



**United States
Department of
Agriculture**

GUIDE

User Guide to Using EFS

Update

Version 1.1

July 30, 2007

Prepared by:
**OCIO Information Technology Services
Infrastructure Deployment Branch**

User Guide to Using EFS

Revision History

RECORD OF CHANGE

Revision/Change Number	Update Number	Date of Change	Description/Reason for Change	Pages/Sections Affected
1.1	1	7/27/2007	Updated to include reference to desktops as this is now for all desktops, tablets, and laptops.	Various

Table of Contents

1. Overview	1
1.1. Purpose.....	1
1.2. Introduction.....	1
2. File Encryption	2
2.1. Implementing File Encryption.....	2
2.2. First Time Logon After Encryption Has Been Administered.....	2
3. How to tell if a File or Directory is Encrypted	3
4. Encrypting a Directory	4
5. Updating Recovery Certificate.....	6
6. Other Useful Information.....	8
6.1. Workstation Backups	8
6.2. Moving and Copying Files	8
6.3. Standard Encrypted Folders.....	9
6.4. File Strategies	9
6.5. Data Files for Applications.....	10
6.6. Multiple Users	10
6.7. Opening an Encrypted File of Another User.....	10
6.8. Removing Encryption On A File	10

1. Overview

1.1. Purpose

The USDA Service Center concept is a cornerstone of the department's reorganization effort undertaken subsequent to the Department of Agriculture Reorganization Act of 1994. By consolidating its individual agency field offices into service centers, the USDA intends to see a greater return on investment, and at the same time provide taxpayers with more efficient service at reduced cost.

One of the key components of this concept is the implementation of the *Information Technology Services* (ITS) organization. The ITS vision is to be recognized as a professional team of customer-driven service providers who respond to the needs of its customers by providing outstanding service and cost-efficient, highly effective technical solutions.

1.2. Introduction

In response to recent concerns regarding the safety of sensitive data on workstations, ITS will be enabling the Encrypted File System (EFS) feature within the WINDOWS XP operating system running on desktop computers. This feature was already enabled on all notebook, laptop, and tablet workstations. The process to enable EFS will be implemented through a start up script when the workstation is rebooted on the ITS network.

- ➔ *For machines that can not receive the start up script, i.e. dialup or vpn locations it will be necessary for the ITS staff to manually install the software to implement EFS.*

The first time a user logs on to these types of devices, a script will execute that will encrypt folders that have been identified in this guide.

IMPORTANT!!! Users need to make sure that when they need to store files on these devices, they must save the files in the folders that have been encrypted.

- ➔ *While the process is running please refrain from using MICROSOFT OUTLOOK and any other programs that store data within the affected directories.*

2. File Encryption

In order to maintain the security of sensitive information on machines that leave USDA property, the Encrypting File System built into Windows XP is going to be used. This will add a number of new concerns to ensure the data is also accessible to authorized persons.

➡ *For the most part, file access is transparent to the creator of the file.*

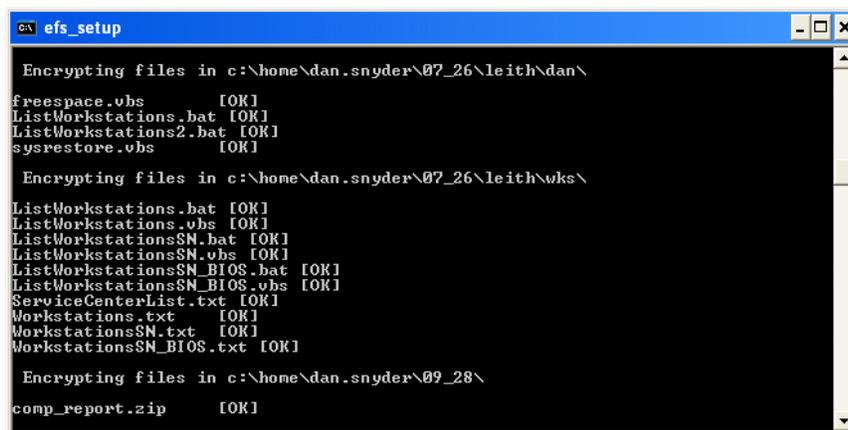
2.1. Implementing File Encryption

A script has been set up to implement the file encryption for each user that logs on to a computer. This script is made available to the computer by performing a reboot of the machine while on the ITS network.

