Practical 3 – Implementing Windows Security Configurations- Part 1

Pre-Requisites

Objectives

- Removing Administrator Autologon
- Enabling User Autologon Account
- Using **cipher** command
- Encrypting Files and Folders
- Exporting a user's private key
- Using Recovery Agent and user's key to decrypt user's files

You will need Administrator rights to do this practical. Therefore, you will need to use VMWare Workstation or Player to run a virtual image of Windows, giving you administrator rights. DO NOT use the original copy of the virtual image. First copy the virtual image to your working folder before you begin this practical.

First Log on using SIT account :

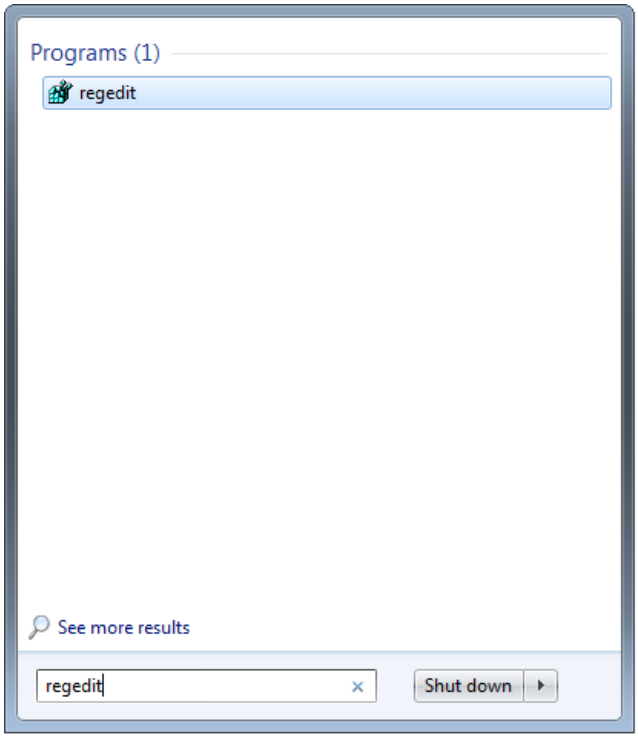
```
User ID = SIT
Password = P@ssw0rd

User ID = Student
Password = P@ssw0rd
```

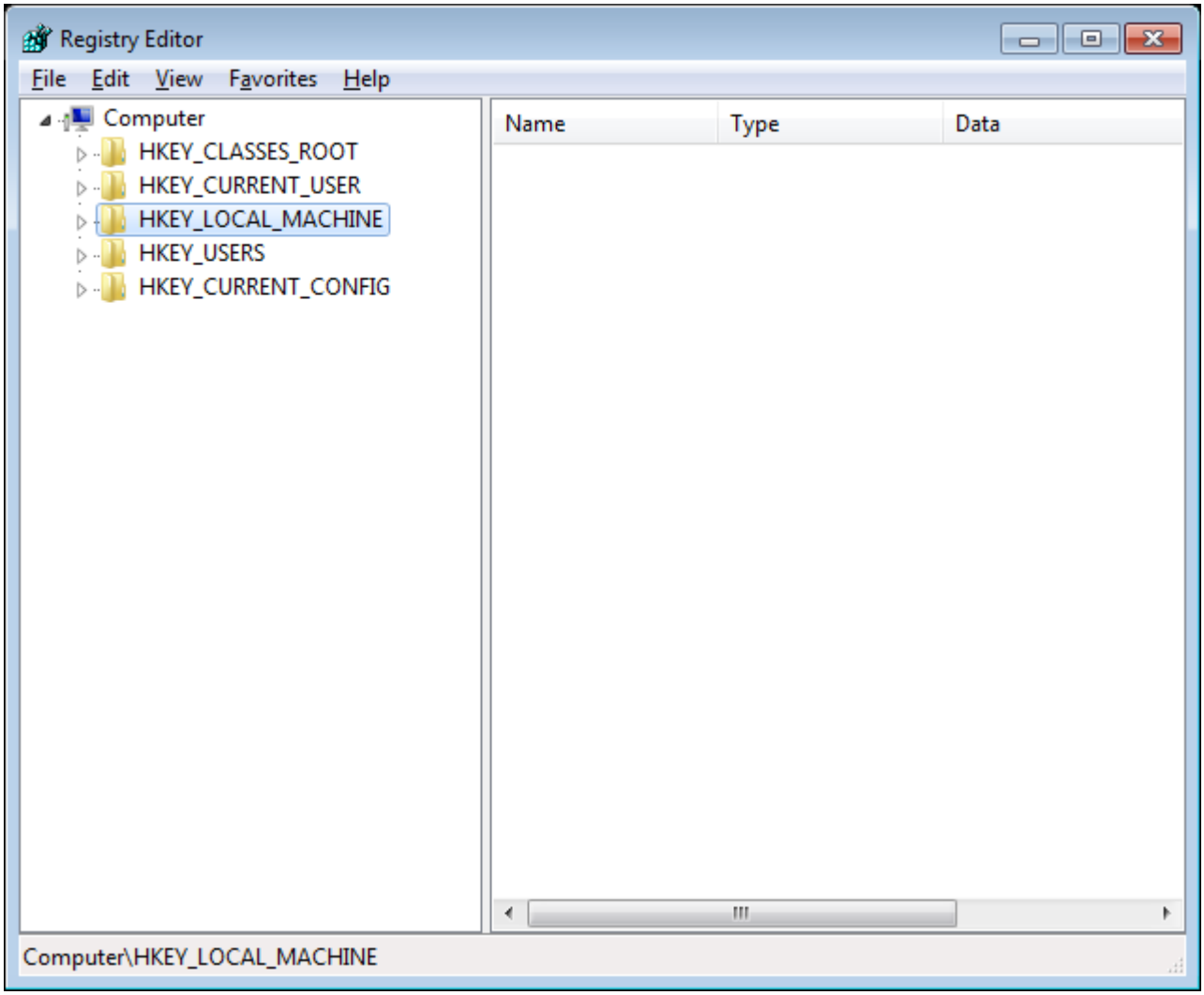
Exercise 1 - Removing Administrator Autologon

1. Autologon is convenient but it can pose a security risk to the system. In this exercise, we will learn how to disable automatic administrator login.

   Enter "regedit" to execute Registry Editor.



Select the “regedit” listed item to execute the command.
The UI and layout may differ in different OS versions.
Registry entries or keys may be renamed, relocated or missing.
Perform an online search for equivalents.



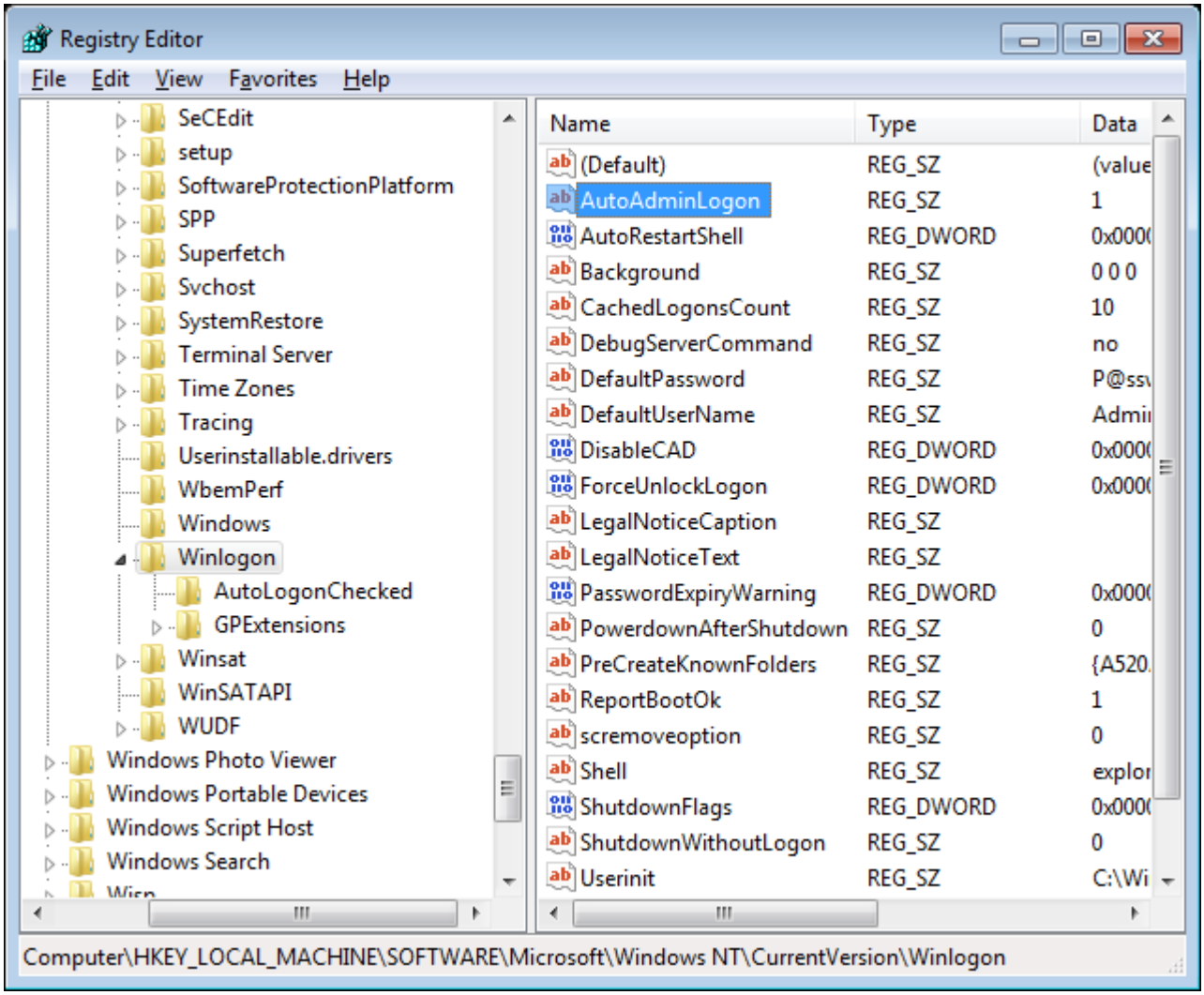
Windows Registry

Windows Registry is a database used to store settings and options for hardware, software, and preferences of the PC. The registry physical files of the are located differently depending on the version of Windows. In Windows 7, the files are found in the "WINDOWS\System32\Config" folder. Registry is managed using "regedit.exe".

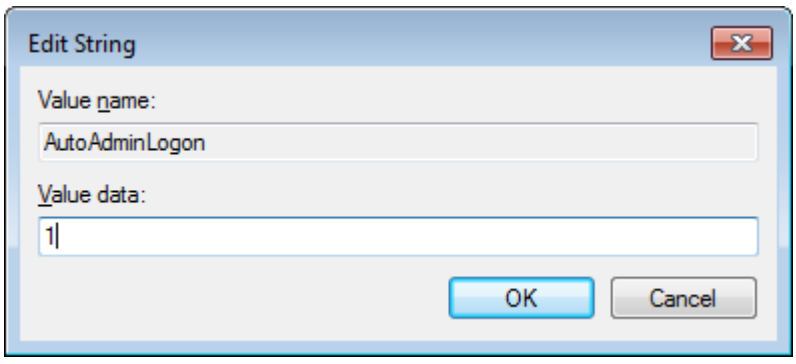
Note

Modifying the Windows registry can cause serious problems to the system. As such, do not making changes unless you are sure of what you are doing. For added protection, back up the registry before you change it.

2. Locate the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" registry key.



Look at the entry "AutoAdminLogon".

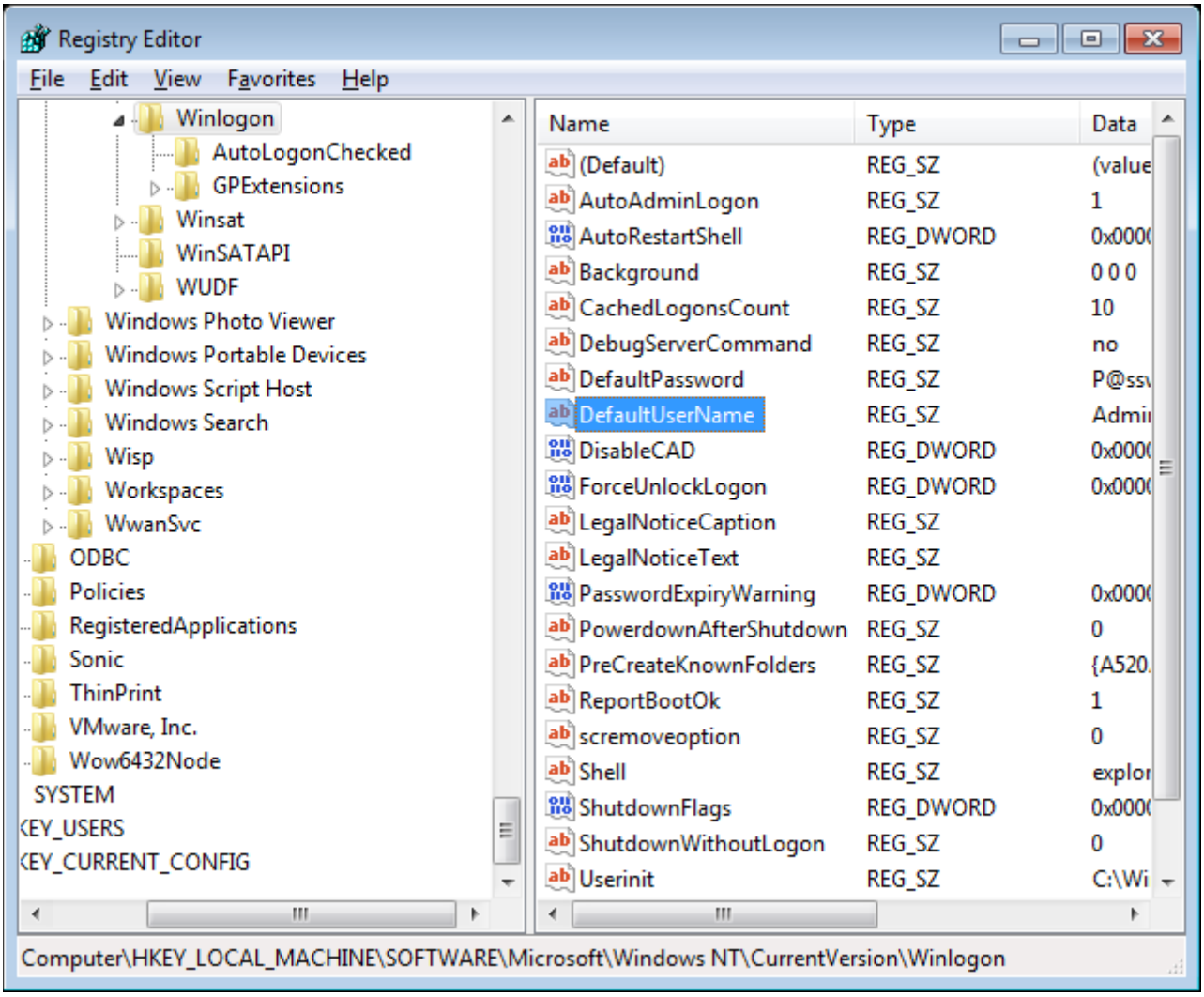


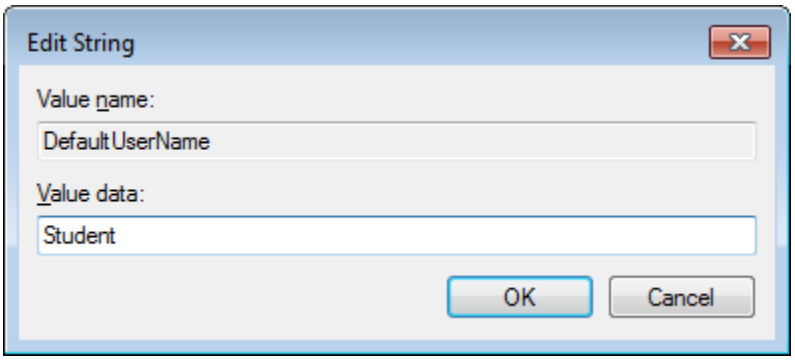
Note

To disable automatic log on, set the value to zero. To enable automatic log on, set the value to one. It is currently set to 1, but there is no DefaultPassword assigned yet.

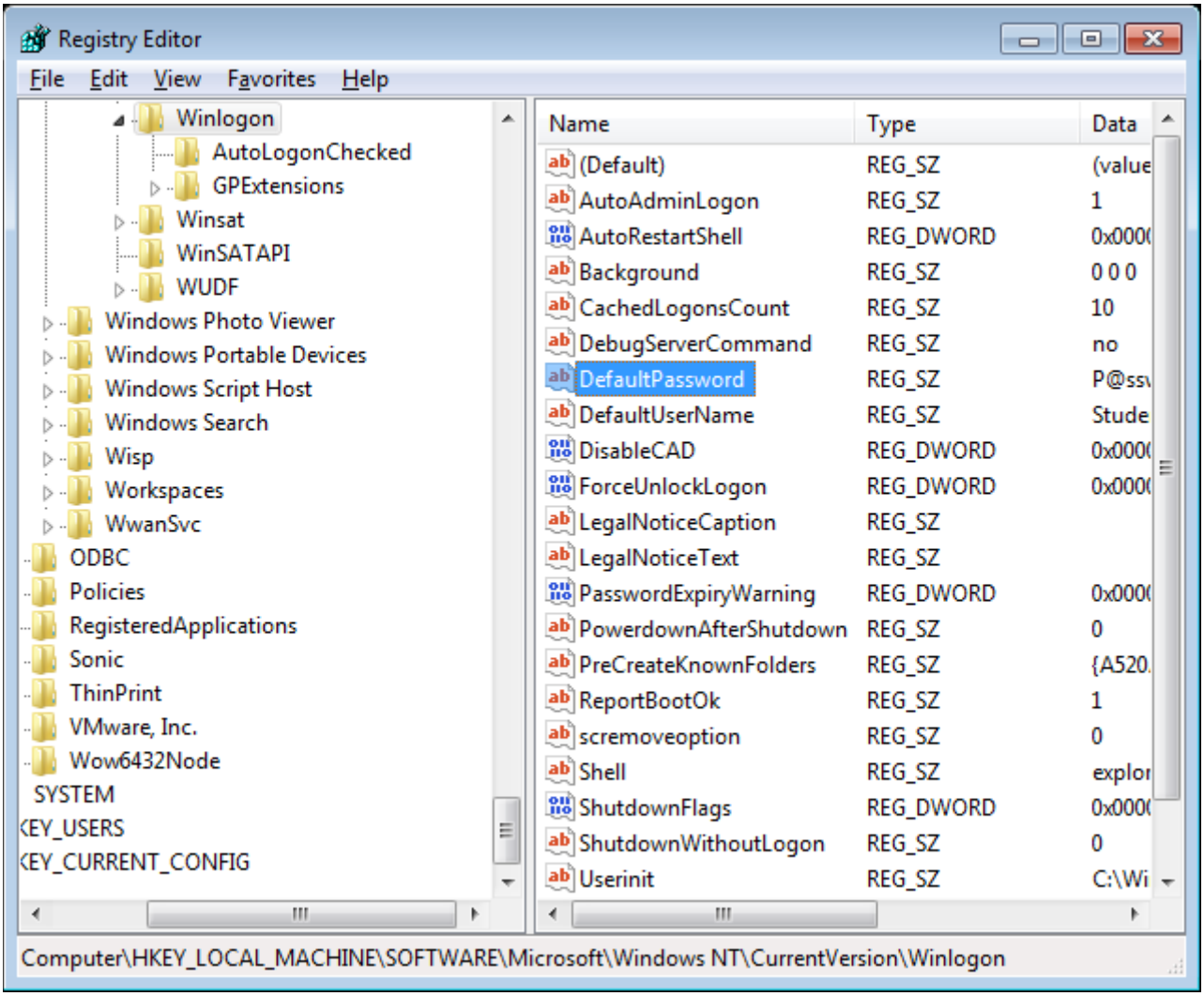
Exercise 2 - Enabling User Autologin for Student

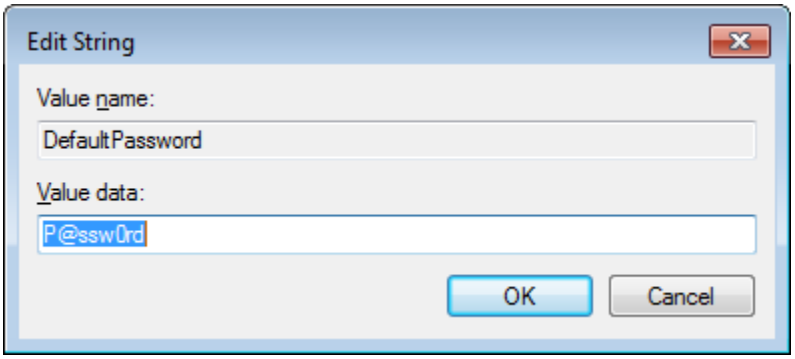
1. Follow the steps as shown to set the autologin user as Student.





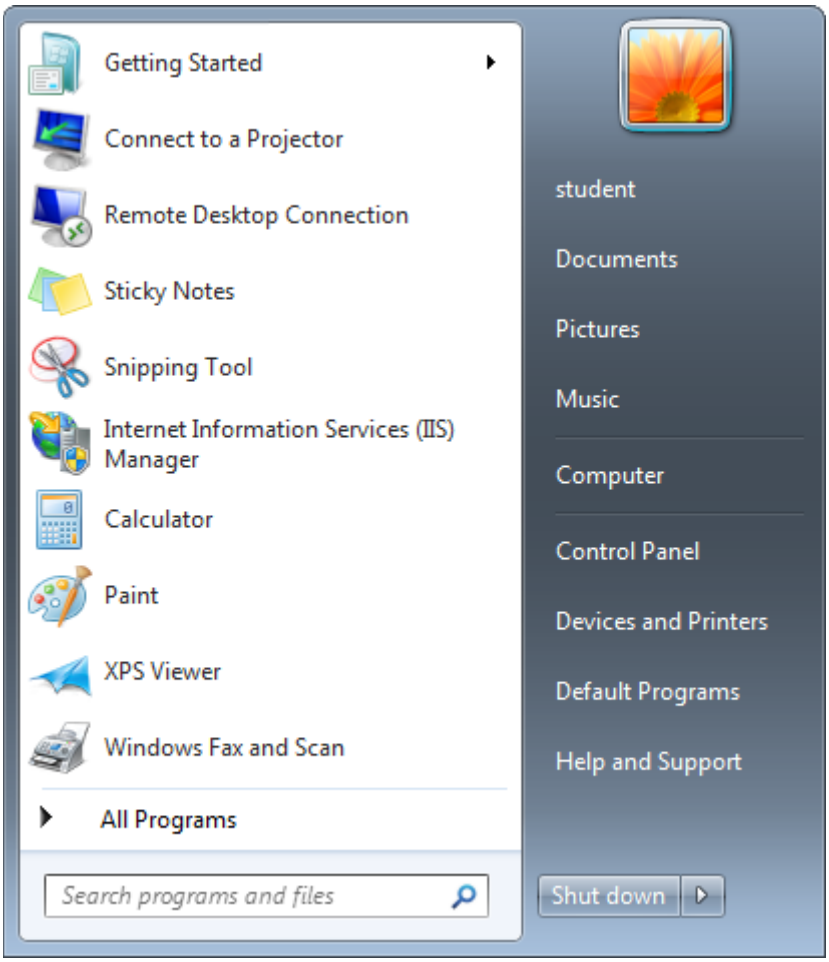
2. Follow the steps as shown to modify the "DefaultPassword" registry value.





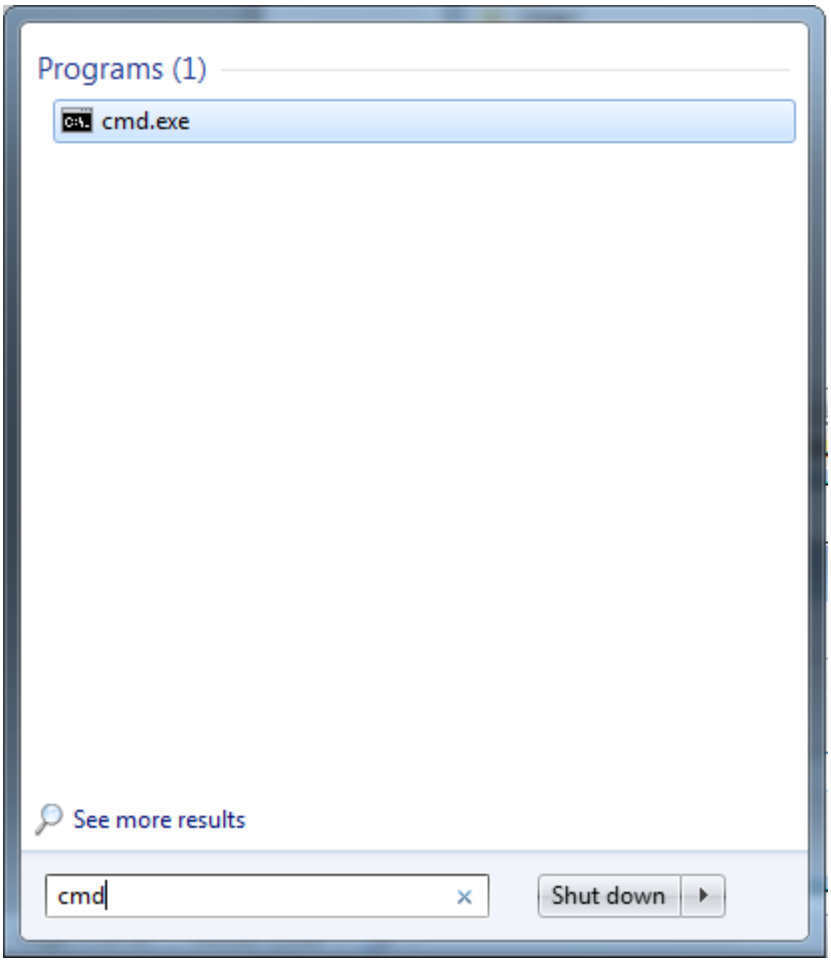
Important
Verify that the AutoAdminLogon registry value is 1. If the value is 0, set the value to 1.

3. Restart the system and verify that the autologon user is correct. Try to think of some situations where autologin is useful.



