FILECLOUD

FileCloud Server

23.253

Installing FileCloud Server

18 December, 2025

Table of Contents

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 (see page 192) first.

Step 1: Install FileCloud Software

- **WINDOWS**: Install FileCloud using the installer on Windows (see page 4) (Windows 64 bit) (or)
- **LINUX** (Ubuntu, RedHat) (see page 23)

- Other options
  - Install FileCloud using the provided Virtual Machine (see page 25) (VMWare etc)
  - Manual install from scratch on Ubuntu (see page 23) or RedHat/Fedora (see page 23)
  - Install FileCloud on Amazon AWS (see page 49)
  - Install FileCloud on Amazon GovCloud AWS (see page 82)

⚠ 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 (see page 119) and EXTENDED (see page 124) checks.
  Note that some checks might fail, but you can resolve them later in the Admin Portal Settings.

Go to Verify Your Installation (see page 116)

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 (see page 124)

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 (see page 129)

Step 5: Set the Managed Storage Path
Set the storage path where FileCloud stores all its files. This only applies if you are using Local Storage.
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 (see page 139)

Step 6: Proceed to Site Setup
Use the Administrator Guide to get your site ready for users to log onto and use.
Go to the Administrator Guide

Windows Defender October 2020
Microsoft has changed some rules for virus detection. As a result, some files are now falsely identified as viruses.

This can lead to the following errors in FileCloud:

- New file uploads fail.
- Files that have already been uploaded are quarantined or deleted so that users can no longer access them.

We recommend **excluding the following directories from the scan in Windows Defender** or other AV programs:

- FileCloud temporary folders **C:\xampp\tmp** and **C:\xampp\htdocs\scratch** (If you installed FileCloud on a different drive, please use that instead of C:\)
- Managed Storage Location (if you do not use object storage / S3): (FileCloud Admin Portal -> Settings -> Storage -> Storage Path)

You may also refer to the following URL for more information on excluding folders in Windows Defender: https://support.microsoft.com/en-us/help/4028485/windows-10-add-an-exclusion-to-windows-security

Are you migrating to FileCloud?
No matter which edition of FileCloud you are using, it is easy to transfer your data after your FileCloud site is setup.

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.

Read the Requirements first.

- WINDOWS: Install FileCloud using the installer on Windows (see page 4) (Windows 64 bit) (or)
- LINUX: Installation of FileCloud on Linux Using the Repository (see page 23)

Installation Options

- Direct Installation (see page 4)
- Virtual Machine Installation (see page 25)
- Microsoft Azure Installation (see page 28)
- Amazon Web Services (AWS) Installation (see page 49)
- Amazon GovCloud AWS Installation (see page 82)
- FileCloud Docker installation (see page 94)
- Alibaba Cloud Installation (see page 99)
- Oracle Cloud Installation (see page 107)

- Direct Installation (see page 4)
- Virtual Machine Installation (see page 25)
- Microsoft Azure Installation (see page 28)
- Amazon Web Services (AWS) Installation (see page 49)
- Amazon GovCloud AWS Installation (see page 82)
- FileCloud Docker installation (see page 94)
- Alibaba Cloud Installation (see page 99)
- Oracle Cloud Installation (see page 107)

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. (see page 4)
- Installation of FileCloud on Linux Using the Repository (see page 23)

Install FileCloud Server on Windows.

Installation on Windows (64-bit)

The installation process on Windows includes the following steps:

1. Run the Setup Wizard (see page 5).
2. Use the FileCloud Control Panel to configure servers (see page 6).
3. Use the FileCloud Control Panel to configure optional components (see page 17).
4. Complete Post-Installation Steps (see page 19).

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

Run the setup wizard

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.[1]
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.

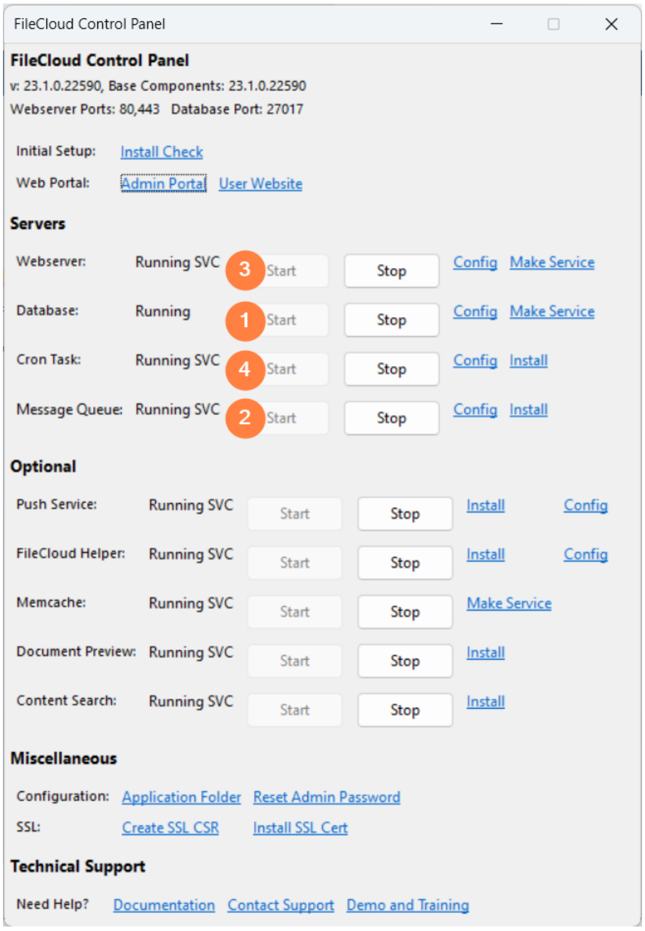
[1] https://portal.getfilecloud.com/ui/user/index.html#dwld.

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

FileCloud Control Panel

v: 23.1.0.22590, Base Components: 23.1.0.22590

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

Webserver: Running SVC

Database: Running

Cron Task: Running SVC

Message Queue: Running SVC

Optional

Push Service: Running SVC

FileCloud Helper: Running SVC

Memcache: Running SVC

Document Preview: Running SVC

Content Search: Running SVC

Miscellaneous

Configuration: Application Folder Reset Admin Password

SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support Demo and Training

The order you should start and configure these servers is:

1. Make and start the **Database** service
2. Configure and start the **Message Queue**
3. Make and start the **Webserver**
4. Configure and start the **Cron Task**

By default the Database and Webserver run as a process.

If the user running the application logs out, the process will exit.

To prevent this, you can run these servers as services.

Start the Database Server

FileCloud Server uses MongoDB as the database server.

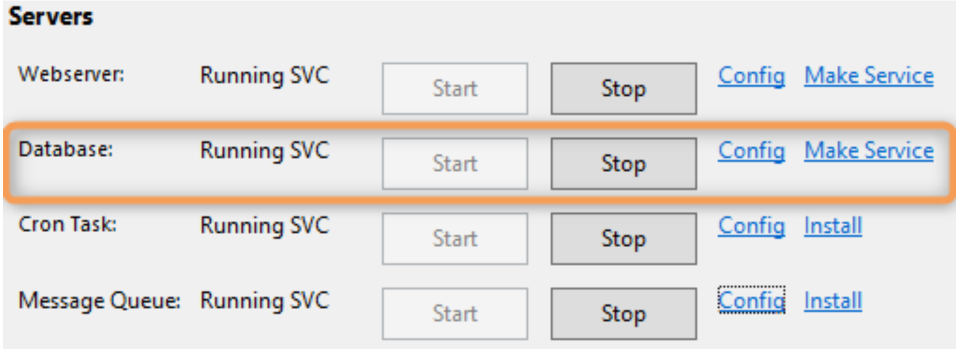
MongoDB is a cross-platform document-oriented database program.

- 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[2]

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 **Servers** 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 **Servers** section, for **Database**, click the **Start** button.
4. In the **FileCloud Control Panel**, in the **Servers** section, confirm that **Running** appears next to **Database**.

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.[3]

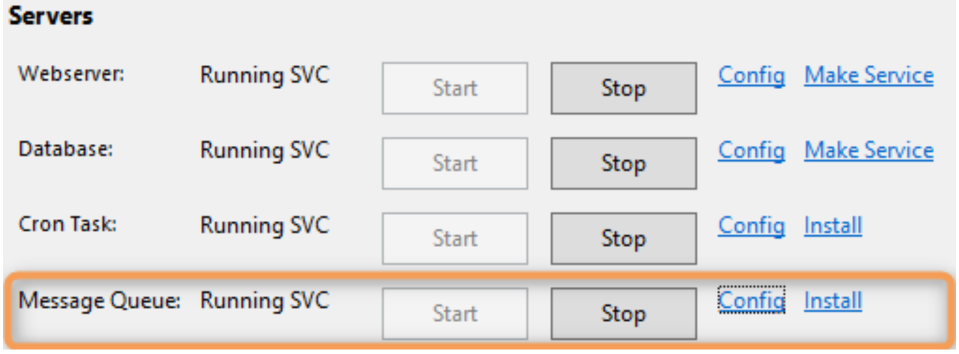
[2] https://www.mongodb.com/

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

Database: Running SVC

Cron Task: Running SVC

Message Queue: Running SVC

To configure and start the Message Queue service:

1. In the **FileCloud Control Panel**, in the **Servers** section, for **Message Queue**, click the *Install* link.
2. In the **FileCloud Control Panel**, in the **Servers** 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 **Servers** section, confirm **Running** appears next to **Message Queue**.

When you make a change to the configuration file

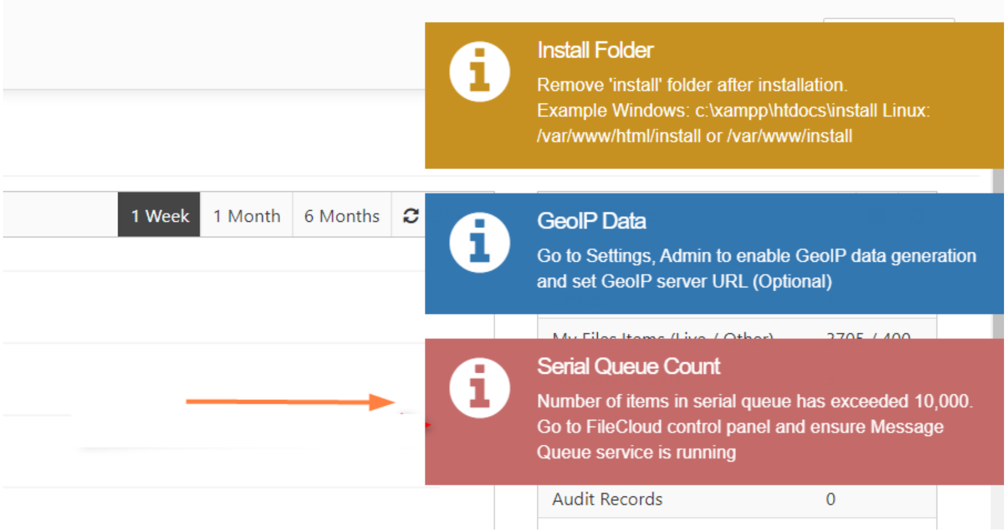
Each time you make a change to the FileCloud configuration file (cloudconfig.php) you must restart the message queue (click **Stop**, and once the service stops, click **Start**).

[3] http://install/

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.



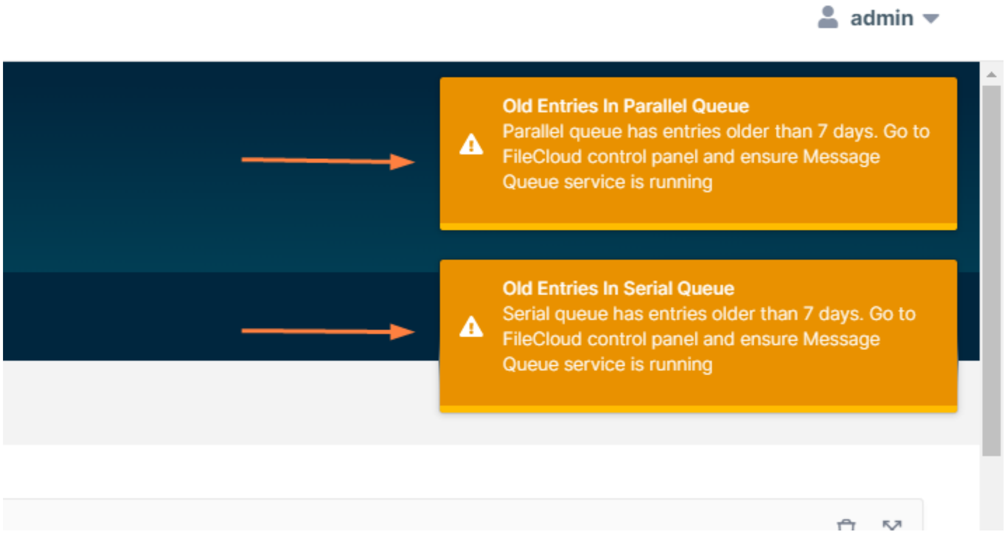
Install Folder
Remove 'install' folder after installation.
Example Windows: c:\xampp\htdocs\install Linux: /var/www/html/install or /var/www/install

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

Serial Queue Count alert

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 In Parallel Queue
Parallel queue has entries older than 7 days. Go to FileCloud control panel and ensure Message Queue service is running

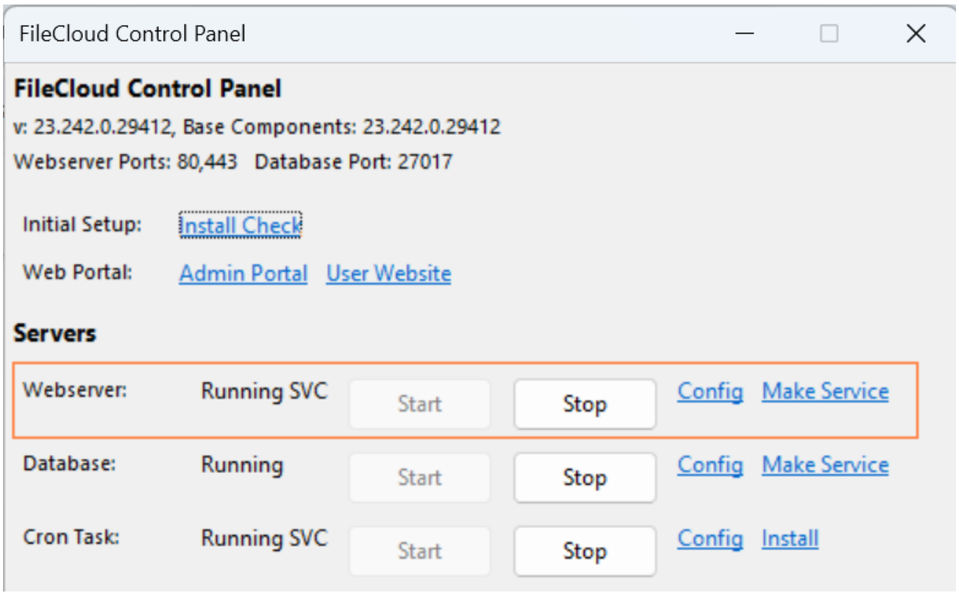
Old Entries In Serial Queue
Serial queue has entries older than 7 days. Go to FileCloud control panel and ensure Message Queue service is running

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 Control Panel

v: 23.242.0.29412, Base Components: 23.242.0.29412

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

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

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**, confirm **Running SVC** appears next to **Webserver**.

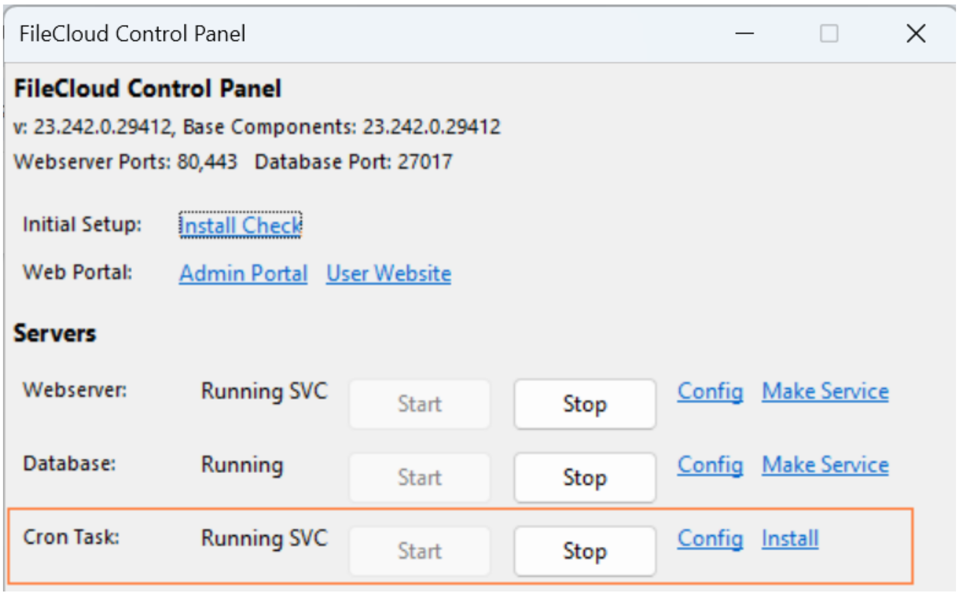
If the WebServer service doesn't start, then another process could be using that port.
To check which program is using that port, see FileCloud not starting on Windows.[4]

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.

[4] http://install/

⚠ FileCloud requires the Cron Task. You must Install this service and start it running before moving on to the next step.



FileCloud Control Panel

FileCloud Control Panel

v: 23.242.0.29412, Base Components: 23.242.0.29412

Webserver Ports: 80,443 Database Port: 27017

Webserver: Running SVC

Database: Running

Cron Task: Running SVC

To install and start the Cron Task service:

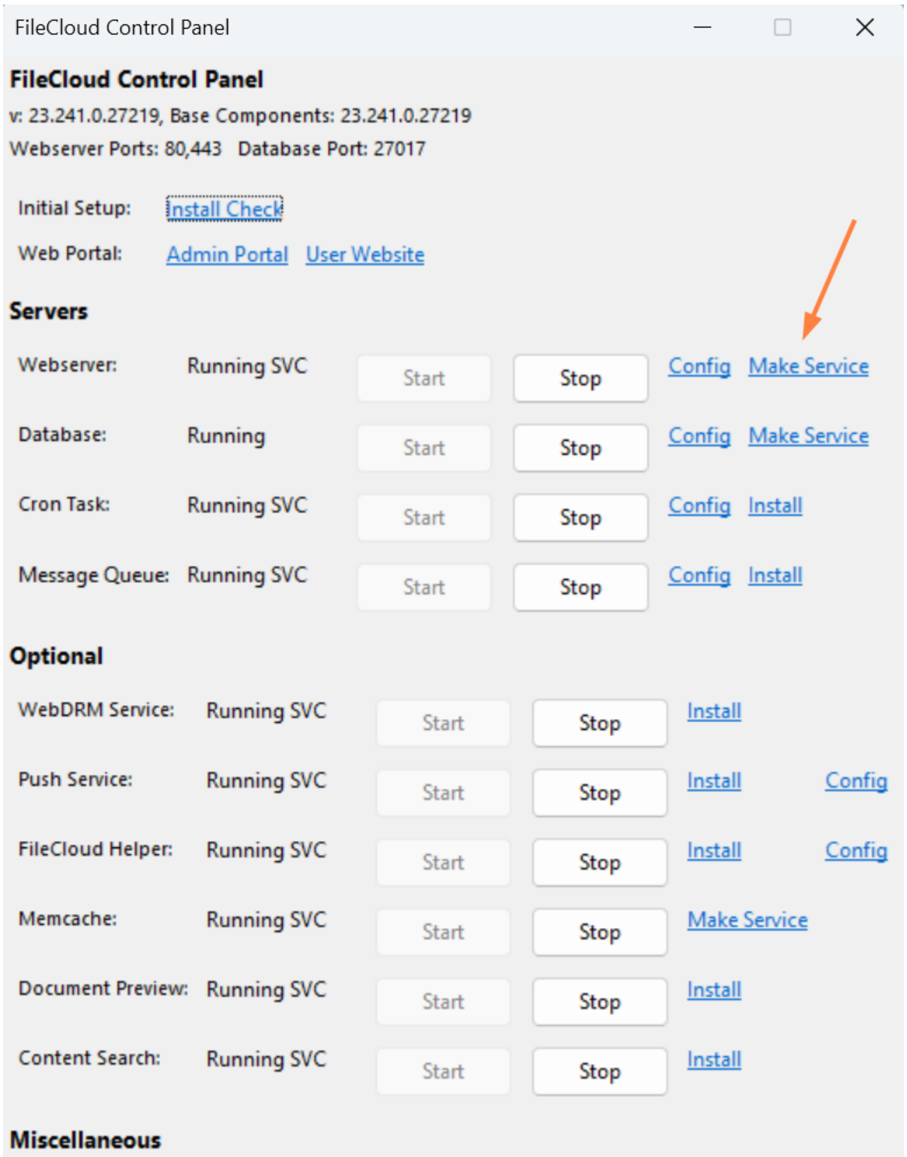
1. In the **FileCloud Control Panel**, for **Cron Task**, click the **Install** link.
2. On the **Confirmation Installation** window, click **Yes**.
3. On the **Service Installed OK** window, click **OK**.
4. In the **FileCloud Control Panel**, for **Cron Task**, click the **Start** button.
5. In the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

Install Web Server as a Service on Windows

By default, the web server that is shipped as 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 the FileCloud web server as a service.

Install as a Service

Click the **Make Service** link in the Control Panel to install the web server as a service. Then click **Start** to start the service.



FileCloud Control Panel

FileCloud Control Panel

v: 23.241.0.27219, Base Components: 23.241.0.27219

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

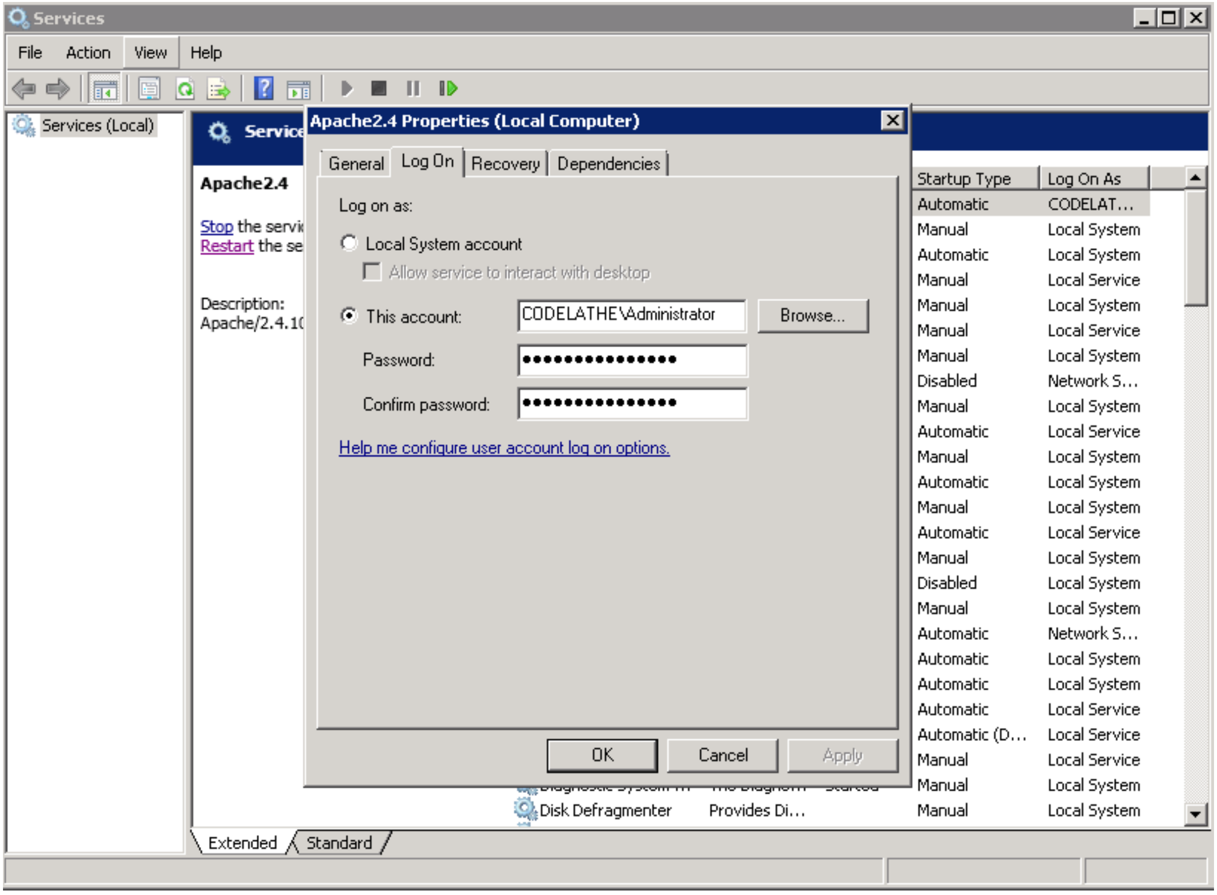
Webserver:	Running SVC	Start	Stop	Config	Make Service
Database:	Running	Start	Stop	Config	Make Service
Cron Task:	Running SVC	Start	Stop	Config	Install
Message Queue:	Running SVC	Start	Stop	Config	Install

Optional

WebDRM Service:	Running SVC	Start	Stop	Install	
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	Install	

Miscellaneous

✖ If you are making existing network shares accessible to FileCloud, we suggest you modify the service log-on permissions to run as a user account with full privileges to network shares (see screenshot below).



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: CODELATHE\Administrator

Password: •••••••••••••••

Confirm password: •••••••••••••••

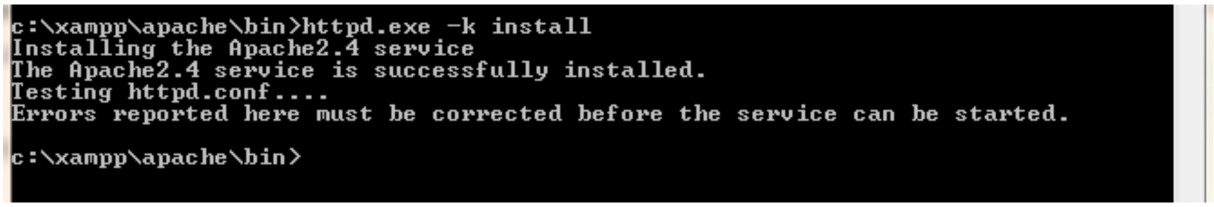
Help me configure user account log on options.

Startup Type	Log On As
Automatic	CODELAT...
Manual	Local System
Automatic	Local System
Manual	Local Service
Manual	Local System
Manual	Local Service
Manual	Local System
Disabled	Network S...
Manual	Local System
Automatic	Local Service
Manual	Local System
Automatic	Local System
Manual	Local System
Automatic	Local Service
Manual	Local System
Disabled	Local System
Manual	Local System
Automatic	Network S...
Automatic	Local System
Automatic	Local System
Automatic	Local Service
Automatic (D...	Local Service
Manual	Local Service
Manual	Local System
Manual	Local System

Disk Defragmenter Provides Di...

Alternatively, to install as a service, open an administrator command prompt and enter:

```
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>
```

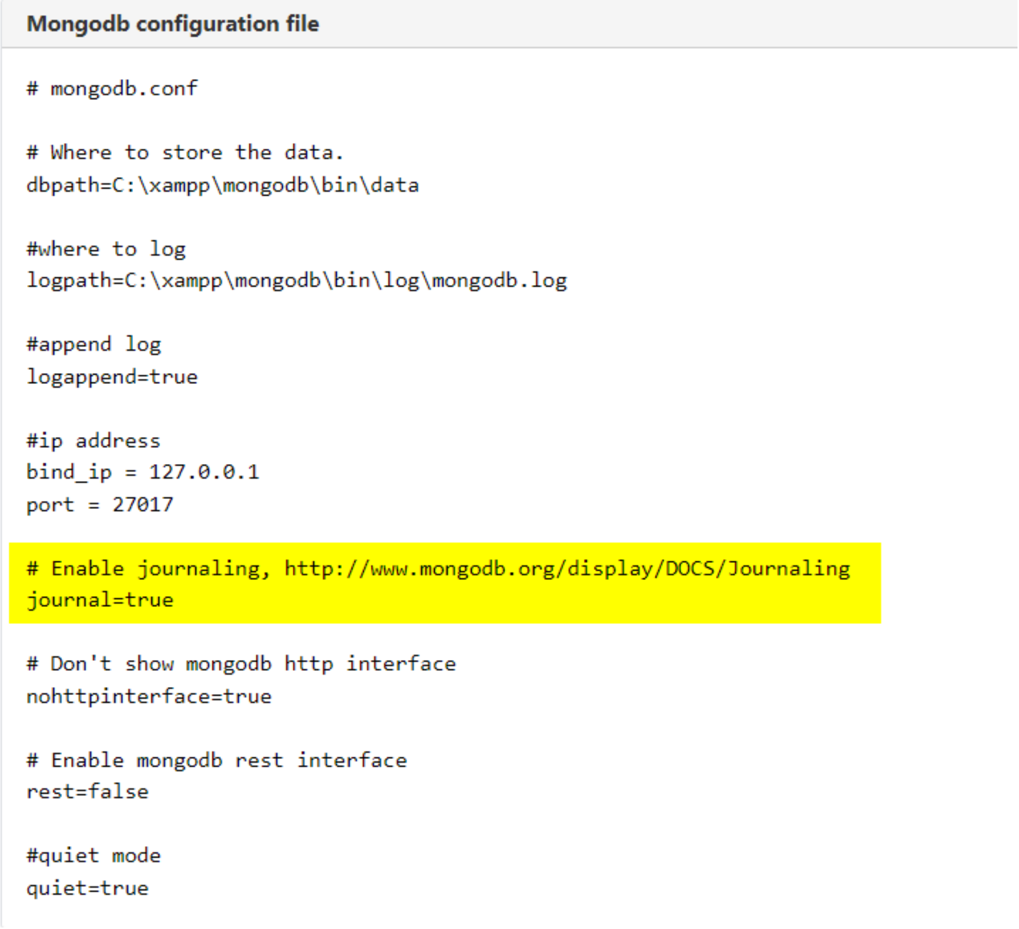
Remove Apache Service

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

Install MongoDB as a Service on Windows

If you are updating from a version earlier than 23.242 to FileCloud 23.242 or later
If you are replacing the supplied mongodb.conf with a custom one, it is important that you remove the **journal=true** setting which is no longer supported.
To delete the journal=true setting

1. Open C:\xampp/mongodb/mongodb.conf.
2. Delete the lines that are highlighted in the image below and save the file.



Mongodb configuration file

```
# mongodb.conf

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

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

#append log
logappend=true

#ip address
bind_ip = 127.0.0.1
port = 27017

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

# Don't show mongodb http interface
nohttpinterface=true

# Enable mongodb rest interface
rest=false

#quiet mode
quiet=true
```

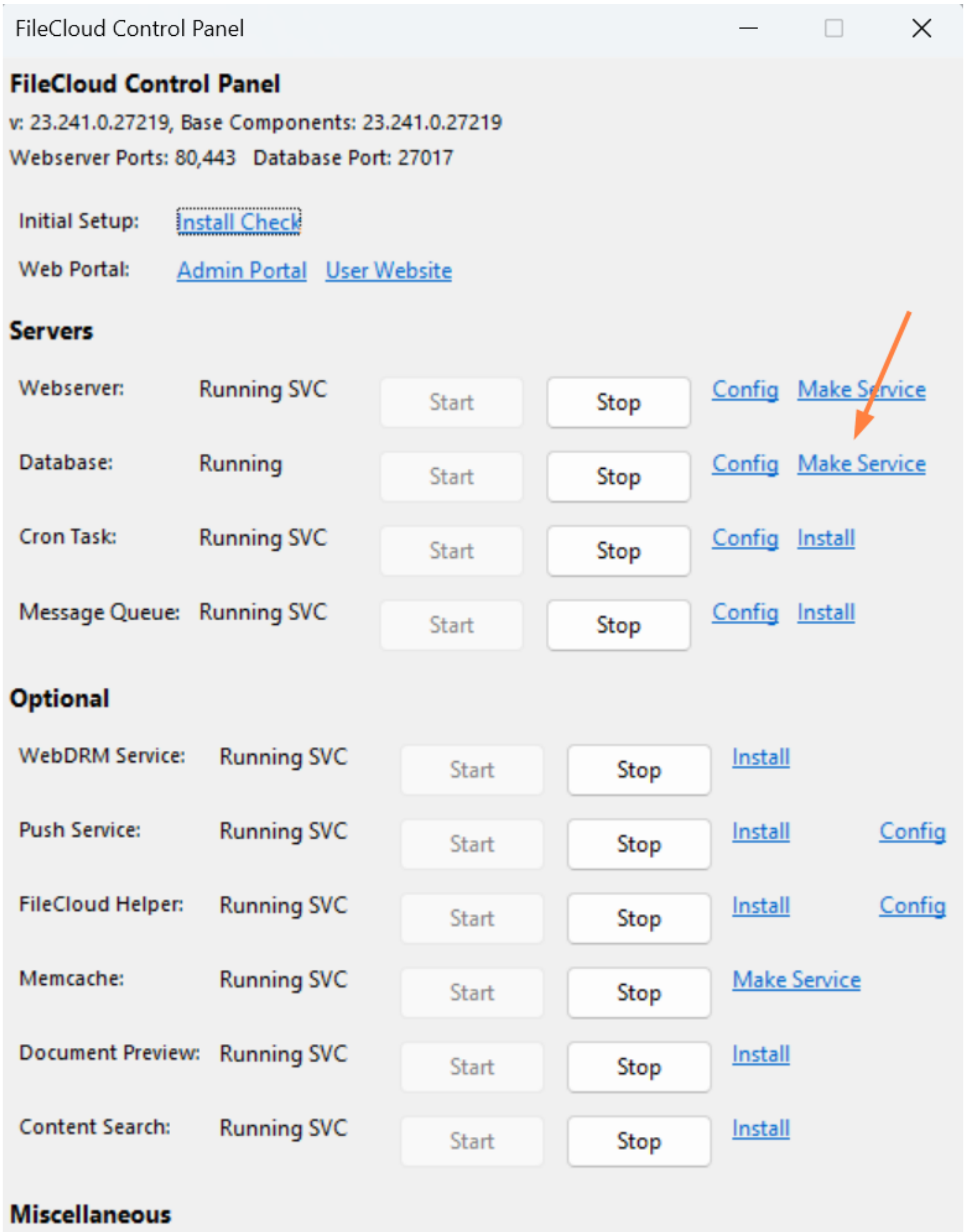
By default MongoDB in Windows runs as a process. If the user running the application logs out, the database process will exit. To prevent this, you can run the MongoDB database as a service.

To run MongoDB as a service in FileCloud

1. Install FileCloud

Before making MongoDB a service, install FileCloud using the Windows installer. By default FileCloud is 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.

2. Set MongoDB to run as a Windows Service



FileCloud Control Panel

FileCloud Control Panel

v: 23.241.0.27219, Base Components: 23.241.0.27219

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

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

Optional

WebDRM Service:	Running SVC	Start	Stop	Install	
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	Install	

Miscellaneous

Alternate Method

1. Create the MongoDB config File

Under **C:\xampp\mongodb\bin**, update **mongodb.conf**, and use absolute paths for the locations of **logpath** and **dbpath**.

> It is important when running mongodb as a service that **dbpath** and **logpath** are provided as full paths instead of relative paths. That is, include the root **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

# 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.

2. Create the MongoDB service

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

Creating MongoDB Service

```
C:\> cd C:\xampp\mongodb\bin
C:\xampp\mongodb\bin> mongod.exe --config C:\xampp\mongodb\bin\mongodb.conf --install
```

You can start the MongoDB service using the FileCloud Control Panel.
Now the service will start automatically on machine reboots.

To remove the MongoDB service

Removing MongoDB Service

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

Configuring Optional Components

The installation process on Windows includes the following steps:

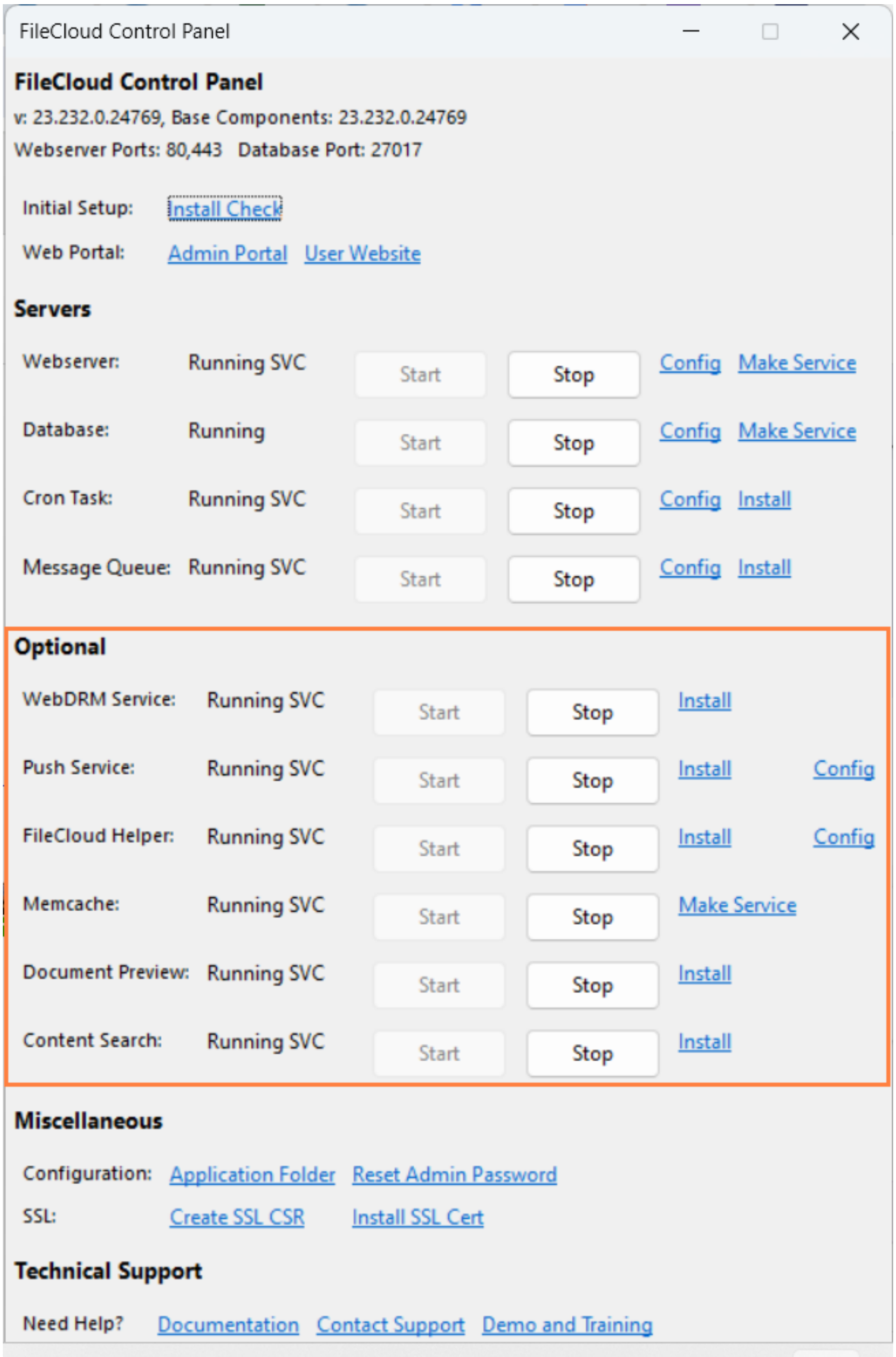
1. Run the Setup Wizard
2. Use the FileCloud Control Panel to configure servers
3. **Use the FileCloud Control Panel to configure optional components**
4. Complete Post Installation Steps

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:

- **Push Service** - Open 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

v: 23.232.0.24769, Base Components: 23.232.0.24769

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

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

Optional

WebDRM Service:	Running SVC	Start	Stop	Install	
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	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

✓ 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.

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**

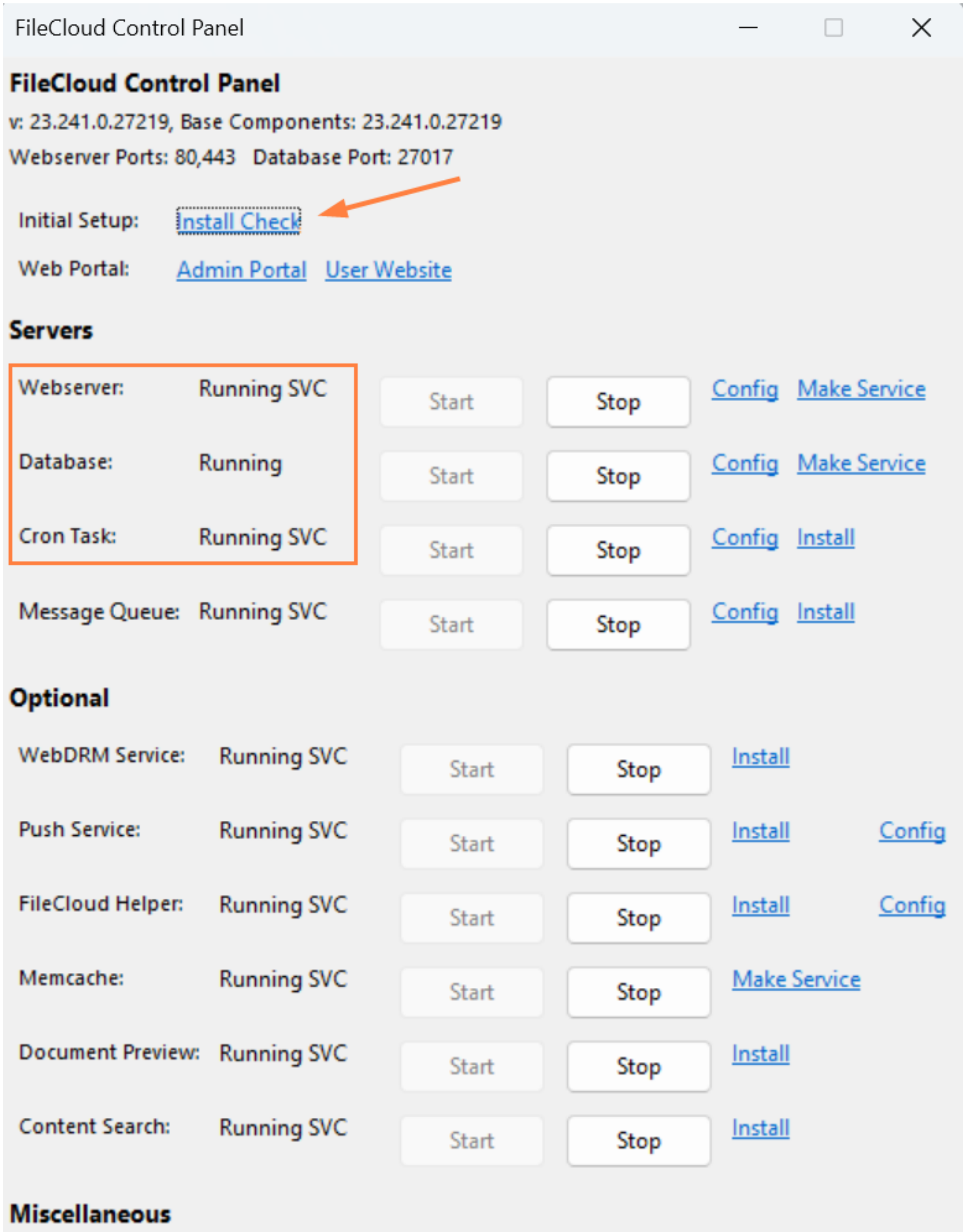
Complete Post Installation Steps

At this point, the basic FileCloud service is ready to be tested. Before logging in to the admin portal, 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.

To perform post-installation checks:

1. Confirm that the FileCloud Control Panel displays:
   - **Running SVC** beside **Webserver**.
   - **Running** beside **Database**.
   - **Running SVC** beside **Cron Task**.

2. In the FileCloud Control Panel, next to **Initial Setup**, click **Install Check**.



FileCloud Control Panel

FileCloud Control Panel

v: 23.241.0.27219, Base Components: 23.241.0.27219

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

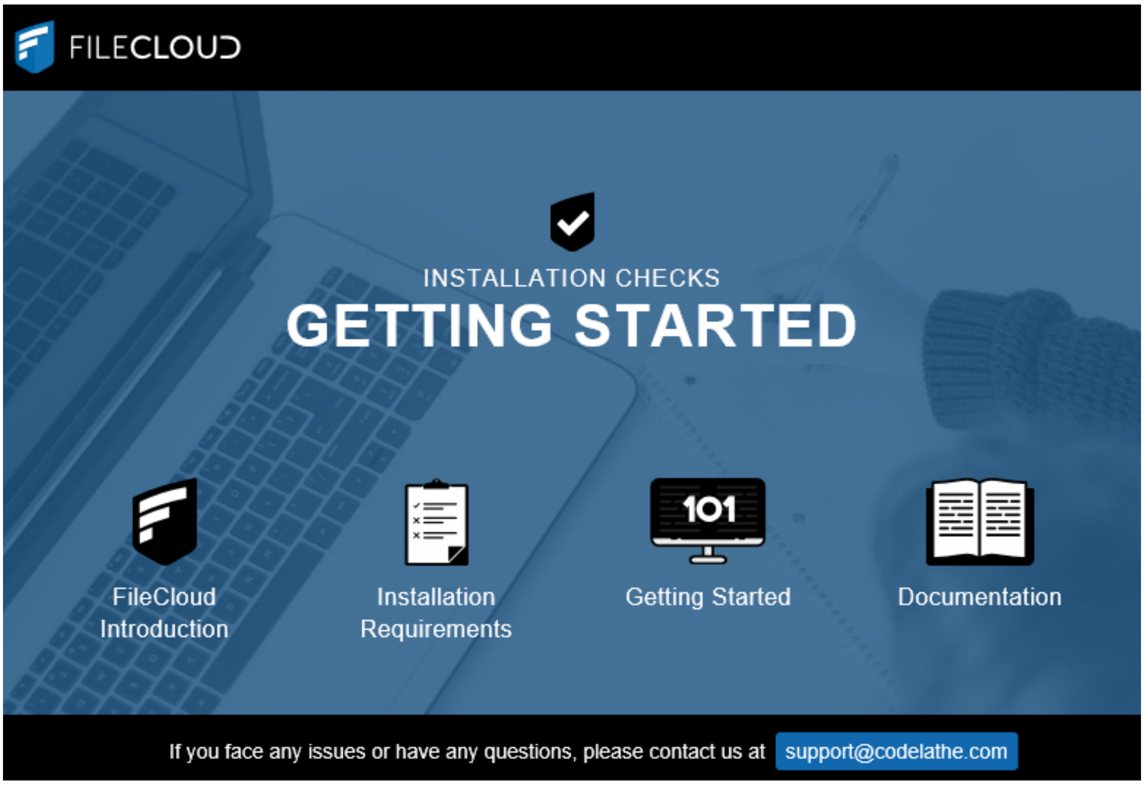
Webserver:	Running SVC	Start	Stop	Config	Make Service
Database:	Running	Start	Stop	Config	Make Service
Cron Task:	Running SVC	Start	Stop	Config	Install
Message Queue:	Running SVC	Start	Stop	Config	Install

Optional

WebDRM Service:	Running SVC	Start	Stop	Install	
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	Install	

Miscellaneous

3. If successful, you should see the **Getting Started** screen.



If you face any issues or have any questions, please contact us at support@codelathe.com

4. Follow the instructions in Post Installation (see page 113) to complete your cloud setup.

FileCloud Watchdog Service

FileCloud Watchdog Service is a service for Windows that automatically monitors the availability of Apache web server and the MongoDB databases and can restart them if they become unavailable or unresponsive.

Installation

1. Open a Windows Administrator command prompt.
2. Navigate to c:\xampp folder (or the xampp folder path).
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 (or the xampp folder path).
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 specifies 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 OpenOffice 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 the FileCloud Watchdog Service is inside the XAMPP folder under the filename cloudwatchdog.log

FileCloud Retention CLI Tool

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[5].
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[6]
RHEL information[7]

Installation instructions for each operating system

Installation for Ubuntu 22.04 LTS

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

[5] https://en.wikipedia.org/wiki/Advanced_Vector_Extensions#CPUs_with_AVX

[6] https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=canonical&CertificateStatus=Active&ValidationYear=0

[7] https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=Red+Hat

Enter the following commands:

```
apt clean cache
curl -fsSL https://pgp.mongodb.com/server-7.0.asc | sudo gpg -o /usr/share/keyrings/
mongodb-server-7.0.gpg --dearmor
echo "deb [ arch=amd64,arm64 signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ]
https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 multiverse" | sudo tee /etc/
apt/sources.list.d/mongodb-org-7.0.list
rm -rf /etc/apt/sources.list.d/mongodb-org-6.0.list

apt update -y
apt install -y mongodb-org=7.0.24 mongodb-org-database=7.0.24 mongodb-org-server=7.0.24
 mongodb-org-mongos=7.0.24 mongodb-org-tools=7.0.24 --allow-downgrades
apt-mark hold mongodb-org mongodb-org-database mongodb-org-server mongodb-org-mongos
mongodb-org-tools
curl -fsSL https://repo.filecloudlabs.com/static/pgp/filecloud.asc | sudo gpg -o /usr/
share/keyrings/filecloud.gpg --dearmor
echo "deb [ arch=amd64 signed-by=/usr/share/keyrings/filecloud.gpg ] https://
repo.filecloudlabs.com/apt/ubuntu jammy/filecloud/23.253 main" | sudo tee /etc/apt/
sources.list.d/filecloud.list
apt update -y
apt install -y apache2 pigz
apt install -y php8.4 php8.4-bcmath php8.4-cli php8.4-igbinary php8.4-common
php8.4-curl php8.4-gd php8.4-gmp php8.4-imap php8.4-intl php8.4-ldap php8.4-mbstring
php8.4-memcache php8.4-memcached php8.4-mongodb php8.4-opcache php8.4-readline
php8.4-soap php8.4-xml php8.4-xsl php8.4-zip php8.4-sqlite3 php-json libapache2-mod-
security2
ACCEPT_EULA=Y apt install filecloud -y
```

Installation for RHEL 9

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

Enter the following commands:

```
yum clean all
dnf module disable httpd -y
dnf module disable php -y

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

cat <<EOF > /etc/yum.repos.d/filecloud-23.253.repo
[filecloud-23.253]
name=FileCloud 23.253
baseurl=https://repo.filecloudlabs.com/yum/redhat/\$releasever/filecloud/23.253/x86_64/
gpgcheck=1
priority=1
enabled=1
gpgkey=https://repo.filecloudlabs.com/static/pgp/filecloud.asc
module_hotfixes=true
EOF

cat <<EOF > /etc/yum.repos.d/mongodb-org-7.0.repo
```

```
[mongodb-org-7.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/\$releasever/mongodb-org/7.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-7.0.asc
EOF

yum update -y --allowerasing
yum install yum-utils -y
yum-config-manager --enable mongodb-org-7.0
yum-config-manager --enable filecloud-23.253
yum install mongodb-org-7.0.24 mongodb-org-database-7.0.24 mongodb-org-server-7.0.24
 mongodb-org-mongos-7.0.24 mongodb-org-tools-7.0.24 -y
ACCEPT_EULA=Y dnf install filecloud -y
```

Virtual Machine Installation

Beginning with version 6, MongoDB requires use of the AVX instruction set, which is available on select Intel and AMD processors[8].
If your CPU doesn't have the AVX instruction set, MongoDB version 6 and higher 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 Server
Disk Size	100 GB
RAM	8 GB

The following is the OS user login information

[8] https://en.wikipedia.org/wiki/Advanced_Vector_Extensions#CPUs_with_AVX

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 at link: https://patch.codelathe.com/tonidocloud/live/vm/TonidoCloud-OVF.zip
2. Unzip the zip file with all the contents into your hard disk
3. See VMWare Player Install Instructions (see page 27).

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
```

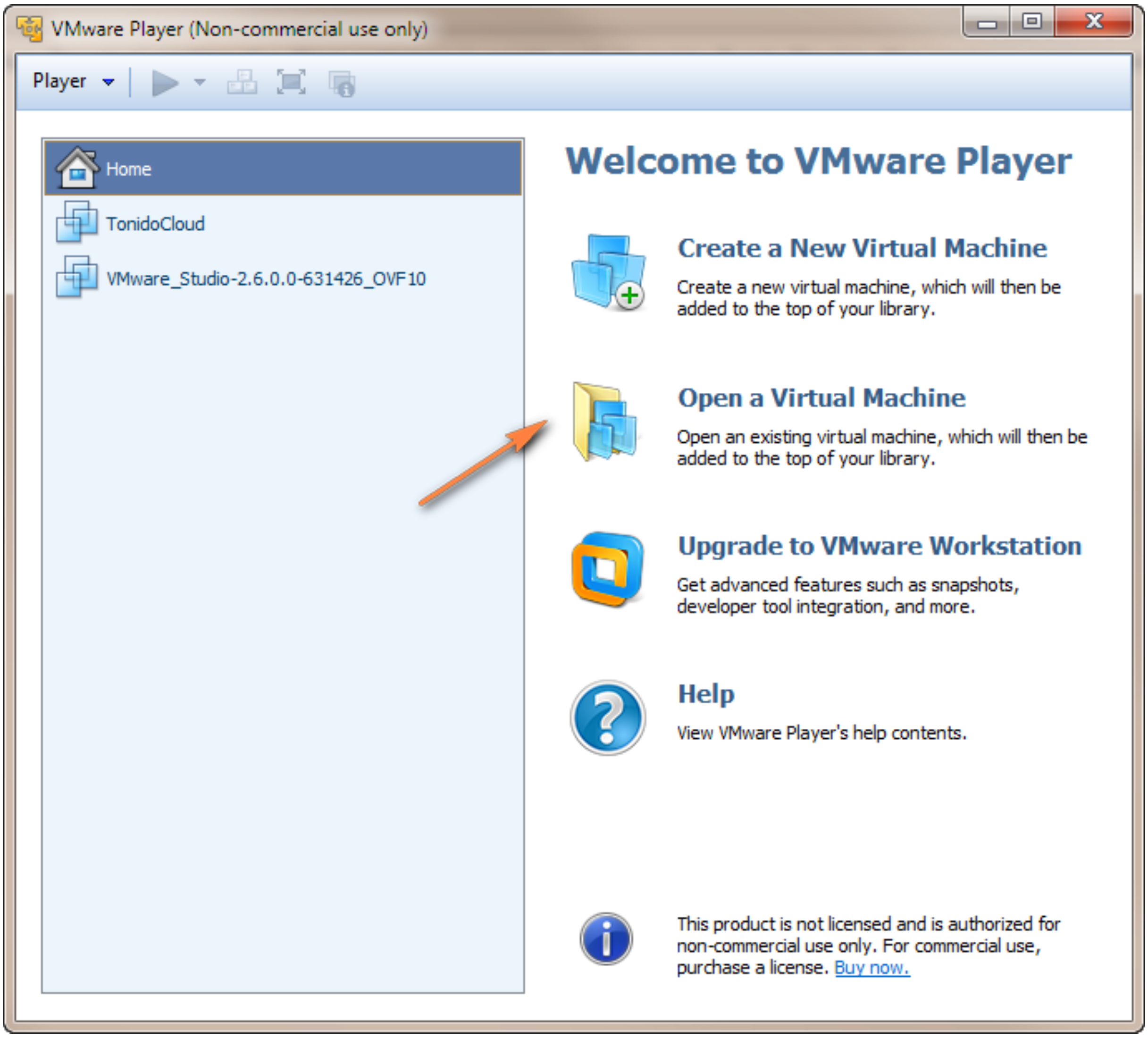
- Unload the multiextent module

```
#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.



VMware Player (Non-commercial use only)
Player
Home
TonidoCloud
VMware_Studio-2.6.0.0-631426_OVF10

Welcome to VMware Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

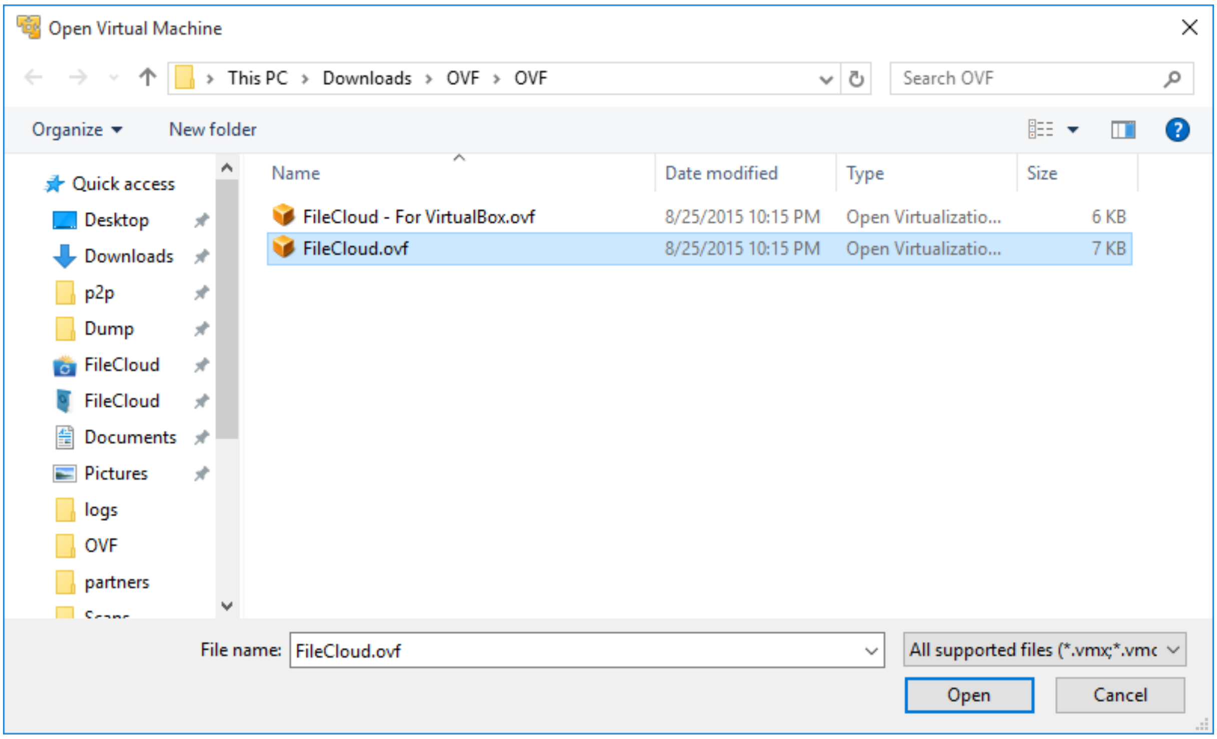
Upgrade to VMware Workstation

Get advanced features such as snapshots, developer tool integration, and more.

Help

View VMware Player's help contents.

