

SAFE Transmission

Reference Guide

Together we'll go far



Contents

1	Overview
1	About SAFE Transmission
1	Getting started
1	SAFE Transmission features and functionality
1	Company ID
1	Product folders
2	Product folder presentation
2	Product folder customizations
2	Retention periods
3	Accessing SAFE Transmission
3	Connectivity options
3	Transmission protocol options
3	Protocol/URL mapping
4	User accounts
4	Browser users
4	Automated users
4	Remote user IDs
4	User roles
4	Transmission user
4	Transmission administrator
5	Security
5	Admin folder
5	Certificate management
5	IP address validation
6	PGP encryption
6	Supported ciphers
7	Value added services
7	Transfer options
7	Wells Fargo initiated transfers
7	Wells Fargo initiated transfer notifications
8	Custom file names
8	Standard inbound file naming conventions
9	Transmission messages
9	Alerts
9	Event notifications
10	Client software
11	SAFE Validation Environment
11	Accessing SAFE Validation
11	User accounts
12	Business continuity
13	Contacting your transmission partners
13	Transmission product team
13	Transmission technical support
13	Reference documents
13	Reports
13	Product documentation

Overview

About SAFE Transmission

The Secure Application File Exchange (SAFE) Transmission service is for use by Wholesale Banking customers and vendors, collectively known as trading partners. The service is built on a family of software products that manage the secure transfer of files over the Internet and provide value-added services to reduce risk while meeting your individual requirements. SAFE Transmission can be configured to support all your transmission needs.

Getting started

The following sections in this guide describe features and functionality provided through the SAFE Transmission service that will help you to:

- Select the appropriate access method for your business needs
- Customize the service to improve your transmission experience
- Understand SAFE Transmission's security controls to safeguard your sensitive data
- Identify support contacts to assist with future needs

In addition, this guide will help you define users, access methods, authorizations, and value-added services.

Note: Some SAFE Transmission features are self-service, meaning that you can make changes yourself without involving a bank representative. We will highlight these self-service features throughout the guide.

SAFE Transmission features and functionality

Company ID

The SAFE Transmission setup process starts by selecting or creating a *Commercial Electronic Office*® (*CEO*®) portal Company ID to use for your transmission setup. If desired, your *CEO* portal Company ID used for transmission can be different from the *CEO* portal Company ID you use for other portal products and services.

Note: When SAFE Transmission is added as a service to your *CEO* portal Company ID, it will be visible within the *CEO* portal Self Administration service, if you subscribe to that service.

Product folders

After your *CEO* portal Company ID is authorized for SAFE Transmission, products can be added and configured for data transfer with Wells Fargo. Transmission products can be set up with one or more product folders.

Transmission product folders are created based on the underlying products you have that use SAFE Transmission such as ACH, Account Reconciliation Plan (ARP), Payment Manager, etc.

Product folders represent the location in SAFE Transmission where files are uploaded to or downloaded from. Folders can also be used to limit user access to sensitive files such as payroll files or allow more extensive access to multiple users when restrictive access controls may not be needed.



Important! Wells Fargo recommends that you set up at least two users with access to each of your transmission product folders so you have a backup if the primary user is unavailable.

SAFE Transmission features and functionality, cont.

Product folders, cont.

Product folder presentation

Once established, product folders are available to authorized users through the SAFE Transmission web application for manual transmission users or through SAFE Transmission's gateway for automated users.

The SAFE Transmission web application displays the product name and nickname to authorized users. Authorized automated user IDs use pathnames to access folders. The SAFE Transmission web application is accessed through the *CEO* portal, or through a direct URL. See the [Accessing SAFE Transmission](#) section for additional information.

Product folder customizations

Nicknames

SAFE Transmission allows you to define a nickname for each product folder. Nicknames are visible to users who upload or download files manually through the SAFE Transmission web application. If you have multiple folders under a product and do not assign a nickname, you will see default values in the field.

