1

Windows 2000 Group Policy

In this chapter, we'll get our feet wet with Group Policies. We'll start to understand conceptually what Group Policies are, how they're created, applied, and modified, and we'll go through some practical examples to assist in getting the basics under our fingers.

Getting Started with Group Policies

In the introduction, we learned about the 10 major categories of Group Policy (and where to locate them in this book):

- Administrative Templates (Registry Settings)
- Security Settings (found under the Windows Settings folder)
- Scripts (found under Windows Settings)
- Remote Installation Services (User node only under Windows Settings)
- Software Settings (Application Management)
- Folder Redirection
- Disk Quotas
- Encrypted Data Recovery Agents (EFS Recovery Policy)
- Internet Explorer Maintenance

- IP Security Policies

In this section, you'll learn how to gain access to the interface, which will let you start configuring these categories.

Accessing the Local Group Policy

Group Policy is a twofold idea. First, without an Active Directory, there's one and only one Group Policy available, and that lives on the local Windows 2000 machine. Officially, this is called a "Local Policy," but it still resides under the umbrella of Group Policy. Later, once Active Directory is available, the non-local (or, as they're sometimes called, "Domain-Based" or "Active Directory Based") Group Policy objects come into play, as we'll see later.

Before we officially dive in to what is specifically contained inside Group Policies or how Group Policies are applied when the Active Directory is involved, you might be curious to see exactly what your interaction with the local Group Policy might look like.

There are multiple ways to edit Group Policy. One way is to load the MMC snap-in by hand. You can perform this exercise logged on to any workstation as a local Administrator.

WARNING For the examples in this book, we'll be performing most of the workstation work on one workstation, W2KPro1, and most of the Active Directory and server work on one Domain Controller, W2KServer1. You can feel free to follow along if you like. Because Group Policy can be so all-encompassing, it is highly recommended that you try these examples in a test lab environment first, before making these changes for real in your production environment.

TIP Perform this first exercise on either a workstation or member-server, not a Domain Controller.

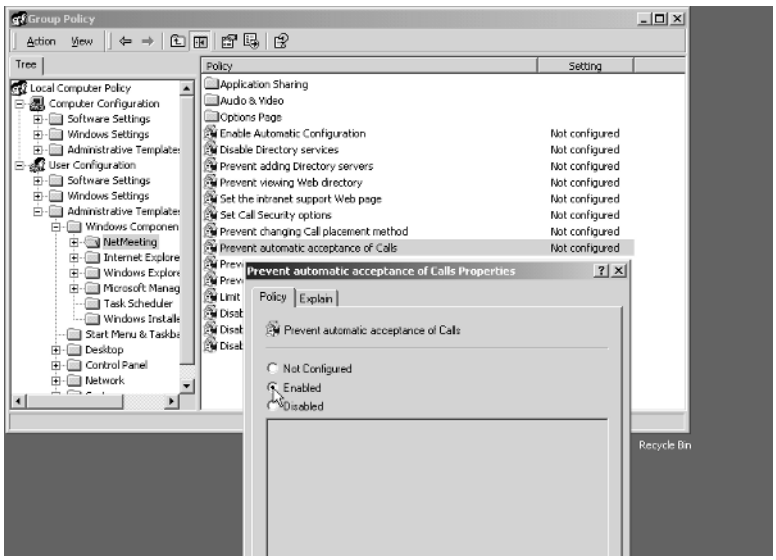
To load the Group Policy editor by hand:

1. Click Start ➢ Run and type in **MMC**. A "naked" MMC appears.
2. From the Console menu, click Add/Remove snap-in.
3. From the Add/Remove snap-in dialog box, click Add.
4. Locate the Group Policy Snap in and click Add.

5. At the "Select Group Policy Object" screen, keep the default "Local Computer Policy" and click Finish.
6. At the Add Standalone snap-in dialog box, click Close.
7. At the Add/Remove snap-in dialog box, click OK.

You should see something similar to Figure 1.1.

Figure 1.1 Edit your first Group Policy by drilling down into the User Configuration settings.



To get started seeing how a local Group Policy applies, drill down into the Computer Node ➢ Administrative Templates ➢ Windows Components ➢ NetMeeting ➢ Prevent Automatic Acceptance of Calls.

As we stated in the Introduction, most of the settings we'll explore in the book are available to workstations or servers that aren't joined to an Active Directory domain. However, the Folder Redirection settings (discussed in Chapter 6, "IntelliMirror, Part 1: Redirected Folders, Offline Folders, Synchronization Manager, and Disk Quotas") and the Software Distribution settings (discussed in Chapter 7, "IntelliMirror, Part 2: Software Deployment via Group Policies"), and Remote Installation Services (discussed in Chapter 8, cleverly entitled "Remote Installation Services"). are not available to standalone machines without Active Directory present.

> ***TIP*** You can also start the local Group Policy editor by clicking Start ➢ Run and then typing in `gpedit.msc`. You can point toward other computers by using the syntax `gpedit.msc /gpcomputer:"targetmachine"` or `gpedit.msc /gpcomputer:"targetmachine.domain.com"`, where the machine name must be in quotes.

Once we understand how Group Policies work in Active Directory, we'll return to other ways to fire up the Group Policy editor—so stay tuned.

Group Policy Entities

Every Group Policy contains two halves: a User half and a Computer half. These two halves are properly called *nodes*. A sample Group Policy editor screen with both the Computer and User nodes can be seen above in Figure 1.1.

The first level found under both the User and the Computer nodes contains Software Settings, Windows Settings, and Administrative Templates.

Double-click Administrative Templates of the Computer node, and underneath, discover additional levels of System, Network, and Printers. There, you'll see settings are hierarchical, like a directory structure. Similar policies are grouped together for easy location. That's the idea anyway, though admittedly, sometimes locating the specific policy you want can prove to be a challenge.

> ***TIP*** See the later section "Using the 'Show Configured Policies Only' Option," for tricks on how to minimize the effort of finding the policy you want.

Windows 2000 Group Policy Application

In order to make use of Group Policy in a meaningful way, you'll need to have Windows 2000 running in an Active Directory environment. An Active Directory environment needn't be anything particularly fancy; indeed, it could consist of a single Windows 2000 Domain Controller and perhaps just one workstation joined to the domain.

But Active Directory can also grow extensively from that original solitary server. Active Directory is typically seen as having four distinct levels: the local computer, Site, Domain, and Organizational Unit (OU).

The rules of Active Directory state that every Windows 2000 machine must both be a member of one (and only one) domain, as well as be located in one (and only one) site.

In Windows NT, additional domains were often created to partition administrative responsibility or to rein in needless chatter between Domain Controllers. With Windows 2000, administrative responsibility can be delegated using OUs.

Additionally, the problem with needless domain bandwidth chatter has been brought under control with the addition of Windows 2000 sites. Windows 2000 sites are concentrations of IP subnets with fast connectivity. There is no longer any need to correlate domains with network bandwidth—that's what sites are for!

Group Policies are applied cumulatively throughout the four levels: Local Computer, Site, Domain, then OU. By default, when a policy is set at one level, the levels below *inherit* the settings from the levels above it. One might look at the hierarchy this way: the levels from left to right increase in the priority. With each level, more policies are piled on top . If any policy from any two levels collide, the last policy applied wins.

If this behavior is undesired for lower levels, all the settings from higher levels can be blocked with a "Block Inheritance" attribute. Additionally, if a higher-level administrator wanted to guarantee a setting was inherited down the food chain, he could apply an attribute called "No Override." Both "Block Inheritance" and "No Override" are explored in detail later, in the "Advanced Manipulation of Group Policy" section.

NOTE Don't sweat it if at this point your head is spinning a little bit from the Group Policy application theory. We'll be going through specific hands-on examples to illustrate of each of these behaviors in order to gain a better understanding of exactly how this works.

Linking Group Policies

Another technical concept that needs a bit of description here is the concept of "linking" Group Policies. When a Group Policy object is created at the Site, Domain, or OU level, via the GUI (which we'll do in a moment) the system automatically takes that Group Policy object and associates it with the level in which it was created. That association is called *linking*.

Linking is an important concept for several reasons. Primarily, understanding the concept and terminology of linking is important should you ever read additional documentation that uses the term. But, practically, it's useful to know what's really going on under the hood.

Envision this: You can think of all the Group Policy objects you create as children who are swimming around in a big pool. Each child could have a tether attached around his waist where a parent is holding the other end of the rope. Indeed, there could also be

multiple tethers around a child's waist, with multiple parents tethered to one child. A sad state indeed would be where a child had no tether at all, but was rather just swimming around in the pool unsecured.

The "pool" in the above analogy is the domain. All Group Policy objects "live" in the domain; specifically, they're replicated to all Domain Controllers. The "parents" in the above analogy represent a level in Active Directory—any site, domain, or OU. Remember, in the example, multiple parents could be tethered to a specific child. With Group Policy objects, multiple levels in Active Directory could be linked to a specific Group Policy—site, domain, or OU.

Remember, though, unless a Group Policy object is linked to a site, domain, or OU, they do not take effect. They're just floating around in the domain waiting for someone to make use of them.

Lastly, Group Policy objects may be generated programmatically via scripts or other methods. When they do, they are just "free floating" in the domain, without being linked to by any Active Directory level.

NOTE To learn how to programmatically create Group Policy objects seek out the Platform SDK at `www.microsoft.com/msdownload/platformsdk/setuplauncher.asp`. Additionally, check out Microsoft's article Q248392, entitled "Scripting the Addition of Group Policy Links."

Later, we'll dive a bit further into the concept of linking in the "Understanding Group Policy Object Linking" section. There we'll see how you can use it to your advantage to get the most out of the concept. Additionally, we'll also discuss why you might want to "unlink" a policy in the section, "Deleting and Unlinking Group Policy Objects."

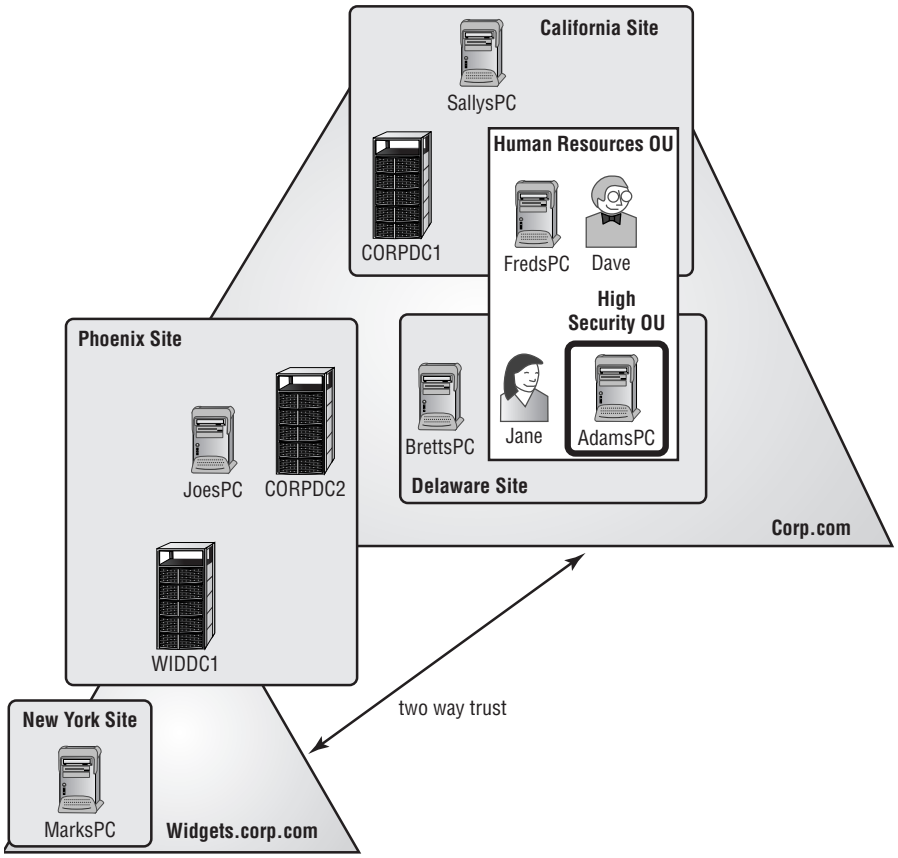
This concept of "linking" can be a bit confusing. For now, it's good to know that whenever you create a new Group Policy using the GUI, you're actually creating the Group Policy object, and it's being automatically linked to the currently focused level (site, domain, or OU).

An Example of Group Policy Application

At this point, it's best not to jump directly into the Group Policy editor and start adding, deleting, or modifying policies. Right now, it's best to understand how Group Policies work "on paper." This is especially true if you're new to Group Policies, but perhaps also when Group Policies have been deployed by other administrators in your Active Directory.

By walking through a fictitious organization which has Group Policies applied at multiple levels, you'll be able to better understand how and why Group Policies are applied. Let's start by taking a look at Figure 1.2, the organization for our fictitious example company, Corp.com.

Figure 1.2 This fictitious Corp.com is relatively simple. Your environment may be more complex.



This picture could easily tell 1,000 words. For the sake of brevity, I've kept it down to around 200.

In this example, for instance, the domain Corp.com has two Domain Controllers. One DC, named CORPCD1, is physically located in the California site. Corp.com's other

Domain Controller, CORPDC2, is physically located in the Phoenix site. Using Active Directory Sites and Services, a schedule could be put in place to regulate communication between CORPDC1 located in California and CORPDC2 located in Phoenix. That way chatter between the two Corp.com Domain Controllers is controlled by the administrator and not the whim of the operating system.

Inside the Corp.com domain are two OUs: Human Resources, and (inside Human Resources) another OU called High Security. FredsPC is located inside the Human Resources OU, as are Dave's User account and Jane's User account. There is one PC inside the High Security OU, called AdamsPC. There is also JoesPC, which is a member of the Corp.com domain, physically resides at the Phoenix site, and isn't a member of any OUs.

There is another domain as well, called Widgets.corp.com, which has an automatic transitive two-way trust to Corp.com. There is only one Domain Controller in the Widgets.Corp.com domain, named WIDDC1, and it physically resides at the Phoenix site. Lastly, there is MarksPC, a member of the Widgets.corp.com domain, which physically resides in the New York site and isn't in any OUs.

Understanding where your users and machines lay is half the battle. The other half of the battle is understanding which policies are expected to appear when they start logging into Active Directory.

Examining the Resultant Set of Policies

Remember that Group Policies are cumulative as they flow down between the local computer, the Site, Domain, and each nested OU. The end result of what winds up affecting a specific user or computer—after all Group Policies have been applied—is called the *Resultant Set of Policies*, or *RSOP*.

Before we jump in to try to discover what the RSOP might be for any specific machine, it's often helpful to break out each of the strata—local computer, site, domain, and OU—and examine, at each level, what would happen to the entities contained therein.

NOTE For this example, I've stripped away the complexity of having to worry about *exactly* which policies are being applied. The goal is to get a better feeling of how Group Policies flow, not necessarily what the specific end-state will be.

Then, we'll bring it all together to see how a specific computer or user would react to the accumulation of policies. For these examples, assume there is no local policy set on any of the computers.

At the Site Level

Based on what we know from Figure 1.2, the policies in effect at the Site level would be as follows:

California Site Computers	The computers affected by the California site are SallysPC, CORPDC1, and FredsPC.
Phoenix Site Computers	The computers affected by the Phoenix site are CORPDC2, JoesPC, and WIDDC1.
New York Site Computers	MarksPC is the only computer affected by the New York Site.
Delaware Site Computers	The Delaware Site affects AdamsPC and BrettsPC.

NOTE Users are affected by site policies only when they log onto computers that are at a specific site. In our diagram, we have users Dave in California (on a California PC) and Jane in Delaware (on a Delaware PC).

At the Domain Level

Here's what we have working at the Domain level:

Corp.com Computers	The computers affected by Group Policies in the Corp.com domain are: SallysPC, FredsPC, AdamsPC, BrettsPC, JoesPC, CORPDC1, and CORPDC2.
Corp.com Users	The users affected by Group Policies in the Corp.com domain are: Dave and Jane.
Widgets.corp.com Computers	WIDDC1 and MarksPC are affected by the Group Policies applied to Widgets.corp.com.

