FileCloud Server

Version 23.263

About FileCloud for Administrators

13 October, 2026

Table of Contents

FileCloud Storage 3
Managed Storage (My Files): 3
Network Shares: 3
Large Deployments 6
Additional Resources 7
FileCloud Sizing Guide 8
FileCloud Hardware Sizing 8
High-Availability Requirements 9
Requirements 13
Supported operating systems and installed software 13
Required hardware 15
Necessary network configurations 15
Open Source Software Libraries Used in FileCloud 18
Logging In to the Admin Portal 19
Accessing the Admin Portal 19
Logging in with Default Credentials 19
Log in using 2FA 20
Collection of usage data 24
Viewing and Clearing Checklist Notifications 25
Customizing the Login Page 26

FileCloud is a scalable, self-hosted enterprise file sharing, synchronization, and endpoint backup solution.

FileCloud is a cloud-agnostic enterprise file services platform. You can self-host it on your on-premises servers and private data centers, or you can host it on public cloud IaaS providers like AWS, Azure or Google Cloud.

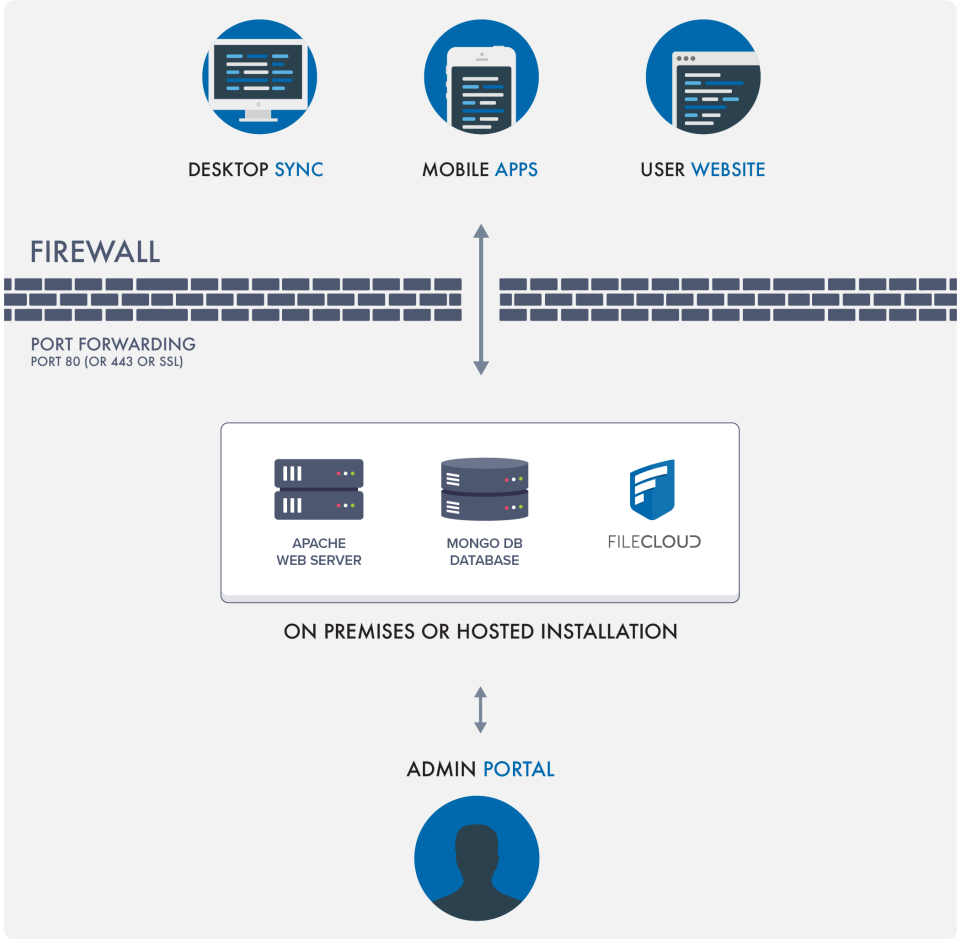
A self-hosted solution such as FileCloud offers the same features and benefits as public cloud SaaS services, but doesn't have many of the drawbacks of public cloud SaaS services, including:

- Issues related to control over critical enterprise and customer data
- Concerns about security and privacy of data
- Issues connected to regulatory compliance for many industries
- Issues related to data residency, sovereignty and ownership of critical data
- Lack of customization: organization branding and custom terms of service

FileCloud allows you to run your own private cloud storage and sync solution for your employees, customers and clients allowing complete control of your organizational data. FileCloud also allows you to securely provide access to existing organizational file shares (Windows NTFS File Shares, CIFS, NFS, etc.) through a web portal and mobile apps without requiring a VPN.

The Underlying Architecture

FileCloud software is typically installed on a server (Linux or Windows). There is an admin portal to configure and manage the system.



Once configured, users can access FileCloud using:

- Web browsers
- Mobile apps
- Desktop clients that keep their desktop folders in sync

See a quick video on the FileCloud Architecture basics.

