

Window
NET MAGAZINE

TECHNICAL REFERENCE



A Guide to

AutoProf
Intuitive Desktop Management

Group Policy

Robert McIntosh
Randy Franklin Smith
Darren Mar-Elia
Emmett Dulaney
John Savill
Mark Joseph Edwards

Windows
& NET MAGAZINE

The logo for eBooks, featuring a stylized blue 'e' inside a white circle, followed by the word "Books" in a bold, black, sans-serif font.

Enter

Windows & .NET Magazine Technical Reference

A Guide to Group Policy

*By Emmett Dulaney, Mark Joseph Edwards, Darren Mar-Elia,
Robert McIntosh, John Savill, and Randy Franklin Smith*

Windows
& .NET MAGAZINE

A Division of Penton Media

Windows[®]

& .NET MAGAZINE

Copyright 2004
Windows & .NET Magazine

All rights reserved. No part of this book may be reproduced in any form by an electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

It is the reader's responsibility to ensure procedures and techniques used from this book are accurate and appropriate for the user's installation. No warranty is implied or expressed.

ISBN 1-58304-510-4

About the Authors

Emmett Dulaney (edulaney@iquest.net) is a partner in DS Technical Solutions, the creator of TestPro software, and an author. He is an MCT, an MCSE, an A+, an i-Net+, a Network+, and a CNA.

Mark Joseph Edwards (mark@ntsecurity.net) is a contributing editor for *Windows & .NET Magazine* and writes the weekly email newsletter *Security UPDATE* (<http://www.winnetmag.net/email>). He is a network engineer and the author of *Internet Security with Windows NT* (29th Street Press).

Darren Mar-Elia (dmarelia@winnetmag.com) is a contributing editor for *Windows & .NET Magazine* and senior product architect for Windows at Quest Software. His most recent book is *The Tips and Tricks Guide to Windows 2000 Group Policy* (Realtimepublishers.com).

Robert McIntosh (rmcintosh@covenantsolutions.com) is a consultant and trainer who teaches about Microsoft and security technologies and is the founder of Covenant Solutions. He is an MCT, an MCSE, and an ISS-certified instructor.

John Savill (john@savilltech.com) is a qualified consultant in England and an MCSE. He is the author of *The Windows NT and Windows 2000 Answer Book* (Addison Wesley).

Randy Franklin Smith (rsmith@montereytechgroup.com) is a contributing editor for *Windows & .NET Magazine* and the primary instructor and course developer for MIS Training Institute's Windows NT/2000 security program. His firm, Monterey Technology Group, provides security consulting.



Table of Contents

Introduction	ix
Chapter 1: Introducing Group Policy	1
Group Policy	1
What Is Group Policy?	1
Group Policy vs. System Policy	1
How Group Policy Applies	2
Group Policy and Security	2
Security Templates	3
Security Configuration and Analysis	3
Group Policy and Software Management	4
Obtaining the Software Package	5
Publishing vs. Assigning Applications	5
When to Use Group Policy	5
Implementing Group Policy	6
Setting Your Priorities	6
Designing AD with Group Policy in Mind	6
Group Policy and Groups	7
Group Policy Tools	7
Gpmlig.exe	7
Gpresult.exe	8
Gpoutil.exe	8
Some Suggestions	8
Chapter 2: Controlling Group Policy	9
The ABCs of GPOs	9
Group Policy Application Sequence	9
Computer's Local GPO	10
Site-Linked GPOs	10
Domain-Linked GPOs	11
OU-Linked GPOs	11
Multiple Same-Level Links	12
GPO-Level Processing Options	13
Link-Level Processing Options	15
Block Policy Inheritance	16

No Override	16
Disabled	16
System- and User-Level Processing Options	16
Disable Background Refresh of Group Policy	17
Group Policy Refresh Interval for Computers	17
Group Policy Refresh Interval for Users	18
Apply Group Policy for Computers Asynchronously During Startup	18
Apply Group Policy for Users Asynchronously During Logon	18
User Group Policy Loopback Processing Mode	18
Group Policy Slow Link Detection	19
Deferring Group Policy Application	19
Allow Processing Across a Slow Network Connection	19
Do Not Apply During Periodic Background Processing	19
Process Even if the Group Policy Objects Have Not Changed	19
One-Stop Shopping	19
Chapter 3: Group Policy Security Settings	21
Isolate Your DCs from Accidental Changes to Group Policy	21
Least Privilege	24
Group Policy Interworkings	27
Applying Account Policies	28
Hide the Domain Controller	29
Security Without the Shortcuts	29
Chapter 4: Optimize GPO-Processing Performance	31
GPO-Processing Basics	31
Performance Boosters	32
Slow-Link Detection	33
GPO Versioning	33
Asynchronous Processing	34
Sidebar: Group Policy Logging	35
Greater Control	34
Disable Unused Settings	36
Set a Maximum Wait Time	36
Design Matters	36
Limit GPOs	36
Limit Security Groups	37
Limit Cross-Domain Links	37
GPOs: Complex but Powerful	38
Chapter 5: Group Policy for Mobile Users	39
Roaming Users Versus Mobile Users	39
Legacy Clients	39
Windows 2000 Clients	40

Creating the Local Policy	40
Password Policies	40
Local Policies	41
Applying Security Templates	41
Occasional Use of Group Policy	41
Other Considerations for Mobile Users	44
Chapter 6: IPSec and Group Policy	45
A Stronger Defense	45
The IPSec Advantage	45
A Fine Example	46
Configuring the Server	46
Configuring the Clients	47
Authentication Alternatives	49
The Next Step	50
Setting Up a Dedicated Enterprise CA	50
Sidebar: Certificate Templates	52
Configuring Automatic Certificate Requests	52
Sidebar: Group Policy Application	53
Editing the IPSec Policy	54
Maintaining Security	56
Sidebar: Secure Administrative Traffic	57
Sidebar: Extend Security Through Preshared Keys	58
Choose Carefully	56
Chapter 7: Group Policy FAQs	59
What is the difference between Windows 2000's Group Policy and Windows NT 4.0's Group Policy Editor (GPE)?	59
Why can't I run Group Policy Editor (GPE) for a domain even though I'm a domain Administrator?	59
How do I add templates to a Group Policy Object (GPO)?	60
Can I use Group Policy to display or remove the Shut Down button on the logon screen?	61
How do I force a user to use a machine-specific Group Policy rather than a user-specific Group Policy?	62
How do I configure Group Policy to apply folder redirection settings to users who access the local network remotely?	63
How do I use Group Policy to set Advanced Internet Explorer (IE) settings?	63
How do I determine which containers link to Group Policy?	64
How do I properly apply security settings in GPOs?	64
How do I use Group Policy to configure screen savers?	65
How can I locate all the GPOs in my domain?	67
How can I address Group Policy conflicts?	68
How do I configure Group Policy's Effective Setting?	68
How do I prevent Group Policy from applying to the Administrator account?	69
How do I use the registry to configure Group Policy update times?	70

Introduction

Windows 2000 and Active Directory (AD) give Windows networks an enterprise-level management platform. But to use that platform effectively, you must understand how to use Group Policy. Group Policy lets network administrators roll out network security settings, control client desktops, deploy software, and perform a variety of other vital administrative functions. This book provides you with essential information for understanding and using Group Policy in Win2K and Windows Server 2003 networks.

This book begins with an introduction to Group Policy in Chapter 1. In this chapter you'll find answers to basic questions, such as What is Group Policy? You'll also learn how Group Policy can help you manage your networks and how a Group Policy applies to a network's systems. Finally, this chapter introduces you to the basic tools that you need to use to work with Group Policies. Chapter 2 explains how you can control Group Policy. Although Group Policy gives network administrators a lot of power, it also has its share of complexities—if you're not careful, you can inadvertently implement unintended changes throughout your entire forest. In Chapter 2 you'll learn how to take control of Group Policies by understanding the sequence in which Win2K applies policies and learning about the options that let you fine-tune Group Policy Object (GPO) application. Chapter 3 provides you with practical tips that you can use to safeguard your domain from unintended Group Policy actions. Here you'll learn about tips such as isolating your domain controller (DC) from accidental Group Policy changes, as well as how you can apply the concept of change control to help formalize the process of testing and applying new policies. Chapter 4 takes a different management approach to Group Policy by showing you how you can optimize GPO processing performance in your domain. As you use GPOs more extensively to manage your network, your users might experience long startup times as the network applies many GPOs when the system starts up or the user logs on. Chapter 4 explains how you can optimize your GPO infrastructure to minimize the impact of multiple GPOs on end users. You'll also learn how to implement GPO logging to troubleshoot GPO processing problems. In Chapter 5 you'll learn how to implement Group Policies on a mobile workforce. Mobile users present a unique challenge to network management because they often work in a disconnected mode and only occasionally have a direct connection to your LAN. This chapter explains how a combination of local policies, security templates, and Group Policy can help you manage your mobile workforce. Chapters 1 through 5 give you the essential knowledge to understand Group Policy and optimally apply and troubleshoot GPOs. Chapter 6 provides you with a detailed step-by-step approach for creating a specific GPO that implements IP Security (IPSec) on your network. IPSec provides strong network authentication and encryption that can protect the information on your network. Chapter 6 explains how to use Group Policy to set up IPSec on your servers and client systems. Finally, the book concludes with a set of FAQs covering some common Group Policy topics. This book is an invaluable resource, full of vital information that will assist you in mastering Group Policy to effectively manage your AD infrastructure.

Chapter 1

Introducing Group Policy

—by *Robert McIntosh*

Group Policy

Having taught many Windows 2000 classes, I hear some questions and comments repeatedly. For example, students sometimes create test user accounts to experiment with a certain feature. However, when they try to log on as the new user, they can't because normal domain users don't have permission to log on locally to a domain controller (DC). In the dozens of Win2K classes that I have taught, I have yet to see one student figure out how to correctly assign the log on locally right the first time, no matter how much Windows NT 4.0 experience he or she has. Their natural instinct, as was mine, is to log on as an administrator and locate the tool that we use to assign user rights in NT 4.0, User Manager for Domains. Only this isn't NT 4.0, so they look for user rights in the tool that replaced the NT tool's basic functionality, Active Directory Users and Computers.

If they know that Group Policy now controls user rights, along with most other configuration settings, most users still can't make the change effective on the first attempt because they edit the wrong Group Policy Object (GPO). When I demonstrate how and where to make the change, I always hear some variation of the same statement: "This was so much simpler in NT 4.0—why did Microsoft have to make it so complicated?"

What Is Group Policy?

Group Policy is a central component of Microsoft's change and configuration strategy for Win2K. With Group Policy, you can define users' environments and system configurations from one location. The settings you can control with Group Policy include environmental settings, user rights assignment, account policies, folder redirection, script assignment, security settings, and software distribution. In other words, you can control everything from what desktop components users have access to, and where they save files, file system and registry permissions, and Internet Explorer (IE) settings, to what software installs on each Win2K machine in your forest and what software is available for each user to install optionally. As you can see, Group Policy provides tremendous capabilities, and if you understand it and implement it correctly, it can be very useful.

Group Policy vs. System Policy

At first glance, many users think that Group Policy is like NT 4.0's System Policies, but with more capabilities. However, several differences exist. System Policies are useful for setting user desktop configurations by controlling registry settings, whereas Group Policies have much broader configuration capabilities. When you use a System Policy to set a registry configuration, the registry setting is persistent, meaning that even if you remove the policy, the setting remains until you change it manually or overwrite it with another policy. Group Policy's registry configurations aren't persistent; the system removes and rewrites the settings whenever any policy change occurs. You create

System Policies at the domain level, and they apply to users based on group membership. Group Policies apply to users and computers depending on where they reside in the Active Directory (AD); security groups only filter Group Policy.

How Group Policy Applies

As I mentioned, Group Policies are applied based on a user's or computer's location in the AD container hierarchy. Specifically, you apply Group Policies to sites, domains, and organizational units (OUs). If a Group Policy's settings apply to one of these AD containers, then by default, those settings apply to every user and computer object in that container. Users and computers belong to a site, domain, and OU at the same time, so it's important to know that the order in which AD processes GPOs is by site, domain, and OU. By default, if conflicting settings exist in each of these containers, the last one processed is the setting that applies—in other words, the OU settings. In the case of nested OUs, AD processes the GPOs from parent container to child container. So, if you have an OU named North America and an OU named Sales within it, AD will process the Sales GPO after the North America GPO. If any conflicts exist, the Sales GPO's settings will apply because it's the last one that AD processes. Although this order is the typical process in which AD applies Group Policy, you can change this behavior by configuring either Block Inheritance or No Override. If you apply both settings at different container levels within AD, No Override takes precedence over Block Inheritance. As you can see, it's important to design your AD with Group Policy in mind. Otherwise, you'll have an implementation that's very difficult to administer and troubleshoot.

So, how do we give users the right to log on locally to a DC? An AD domain has two built-in GPOs: Default Domain Policy, which applies to the domain, and Default Domain Controllers Policy, which applies to the DC's OU. Using the Microsoft Management Console (MMC) Group Policy Editor (GPE) snap-in, we would focus the snap-in on the Default Domain Controllers OU because that's where the DC's computer object resides.

You're probably still wondering why Microsoft had to make this so complicated. As we delve deeper into Group Policy, I'll provide you with some answers.

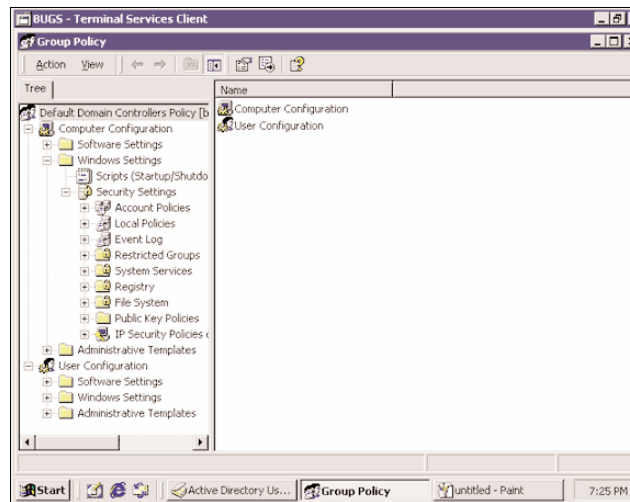
Group Policy and Security

I already discussed Group Policy and how it is applied based on a user's or a computer's location within AD. Next, I look at network security, one of several areas where you can use Group Policy to simplify the tasks that you face as a network administrator. With Group Policy, you can ensure that the machines on your network remain in a secure configuration after you deploy them.

When you create or modify a GPO, you can configure several security settings located under GPE Computer Configuration, Windows Settings, Security Settings. As Figure 1 shows, Security Settings is where you can configure a machine on your network to use IP security and specify settings for everything from user rights to system services. Although some individual settings are easier to configure under NT 4.0, the ability to configure all the settings from one location is a key benefit of Win2K's Group Policy. And because you can apply Group Policy to OUs that contain multiple computers with similar security requirements, it's much easier to apply changes such as assigning permissions to a registry key. One exception is the Account Policies settings, which apply at the domain level and which, by default, the Default Domain Policy sets.

As you can see, Group Policy makes it easy to configure security settings on the machines in your Win2K domain. In addition, two tools, Security Templates and Security Configuration and Analysis, are extremely useful for applying network security policy and evaluating whether individual machines comply with the policy, as Figure 2 shows. With these tools, you can build templates with particular security settings for different groups of machines, apply the settings to the machines, and periodically evaluate the machines to verify that they remain properly configured.

Figure 1
Configuring security settings



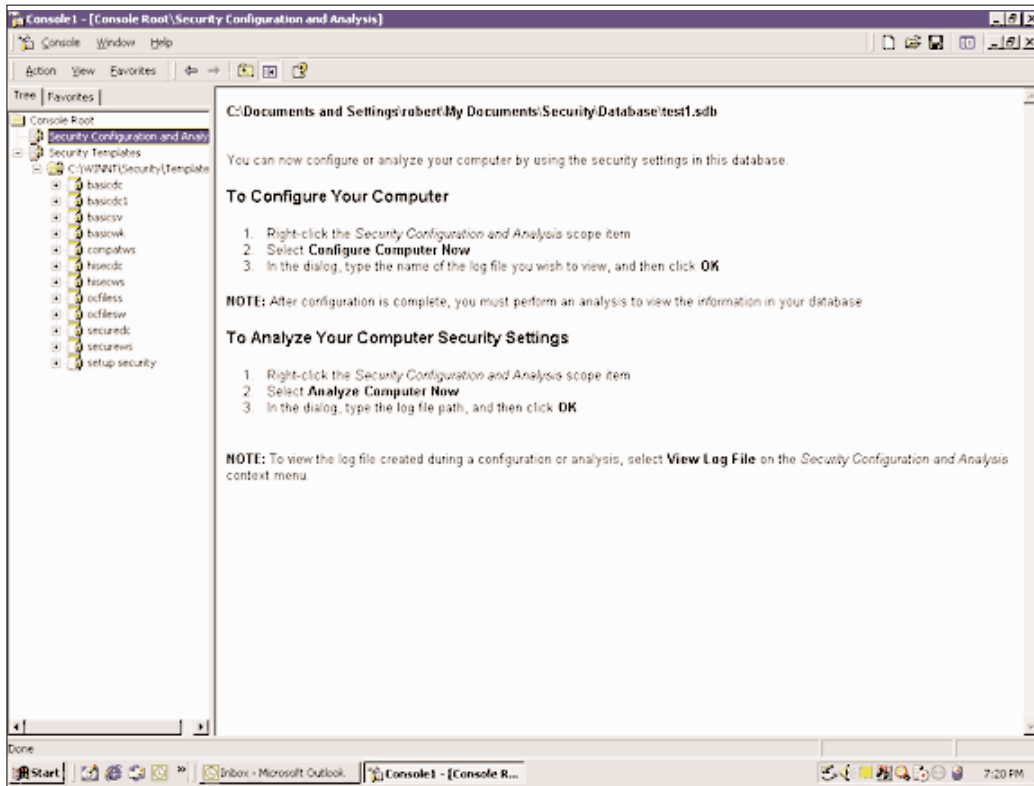
Security Templates

You can use the MMC's Security Templates snap-in to build different templates that you can import into Group Policies. You can either create a new policy from scratch or modify one of the built-in policies. After you decide which template to use, you can import the template settings into your GPO using GPE by right-clicking Computer Configuration, Windows Settings, Security Settings and choosing Import Policy. This process applies all the settings you configured in the template to all the computers in the container (e.g., site, domain, OU) that you link the Group Policy to.

Security Configuration and Analysis

You can use the MMC's Security Configuration and Analysis snap-in to verify that the security settings you apply with Group Policy are in use. Before you perform an analysis, create a database to store the results. After you create and open the database and choose the template containing the settings that you want to apply to a specific machine, right-click the snap-in and choose Analyze Computer Now to check the actual security settings against the desired settings. You can also use Security Configuration and Analysis to apply the security template to the machine, but it's better to use Group Policy. If you use Security Configuration and Analysis to apply the settings, a user can come behind you and change the settings. With Group Policy, if a user changes a security setting, it changes back to its original value the next time Win2K applies the policy.

