Citrix Content Collaboration
What’s new in Citrix Content Collaboration

April 24, 2020

A goal of Citrix is to deliver new features and product updates to Citrix Content Collaboration customers when available.

To you, the customer, this process is transparent. Initial updates are applied to Citrix 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.

April 27, 2020

Citrix Files for Android 2040

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

For more information, see Citrix Files for Android.

April 23, 2020

Citrix Files for iOS 2040

Citrix Files for iOS users have the ability to share files through Citrix Secure Mail.

Citrix Files users can now open Microsoft files with the iOS “Copy to” function. This utilizes the iOS system share menu.

For more information, see Citrix Files for iOS.

April 22, 2020

Files in Citrix Workspace 20.14

Identification information is included in API response headers.

For more information, see Files in Citrix Workspace.
April 2, 2020

Files in Citrix Workspace 20.11

Two factor authentication is required for all ShareFile administrators.
Updated with latest C# SDK.
For more information, see Files in Citrix Workspace.

Citrix Files for iOS 2030

This release addresses a number of issues that help to improve overall performance and stability.
For more information, see Citrix Files for iOS.

April 1, 2020

Citrix Files for Android 2035

This release addresses a number of issues that help to improve overall performance and stability.
For more information, see Citrix Files for Android.

March 11, 2020

Citrix Files for Android 2030

This release addresses a number of issues that help to improve overall performance and stability.
For more information, see Citrix Files for Android.

Files in Citrix Workspace 20.8

Weak password check is now enforced for all users logging into ShareFile.
Two-factor authentication reset notification messages are now updated.
Two-factor authentication can be used with trial accounts.
We now prevent user deletion if items are not reassigned.
Two-factor authentication reset flow is now available.
For more information, see Files in Citrix Workspace.
February 26, 2020

Citrix Files for Android 2020

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for Android.

February 24, 2020

Files in Citrix Workspace 20.3

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Files in Citrix Workspace.

February 18, 2020

Storage zones controller 5.10

.NET Framework is updated to 4.8. Storage zones controller version 5.10 is only supported on Windows Server 2012 and 2016. For more information, see About storage zones controller.

February 4, 2020

Citrix Files for iOS 2010

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for iOS.

January 27, 2020

Citrix Files for Android 2010

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for Android.
January 23, 2020

Citrix Files for Outlook 6.5.1

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for Outlook.

December 20, 2019

Files in Citrix Workspace 1949

Various changes and improvements to UI security have been made including weak password reset. For more information, see Files in Citrix Workspace.

December 5, 2019

Citrix Files for Windows 1912

Perform direct uploads to OneDrive for Business for better speed and reliability. For more information, see Citrix Files for Windows.

November 6, 2019

Citrix Files for Mac 1911

Users with partitioned drives can select where offline data is stored using Preferences. For more information, see Citrix Files for Mac.

Storage zones controller 5.9

This release addresses a number of issues that help to improve overall performance and stability. For more information, see About storage zones controller.
November 5, 2019

Files in Citrix Workspace 1942

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Files in Citrix Workspace.

October 24, 2019

Citrix Files for iOS 1910.5

The MDX Toolkit has been updated to the latest version. For more information, see Citrix Files for iOS.

October 22, 2019

Citrix Files for iOS 1910

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for iOS.

October 17, 2019

Citrix Files for Android 1910

This release addresses a number of issues that help to improve overall performance and stability. For more information, see Citrix Files for Android.

October 9, 2019

Citrix Files for Mac 1910

Citrix Files for Mac is supported on macOS Catalina. For more information, see Citrix Files for Mac.
September 30, 2019

Citrix Files for Windows 1909

When you sign out and sign back in, Citrix Files for Windows keeps your settings and offline files unless you choose to delete those items.

Databases have been cleaned up to save disk space and to improve performance when using Citrix Files for Windows in Citrix Virtual Apps and Desktops environments.

For more information, see Citrix Files for Windows.

September 19, 2019

Citrix Files for iOS 1909.5

The MDX Toolkit has been updated to the latest version.

For more information, see Citrix Files for iOS.

September 13, 2019

Files in Citrix Workspace 1932

Various improvements to the UI have been made including the load progress indicator, status and counter badges, and alerts.

For more information, see Files in Citrix Workspace.

September 9, 2019

Citrix Files for iOS 1909

iOS 13 support: Citrix Files for iOS is supported on iOS 13.

Checkin and checkout for files: Users can check out a file to edit and check the file back in after editing is complete. This prevents file conflicts and overrides by other users who might attempt to work on the same file using the native repository. Checkout places a lock on the file to prevent other users from opening the same file.

For more information, see Citrix Files for iOS.
August 26, 2019

Citrix Files for Outlook 6.5

**Support for recent files:** Citrix Files for Outlook now allows you to access your Recent Files quickly.

![Add from Citrix Files](image-url)
Support for latest file sharing: This update also allows you to share the latest versions of files from Citrix Files and personal cloud connectors.

For more information, see Citrix Files for Outlook

August 20, 2019

Citrix Files for Android 1908

Checkin and checkout for files: Users can check out a file to edit and check the file back in after editing is complete. This prevents file conflicts and overrides by other users who might attempt to work on the same file using the native repository. Checkout places a lock on the file to prevent other users from opening the same file.

For more information, see Citrix Files for Android.
August 13, 2019

Citrix Files for Mac 1908

ShareFile Sync migration: ShareFile Sync users can migrate data and settings from ShareFile Sync to Citrix Files for Mac using the Help menu.

File search (preview): File search allows users to search for files from the Citrix Files for Mac dashboard. You can enable the option in the Preferences menu.

Recover pending files improvements: Improvements have been made to recovering damaged pending files.

For more information, see Citrix Files for Mac.

August 8, 2019

Storage zones controller 5.8

Checkin and checkout for files from Network Shares Connector: Users can checkout a file from Network Shares Connector in Citrix Content Collaboration. This prevents file conflicts and overrides by other users who might attempt to work on the same file using the native repository. Checkout places a lock on the file to prevent other users from opening the same file.

To configure this feature, follow the steps outlined in the section To enable file check in and check out for network file shares.

Create MS Office documents: Users can create MS Office documents (Word, Excel, and PowerPoint) in their on-premises folders when their account is configured with Office Online Server.

For more information, see About storage zones controller.

August 6, 2019

Files in Citrix Workspace 1930

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

For more information, see Files in Citrix Workspace.

July 29, 2019

Citrix Files for iOS 1907

Citrix Files for iOS supports sharing of the latest version of files in personal cloud connectors.
Citrix Content Collaboration

For more information, see Citrix Files for iOS.

Citrix Files for Android 1907.5

This release addresses a number of issues that help to improve overall performance and stability.
For more information, see Citrix Files for Android.

July 15, 2019

Citrix Files for Android 1907

Android and 64-bit compatibility: Citrix Files for Android has been updated to the latest Android SDK and is fully 64-bit compatible.

New error reporting: Citrix Files for Android has been updated to use Firebase for error reporting. In addition, Citrix Files for Android now uses the latest Crashlytics SDK.
For more information, see Citrix Files for Android.

July 12, 2019

Files in Citrix Workspace 1928

Mentions of Citrix Content Collaboration as “ShareFile” have been removed.
When loading components, the screen visuals has been improved to better communicate that Citrix Workspace is loading and has not become unresponsive.
For more information, see Files in Citrix Workspace.

July 11, 2019

Addition of storage zones controller and User Management Tool

Storage zones controller and User Management Tool documentation sets added to Citrix Content Collaboration

July 1, 2019

Citrix Files for Windows 1907

New product version numbers:
Citrix Content Collaboration

- As of this release, product version numbers appear in the format YYMM, where YY is the year and MM the month the product released. For example, a release in July 2019 appears as 1907.