For machines that are not on the ITS network, i.e. use dial-up or VPN connection all of the time, it will be necessary to obtain the manual installation script and have it installed by the ITS staff.

2.2. First Time Logon After Encryption Has Been Administered

1. At the CTRL + Alt+ Delete log on screen, log on to the workstation with regular user account. You will see a new screen, such as the one shown in Figure 2.2.a below, as the encryption of existing files takes place.



```

C:\> efs_setup

Encrypting files in c:\home\dan.snyder\07_26\leith\dan\
freespace.vbs [OK]
ListWorkstations.bat [OK]
ListWorkstations2.bat [OK]
sysrestore.vbs [OK]

Encrypting files in c:\home\dan.snyder\07_26\leith\wks\
ListWorkstations.bat [OK]
ListWorkstations.vbs [OK]
ListWorkstationsSN.bat [OK]
ListWorkstationsSN.vbs [OK]
ListWorkstationsSN_BIOS.bat [OK]
ListWorkstationsSN_BIOS.vbs [OK]
ServiceCenterList.txt [OK]
Workstations.txt [OK]
WorkstationsSN.txt [OK]
WorkstationsSN_BIOS.txt [OK]

Encrypting files in c:\home\dan.snyder\09_28\
comp_report.zip [OK]

```

Figure 2.2.a – Encryption Screen

- ➡ *Depending on the number of files in the folders to be encrypted the encryption can take from 10 minutes to over an hour. Errors will be received if the encryption is attempting to encrypt files that are in use, such as OUTLOOK, so it is necessary to wait until the one time encryption is finished before using the system.*
2. When the encryption is finished you will be returned to the normal desktop. Make sure you perform the action in Section 5 to establish an encryption key for the files that were encrypted.
 - ➡ *All files which are encrypted will have their date/time stamp changed to the time of their file encryption. Thus the first time the script is run; all files in the folder will be updated.*

3. How to tell if a File or Directory is Encrypted

The easiest way to see if a file is encrypted is through the use of WINDOWS EXPLORER. If the file or directory is encrypted, it will display with a green color. See Figure 3.0 below.