Figure 2
Applying network security policy and evaluating whether individual machines comply with the policy



On a final note, be sure that you thoroughly test any security templates in a lab environment before rolling them into production. The Win2K default security setting provides a significant increase in security over the NT 4.0 default settings. If you need to ensure compatibility with any non-Win2K certified applications, you might have to use the built-in Compatible Template (compatws.inf) or put your users in the built-in Power Users group. If you want to ensure that all your machines are using the Win2K default settings, you can apply the appropriate default template (basicwk.inf, basicsv.inf, or basicdc.inf). However, if you apply the changes to machines that you upgraded from NT 4.0, you might experience problems with some applications that were working under NT 4.0.

Group Policy and Software Management

One of the more popular gee-whiz features that Microsoft showcases at Win2K events is automated software installations, updates, and removals using IntelliMirror technology. Group Policy

makes this software management possible. Next, I discuss Group Policy and software management, including its configuration, its capabilities, and its limitations.

You can manage software with the Software Installation snap-in, which you can find in GPE's Software Settings folder. The Software Installation snap-in is the same snap-in that you can find in both User Configuration and Computer Configuration, tools that let you distribute software to either users or computers depending on your needs. Using this Group Policy component, you can implement initial application deployment, perform upgrades, apply patches and service packs, and remove previously distributed applications.

Obtaining the Software Package

Before you can use Group Policy to distribute software, you must obtain a Windows Installer package, which, with the Windows Installer service, manages software installation, modification, and removal. A Windows Installer package consists of an .msi file, which is essentially a database that contains information about installing an application. An .msi file is like a setup.exe file, but it provides more control and consistency when installing applications on Win2K and other Microsoft OSs. Recent versions of most applications ship with .msi files that work with the Windows Installer service.

If the application that you want to distribute with Group Policy doesn't have an .msi file, you might be able to create a suitable Windows Installer package using a repackaging program such as the Veritas WinINSTALL Limited Edition repackaging tool, which you can find in the W2K Server CD-ROM's Valueadd directory. If you can't get or create an .msi file, you can use a .zap file, which is basically a text file that contains instructions for deploying an application. Applications that you deploy using a .zap file typically require user intervention, and you can only publish them—you can't assign them.

Publishing vs. Assigning Applications

When distributing software, you must choose whether to publish applications to users or assign applications to users or computers. When you publish an application, you add it to the list of applications that users can install with the Control Panel Add/Remove Programs applet. Publishing applications is a good technique to use when you want to make applications available to some—but not all—users.

You can assign applications to users or computers. When you assign an application to a user, you add it to a user's Programs menu. The first time the user attempts to run the program, it installs—no matter which machine that user is logged on to. When you assign an application to a computer, it installs the next time the machine restarts, regardless of which user logs on.

When to Use Group Policy

Distributing software with Group Policy is extremely useful when you do it correctly. If you don't do it correctly, you can create more problems than you solve. For example, you want your users to use Outlook as their default mail client, so you use the Default Domain Policy to assign the application to all Win2K computers on your network. On Monday morning, everyone arrives at 9:00 A.M. and starts up their computers, triggering a simultaneous network install to all computers in the company. Odds are, your network bandwidth quickly becomes overwhelmed, and most

installations hang. To avoid such calamities, understand the processes you implement and plan your distributions thoroughly.

You can use Group Policy to install Outlook on your organization's computers, but you'd be wise to phase in the installation over time by making the changes to GPOs at the OU level. If that's not possible, consider using Systems Management Server (SMS) for the deployment. SMS lets you perform bandwidth throttling and load balancing, and you can use it to distribute software to non-Win2K clients.

Implementing Group Policy

I've provided an overview of Group Policy and explained how you can use it for everything from distributing software to securing your network environment. Microsoft has built a tremendous amount of capability into Group Policy, and it's a technology that requires a thorough understanding and a great deal of planning before you implement it. Next, I'll focus on some of the planning and technical issues that you need to be aware of before you get started with Group Policy.

Setting Your Priorities

The GPE snap-in includes several settings that you can set within a GPO. In addition to the security and software distribution capabilities I discussed, you can control everything from clients' desktop appearances to what logon and logoff scripts run. With all the available options, deciding what to implement in your environment can be overwhelming.

A good approach is to develop your own Top 10 lists. For example, what 10 issues generate the most support calls to your Help desk, are the highest priority security risks, or cause the most lost productivity for your users? After you develop your lists, identify those issues from your lists that a proper Group Policy implementation could eliminate or greatly reduce. You might decide to limit users' access to the Run command or remove access to the Control Panel Add/Remove Programs applet. If users need access to certain directories or shared resources, you might want to use logon or startup scripts to map drives. Or, perhaps you want to configure NetMeeting and IE settings to specify controls or disable desktop sharing from a centralized location. By focusing on the most important issues for your environment, you can design an implementation that gives you the greatest Return on Investment (ROI). Implemented in this manner, Group Policy helps build the business case for moving to Win2K and AD.

Designing AD with Group Policy in Mind

The Group Policy settings that you apply to a user or computer are based on the user's or computer's location within the AD structure. Group Policies process in the order of site, domain, and OU. So, if you apply a Group Policy that removes the Run command from the Start menu at the site level, adds it at the domain level, and removes it at the OU level, the Run option will disappear from the Run menu when a user logs on who is a member of the OU because that setting applies at the OU level, and it's the last Group Policy that the system applies. If you have a nested OU structure with Group Policies set at each OU level, the Group Policies process from parent to child, and the policy associated with the immediate parent OU that the user or computer object belongs to is the last one that the system applies.

By now, you should realize the importance of identifying your Group Policy objectives before you design your AD structure. If you implement your AD without considering Group Policy, you are likely to end up with a structure of unnecessary complexity that requires disruptive troubleshooting. Particularly, consider Group Policy when you design your OU structure. OUs are primarily beneficial from an administrative perspective, specifically in delegating administration and assigning Group Policy (because the Group Policy settings you apply at the OU level are, by default, the last ones that the system applies).

Group Policy and Groups

You might expect that you use group membership to assign Group Policies, when in fact you don't assign Group Policies to groups, but rather to sites, domains, and OUs. But groups do let you filter Group Policy settings, which is important. Imagine that you want to prevent users from changing configuration settings, so you create a Group Policy that limits access to the Control Panel. Such a limitation is generally a good solution, unless a user who's logged on at the time is a member of the technical support group and needs to have access to the Control Panel to resolve a problem. To avoid this situation, you can set permissions in the GPO's properties to control who in the site, domain, or OU the settings apply to. For users or computers to receive the settings you apply, they must have Read and Apply Group Policy permissions to that GPO. The authenticated users group has these permissions by default, so to prevent a specific GPO from applying to users, you have to add their group and remove the Apply Group Policy permission from them.

Group Policy is a tremendously powerful feature of Win2K. Implemented correctly, it can provide compelling justifications for moving to Win2K and AD. But implementing it correctly requires a great deal of understanding and planning. For more information, see Microsoft's Group Policy white paper at <http://www.microsoft.com/windows2000/techinfo/howitworks/management/groupolwp.asp>.

Group Policy Tools

Now that I've covered Group Policy capabilities and implementation, let's discuss three helpful troubleshooting tools included in the *Microsoft Windows 2000 Resource Kit*. I'll also share some tips I learned from my own experience that might help you as you design your own Group Policy implementation.

Gpolmig.exe

First, let's talk about migration. Because of the differences that exist between Win2K Group Policies and NT 4.0 System Policies, I recommend that you build your GPOs from scratch instead of migrating your existing System Policy settings. Group Policy capabilities are more extensive than System Policy capabilities, and you must apply Group Policies differently. In other words, the differences between the technologies are too great to justify a migration effort. However, if you really must perform a migration, you can use the resource kit utility *gpolmig.exe*, a command-line tool that lets you migrate settings from NT 4.0 System Policies to Win2K GPOs. Because of NT 4.0 and Win2K registry and setting-location differences, you need to test GPOs after the migration to verify that they're producing the desired effect.

Gpresult.exe

Most of the troubleshooting questions I've received ask why a particular Group Policy affects a particular user or computer or why a GPO isn't producing the desired results. In these situations, the resource kit utility `gpresult.exe` can be very useful. `Gpresult.exe` is a command-line utility that lets you see which GPOs you've applied to the local machine and the user who's logged on. `Gpresult.exe` also lets you see software you installed using Group Policy, folders you've redirected using Group Policy, IP Security (IPSec) settings, disk quota information, applied registry settings, and information about the last time you applied Group Policy. In other words, `GpResult` tells you not only what GPOs you've applied to the user and computer, but also what effect those GPOs have had. `GpResult` can accomplish in a few seconds what might otherwise take half an hour to figure out using Active Directory Users and Computers and GPE.

If we review how you apply GPOs, we might answer many of your migration and troubleshooting questions before they arise. Remember that you apply GPOs to computer objects and user objects based on where those objects reside in the AD hierarchy. When you look at a GPO in GPE, you see that it consists of Computer Configuration, which applies to computer objects, and User Configuration, which applies to user objects. If a user's user object—not the computer object representing the machine that the user logs on to—resides in the Sales OU, and you apply a GPO to the Sales OU, only the GPO's User Configuration settings will apply to that user. The Group Policy settings that apply to the computer configuration will come from the GPO that you apply (or link) to the OU that the computer object is a member of. This arrangement might seem complex, but in a large environment, it's more manageable than System Policy. You apply System Policies to groups, but a user can be a member of multiple groups, all of which can have different System Policies applied. The advantage of Group Policy's application is that a user or a computer will exist in only one AD location at a time.

Gpotool.exe

Another resource kit tool that's useful for supporting Group Policy is `gpotool.exe`. Client machines receive Group Policy settings from the Win2K DC that authenticates them. The authenticating DC stores these settings in its SYSVOL share, and its SYSVOL contents replicate to every other DC in the domain. This replication ensures that you apply the same Group Policy settings regardless of which DC performs authentication. `Gpotool.exe` checks to verify that replication occurs properly by comparing the GPO instances on each DC and verifying their consistencies. This step can be useful when you have to troubleshoot inconsistencies.

Some Suggestions

When you begin to realize all of Group Policy's capabilities, you might feel like the proverbial kid in the candy store. However, like that kid, you can run into problems if you try to implement too much too quickly. Instead of trying to implement a Group Policy design that accomplishes everything, start simply. For example, identify a Top 10 list of problems that your IT support group faces and design Group Policies to address those issues. Also, think as broadly as possible, identifying Group Policy settings that should apply to the vast majority of the users and computers on your network. Such thinking will help you implement a design that you can apply at the domain level with one or a few GPOs, which will simplify troubleshooting.

Chapter 2

Controlling Group Policy

—by Randy Franklin Smith

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

The ABCs of GPOs

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

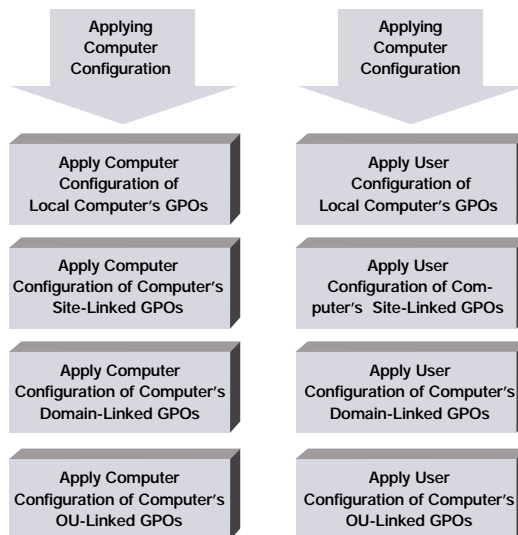
Every Win2K computer stores a local GPO. To let you simultaneously manage multiple computers or users, Win2K lets you link other GPOs to Active Directory (AD) containers, such as organizational units (OUs); Win2K then applies the linked GPOs to all the computers or users in those containers. If you link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

Group Policy Application Sequence

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

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

Figure 1
Win2K's GPO-application sequence



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

Computer's Local GPO

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

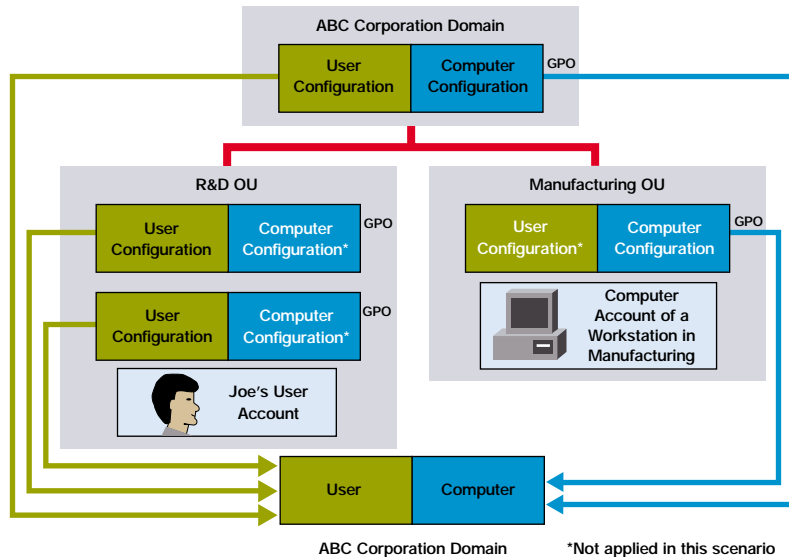
Site-Linked GPOs

When the computer is a member of a domain, Win2K next applies all the GPOs that link to the computer's site. (Sites are AD objects that represent a network's physical layout.) Use site-linked

GPOs only when you need to define a setting (e.g., a network parameter) that is specific to the computer's physical portion of your network. To view a list of a site's GPOs, go to Administrative Tools, Active Directory Sites and Services. Right-click a site, click Properties, and select the Group Policy tab. Win2K doesn't come with any prebuilt site-linked GPOs, and administrators seldom define site-linked GPOs.

Figure 2

Win2K bases domain- and OU-linked GPOs on the user account's domain and branch of the OU tree instead of the computer's location in AD



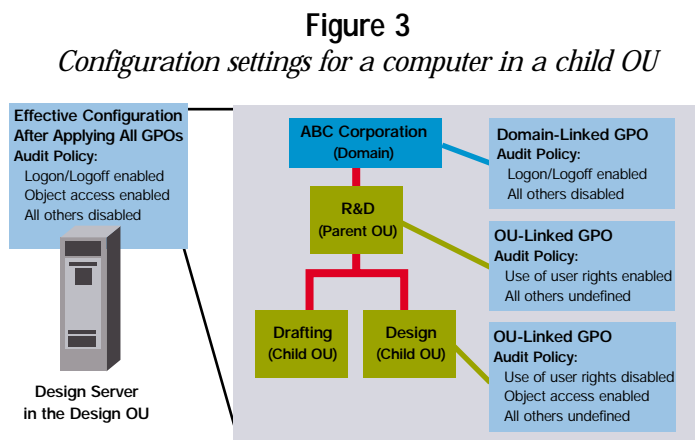
Domain-Linked GPOs

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

OU-Linked GPOs

Finally, Win2K applies GPOs that link to any OUs that contain the computer—or the user, in the case of User Configuration. If more than one OU contains the computer or user, Win2K applies the linked GPOs in order from the highest OU to the lowest OU. Because the last-applied GPO overrides previously applied GPOs, lower-OU-linked GPOs override higher-OU-linked GPOs whenever both GPOs define a value for the same setting. (Figure 3 shows the configuration

settings for a computer in a child OU; Win2K will apply several OU-linked GPOs as well as a domain-linked GPO to the computer.) To view OU-linked GPOs, right-click the OU, click Properties, and select the Group Policy tab.



Multiple Same-Level Links

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

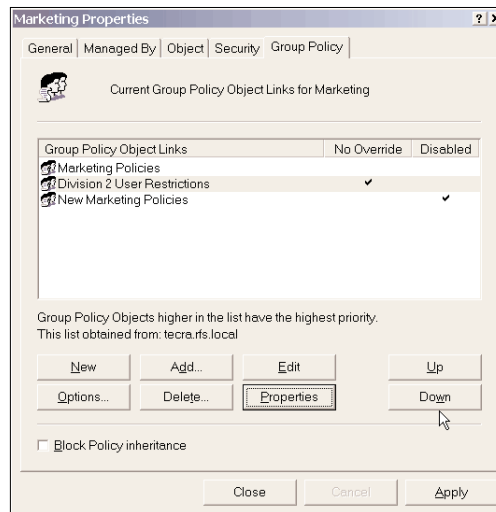
Keep in mind that an important difference exists between a GPO and a link to a GPO. When you delete a GPO, Win2K no longer applies the GPO under any circumstance. When you delete a link, Win2K still applies the GPO to other AD containers to which the GPO is linked. Imagine that a GPO is like a human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

Win2K follows a straightforward GPO-application process. Group Policy's true complexity lies in your options for controlling that process, which I explain next.

I explained how Windows 2000 uses GPOs and the sequence in which Win2K applies them. But you can't truly control Group Policy until you understand the processing options that let you fine-tune your policies. Because you can link a GPO to sites, domains, or OUs, you can control

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

Figure 4
Viewing the Group Policy tab of an example Marketing OU



GPO-Level Processing Options

A GPO has settings that affect a Win2K computer's configuration and a user's profile. The GPO stores computer settings in a Computer Configuration subfolder and stores user settings in a User Configuration subfolder. If you create a GPO that contains only computer settings, you can disable the GPO's User Configuration portion to reduce users' logon time. Likewise, if you define only user settings, you can disable the GPO's Computer Configuration portion to reduce system boot-up time. To disable either portion of a GPO, go to Administrative Tools, Active Directory Users and Computers. Right-click the domain or OU to which the GPO is linked, click Properties, and select the Group Policy tab. Select the appropriate GPO, and click Properties. Go to the General tab, which Figure 5 shows, and select either the *Disable Computer Configuration settings* check box or the *Disable User Configuration settings* check box. These settings are both GPO-level settings.

