



# ACTIVE DIRECTORY PROJECT

## Florida International University

## File Encryption Guide

Encrypted File Service (EFS) allows end users to encrypt the data stored on their machines and network drives so that only authorized users have access to open the files. Any data that contains sensitive information (credit card numbers, SS#, and driver's license numbers) must be encrypted if it is on a FIU workstation or network drive.

### What Users Will See

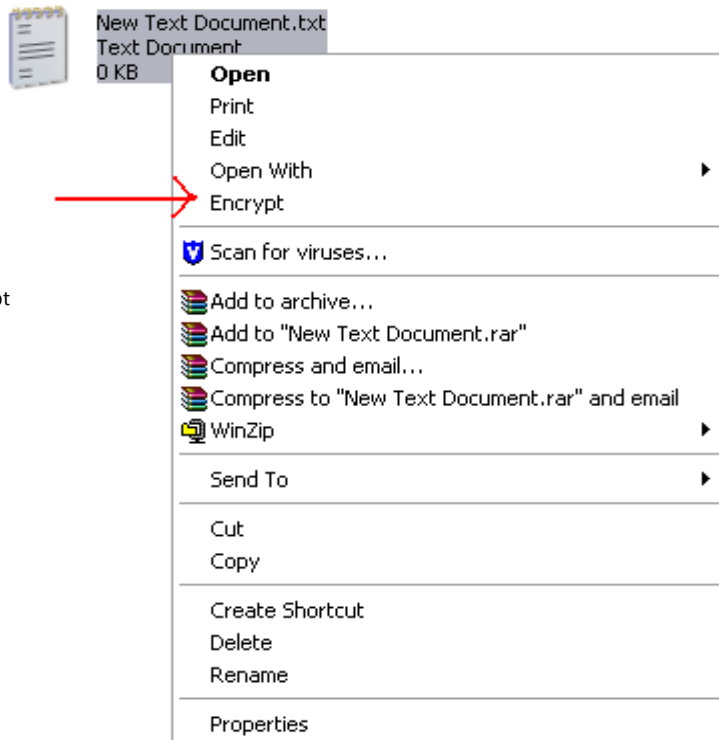
Encrypted file/folder names will show up in a green font. Non-encrypted files/folders will be displayed in the regular font color.

### How to Encrypt a File

The context (right-click) menu will have an entry to Encrypt and Decrypt a file/folder based on its current encryption state.

1. Right click the file
2. Select Encrypt

Note: To decrypt, repeat process and select decrypt



3. Then select the type of file encryption you would like. You will now have the option of encrypting a single file or all files within a folder. Once your selection is made, click “OK.”

