

# FileCloud Security Best Practices & FAQs

FileCloud is used by global organizations and enterprises across industries, including finance, healthcare, government, education, and manufacturing. Thousands of users rely on FileCloud for secure file sharing and collaboration, data governance, and regulatory compliance.

This white paper outlines FileCloud's Security Best Practices, describing tools and settings that clients can leverage to secure data across multiple IT infrastructure layers. The white paper also addresses frequently asked questions related to FileCloud's cybersecurity posture and mechanisms.

## Table of Contents

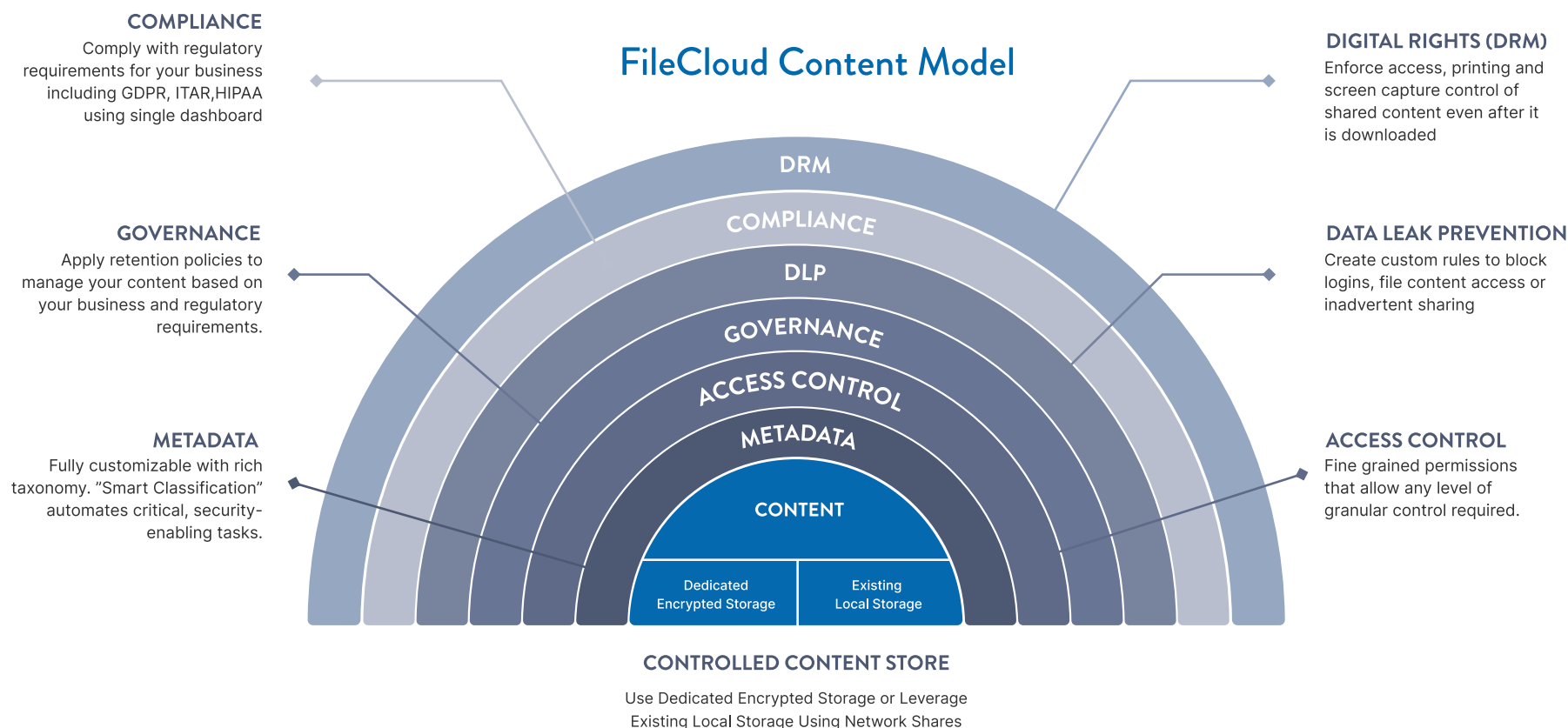
- [FileCloud's Security Best Practices](#) →
- [FAQ 1: How can the FileCloud environment be secured?](#) →
- [FAQ 2: How do I manage user access and authentication?](#) →
- [FAQ 3: How secure is file sharing in FileCloud?](#) →
- [FAQ 4: How does FileCloud support Data Leak Prevention \(DLP\)?](#) →
- [FAQ 5: How can I secure my network and still provide external access?](#) →
- [FAQ 6: How do I secure devices connecting to my FileCloud instance?](#) →
- [FAQ 7: How do I maintain data integrity and availability?](#) →
- [FAQ 8: What if I need to comply with cybersecurity regulations \(e.g., GDPR\)?](#) →



# FileCloud Security Best Practices

When it comes to building (and constantly improving) an enterprise-grade EFSS solution that clients love to use, FileCloud considers security to be a core element influencing all development.

FileCloud has cultivated a product that delivers robust hyper-security integrated alongside easy-to-use file management tools and features. After all, the most effective security solution is the one people actually use.



There are many ways of deploying and configuring FileCloud to meet unique use cases and security requirements. However, FileCloud has identified a set of security best practices that, when implemented, significantly strengthen an organization's content management infrastructure.

### FileCloud Security Best Practices

- Encryption (at rest and in transit)
- Active Directory (AD) Integration
- Antivirus Scanning
- SIEM Integration
- Remote Device Management
- Ransomware protection / Heuristic Scanning Engine
- Multifactor Authentication (MFA)
- Password & Access Policies
- Role-based Access Controls (RBAC)
- Granular User & File Sharing Permissions
- Smart Classification
- Zero Trust File Sharing®
- Smart DLP
- Unlimited External Accounts
- Digital Rights Management (DRM)
- Retention Policies



**This white paper delves deeper into each of these best practices through a series of Frequently Asked Questions.**

These FAQs provide an organized structure to understand how FileCloud's best practices can be implemented as part of a cohesive and multi-layered security strategy.





# FAQ 1

## How can the FileCloud environment be secured?

FileCloud supports a multi-layered cybersecurity strategy, with mechanisms and settings to protect data, users, and the environment itself.

- Encryption options  
(at rest and in transit)
- AD/LDAP integration
- Antivirus Scanning
- SIEM Integration



## FileCloud supports several options to encrypt data, both at rest and in transit

- FIPS 140-2 cryptographic modules (NIST-validated, enforces encryption for data at rest and in transit)
- Bring Your Own Key (BYOK)/Server-side Encryption (Symmetric or Asymmetric Key)
- 128- or 256-bit AES (encryption for data at rest)
- SSL/TLS protocols (encryption for data in transit)

Manage S3 Encryption

Encryption Status

Partial Encryption Active

Encryption is active, but existing files are not encrypted yet.

Status Details

Stored files not encrypted, new files will be encrypted

Note

1. New incoming files will be encrypted.
2. Existing stored files are not encrypted yet.
3. Click on 'Disable Encryption' to remove storage encryption.
2. Click on 'Encryption All' to encrypt all existing stored files.



# Encryption Options in FileCloud

## Storage Level Encryption

FileCloud supports storage-level encryption! Administrators may supply an optional master password and start the initialization process. Without a master password, the encryption module cannot encrypt/decrypt files in FileCloud storage, which adds additional security to the storage system.

## Technical Details

An asymmetric key pair (private/public) of 4096 bits RSA SHA-512 digest known as "Master" key is generated with the optional master password. A symmetric key of AES 128 bits known as "Plain File" key is generated. The file key created is encrypted using the Master Private key resulting in an "Encrypted File" key. All the existing unencrypted files (if they exist) in FileCloud storage will be encrypted before the system will be ready for use.

## File Encryption

File encryption is done using the "Plain File" key automatically. Since this encryption process is a symmetric operation, the time overhead added for this encryption is insignificant.