FileCloud Storage

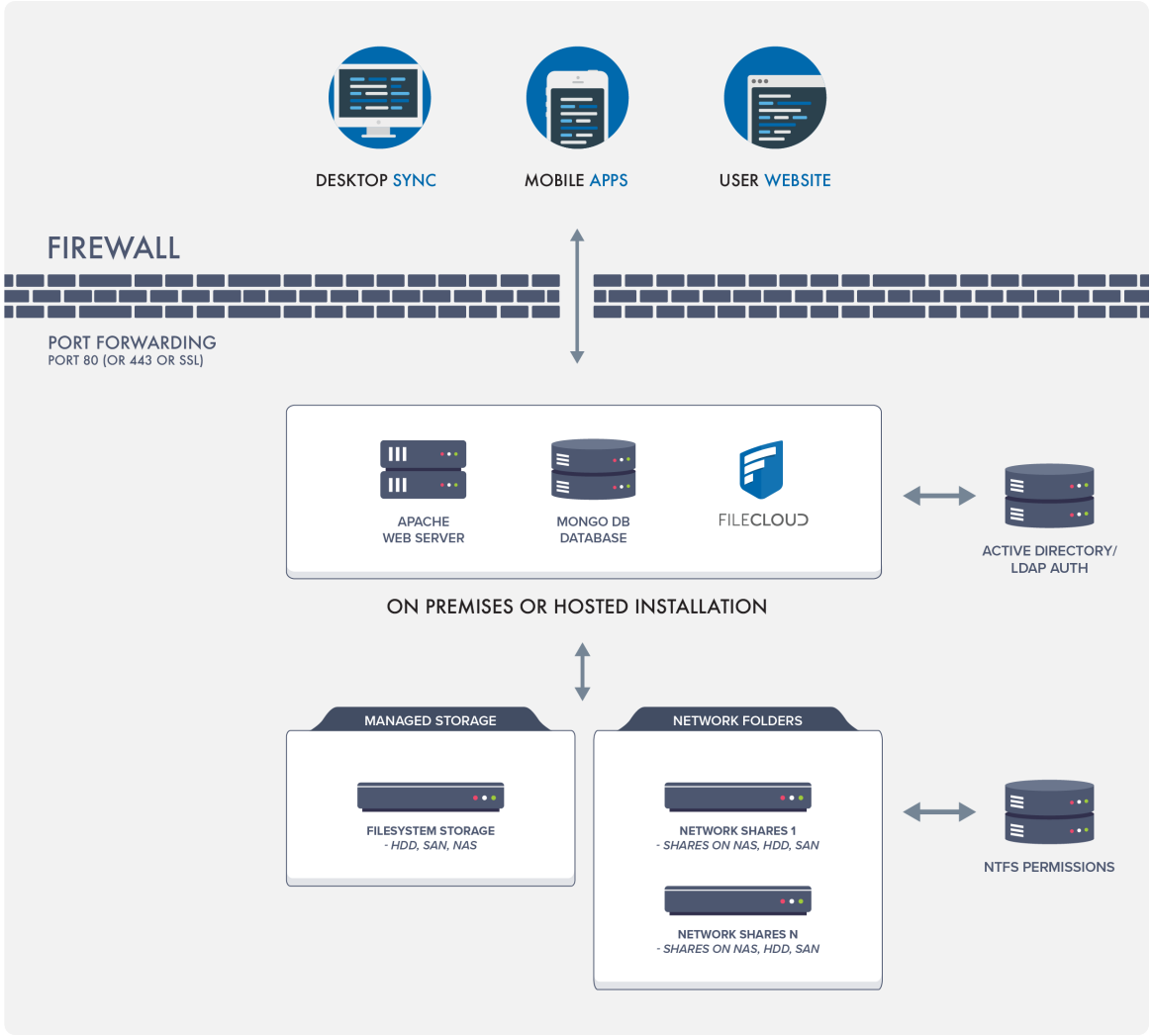
FileCloud can manage and make available two types of storage:

Managed Storage (My Files):

Managed Storage (My Files) is fully managed storage that is maintained by FileCloud. Users get storage quotas and can access, share, and sync all files in managed storage. This is available in the My Files folder.

Network Shares:

Admins can optionally make existing organizational folder shares available through FileCloud. Such shares can be accessed via web browser or mobile apps for instant remote access wherever you are. This is available in the Network Shares folders.



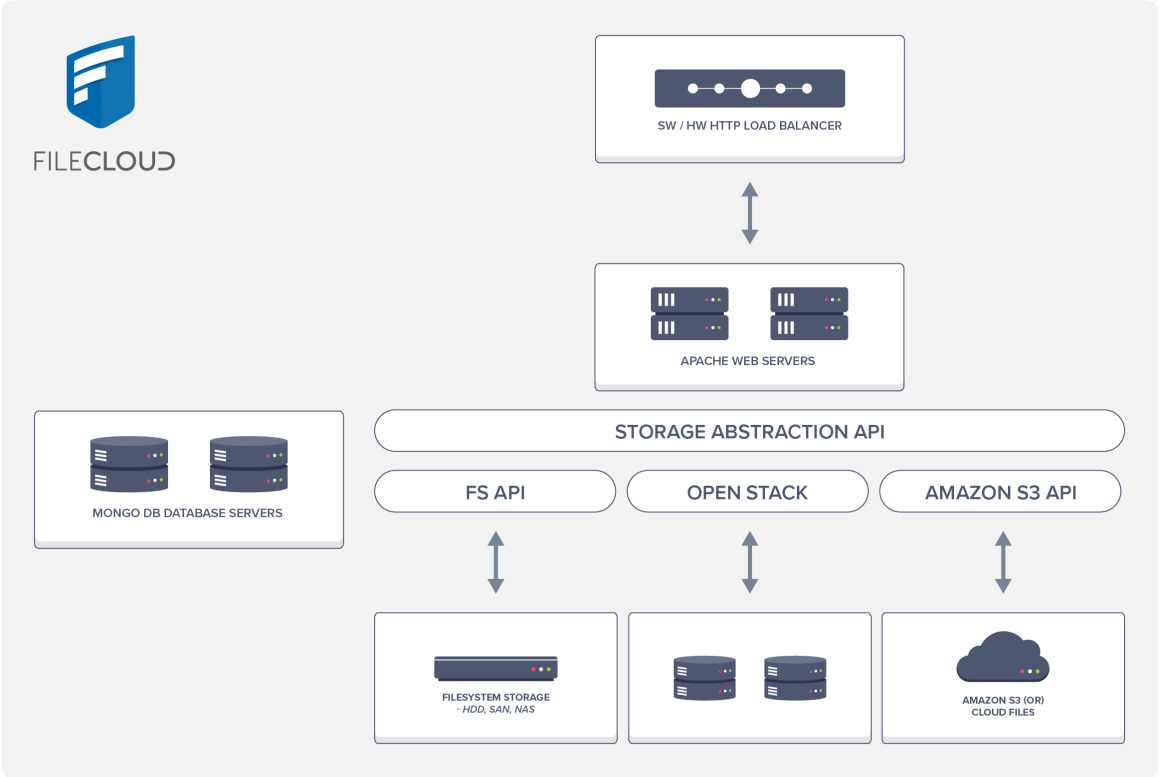
See a quick video on the differences between Managed Storage and Network Shares.