At the OU Level

At the Organizational level, we have the following:

Human Resources OU Computers	FredsPC is in the Human Resources OU; therefore it is affected when the Human Resources OU gets Group Policies applied. Additionally, the High Security OU is contained inside the Human Resources OU. Therefore, AdamsPC, which is in the High Security OU, is also affected whenever the Human Resources OU is affected.
Human Resources OU Users	The accounts of Dave and Jane are affected when the Human Resources OU has Group Policies applied.

Bringing It All Together

Now that you've broken out all the levels and seen what is being applied to them, you can then start to calculate what the devil is happening on any specific user and computer combination. Looking at the above diagram and then analyzing what's happening at each level, makes adding things together between the Local, Site, Domain, and OU policies a lot easier.

Here are some examples of Resultant Sets of Policies for specific users and computers in our fictitious environment:

FredsPC	FredsPC will inherit the RSOP of the policies from the California Site, then the Corp.com domain, then lastly, the Human Resources OU.
MarksPC	MarksPC would first accept the policies from the New York Site, then the Widgets.corp.com domain. MarksPC is not in any OU, therefore no OU policies apply to his computer.
AdamsPC	AdamsPC would be subject to the policies at the Delaware Site, the Corp.Com domain, the Human Resources OU, and finally the High Security OU.
Dave using AdamsPC	AdamsPC would be subject to the computer policies at the Delaware Site, the Corp.com domain, the Human Resources OU, and finally the High Security OU. When Dave

travels from California to Delaware to use Adam's workstation, his user policies are dictated from the Delaware Site, the Corp.com domain, then the Human Resources OU.

NOTE At no time did any domain policies from the Corp.com parent domain get automatically inherited to the Widget.corp.com child domain. Domain inheritance flows downward to OUs only within its own domain, not between any two domains—parent to child, or otherwise.

If you wish to have one Group Policy object affect the users in more than one domain, you have two choices: recreate the policies in each domain, or use policy linking (as described in detail later). Don't assume that adding a policy at a site level will necessarily guarantee the results to more than one domain. In this example, as in real life, there is not necessarily a 1:1 correlation between sites and domains.

Using the Group Policy Editor in Active Directory

NOTE For the sake of examples in this book we will be referring to our sample Domain Controller, W2KServer1, which is part of the Corp.com domain. For these examples, you can choose to rename the Default-First-Site-Name site or not—your choice.

Since we're still warming up to Group Policies, we'll start off with some basics to ensure that things are running smoothly. For most of the examples in this book, you'll be able to get by pretty well with just the one Domain Controller and one or two workstations that participate in the domain, for verifing that your changes took place.

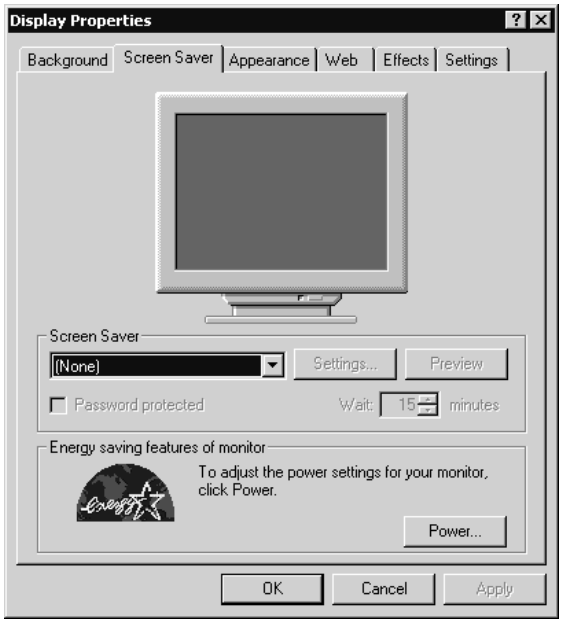
Again, I encourage you to not try these examples on your production network, in order to avoid a *CLM*, or *career limiting move*.

NOTE Instead of naming the domain Corp.com, you might also choose to name the domain Corp.local (for the sake of example), to guarantee you don't bang heads with the *real* Corp.com already registered out on the Internet.

Now that we have a grip on how Group Policies are applied (Local Computer, Site, Domain, then each nested OU), it would probably be helpful to know how to access the Group Policy editor at each of those levels.

For this example, we're going to go after the users who keep fiddling with their Control Panel ➢ Display applet. Inside the display applet are several tabs, including Screensaver, Appearance, and Settings, as shown below in Figure 1.3.

Figure 1.3 All of the tabs in the Display Properties dialog box are available by default.



For this first example, we're going to produce three "edicts." (For dramatic effect, you should stand on your desk and loudly proclaim these edicts with a thick British accent.)

- At the site level, there will be no more Screen Saver tabs.
- At the domain level, there will be no more Appearance tabs.
- At the OU level, there will be no more Settings tabs. And, while we're at it, let's bring back those Screen Saver tabs!

TIP Following along with these concrete examples will really reinforce the concepts presented above. Additionally, they are used throughout the remainder of this chapter and Chapter 3, "Troubleshooting Group Policy."

Accessing the Group Policy Editor at the Site Level

Chances are that the site level will be the least frequently accessed level for Group Policy application. That's because it's got the broadest stroke but the bluntest application. Additionally, since Windows 2000's defaults state that only members of the Enterprise Administrators can modify sites and site links, it's equally true that only Enterprise Administrators (by default) can add Group Policies at the site level.

NOTE When there is more than one domain in a tree or forest, only the Enterprise Admins and the Domain Admins can create and modify sites and site links. When multiple domains exist, Domain Admins in domains other than the root domain may not create sites or site links (or site-level Group Policy objects).

You may wish to set up Site level Group Policy object definitions for network-specific settings, such as Internet Explorer Proxy Settings or IP Security policy for sensitive locations.

Therefore, if you're not an Enterprise Administrator (or Domain Administrator of the root domain), it's likely you'll never get to practice this exercise outside of the test lab. In this example, we'll be working with a basic example to get the feel of the Group Policy editor.

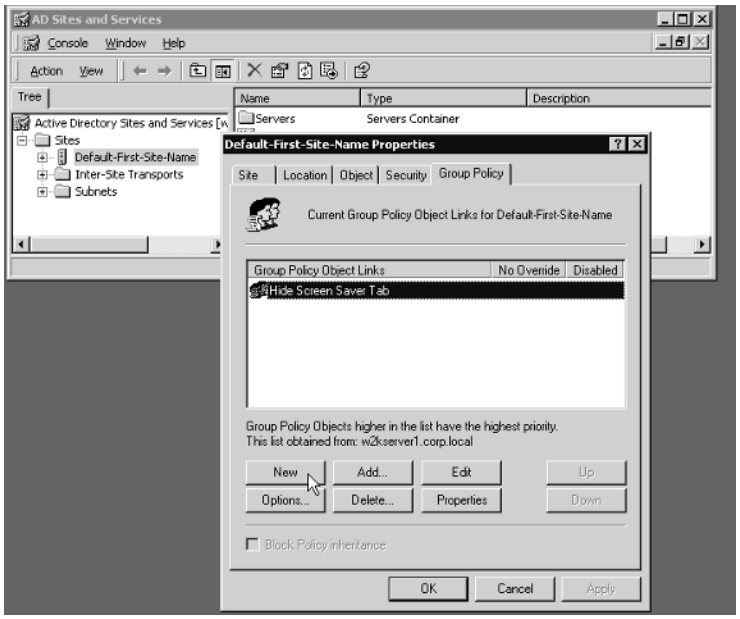
WARNING Implementing Site Policies can have a substantial impact on your logon times and WAN traffic. See Chapter 3, "Troubleshooting Group Policies" for more information.

To remove the Screen Saver tab using the Group Policy Editor at the Site Level, follow these steps:

1. Log on to the Domain Controller W2KServer1 as an Enterprise Administrator (the Administrator account in the first domain is an Enterprise Administrator).
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Sites and Services.

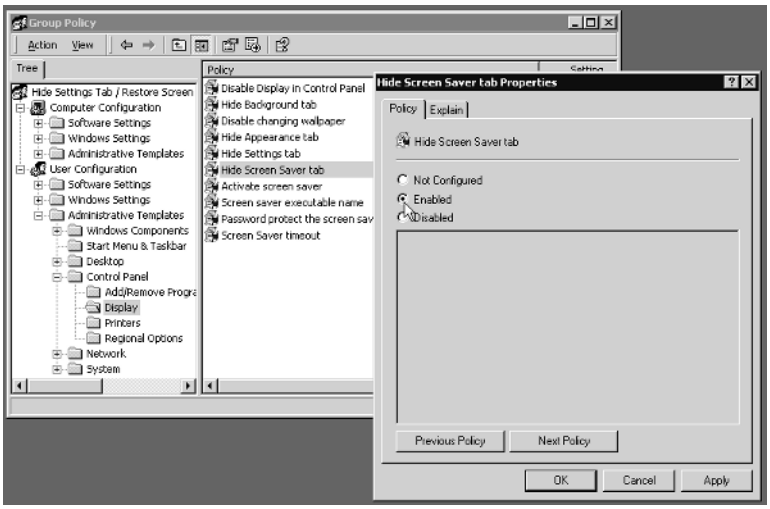
3. Under the Sites folder, drill down until you find the site to which you want to deliver the policy. If you have only one site, it is likely called Default-First-Site-Name, as is shown in the example Figure 1.4.

Figure 1.4 Site Group Policy objects are applied in the site, domain, OU hierarchal order.



4. Right-click the site and click Properties. The Properties of the site appear.
5. Click the Group Policy tab, as shown in Figure 1.4.
6. Click New in the Group Policy dialog box and name the policy something descriptive, such as **Hide Screen Saver Tab**.
7. Once the name is entered, highlight the policy and click Edit. The Group Policy editor should appear.
8. To hide the Screen Saver tab, drill down to User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display and double-click the "Hide Screen Saver Tab" entry. Change the setting from "Not Configured" to "Enabled," and click OK, as shown in Figure 1.5.

Figure 1.5 Double-click the policy and enable it.



9. When you're back at the Group Policy editor screen, close it to return to the Sites and Services screen. Close that as well.

Note that there was no "Are you sure you really want to change this setting?" entry or anything similar. This is behavior similar to the Registry editor (should you choose to go plunking around in there). Whack the wrong item in the Registry editor or make the wrong change, and it's curtains for that particular system.

With the Group Policy editor, you can make major boo-boos on a grand scale. Again—this is why you want to try any setting you wish to deploy in a test lab environment first.

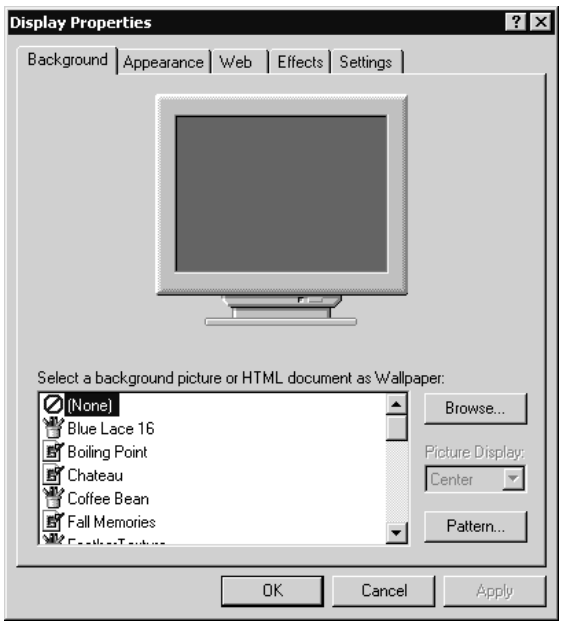
WARNING Try all Group Policy changes in a test lab first.

Verifying Your Changes at the Site Level

Now, log into any workstation or server that falls within the boundaries of the site to which you applied the site-wide Group Policy object. You can choose any user you have defined—even the Administrator of the domain.

Open up the Display applet in Control Panel and note that the Screen Saver tab is missing, as shown in Figure 1.6 below.

Figure 1.6 The Screen Saver tab is missing because the site policy is affecting the user.



TIP Don't panic if you do not see the changes reflected right away. See the section "Forcing Background Processing with SECEDIT" later in the chapter to find out how to encourage changes to occur.

This demonstration should prove how powerful Group Policies are, not only because everyone at the site is affected, but more specifically because Administrators are not immune to Group Policy's effects.

TIP Administrators are not immune to Group Policy because they are automatically members in the "Authenticated Users" security group. You can modify this behavior with the techniques explored in the section, later in this chapter.

Accessing the Group Policy Editor at the Domain Level

At the Domain level, we want to have an edict that says the Appearance tab should be removed from the Display applet in Control Panel.

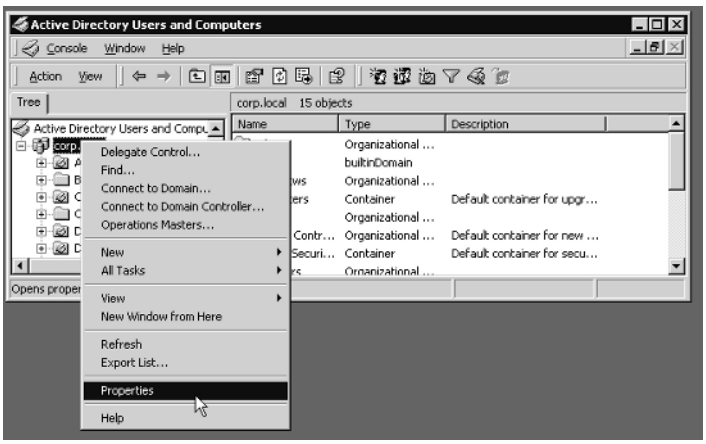
Windows 2000 allows only members of the Domain Administrators the ability to create Group Policy over the domain. Therefore, if you're not a Domain Administrator (or a member of the Enterprise Admins group), it's likely that you'll never get to practice this exercise outside of the test lab.

To make modifications to Group Policy at the Domain level, we need to fire up Active Directory Users and Computers.

To remove the Appearance tab using the Group Policy editor at the domain level, follow these steps:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. Right-click the domain name and click Properties, as shown in Figure 1.7.

Figure 1.7 Right-click the domain name and select Properties.

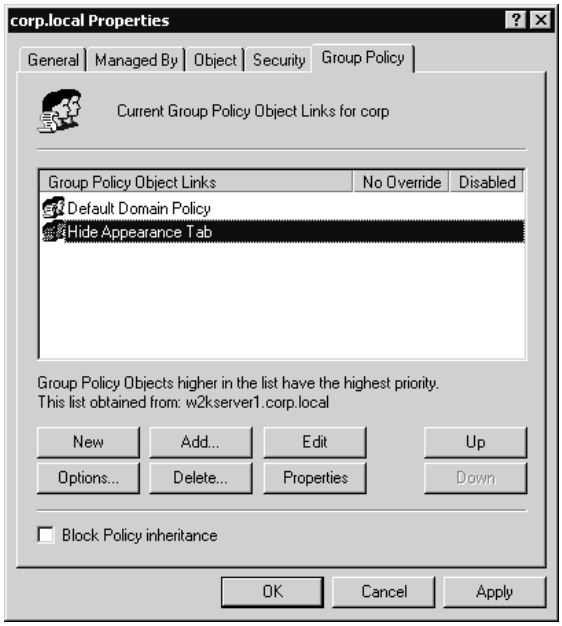


4. The Properties box for the domain appears. Click the Group Policy tab.

TIP Note that there is a Default Domain Policy, but you won't be modifying it at this time. (See the later section "The Two Default Policies" for more details.)

5. It is not recommended that you modify the Default Domain policy for normal settings. Therefore, click the New button and type in a descriptive name, such as "**Hide Appearance Tab**" as shown in Figure 1.8.

Figure 1.8 Create another Group Policy object in the domain called "Hide Appearance Tab."



