Knowledge Base

Best practices for the Encrypting File System

PSS ID Number: 223316

Article Last Modified on 6/10/2004

The information in this article applies to:

- Microsoft Windows XP Professional
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server

This article was previously published under Q223316

SUMMARY

Microsoft Windows includes the ability to encrypt data directly on volumes that use the NTFS file system so that no other user can use the data. You can encrypt files and folders if you set an attribute in the object's **Properties** dialog box.

Because the encryption/decryption process is transparent to users, make sure that organizations that want to use file encryption fully promote strong guidelines about its usage.

MORE INFORMATION

The following is the list of standard practices:

- Teach users to export their certificates and private keys to removable media and store the media securely when it is not in use. For the greatest possible security, the private key must be removed from the computer whenever the computer is not in use. This protects against attackers who physically obtain the computer and try to access the private key. When the encrypted files must be accessed, the private key can easily be imported from the removable media.
- Encrypt the My Documents folder for all users (*User_profile*\My Documents). This makes sure that the personal folder, where most documents are stored, is encrypted by default.
- Teach users to never encrypt individual files but to encrypt folders. Programs work on files in various ways. Encrypting files consistently at the folder level makes sure that files are not unexpectedly decrypted.
- The private keys that are associated with recovery certificates are extremely sensitive. These keys must be generated either on a computer that is physically secured, or their certificates must be exported to a .pfx file, protected with a strong password, and saved on a disk that is stored in a physically secure location.
- Recovery agent certificates must be assigned to special recovery agent accounts that are not used for any other purpose.
- Do not destroy recovery certificates or private keys when recovery agents are changed. (Agents are changed periodically). Keep them all, until all files that may have been encrypted with them are updated.
- Designate two or more recovery agent accounts per organizational unit (OU), depending on the size of the OU. Designate two or more computers for recovery, one for each designated recovery agent account. Grant permissions to appropriate administrators to use the recovery agent accounts. It is a good idea to have two recovery agent accounts to provide redundancy for file recovery. Having two computers that hold these keys provides more redundancy to allow recovery of lost data.
- Implement a recovery agent archive program to make sure that encrypted files can be recovered by using obsolete recovery keys. Recovery certificates and private keys must be exported and stored in a controlled and secure manner. Ideally, as with all secure data, archives must be stored in a controlled access vault and you must have two archives: a master and a backup. The master is kept on-site, while the backup is located in a secure off-site location.
- Avoid using print spool files in your print server architecture, or make sure that print spool files are generated in an encrypted folder.
- The Encrypting File System does take some CPU overhead every time a user encrypts and decrypts a file. Plan your server usage wisely. Load balance your servers when there are many clients using Encrypting File System (EFS).

How to enable Encrypting File System file sharing

In Microsoft Windows XP, EFS supports file sharing of encrypted files among multiple users. With this support, you can give individual users permission to access an encrypted file. The ability to add additional users is restricted to individual files. Support for multiple users on folders is not provided in either Microsoft Windows 2000 or Windows XP. Also, support for the use of groups on encrypted files is not provided by EFS.

After a file has been encrypted, file sharing is enabled through a new button in the user interface. A file must be encrypted first and then saved before additional users can be added. Users can be added either from the local computer or from the Active Directory directory service if the user has a valid certificate for EFS. The ability to add additional users is restricted to individual files. Support for multiple users on EFS encrypted folders is not provided. Also, only individual users can be added to files. Support for the use of groups on encrypted files is not provided by EFS.

For information about how to enable EFS encryption on folders and files, see the "How to encrypt and decrypt using the Encrypting File System" section.

How to encrypt a file for multiple users

Note This procedure applies to Windows XP only. You cannot encrypt a file for multiple users in Windows 2000.

To do this, follow these steps:

1. Start Microsoft Windows Explorer, and then select the encrypted file that you want to add additional users to.
2. Right-click the encrypted file, and then click **Properties**.
3. Click **Advanced** to access the EFS settings.
4. Click **Details** to add additional users.
5. Click **Add**. The **Add** dialog box will display any other EFS-capable certificates in your personal store or those of any other users who

may be in your "Other People" and "Trusted People" certificate stores.

If you do not see the user who you want to add, click **Find User** to search Active Directory. The **Select User** window appears. A dialog box displays valid EFS certificates in Active Directory based on your search criteria. If no valid certificate is found for that user, a message will inform you that there are no appropriate certificates for the selected user. In this case, the intended users must send you a copy of their certificate for you to import. You can then add them to your encrypted file.

