

Installing and Configuring the Secure Transport Windows Client (Version 4.5.2)

1. Import the Federal Reserve Issued Credential into you browser.

In addition to purchasing and installing the client software, you must have a Federal Reserve Security Credential that allows using the client with the Federal Reserve. The Secure Transport client requires a digital certificate for authentication. If you are currently using a user and ID to access Federal Reserve Services, you will be provided a digital certificate to replace your user id and password.

Once you have obtained a certificate and installed within your browser, and installed the software, you are ready to activate the client software by Setting Preferences (if needed) and creating Remote Sites.

For detailed information about retrieving and installing your FRB Credential, please refer to the following URL: <http://www.frb services.org/Electronic-Access/pdf/Cert-Retrieval.pdf>.

Note: If you've previously installed the credential with the "strong private key protection" option, follow these instructions to reinstall your credential with the "strong private key protection" option turned off. The Automated scheduling features of the Secure Transport client will not work if you are prompted for a password to access the certificate.

- A. Right-click the .p12 or .pfx file, and select **Install PFX**.
- B. Click **Next**, then **Next** again.
- C. When the system requests the private key password, enter the password provided when you received the credential.
(Note to server admin: this is the export password, not the root private-key password.)
- D. Deselect "**Enable strong private key protection,**" and select "**Mark this key as exportable.**"
- E. Click **Next**, then **Next** again.
- F. Click **Finish**.
- G. You should get a confirmation dialog box advising the import was successful.

The following are the numbers for the Federal Reserve Customer Contact Center for further information:

Customer District	Toll Free Number	Local Number
Atlanta Boston Chicago Kansas City New York Philadelphia	888-333-7010, option 1	816-881-2690, press 1
Cleveland Dallas Minneapolis Richmond San Francisco St. Louis	888-333-7010, option 1	612-204-7010, press 1

2. Configure the site profiles in the Secure Transport client:

- A. Start up client software by **Selecting Start > Programs > Tumbleweed > SecureTransport Client > Secure Transport.**
- B. The system should open to the "Remote Sites - New Explore" window.
(If the client software is already started, click **F10** to display the "Remote Sites- New Explore" window, or Right Click the Secure Transport Icon in the system tray and select Connect.)
- C. Select the "**Test FedForward-FedReturn**" site profile, and click **Modify**.
- D. Fill in the "**Default Local Folder**" field as appropriate, either manually or using the **Browse** button.
- E. Select the "**User Certificate**" checkbox, then click **Choose** and select the credential installed in step 1.
Optional: under the **Notifications** tab, click **Enable Email Notification** and fill in the fields as appropriate.
- F. Click **OK** to save your settings.
- G. Repeat steps (b) through (f) for the "**Test FedReceipt**" profile.

(Note: These site profiles point to the Federal Reserve test (QA) site. To connect to the production site, remove the "-pp" in the "Default Remote Folder" field. (You may also want to modify the "Site Label" field so it refers to production rather than test.)

3. If you're going through an HTTP proxy, configure the client to use it:

- A. In the client, select **Edit > Preferences > Connection**.
- B. Select the "**Use Proxy/Firewall**" checkbox.

- C. If your proxy settings are defined explicitly in Internet Explorer (i.e., under Proxy Server rather than Automatic Configuration), you can click the **Import** button; otherwise, fill in the settings manually on the HTTP line.
- D. If your proxy server requires authentication, click the **Login** button on the HTTP line, fill in the username and password, and click **OK**.
- E. Click **OK** to save your settings.

4. **Optional Step** - set up global e-mail notification settings (if you configured e-mail notifications in step 2d):

- A. In the client, select **Edit > Preferences > Notifications**.
- B. Fill in the hostname and port number (default=25) of your mail server.
- C. Click **OK** to save your settings.

5. **Optional Step** - set option to remove failed transfers from the queue:

- A. In the client, select **Edit > Preferences > File Transfer**.
- B. If you want to remove failed transfers from the queue, select the "**Remove from transfer queue**" checkbox.

