

Converting to PIV/CAC Authentication for CIR

CIR Connection Guide

TABLE OF CONTENTS

Introdu	iction	3
Part 1.	Linking a user PIV or CAC Certificate to the User Fiscal Service SSO Account	4
Part 2.	Logging in to CIR using your PIV/CAC Credentials	9
Part 3.	Troubleshooting: If you are unable to log in to CIR with your PIV/CAC	10
Α.	403 Error Message When Logging in to CIR with a PIV/CAC	10
В.	Validation Authority Error	10
C.	CIR Server Does Not Recognize PIV/CAC Certificate	11
D.	Additional Troubleshooting Assistance	15

List of Figures

Figure 1. Select a Certificate Window 4	
Figure 2. Certificate Window 5	
Figure 3. Certificate Enhanced Key Usage 5	
Figure 4. Certificate Subject Alternative Name 6	
Figure 5. Enter PIN Window	
Figure 6. SSO Page 7	
Figure 7. CASS Email Registration Page	
Figure 8. SSO User Log in Page	
Figure 9. Request Successfully Sent Page	
Figure 10. Fiscal Service SSO Log in Page	
Figure 11. Certificates Window 11	
Figure 12. Certificate Export Wizard Window 12	
Figure 13. Export Private Key in Certificate Export Wizard 12	
Figure 14. Export File Format in Certificate Export Wizard 13	
Figure 15. File to Export in Certificate Export Wizard 13	
Figure 16. File Explorer Window 14	
Figure 17. Complete Certificate Export Wizard Window14	
Figure 18. Export Successful Window 15	

Introduction

This document details the steps required for a user to link their Personal Identity Verification/Common Access Card, or PIV/CAC certificate to their Fiscal Service Single Sign-On (SSO) account and provides instructions for using their PIV/CAC credentials to log in to CIR.

Users who do not currently have a PIV or CAC credential do not need to take action at this time. Users should escalate internally with their agency if the user is required to obtain a PIV or CAC credential.

Troubleshooting—if a user is unable to log in to CIR with their PIV/CAC credentials, assistance information is available in **Part 3. Troubleshooting: If you are unable to log in to CIR with your PIV/CAC**

Part 1. Linking a user PIV or CAC Certificate to the User Fiscal Service SSO Account

- If you previously linked your PIV/CAC certificate to a Fiscal Service SSO Account, skip this section and proceed to Part 2. Logging in to CIR using your PIV/CAC Credentials.
- You must have an active Fiscal Service SSO account for CIR Online to link a PIV/CAC certificate.
- You can link a PIV/CAC certificate from any location with internet access using your agency-provided workstations. You do not have to be physically located at your agency.

Follow the steps below to link your PIV or CAC credentials to your Fiscal Service SSO account.

- 1. Using your browser, navigate to the CASS application: <u>https://piv.treasury.gov/cass/</u>.
- A Windows Security box displays and prompts the user to select the appropriate certificate, see Figure 1. Select a Certificate Window. You may have to select More Choices to view your other certificate choices. Choose the correct certificate used for authentication and enter the associated PIN for the credential.

Windows Security	×
Select a Certificate	
Site piv.treasury.gov needs ye	our credentials:
Timothy User Issuer: Federal Progr	am Agency Name
Valid From: 1/25/20	22 to 1/25/2025
Click here to view cert	tificate properties
More choices	
ОК	Cancel

Figure 1. Select a Certificate Window

- 3. If multiple certificate selections are available and the user is unsure which certificate to choose, complete the following:
 - Click the **Click here to view certificate properties** hyperlink. The Certificate window displays.
 - Click the **Details** tab, see *Figure 2. Certificate Window*.

Figure	2.	Certificate	Window
--------	----	-------------	--------

		te Information
• P • 2	Proves your	is intended for the following purpose(s): r identity to a remote computer 113839.0.6.10.2 Logon
		Timothy User Federal Program Agency Name
Va	alid from	1/25/2022 to 1/25/2025 rivate key that corresponds to this certificate.

• The **Details** tab displays. Scroll down and select the *Enhanced Key Usage* option as shown in *Figure 3. Certificate Enhanced Key Usage*. *Client Authentication* displays within the lower display window when the correct certificate is selected.

