FILECLOUD

FileCloud Security Checklist

FileCloud v23.241

Security Category	Category Objective	Supporting Actions & Options in FileCloud
User Authentication	Ensure that only authorized users with the right credentials can access data.	• Use Active Directory (AD) or LDAP Authentication. • Set up two-factor authentication (2FA). • Enable strong password management for users (or autogenerate strong passwords and send to users upon account creation). • Review and apply any other authentication options as required by your organization security or compliance standards, such as: ◦ Code-based authentication for desktop apps ◦ New account creation policies ◦ User session expiration ◦ ReCAPTCHA settings
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. • Use role-based access controls (RBAC). • Set up policies for users and groups. • Set expiration dates for temporary users. • Set up additional methods of access control, such as: ◦ DLP rules ◦ Share permissions and policies ◦ File locking/ unlocking.
Data Encryption	Use encryption options for data in transit and at rest to protect its confidentiality and integrity.	• Encrypt data in transit. • Encrypt data at rest.
Deployment & Network Hardening	Keep your infrastructure safe from unwanted access by using secure ports.	• Deploy FileCloud with recommended security settings. • After installing FileCloud, review the Basic and Extended Checks. • Protect data stored in MongoDB. • Manage IP checks for automatic logout. • Restrict UI access based on IP address.
Governance	Fully employ FileCloud’s governance features to make sure your data is safe and saved or deleted when it should be.	• Manage metadata. • Enable Smart Classification. • Enable Smart DLP. • Set up Retention Policies. • Use the Compliance Center to help meet regulatory requirements for ITAR, HIPAA, GDPR, NIST 800-171, and KSA PDPL. • Enable DRM features. • Enable Zero Trust folders. • Adjust Recycle Bin settings.
Secure File Sharing	Ensure that users share files securely by setting up defaults such as share expiry dates, file change notifications, and download limits.	• Review share permissions and options. • Enable admin sharing defaults and limitations. • Set up “Require share approval” workflows. • Add DLP rules to control sharing. • Configure NTFS permissions.

Protection Against Attack	Deter attacks by using antivirus software, configuring secure cookie settings, and limiting file extensions uploaded.	• Enable anti-virus scanning. • Allow and disallow uploading of specific file extensions. • Use FileCloud's heuristic engine to detect ransomware. • Add DLP rules that control file downloads. • Integrate with SIEM. • Delete the installation folder after confirming access. • Improve cookie security. • Back up systems (or enable automatic backups).
Audit History	Configure audit logs to keep track of system events.	• Adjust automatic logging levels. • Set up automated archiving and removal of logs. • Integrate with SIEM.
Client Device Protection & Management	Control user devices through remote client management, and use client application policies to set restrictions on actions.	• Enable monitoring, blocking, and deletion of content on FileCloud clients through Managed Devices. • Configure centralized device management. • Centralize device management for mobile apps. • Configure mass deployment settings.
Keeping FileCloud Up to Date	Apply FileCloud upgrades and patches when they are made available to eliminate any gaps in security.	• Join FileCloud's mailing list to be notified of upgrades and security advisories. • Check the Version Information widget on the FileCloud dashboard. • Check FileCloud's documentation for release notes and security advisories. • Update third-party software used in conjunction with FileCloud regularly. • Upgrade external components when recommended by FileCloud to meet upgrade requirements.
Regular Security Checks	Review recommended security settings regularly for optimal performance.	• Check running FileCloud version and update if necessary. • Ensure 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. ◦ Confirm they are using the above security strategies. • Set expiration dates for new temporary user accounts. • Add granular permissions to newly added Team Folders. • Monitor RBAC permissions to regularly remove those which are no longer needed. • Delete unnecessary user accounts. • Modify governance settings (for workflows, metadata, classification, DLP, retention policies, and compliance) to address security changes. • Block or wipe client devices that are no longer used (or that are problematic). • Reset audit log settings after issues are detected. • Manually delete audit logs if deletion has not been automated.

For more details, access the dynamic Security Checklist in FileCloud's documentation:

https://www.filecloud.com/supportdocs/fcdoc/latest/server/filecloud-administrator-guide/filecloud-security-checklist