

Operating System

Encrypting File System in Windows XP and Windows Server 2003

Microsoft Corporation

Published: August 2002

Abstract

Microsoft® Windows® XP and Windows Server 2003 provide many enhancements in the area of data protection— especially Encrypting File System (EFS). This article provides a technical walkthrough that illustrates how to use important data recovery and protection features in various Windows platforms. Also included are best practices and the steps needed to build an effective data recovery and protection strategy.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This technical article is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2002 Microsoft Corporation. All rights reserved. Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

[Introduction 5](#_Toc30305700)

[EFS Enhancements in Windows XP and Windows Server 2003 6](#_Toc30305701)

[Data Recovery Overview 7](#_Toc30305702)

[Data Recovery and EFS 8](#_Toc30305703)

[Data Recovery on Standalone Machines 9](#_Toc30305704)

[Data Recovery Using EFS 10](#_Toc30305705)

[EFS File Sharing 10](#_Toc30305706)

[Enabling EFS File Sharing 10](#_Toc30305707)

[Changes in Windows Server 2003 16](#_Toc30305708)

[Copying, Moving and Saving Encrypted Files 18](#_Toc30305709)

[Saving Files with EFS File Sharing 19](#_Toc30305710)

[System Folders and Files 19](#_Toc30305711)

[Certificate Caching 19](#_Toc30305712)

[EFS Recovery Policy Procedures 21](#_Toc30305713)

[Removing an Existing Recovery Policy 21](#_Toc30305714)

[Determining If EFS is Being Used on a Machine 22](#_Toc30305715)

[Disabling EFS 22](#_Toc30305716)

[Performing Data Recovery 23](#_Toc30305717)

[Importing and Exporting Data Recovery Agent Keys 24](#_Toc30305718)

[Exporting Keys 24](#_Toc30305719)

[Importing Keys 28](#_Toc30305720)

[Enabling Encrypt/Decrypt on the Windows Explorer Menu 30](#_Toc30305721)

[Data Recovery—Best Practices 31](#_Toc30305722)

[Central Recovery Workstation 31](#_Toc30305723)

[EFS and Certification Authorities 31](#_Toc30305724)

[Auto-enrollment 31](#_Toc30305725)

[Using Default Domain Configuration 32](#_Toc30305726)

[Lost or Expired DRA Private Keys 32](#_Toc30305727)

[Data Protection—Best Practices 33](#_Toc30305728)

[Deleting PlainText Data 33](#_Toc30305729)

[Reducing the Risk of Discovery of Plaintext Shreds 34](#_Toc30305730)

[Cipher.exe Command-line Utility 34](#_Toc30305731)

[Encrypting Offline Files 35](#_Toc30305732)

[Permanent Offline Users 37](#_Toc30305733)

[EFS with WebDAV Folders 37](#_Toc30305734)

[Clearing Page File at Shutdown 37](#_Toc30305735)

[Default Encryption Algorithms 38](#_Toc30305736)

[Show Encrypted Files in Color 40](#_Toc30305737)

[Using EFS with Standalone Machines or NT 4.0 Domains 41](#_Toc30305738)

[Managing EFS in a Non-Active Directory Environment 41](#_Toc30305739)

[Resetting Local Passwords on Windows XP 43](#_Toc30305740)

[Encrypted Files on a Server 43](#_Toc30305741)

[Delegated Server Mode 44](#_Toc30305742)

[File Sharing on Remote Servers 44](#_Toc30305743)

[Performance 45](#_Toc30305744)

[Disaster Recovery 45](#_Toc30305745)

[EFS with WebDAV Folders 46](#_Toc30305746)

[Migrating to New Certificates 48](#_Toc30305747)

[Third Party Certification Authorities 48](#_Toc30305748)

[EFS and System Restore 48](#_Toc30305749)

[Best Practices 49](#_Toc30305750)

[Data Recovery Versus Key Recovery 50](#_Toc30305751)

[Advantages of Data Recovery 50](#_Toc30305752)

[Disadvantages of Data Recovery 50](#_Toc30305753)

[Advantages of Key Recovery 51](#_Toc30305754)

[Disadvantages of Key recovery 51](#_Toc30305755)

[Troubleshooting 52](#_Toc30305756)

[Data Protection API 54](#_Toc30305757)

[Summary 56](#_Toc30305758)

[Related Links 57](#_Toc30305759)

[Knowledge Base Articles on EFS 58](#_Toc30305760)

# Introduction

Microsoft® Windows® XP and Windows Server 2003 provide significant advancements in data recovery and protection and private key recovery. Microsoft Windows 2000 introduced the capability for data protection and protected data recovery with the implementation of Encrypting File System (EFS), and this capability has been enhanced in Windows XP and Windows Server 2003.

EFS—in Windows 2000, Windows XP and Windows Server 2003—supports the use of data recovery agents (DRA) to decrypt files that have been encrypted by other users.

This article is intended to assist system architects and administrators in developing best practices for creating data recovery and data protection strategies using Windows XP and Windows Server 2003.

In addition to explaining strategies for data recovery and data protection in Windows XP, this article includes many step-by-step examples that illustrate how to set up the data recovery and data protection features you’ll want to use when deploying a Windows XP data recovery and protection solution.

The main topics discussed include:

* [EFS Enhancements in Windows XP and Windows Server 2003](#_EFS_Enhancements_in_Windows XP)
* [Data Recovery Overview](#_Data_Recovery)
* [Data Recovery Using EFS](#_Data_Recovery_Using)
* [Data Recovery—Best Practices](#_Data_Recovery—Best_Practices)
* [Data Protection—Best Practices](#_Data_Protection—Best_Practices)
* [Data Recovery Versus Key Recovery](#_Data_Recovery_Versus_Key Recovery)
* [Troubleshooting](#_Troubleshooting)

**Note** EFS is not available in Windows XP Home Edition.

# EFS Enhancements in Windows XP and Windows Server 2003

The increased functionality of EFS has significantly enhanced the power of the Windows XP Professional client. Windows XP Professional now provides additional flexibility for corporate users when deploying security solutions based on encrypted data files and folders. These new features include:

* Full support for revocation checking on certificates used when sharing encrypted files
* Support for EFS with Windows Server 2003 clusters
* Alternate color support (green) for encrypted files to easily locate and verify protected files
* Support for encrypted offline folders in Windows XP
* Multi-user support for encrypted files in the shell user interface (UI)
* Support for Microsoft Enhanced and Strong cryptographic service providers (CSPs)
* Additional support for enhanced algorithm options and strengths
* End-to-end encryption using EFS over WebDAV
* Enhanced recovery policy flexibility
* Performance and reliability enhancements
* Additional security features for protecting EFS data

Read the article What’s New in Security for Windows XP to learn more about EFS enhancements in Windows XP—[http://www.microsoft.com/windowsxp/pro/techinfo/howitworks/security/default.asp.](http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/home.asp)

# Data Recovery Overview

Data recovery is a process by which individual data elements such as files or folders are encrypted for more than one person or entity. By encrypting for more than one person or escrow entity, multiple paths for data decryption are made available, An escrow entity may be a designated administrator within an organization to perform a data recovery role. Data recovery does not necessarily imply that private key recovery has occurred, however, key recovery may be one method to achieve data recovery. Data recovery can be achieved without private key recovery in the Windows XP operating system.

Both Secure Multi-purpose Internet Mail Extensions (S/MIME) and EFS use symmetrically encrypted data blocks, with the symmetric key being protected by one or more public keys of a public/private key pair. In this scenario, the symmetric key may be protected (encrypted) with more than one user, and therefore more than one public key.

Data recovery can occur through a second user decrypting the data. In the case of EFS, files can be opened and data recovered through the use of a data recovery agent (DRA) as shown in Figure 1 below.



Figure 1: Recovering data

In Windows 2000, a DRA is mandatory and by default is the domain administrator for a Windows 2000 domain. Windows XP eliminates this limitation.

Data recovery is managed most effectively by using Active Directory™ and a Microsoft enterprise certification authority. Using Group Policy, Active Directory provides a mechanism to centrally configure one or more data recovery agents. These DRAs have the ability to recover user files should data recovery be necessary.

## Data Recovery and EFS

EFS provides built-in data recovery by enforcing a recovery policy requirement. Windows 2000 mandated a requirement that a recovery policy must be in place before users can encrypt files. The *recovery policy* is a type of public key policy that provides for one or more user accounts to be designated as a DRA. A default recovery policy is automatically put in place for the domain when the administrator logs on to the system (domain controller) for the first time, making the administrator the recovery agent for the domain. Windows XP and Windows Server 2003 no longer require a recovery policy to be in effect to encrypt files.

The default recovery policy is configured locally for standalone computers. For computers that are part of an Active Directory-based domain, the recovery policy is configured at the site, domain, organizational unit (OU), or individual computer level, and applies to all Windows 2000- and Windows XP-based computers within the defined scope of influence. Recovery certificates can be issued by a certification authority (CA) and managed using the Microsoft Management Console (MMC) Certificates snap-in.

In a network environment, the domain administrator controls how EFS is implemented in the recovery policy for all users and computers in the scope of influence. In a default Windows 2000 or Windows Server 2003 installation, when the first domain controller is set up, the domain administrator is the specified recovery agent for the domain. The way the domain administrator configures the recovery policy determines how EFS is implemented for users on their local machines. To change the recovery policy for the domain, the domain administrator logs on to the first domain controller. If a machine is a stand-alone (not joined to a domain), the expiration period of a self-issued administrator account DRA certificate is 100 years. If a machine is joined to a domain, the default DRA certificate issued to the domain administrator has an expiration period of three years.

Administrators can define one of three types of policies:

**Recovery agent policy**. When an administrator adds one or more recovery agents, a recovery-agent policy is in effect. These agents are responsible for recovering any encrypted data within their scope of administration. This is the most common type of recovery policy.

**Empty recovery policy**. When an administrator deletes all recovery agents and their public-key certificates, an empty recovery policy is in effect. An empty recovery policy means that no recovery agent exists, and if the client operating system is Windows 2000, EFS is disabled in this configuration. The Windows XP client allows EFS to operate with an empty DRA policy.

**No recovery policy**. When an administrator deletes the private keys associated with a given recovery policy, a no-recovery policy is in effect. Because no private key is available, there is no way to use a recovery agent and recovery will not be possible. This would be useful for organizations with a mixed environment of Windows 2000 and Windows XP clients where no data recovery is desired.

Although the domain administrator is the default DRA in an Active Directory environment, this capability can be delegated or assigned to one or more users. This is discussed in greater detail later in this article.

### Data Recovery on Standalone Machines

Windows XP no longer creates a default DRA on newly installed machines in a workgroup or in a domain. This effectively prevents previous offline attacks against the administrator account. If a machine is joined to a domain, all users, including local users, inherit the recovery policy form the domain. For workgroup machines, a DRA must be created manually by a user and installed. To manually create a DRA, the cipher.exe utility must be used.

CIPHER /R:filename

/R Generates a PFX and a CER file with a self-signed EFS recovery

certificate in them.

filename A filename without extensions

This command will generate filename.PFX (for data recovery) and filename.CER (for use in the policy). The certificate is generated in memory and deleted when the files are generated. Once the keys have been generated the certificate should be imported into the local policy and the private keys stored in a secure location.

# Data Recovery Using EFS

This section discusses and illustrates the steps required for using EFS file sharing.

## EFS File Sharing

Support for the use of groups on encrypted files is not provided by EFS. Also, support for multiple users on folders is not provided in either Windows 2000 or Windows XP. However, in Windows XP, EFS does support file sharing between multiple users on a single file.

