

Creating Group Policies: Step by Step

In Chapter 1 of this book, I explained Group Policy Objects (GPOs) and what capabilities they provide. Chapter 2 dissected the structure of GPOs and their interaction with Active Directory (AD). In this chapter, I'll take you through the next step—the details and process of creating and maintaining GPOs. As I hope you've gleaned by reading the first two chapters, GPOs are considerably more complex than the old NT 4.0 system policies.

My focus in this chapter is on creating GPOs in an AD environment. Local GPOs can be interesting and useful in certain situations and when you don't have an AD infrastructure, but where the real power (and complexity) lies is in AD-based GPOs. To that end, I'll use Chapter 4 to talk about real-life considerations for designing a GPO implementation for your enterprise. However, first things first—let's dive into the details of creating and maintaining GPOs.

Creating AD-Based GPOs

In Chapter 1, I introduced the Microsoft Management Console (MMC)–based Group Policy snap-in. This tool is your primary (and, indeed, only) interface for creating and editing GPOs. So this is where I'm going to start. Let's suppose you want to create a GPO linked to a domain called mycompany.com. The first thing you need to do is start the AD Users and Computers MMC tool. If you're creating a GPO that is linked to an AD site object, you'll need to start the AD Sites and Services MMC snap-in instead.

 If you don't have the AD Users and Computers or AD Sites and Services MMC console tools installed on your Win2K workstation, you can install them by locating the .msi file called adminpak.msi, located in the i386 folder on the Windows 2000 Server CD. Installing this file will install all the Win2K server administration snap-ins on your workstation.

To begin, you need to ensure that you're logged in to your AD domain with a user ID that is capable of creating GPOs. I'll talk more about GPO security later in this chapter (see “Security Settings”) and in Chapter 5, but to create (and edit) a GPO in a default AD installation, you need to be a member of one of the following groups:

- ∉ Domain Admins (Global Group)
- ∉ Administrators (Domain Local Group)
- ∉ Enterprise Admins (Global Group)
- ∉ Group Policy Creator Owners (Global Group)

When the AD Users and Computers MMC tool loads, it'll focus on the domain to which the workstation or server from where you're running the tool belongs. So, if you're running the tool from a workstation that is a member of the mycompany.com domain, the tool will be focused on that domain when it starts. To create a GPO linked to a domain, right-click the domain name listed at the top of the left-hand pane in the MMC tool. My example shows mycompany.com.

Choose Properties from the context menu, then in the Properties dialog box click the Group Policy tab to see the Group Policy page, shown in Figure 3.1.

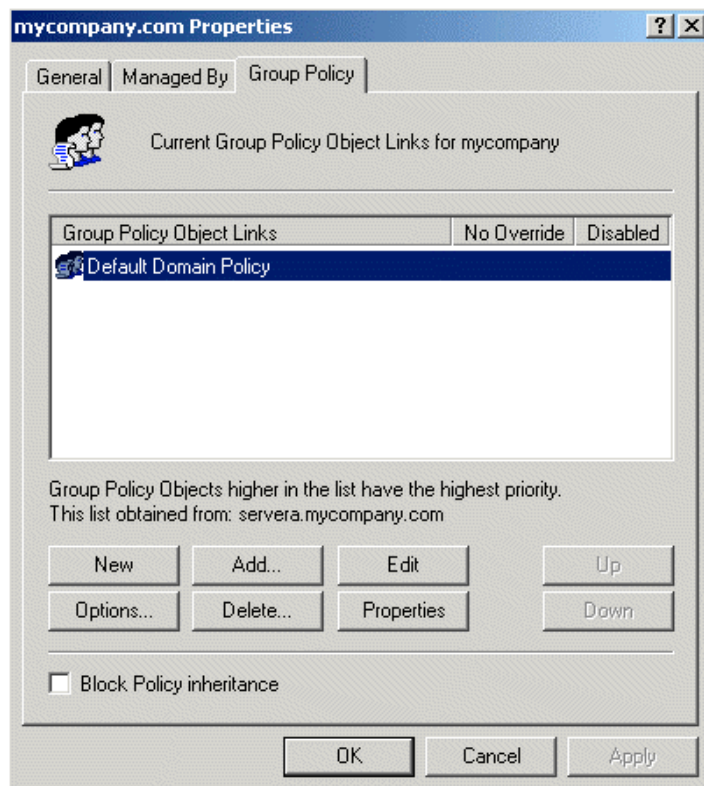


Figure 3.1: Viewing the Group Policy page for the domain properties in the AD Users and Computers MMC snap-in.

The view you see in Figure 3.1 shows you the GPOs that are currently linked to the mycompany.com domain—in this case, it's just the Default Domain Policy. The Default Domain Policy is a special GPO in AD. This policy exists in all default AD installations and in fact can't be deleted by normal means. If you attempt to delete this GPO using the Group Policy snap-in, your request will appear to succeed, but the GPO won't actually be removed.

This is because this GPO serves a special function—namely, guaranteeing that there is always a way of defining domain security policy, irrespective of whether you're using GPOs for any other purpose. Remember from Chapter 1 that one of the key features of the GPO is security configuration management. And, in particular, domain account policy can only be defined in a GPO linked at the domain level. The persistence of the Default Domain Policy guarantees that there is always a way of defining account policy on a domain.

In my example, I'm going to create a GPO, linked to the mycompany.com domain, called Test GPO. To create a GPO, I simply click New on the Group Policy page. A GPO is created with the temporary name New Group Policy Object. Now I'm free to edit the name to something more meaningful for my installation.

When I click New, two operations are happening behind the scenes. First, the physical GPO is created in AD and the SYSVOL share, (For more information on the physical structure of GPOs, see Chapter 2.) Then a link is created between the GPO and the domain. As you saw in Chapter

2, the link is really an AD attribute on the object—domain, site, or Organizational Unit (OU)—that you’re linking to. When these steps are complete, you have a fully functional GPO. And by fully functional, I mean that from that moment forward, your GPO is live and can be processed by any user or computer in the domain with permissions to do so.

 Later in this chapter, I'll show you how you can create a GPO without actually linking it to an AD object. This technique comes in handy if you're creating GPOs that you don't want users or computers to process right away.

Of course, the important part, editing the GPO to set up your management functionality, is the next step.

Editing GPOs

Once you’ve created the GPO, you can turn to the task of editing it. In the Properties dialog box where you created the GPO, select your new GPO and click Edit. At that point, an instance of the Group Policy MMC snap-in opens in a separate MMC console, focused on the new GPO. As you can see, the familiar Group Policy editor interface, as described in Chapter 1, is presented here. Remember that GPOs break configuration information into computer and user nodes. Under each node is the functionality that is available.

To illustrate the editing process, I’ll walk through setting up some security policy on my Test GPO. Let’s suppose that I want to set up auditing policy for all computers in the domain mycompany.com. Because Test GPO is linked to the domain, all computers that are members of the mycompany.com domain will process this GPO.

