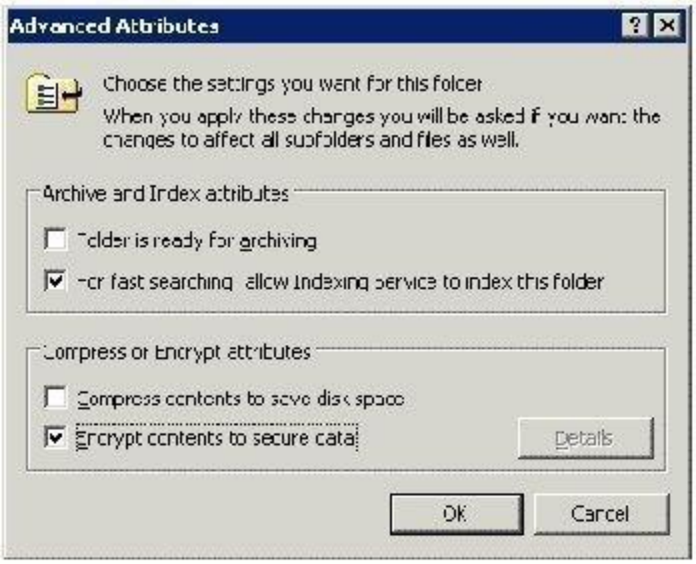
An Overview of EFS

Encrypting File System (EFS) enables users toencrypt files and folders, and entire data drives on NTFS formatted volumes. NTFS enables you to set permissions on files and folders on an NTFS formatted volume which controls access to these files and folders. EFS enables you to encrypt filesand folders to further enhance the security of these files and folders. Even when an unauthorized person manages to access the files and folders because of incorrectly configured NTFS permissions, the files and folders would be encrypted! Only the owner of the files, authorized users and specified recovery agents are able to decrypt encrypted files. In this manner, EFS secures confidential corporate data from unauthorized access.

EFS utilizes industry standard algorithms and public key cryptography to ensure strong encryption. The files that are encrypted are therefore always confidential. Even though logon authentication and NTFS file permissions are geared at protecting confidential data, you can use EFS to add an additional layer of security. This would ensure that when hackers gain full access to the data store of a computer, the data located in files are secured because of EFS encryption. An unauthorized person would not be able to open anencrypted file.

EFS in Windows Server 2003 further improves on the capabilities of EFS in Windows 2000. Users that are utilizing EFS can share encrypted files with other users on file shares and even Web folders. You can configure EFS features throughGroup Policy and command-line tools. EFS is well suited for securing sensitive data on portable computers. It also works well for securing data when computers are shared by multiple users.



Advanced Attributes

Choose the settings you want for this folder

When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

☑ For fast searching, allow Indexing Service to index this folder

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

How EFS works

EFS is actually firmly integrated with NTFS, and itsfile encryption and decryption processes are*transparent to the users*. What this means is that when users save a file, EFS encrypts data as the data is written to disk, and when users open a file, it is decrypted by EFS as data is read from disk. Users are basically unaware of this process, and need not take any action to initiate EFS encryption and decryption. There may be third party technologies that

can provide file encryption capabilities but these programs are not completely transparent to users. With these programs, the responsibility would be placed on users to remember to utilize the encryption program. This in turn leads to weaker security processes, and could possibly create security vulnerabilities for sensitive, confidential data.
EFS utilizes keys to encrypt and decrypt data, and the cryptography application programming interface (CryptoAPI) architecture to supply cryptographic functions. Even though it can use enterprise certificate authority (CA) certificates, this not a requirement. When no CA exists, EFS signs a certificate that can be used with file encryption. Because of this feature, EFS can function on computers that are members of a domain, and on standalone computers.

The keys which EFS uses to encrypt and decrypt data, is a public and private key pair, and a per file encryption key. EFS generates a file encryption key (FEK) which is a symmetric encryption key to encrypt the data. The File Encryption Key (FEK) is next encrypted by means of asymmetric encryption using the user’s public key. Asymmetric encryption actually uses a public and private key pair for stronger security. The encrypted FEK is then stored with the encrypted file. When the file needs to be decrypted, the FEK must be decrypted. The user’s private key is used to decrypt the FEK. The FEK is then used to decrypt the data of the file.