When you disable a GPO's Computer Configuration or User Configuration portion, Win2K disables that portion in every site, domain, or OU to which the GPO is linked. Therefore, before you make this type of GPO-level change, you need to determine how the change will affect those sites, domains, and OUs. To see a complete list of these linked elements, open the GPO's Properties dialog box and go to the Links tab, which Figure 6 shows. Select a domain from the Domain drop-down list and click Find Now. Win2K will search the specified domain and display each site

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

Figure 5
Viewing the General tab

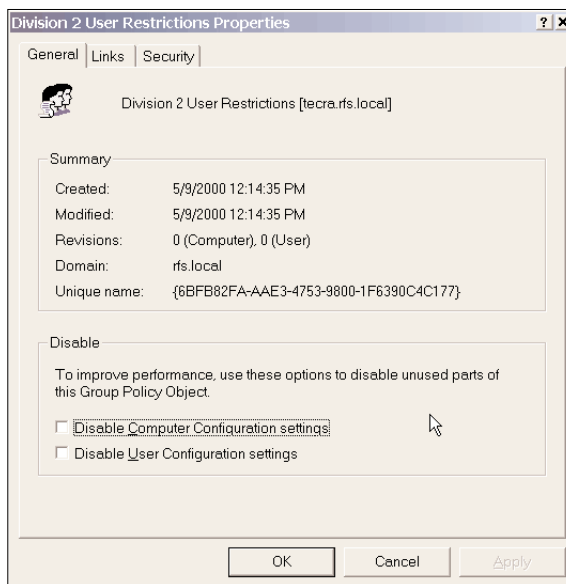
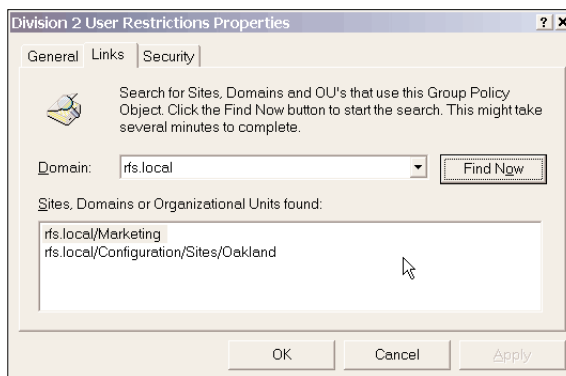


Figure 6
Viewing the Links tab

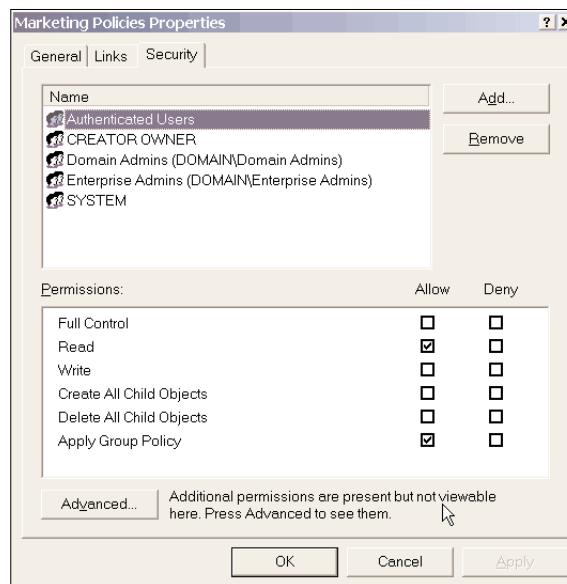


One way to fine-tune a GPO's application is through a GPO's ACL, which defines both who has permission to maintain the GPO and which computers and users Win2K applies the GPO to.

To access the ACL, open the GPO's Properties dialog box and go to the Security tab, which Figure 7 shows. When a Win2K computer that is a member of a Win2K domain boots up, the computer logs on to AD and uses its corresponding computer account in AD to look through its domain, sites, and OUs and determine which GPOs it needs to apply. When applying Group Policy to a computer, Win2K determines whether the computer account has permissions to read and to apply Group Policy for each GPO. If not, Win2K ignores the GPO for that computer. User accounts also require both Read and Apply Group Policy access; Win2K goes through the same determination process each time a user logs on and whenever Win2K reapplies Group Policy.

As Figure 7 shows, Authenticated Users (i.e., all computer and user accounts) have both permissions by default. When you want to disable a GPO's application to specific computers or users in an OU, you can open the GPO's ACL and add an access control entry (ACE) that denies Apply Group Policy access for the groups or accounts that you want to exempt. To view a GPO, you need Read access; to edit a GPO, you need Write access.

Figure 7
Viewing the Security tab



Link-Level Processing Options

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

other sites, domains, or OUs to which the GPO is linked remain unaffected.) You can choose among three link-level processing options.

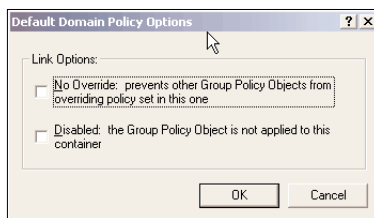
Block Policy Inheritance

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

No Override

Administrators typically enable this setting at a domain level to enforce corporate password and account policies. The No Override setting overrides all lower-level *Block Policy inheritance* settings. For example, when you enable No Override for a site-level GPO link, Win2K applies that GPO to all computers in the site, regardless of the domain's or OU's *Block Policy inheritance* setting. When you enable No Override for a domain- or OU-level GPO link, Win2K applies that GPO to all computers and users, regardless of any lower OUs' *Block Policy inheritance* settings. To enable or disable the No Override setting, select the appropriate GPO from the Group Policy tab and click Options. Select the No Override check box, which Figure 8 shows.

Figure 8
Selecting the No Override and Disabled check boxes



Disabled

Disabling a GPO link is useful when you need to temporarily eliminate the GPO's effect on configuration (e.g., while debugging policy or temporarily suspending a restriction). When you disable a GPO link to a site, domain, or OU, Win2K won't apply the GPO to that site, domain, or OU. By disabling rather than deleting the link, you can more easily reinstate the GPO. To change the Disabled setting for a GPO link, select the appropriate GPO from the Group Policy tab and click Options. Select the Disabled check box, which Figure 8 shows.

System- and User-Level Processing Options

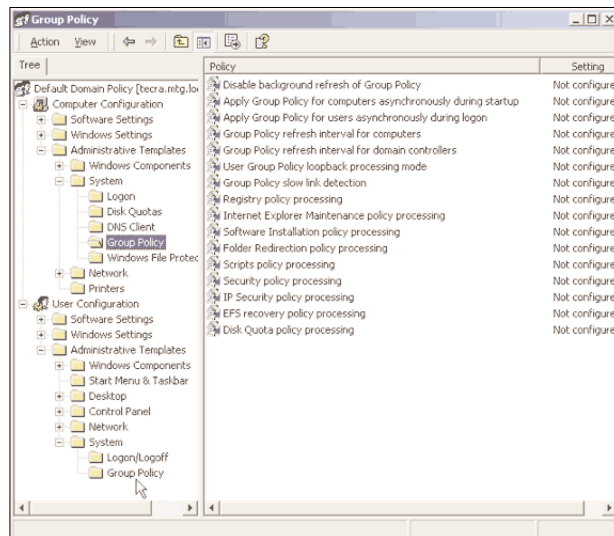
Another set of processing options exists as settings within each GPO; you define these settings at the system or user level. As I explained, each GPO contains a Computer Configuration subfolder

and a User Configuration subfolder; in other words, each GPO has a Group Policy folder under \computer configuration\administrative templates\system and another folder under \user configuration\administrative templates\system, as Figure 9 shows. These folders contain settings that control how Win2K applies Group Policy to every computer and user that links to that GPO.

Changing the Computer Configuration settings for one GPO can affect a system's application of all GPOs. For example, suppose you go to the Marketing OU, create a new GPO, and select the *Disable background refresh of Group Policy* system-level setting. The next time a computer in that OU boots up or refreshes, the system will encounter the new GPO and change the setting in the local system configuration. After making the change, the system will disable background refresh of every GPO, not only of the GPO for which you enabled the setting.

Figure 9

Viewing the Computer Configuration and User Configuration subfolders



Disable Background Refresh of Group Policy

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

Group Policy Refresh Interval for Computers

This setting controls the frequency at which Win2K refreshes Group Policy for Win2K Professional workstations and Win2K member servers (not for domain controllers—DCs). You can use this setting to specify two thresholds: the number of minutes between refreshes and an offset that Win2K uses to prevent every computer from simultaneously rereading Group Policy from the DC. Win2K

computes a random value between zero and the offset, then adds this value to the first threshold after each refresh to determine when the next refresh will occur. By default, Win2K refreshes every 90 minutes and specifies a maximum offset of 30 minutes. The setting applies to policies under the Computer Configuration portion of a GPO.

Group Policy Refresh Interval for Users

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

Apply Group Policy for Computers Asynchronously During Startup

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

Apply Group Policy for Users Asynchronously During Logon

By default, after a user enters a username and password, Win2K doesn't display the user's desktop until it finishes applying Group Policy's User Configuration settings. When you enable the *Apply Group Policy for users asynchronously during logon* setting, users can access the Start menu and desktop before the application is complete. Some policies might not take effect until the next logon or until Win2K refreshes Group Policy. This setting applies to policies under the User Configuration portion of a GPO. Unless users complain about excessive startup or logon times, I recommend you leave both asynchronous-application settings disabled so that you can maintain predictable Group Policy application.

User Group Policy Loopback Processing Mode

When Win2K applies the User Configuration portion of Group Policy, Win2K determines the applicable GPOs based on the user's domain and OUs and applies settings from the User Configuration portion of those GPOs. In other words, Win2K applies User Configuration settings based on the user account's location in AD (i.e., who the user is), not based on the computer account's location (i.e., which computer the user is logging on to). However, you might decide to make an exception to this rule. For example, perhaps you have public-use kiosks for which you want to define specific User Configuration settings regardless of who logs on. In such a situation, you need to create an OU to contain the kiosks, then create an OU-linked GPO and enable the GPO's *User Group Policy loopback processing mode* setting. When you enable this setting, you must select one of two option modes. Replace mode tells Win2K to ignore the user's User Configuration settings (i.e., the User Configuration settings based on the user account's location in AD) and instead apply the system's User Configuration settings (i.e., the User Configuration settings based on the system's location in AD). Merge mode tells Win2K to first apply the user's User Configuration settings, then

apply the system's User Configuration settings. Whenever a conflict occurs, the system's settings take precedence.

Group Policy Slow Link Detection

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

Deferring Group Policy Application

Win2K divides Group Policy into nine processing categories: Registry, Internet Explorer (IE) Maintenance, Software Installation, Folder Redirection, Scripts, Security, IP Security (IPSec), Encrypting File System (EFS) recovery, and Disk Quota. Each category has a corresponding Group Policy option (e.g., Registry policy processing) that resides in `\computer configuration\administrativetemplates\system\group policy`, as Figure 9 shows.

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

Allow Processing Across a Slow Network Connection

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

Do Not Apply During Periodic Background Processing

Select this option to defer processing during background refreshes while a user is logged on. This option defers refreshes in specific categories, whereas *Disable background refresh of Group Policy* defers refreshes in all categories.

Process Even if the Group Policy Objects Have Not Changed

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

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

One-Stop Shopping

Group Policy provides one-stop shopping for computer and user profile configuration. To keep a handle on Group Policy complications, you need to minimize your use of settings such as *No*

Override and *Block Policy inheritance* and customize GPO ACLs only when absolutely necessary. To keep Group Policy simple, use options that are visible on the GPO Properties, Group Policy tab. To control who receives which policies, use OUs, rather than GPO permission restrictions; resort to restrictions only for troublesome exceptions that would otherwise require you to completely redesign your OU hierarchy.

Table 1
Group Policy Processing Categories

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

Chapter 3

Group Policy Security Settings

—by Randy Franklin Smith

When I once presented a Windows 2000 security seminar, one of my students made a simple change to rights assignments in Group Policy, and I discovered how easy it is to lock everyone out of an Active Directory (AD) domain. The incident taught me how important it is to use strict change-management controls, to follow least-privilege doctrine, and to implement some fail-safe measures in AD to protect domain controllers (DCs).

The student, Bob, had completed the hands-on exercises for working with rights assignments using Group Policy and decided to experiment—something I always encourage. Bob edited the Default Domain Policy Group Policy Object (GPO), maneuvered to Computer Configuration, Windows Settings, Security Settings, Local Policies, Rights Assignments, and assigned the *Deny access to this computer from network* right to Everyone. This deny right prevents users with the proper permissions from connecting to any Win2K resources on the computer over the network—basically, all file or printer sharing and any resources in Computer Management, such as the event log, services, and local users and groups. (Users can still connect to other services that don't use Win2K authentication, such as anonymous Web or FTP connections.) Because Bob assigned this right at the root of the domain, the deny right applied to all computers in his domain. Furthermore, because Bob assigned the right to the special Everyone group, he locked everyone out of all the computers in the domain.

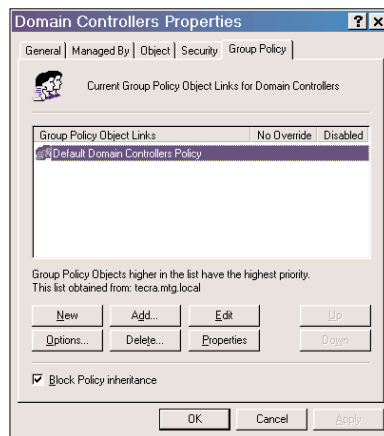
When Bob brought the problem to my attention, we thought we could simply log on locally to the DC. Then we tried to edit the Default Domain Policy GPO to correct the problem, thinking that we'd be using a local connection and would bypass the *Deny access to this computer from network* right. Unfortunately, that approach didn't work either. Whenever you try to edit a GPO, even when you're logged on locally to the DC, Win2K uses a Lightweight Directory Access Protocol (LDAP) network connection to access the AD groupPolicyContainer object, and uses a file-sharing connection to access Group Policy-related files on a shared folder on the DC called sysvol. If the classroom test domain had been a production domain, Bob would have been in big trouble because no one could log on and use any resource on any computer in the domain. Although the problem was the result of one simple change, Bob's only recourse was to restore the DC from a backup, or do a low-level edit of the appropriate Group Policy file on the DC while logged on locally. Unfortunately, the latter option isn't much of an option—the format of Group Policy files is not well documented. You can use three strategies to protect your domain from accidents like this. Let's look at the first strategy.

Isolate Your DCs from Accidental Changes to Group Policy

If you can keep your DCs stable, you should always be able to get into AD and Group Policy to correct any problems. To isolate your DCs, you need to lock down the Group Policy options on the root of your domain and each DC's organizational unit (OU). To lock down a DC's OU, open

Active Directory Users and Computers, and click the OU of Domain Controllers. Create a new group called Domain Controllers GPO Administrators, and populate it with only the people who you have authorized to configure DCs. Right-click the Domain Controllers OU, select Properties, and click the Group Policy tab, as Figure 1 shows. Check *Block Policy inheritance* to prevent GPOs at the root of the domain from affecting DCs. (Note: You might need to duplicate some policies in the Domain Controllers OU if you want to apply the policies to all computers in the domain, including DCs.) Next, select the GPO for the Default Domain Controllers Policy, and click Properties. Select the Security tab, and click Advanced. Under the Permissions tab, click Remove to delete the entries for Domain Administrators and for Enterprise Administrators. Click Add to create an entry that grants full control to the Domain Controllers GPO Administrators, as Figure 2 shows. This step also implements a safeguard that prevents Domain Administrators or Enterprise Administrators from changing this GPO unless they purposely take ownership of it. Next, go back to the Domain Controllers Properties, as Figure 1 shows, and select the Security tab. Clear *Allow inheritable permissions from parent to propagate to this object*. When you are prompted to copy or remove inherited permissions, select Copy, and remove any entries that grant any access to Administrators, Domain Administrators, or Enterprise Administrators. Give full control to your new Domain Controllers GPO Administrators group, as Figure 3 shows. These two changes prevent other administrators from accidentally creating new GPOs in the Domain Controllers OU or clearing the *Block Policy inheritance* check box.

Figure 1
Locking down a DC's OU



At this point, you've isolated your DCs from changes that users make outside their OU and from mistakes administrators might make. However, DCs will still receive any policies you defined in GPOs that you linked to the domain root, where you can check the *No override* check box—*No override* takes precedence over *Block Policy inheritance*. To guard against overriding your policies, you can add an ACL entry on each GPO linked to the root of the domain that explicitly denies Read and Apply Group Policy access to the Domain Controllers Group. If you've flagged a domain

root-linked GPO as *No override*, when a DC tries to read and apply the GPO, the GPO will deny access. Next, I'll show you how to use change control techniques and least privilege to protect the rest of your domain from administrator mistakes.

Figure 2

Creating an entry that grants full control to the Domain Controllers GPO Administrators

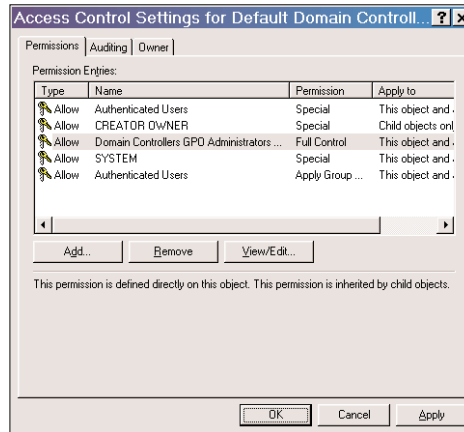
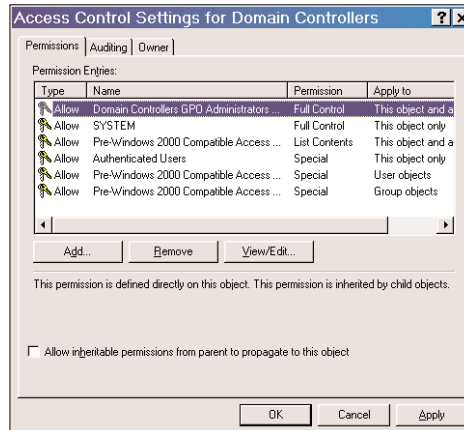


Figure 3

Giving full control to the Domain Controllers GPO Administrators group



Nowhere is change control more important than in AD and Group Policy: A directory service (i.e., AD) and centralized configuration solution (i.e., Group Policy) are fundamental to your IT infrastructure. However, many systems administrators make the mistake of implementing changes in production without a review-and-release cycle that includes peer review and advance mainte-

nance announcements. Change control has always been strong in the mainframe world, but it has never fully matured in the Windows world. Unfortunately, as the opening example illustrates earlier in this chapter, Win2K can make a potentially devastating and wide-ranging change appear to be simple and harmless.

Change Controls

Change control is a concept that software developers adopted after they learned the hard way that uncontrolled changes to source code in production environments wreaks havoc. The key items to implement in your change control process are formalized testing, impact analysis, and separation of the developer and the installer. You should always test new policies before actually changing them in production GPOs. I recommend that you first create a Testing OU, add a computer and some test users to this OU, and test your proposed changes. When you're satisfied with the results, carefully make the same changes in the appropriate production GPO. Prior to making the changes in production, ask a colleague to check your work, and discuss any impact issues that you need to take care of, such as informing users of changes to their desktop that some Group Policy settings cause. If you have a large domain of many users in which the possible damage from mistakes is high, you might consider creating a special GPMaintenance user account where you can lock down GPOs so that only GPMaintenance has Write access. You can channel all changes to Group Policy through the person to whom you assign that account. Not only will using least privilege and change control protect you from mistakes, you'll also have a neater domain that's easier to manage because subadministrators won't be able to clutter up the domain with unneeded objects.