The use of EFS file sharing in Windows XP provides another opportunity for data recovery by adding additional users to an encrypted file. Although the use of additional users cannot be enforced through policy or other means, it is a useful and easy method for enabling recovery of encrypted files by multiple users without actually using groups, and without sharing private keys between users.

Once a file has been initially 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 may be added. After selecting the **Advanced Properties** of an encrypted file, a user may be added by selecting the **Details** button. Individual users may add other users (not groups) from the local machine or from the Active Directory, provided the user has a valid certificate for EFS.

### Enabling EFS File Sharing

Sharing encrypted files using EFS has been supported since Windows 2000 through Win32 application program interfaces (API), but EFS has not been exposed in the Windows Explorer user interface until the development of the Windows XP Professional client.

**To encrypt a file for multiple users**

1. Open Windows Explorer and select the file you want to encrypt
2. Right-click the chosen file and select **Properties** from the context menu.
3. Select the **Advanced** button to enable EFS.
4. Encrypt the file by selecting the **Encrypt contents to secure data** check box as shown in Figure 2 below. Click OK.

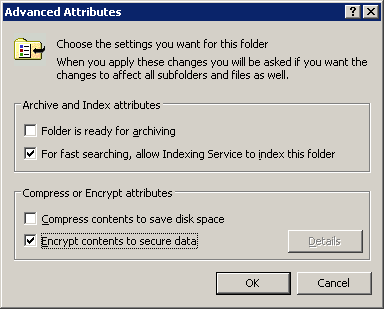


Figure 2. Encrypting contents to secure data

**Note** A file cannot be both compressed and encrypted at the same time.

If this is the first time this file or folder has been encrypted, a dialog box will appear asking if you would like to encrypt the file only or the folder.

1. Select the appropriate choice and click OK. This will return you to the original dialog box.

**Note** The file is not encrypted until you click **OK**. Also, additional users may not be added until the file has been encrypted by the first user.

1. Click OK to encrypt the file.
2. Open the file properties again through the **Advanced** properties button and then select the **Details** button to add additional users. Once the Details dialog box is open, the add user option will be displayed.

**Note** Additional information is available in the Encryption Details dialog box which may be useful for troubleshooting purposes.

**To add users**

1. Click the **Add** button as shown in Figure 3 below.

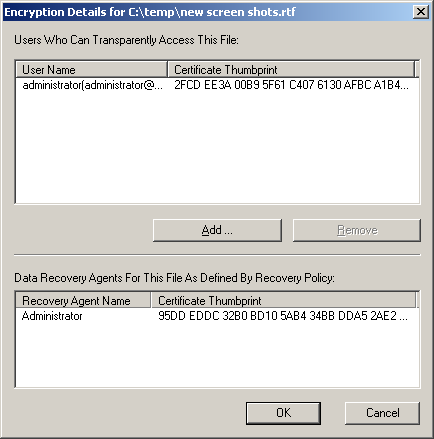


Figure 3. Adding users from Windows XP

A new dialog box will be presented showing the existing users and certificates that are cached in the “Other People” and “Trusted People” certificate stores of the local machine. EFS generated certificates (self-signed certificates) will be cached in the local machine Trusted People Store. Certificates enrolled manually or automatically through auto-enrollment for the user will be cached in the local machine Other People store. It will also allow new users to be added from the Active Directory by clicking the **Find User** button.

**Note** A user must have a valid EFS certificate in the Active Directory to be added.

1. Click the **Find User** button to find new users as shown in Figure 4 below.

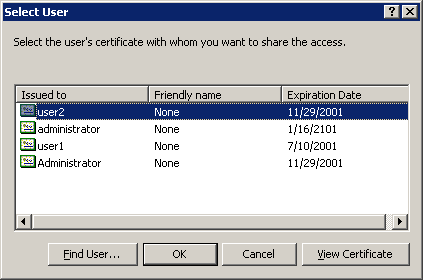


Figure 4. Finding new users from Active Directory

The standard object picker dialog box will be displayed and a search will be conducted.

A dialog box will display users that hold valid EFS certificates in the Active Directory based on your search criteria. If no valid certificate is found for the given user, the dialog box shown below in Figure 5 will be displayed:



Figure 5. Finding user search results

If valid certificates exist in the **userCertificate** attribute of the user object in the directory, they will be displayed in the certificate selection dialog box shown below in Figure 6. This feature will work best when a user has a roaming user profile and only one EFS certificate stored on their user account in Active Directory. If roaming user profiles are not used, multiple certificates may be available on the user account and subsequently, not available when encrypting files on some servers. Note that machine certificates (denoted by a machine name with a $ extension) may be displayed in this UI if encrypted offline folders is in effect on the local machine.

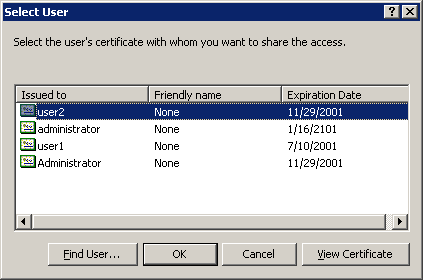


Figure 6. List of user certificates

**Revocation Checking**

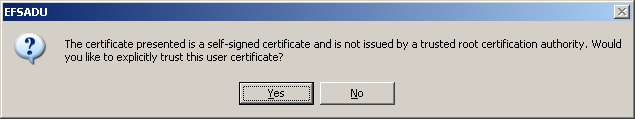
Windows XP and Windows Server 2003 now performs revocation checking on all certificates for other users when they’re added to an encrypted file. For performance reasons, users that hold a private key and recovery agent certificates are not checked for revocation, they are only verified for time validity. However, user certificates that do not contain a CDP (Certificate Revocation List Distribution Point) extension (such as those from some 3rd party CAs) will not be validated for revocation status when added to a file. If the user does not chain to a trusted root CA certificate, or the certificate is not installed in the Trusted People certificate store, the user will be warned before adding the certificate. If the revocation status check on a certificate fails, the messages shown in Figure 7 below will be displayed and the certificate will not be used.

  
or



Figure 7. Failed check of certificate revocation status

If the user selects to add a certificate that does not chain to a trusted root certificate authority, it will not be added:

If the user selects to add a self-signed cert that was installed by another user on the same machine, the user will be allowed to add it if they choose “Yes”:

If the revocation status and chain building completed successfully, the user will be added to the dialog box and the file updated as shown in Figure 8 below. For more information on certificate status and chain building, refer to the following whitepaper: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp>

1. Click **OK** to register the change and continue.

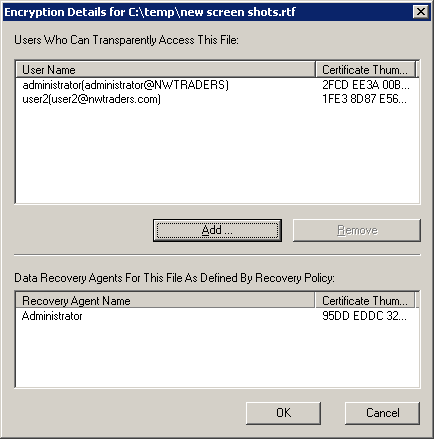


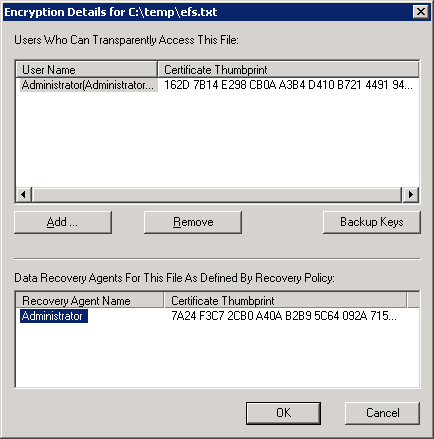
Figure 8. Successfully adding a new user

**Note** Any user that can decrypt a file can also remove other users if the user doing the decrypting also has write permission.

**Note** EFS has a limit of 256K in the file header for the EFS metadata. This limits the number of individual entries for file sharing that may be added. On average, a maximum of 800 individual users may be added to an encrypted file.

### Changes in Windows Server 2003

Several enhancements in the user interface with Windows Server 2003 are available that do not appear in Windows XP or Windows 2000. Windows Server 2003 enables users to backup their EFS key(s) directly from the command-line or the file details property page, as show in the following illustration, by clicking on the **Backup Keys** button:



To backup EFS key(s) from the command-line, the cipher.exe utility may be used:

CIPHER /X[:efsfile] [filename]

/X Backup EFS certificate and keys into file filename. If efsfile is

provided, the current user's certificate(s) used to encrypt the

file will be backed up. Otherwise, the user's current EFS

certificate and keys will be backed up.

Filename: A filename without extensions.

Efsfile: An encrypted file path.

**To view the certificate for information**

You can select a user certificate, and view the certificate for information to make your administrative decision. To view a certificate, as shown in Figure 6 above, complete the following steps:

1. Highlight the certificate in the dialog box and click the **View Certificate** button.
2. Click **OK** to close this dialog box when finished. You will be returned to the previous dialog box within which you can choose the appropriate user to be added to the encrypted file.
3. Highlight the selected user certificate that you want to use and click OK

### Copying, Moving and Saving Encrypted Files

Because of the unique nature of encrypted files, different results can occur when moving or copying encrypted files between locations. For example, when copying an encrypted file from a local machine to a server on the network, different results of the copy operation will occur depending on the operating system being used on the server. In general, copying a file will inherit the EFS properties of the target, but a move operation will not inherit the EFS properties of the target folder.

**When copying an encrypted file:**

* If using Windows 2000 and the target server is running Microsoft Windows NT® Server 4.0, the file will be silently decrypted and copied to the server. If using Windows XP or Windows Server 2003, the user will be warned and prompted to allow the decryption operation.
* If the target server is running Windows 2000 or Windows Server 2003, and the machine account of the server is trusted for delegation in the Active Directory, the file will be silently decrypted and copied to the server where it will be re-encrypted using a local profile and encryption key.

**Note** The file is transmitted on the network between the client and the server in an unprotected format. If this file contains confidential information, care should be given to ensure that the network connection also provides secure transmission of the data. Such network data protection might include IP Security (IPSec).

* If the target server is running Windows 2000 or Windows Server 2003 and the machine account of the server is not trusted for delegation in the Active Directory, or the server is in a workgroup or a Windows NT 4.0 domain, the file will not be copied and the user will receive an “access denied” error message.

The “access denied” error message is returned to applications from the NTFS file system in order to ensure compatibility with existing applications. The use of an alternate or more descriptive error message would cause many applications to fail or behave erratically.

The Windows XP Professional client contains some enhancements in the area of copying encrypted files. Both the shell interface and the command-line now support an option to allow or disallow file decryption. When an encrypted file is copied to a target location that does not allow remote encryption, the user will be prompted with a dialog box that allows a choice of whether or not to decrypt the file.

**The command-line tools**, XCOPY and COPY, allow the same behavior through a special parameter switch to allow decryption on the copy operation.

C:\>copy /? (Copies one or more files to another location.)

COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/A | /B ] source [/A | /B]

[+ source [/A | /B] [+ ...]] [destination [/A | /B]]

source

(Specifies the file or files to be copied.)

/D (Allows the destination file to be created decrypted.)

Note: This will allow a file to be created in plain text on the destination location/server if remote encryption is not supported on the target server.

C:\>xcopy /? (Copies files and directory trees.)

XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]

[/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]

[/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z]

[/EXCLUDE:file1[+file2][+file3]...]

source

(Specifies the files to copy.)

destination (Specifies the location and/or name of new files.)

/G (Allows the copying of encrypted files to a destination that does not support encryption.)

