

# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

Group policy is a complex tool that lets you centrally manage Windows 2000 computers and users. But if you don't understand how Win2K applies Group Policy, you can shoot yourself in the foot. You can easily implement a combination of settings that cancel out one another or cause unexpected results. For example, you might think you've enabled an important security setting throughout your network, only to discover you've inadvertently disabled this setting on a subset of systems. This type of mistake can be inconvenient when it involves an administrative setting but can be devastating when it involves a security setting. To effectively use Group Policy, you need to understand how Win2K uses Group Policy Objects (GPOs) to apply policies, the sequence in which Win2K applies GPOs, and the processing options that let you fine-tune GPO application.

## The ABCs of GPOs

A GPO is a collection of configuration settings that cover nearly every area of a Win2K computer's configuration and a user's profile. Each GPO is divided into two subfolders: Computer Configuration and User Configuration. Win2K initially applies the settings in the Computer Configuration subfolder when a computer boots and applies the settings in the User Configuration subfolder when a user logs on. Then, Win2K typically reapplies Group Policy periodically while the computer is up or the user is logged on. You can customize the frequency and conditions under which Win2K applies different types of Group Policy.

Every Win2K computer stores a local GPO. To let you simultaneously manage multiple computers or users, Win2K lets you link other GPOs to Active Directory (AD) containers, such as organizational units (OUs); Win2K then applies the linked GPOs to all the computers or users in those containers. If you link multiple GPOs to a container, Win2K follows specific rules to apply the relevant GPOs in a predictable sequence that facilitates configuration by exception. Configuration by exception lets you define general settings first, then define exceptions— without repeating the general settings— for a subset of computers or users.

## Group Policy Application Sequence

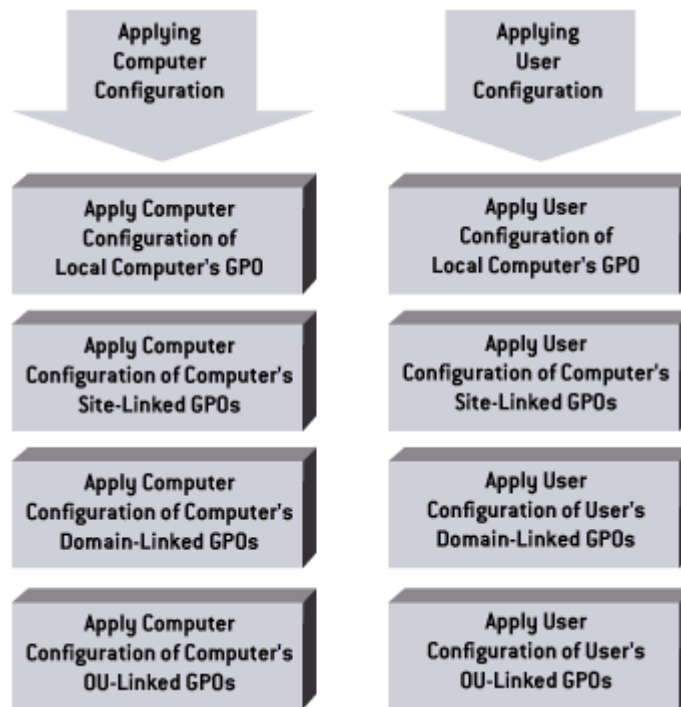
Each GPO has a full complement of computer and user settings. You can specify a value for most GPO settings, or you can leave the settings Not configured (i.e., tell Win2K to take no action). Unconfigured settings tell Win2K not to change existing settings (e.g., settings previously defined in GPOs at another container level) and don't affect configuration.

Multiple GPOs can apply to a computer or user, and some of these GPOs might contain conflicting settings. When several GPOs define a value for the same setting, the last-applied GPO takes precedence. Therefore, you need to understand Win2K's GPO-application sequence, which Figure 1 shows.

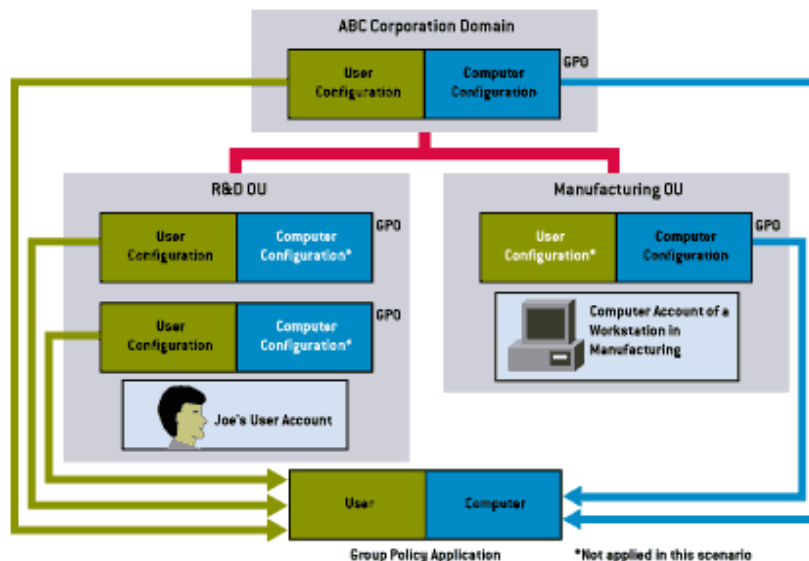
# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)



