ShareFile Security

Providing industry-leading security

Securing data is critical to every enterprise and is a responsibility taken seriously by ShareFile. Savvy IT executives understand that with the plethora of free or low-cost data sharing applications available to end users, it has become critical to provide us-ers with a more secure alternative that still empowers them to sync files across their devices and securely share files with co-workers.

This paper explores the details of how ShareFile is secure by design and highlights the set of security controls available to ShareFile Enterprise customers.

Table of contents

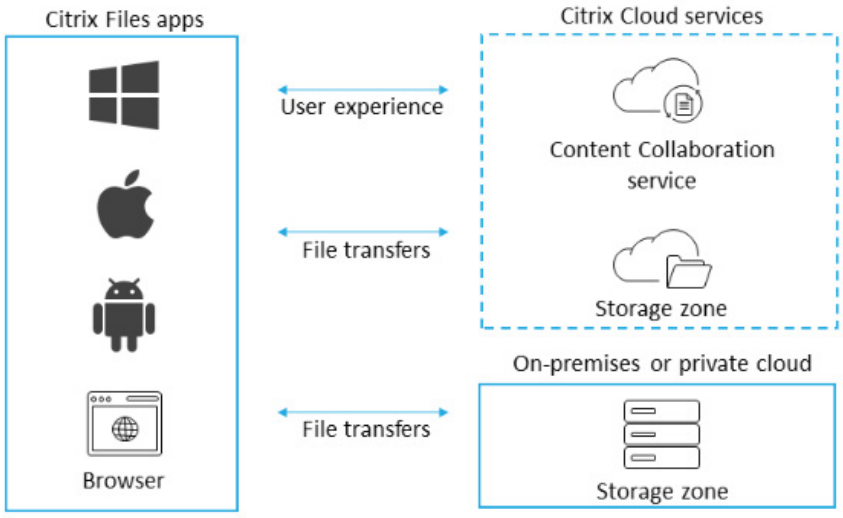
1. Introduction

ShareFile is an enterprise content collaboration platform that enables IT to deliver a robust data sharing and sync service that meets the mobility and collaboration needs of users and the data security requirements of the enterprise.

Securing data is critical to every enterprise and is a responsibility taken seriously by ShareFile. Savvy IT executives understand that with the plethora of free or low-cost data sharing applications available to end users, it has become critical to provide users with a more secure alternative that still empowers them to sync files across their devices and securely share files with co-workers.

This paper explores the details of how ShareFile is secure by design and highlights the set of security controls available to ShareFile Enterprise customers.

Figure 1: High-level architecture of ShareFile service



ShareFile consists of three primary components: the ShareFile management plane, the ShareFile storage zones and the ShareFile apps.

1. **Management plane**: a Citrix-managed component hosting the ShareFile services and business logic, hosted in either the United States or the European Union.

2. **Storage zones**: the location where customer files are stored. Customers have a choice in where to store files, either hosted by Citrix or hosted by the customer in their own datacenter or on their own public cloud service subscriptions. This paper will discuss the workflow and security processes for each of those storage locations.

3. **Apps**: ShareFile offers different native apps for Windows, macOS, Android and iOS, covering different use cases and scenarios to interact with the ShareFile services.

2. ShareFile management plane

Citrix hosts separate ShareFile management planes in the United States (for sharefile.com tenants) and the European Union (for sharefile.eu tenants) to provide the ShareFile services. Both management planes are hosted on Amazon Web Services (AWS), using resiliency within the AWS region by using multiple locations to host the services. For each management plane replication to a secondary region has been implemented, allowing to fail-over to this region when the primary region becomes completely unavailable. This secondary region is also located in the United States (for sharefile.com tenants) and the European Union (for sharefile.eu tenants).

2.1 Architecture

Each of the ShareFile management planes consists of the following components:

- Application Delivery Controllers (ADC)
- Web servers hosting the ShareFile WebUI
- Web servers hosting the ShareFile API services
- Database servers

The ShareFile management planes are operated independently, no customer data is being replicated between the two management planes. The management planes share a single list of all ShareFile tenant subdomain names, where a subdomain name can only be used on either the US hosted or EU hosted management plane.

2.2 Communication to the ShareFile management plane

2.2.1 Secure connections

The ShareFile management planes have been configured to only support TLS 1.x connections with up to 256-bit AES encryption and no less than 128-bit encryption. Connections default to TLS 1.2/AES-256, depending on the device, ShareFile app or browser being used a different cipher suite may be used to secure the connection.

See our Knowledge Base article for details on the ShareFile TLS implementation: https://support.citrix.com/article/CTX236104.

2.2.2 Domain names and IP addresses

The ShareFile service uses different domain names to connect to different microservices within the platform. Apart from the main domain used to connect to the ShareFile tenant (tenant.sharefile.com/.eu), separate domains exist for API connections (tenant.sf-api.com/.eu) or rendering documents inside the browser. A full list of all domain names in use by ShareFile is maintained here: https://support.citrix.com/article/CTX208318.

A list of all IP addresses used by the ShareFile management planes and microservices is maintained here: https://support.citrix.com/article/CTX237213.

2.3 Metadata

Information about the file objects stored inside a ShareFile storage zone, as well as information about the user objects is stored inside the ShareFile management plane. This metadata describes the properties of the objects that are stored.

2.3.1 Metadata for user objects

For user management purposes, as well as to provide detailed information for reporting, the following user attributes are stored for each user in the ShareFile management plane:

- First Name
- Last Name
- User Login (Email Address)
- Company Name (Optional)
- Password Hash
- Security Question
- Security Answer
- Access Control Lists (ACL)

2.3.2 Metadata for file objects

No customer files are processed by, stored in or transferred through the ShareFile management planes. Files are always stored inside a ShareFile storage zone, processed and transferred directly by a ShareFile storage zone controller. Metadata describing the files stored by the ShareFile service is stored inside the management plane. This data allows to identify the stored file objects, the permissions to these objects, as well as the collaboration taking place on these file objects. The following metadata attributes are written to the ShareFile management plane:

- File Name
- File Description
- File Location
- File Size
- File Hash
- File Creation Data
- Email Notification
- Access Control Lists (ACL)
- IP address from which the file was uploaded

2.4 User accounts

The ShareFile service maintains a separate user directory to provide access to ShareFile and set file and folder permissions.