Least Privilege

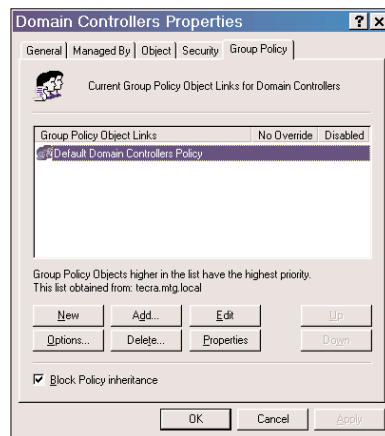
One of the best ways to facilitate change control is to follow the least-privilege doctrine, whereby you grant all IT staff members the minimum authority they need to do their jobs. If you limit their authority to change your environment, fewer users can shoot themselves in the foot. You couldn't follow least-privilege practices with Windows NT because of NT's monolithic, all-or-nothing administrative authority structure. However, with Win2K, you can follow least-privilege practices because each object (e.g., domain, site, OU, user, group, GPO) has its own ACL that controls who can do what to each object. To follow least-privilege practices, follow a few simple rules. First, don't put users in AD's Enterprise Admins, Domain Admins, or Administrators groups. Hardly anyone in a medium-to-large organization should have unlimited authority to the entire network. Second, when delegating maintenance of an OU in your domain to another administrator, don't delegate full control of the OU. Typically, the work you delegate involves maintaining the users or groups in that OU. If you grant full control of the OU, you also let that administrator completely change how to apply Group Policy to the users and computers in that OU.

Two types of objects in AD control who can edit and impact Group Policy: OUs and GPOs. Be careful when you edit the ACLs of these two types of objects—don't delegate more authority than necessary; you can end up with policy changes you don't want.

Each GPO has an ACL that controls who can access the GPO and how. To view a GPO's ACL, open AD, the Microsoft Management Console (MMC) Active Users and Directory Computers snap-in, right-click an OU where you know you have a linked GPO, and select Properties. In the Properties window of that OU, click the Group Policy tab. To view that GPO's properties, select the GPO you want, as Figure 4 shows, and click the Properties button, which will display the

Properties window for the GPO you selected in Figure 4, and select the Security tab to view the GPO's ACL. Note any user or group that you've assigned Full Control or Write access. Either of these permissions lets the user edit the GPO, which affects all users and computers associated with this GPO. Because GPOs define policies for almost every aspect of a Win2K computer, anyone with write access to a GPO has, in effect, administrator authority over all the computers where Win2K applies the GPO. Remember: You can link a GPO to more than one OU; however, no matter how many places you link a GPO, it has only one ACL.

Figure 4
Selecting the GPO



To keep control of Group Policy changes, you should also be careful with OU permissions. The list and options you see on the Group Policy tab of an OU's Properties window correspond to two properties present on every OU: gpLink and gpOptions. gpLink corresponds to the List of GPOs in Figure 4. gpOptions corresponds to the *Block policy inheritance* check box, as the same figure shows. Any user who has Write access to gpOptions can select this check box and prevent important policies you've already defined from taking effect with the users and computers in this OU. Any user with Write access to gpOptions can add or delete GPOs that link to the OU. To view property-level permissions for an OU, select the Security tab that Figure 4 shows, and click Advanced, which will display Figure 5, to display the advanced view of the OU's ACL, as Figure 6 shows. Double-click any of the access control entries (ACEs), and select the Properties tab, as Figure 7 shows. Be aware that granting high-level Full Control or Write access, as Figure 5 shows, also grants Write access permission to gpLink and gpOptions.

If you tightly control who has write access to existing GPOs and to gpLink and gpOptions properties on OUs, you'll be able to worry less about careless or uncooperative administrators who want to contradict policies you define higher in the domain. When you need to delegate authority over an OU to another administrator, think carefully about what abilities the person really needs rather than assigning full control to them. Use the delegation of the control wizard to create custom tasks that include only the amount of authority the other administrator needs.

Although Group Policy is a powerful tool for handling the gargantuan task of configuring Win2K security, it can also cause problems. To avoid these pitfalls, you need to understand how Group Policy works internally, as well as how it works with various Win2K components. Let's look at several important, undocumented caveats that you need to be aware of when using Group Policy that can help you prevent some serious mistakes.

Figure 5
Viewing property-level permissions for an OU

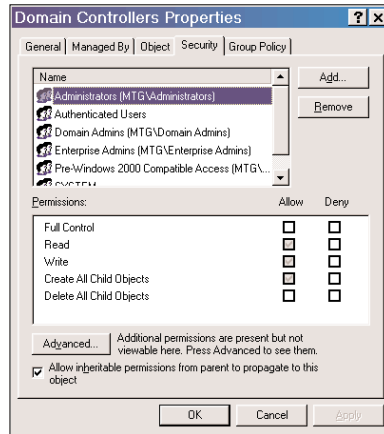


Figure 6
Displaying the advanced view of the OU's ACL

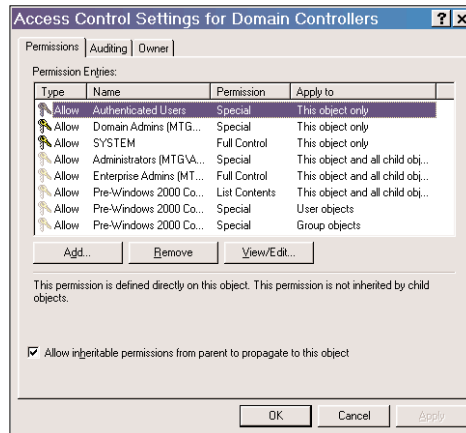
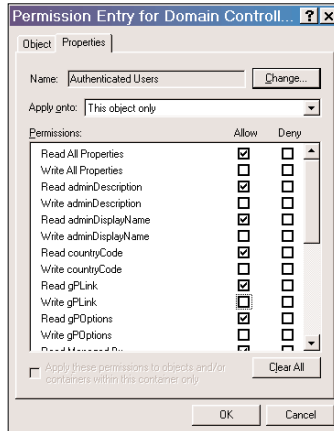


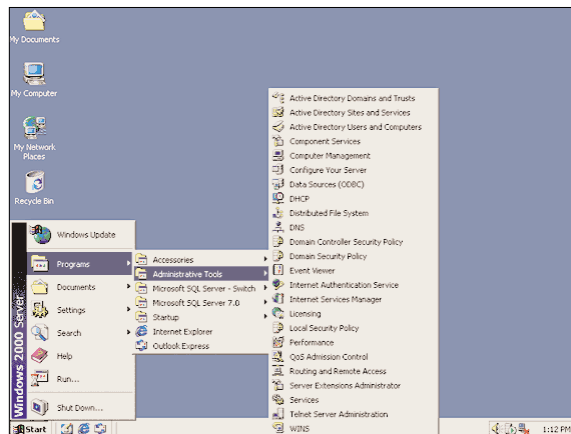
Figure 7
Viewing an ACE's properties



Group Policy Interworkings

Win2K includes shortcuts to two security policies, Domain Security Policy and Domain Controller Security Policy, under Administrative Tools, as Figure 8 shows. Domain Security Policy is a GPO in AD that links to the domain, and Domain Controller Security policy is a GPO that links to an OU called Domain Controllers.

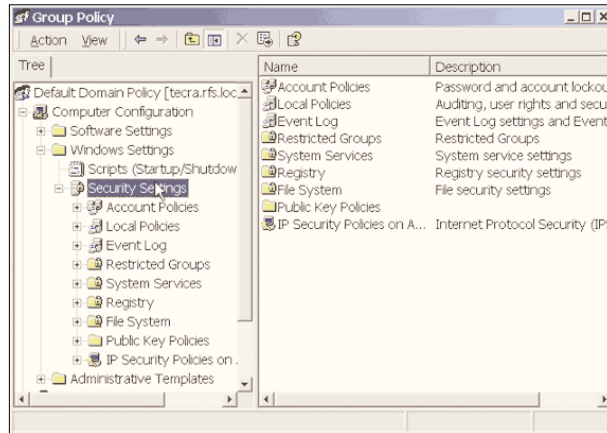
Figure 8
Accessing Domain Security Policy and Domain Controller Security Policy



When you promote a member server to a domain controller (DC) using `dcpromo.exe`, Win2K moves that server's computer object in AD to the Domain Controllers OU. At first glance, you

might think that Domain Security Policy specifies the default policy for general computers in the domain and that Domain Controller Security Policy specifies the policy for all DCs and domain accounts—that’s almost true. The one exception has to do with Account Policies, which is the first folder under a GPO’s Security settings, as Figure 9 shows.

Figure 9
Viewing Account Policies



Applying Account Policies

Account Policies defines user account password requirements and lockout thresholds. In NT 4.0, the OS stores domain user accounts in the DC’s SAM, which is simply a registry hive under HKEY_LOCAL_MACHINE. Any account policies that you define in the DC’s SAM control domain user accounts. In Win2K, the OS doesn’t store domain user accounts in the SAM. Instead, it stores these accounts in the AD replica on the DC. Although every Win2K DC has a SAM, its users and groups are dormant. As a result, the local password requirements and lockout policies on DCs don’t apply to domain user accounts.

Any account policies that you define in GPOs that link to DCs also don’t apply. To prove it, try this little experiment. Set the Minimum Password Length to 0 in Domain Security Policy, and set the Minimum Password Length to 7 in Domain Controller Security Policy. Force an immediate application of Group Policy by typing

```
secdit /refreshpolicy machine_policy /enforce
```

at a command prompt, and give the system a few seconds to refresh. Next, try to create a user account with a password that has fewer than seven characters, such as “abc.” Win2k will permit the operation. This caveat means you might have a false sense of security if you have specified stricter account and lockout policies at the DC level than at the domain level, thinking you are protecting domain accounts. GPOs linked at the domain level are the only ones that affect account policies for domain user accounts. Account Policy is the only setting under GPOs that is subject to

this phenomenon. Win2K applies other policy settings, including rights, permissions, and services, according to the relevant GPOs for each computer, which leads to another caveat.

Hide the Domain Controller

Win2K initially places new DCs in the Domain Controllers OU, but they don't have to stay here—you can move them to any other OU in the domain, yet another difference between Win2K and NT DCs. In NT, the entire SAM and Security registry hives replicate to each DC. These two registry hives constitute all the options under User Manager, including accounts, groups, account policy, audit policy, and rights assignments. Thus, you can't specify different audit policies or user rights assignments for each DC in NT. In Win2K, AD—not the SAM and Security registry hives—replicates to each DC. Therefore, if you scatter DCs into other OUs, they can easily end up with different policies. I don't recommend that you do this, but you need to be aware of the technical capability to protect yourself from seemingly unexplainable network changes that occur over time as administrators come and go. Make sure you include a check in your assessments to verify that all DCs are still in the same OU.

Security Without the Shortcuts

A final related caveat involves the Domain Security Policy and Domain Controller Security Policy shortcuts under Administrative Tools, which I mentioned earlier. Although these two shortcuts correspond to GPOs that typically link to their respective places in AD, don't count on it. I've already seen a situation in which someone inadvertently deleted the link to the Domain Security Policy GPO in the Group Policy tab of the domain properties. The administrator was scrupulously maintaining policy using the appropriately labeled shortcut, but because the domain no longer linked to this GPO, his changes had no effect and the entire domain was using an outdated security policy. The same scenario can appear in several other ways. For instance, someone might accidentally disable the default GPO or link the domain to another GPO and give it a higher priority. If you are a paranoid control freak like me, you'll delete these shortcuts and maintain policy from AD Users and Computers where you can see which GPOs are actually linked at each domain and OU, their priority, and other options.

As you can see, Group Policy is a powerful tool, but many pieces are involved and the group policy inheritance algorithm is complex. Are the policies you define really making it down to the actual systems you must protect? To know for sure, you must look behind the illusory curtain of simplicity that Microsoft has drawn across the largest OS in the world because good intentions don't count for much in security.

Chapter 4

Optimize GPO-Processing Performance

—by Darren Mar-Elia

If you've deployed Active Directory (AD), you know the benefits that it brings to your Windows environment. Among these benefits is the use of Group Policy Objects (GPOs)—powerful tools for managing your Windows 2000 servers and your Windows XP and Win2K workstations. As with any technology, however, too much of a good thing can hurt your systems' performance. You can link GPOs to multiple levels of your AD hierarchy, so a particular computer or user in your infrastructure might be subject to tens of GPOs at system startup or at logon. The result: long startup and logon times while your systems complete GPO processing.

To manage GPO processing and optimize your GPO infrastructure so that the impact on your systems and users is minimal, you need to understand how Win2K stores and applies GPO settings, how you can adjust those settings, and how to design an effective yet efficient Group Policy infrastructure.

GPO-Processing Basics

You link GPOs to container objects (i.e., sites, domains, or organizational units—OUs) within AD, and all user and computer objects under that container process those GPOs. This process can be complicated because user and computer objects must process any GPOs that you link to the domain, parent and child OU, and site in which the object resides. You can link one GPO to multiple container objects, or you can link multiple GPOs to one container object. The former situation has little effect on GPO-processing performance, but the latter situation makes all the difference in the world. The more GPOs that a given computer or user must process, the more time the computer needs to boot or the user needs to log on.

Win2K stores a GPO's settings in two places: the GPO's Group Policy Container (GPC) in AD, and the GPO's Group Policy Template (GPT) within the Sysvol share on your domain controllers (DCs). The process of creating a new GPO through the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in or the MMC Active Directory Sites and Services snap-in creates the GPC and GPT and links the GPO to the selected container object. When you use the MMC Group Policy snap-in to change a GPO, your actions modify both the GPC and the GPT.

Processing the settings in the GPC and GPT is the job of a set of DLLs called client-side extensions. Your XP and Win2K workstations' local registries reference these client-side extensions in separate subkeys under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GPExtensions subkey. The values in each globally unique identifier (GUID)-named subkey list the name of the DLL, the Group Policy processing category that the extension provides (e.g., Folder Redirection, Software Installation), and the settings that control the extension's behavior. These settings determine, for example, whether the extension will process a GPO when the computer connects to the DC over a slow network link, whether the extension will

refresh policy settings periodically, and whether the extension will process GPOs that haven't changed since the last processing time.

Client-side extensions are the primary worker bees of GPO processing. But certain network interactions must occur before a client-side extension can do its work. Network communications usually represent a significant portion of your servers' and workstations' total GPO-processing time. When a Win2K workstation boots in an AD domain that contains GPOs, the following processes take place:

1. The workstation queries a DNS server to locate a DC in the workstation's site. To be precise, the workstation queries DNS for the `_ldap._tcp.sitename._sites.dc._msdcs.domain-name` SRV record. This record returns the name of the DC (in the site sitename) that handles Lightweight Directory Access Protocol (LDAP) requests for the domain.
2. The workstation establishes a secure-channel connection with the DC.
3. The workstation pings the DC to determine whether the workstation's network connection to the DC (e.g., dial-up, T1) constitutes a slow network link. (By default, Win2K considers a transfer rate of less than 500Kbps to be slow. See the Microsoft article "How a Slow Link Is Detected for Processing User Profiles and Group Policy" at <http://support.microsoft.com/?kbid=227260> for information about how Win2K calculates slow links.)
4. The workstation binds to AD over LDAP.
5. The workstation uses LDAP to query AD and get a list of all the GPOs linked to the workstation's OU or parent OU.
6. The workstation uses LDAP to query AD and get a list of all the GPOs linked to the workstation's domain.
7. The workstation uses LDAP to query AD and get a list of all the GPOs linked to the workstation's site.
8. The workstation uses LDAP to query the GPC (in AD) and determine the path to each GPO's GPT (in Sysvol).
9. The workstation reads the `gpt.ini` file that resides in each GPO's GPT. This file lists the GPO's current version number.
10. The workstation's client-side extensions process the retrieved GPOs.

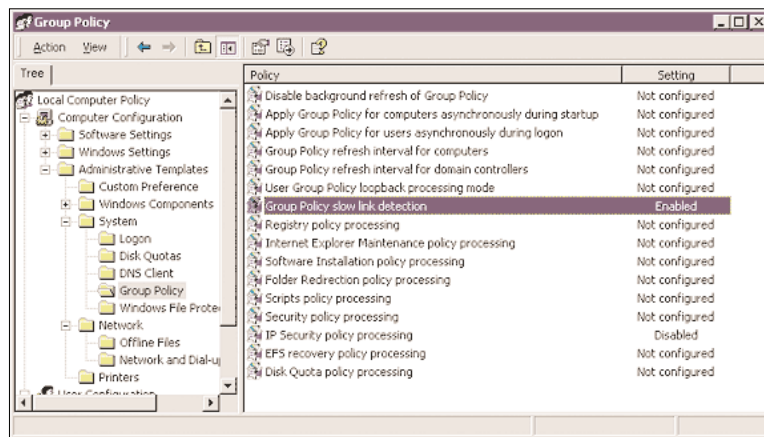
These steps represent the processing of only computer-specific GPOs, which occurs at computer boot. After a user logs on to the system, Win2K must process any user-specific GPOs. During that procedure, the OS repeats Steps 4 through 10 (from a network perspective, Steps 1 through 3 have occurred already).

Performance Boosters

Besides the sheer number of GPOs that a computer or user object must deal with, numerous steps within the GPO-processing operation can affect the amount of time that a computer needs to boot or that a user needs to log on and gain control of the desktop. The ability to promptly resolve the required DNS names and locate a DC in the workstation's site also is important to good GPO-processing performance. The more time these basic setup tasks take, the more time GPO processing consumes. And if your XP or Win2K devices can't resolve the correct SRV records, GPO processing might fail outright.

Even basic GPO processing can be time-consuming. However, several Group Policy settings and features can affect GPO-processing performance. As Figure 1 shows, you can access client-side extension and Group Policy options through the Group Policy snap-in. Open the Group Policy console, then drill down to Computer Configuration, Administrative Templates, System, Group Policy. Select a policy in the right-hand pane and open the policy's Properties dialog box to view or modify the policy's settings. In particular, the policies that control slow-link detection, processing despite GPO version, and synchronous or asynchronous processing can affect performance significantly.

Figure 1
Using the MMC Group Policy snap-in



Slow-Link Detection

By default, the client-side extensions that control Folder Redirection, Software Installation, Scripts, and Disk Quota won't process a GPO when the workstation detects a slow link. Enabling slow-link detection means that fewer client-side extensions will work to process GPOs, so GPO-processing time will lessen under slow-link conditions. You can modify the default slow-link value of 500Kbps through the *Group Policy slow link detection* policy. (However, increasing the threshold to force slow-link detection isn't the best strategy for improving GPO-processing performance.)

GPO Versioning

Each GPO's GPC and GPT contain the GPO's version number. Win2K increments this number each time you change the GPO. XP and Win2K workstations keep a history of each round of GPO processing in their local registries, under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History and HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\History subkeys. By default, client-side extensions won't process a GPO if its version number hasn't changed. When a GPO's version number is 0 (meaning that no settings have been made within the GPO), the client-side extensions won't even attempt to process the GPO.

Forcing the client-side extensions to process all GPOs regardless of version number will increase processing time. From the Group Policy folder, select a policy from the right-hand pane, open the policy's Properties dialog box, select the option to enable the policy, and be sure the *Process even if the Group Policy objects have not changed* check box is cleared.

Asynchronous Processing

By default, Win2K's GPO-processing operations are synchronous: All client-side extensions must finish processing any machine-based GPOs (at system boot) before the computer will present the logon dialog. Similarly, when a user logs on to a Win2K device, the client-side extensions that process user-level GPOs must complete their work before the user can get control of the desktop and start working. If the processing of many GPOs significantly delays system startup or user logon, you can configure Win2K to process GPOs asynchronously (through the *Apply Group Policy for computers asynchronously during startup* and the *Apply Group Policy for users asynchronously during logon* policies). However, a GPO that doesn't complete processing by the time a user logs on might not go into effect until the next time the user logs on—a lapse that could present a problem for Group Policy categories such as Software Installation and Folder Redirection. (XP includes a *Fast logon optimization* feature, so XP's GPO processing is asynchronous by default. Thus, the client-side extensions on an XP device might not finish processing all GPOs before a system presents the logon dialog box or lets a user access the desktop, and Software Installation and Folder Redirection typically require two logons before they take effect.)