Feature	Managed Storage	Network Shares
Connection	HDD, NAS Drive, CIFS, NFS Network Shares, Amazon S3, Azure Blob Storage	CIFS, NFS Network Shares, Amazon S3, Azure Blob Storage
Sync	Yes (Realtime)	Scheduled sync 30 mins, 60 mins etc. Real time syncing has been successful in tests for folders containing up to 100,000 files.
FileCloud Drive	Yes	Yes
Offline Access	Yes via Sync App	Yes via Sync App's Offline Access
Read NTFS Permissions	NA	Yes
Previous Versions Support	Yes	Yes
Recycle Bin Support	Yes	Yes
Text Search	Yes	Yes, when indexing is enabled
Metadata	Yes	Yes
Governance - Retention	Yes	No
Content Classification	Yes	No
DLP	Yes	Yes
DRM	Yes	Yes
Workflows	Yes	Yes

Feature	Managed Storage	Network Shares
Zero Trust File Sharing	Yes	No
ServerSync	Yes	No
ServerLink Support	Yes	No
Path Limits	No Limits	Subject to 256 max path limits when network shares are in Windows

Large Deployments

For small deployments, you can use FileCloud with Local Storage configuration.
For larger deployments, use redundant object storage systems like OpenStack or Amazon S3.
We also recommend using a HA configuration with a database cluster when running a system with many users.



Additional Resources

FileCloud Tour
Blog
Vote for new features!

FileCloud Sizing Guide

This document explains hardware sizing and high availability setup for FileCloud deployments.

- The FileCloud system can be deployed on physical servers
- FileCloud Server can also be deployed in a virtualized environment (VMware, XEN)
- The FileCloud system integrates with any NFS, CIFS, or SAN appliance or s3 compatible object-storage system for file storage

FileCloud Hardware Sizing

The following table shows the underlying usage assumptions used to calculate FileCloud hardware requirements.

The model assumes:

- a user interacts 60 times per day using one of the FileCloud clients (browser, mobile app, Drive client)
- every user synchronizes data with a Sync client on an average of 2.5 devices

Based on these usage assumptions, FileCloud servers need :

- to handle 290-300 calls per second
- to support 3000 users

FileCloud Performance Model	
Browser + Mobile + Drive Apps	
Browser + Mobile + Drive Client Interactions Per Day	60
No of API calls per Interaction	20
Calls Per Second Per User	0.013889
Desktop Sync App	
% of Users using sync app	250
Sync Check Frequency (secs)	30

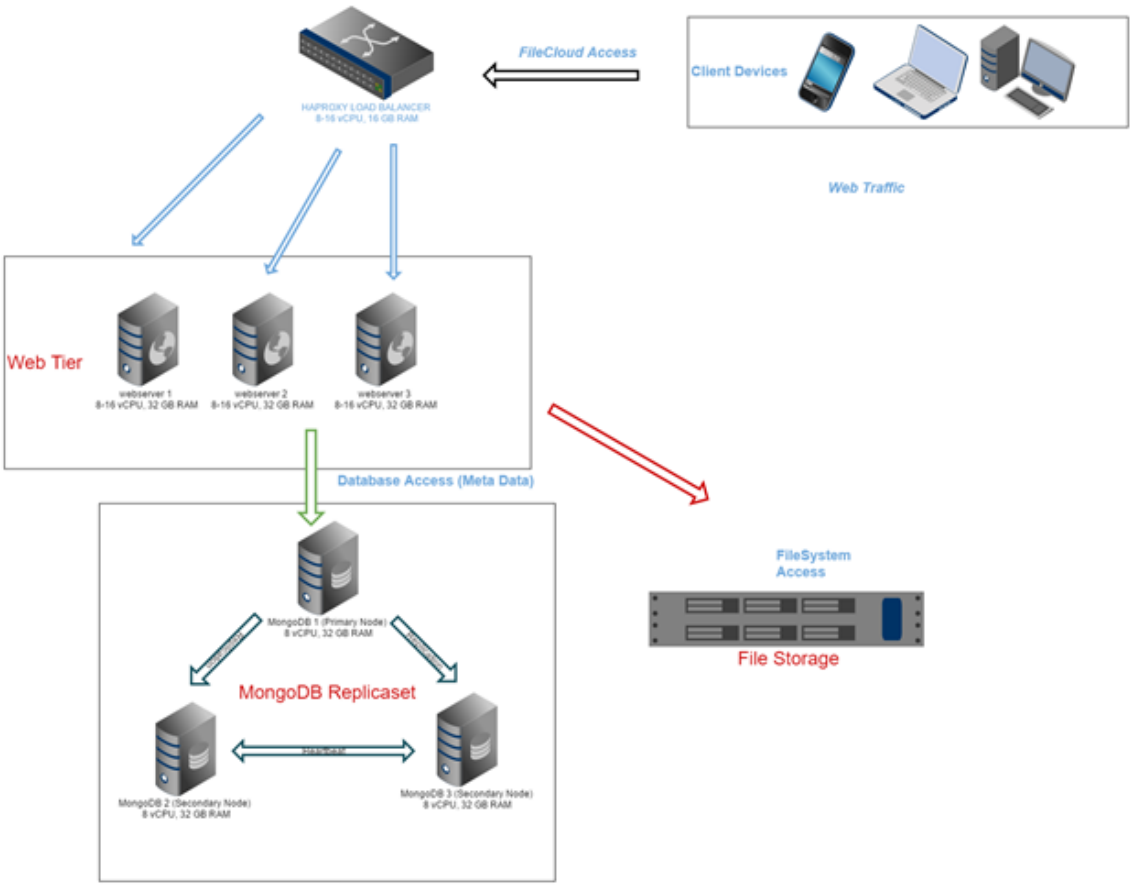
Sync App Online (Hours)	24
Calls Per Second per User	0.083333
Total Calls Per Second Per User (Sync + other Apps)	0.097222
User Counts	
Total users in installation	3000
Total Calls Per Second	291.67
Server Performance	
Server Handles Requests Per Second	125
Servers Needed	**2.33**
8-16 CPU 2.6 GHz Intel Xeon with 32 GB RAM	~125-150 reqs/sec

