Chapter

10

Managing Group Policy

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Implement and troubleshoot Group Policy.**
  - Create a Group Policy object (GPO).
  - Link an existing GPO.
  - Delegate administrative control of Group Policy.
  - Modify Group Policy inheritance.
  - Filter Group Policy settings by associating security groups to GPOs.
  - Modify Group Policy.
- ✓ **Manage and troubleshoot user environments by using Group Policy.**
  - Control user environments by using administrative templates.
  - Assign script policies to users and computers.
- ✓ **Manage network configuration by using Group Policy.**

One of the biggest challenges faced by systems administrators is the management of users, groups, and client computers. It's difficult enough to deploy and manage workstations throughout the environment. When you add in the fact that users are generally able to make system configuration changes, it can quickly become a management nightmare!

For example, imagine that a user notices that they do not have enough disk space to copy a large file. Instead of seeking help from the IT help desk, they decide to do a little cleanup of their own. Unfortunately, this cleanup operation involves the deletion of many critical system files! Or, consider the case of users changing system settings "just to see what they do." Relatively minor changes, such as modifications of TCP/IP bindings or desktop settings, can cause hours of support headaches. Now, multiply these problems by hundreds (or even thousands) of end users. Clearly, there should be a way for systems administrators to limit the options available to users of client operating systems.

So how do you prevent small problems like these from occurring in a Windows 2000 environment? Fortunately, there's a solution that's readily available and easy to implement. One of the most important system administration features in Windows 2000 and the Active Directory is the use of *Group Policy*. Through the use of *Group Policy objects (GPOs)*, administrators can quickly and easily define restrictions on common actions and then apply these at the site, domain, or organizational unit (OU) level. In this chapter, we will examine how Group Policies work and then look at how they can be implemented within an Active Directory environment.

An Introduction to Group Policy

One of the strengths of Windows-based operating systems is their flexibility. End users and systems administrators can configure many different options to suit the network environment and their personal tastes. However, this flexibility comes at a price—there are many options that generally should not be changed by end users. For example, TCP/IP configuration and security policies should remain consistent for all client computers.

In previous versions of Windows, system policies were available for restricting some functionality at the desktop level. Settings could be made for users or computers. However, these settings focused primarily on preventing the user from performing such actions as changing their desktop settings. These changes were managed through the modification of Registry keys. This method made it fairly difficult for systems administrators to create and distribute policy settings. Furthermore, the types of configuration options available in the default templates were not always sufficient, and system administrators often had to dive through cryptic and poorly documented Registry settings to make the changes they required.

Windows 2000's Group Policies are designed to allow systems administrators to customize end user settings and to place restrictions on the types of actions that users can perform. Group Policies can be easily created by systems administrators and then later applied to one or more users or computers within the environment. Although they ultimately do affect Registry settings, it is much easier to configure and apply settings through the use of Group Policy than it is to manually make changes to the Registry. For ease of management, Group Policy settings can be managed from within the Active Directory environment, utilizing the structure of users, groups, and OUs.

There are several different potential uses for Group Policies. We covered one of them, managing security settings, in Chapter 8, "Active Directory Security." And, we'll cover the use of Group Policies for software deployment in Chapter 11, "Software Deployment through Group Policy." The focus of this chapter will be on the technical background of Group Policies and how they apply to general configuration management.

Let's begin by looking at how Group Policies function.

Group Policy Settings

Group Policy settings are based on Group Policy *administrative templates*. These templates provide a list of user-friendly configuration options and specify the system settings to which they apply. For example, the option to enforce a desktop setting for a user or computer would map to a specific Registry key that maintains this value. When the option is set, the appropriate change is made in the Registry of the affected user(s) and computer(s).

By default, Windows 2000 comes with several Administrative Template files that can be used for managing common settings. Additionally, systems administrators and application developers can create their own Administrative Template files to set options for specific functionality.

Most Group Policy items have three different settings options:

Enabled Specifies that a setting for this Group Policy object has been configured. Some settings will require values or options to be set.

Disabled Specifies that this option is disabled for client computers. Note that disabling an option *is* a setting. That is, it specifies that the systems administrator wants to disallow certain functionality.

Not Configured Specifies that these settings have been neither enabled nor disabled. Not Configured is the default option for most settings. It simply states that this Group Policy will not specify an option and that settings from other policy settings may take precedence.

