



# Cybersecurity 701

Certificates Lab



# Certificate Materials

- Materials needed
  - Windows Server 22 Virtual Machine
- Software Tool used
  - mmc



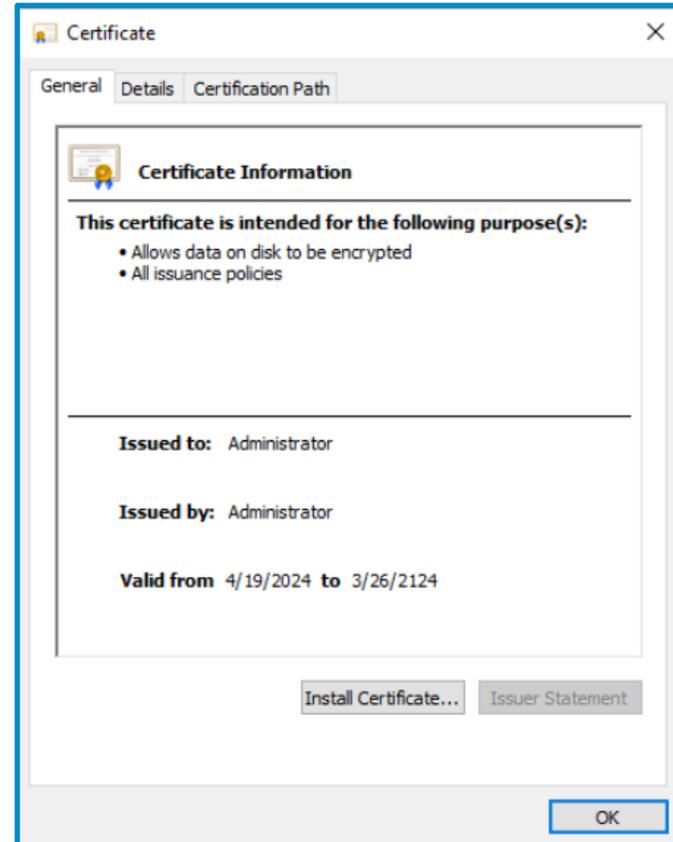
# Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 1.4 - Explain the importance of using appropriate cryptographic solutions.
    - Public Key
    - Private Key
    - Certificates
      - Self-signed



# What are digital certificates?

- Digital certificates are an electronic document used to prove the ownership of a public key
- There are many different formats including: DER, PEM, PFX, .cer, P12, and P7B



# Certificates Lab Overview

1. Set up VM Environment
2. Create a Folder and File
3. Encrypt the Folder and File with EFS
4. Open mmc
5. Setup Software for Exporting Certificates
6. Export Private Key Certificate
7. Export Public Key Certificate



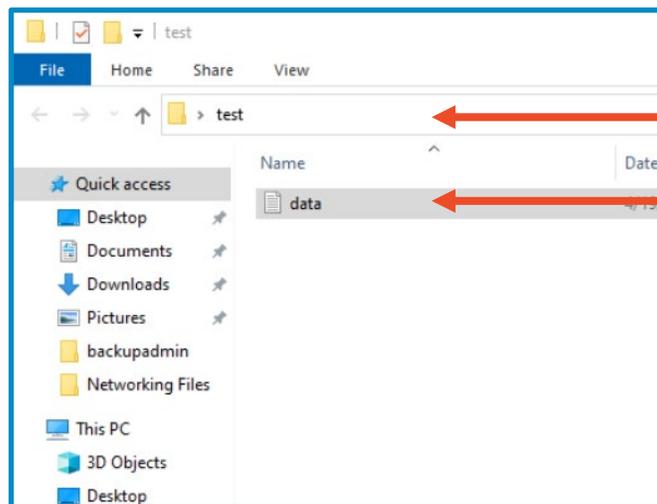
# Set up Environments

- Log into your range
- Open the Windows Server 22 Environment
  - You should be on your Windows Desktop