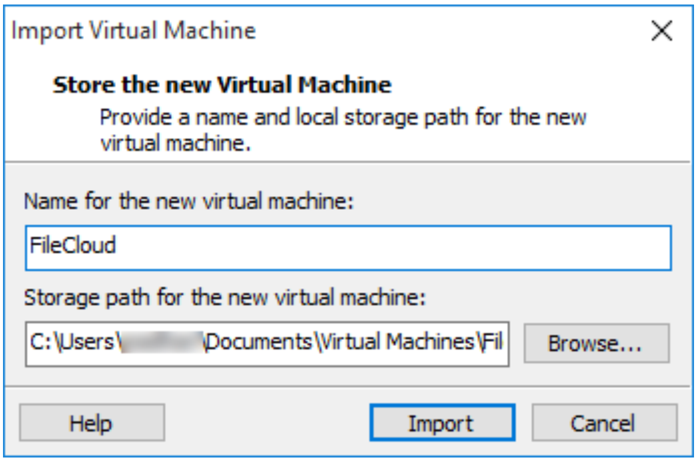
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.



Name	Date modified	Type	Size
FileCloud - For VirtualBox.ovf	8/25/2015 10:15 PM	Open Virtualizatio...	6 KB
FileCloud.ovf	8/25/2015 10:15 PM	Open Virtualizatio...	7 KB

File name: FileCloud.ovf

All supported files (*.vmx;*.vmc



Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: FileCloud

Storage path for the new virtual machine: C:\Users\[redacted]\Documents\Virtual Machines\Fil

Microsoft Azure Installation

FileCloud Virtual Machine is currently available via Azure Marketplace[9].

Using FileCloud VM on Azure, you can host your own file share sync and mobile access solution for your organization. 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[10]depending on

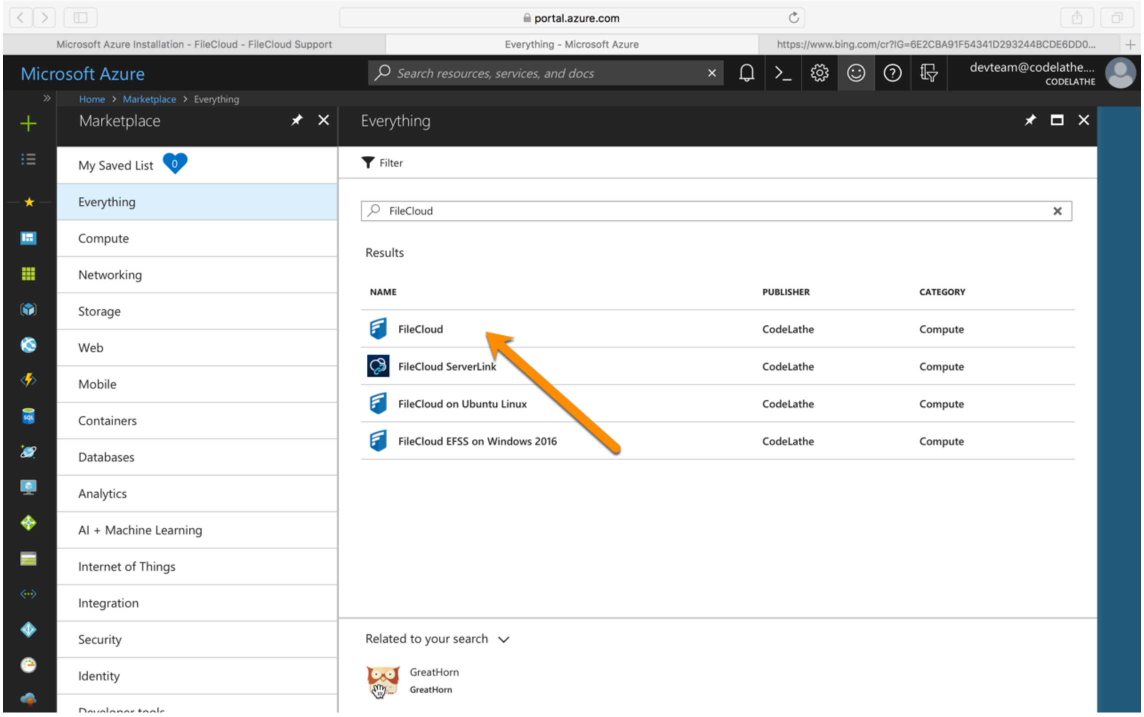
[9] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/codelathe.codelathe-filecloud-win2012r2?tab=Overviewe-filecloud-win2012r2/

[10] https://msdn.microsoft.com/en-us/library/azure/dn167006.aspx

your requirements. We recommend you take periodic snapshots of your running instance for disaster recovery.

Steps To Launch FileCloud Virtual Machine on Azure

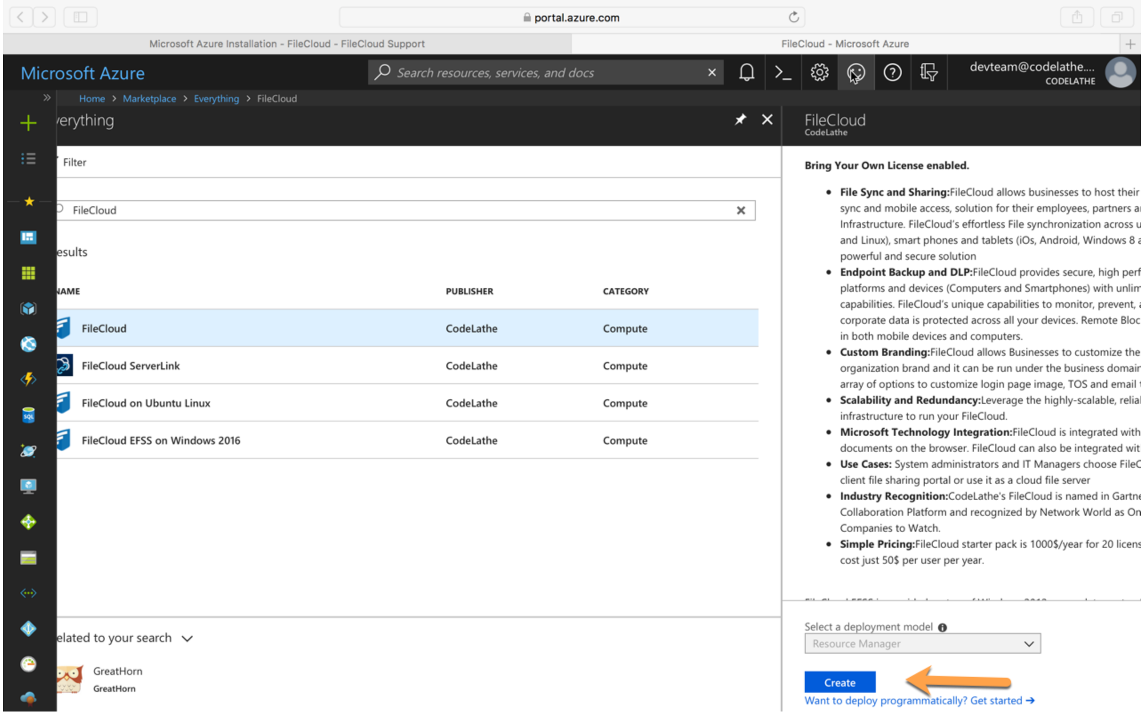
1. Login to https://portal.azure.com using your azure account. Upon successful login, go to Home>> Marketplace >> Everything. Search for FileCloud.



FileCloud

NAME	PUBLISHER	CATEGORY
FileCloud	CodeLathe	Compute
FileCloud ServerLink	CodeLathe	Compute
FileCloud on Ubuntu Linux	CodeLathe	Compute
FileCloud EFSS on Windows 2016	CodeLathe	Compute

2. Select FileCloud and Click Create


portal.azure.com
Microsoft Azure Installation - FileCloud - FileCloud Support
FileCloud - Microsoft Azure
Microsoft Azure
Search resources, services, and docs
devteam@codelathe....
CODELATHE
Home > Marketplace > Everything > FileCloud
verything
Filter
FileCloud
esults
elated to your search
GreatHorn
GreatHorn

NAME	PUBLISHER	CATEGORY
FileCloud	CodeLathe	Compute
FileCloud ServerLink	CodeLathe	Compute
FileCloud on Ubuntu Linux	CodeLathe	Compute
FileCloud EFSS on Windows 2016	CodeLathe	Compute

FileCloud
CodeLathe

Bring Your Own License enabled.

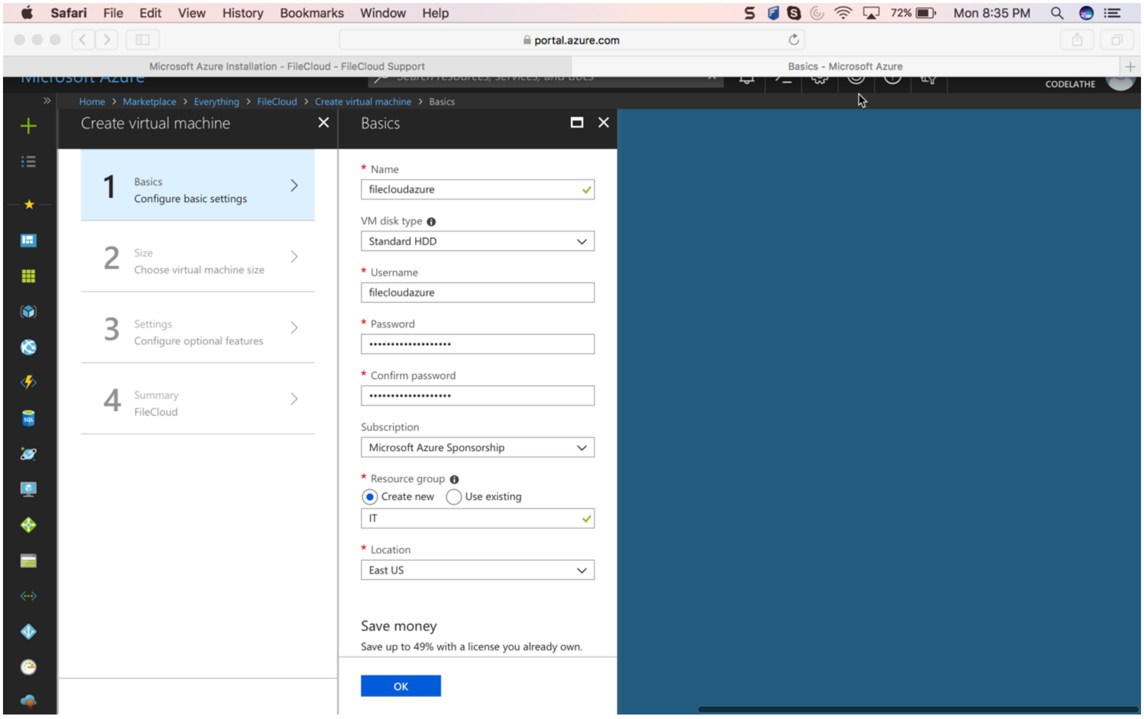
- **File Sync and Sharing:**FileCloud allows businesses to host their sync and mobile access, solution for their employees, partners a Infrastructure. FileCloud's effortless File synchronization across u and Linux), smart phones and tablets (iOs, Android, Windows 8 a powerful and secure solution
- **Endpoint Backup and DLP:**FileCloud provides secure, high perf platforms and devices (Computers and Smartphones) with unlim capabilities. FileCloud's unique capabilities to monitor, prevent, a corporate data is protected across all your devices. Remote Bloc in both mobile devices and computers.
- **Custom Branding:**FileCloud allows Businesses to customize the organization brand and it can be run under the business domair array of options to customize login page image, TOS and email t
- **Scalability and Redundancy:**Leverage the highly-scalable, relial infrastructure to run your FileCloud.
- **Microsoft Technology Integration:**FileCloud is integrated with documents on the browser. FileCloud can also be integrated wit
- **Use Cases:** System administrators and IT Managers choose FileC client file sharing portal or use it as a cloud file server
- **Industry Recognition:**CodeLathe's FileCloud is named in Gartne Collaboration Platform and recognized by Network World as On Companies to Watch.
- **Simple Pricing:**FileCloud starter pack is 1000$/year for 20 licens cost just 50$ per user per year.

Select a deployment model: Resource Manager

Create

Want to deploy programmatically? Get started →

3. Configure Basic Settings: Choose your Windows VM name, user name, password, subscription, resource group[11]and the azure data center location. Once you complete the information click OK.


Safari File Edit View History Bookmarks Window Help
72%
Mon 8:35 PM
portal.azure.com
Microsoft Azure Installation - FileCloud - FileCloud Support
Basics - Microsoft Azure
CODELATHE
Home > Marketplace > Everything > FileCloud > Create virtual machine > Basics

Create virtual machine

1 Basics — Configure basic settings
2 Size — Choose virtual machine size
3 Settings — Configure optional features
4 Summary — FileCloud

Basics

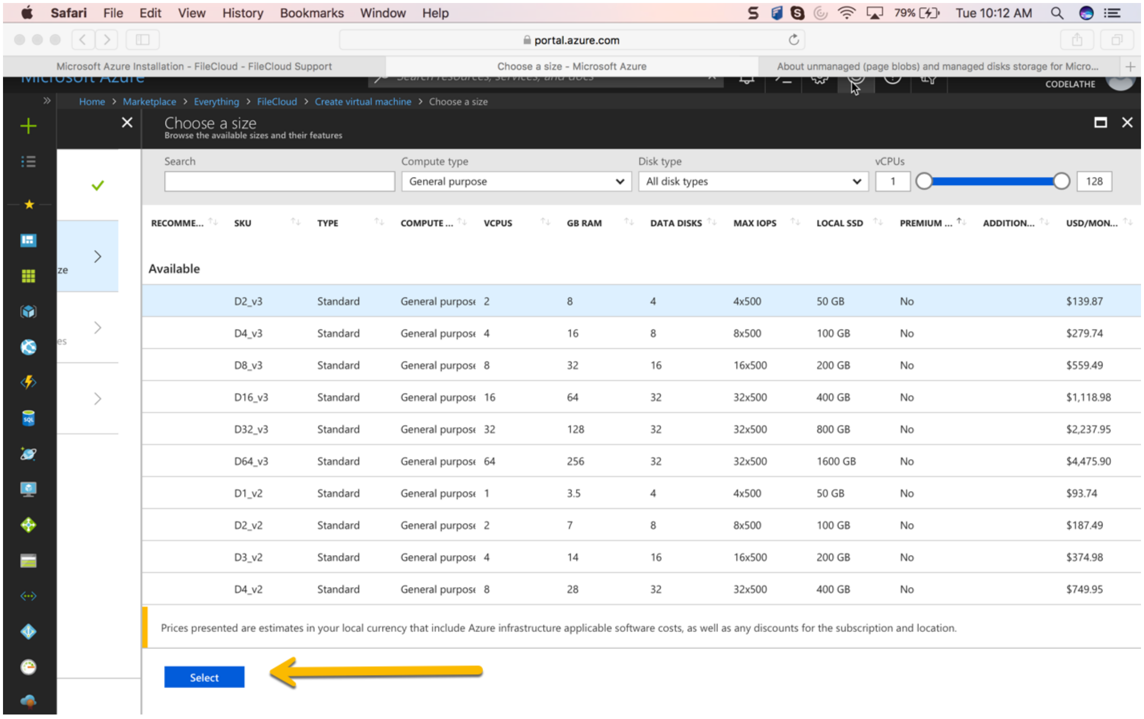
- * Name: filecloudazure
- VM disk type: Standard HDD
- * Username: filecloudazure
- * Password: ••••••••••••••••••••
- * Confirm password: ••••••••••••••••••••
- Subscription: Microsoft Azure Sponsorship
- * Resource group: ● Create new ○ Use existing — IT
- * Location: East US

Save money
Save up to 49% with a license you already own.

OK

[11] https://azure.microsoft.com/en-us/documentation/articles/resource-group-portal/

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



Safari File Edit View History Bookmarks Window Help
79% Tue 10:12 AM
portal.azure.com
Microsoft Azure Installation - FileCloud - FileCloud Support
Choose a size - Microsoft Azure
About unmanaged (page blobs) and managed disks storage for Micro...
CODELATHE
Home > Marketplace > Everything > FileCloud > Create virtual machine > Choose a size

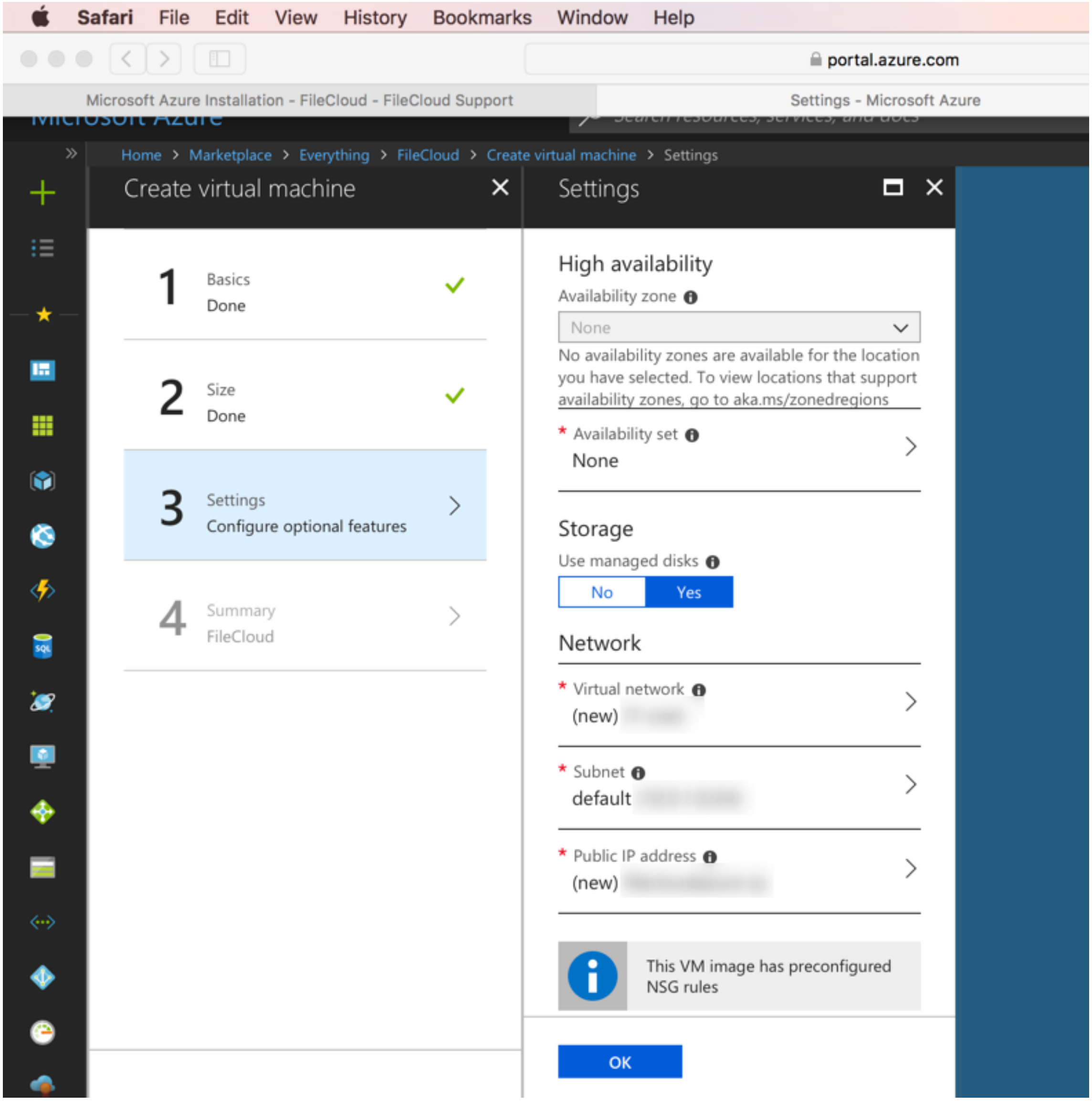
Choose a size
Browse the available sizes and their features

Search:
Compute type: General purpose
Disk type: All disk types
vCPUs: 1 – 128

RECOMME...	SKU	TYPE	COMPUTE ...	VCPUS	GB RAM	DATA DISKS	MAX IOPS	LOCAL SSD	PREMIUM ...	ADDITION...	USD/MON...
Available											
	D2_v3	Standard	General purpose	2	8	4	4x500	50 GB	No		$139.87
	D4_v3	Standard	General purpose	4	16	8	8x500	100 GB	No		$279.74
	D8_v3	Standard	General purpose	8	32	16	16x500	200 GB	No		$559.49
	D16_v3	Standard	General purpose	16	64	32	32x500	400 GB	No		$1,118.98
	D32_v3	Standard	General purpose	32	128	32	32x500	800 GB	No		$2,237.95
	D64_v3	Standard	General purpose	64	256	32	32x500	1600 GB	No		$4,475.90
	D1_v2	Standard	General purpose	1	3.5	4	4x500	50 GB	No		$93.74
	D2_v2	Standard	General purpose	2	7	8	8x500	100 GB	No		$187.49
	D3_v2	Standard	General purpose	4	14	16	16x500	200 GB	No		$374.98
	D4_v2	Standard	General purpose	8	28	32	32x500	400 GB	No		$749.95

Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location.

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


Safari File Edit View History Bookmarks Window Help
portal.azure.com
Microsoft Azure Installation - FileCloud - FileCloud Support
Settings - Microsoft Azure
Microsoft Azure
Search resources, services, and docs
Home > Marketplace > Everything > FileCloud > Create virtual machine > Settings

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features

4 Summary FileCloud

Settings

High availability

Availability zone: None

No availability zones are available for the location you have selected. To view locations that support availability zones, go to aka.ms/zonedregions

* Availability set: None

Storage

Use managed disks: No [✓ Yes]

Network

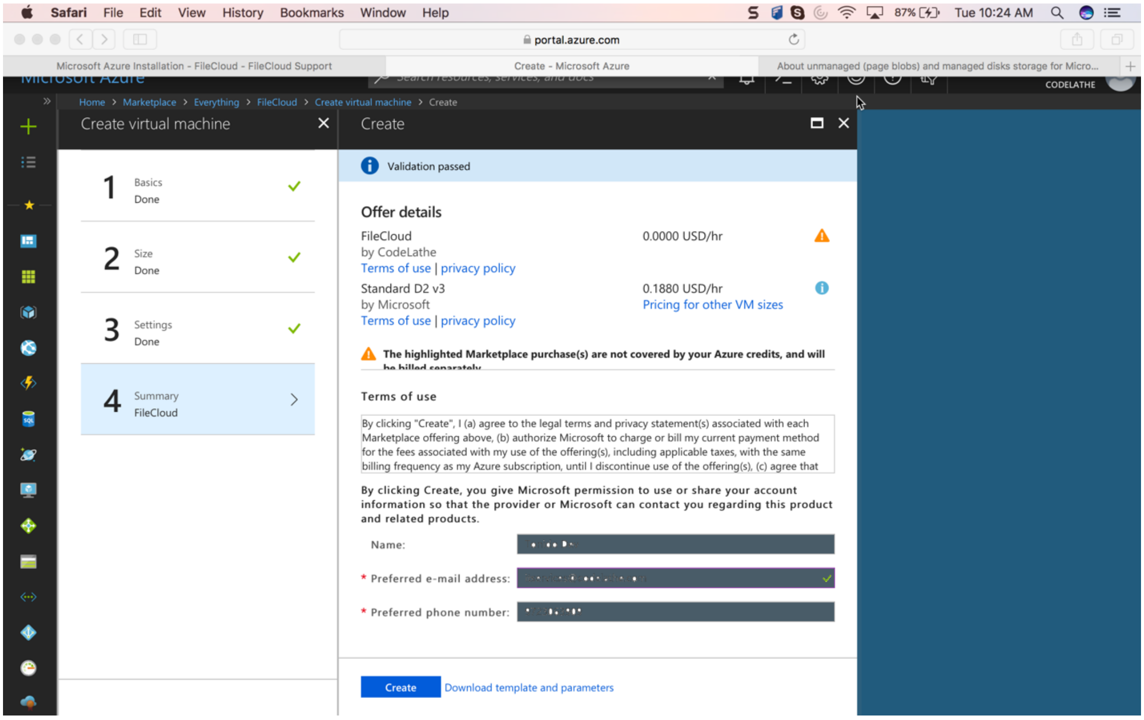
* Virtual network: (new) [redacted]

* Subnet: default [redacted]

* Public IP address: (new) [redacted]

This VM image has preconfigured NSG rules

6. Verify your offer details and click Create.



Microsoft Azure Installation - FileCloud - FileCloud Support | Create - Microsoft Azure | About unmanaged (page blobs) and managed disks storage for Micro...

Home > Marketplace > Everything > FileCloud > Create virtual machine > Create

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Done ✓

4 Summary FileCloud

Create

Validation passed

Offer details

FileCloud by CodeLathe Terms of use | privacy policy	0.0000 USD/hr	⚠
Standard D2 v3 by Microsoft Terms of use | privacy policy	0.1880 USD/hr Pricing for other VM sizes	ⓘ

⚠ The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately

Terms of use

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), (c) agree that

By clicking Create, you give Microsoft permission to use or share your account information so that the provider or Microsoft can contact you regarding this product and related products.

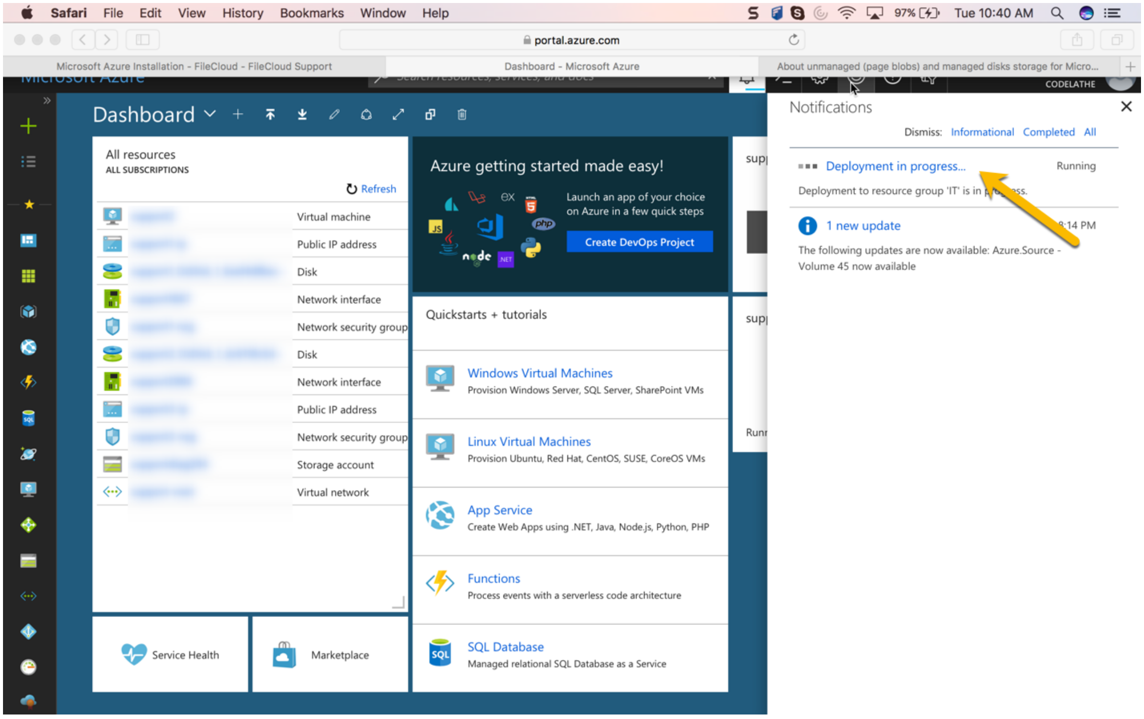
Name: [redacted]

* Preferred e-mail address: [redacted]

* Preferred phone number: [redacted]

Note: FileCloud is offered under Bring your Own License Model. You can get FileCloud trial license by registering in our customer portal[12].

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



Microsoft Azure Installation - FileCloud - FileCloud Support | Dashboard - Microsoft Azure | About unmanaged (page blobs) and managed disks storage for Micro...

Dashboard

All resources
ALL SUBSCRIPTIONS

Refresh

[redacted]	Virtual machine
[redacted]	Public IP address
[redacted]	Disk
[redacted]	Network interface
[redacted]	Network security group
[redacted]	Disk
[redacted]	Network interface
[redacted]	Public IP address
[redacted]	Network security group
[redacted]	Storage account
[redacted]	Virtual network

Azure getting started made easy!

Launch an app of your choice on Azure in a few quick steps

Quickstarts + tutorials

Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP

Functions
Process events with a serverless code architecture

SQL Database
Managed relational SQL Database as a Service

Notifications

Dismiss: Informational Completed All

Deployment in progress... Running

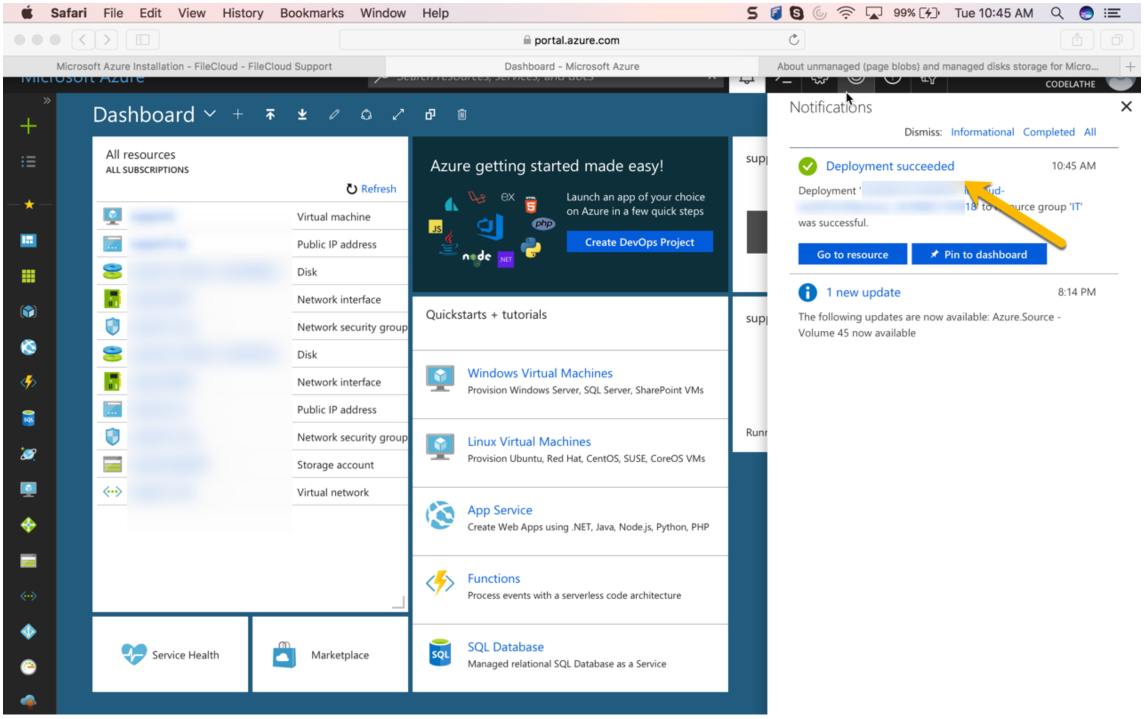
Deployment to resource group 'IT' is in progress.

1 new update 8:14 PM

The following updates are now available: Azure.Source - Volume 45 now available

[12] https://portal.getfilecloud.com/ui/user/index.html

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



Safari File Edit View History Bookmarks Window Help
99% Tue 10:45 AM
portal.azure.com
Microsoft Azure Installation - FileCloud - FileCloud Support
Dashboard - Microsoft Azure
About unmanaged (page blobs) and managed disks storage for Micro...
CODELATHE
Dashboard
All resources
ALL SUBSCRIPTIONS
Refresh
Virtual machine
Public IP address
Disk
Network interface
Network security group
Disk
Network interface
Public IP address
Network security group
Storage account
Virtual network
Azure getting started made easy!
Launch an app of your choice on Azure in a few quick steps
Create DevOps Project
Quickstarts + tutorials
Windows Virtual Machines
Provision Windows Server, SQL Server, SharePoint VMs
Linux Virtual Machines
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs
App Service
Create Web Apps using .NET, Java, Node.js, Python, PHP
Functions
Process events with a serverless code architecture
SQL Database
Managed relational SQL Database as a Service
Service Health
Marketplace
Notifications
Dismiss: Informational Completed All
Go to resource
Pin to dashboard

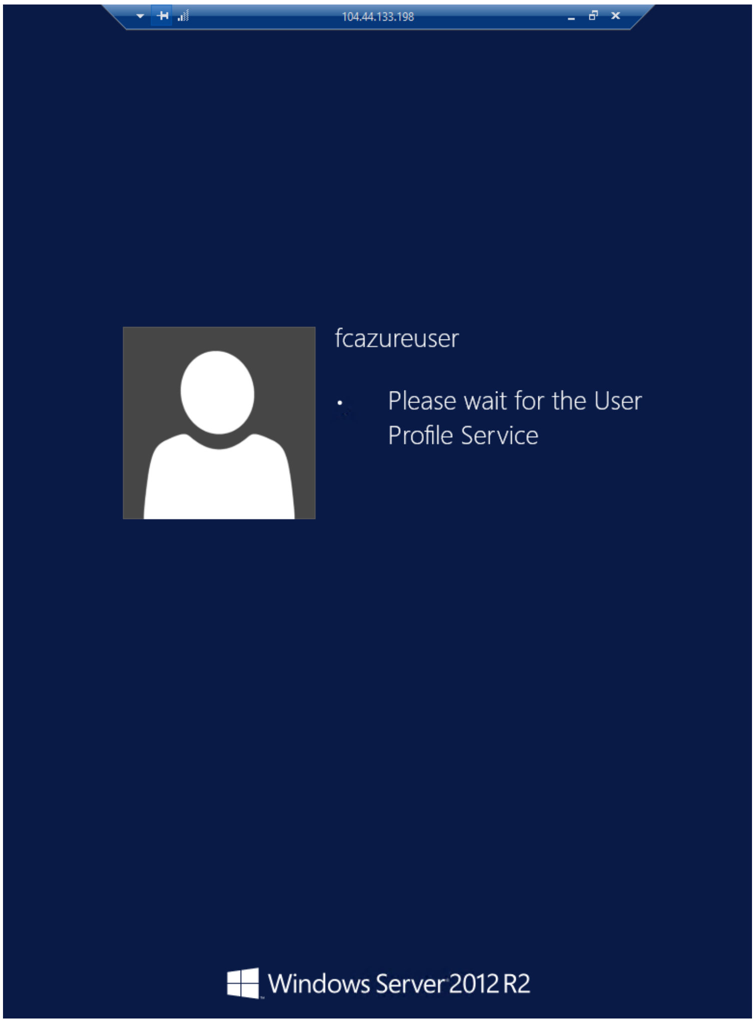
Deployment succeeded 10:45 AM

Deployment '[redacted]' to resource group 'IT' was successful.

1 new update 8:14 PM

The following updates are now available: Azure.Source - Volume 45 now available

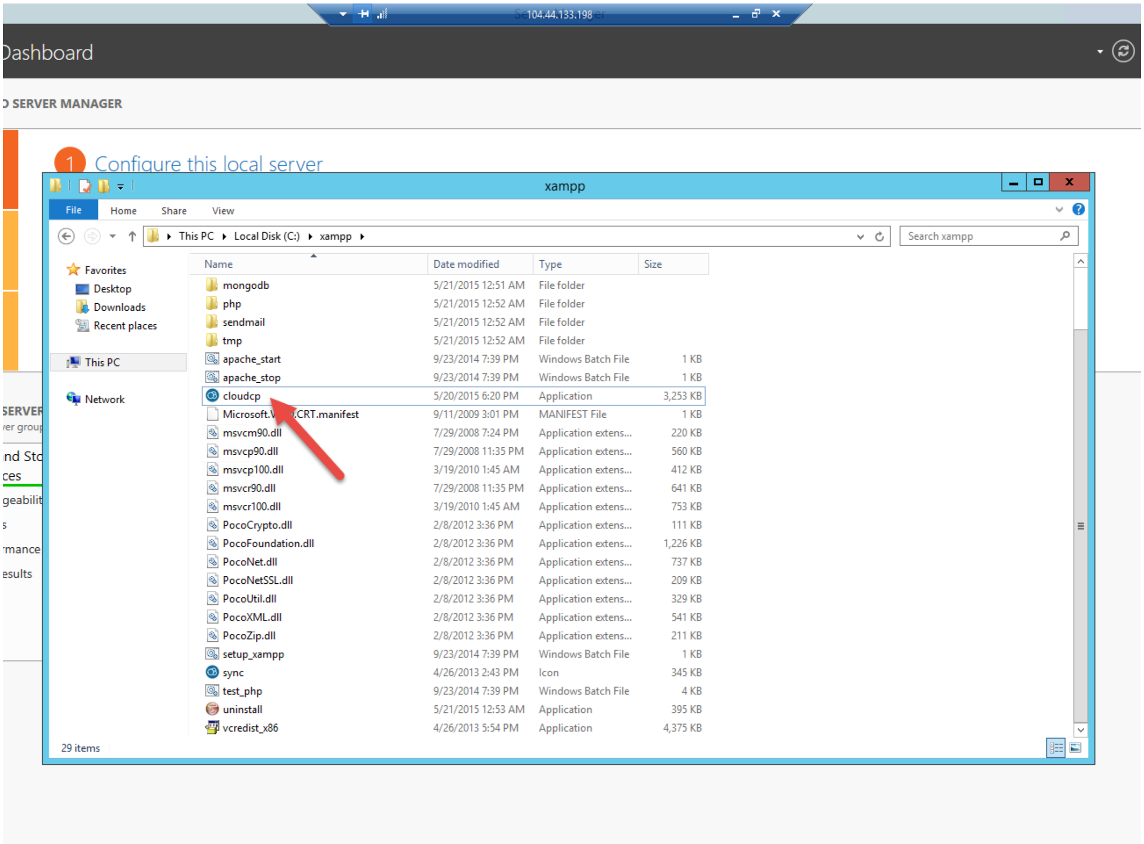
9. Connect to your FileCloud VM instance using RDP connection.



fcazureuser

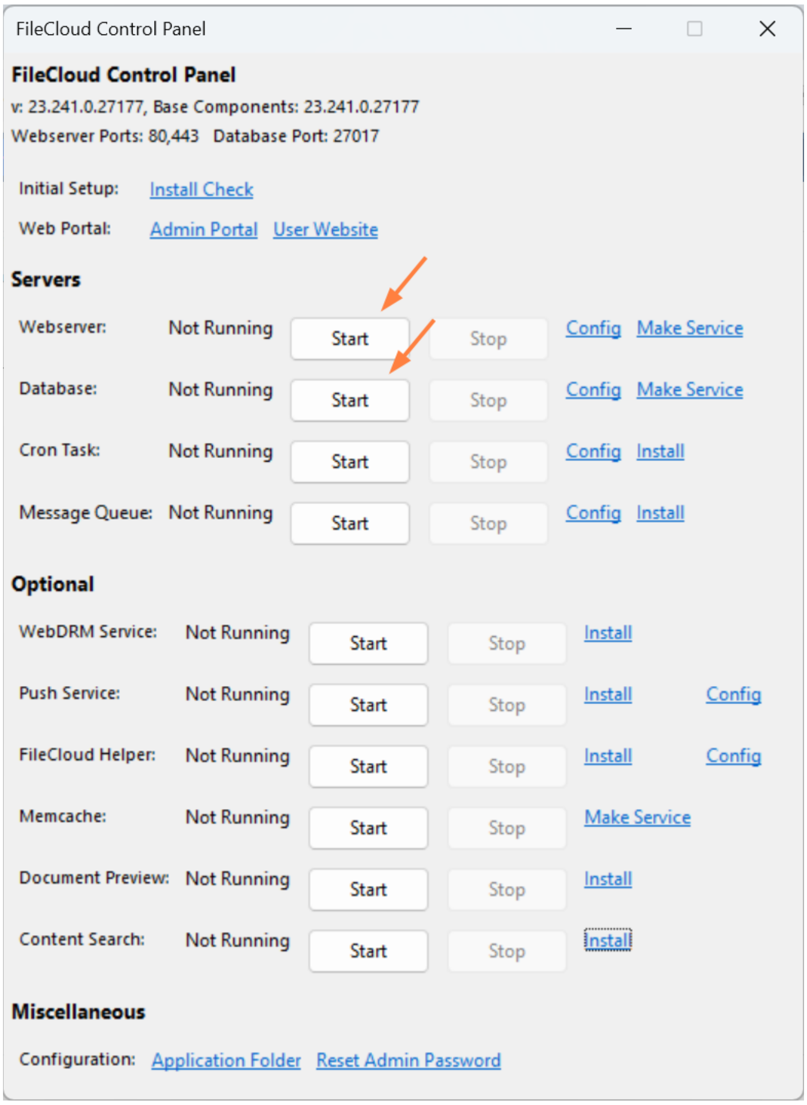
Please wait for the User Profile Service

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



Name	Date modified	Type	Size
mongodb	5/21/2015 12:51 AM	File folder	
php	5/21/2015 12:52 AM	File folder	
sendmail	5/21/2015 12:52 AM	File folder	
tmp	5/21/2015 12:52 AM	File folder	
apache_start	9/23/2014 7:39 PM	Windows Batch File	1 KB
apache_stop	9/23/2014 7:39 PM	Windows Batch File	1 KB
cloudcp	5/20/2015 6:20 PM	Application	3,253 KB
Microsoft.V[illegible].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
PocoNet.dll	2/8/2012 3:36 PM	Application extens...	737 KB
PocoNetSSL.dll	2/8/2012 3:36 PM	Application extens...	209 KB
PocoUtil.dll	2/8/2012 3:36 PM	Application extens...	329 KB
PocoXML.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	Icon	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

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



FileCloud Control Panel

FileCloud Control Panel

v: 23.241.0.27177, Base Components: 23.241.0.27177

Webserver Ports: 80,443   Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

Webserver:	Not Running	Start	Stop	Config	Make Service
Database:	Not Running	Start	Stop	Config	Make Service
Cron Task:	Not Running	Start	Stop	Config	Install
Message Queue:	Not Running	Start	Stop	Config	Install

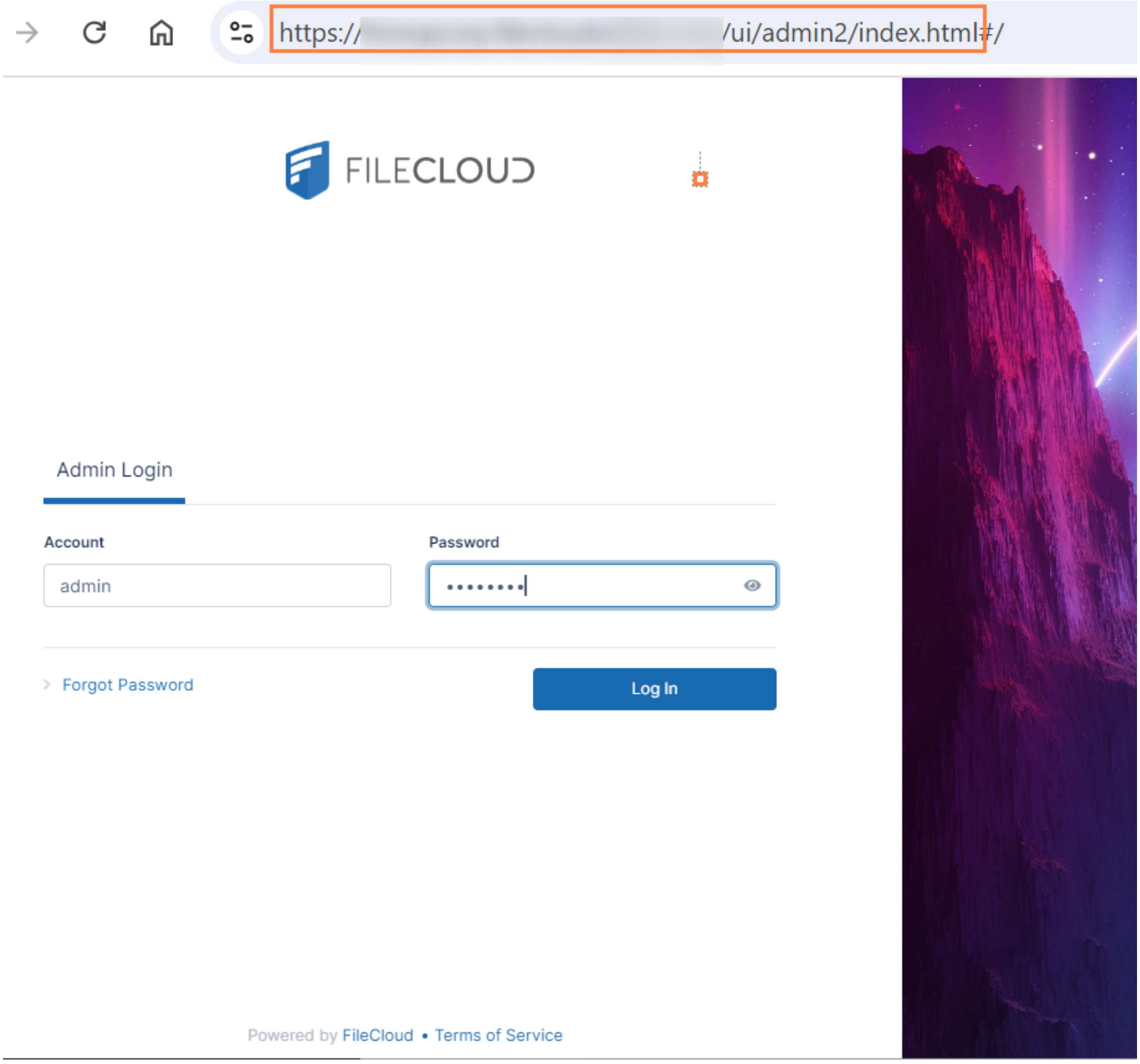
Optional

WebDRM Service:	Not Running	Start	Stop	Install	
Push Service:	Not Running	Start	Stop	Install	Config
FileCloud Helper:	Not Running	Start	Stop	Install	Config
Memcache:	Not Running	Start	Stop	Make Service	
Document Preview:	Not Running	Start	Stop	Install	
Content Search:	Not Running	Start	Stop	Install	

Miscellaneous

Configuration: Application Folder Reset Admin Password

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".



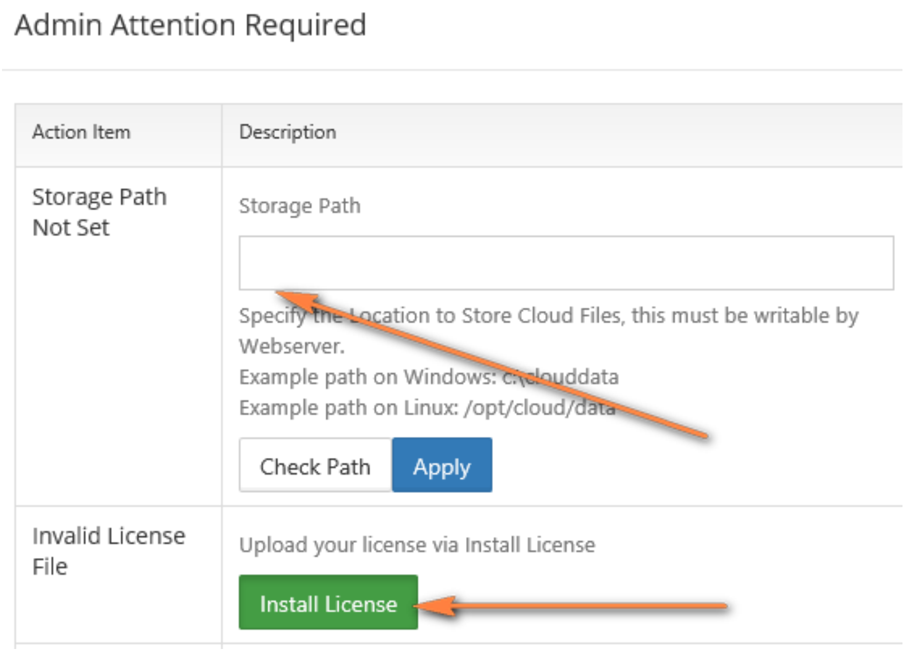
https://[redacted]/ui/admin2/index.html#/

Admin Login

Account: admin

Password: ••••••••

13. Upon successful login, set the storage path for your files and install the trial license you have got from FileCloud customer portal (see page 28).



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
Invalid License File	Upload your license via Install License Install License

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

FileCloud Integration with Azure File Storage

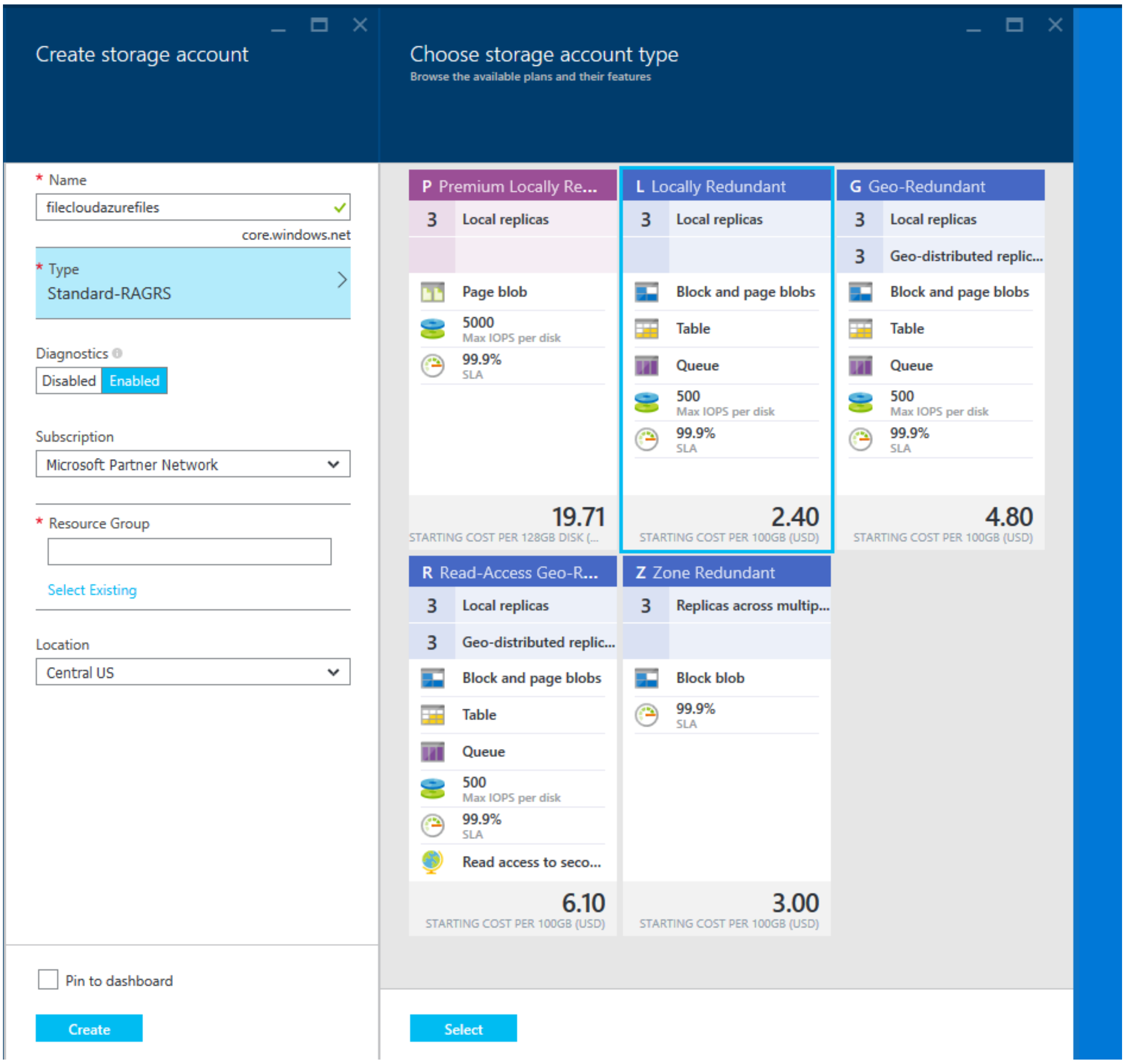
Azure File storage[13]offers file shares in the Azure Cloud using standard SAMBA protocol (SMB 3.0). FileCloud running on Azure VMs can mount the file shares created on Azure Files storage and use it as a main storage path for FileCloud. You can also use the same fileshare to store the MongoDB data files. 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 a few million files successfully. This configuration gives the scalability and data redundancy without a 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 named the storage account **filecloudazurefiles**, and chosen a locally redundant storage account type. We recommend you choose the same location the where FileCloud VM is located.

[13] https://azure.microsoft.com/en-us/services/storage/files/



Create storage account

* Name: filecloudazurefiles .core.windows.net

* Type: Standard-RAGRS

Diagnostics: Disabled [✓ Enabled]

Subscription: Microsoft Partner Network

* Resource Group:

Select Existing

Location: Central US

□ Pin to dashboard

Create

Choose storage account type

Browse the available plans and their features

P Premium Locally Re...
3 Local replicas
Page blob
5000 Max IOPS per disk
99.9% SLA
19.71 STARTING COST PER 128GB DISK (...

L Locally Redundant
3 Local replicas
Block and page blobs
Table
Queue
500 Max IOPS per disk
99.9% SLA
2.40 STARTING COST PER 100GB (USD)

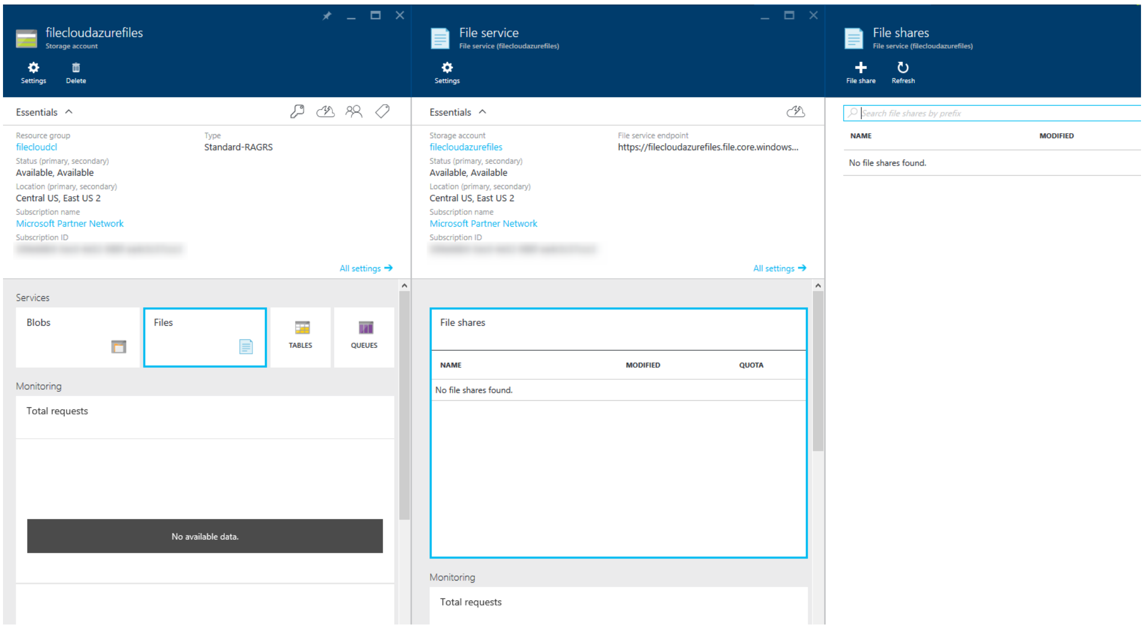
G Geo-Redundant
3 Local replicas
3 Geo-distributed replic...
Block and page blobs
Table
Queue
500 Max IOPS per disk
99.9% SLA
4.80 STARTING COST PER 100GB (USD)

R Read-Access Geo-R...
3 Local replicas
3 Geo-distributed replic...
Block and page blobs
Table
Queue
500 Max IOPS per disk
99.9% SLA
Read access to seco...
6.10 STARTING COST PER 100GB (USD)

Z Zone Redundant
3 Replicas across multip...
Block blob
99.9% SLA
3.00 STARTING COST PER 100GB (USD)

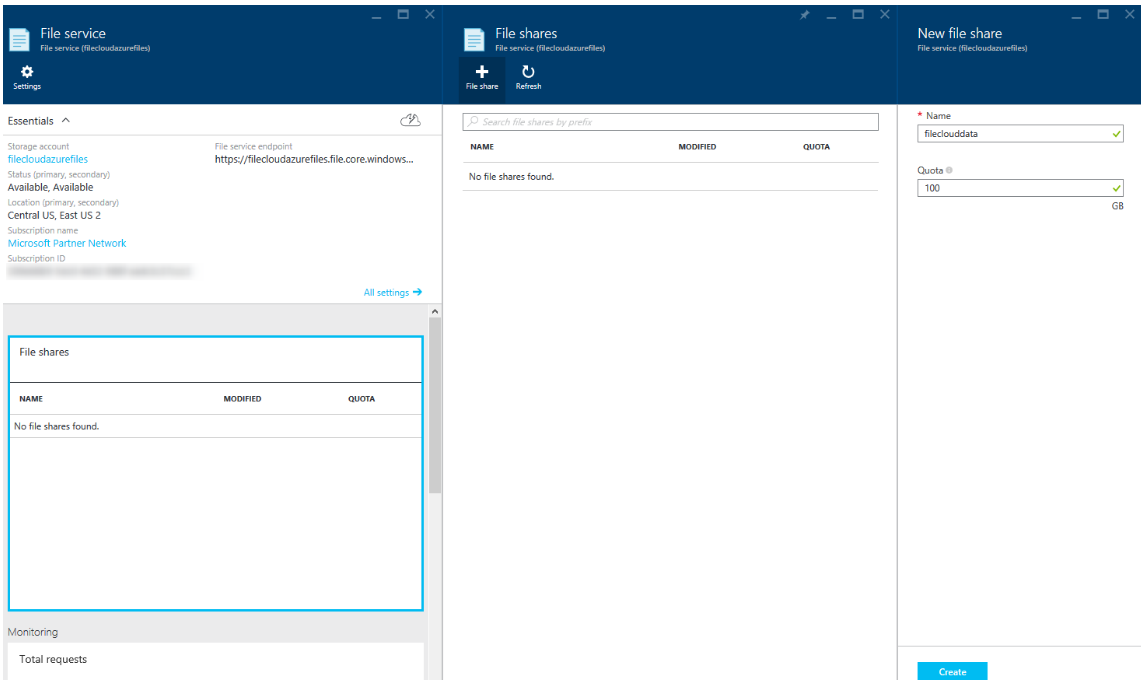
Select

2. Create a file share under your storage account as shown below. You can also choose the storage quota. Maximum storage for a file share is 5120 GB.



