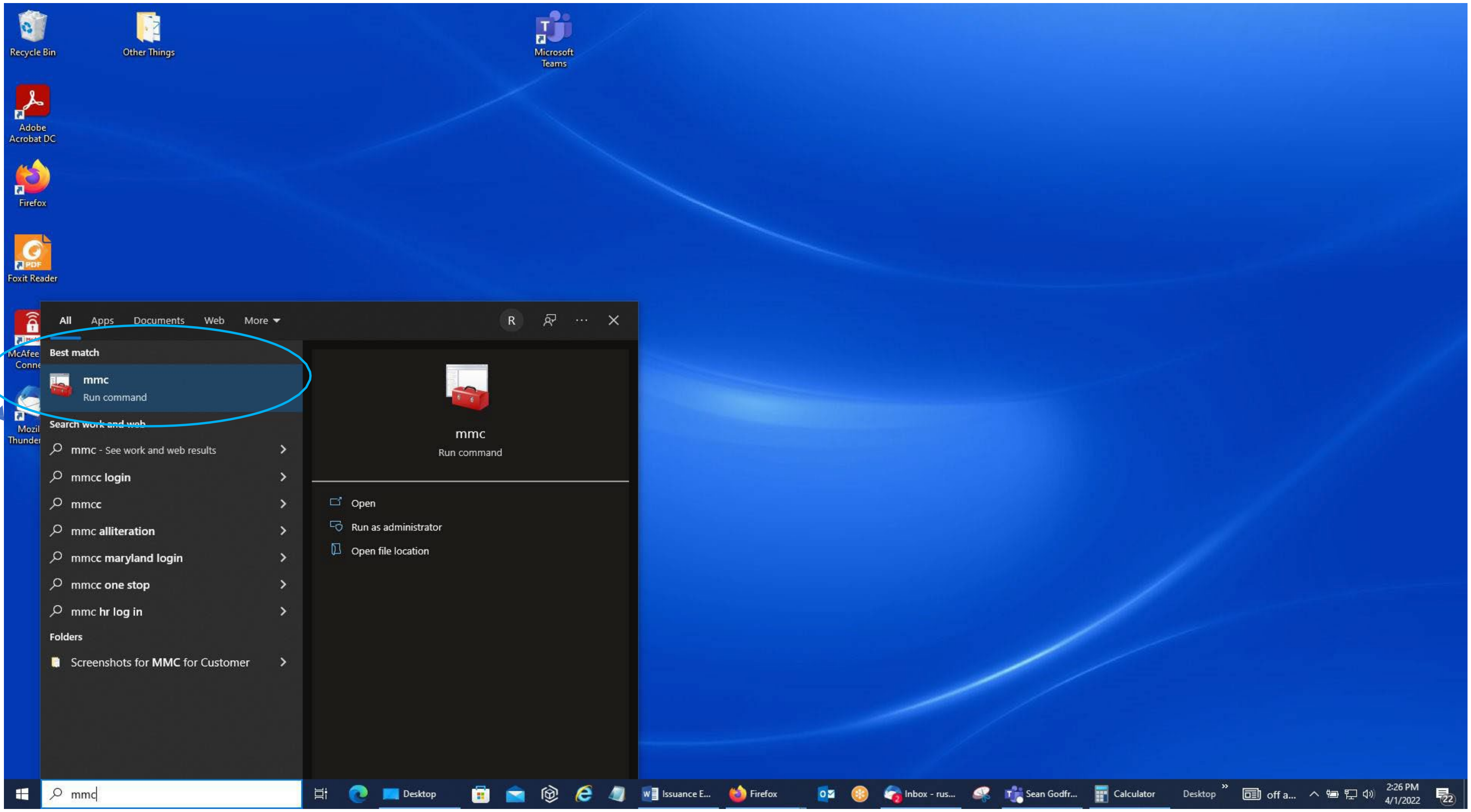
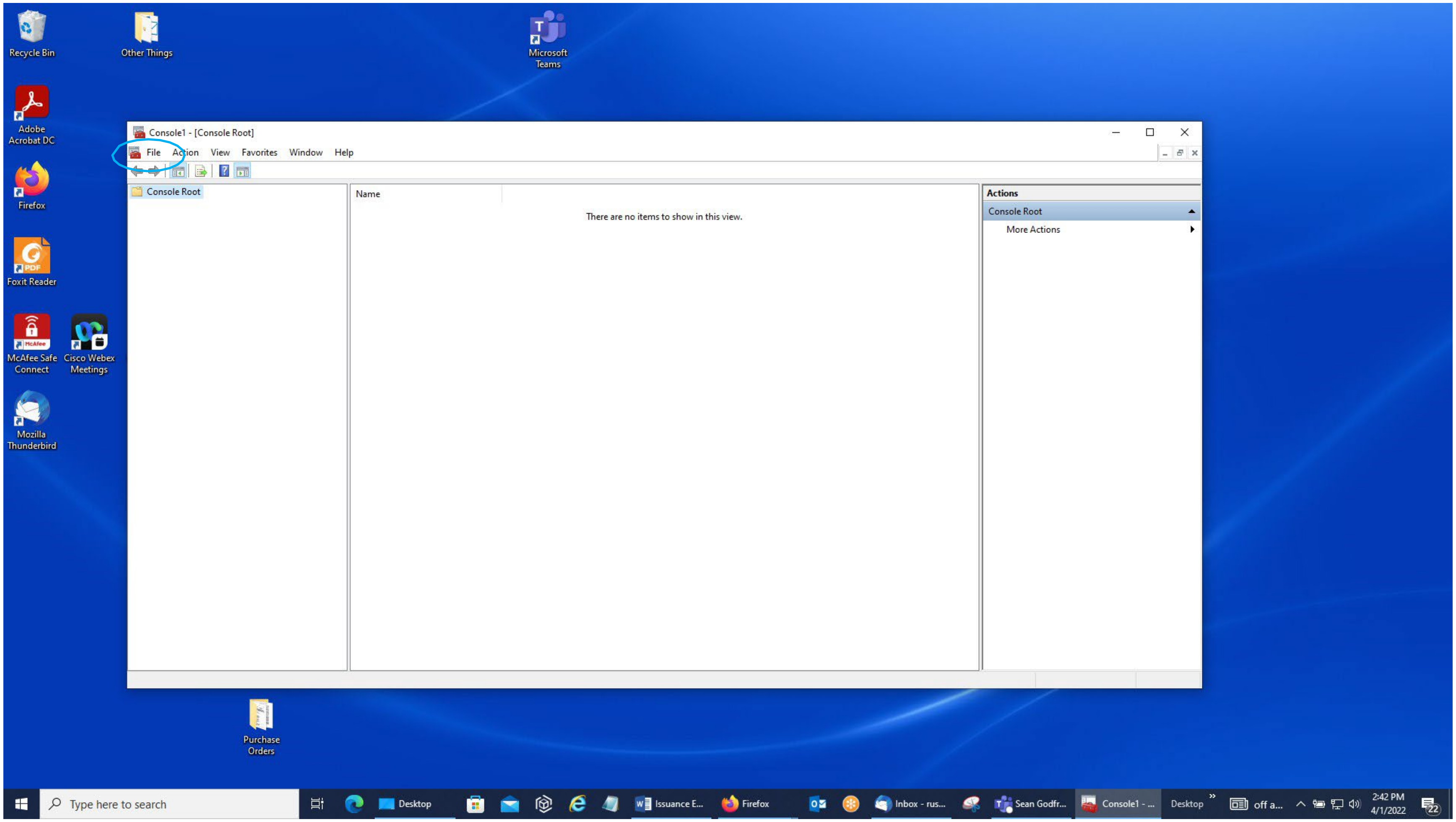
1. Access the Microsoft Management Console (MMC) for your profile on this PC (you may need admin permissions from your IT Department to do this).