**Note** Windows Server 2003 and Windows XP Service Pack allow for a registry setting that will allow files to be decrypted silently by applications or by using the command-line without the additional command-line parameters. To set this option create the following registry DWORD value:

HKLM\Software\Policies\Microsoft\Windows\System\

DWORD Name: CopyFileAllowDecrypted**Remote**Destination

Value: 1

### Saving Files with EFS File Sharing

When a file has been encrypted for multiple users, an application must call a specific API to ensure that the encryption data (certificates) for the additional users is not lost when the file is opened, modified and saved in its native application file format. Native documents opened with Microsoft Office XP will retain the multi-user EFS status while other applications may remove the additional users that were added to the file. Consult the manufacturer of your specific application for more details about its interoperability with EFS.

## System Folders and Files

The operating system also prevents encryption of system folders, files and locations in the %SYSTEMROOT%\... path. When a user attempts to encrypt a system file, or attempts to copy an encrypted file into the system path, the user will receive an “access denied” message.

## Certificate Caching

Once EFS uses a certificate, it is cached on the local machine. This eliminates the need for looking up users in Active Directory every time a new user is added to an encrypted file. Certificates that are part of a certificate chain, and self-signed certificates, can be used and cached. When a user certificate that is part of a certificate chain is added to an encrypted file, the certificate will be cached in the current user’s “Other People” certificate store as shown in Figure 9 below.

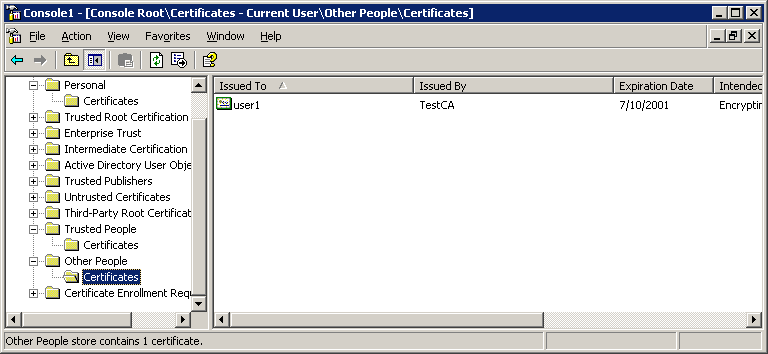


Figure 9. Caching User certificate in “Other People” certificate store

Certificates for other people that are self-signed, such as those generated automatically by EFS when no certification authority is available, are cached in the “Trusted People” certificate store of the current user as shown in Figure 10 below:

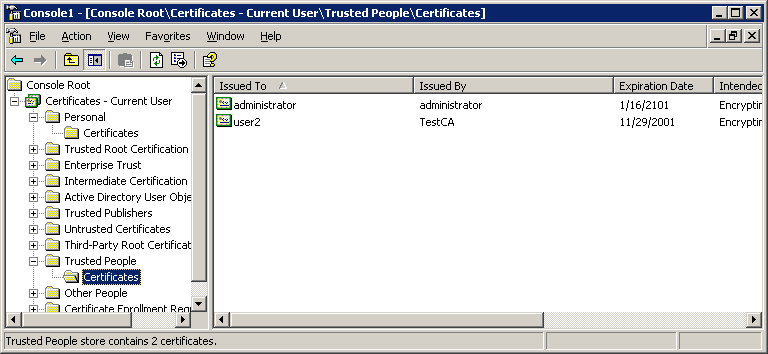


Figure 10. Caching user certificate in the “Trusted People” certificate store

When a certificate is added to the “Trusted People” store, the user is warned that the certificate will be explicitly trusted and asks the user to verify the action. Once a certificate is added to the Trusted People store, no certificate status checking will be performed with the exception of time validity. The Microsoft Outlook® 2002 client may also use the “Trusted People” CryptoAPI store for storage of individual certificate trust decisions.

**Note** Users that hold a private key on the local machine are also added to the “Trusted People” store, in addition to the “Other People” store. This enhances the performance of local encryption on the machine.

## EFS Recovery Policy Procedures

Some of the most common procedures in relation to EFS and data recovery are outlined in the following sections.

### Removing an Existing Recovery Policy

It is possible that an organization may implement a data recovery policy initially, and at a later date choose to remove or eliminate that recovery policy. When a recovery policy has been removed from a domain, no new files may be encrypted after the group policy on Windows 2000 machines has been updated. Windows XP and Windows Server 2003 computers will be unaffected. Users will still be able to open existing encrypted files, but they will not be able to update or re-encrypt those files. Existing encrypted files will not be decrypted until they are accessed and updated by a user that has a private key to decrypt those files.

#### Changing the Recovery Policy for a Domain

1. Open the Active Directory MMC snap-in—Users and Computers for Windows Server 2003.
2. Right-click the domain whose recovery policy you want to change, and then click Properties.
3. Right-click the recovery policy you want to change, and then click Edit.
4. In the console tree, click Encrypting File System. Click through the following path:

* Computer configuration
* Windows settings
* Public Key Policies within Security Settings
* Encrypted Data Recovery Agents

1. Right-click in the details pane and select **Add Data Recovery Agent** or **Create Data Recovery Agent**.

**Important** Before changing the recovery policy in any way, you should first back up the recovery keys to a floppy disk.

**Note** You must be logged on as an administrator of the domain or a user that has rights to update group policies in the domain or OU selected. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

### Determining If EFS is Being Used on a Machine

Some organizations may find it useful to see if users are using EFS on machines in the domain. Although there is no way to determine if EFS is being currently used, several registry keys may be examined to determine if EFS has ever been used by the user on the machine.

If the machine is a Windows 2000 machine, the following registry key can be examined to see if a certificate hash exists:

* **HKCU\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys\CertificateHash**

If the machine is running Windows XP, the following registry keys may be examined:

* **HKCU\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys\CertificateHash**
* **HKCU\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys\Flag**

## Disabling EFS

Disabling EFS is now possible using Windows XP if you want to block certain computers from allowing users within a specific domain or OU in the Active Directory from encrypting data. In a domain environment, EFS may be disabled on computers by using Group Policy.

**To set Group Policy for EFS**

1. Click through the following path in the Group Policy MMC snap-in:

* Computer configuration
* Windows settings
* Security settings
* Public Key Policies
* Encrypting File System

1. Select **Properties**
2. Remove the check from the check box to disable EFS as shown in Figure 11 below.

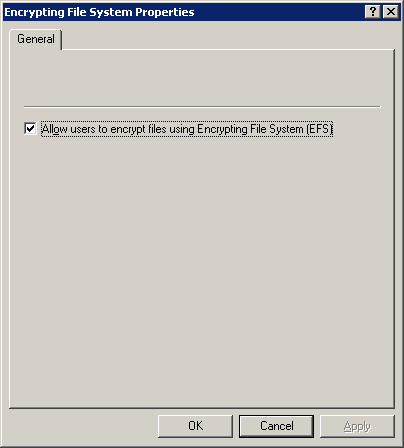


Figure 11. Disabling EFS using Group Policy

Group Policy sets a registry key which is checked by EFS during user operations. The key is:

**HKLM\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\EFS\EfsConfiguration**

In the case of local machines that are not members of a domain, local policy is not available for disabling EFS. However, a different registry key may be set to disable EFS. If the key is set to a DWORD value of 0x01, EFS will be disabled. Registry key:

**HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\EfsConfiguration**

## Performing Data Recovery

Data Recovery is performed in the same manner as file encryption. The only difference is that data recovery implies that a person other than the original user is decrypting the files. Since all files should have at least one user, and one DRA who can decrypt a file, no special process is required to recover a file that has been encrypted by another user.

**To recover a file** for a user that has left the organization, lost their private keys, corrupted private keys, etc., the DRA selects the files in question and opens them normally. The files, once opened, will be in clear form and can be saved in a non-encrypted format.

**Note** The DRA must have the private key of the DRA certificate to perform recovery locally.

**A DRA may also remove encryption** without first opening the files by selecting the files in question, selecting the file properties, choosing the **Advanced** button, and clearing the **Encrypt contents to secure data** checkbox. After clicking **OK** and closing the file properties, the file will be decrypted. These methods are available on Windows 2000, Windows XP and Windows Server 2003 computers.

**Note** A DRA must also have the write permission to decrypt a file in addition to holding the appropriate recovery private key.

## Importing and Exporting Data Recovery Agent Keys

The following steps and illustrations outline the process for importing and exporting DRA keys.

### Exporting Keys

Perform the following steps to export the certificate and private key of the default domain DRA:

1. Log on to the domain with the administrator account on the first domain controller in the domain.
2. Select **Run** from the Start menu.
3. Type **mmc.exe** and press **Enter**. An empty MMC shell starts up.
4. Select the Console menu, and then select **Add/Remove** **Snap-In**. A dialog box appears with a list of all the snap-ins that have been added to this MMC shell.
5. Click the **Add** button. A list of all the registered snap-ins on the current machine appears.
6. Double-click on the **Certificates** snap-in. Choose **My User Account** then click the **Finish** button.
7. Click the **Close** button on the Add Standalone Snap-In dialog box, then click **OK** on the Add/Remove Snap-in dialog box. The MMC now contains the personal certificate store for Administrator.
8. Expand the tree view of the certificate store. Click through **Certificates**, **Current User**, **Personal**, and then **Certificates** as shown in Figure 12 below. When clicking on the Certificates folder on the left, the right-hand pane will display a list of all the certificates for the administrator account. By default, two certificates will most likely be in the store.

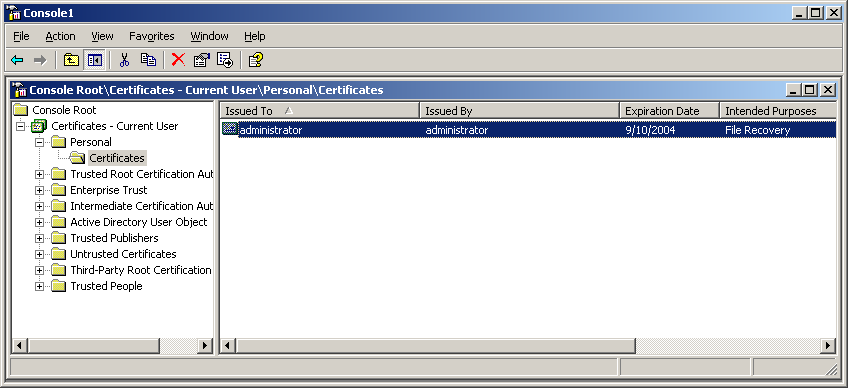


Figure 12. Working with the file recovery certificate

1. Right-click on the certificate intended for file recovery. This default domain DRA certificate should have a 3-year lifetime.
2. After right-clicking on the file recovery certificate, choose **All Tasks** and then **Export** from the context menu. A wizard will guide the export process.

**Important** It’s critical that you choose the correct key during the export process, because once the export process is complete the original private key and certificate will be deleted from the computer. If it cannot be restored to the computer, then file recovery will not be possible using that DRA certificate.

1. Choose **Yes, export the private key** as shown in Figure 13 below and then click **Next**.

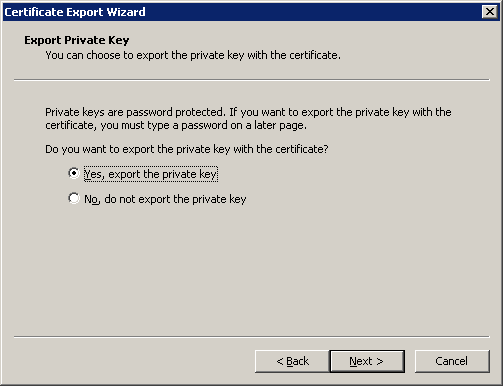


Figure 13. Exporting the private key

**Important** It is important to ensure that the “Yes, export the private key” radio button is selected in the wizard to guarantee that the private key is removed from the computer when the export is complete.

