22.x or older to Version 23.x

FileCloud versions 23.x require MongoDB version 6. To upgrade to MongoDB version 6, you must upgrade the Docker image to 23.x.

A Before upgrade, make a backup or take a snapshot of your server.

To upgrade the Docker image:

1. To create a dump of the database, enter the following into the command line:

docker exec -i filecloud.mongodb /usr/bin/mongodump

2. Copy the dump folder from the container to the host machine. Note: Do not delete the dump folder. You are required to use it in step 7 to restore the database.

docker cp filecloud.mongodb:/dump .

To make sure the dump folder has been copied successfully to the host machine, enter:

```
ls –l dump
```

3. List the volumes:

```
root@docker:/# docker volume ls
```

DRIVER VOLUME NAME local nsadm_cloud_data local nsadm_mongo_database local nsadm_solr_data local nsadm_var_html

4. Delete the database volume and the Filecloud server volume where the application code files are stored, as shown in the following commands.

Please be careful to delete these volumes only.

root@docker:/home/nsadm# docker volume rm nsadm_mongo_database root@docker:/home/nsadm# docker volume rm nsadm_var_html

5. Edit your **docker-compose.yml** file, and change the version of MongoDB to **mongo:6.0.8** and FileCloud server to **filecloud/filecloudserver23.1:latest** as shown below:

```
version: '3'
services:
    filecloud.mongodb:
        container_name: 'filecloud.mongodb'
        image: mongo:6.0.8
        environment:
            - mongodb_data_container=/data/db
        volumes:
            - mongo_database:/data/db
  filecloud.server:
          container_name: 'filecloud.server'
          image: filecloud/filecloudserver23.1:latest
          depends_on:
              - filecloud.mongodb
              - filecloud.preview
          volumes:
              - cloud_data:/var/clouddata
              - var_html:/var/www/html
          links:
              - filecloud.mongodb
          ports:
              - "80:80"
              - "443:443"
```

6. Start Docker using the new docker-compose.yml file

docker-compose up -d

7. Copy the dump folder created in step 2 to the **filecloud.mongodb** container, and restore the database.

```
docker cp dump filecloud.mongodb:/
docker exec -i filecloud.mongodb /usr/bin/mongorestore --noIndexRestore --drop
```

8. Confirm that the containers are running.

```
root@docker:/home/nsadm# docker ps -a
CONTAINER ID
              IMAGE
                                                      COMMAND
CREATED
                STATUS
                                  PORTS
                          NAMES
31a8167e2731
              filecloud/filecloudserver23.1:latest
                                                      "bash /usr/local/bin..."
                                                                               3
                                0.0.0.0:80->80/tcp, :::80->80/tcp, 0.0.0:443->4
minutes ago
              Up 23 seconds
43/tcp, :::443->443/tcp
                          filecloud.server
5bdb04b9f5fb
              mongo:6.0.8
                                                      "docker-entrypoint.s.."
                                                                               3
minutes ago
              Up 34 seconds
                                27017/tcp
                           filecloud.mongodb
              filecloud/filecloudsolr21.3:latest
b1466b6088ab
                                                      "sh /opt/solr/docker..."
                                                                               3
minutes ago
              Up 23 seconds
                                8983/tcp
                           filecloud.solr
304de38d3fa0
              filecloud/filecloudpreview22.1:latest
                                                      "/opt/libreoffice/in..."
                                                                               3
              Up 24 seconds
minutes ago
                           filecloud.preview
```

9. Set the compatibility version for MongoDB to 6.0.

```
root@docker:/home/nsadm# docker exec -it filecloud.mongodb bash -c 'mongosh --eval
"db.adminCommand( { setFeatureCompatibilityVersion: \"6.0\" } )"'
Current Mongosh Log ID: 64b8b48af3fc5d6bfffc1149
Connecting to:
                        mongodb://127.0.0.1:27017/?
directConnection=true&serverSelectionTimeoutMS=2000&appName=mongosh+1.10.1
Using MongoDB:
                       6.0.8
Using Mongosh:
                        1.10.1
For mongosh info see: https://docs.mongodb.com/mongodb-shell/
To help improve our products, anonymous usage data is collected and sent to
MongoDB periodically (https://www.mongodb.com/legal/privacy-policy).
You can opt-out by running the disableTelemetry() command.
_____
  The server generated these startup warnings when booting
   2023-07-20T04:12:49.344+00:00: Using the XFS filesystem is strongly recommended
with the WiredTiger storage engine. See http://dochub.mongodb.org/core/prodnotes-
filesystem
   2023-07-20T04:12:49.774+00:00: Access control is not enabled for the database.
Read and write access to data and configuration is unrestricted
   2023-07-20T04:12:49.774+00:00: vm.max_map_count is too low
_____
{ ok: 1 }
```

10. Confirm that everything is working as expected in the FileCloud user portal and admin portal.

Oracle Cloud Installation

FileCloud is available from the Oracle Cloud Marketplace for installation on the Oracle Cloud Infrastructure.

To install FileCloud on the Oracle Cloud Infrastructure (OCI):

Choose the FileCloud application in Oracle Cloud Marketplace.

- Log in to your Oracle account at: https://www.oracle.com/cloud/sign-in.html or, if you do not yet have an Oracle account, create one at: https://signup.cloud.oracle.com/?sourceType=_ref_coc-asset-opcSignIn&language=en_US
- 2. <u>Click the navigation icon in the upper-left corner:</u>



3. In the drop-down menu, enter Marketplace in the search bar and choose All Applications.

Image: Compute Storage Networking Oracle Database Storage Work Request	X ORACLE Cloud	Search resources, services, documentation, and Marketplace
Databases	Q marketplace X Home Compute Storage Networking Oracle Database Databases Analytics & Al Analytics & Al	Search results for "marketplace" ✓ Instances Custom Images ✓ All Applications ✓ Community Applications ✓ Accepted Agreements ✓ Work Request ✓

Oracle Cloud Marketplace opens to a view that shows all applications.

4. In the search bar, enter **FileCloud**.



5. Click the FileCloud app box.

The box opens up a new window as seen in the below screenshot.

- 6. In **Version**, choose a version. The latest version is labelled **default**.
- 7. In Compartment, choose filecloud (root).
- 8. Check the box to accept the Oracle terms of use and the Partner terms and conditions.

	E Cloud filecloud		✓ ☑ ♣ ② ⊕ ♀
ORACL	Ce Cloud Filectoud	Type Image Version 23.1 (7/5/2023) - default ≎ Compartment filecloud (root) ≎ I have reviewed and accept the <u>Ora</u>	Image: Arrow of the partner terms of use and the Partner terms
		Launch In: Reminder: Patch the in	stance C

9. Click Launch Instance. The page Create compute instance opens.

Configure the details of the instance

In the **Create compute instance page**, enter the details of the instance.

1. In **Name**, enter an instance name or use the default name.

Create compute instance			
Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating	an instance with Resource Manager.		
Name			
instance-20231107-2259			
Create in compartment			
filecloud (root)		0	
Placement	Collapse	2	
The availability domain helps determine which shapes are available.		Summary () Compute instance	
	AD 3	Shape \$36.	.46/mor
gBjX:US-ASHBURN-AD-1 ✓ gBjX:US-ASHBURN-AD-2	gBJX:US-ASHBURN-AD-3	Boot volume \$2.	.00/mc
Show advanced options		Estimated total \$38.	.46/md

2. Scroll down to the **Add SSH keys** box, and generate and save the SSH private key. It is recommended that you select **Generate a key pair for me**, and then click **Save private key**.

Create compute instance	
Add SSH keys Generate an <u>SSH key pair</u> to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have. Generate a key pair for me Upload public key files (.pub) Paste public keys No SSH keys	
Download the private key so that you can connect to the instance using SSH. It will not be shown again. Save private key	

- 3. Scroll down to the **Boot volume** box.
- 4. By default, the boot volume size is 46.6 GB. You may check **Specify a custom boot volume size** and enter a custom size.
- 5. For better performance, increase **VPU** (volume performance units) to 30 or higher.

6. For greater security, check **Use in-transit encryption**.

boot volume is a detachable device that contains the image used to boot the compute instance.	
Specify a custom boot volume size <u>Volume performance</u> varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.	
Boot volume size (GB)	
Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.	
Boot volume performance	Target volume performance (i)
VPU () UHP	IOPS: 5400 IOPS
30 ÷ 10 120	Throughput: 43.2 MB/s
Ultra-high performance, recommended for the most demanding, I/O intensive workloads. Learn more Actual performance depends on the attached instance's shape. Select the appropriate instance shape to optimize performance. Learn more	
Use in-transit encryption	
Encrypts data in transit between the instance, the boot volume, and the block volumes.	
Encrypt this volume with a key that you manage	
By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control encryption keys?	over the key's lifecycle and how it's used. <u>How do I manage my own</u>

7. Click Create.

A page with the instance details opens.

8. When the status **RUNNING** appears, click **Start**.

ORACLE Cloud	fiedoud	×
Compute + Instances + Instance deta	its = Work requests	
	instance-20231107-2259	
	Start Stop Reboot Terminate More actions -	
	Instance information Shielded Instance Oracle Cloud Agent	Notifications Tags
	General information	Instance acce
RUNNING	Availability domain: AD-1 Fault domain: FD-2	You connect to a runnio the private key from the

Connect to the instance

- 1. If you do not have a FileCloud License, register for one at portal.filecloud.com.
- 2. In a web browser, enter the FileCloud admin portal URL: http://<public_dns_name>/ui/admin/index.html

- 3. In the login page, enter the username and password **admin/password**. You must change the username and password after your first login. The **Admin Attention** window opens.
- 4. Install the FileCloud license through this window.

Admin Attention Required ×				
	Example path on Windows: c:\clouddata Example path on Linux: /opt/cloud/data Check Path Apply	^		
Invalid License File	Upload your license via Install License Install License Browse Choose License file (Only .xml) Apply	×		
		S Close		

Perform post-installation tasks

After you have connected to your instance, perform post-installation tasks:

- 1. Delete the installation folder.
- 2. For better security, change the default SMTP servers and accounts used to send emails to your own servers. See Email Settings.
- 3. In Settings > Email, and set a valid Email Reply To Address.
- 4. View and familiarize yourself with the FileCloud components by navigating to http://<public_dns_name>/install in a web browser.
- 5. To set up FileCloud, follow the instructions at FileCloud Site Setup.
- 6. Take periodic snapshots of your running instance for disaster recovery and as additional backup for the FileCloud database and app.

Post Installation

After the FileCloud installation is completed, the following steps will help you prepare FileCloud for use:

- 1. Verify Your Installation.
- 2. Install the FileCloud License.
- 3. Configure the Managed Storage Path.
- 4. Enable MongoDB Bind IP and Authentication.
- 5. Configure SSL if desired.
- 6. Change the account used to run Apache, FileCloud Cron Service, FileCloud Docconverter, FileCloud helper and FileCloud Message Queue Service to an account that is not Local System.

To change accounts from Local System

- a. Open Windows Services.
- b. Right-click Apache2.4, and choose Properties.



- c. In the **Properties** dialog box, click the **Log On** tab.
- d. Select This account.
- e. Enter a Windows account to use for running the service.

f. Enter and confirm the password.

Apache2	.4 Proper	ties (Local	Computer)			×
General	Log On	Recovery	Dependencies			
Log on	as:					
O Loc	al System	account	t with deckton			
			. with desktop			
Inis	account:				Browse	
Pas	sword:	••	•••••			
Con	nfirm passv	vord:	•••••			
			OK	Cancel	Apply	

- g. Click Apply.
- h. Restart the service
- i. Repeat this procedure for each of the services (Apache24, FileCloud Cron Service, FileCloud Docconverter, FileCloud Helper, and fcorchestrator (for FileCloud Message Queue)).
- 7. Delete your installation folder.

To delete your installation folder

Delete the Installation Folder

Once you have verified your installation and can log in to the Admin portal, it is recommended that you delete in the installation directory.

This step provides increased security. If someone can guess the location of your installation folder and access it they could potentially overwrite your site by running the installer again.

The installation folder exists in the following location by default:

OS	Location
Windows	C:\xampp\htdocs\install
Linux	/var/www/html/install
	or
	/var/www/install

To delete the installation folder:

- a. On the FileCloud server, locate the installation folder for your operating system.
- b. On Windows, to delete the folder, right-click its name or icon, and then choose Delete from the pop-up menu.
- c. On Linux, to remove all files and directories within that directory, with no prompt for deleting each file, use the following command:
- rm -rf install
- Failing to delete your FileCloud install folder after you verify installation may cause your system to leak sensitive data.

FAQs

To configure storage, SSL, and other post-installation settings, I need the File Cloud Control panel. How do I open it?

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

Open the File Cloud Control panel

There are several ways to open the FileCloud Control Panel:

Using the Windows Start Menu

1. On the server, from the Windows Start menu, select the FileCloud Control Panel.

Finding the FileCloud control panel executable file (cloudcp.exe)

- 1. On the server, find the *xampp* folder.
- 2. Inside the folder, double-click the cloudcp.exe file.

