

TDClient 3.5.0 Plain Language Certificate Import Guide

Guide for the annual runtime certificate import

ISIR recipients who use **TDClient 3.5.0** to transmit with **Federal Tax Information Student Aid Internet Gateway (FTI-SAIG)** are required to update their expired certificates annually. To support our partners to continue their services, we are providing this guide that summarizes the steps for importing the new certificate in TDClient 3.5.0.

Expected time to complete the steps described in this guide: 30 minutes

Requirements and considerations

These instructions are written for organizations currently using TDClient 3.5.0 and wish to update their certificates to ensure uninterrupted receipt of ISIRs. We anticipate that most institutions reviewing this guidance fall within this category. If you are a new TDClient 3.5.0 user or require more detailed instructions, please refer to the [FTI-SAIG TDClient Host Communication Guide](#).

Terms used in this document:

FT number: Used to identify an organization's newly assigned FTI-SAIG mailbox. The FT number is unique and always begins with "FT" followed by five alphanumeric characters. "FTxxxxx" is used as an example FT number throughout this document; it should be replaced with an organization's actual FT number when following instructions.

Security Code: This is a six-digit code generated from your physical (or software) Security Token.

Instructions:

Section 1: Checking the Certificate Expiration in FTI-TDCM

The purpose of this section is to help you verify the expiration date of your current certificate. All FTI-SAIG registered mailbox users with an **FSA User ID** linked to an **FT mailbox** can check the expiration date of their FT Mailbox certificate by logging into their **FTI-TDCM** account. Please follow the steps outlined below to complete the process.

Step 1: In your web browser, enter the URL <https://ftisaigportal.ed.gov/tdcm> in the address bar and press **Enter**. This will take you to the login screen shown below.

The login screen features a dark teal header with the word "Login" in white. Below the header, there is a yellow warning triangle icon followed by the text "Please log in first" in red. The main area contains four input fields, each with a label and an asterisk: "FSA User Id *", "Password *", "OTP *", and "Mailbox Id *". A dark teal "Login" button is positioned at the bottom right of the form.

Step 2: Enter your **FSA User ID** in the **FSA User ID** field.

Step 3: Enter your **FSA User ID Password** in the **Password** field.

Step 4: Enter the **six-digit Security Code** from your Security Token in the **OTP** field.

Step 5: Enter your **FT Number** (e.g., FTxxxxx) in the **Mailbox Id** field.

Step 6: Click the **Login** button. All FTI-TDCM users will see the **FSA Security Banner** screen after logging in.

Step 7: Navigate to the **Participants** view and select the **Security** tab. Here, you can check the status of your certificate, including its expiration date, any expired certificates, your current certificate, and/or a pending certificate.

The screenshot shows the FTI-SAIG Mailbox interface. At the top, there are logos for "Federal Student Aid" and "PROUD SPONSOR of the AMERICAN MIND®". The main header includes "FTI-SAIG Mailbox" and navigation tabs: "Participants", "Relationships", "Messages", "Archive", and "Help". The "Participants" tab is active, and the "Security" sub-tab is selected. The interface is divided into a "SEARCH" panel on the left and a "PARTICIPANTS" panel on the right. The "SEARCH" panel has fields for "EDI Name" and "Name", a "Only pending" checkbox, and "Go" and "Expand" buttons. The "PARTICIPANTS" panel shows details for a participant, including "Name", "User Logon/Mailbox", "EDI Name", "EDI Qualifier", "Server Name" (FTISAIGPORTAL (EAFTP)), "AS2 Name", "Primary URL" (ftisaigmailbox.ed.gov), "Approval Code", "Approval Status" (Approved), and "Secondary URL". A "Save" button is at the bottom right. Below the details, there are tabs for "Contact", "Enabling", "Security", "ISA Fields", and "Key Exchange". The "Security" tab is active, showing a table with columns: "Type", "Status", "Start Time", "End Time", and "Issuer". The table contains one record: Type: X509, Status: Current, Start Time: Aug 16, 2024 02:00:01 AM, End Time: Aug 16, 2025 02:00:01 AM. "Export Runtime" and "Export INI" buttons are at the bottom right.

Note: The options displayed may vary depending on when your certificate was issued and its expiration date, so you may only see one or two of the options mentioned above. Please refer to the examples below:

Example of Current Certificate:

You will only see the "**Current**" certificate if your initial certificate is still active, and its expiration date is more than 30 days away. **No action** is required at this time. Please note the expiration date of your certificate and check back 30 days before it expires to download the newly assigned certificate.