# Create a Folder and File

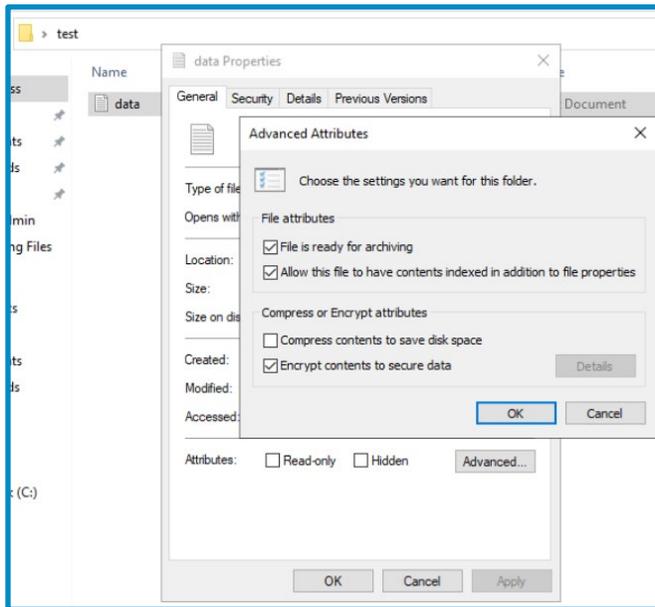
- On the desktop, right-click, hover over New, then select Folder
- Name the folder, "test"
- Open the test folder, right-click, hover over New, then select Text Document
- Name the text document, "data"



Verify there's a text file titled data inside the test folder

# Encrypt the Folder and File with EFS

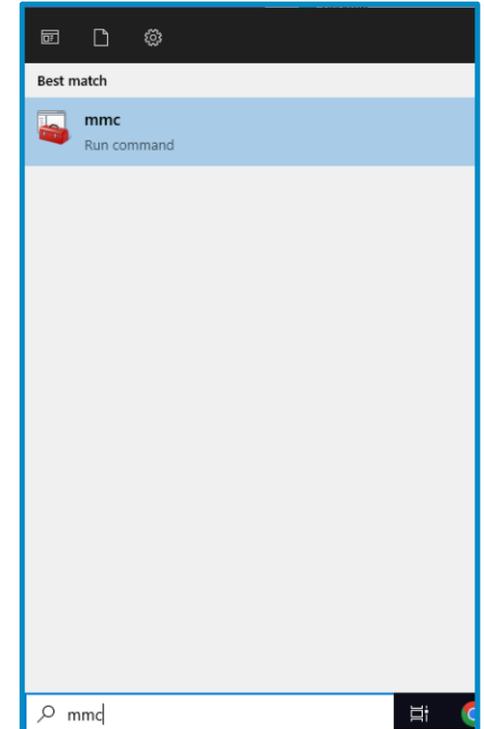
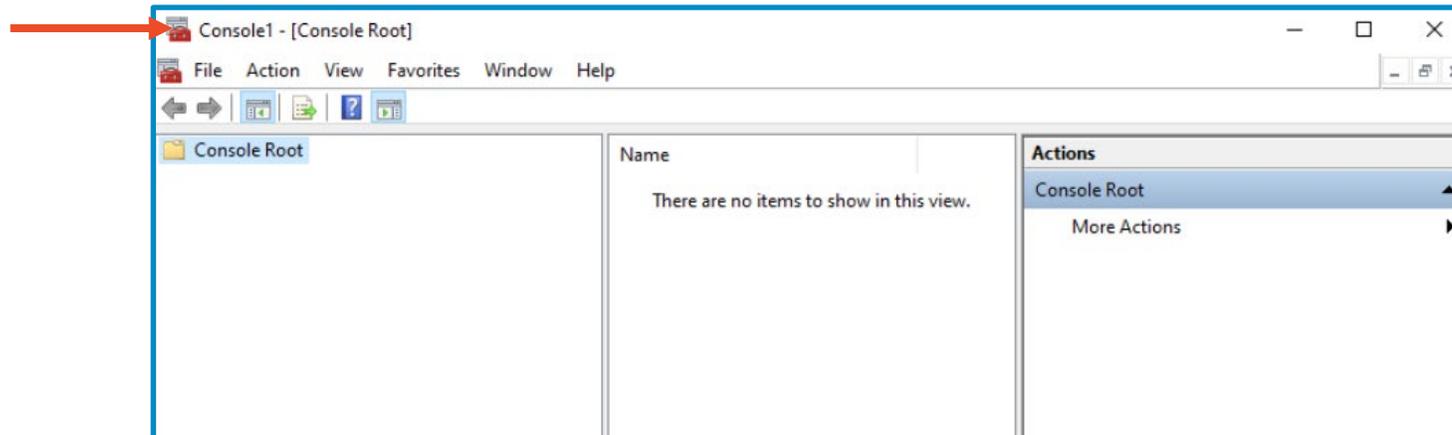
- Right-click the data file, select "Properties"
- Click "Advanced", then select the "Encrypt contents to secure data" box
- Click "OK", then "Apply"
  - Then click "OK again (twice)