## Managed Disk Storage

Default cloud storage is where the user files are stored on a disk file system, which can be accessed directly by FileCloud. The managed storage provides FileCloud complete control over the management of user content. Data can be on file systems, a local hard disk, and SAN or NAS disks.



## FileCloud Online Encryption At-Rest

Manage S3 Encryption

Encryption Status

Encryption is disabled

Encryption Type

Amazon S3-Managed Key Encryption

Amazon KMS-Managed Key Encryption

☒ Customer Supplied Key Encryption

1. Files are currently not encrypted.

Disable encryption

Close

## FileCloud Server Encryption At-Rest

Manage Storage Encryption

Encryption Status

Partial Encryption Active

Encryption is active, but existing files are not encrypted yet.

Status Details

Stored files not encrypted, new files will be encrypted

Note

1. New incoming files will be encrypted.

2. Existing stored files are not encrypted yet.

3. Click on 'Disable Encryption' to remove storage encryption.

2. Click on 'Encryption All' to encrypt all existing stored files.

Disable encryption

Close

## FileCloud Online & FileCloud Server Encryption At-Rest:

FileCloud supports storage-level encryption and provides an easily configurable tool to encrypt files at rest. FileCloud uses AES (Advanced Encryption Standard), one of the most robust encryption standards in the world.

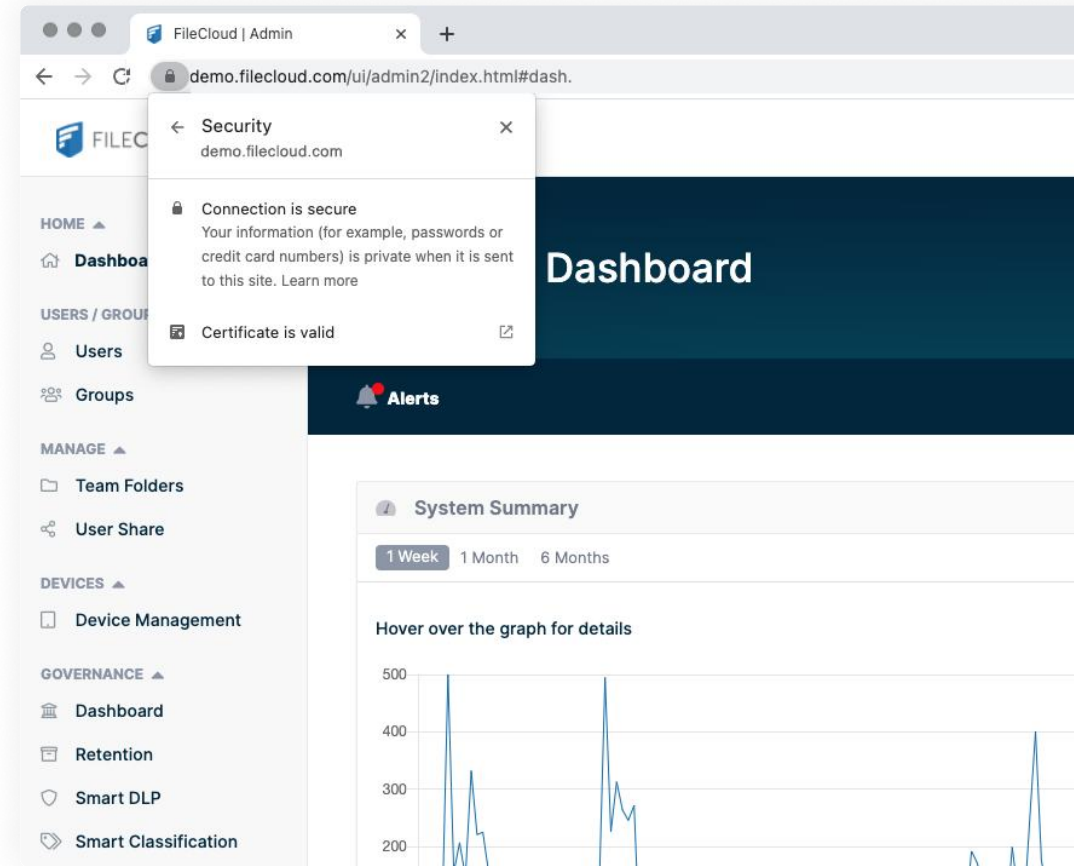
AES encryption is approved by the National Institute of Standards and Technology for federal use. Encryption options may vary depending on the FileCloud service being used (Online or Server) and storage preference.



## Encryption In-Transit:

FileCloud administrators can turn on SSL to enable secure sharing. Simply obtain a new SSL certificate, configure the underlying Apache webserver to use the certificate, and enable HTTPS protocol.

We highly recommend disabling HTTP and/or automatically redirecting all HTTP requests to HTTPS. In-transit encryption, which applies to API calls, web browser portal access, mobile clients, and desktop clients.



## Authentication Settings

Authentication Type

LDAP

Specify the Authentication Type

DEFAULT

Active Directory

LDAP

### LDAP Settings

Check LDAP Test

LDAP Test

LDAP Host\*

ldaps://abc.company.com

Specify the LDAP Host Name

LDAP Port\*

389

Specify the LDAP Port Number

LDAP Account Name\*

username

Specify a valid account to use to query LDAP server

LDAP Account Password\*

.....

Specify account password to use to query LDAP server

LDAP User DN Template

cn=username,ou=Company-Users,dc=company,dc=com

Specify the LDAP User DN Template

LDAP Search DN

ou=Company-Users,dc=company,dc=com

Specify the LDAP Search DN

LDAP User Filter Template

## Active Directory (AD)/LDAP Integration

FileCloud supports integration with enterprise identity management systems such as Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).

Therefore, large organizations who are already using AD can choose to integrate their FileCloud user accounts directly with their existing deployment. This allows companies to quickly adopt cloud functionality without decentralizing user management.

Active Directory integration in FileCloud is a great example of how external identity providers can support secure file sharing and collaboration. As users are created and deleted from Active Directory, they can be automatically granted or denied access to FileCloud. The full range of password and lockout policies set in Active Directory are enforced across all FileCloud access points.

Organizations can also connect to AD over Secure Sockets Layer (SSL). FileCloud supports single sign-on (SSO) through NT LAN Manager (NTLM) as well as Security Assertion Markup Language (SAML) SSO. Additionally, FileCloud supports code-based device authentication for desktop clients and mobile apps.

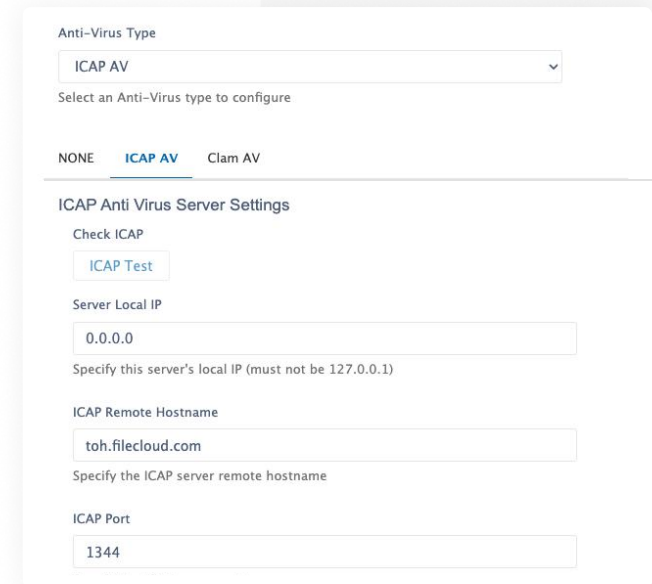


## Antivirus Scanning

FileCloud supports scanning of uploaded files using ClamAV (an open source antivirus software). Uploaded files are scanned automatically, and any malicious files are removed.

You can configure FileCloud to scan uploaded files in the following ways:

- Use [ClamAV](#), an opensource antivirus software that is included with FileCloud.
- Use [ICAP](#) to integrate your own choice of antivirus scanning software with FileCloud.