Contact	Enabling	Security	ISA Fields	Key Exchange		
Type	Status	Start Time		End Time		Issuer
X509	Current	Aug 16, 2024 02:00:01 AM		Aug 16, 2025 02:00:01 AM		
						Export Runtime Export INI

Example of Expired Certificate:

You will see both the "**Expired**" and "**Current**" certificates if your initial certificate has expired, and a new one has been assigned to your account. If you see this option in your Security tab, clicking on the "**Export Runtime**" button will download the current runtime file. You can then proceed to the next sections, which will guide you through downloading and importing the file.

Contact	Enabling	Security	ISA Fields	Key Exchange		
Type	Status	Start Time		End Time		Issuer
X509	Expired	Jul 28, 2023 05:33:47 PM		Jul 28, 2024 05:33:47 PM		
X509	Current	Jul 28, 2024 09:33:47 PM		Jul 28, 2025 09:33:47 PM		
						Export Runtime Export INI

Example of Current and Pending Certificates:

You will see both "**Current**" and "**Pending**" certificates if your current certificate is still valid but set to expire within the next 30 days. . If you see this option in your Security tab, clicking on the "**Export Runtime**" button will download the new runtime file. You can then proceed to the next sections, which will guide you through downloading and importing the file.

Contact	Enabling	Security	ISA Fields	Key Exchange		
Type	Status	Start Time		End Time		Issuer
X509	Current	Aug 24, 2023 08:53:03 PM		Aug 24, 2025 08:53:03 PM		
X509	Pending	Aug 25, 2025 12:53:03 AM		Aug 25, 2027 12:53:03 AM		
						Export Runtime Export INI

Section 2: Downloading the New Certificate from FTI-TDCM

The purpose of this section is to help you download the new certificate by logging into your **FTI-TDCM** account and placing it in the correct folder. Please follow the steps outlined below to complete the process.

Step 1: Follow **Steps 1-7** outlined in **Section 1** to prepare for the next steps.

Step 2: Click the **Export Runtime** button to download the runtime file. You should now have a runtime file (certificate) associated with your institution's name and FT number (E.g.: "School Name FTXXXXX.rtm"). For most users, the downloaded file will be located in the **Windows Downloads** folder.

PARTICIPANTS

Name: *	<input type="text"/>	User Logon/Mailbox: *	<input type="text"/>
EDI Name: *	<input type="text"/>	EDI Qualifier: *	<input type="text"/>
	Change Password		
Server Name *	FTISAIGPORTAL (EAFTP) <input type="text"/>	Approval Code:	<input type="text"/>
AS2 Name	<input type="text"/>	Approval Status	Approved
Primary URL: *	ftisaigmailbox.ed.gov	Secondary URL:	<input type="text"/>

Contact	Enabling	Security	ISA Fields	Key Exchange
Type	Status	Start Time	End Time	Issuer
X509	Current	Aug 16, 2024 02:00:01 AM	Aug 16, 2025 02:00:01 AM	

Step 3: Record the **Approval Code** displayed on this screen. You will need it when importing the runtime file in **TDClient** in **Section 3-Step 5** and **Section 4-Step 5**.