Examples:

Default setting:	Account Recon – Positive Pay (ARPP_1), Account Recon – Positive Pay (ARPP_2)
-------------------------	--

Custom nickname:	Account Recon – Positive Pay (Western_Region), Account Recon – Positive Pay (Northern_Region)
-------------------------	---

Note: The folder nickname is not used by automated users.

Retention periods

Files that you send or receive from SAFE Transmission are stored in product folders for seven business days, by default, before they are purged. However, you can select different retention periods, from 1-7 days, 15 days, and 31 days. File retention is set by product folder and transmission direction.

For example, you could choose to set a three-day retention period for your inbound ACH payroll files and the corresponding outbound files set to seven days, or have your inbound Account Recon – Positive Pay files retained for seven days with the corresponding outbound files kept for 15 days.

Product folder retention settings are determined and set during the implementation process. Once changes are made to the file retention settings, any new file(s) received in the folder will be kept according to the new retention period. Existing files will be purged according to the previous setting.

Accessing SAFE Transmission

The SAFE Transmission service can be accessed by three different methods:

- Selecting Safe Transmission under My Services from the *CEO* portal at **www.wellsfargo.com/com/ceo**.
- Signing on to SAFE Transmission's web application directly at **<https://safe-t.wellsfargo.com>**.
- Connecting to the SAFE Transmission gateway (automated users only). See the [Protocol/URL mapping](#) section for additional information.

Connectivity options

SAFE Transmission supports multiple ways to connect to the service:

- Internet
- Virtual Private Network (VPN)
- Leased line

Transmission protocol options

The following protocols can be used in SAFE Transmission for Internet, VPN, or leased line connectivity.

- Hypertext transfer protocol over SSL (https) using your User ID, password, and digital certificate
- FTP over SSL (FTP/S) using your User ID, password, and digital certificate for authentication
- Secure FTP (S-FTP) using your User ID and key for authentication
- Secure FTP (S-FTP) using your User ID and password for authentication
- FTP with PGP (Pretty Good Privacy) using your User ID and password for authentication. This requires files to be PGP-encrypted
- Applicability Statement 2 (AS2) using your User ID, password, and digital certificate for authentication

Note: Transmission protocols that use a User ID and password only for authentication do not offer the best protection to safeguard funds transfers over the Internet. Wells Fargo recommends that you use a secure protocol that leverages stronger authentication for funds transfers.

Protocol/URL mapping

The table below provides web addresses (URLs) and ports that are used to connect to SAFE Transmission.

Protocol	URL	Port
FTPS (SSL)	safetrans.wellsfargo.com	21*
SFTP (SSH)	safetrans.wellsfargo.com	22 (RSA key)
SFTP (SSH)	safetrans.wellsfargo.com	122 (DSA key)
HTTPS	safetrans.wellsfargo.com	443
FTP with PGP	Safetranspgp.wellsfargo.com	21*
AS2	safetrans.wellsfargo.com	5000 or 5080

*FTP over SSL (FTP/S) and FTP with PGP are dual channel protocols, meaning that one channel controls the transmission connection and another channel is used for data transfer. SAFE Transmission uses port 21 for connectivity and high order ports 20,000 – 21,000 are used for data transfer. If your transmission protocol choice is FTPS or FTP with PGP, Wells Fargo recommends that you open ports to allow for data transfer over ports 20,000 – 21,000.



Important! Wells Fargo recommends you use URLs to connect to SAFE Transmission, not static IP addresses, as the IP addresses are subject to change. However, if you must use static IP addresses, or need to do so for firewall configuration, see the [Business continuity](#) section for IP address information.

User accounts

SAFE Transmission offers flexibility in user accounts and privileges. For transfers that you originate, you can choose between browser users and automated users.

For transfers that originate from SAFE Transmission to push data to you (known as Wells Fargo initiated transfers), you would issue a remote user ID to Wells Fargo.