When a computer boots, Win2K applies the Computer Configuration portion of Group Policy. Win2K first applies the computer's locally stored GPO, then GPOs linked to the computer's site, then GPOs linked to the computer's domain, then GPOs linked to the OUs (in order from highest to lowest) that contain the computer. When a user logs on, Win2K applies the User Configuration portion of Group Policy. The User Configuration application follows the same sequence as the Computer Configuration application, except that Win2K bases domain- and OU-linked GPOs on the user account's domain and branch of the OU tree instead of the computer's location in AD, as Figure 2 shows. The application sequence for User Configuration policies is the locally stored GPO of the computer the user logs on to, then GPOs linked to the computer's site, then GPOs linked to the user's domain, then GPOs linked to the OUs (in order from highest to lowest) that contain the user account. You can view the GPOs that Win2K will apply at each step in the sequence.



# Controlling Group Policy

Randy Franklin Smith

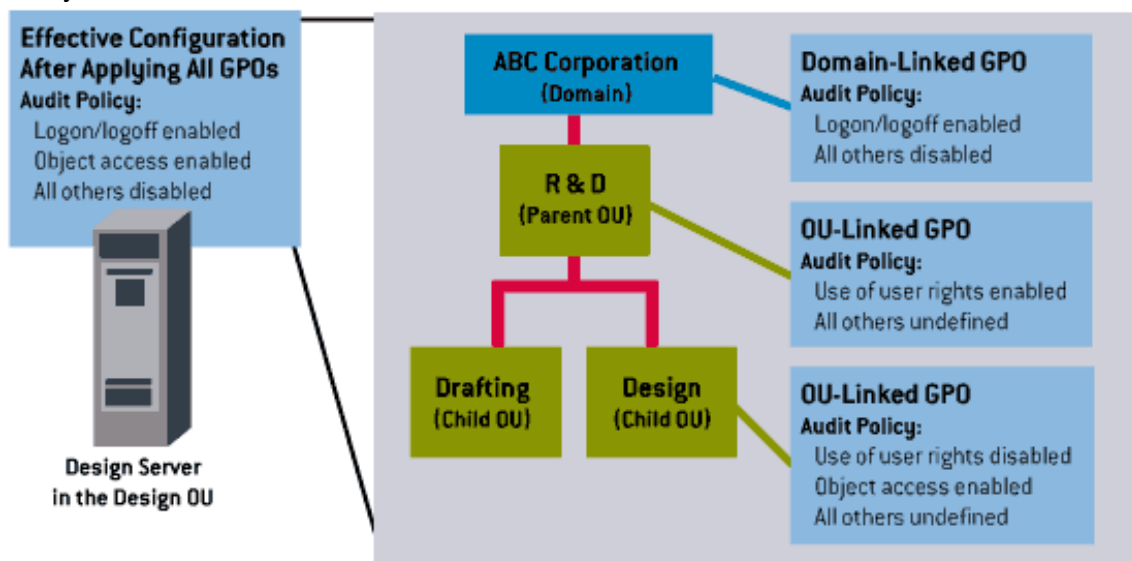
(Reprinted from WindowsItPro Magazine)

Computer's local GPO. Each computer stores one GPO locally. When a computer boots up or a user logs on, Win2K applies the computer's local GPO first. When the computer isn't a member of a domain, Win2K applies only the local GPO, and all its settings take effect. When the computer is a member of a domain, this GPO is the least influential GPO because all AD-linked GPOs that Win2K applies can override the local GPO. To access a computer's local GPO configuration, run mmc.exe from the Win2K Start menu, add the Group Policy snap-in, and select Local Computer.

Site-linked GPOs. When the computer is a member of a domain, Win2K next applies all the GPOs that link to the computer's site. (Sites are AD objects that represent a network's physical layout. For more information about sites, see Sean Deuby, "AD Sites, Part 1," June 2000 and "AD Sites, Part 2," July 2000.) Use site-linked GPOs only when you need to define a setting (e.g., a network parameter) that is specific to the computer's physical portion of your network. To view a list of a site's GPOs, go to Administrative Tools, Active Directory Sites and Services. Right-click a site, click Properties, and select the Group Policy tab. Win2K doesn't come with any prebuilt site-linked GPOs, and administrators seldom define site-linked GPOs.

