# 1

# Group Policy Essentials



In this chapter, you'll get your feet wet with the concept that is Group Policy. You'll start to understand conceptually what Group Policy is and how it's created, applied, and modified, and you'll go through some practical examples to get at the basics.

The best news is that the essentials of Group Policy are the same in Windows 2000, Windows 2003, and Windows XP. If your Active Directory is a mixture of Windows 2000 or Windows 2000 and Windows 2003, the essentials are all the same. Indeed, if you have a mature Active Directory and think you have a handle on Group Policy essentials, I still encourage you to read and work through the examples in this chapter. With the changes in store, I'm sure you'll find some goodies waiting for you.

If you've done any work at all with Group Policy and Active Directory, you're likely familiar with the "usual" Group Policy interface, which is "in the box." The best news of all, though, is that there's a (free) tool in town, called the GPMC, or Group Policy Management Console. Its goal is to give us an updated, refreshing way to view and manage Group Policy; indeed, this tool enables us to view and manage Group Policy the way it was meant to be viewed and managed. The new GPMC interface provides a one-stop shop for managing nearly all aspects of Group Policy in your Active Directory.

To use the new GPMC tool, it doesn't matter if your entire Active Directory (or individual domains) are Windows 2000 or Windows 2003—it just matters that you have Active Directory.

And did I mention it's free?

Stay tuned, dear reader. We'll get to that exciting new and free stuff right away in this first chapter. I don't want to keep you in suspense for too long.

## Getting Started with Group Policy

In this book, you'll learn about the 13 major categories of Group Policy:

- Administrative Templates (Registry Settings)
- Security Settings (in the Windows Settings folder)
- Scripts (under Windows Settings)
- Remote Installation Services (User node only under Windows Settings)
- Software Installation (Application Management)

- Folder Redirection
- Disk Quotas
- Encrypted Data Recovery Agents (EFS Recovery Policy)
- Internet Explorer Maintenance
- IP Security Policies
- Software Restriction Policies (available for Windows XP and Windows 2003 only)
- Quality of Service (QoS) Policies (available for Windows XP and Windows 2003 only)
- Wireless 802.11 Policies (available for Windows XP and Windows 2003 only)

For a quick reference of where to locate them in this book, just flip to the inside back cover. However, in this first section, you'll learn how to gain access to the interface, which will let you start configuring these categories.

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 XP or Windows 2000 workstation. Officially, this is called a *Local Policy*, but it still resides under the umbrella of the concept of Group Policy. Later, once Active Directory is available, the nonlocal (or, as they're sometimes called, *Domain-Based* or *Active Directory–Based*) Group Policy Objects come into play, as you'll see later. Let's get started and explore both options.

## Understanding Local Group Policy

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

You can begin to edit Group Policy in multiple ways. One way is to load the MMC (Microsoft Management Console) snap-in by hand. You can do so logged on to any workstation or member server (but not a Domain Controller) as a local administrator.


For the examples in this book, we'll do most of the workstation work on one workstation, XPPro1, and most of the Active Directory and server work on one Windows 2003 Domain Controller, WINDC01, in a domain called Corp.com. 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. The ideal configuration for this book is that XPPro1 has XP/SP2, and WINDC01 has Windows 2003/SP1.

To load the Group Policy Object Editor by hand, follow these steps:

1. Choose Start ➢ Run to open the Run dialog box, and in the Open box, type **MMC**. A "naked" MMC appears.
2. From the File menu, choose Add/Remove Snap-in to open the Add/Remove Snap-in dialog box.
3. Click Add.

4. Locate and select the Group Policy Object Editor 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.

You are now exploring the Local Group Policy of this Windows XP workstation. Local Group Policy is unique to each specific machine. To see how a Local Group Policy applies, drill down through the User Configuration folder ➢ Administrative Templates folder ➢ System ➢ Ctrl+Alt+Del Options and select **Remove Lock Computer** as seen in Figure 1.1. Once selected, click Enabled and select OK.

When you do, within a few seconds, you should see that if you were to press Ctrl+Alt+Del, then the "Lock Computer" option should be unavailable.

To revert the change, simply re-select **Remove Lock Computer and select Not Configured. This reverts the change back to the way the operating system works by default.**


You can think of Local Group Policy as a way to perform decentralized administration. A bit later, when we explore Group Policy with Active Directory, we'll saunter into centralized administration.

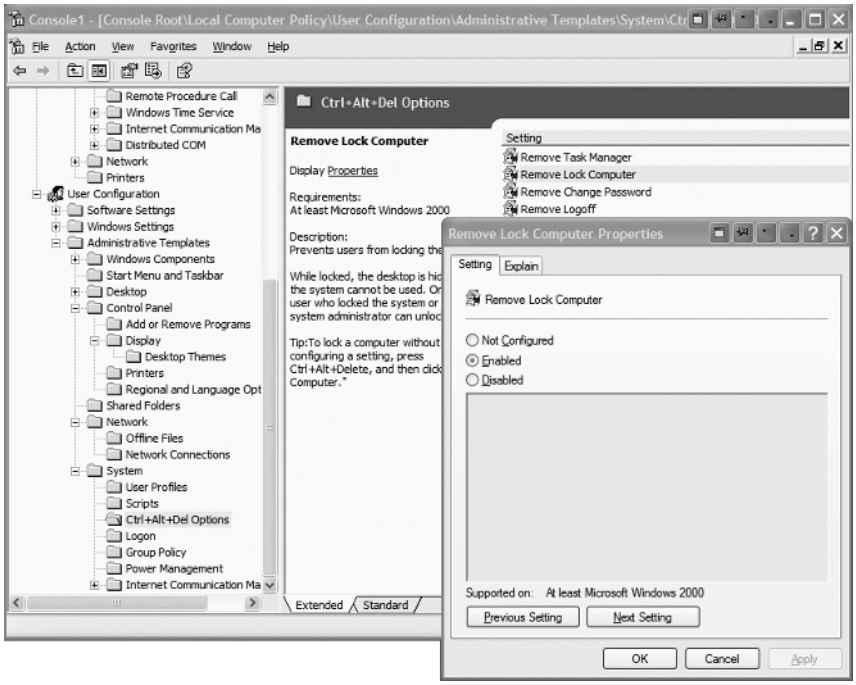
Local Group Policy affects everyone who logs on to this machine—including normal users and administrators. Be careful when making settings here; you can temporarily lock yourself out of some useful functions. For instance, frequently administrators want to remove Run from the Start menu. Then, the first time they themselves want to go to a command prompt, they can't choose Start ➢ Run. It's just gone!


To fix, you have to click the MMC.exe icon in Explorer (or via command line) and manually load the Group Policy Snap-in.

As we stated in the Introduction, most of the settings we'll explore in this book are available to workstations or servers that aren't joined to an Active Directory domain. However, the Folder Redirection settings (discussed in Chapter 9), the Software Distribution settings (discussed in Chapter 10), and Remote Installation Services (discussed in Chapter 11) are not available to stand-alone machines without Active Directory present.


You can also start the Local Group Policy Object Editor by choosing Start ➢ Run to open the Run dialog box and then typing **gpedit.msc** in the Open box. You can point toward other computers by using the syntax `gpedit.msc /gpcomputer: "targetmachine"` or `gpedit.msc /gpcomputer:"targetmachine.domain.com"`; the machine name must be in quotes.

**FIGURE 1.1** Edit a Windows XP Local Group Policy by drilling down into the User Configuration settings.




You can think of Local Group Policy as way to perform desktop management in a decentralized way. That is, you're still running around, more or less, from machine to machine where you want to set the Local Group Policy.

The other strategy is a centralized approach. Centralized Group Policy administration works only in conjunction with Active Directory.

We'll return to other ways to fire up the Group Policy Object Editor—so stay tuned.


Local Group Policy is stored in the `c:\windows\system32\grouppolicy` directory. The structure found here mirrors what you'll see later in Chapter 4 when we inspect the ins and outs of how Group Policy applies from Active Directory.

## Group Policy Entities and Policy Settings

Every Group Policy contains two halves: a User half and a Computer half. This goes for the Local Group Policy that we just saw and for Group Policy objects that are created when we use Active Directory, as you'll see later in this chapter. These two halves are properly called *nodes*, though sometimes they're just referred to as either the *user half* and the *computer half* or the

*user branch* and the *computer branch*. A sample Group Policy Object Editor screen with both the Computer Configuration and User Configuration nodes can be seen in Figure 1.1.

The first level under both the User and the Computer nodes contains Software Settings, Windows Settings, and Administrative Templates. If we dive down into the Administrative Templates of the Computer node, underneath we discover additional levels of Windows Components, System, Network, and Printers. Likewise, if we dive down into the Administrative Templates of the User node, we see some of the same folders plus some additional ones, such as Shared Folders, Desktop, and Start Menu And Taskbar.

In both the User and Computer half, you'll see that policy settings are hierarchical, like a directory structure. Similar policy settings 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.

When manipulating policy settings, you can choose to set either Computer policy settings or User policy settings (or both!). We'll see examples of this shortly. (See the section "Using the Only Show Configured Policy Settings Option" in Chapter 3 for tricks on how to minimize the effort of finding the policy setting you want.)


Most policy settings are not found in both nodes. However, there are a few that overlap. In that case, if the computer policy setting is different from the user policy setting, the computer policy setting overrides the user policy setting.

## Active Directory–Based Group Policy

To use Group Policy in a meaningful way, you need an Active Directory environment. An Active Directory environment needn't be anything particularly fancy; indeed, it could consist of a single Windows 2000 or Windows 2003 Domain Controller and perhaps just one Windows 2000 or Windows XP workstation joined to the domain.

But Active Directory can also grow extensively from that original solitary server. You can think of an Active Directory network as having four constituent and distinct levels:

- The local computer
- The site
- The domain
- The organizational unit (OU)

The rules of Active Directory state that every server and workstation must be a member of one (and only one) domain and 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 Active Directory, administrative responsibility can be delegated using OUs.

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

## Group Policy and Active Directory

When Group Policy is created at the local level, everyone who uses that machine is affected by those wishes. But once you step up and use Active Directory, you can have nearly limitless Group Policy Objects (GPOs)—with the ability to selectively decide which Users and which Computers will get which wishes (try saying that five times quickly). The GPO is the vessel that stores these wishes for delivery.


Actually, you can have only 999 GPOs applied to a user or a computer.

When we create a GPO that can be used in Active Directory, we actually create some brand-new entries within Active Directory, and we automatically create some brand-new files on our Domain Controllers, both of which are known as GPOs.

You can think of Active Directory as having three major levels:

- Site
- Domain
- OU

Additionally, since OUs can be nested within each other, Active Directory has a nearly limitless capacity for where we can tuck stuff away.

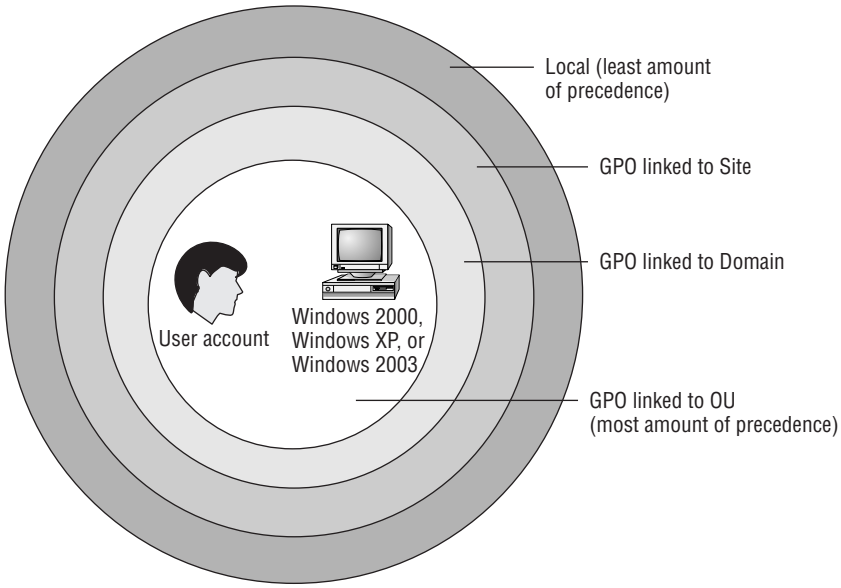
In fact, it's best to think of this design as a three-tier hierarchy: site, domain, and each nested OU. When wishes, er, policy settings, are set at a higher level in Active Directory, they automatically flow down throughout the remaining levels.

So, to be precise:

- If a GPO is set at the site level, the policy settings contained within affect those accounts within the geography of the site. Sure, their user accounts will be in a domain (and/or possibly in an OU), but the account is affected only by the policy settings here because the account is in a specific site.
- If a GPO is set at the domain level, it affects those folks within the domain and all OUs and all other OUs beneath it.
- If a GPO is set at the OU level, it affects those folks within the OU and all other OUs beneath it (usually just called child OUs).

By default, when a policy is set at one level, the levels below *inherit* the settings from the levels above it. You can have "cumulative" wishes that keep piling on.

You might wonder what happens if two policy settings conflict. Perhaps one policy is set at the domain level, and another policy is set at the OU level, which reverses the edict in the domain. The result is simple: Policy settings further down the food chain take precedence. For instance, if a policy setting conflicts at the domain and OU levels, the OU level "wins." Likewise, domain-level settings override any policy settings that conflict with previously set site-specific policy settings. Take a look at the folling graphic to get a graphical view of the order of precedence.




However, one giant caveat should be mentioned at this point. If the Local Group Policy has been set on a specific workstation, everyone logging on to that workstation is affected by that policy setting. Then, the policy settings within Active Directory (the site, domain, and OU) apply. So, sometimes people refer to the *four* levels of Group Policy: local workstation, site, domain, and OU. Nonetheless, GPOs set within Active Directory always "trump" the Local Group Policy should there be any conflict.

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 wants to guarantee that a setting is inherited down the food chain, they can apply the "Enforced" attribute via the GPMC attribute (or "No Override" attribute in the old-school parlance) (Chapter 3 explores both Block Inheritance and Enforced attributes in detail.)


Don't sweat it if your head is spinning a little bit now from the Group Policy application theory. I'll go through specific hands-on examples to illustrate each of these behaviors so that you understand exactly how this works.

## Linking Group Policy Objects

Another technical concept that needs a bit of description here is the "linking" of GPOs. When a GPO is created at the site, domain, or OU level, via the GUI (which we'll do in a moment), the system automatically associates that GPO with the level in which it was created. That association is called *linking*.