Resource group: filecloudcl
Type: Standard-RAGRS
Status (primary, secondary): Available, Available
Location (primary, secondary): Central US, East US 2
Subscription name: Microsoft Partner Network
Subscription ID: [redacted]

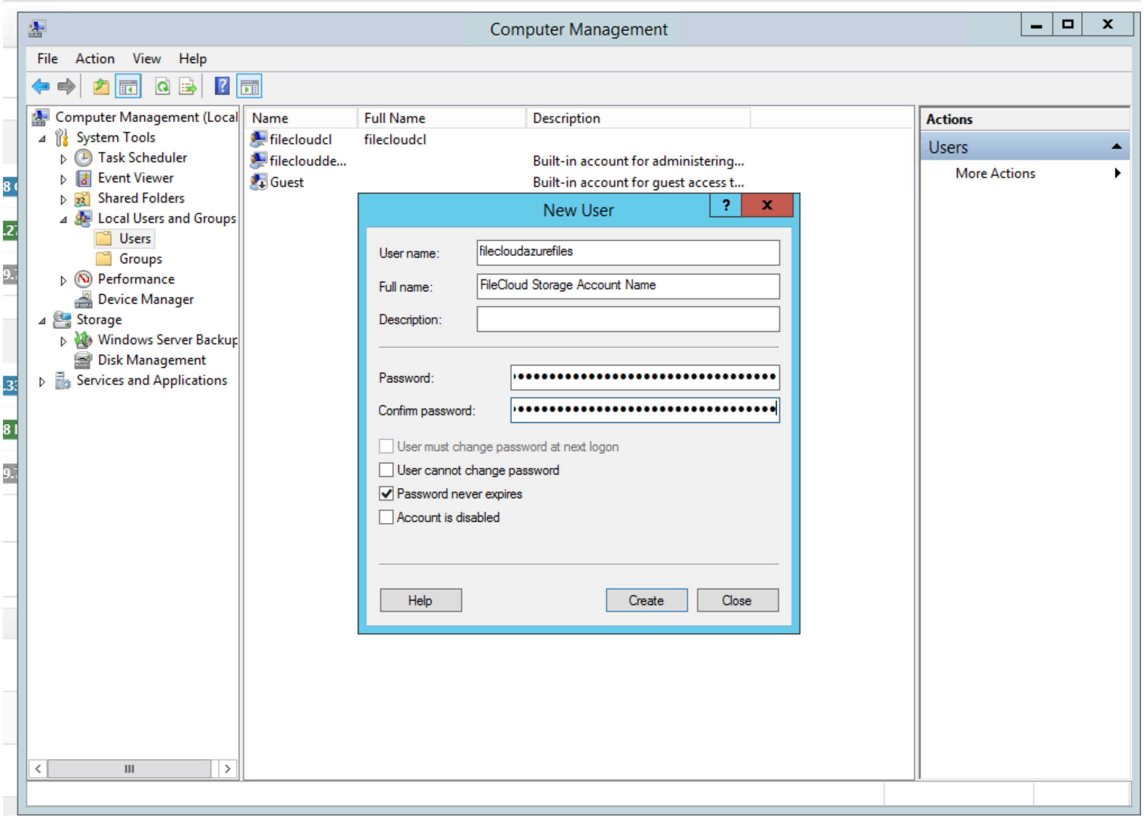
Storage account: filecloudazurefiles
File service endpoint: https://filecloudazurefiles.file.core.windows...
Status (primary, secondary): Available, Available
Location (primary, secondary): Central US, East US 2
Subscription name: Microsoft Partner Network
Subscription ID: [redacted]



Storage account: filecloudazurefiles
File service endpoint: https://filecloudazurefiles.file.core.windows...
Status (primary, secondary): Available, Available
Location (primary, secondary): Central US, East US 2
Subscription name: Microsoft Partner Network
Subscription ID: [redacted]

* Name: filecloudddata
Quota: 100 GB

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, use the access key of Azure Files Storage.



Name	Full Name	Description
filecloudcl	filecloudcl	
filecloudde...		Built-in account for administering...
Guest		Built-in account for guest access t...

New User

User name: filecloudazurefiles

Full name: FileCloud Storage Account Name

Description:

Password: ••••••••••••••••••••••••••••••••••

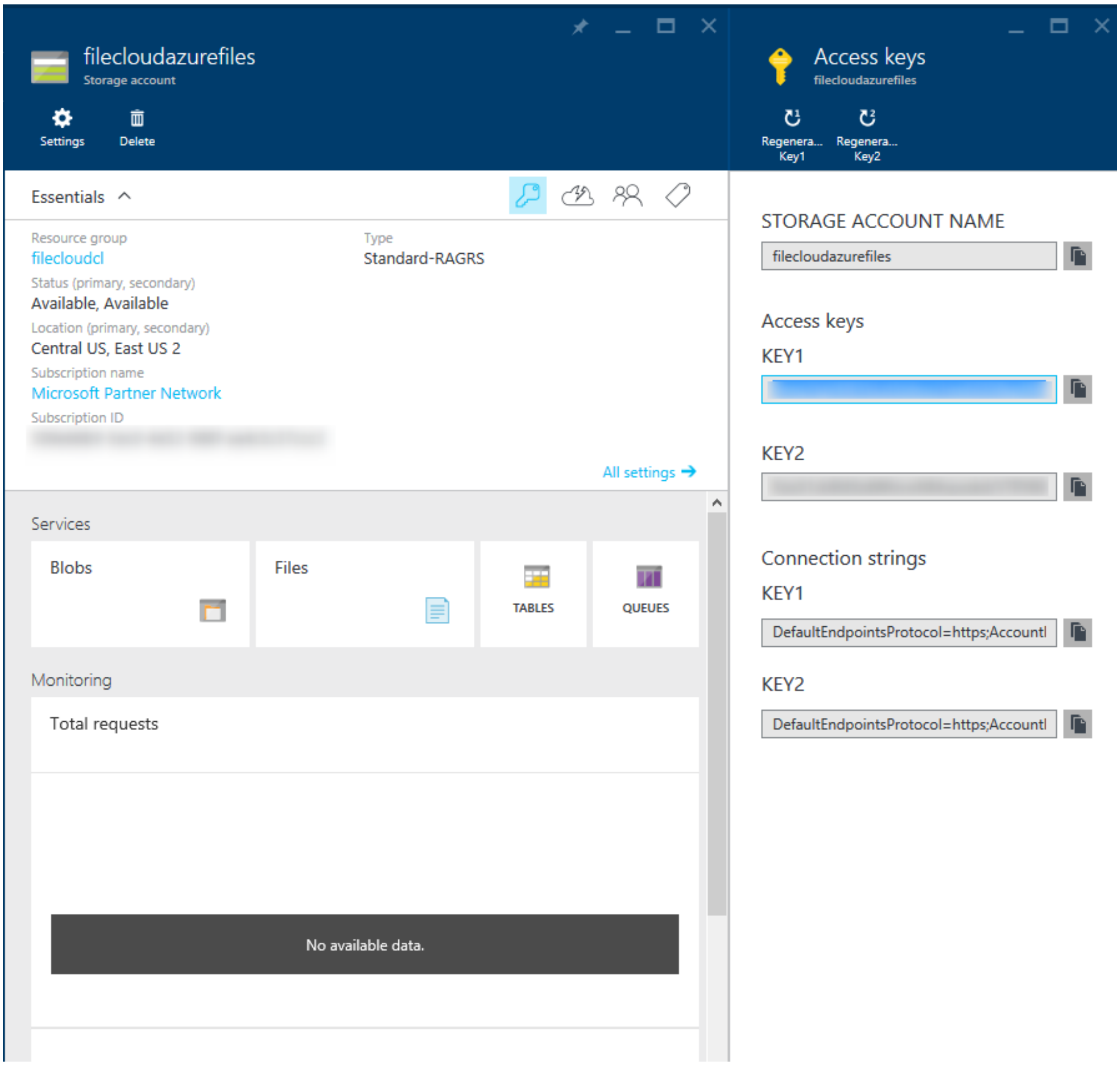
Confirm password: ••••••••••••••••••••••••••••••••••

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled



Resource group: filecloudcl

Type: Standard-RAGRS

Status (primary, secondary): Available, Available

Location (primary, secondary): Central US, East US 2

Subscription name: Microsoft Partner Network

Subscription ID: [redacted]

STORAGE ACCOUNT NAME: filecloudazurefiles

Access keys

KEY1: [redacted]

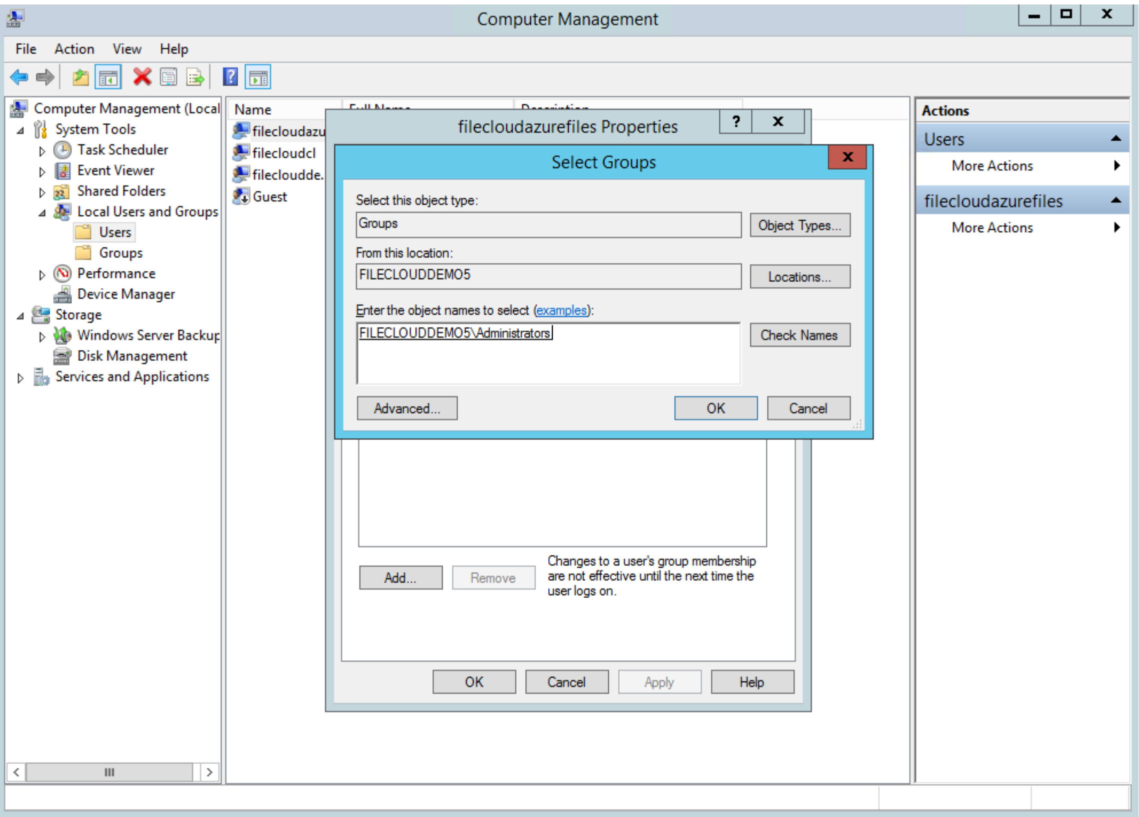
KEY2: [redacted]

Connection strings

KEY1: DefaultEndpointsProtocol=https;AccountI

KEY2: DefaultEndpointsProtocol=https;AccountI

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

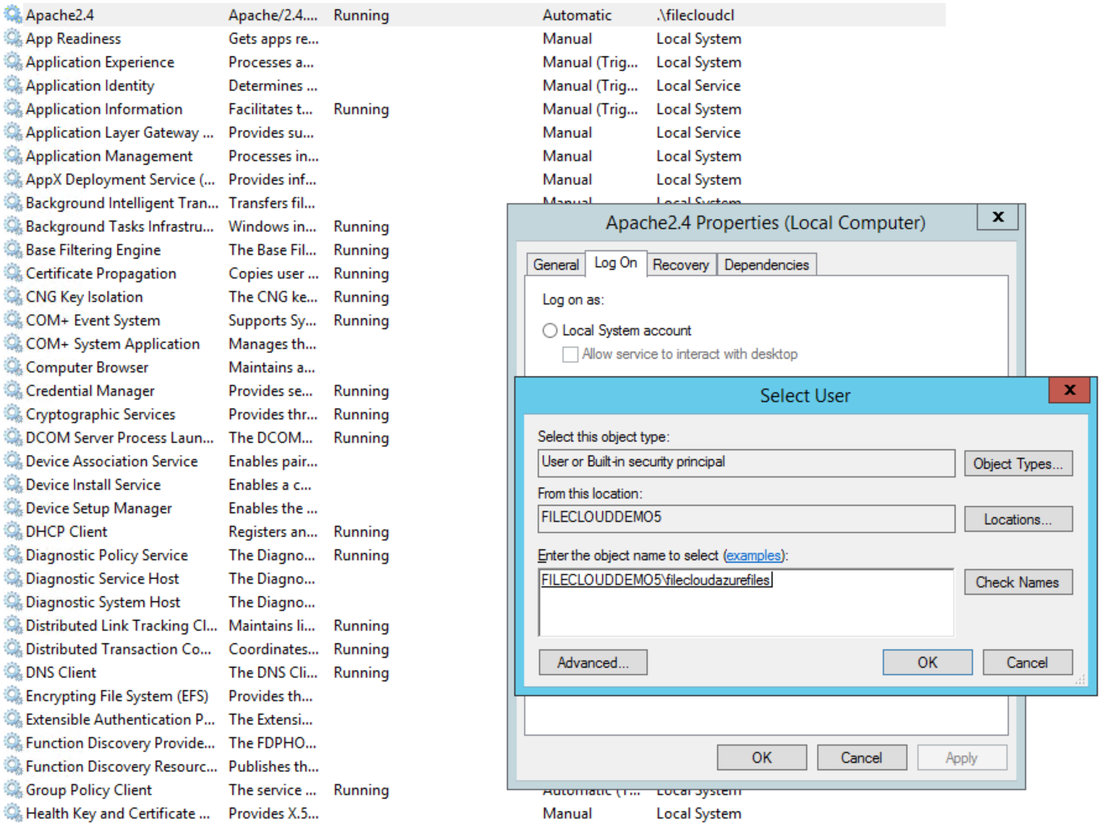


Select this object type:
Groups

From this location:
FILECLOUDDEMO5

Enter the object names to select (examples):
FILECLOUDDEMO5\Administrators

5. Run the Apache and MongoDB services using the local user account created in the previous step.
Note: We do this step for Apache and MongoDB to set 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 System
Background Tasks Infrastru...	Windows in...	Running		
Base Filtering Engine	The Base Fil...	Running		
Certificate Propagation	Copies user ...	Running		
CNG Key Isolation	The CNG ke...	Running		
COM+ Event System	Supports Sy...	Running		
COM+ System Application	Manages th...			
Computer Browser	Maintains a...			
Credential Manager	Provides se...	Running		
Cryptographic Services	Provides thr...	Running		
DCOM Server Process Laun...	The DCOM...	Running		
Device Association Service	Enables pair...			
Device Install Service	Enables a c...			
Device Setup Manager	Enables the ...			
DHCP Client	Registers an...	Running		
Diagnostic Policy Service	The Diagno...	Running		
Diagnostic Service Host	The Diagno...			
Diagnostic System Host	The Diagno...			
Distributed Link Tracking Cl...	Maintains li...	Running		
Distributed Transaction Co...	Coordinates...	Running		
DNS Client	The DNS Cli...	Running		
Encrypting File System (EFS)	Provides th...			
Extensible Authentication P...	The Extensi...			
Function Discovery Provide...	The FDPHO...			
Function Discovery Resourc...	Publishes th...			
Group Policy Client	The service ...	Running	Automatic (T...	Local System
Health Key and Certificate ...	Provides X.5...		Manual	Local System

Apache2.4 Properties (Local Computer)

Log on as:

○ Local System account

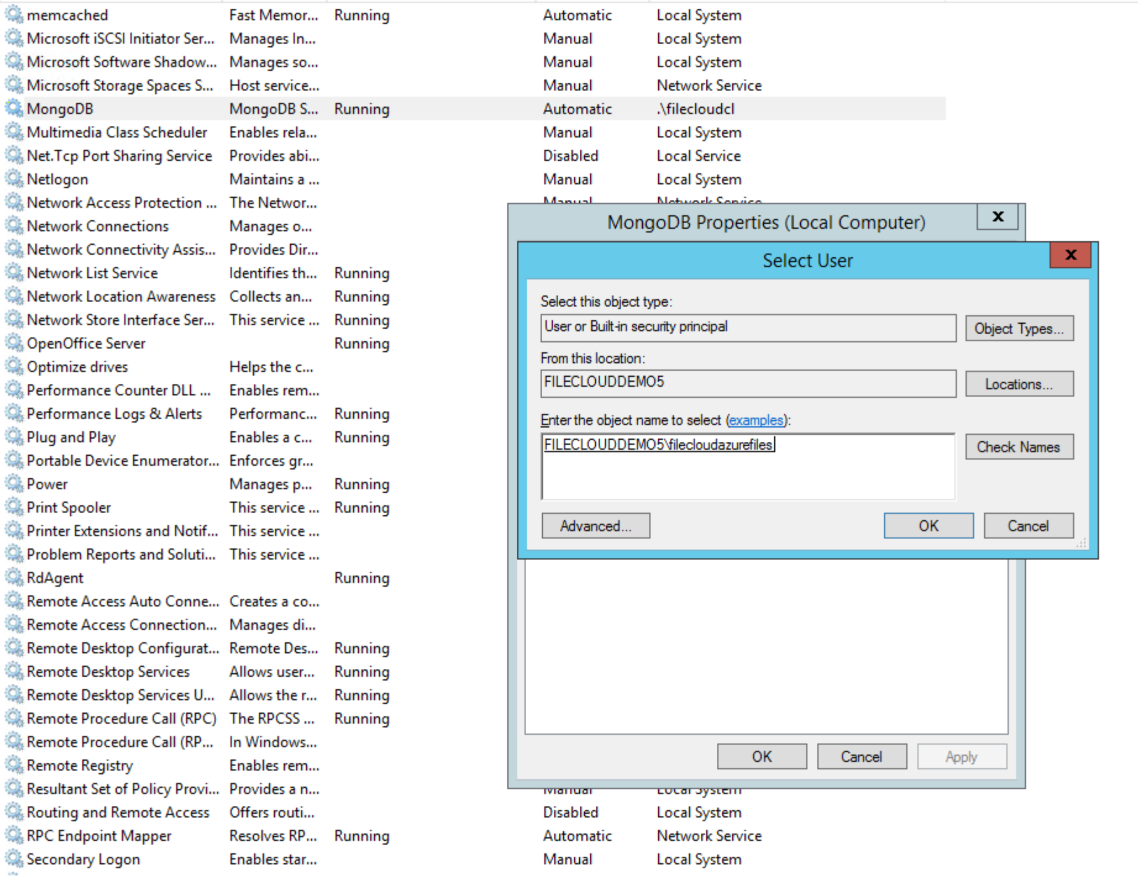
□ Allow service to interact with desktop

Select User

Select this object type:
User or Built-in security principal

From this location:
FILECLOUDDEMO5

Enter the object name to select (examples):
FILECLOUDDEMO5\filecloudazurefiles



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	Network Service
Network Connections	Manages o...			
Network Connectivity Assis...	Provides Dir...			
Network List Service	Identifies th...	Running		
Network Location Awareness	Collects an...	Running		
Network Store Interface Ser...	This service ...	Running		
OpenOffice Server		Running		
Optimize drives	Helps the c...			
Performance Counter DLL ...	Enables rem...			
Performance Logs & Alerts	Performanc...	Running		
Plug and Play	Enables a c...	Running		
Portable Device Enumerator...	Enforces gr...			
Power	Manages p...	Running		
Print Spooler	This service ...	Running		
Printer Extensions and Notif...	This service ...			
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...			
Resultant Set of Policy Provi...	Provides a n...		Manual	Local 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

MongoDB Properties (Local Computer)

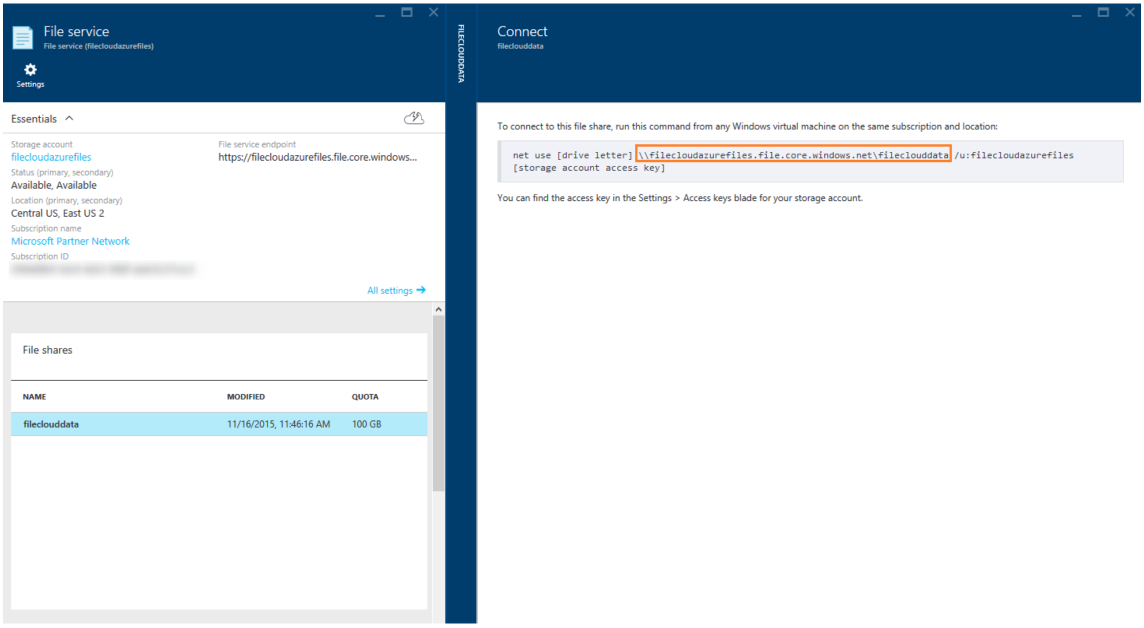
Select User

Select this object type:
User or Built-in security principal

From this location:
FILECLOUDDEMO5

Enter the object name to select (examples):
FILECLOUDDEMO5\filecloudazurefiles

6. Copy the file share path of the file share created in step 2 from the Azure Portal ("**\\*[storage account name].file.core.windows.net\[file share path name]***").



File service
File service (filecloudazurefiles)

Storage account
filecloudazurefiles

File service endpoint
https://filecloudazurefiles.file.core.windows...

Status (primary, secondary)
Available, Available

Location (primary, secondary)
Central US, East US 2

Subscription name
Microsoft Partner Network

Subscription ID
[redacted]

File shares

NAME	MODIFIED	QUOTA
fileclouddata	11/16/2015, 11:46:16 AM	100 GB

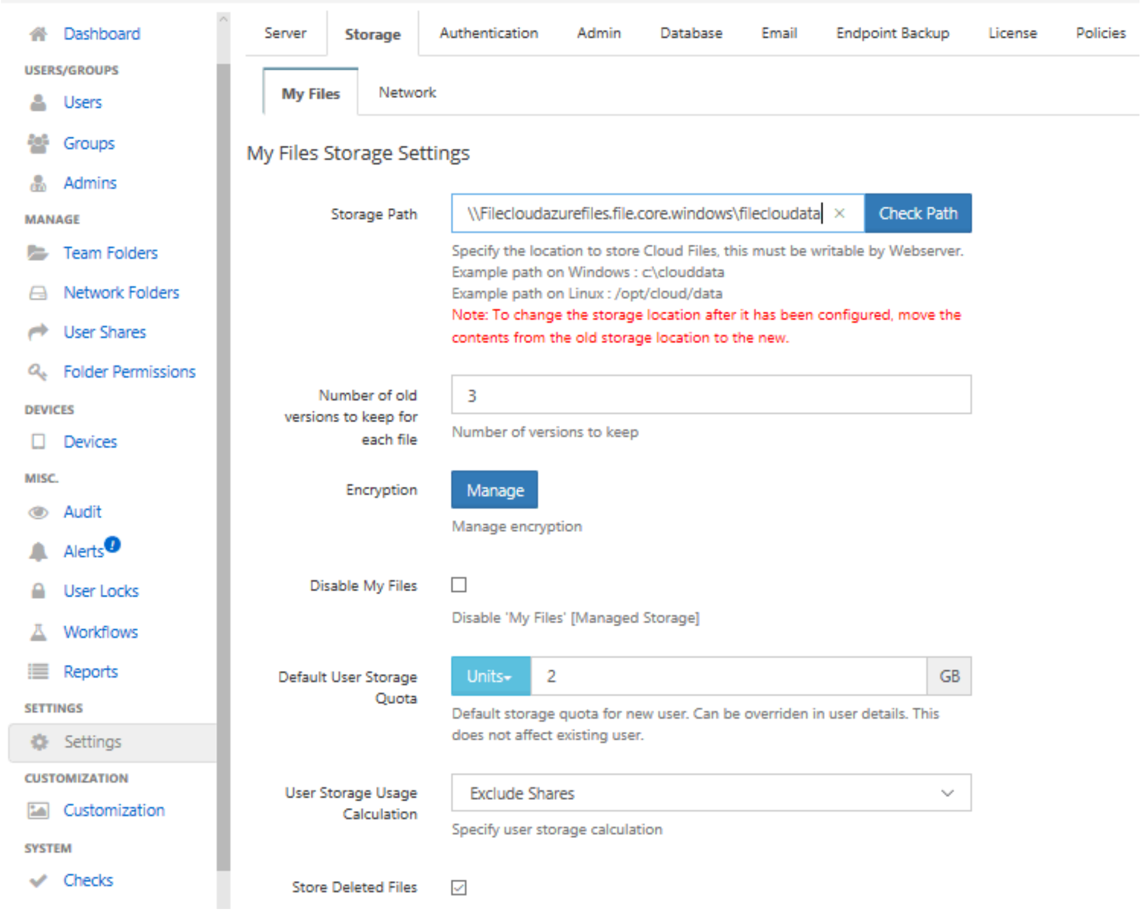
Connect
fileclouddata

To connect to this file share, run this command from any Windows virtual machine on the same subscription and location:

```
net use [drive letter] \\filecloudazurefiles.file.core.windows.net\fileclouddata /u:filecloudazurefiles
[storage account access key]
```

You can find the access key in the Settings > Access keys blade for your storage account.

7. Set the share path("**\\*[storage account name].file.core.windows.net\[file share path name]***") as Storage Path in Managed Storage Settings.



My Files Storage Settings

Storage Path: \\Filecloudazurefiles.file.core.windows\filecloudata

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

Number of old versions to keep for each file: 3

Number of versions to keep

Encryption: Manage

Manage encryption

Disable My Files: □

Disable 'My Files' [Managed Storage]

Default User Storage Quota: 2 GB

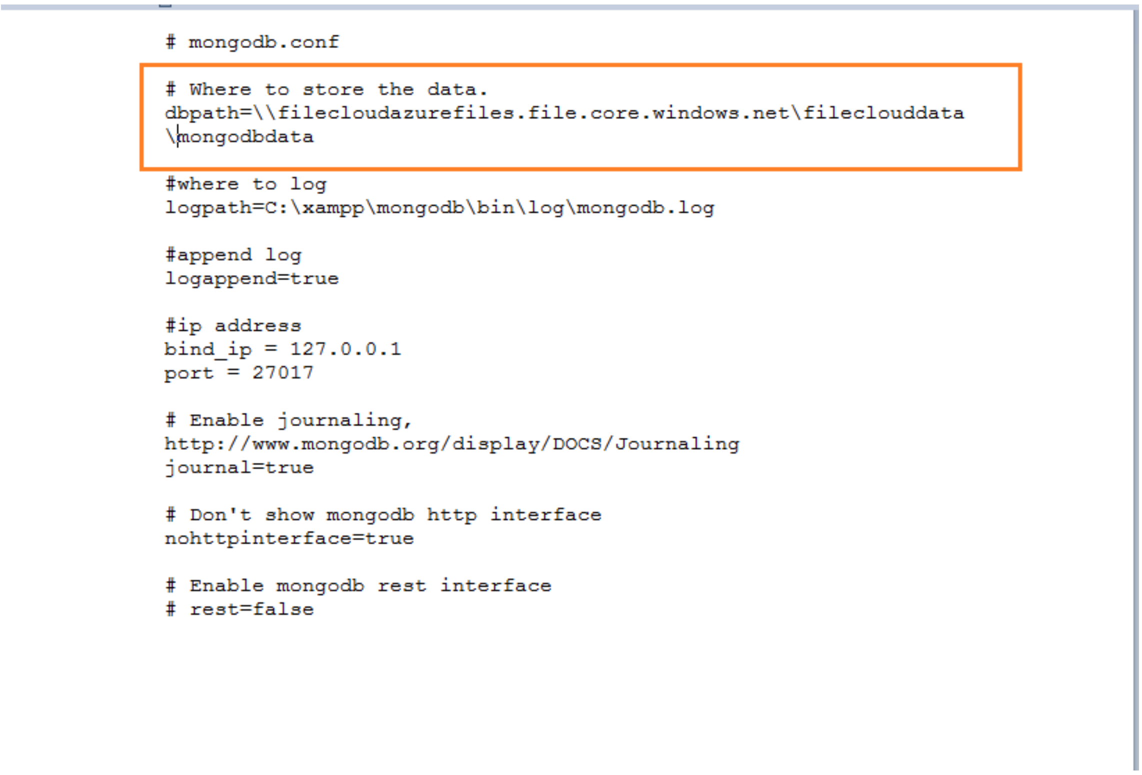
Default storage quota for new user. Can be overriden in user details. This does not affect existing user.

User Storage Usage Calculation: Exclude Shares

Specify user storage calculation

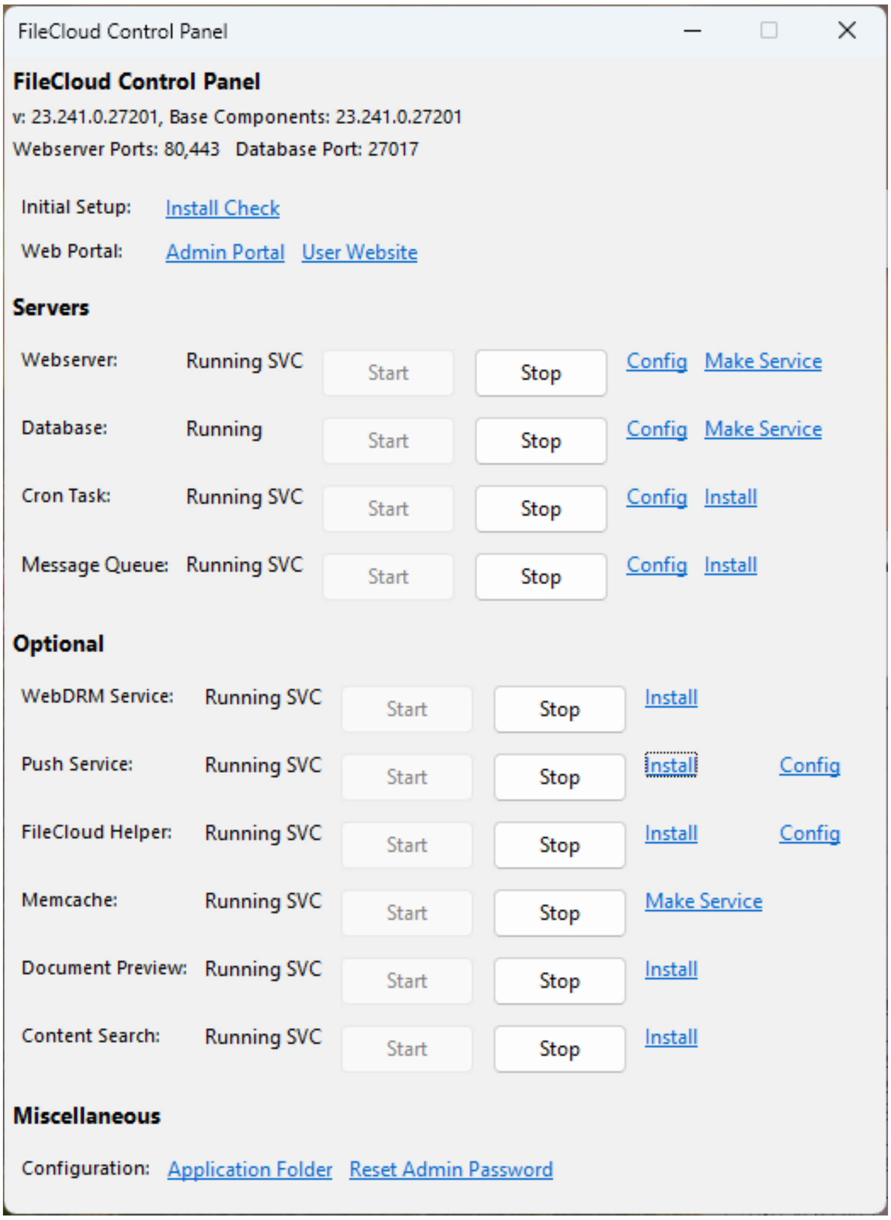
Store Deleted Files: ☑

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 **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: 23.241.0.27201, Base Components: 23.241.0.27201

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

Webserver: Running SVC

Database: Running

Cron Task: Running SVC

Message Queue: Running SVC

Optional

WebDRM Service: Running SVC

Push Service: Running SVC

FileCloud Helper: Running SVC

Memcache: Running SVC

Document Preview: Running SVC

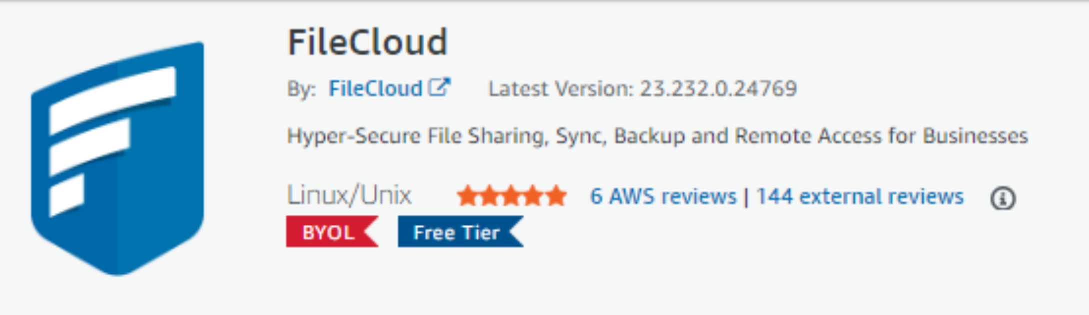
Content Search: Running SVC

Miscellaneous

Configuration: Application Folder Reset Admin Password

Amazon Web Services (AWS) Installation

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



FileCloud

By: FileCloud Latest Version: 23.232.0.24769

Hyper-Secure File Sharing, Sync, Backup and Remote Access for Businesses

Linux/Unix ★★★★★ 6 AWS reviews | 144 external reviews

See FileCloud AMI[14]here on AWS Marketplace.

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

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 2022)[15]

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

FileCloud Enterprise File Sharing and Sync (20 Users)[16]

FileCloud Enterprise File Sharing and Sync - Windows 2022 -(20 Users)[17]

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.

[14] https://aws.amazon.com/marketplace/pp/B00NPCWWFQ
[15] https://aws.amazon.com/marketplace/pp/B072J9H2CX
[16] https://aws.amazon.com/marketplace/pp/B01M7XY4AG
[17] https://aws.amazon.com/marketplace/pp/B01M9JG0R5

- 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.

To launch the FileCloud AMI:

1. Complete the Pre-requisites

An AWS Account

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[18]

You can read more about Amazon Elastic Compute Cloud[19]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**.

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:

[18] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html
[19] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

- compute
- memory
- storage capabilities

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

Read more about Amazon's Instance Types[20]

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[21]

We recommend selecting 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.

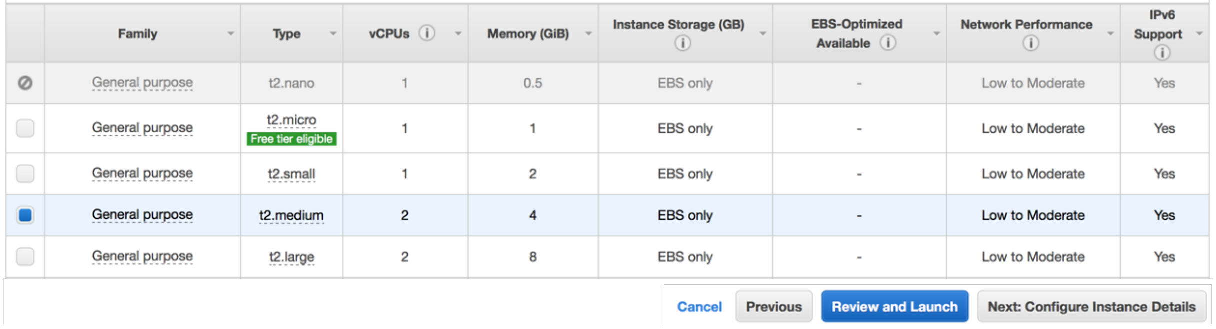
4. Configure Instance Details

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.

[20] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html
[21] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#AvailableInstanceTypes

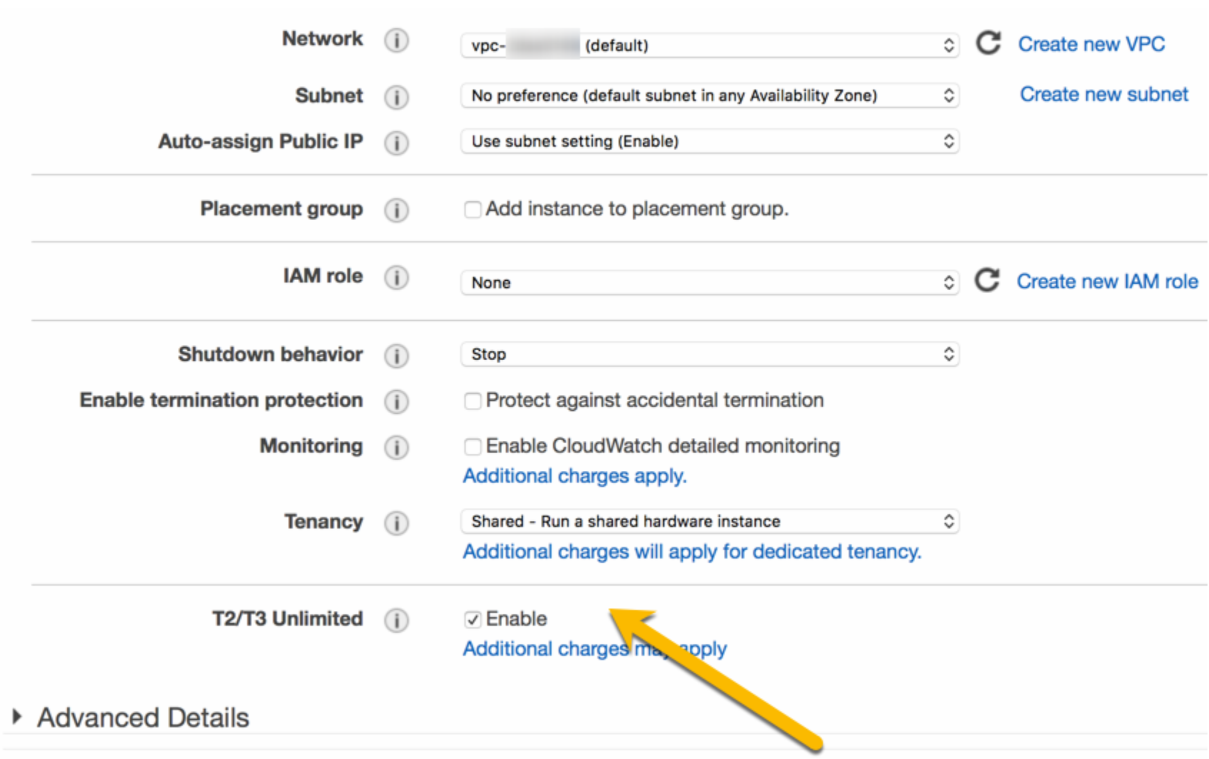


	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
⊘	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to 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

To configure instance details:

1. 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: vpc-[redacted] (default)

Subnet: No preference (default subnet in any Availability Zone)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group.

IAM role: None

Shutdown behavior: Stop

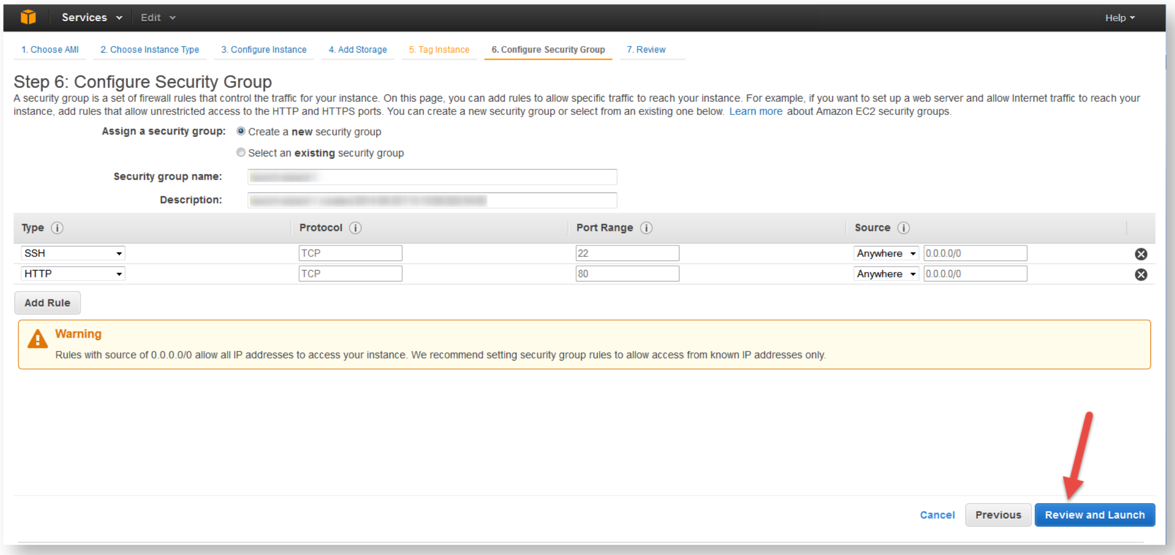
Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

T2/T3 Unlimited: ☑ Enable
Additional charges may apply

Figure 4. Configure Security Groups



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: [redacted]

Description: [redacted]

Type	Protocol	Port Range	Source	
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 recommend setting security group rules to allow access from known IP addresses only.

➡ You can read more about Amazon EC2 Security Groups[22].

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

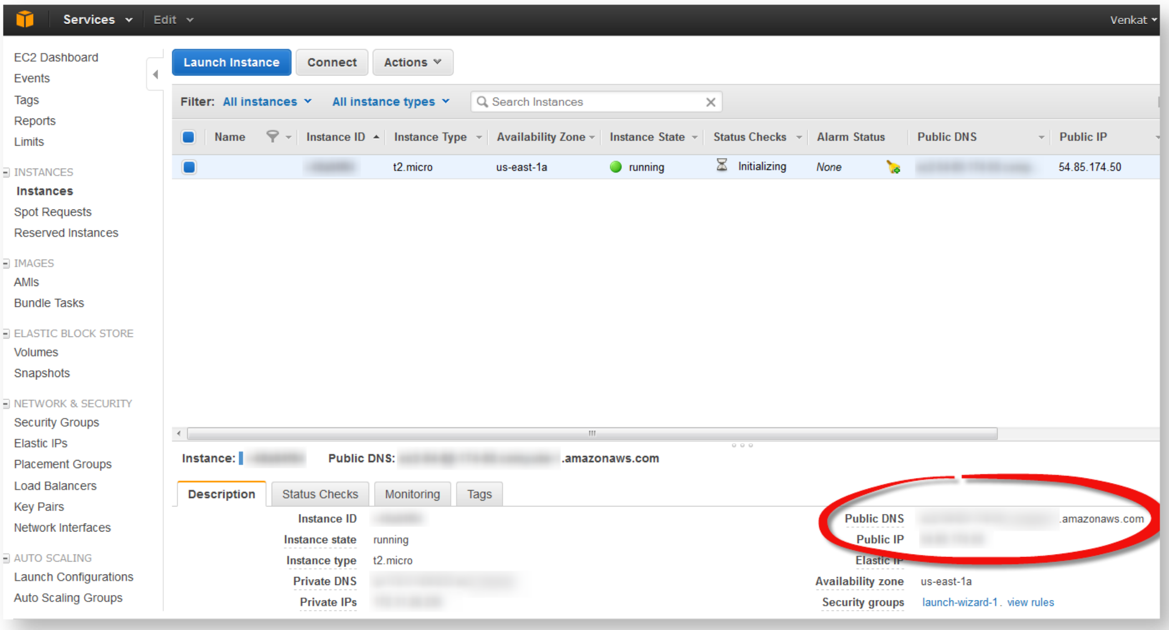
5. Launch the Instance

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**.
   A confirmation page lets you know that your instance is launching.
3. Choose **View Instances** to close the confirmation page and return to the console.
4. On the **Instances** screen, you can view the status of the launch.
   It takes a short time for an instance to launch.
   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.
5. 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).
6. It can take a few minutes for the instance to be ready so that you can connect to it.
7. Check that your instance has passed its status checks in the **Status Checks** column.
8. Note the Public DNS name to access your FileCloud site.

Figure 5. FileCloud Status in Your AWS dashboard.

[22] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#creating-security-group



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
	[redacted]	t2.micro	us-east-1a	running	Initializing	None	[redacted]	54.85.174.50

Instance: [redacted] Public DNS: [redacted].amazonaws.com

Instance ID	[redacted]	Public DNS	[redacted].amazonaws.com
Instance state	running	Public IP	[redacted]
Instance type	t2.micro	Elastic IP	
Private DNS	[redacted]	Availability zone	us-east-1a
Private IPs	[redacted]	Security groups	launch-wizard-1 . view rules

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

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

💡 To receive a license you must register at the FileCloud license management portal[23].

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:

[23] https://portal.getfilecloud.com/ui/user/index.html?mode=register

☑	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 2. Navigate to **http://<public_dns_name>/install**. 3. 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 set up the FileCloud site according to your requirements.
	Take periodic snapshots of your running instance for disaster recovery and as an additional backup for the FileCloud database and app.

Need to seed data quickly into your new FileCloud installation
Seeding FileCloud for Amazon S3 (see page 76)

FileCloud on AWS - User Deployment Guide

Introduction

Use AWS infrastructure (EC2, EBS, S3) to jumpstart your own branded, file storage solution in a 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 serve your clients, customers and partners.
- Endpoint Backup and DLP - Use FileCloud to securely back up 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 your branch office windows files servers to FileCloud running on AWS to get low latency LAN access as well as remote access from anywhere.

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 preconfigured 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 a production workload.

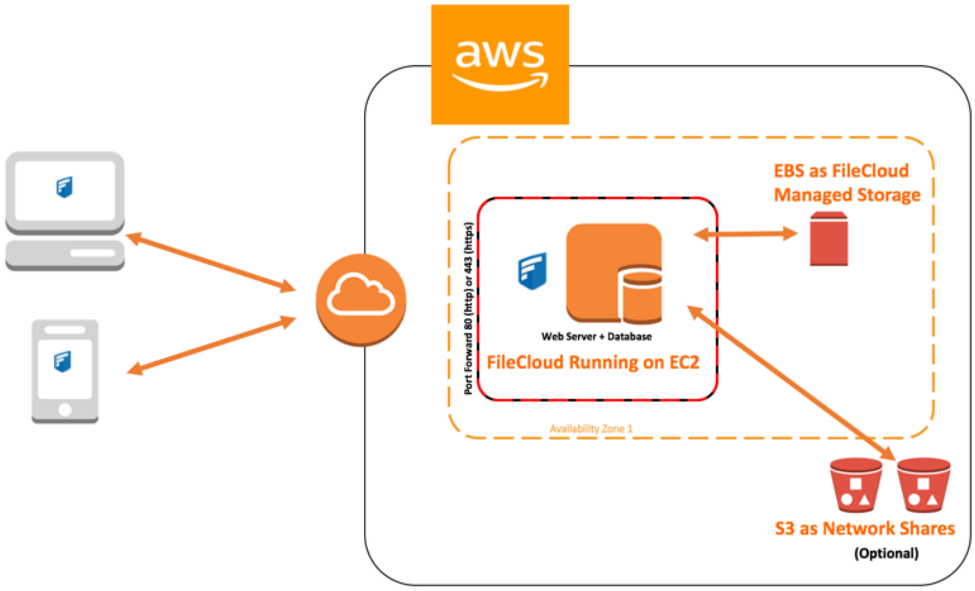
Prerequisites and Requirements

FileCloud AMIs 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. Request a license using this form on our website[24]. Once you get the trial license, upload it to your running EC2 instance. Since FileCloud AMIs are available on Ubuntu and Windows Server OS, you can choose the OS you are familiar with.

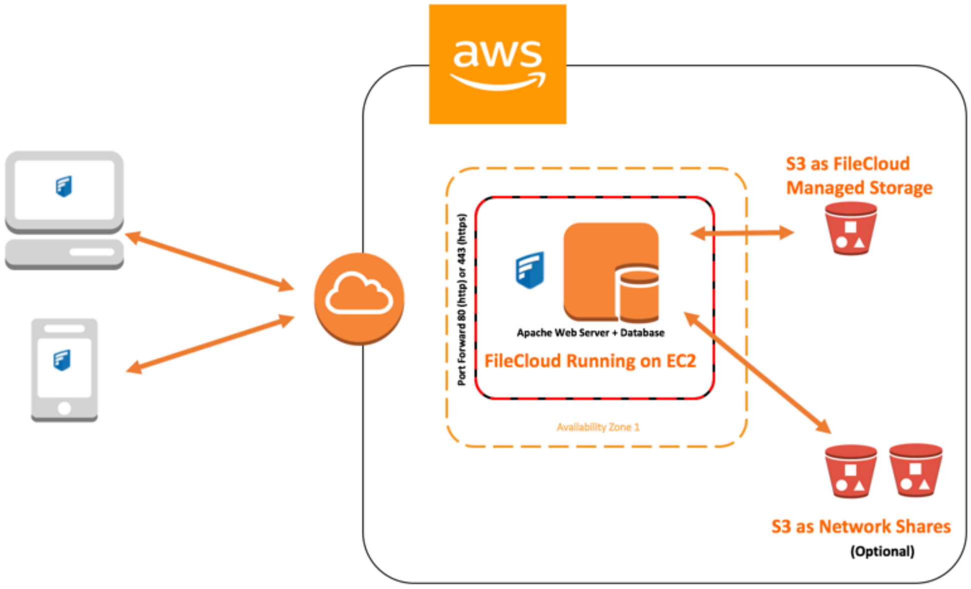
[24] https://www.filecloud.com/#onpremisesTrial

Architecture Diagrams

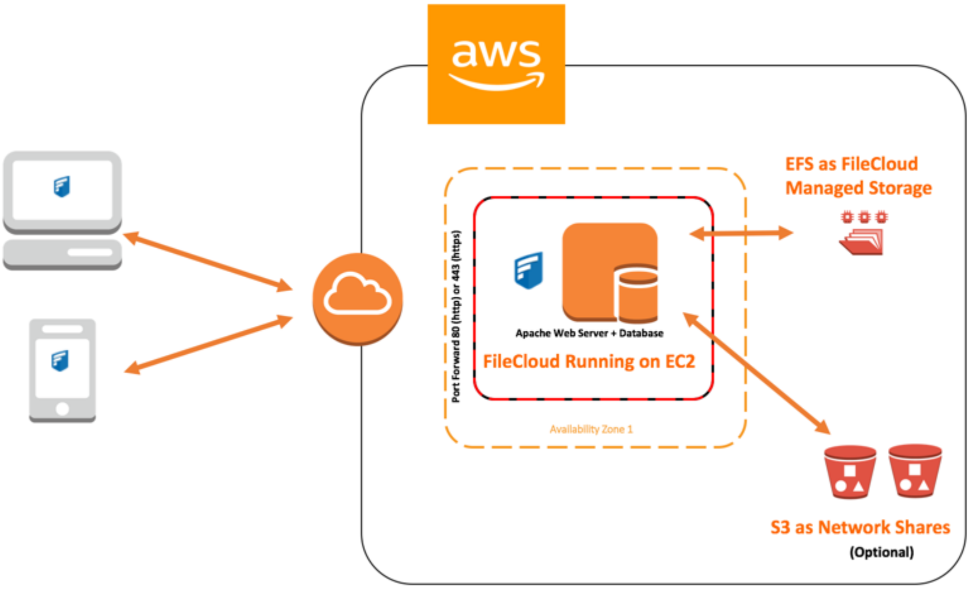
Option 1: FileCloud EC2 + EBS (Files Storage)



Option 2: FileCloud EC2 + S3 (Managed Files Storage)


aws
S3 as FileCloud Managed Storage
Port Forward 80 (http) or 443 (https)
Apache Web Server + Database
FileCloud Running on EC2
Availability Zone 1
S3 as Network Shares
(Optional)

Option 3: FileCloud EC2 + EFS (Managed Files Storage)


aws
EFS as FileCloud Managed Storage
Port Forward 80 (http) or 443 (https)
Apache Web Server + Database
FileCloud Running on EC2
Availability Zone 1
S3 as Network Shares
(Optional)

To access FileCloud, you only need port 80 (http) or 443 (https). We strongly recommend you 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, your administrator may supply an optional master password and start the initialization process. Once the initialization process is started, the following steps occur 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 unencrypted files (if they exist) in FileCloud storage must be encrypted before the system is ready for use. Look at the next section for more information on file encryption.

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

Additional details on the keys:

Key	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	• The 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.
Encrypted File Key	• Encrypted using master public key	None	Encrypted file key is persisted	• Decryption of the Encrypted File key results in the Plain File key. • Decryption of the Encrypted File key will be done using the Master Private key and optional master password. • The Encrypted File key is decrypted every time FileCloud server is started. • The Plain File key that is a result of decryption process is cached for the lifetime of the FileCloud server process. When the server is restarted, a fresh decryption is required.

If you are going to use S3 for Managed File storage, 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, use the following instructions to set up your S3 for FileCloud.

Setting up Amazon S3 Credentials

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   The **Managed Storage** settings page opens by default.
2. Enter the S3 config information. Refer to the following table for more information about each setting.
3. Click **Save S3 Settings**.

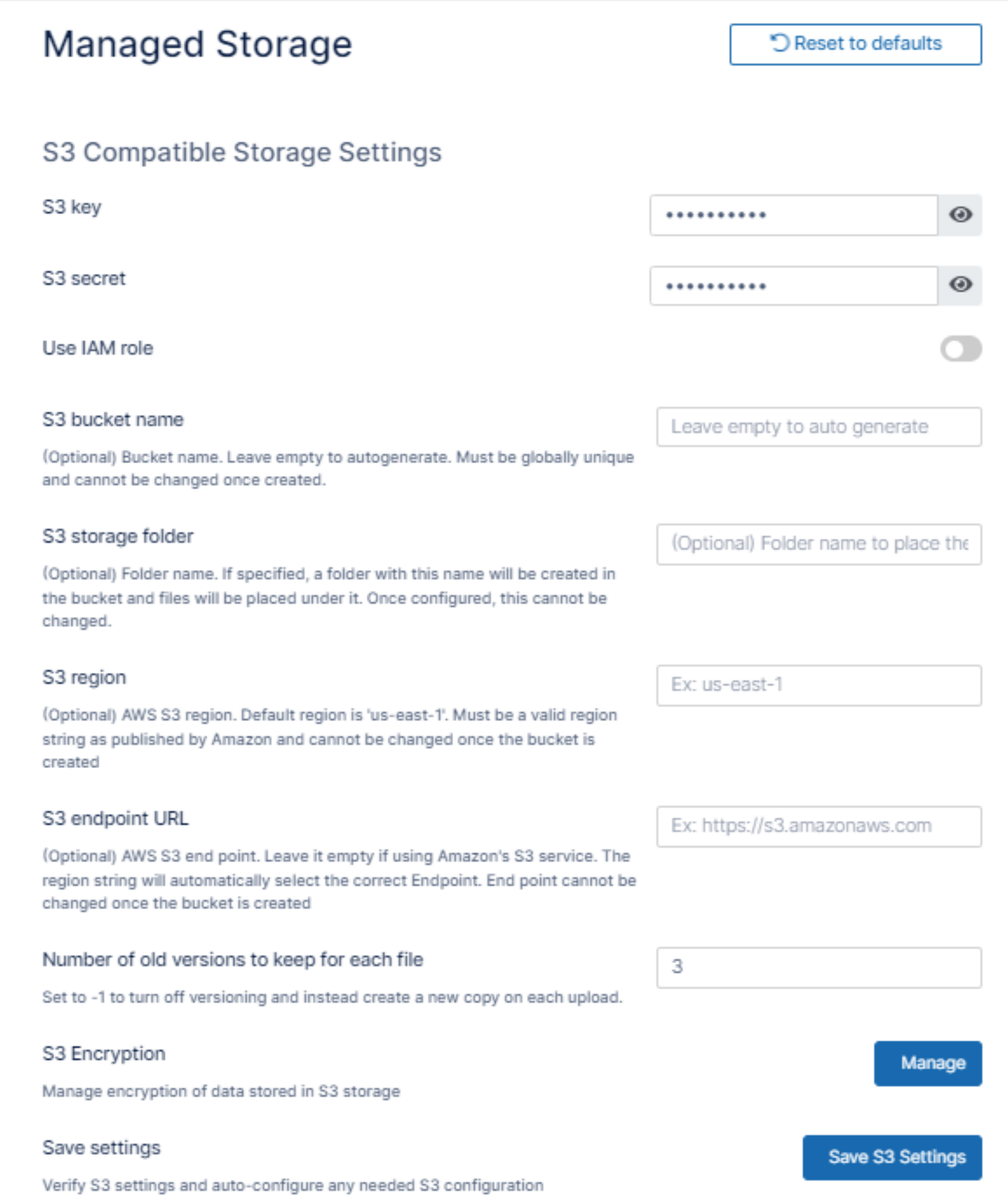
Field	Description
S3 key	This is your amazon authentication key (To get your access key, visit Amazon security portal[25]). For IAM user, it requires the IAM Policy for S3 Access given below.
S3 secret	This is your amazon authentication secret (To get your access key, visit Amazon security portal[26]). For IAM user, it requires the IAM Policy for S3 Access given below .
Use IAM role	Either check **Use IAM role** or type in authentication credentials in **S3 Key** and **S3 Secret**.
S3 bucket name	Provide a bucket name. The bucket should be new (in some circumstance, a 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 (which is 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(for example, europe or south east) provide the correct region string. The strings should match the region string published by amazon[27]. **Note: For govcloud installs, you must use region string: us-gov-west-1**
S3 endpoint 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 an unpublished region. If you are using an AWS endpoint, use one of the endpoints published here[28].

[25] https://console.aws.amazon.com/iam/home#security_credential
[26] https://console.aws.amazon.com/iam/home#security_credential
[27] http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
[28] http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

Field	Description
Number of old versions to keep for each file.	If a file with the same path and name is uploaded, FileCloud versions the file. This setting determines number of recent versions that FileCloud should retain. To disable versioning completely, set the number of versions to 0. **NOTE**: Versioned files count towards the user's storage quota.

