Control of resource terms

Everyone knows that it's important to lock up and protect your resources online. The resources that need to be protected here include folders, files contained in them, as well as some registry keys that are placed on your computer.

Derek Melber

Everyone knows that it's important to lock up and protect your resources online. The resources that need to be protected here include directories and files contained in them, as well as some registry keys that are placed on servers and workstations in the enterprise. We cannot forget the Active Directory objects that reside on domain controllers. All of these resources need to be protected so that users without a task will not be able to access them. To control the terms on these resources, you have a lot of choices. Some options are more appealing, so let's look at these options carefully.

Resource Terms 101

To get a discussion regarding resource terms, we had to refine what resources would attack and how to protect that resource by terms. Indeed we have a huge amount of resources on each network, so there is no way to handle all of them. However, we will introduce the main resources that you are probably also interested in controlling them.

Before managing the list of resources, we want to refine what seems to be very messy and messy even with seasoned administrators. There are two types of permissions that can be configured on each resource. It is NTFS permissions and sharing terms. The terms we will discuss are NTFS permissions. Real terms of sharing do not provide many security features for resources, as they only control access to shared folders instead of providing core access control with the Small folders and files are in that shared folder. To filter out where each of these permissions is configured, the sharing terms are configured using the Share tab shown in Figure 1.

Figure 1: Control items for shared permissions in a shared folder from a network

NTFS permissions are associated with the Security tab as shown in Figure 2.

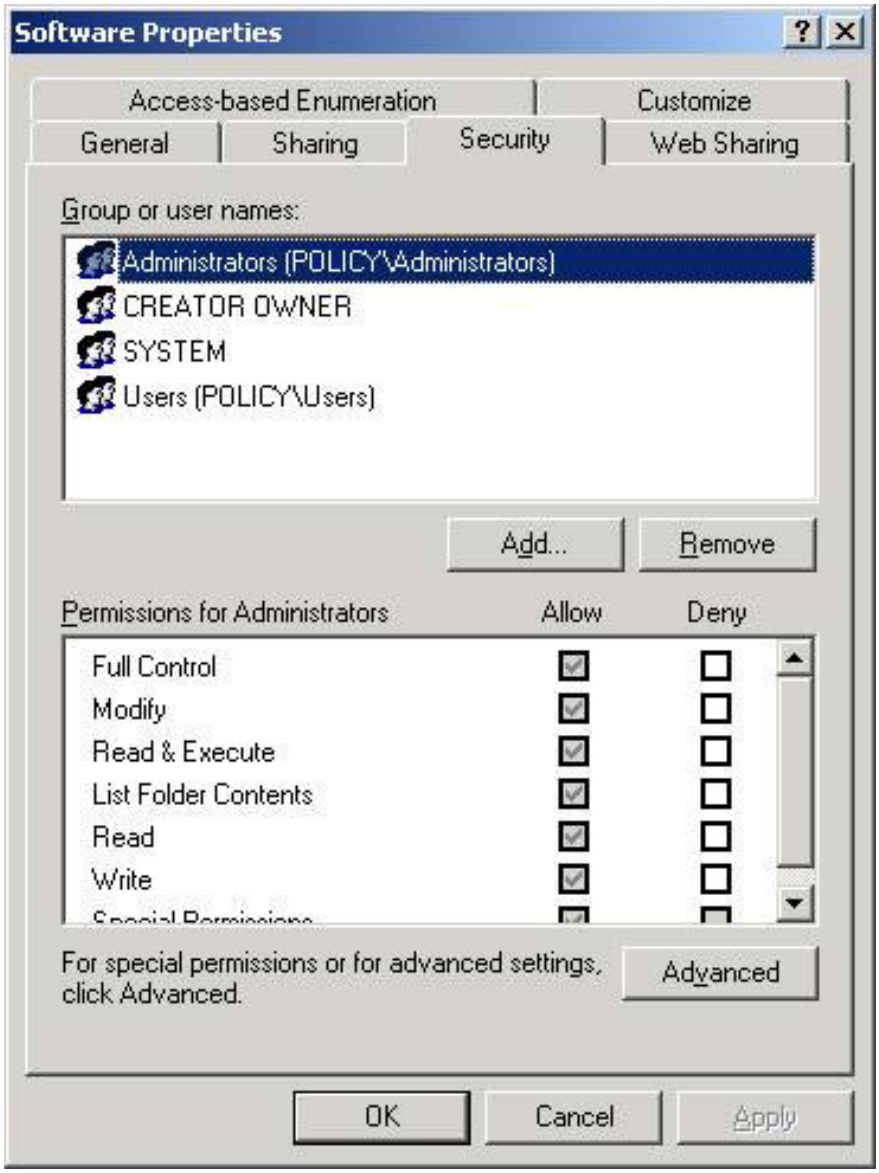

Figure 2: NTFS permissions are set and configured on the Security tab

Note :
The Security tab is usually not available on computers without the configured NTFS edition. These editions are not configured as FAT or FAT32 file systems.

