FileCloud Server Version 23.232

Security Checklist

Printed on 02/08/2024

Copyright Notice

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

FileCloud

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

Fax: +1 (866) 824-9584

Email: support@filecloud.com

Table of Contents

FileCloud includes a number of configurable security features that offer a range of choices. Many of these have recommended settings for most setups or for common deployments.

When you set up FileCloud, go through the following security checklist to make sure you are using the recommended features and setting them to the optimal values for your system and users. Click the names of the topics for more detailed lists and links to help topics.

1) User Authentication

Use default authentication or directory services such as AD and LDAP to ensure that only authorized users can log in to FileCloud.

2) Access control

Set up user and admin permissions to control who can access which data.

3) Data Encryption

Use encryption options for data in transit and at rest to protect its confidentiality and integrity.

4) Deployment and Network Hardening

Keep your infrastructure safe from unwanted access by using secure ports.

5) Governance

Fully employ FileCloud's governance features to make sure your data is safe and saved or deleted when it should be.

6) Secure file sharing

Ensure that users share files securely by setting up defaults such as share expiry dates, file change notifications, and download limits.

7) Protection against attack

Deter attacks by using antivirus software, configuring secure cookie settings, and limiting file extensions uploaded.

8) Maintaining a history of system actions

Configure audit logs to keep track of system events.

9) Client Device Protection and Management

Control user devices through remote client management, and use client application policies to set restrictions on actions.

10) Keeping FileCloud Up To Date

Apply FileCloud upgrades and patches when they are made available to eliminate any gaps in security.

Security Checklist: 1 User Authentication

Ensure that only users with the right credentials can access data by employing default authentication or active directory services such as AD and LDAP. In addition, consider setting up 2FA, requiring strong passwords and adopting other practices like automatic session timeouts and reCaptcha verification.

Use Active Directory (AD) or LDAP Authentication

If you store your users in AD, import them from AD into FileCloud and set up AD authentication. If you are using LDAP to connect to your AD server or a third-party authentication system, you may set up LDAP authentication or AD authentication.

By default, LDAP communications between client and server applications are not encrypted, so we recommend that you enable LDAP over Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
You can also enable AD over SSL.

For help setting up these integrations, see:
Active Directory Authentication
LDAP Based Authentication

Set up two-factor Authentication (2FA)

Once you choose your authentication type, determine whether to require 2FA on both browser and mobile logins. Note that use of 2FA is recommended for all external users.
See Two Factor Authentication.

Another way to set up multiple authorization on mobile devices is to require users to enter a pin code to access any FileCloud app.
See Setting Client Application Policies.
To show users how to configure a pin code on their iOS or Android device, see:
Configure iOS Security
Setting a Lock on Your Android App

Strong Password Management

FileCloud recommends that your users choose strong passwords that require different types of characters, have minimum lengths, and avoid commonly-used passwords. FileCloud provides these settings and several additional ones so you can create a strong password policy.
See Password Settings

Other Authentication Options

Other authentication options may be beneficial in your setup or may be required if you follow software compliance standards.
See:
Desktop Apps Code-Based Authentication
"Who can create and approve accounts" in New Account Creation

User Session Expiration
reCaptcha Settings

Security Checklist: 2 Access Control

Use access control to set up rules determining who can see what data and what actions they can take on it. The following methods are recommended for setting up access control in FileCloud:

Add granular permissions to folders:

You can set up permissions on your Team Folders to specify who has access to each folder and whether they have the ability to view, edit, share, delete, and manage each folder.
For information, see Set Granular Permissions on Team Folders

You can also give users the ability to set up granular permissions to the folders in their My Files folder.
See Enable Folder-Level Permissions

For user instructions for setting granular permissions on folders, see:
Set Permissions on Folders in the User Dashboard

Use role-based access control (RBAC)

In role-based access control (RBAC), admin user roles are given access to different actions and information in the system.
For information about setting up roles and assigning them to admin users, see:
Managing Admin Users.

Set up policies for users and groups

Policies define a set of permissions that apply only to users and groups assigned to the policy.
For information about creating policies and policy options, see:
Policies
Manage A User's Policies

For information on specific security policies, see:
User Session Expiration
Set the Global Share Mode
Desktop Apps Code-Based Authentication
Setting Client Application Policies
Notifications for File Changes
Automated Workflow Management

Set expiration dates for temporary users

This is useful if you have temporary workers such as contractors. You can also disable the user account and enable it again later.
See:
Setting a User Account to Expire
Disable a FileCloud User Account

Additional methods of Access Control

Set up DLP rules that prevent downloads by users who match or don't match criteria.
Smart DLP
Allow downloading files from authorized partners only

Make sure users create shares with proper permissions.
Private Share Permissions for Files
Share Options for Public and Private Folders

Enable file locking and show users how to lock/unlock files.
File Locking

Security Checklist: 3 Data Encryption

For optimal security, encrypt your data in transit and at rest.