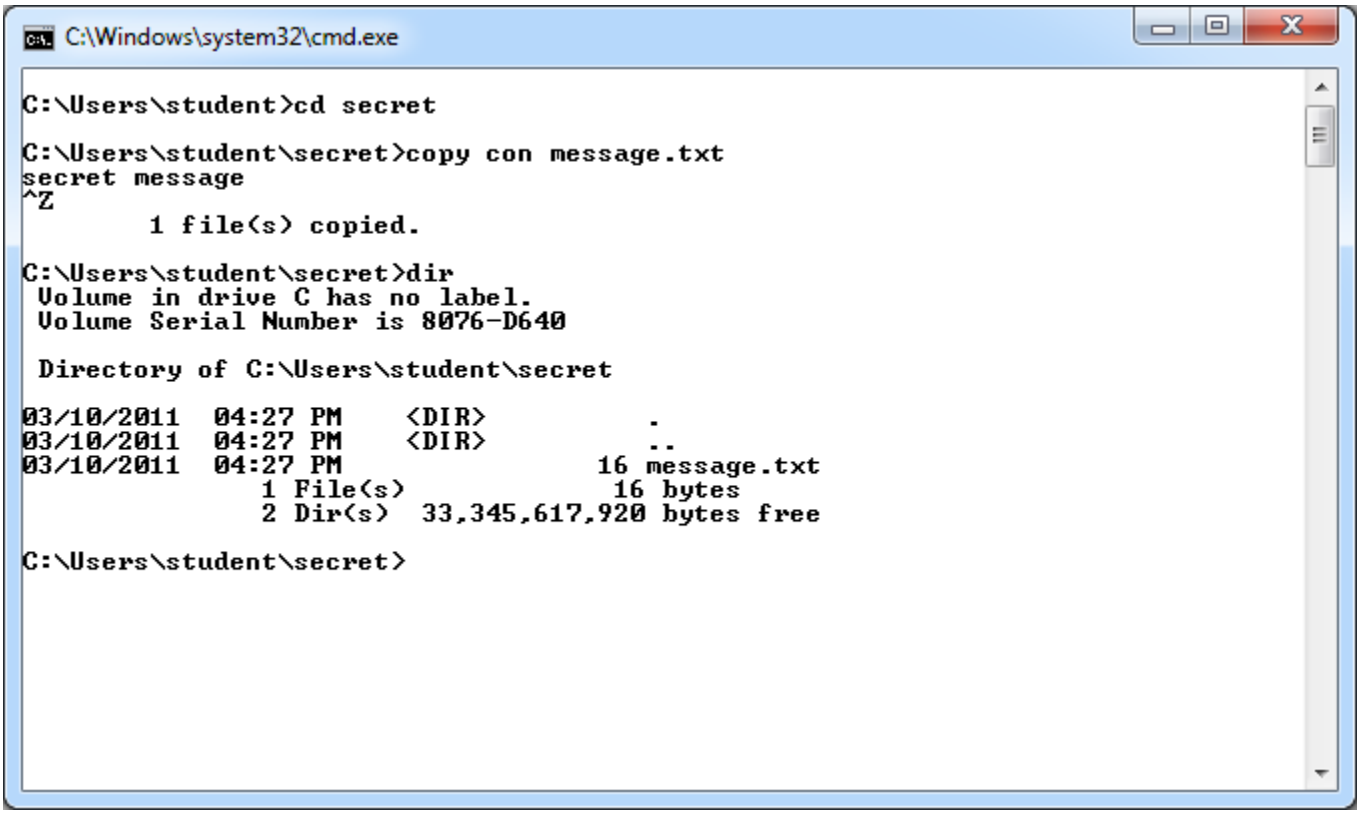
Exercise 3 - Using cipher command

1. Run cmd.exe.

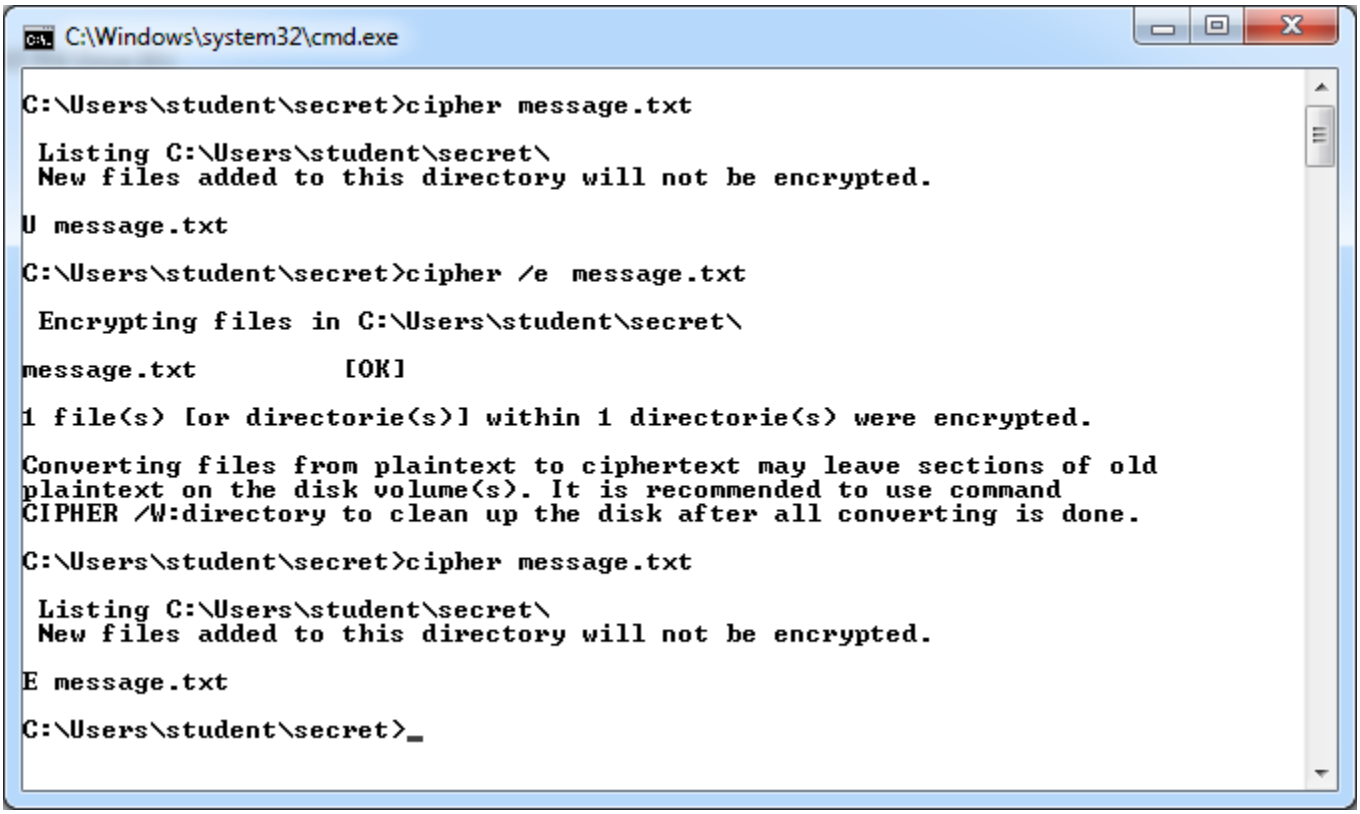


The **cipher** command displays or alters the encryption of directories and files on NTFS partitions.

If there is no 'secret' sub-folder, first create it by typing 'md secret', then do the following:



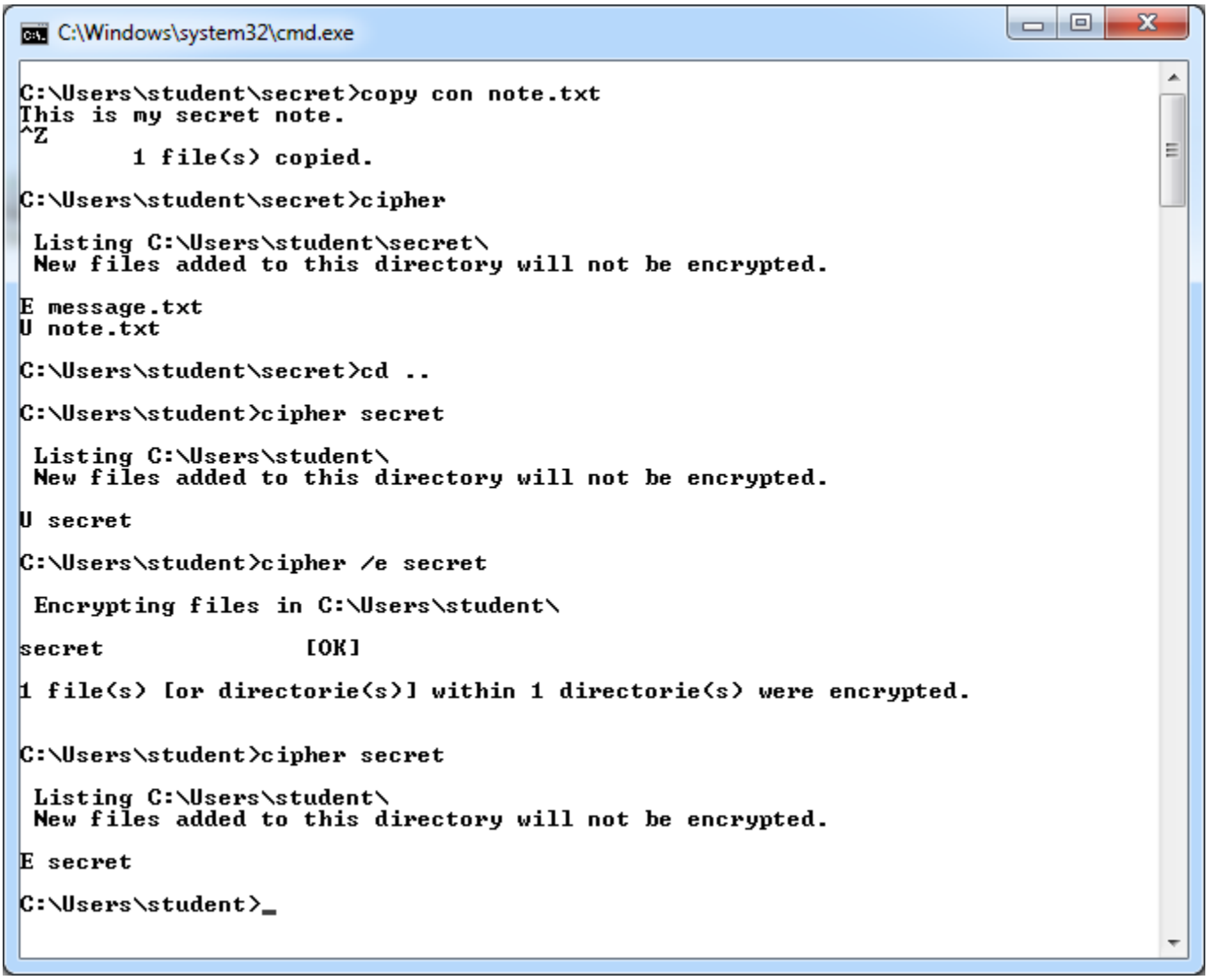
2. Follow the steps as shown to encrypt a file with the **cipher** command.

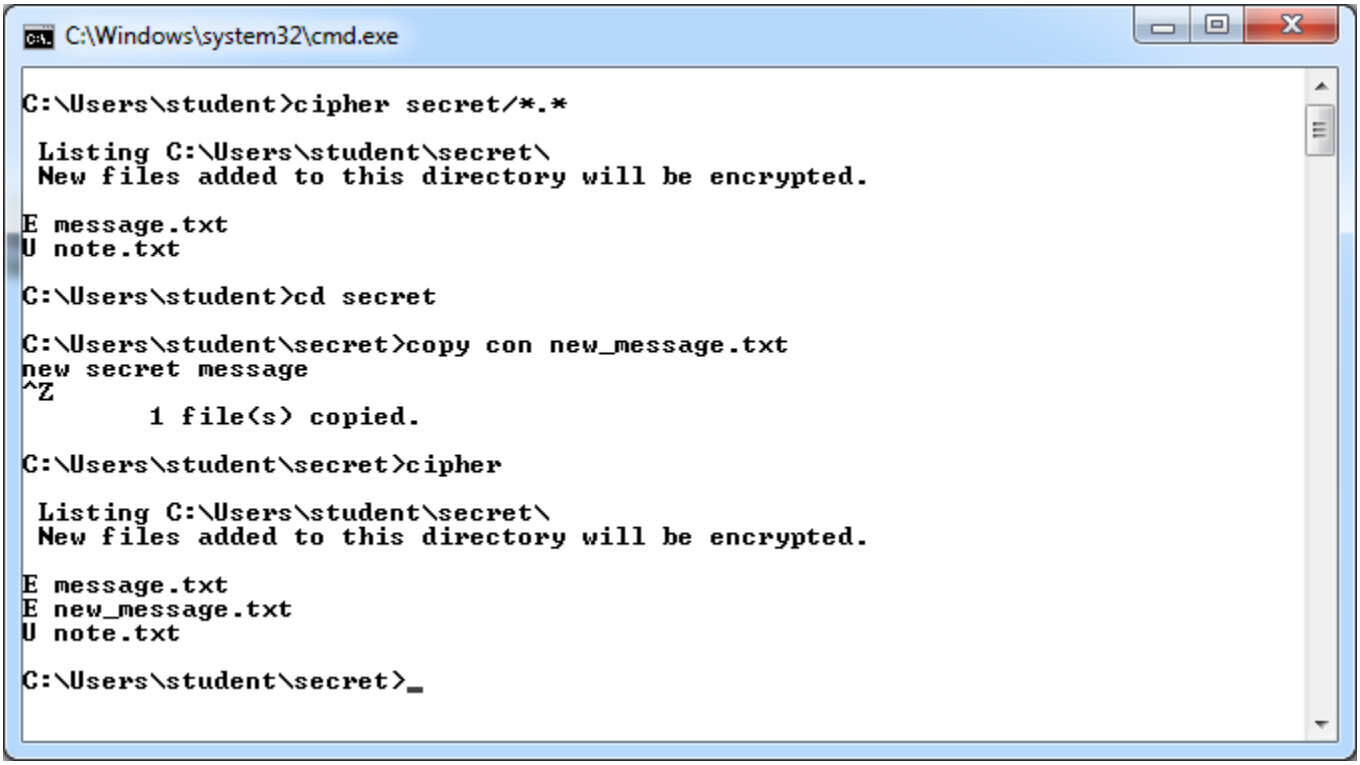


Attribute	Description
E	Encrypted
U	Unencrypted

Note
The option "/E" can be used to encrypt files.

3. Follow the steps as shown to encrypt a directory with the **cipher** command.




C:\Windows\system32\cmd.exe
C:\Users\student>cipher secret/*.*
Listing C:\Users\student\secret\
New files added to this directory will be encrypted.
E message.txt
U note.txt
C:\Users\student>cd secret
C:\Users\student\secret>copy con new_message.txt
new secret message
^Z
1 file(s) copied.
C:\Users\student\secret>cipher
Listing C:\Users\student\secret\
New files added to this directory will be encrypted.
E message.txt
E new_message.txt
U note.txt
C:\Users\student\secret>_

Exercise 4 - User accounts and passwords

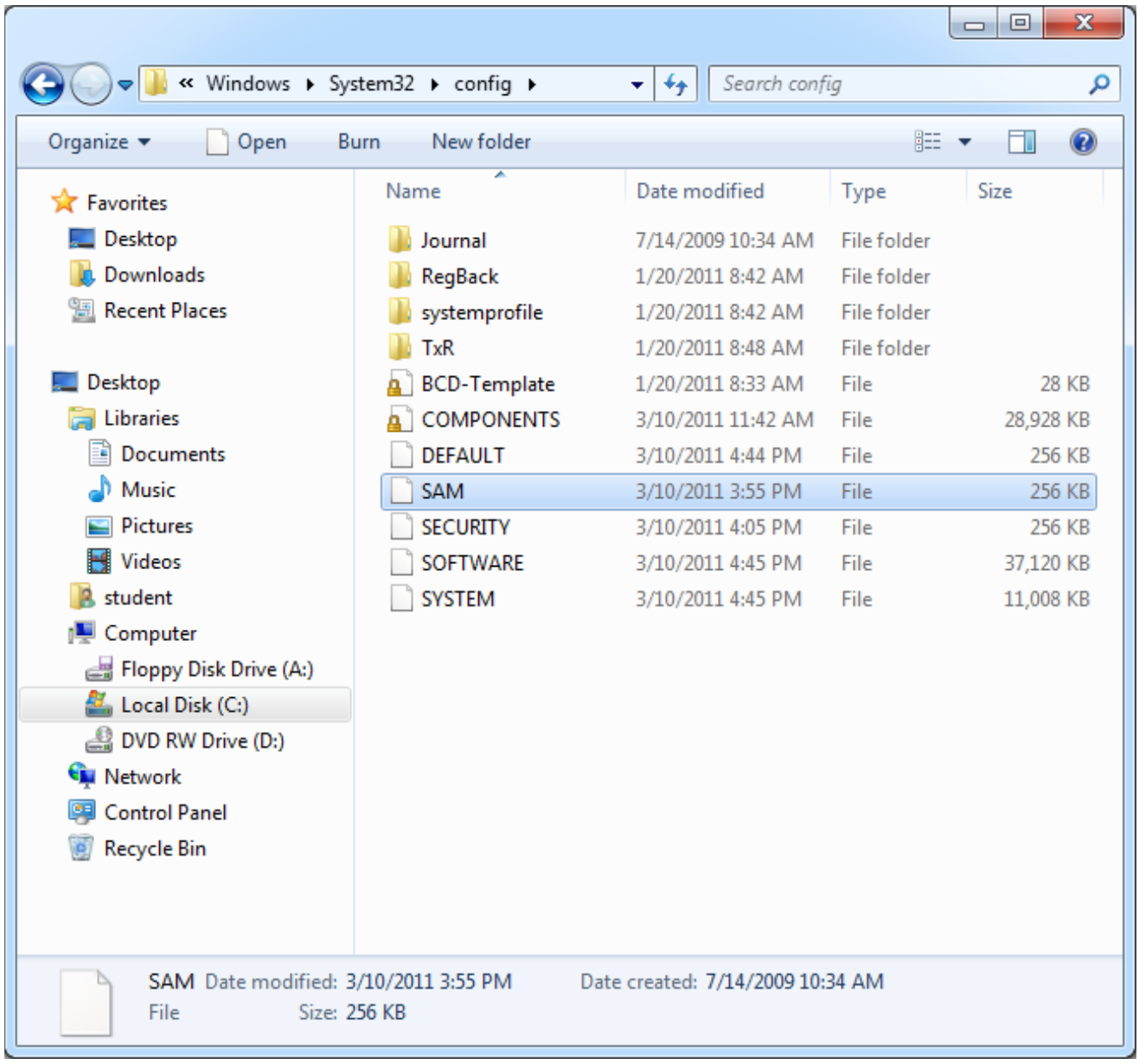
1. The SAM (Security Accounts Manager) file contains the user names and password hashes.

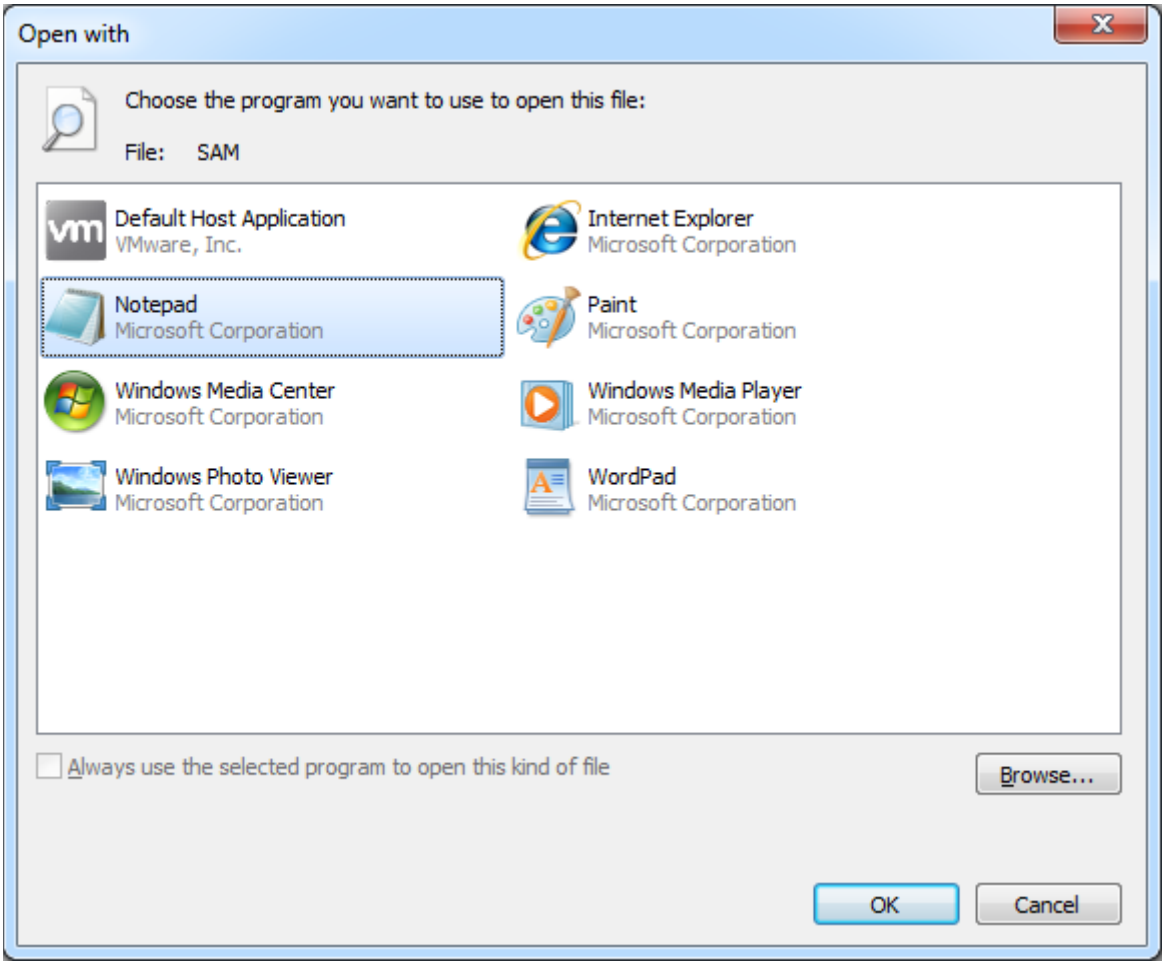
   When you enter your password to login to Windows, the system computes the hash value of your password. This password hash value is checked against the SAM file.

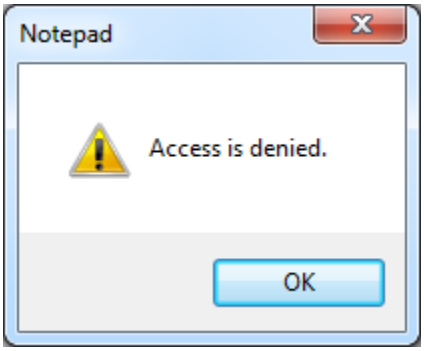
   On Windows 7, the SAM file is located in "C:\WINDOWS\system32\config".

   Try locating the SAM file on your machine.

Question
Are you able to copy the SAM file?







2. The SAM file cannot be copied or moved when Windows is running. But if the machine loads an alternate OS which support NTFS like NTFSDOS or Linux, then the SAM file can copy from the folder.

Exercise 5 - Encrypting File System (EFS)

Encrypting File System (EFS) is a Windows feature for storing information in the hard disk in an encrypted format. It allows a user to encrypt his confidential folders and documents, and a recovery agent (e.g. administrator) to recover the confidential folders and documents.

1 Creating user accounts

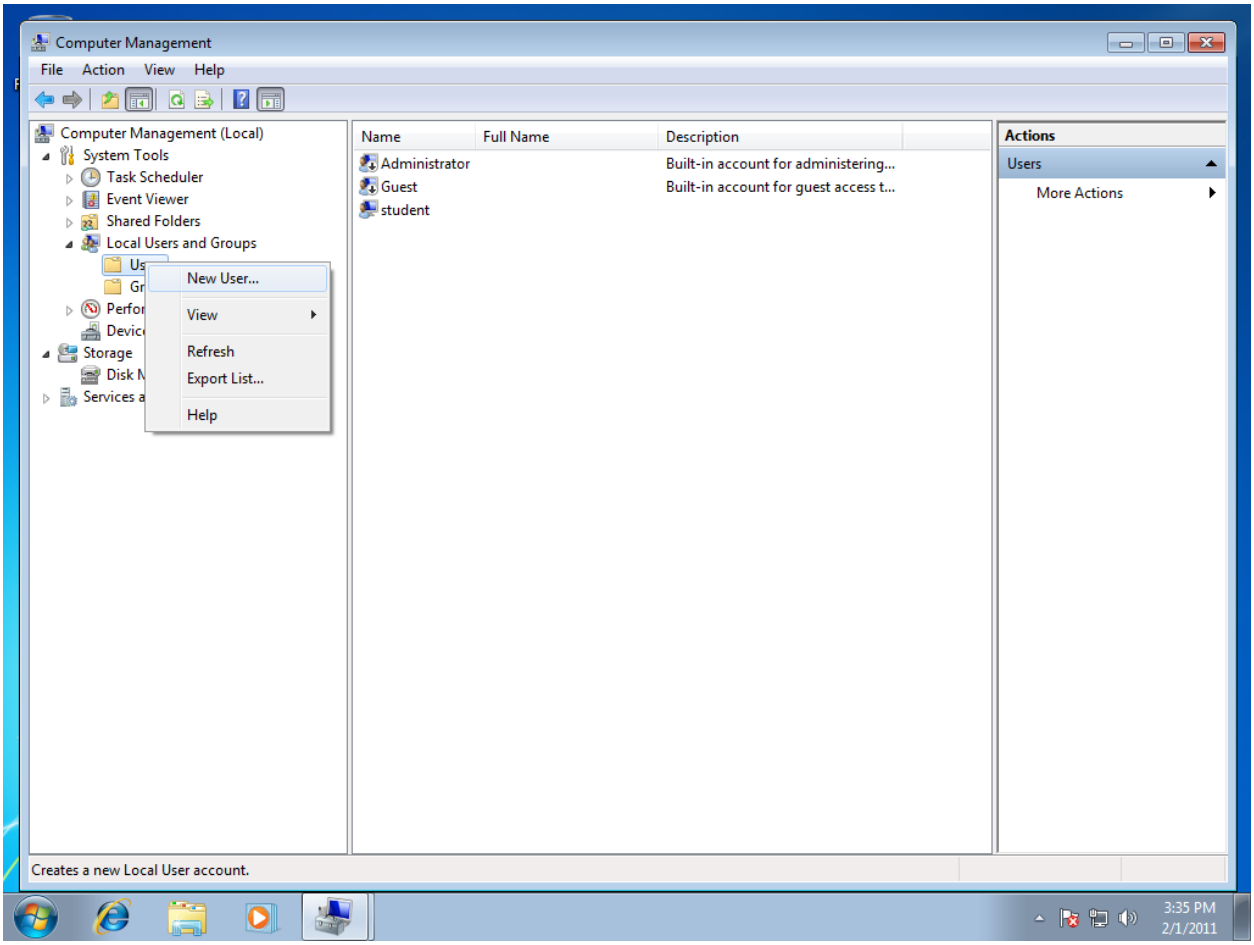
We shall first create two users: "admin1" with Administrator's privilege and "user1" with User's privilege.

Log in to "student" account.

1.1 Creating "admin1" account

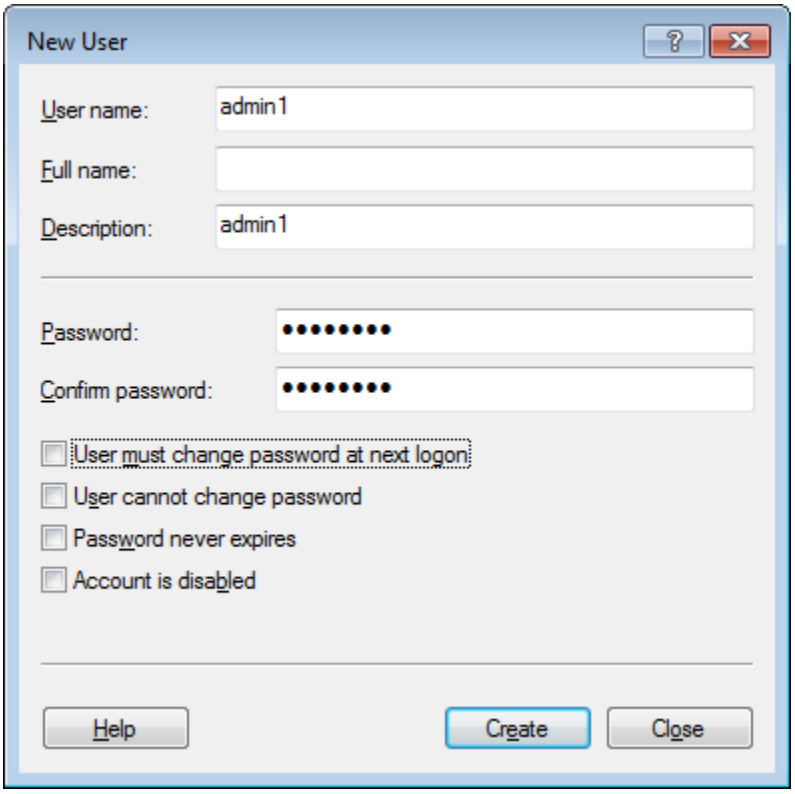
In the Windows search bar at the bottom left, type **compmgmt.msc** to run the Computer Management.

In Computer Management dialog box, right click on System Tools → Local Users and Groups → Users and select New User… to create a new user.

