Control file system encryption (EFS) with Group Policy

File system encryption (EFS) is a useful feature for protecting data stored on Windows computers. EFS is a completely free option and is included in operating systems since Windows 2000.

File system encryption (EFS) is a useful feature for protecting data stored on Windows computers. EFS is a completely free option and is included in operating systems since Windows 2000. Like other issues, EFS also has significant improvements in each version. With the advantages of technology, it is more and more practical for using EFS in your data storage environment. However, you may not want to support EFS anywhere, so narrow the scope and control where it is used. Therefore, the solution to take advantage of Group Policy to help manage EFS is proposed to solve this problem.

Two-tier EFS management

EFS has two configuration levels. The first level is set at the machine, this is the declared level to be used or not. The second level is the file and directory level, which performs data encryption.

Windows 2000 (Server and Professional), Windows XP Professional, Windows Server 2003, Windows Vista, and Windows Server 2008, all support data encryption on computers. By default, all of these computers support data encryption with EFS. Obviously, this is something that is not positive because some data or some computers sometimes do not need to encrypt data.

Computers without data encryption are being talked about as computers that allow users to encrypt data. All computers support the default data encryption and any user can encrypt, the data can be encrypted on the internal desktop as well as shared on the network. Figure 1 illustrates this option, where data can be encrypted on a Windows XP Professional computer.

Figure 1: Encryption is a property of the data

To access the encryption option shown in Figure 1, you only need to access the properties of the files and folders you want to encrypt, done by right-clicking on the object, then selecting Properties. Then select the Advanced button in the Properties dialog box, then the Advanced Attributes dialog box will appear.

Control the support of EFS for computers in the Active Directory domain

When a computer joins an AD domain, it is controlled for the support of EFS. Instead of the Default Domain Policy stored in Active Directory that controls this capability, all computers that are joined to the Windows Active Directory domain support EFS, simply needing to join the domain.

One problem is that Windows 2000 domains manage this configuration in the Default Domain Policy, however, compared to Windows Server 2003 and Windows Server 2008 domains.

The Windows 2000 domain controls EFS

Windows 2000 computers that support EFS are different from other operating systems, which is why configuring EFS is different within the Default Domain Policy. With Windows 2000, the key to enabling and disabling EFS is all based on the existing EFS data recovery agent certificate in the Default Domain Policy. By default, the administrator account will have this certificate and be configured as a data recovery agent. (If there is no certificate to recover the data, then EFS will fail)

To access this configuration in the Default Domain Policy, follow this path when editing a GPO in Group Policy Editor:

Computer Configuration Windows SettingsSecurity SettingsPublic Key PoliciesEncrypted Data Recovery Agents

Here, you will see EFS File Encryption Certificate for administrators, as shown in Figure 2.

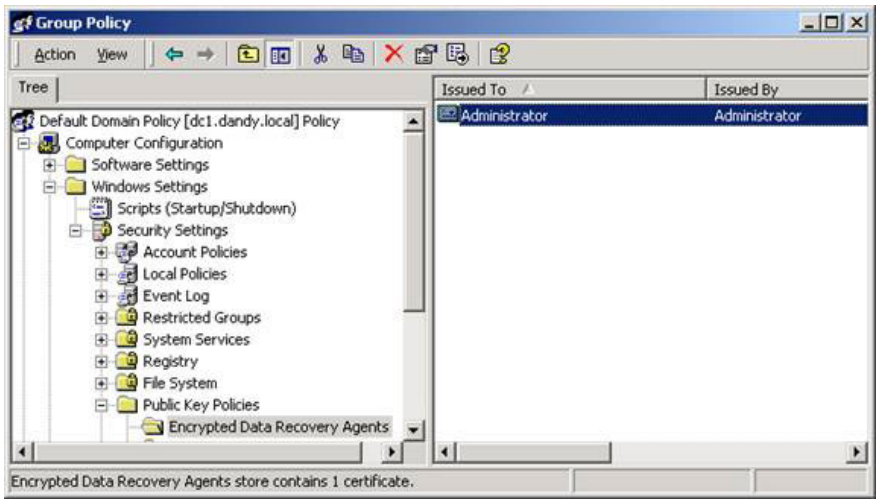

Figure 2: Windows 2000 domain shows the File Encryption Certificate of EFS with a user name, Administrator.

This configuration is all that the computer has the ability to encrypt files. To remove this capability, you must remove the Administrator certificate from the GPO. If you want to later provide EFS to some computers in Active Directory, follow the steps below:

1. Create a new GPO and link it to the organizational unit with all computers that need encryption support.

2. Access the **Encrypted Data Recovery Agents** button in the GPO and add the EFS data recovery certificate.

This will provide computers affected by GPO with the ability to use EFS for data stored on computers.