- In earlier releases of Citrix Files for Windows, version numbers were following the format 4.version, where the version value incremented by one for each release. For example, the release following 4.5 was 4.6. Those earlier releases will not be updated with the new numbering format.

**Auto Check-out:** Auto Check-out allows administrators to permit users to automatically check out Microsoft Office and AutoCAD files after opening. Auto Check-out is enabled using the updated Group Policy.

**Folder conflict resolution:** Folder creation conflicts can now be detected and resolved if a user creates an already existing folder.

For more information, see Citrix Files for Windows.

June 28, 2019

**Citrix Files for Android 1906.5**

Citrix Files for Android supports sharing of the latest version of files in personal cloud connectors.

For more information, see Citrix Files for Android.

June 24, 2019

**Citrix Files for iOS 1906**

**New product version numbers:**

- As of this release, product version numbers appear in the format YYMM, where YY is the year and MM the month the product released. For example, a release in June 2019 appears as 1906.

- In earlier releases of Citrix Files for iOS, version numbers were following the format 7.version, where the version value incremented by one for each release. For example, the release following 7.6 was 7.7. Those earlier releases will not be updated with the new numbering format.

- The Polaris Office SDK has been updated to the latest version.

For more information, see Citrix Files for iOS.
May 28, 2019

Citrix Files for Outlook 6.4

File browser redesign and improvements:
The file browser has been redesigned and improved to make selecting and sharing files and folders even easier.

All functionality has been preserved; access is now faster to shared and personal folders and to cloud connectors.
Validation checks have been improved to provide better error and warning message handling.

New navigation allows you to easily go back to the previous folder or navigate between folders.
Stronger security for files and folders:

- Virus strictness settings at the account level have been expanded with new options to provide stronger security.

- A warning now appears when someone attempts to send or download an infected file. Sending and downloading any unscanned or infected files is blocked. An icon also appears next to unscanned files.

Miscellaneous updates that let you:

- Save attachments to on-premises connectors and personal cloud connectors.
- Submit your feedback in the Help menu under Feedback & Support section.
- Set up a default expiration policy to 3 months or send a link with a custom expiration policy of 3 months.

For more information, see Citrix Files for Outlook

May 9, 2019

Storage zones controller 5.7

Single sign-on to on-premises connectors in Citrix Workspace: With this release, users using Citrix Workspace clients are no longer prompted for authentication when they try to access their network shares or SharePoint folders behind a storage zone controller.

To enable this feature, follow the instructions under Deploy and enable Citrix Content Collaboration in Citrix Workspace.

For more information, see About storage zones controller.
April 30, 2019

Citrix Files for Gmail 2.0

Citrix Files branding: ShareFile for Gmail is now Citrix Files for Gmail. Citrix Files for Gmail brings Citrix Content Collaboration functionality to your Gmail account. This extension is only available for the Google Chrome web browser.

For more information, see Citrix Files for Gmail

Citrix Files for Mac 1904

New product version numbers: As of this release, product version numbers appear in the format YYMM, where YY is the year and MM the month the product released. For example, a release in April 2019 appears as 1904.

In earlier releases of Citrix Files for Mac, version numbers were following the format 4.version, where the version value incremented by one for each release. For example, the release following 4.5 was 4.6. Those earlier releases will not be updated with the new numbering format.

Offline access is now available to every employee user on Citrix Files for Mac. This includes all of the following enhancements:

- Individual file and folders can be made available offline through the Finder window.
- A Manage Offline Sync window, where users can easily select folders they want to keep offline.
- New visual overlays to indicate an offline, syncing, or error state for files and folders.
- Conflict resolutions for files and folders which were modified, renamed, moved, or deleted.
- An Errors tab has been added to the dashboard. It lets users take resolve action on specific errors and get information on other errors.
- When signing out or uninstalling Citrix Files for Mac, you also have the option to keep any offline files on your local machine.
Citrix Content Collaboration

For more information, see Citrix Files for Mac.

Deploy

April 28, 2020

Note:
Not all features available under a Citrix Content Collaboration license are available in Citrix Workspace. Click here for the list.

Deploy and enable Citrix Content Collaboration in Citrix Workspace

To deploy and enable Citrix Content Collaboration in Citrix Workspace, complete the following steps:

1. Fulfill the Citrix Workspace requirements [here](#).
2. Link the Citrix Content Collaboration account to Citrix Cloud as described [here](#).
3. Go to the hamburger menu and select Workspace Configuration.
4. Go to Service Integrations and select the three dots.
5. Select Enable to enable Citrix Content Collaboration.
6. Choose which account, if you have more than one, you want to use for Files within Workspace.
7. Select Save.
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 version 5.7 or 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, new links generate as cloud.com links.
Note:
Single sign-on is not supported when the account is in testing mode. To support single sign-on, 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.

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. Click here for the list.

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.

Note:
To ensure Azure Active Directory works correctly with Citrix Content Collaboration, your Azure Active Directory must have a primary email address for each user. This requires your Microsoft subscription to include an Office 365 subscription with Exchange Online or you must connect your Azure Active Directory to your on-premises Active Directory by using Azure Active Directory Connect.

After you enabled a Citrix Content Collaboration account within Citrix Workspace, you can go back to Workspace Configuration > Service Integrations and decide to enable a different account. If you do, be aware the change affects the files and data a user sees in their workspace.

If Citrix Content Collaboration is the only service enabled in your workspace and depending on which features you are looking for, you can instead go directly to your account using [subdomain].sharefile.com/.

Disable Citrix 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**

Once Citrix Content Collaboration is enabled in Workspace Configuration, all Share and Request links are from yourdomain.cloud.com, and notification emails follow branding from Workspace Configuration.

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
On-premises connectors (CIFS, SharePoint) are supported only in the Citrix Files apps and in Citrix Workspace for web. Connector credentials might expire between browser sessions.

ShareFile virtual data room and features that are limited to ShareFile virtual data room accounts such as Folder Q&A

External (client) users specific two-step verification

Folder Invites

Features and settings that currently require a workaround

The User Management Tool and StorageZone Controller require the administrator to sign in by using ShareFile credentials. The recommended option is to create an employee user service account within the Citrix Content Collaboration tile on the Citrix Cloud Launchpad. When you create the employee user service account, ensure you set a ShareFile password, give it the user the appropriate administration permissions, and deselect the check box to allow the user to change their password.

The following Workflows are available on the web only:

- Request List
- Custom Workflows

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.

SAML authentication is not supported as a way to sign into Workspace.

- Workspace authentication supports either AD or AAD.

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 into 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][FolderPath].log - This log contains the complete details of the migration
  starting from launch of Citrix Files Migration Tool.
- Transfer Info [TimeStamp][FolderPath].log - This log contains verbose information for the
  transfer.
- Transfer [TimeStamp][FolderPath].log - This log contains all the files and folders that were suc-
  cessfully transferred.
- Transfer Failure [TimeStamp][FolderPath].log - This log contains a brief explanation as to why
  a file failed to transfer.
- Transfer Cancelled [TimeStamp][FolderPath].log - This log contains a brief explanation as to
  why a transfer canceled.

For debugging, the “SFMT [TimeStamp][FolderPath].log” and “Transfer Info [TimeStamp][FolderPath].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 Con-
tral Panel, or rerun the installation file.

Warning:

Migration logs that were created during transfers are removed during the uninstall process.

**Disclaimer**

To the extent Customer subscribes to a Citrix Content Collaboration plan with unlimited cloud storage,
Customer shall be entitled to 1TB of storage per User with the ability to increase upon request for
reasonable use as intended hereunder.
Configuration

March 3, 2020

Master administrator

The master administrator maintains all user permissions available on the account and cannot be deleted by any other user. If an account feature is added to the account, the master administrator automatically has access to the feature. Any other users must be granted access as desired by the master administrator.

All subsequent access to the customer’s account is managed by the master administrator account, or administrators designated by the master administrator account.