2.4.1 Employees and external users

ShareFile differentiates between Employee and Client (external) users. Employee users are licensed users with access to all the capabilities of the ShareFile service subscribed to and allowed by their tenant account administrators. Client users are limited to the ShareFile web interface and can only access files and folders that are shared with this external user.

Client user accounts are automatically created upon sharing files and folders where authentication is required. The external user will receive an email to activate their ShareFile user account, set a password and then get access to the shared files and folders.

2.4.2 Distribution groups

ShareFile distribution groups are like Active Directory security groups and can be used in folder access control lists (ACLs), as well as to configure user privileges through policies.

2.4.3 User account and distribution group management

User accounts and distribution groups are managed from the ShareFile WebUI. Only ShareFile users with the Manage employees permission can create, modify or delete Employee user accounts. Only ShareFile users with the Manage clients permission can create, modify or delete Client user accounts.

ShareFile user accounts can be created manually, by importing an Excel worksheet or by using the User Management Tool.

Every ShareFile user can create, modify or delete their own distribution groups. ShareFile users with the Share distribution groups permission can create, modify and delete shared distribution groups for all users.

2.4.4 User Management Tool

The ShareFile User Management Tool (UMT) is a lightweight Windows application that runs in the customer environment. It connects to the customer Active Directory to retrieve group, user and Organizational Unit information. For this, the user account connecting to the Active Directory needs query permissions inside the Active Directory.

The administrator configures rules inside the UMT to manage user accounts and distribution groups inside ShareFile based on AD group or OU membership. The UMT rules include user account settings, including authentication method. Disabling or deleting a user account from Active Directory will disable the user account inside ShareFile the next time the UMT rules are executed. UMT rules can be executed either manually or through the Windows Scheduler.

2.4.5 Policy-based administration

Policies can be created to centrally configure user account privileges for ShareFile Employee users. Separate policies are created for administrative privileges, folder settings such as retention policies and storage zone location for the Personal Folder of the user. The storage zone location policy is only applied when creating the user account, the policies for administrative privileges and folder settings are applied upon user account creation and reapplied when the policy is modified.

Policies are configured in the ShareFile WebUI and the deployed to user accounts through User Management Tool rules for managing user accounts.

2.5 Authentication to ShareFile

By default, authentication occurs by providing a username and password (stored inside the ShareFile management plane), but this can be configured to leverage a SAML identity provider to authenticate with enterprise credentials.

2.5.1 ShareFile credentials

Authentication to ShareFile can be done by providing the username (the email address of the user) and a password. The password is stored hashed and salted as part of the user metadata.

2.5.1.1 Password requirements policy

The tenant administrator can configure the requirements for the password that the users set on their account. The following settings can be configured:

- Minimum password length (default: 8, must be minimum of 8 characters)
- Minimum number of numbers (default: 1, must be minimum of 1 number)
- Minimum number of special characters (default: 0, no minimum requirement)
- Password expiry
- Password history

The ShareFile password can be at most 50 characters long.

2.5.1.2 Two-step verification

Two-step verification can be enabled to add a second step for users authenticating with ShareFile credentials. The verification takes place through a verification code that's being sent to the user via text message (SMS) or voice call or through a time-based one-time passcode (TOTP) authenticator app.

After enabling this functionality on the account, the administrator can make two-step verification required for all users (Employee and/or Client users). Making the verification mandatory will require the user to provide their phone number at user registration or the next logon and enter the received token. After enabling the verification, the user can then add a TOTP authenticator app to use for verification. Each Employee or Client user can choose to enable the verification on their user account when it's not enforced by the administrator.

2.5.1.3 Password reset

There are three ways for the password to be reset.

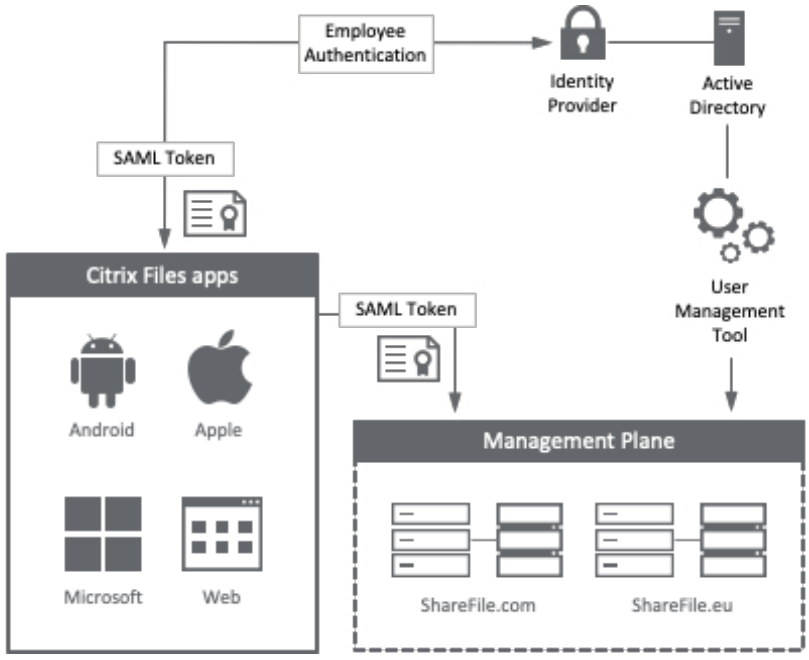
- The user can initiate a password reset. An email will be sent to the user with a link to reset the password. This link is valid for 15 minutes.
- A tenant administrator can set a new password for the user.
- Citrix Support employees cannot change the password for the user. A Support employee can trigger the password reset for the user, similar to the self-service password reset. The user will receive an email with a link to reset the password. This link is valid for 15 minutes.

2.5.2 Authentication with enterprise credentials

ShareFile leverages Security Assertion Markup Language (SAML) identity providers to authenticate users with their enterprise credentials. SAML is a standard for exchanging authentication and authorization data between different security domains, e.g. a SaaS service like ShareFile and a customer Active Directory. SAML is an XML-based protocol that uses security tokens to pass information about a principal (usually the user) between the SAML authority (the identity provider) and a SAML consumer (the service provider).

ShareFile supports Single Sign-On via SAML 2.0 and integrates with a number of identity management solutions. To connect the enterprise credentials to the ShareFile Employee user account, ShareFile uses the NameID property inside the SAML assertion which must include the email address of the user. See this KB article for supported identity providers and step-by-step guides for configuration details: https://support.citrix.com/article/CTX208557.