To calculate how many web server nodes you need based on the number of users, see the linked spreadsheet.

FileCloud Sizing Model.xlsx

High-Availability Requirements

The following diagram explains the FileCloud High Availability Setup


HAPROXY LOAD BALANCER
8-16 vCPU, 16 GB RAM
FileCloud Access
Client Devices
Web Traffic
Web Tier
webserver 1
8-16 vCPU, 32 GB RAM
webserver 2
8-16 vCPU, 32 GB RAM
webserver 3
8-16 vCPU, 32 GB RAM
Database Access (Meta Data)
MongoDB 1 (Primary Node)
8 vCPU, 32 GB RAM
MongoDB Replicaset
MongoDB 2 (Secondary Node)
8 vCPU, 32 GB RAM
MongoDB 3 (Secondary Node)
8 vCPU, 32 GB RAM
FileSystem
Access
File Storage

<table>
<tr><th>Component</th><th>Requirements</th><th>Notes</th></tr>
<tr><td>Web App Server</td><td>1 AWS m4.2xlarge instance can handle approximately 125-150 FileCloud requests per second.
To handle 3000 users one will require 2-3 web server instances with m4.2xlarge configuration.
AWS m4 instances uses processors identical to Intel E5-2670 v3 processors.
To equate this to a virtualized environment, you will require 3 VM nodes and each node need to have the following specs: 8 vCPUs and 32 GB RAM.
SSDs are recommended for application servers.
<table>
<tr><th>Instance Name</th><th>vCPU Count</th><th>RAM</th><th>Instance Storage</th><th>Network Performance</th><th>EBS-Optimized</th></tr>
<tr><td>m4.large</td><td>2</td><td>8 GiB</td><td>EBS Only</td><td>Moderate</td><td>450 Mbps</td></tr>
<tr><td>m4.xlarge</td><td>4</td><td>16 GiB</td><td>EBS Only</td><td>High</td><td>750 Mbps</td></tr>
<tr><td>m4.2xlarge</td><td>8</td><td>32 GiB</td><td>EBS Only</td><td>High</td><td>1,000 Mbps</td></tr>
<tr><td>m4.4xlarge</td><td>16</td><td>64 GiB</td><td>EBS Only</td><td>High</td><td>2,000 Mbps</td></tr>
<tr><td>m4.10xlarge</td><td>40</td><td>160 GiB</td><td>EBS Only</td><td>10 Gbps</td><td>4,000 Mbps</td></tr>
</table></td><td></td></tr>
<tr><td>Load Balancer</td><td>You must have a software (haproxy) or hardware load balancer for the web application servers.
In a virtualized environment, a load balancer is equivalent to a computer with the following specs:
• 1-2 vCPU
• 4-8 GB RAM</td><td>If you choose to go with HAPROXY, you must use one of the specs for the load balancer:
• m4.large</td></tr>
<tr><td>Database Server</td><td>You will need a 3 node MongoDB replica set for FileCloud HA configuration.
• Each node must have the specs of m4.xlarge or equivalent configuration.
• In a virtualized environment it is equivalent to 8-16 vCPU and 16-32 GB RAM.
• More RAM is better for the Database because MongoDB keeps the working set in RAM
• SSDs are recommended for database servers</td><td>You can probably use 1 TB SSD for each of the node.
It is ideal if the MongoDB node VMs can be housed in different physical host.</td></tr>
</table>

Component	Requirements	Notes
Network	For the front-end network, the following is recommended: • A gigabit or 10GigE network leading to a load balancer and from the load balancer to the 3 web app servers. • At least a gigabit Ethernet For internal networking between the servers, the following is also recommend: • At least a Gigabit Ethernet to reduce the potential for bottlenecks.	Each server should have a dedicated connection to: • Database cluster • File storage (CIFS, NFS or SAN).
File Storage	If an average usage is 5-10 GB per user, then you will require: • 25-30 TB space (3000 users) in your storage appliance • Storage must be exposed as CIFS or NFS share in the web application server instances	

Requirements

- Beginning with FileCloud 23.1, FileCloud no longer supports Ubuntu 18.04/20.04, CentOS 7/ RHEL 7 and RHEL 8. In addition, FileCloud no longer supports Debian. If you are using any of those OS versions, please migrate to Ubuntu 22.04 LTS or RHEL 9.
- Beginning with FileCloud 23.1, Linux installation and upgrades moved to a new repository system.
  The operating systems currently supported are:
  Ubuntu 22.04 LTS
  RHEL 9.x
  Since support for OpenSSL 1.1.1 ends on September 11, 2023, FileCloud 23.232 uses OpenSSL 3.x. which is not available for previous Linux versions, and therefore FileCloud requires installation or update on the Linux versions listed above.

MongoDB 6+ requires use of the AVX instruction set, which is available on select Intel and AMD processors.
If your CPU doesn't have the AVX instruction set, MongoDB 6+ will not run.
To check whether your CPU has the instruction set, run:
#lscpu | grep -i avx"

To prepare your environment for FileCloud, make sure that you have the required components.