 GPOs linked to a domain are processed by all computers and users in that domain. The exception to this rule is that you can filter the processing of GPOs using AD security groups. I'll talk more about security-group filtering later in this chapter (see “Security Settings”).

To set up auditing policy, I need to drill into the Computer Configuration section of the GPO under Windows Settings|Security Settings|Local Policies. Figure 3.2 shows where Audit Policy is located in a GPO.



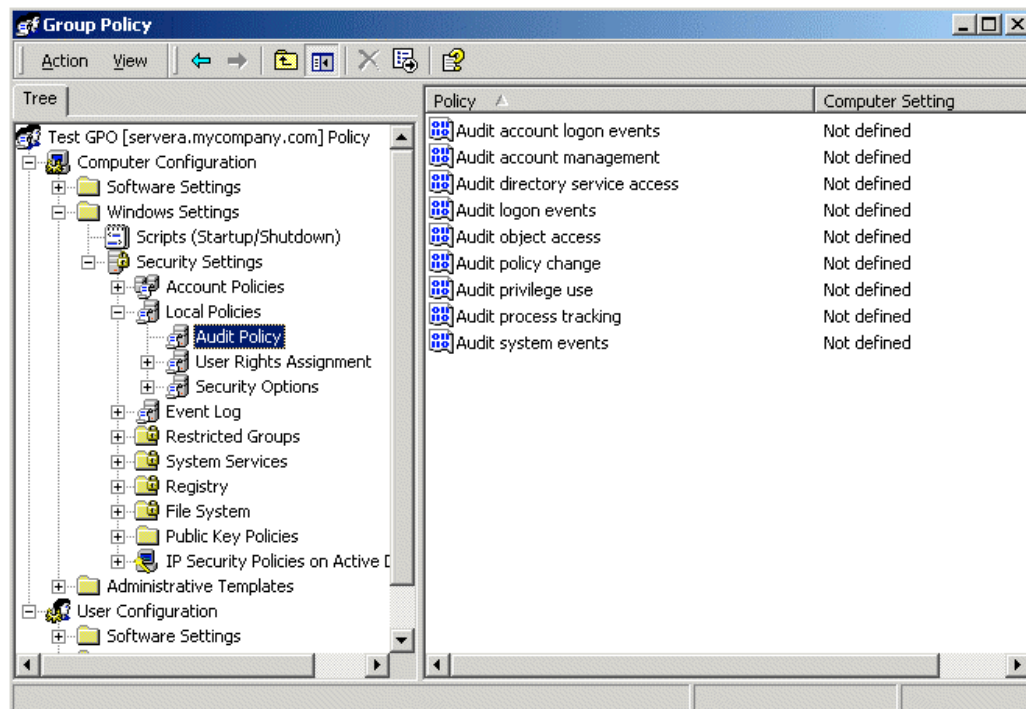


Figure 3.2: Viewing Audit Policy in the Computer Configuration section of a GPO.

As you can see in the right-hand pane in this figure, you can set a number of audit categories. For example, setting Audit Account Logon Events to log success events tells any Win2K computer subject to this GPO to create entries in the security event log any time a user successfully logs onto that account. Domain controllers ignore local policy (for example, auditing policy) set at the domain level in favor of local policy defined in the Default Domain Controllers Policy GPO. However, you can set local policy in a domain-linked GPO for processing by workstations and member servers in the domain. To set auditing policy, simply double-click the policy item of interest in the right-hand pane of the Group Policy console. You'll be presented with the Security Policy Setting dialog box, like that shown in Figure 3.3.

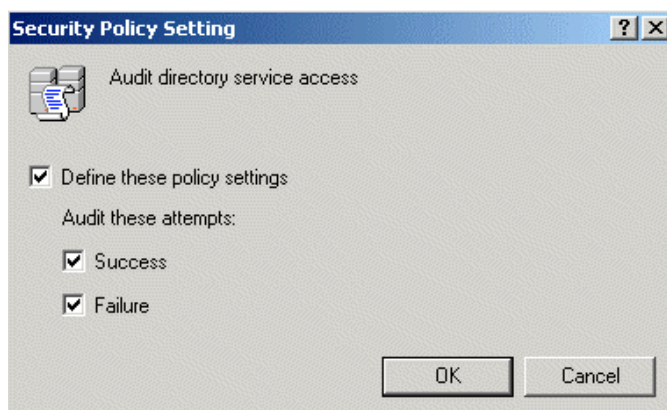


Figure 3.3: Viewing options available when setting auditing policy.

As shown in Figure 3.3, you enable auditing policy by clicking the Define These Policy Settings check box, then choosing to log success events and/or failure events. Specifying success events indicates that you want to generate a security event log entry every time an operation of the chosen type succeeds. For example, in Figure 3.3, I'm enabling auditing of directory service access. Whenever someone successfully accesses AD on a particular domain controller, a success event is registered in the security event log. Likewise, if you specify failure events, when someone attempts to access AD and is denied access for whatever reason, a failure event is logged on that domain controller.

When you click OK in the Security Policy Setting dialog box, your change is immediately committed to the GPO and is available for processing. This example explains editing just one section of a GPO. I'll spend more time later in this chapter detailing how you can set policy on some of the other GPO nodes of functionality.

Setting GPO Options

In addition to making basic edits to a GPO to set the policy's functionality, you have a couple of options that you can set on the GPO to further control its effect. On the Group Policy page of the Properties dialog box shown in Figure 3.1, you'll notice the Options button. Clicking Options displays the Test GPO Options dialog box, shown in Figure 3.4.

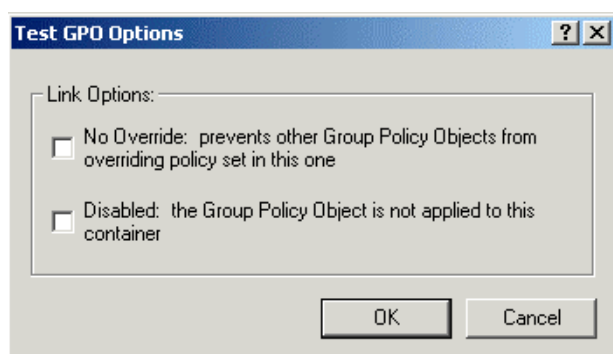


Figure 3.4: Viewing the options settings available on a GPO.

The two check boxes in this dialog box allow you to set the No Override and Disabled options on a GPO.

No Override

When you click the No Override check box, an attribute is set on the container object in AD where this GPO is linked. This attribute, introduced in Chapter 2, is called gPLink. For example, if my Test GPO is linked at the domain level, gPLink is defined on the domain object called mycompany.com in my AD. This object is viewable using the ADSI Edit tool introduced in previous chapters. Setting the No Override option for a GPO linked to a container modifies the gPLink attribute on that container.