Domain-linked GPOs. Win2K then applies all the GPOs that link to the computer's—or user's, in the case of User Configuration—domain. Group policies that you define at this level apply to all computers or users in the immediate domain and overwrite site-linked and local GPOs. Unconfigured domain-linked GPO settings don't change defined values in previously configured site-linked GPOs. Domains are the boundary of Group Policy inheritance: Win2K doesn't apply a parent domain's GPOs to a child domain. To view a list of domain-linked GPOs, go to Administrative Tools, Active Directory Users and Computers. Right-click the computer's or user's domain, click Properties, and select the Group Policy tab. Win2K comes with one prebuilt domain-linked GPO: Default Domain Policy.

OU-linked GPOs. Finally, Win2K applies GPOs that link to any OUs that contain the computer—or the user, in the case of User Configuration. If more than one OU contains the computer or user, Win2K applies the linked GPOs in order from the highest OU to the lowest OU. Because the last-applied GPO overrides previously applied GPOs, lower-OU-linked GPOs override higher-OU-linked GPOs whenever both GPOs define a value for the same setting. (Figure 3 shows the configuration settings for a computer in a child OU; Win2K will apply several OU-linked GPOs as well as a domain-linked GPO to the computer.) To view OU-linked GPOs, right-click the OU, click Properties, and select the Group Policy tab.

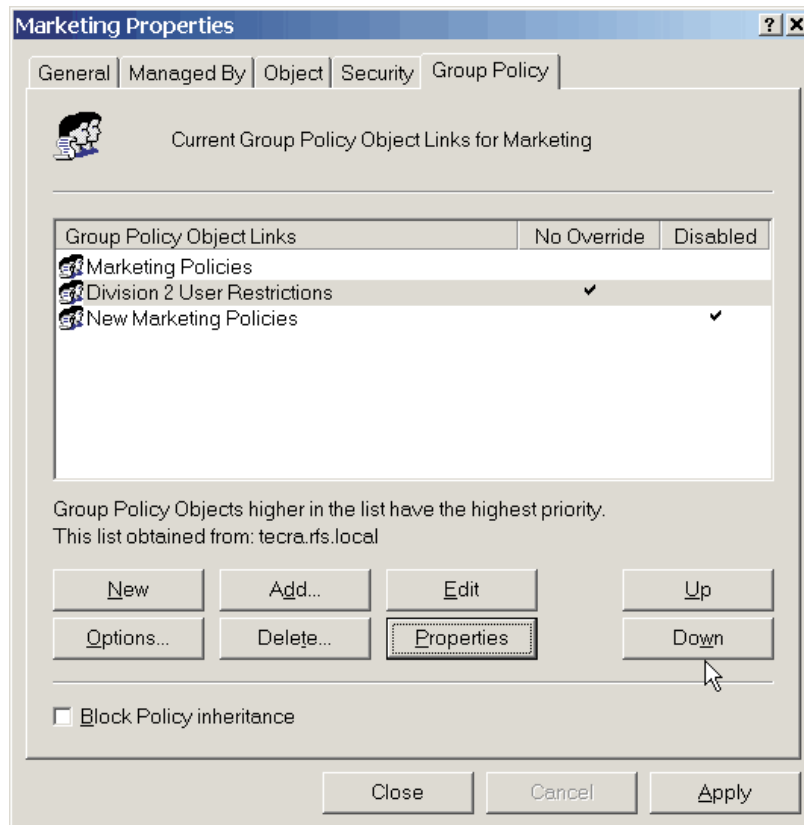


# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

Multiple same-level links. What happens when multiple GPOs link to the same site, domain, or OU? A GPO's relative position in the list of GPO links for the site, domain, or OU determines the GPO's priority; Win2K applies same-level GPOs in order of priority from lowest to highest. (Win2K applies the highest priority GPO last so that the GPO overrides all previously applied GPOs.) Figure 4 shows the Group Policy tab of an example Marketing OU. The New Marketing Policies GPO has the lowest priority, so Win2K applies it first; Win2K applies the Marketing Policies GPO last. To increase or decrease a GPO's priority, use the Group Policy tab's Up and Down buttons to reposition the GPO in the list.



