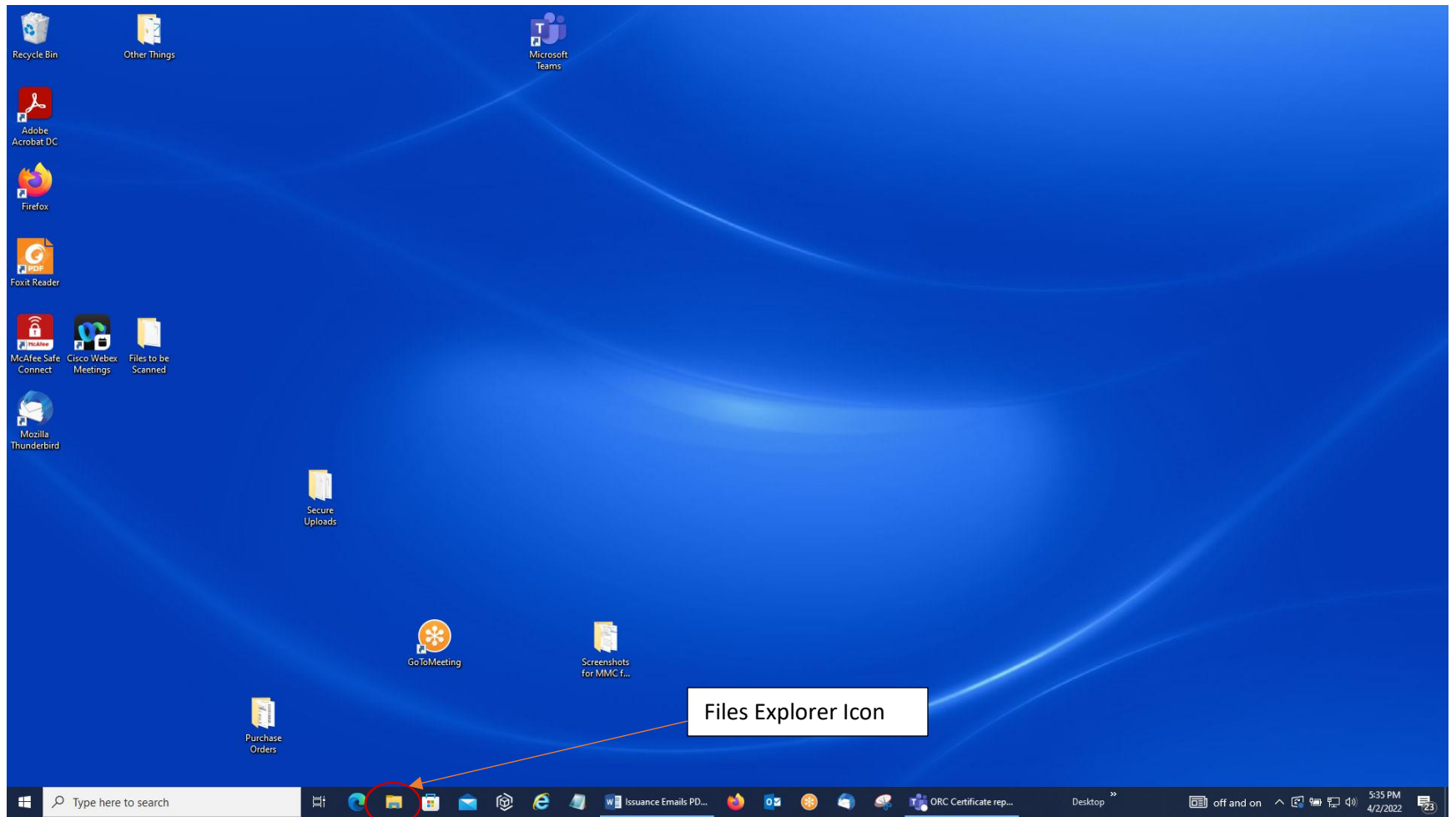
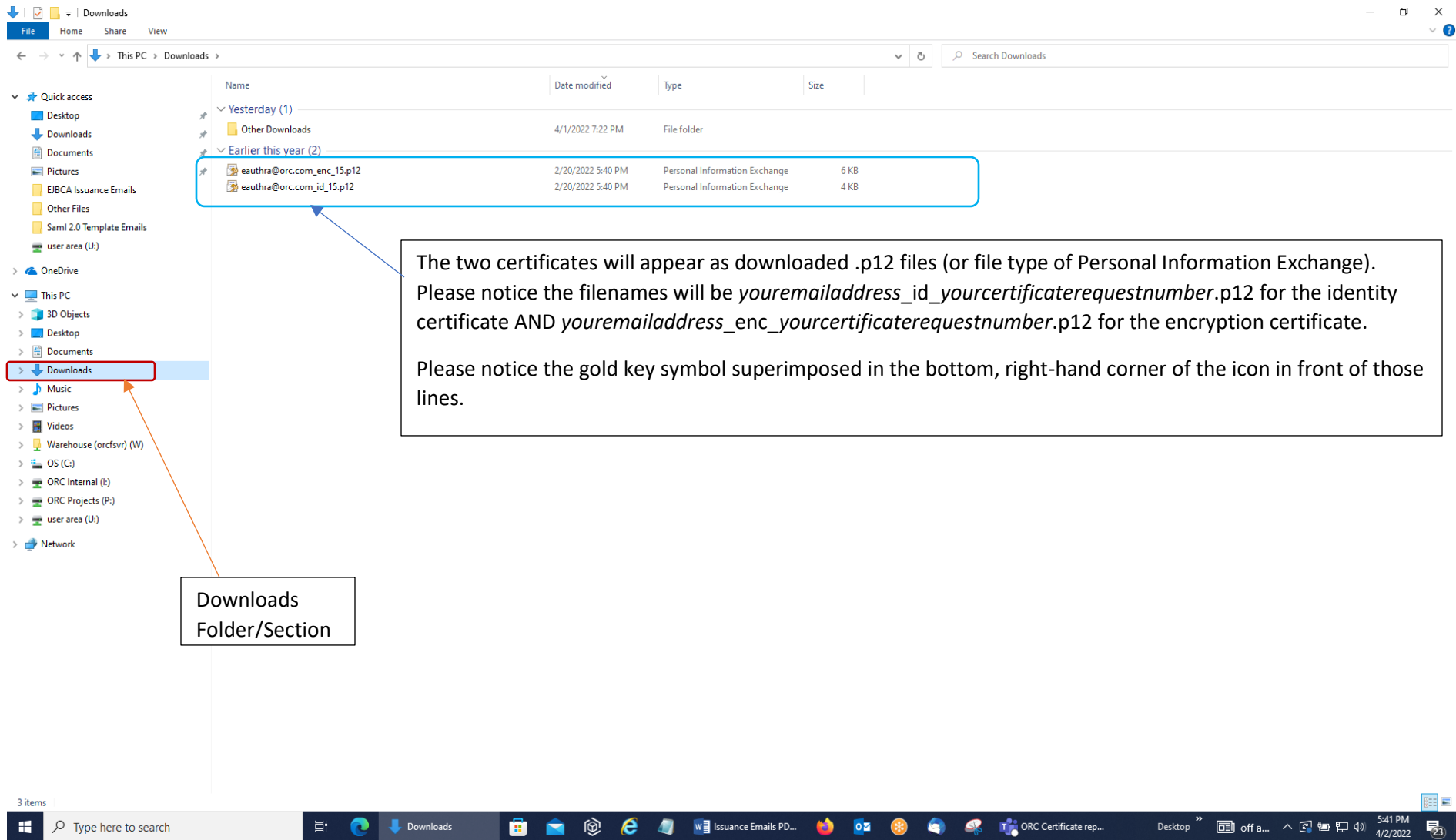


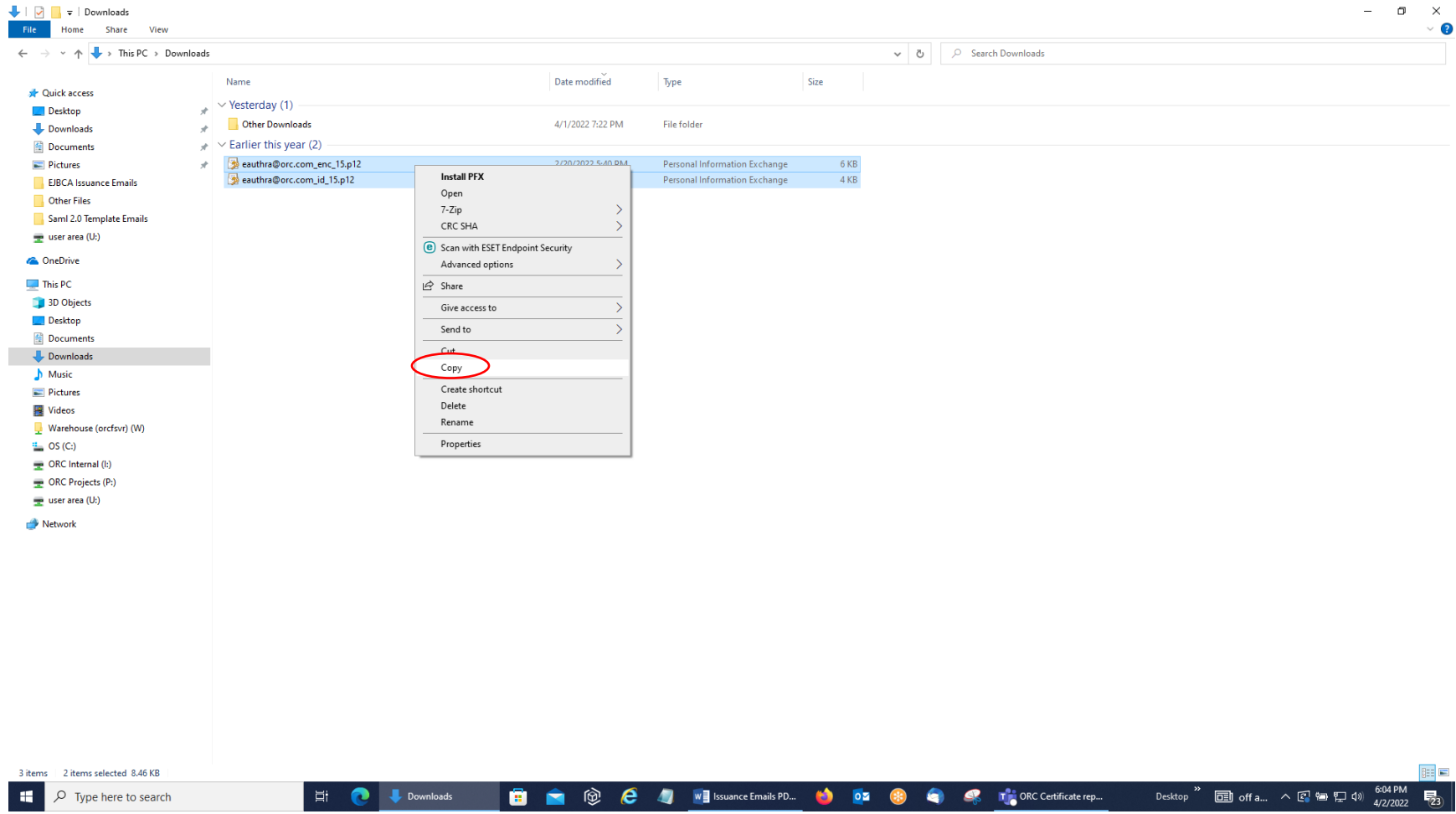
1. To verify that your ECA Medium Assurance Files properly downloaded, open your Files Explorer Screen (if you do NOT have the below icon on your taskbar, then search for Files Explorer in the Search Box next to your Start Button [this is a search within your computer, not on the Internet]).



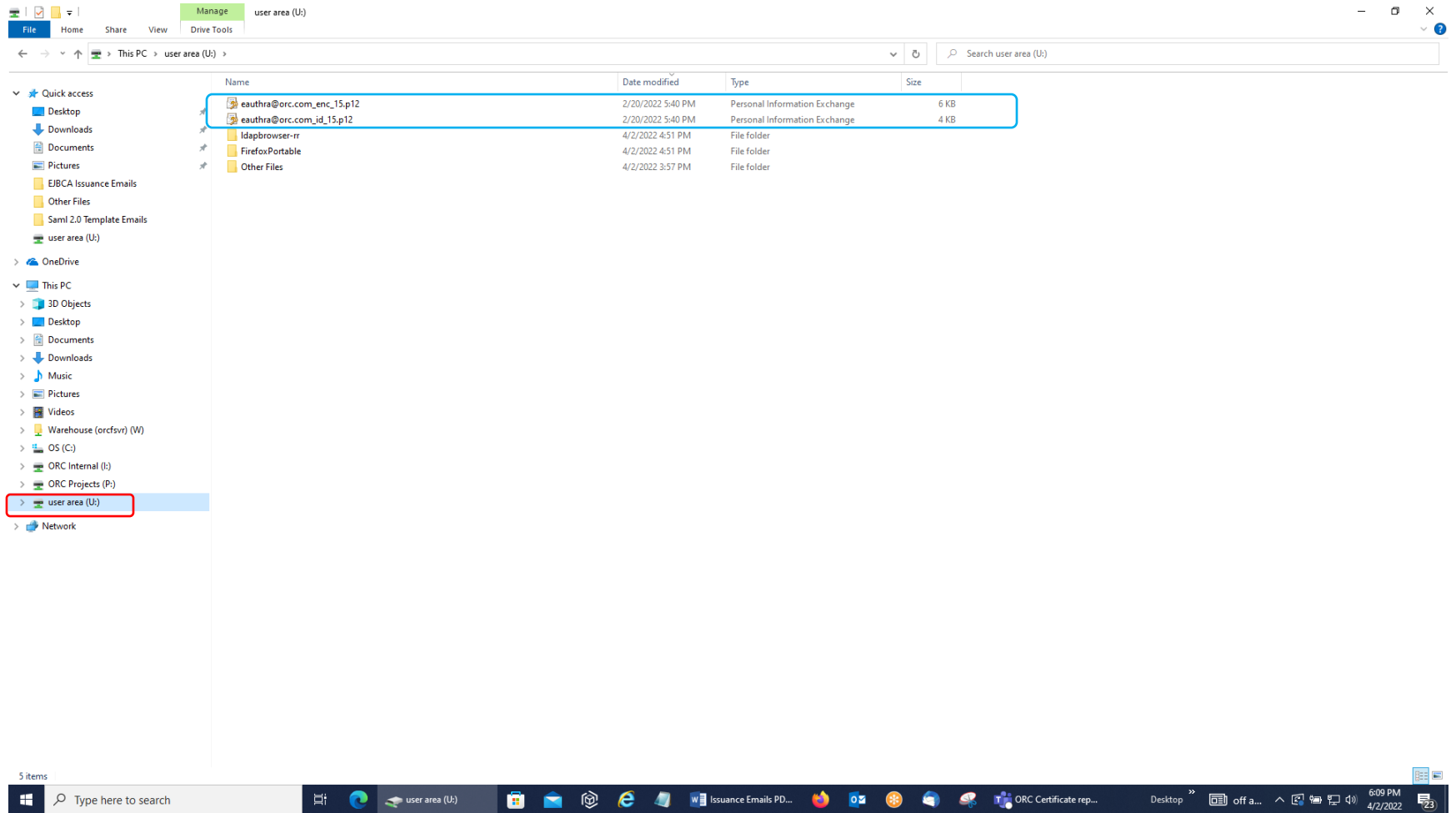
2. Within the Files Explorer Screen, you should see two .p12 files listed in your Downloads Folder/Section. If your computer does NOT show file extensions, then look for the File Types to be Personal Information Exchange.



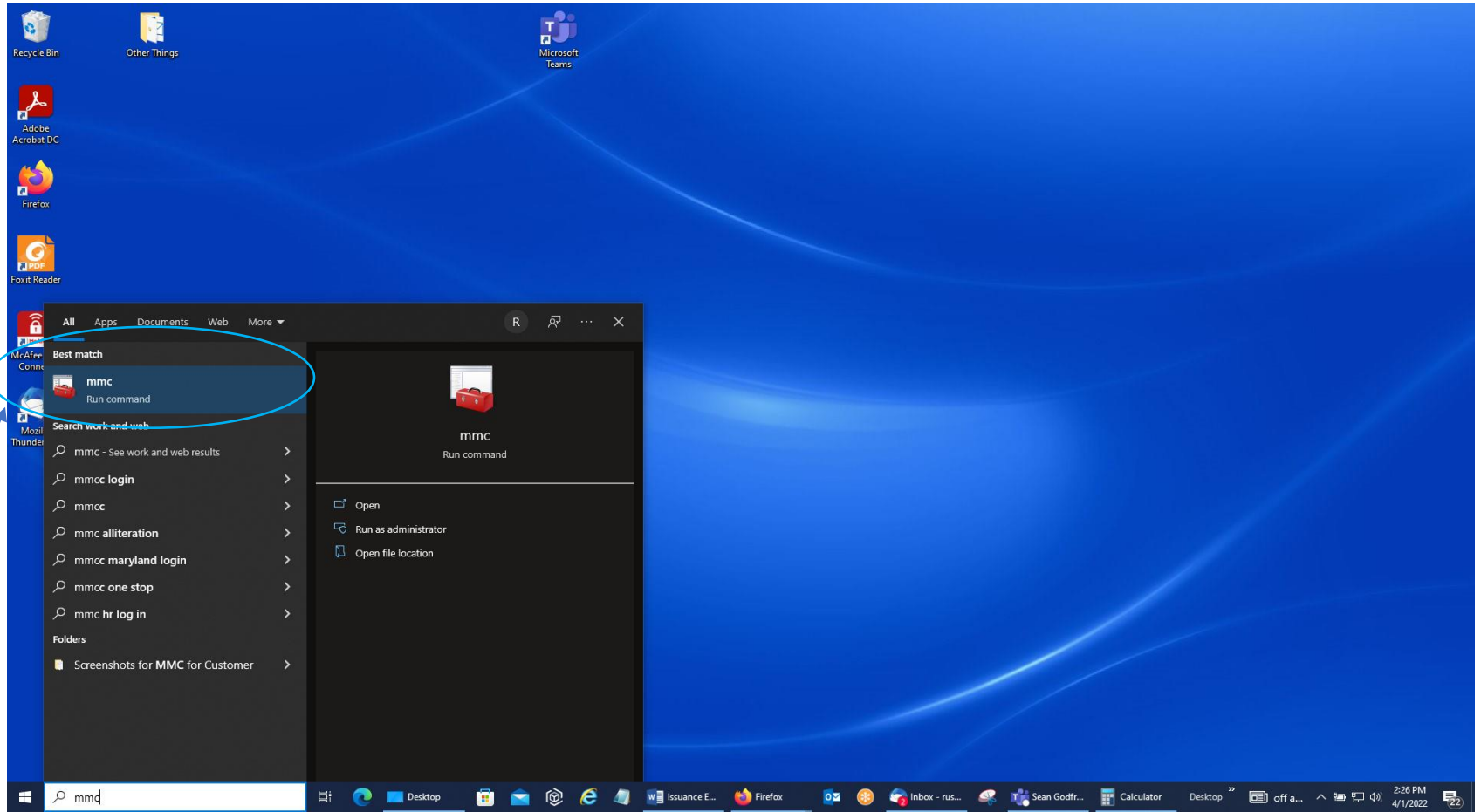
3. You immediately need to save backup copies of **BOTH** of these files to an external network drive (outside of your C: Drive) or flashdrive for operational purposes. These backup files along with the password you assigned to them will allow you to recover the certificates if your computer crashes.



4. Save them to your folder on the network drive in this case. If you use a flashdrive/thumbdrive, make sure that you follow the safe ejection procedure before disconnecting the flashdrive/thumbdrive from the computer.