Resources with related NTFS permissions include:

1. Folder
2. File
3. Registry keys
4. Printer
5. Active Directory object

This list of resources is quite important because only these resources can have the Access Control List (ACL) of the Windows system name. In this article, we will focus on how to change permissions on Active Directory

directories, files and objects.

Configure resource permissions for files and directories

As mentioned before, you can go to the Security tab on each file or folder to access this list of terms. There are a number of key issues to keep in mind when setting up permissions for these resources.

First, when setting permissions for files and folders, the best way to set permissions for groups, not to separate user accounts. Second, you need to set the access level for each file or directory. As shown in Figure 3, there are some standard terms that can be set without having to enter the Advanced terms for the account.

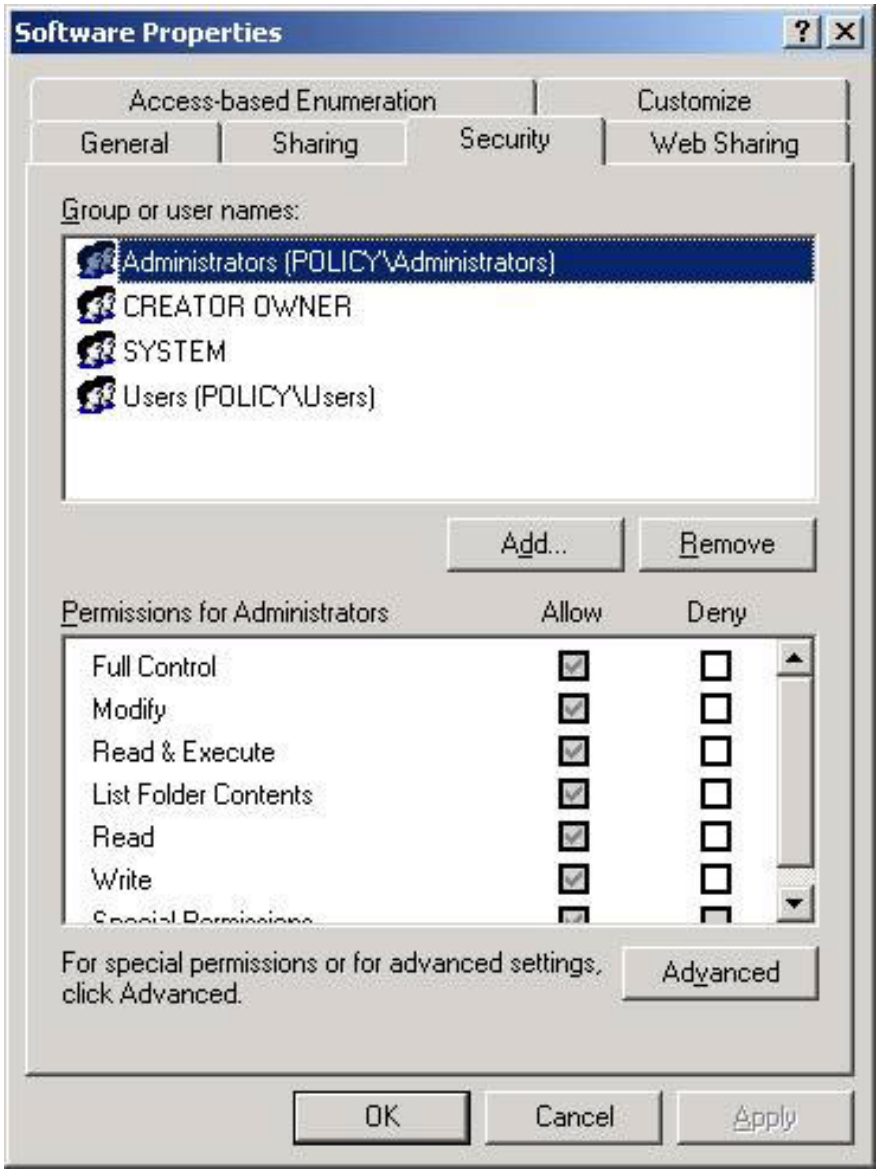

Figure 3: Standard permissions can be set for each account

Figure 4 demonstrates that you can also go to Advanced permissions to provide the core levels of permissions for each resource.

