ShareFile

Contents

What's new in ShareFile documentation

March 11, 2024

A goal of ShareFile is to deliver new features and product updates to ShareFile customers when available.

To you, the customer, this process is transparent. Initial updates are applied to ShareFile internal sites only, and are then applied to customer environments gradually. Delivering updates incrementally in waves helps to ensure product quality and to maximize the availability.

March 8, 2024

ShareFile 24.2.12.0 for Outlook

This release addresses issues that improve overall performance and stability.

For more information, see ShareFile for Outlook.

March 1, 2024

ShareFile secure share and request management

ShareFile admins can manage the defaults for both sharing and requesting files. For more information, see:

- Share Settings
- Request Settings

February 28, 2024

ShareFile 24.2.2

This release addresses issues that improve overall performance including:

ShareFile share and request settings - Admins can set share and request link defaults across all ShareFile applications. For more information, see Secure sharing options.

February 20, 2024

Signatures

This release addresses issues that improve functionality by including the following enhancement:

- **Import fields** - save time by importing fields from previous signature request documets. For more information, see Import fields

ShareFile 24.2.10 for Outlook

February 16, 2024

ShareFile 24.2.10 for Outlook

This release addresses issues that improve overall performance including:

ShareFile share and request settings - Admins can set share and request link defaults across all ShareFile applications. For more information, see Secure sharing options.

For release information regarding fixed issues, see ShareFile for Outlook

February 15, 2024

ShareFile 24.2 for Mac

This release addresses issues that improve functionality by including the following enhancements:

Storage protection - ShareFile for Mac can detect storage overages and block uploads from occurring. For more information, see ShareFile Storage.

ShareFile share and request settings - Admins can set share and request link defaults across all ShareFile applications. For more information, see Secure sharing options.

Supported Language update - ShareFile has updated the supported language list. For more information see Supported languages.

ShareFile API

All public share links accessed through `api.sharefile.com` will require authentication.

For more information, see REST API Quick Start Guide.

February 9, 2024

ShareFile Managing Security Notifications

ShareFile now provides flexible email notifications for Security Alerts. ShareFile now enables Admins to efficiently route security-related email alerts to their organization's internal security team.

For more information, see Manage notifications.

February 6, 2024

Domain inclusion list

ShareFile added `*.harness.io` to the recommened inclusion list of domains.

For more information, see Firewall configuration.

February 5, 2024

Signatures

This release addresses issues that improve functionality by including the following enhancements:

- Use **Saved Signatures** in **Signature Annotations**.
- Align fields when preparing a signature request.
- Add, modify, or remove recipients from the signature requests details page.

> **Note:**
>
> These are only available in ShareFile Signature. For more information, see Signatures.

January 25, 2024

ShareFile for Windows 24.1.26

This release addresses issues that improve overall performance.

For more information, see ShareFile for Windows.

January 9, 2024

Signatures

This ShareFile release provides the bulk send enhancement that allows you to send multiple signers their own copy of a single document.

For more information, see Send in bulk.

December 20, 2023

Signatures

This ShareFile release provides three enhancements that improve the signature flow and abilities when requesting a signature. Select the links below to learn more about these new enhancements.

Revise a signature request - Users can now revise a Signature request that is In-Progress to make any necessary changes.

Using Payment fields - Signature users with **Stripe** integrated can use the new **Payment** field when setting up their signature requests.

Using checkbox groups - Checkbox groups allow you to create optional or required lists of items for the signer to acknowledge when completing a signature request. The flexibility with these checkboxes allow you to customize your signature requests and requirements for different recipients.

December 11, 2023

RightSignature

This release addresses issues that improve overall performance and include the following enhancement:

Signer document download - RightSignature admins can enable or disable the option for recipients to download a document before signing. For more information on using this new option, see Signer document download.

For more product information, see Electronic signature - Fixed issues.

ShareFile

As part of our on going Product improvements, we are in the process of updating our backend systems. This process should be seamless for our customers and new billing functionality might be introduced for your account.

Signatures This release also includes the following enhancement for our ShareFile Signatures users:

ShareFile signature users can now edit a new permission for recipients under Default settings that allow recipients to download a document before signing. For more information regarding this new setting, see Signer permissions.

Saving emails with ShareFile

ShareFile is excited to announce our new product enhancements for ShareFile for Google Workspace and ShareFile for Microsoft Outlook Online. You now have the ability to easily save emails with attachments directly to ShareFile. This enables you to organize, access, and share your email content effortlessly within the same platform you trust for secure file storage.

For more information see:

- Save Outlook Online emails with ShareFile
- Save Google Workspace emails with ShareFile

November 30, 2023

ShareFile Projects (or Engagements) enhancements

Delete and restore Projects (or Engagements) - Deleted projects (or engagements) are easily restored with the latest release.

Restore a deleted document request - Deleted document requests can be restored using the new **Restore** feature.

Delete and restore a file or files in a Project (or Engagement) - Project files can be deleted and restored with the latest release.

November 6, 2023

ShareFile Threat detection alerts and remediation updates

This release includes enhancements to our threat detection and remediation features.

For more information, see ShareFile threat detection alerts.

ShareFile Projects (or Engagements) enhancements

Projects dashboard - updated with the latest ShareFile branding.

Projects search and sort - Users can now search and sort Projects.

Projects user clean-up - Projects are now included in the Delete employee users process and will require reassignment when a Project owner is no longer available.

Document Requests - Project owners can change and add assignees to an active document request list.

Projects status - We now allow filtering based on the Project status of either Open or Closed.

RightSignature enhancement

This release includes an enhancement to RightSignature:

Editing signer name after request is sent - Senders can edit the signer name and email on a signature request.

November 1, 2023

ShareFile for Mac beta release

The beta release of ShareFile for Mac provides the following updates to the application:

- Co-editing a Microsoft Office file
- Add a place - allows ShareFile direct access to your Microsoft Office applications with your Mac.

Download ShareFile for Mac beta release to try these beta features.

For more information, see ShareFile for Mac.

October 31, 2023

ShareFile 23.10 for Mac

We have updated ShareFile for Mac to utilize our new brand in the application. This includes the following updated features:

- Redesigned experience for sharing and requesting files - following the latest secure sharing options implemented in our ShareFile web application, the ShareFile for Mac experience now offer a consistent experience.

- **Editable shares** - ShareFile for Mac now offers the ability to provide editable shares.

For more information, see Share files in ShareFile for Mac.

October 26, 2023

ShareFile managed cloud storage zone is available in the UAE region

A new ShareFile managed cloud storage zone is now available in the UAE region. If you are a customer located in the UAE region, reach out to ShareFile support to get the new storage zone enabled on your account.

For more information including the list of available ShareFile cloud storage zones see, ShareFile managed cloud storage zones.
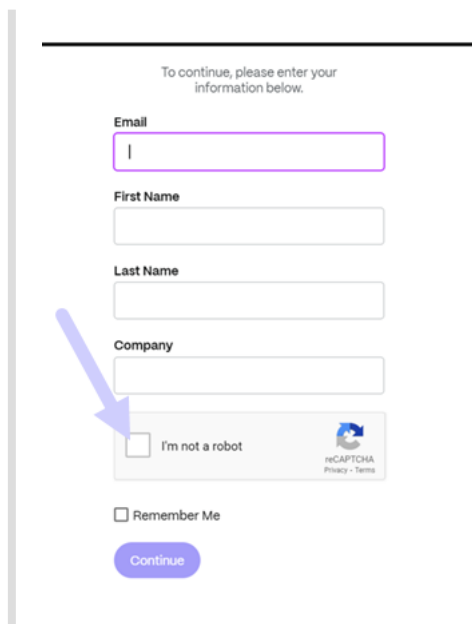
October 23, 2023

New secure sharing options

We are taking steps to improve the security posture of file sharing. From now on all links default to use secure sharing options which will apply across all ShareFile locations: ShareFile desktop app for Mac and Windows, ShareFile Web app, ShareFile Mobile app, ShareFile Plug-in for Microsoft Outlook and Gmail.

- The 'sign in required' option will be selected by default for all shares

- A new alert when you are about to share a link that can be viewed by anyone.

- Admins can require authentication for all share or request links for the account.

> **Note:**
>
> When selecting the "**Anyone (public, must enter a name and email)** option, the recipient is required to complete the **reCAPTCHA** request.

For more information, see our **Learn more** page for New secure sharing options.

October 12, 2023

ShareFile announces a new look and feel to show ShareFile's evolution into a complete solution

We've evolved our solution to go beyond secure document sharing. We're helping our customers embrace digital-first workflows that use automation, native e-signature, and best-in-class security. The efficiencies and cost savings created by these workflows allow our customers to focus on delivering a modern client experience.

At the core of our renewed brand identity is ease. We wanted to capture that feeling of checking off all the boxes from start to finish —without any roadblocks. Our new logo mark, for example, brings this feeling to life by using the iconic check mark, a sign of accomplishment.

From our brand colors to our 3D elements, ShareFile's new look and feel helps us tell the story of smooth processes and the resulting moments of energy and joy that make work meaningful.

To learn more about our evolution, see A modernized brand to take ShareFile into the future of work.

September 26, 2023

New ShareFile storage features

For net-new accounts created after **August 4, 2023**, ShareFile Admins will see a new dashboard for storage consumption on the account in addition to enforcement of storage limits. The following new features are available for net-new accounts.

Storage usage admin dashboard - is a new feature in ShareFile. Storage usage is an admin space that includes a dashboard where admins can view and perform the following:

- View the total storage used by the account through the indicator.
- Review how much storage is consumed out of the allocated storage.
- The date when the storage was updated.
- Get a list of top storage consumers in the account.
- Select and notify the users that are using more storage than needed.

Notifications on the ShareFile UI display the storage consumed by an account and what action must be taken to get the storage within the limit. ShareFile also sends emails to admins when an account reaches 90% and 100% of allocated storage.

Storage enforcement - If an account has consumed 100% of its storage and exceeds the total storage limit, the account actions are blocked, not allowing users of that account to upload files, create documents, add new data, request a file, or duplicate files. However, the users can log in to their account, view, and download.

For more information, see ShareFile storage.

September 25, 2023

ShareFile - Tenant Management

ShareFile allows partners to add new tenant accounts. The new automated provisioning provides more streamlined account management, easy tenant setup, and faster time to market.

For more information, see Tenant Management.

September 19, 2023

ShareFile signature enhancements

This release addresses issues that improve overall performance and include the following features:

Set to date of Signature - Enable this when sending for signature to autofill the date the document is signed. For more information, see Auto-fill date

Date Formats - ShareFile added five additional date format options. For more information on setting the date option in ShareFile, see Time and Date.

ShareFile VDR feature update

ShareFile VDR users can access the following new feature:

Threat detection alerts: Secure client data by getting notified of unusual access to ShareFile account via email.

September 14, 2023

ShareFile for Outlook Online

ShareFile is excited to announce the launch of our **ShareFile for Outlook Online** add-in.

ShareFile for Outlook Online is a feature app available for ShareFile Advanced and Premium customers when using Outlook Online.

To access the ShareFile for Outlook Online add-in, go to Microsoft AppSource. For more information, see ShareFile for Outlook Online.

September 11, 2023

New features now available in the EU control plane

ShareFile Premium subscribers under the EU control plane now have access to several new Premium features. For more information on each of these features, select the feature name:

- **Projects (or Engagements)** - a new collaborative space in ShareFile to organize, digitize, and unify services with clients.

- **Document Requests** our new request list tool that digitizes, organizes, and streamlines document request and collection workflows, such as HR documents for hiring or collecting a list of financial documents.

- **Automated Workflows** - a new workflow builder in ShareFile that can be used to customize workflows based on specific actions and automation triggers.

- **Accelerated Agreements for Client Onboarding** - this ready-to-use workflow streamlines and automates client onboarding agreements, such NDAs, or other signature agreements commonly needed to begin services.

August 31, 2023

Citrix Files for Mobile

ShareFile is happy to announce Microsoft Office 365 co-editing abilities in Citrix Files for iOS and Citrix Files for Android. Advanced and Premium ShareFile users now have the following mobile abilities:

- Live co-editing abilities with multiple users
- View various types of Microsoft Office 365 online files
- Edit Microsoft 365 files online
- View offline files
- Create new Microsoft Office files to share with users

Citrix Files 2380 for Android   For more information on the new co-editing feature with Citrix Files for Android, see Co-editing using your Android device.

Citrix Files 2380 for iOS   For more information on the new co-editing feature with Citrix Files for iOS, see Co-editing using your iOS device.

August 14, 2023

ShareFile new and updated features

Tasks: Now you can easily track the status of tasks related to client matters, including whether they are in progress, completed, overdue, or yet to start. Utilize this new feature within our recently released Projects (or Engagements) functionality.

Threat detection alerts: Secure client data by getting notified of unusual access to ShareFile account via email.

Integrations of prospective client data with Salesforce and QuickBooks.

Projects (or Engagements) has added functionality with the above new Tasks feature.

Accelerated Agreements with auto-fill templates - now with built-in unlimited e-signature, and updated Project Creation to expedite tedious document preparation.

Automated workflows with new **Send an email** action - Personalized welcome emails are effortlessly sent to clients fostering better client relationships and trust, directly from an automated workflow.

ShareFile for Windows

Add a place - ShareFile for Windows users can now connect to native Microsoft applications for a full experience on their desktop tool and automatically save files back to ShareFile while editing or co-editing.

August 7, 2023

ShareFile 2023.8.7 for Mac

We are proud to announce the new ShareFile for Mac application. To download ShareFile for Mac, click here.

The new **ShareFile for Mac** release addresses issues that improve overall performance.

For more information, see ShareFile for Mac.

August 3, 2023

ShareFile Migration Tool v4.4.3.0

Download the latest version of the ShareFile Migration tool here.

See ShareFile Data Migration Tool for more information.

August 2, 2023

ShareFile for Google Workspace

This new ShareFile add-on is seamlessly integrated into your productivity tools and transforms collaboration, simplifies file sharing, and supercharges productivity.

Be notified whenever someone accesses a file or sends you a file so you are always aware of what is going and can take action. You can also set different security and access levels.

For end-user help including accessing and sign in, see User Guidance for ShareFile in Google Workspace

Access the ShareFile add-on by visiting the ShareFile add-on page.

August 1, 2023

ShareFile

ShareFile is happy to announce a major update to our ShareFile Projects (or Engagements) feature:

Delete a project - ShareFile Premium customers now have the ability to delete the projects or engagements they create. For more information, see Delete Projects (or Engagements).

Clients can add other contributors to a project - ShareFile Project (or Engagement) owners can now allow clients on their project to add other contributors from the client's organization. For more information, see Manage project users.

Project owners can add team members - ShareFile Project (or Engagement) owners can add team members from their organization to assist with their project. For more information, see Manage project users.

July 20, 2023

ShareFile for Windows 23.7.10

This release addresses issues that improve overall performance.

For more information, see ShareFile for Windows.

July 11, 2023

ShareFile 23.7.3 for Outlook

This release addresses issues that improve overall performance.

To download the latest release, please see the ShareFile for Outlook downloads page.

For more information, see ShareFile for Outlook

Citrix Files 2370 for iOS

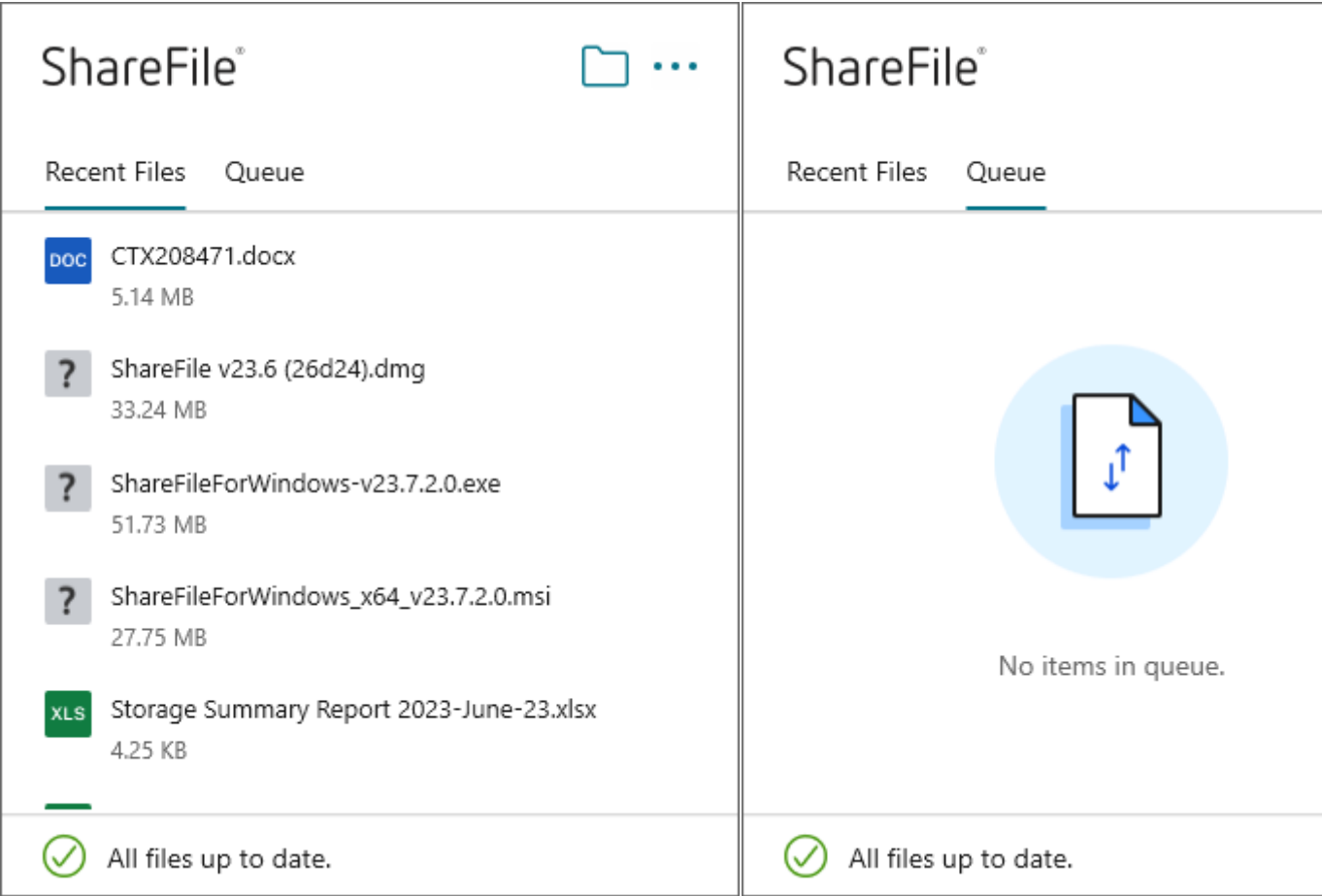This release addresses issues that improve overall performance.

For more information, see Citrix Files for iOS.

July 10, 2023

ShareFile 23.7 for Windows

We are proud to announce the new ShareFile for Windows application. To download ShareFile for Windows, click here.

The new **ShareFile for Windows** release addresses issues that improve overall performance and include the following feature update:

New request files experience - this update offers more options for requesting files including enhanced link creation and definition and access for specific people while using ShareFile for Windows.

For more information, see ShareFile for Windows.

June 26, 2023

Citrix Files 2360 for Android

This release addresses issues that improve overall performance.

For more information, see Citrix Files for Android.

June 20, 2023

Citrix Files 2360 for iOS

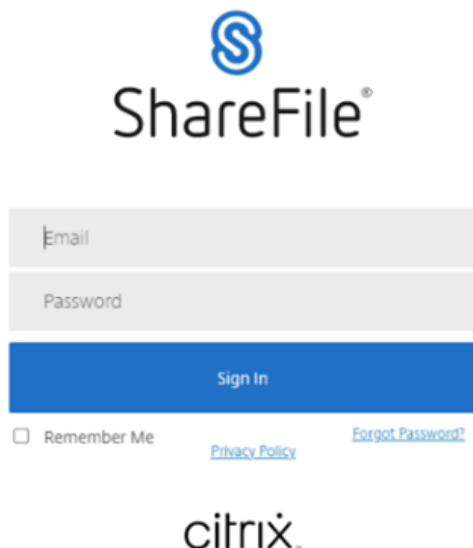This release includes user improvements including an update to version 23.4.0 for MDX SDK.

For more information, see Citrix Files for iOS.
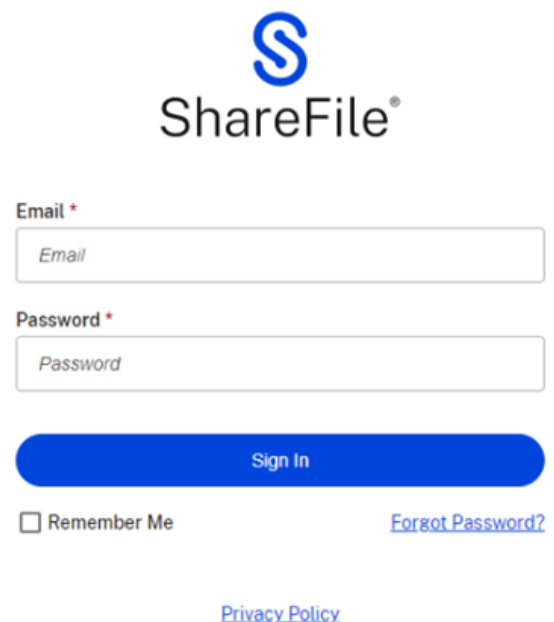
May 23, 2023

ShareFile

ShareFile is happy to announce our redesigned log-in and sign-on screens. We have improved accessibility and security along with a new modernized logo and fresh look and feel. No changes were made to the functionality.