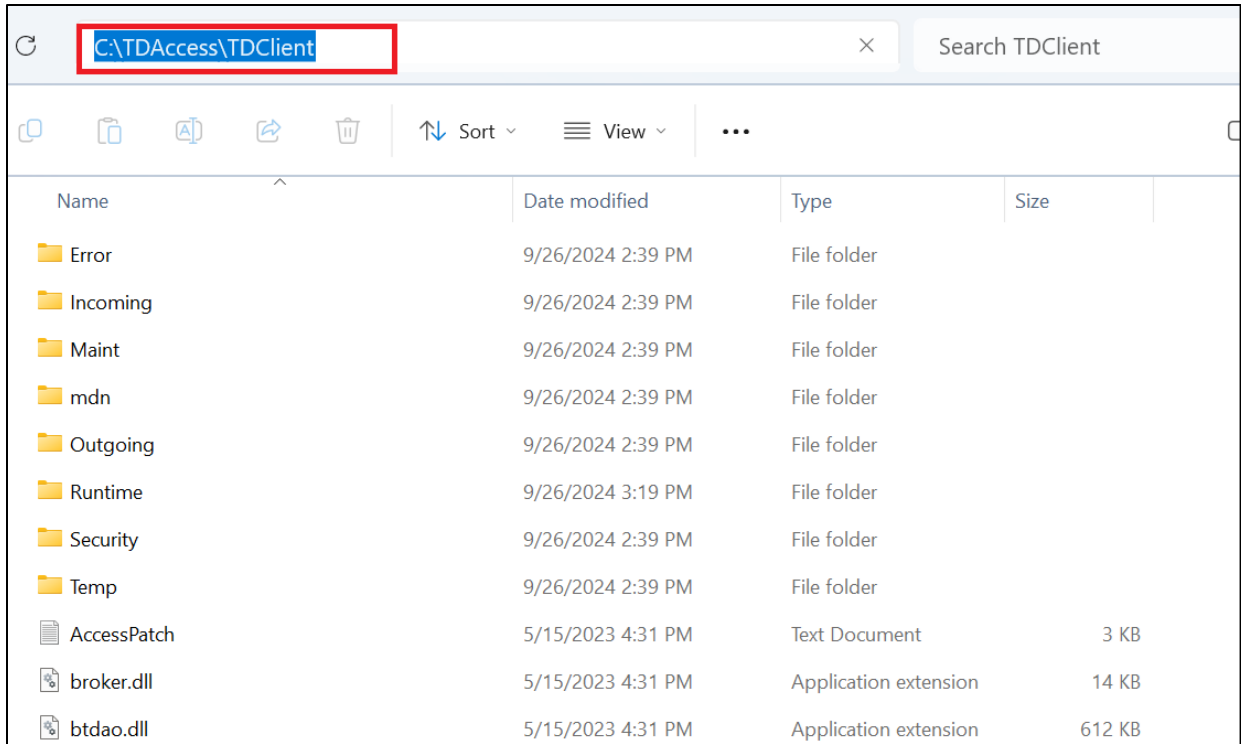
Step 4: Press the **Windows** key on your keyboard or click the **Start** button in the bottom-left corner of your screen.

Step 5: Type **File Explorer** into the search bar and press **Enter** or select **File Explorer** from the search results. Navigate to **This PC > Windows (C:)**.

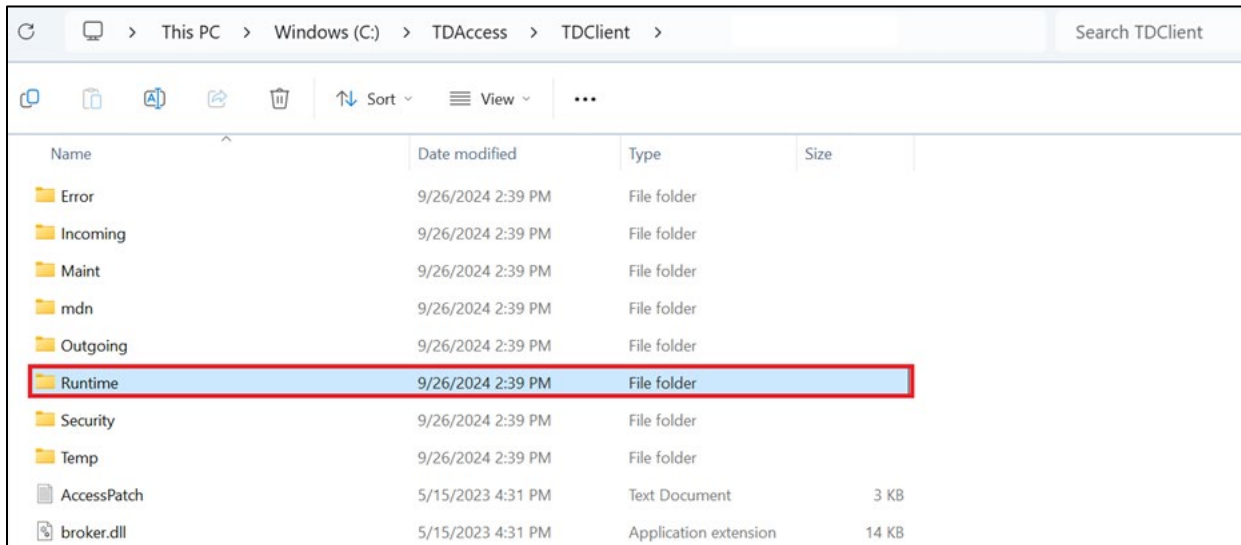
Step 6: Navigate to the where you have installed **TDClient**. TDClient is normally installed in the directory shown in the screenshot below.