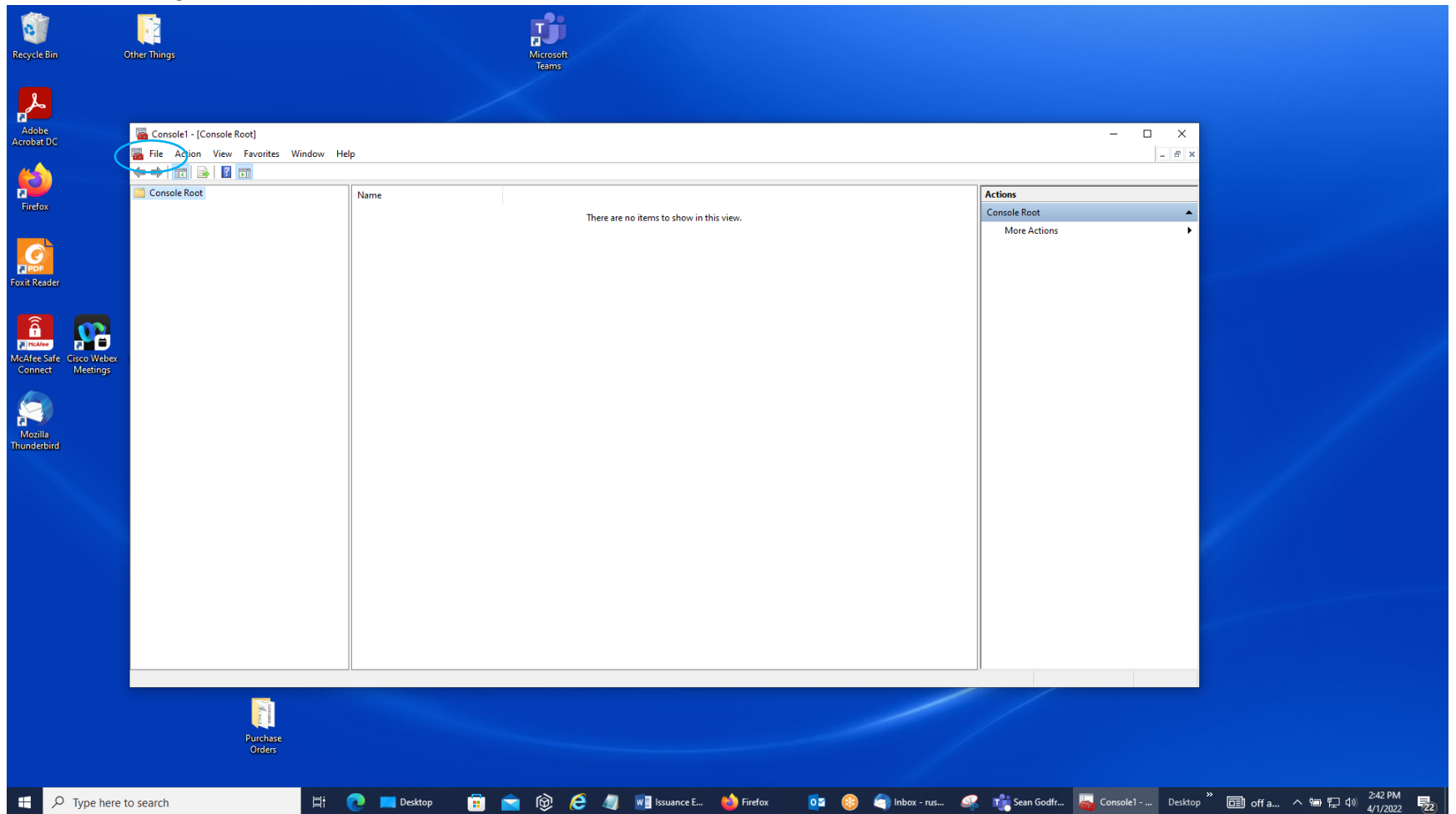


5. Next, you need to import them into the Windows Certificate Store to be able to use them in the browsers and with your applications. Access the Microsoft Management Console (MMC) for your profile on this PC (you may need admin permissions from your IT Department to do this).

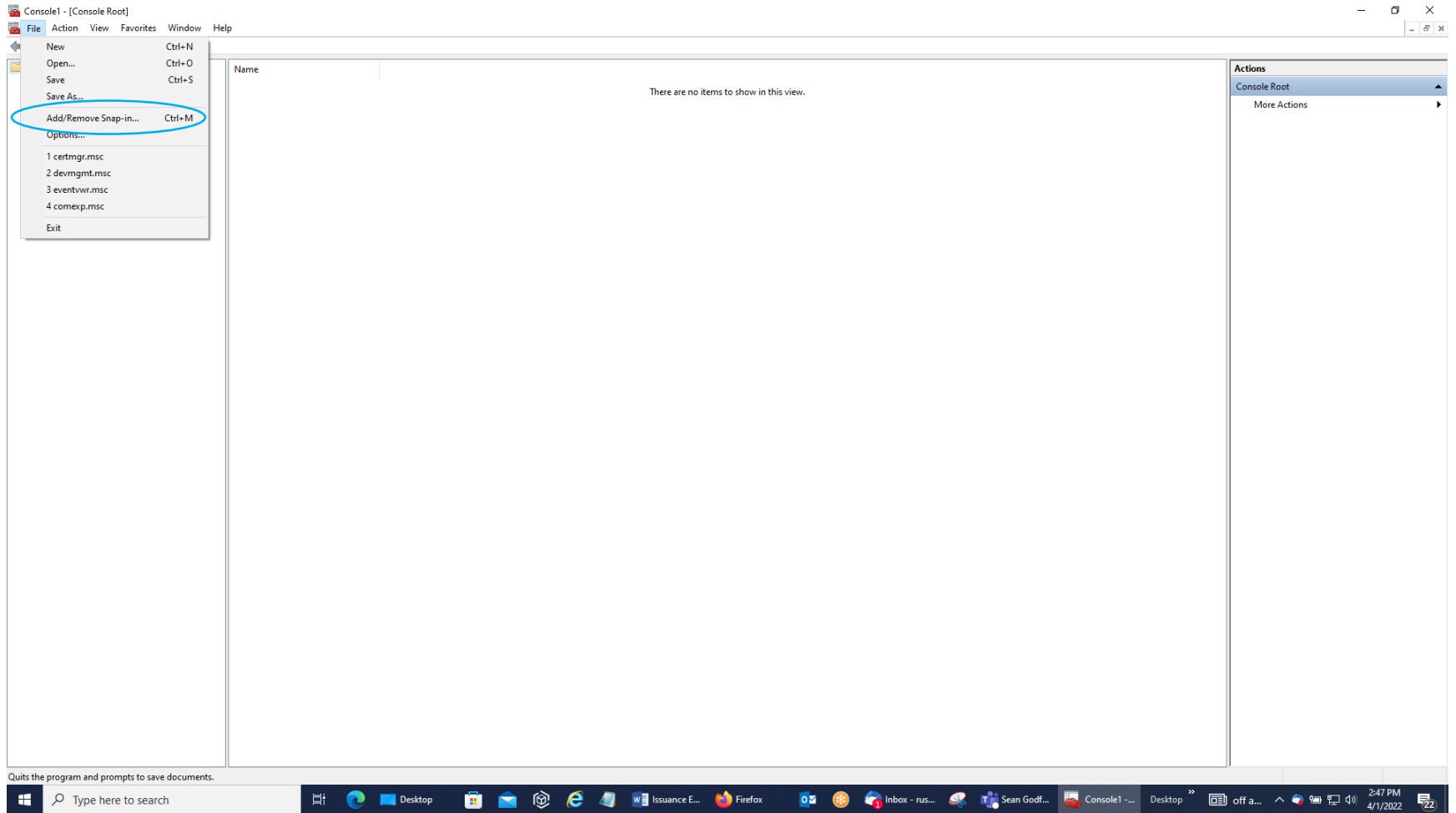


Select this mmc run command by clicking the left mouse button on it.

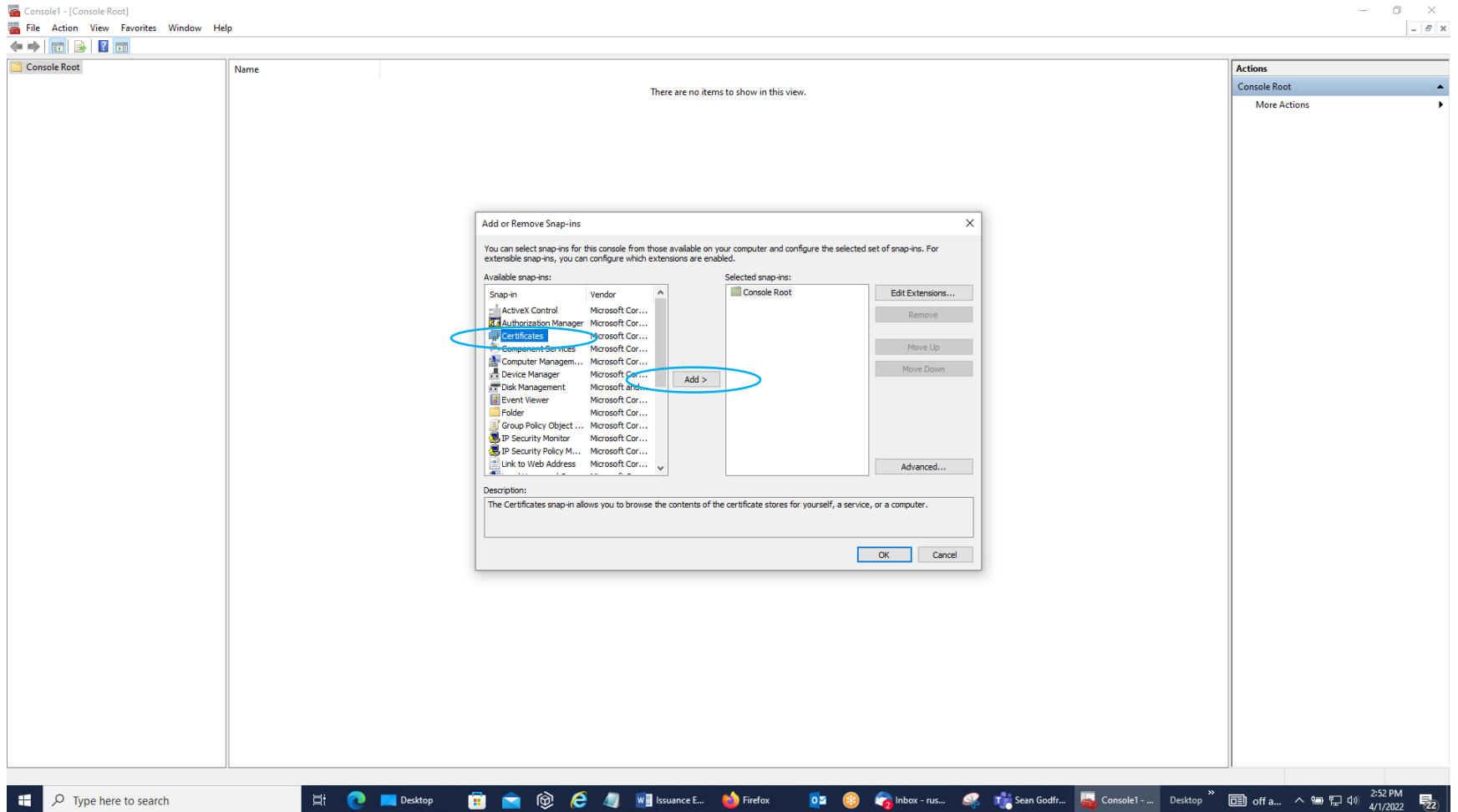
- You should get a User Account Control Screen that will ask you if you want to allow this app to make changes to your device; it will have Microsoft Management Console listed. Click 'Yes' to open up the MMC for your profile on your PC.
- You should then get the Console 1 – Console Root Screen below. Click on the word 'File' in the Menu Bar.



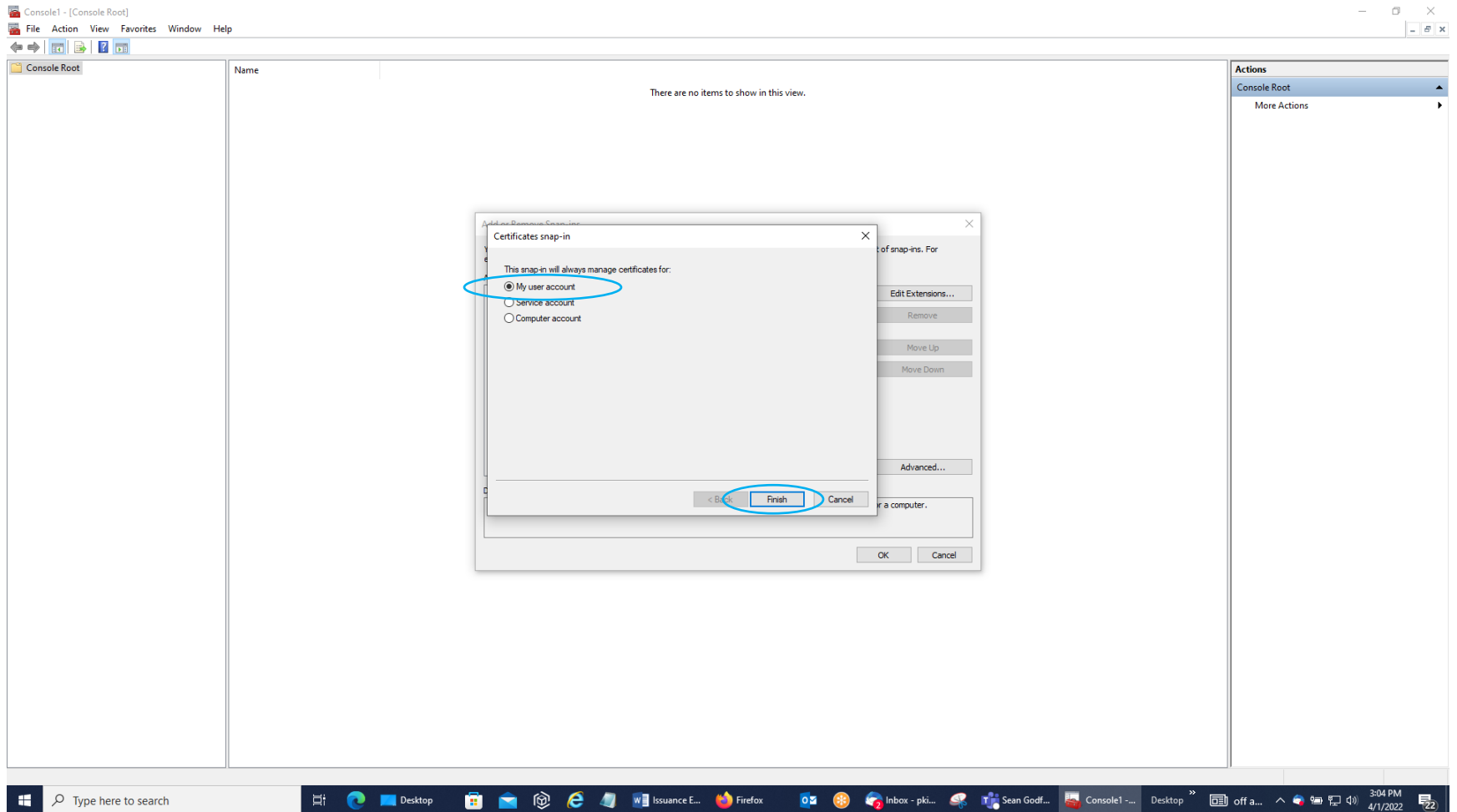
8. Select 'Add/Remove Snap-in' from the list.



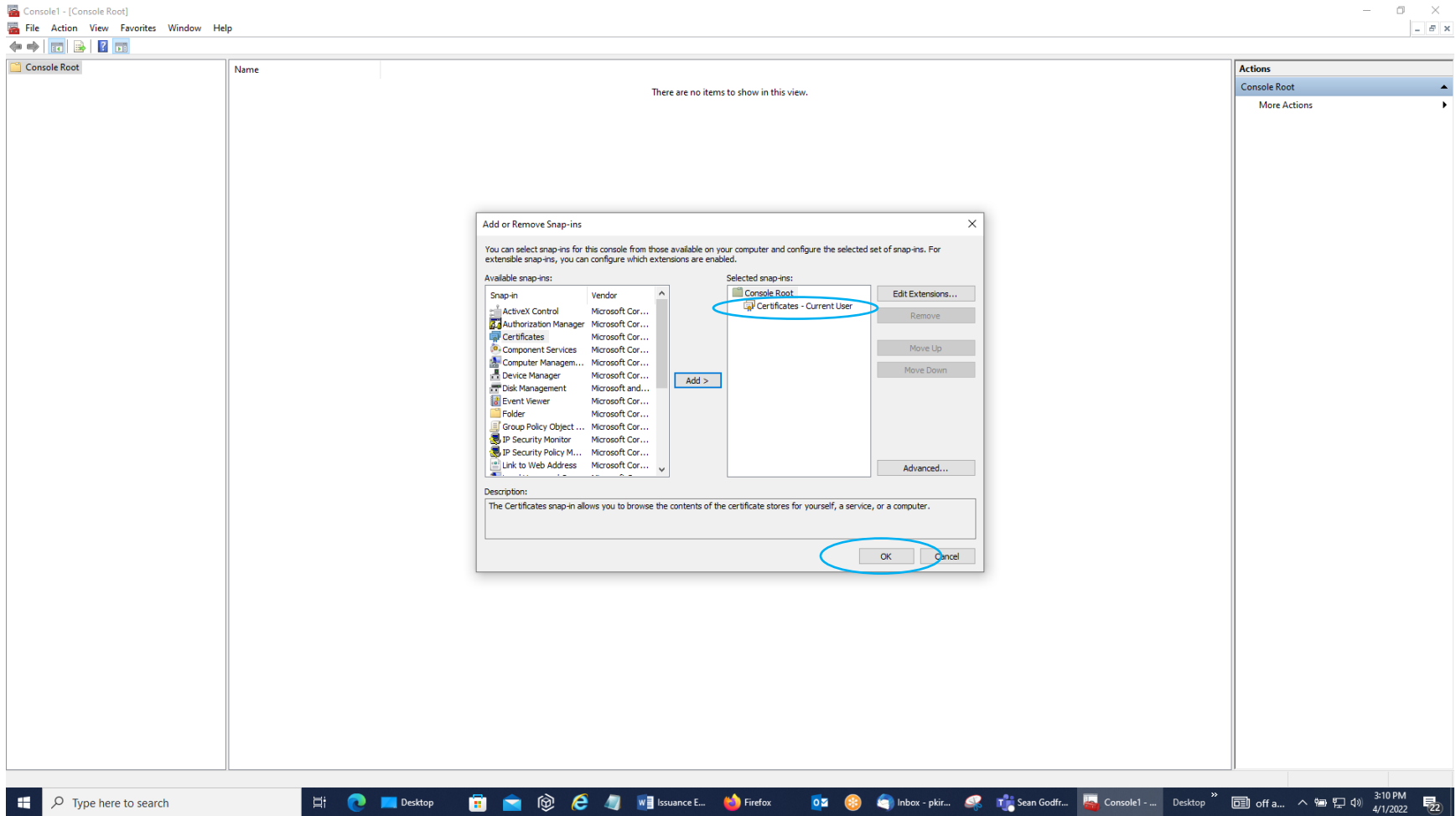
9. Then, in the Add or Remove Snap-ins Screen, go the Available Snap-ins Side, select the word 'Certificates' to highlight it in blue, and click on the 'Add' Button.