Figure 2: Integration with corporate identity



2.5.2.1 SAML authentication flow for ShareFile

1. ShareFile app requests the SAML logon page.

2. ShareFile app discovers SAML identity provider.

3. ShareFile app is redirected via an HTTPS 302 redirect to the URL of the identity provider. A SAML request is included in this message.

4. ShareFile app connects to SAML identity provider.

5. The Identity provider requests the user to authenticate and redirects ShareFile app to Assertion Consumer Service. A SAML response is included in this message.

6. ShareFile app posts SAML response to Assertion Consumer Service.

7. Assertion Consumer Service validates the SAML response and authenticates the user to ShareFile upon successful validation. A session cookie is set and a long-term OAuth token is provided.

8. Access to the ShareFile service is granted. The user defaults to the dashboard on the ShareFile WebUI or the folder structure is displayed in a native ShareFile app.

2.5.2.2 Access and OAuth token

After completing the SAML authentication flow, all ShareFile apps store an access and an OAuth token for authentication purposes to enhance the user experience. The access token has a lifetime duration of 8 hours, which cannot be modified. The duration of the lifetime for the long-term OAuth token can be configured by the tenant administrator.

When the ShareFile app has an unexpired OAuth token, the SAML authentication flow is not executed. Instead it directly provides the OAuth token to the ShareFile Assertion Consumer Service for validation. Upon successful validation, the session cookie is set and the user is presented with the ShareFile interface.

2.5.2.3 Multi-factor authentication

Multi-factor authentication to ShareFile is supported through the configured SAML identity provider. Refer to the vendor of your identity provider for supported multi-factor solutions for their platform.

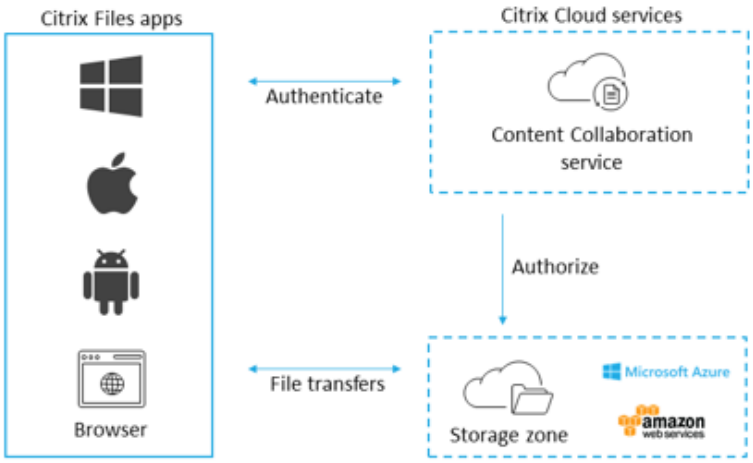
Certificate-based authentication is supported on mobile devices only for devices managed by the Citrix Endpoint Management service. This is due to limitations imposed by the operating system and the certificate being stored inside the Citrix Secure Hub container on the Android or iOS device.

3. Citrix-managed storage zones

3.1 Overview

Citrix operates a hybrid cloud infrastructure, with separate application and storage tiers managed by separate entities. Citrix uses Amazon Web Services to host the ShareFile management plane. The storage zone(s) to store the file objects are hosted on Microsoft Azure or Amazon Web Services, depending on the customer contract and the availability of those cloud providers within the customer region. Inside the storage zone additional microservices are being run, to provide anti-virus scanning, file indexing and creating backups.

Figure 4: High-Level architecture for Citrix-managed storage zones



3.2 Security

3.2.1 Secure connections

The Citrix-managed storage zones have been configured to only support TLS 1.x connections with up to 256-bit AES encryption and no less than 128-bit encryption. Connections default to TLS 1.2/AES-256, depending on the device, ShareFile app or browser being used a different cipher suite may be used to secure the connection.

See our Knowledge Base article for details on the ShareFile TLS implementation: https://support.citrix.com/article/CTX236104.

3.2.2 Domain names and IP addresses

Citrix-managed storage zones are hosted on either Microsoft Azure or Amazon Web Services cloud services.

3.2.3 Hash-based message authentication codes

When a user wants to upload or download a file, the ShareFile architecture prevents forged requests by using hash-based message authentication codes (HMAC) to validate that the request is initiated by an authenticated session to the ShareFile management plane. The shared key between management plane and storage zone is being used to create and validate the HMAC codes by both the management plane and the storage zone controller.

3.3 ShareFile Data repositories

3.3.1 File transfers

All file transfers use direct connections between a Citrix-managed storage zone and the Citrix Files apps.

3.3.2 File download flow

1. Citrix Files app requests to download a file.

2. A prepare message is sent by the ShareFile management plane to the storage zone hosting the file.

3. A download token, which is based on the file ID, is generated at the management plane and sent to the storage zone controller. The random-string token is stored in persistent storage inside the storage zone. For high availability configuration, this download token is available to all storage zone controllers hosting the storage zone.

4. The storage zone controller acknowledges and validates the download token based on the Shared Key. The storage zone controller signs the URL with its copy of the zone secret and confirms the HMAC from the management plane matches its own calculated HMAC.

5. The ShareFile management plane provides the download link containing the Fully Qualified Domain Name (FQDN) of the storage zone to the ShareFile app with the unique download token.

6. To start the file download, the Citrix Files app connects directly to the storage zone.

7. The download token is validated by the storage zone controller.

8. Upon successful validation, the storage zone controller retrieves the file from storage and sends the file to the Citrix Files app. After the file transfer has been completed successfully, the storage zone controller expires the download token.

3.3.3 File upload flow

1. Citrix Files app requests to upload a file.

2. A prepare message is sent by the ShareFile management plane to the storage zone that will receive the file.

3. An upload ID is generated at the management plane and sent to the storage zone controller.

4. The storage zone controller acknowledges and validates the HMAC based on the Shared Key. The storage zone controller signs the URL with its copy of the zone secret and confirms the HMAC from the management plane matches its own calculated HMAC.

5. The ShareFile management plane provides the upload link containing the Fully Qualified Domain Name (FQDN) of the storage zone to the Citrix Files app with the unique upload ID.