To fill in the other S3 settings, see Setting up FileCloud Managed S3 Storage.

☒ The Amazon S3 Bucket should NEVER be modified outside of FileCloud subsystem
Do not add/edit/modify files directly using Amazon tools. Doing so will destabilize your FileCloud installation.



Managed Storage

S3 Compatible Storage Settings

S3 key: •••••••••••

S3 secret: •••••••••••

Use IAM role

S3 bucket name: Leave empty to auto generate

(Optional) Bucket name. Leave empty to autogenerate. Must be globally unique and cannot be changed once created.

S3 storage folder: (Optional) Folder name to place the

(Optional) Folder name. If specified, a folder with this name will be created in the bucket and files will be placed under it. Once configured, this cannot be changed.

S3 region: Ex: us-east-1

(Optional) AWS S3 region. Default region is 'us-east-1'. Must be a valid region string as published by Amazon and cannot be changed once the bucket is created

S3 endpoint URL: Ex: https://s3.amazonaws.com

(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 changed once the bucket is created

Number of old versions to keep for each file: 3

Set to -1 to turn off versioning and instead create a new copy on each upload.

S3 Encryption

Manage encryption of data stored in S3 storage

Save settings

Verify S3 settings and auto-configure any needed S3 configuration

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.

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.

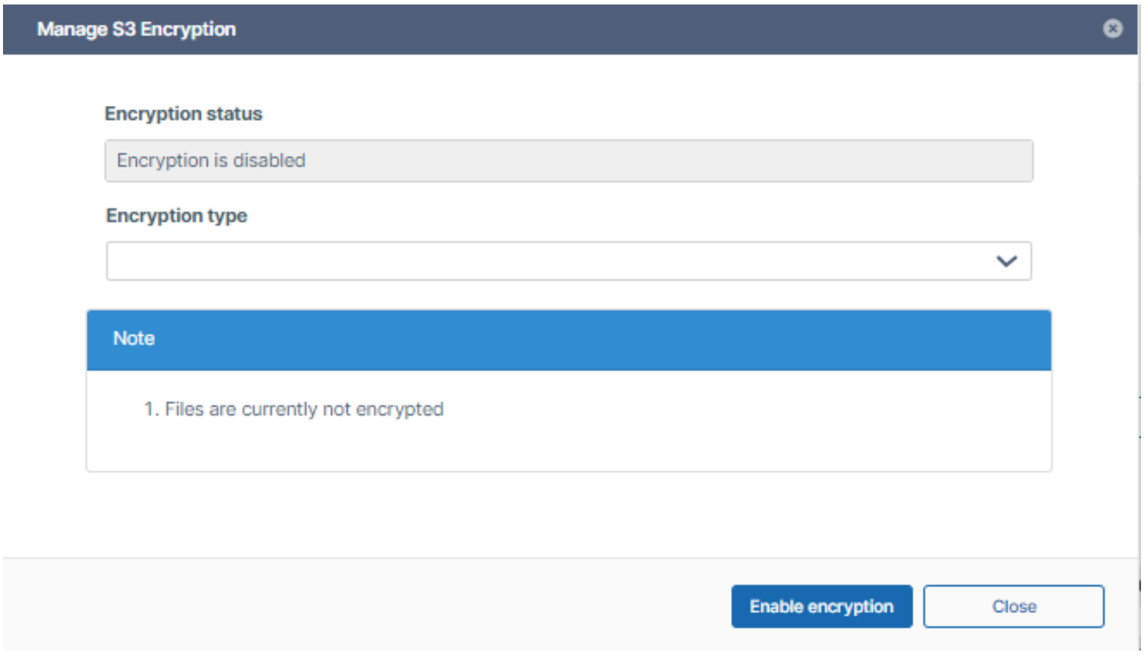
Encryption Type	Notes
Server-Side Encryption with Customer-Provided Keys (SSE-C)	This is a new support available from FileCloud v15 on-wards. The data will be encrypted using customer supplied 32 bit encryption key. This option will have SLOWER performance due to restriction on how this data can be decrypted (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.

When you enable encryption, FileCloud attempts to encrypt all available data in the bucket. This can take some time depending on the amount of existing data in the bucket. Enable or disable encryption when there is minimal activity in FileCloud.
Although, changing encryption can be done at any time, we recommend using off-peak hours to avoid any unexpected access issues

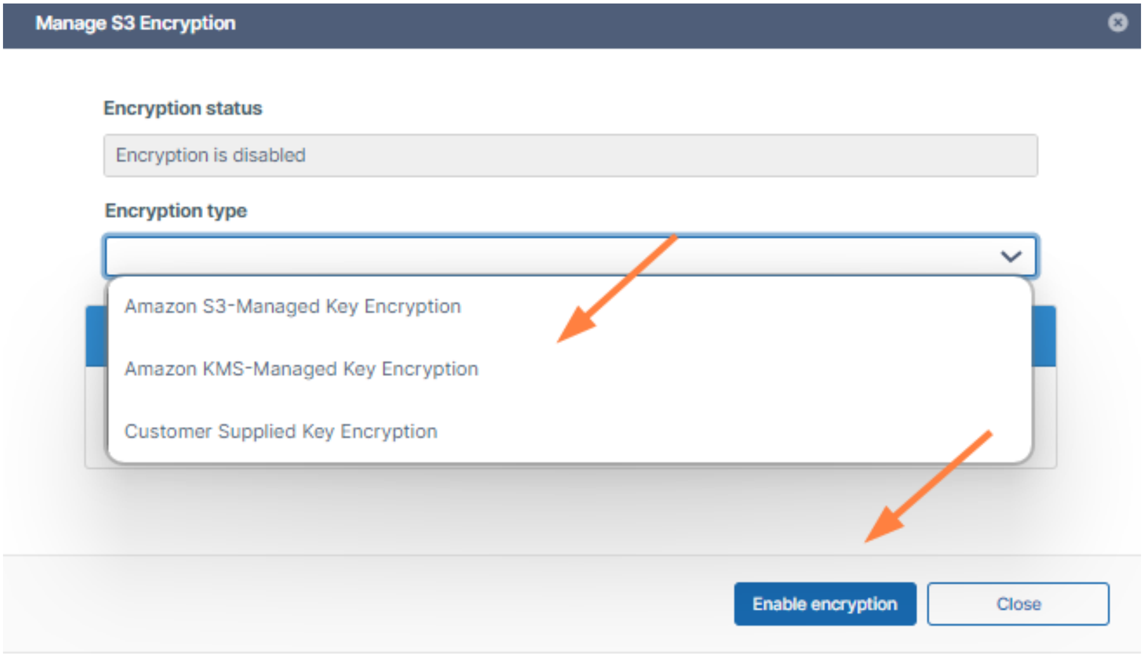
For Windows, If your xampp is installed in a location other than c:\xampp, then add the following key in **<your xampp folder>\htdocs\config\cloudconfig.php**
For example, if your xampp is in D:\xampp, then in file **D:\xampp\htdocs\config\cloudconfig.php**, add the following string (any location before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

To enable S3 encryption:

1. In the Managed Storage settings page, click **Manage** beside **S3 Encryption**



2. Choose one of the **Encryption types.**
3. Then click **Enable** encryption.


Manage S3 Encryption
Encryption status
Encryption is disabled
Encryption type
Amazon S3-Managed Key Encryption
Amazon KMS-Managed Key Encryption
Customer Supplied Key Encryption
Enable encryption
Close

4. Confirm that you want to enable encryption.

Costs

T2.Medium or T3.Medium is sufficient to run FileCloud for 100 users. File storage cost depends on the storage method you choose (EBS, EFS or S3), the amount of files you will store, and the access pattern.

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 the number of users and their access pattern, you can scale your deployment by choosing a bigger instance or adding more instances.

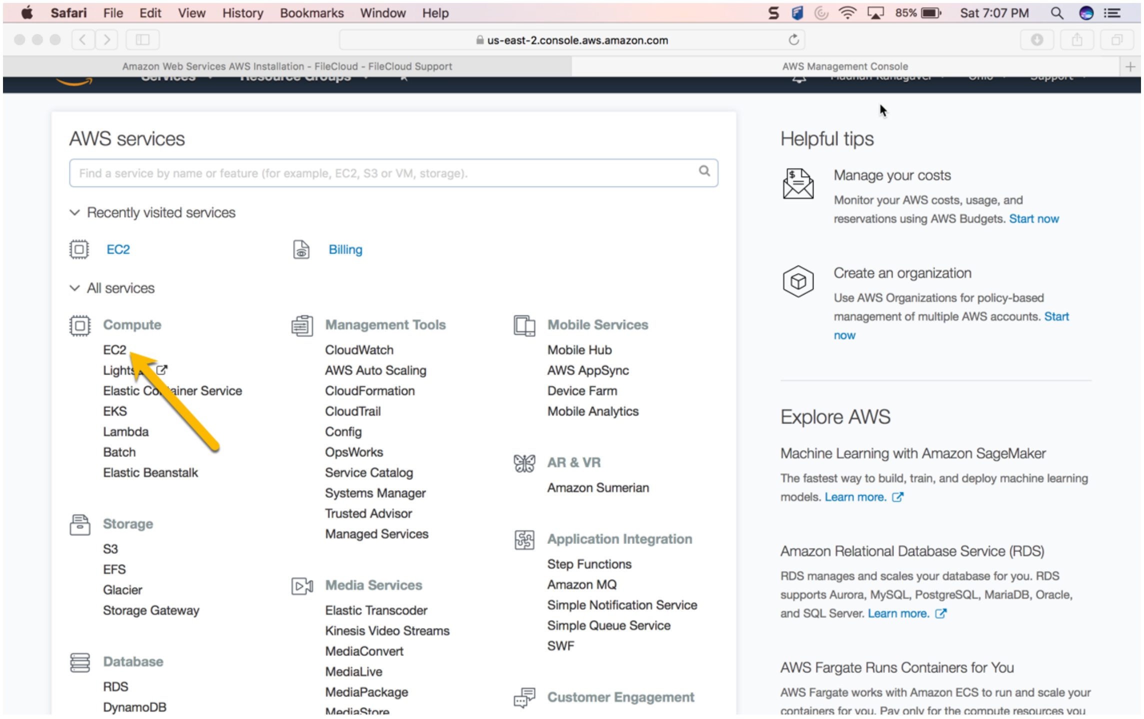
Deployment Guidance

Deployment Assets

FileCloud pre-built AMI's (Amazon Machine Image) are currently available in Amazon AWS Marketplace for both Linux (Ubuntu) and Windows Server OS.

Steps to Launch FileCloud AMI

1. Log in to the AWS management console[29], and click **EC2** (virtual servers in the cloud).



Monitor your AWS costs, usage, and reservations using AWS Budgets. Start now

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

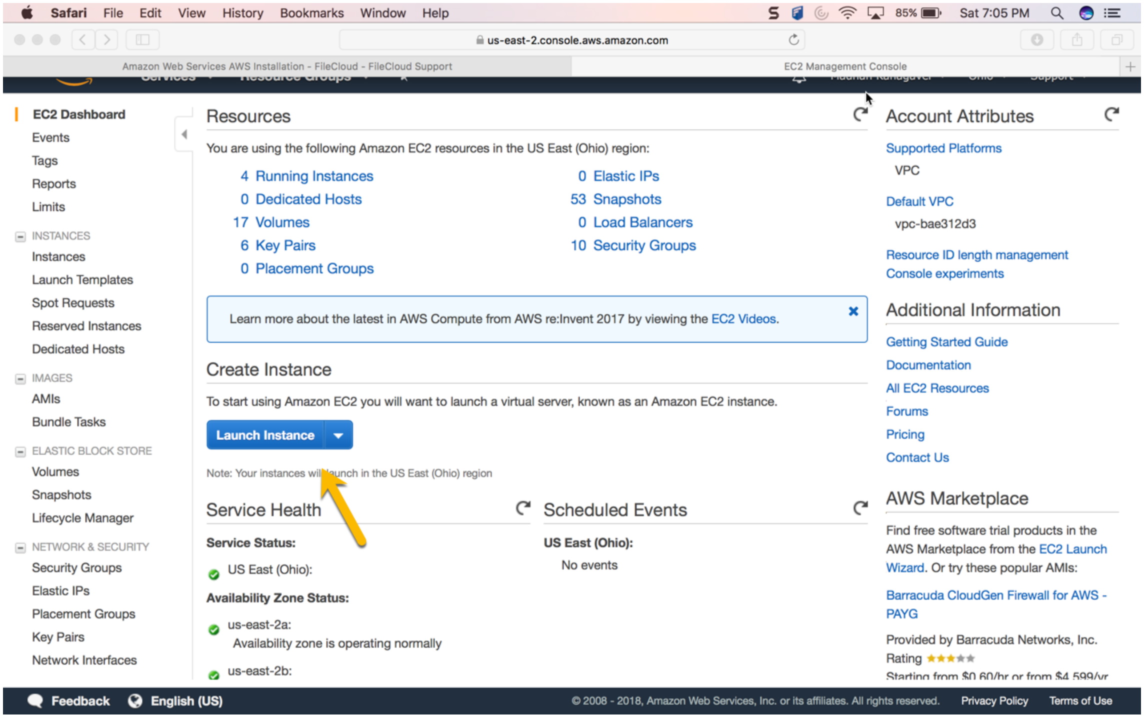
The fastest way to build, train, and deploy machine learning models. Learn more.

RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

AWS Fargate works with Amazon ECS to run and scale your containers for you. Pay only for the compute resources you

2. Click **Launch Instance**.

[29] http://aws.amazon.com/console/


Safari File Edit View History Bookmarks Window Help
85% Sat 7:05 PM
us-east-2.console.aws.amazon.com
Amazon Web Services AWS Installation - FileCloud - FileCloud Support
EC2 Management Console

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Resources

You are using the following Amazon EC2 resources in the US East (Ohio) region:

4 Running Instances	0 Elastic IPs
0 Dedicated Hosts	53 Snapshots
17 Volumes	0 Load Balancers
6 Key Pairs	10 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US East (Ohio) region

Service Health

Service Status:

US East (Ohio):

Availability Zone Status:

us-east-2a:
Availability zone is operating normally

us-east-2b:

Scheduled Events

US East (Ohio):
No events

Account Attributes

Supported Platforms
VPC

Default VPC
vpc-bae312d3

Resource ID length management
Console experiments

Additional Information

Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

AWS Marketplace

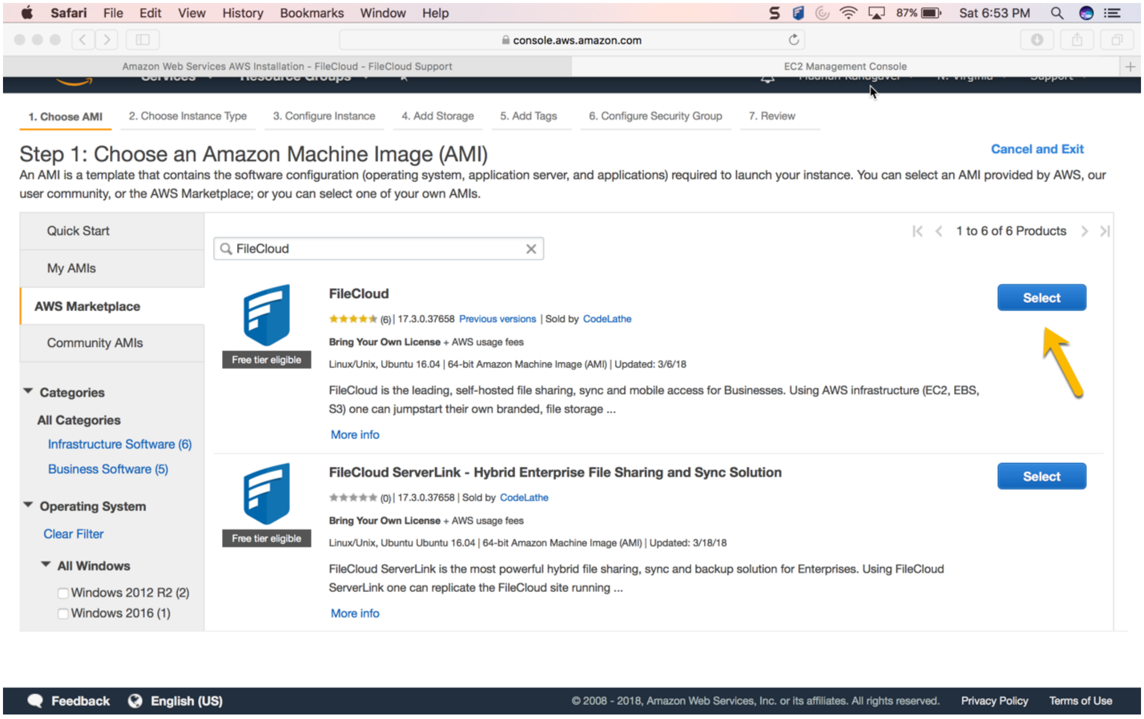
Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these popular AMIs:

Barracuda CloudGen Firewall for AWS - PAYG

Provided by Barracuda Networks, Inc.
Rating ★★★★★
Starting from $0.60/hr or from $4,599/yr

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

3. Search for FileCloud AMI in AWS marketplace. Choose the latest version.
   The latest version details may be different from the information shown.


Safari File Edit View History Bookmarks Window Help
87% Sat 6:53 PM
console.aws.amazon.com
Amazon Web Services AWS Installation - FileCloud - 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 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start
My AMIs
AWS Marketplace
Community AMIs

Categories
All Categories
Infrastructure Software (6)
Business Software (5)

Operating System
Clear Filter
All Windows
□ Windows 2012 R2 (2)
□ Windows 2016 (1)

FileCloud

1 to 6 of 6 Products

FileCloud

Free tier eligible

★★★★★ (6) | 17.3.0.37658 Previous versions | Sold by CodeLathe

Bring Your Own License + AWS usage fees

Linux/Unix, Ubuntu 16.04 | 64-bit Amazon Machine Image (AMI) | Updated: 3/6/18

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using AWS infrastructure (EC2, EBS, S3) one can jumpstart their own branded, file storage ...

More info

Select

FileCloud ServerLink - Hybrid Enterprise File Sharing and Sync Solution

Free tier eligible

★★★★★ (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

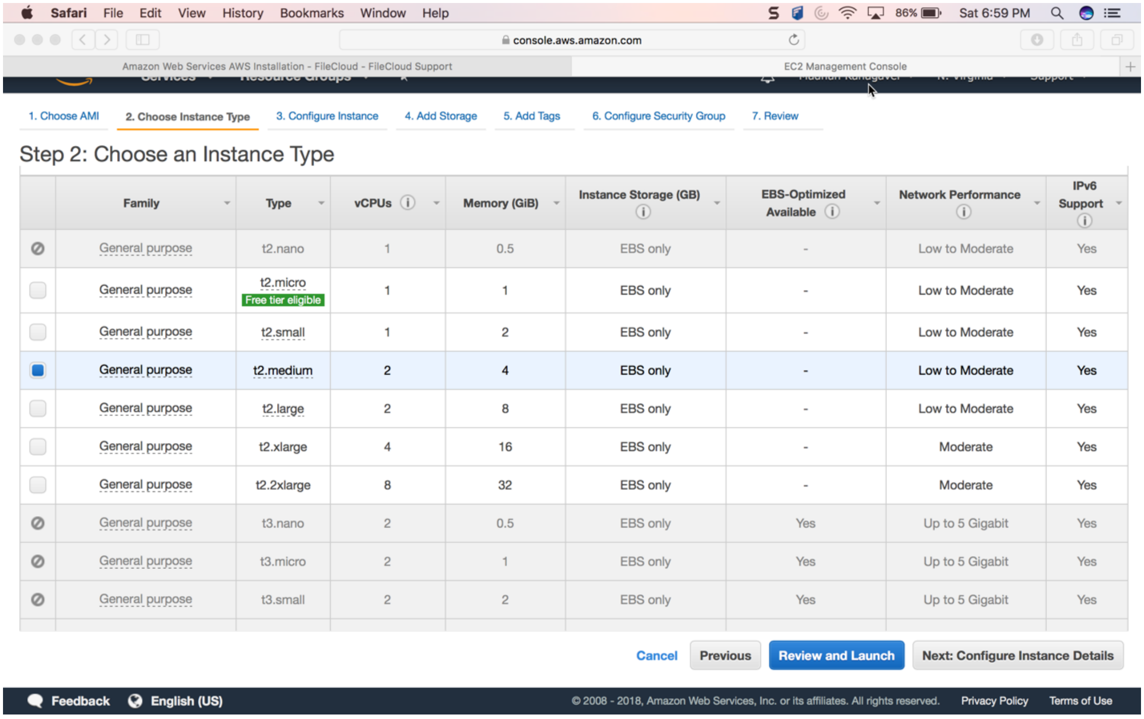
FileCloud ServerLink is the most powerful hybrid file sharing, sync and backup solution for Enterprises. Using FileCloud ServerLink one can replicate the FileCloud site running ...

More info

Select

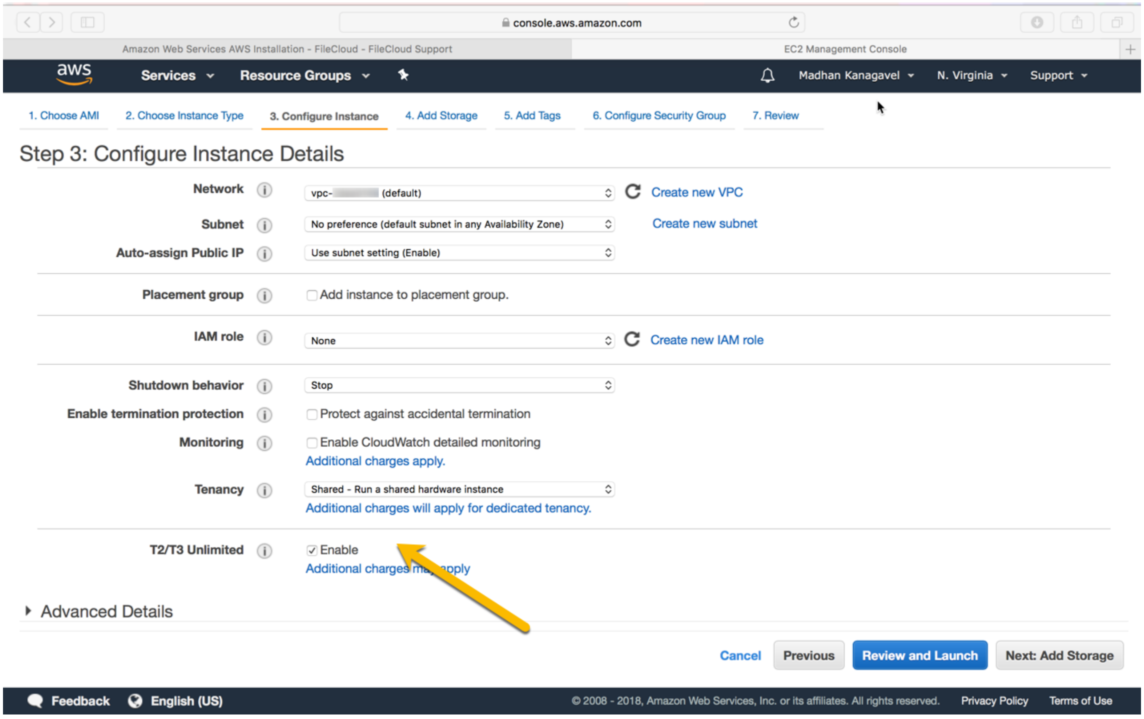
Feedback English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4. Choose the desired Amazon EC2 Instance type. We recommend at least 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, enable T2/T3 unlimited when you configure the instance.**


Safari File Edit View History Bookmarks Window Help
86% Sat 6:59 PM
console.aws.amazon.com
Amazon Web Services AWS Installation - FileCloud - 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
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

Step 2: Choose an Instance Type

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
⊘	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
⊘	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
⊘	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
⊘	General purpose	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes



Step 3: Configure Instance Details

Network: vpc-[redacted] (default)

Subnet: No preference (default subnet in any Availability Zone)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group.

IAM role: None

Shutdown behavior: Stop

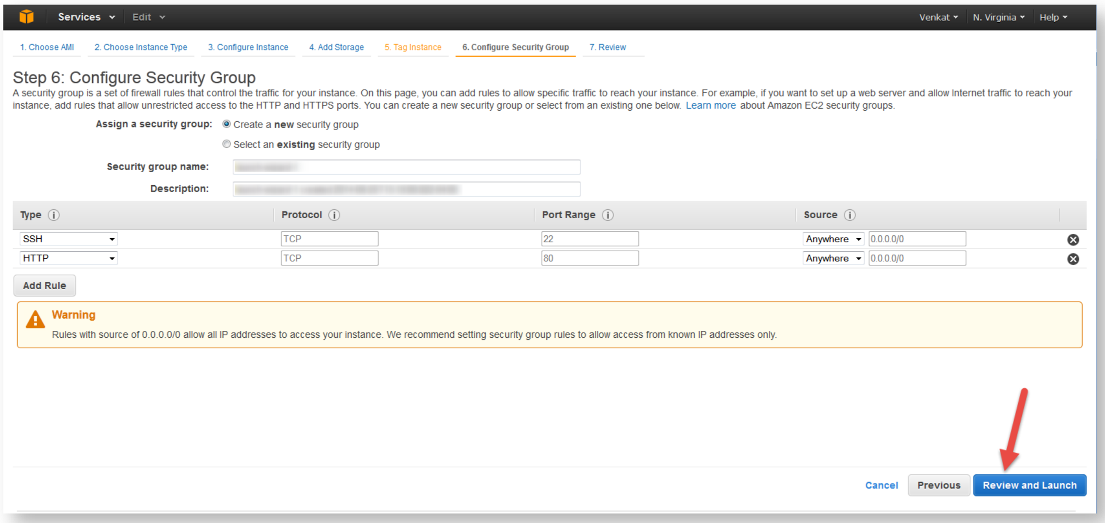
Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

T2/T3 Unlimited: ☑ Enable
Additional charges may apply

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



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: [redacted]

Description: [redacted]

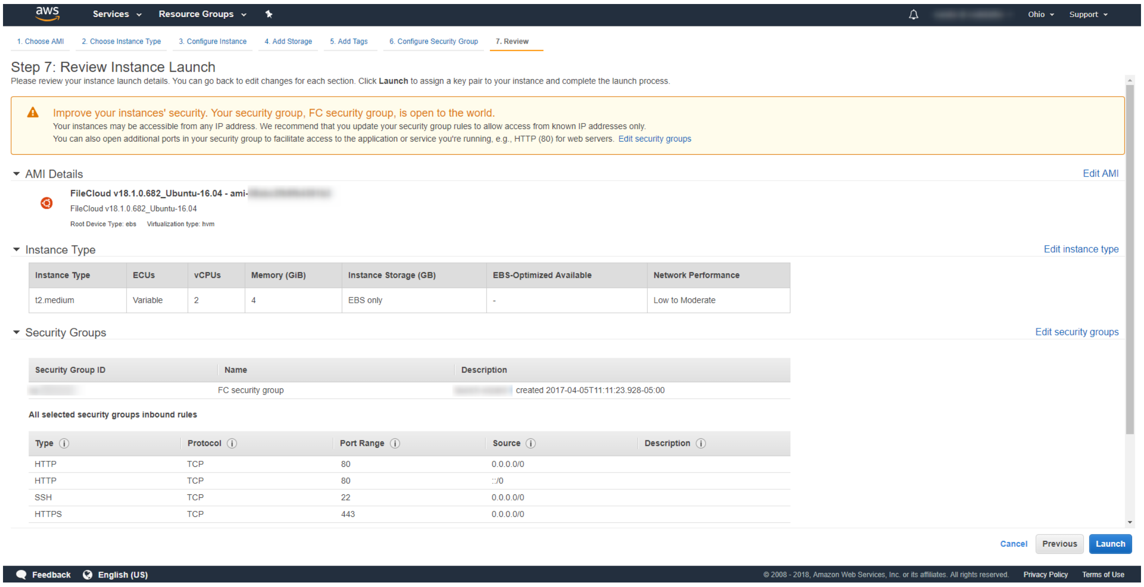
Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTP	TCP	80	Anywhere 0.0.0.0/0

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

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.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, FC security group, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

FileCloud v18.1.0.682_Ubuntu-16.04 - ami-[redacted]

FileCloud v18.1.0.682_Ubuntu-16.04

Root Device Type: ebs Virtualization type: hvm

Instance 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

Security Groups

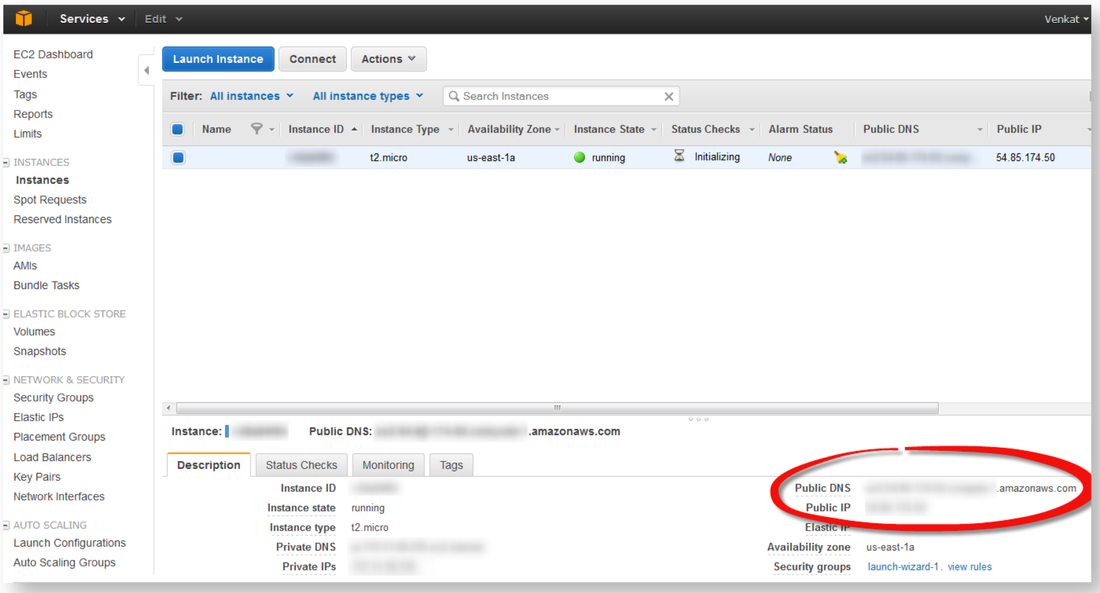
Security Group ID	Name	Description
[redacted]	FC security group	[redacted] created 2017-04-05T11:11:23.928-05:00

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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



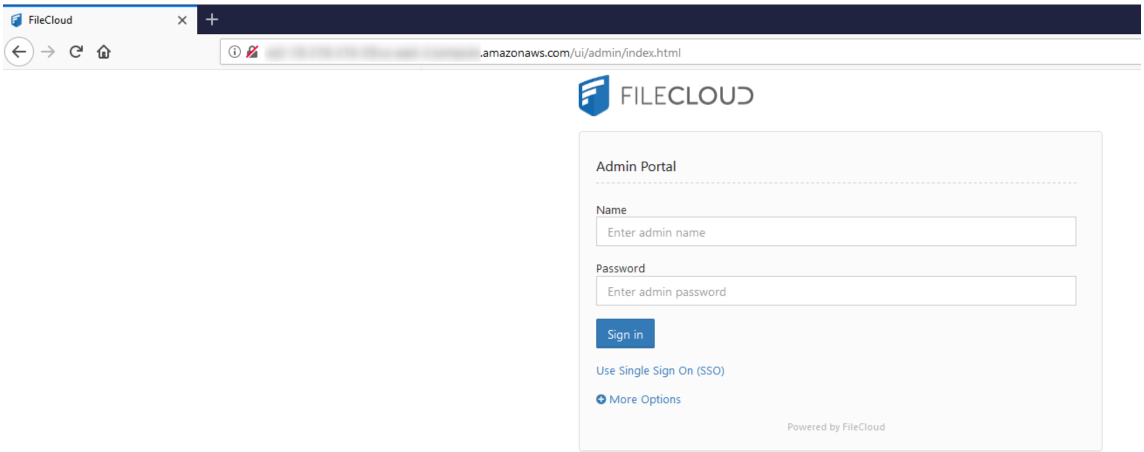
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
	[redacted]	t2.micro	us-east-1a	running	Initializing	None	[redacted]	54.85.174.50

Instance: [redacted] Public DNS: [redacted].amazonaws.com

Instance ID	[redacted]	Public DNS	[redacted].amazonaws.com
Instance state	running	Public IP	[redacted]
Instance type	t2.micro	Elastic IP	
Private DNS	[redacted]	Availability zone	us-east-1a
Private IPs	[redacted]	Security groups	launch-wizard-1 . view rules

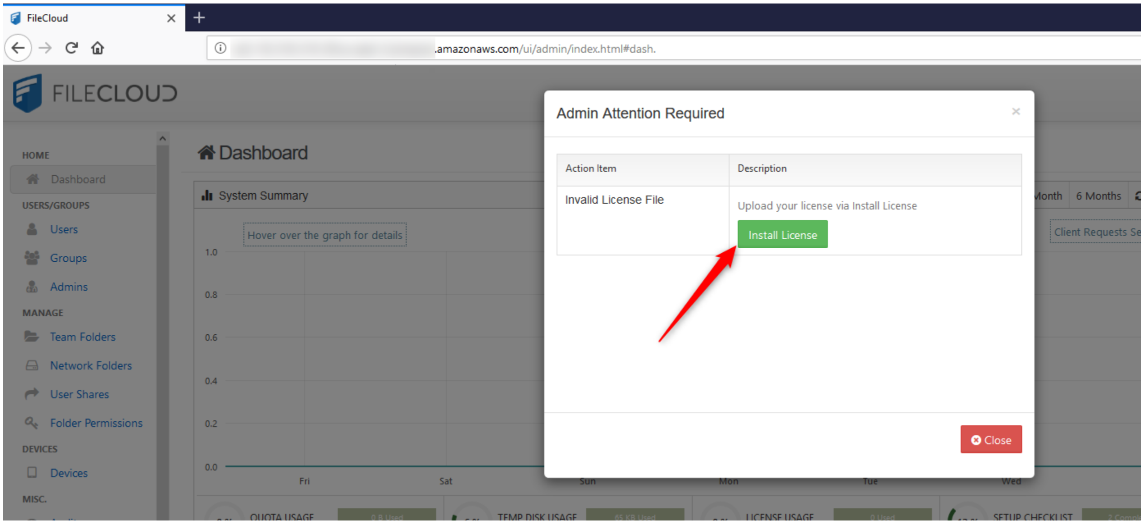
8. Type 'http://<public_dns_name>/ui/admin/index.html' in your browser to access the FileCloud admin portal. If the Webpage fails to load, verify port 80 is open as mentioned above in Step 5.

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



[redacted].amazonaws.com/ui/admin/index.html

9. Once you have logged into the admin portal, install the FileCloud License. Request a license using this form on our website[30] to get trial licenses.



Admin Attention Required

Action Item	Description
Invalid License File	Upload your license via Install License Install License

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. See the following section (Enabling Amazon S3 Storage) for instructions for setting up S3 for FileCloud file storage.
4. The default FileCloud instance uses our SMTP servers and accounts to send emails. Change this to your SMTP server for security purposes.
5. 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

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.

[30] https://www.filecloud.com/#onpremisesTrial

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:

1. Edit the file **WWWROOT/config/cloudconfig.php** and change the line
   define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "local");
   to read as
   define("TONIDOCLOUD_STORAGE_IMPLEMENTATION", "amazons3");
2. Rename the 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

Once you have configured FileCloud storage, 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 to the 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.

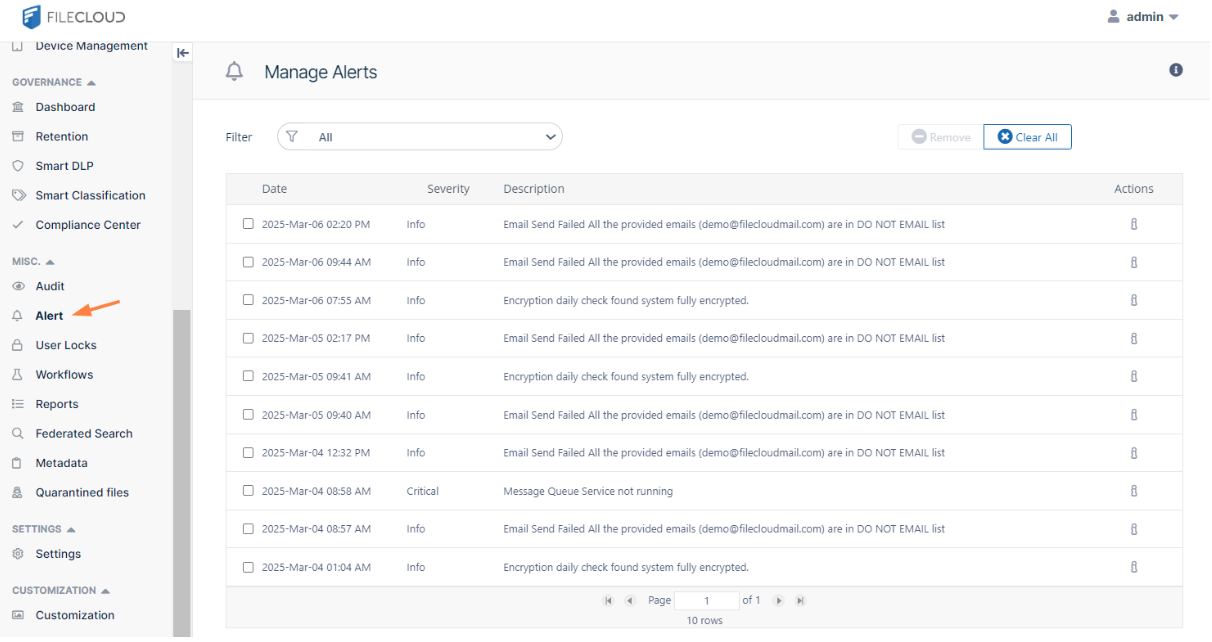
This page tracks all unhandled exceptions and system error messages generated in the FileCloud server. The number of alerts are shown in the Dashboard and the Alerts page shows detailed information about the various errors encountered.

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 screenshot 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 receive periodic Administrator Summary emails that show the number of alerts.



Manage Alerts

Filter: All

	Date	Severity	Description	Actions
□	2025-Mar-06 02:20 PM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-06 09:44 AM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-06 07:55 AM	Info	Encryption daily check found system fully encrypted.	
□	2025-Mar-05 02:17 PM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-05 09:41 AM	Info	Encryption daily check found system fully encrypted.	
□	2025-Mar-05 09:40 AM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-04 12:32 PM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-04 08:58 AM	Critical	Message Queue Service not running	
□	2025-Mar-04 08:57 AM	Info	Email Send Failed All the provided emails (demo@filecloudmail.com) are in DO NOT EMAIL list	
□	2025-Mar-04 01:04 AM	Info	Encryption daily check found system fully encrypted.	

Page 1 of 1
10 rows

Backup and Recovery

FileCloud supports unlimited file versioning and a recycle bin. You can configure these options by logging in to the FileCloud admin portal. These features provide protection from accidental deletions by users.

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

The following command backs up mongodb to a designated s3 bucket (you can also make it a cron job so that it runs periodically).

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

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

1. Before making any changes, stop the 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. Start the mongodb service using following command.`

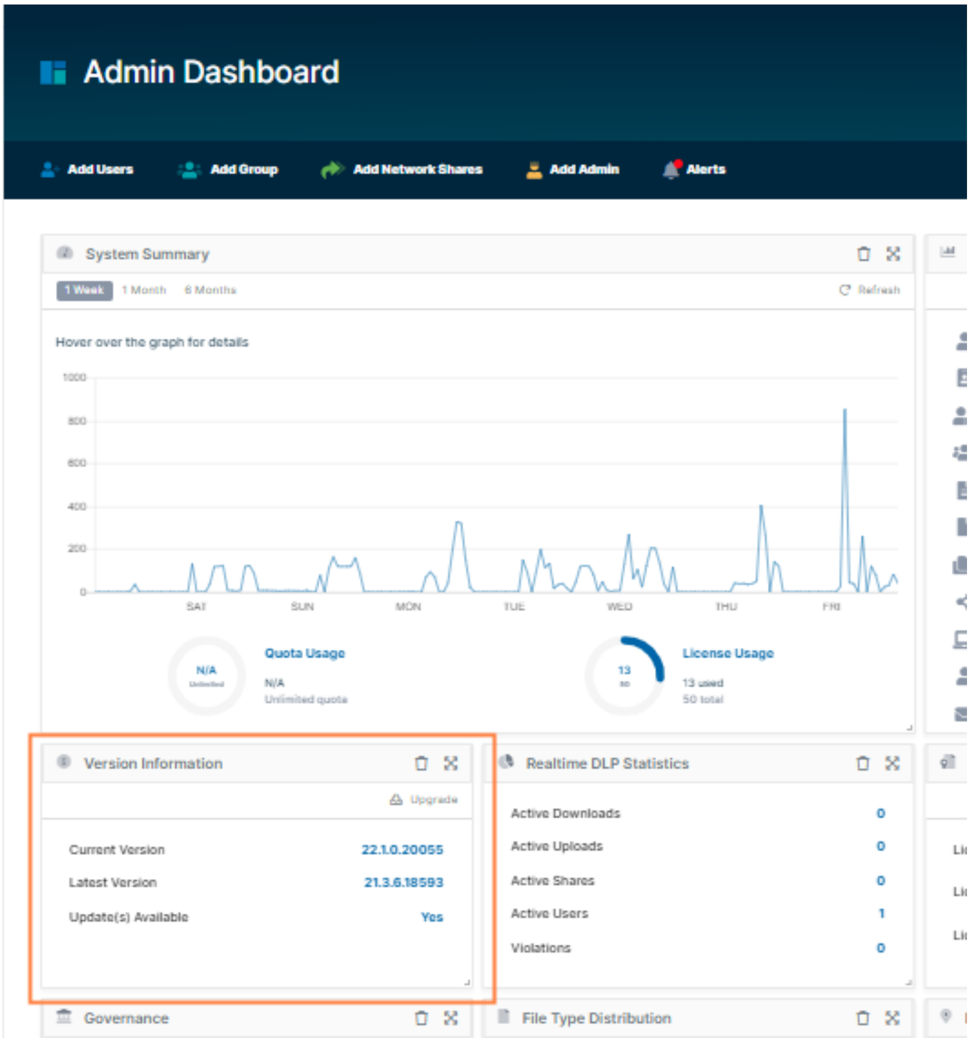
```
service mongod start
```

Routine Maintenance

Routine maintenance helps you keep your FileCloud system updated to the latest version.

Generally, you can find notifications of new FileCloud release availability by:

1. Subscribing to the FileCloud Mailing List.
2. Seeing the version update available in the FileCloud Admin Dashboard.



Current Version	22.1.0.20055
Latest Version	21.3.6.18593
Update(s) Available	Yes

Active Downloads	0
Active Uploads	0
Active Shares	0
Active Users	1
Violations	0

Emergency Maintenance

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

- Take a snapshot of the EBS disk and start an instance from the snapshot.
  or
- If option 1 is not feasible, 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.

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\php.exe -m | findstr mongodb
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 --trim-dot
```

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.
[optional] --trim-dot   For right-to-left languages, removes periods the tool perceives as being in the wrong position and therefore invalid characters. --trim-dot is a flag; it does not have a value.

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[31]to directory 'cloudexport'.

Windows seeding files/folders for multiple users - Default site

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

[31] http://site21.hostedcloud.com

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
```

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
```

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[32] 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. Important: 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 (sample values)

```
aws_storage_bucket = "company.bucket"
aws_storage_folderprefix = "site1"
aws_access_key_id = "AKIAT4YDRDUSRO863KJJ"
aws_secret_access_key = "stPwbS3Y1KrZGUkVbNcYJx+8S/ZZKFROOjUdG9e9"
```

[32] https://docs.aws.amazon.com/cli/latest/userguide/installing.html