The specific options available (and their effects) will depend on the setting. Often, additional information is required. For example, when setting the Account Lockout policy, you must specify how many bad login attempts may be made before the account is locked out. With this in mind, let's look at the types of user and computer settings that can be managed.

User and Computer Settings

Group Policy settings can apply to two types of Active Directory objects: Users and Computers. Since both Users and Computers can be placed into groups and organized within OUs, this type of configuration simplifies the management of hundreds, or even thousands, of computers.

The main types of settings that can be made within User and Computer Group Policies are as follows:

Software Settings Software settings apply to specific applications and software that might be installed on the computer. Systems administrators can use these settings to make new applications available to end users and

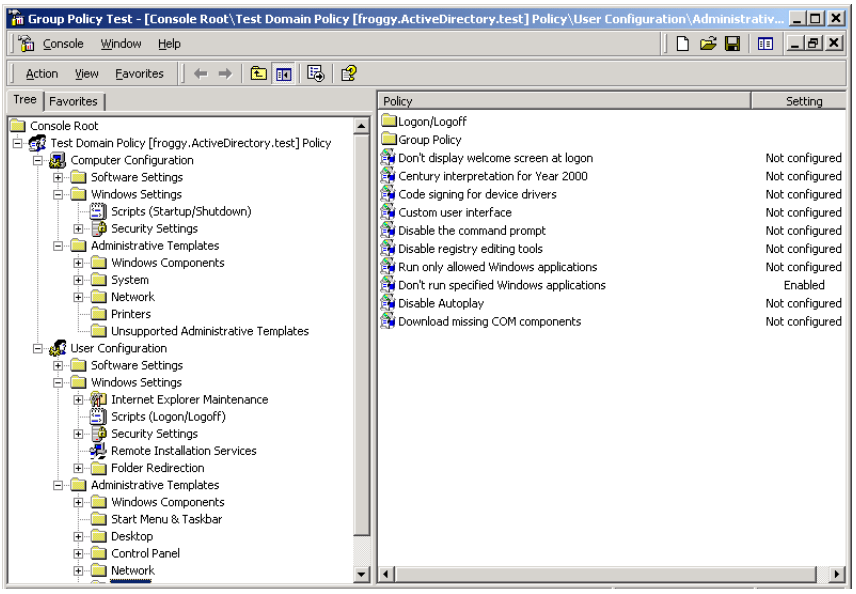
control the default configuration for these applications. For more information on configuring software settings using Group Policy, see Chapter 11, "Software Deployment through Group Policy."

Windows Settings Windows settings options allow systems administrators to customize the behavior of the Windows operating system. The specific options that are available here differ for users and computers. For example, the User-specific settings allow the configuration of Internet Explorer (including the default home page and other settings), while the computer settings include security options such as account policy and event log options.

Administrative Templates The options available in administrative templates are used to further configure user and computer settings. In addition to the default options available, systems administrators can create their own administrative templates with custom options.

Figure 10.1 provides an example of the types of options that can be configured with Group Policy.

FIGURE 10.1 Group Policy configuration options



Later in this chapter, we'll look into the various options available in more detail.

Group Policy Objects

So far, we have been talking about what Group Policies are designed to do. Now, it's time to drill down into determining exactly how they can be set up and configured.

For ease of management, Group Policies may be contained in items called Group Policy objects (GPOs). GPOs act as containers for the settings made within Group Policy files, which simplifies the management of settings. For example, as a systems administrator, you might have different policies for users and computers in different departments. Based on these requirements, you could create a GPO for members of the Sales department and another for members of the Engineering department. Then you could apply the GPOs to the OU for each department.

Another important concept is that Group Policy settings are hierarchical. That is, Group Policy settings can be applied at three different levels:

Sites At the highest level, GPOs can be configured to apply to entire sites within an Active Directory environment. These settings apply to all of the domains and servers that are part of a site. Group Policy settings that are managed at the site level may apply to more than one domain. Therefore, they are useful when you want to make settings that apply to all of the domains within an Active Directory tree or forest. For more information on sites, see Chapter 6, "Configuring Sites and Managing Replication."

Domains Domains are the second level to which GPOs can be assigned. GPO settings that are placed at the domain level will apply to all of the User and Computer objects within the domain. Usually, systems administrators will make master settings at the domain level.