Identifying the master administrator

To identify the current master administrator, go to Users > Browse Employees. The master administrator has a special icon to the left of their name.

![Master, Admin](image)

The master administrator is also indicated on the Manage > Admin Overview page.

Changing the master administrator

To change the master administrator for an account, the current master administrator or account owner must sign in and navigate to Manage > Admin Overview.

The current master administrator can use the Reassign account owner option to designate a new master administrator. In the Reassign Account Owner menu, select the new admin from the employees on your account. The new master administrator 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 master administrator.

Click Assign New Account Owner to complete the process. Once submitted, this change cannot be undone. Only the new master administrator is able to reassign, using the preceding steps.

If the current master administrator is not available to place this request, contact Citrix Support.
Create employees

An employee user is most often 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 **Users > Manage Users Home** in the Citrix Content Collaboration console in Citrix Cloud. Use the **Create Employee** button to begin creating a user.

Type your user’s name, email address, and company info. You can also customize their password. 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 Citrix Content Collaboration, 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: john-doe@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

Citrix Content Collaboration 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 Citrix Content Collaboration, 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

- Date Created
- Email Address
- First Name and Last Name
- Company name.

Notifications

Change the user’s default Notification Frequency settings.

Default email language

Change the user’s default Email Notification Language.
**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 them. It also applies to all of their folders, so that they cannot share files with others more than you would like for them to.

Employee bandwidth limits can also affect clients that the employee supports 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 Citrix Content Collaboration credentials or two-step verification.

**User access**

**General**

**Change their 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.

**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**.

**Files and folders**
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. **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.**

People

Manage Clients

Manage Clients allows the employee to see the People tab in the navigation bar and to add new users to the account. They are also able to edit settings for any clients that they create. Editing a client user's email address requires the Manage Employees permission.

Edit the shared address book

The Shared Address Book is available to employee users on the account so that they can quickly and easily pull up contact information for users on the account. When this option is checked, the employee is able to add users to the Shared Address Book to allow others to see their contacts on the system.

Share distribution groups

When this permission is enabled, the employee user is able to create a Shared Distribution group.

Edit other users' shared 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.

Company Account Info

Edit account appearance

This setting allows the user to configure account branding and appearance settings.
Citrix Content Collaboration

**View receipts and billing notifications**

The Receipts & Billing Notifications link in the Admin Settings > Billing section allows any user with this permission enabled to download copies of any receipt or invoice for the account.

**Advanced Preferences**

The following settings display only when you have the feature enabled on your plan type.

**Connectors**

**Create Network Share Connectors**

This permission grants the user the option to create and manage new Network Share Connectors. This permission is only available to Citrix Content Collaboration users on certain plans.

**Create SharePoint Connectors**

This permission grants the user the option to create and manage new Sharepoint Connectors. This permission is only available to Citrix Content Collaboration users on certain plans.

**StorageZones**

**Select StorageZone 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.

**Delete employees**

From Citrix Content Collaboration, click Users > Browse Employees and locate the employee user. Click their name to access their profile page.

On the right side of the profile page, click Delete from the System to delete the user. When you click this button, you are offered the opportunity to reassign all files and folders to another user on the account. **Files that are not reassigned are unable to be recovered or restored.**
Note: When deleting client users, files cannot be reassigned.

Create an external (client) user

An external (client) user is a user outside of your company who does not need access to employee-level Citrix Content Collaboration features but does have access to shared folders and files. There are several ways that you can add new external (client) users to your account.

Note: Only accounts with a Citrix Content Collaboration entitlement have a selection page that allows them to select if they’re an employee or external (client) user, prior to sign-in. This page enables external (client) user sign-in to Citrix Workspace. The selection page is designed to favor employees, meaning once an employee self-selects, they always land directly on the sign-in page to input their credentials, unless they clear their cookies.

Note: The sign-in selection page does not currently support Citrix Probe Agent.

Requirements to create an external (client) user

- An Employee user.
- The Manage client users permission.
Citrix Content Collaboration

- 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 or Browse Clients in Citrix Content Collaboration. Use the Create Client button to begin creating a user.

Enter your user's email address, first name, last name, and company. If you want to add more users, click Add another. While you can add a set password for first time sign-in without an activation email, by default new external (client) users are prompted to create a password when they sign in to Citrix Workspace for the first time.

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.

Notify Users

Send a customized message to let the new users know they've been added to the account.

Message:

I've added you to my Citrix Workspace account.

Character limit: 954

Preview Email
Citrix Content Collaboration

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.

**Create a client (folder access menu)**

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 on this Folder 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.

**Create an external (client) user (Email with Citrix)**

Email with Citrix allows you to send your files using Citrix Workspace’s 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.

To send a file stored on your computer using Citrix Workspace:

1. Right click any file, then click Email with Citrix.
2. Enter a new external (client) users’ email address as a recipient for your message and file.
3. Enter a subject for your message. You can enter extra text in the body of your message if needed.
4. **Edit Message Options** allows you to customize the following:
   - Send me a copy of this email - Receive a copy of the email message.
   - Email me when files are accessed - Receive a notification email when the file is viewed or downloaded.
   - Encrypt message - This option is available only to users with encrypted email enabled.
   - Require recipients to log in - Require that recipients log in with their Citrix Workspace account. If your recipient is not already a user on your account, they are then required to create a user name and password before accessing the file.
   - Access expires - Set how long you want the download link to be accessible.
Citrix Content Collaboration

- Allow Recipients To - This option is available to users utilizing View-Only or IRM-protected sharing features.
- Accesses per user - Limit the number of views or downloads users can have.
- Always link to the latest version of the file - This option is available only to users with file versioning enabled.
- Remember subject and custom message for next time - Save the subject and custom message so that it is preset the next time you send a file.

5. Click **Send** when ready. You then receive confirmation that the message was sent successfully.

Resend a client activation link

Requirements to resend an external (client) user activation link:
Citrix Content Collaboration

- An admin on Citrix Cloud with access to Citrix Content Collaboration.
- The **Manage client users** permission.
- Changing an external (client) users’ email address or deleting an external (client) user from the system both require the **Manage employee users** permission.

When a user is added to Citrix Content Collaboration, 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 Citrix Content Collaboration, 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**.

**External (client) user: Activate to access shared files**

When you send a file link with the **Require User to Login** option checked to an external (client) user, the external (client) user is asked to create a Citrix Workspace account to access the link they have received. If you send a file request using the Email by Citrix system, the external (client) user receives an email with a link, as shown in the following image.

1. Click the link to activate the account.
2. Before they can download files, they must set a password for their account.
3. Once they have set their password and clicked **Reset Password**, click **Back to Sign In** to sign in to Citrix Workspace to view or download the shared files.

4. If they want to view the files again after leaving the page, go back to the email and click the link. The link takes the external (client) user directly to the files on return.

**External (client) user: Sign in and view shared files and folders**

When you add an external (client) user, the external (client) user can sign in to Citrix Workspace to view the shared files and folders. Sign in by doing the following:

1. Go to the Citrix Workspace account URL (typically something like [company].cloud.com).
2. Click to sign in as an External User. If they have signed in as an Employee User before this, they might not see the split sign-in page to sign in as an External User. If that occurs, clear the cache to see the page again.
3. Enter the user name and password and click **Sign In**.

**Employee and client user abilities**
### Remote wipe

Administrators and employee users who have the **Manage other employee users** permission can wipe devices at any time by selecting **Users** and then **Browse Clients** or **Browse Employees** on the sidebar. Select the name of the user and click **Manage devices for this user**.