Name	Date modified	Type	Size
TDClient	9/26/2024 2:39 PM	File folder	
uninstall	9/26/2024 2:39 PM	File folder	
.installationinformation	9/26/2024 2:39 PM	INSTALLATIONINFOR...	4 KB

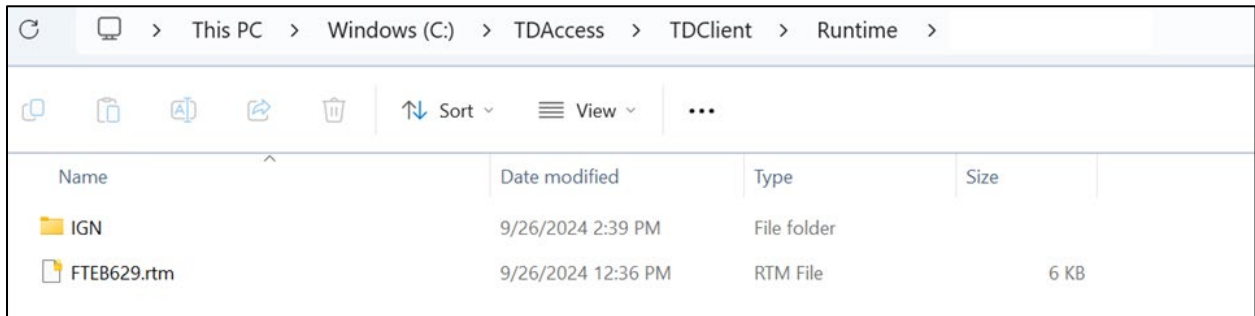
Step 7: Click on the address bar at the top of folder where TDClient is installed to display the full path and record the location as highlighted below. You will use this path in **Section 3-Step 2**.



Step 8: Locate and open the **Runtime** folder within the TDClient folder.

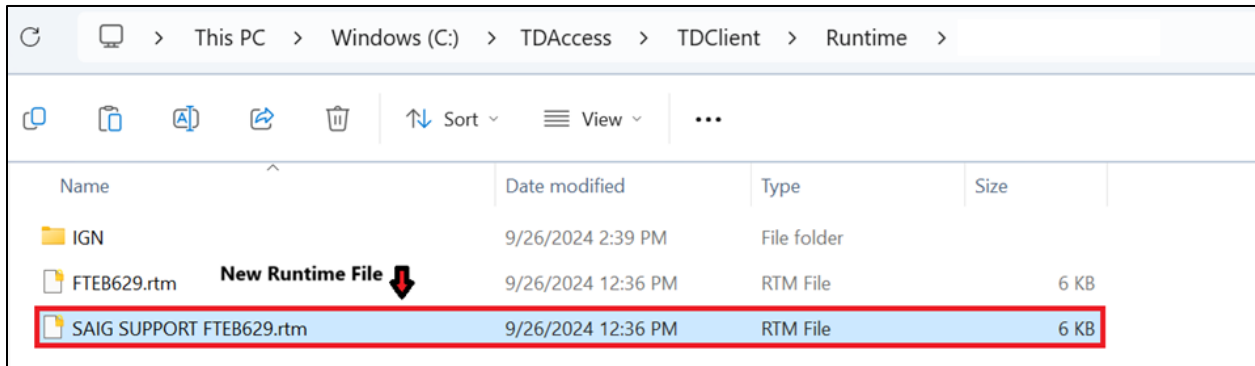


You are in the correct directory if you see the **IGN folder**.

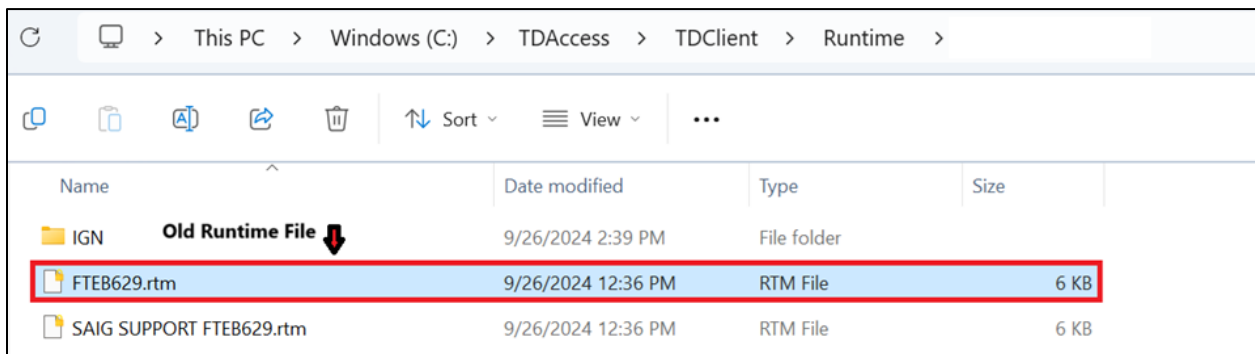


Step 9: Navigate to where you downloaded the new **runtime** file in **Step 2** (For most users this file will be located in the **Windows Downloads** folder). **Right-click** the file and select **Copy**, navigate to the **Runtime** folder.

