Citrix ShareFile Security and Compliance FAQ

How ShareFile Safeguards your data

How does ShareFile secure my files?

ShareFile is a cloud-based Software-as-a-Service (SaaS) solution that enables you to exchange confidential business files easily, securely and professionally.

ShareFile safeguards your files in transit and at rest using industry accepted protocols. ShareFile stores your files in state-of-the-art datacenters equipped to protect against data loss, even in emergencies. Configurable controls let you choose your password policy, set account lockout and session timeout thresholds, and determine who can access files, folders and subfolders. You may create automatic alerts and notifications for certain account activities and set expiration dates on sensitive files. ShareFile mobile apps ensure you can access your files from any device, anytime — without compromising security.

How are my files secured when uploaded to and downloaded from ShareFile?

ShareFile employs Transport Layer Security (TLS) security protocols to protect authentication, authorization and file transfers. Your files are encrypted in transit with up to 256-bit encryption depending on your web browser capabilities. ShareFile employs a keyed-hashed message authentication code (HMAC) to authenticate and ensure the integrity of intra-system communications and relies on file size and hash to ensure file integrity.

How are my files secured when stored in ShareFile?

The ShareFile Software-as-a-Service (SaaS) application is hosted within cloud service providers like Amazon Web Services (AWS) or Microsoft Azure which are SOC 1/SOC 2/ISO 27001 certified. All datacenters holding customer files are (SOC 1)/SOC 2 audited and ISO 27001 certified. Stored files are protected using AES 256-bit encryption in addition to unique per-file keys.

Files are stored in replication with leading providers such as AWS and Azure that ensure high file durability and are backed up according to customer configurable file retention and versioning settings.

How secure are the links I create to share my files?

Each link you send is unique. Links to files are randomly generated using strong hash-based message authentication codes and other countermeasures that protect links from guessing attacks.

ShareFile also offers various configurable settings and permissions that allow you to restrict access to files and folders. Any file you share with ShareFile can be password protected. Additionally, you have the option to limit the number of times a file may be downloaded, or you can set an expiration date for any link you send.

What kind of encryption does ShareFile use?

ShareFile employs TLS protocols with up to 256-bit encryption to protect client authentication, authorization and file transfers (data in transit).

To protect files at rest, ShareFile stores client files using AES 256-bit encryption in addition to unique per-file keys.

Who holds the encryption keys for ShareFile? Can I hold the encryption keys?

Your files and their content are protected at rest using an AES 256-bit encryption key and randomly generated per-file keys. ShareFile manages your encryption keys and maintains a key management policy and supporting procedures. Customers interested in generating and managing their own encryption keys may choose to store and encrypt their files on premises using Citrix StorageZone Controllers.

Additionally, Citrix Managed Storage Zones also support Amazon Web Services Key Management Services (AWS KMS).

ShareFile storage zones gives your company's IT department the flexibility to choose between Citrix-managed, secure cloud storage or IT-managed storage zones (on-premises) to store data within your own data center. Enterprise customers can create and manage on-premises storage zones as part of a ShareFile enterprise account.

What options does ShareFile offer to secure files in ShareFile mobile apps?

ShareFile employs similar security protocols for file access from a mobile device as those used when files are accessed via the web application.

Configurable controls allow you to further protect your data using your mobile device. You can manage permissions and access rights to ShareFile files and folders from a mobile device. You can require a PIN or password to access files on a mobile device to strengthen access controls and enable in-app encryption. You can prevent files from being opened using third-party apps. You can disable offline access to files, requiring users to be actively logged in to view files. You can determine the number of days downloaded files remain on a device before they are automatically removed, even if offline. You can even remotely wipe ShareFile data from a lost or stolen device.

How are my files secured when I send them through email using ShareFile links?

When you replace email attachments with secure ShareFile links to files, you combine the convenience of email with the security of a portal. The document you link to is protected in transit using TLS protocols and with up to 256-bit high-grade encryption.

ShareFile does not encrypt the text of your email message, but you can configure ShareFile to send email notifications, links to files and 'request a file' links via your SMTP (email) server. This allows you to maintain your email system's security features; in addition, your email address will show as the sender and any failed emails will come back to you. Account admins also can configure ShareFile to send messages to a mail server over an SSL encrypted segment, provided the mail server supports SSL connections.