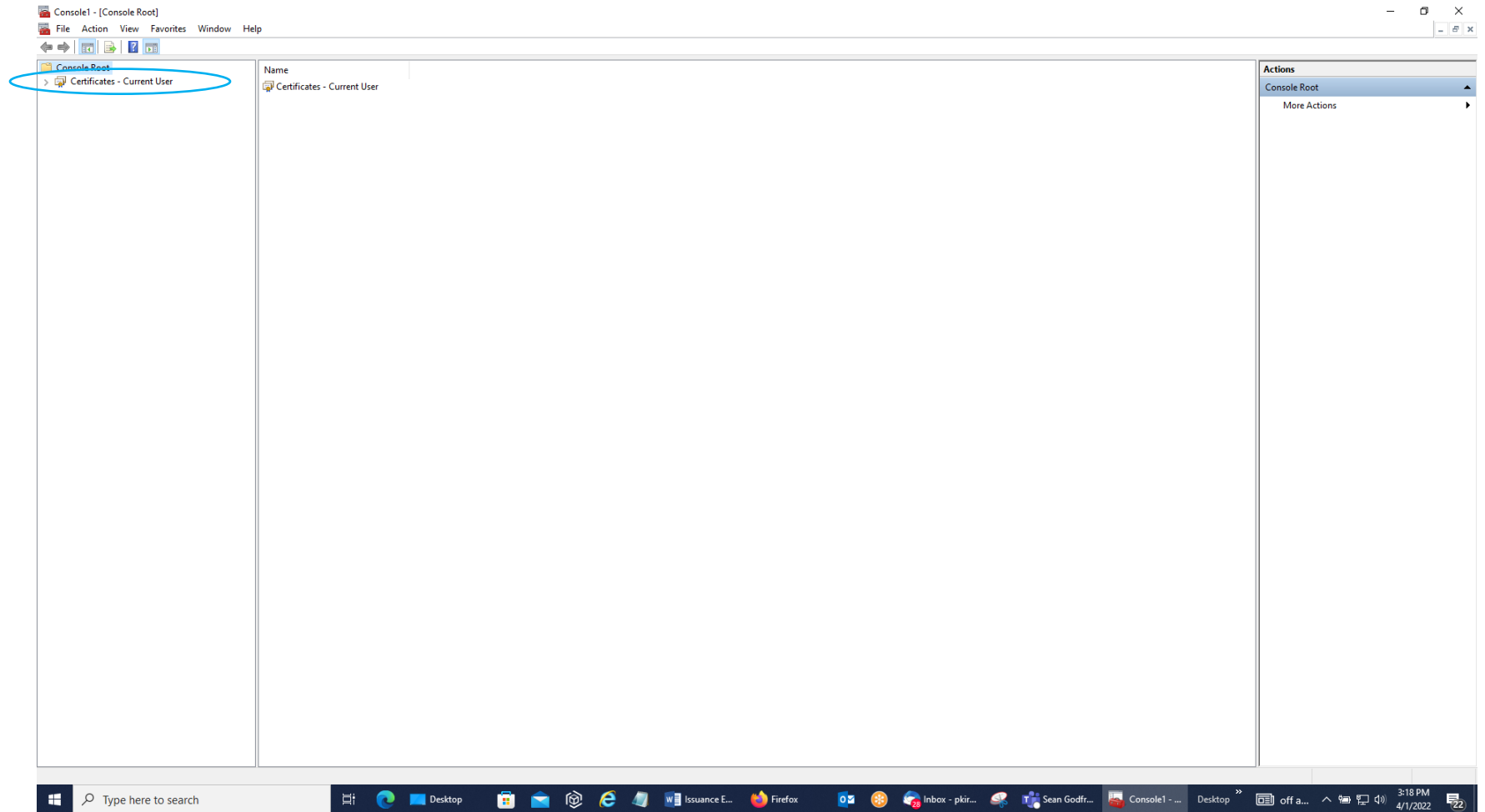
10. You should get a Certificates snap-in screen with 'My user account' selected. Leave it on that selection and click the 'Finish' Button. (Some of you may not get this screen; instead, the computer will jump to the screen on the next page.)



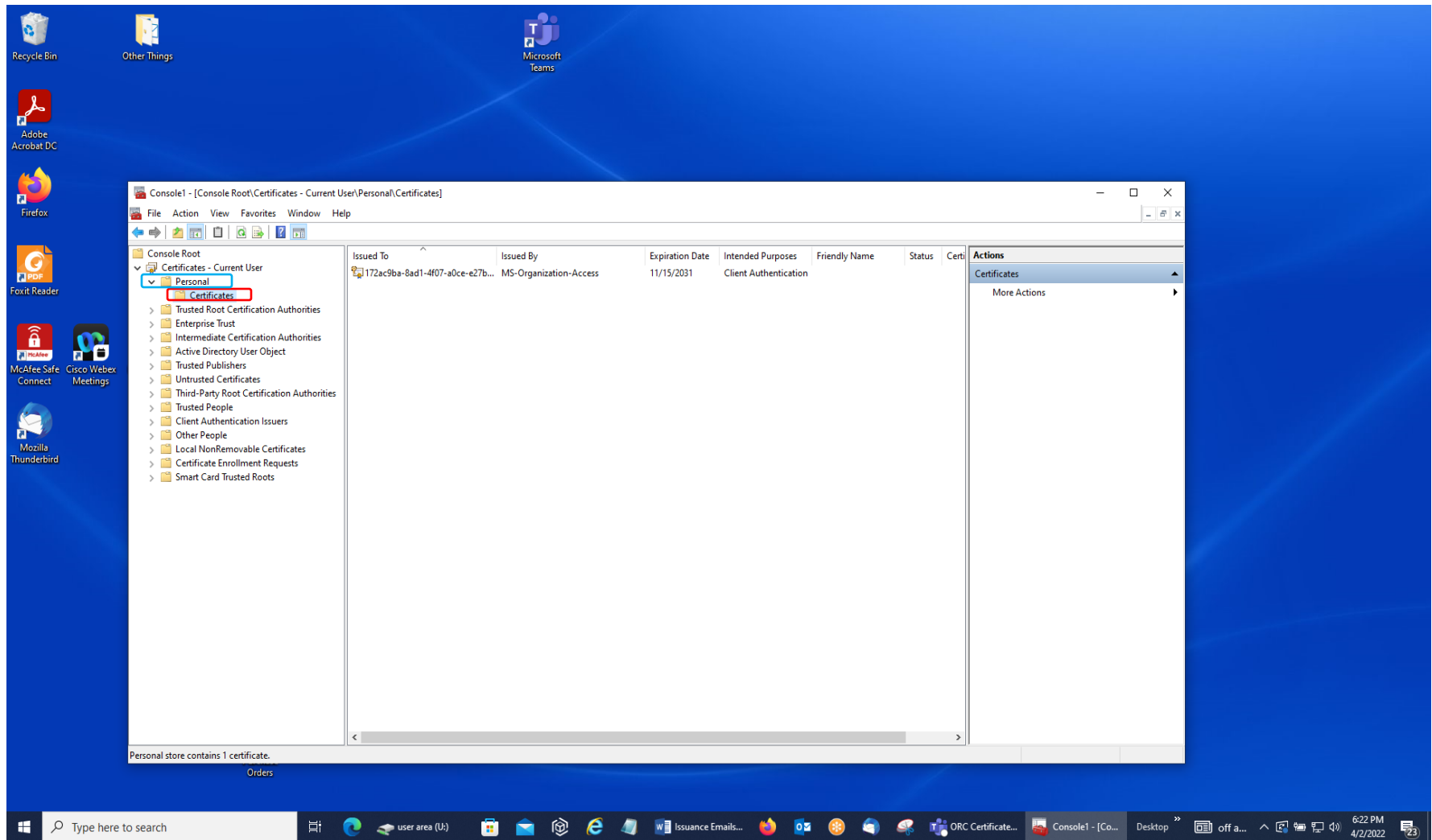
11. You will then get a 'Certificates – Current User' Line on the Selected Snap-ins Side. Click the 'OK' Button.



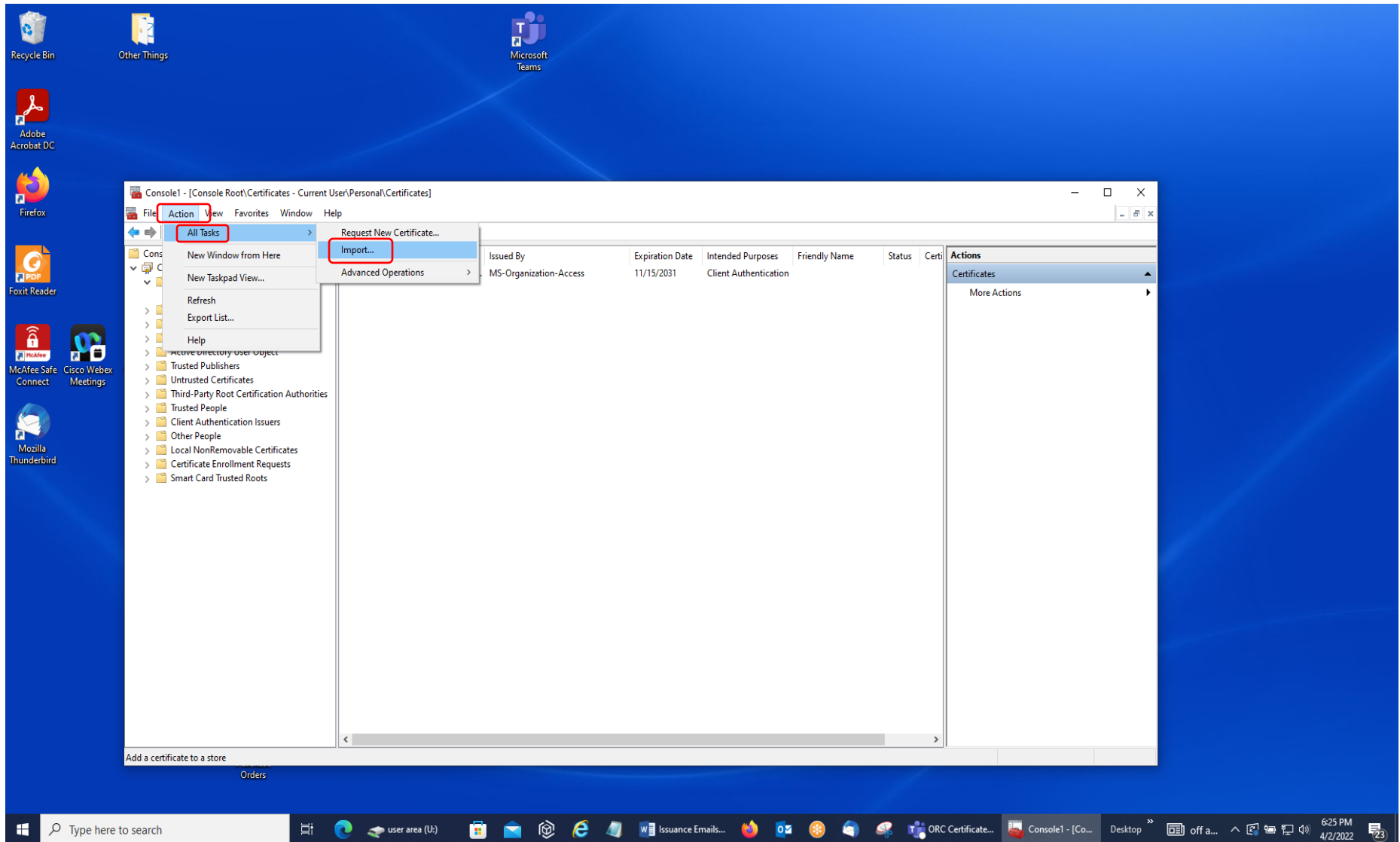
12. You should then come back to the main Console 1 – Console Root Screen with the ‘Certificates – Current User’ Line under the Console Root Folder in the left-side window pane. Click on the arrow or hash mark in front of that line to display the list of folders within that group.



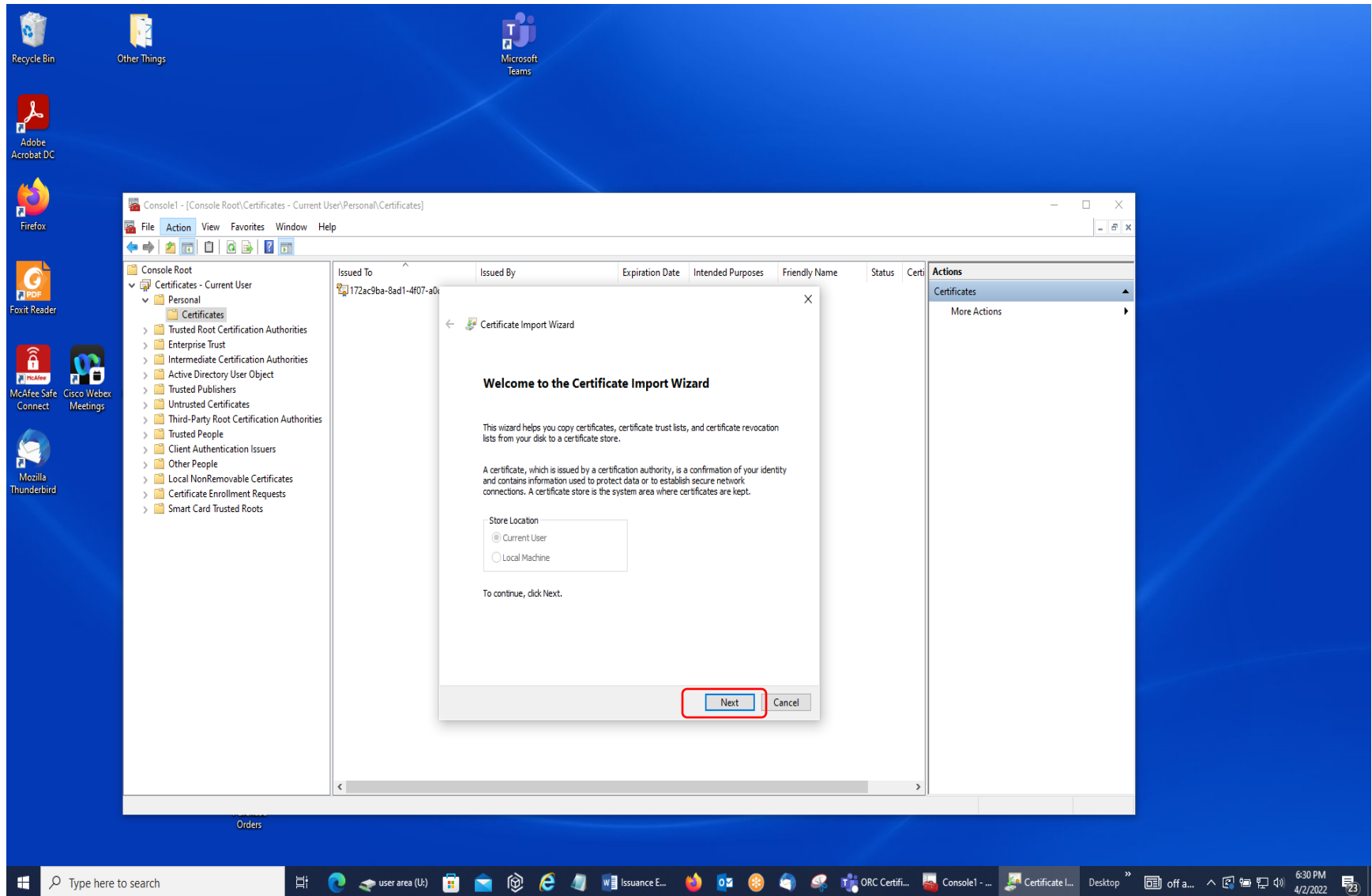
13. Open up the Personal Folder by clicking on the arrow or hash mark (blue outlined box) and then the Certificates Sub-Folder (double-click the left mouse button in the red box) if there is one. If there is NO Certificates Sub-Folder, then highlight the Personal Folder by clicking on it.



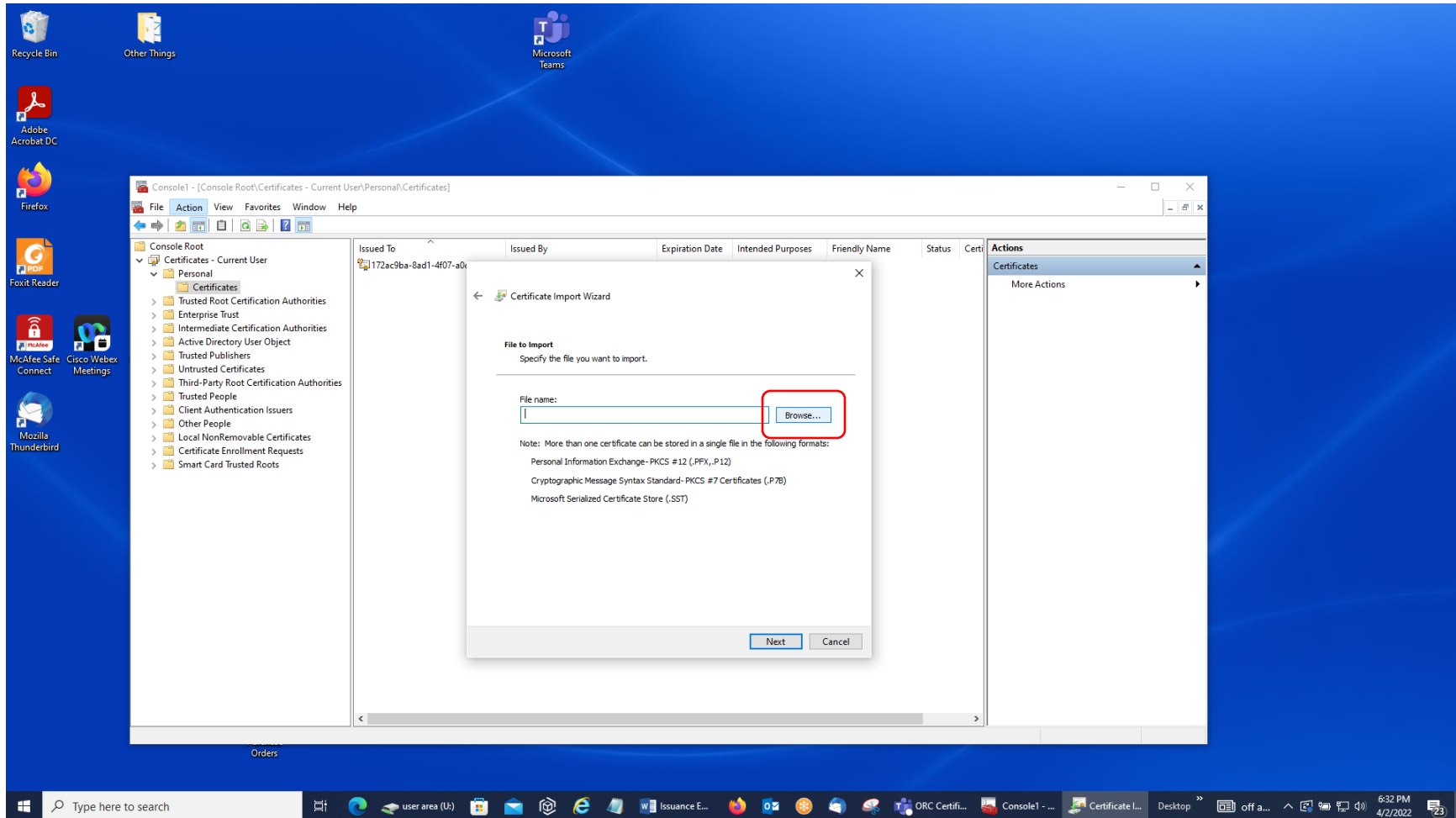
14. Next, start the procedure to import the identity certificate from the Downloads Folder/Section of your PC. In the menu bar select 'Action,' then 'All Tasks,' and 'Import.'