Keep in mind that an important difference exists between a GPO and a link to a GPO. When you delete a GPO, Win2K no longer applies the GPO under any circumstance. When you delete a link, Win2K still applies the GPO to other AD containers to which the GPO is linked. Imagine that a GPO is like a human resources (HR) policy document that you can assign to various departments in your company. When the policy no longer applies to a department, you can remove the document from only that department (i.e., delete the link to the GPO). When the policy is no longer valid on a company basis, you can throw away the document (i.e., delete the GPO). If a department needs to follow the policy but with a few exceptions, you can create an addendum and attach it to the document for that department (i.e., create a second linked GPO, which has higher priority than the original GPO).

Win2K follows a straightforward GPO-application process. Group Policy's true complexity lies in your options for controlling that process, which I'll explain in Part 2 of this series.

In "Controlling Group Policy, Part 1," November 2000, I explained how Windows 2000 uses Group Policy Objects (GPOs) and the sequence in which Win2K applies them. But you can't truly control Group Policy until you understand the processing options that let you fine-tune your policies. Because

# Controlling Group Policy

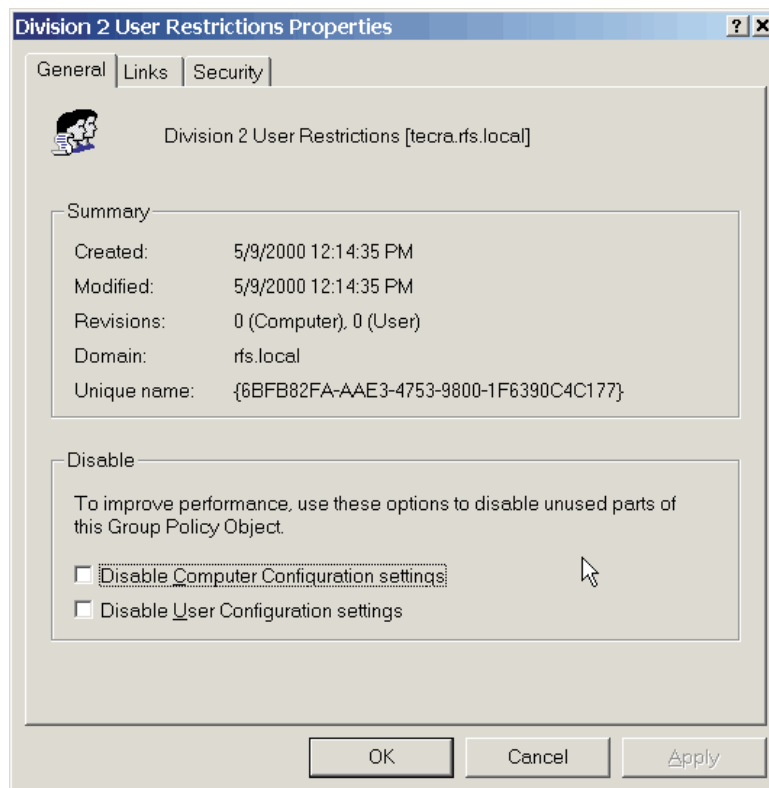
Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

you can link a GPO to sites, domains, or organizational units (OUs), you can control how Win2K applies Group Policy at several levels. You can use GPO-level processing options to control how Win2K applies a GPO regardless of the sites, domains, or OUs to which the GPO is linked. You can use link-level processing options to control how Win2K applies a GPO within a particular site, domain, or OU to which the GPO is linked. Other settings let you tailor how Win2K applies Group Policy at the computer or user level.

## GPO-Level Processing Options

As I explained in "Controlling Group Policy, Part 1," a GPO has settings that affect a Win2K computer's configuration and a user's profile. The GPO stores computer settings in a Computer Configuration subfolder and stores user settings in a User Configuration subfolder. If you create a GPO that contains only computer settings, you can disable the GPO's User Configuration portion to reduce users' logon time. Likewise, if you define only user settings, you can disable the GPO's Computer Configuration portion to reduce system boot-up time. To disable either portion of a GPO, go to Administrative Tools, Active Directory Users and Computers. Right-click the domain or OU to which the GPO is linked, click Properties, and select the Group Policy tab. Select the appropriate GPO, and click Properties. Go to the General tab, which Figure 1 shows, and select either the Disable Computer Configuration settings check box or the Disable User Configuration settings check box. These settings are both GPO-level settings.