# Open mmc

- Click the **Start** button, type **mmc**, and select the icon with the red suitcase.

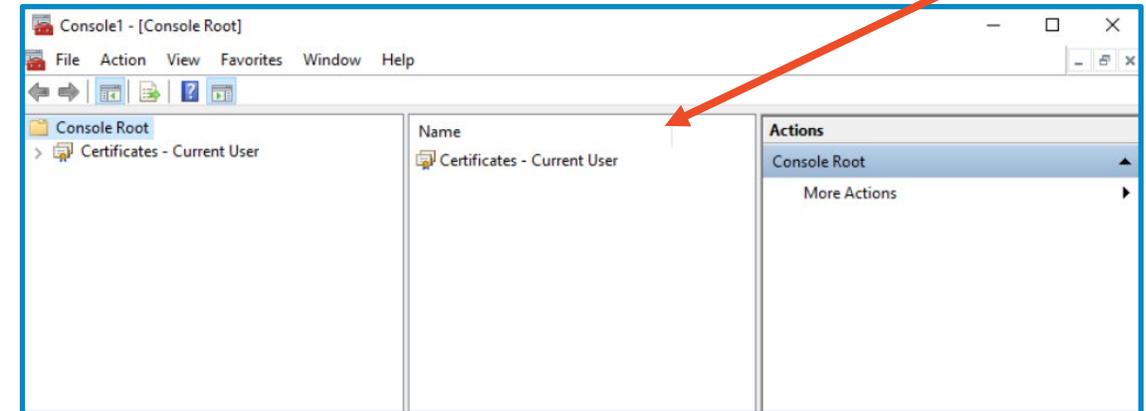
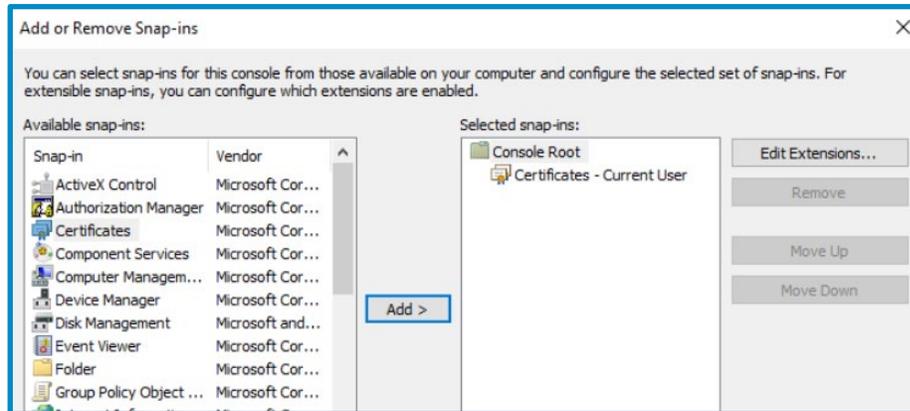
You should see the  
Microsoft  
Management  
Console open