Supported operating systems and installed software

OS Software Requirements

FileCloud Server supports FIPS licenses.
Enterprises who are subject to FIPS regulations must install and run a FIPS-enabled operating system.
When using a FIPS-enabled license, FileCloud Admins will see in the Admin Portal:

- Running in FIPS mode is prominently displayed
- Storage encryption option is always shown

FileCloud - supported operating systems

To run FileCloud, use one of the following supported operating systems:

- Windows Server 2019, Windows Server 2022, Windows Server 2025
- Ubuntu 22.04, Ubuntu Pro 22.04

- RHEL 9.0

For additional options to install on AWS/Azure, see the Installation page.

> Additionally, FileCloud can be run inside a Virtual Machine that can be hosted in almost any operating system including macOS.

Client and mobile apps - supported operating systems

Client App	Minimum Supported Version	Latest Supported version	Notes
FileCloud Desktop for macOS	Sequoia 15.7 (Ventura 13.3.1 is not officially supported, but may function as expected.)	Tahoe 26.01	As a policy, we support the latest point releases of the two latest major macOS operating system releases from Apple.
FileCloud Desktop for Windows	Windows 10 Windows Server 2019	Windows 11 Windows Server 2022	Not supported: Windows Server 2016
FileCloud Sync	Windows 10 Ventura 13.6.3	Windows 11 Sonoma 14.2.1	
FileCloud Drive	Windows 10 Ventura 13.6.3	Windows 11 Sonoma 14.2.1	
FileCloud Outlook Add-in	Windows 10 Monterey Outlook 16		The Outlook Add-in is only supported on the Windows operating system.
FileCloud for Office	Office 2019	Office 365 / Office 2021	
FileCloud ServerSync	Windows 10	Windows 11	

FileCloud Secure Viewer	Windows 10	Windows 11	
FileCloud Desktop Edit	Windows 10 Ventura 13.6.3	Sonoma 14.2.1 Windows 11	
FileCloud for iPhone	iOS 16	Latest version of iOS	
FileCloud for iPad	iOS 16	Latest version of iOS	
FileCloud for Android	Android 8	Latest version of Android	

Required hardware

Hardware Requirements

Small Installations (~ 100 users)

See FileCloud Sizing Guide.

Larger Installations

To support FileCloud, you might need to setup more powerful configurations to include the following:

- Use redundant object storage systems like Amazon S3 or compatible systems.
- Use an HA configuration with a database cluster when running a system with many users.

Necessary network configurations

Network Requirements

If you are using a load balancer, the HTTP response timeout must be set to 5 minutes or more.

Ports

The following are the ports necessary for the operation for FileCloud.

Port No	Purpose	Internal/ External	Remarks
80	HTTP Traffic	External	• Port used for http traffic from all clients such as browser, FileCloud sync, FileCloud drive etc., • This port should be opened to WAN if clients need to access FileCloud over internet. • **For Production, Plain HTTP is NOT RECOMMENDED. ONLY SSL should be used.**
443	HTTPS Traffic	External	• Port used for https traffic from all clients such as browser, FileCloud sync, FileCloud drive etc., • This port should be opened to WAN if clients need to access FileCloud over internet.
389	LDAP	Internal	• Optional port needed if FileCloud users need to be authenticated against Active Directory or LDAP server • This port does not need to be opened to WAN, as only FileCloud server will be using it within LAN.
636	LDAP SSL	Internal	• Optional port needed if FileCloud users need to be authenticated against a secure Active Directory or LDAP server • This port need not be opened to WAN, as only FileCloud server will be using it within LAN.

If MongoDB is set to run on a different computer from the Webserver , then Port 27017 on the computer running MongoDB must be accessible from the Webserver computer in order for it to connect.,

Configuration

Component	Configuration
IP Address	You need a public IP for the server running FileCloud. Typically, this means you need a static IP for the server as dynamic IPs provided by most ISPs keep changing.
Network Connection	You need a good-quality network connection to the FileCloud Server. Minimum should be 5 Mbps upload and download for good experience. The faster the connection the better the experience.

Component	Configuration
Domain Name	You will typically need a top level domain name. For example: cloud.mycompany.com or mycompanycloud.com. You can purchase a domain name from any domain registrar and then point the DNS for that domain name to the public IP of the server that is running FileCloud.
SSL Certificate	You will also need a valid SSL certificate for your domain name to set up and use **https** with your FileCloud server for best security. Beginning with version 23.242, FileCloud requires SSL certificate keys to be 2048 bits in length, which follows the current security recommendation.

Open Source Software Libraries Used in FileCloud

Open Source Software (OSS) libraries used in FileCloud:

OSS library	License
`heic-to`	https://www.gnu.org/licenses/lgpl-3.0.html#license-text

Logging In to the Admin Portal

Log in using your admin account to perform administrative tasks.

