Group Policy special security settings

Many security settings can be configured in Group Policy Object. Those settings range from controlling Administrator accounts to managing LDAP client needs. With so many security settings, understanding the function and c

Derek Melber

Many security settings can be configured in Group Policy Object. Those settings range from controlling Administrator accounts to managing LDAP client needs. With so many security settings, it is important to understand functions and other essentials. In this article, we will detail some of the security settings as well as some of the most common security scenarios.

Implement Group Policy security settings

This topic has a lot of articles written by us or other articles, but the previous articles only show you how you can ensure that these security settings are applied. In this article, I want to introduce some more details on how you can verify which settings are 'policies' and which settings are 'references' so that you have a clear understanding. About how each setting is applied to the computer. For each type of setup, you can execute these settings at the Group Policy refresh interval, which is approximately 90 minutes.

All details are still running smoothly and the techniques in some of the previously published articles are still valid. However, there is another built-in built-in technology that you need to learn more here. This technology allows you to control how long the security settings in the GPO are refreshed without any changes to the GPO. The truth is, you can have all of the automatic security settings applied after a certain X minutes without changing to the GPO. The value of the registry that you need to change is ***MaxNoGPOListChangesInterval*** , see Figure 1.

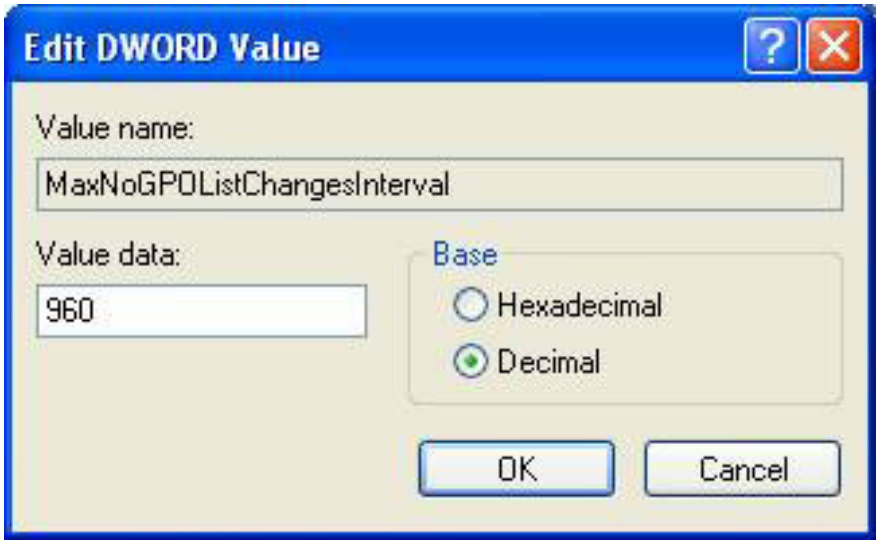

Figure 1: You can change the interval to refresh security settings in the GPO

You can find this setting in the Registry below:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionWinlogonGPExtensions {827D319E-6EAC-11D2-A4EA-00C04F79F83A}

The default value for this setting is 960 minutes (or 0x3c0 in hex numbers).

This setting is important because it allows administrators to ensure that existing security settings are valid or out of date for users without having to wait until each refresh cycle. Now users have a secure workstation without having to worry about the detrimental effects of security settings that exist every 90 minutes.

Note :

There are some adverse effects in setting this value too low, especially if you are using this setting in conjunction with Sysprep images. Please check the settings before executing them on the product.

Security settings in the Domain Controller

There are a number of articles on this topic that describe how Account Policies in GPOs affect domain controllers and internal Security Accounts Manager (SAM) on servers and workstations in the domain. Those settings are unique to the domain controller because the nature of all domain controllers needs to be synchronized with some settings for a wide domain.

The Account Policies are not only a setting that affects domain controllers in this case, but there are several other security settings that can only be applied to the domain root node to influence domain controllers. Next, these settings need the same functionality so that all domain controllers in the domain have one side synchronized and merged when representing the domain. If a client enters a domain controller A and has set X and another workstation to the B controller with Y settings, it can cause significant adverse effects throughout the company.