Sign in to your ShareFile account, using your preferred method today, to see our new look.

May 22, 2023

Citrix Files 2355 for iOS

This release addresses issues that improve overall performance and includes the following new update to our sharing capabilities with iOS devices:

Improved sharing capabilities - this update includes more options for sharing, for link creation and definition, and access for specific people.

For more information, see Upload Files.

May 17, 2023

ShareFile announces the inclusion of *.sharefile.io

Add *.sharefile.io for future ShareFile feature releases and improved functionality.

For more information on who this might impact, see Firewall configuration.

May 11, 2023

Storage zones controller 5.11.24

This release includes security updates and fixed issues for ShareFile storage zone controllers.

For more information, see About storage zones controller.

May 4, 2023

ShareFile Virtual Data Room

ShareFile Virtual Data Room now allows customers to easily configure HIPAA compliance and protect sensitive documents that are stored or distributed during confidential transactions.

Also, during account sign up, customers can now select the EU control plane, which enables VDR to be utilized internationally while being EU compliant and following stringent guidelines like GDPR.

For more information, see ShareFile Virtual Data Room.

May 1, 2023

ShareFile

This release addresses issues that improve overall performance and includes the following new features:

Enhanced Accelerated Agreements for Client Onboarding - this update includes added functionalities for current clients and added capabilities for visibility and management of the workflow. For more information, see:

- Accelerated Agreements
- Create auto-fill agreement templates

Automated Workflows beta release - this new feature, for ShareFile Premium users, enables you to easily track and manage the progress of accelerated agreements. For more information, see:

- Automated Workflows

April 19, 2023

Citrix Files 23.4 for Windows

This release addresses issues that improve overall performance and includes the following updates:

Improved sharing capabilities - this update includes more options for sharing, for link creation and definition, and access for specific people.

Citrix Workspace integration is no longer available.

For more information, see Citrix Files for Windows.

April 17, 2023

ShareFile for Outlook

Citrix Files applications are changing their names to ShareFile. In this release, Citrix Files for Outlook is now **ShareFile for Outlook**.

Citrix Workspace integration is no longer available.

For more information, see ShareFile for Outlook

March 29, 2023

Citrix Files 2330 for iOS

This release addresses issues that improve overall performance and includes the following new update to our upload capabilities with iOS devices:

Upload Files - you can now upload files directly from your device to your ShareFile folders.

For more information, see Upload Files.

March 22, 2023

Citrix Files 23.3 for Mac

This release includes native support for **Apple Silicon** and addresses issues that improve overall performance and stability.

For more information, see Citrix Files for Mac.

February 22, 2023

ShareFile

This release addresses issues that improve overall performance and includes the following new update:

Improved sharing capabilities - this update includes more options for sharing, for link creation and definition, and access for specific people.

For more information, see Share files.

February 14, 2023

Citrix Files 2320 for Android

This release addresses issues that improve overall performance.

For more information, see Citrix Files for Android.

February 6, 2023

RightSignature

This release addresses issues that improve overall performance and include the following feature:

Decline to sign - signers can now decline to sign documents received from RightSignature accounts. For more information, see: RightSignature - Decline to sign.

For more product information, see Electronic signature - Fixed issues.

Citrix Files 2320 for XenMobile

This release addresses issues that improve overall performance including better file uploads from your iOS device.

For more information, see Citrix Files for iOS.

January 24, 2023

Citrix Files 2310 for iOS

This release addresses issues that improve overall performance and includes local file uploads from your iOS device.

For more information, see Citrix Files for iOS.

January 12, 2023

ShareFile 01-12-2023

This release addresses issues that improve overall performance and includes the following new feature:

Accelerated Agreements - This new feature for ShareFile Premium users improves their client onboarding process. This feature reduces onboarding cycle time.

For more information, see Accelerated Agreements - Client Onboarding.

Deploy

June 7, 2023

> **NOTE:**
>
> Starting April 30, 2023, Citrix Workspace customers with ShareFile entitlements will no longer have the embedded files experience in Citrix Workspace. Users will access their files solely through their ShareFile.com account after this date. See FAQ: Decouple your ShareFile account from your Citrix Workspace for more information.

**Single sign-on for on-prem connectors**

By enabling SSO for Connectors, Citrix Workspace clients will no longer prompt for authentication when accessing your Network shares or SharePoint folders behind a storage zone controller.
For accounts utilizing storage zones controller version 5.7 and later, and on-premises connectors, you can enable single sign-on for your network file share or SharePoint connectors. After enabling Citrix Content Collaboration for Citrix Workspace, complete the following steps:

1. From the **Service Integrations** screen, select the three dots.
2. Select **Edit** to edit your Citrix Content Collaboration deployment.
3. Check the box for **Use single sign-on credentials for on-prem connectors**.
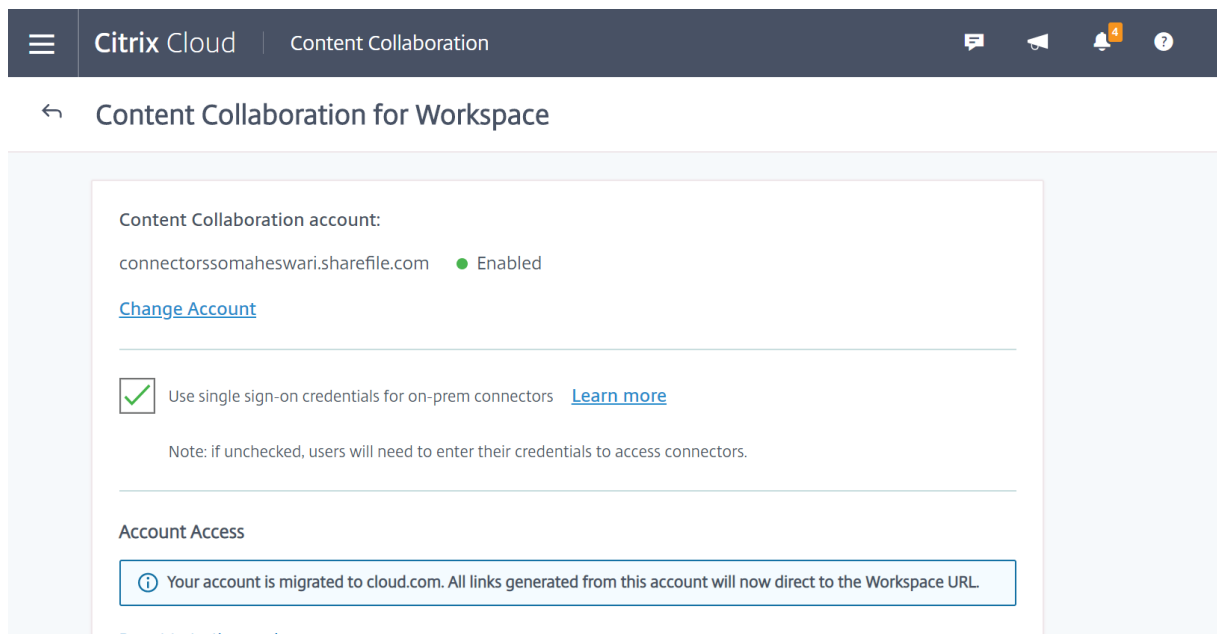
Single sign–on is currently integrated only with Active directory. Single sign-on is not supported with other authentication mechanisms present in Workspace.
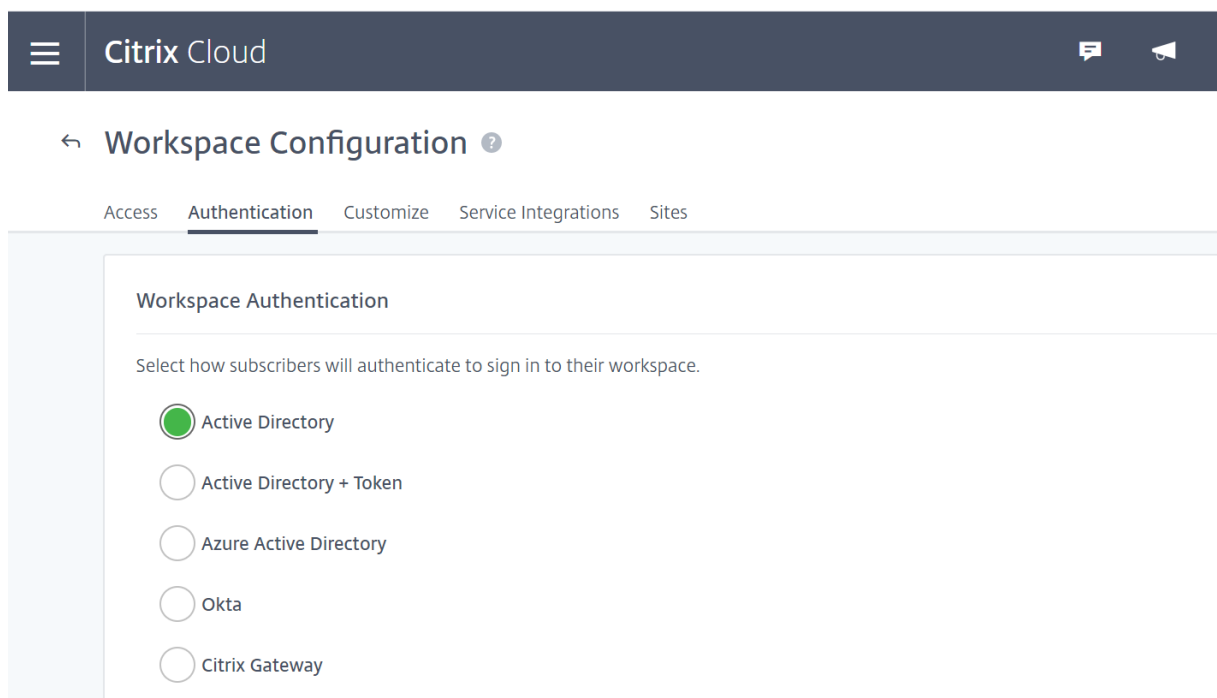
After enabling Citrix Content Collaboration for Citrix Workspace for the first time, the account is in testing mode. Testing mode means that while users are now able to sign in to their workspace and see a Files tab, all new links still generate as sharefile.com links. Once the administrator completes migration to Citrix Workspace for Citrix Content Collaboration, all new links generate as cloud.com links and old sharefile.com links will redirect to the account's respective cloud.com link.

> **Note:**
>
> Single sign-on is not supported when the account is in testing mode. To support single sign-on, the account should be migrated to Citrix Workspace.

To fully migrate accounts to Citrix Workspace, complete the following steps:

1. Go to the hamburger menu and select **Workspace Configuration**.
2. Go to **Service Integrations** and select the three dots.
3. Select **Edit** to edit your Citrix Content Collaboration deployment.
4. Under **Account Access**, select **Migrate account to cloud.com**.

You can also revert to testing mode by following the steps again and selecting **Revert to testing mode**.

When migrating from testing mode, not all features available under a Citrix Content Collaboration license are available in Citrix Workspace.

In order for users to see the Files tab, their employee user email address in Citrix Content Collaboration must match their email address in the company user store (Active Directory or Azure Active Directory). This is done by either manually creating the employee user or by using the User Management Tool.
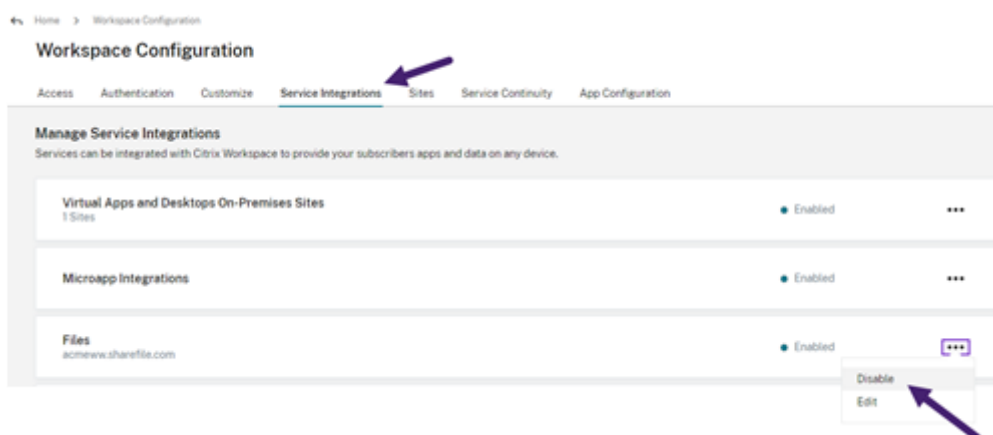
ShareFile

Disable Content Collaboration in Citrix Workspace

In the event you need to disable Citrix Content Collaboration in Citrix Workspace, perform the following steps:

1. Under **Workspace Configuration > Service Integrations > Citrix Content Collaboration**, select the ellipsis.
2. Click **Disable**.

After Citrix Content Collaboration is disabled, all users are expected to access Citrix Content Collaboration via sharefile.com and all new shares use the sharefile.com domain. It can take up to 30 minutes for disablement to fully deploy.

Content Collaboration features not supported in Workspace

When using ShareFile applications, click **Sign in with Citrix Workspace** to sign in with your Citrix Workspace credentials.

Not all features available under a Citrix Content Collaboration license are available in Citrix Workspace. Here is a list of those features:

Features and settings that are not currently supported

- Citrix Virtual Apps and Desktops anonymous apps are not supported when Citrix Content Collaboration (Files) is enabled in a workspace
- ShareFile virtual data room and features that are limited to ShareFile virtual data room accounts such as Folder Q&A
- External (client) user specific two-step verification
- FTP option to access files is not supported in Workspace
- Folder Invites

Feature and settings that are now configured in Citrix Cloud instead of ShareFile

- Existing ShareFile branding - instead, Workspace custom branding is available in Workspace Configuration.
- Secondary ShareFile subdomains - instead, you can customize a single Workspace URL in Workspace Configuration.
- Workspace authentication supports AD, Azure AD, or Okta. SAML and Google Identity are in Tech Preview.

Citrix Files Migration Tool

The Citrix Files Migration Tool allows users to migrate a large amount of data along with folder ownership and permission to Citrix Files from a network share or local file system.

System requirements

- .NET Framework 4.6.2 or later
- Windows 7 or later, Windows 2008 Server or later

Limitations

- This feature is unavailable to client users.
- This application adheres to Microsoft File Path limits. Files that exceed the path limitation are not migrated.
- In the unlikely event that a file transfer causes too much traffic on the Citrix Content Collaboration infrastructure, Citrix Files might pause the transfer. The transfer resumes automatically.
- Files that are currently in use by another program are not migrated.
- This tool does not support migrating more than 50,000 folders.
- You can't use this tool to transfer files to an on-prem restricted storage zone.

- We have not tested this tool on virtual machines, and cannot be fully supported in such an environment.

Best practices

- Because files in use are not uploaded during the migration, we recommend you use the Citrix Files Migration Tool during off hours to minimize interference with your users.
- For best performance, we recommend you use the Citrix Files Migration Tool outside of United States EST business hours.
- Avoid wireless connections when possible.
- The tool has been successfully tested for up to 3 TB of data. If you have more data to migrate, we recommend you break up the data to be at or below 3 TB.

Installation

Download the Citrix Files Migration Tool. Once downloaded, run the installation file to begin setup. If you do not have .NET Framework 4.6.2 or later installed on your machine, it is installed for you. Once installed, a shortcut is added to your desktop and Start menu. For best results, we recommend you install the migration tool on the server or computer where your data resides.

By default, this app installs in *C:\Program Files\Citrix\ShareFile*. If you want to change the install location, click **Options** and specify the location.

Auto update

When you launch the Citrix Files Migration Tool, it checks for updates and prompts you to install when one is available. We recommend you always update to the latest version.

Signing in to the Citrix Files Migration Tool

When launching the Citrix Files Migration Tool, you are prompted to sign into your account. Sign in to the account where you want to upload files.

Once signed in, the account details are encrypted and stored in the app_settings.cfg file, which saves you from signing in every time you launch the app. You can either sign out or delete this file to sign in to a different account. The app_settings.cfg file is located in `USERNAME\AppData\Roaming\Citrix\ShareFile\Migration Tool`. There are also unique files created containing migration details for each unique user signed in.

After signing in, the Home view displays. From the Home view, you can begin a new transfer, view your migration queue, and manage your scheduled migrations, and provide feedback.

Sign in with the master administrator account to transfer data, ownership, and permissions. If the sign-in used is not the master administrator, only data is migrated.

Using the Citrix Files Migration Tool

New Transfer   Select **New Transfer** to initiate a new transfer. The **Choose Transfer Type** window appears.

Choose between **Data only**, **Data + Permissions (Map to Personal Folders)**, or **Data + Permissions (Map to Shared Folders)** for your migration of your data from the original source to Citrix Files. The **New Transfer** window appears.

Use **Select directory to transfer** to browse for a directory to move onto Citrix Files.

When you select **Data only**, **Choose destination** allows you to choose the upload destination folder within your Citrix Files account.

When you select **Data + Permissions (Map to Personal Folders)** or **Data + Permissions (Map to Shared Folders)**, **Configure folder permission options** allows you to transfer folder ownership and access permissions or only folder ownership during migration. You can also create folders for users who have not signed in yet.

Configure transfer options lets you choose a specific time in which to make the transfer, create a folder on the root level and migrate all folders from this transfer inside it, and to enable the option of not uploading files when a newer version of the file exists in the destination folder in Citrix Files.

When using the **Data + Permissions (Map to Personal Folders)**, or **Data + Permissions (Map to Shared Folders)** options, you must sign in to your Active Directory. You can sign in either as the currently signed in user or a different user if desired.

> **Note:**
>
> We recommend you run the Citrix Files Migration Tool on the machine that is connected to the domain from which the user's details are being fetched for ownership and permissions migration.

Once you choose all the options, click **Continue**, and the **Confirm Transfer** window appears.

Confirm Transfer options

- Migration type - Specifies the type of transfer selected by the administrator
- Source - Specifies the location from where the data is being migrated
- Destination - Specifies the location to which the data is being migrated
- Total Number of Files - Number of files being migrated
- Total Files Size - Total size of all the files being migrated

- Expected Time - Approximate time for the migration to complete
- File Types Excluded - Displays a list of file types excluded. Use the **Exclude** link provided to exclude any files from migration.
- Items Unable to Transfer - If there are any files or folders that are unable to be migrated, use the **Review** link to see what they are.

When you click the **Exclude** link, the **Advanced Options: Exclude File Types** window appears. You can choose to manually type in a file type to exclude from migration or choose one of the displayed file types to exclude from migration.

When you click the **Review** link, the **Items Unable to Transfer** window appears. Files and folders are here if the user who signed in does not have the required permissions for migration or if files are currently in use by other applications. Resolve the permissions issue or close any application using the files to proceed with the migration.

When using the **Data + Permissions (Map to Personal Folders)** or **Data + Permissions (Map to Shared Folders)** options and if there are any accounts or groups not present in Citrix Content Collaboration, the **Review missing accounts and groups** link appears. When you click the link, the **List of Accounts and Groups that are not present** window appears. If there are no accounts present in Citrix Content Collaboration for the users listed, those files and folders are not migrated. To avoid this happening, you can quickly create an account for the users and then proceed with migration.

Group permissions are migrated only if groups in Citrix Content Collaboration are created using the User Management Tool. If groups are manually created, then the permissions aren't migrated.

Permission migration files are located in the `USERNAME\AppData\Roaming\Citrix\` `ShareFile\Migration Tool\Permission Data` folder.

Files and folders that remain inaccessible are not migrated. You can continue with the migration of the other files and folders even when there are inaccessible items.

Click **Transfer Files** to start the migration.

Queue

You can use Queue to view transfers that are **Running**, **Pending**, **Cancelled**, or **Complete**.

Running: Clicking **View** on a running job displays the **Transferring…** window. The status of the transfer of files and folders appear. You can pause or cancel the transfer from here.

Pending: Clicking **View** on a pending job displays the **Transfer Pending** window. The details of the pending transfer appear. If the transfer is scheduled, the scheduler details also appear. You can cancel the transfer from here.

Cancelled: Clicking **View** on a canceled job displays the **Transfer Canceled** window. The details of the canceled job appear. You can restart the transfer from here.

Complete: Clicking **View** on a completed job displays the **Transfer Complete** window. The details of the completed transfer appear. Links to logs for failed or canceled uploads can be viewed from here.

Manage Schedules

Manage Schedules allow you to choose when transfers are run. You can use this option to run migrations at times outside of peak usage hours.

Click **Create New Schedule** to make a new schedule. This menu lists created schedules. You can view, edit, or delete the schedules created using the options provided.

> **Note:**
>
> We recommend you handle large data migrations using the scheduler. Schedule transfers outside of peak hours for maximum bandwidth and speed.

Ensure that the correct details are added to the task scheduler. When there are multiple slots selected, multiple instances are added in the task scheduler.

It is required that the user who scheduled the migration be signed in. If the user is not signed in, the migration isn't initiated in that specific time slot.

Transfer pause   In the unlikely event of the transfer causing too much traffic on the Citrix Content Collaboration infrastructure, Citrix Files might pause the transfer. The Citrix Files Migration Tool continuously attempts to resume transfer during this time. A warning message appears at the bottom of the transferring screen. The user can't unpause the transfer manually, but can cancel the transfer.

If the number of retries exceeds 48, contact Citrix Support.

If the user receives the warning message "Your account is currently not available to perform transfers," the pause might still be enabled. The user can either wait for this issue to be resolved or try again later by closing and relaunching the application.