```
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 -h default -m C:\temp\migrates3.ini -e  C:\temp\dbexport
```

Contact FileCloud Support for help with this procedure.

Amazon GovCloud AWS Installation

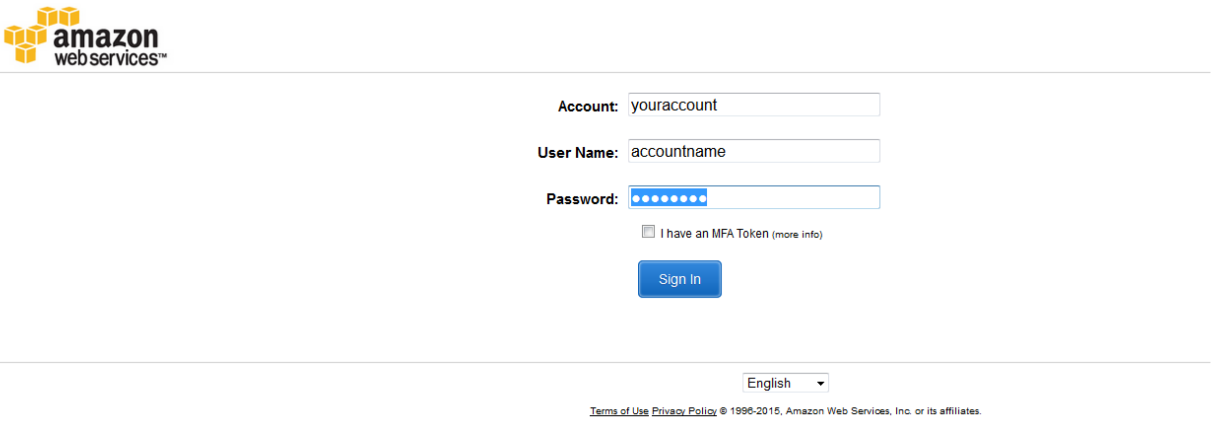
Prerequisite: One needs to have Amazon AWS GovCloud account to use the GovCloud infrastructure. If you are a federal, state govt agency or a US business working with government contracts, you can get AWS GovCloud account from Amazon. You can apply for an Amazon GovCloud account here (https://aws.amazon.com/govcloud-us/contact/). 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, 5, and 6.

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 22.04 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.

Steps to Launch FileCloud AMI on GovCloud

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



Account: youraccount

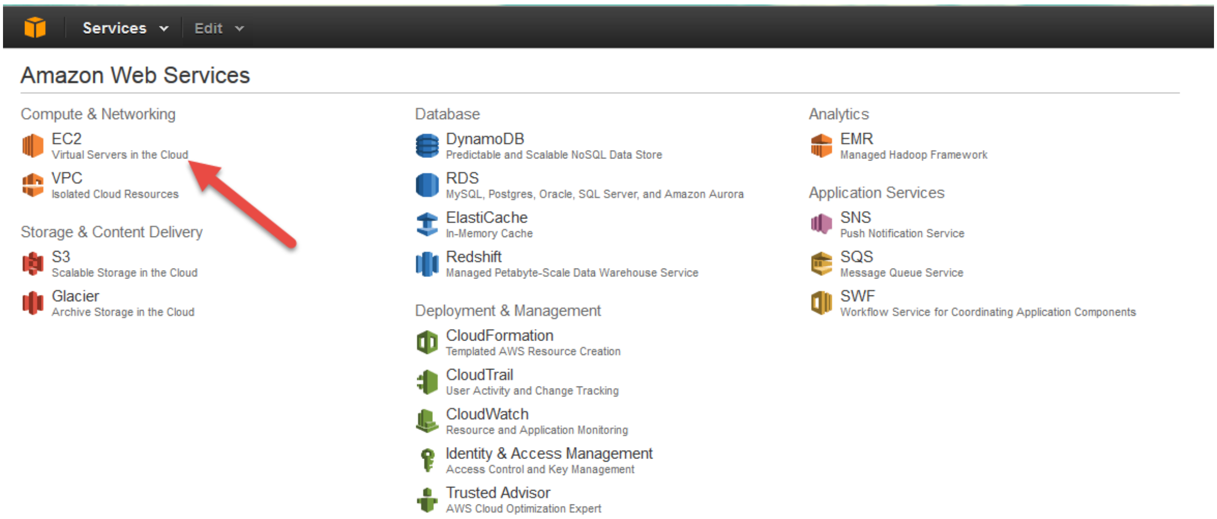
User Name: accountname

Password: ••••••••

□ I have an MFA Token (more info)

Terms of Use Privacy Policy © 1996-2015, Amazon Web Services, Inc. or its affiliates.

2. Click **EC2** (Virtual Servers in the Cloud)



Amazon Web Services

Compute & Networking
- EC2 Virtual Servers in the Cloud
- VPC Isolated Cloud Resources

Storage & Content Delivery
- S3 Scalable Storage in the Cloud
- Glacier Archive Storage in the Cloud

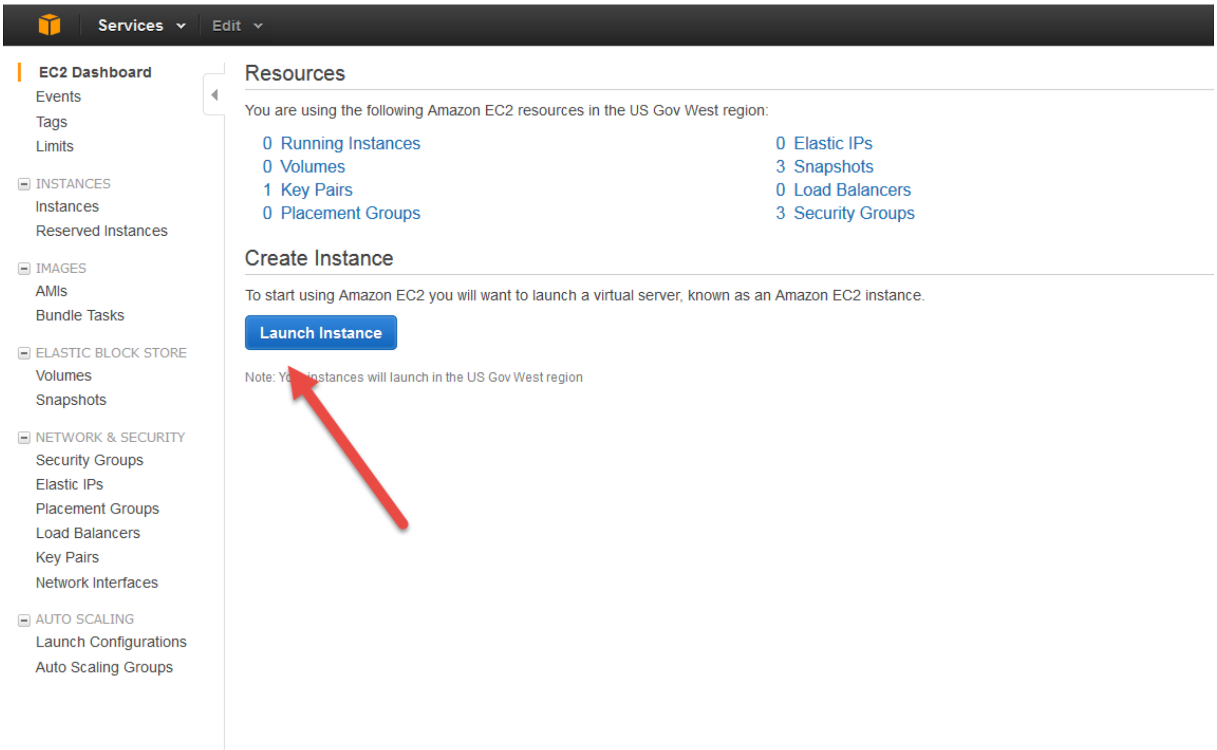
Database
- DynamoDB Predictable and Scalable NoSQL Data Store
- RDS MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora
- ElastiCache In-Memory Cache
- Redshift Managed Petabyte-Scale Data Warehouse Service

Deployment & Management
- CloudFormation Templated AWS Resource Creation
- CloudTrail User Activity and Change Tracking
- CloudWatch Resource and Application Monitoring
- Identity & Access Management Access Control and Key Management
- Trusted Advisor AWS Cloud Optimization Expert

Analytics
- EMR Managed Hadoop Framework

Application Services
- SNS Push Notification Service
- SQS Message Queue Service
- SWF Workflow Service for Coordinating Application Components

3. Click **Launch Instance**



Resources

You are using the following Amazon EC2 resources in the US Gov West region:

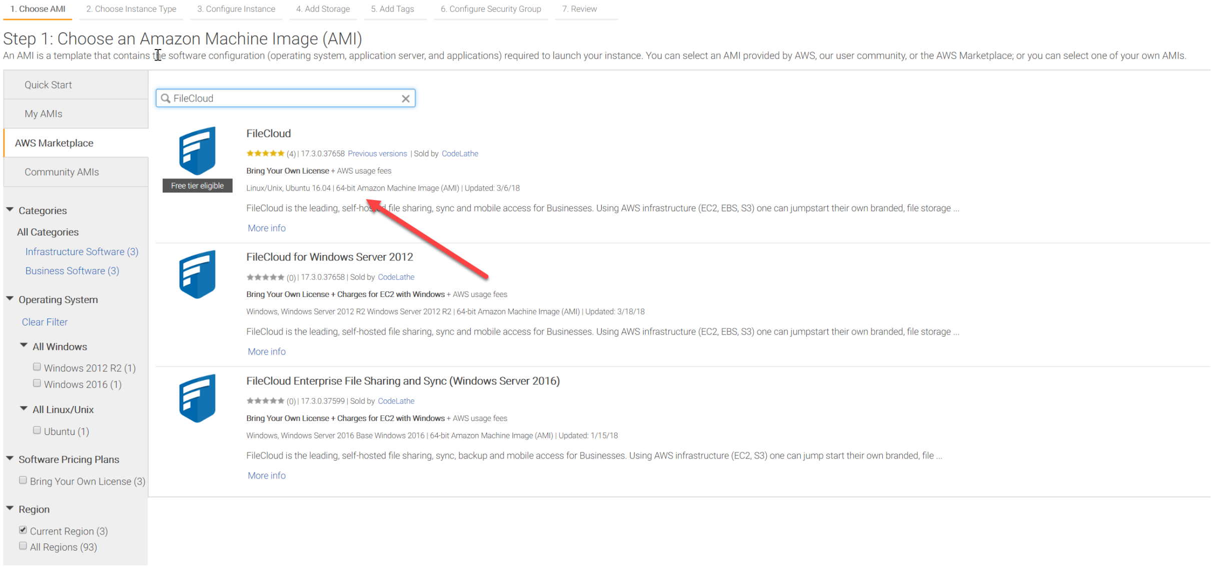
0 Running Instances	0 Elastic IPs
0 Volumes	3 Snapshots
1 Key Pairs	0 Load Balancers
0 Placement Groups	3 Security Groups

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US Gov West region

4. Search **FileCloud AMI** in AWS marketplace



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

FileCloud

FileCloud

★★★★★ (4) | 17.3.0.37658 Previous versions | Sold by CodeLathe

Bring Your Own License + AWS usage fees

Linux/Unix, Ubuntu 16.04 | 64-bit Amazon Machine Image (AMI) | Updated: 3/6/18

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using AWS infrastructure (EC2, EBS, S3) one can jumpstart their own branded, file storage ...

FileCloud for Windows Server 2012

★★★★★ (0) | 17.3.0.37658 | Sold by CodeLathe

Bring Your Own License + Charges for EC2 with Windows + AWS usage fees

Windows, Windows Server 2012 R2 Windows Server 2012 R2 | 64-bit Amazon Machine Image (AMI) | Updated: 3/18/18

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using AWS infrastructure (EC2, EBS, S3) one can jumpstart their own branded, file storage ...

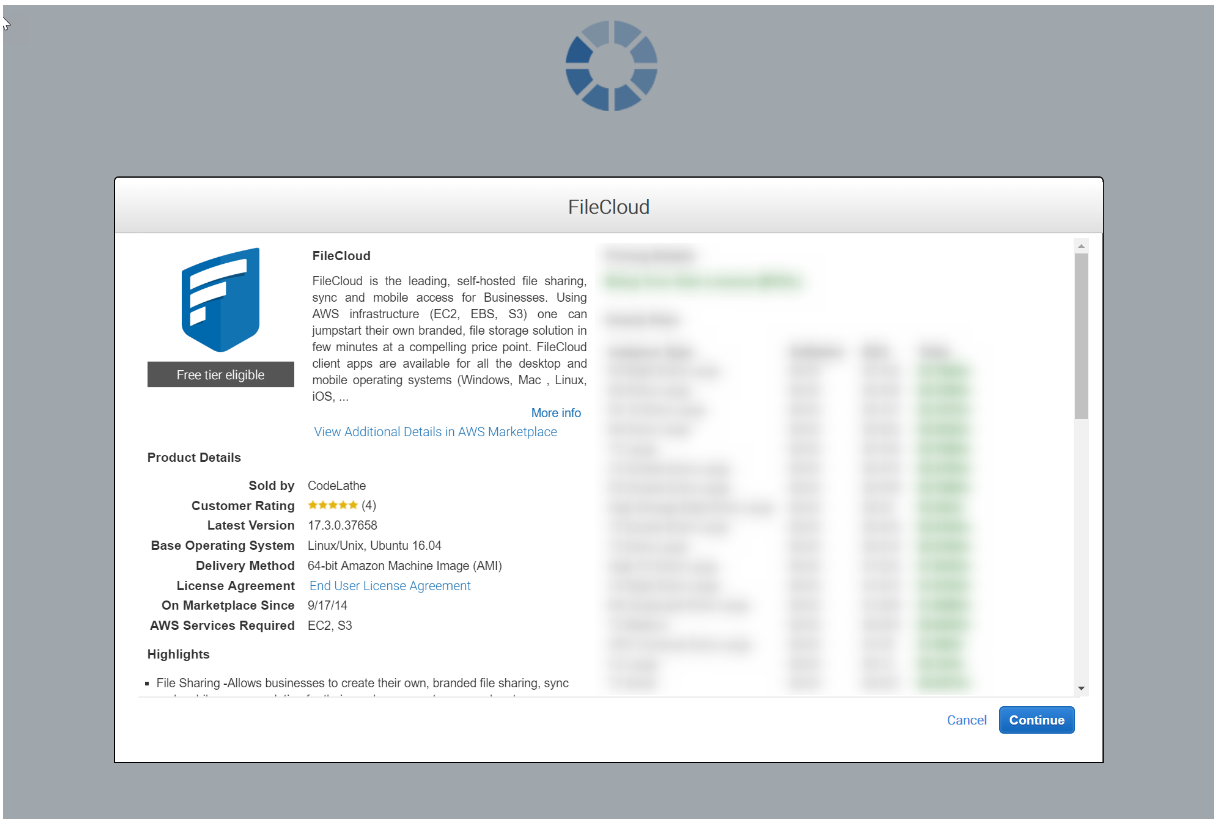
FileCloud Enterprise File Sharing and Sync (Windows Server 2016)

★★★★★ (0) | 17.3.0.37599 | Sold by CodeLathe

Bring Your Own License + Charges for EC2 with Windows + AWS usage fees

Windows, Windows Server 2016 Base Windows 2016 | 64-bit Amazon Machine Image (AMI) | Updated: 1/15/18

FileCloud is the leading, self-hosted file sharing, sync, backup and mobile access for Businesses. Using AWS infrastructure (EC2, S3) one can jump start their own branded, file ...



FileCloud

FileCloud

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. Using AWS infrastructure (EC2, EBS, S3) one can jumpstart their own branded, file storage solution in few minutes at a compelling price point. FileCloud client apps are available for all the desktop and mobile operating systems (Windows, Mac , Linux, iOS, ...

Product Details

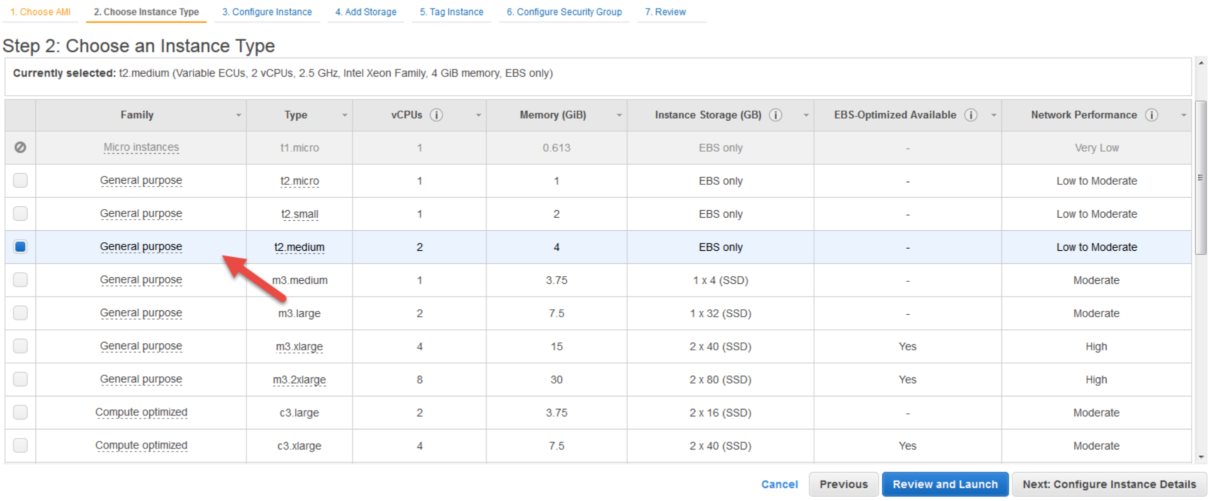
Sold by	CodeLathe
Customer Rating	★★★★★ (4)
Latest Version	17.3.0.37658
Base Operating System	Linux/Unix, Ubuntu 16.04
Delivery Method	64-bit Amazon Machine Image (AMI)
License Agreement	End User License Agreement
On Marketplace Since	9/17/14
AWS Services Required	EC2, S3

Highlights

- File Sharing -Allows businesses to create their own, branded file sharing, sync

and choose **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.

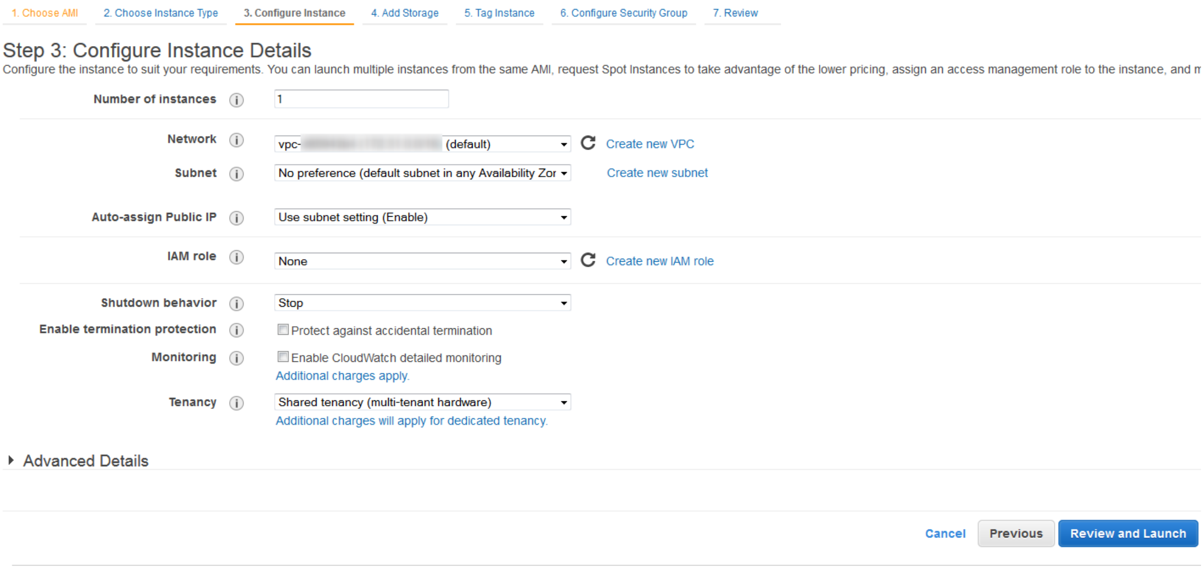


Step 2: Choose an Instance Type

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.5 GHz, Intel Xeon Family, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
⊘	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.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and m

Number of instances: 1

Network: vpc-[redacted] (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zor — Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: None — Create new IAM role

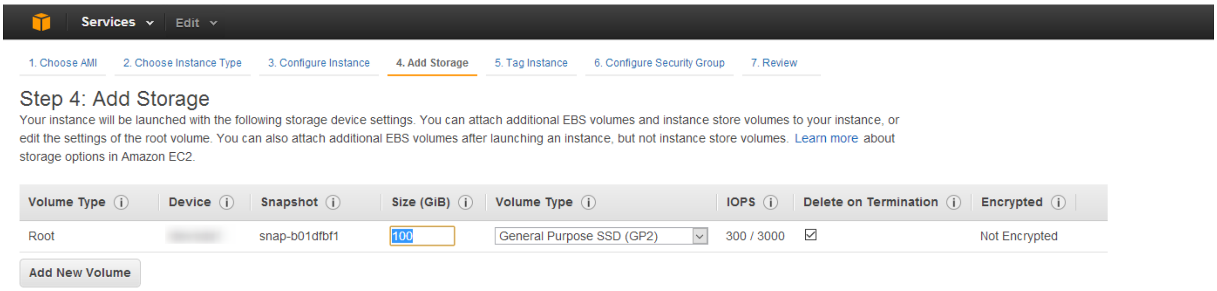
Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared tenancy (multi-tenant hardware)
Additional charges will apply for dedicated tenancy.

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.

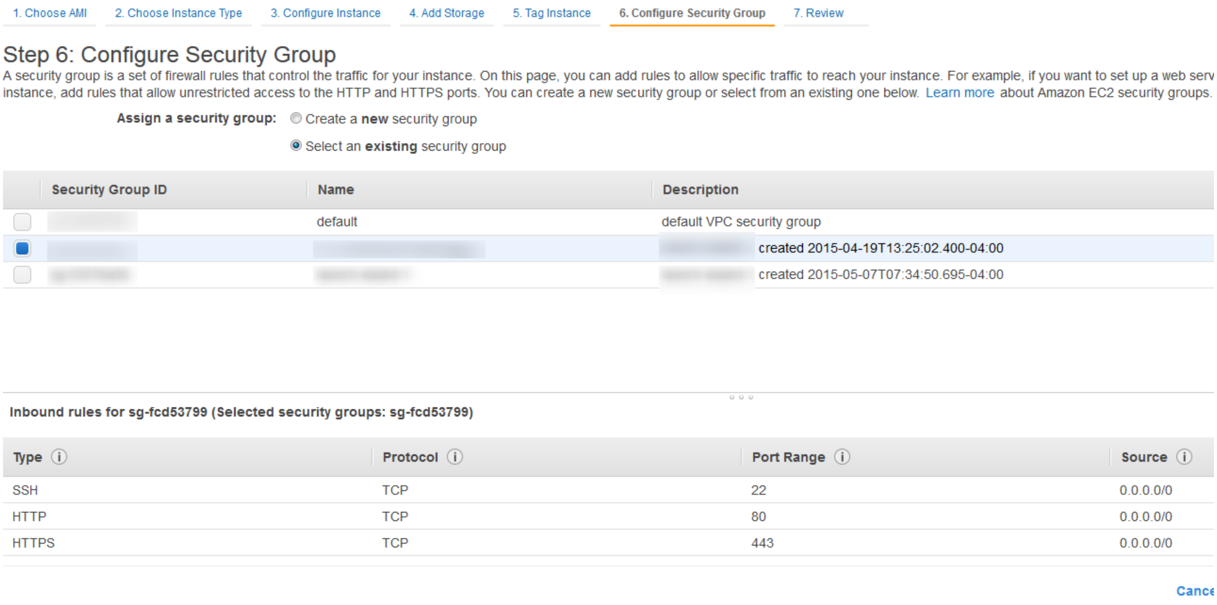


Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	[redacted]	snap-b01dfbf1	100	General Purpose SSD (GP2)	300 / 3000	☑	Not Encrypted

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. Add Storage | 5. Tag Instance | 6. Configure Security Group | 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web serv instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

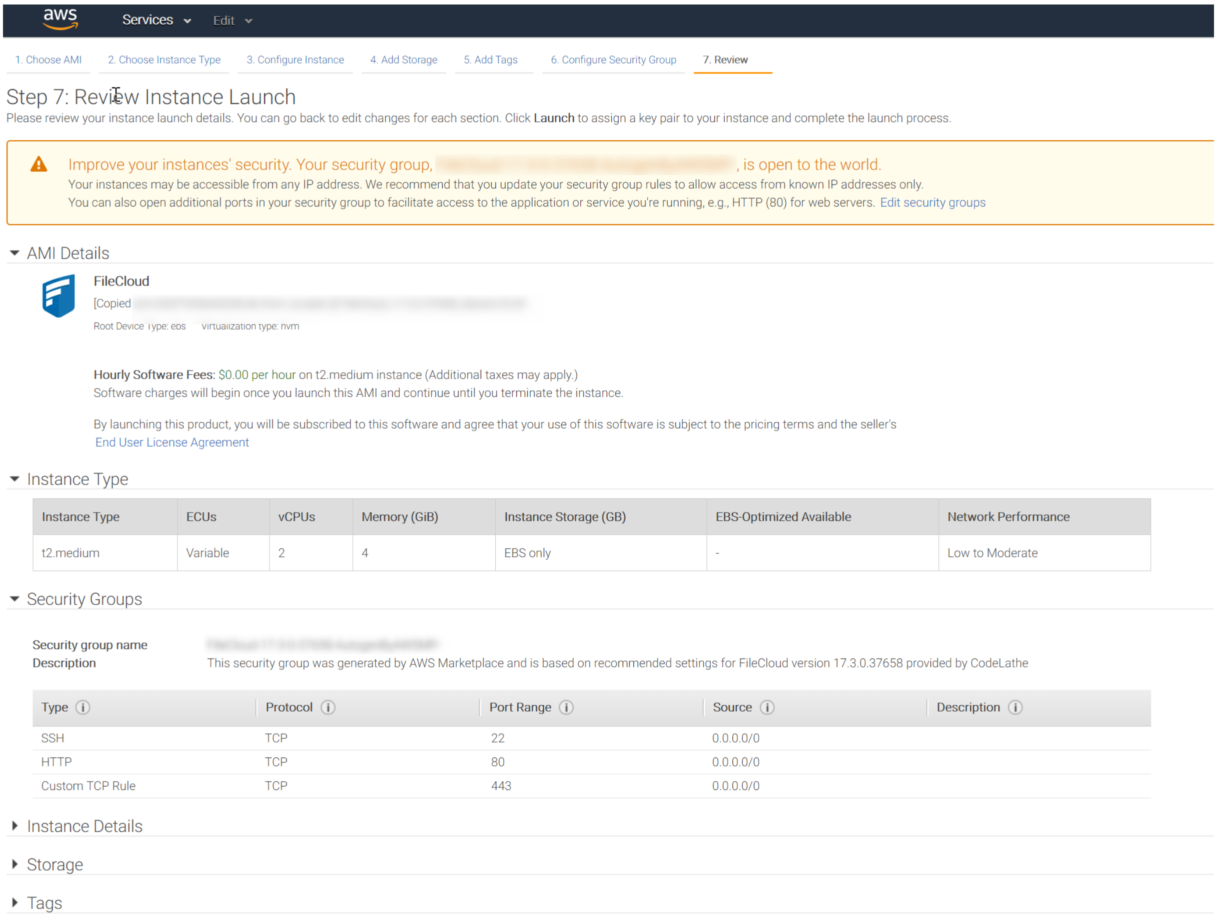
● Select an **existing** security group

	Security Group ID	Name	Description
□	[redacted]	default	default VPC security group
☑	[redacted]	[redacted]	[redacted] created 2015-04-19T13:25:02.400-04:00
□	[redacted]	[redacted]	[redacted] created 2015-05-07T07:34:50.695-04:00

Inbound rules for sg-fcd53799 (Selected security groups: sg-fcd53799)

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH	TCP	22	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

9. Complete the review and launch instance



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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, [redacted], is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

▾ AMI Details

FileCloud
[Copied [redacted]
Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: $0.00 per hour on t2.medium instance (Additional taxes may apply.)
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

▾ Instance 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

▾ Security Groups

Security group name [redacted]
Description This security group was generated by AWS Marketplace and is based on recommended settings for FileCloud version 17.3.0.37658 provided by CodeLathe

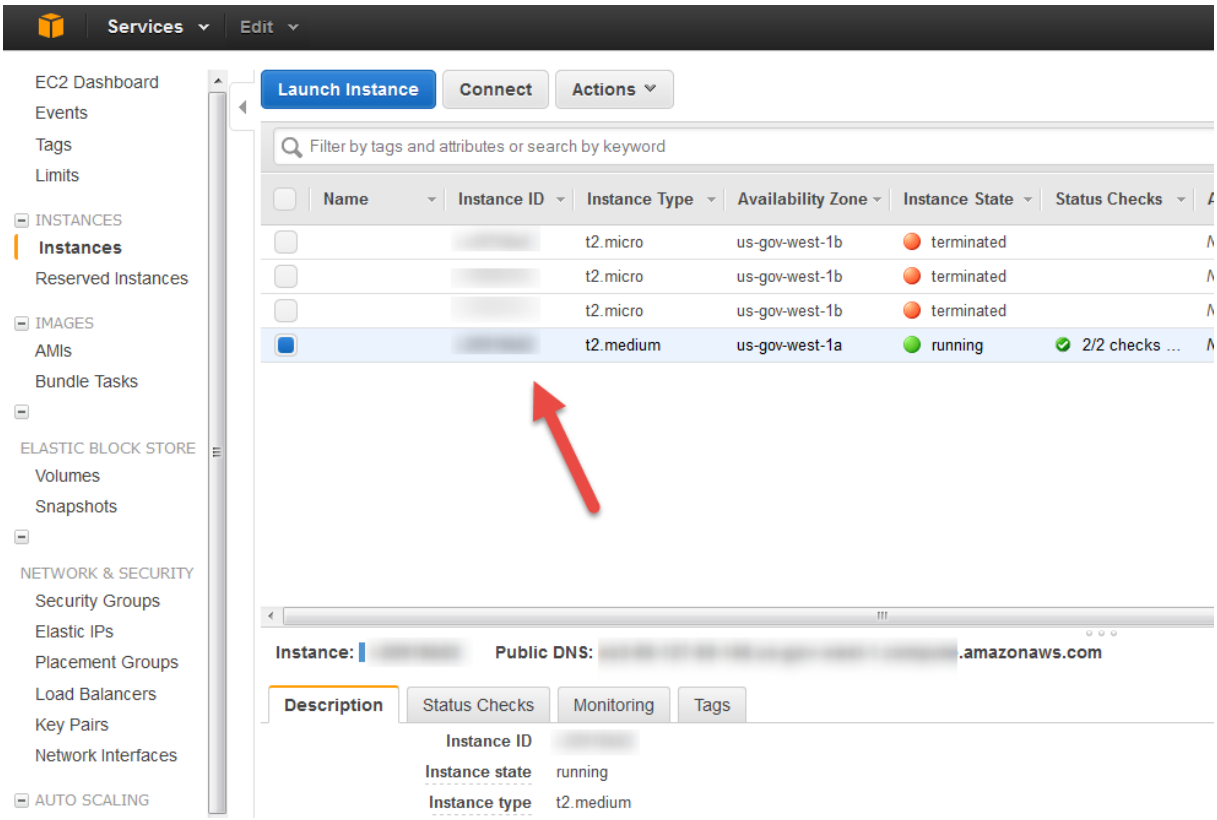
Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	
Custom TCP Rule	TCP	443	0.0.0.0/0	

▸ Instance Details

▸ Storage

▸ Tags

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



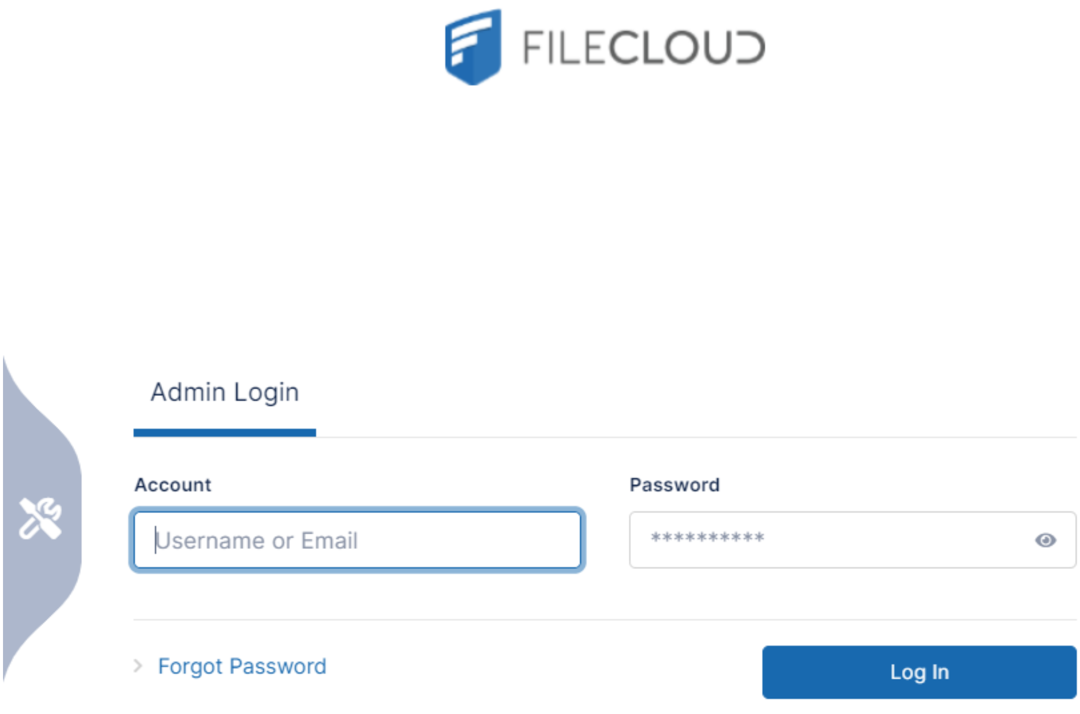
☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	A
☐		[redacted]	t2.micro	us-gov-west-1b	● terminated		N
☐		[redacted]	t2.micro	us-gov-west-1b	● terminated		N
☐		[redacted]	t2.micro	us-gov-west-1b	● terminated		N
■		[redacted]	t2.medium	us-gov-west-1a	● running	✓ 2/2 checks ...	N

Instance: [redacted] Public DNS: [redacted].amazonaws.com

Instance ID	[redacted]
Instance state	running
Instance type	t2.medium

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

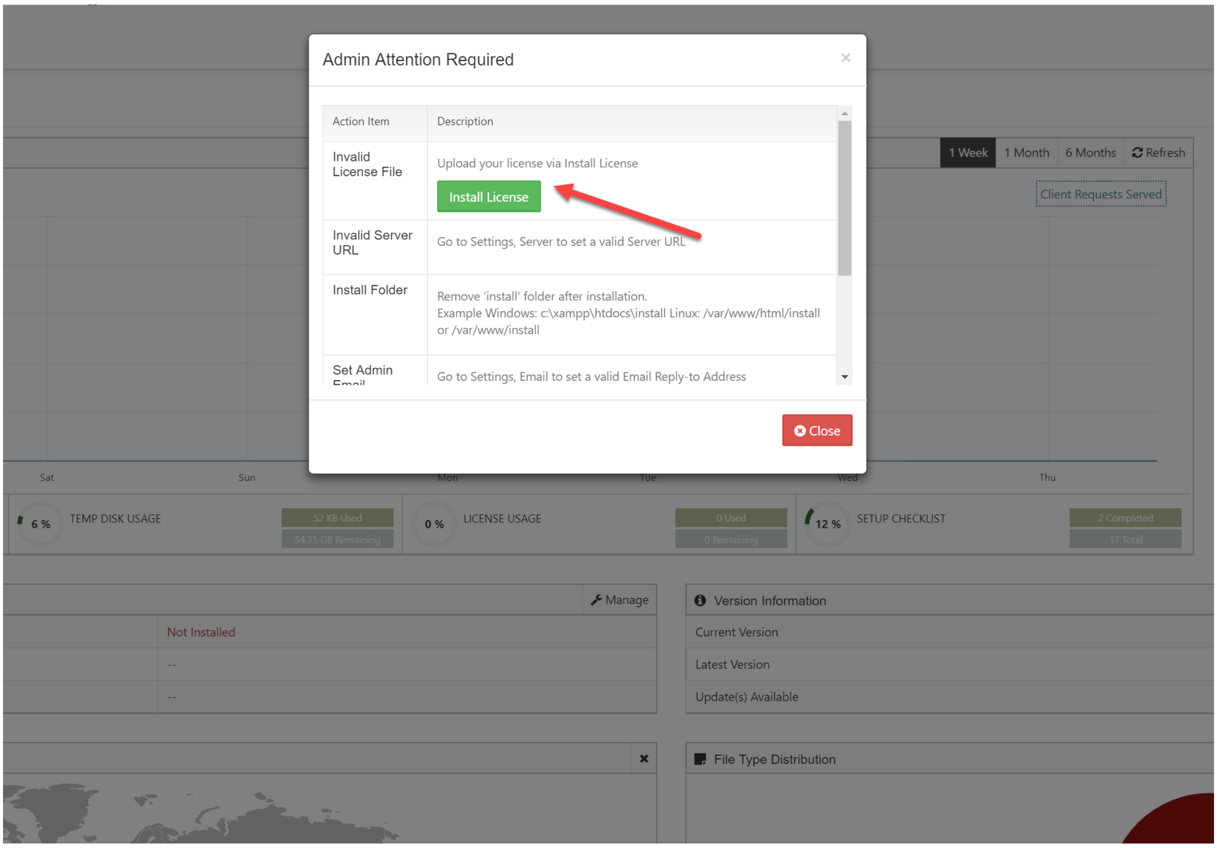
Default Admin	admin
Default Password	Your amazon instance ID
Note	Please change the admin password upon first login.



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.

-



Admin Attention Required

Action Item	Description
Invalid License File	Upload your license via Install License Install License
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\install Linux: /var/www/html/install or /var/www/install
Set Admin Email	Go to Settings, Email to set a valid Email Reply-to Address

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 the 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[33]by addressing their specific regulatory and

[33] http://aws.amazon.com/what-is-cloud-computing/

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 (FedRAMP^{SM}) 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?

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[34](USML).

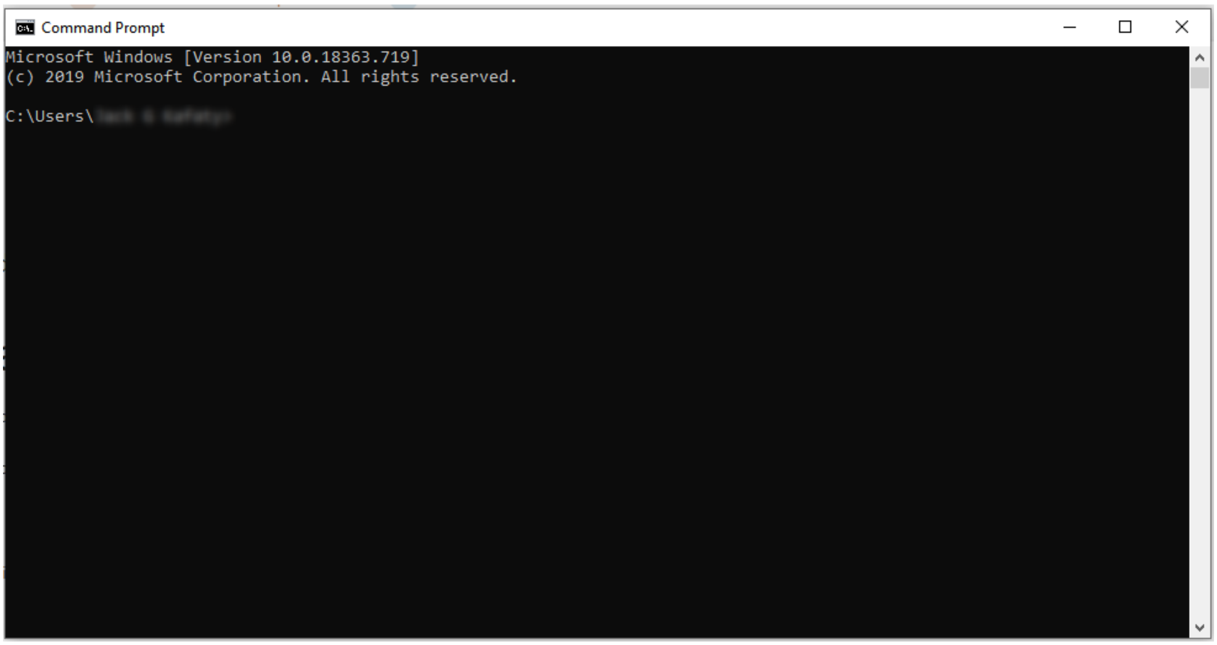
FileCloud Online GovCloud Verification Guide

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:

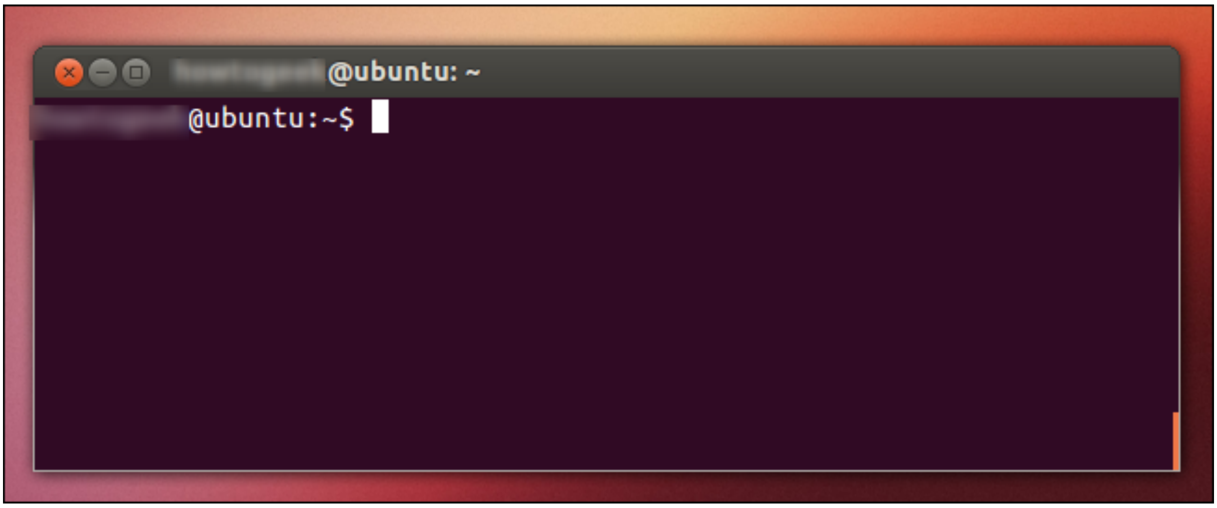
1) In your windows or Linux computer, open the command prompt.
Windows: Windows logo/Search Icon> type CMD> hit Enter.



```
Microsoft Windows [Version 10.0.18363.719]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]
```

[34] http://en.wikipedia.org/wiki/United_States_Munitions_List

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

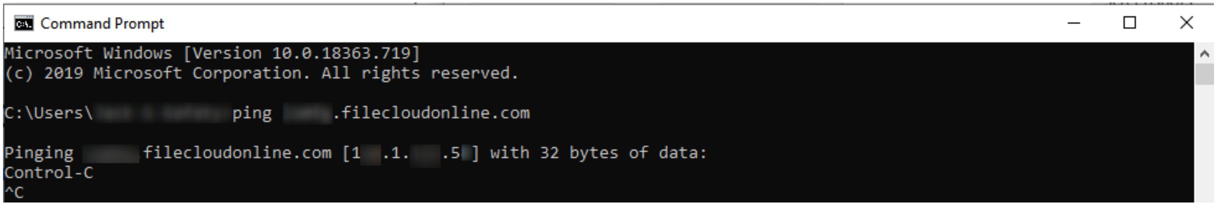


```
[redacted]@ubuntu: ~
[redacted]@ubuntu:~$
```

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[35]

Linux: ping GOVCHECK.filecloudonline.com[36]



```
Microsoft Windows [Version 10.0.18363.719]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]ping [redacted].filecloudonline.com

Pinging [redacted]filecloudonline.com [1[redacted].1.[redacted].5[redacted]] with 32 bytes of data:
Control-C
^C
```

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

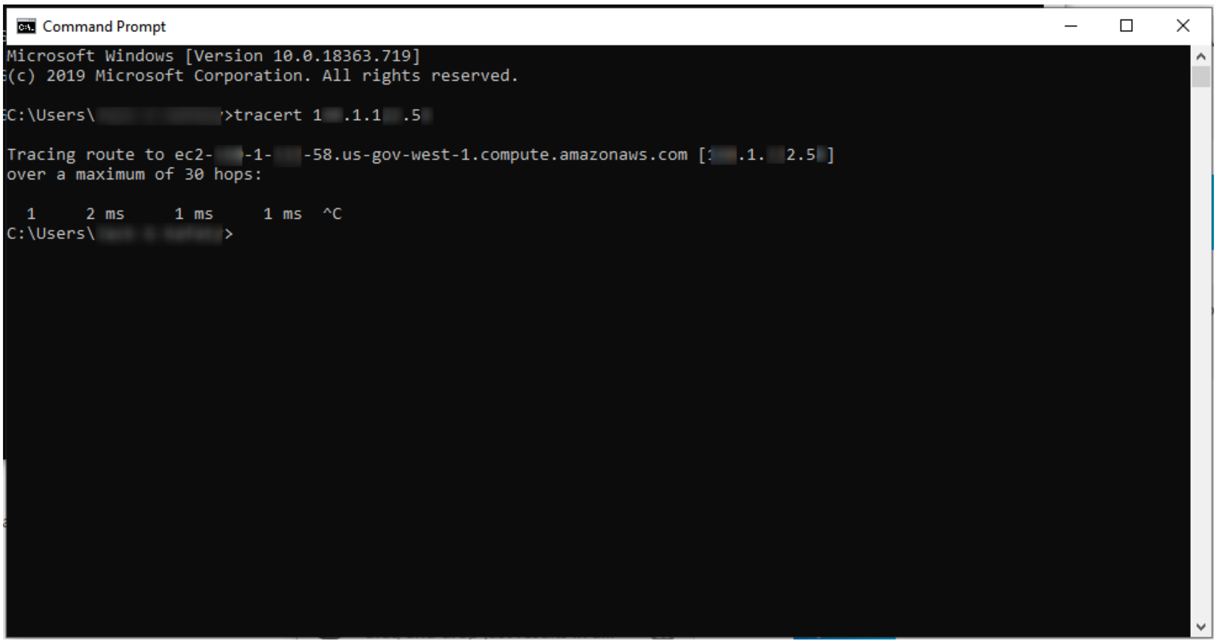
3) Once you have obtained the IP address of your FileCloud you can do a traceroute to verify where your FileCloud is being hosted. This takes about 20 seconds. Once the initial address appears, press **Ctrl + C** at the same time to cancel.

Windows: tracert 52.11.222.333

Linux: traceroute 52.11.222.333

[35] http://GOVCHECK.filecloudonline.com

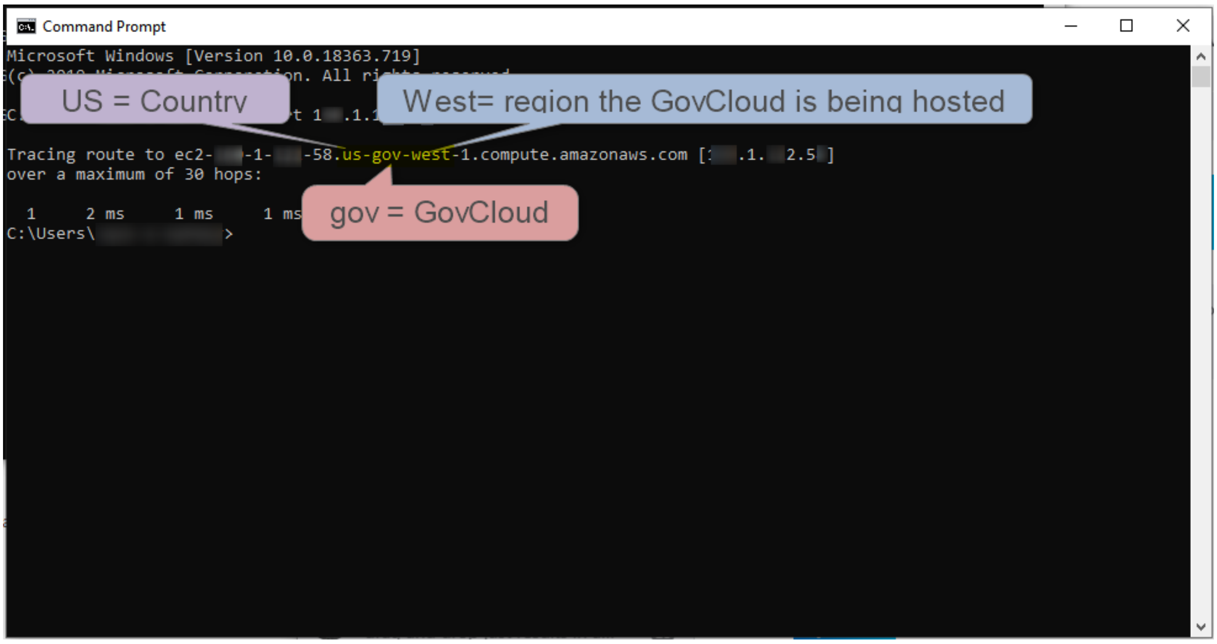
[36] http://GOVCHECK.filecloudonline.com



```
Microsoft Windows [Version 10.0.18363.719]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>tracert 1[redacted].1.1[redacted].5[redacted]

Tracing route to ec2-[redacted]-1-[redacted]-58.us-gov-west-1.compute.amazonaws.com [[redacted].1.[redacted]2.5[redacted]]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  ^C
C:\Users\[redacted]>
```

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

Interpreting the Result



```
Microsoft Windows [Version 10.0.18363.719]
(c                                    n. All ri

C                                t 1[redacted].1.1

Tracing route to ec2-[redacted]-1-[redacted]-58.us-gov-west-1.compute.amazonaws.com [[redacted].1.[redacted]2.5[redacted]]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms
C:\Users\[redacted]>
```

FileCloud Docker installation

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

Running FileCloud on Docker

1. In your Docker server, pull the Docker image:

```
docker pull filecloud/fileclouddocker
```

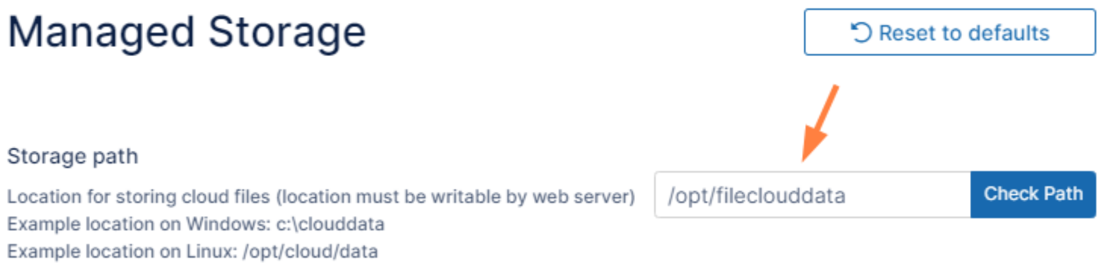
2. Start the container:

```
sudo docker run --privileged -d -p 443:443 -p 80:80 -v fcdata:/opt/fileclouddata
-v dbdata:/var/lib/mongodb -v solrdata:/opt/solrfcdata/var/solr -v htmldata:/var/
www/html --name <yourcontainername> <current_image_name:tag> /lib/systemd/systemd
```

   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**.

3. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   The **Managed Storage settings** page opens by default.

4. Set **Storage Path** to **/opt/fileclouddata**.



Managed Storage

Storage path

Location for storing cloud files (location must be writable by web server)
Example location on Windows: c:\clouddata
Example location on Linux: /opt/cloud/data

/opt/fileclouddata

Setting up LibreOffice preview

Filecloud has two preview methods:

- Built-in web preview
- LibreOffice preview

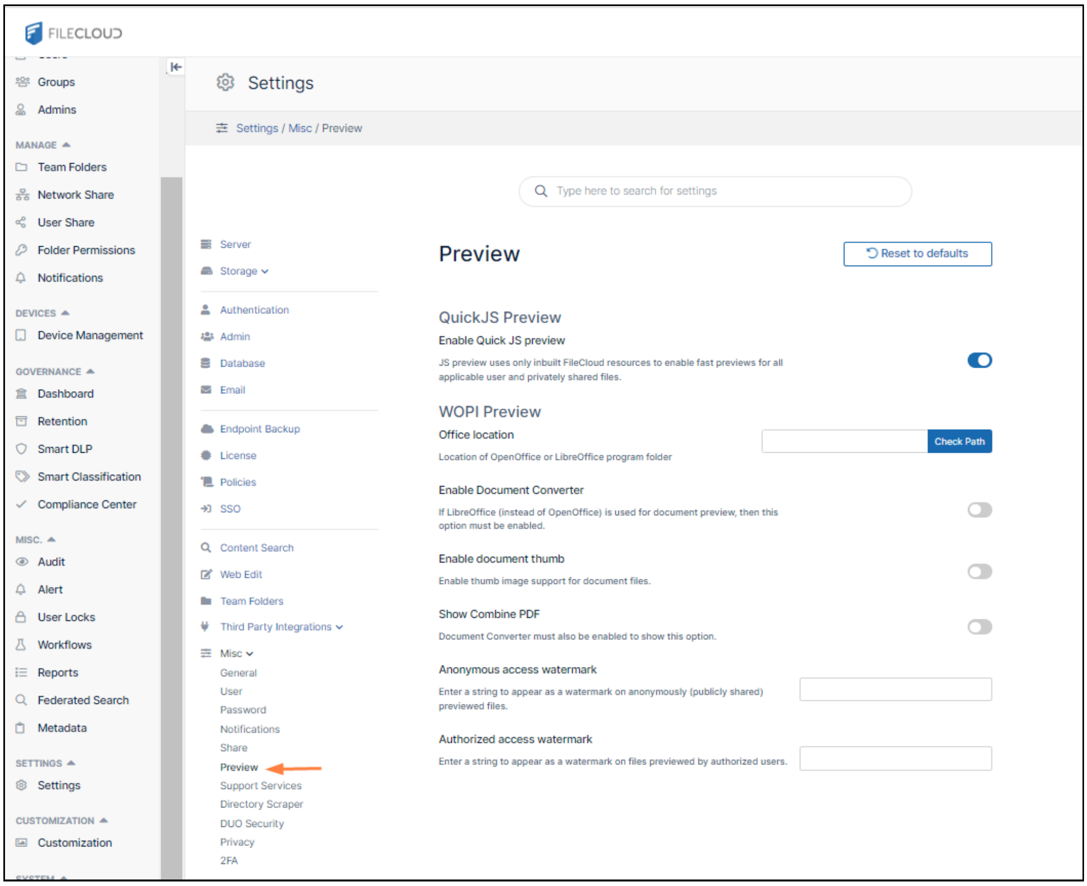
To use LibreOffice

1. Enable preview by entering:

```
docker exec -it <container_id> filecloudcp -p
docker exec -i <container_id> chown www-data /usr/lib/libreoffice/program
```

2. Open the Preview settings page.
   To open the Preview settings page

   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Misc** .
   b. In the inner navigation bar on the left of the **Settings** page, expand the **Misc** menu, and click **Preview**, as shown below.



Preview

QuickJS Preview

Enable Quick JS preview

JS preview uses only inbuilt FileCloud resources to enable fast previews for all applicable user and privately shared files.

WOPI Preview

Office location

Location of OpenOffice or LibreOffice program folder

Enable Document Converter

If LibreOffice (instead of OpenOffice) is used for document preview, then this option must be enabled.

Enable document thumb

Enable thumb image support for document files.

Show Combine PDF

Document Converter must also be enabled to show this option.

Anonymous access watermark

Enter a string to appear as a watermark on anonymously (publicly shared) previewed files.

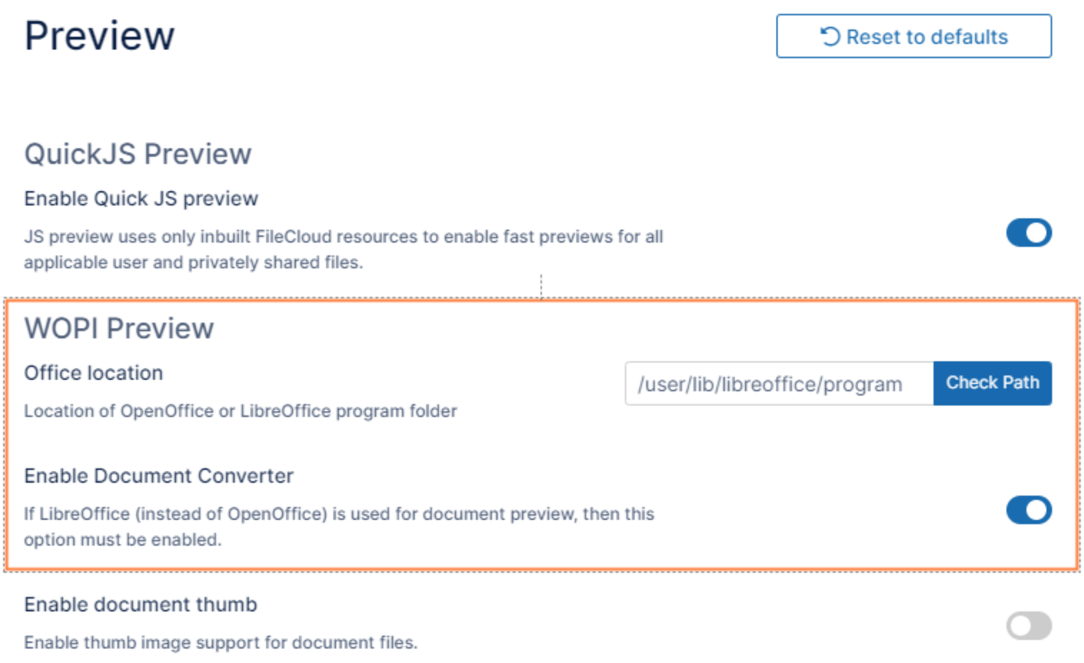
Authorized access watermark

Enter a string to appear as a watermark on files previewed by authorized users.

The **Preview** settings page opens.

3. In **Office Location,** enter **/usr/lib/libreoffice/program**

4. Enable the field **Enable Document Converter**.



Enable Quick JS preview

JS preview uses only inbuilt FileCloud resources to enable fast previews for all applicable user and privately shared files.

Office location

Location of OpenOffice or LibreOffice program folder

/user/lib/libreoffice/program

Enable Document Converter

If LibreOffice (instead of OpenOffice) is used for document preview, then this option must be enabled.

Enable document thumb

Enable thumb image support for document files.

5. Click **Save**.

Configuring Solr

Note: Solr is enabled by

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.

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 7. To upgrade to MongoDB version 7, you must upgrade the Docker image to 23.x.

⚠ 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 <yourcontainername> /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 <yourcontainername>:/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 is stored, as shown in the following commands.
   Please be careful to delete these volumes only.

```
docker volume rm htmldata dbdata
```

5. Pull the latest FileCloud Docker image.

```
docker pull filecloud/fileclouddocker
```

6. Start the container using the freshly pulled Docker image.

```
sudo docker run --privileged -d -p 443:443 -p 80:80 -v fcdata:/opt/fileclouddata
-v dbdata:/var/lib/mongodb -v solrdata:/opt/solrfcdata/var/solr -v htmldata:/var/
www/html --name <yourcontainername> <current_image_name:tag> /lib/systemd/systemd
```

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

```
docker cp dump <yourcontainername>:/
docker exec -i <yourcontainername> /usr/bin/mongorestore --noIndexRestore --drop
```

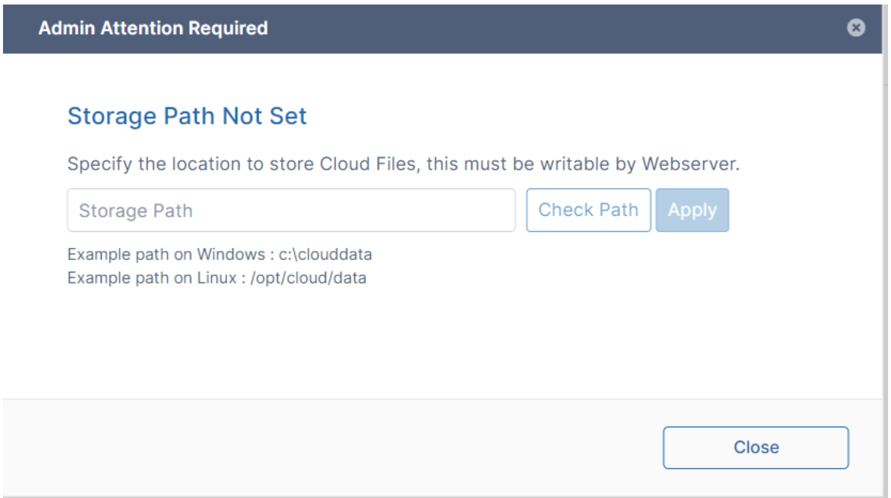
8. Confirm that the container is running.

```
root@docker:/home/nsadm# docker ps -a

CONTAINER ID   IMAGE                                   COMMAND
 CREATED         STATUS            PORTS
                          NAMES
31a8167e2731   filecloud/filecloudserver23.1:latest    "/lib/systemd/..."   3
 minutes ago   Up 23 seconds     0.0.0.0:80->80/tcp, :::80->80/tcp,
0.0.0.0:443->443/tcp, :::443->443/tcp    filecloud.server
```

9. Set the compatibility version for MongoDB to 7.0.