Normally, the gPLink attribute on a container contains a bracket ([])-delimited list of the GPOs that are linked to it. The GPOs are referred to by their Lightweight Directory Access Protocol (LDAP) distinguished names (DNs)—as described in Chapter 2. An example is shown here:

LDAP://CN={BB8724E4-8BD8-4C31-BA12-EA7E69246D16},CN=Policies,CN=System,DC=mycompany,DC=com

The gPLink attribute contains a list of these LDAP distinguished names, with an option flag tacked onto the end of each GPO referenced. If No Override is enabled, this option flag is set to the value 2, as shown in Figure 3.5. (A normal GPO linked to a container without No Override enabled will have a value of 0.)

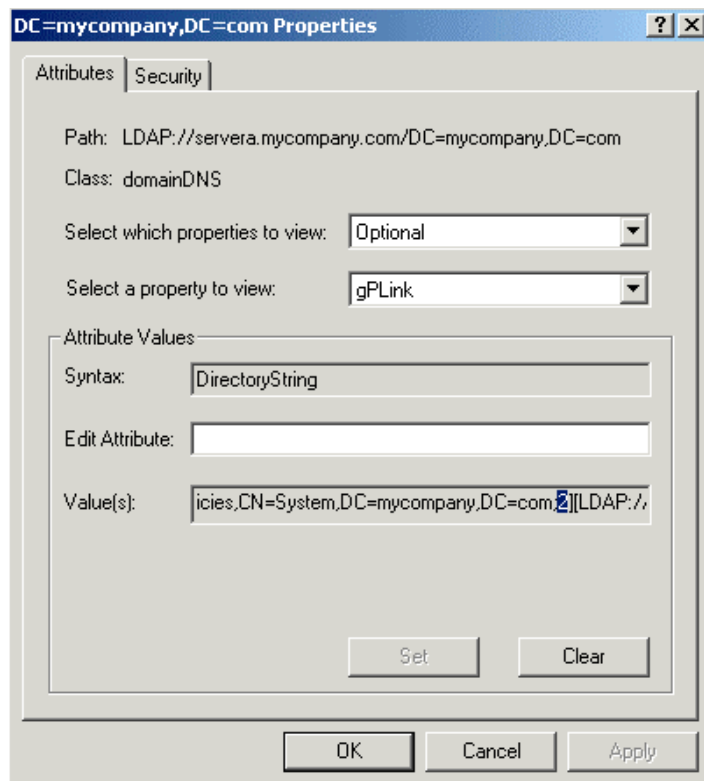


Figure 3.5: Enabling No Override on the gPLink attribute for a linked GPO.

The gPLink value for a GPO with No Override enabled looks like the following:

```
[LDAP://CN={BB8724E4-8BD8-4C31-BA12-EA7E69246D16},CN=Policies,CN=System,DC=mycompany,DC=com;2]
```

Because No Override is set at the gPLink level, a GPO can be linked to, say, a domain, and be set to No Override. However, the same GPO can also be linked to an OU in that domain without No Override being set on that OU. The point here is that the No Override feature is set at the container GPO link level rather than as an option in the GPO itself.

So now that we know what gets set in AD when No Override is enabled, what does this feature actually do? No Override enforces a particular GPO's settings that could otherwise be nullified by another GPO that is processed afterwards. For example, suppose I've defined an Administrative Template policy that has been linked at the domain level in my AD domain. This policy performs a particular desktop lockdown that I want to enforce across all users in my domain.

Now suppose an administrator who manages an OU in my domain creates a GPO that sets a contradictory Administrative Template policy to mine and links that GPO to his OU. Normal

GPO processing precedence, if you'll remember from Chapter 1, is: local, site-linked, domain-linked, and OU-linked. This means that the OU administrator's OU-linked GPO will process last and override my own domain-linked GPO. By setting No Override as an option on my domain-linked GPO, I prevent that from happening—the OU-based GPO settings for Administrative Template lockdown are simply ignored.

It's important to note that No Override is implemented at the client-side extension (CSE) level. That is, if I set No Override on a GPO linked to my domain, and only define Administrative Template settings in that domain GPO, other settings defined by OU-linked GPOs, such as local security policy or software installation settings, won't be overridden by my domain-linked policy. If, after I create my domain-linked GPO, I decide to edit that GPO to add a software installation policy, the No Override option will kick in and override any software installation policy defined on the OU-linked GPO.

Disabled

The other GPO option that you can set is called Disabled. This option is again specific to the container to which the GPO is linked. And as with No Override, Disabled is implemented by setting the value at the end of the LDAP distinguished name for a particular GPO contained in the gPLink attribute. As I mentioned, No Override sets this value to 2. Clicking Disabled sets this value to 1.

 If you set both No Override and Disabled for a GPO link, the value placed in the **gPLink** attribute for that GPO will be 3.

The Disabled option does just as its name implies: It disables the GPO linked to the particular container (for example, site, domain, or OU). A disabled GPO link is no longer processed by computers or users who are subject to it. In addition, if a GPO link is disabled, any settings that had previously been enforced by that GPO are supposed to be undone during the next processing cycle by the computers subjected to it.

I say “supposed to” because I've experienced situations where this was not the case. Specifically, after I implemented the Folder Redirection feature in a GPO, disabling that GPO didn't undo Folder Redirection. I've reproduced this reliably and suggest that you test this in your own environment before making assumptions about what the Disabled option can do for you.

 You can also access the No Override and Disabled options by right-clicking the name of the GPO in the GPO Properties dialog box on a given container. For example, on the Group Policy page (see Figure 3.1), if I right-click Test GPO, I get a context menu with the No Override and Disabled options at the top. Choosing one has the same effect as clicking the corresponding check box in the Test GPO Options dialog box (see Figure 3.4).



Blocking Policy Inheritance

Refer again to Figure 3.1 and notice the Block Policy Inheritance check box. As you know, GPOs are processed using a particular order of precedence. You often see this order represented by the acronym *LSDOU* (Local, Site, Domain, OU). First the local GPO (LGPO) is processed, then any GPOs linked at the site, domain, or OU levels are processed in turn. If a workstation or

user is defined in a nested OU hierarchy (for example, the workstation or user is part of the Accounting OU, which is part of the Finance OU, which is part of the US-Corp OU), that workstation or user may be processing any number of GPOs linked at each level of the hierarchy.

Normally, GPOs are inherited. This means that GPOs linked to a domain are automatically processed by all computers and users in that domain. Those GPOs linked to a parent OU are processed by all computers and users who are a member of that OU as well as in nested OUs. This is called *policy inheritance*, and it can be turned off at either the domain or OU level by clicking the Block Policy Inheritance check box shown in Figure 3.1. (Policy inheritance can't be turned off at the site level: site GPOs are always processed first and can't be nested within each other.)