Migration Logs

Once the transfer is complete, you can review the migration details and any errors encountered during the migration process.

Log files generated

- SFMT `[TimeStamp]` `[FolderName]` `.log` - This log contains the complete details of the migration starting from the launch of the Citrix Files Migration Tool.

- Transfer Info `[TimeStamp][FolderName].log` - This log contains verbose information for the transfer.
- Transfer `[TimeStamp][FolderName].log` - This log contains all the files and folders that were successfully transferred.
- Transfer Failure `[TimeStamp][FolderName]`.log - This log contains a brief explanation as to why a file failed to transfer.
- Transfer Canceled `[TimeStamp][FolderName]`.log - This log contains a brief explanation as to why a transfer canceled.

For debugging, the "SFMT `[TimeStamp][FolderName].log` and "Transfer Info `[TimeStamp][FolderName].log` logs are required. Logs are stored at `USERNAME\AppData\Roaming\Citrix\ShareFile\Migration Tool\Logs`

Uninstall the Citrix Files Migration Tool

To uninstall the Citrix Files Migration Tool, use the Programs and Features menu in the Windows Control Panel, or rerun the installation file.

> **Warning:**
>
> Migration logs that were created during transfers are removed during the uninstall process.

Configuration

June 6, 2023

Set up

1. Provision administrators.
2. Provision users.

Provisioning Administrators

When your account is created, it is provisioned with a main administrator account.

Provisioning Users

To begin using your Content Collaboration account, you must add users and configure authentication.

Admin overview

March 4, 2024

The Admin Overview page gives summarized information on your account using both **Account Summary** and **Storage Usage**. A View release notes link to What's new in ShareFile documentation is provided at the bottom of the page.

Account Information

The account information section provides the following details: Account Name, Account ID, Plan Type, Account Owner, and Allocated User Licenses. The page also displays any entitlements on your account.
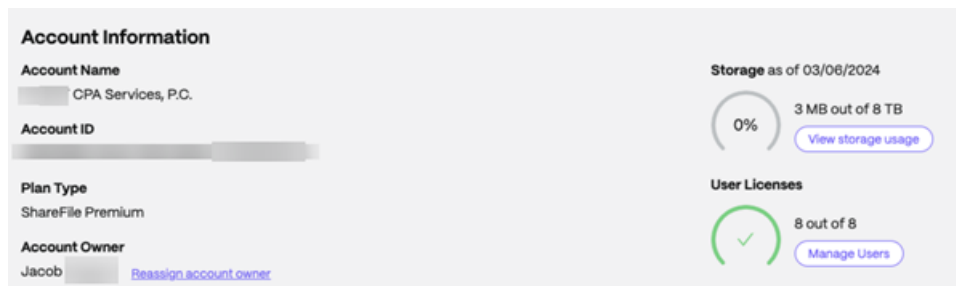
Account owner

This is an administrator whose skills and experience allow for greater permissions and who maintains all user permissions available on the account. It cannot be deleted by any other user. If an account feature is added to the account, the account owner automatically has access to the feature. Any other users must be granted access as desired by the account owner.

All subsequent access to the customer's account is managed by the account owner or administrators designated by the account owner.

Identifying the account owner   To identify the current account owner, go to **People** > **Browse Employees**. The account owner has a special icon to the right of their name.

The account owner is also indicated on the **Manage > Account Information** page.

Changing the account owner   The current account owner can use the **Reassign account owner**
option to designate a new account owner. Use the following steps to complete this task.

1. To change the account owner for an account, the current account owner must sign in and navi-
   gate to **Settings** > **Admin Settings** > **Account Information**.

2. Select **Reassign Account Owner**.

3. Use "Search existing employees"to locate the new account owner then select **Assign New Ac-
   count Owner**.
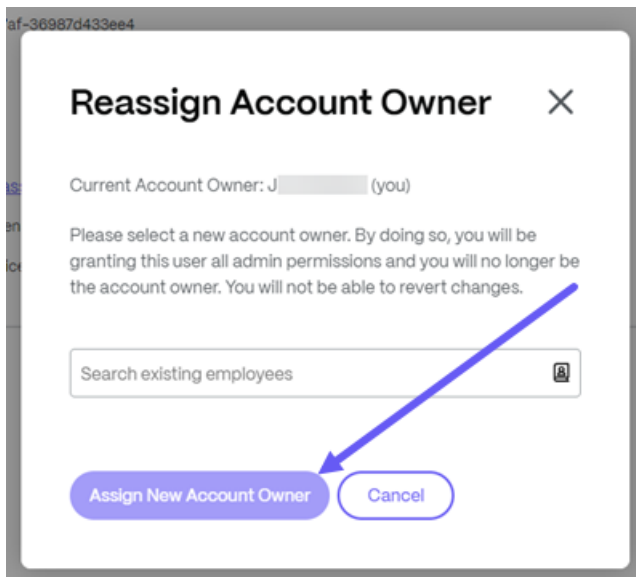
Notes:

- The new account owner must be an employee user on the account, and that employee user
  must have signed in at least once.

- The **Reassign account owner** option is only available to the current account owner.

If the current account owner is not available to place this request, contact ShareFile Support.

Storage   The **Storage** indicator shows the storage utilized (xxGB out of XXTB) and the date when
storage was updated.

Company Information

The company information section provides the following details: Company name, Phone number, Industry, Address, Website, Fax Number and Number of Employees. On top of that, this section includes the contact information for the company key contacts.

- **Billing Contacts** - These contacts may receive billing related communications from ShareFile.
- **Security Contacts** - These contacts may receive security related communications from ShareFile

IMPORTANT

Please ensure that **Billing Contacts** and **Security Contacts** are updated properly to avoid missing important communications from ShareFile.

Company Account Info

August 15, 2023

Reporting

Use ShareFile Reports to see how the account is being used by creating recurring and non-recurring reports that track usage, access, messaging, storage, and other details. For more information on using reports, see ShareFile Reports.
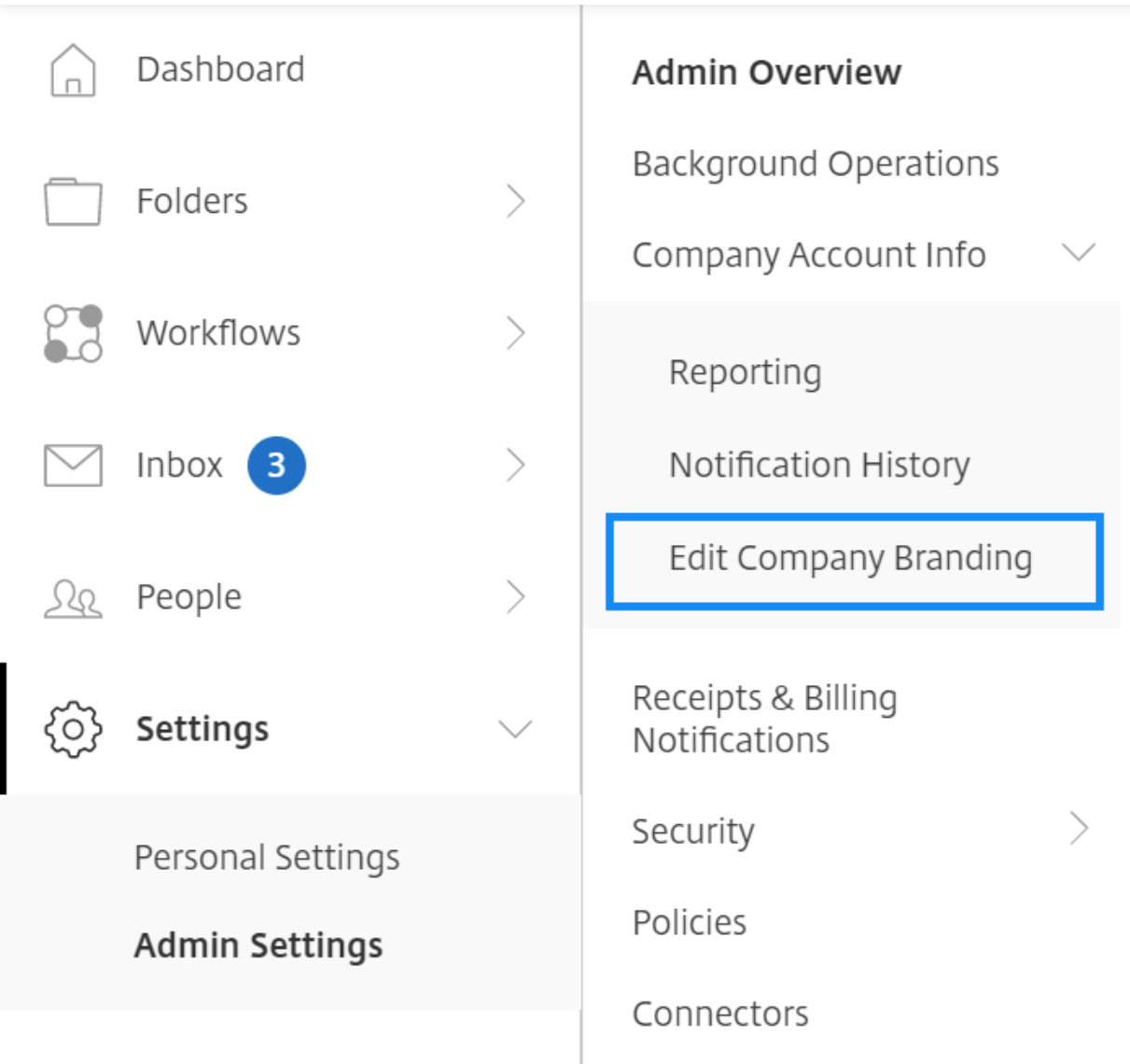
Company Branding

Your account's account or company name allows ShareFile support staff to identify your account. It is also the name that appears on any billing-related correspondences. Typically, your account name is the same as the name of your business.
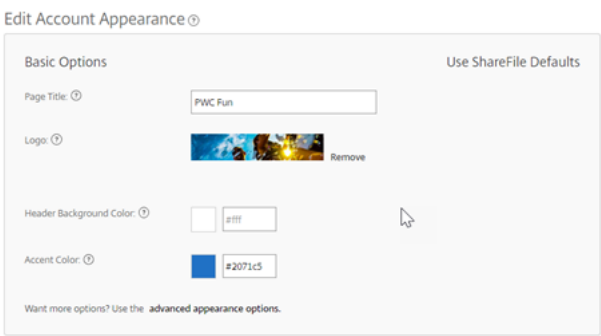
Set up company branding

Use the following instructions to set up your company branding.

1. Navigate to **Settings** > **Admin Settings** > **Company Account Info** > **Edit Company Branding**.

The Edit Company Branding page displays.

1. Under **Acount Name**, type the name of the account.

2. With **Edit Account Appearance** in **Basic Options** you can perform the following actions:

- Change the **Page Title** that appears at the top of the window.

- Upload your company logo.

- Change the **Head Background Color**.

- Change the **Accent Color**.

> **NOTE:**
>
> By default, the **Basic** options page uses the page title, logo, header background color and accent colors that you selected. To customize the appearance use the **advanced appearance options** link on the page to expand the available options. For more information, see Edit Account Appearance.

3. Select **Save** at the bottom of the page to save your branding page changes.

Edit Account Appearance

The following options are set by the users who have the **Edit Account Appearance** permission set. These are optional.

- **Browser Options** - allows you to edit the page title, and favicon in the account appearance.

- **Header Options** - allows you to edit the logo, background image, and background color in the account appearance.

  > **Notes:**
  >
  > – The logo image must be no taller than 80px and no wider than 400px
  > – The background image can be any size, but only display the first 80 vertical pixels and will tile/repeat horizontally and vertically.
  > – The default background color is white but any HTML color code can be used. If both a color and an image are entered, the image displays, and not the color.

- **Page Options** - allows you to set the accent bar color at the top of the tabs and in the content boxes.

- **Login Page Options** - Allows you to upload a logo, select a logo background color, a background color, upload a background image, and provide a description of your page.

- **Email Options** - Allows you to upload a logo, provide a header description and provide a footer description.

When all of your advanced options are completed, select **Save** at the bottom of the page.

Edit Subdomains

With your ShareFile account, you are allowed up to three subdomains. All of these subdomains share the same custom branding for your company account.

The following requirements are necessary to create subdomains:

- Contain only letters, numbers, and hyphens.
- Does not start with a hyphen.
- Is at least 2 characters long.

Once you have added the subdomains, select **Save** at the bottom of the page.

Billing

March 4, 2024

The **Billing** page allows you to view receipts, edit billing information, and other related activities.

In your ShareFile account, navigate to **Settings** > **Admin Settings** > **Billing** to access:

- [Receipts & Billing Notifications](#)

- [Edit Billing Info](#)

Receipts & Billing Notifications

Use the **Receipts & Billing Notifications** page to view and download to print your invoices for your ShareFile account.

You can select **Pay Now** to pay your invoice. See Pay Now for more information.

To download an invoice, select the download icon next to the month you want to review or print. A PDF is downloaded to your device.

Pay Now

Pay Now allows you to make a one time payment using a credit card to pay your invoice.

Use the following steps to pay your account from the **Receipts & Billing Notifications** page.

1. Select **Pay Now** from the **Receipts & Billing Notifications** page.

ShareFile

The **Enter Card Details** pop-up displays.

2. Enter the requested information.

3. Select **Continue** to make the one-time credit card payment.

To pay all future invoices with a credit card, see Edit Billing Information for more information.

Edit Billing Information

The **Edit Billing Information** screen allows you to update your billing type from invoice billing to credit card. You can also make changes to your billing address.

Update Billing Type

Use the **Update Billing Type** to make a change to how your ShareFile bill is paid.

1. Navigate to From ShareFile, navigate to **Settings** > **Admin Settings** > **Billing** > **Edit Billing Info**.

2. In the **Update Billing Type** section, select **Switch to Credit Card**.

   The **Update Billing Type** screen displays.
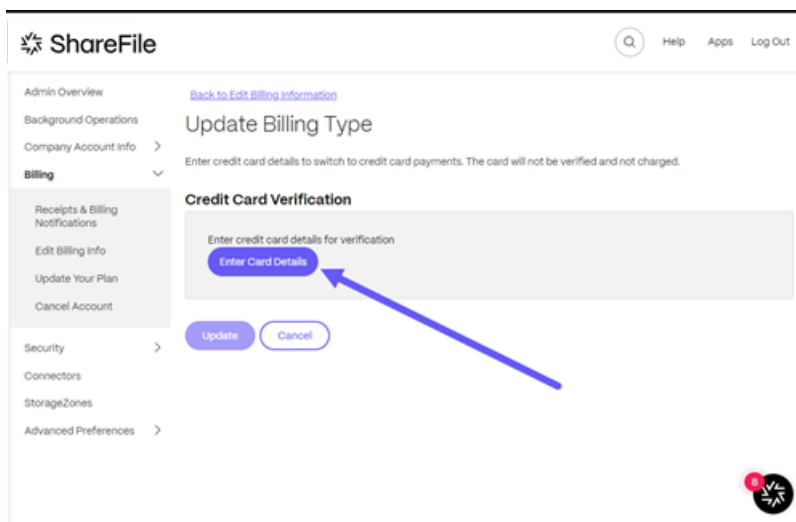
3. Select **Enter Card Details**.

   The **Enter Card Details** pop-up displays.

4. Select **Continue** to go back to the **Edit billing information** screen to receive confirmation of the change.

Update Billing Address

Use the **Update Billing Address** to make changes to your billing address.

1. Navigate to From ShareFile, navigate to **Settings** > **Admin Settings** > **Billing** > **Edit Billing Info**.

2. In the **Update Billing Address** section, select enter the new billing address information.

3. Select **Save**.

Security

January 7, 2024

Password requirements

You can control password requirements for users here. By default, all passwords must contain at least 8 characters, containing at least 1 number, 1 upper case letter, and 1 lower case letter.

To create other password requirements for your users, fill out the form on this page. Any changes you make go into effect the next time a user changes their password.

For all users, passwords:

- Must contain a minimum of 8 characters with a maximum number of 50 characters.
- Must contain 1 upper case and 1 lower case letter.
- Must contain at least 1 number.
- Must contain at least 1 of these special characters: ! # $ % ^ & * ( )− _ + = / . ? \ [ ] | '~ @ '
- Can't be the same as their last 25 passwords.

Forced Password Reset

In response to an increase in internet-account credential (user name and password) theft, ShareFile might require a password reset and will continue to incorporate a regularly scheduled forced password reset into our normal operating procedures.

Login and security policy

Trusted domains

You can enter one or more domains to allow iframe embedding and Cross-Origin Resource Sharing (CORS).

Two-step verification

Two-step verification uses your phone to provide an extra layer of security for your user name. After you sign in, you're asked to enter a verification code that is sent to your phone using a text message (SMS) or voice call. Supported Authenticator apps like Google and Microsoft can be used as an option instead of your usual password.

> **Notes:**
>
> - Two-step verification is enforced for all employee users in all ShareFile accounts.
> - Admins who prefer to disable the two-step verification enforcement for employee users

> can opt out of this enforcement by selecting **Complete Opt-Out Waiver** on the **Two-step verification** pop-up. This disables the enforcement, however, employee users are able to enable it for themselves to improve the security of their account.
>
> - Client users can use two-step verification even if the admin did not enforce the use of the feature.

This feature is available to both Client and Employee users. Two-step verification is supported on iOS and Android mobile devices.

Some apps require an app-specific password that must be generated each time you want to sign in to the app.

Account lock-out configuration

This allows you to select the number of times a user can enter an invalid password before being locked out of the account for a specific time period of your choosing.

Terms and conditions

Terms and conditions can be added to the sign-in page for customers. We recommend that single sign-on customers also implement the terms and conditions on their sign-in page for full coverage. You have the option of including customizable terms and conditions that must be accepted to indicate compliance with the terms before entering the account. Contact ShareFile Support for assistance with adding terms to your sign-in page.

Users with the **Admin Account Policies** permission can request Terms and Conditions to be added.

IP restrictions

Use IP restrictions to restrict where your users can sign in to your account. contact ShareFile Support to set IP restrictions.

Authentication
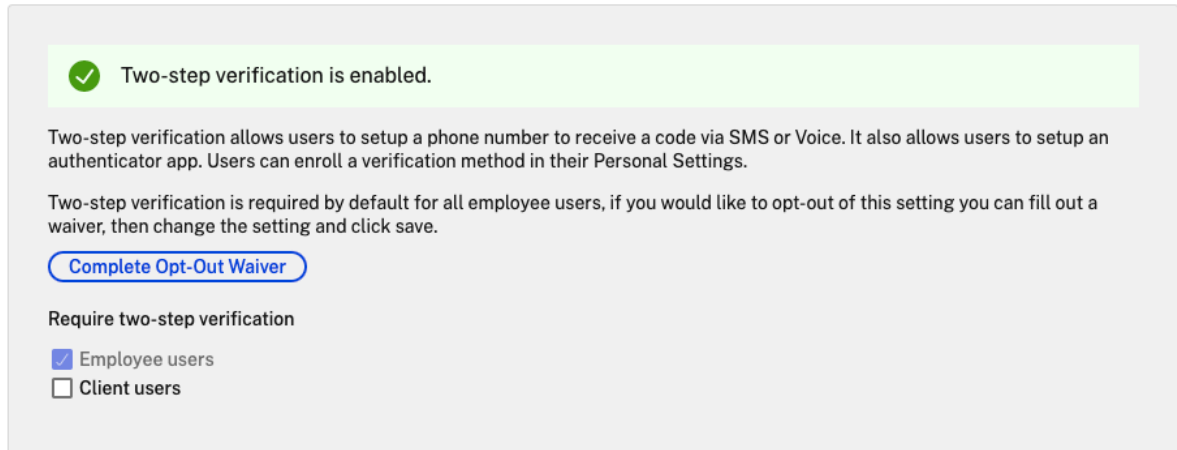
Inactive users can be signed out of the account after a chosen duration of inactivity. By default, this duration is set to 1 hour.

OAuth tokens are used by apps and the API to authenticate. After the period selected here, users will be required to reauthenticate with all apps. If set to **Never**, OAuth tokens can still be manually expired through **My Connections** under **Personal Settings**, or by an administrator on the user's profile page using the **Users** menu.

Limitations

- This feature isn't available for trial accounts.
- This feature can't be used with company credentials or a custom sign-in page.

Require two-step verification requires that the user group enrolls and opts in for two-step verification. When enabled, the setting is enabled for all Employee Users or Client Users or both. By default, it is required for all employee users on all ShareFile accounts.

For new users, the activation process requires that the user enter a phone number that is enabled for text message (SMS) or voice. For existing users, the user is prompted to enter the phone number that is enabled for text message (SMS) or voice on the next sign-in from the web, desktop, or mobile app.

Device security

You can use these options to control the security level for devices used to access the ShareFile account by other users. These settings override any individual user preferences.

Modifiable device security settings include:

File self destruct - Determines the number of days without the user logging in or accessing the account before the account is automatically removed from the mobile device. Self-Destruct occurs even if the user is offline. Options are: Never, 1, 3, 7, 14, 30, 45, or 60 days. When `self-destruct` is triggered on a device, users with mobile push notifications enabled might receive a notification referencing a *Poison Pill* activation.

Require user passcode - Controls whether users are required to enter a 4-digit PIN or a password to access their content. When set, all content is encrypted. Options are: PIN, Password, or User-Selected Passcode.

Enable external applications - Determines whether users can open downloaded files outside of the ShareFile application.

Enable offline access to files - Controls whether users can see ShareFile content when the device is offline.