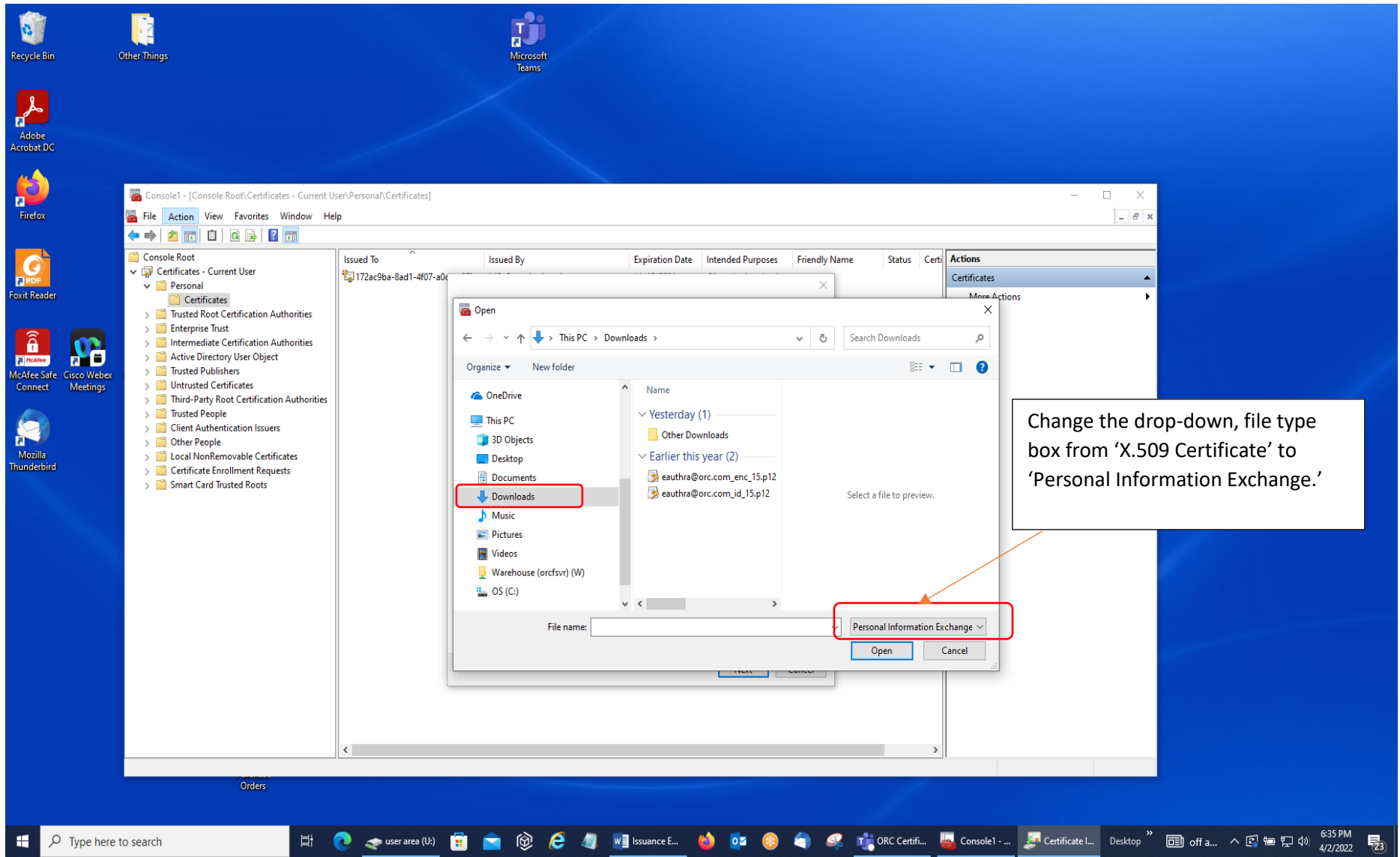
15. Select 'Next' on the Welcome to the Certificate Import Wizard Screen that opens up.



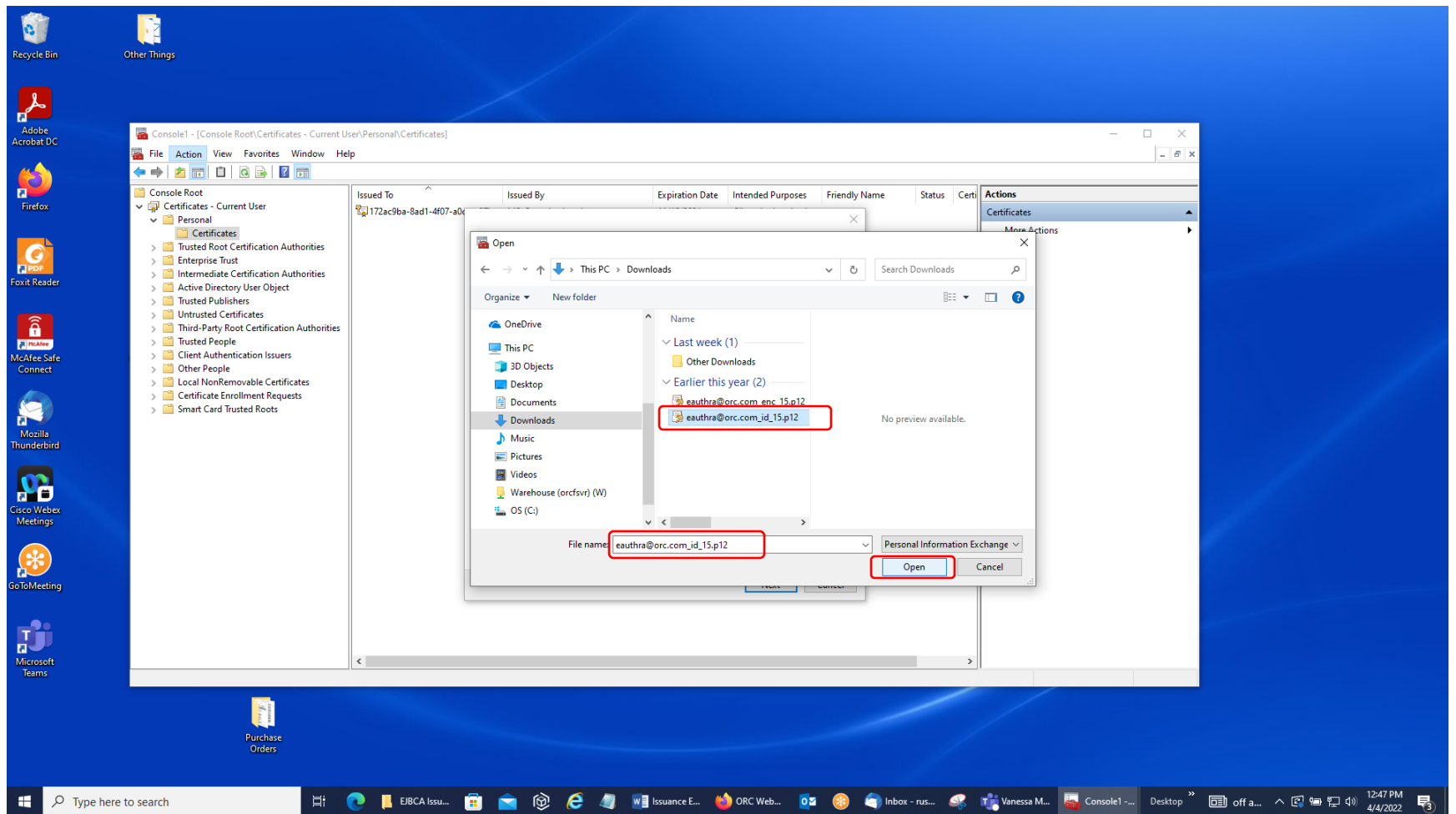
16. Click on the 'Browse' Button in the File to Import Screen.



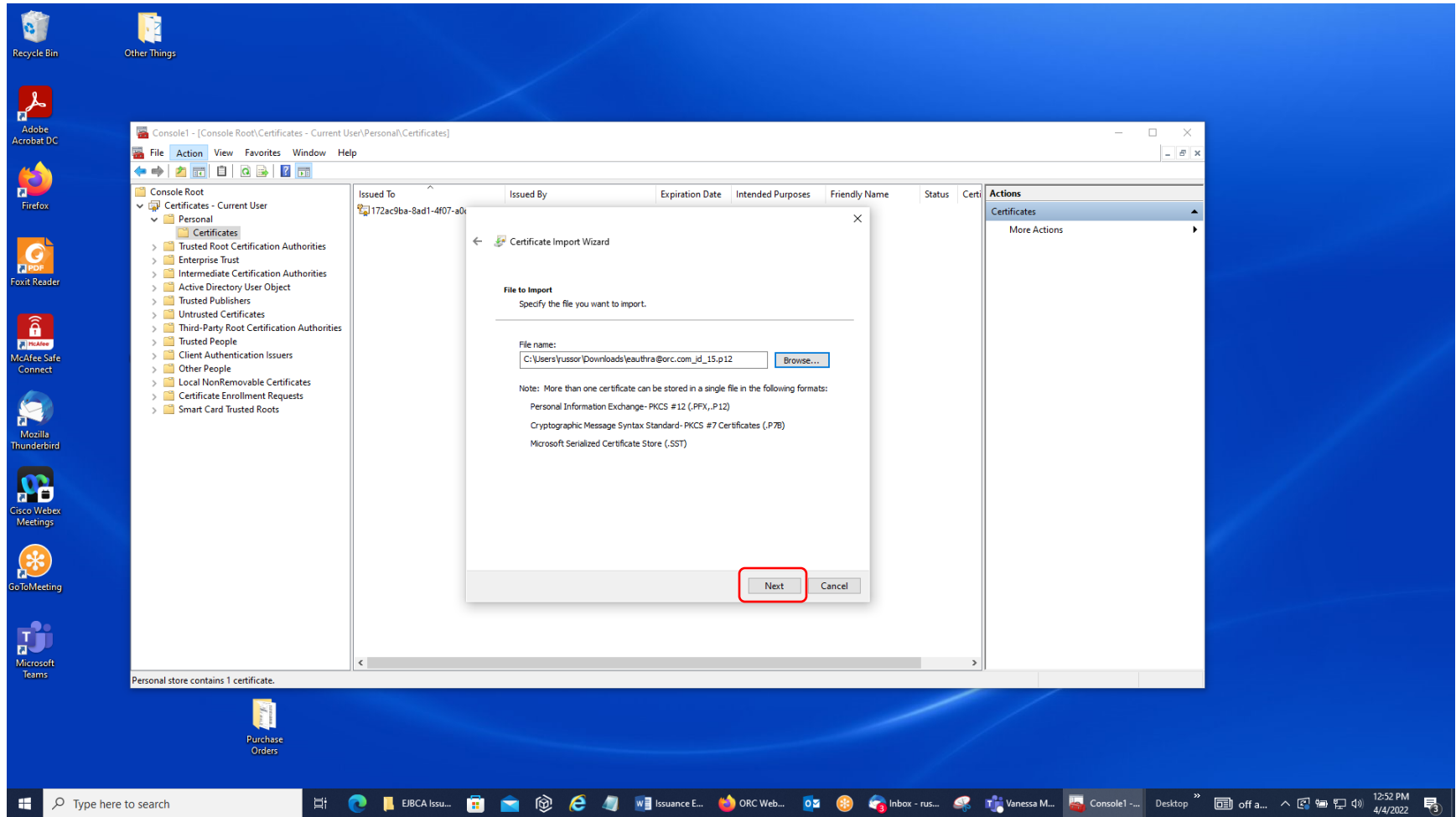
17. Select the Downloads Folder/Section in the Files Explorer Screen and then change the file format in the bottom, right-hand corner of the screen from X.509 Certificate to Personal Information Exchange.



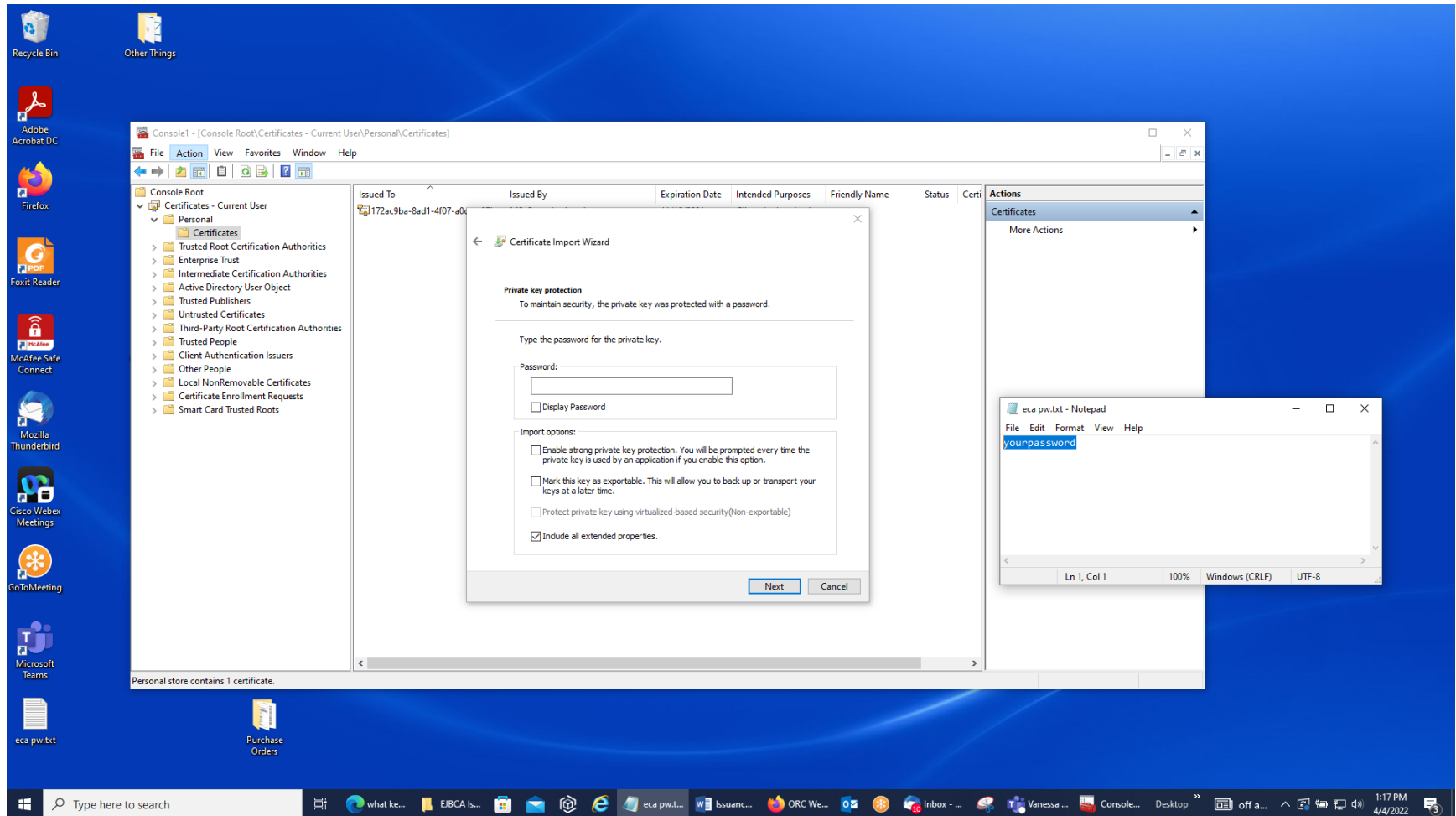
18. Select the certificate file that has 'id' in it so that it appears in the blank File name box at the bottom. Then, select the 'Open' Button.



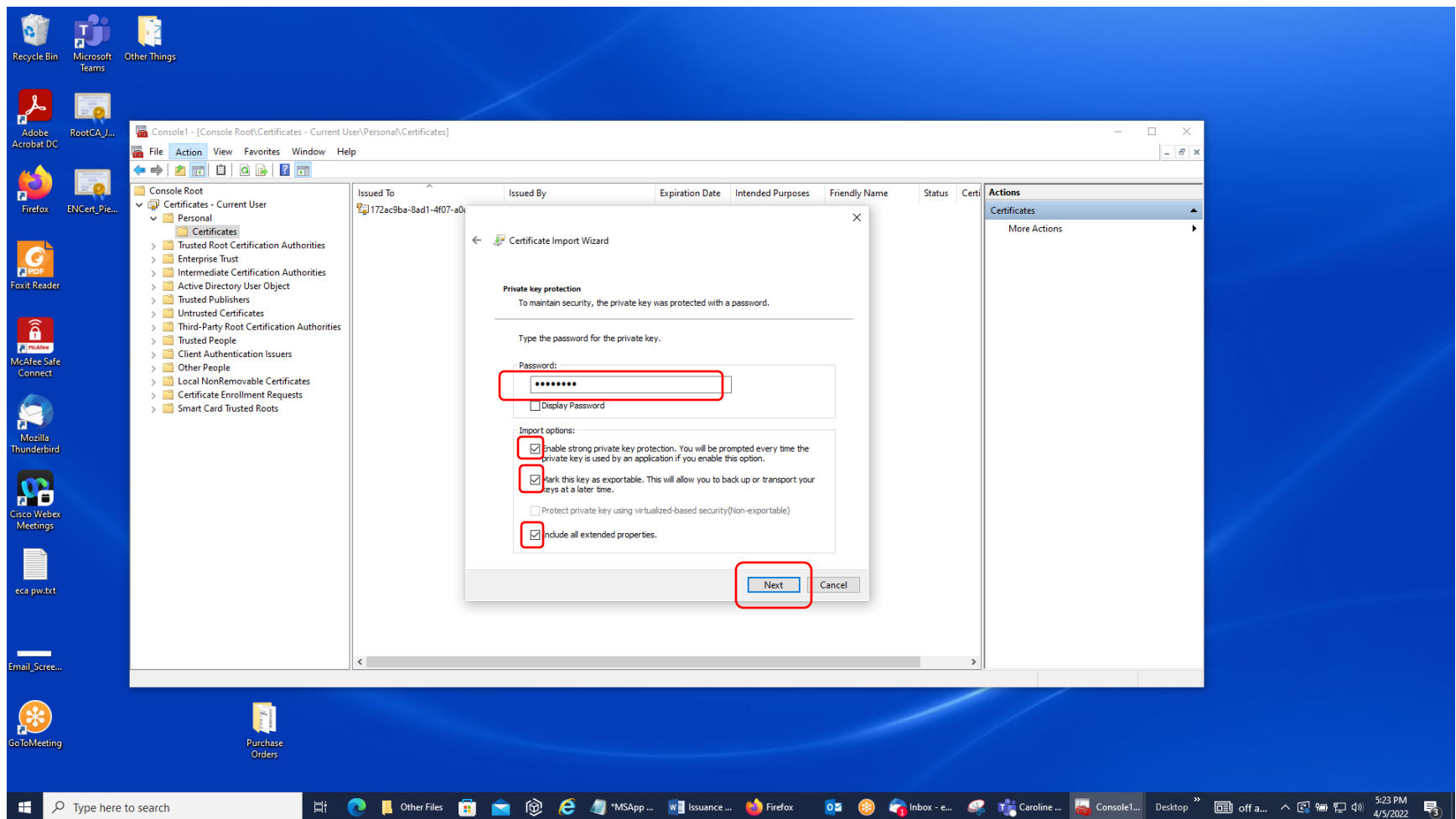
19. You will see the following screen. Select the 'Next' Button.