Step 10: **Right-click** inside the **runtime** folder and choose **Paste**. The new runtime file will now be visible in the folder. **Note:** the new runtime file will have the name of the organization associated with the mailbox and the mailbox number as shown in the screenshot below:



Step 11: Now that you have the new runtime file pasted in the folder, delete the old runtime file if one exists in this folder. See highlighted example below:



Step 12: Right-click on the new runtime file you have pasted in the folder, select **Rename**, and rename the file to match your FT number (e.g., FTxxxxx.rtm) as shown in the example below.

Important Note: Make sure there are **no spaces** when renaming the file. The file should now be ready to be installed.

SAIG SUPPORT	FTEB629.rtm	9/26/2024 12:36 PM	RTM File	6 KB
--------------	-------------	--------------------	----------	------



Renaming the runtime file to the correct format

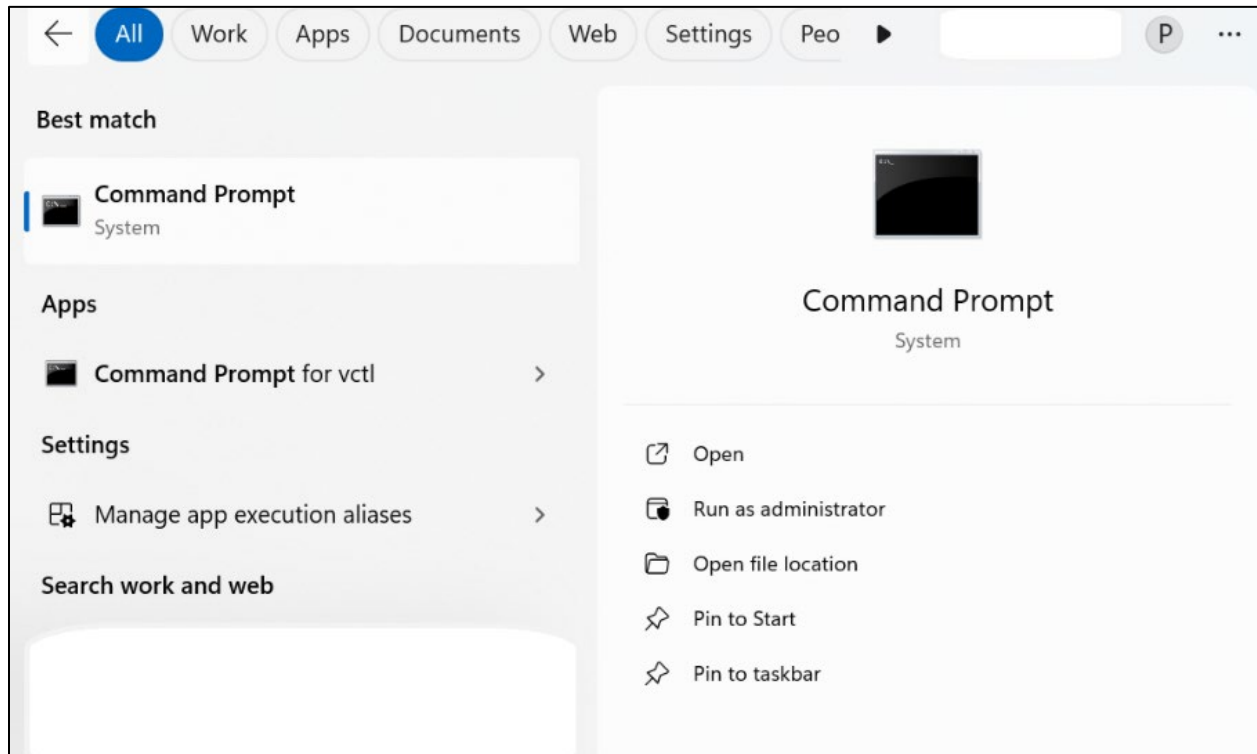
FTEB629.rtm		9/26/2024 12:36 PM	RTM File	6 KB
-------------	--	--------------------	----------	------

Section 3: Importing the New Certificate – TDClient (Windows)

The purpose of this section is to help import the new certificate in TDClient. Please follow the steps outlined below to complete the process.

Note: Please ensure you have completed all the Steps in **Section 1** and **Section 2** before proceeding.

Step 1: Open the **Windows Start** menu then locate the **Command Prompt** by typing "**Command Prompt**" in the search bar and clicking on it.



Step 2: In the **Command Prompt**, Type “**cd**” followed by the directory where you have TDClient installed and hit **Enter**. This is the same path recorded in **Section 2-Step 7**.