Restrict modified devices - Enabling this restricts users from being able to use ShareFile on a jail-broken device. ShareFile can't fully troubleshoot issues encountered by users that have chosen to jailbreak their device.

Enable automatic login - Determines whether users can opt to save their password on their device.

Device security presets

You can configure each setting individually at the **Configure Device Security** menu. In addition to a Custom setting option, ShareFile offers several presets with various differences.

- Standard
- Secure
- Online Only
- Custom

Super user group

Administrators, also known as super users, are automatically added to all new and existing folders on a given ShareFile account. Super users permissions include upload, download, delete, and administrator ability on all folders. Super-user group access to a folder can't be modified or removed in the folder access menu. This feature is enabled on your account by default.

Manage a super user group

Management of super users requires the **Manage Super User Group** membership permission.

1. Go to **Manage > Security > Edit Super User Group**.
2. To add a user, click **Add New User**.
3. Select a user from the menu from the list of employees on your account.
4. Use the checkboxes to select the users you want to add. Click *Add**.
5. Click **Save**.

You can also remove all users from the super user group. The group can be edited by any employee user with the **Allow this user to manage Super User Group** admin permission. Super users appear

in the **Folder Access** section on each folder. Admin users can choose not to display the group in the access list.

To hide super users from the **Folder Access** section, go to **Manage > Security > Edit Super User Group**, then select the **Hide Super Group from Folder Access List** checkbox.

Download or upload alerts can be enabled for the super user group in the folder access menu on a folder-by-folder basis.

Single sign-on (SSO)

Single sign-on (SSO) can be configured using various IdPs and certain SAML 2.0 or 3.0-based federation tools using basic, integrated, or forms authentication. This feature is available for Business and Enterprise plans.

Supported configurations

The following configurations have been tested and are supported for most environments.

- Citrix Endpoint Management
- ADFS 3.0
- ADFS 4.0 (Windows Server 2016)
- Dual IdP - ADFS and Citrix Endpoint Management
- Microsoft Azure AD

More configurations

These configurations have been successfully configured and tested by our engineering teams. The following configuration documentation is subject to change due to continued product enhancements and improvements. The following configuration guides are presented as is:

- Centrify/Idaptive
- G Suite for Business
- Okta
- Ping-Federate
- PingOne / PingID
- OneLogin

> **Note:**
>
> ShareFile no longer supports custom logout URLs for the SAML configuration. All users will be directed to the ShareFile authentication service's logout page when they sign out. Some of the above configuration guides may still provide a logout URL, but are no longer necessary.

Data loss prevention

ShareFile integrates with third-party Data Loss Prevention (DLP) systems to identify files that contain sensitive information. To limit access and sharing of items based their content, enable DLP scanning on your storage zone controller and then configure the settings on this page.

Enable the **Limit access to files based on their content** setting if you have one or more private storage zones configured to use a third-party DLP system to scan and classify documents. With this setting enabled, sharing and access filters are applied to documents based on the results of the DLP scan. Use the settings on this page to define the sharing and access filters for each classification.

- **Unscanned documents** - Allow these actions for documents that your DLP system hasn't scanned. This includes all documents stored in ShareFile-managed storage zones or other storage zones where DLP isn't enabled.
- **Scanned: OK** - Allow these actions for documents that your DLP system allowed.
- **Scanned: Rejected** - Allow these actions for documents that your DLP system rejected because they contain sensitive data.

For more information on Data Loss Prevention, see Data Loss Prevention.

Connectors

January 30, 2024

Connectors overview

Connectors allow employees to access files and folders stored on a connected on-premises or cloud-based resource. Users can use the web application and ShareFile apps to view and interact with data stored in connected locations.

> **NOTE:**
>
> ShareFile is decoupling accounts from Citrix Cloud and Workspace. **Files** integration is disabled from Citrix Workspace. Users can download, upload, move, copy, and delete data from within

the ShareFile web application. For more information see, Decouple your ShareFile account from your Citrix Workspace.

Connector type	Description	Supported services
ShareFile Cloud Connectors	Allows ShareFile account users access to personal cloud-based data storage services within ShareFile apps. Users can download, upload, move, copy, and delete data within these connected resources. These connectors require each user to authenticate with their service credentials. Users must and allow the ShareFile service to communicate with the permitted cloud-based service.	Office 365, OneDrive for Business, SharePoint Online, Dropbox, Box, OneDrive, Google Drive

ShareFile

Connector type	Description	Supported services
On-premises Connectors	On-premises connectors allow users to access data locations within Network file shares or as SharePoint sites. These connectors require an additional configuration of storage zone controller in a local environment.	SharePoint sites, collections, libraries, Network file shares, Documentum Connector

Supported apps

App type	Supported
Web app	Latest version
Mobile apps	iOS, Android, Universal Windows Platform
Desktop apps	ShareFile

Connector types

The following connector types can be enabled once:

- Box
- Dropbox
- Google Drive
- OneDrive

Alternatively, the remaining connectors require additional configuration. The following connector types can configure multiple connections for user access:

- On-premise connections

- OneDrive for Business

- SharePoint Online

Please note an Office 365 administrator must add the Citrix ShareFile Connector for Office 365 to secure ShareFile service access to Office 365 data.

Recommendations for using OneDrive for Business connector via ShareFile for Windows application

Problem

While using the OneDrive for Business connector via the ShareFile for Windows application, a default **Folder and Files** setting within the Windows operating system may lead to a large amount of API calls to the **Microsoft Graph API** when hovering over files or folders in the UI to display file size and file count information.

Recommendations

To avoid a large number of inadvertent calls to the **Graph API**, ShareFile recommends that you or your administrator disable the **Display file size information in folder tips** using the following steps:

1. In **Windows Settings** navigate to **File Explorer Options** > **View tab** > **Advanced Settings** > **Files and Folders** menu.
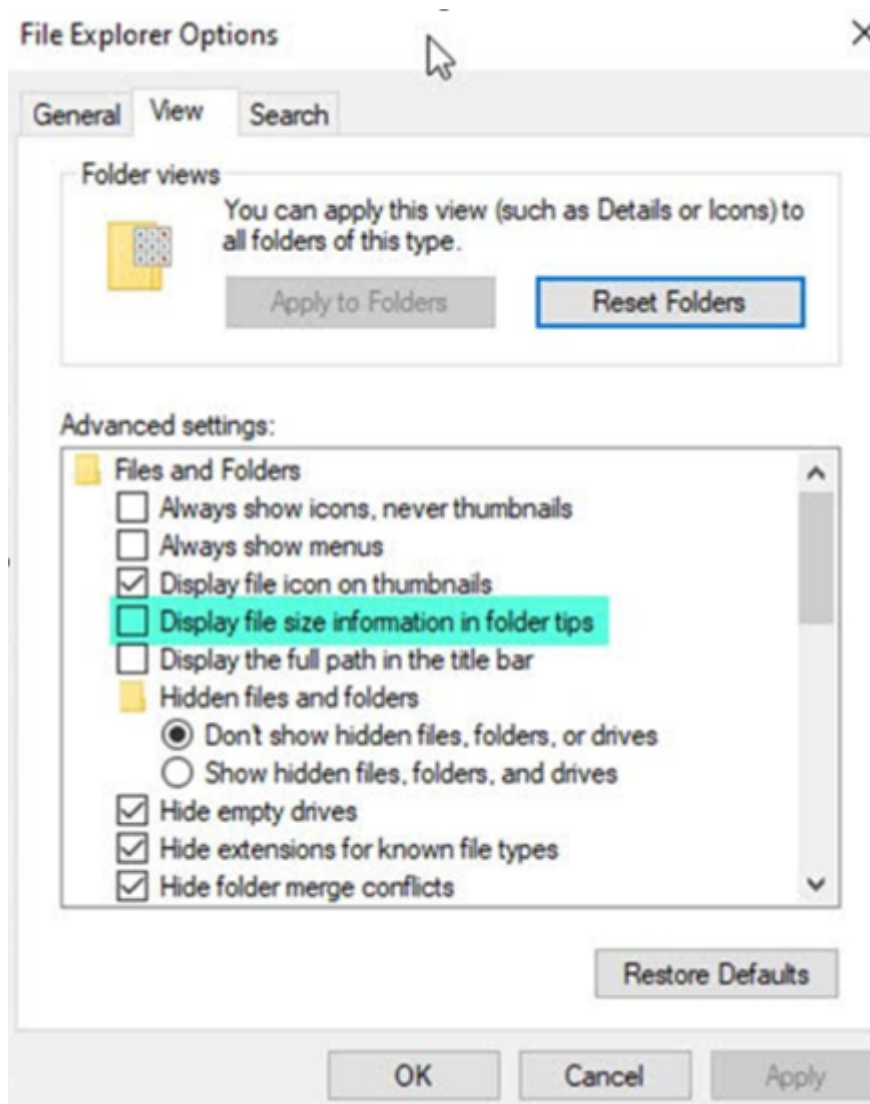
2. Deselect the **Display file size information in folder tips** option.

NOTES:

- This setting drastically reduces your API calls to **Microsoft Graph API** resulting in optimized performance of the ShareFile connector. For more information about throttling limits posed by Microsoft, see Microsoft's API throttling limits.

- As a best practice to lessen the complexities, ShareFile recommends avoiding large and complex folder structures when creating a Connector.

Configuration requirements

- Personal Cloud Connector access is enabled for a ShareFile account.

- Existing on-premises storage zone has connector features enabled on the primary storage zone controller.
- Employee users with the permission to Create and Manage Connectors have access to Connector settings in Admin Settings.
- To share files from connectors, Connector Sharing access must be enabled for the ShareFile account.
- Users with access to Connectors require **Use Personal File Box** permissions to share files from Connectors. Files shared from Connectors are copied to the File Box first. Recipients of the share link or email might not have immediate access to download those files until the copy is complete.
- This feature requires ShareFile managed storage zones (cloud storage).

Enable and add connectors for ShareFile users

> **Note:**
>
> Account owners can request to activate this feature on their ShareFile account.

For accounts that have Personal Cloud Connectors features enabled, employee users with the required permissions to manage and add connectors can open **Admin settings** > **Connectors**.

Select **Enable** or **Add** from the available connectors.
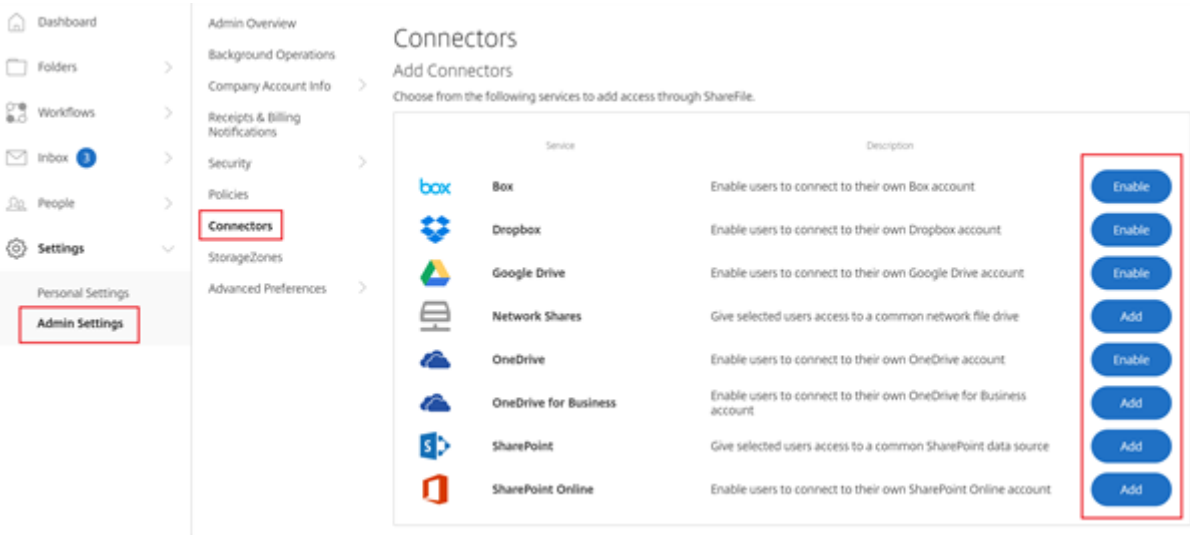
Manage access to connectors

When enabling and adding a Connector, you grant other users access to the Connector within their ShareFile account. The user has access to data locations within their own accounts. Local storage resource determines access-control permissions to those cloud-based data locations.

You can choose which employee users or distribution groups have access to their cloud-based or on-premises connector in the **Manage Access** dialog box. Click **Save** or **Skip** when done adding users. If you select skip, only the user that creates the connector, and the Super User Group, have access to the connector.
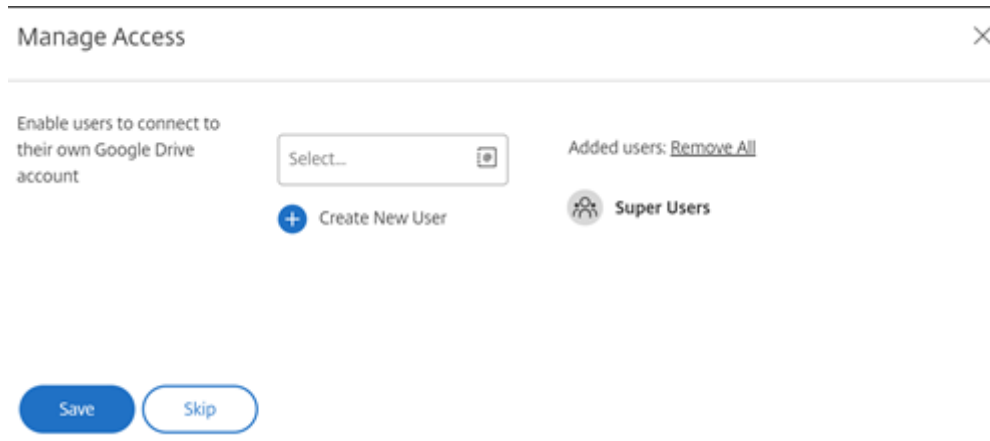
Add an on-premises SharePoint, Network File share, or Documentum Connector

> **Note:**
>
> An existing storage zone with Network Share or SharePoint connector features enabled is required to add on-premises connectors. For more information, see Create and manage storage zone connectors.

Employee users must have the permissions to **Create and Manage Connectors** and **Create root-level folders** to add on-premises connectors.

1. Navigate to **Admin Settings** > **Connectors** and then select **Add** next to Network Share or SharePoint connector. Please note that if you are using Citrix Cloud these settings are found in **Content Collaboration** > **Manage** > **Connectors**.

2. Within the **Add Connector** dialog box, enter the display name for the Connector. Connectors must have a unique name and not one currently used on the account.

3. You can choose the on-premises zone that is local to the Network Share or SharePoint site.

> **Note:**
>
> The zone must either be in the same domain or have a trust relationship with the storage resource.

4. Enter the path to the Network File Share connector using the UNC Path or enter the Site using the HTTP or HTTPS URL of the SharePoint site or document library.

Other considerations include:

- Network File shares and SharePoint document libraries will require additional (basic) authentication upon opening the connector. The credentials used to log in to the ShareFile account might be different than the credentials required to authenticate to the Connector.
- If both Network File share and SharePoint connectors are configured, note the same credentials are used to authenticate with SharePoint libraries and Network File shares. If a user needs to use different credentials to access a connected library or share, the user must log out of their ShareFile account and close the browser session. When you open the connector, you need to authenticate using the alternate credentials.
- Basic Authentication does not support non-ASCII characters. If using localized user names, try using NTLM or Negotiate authentication.

- Due to a known Microsoft Issue, Network File share connectors cannot be accessed from the Microsoft Edge browser when utilizing a Citrix ADC for connector authentication.

Enable SharePoint Online Connector

SharePoint Online requires a few additional steps to work properly with ShareFile. Before taking any action in the ShareFile web application, you need to add the ShareFile app to your SharePoint Online site.

First, add the ShareFile App to your SharePoint Online site.

Navigate to this site where you replace the `<Tenant>` with your company/tenant name: `https://<tenant>.sharepoint.com/_layouts/15/appStore.aspx/appDetail/WA104379108`

Select the **Add** button, then follow the prompts.
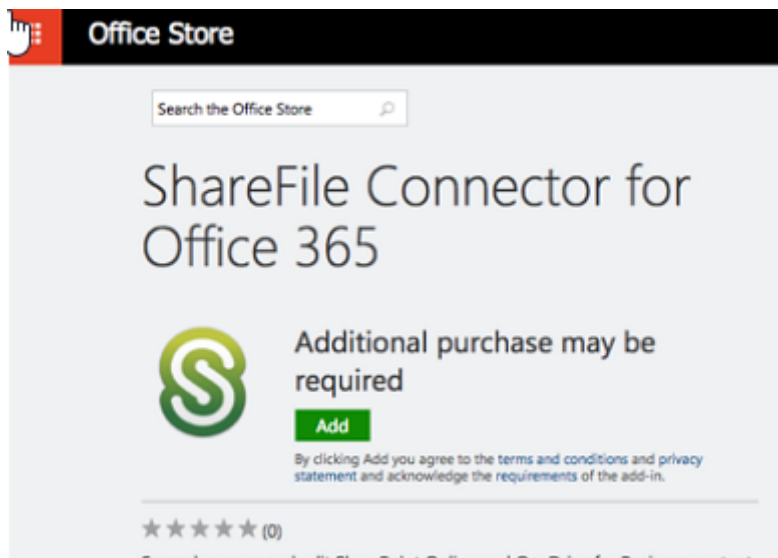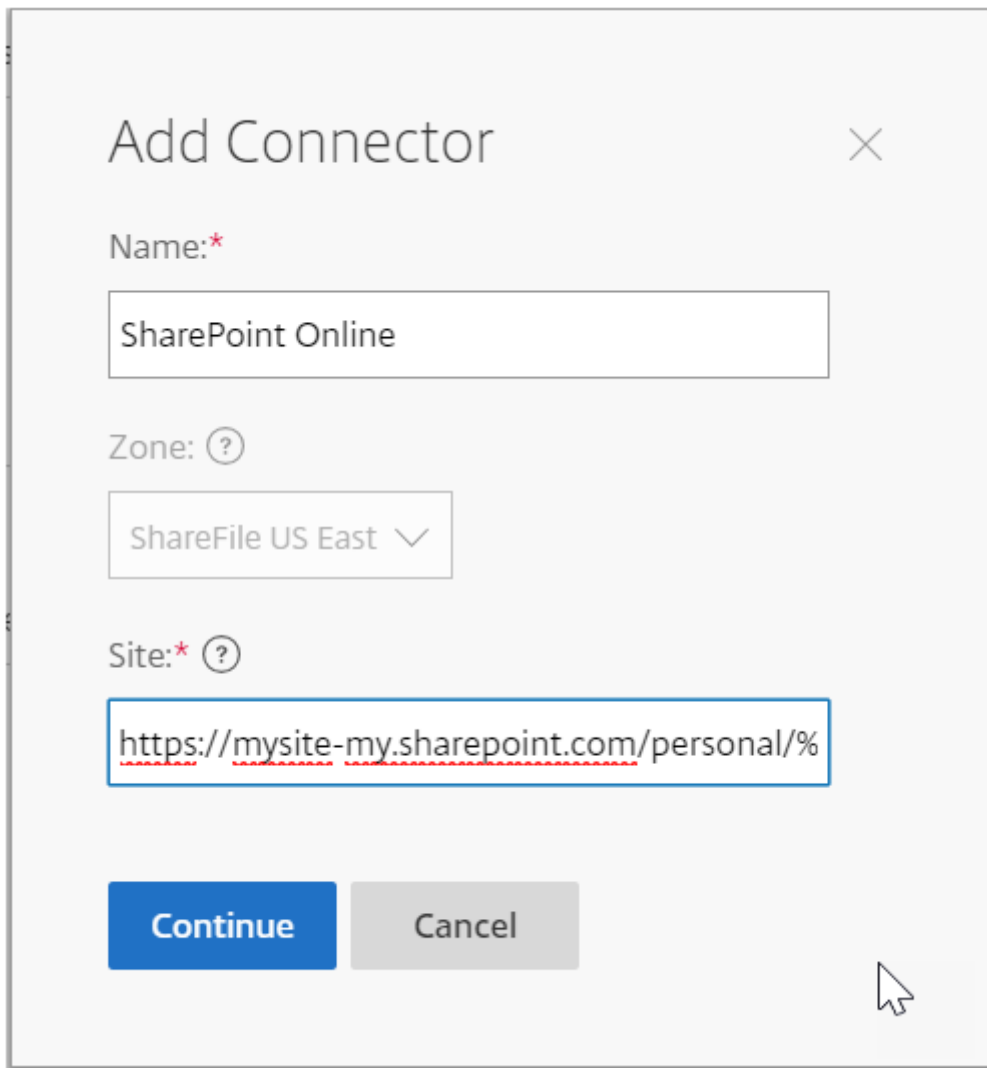
> **NOTE:**
>
> In order for the app to function properly, please take the required steps to **Trust the ShareFile app** when prompted.

Once you have installed the app, navigate to **Admin Settings** > **Connectors** to view all Connectors available for your account.

Select **Enable** for the SharePoint Online connector. You are prompted to name the Connector and provide a Site URL.

Enter the URL path to your OneDrive for Business or SharePoint Online account. Enter the URL as follows, replacing "mysite"with your own domain/site name and adding the %loginname% wildcard where indicated. If you do not know your subdomain, you can find it in your web browser when you sign into OneDrive or SharePoint.