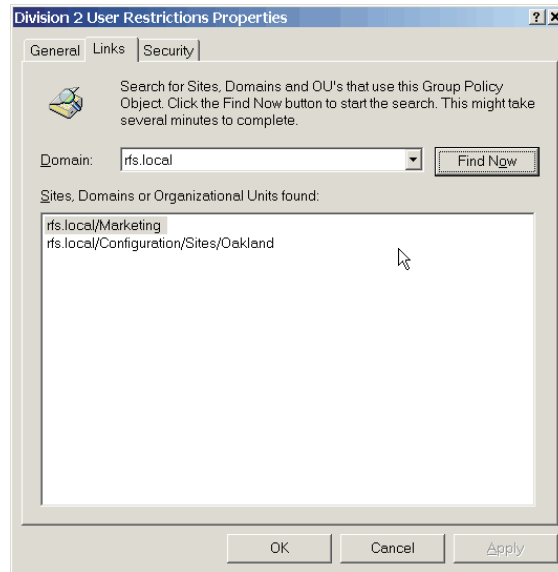
When you disable a GPO's Computer Configuration or User Configuration portion, Win2K disables that portion in every site, domain, or OU to which the GPO is linked. Therefore, before you make this type of GPO-level change, you need to determine how the change will affect those sites, domains, and OUs. To see a complete list of these linked elements, open the GPO's Properties dialog box and go to the Links tab, which Figure 2 shows. Select a domain from the Domain drop-down list and click Find Now. Win2K will search the specified domain and display each site and OU to which the GPO

# Controlling Group Policy

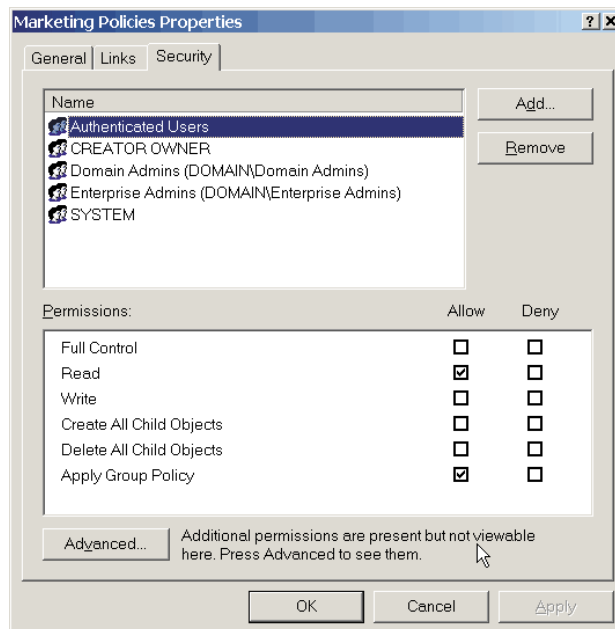
Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

links. (The domain link will also show up on the list if the GPO is linked at the domain level.) Because you can link a GPO to multiple domains, you need to search all the domains that appear in the drop-down list.



One way to fine-tune a GPO's application is through a GPO's ACL, which defines both who has permission to maintain the GPO and which computers and users Win2K applies the GPO to. To access the ACL, open the GPO's Properties dialog box and go to the Security tab, which Figure 3 shows. When a Win2K computer that is a member of a Win2K domain boots up, the computer logs on to Active Directory (AD) and uses its corresponding computer account in AD to look through its domain, sites, and OUs and determine which GPOs it needs to apply. When applying Group Policy to a computer, Win2K determines whether the computer account has permissions to read and to apply Group Policy for each GPO. If not, Win2K ignores the GPO for that computer. User accounts also require both Read and Apply Group Policy access; Win2K goes through the same determination process each time a user logs on and whenever Win2K reapplies Group Policy.



# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

As Figure 3 shows, Authenticated Users (i.e., all computer and user accounts) have both permissions by default. When you want to disable a GPO's application to specific computers or users in an OU, you can open the GPO's ACL and add an access-control entry that denies Apply Group Policy access for the groups or accounts that you want to exempt. To view a GPO, you need Read access; to edit a GPO, you need Write access.

## Link-Level Processing Options

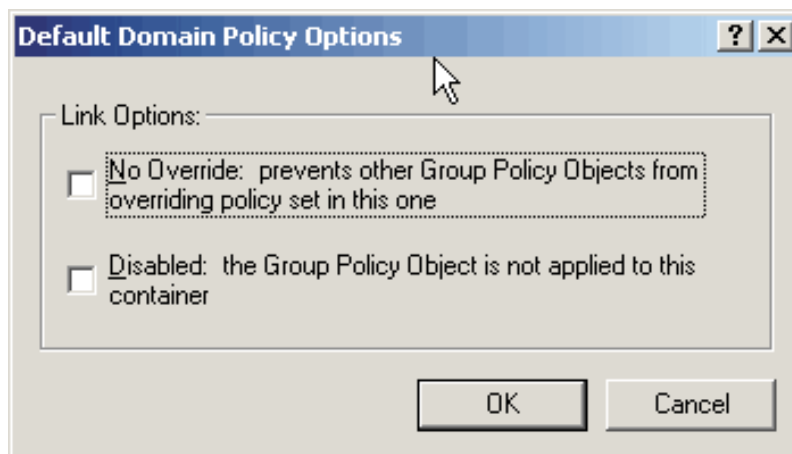
An important difference exists between a GPO-level processing option and a GPO-link-level processing option. Whereas GPO-level processing options apply to all sites, domains, or OUs to which the GPO is linked, link-level processing options apply to only the immediate site, domain, or OU to which the GPO is linked. (A difference also exists between deleting a GPO and deleting a link to the GPO. When you select a GPO from the Group Policy tab and click Delete, Win2K asks whether you want to delete the entire GPO or only the link. When you delete the GPO, it disappears from every site, domain, or OU to which it is linked. When you delete the link, the other sites, domains, or OUs to which the GPO is linked remain unaffected.) You can choose among three link-level processing options.