EFS Key Characteristics

- EFS is enabled by default. Users however need a public and private key pair, and permission to use EFS.
- EFS needs a recovery agent certificate for it to work. It will generate the certificate if you do not have one.
- EFS can only encrypt files when the NTFS file system is being used. li>Encryption has no impact on file and folder permissions
- You can authorize multiple users to share encrypted files.
- When you move EFS files to a different file system, encryption is removed.
- When you move files to a folder that is encrypted, the file stays in its original form. It stays either encrypted or unencrypted.
- When you copy a file to an encrypted folder, the file will be encrypted.
- When a folder is encrypted, all temporary files in that particular folder are encrypted as well.
- Encryption is listed as a file attribute, and is therefore displayed with the remainder of the attributes of the file.

- EFS can encrypt and decrypt files on a remote computer.
- Offline files can also be encrypted by EFS.
- Files that are encrypted can be stored in Web folders.
- EFS previously utilized Data Encryption Standard Extended (DESX) for encryption. With Windows Server 2003, the triple-DES (3DES) encryption algorithm can be utilized to enhance the security of EFS.
- You can back up encrypted files.
- Any compressed files and folders need to be decompressed before they can be encrypted.
- System files and folders cannot be encrypted.
- Files or folders in a roaming user profile cannot be encrypted.

The Components of EFS

EFS uses the following components to perform its functions:

- *EFS service*: The EFS service communicates with the EFS driver through the local procedure call (LPC) port. The EFS service and the Microsoft Cryptographic Application Programming Interface (CryptoAPI) communicate, with the EFS service receiving file encryption keys from the CryptoAPI. It uses these keys to generate data decryption fields (DDFs) and data recovery fields (DRFs). The file encryption key (FEK) is utilized for the data of the files. The EFS service passes the FEK, DRF, and DDF to the EFS driver through the EFS File System Run-Time Library (FSRTL).
- *EFS driver*: The EFS driver requests file encryption keys, DDFs and DRFs from the EFS service. It then relays these to the EFS FSRTL.
- *EFS File System Run-Time Library (FSRTL)*: The EFS FSRTL exists in the EFS driver, and operates with the EFS driver as one component. NTFS file control callouts are utilized as the communication mechanism between the two. The EFS FSRTL carries out a set of file system functions which include encrypting, decrypting, and recovering file data when it is read from disk or written to disk.
- *Microsoft Cryptographic Application Programming Interface (CryptoAPI)*: CryptoAPI is utilized by EFS for cryptographic functions. CryptoAPI supports encryption, decryption, hashing, digital signatures and the verification thereof, key management, secure storage, and key exchange operations.

How files are encrypted and decrypted

As mentioned earlier, EFS utilizes public key and symmetric key encryption to secure the contents of files and folders. The algorithms in public key encryption utilize asymmetric keys for encryption and decryption. What this means is that the keys utilized to encrypt and decrypt data are different because a private key and a public key is utilized. The private key is kept by the owner of the key. The public key can be utilized on the network.

When data is encrypted, EFS generates a unique FEK to encrypt the file. It then encrypts the FEK using the public key of the certificate of the user. EFS uses the FEK to ensure that encryption occurs speedily. The private key of the user is utilized to decrypt the FEK.

The process outlined below occurs when a user encrypts a file:

- The file is opened by the EFS service.
- The data streams of the file are next copied to a plaintext temporary file located in the temporary directory of the system.
- EFS generates the unique FEK.
- The FEK is utilized to encrypt the file either through DESX or 3DES.
- The data decryption field (DDF) is created. The DDF holds the FEK encrypted through the public key of the user.
- Where a recovery agent is defined by means of Group Policy, the data recovery fields (DRFs) is created.
- The encrypted data, DDF, and DRF are stored in the file.
- The plaintext temporary file located in the temporary directory of the system is deleted.

The process outlined below occurs when a file is decrypted:

- NTFS actually identifies the files as being encrypted, and then submits a request for decryption through to the EFS driver.
- The EFS driver next obtains the data decryption field (DDF) and sends it to the EFS service.
- The EFS service obtains the private key of the user. It uses this key to decrypt the DDF.
- Once the EFS service has decrypted the DDF and obtained the FEK, it sends the FEK on to the EFS driver.
- The EFS driver utilizes the FEK it received from the EFS service to decrypt the data in the file.
- The EFS driver then passes the decrypted data to NTFS.

EFS and Certificates

As soon as a user enables encryption for a folder or files, EFS checks whether the user has an enterprise certificate stored in the personal certificate store. EFS requests a certificate for the user when it cannot find a certificate in the personal certificate store, from a certification authority (CA). EFS proceeds to create a self signed certificate for the user if there is no enterprise CAs. The EFS certificate of the user is accessed when EFS needs to encrypt and decrypt the FEK. EFS also renews EFS certificates that have expired.