For domains of Windows 2003 and 2008

Newer domains and new operating systems (after Windows 2000) all support EFS with almost the same features, with only a few changes below:

1. No data recovery agent is needed for encryption on Windows 2000 computers.

2. EFS is not controlled with the inclusion of the data recovery agent certificate in the GPO.

3. EFS supports multi-user access to encrypted files.

Therefore, for Windows 2003 and 2008 domains, you will have a set of other tasks to perform EFS control for computers located in the domain. However, the setup is still in the Default Domain Policy. The new path you need to access will be:

Computer Configuration Windows SettingsSecurity SettingsPublic Key PoliciesEncrypting File System

Now instead of adjusting the data recovery agent, just right-click the **Encrypting File System** button. From the right-click menu, select **Properties** . In the **Properties** window, you will see a ' **Allow users to encrypt files** ' box **using Encrypting File System (EFS)** ' - *allowing* **users to encrypt files using** *EFS* (for Windows 2003). Windows 2008 domains have many interface changes, providing support for EFS from this property page as shown in Figure 3 below.

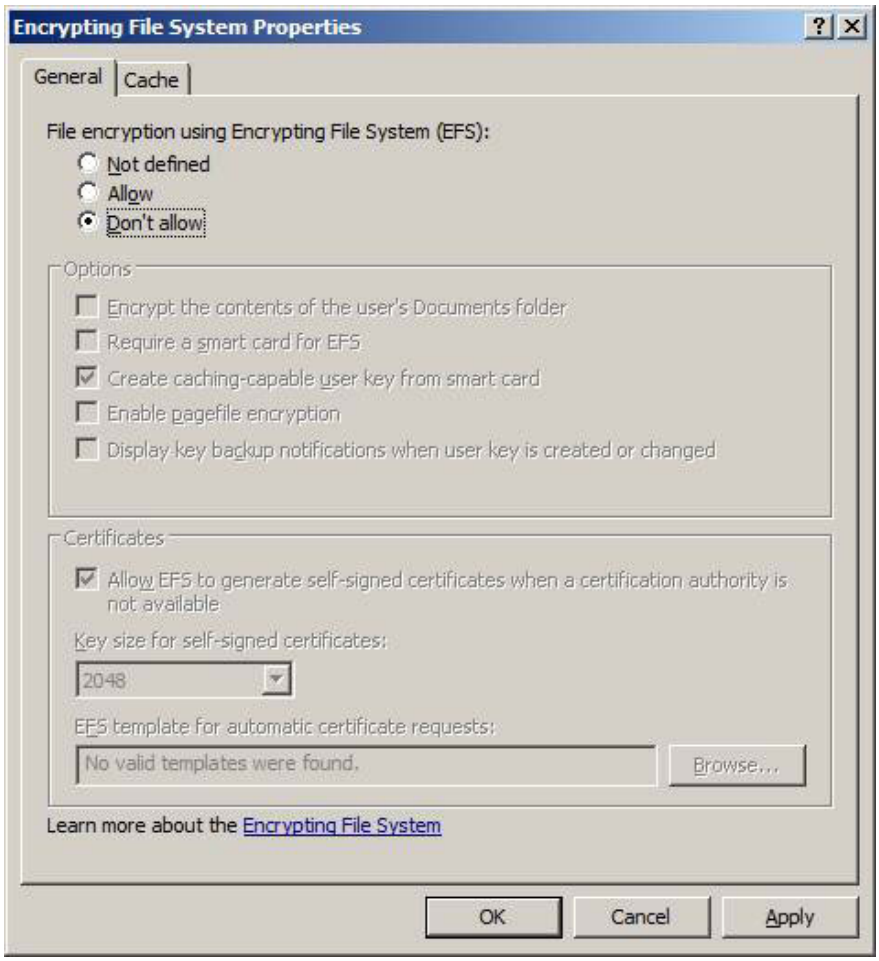

Figure 3: Windows Server 2008 allows EFS control

Note on the **General** tab, there is a ' **Don't allow** ' button. This is the configuration that can be set to disable EFS on all computers in the domain. Also note that many of the settings provided in this dialog box are also related to EFS control.

You can also target certain computers in the domain by following the steps above for Windows 2000.

Conclude

EFS is really a very useful and superior component. It can encrypt data saved in Windows computers. This encryption will help protect against users and attackers who want to access unauthorized data. EFS is a two-step process, the first step EFS must be activated on the computer. This is a step that can be controlled by Group

Policy, and when computers join a domain. The administrator can enable or disable EFS on any computer in the domain by configuring the GPO. By disabling EFS for all computers in the domain and then creating and configuring a new GPO, then only designated machines can use EFS.