You block policy inheritance at the container level (that is, at the domain or OU level). Blocking policy inheritance at the domain level means that any site-linked GPOs are ignored by users or computers processing GPOs. Blocking policy inheritance at the OU level means that site, domain, and any higher-level OU-linked GPOs are ignored. Figure 3.6 illustrates how blocking policy inheritance works.



Figure 3.6: Blocking policy inheritance in an AD domain.

In this figure, a number of GPOs are defined at the domain, site, and OU levels. When we block policy inheritance on the Accounting OU, not all “upstream” GPOs are processed by users and computers defined in Accounting. Only the Accounting OU GPO is processed.

You block policy inheritance by setting an attribute on the container where you set this feature. Using the ADSI Edit MMC snap-in, right-click the container object in the console, then choose Properties from the context menu. In the Properties dialog box, click the Attributes tab. When block policy inheritance is enabled, the gPOptions attribute is set to 1; when it's not, it's set to 0. Figure 3.7 illustrates setting this value.

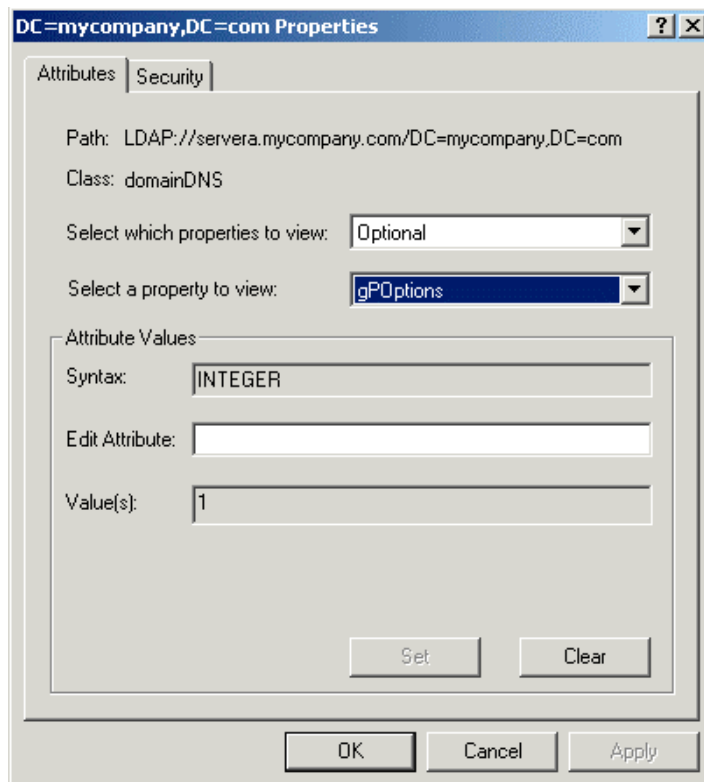


Figure 3.7: Viewing the gPOptions attribute set on an AD container (domain or OU) object.

There is one exception to how the block policy inheritance feature is used. If an administrator for a higher-level container (site, domain, or parent OU) specifies that a linked GPO supports the No Override option (see “No Override” earlier in this chapter), that GPO cannot be blocked by a downstream container. This allows an administrator at, for example, the domain level to make sure that a particular policy is enforced regardless of what a downstream administrator may attempt to do.

Preventing a downstream container from being blocked is useful for enforcing policy related to security or desktop lockdown, and it may be corporate policy for all company computers. For example, I use No Override in a GPO linked to my domain to enforce a particular set of event log settings on all computers that are part of my domain. This guarantees that all computers have event logs of sufficient size and rollover behavior to capture system, application, and security events that I’m interested in.

Setting GPO Properties

Another button on the Group Policy page of the Properties dialog box shown in Figure 3.1 is Properties. Clicking Properties displays the Test GPO Properties dialog box, shown in Figure 3.8. This dialog box lets you set three types of properties—general, links, and security.

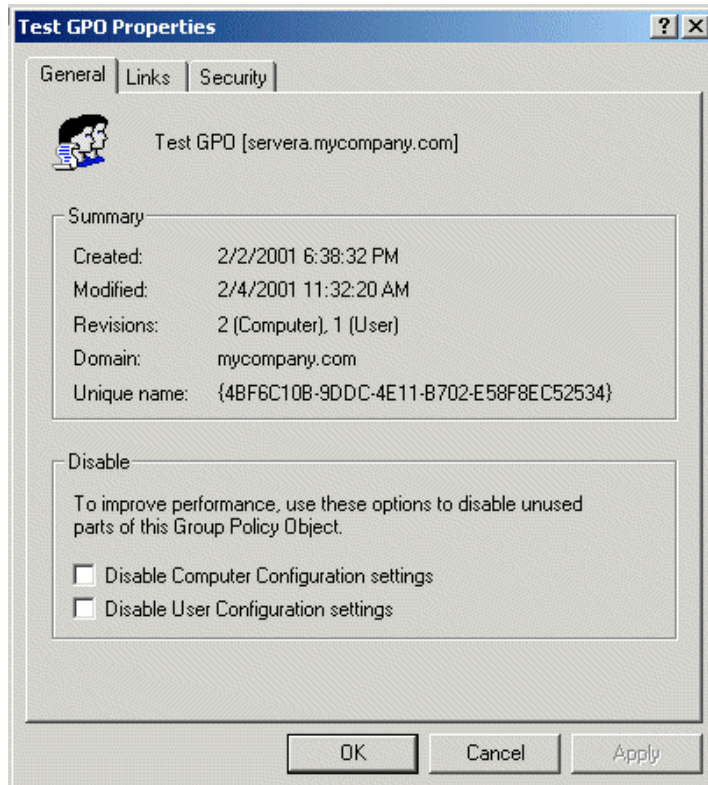


Figure 3.8: Viewing the GPO Properties dialog box.

General

The General page, shown in Figure 3.8, lets you view general information about a GPO and also lets you disable either computer or user settings in the GPO. Chapter 2 describes most of the information on this page, including the Globally Unique ID (GUID) for this GPO, its version number, and domain.

The two check boxes, which were also described briefly in Chapter 2, let you disable one or both sides of GPO processing in this specific GPO. These settings are GPO-specific. This means that if this GPO is linked to multiple sites, domains, or OUs, clicking one of these check boxes will have an impact on them all. This feature lets you optimize the performance of GPO processing in cases where a GPO may only be using part of its total policy functionality.

For example, if I've defined a GPO that only processes user-based software installation policy, I might want to click the Disable Computer Configuration Settings check box. This tells the CSE on a Win2K device that is processing this GPO to simply ignore any computer-specific CSE processing because none is set. (Even if they're defined, they won't be processed.) This can have the effect of speeding the processing of GPOs in cases where a user or computer must process

many GPOs on logon or startup. I'll talk more about designing a GPO implementation with an eye towards performance in Chapter 4.

Links

The Links page is useful for locating other container objects that have linked to this GPO. For example, as Figure 3.9 shows, I can select a domain in my AD forest to search, then click Find Now.