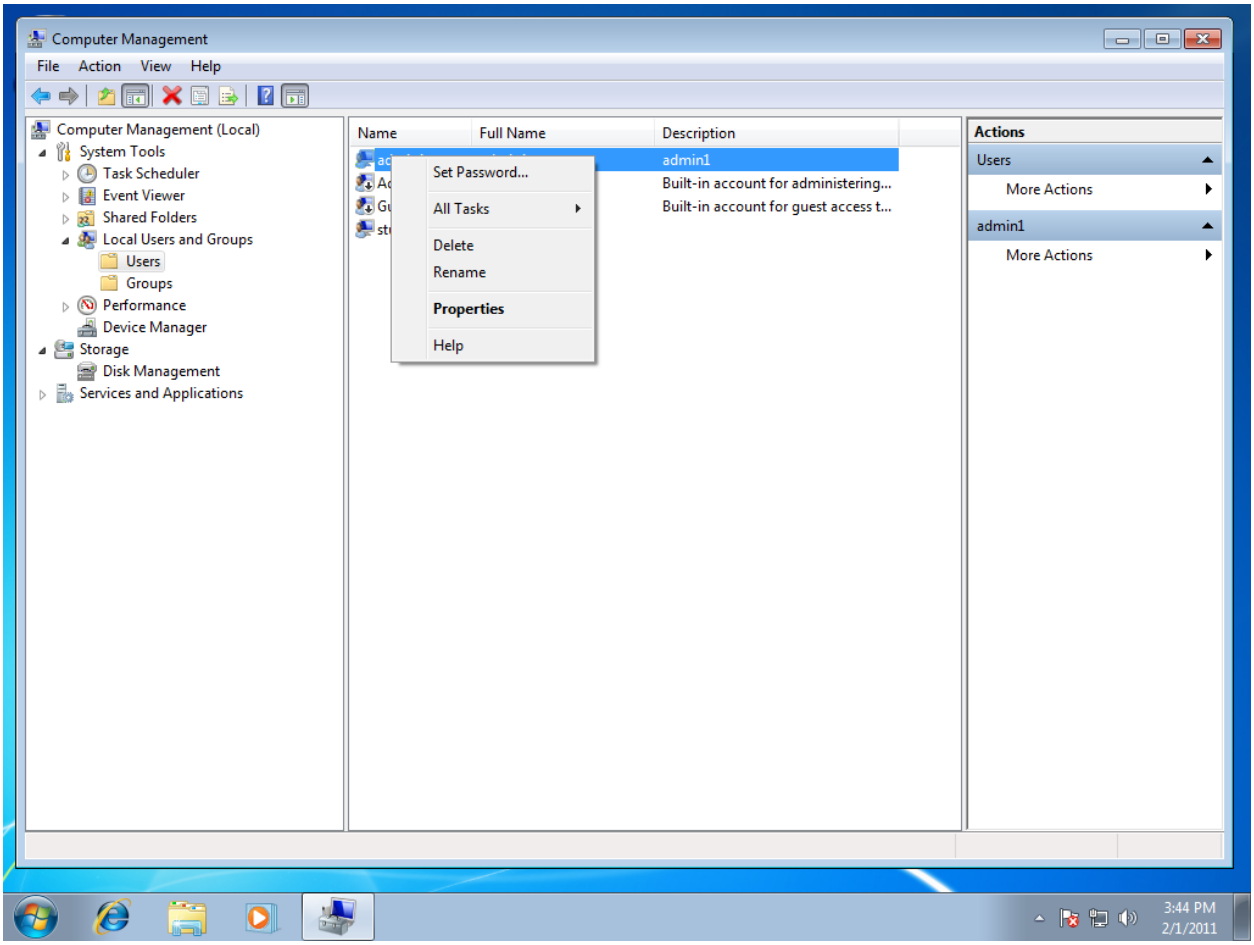


Enter the information for admin1, and click Create button to create admin1 account, followed by Close button.

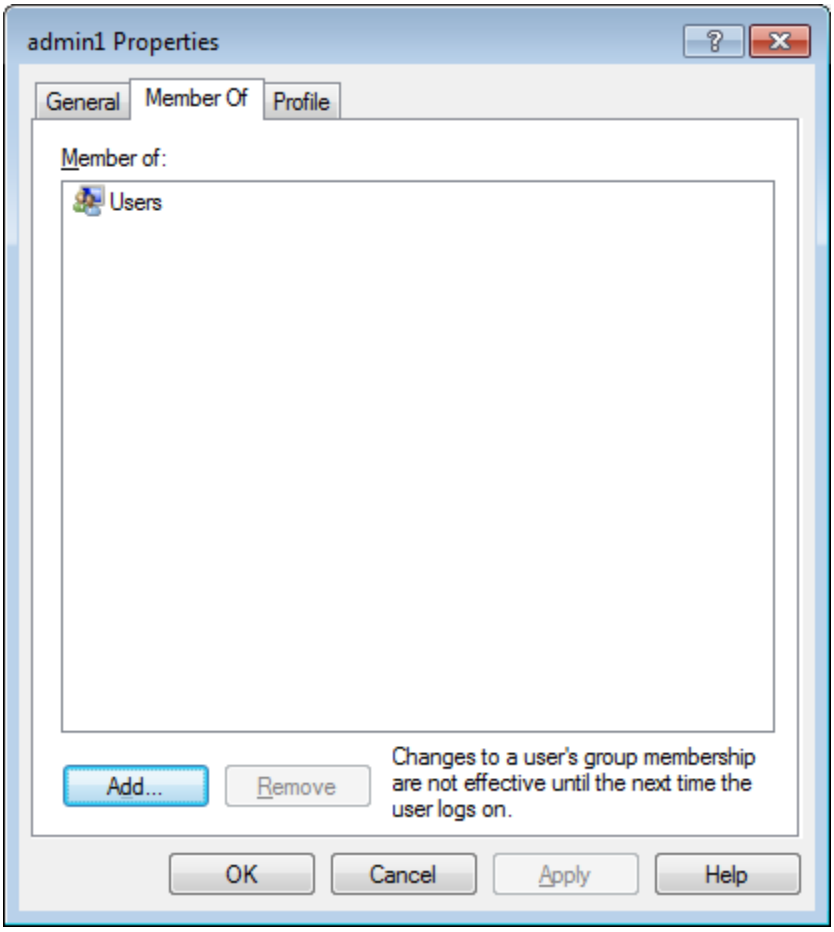
For password, use: p@ssw0rd



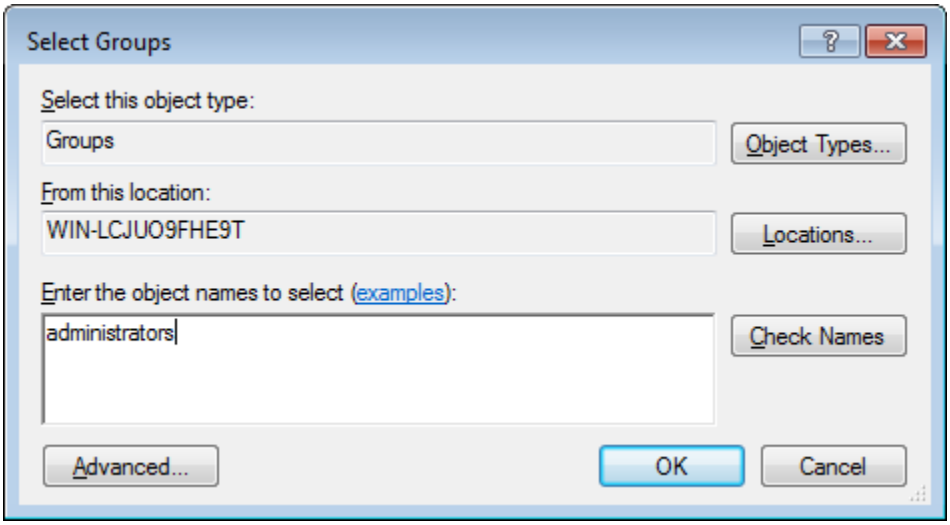
In Computer Management dialog box, right click on admin1 and select Properties.



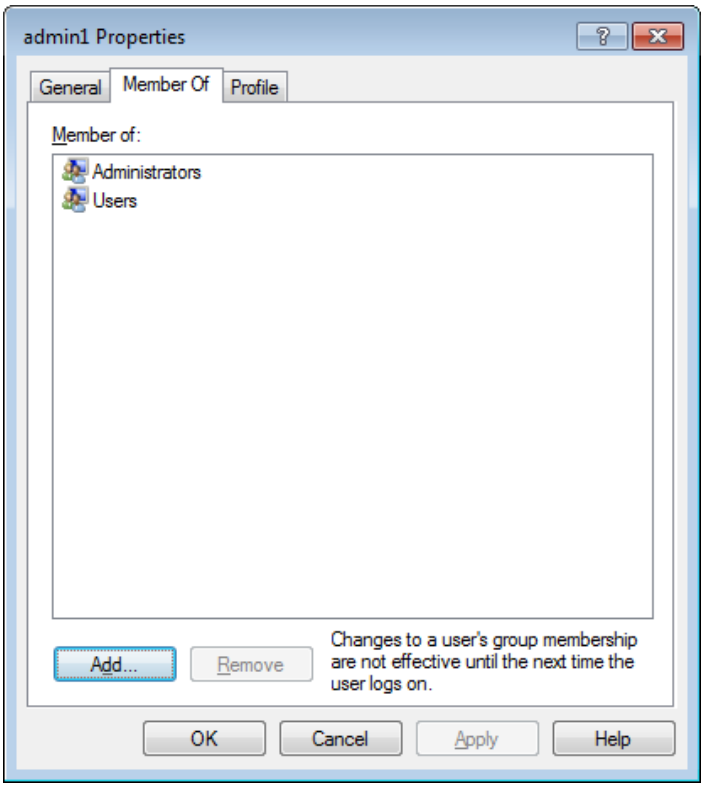
In admin1 Properties dialog box, select Member Of tab, and click Add… button.



In Select Groups dialog box, type "administrators" in the text box and click on OK button to add admin1 to the Administrators group.

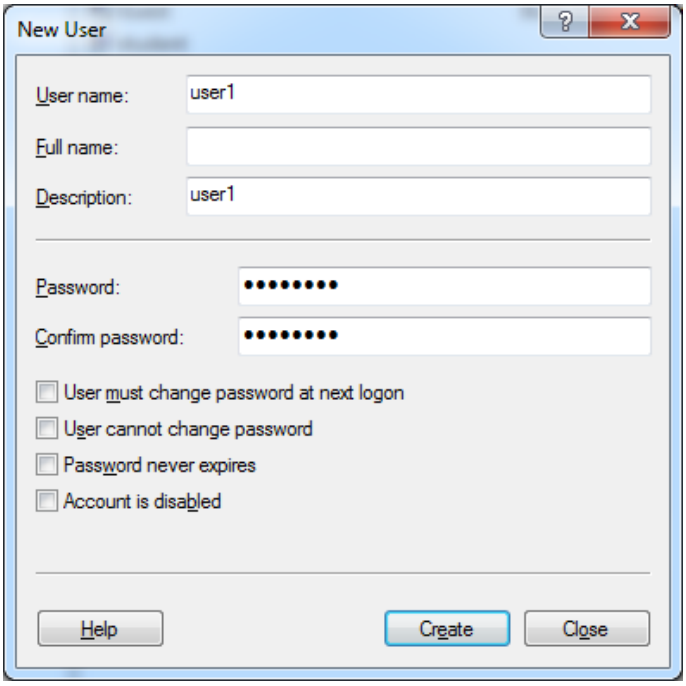


In admin1 Properties, click on OK button. Open admin1 Properties dialog box again and check that admin1 is a member of Administrators group.

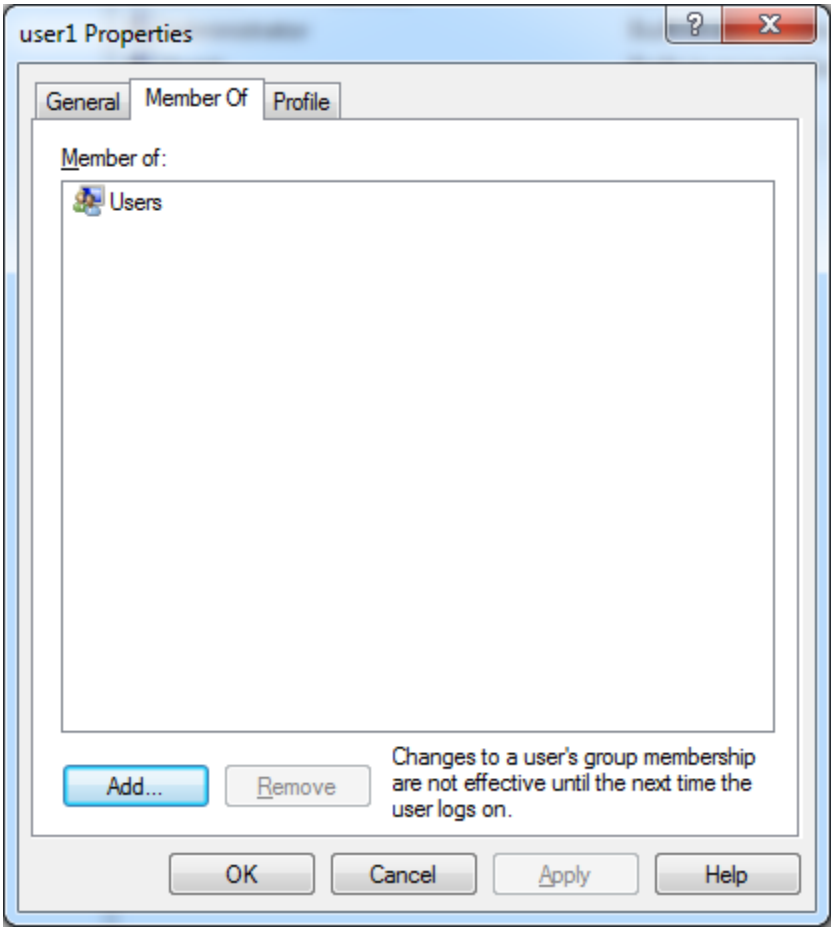


1.2 Creating "user1" account

Create another account called "user1".



By default, user1 is a member of Users goup. Do not add it as a member of Administrators.



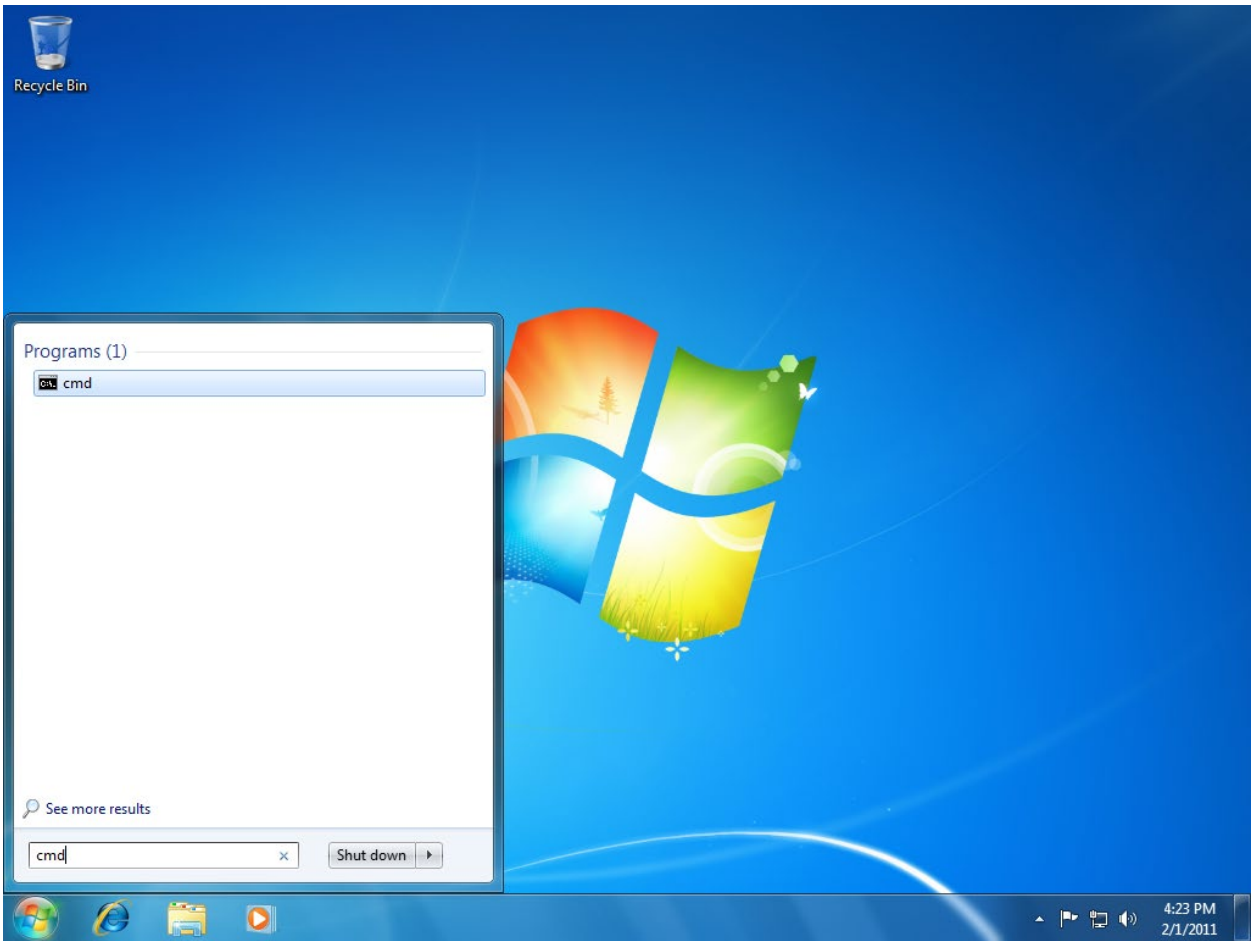
2 Using "cipher" command

In this section, we shall use the "cipher" command to encrypt files and folders.

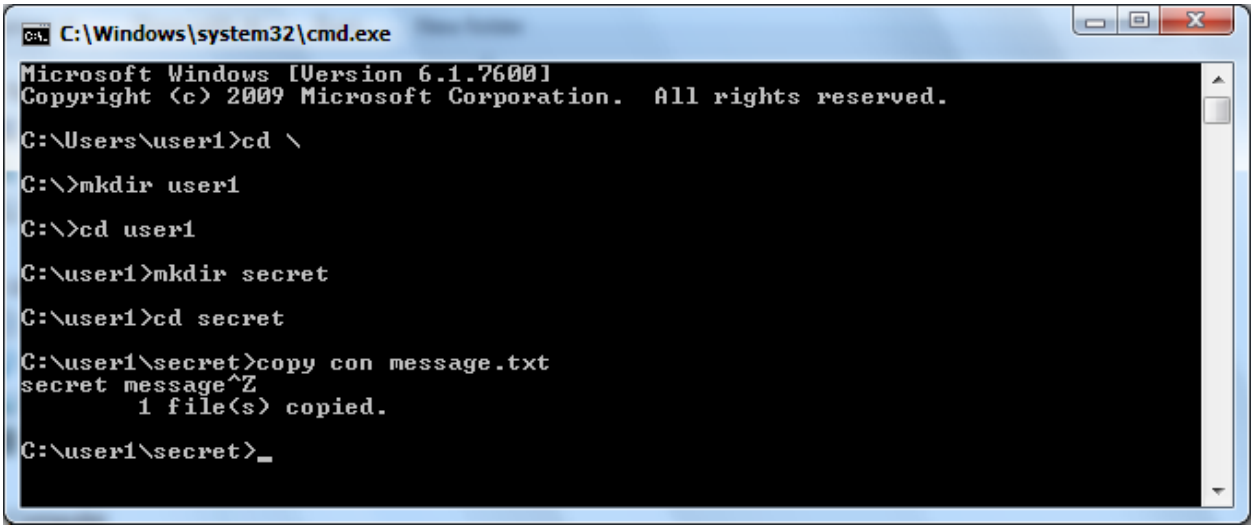
Switch to "user1" account.

Note: In VMware, type control-alternate-insert, and select switch user. Select **user1** and enter the password.

Click Start and enter cmd in the search textbox to start the DOS command interpreter.

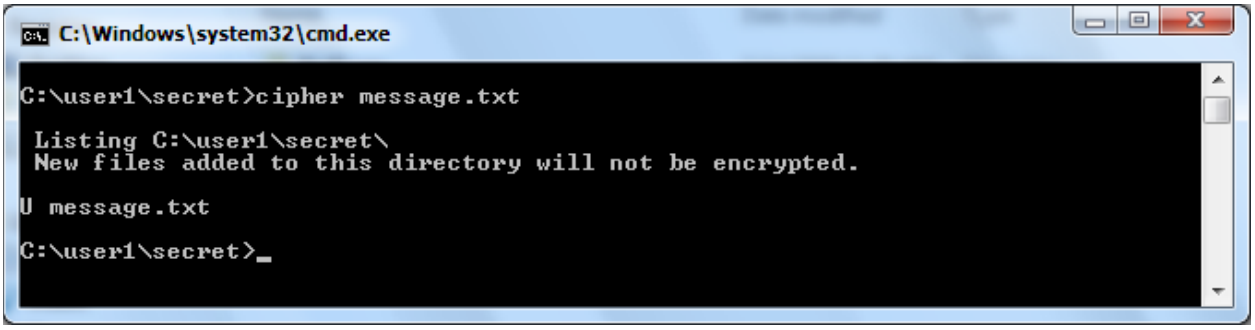


Create a folder c:\user1\secret and a file message.txt inside the folder.

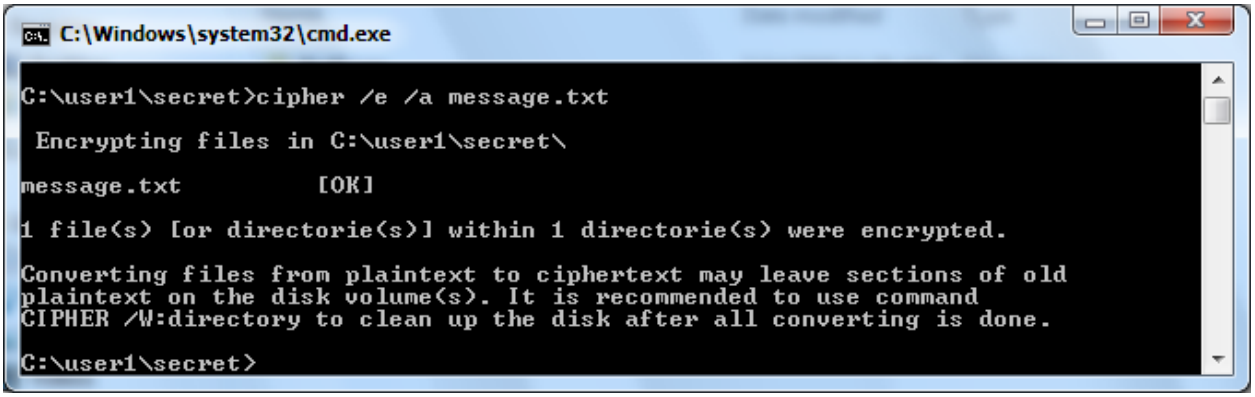


2.1 Encrypting files

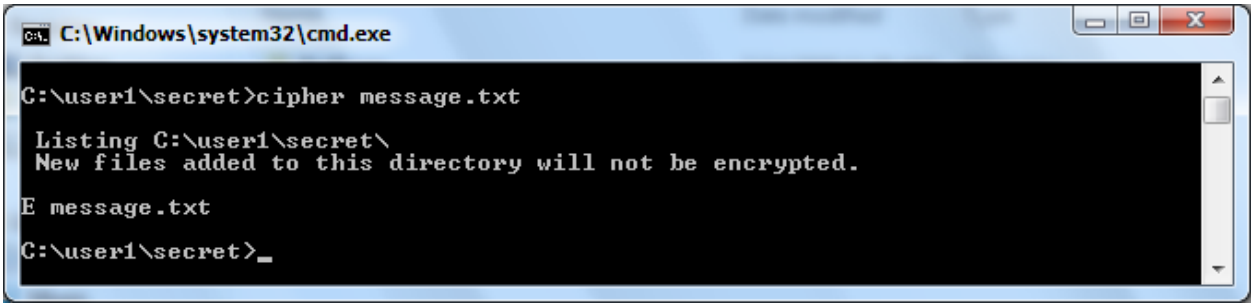
Check if message.txt is encrypted. Prefix "U" indicates it is not encrypted.



Encrypt message.txt.

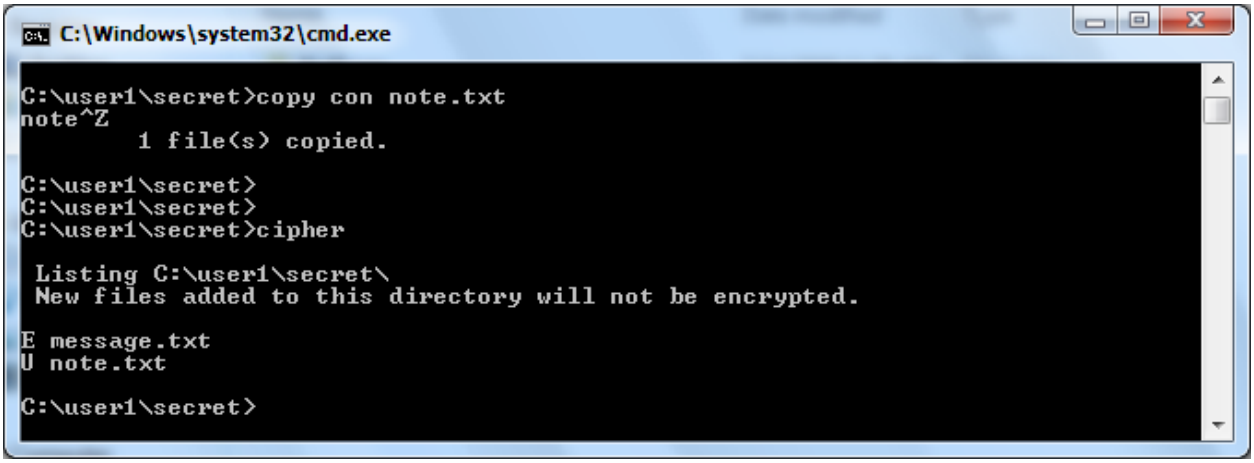


Check the encryption status of message.txt again. Prefix "E" indicates it is now encrypted.

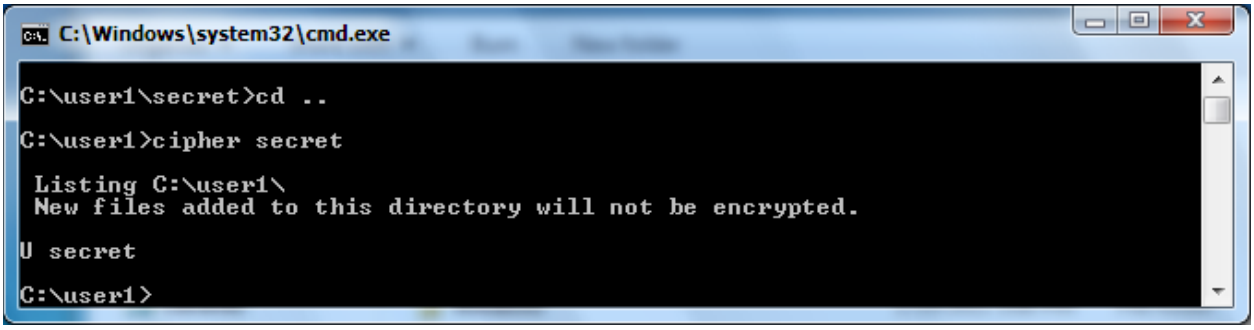


2.2 Encrypting folders

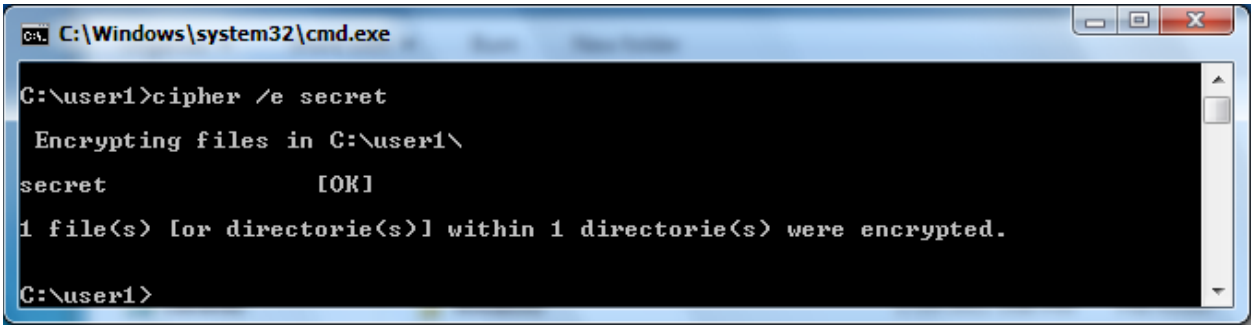
Create another file called note.txt inside the folder, and check its encryption status. Note that note.txt is not encrypted.