6. To start the file upload, the Citrix Files app connects directly to the storage zone.

7. The upload ID is validated by the storage zone controller.

8. Upon successful validation, the file transfer is started by the ShareFile app. The Citrix Files app also sends an MD5 hash to validate that the file has been uploaded correctly.

9. Once the file has been successfully uploaded, the storage zone controller sends the file object information to the ShareFile management plane.

3.3.4 Encryption at rest

All tenant files are encrypted using AES 256-bit symmetric key encryption. Per-file encryption keys are randomly generated and stored as part of the file metadata.

3.3.5 Encryption at rest with customer-managed encryption keys

ShareFile provides the flexibility to encrypt files stored inside a Citrix-managed storage zone with an encryption key stored inside the Amazon Key Management Service (KMS). This provides customers with the data security control they require or desire, while maintaining to benefit from the flexibility and functionality that storing files inside a Citrix-managed storage zone provides.

The encryption of the file is dependent on ShareFile having access to the KMS Master Key inside the customer KMS account. At any point the customer can revoke access to this KMS Master Key for the ShareFile service. Once access has been revoked, all encrypted files stored by ShareFile tied to this KMS Master Key are inaccessible.

3.3.5.1 Upload flow to Citrix-managed storage zone

1. Customer initiates a request to upload a file to their Citrix-managed storage zone.

2. ShareFile initiates a conversation with Amazon KMS associated with the customer KMS account, requesting a data key that can be used to encrypt the file.

3. Amazon KMS generates the plain text data key and the encrypted copy, returning both to ShareFile.

4. ShareFile encrypts the customer file using the plain text key and discards the plain text key after encrypting the file. The encrypted customer file is stored inside the Citrix-managed storage zone.

5. ShareFile stores the encrypted copy of the data key inside the Citrix-managed storage zone.

3.3.5.2 Download flow from Citrix-managed storage zone

1. Client initiates a download of a file secured with a KMS encryption key. ShareFile retrieves the encrypted file.

2. ShareFile retrieves the stored encrypted data key.

3. ShareFile initiates a conversation with Amazon KMS and sends the encrypted data key to Amazon KMS.

4. Amazon KMS locates the master key associated with the customer KMS account, decrypts the data key and returns the plain text data key back to ShareFile.

5. ShareFile now decrypts the file using the plain text copy of the key. The plain text copy of the key is discarded, and the requested file is returned to the client initiating the download request.

3.3.6 Data availability

Every Citrix-managed storage zone leverages data replication within the same availability zone of Amazon Web Services or Microsoft Azure. All files are written to at least three separate zones, making sure files remain available even when the availability zone becomes unavailable due to local events like fires or floods.

3.3.7 Data backup

ShareFile maintains a slow deletion principle where files deleted by a user are stored inside the Recycle Bin. Files stay inside the recycle bin for a brief period of time, during which both the user and administrator can restore the file. More details are available here: https://support.citrix.com/article/CTX208300.

3.3.8 Anti-virus

ShareFile deploys dedicated anti-virus servers that scan all uploaded tenant files for viruses and malware. The result of the scan is added to the file metadata. Based on the anti-virus policy configured for the account, access to infected and/or unscanned files may be blocked for users.

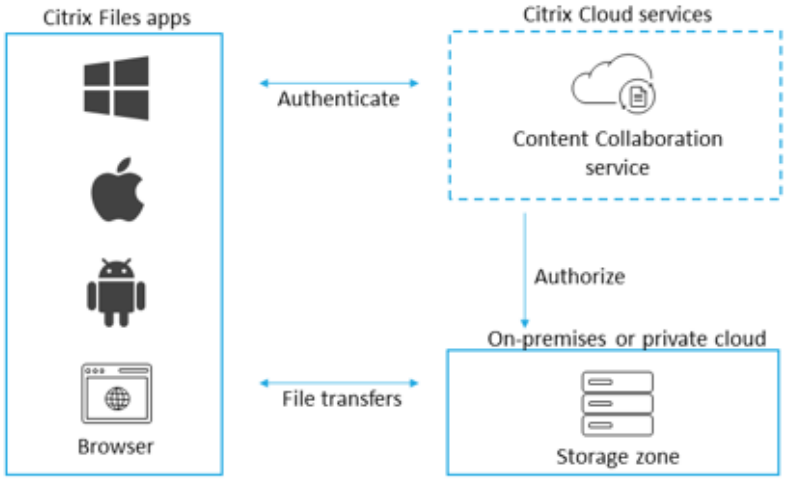
4. Customer-managed storage zones

4.1 Overview

Customer-managed storage zones allow IT administrators to choose where corporate data will be processed and stored. IT can store data in the organization's datacenter to help meet unique data sovereignty and compliance requirements, or an organization can choose to host ShareFile data natively in a public cloud storage location, helping IT build the most cost-effective and customized solution for their organization.

A customer-managed storage zone hosts a ShareFile Data repository, stored on a network share or inside a private cloud storage subscription (supported on Microsoft Azure, Amazon Web Services or Google Cloud). Additionally, it can host storage zone connectors to on-premises file shares, SharePoint Server 2010 or newer, as well as ECM Documentum repositories.

Figure 4: High-Level architecture for customer-managed storage zones



4.2 Security

4.2.1 Secure connections

The inbound connection to the storage zone controllers is determined by the cipher suite that has been configured by the customer. All ShareFile apps support up to TLS 1.2 connections with AES 256-bit encryption keys to communicate with a storage zone controller.

4.2.2 Shared Key between management plane and storage zone

Upon configuration of the storage zone, a unique shared key is established between the ShareFile management plane and the storage zone. This shared key is stored as part of the storage zone configuration and is shared between all storage zone controllers hosting the storage zone. Access to the shared key is secured with a passphrase, specified by the administrator upon configuring the first storage zone controller.

4.2.3 Hash-based message authentication codes

When a user wants to upload or download a file, the ShareFile architecture prevents forged requests by using hash-based message authentication codes (HMAC) to validate that the request is initiated by an authenticated session to the ShareFile management plane. The shared key between management plane and storage zone is being used to create and validate the HMAC codes by both the management plane and the storage zone controller.

4.3 ShareFile Data repositories

4.3.1 File transfers

All file transfers use direct connections between a customer-managed storage zone and the Citrix Files apps.