Encrypt data in transit

To protect your data in transit, obtain an SSL certificate so you can run your production server on the HTTPS protocol.
See:
SSL Configuration
HTTPS Best Practices for FileCloud
Changing a Default Port or Web Server Setting

For information about connecting with TLS, see:
Enforcing TLS 1.2 and TLS 1.3 and Strong Ciphers - FileCloud Docs - Server
Configure MongoDB Cluster to Use TLS-SSL with Cluster Authentication and Mongodb Authentication on Linux

Encrypt data at rest

Protect the confidentiality and integrity of your stored files by configuring managed storage with encryption keys.

For detailed information, see:
Setting up Managed Storage Encryption - FileCloud Docs - Server
Setting up Managed S3 Storage Encryption - FileCloud Docs - Server
S3 Storage Encryption with AWS Cross-Account KMS Key

Security Checklist: 4 Deployment and Network Hardening

Follow best practices for deploying FileCloud and securing MongoDB.

Deploy FileCloud securely

Use one of the recommended deployments for FileCloud.
See Deployment.

After installing FileCloud

Review the basic and extended checks.
See:
Basic Checks
Extended Check

Protect data stored in MongoDB

Configure MongoDB securely.

Advisory: Bind MongoDB to 127.0.0.1 Only
Enable MongoDB Bind IP and Authentication
Configure MongoDB Cluster to Use TLS-SSL with Cluster Authentication and Mongodb Authentication on Linux

IP Address changes

FileCloud performs automatic logouts when users' IP addresses change.
If this is not desired in your system, see Manage IP Checks.

Restrict UI access based on IP address

For additional protection, restrict access to the admin or user portal by denying or allowing specific IP addresses.
See:
Restricting Access To Admin UI Based On IP Addresses
Restricting Access To User UI Based On IP Addresses

Security Checklist: 5 Governance

Use FileCloud's data governance features to ensure the security of your data whether your are protecting personal information, preventing data leaks, or remaining compliant by storing data for required time periods. The following features can help you create a solid data governance strategy:

Metadata

Use metadata to tag files and folders containing important information, such as personal data or company information, so that other governance features like DLP and retention policies can locate files that must be made secure.

See Managing Metadata.

Smart Classification

Use FileCloud's smart classification engine to identify files containing specific words or text patterns, and then tag them with selected metadata, so that DLP rules and retention policies may be applied to them.

See the section Smart Classification.

Smart DLP

Use Smart DLP or data leak prevention to safeguard against leaking of secure data. Use DLP to create rules that enable downloading, sharing and logging only on conditions you specify such as certain metadata values or IP addresses.

See the section Smart DLP.

Retention Policies

Create retention policies to specify how long files must be retained and to set limits on other actions performed on them.

See the section Retention Policies.

Compliance Center

Use the **Compliance Center** to check which regulatory requirements your system meets and which it fails to meet. Currently, the compliance regulations covered are:

- ITAR
- HIPAA
- GDPR

See Compliance Center.

DRM

Use FileCloud's digital rights management (DRM) file export feature to export and share files securely by requiring recipients to view them through a secure viewer.

See DRM for exporting secure documents.

Beginning in FileCloud 23.232, a web-based Secure Web Viewer is available as a beta version for viewing files that have been shared with the **Allow anyone with Secure Web Viewer link and a password** sharing option.

See Secure Web Viewer for DRM.

Zero Trust folders

Show users how to create Zip files within FileCloud and add a password to them to create them as encrypted Zero Trust folders.

For information about setting up Zero Trust folders, see Configuring Zip Files and Zero Trust File Sharing.

For details on how users can create Zero Trust folders, see Working with Zip Files.

Recycle Bin Settings

Use recycle bin settings to make sure unintentionally deleted data can be restored and data that shouldn't be disseminated is deleted.
See Manage the Recycle Bin Using Policies.

Security Checklist: 6 Secure File Sharing

Make sure users set up shares securely so that only authorized recipients can access shares and perform those actions that are granted to them.

Share permissions and options

Private shares are only available to specified users and groups and allow share creators to assign a range of permissions - view; download; upload; share; sync; delete; and manage - to each user or group. As a best practice, users should only assign share recipients the permissions they need to complete their tasks.

Share options enable users to add extra security by setting expiration dates on shares, limiting the number of times a share can be downloaded, and sending email notifications to share owners when shares are modified.

Users can view information about setting private share permissions and options at:
Private Share Options for Files
Private Share Permissions for Files
Share Options for Public and Private Folders

Admin Sharing defaults and limitations

Use administrator-set defaults and limitations to control how users configure their shares.

For more information about setting share defaults and limitations, see:
Configure Sharing Defaults
Secure Shares
Set the Global Share Mode

Require Share Approval Workflow

Whether or not you require share approvals for your users depends on the content being shared, who the share recipients are, and your compliance rules.

For information about requiring and specifying share approval workflows for users, see Automated Workflow Management.
For information about creating a share approval workflow, see Share Approval Workflows.

Add DLP Rules that Control Sharing

Use FileCloud's Smart DLP to set up rules that control sharing actions based on file or folder metadata, share recipient's domains, and other information.

For information about using Smart DLP, see Smart DLP.

