FILECLOUD

FileCloud Security FAQ

FileCloud is currently used by many large organizations including banks, health care organizations, educational institutions and government agencies. Thousands of organizations rely on FileCloud for their file sharing and collaboration needs. Our customers handle sensitive data and they give utmost importance to data security, system ownership and regulatory compliance. FileCloud provides end-to-end data protection with multiple levels of security at each layer. With FileCloud, one can be rest assured that corporate data is well protected in company servers and employee devices. This document answers frequently asked questions regarding FileCloud Security Features.

Table of contents

1.

How Secure is FileCloud?

FileCloud is completely secure and offers multiple levels of data protection. Below is a list of the most notable security features:

Encryption in-transit and at rest

FileCloud protects the confidentiality and integrity of your files in transit and at rest.

+ AES 256-bit encryption to store files at rest.
+ SSL/TLS secure tunnel for files transmission.
+ Site specific, customer managed encryption keys in a multi-tenant setup.

Two-factor authentication

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 login to FileCloud or link a new phone, or tablet.

Anti-virus 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.

Industry Best Practices

FileCloud security includes 256-bit AES SSL encryption at Rest, Active Directory integration, two-factor authentication, granular user and file sharing permissions, client application security policies, anti-virus scanning, unlimited file versioning, recycle bin, file locking, endpoint device protection and comprehensive HIPAA compliant audit trail.

2.

FileCloud Security Measures and Features

How can I control who is authorized to use FileCloud system?

FileCloud supports integration with enterprise identity management systems such as LDAP and AD. Therefore, large organizations with existing authentication systems in place can choose to integrate their FileCloud user accounts directly with their active directory deployment.

This allows companies to embrace the cloud without decentralizing user management. 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 SSL. FileCloud supports single sign-on through NTLM as well as SAML SSO.

How is access control handled in FileCloud?

User authentication

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.

Two-factor authentication

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 2FA 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 a another computer, FileCloud immediately recognizes the unauthorized request by making only one 2FA code available at any point in time.

FileCloud also provides the ability for admins to set shorter length default login sessions using the session timeout parameter. This will keep users actively logged into their account for a limited time only. Once the user excesses the inactivity period the session expires, and the users are required to login again.

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 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 adding an extra layer of password protection against unwanted intrusion.

Login credentials

All users are required to enter their username and password. Administrators can set user password strength (i.e. require complex alphabetical and numerical permutations). Additionally, FileCloud monitors and logs all access attempts to user portal.

To protect login credentials, user passwords are hashed using secure hash algorithm. SHA-1 is a secure hash algorithm required by law for use in certain U.S. Government applications, is used in conjunction with other cryptographic algorithms and protocols for the protection of sensitive unclassified information.

How secure is file sharing in FileCloud?

FileCloud employs several layers of authentication to ensure that only authorized recipients can access the files.

Share expiry

The shared folder/file can be configured for expiry by admin and blocks access to the file after its expiration.

File change notification

Admin and users automatically receive notifications through email when files are added, updated or deleted. FileCloud administrators can enable/disable file change notification emails to be sent whenever files have been changed.

Download limit restrictions for public shares

Download limit restrictions can be set for files, which are publicly shared. This limited the number of downloads thus reducing the risk of misusing the file.

NTFS shares

Many organizations have Windows-based network folders that are shared among employees. The permissions on these network folders are managed using NTFS rights setup for various users and groups (generally from active directory). FileCloud can use the same NTFS permissions on the Network Folders for user authorization and access to these resources.

How is data leak prevention done in FileCloud?

FileCloud has unique capabilities to monitor, prevent, and fix data leakage assuring corporate data is protected across all devices (laptops, desktops, smartphone, and tablets).

Remote wipe

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

Audit reporting

Activity logs capture the, “what, when, who, why, and how,” attributes of every user action within the system. Admins can easily filter logs and identify problems.

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.

3.

Permission Control

How to manage 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 permissions for each individual user. Access permissions are generally enforced uniformly regardless of location and access method (web browser, FileCloud drive, WebDAV, FileCloud sync, mobile/tablet app).

Admins can also set an expiration date for a user, after which the user permissions will expire and will no longer have access to the FileCloud system. Admin can also disable the user for a certain period of time.

4.