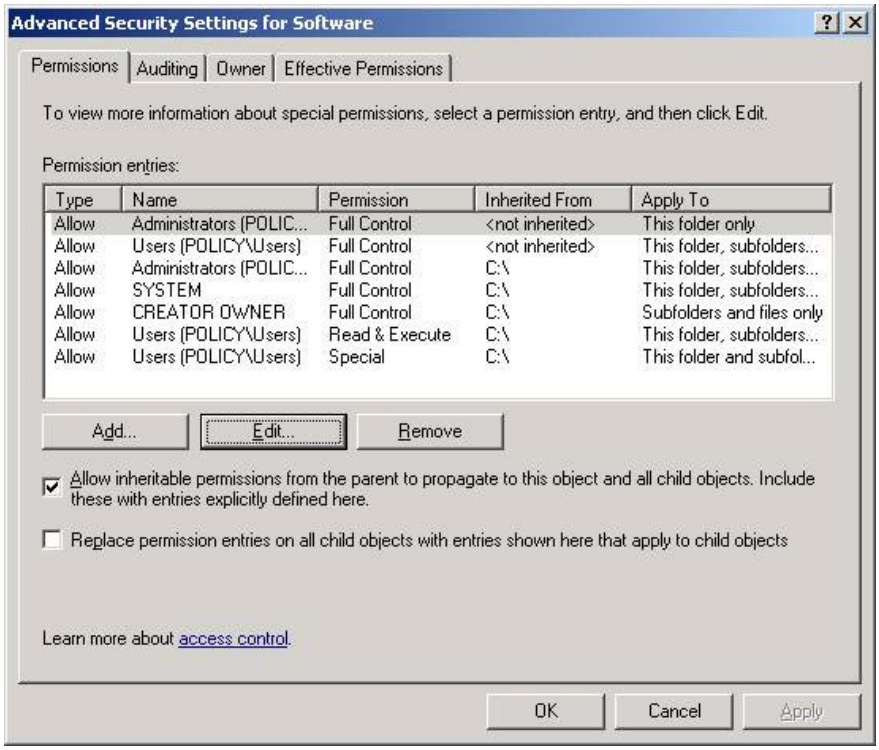

Figure 4: Advanced permissions allow control of the core on access to resources.

Note :
Click the Edit button in Figure 4 and you will see a full list of Advanced details. This is not the best way to manage resources, as it can cause significant difficulties in configuring, managing, and troubleshooting access to resources.

Configure permissions for the Active Directory object

The process of configuring Active Directory objects is the same, but there are a number of wizards that can help you configure it completely. This is a useful wizard because it has over 1000 advanced permissions for Active Directory objects, like organizational units, see Figure 5.