4.3.2 File download flow

1. Citrix Files app requests to download a file.

2. A prepare message is sent by the ShareFile management plane to the storage zone hosting the file.

3. A download token, which is based on the file ID, is generated at the management plane and sent to the storage zone controller. The random-string token is stored in persistent storage inside the storage zone. For high availability configuration, this download token is available to all storage zone controllers hosting the storage zone.

4. The storage zone controller acknowledges and validates the download token based on the Shared Key. The storage zone controller signs the URL with its copy of the zone secret and confirms the HMAC from the management plane matches its own calculated HMAC.

5. The ShareFile management plane provides the download link containing the Fully Qualified Domain Name (FQDN) of the storage zone to the Citrix Files app with the unique download token.

6. To start the file download, the Citrix Files app connects directly to the storage zone.

7. The download token is validated by the storage zone controller.

8. Upon successful validation, the storage zone controller retrieves the file from storage and sends the file to the Citrix Files app. After the file transfer has been completed successfully, the storage zone controller expires the download token.

4.3.3 File upload flow

1. Citrix Files app requests to upload a file.

2. A prepare message is sent by the ShareFile management plane to the storage zone that will receive the file.

3. An upload ID is generated at the management plane and sent to the storage zone controller.

4. The storage zone controller acknowledges and validates the HMAC based on the Shared Key. The storage zone controller signs the URL with its copy of the zone secret and confirms the HMAC from the management plane matches its own calculated HMAC.

5. The ShareFile management plane provides the upload link containing the Fully Qualified Domain Name (FQDN) of the storage zone to the ShareFile app with the unique upload ID.

6. To start the file upload, the Citrix Files app connects directly to the storage zone.

7. The upload ID is validated by the storage zone controller.

8. Upon successful validation, the file transfer is started by the Citrix Files app. The Citrix Files app also sends an MD5 hash to validate that the file has been uploaded correctly.

9. Once the file has been successfully uploaded, the storage zone controller sends the file object information to the ShareFile management plane.

4.3.4 Encryption at rest

The storage zone controller has the ability to encrypt the files before storing these in the persistent storage location of the storage zone. Files are encrypted using an AES 256-bit encryption key that's being generated during the initial configuration of the storage zone and stored in the SCKeys.txt file inside the storage zone. It's therefore essential to create a backup of the SCKeys.txt file and passphrase, as loss of both will make it impossible to decrypt files stored inside the storage zone.

Alternatively, the ShareFile storage zone can be hosted on a storage solution that supports native encryption of the storage volume.

4.3.5 Data backup

All files stored inside a customer-managed ShareFile repository can be part of the backup solution in place by the customer. All file objects are stored inside the repository are stored inside the \persistentstorage folder. It's recommended to also make backups of the registry of the primary storage zone controller and the SCKeys.txt file stored inside the ShareFile repository.

As the file objects are separated from the file metadata inside the ShareFile management plane, to restore file objects to the ShareFile repository are initiated from the ShareFile management plane. File metadata remains available for three years after the file has been deleted. The file restoration process leverages a PowerShell script to match the file metadata to the correct file object to be retrieved from backup. After restoring the file object from backup, a second PowerShell script is used to attach the file object to the file metadata again.

Details on backup and restore for ShareFile repositories can be found here: https://docs.citrix.com/en-us/storagezones-controller/5-0/manage-storagezone-controllers/file-recovery.html.

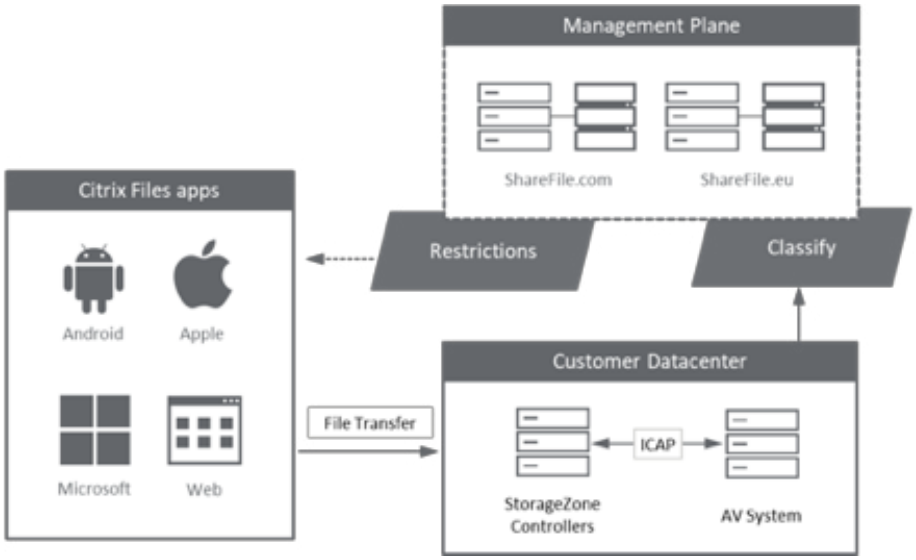
4.3.6 Integration with anti-virus solutions

A customer-managed storage zone can be integrated with an anti-virus solution in place by the customer to scan all uploaded tenant files for viruses and malware. The result of the scan is added to the file metadata. Based on the anti-virus policy configured for the account, access to infected and/or unscanned files may be blocked for users.

The integration between the storage zone and the anti-virus solution can be configured in two ways. The first integration is to scan files by using a command-line anti-virus engine, that returns the result of the scan. Files that are scanned by using the command-line integration are retrieved directly by the anti-virus solution and as a result cannot be encrypted at rest by the storage zone controller.

The second integration is by using an anti-virus solution that leverages ICAP to receive the files and return the scan results. All uploaded files are being added to the AV Scan Queue on the storage zone controller with an unscanned flag added to the file metadata in the management plane. Once the anti-virus solution is ready to receive the files, the storage zone controller retrieves the file from storage and sends them over ICAP to the anti-virus solution. Files that have been encrypted by the storage zone controller are decrypted first before being sent to the anti-virus solution. The anti-virus solution returns a file clean or file infected status, which is being added by the storage zone controller to the file metadata replacing the unscanned flag.