## Block Policy Inheritance

Administrators use this option to isolate domains or OUs from group policies defined for a site or higher-level OU. When you select the Block Policy inheritance check box on the Group Policy tab, you effectively erect a gate above that domain or OU that blocks GPOs from trickling down. When you block policy inheritance at the domain level, Win2K won't apply any site-linked GPOs. When you block policy inheritance at the OU level, Win2K won't apply domain- or higher-OU-linked GPOs for computers or users in that OU. However, remember that Win2K always applies the computer's local GPO regardless of the Block Policy inheritance setting.

## No Override

Administrators typically enable this setting at a domain level to enforce corporate password and account policies. The No Override setting overrides all lower-level Block Policy inheritance settings. For example, when you enable No Override for a site-level GPO link, Win2K applies that GPO to all computers in the site, regardless of the domain's or OU's Block Policy inheritance setting. When you enable No Override for a domain- or OU-level GPO link, Win2K applies that GPO to all computers and users, regardless of any lower OUs' Block Policy inheritance settings. To enable or disable the No Override setting, select the appropriate GPO from the Group Policy tab and click Options. Select the No Override check box, which Figure 4 shows.



# Controlling Group Policy

Randy Franklin Smith

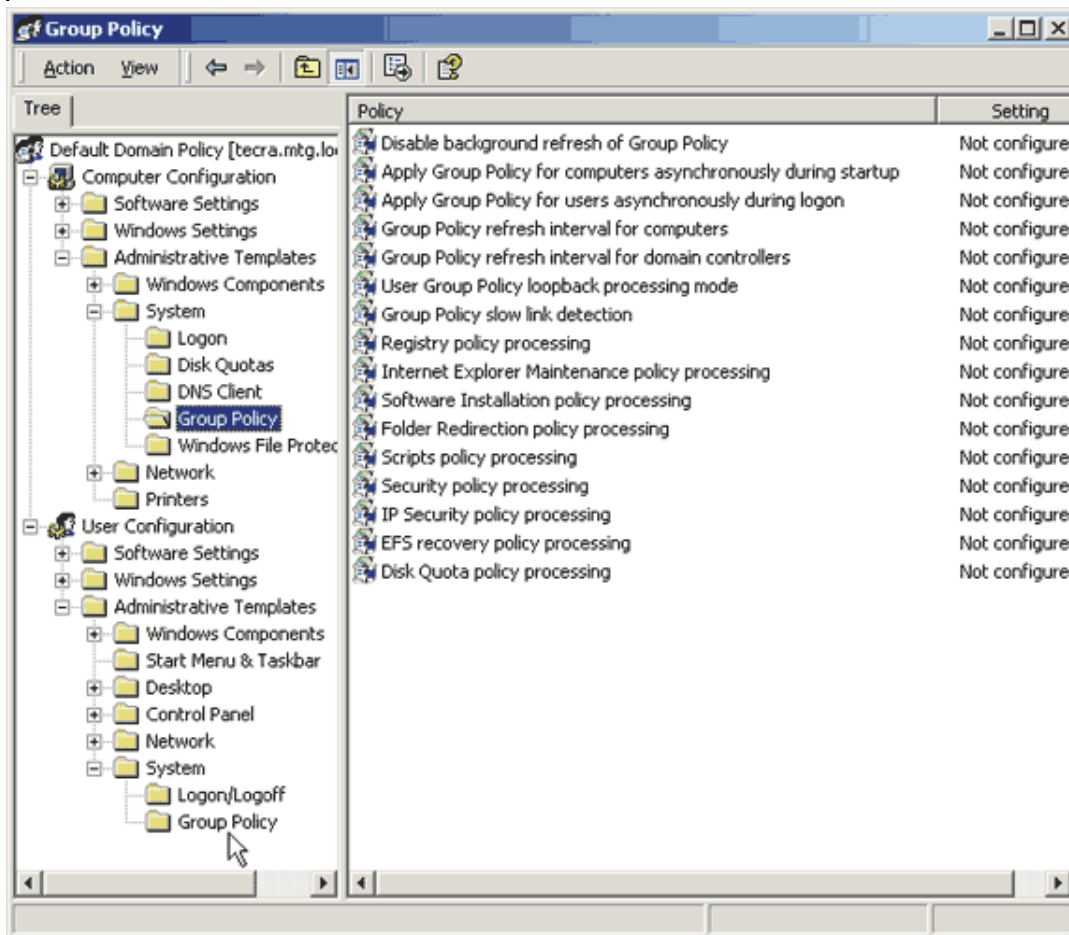
(Reprinted from WindowsItPro Magazine)