(Note: With this option set, if one transfer fails, subsequent transfers will be able to run successfully. However, you'll need some way of determining that the transfer indeed failed. You can use the e-mail notification option for this purpose, or you can use the value of %FileDriveStatus% (see below for an example) and branch accordingly in your script.)

6. Once everything is set up, test to ensure you have connectivity:

- A. Select the **Remote Site Profile** as in steps 2a-2b, and click **Connect**.
- B. If you see the "incoming" or "outgoing" folder in the middle pane, it works.
- C. If not, call the Customer Contact Center for assistance.

7. Testing Reminders

- A. Coordinate all testing with your assigned FRB Implementation Manager or your Account Executive.
- B. If you want to simulate just communication testing, the outgoing directory can be used to send and receive files. Dummy text file can be used for this purpose. Files sent to the outgoing directory are not processed.
- C. When testing, the Test File Indicator in the File Header record should be appropriately set to a "T" during testing and change to a "P" when you implement.
- D. If you will have a need to continue testing after you implement, you may want to consider defining test remote sites on a separate device.

8. General Notes on Using the Secure Transport Client with the Federal Reserve

- A. Your institutions credentials are mapped to a unique directory with three sub directories. The /incoming/ directory is used for you to upload files. Files successfully transmitted are immediately moved to the next stage of processing. The /outgoing/ directory is used for the Federal Reserve to place FedReceipt and FedReceipt Plus files for you to download. After a file is successfully downloaded, files are moved from the /outgoing/ directory to the /downloaded/ directory. The downloaded directory may be used to retrieve a file that has already been downloaded from the outgoing folder.
- B. An acknowledgement report is created for each file uploaded and for each file that is available for receipt. The acknowledgement report should be monitored to ensure files were received and accepted by us or to determine when files are available for download. Please refer the Check21 Services Fedline for the Web User Guide to view acknowledgements or to activate email alerts of acknowledgements.
- C. Please refer to Tumbleweed Secure Transport User for instructions on how to download and upload files:

FRB FedForward and FedReceipt files can be uploaded to the Federal Reserve using one of the following methods with the Test Fedforward-FedReturn or FedForward-Return remote sites:

Right Click a file in your local folder to upload a file to the /incoming/ directory.

Drag a file from you local folder in the left pane to the incoming folder in the right pane.

Using the Schedule Download Dialog box.

Using command line option with batch files (see sample FedFoward batch file).

FRB FedReceipt and FedReceipt Plus files can be downloaded from the Federal Reserve using one of the following methods with the Test FedReceipt or FedReceipt remote sites:

Right Click a file in your /outgoing/ directory to download a file to you local folder in the left pane.

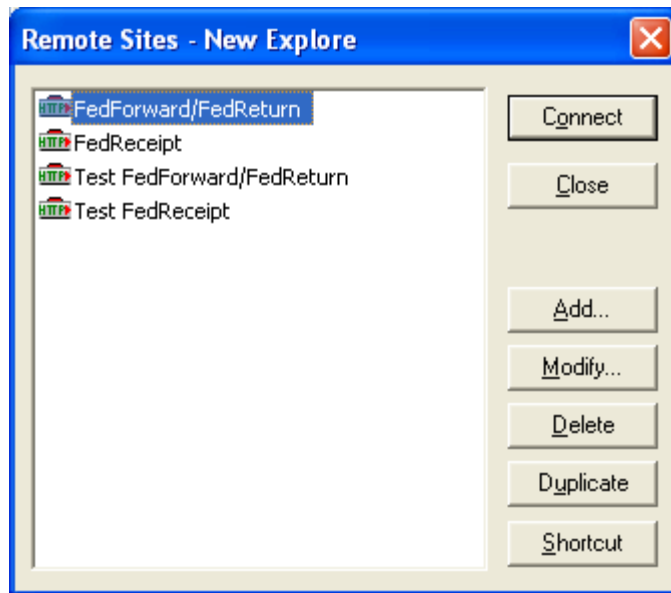
Drag a file from /outgoing/ folder in the right pane to you local folder in the left pane.