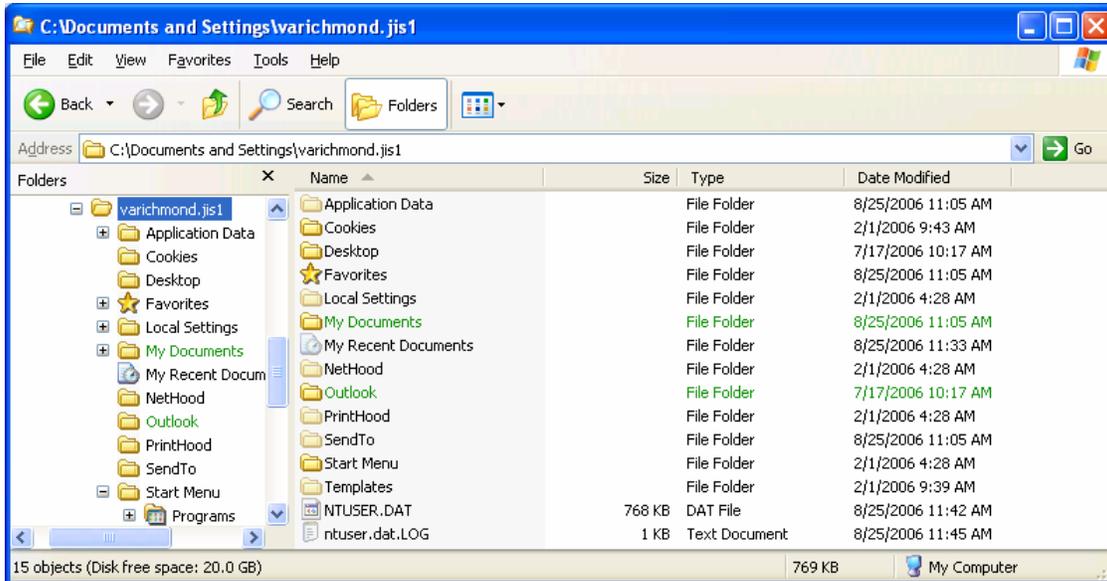


Figure 3.0.a – Sample Showing Encrypted Files

4. Encrypting a Directory

Although ITS is setting what it considers the most common directories for file storage to encrypt by default, there will be additional directories that may contain sensitive information. As those directories are identified by the Agency or user, they should be encrypted as well.

➡ *Bear in mind that programs encrypted by one user are usually not usable by another user.*

The steps to encrypt files in a directory are below:

1. Open **WINDOWS EXPLORER** by right-clicking the [Start] button.
2. Choose [**Explore**]. Navigate to the directory where encryption is to take place.
3. Right-click the **Directory** and choose [**Properties**]. See Figure 4.0.a below.

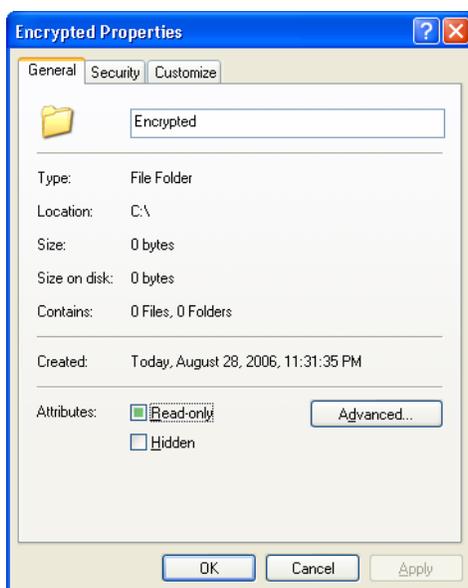


Figure 4.0.a – Properties Dialog Box

4. Click the [**Advanced**] button. See Figure 4.0.b on the following page.

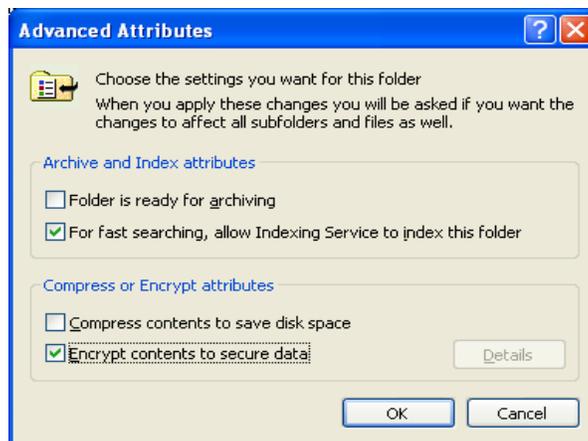


Figure 4.0.b – Advanced Attributes

- Put a check in the box next to [**Encrypt Contents to secure data**] and click [**OK**]. You will be returned to the previous screen. See Figure 4.0.c below.