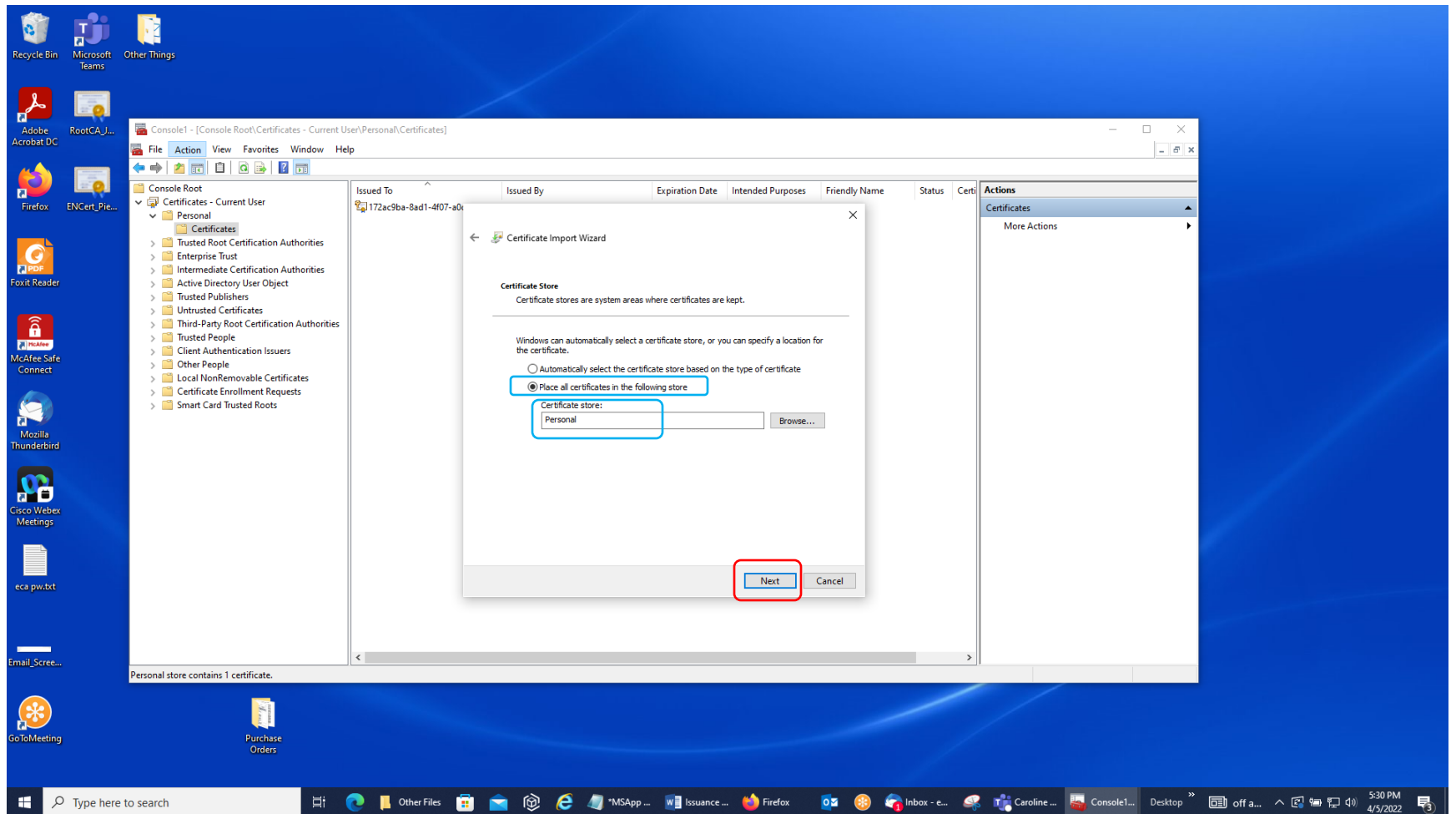
20. You will see the following screen, with the exception of the open Notepad File. Open up the Notepad File with the password that you assigned to those certificate download files during the download process while you were logged into your account at our site, highlight it in the Notepad File, and put it in the copy queue (ctrl button + C; or right-click the mouse button on the highlighted password and select 'Copy'). Do NOT use 'yourpassword' as the certificate password!



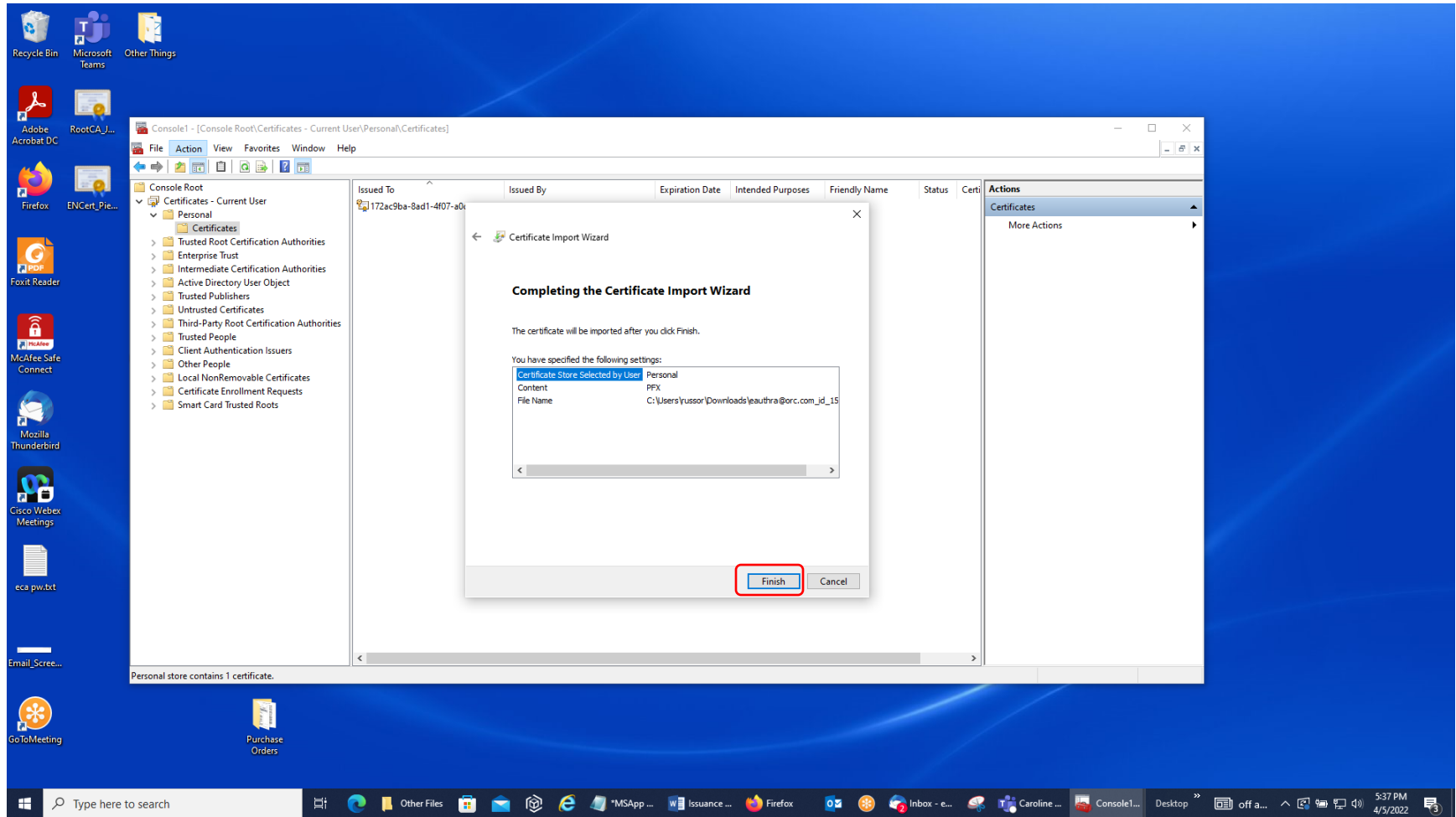
21. Next, paste your password into the 'Password' Box in the Certificate Import Wizard Screen (you can check to see if it is correct by checking the 'Display Password' Box). Also, check the first, second, and fourth boxes under 'Import options.' Then, click 'Next.'



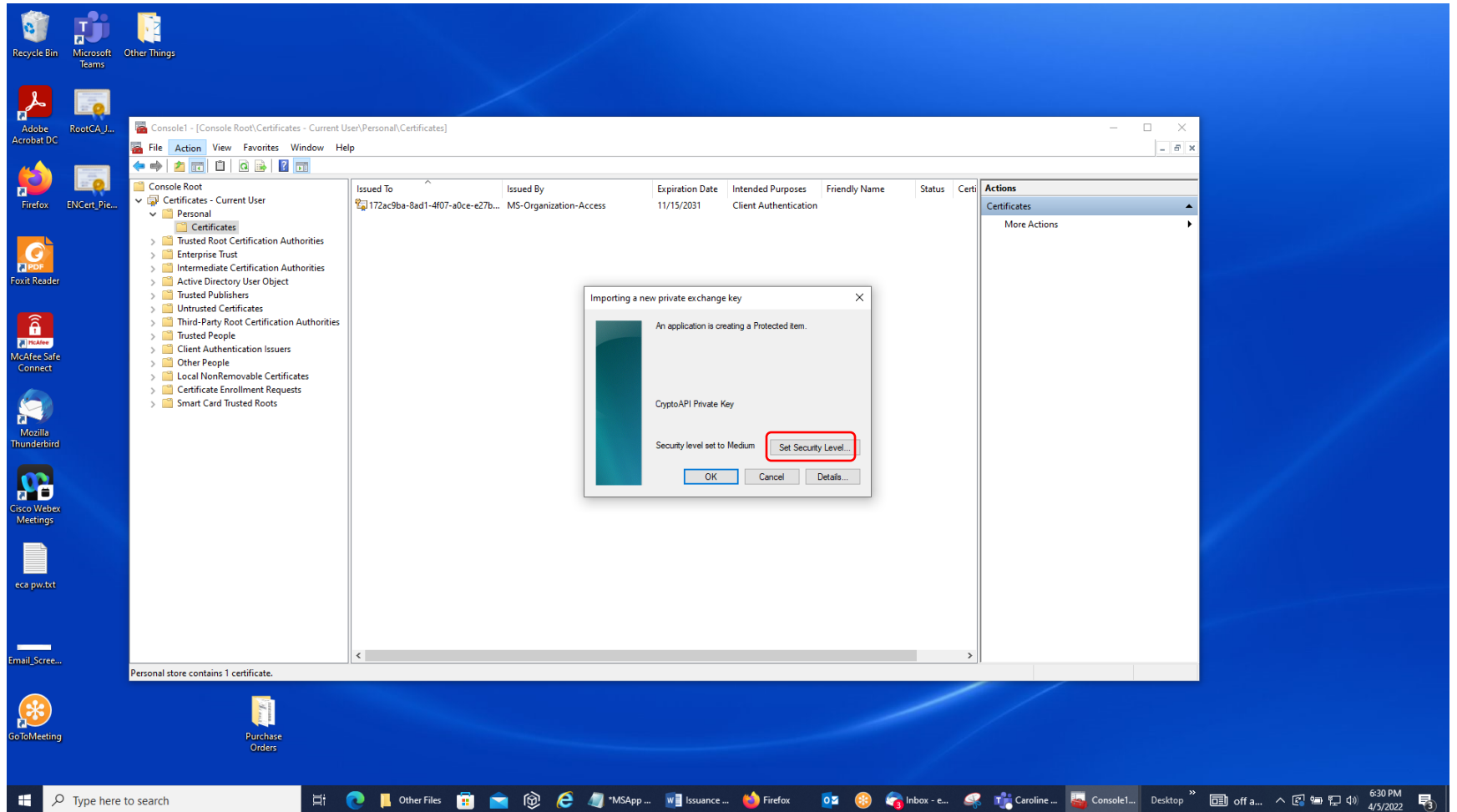
22. You should see the following screen. 'Place all certificates in the following store' should be selected, and the 'Certificate store' Box should have the word 'Personal' in it. Click 'Next.'



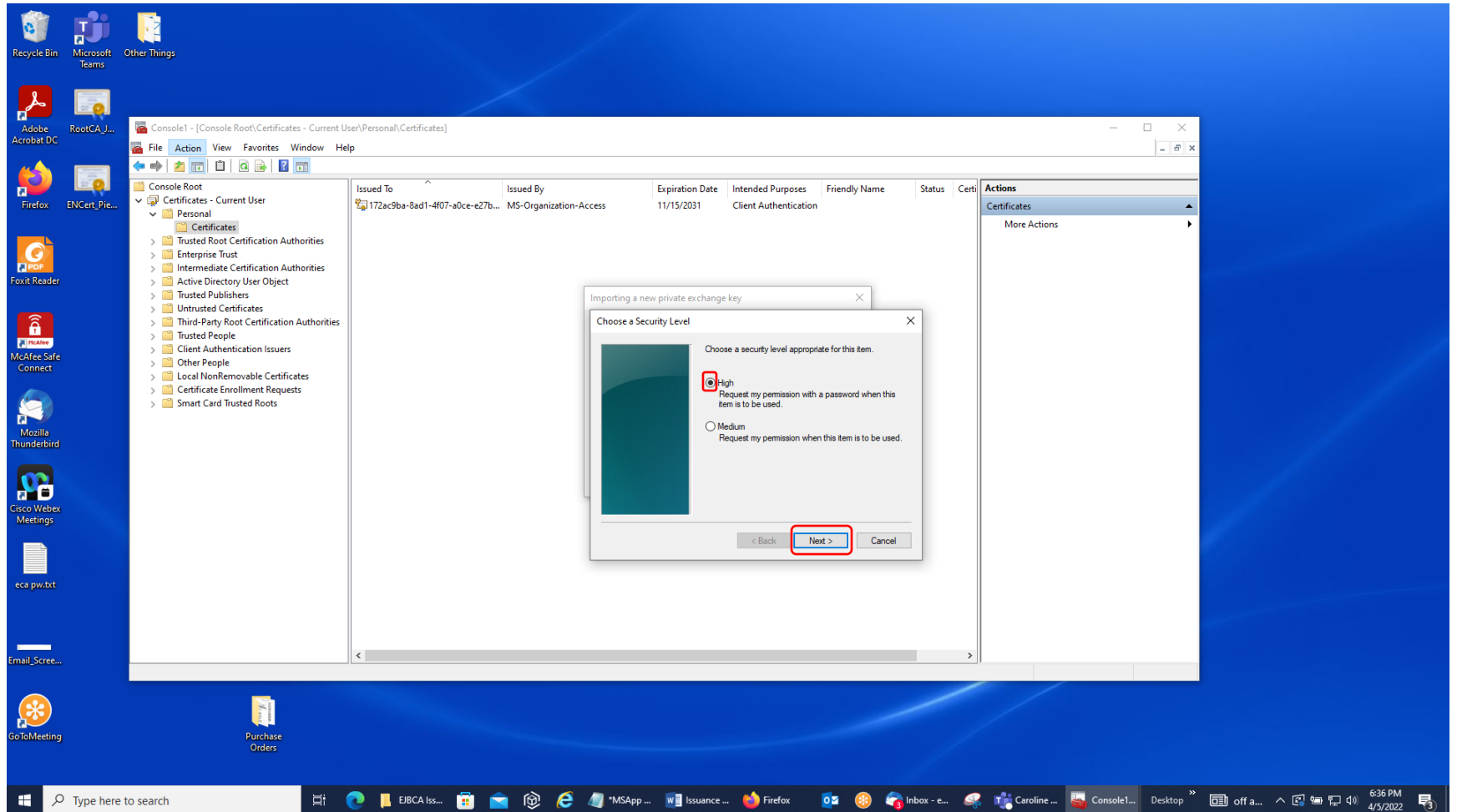
23. Click 'Finish' on the 'Completing the Certificate Import Wizard' Screen.



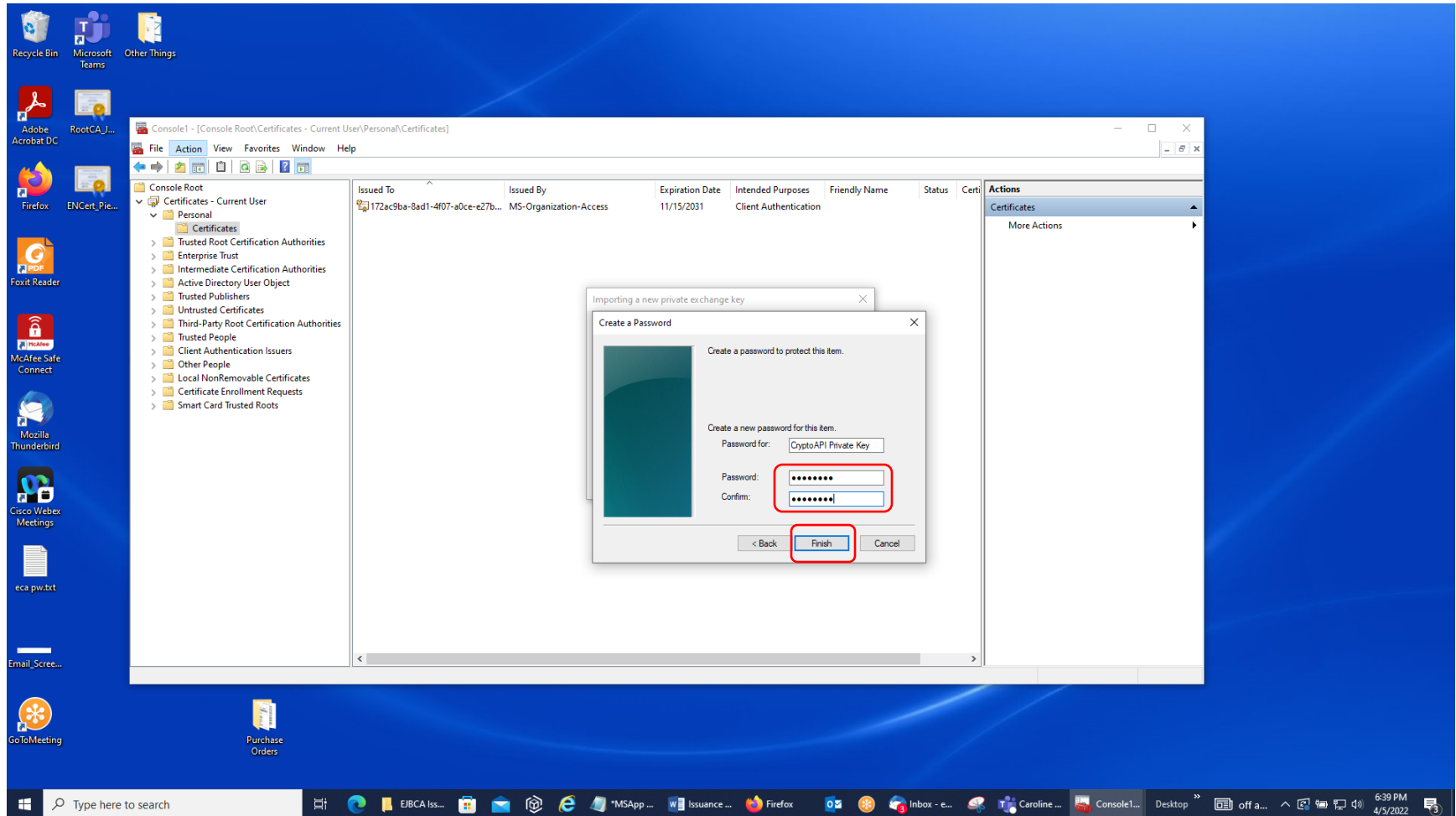
24. Select the 'Set Security Level' Button.



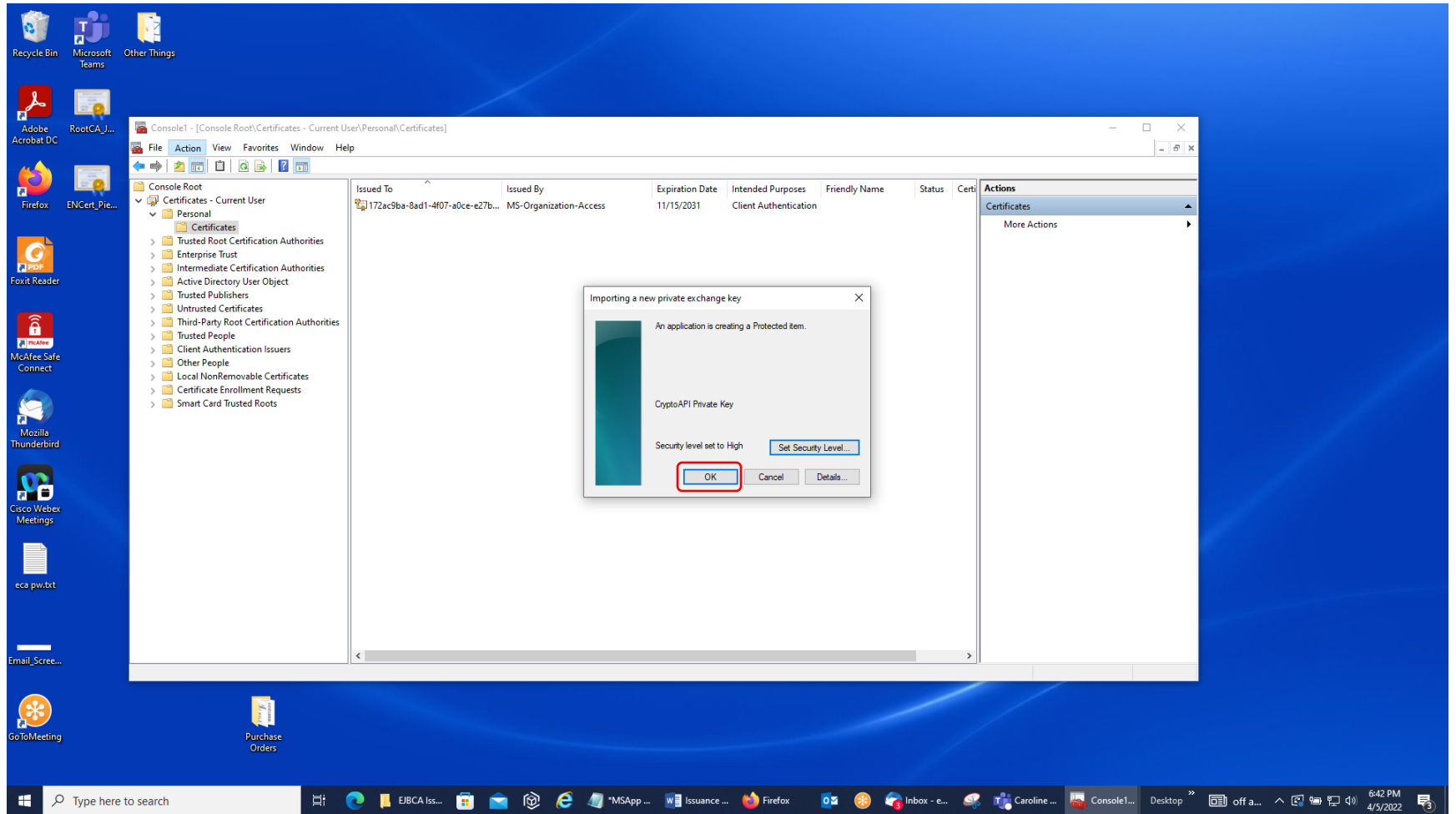
25. Select the Radio Button for 'High' and click 'Next.'