Linking is an important concept for several reasons. First, it's generally a good idea to understand what's going on under the hood. However, more practically, the new Group Policy Management Console, or GPMC, as we'll explore in just a bit, displays GPOs from their linked perspective.

You can think of all the GPOs you create in Active Directory as children within a big swimming pool. Each child has a tether attached around their waist, and an adult guardian is holding the other end of the rope. Indeed, there could be multiple tethers around a child's waist, with multiple adults tethered to one child. A sad state indeed would be a child who has no tether but is just swimming around in the pool unsecured. The "swimming pool" in this analogy is a specific Active Directory container named Policies (which we'll examine closely in Chapter 4). All GPOs are born and "live" in that specific domain. Indeed, they're replicated to all Domain Controllers. The adult guardian in this analogy represents a *level* in Active Directory—any site, domain, or OU.

In our swimming pool example, multiple adults can be tethered to a specific child. With Active Directory, multiple levels can be linked to a specific GPO. Thus, any level in Active Directory can leverage multiple GPOs, which are standing by in the domain ready to be used.

Remember, though, unless a GPO is specifically linked to a site, a domain, or an OU, it does not take effect. It's just floating around in the swimming pool of the domain waiting for someone to make use of it.

I'll keep reiterating and refining the concept of linking throughout these first four chapters. And, in Chapter 3, I'll discuss why you might want to "unlink" a policy.

This concept of linking to GPOs created in Active Directory can be a bit confusing. It will become clearer a bit later as we explore the processes of creating new GPOs and linking to existing ones. Stay tuned. It's right around the corner.

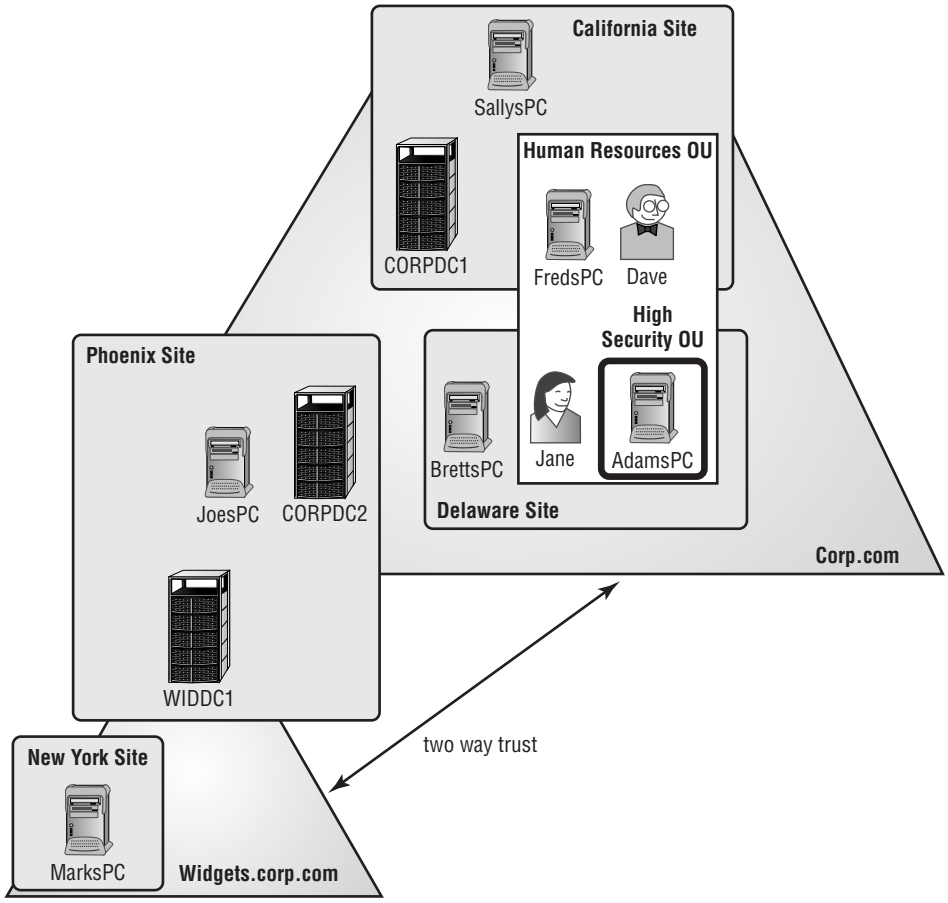
# An Example of Group Policy Application

At this point, it's best not to jump directly into adding, deleting, or modifying our own GPOs. Right now, it's better to understand how Group Policy works "on paper." This is especially true if you're new to the concept of Group Policy, but perhaps also if Group Policy has been deployed by other administrators in your Active Directory.

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

This picture could easily tell 1000 words. For the sake of brevity, I've kept it down to around 200. In this example, the domain Corp.com has two Domain Controllers. One DC, named CORPDC1, 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 can be put in place to regulate communication between CORPDC1 located in California and CORPDC2 located in Phoenix. That way the administrator controls the chatter between the two Corp.com Domain Controllers, and it is not at the whim of the operating system.

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




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, called AdamsPC, inside the **High Security** OU. There is also JoesPC, which is a member of the Corp.com domain. It physically resides at the Phoenix site and isn't a member of any OU.

Another domain, called Widgets.corp.com, 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. Last, there is MarksPC, a member of the Widgets.corp.com domain, which physically resides in the New York site and isn't in any OU.

Understanding where your users and machines are is half the battle. The other half is understanding which policy settings are expected to appear when they start logging on to Active Directory.

# Examining the Resultant Set of Policy

As stated earlier, the effect of Group Policy is cumulative as GPOs are successively applied—starting at the local computer, the site, the domain, and each nested OU. The end result of what affects a specific user or computer—after all Group Policy at all levels has been applied—is called the *Resultant Set of Policy*, or *RSoP*. This is sometimes referred to as the *RSoP Calculation*.

Throughout your lifetime working with Group Policy, you will be asked to troubleshoot the RSoP of client machines.


Much of our dealings with Group Policy will be trying to understand and troubleshoot the RSoP of a particular configuration. Getting a good understanding early of how to perform manual RSoP Calculations on paper will be a useful troubleshooting skill. In Chapter 3 and Chapter 4, we'll also explore additional RSoP skills—with tools and additional manual troubleshooting.

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 happens to the entities contained in them. I'll then bring it all together to see how a specific computer or user reacts to the accumulation of GPOs. For these examples, assume that no local policy is set on any of the computers: The goal is to get a better feeling of how Group Policy flows, not necessarily what the specific end-state will be.

## At the Site Level

Based on what we know from Figure 1.2, the GPOs in effect at the site level are as follows:

| Site | Computers Affected |
|---|---|
| California | SallysPC, CORPDC1, and FredsPC |
| Phoenix | CORPDC2, JoesPC, and WIDDC1 |
| New York | MarksPC |
| Delaware | AdamsPC and BrettsPC |


Users are affected by site GPOs only when they log on to computers that are at a specific site. In Figure 1.2, 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:

| Domain | Computers/Users Affected |
|---|---|
| Corp.com Computers | SallysPC, FredsPC, AdamsPC, BrettsPC, JoesPC, CORPDC1, and CORPDC2 |
| Corp.com Users | Dave and Jane |
| Widgets.corp.com Computers | WIDDC1 and MarksPC |

## At the OU Level

At the organizational unit level, we have the following:

| Organizational Unit | Computers/Users Affected |
|---|---|
| Human Resources OU Computers | FredsPC is in the Human Resources OU; therefore it is affected when the Human Resources OU gets GPOs 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 GPOs applied. |

### Bringing It All Together

Now that you've broken out all the levels and seen what is being applied to them, you can start to calculate what the devil is happening on any specific user and computer combination. Looking at Figure 1.2 and analyzing what's happening at each level makes adding things together between the local, site, domain, and organizational unit GPOs a lot easier.

Here are some examples of RSoP for specific Users and Computers in our fictitious environment:

| | |
|---|---|
| FredsPC | FredsPC inherits the RSoP of the GPOs from the California site, then the Corp.com domain, and then, last, the Human Resources OU. |
| MarksPC | MarksPC first accepts the GPOs from the New York site and then the Widgets.corp.com domain. MarksPC is not in any OU; therefore, no organizational unit GPOs apply to his computer. |

| | |
|---|---|
| AdamsPC | AdamsPC is subject to the GPOs at the Delaware site, the Corp.Com domain, the Human Resources OU, and the High Security OU. |
| Dave using AdamsPC | AdamsPC is subject to the computer policies in the GPOs for 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 GPOs are dictated from the Delaware site, the Corp.com domain, and the Human Resources OU. |


At no time are any domain GPOs from the Corp.com parent domain automatically inherited by the Widget.corp.com child domain. Inheritance for GPOs only flows downward to OUs within a single domain—not between any two domains—parent to child or otherwise.

If you want one GPO to affect the users in more than one domain, you have four choices:

- Precisely re-create the GPOs in each domain with their own GPO.
- Copy the GPO from one domain to another domain (using the GPMC, as explained in the Appendix).
- Use a third-party tool that can perform some magic and automatically perform the copying between domains for you. (Check out `www.GPanswers.com` for a list of tools.)
- Do a generally recognized no-no called *cross-domain policy linking*. (I'll describe this no-no in detail in Chapter 3.)

Also, don't assume that linking a GPO at a site level necessarily guarantees the results to just one domain. In this example, as in real life, there is not necessarily a 1:1 correlation between sites and domains.

# Group Policy, Active Directory, and the GPMC

Windows 2000 administrators already somewhat familiar with Group Policy will tell you that finding what you need and understanding what's going on under the hood can sometimes be confusing. The interface used to create, modify, and manipulate Group Policy in Windows 2000 has led to numerous missteps and head scratching when people try to figure out why something isn't going the way it should.

Occasionally, Microsoft has recognized that the first iteration of a product release has missed the mark a little in the way the product works, acts, or interfaces. They often request additional customer feedback, embrace it, regroup, and return a "2.0 version" of the product.

To make optimal use of Group Policy in an Active Directory environment, the Group Policy team at Microsoft introduced a free, downloadable "2.0 version" for managing Group Policy in Active Directory. It's called the Group Policy Management Console, or GPMC, as mentioned earlier. The GPMC isn't part of the Windows 2000, Windows 2003, or Windows XP operating systems; you need to fetch it and install it.

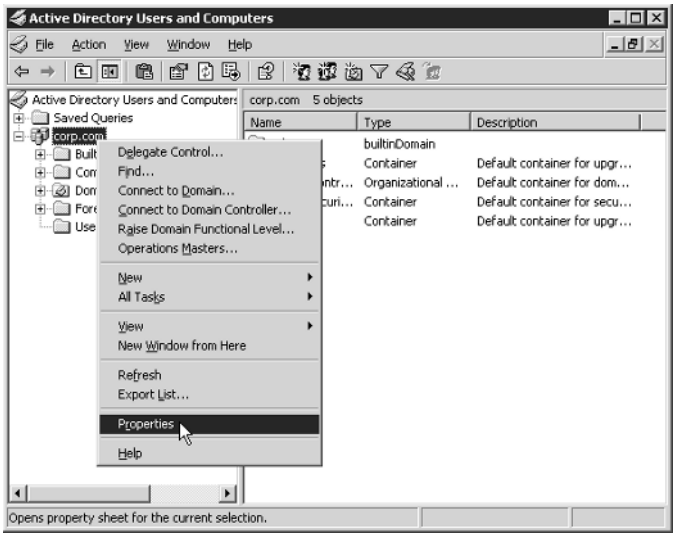
## Kickin' It Old-School

Out of the box, Windows 2000 and Windows 2003 domains use the old-style GPMC interface. If you've never seen the old-style interface, you can do so right now before we leave it in the dust for the new GPMC in the next section.

To see the old-style interface and create your first GPO at the domain level, follow these steps:

1. Log on to the Domain Controller WINDC01 as Domain Administrator.
2. Choose Start ➢ Programs ➢ Administrative Tools and select Active Directory Users And Computers.
3. Right-click the domain name and choose Properties from the shortcut menu, as shown in Figure 1.3, to open the Properties dialog box for the domain.
4. Click the Group Policy tab.

**FIGURE 1.3** Right-click the domain name and choose Properties.



There is a "Default Domain Policy" GPO but you won't modify it at this time. (I'll talk about it in Chapter 6.) As I'll discuss, it is not recommended that you modify the "Default Domain Policy" GPO for regular settings.

5. Click the New button to spawn the creation of your first GPO.
6. For this first example, type **My First GPO**, as shown in Figure 1.4.
7. Highlight the policy, and click Edit to open the Group Policy Object Editor.

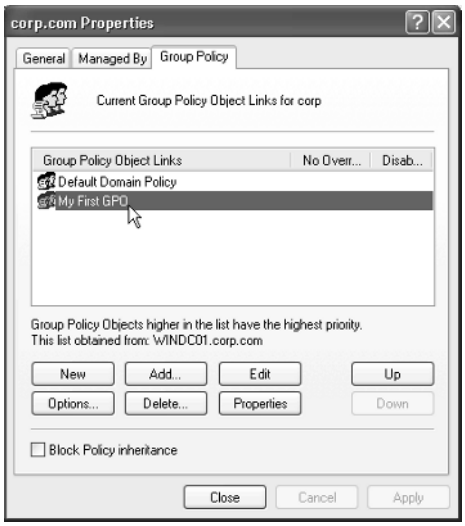
At this point, things should look familiar, just like the Local Group Policy Object Editor, with the user and computer nodes. For example, if you drill down into the Administrative Templates folder in the User Configuration folder, you can make a wish at the domain level, and all your computers will obey.

For now, don't actually make any changes; just close the Group Policy Object Editor and read on.

## GPMC Overview

The GPMC is a tool you download from Microsoft for free, which can then be loaded on Windows XP or Windows 2003 client machines. Once loaded, the GPMC provides a one-stop shop for managing nearly all aspects of Group Policy in your Active Directory. Again, it doesn't matter if your Active Directory or domains are Windows 2000 or Windows 2003; it just matters that you have Active Directory.

**FIGURE 1.4** You've just created your first GPO in Active Directory.



### Why Abandon Old School?

In Figure 1.4, we were able to create our first GPO (even though we didn't actually place any policy settings in there). The interface seems reasonable enough to take care of such simple tasks. And, heck, this interface is already part of the operating system, so, why move away from it?

The old-school way of viewing and managing Group Policy just isn't scalable over the long haul. This interface doesn't show us any relationship between the GPO we just created and the domain it's in. As you'll see in this chapter, the new interface demonstrates a much clearer relationship between the GPOs you create, the links it takes to use them, and the domains where the GPOs actually "live."