`https://mysite-my.sharepoint.com/personal/%loginname%/Documents` or `https://.sharepoint.com/SitePages/Home.aspx`

ShareFile
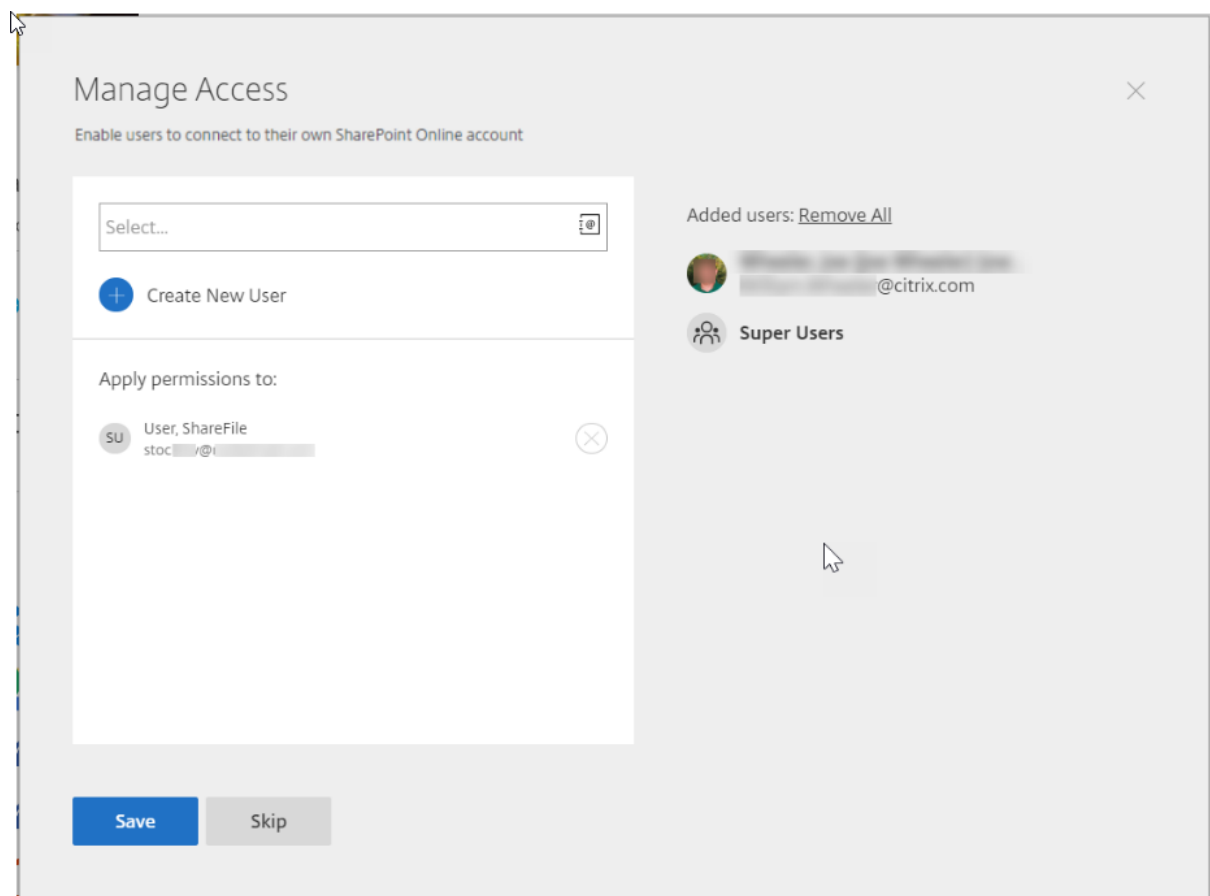
By adding a user to the access list for a specific Connector, that user is able to use the Connector to link their account to another data storage service. Select **Save** to continue.

Alternatively add the Connector app to the respective SharePoint Online account if the above option does not work.
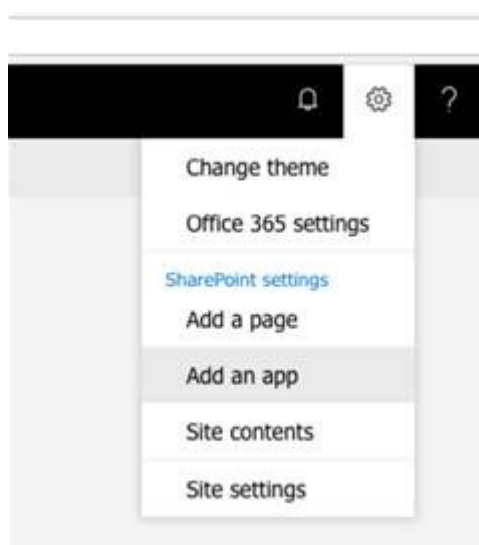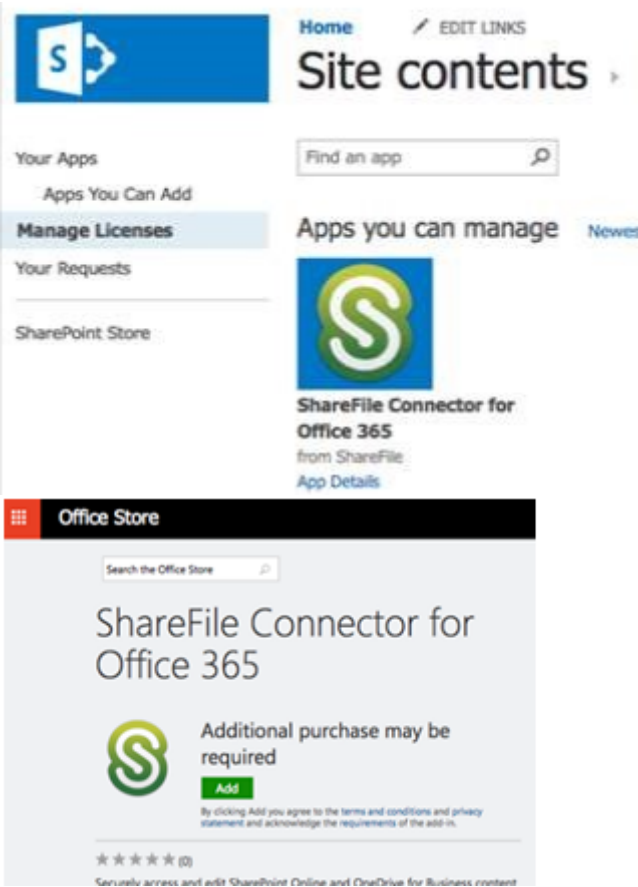
Notes and limitations

Item	Description
On-Prem Customer Restrictions	Personal Cloud Connectors are supported for accounts utilizing Customer-Managed storage zones that are associated with ShareFile-Managed storage zones. This feature is not available to accounts with no association to a ShareFile-Managed storage zone including on-prem or tenant setups.
Limitation	File uploads to Personal Cloud or SharePoint Online currently have a **maximum upload size of 200 MB per file**.
Limitation	File uploads to the OneDrive for Business Connector currently has a maximum upload size of 16GB.

Item	Description
Limitation	**Connectors must have a unique display name**. Users are blocked from using a connector name that is currently in use elsewhere on the account.
Limitation	Actions such as browsing folders or downloading files may fail when using Safari web browser. To resolve any issues, please ensure cookies are allowed in your Safari system preferences.

Storage zones

June 7, 2023

Storage zone provides administrators the flexibility to choose between Citrix-managed, secure cloud storage, or IT-managed storage zones (on-prem) storage within your own data center. In addition to allowing users the ability to create and manage on-premises storage zones, users also have the option of utilizing Citrix-managed storage zones.

For more information about storage zones controller including components, data storage, and more, see Storage zones controller 5.x.

Select storage zone for root-level folders

Membership to the Super User Group is required to change another user's default storage location. This permission is only available to Citrix Content Collaboration users on certain plans.

Enable the **Limit access to files based on their content** setting if you have one or more private storage zones configured to use a third party DLP system to scan and classify documents. With this setting enabled, sharing and access filters are applied to documents based on the results of the DLP scan. Use the settings on this page to define the sharing and access filters for each classification.

- **Unscanned documents** - Allow these actions for documents that your DLP system has not scanned. This includes all documents stored in Citrix-managed storage zones or other storage zones where DLP is not enabled.
- **Scanned: OK** - Allow these actions for documents that your DLP system accepted.
- **Scanned: Rejected** - Allow these actions for documents that your DLP system rejected because they contain sensitive data.

Managing public storage zones on your account

Administrators can choose to enable a customized subset of Citrix-managed storage zones on their account. Storage zones can be viewed at **Manage > StorageZones**. From the StorageZones menu, select **Citrix Managed**.

From this menu, you can enable or disable specific zones on your account by clicking the check box to the left of the zone name. You can also edit the alias of a particular public zone by mousing over the **Alias** column to the right of the zone title. Edit the alias of a public zone to better suit the users on your account. In addition to editing your storage zones, you can see your current usage in MB in the **Usage** column.

Selecting the default public storage zone for a user

Account administrators can designate the default public storage zone for a specific user on their account, and allow the user to select a zone when creating a root-level folder.

1. To modify the settings for a user on your account, navigate to **Users > Manage Users Home**.
2. Locate the user you would like to modify using the Browse or Search function, then use the **Manage** icon to open the user's profile page.
3. In the **Employee User Settings** section of the user page, use the Storage Location menu to choose the user's default storage zone.
4. In the **Admin Privileges** section, you can choose to allow the user the ability to create and manage zones by clicking the check box to the left of **Create and manage zones**.
5. Once you have finished managing your user's storage zone and permissions, select **Save Changes**.

Advanced preferences

March 14, 2024

Email Settings

Send e-mails from

Some email services reject messages sent using the Citrix Content Collaboration mail server or flag the messages as spam. If you are getting any reports of email delivery problems, setting the preference to **user sending message** might resolve the issue. Once the preference is set, the name of the

user sending the message appears in the **From** field and that user's email address is used when the message recipient replies to the message. This option might trigger message rejection as well, so do not use this option unless you are experience deliverability issues.

SMTP Server

By default, system notifications are sent from Citrix Content Collaboration mail servers to clients. At times this might not be ideal, especially when dealing with recipient mail servers that employ aggressive spam filters or whitelists. In these cases, setting a custom SMTP server allows you to send system notifications from your own mail server instead. Once these settings are configured, all emails sent through your account are sent through your mail server, instead of Citrix's servers. By setting a custom SMTP on your account, your users recognize your email address as the sender and any failed emails come back to you. To use a custom SMTP, an employee user must have the **Allow this user to modify account-wide policies** permission.

If you use Microsoft Office 365 and would like to utilize custom SMTP, view this set up guide from Microsoft.

Setting up custom SMTP   1. Go to **Manage > Advanced Preferences > Email Settings > SMTP Server**.

2. Click **Configure SMTP Settings**. The Custom SMTP Configuration page appears.

3. Enter the appropriate information to enable this feature.

Required fields:

- **Enable Custom SMTP** –This option must be selected if you want to use these settings.
- **Email Address** –This is the *from* email address of sent emails.
- **Server** –This is the host name of the email server that is used to send emails.
- **Port** –This is the port number to be used. Port 25 is the default. The following ports are also allowed: 26, 443, 465, 587, 2525.
- **Username** –This is the user name needed to access the server.
- **Password** –This is the password needed to access the server.
- **Notify Email on Failure** –This email address is sent notices if Citrix Content Collaboration is unable to send an email with the given settings.

Optional fields:

- **Use SSL** –Choose between Implicit, Explicit, or Off.
- **Failback to ShareFile** –If selected, messages that fail to send using the custom settings prompt Citrix to send future emails through standard email settings.

- **Authentication Method** —Select an authentication method here if a particular one is required by your server.

4. Click **Save and Sent Test Email** to complete the setup.

Troubleshooting your SMTP setup   Email Notifications / Messages are Delayed - This issue might occur when you are utilizing certain filter services or programs processing messages on your local mail servers. Before contacting Citrix about delays in our system, verify that your messages are not being delayed by local filter services. One means of verifying that information is to review the full header details of a message and reviewing the time messages send between services or filters.

Too many connections from your host - This issue might occur when you have exceeded the maximum allowed connections on your SMTP server. To resolve this, you must update or increase your maximum allowed connections in your SMTP configuration, or use consolidated notifications to limit the number of connections you receive on a typical basis.

Notify users of their own activity

By default, even if a user has upload or download notifications for a folder, they do not receive notifications about their own activity in those folders. Enabling this option causes users with folder notifications set to receive updates about their own activity.

Upload Receipts

After enabling this setting, **Request a File** links that require recipients to enter their name and email before uploading emails a receipt email to the person uploading a file. Only request links that require name and email send upload receipts.

Email Notifications

When you set upload or download notifications for certain users on folders, users receive notifications about the uploads or downloads in real time by default. Users can change this default behavior by clicking the **Personal Settings** link in their account. However, if you want to set a default value for this setting for all users on your account, you can do so using this setting.

Changing this setting does not affect existing users in the system. It is only applied to newly created users. You can update this setting for individual users at their individual profile page.

Users can receive email notifications in the following languages: English, German, Spanish, French, Dutch, Chinese, Russian, Japanese, Korean, or Portuguese.

Q&A Email Text

This feature determines whether the Folder Q&A feature sends the text of the questions and answers in the body of the notification emails. When set to no, the emails do not contain the question or answer text, but do include a link to sign in and view that information instead.

Encrypted Email

This option is used to enable the encrypted email feature. Setting the option to **No** prevents users from sending or responding to encrypted email messages.

Secondary Email Addresses

By default, all users on the account can configure a secondary email address for their profile. Setting the value to **No** removes the ability to configure a second email address for all users, including both employees and clients.

Permissions

Client Shares

By default, all clients who have download access to a particular folder have a **Send** button that allows them to send any of the files in the folder to a third-party recipient. However, in some use cases, companies do not want clients to be able to send files to third-parties, even though the client can download the files and send them to third-parties outside of the system. If **Yes** is selected, the **Share** button appears for clients inside all folders. If **No** is selected, the **Share** button only appears for employee users.

File settings

Retention policy

For accounts on the Professional plan and higher, the File Retention policy causes files to automatically be deleted some days after they are uploaded. This option can be configured separately for each root-level folder in the system. This setting determines the default file retention policy used when a new root-level folder is created. **Never** is the default value.

Sorting

By default, files and folders are displayed so that the most recent items are listed first. Users can choose a different order for files and folders by clicking the Title, MB, Uploader, or Creator headings. Citrix Content Collaboration remembers the order that they choose and uses this option to display files in the same order within that folder in the future. You can choose a different order in which files and folders display. To do so, choose a category to use to display files and whether they are to be displayed in **Ascending** or **Descending** order.

Versioning

If **Yes** is marked, when a user uploads a file to a folder that already contains a file with the same name, both versions of the file are saved so you can follow the progress of the file and prevent any data loss from overwriting. If **No** is chosen, uploading a file with the same name as an existing file causes the system to overwrite the older version of the file on your account.

You can set a maximum number of versions of files that the system saves. For example, if you choose to save up to 10 versions of a file, and you have 10 versions of a file stored on your account, any new uploads cause the oldest version of the file to be deleted.

Editing

When using Microsoft Office Online for viewing and editing, Office Online keeps a temporary copy of the file being viewed and edited for the purposes of rendering and making changes to the file. It is recommended that all administrators communicate this information to users along with reviewing the Microsoft Terms of Use and Privacy Policy. An Office 365 subscription is required for editing.

Cloud rendering

If Cloud Rendering is enabled, Citrix Content Collaboration keeps a temporary copy of the files (images, audio, PDFs) involved in your workflow.

When the workflow completes, Citrix Content Collaboration moves the files to the selected on-prem folder. If a user views any file related to a completed workflow, Citrix Content Collaboration makes a temporary copy of the file from on-prem to the Citrix Content Collaboration cloud cache. A file is available for up to one week in the cloud cache after the last time the file is viewed.

If Cloud Rendering is disabled, users are not able to use Feedback and Approval or Custom Workflow features with files stored on a customer managed storage zone. It is recommended that all administrators communicate this information to their users along with reviewing the Citrix End User Services Agreement and Privacy Policy.

Enable ShareFile tools

You can enable or disable access to individual apps and tools on your account. Any changes in this menu impact all users on the account.

Show Apps Page in Navigation Bar allows the Apps link to be present in the upper right corner of your account. You can customize which tools are shown in this list. You can enable or disable the tools listed in this menu.

Folder templates

This tool allows you to create a default set of subfolders that can be added to new or existing folders on your account to allow for easy folder structure setup when the same subfolders are frequently used. An example of this is if you have separate folders for specific projects or clients on your account and information in each folder is always organized into the same subfolder categories. Applying a folder template to the folder automatically creates the default subfolders within the selected folder to streamline folder setup.

> **Important:**
>
> - Folders associated with a template cannot be deleted until the template association has been removed.
> - Folder template features rely on permissions that users must be granted.
> - When deleting a subfolder from the folder template, all instances of that folder within your account and all files contained within said folders are deleted. Folders deleted from a change to the template can be restored from the Recycle Bin.

Limitations

Users with a large amount of folders or deeply nested folder structures might not be able to apply folder templates to subfolders in bulk or rename existing folders in bulk.

There might be a delay while Citrix Content Collaboration processes template changes across your account. If you are editing templates that have been associated with many folders on your account, allow the web app time to process these changes before navigating away from the folder template menu.

Instructions

Create folder template   To create a template, go to **Manage > Advanced Preferences > Folder Templates**.

You can enter a name for this template which allows you to identify the template if you set up more than one on the system. This title is not displayed in the folder screen. You can also enter a description which is displayed on the Dynamic Folder Templates page to help you further identify a specific template, if you create more than one on your account. When you are done, click **Create Template**.

On the next screen, click the title of your template to highlight it, and then click **Add Folder**. You can set up as many subfolders as you would like. To create a subfolder of a folder in the template, you can click the name of the folder that the new subfolder will be in, then click **Add Folder**. Once you are done, click **Finish**.

Add a template during folder creation   You can add a template when creating a folder. To do so, create a folder and use the **Apply Template** drop-down menu to apply a folder template. When you create the folder, the subfolders in the template are automatically set up inside the new folder.

You can also use a template to add subfolders to a folder that you have already created. To do so, navigate to the folder you want to modify and hover your mouse over the drop-down menu carat directly to the right of the folder's name, then click **Edit Folder Options**. In the folder template section, apply a template from the drop-down menu. To remove a template from a given subfolder, check the **Do not use a folder template** option in the menu.

Apply folder templates to subfolders in bulk   You can apply folder templates to subfolders in bulk. You must be an Employee user with the **Allow this user to edit folder templates** permission. You must also be a member of the super user group to use the **Apply Templates to Folder** button.

To apply templates, click **Manage > Advanced Preferences > Folder Templates**. Locate the template you want to apply in bulk and click the **Apply To Folders** icon. At the menu, you can designate which folder you want to apply the template to. The template is then applied to all subfolders within the folder you choose. Once you have selected the folder, click **Apply**. Depending on your template, you might see a status screen as your templates are applied. Click **Apply** to finish.

Folder template permission requirements   To create folder templates, you must be an employee user with the **Allow this user to edit folder templates** permission enabled. You must also have access to set up root level folders on the account or have upload permissions in one or more folders where you can add subfolders.

To apply folder templates to subfolders in bulk, you must be an employee user with the **Allow this user to edit folder templates** permission enabled. You must also be a member of the Super User Group to use the **Apply Templates to Folder** button.

To apply a template to a folder, you must have Admin permissions on a folder to access the **Advanced Folder Settings** menu where you can view template association.

To edit or delete a folder associated with a template, you must first remove the template association. To do so, navigate to the folder in question and click the **Advanced Folder Options** using the drop-down menu beside the folder name. In the menu, scroll down to the folder template section and click **Remove Association**. You can now able to edit and delete the folder.

When deleting a subfolder from the folder template, all instances of that folder within your account and all files contained within the folders are deleted. Folders deleted from a change to the template can be restored from the Recycle Bin.

Remote Upload Forms

Remote Upload Forms let you place HTML code on your website that allows visitors to upload files from your website directly into your account. You can specify the folder that uploaded files get saved to, and what additional information to collect from the person uploading files.

> **Warning:**
>
> Citrix does not provide extra code or advice beyond the provided sample. Citrix cannot provide customer support for remote upload form code that has been modified beyond the template generated in the web application at the time of creation.

Users must be an employee user with the "Manage Remote Upload Forms" permission to create a remote upload form.

You can create a form in the Citrix Content Collaboration console by going to **Manage > Advanced Preferences > Remote Upload Forms**, then clicking **Add New Form**.

Adding a new form

Form Description: This is the name of the form in the remote upload wizard page of your account. This name is not be shown on the form itself.

Choose Destination: Choose whether to store uploaded files in a specific Folder or a File Drop. If the File Drops feature is enabled on your account, you can designate a created File Drop as the upload destination. When choosing the File Drop option, use the list to choose from a list of File Drops that you have already created.

Choose Upload Folder: Choose the folder where you want uploaded files to be stored. This folder must be a folder in the **Shared Folders** section of your account. If this folder has not been created yet, you must create it before using the remote upload wizard.

Return users to: When a website is correctly entered into this field, a user that has uploaded a file to the Remote Upload Form is taken to the website chosen. Note that any address in this field requires `https://` to function properly.

Request Uploader Info: When checked, users must enter their email, first and last name, and company before adding files to the form. If this box is not checked, uploaders appear as Anonymous.

Custom Fields: You can add more fields using the + Add Custom Field option. You have the option of marking these fields as required.

Once you have completed the form, click **Save and Get Code**. You can then copy the raw HTML iframe for your Remote Upload Form.

This code remains available in the **Remote Upload Forms** section of your account. You can retrieve it by clicking the **View Code** icon, or delete it from the list by choosing the **Remove** icon.