6. Select the certificate of the user who you want to add, and then click **OK**. You will be returned to the **Details** tab, and the tab will show the multiple users who will have access to the encrypted file and the users' EFS certificates.
7. Repeat this process until you have added all the users who you want to add. Click **OK** to register the change and continue.

Note Any user who can decrypt a file can also remove other users if the user who does the decrypting also has write permissions on the file.

How to encrypt and decrypt using the Encrypting File System

The following steps encrypt and decrypt a file or folder using the Encrypting File System.

Note These guidelines apply to Windows 2000 and Windows XP.

Encrypting a folder

Although you can encrypt files individually, we strongly recommend that you designate a specific folder for storing encrypted data.

Encrypt a folder and its contents

Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.

To encrypt a folder and its current contents, follow these steps:

1. Right-click the folder that you want to encrypt, and then click **Properties**.
2. In the **Properties** dialog box, click **Advanced**.
3. The **Advanced Attributes** dialog box displays attribute options for compression and encryption. This dialog box also includes archive and indexing attributes.

   Note Although the NTFS file system supports both compression and encryption, it does not support both at the same time. This means that you can only select one or the other. A file or folder cannot be both encrypted and compressed at the same time.

   To encrypt the folder, click to select the **Encrypt contents to secure data** check box, and then click **OK**.
4. Click **OK** to close the **Advanced Attributes** dialog box.
5. If the folder you chose to encrypt in steps 1 to 3 already contains files, a **Confirm Attribute Changes** dialog box will appear.

   You can choose to encrypt only the folder so that all files subsequently moved to the folder or created in this folder will be encrypted. If you want to also encrypt all the contents of this folder, click **Apply changes to this folder, subfolders, and files**, and then click **OK**.

Decrypting a folder

To decrypt a folder, use basically the same process but in reverse order:

1. Right-click the folder that you want to decrypt, and then click **Properties**.
2. Click **Advanced**.
3. Click to clear the **Encrypt contents to secure data** check box to decrypt the data.
4. Click **OK** to close the **Advanced Attributes** dialog box.
5. Click **OK** to close the **Properties** dialog box.
6. If the folder has files in it, the **Confirm Attribute Changes** dialog box appears. You can choose to decrypt only the folder. However, this will not decrypt any files currently contained in the folder.

   If you want to decrypt all the contents of this folder, click **Apply changes to this folder, subfolders, and files**, and then click **OK**.

Additional information

How files are encrypted

Files are encrypted through the use of algorithms that essentially rearrange, scramble, and encode the data. A key pair is randomly generated when you encrypt your first file. This key pair is made up of a private and a public key. The key pair is used to encode and decode the encrypted files.

If the key pair is lost or damaged and you have not designated a recovery agent, and then there is no way to recover the data.

Why you must back up your certificates

Because there is no way to recover data that has been encrypted with a corrupted or missing certificate, it is critical that you back up the certificates and store them in a secure location. You can also specify a recovery agent. This agent can restore the data. The recovery agent's certificate serves a different purpose than the user's certificate.

How to back up your certificate

To back up your certificates, follow these steps:

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 There may be several certificates present, depending on whether you have installed certificates for other purpose.
5. Select one certificate at a time until the **Certificate Intended Purposes** field shows **Encrypting File System**. This is the

certificate that was generated when you encrypted your first folder.

6. Click **Export** to start the **Certificate Export Wizard**, and then click **Next**.
7. Click **Yes, export the private key** to export the private key, and then click **Next**.
8. Click **Enable Strong protection**, and then click **Next**.
9. Type your password. (You must have a password to protect the private key.)
10. Specify the path where you want to save the key. You can save the key to a floppy disk, another location on the hard disk, or a CD. If the hard disk fails or is reformatted, the key and the backup will be lost. (If you back up the key to a floppy disk or CD, you must store that disk or CD in a secure location.)
11. Specify the destination, and then click **Next**.

For additional information about the Encrypting File System (EFS), visit the following Microsoft Web sites:

Encrypting File System in Windows 2000
http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp

Encrypting File System in Windows XP and Microsoft Windows Server 2003
http://www.microsoft.com/WINDOWSXP/pro/techinfo/administration/recovery/default.asp

Keywords: kbhowto kbenv kbinfo KB223316
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch kbWinXPPro kbWinXPProSearch kbWinXPSearch

---