# Setup Software for Exporting Certificates

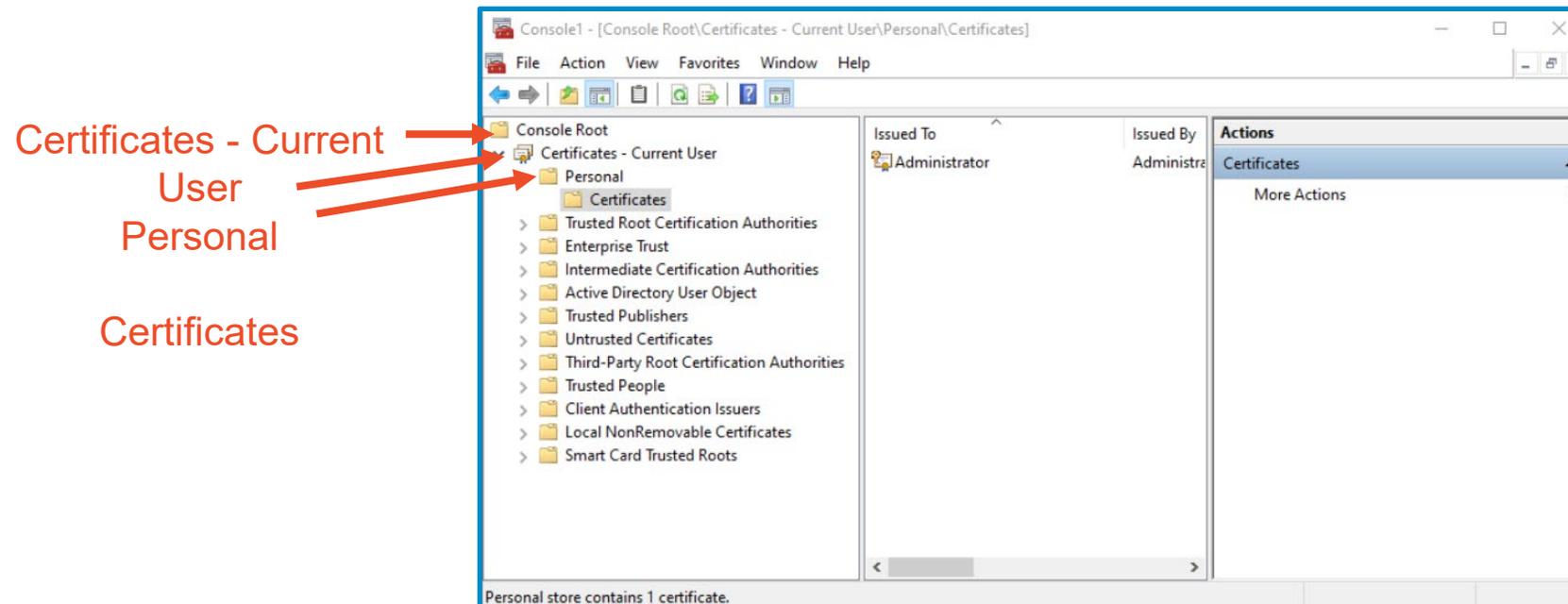
- With Console1 open, select **File**, then select **Add/Remove Snap-In**
- Select **Certificates**, then click **Add**, followed by **Finish**, and then **Ok**.
- Console1 should now include a "Certificates – Current User" tab