Anti-Virus Type

ICAP AV

Select an Anti-Virus type to configure

NONE **ICAP AV** Clam AV

ICAP Anti Virus Server Settings

Check ICAP

ICAP Test

Server Local IP

0.0.0.0

Specify this server's local IP (must not be 127.0.0.1)

ICAP Remote Hostname

toh.filecloud.com

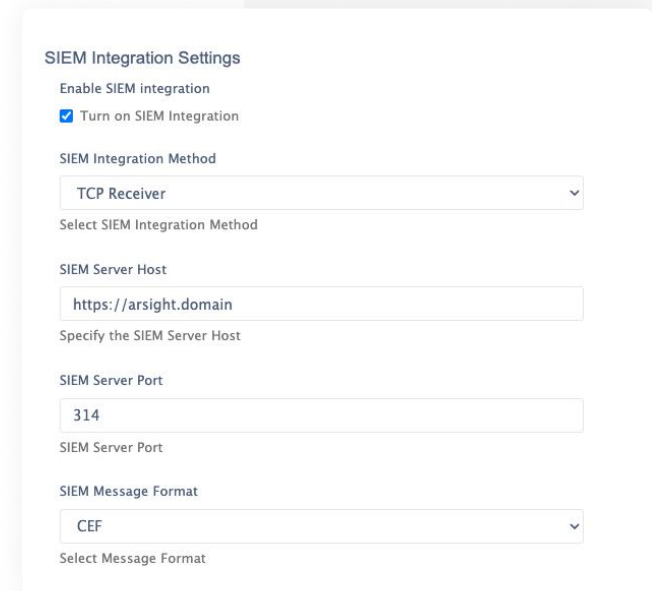
Specify the ICAP server remote hostname

ICAP Port

1344

## SIEM Integration

Since version 19.2, FileCloud has allowed system administrators to [integrate FileCloud's system alerts and auditing with external SIEM systems](#), enabling them to monitor all alerts and potential security issues in one place.



SIEM Integration Settings

Enable SIEM integration

☒ Turn on SIEM Integration

SIEM Integration Method

TCP Receiver

Select SIEM Integration Method

SIEM Server Host

https://arsight.domain

Specify the SIEM Server Host

SIEM Server Port

314

SIEM Message Format

CEF

Select Message Format





# FAQ 2

## How do I manage user access and authentication?

FileCloud admins can manage user access and authentication using a variety of mechanisms. Through the configuration of FileCloud with existing IT infrastructure to the establishment of specific user and folder policies, FileCloud provides all the necessary tools to support user identity authentication and access authorization.

- Two-factor Authentication (2FA)
- Password management
- Automatic Logoff
- ReCAPTCHA
- Role Based Access Controls (RBAC)



## Multifactor Authentication (MFA) or Two-factor Authentication (2FA)

2FA adds an extra layer of protection to FileCloud user logins by combining the use of “something you know” (your login credentials and password) and “something you possess” (One Time Passcode) to access FileCloud.

- Adds an extra layer of protection to your FileCloud account.
- Once enabled, FileCloud will require a passcode in addition to your password whenever you log into FileCloud or link a new device.

**In most infrastructures, the login screen is the most exposed part of an application.**

This is why FileCloud enables strict user authentication and permission enforcement at every access point, ensuring that only users with the right credentials can access data.

Most security threats today are a result of compromised user credentials. With FileCloud's two-factor authentication, users can require an extra 2FA code as part of the user authentication process. The additional login step requires users to verify their identity using a one-time code sent via email, creating a double check for every authentication.

Even without knowing the login information, unauthorized users can still find ways to access company data by piggybacking through the user's computer while logged in.

This is true for any web application, whether accessing a bank account website or personal email. FileCloud is fully aware of these attempts and takes multiple steps to prevent unauthorized access after a user has logged in.

First, FileCloud prevents cross-site request forgery and cross-site scripting, meaning that if another website attempts to access FileCloud through another computer, FileCloud immediately recognizes the unauthorized request by making only one 2FA code available at any point in time.



## Enable Multifactor Authentication

FileCloud admins can enforce a global 2FA method through Admin Settings or use policies to set methods for different users and groups.

**Policy Settings - TEAM FOLDER POLICY**

**Note:** Some policy settings will not be applicable for Guest and External users.

General

**2FA**

User Policy

Client Application Policy

Device Configuration

Notifications

### 2 Factor Authentication

Enable Two Factor Authentication

YES

Enable to require a one time passcode to be entered along with the account password

Two Factor Authentication Mechanism

✓ Email

TOTP (Authenticator App)

DUO Security

SMS Security

Save

Reset All

Close



## Password Management

FileCloud password policy management allows admins to set minimum password length for user accounts and account lockout after failed logins. Account lockout prevents brute force password attacks by immediately locking out the access point after multiple failed login attempts.

Once the account is locked, both the user and admins are notified through email notification. These best practice access controls allow administrators to enforce stringent business policies and add an extra layer of password protection against unwanted intrusion.

In FileCloud Admin UI / Settings / Misc / [Passwords](#) we recommend you enable:

- Minimum password length (8).
- Enable strong Passwords.
- Disallow commonly used passwords.
- Set a max number for the incorrect attempts before account lockout.
- Set an account lockout length in minutes.
- Set a number of Previous Password that cannot be reused.

### Password Settings

#### Minimum Password Length

#### Minimum acceptable length of Password

#### Enable Strong Passwords

- ☐ Enabling this will require the password to contain at least one uppercase, lowercase, number and a special character in the password

#### Disallow Commonly Used Passwords

- ☐ Enabling this checkbox will prevent users from using commonly used passwords for their user accounts

#### Incorrect Attempts Before Account Lockout

Number of times wrong password can be entered before an account is locked out. Value 0 implies account will not be locked out.

#### Account Lockout Length In Minutes

Number of minutes account will be locked out. Value 0 implies account will not be locked out.

#### Disallow User Login With Password

Disallow Login with password on user accounts.

#### User Password Expires In Days

Number of days passwords are valid for user accounts. Value 0 implies passwords will not expire. Applicable only for user accounts.



Server Settings

Session Timeout (Minutes)

30

Specify user web login session timeout.  
Example: 15 = Default timeout of 15 minutes, 30 = 30 minutes, 60 = 1 hour.  
Note: Session will always expire when browser is closed unless advanced configuration is done.

Allow Sync Apps

☒ Enable to allow CloudSync Apps

Allow Old Devices To Login

☒ Enable to allow services without device management support to login

Allow Advanced Telemetry

☐ Enable to gather and generate reports on data for gaining insights into product usage [Learn more](#)

Log Level

DEV

Specify server log level

Default User Portal Language

english

Specify the user portal language to use

# Automatic Logoff

FileCloud's [User Session Expiration](#) feature ends a session after a predetermined time of inactivity. Administrators can configure this time based on their organization's policies. Once a user session exceeds the inactivity period, the session expires, and the user is required to log in again.



## Enable ReCAPTCHA login authentication

FileCloud supports [reCaptcha](#) v2. When you enable reCaptcha integration, reCaptcha is applied when users log in to FileCloud and when they access a password-protected file or folder share.



reCAPTCHA Integration Settings

Enable reCAPTCHA integration


☒ Select to enable Captcha

reCAPTCHA Site Key

..... 