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

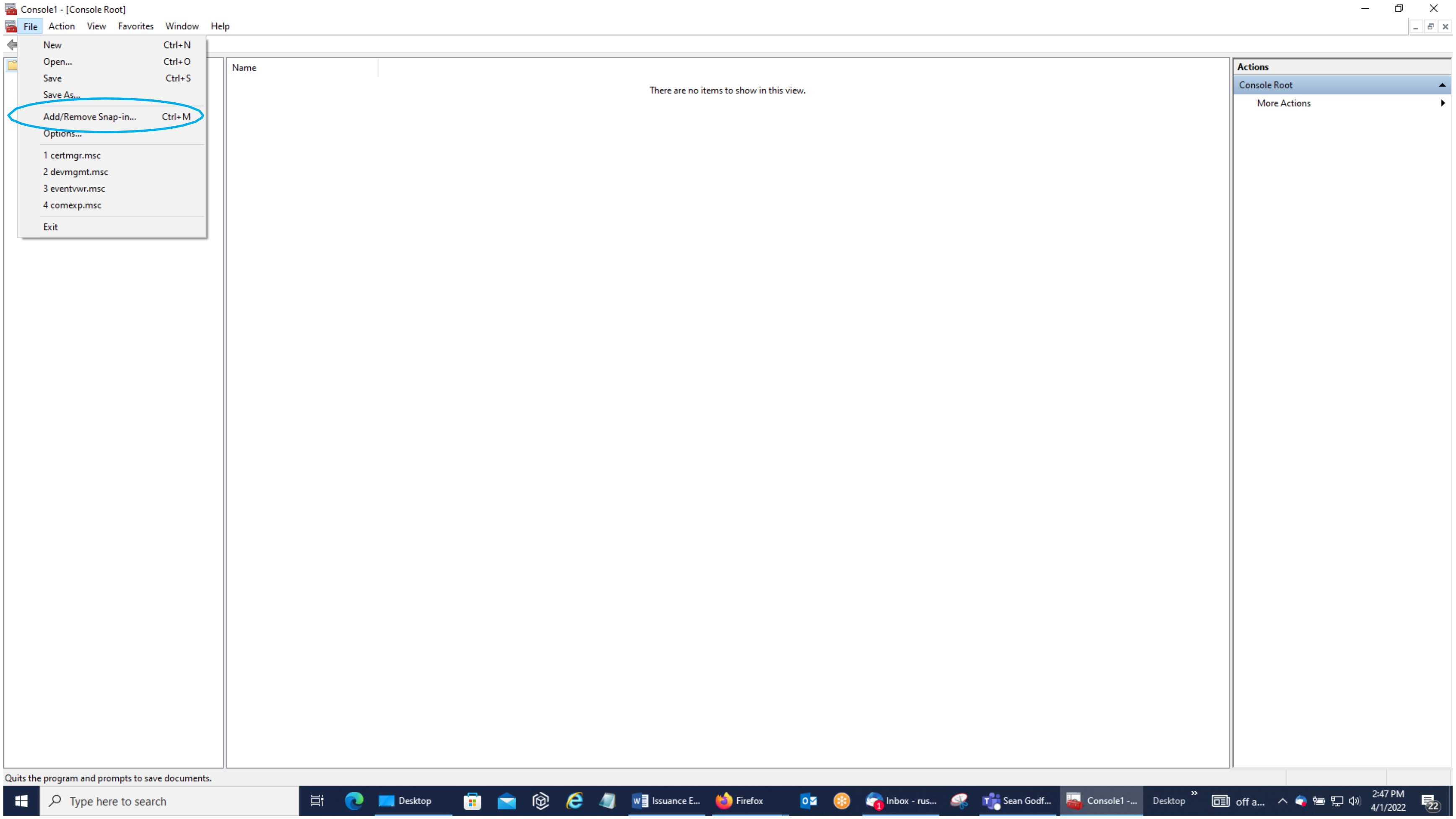
2. You may get a User Account Control Screen that will ask you if you want to allow this app to make changes to your device; it will have Microsoft Management Console listed. Click ‘Yes’ to open up the MMC for your profile on your PC.

3. You should then get the Console 1 – Console Root Screen below. Click on the word ‘File’ in the Menu Bar.



There are no items to show in this view.