When exporting a private key, the \*.PFX file format is used. The \*.PFX file format is based on the PKCS #12 standard which is used to specify a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc. For additional information, refer to the PKCS #12 standard listed in the Related Links section of this document.

As a best practice, the private key should be deleted from the system when a successful export is complete. Strong private key protection should also be used as an extra level of security on the private key.

* Check the appropriate check boxes as shown in Figure 14 below and click **Next**.

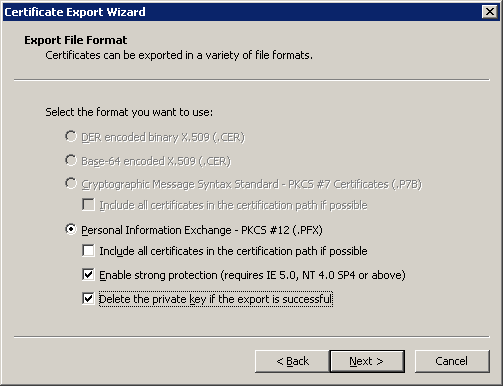


Figure 14. . Choosing a file format

The \*.PFX file format (PKCS #12) allows a password to protect the private key stored in the file. Choose a strong password and click **Next**.

The last step is to save the actual \*.PFX file. The certificate and private key can be exported to any writeable device, including a network drive or floppy. After typing or browsing for a file name and path, click **Next**.

Once the \*.PFX file and private key have been exported, the file should be secured on stable removable media in a secure location in accordance with the organization’s security guidelines and practices. For example, an organization may preserve the \*.PFX file on one or more CD-ROMs that are stored in a safety deposit box, vault, etc. that has strict physical access controls. If the file and associated private key are lost, it will be impossible to decrypt any existing files that have used that specific DRA certificate as the data recovery agent.

### Importing Keys

Importing keys is a much simpler step than exporting. To import a key stored as a PKCS #12 formatted file (\*.PFX file), double-click on the file to launch the Certificate Import Wizard. Otherwise complete the following steps:

1. Log on to the workstation with a valid account.
2. Select **Run** from the Start menu.
3. Type in **mmc.exe** and press **Enter**. An empty MMC shell starts up.
4. Select the **Console** menu, and then select **Add/Remove Snap-In**. A dialog box appears with a list of all the snap-ins that have been added to this MMC shell.
5. Click the **Add** button. A list of all the registered snap-ins on the current machine appears.
6. Double-click on the **Certificates** snap-in. Choose **My User Account** then click the **Finish** button.
7. Click the **Close** button on the Add Standalone Snap-In dialog box, then click **OK** on the Add/Remove Snap-in dialog box. The MMC now contains the personal certificate store for Administrator.
8. Expand the tree view of the certificate store. Click **Certificates**, **Current User**, **Personal**, and then **Certificates**. Right-click on the folder and choose **All Tasks**, then **Import**. The Certificate Import Wizard will launch.
9. Click **Next**.

The wizard will prompt for a file and path location for the file as shown if Figure 15 below.

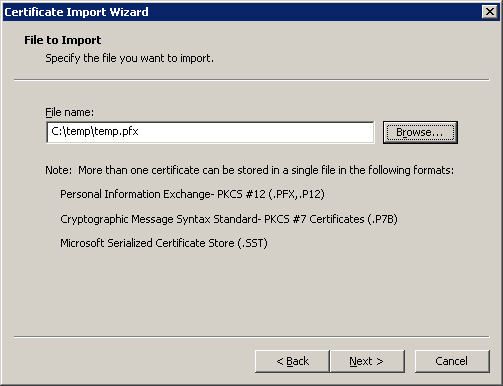


Figure 15. Prompting for file and path location

1. Type in the password for the file being imported if it is a PKCS #12 file.

**Note** It is always a best practice to store private keys protected with a strong password.

1. If you want to export the key again later from the current machine, it is important to check the Mark this key as exportable check box. Click Next.
2. The wizard may prompt for what store the certificate and private key should be imported into. To ensure that the private key is imported into the personal store, do not use the automatic radio button. **Choose Place all certificates in the following store**, and then click **Next**.
3. Highlight the Personal store and click **OK**.
4. Click Next as shown in Figure 16 below.

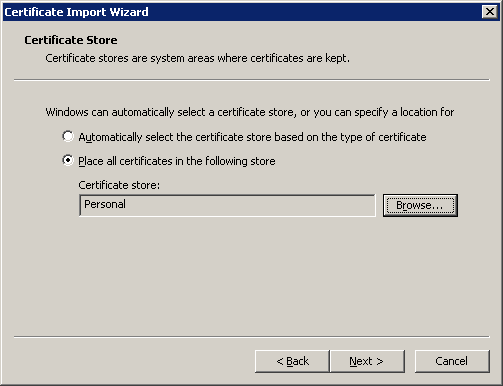


Figure 16.. Confirming location of the certificate store

1. Click Finish to complete the import.

**Important** A domain-based account should always be used in association with a DRA . Local workstation accounts may be susceptible to physical offline attacks.

## Enabling Encrypt/Decrypt on the Windows Explorer Menu

Some organizations may find it easier to enable EFS by placing “Encrypt” and “Decrypt” on the Microsoft Windows Explorer context menu when a file is right-clicked with the mouse. To enable this feature, under the following registry hive path, create a DWORD value:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\

DWORD Name: EncryptionContextMenu

Value: 1

**Note** This registry value must be created and does not exist by default.

Windows Server 2003 enables the **Encryption Details** button to also be added to the Explorer menu by creating a registry file \*.reg) with the following information and running the registry batch file for each user:

[HKEY\_CLASSES\_ROOT\\*\Shell\Encrypt To User...\Command]

@="rundll32 efsadu.dll,AddUserToObject %1"

# Data Recovery—Best Practices

In general, the best practice for organizations to follow regarding data recovery is to deploy a public key infrastructure (PKI) to issue certificates to users and data recovery agents that are issued from a certification authority (CA). The Microsoft Enterprise Certification Authority makes it easy for users to automatically get certificates for use by EFS.

Other best practices include:

* Using a certificate generated by a CA for DRAs. Certificates issued by CAs are not self-signed and can be more easily managed in terms of revocation, renewal and expiration.
* Using more than one DRA per domain, and storing the actual private keys for the DRAs on a medium (floppy disk, CD-ROM, etc.) that can be secured and retrieved only when appropriate security policies and practices have been followed. DRAs may be defined at the site, domain or OU like any other Group Policy, and may be combined as an aggregate policy based on the organization of Active Directory.

## Central Recovery Workstation

The best practice and most secure mechanism for data recovery is to use a central recovery workstation in the enterprise. This may be performed by using a backup utility to perform a raw backup of the encrypted files and then restore those files on a central recovery machine. The DRA private keys may be stored on the recovery machine or imported as necessary. This method is valuable for organizations that maintain a single DRA centrally for recovery. Maintaining a secure central recovery console ensures that the DRA private key is never exposed or compromised by machines that may have untrusted code running during the recovery process.

## EFS and Certification Authorities

Through a Windows Server 2003 enterprise CA, users may obtain a certificate employable by EFS using one of the three following methods:

* Automatically using user certificate auto-enrollment
* On-demand enrollment using an enterprise CA and properly configured certificate templates
* Manual enrollment by the end-user

Using an enterprise CA will ensure that users easily get certificates for use by EFS. It will also ensure a very low cost for certificate deployment compared to other technologies and methods. For more information on certificate authorities: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/pkitech.asp>

### Auto-enrollment

The easiest and most reliable method of certificate distribution for intranet users is auto-enrollment. Auto-enrollment occurs in the background and ensures that certificates will be available when users need them.

**Key advantages of auto-enrollment include:**

* Auto-enrollment can also be used to combine certificate enrollment with data and key recovery methods. A version 2 certificate template can be used to enroll a user automatically in the background and at the same time archive the private key.
* Auto-enrollment can also use certificate templates that require a certificate request be signed by another certificate. That is, an organization could manually (and securely) issue smart cards through a person-to-person exchange and then require that the smart card certificate be used to sign a request for an auto-enrolled certificate. This is known as “self registration authority” and is a very strong mechanism for securely issuing certificates via an automatic process.
* User store certificate management (cleanup).
* Automatic certificate renewal (revoked certificates, expired certificates, etc.).
* Automatic retrieval of pending certificate requests.

## Using Default Domain Configuration

By default, the administrator of a domain is the default DRA in a Windows 2000 or Windows Server 2003 domain. When the administrator for a domain first logs in with that account: a self-signed certificate is generated, the private key is stored in the profile on that machine, and the default domain Group Policy contains the public key of that certificate as the default DRA for the domain.

## Lost or Expired DRA Private Keys

Although the expiration of a DRA certificate is a minor event, the loss or corruption of the DRA’s private keys can be potentially catastrophic for an organization.

An expired DRA certificate (private key) can still be used to decrypt files, however new or updated files cannot use the expired certificate (public key). When an organization has either lost the private keys of a DRA or the certificate of a DRA has expired, the best practice for an organization to follow is to immediately generate one or more new DRA certificates and update the Group Policy or Policies to reflect the new DRAs. When users encrypt new files or update existing encrypted files, the files will automatically be updated with the new DRA public keys. It may be necessary for an organization to encourage users to update all existing files to reflect the new DRA(s).

In Windows XP, the command-line utility cipher.exe has been updated with a /U parameter to update the file encryption key or recovery agent keys on all files on local drives. For example:

Cipher.exe /U

C:\Temp\test.txt: Encryption updated.

C:\My Documents\wordpad.doc: Encryption updated.

**Note** When using the default self-signed certificate in a domain without a certification authority, the lifetime of the. certificate is 99 years

# Data Protection—Best Practices

For organizations that are concerned with protecting the data of mobile users in case of theft or loss, the following best practices should be followed:

* Physical protection of the computer is paramount. There is no technological substitute for taking every precaution to ensure the computer is not stolen or physically compromised.
* Always use the mobile computer as part of an Active Directory domain.
* Store the private keys for users separately from the mobile computer and import when needed.
* For common storage folders such as “My Documents” and “temporary folders” encrypt the folder so that all new and temporary files will be encrypted when created.
* Always create new files, or copy existing plaintext files, into an encrypted folder when the data is extremely sensitive. This will ensure that all files have never existed in plaintext form on the machine, and that temporary data files cannot be recovered from sophisticated disk analysis attacks.
* Encrypted folders may be enforced in a domain through the use of a combination of group policies, logon scripts and security templates to ensure that standard folders such as “My Documents” are configured as encrypted folders.
* The Windows XP operating system supports the encryption of data in offline files. Offline files and folders that are cached locally should be encrypted when using client-side caching policies.
* Use SYSKEY in mode 2 or mode 3 (boot floppy or boot password) on the mobile computer to prevent the system from being booted by malicious users
* Enable SMB signing in Group Policy for servers that are trusted for delegation and used for storing encrypted files
* Ensure unencrypted data is removed from the hard drive after encryption of files and periodically thereafter.

**Note** SYSKEY mode 1 Is enabled by default on Windows 2000 and Windows XP. To invoke SYSKEY, from a command prompt or from the Run line on the Start menu, type “syskey.exe”. (See [**http://support.microsoft.com/support/kb/articles/q143/4/75.asp**](http://support.microsoft.com/support/kb/articles/q143/4/75.asp)for more information on SYSKEY).