Certificates which are obtained from enterprise CAs use certificate templates that are stored in Active Directory. Certificate templates detail the attributes of certificate types that can be issued to users and computers. The certificate templates that support EFS are User, Administrator, and Basic EFS. Enterprise. CAs utilizes Access Control Lists (ACLs) when they need to ascertain whether certificate requests should be approved. A user therefore has to have the Enroll permission for a certificate template to have a certificate issued. Members of the Domain Admins group and Domain Users group have this permission. Users can use the Certificates snap-in to request certificates.
Use the steps below to request a certificate from a CA via the Certificates snap-in.

1. Open the Certificates snap-in.
2. Proceed to expand the Personal folder.
3. Right-click Certificates and choose All Tasks, and then Request New Certificate from the shortcut menu.
4. The Request New Certificate wizard launches.
5. Choose the Basic EFS option on the Certificate Types screen. Click Next.
6. Provide information for Friendly name and Description. Click Next.
7. Click Finish to exit the wizard.
8. The new certificate is stored in the Certificates folder.

You can use the Certificates snap-in to check whether you already have a certificate.

1. Proceed to navigate to and open the Certificates snap-in set up for the My user account.
2. Expand the Personal folder.
3. Right-click Certificates to view whether a certificate exists.

Encrypting/Decrypting files using EFS

It is recommended to enable EFS encryption for folders instead of enabling it for individual files. By doing this, you would not need to encrypt each individual file when saving the file.

Use the steps below to encrypt a folder.

1. Open My Computer.
2. Right-click the folder that you want to encrypt, and select Properties from the shortcut menu.

3. When the Properties dialog box of the folder opens, click the Advanced button on the General tab.
4. The Advanced Attributes dialog box is displayed.
5. In the Compress or Encrypt attributes section of the Advanced Attributes dialog box enable the Encrypt contents to secure data checkbox.
6. Click OK to enable encryption for the folder and all files included in the folder.
7. An additional message is displayed in a dialog box when the folder includes subfolders and files that are unencrypted. The message prompts you to verify whether your settings should be applied to the folder only or to the folder's subfolders and files as well.
8. If you choose the Apply changes to this folder only option, the following occurs:
   - Files already stored in the folder and any subfolders remain in their original state.
   - Files that you create in the folder are encrypted.
   - Files copied to the folder by you and other users are encrypted.
   - Files created in, copied or moved to subfolders remain in their original state.
9. If you choose the Apply changes to this folder, subfolders, and files option, the following occurs:
   - Files already stored in the folder and any subfolders are encrypted if you have the Write permission.
   - Files created in, copied or moved to subfolders are encrypted, whether by you or other users.

Use the steps below to decrypt a folder.

1. Right-click the folder that you want to decrypt, and select Properties from the shortcut menu.
2. When the Properties dialog box of the folder opens, click the Advanced button on the General tab.
3. When the Advanced Attributes dialog box is displayed, clear the Encrypt contents to secure data checkbox.

How to encrypt offline files

1. Open My Computer.
2. Use the Tools menu to select the Folder Options item.
3. Use the Offline Files tab to:
   - Enable Offline Files.
   - Encrypt offline files.
4. Click OK.

How to view the status of EFS encryption

1. Open My Computer.
2. Use the Tools menu to select the Folder Options item.
3. Click the View tab.
4. Enable the Show encrypted or compressed NTFS files in color checkbox.
5. Click OK.
6. Encrypted folder and file names are displayed in green.

How to enable EFS options on the shortcut menu

If EFS options are enabled on the shortcut menu, a user merely has to right-click the folder or file to encrypt or decrypt the folder or file.

1. Click Start, Run, and enter regedit.exe in the Run dialog box. Click OK.
2. The Registry Editor opens.
3. Locate the following subkey:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvanced

4. Use the Edit menu to select New, and then DWORD Value.
5. Proceed to specify EncryptionContextMenu for value name, and 1 for value data.
6. Registry changes are effective immediately.

How to use cipher.exe to view, create or modify encryption on folders and files

Cipher.exe is a command line tool that can be used to encrypt and decrypt folders or files. Using the cipher command with no switches will display the status of encryption on the folder and files located within the folder.