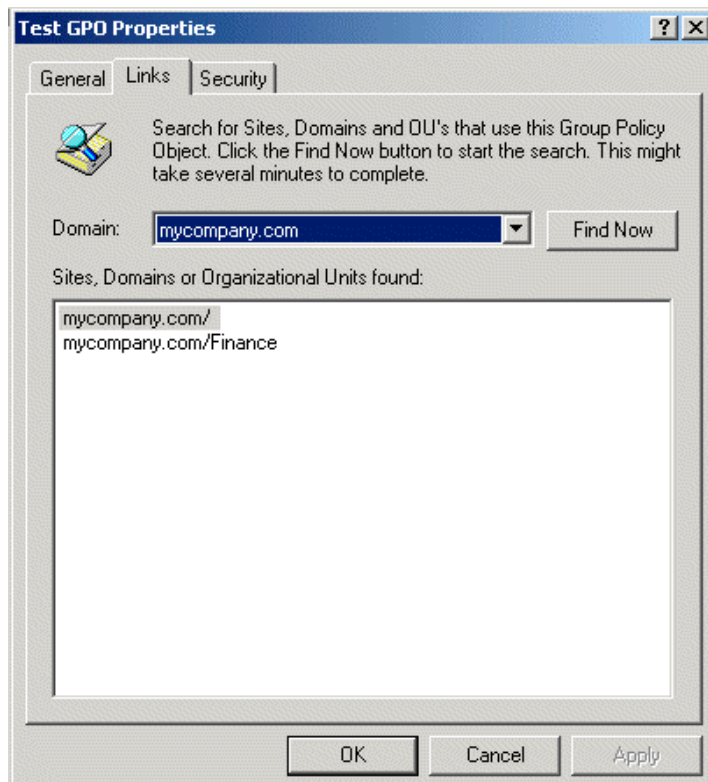


Figure 3.9: Searching for all links to the selected GPO using the Links page in the Test GPO Properties dialog box.

As Figure 3.9 shows, this particular GPO, called Test GPO, was found linked at both the domain level (in mycompany.com) and OU level (in the Finance OU). This search capability can also locate links that cross domain boundaries because, as Chapter 2 pointed out, you're free to link to GPOs that are stored across domains in a forest.

Security

The final page is Security. Clicking the Security tab displays the familiar Win2K ACL Editor dialog box. Just as with other objects in AD, GPOs have security associated with them. Security is in place for two reasons: to control who can edit or link to a particular GPO and to control what computers and users can process a particular GPO.

I'll describe using security as a GPO processing filter in more detail later in this chapter. (I also describe using GPO security to delegate administration of GPOs in Chapter 4.) For now, suffice

it to say that you can use security, in addition to the No Override and block policy inheritance features described earlier in this chapter, to control at a fine level of granularity what computers and users can process.

Controlling GPO Precedence

As you've probably guessed by now, the Group Policy page of the Properties dialog box, shown in Figure 3.1, is the hub of activity for my discussions of the various capabilities of GPOs that you can enable! This figure provides a "container-view" of GPOs. That is, for a given site, domain, or OU, it shows all of the GPOs currently linked to the container.

You'll note that when multiple GPOs are listed, the Up and Down buttons become available. These buttons let you control the ordering, or *precedence*, of GPO processing at any container level. This makes sense when you think about it. There has to be some predictable order in which GPOs are processed not only across containers (for example, LSDOU) but also in a container.

This Up/Down capability is very similar to the Group Priority capability that was available in NT 4.0 system policy. In the case of system policy, when a user was a member of multiple policy groups, user groups that were assigned to a particular policy were given an order of precedence that controlled which group-specific policy was processed first.

The Up and Down buttons on a container control which GPO is processed first, second, third, and so on. In the case of GPO processing, the higher a GPO is in the list, the later it's processed, and therefore, the more overriding its policy. For example, in Figure 3.10, three GPOs are linked at the domain level—Default Domain Policy, Test GPO, and Domain User Policy. The Default Domain Policy has the highest priority because it's at the head of the list and is processed last.



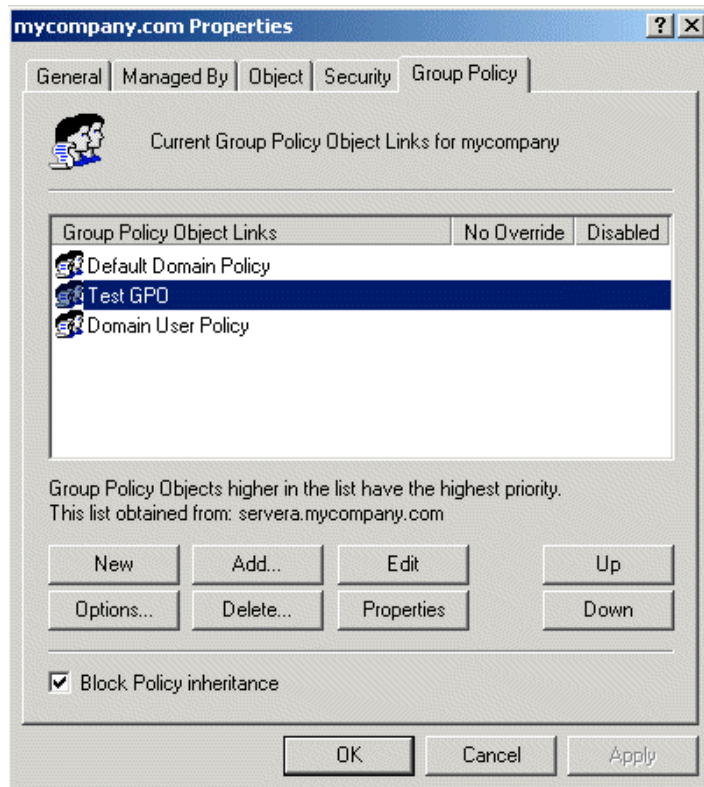


Figure 3.10: Viewing the precedence of multiple GPOs defined on an AD container.

Behind the scenes, this precedence is controlled, again, using the **gPLink** attribute on the container to which the GPOs are linked. Each GPO is referenced in this attribute by its GUID, starting from the lowest GPO to the highest. The following string represents a dump of the gPLink attribute for the container shown in Figure 3.10:

```
[LDAP://CN={BB8724E4-8BD8-4C31-BA12-
EA7E69246D16},CN=Policies,CN=System,DC=mycompany,DC=com;0][LDAP://CN={4BF6C10B
-9DDC-4E11-B702-
E58F8EC52534},CN=Policies,CN=System,DC=mycompany,DC=com;0][LDAP://CN={31B2F340-
016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=mycompany,DC=com;0]
```

Listing 3.1: Example of the LDAP path contents of a container's gPLink attribute.