Organizational Units The most granular level of settings for GPOs is at the OU level. By configuring Group Policy options for OUs, systems administrators can take advantage of the hierarchical structure of the Active Directory. If the OU structure is planned well, it will be easy to make logical GPO assignments for various business units at the OU level.

Based on the business need and the organization of the Active Directory environment, systems administrators might decide to set up Group Policy settings at any of these three levels. Since the settings are cumulative by default, a User object might receive policy settings from the site level, from the domain level, and from the organizational units in which it is contained. Group Policy settings can also be applied to the local computer (in which case the Active Directory is not used at all), but this limits the manageability of the Group Policy settings.

Group Policy Inheritance

In most cases, Group Policy settings will be cumulative. For example, a GPO at the domain level might specify that all users within the domain must change their passwords every 60 days, and a GPO at the OU level might specify the default desktop background for all users and computers within that OU. In this case, both settings will apply, and users within the OU will be forced to change their password every 60 days and have the default desktop setting.

So what happens if there's a conflict in the settings? For example, suppose a GPO at the site level specifies that users are to change passwords every 60 days while one at the OU level specifies that they must change passwords every 90 days. This raises an important point about *inheritance*. By default, the settings at the most specific level (in this case, the OU, which contains the User object) will override those at more general levels.

Although the default behavior is for settings to be cumulative and inherited, systems administrators can modify this behavior. There are two main options that can be set at the various levels to which GPOs might apply:

Block Policy Inheritance The Block Policy Inheritance option specifies that Group Policy settings for an object are not inherited from its parents. This might be used, for example, when a child OU requires completely different settings from a parent OU. Note, however, that blocking policy inheritance should be managed carefully, since this option allows other systems administrators to override the settings made at higher levels.

Force Policy Inheritance The Force Policy Inheritance option can be placed on a parent object and ensures that all lower-level objects inherit these settings. In some cases, systems administrators want to ensure that Group Policy inheritance is not blocked at other levels. For example, suppose it is corporate policy that all Network accounts are locked out after five incorrect password attempts. In this case, you would not want lower-level systems administrators to override the option with other settings.

This option is generally used when systems administrators want to globally enforce a specific setting. For example, if a password expiration policy should apply to all users and computers within a domain, a GPO with the Force Policy Inheritance option enabled could be created at the domain level.

One final case must be considered: If there is a conflict between the computer and user settings, the user settings will take effect. If, for instance, there is a default desktop setting applied for the Computer policy, and there is a different default desktop setting for the User policy, the one specified in the User object will take effect. This is because the user settings are more specific, and it allows systems administrators to make changes for individual users, regardless of the computer they're using.

Implementing Group Policy

Now that we've covered the basic layout and structure of Group Policies and how they work, let's look at how they can be implemented in an Active Directory environment. In this section, we'll start by creating GPOs. Then, we'll apply these GPOs to specific Active Directory objects.

Microsoft Exam Objective

Implement and troubleshoot Group Policy.

- Create a Group Policy object (GPO).
- Link an existing GPO.
- Modify Group Policy.

Manage and troubleshoot user environments by using Group Policy.

- Control user environments by using administrative templates.
- Assign script policies to users and computers.

See the section "Managing Group Policy" later in this chapter for coverage of the material related to the "Assign script policies to users and computers" subobjective.

Creating GPOs

Although there is only one Group Policy editing application included with Windows 2000, there are several ways to access it. This is because systems administrators may choose to apply the Group Policy settings at different levels within the Active Directory. In order to create GPOs at different levels, you can use the following tools:

Active Directory Sites and Services Used for linking GPOs at the site level.

Active Directory Users and Computers Used for linking GPOs at the domain or OU level.

MMC Group Policy Snap-In By directly configuring the Microsoft Management Console (MMC) Group Policy snap-in, you can access and edit GPOs at any level of the hierarchy. This is also a useful option since it allows you to modify the local Group Policy settings and create a custom console that is saved to the Administrative Tools program group.

Exercise 10.1 walks you through the process of creating a custom MMC snap-in for editing Group Policy settings.

You should be careful when making Group Policy settings since certain options might prevent the proper use of systems on your network. Always test Group Policy settings on a small group of users before deploying GPOs throughout your organization. You'll probably find that some settings need to be changed in order to be effective.