Browser users

SAFE Transmission is fully integrated with the *CEO* portal. Browser users that are created under your *CEO* portal Company ID will be able to take advantage of the *CEO* portal's single sign-on functionality and security features.

The SAFE Transmission service requires token authentication to access the service through the *CEO* portal or by using the SAFE Transmission direct access URL.

Self service: You can use the *CEO* portal Self Administration service to set up and authorize browser users on SAFE Transmission and grant users access to specific product folders.

New users who are set up through Self Administration will be issued tokens as part of the process.

Automated users

If you prefer to schedule your file transmission activity, you can choose to have automated user IDs created on SAFE Transmission. Automated User IDs are system accounts and are not issued to a person. You will be asked to provide at least one contact to be associated with each automated user ID issued to you. The automated user contact is the responsible party that Wells Fargo will contact for issue resolution and to perform normal maintenance associated with the automated user.

When deciding if automated user IDs are appropriate for your needs, it is important to consider the availability, expertise, and comfort level with FTP tools and schedulers of your company's technical resources.



Important! Wells Fargo recommends that if you choose to use automated user IDs, you also set up browser user IDs who are authorized to the same product folders as the automated user IDs. This will provide an alternative method for transferring critical files in a crisis situation when automated transfers may not be available.

Remote user IDs

Remote user IDs allow SAFE Transmission to authenticate to external sites and deliver files. Remote user IDs are issued by you to SAFE Transmission. This value-added service is also called Wells Fargo initiated file transfers or outbound push transfers. Wells Fargo initiated file transfer information is covered in the [Transfer options](#) section.

User roles

Transmission user

Within the SAFE Transmission channel, users who are authorized to upload files, download files, or view file upload history are called transmission users.

Transmission administrator

Transmission administrators are privileged users in the SAFE Transmission channel. Transmission administrators are trading partner representatives who are responsible for authentication credential and key exchange with Wells Fargo. They can access the Admin folder to download client software and documentation. Transmission administrators partner with the SAFE Transmission teams to preserve the security of your sensitive data.

Depending on your security policies and staffing, you can allow transmission users to have administrator rights or keep the roles separate.

Security

At Wells Fargo, safeguarding your confidential data is a priority. Some of the secured features and controls associated with the SAFE Transmission service are described in this section.

Admin folder

The SAFE Transmission admin folder is used to exchange IDs, passwords, and authentication credentials for automated and remote user IDs. This folder is accessible through the browser application only and is a security control mechanism Wells Fargo uses to protect your confidential information.

Transmission administrators are authorized to the admin folder. By using the admin folder to exchange keys or send and receive user IDs and passwords, you have more confidence that only your authorized representative has access to these critical transmission components.

The admin folder is also used to transfer information related to your automated transmission setup such as folder/directory path information, Secure Client software, and other information specific to your implementation request.

Certificate management

Digital certificates are required for authentication with any automated user protocol that is conducted over SSL. Only transmission administrators can request or renew digital certificates used for authorization on the SAFE Transmission platform.

For increased security, Wells Fargo digital certificates use a SHA-256 hashing algorithm and 2048-bit RSA keys. If your system is not able to support this increased security, at the time you create a digital certificate you can request a Wells Fargo digital certificate for SHA1 and 1024-bit RSA keys.

Self service: Manage Certificates and Keys is a function available through the SAFE Transmission web application. Using the certificate management function, your transmission administrator can request new digital certificates or renew expiring digital certificates on demand.

IP address validation

Automated connections to SAFE Transmission are checked to ensure the connection originates from an IP address that is authorized for the user ID. If the IP address is valid for the user ID, the transmission session continues. IP address validation ensures that only your authorized users from approved locations can send or receive data on the channel. If the IP address for the user ID is not valid, the session is terminated.

Note: Customers with automated user IDs that were set up prior to July 2013 will be contacted about enabling the service. New automated users set up after July 2013 will be enabled for IP address validation at implementation time.