This brings up the **Connections** page for the user, where the user’s connected apps and connected devices are listed. **Lock** a user account on the device to prevent the user from accessing the data on it. The data remains on the device unless you wipe the account from it. **Wipe** a user’s account from a device to remove the data from it the next time the device connects to the account. **Revoke** a device’s

<table>
<thead>
<tr>
<th>Feature</th>
<th>Employee</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create root level folders</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Access personal folders</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Be granted admin permissions</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Be granted super user status</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Create users and manage permissions</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Modify account appearance</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Access File Box</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Share a file stored on PC</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Request a file into File Box</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Run reports</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Citrix Files for Windows or Mac</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Citrix Files for Outlook</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Citrix Files for iOS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Files for Android</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encrypted email</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Mobile editing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Mobile PDF annotation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Create and manage connectors</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
access to Citrix Content Collaboration if you no longer need to manage the user’s account on it.

You cannot wipe the device of a user that has been removed from the Citrix Content Collaboration account. Users that have been deleted or removed cannot access their accounts.

Admin overview

The Admin Overview page gives summarized information on your account, including Account Name, ID, Billing Plan Type, Account Owner, and Allocated Licenses. The page also displays any entitlements on your account and links to view release notes and open source licenses. This page is the landing page after you click Manage in the Citrix Cloud console.

Background operations

The Background Operations page displays any current or completed operations that might take a long time to complete. The page shows you all pending, in progress, and recently completed operations.

Content Collaboration reports

To see how your Citrix Content Collaboration account is being used, you can create recurring and non-recurring reports that track usage, access, messaging, storage, and other details.

Prerequisites

- An Administrative user on the Citrix Content Collaboration account.
- An Employee user with the Allow this user to access account-wide reporting permission.
- If running a report for a specific user, that user must be a member of the Shared Address Book.

Create report

Complete the following steps to create a Citrix Content Collaboration report:

1. In your Citrix Cloud account, go to Citrix Content Collaboration.
3. Click the Create Report button and choose the type of Report you want to run, then click Next.
4. Fill in the details as required and click **Create**. Reports can be generated as Excel or CSV files.
Recurring report:

To create a recurring report, follow the earlier steps through Step 3. Then, choose Recurring as Yes, fill in the other details as required and click Next.
Citrix Content Collaboration

Choose **Daily**, **Weekly**, or **Monthly** based on your needs. Choose the folder where you want the recurring reports to be saved on your account and click **Create**.

Do not remove the destination folder from the system. If you do, future recurring reports might fail.

**Report Pending:**

Allow time for your report to be processed and completed. Depending on the amount of time and final size of your report, the time it takes for the report to finish might vary.
View Completed Report:

You can view, download, move, or delete reports at any time by returning to the Reporting menu and accessing the list to the right of the Report Title.

Note:
Reports support a maximum period of 90 days. Citrix recommends a maximum of 30 days.

Report types

Usage
Reviews activity based on account, folder, or user and includes items such as: login, failed login, downloads/views, uploads, create folder, check in / checkout, move, restore, create notes, edit, create URLs, delete, DLP scan (OK), DLP scan (rejected), and DLP share. If the activity name is not checked when creating the report, no data is returned for that activity name.

Access
Reviews access and permissions on folders. This report can be run at the account level, for a specific user, or on a specific folder.

Access change
Reviews when users were added, edited, or removed from folders. This report can be run at the account level, for a specific user, or on a specific folder. This report can only be run with a date range no longer than 90 days.

Storage detail
Reviews files stored in your account.
Citrix Content Collaboration

Storage Summary
Reviews data for the account or an individual user. Due to the scope of this report, it can only be run once a week, on a recurring basis. The named user in this report represents the owner of the folder in which the item resides.

Share
Reviews activity related to files that are shared by users on the account. This includes any Share messages created in other Citrix Files apps. This report can be run at the account level or for a specific user. This report can only be run with a date range no longer than 90 days.

Request
Reviews activity related to file requests that have been sent by users on the account. This includes any Request messages created in other Citrix Files apps. This report can be run at the account level or for a specific user. This report can only be run with a date range no longer than 90 days.

Users
Reviews a list of users on your account and their status as it relates to things like the address book or user policies. If your account does not have or use the features associated with certain fields, they return as blank.

Bandwidth detail
Reviews all uploads and downloads, including details about those transfers.

Bandwidth summary
Reviews all uploads and downloads, including details about those transfers.

Messaging
Details all messages and links created by the specified user.

Notification history
The Notification History page contains a history of all email messages that have been sent from your account. You can select a date or a specific email with the options shown.
Company branding

Your account’s account or company name allows Citrix 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.

Account name

To change your account’s name, go to Manage > Company Account Info > Edit Company Branding and enter the account name as you would like it to appear, then click Save.

Account appearance

You can edit your account’s sign-in page appearance here. Basic options include Page Title, Logo image, Header Background Color and Accent Color. Click the advanced appearance options link to access more customization, including favicons, background images, page text, and more.

Subdomains

For you or your clients to view your custom branding, you must access Citrix Content Collaboration through a subdomain. You can choose up to three subdomains, which all share custom branding.

Subdomain requirements

The subdomain:

• Must contain only letters, numbers, and hyphens.
• Must not start or end with a hyphen.
• Must be at least 2 characters long.

This page updates to preview your selections and is not visible to users while in edit mode. When you’re ready to apply these settings to your whole account, click Save.

Receipts and billing notifications

To view or print billing receipts for your account, click the appropriate date on this page. You can request an email notification when your account is billed.
Citrix Content Collaboration

Data loss prevention

Citrix Content Collaboration 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 zones 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 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.

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

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.
- 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: ! # $ % ^ & * ( ) _ + = / . ? \ [ ]
- Cannot be the same as their last 25 passwords.
Security settings

Trusted domains

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

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 single sign-on customers also implement 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 Citrix Support for assistance with adding terms to your sign-in page.

IP restrictions

Use IP restrictions to restrict where your users can sign in to your Citrix Content Collaboration account. Contact Citrix 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.

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 are asked to enter a verification code that is sent to your phone using a text message...
Citrix Content Collaboration

(SMS) or voice call. Supported Authenticator apps like Google and Microsoft can be used as an option instead of your usual password.

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.

Limitations

- This feature is not available for trial accounts.
- This feature cannot be used with company credentials or a custom sign-in page.

By enabling this feature, you make the two-step verification option available to all users on the account. Administrators can set policies to require user enrollment for two-step verification.

Login & Security Policy

Two-step verification

<table>
<thead>
<tr>
<th>Enable two-step verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

When enabled, users can enroll a device from Two-Step Verification in Personal Settings.

Require two-step verification

| Require for employee users
| Require for client users |

When required, users must enroll a device when signing in.

Enable “trust this device” for client users

| Yes | No |

When enabled, clients can mark a device as trusted, so entering a verification code is not necessary for every sign-in.

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. 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.

Enable “trust this device” for client users can be enabled so when client users mark a device as trusted, they are not required to enter a verification code every time they sign in.
Device security

You can use these options to control the security level for devices used to access the Citrix Content Collaboration 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 Citrix Files application.

**Enable offline access to files** - Controls whether users can see Citrix Content Collaboration content when the device is offline.

**Restrict modified devices** - Enabling this restricts users from being able to use Citrix Files on a jailbroken device. Citrix cannot 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, Citrix 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 Citrix Content Collaboration account. Super users have upload, download, delete, and administrator permissions on all folders. Super user group access to a folder cannot be modified or removed in the folder access menu. This feature is enabled on your account by default.
Manage 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 check boxes 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** check box.

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

**Personal cloud connectors**

Personal cloud connectors allow users to access their Box, Dropbox, Google Drive, and OneDrive (Consumer Version) accounts, providing customers with the flexibility to determine how and where users store files. Personal cloud connectors can be accessed using the web app, but certain file interactions might not be available.