Network security

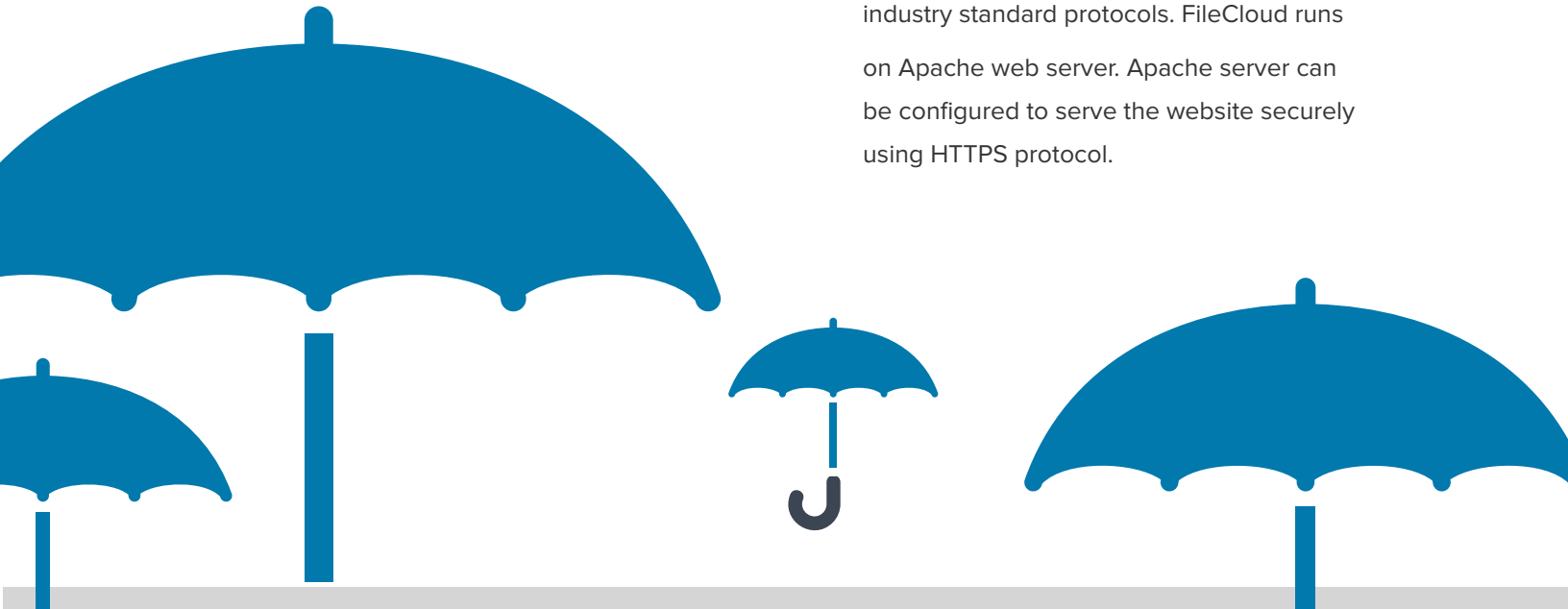
How is FileCloud configured for security with external recipients?

In some networks, it may not be possible or desired to open the firewall port directly to a machine on the LAN, in this case, a server running a HTTP reverse proxy (Microsoft IIS or Apache and others) in the DMZ outside the LAN can forward HTTP requests to the actual FileCloud server in the LAN.

5.

Transport security

Transportation security is enforced with industry standard protocols. FileCloud runs on Apache web server. Apache server can be configured to serve the website securely using HTTPS protocol.



6.

Data Security

How is data secured in FileCloud?

Storage level encryption

FileCloud supports storage level encryption, administrator may supply an optional master password and start the initialization process. Without a master password the encryption module cannot encrypt/decrypt files in the 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 the 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 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.

7.

Endpoint Device Protection and Management

How to manage remote devices connected to FileCloud?

FileCloud provides a centralized dashboard to control and monitor all remote devices. Within the device control panel, administrators can enforce additional security settings to manage mobile data and devices.

Block a device and force wipe of application data

FileCloud's RCM (Remote Client Management) function allows the Administrator to selectively block a specific client device from logging into the FileCloud server.
In addition to blocking a client device from logging in, the administrator can also wipe FileCloud folders in the remote device

+ If the client is not connected, the block (and remote wipe) will happen when a user tries to log into the server.
+ If the client is connected, the block and remote wipe will occur, and the client will automatically exit out.

Remove client record from the FileCloud system

This can be due to number of reasons such as the user ID is no longer valid, or the associated client record no longer needs to be managed.

What are the various client application policies available in FileCloud?

FileCloud allows clients to customize client application policies (mobile clients, sync clients, drive client).

+ **Force mobile clients to enable FileCloud app pin lock.**
  If the pin lock is not enabled, the login will be rejected with appropriate message
+ **Disable all mobile client apps from connecting**
  This will prevent login into FileCloud system using mobile client apps (users will be allowed to login only via the web browser).
+ **Disable features such as - download, print, edit, open with, share, or option in mobile client apps.**
  Admin can set each policy to be overridden for specific user enabling the user to override the global policy.

8.

Data Removal

Store Deleted Files

This feature provides a way to keep deleted files in a "recycle bin." When this option is enabled and 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 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, he can empty or restore the deleted files via admin portal for all the users.

9.

What general security precautions should I take?

+ The FileCloud should run under SSL (HTTPS). The Apache webserver requires SSL enabled and SSL certificate valid for the domain needs to be installed. This ensures all data transmitted on transit is secure.
+ Ensure MongoDB database is bound to port 127.0.0.1 only **(See advisory).**
+ The clients must utilize ***https://domain*** instead of the standard ***http://domain***
+ Require stronger passwords by changing the required strength using the minimum password length setting.
+ Set default login session length shorter using the session timeout parameter.
+ Remote data wipe on mobile phones and PCs when needed.
+ Remote block of sync/drive clients and mobile devices.

+ Enable detailed audit logs (What, When, Who, Why and How)
+ Enable two factor authentication for all user logins.
+ Enable two factor authentication using PIN code for iPad and iPhone app.
+ Enable anti-virus scanning.
+ Enable server side file encryption for managed storage. Enable account lockout when wrong password is entered many times.