Win2K also uses asynchronous processing for background refresh of Group Policy. Win2K periodically refreshes certain client-side extensions, such as those responsible for security settings and administrative templates, after the initial processing at boot or logon. For example, the client-side extension responsible for security settings on a Win2K server or workstation refreshes all applicable GPO settings every 90 minutes by default. On DCs, the default refresh interval is 5 minutes. This type of periodic processing limits the damage from users who muck with security settings between logons or reboots.

Not all client-side extensions support background refresh. For example, the Software Installation policy doesn't refresh (uninstalling Microsoft Word while someone is using it would be a bad idea). Also, client-side extensions won't refresh a GPO that hasn't changed. To prevent a GPO from refreshing, open a policy's Properties dialog box and select the *Do not apply during periodic background processing* check box. To change a device's overall background processing settings, enable and modify the *Disable background refresh of Group Policy*, *Group Policy refresh interval for computers*, or *Group Policy refresh interval for domain controllers* policy.

Although background processing doesn't have a big effect on your system's performance, you should be aware that it's happening. You can enable event logging for GPO processing so that you can monitor background processing and troubleshoot processing problems (see the sidebar "Group Policy Logging" for details).

Greater Control

Performance-enhancing behaviors such as slow-link detection, GPO versioning, and asynchronous-processing options are available in XP and Win2K. You can also explicitly tune a couple other settings to further reduce the overhead of GPO processing.

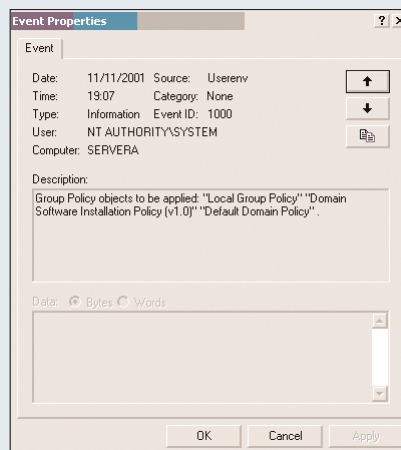
Group Policy Logging

Attempting to optimize Group Policy Object (GPO) processing can make you feel as though you're fumbling in the dark because by default, you have no easy way to monitor GPO processing as it occurs. However, Windows XP and Windows 2000 do provide some useful logging features that let you drill down into a system's processing cycle.

By default, client-side extensions log some high-level processing activity to the Application log. However, this activity rarely provides enough detail to be useful. You can enable additional logging through a registry change on each machine that you want to examine. Create a Diagnostics subkey under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion subkey, then add the RunDiagnosticLoggingGroupPolicy value (of type REG_DWORD) and assign it a value of 0x1. Restart the computer.

After this registry change takes effect, verbose GPO logging occurs within the Application log, as Figure A shows. You can follow the entire GPO-processing cycle within the event log and note which client-side extensions are running, which GPOs the system is processing, whether the system isn't processing a GPO because the GPO version hasn't changed, and the length of the processing cycle. Logging also comes in handy when you need to troubleshoot GPO-processing problems. The verbose logging shows when a particular client-side extension fails to run against a particular GPO, and in some cases, why the failure occurred. (Any verbose logging will fill up event logs over time and can generate a certain amount of system overhead. However, verbose GPO logging happens only during GPO-processing cycles, and I've yet to see it adversely affect system performance.)

Figure A
Viewing the Application log



Disable Unused Settings

Within each GPO, you can define settings that apply to computers or to users. However, you don't need to define both within a given GPO. Therefore, the first and easiest step to enhance performance is to disable a GPO's unused computer-level or user-level settings. Suppose that a workstation determines during boot that it needs to process four GPOs, only two of which have a defined computer-level policy. You can flag the other two GPOs as not having any computer-level policy. As a result, the workstation's client-side extensions won't bother to look for the nonexistent computer-level settings, and you'll save some time in the processing cycle.

To disable a GPO's computer- or user-level settings, open the Active Directory Users and Computers snap-in or the Active Directory Sites and Services snap-in, right-click the container to which the GPO is linked, then choose Properties from the context menu. Go to the Properties dialog box's Group Policy tab. Select the GPO and click Properties to open the GPO's Policy Properties dialog box. Use the check boxes in the Disable section to disable unused computer or user configuration settings. (You can select both check boxes, but doing so effectively disables the GPO.)

Set a Maximum Wait Time

Another way to keep GPO-processing times in check is to establish a maximum interval for running scripts. GPOs support computer startup and shutdown scripts as well as user logon and logoff scripts. Such scripts can be any form of executable, batch file, or Windows Script Host (WSH) script. Because you can apply multiple GPOs to a given user or computer, you might have multiple scripts running one after the other. But ill-functioning or poorly programmed scripts could hang or run forever. For example, when you use synchronous GPO processing, your XP and Win2K systems might hang for as many as 10 minutes, and you have no easy way to determine the problem.

To mitigate this type of problem, you can set a maximum time for all scripts to run. In a worst-case scenario, a script that is hung or caught in some kind of loop will run for only the specified time. Be aware, however, that the wait time applies to the total runtime of all scripts. For example, if you've defined logon scripts in each of 10 GPOs in your AD domain and you set the wait time to 60 seconds, all those scripts must be completely executed within 60 seconds. To specify a maximum script-processing interval, open the Group Policy snap-in, drill down to Computer Configuration, Administrative Templates, System, Logon (or Administrative Templates, System, Scripts in XP), and open the *Maximum wait time for Group Policy scripts* policy's Properties dialog box, which Figure 2 shows. You can enable the policy and configure the wait time on the Policy tab.

Design Matters

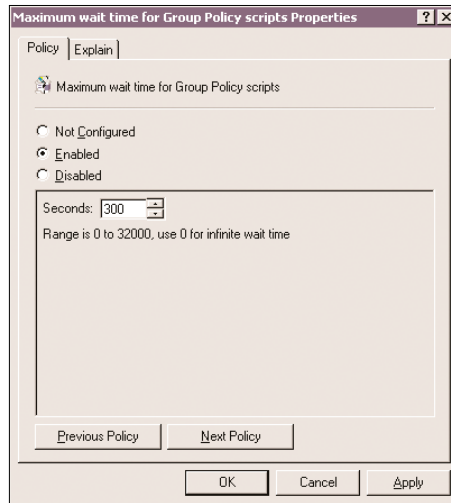
Aside from tweaking Group Policy behaviors, you can mitigate or prevent performance problems through a well-planned Group Policy infrastructure. Limiting the number of GPOs you create, the security groups you use, and the cross-domain GPO links you establish can speed up processing time.

Limit GPOs

The most basic step is to limit the number of GPOs that a computer or user must process at startup or logon. In general, I suggest limiting this number to 10 as a starting point, but you need to test this number for yourself because it depends heavily on what each GPO does. Also keep in

mind that wait times are longer the first time a computer or user processes a GPO because the client-side extensions must initially apply all the settings. After the initial processing cycle, subsequent system restarts or user logons will process only GPOs that have changed (unless you force them to do otherwise).

Figure 2
Specifying a maximum script-processing interval



Limit Security Groups

The use of security groups (i.e., AD local, global, or universal groups containing computers or users) can affect GPO processing. You can use security groups to filter GPOs' effects—for example, when you want to apply a domain-level GPO to only a handful of users or computers. However, security-group filtering comes with a performance cost. The more access control entries (ACEs) you associate with a GPO, the more work the GPO's client-side extension must do to figure out whether a computer or user belongs to one of the groups to which you've applied filtering. Thus, keeping your GPOs' ACLs short and concise further improves (or at least maintains) performance. Don't use ACLs indiscriminately to filter GPOs for every computer or user. Instead, rethink the level at which you're linking your GPOs. You might get the desired effect by relinking the GPO lower in your AD hierarchy (e.g., at the OU level rather than the domain level).

Limit Cross-Domain Links

Another design aspect that can play a role in performance is the use of GPOs that are linked across domain boundaries. Every GPO belongs to one AD domain, and the GPO's GPC and GPT reside on that domain's DCs. Suppose you have a multidomain AD forest. You could link a GPO in one domain (Domain A) to another domain in the forest (Domain B). But when a computer or user in Domain B processes the GPO that resides in Domain A, the client-side extensions on the Domain B computer must traverse trust relationships within the forest to access the GPO's GPC

and GPT. Such an operation is more expensive from a performance perspective than communicating with GPOs within the same domain. Furthermore, if the Domain B computer can't find a Domain A DC within the same AD site, the computer might need to traverse WAN links to reach a DC and process the GPO.

The best solution is to avoid linking GPOs across domain boundaries. Instead, copy a defined GPO from one domain to another. (XP and Win2K don't provide an easy way to copy GPOs from one domain to another, but third-party tools can provide such functionality.)

GPOs: Complex but Powerful

GPOs can be powerful tools in your Windows systems-management arsenal, but GPO configuration and behaviors are complex and can slow down system startups and user logons. Armed with the knowledge of how to modify GPO behavior and infrastructure to improve GPO-processing time, however, you can minimize GPO performance penalties—and get the most out of your AD infrastructure.

Chapter 5

Group Policy for Mobile Users

—by Emmett Dulaney

One of the most far-reaching, new administrative features that Windows 2000 offers is Group Policy. As part of IntelliMirror, Group Policy lets administrators control desktop settings, use scripts, perform Internet Explorer (IE) maintenance, roll out software, redirect folders, and more. All of these features can be an administrator's dream in supporting LAN users.

Group Policy places restrictions on what a user or computer can do by removing liberties; as such, Group Policy is a tool that simplifies the administrator's job and is not for the benefit of the user (restrictions do not equal benefits). So, for example, on standalone Win2K Professional workstations, Group Policy lets you prevent users from deleting programs, sending huge files to a slow printer, and deleting the system registry.

By limiting what users can do, you also limit the features and equipment that you must support, thereby reducing the overall administrative cost of supporting the network, computers, and users. So, if you take away the user's ability to add new software, you don't have to worry about supporting untested applications. Likewise, if you remove the ability to delete installed printers, you don't have to waste time reinstalling printers.

But what if your workforce is mobile? How do you enforce restrictions on users who don't have a direct connection to your LAN? With a few local policies, some security templates, and the occasional use of Group Policy, you can place restrictions on your mobile workforce.

Roaming Users Versus Mobile Users

Before we go any further, it is important to differentiate between roaming users and mobile users. As the name implies, roaming users roam the network and use different computers within the same LAN. Mobile users use the same workstation but don't have a direct connection to the LAN. Because you can't force mobile users to connect to a server on your LAN each time they boot, you are less able to enforce administrative restrictions such as Group Policies. However, you can apply administrative restrictions on mobile users using other means, depending on the type of client you're dealing with.

Legacy Clients

If a mobile computer runs Windows NT or Windows 9x, you can use System Policies to apply registry restrictions to that system and hide the policies locally. System Policies, which are the predecessors of Group Policies, restrict only registry settings, whereas Group Policies exceed that functionality by going far beyond registry settings alone.

Windows 2000 Clients

Even if you can't use Group Policies on Win2K clients without a direct connection, you can still place many settings directly on the mobile computer and make these settings local policies. Local policies can apply to several areas, including Policy, encryption, and so forth.

Creating the Local Policy

Before you can implement a local policy for a mobile client, you need to create the policy using Group Policy Editor (GPE). To start GPE, either click Run from the Start menu and enter

```
gpedit.msc
```

or click Run from the Start menu and enter

```
MMC
```

to open the Microsoft Management Console (MMC). If you choose the MMC option, go to the Console menu, select Open, and select gpedit.msc from the System32 directory.

When opened, a local policy has two primary divisions: Computer Configuration and User Configuration. The settings that you configure for Computer Configuration apply to the computer, regardless of who is using it. Conversely, the settings that you configure for User Configuration apply only if the specified user is logged on. Both primary divisions can be useful with a mobile workforce. Note that the OS applies the Computer Configuration settings whenever the computer is on, whereas it applies the User Configuration settings only when the user logs on.

Password Policies

Because the likelihood of laptops being stolen is always a possibility, you will want to make use of good password policies for your mobile users. You can access password settings in gpedit.msc at the following path: Computer Configuration - Windows Settings - Security Settings - Account Policies - Password Policy. An example password policy is as follows:

Enforce password history:	8 passwords remembered
Maximum password age:	42 days
Minimum password age:	3 days
Minimum password length:	6 to 8 characters

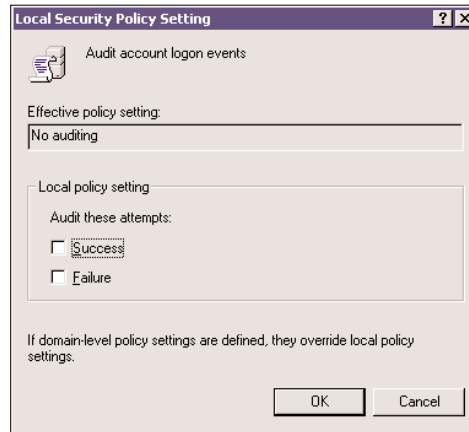
Leave the other three settings (minimum password length, passwords must meet complexity requirements, and store passwords using reverse encryption for all users in the domain) disabled.

When you work with a mobile workforce, you must weigh the choice of having users call you in the middle of the night when they forget their password against the security of those users' systems if their laptops fall into the wrong hands. A good rule of thumb is to lock out the user after five attempts for a period of between 30 and 60 minutes.

Local Policies

Gpedit.msc contains a Local Policies section at Computer Configuration – Windows Settings – Security Settings that consists of three subsections: Audit Policy, User Rights Assignment, and Security Options. The Audit Policy subsection contains nine settings, the default value for each being “No auditing.” Valid options are Success and/or Failure, as Figure 1 shows, for *Audit account logon events*. However, you will want to consider turning on this auditing for mobile users to see how often they log on and log off their machines. For all these settings, when you turn on auditing for an event, Win2K logs the entries in the Security log file.

Figure 1
Configuring the Audit account logon events setting



Applying Security Templates

Rather than editing the local policy on each machine, you can use the Security Templates snap-in to create a sample file that you can readily apply on any machine. The Security Templates snap-in includes several default templates that you can use to create the baseline.

To reach the Security Templates snap-in, start the MMC, go to the Console menu, and select Add/Remove Snap-in. Next, click Add, select Security Templates, and click OK twice to return to the snap-in within the MMC. Figure 2 shows the Security Templates snap-in and the default templates.

Of particular interest for a mobile workforce is the secure workstation template (securews). Table 1 shows the default settings that this template applies.

Occasional Use of Group Policy

You can configure Group Policies that will apply to Win2K Pro clients when your mobile users do connect directly to the network (such as a mobile laptop user sitting in the office with the machine in the docking station), yet not force updates on clients connecting over slow links. If you try to force the policy in the field, it can take considerable time and even prevent users from performing simple tasks (e.g., dialing in to upload an order).

Figure 2
Viewing the Security Templates snap-in and the default templates

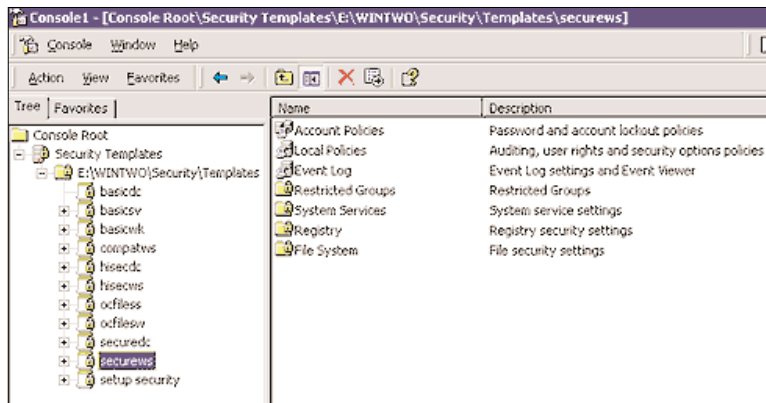


Table 1
Secure Workstation Template Settings

Category	Policy	Default Setting
Account Policies - Password Policy	Enforce password history	Remember 24 passwords
	Maximum password age	42 days
	Minimum password age	2 days
	Minimum password length	8 characters
	Passwords must meet complexity requirements	Enabled
	Store password using reversible encryption for all users in the domain	Disabled
Account Policies - Account Lockout Policy	Account lockout duration	30 minutes
	Account lockout threshold	5 invalid logon attempts
	Reset account lockout counter after	30 minutes
Local Policies - Audit Policy	Audit account logon events	Success, Failure
	Audit account management	Success, Failure
	Audit logon events	Failure
	Audit policy change	Success, Failure
	Audit privilege use	Failure
Local Policies - Security Options	Amount of idle time before disconnection session	15 minutes
	Unsigned driver installation behavior	Warn but allow installation

The Group Policy slow link detection setting, as Figure 3 shows, is located beneath Computer Configuration. To access this setting, go to Administrative Templates, choose System, and choose Group Policy. The slow link detection setting applies to security settings, administrative templates, software installation and maintenance, scripts, folder redirection, and IE maintenance. The default definition of a slow link is 500Kbps; however, you can change it to any value you desire.

In situations where you are applying both local policies and Group Policies (such as when the computer is in the office connecting to the docking station), Win2K applies the local policies first. Because the OS applies any Group Policies second, the Group Policy settings can easily override, compliment, or simply not affect those within the local policies.

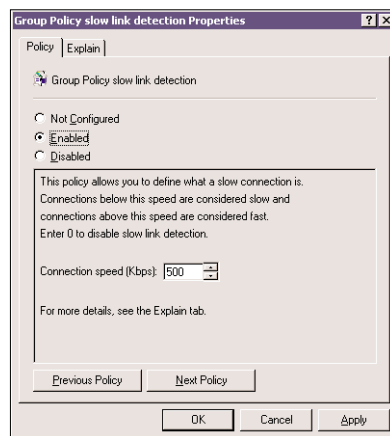
For example, a local policy can't contain folder redirection, but a Group Policy can. In the field, folder redirection won't be in place, but it will be present in the office. Not only do Group Policies run after the local policies, but multiple Group Policies can run—each changing or adding to the restrictions and settings. After local policies, the order of execution is as follows:

- A site Group Policy, if applicable
- A domain Group Policy, if applicable
- Organizational unit (OU) policies, if applicable

(Microsoft refers to this order of execution as sites, domains, and organization units—SDOU.)

Be aware that in the absence of a direct connection to the LAN (and, therefore, to Active Directory—AD), there are several Group Policy restrictions that you can't enforce. These restrictions include assigning and publishing software, folder redirection, remote installation, and roaming profiles.