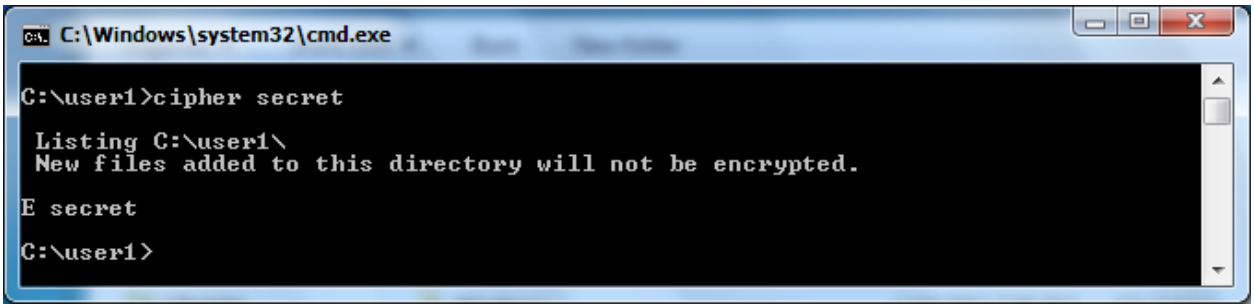
Check the encryption status of c:\user1\secret.



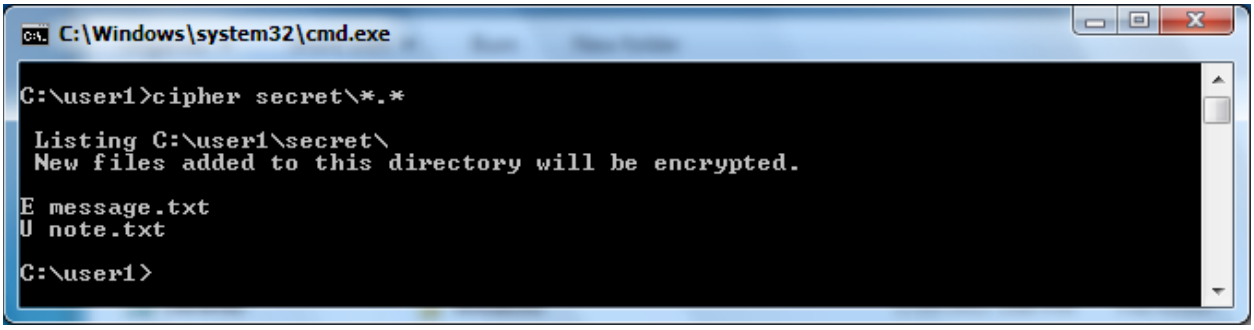
Encrypt the folder c:\user1\secret.



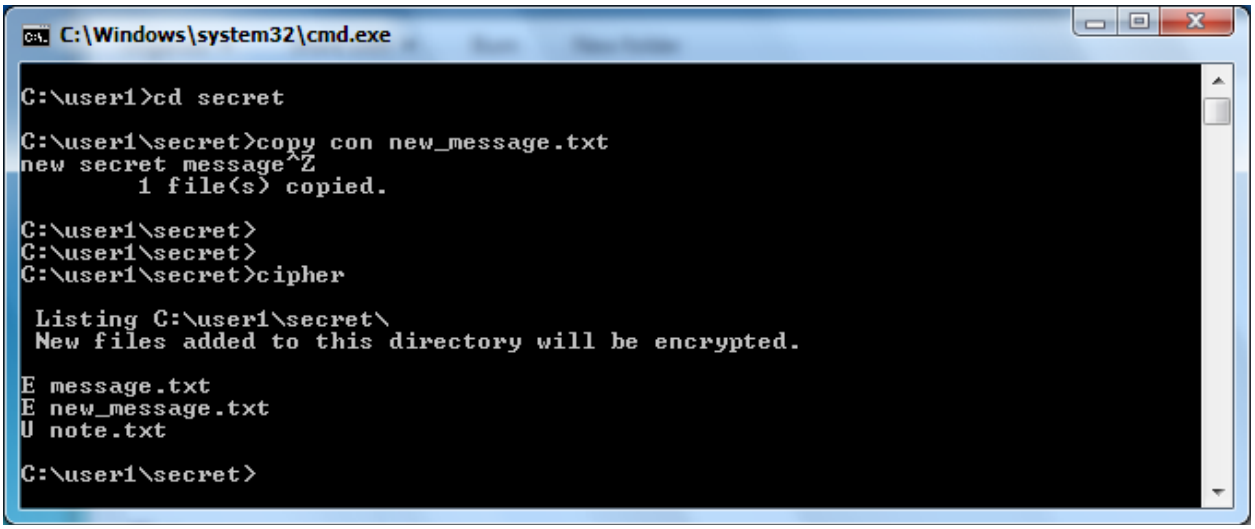
Check the encryption status of the folder again. The prefix "E" indicates it is now encrypted.



Check the encryption status of the files inside the encrypted folder c:\user1\secret. Note there is no change to the status: note.txt remains un-encrypted.



Create a new file new_message.txt in the encrypted folder and check its status. Observe that new_message.txt is encrypted. Note a file newly added to an encypted folder is automatically encrypted.



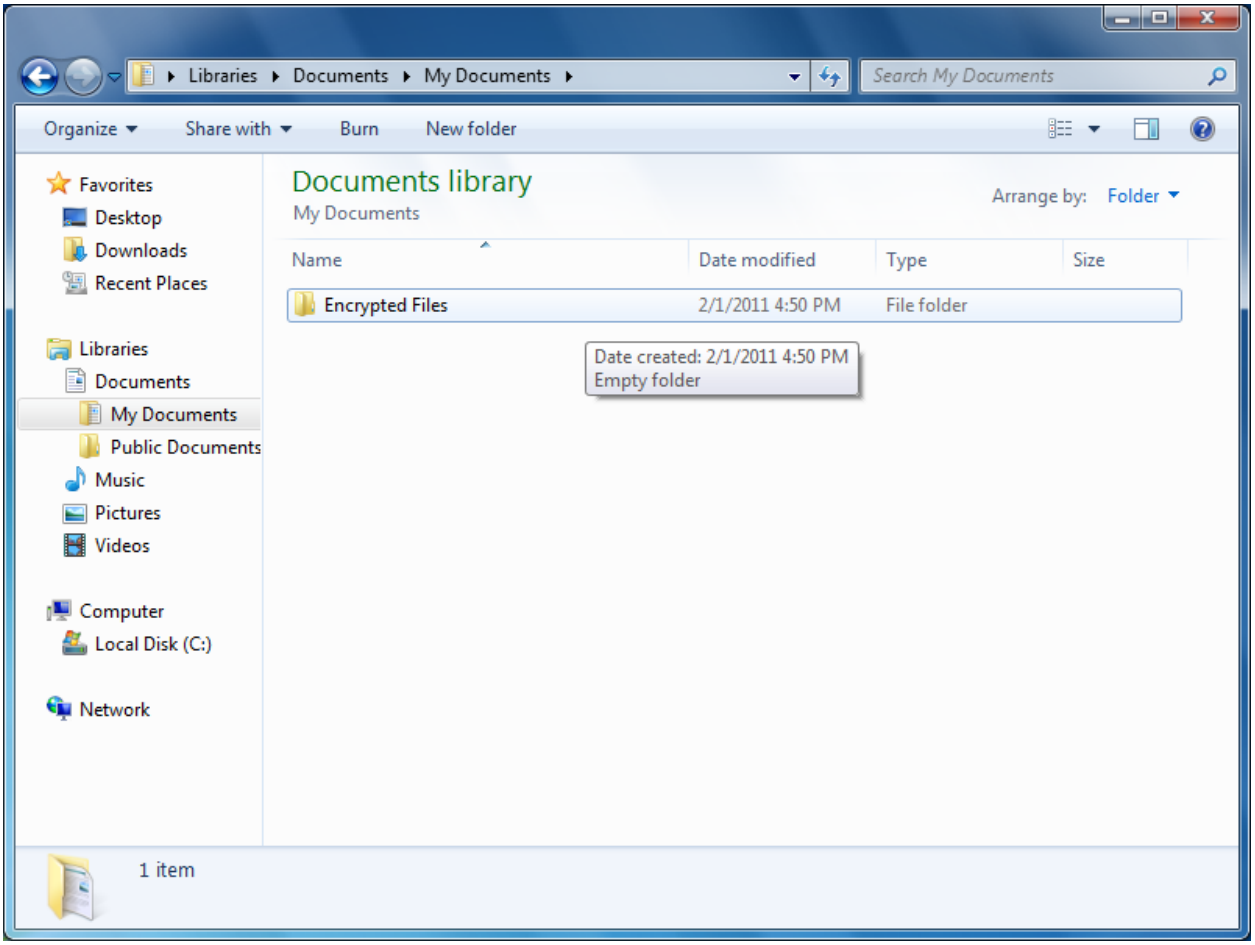
3 User1: using EFS for encryption

Remain logged in as "user1".

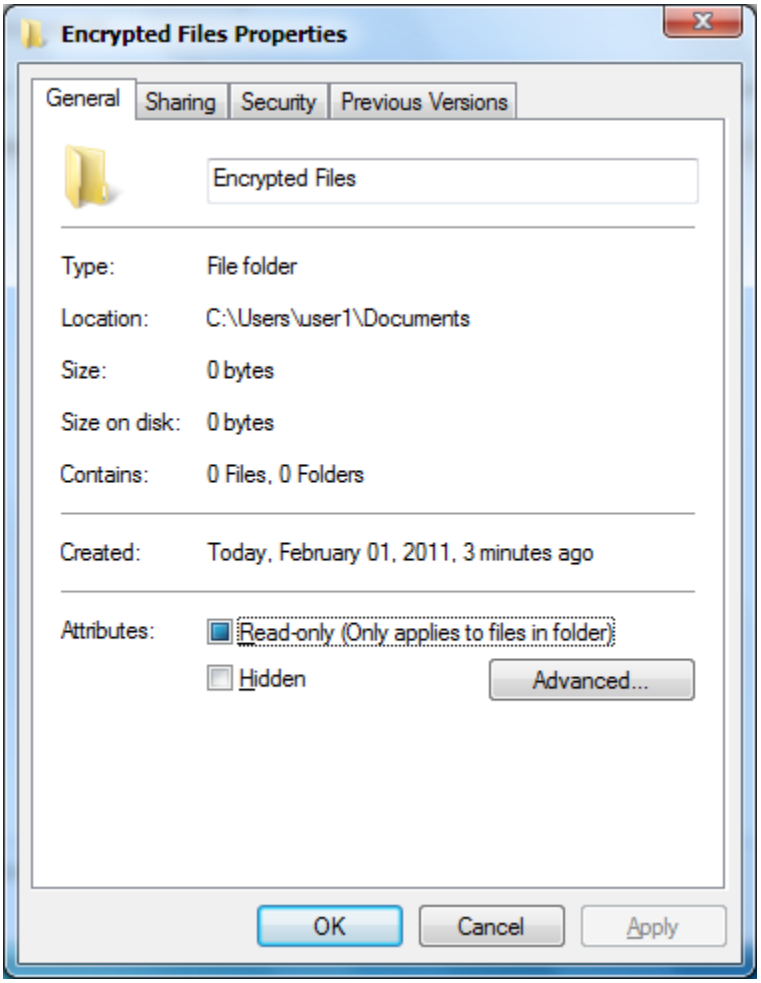
3.1 Encrypting files and folders

In this section, we shall use Windows UI to encrypt a folder and the files inside the folder.

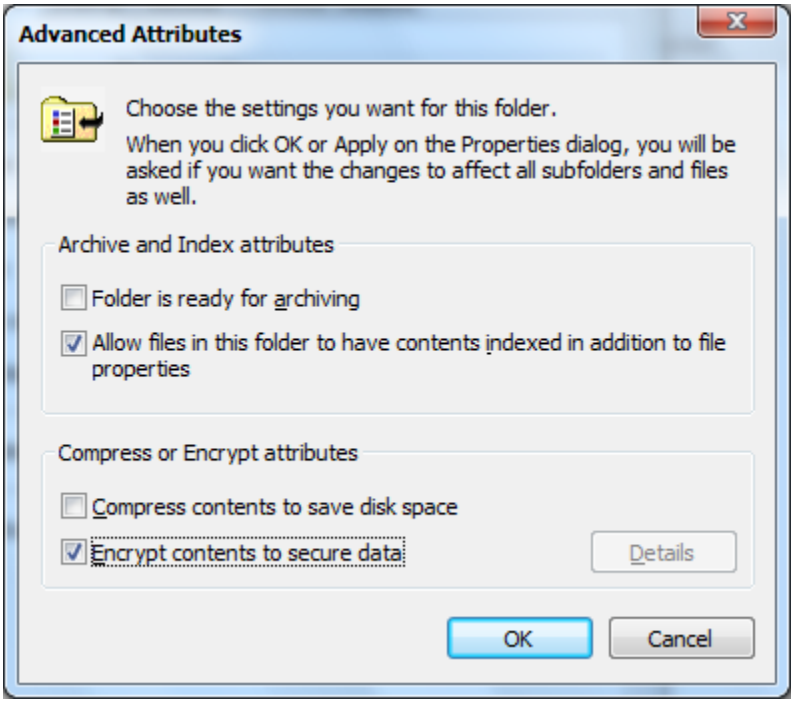
Create a new folder called "Encrypted Files" inside "My Documents" folder.



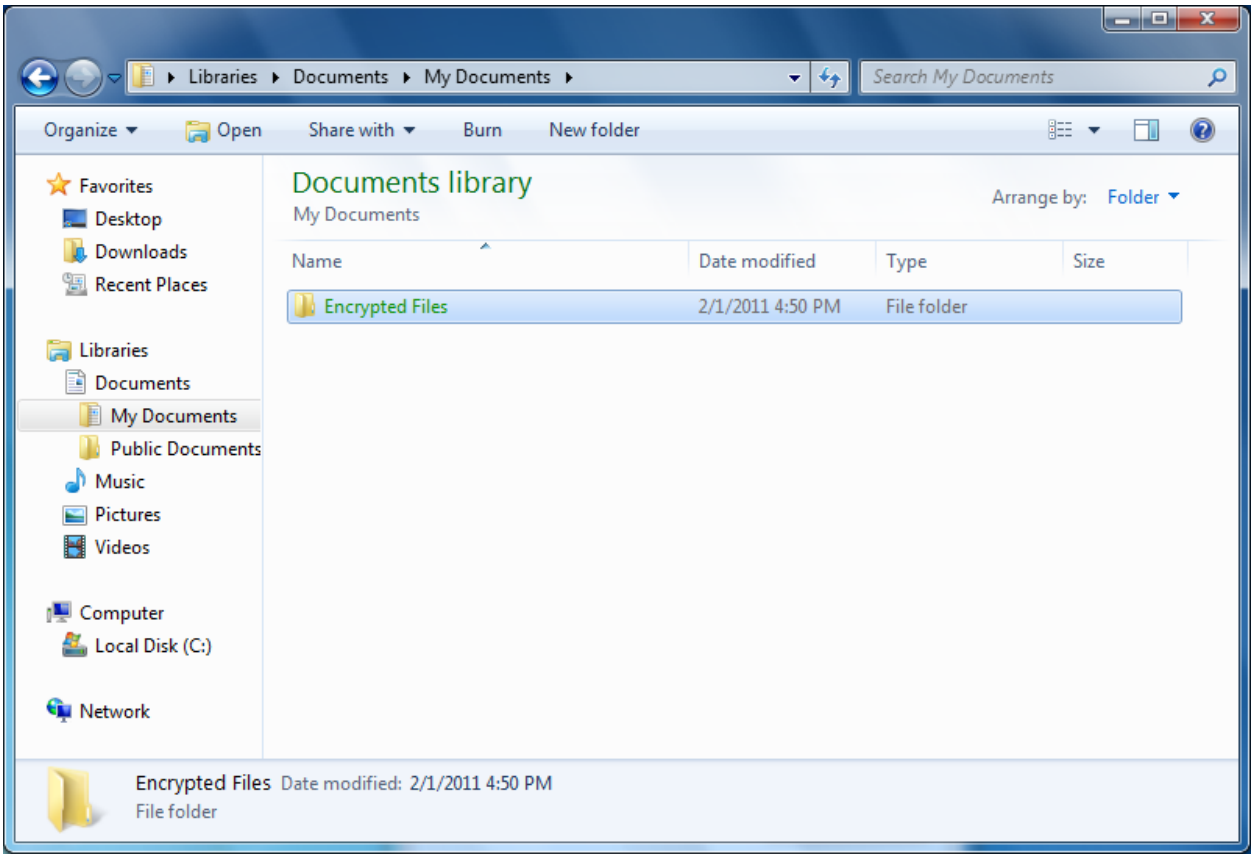
Right click on "Encrypted Files" and select Properties. Click on Advanced… button.



Select the checkbox "Encrypt contents to secure data" and click on OK button.

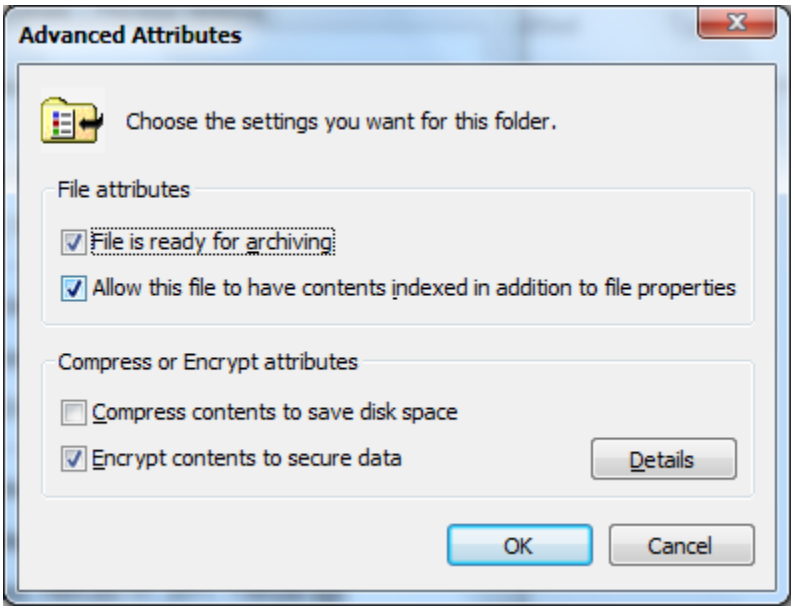


Click on OK button on the Encrypted Files Properties dialog box. The folder is now encrypted.

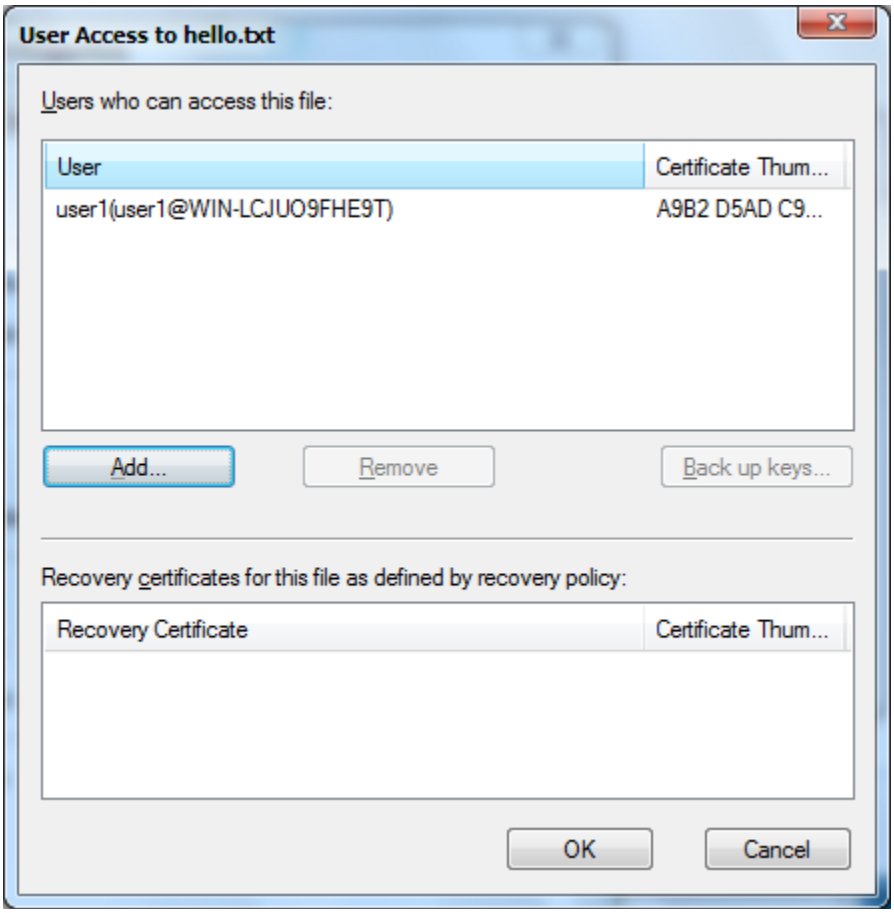


Create a new file called hello.txt inside the encrypted folder, and enter a message "Hello World!" and save it. Note the file name "hello.txt" is also in green colour.

Right click on hello.txt and select Properties. Click on Advanced button and observed that the checkbox "Encrypt contents to secure data" is checked.



Inside Advanced Attributes dialog box, click on Details button. Note user1 can access the file, but no recovery certificate is present.



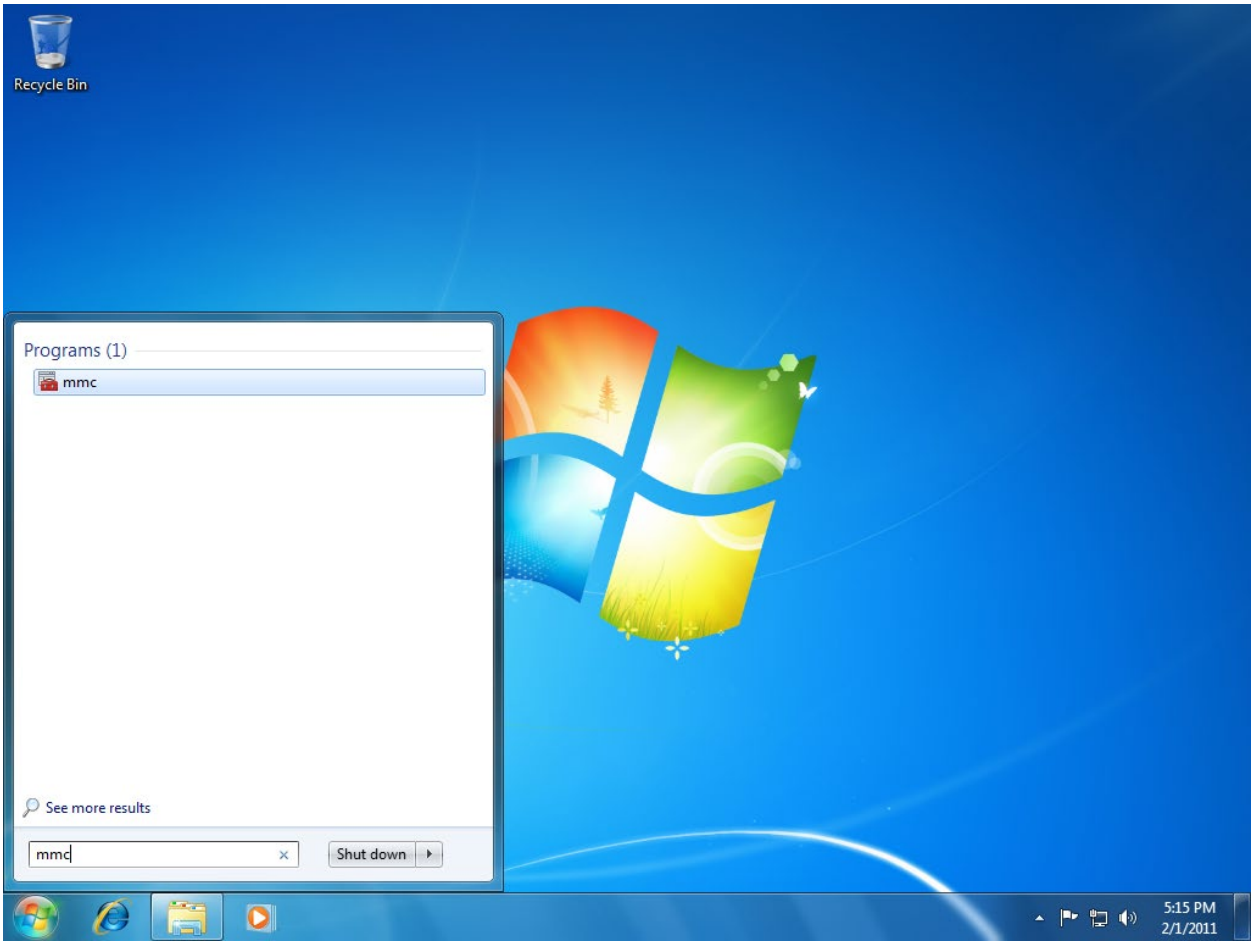
Click on Cancel buttons to close all the opened dialog boxes.

3.2 Exporting user1's private key

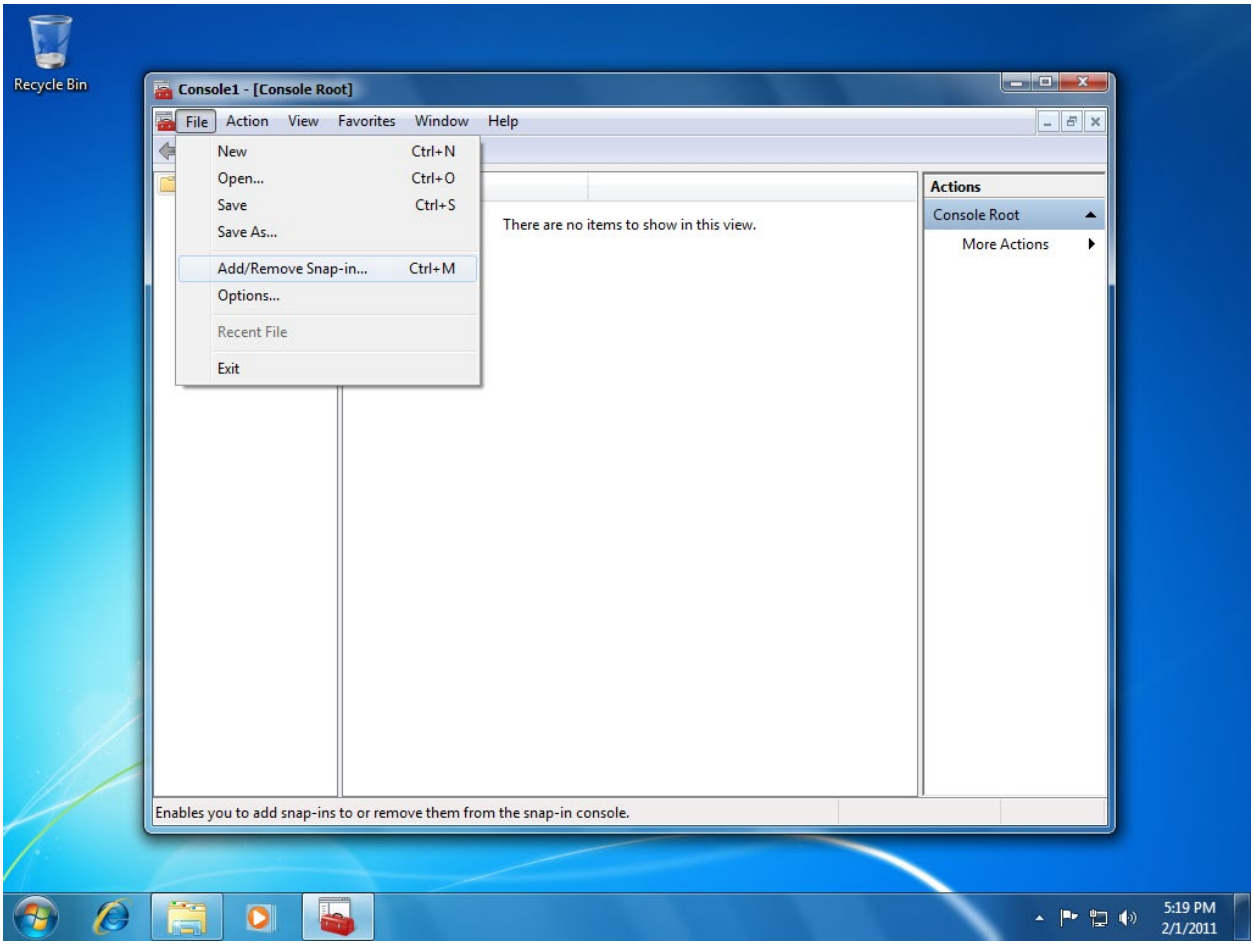
An organization may require the users of EFS to export their keys (private keys) and certificates. The administrators can then use the users' keys for recovery of the encrypted folders and files where appropriate.

In this section, we shall use the Microsoft Management Console (MMC) to export user1's private key.