**Limitations**

- Due to compliance concerns, this feature cannot be used by users utilizing a HIPAA storage server, a VDR account, or an account with Archiving enabled.
- For on-prem customers, personal cloud connectors are supported for accounts utilizing Customer-managed StorageZones so long as the account is also associated with a Citrix-managed StorageZone.
- Currently, accounts with no association to a Citrix-managed StorageZone (such as strictly on-prem or tenant setups) cannot utilize this feature.
- File uploads to personal cloud or Office 365 connectors currently have a maximum upload size of 100 MB per file.
- Currently, connectors must have a unique display name. Users are blocked from using a connector name that is currently in use elsewhere on the account.
Enable a personal cloud connector

A personal cloud connector must be enabled by an Admin user before it can be accessed. Only users with the Create and Manage Connectors permission can enable connectors on the account.

Navigate to Manage > Connectors. Here you can view the connectors available for your account.

Click the Enable button to turn on that connector for users on your account.

Once a connector has been enabled, you can manage connector access. By adding a user to the access list for a specific connector, that user is then able to use the connector to link their account to another data storage service. Save your access changes to continue.

The connector creator and the super user group are automatically granted access to the connector type.

Once you have enabled the connector, any user that has been granted access to it can now set up the connector in their own Personal Settings menu.

To configure your connector, navigate to Personal Settings > My Connectors. You must authenticate with your desired connector service so that Citrix Content Collaboration can be authorized to interact with it. Once you have connected services, your connector appears in the Folders section of your sidebar.

Office 365 connector

The connector for Office 365 allows users to access, edit, and share from their SharePoint Online and OneDrive for Business accounts from Citrix Content Collaboration, providing enterprises with the flexibility to determine how and where users store files. Configuration of the Office 365 connector and user assignment can be done from the web application.

Notes and limitations

- This feature is included with the Advanced Plan, Workspace Premium, Workspace Premium Plus, and others.
- SharePoint Online and OneDrive for Business connectors require Citrix-Managed (cloud) StorageZones. Therefore, these connectors are not available for accounts utilizing a HIPAA storage server.
- Office 365 connectors are not compatible with GCC High (Azure Gov) deployments.
- File uploads to SharePoint Online has a maximum upload size of 200 MB per file; OneDrive for Business’ upload limit is 15 GB per file.
- Connectors must have a unique display name. Users are blocked from using a connector name that is currently in use elsewhere on the account.
• Actions such as browsing folders or downloading files might fail when using the Safari web browser. To resolve any issues, ensure cookies are allowed in your Safari system preferences.

**Supported apps for Office 365 connector**

- Citrix Files for iOS
- Citrix Files for Android
- Citrix Files for Windows
- Citrix Files for Mac
- Web application (Copy and Check-In, Check-Out are not supported via the web browser)

**Supported functions**

- Link your Citrix Content Collaboration account to your Office 365 account
- Access OneDrive for Business files and folders and SharePoint Online document libraries from Citrix Files
- Move content securely from Office 365 to Citrix Content Collaboration
- Share Office 365 content securely from Citrix Files
- Favorite folders

**Storage zones**

Storage Zones gives 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.

**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 > Storage Zones. From the storage zones 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

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.

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.

STMP 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 custom SMTP on your account, your users recognize your email address as the sender and any failed emails
come back to you. To use custom STMP, 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 > STMP Server**.
2. Click **Configure STMP Settings**. The Custom STMP Configuration page appears.
3. Enter the appropriate information to enable this feature.

**Required fields:**

- **Enable Custom STMP** – This option must be selected if you want to use these settings.
- **EmailAddress** – 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 Send 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.

**Email Notifications / Messages Do Not Arrive** - This issue might occur if you have IP restrictions or policies on your local mail servers. See Knowledge Center article [CTX208318](#) to ensure you have
whitelisted the custom SMTP IPs. Likewise, review your mail server authentication methods to ensure that Citrix can communicate with your servers.

**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.

**Folder Access List**

If **Yes** is selected, all users are able to see the folder access list inside folders they have access to. If **No** is selected, only users with admin rights on the folder are able to see the list of other users in the folder.

**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 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](https://www.microsoft.com/litigation/privacy-Statement) and [Privacy Policy](https://www.microsoft.com/privacypolicy/privacystatement). An Office 365 subscription is required for editing.

For more information on Microsoft Office previewing and editing, see Knowledge Center article [CTX208340](https://support.citrix.com/article/CTX208340).

**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 customer managed storage zones. 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: (Any address in this field requires \texttt{https://} to function properly.) 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.

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.

Single sign-on (SSO) for Citrix Content Collaboration

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
- Citrix Gateway
- 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

Citrix Ready Partners

Click here for information on the Citrix Ready Program

Files in Citrix Workspace

April 22, 2020

About Files in Citrix Workspace

When using Citrix Workspace and Citrix Workspace app along with the Citrix Content Collaboration service, you can access all of your files from the Files tab in Citrix Workspace. You can view all your Favorites, Personal and Shared Folders, and access any cloud connectors you might have. You can also submit files for Feedback and Approval, view your File Box, and manage your Recycle Bin. You can even edit your files using Citrix Workspace.

For more information on Citrix Workspace, see Citrix Workspace platform. For more information on Citrix Workspace app, see Citrix Workspace app.

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

Fixed issues in 20.14

• When moving a folder, previous folder permissions might not be applied. [SFPLATFORM-11316]

Fixed issues in 20.11

• Thumbnails and PDF previews might not display in ShareFile. [SFPLATFORM-12082]

Fixed issues in 20.8

• Users might be required to enter phone number to enable two-factor authentication on web even if they have activated and enabled it on client. [SFPLATFORM-11743]
• If company info is not provided when two-factor authentication is enabled, non-admin employees or client users might not activate successfully. [SFPLATFORM-11744]
• Get a link URL might not display items if the link is for a restricted zone. [SFPLATFORM-11844]
• When force SSO is enabled, only master admins are allowed to set up two-factor authentication. [SFPLATFORM-11855]

Fixed issues in 20.3

• Address Book within Safari browser might be unusable due to poor formatting. [SFWEB-12486]
• Default Start Date of User Activity Log might exceed maximum value. [SFWEB-12511]
• Add People to Folder window is poorly formatted. [SFWEB-12541]
• Incorrect message might display when Continue button is selected after an invalid URL is provided. [SFWEB-12552]
• A display issue might occur with the signature field form using workflows while signing in from mobile browsers on both iOS and Android. [SFWEB-12556]
• Clicking the browser back button on weak password policy might land on subdomain page instead of email/password page. [SFWEB-12563]
• Incorrect text might display for “Dont know your subdomain.” [SFWEB-12574]

Fixed issues in 19.49

• FTP login fails when shortname and two-step app specific password is used. [SFWEB-10112]
• Removing download permission is not removing the hidden view permission. [SFWEB-11065]
• First attempt to open a file using email on iOS devices fails. [SFWEB-11080]
• Activation links fail when created by adding new users to a folder and email with ShareFile requiring log in. [SFWEB-11081]
• “No Items Available” message appears after accessing the download link in email due to files expiring just after they are created in File Drop. [SFWEB-11176]
• Activity Log option is missing in Person Folders. [SFWEB-11187]
• ShareFile login page has logo display issues in IE11. [SFWEB-12407]
• Single items sent or received in an encrypted email using name and email address requirements causes download error. [SFWEB-12484]

Fixed issues in 19.42

• Attempts to save a .jpg image as a logo on the Company Branding page fail. [SFWEB-12410]

Fixed issues in 19.32

• Certain download notifications might appear with an anonymous user. [SFPLATFORM-10647]

Fixed issues in 19.30

• When deleting multiple client users at a time, the last client user you delete receives multiple notifications. Other client users you delete as part of the same batch don’t receive any notifications. [SFPLATFORM-10221]
• Locations of customers might be incorrect when generating a usage report. [SFPLATFORM-10394]
• The “People on this Folder” tab might not work correctly for non-admin users. [SFPLATFORM-10494]
• Users without folder admin permissions might not be able to manage their own folder notifications. [SFPLATFORM-10512]
• When configuring the Outlook plug-in, the Send Text option might not display any text. [SFPLATFORM-10500]

