FILECLOUD’S ENCRYPTION CAPABILITIES

FileCloud’s Enterprise-Level Data Security Capabilities

FILECLOUD
WWW.GETFILECLOUD.COM

CONTENTS

Introduction

In the following documentation, you will learn how FileCloud can be used to protect your data. In today's era of modern technology, data encryption has become an industry standard. Data encryption is a method of data security where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encryption, in question, can be used to deter malicious or negligent parties from leaking sensitive data.

An important line of defense in a cybersecurity architecture, encryption makes using intercepted data as difficult as possible. It can fulfill all kinds of data protection needs, ranging from classified government intel to personal credit card transactions.

Security, privacy, and data ownership is fundamental to FileCloud's security architecture. FileCloud security starts with 256-bit AES SSL encryption at-rest and in-transit, Active Directory integration, multi-factor authentication, granular user and file-sharing permissions, client application security policies, anti-virus scanning, unlimited file versioning, file locking, endpoint device protection, anda comprehensive HIPAA compliant audit trail. With FileCloud, you always rest assured that your corporate data is well protected in your servers and employee devices.

By 2022, 50% of midsize and large organizations in mature regional markets will use a content collaboration (previously known as Enterprise Sharing and Sync - EFSS) platforms to implement document workflows and improve collaboration and productivity.

Strategic Assumption in
Gartner's Magic Quadrant for Content Collaboration 2018

Gartner peerinsights customers' choice 2018 ™

Gartner peerinsights customers' choice 2019 ™

FileCloud Recognized as a 2018 Gartner Peer Insights Customers' Choice for Content Collaboration Platforms

What is FileCloud?

FileCloud Server is a cloud-agnostic enterprise file-services solution. You can self-host FileCloud Server on your own on-premise servers and private data centers, or on public cloud IaaS providers such as AWS, Azure and Google Cloud. A self-hosted solution such as FileCloud Server offers the same features and benefits of public cloud SaaS services like Box and Dropbox while avoiding the drawbacks commonly found in these services, such as expensive pricing and essential features locked behind paywalls. FileCloud Server lets you run your own private cloud storage and sync solution for your employees, customers, and clients, all while maintaining complete control of your organizational data. FileCloud Server also helps you to increase ease-of-access to your existing organizational folder and file shares (Windows NTFS File Shares, CIFS, NFS, etc.) using a web portal and mobile apps without the need for a VPN.

What Types of Encryption Does FileCloud Support?

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

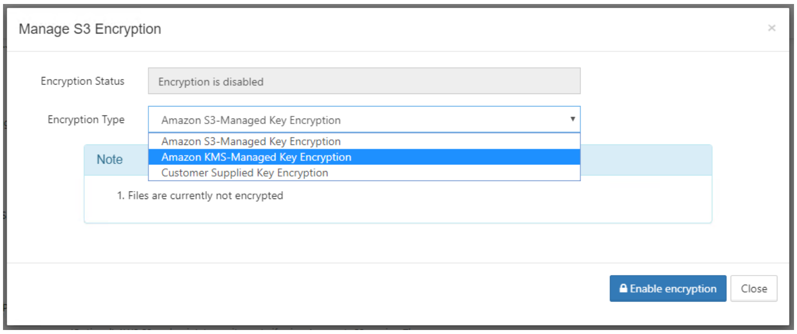
- AES 256-bit encryption to store files at rest.
- SSL/TLS secure tunnel for data transmission.
- Site-specific, customer-managed encryption keys in a multi-tenant setup.

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 256-bit AES encryption, one of the strictest 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.