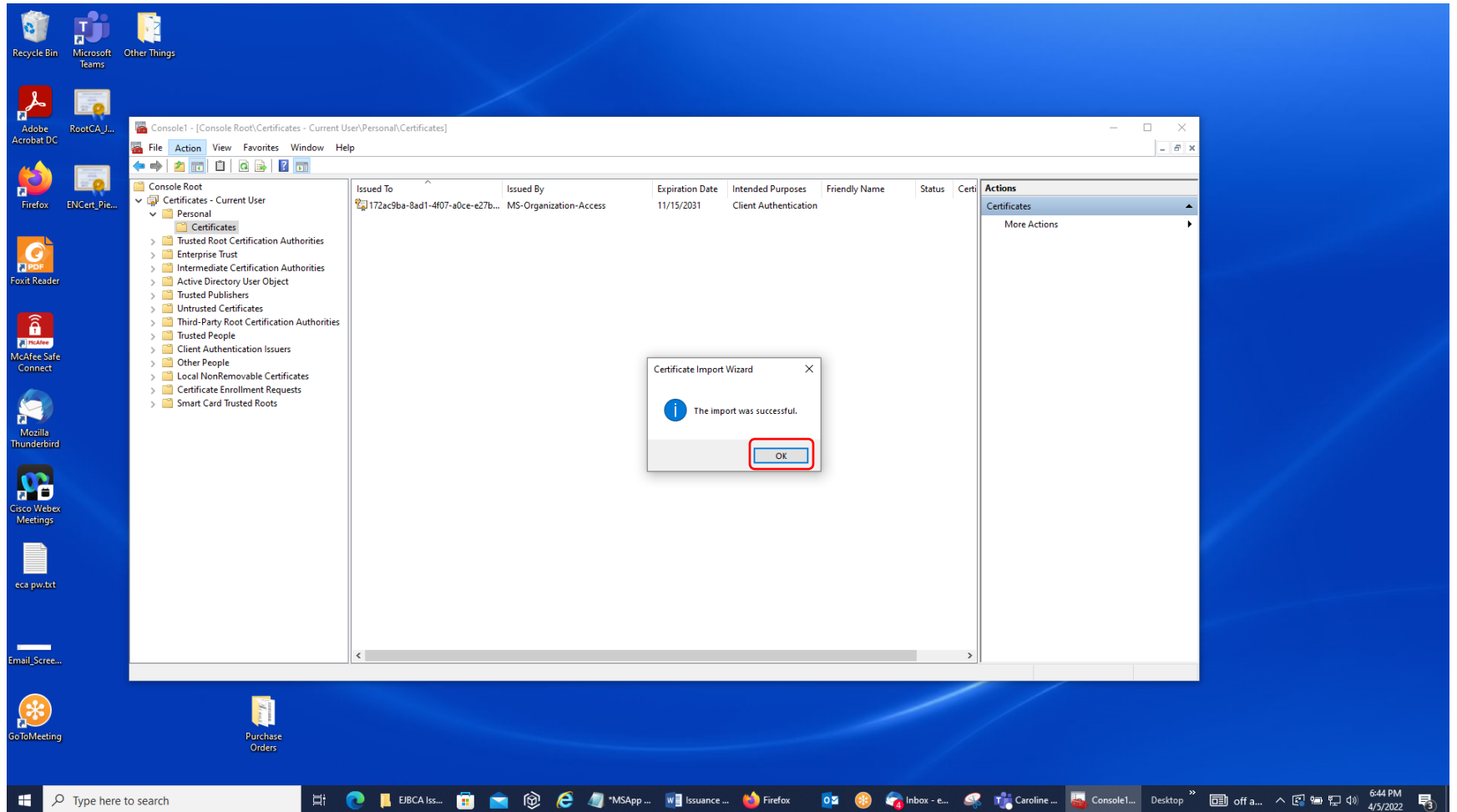
26. Paste your password into the two blank boxes using the certificate password you typed into Notepad and click 'Finish.'



27. Then, click 'OK.'



28. You should get the following response. Click 'OK.'



29. You will see your identity certificate in the Certificates Sub-Folder of the Personal Folder in the Windows Certificate Store. Notice the gold key symbol on the left edge of the certificate icon at beginning of the line. You may get extra trust chain certificates to appear along with it in that Center Pane; just ignore them.

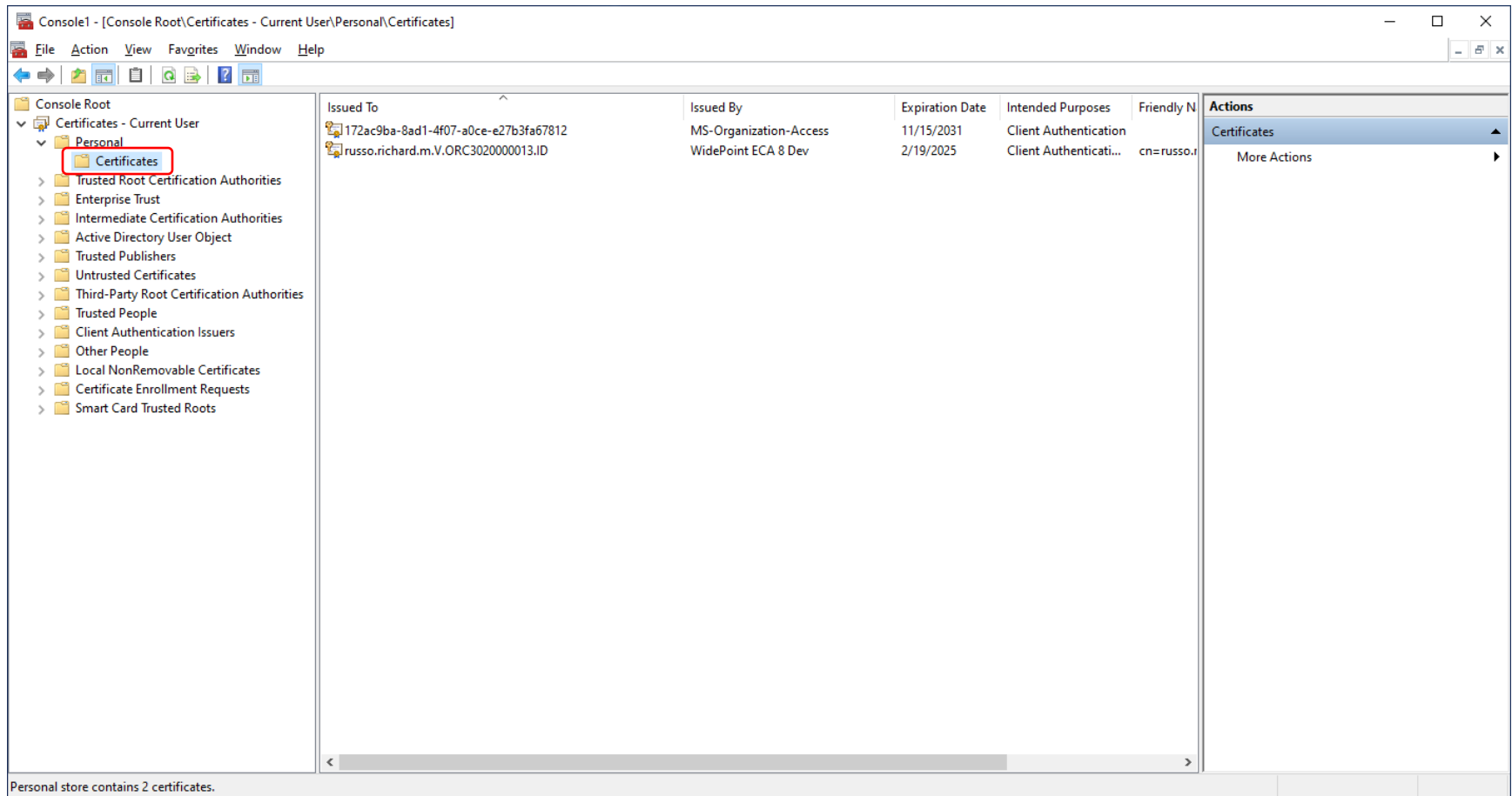
The screenshot shows the Windows Certificate Store console. The left pane displays the tree structure: Console Root > Certificates - Current User > Personal > Certificates. The right pane shows a table of certificates with the following columns: Issued To, Issued By, Expiration Date, and Intended Purposes.

Issued To	Issued By	Expiration Date	Intended Purposes
172ac9ba-8ad1-4f07-a0ce-e27b3fa67812	MS-Organization-Access	11/15/2031	Client Authentication
russo.richard.m.V. ORC302000013.ID	WidePoint ECA 8 Dev	2/19/2025	Client Authenticati...

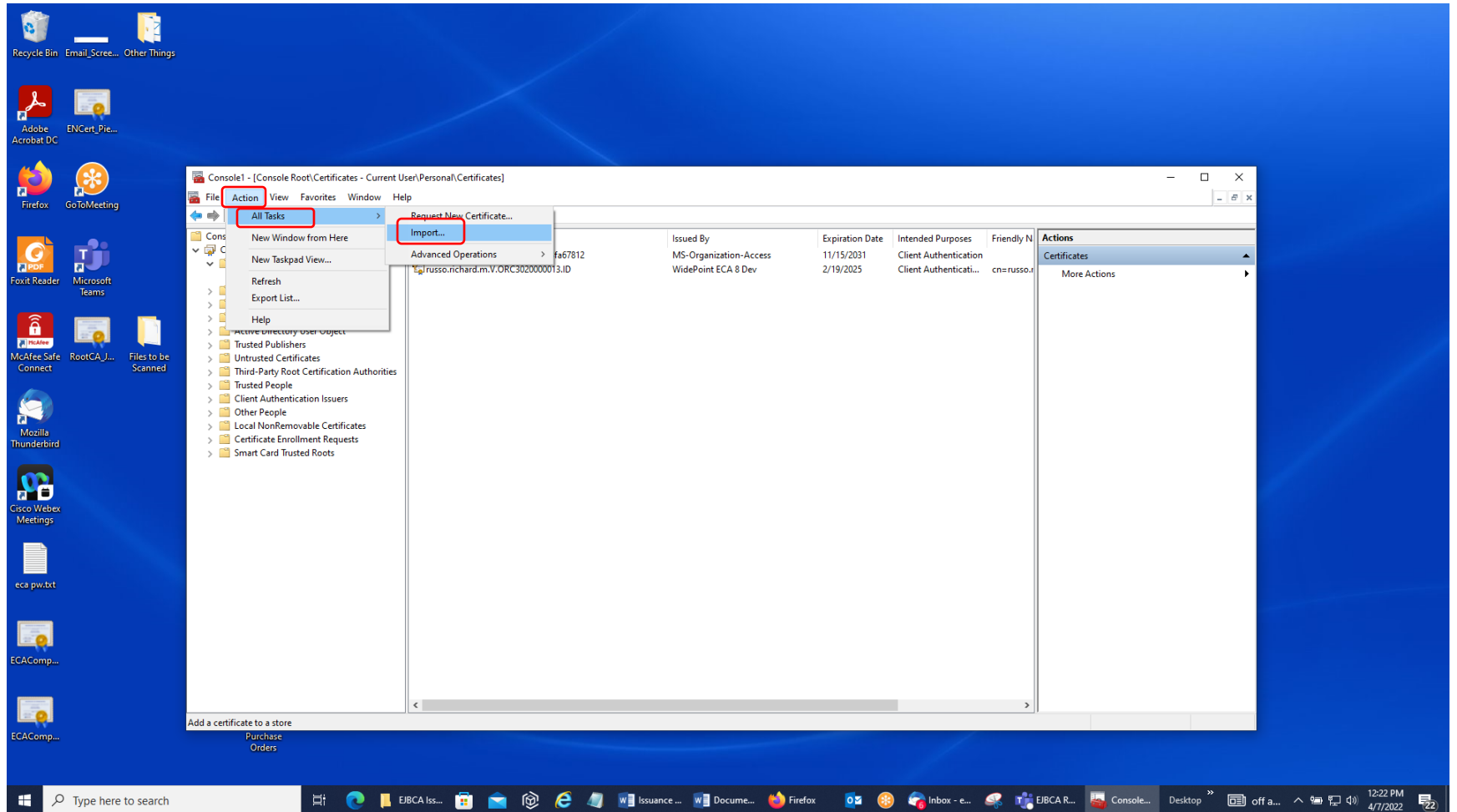
A red box highlights the 'WidePoint ECA 8 Dev' value in the 'Issued By' column of the second row. A blue arrow points from a text box below to this value.

Your NEWLY issued certificates will say Issued By WidePoint ECA 8 and **NOT** WidePoint ECA 8 **Dev** as the example above says!

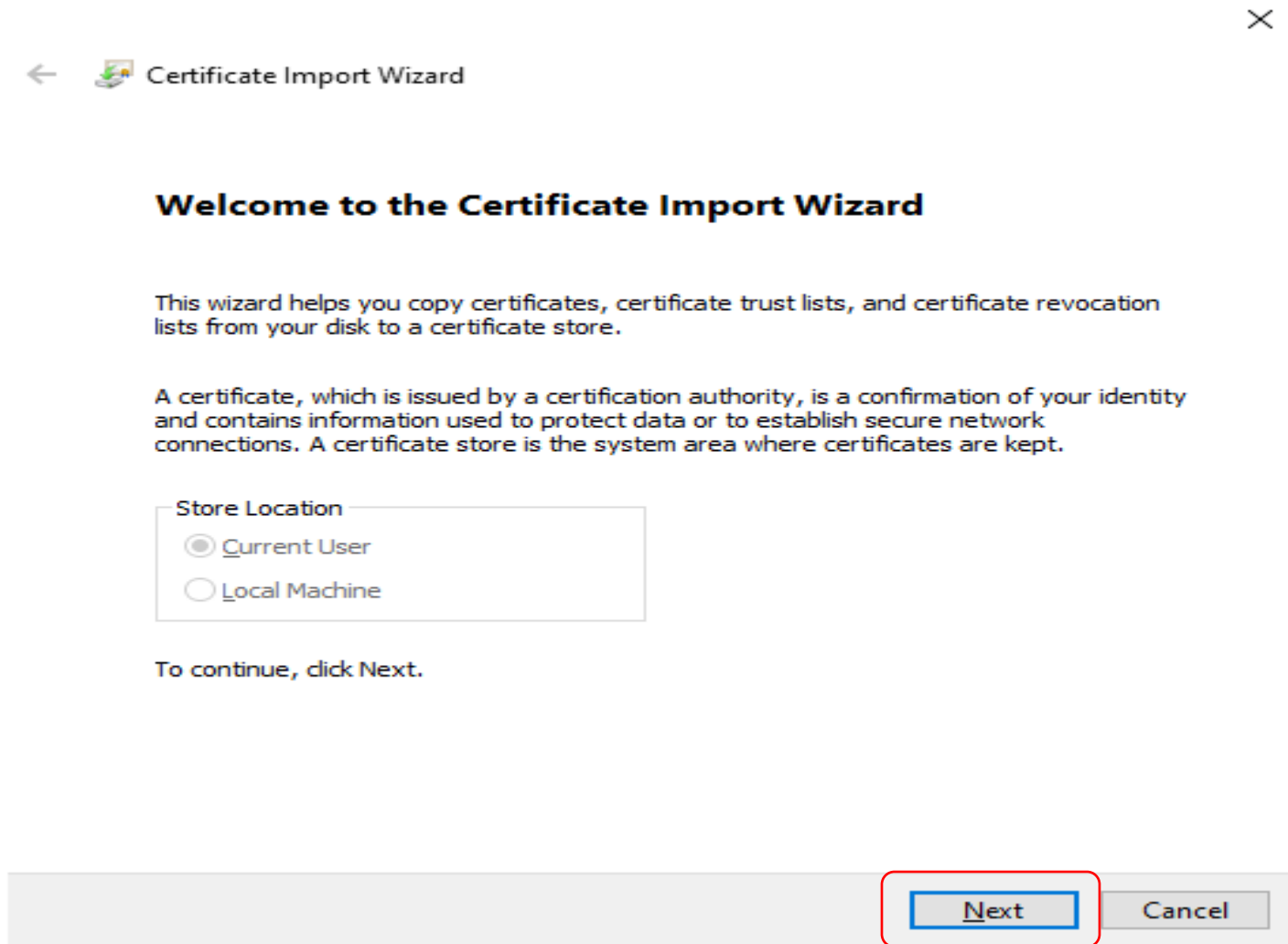
30. Repeat the process for the encryption certificate. Re-highlight the Certificates Sub-Folder under the Personal Folder in the left margin.



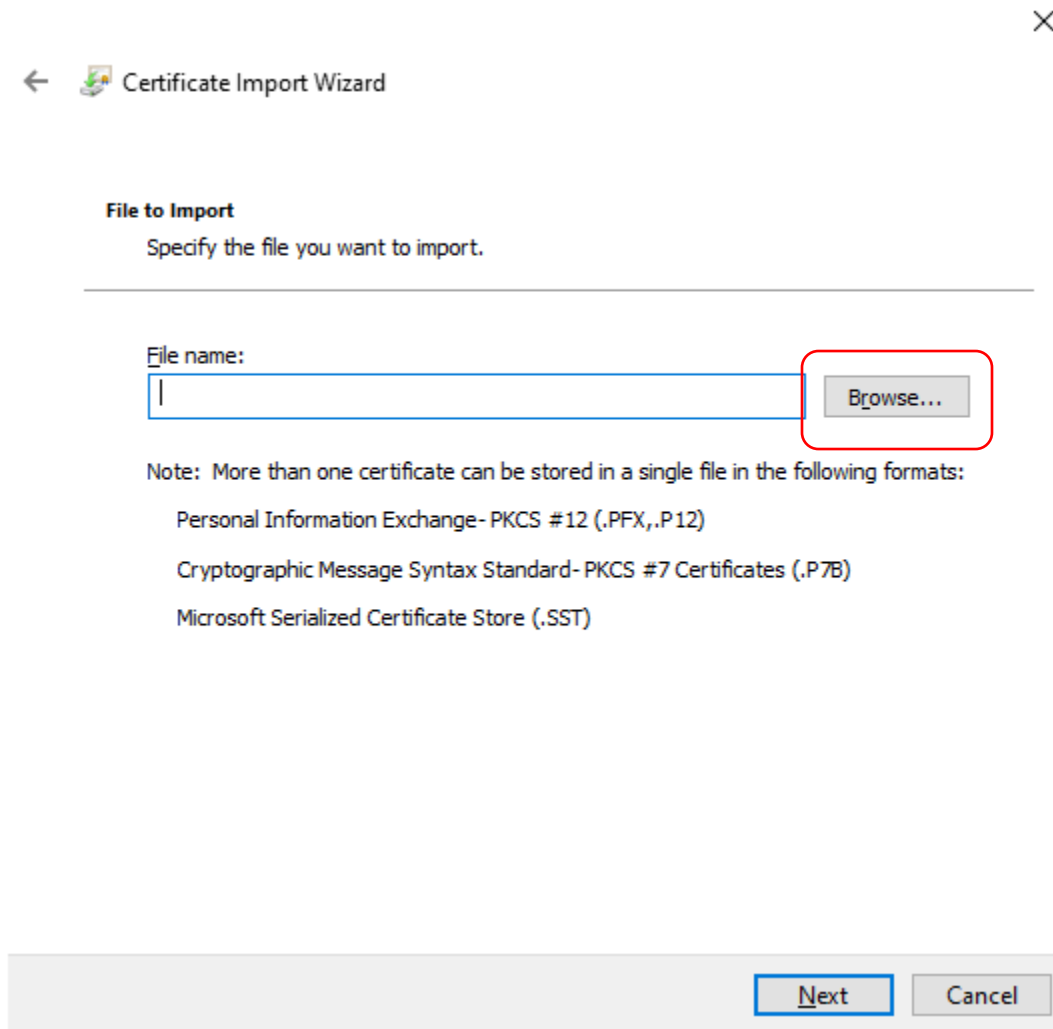
31. Then, click on 'Action' in the Menu Bar, then click on 'All Tasks' in the list, and then click on the 'Import' Selection.