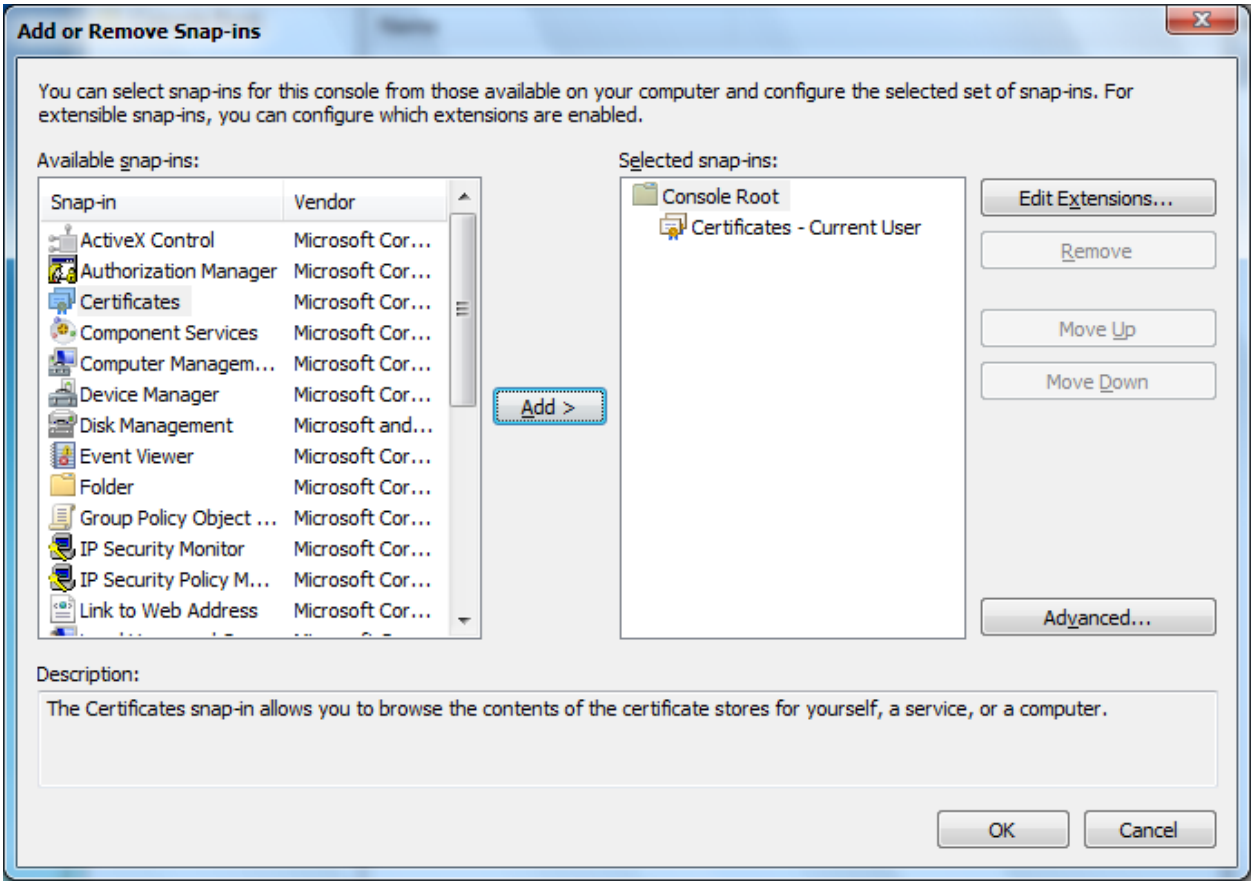
Click Start and enter mmc to run the MMC.



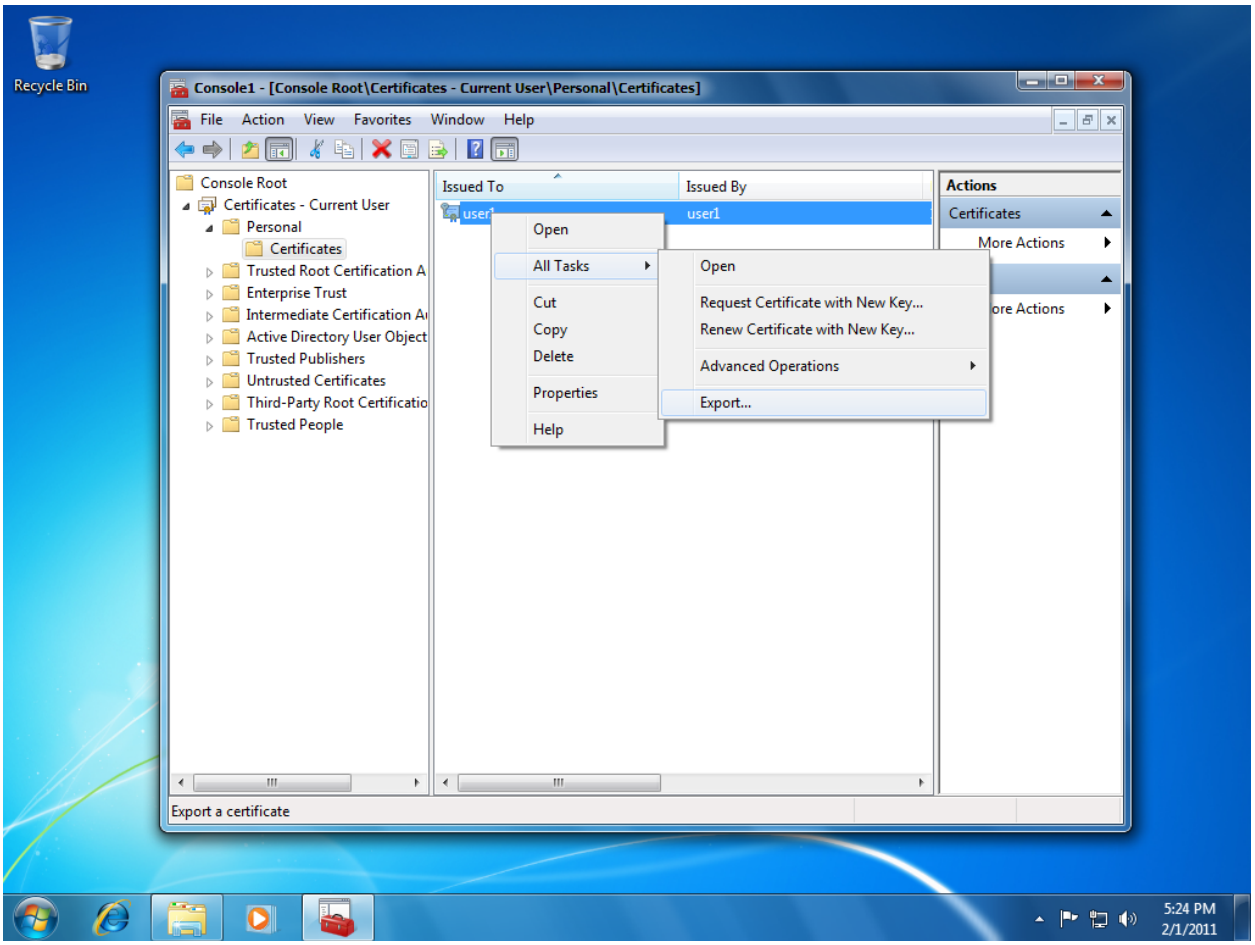
Selelect File → Add/Remove Snap-in…



In Add or Remove Snap-in dialog box, select Certificates and click on Add> button. Then, click on OK button.

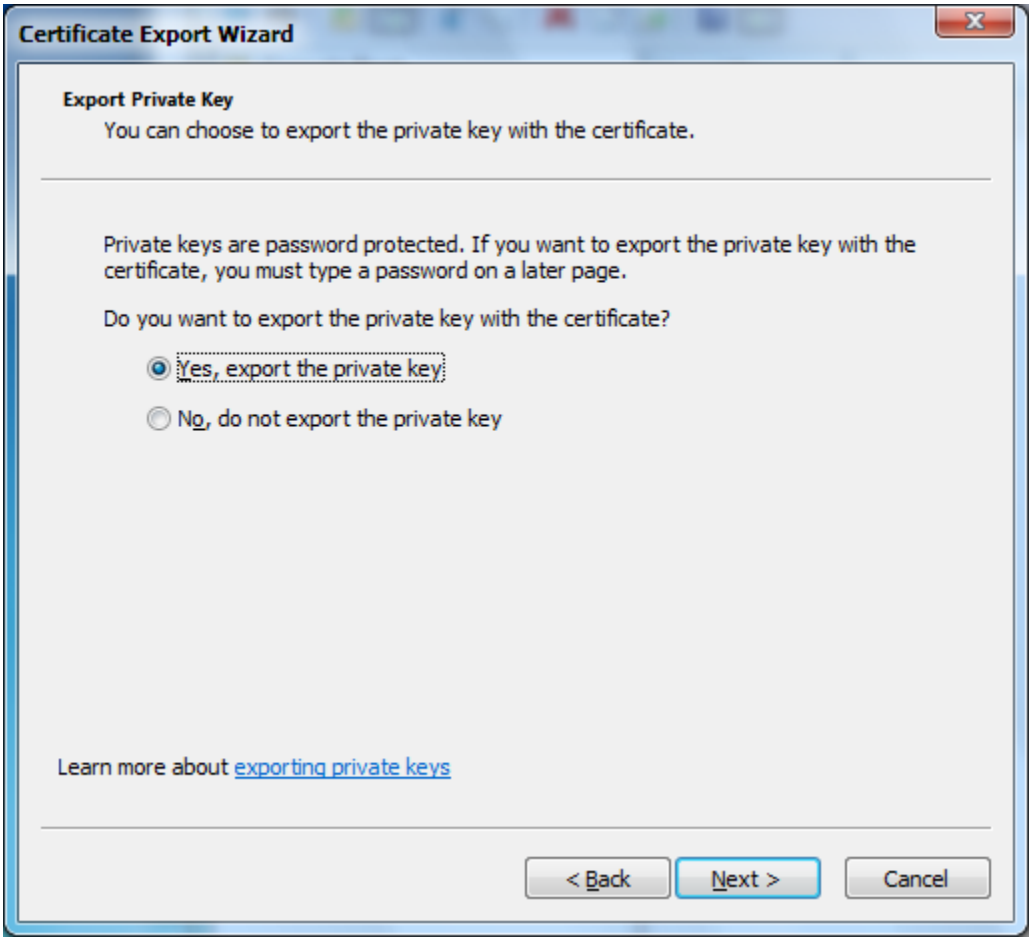


In MMC Console dialog, right click on user1, and select All Tasks → Export… to run the Certificate Export Wizard.

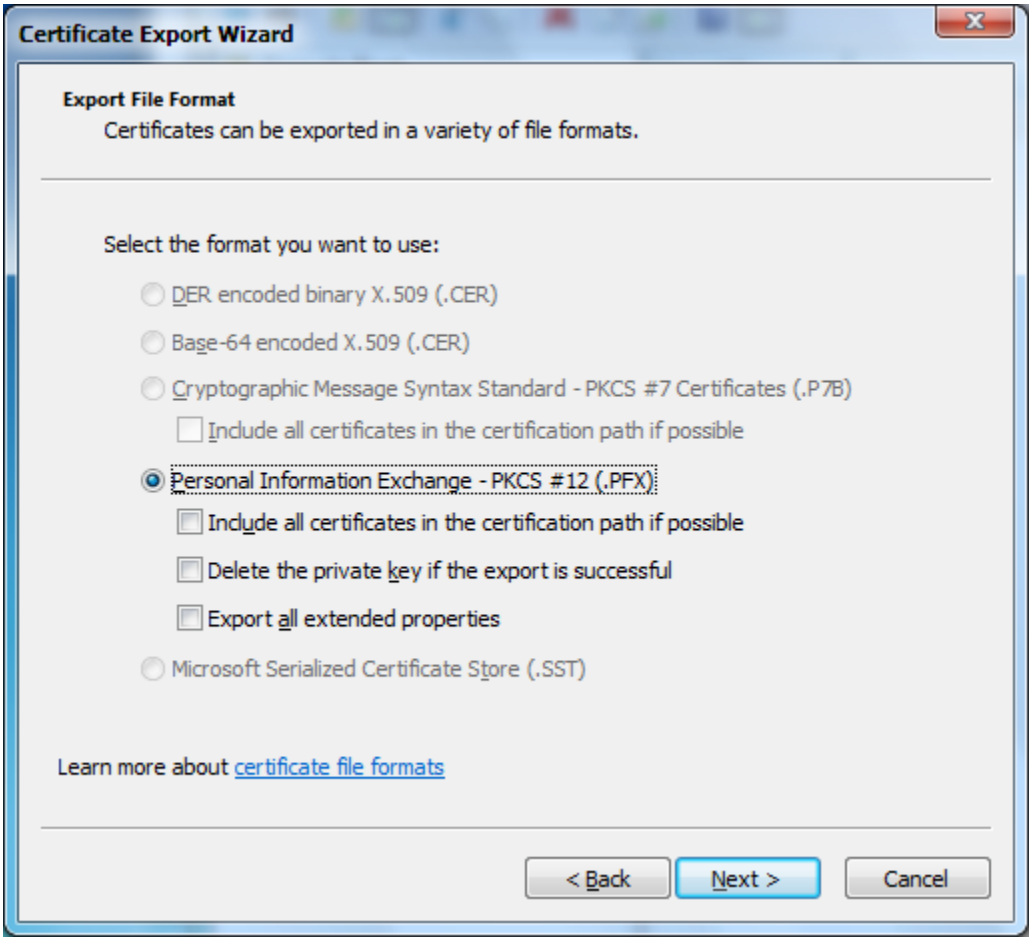


Click on Next> button in the wizard.

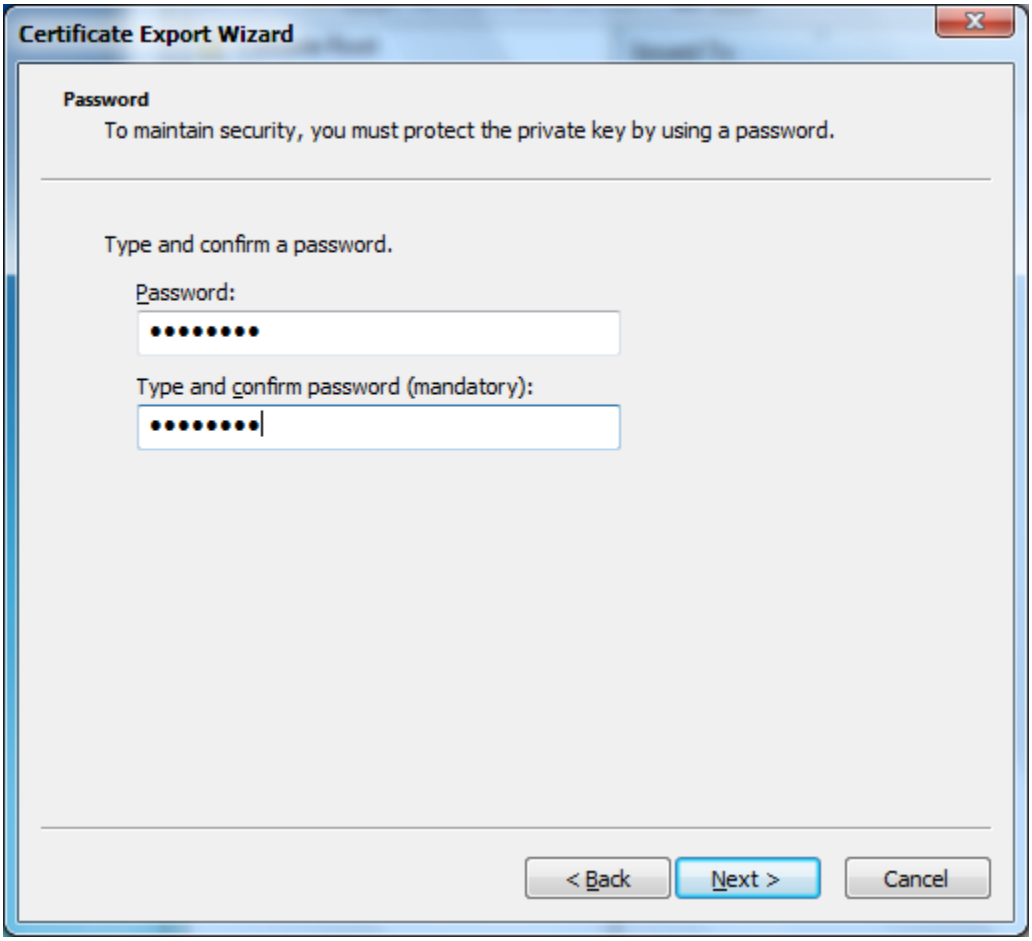
Select “Yes, export the private key” radio button, and click on Next> button.



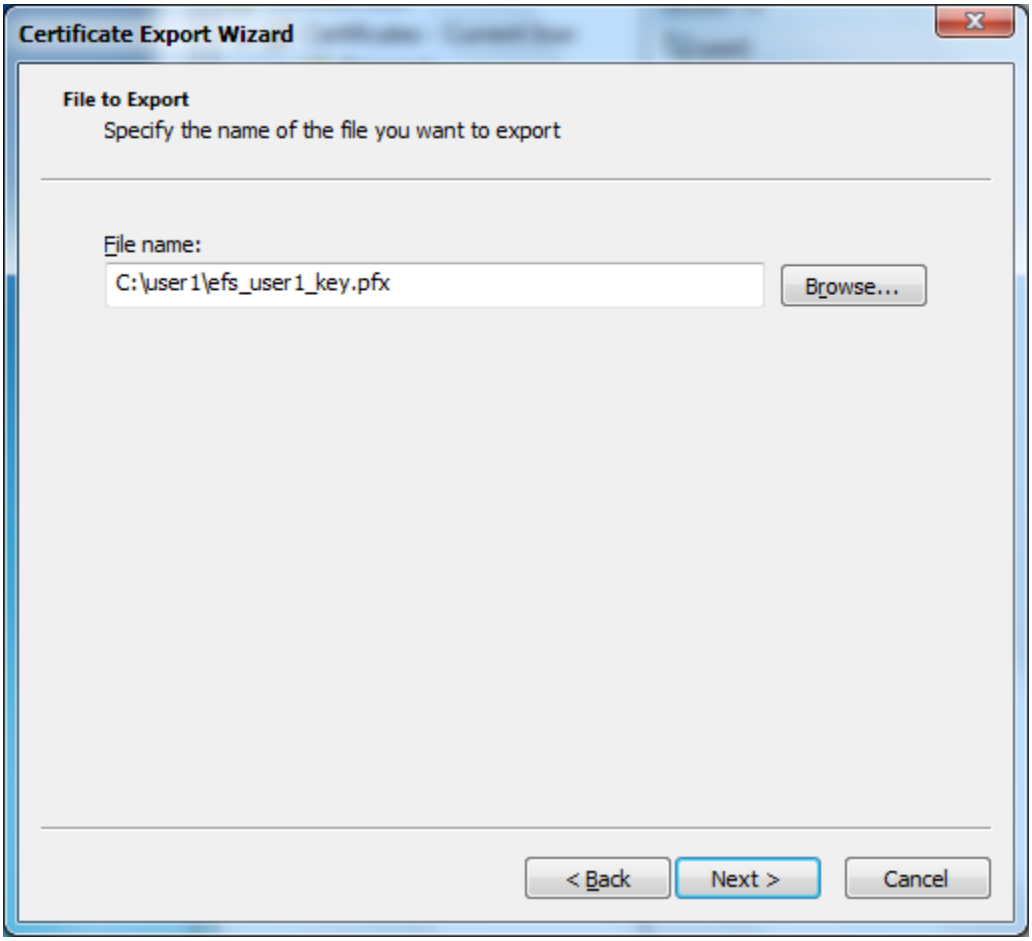
Select Personal Information Exchange – PKCS #12 (.PFX) radio button and click on Next> button.



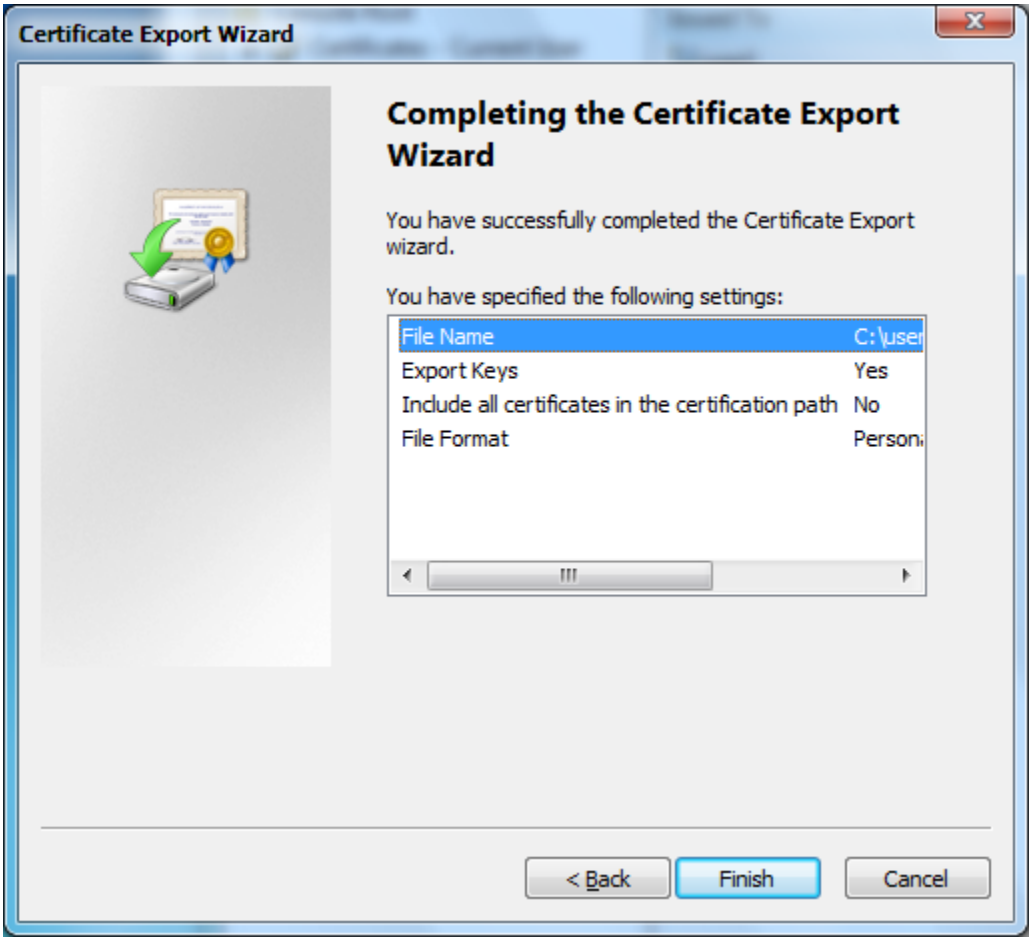
Enter “password” to protect the private key, and click on Next> button.



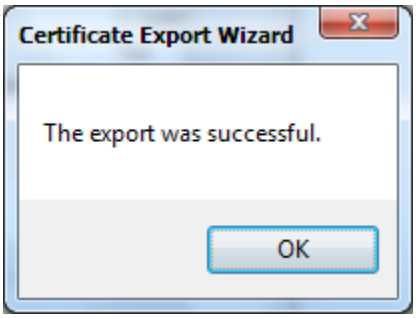
Enter a file name to store user1's key, and click Next> button.



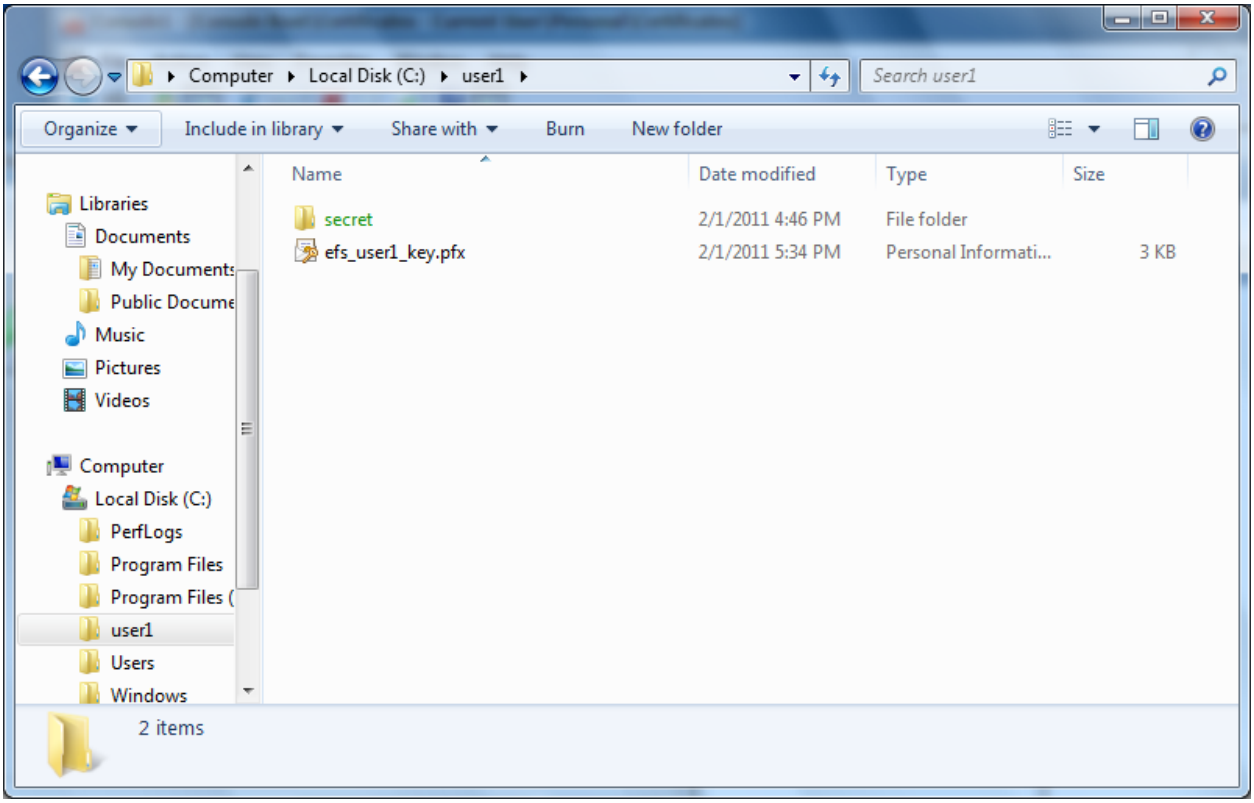
Click on Finish button.



The following dialog box indicates the certificate is successfully exported.



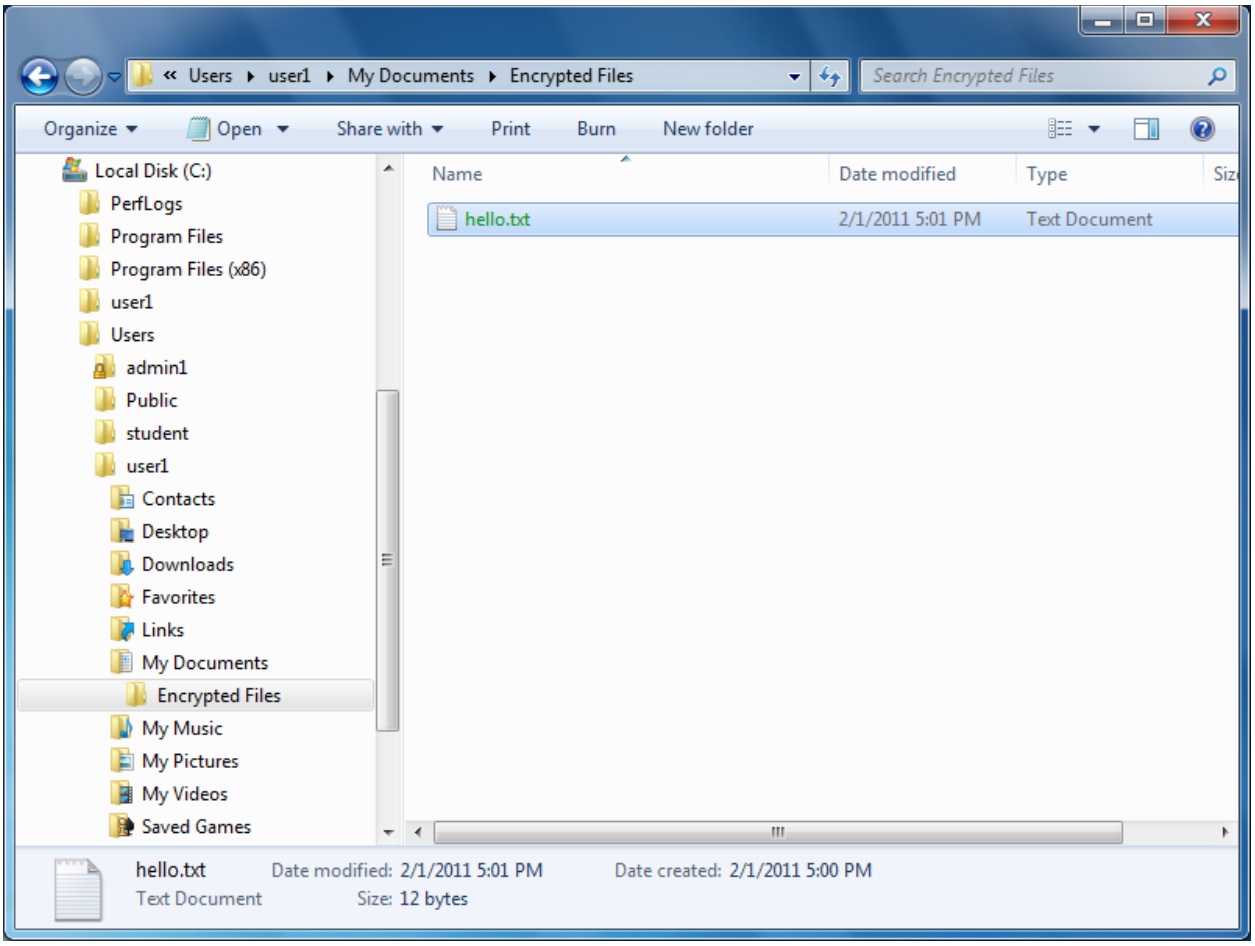
Check that the certificate, efs_user1_key.pfx, is created in the folder.