Accessing the Admin Portal

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

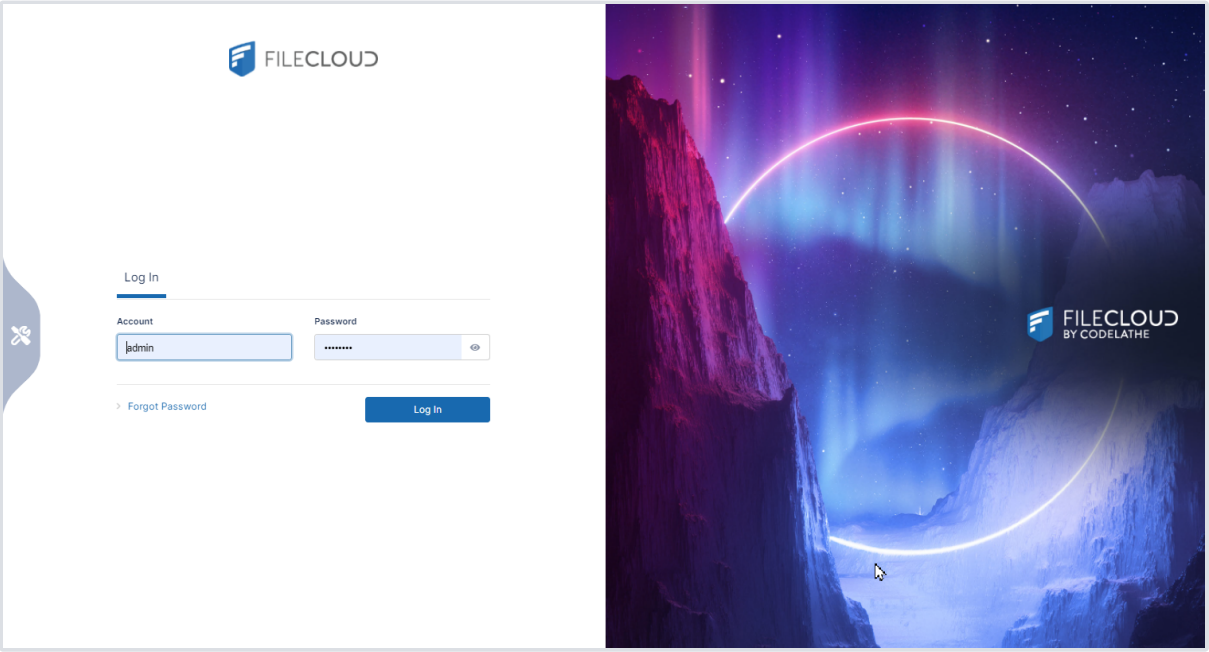
Admin URLs
http://<your filecloud address or IP>/admin (or)
https://<your filecloud address or IP>/admin
This redirects to
http://<your filecloud address or IP>/ui/admin/index.html (or)
https://<your filecloud address or IP>/ui/admin/index.html

Logging in with Default Credentials

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

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

If you are a promoted admin (an end user with admin privileges), you may be required to accept terms of service the first time you log in to the admin portal. Once you accept the terms of service, the login screen opens.
If you are the main admin of the system (your username is Admin) you can log in directly the first time.



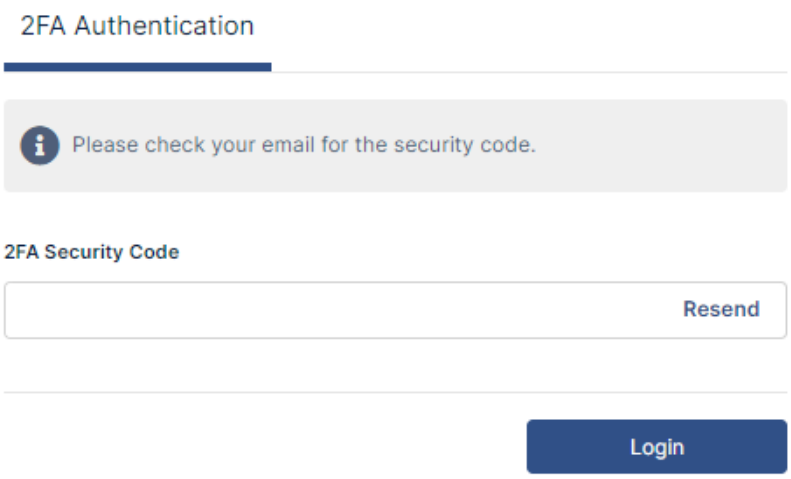
Log in using 2FA

- 2FA validation codes remain valid for 5 minutes by default. After 5 minutes, you must click **Resend** to get a new code.
- If you are a promoted admin, the login method configured for your user portal login is used for your admin portal login. However, if 2FA is set up for your admin portal login, your admin may require you to use that method for logging in to the admin portal.

Two-factor authentication via email code delivery

If two-factor authentication is configured to use your email address, then the 2FA security code is sent to the email address associated with your FileCloud account.

1. Log in to FileCloud using your username and password.
   The following screen appears:



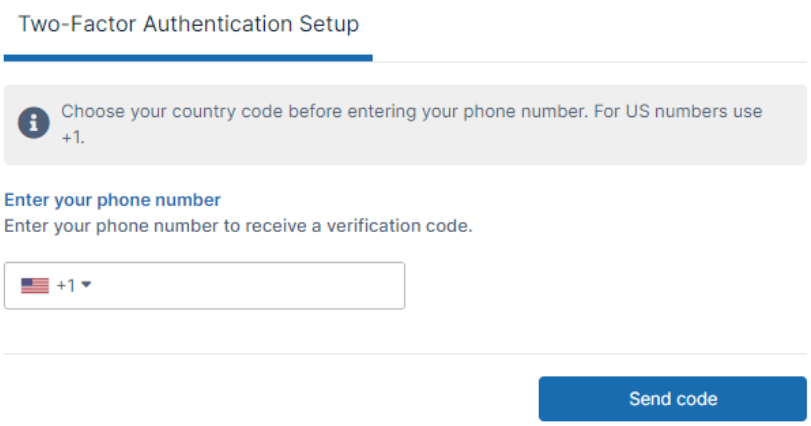
2. Check your email for the message with the code, and enter it into **2FA Security Code**.
3. Click **Login**.
   You are logged in to FileCloud.

Two-factor authentication via SMS code delivery

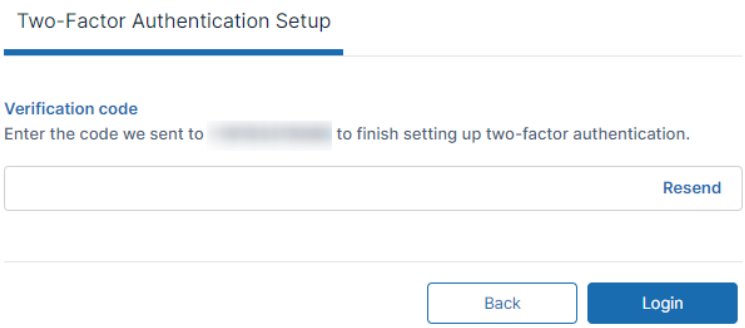
If two-factor authentication is set up to use SMS, then you will receive a code via the phone number associated with the account.