Fixed issues in 19.28

• Moving folders might not reassign owners correctly. [SFPLATFORM-9605]
• When signing in using FTP, using just the user name instead of the domain and user name might fail. [SFPLATFORM-10112]
• Thumbnails for images might not display correctly. [SFPLATFORM-10123]
• The “noreply@sf-notifications.com” email might show as a user who has downloaded data in the logs. [SFPLATFORM-10143]
- The location of the created usage report might not be where it is expected. [SFPLATFORM-10149]
- Files with certain character format names are displayed in the wrong format or language. [SFWEB-12139]

**Fixed issues in 19.19**

- After disabling a storage zone and migrating files to a new storage zone, the account might not update correctly. [SFPLATFORM-9228]
- When setting up two-step verification, the app remembers the first country code you select and attempt - even if you change the selection to a different country code. [SFPLATFORM-9814]
- When adding a new note to a versioned item, the new note overwrites all previous notes created in that versioned items list. [SFPLATFORM-9848]
- Using Request a File and requiring sign-in causes both the sender and the recipient to be logged as the intended user. [SFPLATFORM-9871]
- When replying to an encrypted email in Safari using iOS, tapping Send takes you to the sign-in page and the reply is not sent. [SFWEB-12142]
- When using two-factor authentication, using a non-US phone number for the backup phone causes the following error message to appear: “Failed to send, please make sure you entered a valid phone number.” [SFWEB-12256]
- When the administrator navigates to the Login and Security page in the Citrix Cloud console, the following error message appears: “AccountProvider: The item could not be found.” [SFWEB-12262]

**Fixed issues in 19.17**

- Creating a new Microsoft Office file might fail due to invalid characters in the file name. [SFPLATFORM-7269]
- When IP restrictions are set in Citrix Content Collaboration, Citrix Virtual Apps might not enumerate correctly. [SFPLATFORM-9225]
- Users might be able to edit the folder expiration date for Personal Folders. [SFPLATFORM-9621]
- When exporting logs using a cross tenant or cross user, no exception is thrown. [SFLATFORM-9642]
- Child folders might appear at the same level as their parent folders. [SFPLATFORM-9831]
- This fix addresses an issue with the creation of client users in the add user to folder process. [SFPLATFORM-9849]

**Fixed issues in 19.15**

- Files might be deleted after users are reassigned. [SFPLATFORM-8307]
• The storage zone shown in the webapp and the database for the account might not match. [SFPLATFORM-8902]
• The NotificationSweeper app might consume an excessive amount of CPU. [SFPLATFORM-9202]
• User roles might not be set during validation. [SFPLATFORM-9433]
• Sync might mistake the master administrator for a client user, pausing Sync. [SFPLATFORM-9700]
• When a DS group is added to a workflow, the workflow cannot be edited. [SFPLATFORM-9755]
• Adding a new client user might not create an activation token when using a Citrix Workspace account. [SFPLATFORM-9757]
• When attempting to move or archive a file using the ShareFile Desktop App for Windows, the following error message appears: “You are not authorized to perform this operation.” [SFPLATFORM-9804]
• Links sent with ShareID might redirect to the dashboard rather than to the downloadable file. [SFWEB-12186]
• Encrypted emails sent to email addresses beginning with “g” might not be sent. [SFWEB-12196]
• Help links were gray on a dark background, making them difficult to see. [SFWEB-12207]
• Administrators might not be able to switch to a valid storage zone. [SFWEB-12224]

Fixed issues in 19.12

• The EncryptedEmailInbox is visible in Shared Folders for super users. [SFPLATFORM-9277]
• Users might not get autoconfirmed as created if the administrator creating them does not have the Admin SSO or Admin Policy roles. [SFPLATFORM-9501]
• When moving a folder structure, ownership of the subfolders is given to the original owner as well as to the owner of the new location. [SFPLATFORM-9567]
• Uploads to a “request files” link might cause excessive load on the database server. [SFPLATFORM-9633]
• Users cannot print .msg files from the web application. [SFWEB-12189]
• When Citrix Workspace is maximized, selecting the last file in the Recent/Favorites section might not show all available menu options. [WSUI-368]
• The top menu UI might overlap with the file list when selecting a file in Citrix Workspace app. [WSUI-487]

Fixed issues in 19.9

• Trying to save a Microsoft Word file to ShareFile might result in an error. [SFPLATFORM-8931]
• Attempting to move more than 15 files at a time to another folder might fail. [SFPLATFORM-9085]
• RightSignature users attempting to change permissions of another user might not work and the following error message appears: “[Error2] 403 Forbidden.” [SFPLATFORM-9138]
• Attempts to change Folder Options to modify subfolders might not apply correctly. [SFPLATFORM-9266]
• Users with larger than normal folder structures cannot set retention policies. [SFPLATFORM-9292]
• File Drops do not upload if “select recipient from drop-down list” is cleared. [SFPLATFORM-9509]

Known issues

Known issues in 20.14
No new issues have been observed in this release.

Known issues in 20.11
No new issues have been observed in this release.

Known issues in 20.8
No new issues have been observed in this release.

Known issues in 20.3
No new issues have been observed in this release.

Known issues in 19.49
No new issues have been observed in this release.

Known issues in 19.42
No new issues have been observed in this release.

Known issues in 19.32
No new issues have been observed in this release.
Known issues in 19.30
No new issues have been observed in this release.

Known issues in 19.28
No new issues have been observed in this release.

Known issues in 19.19
No new issues have been observed in this release.

Known issues in 19.17
No new issues have been observed in this release.

Known issues in 19.15
No new issues have been observed in this release.

Known issues in 19.12
No new issues have been observed in this release.

Known issues in 19.9
No new issues have been observed in this release.

Citrix Files apps

August 15, 2019
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 — any time, 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)
- Outlook Online (and Mac)
- Gmail

**Configuration for Citrix Files**

January 14, 2020

**Citrix Files desktop applications authentication in Workspace**

Citrix Files integrates with the authentication system used by Citrix Workspace app to provide a single sign-on experience to both Citrix Files and the Citrix Workspace app.

Users first sign in through Citrix Workspace and upon next start of Citrix Files are automatically signed in using their Citrix Workspace account. Similarly, users can first sign on to Citrix Files, which automatically signs them into Citrix Workspace.
When any compatible application triggers a logoff operation, all applications that use the Citrix Workspace logon are signed off.

Requirements

- Citrix Workspace app for Windows or Mac (must be configured to Citrix Workspace Store URL)
- Citrix Files for Windows or Mac, or Citrix Files for Outlook
- Citrix Workspace account with a Citrix Content Collaboration entitlement

Logon

1. Configure the Citrix Workspace app using a Citrix Workspace Store URL. The Store must contain a Citrix Content Collaboration entitlement.
2. When prompted for authentication, sign in using your Citrix Workspace credentials.
3. Start Citrix Files. You are automatically signed on.

Logoff

Any of the Citrix Workspace-compatible desktop applications can issue a logoff.

To log off from Citrix Workspace app, right-click the Citrix Workspace app icon in the notification area and select Log off. This action also logs off Citrix Files, if running.
To log off from the Citrix Files app, right-click the notification area icon and select **Settings**. Choose **Log Out** to log off. This action also forces a logoff of Citrix Workspace app.
Known limitations

- If the Store URL is not configured, or if the Store does not contain a Citrix Content Collaboration account, the Citrix Files client does not attempt Citrix Workspace authentication. Instead, it uses ShareFile authentication.
- Citrix Files supports single sign-on only by using the primary store URL configured in Citrix Workspace app.