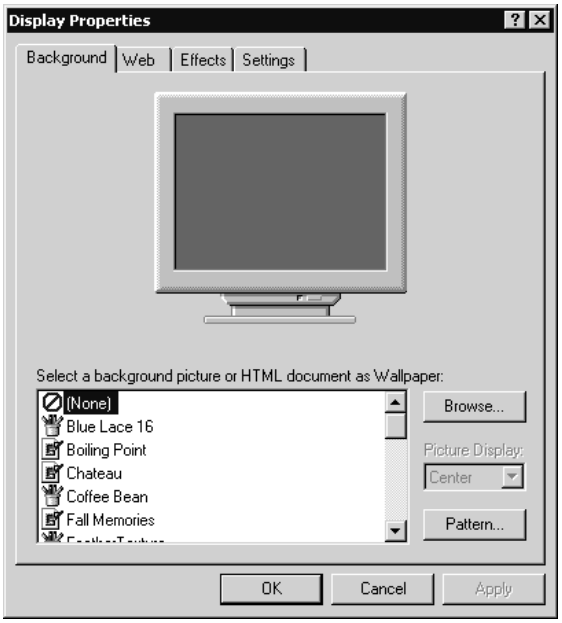
6. Once the name is entered, highlight the policy and click Edit. The Group Policy editor should appear.
7. To hide the Appearance tab, drill down to User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display and double-click the "Hide Appearance Tab" entry. Change the setting from "Not Configured" to "Enabled," exactly the way you performed the change earlier. Click OK to close the entry.
8. When back at the Group Policy editor screen, close it to return to the Domain Properties screen. Close that as well. You can leave Active Directory Users and Computers open if you desire.

Verifying Your Changes at the Domain Level

Now, log in as any user in the domain. You can choose any user you have defined—even the Administrator of the domain.

Traverse to Control Panel ➢ Display and note that the Appearance tab is now also missing, as shown in Figure 1.9 below.

Figure 1.9 The Appearance tab is now also missing because the user is affected by the domain-level policy.



Once again, Administrators are not immune to Group Policy's effects. You can change this behavior by exploring the "Filtering Group Policy Application" section later in the chapter.

TIP Again, don't panic if you do not see the changes reflected right away. See the section "Forcing Background Processing with SECEDIT" later, for more on encouraging changes to occur.

Accessing the Group Policy Editor at the OU Level

We will likely find ourselves making most of our Group Policy additions and changes at the OU level. OUs are wonderful tools for delegating away unpleasant administrative duties, such as password resets or modifying group memberships.

Once OU administrators become comfortable in their surroundings sometime down the line, we can expect that they will want to harness the power of Group Policy.

Preparing to Delegate Control

In order to create Group Policies at the OU level, you must first have the OU created and a plan to delegate. For this example, we'll create the Human Resources OU in our Corp.com domain, then create the HR-OU-Admins Group and put our first HR-OU-Admins inside that group. Then, we'll delegate the appropriate rights necessary for them to use.

To create the Human Resources OU, proceed as follows:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. Right-click the domain name and click New ➢ Organizational Unit. Enter in **Human Resources** as the name.

To create the HR-OU-Admins Group:

1. Right-click the new Human Resources OU and select New ➢ Group.
2. Create the new group **HR-OU-Admins** as a new Global Security group.

To create the first HR-OU-Admins User:

1. Right-click ver the Human Resources OU and select New ➢ User.
2. Name the user **Frank Rizzo**, with an account name of "**frizzo**" Click Next.
3. Choose to enter a password, or keep it blank if you're working in a test lab.
4. Finish and close the Wizard.

To add Frank Rizzo to the HR-OU-Admins group:

1. Double-click on the HR-OU-Admins group.
2. Click the Members tab.
3. Add Frank Rizzo.

NOTE The "Computers" folder and "Users" folder seen in Active Directory Users and Computers are not OUs. They are generic "folders" where new users and computers are created by default. Then administrators are supposed to move the accounts into OUs. You cannot associate Group Policy objects with these folders; however, these users and computers are affected by site and domain level policies.

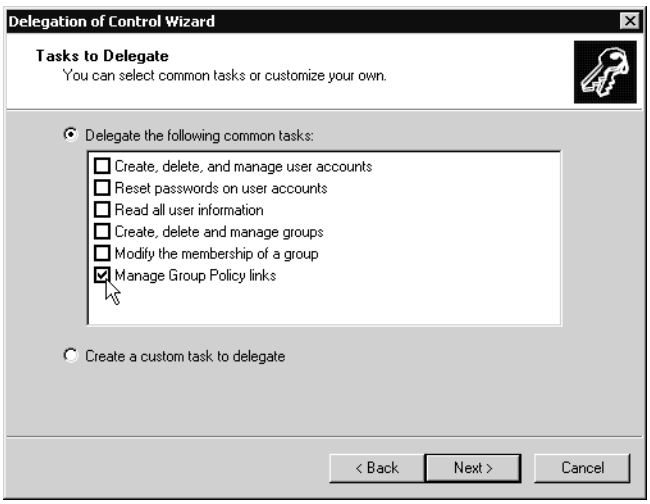
Delegating Control for Group Policy Management

Now that you've created the OU and the security group and put the actual HR-OU-Admins into the group, you're ready to delegate control:

1. Right-click the Human Resources OU you created.
2. Select "Delegate Control."
3. The Delegate Control Wizard starts. Click Next to continue.
4. You'll be asked to select Users and/or Groups. Click Add, and add the HR-OU-Admins group and click Next.
5. At the "Tasks to Delegate" screen, be sure to click on the "Manage Group Policy Links" (shown in Figure 1.10), and click Next.

TIP You may wish to click on all the other check boxes as well, but for this demonstration only the "Manage Group Policy Links" is required.

Figure 1.10 You may select any and all check boxes as long as you select "Manage Group Policy Links."



6. At the Wizard review screen, click Finish.

NOTE The "Manage Group Policy Links" predefined wizard task assigns the user or group read and write access over the the "gPLink" and "gPOptions"

properties for that level. To see or modify these permissions by hand, use the View ➢ Advanced Features option in the Active Directory Users and Computers MMC snap-in, then find the permission by right-clicking the delegated object (such as OU), clicking the Properties tab, then clicking the Security tab and digging around until you come across the permission you wish to remove, and then delete the corresponding Access Control Entry (ACE).

Adding a User to the Server Operators Group

Under normal conditions, nobody but Domain Administrators or Enterprise Administrators can walk up to Domain Controllers and log on. For testing purposes only, though, we're going to add our user, Frank, to the Server Operators group so he can easily work on our W2KServer1 Domain Controller.

To add a user to the Server Operators group, do the following:

1. In Active Directory Users and Computers, double-click on Frank Rizzo's account under the Human Resources OU.
2. Click the "Member Of" tab and click Add.
3. Select the Server Operators group and click OK.
4. Close Frank Rizzo's Properties by clicking OK.

WARNING Normally, you wouldn't give your delegated OU administrators "Server Operators" access. You're doing it solely for the sake of this example.

Testing Your Delegation of Group Policy Management

Log off as the Administrator on W2KServer1 and log back on as Frank Rizzo.

1. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.

NOTE If the Administrative Tools are not present, you'll need to click Start ➢ Run and type **`mmc`** to load a "naked" MMC. Then load in Active Directory Users and Computers.

2. Drill down until you reach the Human Resources OU, right-click it, and select Properties. The Human Resources Properties page appears.

3. Select the Group Policy tab. Click New to attempt to add a Group Policy. You should be presented with the error shown in Figure 1.11.

Figure 1.11 This error occurs when you do not have access to create Group Policies.

You will get this error because, while Frank (and more specifically, the HR-OU-Admins) have been delegated the ability to *access* the Group Policy object properties, they have not been given the access to *create* new Group Policy objects. Rather, they have only been delegated the ability to perform a Group Policy link using the Add button.

Understanding Group Policy Object Linking

Without the ability to actually create these Group Policy objects (as explored later), delegated permissions can only yield *Group Policy linking*.

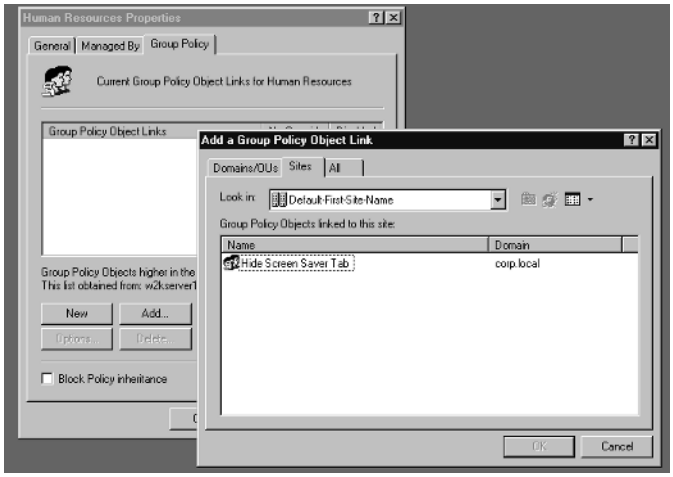
Recall that when you create a new Group Policy object at any currently focused level (Site, Domain, or OU), you are really creating the Group Policy object and linking it directly to that level. But you can take that one step farther.

Fully utilizing Group Policy object linking is a great idea in theory; someone with a lot of brains in the organization does all the work in creating a complex, well thought-out and well-tested Group Policy object. Then, others in the organization are delegated the ability to *link* to that Group Policy object and use it at their level.

This solves the problem of delegating control to administrators who might be ready to create their own users and groups, but who may not be quite ready to jump into the cold waters of Group Policy object administration. You can design the Group Policies for them; they can just link to the ones you (or others) create.

When you click the Add button in the Group Policy tab on the Human Resources properties page, you are given the opportunity to choose "someone else's" Group Policy object. It's sectioned off into easy chunks: Domains/OUs, Sites, or All, represented in the tabs on the "Add Group Policy Object Link" box in Figure 1.12.

Figure 1.12 You can link to another Group Policy object via the Add button.



In this example, the HR-OU-Admins could use any currently created Group Policy object to affect the users and computers in their OU—even if they didn't create it themselves. Again, this is a good idea in practice, but often OU administrators are simply given full authority to create their own Group Policies, as we'll see later.

For this example, don't worry about linking to any policies. Simply cancel out of the "Adding a Group Policy Object" link, close the Properties page of the Human Resources OU, and log off as Frank Rizzo from the server.

TIP While it's possible to link to Group Policies in other domains, it often makes things very slow and painful for your users. Whenever possible, only link to Group Policies in your own domain.

Granting OU Admins Access to Create New Group Policy Objects

By using the Delegation of Control Wizard to delegate the "Manage Group Policy Links" attribute, you've performed half of what is needed to grant the appropriate authority to Frank and the HR-OU-Admins so that they can create their own Group Policy objects upon the Human Resources OU.

One of Windows 2000's built-in security groups, "Group Policy Creator Owners," holds the key to the other half of our puzzle. You'll need to add those users whom you want to have the ability to add new Group Policy objects into this built-in group.

1. Log back on as the Domain Administrator.
2. Click Start ➢ Run ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. By default the "Group Policy Creator Owners" group is located in the "Users" folder in the domain. Double-click the "Group Policy Creator Owners" group and add the HR-OU-Admins group and/or Frank Rizzo.

TIP You will not be able to add the HR-OU-Admins group until the domain mode has been switched to Native. Switch the domain to Native mode, if you desire, using Active Directory Domains and Trusts. Switching to Native mode is a one-way operation, which shuts out all Windows NT 4.0 BDCs. If you are not prepared to make the switch to Native mode, you'll only be able to add Frank Rizzo.

4. Log off as the Administrator from W2KServer1.

Adding a New Group Policy Object at the OU Level

At the Site level, we chose to hide the Screen Saver tab in the Display applet. At the Domain level, we chose to hide the Appearance tab in the Display applet.

At the OU level, we have two jobs to do:

- Hide the Settings tab in the Display applet.
- Restore the Screen Saver tab that was taken away at the Site level.

To create a Group Policy object at the OU level, proceed as follows:

1. Log off as the Administrator on W2KServer1 and log back on as Frank Rizzo.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.

NOTE If the Administrative Tools are not present, you'll need to click Start ➢ Run and type **mmc** to load a "naked" MMC. Then load in Active Directory Users and Computers.

3. Drill down until you reach the Human Resources OU, right-click it, and select Properties. The Human Resources Properties page appears.
4. Click New in the Group Policy dialog box and name the policy something descriptive, such as **"Hide Settings Tab/Restore Screen Saver Tab**."
5. Once the name is entered, highlight the policy and click Edit. The Group Policy editor should appear.
6. To hide the Settings tab, drill down to User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display and double-click the "Hide Settings Tab" entry. Change the setting from "Not Configured" to "Enabled," and click OK as you did with the other two policies.
7. To restore the Screen Saver tab, double-click the "Hide Screen Saver Tab" entry. Change the setting from "Not Configured" to "Disabled," and click OK as you did with the other two policies.

NOTE By "disabling" the "Hide Screen Saver Tab" setting, you're reversing the "Enable" setting set at a higher level.

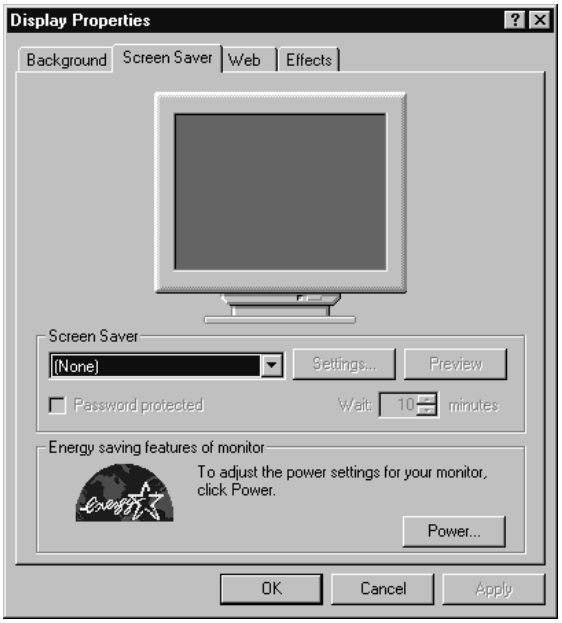
8. When back at the Group Policy editor screen, close it to return to the OU Properties screen. Close that as well. You can leave Active Directory Users And Computers open if you desire.

Verifying Your Changes at the OU Level

Since you're already logged in as Frank, you should see your changes take place almost immediately.

Traverse to Control Panel ➢ Display and note that the Settings tab is also missing, but the Screen Saver tab is back, as shown in Figure 1.13 below.

Figure 1.13 The Settings tab is missing along with the Appearance tab, and the Screen Saver tab has returned.



This test proves, once again, that even OU administrators are not automatically immune from their own policies. This is because they are in the "Authenticated Users" security group. You can modify this behavior by exploring the "Filtering Group Policy Application" section later on.

TIP Don't panic if you do not see the changes reflected right away. See the section on "Forcing Background Processing with SECEDIT" later for advice on how to encourage changes to occur.

Group Policy Strategy

There will be times when you will want to lock down additional functions. For instance, you may wish to affect all Human Resources computers so that the Task Scheduler (found in Control Panel ➢ Scheduled Tasks) cannot be used.

At the Human Resources OU level, you've already set up a policy to hide the Settings Tab in the Display applet in Control Panel.

Group Policy Strategy *(continued)*

You now have a decision to make. You can create a new Group Policy object which affects the Human Resources OU, give it a descriptive name, say "Remove Task Scheduler," and then drill down to the Computer Configuration ➢ Administrative Templates ➢ Windows Components ➢ Task Scheduler ➢ "Disable New Task Creation" setting and enable it. (Be aware of strange Microsoft verbiage where you need to "Enable" a policy to disable a setting.)

Or you could simply modify your existing Group Policy object, the "Hide Settings Tab/Restore Screen Saver Tab" policy, so it contains additional policies. Then you could rename your Group Policy object to something that makes sense and encompasses the qualities of all the policy changes, say, "Desktop Settings."

Here's the quandary: the former method (one policy per Group Policy object) is certainly more descriptive, and definitely easier to debug should things go awry. If you only have one policy per Group Policy object, you have a better handle on what each one is affecting. If something goes wrong, you can dive right into the Group Policy object, track down the policy, and make the necessary changes, or disable the ornery Group Policy object (as discussed later).

The second method (multiple policies per Group Policy object) is faster for your computers and users at boot or logon time, because each additional Group Policy object takes some additional processing time. But if you stuff too many settings in an individual Group Policy object, the time to debug should things go wrong goes up exponentially, because Group Policies have so many nooks and crannies, they can be difficult to debug.

So, in a nutshell, if you have more Group Policy objects at a particular level,

- You can name each of them more descriptively.
- You can debug them easily if things go wrong.
- You can disable individually misbehaving Group Policies.

If you have fewer Group Policy objects at a particular level,

- Logging on is slightly faster for the user
- It is harder for you to debug if things go wrong
- You can disable individually misbehaving Group Policies. (But if they contain many settings, you may be disabling more than you desire.)

