



# Getting Started With Windows Encryption

Author: Deanna Pasternak

Introduction .....	2
What is Encryption? .....	2
Methods of Encryption .....	2
What kinds of data should be encrypted? .....	3
What to do before you Encrypt your data.....	3
How to Encrypt a file or folder in Windows XP.....	3
Things to do after you encrypt your data.....	4
Rules for working with encrypted files.....	4
Emailing and Backing up encrypted files .....	4
Other Things to Note .....	5
Error Messages .....	5
How to decrypt an encrypted file or folder.....	5
Changing your user password.....	6
Encryption in Windows 2000 .....	6
Encryption in Windows Vista.....	6
More Information.....	7
Getting Help .....	7

## Introduction

---

This document is a brief introduction to Encryption on the Windows operating system.

*Note: This document will mainly focus on Windows XP Professional, but there are short sections listed at the end of the document on Windows 2000 and Windows Vista.*

## What is Encryption?

---

Encryption is an effective way to achieve data security by converting your data into a format that cannot be read by others. You can think of encrypting something as translating it into a secret code. In order to translate the code into something that you can read, you need a secret key or password.

## Methods of Encryption

---

There are many different methods of encryption and kinds of data that you can encrypt. For example, you can encrypt emails, your network traffic at different points, and passwords on websites. For this document we will be focusing only on data encryption with the Windows XP Professional operating system; more specifically data that is on your computers hard drive. Windows XP Professional uses the Encrypting File System (EFS).

EFS is not included in Windows XP Home Edition. To verify that you are using Windows XP Professional you can do the following:

Right-click on **My Computer** and choose **Properties**

On the **General** tab, under the **System** section it will list the version of the operating system you are using.

In Windows XP Home edition the option for encryption will still be in the document properties, but it will be grayed out.

## **What kinds of data should be encrypted?**

---

Sensitive data that is kept on your hard drive, especially laptops that travel with you, should be encrypted. Examples of sensitive data are tax return files, online banking information and documents that contain social security numbers.

## **What to do before you Encrypt your data**

---

To ensure that you don't lose data if something happens to your data while it's being encrypted you should always make a backup copy of your data before you encrypt it. You can copy the data to another location on the hard drive or burn the data to a CD or a DVD. Once the files are encrypted successfully you can destroy or delete this backup copy.

## **How to Encrypt a file or folder in Windows XP**

---

1. Click **Start**, point to **All Programs**, point to **Accessories**, then click on **Windows Explorer**
2. Locate and right-click on the file or folder\* that you want to encrypt and click **Properties**.
3. On the **General** tab, click **Advanced**.
4. Under **Compress or Encrypt attributes**, select the **Encrypt contents to secure data** check box, and then click **OK**.
5. In the **Confirm Attribute Changes** dialog box, choose one.
  - If you want to encrypt only the folder, click **Apply changes to this folder only**, and then click **OK**.
  - If you want to encrypt the contents in the folder along with the folder click **Apply changes to this folder, subfolders and files**, and then click **OK**.
6. Windows will now proceed to encrypt your data. How long it takes depends on the amount and size of the files you choose to encrypt. When it is complete the folder will be encrypted. However, this does not mean that others cannot view the contents of the folder. Encrypting the files prevents them from opening items in the encrypted folder. See section following on "Error Messages" that are common to encrypted files.

*Note: While it is possible to encrypt both files and folders, Microsoft's Best Practices suggest encrypting folders not individual files. This prevents applications from unintentionally removing the encryption from a file. For more information see <http://support.microsoft.com/kb/223316>*

## Things to do after you encrypt your data

---

Now that you have encrypted your folders it is important that you do not skip this step to ensure that you do not lose access to your files should you forget your password.

If you do not do this and forget your password, there will be no way to recover your data. It is important to back up your certificate and store it in a secure location.

### How to backup your certificate

1. Start Microsoft Internet Explorer
2. On the **Tools** menu, click **Internet Options**
3. On the **Content** tab, in the **Certificates** section, click **Certificates**.
4. Click the **Personal** tab.

*Note: you may have multiple certificates listed. Click on each one until you find the one that has the **certificate intended purposes** field showing **encryption file system**.*

5. Click **Export** to start the **Certificate Export Wizard**, and then click **Next**.
6. Click **Yes, export the private key** to export the private key, and then click **Next**.
7. Click **Enable Strong protection**, and then click **Next**.
8. Type and confirm a password (You must use a password to protect the exported certificate)
9. Specify the location of where you want to save the key. You can back up to a floppy disk, another location on your hard-drive, or a USB drive. You can also back up the certificate to multiple locations.
10. Specify the destination and click **Next**.