Figure 3
Viewing the Group Policy slow link detection setting



Other Considerations for Mobile Users

In addition to using Win2K's Group Policy feature, you will want to consider several other factors for the mobile workforce. The first and foremost of these is security. Every mobile computer should be running NTFS to take advantage of its file- and folder-level security features. Additionally, you should protect the data with Encrypting File System (EFS) to keep it from prying eyes (e.g., if a laptop is stolen). You should also create usernames that are not easy to guess and encourage users to make use of good password practices.

Chapter 6

IPSec and Group Policy

—by Randy Franklin Smith

A Stronger Defense

As you make your network more porous to support connections to your business partners and customers, you must shore up defenses around the crucial resources on your internal network. Sometimes you can implement internal firewalls to separate your network into zones and accomplish this goal. But what if the traffic or computers that you need to protect don't correspond to convenient physical LAN segments? In such cases, you can take a cue from the Internet and apply the VPN concept to your internal network, using IP Security (IPSec) and Group Policy to shield your mission-critical Windows 2000 servers from attackers who manage to penetrate your perimeter defenses.

The IPSec Advantage

You can use IPSec to secure all IP traffic on your network. The protocol provides authentication, integrity checking, and optional encryption at the packet level—and does so in a way that's transparent to your applications. IPSec authentication is stronger than source-IP address filtering, which is subject to spoofing and is difficult to maintain.

IPSec uses Kerberos, preshared keys, or certificates for its initial authentication. You can assign (i.e., activate) only one IPSec policy at a time on a Win2K computer, but that policy can contain multiple IPSec rules so that the computer treats different kinds of traffic in different ways. An IPSec rule specifies a filter list, action, and authentication method. The filter list catches appropriate packets (according to source IP address, destination IP address, and ports), then subjects those packets to a specified action—Permit, Block, or Negotiate security. The Permit action causes the system to process the packet traffic as if you hadn't implemented IPSec. Block causes the system to drop packets. Negotiate security causes the system to secure traffic using the Authentication Header (AH) or Encapsulating Security Payload (ESP) mode, depending on how you've configured the action. If the system receives a packet that isn't secured by AH or ESP, it sends a message to the originating computer, inviting it to retry the exchange by using IPSec. If the originating computer doesn't respond (because it isn't enabled for or doesn't support IPSec), the receiving computer either acquiesces and drops back to unsecure traffic or rejects communications (depending on the action's configuration). AH mode guarantees both computers that the traffic is authentic, meaning that the computer that claims to have transmitted the traffic truly did so. AH mode also uses integrity checking to make sure the packet wasn't modified in transit. AH is sufficient when you don't care about confidentiality but simply want to limit which computers can communicate with a system and make sure that traffic hasn't been modified in transit. ESP, which is a superset of AH, provides encryption in addition to authentication and integrity checking so that only the receiving system can read the data in the packet.

When you receive an IPSec-secured packet, you know that it came from an authorized computer and hasn't been forged or modified in transit. An IPSec-configured computer that drops unauthenticated packets before they reach your applications can foil attackers: Intruders can't attack an application if they can't communicate with it. With some creative thinking, you can find ways to use IPSec and Group Policy to specify which computers in your domain can communicate with one another, thereby adding security and preventing attacks on mission-critical applications such as SAP, Oracle, PeopleSoft, Microsoft Exchange Server, and Microsoft SQL Server.

A Fine Example

Suppose you want to protect an important Win2K system that runs SQL Server. You want to implement security above and beyond what conventional Win2K and SQL Server options can provide. Out of a network of 5000 user workstations, only 100 workstations need to communicate with the SQL Server system, over port 1433. However, these 100 computers are scattered throughout your network, so restricting traffic to the server according to source IP address is impractical (not to mention unsecure). However, you can use IPSec authentication to limit, in two steps, the computers that can communicate with the SQL Server machine through port 1433.

First, you need to create an IPSec policy on the SQL Server machine to require ESP mode for any traffic on the port. (In this example, I suggest that you use ESP mode to encrypt confidential data traveling between the clients and server.) Then, you need to enable IPSec on the 100 authorized client computers.

Configuring the Server

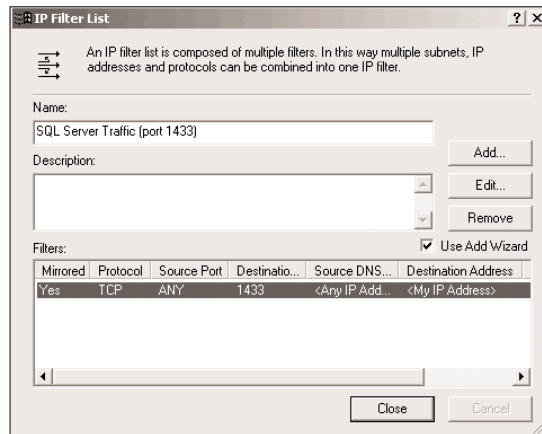
Open the Microsoft Management Console (MMC) Local Security Policy snap-in on the SQL Server system, and select *IP Security Policies on Local Machine* in the left-hand pane. Right-click a blank area in the right-hand (aka details) pane, then select Create IP Security Policy from the context menu to launch the IP Security Policy Wizard. Click Next, enter a name such as Secure SQL Server, then click Next again. Clear the *Activate the default response rule* check box, click Next, then click Finish. (The default response rule causes Win2K to acquiesce to any IPSec request from computers that the system contacts. You want to stay in control of IPSec negotiation in this example, so you need to deactivate the rule.)

The Secure SQL Server Properties dialog box opens automatically. On the Rules tab, click Add to launch the Security Rule Wizard. Click Next until you reach the Authentication Method screen. Keep in mind that you're configuring computer-to-computer authentication, not user authentication. When all the computers involved are part of an Active Directory (AD) forest, Kerberos is the easiest authentication method to use because each computer already has a Kerberos-enabled AD computer account. Kerberos isn't as secure as the other options (i.e., certificates and preshared keys), but it's much less work. Therefore, let's start by examining how to use Kerberos authentication. Select the *Windows 2000 default (Kerberos V5 protocol)* option.

Click Next to advance to the wizard's IP Filter List screen. A filter list contains one or more filters that you configure to catch specific types of traffic and to handle that traffic according to actions that you specify. Click Add to open the IP Filter List dialog box. In the Name box, enter *SQL Server Traffic (port 1433)*, then click Add to launch the IP Filter Wizard. Click Next, then select Any IP Address from the *Source address* drop-down list. Click Next, then select My IP Address from the *Destination address* drop-down list. Click Next, select TCP from the *Select a pro-*

to col type drop-down list, then click Next again. Select the *To this port* option and enter 1433 in the text box. Click Next, clear the *Edit properties* check box, then click Finish to return to the IP Filter List dialog box, which will now look like the dialog box that Figure 1 shows. Click Close. On the Security Rule Wizard's IP Filter List screen, select *SQL Server Traffic (port 1433)*, then click Next to advance to the Filter Action screen.

Figure 1
Configuring the IP Filter List



You're now ready to select an action. The prebuilt filter actions won't suffice because none of them make ESP mandatory; therefore, you need to create a custom action. On the Security Rules Wizard's Filter Action screen, click Add to launch the Filter Action Wizard. Click Next. Enter a name such as Require ESP Mode, then click Next. On the Filter Action General Options screen, select the *Negotiate security* option, then click next. Select *Do not communicate with computers that do not support IPSec*, then click Next. On the IP Traffic Security screen, select the High (Encapsulated Security Payload) option, click Next, then click Finish to return to the Security Rule Wizard's Filter Action screen. Select Require ESP Mode, click Next, then click Finish. On the Secure SQL Server Properties dialog box, clear the selected *SQL Server Traffic (port 1433)* check box, then click Close.

You've created the Secure SQL Server policy, but don't assign it yet. Doing so would immediately prevent clients from communicating with the server because you haven't yet configured the clients for IPSec.

Configuring the Clients

To configure the 100 client computers, you need to create a group, add the client computers to the group, create a Group Policy Object (GPO) in AD, and modify the GPO's ACL to give the *Read* and *Apply Group Policy* permissions only to members of the new group. After you configure the GPO and enable IPSec for the GPO, and after the client computers apply the GPO, they'll be able to communicate with the SQL Server system. (Other systems will be shut out after you activate the policy on the SQL Server machine.)

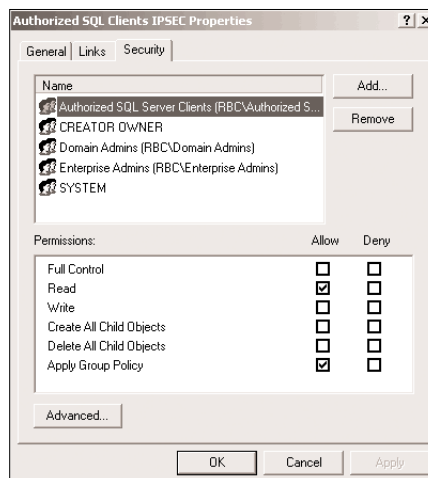
Open the MMC Active Directory Users and Computers snap-in, and select the domain root or organizational unit (OU) in which you want to create the group. Select Action, New, Group from the menu bar. Enter Authorized SQL Server Clients in the *Group name* text box, click Next, then click Finish. Open the new group's Properties dialog box, and go to the Members tab. Add the 100 client computers to the group as members, then click OK.

Now you're ready to create the GPO. Open the domain's Properties dialog box and go to the Group Policy tab. Click New to create a new GPO in the Group Policy Object Links list. Name the GPO Authorized SQL Clients IPSEC.

Typically, when you link a GPO to a domain root, Win2K applies that GPO to all the computers and users in the domain. However, you want the IPsec policy in this new GPO to apply only to the 100 or so computers that are authorized SQL Server clients. You could create a new OU to hold those computers, then link the GPO to the OU—thus limiting application of the GPO. But the SQL Server client computers are already scattered throughout existing OUs. Other GPOs link to these OUs and supply other important policies for the computers. Therefore, you need another way to limit the new GPO to the appropriate computers. The solution is to modify the GPO's ACL.

Open the GPO's Properties dialog box and go to the Security tab. This tab displays the GPO's ACL, which controls who can edit the GPO and provides a way to limit the computers or users to which the GPO applies. Notice that the default ACL grants the *Read* and *Apply Group Policy* permissions to the Authenticated Users group. Select that group, then click Remove. Click Add, select the Authorized SQL Server Clients group, click Add again, then click OK. Select the group, then select the *Read* and *Apply Group Policy* permissions, as Figure 2 shows. Click OK to close the Authorized SQL Clients IPSEC Properties dialog box. Now, the GPO will apply only to computers that are members of the Authorized SQL Server Clients group even though you've linked this GPO to the domain root.

Figure 2
Selecting the Read and Apply Group Policy permissions



You now need to configure an IPSec policy for the GPO. On the Group Policy tab of the domain's Properties dialog box, select Authorized SQL Clients IPSEC, then click Edit. Select Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory. Right-click Client (Respond Only) in the details pane, then select Assign from the context menu. This prebuilt policy causes a Win2K computer to acquiesce when it tries to communicate with another computer that requests IPSec negotiation. Wait at least 2 hours for all the clients to update Group Policy. (By default, Win2K computers reapply Group Policy every 90 minutes, with a random offset of up to 30 minutes.)

You can now activate the Secure SQL Server policy on your SQL Server system. To do so, open the Local Security Policy snap-in on the SQL Server system, right-click the policy (under IPSec Policies on Local Machine), then select Assign from the context menu. Now, only authorized computers can connect to port 1433 on your SQL Server system, and IPSec will encrypt traffic on that port as it traverses the network.

Authentication Alternatives

As I mentioned earlier, for our sample scenario (in which we're limiting the computers within a forest that can communicate with one another) Kerberos authorization is often the simplest—but not the strongest—option. When you use Kerberos, anyone with Administrator access to a computer in the forest need only assign the Client (Respond Only) policy on that computer to attack the SQL Server system through port 1433. In such a scenario, preshared key authentication is a better alternative than Kerberos. To use preshared key authentication, you need to configure both the server and client IPSec policies with a secret key.

Open the Local Security Policy snap-in on the SQL Server system. Right-click the Secure SQL Server policy (under the IP Security Policies on Local Machine object), then select Unassign so that you won't interrupt communications with clients.

Open the policy's Properties dialog box. On the Rules tab, select the *SQL Server Traffic (port 1433)* rule from the IP Security Rules list, then click Edit to open the Edit Rule Properties dialog box. Go to the Authentication Methods tab and remove the Kerberos entry. Click Add. On the New Authentication Method Properties dialog box, select the *Use this string to protect the key exchange (preshared key)* option and enter a string of numbers, symbols, and letters at least 20 characters long. Make a note of this string, then click OK three times to close all the dialog boxes.

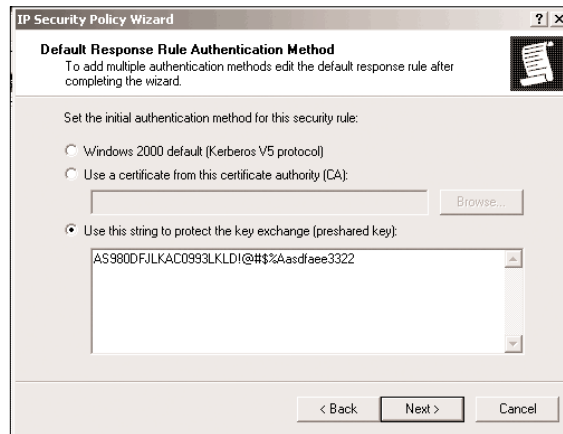
Next, open the Active Directory Users and Computers snap-in and open the domain's Properties dialog box. Go to the Group Policy tab, select Authorized SQL Clients IPSEC, then click Edit. Select the Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory object. The Client (Respond Only) policy is assigned. The simplest way to change this assignment is to edit the policy and add a new authentication method. However, I don't recommend this approach because GPOs share IPSec policies. If you use a given IPSec policy, such as Client (Respond Only), in more than one GPO and you change the policy, those changes will take effect in all the GPOs to which you've assigned the policy. Instead, right-click a blank area in the details pane and select Create IP Security Policy from the context menu to launch the IP Security Policy Wizard. Click Next, name the new policy Authorized SQL Clients, then click Next. Select the *Activate the default response rule* check box, then click Next. Select *Use this string to protect the key exchange (preshared key)*, then enter the same key you entered for the Secure SQL Server policy, as Figure 3 shows. Click Next, then click Finish. Click OK to close the Properties dialog

box. Right-click the new policy, then select Assign from the context menu; this action also unassigns the Client (Respond Only) policy.

Wait at least 2 hours for all the clients to reapply Group Policy. After 2 hours, you can reassign the policy on the SQL Server system. At that point, no computer will be able to connect to your SQL Server system unless that computer is a member of the Authorized SQL Server Clients group.

Figure 3

Entering the same key you entered for the Secure SQL Server policy



The Next Step

Preshared key authentication also has some weaknesses. Preshared keys are stored in clear text in the registry and are therefore subject to compromise. Also, you've protected only port 1433. What about other ports that an attacker could target, such as those associated with the Server service or Windows Terminal Services? For this sample scenario, the strongest authentication option—albeit the most complicated—is certificates. In the following section, I show you how to set up a Certificate Authority (CA) and configure IPSec to use it to lock down access to our sample SQL Server service. I also shed more light on sequencing changes to IPSec to make sure you don't temporarily interrupt communications while Win2K applies Group Policy throughout your domain.

In addition, you need to examine your network and consider other ways in which you can use IPSec to erect defenses behind your firewall. After all, to secure an office building, you don't just lock the front door, you also lock the offices that contain crucial equipment to protect against malicious insiders as well as outsiders who make it past your front door. Likewise, don't give up your whole network just because someone makes it through your firewall—use IPSec to limit communication with your mission-critical servers.

Setting Up a Dedicated Enterprise CA

First, you need to install Win2K Certificate Services and create and configure an Enterprise CA. (An Enterprise CA integrates with AD and has several advantages, the most important in our sample

scenario being that you can automate certificate requests and approvals for member computers in the domain. With standalone CAs, you must manually request and approve a certificate for each computer in the domain.) When you use IPsec certificate-based authentication, you limit authentication to certificates from a specific CA. Therefore, you need to use a dedicated Enterprise CA for each IPsec policy you plan to configure. In our sample scenario, you'll create a special-purpose CA to issue IPsec certificates only to the 100 computers that need to communicate with the SQL Server machine; little CA activity will occur after the initial enrollment of the authorized clients. You can use an existing Enterprise CA, so long as you don't need to issue IPsec certificates from that CA for other reasons. If you don't have an existing CA that you can use for this purpose, install Certificate Services on any Win2K server—other than the SQL Server machine—that's a member of your AD domain.

Open the Control Panel Add/Remove Programs applet. Click Add/Remove Windows Components in the applet's left-hand taskbar, then select Certificate Services. This action displays a warning that you can't rename the computer or change domains after installing Certificate Services. Click Yes to launch the Windows Components Wizard. Click Next. The wizard asks you to select the type of CA; select *Enterprise root CA* and click Next. Enter the appropriate identification information for the CA (we'll use *SqlIPSecCA* as a sample name) and your organization, then click Next.

If you already have an Enterprise root CA, consider making *SqlIPSecCA* a subordinate CA. In larger public key infrastructure (PKI) implementations, best practice is to build one root CA, which issues certificates only to subordinate CAs rather than to users or computers. This root CA has strong physical security and stays powered down and disconnected from the network except when needed to issue a new CA certificate. The purpose of this root CA is to help you recover if a subordinate CA's private key is compromised. You can use the root CA to revoke the subordinate CA's certificate and publish the certificate in the certificate revocation list (CRL) in AD, thus preventing anyone from trusting certificates issued by the compromised subordinate CA. Without a root CA, you'd need to update all computers manually to stop them from trusting certificates that the compromised subordinate CA signed.

Accept the default paths for *SqlIPSecCA*'s database, click Next, then click Finish. You now have a CA that all the domain computers trust automatically.

At this point, however, any authenticated user can request certificates from *SqlIPSecCA*. You need to limit this ability to the SQL Server system and the Authorized SQL Server Clients group, which contains the 100 authorized computers. Open the MMC Certification Authority snap-in, and open *SqlIPSecCA*'s Properties dialog box. Go to the Security tab. Select the Authenticated Users group, then clear the Allow check box for the Enroll permission. Add the Authorized SQL Server Clients group and the SQL Server system's computer account, then select the Enroll permission's Allow check box for both (this action automatically selects the Allow check box for the Read permission as well).

Next, you need to configure *SqlIPSecCA* to enable it to issue certificates according to the IPSEC certificate template and prevent it from issuing certificates according to other certificate templates. (To learn more about certificate templates and automatic certificate requests, see the sidebar "Certificate Templates.") Open the Certification Authority snap-in on the CA system, and select the Policy Settings folder to view a list of the certificate templates that *SqlIPSecCA* can issue. Right-click any empty space in the right-hand (aka details) pane, then select New, *Certificate to Issue* from the

context menu. In the Select Certificate Template dialog box, select IPSEC and click OK to add the IPSEC certificate template to the Policy Settings folder. SqlIPSecCA needs to issue only IPSEC certificates, so delete the other certificate types from the folder. The CA will now issue certificates based on only the IPSEC certificate template.