So, how do you form a Group Policy object strategy?

There is no right or wrong answer; you need to decide what's best for you. There are, however, several options to help you decide.

Group Policy Strategy *(continued)*

One "middle of the road" strategy is to start off with multiple Group Policy objects with one lone policy in each. Once you are comfortable that they are individually working as expected, you can create another *new* Group Policy object which would contain the sum of the settings from, the "Hide Settings Tab" and the "Disable New Task Creation" in this example, and then delete (or disable) the old individual Group Policies.

Another, less frequently used strategy is to group together only User node settings or only Computer node settings and disable the unused half (as described later). This allows for policies affecting one node to be grouped together for ease of debugging but also allows the flexibility to put the brakes on by disabling them should things go wrong.

Creating a New Group Policy Object in an OU

For the sake of learning and working through the rest of the examples in this section, you'll be creating a new Group Policy object in the Human Resources OU.

This Group Policy object will remove the ability to create new scheduled tasks using the Scheduled Tasks applet in Control Panel for all the Windows 2000 machines in the Human Resources OU.

NOTE The same setting exists under the User Node, but we'll be experimenting with the Computer Node policy.

First, you'll need to create the new Group Policy object and modify the settings. Then, you'll need to move some client machines into the Human Resources OU in order to see your changes take effect.

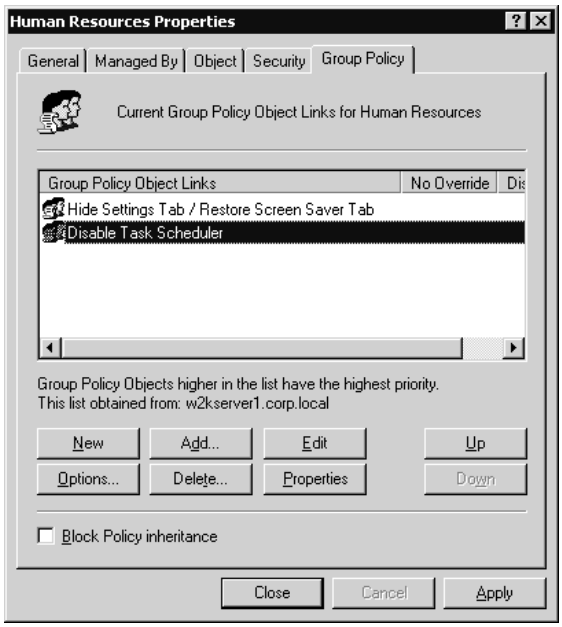
To disable the ability to use the Task Scheduler for the Human Resources OU computers, follow these steps:

1. Log off as the Administrator on W2KServer1 and back on as Frank Rizzo, the Human Resources OU Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.

NOTE If the Administrative Tools are not present, you'll need to click Start ➢ Run and type **mmc** to load a "naked" MMC. Then load in Active Directory Users and Computers.

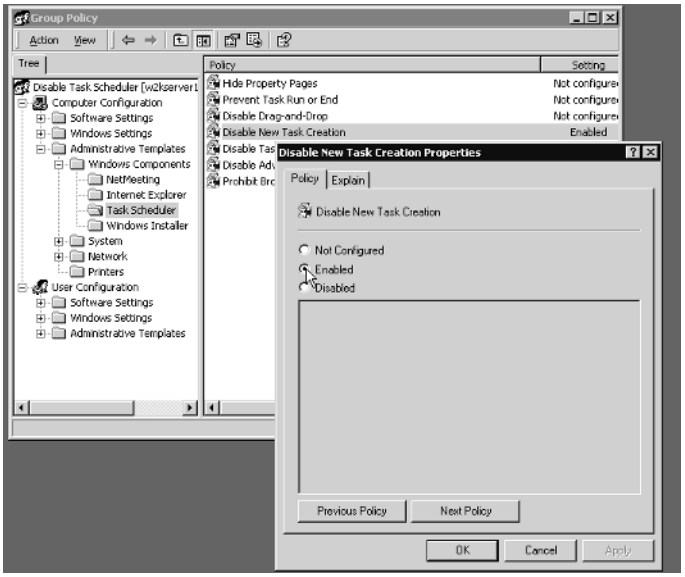
3. Drill down until you reach the Human Resources OU, right-click it, and select Properties. The Human Resources Properties page appears.
4. Select the Group Policy tab, then click New in the Group Policy tab and name the policy something descriptive, such as "**Disable Task Scheduler**," as shown in Figure 1.14.

Figure 1.14 Create your second Group Policy object in the Human Resources OU.



5. Once the name is entered, highlight the policy and click Edit. The Group Policy editor should appear.
6. To disable the Task Scheduler, drill down to Computer Configuration ➢ Administrative Templates ➢ Windows Components ➢ Task Scheduler and double-click the "Disable New Task Creation" entry. Change the setting from "Not Configured" to "Enabled," and click OK as shown in Figure 1.15.

Figure 1.15 Remember—you're "Enabling" the fact that you're *disabling* the Task Scheduler.



7. When back at the Group Policy editor screen, close it to return to the OU Properties screen. Close that as well. You can leave Active Directory Users and Computers open if you desire.

Moving Computers into the Human Resources OU

Since you just created a policy that will affect computers, you'll need to place a workstation or two inside the Human Resources OU to see the results of your labor.

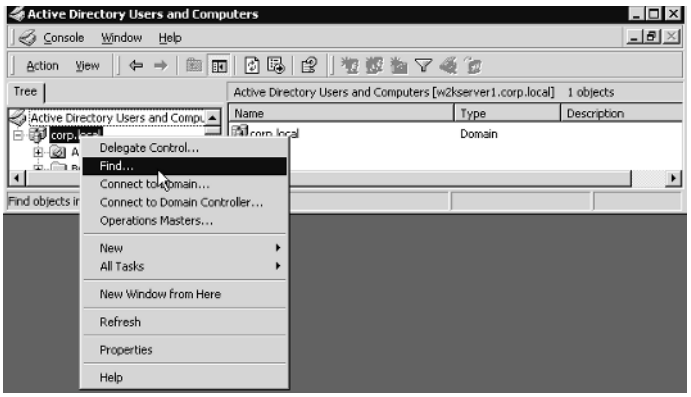
> ***TIP*** Quite often computers and users are relegated to separate OUs. That way, certain policies can be applied to certain computers, but not others. For instance, isolating laptops, desktops, and servers is a common practice.

In this example, we're going to use the Find command in Active Directory Users and Computers to find a workstation named W2KPro1 and move it into the Human Resources OU.

To find and move computers into a specific OU, proceed as follows:

1. In Active Directory Users and Computers, right-click the domain, and click Find as shown in Figure 1.16.

Figure 1.16 Use the Find command to find computers in the domain so you can move them.



2. The "Find Users, Contacts and Groups" screen appears. Pull down the Find drop-down and select Computers. In the Name field, type in **W2KPro1** to find the computer account of the same name. Once you've found it, right-click the account and click Move. Move the account to the Human Resources OU.

Repeat for all other computers that you wish to move to the Human Resources OU.

Verifying Your Cumulative Changes

At this point, you've set up three levels of Group Policy:

- Site—"Hide Screen Saver Tab" for users
- Domain—"Hide Appearance Tab" for users
- Human Resources OU—"Hide Settings Tab" for users, "Restore Screen Saver Tab" for users, and "Disable New Task Creation" for computers

To see the accumulation of your policies, you'll need to log on as a user who is affected by the Human Resources OU and a computer affected by the Human Resources OU. Therefore, log in as Frank Rizzo on W2KPro1.

Traverse to Control Panel ➢ Display and note that the Settings tab is still missing from the previous exercise (and the Screen Saver tab is restored), and now the "Add Scheduled Task" icon is missing from inside the Scheduled Tasks applet.

This test proves that even OU administrators are not automatically immune from their own policies. This is because they are in the "Authenticated Users" security group. You can modify this behavior by exploring the "Filtering Group Policy Application" section later.

TIP Again, don't panic if you do not see the changes reflected right away. See the later section "Forcing Background Processing with SECEDIT" for more on encouraging changes to occur.

How Group Policies Are Processed

Group Policies are not always dropped upon the target machines "right away" after a policy is changed in the editor. Rather, the policies are processed at specific times, depending on where they reside.

Initial Policy Processing

Recall that each policy has two halves, a Computer half and a User half. The Computer half of the policy is always processed at the target machines upon reboot. When Windows 2000 is starting up it will state that it is "Processing security policy." At that time the workstation figures out which site it belongs to, which domain it belongs to, and which OU it is in, and processes the Group Policies in that order. When the processing is finished, the user is prompted to log on.

The User half of the policy is always processed at logon time. The first Domain Controller to validate the user determines which site the user and computer are in and which domain and OU the user belongs to. The Group Policies are then processed in that natural order of site, domain, then each nested OU.

Background Policy Processing

Once the initial policies are processed, either at reboot time for computers, or at logon time for users, what happens when an administrator adds or changes a policy? What if something is modified in the Group Policy editor that should affect a user or computer?

When this happens, the new changes (and only the new changes) are reflected upon the user or computer that should receive them. But this delivery doesn't happen immediately, rather they are delivered according to the background interval.

The *background interval* dictates how often newly changed policies will be delivered. There are different background intervals for different machine types.

Background Intervals for Workstations and Member Servers

By default, the background interval for workstations and member servers is 90 minutes, with a 30 minute plus or minus random differential added to the mix to ensure that no gaggle of PCs will refresh at any one time and clog your network. Therefore, a new change in the Group Policy editor could take as little as 60 minutes or as long as 120 minutes for each user or workstation that is already logged on.

The background interval can be changed using Group Policy as described later in the section cleverly entitled "Using Group Policy to Affect Group Policy."

TIP You can prevent an individual Computer from asking for the background refresh by hacking `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system`, adding a key `DisableBkGndGroupPolicy` and giving it a value of 1.

Background Intervals for Domain Controllers

Domain Controllers in Windows 2000 are a bit special, and they are handled as such. Because Group Policy contains sensitive security settings (e.g. Password and Account Policy, Kerberos Policy, Audit Policy) any policy geared for a Domain Controller is refreshed within five minutes. This adds a tighter level of security to Domain Controllers. For more information, see the later section, "The Two Default Group Policies."

The background interval for Domain Controllers can be changed using Group Policy (as described later in the section entitled "Using Group Policy to Affect Group Policy.")

Policies Exempted from Background Refresh

There are some policies, however, that are not ever affected by background processing:

For instance, Folder Redirection (explored in detail in Chapter 6) is one of those policies. Folder Redirection's goal is to anchor specific directories, such as the My Documents folder, to certain network sharepoints. This policy is never refreshed during a background refresh. The logic behind this is that if an administrator changes this location while the user is using it (and the system responds), the user's data could be at risk for corruption. If Folder Redirection is changed by the Administrator via Group Policy, this change will only take affect for the user at next logon.

Software Installation (explored in detail in Chapter 7) is another policy which is exempt from background refresh. You can use Group Policies to send down software packages, large and small, to your users. You can also use Group Policies to revoke distributed packages. But the software deployed using Group Policies' Software Installation is prevented from being yanked out from under users while they are currently *running* the package. If a package is revoked, it will only be removed upon next logon or reboot.

Additionally, Logon, Logoff, Startup and Shutdown scripts are not run when the background processing interval comes around. They are only run at the appointed time (i.e., at logon, logoff, startup or shutdown).

Forcing Background Processing with SECEDIT

Sometimes, you may wish to bypass the normal "wait time" before background processing kicks in. The good news is that you can run a simple command line that will tell the client to bypass the normal background processing interval and request a refresh from the server. The command-line tool is entitled `SECEDIT`. `SECEDIT` can request the refresh of policies from either the User Configuration node or the Computer Configuration node.

There is one major downside to the `SECEDIT` command: it can only be run on the target workstation. In other words, there is no way, from up on high, to say, "Go forth and refresh, all ye users or computers affected by this recent change in policy!" In order to utilize `SECEDIT`, you must physically be present at the target machine and execute the command. Otherwise, you must wait for the background refresh interval to kick in.

NOTE You can independently change the background refresh interval of both the user and computer. See the section "Using Group Policy to Affect Group Policy" later in this chapter.

To request a refresh of policies from the User Configuration node:

1. Open a DOS prompt by typing Start ➢ Run ➢ cmd.
2. Type in **`secedit /refreshpolicy user_policy`**.

To request a refresh of policies from the Computer Configuration node:

1. Open a DOS prompt by typing Start ➢ Run ➢ cmd.
2. Type in **`secedit /refreshpolicy machine_policy`**.

TIP Additional uses of the `SECEDIT` command can be found in Chapter 4, "Security Configuration and Analysis."

By default, only the newly changed policies will be requested from the Domain Controller to the workstation or server.

To bring down all security policies (changed or not) tack on the `/enforce` switch at the end of the command. For instance:

```
secedit /refreshpolicy machine_policy /enforce
```

Normally the /enforce switch is not needed, as the last applied policies are already active on the machine or applied to the user. But, consider the following example: imagine that, via Group Policy, we use the material in Chapter 4 to create a policy that locks down the \winnt\repair directory. For this example, imagine we set the \winnt\repair directory so only Domain Administrators have read-only access.

Then, someone with local administrative privileges on the workstation changes those settings on the \winnt\repair directory to be wide open. Then, the policy that locks down the \winnt\repair directory is scheduled to refresh.

In that instance, the policy thinks it has already sent down the latest version of the policy, but it doesn't know about the nefarious security change the local workstation administrator performed behind its back. The /enforce switch ensures that the latest security settings are always sent to the workstation—even if it doesn't know anything has changed.

Windows.NET Server's new GPUpdate tool

Refreshing policies with SECEDIT requires typing a long command-line string. Microsoft simplified this somewhat in Windows.NET Server by supplying a separate utility for refreshing policies, GPUpdate.

GPUpdate is similar to SECEDIT in that it can refresh either the user or computer policies, or both! The syntax is either GPUpdate/Target:Computer or /Target:User, or just GPUpdate by itself to trigger both.

Additionally, GPUpdate can figure out if newly changed items require a logoff or reboot to be active. For instance, software deployment and folder redirection settings only get processed at next logon time. Therefore, specifying GPUpdate with a /Logoff switch will figure out if something requires a logoff and automatically log you off. If the updated Group Policy object does not require a logoff, nothing happens and the currently logged in user remains logged in.

Similarly, Software Deployment for computers requires a reboot. Therefore specifying GPUpdate with a /Reboot switch will figure out if something requires a reboot, and automatically reboot the computer if necessary. If the updated Group Policy object does not require a reboot, nothing happens.

By default, the /Logoff and /Reboot switches are optional.

Additionally, Group Policy security settings are automatically periodically refreshed upon workstations for just such occasions. Every 16 hours, workstations will ask the Domain Controllers for the latest version of the Group Policy, and apply all the settings, including security.

NOTE You can manually change this security refresh interval by editing the workstation's Registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}\MaxNoGPOListChangesInterval` and adding a `REG_DWORD` signifying the number of minutes to pull down the entire security policy (by default, every 16 hours).

Policy Application via Remote Access or Slow Links

Windows 2000 will, by default, detect how fast the incoming connection is and make a snap judgment on whether or not to put the user and computer through the ritual of Group Policy processing.

If the machine using RAS is TCP/IP based, it is considered "fast enough to process group policy" if the connection is 500Kb or greater. If the connection is deemed "fast enough," Group Policy is to be applied.

Surprisingly, even if the connection is not deemed fast enough, several sections of Group Policy are *still* applied. Both the security settings and Administrative Templates are guaranteed to be downloaded during logon over a RAS connection—no matter what the speed. And there's nothing you can do about it. Additionally, the EFS Recovery Policy and IPSec policies are *always* downloaded over slow links.

WARNING The Group Policy interface suggests that downloading of EFS Recovery Policy and IPSec policies may be switched on or off over slow links. This is not true. (See the note in the "Using Group Policy to Affect Group Policy" section later in this chapter.)

If the user connects using RAS *before* logging in to the workstation (utilizing the "Logon Using Dial-Up Connection" check box), then once the user is authenticated, the security and Administrative Templates policies of the Computer node of the Group Policy object are downloaded and applied to the computer. Then, the security and Administrative Templates policies of the User node of the Group Policy object are applied to the user.