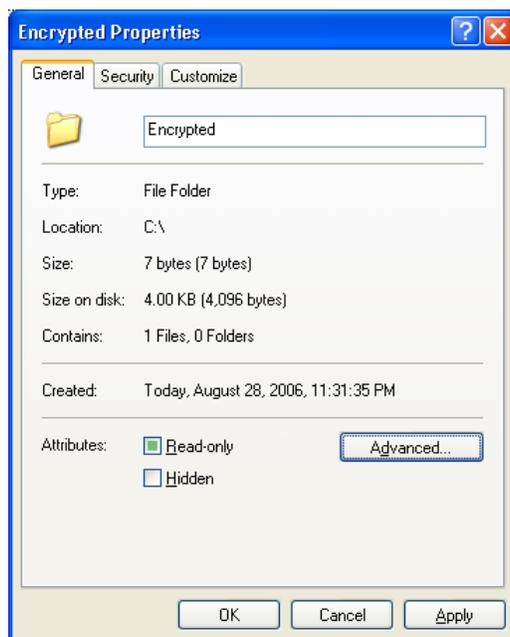


Figure 4.0.c – Properties Dialog Box

- You should see the screen shown in Figure 4.0.c. Click [**OK**].
- If the directory already contains items, it will ask if you would like to encrypt those as well. See Figure 4.0.d below. Choose [**Apply changes to this folder, subfolders and files**] and click [**OK**].



Figure 4.0.d – Confirm Attribute Changes

- When the encryption is finished, click [**OK**] to close out the **PROPERTIES** screen.

5. Updating Recovery Certificate

In order to use files you have encrypted, it is important that you have two items that are referred to as a Certificate and a Key. Normally, the existence and usage of these items is transparent.

However, in the case of a critical failure of the workstation, it is important that a backup of the Certificate for these files be kept off the machine. There is a semi-automated process on the machine that will guide you through the process and then save the file to your **H:\certificates** folder. In this example the H: drive is on the ITS Server.

- ➡ *It is recommended that you run this process every time you change your password on the computer so that you will easily remember what the password is. If you have a way of remembering the password you would not have to change it every time your password expires. Typically the only time you need to use the password would be if your workstation hard drive fails and ITS needs to rebuild the workstation.*