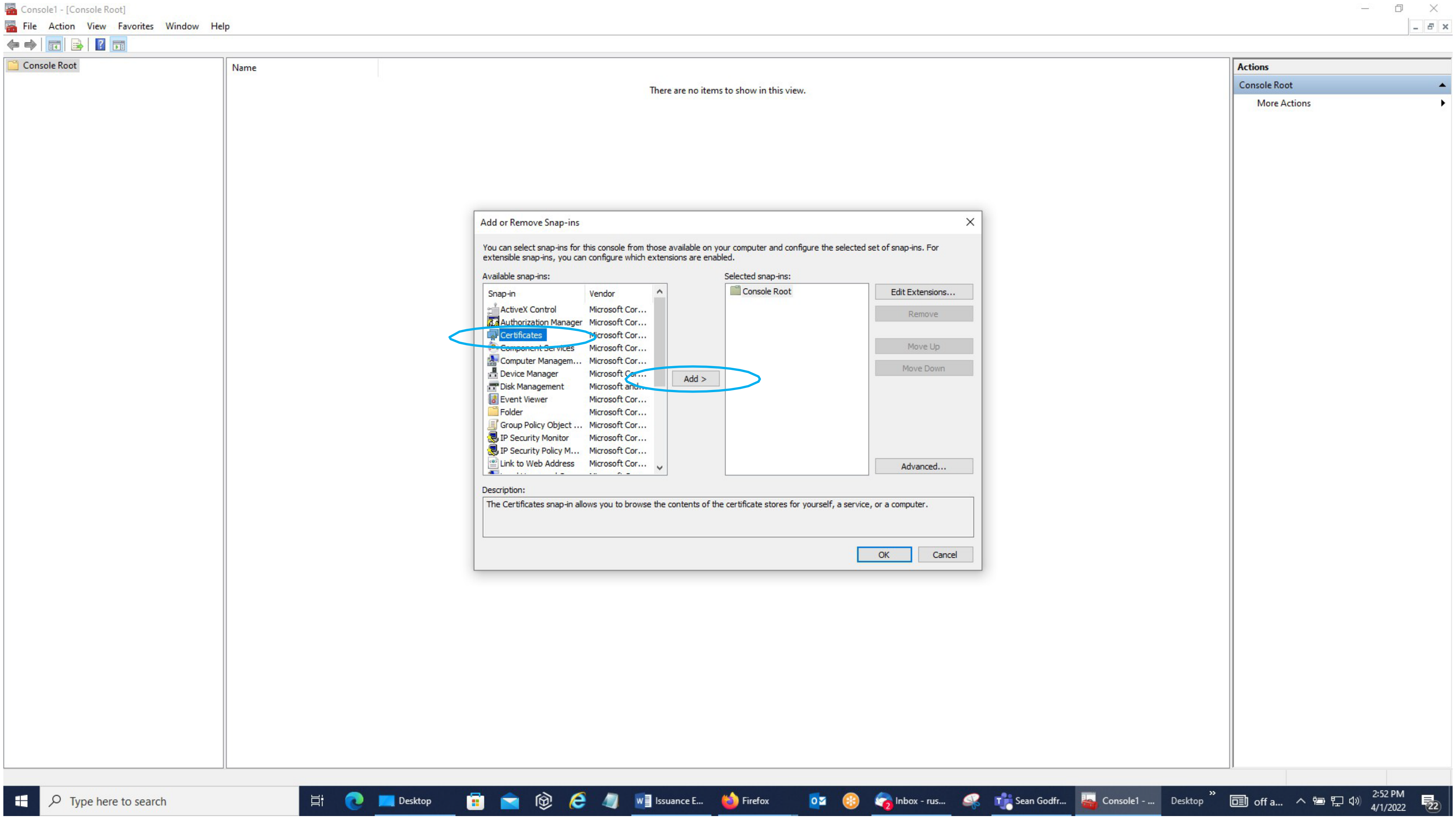
4. Select ‘Add/Remove Snap-in’ from the list.



There are no items to show in this view.

Quits the program and prompts to save documents.

5. 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.



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

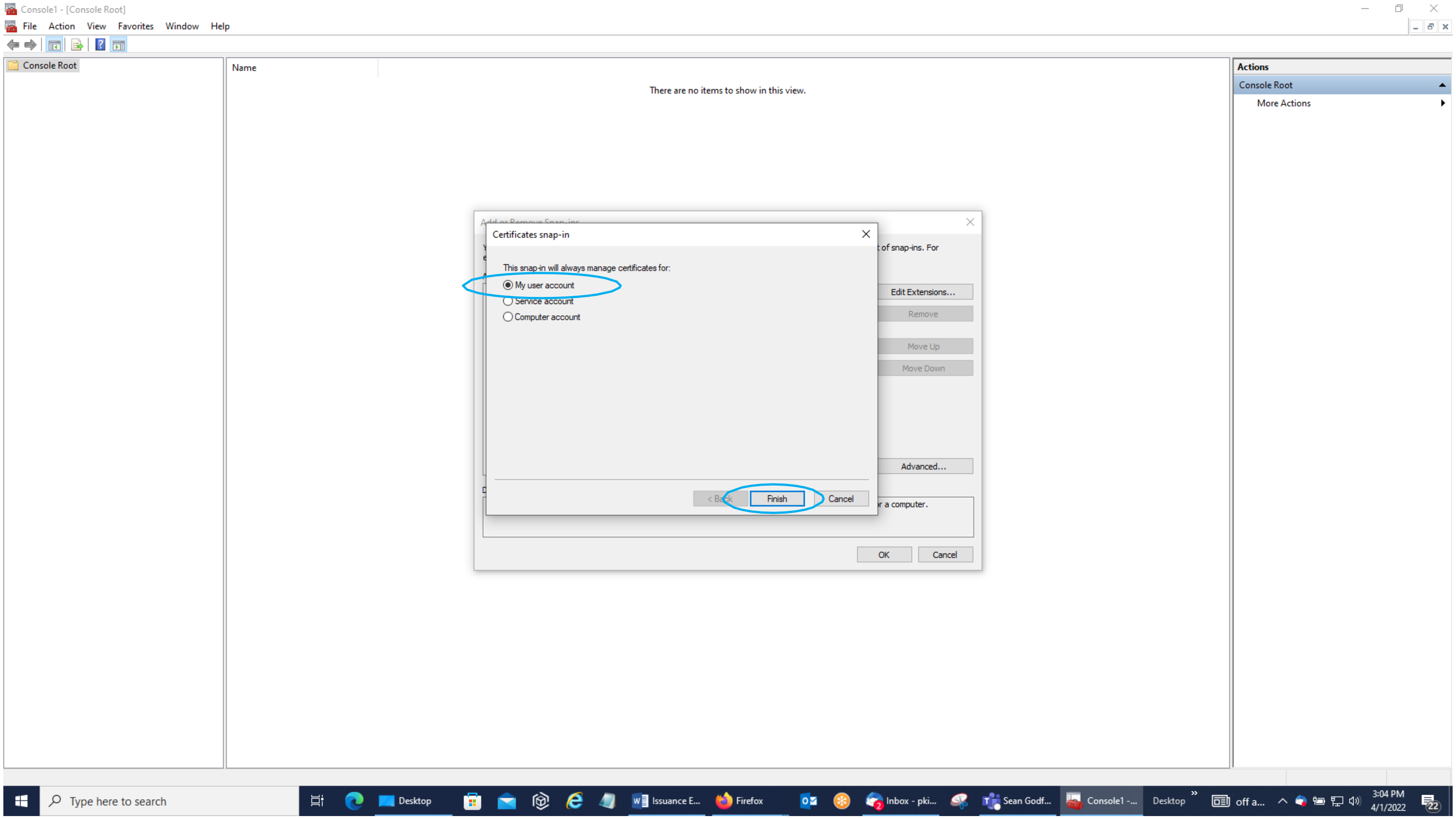
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