If the user connects using RAS *after* logging in to the workstation (using the "Network and Dial-up Connections" icons), then the security Administrative Templates policies for the user and computer are not applied right away, rather they are applied during the next normal background refresh cycle (every 90 minutes by default).

Other sections of Group Policy are handled as follows during a slow connection:

Internet Explorer Maintenance settings These are *not* downloaded by default over slow links. (This condition is changeable using the information found in section "Using Group Policy to Affect Group Policy" later in the chapter.)

Folder Redirection settings These are *not* downloaded by default over slow links. (This condition is changeable using the information found in the section "Using Group Policy to Affect Group Policy" later in the chapter.)

Scripts (Logon, Logoff, Startup and Shutdown) These are *not* downloaded by default over slow links. (This condition is changeable using the information found in the section "Using Group Policy to Affect Group Policy" later in the chapter.) Note that currently cached scripts are still run.

Disk Quota settings These are *not* downloaded by default over slow links. (This condition is changeable using the information found in the section "Using Group Policy to Affect Group Policy" later in the chapter.) Note the currently cached disk quota settings are still enforced.

Software Installation and Maintenance These are *not* downloaded by default over slow links. Users can choose whether or not to pull down the latest versions of applications at their whim, as detailed in Chapter 7, specifically in the "Using Software Installation and Maintenance over Slow Links" section. Or you can change the default behavior to torture your dial-in users with the corresponding setting described later in this chapter in the section on "Using Group Policy to Affect Group Policy."

Additionally, what is considered "fast enough" can be changed from 500Kb to whatever speed you desire, as detailed in the section "Using Group Policy to Affect Group Policy."

Advanced Manipulation of Group Policy

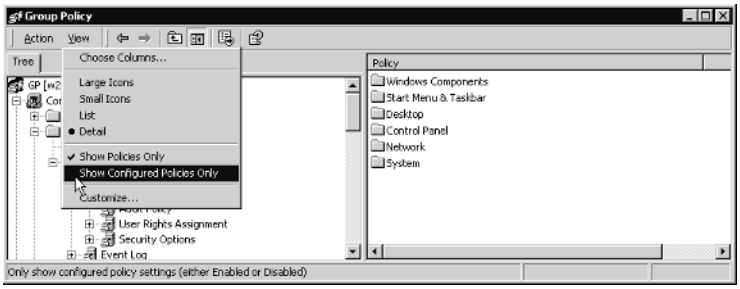
In previous examples we added additional Group Policies to see how, at each level, we were affecting our users. In this section, we'll explore some of the advanced options for applying, manipulating, and using Group Policies.

Using the "Show Configured Policies Only" Option

Sometimes, you just don't know where to start clicking inside the Group Policy editor in order to determine where to modify a previously set setting. The "Show Configured

Policies Only" option, is available in the editor by clicking on the View menu and selecting the "Show Configured Policies Only" setting, as shown in Figure 1.17.

Figure 1.17 "Show Configured Policies Only" only works with the Administrative Template branch.



The good news is that only policies that are enabled or have values will show up, thus making the hunt-and-peck search a little easier. The bad news is that this "Show Configured Policies Only" is only available while browsing the Administrative Templates branch.

By default, this check box is not checked, therefore you can see both configured and unconfigured settings.

NOTE The "Show Configured Policies only" check box is independent for both the Computer and User node settings. Additionally, note that when you close the editor and return, the check box is always cleared.

Filtering Based on OS with Windows.NET Server

The Group Policy Editor console in Windows.NET Server (formally Whistler) permits filtering based on operating system version. For example, you can filter out all policies except those applicable to Windows.NET Server.

Filtering Based on OS with Windows.NET Server *(continued)*

The View filter only works with Administrative Template policies. Other policies are displayed regardless of the applicable platform.

Using the "Show Policies Only" Option

As we'll explore in Chapter 9, "Windows 9*x* and NT System Policies," you can actually use old-style "legacy" NT 4.0 ADM templates inside the Windows 2000 Group Policy editor. Normally, they are "bad" because they don't modify the "correct" portion of the Registry.

In general, this is highly undesirable because most NT 4.0 templates don't act like Windows 2000 Group Policies. NT 4.0 style ADM preferences usually permanently "tattoo" the target machine until the settings are explicitly removed.

NOTE For more on the distinction between "Policies" and "Preferences" with respect to Windows 2000 settings, see the "Policies vs Preferences" section in Chapter 2, "Windows 2000 ADM Templates."

This check box is checked by default, as seen above in Figure 1.17. This gives a gentle persuasion to avoid the importation of old NT 4.0 ADM templates.

TIP You can wisely keep this checkmark permanently checked by using the "Enforce Show Policies Only" setting as described in the "Using Group Policy to Affect Group Policy" section later in this chapter.

Raising or Lowering the Priority of Multiple Policies

As we saw earlier in Figure 1.14, you have created two separate policies that affect the Human Resources OU. You already know the "flow" of Group Policies is inherited from the site level, domain level, then from each nested OU level.

But, additionally, *within* each level, multiple Group Policies are processed from bottom to top, where the topmost policy has the final authority.

In the example in Figure 1.14, the Group Policies would be brought down from the Site definition ("Hide the Screen Saver Tab"), the Domain definition ("Hide the Appearance Tab"), and the OU definitions ("Hide Settings Tab/Restore Screen Saver Tab" and "Disable Task Scheduler"). Windows 2000 will process those two OU level policies from the bottom to the top, therefore the "Disable Task Scheduler" is processed before "Hide Settings Tab/Restore Screen Saver Tab."

In this specific case, we are fortunate because it doesn't really matter in what order they are processed, as the settings that each Group Policy object affects do not overlap. But, should two (or more) Group Policies within the same level contain values for the same policy settings, the settings will be processed from bottom to top, where each consecutive setting overlays (and perhaps overwrites) the previous one.

If you want to change the order of the processing of multiple Group Policies at a specific level, it's an easy task. For instance, suppose you wanted to change the order of the processing such that the "Disable Task Scheduler" is processed after the "Hide Settings Tab/Restore Screen Saver Tab." You would simply click on the policy you wish to process last and click the Up button. Similarly, if you had additional policies you wanted to process first, you would click the policy and click the Down button.

Again—the last applied policy "wins." So the policy at the top of the list is applied last and hence has the "final" say at that level. This is always true unless the "No Override" flag is used (as discussed later).

Disabling Group Policies

After you create your hierarchy of Group Policies that apply to your users and computers, you may wish to occasionally disable one of them temporarily—usually because some user is complaining that something is wrong.

You can disable a specific Group Policy object in several ways.

First, you can wholly disable a specific Group Policy object—such as the "Hide Settings Tab/Restore Screen Saver Tab" Group Policy object we created at the Human Resources OU level. Moreover, recall that each Group Policy object has two "halves"—User and Computer.

The second way to disable a specific Group Policy object is by disabling just one half of a Group Policy. Disable both halves, and the entire Group Policy object is disabled.

You might be wondering why you might want to disable just half of a Group Policy object. On the one hand, disabling a Group Policy object (or half of a Group Policy object) actually makes startup and logon times a tiny-weeny bit faster for the computer or user, because each Group Policy object you add to the system adds a smidgen of extra processing—either for the user or the computer. Once you disable the unused portion of the Group Policy object, you've shaved that processing time off the startup or logon time. Microsoft calls this "modifying Group Policies for performance."

> ***NOTE*** Don't go bananas disabling your unused half of Group Policy object just to save a few cycles of processing time. Trust me, it's just not worth the headaches figuring out later where you did and did not disable a half of a policy.

On the other hand, disabling half of the Group Policy object makes troubleshooting and usage quite a bit harder, as you might just plumb forget you've disabled half of the policy. Then, down the road, when you modify the disabled half of the policy for some future setting, it won't take effect on your clients! You'll end up pulling your hair out wondering why, once things *should* change, they just don't!

One good reason to disable a specific Group Policy object is in the case where you may wish to manually "join" several Group Policies together into one larger Group Policy object. In the previous example, we may wish to make sure each policy is working as expected. Then, once we're comfortable with the reaction, we can recreate the policy settings from multiple Group Policy objects into another new Group Policy object, and disable the old individual Group Policy objects.

If there are signs of trouble with the new policy, you can always just disable (or delete) the large Group Policy object, and re-enable the individual Group Policy objects to get right back to where you started.

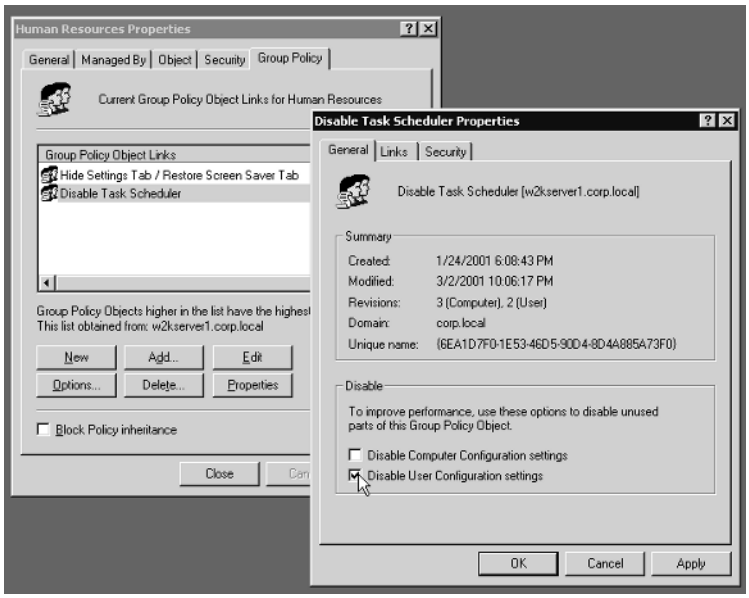
There is still another reason you may wish to immediately disable a new Group Policy object—that is, before you even start to edit it. This helps when you have lots of settings you wish to make in one Group Policy object. Remember that each setting is immediately written inside the Group Policy editor, and computers are continually requesting changes when their refresh interval triggers. The affected users or computers might hit their background refresh cycle and start accepting the changes before you've finished writing all your changes to the Group Policy object! Therefore, if you disable the Group Policy object before you edit and re-enable the policy after you edit, you can ensure that your users are getting all the newly changed settings at once.

This tip works best only when creating new Group Policy objects; if you disable the Group Policy object after creation, there's an equally likely chance that critical settings will be removed while the policy is disabled in the event the refresh cycle should kick in on the client during that time.

To disable an unused half of Group Policy object:

1. Select the Group Policy object you wish to modify. In this case, select the "Disable Task Scheduler" and select the Properties button.
2. Since the "Disable Task Scheduler" modifies only the Computer Node, it is safe to disable the User Node. Click the check box labeled "Disable User Configuration Settings," as shown in Figure 1.18.

Figure 1.18 You can disable half of the Group Policy object to make it load faster.



3. You will be prompted to confirm that the settings in the User Node will be wiped off the target accounts. Choose that you accept.
4. Click OK at the Group Policy Properties page to return to the OU Properties page.

TIP Feel free to repeat the exercise to disable the Computer Node for the "Disable Settings Tab" Group Policy object.

TIP You can disable the entire Group Policy object (both halves) by selecting the Group Policy object, then clicking the Options button and selecting the "Disabled" option.

Block Inheritance

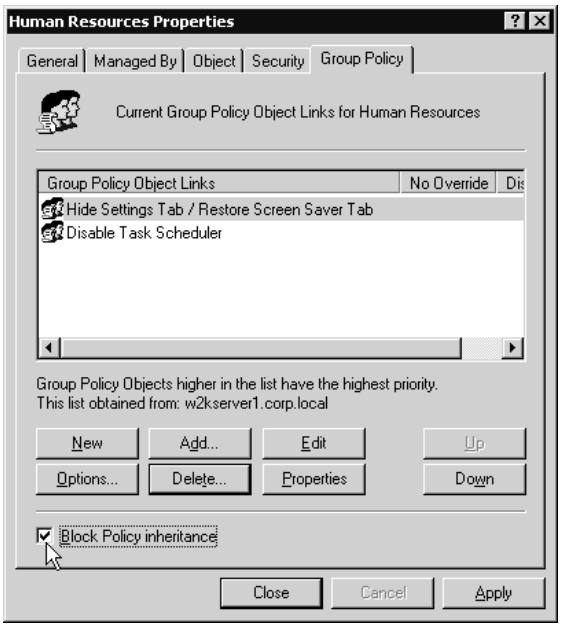
As we've already discovered by example, the normal course of Group Policy inheritance is from the Site to the Domain to each nested OU. A setting at any level automatically affects all levels beneath it.

But perhaps this is not always the desired behavior. For instance, let's say that at the Domain Level, the Domain Administrator has specified that there will be no Appearance tab in the Display settings in Control Panel.

This edict from the Domain Administrator King is fine for most of the OU administrators and their subjects who are affected. But Frank Rizzo, the Human Resources OU Administrator, believes that the folks in his OU can handle the responsibility of the Appearance tab and the Screen Saver tab, and he wants to bring them back to his users. (But, he's not ready to relinquish back the Settings tab.)

In this case, Frank Rizzo can prevent policies defined at higher levels (Domain and Site) from affecting his users. If Frank chooses to select the "Block Inheritance" check box as shown in Figure 1.19, then Frank is choosing to block the flow of *all* policies from *all* higher levels.

Figure 1.19 Use the "Block Inheritance" feature to prevent all policies from all higher levels from affecting your users and computers.



Once the check box is checked and the policies are re-processed on the client, only those settings that Frank dictates at the OU level will be applied.

If you wish to see the effect of "Block Inheritance," click the check box as shown in Figure 1.19. Then, log in as a user affected by the Human Resources OU—say, Frank Rizzo.

When you do, you'll note that the Appearance Tab has reappeared in the Display applet in Control Panel, but the Settings tab is still absent because that policy is explicitly defined at the Human Resources OU level.

No Override

Frank Rizzo and his Human Resources folks are happy that the Screen Saver and Appearance tabs have made a triumphant return. There's only one problem: the Domain Administrator has found out about this transgression, and wants to ensure that the Appearance tab is permanently revoked.

Because the normal flow of inheritance is site, domain, then OU, the Domain policies can trump the "Block Inheritance" definition of the Human Resources OU (or any OU). Likewise site policies can trump domain policies.

To trump a lower level's "Block Inheritance," a higher-level administrator will use the "No Override" function. The idea behind the "No Override" function is simple: it guarantees that settings defined at one level are always inherited by lower levels. It doesn't matter if the lower administrator has blocked inheritance or has a Group Policy object that modifies the same policy setting.

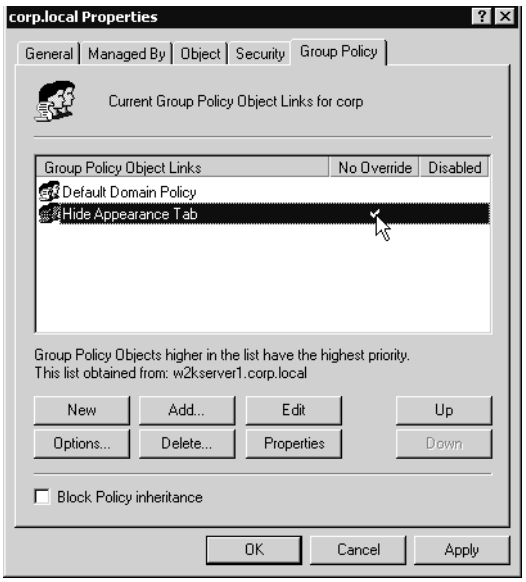
In this example, you'll log in as the Domain Administrator and force the removal of the Appearance tab.

To use "No Override" to force a Group Policy setting, follow these steps:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. Right-click the domain name and click Properties, as seen way back in Figure 1.7.
4. The Properties for the domain appear. Click the Group Policy tab.
5. Select the "Hide Appearance Tab" and click the Options button. Click the option to select "No Override."

Note that the blank area in the "No Override" column next to the "Hide Appearance Tab" definition. A checkmark will appear as shown in Figure 1.20 below.

Figure 1.20 Use the "No Override" check box to guarantee settings contained within a specific Group Policy object affect all users downward via inheritance.



TIP You can double-click the area of the checkmark to add or remove a "No Override" as well. You needn't traverse into the options as we did in Step 5 above.

6. Click OK to close the Domain Properties screen.

To test your "No Override" edict, log in as a user affected by the Human Resources OU—Frank Rizzo. In the Display applet in Control Panel, the Appearance tab should be absent because it is being forced from the "No Override" at the domain level even though "Block Inheritance" is used at the OU level.