## Rules for working with encrypted files

---

- Encrypted files can be renamed, copied, moved or deleted
- Renaming does not cause decryption, but moving or copying a file can
- When you move or copy an encrypted file to an unencrypted folder, the file is still encrypted.
- If you move or copy the file to a FAT volume\*, a floppy drive or other removable media it will no longer be encrypted.
- Copying to an NTFS formatted USB drive will keep the file encrypted, but if you use that USB drive on another machine, you will need to install the encryption certificate to read that encrypted file.

## Emailing and Backing up encrypted files

---

When you send an encrypted document through email as an attachment the email will be sent and received decrypted.

Please remember that when you backup your encrypted files, if you are not backing them up to an NTFS\* formatted hard disk they will no longer be encrypted and shall be instead stored in a secure location.

## Other Things to Note

---

- \*You can encrypt any file or folders only on NTFS volumes. To check if you are using the NTFS file system double click on **My Computer**. Highlight the volume where the file you are encrypting is located (most likely the C: drive) on the left side you will see details of the drive. Under **File System** the drive will either say NTFS or FAT.
- When you encrypt a file, it will show the file name in green.
- You can not both encrypt and compress documents or folders at the same time.
- This feature is only useful on desktops if you do not allow everyone to log on with the same username or as administrator to your computer.
- You cannot open documents that are stored by other users in an encrypted folder that you create.
- Only the account administrator can by default open encrypted files, not other accounts even if they are given administrator privileges.

## Error Messages

---

If another user attempts to open a Microsoft Word document that is in the encrypted folder, the following message appears:

**Word cannot open the document: *Username* does not have access privileges  
(drive:\filename.doc)**

If another user attempts to copy or move from the encrypted folder to another location on the disk, the following message appears:

**Error Copying File or Folder**

**Cannot copy *Filename*: Access is denied.**

**Make sure the disk is not full or write-protected and that the file is not currently in use.**

## How to decrypt an encrypted file or folder

---

Decrypting a folder uses basically the same process of encrypting the file, but in reverse order.

1. Right-click on the folder or file you want to decrypt, then click **Properties**.
2. Click **Advanced**
3. Click to clear the **Encrypt contents to secure data** check box to decrypt
4. Click **OK** to close the **Advanced Attributes** dialog box.
5. If it is a folder, and it has files in it, the **Confirm Attribute Changes** dialog box appears. You can choose to decrypt only the folder, but this won't decrypt any of the files in the folder.
6. If you want to decrypt all the contents of the folder, click **Apply changes to this folder, subfolders, and files**, and then click **OK**.

## **Changing your user password**

---

If another account (such as the administrator account) changes the password on your account, you will no longer be able to access your encrypted documents. When the administrator tries to change your password they will get the following message

**Warning:** “Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user’s password is reset.”

This feature helps guard against attacks on your machines and against other people accessing your files.

## **Encryption in Windows 2000**

---

The process for encrypting files is the same in Windows 2000 as it is in Windows XP. For the highest level of security for data encryption, you will want to make sure that you are running Windows 2000 SP2.

Information on Windows 2000 SP2

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.msp>

Encrypting files in Windows 2000

<http://support.microsoft.com/kb/222054>

## **Encryption in Windows Vista**

---

Before upgrading to Windows Vista, make sure you check the applications that you use against the UH Vista Application Compatibility askus article at <http://www.hawaii.edu/askus/773>

Windows Vista adds additional security to encryption with BitLocker Drive Encryption in the Enterprise and Ultimate versions. This is a hardware based data protection feature which allows users to encrypt their entire hard drive. Vista also supports EFS in all versions except Windows Starter 2007, Windows Vista Home N (Europe only), and Windows Vista Home Basic.

The University of Hawaii site license will only be able to sell Vista Business OS upgrade, or if you purchased the Software Assurance from the Site License office, Vista Enterprise upgrade is available. You would need the Enterprise version in order to take advantage of the features of BitLocker. Both of these versions support EFS.

Windows Vista BitLocker Step-by-Step Guide

<http://www.microsoft.com/technet/windowsvista/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.msp>

## More Information

---

For more Information on encryption and security:

ITS Helpdesk Security Documents:

<http://www.hawaii.edu/help/security/>

Microsoft Windows Encryption KB article Q308989

<http://support.microsoft.com/kb/308989>

## Getting Help

---

Click on the **Help** link (usually in the upper right hand corner of the window) for on-line help. There is extensive on-line help available. Please refer to this on-line help first for any questions not answered by this document.

For additional assistance, please phone the ITS Help Desk at (808) 956-8883, send e-mail to **help@hawaii.edu**, or fax (808) 956-2108. The Help Desk's toll-free phone number is (800) 558-2669.

Or visit the ITS Help Desk home page at **http://www.hawaii.edu/help**

The ITS Help Desk functions are located in Keller 105, Keller 213, ITS Hamilton Lab (2<sup>nd</sup> Floor Addition) and CLIC Lab (Sinclair Lib, 1<sup>st</sup> Floor) on the UH Mānoa Campus.

The University of Hawai'i is an equal opportunity/affirmative action institution.