EXERCISE 10.1

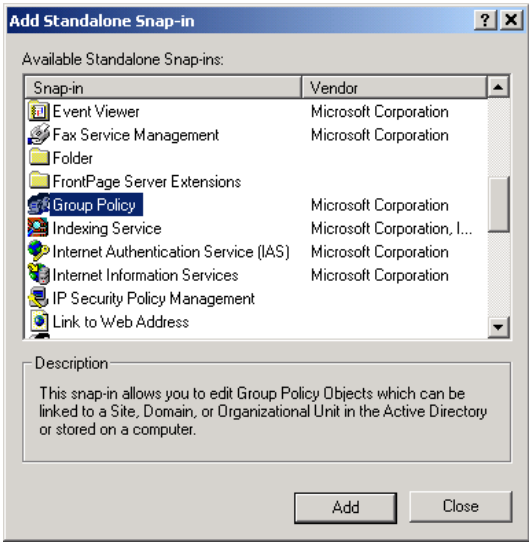
Creating a Group Policy Object Using MMC

In this exercise, we will create a custom Group Policy snap-in for managing user and computer settings.

1. Click Start ➢ Run, type **mmc**, and press Enter.
2. On the Console menu, click Add/Remove Snap-In.

EXERCISE 10.1 *(continued)*

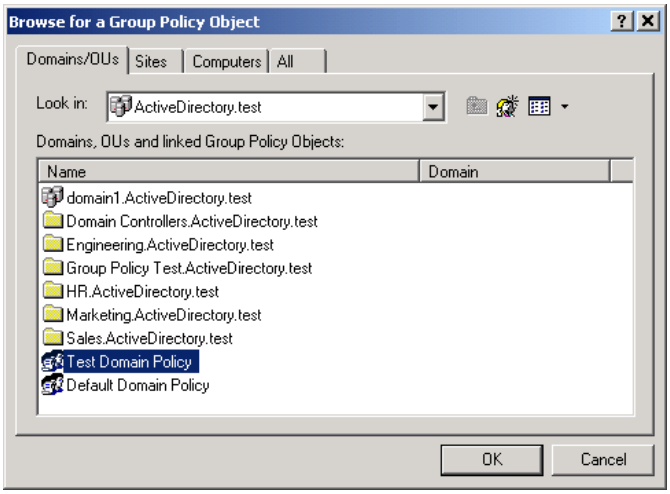
3. Click the Add button. Select Group Policy from the list, and click Add.



4. For the Group Policy Object setting, click Browse. Note that you can set the scope to Domains/OUs, Sites, or Computers. On the Domains/OUs tab, click the New Policy button (located to the right of the Look In drop-down list).

EXERCISE 10.1 *(continued)*

5. To name the new object, type **Test Domain Policy**. Click OK to open the Policy object.



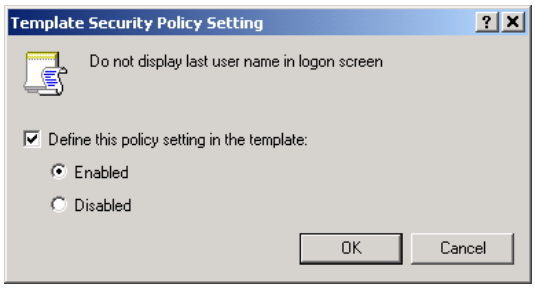
6. Place a check mark next to the Allow the Focus of the Group Policy Snap-In to Be Changed When Launching from the Command Line option. This will allow the context of the snap-in to be changed when you launch the MMC item.

7. Click Finish to create the Group Policy object. Click Close in the Add Standalone Snap-In dialog box. Finally, click OK to add the new snap-in.

8. Next, we'll make some changes to the default settings for this new GPO. Open the following items: Test Domain Policy ➢ Computer Configuration ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Security Options.