```
root@docker:/home/nsadm# docker exec -it <yourcontainername> bash -c 'mongosh --
eval "db.adminCommand( { setFeatureCompatibilityVersion: \"7.0\" } )"'
```

10. When you log in to FileCloud, if you see the following notification, set **Storage Path** to **/opt/fileclouddata**.



Admin Attention Required

Storage Path Not Set

Specify the location to store Cloud Files, this must be writable by Webserver.

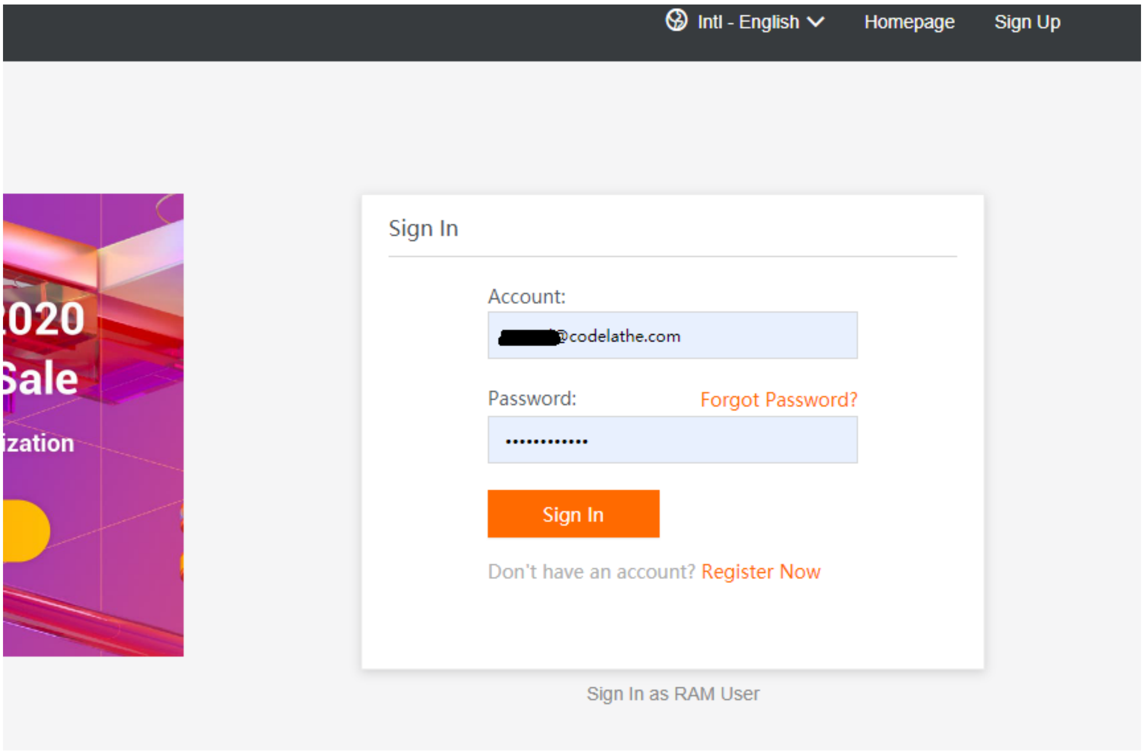
Example path on Windows : c:\clouddata
Example path on Linux : /opt/cloud/data

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

Alibaba Cloud Installation

Steps to Launch FileCloud AMI on GovCloud

1. Log in to your Alibaba Cloud account.



Intl - English

Homepage

Sign Up

Sign In

Account: [redacted]@codelathe.com

Password: ••••••••••••

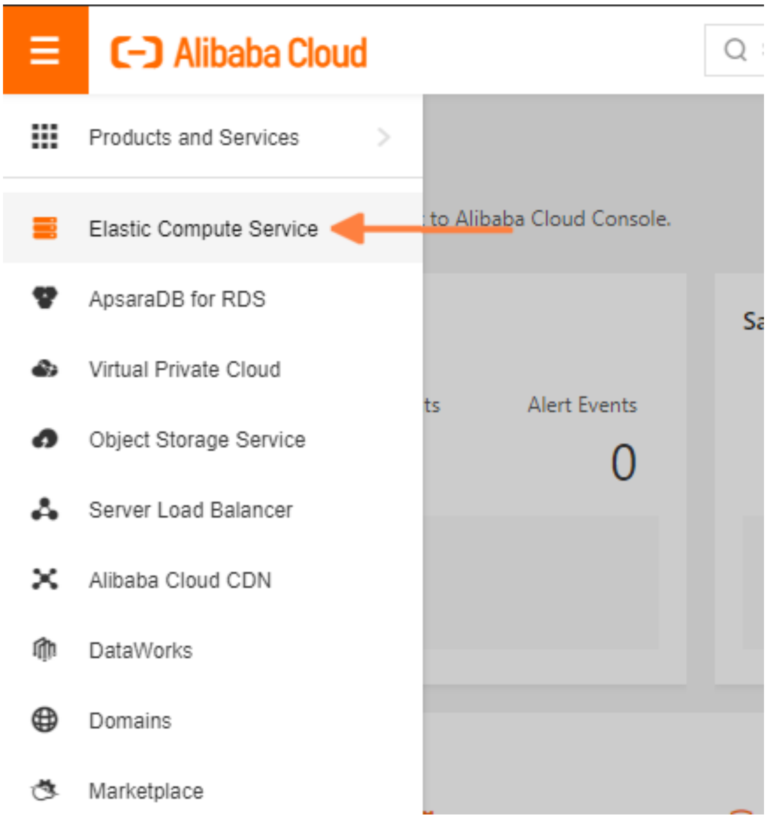
Forgot Password?

Sign In

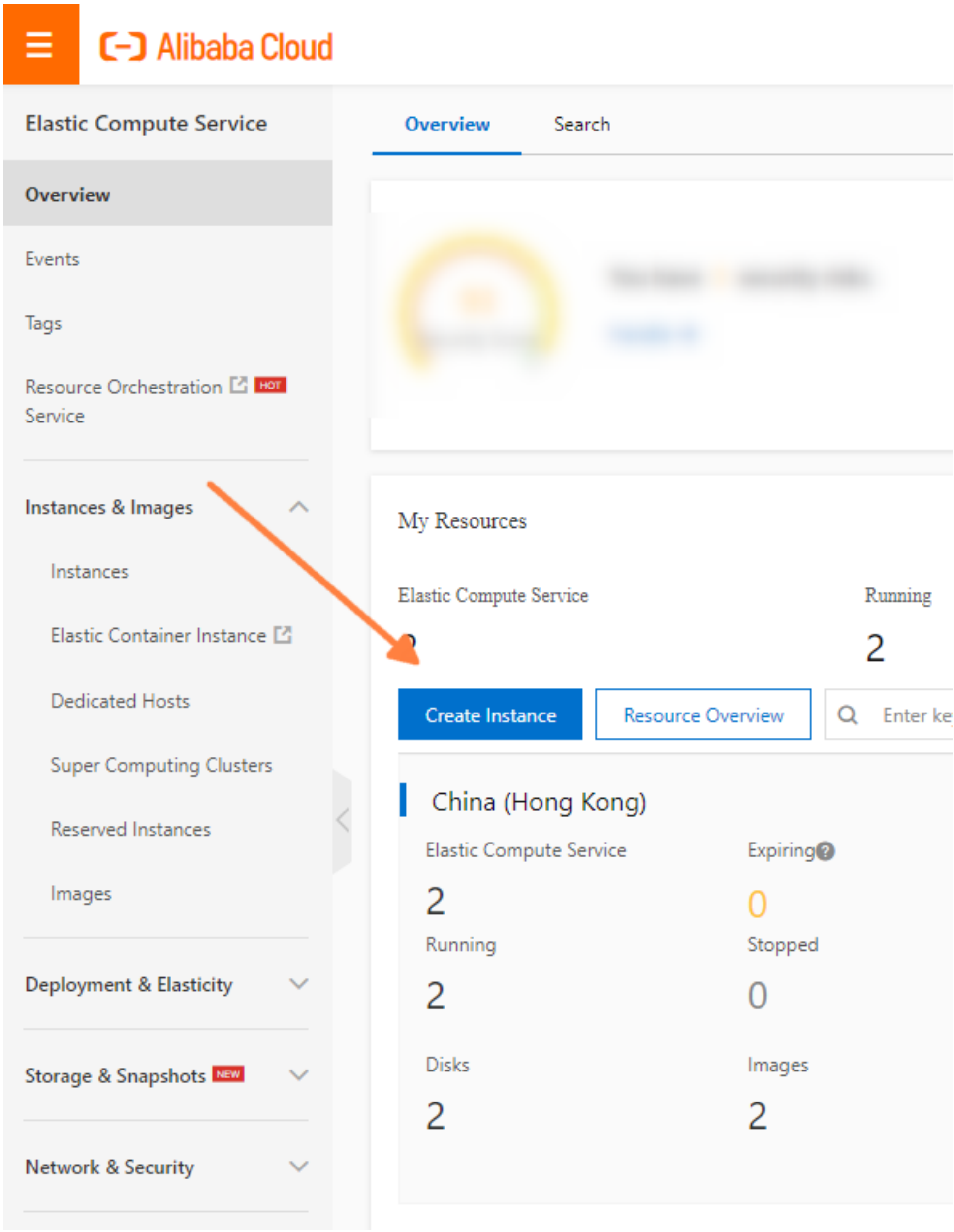
Don't have an account? Register Now

Sign In as RAM User

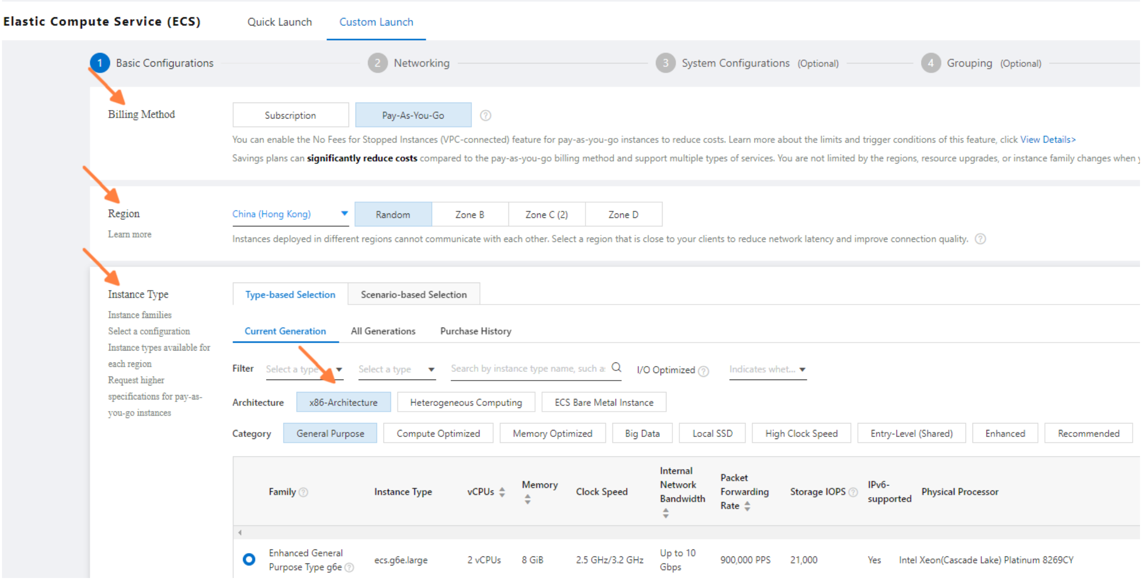
2. Click **Elastic Compute Service.**



3. Click **Create Instance**.



4. Select the **Billing Method** and **Region** as per your requirements.
   For **Instance Type**, select **x86-Architecture**.



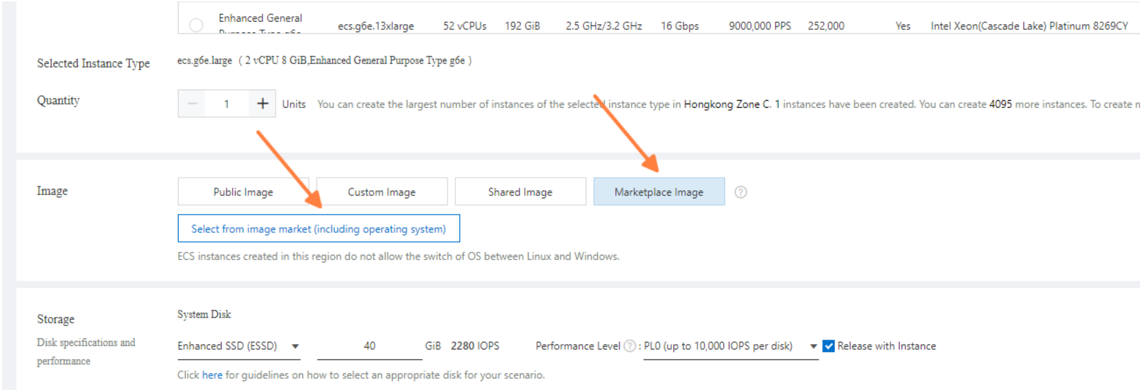
You can enable the No Fees for Stopped Instances (VPC-connected) feature for pay-as-you-go instances to reduce costs. Learn more about the limits and trigger conditions of this feature, click View Details>

Savings plans can **significantly reduce costs** compared to the pay-as-you-go billing method and support multiple types of services. You are not limited by the regions, resource upgrades, or instance family changes when y

Instances deployed in different regions cannot communicate with each other. Select a region that is close to your clients to reduce network latency and improve connection quality.

	Family	Instance Type	vCPUs	Memory	Clock Speed	Internal Network Bandwidth	Packet Forwarding Rate	Storage IOPS	IPv6-supported	Physical Processor
●	Enhanced General Purpose Type g6e	ecs.g6e.large	2 vCPUs	8 GiB	2.5 GHz/3.2 GHz	Up to 10 Gbps	900,000 PPS	21,000	Yes	Intel Xeon(Cascade Lake) Platinum 8269CY

5. Scroll down and select **Marketplace Image** and then click **Select from image market (including operating system)**.



	Family	Instance Type	vCPUs	Memory	Clock Speed	Internal Network Bandwidth	Packet Forwarding Rate	Storage IOPS	IPv6-supported	Physical Processor
○	Enhanced General Purpose Type g6e	ecs.g6e.13xlarge	52 vCPUs	192 GiB	2.5 GHz/3.2 GHz	16 Gbps	9000,000 PPS	252,000	Yes	Intel Xeon(Cascade Lake) Platinum 8269CY

Selected Instance Type: ecs.g6e.large (2 vCPU 8 GiB,Enhanced General Purpose Type g6e)

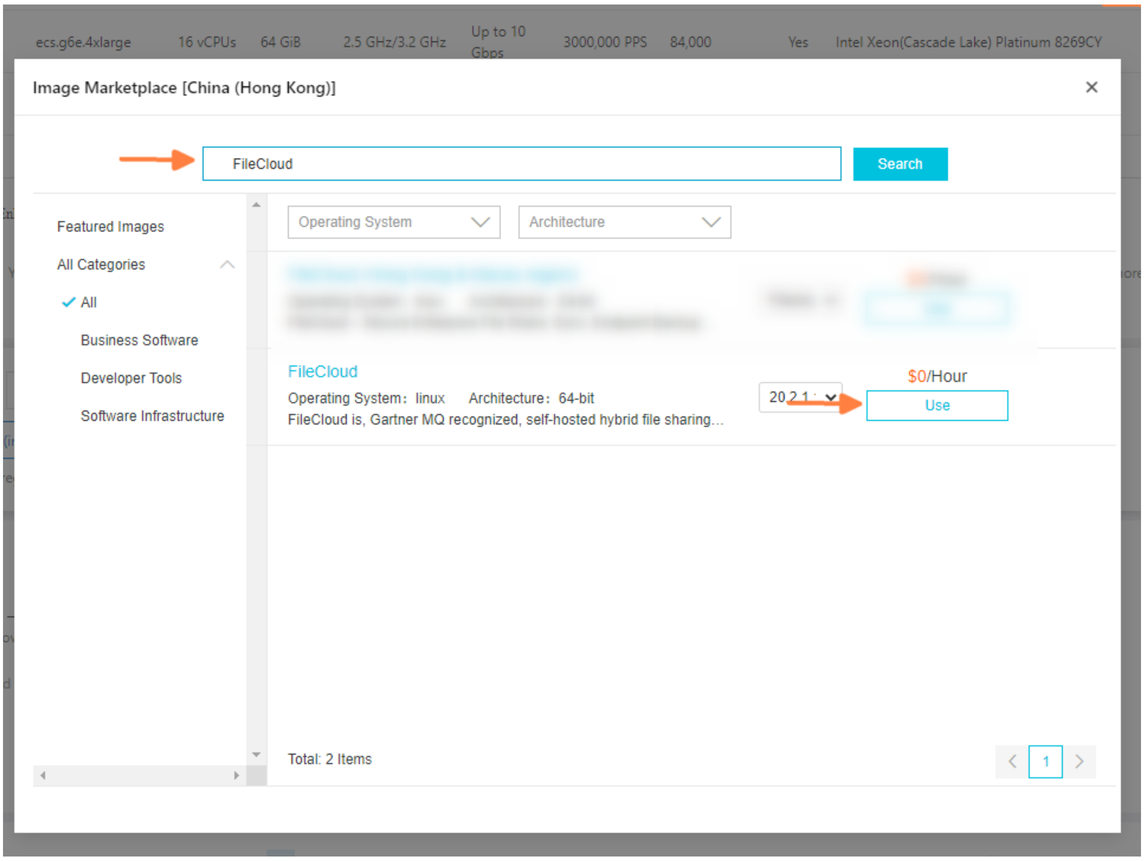
Quantity: 1 Units You can create the largest number of instances of the selected instance type in Hongkong Zone C. 1 instances have been created. You can create 4095 more instances. To create n

ECS instances created in this region do not allow the switch of OS between Linux and Windows.

System Disk: Enhanced SSD (ESSD) 40 GiB 2280 IOPS Performance Level : PL0 (up to 10,000 IOPS per disk) ☑ Release with Instance

Click here for guidelines on how to select an appropriate disk for your scenario.

6. In the **Image Marketplace ...** screen, **search for FileCloud and click Use.**



ecs.g6e.4xlarge 16 vCPUs 64 GiB 2.5 GHz/3.2 GHz Up to 10 Gbps 3000,000 PPS 84,000 Yes Intel Xeon(Cascade Lake) Platinum 8269CY

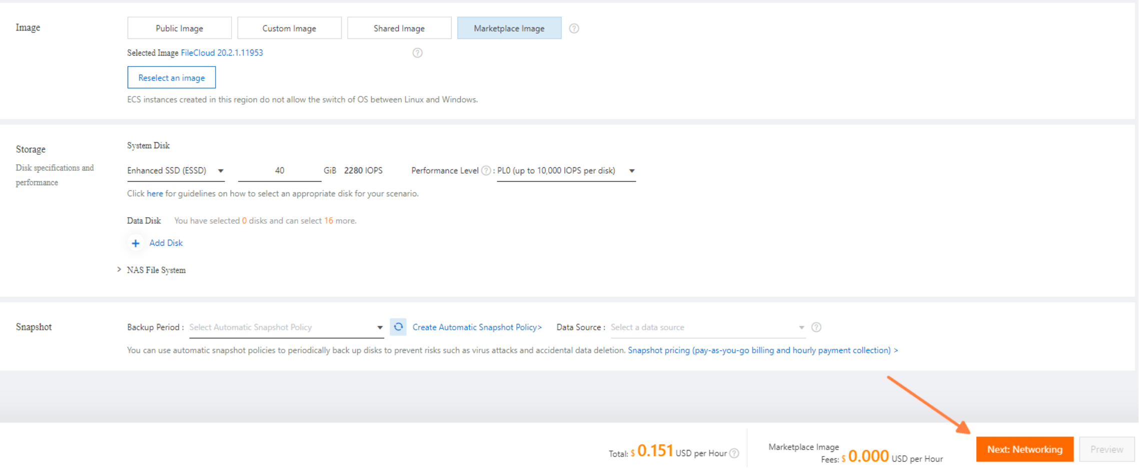
Image Marketplace [China (Hong Kong)]

FileCloud

FileCloud
Operating System： linux Architecture： 64-bit
FileCloud is, Gartner MQ recognized, self-hosted hybrid file sharing…
20.2.1
$0/Hour

Total: 2 Items

7. Select the desired storage configuration (you can use the defaults provided by Alibaba), then click **Next: Networking**.



Image

Selected Image FileCloud 20.2.1.11953

ECS instances created in this region do not allow the switch of OS between Linux and Windows.

Storage
Disk specifications and performance

System Disk
Enhanced SSD (ESSD) 40 GiB 2280 IOPS Performance Level : PL0 (up to 10,000 IOPS per disk)
Click here for guidelines on how to select an appropriate disk for your scenario.

Data Disk You have selected 0 disks and can select 16 more.

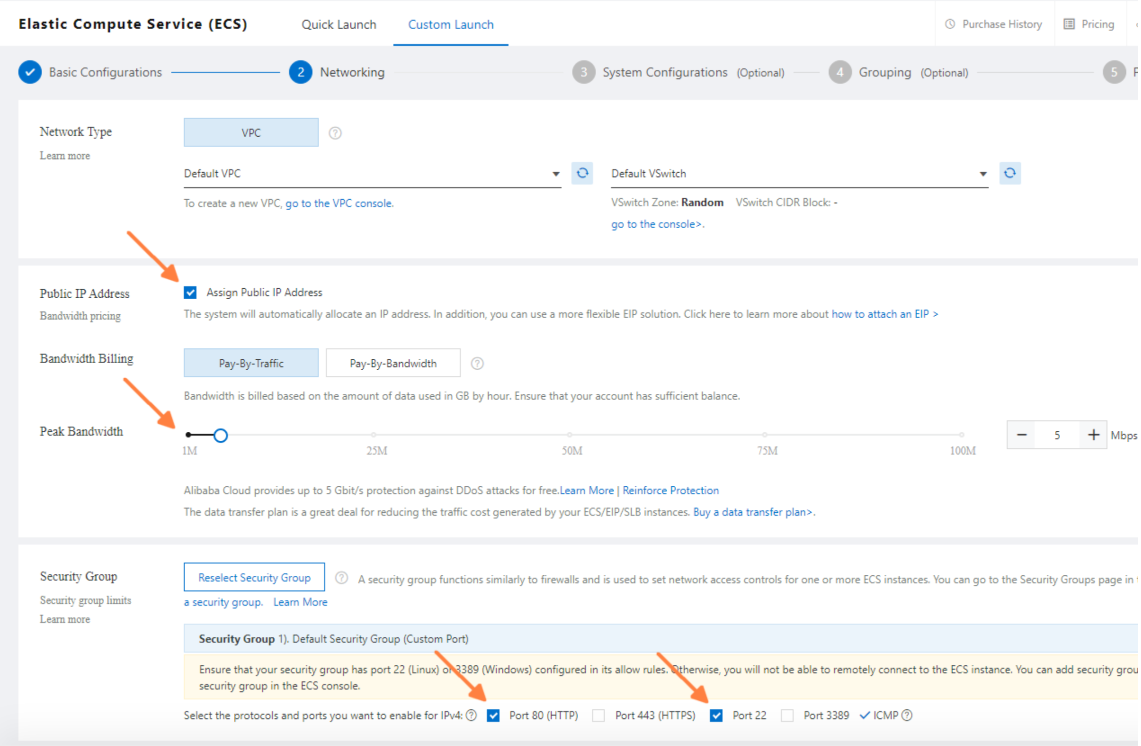
Snapshot

Backup Period : Select Automatic Snapshot Policy Create Automatic Snapshot Policy> Data Source : Select a data source
You can use automatic snapshot policies to periodically back up disks to prevent risks such as virus attacks and accidental data deletion. Snapshot pricing (pay-as-you-go billing and hourly payment collection) >

Total: $ 0.151 USD per Hour
Marketplace Image Fees: $ 0.000 USD per Hour

8. if the server is to be accessed publicly, check **Assign Public IP Address**.
   Set **Peak Bandwidth** according to your requirements.
   Select **Port 80 (HTTP)** and **Port 22** to enable IPv4.

You can change this after setup is completed.



Elastic Compute Service (ECS) Quick Launch Custom Launch Purchase History Pricing

✓ Basic Configurations 2 Networking 3 System Configurations (Optional) 4 Grouping (Optional) 5

Network Type
Learn more

VPC

Default VPC | Default VSwitch

To create a new VPC, go to the VPC console.

VSwitch Zone: **Random** VSwitch CIDR Block: -
go to the console>.

Public IP Address
Bandwidth pricing

☑ Assign Public IP Address

The system will automatically allocate an IP address. In addition, you can use a more flexible EIP solution. Click here to learn more about how to attach an EIP >

Bandwidth Billing

Pay-By-Traffic | Pay-By-Bandwidth

Bandwidth is billed based on the amount of data used in GB by hour. Ensure that your account has sufficient balance.

Peak Bandwidth

Alibaba Cloud provides up to 5 Gbit/s protection against DDoS attacks for free.Learn More | Reinforce Protection

The data transfer plan is a great deal for reducing the traffic cost generated by your ECS/EIP/SLB instances. Buy a data transfer plan>.

Security Group
Security group limits
Learn more

Reselect Security Group

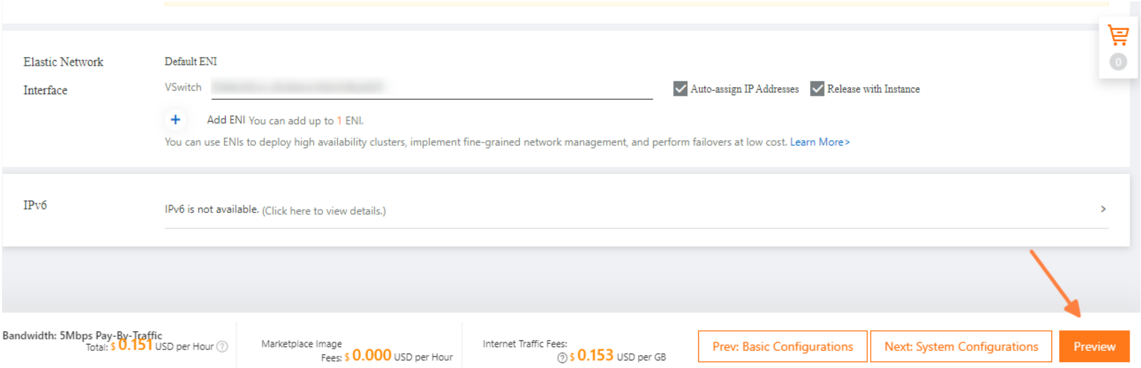
A security group functions similarly to firewalls and is used to set network access controls for one or more ECS instances. You can go to the Security Groups page in
a security group. Learn More

Security Group 1). Default Security Group (Custom Port)

Ensure that your security group has port 22 (Linux) or 3389 (Windows) configured in its allow rules. Otherwise, you will not be able to remotely connect to the ECS instance. You can add security grou
security group in the ECS console.

Select the protocols and ports you want to enable for IPv4: ☑ Port 80 (HTTP) □ Port 443 (HTTPS) ☑ Port 22 □ Port 3389 ✓ ICMP

9. Click **Preview** after you have selected the ports to allow.



Elastic Network Interface

Default ENI
VSwitch [redacted] ☑ Auto-assign IP Addresses ☑ Release with Instance

+ Add ENI You can add up to 1 ENI.

You can use ENIs to deploy high availability clusters, implement fine-grained network management, and perform failovers at low cost. Learn More>

IPv6

IPv6 is not available. (Click here to view details.)

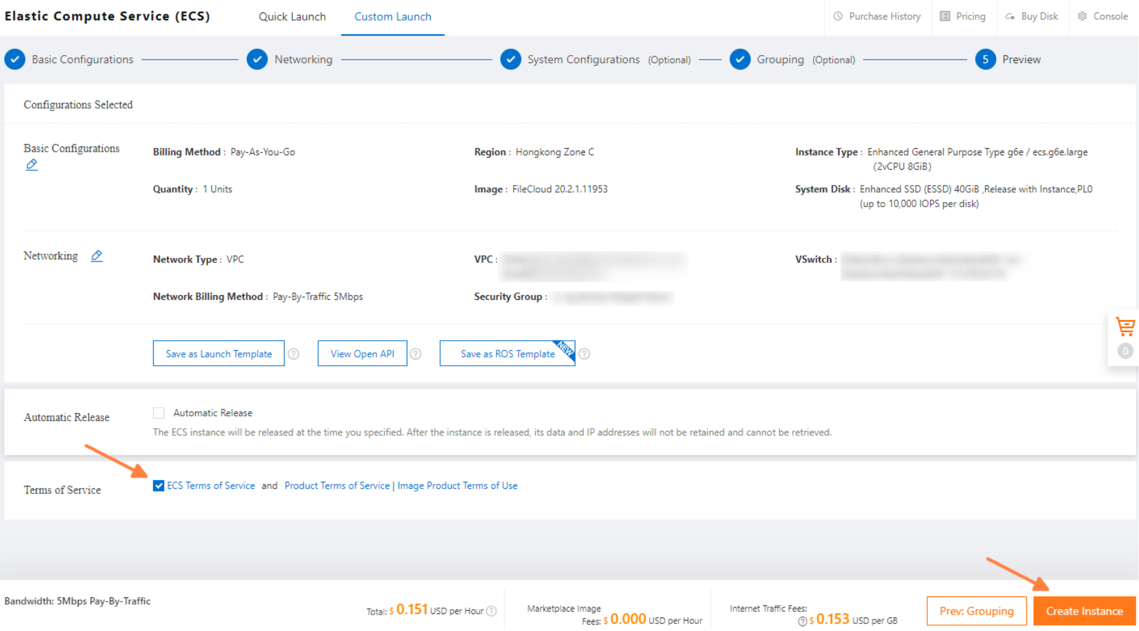
Bandwidth: 5Mbps Pay-By-Traffic
Total: $ 0.151 USD per Hour

Marketplace Image
Fees: $ 0.000 USD per Hour

Internet Traffic Fees:
$ 0.153 USD per GB

Prev: Basic Configurations | Next: System Configurations | Preview

10. Review your settings.
Check **ECS Terms of Service**, and click **Create Instance** to launch the instance.



Configurations Selected

Basic Configurations

Billing Method : Pay-As-You-Go

Quantity : 1 Units

Region : Hongkong Zone C

Image : FileCloud 20.2.1.11953

Instance Type : Enhanced General Purpose Type g6e / ecs.g6e.large (2vCPU 8GiB)

System Disk : Enhanced SSD (ESSD) 40GiB ,Release with Instance,PL0 (up to 10,000 IOPS per disk)

Networking

Network Type : VPC

Network Billing Method : Pay-By-Traffic 5Mbps

VPC : [redacted]

Security Group : [redacted]

VSwitch : [redacted]

Automatic Release

□ Automatic Release

The ECS instance will be released at the time you specified. After the instance is released, its data and IP addresses will not be retained and cannot be retrieved.

Terms of Service

☑ ECS Terms of Service and Product Terms of Service | Image Product Terms of Use

Bandwidth: 5Mbps Pay-By-Traffic

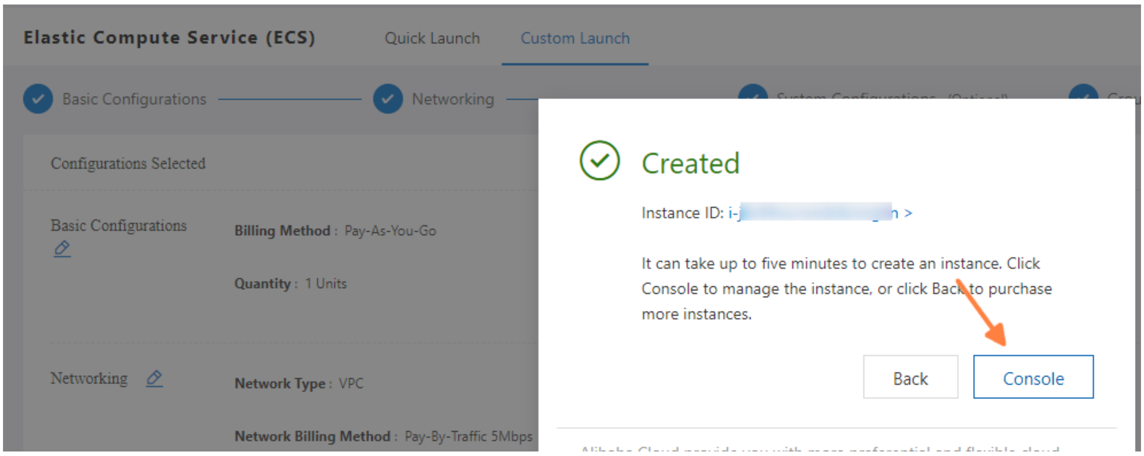
Total: $ 0.151 USD per Hour

Marketplace Image Fees: $ 0.000 USD per Hour

Internet Traffic Fees: $ 0.153 USD per GB

A confirmation box indicates that the instance has been created.

11. Click **Console** to open the **Instances** screen.



Configurations Selected

Basic Configurations

Billing Method : Pay-As-You-Go

Quantity : 1 Units

Networking

Network Type : VPC

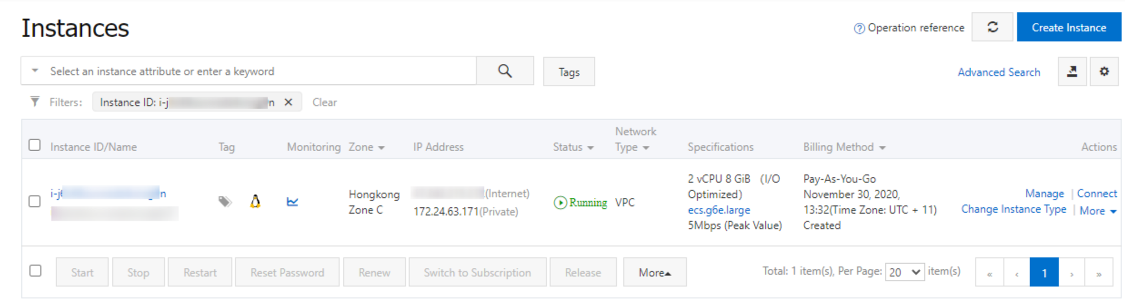
Network Billing Method : Pay-By-Traffic 5Mbps

Created

Instance ID: i-[redacted]n >

It can take up to five minutes to create an instance. Click Console to manage the instance, or click Back to purchase more instances.

12. Confirm that FileCloud is running in your Alibaba **Instances** dashboard. Please note the public **IP Address** and **Instance ID** to access your FileCloud server.



Instances

Operation reference | Create Instance

Select an instance attribute or enter a keyword | Tags | Advanced Search

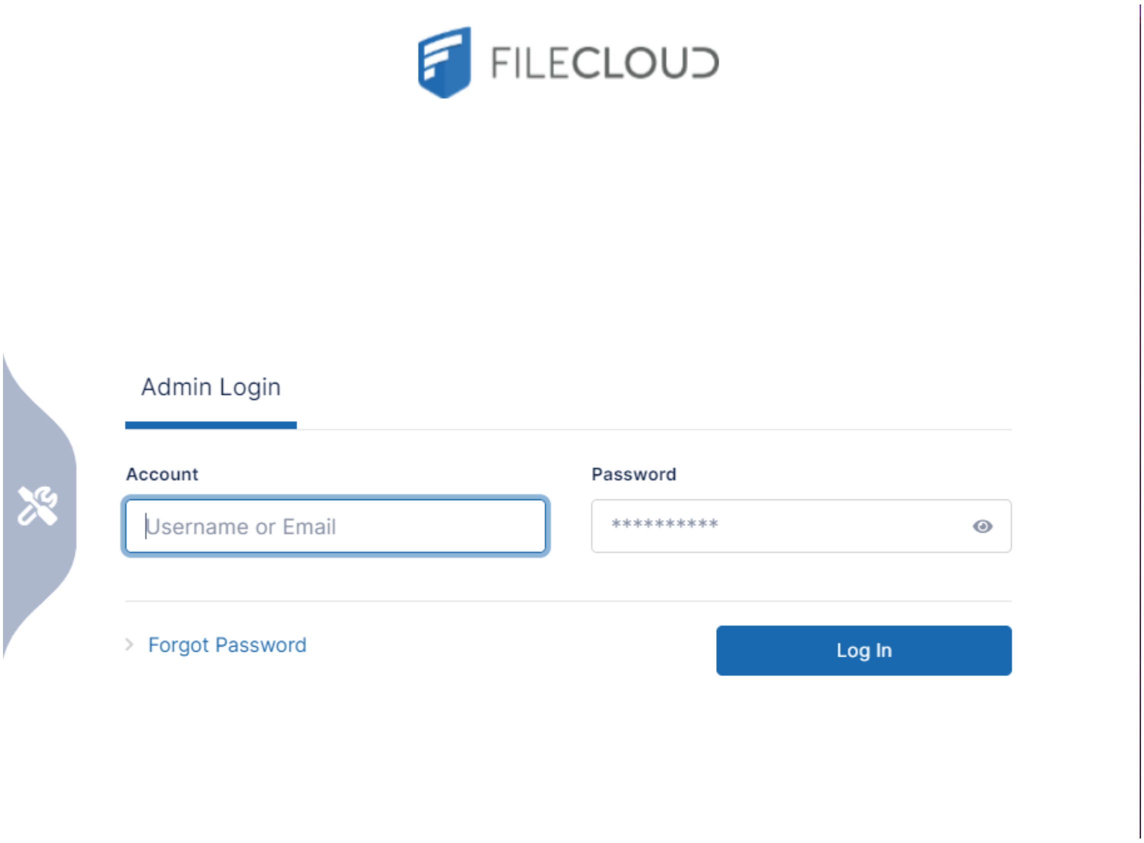
Filters: Instance ID: i-j[redacted]n ✕ Clear

□	Instance ID/Name	Tag	Monitoring	Zone	IP Address	Status	Network Type	Specifications	Billing Method	Actions
□	i-j[redacted]n [redacted]			Hongkong Zone C	[redacted](Internet) 172.24.63.171(Private)	Running	VPC	2 vCPU 8 GiB (I/O Optimized) ecs.g6e.large 5Mbps (Peak Value)	Pay-As-You-Go November 30, 2020, 13:32(Time Zone: UTC + 11) Created	Manage | Connect Change Instance Type | More

□ Start Stop Restart Reset Password Renew Switch to Subscription Release More
Total: 1 item(s), Per Page: 20 item(s)
« ‹ 1 › »

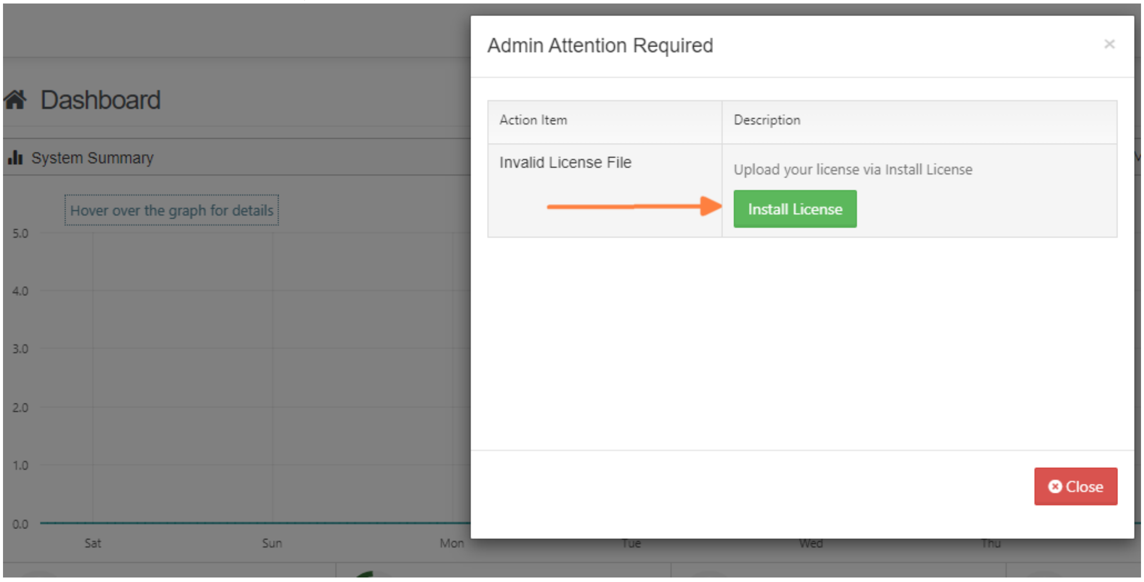
13. In your browser, access the FileCloud admin portal at **http://<public_ip_address>/ui/admin/index.html**.

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



14. 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.


Admin Attention Required

Action Item	Description
Invalid License File	Upload your license via Install License Install License

- The user name for the underlying Ubuntu OS is **root**. Before launching the instance you must either create a key pair or use your existing key pair.
- The page **http://<public_ip_address>/install** displays all the installed packages in this instance. Check the page and familiarize yourself with FileCloud components. Before going to production move the install folder **/var/www/html/install** to a different location.
- Take periodic snapshots of your running instance for disaster recovery and as an additional backup for the FileCloud database and app.

Oracle Cloud Installation

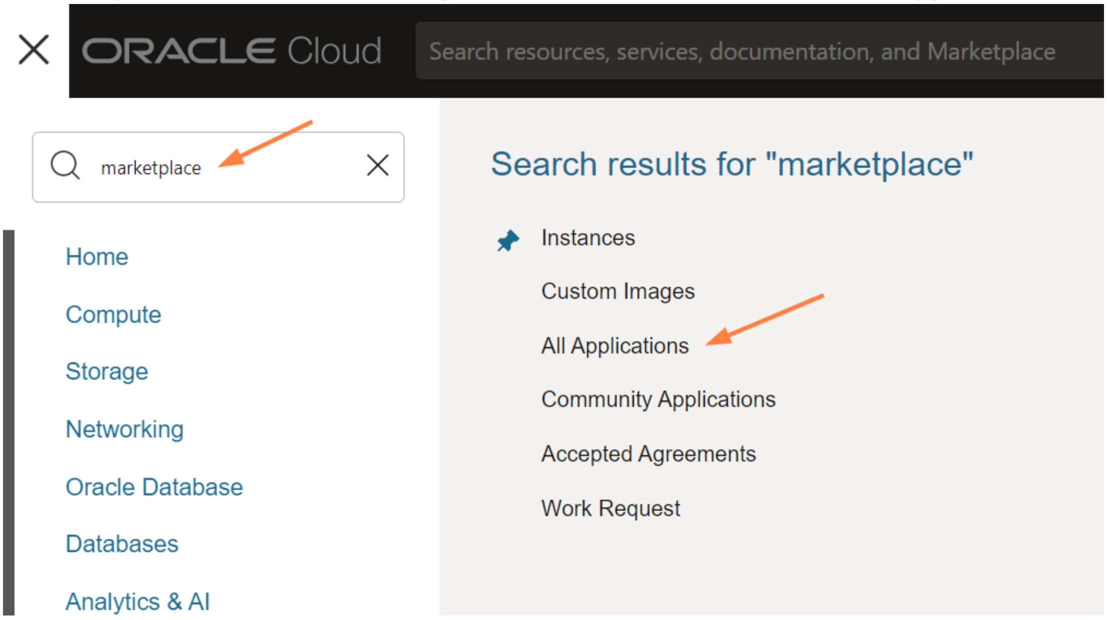
FileCloud is available from the Oracle Cloud Marketplace for installation on the Oracle Cloud Infrastructure.

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

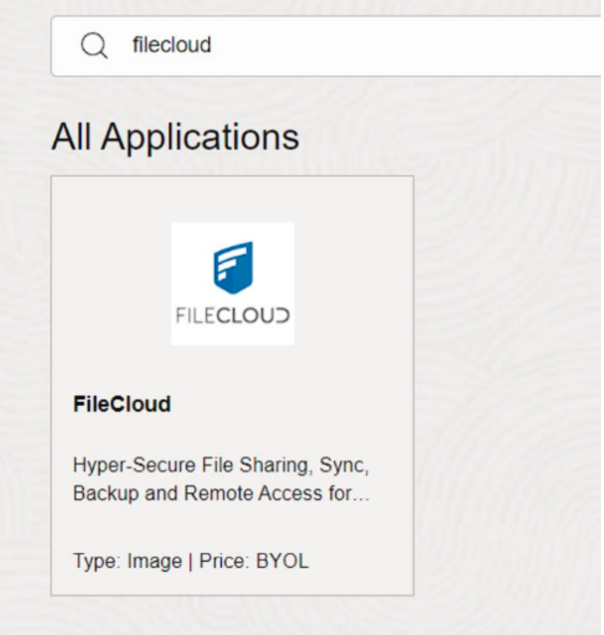
Choose the FileCloud application in Oracle Cloud Marketplace.

1. 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. Click the navigation icon in the upper-left corner:
   ☰
3. In the drop-down menu, enter **Marketplace** in the search bar and choose **All Applications**.



   Oracle Cloud Marketplace opens to a view that shows all applications.
4. In the search bar, enter **FileCloud**.

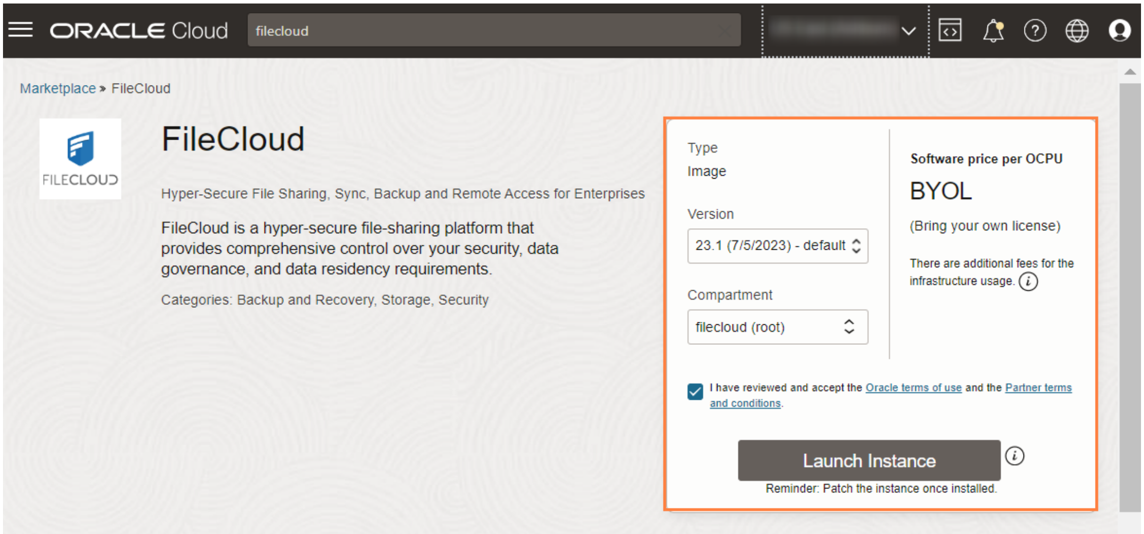


Hyper-Secure File Sharing, Sync, Backup and Remote Access for...

Type: Image | Price: BYOL

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**.



Marketplace » FileCloud

FileCloud

Hyper-Secure File Sharing, Sync, Backup and Remote Access for Enterprises

FileCloud is a hyper-secure file-sharing platform that provides comprehensive control over your security, data governance, and data residency requirements.

Categories: Backup and Recovery, Storage, Security

Type
Image

Version
23.1 (7/5/2023) - default

Compartment
filecloud (root)

Software price per OCPU
BYOL
(Bring your own license)

There are additional fees for the infrastructure usage.

☑ I have reviewed and accept the Oracle terms of use and the Partner terms and conditions.

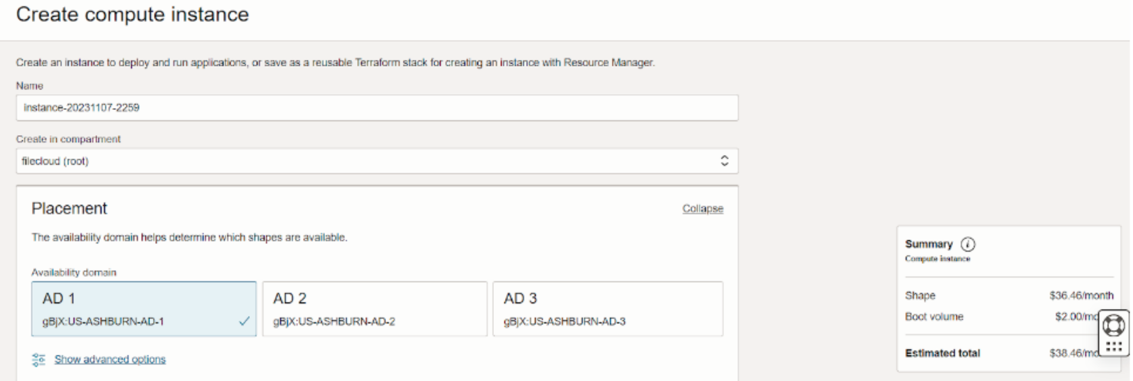
Reminder: Patch the instance once installed.

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)

Placement

The availability domain helps determine which shapes are available.

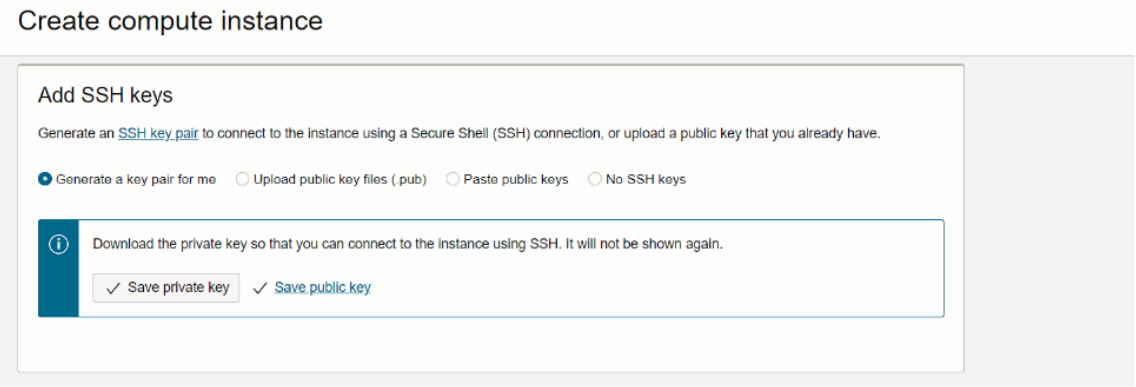
Availability domain

AD 1 gBjX:US-ASHBURN-AD-1 ✓
AD 2 gBjX:US-ASHBURN-AD-2
AD 3 gBjX:US-ASHBURN-AD-3

Summary
Compute instance

Shape	$36.46/month
Boot volume	$2.00/mo
Estimated total	$38.46/mo

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

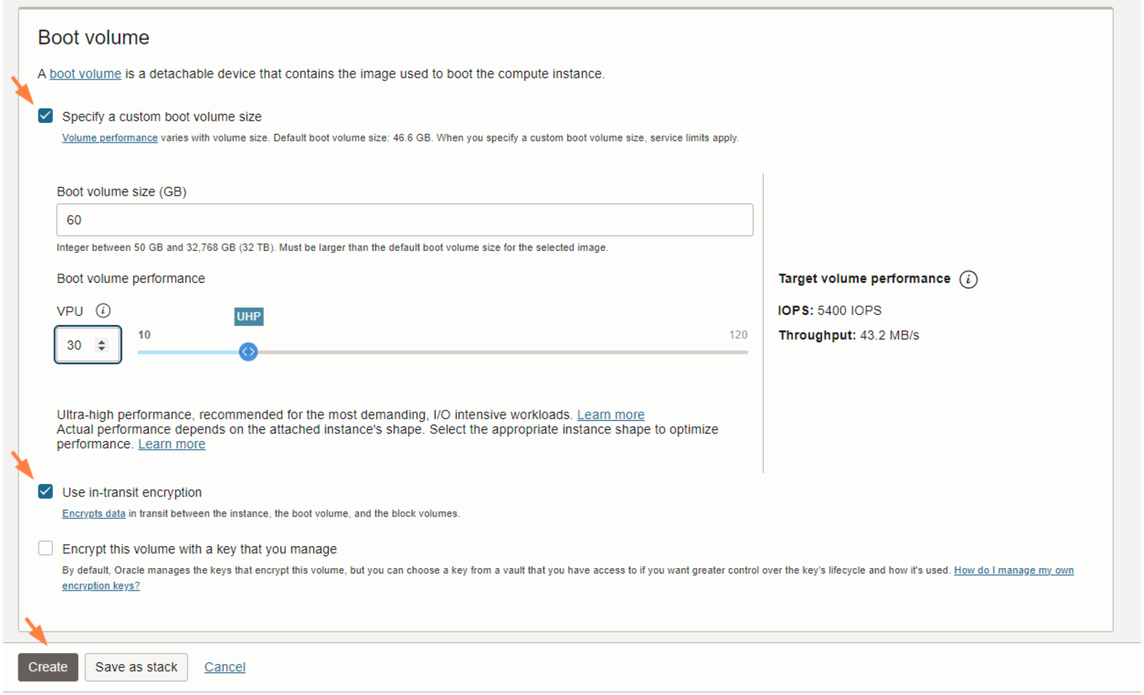
Add SSH keys

Generate an SSH key pair 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.

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

A boot volume is a detachable device that contains the image used to boot the compute instance.

☑ Specify a custom boot volume size

Volume performance 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): 60

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

VPU: 30

Target volume performance

IOPS: 5400 IOPS

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

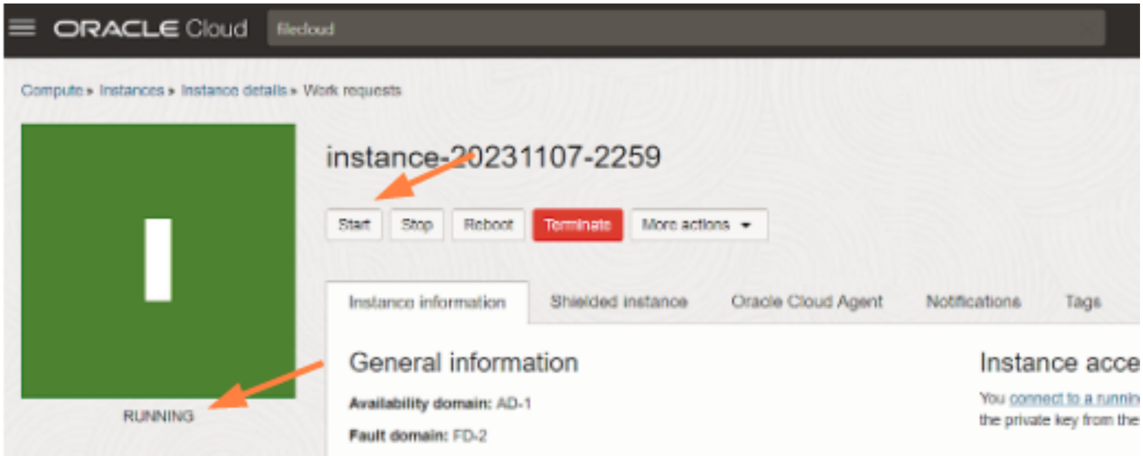
Encrypts data in transit between the instance, the boot volume, and the block volumes.

☐ 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 over the key's lifecycle and how it's used. How do I manage my own encryption keys?

7. Click **Create**.
   A page with the instance details opens.

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

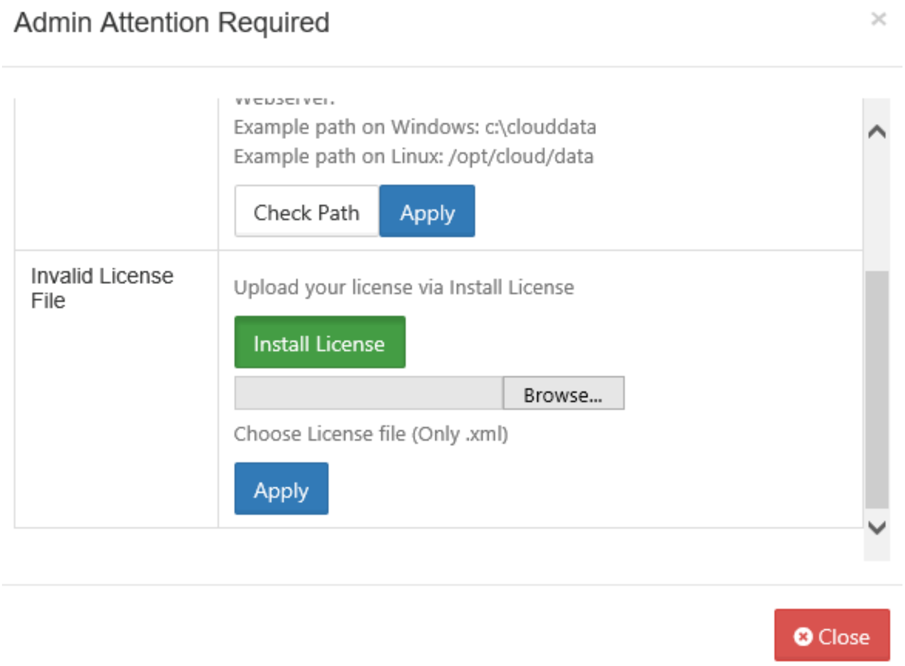


Availability domain: AD-1

Fault domain: FD-2

Connect to the instance

1. If you do not have a FileCloud License, register for one at portal.filecloud.com[37].
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.



Webserver.
Example path on Windows: c:\clouddata
Example path on Linux: /opt/cloud/data

Invalid License File

Upload your license via Install License

Choose License file (Only .xml)

[37] https://portal.filecloud.com

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.

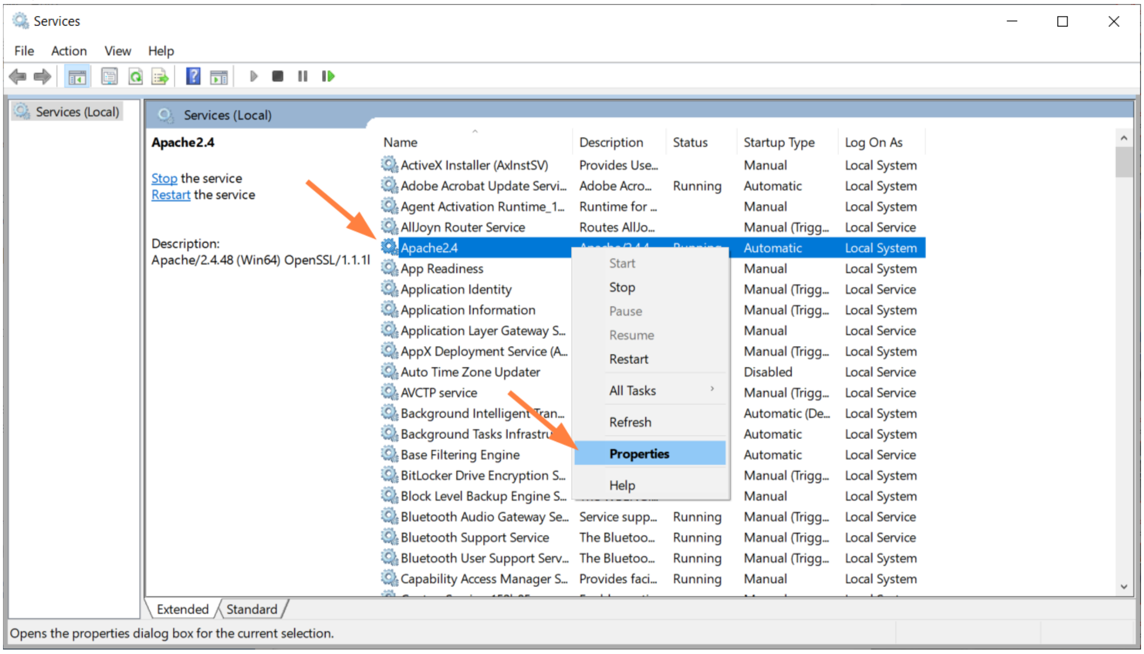
Post Installation

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

1. Verify Your Installation. (see page 116)
2. Install the FileCloud License. (see page 129)
3. Configure the Managed Storage Path. (see page 139)
4. Enable MongoDB Bind IP and Authentication (see page 143).
5. Configure SSL if desired (see page 152).
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

1. Open Windows Services.
2. Right-click **Apache2.4**, and choose **Properties**.



Apache2.4

Stop the service
Restart the service

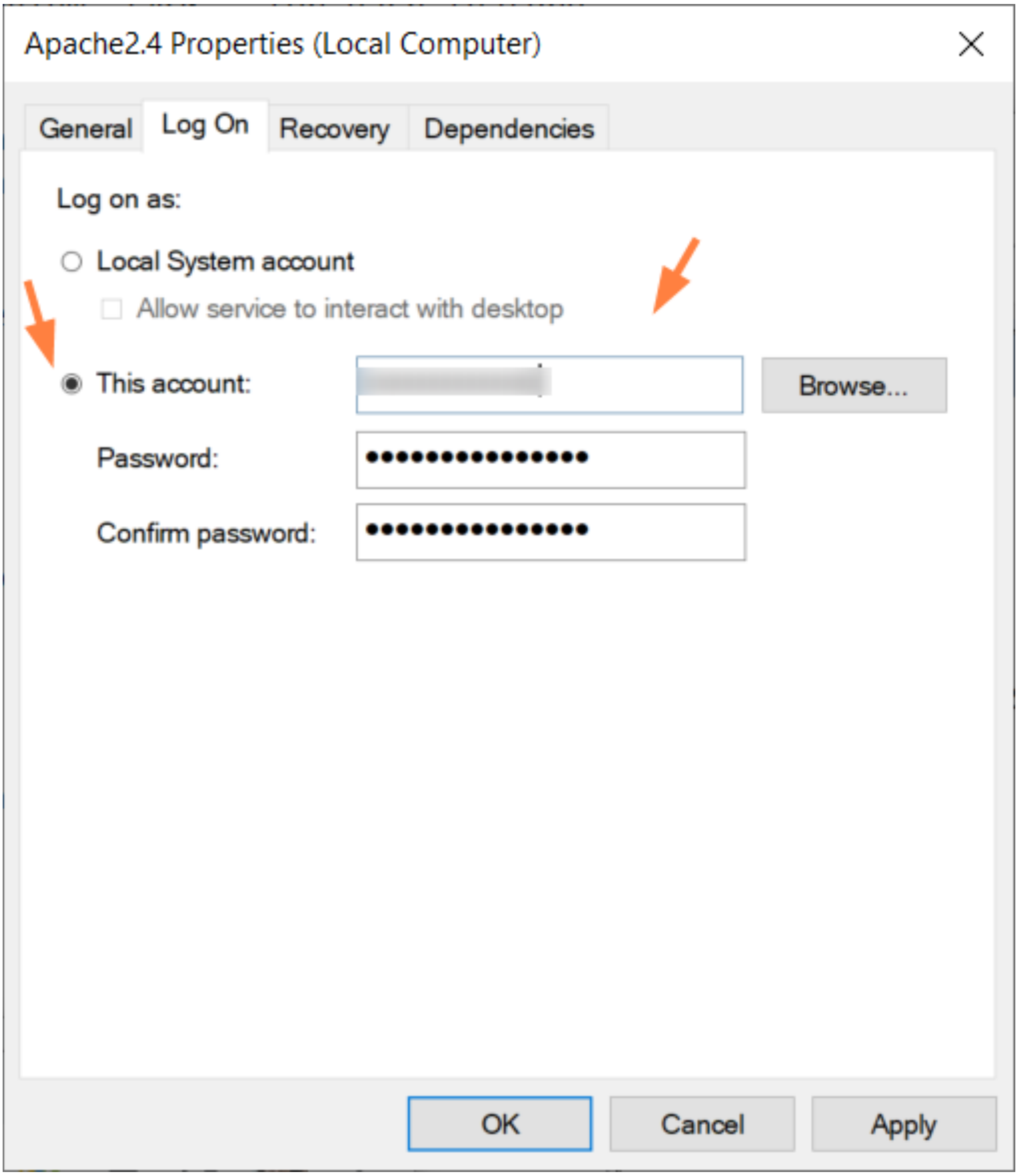
Description:
Apache/2.4.48 (Win64) OpenSSL/1.1.1l

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Adobe Acrobat Update Servi...	Adobe Acro...	Running	Automatic	Local System
Agent Activation Runtime_1...	Runtime for ...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
Apache2.4			Automatic	Local System
App Readiness			Manual	Local System
Application Identity			Manual (Trigg...	Local Service
Application Information			Manual (Trigg...	Local System
Application Layer Gateway S...			Manual	Local Service
AppX Deployment Service (A...			Manual (Trigg...	Local System
Auto Time Zone Updater			Disabled	Local Service
AVCTP service			Manual (Trigg...	Local Service
Background Intelligent Tran...			Automatic (De...	Local System
Background Tasks Infrastru			Automatic	Local System
Base Filtering Engine			Automatic	Local Service
BitLocker Drive Encryption S...			Manual (Trigg...	Local System
Block Level Backup Engine S...			Manual	Local System
Bluetooth Audio Gateway Se...	Service supp...	Running	Manual (Trigg...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trigg...	Local Service
Bluetooth User Support Serv...	The Bluetoo...	Running	Manual (Trigg...	Local System
Capability Access Manager S...	Provides faci...	Running	Manual	Local System

Opens the properties dialog box for the current selection.

In the **Properties** dialog box, click the **Log On** tab.

3. Select **This account**.
4. Enter a Windows account to use for running the service.
5. Enter and confirm the password.



Apache2.4 Properties (Local Computer)

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: [redacted] Browse...

Password: •••••••••••••••

Confirm password: •••••••••••••••

OK Cancel Apply

6. Click **Apply.**
7. Restart the service
8. 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 FileCloud Control panel. How do I open it?

Open the FileCloud Control panel

There are several ways to open the FileCloud Control Panel:

Using the Windows Start Menu

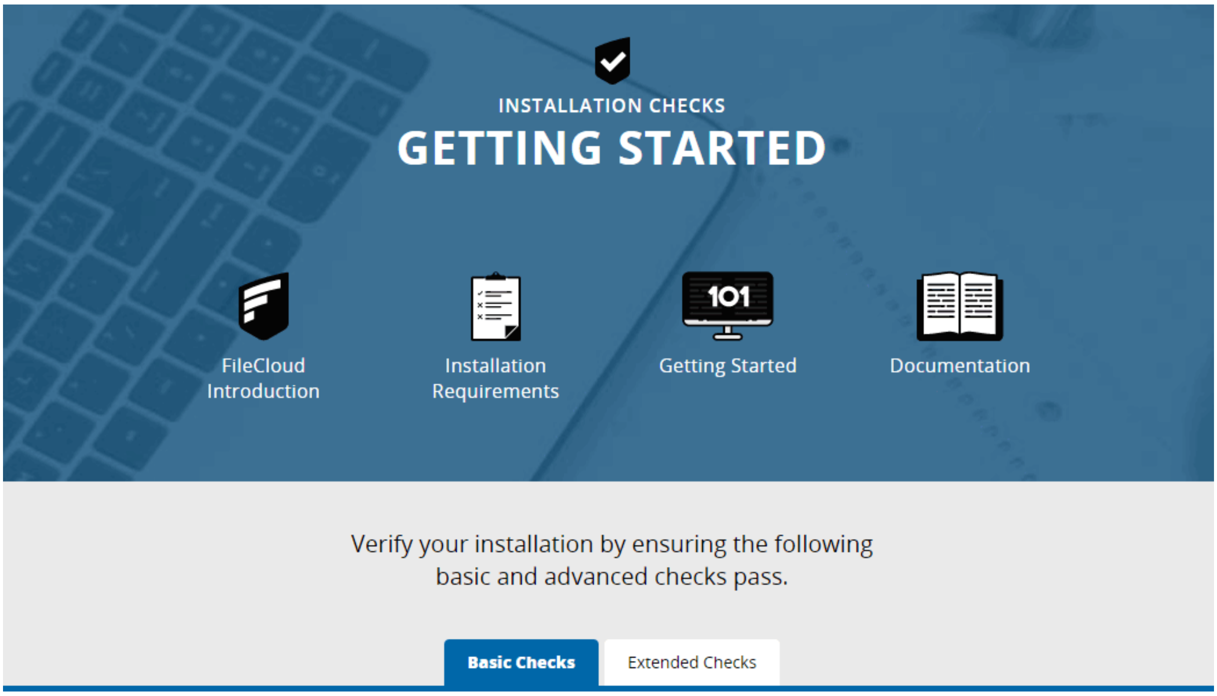
1. On the server, from the *Windows Start* menu, select the *FileCloud Control Panel*.

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.



Verify your installation by ensuring the following basic and advanced checks pass.

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	

Exif Extension • The Exif extension is used when uploading an image to generate a thumbnail. • It is also used to extract information for the built-in metadata set for images. To disable: Open the php.inic file, comment out the Exif extension, and restart the web server. When Exif is disabled in PHP: • In the logs the Exif extension is listed as disabled. • Uploaded images do not have a thumbnail, and the Image metadata set is empty. When Exif is enabled in PHP: • Uploaded images have a thumbnail. • The Image metadata set contains attributes for all image files. • This is the default behavior. FileCloud does not apply Image metadata for Azure/S3 Network Folders.	

This tool also reports 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
```

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 (see page 119).

3. To review more thorough tests, select Extended Checks (see page 124).

Basic Checks

Clicking on the Basic Checks tab displays:

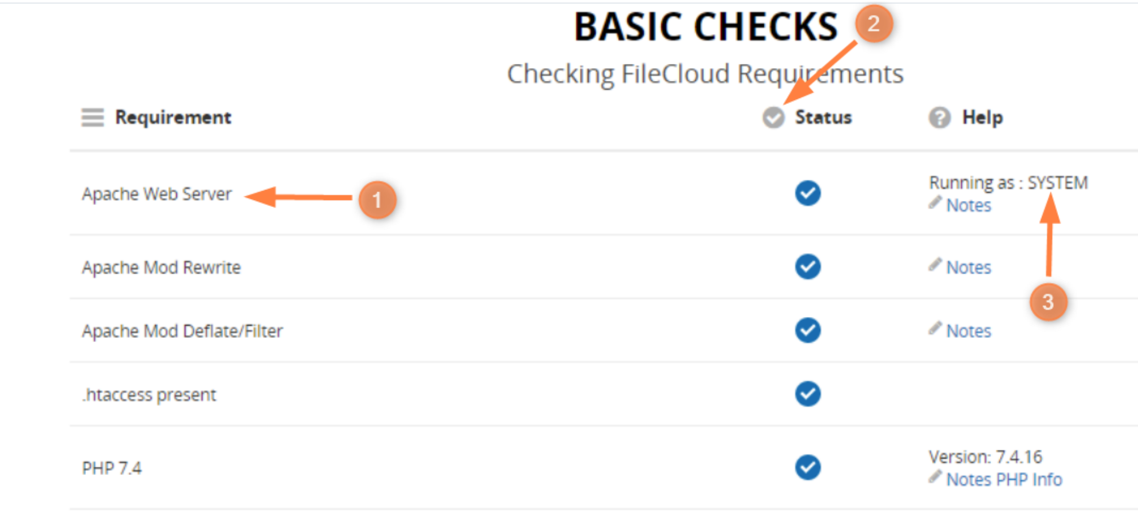
1. The name of the item that was checked.
2. The result of the check. A blue checkmark

   ✓

   = PASS, and a red X

   ✖

   = FAIL.
3. Additional information for installing, troubleshooting, or correcting an issue for this item.