FileCloud Online Encryption At-Rest



Manage S3 Encryption

Encryption Status: Encryption is disabled

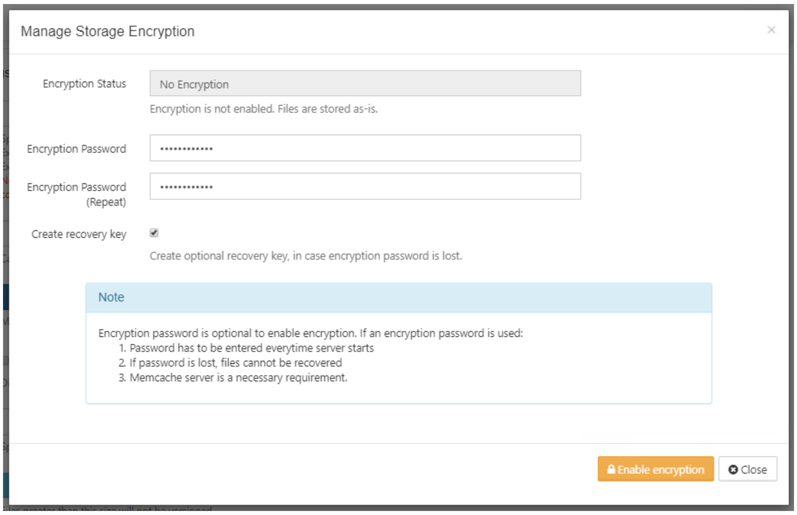
Encryption Type: Amazon S3-Managed Key Encryption

×
Amazon S3-Managed Key Encryption
Amazon KMS-Managed Key Encryption
Customer Supplied Key Encryption
Enable encryption
Close

Note

1. Files are currently not encrypted

FileCloud Server Encryption At-Rest



Manage Storage Encryption

Encryption Status: No Encryption

Encryption is not enabled. Files are stored as-is.

Encryption Password: ••••••••••••

Encryption Password (Repeat): ••••••••••••

Create recovery key: ☑

Create optional recovery key, in case encryption password is lost.

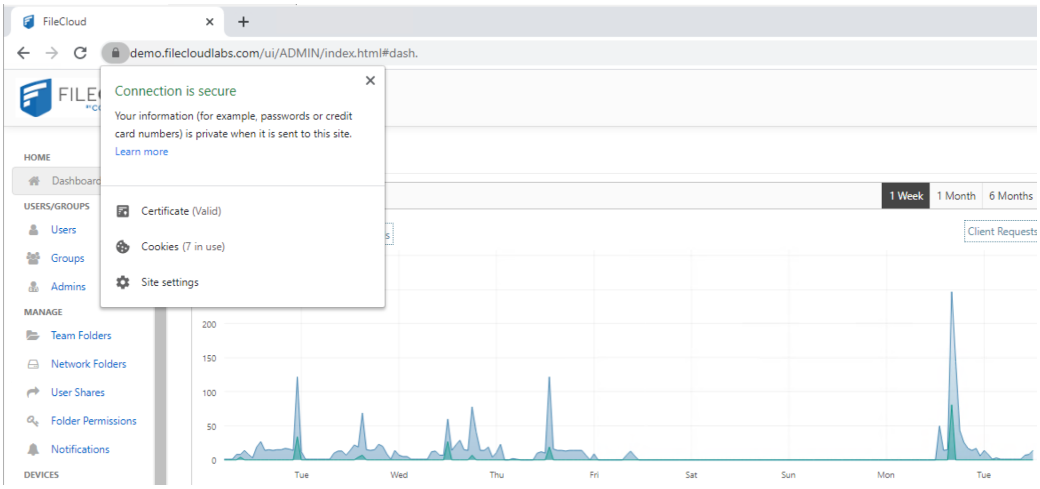
Note

Encryption password is optional to enable encryption. If an encryption password is used:

1. Password has to be entered everytime server starts
2. If password is lost, files cannot be recovered
3. Memcache server is a necessary requirement.

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.