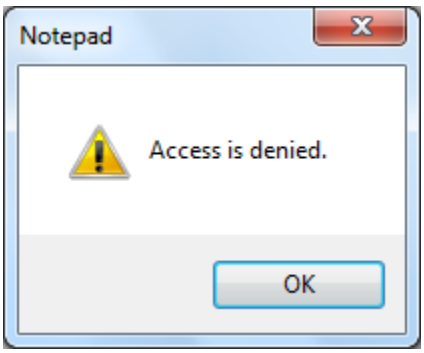
4 Admin1: configuring admin1 as a recovery agent

In this section, we shall configure admin1 as a recovery agent so that it can recover files encrypted by user1.

Switch to **admin1** account, and try opening hello.txt in the encrypted folder of user1.



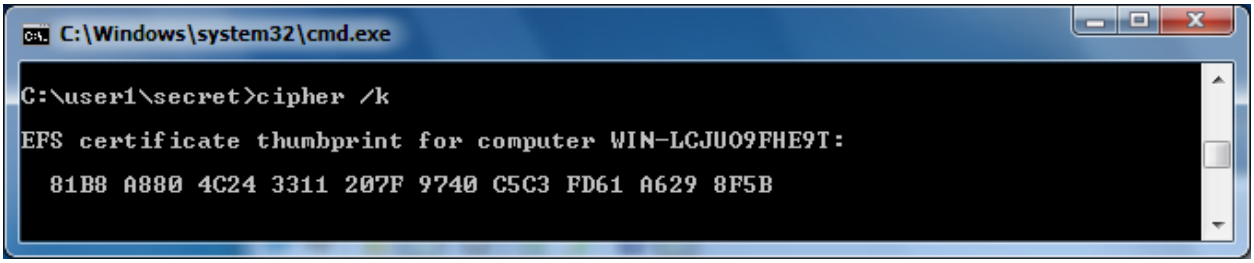
Note you have no access to the file as it is encrypted by user1.



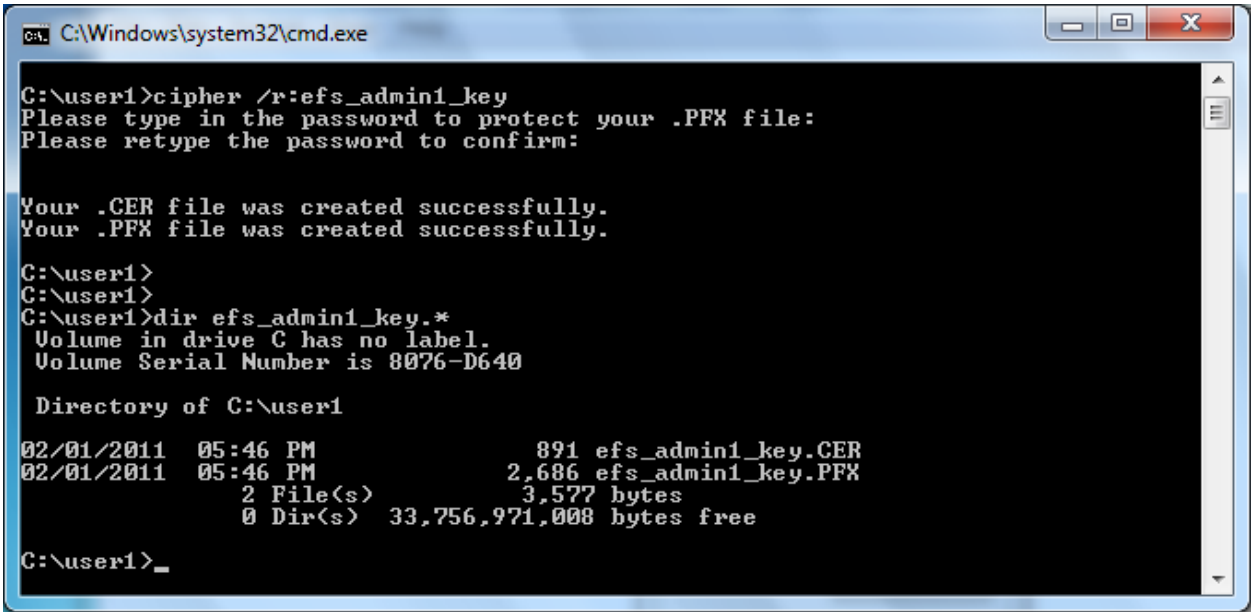
4.1 Generating recovery agent's certificate and key

We need to create recovery agent's certificate and key for admin1.

Create an EFS certificate for admin1.



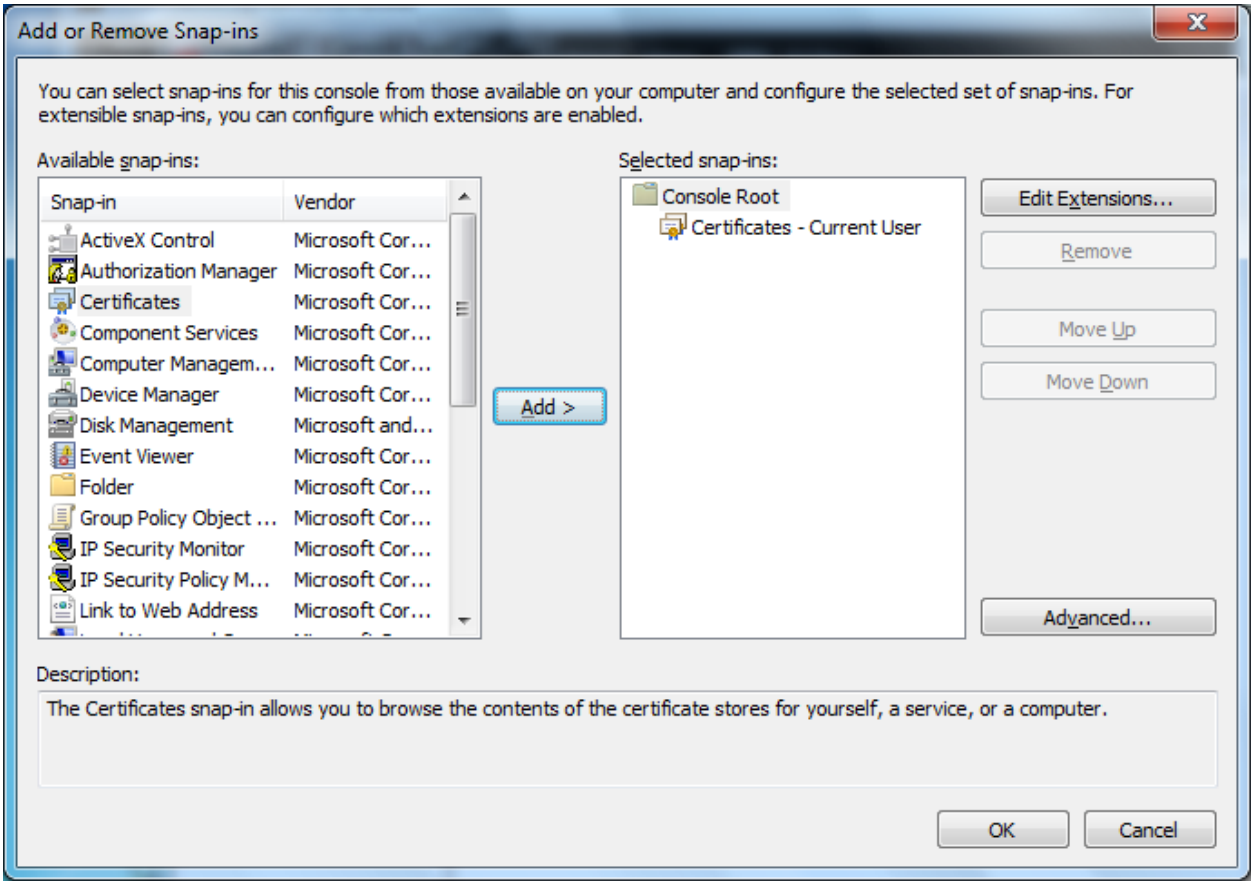
Generate recovery agent's certificate (efs_admin1_key.cer) and key (efs_admin1_key.pfx).



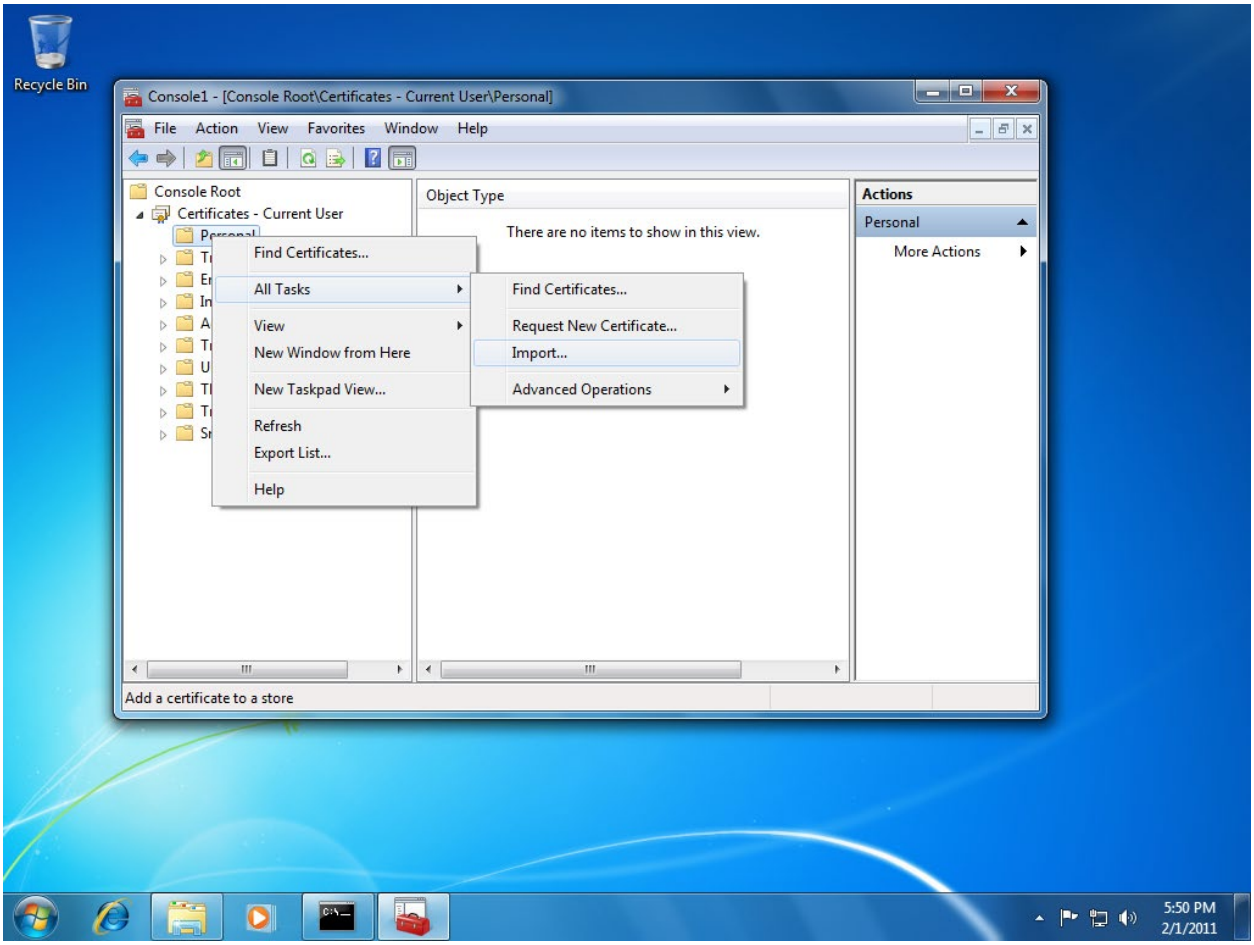
4.2 Importing recovery agent's certificate

Next, we need to import the recovery agent's certificate.

Run MMC and add the Certificates snap-in.

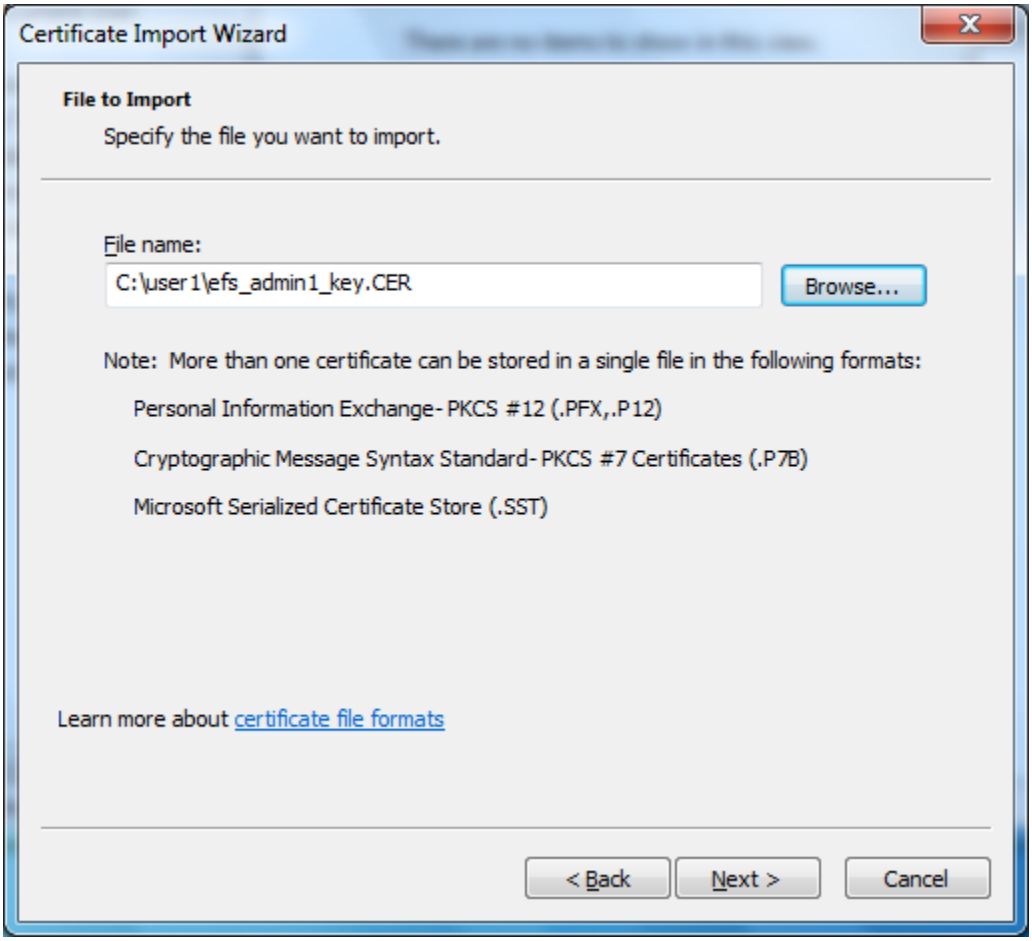


In the MMC Console, right-click on Console Root → Certificates – Current User → Personal → All Tasks and select Import… to run the Certificate Import Wizard.

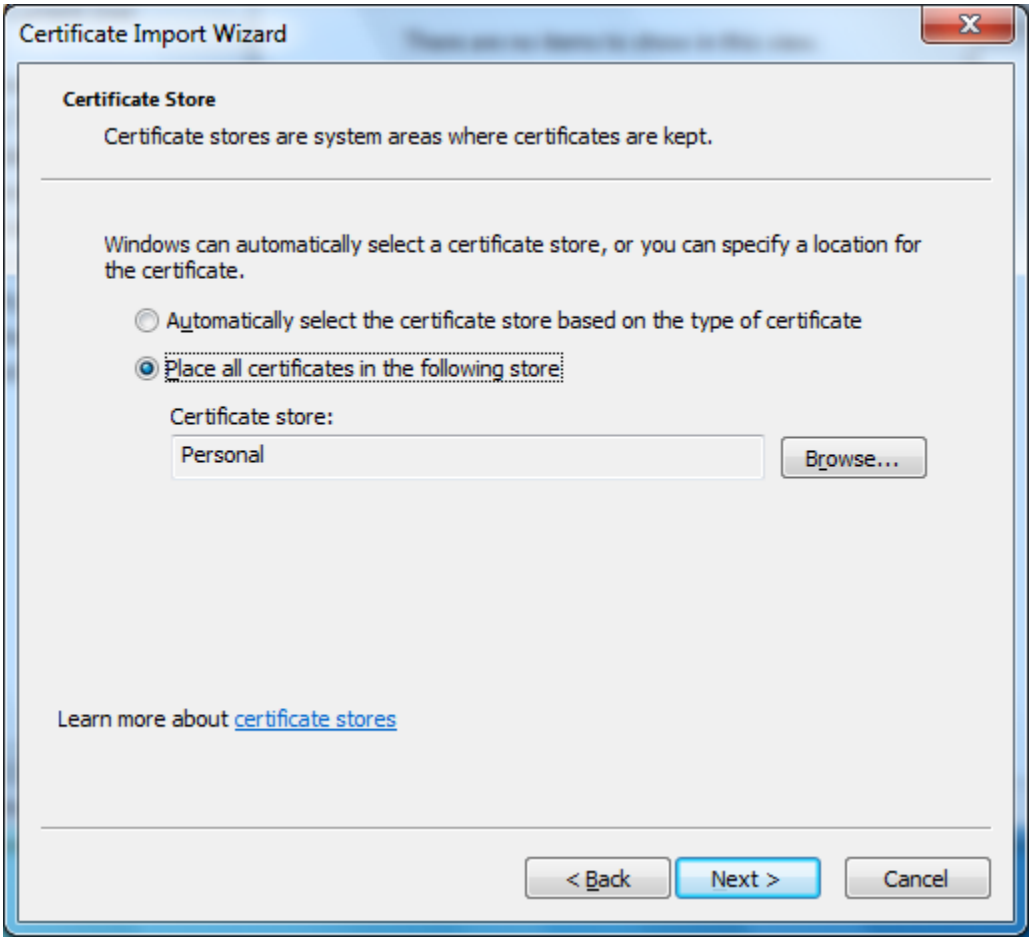


In the Certificate Import Wizard dialog box, click on Next> button.

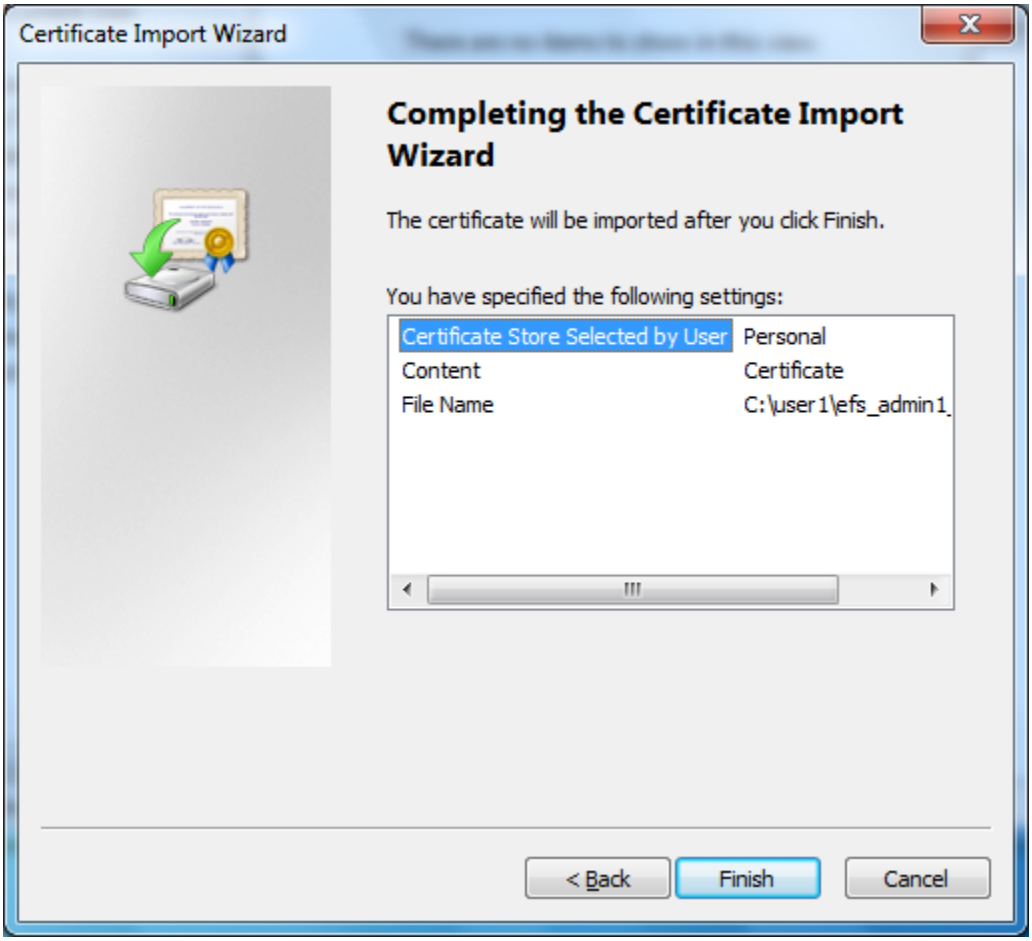
Enter c:\user1\efs_admin1_key.cer as the file to import, and click Next> button.



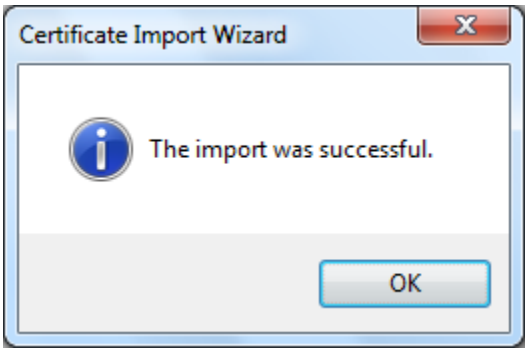
Click Next> button in the dialog box.



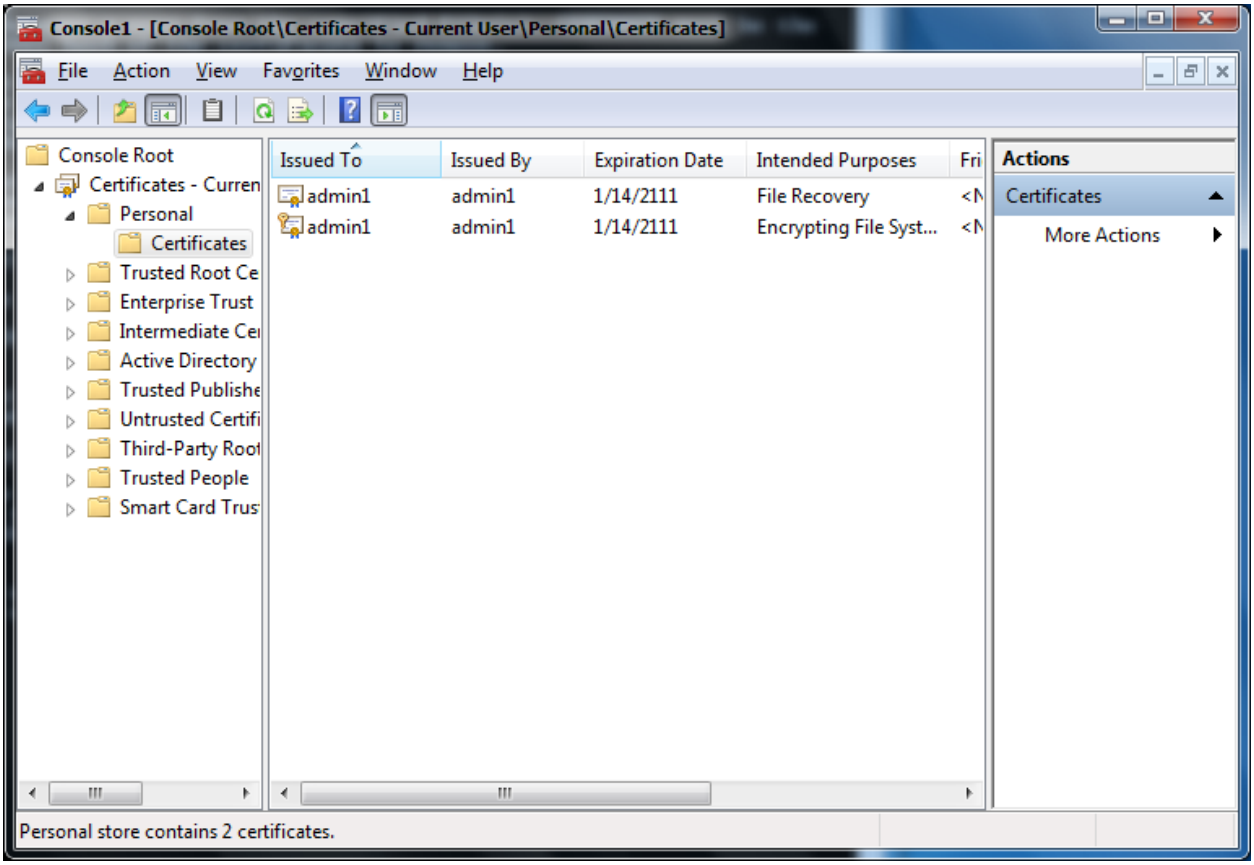
The following dialog is shown. Click on Finish button.



The following dialog box indicates the successful import of admin1's certificate.