For example, if you have TDClient installed in C:\TDAccess3.5\TDClient, enter:

```
cd C:\TDAccess3.5\TDClient
```

```
C:\Users\hughw>cd C:\TDAccess3.5\TDClient
C:\TDAccess3.5\TDClient>
```

Step 3: Next, type ‘**import**’ and press **Enter**.

```
C:\TDAccess3.5\TDClient>import
Enter full pathname of 'rtm' file from KeyManager:
```

Step 4: Next, type the location of the runtime file and press **Enter**. The format should look like this:

```
.\Runtime\FTXXXXX.rtm
```

```
C:\TDAccess3.5\TDClient>import
Enter full pathname of 'rtm' file from KeyManager:
.\Runtime\FTCZ519.rtm
```

Step 5: Type the following command to set the location for the runtime file:

```
.\Runtime
```

```
Enter output path for runtime files (128 char max):
.\Runtime
```

Step 6: When prompted, type the **Approval Code** from **Section2-Step3** and press **Enter**. You should then see the certificate information displayed, which will scroll off of the screen.

```
Enter approval code if required (16 characters):
ABCDEFGHIJ12349786
```

The end of the certificate information will look similar to the screenshot below.

```
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Subject Key Identifier:
C8:EB:FA:2C:6D:9D:75:D3:AC:F0:5C:34:5D:57:2B:60:72:03:3D:B4
X509v3 Authority Key Identifier:
C8:EB:FA:2C:6D:9D:75:D3:AC:F0:5C:34:5D:57:2B:60:72:03:3D:B4
Signature Algorithm: sha512WithRSAEncryption
Signature Value:
3c:51:f1:26:01:c1:26:9c:f6:d8:bf:a1:c6:d1:d3:c4:ee:a5:
2f:bf:20:12:5a:bf:f3:a6:81:39:64:d5:9b:38:6a:ed:3e:70:
61:0d:30:20:e5:0e:eb:7d:fa:71:f0:df:6b:eb:c3:55:c7:4f:
a9:e4:86:2d:7f:b5:3d:7a:00:ae:44:82:34:ae:48:0c:f9:66:
bc:42:58:02:47:c4:58:22:1c:80:c4:4c:9c:54:d5:bb:3b:10:
2b:ca:16:4e:c6:d8:4b:f7:ff:1e:44:2b:8a:c0:d0:e2:3c:e0:
a2:77:43:83:00:f8:36:82:56:48:66:74:49:7b:3a:39:bf:b9:
ed:cf:e1:67:fe:3b:95:a2:88:77:e9:9f:ce:b1:a7:35:4b:86:
05:e3:c6:aa:68:81:e8:a4:59:e2:0b:68:f3:60:2a:27:0c:02:
95:31:83:b0:1b:b4:26:e0:7e:a6:6f:44:6e:29:bd:6d:08:05:
1e:59:f4:3d:0c:09:26:b4:51:64:c1:e3:7c:c0:9d:36:a5:84:
e8:a5:eb:97:d0:4c:3b:04:82:2d:65:bd:2b:34:22:9b:07:22:
3d:04:fc:ce:99:58:37:31:bf:c7:0f:27:4c:c7:7f:eb:9f:55:
04:f9:d5:bb:f7:7c:b5:48:20:fa:d4:72:1c:9c:68:e8:d0:5b:
0e:66:7b:12
3.)
Migrating .\Runtime\extcert.fil ...
```

You can use the **scroll bar** on the right side of the **Command Prompt** window to scroll up to see the entire information. The first part of the certificate information will be similar to this screenshot:

```

Decompressing .\Runtime\cert.fil
Decompressing .\Runtime\private.fil
Decompressing .\Runtime\symkey.fil
Decompressing .\Runtime\cplookup.tbl
Decompressing .\Runtime\partic.tbl
Decompressing .\Runtime\alias.tbl
Migrating .\Runtime\cert.fil ...
1.)
Record length      : 993
Chain status       : 1
Edi Name Length    : 7
EDI Name           : FTCZ519
Issuer/Serial Hash : 1C5040DE51065CBF33D682F5258FCB9A
Calc Issuer/Serial Hash : 1C5040DE51065CBF33D682F5258FCB9A
Serial Number (encoded) : 03A2
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 930 (0x3a2)
    Signature Algorithm: sha512WithRSAEncryption
    Issuer: C=US, O=NCS
    Validity
      Not Before: Nov  5 16:00:57 2023 GMT
      Not After : Nov  5 16:00:57 2024 GMT
    Subject: C= , ST= , L: , O=SAIG, OU=
      /postalCode=
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:dd:05:dc:ee:47:4a:72:8c:c4:4a:25:85:61:c7:
        20:e8:b4:e0:0e:99:ac:67:31:cf:59:e9:06:c1:2f:

```

Step 7: To check if the import was successful, type the following command to log in:

tdclientc query_list

If the process worked, you would see a **success** message.

```

C:\TDAccess3.5\TDClient>tdclientc query_list

bTrade TDAccess Client Command Line      Version V3.5.0  May 15 2023

Present working directory is [.\]
Using ini-file                [.\tdclient.ini]
Using secondary ini-file      [.\exfer.ini]
Using address book            [.\tpaddrss.ini]
***** Start Communications Session
Connecting to server FTISAIGPORTAL...
200 Command OK.
Connected.
200 Command OK.
200 Command OK.
Logged into FTP server as user FTCZ519
Obtaining file list from server
226 Transfer complete.
Termination started...
Disconnecting...
221 Goodbye.
***** End Communications Session
Task exit status: OK
Program run completed successfully!
Exit status: SUCCESS (000000)

C:\TDAccess3.5\TDClient>

```

Section 4: Importing the New Certificate – TDClient (Linux)

The purpose of this section is to help import the new certificate in TDClient. Please follow the steps outlined below to complete the process.

Step 1: Type “**cd**” followed by the directory where you have TDClient installed and hit **Enter**.

```
$cd /eaadmin/app/TDAccess3_5  
$
```

Step 2: In the Command Prompt, type **./import** and hit **Enter**.

```
$.import  
Enter full pathname of 'rtm' file from KeyManager:  

```

Step 3: Next, type the location of the runtime file and press **Enter**. The format should look like this:

```
./runtime/FTXXXXX.rtm
```

```
$ ./import  
Enter full pathname of 'rtm' file from KeyManager:  
./runtime/FT73082.rtm
```

Step 4: Type the following command to set where the runtime files should go:

```
./runtime
```

Step 5: When prompted, type the Approval Code from **Section2-Step3** and press **Enter**.

```
Enter approval code if required (16 characters):  

```

You should then see a confirmation message.

```

X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
X509v3 Subject Alternative Name:
EdiPartyName:<unsupported>
X509v3 Subject Key Identifier:
EF:71:34:E7:80:DF:E5:B9:62:DC:8F:0C:A5:7A:9F:63:82:01:FC:98
X509v3 Authority Key Identifier:
EF:71:34:E7:80:DF:E5:B9:62:DC:8F:0C:A5:7A:9F:63:82:01:FC:98
Signature Algorithm: sha512WithRSAEncryption
Signature Value:
15:1d:c2:68:e6:a4:67:87:a6:4b:59:18:c3:d3:30:06:5f:51:
82:a1:f3:5f:52:5e:48:29:9e:4a:b2:10:a5:76:c3:b3:39:09:
ce:b6:fb:a9:ee:f2:71:d0:31:79:37:58:88:34:76:2a:8d:7a:
90:ef:2b:31:85:7d:dc:c3:d4:f7:fb:c5:19:35:3b:8c:4b:50:
f3:d7:7e:c3:30:88:5a:ac:4b:2e:66:30:7c:23:a0:77:24:5b:
fb:bc:ed:a6:1e:f7:7f:66:d1:5b:90:4e:cd:a4:cf:63:f9:0f:
1d:4f:ff:a3:43:dd:ab:92:ab:20:80:70:45:ff:86:bc:d3:9c:
84:5e:b6:5e:22:55:91:df:1a:30:2a:9d:bd:39:a0:6b:5a:1f:
0c:60:66:f3:2b:d6:fb:17:45:45:c1:8b:fc:da:ba:24:78:16:
eb:77:72:62:37:55:50:2a:bd:e2:29:18:87:c8:0c:6c:d1:fc:
9e:cb:7d:ae:df:c9:1d:de:2e:00:f4:b0:c8:f6:14:32:0f:21:
c0:a3:6a:87:4a:9d:4f:fa:82:2d:73:a0:36:b7:e7:f7:2d:71:
fd:c4:ac:a4:ed:4a:e8:3e:57:78:e6:48:19:d7:6f:dd:43:80:
3f:0e:96:ad:b5:e6:3d:5b:9e:cd:b7:38:10:b6:47:f4:14:e6:
7d:69:0b:df
3.)
Migrating ./runtime/extcert.fil ...
$ █

```

Step 6: To test whether the import was successful, use the following command to log in:

```
tdclientc query_list
```