Filtering Group Policy Application

The normal day-to-day Human Resources workers inside the Human Resources OU are fine with the facts of life:

- The Enterprise Administrator says that no one at the site will have the Screen Saver tab.
- The Domain Administrator says that no one will have the Appearance tab. He is forcing this edict with "No Override."
- Frank Rizzo, the Human Resources OU Manager says that he will remove the Settings tab, but restore back the Screen Saver tab for his users. For his computers, he'll be removing the Scheduled Tasks icon. Additionally, he will block inheritance to give back the Screen Saver tab removed by the Enterprise Administrator at the Site level. But Frank is forced to live with the fact he won't be able to return to his people the Appearance tab that the Domain Administrator has taken away.

But Frank, and other members of the HR-OU-Admins Security group are getting frustrated that they cannot access the Settings tab. Sure, it was Frank's own idea to make this policy setting, as it affects his users. The problem is, however, it also affects Frank and the other members of the HR-OU-Admins team, and you can see where that can be annoying.

Frank needs a way to "filter" the application of the "Hide Settings Tab/Restore Screen Saver Tab" Group Policy object definition, such that he (and his team) are excluded from the Group Policy application.

Recall from the beginning of this chapter we noted that, bizarrely, Group Policy does not affect Security groups. Remember that you cannot just wrap up a bunch of similar users in a Security group and thrust a Group Policy upon them. You need to round them up into an OU first.

In an even *more* bizarre twist, even though we can't use Security groups to apply Group Policy, it's the Security group that we'll leverage (in most cases) in order to enable us to *filter* Group Policy application!

In order for someone to get Group Policy to apply to them, they need two rights: "Read" and "Apply Group Policy" set on the Group Policy in question. By default all "Authenticated Users" are granted the "Read" and "Apply Group Policy" rights to all new Group Policies. Therefore, everyone can process the policies geared for them by default. With those nuggets of information in mind, there are two ways to approach the goal.

NOTE By default all "Authenticated Users" are granted the "Read" and "Apply Group Policy" to all new Group Policies, because Administrators are members inside of "Authenticated Users" they are affected by Group Policy.

In the first approach, you'll round up only the users, computers, or Security groups who *should* get the policy applied to them. Note that with this approach, you could first remove the default definition that lets the "Authenticated Users" group process the Group Policy. Then, specifically add in the user, computer, or Security groups you want the policy to apply to, and ensure they are granted the "Read" and "Apply Group Policy" rights.

The other approach is to leave the default definition in for the Group Policy object such that "Authenticated Users" are granted the "Read" and "Apply Group Policy." Then, figure out who *should not* get the policy applied to them, and use the "Deny" attribute over the "Apply Group Policy" right.

In either case, when Windows security is evaluated, the designated users are not able to process the Group Policy object, and the policy passes over them.

In this case, we want the "Hide Settings Tab/Restore Screen Saver Tab" Group Policy object to "pass over" our heroes in the HR-OU-Admins security group, but apply to everyone else by default. We'll use the second technique, such that the "Deny" permission ensures that the HR-OU-Admins Security group cannot apply (and hence process) the Group Policy object.

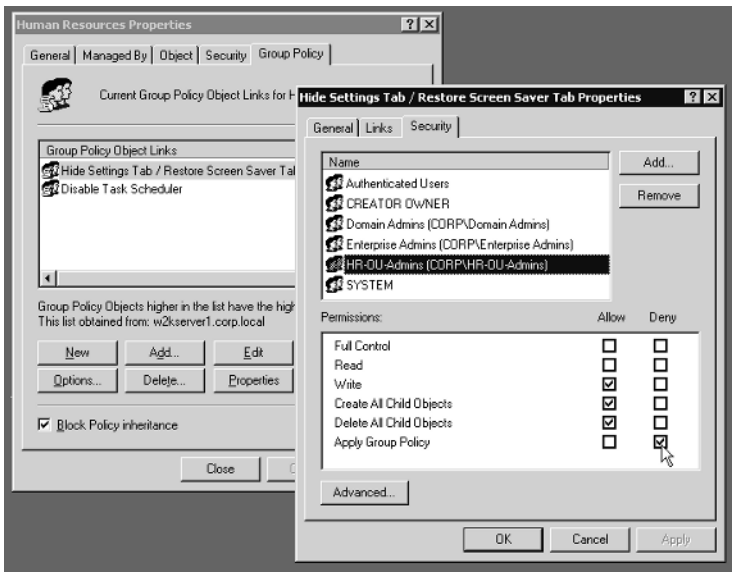
1. Log off as the Administrator on W2KServer1 and back on as Frank Rizzo.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.

NOTE If the Administrative Tools are not present, you'll need to click Start ➢ Run and type `mmc` to load a "naked" MMC. Then load in Active Directory Users and Computers.

3. Drill down until you reach the Human Resources OU, right-click it, and select Properties. The Human Resources Properties page appears.
4. Select the Group Policy tab.
5. Select the "Hide Settings Tab/Restore Screen Saver Tab" policy and select Properties. Select the Security Tab.

6. Because Frank created this Group Policy object, he is specifically listed in the security list. You want to remove Frank and add the HR-OU-Admins group. Click Frank and click Remove. Then click Add, and add the HR-OU-Admins group.
7. Make sure the "Apply Group Policy" check box is set to "Deny" for the HR-OU-Admins group, as shown in Figure 1.21 below.

Figure 1.21 Use the "Deny" bit to prevent Group Policy application.



WARNING Do not Deny the HR-OU-Admins (the group you're currently a member of when logged in as Frank) access over the "Read" or "Write" attribute. If you do, you'll essentially lock yourself out and you'll have to ask for the Domain Administrator's help to grant you access again.

8. Click OK to close the Group Policy settings page.
9. Click OK to close the OU Properties page.

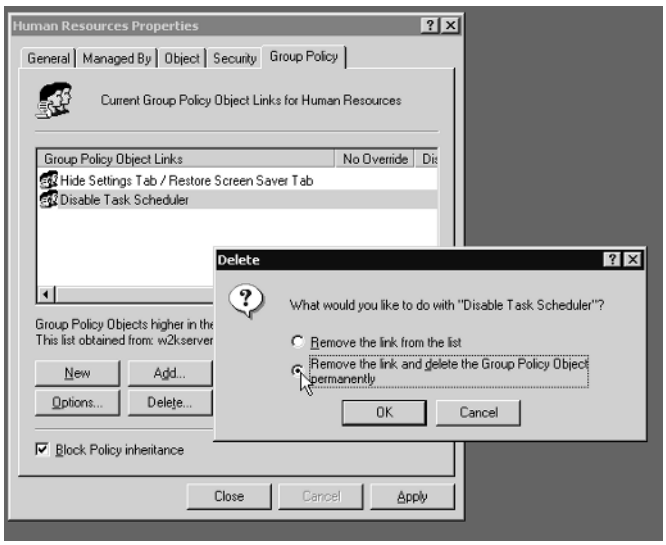
TIP The "Write" permission is the setting which determines who can modify the settings contained with the Group Policy object.

To test your filtering, log in as Frank Rizzo. Note that the Settings tab has returned to him because he is part of the HR-OU-Admins group. The "Hide Settings Tab/Restore Screen Saver Tab" Group Policy object has passed over him because he is unable to process the policy.

Deleting and Unlinking Group Policies

From time to time it will become necessary to delete a Group Policy object. For instance, you may want to return the normal behavior of the Task Scheduler. When you click the Group Policy object and click Delete, you have two options, as shown below in Figure 1.22.

Figure 1.22 You can delete the link, or delete the link and policy altogether.



Recall from the "Understanding Group Policy Linking" section that other levels (site, domain or other OUs) can link to the Group Policies you create. The idea is simple: you design your Group Policy object masterpiece, and someone else gets to hang it on their wall.

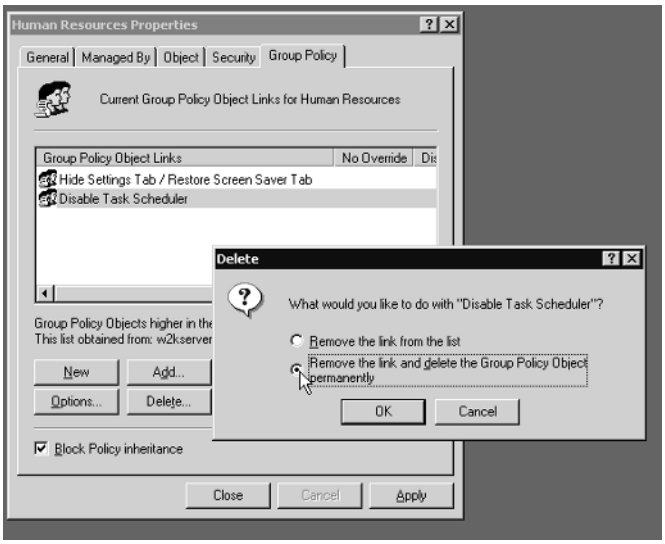
When you choose to delete a Group Policy object, you can choose to stop using it at the level it was created, but keep the opportunity available for other administrators to link to that policy, or you can choose to delete the policy altogether—lock, stock and barrel.

If you delete it altogether, there's only one problem. There is no indication sent to the folks who are linking to this Group Policy object that you've just deleted it altogether.

Thankfully, there's a mechanism built in to the Group Policy object Properties screen to help you determine if anyone else is linked to your Group Policy object.

Before deleting the Group Policy object, select the Group Policy object and click the Properties button. Then select the Links tab, as shown in Figure 1.23 below.

Figure 1.23 Use the Links tab to figure out which other levels may be linked to your Group Policies.



Because the policy could be linked from any domain in the forest, you'll need to manually pull down the domain from which you think someone might have linked and click the Find Now button.

In this case, there are no other levels in any domains linked to the "Disable Task Scheduler" Group Policy object. It is safe to delete. If other administrators from other levels were linking to our Group Policy object, we would probably want to simply choose the first option in Figure 1.22, "Remove the Link from the List," which removes our level's use of the Group Policy object but allows other administrators to continue to link to it.

NOTE For now, don't delete the policy. We'll use it again in later chapters. If you want to play with deleting a policy, create a new one and delete it.

Using Group Policy to Affect Group Policy

There are times when you may wish to change the behavior of Group Policy. Amazingly, you actually use Group Policy settings to affect the behavior of Group Policy!

Several Group Policy Settings appear under both the User and Computer nodes. Recall that, when settings overlap, that the Computer node "wins."

Affecting the User Settings of Group Policy

The Group Policy settings that affect the User node appear under User Configuration ➢ Administrative Templates ➢ System ➢ Group Policy. Remember that user accounts must be subject to the site, domain, or OU where these policies are executed, in order to be affected.

Group Policy Refresh Interval for Users

This setting changes the default User node background refresh rate of 90 minutes with a 30 minute randomizer to almost any number of refresh and randomizer minutes you choose. Choose a smaller number for the background refresh to make Group Policy happen faster on your machines or a larger number to quell the traffic a Group Policy refresh takes across your network. There is a similar refresh interval for computers, which is on an alternate rate and randomizer. A setting of 0 is equal to seven seconds. Set to 0 only in the test lab.

Group Policy Slow Link Detection

You can change the default definition of "fast connectivity" from 500Kbps to any speed you like. Recall that certain aspects of Group Policy are not applied to machines that are deemed coming in over slow links. This setting specifies what constitutes a slow link for the User node. Note that, independently, it's twin under the Computer node (explored later), also needs to be set to define what is slow for the Computer node. Preferably set these to the same number.

Group Policy Domain Controller Selection

Group Policies are written to the PDC Emulator by default. When users (generally Domain Administrators or OU Administrators) are affected by this setting, they are allowed to write Group Policies to Domain Controllers other than the PDC emulator. (See the "Under the Hood of Group Policies" section in Chapter 3, for more information on this setting and how and why to use it.)

Create New Group Policy Object Links Disabled by Default

When users (generally Domain Administrators or OU Administrators) are affected by this setting, the Group Policies they create are disabled by default. This ensures that users and computers are not hitting the refresh interval and downloading "half finished" policies you are in the process of creating. Enable the policies when finished, and they will download during the next background refresh cycle. This theory is also discussed earlier in the "Disabling Group Policies" section.

Enforce Show Policies Only

When users (generally Domain Administrators or OU Administrators) are affected by this setting, the "Show Policies Only" setting (explored earlier) is forced on. This prevents the importation of old-style NT 4.0 ADM templates, which have the unfortunate side effect of "tattooing" the registry until they are explicitly removed. (See Chapter 2, for more information on using NT 4.0 style ADM templates with Windows 2000.)

Disable Automatic Update of ADM Files

If you've gone through the trouble of adding in old-style NT 4.0 ADM templates, there are two ways use them.

The default behavior is to check the "launching point," that is, the \winnt\INF folder, to see if the NT 4.0 ADM template has been updated. This check for an update occurs, by default, every time you double-click the Group Policy object as if you were going to modify it.

However, if you enable this setting, you're saying to ignore the normal update process, and simply keep on using the ADM template you initially used. In other words, you're telling the system you'd prefer to keep the initial ADM template no matter if a newer one is available or not.

See Chapter 2 for more information on using NT 4.0–style ADM templates with Windows 2000.

Affecting the Computer Settings of Group Policy

The Group Policy settings that affect the Computer node appear under Computer Configuration ➢ Administrative Templates ➢ System ➢ Group Policy. Once computers are affected by these policies, they will change the processing behavior of Group Policy. Remember that computers must be subject to the site, domain, or OU where these policies are executed in order to be affected.

Disable Background Refresh of Group Policy

When this setting is enabled, the affected computer downloads the latest policies for both the user and the computer, according to the Background Refresh Interval—but it doesn't apply them. The policies are applied when the user logs off but before the next user logs on. This is helpful in situations where you want to guarantee that a user's experience stays the same throughout the session.

Apply Group Policy for Computers Asynchronously During Startup

Normally, all computer policies are applied to computers when they start up, and before the user is given the opportunity to press Control+Alt+Delete to log on.

By enabling this setting, you're allowing the user to log on, perhaps before the policies have finished downloading to the computer. Indeed, the computer policies will simply be downloaded as fast as possible—perhaps before or perhaps after the user is fully logged on.

This can speed up the time it takes for a computer to start up, and hence, how fast the user is given the opportunity to press Control+Alt+Delete to log on. But, once they do log on it could confuse your users when the settings inside policies start changing the environment around the user as they are inherited from level to level.

Apply Group Policy for Users Asynchronously During Startup

Similar to the preceding policy, a user's logon time is reduced, but the change could confuse your users when the settings change once they are fully logged on. Normally, Group Policy objects are processed in the natural order, so this isn't a problem.

Group Policy Refresh Interval for Computers

This settings changes the default Computer node background refresh rate of 90 minutes with a 30 minute randomizer to almost any number of refresh and randomizer minutes you choose. Choose a smaller number for the background refresh to make Group Policy happen faster on your machines, or a larger number to quell the traffic a Group Policy refresh takes across your network. There is a similar refresh interval for the Users node, which is on an completely separate and unrelated timing rate and randomizer. A setting of 0 is equal to seven seconds. Set to 0 only in the test lab.

Group Policy Refresh Interval for Domain Controllers

Recall that Domain Controllers are updated regarding Group Policy changes within five minutes. You can close or widen that gap as you see fit. Note that the closer the gap, the more network chatter. Widen the gap, and the security settings will be inconsistent

until the interval is hit. A setting of 0 is equal to seven seconds. Set to 0 only in the test lab.

User Group Policy Loopback Processing Mode

We'll explore this setting separately with an example in the next section.

Group Policy Slow Link Detection

You can change the default definition of "fast connectivity" from 500Kbps to any speed you like. Recall that certain aspects of Group Policy are not applied to those machines that are deemed to be coming in over slow links. Note that, independently, its twin under the User node (explored earlier), also needs to be set to define what is slow for the User node. Preferably, set these to the same number.

Registry Policy Processing

This setting affects your Administrative Templates subtrees (and any other policy that affects the Registry).