1. Press [Start] ➔ [All Programs] ➔ [USDA Applications] ➔ [Utilities] ➔ [EFS Key Backup]. See Figure 5.0.a below.

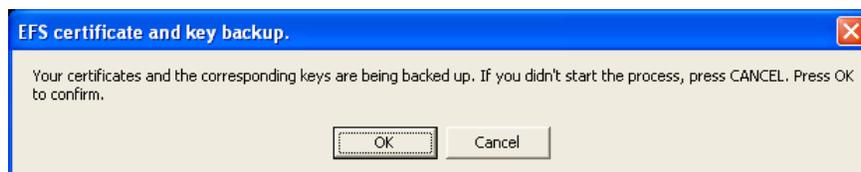


Figure 5.0.a – EFS Certificate and Key Backup

2. Click the [OK] button to back up your EFS key. You should receive the screen shown in Figure 5.0.b below.

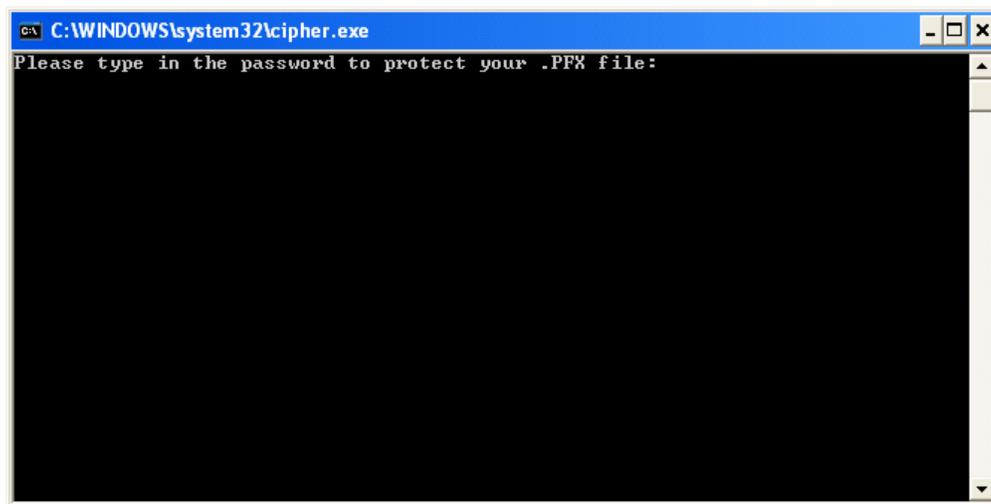


Figure 5.0.b – Password Protect cmd Screen

3. Type in a **password**

- ➡ *For simplicity, you can use your domain user account password.*

4. Re-type your **password**.
5. The file should now be saved in H:\certificates with a name containing both your user name and machine name.
6. If you did not input the password the same way both times it will fail in creating the certificate and the screen will not be able to display the failure. It is critical you access your H:\certificates folder and verify the certificate has been created. To access the folder, double click on the [My Computer] icon that is on your desktop.
7. Locate your H: drive and drill down to the **certificates** folder. Look for a file based on your name, machine name and ends with PFX. See the following example.

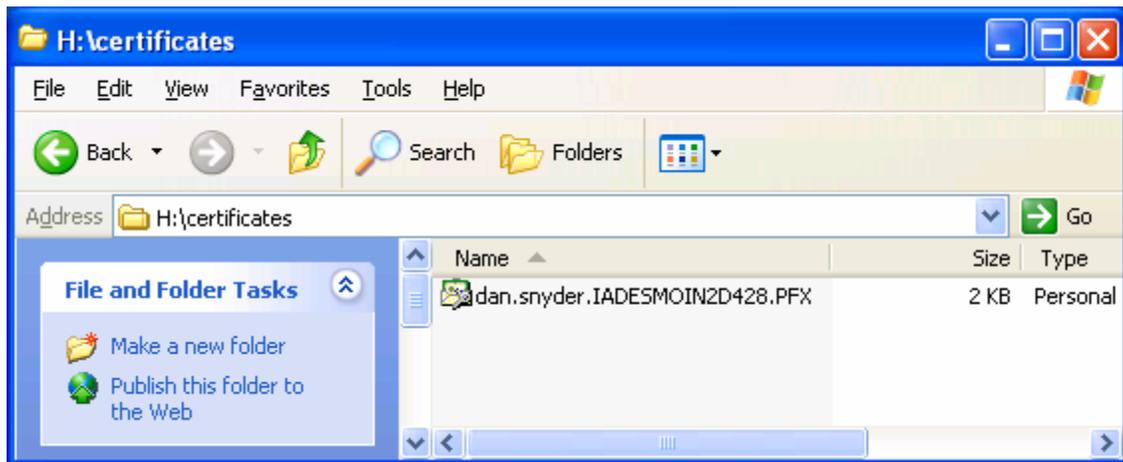


Figure 5.0.c – Verification of Certificate

8. Click on [File] ➔ [Exit].

6. Other Useful Information

6.1. Workstation Backups

One of the workstation backup strategies that has been in place is for a scheduled task that is on the ITS Server to perform a connection to each workstation during the night and utilize the WINZIP software to perform a backup of the user and data files that reside on the workstation. With the implementation of encryption the WINZIP software can not back up the folders which have been encrypted unless the task is performed by the user that owns the files. The workstation backups that are performed from the Server will continue to run but it will only backup the files that are not in the encrypted folders. This allows the data files to still be backed up by a scheduled task.

Until a long term solution can be found it will be necessary for the individual user to perform a backup of the computer by using the **Nightly Backup** menu option that is on the machine.

One item to be aware of is that the manual execution of the nightly backup will only allow the encrypted files of the user that is logged on to be created in the backup zip file. You will get access denied messages for files that are not owned by the user performing the backup.

To perform a manual backup execute the following steps.

1. While logged on as Regular User Account, click [Start] ➔ [All Programs] ➔ [USDA Applications] ➔ [Backup] ➔ [Manual Run of Backup].
2. This will perform a backup of the user files and data files that have been configured on the workstation. A copy of the backup file will be located under the c:\usda\backup folder as well as to the H: drive for the user.

There is also an option to schedule this as a nightly task.

6.2. Moving and Copying Files

When needing to make your files available in other folder locations than the current encrypted folder you need to be aware of what happens to the encryption based on where you place the files or folders. The following guide lines are helpful in understanding this scenario.