Enter reCAPTCHA Site Key

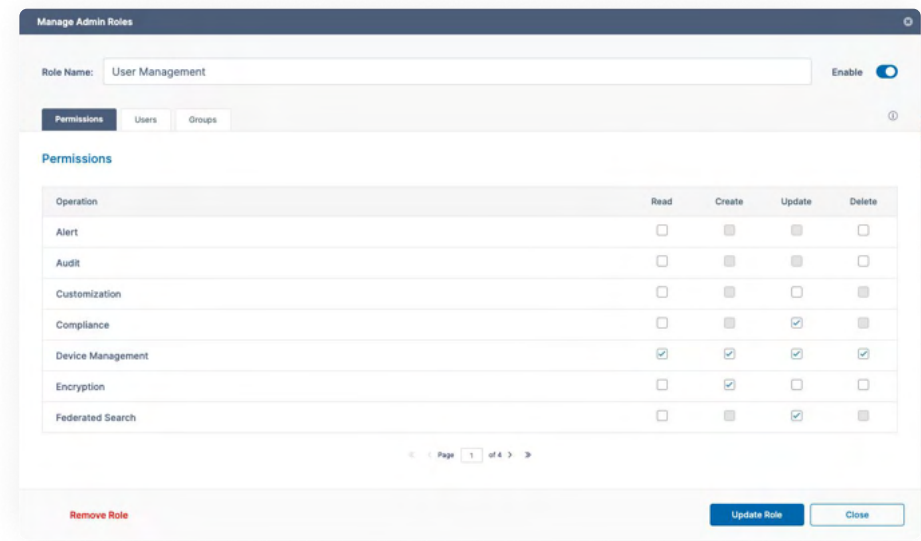
reCAPTCHA Secret

..... 

Enter reCAPTCHA Secret

## Role-based Access Controls (RBAC)

FileCloud supports role-based access controls or RBAC by enabling admins to promote users to the role of admin-user. These promoted roles are given access to different actions and information in the system. This provides an easy tool for admins to grant advanced permissions and access to types of users that need to manage other users (such as department heads, team leads, and other leadership roles).



Manage Admin Roles

Role Name:  Enable ☒

Permissions Users Groups

Permissions

Operation	Read	Create	Update	Delete
Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Audit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Encryption	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federated Search	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Page 1 of 6

Remove Role Update Role Close





## FAQ 3

### How secure is file sharing in FileCloud?

As a hyper-secure EFSS, file sharing is a major component of FileCloud. From simple, fast file sharing through public links to highly controlled and encrypted internal file shares with select internal groups, FileCloud offers a wide range of tools and settings to ensure content can be shared exactly the way it's needed, without exposing or compromising the data.

- Granular Permissions
- Share Access Limits
- Zero Trust File Sharing®





## Granular User, File, & Folder Permissions

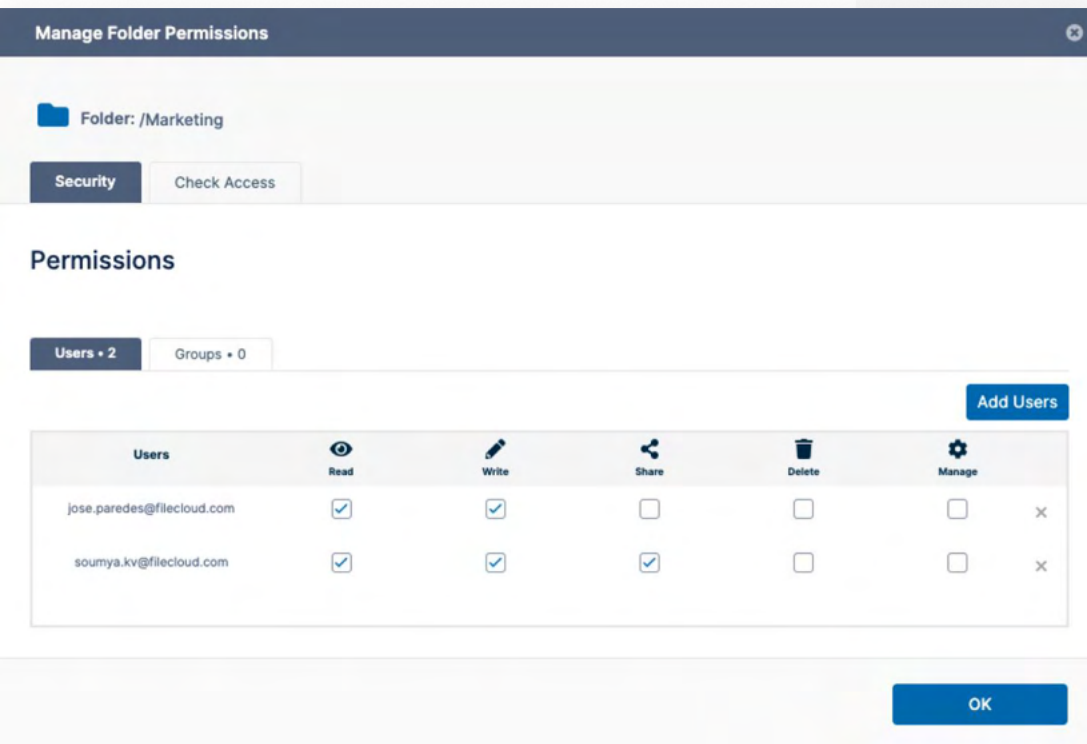
FileCloud provides advanced access controls for assigning and managing folder permissions. These access controls are critical to the implementation of data structure and hierarchy.

Admins have the ability to set specific permissions for users and groups, as well as Team Folders and subfolders. These granular permissions ensure that people have access only to the information they need.

Access permissions are generally enforced uniformly regardless of location and access method (web browser, FileCloud drive, WebDAV, FileCloud sync, mobile/tablet app).

## Share Access Limits

Users can share files with a set expiration date. Once the date is reached, the recipient will no longer have access to the file or folder. Users can also restrict the number of downloads to ensure content has a limited distribution potential.

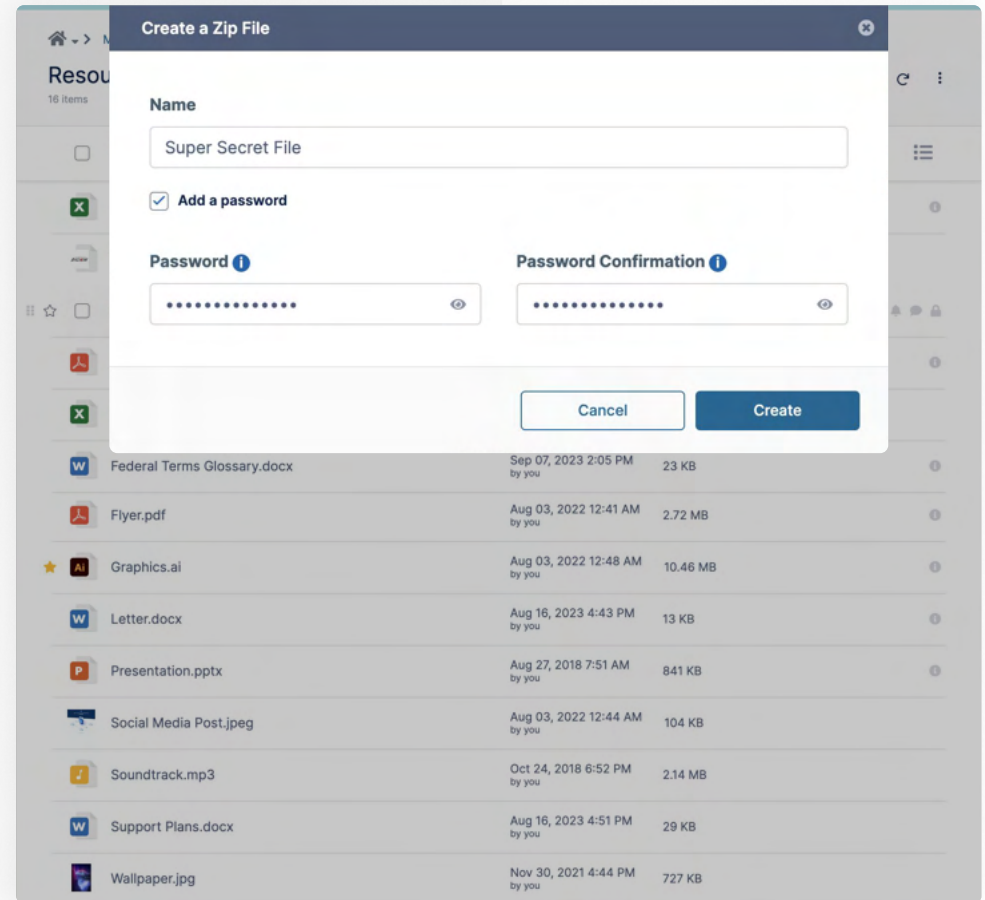


## Zero Trust File Sharing®

Users can share files and folders with Zero Trust protection in their FileCloud Managed (local) storage.