Certificate Templates

Certificate templates let you specify the types of certificates that users or computers can request from your Certificate Authority (CA). A certificate template limits the purposes (e.g., email, smart card logon, Windows 2000 Encrypting File System—EFS—IP Security—IPSec) for which you can use certificates that you base on that template. You can also edit a template's ACL to restrict the users or computers who can request certificates based on the template. Because the users, computers, and CA are all part of a Win2K Active Directory (AD) forest, the CA can rely on Kerberos to identify and authenticate the users or computers who make certificate requests, thereby enforcing the certificate template's ACL.

You can use Group Policy to configure authorized computers to automatically request a certificate from the CA according to the IPSEC certificate template. That way, only those computers can obtain a certificate from the CA and use that certificate to authenticate and communicate with a specified server through IPSec.

The IPSEC certificate template's default ACL, however, limits enrollment to the Administrators group, a restriction you need to change. Win2K doesn't store certificate templates on each CA, but rather maintains one set of certificate templates in AD, at the domain level. All Enterprise CAs in the domain share this set of templates. To access the IPSEC certificate template's ACL, open the MMC Active Directory Sites and Services snap-in. Select View, Show Services from the menu bar. Select the Services\Public Key Services\Certificate Templates folder in the left-hand pane. Select the IPSECIntermediateOnline object in the details pane, and open the object's Properties dialog box. Go to the Security tab. Add the Authorized SQL Server Clients group, select the group, then select the Allow check box for the Enroll permission, as Figure 4 shows.

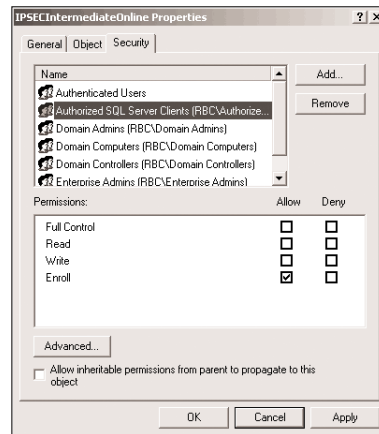
SqlIPSecCA is ready to issue IPSec certificates to any authorized SQL Server client and to the SQL Server system. Now you need to configure these authorized computers to request certificates.

Configuring Automatic Certificate Requests

First, you'll configure the authorized client computers to request certificates automatically. To do so, you need to edit the Authorized SQL Clients IPSEC GPO, which I explained previously. (I also explained how to link this GPO to the domain root and how to limit the Apply Group Policy permission to only the Authorized SQL Server Clients group so that Win2K will apply the GPO to only the computers in that group regardless of their location in the domain.) Open the MMC Active Directory Users and Computers snap-in. Select the domain root object and open its Properties dialog box. Go to the Group Policy tab, select the Authorized SQL Clients IPSEC GPO, then click Edit to open an MMC Group Policy console specific to the GPO. In the Group Policy console, select the Computer Configuration\Windows Settings\Security Settings\Public Key Policies\

Automatic Certificate Request Settings folder, then right-click any empty space in the details pane. Select New, Automatic Certificate Request from the context menu to start the Automatic Certificate Request Setup Wizard, then click Next. Select IPSEC for the certificate template, then click Next. Select SqlIPSecCA from the list of available CAs, click Next, then click Finish. Reboot the computers that are members of the Authorized SQL Server Clients group. (See the sidebar “Group Policy Application” for an explanation of Win2K’s method of applying these changes.)

Figure 4
Selecting the Allow check box for the Enroll permission



Group Policy Application

By default, Windows 2000 computers reapply Group Policy every 90 minutes, plus a random offset of 30 minutes; so, within a few hours, all the authorized SQL clients should request an IPsec certificate from SqlIPSecCA. However, keep in mind that when checking access to objects, Win2K uses access tokens to determine group membership. An access token contains the user or computer account’s SID and the SIDs of all the groups to which the account belongs. Win2K builds an access token when an account logs on, then doesn’t update the token. Therefore, group membership changes that occur while a user is logged on don’t take effect until the user logs off and logs back on. Group membership changes that affect a computer account don’t take effect until the next time the computer reboots (the computer logs on to the domain when it first boots and remains logged on until it’s shut down). Because many of the settings I specify in Chapter 6 depend on membership in the Authorized SQL Server Clients group, make sure those computers are rebooted after you edit the Group Policy Object (GPO), to ensure that the changes take place on a timely basis.

To verify that a computer has successfully requested an IPsec certificate from SqlIPsecCA, log on to the computer as an Administrator and open a blank MMC console. Select Console, Add/Remove Snap-in from the menu bar. In the Add/Remove Snap-in dialog box, click Add to open the Add Standalone Snap-in dialog box. In that dialog box, select Certificates and click Add to open the *Certificates snap-in* dialog box. In that dialog box, select *Computer account*, then click Next. In the Select Computer dialog box, select the *Local Computer: (the computer this console is running on)* option, then click Finish. Click Close in the Standalone Snap-in dialog box, then click OK in the Add/Remove Snap-in dialog box. In the MMC console's left-hand pane, select Certificates (Local Computer)\Personal\Certificates. You should see a certificate, which SqlIPsecCA issued and with an intended purpose of 1.3.6.1.5.5.8.2.2, which corresponds to IPsec. (Save the new MMC console, which you'll need to use again in a few minutes.)

If the computer hasn't obtained a certificate, force a Group Policy refresh. At the computer, run the command

```
secedit /refreshpolicy machine_policy
```

Wait a minute, reopen the console, right-click the Certificates (Local Computer)\Personal\Certificates folder, and select Refresh. If you still don't see the certificate, check the Application log for events with a source of SceCli; analyze those events to determine why the automatic certificate request is failing.

Next, you need to manually request a certificate for the SQL Server system (which isn't part of the Authorized SQL Server Clients group and therefore hasn't requested a certificate automatically). Log in to the SQL Server machine as an Administrator, open a blank MMC console, and go through the process I just described to add the Certificates snap-in. In the MMC console's left-hand pane, right-click the Certificates (Local Computer)\Personal\Certificates object, then select All Tasks, Request New Certificate from the context menu to start the Certificate Request Wizard. Click Next, select IPSEC as the certificate template, then click Next again. Enter IPSEC Certificate as the friendly name, click Next, then click Finish. You'll see a message that tells you the *Certificate request was successful*, and a new certificate will appear in the console.

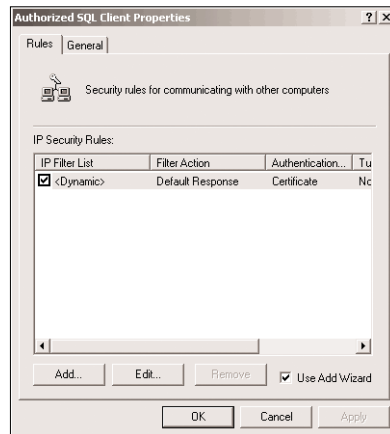
Editing the IPsec Policy

Now it's time to edit your IPsec policy. On the clients, you need to add an authentication method that permits authentication through a certificate that SqlIPsecCA issues. On the SQL Server system, you need to require authentication through a certificate that SqlIPsecCA issues. To prevent interrupted communications, you need to temporarily enable both the preshared key and certificate authentication methods on the clients and the server. (You can use multiple authentication methods in IPsec policies; Win2K tries each method in the specified order.)

First, configure the clients. Open the Active Directory Users and Computers snap-in, go to the Group Policy tab of the domain root's Properties dialog box, select the Authorized SQL Clients IPSEC GPO, then click Edit. In the Group Policy console, select the Computer Configuration\Windows Settings\Security Settings\IP Security Policies on Active Directory object. In the details pane, select the Authorized SQL Clients policy (I explained how to create and assign this policy earlier) and open the policy's Properties dialog box, which Figure 5 shows. Select the rule in the IP Security Rules window (you'll see only one rule), then click Edit to open the Edit Rule Properties

dialog box. Go to the Authentication Methods tab. If you followed the earlier instructions, the pre-shared key authentication method will be listed on this tab. Click Add, select *Use a certificate from this certificate authority (CA)*, then click Browse. Win2K warns you that *The Active Directory does not contain a shared certificate store* and asks *Do you want to select a certificate authority from the local machine certificate store?* Click Yes, select SqlIPSecCA's certificate in the Select Certificate dialog box, then click OK. Click OK to close the New Authentication Method Properties dialog box. Click OK to close the Edit Rule Properties dialog box, then click OK to close the Authorized SQL Clients Properties dialog box. In the Group Policy console's details pane, right-click the Authorized SQL Clients policy and select Un-assign. Right-click the policy again and select Assign. These final steps are important because Win2K won't reapply the edited policy to the GPO until you reassign the policy.

Figure 5
Viewing the policy's Properties dialog box



Next, configure your SQL Server machine's IPSec policy to require certificate authentication. Open the MMC Local Security Policy snap-in on your SQL Server machine, and select the IP Security Policies on Local Machine object. Open the Secure SQL Server policy's Properties dialog box, and add certificate-based authentication to the policy in the same way you added it to the Authorized SQL Clients policy. Close the policy's Properties dialog box, then unassign and reassign the policy. To force the SQL Server system to refresh Group Policy, run the command

```
secedit /refreshpolicy machine_policy
```

(Note that this command is valid on Win2K servers. If you're running Windows XP, simply run the Gpupdate command, with no parameters.) After all the SQL Server clients have applied Group Policy (which should be within 2 hours but could be delayed if some of the client computers aren't connected to the network or are down), you can reedit the GPO's and SQL Server system's policies to remove the pre-shared key authentication method.

Maintaining Security

Now that you've configured your SQL Server system to require certificate-based authentication, you've locked down access to the machine so that only the 100 authorized client computers can communicate with the server over TCP port 1433. No one at an unauthorized computer can send a packet to port 1433 on the SQL Server system, much less try to guess passwords, exploit SQL Server-specific buffer overflows, or launch SQL Server-specific Denial of Service (DoS) attacks. Additionally, traffic to and from the server over port 1433 is protected against sniffing. What are the keys to keeping this scheme secure?

In addition to implementing general domain security controls and monitoring, make sure that no one adds an inappropriate computer to the Authorized SQL Server Clients group. Such an addition would enable users of that computer to request a certificate from SqlIPSecCA. Note also that you've protected access to the SQL Server system over only port 1433. What about other forms of communication, such as traffic that relates to administering the server remotely (i.e., through Windows terminal services, file sharing, FTP, or Telnet)? To close these doorways into the system, you need to add another rule to the SQL Server's IPSec policy. This rule will require IPSec for all traffic over ports other than TCP port 1433. Also, you need to limit that traffic to the relatively few administrators and computers that need to communicate with the SQL Server system on those ports.

To use certificates to secure such administrative traffic to the SQL Server system, you need to follow the instructions I've provided to repeat the entire process for a SQL Server administrative group. (See the sidebar "Secure Administrative Traffic" for details.) Creating multiple CAs just to protect one server is a significant inconvenience but is a limitation of IPSec Policies. (You can limit IPSec Policy authentication methods according to only CA name, not template name or custom field.) As an alternative, you can use preshared key authentication to restrict communications between the SQL Server system and the administrative computers. For details, see the sidebar "Extend Security Through Preshared Keys."

Choose Carefully

The key to using IPSec policies to limit network access lies in the use of authentication methods. Kerberos is useful for limiting network access to computers within a forest and requires little effort to set up because all computers within a forest automatically support Kerberos authentication. Preshared key authentication is simple to deploy and is the most flexible method because it lets you control exactly which computers within or outside of a forest can communicate with a server. However, preshared key authentication is vulnerable to key theft. Certificate-based authentication lets you limit communication to connections from certain computers within or outside of a forest but isn't very flexible because you need to maintain a different CA for each IPSec policy. The sample scenario I've presented is just one of the many ways you can use IPSec policies to increase protection within your network. Think about the important resources within your network, and consider which authentication method will work best for each.

Secure Administrative Traffic

You can use certificates to tighten down security for administrative traffic. Create a new group in Active Directory (AD) and name the group Authorized Administrative SQL Server Clients. Add the administrative computers that need to communicate with the SQL Server on ports other than 1433. Set up another Certificate Authority (CA) and edit the new CA's ACL to Allow the Enroll permission to the new group only. Create a new Group Policy Object (GPO), name it Authorized Administrative SQL Server Clients IPSEC, and add two automatic certificate requests: one for an IPSec certificate from the new CA and one for an IP Security (IPSec) certificate from SqlIPSecCA. (You need to include a certificate request to SqlIPSecCA so that you don't prevent the administrative clients from accessing the server through port 1433.) In the Authorized Administrative SQL Server Clients IPSEC GPO, create an IPSec policy and activate the policy's default response rule to use two authentication methods—certificate authentication for SqlIPSecCA and certificate authentication for the new CA. Limit the Apply Group Policy permission on the new GPO to the Authorized Administrative SQL Server Clients group, then assign the policy.

Edit the Secure SQL Server policy on the SQL Server system to add another rule. Use the All IP Traffic filter list, and set the authentication method to require a certificate from the new CA. Reassign the policy, and request a certificate from the new CA for your server. Now the server will require computers connecting to port 1433 to present a certificate from SqlIPSecCA and will require computers connecting to other ports to present a certificate from the new CA.

Extend Security Through Preshared Keys

In the sample scenario I present in Chapter 6, you're dealing with only a few computers, and you can probably assume that the administrative systems maintain better physical security than the client systems. Therefore, preshared key authentication is a reasonably safe way to extend security.

To use preshared key authentication, follow the same procedure as for certificate-based authentication, but add only the preshared key authentication method in the Authorized Administrative SQL Clients IPSEC Group Policy Object (GPO), take note of the key, and use that key to configure preshared key authentication for the Microsoft SQL Server system. If you're worried about someone capturing the preshared key from Group Policy packets traversing the network, manually configure IP Security (IPSec) on each administrative computer instead of creating the Authorized Administrative SQL Clients group, or change the key on a regular basis. To keep things in perspective, though, consider that sniffing a key from a GPO requires physical access to the network and a fair amount of skill. If someone does capture the key, they've made it past only the first level of your defenses. The attacker still needs to penetrate your SQL Server-level and application-level defenses. If you change the key each week, you can limit the amount of time an intruder has to attack those defenses.

Chapter 7

Group Policy FAQs

Q. What is the difference between Windows 2000's Group Policy and Windows NT 4.0's Group Policy Editor (GPE)?

A. Win2K's Group Policy model is an extensively updated version of NT 4.0's GPE, which lets you restrict various registry settings. Win2K's Group Policy uses Active Directory (AD) and offers more than just registry restrictions—for example, application deployment; folder redirection; logon, logoff, startup, and shutdown scripts.

You can apply Group Policy Objects (GPOs) to a site, domain, or organizational unit (OU). Users and computers often have multiple GPOs that apply to them; in case of a setting conflict, the order of precedence is local computer, site, domain, OU (i.e., LSDOU). An OU setting overrides a domain setting, a domain setting overrides a site setting, and a site setting overrides a local computer setting.

To apply a Group Policy for a site, start the Microsoft Management Console (MMC) Active Directory Sites and Services snap-in, expand the sites, right-click the site you want, and select Properties. Select the Group Policy tab.

To apply a Group Policy for a domain, start the MMC Active Directory Users and Computers snap-in, right-click the OU, and select Properties. Select the Group Policy tab.

To apply a Group Policy for an OU, start the MMC Active Directory Users and Computers snap-in, right-click the domain, and select Properties. Select the Group Policy tab.

By default, when you select Group Policy for a container, no GPO exists. You can add an existing GPO to the container or create a new GPO. To create a new GPO, click New and enter a name for the GPO. After you create a policy, you can click Edit to modify the policy. The MMC will open with GPE loaded and the selected GPO at the root.

NT 4.0 policies don't migrate to Win2K; if you upgrade, you need to redefine your policies as GPOs. In a mixed Win2K and NT 4.0 environment, you need to keep the `ntconfig.pol` file in the domain controllers' (DCs') Netlogon share to ensure that NT 4.0 clients receive their policy settings (including Win2K DCs, which might authenticate NT 4.0 client logons in a mixed environment). Win2K clients will ignore `ntconfig.pol` unless you make a policy change to instruct the clients to implement the file's contents. If you make such a change, the correct reading order is GPO(s) computer at startup, computer's `ntconfig.pol` file at logon, user's `ntconfig.pol` file at logon, GPO(s) user at logon.

—by John Savill

Q. Why can't I run Group Policy Editor (GPE) for a domain even though I'm a domain Administrator?

A. You can use Group Policy to restrict users to a set of snap-ins and administrative tools.

If you can't run GPE or other administrative tools and you receive the message *The snap-in below, referenced in this document, has been restricted by policy. Contact your administrator for details*, you need to change your domain's configuration settings.

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the domain and select Properties.
3. Select the Group Policies tab.
4. Select the default domain policy and click Edit.
5. Navigate to User Configuration\Administrative Templates\Windows Components\Microsoft Management Console.
6. Double-click *Restrict Users to the explicitly permitted list of snap-ins*.
7. Select *Not configured*.

You can drill down farther to Restricted/Permitted snap-ins\Group Policy and set *Group Policy snap-in* to enabled and *Administrative Templates (User)* to enabled or not configured.

On a local computer, you can edit the registry to make these changes.

1. Start regedit.exe.
2. Go to the HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC registry entry.
3. Double-click RestrictToPermittedSnapins.
4. Set to 0 and click OK.
5. Close the registry editor.

If you still can't start the Group Policy snap-in, perform the following additional actions.

1. Start regedit.exe.
2. Go to the HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC registry entry.
3. Change the Restrict_Run value to 0 in the following keys if they exist:
 {8FC0B734-A0E1-11D1-A7D3-0000F87571E3} (this is the restriction for Group Policy snap-in)
 {0F6B957E-509E-11D1-A7CC-0000F87571E3} (this is the restriction for the Administrative Templates)
4. Close the registry editor.

—by John Savill

Q. How do I add templates to a Group Policy Object (GPO)?

A. Windows 2000's GPOs still support Windows NT 4.0's .adm templates, which are registry-based settings. Win2K's Group Policy lists these templates under the Administrative Templates branch. Win2K's .adm files include system.adm for general system settings and inetres.adm for Internet Explorer (IE)-specific settings. When you apply a .adm file to a GPO, the file copies from the %systemroot%\inf folder to the %systemroot%\SYSVOL\domain\Policies\<GUID of GPO>\Adm folder.

To add or remove a new template from a GPO, perform the following steps.

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the container whose GPO you want to change and select Properties.
3. Select the Group Policy tab.

4. Select the GPO and click Edit.
5. The MMC Group Policy snap-in will start, with the GPO at the root.
6. Under *User or Computer configuration*, right-click Administrative Templates and select Add/Remove Templates.
7. Click Add. (To remove a template, select the template and click Remove.)
8. Select the .adm file to add and click Open.
9. Click Close.

—by John Savill

Q. Can I use Group Policy to display or remove the Shut Down button on the logon screen?

A. To use Group Policy to configure the logon screen on a local computer, perform the following steps.

1. Go to a command prompt and enter

```
gpedit.msc
```

to start Group Policy Editor (GPE).