Note that this listing shows the LDAP path to the three GPOs. In this case, the GUID that starts with *31B2F* is the Default Domain Policy, and the one that starts with *BB872* is the Domain User Policy.

 In Listing 3.1, the ;0 after each LDAP path represents the value that holds the GPO options described in “Setting GPO Options” earlier in this chapter. A 0 means that neither No Override nor Disabled is configured for any of these three GPO links.

If I were to reorder the three GPOs listed in Figure 3.10, the precedence of the **gPLink** attribute would change to reflect this.

It's important to keep this precedence in mind when you're designing your GPO implementation. It's very possible that two GPOs linked in the same container could have policy settings that contradict each other. In this case, the GPO with the higher precedence (higher in the list) would win, resulting in potentially unwanted policy consequences.

Adding New GPO Links

I've described almost all the buttons and check boxes shown on the Group Policy page of the Properties dialog box, shown in Figure 3.1. One I have yet to mention is the Add button. How is this button different from New? Well, New lets you create a brand new GPO—with its attendant Group Policy Template (GPT) and Group Policy Container (GPC)—and link it to the current container, all in one fell swoop. (For more information on the GPC and GPT, see Chapter 2.) However, if you simply want to create a link from an existing GPO that was defined elsewhere to this container, click Add. This displays the Add a Group Policy Object Link dialog box, shown in Figure 3.11.

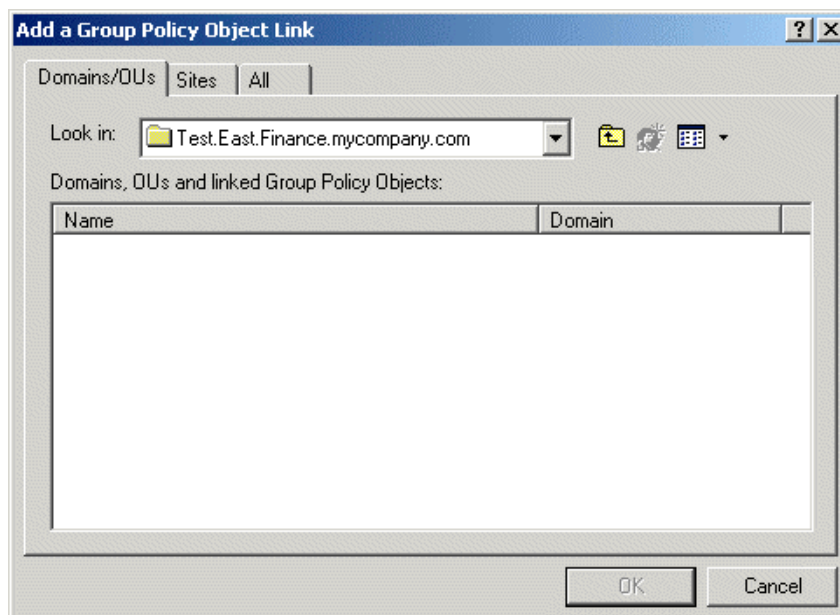


Figure 3.11: Viewing the Add a Group Policy Object Link dialog box from the GPO Properties dialog box.

This figure shows this dialog box for an OU called Test. Test is a child OU to another OU called East, which is yet another child OU to an OU called Finance. This dialog box has three tabs—Domains/OUs, Sites, and All. The Domains/OUs tab displays any GPOs currently linked to the container selected in the Look In text box. In this case, no GPOs are currently linked to the Test OU.

To see whether the GPO I'm interested in linking to is present, I can select the parent OU from the drop-down list. Or if the GPO I'm interested in linking to is defined on a site, I can click the Sites tab. Finally, to see all of the GPOs defined in this domain (or, using the drop-down list, any domain in the forest), I can click the All tab. If I select a GPO to link to and click OK, the GPO is added to the **gPLinks** attribute on the selected container—and any computers or users in this container will process the GPO. It's that simple!

On the All page in the Add a Group Policy Object Link dialog box, you can also create a GPO without performing the second step described above—the linking process. That is, you can create a physical GPO but not link it to any AD object. This can be useful if you're creating large numbers of GPOs in a production domain but don't want them to be processed yet. To create an unlinked GPO, click the All tab, then perform one of two actions. In any white space in the portion of the dialog box that lists the GPO, right-click and choose New from the context menu. A GPO is created there, and you can give it a name. Or click the icon in the upper right of the dialog box that looks like the Win2K user group icon. In either case, you can create a GPO (with associated GPC and GPT) without linking it to a container.

You can think of the Add function as providing the inverse of the functionality provided by the Links page shown in Figure 3.9. The Links page lets you search the AD for all containers that have linked to the selected GPO. The Add function lets you survey all available GPOs defined in a forest, then choose one to link to the currently selected container.

Deleting GPOs

The final button on the Group policy page in the Properties dialog box shown in Figure 3.1 is Delete. This button, as its name implies, lets you delete a GPO link from the selected container. When you click Delete, there are actually two options available to you, shown in Figure 3.12.

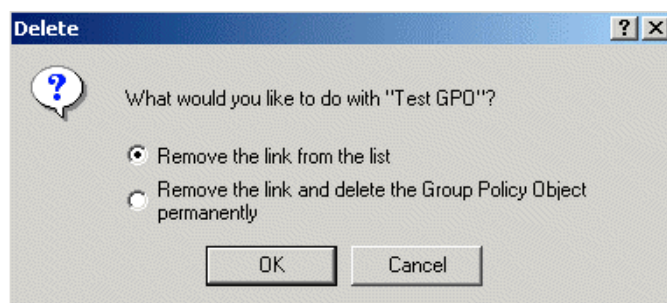


Figure 3.12: Viewing the options for deleting a GPO or GPO link from an AD container.

As this figure shows, you can either remove the link associating this GPO to the container object, or you can remove the link *and* delete the GPO itself (that is, its associated GPT and GPC). If you choose the latter option, any other links to that GPO on other container objects will also be removed. For example, if my Test GPO is linked to both the mycompany.com domain and the Finance OU, deleting the link to mycompany.com *and* deleting the GPO itself also removes the link to the Finance OU.

You can delete a link to a GPO without much consequence. But deleting the GPO itself—including its attendant GPT and GPC pieces—is an irreversible process. There is no Undo button. You can restore a GPO from a backup of both AD and SYSVOL, but it's very difficult, if not impossible, to restore an individual GPO from such a backup without affecting all other GPOs in the domain.

Setting Domain Controller Options

I'm going to shift gears now and describe a feature that allows you to set domain controller options. It's available in the Group Policy MMC snap-in when you open a GPO for editing. When you choose DC Options from the View menu, the Options for Domain Controller Selection dialog box opens, shown in Figure 3.13.