How are my files protected when I use the Citrix Files for Microsoft Outlook?

Citrix Files for outlook for Microsoft Outlook allows you to insert secure links to files, upload and send new files, and request files directly from Microsoft® Outlook email messages. Custom settings let you determine the security and use policies so your data can be delivered safely.

How is ShareFile more secure than solutions?

FTP

FTP is a standard network protocol used to transfer files from one host to another via a network. Because standard FTP is not able to encrypt data traffic, documents are not protected during transfer. Many people choose to switch from FTP to other tools because FTP can be difficult to set up and manage, lacks user control and reporting features, and is not compatible with mobile devices.

ShareFile uses and TLS protocols with up to 256-bit high-grade encryption to protect files during transfer. ShareFile can be accessed using any web browser that can access the Internet and does not require the opening of additional ports or the installation of special software.

Though ShareFile supports FTP to enable backward compatibility with legacy systems, you can optionally connect to ShareFile using FTP over SSL (FTPS connection over port 990), an inherently more secure method than standard FTP. You can connect to ShareFile directly from an FTP/FTPS program, providing a way for users to upload or download files to or from a secure location using existing FTP/FTPS programs.

Password-protected PDFs

Password-protected PDFs do not provide robust security for sensitive data. Even a strong password is susceptible to hackers. Sending the PDF password over email further increases the chance of a security breach.

With ShareFile, you can bypass the hassle of password-protecting a PDF and sending the password over insecure email. ShareFile allows you to send secure links to PDFs and other document types directly from ShareFile or email and lets you track when and by whom the document is downloaded. (Of course, you can also send password protected PDFs using ShareFile if needed.)

Consumer-grade file-sharing tools

There are many file-sharing tools on the market today and deciding which one is right for you can be a challenge. The tool you use to share photos with your family might not be the right tool for sharing business documents or confidential client files with colleagues or customers. Because ShareFile was built specifically for business use, many find it is a good choice for businesses that need to safely send and receive sensitive or confidential documents. Specialized offerings, such as ShareFile Archiving (for entities subject to SEC or other requirements for data retention), the ShareFile Cloud for Healthcare (for entities that process and store Protected Health Information (PHI)), and a large selection of user-managed security settings help businesses address government and industry mandates around data security, privacy, and retention.

What configurable controls does ShareFile offer to enhance security?

ShareFile protects data during transit and while it is at rest on our servers — we call it top-to-bottom security. In addition to the measures we take to protect your data, ShareFile provides you with many options for customizing your security settings. The broad range of user-managed security settings and the granular level of controls we offer are among our most distinctive features (and the very reason so many businesses choose ShareFile).

Configurable controls include:

- Setting password policy, session timeout and account lockout thresholds.
- Setting folder and subfolder permissions to ensure that users only have access to the files or folders you want them to see.
- Tracking account activity with customized email notifications to give a better understanding of how often users access information.
- Enabling file versioning and retention so all versions of a file with the same name will be saved to the account according to the desired retention period.
- Setting multifactor (or strong) authentication that requires a secondary authentication method, such as an SMS verification code, in addition to a username/password combination.

Does ShareFile support HIPAA compliance?

ShareFile supports your HIPAA compliance and will provide and sign a HIPAA Business Associate Agreement upon request. ShareFile has taken steps to comply with relevant aspects of HIPAA and provides customers interested in processing and storing Protected Health Information (PHI) with customer-configurable application security controls designed to satisfy HIPAA requirements.

ShareFile provides you with the tools you need to meet strict security standards, including the encryption and data-protection requirements of the HIPAA Security Rule. Additionally, you can customize ShareFile to your organization's security needs by setting ShareFile to session timeout with periods of inactivity and creating password settings for individuals who access files.

What is the ShareFile Cloud for Healthcare?

The ShareFile Cloud for Healthcare is a securely segmented, multi-tenant, virtual private cloud where only customers who use ShareFile to upload and share protected health information (PHI) have that data processed and stored. This private cloud hosts multiple customers, but it is dedicated for only those customers in industries who process or store PHI, such as healthcare and insurance. (Customers who do not process and store files containing PHI use secure cloud storage that hosts multiple customers in a wide variety of industries.)

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States