By creating and encrypting Zip files in FileCloud, users can create a shareable Zero Trust container to relay and collaborate on sensitive information with authorized recipients beyond the organization's network.

Zero Trust files can be shared with read-only (preview, download) or read-write (preview, download, add, delete) permissions.



## FAQ 4

### How does FileCloud support Data Leak Prevention (DLP)?

FileCloud offers unique capabilities to help monitor data movement as well as prevent and remediate leaks, ensuring that enterprise data is protected across all connected devices.

This includes access controls and granular file sharing permissions, which ensure that only authorized users with the appropriate permissions can interact with protected content.

Admins can also create global policies to restrict certain types of sharing or user activities, as required. For more fine-tuned control, admins can leverage DLP rules to monitor and guard sensitive or confidential data based on a variety of criteria, including metadata tags, file type, and method of access.

- DLP rules
- Smart DLP



## Control File Access with DLP Rules

Admins can create DLP rules through the Governance tab in FileCloud that controls not only how (and by whom) files can be accessed. DLP rules can be set up to limit user login, file access and sharing, and download operations across the platform.

For example, an admin can set a rule to:

- Limit access to files based on the user's IP address.
- Restrict login, share, and download operations based on the user type.
- Prevent external sharing of files to certain email domains or countries

Rule Update

Rule Name ⓘ

Block Access

Affected User Actions ⓘ

DOWNLOAD

Rule Expression ⓘ

Rule Expression Builder

Rule Expression Text Editor

DLP Action ⓘ

DENY

DLP Mode ⓘ

ENFORCE

Rule Notification (optional) ⓘ

The download is not Authorize from your location.

[Rule Creation Help](#)

Cancel

Create



























## Smart DLP

**Data leak prevention (DLP)** is a FileCloud feature that enables administrators to closely control the degree to which users can access, edit, download, and transfer their organization's files and folders. While DLP can be useful for many different kinds of data, it can be especially critical for the secure handling of Personal Identification Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI).

DLP also offers greater security to organizations that are required to operate in compliance with HIPAA or GDPR.

Smart DLP

Add DLP Rule

Rule Name	WHEN (Affected User Action)	IF (Rule Expression)	THEN (DLP Action)	MODE	Recent Violations	Active	Actions
Client PII	SHARE	<code>(_metadata.exists('cce.pii'))</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Shares of files with ePHI	SHARE	<code>(_metadata.existsWithValue('content.category','ePHI'))</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Download	DOWNLOAD	<code>_file.pathStartsWith('/master/DLP/DLP Download')</code>	DENY	ENFORCE	0	<input type="checkbox"/>	  
Deny Login based on Group	LOGIN	<code>!_user.inGroup('fired')</code>	ALLOW	ENFORCE	0	<input checked="" type="checkbox"/>	  
Prevent Sharing with outside email domain	SHARE	<code>_share.hasUsersFromDomain('gmail.com')</code>	DENY	ENFORCE	0	<input type="checkbox"/>	  
Deny Downloads on HR folder	DOWNLOAD	<code>_file.pathStartsWith('/master/HR')</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Download from network shares	DOWNLOAD	<code>_file.pathStartsWith('/opt/partner_agreement')</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  
Deny Sharing of CC information	DOWNLOAD	<code>_metadata.existsWithValue('CreditCard.CreditCard','VISA')</code>	DENY	ENFORCE	0	<input checked="" type="checkbox"/>	  



## FAQ 5

### How can I secure my network and still provide external access?

FileCloud provides several mechanisms to protect the environment (and the data stored within the network), while also enabling secure external access.

Secure file sharing is one way of extending content in a controlled and protected manner. However, admins can also set specific policies or leverage advanced tools that support limited access for external parties.

- "Private Shares Only" policy
- Unlimited external accounts
- Automated external account creation
- Watermarking
- Digital Rights Management (DRM)



**Note:** Some policy settings will not be applicable for Guest and External users.

General

2FA

User Policy

Client Application Policy

Device Configuration

Notifications

Share mode

Allow All Shares

Set Share Mode

Default Share Expiry in Days

0

Number of days shares remain active. Value 0 implies the shares do not expire.

Default Max Number of Downloads Allowed

2

Number of downloads allowed. Value 0 implies that the maximum number of downloads is unlimited.

User Storage Quota

Units

14336

MB

Specify storage quota. 0 implies Unlimited Quota.

Enable Privacy Settings

NO

Enables/disables privacy settings

Store Deleted Files

YES

Move file to recycle bin on delete action

Automatically Delete Files from Recycle Bin After Set Number of Days

0

Number of days once deleted files will be cleared. Value of 0 indicates that deleted files will not be cleared automatically.

## Set a Global Share Mode to Private Only

This can be managed by [Policy groups](#).

**In your admin portal,**  
click on Settings, then Policies.  
In “all” your policy groups,  
change the “Share Mode”  
to “Allow Private Shares Only”

This will prevent users from creating public share links. Instead, sharing content will prompt the recipient to create an account.

With unlimited external accounts at no extra charge, organizations can securely share content in a controlled manner. (Admins can also automate this account creation process through a file sharing policy.)





## Automate Account Creation for External Sharing

Following up on the previous page recommendation (set global share mode to private), we recommend enabling users to *implicitly* [create external accounts](#) when sharing content privately.

