

Quick Reference Guide

Overview

SAFE Transmission allows you to transfer large volumes of data between your company and Wells Fargo securely. When you use any Wells Fargo treasury management product requiring data transmission, such as ACH, account reconciliation, and lockbox, the security features in the SAFE Transmission service will protect your files and data from unauthorized access during transit.

SAFE transmission provides the following benefits:

- **Single sign-on:** Access the service through the *Commercial Electronic Office® (CEO®)* portal, where a single ID opens all applications.
- **Multifactor authentication:** Prevent unauthorized access with multifactor authentication, including use of an RSA SecurID® token when accessing the service through the *CEO* portal.
- **Support for multiple internet browsers:** Deliver or retrieve files securely over the internet using https. For additional information, go to:
<https://wellsoffice.wellsfargo.com/ceportal/signon/public/SystemReqs.jsp>
- **Convenient online user management:** As a *CEO* portal user, you can manage user access through the *CEO* Self Administration service.
- **Digital certificate management:** Issue and renew digital certificates by accessing SAFE Transmission through the *CEO* portal; pertains to SAFE automation only.
- **IP address management:** Add, update and delete IP addresses used to validate authorized automated connections to SAFE Transmission by accessing SAFE Transmission through the *CEO* portal (pertains to automated connections only).
- **Anti-virus scanning:** All inbound and outbound files are automatically scanned for viruses and malware, reducing risks to your internal systems.

Value-added services are available at no additional charge and include:

- **PGP encryption:** Increase the security and confidentiality of your sensitive data with PGP encryption. Wells Fargo provides its public PGP key to encrypt files that you upload using the SAFE Transmission service. Once we receive the file, we decrypt it using our private PGP key.

For files that you download, you provide your public PGP key to Wells Fargo to encrypt the files before we place them in your outbound folder. Once you download a file, you can decrypt it using your private PGP key.

Note: “Pretty Good Privacy” (PGP) encryption is an industry standard. You must support PGP encryption in your system environment in order to use this service option.

Overview, cont.

• Transmission messaging:

- **Alerts:** Receive alerts when a file fails a service check and can't be delivered to its destination system within Wells Fargo. See the [File upload value-added services performed](#) section for information on service checks.
- **Notifications:** Choose to receive courtesy notifications when:
 - A file is ready for download
 - A file has been successfully received by Wells Fargo
- **Expected Events service:** Receive critical notification when an expected event occurs or fails to occur within the expected timeframe for specified recipients. This service provides notification when:
 - An expected file is not received
 - An unexpected file is received outside the expected window
 - A zero-byte file is received
 - A file is pending download
 - A pending file is purged
- **Validation environment:** A separate validation environment is available for testing purposes.
- **Custom file renaming:** For files you receive from Wells Fargo, the file-naming convention can be customized to match your internal systems for quick identification and reference.
- **Client automation software:** Wells Fargo can provide client automation software.

Transmission folders

User authorization for accessing folders

Users can view and transmit files only for those folders they are authorized to use. Separate product folders are created for each Treasury Management product/service you have for which SAFE Transmissions is set up. More than one product folder may be created for each product/service. Users can be authorized for one or many product folders. The user authorization can be performed and controlled within the *CEO* Self Administration service, if you subscribe to this service.

Storage

You can request one of the following file storage periods:

1 day	2 days	3 days	4 days	5 days
6 days	7 days	15 days	31 days	

Note: The default storage period is seven calendar days. The storage period applies to both the files in the file upload history and in the download area and the storage period can be the same or different for each.

Together we'll go far



Naming conventions for uploading files

Allowable characters

For files you upload to Wells Fargo, the following characters are allowed in a file name:

- Uppercase letters A-Z
- Lowercase letters a-z
- Digits 0-9
- Hyphen (-)
- Period (.)
- Underscore (_)
- Space

Note: No other characters are allowed.