 \times 🐖 Certificate General Details Certification Path Show: <All> \sim Field Value ^ KeyID=8c3d5409c4... [1]Certificate Policy:... all Authority Key Identifier Certificate Policies CRL Distribution Points [1]CRL Distribution ... Subject Alternative Name RFC822 Name=ti ... Subject Key Identifier 7f4da857ff9c6dcdf3.. Client Authenticatio... 🔣 Key Usage Digital Signature (80) Thumbprint 402891be60c6f6a4a... v Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Edit Properties... Copy to File... ОК

Figure 3. Certificate Enhanced Key Usage

• Ensure the selected certificate includes *RFC822 Name=your email address* in the *Subject Alternative Name* certificate field, see *Figure 4. Certificate Subject Alternative Name*.

		>
General Details Certification	Path	
Show: <all></all>	×	
Field	Value	^
Authority Key Identifier	KeyID=8c3d5409c4	
Certificate Policies	[1]Certificate Policy:	
CRL Distribution Points	[1]CRL Distribution	A
Subject Alternative Name	e RFC822 Name=ti	
Subject Key Identifier	7f4da857ff9c6dcdf3	•
Enhanced Key Usage	Client Authenticatio	
Key Usage	Digital Signature (80)	
Thumbprint 🔄	402891be60c6f6a4a	
		•
RFC822 Name=timothy.user	@federalagency.gov	
Other Name:		
	user@federalagency.gov	
Other Name:	user@federalagency.gov	<u>C</u> opy to File
Other Name:		<u>C</u> opy to File
Other Name:		<u>C</u> opy to File

Figure 4. Certificate Subject Alternative Name

4. A PIN prompt displays once the correct certificate is chosen. The user enters their Smart Card PIN. See *Figure 5. Enter PIN Window*.

Windows Security		×
Smart Card		
Please enter your digital signatu	ire PIN.	
EII PIN		
Click here for more in	formation	
ОК	Cancel	

Figure 5. Enter PIN Window

5. The CASS Application Home page appears in your browser. Click the I need to link my PIV or PIV-I cert to an existing Fiscal Service SSO account hyperlink. See *Figure 6. SSO Page*.

759	SIGK	<u>N</u>
Change Password	Contact	PIV/CAC Linking Guide
do not have a Fisca	Comise CO	

Figure 6. SSO Page

- If you receive the message "Your credential has already been linked to an SSO account. Your access should already be in place" your PIV/CAC credentials may already be linked to your SSO account due to another Fiscal Service or Treasury application. Continue to Part 2 of this document to confirm you can use your PIV/CAC credentials to log in to CIR.
- If you receive the message "Unable to decode certificate. This is likely not an authentication certificate." The certificate you selected cannot be used; this is possibly because it is not an authentication certificate, or it may not be a PIV, PIV-I, or CAC certificate. Ensure your PIV, PIV-I, or CAC is inserted into your workstation's card reader and repeat steps 1 through 4, ensuring that you select a valid PIV, PIV-I or CAC authentication certificate (per steps 2 through 4).
- 6. For PIV/CAC certificates without an email address, enter your name and email address and click Submit, see Figure 7. CASS Email Registration Page. You will receive an email with a link to register. Click this link or enter it into your web browser. If your certificate has an email, CASS will automatically skip to the next step.

Manage Identity/Account Contact	
manage mentary recount conduct	
Enter your personal info	ormation.
*Legal First Name:	
Legal Middle Name:	
*Legal Last Name:	
*Official Email Address	Submit

Figure 7. CASS Email Registration Page

7. Enter your Fiscal Service SSO **UserID** and **Password** and click **Submit**. See *Figure 8. SSO User Log in Page*.

Manage Identity/Ad	ccount Contact	
Enter the userID an UserID: Password: Submit	d password for the SSO accor	unt you wish to link to your PIV or PIV-I credent

Figure 8. SSO User Log in Page

Once logged in to CASS, a message displays: "Your request has been submitted successfully", see Figure 9. Request Successfully Sent Page. An email is then sent to the user email address associated with the Fiscal Service SSO profile. The email contains "Treasury Fiscal Service SSO Certificate Activation Notification" in the subject line.