For examples of using DLP to control sharing, see:
Detect confidential documents with PII and allow internal shares only
Detect documents with US Social Security Number and allow sharing only with specific domains

NTFS Permissions

If your organization has Windows-based network folders that are shared among employees, the permissions on these network folders are managed using NTFS rights set up for various users and groups (generally from Active Directory). Configure FileCloud to use these same NTFS permissions on Network Folders to strengthen user authorization and access control.

Network Folders with NTFS permissions

Security Checklist: 7 Protection Against Attack

Protect your system against cyber attack by using anti-virus software as well as other methods to restrict the types of files that enter your system and the locations where they come from.

Anti-virus scanning

Either use ClamAV, an open-source anti-virus product that comes with FileCloud or ICAP, a protocol that enables you to use your own anti-virus software with FileCloud.
See the section Enable Antivirus Scanning.

Allow and Disallow uploading of specific file extensions

As another method of preventing malicious content, either choose to allow or disallow specific file extensions from being uploaded to FileCloud.
See Managing File Extensions.

Use FileCloud's heuristic engine to detect ransomware

FileCloud includes a heuristic engine that looks for files that identify their content inaccurately, a method sometimes used to perform ransomware attacks or otherwise trick users into opening files containing malicious code.
See File Content Heuristic Engine.

Add DLP rules that control file downloads

Use FileCloud's Smart DLP to set up rules that only allow downloads by internal users or external users from specific locations.
For information about using Smart DLP, see Smart DLP.
For an example of using DLP to control downloading, see Allow downloading files from authorized partners only

Integrate with SIEM

FileCloud enables you to integrate with a third-party SIEM (Security Information and Event Management) product which analyzes information from FileCloud to find potential security threats.
See the section SIEM Integration.

Improve Cookie Security

FileCloud includes several cookie settings that enable you to strengthen your security when information is sent in response to requests.
See Improving Cookie Security.

Backing up

To protect your system against the loss of data caused by a ransomware attack, back it up regularly so you have a saved copy that you can restore if necessary.
See Backing Up and Restoring FileCloud Server.

Security Checklist: 8 Audit History

Audit log

FileCloud keeps an audit log which can grow large very quickly.

To change the logging level and set up automatic archiving and removal:
see Configure What is Logged and Delete Audit Log Entries.

For general information about configuring and viewing audit logs in FileCloud:
see the section Audit Logs.

Integrate with SIEM

FileCloud enables you to send events (similar to those sent to the FileCloud audit log) to a third-party Security Information and Event Management (SIEM) product which further analyzes the events and detects threats and trends. See the section SIEM Integration.

Security Checklist: 9 Client Device Protections

Your users may connect to FileCloud through the wide number of clients such as FileCloud Sync, FileCloud Drive, and your Android or iOS device.

Monitoring, blocking, and wiping devices

You can monitor, block, and delete content on FileCloud clients using FileCloud's **Manage Devices** screen.
For more information, see:
Managing Client Devices
Blocking and Remotely Wiping a Client Device

Configuring centralized device management

For most of the FileCloud clients, you can configure default settings in policies, such as authentication types and file deletion requirements.
See the section Configure Centralized Device Management.

Centralized device management for mobile apps

FileCloud allows you to add custom security policies for its mobile apps, such as requiring an app pin or disabling sharing.
For more information, see Setting Client Application Policies.

Mass deployment

For most of the FileCloud clients, you can configure mass deployment settings for security features such as required use of TLS servers, automatic file locking, and authentication type.
For more information, see:
Mass Deployment - Default Configuration Support.

Security Checklist 10 Keeping FileCloud Up To Date

A large part of maintaining any system's security is keeping informed about updates, patches, and security advisories and making sure you apply them.

- When an upgrade to FileCloud is available, FileCloud informs you through email and the **Version Information** widget on the FileCloud dashboard.
  See Upgrade FileCloud and Release Notes.
- When a FileCloud security advisory is published, FileCloud sends you an email noting the severity level of the issue and what you should do to protect yourself against it.
  See Security Advisories.
- FileCloud upgrades third-party components that are used as part of the system. However, you should keep external software that you use in conjunction with FileCloud updated as well.
- FileCloud informs you if required external components must be upgraded to specific versions and attempts to document instances where minimum versions of optional external components should be installed.

Regular Security Checks

The following is a suggested list of security settings you can review at scheduled times to make sure your FileCloud system's security is continuously maintained.

- FileCloud is updated to latest version.
- New users have been taught how to:
    - Add security to file/folder shares
    - Set permissions on folders
    - Lock files they are working on
    - Use DRM and Zero trust folders
    - Current users have confirmed that they are using the above security strategies
- New temporary user accounts have expiration dates.
- Newly added Team Folders have granular permissions added.
- RBAC permissions have been monitored to remove permissions certain admin users no longer need.
- Unnecessary user accounts have been deleted.
- Governance settings (for workflows, metadata, CCE, DLP, retention policies, and compliance) have been modified to address security need changes as requirements and users have changed.
- Client devices that are problematic or no longer used have been blocked or wiped.
- During any issues audit log settings have been changed and then set back.
- If automated audit log deletion is not set up, manual deletion of audit logs has been performed.