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 logon 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 StorageZones 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, StorageZone 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Application</td>
<td>If disabled, Citrix Files exits before mounting any drives or displaying any UI.</td>
</tr>
<tr>
<td>Enable Auto Check-out</td>
<td>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.</td>
</tr>
<tr>
<td>Enable on-premises Connectors</td>
<td>If disabled, Network Share, Sharepoint, and Documentum connectors are not visible in Citrix Files.</td>
</tr>
<tr>
<td>Enable Personal Cloud Connectors</td>
<td>If disabled, Personal Cloud and Office 365 Connectors are not visible in Citrix Files.</td>
</tr>
<tr>
<td>Enable Auto-update</td>
<td>If disabled, Citrix Files does not automatically update to the latest version.</td>
</tr>
<tr>
<td>Delete Cache on Exit</td>
<td>If enabled, downloaded file contents are removed when the application exits.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>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.</td>
</tr>
<tr>
<td>Cache Location</td>
<td>Configures the location of the file content cache. By default, the location is <code>AppData\Local\Citrix\Citrix Files\PartCache</code>. If a custom path is set, that folder must exist.</td>
</tr>
</tbody>
</table>
## Setting Purpose

**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.

**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.

<table>
<thead>
<tr>
<th>Folder type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Folders</td>
<td>Personal Folders&lt;FolderName&gt; or %personal%&lt;FolderName&gt;</td>
</tr>
<tr>
<td>Shared Folders</td>
<td>Shared Folders&lt;FolderName&gt;&lt;FolderName2&gt; or %shared%&lt;FolderName&gt;</td>
</tr>
<tr>
<td>Favorites</td>
<td>Favorites or %favorites%&lt;FolderName&gt;</td>
</tr>
<tr>
<td>Network Shares connector</td>
<td>Network Shares&lt;ConnectorName&gt; or %networkshares%&lt;ConnectorName&gt;</td>
</tr>
<tr>
<td>SharePoint connector</td>
<td>SharePoint&lt;ConnectorName&gt; or %sharepoint%&lt;ConnectorName&gt;</td>
</tr>
<tr>
<td>Box connector</td>
<td>Personal Cloud\Box or %personalcloud%\Box</td>
</tr>
<tr>
<td>Dropbox connector</td>
<td>Personal Cloud\Dropbox or %personalcloud%\Dropbox</td>
</tr>
<tr>
<td>Google Drive connector</td>
<td>Personal Cloud\Google Drive or %personalcloud%\Google Drive</td>
</tr>
<tr>
<td>OneDrive connector</td>
<td>Personal Cloud\OneDrive or %personalcloud%\OneDrive</td>
</tr>
<tr>
<td>Office365 connectors</td>
<td>Office 365&lt;ConnectorName&gt; or %office365%&lt;ConnectorName&gt;</td>
</tr>
<tr>
<td>Root of account (default view)</td>
<td>\</td>
</tr>
</tbody>
</table>
Citrix Files for Android

April 22, 2020

About

Citrix Files for Android helps you exchange files easily, securely and professionally.
Designed for business, Citrix Files for Android 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 Android device — any time, anywhere.

Download Citrix Files for Android at Google Play Store

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

Fixed issues

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]

Fixed issues in 2020

- German umlaut characters, such as ä, ü, and ö, might not be usable while editing documents in Citrix Files for Android. [SFAND-5270]
- Copy link might not display all the apps on Samsung Android 10. [SFAND-5290]

Fixed issues in 2010

- Authman Lite SDK integration into Citrix Files to provide a more seamless experience across apps. [SFAND-5195]
- Quick Edit for Android might exit unexpectedly after trying to add a picture from Gallery or Camera to a spreadsheet. [SFAND-5280]
Fixed issues in 1909

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

Fixed issues in 1908

- Redirects from http:// to https:// URLs might not resolve as expected. [SFAND-5204]

Fixed issues in 1907.5

- Attaching a file from within Secure Mail might cause Citrix Files for Android to exit unexpectedly. [SFAND-5175]

Fixed issues in 1907

- Citrix Files for Android might not route connections through tunnels. [SFAND-5121]

Fixed issues in 1906.5

- When recording audio longer than one hour and the device’s screen get locked, the recording stops on devices running Android 8 or later, [SFAND-5178]

Fixed issues in 1906

- Large PDFs might not open or render correctly due to a large memory requirement. [SFAND-5058]
- PDFs using the Gotham font might not display text correctly when viewed through Citrix Files for Android. [SFAND-5100]
- Opening a shared link on Citrix Files for Android when no account has been configured results in an error. [SFAND-5114]
- Citrix Files for Android exits unexpectedly when attempting to open a .txt file when using 64-bit libraries. [SFAND-5142]
- The information in Folder Details might not update after renaming a folder. [SFAND-5171]
- The error “Your organization does not allow this action error when uploading files.” might appear when attempting to upload files. [TSCASE-134523]
- Attachments might be corrupted when attempting to open a file in Citrix Files for Android saved from Secure Mail 19.3.5. [TSCASE-147718]
Fixed issues in 7.6.2

- Session IDs might be visible in logs for jailbroken and rooted devices. [SFAND-5073]
- Using single sign-on to sign on to network shares might fail. [SFAND-5093]
- Files might not open correctly using certain apps and QuickEdit. [SFAND-5120]

Fixed issues in 7.6.1

- Users might not be able to navigate to home drives. [SFAND-5072]
- When using a stand alone connector, a blank screen might display when navigating back through the connector. [SFAND-5095]

Fixed issues in 7.6

- Certain elements of PDFs might not display correctly. [SFAND-5022]
- Adding a user to a folder using Shared Contacts might not work correctly. [SFAND-5035]

Known issues

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.
Known issues in 1910
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 1908
No new issues have been observed in this release.

Known issues in 1907.5
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 1906.5
No new issues have been observed in this release.

Known issues in 1906
No new issues have been observed in this release.

Known issues in 7.6.2
No new issues have been observed in this release.

Known issues in 7.6.1
No new issues have been observed in this release.
Known issues in 7.6

No new issues have been observed in this release.

System requirements

OS requirements

Android 5.x (Lollipop) or later

Citrix Files for Gmail

January 15, 2020

About

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.

Fixed issues

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.
System requirements

Browser requirements

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

Citrix Content Collaboration requirements

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

Citrix Files for iOS

April 27, 2020

About

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

Designed for business, Citrix Files for iOS 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 iOS device — any time, anywhere.

Download Citrix Files for iOS at Apple App Store.

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

Fixed issues

Fixed issues in 2040

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

Fixed issues in 2030

Uploading a file using Citrix Files might cause an error. [SFIOS-6419]
Fixed issues in 2010

- Push notifications might not work in iOS 13. [SFIOS-6363]
- Pausing audio recordings in Citrix Files for iOS might cause a recording error. [SFIOS-6400]

Fixed issues in 1910.5

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

Fixed issues in 1910

- MDX encryption might cause files to not open. [SFIOS-5468]
- After uploading one file, the Close button might be missing. Users are unable to upload more files and must restart the app. [SFIOS-6297]

Fixed issues in 1909.5

When the Inbound Document Exchange policy is set to restricted, opening files from Secure Mail might fail. [SFIOS-6344]

Fixed issues in 1909

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

Fixed issues in 1907

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

Fixed issues in 1906

- Session ID cookie is present in log file. [SFIOS-5458]
- Citrix Files 7.1 selects current folder as the default location. [SFIOS-6262]

Fixed issues in 7.10

- PDFs might not be able to be edited using QuickEdit 7.8. [QEIOS-154]
- Videos recorded using the “Take Video” option might not play on devices running iOS 12.2. [SFIOS-6269]
Citrix Content Collaboration

- Citrix Files for iOS might exit unexpectedly when deleting a Word file and then opening an Excel file in the Recents tab. [SFIOS-6286]

**Fixed issues in 7.9**

- PDFs uploaded to Citrix Files might display with a black screen. [SFIOS-5420]
- Attempts to save an audio file might fail when double-tapping Done quickly. [SFIOS-5421]
- Opening PDF files might cause Citrix Files for iOS to exit unexpectedly. [SFIOS-5433]
- The display might not restore to normal size after viewing a document in full screen on the iPhone XR. [SFIOS-5437]
- Files edited in offline mode might not upload correctly once back online. [SFIOS-5451]
- PDFs using the Gotham font might not display correctly. [SFIOS-6238]
- Videos might not play on devices running iOS 12.2. [SFIOS-6252]

**Fixed issues in 7.8**

- Users are unable to log on using the “Log in with my company credentials” option. [SFIOS-5396]
- When using two-factor authentication, Citrix Files for iOS keeps requesting to log on. [SFIOS-5417]
- When attempting to access a personal cloud connector that has been unlinked, Citrix Files for iOS exits unexpectedly. [SFIOS-5422]

**Known issues**

**Known issues in 2040**

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 2010**

No new issues have been observed in this release.