If successful, you will see a success message displayed in the terminal.

```

200 Command OK.
Connected.
200 Command OK.
200 Command OK.
Logged into FTP server as user FT73082
Obtaining file list from server
226 Transfer complete.
Termination started...
Disconnecting...
221 Goodbye.
***** End Communications Session
Task exit status: OK
Program run completed successfully!
Exit status: SUCCESS (000000)
$ █

```

Possible Certificate Related Errors:

'No such file or directory' error message

If you encounter the '**No such file or directory**' error message, it typically indicates an issue with the RTM file name. The error occurs when there is a space in the file name, which prevents the import from being completed. To resolve this, please check the RTM file name and ensure there are no spaces. Removing the space should allow the import to proceed successfully. If the problem persists, please contact the FPS Help Desk.

```
Error opening ./runtime/"FT 73802.rtm"  
: No such file or directory
```

'Decompression error' error message

If you encounter the '**Decompression error**' message, it typically indicates that you entered an invalid Approval Code. To resolve this, please verify that you have entered the correct approval code and re-run the import process. If the problem persists, please contact the FPS Help Desk.

Error on Linux:

```
Enter approval code if required (16 characters):  
FC226C3FB639A3EA  
Decompressing ./runtime/cert.fil  
Decompression error: rc=55  
$ █
```

No information shown by listrtm

If you run the "**listrtm**" command and receive **no information** about the certificate (see screenshots for Windows and Linux), it is an indication that at least one of the files extracted from the .RTM is corrupt. If this happens, try re-importing the certificate. If that fails, re-download the .RTM file, and importing it may resolve it. If the problem persists, please contact the FPS Help Desk.

Error on Windows:

```
C:\TDAccess3.5\TDClient>listrtm path=.\Runtime  
RUNTIMEPATH = .\Runtime  
  
*****  
Listing Certificates  
*****  
  
*****  
Listing Symmetric Keys  
*****  
  
C:\TDAccess3.5\TDClient>
```

Error on Linux:

```
$ pwd
/eaadmin/app/TDAccess
$ ll runtime/
total 36
-rw-r-----. 1 btadmin btradegrp 708 Sep 24 17:30 alias.tbl
-rw-r-----. 1 btadmin btradegrp 0 Sep 24 17:55 cert.fil
-rw-r-----. 1 btadmin btradegrp 816 Sep 24 17:30 cplookup.tbl
-rw-r-----. 1 btadmin btradegrp 5124 Sep 24 14:20 FT73082.rtm
-rw-r-----. 1 btadmin btradegrp 5124 Sep 24 15:41 FT 73802.rtm
drwxrwxr-x. 2 btadmin btradegrp 6 Jul 24 2023 ign
-rw-r-----. 1 btadmin btradegrp 120 Sep 24 17:30 partic.tbl
-rw-r-----. 1 btadmin btradegrp 1345 Sep 24 17:30 private.fil
-rw-r-----. 1 btadmin btradegrp 652 Sep 24 17:30 symkey.fil
drwxr-x---. 2 btadmin btradegrp 114 Sep 24 15:57 temp
drwxr-x---. 2 btadmin btradegrp 6 Sep 24 15:56 temp?
$ ./listrtm PATH=./runtime
RUNTIMEPATH = ./runtime

*****
Listing Certificates
*****

*****
Listing Symmetric Keys
*****
$
```

Error 422

If you encounter **Error 422**, it means you do not have the necessary access, which could be due to an expired certificate. To resolve this issue, check if your certificate has expired. If it has, you must download and import a new certificate to regain access. If the problem persists, please contact the FPS Help Desk.

```
C:\TDAccess3.5\TDClient>tdclientc query_list

bTrade TDAccess Client Command Line          Version V3.5.0  May 15 2023

Present working directory is [.]
Using ini-file                [.\tdclient.ini]
Using secondary ini-file     [.\exfer.ini]
Using address book           [.\tpaddrss.ini]
***** Start Communications Session
Connecting to server FTISAIGPORTAL...
422 lost connection with server
Connected.
FTP login failed.422 lost connection with server
Login for UserId: [FTCZ519] failed
(422) FTP login failed.422 lost connection with server

WARNING: Logon to server failed
Login for UserId: [FTCZ519] failed
(422) FTP login failed.422 lost connection with server

Termination started...
Disconnecting...
422 lost connection with server
***** End Communications Session
Task exit status: FAILED
Task completed with failure code 422
Exit status: FAILURE (999999)

C:\TDAccess3.5\TDClient>
```

Additional Questions

If you have questions or need additional assistance, please contact the FPS Help Desk (formerly CPS/SAIG Technical Support) at 1-800-330-5947 or by email at support@fps.ed.gov.