- Any file that is created or saved in an encrypted folder will automatically become encrypted and only accessible by the user that placed the file in the folder location.
 - Any files that are saved to the User's desktop will not be encrypted as the desktop is not an encrypted folder location.
- ➡ *Sensitive data should not be stored on the User's desktop.*
- If you attach an encrypted file to an e-mail it will automatically be un-encrypted when the recipient receives the e-mail. Remember it is not a good security practice to send sensitive information via e-mail.
 - If you copy, cut or move files or folders from an encrypted location, the encryption will stay on the files or folders, if they will be placed in another location on the hard drive. For example, you go into WINDOWS EXPLORER and copy a file from c:\home\firstname.lastname and then paste the file into c:\temp. The copied file will now

be in the c:\temp folder and it will be encrypted based on your user account and no one else can open the file.

- If you attempt to copy an encrypted file or folder to the ITS Server the file will not be encrypted.
- Encryption **will not** stay on a file or folder if you write the files to a CD-ROM. The original file or folder that is still on your system will remain encrypted.
- In addition, if you copy the file to a USB Memory Stick, encryption **will not** remain on the file and you will get a screen similar to the one shown in Figure 6.2.a below. The original file or folder that is still on your system will remain encrypted.

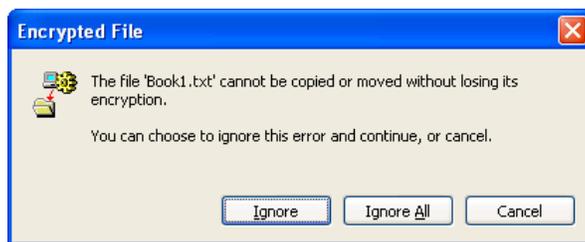


Figure 6.2.a – Encrypted File Screen

6.3. Standard Encrypted Folders

The following folder locations will be encrypted upon setting up encryption for the first time.

- C:\home and all subfolders – The folder specific to the user would be c:\home\firstname.lastname
- User's My Documents Folder, (C:\documents and settings\username\My Documents) - providing they are on the workstation
- User's C:\documents and settings\username\Outlook
- C:\USDA\Backup

6.4. File Strategies

For users that spend most of their time in the office with a network Server and occasionally take their laptop or tablet out of the office, you may want to make sure you save the files that you use on the Server and then when you need to leave the office, copy the files that you need to the encrypted folder (c:\home\firstname.lastname), use them while out of the office and then when you get back copy them back to the Server.

6.5. Data Files for Applications

At this time we are not encrypting folders that would contain data files for applications, with the exception of the Customer Service Toolkit (NRCS) and DALRS (FSA). Additional testing must be performed before we can implement this strategy. If the application allows you to store the file in a different folder and then move it back when needed then you could store the file in an encrypted area and then when you need to access it, move it to the folder where the application resides, un-encrypt the data and then use the data.

- ➡ *Remember if you perform this action you need to make sure you move the data file back to the encrypted folder when you are finished using it.*

6.6. Multiple Users

If there are multiple users that utilize the same computer you will not be able to access the other person's files that are located in their encrypted folder. For example a file located in `c:\home\joe.smith` and was created by joe.smith can not be accessed by another user that logs onto the workstation.

6.7. Opening an Encrypted File of Another User

If you try to open an encrypted file that another user owns you will get an error message similar to the following;

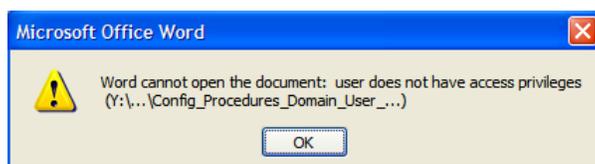


Figure 6.7.a – Access Privileges Screen

6.8. Removing Encryption On A File

1. If is necessary to remove encryption on a file so that someone else can use it you can copy the file to another folder location such as `c:\temp` and then right-click the file and select [Properties].
2. Click on the [Advanced] tab and remove the check mark in front of [Encrypt Contents to Secure Data].
3. Make sure that you do something with the file and then remove it from this location so that the data is secure.