Self service: Manage IP Addresses is a service available through the SAFE Transmission web application. Using the Manage IP Addresses function, your transmission administrator can add, update or delete IP addresses your company uses to initiate sessions with SAFE Transmission. Changes made using Manage IP Addresses are effective on the next connection attempt for the automated user ID.

Security, cont.

PGP encryption

If you want the additional security of file-based encryption, the SAFE Transmission service supports PGP and Gnu Privacy Guard. These are based on the open PGP standard, as defined by RFC 4880. You must be able to support the PGP standard in your system environment in order to use this SAFE Transmission service option.

In SAFE Transmission, PGP is configured at the product folder level and is directional. You can choose to encrypt any file you submit to Wells Fargo, and any file you receive from Wells Fargo. For example, you can encrypt your ACH payroll file sent to SAFE Transmission, but not your ACH confirmation you receive or download from the channel.

PGP keys are valid for two years from issue date. Before the key expires, notices are sent to transmission administrators and PGP contacts to request a new key. Valid keys are required to encrypt files sent to SAFE Transmission as well as files that SAFE Transmission digitally signs before making a file available for pickup or push.

As a security precaution, SAFE Transmission will validate digital signatures on all files delivered to the channel. If a file is expected to be digitally signed but the signature is invalid or missing, the file will be rejected and the user will be alerted. SAFE Transmission digitally signs all PGP-encrypted files that are ready for pickup or push.

Self service

Manage Certificates and Keys is a service available through the SAFE Transmission web application. Using Manage Certificates and Keys, your transmission administrator can request a new PGP key or retrieve the current, active key. Your transmission administrator can also activate the key online. When a key is activated, the next PGP activity (decrypting or signing) will take place using the new key.

Supported ciphers

SAFE Transmissions supports the use of these cryptographic algorithms with PGP:

- AES with 256-bit or greater keys
- 3DES with 256-bit or greater keys
- CAST5 with 128-bit keys (not allowed for use with native FTP – that is FTP with PGP)

How the service works

You will exchange PGP public keys with SAFE Transmission using the admin folder. For files that you send to SAFE Transmission, you will need to encrypt each file with SAFE Transmission's public PGP key. You will also digitally sign each encrypted file with your private PGP key.

SAFE Transmission will validate your digital signature on each PGP-encrypted file received. If the signature is valid, SAFE Transmission will decrypt the file and processing continues. If the signature is missing or invalid, SAFE Transmission rejects the file and alerts the appropriate user or contacts.

Files you receive from SAFE Transmission will be encrypted using your public PGP key and digitally signed with SAFE Transmission's private PGP key. Once you have the file, your authorized users can:

- Validate our digital signature to ensure the file originated from SAFE Transmission and that the file was not altered in transit.
- Decrypt the file for further processing.

Value added services

Transfer options

Within the channel, transfers to deliver files to SAFE Transmission must be initiated by our trading partners. SAFE Transmission does not support remote connections to pick up files. Files that are available for pickup from SAFE Transmission can be pushed to trading partners as a value-added service.

Wells Fargo initiated transfers

SAFE Transmission can initiate file transfers to you by signing on to your system and pushing files. This service ensures that you will receive your critical files shortly after they are available to the SAFE Transmission service by the originating service at Wells Fargo. There is no need to create scripts and schedules to check for files and retrieve them.

Wells Fargo initiated transfer notifications

In conjunction with files that are setup for Wells Fargo initiated transfers, SAFE Transmission can notify a trading partner when a pushed file transfer has completed. These notifications are known as triggers. Triggers can be set up as a file, an email, or both.

Trigger files

Trigger files are zero-byte files that are pushed to the trading partner immediately following the completed transfer of the original file.

Trigger file names can be configured with a prefix and suffix that is added to the original file name. Prefix and suffix options are RDY, DONE, or a custom character string that you provide.

Trigger emails

Trigger notifications can be emailed to recipients who have a need to know or when a trigger file is not appropriate.

Value added services, cont.