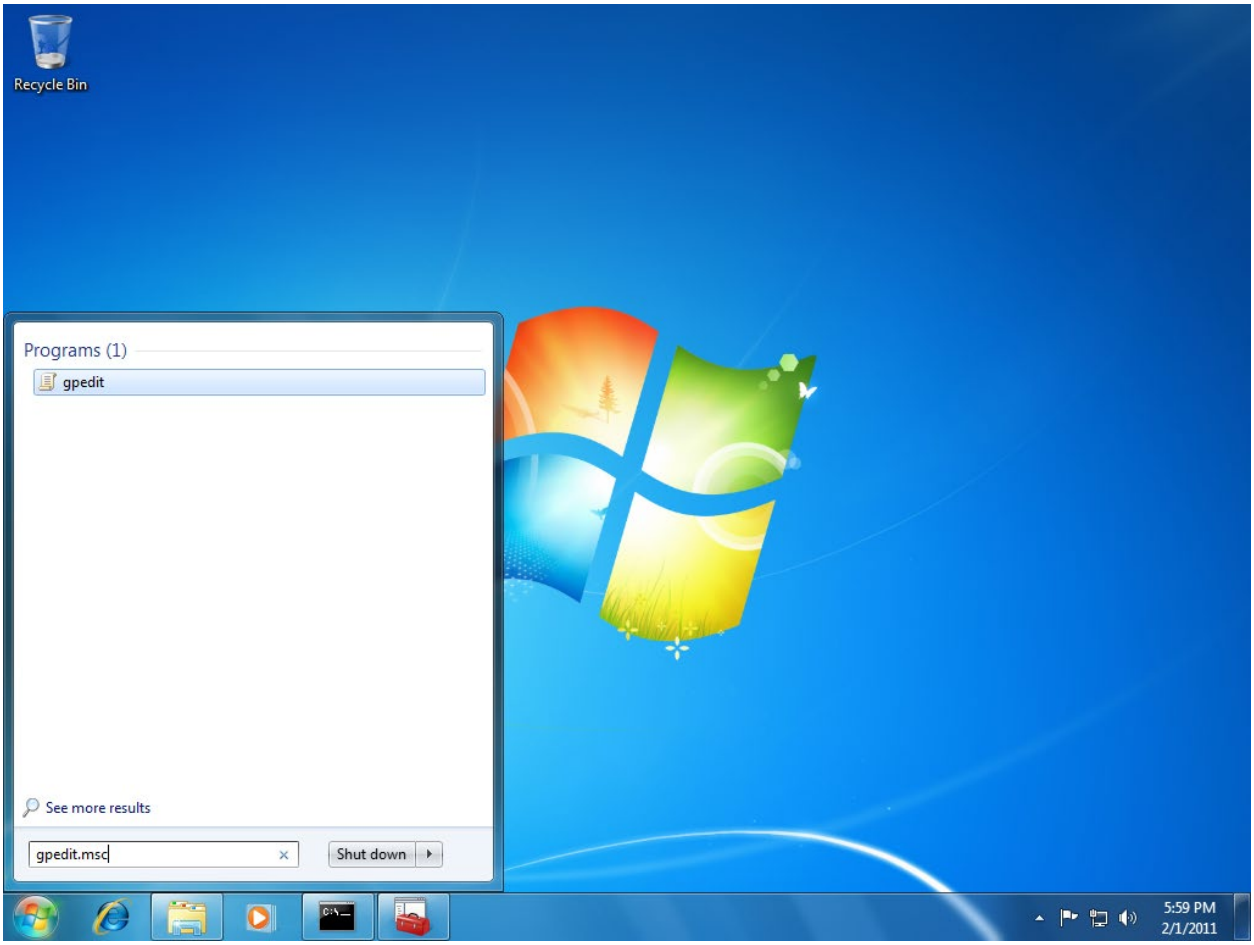
At this juncture, you should see two certificates for admin1, one for EFS and another for file recovery.



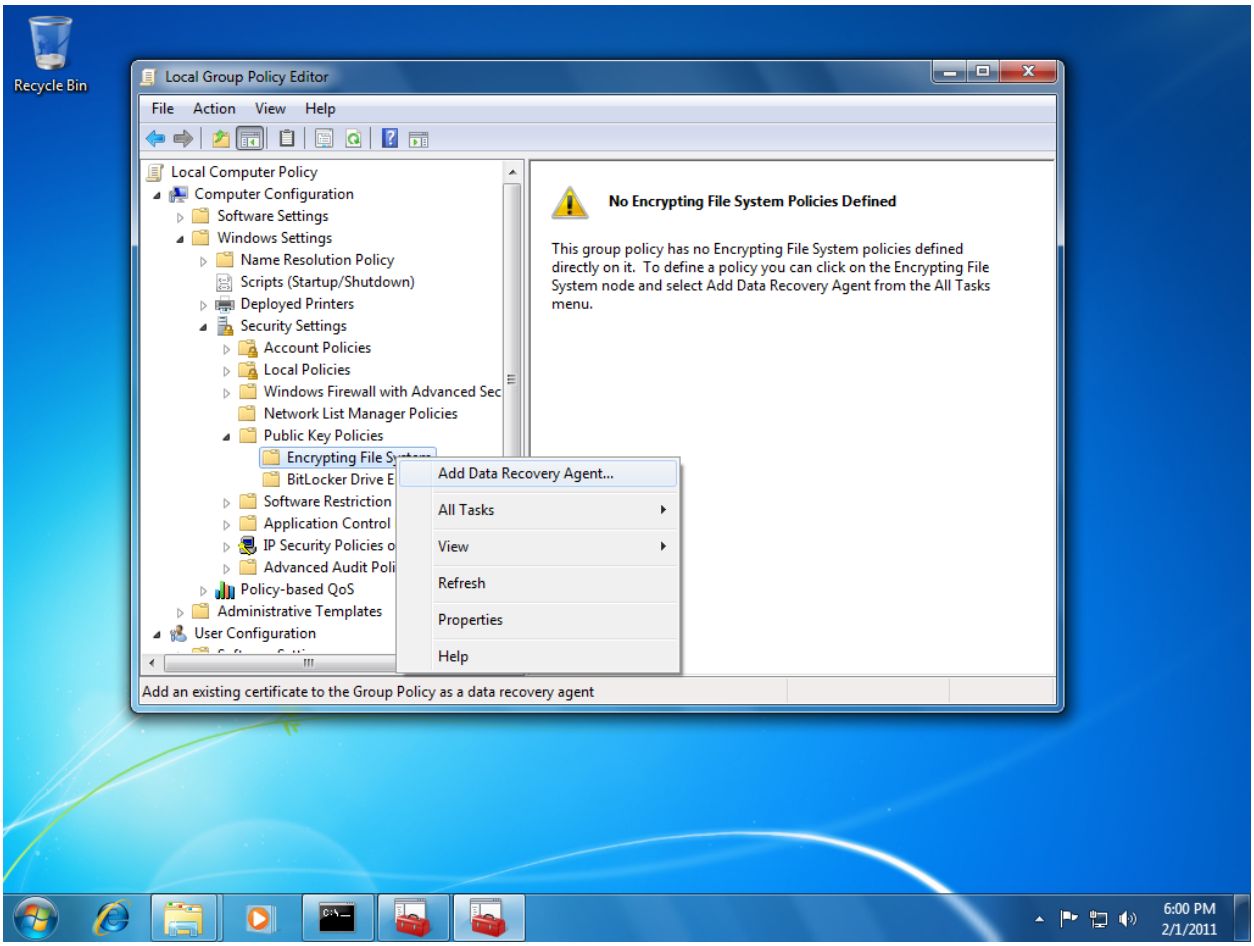
4.3 Adding recovery agent's key

Next, the recovery agent's key has to be added.

Click start and enter gpedit.msc to run the Local Group Policy Editor.

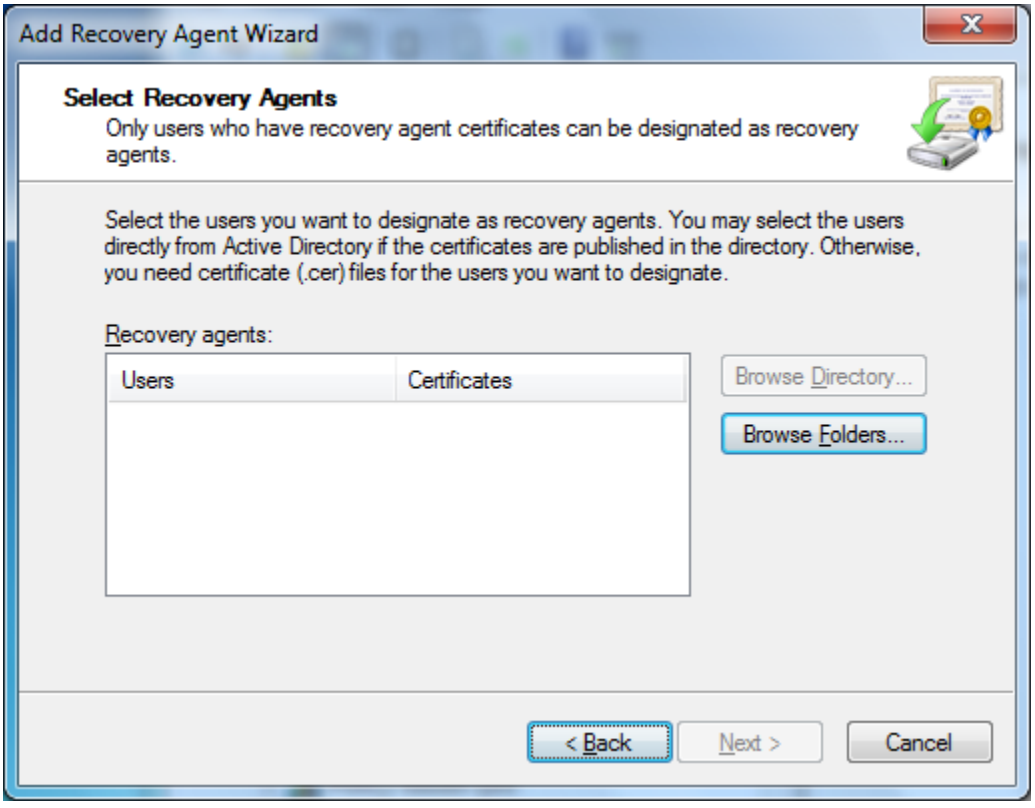


In the Local Group Policy Editor dialog box, select Local Computer Policy → Computer Configuration → Windows Settings → Security Settings → Public Key Policies, and right click on Encrypting File System and select Add Data Recovery Agent…

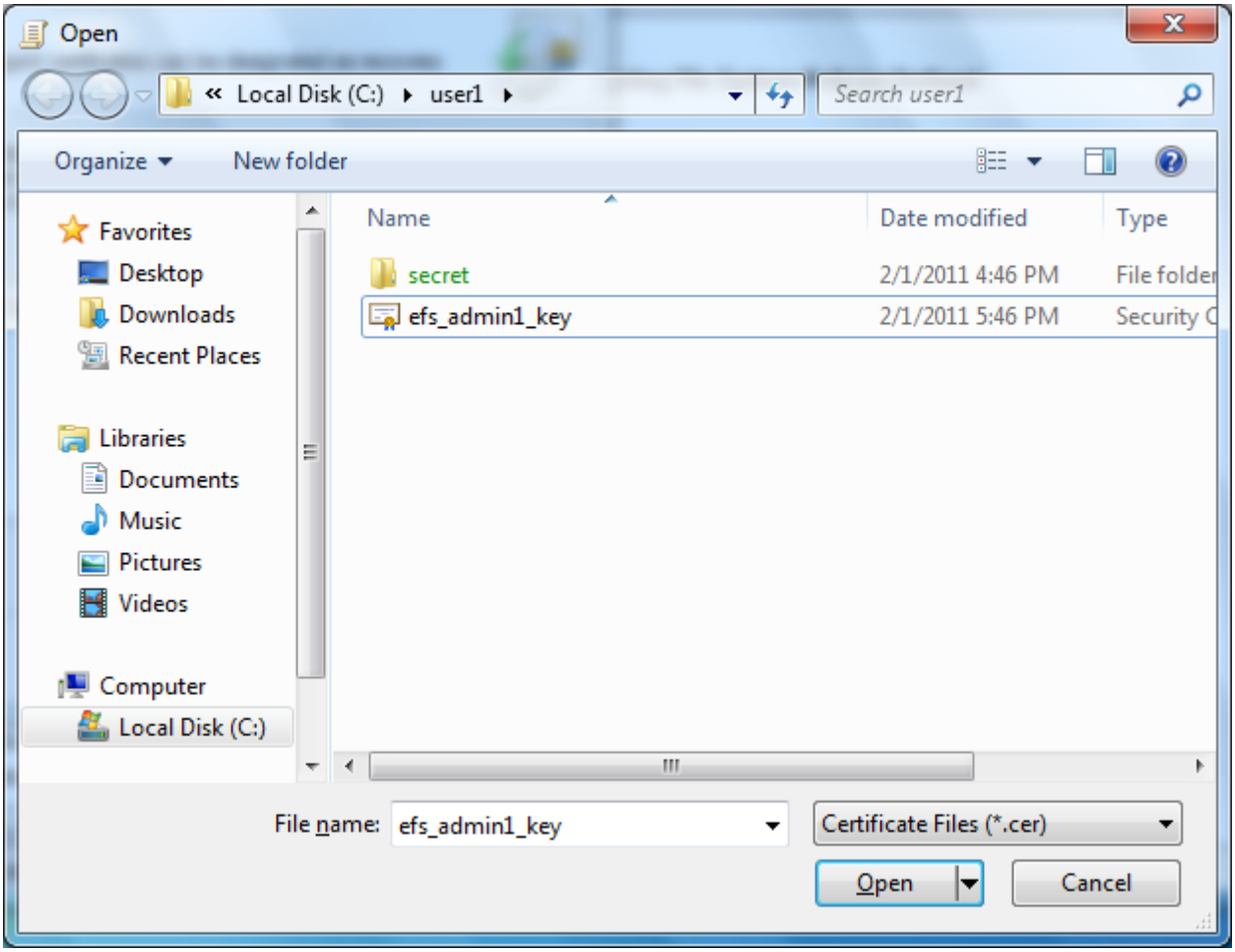


Click Next> in the dialog box.

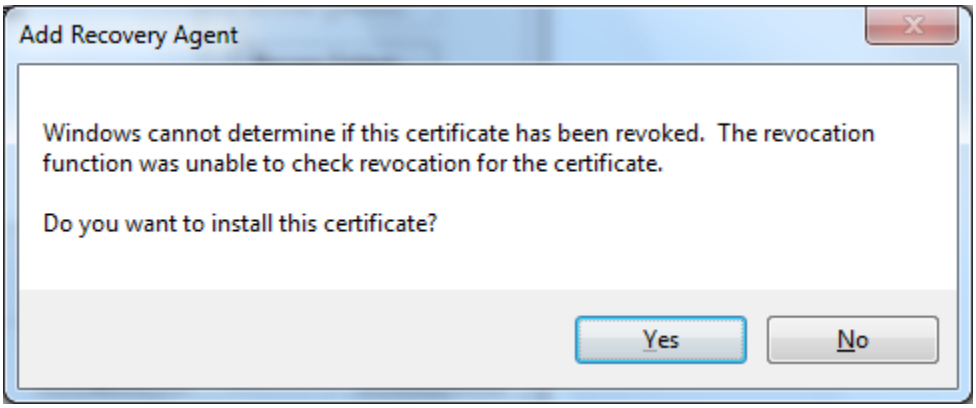
Click on Browse Folders… button.



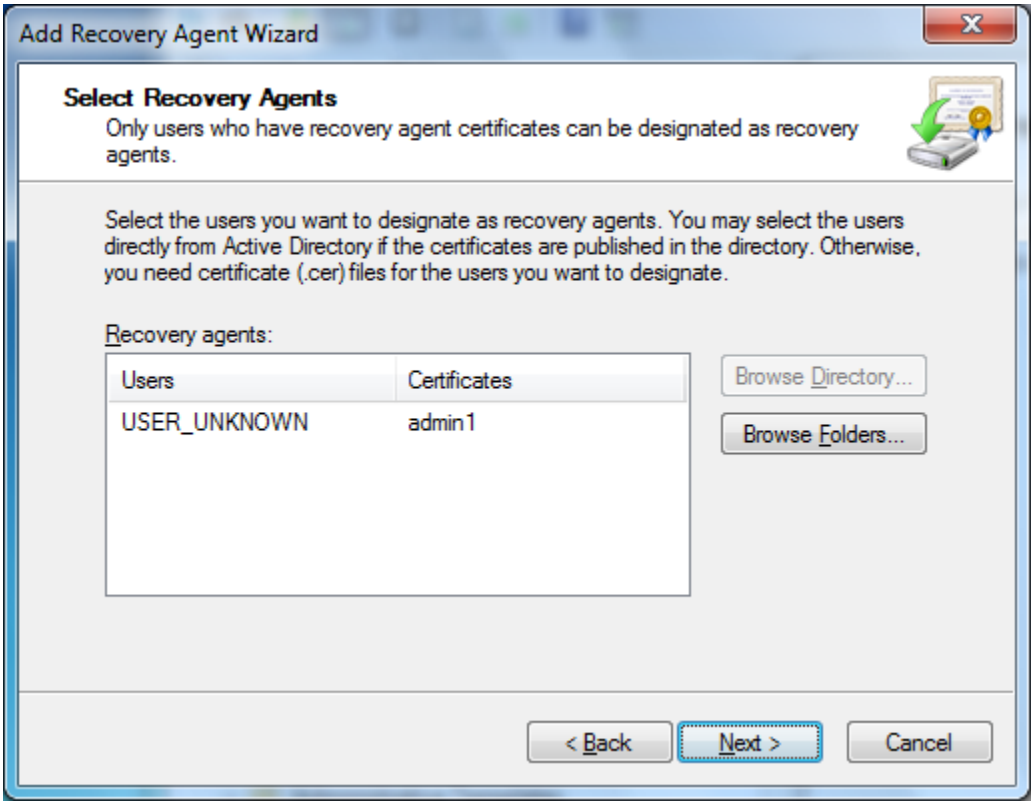
Select c:\user1\efs_admin1_key.cer and click on Open button.



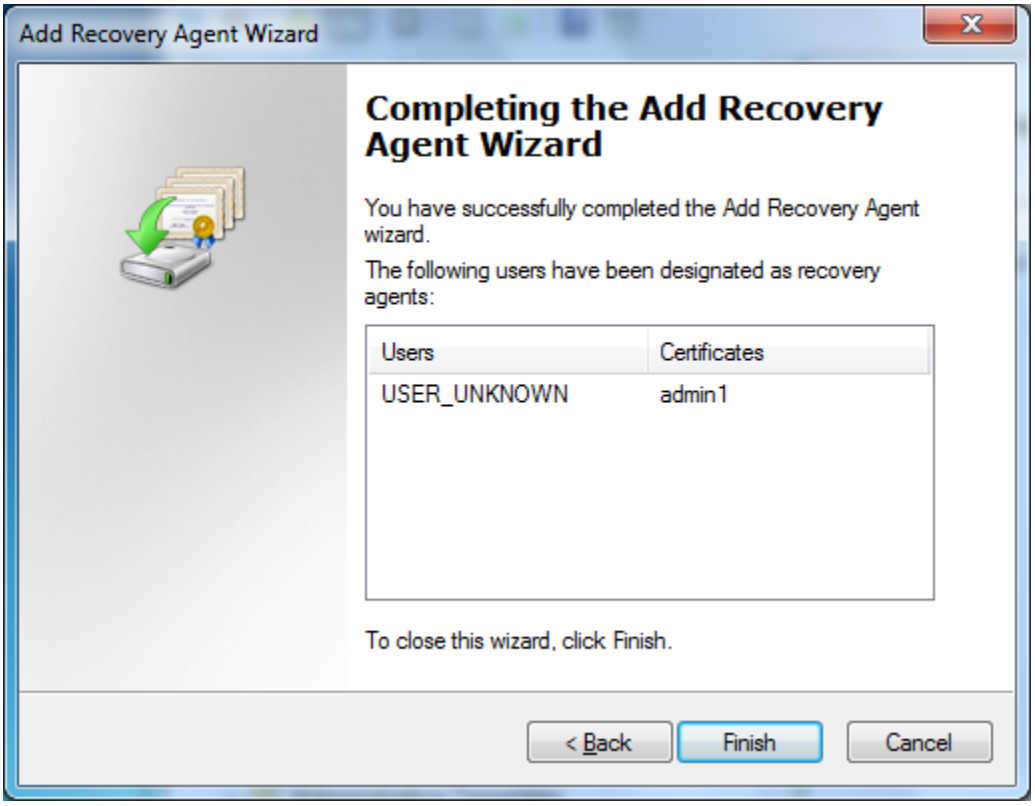
Click on Yes button to install the certificate.



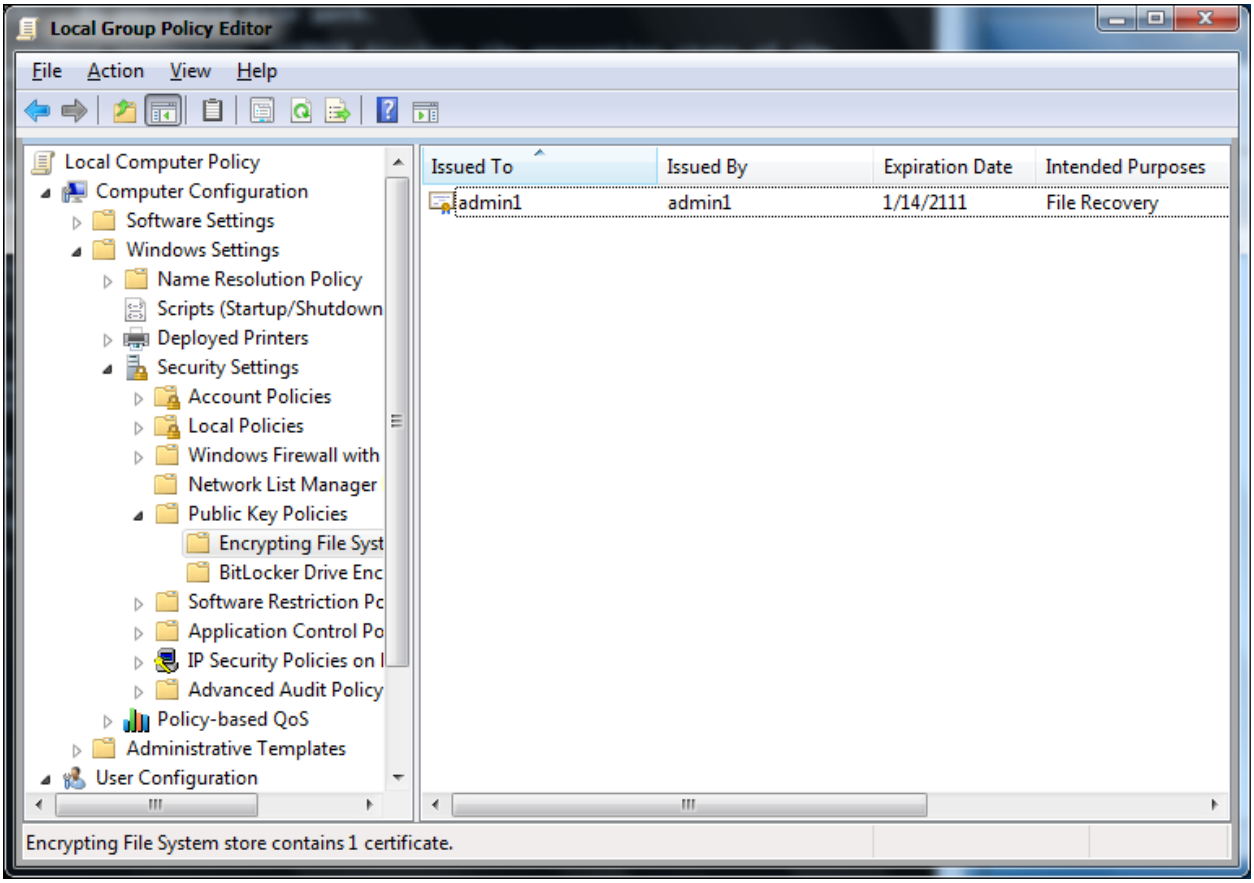
Click Next> button in the dialog box.



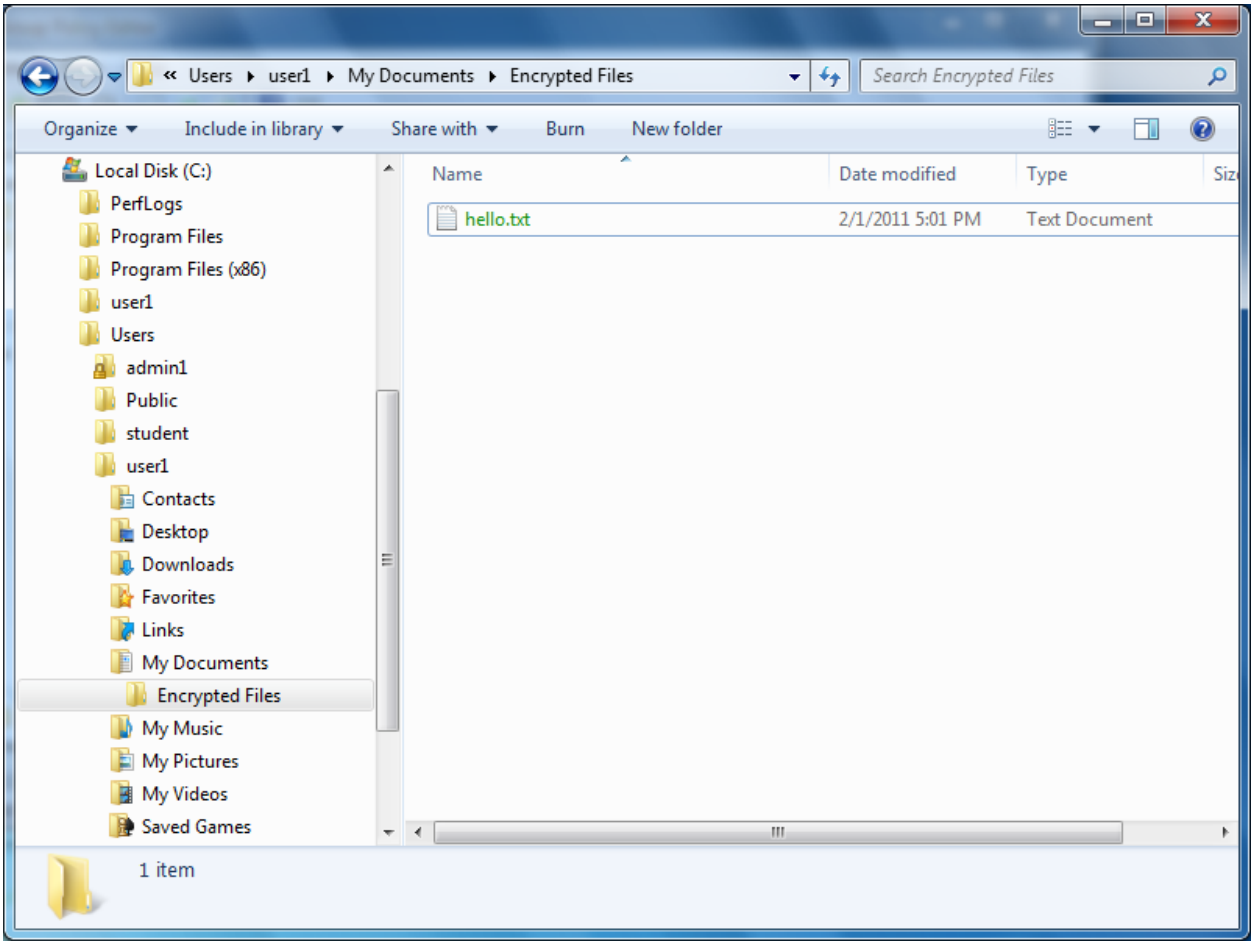
Click Finish button in the dialog box to complete the adding of recovery agent.



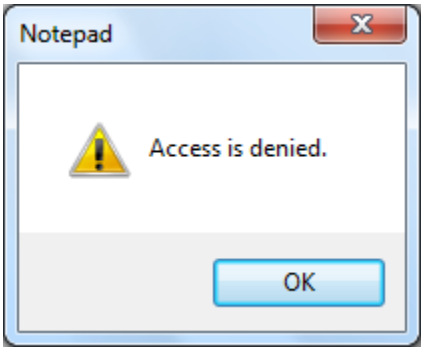
In the Local Group Policy Editor, check that admin1 has been added.



Try to access hello.txt.