Verify Your Installation

FileCloud is bundled with a verification tool to help you test your installation. You can run this tool from the server where FileCloud is installed or remotely from a different system. This tool will perform various configuration checks related to your FileCloud environment.

FileCloud Server Version 23.232 Installation Guide



Verification checks are grouped into two categories: basic and extended. It is strongly recommended that you review the basic checks to ensure that the required components are available to FileCloud. Once the Basic checks pass, Extended checks should be reviewed to verify that required directories and configurations are available.

Basic Checks	Extended Checks
Apache Web Server	CloudConfig.php readable
Apache Mod Rewrite	Localstorageconfig.php readable
.htaccess Present	Scratch Directory Writable
PHP 7.4	Config Directory Readable
PHP MongoDB (mongodb ext) driver 1.2.3 or higher	Mod Rewrite Apache Configuration Setup Check
PHP GD Library	PHP Memcache Server (Optional)
PHP Zip library	Verification of Mongo DB connection

PHP Curl Library	
PHP OpenSSL library	
PHP ionCube extension 4.4.1 or higher	
PHP bcmath extension	
PHP SimpleXML extension	
PHP mbstring extension	
PHP LDAP library (optional)	
PHP Memcache Extension (optional)	
Install in Server WWW root folder	
CloudConfig.php Readable	



This tool will also report problems so you can correct them before using FileCloud.

All failures reported by the verification tool must be fixed before attempting to use FileCloud.

Reviewing the Verification Checks

To verify your FileCloud installation:

1. From the FileCloud server, or the VM instance, open a web browser and enter the following address:

http://<yourdomain>//install

A Notes

- By default, the address is: http://127.0.0.1/install
- To run verification tests from a system that does not have the FileCloud installation, replace 127.0.0.1 with the IP of the system where FileCloud is installed.
- 2. To review basic tests, select Basic Checks.

3. To review more thorough tests, select Extended Checks.

Basic Checks

Clicking on the Basic Checks tab displays:

- 1. The name of the item that was checked.
- 2. The result of the check. A blue checkmark \leq = PASS, and a red X \otimes = FAIL.
- 3. Additional information for installing, troubleshooting, or correcting an issue for this item.

(BASIC CHECKS 2 Checking FileCloud Requirements	
E Requirement	Status 🕜 Help	0
Apache Web Server	✓ Running	as : SYSTEM
Apache Mod Rewrite	Notes	
Apache Mod Deflate/Filter	Notes	3
.htaccess present	O	
PHP 7.4	Version:	7.4.16 PHP Info

You should review each item in the list to understand how your system is configured and functioning.

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

To review Basic Checks:

1. How to review basic checks

How to review basic checks

The following table explains how to use the Basic Checks information:

What You See		What It Means	
.htaccess present	0	For a blank entry with a blue checkmark, the item has passed the verification test and there is nothing further for you to do.	

What You See			What It Means
Apache Mod Rewrite	0	Notes 🖉	For a notes entry with a blue checkmark, the item has passed the verification test. Optional: To read more about the item, click on Notes (the Notes icon).
PHP Memcache Extension	0	version 3.0.9-dev Notes	For a version entry with a blue checkmark, the item has passed the verification test using the specific version. <i>Optional:</i> To read more about the item, click on Notes (the Notes icon).
PHP ionCube extension 10.1.0 or higher	<	Version: 10.2.0 Install ionCube Loader	For a version entry with a blue checkmark and links, the item has passed the verification test using the specific version and you must complete the items listed by clicking on the link. <i>REQUIRED:</i> To install this component, click the Install link.
PHP LDAP Library (optional, for AD/LDAP support)		Ignore failure if AD/LDAP is not needed Notes	 For an Ignore - IF entry with a blue checkmark, the item has passed the verification test conditionally. 1. Check the condition. In this example, determine whether you need AD/LDAP. 2. If the condition is true, then there is nothing further for you to do. In this example, you do NOT need AD/LDAP. 3. If the condition is false, then resolve the issue. In this example, if you DO need AD/LDAP, then you must go and install it. Optional: To read more about the item, click on Notes (the Notes icon).
PHP Memcache Server (optional)	8	Version:	 For any entry with a red X, you must correct the issue. For help resolving an issue, use the following resources: Read more about the item in the Review the Requirements page. Review the installation procedures. Review the Installation Troubleshooting page.

The Help column provides information and resources for understanding how your system is working.

In the Help column, if you click on

(the Notes icon), the FileCloud Help page opens.

(the Notes icon), the FileCloud Help page opens.

(Control of the Cloud Control of the Clo

2. Resolve Failed Checks

Resolve Failed Checks

To resolve an issue:

- 1. Return to the FileCloud control panel and install any missing required components or start any required services.
- 2. For help resolving an issue, use the following resources:
 - Notes
- Read more about the item in the
- Review the Requirements page.
- Review the installation procedures. Review the Installation Troubleshooting page.

heren ale installation frousteshooting page.

Here are details about some of the important extended checks performed.

This is the set of basic checks performed on your FileCloud installation environment.

Check	Details

Apache Web Server	Checks if your environment has a working Apache server installation.
Apache Mod Rewrite	Checks if mod rewrite module is enabled and activated.
Apache Mod Deflate/ Filter (optional)	Checks if the Apache mod_deflate module is present. This is optional.
.htaccess Present	Checks if the .htaccess is present in the root WWWROOT folder
PHP 7.4 or higher	Checks if the environment has PHP v7.4 or higher.
PHP MongoDB (mongodb ext) driver 1.6.0 or higher	Checks if PHP Mongo DB drivers are installed properly and are version 1.6.0 or higher.
PHP GD Library	Checks if GD library is installed properly.
PHP Zip library	Checks if Zip library is installed properly
PHP Curl Library	Checks if PHP Curl library is installed, this is required if you are using open stack, Amazon S3 or NTFS permissions or Multi-tenancy.
PHP OpenSSL library	Checks if OpenSSL library is installed properly.
PHP ionCube extension 10.4.0 or higher	<pre>FileCloud PHP files are protected by ioncube encoder. So ioncube decoder is essential for FileCloud to function. Click on the "Install ionCube Loader" link to get instructions on configuring ionCube loader on your environment. Choose "Local Server" when selecting your environment.</pre>

PHP bcmath extension	Checks if PHP bcmath extension is installed.
PHP SimpleXML extension	Checks if PHP SimpleXML extension is installed.
PHP mbstring extension	Checks if PHP mbstring extension is installed.
PHP LDAP library (optional)	Checks if PHP LDAP extension is installed. This is optional and only required if your environment will be using LDAP or Active Directory authentication.
PHP Memcache Extension (optional)	Checks if PHP Memcache extension is installed. This is optional and only required if you will be using encryption for Local Storage (Managed Storage)
Install in Server WWW root folder	Checks if FileCloud installation is in the main server root and not in the subfolder, ie. http://mydomain.com and not http://mydomain.com/cloud
CloudConfig.php Readable	Checks if cloudconfig.php exists and readable. cloudconfig.php file is present in WWWRoot/config folder

Extended Checks

Clicking on the Extended Checks tab displays:

EXTENDED CHEC	KS	
Checking FileCloud Requirements		
≡ Requirement	📀 Status	Help
CloudConfig.php Readable:C:\xampp\htdocs\config\cloudconfig.php 🔫 👥 🚺	0	
localstorageconfig.php Readable:C:\xampp\htdocs\config\localstorageconfig.php	2 → ⊘	
Scratch Directory Writable:C:\xampp\htdocs\scratch	0	& Notes
Config Directory Readable:C:\xampp\htdocs\config	0	& Notes
Mod Rewrite Apache Configuration Setup Check	0	
FileCloud Message Queue Service	0	
PHP Memcache Server (optional)	0	Version: 1.4.4-14-g9c660c0 Notes

- 1. The name of the item that was checked.
- 2. The result of the check. A blue checkmark \checkmark = PASS, and a red X \bigotimes = FAIL.
- 3. Additional information for installing, troubleshooting, or correcting an issue for this item.

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

To finish verifying your installation using Extended Checks, complete the following steps:

1. Resolve Failed Checks

Resolve Failed Checks

To resolve an issue:

- 1. Return to the FileCloud control panel and install any missing required components or start any required services.
- 2. For help resolving an issue, use the following resources:
- Read more about the item in the

- Review the Requirements page.
- Review the installation procedures.
- Review the Installation Troubleshooting page.

Here are details about some of the important extended checks performed.

Check	Details
CloudConfig.php readable	Checks if the cloudconfig.php file is present in the config folder
Localstorageconfig.php readable	Checks if the localstorageconfig.php file is present in the config folder
Scratch Directory Writable	Checks if WebServer process has write permissions to WEBROOT/scratch directory. In Linux, usually chown -R www-data:www-data WEBROOT/ scratch followed by chmod -R 700 WEBROOT/scratch would be sufficient.
Config Directory Readable	Checks if Apache web server process has read permissions to WEBROOT/config directory.
Mod Rewrite Apache Configuration Setup Check	Checks if Apache website configuration has mod rewrite rules allowed.
FileCloud Message Queue Service	Checks to see if Message Queue Service is up and running.
PHP Memcache Server (Optional)	Checks if Memcache server is running. This is currently optional.

2. Verify the Mongo Database Connection

Verify Mongo Database Connection

In step 2, if you see the following:

2 Verification of Mongo DB connection

MongoDB connection OK: MongoDB Version: 4.2.13

We recommend you use MongoDB 4.2.x and above with PHP MongoDB ext driver 1.6.0 and above for best stability and performance.

Then you can move on to step 3, and install any missing updates.

1 If your connection is not OK, then return to the FileCloud control panel to troubleshoot and resolve the issue.

3. Install Any Required Updates

Install Any Required Updates

In step 3, review the Status for the following required modules, and take any required Actions:

MODULE	ACTION
Build Version	After finishing the Post Installation steps, you can upgrade FileCloud from the Admin portal.
Database Schema	Click on the Update link to update your database to the latest schema version.
Config Files	To see the configuration entries that need to be added, in the Action column, click the link. Whenever you update to a new version, it is normal to have to add new entries.

FileCloud Update			
nodule	📀 Status	Notes	C Action
Build Version	ок	Installed Version 21.1.1.15106	
Database Schema	ок	Current Database Version is 67	
Config Files	ок	All required constants are defined	

4. Set Up Outside Access

Set Up Outside Access

In step 4, if you want to allow someone from outside your organization to access FileCloud, then you can configure your Web server ports for port forwarding. Port forwarding, or port mapping, is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. The process for this will vary depending on the operating system you are using.

To set up outside access:

- 1. To ensure port 80 is accessible from the outside, forward the ports from your Public WAN IP to the internal IP address of the FileCloud server.
- 2. Ensure port 80 is accessible through any organizational firewalls.
- 3. For additional security, it is recommended that you use only port 443 for secure access via HTTPS.
- 4. For additional security, purchase and install and SSL certificate for your domain.

For more information on port forwarding, see the following references:

- Windows Remote access and server management
- Ubuntu SSH/OpenSSH/PortForwarding
- Debian 8 Port forwarding with IP tables

5. Configure Any Missing Integrations

Configure Any Missing Integrations

In step 5, you should make sure you have the Cron task service configured so background tasks will be run. FileCloud uses a cron job to perform certain ongoing maintenance tasks, such as sending email notifications for file changes, share notification etc.

Other optional items can be configured at this time too.

For additional details, click More Info:

Other Integrations

- Background Jobs: IMPORTANT: Setup the cron task service to ensure background tasks get executed. More Info 🤤
- Document Web Preview Support. More Info 🤤
- Active Directory or LDAP Authentication support (Optional) More Info Info

6. Log In to the Admin Portal

Log In to the Admin Portal

In step 6, use the link provided to log in to the Admin portal.

When you log in to the Admin portal for the first time, you may see informational flags for configuration tasks and a Welcome wizard.

You do not have to complete these tasks in step 6, but before users can log in to the User portal, those tasks must be completed.

The first time you log in, the Admin Username is **admin**, Admin Password is **password**. It is recommended that you change this password using the FileCloud control panel. To reset the password for the Admin portal:

- 1. Open the FileCloud control panel.
- Under Miscellaneous, click Reset Admin Password.

To verify login ability:

- 1. To log in to the Admin portal, click the URL link for the Admin Portal.
- 2. Make sure your Dashboard loads.
- 3. If you can log in and see the dashboard, move on to step 7 to delete the installation directory.

7. Delete the Installation Folder

Delete the Installation Folder

Once you have verified your installation and can log in to the Admin portal, it is recommended that you delete in the installation directory.

This step provides increased security. If someone can guess the location of your installation folder and access it they could potentially overwrite your site by running the installer again.

The installation folder exists in the following location by default:

OS	Location
Windows	C:\xampp\htdocs\install
Linux	/var/www/html/install
	0
	/var/www/mstatt

To delete the installation folder:

- 1. On the FileCloud server, locate the installation folder for your operating system.
- 2. On Windows, to delete the folder, right-click its name or icon, and then choose Delete from the pop-up menu.
- 3. On Linux, to remove all files and directories within that directory, with no prompt for deleting each file, use the following command:

rm -rf install

Install the FileCloud License

Your FileCloud license provides legally binding guidelines on the use and distribution of your newly installed FileCloud software.