## Disabled

Disabling a GPO link is useful when you need to temporarily eliminate the GPO's effect on configuration (e.g., while debugging policy or temporarily suspending a restriction). When you disable a GPO link to a site, domain, or OU, Win2K won't apply the GPO to that site, domain, or OU. By disabling rather than deleting the link, you can more easily reinstate the GPO. To change the Disabled setting for a GPO link, select the appropriate GPO from the Group Policy tab and click Options. Select the Disabled check box, which Figure 4 shows.

## System- and User-Level Processing Options

Another set of processing options exists as settings within each GPO; you define these settings at the system or user level. As I explained in "Controlling Group Policy, Part 1," each GPO contains a Computer Configuration subfolder and a User Configuration subfolder; in other words, each GPO has a Group Policy folder under \computer configuration\administrative templates\system and another folder under \user configuration\administrative templates\system, as Figure 5 shows. These folders contain settings that control how Win2K applies Group Policy to every computer and user that links to that GPO.



Changing the Computer Configuration settings for one GPO can affect a system's application of all GPOs. For example, suppose you go to the Marketing OU, create a new GPO, and select the Disable background refresh of Group Policy system-level setting. The next time a computer in that OU boots up or refreshes, the system will encounter the new GPO and change the setting in the local system

# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

configuration. After making the change, the system will disable background refresh of every GPO, not only of the GPO for which you enabled the setting.

## Disable Background Refresh of Group Policy

Win2K periodically reapplies Group Policy after the initial system boot-up or user logon. The Disable background refresh of Group Policy setting disables this reapplication while a user is logged on to the system. The setting applies to policies under both the Computer Configuration and User Configuration portions of a GPO.

## Group Policy Refresh Interval for Computers

This setting controls the frequency at which Win2K refreshes Group Policy for Win2K Professional workstations and Win2K member servers (not for domain controllers). You can use this setting to specify two thresholds: the number of minutes between refreshes and an offset that Win2K uses to prevent every computer from simultaneously rereading Group Policy from the domain controller. Win2K computes a random value between zero and the offset, then adds this value to the first threshold after each refresh to determine when the next refresh will occur. By default, Win2K refreshes every 90 minutes and specifies a maximum offset of 30 minutes. The setting applies to policies under the Computer Configuration portion of a GPO.

## Group Policy Refresh Interval for Users

Similar to the Group Policy refresh interval for computers setting, Group Policy refresh interval for users controls how frequently Win2K refreshes User Configuration. The setting applies to policies under the User Configuration portion of a GPO.

## Apply Group Policy for Computers Asynchronously During Startup

By default, a Win2K system won't present the logon prompt until Win2K finishes applying Group Policy. When you enable the Apply Group Policy for computers asynchronously during startup setting, Win2K lets users log on before Group Policy application is complete. The system displays the message Applying computer settings until application is complete. Although enabling this setting doesn't usually cause problems, some policies might not take effect until the next time Win2K applies or reapplies Group Policy. This setting applies to policies under the Computer Configuration portion of a GPO.

## Apply Group Policy for Users Asynchronously During Logon

By default, after a user enters a username and password, Win2K doesn't display the user's desktop until it finishes applying Group Policy's User Configuration settings. When you enable the Apply Group Policy for users asynchronously during logon setting, users can access the Start menu and desktop before the application is complete. Some policies might not take effect until the next logon or until Win2K refreshes Group Policy. This setting applies to policies under the User Configuration portion of a GPO.

Unless users complain about excessive startup or logon times, I recommend you leave both asynchronous-application settings disabled so that you can maintain predictable Group Policy application.