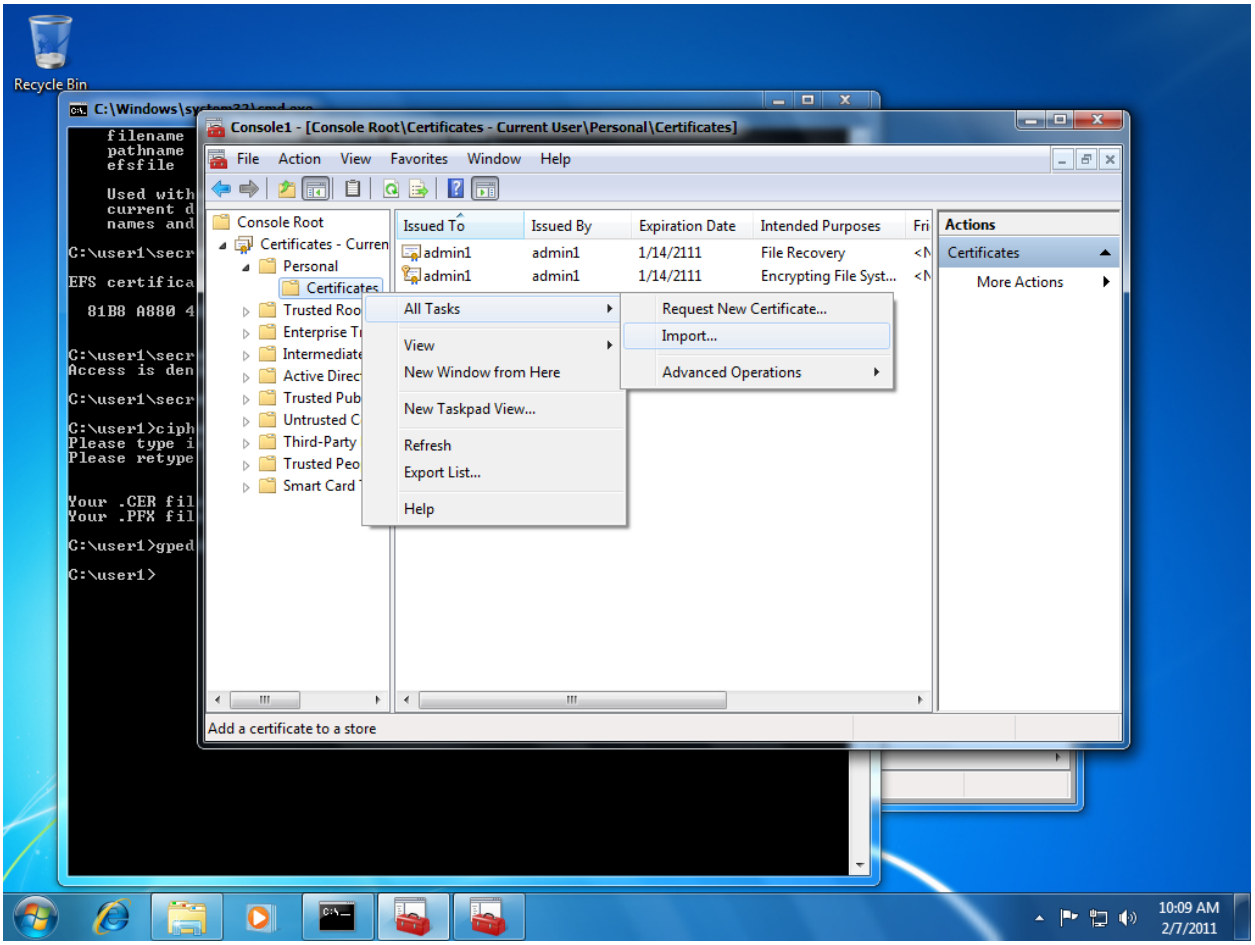


Note you are still unable to access hello.txt.

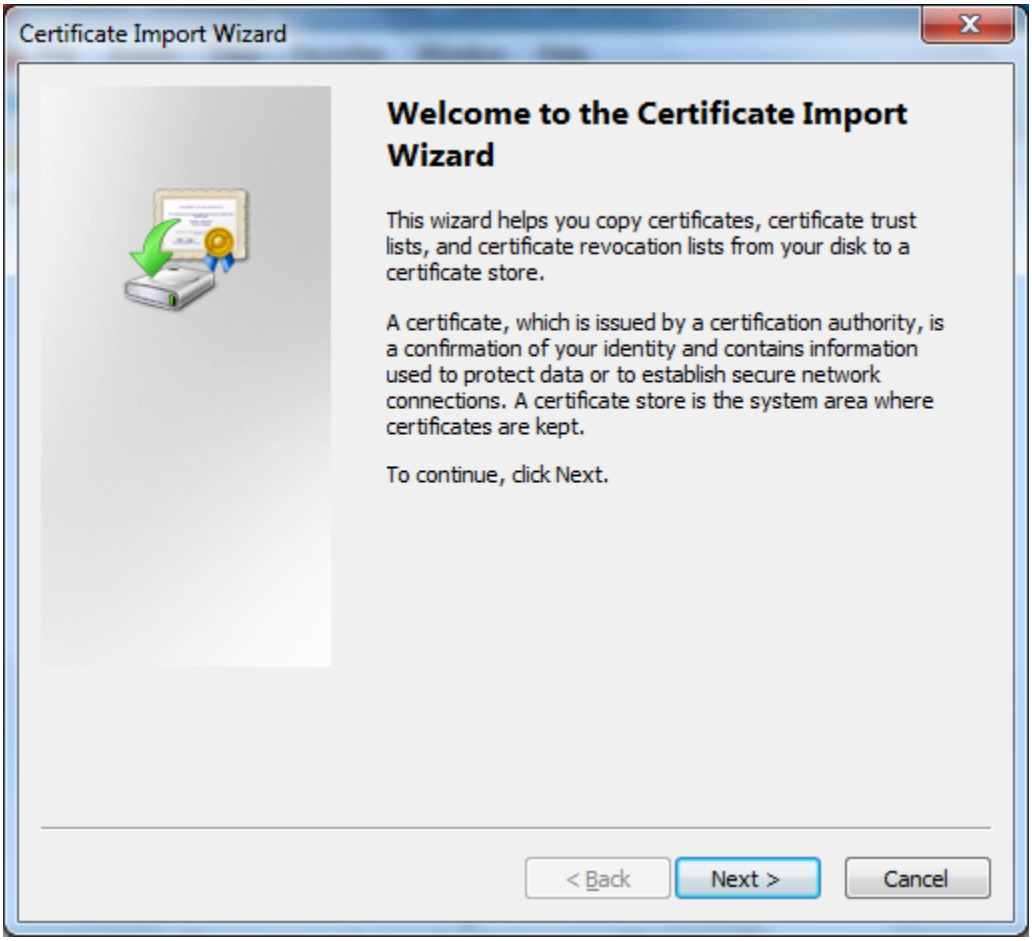


To allow the recovery agent to access hello.txt, we need to import efs_user1_key.pfx, which contains user1's private key.

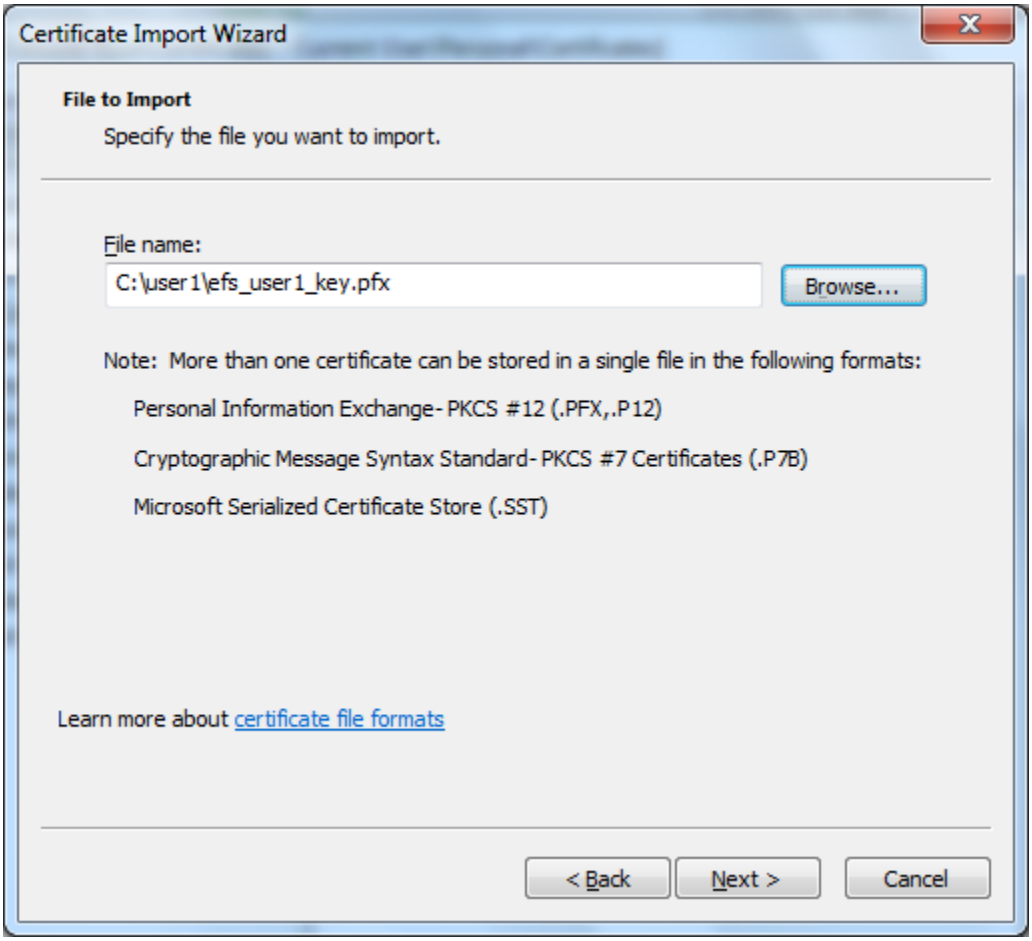
Run MMC again to import efs_user1_key.pfx.



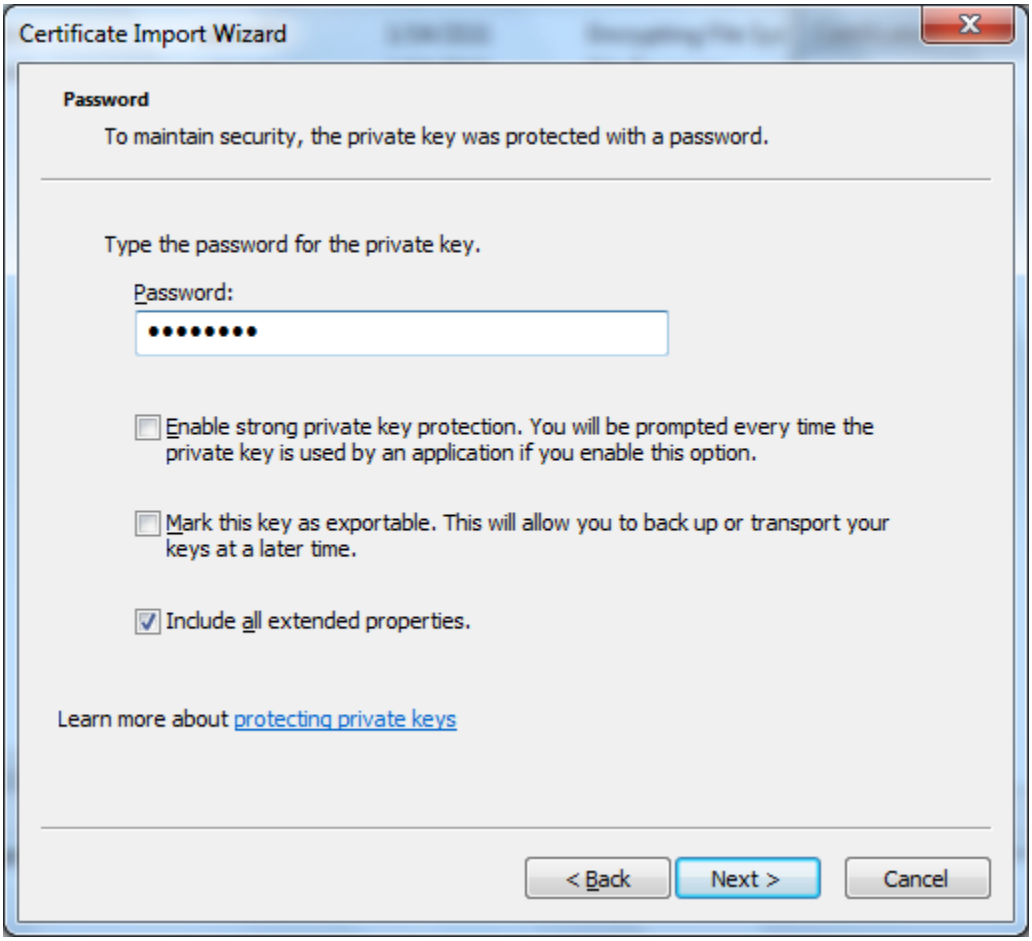
Click on Next> button.



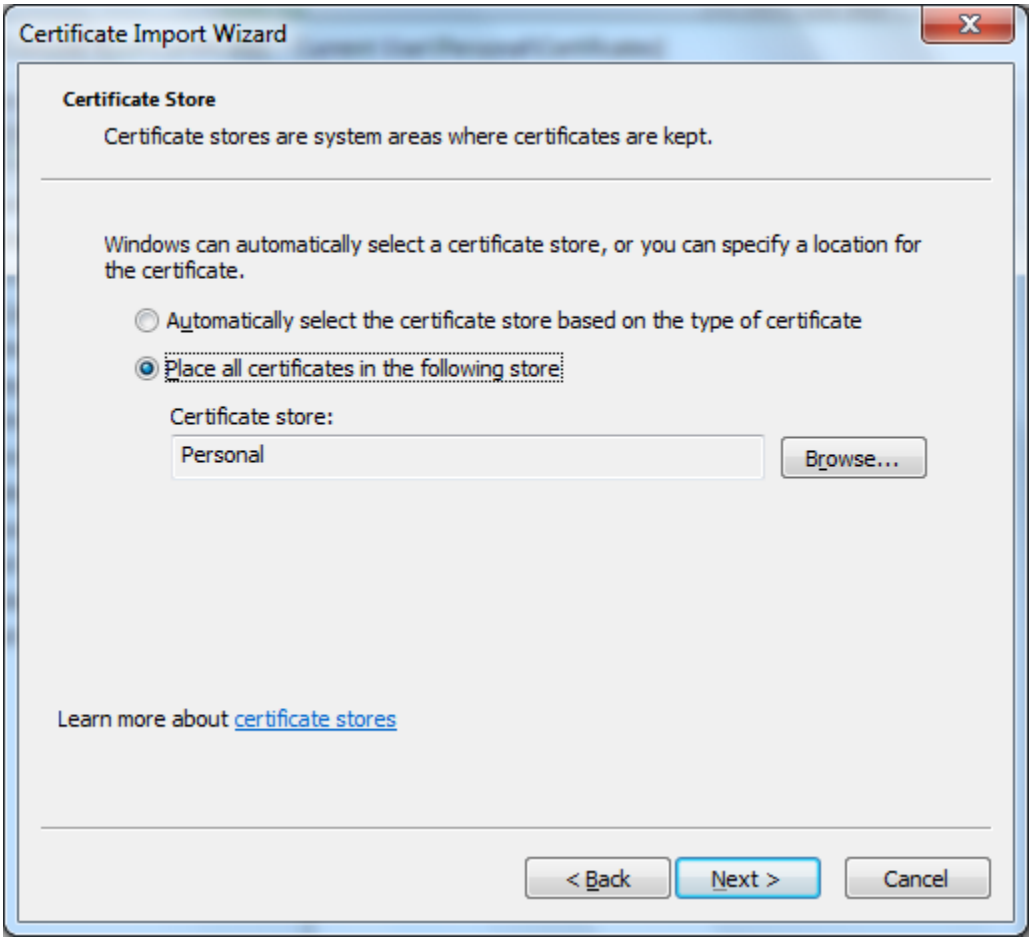
Select c:\user1\efs_user1_key.pfx and click Next> button.



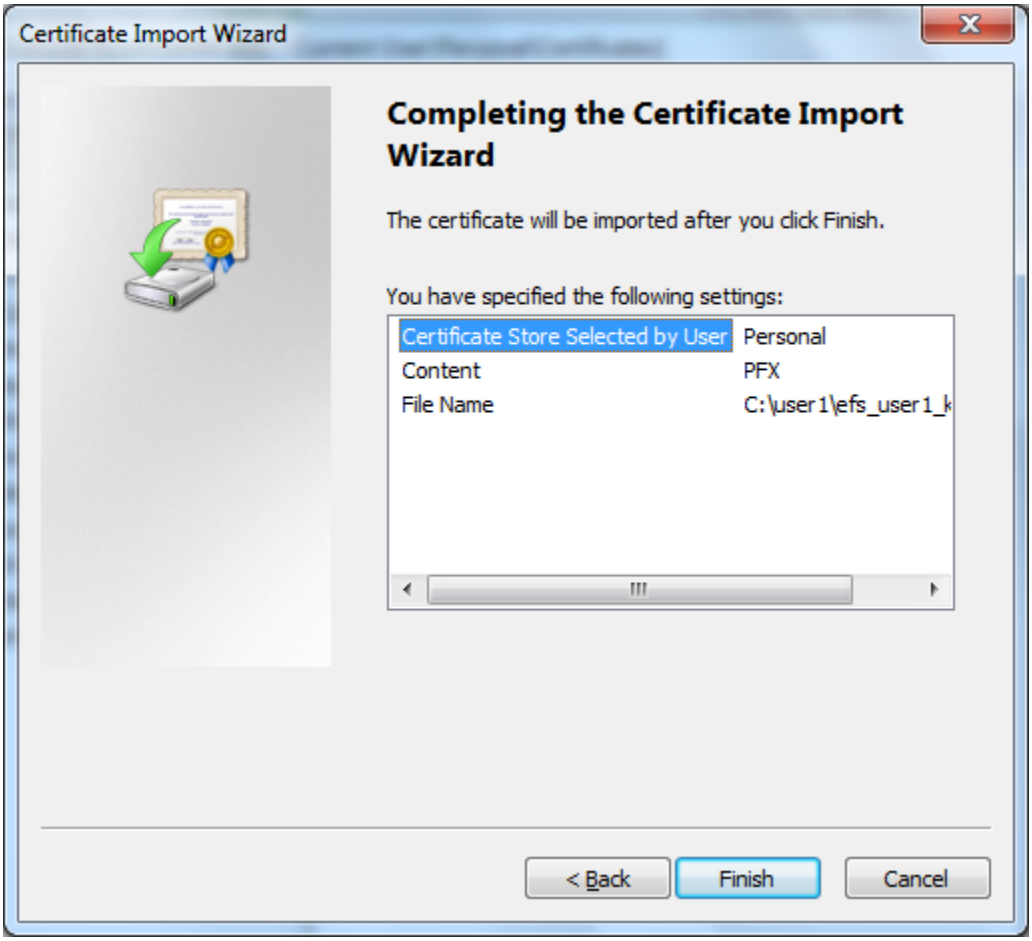
Enter “password” and click Next> button.



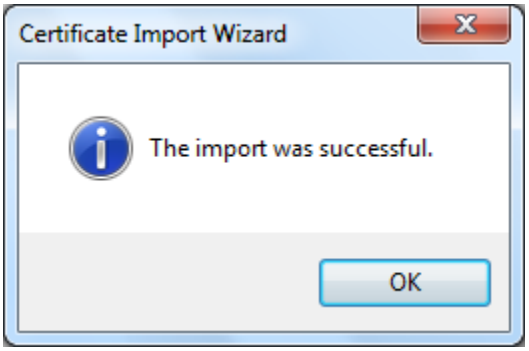
Click Next> button in the dialog box.



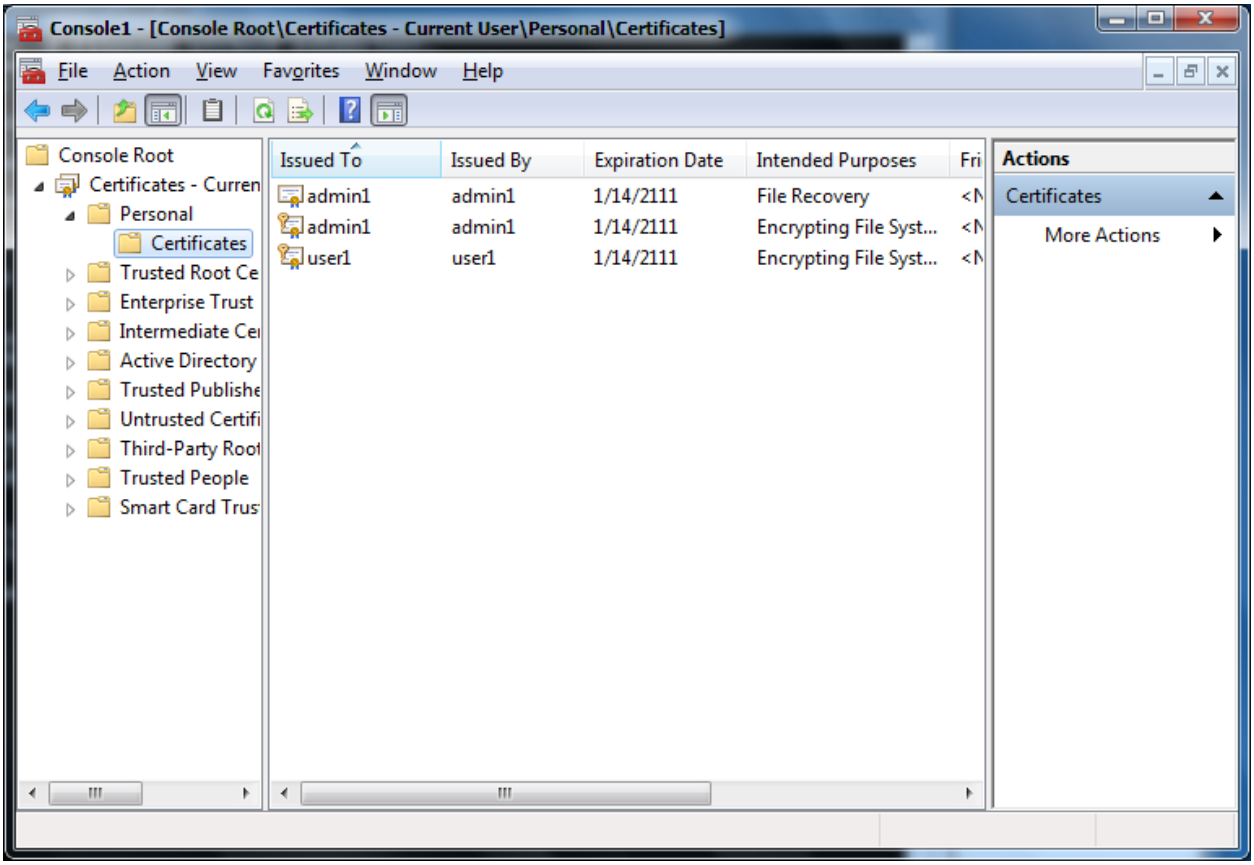
Click Finish button in the dialog box.



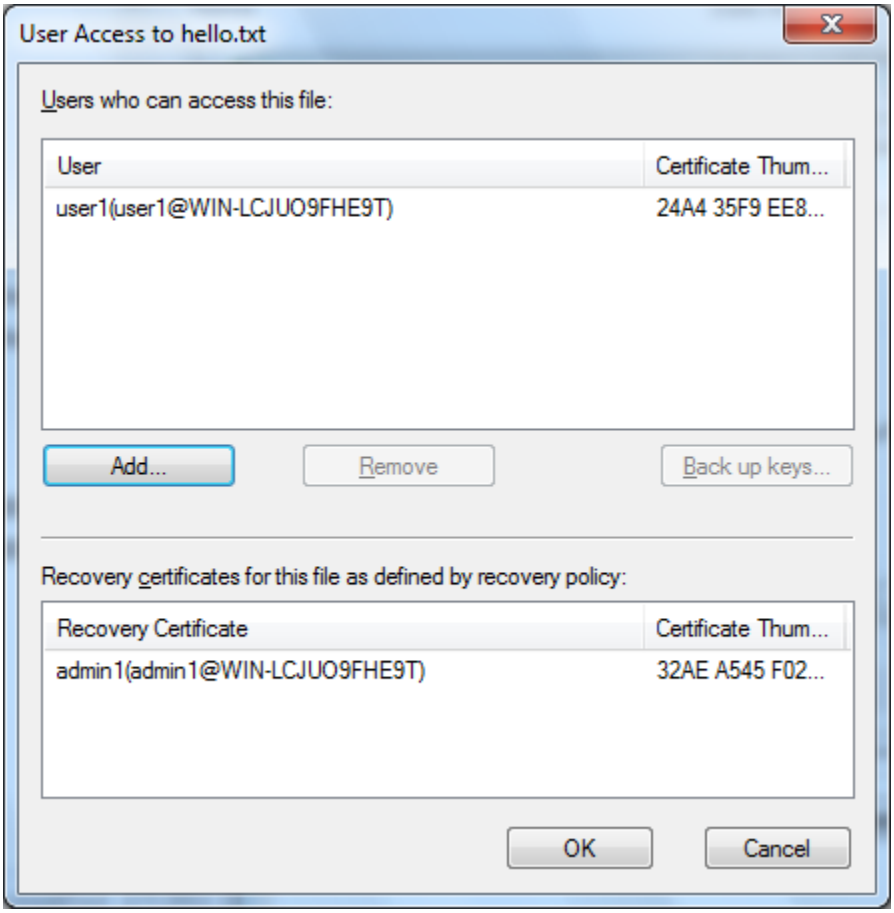
Click on OK button to complete the certificate import.



In MMC Console dialog box, check that user1's certificate is imported.

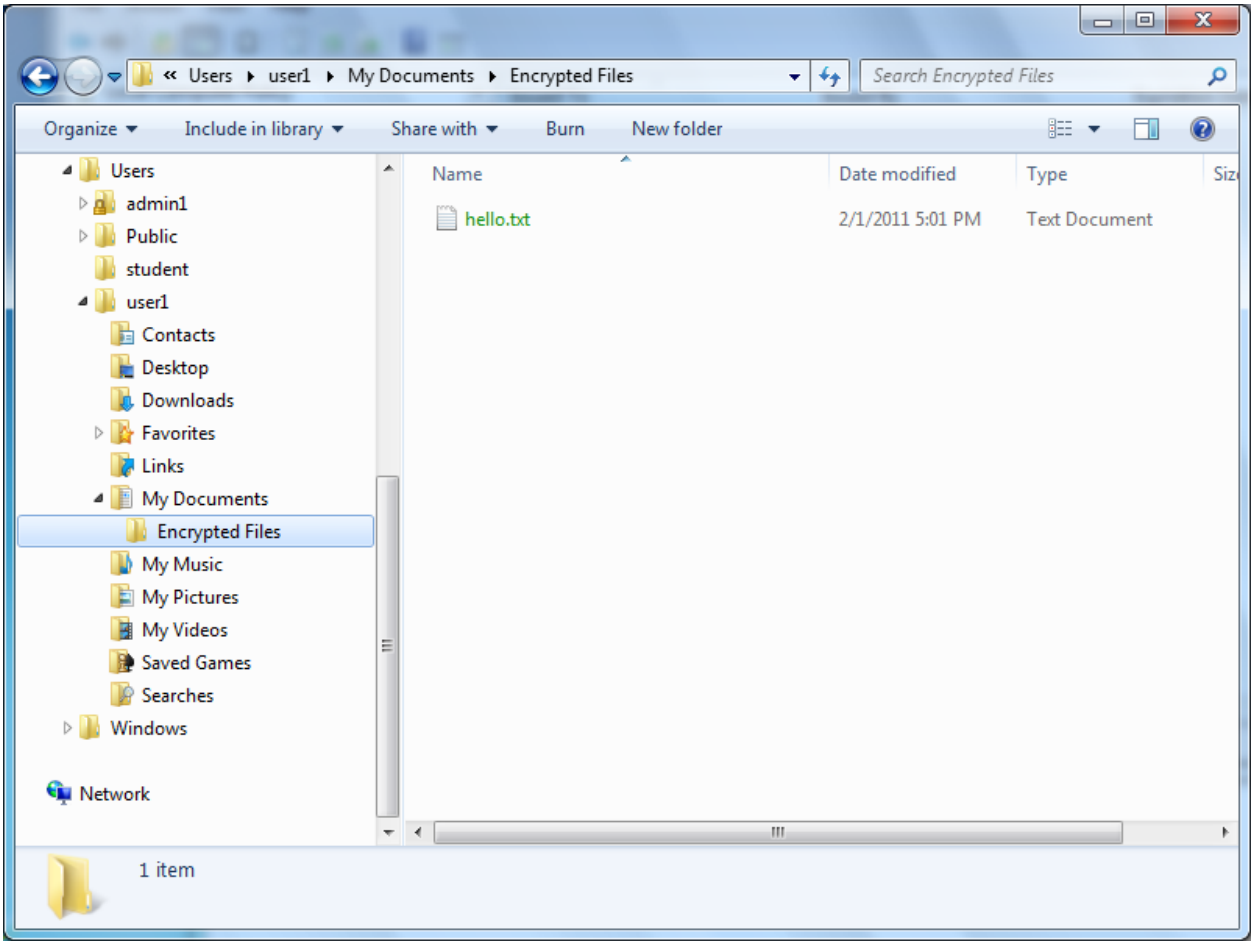

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Curren
Personal
Certificates
Trusted Root Ce
Enterprise Trust
Intermediate Ce
Active Directory
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Smart Card Trus
Issued To
Issued By
Expiration Date
Intended Purposes
Fri
admin1
admin1
1/14/2111
File Recovery
admin1
admin1
1/14/2111
Encrypting File Syst...
user1
user1
1/14/2111
Encrypting File Syst...
Actions
Certificates
More Actions

Next, check user's access to hello.txt. Note that admin1's certificate is added as a recovery certificate.



4.4 Decrypting files and folders

Try opening hello.txt.



You should be able to open hello.txt now.