**Important** Encrypting the system TEMP folder or path may have negative performance consequences on the overall performance of the system. Encrypting all temporary files may increase system CPU usage dramatically and should be carefully considered before enabling. Some application installation programs may also incorrectly copy encrypted temp files to the program folder and fail to run properly. Users should contact the application vendor when this behavior occurs.

## Deleting PlainText Data

Whenever a new data file is created on an NTFS drive, the file system allocates data to it in clusters. If the file outgrows the clusters it’s been allocated, NTFS allocates additional clusters. If the file later shrinks or is deleted, NTFS deallocates the unneeded clusters from the file, and marks them as being available for allocation to a different file, if needed. Over time, de-allocated files are overwritten as new files and data are written to the disk. Understanding how NTFS works is important when implementing a data protection strategy with EFS.

Additional information on NTFS and its operation may be found on the Microsoft Developer Network (MSDN): <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/hh/winbase/fsys_538t.asp>

### Reducing the Risk of Discovery of Plaintext Shreds

EFS incorporates a crash recovery scheme whereby no data is lost in the event of a fatal error such as system crash, disk full, or hardware failure. This is accomplished by creating a plaintext backup of the original file being encrypted or decrypted. Once the original is successfully encrypted or decrypted, the backup is deleted. Creating a plaintext copy has a side effect; the plaintext version of the file may exist on the disk until those disk blocks are overwritten by NTFS for some other file.

The recommended way to encrypt sensitive data using EFS is to create a folder, set the encrypt attribute on it, and then create files within it. If this is done, the files will be encrypted from the start. EFS will never create a backup file containing plaintext; this ensures that there will never be plaintext shreds on the drive.

### Cipher.exe Command-line Utility

The Cipher.exe command-line utility may be used to overwrite deallocated file clusters on the NTFS disk to reduce the risk of discovery of plaintext shreds left over from file conversion. Cipher.exe /W makes three disk write passes on all unused clusters on the disk. The first pass writes 0. The second pass writes 0xF. The third pass writes pseudorandom data.

CIPHER /W:directory

/W

Removes data from available unused disk space on the entire volume. If this option is chosen, all other options are ignored. The directory specified can be anywhere in a local volume. If it is a mount point, or points to a directory in another volume, the data on that volume will be removed.

**Note** Cipher.exe wipes all deallocated files from the specified disk even if a specific folder is named. It may not be possible to wipe files smaller than 4K in size as they may exist in the Master File Table (MFT) and not in separate clusters on the disk.

**To run Cipher.exe**

1. Log on as an administrator of the local machine.
2. Close all applications.
3. Open a command prompt by selecting Start, then Run, and entering CMD as the command.
4. Type "Cipher /W:<'directory'>" (without the quotes), where <'directory'> is any directory on the drive you want to clean. For instance, "Cipher /W:c:\ " will cause the deallocated space on the C: drive to be overwritten.
5. Cipher.exe will begin running, and will display a message when it’s completed.

**Important** Cipher.exe /W may take a very long time to run, especially on large volumes. It is not possible to stop it once it has started. Running the chkdsk.exe command on the volume after completion is a best practice. Also, it is not recommended that the cipher.exe /W be run multiple times; the intent of the process is a one time cleanup of the disk.

**Note** NTFS drives can be mounted as directories. For instance, a drive could be mounted as C:\folder1\D\_Drive. This usage enables drives of this type to be cleaned.

The new cipher tool is also available for Windows 2000 by downloading from the Microsoft Web site: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q298009

## Encrypting Offline Files

Windows 2000 introduced the capability to cache offline files (also known as client side caching). This IntelliMirror™ management technology allows network users to access files on network shares, even when the client computer is disconnected from the network.

For example, when a mobile user views the share while disconnected, he or she can still browse, read, and edit files, because the files have been cached on the client computer. When the user later connects to the server, the system reconciles the changes with the server.

The Windows XP client now enables offline files and folders to be encrypted using the Encrypting File System. This feature is especially attractive for traveling professionals that need to work offline periodically while maintaining the security of their data. Offline folders and caching, however, are not available for WebDAV shares.

A common database on the local machine is used to store all user files and to limit access to those files through explicit access control lists (ACLs). The database displays the files to the user in a manner that hides the database structure and format and appears as a normal folder to the user. Other user files and folders are not shown, and are not available to other users. When the offline files are encrypted, the entire database is encrypted using an EFS machine certificate. Individual files and folders may not be selected for decryption. Therefore, the entire offline files database is protected by default from attacks using the native EFS when this feature is enabled. However, one limitation of the encrypted offline files database is that files and folders will not be shown as an alternate color to the user when working offline. The remote server may also be using encryption of files and folders selectively when online, so this may appear as an inconsistency to the user when displaying encrypted files online and offline.

**Important** The CSC runs as a SYSTEM process and therefore may be accessed by any user or process that may run as SYSTEM or act as a SYSTEM process. This includes administrators on the local machine. Therefore, when sensitive data is stored in offline folders, administrative access should be restricted to users and SYSKEY should always be used to thwart offline attacks.

**To encrypt offline files**

Encrypted offline files is enabled by setting folder options which can be found in Windows Explorer by selecting **Tools** and then **Folder Options** in the command menu.

1. Select the **Offline Files** tab as shown in Figure 17 below.

**Note** This option is available in Windows XP Professional. and in Windows Server 2003 if the Remote Desktop is disabled.



Figure 17. Selecting the Offline Files tab

1. Select **Enable Offline Files** and **Encrypt offline files to secure data**.

**Note** This option will be unavailable if the policy is set through group policy in the domain.

1. Click **OK**.

Offline files will be encrypted when cached locally using a private key and certificate for the SYSTEM account on the client machine.

**Important** Never encrypt files that are stored in a roaming user profile as the system will not be able to open the files in the profile when it is loaded at logon.

## Permanent Offline Users

In a general sense, offline users of EFS (those not regularly connected to a domain or network) will have little or no special requirements for EFS operations. However, some organizations may choose to allow some offline users to maintain a copy of a DRA’s private key and certificate on a floppy disk for emergencies while the user is traveling and offline. It should be noted that this practice is generally not recommended and should only be used in extreme circumstances. When employed, the private key file (\*.PFX) should be protected with a strong password and the floppy disk should be kept separate from the mobile computer.

## EFS with WebDAV Folders

EFS with Web Distributed Authoring and Versioning (WebDAV) folders provides simple and secure ways for individual and corporate users to share sensitive data across insecure networks. EFS with WebDAV eliminates the need to purchase specialized software to share encrypted files between users, businesses or organizations in a secure manner. The strong encryption capabilities of EFS, combined with the file sharing functionality enabled in Windows XP, simplifies the process of sharing sensitive data. Files may be stored on common file servers or Internet communities such as the Microsoft Network ([www.msn.com](http://www.msn.com)) for easy access while maintaining strong security through EFS.

EFS with WebDAV folders also enables numerous business-to-business and collaboration scenarios for organizations looking to achieve simple security solutions without deploying complex infrastructure or expensive product technologies. For more information on EFS with WebDAV folders, see Encrypted Files on a Server later in this article.

## Clearing Page File at Shutdown

Ensure that the system page file is cleared before shutdown. This will ensure that memory data fragments will not be paged to disk in clear text form at shutdown. This is enabled through local or domain Group Policy.

**To clear page file at shutdown**

1. Click through the following path using the Group Policy MMC snap-in:

* Computer configuration
* Windows settings
* Security settings
* Local Policies
* Security Options

1. Open the **Shutdown: Clear virtual memory pagefile** object.
2. Select the **Enabled** radio button as shown below in Figure 18 and click **OK**.
3. Close the **Group Policy MMC snap-in**.

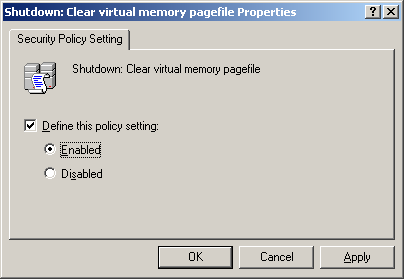


Figure 18. Defining Shutdown: Clear virtual memory pagefile policy setting

## Default Encryption Algorithms

All exported versions of Windows 2000 use 56-bit key sizes by default unless the 128-bit encryption pack is applied. Workstations that have the 128-bit encryption pack installed may decrypt files with 56-bit key lengths and will encrypt all new files with 128-bit key lengths. However, machines that are only 56-bit-capable may not open files that have been encrypted with 128-bit key lengths. This scenario is especially important where a user has a roaming user profile and may use different machines that have different encryption capabilities.

The Windows XP operating system supports the use of a stronger symmetric algorithm than the default DESX algorithm included with the Windows 2000 operating system. The default algorithm for Windows 2000 and Windows XP is DESX. The default algorithm for Windows XP Service Pack 1 and Windows Server 2003 is Advanced Encryption Standard (AES) using a 256-bit key. For users requiring greater symmetric key strength with a FIPS 140-1 compliant algorithm, the 3DES algorithm can be enabled.

**To enable the 3DES algorithm in Windows XP**

To enable the 3DES algorithm in Windows XP, either enable the local computer policy or the appropriate Group Policy in the site, domain or OU of the targeted computers.

1. Click through the following path:

* Computer configuration
* Windows settings
* Security settings
* Local Policies
* Security Options

1. Open the **System cryptography: Use FIPS compliant algorithms for encryption** object.

**Important** System cryptography applies to both EFS and IP Security (IPSec).

1. Select the **Enabled** radio button as shown in Figure 19 below, then click **OK**.

Once enabled, a Windows XP client may open files encrypted with both the DESX and 3DES algorithms However, all new files will be encrypted with the new 3DES algorithm.

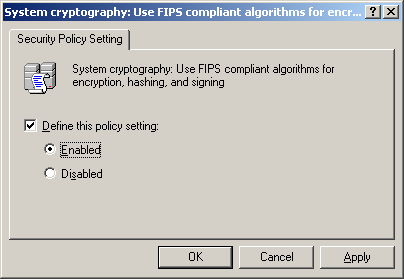


Figure 19. Defining the System cryptography: Use FIPS compliant algorithms policy setting

**Note** If a user needs to access an encrypted file from both Windows 2000 and Windows XP, the AES 256 nor the 3DES algorithm should not be enabled. The Windows 2000 operating system does not support the AES or 3DES algorithms.

Windows Server 2003 also supports the ability specify larger default RSA key sizes for keys generated for EFS. The default key size used by Windows XP and Windows 2003 is 1024 bits with the Microsoft Bsse Provider. With Windows Server 2003, this default size can be changed by setting the following registry key with a DWORD value:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\RSAKeyLength

Range: 1024 to 16384.

If a number is larger than 16384, it will be ignored. If the number is not a multiple of 8, it will be reduced to the next multiple of 8. If the length is greater than 1024, the Microsoft Enhanced Provider CSP will be used for generating the key.

**Importan**t Only the Microsoft Base, Enhanced and Strong Cryptographic Service providers may be used with the encrypting file system. Smartcards and strong private key protection places on key containers are also not supported with EFS

For other EFS best practices, see Microsoft Knowledge Base article: <http://support.microsoft.com/support/kb/articles/Q223/3/16.ASP>

## Show Encrypted Files in Color

The Windows XP client now allows both encrypted and compressed files to be displayed with alternate colors in Windows Explorer. This feature is enabled by setting folder options which can be found in Windows Explorer by selecting **Tools** and then **Folder Options** in the command menu.