The old-style interface also provides no easy way to figure out what's going on inside the GPOs you create. To determine what changes are made inside a GPO, you need to reopen each GPO and poke around. I've seen countless administrators open each and every GPO in their domain and manually document their settings on paper for backup and recovery purposes.

Indeed, backup and recovery is a really, really big deal, and the old-school mechanism (via NTBACKUP) provided no realistic way to back up and recover GPOs without copious amounts of surgery.

With that in mind, I encourage all of you—those currently using the original Windows 2000 old-school way (and those who haven't even yet been to school)—to step up and try the new way of doing things, the GPMC.

Throughout this chapter and the book, I'll give you pointers about what to do if you're still stuck on working with the old-school way of doing things. However, there's little reason to stay old school when the new way has so much to offer. Did I mention that the GPMC is free? (Yes, Jeremy, about 10 times already.)

It's my hope that those of you already familiar with Group Policy will use the examples in this chapter to get comfy with the new GPMC interface. Also, if you're totally new to the concept of Group Policy, I hope you'll keep your eyes forward and don't look back to the old-school way.

Microsoft has made it quite clear that their direction for all future Group Policy efforts, including white papers, TechNet articles, paid phone support, free newsgroup support, Microsoft Official Curriculum, and even future MCSE/MCSA (Microsoft Certified Systems Engineer/ Microsoft Certified Systems Administrator) exams, will be geared with a heavy eye toward the use of the GPMC.

Basically, the GPMC is here to stay; we need to get up to speed with it and embrace it. The good news is that it's quite pleasant to work with and it's powerful to boot. The best news is that it only takes one Windows XP machine to load the GPMC, and it can be used with both Windows 2000 Active Directory and Windows 2003 Active Directory domains.

So enough yakkin' already about the virtues of the GPMC. Let's get going already!

Even though you cannot load the GPMC on a Windows 2000 Domain Controller or a Windows 2000 Professional machine, it's still capable of controlling Windows 2000 domains. Again, the idea is to simply load the GPMC on just one Windows XP machine in your Windows 2000 domain, and you'll be in good company managing your Windows 2000 Active Directory.

The GPMC's name says it all. It's the Group Policy Management Console. Indeed, this will be the MMC snap-in that you use to manage the underlying Group Policy mechanism. The GPMC just helps us tap into those features already built into Active Directory. I'll highlight the mechanism of how Group Policy works throughout the next three chapters.

One major design goal of the GPMC is to get a Group Policy–centric view of the lay of the land. Compared with the old interface, the GPMC does a much better job of aligning the user interface of Group Policy with what's going on under the hood.

The GPMC also provides a programmatic way to manage your GPOs. In fact, the GPMC scripting interface allows just about any GPO operation (other than to dive in and create or modify actual policy settings). We'll explore scripting with the GPMC in Chapter 7. So, if you're interested in scripting, you'll need to have the GPMC bits loaded on the XP systems you want to script.

You'll load the GPMC on the same machines that you use to manage your current Group Policy universe. Some people walk up to their Domain Controllers, log on to the console, and manage their Group Policy infrastructure there. Others use a management workstation and manage their Group Policy infrastructure from their own Windows XP workstations. In either case, to use the GPMC, you'll need to load the GPMC installation software (and the prerequisites) on the machines on which you want this sexy new view to appear. GPMC will only load on Windows XP/SP1 (or greater) and Windows 2003 machines (Domain Controllers and member servers) as discussed in the next section.

I'll talk more about the use and best practices of a Windows XP management workstation in Chapter 5.

## Installing the GPMC

As I mentioned, the GPMC isn't part of the standard Windows 2003 or Windows XP package out of the box. You can, however, download it for free from `www.microsoft.com/grouppolicy`. Click the link for the Group Policy Management Console to locate the download.

Once it's downloaded, the GPMC is called GPMC.MSI. You can install this on either Windows 2003 or Windows XP with at least SP1, but nothing else. That is, you cannot load the GPMC on Windows 2000 servers or workstations; but, as I noted before, the GPMC can manage Windows 2000 domains with Windows 2000 and Windows XP clients as well as Windows 2003 domains with Windows 2000 or Windows XP clients.

### The Original GPMC versus the GPMC with SP1

The GPMC you can download today is called "GPMC with SP1" And it's all good. Not just because of the minor bug fixes, but because of the licensing agreement the GPMC with SP1 provides.

The original GPMC license stipulated that the GPMC was to be loaded only on machines with at least one license of Windows 2003 server on record. However, with GPMC with SP1, that licensing restriction has been lifted. GPMC with SP1 can be used to manage domains without any Windows 2003 servers and without any Windows 2003 Client Access Licenses (CALs).

Therefore, for shops with only Windows 2000, the only requirement is that you have but one Windows XP machine (with at least Service Pack 1) with which to load the GPMC and manage your Active Directory and Group Policy. Oh, and, of course, that one Windows XP client needs a CAL. And that's it.


If you will use the GPMC to manage Windows 2003 domains, all the functionality of the tool is present. If you will use the GPMC to manage Windows 2000 domains, some functionality will not be present. Windows 2003 Active Directory contains several new Group Policy features that Windows 2000 domains cannot use. I'll explicitly explain those features that are not accessible within Windows 2000 domains as they come up. These features are largely explored in Chapter 3.


Additionally, if you have any remaining Windows 2000 Domain Controllers, you should have at least SP2 and preferably SP3 applied to them. This is because most Windows 2003 tools, including the GPMC, use LDAP (Lightweight Directory Access Protocol) signing for all communication. For more information, see the Microsoft Knowledge Base article 325465, "Windows 2000 Domain Controllers Require SP3 or Later When Using Windows Server 2003 Administration Tools."

## Installing the Prerequisites and GPMC Manually

Installing the GPMC does require certain prerequisites, which must be loaded in the order listed here.

### Loading the GPMC on Windows XP

If you intend to load the GPMC on a Windows XP machine to manage Group Policy in your domain, follow these steps:

1. The Windows XP Service Pack 1 is required. If you are unsure whether SP1 (or later) is installed, run the `WINVER` command, which will tell you whether a service pack is installed. So, if your Windows XP system doesn't have at least SP1 installed, you should install it.
2. The GPMC requires the .NET Framework to run properly. If it's not installed, you'll need to download and install it. At last check, the .NET Framework download was at `http://msdn.microsoft.com/netframework/downloads/updates/default.aspx` (shortened to `http://tinyurl.com/ekc7`). If it's not there, search the Microsoft site for ".NET Framework."

   After downloading .NET Framework, double-click the install to get it going on your target Windows XP/SP1 (or greater) machine. It isn't a very exciting or noteworthy installation.
3. To install the GPMC, double-click the GPMC.MSI file you downloaded. If you're running Windows XP with SP1, the GPMC installation routine will report that a hotfix (also known as a QFE) is required and then proceed to automatically install the hotfix on the fly. This hotfix (Q326469) is incorporated into Windows XP's SP2. So, if installing on an Windows XP/SP2 machine, you won't be asked to bother to install it.

### Loading the GPMC on a Windows 2003 Domain Controller

If you intend to load the GPMC on a Windows 2003 Domain Controller or a member server, there are just a couple of things to do:

1. Although there aren't any Windows 2003 prerequisites, it's a good idea to install the latest version of the .NET Framework and the latest version of the Windows 2003.
2. To install the GPMC, double-click the GPMC.MSI file you downloaded.

#### Installing the Prerequisites and GPMC via Group Policy Software Distribution

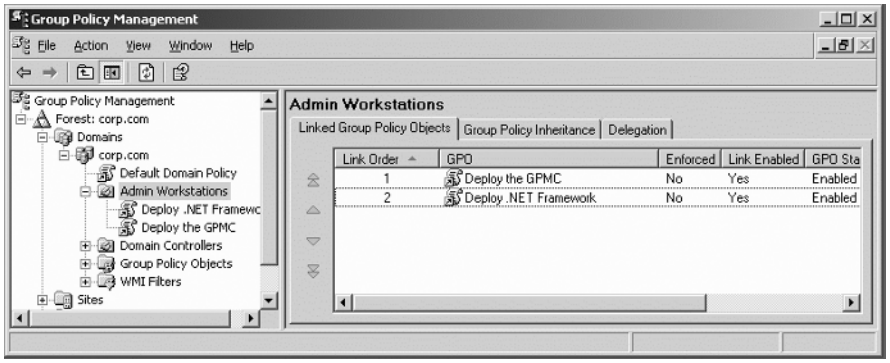
In Chapter 10, you'll learn how to automate your software distribution with Group Policy. Here, however, is a quick reference for how to perform automated installations of the GPMC and its prerequisites. Again, recall that you can load the GPMC only on Windows XP and Windows 2003 machines.

The .NET Framework 1.1 or later must be installed on all target Windows XP machines intended to use the GPMC. And there's no penalty for loading it on Windows 2003 target machines. Download the Redistributable Package (from the Microsoft link described above), expand its contents, and assign the NETFX.MSI to the Windows XP (and/or Windows 2003) machines on which you intend to load the GPMC.

You'll find an expanded discussion on how to deploy the .NET Framework via Group Policy Software Distribution (and also Microsoft SMS) at `http://tinyurl.com/458zj` and, even more specifically, `http://tinyurl.com/772u6`.

You can also assign the GPMC.MSI file itself to either Windows XP or Windows 2003 machines—either member servers or Domain Controllers.

You'll perform the magic in three steps: You'll need to create two GPOs (one that deploys the .NET Framework and another that deploys the GPMC). Then you'll need to order the GPOs so that .NET Framework is deployed *first*. You need to ensure that the GPO which deploys the .NET Framework is set with the highest priority in the link order (confusing, I know.) Stay tuned, we talk about ordering and prioritization of GPOs in Chapter 2.




### Upgrading from NT 4.0 to Windows 2000, Windows 2003, or Windows 2003/ SP1: Cleaning Up Old GPOs

After you run the GPMC, you may be prompted to "clean up" older GPOs the first time you touch one. You should do so. Under the hood, the GPMC is adjusting some key security descriptors in Active Directory.

The precise error message you'll get is "The permissions for this GPO in the SYSVOL folder are inconsistent with those in Active Directory. It is recommended that these permissions be consistent. To change the SYSVOL permissions to those in Active Directory, click OK."

By allowing this, you can do some fancy footwork later, as you'll see in the section "Advanced Security and Delegation with the GPMC" in Chapter 2. You will only see this message if your Windows 2000 PDC-Emulator domain was upgraded from anything prior to SP4.

## The Results of Loading the GPMC

After the GPMC is loaded on the machine from which you will manage Group Policy (the management workstation), you'll see that the way you view things has changed. If you take a look

in Active Directory Users And Computers (or Active Directory Sites And Services) and try to manage a GPO, you'll see a curious link on the existing Group Policy tab (as seen in Figure 1.5).

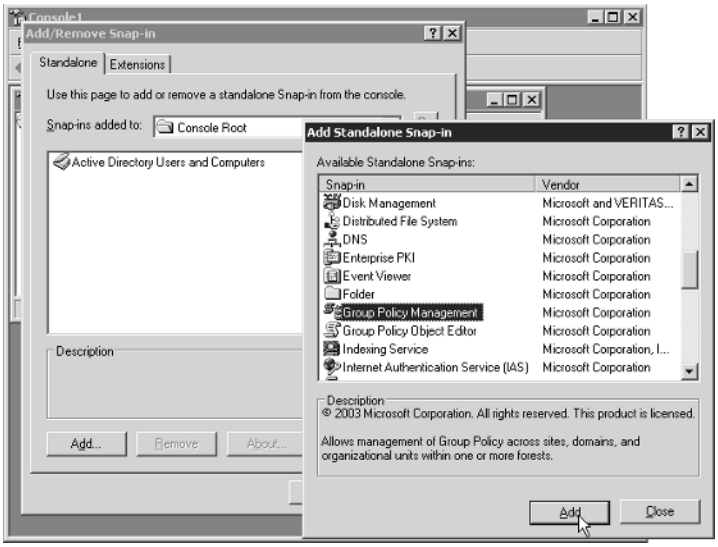
Additionally, you'll see a Group Policy Management icon in the Administrative Tools folder in the Start Menu folder.

### Creating a One-Stop Shop MMC

As you'll see, the GPMC is a fairly comprehensive Group Policy management tool. But the problem is that right now, the GPMC and the Active Directory Users And Computers snap-ins are not integrated beyond what you see in Figure 1.5.

Often, you'll want to change a Group Policy on an OU and then move computers to that OU. Unfortunately, you can't do so from the GPMC; you must to return to Active Directory Users And Computers to finish the task. This can get frustrating quickly. The GPMC does allow you to right-click at the domain-level to choose to launch the Active Directory Users And Computers console when you want, but I prefer a one-stop shop view of my Active Directory management. It's a matter of taste.

To that end, my preference is to create a custom MMC by running MMC from the Run dialog box and then add in both Active Directory Users And Computer and Group Policy Management snap-ins as shown here.




Now, you'll really have a near-unified view of most of what you need at your fingertips. Both Active Directory Users And Computers and the GPMC can create and delete OUs. Both tools also allow administrators to delegate permissions to others to manage Group Policy, but that's where the two tools' functionality overlap ends.

The GPMC won't show you the actual users and computer objects inside the OU; so deleting an OU from within the GPMC is dicey at best, because you can't be sure of what's inside!

You can choose to add other snaps-ins too, of course, including Active Directory Sites And Services or anything else you think is useful. The illustrations in the rest of this book will show both snap-ins loaded in this configuration.

**FIGURE 1.5** The Group Policy tab now refers you to the GPMC and provides a link.


You can launch the GPMC from either the new link in Active Directory Users And Computers (or Active Directory Sites And Services) or directly from new icon in the Start Menu. However, clicking Open in the existing tools has a slight advantage of telling the GPMC to "snap to" the location in Active Directory on which you are currently focused.

# Using the GPMC in Active Directory


For the examples in this book, I'll refer to our sample Domain Controller, WINDC01, which is part of my example Corp.com domain. For these examples, you can choose to rename the Default-First-Site-Name site or not—your choice.

Since many of us are still warming up to Group Policy, and even more people are warming up to the GPMC, I'll start with some basics to ensure that things are running smoothly. For most of the examples in this book, you'll be able to get with just the one Domain Controller and one or two workstations that participate in the domain, for verifying that your changes took place.