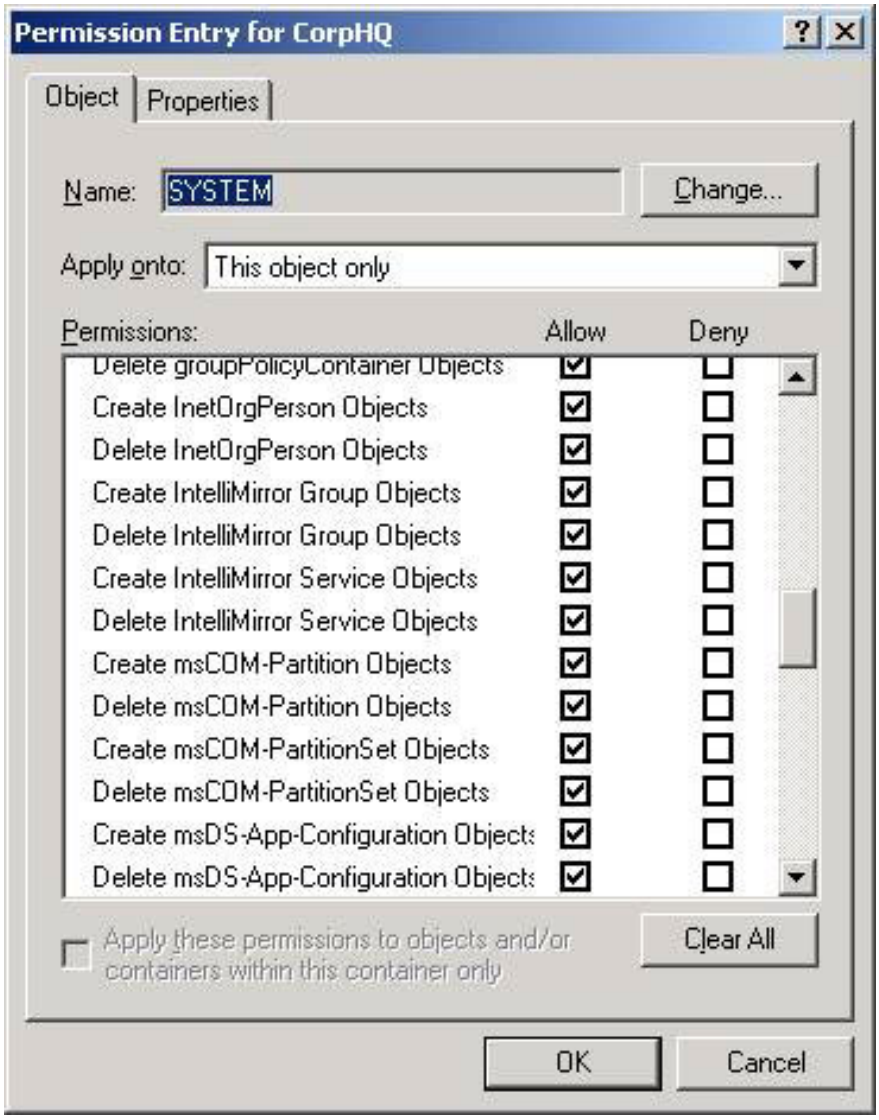

Figure 5: A partial list of terms for the organization block

To access this wizard, simply click on the button that needs to be configured. This click will reveal the Delegate Control menu option. Once selected, the Delegation of Control Wizard dialog box appears as shown in Figure 6 below.

Figure 6: The Delegation of Control Wizard allows you to easily configure the permissions on Active Directory Objects

This wizard will allow you to specify 'who' (user or group) will have 'what' access level (permissions) for objects in Active Directory.

Note :
It is possible to use the Security tab for Active Directory objects like directory and file configuration. However, this is a pretty boring task that can be confusing for most experienced administrators.

Configure resource permissions with Group Policy

When it comes to managing resource terms with Group Policy, you can only manage files and directories that cannot manage Active Directory objects. (The main permissions of the Registry can also be managed by Group Policy). The settings for controlling this provision are in the Computer Configuration section of Group Policy, as you can see in Figure 7.

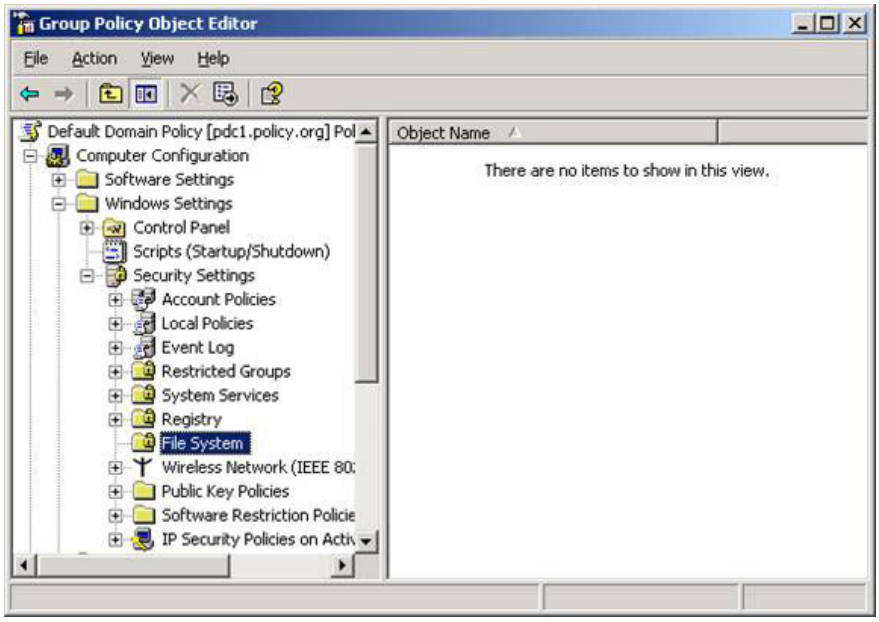

Figure 7: The File System button allows you to configure file and folder permissions using Group Policy

To use this option, you simply create and link a Group Policy Object (GPO) to a node that includes the computer account you want to configure. When you're done, edit the GPO and right-click the File System button. Select the Add File menu option, you can browse or type in the path to the file or folder you want to manage the permissions on. When you add that path, you will see the Security tab displayed for that resource, see Figure 8.