File extensions

The following file name extensions are **not** allowed:

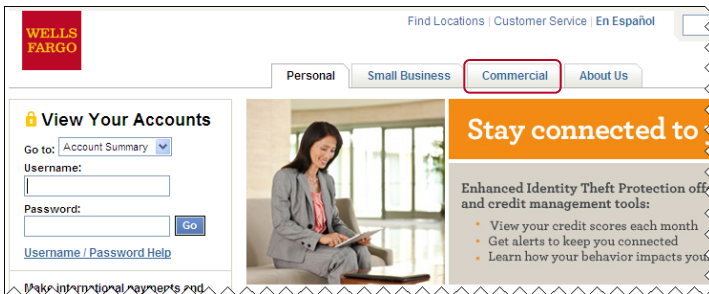
BAT EXE RAR CMD HTA SCR COM JOB
SDA CPL OCX SHS DLL PIF VBS

Accessing SAFE Transmission

Note: If this is your first time accessing the *CEO* portal, you will need to complete several steps required for new users. For additional information, click the *First Time Sign On Tips* link from the *CEO* portal home page.

1. To access the *CEO* portal, go to **wellsfargo.com**.

The Wells Fargo home page displays.



2. Click the **Commercial** tab.

The Commercial home page displays.



3. Click the *Commercial Electronic Office* portal sign on.

The *CEO* portal home page displays.



Accessing SAFE Transmission, cont.

Note: To bookmark the page, click **Bookmark this page** and follow the instructions.

4. Enter your **Company ID**, **User ID**, and **Password**.

Note: Your IDs and RSA SecurID® token device (if required) are available from your company administrator. Your temporary password is included in your *CEO* welcome letter.

5. Click **Sign On**.

Note: For information on how to reset your password, click **Password Reset Tutorial** from the home page.

Signing on using your token passcode

1. From the **Token Authentication** page, enter your token passcode in the **Token Passcode** field. Your token passcode is your PIN plus (without a space) your RSA SecurID token code.

Example: If your PIN is “**1fargo**” and the token code is “**234836**,” the token passcode would be “**1fargo234836**.”

2. Click **Continue**.

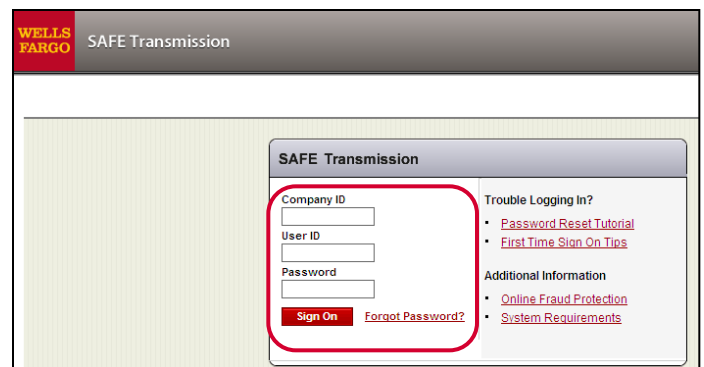
You have successfully signed on to the SAFE Transmission service

CEO portal impairment

The Wells Fargo *CEO* portal is designed for high availability. However, if for any reason it is not available, you may still be able to access SAFE Transmission using the same credentials and sign-on information, by accessing a separate web address. Follow the instructions below to perform your file uploads/downloads.

1. Go to **https://safe-t.wellsfargo.com**.

The SAFE Transmission sign-on page displays.



2. Enter the same information you would normally enter on the Wells Fargo *CEO* portal sign-on page: **Company ID**, **User ID**, and **Password**.
3. Click **Sign On**.
4. After you sign on, select the same functions you normally would by accessing SAFE transmission through the Wells Fargo *CEO* portal.

Using the validation environment

As part of the SAFE Transmission value-added services, a separate validation environment is available for you to use when conducting the file format testing.

To access the SAFE Transmission validation environment, go to: **https://safe-t-validate.wellsfargo.com** instead of signing on to the *CEO* portal. You will use the same user ID, password, and token passcode as you would use to access SAFE Transmission through the *CEO* portal.

The SAFE Transmission validation environment offers the following features:

- **Separate testing environment:** The validation environment mirrors your file transfer setups. Product folder names and identifiers, user authorization, and value-added services provide the same functionality in the test environment as in production with the exception of the email delivery feature that is coming soon.
- **Multi-user application profiles:** The SAFE Transmission validation environment mirrors the SAFE Transmission service. The same user authorizations are enforced for each product that is set up.
- **PGP encryption:** The SAFE Transmission validation environment uses the same Pretty Good Privacy (PGP) controls as set up in the SAFE Transmission service to replicate the transfer experience.
- **Transmission alerts:** The SAFE Transmission validation environment alerts users when a file fails value-added service checks that would prevent the SAFE Transmission service from delivering the file to its destination within Wells Fargo. Look for a future feature to include email delivery.
- **Transmission messages:** The SAFE Transmission validation environment provides the same courtesy notifications and messaging that are available in the SAFE Transmission service. Look for a future feature to include email delivery.