### User Settings

#### Import Files From Folder On User Creation

Team

Check Path

Exact Email Search With Explicit Account Invite

Exact Email Search With Implicit Account Invite

Exact Name/Email Search

✓ Partial Name/Email Search

Ability for an user to search other user accounts for sharing

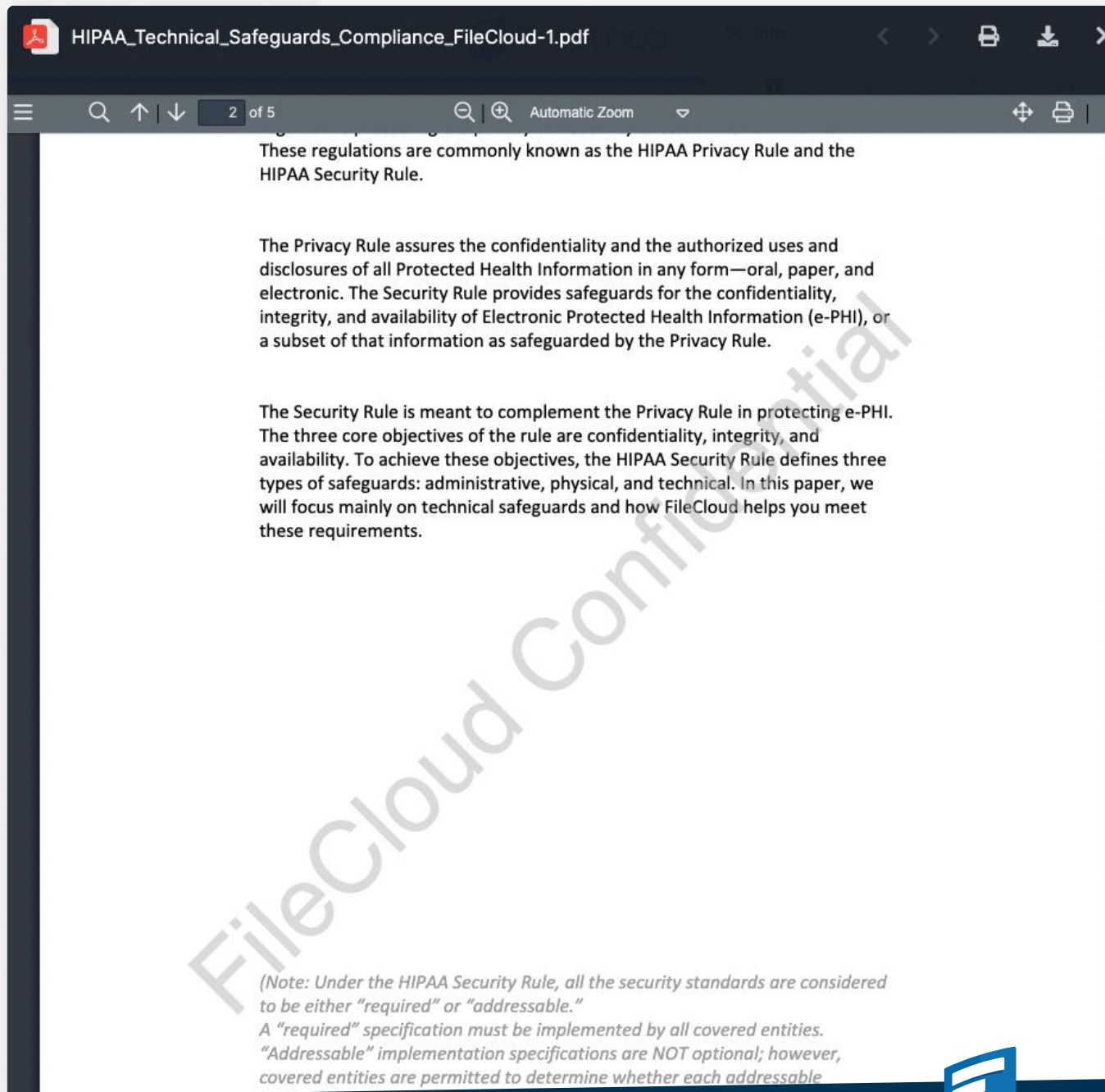
#### User Account Type Search Mode

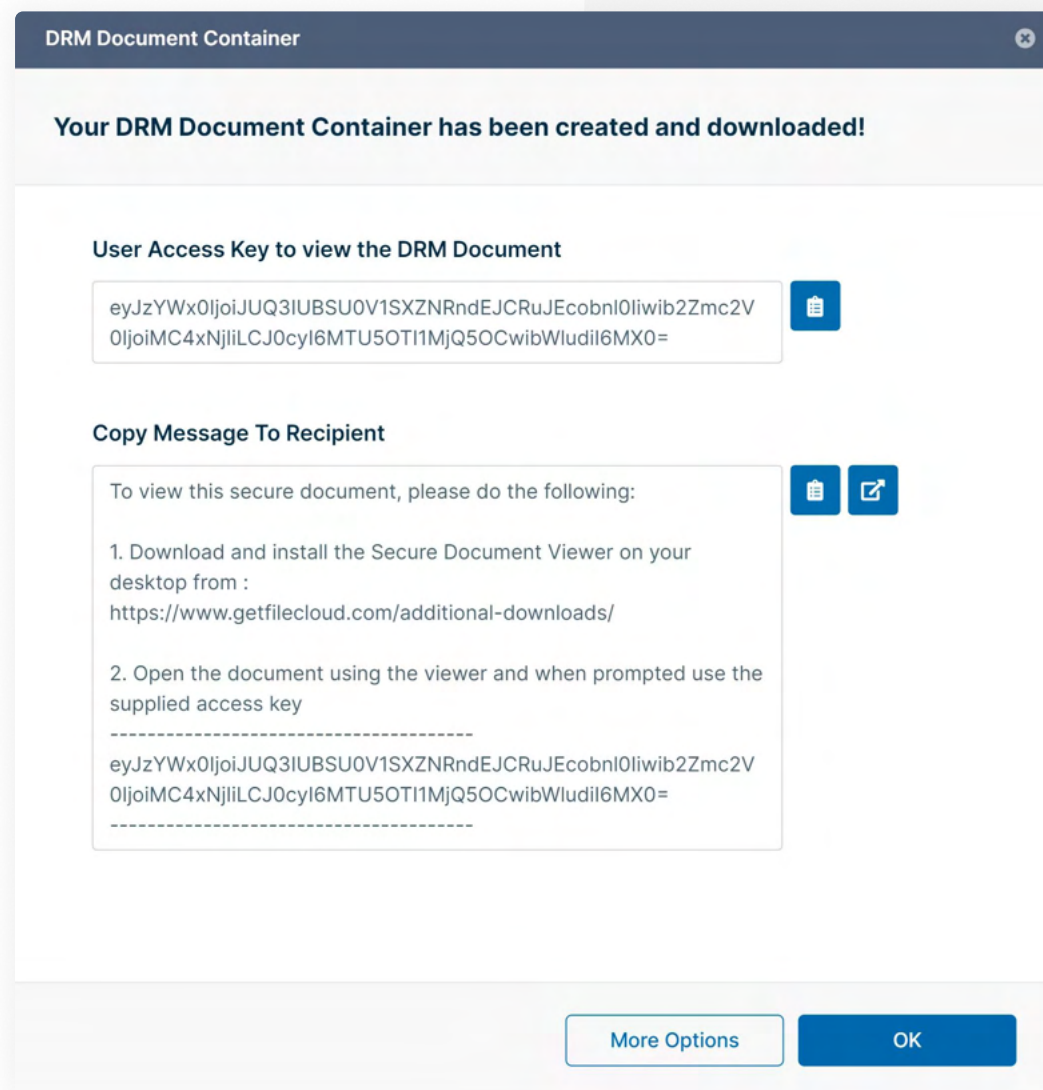
All Users



## Show Watermark on File Preview in Web Browser

Admins can create customizable watermarks that appear on all files through the file preview. These watermarks can show file metadata, such as time accessed or IP address, as well as custom tags (e.g., "Confidential").





## Digital Rights Management (DRM)

FileCloud offers two mechanisms to enforce Digital Rights Management (DRM) beyond the FileCloud environment.

The **Secure Web Viewer** is a lightweight, browser-based viewer that provides DRM protection. Recipients can view shared documents but they are never in possession of the file itself. FileCloud users can further protect records by enforcing a limited view; recipients must hover over sections to see content, reducing physical file exposure.

The **Secure Document Viewer** is a heavier-duty desktop client that enforces access limits and prevents screenshots, screensharing, and printing. Even after sharing files, users can update protections and permissions as needed. This desktop client must be downloaded by the sender and recipient.



## FAQ 6

### How do I secure devices connecting to my FileCloud instance?

FileCloud supports endpoint protection across several mechanisms. It starts with device and client applications, which serve to connect remote users (more specifically, their devices) to the FileCloud environment.

Users can leverage these applications as an access port to files and folders within their managed storage, Team Folders, or Shared Folders. Users can also sync and back up data from their endpoint device (desktop, laptop, tablet, or mobile device) to the FileCloud environment, in a comprehensive or selected manner.

However, these applications do not provide blank-check access to users. These connections can be closely monitored and managed by administrators with Centralized or Remote Device Management.

- Remote wipe
- Block devices & users
- Disable mobile or client connection
- Enforce application locks
- Disable features within mobile apps





## Centralized Management

Admins can view and manage all connected devices through a centralized device inventory dashboard. Admins can also enforce device and client application policies that restrict file access or behaviors



### Force mobile clients to enable FileCloud app pin lock.

If the pin lock is not enabled, the login will be rejected.



### Remote wipe

If a user loses a mobile device, the admin can remotely wipe the FileCloud data on that device, protecting confidential files.



### Block devices, clients

In case of any suspicious activity, admins can selectively block devices, clients (e.g. sync) or permanently remove users from accessing the system.



### Disable mobile or desktop client connections

Prevent login to FileCloud from mobile client apps (enforce login only via web browser); Disable sync so FileCloud Desktop or Drive applications open files on demand (no files stored at rest on user machines).