6. 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.)

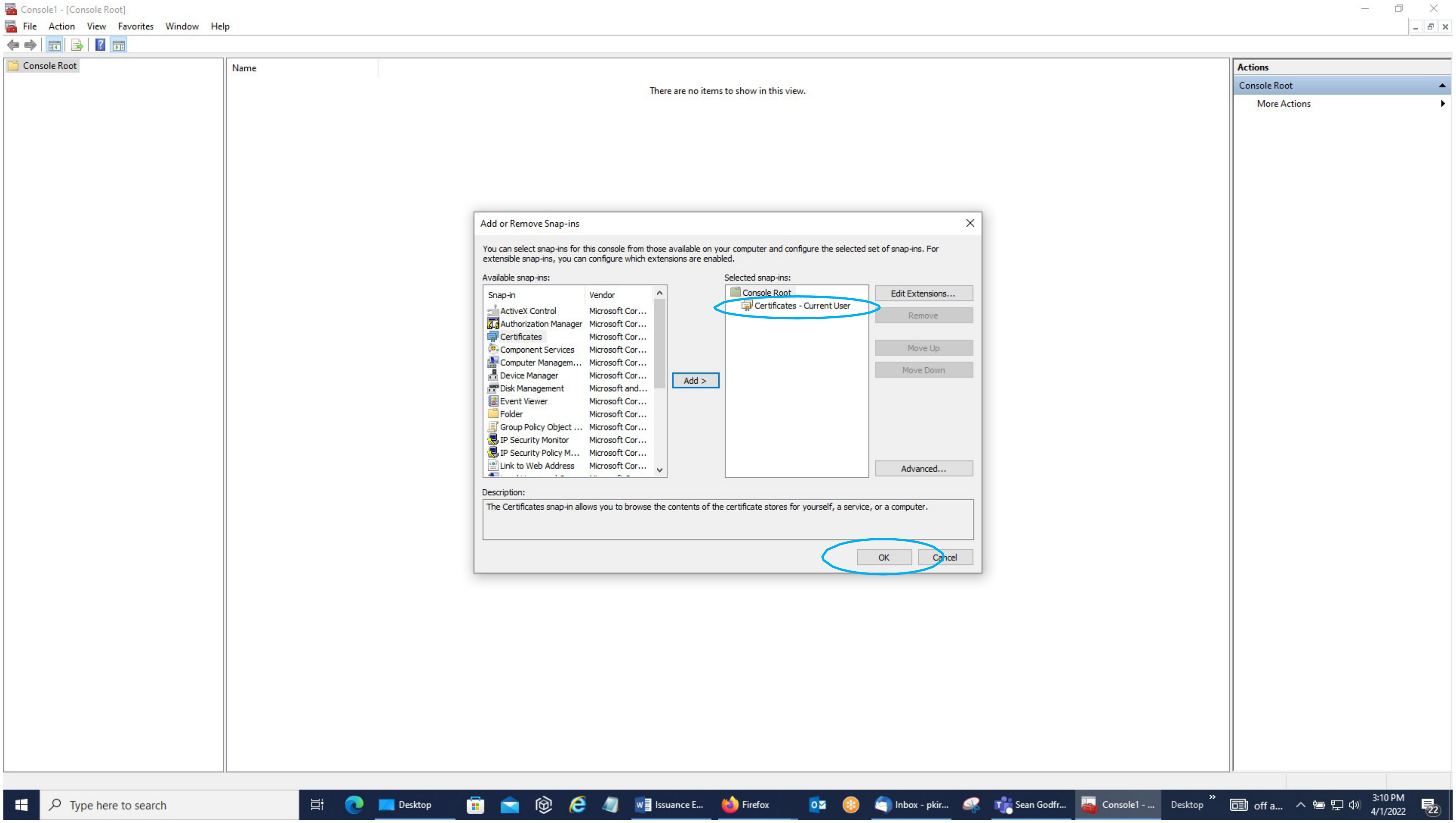


Certificates snap-in

This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

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



There are no items to show in this view.

Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

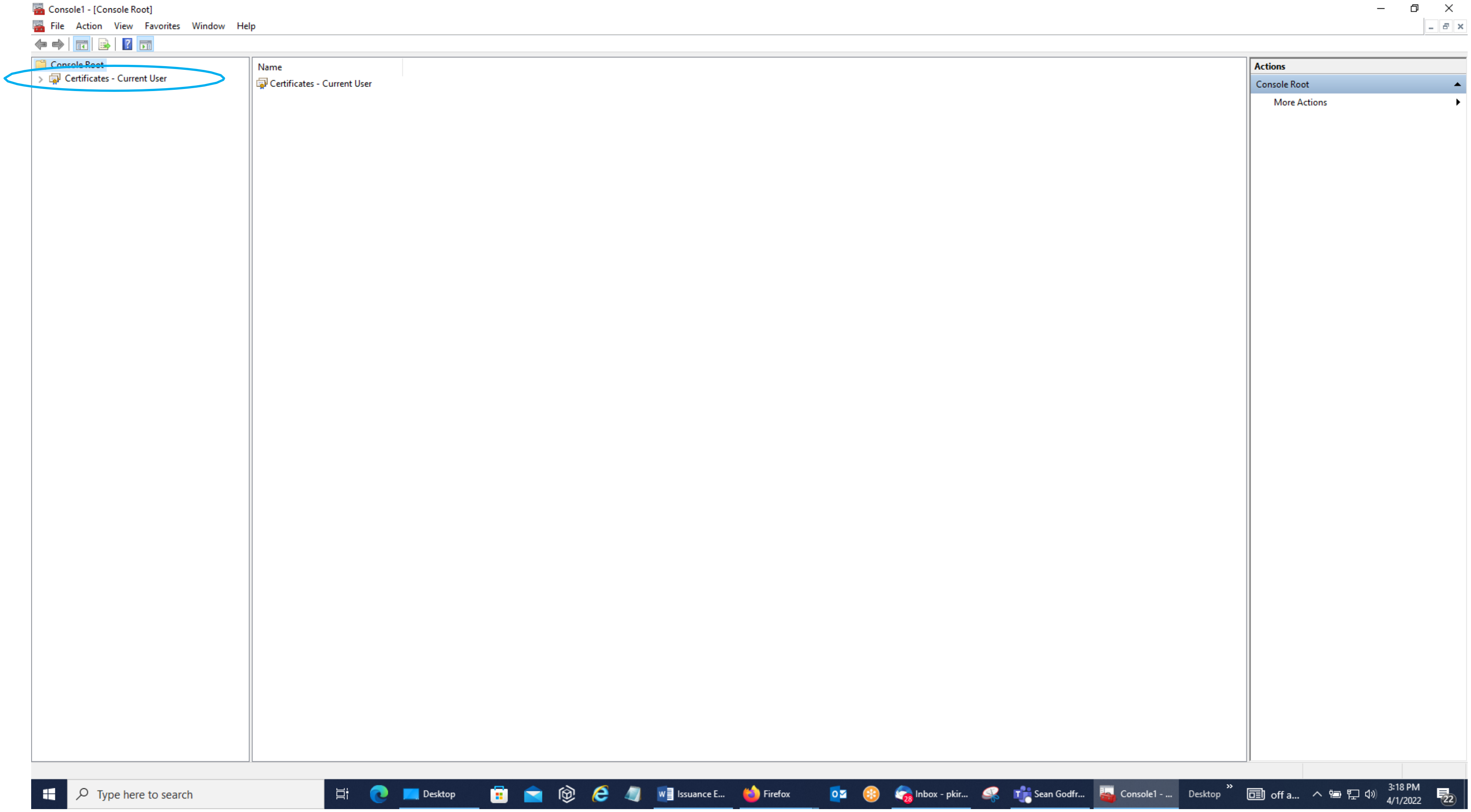
Selected snap-ins:

Console Root
Certificates - Current User

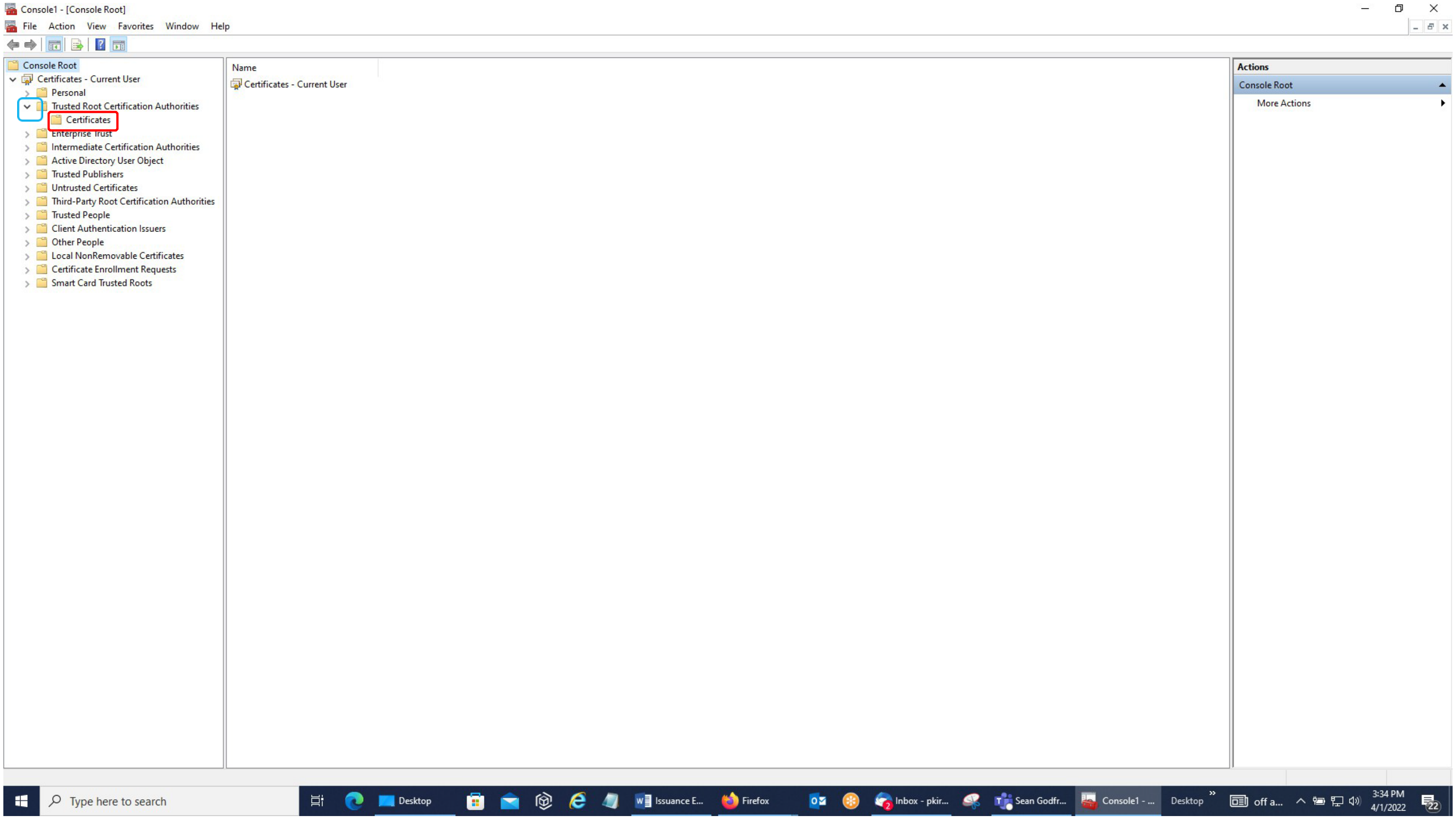
Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