Figure 9. Request Successfully Sent Page

8. Once the email is received, log in to the Fiscal Service Application using your PIV/CAC credentials.

Part 2. Logging in to CIR using your PIV/CAC Credentials

Once your PIV or CAC certificate is successfully linked to your Fiscal Service SSO account, log in to CIR using your PIV/CAC:

 Use Microsoft Edge or Google Chrome to access CIR Production at: <u>https://www.CIR.fiscal.treasury.gov.</u> The browser will redirect to the standard Fiscal Service SSO log in page, see Figure 10. Fiscal Service SSO Log in Page.

RUREAU OF THE FISCAL SERVICE LIS BUTATURET OF THE TEXABLE LIS BUTATURET OF THE TEXABLE	Forget your Personert?) Forget your User 12? Register 💡
Select an authentication method and er	ter your credentials
Log In using your Fiscal Service ID:	
SSO User ID and Password >	To log in using your Fixed Serves Single Sign On User 10 and Password. By logging in with your PNL SecurID, or User 10 and Password, you addrowledge and agree that you have read, understand, and agreed to abide by the <u>Byles of Behavior</u>
Securit Token	User ID: Password: Log In Reset
PKI Certificate	Except value Mar M2 Except value Familie Color Familie Col
WARNING WARNING WARNING	Vou have accessed a U.S. Government information system, which includes (1) this computer (2) this network, (2) all computers connected to this network, and (4) all devices and storage media attached to this network to to a composer on this network. U.S. Government information system is prohibited in my subject you to displaying action, as well as of valid and chimical perstemic information in the system on the system of the system o
NOTE	This system may contain Sensitive But Unclassified (SBU) data that requires specific data privacy handling requirements as dictated by law, mandate or government agency.
	Accessibility 1 Contexts Privacy Nility Bylles of Behavior U. S. Department of the Treasury - Bureau of the Fiscal Service

Figure 10. Fiscal Service SSO Log in Page

- a. Click the PKI Certificate hyperlink, see *Figure 10. Fiscal Service SSO Log in Page*. You will be prompted to select your PIV/CAC authentication certificate.
- b. Select your PIV/CAC certificate and click **OK** to log in to CIR. You may be prompted to enter your PIV/CAC PIN before the log in process completes. Once successfully logged in, you can use your PIV/CAC credentials to log in to CIR in the future. The process is complete and no additional steps are required.

If you receive an error while attempting to log in with your PIV/CAC, continue with **Part 3. Troubleshooting:** If you are unable to log in to CIR with your PIV/CAC.

Part 3. Troubleshooting: If you are unable to log in to CIR with your PIV/CAC

A. 403 Error Message When Logging in to CIR with a PIV/CAC

If you receive the message, "The website declined to show this webpage / HTTP 403" or "Forbidden / You are not authorized to access the requested resource", follow the steps below:

1. In the browser address bar, delete all the characters after "home.xhtml".

You should see the characters **%3E%3Cbody%20bgcolor=** or **><body%20bgcolor=**. Delete these characters from the address bar and press the **Enter** key on your keyboard.

- 2. You should now see the CIR home page. If you see the log in screen instead, your session has timed out; click the PKI Certificate hyperlink and log in using your PIV/CAC credentials again and you should see the CIR home page.
- 3. Bookmark the URL <u>https://www.CIR.fiscal.treasury.gov</u> and use this URL for future CIR log in.

B. Validation Authority Error

If you receive a "*Validation Authority*" error or other errors related to your certificate when attempting to log in to CIR using your PIV/CAC credentials, follow the steps below:

Note: The steps below only apply to validation errors and authentication errors relating to certificates.

- 1. Take a screenshot of the certificate error when attempting to log in to CIR with your PIV/CAC credentials.
- The Fiscal IT Service Desk will address your inquiry. They can be reached by phone at (304) 480-7777.

C. CIR Server Does Not Recognize PIV/CAC Certificate

If you receive a "*Validation Authority*" error or an error was caused by the CIR server not recognizing your PIV/CAC certificate issuer, your PIV/CAC certificate's issuer may not yet be supported by the Treasury Web Applications Infrastructure (TWAI) for authentication.