EXERCISE 10.1 *(continued)*

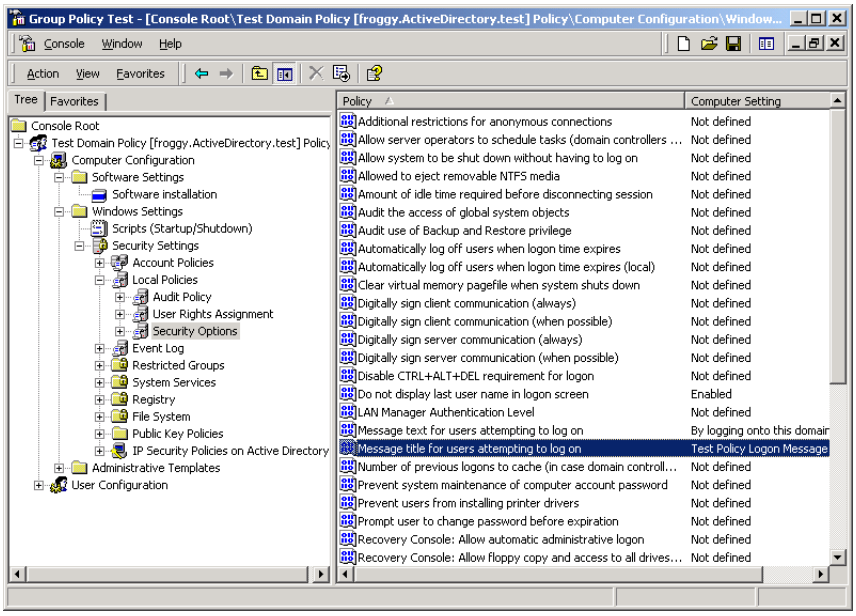
9. Double-click the Do Not Display Last User Name in Logon Screen option. Place a check mark next to the Define This Policy Setting in the Template option, and then select Enabled. Click OK to save the setting.



10. Double-click the Message Title for Users Attempting to Log On option. Place a check mark next to the Define This Policy Setting in the Template option, and then type the following: **By logging onto this domain, you specify that you agree to the usage policies as defined by the IT department**. Click OK to save the setting.

EXERCISE 10.1 *(continued)*

11. Double-click the Message Title for Users Attempting to Log On option. Place a check mark next to the Define This Policy Setting in the Template option, and then type **Test Policy Logon Message**. Click OK to save the setting.



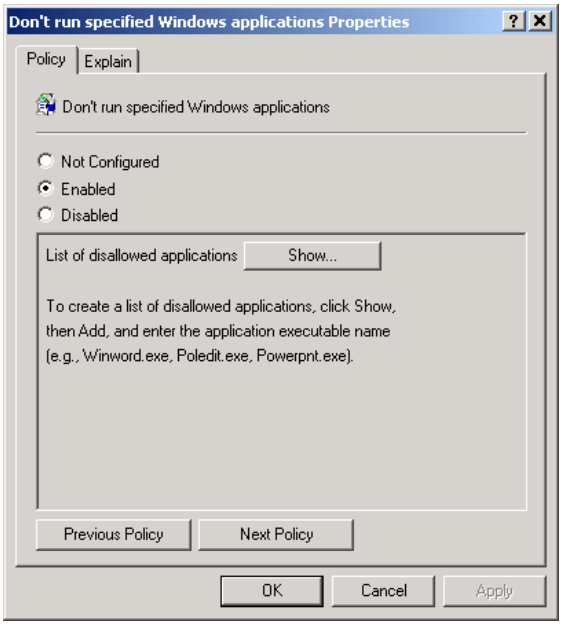
12. Now, to make changes to the User settings, expand the following objects: Test Domain Policy ➢ User Configuration ➢ Administrative Templates ➢ Start Menu & Task Bar.

13. Double-click the Add Logoff to the Start Menu option. Note that you can get a description of the purpose of this setting by clicking the Explain tab. Select Enabled, and then click OK.

14. Expand the following objects: Test Domain Policy ➢ User Configuration ➢ Administrative Templates ➢ System.

EXERCISE 10.1 *(continued)*

15. Double-click the Don't Run Specified Windows Applications option. Select Enabled, and then click the Show button. To add to the list of disallowed applications, click the Add button. When prompted to enter the item, type **wordpad.exe**. To save the setting, click OK three times.



16. To change network configuration settings, click Test Domain Policy ➢ User Configuration ➢ Administrative Templates ➢ Network ➢ Offline Files. Note that you can change the default file locations for several different network folders.

17. To change script settings (which we will cover later in this chapter), click Test Domain Policy ➢ Computer Configuration ➢ Windows Settings ➢ Scripts (Startup/Shutdown). Note that you can add script settings by double-clicking either the Startup and/or the Shutdown item.