Obtaining a FileCloud License

Obtaining a FileCloud License

The length of access and site configuration will vary depending on your license type.

There are two basic forms of FileCloud licenses:

License Type	Duration	Features	Availability
Trial (free)	Temporary 30 days for a server license 15 days for an online license	 All features Mobile and desktop apps Free support Peployment URL will be set as "*" (accessible from any URL) 	Server (Self-host) Online (Hosted by us)
Production	Permanent based on length paid for Usually 1 year	 All features Mobile and desktop apps Choose from 3 levels of support Deployment URL can be set to use your specific domain (URL accessibility from within your company and outside access managed by Administrators) 	Server (Self-host) Essentials Advanced Service Provider Online (Hosted by us) Essentials Advanced GovCloud

For more information, read the license descriptions and Key Features on the FileCloud Pricing page.

To purchase a license, see License Purchase and Renewal

For a trial license, go to https://www.filecloud.com/#hostedTrial and follow the instructions in the wizard.

When you register on the FileCloud web site to access the installation software, you should receive your trial license, although it still needs to be installed.

- If you already downloaded your license, proceed to the steps for installing it.
- If you did not download your license yet, use the next procedure to download it, and then proceed to the steps for installing your license.

Downloading your license

Downloading your License

To downloading your license:

1. Navigate to https://portal.getfilecloud.com/ui/user/index.html

2. Type in the registered email and the password provided to access the license portal. The license portal opens to the dashboard, where it lists all of your licenses.

Downloads	Want to try FileCloud? Start a new tr	rial		
SPLA Reports	+ New license Click here to buy a new license	FILECLOUD (pending) www \$ 5 seats The license is being issued	FILECLOUD citest1.filecloudonline.com 20 seats The license is expired	View all
	Useful Resources			
	Get started	Learn More	Downloads	
	Need guidance? Schedule a free demo	Case Studies Data Sheet / FAQ <u>Documentation</u> Release Notes Suggest an idea Developers	Server Sync Drive Secure Document Viewer Mobile Apps Other Downloads	
	Schedule a free demo	Case Studies Data Sheet / FAQ <u>Documentation</u> Release Notes Suggest an idea Developers	Server Sync Drive Secure Document Viewer Mobile Apps Other Downloads	< >

If you don't see the license you want to download listed, click View all to see all of your licenses. (You can also expand Sites in the navigation pane to access links to all of your licenses).
 Click the license that you want to download.

Sites - Downloads	Want to try FileCloud? Start a new tria	al \Upsilon S	T Show all V T Sort by V (Search for sites, Q)				
SPLA Reports Billing	+ New license	FILECLOUD (pending)	FILECLOUD	FILECLOUD Server Trial			
	Click here to buy a new license	 5 seats The license is being issued 	 20 seats The license is expired 	 20 seats The license is expired 			
	FILECLOUD	FILECLOUD	FILECLOUD	FILECLOUD			
	 ✤ 500 seats ➢ Expires in 173 days 	 a 20 seats > Image: Seate of the seate of t	 20 seats The license is expired 	 100 seats The license is expired 			
	FILECLOUD SPLA	FILECLOUD					
	 ✤ 10 seats ➤ The license is expired 	 200 seats Expires in 108 days 					
		View	less				
Need help?	Useful Resources						

5. The license is stored on your server as license.xml.

Installing Your License

(i) The ability to install license components such as SALESFORCE is available in FileCloud Server version 18.2 and later.

 \times

Close

Installing Your License

You can operate FileCloud Server using any of the license types.

- If you do not need to use individual additional components, such as SALESFORCE, and Pattern Search, you can use an Essentials license.
- However, if you need to use individual additional components, such as SALESFORCE, and Pattern Search, then you must use an Advanced or Service Provider license.

There are multiple places where you can install your FileCloud license:

- Admin alert dialog box
- The dashboard's License Information widget
- The admin portal's **Settings > License** tab

It doesn't matter which one of these places you use; they all perform the same task.

After installation, to update or manage licenses, use the dashboard's License Information widget or the admin portal's Settings > License tab.

Admin Alert Dialog

During initial setup, when you log in to the admin portal, you see the **Admin Attention Required** dialog box, which allows you to upload your **license.xml** file and apply the license.

Admin Attention Required

	Example path on Windows: c:\clouddata Example path on Linux: /opt/cloud/data	^
	Check Path Apply	
Invalid License File	Upload your license via Install License Install License Browse	
	Choose License file (Only .xml)	
	Apply	
		~

To install your license from the Admin dialog:

- 1. In the Invalid License File row, click Install License.
- 2. In the new section that appears, click **Browse**.
- 3. Locate the license.xml file, and then click **Apply**.
- 4. The installed license appears in green under the textbox.

Dashboard

If you close the Admin dialog without installing a license, you can always use the FileCloud dashboard to manage your licenses. You can also use it to update a license.

P The dashboard opens the same window that opens when you click **Settings > License**.

To install your license from the Dashboard:

- 1. Log in to the Admin Portal.
- 2. In the dashboard's the License Information widget, click Manage.

	(* Add Hetwork Shares	🗕 Add Admin 🔶 Al	erts		*** M0
System Summary			ΰX	🔟 Statistics	Û X
1 Week 1 Month 6 Months			C ⁴ Refresh		🖾 Email 🛛 📿 Refresh
Hover over the graph for details				💄 Full Users	18
300				Guest Users	1
250				External Users	2
200				Croups	5
150				Live Files	1,963
100				Other Files	151
50				Network Folders	1
0		/L//L_/L		User Shares	23
THU FRI SAT	SUN N	MON TUE	WED THU	Devices	6
Quota Usage	461.47 GB	sk Usage	License Usage	Audit Records	132,815
Unlimited N/A Unlimited quota	228.03 GB 461.47 GB 229.03 GE	B used B free	20 19 used 20 total	Emails Sent in the last 24h	12
Governance	ÔX @	Realtime DLP Statistics	۲ X	License Information	Ó X
Compliance	2/3	Active Downloads	0		Manage
DLP Rules	10	Active Uploads	o	Licenses	19 Used / 20 Total
Retention	0	Active Shares	o	License Every	31-Aug-2023
Content Classification	0	Active Users	2	Litense Expiry	(272 days left)
		Vielations	0	License Owner	CodeLathe

```
💡 The dashboard opens the same window that opens when you click Settings > License.
```

Server	Storage	Authentication	Admin	Database	Email	Endpoint Backup	License	Policies
License								
License C	wner							
CodeLati	he							
Expiry Da	te							
31-Aug-3	2023 (272 day	ys left)						
Usage Inf	formation							
19 Used	/ 20 Total							
Compone	ents	/						
BASE, EN	ITERPRISE							
Update Li	icense 🍐							
Choose	File No file	e chosen						
Choose L	icense file to	Update (Only .xml)						

- 3. On the License page, click the Choose File button.
- 4. Select the license.xml file and click **OK**.
- 5. On the License page, click Save.

Also see:

- Installing FileCloud License On Multiple Sites
- Viewing Your License Details

Installing FileCloud License On Multiple Sites

If you are an administrator of a multi-site installation and need to update the site license of all your sites, you can use the steps described below:

Installing a License on Specific Sites

To install a license on a subset of your sites:

1. Create a file named license.txt that lists the sites that you want to update in the format:

```
site1.test.com
site2.test.com
```

- 2. Install the **license.txt** file into your backup folder: Linux: **/var/www/html/resources/backup** Windows: **c:\xampp\htdocs\resources\backup**
- 3. Copy the **license.xml** to the **/resources/backup** folder. Do not change its name.

4. In a command line enter:

For Windows:

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

For Linux:

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

5. Then, for both Windows and Linux, enter:

php licenseinstaller.php license.xml

The license is only applied to the sites listed in **license.txt**. Note: If **license.txt** is blank, the license is applied to all sites.

Viewing Your License Details

(i) License components information is available in FileCloud version 18.2 and later. It identifies the areas of FileCloud Server that you have purchased access to.

For information on the different license types, read about the key features on the Pricing page.

The details of your license are displayed in the following places:

- The Admin portal dashboard Use this to see quick details about your license, such as when it expires.
- The License tab in the Settings screen Use this to update your license or to see the license components that are available.

From the Dashboard

To review your license details:

1. Log in to the admin portal.

2. On the dashboard, a widget for License Information appears.

🛚 Add Users 🛛 😤 Add Group	ntwork Shares Add Network Shares	🚢 Add Admin	Alerts		••• More
System Summary			ΰX	Jai Statistics	ΰX
1 Week 1 Month 6 Months			C ^e Refresh		🖾 Email 🛛 C ^a Refresh
Hover over the graph for details				Full Users	18
250				External Users	2
150			,	Live Files	1,963
50				Other Files Network Folders	151
0. THU FRI SAT	SUN N	ION TUE		User Shares	23
N/A Quota Usage N/A Unimited	461.47 GB 228.02 GB 461.47 GB 228.02 GB	sk Usage used	19 20 19 used 20 total	Audit Records Emails Sent in the last 24h	132,815
	A 14	Dealking DI D Chatig	ر بر بر بر بر	⇒ Linnan Information	-
Compliance	2/3	Active Downloads		of License information	© Manage
DLP Rules	10	Active Uploads	0	Licenses	19 Used / 20 Total
Retention	0 /	Active Shares	0	License Expiry	31-Aug-2023
Content Classification	0 /	Active Users /iolations	2 0	License Owner	CodeLathe

3. In the upper-right corner, click **Manage** to go to the License tab in **Settings**, shown below.

In the Settings screen

To update your license details:

- 1. Log in to the admin portal.
- 2. From the left navigation panel, click **Settings**.



3. On the Manage Settings screen, click the License tab.

- 4. Review the license information.
- 5. In **Components**, make sure the features you need are listed.
- 6. To install a new license, click **Choose File**.

Configure the Managed Storage Path

FileCloud Server is sometimes called on-premises. This is because you are using the storage space you have locally in your infrastructure to store the files managed by FileCloud Server.

- Managed Disk Storage is just a path to the location where the user files are stored locally and can be accessed directly by FileCloud Server
- When you specify the path to managed storage, you allow FileCloud complete control over the management of user content
- Managed storage can be a path to file systems, a local hard disk, and Storage Area Network (SAN) or Network Area Storage (NAS) disks

When setting up FileCloud, a critical setting is the path where FileCloud stores its files.

Setting up Managed Storage Path for Local Storage is only needed if you are using FileCloud Local Storage. If you are using Amazon S3, you don't need to set this path.

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

To configure the storage path:

1. Use the Admin Attention Required dialog for the initial setup.

Initial Setup

Initial Setup

On initial login into the Admin Portal, if the storage path is not set or not writable, an "Admin Attention Required" dialog is shown as below.
Admin Attention Required ×				
Action Item	Description	^		
Storage Path Not Set	Storage Path			
	Specify the Location to Store Cloud Files, this must be writable by Webserver. Example path on Windows: c:\clouddata Example path on Linux: /opt/cloud/data Check Path Apply	1		
Invalid License File	Upload your license via Install License Install License	ł		
Install Folder	Remove 'install' folder after installation Example Windows: c:\xampp\htdocs\install or Linux: /var/www/install			
Set Admin Email	Go to Settings, Email to set a valid Email Reply-to Address			
Set Email Server	Go to Settings, Email to set a valid email server to send email. Demo SMTP Server enabled during trial	L		
GeolP Data	Go to Settings, Admin to enable GeoIP data generation and set GeoIP server URL (Optional)			
	S Clos	e		

Type in the path to the storage location in the box. You can click on the "Check Path" button to verify that the path exists and write permissions are available. Click on "Apply" button to set the storage path correctly.

Example Paths for Windows Installs: "c:\data", "e:\fileclouddata"

Example Path for Linux Installs: "/opt/fileclouddata"

Admin Attenti	on Required	×
Action Item	Description	^
Storage Path Not Set	Storage Path c:\data\cloud	
	Specify the Location to Store Cloud Files, this must be writable by Webserver. Example path on Windows: c:\clouddata Example path on Linux: /opt/cloud/data	
	Check Path Apply	
Invalid License File	Upload your license via Install License	~
	S CI	ose

2. Use the Admin portal to manage storage path changes.

Managing the Storage Path

Managing the Storage Path

To set or change storage path, open the FileCloud Admin Portal and then open the Settings->Storage Tab. Set the path as needed (for example on Windows c:\filecloud, or on Linux /opt/filecloud) and finally save the settings. Note that making this change after users have started uploading the files to the system will make many files missing unless the original files are carefully copied over to the new location.

(i) Do not change the storage path to the new location without copying over ALL folders and file that exist in the old path. Not copying the old data might lead to data loss.