### Disable features such as download, print, edit, open with, or share in mobile client apps.

Admins can set a global policy to disable features in mobile apps, while supporting exceptions for specific users, as needed.





## FAQ 7

### How do I maintain data integrity and availability?

Security is not just about implementing secure boundaries and enforcing controls over access channels. A robust security strategy must also ensure that data under management can be identified, authenticated, and leveraged as needed. In the process, strategies must also protect data from corruption and misuse.

FileCloud achieves these security mechanisms through several features and functionalities.

- Ransomware protection
- Audit logs
- Data visibility
- Content classification
- Retention policies



## Ransomware Protection

FileCloud provides a heuristic engine that ensures data integrity is protected against ransomware attacks. This will check each file when they are created, edited or deleted.

Additional protection for normal files operations include:

- Preserving deleted files
- File versioning
- Antivirus integration

**Unlimited file versioning** provides another layer of ransomware protection. Any time a file is modified, FileCloud documents the change. Users and admins can view and restore file versions, particularly if important data is overwritten or compromised. Administrators can set file versioning limits to a specific number to manage storage, but the default is unlimited.



### Manage Workflows

#### Workflow

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action
New App Connection	If any new client app connects	Block the device for admin approval	September 11, 2024, 3:47 am	September 11, 2024, 3:47 pm
delete folder – copy path	If a folder is deleted	Copy the file(s) to some location	August 3, 2023, 12:54 am	May 7, 2023, 12:54 pm
delete notify users	If a file is deleted	Notify file actions to user(s)	August 2, 2023, 5:47 pm	May 6, 2023, 5:47 pm
disable user account	If a new user is created	Disable user account	August 2, 2023, 5:47 pm	March 1, 2023, 5:47 pm
Release locks	Perform an action periodically	Release locks	September 11, 2024, 3:47 am	July 23, 2024, 3:47 pm
If not modified	If file was not modified for specified days	Notify file actions to user(s)	May 1, 2023, 2:47 pm	May 1, 2023, 2:47 pm
List if not logged in for #days	If a user's last login is older than ..	Generate an email report	May 1, 2023, 2:47 pm	April 3, 2023, 2:47 pm
notify file download	If file downloaded is bigger than expected size	Notify file actions to user(s)	August 2, 2023, 5:47 pm	December 1, 2023, 5:47 pm
filecreatedtest	If a file is created	Run a report	September 9, 2021, 2:33 pm	September 9, 2021, 2:33 pm
9240ticket	If a file is created	Execute a command	May 1, 2023, 2:47 pm	October 1, 2023, 2:47 pm






# Audit Logs

All FileCloud activity is recorded in the [audit logs](#), which can be viewed and exported from the "Audit" tab in the admin portal. This feature is enabled by default and will keep all request records.

We recommend automating archival and removal of audit logs to support optimal system performance and maintenance of audit records.

 Audit Logs

Search Term

Filter Start Date

Filter End Date

Filter

Operation Filter : Common

User Agent : All

Show 10 Items

Manage

Refresh

User name	Message	IP	Agent	Created On
admin (demo)	admin (demo) getloggedinadminpermissions	187.183.44.151	Web browser	2024-Sep-11 10:07 AM
admin (demo)	admin (demo) getauthstatus	187.183.44.151	Web browser	2024-Sep-11 10:07 AM
admin (demo)	admin (demo) getloggedinadminpermissions	187.183.44.151	Web browser	2024-Sep-11 10:07 AM
admin (demo)	admin (demo) getadminlanguagelist	187.183.44.151	Web browser	2024-Sep-11 10:07 AM
admin (demo)	admin (demo) getauthstatus	187.183.44.151	Web browser	2024-Sep-11 10:07 AM
deepti	Retrieved RMC Commands for device [d317e22d-d456-40b8-b1a9-61b55f6e2267] of user deepti	171.76.81.243	Cloud Sync	2024-Sep-11 10:02 AM
ANONYMOUS	Retrieved announcement feed (rssfeed)	178.73.48.164	Web browser	2024-Sep-11 10:01 AM
admin (demo)	admin (demo) getworkflows	187.183.44.151	Web browser	2024-Sep-11 10:01 AM
deepti	Retrieved RMC Commands for device [d317e22d-d456-40b8-b1a9-61b55f6e2267] of user deepti	171.76.81.243	Cloud Sync	2024-Sep-11 09:57 AM



## Data Visibility with Metadata Tags

Metadata is a critical element of FileCloud's content model; it provides information about the content itself, supporting data visibility and availability within the FileCloud system.

FileCloud includes built-in metadata sets that address:

- Image attributes
- Document Life Cycle
- Microsoft Office Tag
- Color Tag
- PDF Tag
- AIP Sensitivity Label

Admins can also create any number of custom metadata sets. Collectively, metadata underpins various functionalities within FileCloud, including content classification, DLP rules, retention policies, and workflows.

Properties

Details

Metadata

Versions

Add Metadata

Add

Image metadata

Width

2448

Height

3264

Image Orientation

Image Orientation - Numeric



Manage Content Classification Rules

Switch to new

Rules

Add rule

Manage Pattern Group

Rule Name	Match Action	Status	Auto-classification Enabled	Last Run Date/Time	Actions
6-digit test	{"Pii":{"Confidentiality Level":"HIGH"}}	UNEXECUTED	FALSE		▶ ⚙ ✕
CL-10541 Rule 1	{"Pii CL-10541":{"Confidentiality Level":"HIGH - Rule 1"}}	UNEXECUTED	FALSE		▶ ⚙ ✕
CL-10541 Rule 2	{"Pii CL-10541":{"Confidentiality Level":"HIGH - Rule 2"}}	UNEXECUTED	FALSE		▶ ⚙ ✕
CL-10541 Rule 3	{"Pii CL-10541":{"Confidentiality Level":"HIGH - Rule 3"}}	EXECUTING	YES	Sep 20, 2023 6:30 PM	▶ ⚙ ✕
PDF upload	{"Mobile test":{"Test attribute":"testTest text"}}	EXECUTING	FALSE	Jan 31, 2024 1:34 PM	▶ ⚙ ✕
Visa Card Provider	{"Pii":{"Confidentiality Level":"LOW"}}	EXECUTING	YES	Jan 31, 2024 1:34 PM	▶ ⚙ ✕
icap_dlp	{"DLP allowed":{"dlp-allowed":false}}	EXECUTING	YES	Aug 23, 2023 6:30 PM	▶ ⚙ ✕
test	{"DLP allowed":{"dlp-allowed":false}}	EXECUTING	YES	Sep 20, 2023 6:30 PM	▶ ⚙ ✕
test dlp 9 digits	{"Pii":{"level":"HIGH"}}	EXECUTING	YES	Aug 23, 2023 6:30 PM	▶ ⚙ ✕

◀

Page

1

of 1

▶

9 rows

## Automatic Document Organization with Smart Classification

The [Smart Content Classification Engine \(CCE\)](#) further refines how files are organized and tracked by FileCloud. With one or more sets of initial metadata, classification can automatically add or alter metadata.

Examples of this process include:

- For files containing nine-digit credit card numbers, CCE can mark PII security level as “HIGH”
- For PDFs with the metadata text attribute “Holiday vacation requests” uploaded after October 1st, CCE can add text attribute “HOLIDAY REQUESTS” and number attribute “2019”.



## Retention Policies

As an administrator, you can create [Retention Policies](#) to automate some of the processing related to protecting files and their folder groupings. This policy-based automation is designed to help secure digital content for compliance, but it can also enhance the management of digital content for other business reasons.

- Retention policies are created and attached to files and folders.
- These special policies allow you to define the conditions that enforce a set of restrictions on how each file or folder can be manipulated.

### Store Deleted Files

This feature provides a way to keep deleted files in a "recycle bin." When this option is enabled and a user deletes a file/folder, the deleted item gets moved into his/her personal deleted files area. Then the user can restore files from recycle bin or empty recycle bin completely.