Using the Schedule Download Dialog box.

Using command line options with batch files (see sample FedReceipt batch file).

The following is an example for the Remote sites New Explore Dialog Box.

Remote Sites – New Explore Dialog Box



The Following is an example of the Remote Site for Test FedForward-FedReturn.

The image shows a Windows-style dialog box titled "Explore Remote Sites" with a blue title bar and a close button (X) in the top right corner. The dialog has three tabs: "General", "Security", and "Notifications", with "General" selected. The "General" tab contains the following fields and controls:

- Site Label:** A text box containing "Test FedForward/FedReturn".
- Site Settings:** A group box containing:
 - Transfer Protocol:** A dropdown menu set to "HTTPS".
 - Site Host Address:** A text box containing "www.federalreserve.org".
 - Port:** A text box containing "443".
 - Default Local Folder:** A text box containing "C:\c21files" with a "Browse" button to its right.
 - Default Remote Folder:** A text box containing "/flwsecuretransport-pp/incoming".
- Login Type:** A group box containing:
 - Login to Site:** Two radio buttons: "as Anonymous" (unselected) and "using the following identification" (selected).
 - Login and Password:** A checkbox (unselected) with the label "Login and Password". Below it are two text boxes: "Login:" and "Password:".
 - User Certificate:** A checkbox (checked) with the label "User Certificate". Below it is a text box containing "FRB ELoad Test Cwis013" and a "Choose" button to its right.

At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Apply", and "Help".

The following is for production. The only difference is the “-pp” is not in the production version in the URL or default remote site.

The screenshot shows a dialog box titled "Explore Remote Sites" with a blue title bar and a close button (X) in the top right corner. The dialog has three tabs: "General", "Security", and "Notifications", with "General" selected. The "General" tab contains the following fields and options:

- Site Label:** A text box containing "FedForward/FedReturn".
- Site Settings:** A group box containing:
 - Transfer Protocol:** A dropdown menu set to "HTTPS".
 - Site Host Address:** A text box containing "www.federalreserve.org".
 - Port:** A text box containing "443".
 - Default Local Folder:** A text box containing "C:\c21files\" with a "Browse" button to its right.
 - Default Remote Folder:** A text box containing "/flwsecuretransport/incoming".
- Login Type:** A group box containing:
 - Login to Site:** Two radio buttons: "as Anonymous" (unselected) and "using the following identification" (selected).
 - Login and Password:** A checkbox (unselected) with the label "Login and Password". Below it are two text boxes: "Login:" and "Password:".
 - User Certificate:** A checkbox (checked) with the label "User Certificate". Below it is a text box containing "FRB ELoad Test Cwis013" and a "Choose" button to its right.

At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

Scheduling and Scripting the Secure Transport Windows Client

The client has a built-in scheduler, but that operates only as long as someone is logged into the machine (i.e., it can't be run as a service). If you want scheduled tasks to run when no one is logged in, you'll need to run a batch file that calls Secure Transport, and run it using the Windows Task Scheduler.

A sample batch file for FedForward-FedReturn and a batch file for FedReceipt have been included with your download. (Note: These batch files should be customized as needed for your site. (Note, the sample batch file for FedForward –FedReturn contains a remarked upload command that sends files to the outgoing directory to facilitate testing of the batch files, so be sure to comment out or remove the appropriate one.)

When you schedule this using the Windows Task Scheduler, be sure to set the username and password to be the same as those you used when you installed the Secure Transport client. (This will allow the scheduled task to use the correct preferences settings.)

Note: the batch files and command line options will not work if you selected "strong private key protection" when you installed your FR certificate.