Server Stora	ge /	Authentication	Admin	Database	Email	Endpoint Backup	License
My Files	Vetwork						
My Files Storag	e Settir	ngs	Ŷ				
Storage	e Path	C:\Clouddata	a			Check Path	
		Example path o Example path o Note: To change contents from t	n Windows : n Linux : /op e the storage he old storage	c:\cloud riles, th c:\cloud/data t/cloud/data e location after ge location to t	it has been he new.	configured, move the	_
Number of old ver to keep for eac	rsions ch file	3 Number of vers	ions to keep	1			
Disable My	/ Files	Disable 'My File	s' [Managed	Storage]			
User Storage L Calcu	Jsage lation	Exclude Sha Specify user sto	res rage calcula	tion		•	

3. After setting the path, you can rerun the install checks.

Enable MongoDB Bind IP and Authentication

By default, FileCloud installs the Mongo database server on the same machine as the web server without any authentication settings.

However, you may need to enable authentication for the following reasons:

- Added security
- Hosting the database server on a different machine than the web server.

Follow the steps here to enable authentication for MongoDB.

Set Up a Database User

A DB user has to be first created in MongoDB and this user can be later used in FileCloud for secure database access. Assuming we will add a user with following details:

User Name	Password
dbuser	passw0rd1

Use a command line mongo client and execute the following commands to create the required DB user.

The following command lists all the databases in the system (depending on the configuration one or more dbs may not exist (or new ones may be present). So it is important to set authentication for each of the DB in the system. (Ignore the "local" database that shows up when you type "show databases")

For MongoClient v3.0 and above

```
use admin
db.createUser( {    user:"dbuser",    pwd:"passw0rd1",    roles:[ "root" ] })
```

For Mongo Client v 2.4

Mongo Client		
> show databases	2S	
admin	0.078GB	
tonidoauditdb	0.078GB	
tonidoclouddb	0.078GB	
tonidos3storage	0.078GB	
tonidosettings	0.078GB	
tonidostoragedb	0.078GB	
tonidosyncdb	0.078GB	
> use admin:		
> db.addUser('db	lbuser','passw0rd1')	
> use tonidoaudi	litdb:	
> db.addUser('db	lbuser', 'passw0rd1')	
> use tonidoclou	buddb:	
> db.addUser('db	lbuser', 'passw0rd1')	
> use tonidostor	pragedb:	
> db.addUser('db	lbuser', 'passw0rd1')	
> use tonidosync	icdb;	
> db.addUser('db	lbuser', 'passw0rd1')	
> use tonidosett	tings;	

```
> db.addUser('dbuser','passw0rd1')
```

Upon executing all the above commands, 'dbuser' is added as a valid database user.

FC Push Service Configuration

In FileCloud version 23.1, a Push service has been added to allow clients (in particular, FileCloud Desktop) to receive server-initiated notifications (for example, file upload, share). Upgrading to FileCloud 23.1 or higher 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/.env
```

2. Update the MongoDB connection string:

FCPS_DB_DSN=mongodb://dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017

3. Restart the **fcpushservice**.

systemctl restart fcpushservice

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@mongosrv1.myfilecloud.com:27017

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

Changing the MongoDB IP binding

To change the MongoDB IP binding:

- Open the mongodb configuration file: Linux: /etc/mongodb.conf Windows: C:\xampp\mongodb\bin\mongodb.conf
- Find bind_ip and change its value to the IP or hostname that you want MongoDB to listen to.
 For example, if you want MongoDB to listen on the hostname mongosrv1.myfilecloud.com set bind_ip as follows:

bind_ip = mongosrv1.myfilecloud.com

Configure Settings DB URL

FileCloud's settings database is where all the information is bootstrapped from. The default implicit URL for this database is "mongodb://127.0.0.1". Set this URL explicitly to reflect the fact that a database user needs to be used and the database server resides on different server. To do this, edit the configuration file WWWROOT/config/ cloudconfig.php and add the following line:

Override Settings DB URL

```
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://
dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017");
```

In the above example, we assumed the database server is installed on a different machine (i.e., mongosrv1.myfilecloud.com) than the webserver. In collocated scenarios, 127.0.0.1 can be used as well.

Note: If you use special characters in the password, make sure to URI encode them. For example: using 'password@2090' as the password, you will need to specify it like

(i) mongodb://dbuser:password%402090@localhost:27017

Configure Other DB URLs In Config File

If you have never updated the database URLs in the admin UI, follow this sub-section. If not, skip to the next subsection.

Other database URLs required for FileCloud needs to be changed to reflect the database user as well. To do this, edit the configuration file WWWROOT/config/cloudconfig.php and update the following lines:

Update DB URLs in cloudconfig.php

```
// ... Cloud Database
define("TONIDOCLOUD_DBSERVER", "mongodb://
dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017");
// ... Audit Database
define("TONIDOCLOUD_AUDIT_DBSERVER", "mongodb://
dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017");
// ... Settings Database
define("TONIDOCLOUD_SETTINGS_DBSERVER", "mongodb://
dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017");
```

and configuration file WWWROOT/config/localstorageconfig.php and update the following line:

Update DB URLs in localstorageconfig.php

```
// ... Cloud Database
define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://
dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017");
```

Configure Other DB URLs In Settings DB

If you have updated the database URLs in the admin UI, then changing the values in the config files as described above will not work.

In this case use a mongodb client and update the URLs with the following information.

```
Update settings database with a mongo client
Database: tonidosettings
Collection: sites
Records: {
    "name" : "TONIDOCLOUD_DBSERVER",
    "value" : "mongodb://dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017"
    }, {
        "name" : "TONIDOCLOUD_AUDIT_DBSERVER",
        "value" : "mongodb://dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017"
    }, {
        "name" : "TONIDO_LOCALSTORAGE_DBSERVER",
        "value" : "mongodb://dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017"
    }, {
        "name" : "TONIDO_LOCALSTORAGE_DBSERVER",
        "value" : "mongodb://dbuser:passw0rd1@mongosrv1.myfilecloud.com:27017"
    }
```

Encrypting the DB User's Password

You may optionally encrypt the DB User's password so that it does not appear in cloudconfig.php.

To encrypt the password:

- Generate a secure key for encryption. First run the tool genkey to create a random password.
 - a. In a command line enter: For Windows:

cd c:\xampp\htdocs\resources\tools\security
PATH=%PATH%;C:\xampp\php

For Linux:

cd /var/www/html/resources/tools/security

b. Then, for both Windows and Linux, enter the genkey.php script to generate the secure key you will use to encrypt the plain ext password. Since genkey.php outputs to the screen by default, direct the output to the file securekey.key:

php genkey.php > securekey.key

- 2. Use the fcencrypt.php script with the key generated in the previous step (securekey.key) to encrypt the plain text password ("aSecretPassword" in the example below).
 - a. At the command prompt, enter the first line. The encrypted message is returned.

```
php fcencrypt.php --message "aSecretPassword" --key "securekey.key"
Encrypted message:
PgxQKdMU+k5756194hllcUcp5Qod7oXe2XgaQN0+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/vQ==
```

- b. Copy and save the encrypted message, which you will use as your encrypted password.
- 3. Save the key file and the encrypted password in cloudconfig.
 - a. Open the cloudconfig.php file Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php Linux Location: /var/www/config/cloudconfig.php
 - b. Enter settings for storing the encrypted password:

```
define('TONIDOCLOUD_ENCRYPTION_KEYFILE', 'c:
\xampp\htdocs\resources\tools\security\securekey.key');
define('TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD',
'PgxQKdMU+k5756194hlIcUcp5Qod7oXe2XgaQNO+qri9nHIoTBVYBA7PuLthEu7Eq+Mx4vZ/
vQ==');
```

Where the value for TONIDOCLOUD_ENCRYPTION_KEYFILE is the location of your securekey.key tool and the value for TONIDOCLOUD_MONGODB_ENCRYPTED_PASSWORD is your encrypted password.

- 4. Replace occurrences of the plain text password in cloudconfig with the placeholder
 - %tonidocloud_mongodb_password% in the settings:
 - FC_MONGODB_URI_OPTIONS
 - AUTOBACKUP_MONGODUMP_PARAMS

For example, instead of:

```
define("AUTOBACKUP_MONGODUMP_PARAMS", '--host 127.0.0.1 --username dbuser --
password aSecretPassword --authenticationDatabase admin');
```

enter:

define("AUTOBACKUP_MONGODUMP_PARAMS", '--host 127.0.0.1 --username dbuser -password %tonidocloud_mongodb_password% --authenticationDatabase admin');

Enable MongoDB Security

Now that FileCloud is updated with the security info, enable security in MongoDB. To do this open the file mongodb.conf that can be typically found in the following location:

Windows	C:\xampp\mongodb\bin\mongodb.conf
Linux	/etc/mongodb.conf

Edit this file and add/update with the following line. If the line is already there, ensure it is not commented.

Enable MongoDB security in Windows and mongodb v2.x on Linux

```
# Turn on/off security. Off is currently the default
#noauth = true
auth = true
```

If you are using a version of MongoDB that creates a YAML conf file, you might need to enable authentication using the following format.

Enable MongoDB v3.x on Linux

```
security:
authorization: enabled
```

For MongoDB replica set cluster configurations:

1. Run the below command to generate a key file. This key will be used for internal replicaset authentication:

openssl rand -base64 741 >"/var/lib/mongodb/mongodb-keyfile"

- 2. Copy the file /var/lib/mongodb/mongodb-keyfile to the other 2 database nodes.
- 3. Run the below commands to set permission and ownership.

```
chmod 400 /var/lib/mongodb/mongodb-keyfile
chown mongodb. /var/lib/mongodb/mongodb-keyfile
```

4. Add the below lines to /etc/mongod.conf