Again, I encourage you to not try these examples on your production network, in order to avoid a CLM (*Career-Limiting Move*).

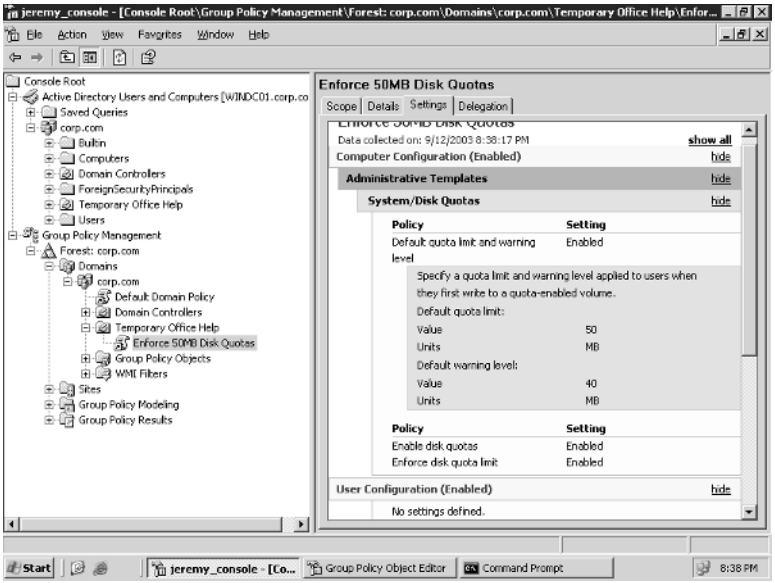
## Active Directory Users and Computers versus GPMC

The main job of Active Directory Users And Computers is to give you an "Active Directory object centric" view. Active Directory Users And Computers lets you deal with users, computers, groups, contacts, the operations masters (FSMOs), and delegation of control over user accounts as well as change the domain mode and define advanced security and auditing inside Active Directory. When you drill down inside Active Directory Users And Computers into an OU, you see the computers, groups, contacts, and so on contained within the OU.

But the GPMC has one main job: to provide you with a "Group Policy centric" view of all you control. All the OUs that you see in Active Directory Users And Computers are visible in the GPMC; however, the GPMC does not show you users, computers, contacts, and such. When you drill down into an OU inside the GPMC, you see but one thing—the GPOs that affect the objects inside the OU.

In Figure 1.6, you can see the Active Directory Users And Computers view as well as the GPMC view—rolled up into one MMC that we created earlier. The Active Directory Users And Computers view of **Temporary Office Help** and the GPMC view of the same OU is radically different.

**FIGURE 1.6** GPMC shows the same OUs as Active Directory Users and Computers. However, the GPMC shows GPO relationships, not users, computers, or other objects.



When focused at a site, a domain, or an OU within the GPMC, you see only the GPOs that affect that level in Active Directory. You don't see the same "stuff" that Active Directory Users And Computers sees, such as users, computers, groups, or contacts.

The basic overlap in the two tools is the ability to create and delete OUs. If you add or delete an OU in either tool, you need to refresh the other tool by pressing F5 to see the update. For instance, in Figure 1.6, you can see that my Active Directory has several OUs, including one named **Temporary Office Help**.


Deleting an OU from inside the GPMC is generally a bad idea. Because you cannot see the Active Directory objects inside the OU (such as users and computers), you don't really know how many objects you're about to delete. So be careful!

If I delete the **Temporary Office Help** OU in Active Directory Users And Computers, the change is not reflected in the GPMC window until it's refreshed. And vice versa.

## Adjusting the View within the GPMC

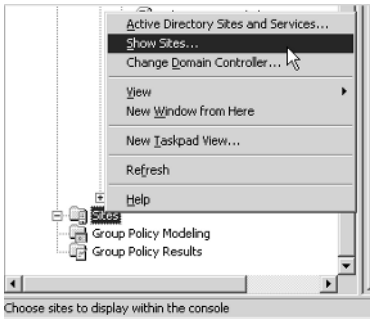
The GPMC lets you view as much or as little of your Active Directory as you like. By default, you view only your own forest and domain. You can optionally add in the ability to see the sites in your forest, as well as the ability to see other domains in your forest or domains in other forests, although these views might not be the best for seeing what you have control over.

**Viewing Sites in the GPMC** When you create GPOs, you won't often create GPOs that affect sites. The designers of the GPMC seem to agree; it's a bit of a chore to apply GPOs to sites. To do so, you need to link an existing GPO to a site. You'll see how to do this a bit later in this chapter.

However, you first need to expose the site objects in Active Directory. To do so, right-click the Sites object in GPMC, choose "Show Sites" from the shortcut menu (see Figure 1.7), and then click the check box next to each site you want to expose.

In our first example, we'll use the site level of Active Directory to deploy our first Group Policy Object. At this point, go ahead and enable the Default-First-Site so that you can have it ready for use in our own experiments.

**FIGURE 1.7** You need to expose the Active Directory sites before you can link GPOs to them.



**Viewing Other Domains in the GPMC** To see other domains in your forest, drill down to the Forest folder in Group Policy Management, right-click Domains, choose Show Domains, and select the other available domains in your forest. Each domain will now appear at the same hierarchical level in the GPMC.

**Viewing Other Forests in the GPMC** To see other forests, right-click the root (Group Policy Management), and choose "Add Forest" from the shortcut menu. You'll need to type the name of the Windows 2003 forest you want to add. If you want to add or subtract domains within that new forest, follow the instructions in the preceding paragraph.


You can add forests with which you do not have a two-way cross-forest trust. However, GPMC defaults will not display these domains as a safety mechanism. To turn off the safety, choose View menu ➢ Options to open the Options dialog box. In the General tab, clear "Enable Trust Detection" and click OK.

Now that we've adjusted our view to see the domains and forests we want, let's examine how to manipulate our GPOs and GPO links.

## The GPMC-centric view

As we stated earlier, one of the fundamental concepts of Group Policy is that the GPOs themselves live in the "swimming pool" that is the domain. Then, when a level in Active Directory needs to use that GPO, there is simply a link to the GPO.

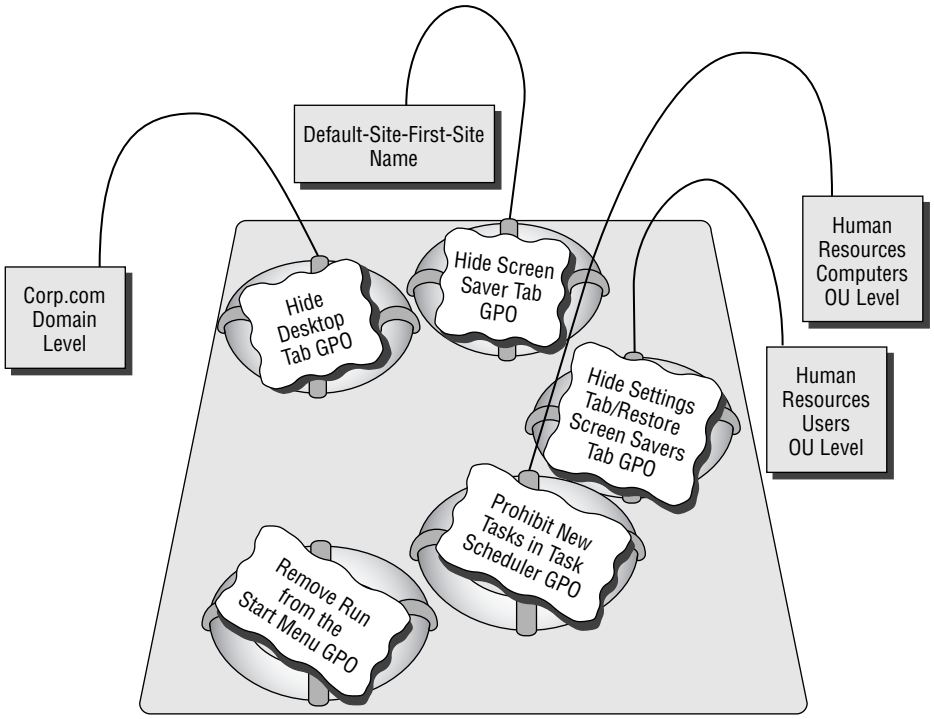
Figure 1.8 shows what our swimming pool will eventually look like when we're done with the examples in this chapter.

Our swimming pool will be full of GPOs, with various levels in Active Directory "linked" to those GPOs. To that end, you can drill down, right now, to see the representation of the swimming pool. It's there, waiting for you. Click Group Policy Management ➢ Forest ➢ Domains ➢ corp.com ➢ Group Policy Objects to see all the GPOs that exist in the domain. (See Figure 1.9.)


If you're just getting started, it's not likely you'll have more than the "Default Domain Controllers Policy" GPO and "Default Domain Policy" GPO. That's OK. You'll start getting more GPOs soon enough. Oh, and for now, please don't modify the default GPOs. They're a bit special and are covered in great detail in Chapter 6.

All GPOs in the domain are represented in the Group Policy Objects folder. As you can see, when the **Temporary Office Help** OU is shown within the GPMC, a relationship exists between the OU and the "Enforce 50MB Disk Quotas" GPO. That relationship is the tether to the GPO in the swimming pool—the GPO link back to Enforce 50MB Disk Quotas. You can see this linked relationship because the "Enforce 50MB Disk Quotas" icon inside **Temporary Office Help** has a little arrow icon, signifying the link back to the actual GPO in the domain.

**FIGURE 1.8** Imagine your upcoming GPOs as just hanging out in the swimming pool of the domain.



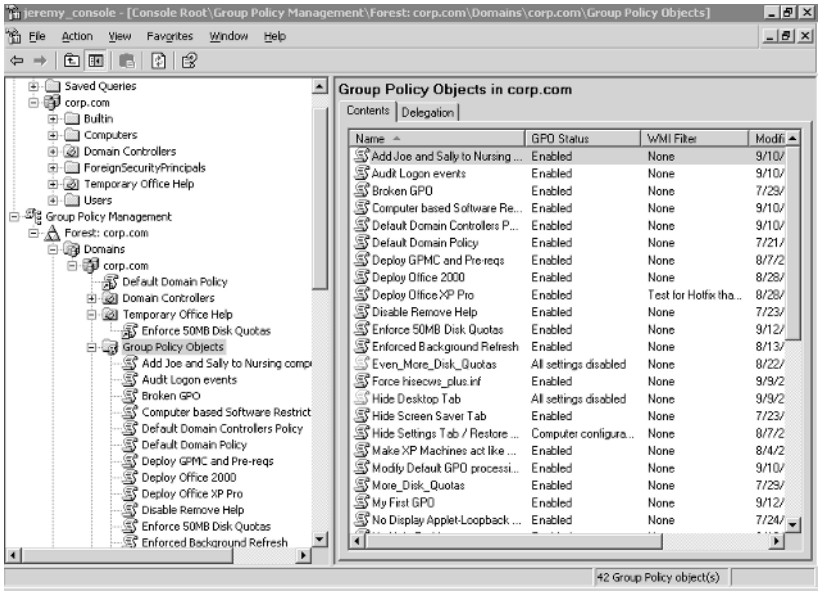

**The Corp.com GPO Swimming Pool**

# Our Own Group Policy Examples

While you're plunking around inside the Group Policy Object Editor, you'll see lots of policy settings that are geared toward Windows 2000, Windows XP, and/or Windows 2003. Some are geared only for Windows XP, and others are geared only for Windows 2003. If you happen to apply a policy to a system that isn't listed, the policy is simply ignored. For instance, policy settings described as working for Windows XP will not typically work on Windows 2000 machines.

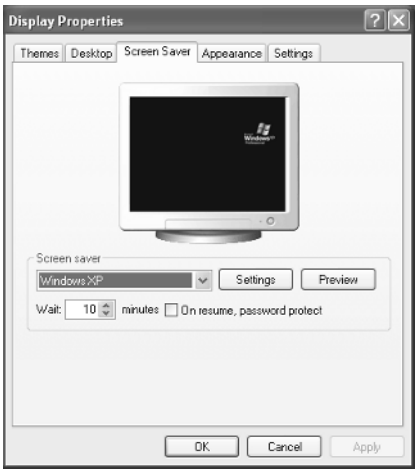
Now that you've got a grip on honing your view within the GPMC, let's take it for a quick spin around the block with some examples!

**FIGURE 1.9** The Group Policy Objects folder highlighted here is the representation of the swimming pool of the domain that contains your actual GPOs.




For this series of examples, we're going after the users who keep fiddling with their display applets in Windows XP (and Windows 2000). In the Display Properties dialog box (right-click the Desktop and choose Properties from the shortcut menu) are several tabs, including Screensaver, Appearance, and Settings, as shown in Figure 1.10.

**FIGURE 1.10** In Windows XP, all the tabs in the Display Properties dialog box are available by default.



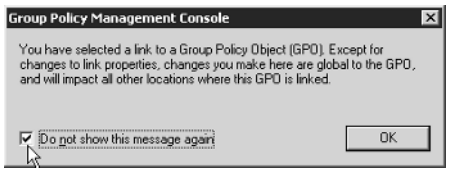
For our first use of Group Policy, we're going to produce four "edicts." (For dramatic effect, you should stand on your desk and loudly proclaim these edicts with a thick British accent):

- At the site level, there will be no more Screen Saver tabs.
- At the domain level, there will be no more Desktop tabs.
- At the **Human Resources Users** OU level, there will be no more Settings tabs. And, while we're at it, let's bring back those Screen Saver tabs!
- At the **Human Resources Computers** OU, we'll prohibit the use of the Task Scheduler.

Following along with these concrete examples will reinforce the concepts presented earlier. Additionally, they are used throughout the remainder of this chapter and the book.

### Understanding GPMC's Link Warning

As you work through the examples, you'll do a lot of clicking around. When you click a GPO link the first time, you'll get this message:




This message is trying to convey an important sentiment. That is, multiple levels in Active Directory may be linked back and using the exact same GPO. The idea is that multiple levels of Active Directory could be using the exact same Group Policy Object contained inside the Group Policy Objects container—but just linked back to it.

What if you modify the policy settings by right-clicking a policy link and choosing Edit from the shortcut menu? All instances in Active Directory that link to that GPO embrace the new settings. If this is a fear, you might want to create another GPO and then link it to the level in Active Directory you want. More properties are affected by this warning, and we'll explore them in Chapter 3.

If you've squelched this message by selecting "Do not show this message again", you can get it back. In the GPMC in the menus, choose View ➢ Options and select the General tab and select "Show Confirmation Dialog To Distinguish Between GPOs And GPO Links" and click OK.