To do this, locate and export your **public end-entity authentication certificate** by completing the following steps:

- 1. With your CAC/PIV card inserted in your workstation, type **Internet Options** in the Windows search bar.
- 2. Select and launch the Internet Options application.
- 3. Click the **Content** tab at the top of the **Internet Properties** application.
- 4. Click the **Certificates** button.
- 5. Under the **Personal** tab on the **Certificates** screen, see the **Issued To** column and look for your name or Government ID.
- 6. Select the item with your name or Government ID, the **Authentication Certificate** may appear under the **Friendly Name** column. See *Figure 11. Certificates Window*.
- 7. Click **Export**, see *Figure 11. Certificates Window*.

ended purpose:	<all></all>			_
ersonal Other People	Intermediate Cer	tification Authorities	Trusted Root Certification	•
Issued To	Issued By	Expiration Date	Friendly Name	-
Jonathan Pavlik	OCIO CA	7/10/2016	Authentication Certificat	
4		111	•	
	ort Remov			-
	ort <u>B</u> ernov		<u>ک</u> dvan	nce
Jmport Exp				nce

Figure 11. Certificates Window

8. The Certificate Export Wizard Start dialog box displays. Click **Next** >, see *Figure 12. Certificate Export Wizard Window*.

Certificate Export Wizard	
	Welcome to the Certificate Export Wizard This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk. A certificate store to your disk. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, dick Next.
	:
	< gack Next > Cancel

Figure 12. Certificate Export Wizard Window

9. The Export Private Key dialog box displays. Select the **No**, **do not export the private key** button and click **Next** >, see *Figure 13. Export Private Key in Certificate Export Wizard*.

Figure 13. Export Private Key in Certificate Export Wizard



10. The Export File Format dialog box displays. Select the **Base-64 encoded X.509 (.CER)** button. Click **Next >**, see *Figure 14. Export File Format in Certificate Export Wizard*.

Figure 14. Export File Format in Certificate Export Wizard

	ort File Format Certificates can be exported in a variety of file formats.
	Select the format you want to use:
	DER encoded binary X.509 (.CER)
	Bage-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	O Microsoft Serialized Certificate Store (.SST)
Lear	n more about <u>certificate file formats</u>

11. The File to Export dialog box displays. Click **Browse**, see *Figure 15. File to Export in Certificate Export Wizard*.

Certificate Export Wizard			
ile to Export Specify the name of the fi	e you want to export		
<u>F</u> ile name:			
			Browse
		Back Ne	xt > Cancel

Figure 15. File to Export in Certificate Export Wizard

12. Navigate to a folder you want to export your certificate file and type in your desired file name. Click **Save**, see *Figure 16. File Explorer Window*. On the File to Export screen click **Next**.

	+ + Search Temp
Organize • New folder	z. 0
Program Files (x86) ProgramData Quarantine Recovery Sun System Volume Information Temp Users Windows Network T	
File name: EndEntitiyCert	
Save as type: Base64 Encoded X.509 (*.cer)	
Hide Folders	Save

Figure 16. File Explorer Window

13. A confirmation screen displays. Click **Finish**, see *Figure 17. Complete Certificate Export Wizard Window*.

Figure 17. Complete Certificate Export Wizard Window

Certificate Export Wizard		×	
E	Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings:		
	File Name Export Keys	C:\Ter No	
	Include all certificates in the certification path File Format	No Base64	
	<	Þ	
	< gack Finish	Cancel	

14. A confirmation dialog box displays. Click **OK**, see *Figure 18. Export Successful Window*.

Figure 18. Export Successful Window

👚 Certificate Export Wiz 🗾		
The export was successful.		
ОК		

15. Navigate to the folder where you saved the file and rename the file extension of the file to **.txt**. Confirm that you want to change the file name extension and click **Yes** to confirm. If using the example above, the exported file is called **EndEntityCert.cer**, and it should be renamed to **EndEntityCert.txt**

Contact the Fiscal IT Service Desk to discuss any additional error message steps needed or verification of your existing PIV/CAC Certificate.

Additional Troubleshooting Assistance

For additional troubleshooting assistance, visit the *Fiscal Service Guide to Linking Fiscal Service SSO UserID to a SmartCard*: <u>https://www.fiscal.treasury.gov/files/reference-guidance/linking-fiscal-service-sso-piv-cac-guide.pdf</u>.

Thank you for converting to PIV/CAC for your authentication to CIR!