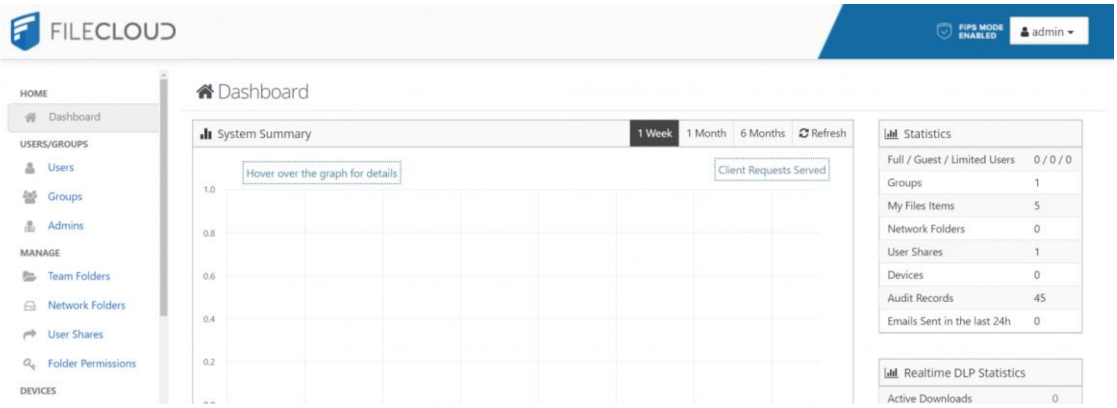
demo.filecloudlabs.com/ui/ADMIN/index.html#dash.

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

FIPS Compliance – Ensuring Data Security

FileCloud meets all necessary security requirements for Cryptographic Modules, which are formalized by the Federal Information Processing Standard (FIPS publication 140-2), validated by the US National Institute of Standards and Technology (NIST 800-171) and Canadian Communication Security Establishment (CSE). FIPS compliant encryption modules is required for US Federal organizations as well as government contractors that work for them.



Statistics	
Full / Guest / Limited Users	0 / 0 / 0
Groups	1
My Files Items	5
Network Folders	0
User Shares	1
Devices	0
Audit Records	45
Emails Sent in the last 24h	0

Realtime DLP Statistics	
Active Downloads	0

The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. The protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard also provides for increasing qualitative levels of security intended to cover a wide range of potential applications and environments. Enterprises who are subject to the FIPS regulations must install and run a FIPS-enabled operating system -- for example, CentOS in FIPS mode.

When using a FIPS-enabled license, FileCloud Admins will now see in the following changes in the Admin Portal:

- Running in FIPS mode is prominently displayed
- SSO features are hidden
- The storage encryption option is always shown

Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Note

- The data can only be accessed using the supplied key/secret credentials. The data will be accessible via S3 Console (which should NOT be done for FileCloud Managed storage data).
- The key to use the encryption is different as it will be associated with your own account, while the random key is based on generated based on the AWS account. This key is used to encrypt and decrypt files at an S3 level, 256-bit encryption.

Encryption

- 256-bit Advanced Encryption Standard (AES-256)

Benefits

- Each object is encrypted with a unique key.
- As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates.
- SSE-S3 uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Performance Impact:

- This option is the fastest encryption option available compared to others such as SSE-KMS or SSE-C
- Uploading files will not decrease performance for small files (5MB). However, bigger files (1GB or greater) will have a small impact on performance when compared to an environment without encryption.
- There is no noticeable impact when downloading encrypted files.

Impact on Restart:

- There is no impact, nor is there any user input required on restart as AWS KMS will handle the encryption/decryption process.

Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Similar to SSE-S3, but the key itself is managed using Amazon's KMS service. This allows the management of specific keys and their permissions for encrypting the data. The data is still encrypted at rest and accessible via S3 Console with appropriate credentials. When you use server-side encryption with AWS KMS (SSE-KMS), you can use the default AWS managed CMK, or you can specify a customer managed CMK that you have already created. If you do not specify a customer-managed CMK, Amazon S3 automatically creates an AWS managed CMK in your AWS account the first time that you add an object encrypted with SSE-KMS to a bucket. By default, Amazon S3 uses this CMK for SSE-KMS.

Note

- The data can only be accessed using the supplied key/secret credentials. The data will be accessible via S3 Console (which should NOT be done for FileCloud Managed storage data)
- You must create your own key resource in the AWS KMS. This provide you with an encrypted key, which you can use in FileCloud when configuring your encryption to encrypt and decrypt files.