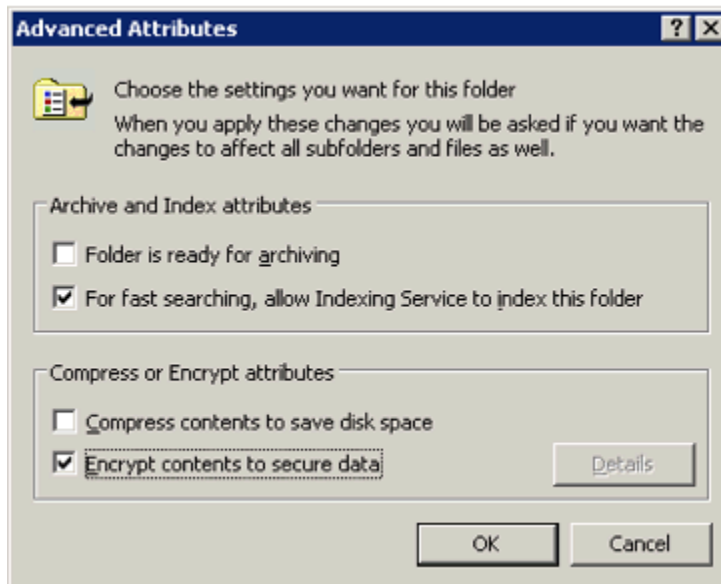


### **How to Share Encrypted Files**

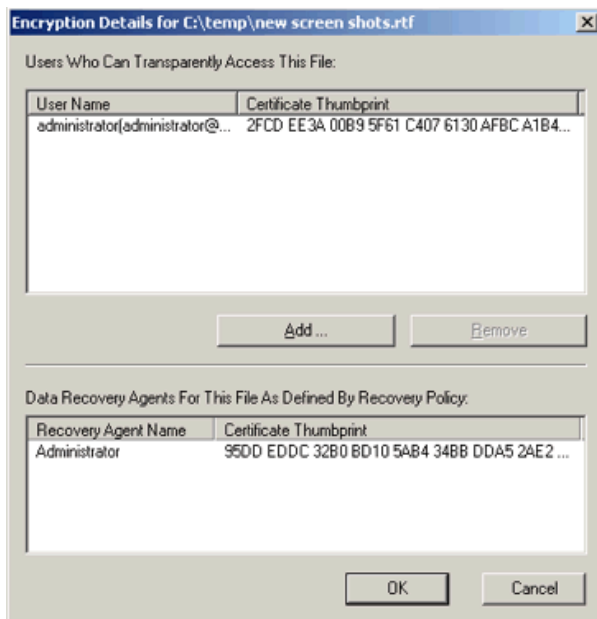
Sharing files that you have encrypted requires additional steps. To do this, simply add the certificate of the person to whom you want to allow access for each file in question.

Follow the steps below to allow a user to access an encrypted file:

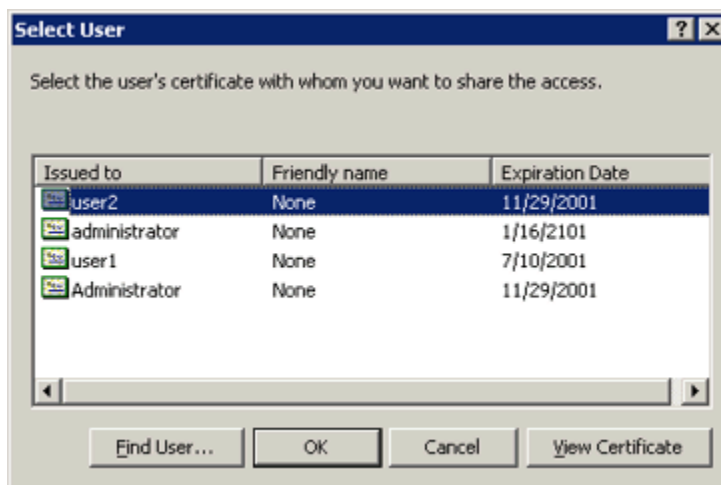
1. Right-click on the encrypted file
2. Click on 'Properties'
3. Click on the 'Advanced' button near the bottom right corner of the dialog box
4. The 'Advanced Attributes' dialog box should appear. Ensure the checkbox next to 'Encrypt contents to secure data' is selected, and click on the 'Details' button to the right



5. In the 'Encryption Details' dialog box that appears, you will see your username in the top box
6. To add users to that list, click on the 'Add' button.