Verify the  
"Certificates -  
Current User"  
appears



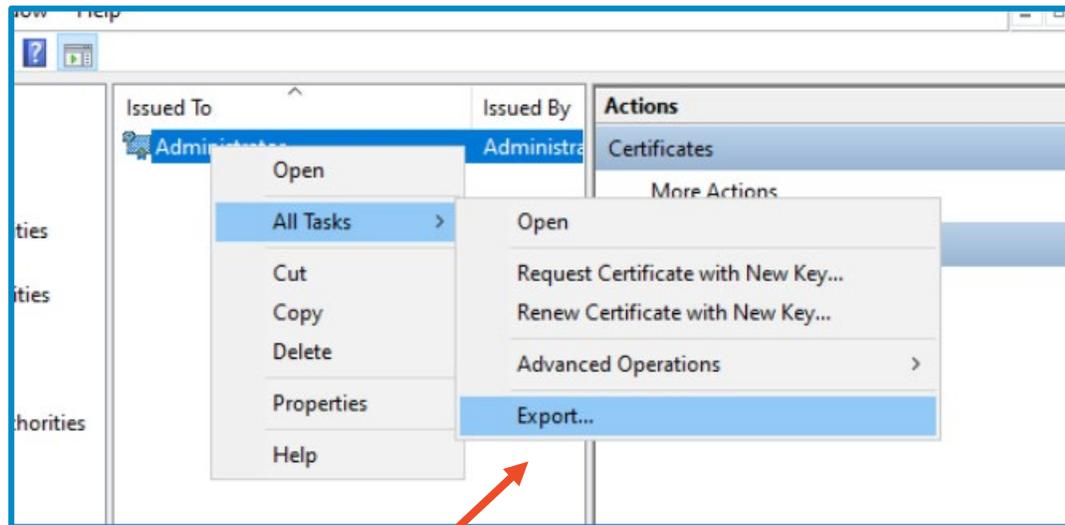
# Export Private Key Certificate Step 1

- Click the + beside "Certificates – Current User"
- Click the + beside "Personal"
- Click the "Certificates" folder that appears

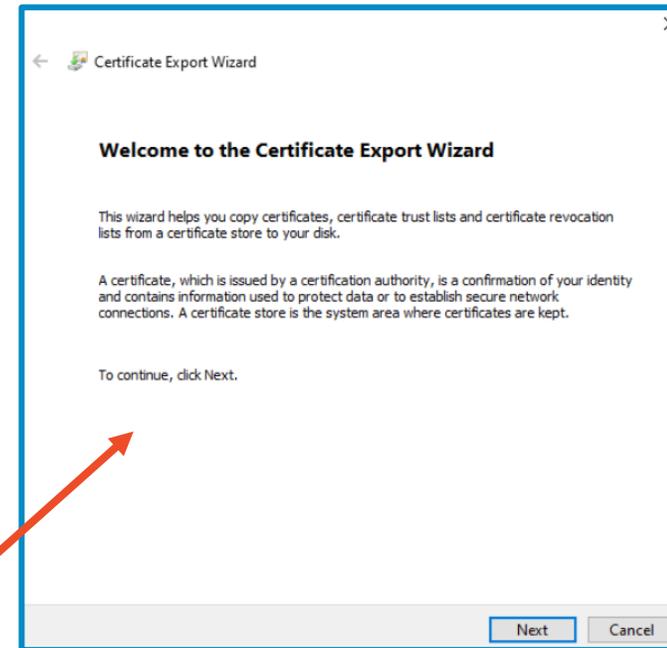


# Export Private Key Certificate Step 2

- In the center display, right-click "Administrator".
- Hover over the "All Tasks" option and click "Export"



Click on Export...

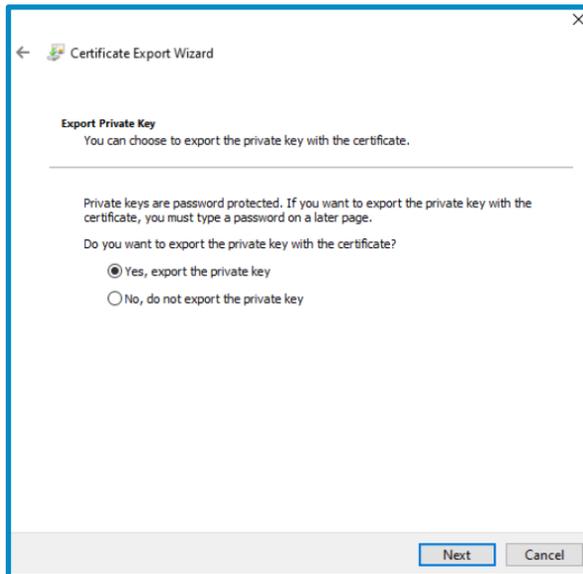


Verify the Certificate  
Export Wizard  
appears

# Export Private Key Certificate Step 3

The certification export wizard appears.