The first time you log in using SMS

1. Log in to FileCloud using your username and password.
   The following screen appears:



2. Enter your phone number and click **Send code**.
   The following screen appears:

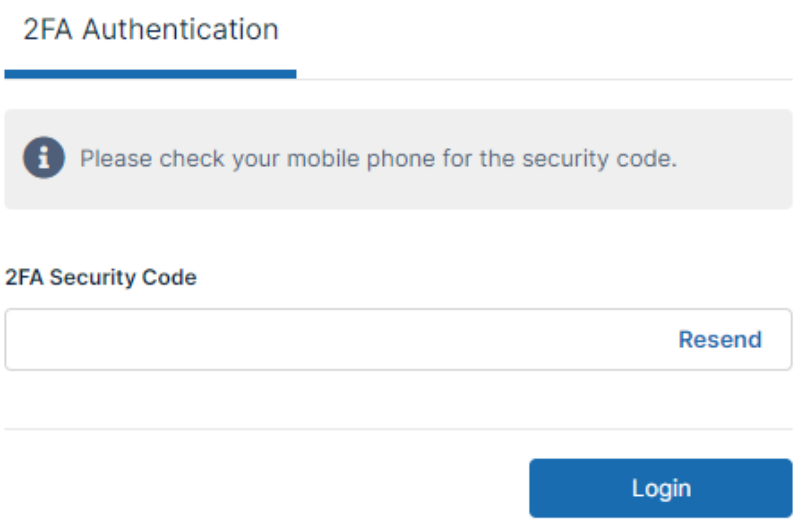


3. Check your phone for the code, and enter it into **Verification code**.
4. Click **Login**.
   You are logged in to FileCloud.

After the initial time you log in using SMS

FileCloud has saved your phone number the first time you logged in using SMS, so you do not have to enter it again.

1. Log in to FileCloud using your username and password.
   The following screen appears:



2. Check your phone for the code, and enter it into **2FA Security Code.**

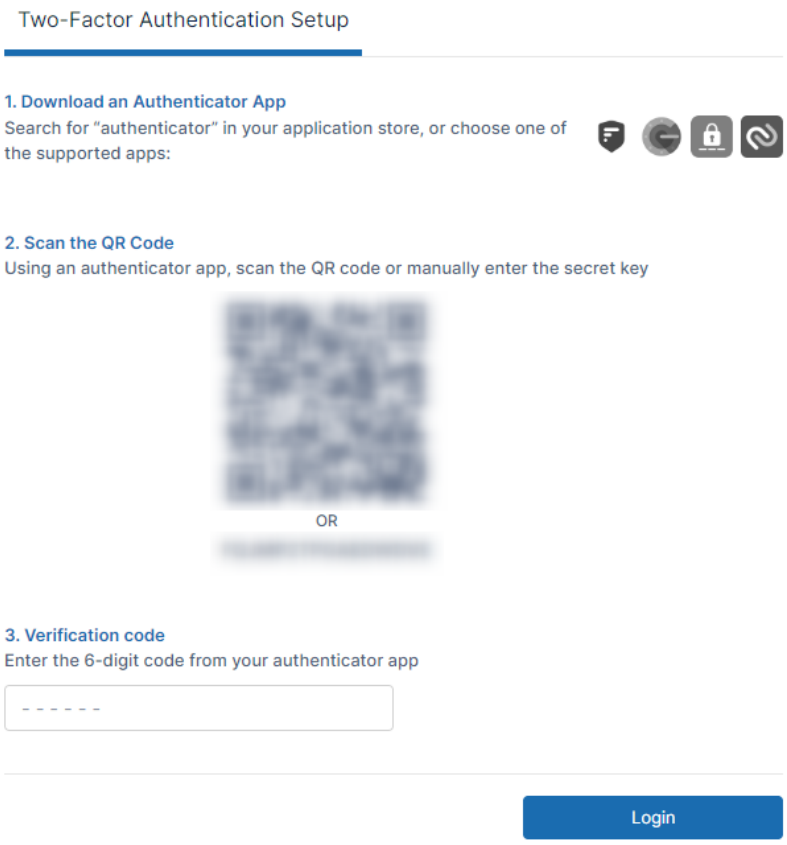
3. Click **Login**.
   You are logged in to FileCloud.

Two Factor Authentication with TOTP

If your admin sets up 2FA with TOTP, the dialog box prompting you for your security code will direct you to check your authenticator app for the code.

The first time you log in using TOTP

1. Log in to FileCloud using your FileCloud username and password.
   The following screen appears:

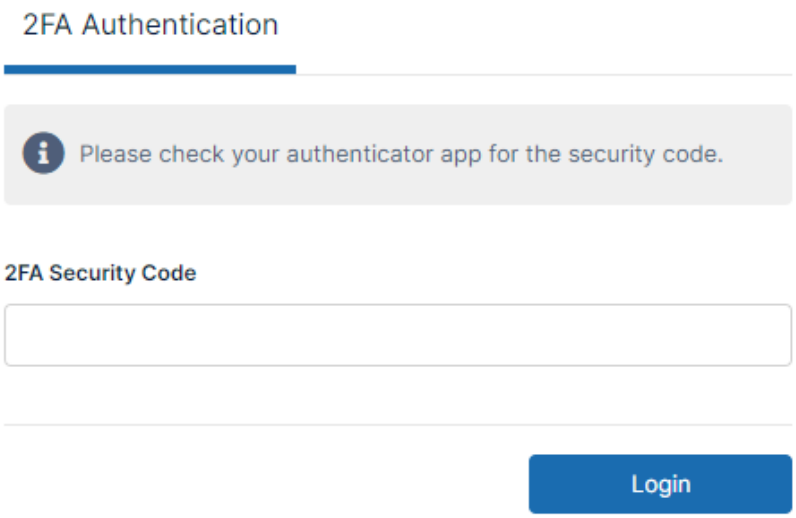


2. If an authenticator app is not yet set up, install it on your mobile device; you may click one of the download icons to install it.
3. Either scan the QR code or type the text code into the authenticator app.
   The authenticator app creates the account and lists it with a code.
4. Enter the code listed on the authenticator app for your account into **Verification code**, and click **Login**.
   You are logged in to FileCloud.