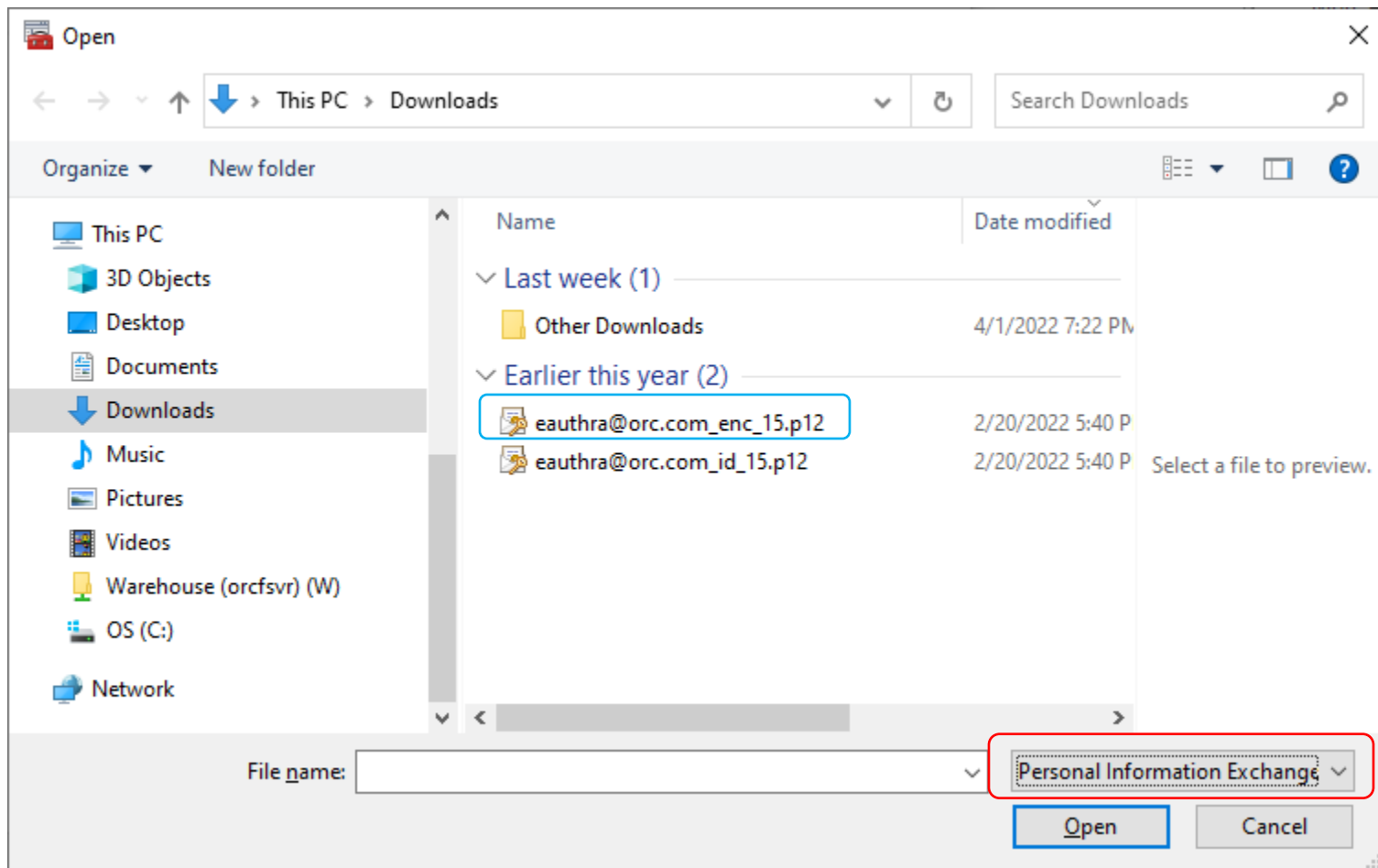
32. Then select 'Next' on the 'Certificate Import Wizard' Screen.



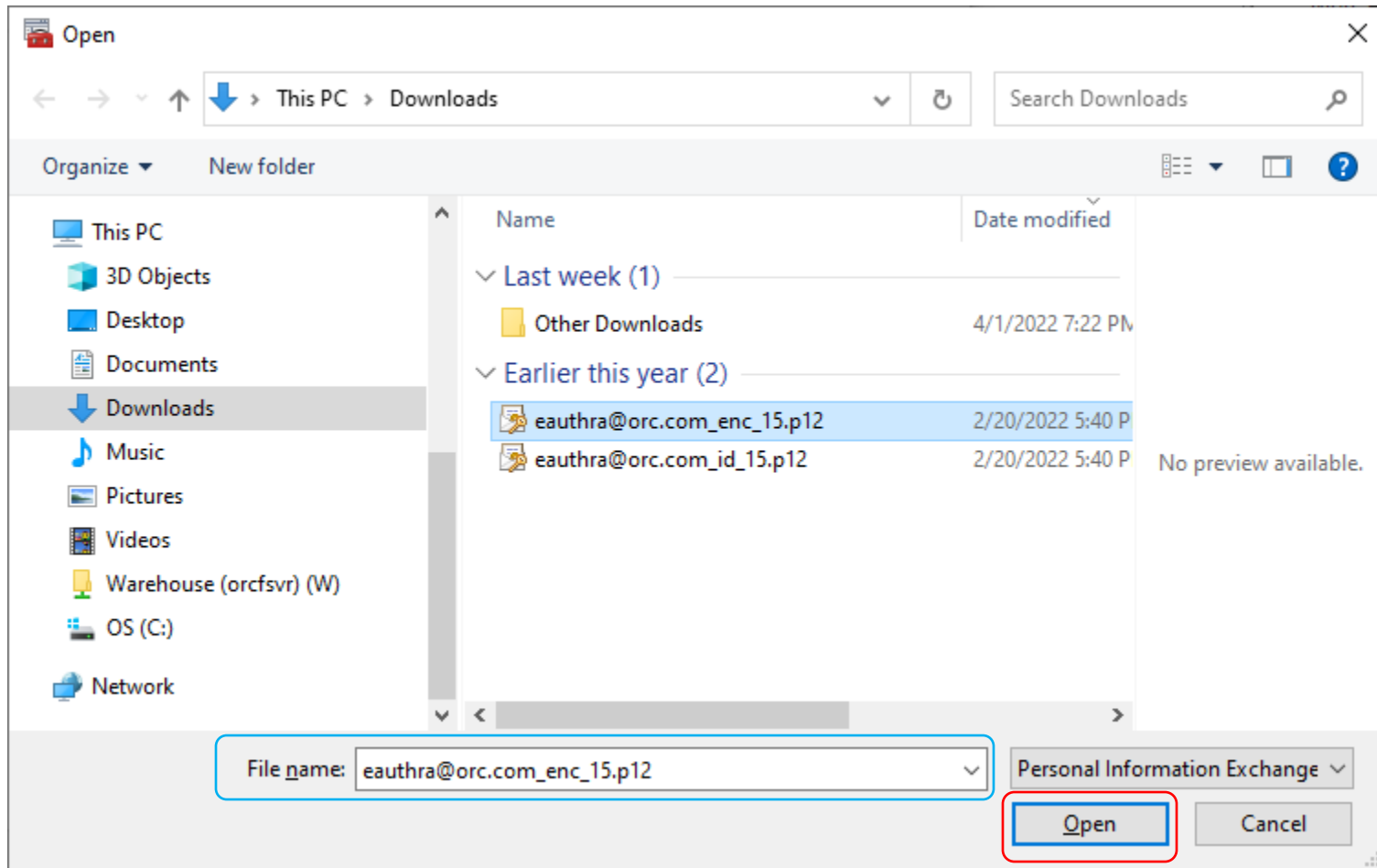
33. Select the 'Browse' Button on the 'File to Import' Screen.



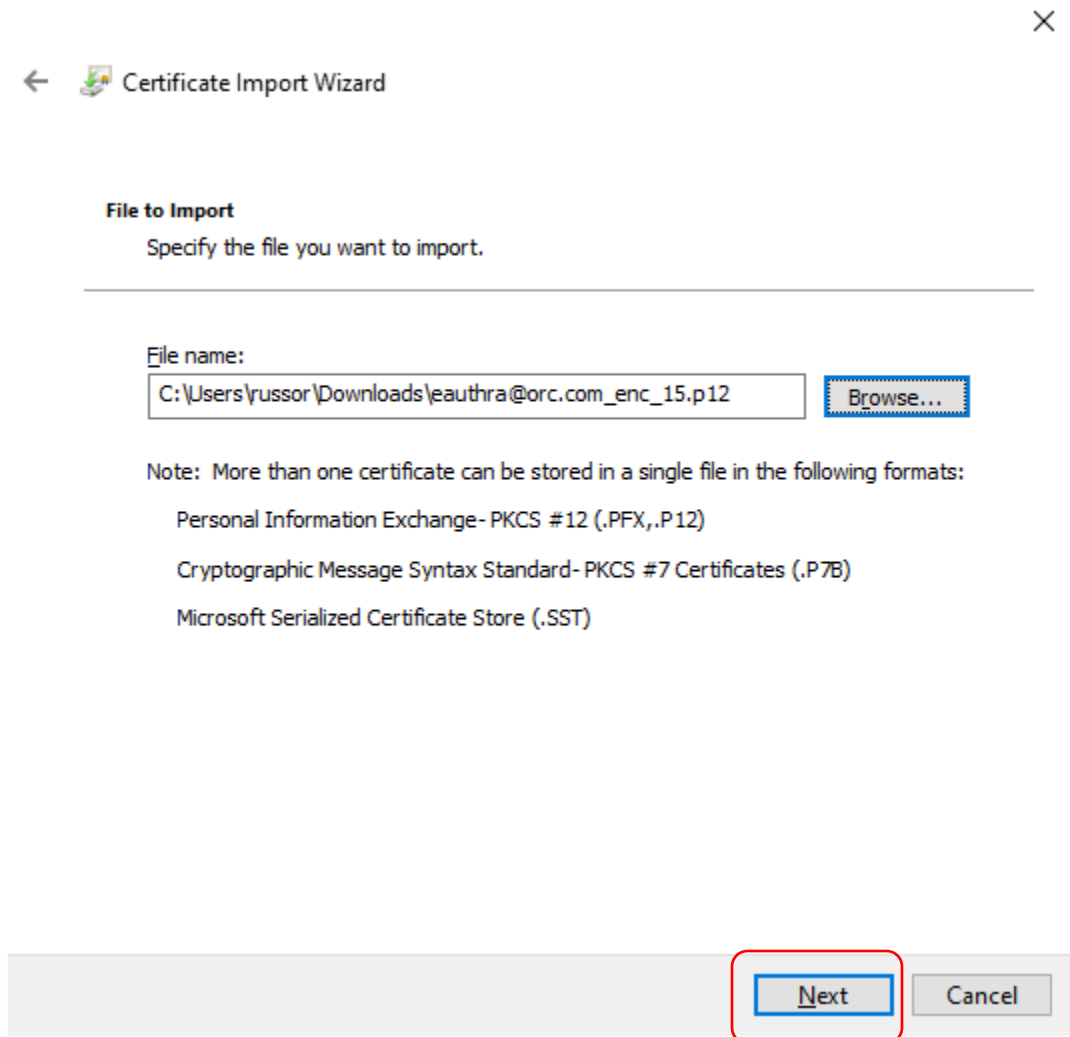
34. Change file type from X.509 Certificate to Personal Information Exchange in the bottom, right-hand corner of the screen and then highlight your new encryption certificate file.



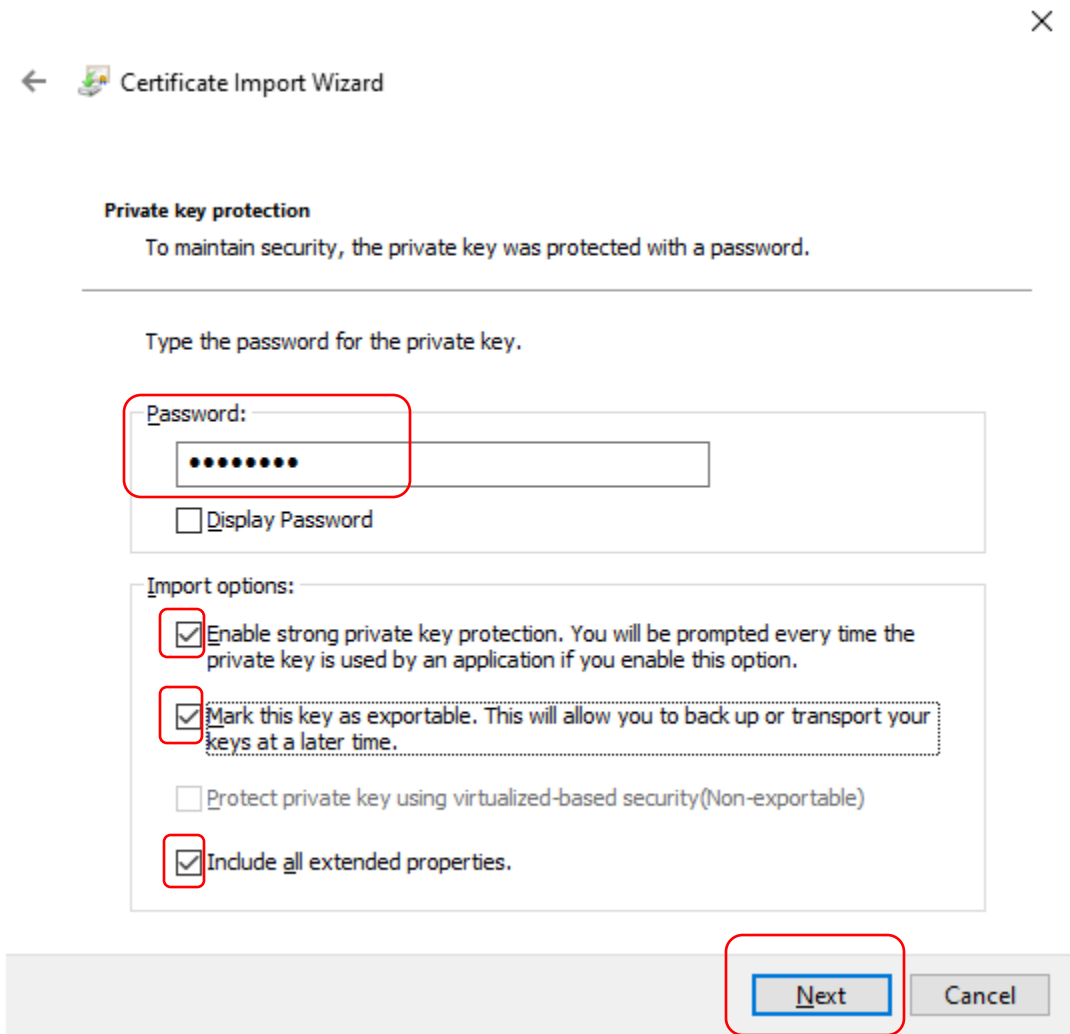
35. When it appears in the 'File name' Box at the bottom of the screen, click on the 'Open' Button.



36. When you go back to the 'File to Import' Screen below, click 'Next.'



37. Paste your password from the Notepad File into the 'Password' Box. Check the first, second, and fourth 'Import options' Boxes. Then, click 'Next.'



The image shows a screenshot of the 'Certificate Import Wizard' dialog box. At the top right, there is a close button (X). Below the title bar, there is a back arrow and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the text: 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a 'Password:' label next to a text input field containing ten dots. Below the input field is a checkbox labeled 'Display Password'. Underneath is the 'Import options:' section with four checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', 'Protect private key using virtualized-based security(Non-exportable)', and 'Include all extended properties.' At the bottom right, there are two buttons: 'Next' and 'Cancel'. Red boxes highlight the 'Password:' label, the password input field, the first, second, and fourth checkboxes, and the 'Next' button.

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: [.....]