- Click "Next"
- Click "Yes, export the private key"
- Click "Next" (twice)
- Create a password, and click "Next"



← Certificate Export Wizard

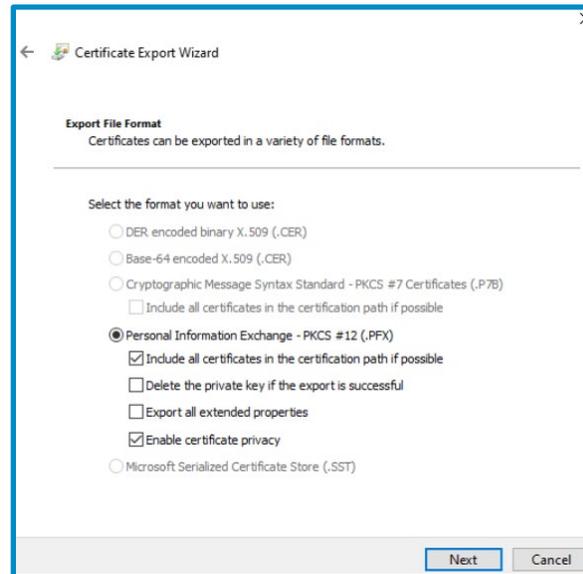
**Export Private Key**  
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key  
 No, do not export the private key

Next Cancel



← Certificate Export Wizard

**Export File Format**  
Certificates can be exported in a variety of file formats.

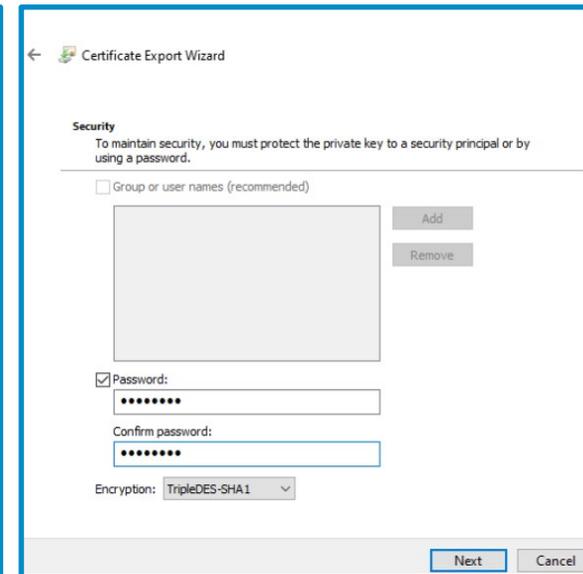
Select the format you want to use:

DER encoded binary X.509 (.CER)  
 Base-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  
 Enable certificate privacy

Microsoft Serialized Certificate Store (.SST)

Next Cancel



← Certificate Export Wizard

**Security**  
To maintain security, you must protect the private key to a security principal or by using a password.

Group or user names (recommended)

Add Remove

Password:  
.....

Confirm password:  
.....

