FILECLOUD

Hyper-Secure Content Collaboration. **Simplified.**

Get complete control, security, governance, compliance and data residency

Technical Specifications

Flexible Deployment Options	
FileCloud Enterprise Server	Self-host FileCloud on-premises or with a cloud service provider: • Amazon S3, Microsoft Azure Blob, Alibaba Cloud, Linode + • NFS, CIFS, SAN appliances
FileCloud Enterprise Online	Let us host FileCloud for you on our world-class infrastructure, on Amazon AWS in the region of your choice. • Deploy in GovCloud for greater security and compliance with federal regulations (US only)
FileCloud ServerSync (Hybrid)	Cloud-enable your on-prem file servers for easier access while preserving folder hierarchy and permissions (including NTFS).

Functional Requirements	
Supported Operating Systems	• Windows 2016 and 2019, Ubuntu 22.04 and RedHat 9 (RHEL 9).
Supported Browsers	• Microsoft Edge 15 and above, Google Chrome 55.0 and above, Mozilla Firefox 52 and above, Safari 11 and above
Network Ports	• 80 (HTTP traffic - external), 443 (HTTPS traffic - external) • Optional: 389 (LDAP – internal), 636 (LDAP SSL – internal)
Configuration	• Static and public IP address, minimum network connection of 512 Kbps upload and download, domain name, SSL certificate (recommended)

Hyper-Secure Infrastructure

Data Residency

Host your own data (FileCloud Enterprise Server) or allow us to host your data (FileCloud Online) in the region of your choice. Either option ensures that your data stays where you need it, to comply with data regulations and residency requirements.

Remote Access via Secure Clients & Apps

- FileCloud Drive and Sync clients
- Mobile Apps: iOS and Android
- FileCloud ServerLink - enables different offices to run separate FileCloud instances to reduce latency, improve uptimes, and support disaster recovery.

Run FileCloud Server in FIPS Mode

FileCloud FIPS license ensures that FileCloud runs in a FIPS 140-2 enabled OS with approved libraries and encryption:

- 256-bit AES encryption for data at rest
- TLS 1.3 encryption for data in transit
- SSO features hidden

Scalable Infrastructure

FileCloud offers scalable infrastructure options to meet functional or performance needs, including High Availability architecture, multitenancy, automated server backups and rollback features, and professional support services for mass deployments.

Zero Trust File Sharing℠

FileCloud users can leverage Zero Trust architecture in FileCloud through password-protected Zip files. The decryption key is not stored within the FileCloud system, so clients retain exclusive control and visibility over data.

FileCloud Encryption

By default, FileCloud offers 128-bit AES encryption for data at rest. 256-bit AES encryption is available upon request or with a FIPS license. FileCloud can deploy symmetric or asymmetric encryption. For clients using AWS S3 storage, S3 uses 256-bit AES encryption by default.

SSE + Customer Provided Key
SSE + Customer Master Key

- Client provides a master key, which is not known to FileCloud (asymmetric encryption); guarantees that data will only be read by the customer.
- Key is sent with every upload to the storage container.
- Slowest encryption speed

SSE + KMS (Key Management Services)

- KMS can be hosted in FileCloud Online or run on a customer's FileCloud Server account. FileCloud has access to this key with integration.
- New data/objects uploaded to the system auto-generate an object key, which is needed for decryption.
- Medium encryption speed

Server-Side Encryption (SSE)

- Plain file key used to encrypt and decrypt (symmetric) all files; key is cached for performance.
- Fastest encryption