File drops

If the File Drops feature is enabled on your account, you can designate a created File Drop as the upload destination. When choosing the File Drop option, use the list to choose from a list of File Drops that you have already created.

Folders

March 22, 2023

Assigning folders and setting permissions

You can customize your new employee's **User Access** and **File** settings. Depending on your account or plan and your own permissions, certain permissions might not be visible or applicable. **User Access** settings are typical access and feature-based permissions you can use to manage your employee's access and abilities on the account.

You can assign folders to your user, and add the user to Distribution Groups. You can also customize the user's permissions to various folders on your account. To grant a user access to a folder, choose the check box beside the folder name.

Folder limitations

Users with a large amount of folders or deeply nested folder structures might not be able to apply folder templates to subfolders in bulk or rename existing folders in bulk.

There might be a delay while ShareFile processes template changes across your account. If you are editing templates that have been associated with many folders on your account, allow the web app time to process these changes before navigating away from the folder template menu.

Personal Folders

As an employee user, you have **Personal Folders** in your assigned ShareFile account. By default, you can upload and download files from this folder. You can also create subfolders inside this folder and add other users to those subfolders with the permissions you desire.

> **Notes:**
>
> - Personal Folders are named with email address of the user at time of first login.
> - This is not synchronized with the users email address if changed and changing the name of the folder is not supported.

Shared Folders

Shared Folders contains all folders (created by you or other users) that you have access to. This is considered the root of the entire account.

Accessing another user's personal folders

Requirements

- Employee user with the following administrative permissions enabled:

  - **People: Manage employees**

  - **Company Account Info: Access reporting**

Instructions to access another's personal folders

1. Go to **People** > **Manage Users** > **Browse Employees**.

2. Select the **Manage** icon to the right of the user's name.

3. Select **View folders and activity logs**.

> **Note:**
>
> - As a super user, you can upload and download files as well as manage user access on any subfolders.
> - You can make any subfolder a favorite folder for easy access through the **Favorites** tab in the future.

Use personal File Box

The File Box is a personal storage space where employees can store files for a limited period. This space is not generally a collaborative or shared space, although some users might be given access to see other employee's File Boxes.

> **Note:**
>
> If you do choose to take away a user's access to the File Box, they are not able to use any email plug-in tool or add files from their computer when creating a Share message or Link.

See File Box for more information.

People settings

March 5, 2024

Manage Users Home

Utilize manage users to do the following:

- Search for users including employee and client users.
- Create employee users and set access to folders, storage locations, and add to distribution groups.
- Create client users and set access to folders and distribution groups.

Search Users

Use the search function to find existing employee or client users.

Create New Users

New users for the ShareFile account can be created as either an employee user or a client user.

Create Employee   An employee user is an internal user within your company. Employee users are granted a wide range of permissions and access to your account. Creating an employee user consumes an employee license.
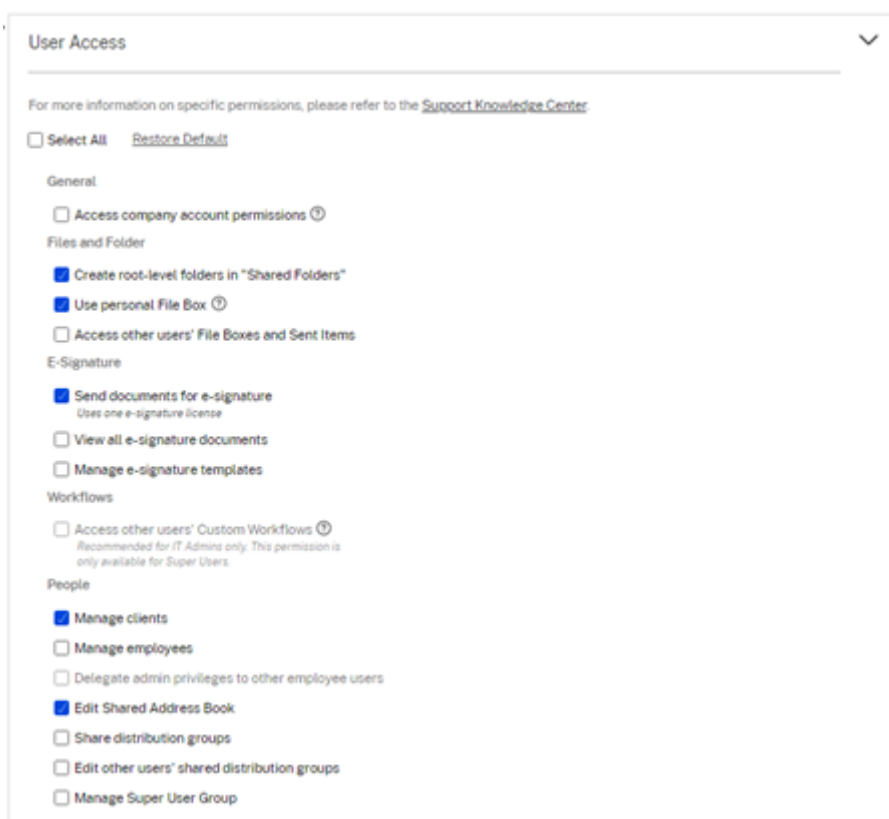
Requirements to create an employee user

- The **manage employee users** permission.
- Employee users can only grant or revoke permissions that they themselves have been granted.
- Only **account administrators** can delete users from the system.
- An email address can only be associated with ONE user at a time. You cannot use the same email address for multiple users.

To create an employee, go to **People > Manage Users Home** in ShareFile. Use the **Create Employee** button to begin creating an employee user.

Type your user's name, email address, and company info. Depending on your account type, you can customize the user's individual bandwidth limit.

You can customize your new employee's **User Access** and **File** settings. Depending on your account or plan and your own permissions, certain permissions might not be visible or applicable. **User Access** settings are typical access and feature-based permissions you can use to manage your employee's access and abilities on the account.

You can assign folders to your user, and add the user to Distribution Groups. You can also customize the user's permissions to various folders on your account. To grant a user access to a folder, choose the check box beside the folder name.

You can send a Welcome Email to your new user or opt to do so later. This email includes a link to activate their new account.

Resend a welcome email or employee activation link   When a user is added, they are provided an activation link (by email or by a link generated and delivered by the creator). If the newly created user does not access that activation link within 30 days, a new activation link must be sent. When resending an activation link, the previous activation link is deactivated.

To resend the welcome email containing the activation link

1. In ShareFile, go to **Users > Resend Welcome Emails**.
2. Enter your user's email address or name to add them to the To field, or select them from the Address Book.
3. Customize your email message as needed.
4. Click **Send**.

Accounts utilizing SAML   If you have configured a SAML SSO provider on your account and have created an employee user without any admin permissions, the user does not see or is not prompted to change their password within the activation email. Instead, that user is expected to sign in with their SAML credentials.

Strict employee licensing and company email address   By default, you cannot create a client user with the same email suffix as your company (ex: johndoe@company.com). This option is designed to prevent accounts from circumventing employee licensing requirements.

When a user attempts to create a client user with an employee company email, the user is prompted to send a request to an admin on the account to create the user as an employee.

Admins receive an email notification that allows them to review and approve the user creation request.

Manage employee permissions

ShareFile permissions are designed to give you granular control of your account and the permissions of your users.

Requirements to modify permissions

- The **delegate administrator privileges to other employee users** permission or **Manage Employee Users** permission.
- Employee users might only give or edit the permissions that they themselves have been given.

How to manage permissions

1. In ShareFile, go to **Users > Manage Users Home**.
2. Browse or search for your user. Choose the user or the **Manage** icon on the right to open the user profile.
3. Change permissions as needed, then **Save**.

Default employee permissions   When creating an employee, the following permissions are granted by default. You can change these settings during the user creation process.

Note:

A gray setting indicates a permission that the creating user does not have access to or is not permitted to give to others, so they cannot grant that permission to another user.

Basic information

- Created - Date account is created.
- Email Address - The user's email address.
- First Name
- Last Name
- Company name
- Notifications - Change the user's default **Notification Frequency** settings.
- Default email language - Change the user's default **Email Notification Language**.
- Password - When a user wants to change their password, they can use the **Forgot Password** link on the sign-in screen. If the link is not marked, they need to contact an employee who can manage employee permissions for help with signing in.
- Bandwidth limit - You can choose a maximum monthly bandwidth allowance for the employee. This limit prevents the employee from personally uploading and downloading more data than you allow. It also applies to all of their folders, so that they cannot share files with others more than you would like. Employee bandwidth limits can also affect clients that the employee sup-

ports by limiting how much they can download from the employee's folders. Bandwidth limits are used by accounts where employee use might need to be limited to prevent bandwidth overages.

- Authentication - This setting is offered if the customer is using ShareFile credentials or two-step verification.

Access personal settings   In personal settings, a user can manage their name, company name, and avatar. They are able to update or change their password on this page if they have the permission to change their password.

Access Company Account Permissions   Advanced Preferences are account-wide settings that can be turned on or off by an employee user granted the **Access Company Account Permissions** permission. These settings can be found at **Manage > Advanced Preferences**.

Create Client   Create an external client with limited access to shared folders.

Requirements to create an external (client) user

- Any employee user can go to **People** > **Browse Client** > **Add Client** to send an email request to a prospective client.
- The **Manage client users** permission.
- Changing an external (client) email address or deleting an external (client) user from the system both require the **Manage employee users** permission.

To create an external (client) user, navigate to **Users > Manage Users Home**. Select the **Create Client**. The **Create New Client** screen displays.

You can assign folders to your user, and add the user to distribution groups. You can also copy folder permissions from an existing user to your new one. Using the **Copy Folder Access** option copies only folder permissions, not account permissions.

You can then send a welcome email to your new user, or opt to do so later. This email includes a link to activate their new account.

Give User Access to Folders   You can also create a client user from the **Add People to Folder** menu. A client user is created if you add an individual to a folder that is not currently a member of your account.

1. Click the name of the folder where you would like to grant the new user access.
2. Access the **People** tab or the folder access menu.
3. Click the **Add People to Folder** button.

4. Click **Create New User** to add a client user to your account with access to this specific folder.
5. The user's email address, first name, and last name are required. The user is created as a client user and added to the list of users in the pane on the left.
6. Check the **Notify Added Users** option in the bottom right.
7. Save the changes. Your user then receives an email notification that they have been added to the folder and must activate their account.

Send to specific people   **Send to specific people** allows you to send your files using ShareFile email system. With this method, the recipient receives an email message containing a secure link to download the files. You can send a file stored on your account, or send a file stored on your computer.

See Send to specific people for more information.

Browse Employees

From ShareFile, click **People > Browse Employees** and locate the employee user. Click their name to access their profile page.

Browse Clients

From ShareFile, click **People > Browse Clients** and locate the client user. Click their name to access their profile page.

Shared Address Book

The Shared Address Book is shared across all employee users. This address book can be accessed when you are adding users to folders or quickly sending a file.

Distribution Groups

When setting up a new Distribution Group, users can share the group with all employees. If this permission is enabled, the employee user is able to add more users to a group that has been created on the system and shared with others.

Resend Welcome Emails

> **Note:**
>
> If you need to resend an existing user an activation email, you will need the **Manage employees**

> or **Manage clients** permission.

To resend the welcome email containing the activation link:

1. In ShareFile, go to **People > Resend Welcome Emails**.
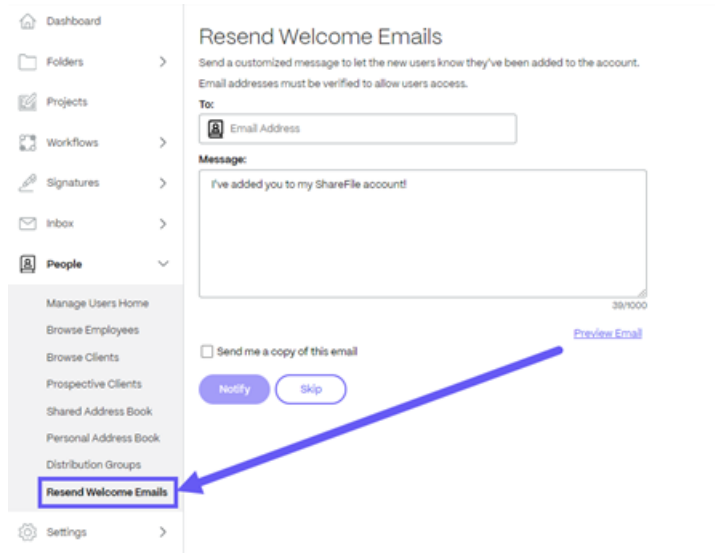
2. Enter your user's email address or name to add them to the To field, or select them from the address book.

3. Customize your email message as needed.

4. Select **Send**.

ShareFile Web

April 25, 2023

ShareFile is a file sharing service that enables users to easily and securely exchange documents.

ShareFile helps you exchange files easily, securely and professionally with secure data sharing and storage, customizable usage and settings, and tools that allow you to collaborate more easily and get your work done.

For information about new features, see What's new.

System requirements

ShareFile is accessible by any computer with a supported web browser and an internet connection. In order to utilize all features and functions of the ShareFile web application, we recommend the fol-

lowing browser types:

- **Microsoft Edge** - Latest version

  > **Notes:**
  >
  > – Due to a known Microsoft issue, CIFS connectors cannot be accessed from the Microsoft Edge browser when utilizing NetScaler for authentication.
  > – ShareFile password reset uses the reCAPTCHA tool for verification. reCAPTCHA is not supported by Microsoft Edge. See ShareFile No Password Reset in Microsoft Edge for more information.

- **Mozilla Firefox** - Latest version

- **Google Chrome** - Latest version

- **Apple Safari** - Version 10 through latest version

  > **Note:**
  >
  > Due to issues with displaying certain folders and menus, the ShareFile web application may not be accessible via Safari in **Private Browsing** mode.

Fixed issues

Fixed issues in 22.0615

- Expiration dates for uploaded files might not update correctly when using **Get A Link**. [SFWEB-13309]

Fixed issues in 21.1210

- File details might not display for some uploaded files. [SFPLATFORM-14977]
- Moving files using Citrix Files for Windows might cause an error. [SFPLATFORM-15008]
- Attempts to save account preferences might fail. [SFWEB-13173]

Fixed issues in Files 21.1007

- File requests might fail when invalid recipients are included. [SFPLATFORM-14852]

Fixed issues in 21.0813

> **Note:**
>
> Releases for Files in Citrix Workspace now incorporate the date into the release version number. Multiple releases are provided at the end of the week.

- Clients created in some Content Collaboration acounts might not receive an activation email. [SFPLATFORM-14323]

Fixed issues in 21.26

- Attempts to link Cloud licenses might cause Premium Plan customers to lose electronic signature capability. [SFPLATFORM-14198]
- Bounce notifications might not be received after Welcome Emails are sent to bad addresses. [SFPLATFORM-14208]
- Attempts to change the account wide retention policy might fail. [SFWEB-13094]
- When uploading an updated file with the same name but different case, the correct versioning of the file might fail. [SFWEB-13095]

Fixed issues in 21.22

- Attempts to copy files in the same storage zone might fail. [SFPLATFORM-14183]
- Attempts to delete files or folders created by the user might fail. [SFPLATFORM-14177]

Fixed issues in 21.21

- Attempts to update your account with a new credit card might fail. [SFWEB-13080]

Fixed issues in 21.20

- Attempts to send an encrypted email in the WebApp or Citrix Files for Outlook might fail. [CCCHELP-524]

Fixed issues in 21.14

- Accessing .mp4 files might not trigger a notification to the file owner. [SFPLATFORM-13955]
- When you enable restricted sharing for connectors, you might lose the ability to edit link options. [SFWEB-12728]
- Some .jpg files do not display correctly in preview. [SFWEB-13040]

Fixed issues in 21.9

- The download access setting might display the option of "29 days"in error. [SFWEB-13024]

Fixed issues in 21.4

- During parallel syncs, attempting to pause a multiple file upload might not work. [SFWEB-12983]

Fixed issues in 21.1

- This release addresses several issues that help to improve overall performance and stability.

Known issues

Known issues in 21.1

No new issues have been observed in this release.

Known issues in 20.31

No new issues have been observed in this release.

Known issues in 20.30

No new issues have been observed in this release.

Citrix Files apps

November 9, 2022

Citrix Files helps you exchange files easily, securely and professionally.

Designed for business, Citrix Files is a file manager that offers secure data sharing and storage, customizable usage and settings, award-winning customer service, and tools that allow you to collaborate more easily and get your work done from any device —anytime, anywhere.

With your Citrix Files account and app, you can:

Access:

- Access files and folders located in your Citrix Files account.
- Edit files located in your Citrix Files account (not available on all plans).
- Download and upload files between your Citrix Files account and your local device.
- Sync files in your Citrix Files account from all of your devices.

Share:

- Share or sync multiple files with multiple users at once.
- Request files and provide secure links for recipients to upload files to your Citrix Files account.

Manage:

- Set custom access permissions to files and folders for individual users.
- Specify a passcode for additional protection for your Citrix Files account.
- Add users to existing folders in your Citrix Files account.

To download Citrix Files for your operating system, see below:

- Windows
- Mac
- Android
- iOS
- Outlook (Windows)
- Gmail

> **TIP:**
>
> Visit the Citrix User Help Center for Citrix Files user guidance.

Supported languages

Citrix Files supports the following languages:

- Dutch

- English

- French

- German

- Japanese

- Korean

- Portuguese

- Russian

- Simplified Chinese

- Spanish

Configure apps

January 4, 2024

Authentication to network share and SharePoint connectors

Citrix Files users can access their existing data repositories such as network shares and SharePoint by creating and accessing connectors.

For information on creating and managing connectors for your account, see Create and manage storage zone connectors.

> **Note:**
>
> This configuration applies only to Citrix Files for Windows, Citrix Files for Mac, and Citrix Files for Outlook.

Manual user sign on to connectors

When browsing to a network share or SharePoint connector, you must first log on (unless you are using single sign-on. To log on, right-click the connector name and choose **Sign in** from the Windows or macOS context menu.

After you select **Sign in**, you are presented with a login dialog. Enter your domain user name and password. After logging on, you can browse your connector folders.

Single sign-on to connectors using Citrix Workspace app

When logged on to Citrix Workspace app, you are automatically signed into the connector without the need to provide credentials again. The use of single sign-on to connect to network shares or SharePoint connectors using Workspace authentication requires storage zones controller version 5.4.1 or later.

In addition to installing Citrix Files for Windows or Mac, Citrix Workspace app must be installed on the endpoint and configured for the Citrix Workspace account.

Single sign-on to connectors using VDA authentication

When accessing connectors inside a VDA session through Citrix Workspace, users will be automatically signed into the connector without a need to provide credentials. In order to use single sign-on to network shares or SharePoint connectors using Workspace authentication inside a VDA environment, storage zones controller 5.4.1 or later is required.

Group policy definitions for Citrix Files for Windows

> Note:
>
> The following information was previously published on Knowledge Center article CTX228273.

Citrix Files includes policy definitions that can be used to push out settings and configuration using Group Policy (GPO). The .admx and .adml files are at `C:\Program Files\citrix\Citrix Files\PolicyDefinitions`

Installation

1. Copy the .admx file to `c:\Windows\PolicyDefinitions` and the \en-us\ .adml file to `c:\Windows\PolicyDefinitions\en-us\`

2. Open Group Policy Editor and the policy options are available under:

   a. **Computer Configuration → Administrative Templates → Citrix Files**

   b. **User Configuration → Administrative Templates → Citrix Files**

Configuring the group policies

Setting	Purpose
Computer Configuration	
Enable Application	If disabled, Citrix Files exits before mounting any drives or displaying any UI.
Enable Auto Check-out	If enabled, Citrix Files automatically checks out Microsoft Office files when they are opened. The files are also automatically checked in after they are closed.

ShareFile

Setting	Purpose
Enable on-premises Connectors	If disabled, Network Share, Sharepoint, and Documentum connectors are not visible in Citrix Files.
Enable Clear Cache on Logout	If disabled, Citrix Files will not clear cached metadata and content when users log out.
Enable Personal Cloud Connectors	If disabled, Personal Cloud and Office 365 Connectors are not visible in Citrix Files.
Enable Auto-update	If disabled, Citrix Files does not automatically update to the latest version.
Delete Cache on Exit	If enabled, downloaded file contents are removed when the application exits.
Cache Size	Controls how much disk space (in MB) to use for cached files. The minimum cache size is 256 MB and the maximum is 9999 MB.
Cache Location	Configures the location of the file content cache. By default, the location is `AppData\Local\Citrix\Citrix Files\PartCache`. If a custom path is set, that folder must exist.
Cache Mode	**Default:** Citrix Files chooses a cache mode appropriate for the environment where it is executing. **Immediate:** Citrix Files writes and reads directly to and from its cache. This mode uses the least memory, but might be slow if the application cache is not on the local disk. **Queued:** Citrix Files retains some data in memory and writes to its cache in the background. This mode is recommended if the application cache is stored on a network location.
Maximum Log Size	Controls how much disk space (in MB) is used for application logs.
Disable Tutorial	If enabled, Citrix Files does not show the tutorial on the initial sign-in of the user.
Enable Offline Access	If disabled, users can't mark folders or files to be available while not connected to the internet.

Setting	Purpose
Prefetch Metadata	If enabled, Citrix Files preloads its filesystem structure. This improves responsiveness at the expense of some CPU, memory, disk, and network usage. By default, this functionality is disabled on virtual desktops.
User Configuration	
Account	Configures the account to use for Citrix Files.
Enable Application	If disabled, Citrix Files exits before mounting any drives or displaying any UI.
Excluded from Upload	File name extensions that are not saved back to Citrix Files. These files can still be read and edited locally.
Mount Point 1–10	Mounts a specific Citrix Files folder as a network drive.