Figure 5: Anti-virus scanning with an ICAP-based solution

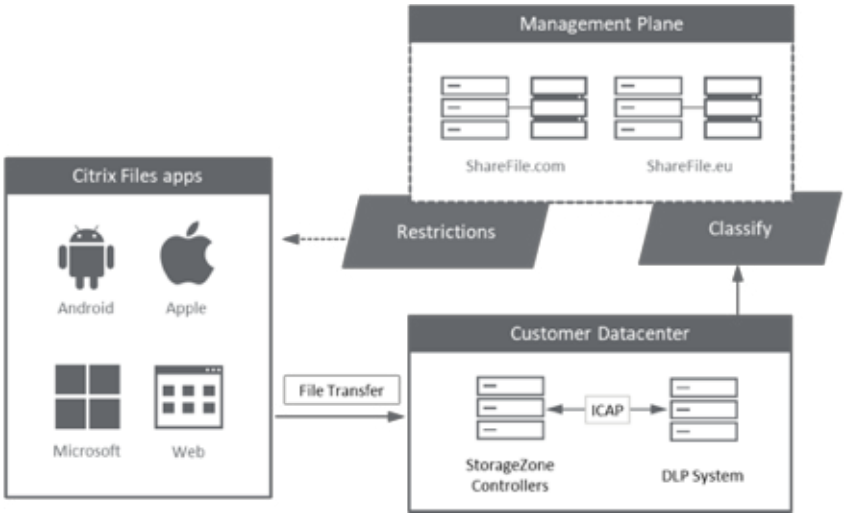


More details on the configuration of the anti-virus integration can be found here: https://docs.citrix.com/en-us/storagezones-controller/5-0/manage-storagezone-controllers/antivirus-scans.html.

4.3.7 Integration with Data Loss Prevention (DLP) solutions

ShareFile integrates with several market-leading Data Loss Prevention (DLP) products enabling content-aware sharing restrictions. Files stored inside a customer-managed storage zone can be examined by any third-party DLP security suite that supports ICAP, a standard network protocol for inline content scanning. Sharing and access privileges can then be adjusted based on the results of the DLP scan and your preferences for how strictly you want to control access.

Figure 6: Data Loss Prevention scanning with an ICAP-based solution



Tying ShareFile security policies to your existing DLP security suite means you can maintain a single point of policy management for data inspection and security alerts. The DLP ICAP integration works with any DLP solutions that supports the ICAP protocol for scanning outgoing e-mail attachments or web traffic, you can point the ShareFile storage zone controllers to the same server. Per customer-managed storage zone a single DLP server URL can be configured.

All uploaded files are being added to the DLP Scan Queue on the storage zone controller with an unscanned flag added to the file metadata in the management plane. Once the DLP sever is ready to receive the files, the storage zone controller retrieves the file from storage and sends them over ICAP to the DLP sever. Files that have been encrypted by the storage zone controller are decrypted first before being sent to the DLP server. The DLP server returns a file OK or file blocked status, which is being added by the storage zone controller to the file metadata replacing the unscanned flag.

Based on the data classification returned by the DLP server, the ShareFile platform will impose configured policies for downloading files from or sharing files through the ShareFile platform. Separate policies can be configured for files flagged Scanned:OK, Scanned:Blocked and Unscanned, each of them having separate policies for Employee or Client users.

More details on the configuration of the DLP integration can be found here: https://docs.citrix.com/en-us/storagezones-controller/5-0/data-loss-prevention.html.

5. Storage zone connectors

5.1 Overview

Storage zone connectors allow ShareFile customers to access files stored inside existing on-premises or cloud repositories, such as network file shares or OneDrive for Business document libraries, helping organizations to leverage and mobilize those enterprise data platforms. All Citrix Files apps and the web interface can access files from existing repositories through storage zone connectors.

5.2 Storage zone connectors to on-premises repositories

5.2.1 Architecture

Existing on-premises repositories made available with storage zone connectors use a customer-managed storage zone controller to access those repositories. Supported existing repositories are network file servers (SMB), SharePoint Server 2010 to 2016 document libraries and OpenText Documentum.

5.2.2 Authentication

Authentication to storage zone connectors repositories requires the user to authenticate with their Active Directory credentials to the storage zone controller. The storage zone controller will impersonate the Active Directory user when authenticating to the repositories on behalf of the user. All existing permissions to files and folders within the repository will apply when connecting to storage zone connectors. For instance, if a user doesn't have the permission to open files from a certain network share, this user will not be able to open the file through storage zone connectors.

The first point of authentication from Citrix Files apps always leverages Basic authentication. As all Citrix Files apps only connect to the ShareFile management plane and storage zone controllers over HTTPS, no user credentials are ever sent in plain text across the network. The first point of authentication can be the storage zone controller, in most deployments this authentication will take place on an Application Delivery Controller such as the Citrix ADC. See Appendix A for more details on this. After the first point of authentication, the authentication method in place will be used (e.g. NTLM or Kerberos).

5.2.3 Traffic flow for Connectors to on-premises repositories

1. User accesses tenant.sharefile.com to retrieve the list of configured Connectors for the user.

2. Configured Connectors for the user are displayed.

3. User accesses configured Connector and connects to storage zone controller.

4. Storage zone controller requests user to authenticate with Active Directory credentials.

5. Storage zone controller uses impersonation to authenticate with user credentials to Connectors repository. Storage zone controller enumerates files and folders available within the accessed Connector.

6. User interacts with files and folders, the storage zone controller acts as a proxy to download and upload files.

5.3 Storage zone connectors to cloud repositories

5.3.1 Architecture

Existing cloud repositories made available with storage zone connectors use a Citrix-managed storage zone controller to access those repositories. Supported cloud repositories are Office 365 (OneDrive for Business and SharePoint Online) and personal cloud storage services from Dropbox, Box, Google Drive and Microsoft OneDrive.

5.3.2 Traffic flow for Connectors to cloud repositories

1. User accesses tenant.sharefile.com to retrieve the list of configured Connectors for the user.

2. Configured Connectors for the user are displayed.

3. User accesses configured Connector and connects to storage zone controller.

4. Storage zone controller requests user to authenticate with credentials for the configured cloud service. The returned authentication token from the cloud service is stored inside a secure database in the Citrix-managed storage zone for future authentication requests.

5. Storage zone controller uses authentication token to authenticate with cloud service. Storage zone controller enumerates files and folders available within the accessed Connector.

6. User interacts with files and folders, the storage zone controller acts as a proxy to upload files, file downloads use direct links to the files stored inside the cloud repository.