Encryption: TripleDES-SHA1

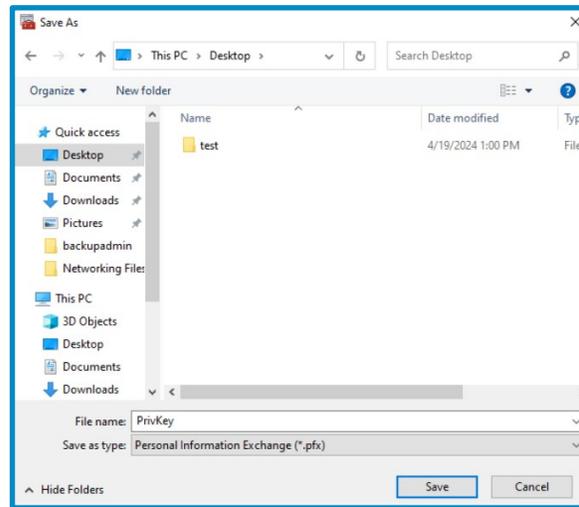
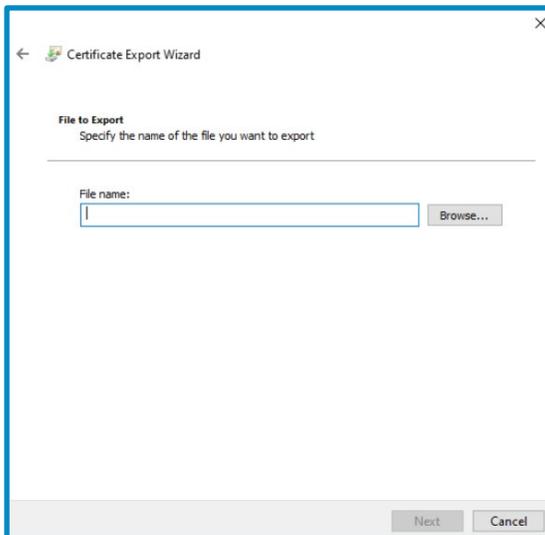
Next Cancel

You should see a  
"File to Export"  
appear



# Export Private Key Certificate Step 4

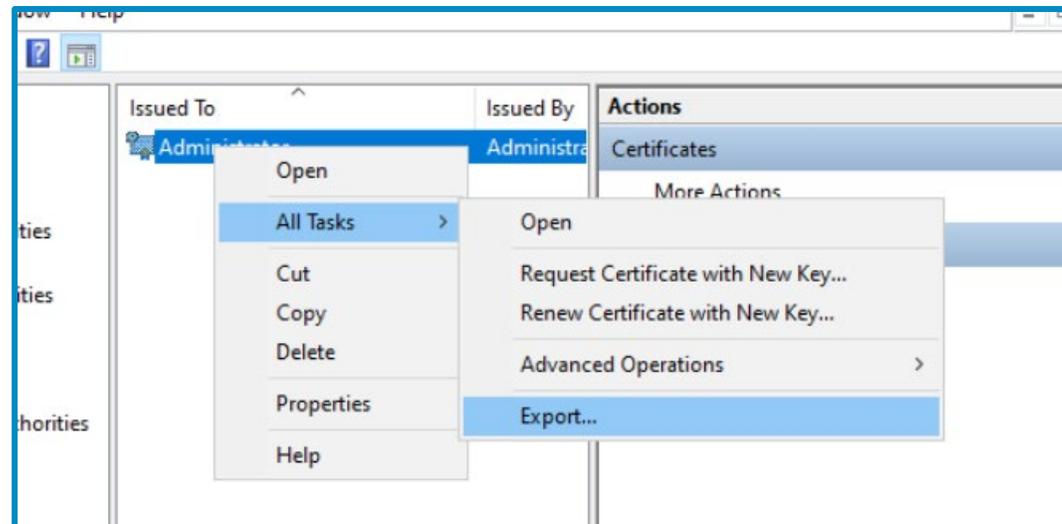
- Click "Browse"
- Navigate to the Desktop
- Save the File as "PrivKey"
- Click "Next"
- Click "Finish"