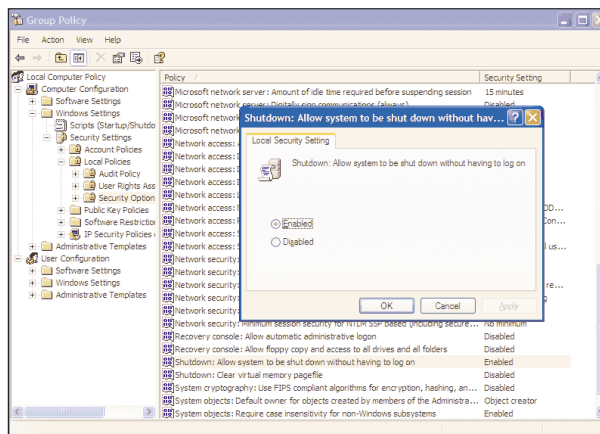
2. Expand Computer Configuration, Windows Settings, Security Settings, Local Policies. Select Security Options.
3. Double-click *Shutdown: Allow system to be shut down without having to log on*, configure the setting to Enabled or Disabled, and click OK, as Figure 1 shows.
4. Close GPE.

To configure the Shutdown setting as a domain Group Policy Object (GPO), perform the following steps.

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click the container that holds the GPO you want to modify (e.g., a domain, an organizational unit—OU), select Properties, select the Group Policy tab, select the policy, and click Edit.
3. Double-click *Shutdown: Allow system to be shut down without having to log on*, configure the setting to Enabled or Disabled, and click OK.
4. Close the MMC.

—by John Savill

Figure 1
Enabling the Shutdown local security setting



Q. How do I force a user to use a machine-specific Group Policy rather than a user-specific Group Policy?

A. Typically, the settings that the OS applies when a user logs on are based on the user's account container (e.g., a domain, a site, an organizational unit—OU), regardless of which container the user's machine belongs to. In some instances, you might want to forgo using this default behavior and instead associate a user's settings with the location of the user's computer within Active Directory (AD). For example, you might want to set a strict, defined set of policies for a publicly accessible computer, regardless of who logs on to that computer.

To establish machine-specific settings, use Group Policy to set the computer's container to *loopback* mode—so that the computer's client settings take precedence—by performing the following steps.

1. Start Group Policy Editor (GPE) and load the policy that affects the computer whose behavior you want to modify (alternatively, you can start the Microsoft Management Console—MMC—Active Directory Users and Computers snap-in, right-click the container, select Properties, then select the Group Policy tab).
2. Expand the Computer Configuration, Administrative Templates, System, Group Policy branches.
3. Double-click the Loopback Policy option (or *User Group Policy loopback processing mode* in Windows .NET Server—Win.NET Server).
4. Select the Enabled option, then select the Mode:
 - Merge Mode—loads a user's normal settings first, then loads any settings based on the computer's location, thus overwriting any conflicting user settings
 - Replace Mode—loads only settings based on the computer's location
5. Click OK.

—by John Savill

Q. How do I configure Group Policy to apply folder redirection settings to users who access the local network remotely?

A. By default, Windows 2000 doesn't apply Group Policy folder redirection settings to users on slow network connections. To modify this behavior, perform the following steps.

1. Start Group Policy Editor (GPE) and load the policy in question. (Alternatively, you can right-click the Active Directory—AD—container that the policy applies to, select Properties, select the Group Policy tab, and click Edit.)
2. Navigate to Computer Configuration, Administrative Templates, System, Group Policy.
3. Double-click *Folder Redirection policy processing*.
4. Select Enabled.
5. Select the *Allow processing across a slow network connection* check box. (You can also double-click *Group Policy slow link detection* to set what constitutes a slow link.)

—by John Savill

Q. How do I use Group Policy to set Advanced Internet Explorer (IE) settings?

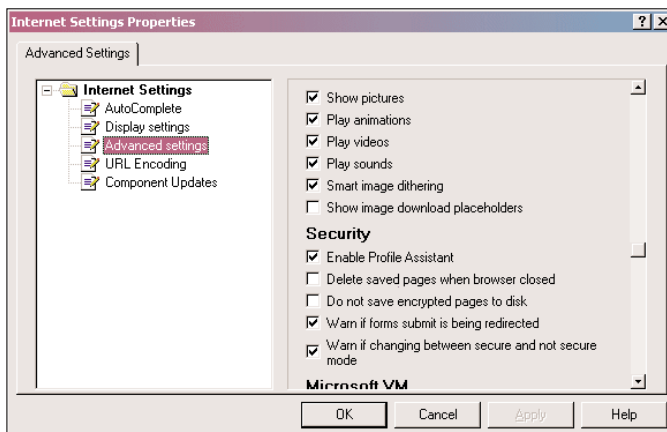
A. The Internet Explorer Maintenance portion of the Group Policy (User Configuration, Windows Settings) has a hidden option. To access this option, perform the following steps.

1. Open the Group Policy you want to modify.
2. Expand User Configuration, Windows Settings.
3. Right-click Internet Explorer Maintenance.
4. Select Preference Mode from the context menu.
5. The system will add a new Advanced branch with two groups, Corporate and Internet Settings. Double-click one of them.
6. The system will open a dialog box with various settings that you can change. (The *Advanced settings* option under Internet Settings, which Figure 2 shows, is useful.)
7. Click OK.

If you want to remove the Advanced object, you must select Reset Browser Settings, which loses all your other settings but removes the Advanced object. Likewise, if a Group Policy is already applied, you need to reset it and then enable the Preference mode.

—by John Savill

Figure 2
The Internet Settings Advanced settings option



Q. How do I determine which containers link to Group Policy?

A. Windows 2000 lets an administrator link Group Policy to several different domains, sites, and organizational units (OUs). Before you delete a Group Policy, you must be sure no container still links to the Group Policy. To check a Group Policy's links, perform the following steps.

1. Start the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.
2. Right-click a container that links to the Group Policy you want to check.
3. Select the Group Policy tab.
4. Select the Links tab.
5. Select the domain you want to search for the Group Policy and click Find Now. You'll see a list of all containers linking to the selected Group Policy.

—by Mark Joseph Edwards

Q. How do I properly apply security settings in GPOs?

I want to make sure that I'm applying the security settings in my Group Policy Objects (GPOs) correctly. In Group Policy, what's the relationship between the Block Policy inheritance and No Override options, and how can I best use them?

A. In short, No Override takes precedence over *Block Policy inheritance*. Remember that Windows 2000 applies GPOs in a specific sequence. Win2K first applies a local computer's GPO, then (in order) any site-linked GPOs, domain-linked GPOs, and organizational unit (OU)—linked GPOs. When two or more GPOs define a value for the same policy (with very few exceptions, such as logon scripts), the last policy wins. For example, if you define the *Audit account management*

category with Success, Failure at the domain level but specify Failure for the same policy in a GPO linked to a lower-level OU (i.e., OUs beneath the domain), computers in that lower-level OU will end up with the *Audit account management* category set to Failure.

You can specify the *Block Policy inheritance* setting on domains and OUs. To do so, open the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in, double-click a domain or OU, and click the Group Policy tab. If you select the *Block Policy inheritance* option at the domain level, when computers in this domain apply Group Policy, they won't apply any site-linked GPOs. If you select the *Block Policy inheritance* option on an OU, computers in this OU won't apply site-linked GPOs, domain-linked GPOs, or GPOs linked to higher-level OUs. Note that Win2K always applies a computer's local GPO regardless of *Block Policy inheritance* settings, but because the local GPO is the first one applied, any conflicting policies in subsequent GPOs override the local GPO. You can use the *Block Policy inheritance* option when you have a subset of computers or users that you want to insulate from policies you set at the domain or higher level. Put those users or computers in an OU and select the *Block Policy inheritance* check box. Now, you can manage those computers exclusively through GPOs linked to that OU.

What I've described is default behavior, but consider what happens when you use the No Override option. You select the No Override option by clicking that column in the list of GPOs. No Override is a GPO link-level setting instead of a domain- or OU-level setting. Therefore, if you link the same GPO to more than one site, domain, or OU, the No Override setting won't follow the GPO. You can control No Override at each point at which a GPO is linked. If you specify No Override on a GPO link, the policies you've defined in that GPO override any conflicting policies in GPOs processed later in the Group Policy application sequence. Policies that you define in No Override GPO links defeat conflicting policies even in GPOs that specify the *Block Policy inheritance* setting or other subsequently applied GPOs that specify the No Override setting.

You can use the No Override setting to configure mandatory policies. For example, you might have certain default domain-level policies (i.e., you can override them at lower OUs to manage legitimate exceptions). You can configure these policies in the Default Domain Policy GPO. You might also have policies that you want to apply without exception to all computers or users in the domain. If so, define these mandatory policies in a new GPO that you create called Mandatory Domain Policies, link the Mandatory Domain Policies GPO to the domain, and configure the new GPO link with the No Override setting. Rest assured that policies that you define in Mandatory Domain Policies will override any policy conflicts that OU-linked GPOs inadvertently create at lower levels in the domain.

—by Randy Franklin Smith

Q. How do I use Group Policy to configure screen savers?

I'm trying to use a group policy to enforce a password-protected screen saver for users in my domain. Although I enforce a screen saver in the \\default domain policy\user configuration\administrative templates\control panel\display folder, the screen saver is never activated. How can I activate the screen saver? Also, can I specify how long the workstation must be inactive before the screen saver is activated?

A. Enforcing a password-protected screen saver is important because many users don't like the nuisance of unlocking their workstation after they've been away from it. As a result, some users disable the screen saver, which leaves their workstations open when unattended.

Windows 2000 Service Pack 1 (SP1) solves this security problem. Before SP1, the Display folder of a Group Policy Object (GPO) offered four screen saver policy settings:

Hide Screen Saver tab

Screen saver executable name

No screen saver

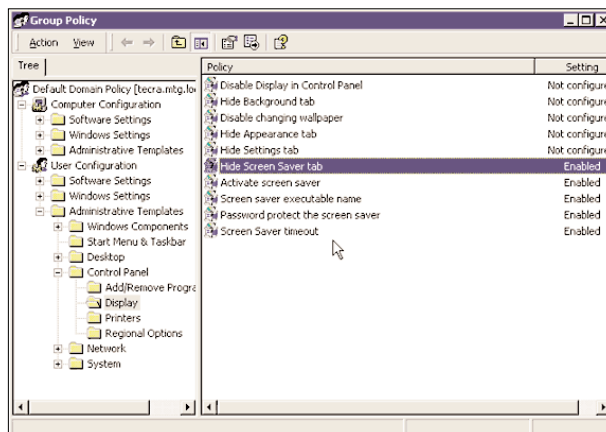
Password protect the screen saver

Although Microsoft doesn't document the bug in the service pack's list of bug fixes, pre-SP1 Win2K doesn't properly configure the screen saver when you use these group policy settings. For some reason, the screen saver you specify with a group policy takes effect only on user profiles in which the user has previously opened Control Panel and configured a screen saver. SP1 fixes this problem and replaces *No screen saver* with *Activate screen saver*. SP1 also adds a new policy called *Screen Saver timeout*, as Figure 3 shows.

So, you now have five screen saver policies that you can use to ensure that unattended workstations automatically lock the console. For example, you can use the *Hide Screen Saver tab* policy to prevent users from accessing and disabling their screen saver settings. However, you still need to specify a screen saver. To specify a screen saver, you must specify the filename of a screen saver in the *Screen saver executable name* policy. Screen savers that come with Win2K exist in the `%systemroot%\system32\config` folder. I recommend using `default.scr`: It's boring, but it doesn't use unnecessary CPU cycles drawing 3-D images on your screen. Next, you need to enable the *Activate screen saver* and *Password protect the screen saver* policies, then specify the number of seconds to wait in the *Screen Saver time-out* policy. Be sure to make these policy changes in a GPO linked to the appropriate level of your domain. If you want to apply this policy to every user in your domain (including you), define the policy in the Default Domain Policy linked to the root of your domain. Otherwise, use a GPO linked to the organizational unit (OU) that contains the users you want to configure.

—by Randy Franklin Smith

Figure 3
SP1's Screen Saver timeout policy



Q. How can I locate all the GPOs in my domain?

To keep track of where other administrators and I have defined security policies, I'd like to generate a list of all the Group Policy Objects (GPOs) in my domain without having to open the Properties dialog box of each organizational unit (OU) and click the Group Policy tab. How can I generate such a list quickly?

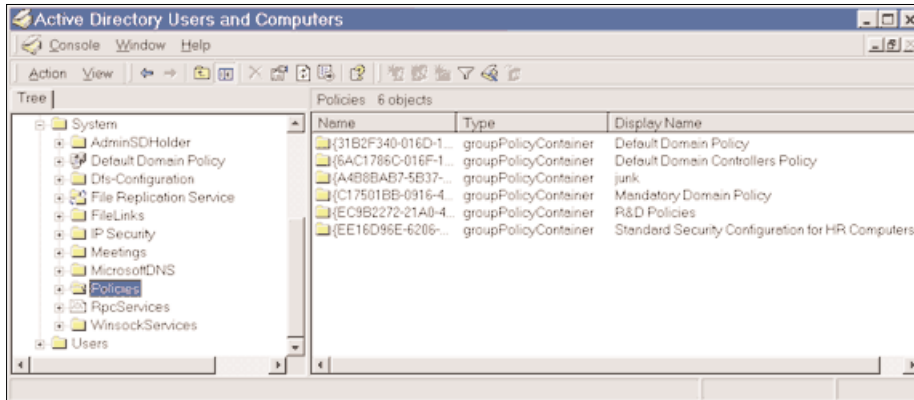
A. You can see all the GPOs in your domain by looking in the \system\policies container in the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in. When you open the Active Directory Users and Computers snap-in, you won't at first see the System container. Choose View, Advanced Features from the console's menu bar, then navigate to the \system\policies container, as Figure 4 shows.

System is a special container in which Active Directory (AD) stores system objects such as IP Security (IPSec) policies, DNS records, GPOs, and other objects that don't belong in your usual OU hierarchy. AD stores GPOs in the \system\policies container. However, when you first view the GPOs in the Policies container, you'll see only the globally unique identifiers (GUIDs) of each GPO, which isn't useful. Choose View, Columns from the console's menu bar, add Display Name to the displayed columns list, then click OK. Now, you'll be able to see all the GPOs in your domain with the same display name that you usually see when you view the Group Policy tab of an OU, site, or domain.

The only disadvantage of this method is that you can't edit GPOs from the Policies container or find out where a given GPO is linked. Therefore, another method is to right-click any OU, select Properties, click the Group Policy tab, click Add, then click All. You'll see all the GPOs in your domain, and you can right-click a GPO and select Edit, or—to find out where the GPO is linked—select Properties, then click the Links tab, which displays all the sites, domains, and OUs to which the GPO is linked.

—by Randy Franklin Smith

Figure 4
Viewing the \system\policies container



Q. How can I address Group Policy conflicts?

I understand that enabling *Disable background refresh of Group Policy* for one policy will turn off refreshes for all policies. Where can I find a list of all the settings available for individual group policies that affect all group policies? I've seen identical settings enabled in different Group Policy Objects (GPOs) that have different effects: They might override the previous GPO, mesh with the previous GPO (e.g., Microsoft Internet Explorer—IE—Favorites), or affect all GPOs. Please let me know about any articles or utilities that can help me identify key aspects of Group Policy.

A. The only settings in Group Policy that affect all other group policies are those listed under \computer configuration\administrative templates\system\group policy and \user configuration\administrative templates\system\group policy. These settings control the Group Policy engine that processes GPOs at system startup, user logon, and at refresh intervals thereafter. I agree that the task of understanding how group policies will be applied and diagnosing conflicts between group policies is complex. I've found FullArmor's FAZAM, available in the *Microsoft Windows 2000 Server Resource Kit Supplement One*, to be extremely helpful with this problem. FAZAM lets you trace how Group Policy is applied and run "what-if" scenarios that simulate Group Policy application with users, computers, and organizational units (OUs) of your choosing.

—by Randy Franklin Smith

Q. How do I configure Group Policy's Effective Setting?

I have Administrator privileges on my Windows 2000 computer. I'm not part of any domain, just part of a workgroup on a university LAN. I want to change the security policy's user rights assignments. However, I can't change the designation in the Effective Setting column in the Local Security Settings' User Rights Assignments, which Figure 5

shows. I can change the Local Setting, but that doesn't accomplish anything because the Effective Setting isn't changed. Given that I have Administrator privileges, how can I change the setting?

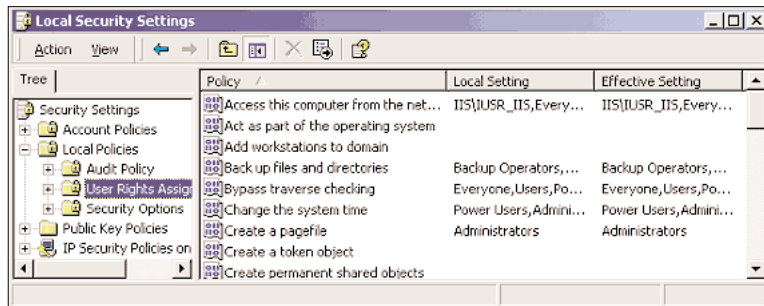
A. Effective Setting is always a read-only column that shows the actual settings for your computer after all relevant Group Policy Objects (GPOs) have been applied. In your case, only the local GPO is applied. You must configure settings through the Local Setting column, then type

```
secedit/refreshpolicy machine_policy
```

at the command line. Win2K then reapplies Group Policy. The computer's local GPO is the first object Win2K applies and, in your situation, the only one—because your computer isn't a member of an Active Directory (AD) domain. Then, right-click Security Settings and select Reload. The Effective Setting should now match the Local Setting.

—by Randy Franklin Smith

Figure 5
Viewing the Local Security Settings' User Rights Assignments



Q. How do I prevent Group Policy from applying to the Administrator account?

I need to prevent Group Policy from being applied to the Administrator group on my local machines. I know that I can add permissions to the Group Policy Object's (GPO's) ACL to deny Apply Group Policy access to the Administrator account. Must I have a Windows 2000 Active Directory (AD) server? (I won't have a Win2K server in my Windows NT domain when I roll out the desktops.)

A. To take full advantage of Win2K's new security and management features, you need to implement AD. Win2K Professional computers by themselves offer few advances beyond easier installation and better device recognition. In your situation, without AD installed, the only GPOs applied are the local GPOs on each computer. Each computer's local GPO is applied whenever the computer boots or someone logs on. Unfortunately, you can't shield administrators from the policies defined in local GPOs.

—by Randy Franklin Smith

Q. How do I use the registry to configure Group Policy update times?

A. You usually configure Group Policy update times under the Computer Configuration\Administrative Templates\System\Group Policy and the User Configuration\Administrative Templates\System\Group Policy branches; however, you can also directly set the registry to configure Group Policy update times by performing the following steps.

1. Start regedit.exe.
2. Go to the HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System registry entry to set Computer refresh. Or, alternatively, go to the

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System registry entry to set User refresh.

3. Create a DWORD value with a name of GroupPolicyRefreshTime, and set it to a number between 0 and 648000 minutes.
4. Create a DWORD value with a name of GroupPolicyRefreshTimeOffset, and set it to a number between 0 and 1440 minutes. (You specify an offset value to prevent many clients from trying to refresh at the same time.)
5. Close regedit.

—by John Savill