6. Secure collaboration

Collaboration with other people on files and folders is increasing. And in the majority of these activities, the collaboration takes place with people who are not sitting at a desk nearby. Making sure that our employees can collaborate in a secure fashion is thus very important. In this chapter, the methods of collaboration and the security practices in place are discussed in further detail.

6.1 Sharing files and folders

When sharing files and folders with others, both sending and requesting files and folders, the initiator of this sharing activity can control how this sharing takes place.

6.1.1 View-only or download permission

When sharing files or folders, the initiator can specify whether the recipient can download the shared files or is limited to viewing the files from inside the browser. See the paragraphs on file previews inside the browser below for implementation details on view-only sharing.

6.1.2 Share access expiration

When sending or requesting files, the initiator can configure how long the link will remain available. A pre-configured list of duration times is available to select from. The default value is 180 days. After this duration has expired, the link is no longer valid and recipients will not be able to access the resources behind the link.

6.1.3 Downloads per user

When sending files or folders, the sender can configure how many times the recipient can download the shared files or folders. The pre-configured list contains values from 1 to 10, plus unlimited. The default value is unlimited.

6.1.4 Sharing files with unspecified recipients

A link that can be accessed by anyone can be created by the initiator of the sharing action. The initiator can require the recipient to provide first name, last name, email address and company name upon accessing the resources behind the link, or choose to allow downloads without requiring any additional information.

6.1.5 Sharing files with specified recipients requiring authentication

Sharing files with authentication will only allow the recipients specified by the initiator of the sharing activity to access the resources behind the link. Upon creating the link, a Client user is created by the ShareFile platform (if none exists for the recipient) and the recipient is first required to activate their Client user account. After activating the user account, the recipient can log on to the ShareFile platform to access the shared resources.

Authenticated links that are forwarded beyond the original recipient or recipients, will not be accessible by those new recipients. The email addresses of the original recipients are tied to the link inside the ShareFile platform, preventing unwanted access to the resources.

6.1.6 Enforcing authentication for sending and requesting files and folders

A back-end setting can be configured by Citrix Support to enforce authentication on all sharing activities. After enabling this setting, the user will not be able to share files and folders without authentication enabled, removing the option to generate links outside the Email with Citrix Files option.

6.1.7 Revoking access to share links

The sender of sharing links can revoke access to the links before the access has expired (if configured) or for sharing links that never expire. From the Inbox on the web interface the user can select the links and click expire. Access to the sharing links is immediately revoked.

6.1.8 Sharing files from storage zone connectors

When sharing files from a storage zone connectors repository, the recipient may not have permissions to access the repository where the file is located. An external recipient will not have the credentials to access the repository, an internal recipient may not have the permission to access the folder or document library where the file is located. To allow sharing of those files, ShareFile copies the file to the FileBox of the user and then shares the file through the ShareFile platform.

The ShareFile platform will regard the first step as a normal upload to the platform, meaning that configured DLP and/or anti-virus scanning integrations will be triggered. Any sharing restrictions configured for the outcomes of the configured scanning activity will be honored. For instance, if a DLP policy has been created to prevent sharing of files containing Social Security Numbers and the file shared from a storage zone connectors repository contains such information, the ShareFile platform will prevent the sharing of that file.

6.1.8.1 Sharing with direct links for on-premises Connectors

For those environments where files on on-premises storage zone connectors are only shared with recipients that have access to the original location of the file, the administrator can configure the storage zone controller to create direct links to the shared files. As a result, the recipient will receive a link pointing directly to the configured resource, e.g. \\File Server\Share\Filename.ext. Details on the configuration for direct links on sharing can be found here: https://docs.citrix.com/en-us/storagezones-controller/5-0/create-and-manage-connectors.html#get-a-direct-link-from-network-share--sharepoint-connectors.

6.2 Online previews and editing

6.2.1 Previewing files stored in Citrix-managed storage zones

To preview files stored inside a Citrix-managed storage zone, ShareFile leverages a dedicated rendering service, operated by Citrix inside the Citrix-managed storage zones. For Office documents, ShareFile hosts its own Office Online Server infrastructure in each storage zone location to render the files. After viewing the file, the cached copy of the file is removed from the servers.

When enabling editing for Office documents, the file preview of Office documents is rendered by Microsoft Office 365 web services. A copy of the file is transferred to the Microsoft servers for rendering, the cached copy of the file is removed by Microsoft after closing the preview.

6.2.2 Editing files stored in Citrix-managed storage zones

ShareFile leverages Microsoft Office 365 web services to edit files stored inside a Citrix-managed storage zone. Upon opening a file for editing, the user is required to authenticate with their Office 365 credentials. A copy of the file is transferred to the servers hosted and operated by Microsoft. All changes made to the document are automatically stored back into ShareFile. Editing of files is supported for Microsoft Excel, PowerPoint and Word documents, as well as text files.

After closing the file, the temporary copy is cleared by Microsoft from the cache of their servers.

6.2.3 Previewing and editing files stored in customer-managed storage zones

Image files stored inside a customer-managed storage zone can be previewed directly in the browser. The storage zone controller renders the image, leveraging cross-origin resource scripting to display the rendered image inside the ShareFile web interface.

To preview and edit Office documents stored inside a customer-managed storage zone directly in a browser, the customer must deploy their own Office Online Server. The Office Online Server must be able to communicate with tenant.sf-api.com (US hosted tenants) or tenant.sf-api.eu (EU hosted tenants) to download files for rendering and to upload the edited files.

Further details can be found here: https://support.citrix.com/article/CTX208340.

6.3 Information Rights Management

6.3.1 Sharing with watermarks

When sharing files with others, a watermark can be added to the rendered document shown inside the browser or that is being made available for download. Watermarking is supported for Microsoft Word, Excel and PowerPoint, as well as PDF files.

Sharing with watermarks leverages a dedicated rendering service, operated by Citrix inside the Citrix-managed storage zones. Upon rendering the document, the configured watermark is added to the output. The rendering service works for files stored in both Citrix-managed and customer-managed storage zones. The files are uploaded and cached on the servers providing the rendering service. Files are deleted from this cache after 7 days after last being accessed.

Further details on protected sharing with watermarks can be found here: https://support.citrix.com/article/CTX233360.