**To show encrypted files in color**

1. Select the **View** tab in the **Folder Options** dialog box
2. Check the box for Show encrypted or compressed NTFS files in color as shown in Figure 20 below. When this is applied to a folder, all encrypted files will be displayed as green in Windows Explorer.
3. If you would like to have this setting apply to all folders on the machine, select the **Apply to All Folders** button and choose **Yes** when prompted.
4. Click OK to close the dialog box.

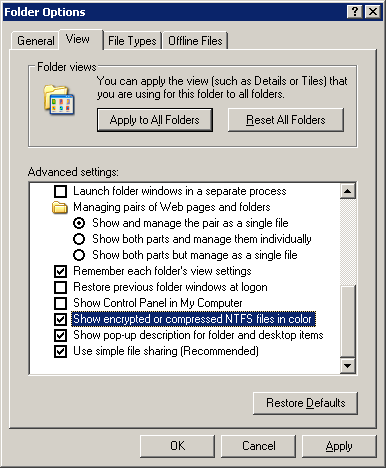


Figure 20. Selecting options for showing encrypted files in color

## Using EFS with Standalone Machines or NT 4.0 Domains

Although EFS does not have the same capabilities or benefits when used on standalone machines, using EFS in workgroup mode or as members of NT 4.0 domains is a valid scenario.

**Note** Only Windows 2000 or Windows XP computers may use EFS. The EFS capability is bound to the machine and not to the user account. This also means that in a mixed NT4.0/Windows 2000 environment, a roaming user who has the appropriate EFS keys in his profile cannot open or read EFS encrypted files from a Windows NT 4.0 Workstation.

### Managing EFS in a Non-Active Directory Environment

The largest issue with EFS in a non-Active Directory environment is one of manageability.

Considerations include:

* For Windows 2000, the default setting allows anyone that can log on to the workstation or server as the local Administrator account to decrypt any user’s encrypted files on that machine. This makes workgroup mode machines especially vulnerable to offline disk editor attacks. Windows XP and Windows Server 2003 computers are not susceptible to this attack.
* If a user encrypts a file and corrupts or deletes the certificate store of both the user and the local DRA, it will be impossible to recover or decrypt the files.
* If there is a need to recover the files without the user’s permission, such as after termination or in response to a subpoena by a law enforcement agency, the files will be unrecoverable if the user both corrupts the certificate store and mistakenly or maliciously deletes the DRA certificate.
* No central key database exists for recovery.

When using EFS in a non-Active Directory environment, some key best practices should be followed:

* When using Windows 2000 computers, the default DRA private key should always be removed from a system running in workgroup mode and stored separately from the system. Computers in workgroup mode are especially vulnerable to offline disk editor attacks. Windows XP and Windows Server 2003 computers are not susceptible to this attack.
* Use a SYSKEY mode with a boot floppy or master password that must be entered prior to system boot. The floppy and/or master password should be stored separately from the system.
* Install machines using sysprep and custom scripts to enable a central recovery agent. This can be achieved by having a run-once registry key that deletes the existing local DRA and inserts a centralized DRA for the organization. The change must be performed after the sysprep mini-setup that generates the default DRA. This method is especially useful for machines in NT 4.0 domains. The best practice is to use a Microsoft CA to issue a DRA certificate for the central recovery agent.
* If a machine and/or user are migrated to a Windows 2000 or Windows Server 2003 Active Directory environment at a later date with an enterprise CA, it is important to note that clients will continue to use the self-signed certificates, and not automatically enroll for a new certificate once they are joined to an Active Directory domain. However, the default domain recovery agent will automatically take effect for all new files and older encrypted files as they are modified.

**To view the current DRA certificate for a standalone machine or a machine in an NT 4.0 domain**

1. Open the Group Policy MMC snap-in for the Local Computer. Click through to the local computer policy to find the local DRAs as shown in Figure 21 below.

* Computer configuration
* Windows settings
* Security settings
* Public Key Policies
* Encrypted File System

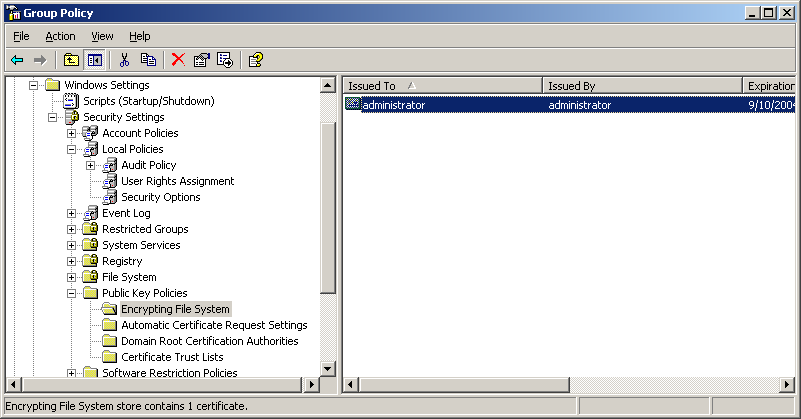


Figure 21. Finding the local Encrypted Data Recovery Agents

## Resetting Local Passwords on Windows XP

Windows XP has new behavior regarding locally changed passwords and EFS. In Windows 2000, when a local user password was reset by an administrator, the administrator or third party could theoretically use the newly changed account to log on as the user and decrypt the encrypted files. In Windows XP, the changing of a local user password by an administrator, or through a method other than by the user, will block all access to previously encrypted files by the user.

In summary, the profile and keys of the user will be lost and will not be available to the account with the reset password. Windows XP gives the following warning when attempting to reset a user account password:

**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 to guard against offline attacks and prevents rogue administrators from gaining access to encrypted files of other users.

## Encrypted Files on a Server

Windows XP supports two types of encrypted files on remote servers:

* Delegated server mode
* EFS over WebDAV

**Note** The Windows 2000 operating system does not support EFS over WebDAV.

## Delegated Server Mode

Windows 2000, Windows XP and Windows Server 2003 permit a user to remotely encrypt files on a server if the server has an NTFS partition and the server is trusted for delegation in the Active Directory. The user account must **not** be marked as “sensitive and cannot be delegated” in the Active Directory.

Remote encryption requires that a user's certificate and private key be loaded in a local profile on the server for encryption and decryption operations. The server obtains access to the profile through Kerberos delegation. Remotely encrypted files will only be encrypted using the private keys stored in this profile. If a roaming profile is available, it will be copied locally.

**Note** A user will have a profile and private keys stored on the server even if the user has never logged on interactively to the server.

Smart card-based certificates and keys are not currently supported with the Encrypting File System. Cross-forest encryption of files on remote servers is also not supported in delegated server mode for remote encryption. If constrained delegation is used with a Windows Server 2003-based server, the server and the user account must exist in the same Active Directory domain. For more information on this topic, refer to the Windows Server 2003 help files. For encryption of files on remote servers across forest boundaries, the EFS over WebDAV method should be employed.  
  
The profile can be obtained in one of two ways:

* The user has a roaming user profile (RUP), which is downloaded when the server impersonates the user.
* The server generates a new local profile on behalf of the user and subsequently requests or generates a self-signed EFS certificate.

**Important** If you are using EFS in delegated server mode with a Microsoft cluster server, it is important that all users have roaming user profiles. Due to the nature of user key material existing in the user profile, a roaming profile is necessary for the same key to be available on both cluster nodes in case of failover. If a roaming user profile is not used, the user data will not be able to be decrypted on the second node when failover occurs. EFS with clusters is only supported with Windows Server 2003. For more information on configuring a Windows Server 2003 cluster to support Kerberos authentication and EFS, please refer to the checklist in the Windows Server 2003 help files.

## File Sharing on Remote Servers

File sharing on remote servers that are trusted for delegation has some very unique challenges regarding sharing certificates of other users. If the users are not using roaming user profiles, then the server will be using unique certificates for the users for the files encrypted on the server. This condition exists despite the fact that the user may already have enrolled for an EFS certificate and published that certificate to the Active Directory. Effectively, the user will not know which certificate to choose from the Active Directory when adding other users to an encrypted file. There is no way to determine which certificate the server has used for encryption.

This scenario is exacerbated by the fact that users choose certificates from their local machine store or the Active Directory, not from the Other People or Trusted People store on the server. It is not recommended to share files that are encrypted on the server unless one of the following workarounds is employed:

* The users have roaming user profiles
* EFS over WebDAV file sharing is used
* An alternate method for identifying the correct certificate is provided (For example: Only publishing server created certificates to Active Directory)

### Performance

Windows Server 2003 is tuned to optimize the caching of user keys on the server when the server is being used for remote server encryption. By default, the server will cache up to 15 user key handles in memory to increase encryption performance on the server. However, the default may be changed by an administrator by editing the following registry value:

**HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\UserCacheSize DWORD**

The acceptable values are between 5 and 30 for this registry value.

**Note** Private keys are not stored in cached memory, but only as a handle to the CryptoAPI key container. The server cache will be held in memory and cleared only on reboot of the computer.

### Disaster Recovery

Remote encryption of files on a server introduces new challenges in disaster recovery that require administrators to take steps to preserve the ability of users to decrypt files that have been previously encrypted. In disaster recovery scenarios, if data files have been backed up but the secured user profiles containing the private keys of users have not been backed up(and RUPs are not used), users will not be able to decrypt or access the previously encrypted files. If this should occur, only the data recovery agents will be able to decrypt previously encrypted files.  
  
This may be a tedious process for some organizations. In order to avoid this scenario, several options exist:

* Back up the full operating system and profile hives, not just data files.
* Use roaming user profiles.
* In the case of a re-directed "My Documents" folder to a file server through Group Policy, change Group Policy Objects (GPO) to re-direct "My Documents" to an alternate server. (For example, if you are encrypting files in "My Documents" and "My Documents" is redirected to a server through Group Policy, changing the server path in the Group Policy will mitigate the issue.) For additional information on Group Policy, refer to the Group Policy article on <http://www.microsoft.com/windows2000/library/howitworks/management/grouppolwp.asp>

For more information on this topic, refer to Microsoft Knowledge Base article: [Q283223 - Recovery of Encrypted Files on a Server](http://sdbuild1/kb/Q283/2/23.asp).

## EFS with WebDAV Folders

The Windows XP client supports a new method for encrypting files to remote servers through a protocol known as WebDAV. When the Windows XP client maps a drive to a WebDAV access point on a remote server, files may be encrypted locally on the client and then transmitted as a raw encrypted file to the WebDAV server using an HTTP PUT command. Similarly, encrypted files downloaded to a Windows XP client are transmitted as raw encrypted files and decrypted locally on the client using an HTTP GET command. The temporary internet files location is used for intermediate transfer of the files using HTTP where the WebDAV “proppatch” and “propfind” verbs are used to detect and set the encrypted file attribute for Windows XP. Therefore, only public and private key pairs on the client are ever used in encrypting files.

The WebDAV redirector is a new mini-redirector that supports the WebDAV protocol for remote document sharing using hypertext transfer protocol (HTTP). The WebDAV redirector supports the use of existing applications, and it allows file sharing across the Internet (through firewalls, routers, etc.) to HTTP servers. Both Internet Information Server (IIS) 5.0 (Windows 2000) and IIS 6.0 (Windows Server 2003) support WebDAV folders known as Web folders. The WebDAV re-director does have some general limits on the file that may be transmitted using the WebDAV protocol. The actual limitation may vary dependent on the amount of virtual memory available, but in general 400 megabytes is the maximum file size that may be used in Windows XP with EFS over WebDAV.

The WebDAV protocol does not necessarily support rich file ACLs on files made available on a WebDAV share (publishing point). WebDAV abstracts files much like the FAT file system which does not have per-file based ACLs.