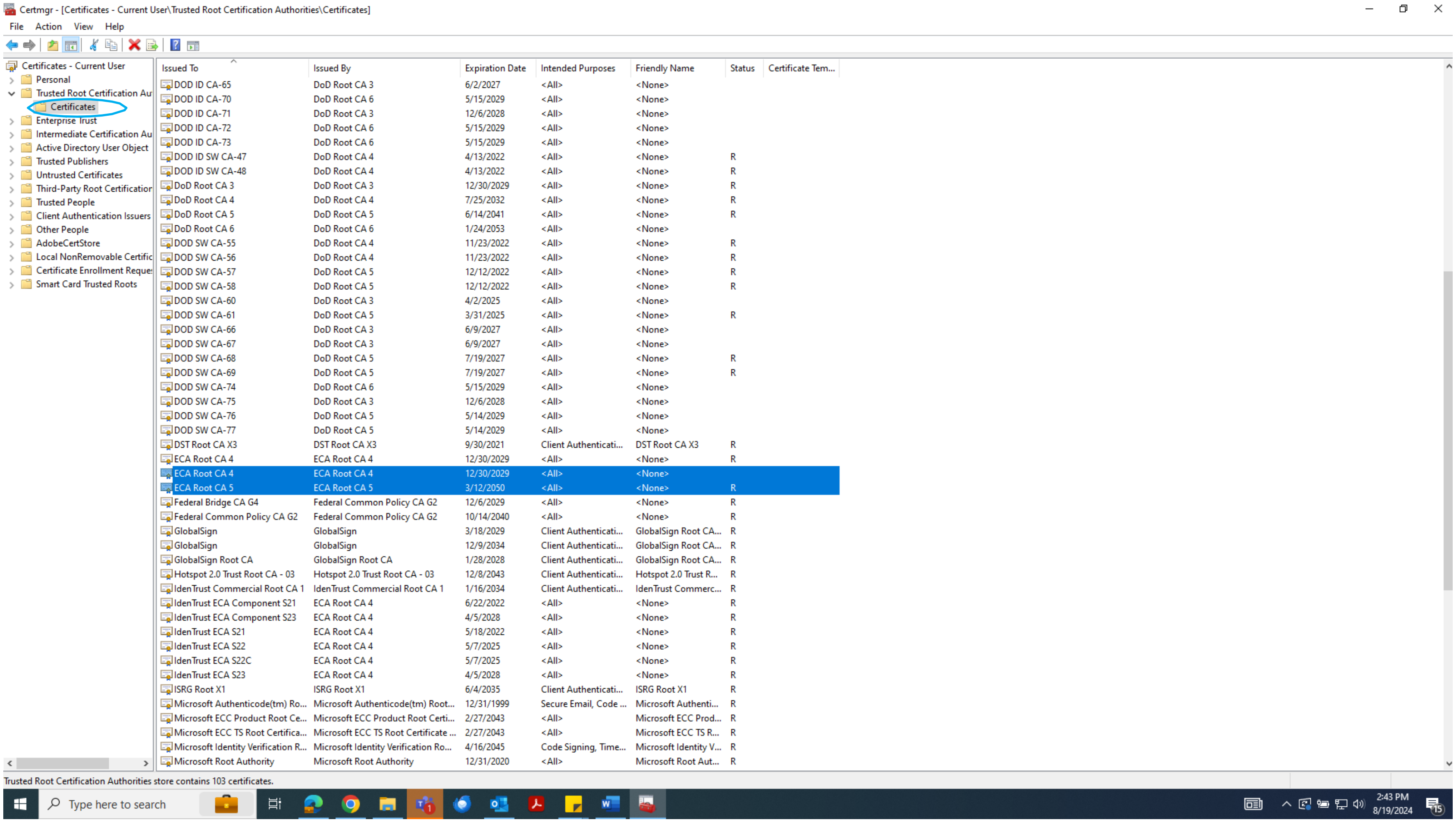
8. You should then come back to the main Console 1 – Console Root Screen with the 'Certificates – Current User' Line under the Console Root Folder in the left-side window pane. Click on the arrow or hash mark in front of that line to display the list of folders within that group.



9. Open up the Trusted Root Certification Authorities Folder by clicking on the arrow or hash mark (blue outlined box) and then double-click the left mouse button on the Certificates Sub-Folder (red box).



10. In the Center Pane of that Screen, you will see the Trusted Root Certification Authorities Certificates that are currently loaded in your Windows Certificate Store. You need to see the two lines in the center pane where it says Issued To ECA Root CA 4, Issued By ECA Root CA 4, and Expiration Date 12/30/2029, and Issued To ECA Root CA 5, Issued By ECA Root CA 5, and Expiration Date 3/12/2050.

