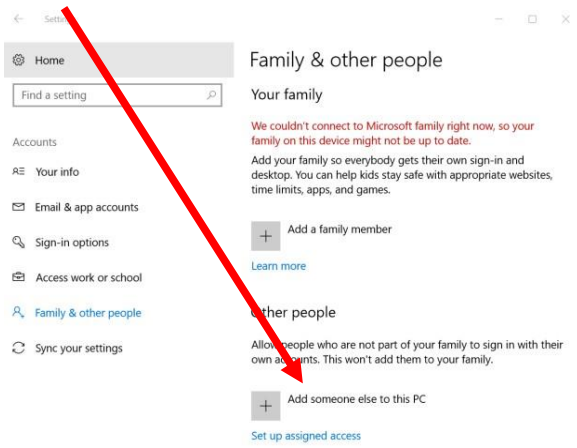
Cryptography Using EFS

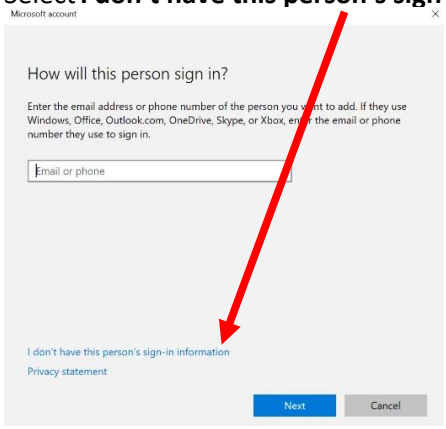
IT2700

Part I: Create two new local users on your Windows 10/11 virtual machine.

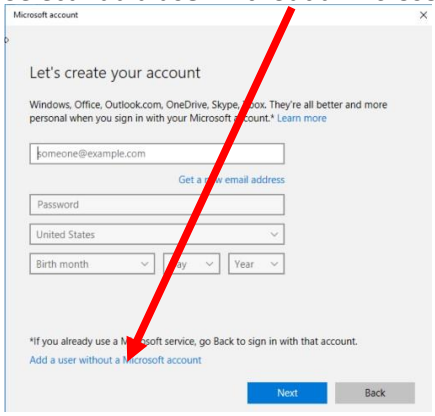
1. Under Settings – Accounts – Family & other People
   a. Select **Add someone else to this PC**



b. Select **I don't have this person's sign in information**

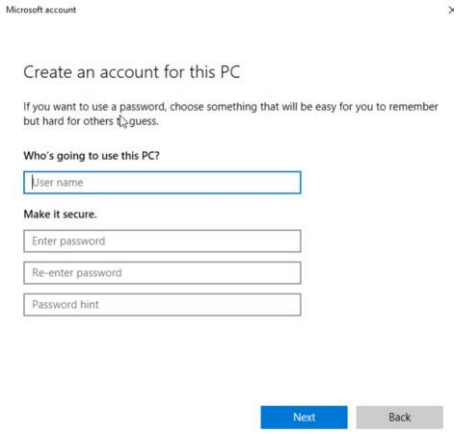


Select **Add a user without a Microsoft account**



c.

d. Create the account. Choose the username, password and hint. Then click Next.



e. Repeat the process to create a second new user.

Part II: Using Microsoft's Encrypting File System (EFS)

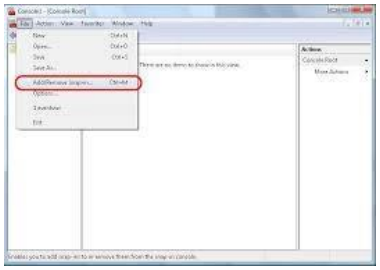
Microsoft's Encrypting File System (EFS) is a cryptography system for Windows operating systems that uses the Windows NTFS file system. Because EFS is tightly integrated with the file system, file encryption and decryption are transparent to the user. In this project, you turn on and use EFS.

EFS works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key, or FEK. It uses a symmetric encryption algorithm because it takes less time to encrypt and decrypt large amounts of data than if an asymmetric key cipher is used.

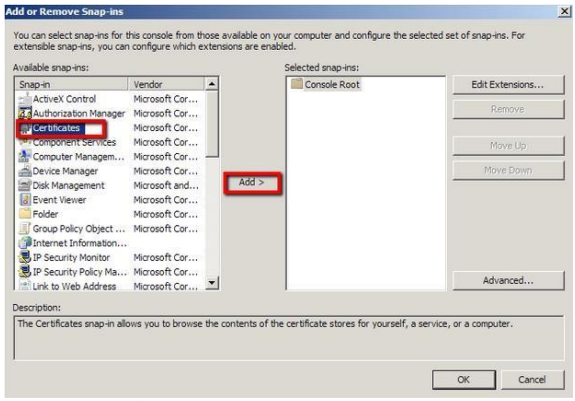
The file encryption key (FEK) is used to encrypt the file, and is then itself encrypted by using the public key taken from the user's certificate, which is located in the user's profile. The encrypted FEK is stored with the encrypted file and is unique to it. To decrypt the FEK, EFS uses the encryptor's private key which only the file encryptor has.