Encryption

- 256-bit Advanced Encryption Standard (AES-256)

Benefits

- The encryption of data at its destination by the application or service that receives it.
- (AWS KMS) is a service that combines secure, highly available hardware and software to provide a key management system scaled for the cloud.
- Amazon S3 uses AWS KMS customer master keys (CMKs) to encrypt your Amazon S3 objects.
- The asymmetric encryption key that you can use to encrypt data outside of AWS KMS. This key is protected by asymmetric CMK in AWS KMS; it’s a single 256-bit secret encryption key that never leaves AWS KMS unencrypted.
- In addition to FileCloud auditing, this encryption method will also grant auditing capabilities at an S3 level.
- Single point kill-switch at an S3 level to avoid any service to consume data.

Performance Impact:

- This option not as fast as SSE-S3 encryption. However, it is faster than SSE-C.
- Uploading files will not decrease performance for small files (5MB). However, bigger files (1GB or greater) will have a small impact on performance when compared to an environment without encryption.
- There is no noticeable impact when downloading encrypted files.

Impact on Restart:

- There is no impact, nor is there any user input required as AWS S3 will handle the encryption/decryption process.

Server-Side Encryption with Customer-Provided Keys (SSE-C)

The data will be encrypted using customer supplied 32-bit encryption key.

Encryption

- 256-bit Advanced Encryption Standard (AES-256)

Note

- You cannot download or edit the files without FileCloud, data is provided in a read-only format.

Benefits

- Server-side encryption with customer-provided encryption keys (SSE-C) allows you to set your own encryption keys.
- Amazon S3 manages encryption as it writes to disks and decryption when you access your objects. Therefore, you don't need to maintain any code to perform data encryption and decryption.
- When you upload an object, Amazon S3 uses the encryption key you provide to apply AES-256 encryption to your data and removes the encryption key from memory.

Performance Impact:

- This option will have a SLOWER performance due to restriction on how this data can be decrypted (Amazon server will NOT be able to decrypt the data and the data has been first downloaded to FileCloud server and decrypted).
- The data will NOT be accessible via the S3 console as well.

Impact on Restart:

- For security purposes, FileCloud requires that a password is created to encrypt the encryption/decryption key. Prior to restarting the server, you will need to decrypt the key. Once done, you can proceed on restarting the server. It is important that when the server is back up you re-encrypt the key so that nely-added files are encrypted.

S3 Storage Encryption with AWS Cross-Account KMS Key

When you enable automatic key rotation for a CMK, AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. Key rotation changes only the CMK's backing key, which is the cryptographic material that is used in encryption operations. However, the automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key.

Note

- Manual key rotation is not supported by FileCloud.

Encryption

- 256-bit Advanced Encryption Standard (AES-256)

Benefits

- Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket.
- All new objects are encrypted when they are stored in the bucket
- When you use server-side encryption, Amazon S3 encrypts an object before saving it to disk and decrypts it when you download the object.

Performance Impact:

- This option is the is not as fast as SSE-S3 encryption. However, it is faster than SSE-C.
- File uploading will not decrease performance for small files (5MB). However, for bigger files (1GB or greater) will have a small decrease on performance when compared to an environment without encryption.
- There is no noticeable impact when downloading encrypted files.

Impact on Restart:

- There is no impact nor is there any user input required as AWS S3 will handle the encryption/decryption process.

Key	Key Details	User Input	Persistence	Remarks
Encrypted File Key	• Encrypted using a master public key	None	Encrypted file key is persisted	• The decryption of the encrypted file key results in plain file key • The decryption of the encrypted file key will be done using the master private key and optional master password • The plain key that is a result of the decryption process is cached for the lifetime of the FileCloud server process Note: Whenever you restart the server, the encrypted file key is decrypted again.
Master public/private key pair	• Asymmetric • 4096 bits • RSA • sha512 digest	Password (optional)	Both private and public keys are persisted	• It is important to save the password (if one was provided)
Plain File Key	• Symmetric • AES • 128 bits	None	Not persisted	• The plain file key will be used to encrypt decrypt all files using symmetric encryption • This key will not be persisted but will be cached for performance • The cache will be valid for the lifetime of the FileCloud server process