Save to the Desktop, and you should see the PrivKey appear on the Desktop

# Export Public Key Certificate Step 1

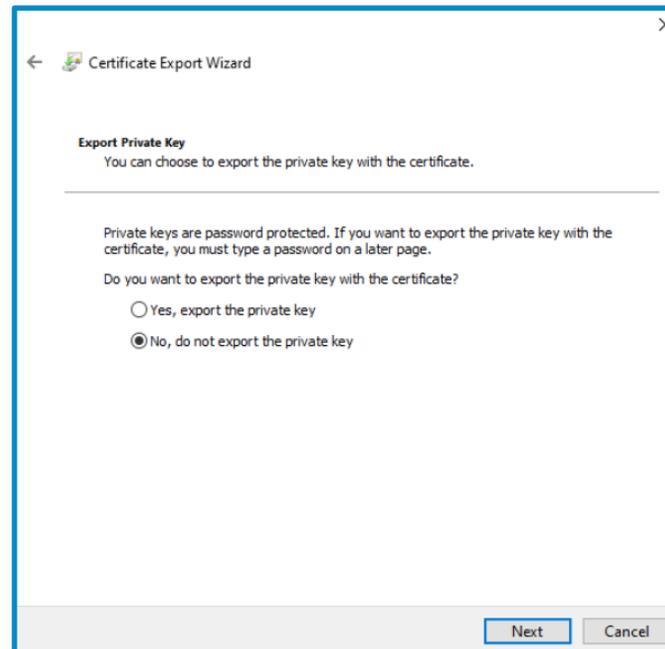
- In the center display, right-click "windows"
- Hover over the "All Tasks" option and click "Export"



# Export Public Key Certificate Step 2

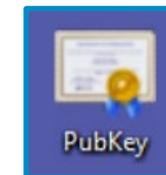
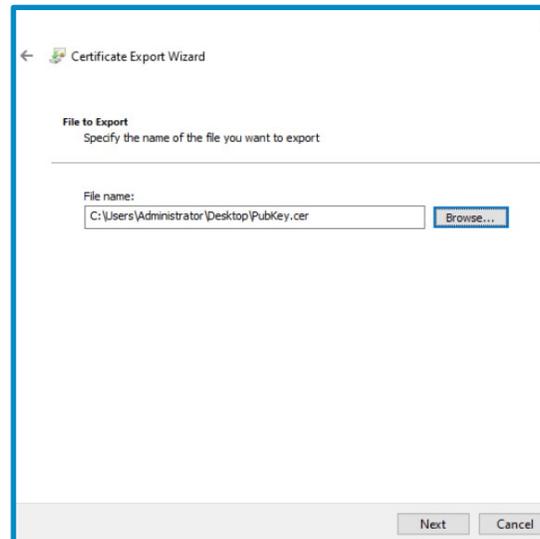
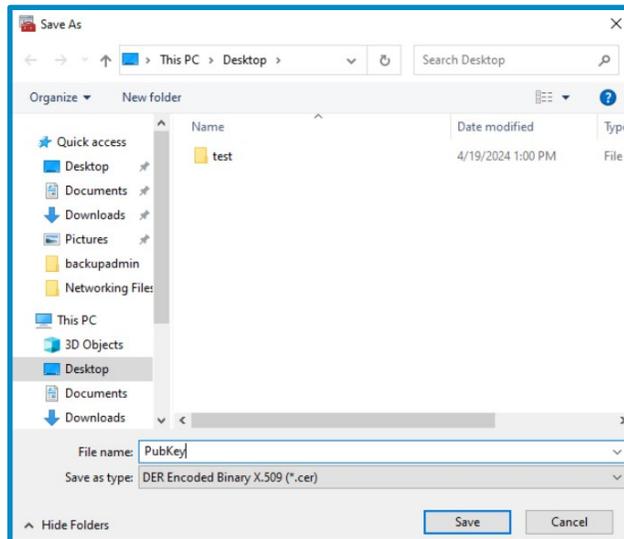
The certificate export wizard appears.

- Click "Next"
- Click "No, do not export the private key"
- Click "Next" (twice)



# Export Public Key Certificate Step 3

- Click "Browse"
- Navigate to the Desktop
- Save the File as "PubKey"
- Click "Next"
- Click "Finish"



Save it to the Desktop, and you should see the PubKey appear on the Desktop

# Investigate the Certificates

- Notice, if you open the PrivKey file, an Import wizard appears, however, if you open the PubKey file, information about the certificate is readily available.