Mount Points

Mount points let you specify a Citrix Files folder to mount as a network drive. You can specify up to 10 mount points. Mount points can be configured through the group policy editor.

To create a mount point, specify the Citrix Files folder by the path to that folder, separated by the \ character. The top-level folder name might vary across user types and across different end-user languages. In such cases, you can create the mount point using %wildcard% alias as outlined in the following examples.

Folder type	Example
Personal Folders	Personal Folders or %personal%
Shared Folders	Shared Folders or %shared%
Favorites	Favorites or %favorites%
Network Shares connector	Network Shares or %networkshares%
SharePoint connector	SharePoint or %sharepoint%
Box connector	Personal Cloud\Box or %personalcloud%\Box
Dropbox connector	Personal Cloud\Dropbox or %personalcloud%\Dropbox

Folder type	Example
Google Drive connector	Personal Cloud\Google Drive or %personalcloud%\Google Drive
OneDrive connector	Personal Cloud\OneDrive or %personalcloud%\OneDrive
Office365 connectors	Office 365 or %office365%
Root of account (default view)	"\"

Citrix Files for Android

September 1, 2023

Citrix Files for Android helps you exchange files easily, securely and professionally.

Citrix Files for Android is a file manager that offers secure data sharing and storage. Citrix Files offers customizable usage and settings allowing you to collaborate more easily and get your work done from any Android device —anytime, anywhere.

Download Citrix Files for Android at Google Play Store

For information about new features, see What's new.

System requirements

OS requirements

Android 7.0 (Nougat) or later

Fixed issues

Fixed issues in 2360

- This release addresses issues that improve overall stability.

Fixed issues in 2320

- Client certificate authentication is updated. [SFAND-5895]

Fixed issues in 2250

- This release addresses issues that improve overall stability.

Fixed issues in 2230

- Attempts to authenticate using **Secure Mail** might cause the Citrix Files application to fail. [SFAND-5819]

Fixed issues in 2220

- This release addresses issues that improve overall stability.

Fixed issues in 21120

- Attempts to sign on to the Citrix Files application might cause an error. [CCCHELP-2439]

Fixed issues in 21110

- This release addresses issues that help to improve overall performance.

Fixed issues in 2175

- This release addresses issues that help to improve overall performance.

Fixed issues in 2130

- Using Quick Edit for Excel files might produce an errant date format. [CCCHELP-1415]
- Attempts to launch Quick Edit in Citrix Files for Android using SSO might fail. [CCCHELP-1501]

Fixed issues in 20110

- When you launch the Citrix Files app from Citrix Workspace, you might be required to manually sign in to Citrix Files. [SFAND-5454]

Fixed issues in 2080

- This release addresses issues that improve overall stability.

Fixed issues in 2070

- When you launch Citrix Workspace app from Citrix Files, you might be required enter a pin. [SFAND-5407]

88

Fixed issues in 2060

- When accessing a shared link in Secure Mail, Citrix Files for Android might not open. [SFAND-5325]

- Shared anonymous links requiring an email or username might cause an error. [SFAND-5377]

Fixed issues in 2050

This release also addresses issues that help to improve overall performance and stability.

Fixed issues in 2040

- After logging out of Citrix Files for Android, you might receive an error message. [CCCHELP-383]

- When **Notify user that he/she has been added to this folder** is unchecked, the user might receive a notification. [SFAND-5249]

- When offline and requesting files using Citrix Files email, an unknown error might occur. [SFAND-5268]

Fixed issues in 2035

- Launching Quick Edit in Citrix Files for Android might stop the app from working. [CCCHELP-302]

Fixed issues in 2030

- Using Citrix Files for Android to rename files within a network share might cause an unknown error. [XMHELP-2555]

Known issues

Known issues in 2380

When attempting to open a file from **Citrix Files for Android** in your device's Microsoft Office 365 application for the first time, Microsoft Office 365 might fail to launch. We are working with Microsoft to resolve this issue.

Known issues in 2175

No new issues have been observed in this release.

Known issues in 2130

No new issues have been observed in this release.

Known issues in 20110

No new issues have been observed in this release.

Known issues in 2080

No new issues have been observed in this release.

Known issues in 2070

No new issues have been observed in this release.

Known issues in 2060

No new issues have been observed in this release.

Known issues in 2040

No new issues have been observed in this release.

Known issues in 2035

No new issues have been observed in this release.

Known issues in 2030

No new issues have been observed in this release.

Known issues in 2020

No new issues have been observed in this release.

Known issues in 2010

No new issues have been observed in this release.

Citrix Files for Gmail

March 14, 2024

The Citrix Files for Gmail Chrome extension allows you to bypass file size restrictions and add security to your attachments. You can provide a secure file upload request for co-workers, customers, and partner directly from Gmail.

Be notified whenever someone accesses a file or sends you a file so you are always aware of what is going and can take action. You can also set different security and access levels.

Download Citrix Files for Gmail at the Chrome Web Store.

For information about new features, see What's new.

System requirements

Browser requirements

- Ensure users are on the latest version of Google Chrome.

User guidance

Use the following links to access user guidance for Citrix Files for Gmail.

- About
- Access
- Add and enable
- Change default settings
- Request files
- Share files

Fixed issues

Fixed issues in 2.1

- Some recipients of shared file links from Citrix Files for Gmail might not have the ability to access the file. [SFGP-175]

Fixed issues in 2.0

There are no fixed issues in this release.

Known issues

Known issues in 2.0

No new issues have been observed in this release.

Citrix Files for iOS

July 11, 2023

Citrix Files for iOS helps you exchange files easily, securely and professionally.

Citrix Files for iOS is a file manager with tools that allow you to collaborate easily and get your work done from any iOS device —anytime, anywhere.

Download Citrix Files for iOS at Apple App Store.

For information about new features, see What's new.

System requirements

OS requirements

iOS 14 or later

Fixed issues

Fixed issues in 2370

- When sending a watermarked file to specific people, the watermark might not display. [SFIOS-7208]

- When sending a watermarked file to specific people, if the sign in option isn't checked, information might improperly display. [SFIOS-7209]

- Selecting **Add a link** several times might cause an error. [SFIOS-7214]

- The **Add watermark** option isn't available in **Edit options**. [SFIOS-7215]

- Opening a shared file in co-editing might cause an error. [SFIOS-7216]

- When opening a file for view, the **Share** option doesn't work. [SFIOS-7219]

- Opening a checked out file with download permission might cause an error. [SFIOS-7233]

Fixed issues in 2360

- Creating a duplicate link might not deactivate the share link option. [SFIOS-7164]

- When sharing multiple files, the file list might display the entire list before selecting **Show all**. [SFIOS-7172]

- **Date added** might not display for photo and video uploads. [SFIOS-7199]

Fixed issues in 2355

- This release addresses issues that improve overall stability.

Fixed issues in 2350

- This release addresses issues that improve overall stability.

Fixed issues in 2340

- This release addresses issues that improve overall stability.

Fixed issues in 2320

- This release addresses issues that improve overall stability in XenMobile iOS.

Fixed issues in 2310

- This release addresses issues that improve overall stability.

Fixed issues in 22125

- This release addresses issues that improve overall stability.

Fixed issues in 2212

- This release addresses issues that improve overall stability.

Fixed issues in 2290

- Attempting to print Microsoft Office files might cause an error. [CCCHELP-2654]

Fixed issues in 2250

- This release addresses issues that improve overall stability.

Fixed issues in 2220

- Some PDF file annotations do not display until file content is tapped. [SFIOS-6768]

Fixed issues in 2210

- The number keypad alignment might be off when entering a pin. [SFIOS-6801]

Fixed issues in 21115

- This release addresses several issues that help to improve overall performance.

Fixed issues in 21110

- Adding people to a folder might cause Citrix Files to exit unexpectedly. [SFIOS-6794]

Fixed issues in 2190

- This release addresses several issues that help to improve overall performance.

Fixed issues in 2185

- This release addresses several issues that help to improve overall performance.

Fixed issues in 2175

- This release addresses several issues that help to improve overall performance.

Fixed issues in 2170

- This release addresses several issues that help to improve overall performance.

Fixed issues in 2150

After editing a video in the Photos for iOS app, attempting to upload the video might fail. [SFIOS-6684]

Fixed issues in 2120

- We are now integrating the Authman Lite SDK into Citrix Files to provide a more seamless experience across apps. [SFIOS-6303]
- This release also includes general security and user improvements. [SFIOS-6640]

Fixed issues in 2110

This release addresses several issues that help to improve overall performance and stability.

Fixed issues in 20112

Editing and saving a PowerPoint document might cause Citrix Files to exit unexpectedly. [SFIOS-6595]

Fixed issues in 20110

- Attempting to open files with the view only permission might cause an error. [CCCHELP-997]
- When accessing a shared link created in Citrix Files for Windows, Citrix Files for iOS might display an error. [CCCHELP-1096]
- PDF notes written with an iPad pen might be visible only on other iOS devices. [CCCHELP-1147]
- In Citrix Files for iOS, the **Cancel** button might not be localized. [SFIOS-6359]
- When opening a shared file from a non-linked Citrix Workspace account, Citrix Files might cause Citrix Workspace app to exit unexpectedly. [SFIOS-6590]

Fixed issues in 20100

- Hand written notes in Citrix Files might degrade after multiple saves. [CCCHELP-272]
- Opening a verified DocuSign PDF might cause an error. [CCCHELP-649]
- Canceling a print screen might disable the **Save** option. [SFIOS-6461]

Known issues

Known issues in 2120

Editing a text file might cause Citrix Files for iOS to fail. [SFIOS-6603]

Known issues in 2110

Editing a text file might cause Citrix Files for iOS to fail. [SFIOS-6603]

Known issues in 20112

Editing a text file might cause Citrix Files for iOS to fail. [SFIOS-6603]

Known issues in 20110

- Editing a PowerPoint document might cause Citrix Files for iOS to fail. [SFIOS-6595]
- Editing a text file might cause Citrix Files for iOS to fail. [SFIOS-6603]

Known issues in 20100

No new issues were observed in this release.

Citrix Files for Mac

March 14, 2024

Citrix Files for Mac allows you to access your files directly through a mapped drive, providing a native Finder experience. Files are downloaded only when accessed, and temporarily stored on your computer. Changes made to the files are automatically saved back to the cloud. You can access more functionality through the right-click context menu and perform operations such as sharing or requesting of files.

> **Important:**
>
> For information regarding Citrix Files for Mac and Apple Silicon, see Citrix Files for Mac and Apple Silicon.

For information about new features, see What's new.

For end-user help including downloading and sign in, see Citrix User Help Center.

Supported versions

Minimum supported version

- Citrix Files for Mac v 22.1 or later

Download the latest version of Citrix Files for Mac at ShareFile Downloads.

System requirements

OS requirements

- macOS 10.13 Sierra or later

Other requirements

- Local administrator rights are needed to install the app.

Fixed issues

Fixed Issues in 23.3

- Citrix Files for Mac authentication for connectors might fail. [CFMAC-3401]

Fixed Issues in 22.10

- This release addresses issues that help to improve overall performance.

Fixed Issues in 22.4

- Citrix Files for Mac authentication prompt might not display when Citrix Workspace is installed. [CFMAC-3296]

Fixed Issues in 22.2

- Citrix Files for Mac might not complete an interrupted download. [CFMAC-3296]

Fixed Issues in 21.10

- Citrix Files for Mac might not launch after sign-on. [CFMAC-3224]
- Some items might not display correctly in the **Queue** tab. [CCCHELP-1355]
- Citrix Files for Mac might become unresponsive after authentication errors. [CFMAC-3260]
- Opening and editing some Adobe Creative Suite files might cause an error. [CFMAC-3228]
- Opening and editing some Vectorworks files might cause an error. [CFMAC-3228]

Fixed issues in 21.2

- The option to discard a checkout might not be available for administrators. [CCCHELP-1022]
- Some failed uploads might require a manual retry. [CCCHELP-1291]
- Some folder names containing a period might be treated as temporary files. [CCCHELP-1456]
- Some remote updates might not show in **Finder**. [CFMAC-3185]
- Client users with delete permission might not have the ability to use it. [CFMAC-3193]

Fixed issues in 20.9

- Saving Adobe Photoshop files might cause an error. [CFMAC-3179]
- When saving Adobe InDesign project files, the files might delete unexpectedly. [CFMAC-3179]

Fixed issues in 20.7.2

- This release addresses a number of issues that help to improve overall performance and stability.

Fixed issues in 20.7

- When editing a file in Catalina, the Finder icon might not appear. [CFMAC-3069]
- When saving Adobe After Effects project files, the files might delete unexpectedly. [CFMAC-3128]
- Attempts to edit a file in Adobe Photoshop might cause an error. [CFMAC-3128]
- When signing into a previously used Mac, a new device sign-in notification might be sent. [CFMAC-3137]
- Using Citrix Files for Mac might require you to re-authorize the application multiple times. [CFMAC-3158]

Fixed issues in 1911

- This fix addresses a sharing violation error that appeared on Microsoft Excel files. [CFMAC-3067]
- When using macOS Catalina, files might download to the cache when the user browses through the folder. [CFMAC-3076]

Fixed issues in 1910

- Moving the cache limit slider might toggle the beta flag on and off instead of changing the cache limit. [CFMAC-3045]
- Dutch localization might not display correctly. [CFMAC-3056]

Fixed issues in 1908

- Moving a subfolder and then deleting its parent folder might cause the subfolder to be removed. [CFMAC-2249]

Fixed issues in 1904

- Citrix Files for Mac might consume an excessive amount of CPU. [CFMAC-2719]
- Attempts to open files from the dashboard can fail for files that have not been opened previously. [CFMAC-2738]
- When editing a file or folder offline and going back online, the file might not be moved to a recovery folder. [CFMAC-2762]
- Users might have to reauthenticate by relaunching the app. [CFMAC-2765]
- Deleting files during offline sync might cause Citrix Files for Mac to exit unexpectedly. [CFMAC-2787]

Fixed issues in 4.6

- Citrix Files for Mac might exit unexpectedly when switching from dark to light mode or light to dark mode. [CFMAC-2661]
- Locally edited files might not update correctly if there's a new remote version. [CFMAC-2676]
- The database crawler might look up items without caching, which can consume a lot of CPU. [CFMAC-2684]
- File and folder might not stay up to date. [CFMAC-2695]

Known issues

Known issues in 21.10

Users who have Citrix Files v21.4 (19rc5) are required to manually install Citrix Files 21.10 for Mac.

Known issues in 21.2

- Users on Big Sur might be required to reboot several times to allow the extension. This known issue should be resolved with the release of Big Sur 11.3.

Known issues in 20.7

- This release includes partial Italian language support. Full Italian language support will be included in a future release. [CFMAC-3130]
- Authentication screens do not include Italian language support.

Known issues in 1911

- A file might not delete properly if it is open in another application. As a workaround, close all applications accessing a file before deleting it. [CFMAC-2998]

Known issues in 1910

- A file might not delete properly if it is open in another application. As a workaround, close all applications accessing a file before deleting it. [CFMAC-2998]

Known issues in 1908

- A file might not delete properly if it is open in another application. As a workaround, close all applications accessing a file before deleting it. [CFMAC-2998]

Known issues in 1904

- When opening and editing Adobe InDesign files, Citrix Files for Mac might not save the files and cause Adobe InDesign to exit unexpectedly. [CFMAC-2552]
- When installing Citrix Files for Mac for the first time, a kernel extension approval dialog appears.
- Restricted Zones are not supported. [SFWGTM-515]
- When using offline access, folders might not copy properly. [SFWGTM-2145]
- Items in the dashboard might not open when double-clicked. [SFWGTM-2387]

Known issues in 4.6

- When opening and editing Adobe InDesign files, Citrix Files for Mac might not save the files and cause Adobe InDesign to exit unexpectedly. [CFMAC-2552]
- When installing Citrix Files for Mac for the first time, a kernel extension approval dialog appears.
- Restricted Zones are not supported. [SFWGTM-515]
- When using offline access, folders might not copy properly. [SFWGTM-2145]
- Items in the dashboard might not open when double-clicked. [SFWGTM-2387]

Known issues in 4.5

- When opening and editing Adobe InDesign files, Citrix Files for Mac might not save the files and cause Adobe InDesign to exit unexpectedly. [CFMAC-2552]
- When installing Citrix Files for Mac for the first time, a kernel extension approval dialog appears.
- Restricted Zones are not supported. [SFWGTM-515]
- When using offline access, folders might not copy properly. [SFWGTM-2145]
- Items in the dashboard might not open when double-clicked. [SFWGTM-2387]

Known issues in 4.4

- When installing Citrix Files for Mac for the first time, a kernel extension approval dialog appears.
- Restricted Zones are not supported. [SFWGTM-515]
- When using offline access, folders might not copy properly. [SFWGTM-2145]
- Items in the dashboard might not open when double-clicked. [SFWGTM-2387]

Known issues in 4.3

- When installing Citrix Files for Mac for the first time, a kernel extension approval dialog appears.
- Restricted Zones are not supported. [SFWGTM-515]
- When using offline access, folders might not copy properly. [SFWGTM-2145]
- When using offline access, in-progress badges for files and folders might take longer than usual to update. [SFWGTM-2310]

Limitations

- Several features are temporarily disabled while there is no internet connectivity. These features will become available again when internet connectivity is restored.
- Restricted Zones are not supported.
- When opening and editing Adobe InDesign files, Citrix Files for Mac might not save the files and cause Adobe InDesign to exit unexpectedly.
- When using offline access, folders might not copy properly.
- Items in the dashboard might not open when double-clicked.

Citrix Files for Outlook

March 14, 2024

Citrix Files for Outlook allows you to bypass Outlook's file size limit on attachments and add security to your attachments or emails. You can provide a secure file upload request directly in your email.

Citrix Files for Outlook provides notifications to alert you when someone accesses a file or sends you a file. You can also set different security and access levels on a file-by-file basis.

For information about new features, see What's new.

Supported versions

Minimum supported version

- Citrix Files for Outlook v 22.1.10.0 or higher

Download Citrix Files for Outlook at Citrix Downloads.

System requirements

OS requirements

- Windows 10 or later

.NET requirements

- Microsoft .NET Framework 4.7.1 or later

Microsoft Outlook version requirements

- Microsoft Outlook 2007, 2010, 2013, 2016, 2019 (32-bit and 64-bit).
- Office 365 plans that include full, installed Office applications.

> **Note:**
>
> The local version of the plug-in is not compatible with Microsoft Outlook Express, Outlook for Mac, or web-based Outlook.

Citrix Content Collaboration requirements

- A Citrix Content Collaboration Advanced, Premium, or Virtual Data Room plan.
- User must be an Employee user on the account.

Fixed issues

Fixed issues in 22.7.5

- When viewing encrypted emails, Outlook might shutdown unexpectedly. [SFOLP-1531]

- Multiple login prompts might occur when opening new compose window. [SFOLP-1532]

- WebView2 might not install an update if the previous version is too old. [SFOLP-1533]

Fixed issues in 22.4

- Failure to send error message might not display after a failed encrypted email. [SFOLP-1525]

- The ability to install WebView2 twice might occur. [SFOLP-1528]

Fixed issues in 22.1

No fixed issues in this release.

Fixed issues in 21.10

- Resending a message with an attachment might fail. [SFOLP-1484]

Fixed issues in 21.9

- Sending encrypted emails might fail. [SFOLP-1474]
- Attempting a reauthentication, the authentication might fail. [SFOLP-1481]
- If sending a file when not signed into Citrix Files, the message might not work properly. [SFOLP-1485]
- When replying to emails, the Outlook reply window might go out of focus. [SFOLP-1494]
- Outlook Today feature might be disabled now that Internet Explorer is the default browser for Outlook. [SFOLP-1501]

Fixed issues in 6.7

- Changing networks might cause an error with Citrix Files for Outlook. [SFOLP-1369]
- When using the German version, starting a workflow might result in a wrong description. [SFOLP-1458]
- Attaching files to an encrypted email might cause an error. [SFOLP-1460]
- RTF formatted emails with photo attachments might fail on delivery. [SFOLP-1463]

Fixed issues in 6.6

- When dragging files into Citrix Files for Outlook, some files might not convert. [SFOLP-1436]
- Attempts to sign into Citrix Files for Outlook might fail when using Outlook 2013 and Outlook 2019. [SFOLP-1437]
- The options window might display with errors when using a resolution smaller than 1280 x 960. [SFOLP-1438]
- Attempts to re-open the Citrix Files for Outlook sign-in window might fail. [SFOLP-1447]

Fixed issues in 6.5.1

- The banner might not localize when attaching a file for the first time after changing the language under the "Encryption" toggle button. [SFOLP-1306]

- After attaching a file, the "Insert File" window might pop up again after the file is loaded. [SFOLP-1396]
- The English language might not show up as an available option when operating system culture is set to another country. [SFOLP-1398]
- "Convert Attachments" might not be disabled when the user isn't authenticated. [SFOLP-1399]
- Citrix Files for Outlook add-in might crash when building a culture list. [SFOLP-1401]

Fixed issues in 6.5

- Attachments might get converted to Citrix Files attachments even if the user is not signed in. [SFOLP-1307]
- Closing a folder that is still loading might display an incorrect folder when reopened. [SFOLP-1334]
- Attachments might be added as Citrix Files attachments even if the user is not signed in. [SFOLP-1355]
- Authentication intermittently fails when launching Outlook. [SFOLP-1360]

Fixed issues in 6.4

- The icon that displays on the welcome message after installing a new version of Citrix Files for Outlook might be pixelated. [SFOLP-1042]
- Users might have to manually authenticate again after using single sign-on to sign in. [SFOLP-1152]

Fixed issues in 6.3.1

- Recipients might not be able to access shares that require logon. [SFOLP-1051]

Fixed issues in 6.3

- When logging out from Citrix Workspace app, Citrix Files for Outlook might remain logged in. [SFOLP-1020]
- Citrix Files for Outlook might prompt to log on frequently. [SFOLP-1025]
- Attachments might auto-convert even if you are not logged on. [SFOLP-1046]
- Launching Microsoft Outlook after 15 minutes in a Citrix Virtual App or Citrix Virtual Desktop session would prompt for logon instead of using single sign-on. [SFOLP-1048]
- Top-level personal cloud connector folders can be selected to share. [SFOLP-1092]
- When personal cloud connectors are not configured, an empty logon page appears. [SFOLP-1093]

- Some settings are preserved after tokens have expired and a different user has logged on. [SFOLP-1128]

Fixed issues in 6.2

- Items might fail to attach if the email is saved as a draft. [SFOLP-984]
- The Custom Settings dialog might appear at the bottom of the screen. [SFOLP-990]
- The Citrix Attachments banner might appear outside of an email window. [SFOLP-1006]
- Special characters might not be allowed in email addresses. [SFOLP-1014]
- When using the per-machine install option, a "Browser out of date" prompt might appear after entering a subdomain. [SFOLP-1018]

Known issues

Known issues in 6.5

No new issues have been observed in this release.