## More about Linking and the Group Policy Objects Container

The GPMC is a fairly flexible tool. Indeed, it permits the administrator to perform many tasks in different ways. One thing you'll do quite a lot in your travels with the GPMC is to actually create your own Group Policy Objects. Again, GPOs live in a container within Active Directory and are represented within the Group Policy Objects container (the swimming pool) inside the domain (seen in Figure 1.9, earlier in this chapter.) Any levels of Active Directory—site, domain, or OU—simply link back to the GPOs hanging out in the Group Policy Objects container.

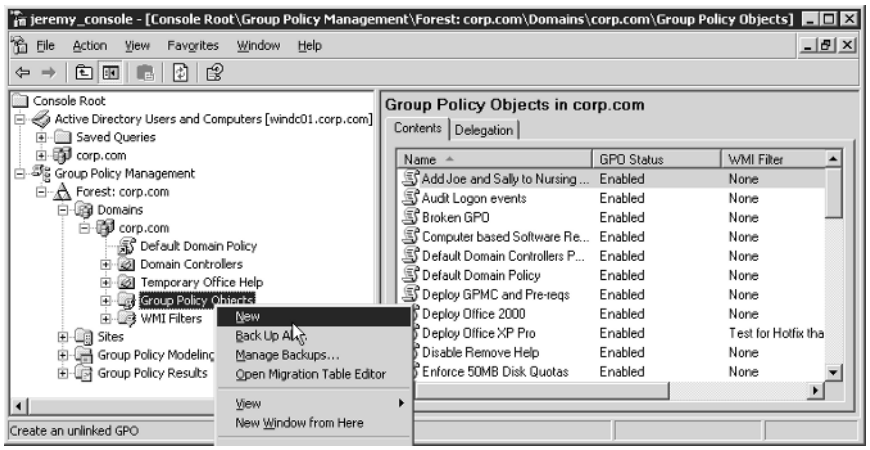
To apply Group Policy to a level in Active Directory (site, domain, or OU) using the GPMC, you have two options:

- Create the GPOs in the Group Policy Objects container first. Then, while focused at the level you want to command in Active Directory (site, domain, or OU), manually add a link to the GPO that is in the Group Policy Objects container.
- While focused at the level you want to command in Active Directory (domain or OU), create the GPOs in the Group Policy Objects container and automatically create the link. This link is created at the level you're currently focused at *back* to the GPO in the Group Policy Objects container.

Which is the correct way to go? Both are perfectly acceptable, because both are really doing the same thing.

In both cases the GPO itself does not "live" at the level in Active Directory at which you're focused. Rather, the GPO itself "lives" in the Group Policy Objects container. The link back to the GPO inside the Group Policy Objects container is what makes the relationship between the GPO inside the Group Policy Objects container swimming pool and the level in Active Directory you want to command.

**FIGURE 1.11** You create your first GPO in the Group Policy Object container by right-clicking and choosing New.



To get the hang of this, let's work through some examples. First, let's create our first GPO in the Group Policy Objects folder. Follow these steps:

1. Launch the GPMC.
2. Traverse down by clicking Group Policy Management ➢ Forest ➢ Domains ➢ corp.com ➢ Group Policy Objects.
3. Right-click the Group Policy Objects folder and choose New from the shortcut menu to open the New GPO dialog box as seen in Figure 1.11.
4. Let's name our first edict, er, GPO, something descriptive, such as "Hide Screen Saver Tab."
5. Once the name is entered, you'll see the new GPO listed in the swimming pool. Right-click the GPO, and choose Edit to open the Group Policy Object Editor as seen in Figure 1.12.
6. To hide the Screen Saver tab, drill down by clicking User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display. Double-click the **Hide Screen Saver Tab** policy setting to open the **Hide Screen Saver Tab** Properties screen, as shown in Figure 1.13. Select the Enabled setting, and click OK.
7. Close the Group Policy Object Editor.

**FIGURE 1.12** You can right-click the GPO in the Group Policy Objects container and choose Edit from the shortcut menu to open the Group Policy Object Editor.

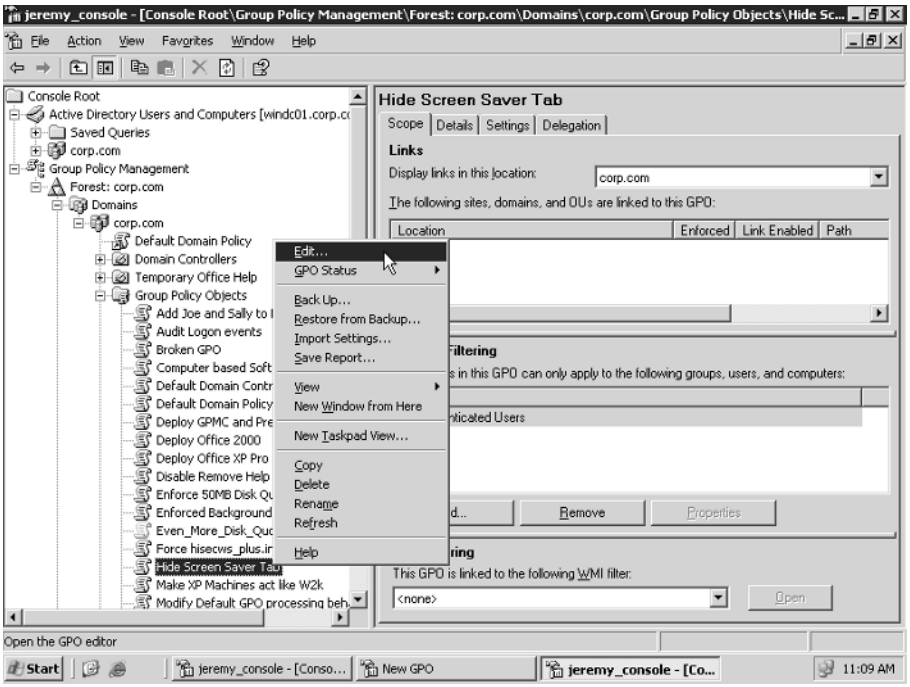
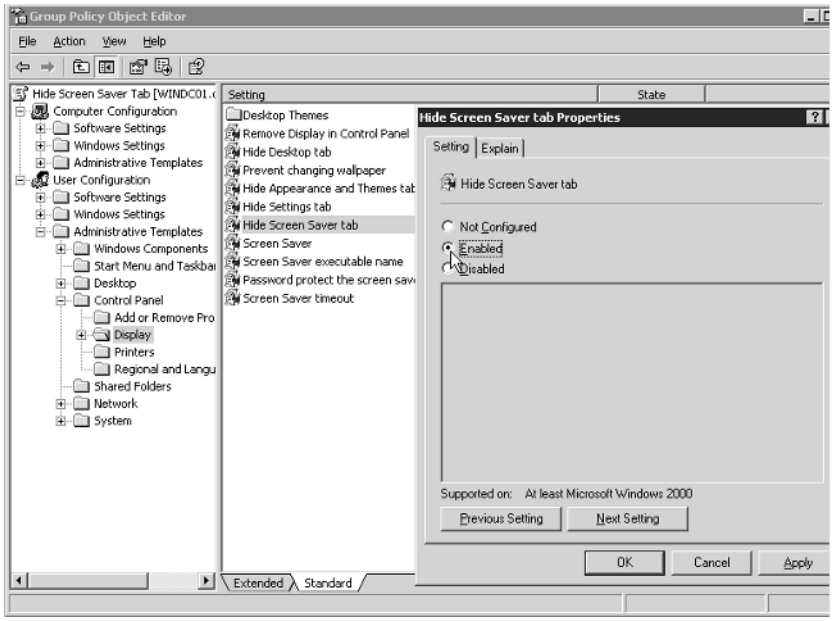


**FIGURE 1.13** Double-click the policy setting and enable it.




## Understanding Our Actions

Now that we have this "Hide Screen Saver Tab" edict floating around in the Group Policy Objects container—in the representation of the swimming pool of the domain—what have we done? Not a whole lot, actually, other than create some bits inside Active Directory and upon the Domain Controllers. By creating new GPOs in the Group Policy Objects folder, we haven't inherently forced our desires on *any* level in Active Directory—site, domain, or OU.

To actually make a level in Active Directory accept our will, we need to link this new Group Policy Object to an existing level. Only then will our will be accepted and embraced. Let's do that now.

# Applying Group Policy Object to the Site Level

The least-often-used level of Group Policy application is at the site. This is because it's got the broadest stroke but the bluntest application. Additionally, since Active Directory states that only members of the Enterprise Administrators (EAs) can modify sites and site links, it's equally true that only EAs (by default) can add and manipulate GPOs at the site level.


When a tree or a forest contains more than one domain, only the EAs and the Domain Administrators (DAs) of the root domain can create and modify sites and site links. When multiple domains exist, DAs in domains other than the root domain cannot create sites or site links (or site-level GPOs).

However, site GPOs might come in handy on an occasion or two. For instance, you might want to set up site-level GPO definitions for network-specific settings, such as Internet Explorer proxy settings or IP security policy for sensitive locations. Setting up site-based settings is useful if you have one building (set up explicitly as an Active Directory site) that has a particular or unique network configuration. You might choose to modify the Internet Explorer proxy settings if this building have a unique proxy server. Or in the case of IP security, perhaps this facility has particularly sensitive information, such as confidential records or payroll information.

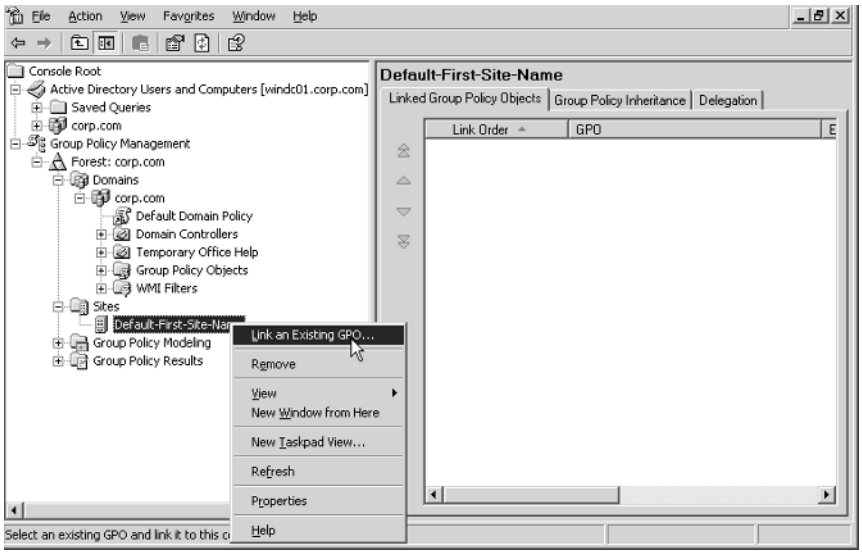
Therefore, if you're not an EA (or a DA of the root domain), it's likely you'll never get to practice this exercise outside the test lab. In this example, we'll work with a basic example to get the feel of the Group Policy Object Editor.


Implementing GPOs linked to sites can have a substantial impact on your logon times and WAN (Wide Area Network) traffic if not performed correctly. For more information, see Chapter 3.

We already stood on our desks and loudly declared that there will be no Screen Saver tabs at our one default site. The good news is that we've already done two-thirds of what we need to do to make that site accept our will: we exposed the sites we want to manage, and we created the "Hide Screen Saver Tab" GPO in the Group Policy Objects container.

Now, all we need do is to tether the GPO we created to the site with a GPO link.

**FIGURE 1.14** Once you have your first GPO designed, you can link it to your site.



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

1. Inside the GPMC snap in, drill down by clicking the Group Policy Management folder, the Forest folder, and the Sites folder.
2. 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.
3. Right-click the site, and choose "Link an Existing GPO", as shown in Figure 1.14.
4. Now you can select the "Hide Screen Saver Tab" GPO from a list of GPOs in the Group Policy Objects container in the domain.

Once you have chosen the GPO, it will be linked to the site. You can also view it in the "Linked Group Policy Objects" tab in the right pane.


Did you notice that there was no "Are You Sure You Really Want To Do This?" warning or anything similar? The GPMC trusts that you set up the GPO correctly. If you create GPOs with incorrect settings and/or link them to the wrong level in Active Directory, you can make boo-boos on a grand scale. Again—this is why you want to try any setting you want to deploy in a test lab environment first.

## Verifying Your Changes at the Site Level

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

If you are logged onto a Windows XP Professional machine, you can open up the Display applet in Control Panel and note that the Screen Saver tab is missing, as shown in Figure 1.15 below.

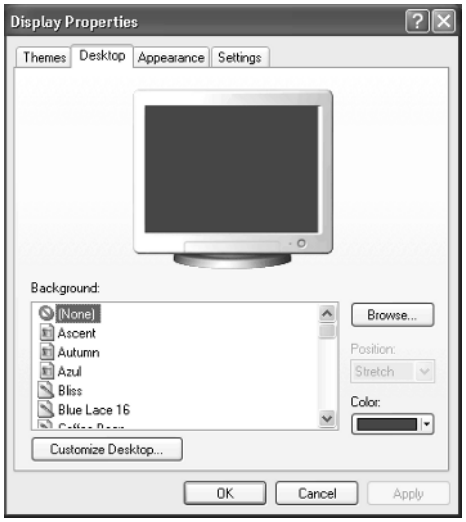

Don't panic if you do not see the changes reflected the first time you log on. See the sections "Group Policy processing behavior" and "Forcing Background Processing" in Chapter 3 to find out how to encourage changes to occur. To see the Screen Saver tab disappear on Windows XP machines right now, log off and log back on. The policy should take effect.

This demonstration should prove how powerful Group Policy is, not only because everyone at the site is affected, but more specifically because administrators are not immune to Group Policy effects. Administrators are not immune because they are automatically members in the Authenticated Users security group. (You can modify this behavior with the techniques explored in Chapter 3.)

## Applying Group Policy Objects to the Domain Level

At the domain level, we want an edict that says the Desktop tab should be removed from the Display Properties dialog box. Active Directory domains allow only members of the Domain Administrators group the ability to create Group Policy over the domain. Therefore, if you're not a DA (or a member of the EA group), it's likely that you'll never get to practice this exercise outside the test lab.

**FIGURE 1.15** The Screen Saver tab in Windows XP is missing because the site policy is affecting the user.




To apply the edict, follow these steps:

1. In the GPMC, drill down by clicking Group Policy Management ➢ Forest ➢ Corp.com.
2. Right-click the domain name to see the available options, as shown in Figure 1.16.