## User Group Policy Loopback Processing Mode

When Win2K applies the User Configuration portion of Group Policy, Win2K determines the applicable GPOs based on the user's domain and OUs and applies settings from the User Configuration portion of those GPOs. In other words, Win2K applies User Configuration settings based on the user account's location in AD (i.e., who the user is), not based on the computer

# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

account's location (i.e., which computer the user is logging on to). However, you might decide to make an exception to this rule. For example, perhaps you have public-use kiosks for which you want to define specific User Configuration settings regardless of who logs on. In such a situation, you need to create an OU to contain the kiosks, then create an OU-linked GPO and enable the GPO's User Group Policy loopback processing mode setting. When you enable this setting, you must select one of two option modes. Replace mode tells Win2K to ignore the user's User Configuration settings (i.e., the User Configuration settings based on the user account's location in AD) and instead apply the system's User Configuration settings (i.e., the User Configuration settings based on the system's location in AD). Merge mode tells Win2K to first apply the user's User Configuration settings, then apply the system's User Configuration settings. Whenever a conflict occurs, the system's settings take precedence.

## Group Policy Slow Link Detection

This setting lets you specify the threshold (in Kbps) for slow network links. The default threshold is 500Kbps. Win2K uses this threshold to determine when to defer Group Policy application.

## Deferring Group Policy Application

Win2K divides Group Policy into nine processing categories: Registry, Internet Explorer (IE) Maintenance, Software Installation, Folder Redirection, Scripts, Security, IP Security (IPSec), Encrypting File System (EFS) recovery, and Disk Quota. Each category has a corresponding Group Policy option (e.g., Registry policy processing) that resides in `\computer configuration\administrativetemplates\system\group policy`, as Figure 5 shows.

You can defer a category's Group Policy application to prevent slowdowns on the workstation while Win2K applies Group Policy. You can also defer application to prevent sudden changes that can occur on a user's desktop when you implement Desktop or Start Menu & Taskbar restrictions (e.g., disable the Screen Saver tab in Control Panel, Display; remove the Map Network Drive option in Windows Explorer) while the user is logged on. (These restrictions reside in `\user configuration\administrative templates`.) To control a category, right-click the corresponding option under `\computerconfiguration\administrative templates\system\group policy` and select Properties. Select Enabled, then select one or more of the following scenario check boxes.

Allow processing across a slow network connection. Select this option to permit processing while the computer is connected to the domain controller on a slow network link (according to the definition you set using the Group Policy slow link detection setting). Notice that to defer processing, you must clear the check box.

Do not apply during periodic background processing. Select this option to defer processing during background refreshes while a user is logged on. This option defers refreshes in specific categories, whereas Disable background refresh of Group Policy defers refreshes in all categories.

Process even if the Group Policy objects have not changed. This option lets you control whether Win2K applies certain categories even though the policies haven't changed. For example, you can use this option to tell Win2K to regularly reapply a category in case users have disabled restrictions that you implemented through Group Policy. To defer application, clear the check box.

Table 1 lists each category and its corresponding Group Policy option, shows the location of the policies for which the category controls application, and identifies which of the three processing situations you can defer each category in.

# Controlling Group Policy

Randy Franklin Smith

(Reprinted from WindowsItPro Magazine)

TABLE 1: Group Policy Processing Categories

Category	Group Policy Option	Policies in Category	Control Processing During Slow Links	Control Processing During Backward Refreshes	Control Processing to Reapply Policies Even When They Haven't Changed
Registry	Registry policy processing	All policies in \administrative templates; any other policies that are stored as values in the Registry	No	Yes	Yes
IE Maintenance	Internet Explorer Maintenance policy processing	All policies in \computer configuration\windows settings\internet explorer maintenance	Yes	Yes	Yes
Software Installation	Software Installation policy processing	All policies in \computer configuration\software settings\software installation	Yes	No	Yes
Folder Redirection	Folder Redirection policy processing	All policies in \computer configuration\windows settings\folder redirection	Yes	No	Yes
Scripts	Scripts policy processing	All policies in \computer configuration\windows settings\scripts	Yes	Yes	Yes
Security	Security policy processing	All policies in \computer configuration\windows settings\security settings	No	Yes	Yes
IPSec	IP Security policy processing	All policies in \computer configuration\windows settings\security settings\ip security policies	Yes	Yes	Yes
EFS recovery	EFS recovery policy processing	Encryption settings under \computer configuration\windows settings\security	Yes	Yes	Yes
Disk Quota	Disk Quota policy processing	All policies in \computer configuration\administrative templates\system\file system\disk quotas	Yes	Yes	Yes

## One-Stop Shopping

Group Policy provides one-stop shopping for computer and user profile configuration. To keep a handle on Group Policy complications, you need to minimize your use of settings such as No Override and Block Policy inheritance and customize GPO ACLs only when absolutely necessary. To keep Group Policy simple, use options that are visible on the GPO Properties, Group Policy tab. To control who receives which policies, use OUs, rather than GPO permission restrictions; resort to restrictions only for troublesome exceptions that would otherwise require you to completely redesign your OU hierarchy.