The syntax for the cipher command and its switches are noted below:

```
cipher [{/e|/d}][/s:Folder][/a][/i][/f][/q][/h][/k][/u [/n]]
```

- `/e`, encrypts the particular folders, and files added are encrypted as well.
- `/d`, decrypts the particular folders. The encryption attribute is removed from the folders.
- `/s:Folder`, used to indicate the folder and subfolders that should be utilized.
- `/a`, used to encrypt files in the current directory.
- `/i`, used to indicate that the current process should continue even though errors are present.
- `/f`, used to force encryption or decryption for all defined files and folders.
- `/q`, lists only the important information.
- `/h`, lists files that have hidden attributes and system attributes.
- `/k`, generates a new FEK for the particular user running the command.

- `/u`, updates the FEK of the user and the key of the recovery agent. Used with /n switch.
- `/n`, stops keys from being updated. Used with /u switch.

How to authorize multiple user access to encrypted files

Before authorizing multiple users access to encrypted files, consider the following:

- A file share, web folder or remote session is required for authorized users to share EFS files across the network.
- The users that you are going to authorize to access the EFS files must have EFS certificates.
- When you authorize a user to decrypt a file, the user is automatically able to authorize additional users with access to the file.

Use the steps below to share an EFS file with additional users.

1. Open My Computer.
2. Right-click the encrypted file and select Properties from the shortcut menu.
3. When the Advanced Attributes dialog box opens, click the Details button.
4. The Encryption Details dialog box opens.
5. Click Add to open the Select User dialog box.
6. You can now add a user from the local computer, or from Active Directory.
7. Click the certificate of the user to add a user from the local computer. Click OK.
8. Click the Find User button to find a user in Active Directory.
9. Then click Browse when the Find Users, Contacts, and Groups dialog box opens to find the user(s).
10. Click the folder or domain that should be searched in the Browse for Container dialog box.
11. Select the user(s) and then click OK.

File Recovery Agents

Being able to recover data becomes important when employees misplace their private keys or leave the organization without decrypting all of their files. This is when recovery agent becomes important. In order to utilize EFS, an Encrypted Data Recovery Agent policy must exist. EFS automatically utilizes a default recovery agent account when no Encrypted Data Recovery Agent policy exists. Members of the Domain Admins group can specify an account to use for the recovery agent account. Local policy can be used on standalone computers to specify accounts as data recovery agents. These accounts are normally an Administrator account. DRA certificates are stored in the certificate store of the computer when a user accesses a domain computer that is included in the range of the EFS recovery policy. This makes it possible for each domain computer to access the public key of the DRA. Encrypted files contain a data recovery field that in turn holds the file encrypted FEK. A DRA can decrypt an encrypted file that is in the range of the EFS recovery policy through the utilization of the private key.

You should define multiple DRAs through EFS recovery policy if you want multiple users to be able to decrypt files. Files are generally more secure if only one person is able to decrypt the file. The downside though is that the file is less recoverable.

Use the steps below to add a recovery agent for the local computer.

1. Click Start, Run, and then enter mmc in the Run dialog box. Click OK.
2. Choose Add/Remove Snap-in from the File menu, and click Add.
3. When the Add Standalone Snap-in dialog box appears, choose Group Policy Object Editor. Click Add.
4. Ensure that Local Computer is selected. Click OK.
5. In the left pane, proceed to expand Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, and Public Key Settings.
6. Right-click Encrypting File System, and then choose Properties from the shortcut menu.
7. EFS is running on the computer if the Allow users to encrypt files using Ecrypting File System (EFS) checkbox is enabled. Click OK.
8. Right-click Encrypting File System and choose Add Data Recovery Agent from the shortcut menu.
9. The Add Recovery Agent Wizard starts.
10. Provide a user name for the user that has a recovery certificate. Click Next.
11. On the Select Recovery Agents screen, browse through folders/directories to specify users.
12. Click Next. Click Finish.

Use the steps below to remove a DRS.

1. Using Group Policy, in the left pane, proceed to expand Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Public Key Policies, and Encrypting File System.
2. Choose the DRA that you want to delete, and delete the certificate.

How to export and import EFS and DRA certificates and private keys

Users can ensure access to encrypted files by exporting their EFS certificates and private keys to removable media.

Use the steps below to export a certificate to a removable medium.