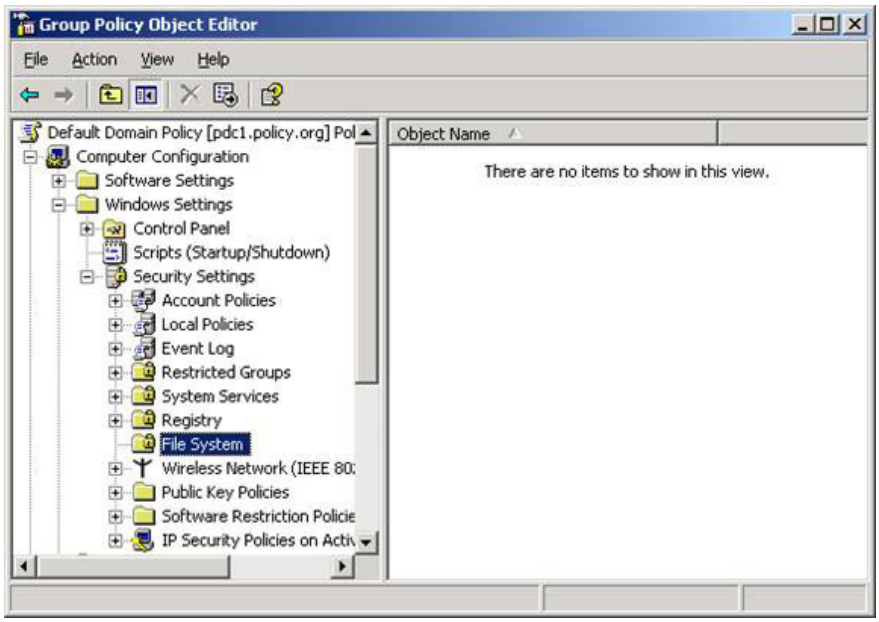

Figure 8: Security permissions can be set on files and folders in GPOs

Although you can use Group Policy to change or set permissions on that resource, you should not do so because of the application's performance. One problem has been demonstrated that too many existing permissions have been set up by Group Policy which will slow down the initial login and can slow down the system during the

periodic background refresh period. If these settings are used we should only use one part on each of these resources.

Configure resource permissions by script

After much research and analysis, we have shown that by using a script to set up resource terms, it is completely ineffective for setting permissions for both directories and files as well as Active Directory objects. However, we still want to mention some tools that can help you perform these actions, if you still want to use the script.
To use the script with directory and file permissions, you can use CACLS. CACLS will allow you to set and create permissions for files and folders. This tool is completely free from Microsoft and can be used independently or within VB or other scripts.

With Active Directory object permissions, you can use the new PowerShell options. PowerShell is provided for Windows XP and its operating systems. PowerShell has a lot of strengths to be able to control Active Directory permissions.

With both of the above options, script issues and PowerShell that we have told all of our own understandings, although these options are available, are easier and more efficient. If you use standard methods to set up and control terms. However, it is impossible not to mention the strengths of the script, they really have many strengths and uses, so if you want more details about these options, we will provide them with You have some links in English below:

http://www.microsoft.com/technet/scriptcenter/learnit.mspx
http://www.scriptinganswers.com/
http://en.wikipedia.org/wiki/Cacls

Conclude

Control of network resources and their terms is an extremely important issue for protecting resources in your company. If you need to control HR files, company secrets, group of organizational units, or other resources, you will need to set up and manage the permissions related to each of these resources. You have a lot of options in this, but deciding which options are used to make a big impact on your management and efficiency is important. Manual methods are not all easy and effective, but they can perform some of your tasks well with accuracy and without any computer-related problems at the start dynamic. Group Policy is also a good option, but you need to limit the options in it to just a few folders and files because the application of these permissions can take a long time. Scripts are also an option, but the time to test scripts may take more than using the available settings.