### Create and Link a GPO Here versus Link an Existing GPO

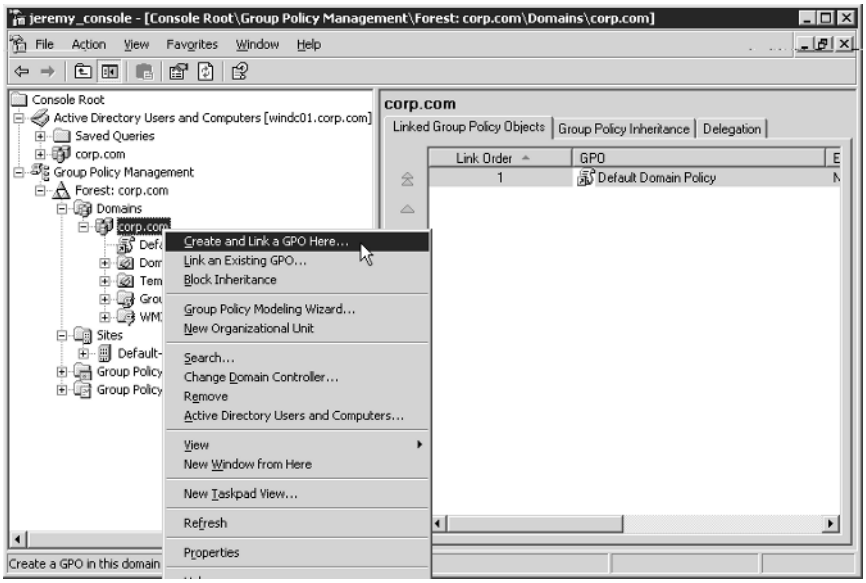
In the previous example we forced the site level to embrace our Hide Screen Savers Tab edict. First, we created the GPO in the Group Policy Objects folder, and then in another step we linked the GPO to the site level. However, at the domain level (and, as you're about to see, the OU level), we can take care of both steps at once via the Create And Link A GPO Here command.

This tells the GPMC to create a new GPO in the Group Policy Objects folder and then automatically link the new GPO back to this focused level of Active Directory. This is a time-saving step so we don't have to dive down into the Group Policy Objects folder first and then create the link back to the Active Directory level.

So why is this "Create and Link a GPO Here" option possible only at the domain and OU level, but not the site level? Because Group Policy Objects linked to sites can often cause excessive bandwidth troubles using the old-school way of doing things. With that in mind, the GPMC interface makes sure that when you work with GPOs that affect sites, you're consciously choosing from which domain the GPO is being linked.

I'll talk more about this concept and how it's rectified with the GPMC way of doing things at the top of Chapter 3.

**FIGURE 1.16** At the domain level, you can create the GPO in the Group Policy Objects container and then immediately link to the GPO from here.




Don't panic when you see all the possible options. We'll hit them all in due time; right now we're interested in the first two: "Create and Link a GPO Here" and "Link an Existing GPO."

Since you're focused at the domain level, you are prompted for the name of a new Group Policy Object when you right-click and choose to "Create and Link a GPO Here." For this one, type a descriptive name, such as "Hide Desktop Tab." Your new "Hide Desktop Tab" GPO is created in the Group Policy Objects container, and, automatically, a link is created at the domain level from the GPO to the domain.

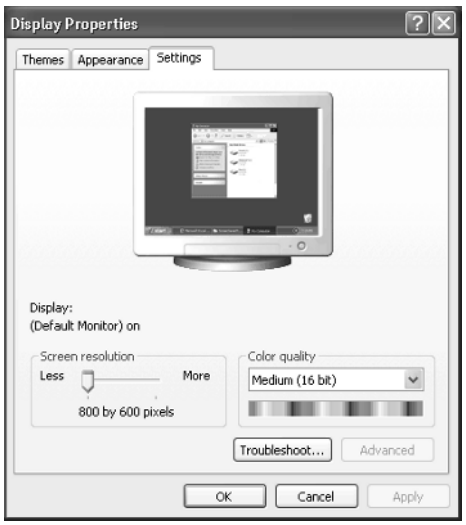

You can be sure that the GPO was created by simply drilling down through Group Policy Management, Forest, Domains, Corp.com, and Group Policy Objects and looking for your new Hide Desktop Tab GPO.

Right-click either the link to "Hide Desktop Tab" (or the GPO itself) and choose Edit to open the Group Policy Object Editor. To hide the Desktop tab, drill down through User Configuration, Administrative Templates, Control Panel, and Display, and double-click Hide Desktop Tab. Change the setting from Not Configured to Enabled, and click OK. Close the Group Policy Object Editor to return to the GPMC.

### Verifying Your Changes at the Domain Level

Now, log on as any user in the domain. You can log on to any computer in the domain or as any user you have defined—even the administrator of the domain. Open the Display Properties dialog box. You'll see that the Desktop tab is now also missing, as in Figure 1.17.

**FIGURE 1.17** The Desktop tab is now also missing because the user is affected by the domain-level policy.




Once again, administrators are not immune to Group Policy effects. You can change this behavior as you'll see in Chapter 3.

## Applying Group Policy Objects to the OU Level

OUs are wonderful tools for delegating away unpleasant administrative duties, such as password resets or modifying group memberships. But that's only half their purpose. The other half is to be able to apply Group Policy.

You'll likely find yourself making most of Group Policy additions and changes at the OU level, because that's where you have the most flexibility and the OU is the most-refined instrument to affect users. Once OU administrators become comfortable in their surroundings, they want to harness the power of Group Policy.

## Preparing to Delegate Control

To create a GPO at the OU level, you must first create the OU and a plan to delegate. For the examples in this book, we'll create three OUs that look like this:

- **Human Resources**
  - **Human Resources Users**
  - **Human Resources Computers**

Having separate OUs for your users and computers is a good idea—for both delegation of rights and also GPO design. Microsoft considers this a "best practice."

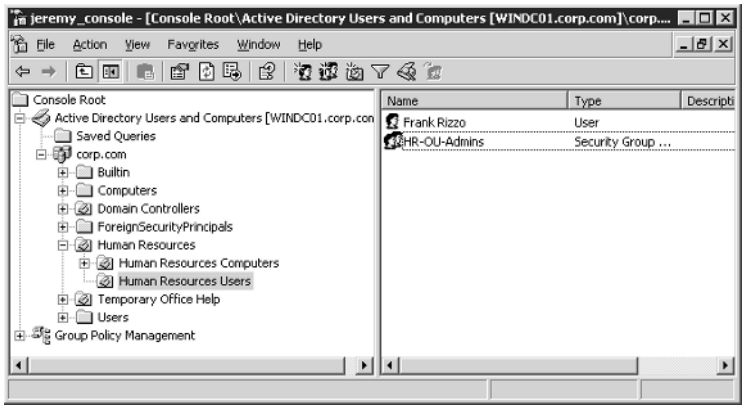
In the **Human Resources Users** OU in our Corp.com domain, we'll create and leverage an Active Directory security group to do our dirty work. We'll name this group HR-OU-Admins and put our first users inside the HR-OU-Admins inside group. We'll then delegate the appropriate rights necessary for them to use the power of GPOs.

To create the **Human Resources Users** OU, follow these steps:

1. Log on to the Domain Controller WINDC01 as Domain Administrator.
2. In Active Directory Users And Computers, right-click the domain name and choose New ➢ Organizational Unit, which will allow you to enter in a new OU name. Enter **Human Resources** as the name.
3. Inside the **Human Resources** OU, create two more OUs—**Human Resources Computers** and **Human Resources Users**, as shown in Figure 1.18.

Alternatively, you can create the OU in the GPMC. Just right-click the domain and choose "New Organizational Unit" from the shortcut menu.

**FIGURE 1.18** When you complete all these steps, your Human Resources OU should have Frank Rizzo and the HR-OU-Admins as well as the Human Resources Users OU and Human Resources Computers OU.



To create the HR-OU-Admins group, follow these steps:

1. In Active Directory Users And Computers, right-click the new **Human Resources Users** OU and choose New ➢ Group.
2. Create the new group HR-OU-Admins as a new Global Security group.

To create the first user to go inside HR-OU-Admins, follow these steps:

1. In Active Directory Users And Computers, right-click the **Human Resources Users** OU and choose New ➢ User.
2. Name the user Frank Rizzo, with an account name of **frizzo,** and click Next.
3. If you've established a Windows 2003 domain, you must now enter a complex password for a user.
4. Finish and close the wizard.

### Easily Manage New Users and Computers

The Computers folder and Users folder in Active Directory Users and Computers are not OUs. They are generic containers. You'll notice that they are not present in the GPMC view of Active Directory. Because they are generic containers (and not OUs), you cannot link Group Policy Objects to them.

These folders have two purposes:

- If an NT 4 domain is upgraded, the user and computer accounts will wind up in these folders. (Administrators are then supposed to move the accounts into OUs.)
- It's the default location where older tools create new users and computers. These older tools are in the Windows NT 4 User Manager (which still works in a Windows 2000 or Windows 2003 domain). Additionally, command-line tools, such as the `net user`, `net group`, will add user accounts to this location. Similarly, the Computers folder is the default location for any new client workstation or server that joins the domain. Or, similarly, should you pre-create computer accounts using the `net computer` command.

If you execute one of these commands, the objects you create will wind up in either the Users folder or the Computers folder. But really, you don't want your users or computers to be in these folders—you want them in OUs. That's where the action is because you can apply Group Policy to OUs, not to these folders! Yeah, sure, these users and computers are affected by site and domain level GPOs. But really the action is at the OU level, and you want your computer and user objects to be placed in OUs as fast as possible—not sitting around in these generic Computers and Users folders.

To that end, Windows 2003 domains (in full functional level) have two tools to redirect the default location of new users and computers to the OUs of your choice. For example, suppose you want all new computers to go to a **NewComputers** OU and all new users to go to a **NewUsers** OU. And you want to link several GPOs to the **NewUsers** and **NewComputers** OUs to ensure that new accounts immediately have some baseline level of security, restriction, or protection. Without a little magic, new user accounts created using older tools won't automatically be placed there.

In Windows 2003 Active Directory, Microsoft has provided REDIRUSR and REDIRCMP commands that takes a distinguished name, like:

```
REDIRCMP ou=newcomputers,dc=corp,dc=com and/or
REDIRUSR ou=newusers,dc=corp,dc=com
```

Now if you link GPOs to these OUs, your new accounts will get the Group Policy Objects dictating settings to them at an OU level. This will come in handy when users and computers aren't specifically created in their final destination OUs.

To learn more about these tools, see the Microsoft Knowledge Base article 324949.

To add Frank Rizzo to the HR-OU-Admins group, follow these steps:

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

When it's all complete, your OU structure with your first user and group should look like Figure 1.18.

## Delegating Control for Group Policy Management

Now that you've created the **Human Resources** OU, which contains the **Human Resources Users** OU and the **Human Resources Computers** OU and the HR-OU-Admins security group, and put Frank inside the **HR-OU-Admins group**, you're ready to delegate control. You can delegate control to use Group Policy in two ways: using Active Directory Users And Computers, and using the GPMC.


For this first example, we'll kick it old school and use the Active Directory Users And Computers way. Then, in Chapter 2, I'll demonstrate how to delegate control using the GPMC.

To delegate control for Group Policy management, follow these steps:

1. In Active Directory Users And Computers, right-click the top-level **Human Resources** OU you created, and choose Delegate Control from the shortcut menu to start the "Delegation of Control Wizard."
2. Click Next to get past the Wizard introduction screen.
3. You'll be asked to select users and/or groups. Click Add, add the HR-OU-Admins group, and click Next to open the "Tasks to Delegate" screen, as shown in Figure 1.19.
4. Click "Manage Group Policy links", and then click Next.
5. At the wizard review screen, click Finish.

**FIGURE 1.19** Select the "Manage Group Policy Links" task.


You might want to click some or all the other check boxes as well, but for this example, only "Manage Group Policy links" is required. Try to avoid selecting "Generate Resultant Set of Policy (Planning)" and "Generate Resultant Set of Policy (Logging)" at this time. You'll see where they come in handy in Chapter 3.

The Manage Group Policy Links task assigns the user or group "Read" and "Write" access over the `gPLink` and `gPOptions` properties for that level. To see or modify these permissions by hand, open Active Directory Users And Computers, choose View ➢ Advanced Features, If later you want to remove a delegated permission, it's a little challenging. You can locate the permission that you set by right-clicking the delegated object (such as OU), then click on the Properties tab, click the Security tab, choose Advanced, and dig around until you come across the permission you want to remove. Finally, delete the corresponding access control entry (ACE).

### Adding a User to the Server Operators Group

Under normal conditions, nobody but Domain Administrators, Enterprise Administrators, or Server Operators 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 WINDC01 Domain Controller.

To add a user to the Server Operators group, follow these steps:

1. In Active Directory Users And Computers, double-click Frank Rizzo's account under the **Human Resources Users** OU.
2. Click the Member Of tab and click Add.
3. Select the Server Operators group and click OK.
4. Click OK to close the Properties dialog box for Frank Rizzo.

Normally, you wouldn't give your delegated OU administrators Server Operators access. You're doing it solely for the sake of this example to allow Frank to log on locally to your Domain Controllers.

## Testing Your Delegation of Group Policy Management

Log off as Administrator on WINDC01 and log back on as Frank Rizzo. Now follow these steps to test your delegation:

1. Choose Start ➢ Programs ➢ Administrative Tools ➢ Group Policy Management to open the GPMC.


If the Administrative Tools folder is not present, you'll need to choose Start ➢ Run to open the Run dialog box, and then type `mmc` in the Open box to load a "naked" MMC. Then load the Group Policy Management snap-in.

2. Drill down through Group Policy Management, Domains, Corp.com, and Group Policy Objects. If you right-click Group Policy Objects in an attempt to create a new GPO, you'll see the shortcut menu shown in Figure 1.20.

As you can see, Frank is unable to create new GPOs in the swimming pool of the domain. Since Frank has been delegated some control over the **Human Resources** OU (which also contains the other OUs), let's see what he can do. If you right-click the **Human Resources** OU in the GPMC, you'll see the shortcut menu shown in Figure 1.21.

Because Frank is unable to create GPOs in the swimming pool of the domain (the Group Policy Objects container), he is also unable by definition to create and link a GPO here. Although Frank (and more specifically, the HR-OU-Admins) has been delegated the ability to "Manage Group Policy links", he cannot *create* new GPOs. Frank (and the other potential **HR-OU-Admins**) has only the ability to *link* an existing GPO.