Known issues in 6.4

No new issues have been observed in this release.

Known issues in 6.3.1

No new issues have been observed in this release.

Known issues in 6.3

No new issues have been observed in this release.

Known issues in 6.2

No new issues have been observed in this release.

Citrix Files for Outlook Online

March 14, 2024

Citrix Files for Outlook Online allows you to bypass file size restrictions and add security to your attachments or emails by sending them through Citrix Files. You can provide a secure file upload request for co-workers, customers, and partners directly in your email.

Be notified whenever someone accesses a file or sends you a file so you are always aware of what is going and can take action. You can also set different security and access levels on a file-by-file basis for greater control.

Download Citrix Files for Outlook Online at Microsoft AppSource or through the Store icon in the Outlook Online ribbon.

For information about new features, see What's new.

> **Note:**
>
> Citrix Files for Outlook Online works with macOS and Microsoft Office for Mac.

System requirements

Microsoft account requirements

- Outlook.com
- Office 365
- Microsoft Exchange

    - 2013 SP1
    - 2016

Outlook requirements

- Outlook WebApp
- Outlook for Mac 2016 or later (version 15.33 or later)
- Outlook for Windows 2013 or later is supported
- For more information, see Microsoft Office requirements

Citrix Content Collaboration requirements

- A Citrix Content Collaboration Advanced, Premium, or Virtual Data Room plan.
- User must be an Employee user on the account.

Browser requirements

- Chrome (latest version)
- Firefox (latest version)
- Safari (latest version)
- Edge (latest version)
- Internet Explorer 11

Fixed issues

Fixed issues in 2.0.3

There are no fixed issues in this release.

Known issues

Known issues in 2.0.3

No new issues have been observed in this release.

Citrix Files for Windows

March 14, 2024

Citrix Files for Windows allows you to access your files directly through a mapped drive, providing a native Windows Explorer experience. Files are downloaded only when accessed, and temporarily stored on your computer. Changes made to the files are automatically saved back to the cloud. You can access more functionality through the Windows right-click context menu and perform operations such as sharing or requesting of files.

For information about new features, see What's new.

Supported versions

Minimum supported version

- Citrix Files for Windows v 22.1.0 or higher

Download the latest version of Citrix Files for Windows at Citrix Downloads.

System requirements

OS requirements

- Windows 10 or later
- Windows Server 2012 R2 or later

VDA requirements

- XenApp and XenDesktop 7.15 LTSR, XenApp and XenDesktop 7.18, or Citrix Virtual Apps and Desktops 7 1808 or later

Other requirements

- Local administrator rights are needed to install the app.
- .NET 4.7.1 Framework is required

Fixed issues

Fixed issues in 23.4

- Saving Excel files using OneDrive for Business connector might cause a file conflict. [SFWIN-3381]
- Google Drive connector might not mount initially. [SFWIN-3388]
- Desktop icons might not display properly. [SFWIN-3392]
- Adding a client user to a folder might cause an error. [SFWIN-3409]
- Renaming a connector folder might cause an error. [SFWIN-3419]
- Renaming a connector folder remotely might cause an error. [SFWIN-3455]
- Renaming desktop icons might cause a position change. [SFWIN-3457]

Fixed issues in 22.11

- Clicking the reset button in the **Sync** window might not release the selected folders. [SFWIN-3169]
- Selecting **Cancel** after modifying a folder in **Sync** might fail. [SFWIN-3358]
- Modifying a folder in **Sync** to "Make online only"might cause an error. [SFWIN-3358]
- Uploading a file might cause a conflict if a previously deleted file had the same name. [SFWIN-3363]
- Saving to a sub-folder might cause a permission error to display. [SFWIN-3364]

Fixed issues in 22.8

- **Clone user** checkbox might not work when adding folder permissions.[SFWIN-3325]
- CBFS driver might remain after new installation of Citrix Files for Windows. [SFWIN-3331]
- On non-English systems, an assert error box might display. [SFWIN-3337]
- **Get a Link** and **Request a Link** might show invalid access levels based on account settings. [SFWIN-3343]
- Office file changes might cause an inaccurate conflict detection notification. [SFWIN-3345]

Fixed issues in 22.5

- The correct error icon might not display when a network connection is unavailable. [SFWIN-2732]
- The virus status for some files might not display after a refresh. [SFWIN-3269]
- Driver conflicts might occur with Windows Docker containers. [SFWIN-3285]
- Autoupdates might fail to install. [SFWIN-3290]
- The Citrix Files for Windows auto-updater might run cmd.exe indirectly. [SFWIN-3292]
- The Citrix Files for Windows installer might re-install WebView2. [SFWIN-3294]
- When utilizing the **Get a Link** function, the notify task might fail. [SFWIN-3323]

Fixed issues in 22.3

- Checking files in or out within a SharePoint connector folder might cause an error. [SFWIN-3218]
- If the local cache is manually deleted while uploading files, a failure to upload might not display. [SFWIN-3223]
- Modified dates might not display the correct information with saved WordPerfect files. [SFWIN-3241]

Fixed issues in 22.1

- Folders moved remotely might cause an error. [SFWIN-3172]
- Some network share connectors might not display a check out option. [SFWIN-3185]
- Automatic selection of a client certificate might fail. [SFWIN-3190]
- The accidental creation of item names with invalid Unicode characters might cause an error. [SFWIN-3207]
- Files might not update when there is no change in file size. [SFWIN-3212]

Fixed issues in 21.10

- Uploading files with certain Unicode characters might fail. [SFWIN-3145]
- File contents might not be updated when versioning is turned off. [SFWIN-3153]
- **Get a Link** option for connector folders and files might fail. [SFWIN-3168]
- Moving folders might result in high CPU utilization. [SFWIN-3180]

Fixed issues in 21.7

- Attempts to move a folder might cause the application to fail. [SFWIN-3018]
- Files that are renamed remotely might appear twice. [SFWIN-3073]

Fixed issues in 21.5

- A file might display the wrong upload time when accessed in another time zone. [SFWIN-2740]
- After versioning is disabled for a folder, the ability to check files in and out of the folder might continue. [SFWIN-2743]
- The offline sync window might display an incorrect content size. [SFWIN-2760]
- When leaving files open during sign out, the cache might not clear. [SFWIN-2775]
- After signing out, the **Confirm Sign Out** window might remain on the screen after revoking the device. [SFWIN-2778]
- When remotely updating a file, the file might modify the date of the parent folder. [SFWIN-3030]
- Files saved with a CAPS application might not sync to the cloud. [SFWIN-3066]
- The **Manage Folder Permissions** window might not display permission content for some users. [SFWIN-3077]

Fixed issues in 21.2

- Rotating an image file in Windows Photo Viewer might delete the original file. [CCCHELP-376]
- Attempting to connect to CNS servers might fail. [CCCHELP-868]
- Accessing restricted zone folders might cause an authentication issue. [CCCHELP-932]
- Saving AutoCad and AutoCadLT files might not include temp files. [CCCHELP-989]
- Some files and folders created in Citrix Files might not sync. [CCCHELP-1008]
- Authentication might fail causing the error message: "Failed to retrieve two factor backup options, please try again."[CCCHELP-1366]
- Saved AutoCad and AutoCadLT .dwg files in Citrix Files might display as .bak files. [CCCHELP-1369]
- Attempting to sign in using workspace authentication might cause a script error. [CCCHELP-1379]

- Citrix Files for Windows might provide an incorrect URL during a redirect. [CCCHELP-1590]
- Modified AutoCad Revit files might not save to the cloud in Citrix Files for Windows. [SFWIN-3052]
- Using WebView2 might cause a large cache file. [SFWIN-3054]
- WebView2 might suffer compatibility issues during login on older machines. [SFWIN-3063]

Fixed issues in 20.9

- Opening Citrix Files for Windows might cause high memory usage. [SFWIN-2911]
- Cloud contents moved to a new local folder might disappear if the local folder isn't created successfully. [SFWIN-2915]
- Local cache might fail if sign in is unsuccessful. [SFWIN-2916]
- Attempts to create files and folders might fail after an unsuccessful sign-in. [SFWIN-2916]
- Using the overwrite option during a file upload conflict might not work. [SFWIN-2919]
- Authentication might fail in some environments. [SFWIN-2920]

Fixed issues in 20.7

- Attempting multiple edits using Excel might cause an error message. [SFWIN-2809]

Fixed issues in 2032

- Files and folders displaying in Citrix Files for Windows might differ from the WebApp. [CCCHELP-186]
- Some PowerPoint files might lose images when stored with Citrix Files for Windows. [CCCHELP-186]
- Citrix files might error out after logout and synchronization stops working [CCCHELP-186]
- Excel files might be deleted after editing in Citrix Files for Windows. [CCCHELP-68]
- Opening and saving Excel files might cause an error message. [CCCHELP-111]
- Citrix Files for Windows content refresh might cause an error. [CCCHELP-150]
- Changing networks might cause an error with Citrix Files for Windows. [SFWIN-2780]
- Folders in Citrix Files for Windows might display as files. [CCCHELP-55]
- Citrix Files for Windows might fail to download files to a location with a long path name. [SFWIN-2597]
- Overlay icons might not appear consistently on files in connectors. [SFWIN-2610]
- Single sign-on might not work correctly on certain deployments. When this occurs, an error message appears: "We're sorry, access is not allowed because you have out-of-date software." [SFWIN-2641]

- Citrix Files for Windows might display a warning about unsaved changes to files when exiting. [PD-1404]
- SSO might fail using SAML with Azure AD. [SFWIN-2783]

Note:

The user agent during authentication is now: Mozilla/5.0 (Windows NT; Win64; x64; Trident/7.0; rv:) like Gecko NT, is the kernel version of the Windows Operating System and RV is the version of Internet Explorer/Edge installed.

Fixed issues in 1912

- Citrix Files for Windows might fail to download files to a location with a long path name. [SFWIN-2597]
- Overlay icons might not appear consistently on files in connectors. [SFWIN-2610]
- Single sign-on might not work correctly on certain deployments. When this occurs, an error message appears: "We're sorry, access is not allowed because you have out-of-date software." [SFWIN-2641]

Fixed issues in 1909

- The Last Modified Date on folders might not update correctly when changing files inside the folder. [SFWIN-2397]
- Citrix Files for Windows might not save the PDF correctly after editing a file in Adobe Acrobat. [SFWIN-2543]
- Certain Windows applications might exit unexpectedly intermittently. [SFWIN-2559]
- Users are not prompted to authenticate again after failure to authenticate when using network share connectors. [SFWIN-2570]
- Microsoft Office files might be deleted from Citrix Files after saving. [SFWIN-2596]

Fixed issues in 1907

- Citrix Files fail to mount in certain environments. [SFWIN-1775]
- Folders with large image and video files might take longer than normal to load. [SFWIN-2273]
- Offline files might not be accessible if the files remained offline. [SFWIN-2464]
- AutoCAD files with changes might remove older versions of uploaded files. [SFWIN-2470]
- When Citrix Files for Windows is signed in without a network connection, offline files cannot be edited. [SFWIN-2483]

Fixed issues in 5.0

- AutoCAD files might be randomly deleted. [SFWIN-2094]
- When users open a changed file, the content in the file might be outdated. [SFWIN-2132]
- Opening files might incorrectly show a conflict message [SFWIN-2267]
- Exporting a document as a PDF might fail.

Fixed issues in 4.6

- An "Incorrect function"error message appears when accessing the mapped Citrix Files drive. [SFWIN-2009]
- Files saved using Microsoft Edge might not upload correctly. [SFWIN-2113]
- When a user's AppData system variable points to a UNC path, Citrix Files for Windows exits unexpectedly. [SFWIN-2117]
- PDF files might get corrupted when saving. [SFWIN-2120]

Fixed issues in 4.5

- PDF files edited using Bluebeam become corrupted. [SFWIN-1451]
- Citrix Files incorrectly shows "Your access token might be expired or revoked"when logged on to a VDA. [SFWIN-1686]
- After upgrading Citrix Files, the application maps to the wrong drive letter. [SFWIN-1819]
- Saving to a Citrix Files location eventually corrupts the saved file. [SFWIN-1890]
- Disconnecting or changing networks might cause Citrix Files to exit unexpectedly. [SFWIN-1967]

Fixed issues in 4.4

- Citrix Files might consume high memory. [SFWIN-1502]
- When saving a file to Citrix Files, high latency might occur. [SFWIN-1556]
- Users might see outdated versions of files. [SFWIN-1570]
- Citrix Files might perform slowly. [SFWIN-1642]
- Citrix Files might not save .dwg files from AutoCAD. [SFWIN-1669]
- Jupyter Notebooks keep adding new checkpoint folders into Citrix Files. [SFWIN-1676]
- Windows Explorer might freeze when opening a folder. [SFWIN-1707]
- When editing files with Blue Beam, zero-byte files might get uploaded. [SFWIN-1758]
- Moving folders from Citrix Files to the local machine might not transfer files inside the folder. [SFWIN-1782]

Fixed issues in 4.3

- Project files might become corrupt when opened. [SFWIN-1437]
- When storing app data using Fslogix, Citrix Files might not work. [SFWIN-1460]
- When renaming a file before it is fully uploaded to the server, two files might be created locally. [SFWIN-1468]
- When using SAML single sign-on in a VDA, the automatic logon might not work. [SFWIN-1507]
- PDF files might become corrupt when opening or editing. [SFWIN-1509]
- File and folders might be mismatched between Citrix Files remotely and locally. [SFWIN-1524]
- When saving a file to the Citrix Files drive, the drive might write slowly. [SFWIN-1556]
- When right-clicking a file, the context menu might not appear. [SFWIN-1559]
- The Last Modified Date on files might not be consistent. [SFWIN-1670]

Known issues

Known issues in 22.5

No new issues have been observed in this release.

Known issues in 1912

No new issues have been observed in this release.

Known issues in 1909

No new issues have been observed in this release.

Known issues in 1907

No new issues have been observed in this release.

Known issues in 5.0

- Certain third party software might interfere with Citrix Files for Windows'ability to mount the folder structure. For more information and workarounds, see Knowledge Center article CTX250001.
- Citrix Files for Windows fails to mount on Windows 10. A recent Windows update in version 1809 introduced issues with drive mounting. For more information and workarounds on mapped drives and Windows 10 1809, see Windows Support.

- Accessing folders with large amounts of multimedia files causes slow loading times. For workarounds, see Knowledge Center article CTX241253.
- Renaming a file or folder to the same name with different case does not work. [SFWIN-1711]

Known issues in 4.6

- Upgrading from version 4.5 to version 4.6 with Beta features enabled while uploads are occurring cancels those uploads. As a workaround, wait for your uploads to complete before you upgrade.
- Citrix Files for Windows fails to mount on Windows 10. A recent Windows update (version 1809) introduced issues with drive mounting. For more information and workarounds on mapped drives and Windows 10 1809, see Windows Support.
- Accessing folders with large amounts of multimedia files causes slow loading times. For workarounds, see Knowledge Center article CTX241253.
- Renaming a file or folder to the same name with different case does not work. [SFWIN-1711]

Known issues in 4.5

- Citrix Files for Windows fails to mount on Windows 10. A recent Windows update (version 1809) introduced issues with drive mounting. For more information and workarounds on mapped drives and Windows 10 1809, see Windows Support.
- Renaming a file or folder to the same name with different case does not work. [SFWIN-1532]

Known issues in 4.4

- Citrix Files for Windows fails to mount on Windows 10. A recent Windows update (version 1809) introduced issues with drive mounting. For more information and workarounds on mapped drives and Windows 10 1809, see Windows Support.
- Renaming a file or folder to the same name with different case does not work. [SFWIN-1532]

Known issues in 4.3

No new issues have been observed in this release.

Limitations

Dynamic Disk Fair Sharing (used on Windows Server operating systems) may cause folder explorer operations to hang. As a workaround, you can disable Disk Fair Sharing. This can be done using the following PowerShell Script:

```
1    $temp = (gwmi win32_terminalservicesetting -N "root\cimv2\
        terminalservices")
2    $temp.enableDiskFSS = 0
3    $temp.put()
4 <!--NeedCopy-->
```

You can verify the changes via the following PowerShell command:

```
1    (gwmi win32_terminalservicesetting -N "root\cimv2\terminalservices")
2 <!--NeedCopy-->
```

For additional information see: Fair Share technologies are enabled by default in Remote Desktop Services.

> The following information was previously published on Knowledge Center article CTX228273.

- Several features are temporarily disabled while there is no internet connectivity. These features will become available again when internet connectivity is restored.
- Uninstalling the Citrix Files app removes the currently signed in user's local AppData, but does not remove any other user's Citrix Files AppData on that machine. As a workaround, remove the `C:\users\<user>\Appdata\Local\Citrix\Citrix Files\` and `C:\Users\<user>\AppData\Roaming\Citrix\Citrix Files` directories for each user.
- Users might see "Failed to execute action" when signing in. As a workaround, clear the folder `C:\Users\<user>\AppData\Roaming\Citrix\Citrix Files` and restart the app.
- Attempts to create or rename a folder, giving it the same name as that of a child folder inside it, can fail. The issue occurs if you don't have permission to see the namesake child folder inside.
- Windows Explorer performance might be degraded if browsing a folder containing a large-sized .exe file. As a workaround, users can wait momentarily while Explorer responds.
- Windows Explorer performance might be degraded if browsing a folder containing a large number of image or video files. For more information, see Knowledge Center article CTX241253.
- Files are not displayed when browsing a long folder path exceeding 260 characters.
- When changing drive letters for Citrix Files, the left navigation pane might not refresh to the new drive letter immediately. As a workaround, navigate to the PC folder and then into your new drive letter.
- Citrix Files for Windows fails to mount on Windows 10. A recent Windows update in version 1809 introduced issues with drive mounting. For more information and workarounds on mapped drives and Windows 10 1809, see Windows Support.
- File or folder names starting with the ~ symbol cannot be uploaded.
- When copying a file to a different folder, earlier versions of the file might not be copied over. This issue applies only to copy operations. It does not apply to move operations.
- Renaming a file or a folder to the same name with different case is not allowed.
- Editing a checked-out file might result in errors if the user does not have the delete permission.

As a workaround, give the user delete permissions for that particular folder, or do not check out and edit the file.

- Temporary Office files might be seen in Windows Explorer during editing of a file. As a workaround, refresh the Explorer view to remove the temp files.

- Mount points configured for the OneDrive for Business subfolder might intermittently fail to load. As a workaround, create the mount point to point to the root of the connector.

- If Citrix Files is installed on the same machine as ShareFile Sync, the overlay for Check-in/Check-out might not appear.

- Restricted zones are not supported.

- When attempting to delete a file from Citrix Files, the file temporarily disappears from the Explorer view and then reappears within a few seconds. Along with it, a system notification message appears, stating that the delete operation failed. The issue occurs when the user does not have delete permissions.

RightSignature

December 8, 2023

ShareFile delivers electronic signature ability using RightSignature. An electronic signature, sometimes known as an e-signature, is the same as your handwritten signature on a paper document, except electronic —a mark on an electronic contract or document you make to demonstrate your intent to agree to the terms of that document.

Integrating ShareFile RightSignature with ShareFile gives you the power to obtain legally binding signatures on documents entirely online, being completed more quickly and securely than executing paper documents. ShareFile delivers electronic signature capability at different levels:

- ShareFile electronic signature lets you send files stored in your ShareFile account for electronic signature. For integration steps, see Getting started.

- RightSignature is also available as a stand-alone solution. To get started, see RightSignature.

> **TIP:**
>
> Visit the RightSignature user guidance for electronic signature user information.

Fixed issues

December 11, 2023

Attempting to upload a file using periods in the filename might fail to upload. [ESPILET-351]

February 6, 2023

This release addresses a number of issues that help to improve overall performance and stability.

June 26, 2022

This release addresses a number of issues that help to improve overall performance and stability.

January 20, 2021

This release addresses a number of issues that help to improve overall performance and stability.

RightSignature FAQs

For more information about RightSignature, see RightSignature FAQs.

Storage zones controller

February 25, 2020

Storage zones controller 5.x

Storage zones controller 4.x

User Management Tool

February 25, 2020

User Management Tool

User Management Tool for Policy-Based Administration