

The information for this Task Sheet originally appeared in the TechProGuild article, "[Remove EFS from Win2K/XP clients to avoid security breaches](#)". In this article, Karl Koehler provides a detailed explanation of Microsoft's Encrypting File System (EFS) that is included in Windows 2000 and Windows XP Professional. Koehler outlines when you should use EFS, when you shouldn't, and how to disable EFS.

By Bill Detwiler

## Problem

Microsoft's Encrypting File System (EFS) is enabled on Windows 2000 and XP Professional systems by default and allows any user with modify permissions to encrypt a file or folder. Because users with modify permission to a file or folder can encrypt those files and folders (even ones they did not create), it is possible for users to encrypt an item shared by a large group of people, accidentally making it inaccessible to everyone else.

## Solution

### Disable EFS on Windows 2000

1. Open the local system security policy.
2. Delete the administrator certificate from the folder marked **Encrypted Data Recovery Agents**, as shown in **Figure A**.

### Windows XP Pro

#### Using Group Policy in an Active Directory environment

1. You disable EFS through Group Policy on XP systems in an Active Directory network, but an admin template must be created and imported into the Domain Group Policy first. To do, paste the following into a text file in Notepad:

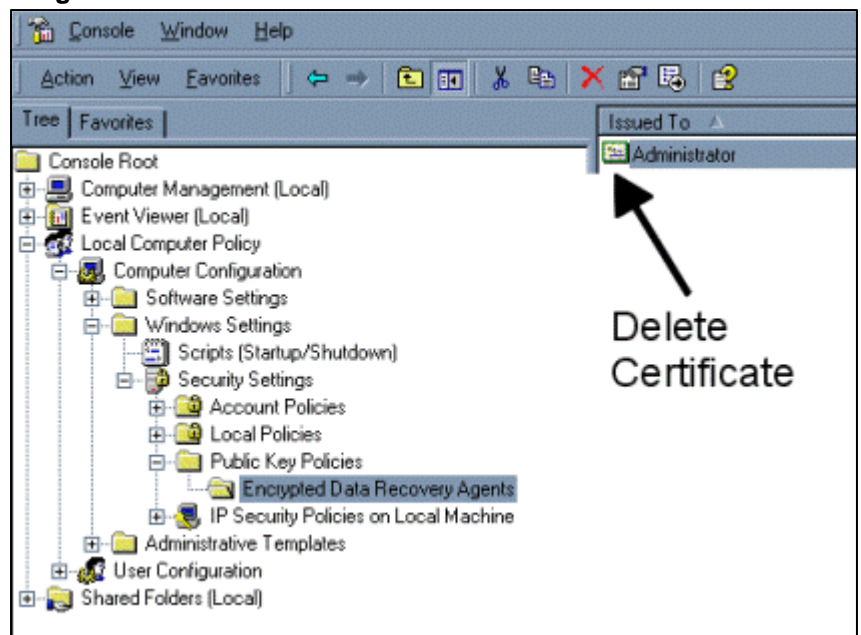
```

CLASS MACHINE
CATEGORY "Special EFS Handling"
POLICY "Disable XP and .NET EFS"
#if version >= 4
SUPPORTED "At least Microsoft Windows XP Professional"
#elseif
KEYNAME "Software\Policies\Microsoft\Windows NT\CurrentVersion\Efs"
EXPLAIN "This policy stops XP desktops from encrypting files in a Win2K domain. Enable the policy to disable EFS."
VALUENAME "EfsConfiguration"
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
END POLICY
END CATEGORY

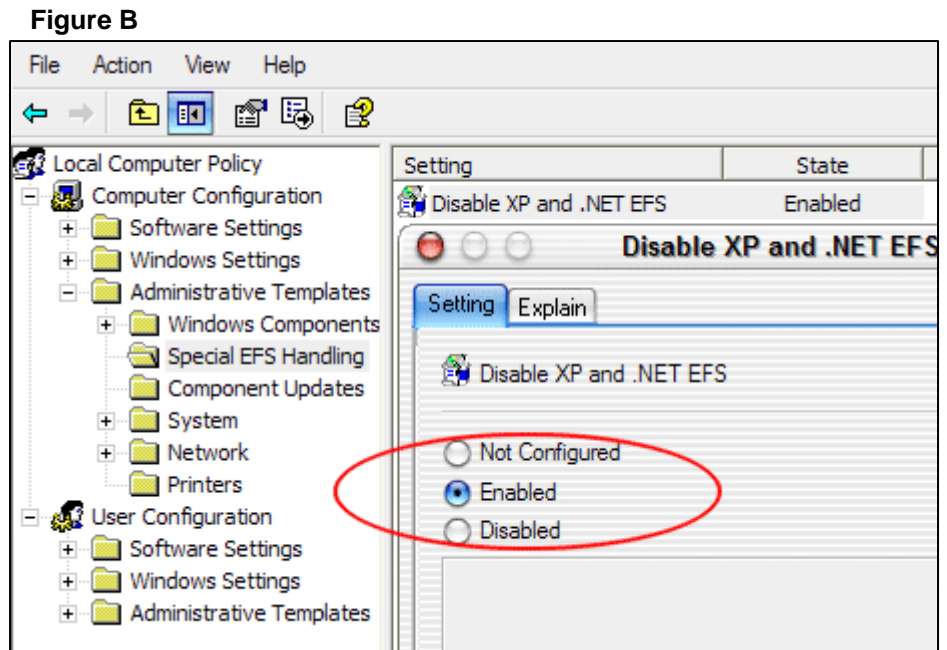
```

2. Save the file with the name efs-disable.adm
3. Open the Group Policy for the domain. (Right-click on the domain inside the AD Users And Computers tool, and choose Properties. Click on the Group Policy tab and then click Edit.)

Figure A



4. Open the computer configuration section.
5. Right-click on the Administrative Templates folder. You should have the option to Add/Remove Templates. Choose that option and then click on the Add button. Browse to the .adm file you just created and click on Open. Now click on Close. You'll now find a folder under Administrative Templates called Special EFS Handling.
6. Enable the Disable XP and .NET EFS and all XP systems in the domain will have their EFS disabled, as shown in **Figure B**.



This process works on the local system Group Policy for Windows XP Professional systems that are not running in an ADS environment if they're running SP1.

## Hacking the Windows XP Registry

To disable EFS, set the following Windows registry key's DWORD value to 1:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Efs**

You can set this key's DWORD value using several methods, including manually editing the registry and pushing a REG file to the target machines via e-mail or a script. Create a REG file that disables the splash screen with the following steps:

1. Open a new file using Notepad or another text editor.
2. Enter the following four lines. (Note: The second line must be blank.)

### Windows Registry Editor Version 5.00

**[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Efs]**

**"EfsConfiguration"=dword:00000001**

3. Save the file with a file name such as efs-disable.reg
4. Running the REG file from the target machine will now disable EFS. This process works better on XP systems not running SP1.

*Title goes here*

## **Additional resources**

- Sign up for the [Windows XP newsletter](#), delivered on Thursdays
- Sign up for the [Windows 2000 Professional](#), delivered on Tuesdays
- See all of [TechRepublic's newsletter offerings](#)
- ["Lock down corporate data with EFS"](#) (TechRepublic)
- ["Tech Tip: Add recovery agents for EFS/Back up the registry with the Backup utility"](#) (TechRepublic)

## **Version history**

**Version:** 1.0

**Published:** March 28, 2005

## **Tell us what you think**

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team