A WebDAV folder can be created on a Windows 2000 or Windows XP server by enabling Web Sharing on a folder on a server.

**To enable Web sharing**

1. Right-click on a folder on the server and select **Properties**.
2. Select the **Web Sharing** tab as shown in Figure 22 below.

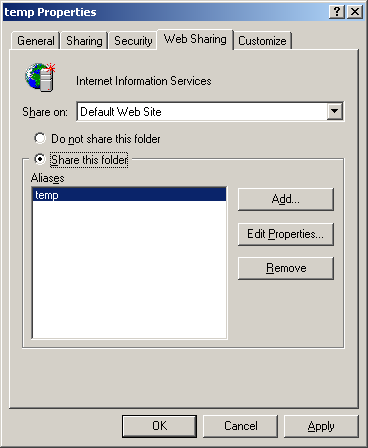


Figure 22. Properties—Web Sharing

1. Next, click the **Share this folder** radio button and then click **OK**. WebDAV is now enabled on the server through this folder.

Files and folders, when encrypted using a WebDAV share, will appear as unencrypted if a user or administrator logs on to the server locally. Once a file has been encrypted using WebDAV, that file should only be accessed and decrypted using WebDAV. This unique behavior, however, does not affect the ability to backup and restore the server using NTBACKUP.exe or the NT backup API set.

Administrators and users should take care to not encrypt files locally on a volume that hosts a WebDAV share or to set the encryption attribute locally. All administration should be through the WebDAV share only. It is also important to note that if a user does not have a key to decrypt the file on a WebDAV share, the user will not be able to specify the advanced EFS details of the file, such as the users that are allowed to decrypt the file. The user will instead get an “access denied” error.

**Note** A WebDAV server may not be used as a Distributed File System (DFS) root. However, a WebDAV folder (share) may be used as a leaf link in a DFS path.

## Migrating to New Certificates

For a number of reasons, a user may wish to migrate to using a new certificate or a new key after a period of time. This is especially important for users that have been using EFS in a non-domain environment, or an environment without a Microsoft certificate authority. It is possible to replace the certificate being used by EFS for local file encryption in two steps:

1. Replace the following registry value on the local machine for the current user with the thumbprint of the new certificate to be used:

**HKCU\Software\Microsoft\Windows NT\EFS\CurrentKeys\CertificateHash**

1. Run the cipher.exe utility with the /K option

C:\>cipher /?

Displays or alters the encryption of directories [files] on NTFS partitions.

CIPHER [/E | /D] [/S:directory] [/A] [/I] [/F] [/Q] [/H] [pathname [...]]

CIPHER /K

/K

Creates new file encryption key for the user running Cipher. If

this option is chosen, all the other options will be ignored.

### Third Party Certification Authorities

A third party certification authority may be used to issue certificates for EFS and a data recovery agent. For more information, refer to Microsoft knowledge base article Q273856: <http://support.microsoft.com/support/kb/articles/q273/8/56.asp>

## EFS and System Restore

Windows XP includes a new feature known as “System Restore”. System Restore allows a user to restore the operating system to a previously known state by automatically monitoring and archiving system files. In general, System Restore does not affect EFS since normal user files that would be encrypted are not monitored. Also, since system files may not be encrypted with EFS, there is no impact in that area either. However, since application files may be encrypted, it is important to understand how using System Restore may affect the security of encrypted files.

* If you decrypt a previously encrypted monitored file, then restore to a point before the file was decrypted, System Restore will not revert the file to its encrypted state, it will remain decrypted after the restore. If you undo the restore, the file will remain decrypted.
* If you encrypt a monitored file, then restore to a point before the monitored file was encrypted, System Restore will revert the file to a pre- or unencrypted state. If you undo the restore, the file will remain un-encrypted.
* If you modify a monitored file which is encrypted for multiple users, then restore to a point before the modification occurred, System Restore will revert the file modification, but the file will now only be accessible by the first user who modified the file after the restore point was created.
* When you undo the restore, only the user who ran the restore will be able to access the file since the filter will backup the file during restore in the context of the user who is running the restore operation.
* If you encrypt a directory and then restore to a point before it was encrypted, the directory will remain encrypted. Monitored files created in this directory, during this restore point, will inherit the directory’s encryption attribute, but will be deleted by restore. Monitored (and unmonitored) files moved into this directory, will retain the encryption status from the directory in which they were created (if there is one). After restore, monitored files will be moved back to the original directory and retain the encryption status from the directory in which they were recreated. If you undo the restore, the directory will remain encrypted and the files created in this directory will be restored with all their previous encryption keys. Also, any files moved into this directory will be restored with their correct encryption state (which may mean they are not encrypted).
* If you delete a monitored encrypted file and then restore to a point before the delete, System Restore will revert the delete and the deleted file will be restored with its encryption attributes intact. Undoing this restore will result in the file again being deleted.
* If you delete a directory which is encrypted, then restore to a point before it was deleted, System Restore will restore the directory with its encryption attributes intact. Undoing this restore will result in the directory again being deleted.
* If you modify an encrypted directory (change names), then restore to a point before the modification, System Restore will revert the modifications and leave the directory’s encryption attributes intact. Undoing the restore will undo the replace and the modification, and the encryption attributes will remain intact.

### Best Practices

The following is recommended to retain the best security coverage when using encryption on monitored file types (for example: .dll, .exe, .ini, etc.):

* Turn off System Restore (losing all previous restore points).
* Complete the encryption settings, and then turn System Restore back on to ensure that the system cannot be reverted to a pre-encrypted state.
* If encryption is used on System Restore monitored file types, it is recommended that encryption be applied to these files in a partition/drive that’s excluded from System Restore protection. This will reduce the risk of restoring to a pre-encrypted state.

# Data Recovery Versus Key Recovery

The Windows XP and Windows Server 2003 operating systems support both key recovery and data recovery. Both solutions have advantages and disadvantages. There is no definitive answer to the question, “Which recovery option—key or data— is better?” Both solutions have technical advantages and disadvantages, and the decision to use one or both is a subjective one. Both provide viable solutions when used either individually or together. This section is intended to identify some of the key advantages and disadvantages associated with these recovery options so that an organization can make an informed decision.

**Data recovery** should be used when an organization desires the ability to recover data, but not access to the individual private keys of a user. An organization may disable the ability to perform data recovery in a Windows 2000 domain environment by first enabling a data recovery agent in the domain and then destroying the private keys associated with the DRA. This has the net effect of enabling EFS, but disabling the ability to recover data. Windows Server 2003 domains with Windows XP clients can disable the recovery agent.

**Data recovery and key recovery** should not be used when an organization wants to protect data from all parties except the original user. If data should not be accessed or recovered by any person other than the author/owner, neither data recovery nor key recovery processes should be implemented.

## Advantages of Data Recovery

* Does not require a certification authority or PKI infrastructure.
* Data recovery policies can be managed centrally using the Active Directory.
* Users do not have to manage certificates or private keys.
* Decryption can be limited to the user only (requires deleting DRA keys while maintaining policy).

## Disadvantages of Data Recovery

* An administrative process must recover user data. A user may not recover their own data.
* Data recovery occurs on a file-by-file basis as a manual process.
* Users must re-enroll for new certificates. This is because only data is recovered and not the keys of a user.
* Administrators must revoke old certificates. This is because it is assumed that when a key is lost it’s been compromised.
* Standalone workstations, or workstations in non-Active Directory environments, cannot be centrally managed.
* Data recovery is specific to the EFS application.

## 

## Advantages of Key Recovery

* Users do not have to perform re-enrollment for certificates, change security settings, etc.
* Existing certificates do not have to be revoked.
* Users do not have to recover any data or e-mail due to lost private keys.
* All data encrypted by a public key in a certificate can be recovered after a private key has been recovered.

## Disadvantages of Key recovery

* User key recovery is a manual process involving administrators and users
* Key recovery allows administrative access to the private keys of users.
* Non-repudiation assurance may not be available with key archival and recovery.

# Troubleshooting

The most common issue in using EFS is the association of the file and the certificate used to encrypt the file. If the user or DRA does not have the private key associated with the certificate identified in the file’s advanced details, the user will not be able to open the file.

The most common error a user will receive is “access denied”. Often this is caused by the user not having access to the private key associated with the certificate that encrypted the file. This occurs frequently when users re-install a workgroup machine without backing up the local user keys and certificates associated with EFS. To easily determine which certificates were used to encrypt the file, select the **Advanced Details** button of the file properties. Both the user that can decrypt the file and the DRA that can recover the file are listed, along with the certificate thumbprint of the certificates used to encrypt the session key for the file as shown in Figure 23 below The certificate thumbprint is the hash of the certificate actually used to encrypt the session key for the given user.

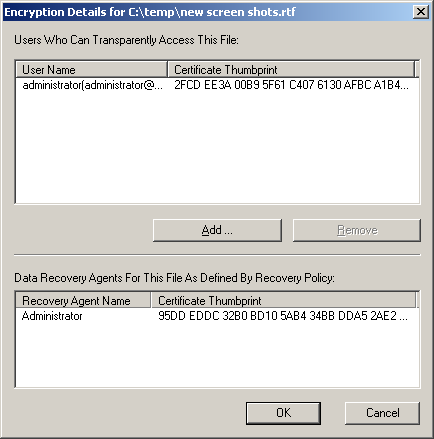


Figure 23. Illustrating encryption details

The certificate hash, or thumbprint, for a certificate can be viewed by opening the certificate in the **Certificates** MMC snap-in for the user as shown in Figure 24 below.

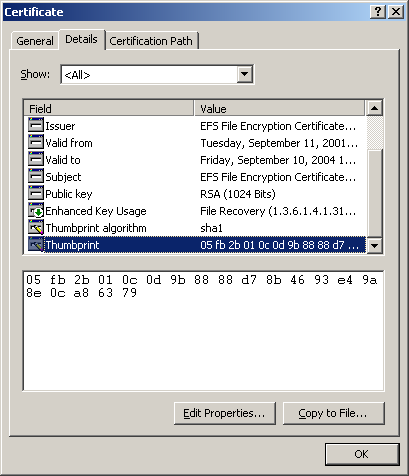
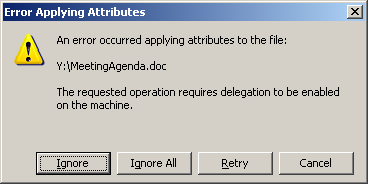


Figure 24. Certificate details

The second most common issue is that a server is not trusted for delegation when trying to encrypt or decrypt a file on a remote server. This is usually exhibited by the dialog box shown in Figure 25 below:

Figure 25. Error Applying Attributes

Additional issues that may result involve the use of an improper cryptographic service provider (CSP) or invalid certificate extensions required by EFS. If a non-Microsoft CSP is used to generate an EFS key, the system will reject the certificate and generate a new key and certificate automatically to be used without user warning. EFS will also reject certificates that correspond to key containers that have strong private key protection set.

For additional details, please refer to the Microsoft Knowledge Base at <http://support.microsoft.com>.

## Data Protection API

To understand the third most common issue that users encounter with Encrypting File System, it is necessary to understand how the Windows operating system protects private keys, passwords and user secrets using the Data Protection API.

**The Data Protection API (DPAPI) creates a master encryption key** derived from the user password to protect this information, which is stored in the Active Directory or on local machines, and made available after successful user logon. For more information on DPAPI, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp

**The most common issue with Windows XP** occurs when a local user on a workgroup computer has their password reset by a local administrator. When a local password reset occurs, the DPAPI master key is lost, and the user will no longer be able to access their private keys associated with encrypted files. This behavior is designed as a security feature against offline attacks and does not apply to domain joined machines with domain based user accounts.