The settings are applied to all domain controllers through GPOs that link to the domain:

1. Account Policy
2. Network Security: Force logoff when logon hours expire - Catch logout when the login period expires
3. Accounts: Administrator account status - Administrator account status
4. Accounts: Guest account status - Guest account status
5. Accounts: Rename Administrator account - Change the administrator account name
6. Accounts: Rename guest account - Change the guest account name

The remaining points of security settings

Most recently there is a lot of activity around Registry settings and System files in GPOs. These settings are located under the Computer Configuration button as shown in Figure 2.

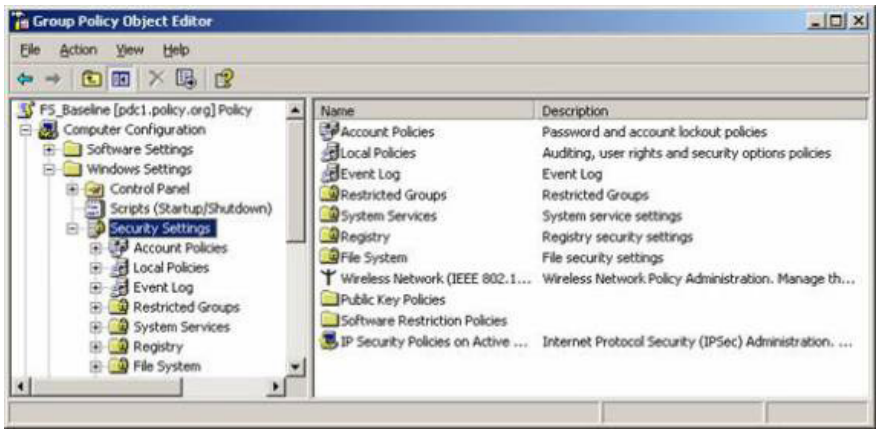

Figure 2: Registry and File System buttons in a GPO can control most Registry Keys or Files

These settings in the GPO can control the permissions of the Registry Key, files or folders. They can be configured simply and perform very efficient tasks. However, the reason for the disadvantage is that they can take a long time to apply. When a computer starts these settings it can take up to several cycles to apply, which causes significant delays for users on their workstations.

Generally these settings need to be used sparingly. Instead of using those settings, it's best to configure this security in the workstation image. Use these policy settings only when you cannot set permissions in the original image or you are in a situation where only a few existing settings are distributed through Group Policy.

Security description during the conversion process

Using GPMC, you can convert GPOs from one domain to another. This is a very useful capability and is often done while moving objects from a test domain to a real product, or between two product domains. In most cases, the settings included in the GPO are 'neutral', meaning they are just a feature switch between 'On' and 'Off'. However, when it comes to security settings, not all settings are as simple as that. There are many security settings based on user accounts or group accounts to target where they apply. Those settings require special attention when making a transition from one domain to another. Because each domain has group accounts and a separate user account needs to be translated. The affected settings include:

1. User rights assignment - Assign user rights
2. Restricted groups - Limited groups

3. Services - Services
4. File system - File system
5. Registry
6. GPO DACL, if you choose to remain in the copy process.

The solution to this problem is to use the Migration Tables conversion table in GPMC as shown in Figure 3.

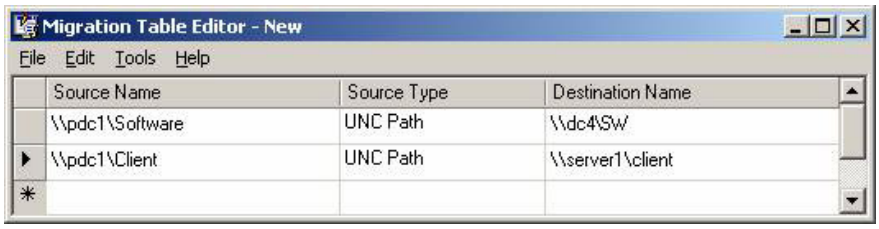

Figure 3: Allowable translation tables for domain GPO conversions

Conclude

Not all GPO settings are created the same as we have seen. When it comes to security settings, this is indeed a complete case. You need to take a closer look and check all security settings before putting them into the product. The best practice here is that security settings should be applied every 16 hours, even without changing the policy settings. That will ensure the reliability and stability in the security of your workstations and servers. For domain controllers, you also need to have a better understanding of where the settings are located and applied, how different domain controllers work on most computers. Finally, when setting up user and group accounts, you must translate from one domain to another with Migration tables. When mastering these security settings, your network will become very secure and stable!