## Understanding Group Policy Object Linking Delegation

When we were logged on as the Domain Administrator, we could create GPOs in the Group Policy Objects container, and we could create and link a GPO here at the domain or OU levels. But Frank cannot.

**FIGURE 1.20** Frank cannot create new GPOs in the Group Policy Objects container.

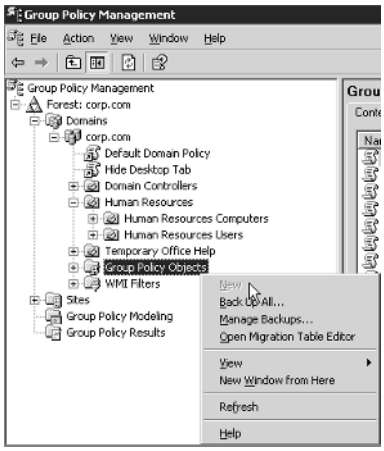
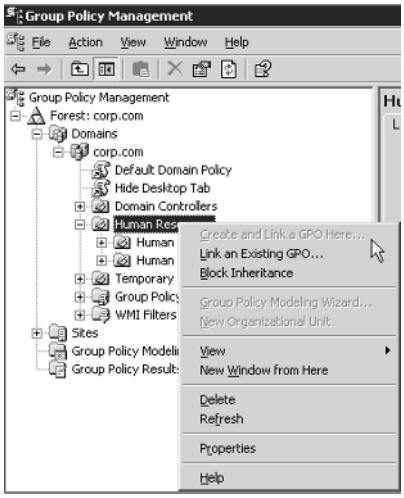



**FIGURE 1.21** Frank's delegated rights allow him to link to existing GPOs, but not to create new GPOs.




Here's the idea about delegating the ability to link to GPOs: someone with a lot of brains in the organization does all the work in creating a well-thought-out and well-tested GPO. Maybe this GPO distributes software, maybe it sets up a secure workstation policy, or perhaps it runs a startup script. You get the idea.

Then, others in the organization, like Frank, are delegated just the ability to *link* to that GPO and use it at their level. This solves the problem of delegating perhaps too much control. Certainly some administrators are ready to create their own users and groups, but other administrators may

not be quite ready to jump into the cold waters of Group Policy Object creation. Thus, you can design the GPOs for other administrators; they can just link to the ones you (or others) create.

When you (or someone with the right to link GPOs) selects "Link an Existing GPO", as seen in Figure 1.21, you can choose a GPO that's already been created—and hanging out in the domain swimming pool—the Group Policy Objects container.

In this example, the HR-OU-Admins members, such as Frank, can leverage any currently created GPO to affect the users and computers in their OU—even if they didn't create it themselves. In this example, Frank has linked to an existing GPO called "Word 2000 Settings". Turns out that some other administrator in the domain created this GPO, but Frank wants to use it. So, because Frank has "Manage Group Policy Links" rights on the **Human Resources** OU (and OUs underneath it), he is allowed to link to it.

But, as you can see in Figure 1.22, he cannot edit the GPOs. Under the hood, Active Directory doesn't permit Frank to edit GPOs he didn't create (and therefore doesn't own).


In Chapter 2, I'll show you how to grant specific rights to allow more than just the original creator (and now owner) of the object to edit specific GPOs.

Giving the ability to just link to existing GPOs is a good idea in theory, but often OU administrators are simply given full authority to create their own GPOs (as you'll see later.) For this example, don't worry about linking to any GPOs. Simply cancel out of the Select GPO screen, close the GPMC, and log off from the server as Frank Rizzo.

## Granting OU Admins Access to Create New Group Policy Objects

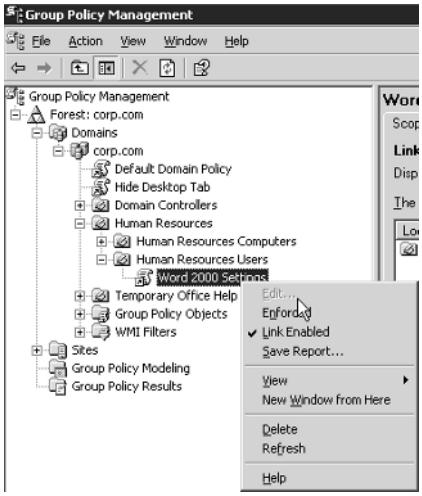
By using the Delegation of Control Wizard to delegate the Manage Group Policy Links attribute, you performed half of what is needed to grant the appropriate authority to Frank (and any additional future HR-OU-Admins) to create GPOs in the Group Policy Objects container and link them to the **Human Resources** OU, the **Human Resources Users** OU, or the **Human Resources Computers** OU. (Though we really don't want to link many GPOs directly to the **Human Resources** OU.)

You can grant the HR-OU-Admins the ability to create GPOs in the Group Policy Objects container in two ways. For now, I'll show you the old-school way; in Chapter 3, I'll show you the GPMC way.

One of Active Directory'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 or groups whom you want to have the ability to create GPOs to a built-in group, cleverly named Group Policy Creator Owners. To do so, follow these steps:

1. Log back on as Domain Administrator.
2. Fire up 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.

**FIGURE 1.22** The GPMC will not allow you to edit an existing GPO if you do not own it (or do not have explicit permission to edit it).




If you just created a new Windows 2003 domain or upgraded your domain from NT 4, you will not be able to add the HR-OU-Admins group until the domain mode has been switched to Windows 2000 Native or Windows 2003 Functional level. Switch the domain by using Active Directory Domains and Trusts. Switching the domain mode is a one-way operation, which shuts out older Domain Controllers. If you are not prepared to make the switch to Native mode, you'll only be able to add individual members, such as Frank Rizzo—and not a group.

4. Log off as Domain Administrator from WINDC01.

In Chapter 2, you'll see an alternate way to allow users to create GPOs.

## Creating and Linking Group Policy Objects at the OU Level

At the site level, we hide the Screen Saver tab in the Display Properties dialog box. At the domain level, we chose to hide the Desktop tab in the Display Properties dialog box. At the OU level, we have two jobs to do:

- Hide the Settings tab in the Display Properties dialog box.
- Restore the Screen Saver tab that was taken away at the site level.

To create a GPO at the OU level, follow these steps:

1. Log off as Administrator on WINDC01 and log back on as Frank Rizzo.
2. Choose Start ➢ Programs ➢ Administrative Tools ➢ Group Policy Management to open the GPMC.

If the Administrative Tools are not present on the machine you are using, choose Start ➢ Run to open the Run dialog box, and in the Open box, type `mmc` to load a "naked" MMC. Then load the Group Policy Management snap-in.

3. Drill down until you reach the **Human Resources Users** OU, right-click it, and choose "Create and Link a GPO Here" from the shortcut menu to open the "New GPO" dialog box.
4. In the "New GPO" dialog box, type in the name of your new GPO, say "Hide Settings Tab/ Restore Screen Saver Tab." This will create a GPO in the Group Policy Objects container and link it to the **Human Resources Users** OU.
5. Right-click the Group Policy link and choose Edit from the shortcut menu to open the Group Policy Object Editor.
6. To hide the Settings tab, drill down through User Configuration ➢ Administrative Templates ➢ Control Panel ➢ Display and double-click the **Hide Settings Tab** policy setting. Change the setting from "Not Configured" to "Enabled", and click OK.
7. To restore the Screen Saver tab, double-click the **Hide Screen Saver Tab** policy setting. Change the setting from "Not Configured" to "Disabled", and click OK.
8. Close the Group Policy Object Editor to return to the GPMC.

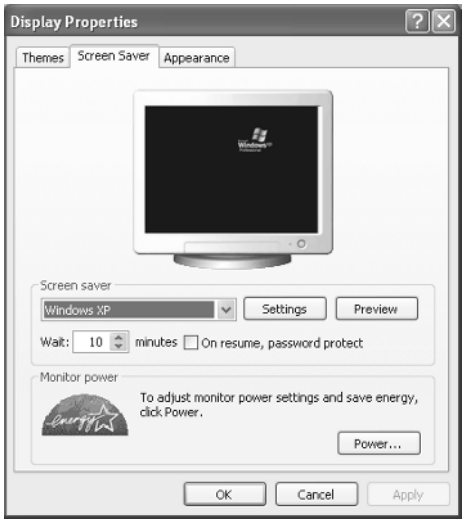
By disabling the Hide Screen Saver Tab policy setting, you're reversing the Enable setting set at a higher level. See the sidebar "A Note about the Three Possible Settings: Not Configured, Enabled, and Disabled" later in this chapter.

## Verifying Your Changes at the OU Level

On your test Windows XP machine in the domain, log back on as Frank. Right-click the Desktop and choose Display from the shortcut menu to open the Display Properties dialog box. Note that the Settings tab is missing, but that the Screen Saver tab is back, as shown in Figure 1.23.

This test proves, once again, that even OU administrators are not automatically immune from policy settings. Chapter 3 explains how to change this behavior.

**FIGURE 1.23** The Settings tab is missing along with the Desktop tab, but the Screen Saver tab has returned.




### Group Policy Strategy: Should I Create More or Fewer GPOs?

At times, you'll want to lock down additional functions for a collection of users or computers. For example, you might want to specify that no users in the **Human Resources Users** OU can use Control Panel.

At the **Human Resources Users** OU level, you've already set up a GPO that contained a policy setting to hide the Settings tab in the Display Properties dialog box. You now have a decision to make. You can create a new GPO that affects the **Human Resources Users** OU, give it a descriptive name, say "No One Can Use Control Panel", and then drill down through User Configuration ➢ Administrative Templates ➢ Windows Components ➢ Control Panel and enable the policy setting named **Prohibit Access to Control Panel**.

Or you could simply modify your existing GPO, named "Hide Settings Tab/Restore Screen Saver Tab" so that it contains additional policy settings. You can then rename your GPO to something that makes sense and encompasses the qualities of all the policy changes, say, "Our **Human Resources Users**' Desktop Settings."

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

The second method (multiple policy settings per GPO) is teeny-weeny bit faster for your computers and users at boot or logon time, because each additional GPO takes some miniscule fraction of additional processing time. But if you stuff too many settings in an individual GPO, the time to debug should things go wrong goes up exponentially. Group Policy has so many nooks and crannies that can be difficult to debug.

So, in a nutshell, if you have multiple GPOs at a particular level, you can do the following:

- Name each of them more descriptively.
- Debug them easily if things go wrong.
- Disable individually misbehaving GPOs.
- Associate that GPO more easily to a WMI filter (explored in Chapter 10).
- More easily delegate permissions to any specific GPO (explored in Chapter 3).

If you have fewer GPOs at a particular level, the following is the case:

- Logging on is slightly faster for the user (but really only slightly).
- Debugging is somewhat more difficult if things go wrong.
- You can disable individually misbehaving GPOs or links to misbehaving GPOs. (But if they contain many settings, you might be disabling more than you desire.)

So, how do you form a GPO strategy? There is no right or wrong answer; you need to decide what's best for you. Several options, however, can help you decide.

One middle-of-the-road strategy is to start with multiple GPOs and one lone policy setting in each. Once you are comfortable that they are individually working as expected, you can create another new GPO that contains the sum of the settings from, in this example, **Hide Settings Tab** and **Prohibit Access to Control Panel** and then delete (or disable) the old individual GPO.

Another middle-of-the-road strategy is to have a single GPO that contains only the policy settings required to perform a complete "wish." This way, if the wish goes sour, you can easily address it or disable it (or whack it) as needed.

Here's yet another strategy. Some Microsoft documentation recommends that you create GPOs such that they affect only the User half or the Computer half. You can then disable the unused portion of the GPO (either the Computer half or the User half). This allows for policy settings affecting one node to be grouped together for ease of naming and debugging and allows for flexible troubleshooting. However, be careful here because after you disable half the GPO, there's no iconic notification, and, in my opinion, troubleshooting can become harder if not performed perfectly and consistently. In all, I'm not a huge fan of disabling "half" the GPO.

## 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 create another GPO and link it to the **Human Resources Computers** OU. This GPO will remove the ability to create new scheduled tasks using the Task Scheduler for all the Windows 2000 and Windows XP machines in the **Human Resources Computers** OU.

The same setting exists under the User node, but we'll experiment with the Computer node policy.

First, you'll need to create the new GPO and modify the settings. You'll then need to move some client machines into the **Human Resources Computers** OU in order to see your changes take effect.

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

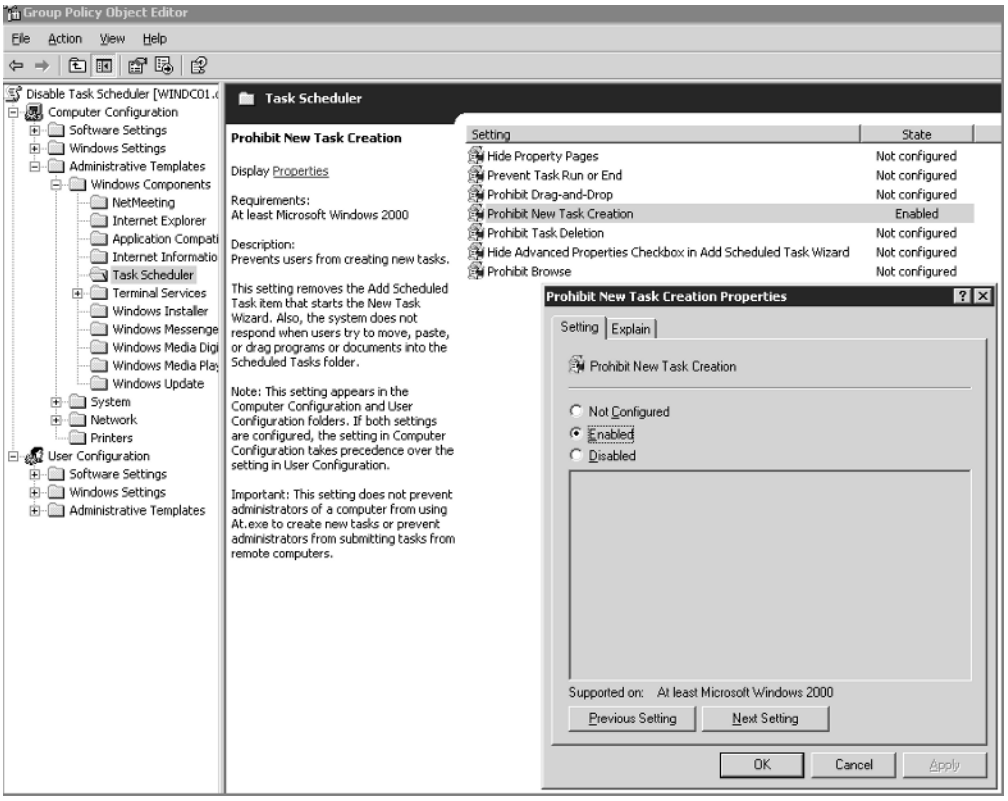
1. If you're not already logged in as Frank Rizzo, the **Human Resources** OU administrator, do so now.
2. Choose Start ➢ Programs ➢ Administrative Tools ➢ Group Policy Management to start the GPMC.