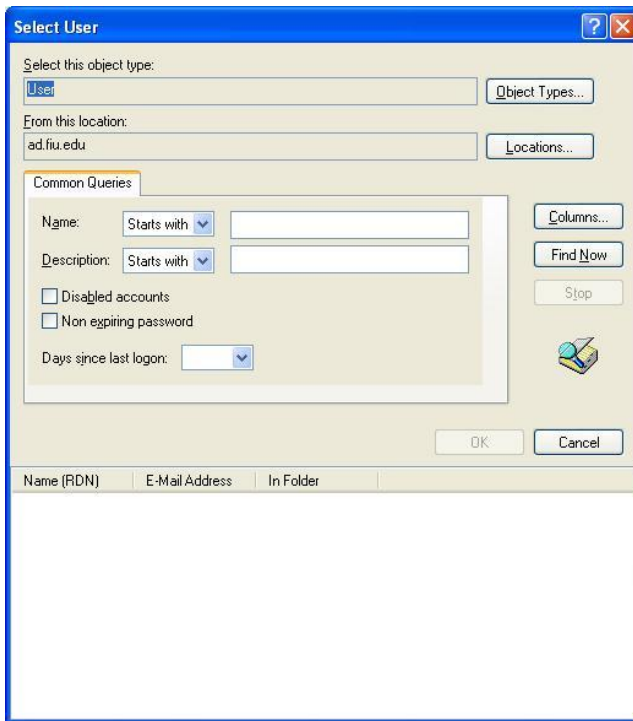
7. A 'Select User' dialog box will appear. From here, you can scroll down to find the username of the person to whom you want to grant access.
8. Select the user and click 'OK'. You should now see the user you added under your name. If the user is not found on the list, proceed to Step 9.



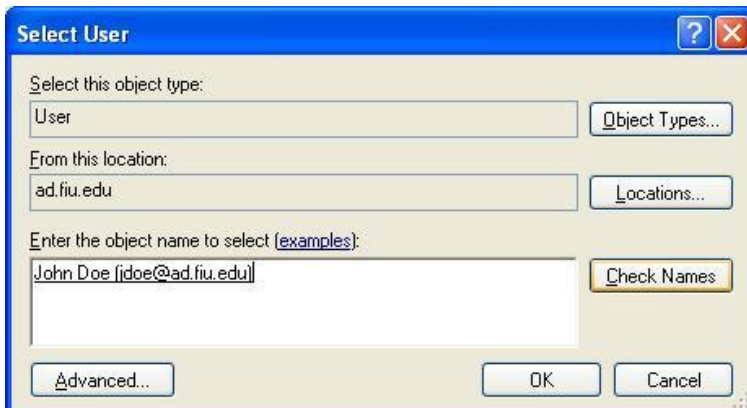
9. Click on the 'Find User' box to search for them by username or name.



10. If you still cannot locate the correct user, you can perform a search for the user by clicking on "Advanced."



11. Once you have typed the name, select "Check Names" to ensure that the user you are granting access to is indeed the correct user.



12. Once you have selected the correct user, click “OK” to proceed.

13. Repeat this procedure for any other users you would like to add. When you are finished, click ‘OK’ twice to exit the dialog boxes.

Note: You may allow additional users to access files but not folders.

### **Data and Key Recovery**

In the event that your user certificates are lost, or that your profile or machine is inoperable, you can contact UTS to have your certificates restored. An administrator can export your certificate and import it to the workstation thereby allowing you to decrypt your files. In extreme cases, an Administrator can use a Data Recovery Account to decrypt the file(s) for you.

### **Some things to note:**

- If you encrypt a file or folder, then you can move or copy it to any other location that supports Encryption File Services, and it will retain its encrypted state. Copying it to a location that does not support encryption will decrypt the file, but not before warning you.
- If you are the only authorized user of the encrypted file, only you can copy or move the file to an alternate location.
- E-mailing encrypted files through WebMail and Lotus Notes decrypts the file for the recipient. **However, it is not advisable to e-mail any sensitive data.**
- If you encrypt a folder, all files placed in that folder will become encrypted by default. The files will retain their encrypted state even when moved out of the folder. It is good practice to encrypt a folder on your machine and move the files you would like to encrypt into that folder.
- Users can be added to files only, not folders. So, if you have an encrypted folder that contains files you want to share, you’ll need to add the user(s) certificates to each file individually.
- Groups cannot be added to encrypted files. Only user certificates can be added for access.

For more information, visit [fiuad.fiu.edu](http://fiuad.fiu.edu), or contact the

UTS Support Center at (305)348-2284 for Help.