1. Proceed to access the Certificates snap-in.
2. Expand the Personal folder, and then double-click Certificates.
3. Find and right-click the certificate which you want to export, and choose All Tasks, and then Export from the shortcut menu.
4. Choose Yes, export the private key.
5. You can now either choose to delete the private key from the computer after it has been exported, or you can choose to leave it on the computer. After selecting an option that suits your needs, click Next.
6. Provide a password for the protection of the exported private key. Click Next.
7. Provide a name for the exported certificate and private key.
8. Click Next. Click Finish.

Use the steps below to import a certificate.

1. Proceed to access the Certificates snap-in.
2. Expand the Personal folder, and then right-click Certificates, choose All Tasks, and then Import from the shortcut menu.
3. Enter the certificate file that should be imported.
4. Provide the proper password to open the file.
5. Specify a location where the certificate should be imported to.

How to strengthen key and file security

You can strengthen security by replacing the DESX algorithm that EFS utilizes, with the stronger 3DES algorithm. You can use the system cryptography Group Policy setting to enable 3DES for encryption for IP Security and EFS. You can however change the appropriate registry setting in the HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsNTCurrentVersionEFS key via the Registry Editor to enable 3DES for encryption for EFS only.

You can also use a startup key to protect master keys and confidential information that resides on the computer. A startup key is also called a syskey. Startup keys are automatically created for computers that are members of a domain. You have to manually create a startup key for a standalone computer.

A startup key protects the following confidential information:

- Master keys: These are keys utilized to protect private keys.
- Protection keys: These are keys for user account passwords stored in either Active Directory, or in the local Security Accounts Manager (SAM) registry key.
- Protection keys for your LSA secrets.
- The protection key for the administrator account password.

After a startup key is enabled, the procedure that takes place at startup is as follows:

- The system retrieves the startup key.
- It is then utilized to decrypt the master protection key.
- This key is then utilized to obtain the user account encryption key.
- The user account encryption key is utilized to decrypt the password information in Active Directory, or in the local Security Accounts Manager (SAM) registry key.

Use the steps below to enable 3DES for encryption for EFS only.

1. Open the Registry Editor.
2. Locate the HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionEFS registry subkey.
3. Use the Edit menu to click New, and then DWORD Value.
4. Insert AlgorithmID for value name, and 0×6603 for value data.
5. These values enable 3DES.
6. Restart the computer.

Use the steps below to enable 3DES using Group Policy.

1. Using Group Policy, in the left pane, proceed to expand Computer Configuration, Windows Settings, Security Settings, Local Policies, and Security Options.
2. Double-click the System cryptography: Use FIPS compliant algorithms for encryption policy.
3. Choose Enable.
4. Click OK.

Use the steps below to enable the startup key.

1. Enter syskey at the command line.
2. Proceed to click Encryption Enabled.
3. Click OK.
4. Choose an option for the key. The system-generated password that is stored locally option is the default option.
5. Click OK to restart the computer.

Use the steps below to change the startup key options.

1. Enter syskey at the command line.
2. Proceed to click Update.
3. Proceed to change the password, or choose a different key option.
4. Click OK. Restart the computer.

How to disable EFS

You can either disable EFS for a computer or for the domain. Use the steps below to disable EFS using the Registry Editor

1. Open the Registry Editor.
2. Locate the HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionEFS registry subkey.
3. Use the Edit menu to click New, and then DWORD Value.
4. Insert EfsConfiguration for value name, and 1 for value data.
5. These values disable EFS.
6. Restart the computer.

EFS Best Practices

A few best practices for EFS are summarized below:

- Always *select to encrypt folders, and not individual files*. Encrypting folders facilitates simple file encryption management. Remember that any files located in, or created in an encrypted folder are automatically encrypted.
- You can use Microsoft Certificate Services to manage EFS and DRA certificates/private keys.
- Users should export their EFS certificates and private keys to removable media, and also store the media in a safe place.
- Try to have a small number of specified recovery agents. The less the number of recovery agents, the simpler it is to manage them, and ensure that they are not incorrectly decrypting files.
- You should also export the private keys for recovery accounts, and secure them in a safe location.
- You should strive to encrypt sensitive data on each computer that is a member of a domain.
- Enable a startup key on standalone computers to further enhance security for the private keys of users.

- Ensure that the My Documents folder is encrypted in cases where the user connects to the same computer.
- You should encrypt offline files to ensure protection for locally stored documents.
- Using Server Message Block (SMB) signing with EFS assists in ensuring that files are securely transmitted/received over the network.
- You can also use IPSec to encrypt data as it moves over the network.

Source:

http://www.tech-faq.com/encrypting-file-system-efs.html