After your first login with TOTP

The authenticator app has saved your account the first time you logged in using TOTP, so you do not have to enter it again.

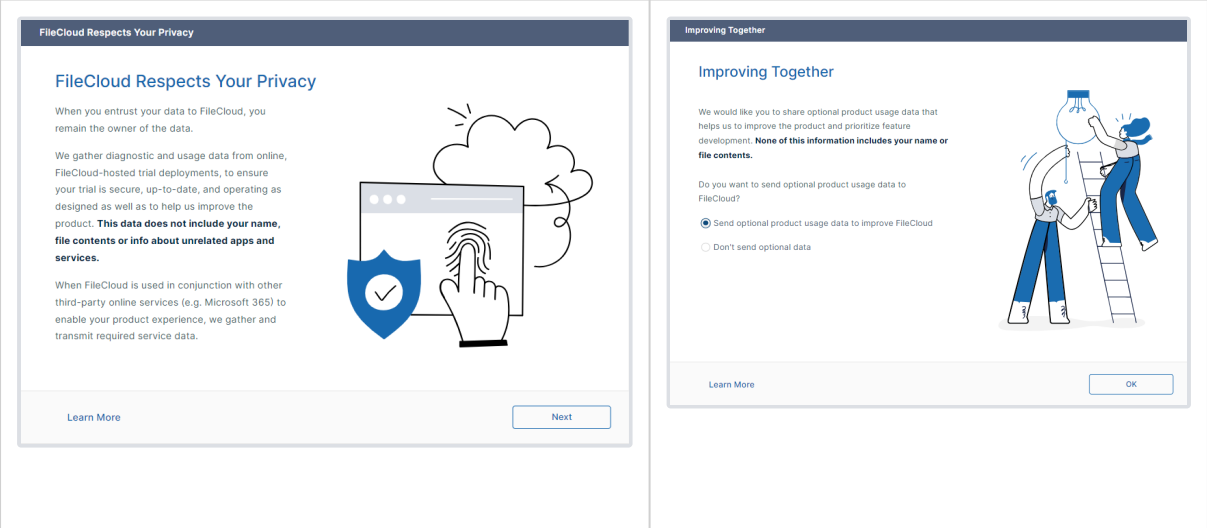
1. Log in to FileCloud using your FileCloud username and password.
   The following screen appears:



2. Enter the code listed on the authenticator app for your account into **2FA Security Code**, and click **Login**.
   You are logged in to FileCloud.

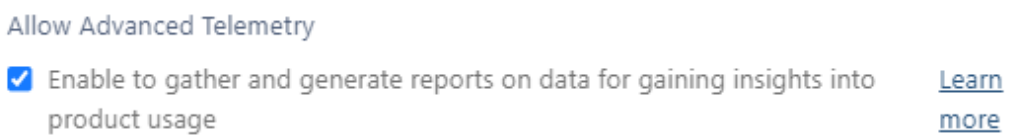
Collection of usage data

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



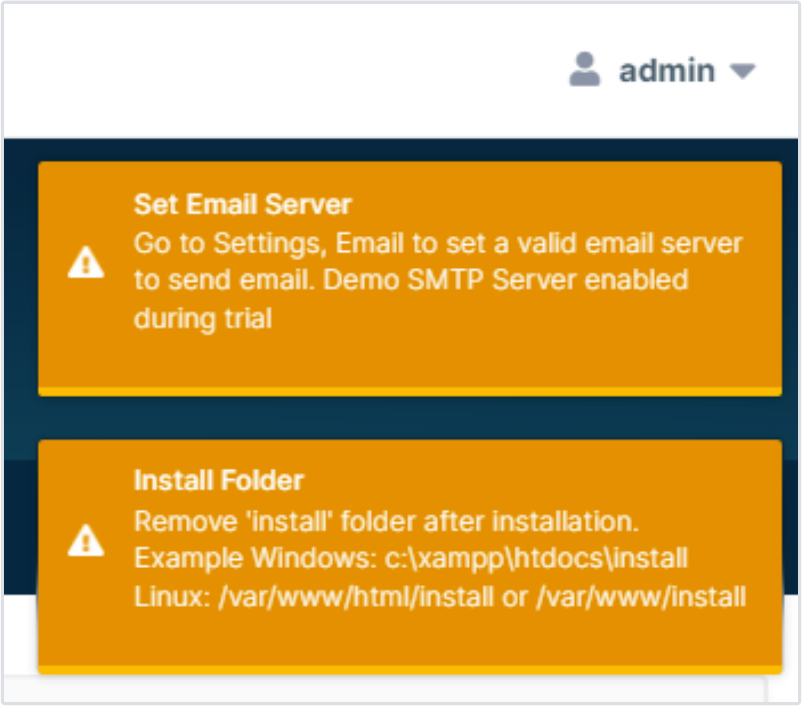
To allow sending of optional product usage data to FileCloud, leave **Send optional product usage data to improve FileCloud** selected, and click **OK**.
To prevent sending of optional product usage data to FileCloud, select **Don't send optional data**, and click **OK**.

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



Viewing and Clearing Checklist Notifications

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



To avoid seeing the alerts again, correct the settings. To clear an alert for this session, click on it. To clear all alerts for this session, click Escape.

Customizing the Login Page

To customize the image on the admin login screen, see Themes, Labels, and Logos.