If the Administrative Tools are not present, choose Start ➢ Run to open the Run dialog box, and in the Open box, type `mmc` to load a "naked" MMC. Then load the GPMC.

3. Drill down until you reach the **Human Resources Computers** OU, right-click it, and choose "Create and Link a GPO Here" from the shortcut menu.
4. Name the GPO something descriptive, such as "Prohibit New Tasks in Task Scheduler."
5. Right-click the GPO, and choose Edit to open the Group Policy Object Editor.
6. We want to affect our Windows XP computers, so we need to use the Computers node. To disable the Task Scheduler, drill down through Computer Configuration ➢ Administrative Templates ➢ Windows Components ➢ Task Scheduler, and double-click **Prohibit New Task Creation**. Change the setting from Not Configured to Enabled, and click OK, as shown in Figure 1.24.
7. Close the Group Policy Object Editor to return the GPMC.

Be aware of occasional strange Microsoft verbiage when you need to enable a policy to *disable* a setting. In Windows 2003, most policy settings have been renamed to Prohibit <*whatever*> to reflect the change from confusion to clarity.

**FIGURE 1.24** By enabling this policy setting, you're disabling the Task Scheduler.




## Moving Computers into the Human Resources Computers OU

Since you just created a policy that will affect computers, you'll need to place a workstation or two inside the **Human Resources Computers** OU to see the results of your labor. You'll need to be logged on as Administrator to WINDC01 to do this.


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

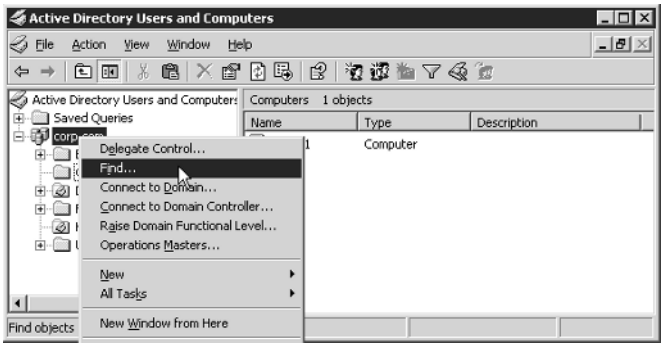
In this example, we're going to use the Find command in Active Directory Users And Computers to find a workstation named XPPro1 and move it into the **Human Resources Computers** OU.

To find and move computers into a specific OU, follow these steps:

1. In Active Directory Users And Computers, right-click the domain, and choose Find from the shortcut menu, as shown in Figure 1.25, to open the Find Users, Contacts, and Groups dialog box.
2. From the Find drop-down menu, select Computers. In the Name field, type **XPPro1** to find the computer account of the same name. Once you've found it, right-click the account and choose Move from the shortcut menu. Move the account to the **Human Resources Computers** OU.

Repeat these steps for all other computers that you want to move to the **Human Resources Computers** OU.

**FIGURE 1.25** Use the Find command to find computers in the domain so you can move them.





After you move the computer accounts into the **Human Resources Computers** OU, reboot your client machines. As you'll see in Chapter 3, the computer does not recognize the change right away when computer accounts are moved between OUs.

As you can see in this example (and in the real world), a best practice is to separate users and computers into their own OUs and then link GPOs to those OUs. Indeed, underneath a parent OU structure, such as the **Human Resources** OU, you might have more OUs, (i.e., **Human Resources Laptops** OU, **Human Resources Servers** OU, etc.). This will give you the most flexibility in design between delegating control where it's needed and the balance of GPO design within OUs. Just remember that in order for GPOs to affect either a user or computer, that user or computer must be within the scope of the GPO—site, domain, or OU.

## Verifying Your Cumulative Changes

At this point, you've set up three levels of Group Policy that accomplishes multiple actions:

- At the site level, the "Hide Screen Saver Tab" GPO is in force for users.
- At the domain level, the "Hide Desktop Tab" GPO is in force for users.

- In the **Human Resources Users** OU, the "Hide Settings Tab / Restore Screen Saver Tab" GPO is in force for users.
- In the **Human Resources Computers** OU the "Prohibit New Tasks in Task Scheduler" GPO is in force for computers.

At this point, take a minute to flip back to Figure 1.8 (the swimming pool graphic) to see where we're going here. To see the accumulation of your policy settings inside your GPOs, you'll need to log on as a user who is affected by the **Human Resources Users** OU and at a computer that is affected by the **Human Resources Computers** OU. Therefore, log on as Frank Rizzo on XPPro1.

Right-click the Desktop and choose Display from the shortcut menu to open the Display Properties dialog box. Note that the Settings tab is still missing from the previous exercise (and the Screen Saver tab is restored). In Control Panel, select Classic View, and double-click Scheduled Tasks. Now missing is the ability to create new tasks. (Although you can choose File ➢ New ➢ Schedule Task, you won't to able to create a new task once this policy setting is in force.)

This test proves that even OU administrators are not automatically immune from GPOs and the policy settings within. Under the hood, they are in the Authenticated Users security group. See Chapter 3 for information on how to modify this behavior.


Again, don't panic if you don't see the changes reflected right away. See Chapter 3, for more text on how to encourage changes to occur.

### A Note about the Three Possible Settings: Not Configured, Enabled, and Disabled

As you saw in Figure 1.24 earlier in this chapter, nearly all policy settings can be set as Not Configured, Enabled, or Disabled. These three settings have very different consequences, so it's important to understand how each works.

**Not Configured** The best way to think about Not Configured is to imagine that it really says, "Don't do anything" or even "Pass through." Why is this? Because if a policy setting is set to Not Configured, then what it's being told to do is to look at a higher level and see if anything is set there. If there is nothing set at a higher level, then there's nothing to do—the operating system simply does whatever its default is.

**Enabled** When a specific policy setting is enabled, the policy will take effect. In the case of the Hide Screen Saver Tab policy, the effect is obvious. However, lots of policy settings, once enabled, have myriad possibilities *inside* the specific policy setting! (For a gander at one such policy setting use the Group Policy Object Editor and drill down to User Configuration ➢ Administrative Templates ➢ Windows Components ➢ Internet Explorer ➢ Toolbars and select the policy setting named **Configure Toolbar Buttons**.) So, as we can see, enabled really means "Turn this policy setting on." It will then either do what it says, or there will be more options inside the policy setting that can be configured.

**Disabled** This setting leads a threefold life.

- Disabled usually means that if the same policy setting is enabled at a higher level, reverse its operation. For example, we chose to enable the Hide Screen Saver Tab policy setting at the site level. If at a lower level (say, the domain or OU level), we chose to disable this policy setting, the Screen Saver tab will pop back at the level at which we disabled this policy.
- Additionally, Disabled often forces the user to accept the administrator's will. That is, if a policy setting is disabled, some default behavior of the policy setting is enforced, and the user cannot change it. To see an example policy setting like this, use the Group Policy Object Editor and drill down through User Configuration ➢ Administrative Templates ➢ Control Panel and select the policy setting named Force Classic Control Panel Style. Once this policy setting is disabled, the policy forces Windows XP users to use the Control Panel in the new task-based style. The point here is that the Disabled setting is a bit tricky to work with. You'll want to be sure that when you disable a policy setting, you're doing precisely what you intend.
- Disabled sometimes has a special and, typically, rare use. That is, something might already be hard-coded into the Registry to be "turned on" or work one way, and the only way to turn it off is to select Disabled. One such policy setting is the Shutdown Event Tracker. You disable the policy setting, which turns it off, because on Windows 2003 it's already hard-coded on. In Windows XP, it's already hard-coded off. Likewise, if you want to kill Windows XP/SP2's firewall, you need to set Windows Firewall: Protect All Network Connections to Disabled. (You can find that policy setting at Administrative Templates ➢ Network ➢ Network Connections ➢ Windows Firewall ➢ Domain Profile while editing GPOs on Windows XP/Service Pack 2 computers.)

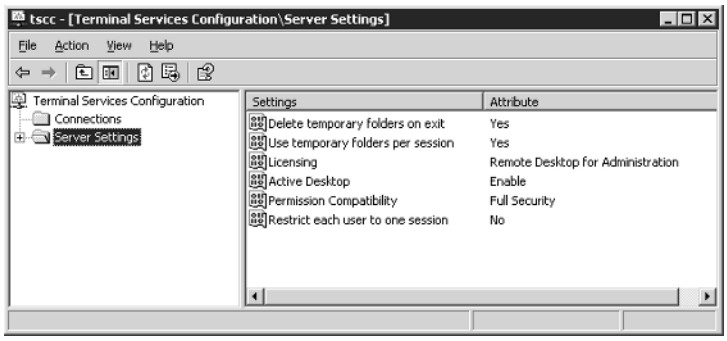
So, think of Not Configured as having neither Allow nor Deny being set. Enabled will turn it on, and possibly have more functions. Disabled has multiple uses, and be sure to test, test, test to really make sure that once you've manipulated a policy setting, it's doing precisely what you had in mind.

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

Windows Server 2003 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 two sections inside Windows 2000 and Windows 2003 sometimes look like they might have some tie-ins to Group Policy. Actually, they're totally separate.

## Terminal Services

Both Windows 2000 Server and Windows Server 2003 come with a built-in Terminal Services service. To configure the service in Windows 2000, you have only one option—use the Terminal Services Configuration utility.




Don't let the little binary 1/0 icons fool you into thinking this window is Group Policy related. It is not. However, Windows 2003 does have multiple policy settings, and once they are set, the outcome is reflected in this window. (See Chapter 3 for information about how to locate the applicable policy settings.)

## Routing and Remote Access

Routing and Remote Access (RRAS) allows users to connect to Windows 2003 servers over dial-in or VPN (virtual private network) connections, among other functions. To specify who can and cannot get through the gates, Windows Server 2003 has a facility to create rules to allow or deny access. Those rules happen to be called "Policies," as shown in Figure 1.26.

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

# Final Thoughts

The concepts here are valid whether your Active Directory domains are Windows 2000 or Windows 2003. The point is that to make the most use of Group Policy, you'll need an Active Directory. But the best news is that the GPMC (once loaded on a Windows XP or Windows 2003 machine) can control either Windows 2000 or Windows 2003 domains.

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

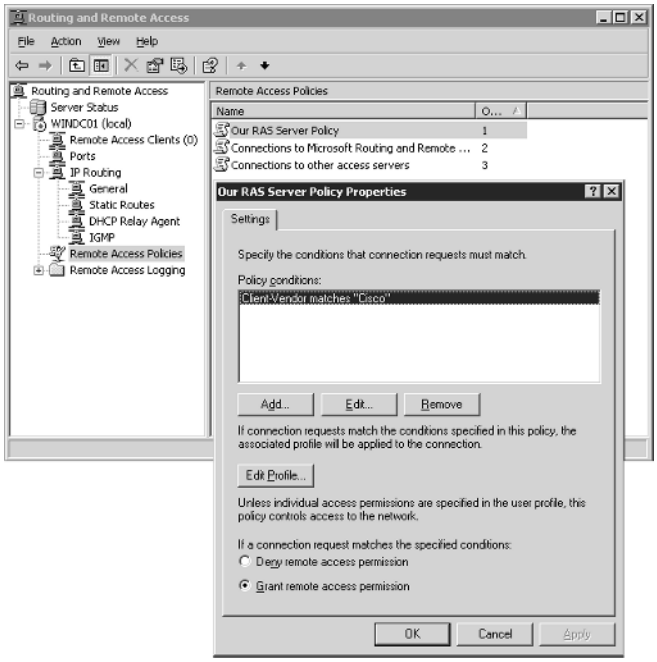
**GPOs don't "live" at the site, domain, or OU level.** GPOs "live" in Active Directory and are represented in the swimming pool of the domain called the Group Policy Objects container. To use a GPO, you need to link a GPO to a level in Active Directory that you want to affect: a site, a domain, or an OU.

**GPOs apply to Active Directory sites, domains, and OUs.** Active Directory is a hierarchy, and Group Policy takes advantage of that hierarchy. There is one local GPO that can be set, which affects everyone who uses that machine. Then, Active Directory Group Policy Objects apply—site, domain, and then OU. Active Directory GPOs "trump" any local policy settings if set within the Local Group Policy.

**Avoid using the site level to implement GPOs.** Users can roam from site to site. When they do, they can be confused by the settings changing around them. Use GPOs linked to the site only to set up special site-wide security settings, such as IPSec or the Internet Explorer Proxy. Use the domain or OU levels when creating GPOs whenever possible.

**Implement common settings high in the hierarchy when possible.** The higher up in the hierarchy GPOs are implemented, the more users they affect. You want common settings to be set once, affecting everyone, instead of having to create additional GPOs performing the same functions at other lower levels, which will just clutter your view of Active Directory with the multiple copies of the same policy setting.

**FIGURE 1.26** RRAS policies are not associated with Windows 2003 Group Policy.



**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 to them. This is much better than applying the settings high in the hierarchy and using Group Policy filtering later.

**Use more GPOs at any level to make things easier.** When creating a new wish, isolate it by creating a new GPO. This will enable easy revocation by unlinking it should something go awry.

**Strike a balance between having too many and too few GPOs.** There is a middle ground between having one policy setting within a single GPO and having a bajillion policy settings contained within a single GPO. At the end of your design, the goal is to have meaningfully named GPOs that reflect the "wish" you want to accomplish. If you should choose to end that wish, you can easily disable or delete it.

**As you go on your Group Policy journey…** Don't go at it alone. There are some nice third-party independent resources to help you on your way. I run `www.GPanswers.com`. My pal Darren Mar-Elia runs `www.GPOguy.com`. And, there's also Microsoft's independent Group Policy Wiki at `http://grouppolicy.editme.com/`. All of these locations are here to help you get more advanced with Group Policy as you progress.