BASIC CHECKS

Checking FileCloud Requirements

Requirement	Status	Help
Apache Web Server	✓	Running as : SYSTEM Notes
Apache Mod Rewrite	✓	Notes
Apache Mod Deflate/Filter	✓	Notes
.htaccess present	✓	
PHP 7.4	✓	Version: 7.4.16 Notes PHP Info

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

To review Basic Checks:

1. How to review basic checks

How to review basic checks

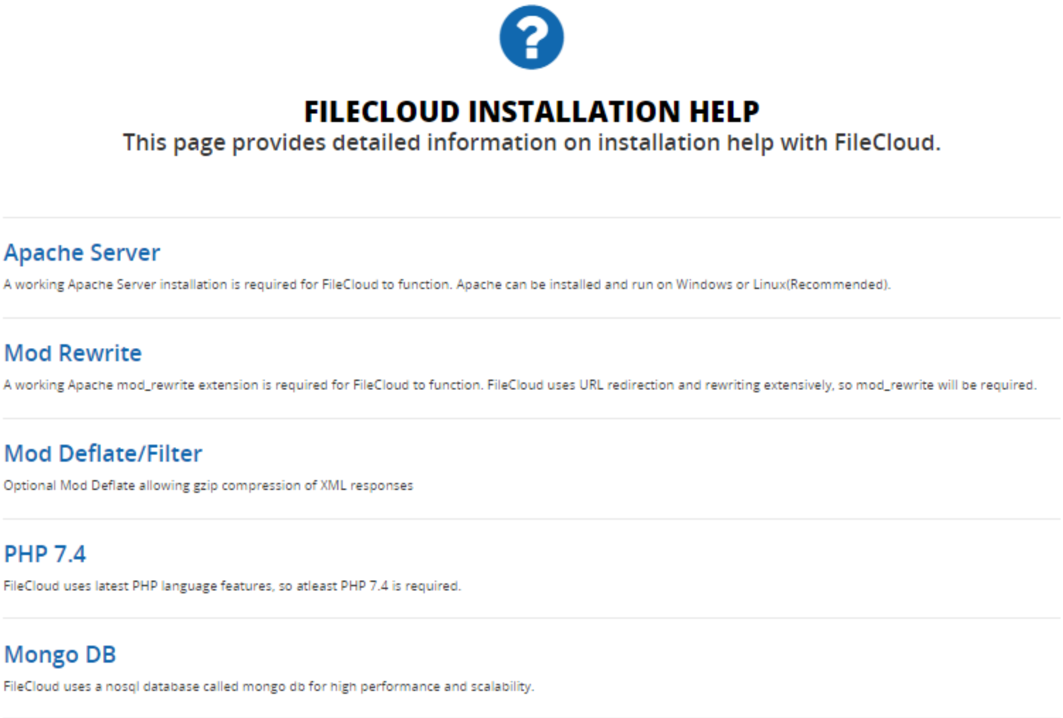
The following table explains how to use the Basic Checks information:

What You See			What It Means
.htaccess present	✓		For a blank entry with a blue checkmark, the item has passed the verification test and there is nothing further for you to do.
Apache Mod Rewrite	✓	✎ 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	✓	Version 4.0.52 ✎ Notes	For a version entry with a blue checkmark, the item has passed the verification test using the specific version. Optional: To read more about the item, click on ✎ Notes (the Notes icon).
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).

What You See			What It Means
PHP Memcache Server (optional)	✖	Version: ✎ Notes	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 ✎ Notes . • Review the Requirements page. • Review the installation procedures (see page 4). • Review the Installation Troubleshooting (see page 189) page.

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

In the Help column, if you click on ✎ Notes (the Notes icon), the FileCloud Help page opens.



FILECLOUD INSTALLATION HELP

This page provides detailed information on installation help with FileCloud.

Apache Server

A working Apache Server installation is required for FileCloud to function. Apache can be installed and run on Windows or Linux(Recommended).

Mod Rewrite

A working Apache mod_rewrite extension is required for FileCloud to function. FileCloud uses URL redirection and rewriting extensively, so mod_rewrite will be required.

Mod Deflate/Filter

Optional Mod Deflate allowing gzip compression of XML responses

PHP 7.4

FileCloud uses latest PHP language features, so atleast PHP 7.4 is required.

Mongo DB

FileCloud uses a nosql database called mongo db for high performance and scalability.

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:
3. Read more about the item in

   .
4. Review the Requirements page.
5. Review the installation procedures (see page 4).
6. Review the Installation Troubleshooting (see page 189) 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.

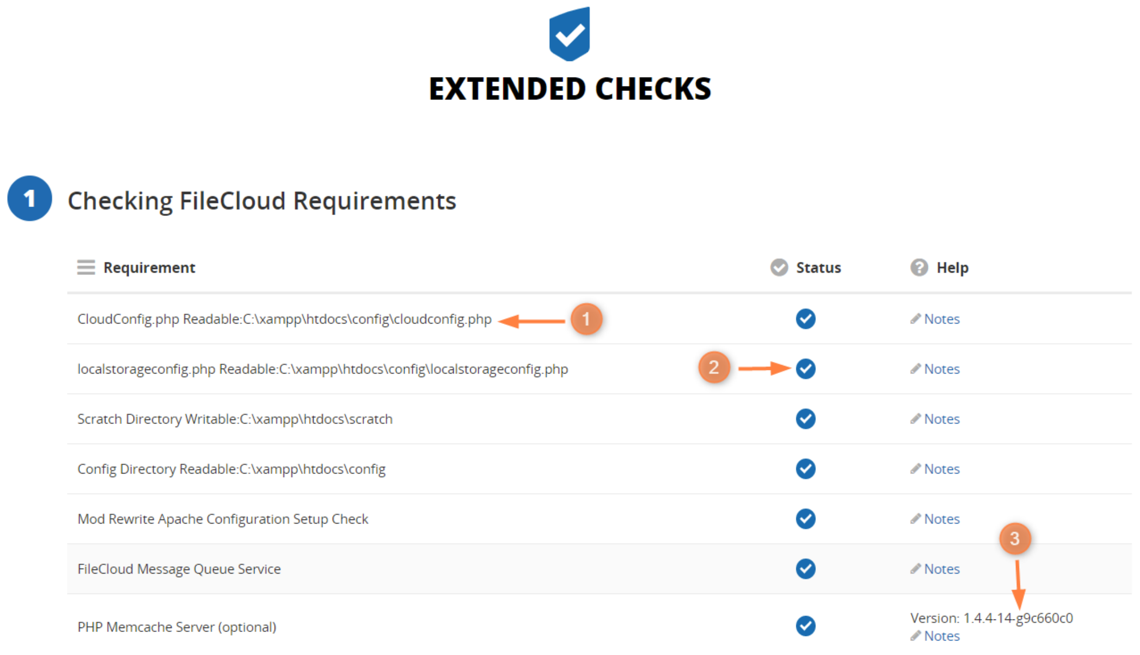
Check	Details
Apache Web Server	Checks if your environment has a working Apache server installation.
Apache Mod Rewrite	Checks if mod rewrite module is enabled and activated.
Apache Mod Deflate/ Filter (optional)	Checks if the Apache mod_deflate module is present. This is optional.
.htaccess Present	Checks if the .htaccess is present in the root WWWROOT folder
PHP 8.2 or higher	Checks if the environment has PHP v8.2 or higher.
PHP MongoDB (mongodb ext) driver 1.15.0 or higher	Checks if PHP Mongo DB drivers are installed properly and are version 1.15.0 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 SourceGuardian extension 14.0.0 or higher	Checks if SourceGuardian, which protects FileCloud PHP files, is installed.

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 (http://mydomain.com[38]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

[38] http://mydomain.com/

Extended Checks

Clicking on the Extended Checks tab displays:



EXTENDED CHECKS

1 Checking FileCloud Requirements

Requirement	Status	Help
CloudConfig.php Readable:C:\xampp\htdocs\config\cloudconfig.php	✓	Notes
localstorageconfig.php Readable:C:\xampp\htdocs\config\localstorageconfig.php	✓	Notes
Scratch Directory Writable:C:\xampp\htdocs\scratch	✓	Notes
Config Directory Readable:C:\xampp\htdocs\config	✓	Notes
Mod Rewrite Apache Configuration Setup Check	✓	Notes
FileCloud Message Queue Service	✓	Notes
PHP Memcache Server (optional)	✓	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

   ✓

   = PASS, and a red X

   ✖

   = FAIL.
3. Additional information for installing, troubleshooting, or correcting an issue for this item.

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 by clicking the Notes link in the Help column.
- Review the Requirements page.
- Review the installation procedures (see page 4).
- Review the Installation Troubleshooting (see page 189) page.

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

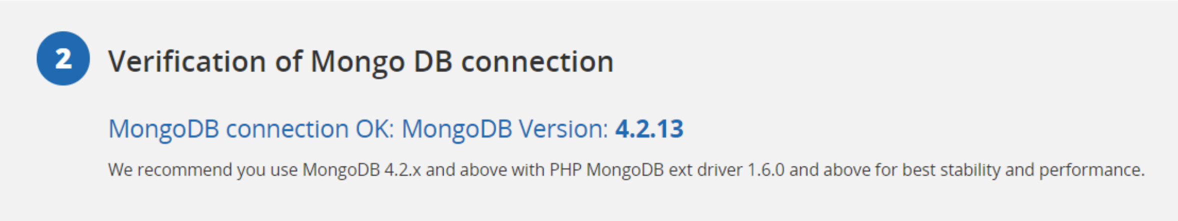
Check	Details
CloudConfig.php readable	Checks if the cloudconfig.php file is present in the config folder
Localstorageconfig.php readable	Checks if the localstorageconfig.php file is present in the config folder
Scratch Directory Writable	Checks if WebServer process has write permissions to WEBROOT/scratch directory. In Linux, usually chown -R www-data:www-data[39]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.
Mod Proxy HTTP Apache Configuration Setup Check	
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:

[39] http://www-datawww-data/



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.

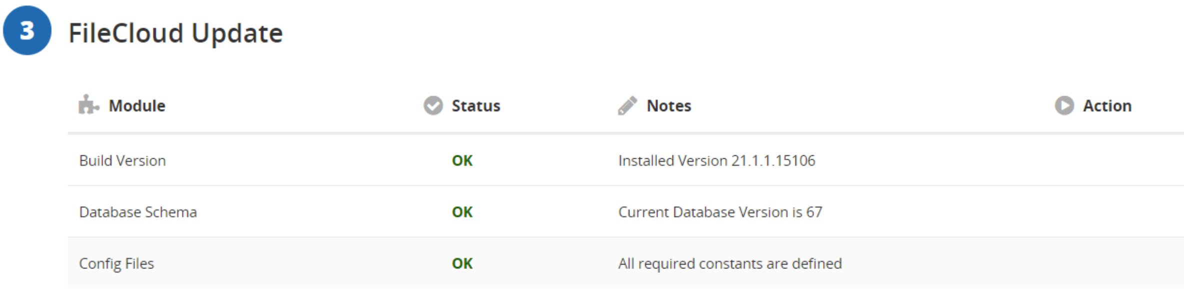
If your connection is not OK, then return to the FileCloud control panel to troubleshoot and resolve the issue.

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 or changed, in the **Action** column, click the link. When you update to a new version, it is common to have to add new entries.



3 FileCloud Update

Module	Status	Notes	Action
Build Version	OK	Installed Version 21.1.1.15106	
Database Schema	OK	Current Database Version is 67	
Config Files	OK	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[40]
- Ubuntu - SSH/OpenSSH/PortForwarding[41]
- RHEL - Red Hat Documentation - Port Forwarding[42]

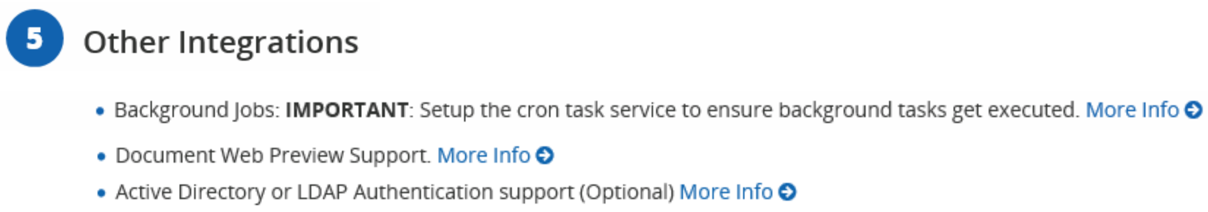
5. Configure Any Missing Integrations

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**:



5 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

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.

[40] https://docs.microsoft.com/en-us/windows-server/remote/

[41] https://help.ubuntu.com/community/SSH/OpenSSH/PortForwarding

[42] https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/sec-port_forwarding

✓ 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.
2. 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 or /var/www/install

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 Deployment URL will be set as "*" (accessible from any URL)	Server (Self-host) Online (Hosted by us)

License Type	Duration	Features	Availability
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[43]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

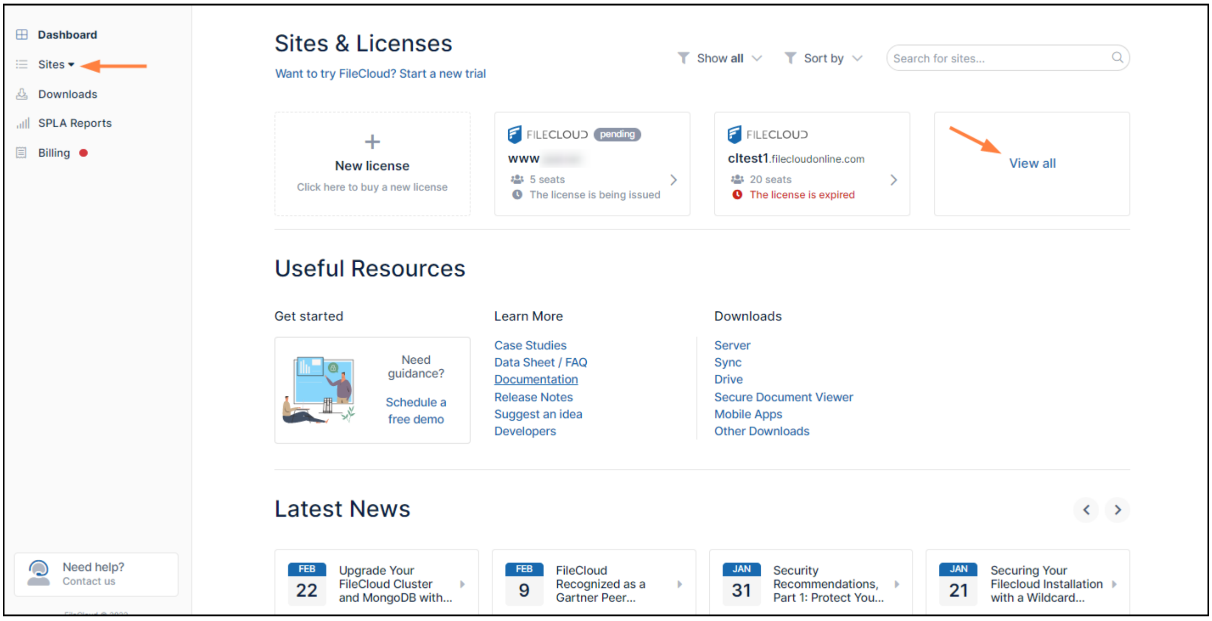
Downloading your License

To download your license:

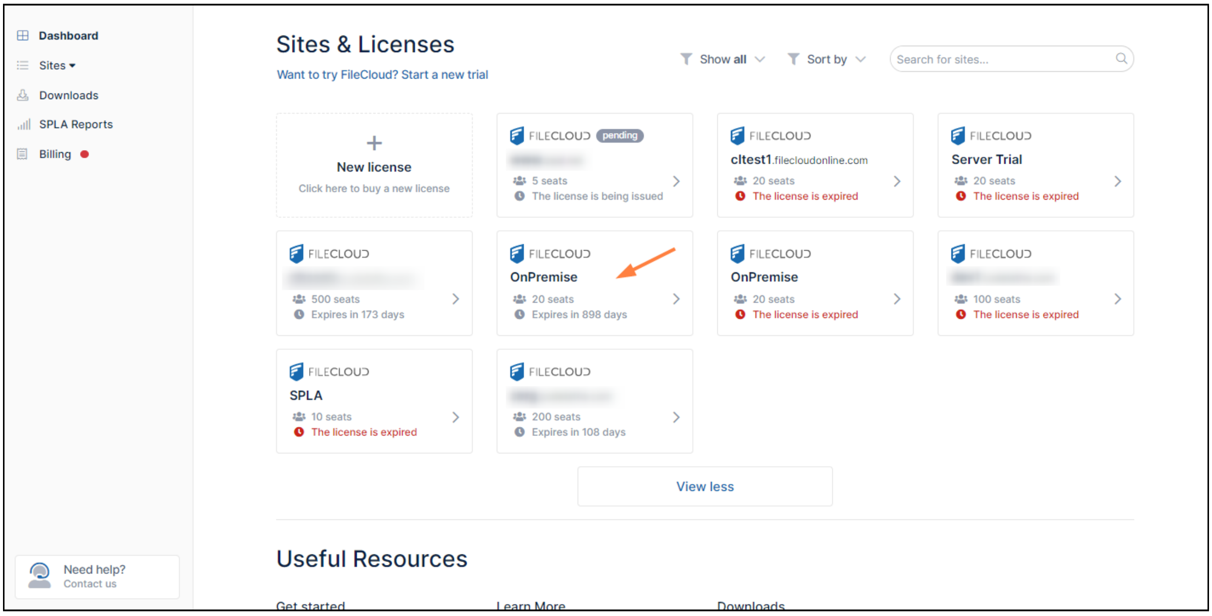
1. Navigate to https://portal.getfilecloud.com/ui/user/index.html

[43] https://www.filecloud.com/pricing

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.



3. 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).
4. Click the license that you want to download.



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

Installing Your License

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

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:

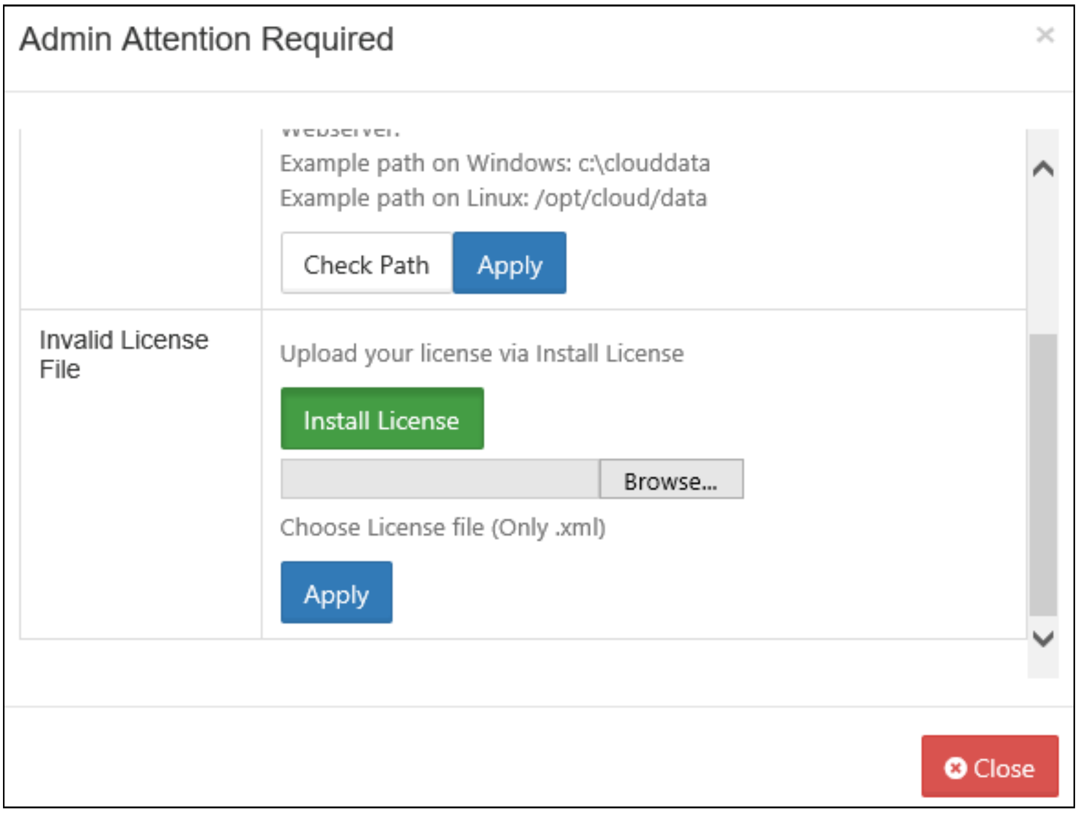
- Admin alert dialog box
- The dashboard's **License Information** widget
- The admin portal's License settings page.

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

Webserver.
Example path on Windows: c:\clouddata
Example path on Linux: /opt/cloud/data

Invalid License File

Upload your license via Install License

Choose License file (Only .xml)

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

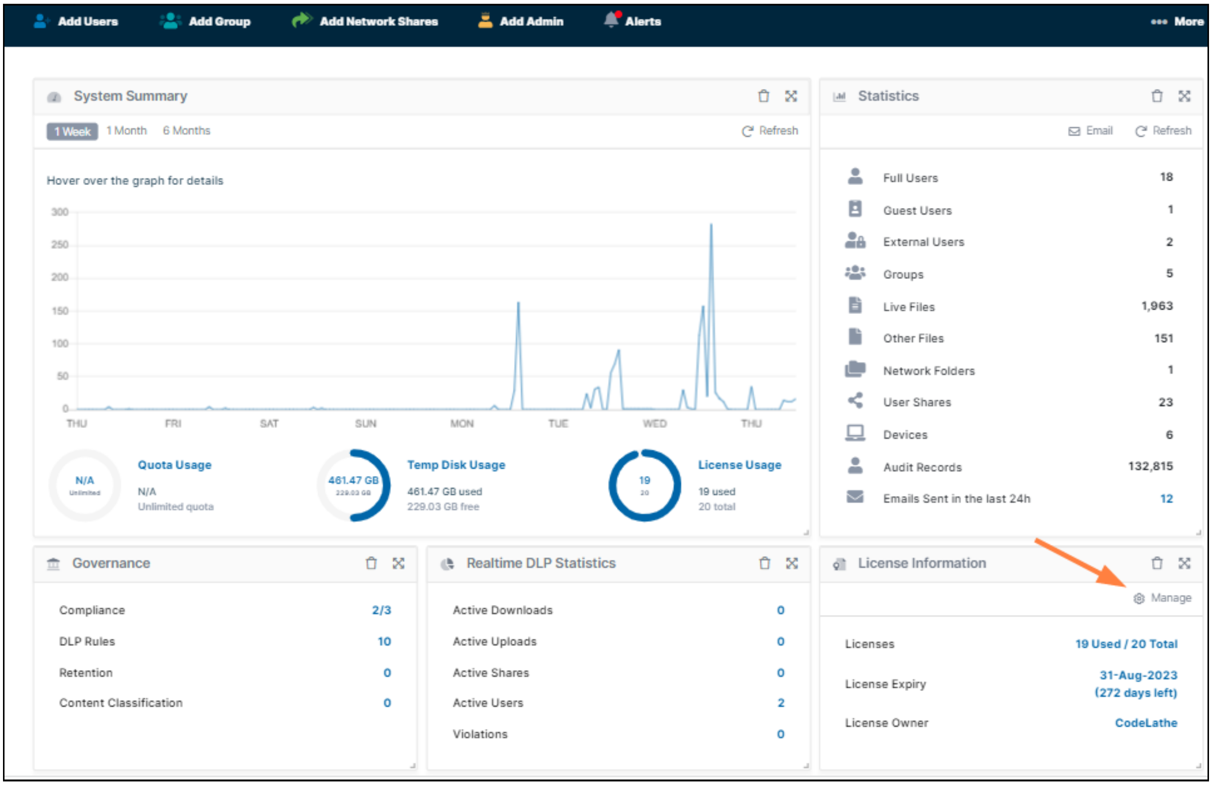
If you close the Admin dialog without installing a license, you can always use the FileCloud dashboard to manage your licenses. You can also use it to update a license.

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**.



Full Users	18
Guest Users	1
External Users	2
Groups	5
Live Files	1,963
Other Files	151
Network Folders	1
User Shares	23
Devices	6
Audit Records	132,815
Emails Sent in the last 24h	12

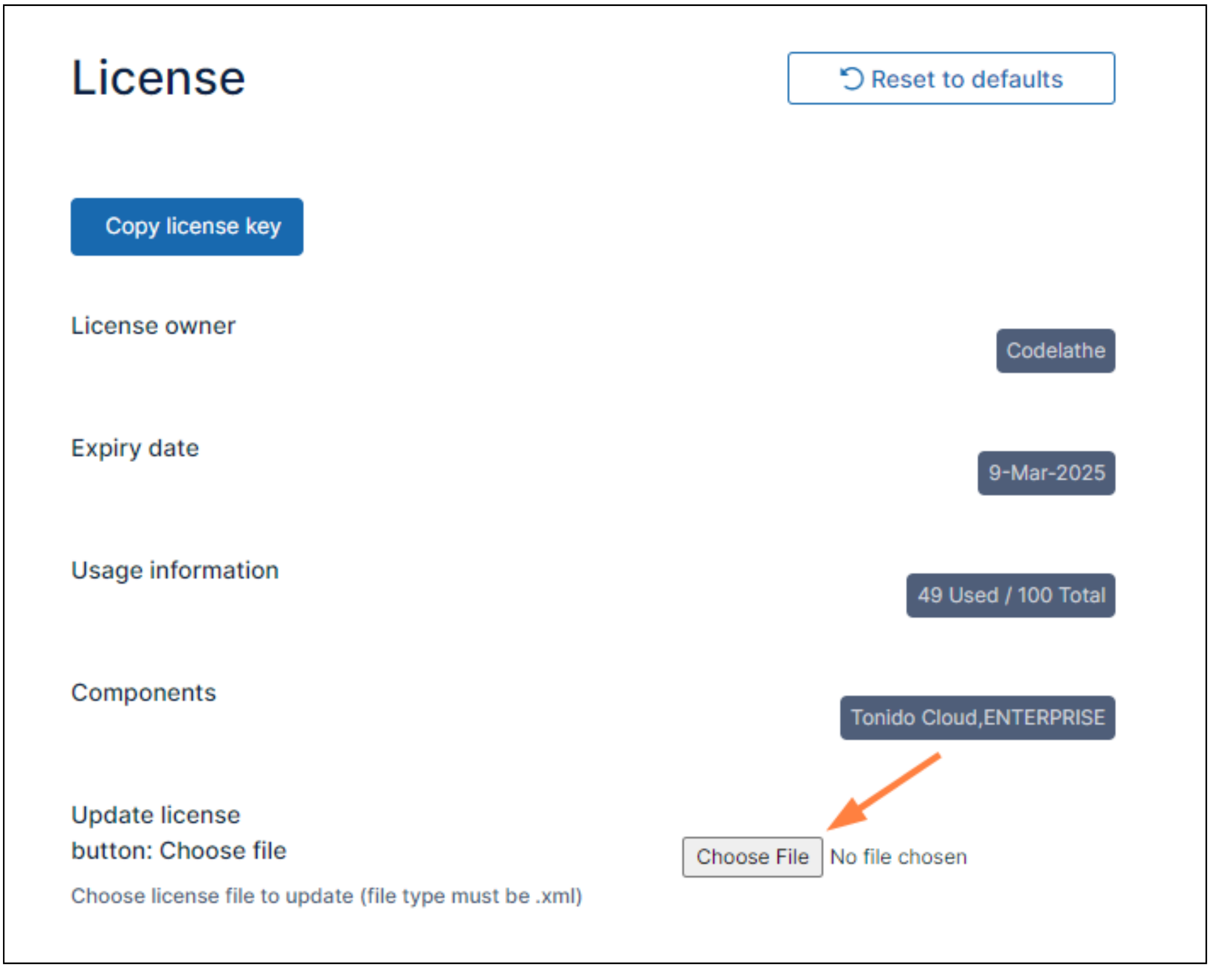
Compliance	2/3
DLP Rules	10
Retention	0
Content Classification	0

Active Downloads	0
Active Uploads	0
Active Shares	0
Active Users	2
Violations	0

Licenses	19 Used / 20 Total
License Expiry	31-Aug-2023 (272 days left)
License Owner	CodeLathe

The dashboard opens the same window that opens when you go to the License settings page (see page

135).



License owner: Codelathe

Expiry date: 9-Mar-2025

Usage information: 49 Used / 100 Total

Components: Tonido Cloud,ENTERPRISE

Update license button: Choose file — Choose File No file chosen

Choose license file to update (file type must be .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**.

⚠ If you have hosts available for accessing FileCloud in addition to the one listed in Server URL, your FileCloud installation log may display **Not allowed host** errors for those hosts.

To avoid getting Not allowed host errors:

1. Open cloudconfig.php at
   - Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   - Linux: /var/www/config/cloudconfig.php
2. Add the following, replacing the Server URLs with your own.

```
define("TONIDOCLOUD_ALLOWED_HOSTS",
"mycompany.store1.com,mycompany.store2.com,mycompany.store3.com");
```

Also see:

- Installing FileCloud License On Multiple Sites (see page 136)
- Viewing Your License Details (see page 137)

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 **licenses.txt** that lists the sites that you want to update in the format:

   ```
   https://site1.test.com
   https://site2.test.com
   ```

2. Install the **licenses.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, enter:

   For Windows:

   ```
   php licenseinstaller.php c:\xampp\htdocs\resources\backup\license.xml
   ```

   For Linux:

   ```
   php licenseinstaller.php /var/www/html/resources/backup/license.xml
   ```

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

Viewing Your License Details

ℹ License components information 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[44]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.

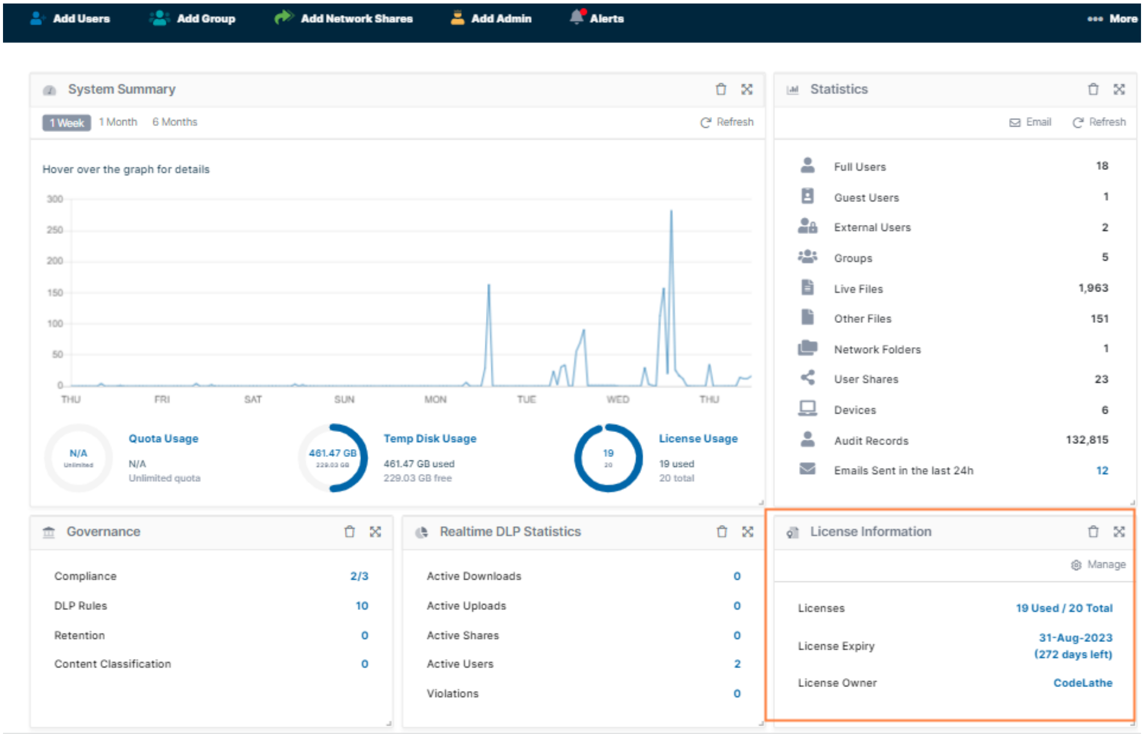
From the Dashboard

To review your license details:

1. Log in to the admin portal.

[44] https://www.filecloud.com/pricing/

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



Full Users	18
Guest Users	1
External Users	2
Groups	5
Live Files	1,963
Other Files	151
Network Folders	1
User Shares	23
Devices	6
Audit Records	132,815
Emails Sent in the last 24h	12

Governance

Compliance	2/3
DLP Rules	10
Retention	0
Content Classification	0

Realtime DLP Statistics

Active Downloads	0
Active Uploads	0
Active Shares	0
Active Users	2
Violations	0

License Information

Manage

Licenses	19 Used / 20 Total
License Expiry	31-Aug-2023 (272 days left)
License Owner	CodeLathe

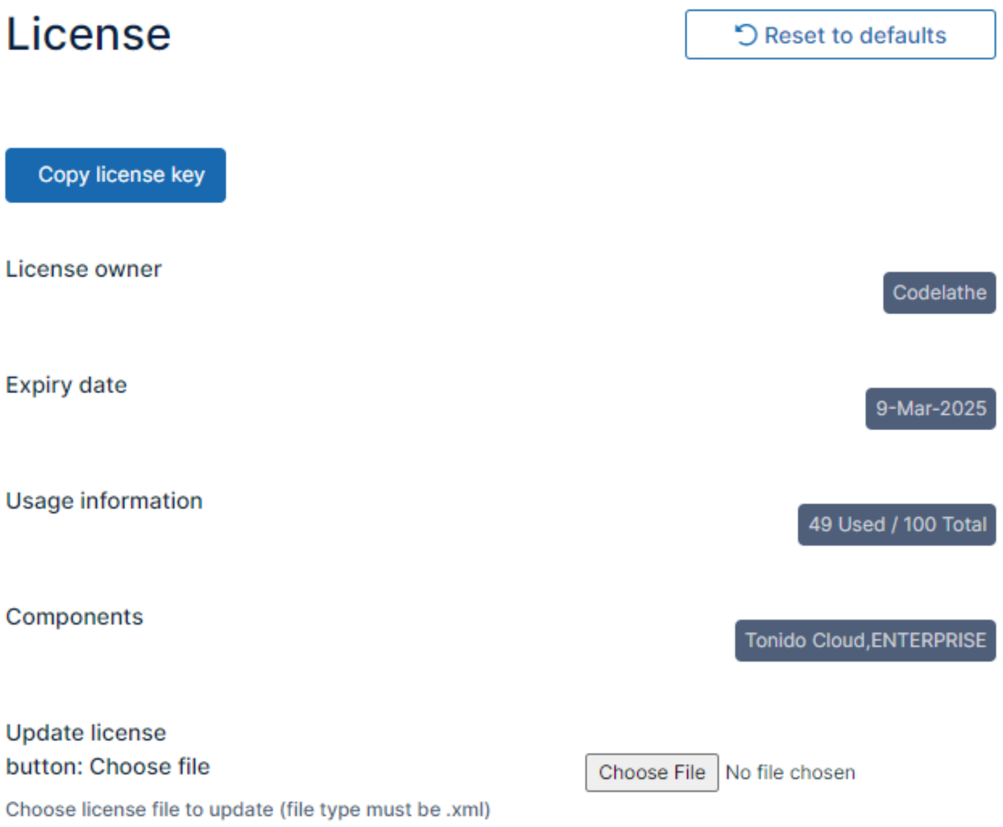
.

3. In the upper-right corner, click **Manage** to go to the license settings shown below.

In the Settings screen

To update your license details:

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



License

Reset to defaults

Copy license key

License owner: Codelathe

Expiry date: 9-Mar-2025

Usage information: 49 Used / 100 Total

Components: Tonido Cloud,ENTERPRISE

Update license
button: Choose file

Choose license file to update (file type must be .xml)

Choose File No file chosen

2. Review the license information.
3. In **Components**, make sure the features you need are listed.
4. To install a new license, click **Choose File**.
5. If the **Copy license key** button appears, click it to copy your license key to your **clipboard**. This is useful if you need to register in the support portal[45], which initially requires you to enter your license key.

Note: The **Copy license key** button does not appear for systems with SPLA licenses. If your system uses an SPLA license, you can get your license key from the customer portal at portal.filecloud.com[46].

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

[45] https://help.filecloud.com/support

[46] https://www.filecloud.com/supportdocs/display/FCDOC/Contact+FileCloud+Support

- 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.

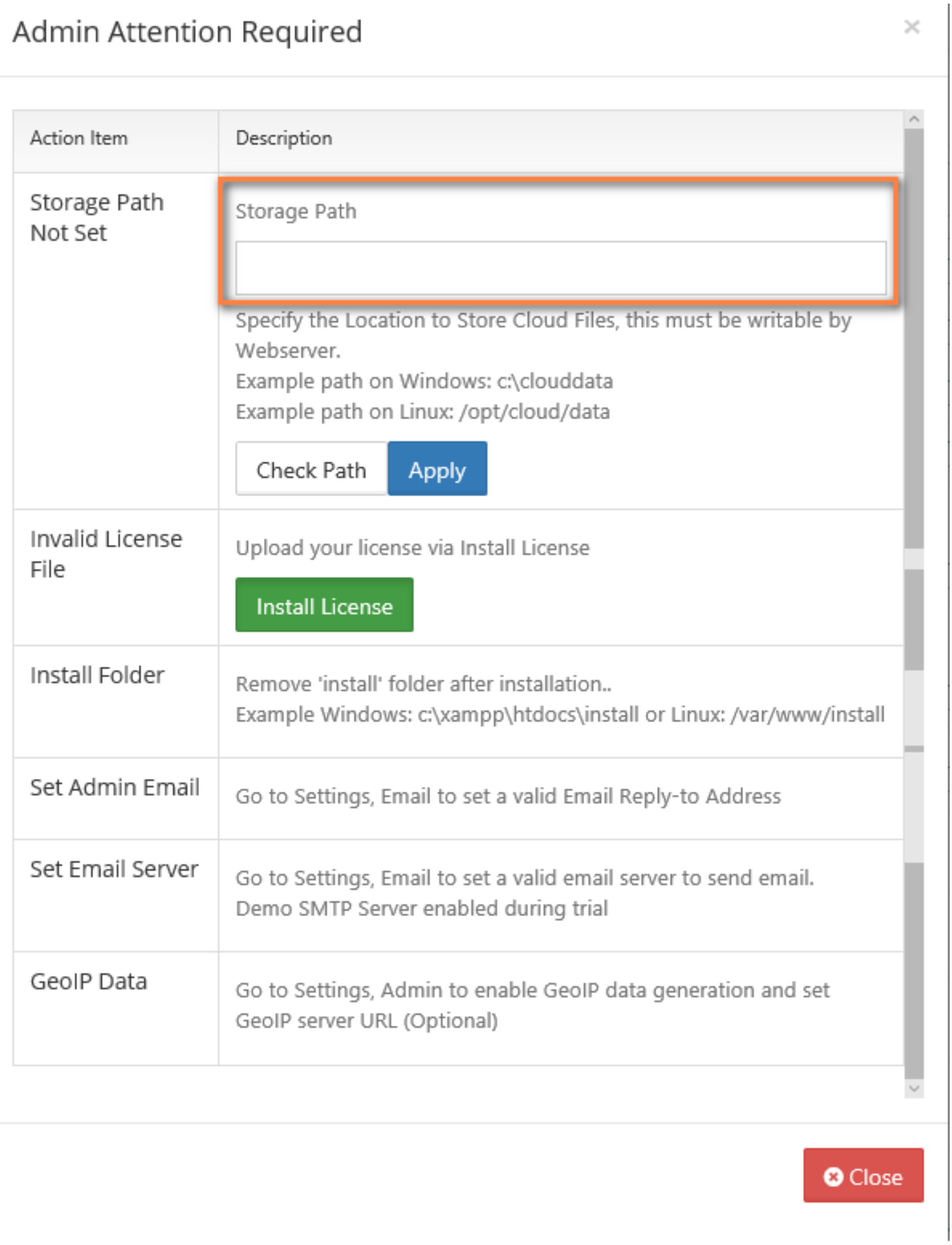
Setting up Managed Storage Path for Local Storage is only needed if you are using FileCloud Local Storage.
If you are using Amazon S3, you don't need to set this path.

To configure the storage path:

Use the Admin Attention Required dialog for the 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.



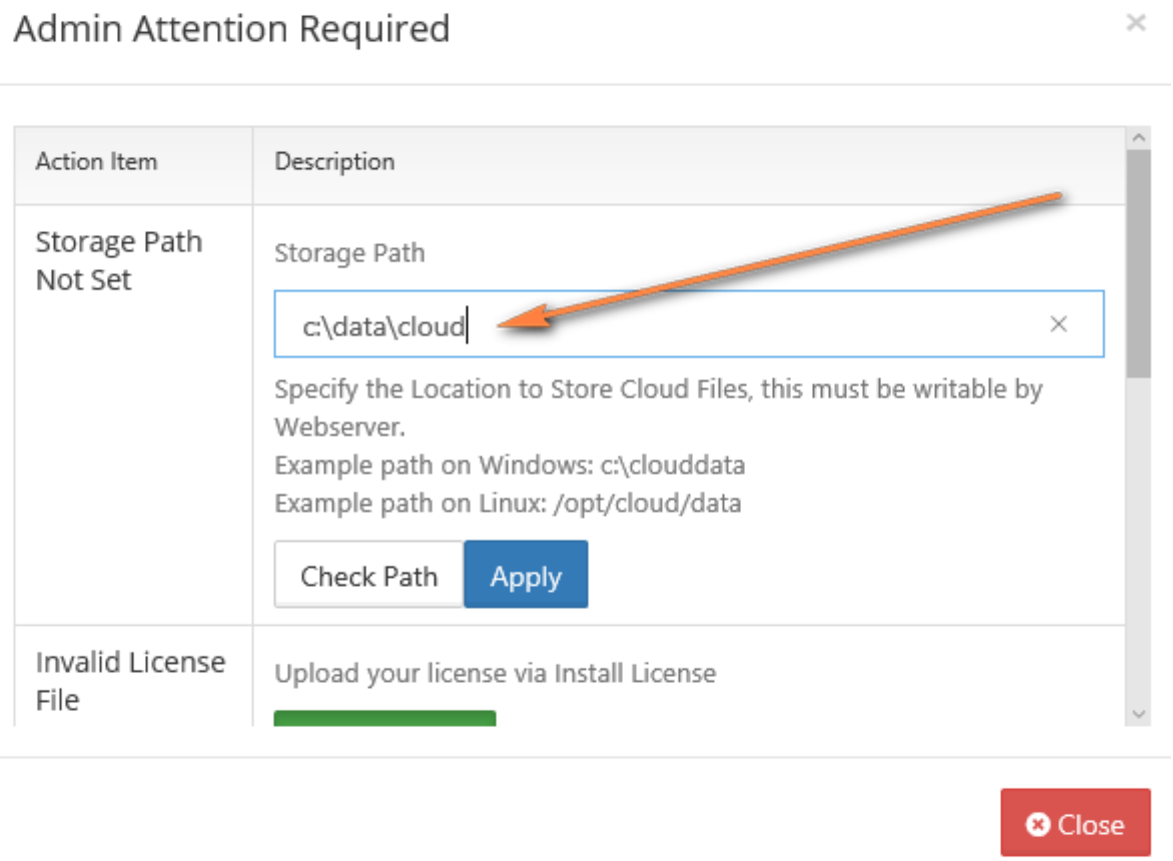
Admin Attention Required

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
Invalid License File	Upload your license via Install License Install License
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
GeoIP Data	Go to Settings, Admin to enable GeoIP data generation and set GeoIP server URL (Optional)

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 Attention 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
Invalid License File	Upload your license via Install License

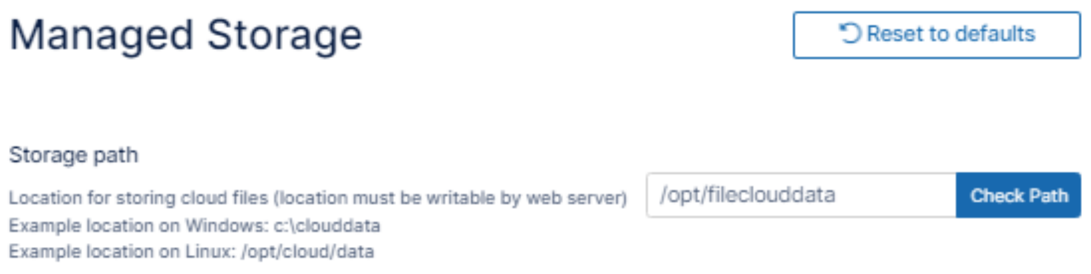
Use the Admin portal to manage storage path changes.

Managing the Storage Path

To set or change storage path:

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Storage** .
   By default, the **Managed storage** settings page opens.
2. In **Storage path**, set the path as needed (for example on Windows c:\filecloud, or on Linux /opt/filecloud), and click **Save**.

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



Managed Storage

Storage path

Location for storing cloud files (location must be writable by web server)
Example location on Windows: c:\clouddata
Example location on Linux: /opt/cloud/data

/opt/fileclouddata

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
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('dbuser','passw0rd1')
> use tonidoauditdb;
> db.addUser('dbuser','passw0rd1')
> use tonidoclouddb;
> db.addUser('dbuser','passw0rd1')
> use tonidostoragedb;
> db.addUser('dbuser','passw0rd1')
> use tonidosyncdb;
> db.addUser('dbuser','passw0rd1')
> use tonidosettings;
> 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:

1. Open the mongodb configuration file:
   Linux: **/etc/mongodb.conf**
   Windows: **C:\xampp\mongodb\bin\mongodb.conf**
2. 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**[47]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:

[47] http://mongosrv1.myfilecloud.com

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[48]) 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

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 sub-section.

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
```

[48] http://mongosrv1.myfilecloud.com

```
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"
}
```

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:

1. 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+k5756194hlIcUcp5Qod7oXe2XgaQNO+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/html/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.

Enable FileCloud SSL Mode Connection To MongoDB

Introduction

By default, FileCloud connects to a MongoDB server in plain text mode, but FileCloud can be enabled to connect to MongoDB server in SSL mode.

Enabling SSL Mode Connection

1. To enable SSL based connection to MongoDB server, edit the file WWWROOT/core/framework/slmongoclientcontext.class.php and replace the contents of the file with the following:

   Mongo Client

```
<?php
/*
 * Copyright(c) 2015 CodeLathe LLC. All rights Reserved.
 * This file is part of Tonido FileCloud  http://www.tonido.com
 */
namespace core\framework;
defined('TONIDO_CLOUD_ROOT_DIR') or exit('Forbidden');
/**
 * Description of slmongoclientcontext
 *
 * @author madhan
 */
class SLMongoClientContext{

    public static $USECONTEXT = TRUE;


    public static function getOptions(){
        return array("ssl" => true);
    }

    public static function getContext(){
        //$SSL_DIR = "c:\\xampp\\mongodb\\bin\\certs";
        //$SSL_FILE = "CA_Root_Certificate.pem";
        $ctx = stream_context_create(array(
            "ssl" => array(
                /* Certificate Authority the remote server certificate must be
signed by */
                //"cafile"            => $SSL_DIR . DIRECTORY_SEPARATOR .
$SSL_FILE,
                "local_cert" => "c:\\xampp\\mongodb\\bin\\certs\\mongodb.pem",
                /* Disable self signed certificates */
                "allow_self_signed" => true,
                /* Verify the peer certificate against our provided Certificate
Authority root certificate */
                "verify_peer"       => false, /* Default to false pre PHP 5.6 */
                /* Verify the peer name (e.g. hostname validation) */
                /* Will use the hostname used to connec to the node */
                "verify_peer_name"  => false,
                /* Verify the server certificate has not expired */
                "verify_expiry"     => true, /* Only available in the MongoDB PHP
Driver */
            ),
        ));
        return array("context" => $ctx);
    }
}
```

2. Modify the context parameters as necessary to suit your environment and save the file. There is no need to change any other MongoDB connection URLs.
3. Restart MongoDB and apache servers. Now FileCloud should be able to connect to SSL enabled MongoDB server.

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 need an SSL certificate.

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 need to configure additional settings and install an SSL certificate on the AD server.

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

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 remains private and integral.

To create an SSL connection a web server requires an SSL Certificate. When you activate SSL on your web server you are asked 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.

Your customers' browsers display 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. They can click the lock icon to view the SSL Certificate and details about it.

To learn more about SSL, read knowledge base articles on the SSL web site[49].

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.

The result is a certificate chain that includes the trusted root certificate, the intermediate certificate, and the SSL certificate issued to you.

[49] https://www.ssl.com/info/

The use of intermediate certificates for issuing SSL certificates to end entities provides an added level of security. You must install the intermediate certificate on your web server along with your SSL certificate to allow the certificate to be effective.

Your certificate files' extensions enable you to know what's in the files, and if you need to convert them.

What are the different certificate 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 (see page 154)

Use SSL on Linux (see page 172)

Convert a PFX to a PEM SSL Certificate (see page 176)

Use SSL on Windows

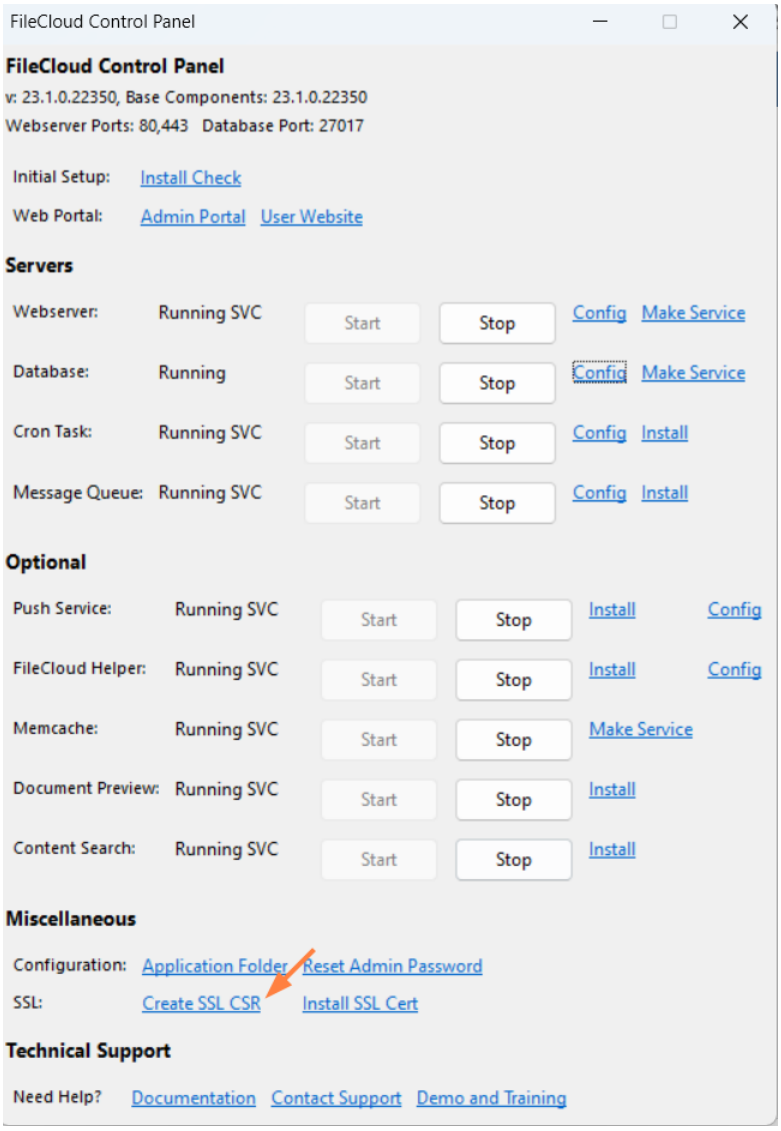
Use SSL on WIndows to establish an encrypted link between the FileCloud server and a client browser.

- This link ensures that all data passed between the web server and browsers remains 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, no additional configuration is required in FileCloud. Once the certificate is installed, all connections between the FileCloud Server and clients are secured over SSL.

To Use SSL on Windows:

1. Create a CSR in the FileCloud Control Panel. (see page 156)



FileCloud Control Panel

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 Website

Servers

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

Optional

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	Install	

Miscellaneous

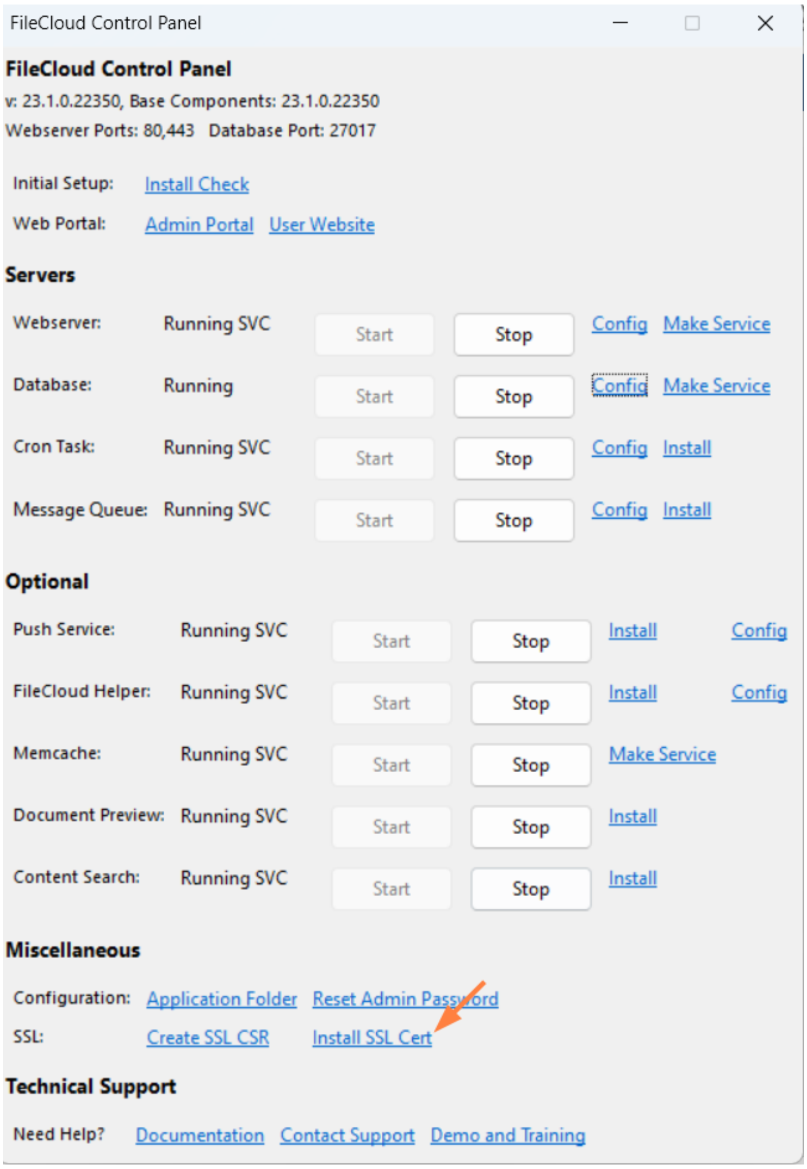
Configuration: Application Folder Reset Admin Password

SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support Demo and Training

2. Submit the CSR to your SSL provider. (see page 159)
3. The provider verifies and issues 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 you are given one download option, download that.
4. Install the certificate. (see page 161)



FileCloud Control Panel

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 Website

Servers

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

Optional

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	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

5. Follow the HTTPS Best Practices for FileCloud (see page 178).

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

Manually create a CSR to receive an SSL certificate (see page 163)

Manually install a CRT file (see page 165)

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.
- Submit the CSR to your SSL provider.
- Your provider verifies the CSR and issues an SSL certificate file.

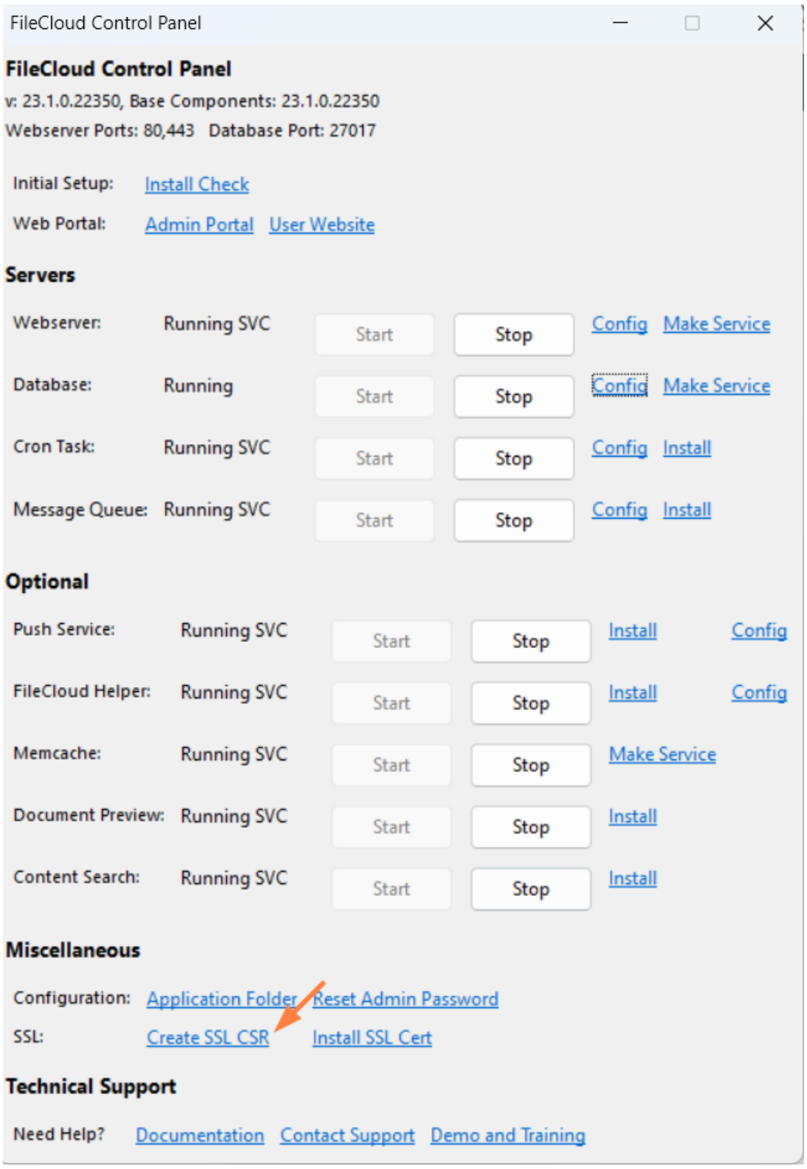
If you encounter issues using the FileCloud control panel, you can:

Manually create a CSR to receive an SSL certificate (see page 163)

To create a CSR in the FileCloud control panel:

1. Open the **FileCloud Control Panel**

2. Click **Create SSL CSR**.



FileCloud Control Panel

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 Website

Servers

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

Optional

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	Install	

Miscellaneous

Configuration: Application Folder Reset Admin Password

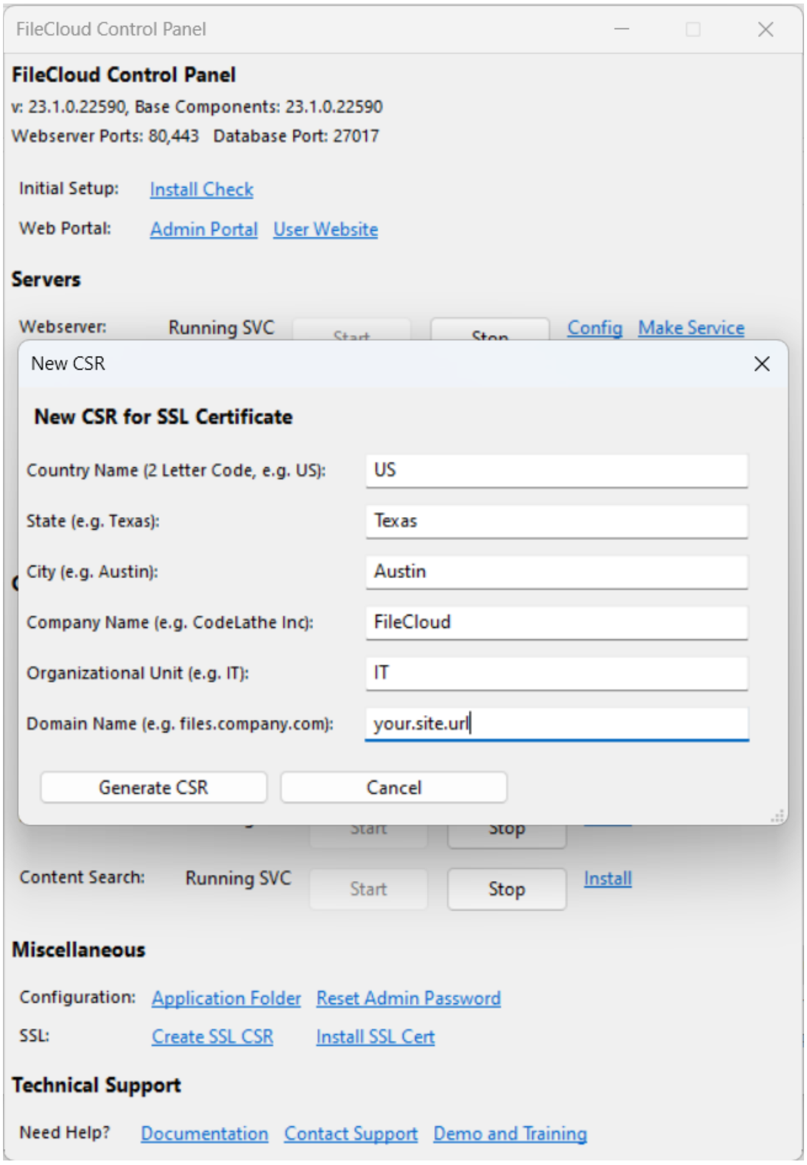
SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support Demo and Training

New CSR fields appear.

3. Enter your data into the fields.



FileCloud Control Panel
FileCloud Control Panel
v: 23.1.0.22590, Base Components: 23.1.0.22590
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
Content Search: Running SVC Start Stop Install
Miscellaneous
Configuration: Application Folder Reset Admin Password
SSL: Create SSL CSR Install SSL Cert
Technical Support
Need Help? Documentation Contact Support Demo and Training
New CSR
Generate CSR
Cancel

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

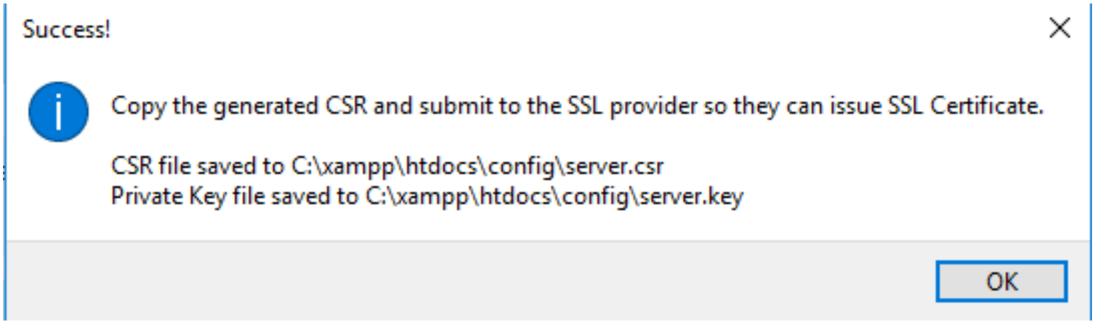
Organizational Unit (e.g. IT): IT

Domain Name (e.g. files.company.com): your.site.url

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

Information	Example	Notes
Domain Name	filecloud.IWPL.com[50]	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[51] *.yourdomain.com

4. Click **Generate CSR**.
   The following popup appears:



Success!

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

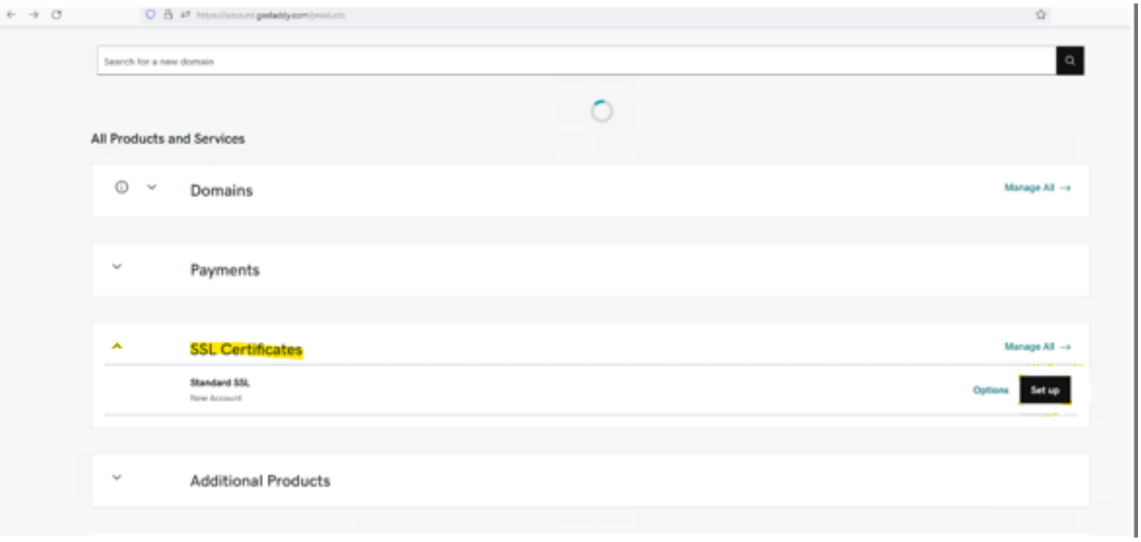
5. Submit the CSR to your SSL provider (see page 159).

Submit a CSR to Your SSL Provider

You must create your CSR (see page 156) 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.

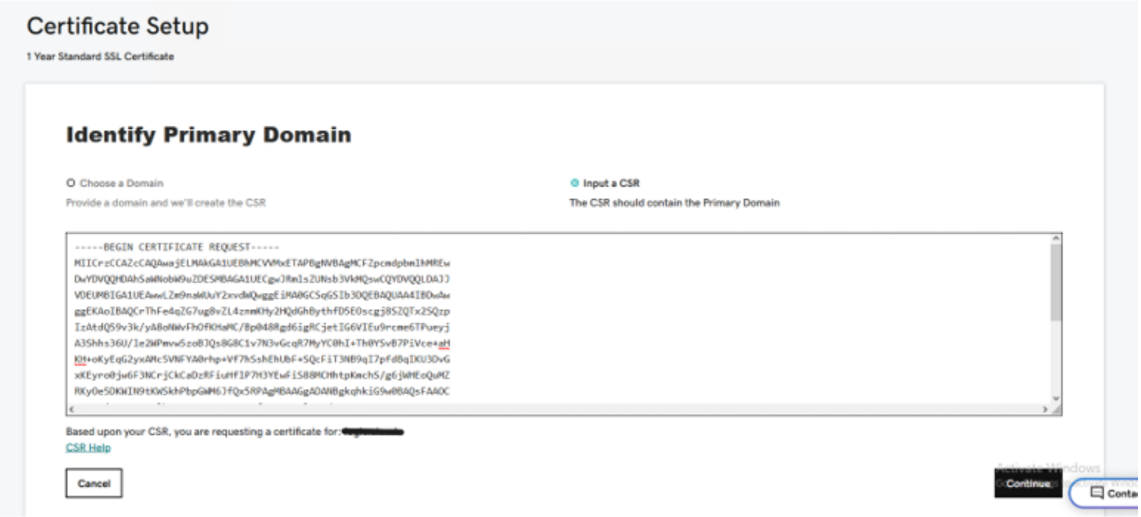
[50] http://filecloud.IWPL.com
[51] http://yourdomain.com

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



The **Certificate Setup** screen opens.

2. Click **Input a CSR.**
   Paste the content of your CSR file into the text field.



Certificate Setup

1 Year Standard SSL Certificate

Identify Primary Domain

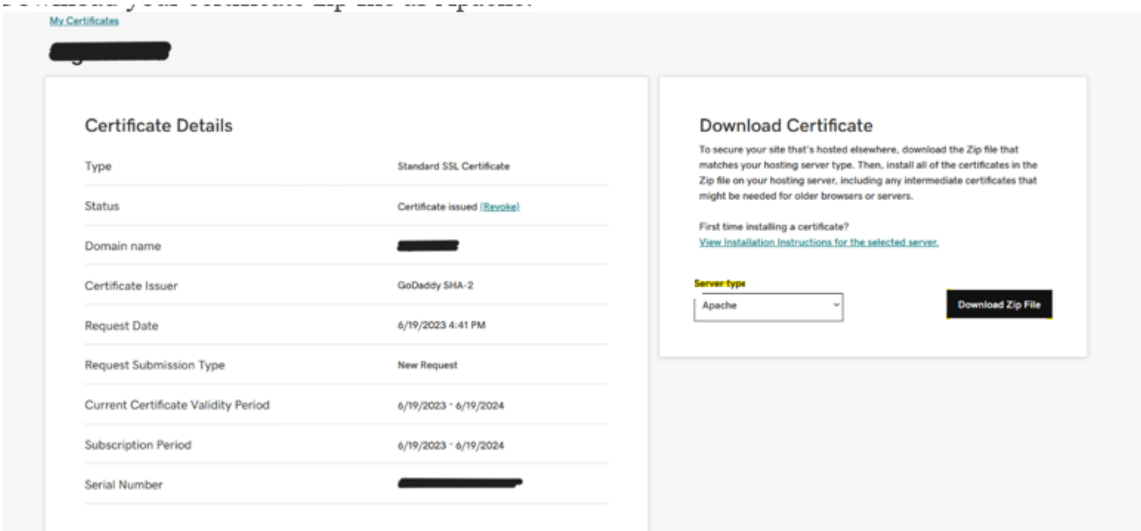
○ Choose a Domain
Provide a domain and we'll create the CSR

● Input a CSR
The CSR should contain the Primary Domain

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrzCCAZcCAQAwajELMAkGA1UEBhMCVVMxETAPBgNVBAgMCFZpcmdpbmlhMREw
DwYDVQQHDAhSaWNobW9uZDESMBAGA1UECgwJRmlsZUNsb3VkMQswCQYDVQQLDAJJ
VDEUMBIGA1UEAwwLZm9naWUuY2xvdWQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCrThFe4qZG7ug8vZL4zmmKHy2HQdGhBythfD5E0scgj8SZQTx2SQzp
IzAtdQ59v3k/yA8oNWvFhOfKHaMC/8p048Rgd6igRCjetIG6VIEu9rcme6TPueyj
A3Shhs36U/1e2WPmvw5zoBJQs8G8C1v7N3vGcqR7MyYC0hI+Th0YSvB7PiVce+aH
KH+oKyEqG2yxAMc5VNFYA0rhp+Vf7hSshEhUbF+SQcFiT3NB9qI7pfdBqIKU3DvG
xKEyro0jw6F3NCrjCkCaDzRFiuHf1P7H3YEwFiS88MCHhtpKmch5/g6jWMEoQuMZ
RKyOe5DKWIN9tKWSkhPbpGWM6JfQx5RPAgMBAAGgADANBgkqhkiG9w0BAQsFAAOC
```