```
security:
  authorization: enabled
  keyFile: /var/lib/mongodb/mongodb-keyfile
```

Restart services

Finally, it is necessary to restart both MongoDB and Apache to get the security in-place.

🔒 Note

- In case of any issues, disable security in mongodb and fix the problems.
- To disable security, mongodb auth has to be disabled and the database URLs has to be reverted back.

SSL Configuration

FileCloud runs on Apache web server.

- Apache server can be configured to serve the website securely using HTTPS protocol.
- To enable the HTTPS protocol, you will need an SSL certificate.

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

What if I want to use SSL to secure AD?

If you are using Active Directory and want to:

- Add AD users
- Change AD passwords
- Secure the connection to Active Directory

Then you will need to configure additional settings and also install an SSL certificate on the AD server.

This topic does not relate to securing connections with your AD Server.

For that information, please read Connecting to AD via SSL

What is an SSL certificate?

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals.

To learn more about SSL, read knowledge base articles on the SSL web site.

What is an intermediate certificate?

To enhance the security of the Root certificate, two intermediate certificates are created from which SSL certificates are signed and issued.

• An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates.

The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. Such certificates are called chained root certificates.

Creating certificates directly from the CA root certificate increases the risk of root certificate compromise, and if the CA root certificate is compromised, the entire trust infrastructure built by the SSL provider will fail. The usage of intermediate certificates for issuing SSL certificates to end entities, therefore, provides an added level of security. You must install the intermediate certificate in your Web server along with your issued SSL certificate to complete the trust chain and allow the certificate to be effective.

Once you've got your certificate files, seeing your file extension will allow you to know what's in the file, and if you need to convert them.

What are the different file types?

File Extension	Contents
*.pem	Concatenated certificate container files
	Frequently required for certificate installations when multiple certificates are being imported as one file.
*.crt *.cer	The *.crt and *.cer file formats are interchangeable and contain the same information.
	the *.crt file is a Microsoft convention and can be easily converted to *.cer.
	An SSL certificate contains both:
	*.key = the private key to the certificate
	*.crt = the signed certificate
*.ca-bundle	A file that contains root and intermediate certificates.
	 The end-entity certificate along with a CA bundle constitutes the certificate chain.
	The chain is required to improve compatibility of the certificates with web browsers and other kind of clients.
	This allows browsers to recognize your certificate so that no security warnings appear.
*.pfx	This is an archive file format for storing several cryptographic objects in a single file.
	 contains the end-entity certificate (issued to your domain) a matching private key
	 may optionally include an intermediate certification authority (a.k.a. CA Bundle).
	All this is wrapped up in a single file which is then protected with a pfx password.

What do you want to do?





Use SSL on Windows

You can use the standard security technology to establish an encrypted link between the FileCloud server and a client browser.

- This link ensures that all data passed between the web server and browsers remain private and integral.
- SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

After you install the SSL certificate on your Apache web server, there is no additional configuration you need to do in FileCloud Server. Once a certificate is installed, all connections between to the FileCloud Server and clients are secured over SSL.

To Use SSL on Windows:

1. Create a CSR in the FileCloud Control Panel.

		- 0	×
.22350			
27017			
ehsite			
<u>coste</u>			
Start	Stop	Config Make	Service
		Config Make	Service
Start	Stop	Coning Make	Service
Start	Stop	Config Install	
		C	
Start	Stop	Config Install	
Start	Stop	Install	Config
Start	Stop	Install	<u>Config</u>
Start	btop	_	
Start	Stop	Make Service	
Start	Stop	Install	
Start	Stop		
Start	Stop	Install	
eset Admin Pas	sword		
stall SSL Cert			
ct Support De	emo and Trainin	g	
	22350 27017 ebsite Start Start Start Start Start Start Start Start Start Start Start Start Start Start Start	22350 27017 ebsite Start Stop Start Stop Start Stop Start Stop Start Stop Start Stop Start Stop Start Stop Start Stop	22350 27017 ebsite Start Stop Config Make Start Stop Config Make Start Stop Config Install Start Stop Config Install Start Stop Install

- 2. Submit the CSR to your SSL provider.
- 3. The provider will verify and then issue an SSL certificate. You may be given options to download the SSL certificate as a bundle certificate or as a main and bundle certificate. If you are given both download options, download both. If it comes in just one download option, download that.

4. Install the certificate.

FileCloud Control Panel			- 0	×	
FileCloud Control Panel					
v: 23.1.0.22350, Base Components: 23.1.0	.22350				
Webserver Ports: 80,443 Database Port:	27017				
Initial Setup: Install Check					
Web Portal: Admin Portal User W	ebsite				
Servers					
Webserver: Running SVC	Start	Stop	Config Make S	Service	
Database: Running	Start	Stop	Config Make S	Service	
Cron Task: Running SVC	Start	Stop	Config Install		
Message Queue: Running SVC	Start	Stop	Config Install		
Optional					
Push Service: Running SVC	Start	Stop	Install	<u>Config</u>	
FileCloud Helper: Running SVC	Start	Stop	Install	<u>Config</u>	
Memcache: Running SVC	Start	Stop	Make Service		
Document Preview: Running SVC	Start	Stop	Install		
Content Search: Running SVC	Start	Stop	Install		
Miscellaneous					
Configuration: Application Folder Reset Admin Passy ord					
SSL: Create SSL CSR Install SSL Cert					
Technical Support					
Need Help? Documentation Contact Support Demo and Training					

5. Follow the HTTPS Best Practices for FileCloud.

If you encounter issues using the FileCloud control panel, you can:

Manually create a CSR to receive an SSL certificate

Manually install a CRT file

Create a CSR in the FileCloud Control Panel

When using SSL on Windows, you must create a Certificate Signing Request (CSR) to receive an SSL certificate.

• A CSR is a data file that contains a Public Key and your domain details.

- You will submit the CSR to your SSL provider.
- Your provider will verify and then issue an SSL certificate file

If you encounter issues using the FileCloud control panel, you can:
 Manually create a CSR to receive an SSL certificate

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

To create a CSR in the FileCloud control panel:

1. Open the FileCloud Control Panel

2. Click Create SSL CSR.

FileCloud Control Panel			- 🗆 X	
FileCloud Control Panel				
v: 23.1.0.22350, Base Components: 23.1.0	0.22350			
Webserver Ports: 80,443 Database Port:	27017			
Initial Setup: Install Check				
Web Portal: Admin Portal User W	/ebsite			
Servers				
Webserver: Running SVC	Start	Stop	Config Make Service	
Database: Running			Config Make Service	
	Start	Stop		
Cron Task: Running SVC	Start	Ston	Config Install	
	Start	stop		
Message Queue: Running SVC	Start	Stop	Config Install	
Optional				
Push Service: Running SVC	Start	Ston	Install Config	
	Start	stop		
FileCloud Helper: Running SVC	Start	Stop	Install Config	
Mamorachai Bunning SVC			D. Maka Candian	
Memcache. Running SVC	Start	Stop	IVIAKE SERVICE	
Document Preview: Running SVC	Chard	Sten	Install	
	Start	Stop		
Content Search: Running SVC	Start	Stop	Install	
Miscellaneous				
Configuration: Application Folder Reset Admin Password				
SSL: Create SSL CSR Install SSL Cert				
Technical Support				
i comen support				
Need Help? Documentation Contact Support Demo and Training				

New CSR fields appear.

3. Enter your data into the fields.

FileCloud Control Panel	_			
FileCloud Control Panel v: 23.1.0.22590, Base Components: 23.1.0.225 Webserver Ports: 80,443 Database Port: 270	90			
Initial Setup: Install Check Web Portal: Admin Portal User Websi	<u>te</u>			
Servers				
Webserver: Running SVC	Stop Config	Make Service		
New CSR		×		
New CSR for SSL Certificate				
Country Name (2 Letter Code, e.g. US):	US			
State (e.g. Texas):	Texas			
City (e.g. Austin):	Austin			
Company Name (e.g. CodeLathe Inc):	FileCloud			
Organizational Unit (e.g. IT): IT				
Domain Name (e.g. files.company.com): your.site.ur				
Generate CSR	Cancel			
51	art Stop	.::		
Content Search: Running SVC St	art Stop Install			
Miscellaneous				
Configuration: Application Folder Reset Admin Password				
SSL: Create SSL CSR Install SSL Cert				
Technical Support				
Need Help? Documentation Contact Support Demo and Training				
Information Example Notes				

Information	Example	Notes
Country Name	US	2letter code
State	TEXAS	full name - no abbreviations
City	Austin	full city name
Organization Name	MyCompany	company name

FileCloud Server Version 23.232 Installation Guide

Information	Example	Notes
Organizational Unit Name	IT	section name
Domain Name	filecloud.IWPL.com	<pre>server FQDN or YOUR name Be sure to enter the actual server's fully qualified name filecloud.yourdomain.com If it is a wildcard certificate for all sub domains (for example for using multi tenancy), then be sure to enter *.yourdomain.com *.yourdomain.com</pre>

4. Click Generate CSR.

The following popup appears:

Succes	s! X
1	Copy the generated CSR and submit to the SSL provider so they can issue SSL Certificate. CSR file saved to C:\xampp\htdocs\config\server.csr Private Key file saved to C:\xampp\htdocs\config\server.key
	ОК

5. Submit the CSR to your SSL provider.

Submit a CSR to Your SSL Provider

You must create your CSR before you can submit it to your SSL provider. The following procedure uses GoDaddy as an example. Change the steps as necessary to perform the same actions in your SSL provider.

1. Log in to your SSL provider, and under SSL Certificates, click Set up.

< → 0	0 A	#* https://www.mi.gedaktyeambrevium		\$
	Search for a ner	w domain		۹.
			0	
	All Products a	and Services		
	• ×	Domains		Manage All 🛶
	ř	Payments		
	*	SSL Certificates		Manage All ->
		Standard SSL New Account		Options Set up
	~	Additional Products		

The **Certificate Setup** screen opens.

2. Click Input a CSR.

Paste the content of your CSR file into the text field.

Identify Primary Domain		
O Choose a Domain	Input a CSR	
Provide a domain and we'll create the CSR	The CSR should contain the Primary Domain	
BEGIN CERTIFICATE REQUEST		^
MIICrrCCAZcCAQAwajELMAkGA1UEBhMCVVMxETAPBgNVBAgMCFZpcmdpbn1hMREw		
DwYDVQQHDAhSaMNobW9uZDESH8AGA1UECgw3Rm1sZUNsb3VkHQswCQYDVQQLDA33		
VDEUMBIGA1UEAuwLZm9naWUuY2xvdWQwggEiMA8GCSqGSIb30QEBAQUAA4IBDwAw		
ggEKAoIB4QCrThFe4qZG7ug8vZL4znmKHy2HQdGh8ythfD5E0scgj8SZQTx2SQzp		
IzAtdQ59v3k/yA8oNWvFhOfKHaMC/8p048Rgd6igRCjetIG6VIEu9rcme6TPueyj		
A3Shhs36U/le2WPmvw5zoBJQs8G8C1v7N3vGcqR7MyYC0hI+Th0Y5vB7PiVce+aH		
K0++oKyEqG2yxAMc5VNFYA0rhp+VF7hSshEhUbF+SQcFiT3NB9qI7pfdBqIKU3DvG		
xKEyro0jw6F3NCrjCkCaDzRFiuHf1P7H3YEwFiS88MCHhtpKmch5/g6jWHEoQuMZ		
RKyOe5DKWIN9tKW5khPbpGWH6JfQx5RPAgMBAAGgADANBgkqhkiG9w8BAQsFAAOC		

- 3. Click **Continue** and complete the certificate setup.
- 4. Navigate to **Certificates** and select your certificate.
- 5. In Server Type, choose Apache.

6. Click **Download Zip File**.

Outlifeste Datalla		Devertee d Oastlife sta
Certificate Details		Download Certificate
Туре	Standard SSL Certificate	To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that
Status	Certificate issued (Revoke)	might be needed for older browsers or servers.
Domain name		View Installation Instructions for the selected server.
Certificate Issuer	GoDaddy SHA-2	Server type Anache Y Deventeed Zie Eile
Request Date	6/19/2023 4:41 PM	Aparina
Request Submission Type	New Request	
Current Certificate Validity Period	6/19/2023 - 6/19/2024	
Subscription Devied	1 00 0000 - 1 00 000 I	

7. Install the certificate.

Install a certificate using the FileCloud Control Panel

The ability to create and install an SSL certificate from FileCloud Control Panel is available in FileCloud Server version 14.0 and later.
 The option to add an Intermediate Certificate is available in FileCloud Server version 18.2 and later.
 If you want to include an intermediate certificate and do not have one saved locally, see Extracting an Intermediate Certificate from your Browser.

After you receive an SSL certificate, you can use the FileCloud Control Panel to install it.

If you encounter issues using the FileCloud control panel, you can:

Hanually install an SSL certificate in Windows

To install an SSL Certificate using the FileCloud Control Panel:

1. On the server, open the FileCloud Control Panel. Show me the control panel

FileCloud Control Panel			—		×
FileCloud Control Panel v: 23.1.0.22350, Base Components: 23.1.0 Webserver Ports: 80,443 Database Port:	.22350 27017				
Initial Setup: Install Check					
Web Portal: <u>Admin Portal</u> <u>User W</u>	<u>ebsite</u>				
Servers					
Webserver: Running SVC	Start	Stop	<u>Config</u>	<u>Make S</u>	ervice
Database: Running	Start	Stop	Confic	<u>Make S</u>	ervice
Cron Task: Running SVC	Start	Stop	<u>Config</u>	<u>Install</u>	
Message Queue: Running SVC	Start	Stop	<u>Config</u>	<u>Install</u>	
Optional					
Push Service: Running SVC	Start	Stop	<u>Install</u>		<u>Config</u>
FileCloud Helper: Running SVC	Start	Stop	<u>Install</u>		<u>Config</u>
Memcache: Running SVC	Start	Stop	Make	Service	
Document Preview: Running SVC	Start	Stop	Install		
Content Search: Running SVC	Start	Stop	Install		
Miscellaneous					
Configuration: Application Folder Re	eset Admin Pas	sylord			
SSL: <u>Create SSL CSR</u> In	stall SSL Cert				
Technical Support					
Need Help? Documentation Conta	ct Support De	mo and Trainin	g		

2. Under Miscellaneous, click Install SSL Cert.

3. Your screen should look similar to the following example:

Install SSL Certificate		×
Install SSL Certificates		
SSL Certificate File:		Select
SSL Private Key File:		Select
SSL Intermediate Certificate File (Optional):		Select
Install Certificates Ca	incel	

- 4. Across from SSL Certificate File, click Select.
- 5. Browse to the default location in: c:\xampp\htdocs\config\server.crt or to the place where the file is saved.
- 6. Across from SSL Private Key File, click Select.
- 7. Browse to the default location in: c:\xampp\htdocs\config\server.key or to the place where the file is saved.
- 8. Optionally, to install an intermediate certificate, across from SSL Intermediate Certificate File, click Select.
- 9. Browse to the default location in: c:\xampp\htdocs\config\server-ca.crt or to the place where the file is saved.
- 10. Your screen should look similar to the following example:

Install SSL Certificate		×
Install SSL Certificates		
SSL Certificate File:	C:\Users\Administrator\Desktop\server.crt	Select
SSL Private Key File:	C:\Users\Administrator\Desktop\server.key	Select
SSL Intermediate Certificate File (Optional):	C:\Users\Administrator\Desktop\server-ca.crt	Select
Install Certificates Ca	ncel	

- 11. Click Install Certificates.
- 12. On the **Confirm Installation** dialog box, to install the provided certificate and key, click **Yes**.
- 13. When you see the **Installed OK** dialog box, click **OK**.
- 14. To allow the changes to take effect, restart the server.

Manually Create a CSR in Windows

When using SSL on Windows, you must create a Certificate Signing Request (CSR) to receive an SSL certificate.

- A CSR is a data file that contains the Public Key and your domain details.
- You will submit the CSR to your SSL provider.
- Your provider will verify and then issue a SSL certificate in a .crt file.

F

You should use the FileCloud control panel to create a CSR. If you encounter issues, you can create the request manually.

🔫 Create a CSR using the FileCloud Control Panel

To manually create an SSL certificate, you can use the openssl tool included with FileCloud Server.

To manually create a CSR:

1. On the FileCloud server, navigate to the following directory:

c:\xampp\apache\bin

2. To open the tool, double-click OpenSSL.

3. To create a Private Server Key, type the following code: (If your SSL provider does not accept key lengths of 2048, a higher length of 4096 can be used in the following command.)

C:\xampp\apache\bin>openssl genrsa -des3 -out server.key 2048 -config "C: \xampp\apache\conf\openssl.cnf"

Note

If you encounter any errors related to: unable to open configuration file

Then run the following in the command prompt to set the path. set OPENSSL_CONF=c:\xamp\apache\conf\openssl.cnf

4. To create a Certificate Request (CSR), type the following command:

C:\xampp\apache\bin>openssl req -new -key server.key -out server.csr -config "C: \xampp\apache\conf\openssl.cnf"

5. You will be prompted to enter the following information:

Information	Example	Notes
Country Name	US	2letter code
State or Province Name	TEXAS	full name - no abbreviations
Locality Name	Houston	full city name
Organization Name	Internet Widgits Pty Ltd	company name
Organizational Unit Name	Accounts Payable	section name

Information	Example	Notes
Common Name	filecloud.IWPL.com	server FQDN or YOUR name
		Be sure to enter the actual server's fully qualified name
		filecloud.yourdomain.com
		If it is a wildcard certificate for all sub domains (for example for using multi tenancy), then be sure to enter *.yourdomain.com
		*.yourdomain.com
Email Address	moneyman@iwpl.com	
A challenge password		Use the same passphrase you typed in when opening the tool.

6. Apache won't start up properly if the key is secured with passphrase, so to remove it, type the following command:

```
copy server.key server.key.secure
openssl rsa -in server.key.secure -out server.key
```

7. You can now submit the CSR to your SSL provider.

The provider will sign and give you an SSL certificate usually called as server.crt.

Manually Install SSL Certificates for FileCloud on Windows

This section explains how to manually install the SSL certificate you received from your certificate provider.

If you want to include an intermediate certificate and do not have one saved locally, see Extracting an Intermediate Certificate from your Browser.

You should use the FileCloud control panel to install an SSL certificate. If you encounter issues, you can install the certificate manually.

To install an SSL certificate manually:

1. Install the SSL certificates

To enable SSL in Apache, the following are required:

- A signed certificate received from the certifying authority
- Your private key
- The location where FileCloud is installed, if not under the default location c:\xampp

To install the SSL certificates:

- 1. Rename your signed certificate to: server.crt
- 2. Rename your private key file to: server.key
- 3. Copy these two files using the following commands, replacing the xampp directory with the appropriate path if necessary:

copy server.crt C:\xampp\apache\conf\ssl.crt\ copy server.key C:\xampp\apache\conf\ssl.key\

2. Open the SSL config file, and enter your server name

1. Open the following file for editing:

C:\xampp\apache\conf\extra\httpd-ssl.conf

2. Find the following line:

ServerName "www.example.com:443"

3. Change the ServerName in quotes to your domain name.

1. In the serverName do not use * . For wild card certificates, use the FQDN excluding the *

The domain name should also match the FQDN/common name field of your CSR. Certificate Signing Request (CSR) is a data file that contains the Public Key and your domain details.

3. Install the Certificate Chain file

If your signed certificate needs a certificate chain file containing all the intermediate certificates, then you need to install the certificate chain file as well. To do this, you need to edit a configuration file and specify the chain file's location.

💡 If your intermediate certificates are not part of the standard ca-bundle, you must:

• Install the intermediate certificates on the FileCloud server

This will prevent issues with the Desktop client apps.

To install the certificate chain file:

Merge the chain certificate with your server certificate:

copy /Y server.crt+server-chain.crt C:\xampp\apache\conf\ssl.crt\server.crt

4. Restart the server

After you have completed:

- 1. Installing the SSL certificate
- 2. Installing the chain file

You must restart the Apache server.

This will activate the new SSL certificates and allow Apache to operate in HTTPS mode.

Extracting an Intermediate Certificate from your Browser

You can specify an SSL intermediate certificate file to include when you install your SSL certificate file on Windows.

Install SSL Certificate		×
Install SSL Certificates		
SSL Certificate File:	C:\Users\Administrator\Desktop\server.crt	Select
SSL Private Key File:	C:\Users\Administrator\Desktop\server.key	Select
SSL Intermediate Certificate File (Optional):	C:\Users\Administrator\Desktop\server-ca.crt	Select
Install Certificates Ca	ancel	

If you don't already have an intermediate certificate file stored locally, you can download one from your browser.

To download an SSL intermediate certificate file:

- 1. Go to a page on your browser that is using HTTPS, and click **F12**. The developer tools open.
- Click the Security tab. Just under the listing for Certificate is a View certificate button.
 Click the View certificate button.

🕞 💼 🛛 Elements Console	Sources Network Performance Memory Application Security 🗙 Lighthouse Recorder 🛦 Performance insights 🛦
Overview	This page is secure (valid HTTPS).
Main origin (secure)	Certificate - valid and trusted
https://projects.codelathe.com	The connection to this site is using a valid, trusted server certificate issued
Secure origins	by Sectigo RSA Domain Validation Secure Server CA.
https://resources.jetbrains.com	View certificate

The certificate window opens.

- 4. Click the **Certification Path** tab.
- 5. Select the third embedded certificate, which is the intermediate certificate.

6. Click View Certificate.

🗾 Certif	icate		<u>(</u>	×
General	Details	Certification Path		
Certif	ication pa	ath Frust RSA Certificati ctigo RSA Domain V *.codelathe.com	on Authority 'alidation Sec	ure Server CA
Certific This ce	ate statu ertificate	s: is OK.		View Certificate
				ОК

Another certificate window opens.

7. Click the **Details** tab.

8. Click Copy to File.

🖬 Certificate	×
General Details Certification	Path
Show <all></all>	~
Field Field Field Serial number Signature algorithm Signature hash algorithm Valid from Subject Contemport	Value V3 7d5b5126b476ba11db741 sha384RSA sha384 USERTrust RSA Certificati Thursday, November 1, 2 Sectigo RSA Domain Vali Sectigo RSA Domain Vali Edit Properties Copy to File
	ОК

The Certificate Export Wizard opens.

9.	Click Next.	
	← 🛛 ᡒ Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, click Next.	
	Next Can	cel

10. In the next window of the wizard, select Base-64 encoded X.509 (.CER), and click Next.

Exp	ort File Format Certificates can be exported in a variety of file formats.
	Select the format you want to use:
	O DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	Microsoft Serialized Certificate Store (.SST)

11. In the next window of the wizard, browse to the folder where you want to save the intermediate certificate, and name it with the extension crt.

12. Click Next.

🗧 😼 Certificate Export Wizard	
File to Export Specify the name of the file you want to export	
File name:	
C: Users yummisulator pesktop perver-ca.dit	
	Next Cancel

The last window confirms that you have completed the wizard.

13. Click Finish.

← 🛛 & Frificate Export Wizard	×
Completing the Certific	ate Export Wizard
You have successfully completed the Co	ertificate Export wizard.
You have specified the following setting	gs:
File Name	C:\Users\
Export Keys	No
Include all certificates in the certificat	ion path No
File Format	Baseo4 Encoded Y.209 (*,Cer)
<	>
	Finish Cancel

14. Return to the Install SSL Certificate window and select the intermediate certificate for SSL Intermediate Certificate File.

Install SSL Certificate		×
Install SSL Certificates		
SSL Certificate File:	C:\Users\Administrator\Desktop\server.crt	Select
SSL Private Key File:	C:\Users\Administrator\Desktop\server.key	Select
SSL Intermediate Certificate File (Optional):	C:\Users\Administrator\Desktop\server-ca.crt	Select
Install Certificates Ca	ancel	

Use SSL on Linux

You can use the standard security technology to establish an encrypted link between the FileCloud server and a client browser.

- This link ensures that all data passed between the web server and browsers remain private and integral.
- SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

After you install the SSL certificate on your Apache web server, there is no additional configuration you need to do in FileCloud Server. Once a certificate is installed, all connections between to the FileCloud Server and clients are secured over SSL.

To Use SSL on Linux:

- 1. Create a CSR for FileCloud.
- 2. Submit the CSR to your SSL provider.
- 3. The provider will verify and then issue a SSL certificate. You may be given options to download the SSL certificate as a bundle certificate or as a main and bundle certificate. If you are given both download options, download both. If it comes in just one download option, download that.
- 4. Install the certificate on Linux.
- 5. Follow the HTTPS Best Practices for FileCloud.

Create a CSR for FileCloud

When using SSL on Linux, you must create a Certificate Signing Request (CSR) to receive an SSL certificate.

- A CSR is a data file that contains the Public Key and your domain details.
- You will submit the CSR to your SSL provider.
- Your provider will verify and then issue a SSL certificate in a .cer file.

To create an CSR for you FileCloud Server:

1. To generate a request, use the following command: (The key for the SSL certificate is stored in the server.key file.)

openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr

2. You will be prompted to enter the following information:

Information	Example	Notes
Country Name	US	2letter code
State or Province Name	TEXAS	full name - no abbreviations
Locality Name	Houston	full city name
Organization Name	Internet Widgits Pty Ltd	company name
Organizational Unit Name	Accounts Payable	section name

Information	Example	Notes	
Common Name	filecloud.IWPL.com	server FQDN or YOUR name	
		Be sure to enter the actual server's fully qualified name	
		filecloud.yourdomain.com	
		If it is a wildcard certificate for all sub domains (for example for using multi tenancy), then be sure to enter *.yourdomain.com	
		*.yourdomain.com	
Email Address	moneyman@iwpl.com		
Please enter the following extra attributes to be sent with your certificate request:			
A challenge password			
An optional company name			

Install an SSL certificate on Linux

It's important to use SSL any time sensitive data is involved such as personal information, and authentication credentials such as passwords.

Your Linux system should be:

- running Ubuntu or RHEL
- accessible over the internet
- using a valid DNS entry that points to your Linux system
- 1. Copy the SSL certificate provided by your certification provider and SSL private key file to the apache directory. The certificate file is renamed as server.crt and private key file is renamed as server.key

```
etcssl=/etc/apache2/ssl # for Ubuntu
etcssl=/etc/httpd/ssl # for RHEL
sudo mkdir -p $etcssl
sudo cp server.crt $etcssl
sudo cp server.key $etcssl
```

2. If your signed certificate needs a certificate chain file containing all the intermediate certificates, then you need to install the certificate chain file as well.

```
sudo echo >> $etcssl/server.crt
sudo cat server-ca.crt >> $etcssl/server.crt
```

3. Modify your webserver configuration. **ServerName** must match the server name in the SSL certificate.

Ubuntu 22.04 or higher: Add this code to /etc/apache2/sites-enabled/000-default-conf

```
Ubuntu 22.04 or higher
<VirtualHost *:443>
# Admin email, Server Name (domain name) and any aliases
ServerAdmin support@xyz.com
ServerName server1.xyz.com
# Index file and Document Root (where the public files are located)
DirectoryIndex index.php
DocumentRoot /var/www/html
<Directory /var/www/html>
Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow, deny
allow from all
</Directory>
ErrorLog ${APACHE_LOG_DIR}/error.log
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
LogLevel warn
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLEngine On
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
</VirtualHost>
```

RHEL 9.0 or higher: Replace the **SSLCertificateFile** and **SSLCertificateKeyFile** lines in **/etc/httpd/conf.d/ ssl.conf** with the following:

	RHEL 9.0 or higher
	SSLCertificateFile /etc/httpd/ssl/server.crt SSLCertificateKeyFile /etc/httpd/ssl/server.key
4.	Restart Apache.
```
sudo systemctl restart apache2 # for Ubuntu
sudo systemctl restart httpd # for RHEL
```

Converting Existing PFX SSL Certificate to PEM SSL Certificate

Sometimes you will have an existing PFX file that you want to convert to PEM format. Usually this is due to specific server requirements.

To convert PFX to PEM:

1. To find the password used when the PFX was exported, use the following commands:

Linux	\$ openssl pkcs12 -in [yourfile.pfx] -nocerts -out [keyfile-encrypted.key]			
	<pre>\$ openssl pkcs12 -in [yourfile.pfx] -nocerts -nodes -out [keyfile- encrypted.key] # use this command if the first command generates empty certificate.</pre>			
Windows	C:\xampp\apache\bin\openssl pkcs12 -in [yourfile.pfx] -nocerts -out [keyfile-encrypted.key]			
	C:\xampp\apache\bin\openssl pkcs12 -in [yourfile.pfx] -nocerts -nodes -out [keyfile-encrypted.key] # use this command if the first command generates empty certificate.			

2. Convert encrypted key to unencrypted key:

Linux	\$ openssl rsa -in [keyfile-encrypted.key] -out server.key			
Windows	C:\xampp\apache\bin\openssl rsa -in [keyfile-encrypted.key] -out server.key			

3. Extract the server certificate and convert to PEM format:

Linux	\$ openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out server.crt		
Windows	C:\xampp\apache\bin\openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out server.crt		

4. Extract the server certificate chain:

Linux	\$ openssl pkcs12 -in [certificate.pfx] -cacerts -nokeys -out [server-ca.crt]
Windows	C:\xampp\apache\bin\openssl pkcs12 -in [certificate.pfx] -cacerts -nokeys -out [server-ca.crt]

5. (optional) In case your file is in p7b format, extract the server certificate and convert to PEM format

Linux	\$ openssl pkcs7 -print_certs -in [yourfile.p7b] -out server.crt
Windows	C:\xampp\apache\bin\openssl pkcs7 -print_certs -in [yourfile.p7b] -out server.crt

Now you can use the server.crt, server-ca.crt and server.key files appropriately.

Use Let's Encrypt to Renew SSL Certificates

() Starting with Version 19.3, FileCloud supports auto-renewing SSL certificates with Let's Encrypt.

To auto-renew your SSL certificate, you must first contact the Let's Encrypt team.

To use Let's Encrypt's HTTP-01 challenge for adding/renewing SSL certificates:

- 1. Contact the Let's Encrypt team and request auto-renewal of your SSL certifcate.
- 2. Open the following file:
 - Windows: C:\xampp\htdocs\.htaccess
 - Linux: /var/www/html/.htaccess
- 3. Find the following code:

```
#-----# Let's Encrypt Support
# Let's Encrypt Support
# RewriteRule ^.well-known/(.*)$ .well-known/$1 [L]
#-----
```

4. Remove # in front of:

RewriteRule ^.well-known/(.*)\$.well-known/\$1 [L]

so that the code appears as:

```
#-----# Let's Encrypt Support
RewriteRule ^.well-known/(.*)$ .well-known/$1 [L]
#-----
```

5. Save and close .htaccess.

HTTPS Best Practices for FileCloud

FileCloud recommends that you run all servers in a production environment only on:

• HTTPS (SSL)

• Port 443

This ensures that all communications between clients and FileCloud are completely encrypted.

💡 To access these secured sites, users will have to type in:

https://<SITENAME>

Best Practice	Reason	Steps				
Disable the existing HTTP port.	So that FileCloud can be accessed only securely via HTTPS. Setting redirects from HTTP to HTTPS is not recommended because mobile apps and other clients do not follow redirects (for security) Therefore removing the HTTP port completely is the best option.	 To Disable HTTP (port 80) for Windows: 1. Open the webserver config file for editing: c: \xampp\apache\conf\httpd.conf and 2. Comment out the line with Listen 80. 3. Save and close the file. 4. Restart the server. To Disable HTTP (port 80) for Linux: Open the webserver config file for editing: /etc/apache2/ports.conf 				
		 Save and close the file. Restart the server. 				
Verify your certificates are valid.	If you have an invalid SSL configuration, your users would receive various errors on the browser, and iPhone/iPad apps cannot preview Office documents.	You can check the validity of the SSL certificate by testing your install against a SSL certificate checker like https://www.sslshopper.com/ssl-checker.html				
		Provide your FileCloud URL and it will report any potential problems your SSL installation might have.				
		These tools should report no errors for your FileCloud to function properly in SSL mode.				

Best Practice	Reason	Steps
Change the default listening port (80).	If you have are conflicts with other ports.	<pre>For Windows: 1. Open the following file for editing: C: \xampp\apache\conf\httpd.conf 2. Locate the following two lines: Listen 80 ServerName localhost:80 3. Change these lines to the following: Listen your_new_port ServerName localhost:your_new_port 4. Save and close the file. For Linux: 1. Open the following file for editing: /etc/apache2/ports.conf 2. Locate the following line: Listen 80 3. Change it to Listen Your_new_port 4. Open the following file for editing: /etc/apache2/sites-enabled/000- default.conf 5. Locate the following line </pre> 4. Open the following file for editing: /etc/apache2/sites-enabled/000- default.conf 5. Locate the following line 4. Open the following line 5. Locate the following line 6. Change it to 7. Save and close the file.

Best Practice	Reason	Steps
Change the default HTTPS port (443).	If you have are conflicts with other ports.	<pre>For Windows: 1. Open the following file for editing: C: \xampp\apache\conf\extra\httpd- ssl.conf 2. Locate the following line Listen 443 3. Change it to Listen your_new_port 4. Locate the following line <virtualhost 5.="" <virtualhost="" _default_:443="" _default_:your_new_port="" change="" it="" to=""> 6. Save and close the file. For Linux: 1. Open the following file for editing: /etc/apache2/ports.conf 2. Locate the following lines <ifmodule mod_ssl.c="">Listen 443</ifmodule></virtualhost></pre> 3. Change it to <ifmodule mod_ssl.c="">Listen 443 4. Open the following file for editing: /etc/apache2/sites-available/ default_ssl 5. Locate the following lines <ifmodule <="" =="" pre=""> 4. Open the following file for editing: /etc/apache2/sites-available/ default_ssl 5. Locate the following line: <virtualhost _default_:443=""> 6. Change it to <virtualhost _default_:443=""> 7. Save and close the file.</virtualhost></virtualhost></ifmodule></ifmodule>

Best Practice	Reason	Steps
Disable server information in headers.	To prevent the Web application from disclosing the server name and server version in the response header.	 Open the Apache configuration file: Ubuntu location: /etc/apache2/apache2.conf CentOS location: /etc/httpd/conf/httpd.conf Windows location: C: \xampp\apache\conf\httpd.conf Add the following: ServerSignature Off ServerTokens Prod Restart the Apache server.

HTTP To HTTPS Redirects

It is recommended that you configure FileCloud Server so that it can be accessed securely only via HTTPS.

Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security).

Therefore removing the HTTP port completely is the best option.

If you must use a redirect, add the following lines:

```
<VirtualHost *:80>
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

• In Windows, the above lines should we added to file c:\xampp\apache\conf\extra\httpd-vhosts.conf. Restart the apache server.

Also make sure the following line is uncommented in the file C:\xampp\apache\conf\httpd.conf.

Virtual hosts Include conf/extra/httpd-vhosts.conf

• In Linux, the above lines should be added to the /etc/apache.d/sites-enabled/000-default.conf file. If you already have a VirtualHost directive, add only the lines starting with "Rewrite". Restart the apache server.

Configure HTTP SSL Redirects

It is recommended that you configure FileCloud Server so that it can be accessed securely only via HTTPS.

Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security).

Therefore removing the HTTP port completely is the best option.

HTTPS FileCloud Best Practices

If you must use a redirect, you will need to edit the webserver config file.

For Windows:

1. Open the following file for editing:

c:\xampp\apache\conf\extra\httpd-vhosts.conf

2. Add the following code

```
<VirtualHost *:80>
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

- 3. Save and close the file.
- 4. Open the following file for editing:

C:\xampp\apache\conf\httpd.conf

5. Make sure the following *Include* line is uncommented:

Virtual hosts Include conf/extra/httpd-vhosts.conf

- 6. Save and close the file.
- 7. Restart the server.

For Linux:

1. Open the following file for editing:

/etc/apache.d/sites-enabled/000-default.conf

2. Add the following code: (If you already have a VirtualHost directive, add only the lines starting with "Rewrite".)

<VirtualHost *:80>

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
```

- 3. Save and close the file.
- 4. Restart the server.

Changing a Default Port or Web Server Setting

The ports and Web servers used by FileCloud are normally set during installation. After installation is completed, if you need to, you can change the default listening ports and Web servers.

By default, FileCloud uses these 3 ports:

- 80 (web server)
- 443 (web server)
- 27017 (database)

If other programs are using these ports, the FileCloud server will not start up properly.

You might want to change the port numbers or Web servers in some of the following scenarios:

- You need to disable anything that uses port 80 and 443
- You want Apache to run on non standard ports or servers or use firewall rules
- You need to use IIS on standard ports

💡 It is also recommended to disable HTTP port on the FileCloud server.

To change the ports, you will need to open the FileCloud Control Panel.

FileCloud Server Version 23.232 Installation Guide

FileCloud Control Panel – 🗆 🗙							
FileCloud Control Panel v: 17.3.0.37651, Base Components: 17.3.0.37625 Webserver Ports: 80,443 Database Port: 27017							
Initial Setup: Install Check Web Portal: Admin Portal User Website							
Servers							
Webserver: Running SVC	Start	Stop Config	Make Service	1			
Database: Running	Start	Stop	Make Service	1			
Cron Task: Running SVC	Start	Stop Config	<u>ı İnstall</u>				
Optional							
FileCloud Helper: Running SVC	Start	Stop	<u>Install</u>	<u>Config</u>			
Memcache: Not Running	Start	Stop	Make Service				
Document Preview: Running SVC	Start	Stop	<u>Install</u>				
Content Search: Running SVC	Start	Stop	<u>Install</u>				
Miscellaneous							
Configuration: Application Folder	Reset Admin Pa	issword					
SSL: <u>Create SSL CSR</u>	Install SSL Cert						
Technical Support							

Need Help? Documentation Contact Support

To change a port or Web server setting:

- 1. On the server, from the *Windows Start* menu, select the *FileCloud Control Panel*, or double-click the *xampp/cloudcp.exe* file.
- 2. In the Servers section, for Webserver, click Stop.
- 3. Change the Port configuration according to HTTPS Best Practices for FileCloud.
- 4. To start the Webserver, click Start next to Webserver.
- 5. In the Servers section, for Database, click Stop, then Config.
- 6. Make your changes, save them, and next to Database, click Start.

 If you have changed the default Web server, open localconfig.php at: Windows Location: XAMPP DIRECTORY/htdocs/config/localconfig.php Linux Location: /var/www/config/localconfig.php and add the following, replacing n.n.n.n with the correct IP address.

define("TONIDOCLOUD_APACHE_BIND_IP", "n.n.n.n");

Installation Troubleshooting

Unexpected problems can happen when you are installing or configuring your new FileCloud software. The reasons vary, depending on your computer, your operating system, network speed, license, and other factors.

 ${}^{\circ}_{2}$ In the following section, to display more information, click on a topic.

The following list presents some of the issues we've encountered.

Webserver or Database Does Not Start

FileCloud Server not starting on Windows

If FileCloud Webserver or Database does not startup, it is most likely that another process is using the ports used by the Webserver and the Database. By default, FileCloud uses these 3 ports (**80, 443, 27017**), so if other programs are using these ports, the servers will not start up properly.

Most common applications that use these ports are Microsoft IIS, Skype, TeamViewer.

To figure out which application is using this port, open a command prompt and type the following command.

🛕 netstat -ano | find "LIST"

Con Select	C:\Windows\system32\cmd.ex	e		
C:\User	s∖madhan>netstat -an	o ¦ find "LIST"		^
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	9368
TCP	0.0.0.0:135	0.0.0:0:0	LISTENING	904
TCP	0.0.0.0:443	0.0.0:0:0	LISTENING	9368
TCP	0.0.0.0:445	0.0.0:0:0	LISTENING	4
TCP	0.0.0.0:554	0.0.0:0:0	LISTENING	3544
TCP	0.0.0.0:902	0.0.0:0	LISTENING	2732
TCP	0.0.0.0:912	0.0.0:0	LISTENING	2732
TCP	0.0.0.0:1512	0.0.0:0	LISTENING	12648
TCP	0.0.0.0:2869	0.0.0:0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0:0	LISTENING	272
TCP	0.0.0.0:5357	0.0.0:0	LISTENING	4
TCP	0.0.0.0:10010	0.0.0:0	LISTENING	12648
TCP	0.0.0.0:10243	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:45670	0.0.0.0:0	LISTENING	6936
TCP	0.0.0.0:49152	0.0.0:0	LISTENING	572
TCP	0.0.0.0:49153	0.0.0:0	LISTENING	988
TCP	0.0.0.0:49154	0.0.0:0	LISTENING	652
TCP	0.0.0.0:49155	0.0.0:0	LISTENING	1100
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING	1508
TCP	0.0.0.0:49159	0.0.0.0:0	LISTENING	636
TCP	0.0.0.0:49160	0.0.0:0	LISTENING	3344
TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING	1760

You can look at the process using ports 80, 443 or 27017. (for example 0.0.0:80). The right most column shows the process ID of the process using that port.

You can get the name of the process, by

▲ tasklist /svc /PI "PID eq 988"

GUI Option

Alternative option to see Process running on ports 80,443 or 27017 is through GUI. Go to Start>>All Programs>>Accessories>>System Tools>>Resource Monitor (or **Run** resmon.exe)

PID (4) - Image (System) running on port 80 implies IIS may be running. Stop the IIS and try to restart Apache.