Custom file names

Files that Wells Fargo pushes to you or are available from SAFE Transmission can be renamed according to your company's specific needs. In the SAFE Transmission channel, this is known as custom file naming. Custom file naming is available at the folder level and all files delivered to the folder will be renamed according to the structure that is defined.

Files can be renamed to use the original name as provided by our product partners with extra elements that you select, or the service can replace the original name with something you specify. Your options for custom file naming are:

- Original file name
- Date or any part of the date (month, day, century, year)
- Julian date
- Time, or any part of the time field (hour, minute, second, millisecond)
- Product identifier code
- Product folder nickname
- Customer-defined character string
- CEO portal company ID

Separators can be space, period, and underscore characters. The elements and separators can be mixed, matched, and arranged in any order. It is also possible to replace or add a different file extension.

Note: Renamed files have a 255-character limitation for the name, including the file extension.

Standard inbound file naming conventions

For files you send to Wells Fargo, the underlying product provides the file name within these parameters:

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	

Value added services, cont.

Transmission messages

Your SAFE Transmission team understands how critical accurate and timely information about your transmission service is to your success, so Wells Fargo has developed an array of notifications for you. Some communications are set up for all users — these are alerts and others are optional notification messages.

Alerts

Alert messages are sent to transmission users and transmission administrators when specific conditions occur. These conditions include:

- File failures after a successful upload to SAFE Transmission (e.g., failing an anti-virus scan)
- Password pending expiration notices for an automated user ID
- Digital certificate request or renewal that needs attention
- A zero-byte file was received

Alerts are sent to the responsible user or user contacts in the case of an automated user ID. Alerts are mandatory communications and cannot be turned off. Alerts require an action to be taken to resolve the condition.

Event notifications

Event notifications are optional messages that can be configured in the SAFE Transmission channel. Event notifications are delivered to email recipients when an event condition exists. Event notifications can be delivered to anyone; they are not limited to transmission users or transmission administrators. Each event notification can be sent to 99 email recipients.

SAFE Transmission can notify when:

- An expected file has not been received
- An unexpected file has been received
- A file has been received by SAFE Transmission
- A zero-byte file was received by SAFE Transmission
- An available file is ready for pickup
- An available file has been pushed (trigger email)
- An available file has not been picked up
- An available file was purged

How the service works

During the implementation process, you can identify the event conditions under which you would like to receive a communication from SAFE Transmission. Some events are based on a condition being met, e.g., there is an available file ready for you to pick up, SAFE Transmission purged an available file (and that file was never picked up).

Transmission messaging notifications are sent by email to the recipients you identify, for the activity you designate, and for the product folders you choose.

Other communications are sent when an event condition has been met or not met. These include an expected file that has not been received, based on a pre-set calendar, or where a file has been received that falls outside of a pre-set calendar. Calendared event notifications can be used to ensure your critical files are received as expected.

For expected events, you will define a schedule of event transmissions that covers dates and a transmission window during which a transfer would normally occur. After the transmission window ends, if SAFE Transmission determines the event did not take place as scheduled, a notification is sent.

Notification for unexpected files works in the same manner as a notification for an expected file that is not received. Based on a scheduled event and an expected transmission window, SAFE Transmission can notify you when a file is received outside of the file transmission window.

Value added services, cont.

Client software

The SAFE Transmission service is compatible with many RFC-compliant file transfer software packages. If needed, Wells Fargo can provide you with Secure Client if you want to use automation for your file transfers. Secure Client is fully RFC-complaint and was developed in partnership with our vendor to meet Wells Fargo's requirements.

Secure Client is compatible with the operating systems and versions listed below.

Operating system	Supported version
IBM AIX	5.3, 6.1
HP-UX	11.11
RedHat Enterprise Linux	5.x
Oracle Solaris SPARC	9, 10
SUSE Linux Enterprise Server	10.3
Microsoft Windows	XP, 2003, Vista, 7*, Itanium
	*Supports 32-bit and 64-bit systems

Secure Client installations require an activation ID that is provided to you by Wells Fargo. Each separate installation of the Secure Client software requires a separate activation ID.