### Clear Deleted Files in Specified Days

The administrator can set the number of days after which the deleted files will be emptied automatically. Admin has full control over the deleted files, and can empty or restore the deleted files via admin portal for all the users.

### Add Retention Policy

#### Policy Attributes

Policy Name\*

DPO\_Admin

Policy Type

✓ Retention

Archival

Legal Hold

Trash Retention

Admin Hold

Hide Policy From Users ⓘ

Enabled ⓘ

Alert On Violation ⓘ

Send email alert ⓘ

Alerts\*

Type in a comma-separated list of email addresses of users who need to know that a policy expires



## FAQ 8

### What if I need to comply with cybersecurity regulations (e.g., GDPR)?

FileCloud is a powerful EFSS solution that balances hyper-security with ease of use.

For enterprise and government clients all over the world, the ability to securely share and collaborate on files while enforcing data governance controls within a protected environment is a critical component within a greater strategy of continuity and growth. This reason alone is enough for these clients to deploy FileCloud as part of their IT infrastructure.

However, many organizations must also meet cybersecurity requirements and regulations. FileCloud enables these organizations to meet such requirements and demonstrate compliance.

Interested in learning how FileCloud supports a specific regulation or compliance requirement?

[Visit our Compliance & Security Library →](#)

- [Compliance Center](#)
- [Compliance & Security Resource Library](#)

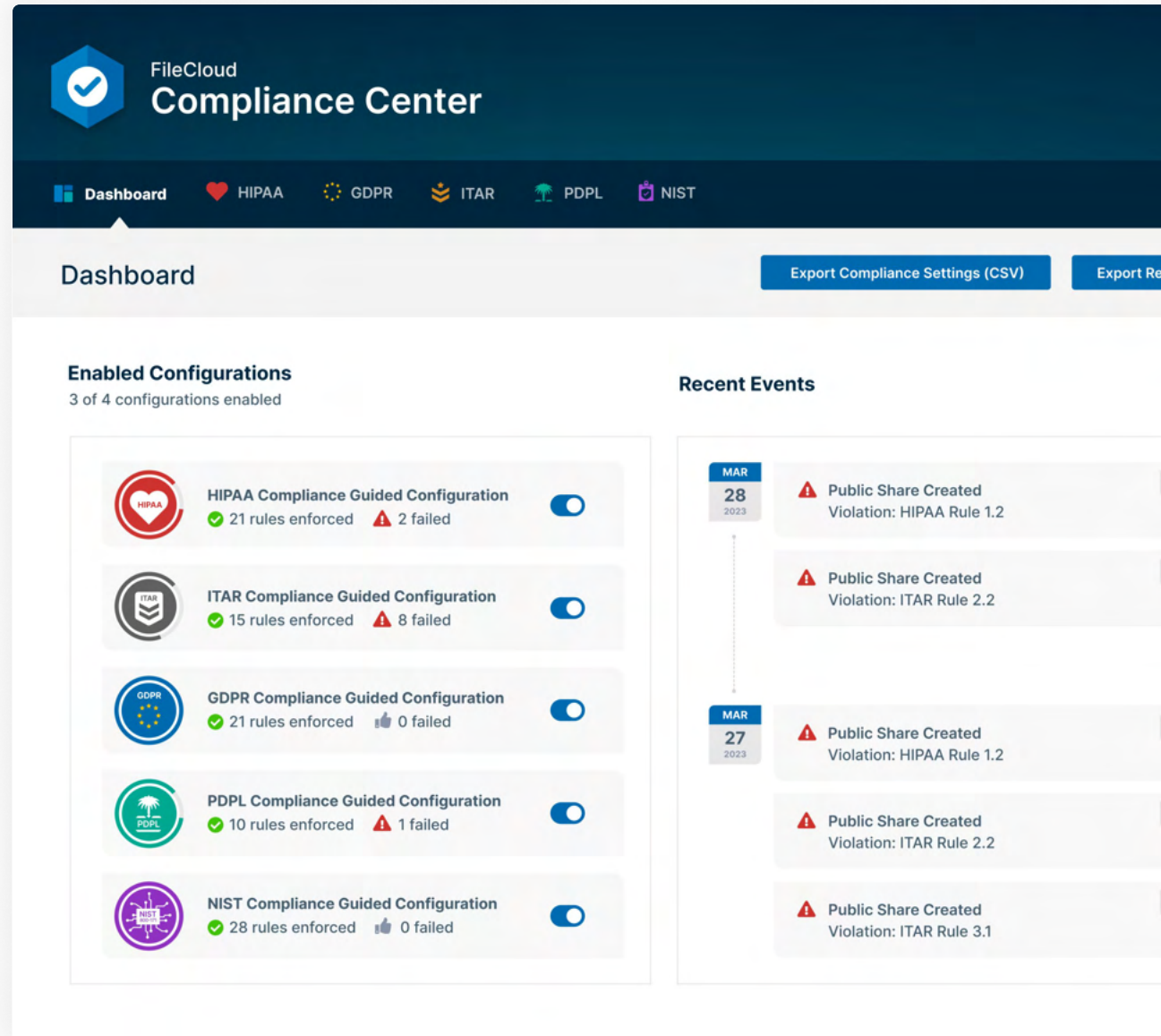


## Compliance Center

FileCloud's [Compliance Center](#) is a streamlined interface that organizations can use to support regulatory requirements. Specialized support configurations are available in the dashboard for GDPR, HIPAA, NIST 800-171, ITAR, and the Saudi Arabian PDPL.

Admins can select the relevant configuration and toggle rules they would like to activate. FileCloud will then scan the system and provide feedback on any possible issues or violations, along with recommendations to resolve them.

For regulations not covered by the Compliance Center, FileCloud also offers a [Compliance & Security Resource Library](#), which includes in-depth white papers and guidance on an even broader range of regulations and how FileCloud can support them.



The screenshot displays the FileCloud Compliance Center dashboard. At the top, the FileCloud logo and 'Compliance Center' title are visible. Below this is a navigation bar with icons for Dashboard, HIPAA, GDPR, ITAR, PDPL, and NIST. The main content area is titled 'Dashboard' and includes two primary sections: 'Enabled Configurations' and 'Recent Events'.

**Enabled Configurations**  
3 of 4 configurations enabled

Configuration	Rules Enforced	Rules Failed	Status
HIPAA Compliance Guided Configuration	21	2	On
ITAR Compliance Guided Configuration	15	8	On
GDPR Compliance Guided Configuration	21	0	On
PDPL Compliance Guided Configuration	10	1	On
NIST Compliance Guided Configuration	28	0	On

**Recent Events**

Date	Event
MAR 28 2023	Public Share Created Violation: HIPAA Rule 1.2
MAR 28 2023	Public Share Created Violation: ITAR Rule 2.2
MAR 27 2023	Public Share Created Violation: HIPAA Rule 1.2
MAR 27 2023	Public Share Created Violation: ITAR Rule 2.2
MAR 27 2023	Public Share Created Violation: ITAR Rule 3.1



## About Us

FileCloud is a hyper-secure file sharing, collaboration, and governance solution that provides industry-leading tools for compliance, data leak protection, data retention, and digital rights management. Workflow automation and granular control of content sharing are fully integrated into the complete feature stack.

The FileCloud platform offers powerful file sharing, sync, and mobile access capabilities on public, private, and hybrid clouds. Headquartered in Austin, Texas, FileCloud is deployed by top Global 1000 enterprises, educational institutions, government organizations, and managed service providers, with over one million users worldwide.



**1M+**  
USERS



**3000+**  
ENTERPRISES



**100+**  
RESELLERS



**90+**  
COUNTRIES



13785 Research Blvd, Suite 125  
Austin TX 78750, USA

**Phone:** U.S: +1 (888) 571-6480

**Fax:** +1 (866) 824-9584

[CONTACT US](#)



US Army Corps  
of Engineers



Deloitte.



## Copyright Notice

© 2024 FileCloud. All rights reserved.  
No reproduction without written permission.

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