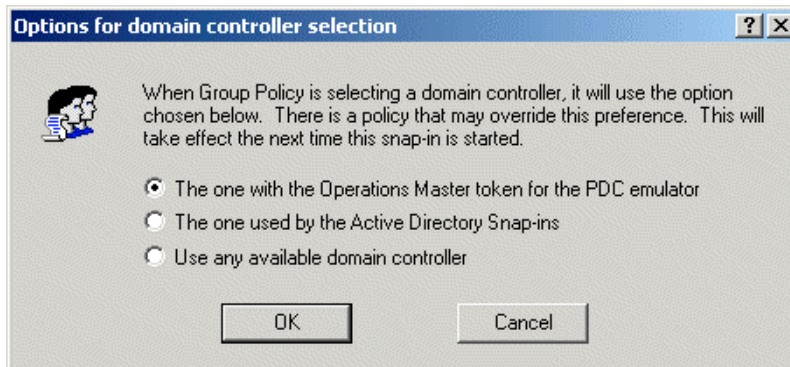


Figure 3.13: Viewing the Options for Domain Controller Selection dialog box from the Group Policy MMC snap-in.

This dialog box controls which domain controller you're focused on (and connected to) whenever you edit a GPO. Why is this important? As Chapter 2 presented, the physical GPO is composed of two components: the GPC (stored in AD) and the GPT (stored in SYSVOL). Each of these components replicates on a different schedule, and each is replicated to every domain controller in a domain. If more than one person is editing a GPO, each can be doing so from copies of the GPT/GPC stored on different domain controllers. This can obviously cause lots of unexpected and undesirable results in that GPO as each domain controller replicates its changes to the other.

To minimize this possibility, whenever an administrator starts up the Group Policy snap-in, focused on a particular GPO, a connection is made to the PDC Operations Master role-holder in that domain. Any changes the administrator makes to the GPO are made against the GPC/GPT copy stored on the PDC role-holder. This minimizes the chance that two people, editing a GPO, will make changes that will be out of sync with each other. However, you can override this behavior using the Options for Domain Controller Selection dialog box shown above. It's the default setting. The second option—The One Used by the Active Directory Snap-Ins—tells the snap-in to use the domain controller that is currently focused on and connected to by any AD snap-ins that are loaded.

For example, because you often launch the AD Users and Computers MMC snap-in before editing a GPO setting this option opens the Group Policy snap-in against the same domain controller that is currently in focus for AD Users and Computers. (You can see which domain controller an AD snap-in is currently connected to by viewing the server name shown in brackets next to the name of the snap-in in the left-hand pane of the MMC tool.)

The third option—Use Any Available Domain Controller—tells the Group Policy snap-in to use the first domain controller it can find. No particular GPO is preferred. This last option is obviously the most risky, but it's almost the most robust.

If the PDC role-holder was the preferred domain controller for GPO editing and that server was down, the GP snap-in would fail to load. The Use Any Available Domain Controller option allows an administrator to always be able to connect to a domain controller and edit the GPO. You can use this option safely if you have tight control over who is editing GPOs and when. If one person always edits GPOs in your forest, this option may be acceptable.

Using Security Groups to Filter the Processing of GPOs

As I mentioned earlier, you have several ways of controlling which GPOs are processed by which computers and users. Of course, you can link GPOs to particular OUs. Any users or computers that aren't members of the OU (or its child OUs) won't process the GPO simply by virtue of the rules of inheritance. You can also use one of the features discussed above, such as No Override or blocking policy inheritance, to control GPO processing.

But Win2K also provides a more fine-grained feature for controlling GPO processing—namely, filtering based on security groups. Security-group filtering leverages the fact that both users and computers are security principals in AD. Both users and computers can belong to security groups—be they local, global, or Universal groups. Thus, security groups provide access to a variety of resources, including file systems, printers, shares, and so on. It follows that you should also be able to use security groups to control access to and processing of GPOs. This is indeed the case.

Figure 3.14 shows the familiar ACL editor dialog box you're presented with when you click the Security tab in the Properties dialog box on a GPO.

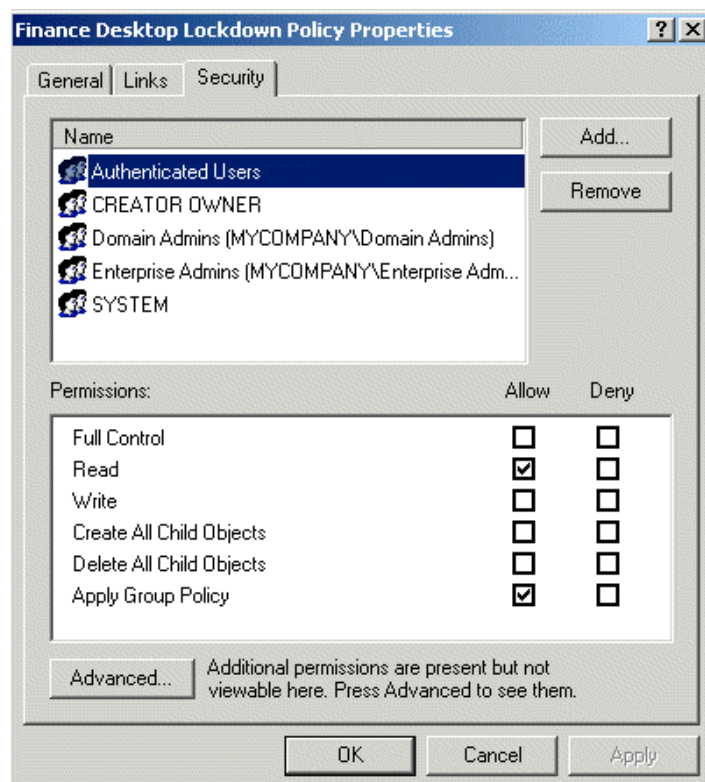


Figure 3.14: Viewing the security on a GPO in the familiar ACL editor dialog box.

As you can see in this figure, the Authenticated Users group has two permissions on this Finance Desktop Lockdown Policy: Read and Apply Group Policy. As it turns out, these are the same two permissions that are required to process a GPO. Together, they grant the right to process a GPO. If you have one but not the other, GPO processing will fail, and the computer or user trying to read the GPO will receive errors in the computer's application event log, indicating permission problems.

When you create a GPO, the Authenticated Users group is automatically granted these two permissions on the new GPO. Authenticated Users applies to both computer and user accounts; this means that by default, all computers and users who are subject to the GPO will process it. Of the other access control entries (ACEs) listed in the dialog box in Figure 3.14, none of the others have the Apply Group Policy permission. This means that only the Authenticated Users ACE controls the processing of this GPO.

It also means that, by default, members of the various built-in administrative groups like Domain Admins and Enterprise Admins don't process GPOs. This makes sense if you think about it because many policies might have a tendency to hobble an administrator's day-to-day work. Of course, if an administrator is also part of the Authenticated Users group, he or she would still be subject to the policy. You might also note that other permissions are listed in the ACL editor dialog box, such as Full Control, Write, Create All Child Objects, and Delete All Child Objects. These permissions have to do with delegating the editing of a GPO, and I'll discuss them in more detail in Chapter 4.