Once it's set, you have two options:

- The "Do Not Apply During Periodic Background Processing" is a safety measure to help prevent an application from receiving the latest copy of a change inside Administrative Templates. For instance, in Chapter 2, we'll use an Administrative Template to turn off the Grammar checker in Word 2000. If this is set, users won't get the change we dictate until the next time they log on.
- The "Process Even If the Group Policy Objects Have Not Changed" option corresponds to enabling the `/enforce` switch that we explored earlier in the "Forcing Background Processing with SECEDIT" section. It updates and reapplies the policies even if the policies have not changed. Recall that this type of processing is meant to "clean up" should a user have nefariously gone around our backs and modified a local setting.

TIP You cannot turn off Registry policy processing over slow links. They are always downloaded and applied.

Internet Explorer Maintenance Policy Processing

Once set, this policy has three settings:

- The "Allow Processing Across a Slow Network Connection" can be turned on or off to determine if Internet Explorer Maintenance settings should download when logging in over slow links. Enabling this could cause your users to experience a longer logon time.

- The "Do Not Apply During Periodic Background Processing" is similar to the experience we saw earlier. The policies are downloaded but not applied until the user next logs on.
- The "Process Even If the Group Policy Objects Have Not Changed" option corresponds to enabling the `/enforce` switch that we explored earlier in the "Forcing Background Processing with SECEDIT" section. Again, it updates and reapplies the policies even if the policies have not changed.

Software Installation Policy Processing

By default, software deployed using Group Polices is not shot down to the user over slow links. This is a good thing, as I doubt your users will like you very much if you try to deploy Office 2000 over a 56K dial-up line. Use this setting to change this behavior.

Once set, this policy has two settings:

- The "Allow Processing Across a Slow Network Connection" can be turned on or off to stipulate whether applications using IntelliMirror's software deployment features should be downloaded when logging in over slow links. Enabling this could cause your users to experience a very painful logon time.
- The "Process Even If the Group Policy Objects Have Not Changed" option corresponds to enabling the `/enforce` switch that we explored earlier in the "Forcing Background Processing with SECEDIT" section. Again, it updates and reapplies the policies even if the policies have not changed.

NOTE Users can still opt to download software over slow links. See all of the Software Installation settings which are described in detail in Chapter 7.

Recall that Folder Redirection policy is only changed at logon time. Chances are, you wouldn't want dialed-in users to experience that new change. Rather, you would want to wait until they are on your LAN. If you want to torture your users and allow them to accept the changed policy anyway—use this setting to change this behavior.

NOTE Folder Redirection settings are discussed in detail in Chapter 6.

Scripts Policy Processing

Recall that, by default, Startup, Shutdown, Logon and Logoff scripts are not downloaded and run over slow networks. (Also recall that scripts are not re-run again during the background refresh.) With this policy, however, you can force the scripts to execute over a slow link. You can also allow the latest scripts to be downloaded (but not re-run) during the background refresh.

Security Policy Processing

Recall that the security settings are refreshed on the machines every 16 hours, whether they need it or not. This setting is analogous to running the `SECEDIT` command with the `/enforce` switch set, as we covered earlier in the "Forcing Background Processing with SECEDIT" section.

Recall that savvy users may hack into the local Group Policy change a security setting unbeknownst to our system. If this check box is checked, those settings specified by you will be automatically cleaned up.

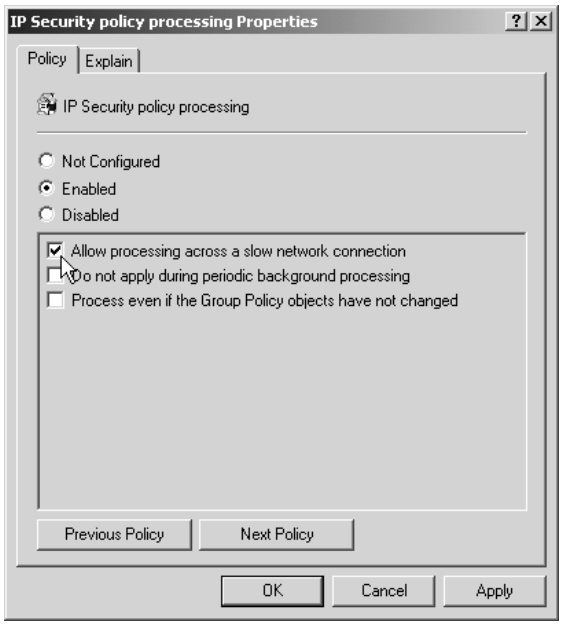
IP Security Policy Processing

IP Security settings are *always* able to download, whether or not the computer is coming in over a slow network. So, you might be asking yourself what the "Allow Processing Across a Slow Network Connection" check box does in Figure 1.24. Answer: Nothing—it's a bug in the interface.

As of Service Pack 2 for Windows 2000, this is simply an interface bug that does nothing when you check or uncheck the check box. Perhaps this will be fixed for Service Pack 3.

To repeat, IP Security is always processed, regardless of the link speed.

Figure 1.24 "Allow Processing across a Slow Network Connection" is not used in Windows 2000 for IP Security or EFS settings.



NOTE Note that IP Security policies act slightly different than other policies. IP Security policies are not "additive" like other policies. For IP Security, the last applied policy wins.

EFS Recovery Policy Processing

EFS settings are *always* available for downloading over slow networks. Like IP Security, the EFS recovery settings are *always* downloaded even over slow networks.

Once again, this is the same bug as shown in Figure 1.24. This does nothing when you check or uncheck the check box.

To repeat, EFS recovery policy is always processed, regardless of link speed.

NOTE Note that EFS Recovery policies act slightly different than other policies. EFS Recovery policies are not "additive" like other policies. For EFS Recovery, the last applied policy wins.

Disk Quota Policy Processing

Once Disk Quotas are applied using Group Policy, they are enforced even over slow links. However, new or updated disk quota settings are not downloaded over slow networks by default. You can force the policy to be downloaded and used over a slow link. You can also exempt this policy from processing during the background refresh.

NOTE Disk Quotas and their corresponding Group Policy settings are discussed in detail in Chapter 6.

Group Policy Loopback Processing

As we've already discovered through example, the normal course of Group Policy application is local computer, site, domain, then each nested OU.

But sometimes it might be necessary to deviate from the normal routine. For instance, you may want all users, whoever they are, to be able to walk up and log on to a specific machine and get the same user node settings. This might be handy in public computing environments, such as libraries, nurses' stations, or kiosks.

If you could round up all the special computers where users need the same user settings into an OU, wouldn't it be keen if you could always force all users to get some of the same settings? Whoever logged into those special computers could get the same Internet

Explorer Settings (such as a special proxy), or different logon script, or certain Control Panel restrictions—just for those workstations.

Reviewing Normal Group Policy Processing

Recall that sometimes computers and users can each be relegated into different OUs. They needn't always be so neatly tucked under the same OU heading like we did when we put Frank Rizzo's user account and W2KPro1 in the same Human Resources OU.

Indeed, a user from any other portion of the domain, say the Domain Administrator (or anyone else), could log on to W2KPro1 located under the Human Resources OU. When this happens (for example, the computer and user accounts affected by GPOs are located in different processing locations), the normal behavior is to process the Computer GPOs based on the normal hierarchy then the User GPOs based on the normal hierarchy. This is true just by the rules of time: computers start up, and their policies are processed; users then log on, and their policies are processed.

So, if the Domain Administrator were to sit down at the W2KPro1 machine in the Human Resources OU, the normal course of events would apply the computer policies from the Default-First-Site, then the Corp.com domain, and then, finally, the Human Resources OU. Next, the User GPOs would apply; first from the Default-First-Site, and then only the Corp.com domain (as the Administrator account is not sitting under any OU).

With Group Policy Loopback processing, the rules change. There are two Group Policy Loopback Modes: Merge and Replace.

Group Policy Merge Mode

When computers are subject to Group Policy Merge Mode, Group Policies objects process in the normal way at start up (and background refresh time): Computer Node for site, domain, then for each nested OU.

Then the user logs on, and User Policies are applied to that user in the normal way: Site, Domain, then each nested OU.

But when computers are affected by Group Policy Loopback Merge mode, the system determines where the *computer* account is, and applies another round of *user* node settings—the ones contained in all Group Policies that lead to that computer.

This means the logged on user gets whacked with two different sets of User node policies—one set of User node policies for when they log on, and then another set of User node policies for where the computer account is situated.

The net result is that the user settings from the user's account, and the user settings from the computer account are on par and equal to each other; none is more important than the other, except where they overlap. In that case, the computer settings win, as usual.

Group Policy Replace Mode

When computers are subject to Group Policy Replace Mode, Group Policies process in the normal way at start up (and background refresh time): Computer node for site, domain, then each nested OU.

Then, the user logs on, and User Policies are totally ignored down the food chain for the logged in user.

Instead, the system determines where the *computer* account is, and applies the *User* node settings contained in all Group Policies that lead to that computer.

Therefore, you change the balance of power so all users are forced to heed the User settings based on what is geared for the computer. Confused? Let's generate an example to "unconfuse" you.

In this example, we'll be performing a variety of steps:

- Create a new OU called "Public Kiosk."
- Move a Windows 2000 machine into the Public Kiosk OU.
- Create a new Group Policy object for the Public Kiosk that performs two functions:
  - First, it will totally disable the Display applet in Control Panel.
  - Second, it will perform "Replace Loopback Processing" so all users logging onto the computers in the Public Kiosk OU will be unable to use the Display applet in Control Panel.

To Create a New OU Called Public Kiosk

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. Right-click over the domain name and click New ➢ Organizational Unit. Enter in "**Public Kiosk**" as the name.

WARNING You are creating this new OU on the same level as Human Resources. Do not create this new OU underneath Human Resources.

To Move a Windows 2000 Machine into the Public Kiosk OU

In this case, we'll move a different Windows 2000 Professional machine, W2KPro2 into the Public Kiosk OU:

1. In Active Directory Users and Computers, right-click the domain and click Find, as shown in Figure 1.16.
2. The Find Users, Contacts and Groups screen appears. Pull down the Find drop-down and select Computers. In the Name field, type in W2KPro2 (or other) to find the computer account of the same name. Once you've found it, right-click the account and click Move. Move the account to the Public Kiosk OU.

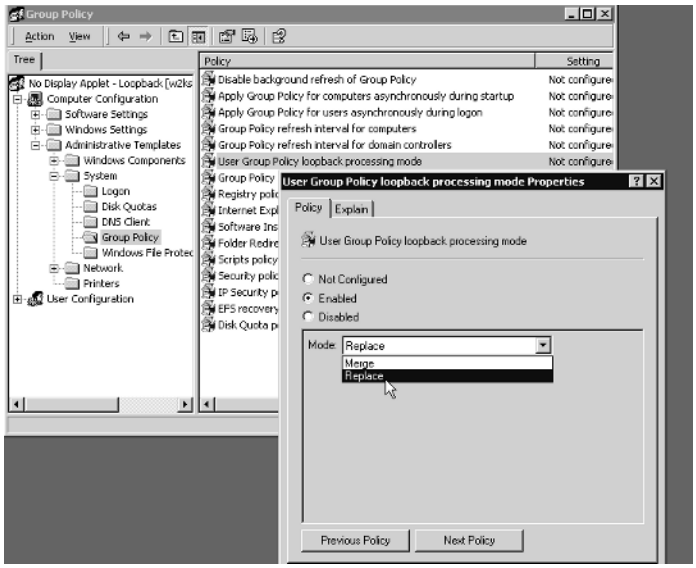
Repeat for all other computers you wish to move to the Public Kiosk OU.

To Create a Policy with Replace Loopback Processing

We want all users who log on to W2KPro2 to have the Display applet disabled. To do this, we need to set two settings on a single Group Policy object: the "Disable Display in Control Panel" and the "User Group Policy Loopback Processing Mode."

1. Right-click the Public Kiosk OU and select Properties The Public Kiosk Properties page appears.
2. Click New in the Group Policy dialog box and name the policy something descriptive, such as **No Display Applet–Loopback Replace**.
3. Once the name is entered, highlight the policy and click Edit. The Group Policy editor should appear.
4. To hide the Settings tab, drill down to User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display and double-click the "Disable Display in Control Panel" entry. Change the setting from "Not Configured" to "Enabled," and click OK as you did with the other policies.
5. To enable loopback processing, drill down to Computer Configuration ➢ Administrative Templates ➢ System ➢ Group Policy and double-click the "User Group Policy Loopback Processing Mode" entry. Change the setting from "Not Configured" to "Enabled," and use the pull-down to select Replace mode, as shown in Figure 1.25.

Figure 1.25 Choose the Loopback Processing mode desired, in this case, "Replace."



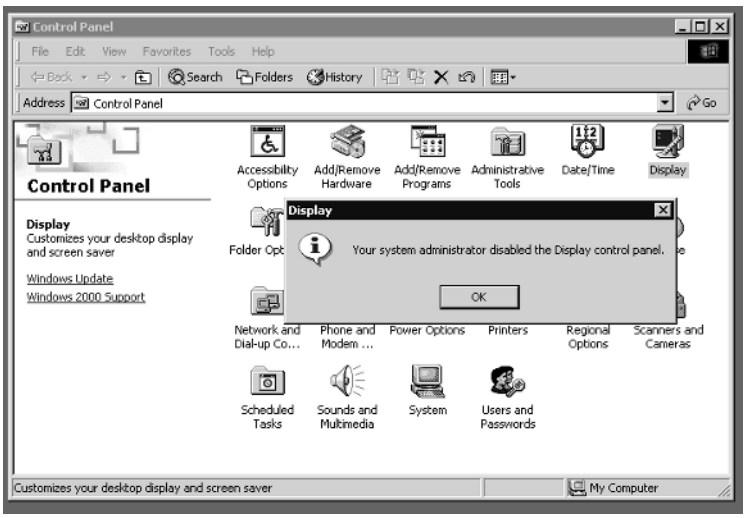
6. When back at the Group Policy editor screen, close it to return to the OU Properties screen. Close that as well. You can leave Active Directory Users and open if you desire.

Verifying That Loopback Policy Is Working

Now, log into any W2KPro2 (or any workstation you moved into the Public Kiosk OU). Since we're using Loopback Policy processing in Replace mode, you can choose any user you have defined—even the Administrator of the domain.

Traverse to Control Panel ➢ Display and note that no one is able to access the Display applet in Control Panel, as shown in Figure 1.26.

Figure 1.26 With Loopback Replace processing enabled, all users are affected by a computer's setting.



TIP Don't panic if you do not see the changes reflected right away. See the earlier section on "Forcing Background Processing with SECEDIT" on how to encourage changes to occur.

Loopback Policy Processing is very powerful, but really is only useful for "specialty" machines. Additionally, you'll need to use it sparingly, as loopback policies are CPU intensive for the client and servers, and difficult to troubleshoot should things go wrong.

Another Practical Use for Group Policy Loopback Replace Mode

I don't know about you, but I just hate it when I walk up to a server and log on. Usually, I have no idea what the server's name, function, IP address, etc could possibly be.

In the NT 4.0 days, I used the following trick:

- First, I would fire up Windows' Paint utility.
- I would create a `.bmp` file that detailed what the name, function, and IP address was. Then, I would save it out as, say—c:\winnt\background.bmp.

Another Practical Use for Group Policy Loopback Replace Mode *(continued)*

- I would then modify the ".default" user profile so, when no one was logged in at the console, the .bmp was displayed. This is done by diving into the registry of the local server and changing HKEY_USERS \.DEFAULT\Control Panel\Desktop\Wallpaper to path of c:\winnt\background.bmp.

But there was one major problem—as soon as I logged onto to the server, the background went away (because my local profile took over) and twenty seconds later, I forgot what the machine's name, function, and IP address were.

With Windows 2000 and the Group Policy Loopback Replace mode policy, I've discovered a very cool trick; you can now force the same background .bmp for every user who physically logs on to any given machine.

The idea is simple:

- Create the .bmp file as above and store it once again, locally, as c:\winnt\background.bmp.
- Create a new Group Policy object on the Domain Controllers OU or on your own OU for your servers. Call the policy "Forced Background Wallpaper—Loopback Replace."
- Modify the User node of the policy as follows:
  1. Drill down into User Node ➢ Administrative Templates ➢ Desktop ➢ Active Desktop ➢ Enable Active Desktop, and set to "Enabled."
  2. Drill down into User Node ➢ Administrative Templates ➢ Desktop ➢ Active Desktop ➢ Active Desktop Wallpaper, and set to "Enabled." Set the wallpaper name to c:\winnt\background.bmp.
  3. Drill down into User Node ➢ Administrative Templates ➢ Desktop ➢ Active Desktop ➢ Allow Only Bitmapped Wallpaper, and set to "Enabled."
- Modify the Computer node of the policy as follows:
  1. Drill down into Computer Node ➢ Administrative Templates ➢ System ➢ Group Policy ➢ User Group Policy Loopback Processing Mode, and set to "Enabled" and "Replace."