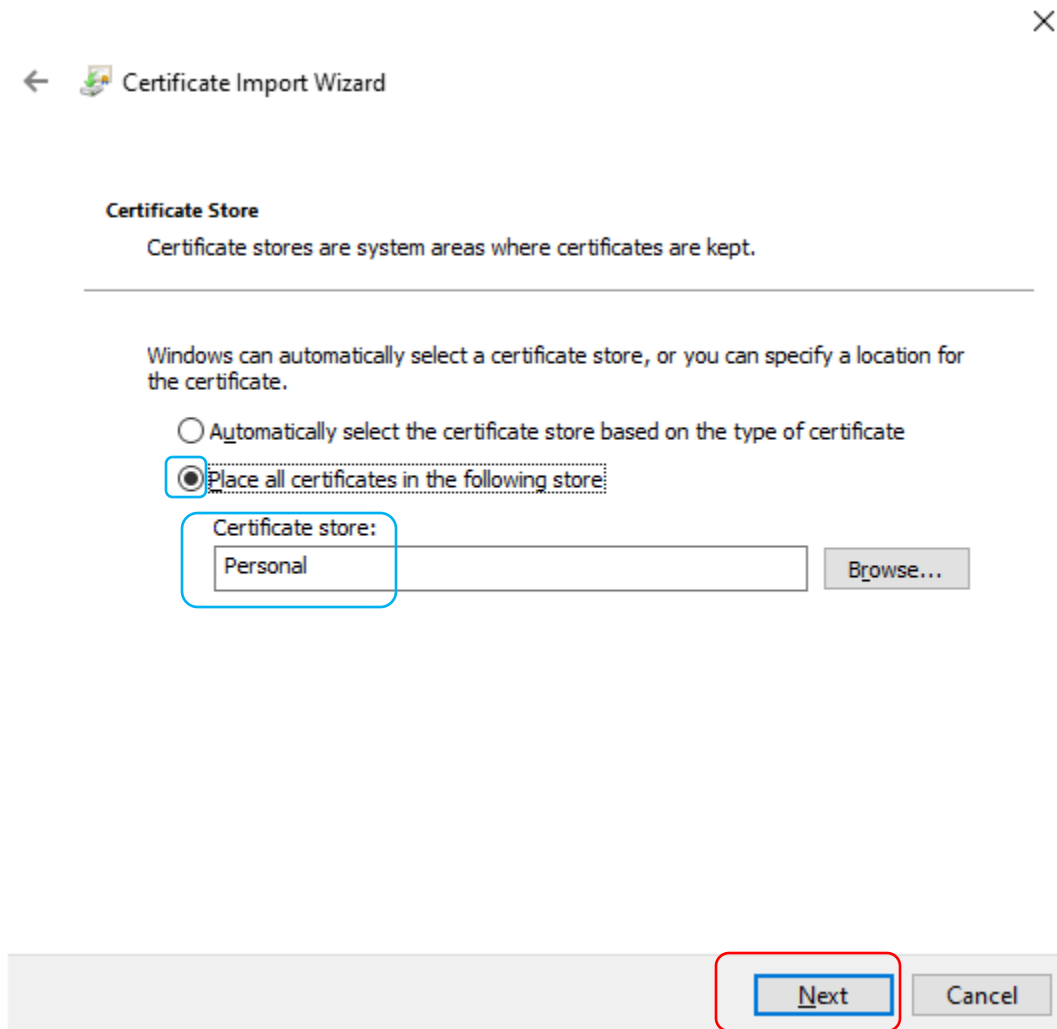
Display Password

Import options:

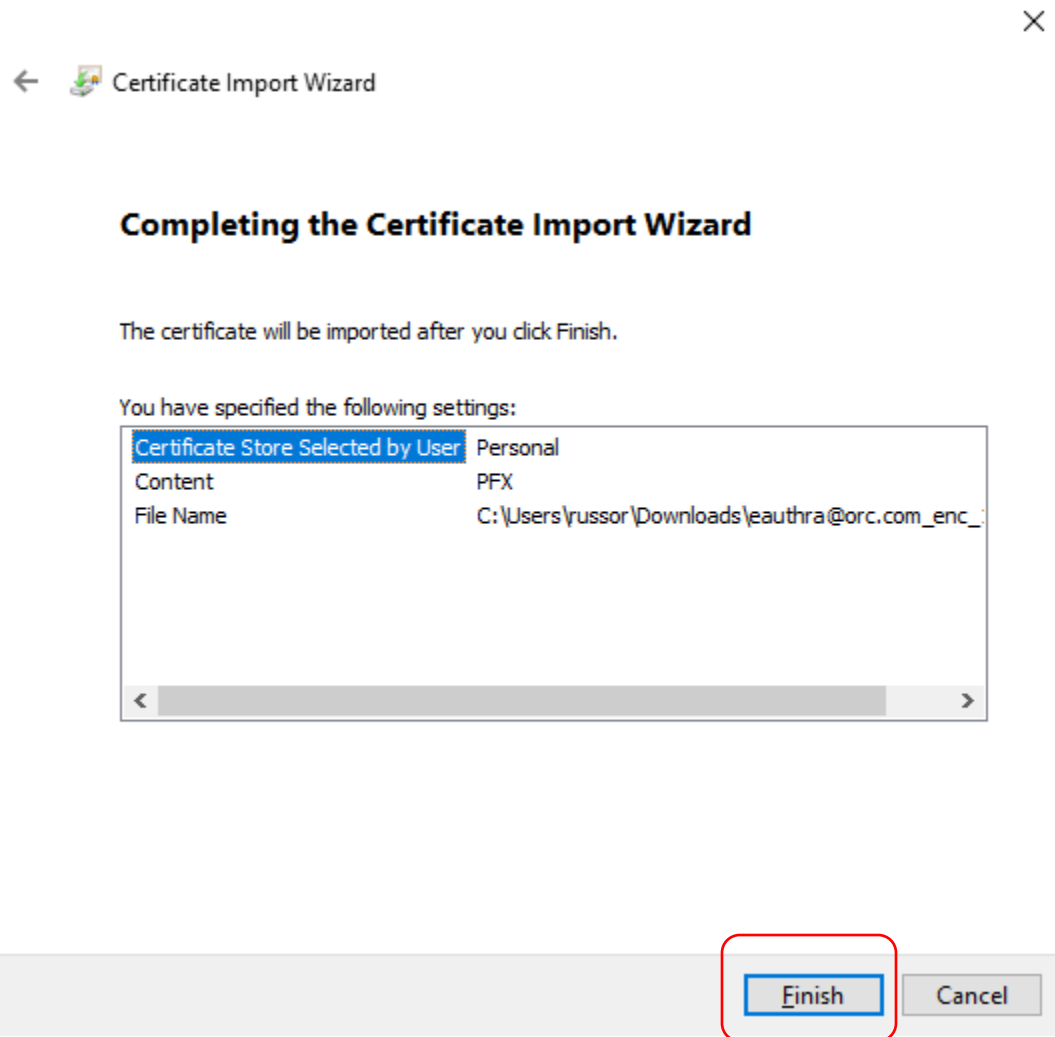
- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Protect private key using virtualized-based security(Non-exportable)
- Include all extended properties.

Next Cancel

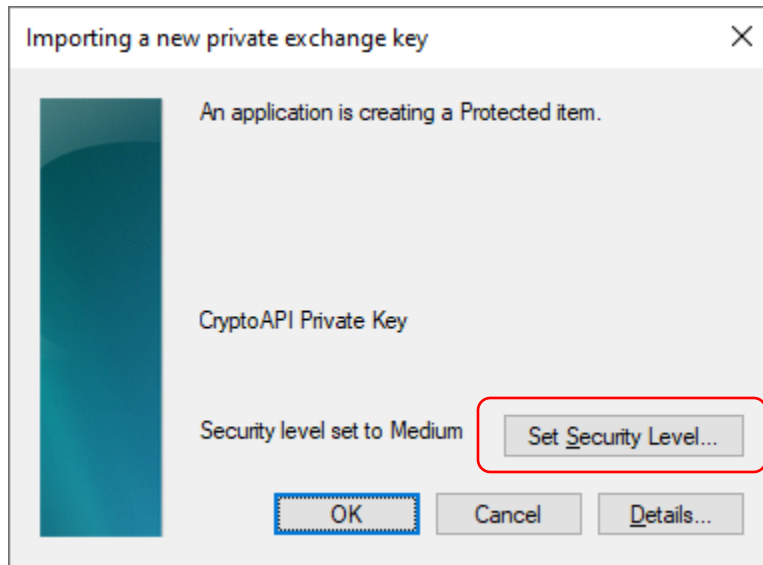
38. Make sure the radio button for 'Place all certificates in the following store' is selected and that 'Personal' is in the 'Certificate store' Box. Then, click 'Next.'



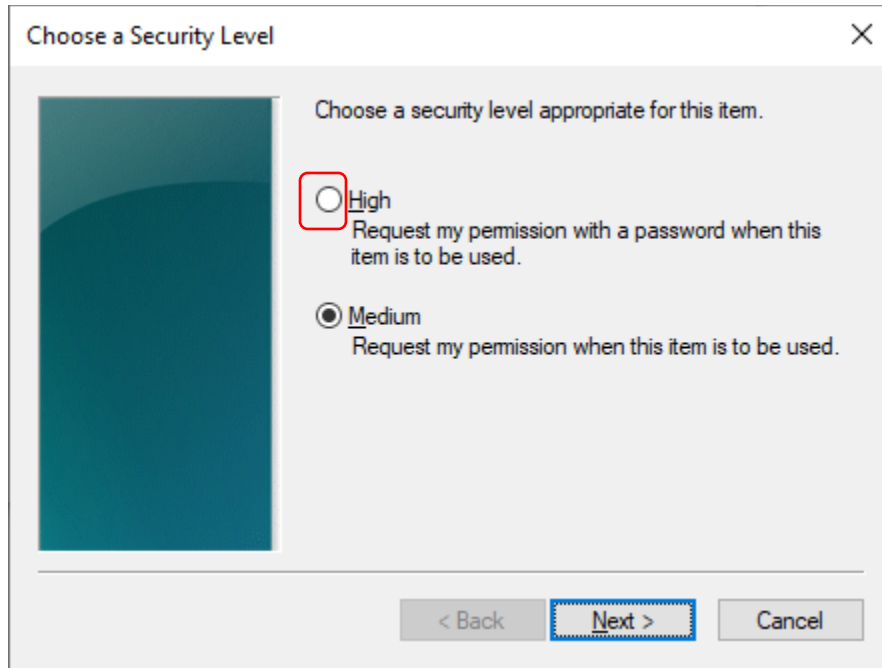
39. Click 'Next' in the screen below.



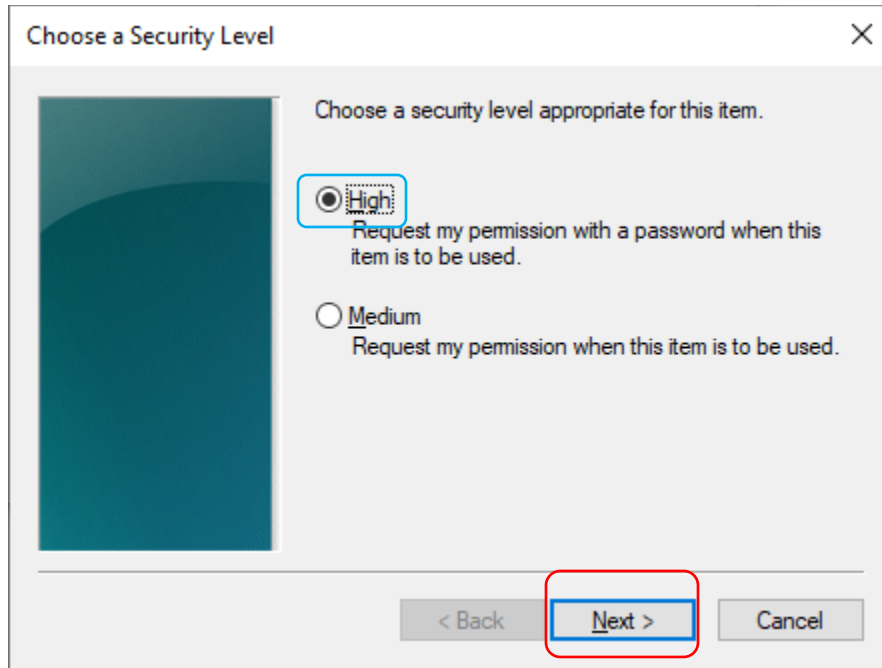
40. The 'Importing a new private exchange key' Screen will appear with the 'Security level set to Medium.' Click on the 'Set Security Level' Button.



41. Change the Security Level from Medium to High by selecting the top radio button.



42. Then click 'Next.'



43. Paste your password into both boxes from the Notepad File and click 'Finish.'

Create a Password

Create a password to protect this item.

Create a new password for this item.

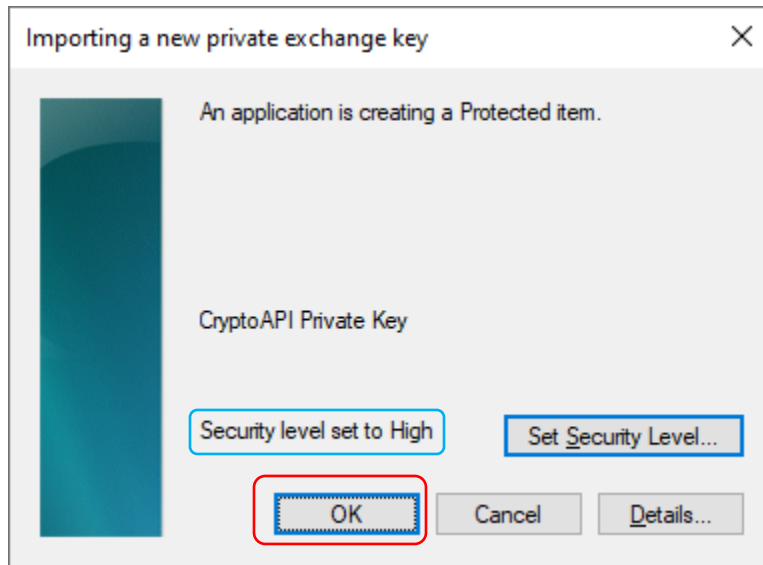
Password for:

Password:

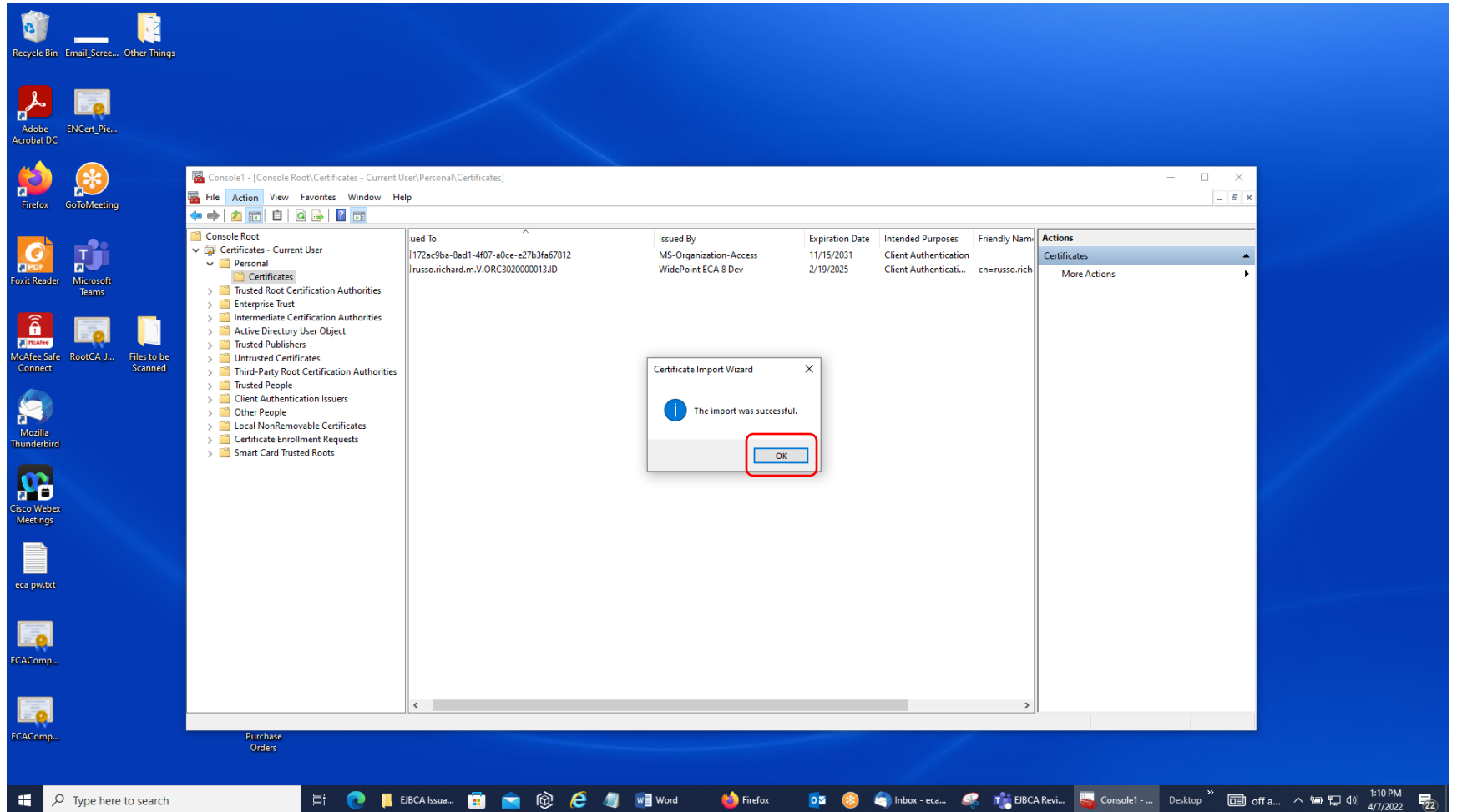
Confirm:

< Back Cancel

44. Security level will be set to High. Click 'OK' on the next screen.



45. You should get the response that the import was successful. Click the 'OK' Button.



46. Your encryption certificate will appear in the Center Pane. You may get extra trust chain certificates to appear along with it in that Center Pane; just ignore them.

The screenshot shows the Windows Certificate Manager console window titled "Console1 - [Console Root\Certificates - Current User\Personal\Certificates]". The left pane shows the tree view with "Certificates - Current User" expanded to "Personal" and then "Certificates". The right pane displays a table of certificates:

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
172ac9ba-8ad1-4f07-a0ce-e27b3fa67812	MS-Organization-Access	11/15/2031	Client Authentication	
russo.richard.m.V. ORC3020000013.Encrypt	WidePoint ECA 8 Dev	2/19/2025	Secure Email	russo.richa
russo.richard.m.V. ORC3020000013.ID	WidePoint ECA 8 Dev	2/19/2025	Client Authenticati...	cn=russo.r

A callout box with a blue arrow pointing to the "WidePoint ECA 8 Dev" entry in the "Issued By" column contains the following text:

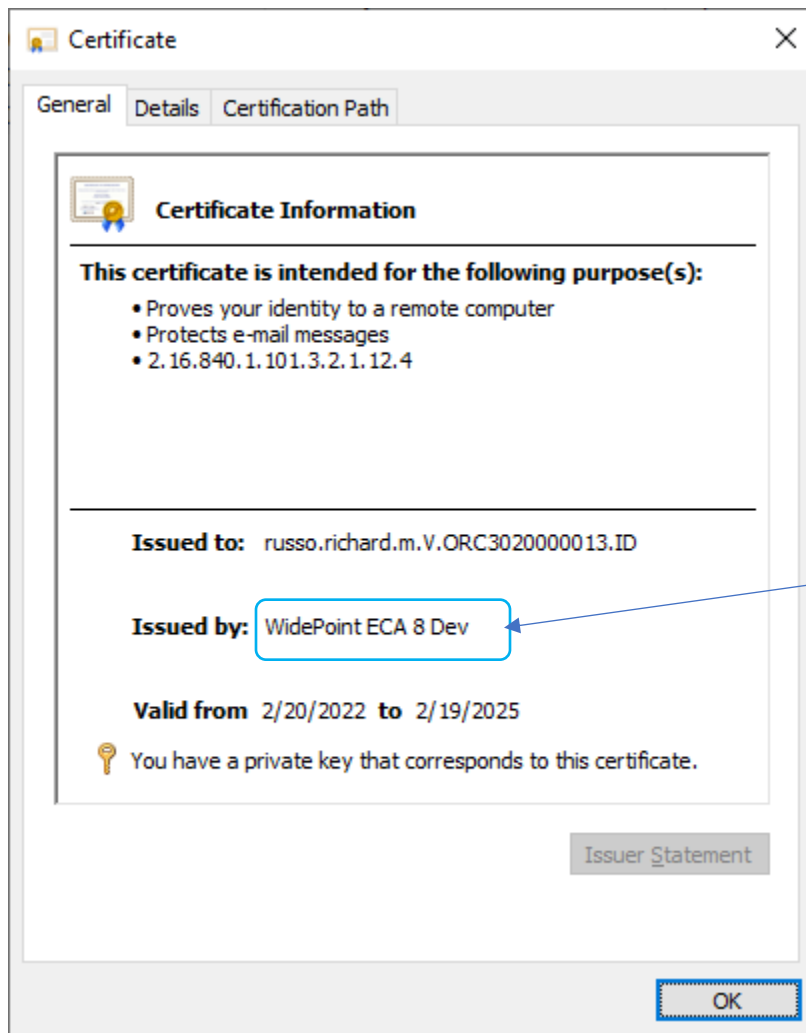
Again, your **NEWLY** issued certificates will be Issued By WidePoint ECA 8 and **NOT** by WidePoint ECA 8 **Dev** as the example above says!

47. Next, select your identity certificate (Issued To ends in .ID).

The screenshot shows the Windows Certificate Manager console. The left pane displays the tree structure under 'Certificates - Current User' > 'Personal' > 'Certificates'. The right pane shows a table of certificates with the following columns: Issued To, Issued By, Expiration Date, Intended Purposes, and Friendly Name. The certificate 'russo.richard.m.V.ORC302000013.ID' is selected.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
172ac9ba-8ad1-4f07-a0ce-e27b3fa67812	MS-Organization-Access	11/15/2031	Client Authentication	
russo.richard.m.V.ORC302000013.Encrypt	WidePoint ECA 8 Dev	2/19/2025	Secure Email	russo.richard.m.V.O...
russo.richard.m.V.ORC302000013.ID	WidePoint ECA 8 Dev	2/19/2025	Client Authenticati...	cn=russo.richard.m...

48. Double-left click the mouse button on that identity certificate to open it up. Your screen should like this, except for Issued To, Issued By, and Validity Dates.



Again, your certificate will say Issued By WidePoint ECA 8 and **NOT** WidePoint ECA 8 **Dev!!!**