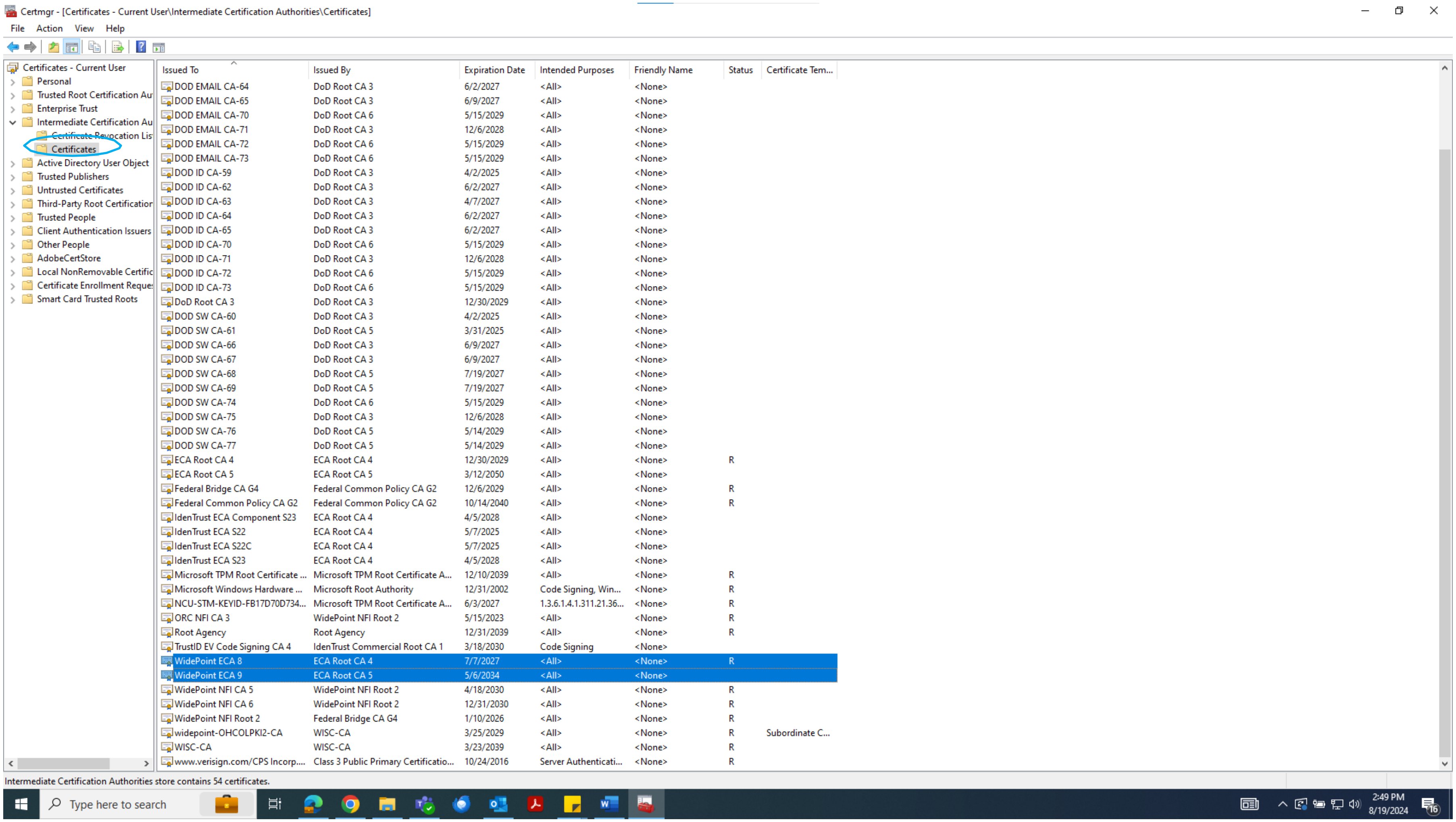

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
AdobeCertStore
Local NonRemovable Certific
Certificate Enrollment Reque:
Smart Card Trusted Roots
Type here to search
2:43 PM
8/19/2024

Certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
DOD ID CA-65	DoD Root CA 3	6/2/2027	<All>	<None>		
DOD ID CA-70	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID CA-71	DoD Root CA 3	12/6/2028	<All>	<None>		
DOD ID CA-72	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID CA-73	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID SW CA-47	DoD Root CA 4	4/13/2022	<All>	<None>	R	
DOD ID SW CA-48	DoD Root CA 4	4/13/2022	<All>	<None>	R	
DoD Root CA 3	DoD Root CA 3	12/30/2029	<All>	<None>	R	
DoD Root CA 4	DoD Root CA 4	7/25/2032	<All>	<None>	R	
DoD Root CA 5	DoD Root CA 5	6/14/2041	<All>	<None>	R	
DoD Root CA 6	DoD Root CA 6	1/24/2053	<All>	<None>		
DOD SW CA-55	DoD Root CA 4	11/23/2022	<All>	<None>	R	
DOD SW CA-56	DoD Root CA 4	11/23/2022	<All>	<None>	R	
DOD SW CA-57	DoD Root CA 5	12/12/2022	<All>	<None>	R	
DOD SW CA-58	DoD Root CA 5	12/12/2022	<All>	<None>	R	
DOD SW CA-60	DoD Root CA 3	4/2/2025	<All>	<None>		
DOD SW CA-61	DoD Root CA 5	3/31/2025	<All>	<None>	R	
DOD SW CA-66	DoD Root CA 3	6/9/2027	<All>	<None>		
DOD SW CA-67	DoD Root CA 3	6/9/2027	<All>	<None>		
DOD SW CA-68	DoD Root CA 5	7/19/2027	<All>	<None>	R	
DOD SW CA-69	DoD Root CA 5	7/19/2027	<All>	<None>	R	
DOD SW CA-74	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD SW CA-75	DoD Root CA 3	12/6/2028	<All>	<None>		
DOD SW CA-76	DoD Root CA 5	5/14/2029	<All>	<None>		
DOD SW CA-77	DoD Root CA 5	5/14/2029	<All>	<None>		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA X3	R	
ECA Root CA 4	ECA Root CA 4	12/30/2029	<All>	<None>	R	
ECA Root CA 4	ECA Root CA 4	12/30/2029	<All>	<None>		
ECA Root CA 5	ECA Root CA 5	3/12/2050	<All>	<None>	R	
Federal Bridge CA G4	Federal Common Policy CA G2	12/6/2029	<All>	<None>	R	
Federal Common Policy CA G2	Federal Common Policy CA G2	10/14/2040	<All>	<None>	R	
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign Root CA...	R	
GlobalSign	GlobalSign	12/9/2034	Client Authenticati...	GlobalSign Root CA...	R	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	GlobalSign Root CA...	R	
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati...	Hotspot 2.0 Trust R...	R	
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	1/16/2034	Client Authenticati...	IdenTrust Commerc...	R	
IdenTrust ECA Component S21	ECA Root CA 4	6/22/2022	<All>	<None>	R	
IdenTrust ECA Component S23	ECA Root CA 4	4/5/2028	<All>	<None>	R	
IdenTrust ECA S21	ECA Root CA 4	5/18/2022	<All>	<None>	R	
IdenTrust ECA S22	ECA Root CA 4	5/7/2025	<All>	<None>	R	
IdenTrust ECA S22C	ECA Root CA 4	5/7/2025	<All>	<None>	R	
IdenTrust ECA S23	ECA Root CA 4	4/5/2028	<All>	<None>	R	
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati...	ISRG Root X1	R	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...	R	
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Microsoft ECC Prod...	R	
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS R...	R	
Microsoft Identity Verification R...	Microsoft Identity Verification Ro...	4/16/2045	Code Signing, Time...	Microsoft Identity V...	R	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	R	