Now, whenever anyone logs on to that server, they will get the exact same background .bmp! This is still true even if they usually get a background dictated via some other Group Policy for their own personal account!

Another Practical Use for Group Policy Loopback Replace Mode *(continued)*

There is one more accompanying tip to seal the deal. If you've enabled Terminal Services Administration mode, you cannot, by default, see the wallpaper when coming in over Terminal Services. Change the default behavior of Terminal Services by using the Terminal Services configuration application, right-clicking over the RDP protocol, and selecting the Environment tab. Choose to view the wallpaper by deselecting the "Disable the Wallpaper" check box.

The Two Default Group Policies

Whenever a new domain is created, three things automatically happen. First, the initial (and only) OU, called "Domain Controllers," is created automatically by the system. Next, a default Group Policy object is created for both the Domain itself and the Domain Controllers OU. These are called "Default Domain Policy" and "Default Domain Controllers Policy" respectively.

These two policies are special. First, they cannot be easily deleted (though they can be renamed). Next, each default Group Policy object generated by the system contains a special property that doesn't quite act like the Group Policies that we mere mortals can create.

NOTE The Default Domain Policy and Default Domain Controller policy can actually be deleted, but it is highly unrecommended. If you truly wish to delete either of the Default policies, you'll need to add back in the "Delete" Access Control entry to a group you belong to, Domain Administrators for instance.

In all the previous examples, we saw how the settings at one level trickled down through all the remaining levels. For these policies, this is not the case—they defy the laws of nature.

Default Domain Policy

It's easy to find the Default Domain Policy.

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.

3. Right-click the domain name and click Properties.
4. The Properties for the domain appear. Click the Group Policy tab.

You can see the Default Domain Group Policy object definition way back at the beginning of the chapter in Figure 1.8.

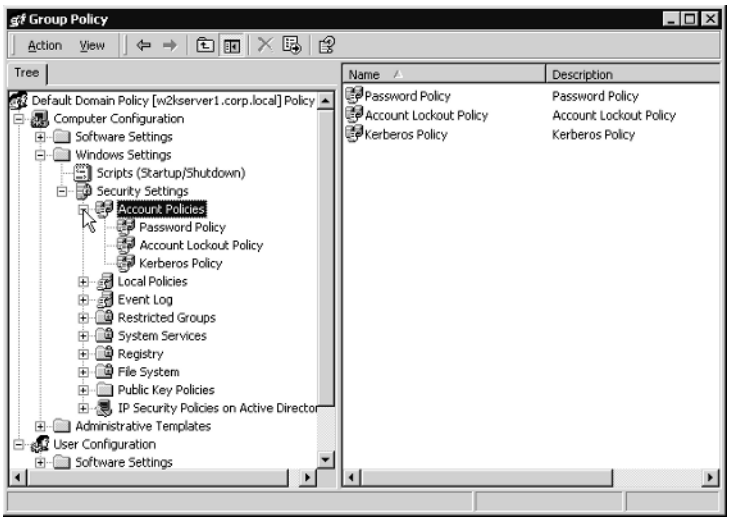
There's an alternate way to get right into the Security settings of the Default Domain Policy. That is, you can:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Domain Security Policy.

You will be immediately placed into the Default Domain Policy focused on the Security settings. These two methods are identical and modify the exact same location.

The Default Domain Group Policy object definition holds three very important domain-wide settings: Password Policy, Account Lockout Policy, and Kerberos Policy, as shown in Figure 1.27.

Figure 1.27 The Account Policies that affect Active Directory users can only be set at the Default Domain Group Policy object. Set them anywhere else, and they are ignored when Active Directory is being used.



For instance, you can specify (among other settings) that the password length is 10 characters, the user is locked out after the third password attempt, and Kerberos ticket expiration time is 12 hours.

The special part about this level of Group Policy is that this is the only place these three policies can be set for the domain. By default, the settings are pre-specified in the Default Domain Policy.

> ***NOTE*** Technically, you could wipe out the Default Domain Policy and create a new policy with these settings. Or, you could add another policy here in the domain and set it with a higher priority than the Default Domain Policy. Doing that takes away the "special nature" of the Default Domain Policy, and is not recommended.

If these are set anywhere else in the domain, at any OU or on any site, the settings are ignored when users log on to the domain; they don't matter and only the ones set up in this Default Domain Policy take effect.

> ***NOTE*** Administrators, however, may additionally choose to set the Password Policy, Account Lockout Policy at an OU level. At first glance this would seem to be counterproductive, because, as already stated, these policies only take hold of the accounts in the domain at the "Default Domain Policy." But Administrators may do this for another reason. That is, when the user logs on *locally* to the Windows 2000 Workstation, the account policy settings at the OU will have been planted on his machine to take effect for *local* accounts.

Microsoft has taken a lot of heat for the fact that account policies must agree for all the accounts in the domain. This means that if two OUs can't agree on account policies, they need to split up into two domains—a major administrative overhead and nightmare.

While you can use the Default Domain Policy for things other than the account policy, it is not recommended. This is because it is, indeed, special, and in case debugging it becomes necessary, only the account policies will have been modified. If you want to add more policies at the domain level—great! But try to leave the Default Domain Policy alone, except where you need to change the account policies.

There are three additional settings that can only be set at the domain level which affect Active Directory users. They are located under Computer ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options:

Automatically Log Off Users When Logon Time Expires When users are logged into the Active Directory, accounts can be set up to forcefully log off when the hours available to log on have passed.

Rename Administrator Account The Administrator account can be renamed using a policy. It only works for the Domain Administrator account when set at the domain level.

Rename Guest Account The domain guest account can be renamed using a policy. It only works for the Guest account when set at the domain level. Hanging them at any other level has no affect on Active Directory computers.

Again, if you wish to use these settings, it is best done so by editing the Default Domain policy and not by adding another Group Policy object at the domain level.

TIP If you modify the Default Domain policy beyond repair, you might have one shot at getting it back to normal. See Microsoft's article entitled "How to Reset User Rights in the Default Domain Group Policy (Q22624)."

Default Domain Controllers Policy

Think of Domain Controllers as all essentially equal. Change the settings on one, and you've changed the settings on all of them. That's where the Default Domain Controllers Policy comes in to play.

It's easy to find the Default Domain Controllers Policy:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Active Directory Users and Computers.
3. Right-click the Domain Controllers OU and click Properties.
4. The properties for the Domain Controllers OU appears. Click the Group Policy tab.
5. The Default Domain Controllers Policy Appears. Click Edit.

All Domain Controllers are affected by all the Security aspects inside the policy, as shown in Figure 1.28.

There's an alternate way to get right into the Default Domain Controller Policy. You can do the following:

1. Log on to the Domain Controller W2KServer1 as a Domain Administrator.
2. Click Start ➢ Programs ➢ Administrative Tools ➢ Domain Controller Security Policy.

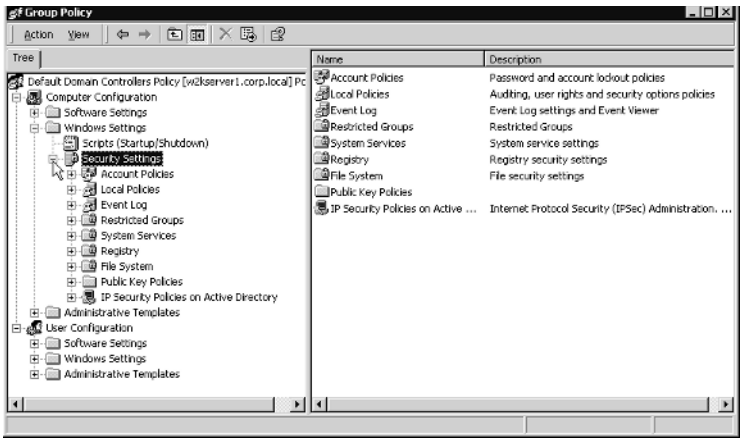
You will be immediately placed into the Default Controller Domain Policy focused on the Security settings.

These two methods are identical and modify the exact same location.

> ***WARNING*** If you use the "Domain Controller Security Policy" to open the security settings, you'll find a tasty bug waiting for you. That is, you *can* drill down to Account Policies ➢ Kerberos Policy, except that this branch doesn't correspond to anything. The *real* Kerberos policies can be found either in the "Domain Security Policy" or in the Default Domain Group Policy object.

You might want to pay special attention to the things that matter most on Domain Controllers: local policies, and the event log settings, as shown below in Figure 1.28.

Figure 1.28 The Default Domain Controllers policy affects every Domain Controller in the domain.



The local policies can dictate the Audit Policies, the User Rights and Assignments (such as who can log on locally to Domain Controllers), and Security Options (such as not displaying the last logged in user).

The event log policy settings allow you to set from up upon high how big the log files can grow and how long they should be retained.

The Default Domain Controllers OU itself has one additional superpower. That is, no matter where a Domain Controller is placed, under any OU, it is still automatically affected by the Group Policy objects placed inside the Default Domain Controllers OU. Therefore, security settings, Administrative Templates—the works, will all locate the Domain Controllers in your domain. You needn't keep your Domain Controllers in the Domain Controllers OU; you can move them anywhere, and the Security settings—say, in the Default Domain Controller Group Policy object—set here will automatically seek out and find all the Domain Controllers in the nooks and crannies of your OUs.

NOTE If you modify the Default Domain Controllers Group Policy object beyond repair, you might have one shot at getting it back to normal. See Microsoft's article entitled "How to Reset User Rights in the Default Domain Controllers GPO (Q267553)."

Things That Aren't Group Policy but *Look* Like Group Policy

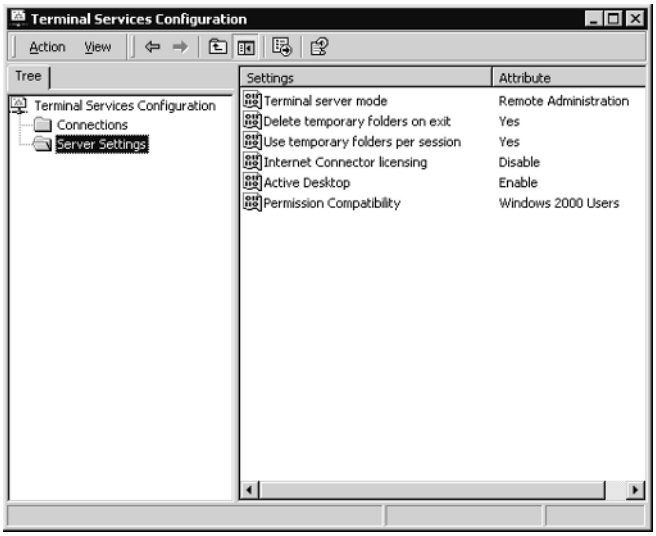
Windows 2000 Server is a big place. There are a lot of nooks and crannies, and occasionally things start to look similar, even though they're unrelated.

Indeed there are two sections inside Windows 2000 that, sometimes, look like they might have some tie-ins to Group Policy. Actually, they're totally separate.

Terminal Services

Windows 2000 Server comes with a built-in Terminal Services service. Each machine must be configured separately using the "Terminal Services Configuration" manager as shown in Figure 1.29.

Figure 1.29 These attributes cannot be set from Group Policy. They must be set in the Terminal Services Configuration manager.



Don't let the little "binary 1/0" icons fool you into thinking they are somehow related to Group Policy. They're not.

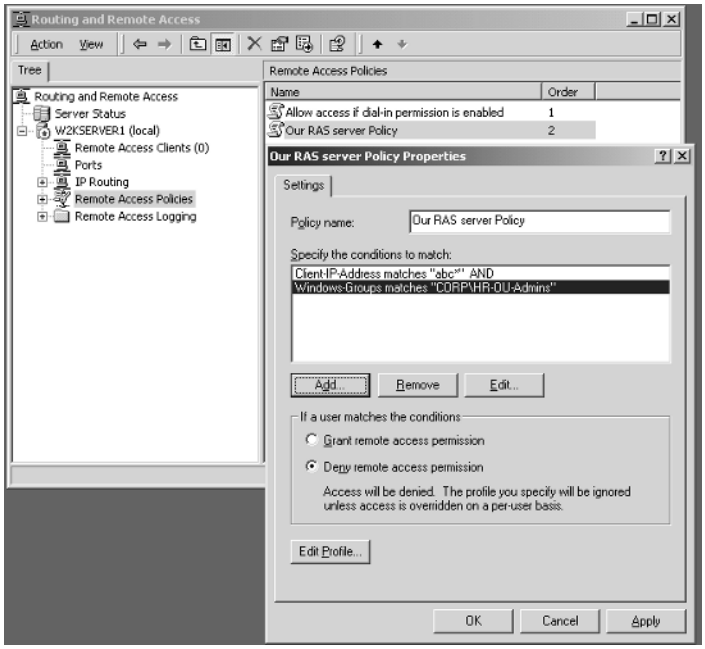
NOTE There is one policy inside Group Policy that does affect Terminal Services. It is located at Computer Configuration ➢ Administrative Templates ➢ Windows Components ➢ Windows Installer and is called "Allow Admin to Install from Terminal Services Session." It is discussed in Chapter 7.

Routing and Remote Access

Routing and Remote Access (or RRAS) allows users to connect to Windows 2000 servers over dial-in or VPN connections, among other functions.

In order to specify who can and cannot get through the gates, Windows 2000 Server has a facility to create "rules" to allow or deny access. Those "rules" are called "Policies," as shown in Figure 1.30.

Figure 1.30 RRAS Policies are not associated with Windows 2000 Group Policies.



Don't let the little "scroll" icons fool you into thinking these are somehow related to Windows 2000 Group Policies. They're not.

Final Thoughts

The more you use and implement Group Policies in your environment, the better you'll become at avoiding pitfalls when it comes to using them. These tips were individually scattered throughout the chapter, but are repeated and emphasized here for quick reference, to help you along your Group Policy journey:

Avoid using the site level to implement GPOs. Users may roam from site to site. When they do, they can be confused by the settings changing around them. Use site policies to set up special site-wide security settings, such as IPSec or the Internet Explorer Proxy. Use the Domain or OU levels to set Group Policies whenever possible.

Implement common settings high in the hierarchy when possible. The higher up in the hierarchy Group Policies are implemented, the more users they

affect. You want common settings to be set once, affecting everyone, instead of having to create additional Group Policies performing the same functions at other lower levels, which will just slow startup and logon times.

Implement unique settings low in the hierarchy. If a specific collection of users is unique, try to round them up into an OU and then apply Group Policy upon them. This is much better than applying the settings high in the hierarchy and using Group Policy filtering later.

Avoid linking to Group Policies in other domains. Policies linked to other domains are inherently slower. Consider copying the settings manually to your own "more local" Group Policy whenever possible.

Use "Block Inheritance" and "No Override" sparingly. The less you use these features, the easier it will be to debug the application of settings. Figuring out at which level in the hierarchy one administrator has "blocked inheritance" and another has declared "no overrides," can eat up days of fun at the office.

Use more Group Policies at any level to make things easier. When creating a new Group Policy, isolate it by creating a new Group Policy object. This will enable easy revocation using the "Disable" command should something go awry and not affect your other Group Policies.

Round up multiple policies into one Group Policy object. Start out in your Group Policy journey by having only one or two settings per Group Policy object. Then use the "Disable" feature to disable the smaller Group Policy objects and concatenate them into one large Group Policy object once you're absolutely sure the settings are working as advertised.

Disable Group Policy objects until finished. When you're creating a new Group Policy object, you don't want your users applying "half finished" Group Policies. Once you are done, enable the Group Policy object and the users and/or computers will apply them during the next background refresh cycle.

Use Loopback processing only for "special" computers and use it sparingly. This take extra processing power and makes things difficult to debug.

Remember Group Policies are notoriously tough to debug. Once you start linking things at multiple levels, throwing a "Block Inheritance," a "No Override," and a filter or two, you're up to your eyeballs in troubleshooting hell. The best thing you can do is document the heck out of your policies. Since there's no quick way to figure out what a specific Group Policy object does just by looking at it, your documentation will be your sanity check when trying to figure things out.