FileCloud Server Version 23.232 Installation Guide

Nesource Monitor	-							- • ×
File Monitor Help								
Overview CPU Memory	Disk	Network						
Processes with Network Ac	tivity					0	-	Vit
Network Activity	2	Kbps Network I/O		0% Network Utilizatio	on (S	0		Network
TCP Connections	_					0		
Listening Ports		_	_	_	e			
Image	PID	Address	Port	Protocol	Firewall Status	*		MAR ANA
tagsrv.exe	3004	IPv4 unspecified	6006	UDP	Not allowed, n			60 Seconds
ApplicationWebServer.exe	4412	IPv4 unspecified	8080	TCP	Allowed, not r		=	TCP Connections
VBoxHeadless.exe	17484	IPv4 unspecified	8888	TCP	Allowed, not r			
EKAiOHostService.exe	2060	IPv4 unspecified	9322	TCP	Allowed, not r			
netsession_win.exe	4656	IPv4 loopback	9421	TCP	Allowed, not r			
Dropbox.exe	4496	IPv4 unspecified	17500	TCP	Allowed, not r	=		
Dropbox.exe	4496	IPv4 unspecified	17500	UDP	Allowed, not r			
System	4	IPv6 unspecified	26143	TCP	Not allowed, n			
System	4	IPv4 unspecified	26143	TCP	Not allowed, n			
AppleMobileDeviceService.exe	1888	IPv4 loopback	27015	TCP	Allowed, not r			Wireless Network Conr
googledrivesync.exe	5684	IPv4 loopback	37483	TCP	Allowed, not r			
tansny eve	3004	IPv4 unspecified	48080	TCP	Not allowed in	Ŧ	-	

Common Services Interfering with Ports using by FileCloud Server

Other Apps Using same Network Services
WWW Publishing Service
Microsoft IIS
Microsoft Skype
HTTPD.sys

For 2012 server, you might need to do this

(i) Windows server 2012

net stop http /y sc config http start= disabled

You might need to reboot after this

https://www.devside.net/wamp-server/opening-up-port-80-for-apache-to-use-on-windows

Mod Rewrite Fails

Mod Rewrite Setup Check Fails during Install

- 1. Verify that the mod_rewrite apache module is properly installed and activated
- 2. In Apache configuration file for the site, ensure "AllowOverride All" is set correctly for the site.
- 3. Ensure, that the Apache .htaccess file is present in the WWW Root (say /var/www or c:\xampp\htdocs)

() For HTTPS sites if everything else works but mod rewrite check error still is reported you can ignore it.

If you still have questions, send an email to our FileCloud Support Team (support@codelathe.com)

Mount a Share that FileCloud Can Access

You might need to mount a network share in the following situations:

- For installation purposes
- To allow FileCloud to use storage from devices over the network for both local storage as well as external shares

Use these instructions to mount a share that FileCloud can access without encountering any permission issues.

FAQ's

What is CIFS?

Common Internet File System (CIFS) is a file-sharing protocol that provides an open and cross-platform mechanism for requesting network server files and services.

• CIFS is based on the enhanced version of Microsoft's Server Message Block (SMB) protocol for Internet and intranet file sharing.

CIFS is typically used in workstation and server OSs and was a native file-sharing protocol in Windows 2000.

- CIFS is also used in embedded and appliance systems.
- Recent storage products, like Storage Area Network (SAN) and Network Access Server (NAS), are based on CIFS.

What is NFS?

Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984.

- This file system allows a user on a client computer to access files over a computer network much like local storage is accessed.
- NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.
- The NFS is an open standard defined in Request for Comments (RFC), allowing anyone to implement the protocol.

Mounting Scenarios

Shares are mounted using command line statements.



Mount a CIFS Share on Linux for FileCloud

You might need to mount a CIFS network share on Linux, so that FileCloud server can use storage from devices over the network for both local storage as well as external shares.

Use these instructions to mount a CIFS share in a way that prevents that FileCloud from encountering any permission issues.

Assumptions

Parameter	Value
Remote CIFS share path	//192.168.1.120/storage
Local mount path	/mnt/storage
CIFS user	username
CIFS password	password
Apache user uid	33. Note: check your server for the right uid
Apache user gid	33. Note: check your server for the right gid

Pre-requisites

Ensure the command mount.cifs is present in your distro. Here is the list of packages that provide this utility in different distros.

(i) Required Packages

Ubuntu: cifs-utils

Installing cifs-utils in Ubuntu

```
user@host:~$ sudo apt-get update
user@host:~$ sudo apt-get install cifs-utils
```

Mounting

Use the following command to mount the CIFS share

Command Line

```
user@host:~$ mount -t cifs -o
```

```
username=username,password=password,uid=33,gid=33,rw,nounix,iocharset=utf8,file_mode=077
7,dir_mode=0777 //192.168.1.120/storage /mnt/storage
```

```
or if you have credential files at /root/.this-creds-file
user@host:~$ mount -t cifs -o credentials=/root/.the-creds-file,uid=33,gid=33,rw,nounix,
iocharset=utf8,file_mode=0777,dir_mode=0777 //192.168.1.120/storage /mnt/storage
```

Auto Mounting

To perform auto mounting of windows share, you need to create a password file and use that in /etc/fstab. Follow the steps here:

1. Create a file /root/.smbcredentials with the following content.

Command Line	
username=winuser password=winpass	
Here <i>winuser</i> and <i>winpass</i> are the username and password for the remote CIFS share.)

2. Change the permissions such that only root can read the file.

Command Line	
# sudo chmod 700 /root/.smbcredentials	

3. Now add the following line in /etc/fstab file.

Command Line

```
//192.168.1.120/storage /mnt/storage cifs credentials=/
root/.smbcredentials,uid=33,gid=33,rw,nounix,iocharset=utf8,file_mode=0777,dir_mod
e=0777 0 0
```

4. Test if the line added in the fstab file works.

Command Line

```
# sudo mount -a
If you are getting any error while mounting like " host not found ", add version
as below at the end of dir_mode=0777 as shown in the below//192.168.1.120/
storage /mnt/storage cifs credentials=/
root/.smbcredentials,uid=33,gid=33,rw,nounix,iocharset=utf8,file_mode=0777,dir_mod
e=0777,vers=3.0 0 0
```

Now the remote share should be mounted at /mnt/storage.

Mount an NFS share on Linux for FileCloud

FileCloud server might need use storage from devices over network for both local storage as well as external shares. This document explains how to mount a NFS network share on Linux.

Pre-requisites

(i) Required Packages Ubuntu: nfs-common

Installing nfs-common in ubuntu

```
user@host:~$ sudo apt-get update
user@host:~$ sudo apt-get install nfs-common
```

Mounting

Use the following command to mount the NFS share

Commandline

```
user@host:~$ mount simpson.example.com:/misc/export /misc/local
```

In this command, simpson.example.com is the hostname of the NFS file server, /misc/export is the directory that simpson is exporting, and /misc/local is the location to mount the file system on the local machine. After the mount command runs (and if the client has proper permissions from the simpson.example.com NFS server) the client user can execute the command ls /misc/local to display a listing of the files in /misc/export on simpson.example.com.

(i) The mount point directory on local machine (/misc/local in the above example) must exist.

Mount CIFS Shares from Windows Command Line

Connect Network Drive

To map a network drive from windows command line:

- 1. Click Start, and then click Run.
- 2. In the **Open** box, type cmd to open command line window.
- 3. Type the following, replacing Z: with drive letter you want to assign to the shared resource: net use Z: \\computer_name\share_name /PERSISTENT:YES

Disconnect Network Drive

To disconnect a mapped drive:

- 1. Open command line window.
- 2. Type the following, replacing X: with drive letter of the shared resource: net use Z: /delete

Storage and Client Application Limits

One of FileCloud's most important features is the number of different storage options it offers for the user website and client applications. When choosing your storage options, consider the limitations of each option. The following table lists the most common limitations to consider when using FileCloud with Network Folders, including Drive and Sync applications. Where applicable, the table includes ways of working around these limitations:

Server Component or Client Application	Description of the limitation
Network Folders	Since Network Folders are stored outside of FileCloud, offline syncing of files using the FileCloud Sync app may be slower and cause more server CPU load then offline syncing with Managed Storage.
	If offline syncing of folders with 5,000 folders or more is needed, we recommend that you use Managed Storage.
	Folder and File listings may be slower: Depending on the network connectivity to the Network Share, it may take more time to access and list files and folders in Network Folders than in Managed Storage.
	When using Network Folders on Windows, you cannot access files or folders if the entire path exceeds 256 characters.
	Files starting with "." are not supported in network folders
FileCloud Sync App & FileCloud Drive App	Windows Operating Systems only allow file and folder names of 256 characters or less, so if an entire file path and name exceed 256 characters, you cannot access it locally using Windows Explorer.
	Shorten the name or move the file or folder to a higher-level folder within FileCloud.
	Names Ending with "." or "," Files and folders ending with these characters cause processing errors.
	Rename these files and folders.
	FileCloud Sync and FileCloud Drive don't sync files with characters that are incompatible with certain operating systems.
	Rename them to something more suitable for use across multiple operating systems.
	Invalid characters are: * <> : \/ ?~

Server Component or Client Application	Description of the limitation
	 The following files are not uploaded: tonido.db Thumbs.db desktop.ini files ending with .tmp files ending with .lnk files or folders ending with space .tonidocache files starting with Conflict_ sync.ico .ds_store hidden files (usually files starting with . in Linux and files with a hidden attribute in Windows) file names and file extensions which are restricted by the server admin files that are in use (locked by the system or any other application) Beginning in Version 19.1, FileCloud supports overriding file type restrictions. To allow users to sync file types such as lnk, ini and thumbs.db, as well as hidden files, use
FileCloud Drive App	The FileCloud Drive App supports Windows 8+. It can be installed on Windows 7; however, we do not provide support since the
	If Sophos Antivirus is installed, Drive application performance with large files (10MB+) is impacted.
	If a folder in FileCloud (or a Network Folder) has over 1K files and folders inside it, Drive can take approximately 30 seconds or more to list the files/folders, depending on folder content, network speed, Internet access speed, and so on. In some cases, it can fail to list the folder's content. We recommended that you reorganize the content in lower count subfolders (-1K).
	Network Folder and File listings may be slower: Depending on the network connectivity to the Network Share, it may take more time to access and list files and folders in Network Folders than in Managed Storage.

Mounting CIFS and NFS Shares

- How to Mount CIFS Shares from Windows Command Line
- How to properly mount a CIFS share on Linux for FileCloud
- How to properly mount a NFS share on Linux for FileCloud

How to Mount CIFS Shares from Windows Command Line

Connect Network Drive

To map a network drive from windows command line:

- 1. Click Start, and then click Run.
- 2. In the **Open** box, type cmd to open command line window.
- 3. Type the following, replacing Z: with drive letter you want to assign to the shared resource:

net use Z: \\computer_name\share_name /PERSISTENT:YES

Disconnect Network Drive

To disconnect a mapped drive:

- 1. Open command line window.
- Type the following, replacing X: with drive letter of the shared resource: net use Z: /delete

How to properly mount a CIFS share on Linux for FileCloud

You might need to mount a CIFS network share on Linux so that FileCloud can use storage from devices over the network for both local storage and external shares.

Use these instructions to mount a CIFS share in a way that prevents FileCloud from encountering any permission issues.

Assumptions

Parameter	Value
Remote CIFS share path	//192.168.1.120/filecloud
Local mount path	/mnt/storage
CIFS user	username

Parameter	Value
CIFS password	password
Apache user uid	48. Note: check your server for the right uid
Apache user gid	48. Note: check your server for the right gid

Pre-requisites

Ensure the command mount.cifs is present in your distro. Here is the list of packages that provide this utility in different distros.

(i) Required Packages

RHEL: cifs-utils

```
yum update -y
yum install cifs-utils
```

Mounting

Use the following command to mount the CIFS share:

```
mount -t cifs -
o username=username,password=password,uid=48,gid=48,rw,nounix,iocharset=utf8,file_mode=0
777,dir_mode=0777 //192.168.1.120/storage /mnt/storage
```

or if you have credential files at /root/.this-creds-file:

```
mount -t cifs -o credentials=/root/.the-creds-file,uid=48,gid=48,rw,nounix,iocharset=utf
8,file_mode=0777,dir_mode=0777 //192.168.1.120/storage
```

Auto Mounting

To perform auto mounting of a Windows share, create a password file, and use it in /etc/fstab. Follow the steps here:

1. Create a file /root/.smbcredentials with the following content.

username=filecloud password=password

2. Change the permissions such that only root can read the file.

```
chmod 700 /root/.smbcredentials
```

3. Now add the following line in /etc/fstab file.

```
//192.168.1.120/storage /mnt/storage cifs credentials=/
root/.smbcredentials,uid=48,gid=48,rw,nounix,iocharset=utf8,file_mode=0777,dir_mod
e=0777 0 0
```

4. Reload systemctl daemon.

```
systemctl daemon-reload
```

5. Test if the line added in the fstab file works.

mount -a

Now the remote share should be mounted at /mnt/storage.

How to properly mount a NFS share on Linux for FileCloud

Introduction

FileCloud server might need use storage from devices over network for both local storage as well as external shares. This document explains how to mount a NFS network share on Linux.

Pre-requisites

(i) Required Packages Ubuntu: nfs-common

Installing nfs-common in ubuntu

```
user@host:~$ sudo apt-get update
user@host:~$ sudo apt-get install nfs-common
```

Mounting

Use the following command to mount the NFS share

Commandline

user@host:~\$ mount simpson.example.com:/misc/export /misc/local

In this command, simpson.example.com is the hostname of the NFS file server, /misc/export is the directory that simpson is exporting, and /misc/local is the location to mount the file system on the local machine. After the mount command runs (and if the client has proper permissions from the simpson.example.com NFS server) the client user can execute the command ls /misc/local to display a listing of the files in /misc/export on simpson.example.com.

(i) The mount point directory on local machine (/misc/local in the above example) must exist.