Based upon your CSR, you are requesting a certificate for: [redacted]
CSR Help

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**.



My Certificates

[redacted]

Certificate Details

Type	Standard SSL Certificate
Status	Certificate issued (Revoke)
Domain name	[redacted]
Certificate Issuer	GoDaddy SHA-2
Request Date	6/19/2023 4:41 PM
Request Submission Type	New Request
Current Certificate Validity Period	6/19/2023 - 6/19/2024
Subscription Period	6/19/2023 - 6/19/2024
Serial Number	[redacted]

Download 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 might be needed for older browsers or servers.

First time installing a certificate?
View Installation Instructions for the selected server.

Server type: Apache

7. Install the certificate. (see page 161)

Install a certificate using the FileCloud Control Panel

> If you want to include an intermediate certificate and do not have one saved locally, see Extracting an Intermediate Certificate from your Browser (see page 167).

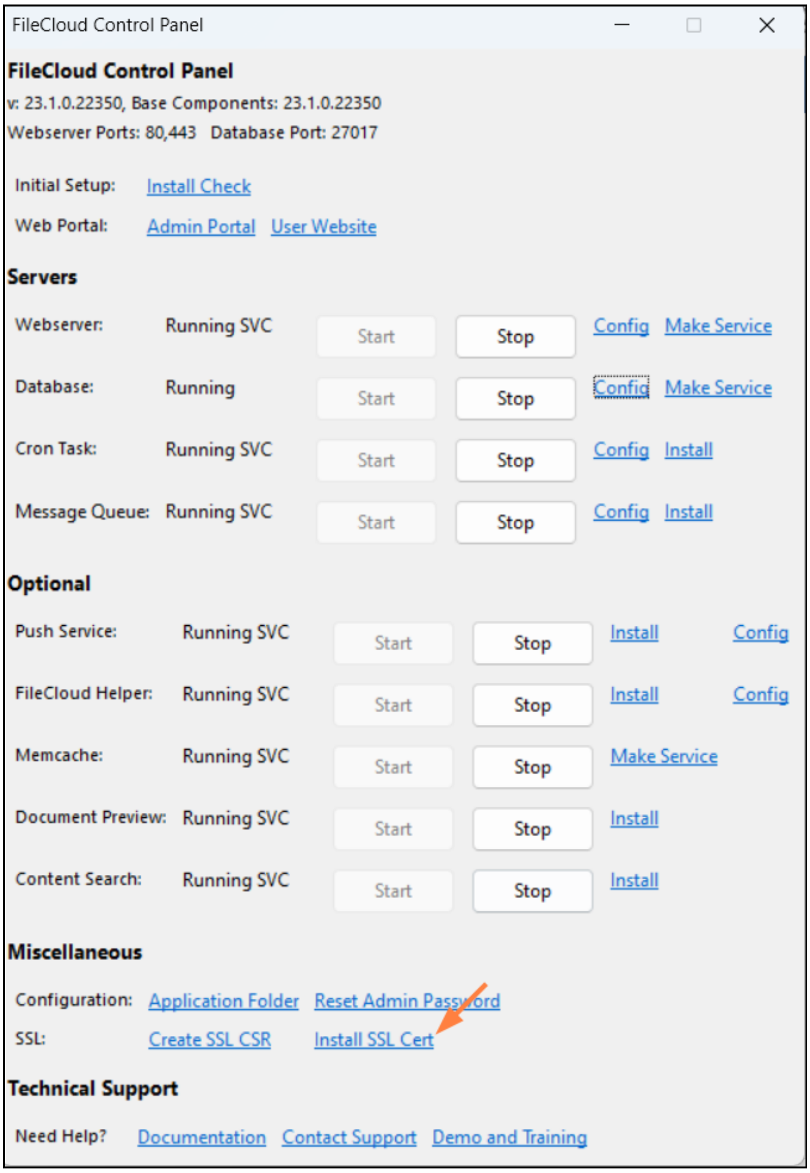
After you receive an SSL certificate, you can use the **FileCloud Control Panel** to install it.

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

Manually install an SSL certificate in Windows (see page 165)

To install an SSL Certificate using the FileCloud Control Panel:

1. Open the **FileCloud Control Panel**.
   Show me the control panel



FileCloud Control Panel

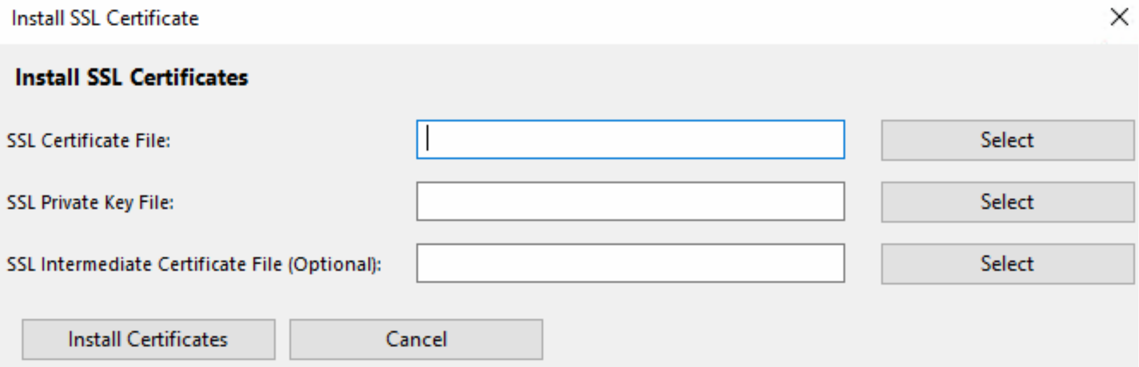
v: 23.1.0.22350, Base Components: 23.1.0.22350

Webserver Ports: 80,443 Database Port: 27017

Webserver:	Running SVC
Database:	Running
Cron Task:	Running SVC
Message Queue:	Running SVC
Push Service:	Running SVC
FileCloud Helper:	Running SVC
Memcache:	Running SVC
Document Preview:	Running SVC
Content Search:	Running SVC

FileCloud Control Panel
Initial Setup: Install Check
Web Portal: Admin Portal User Website
Servers
Start Stop Config Make Service Install
Optional
Miscellaneous
Configuration: Application Folder Reset Admin Password
SSL: Create SSL CSR Install SSL Cert
Technical Support
Need Help? Documentation Contact Support Demo and Training

2. Under **Miscellaneous**, click **Install SSL Cert**.
3. Your screen should look similar to the following example:



Install SSL Certificate

Install SSL Certificates

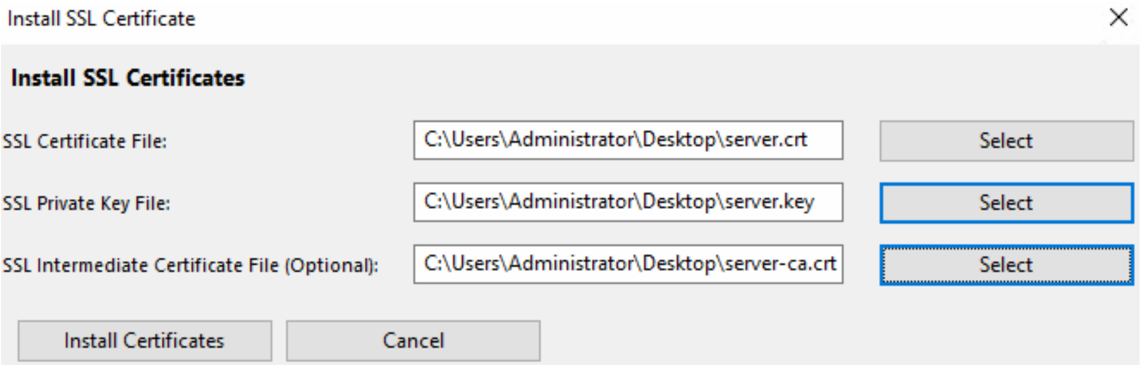
SSL Certificate File:

SSL Private Key File:

SSL Intermediate Certificate File (Optional):

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

SSL Private Key File: C:\Users\Administrator\Desktop\server.key

SSL Intermediate Certificate File (Optional): C:\Users\Administrator\Desktop\server-ca.crt

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.
- Submit the CSR to your SSL provider.
- Your provider verifies the CSR and issues an SSL certificate in a .crt file.

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 (see page 156)

To manually create an SSL certificate, 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 follwing 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:\xampp\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`

Information	Example	Notes
Organizational Unit Name	Accounts Payable	`section name`

Common Name	filecloud.IWPL.com[52]	`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**[53]
		`*.yourdomain.com`

Email Address	moneyman@iwpl.com[54]	
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 (see page 167).

You should use the FileCloud control panel to install an SSL certificate (see page 161). If you encounter issues, you can install the certificate manually.

[52] http://filecloud.IWPL.com
[53] http://yourdomain.com
[54] mailto:moneyman@iwpl.com

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.

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:

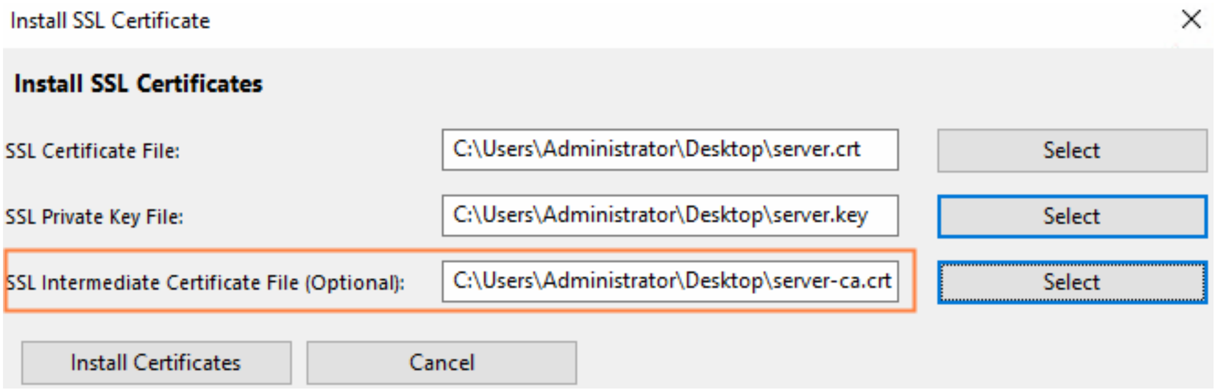
1. Installing the SSL certificate
2. Installing the chain file

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 (see page 161).



SSL Certificate File: C:\Users\Administrator\Desktop\server.crt

SSL Private Key File: C:\Users\Administrator\Desktop\server.key

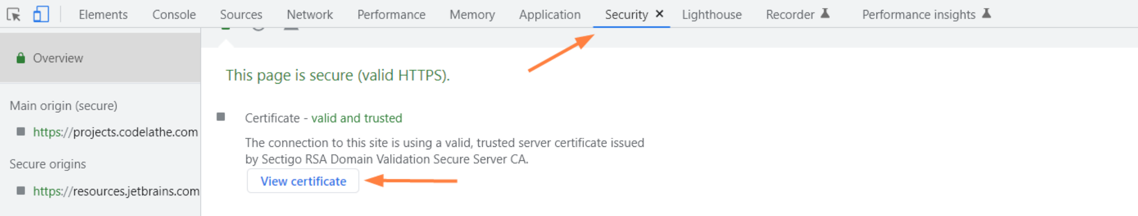
SSL Intermediate Certificate File (Optional): C:\Users\Administrator\Desktop\server-ca.crt

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.

2. Click the **Security** tab.
   Just under the listing for **Certificate** is a **View certificate** button.
3. Click the **View certificate** button.



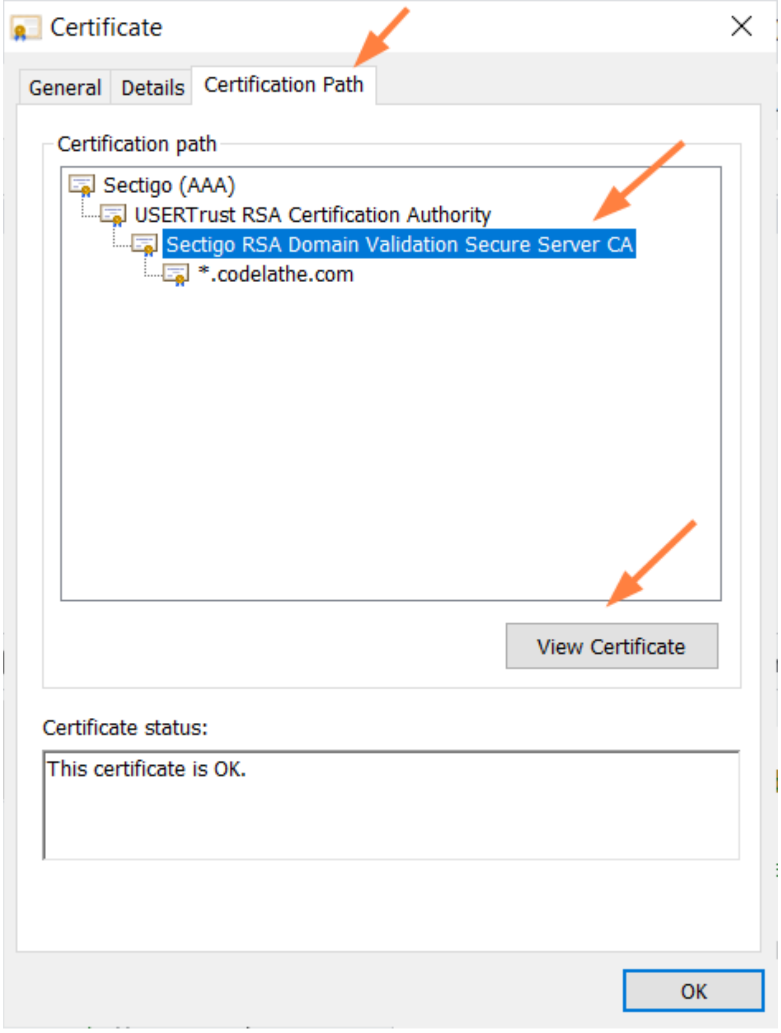
This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by Sectigo RSA Domain Validation Secure Server CA.

The certificate window opens.

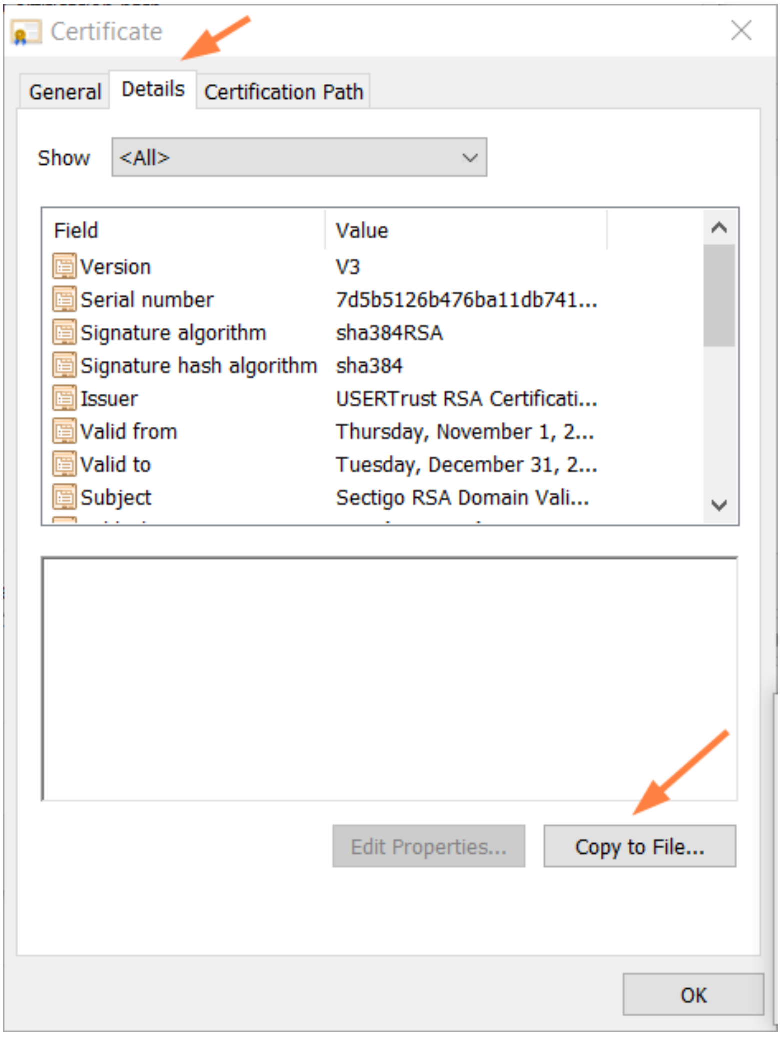
4. Click the **Certification Path** tab.
5. Select the third embedded certificate, which is the intermediate certificate.
6. Click **View Certificate**.



This certificate is OK.

Another certificate window opens.

7. Click the **Details** tab.
8. Click **Copy to File**.

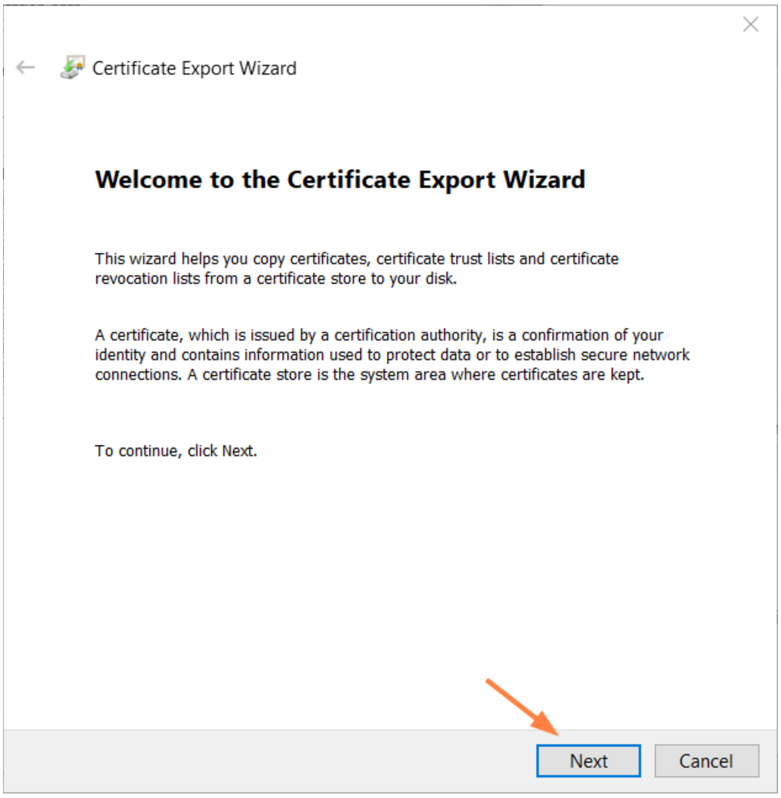


Show <All>

Field	Value
Version	V3
Serial number	7d5b5126b476ba11db741...
Signature algorithm	sha384RSA
Signature hash algorithm	sha384
Issuer	USERTrust RSA Certificati...
Valid from	Thursday, November 1, 2...
Valid to	Tuesday, December 31, 2...
Subject	Sectigo RSA Domain Vali...

The **Certificate Export Wizard** opens.

9. Click **Next**.



Certificate Export Wizard

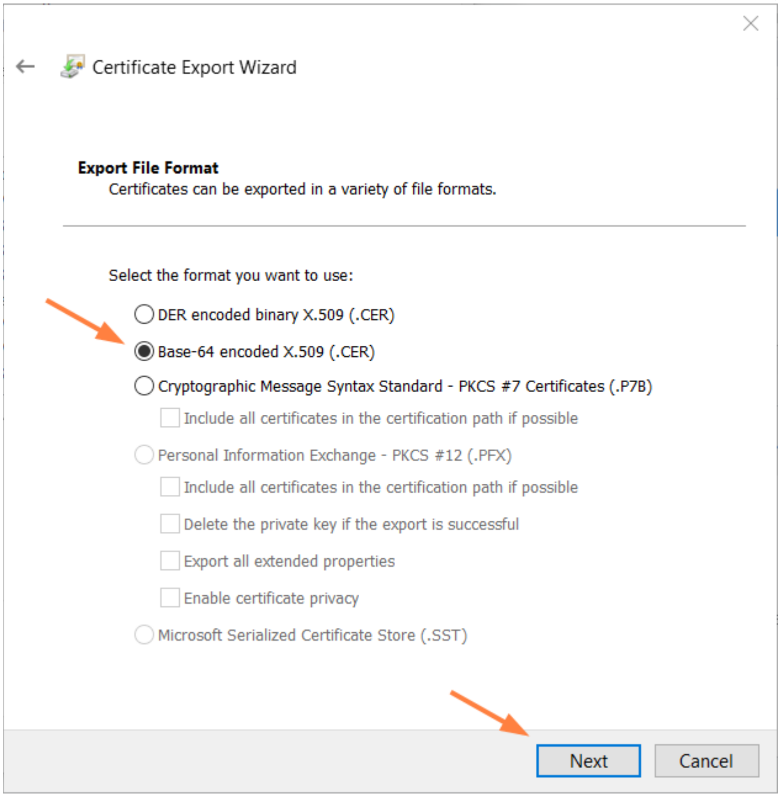
Welcome to the Certificate Export Wizard

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.

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



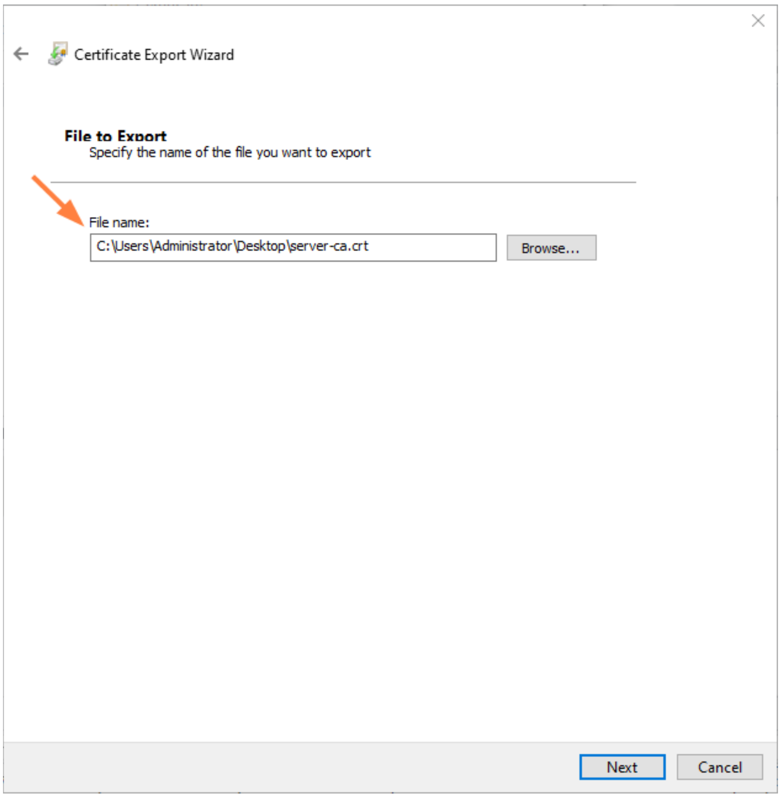
Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ 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
○ 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**.

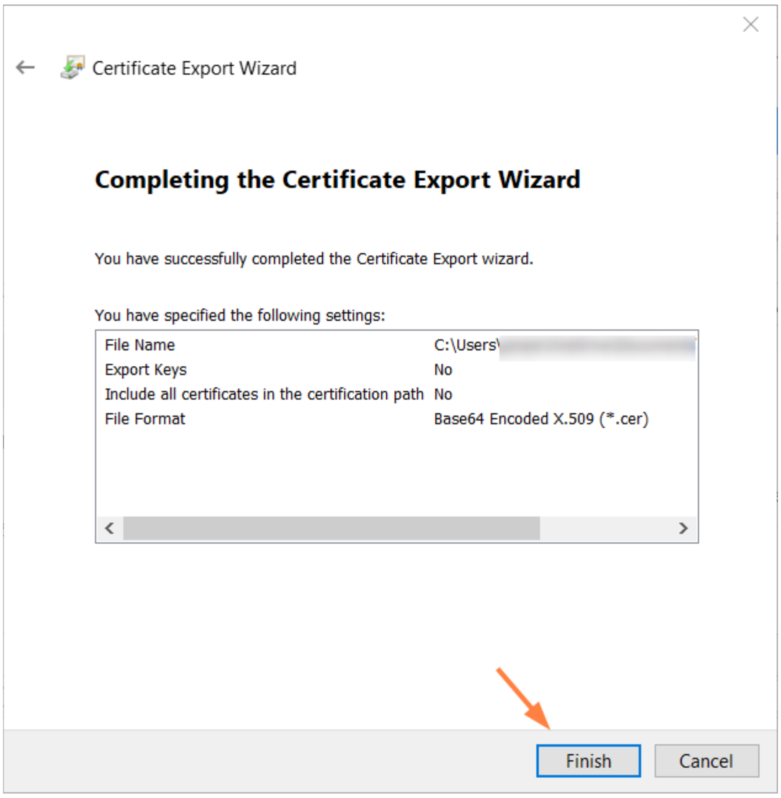


File to Export
Specify the name of the file you want to export

File name:
C:\Users\Administrator\Desktop\server-ca.crt

The last window confirms that you have completed the wizard.

13. Click **Finish**.



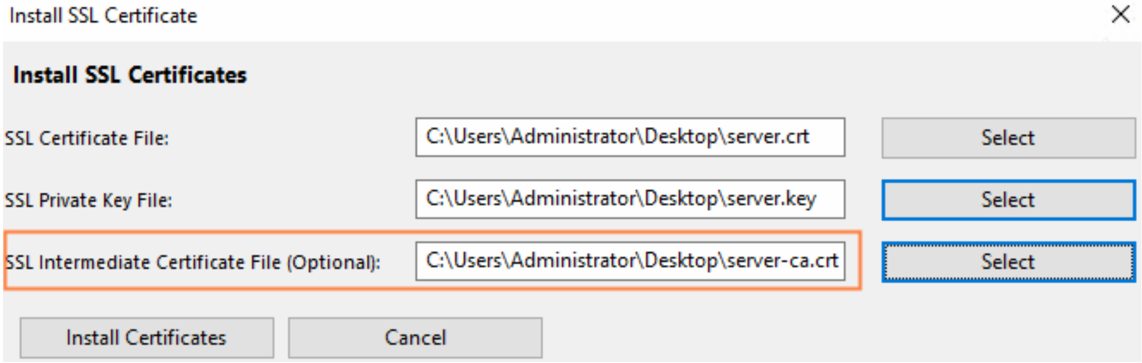
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\[redacted]
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

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



Install SSL Certificates

SSL Certificate File: C:\Users\Administrator\Desktop\server.crt

SSL Private Key File: C:\Users\Administrator\Desktop\server.key

SSL Intermediate Certificate File (Optional): C:\Users\Administrator\Desktop\server-ca.crt

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. (see page 173)
2. Submit the CSR to your SSL provider.
3. The provider verifies the CSR, and then issues 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 (see page 174).
5. Follow the HTTPS Best Practices for FileCloud (see page 178).

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. Respond the the prompts with 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`

Information	Example	Notes
Organization Name	Internet Widgits Pty Ltd	`company name`
Organizational Unit Name	Accounts Payable	`section name`

Common Name	filecloud.IWPL.com[55]	`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[56]
		`*.yourdomain.com`

Email Address	moneyman@iwpl.com[57]	
`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

[55] http://filecloud.IWPL.com
[56] http://yourdomain.com
[57] mailto:moneyman@iwpl.com

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] $ openssl pkcs12 -in [yourfile.pfx] -nocerts -nodes -out [keyfile-encrypted.key] # use this command if the first command generates empty certificate.
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 [yourfile.pfx] -cacerts -nokeys -out [server-ca.crt]
Windows	C:\xampp\apache\bin\openssl pkcs12 -in [yourfile.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

Let's Encrypt is a third-party free SSL provider authority. Debugging issues with Let's Encrypt SSL generation or renewal are outside FileCloud's scope. This document only covers the changes that need to be made in the FileCloud .htaccess file to allow URL access.

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

1. Open the following file:
   - `Windows:  C:\xampp\htdocs\.htaccess`
   - `Linux: /var/www/html/.htaccess`
2. Find the following code:

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

```
#---------------------------------------------------
```

3. 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]
#---------------------------------------------------
```

4. Save and close .htaccess.
5. Use certbot to renew your certificates. For instructions, see https://certbot.eff.org/instructions.

HTTPS Best Practices for FileCloud

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

- HTTPS (SSL)
- Port 443

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

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

https://<SITENAME>

Best Practice	Reason	Steps

Disable the existing HTTP port.	So that FileCloud can be accessed only securely via HTTPS.
	Setting **redirects from HTTP to HTTPS is not recommended** because mobile apps and other clients do not follow redirects (for security)
	Therefore removing the HTTP port completely is the best option.
	If you must use a redirect, Configure HTTP SSL Redirects (see page 183).
		To disable HTTP (port 80) for Windows:
		1. Open the webserver config file for editing:
		`c:\xampp\apache\conf\httpd.conf` `and`
		2. Comment out the line with Listen 80.
		3. Save and close the file.
		4. Restart the server.
		To disable HTTP (port 80) for Linux:
		1. Open the webserver config file for editing:
		`/etc/apache2/ports.conf`
		2. Comment out the line with Listen 80.
		3. Save and close the file.
		4. Restart the server.

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 Prov[58]ide 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.

[58] https://www.sslshopper.com/ssl-checker.html

Best Practice	Reason	Steps

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

Best Practice	Reason	Steps

Change the default HTTPS port (443).	If you have are conflicts with other ports.	**For Windows**:
		1. Open the following file for editing:
		`c:\xampp\apache\conf\extra\httpd-ssl.conf`
		2. Locate the following line
		`Listen 443`
		3. Change it to
		`Listen your_new_port`
		4. Locate the following line
		`<VirtualHost _default_:443`
		5. Change it to
		`<VirtualHost _default_:your_new_port>`
		6. Save and close the file.
		
		For Linux:
		1. Open the following file for editing:
		`/etc/apache2/ports.conf`
		2. Locate the following lines
		`<IfModule mod_ssl.c>Listen 443</IfModule>`
		3. Change it to
		`<IfModule mod_ssl.c>Listen Your_New_Port</IfModule>`
		4. Open the following file for editing:
		`/etc/apache2/sites-available/default-ssl`
		5. Locate the following line:
		`<VirtualHost _default_:443>`
		6. Change it to
		`<VirtualHost _default_:your_new_port>`
		7. Save and close the file.

Best Practice	Reason	Steps

Disable server information in headers.	To prevent the Web application from disclosing the server name and server version in the response header.	1. Open the Apache configuration file:
		Ubuntu location: /etc/apache2/apache2.conf
		RHEL location: /etc/httpd/conf/httpd.conf
		Windows location: C:\xampp\apache\conf\httpd.conf
		2. Add the following:
		`ServerSignature Off`
		`ServerTokens Prod`
		3. Restart the Apache server.

HTTP To HTTPS Redirects

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

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

Therefore removing the HTTP port completely is the best option.

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

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

- In Windows, the above lines should we added to file c:\xampp\apache\conf\extra\httpd-vhosts.conf. Restart the apache server.
  Also make sure the following line is uncommented in the file C:\xampp\apache\conf\httpd.conf.

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

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

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 (see page 178)

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)**

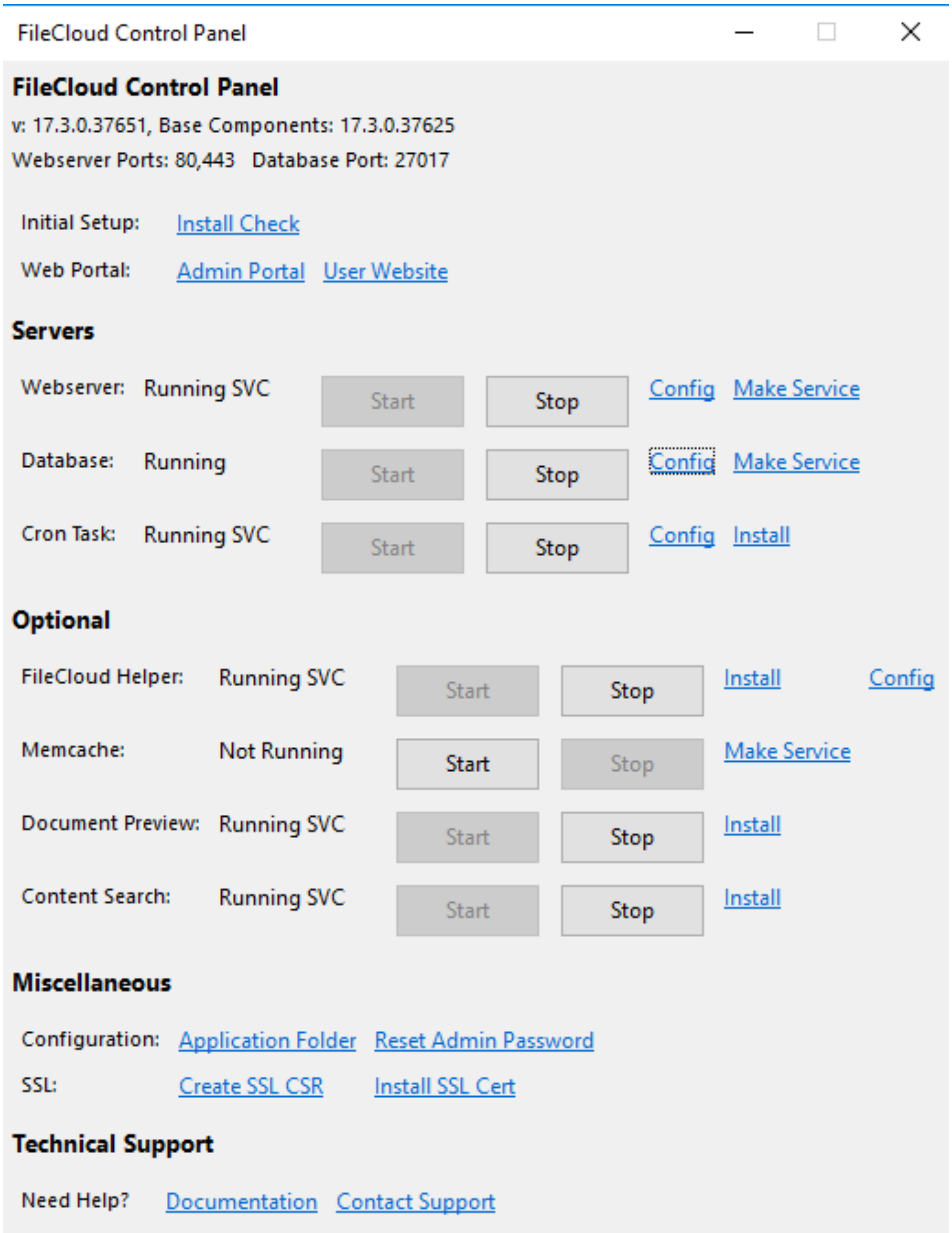
If other programs are using these ports, the FileCloud server will not start up properly.

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 that you disable HTTP port on the FileCloud server.

To change the ports, open the FileCloud Control Panel.



FileCloud Control Panel

FileCloud Control Panel

v: 17.3.0.37651, Base Components: 17.3.0.37625

Webserver Ports: 80,443 Database Port: 27017

Initial Setup: Install Check

Web Portal: Admin Portal User Website

Servers

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

Optional

FileCloud Helper:	Running SVC	Start	Stop	Install	Config
Memcache:	Not Running	Start	Stop	Make Service	
Document Preview:	Running SVC	Start	Stop	Install	
Content Search:	Running SVC	Start	Stop	Install	

Miscellaneous

Configuration: Application Folder Reset Admin Password

SSL: Create SSL CSR Install SSL Cert

Technical Support

Need Help? Documentation Contact Support

To change a port or Web server setting:

1. On the server, from the *Windows Start* menu, select the FileCloud Control Panel, or double-click the **xampp/cloudcp.exe** file.
2. In the Servers section, for Webserver, click **Stop**.
3. Change the Port configuration according to HTTPS Best Practices for FileCloud (see page 178).
4. To start the web server, click **Start** next to **Webserver**.
5. In the **Servers** section, for **Database**, click **Stop**, then **Config**.
6. Make your changes, save them, and next to **Database**, click **Start**.

7. If you have changed the default web server, open **localconfig.php** at:
   Windows Location: **XAMPP DIRECTORY/htdocs/config/localconfig.php**
   Linux Location: **/var/www/config/localconfig.php**
   and add the following, replacing n.n.n.n with the correct IP address.

   ```
   define("TONIDOCLOUD_APACHE_BIND_IP", "n.n.n.n");
   ```

SELinux Policies For FileCloud Installation

SELinux is a Linux kernel security module that defines the access and transition rights of every user, application, process, and file on the system.

- It then governs the interactions of these entities using security policies that specifies how strict or lenient a given Linux installation should be.
- It is available as part of distros like Red Hat Enterprise Linux.

In order to use Filecloud on a selinux enforcing OS, the following steps need to be followed.

1) If SELinux is disabled, it needs to be enabled. For that, use the below command

> *setenforce 1*

2) To allow writable access to folders used by FileCloud, use the following commands. These commands label the mentioned folder and it's contents with required context.

For a managed storage path "/opt/fileclouddata" :

> *semanage fcontext -a -t httpd_sys_rw_content_t /opt/fileclouddata.**
>
> *restorecon -Rv /opt/fileclouddata*

For default FileCloud install folder path "/var/www/html"

> *semanage fcontext -a -t httpd_sys_rw_content_t /var/www/html.**
>
> *restorecon -Rv /var/www/html*
>
> *semanage fcontext -a -t httpd_sys_script_exec_t /var/www/html/thirdparty/prop/p23l*

```
restorecon -Rv /var/www/html/thirdparty/prop/p23l
```

Add all additionally required folders (such Network folders) using semanage and restorecon commands

3) To allow FileCloud access to services like MongoDB and Solr, use the following commands

```
setsebool -P httpd_can_network_connect_db 1

setsebool -P httpd_can_network_connect 1

setsebool -P httpd_builtin_scripting 1  # Enabled by default
```

Optional

Apart from the above steps, you can do SELinux filesystem auto labeling, or if firewall or iptables is running on the system, then the below commands need to be executed.

Selinux

-for SELinux to do auto labeling of the whole filesystem after a reboot we do this command, this command is used generally with a new system:

```
touch /.autorelabel; reboot
```

Iptables

To allow FileCloud public access, use the below commands.

```
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT  # Use only if HTTPS not enabled : This enables access on unsecure HTTP port 80

iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Firewalld

To allow FileCloud public access, use the below commands.

```
firewall-cmd --add-service=http --zone=public --permanent  # Use only if HTTPS not enabled : This enables access on unsecure HTTP port 80

firewall-cmd --add-service=https --zone=public --permanent

firewall-cmd --reload
```

Troubleshooting

In Some cases, Selinux may cause problems with services running Filecloud, the proper troubleshooting need to be done in order to identify the missing policies to make different services work properly.

On Redhat based Linux systems the first place to look for SELinux warnings is /var/log/messages, where you will find different warnings with their explanation and the command to execute in order to add the related policy.

another place to look for SElinux logging messages and it depends on the Linux distribution is /var/log/audit/audit.log, you will find a detailed audit log file and its very verbose which will help you investigate your problem.

once you identified the missing policy you can add it with "setsebool -P", knowing that -P will make all pending values written to the policy file on disk. So they will be persistent across reboots.

some of the SElinux command that can be added to make Filecloud work properly depending on the use case and architecture are :

```
setsebool -P httpd_can_network_connect_db 1

setsebool -P httpd_can_network_connect 1

setsebool -P httpd_builtin_scripting 1 # Enabled by default

setsebool -P httpd_execmem 1

setsebool -P httpd_use_nfs 1
```

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.

The following list presents some of the issues we've encountered.

Webserver or Database Does Not Start

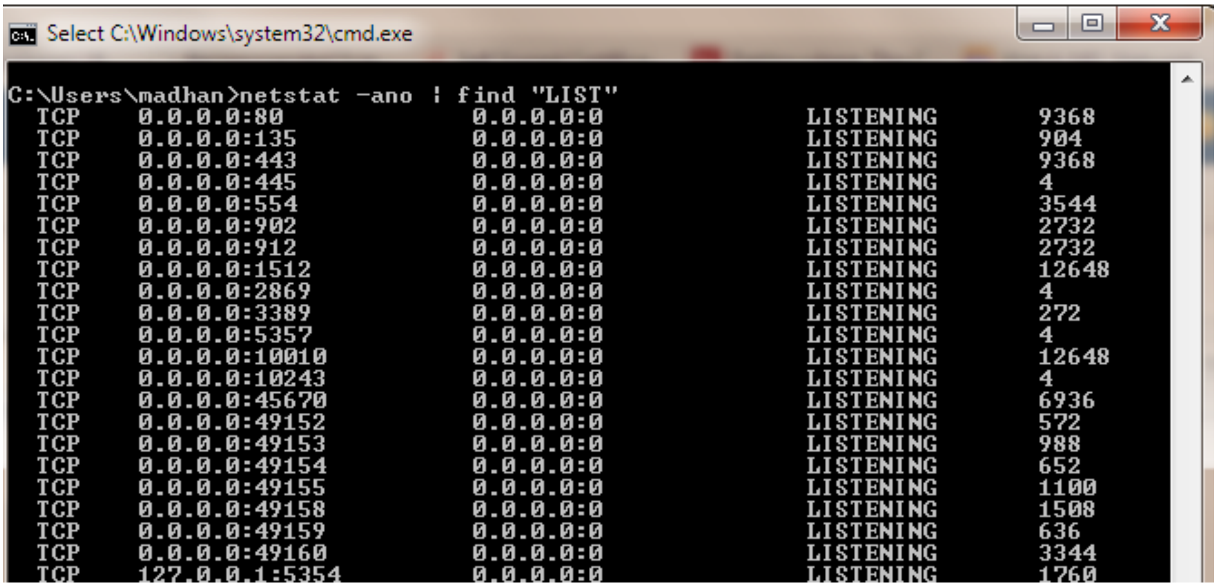
FileCloud Server not starting on Windows

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"



```
C:\Users\madhan>netstat -ano | 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            0.0.0.0:0              LISTENING       2732
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       2732
  TCP    0.0.0.0:1512           0.0.0.0:0              LISTENING       12648
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       272
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:10010          0.0.0.0:0              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          0.0.0.0:0              LISTENING       572
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       988
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:49155          0.0.0.0:0              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          0.0.0.0:0              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.

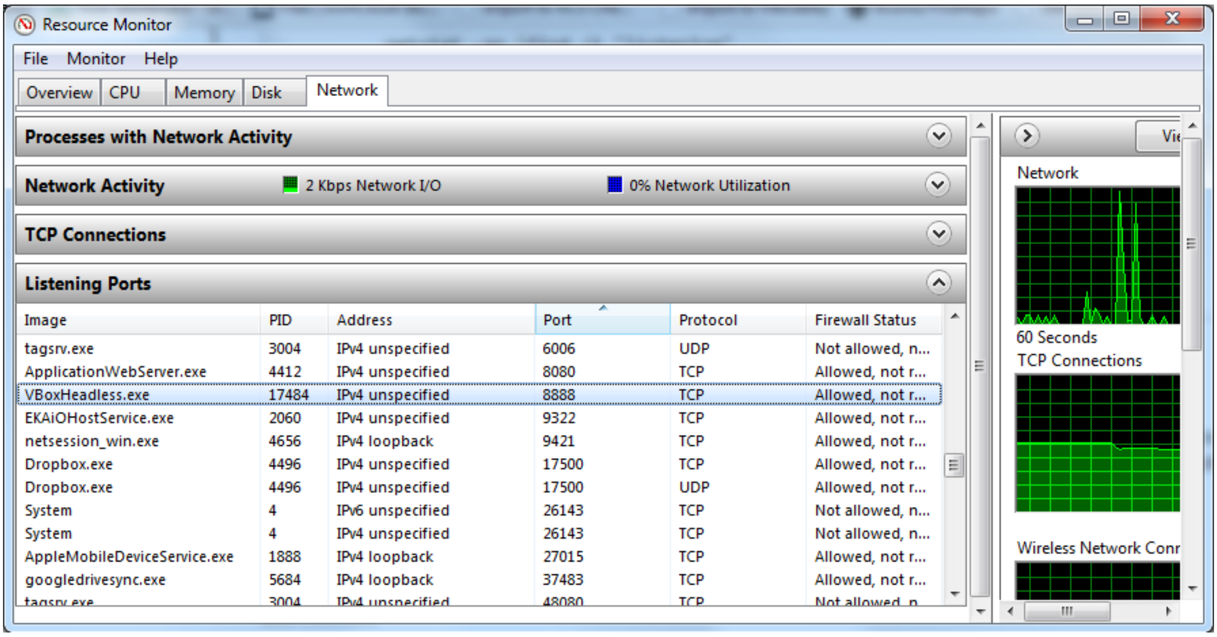


Image	PID	Address	Port	Protocol	Firewall Status
tagsrv.exe	3004	IPv4 unspecified	6006	UDP	Not allowed, n...
ApplicationWebServer.exe	4412	IPv4 unspecified	8080	TCP	Allowed, not r...
VBoxHeadless.exe	17484	IPv4 unspecified	8888	TCP	Allowed, not r...
EKAiOHostService.exe	2060	IPv4 unspecified	9322	TCP	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...
googledrivesync.exe	5684	IPv4 loopback	37483	TCP	Allowed, not r...
tagsrv.exe	3004	IPv4 unspecified	48080	TCP	Not allowed, n

Common services interfering with ports used by FileCloud:

Other Apps Using same Network Services
WWW Publishing Service
Microsoft IIS
Microsoft Skype

Other Apps Using same Network Services
HTTPD.sys

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)

ℹ 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@filecloud.com[59])

[59] http://codelathe.com

Storage and Client Application Limits

FileCloud offers a number of different storage options. When choosing your storage options, consider the limitations of each. 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 the **allowedfilelist** option on the page XML Options for Sync.
FileCloud Drive App	See Requirements for the minimum and maximum Windows versions supported by FileCloud.
	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

CIFS and NFS

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.

To mount shares

- How to Mount CIFS Shares from Windows Command Line (see page 194)
- How to properly mount a CIFS share on RHEL for FileCloud (see page 195)
- Mount a CIFS Share on Ubuntu for FileCloud (see page 197)
- How to properly mount a NFS share on Linux for FileCloud (see page 199)

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.
2. Type the following, replacing *X:* with drive letter of the shared resource:

   ```
   net use  Z: /delete
   ```

How to properly mount a CIFS share on RHEL 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
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

Prerequisites

Ensure the command mount.cifs is present in your distro. Here is the list of packages that provide this utility in different distros.

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=07
77,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=utf8,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.

Mount a CIFS Share on Ubuntu 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.

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=07
77,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 *winuser* and *winpass* 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.

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.

Prerequisites

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
/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.