7 Conclusion

This paper details how ShareFile is secure by design and enumerates security and compliance controls available to ShareFile Enterprise customers.

• Flexible data storage – Organizations can selectively store ShareFile data in Citrix-managed storage zones, which provide highly secure cloud storage without the need for on-premises infrastructure or maintenance; in storage zones managed directly within the customer's own datacenter; or in both. The flexibility helps IT address the organization's unique data sovereignty and compliance requirements while building the most cost effective and customized solution.

• Seamless integration with existing data platforms – Working in conjunction with customer-managed storage zones, storage zone connectors let IT create a secure connection between the ShareFile service and user data stored in existing repositories such as network file shares and SharePoint Server without the need for data migration.

• Enterprise-grade security – ShareFile is an enterprise solution that provides extensive data protection features. Files are encrypted both at rest and in transit. Remote wipe allows secure destruction of all ShareFile-stored data and account information on a device that has been compromised. IT can also remove a device from the list of devices that can access ShareFile accounts, or lock a device to restrict its use for a defined period. A poison pill capability lets IT prescribe data expiration policies for mobile devices.

• Auditing and reporting – IT can track and log all user activity, including both data access and data sharing, to support compliance requirements and provide visibility into data usage. Users and IT can also create custom reports on account usage and access.

ShareFile makes it possible for IT to provide the anywhere, any device data access and collaboration people need while meeting the organization's requirements for security, manageability and compliance. With more than two decades of experience serving enterprise IT, Citrix designed ShareFile as a true enterprise-class solution that eliminates the threat posed by consumer file sharing services while providing the industry's most comprehensive feature set. By making follow-me data a seamless and intuitive part of every user's day, ShareFile enables optimal productivity for todays highly mobile, anywhere, any device workforce.

Appendix A: Citrix Endpoint Management integrations

This section summarizes the ShareFile security controls available for mobile devices. Many controls are provided as a native part of ShareFile. When ShareFile is used in conjunction with the Citrix Endpoint Management solution, more controls become available. The table below indicates which security controls are

Security Control	Description	iOS	Android
Provided by ShareFile			
Disable offline access	Allow or deny download of documents to the mobile device for offline viewing or editing. When enabled, the user must be on the network to view or edit documents.	●	●
Require password	Whether end users can save their password on the device. When disabled, users must authenticate each time the app is launched.	●	●
File self-destruct	Documents downloaded to the device are automatically removed after a fixed amount of time.	●	●
Encrypt files at rest	Device-specific file encryption within the ShareFile app - requires passcode lock setting to be enabled.	●	●
Passcode lock	Prompts user for a ShareFile-specific passcode whenever the ShareFile app is launched.	●	●
Device lock	Prevents user from logging onto the current account with the ShareFile app until the administrator unlocks the device.	●	●
Jail-break detection	Prevent use of the ShareFile app if the device is jail-broken.	●	●
Wipe	Removes all ShareFile account information and data from the device. Status of the wipe operation is communicated to the management plane.	●	●
Wipe status and auditing	Status of the wipe request is communicated to the ShareFile administrator as pending or complete. After wipe completion, any actions performed by the client after the wipe was requested are reported to the administrator.	●	●
Disable external applications	Prevents opening of downloaded ShareFile documents in third- party apps (“open in”).	●	●
Secure sharing	Require recipients of shared files and folders to log on prior to download.	●	●
Session inactivity timeout	Automatically log out inactive users after a configured amount of time.	●	●
Provided by Citrix Endpoint Management			
Constrain clipboard cut and copy	Allow/disallow cut and copy of data from the ShareFile app to be pasted into other applications.	●	●
Constrain clipboard paste	Allow/disallow data from other applications to be pasted into the ShareFile app.	●	
Constrain external access	Allow/disallow only approved external applications to be used for opening ShareFile documents (open in).	●	●
Constrain URL schemes	Filter the URL schemes that are passed into the ShareFile application for handling.	●	●
Block camera	Prevent ShareFile from using the device camera to upload photos or videos taken with the device.	●	●
Block microphone	Prevent ShareFile from using the device microphone to capture and upload videos taken with the device.	●	●
Block screen capture	Prevent a user-initiated screen capture operation while ShareFile is running.	●	●

Security Control	Description	iOS	Android
Provided by Citrix Endpoint Management			
Block email compose	Prevent ShareFile from sending e-mails via the native mail application.	●	
Disable print	Enable or disable printing of ShareFile documents from the mobile device to a network printer.	●	
Require Citrix Secure Hub authentication	The user must have a valid session with Secure Hub in order to use ShareFile. A separate password can be required for offline access.	●	●
Define maximum offline period	Defines the maximum period ShareFile can run offline without a network logon.	●	●
Require regular re-authentication	Challenge an authenticated user to re-authenticate at regular intervals in order to continue using ShareFile.	●	●
Wipe data after security event	Any persistent data maintained by the ShareFile app can be erased, effectively resetting the app to its just installed state, if any of the following events occur: • Loss of app entitlement for the user • App subscription removed • Workspace App account removed • Workspace App uninstalled • Too many app authentication failures • Jail-broken or rooted device detected • Device placed in lock state by administrative action.	●	●
Online access only	The user must log on to Secure Hub in order to use the ShareFile app—no offline access.	●	●
Constrain Wi-Fi networks	Require the device be connected to one of a white list of named Wi-Fi networks in order to launch the app.	●	●
Require internal network	Require the device to be connected to an internal company network (determined by connectivity to an internal beacon).	●	●
Constrain network access	Require the ShareFile app to route all of its traffic through the company network.	●	●
App update grace period	Defines the grace period during which users may use ShareFile after the system has discovered that a ShareFile app update is available. If set to 0, the update must be applied as soon as it becomes available.	●	●
Require device encryption	Locks the ShareFile app if the device does not have encryption configured.	●	●
Require device pattern screen lock	Locks the ShareFile app if the device does not have a pattern screen lock configured		●
Provided by Citrix Endpoint Management - Mobile Device Management			
Application white list / black list	Allow or deny use of the ShareFile app on the device. If the application is installed before a black list policy is applied to the device, the app is removed.	●	●
Application provisioning	Install the ShareFile application automatically when the device is enrolled by Citrix Endpoint Management.	●	●
Application removal	Remove the ShareFile application by administrator action or if the device is un-enrolled from Citrix Endpoint Management by the end user.	●	●

CITRIX®