SAFE Transmission home page

Based on your authorizations, the following options are available on the SAFE Transmission home page:

- Upload Files
- File Upload History
- Download Files

Note: Wells Fargo recommends that you authorize two users to access SAFE Transmission to allow for business continuity planning or backup purposes.

Uploading files

1. Click **Upload Files**.

The Upload Files page displays.

Note: You can upload up to five files at a time. Do not skip rows when selecting your files.

2. Click **Browse** in the first file column to select your file for upload.
3. Select the product folder in the **Product Folder** dropdown menu.
Note: You will only see product folders to which you have been authorized to upload.
4. Click **Upload**.

When the upload begins, the system displays the estimated upload time.

Note: Click **Cancel** to stop the upload.

When the upload is complete, the system displays the status of the uploaded file(s) in the **Status** column.

5. Click **Print** to print the information for your records. From this page you can also click **Return to Upload Files** to upload another file.

Uploading files, cont.

To cancel an upload for a single file

1. When a file upload begins, the system displays the upload progress. Click **Cancel** to cancel the upload process.
2. The system asks you to confirm that you want to stop the file upload. Click **OK**.

To cancel an upload for multiple files

To understand how cancelling an upload works for multiple files, let's use an example of uploading three files, and canceling the upload process while the system is uploading file 2.

- The upload of file 1 is complete and is not affected.

Note: Contact Treasury Management Client Services if you did not want file 1 to be uploaded to determine if the file has been processed by the receiving application.

- The upload of file 2 is cancelled.
- The system does not upload file 3.

If you want all three files uploaded, you would need to upload file 2 and file 3 again. However, you would not need to upload file 1 again because it was already uploaded when you cancelled the upload process.

The following is how the files would be listed on the Upload File History page:

- File 1: **Uploaded** status.
- File 2: **Cancelled** status.
- File 3: Would not be listed.

Note: For information on allowable characters and file extensions, refer to the [Naming conventions for uploading files](#) section.

File upload value-added services performed

Each time you upload a file, the system does the following:

1. Renames the file to include:
_TID[number]_datetime
The date format is YYYYMMDD, and the time format is HHMMSS.
2. Scans the file for viruses.
3. Verifies that the file name does not include any prohibited characters. See the [Naming conventions for uploading files](#) section for more information.
4. Verifies that the file name extension is correct for the type of file being uploaded and does not include a prohibited file name extension. See the [File extensions](#) section for more information.
5. Verifies that the file name includes the required product identifier.
6. Verifies that the file is encrypted with PGP and decrypts the file.
Note: This applies to sessions using PGP only.
7. Verifies the expected headers are present.

The system sends you an email if any of the file check processes fail.

File Upload History

You can display information for files uploaded during the period designated by your company. The default storage period is seven days.

Note: You can request that the storage time period be changed. For further information, refer to the [Storage](#) section.

To display your File Upload History

1. Click **File Upload History**.

The File Upload History page displays.

File Upload History

To view upload history for another product, select [View Another Folder](#).

ACH (Payroll)

[View Another Folder](#)

Display 10 | 25 | 50 | 100 Items Per Page

Page 1

Viewing 1 to 2 of 10 items

Previous Page

Next Page

File Name	Size	Date/Time	User ID	Status	Batch ID
1. ACHFile1.txt	2.6 MB	03/15/20XX 02:25 PM PT	HWELLS	Uploaded	1188B888733
2. ACHFile2.txt	1.53 MB	03/14/20XX 02:00 PM PT	HWELLS	Uploaded	1188AD7E214

Display 10 | 25 | 50 | 100 Items Per Page

Page 1

Viewing 1 to 6 of 10 items

Previous Page

Next Page

Fields of information on the File Upload History page include:

- File Name
- Size
- Date/Time
- User ID
- Status
- Batch ID

If you have multiple product folders, you can display the file upload history for another product folder by clicking the **View Another Folder** link and selecting the product folder from the list.