**A common issue with domain-based accounts** may occur when changing a user password over RAS (dial-up or VPN). In this case, the user password is changed with the domain controller and the DPAPI master key updated, however it will not be replicated immediately. When users disconnect and attempt to access locally encrypted files, they may receive an “Access Denied” error message. To resolve this issue, the user may connect to the network normally and log on to update the DPAPI master key, or to set the following registry DWORD value in the registry:

HKLM\SOFTWARE\\Microsoft\\Cryptography\\Protect\\Providers\\df9d8cd0-1501-11d1-8c7a-00c04fc297eb

Name: ProtectionPolicy

Value: 0x1

**Warning** Use of this registry key may place the user account at risk for offline attack as a local password reset will no longer invalidate the DPAPI master key.

# Summary

Windows XP and Windows Server 2003 provide significant advancements in data recovery and protection, and private key recovery. This article is intended to assist system architects and administrators in developing best practices for creating data recovery and data protection strategies using Windows XP and Windows Server 2003.

In addition to explaining strategies for data recovery and data protection, this article includes many step-by-step examples that illustrate how to set up the data recovery and data protection features you’ll want to use when deploying a Windows XP or Windows Server 2003 data recovery and protection solution.

# Related Links

See the following resources for further information:

* [Technical Overview of Security Services](http://www.microsoft.com/windows.netserver/techinfo/overview/security.mspx) at <http://www.microsoft.com/windows.netserver/techinfo/overview/security.mspx>
* [What’s New in Security for Windows XP](http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/home.asp) at  
  <http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/home.asp>
* [PKI Enhancements in Windows XP Professional and Windows .NET Server](http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp) at  
  <http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp>
* [Windows XP and .NET: An Overview](http://www.microsoft.com/windowsxp/pro/techinfo/planning/dotnet/default.asp) at  
  <http://www.microsoft.com/windowsxp/pro/techinfo/planning/dotnet/default.asp>
* [Windows 2000 Certificate Services](http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/2000cert.asp) at  
  <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/2000cert.asp>
* [Encrypting File System for Windows 2000](http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp) at  
  <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp>
* [Third-Party Certification Authority Support for Encrypting File System](http://support.microsoft.com/support/kb/articles/q273/8/56.asp) at <http://support.microsoft.com/support/kb/articles/q273/8/56.asp>
* [Windows Platform SDK](http://msdn.microsoft.com/library/default.asp) at  
  <http://msdn.microsoft.com/library/default.asp>
* [Certificate Management Messages over CMS (CMC)](http://www.ietf.org/rfc/rfc2797.txt) at  
  <http://www.ietf.org/rfc/rfc2797.txt>
* [PKCS #12 - Personal Information Exchange Syntax Standard](http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/) at  
  <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/>
* [Troubleshooting Certificate Status and Revocation](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp) at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp>
* [Data Protection API](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp) at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/windataprotection-dpapi.asp>

For the latest information about Windows XP Professional, see the Windows XP Web site at <http://www.microsoft.com/windowsxp/pro/>.

For the latest information about Windows Server 2003, see the Windows Server 2003 Web site at <http://www.microsoft.com/windows.netserver.>

# Knowledge Base Articles on EFS

The following articles are part of the Microsoft product support knowledge base:

Q243756 [HOWTO: Use Encrypting File System (EFS) with IIS](http://support.microsoft.com/support/kb/articles/Q243/7/56.ASP)  
 Q222022 [Disabling EFS for All Computers in a Windows 2000-Based Domain](http://support.microsoft.com/support/kb/articles/Q222/0/22.ASP?LN=EN-US&SD=gn&FR=0&qry=%20Q222022%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q223338 [Using a Certificate Authority for the Encrypting File Service](http://support.microsoft.com/support/kb/articles/Q223/3/38.ASP?LN=EN-US&SD=gn&FR=0&qry=Q223338%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q241201 [How to Back Up Your Encrypting File System Private Key](http://support.microsoft.com/support/kb/articles/Q241/2/01.ASP?LN=EN-US&SD=gn&FR=0&qry=Q241201%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q242296 [How to Restore an EFS Private Key for Encrypted Data Recovery](http://support.microsoft.com/support/kb/articles/Q242/2/96.ASP?LN=EN-US&SD=gn&FR=0&qry=Q242296%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q243026 [Using Efsinfo.exe to Determine Information About Encrypted Files](http://support.microsoft.com/support/kb/articles/Q243/0/26.ASP?LN=EN-US&SD=gn&FR=0&qry=Q243026%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q243035 [How to Disable/Enable EFS on a Standalone Windows 2000 Computer](http://support.microsoft.com/support/kb/articles/Q243/0/35.ASP?LN=EN-US&SD=gn&FR=0&qry=Q243035%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q255742 [Methods for Recovering Encrypted Data Files](http://support.microsoft.com/support/kb/articles/Q255/7/42.ASP?LN=EN-US&SD=gn&FR=0&qry=Q255742%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q259732 [EFS Recovery Agent Cannot Export Private Keys](http://search.support.microsoft.com/kb/psssearch.asp?SPR=chs&KT=ALL&T=Q&T1=7d&LQ=Q259732+&PQ=PastQuery&S=F&A=T&DU=C&FR=0&D=&LPR=&LNG=ENG&VR=http%3A%2F%2Fsupport.microsoft.com%2Fsupport%3Bhttp%3A%2F%2Fsupport.microsoft.com%2Fservicedesks%2Fwebcasts)  
 Q264178 [Description of the Windows 2000 Resource Kit Security Tools](http://support.microsoft.com/support/kb/articles/Q264/1/78.ASP?LN=EN-US&SD=gn&FR=0&qry=Q264178%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q272412 [Error Message "Access Denied" When Starting a Program](http://support.microsoft.com/support/kb/articles/Q272/4/12.ASP?LN=EN-US&SD=gn&FR=0&qry=Q272412%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q273856 [Third-Party Certificate Authority Support for EFS](http://support.microsoft.com/support/kb/articles/Q273/8/56.ASP?LN=EN-US&SD=gn&FR=0&qry=Q273856%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q230520 [How to Encrypt Data Using EFS in Windows 2000](http://support.microsoft.com/support/kb/articles/Q230/5/20.ASP?LN=EN-US&SD=gn&FR=0&qry=Q230520%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHSQ230520)  
 Q222054 [Encrypting Files in Windows 2000](http://support.microsoft.com/support/kb/articles/Q222/0/54.ASP?LN=EN-US&SD=gn&FR=0&qry=Q222054%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q221997 [Cannot Gain Access to Previously Encrypted Files on Windows 2000](http://support.microsoft.com/support/kb/articles/Q221/9/97.ASP?LN=EN-US&SD=gn&FR=0&qry=Q221997%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q227825 [Backup Tool Backs Up Files to Which You Do Not Have Read Access](http://support.microsoft.com/support/kb/articles/Q227/8/25.ASP?LN=EN-US&SD=gn&FR=0&qry=Q227825%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q227369 [Default Behavior for Group Policy Extensions with Slow Link](http://support.microsoft.com/support/kb/articles/Q227/3/69.ASP?LN=EN-US&SD=gn&FR=0&qry=Q227369%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q221107 [File and Folder Attributes Not Replicated by FRS](http://support.microsoft.com/support/kb/articles/Q221/1/07.ASP?LN=EN-US&SD=gn&FR=0&qry=Q221107%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q230490 [The Encrypted Data Recovery Policy for Encrypting File System](http://support.microsoft.com/support/kb/articles/Q230/4/90.ASP?LN=EN-US&SD=gn&FR=0&qry=Q230490%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q243850 [Cannot Gain Access to Microsoft Encrypted File Systems](http://support.microsoft.com/support/kb/articles/Q243/8/50.ASP?LN=EN-US&SD=gn&FR=0&qry=Q243850%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q250581 [Windows 2000 Keywords for Searching the Microsoft Knowledge Base](http://support.microsoft.com/support/kb/articles/Q250/5/81.ASP?LN=EN-US&SD=gn&FR=0&qry=Q250581%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q256168 [Cannot Open Encrypted Files with Multiple Windows Installations](http://support.microsoft.com/support/kb/articles/Q256/1/68.ASP?LN=EN-US&SD=gn&FR=0&qry=Q256168%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q257705 [How to Reinitialize the EDRP on a Workgroup Computer](http://support.microsoft.com/support/kb/articles/Q257/7/05.ASP?LN=EN-US&SD=gn&FR=0&qry=Q257705%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q216899 [Best Practice Methods for Windows 2000 Domain Controller Setup](http://support.microsoft.com/support/kb/articles/Q216/8/99.ASP?LN=EN-US&SD=gn&FR=0&qry=Q216899%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q223093 [Encrypted Files Cannot Be Compressed](http://support.microsoft.com/support/kb/articles/Q223/0/93.ASP?LN=EN-US&SD=gn&FR=0&qry=Q223093%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q223178 [Transferring Encrypted Files That Need to Be Recovered](http://support.microsoft.com/support/kb/articles/Q223/1/78.ASP?LN=EN-US&SD=gn&FR=0&qry=Q223178%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q223316 [Best Practices for Encrypting File System](http://support.microsoft.com/support/kb/articles/Q223/3/16.ASP?LN=EN-US&SD=gn&FR=0&qry=Q223316%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q223448 [Cannot Use Shared Encrypted Files in Windows 2000](http://support.microsoft.com/support/kb/articles/Q223/4/48.ASP?LN=EN-US&SD=gn&FR=0&qry=Q223448%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q245044 ["Warning: The Restore Destination Device..." During Restore](http://support.microsoft.com/support/kb/articles/Q245/0/44.ASP?LN=EN-US&SD=gn&FR=0&qry=Q245044%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q250494 ["Access Is Denied" Error Message Appears w/ Correct Permissions](http://support.microsoft.com/support/kb/articles/Q250/4/94.ASP?LN=EN-US&SD=gn&FR=0&qry=Q250494%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q254156 [Encrypted Files Made Available Offline Not Encrypted on Client](http://support.microsoft.com/support/kb/articles/Q254/1/56.ASP?LN=EN-US&SD=gn&FR=0&qry=Q254156%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q255554 [Selecting Encrypted File Over Network Hangs Client Window](http://support.microsoft.com/support/kb/articles/Q255/5/54.ASP?LN=EN-US&SD=gn&FR=0&qry=Q255554%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q264064 ["Access is Denied" When Encrypting/Decrypting Files or Folders](http://support.microsoft.com/support/kb/articles/Q264/0/64.ASP?LN=EN-US&SD=gn&FR=0&qry=Q264064%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q263419 [Software Inventory on Encrypted Vol Degrades Performance](http://support.microsoft.com/support/kb/articles/Q263/4/19.ASP?LN=EN-US&SD=gn&FR=0&qry=Q263419%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q269397 [Logon Process Hangs After Encrypting Files on Windows 2000](http://support.microsoft.com/support/kb/articles/Q269/3/97.ASP?LN=EN-US&SD=gn&FR=0&qry=Q269397%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q272279 [How to Troubleshoot FRS and DFS](http://support.microsoft.com/support/kb/articles/Q272/2/79.ASP?LN=EN-US&SD=gn&FR=0&qry=Q272279%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q283223 [Recovery of Encrypted Files on a Server](http://support.microsoft.com/support/kb/articles/Q283/2/23.ASP?LN=EN-US&SD=gn&FR=0&qry=Q283223%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)  
 Q248723 [INFO: Understanding Encrypted Directories](http://support.microsoft.com/support/kb/articles/Q248/7/23.ASP?LN=EN-US&SD=gn&FR=0&qry=Q248723%20&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=CHS)