SAFE Validation Environment

After your transmission service is set up, you are ready for testing. SAFE Validation is a separate environment where you can test connectivity, scripts used for automated transfers, file format testing, and Wells Fargo initiated transfers from SAFE Transmission.

You will receive additional information regarding setup of the SAFE Validation environment and its uses during the implementation process.

Accessing SAFE Validation

If you use automation, you will access the validation environment using one of the following URLs

Protocol	URL	Port
FTPS (SSL)	safetransvalidate.wellsfargo.com	21
SFTP (SSH)	safetransvalidate.wellsfargo.com	22 (RSA key)
SFTP (SSH)	safetransvalidate.wellsfargo.com	122 (DSA key)
HTTPS	safetransvalidate.wellsfargo.com	443
FTP with PGP	safetranspgpvalidate.wellsfargo.com	21
AS2	safetransvalidate.wellsfargo.com	5000 5080

If you are a browser user, you will access the validation environment at **<https://safe-t-validate.wellsfargo.com>**.

Note: This is a different URL than the URL you use to access SAFE Transmission.

User accounts

Browser users are automatically set up for SAFE Validation access using the same credentials they use for SAFE Transmission productions access.

Automated users can be set up with either the same automated user ID and authentication credentials, or a different automated user ID and credentials (preferred setup).

Note: Automated user ID credentials that are used in SAFE Validation are exchanged through the SAFE Transmissions admin folder.



Important! Using different automated user IDs in SAFE Validation helps prevent a test file from accidentally being uploaded and processed to production.

Business continuity

SAFE Transmission may exercise its business continuity plan during the year. These are scheduled events and users of the transmission service are notified in advance. Unfortunately, there may be situations when a switch to an alternate processing site is required without advance notice to our user base.

For accessing the SAFE Transmission service, Wells Fargo recommends using the URLs in your automation scripts. This will provide uninterrupted service if changes between SAFE Transmission sites is required.

If you use IP addresses to access SAFE Transmission, refer to the chart below for all SAFE Transmission IP addresses.

For automated connections to SAFE Transmission and SAFE Validation, the following is the URL mapping to IP addresses:

URL	Primary	Alternate
Safetrans.wellsfargo.com	151.151.18.51	151.151.65.214
Safetranspgp.wellsfargo.com	151.151.18.52	151.151.65.215
Safetransvalidate.wellsfargo.com	n/a	151.151.65.204
Safetranspgpvalidate.wellsfargo.com	n/a	151.151.65.209

The following IP addresses are for transmissions originating from SAFE Transmission and SAFE Validation:

Primary	Alternate
151.151.19.131	151.151.68.67
151.151.18.38	151.151.65.195

Contacting your transmission partners

Transmission product team

If you have a suggestion for improving the transmission service, or if you are interested in being a pilot participant in future value-added services, feel free to email the transmission product team at SAFETransmissionProduct@wellsfargo.com.

Transmission technical support

Transmission Support Services is our dedicated transmission technical support team. They are available to assist with issues or questions that may arise after implementation. For questions or issues with SAFE Transmission, call 1-800-835-2265, extension 75555.

Live support is available Sunday 11:30 p.m. Central Time through Saturday 2:30 a.m. Central Time. For support after hours, please leave a message and a support representative will be paged to assist you.

Reference documents

There are reference reports and documents available to assist you with the SAFE Transmission service. Please contact your implementation coordinator for copies of any of the following:

Reports

- Product & Folder Authorization report by product and folder
- Product & Folder Authorization report by product and folder with directory path names
- Product & Folder Authorization report by user ID

Product documentation

- SAFE Transmission – Automated Transmission Quick Reference Guide
- SAFE Transmission – CEO Portal Users Quick Reference Guide
- SAFE Transmission PGP Fact Sheet