Changing the Default Processing

Knowing this little bit of information, you can begin to see how you can use security groups to filter the processing of a GPO. The first step to change the default processing of a GPO is to remove the Authenticated Users ACE. You can do this in the ACL Editor dialog box shown in Figure 3.14 by highlighting Authenticated Users and clicking Remove.

The next step is to add the user or computer group for which you want to allow policy processing. For example, suppose this desktop lockdown policy only applies to a subset of users in the Finance OU who are members of a group called Locked Down Finance Users. Click Add in the ACL editor dialog box, then browse to the Finance OU where this group is defined. Select the group and add it to your list of permitted groups. You'll see that it automatically receives the Read permission on the GPO. You only need to add the Apply Group Policy permission to complete the filtering of this GPO. Figure 3.15 shows what this will look like.



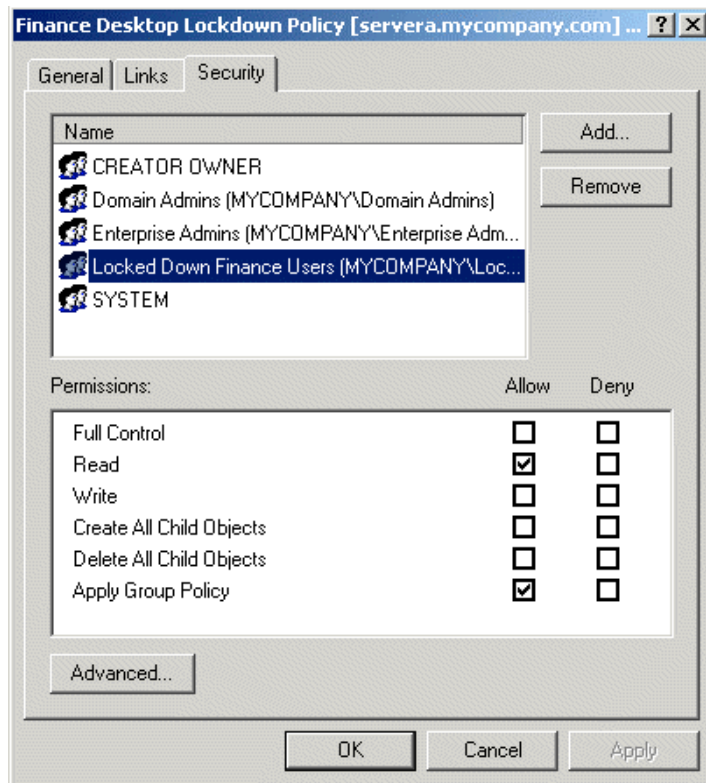


Figure 3.15: Using security groups to filter the processing of GPOs.

You'll want to use user-based security groups to filter the processing of user-specific portions of a GPO and computer-based security groups to filter the processing of computer-specific portions of a GPO. For example, if you have a GPO that only sets computer-specific Administrative Template policy, adding an ACE that filters the processing of that GPO based on membership in a user group won't affect processing. This is because what you're really interested in is controlling which computers process a GPO, not which users. The inverse is true as well, of course. However, keep in mind that security-group filtering is an all-or-nothing approach for controlling GPO processing. You can't filter out only certain nodes of functionality in a GPO. (The exception to this is software installation security, which I'll discuss in "Security Settings" later in this chapter.) If you remove the Apply Group Policy permission for a particular group, the members of that group will no longer be able to process that GPO.

Using the Deny ACE

Another approach you can take is to grant the permission to process a GPO to a wide audience like Authenticated Users, then add what's called a Deny ACE, which takes away that right from a particular subset of users or computers. A Deny is a type of ACE that revokes a set of permissions to an object. As you might expect, a Deny ACE overrules any normal Allow ACEs that might be defined on an object. So for example, I might have a group in my Finance OU called Open Users that I don't want to be subject to my desktop lockdown policy. I can add a Deny ACE to the ACL on my GPO to exclude this group from the processing of the GPO. This is shown in Figure 3.16.

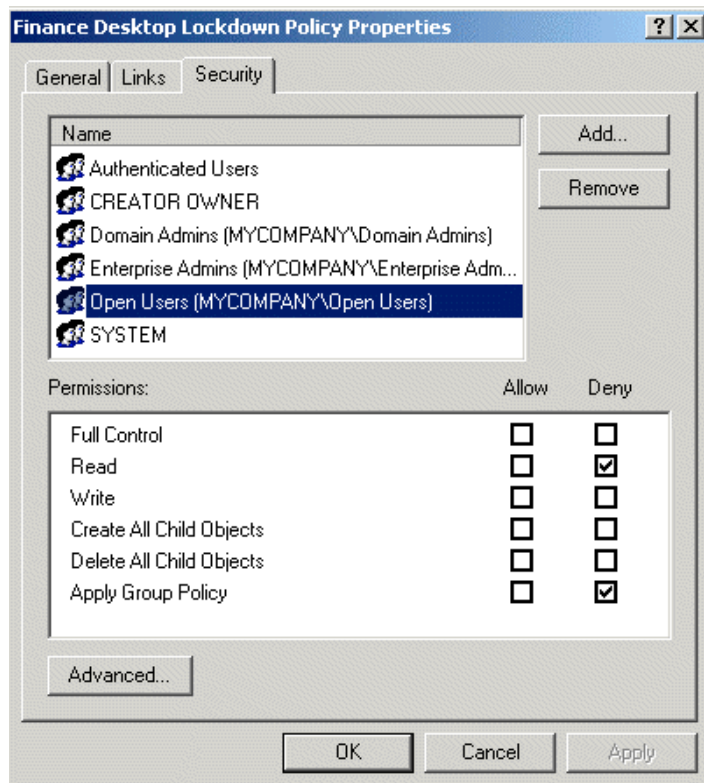


Figure 3.16: Using a Deny ACE to filter the processing of a GPO.

In this figure, you'll see that I've set the Read and Apply Group Policy permissions to Deny for the Open Users group, while the Authenticated Users group still has those permissions set to Allow. This means that all users except those who are members of the Open Users group will process this GPO.

Treading Carefully

As you can imagine, using security-group filtering to affect GPO processing can get tricky and complicated very quickly. This is especially true if you begin to use Deny ACEs to control processing. I recommend not using Deny ACEs unless you really want to exclude a small subset of users or computers from processing a GPO—and only if that group isn't likely to grow. Deny ACEs make troubleshooting GPO-processing problems very difficult because of the sheer complexity of managing all the permutations. This is especially true if your users or computers process many GPOs at logon or startup.

I also recommend going easy on security-group filtering of GPOs to begin with. Even that approach can be fraught with peril: If you're managing a lot of GPOs, you may start to lose track of what permissions you've granted to which GPOs.

 **FAZAM 2000**