Trusted Root Certification Authorities store contains 103 certificates.

11. Next, you need to check the Intermediate Certification Authorities Folder and its Certificates Sub-Folder for the lines of Issued To WidePoint ECA 8, Issued By ECA Root CA 4, and Expiration Date 7/7/2027, and Issued To WidePoint ECA 9, Issued By ECA Root CA 5, and Expiration Date 5/6/2034.


Certmgr - [Certificates - Current User\Intermediate Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Certificate Revocation Lis
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Other People
AdobeCertStore
Local NonRemovable Certific
Certificate Enrollment Reque
Smart Card Trusted Roots
Type here to search
2:49 PM
8/19/2024

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
DOD EMAIL CA-64	DoD Root CA 3	6/2/2027	<All>	<None>		
DOD EMAIL CA-65	DoD Root CA 3	6/9/2027	<All>	<None>		
DOD EMAIL CA-70	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD EMAIL CA-71	DoD Root CA 3	12/6/2028	<All>	<None>		
DOD EMAIL CA-72	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD EMAIL CA-73	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID CA-59	DoD Root CA 3	4/2/2025	<All>	<None>		
DOD ID CA-62	DoD Root CA 3	6/2/2027	<All>	<None>		
DOD ID CA-63	DoD Root CA 3	4/7/2027	<All>	<None>		
DOD ID CA-64	DoD Root CA 3	6/2/2027	<All>	<None>		
DOD ID CA-65	DoD Root CA 3	6/2/2027	<All>	<None>		
DOD ID CA-70	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID CA-71	DoD Root CA 3	12/6/2028	<All>	<None>		
DOD ID CA-72	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD ID CA-73	DoD Root CA 6	5/15/2029	<All>	<None>		
DoD Root CA 3	DoD Root CA 3	12/30/2029	<All>	<None>		
DOD SW CA-60	DoD Root CA 3	4/2/2025	<All>	<None>		
DOD SW CA-61	DoD Root CA 5	3/31/2025	<All>	<None>		
DOD SW CA-66	DoD Root CA 3	6/9/2027	<All>	<None>		
DOD SW CA-67	DoD Root CA 3	6/9/2027	<All>	<None>		
DOD SW CA-68	DoD Root CA 5	7/19/2027	<All>	<None>		
DOD SW CA-69	DoD Root CA 5	7/19/2027	<All>	<None>		
DOD SW CA-74	DoD Root CA 6	5/15/2029	<All>	<None>		
DOD SW CA-75	DoD Root CA 3	12/6/2028	<All>	<None>		
DOD SW CA-76	DoD Root CA 5	5/14/2029	<All>	<None>		
DOD SW CA-77	DoD Root CA 5	5/14/2029	<All>	<None>		
ECA Root CA 4	ECA Root CA 4	12/30/2029	<All>	<None>	R	
ECA Root CA 5	ECA Root CA 5	3/12/2050	<All>	<None>		
Federal Bridge CA G4	Federal Common Policy CA G2	12/6/2029	<All>	<None>	R	
Federal Common Policy CA G2	Federal Common Policy CA G2	10/14/2040	<All>	<None>	R	
IdenTrust ECA Component S23	ECA Root CA 4	4/5/2028	<All>	<None>		
IdenTrust ECA S22	ECA Root CA 4	5/7/2025	<All>	<None>		
IdenTrust ECA S22C	ECA Root CA 4	5/7/2025	<All>	<None>		
IdenTrust ECA S23	ECA Root CA 4	4/5/2028	<All>	<None>		
Microsoft TPM Root Certificate ...	Microsoft TPM Root Certificate A...	12/10/2039	<All>	<None>	R	
Microsoft Windows Hardware ...	Microsoft Root Authority	12/31/2002	Code Signing, Win...	<None>	R	
NCU-STM-KEYID-FB17D70D734...	Microsoft TPM Root Certificate A...	6/3/2027	1.3.6.1.4.1.311.21.36...	<None>	R	
ORC NFI CA 3	WidePoint NFI Root 2	5/15/2023	<All>	<None>	R	
Root Agency	Root Agency	12/31/2039	<All>	<None>	R	
TrustID EV Code Signing CA 4	IdenTrust Commercial Root CA 1	3/18/2030	Code Signing	<None>		
WidePoint ECA 8	ECA Root CA 4	7/7/2027	<All>	<None>	R	
WidePoint ECA 9	ECA Root CA 5	5/6/2034	<All>	<None>		
WidePoint NFI CA 5	WidePoint NFI Root 2	4/18/2030	<All>	<None>	R	
WidePoint NFI CA 6	WidePoint NFI Root 2	12/31/2030	<All>	<None>	R	
WidePoint NFI Root 2	Federal Bridge CA G4	1/10/2026	<All>	<None>	R	
widepoint-OHCOLPKI2-CA	WISC-CA	3/25/2029	<All>	<None>	R	Subordinate C...
WISC-CA	WISC-CA	3/23/2039	<All>	<None>	R	
www.verisign.com/CPS Incorp....	Class 3 Public Primary Certificatio...	10/24/2016	Server Authenticati...	<None>	R	

Intermediate Certification Authorities store contains 54 certificates.

12. As long as you have all four of these of these in their respective locations shown above, then you have the trust chain for your certificates properly loaded. You can close the MMC.