To open or save an uploaded file

1. From the File Upload History page, click the file link in the **File Name** column.

File Upload History

To view upload history for another product, select [View Another Folder](#).

ACH (Payroll)

[View Another Folder](#)

Display 10 | 25 | 50 | 100 Items Per Page

Page 1

Viewing 1 to 2 of 10 items

Previous Page

Next Page

File Name	Size	Date/Time	User ID	Status	Batch ID
1. ACHFile1.txt	2.6 MB	03/15/20XX 02:25 PM PT	HWELLS	Uploaded	1188B888733
2. ACHFile2.txt	1.53 MB	03/14/20XX 02:00 PM PT	HWELLS	Uploaded	1188AD7E214

Display 10 | 25 | 50 | 100 Items Per Page

Page 1

Viewing 1 to 6 of 10 items

Previous Page

Next Page

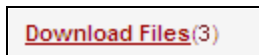
Note: If the system does not display a link for a file, that file was not successfully uploaded. Refer to the status of the file in the **Status** column.

A File Download page displays.

2. Click **Open** to open the file, or click **Save** to save the file.

Downloading files

The **Download Files** link indicates if you have files available for download. In the example below, there are three files available to download. Only product folders that you are authorized to view display.

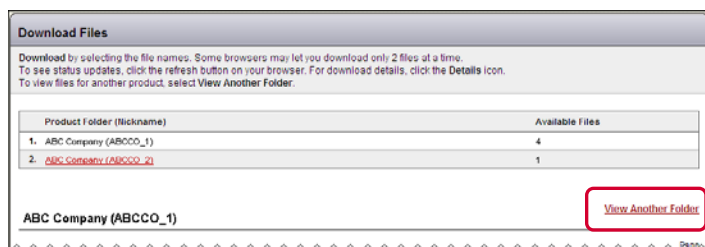


Note: Files remain available to download for the period designated by your company (usually seven calendar days).

To download a file

1. Click **Download Files**.


The Download Files page displays the number of files available to download for each product folder and lists the files to download for the first product folder.



Note: If you have multiple folders and want to download a file for another product folder, click **View Another Folder** and select the product folder from the pop-up list.

2. Click the **File Name** link for the file to download.
3. When asked whether to open or save the file, click **Save**.
4. Select the download location for the file, and click **Save**.

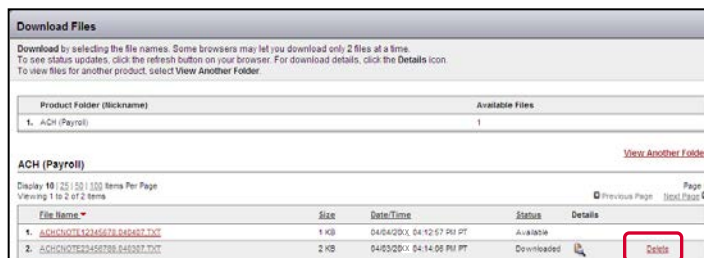
When you return to the Download Files page, the downloaded file initially displays with a **Downloading** status. Click **Refresh** to update the status.

5. Click the details icon () to view more information about the file including:
 - Date and time the download was available
 - Date and time the file was downloaded
 - User ID of person who downloaded the file

Downloading files, cont.

To delete a file

You can delete a file after it has been retrieved.



1. From the Download Files page, click **Delete** for the applicable file.

A pop-up displays, confirming that you want to delete the file.

2. Click **OK** to delete the file. To cancel the deletion, click **Cancel**.

Sign off the SAFE Transmission service

1. From the SAFE Transmission service main page, click **Sign Off** in the upper right-hand corner.

The system returns to the *CEO* portal main page.

Credential protection

As a reminder, Wells Fargo never requests that you send confidential information (IDs, passwords, and PINs) through emails, websites, pop-up windows, or unsolicited telephone calls.

You should consider these attempts as potentially fraudulent and report them immediately, without responding to them, to **ReportPhish@wellsfargo.com**. If you do disclose confidential information to a suspicious or fraudulent source, you should immediately call your relationship manager, customer service contact, or 1-800-289-3557.