On your Windows 10/11 Virtual Machine:

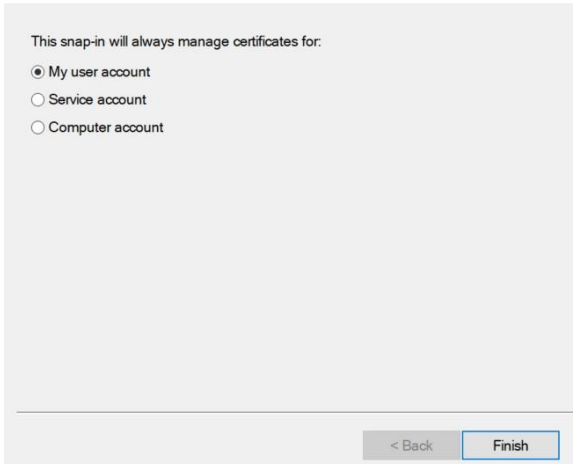
1. Sign in as the first user you created. The first time logging in might take a bit, as it has to create the profile.
2. Open Microsoft Management Console by running **mmc** from a command prompt or from Cortana. If prompted, click YES
3. Click **File – Add/Remove Snapin…**



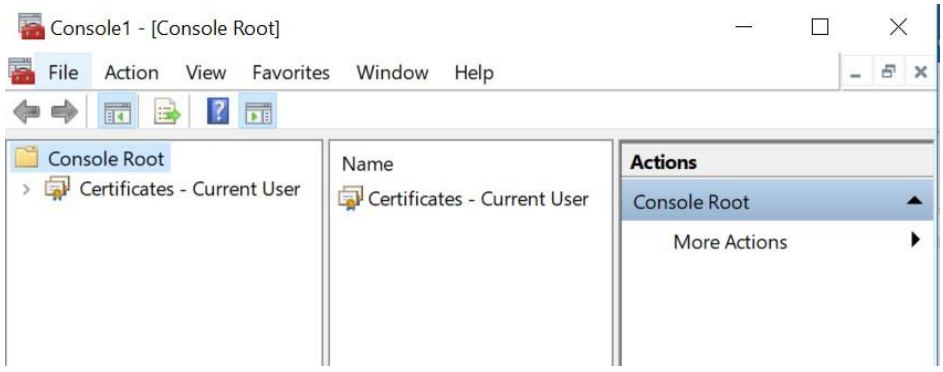
4. Add Certificates – My user account – Finish - OK



Certificates snap-in



5. You should see this:



6. From the Console1 window, expand the **Certificates** node in the left pane and select **Personal** folder. The Object Type in the middle indicates that there are no items to show.

From the File menu, click **Save As**; in the File name box, type the user's name along with Certs (for example, if I were logged in as Ralph, I would type in Ralph Certs). Click the **Desktop** icon to direct the file to the desktop, and click **save**. Close the console.

7. Go to a command prompt. Navigate to the root of c: by typing **cd ** and pressing **Enter**.
8. Type **cipher /?** to read a little about the cipher encryption command.
9. Type **cipher** and press **Enter**. The items with a U indicate the folder is unencrypted.

Submit a screenshot of the results.

10. Type **md confidential** to create a new folder. Run the cipher command again. *What is the encryption status of the confidential folder?*
11. Type **copy con c:\confidential\passwords.txt** and press **Enter**. Type **This is my super secret list of all the passwords.** Press **Enter** then **Ctrl-Z** and **Enter** again. Type **c:\confidential\passwords.txt** and press **Enter**.
12. Type **type c:\confidential\passwords.txt** to view the contents of passwords.txt.
13. Type **cipher /e c:\confidential\passwords.txt** and press **Enter**. This encrypts the passwords.txt file.
14. Type **cipher c:\confidential\passwords.txt**. *What does the E indicate?*
15. Reissue **type c:\confidential\passwords.txt** *Is your user able to see the contents of passwords.txt?*
16. From the desktop, open your user's certs that you saved on the desktop. Expand Certificates, Expand the Personal folder. Note the changes. Click the Certificates folder inside the Personal folder. Double click the certificate inside the middle pane. *Submit a screenshot of the **General** Tab of this certificate.*

Part III – Another User Tries to Access passwords.txt

1. Sign out as your first user. Sign in as your second user.
2. Open Windows Explorer. Navigate to c:\confidential. Create a new text document by right clicking inside the folder and choosing **New - Text Document** from the pop out menu.
3. Give the new text document a name of your choosing and press **Enter**.
4. Compare the icons from passwords.txt and your new text document. *How are the two icons different?*
5. From a command prompt, navigate to c:\confidential by typing **cd \confidential**.
6. Type **type passwords.txt** to view the contents of passwords.txt. What was the result and why did you get that result?
7. From the command prompt, type **runas "/user:<your first username>" cmd** and press **Enter**. For example, if my first username was Ralph Parker, I would type **runas "/user:Ralph Parker" cmd**
8. Enter the first user's password then enter. A new command prompt will appear, running under your first user.

9. Navigate to c:\confidential by typing **cd \confidential**.
10. Type **type passwords.txt** to view the contents of passwords.txt. What was the result and why did you get that result?
11. Type **cipher /c** and press **Enter**. Submit a screenshot of the results.
12. What encryption standard was used to encrypt the file? Was this file encrypted with Symmetric or Asymmetric methods? What is the purpose of the certificate? Is the certificate for Symmetric or Asymmetric use?