**Known issues in 1930**

No new issues have been observed in this release.
Known issues in 1910

No new issues have been observed in this release.

Known issues in 1909.5

No new issues have been observed in this release.

Known issues in 1909

When the Inbound Document Exchange policy is set to restricted, opening files from Secure Mail might fail. [SFIOS-6344]

Known issues in 1907

No new issues have been observed in this release.

Known issues in 1906

No new issues have been observed in this release.

Known issues in 7.10

No new issues have been observed in this release.

Known issues in 7.9

No new issues have been observed in this release.

Known issues in 7.8

No new issues have been observed in this release.

System requirements

OS requirements

iOS 10 or later
Citrix Files for Mac

January 15, 2020

About

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.

Download Citrix Files for Mac at Citrix Downloads.

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

Fixed issues

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 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]
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. [SFWGTM-515]
- 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. [SFWGTM-515]
- 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. [SFWGTM-515]
- 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. [SFWGTM-515]
- 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.

System requirements

OS requirements

- macOS 10.12 Sierra or later

Other requirements

- Local administrator rights are needed to install the app.

Citrix Files for Mac includes open source software licensed under the terms defined in the following document: Citrix Files for Mac open source notices.

Citrix Files for Outlook

January 23, 2020

About

Citrix Files for Outlook 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 at Citrix Downloads.

For information about new features, see What’s new.
Fixed issues

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 a file loads. [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]
Citrix Content Collaboration

- 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.
System requirements

OS requirements

• Windows 7 or later

.NET requirements

• Microsoft .NET Framework 4.6 or later

Microsoft Outlook version requirements

• 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.

Citrix Files for Outlook Online

January 15, 2020

About

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.

Note:

Citrix Files for Outlook Online works with macOS and Microsoft Office for Mac.

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

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.

System requirements

Microsoft account requirements

- Outlook.com
- Office 365
- Microsoft Exchange
  - 2013 SP1
  - 2016

Outlook requirements

- Outlook Web App
- Outlook for Mac 2016 or later (version 15.33 or later)
- Outlook for Windows 2013 or later is supported, but Citrix recommends using Citrix Files for Outlook
- For more information, see Microsoft Office requirements
Citrix Content Collaboration

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

Citrix Files for Windows

January 15, 2020

About

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.

Download Citrix Files for Windows at Citrix Downloads.
For information about new features, see What’s new.

Fixed issues

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 documents 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 Content Collaboration

- Citrix Files incorrectly shows “Your access token might be expired or revoked” when logged onto 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, 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 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

Note:
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 \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.

System requirements

OS requirements

• Windows 7 or later
• Windows Server 2008 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.

Citrix Files on Citrix Virtual Apps and Desktops

December 18, 2019
Citrix Content Collaboration

Citrix Files on VDA

When installed on a Virtual Delivery Agent (VDA), the Citrix Files app is set to launch automatically inside the published application or desktop and created a mapped S: drive to your Files content. Citrix Files can be set to start as part of the user’s windows logon process.

Publishing the CitrixFiles.exe application directly is not supported.

Installation

1. Install the VDA.
2. After the VDA is set up, install the Citrix Files for Windows application on your VDA.

Note:
Starting with VDA 1808, Citrix Files for Windows is an optional component that can be selected during the installation process.

Installing the VDA through the command line

To install the VDA using the command line, use the /IncludeAdditional parameter to include “Citrix Files for Windows” as an install component. For example:

```
XenDesktopVDASsetup.exe /quiet /verbosemlog /optimize /PORTNUMBER 80 /logpath
'"C:\CitrixInstallationLogs\TSVDA'/components VDA,PLUGINS /ENABLE_HDX_PORTS
/ENABLE_REAL_TIME_TRANSPORT /disableexperiencemetrics /NOREBOOT /MASTERIMAGE
/IncludeAdditional "Citrix Files for Windows"/NORESUME
```

Note:
This option is only available on VDA 1808 and later.

Authentication

When accessed through Citrix Workspace, the user’s logon information is automatically passed to the VDA session, allowing users to use single sign-on for their Files account. Authentication requires VDA version 7.18 or later and Delivery Controller.

When deployed in an on-premises Citrix Virtual Apps and Desktops environment, Citrix Files can be set up to use SAML single sign-on using Windows authentication or a user name and password through the Citrix Files web logon screen. To configure Windows integrated SAML single sign-on, you must specify your account subdomain in the AccountGroup policy setting. For more information on Group Policy configuration and set up, see Knowledge Center article CTX228273.
Application session lingering

Sometimes, the user might close a Citrix Virtual Apps application before the Citrix Files upload was able to complete. Configure session lingering for published applications to allow Citrix Files to complete the upload before the Citrix Virtual Apps session is terminated.

To configure application session lingering, edit your Delivery Group from Citrix Studio:

File cache

Citrix Files caches accessed files on disk for faster performance. By default, each user’s cache is set to 5,120 MB. The size and extra configuration of the cache can be set through group policy. Cache size works best by considering available disk space and the number of users planning to access the server at a given time.

Roaming profiles

The Citrix Content Collaboration data and cache directories are excluded to avoid profile bloat. The following path is where the default cache and logs are stored:

%userprofile%\appdata\local\citrix\Citrix Files

User settings are stored in the roaming path as follows:
Auto-updates

Auto-update allows for new versions of the tool to be updated for end user clients. Auto-update is disabled automatically when Citrix Files is installed on a VDA.

Group Policy definitions

Administrators can configure user or computer settings via Group Policy definitions. For information on the policy templates and available policies, see Group policy definitions for Citrix Files for Windows.

Open files in Citrix Virtual Apps

Opening files in a published app allows users to work on content when the software needed is not installed locally.

Enable opening files in published applications

1. Enable the following services in the Citrix Cloud console. Users must have licenses for the following as well.
   - Citrix Content Collaboration
   - Citrix Virtual Apps
   
   Note: VDA version 1808 or later must be installed for this feature to work.

2. Ensure Citrix Files is installed on the VDA.

3. Set up File Type Association in the console. For each file type that you plan to associate with this feature, you must enable FTA for that particular application you want to start.

   - Setting a Session Lingering value for your delivery group when enabling this feature is recommended. This is to allow sufficient time for the uploads to complete in the event a published application is closed quickly before the upload can complete. To do this, enable your Delivery Group and set a value for Application Lingering.
   - VM hosted apps published on Desktop VDAs are not supported.
Note:
If there are multiple apps associated using the same file type, the first one is used.

Editing files in a published application

1. Users must have licenses for Citrix Content Collaboration and Citrix Virtual Apps.
2. In Citrix Workspace, users can select files in web or desktop mode to open those files in a published app.
   - **Open** is only an option when there is a published app associated with the file type.
   - When there is no published app associated with the file type, clicking the file opens the file in preview mode.
3. Users can also open a file in a published app by right-clicking on the file or from preview mode.
4. Save changes and close the tab to exit editing mode.

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