EXERCISE 10.1 *(continued)*

18. The changes you have made for this GPO are automatically saved. You can optionally save this customized MMC console by selecting Save As from the Console menu. Then provide a name for the new MMC snap-in (such as "Group Policy Test"). You will now see this item in the Administrative Tools program group.
19. When you are finished modifying the Group Policy settings, close the MMC tool.

Note that Group Policy changes do not take effect until the next user logs in. That is, users that are currently working on the system will not see the effects of the changes until they log off and log in again.

Now that we've seen how to create a custom MMC snap-in for modifying Group Policy, let's look at how GPOs can be linked to Active Directory objects.

Linking GPOs to the Active Directory

The creation of a GPO is the first step in assigning Group Policies. The second step is to link the GPO to a specific Active Directory object. As mentioned earlier in this chapter, GPOs can be linked to sites, domains, and OUs.

Exercise 10.2 walks through the steps required to assign a GPO to an OU within the local domain.

EXERCISE 10.2

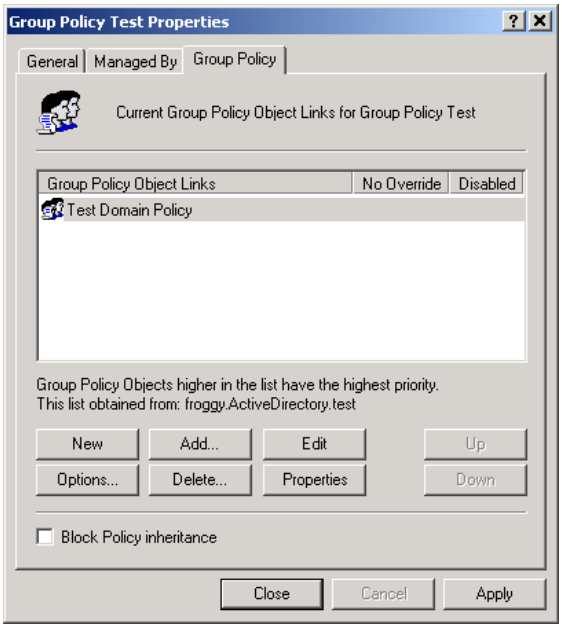
Linking GPOs to the Active Directory

In this exercise, we will link the Test Domain Policy GPO to an OU. In order to complete the steps in this exercise, you must have first completed Exercise 10.1.

1. Open the Active Directory Users and Computers tool.
2. Create a new top-level OU called Group Policy Test.
3. Right-click the Group Policy Test OU, and click Properties.

EXERCISE 10.2 *(continued)*

4. Select the Group Policy tab. To add a new policy at the OU level, click Add. In the Look In drop-down list, select the name of the local domain. Select the Test Domain Policy GPO, and then click OK.



5. Note that you can also add additional GPOs to this OU. When multiple GPOs are assigned, you can also control the order in which they apply by using the Up and Down buttons. Finally, you can edit the GPO by clicking the Edit button, and you can remove the link (or, optionally, delete the GPO entirely) by clicking the Delete button.

6. To save the GPO link, click OK. When finished, close the Active Directory Users and Computers tool.

Note that the Active Directory Users and Computers tool offers a lot of flexibility in assigning GPOs. We could create new GPOs, add multiple GPOs, edit them directly, change priority settings, remove links, and delete GPOs all from within this interface. In general, creating new GPOs

using the Active Directory Sites and Services or the Active Directory Users and Computers tool is the quickest and easiest way to create the settings you need.

To test the Group Policy settings, you can simply create a User or Computer account within the Group Policy Test OU that we created in Exercise 10.2. Then, using another computer that is a member of the same domain, log on as the newly created user. First, you should see the pre-logon message that we set in Exercise 10.1. After logging on, you'll also notice that the other changes have taken effect. For example, you will not be able to run the `WordPad.exe` program.

When testing Group Policy settings, it is very convenient to use the Terminal Services functionality of Windows 2000. Although it is beyond the scope of this book to describe the use and configuration of Terminal Services in detail, this feature allows you to have multiple simultaneous logon sessions to the same computer. With respect to Group Policy, it is useful when you want to modify Group Policy settings and then quickly log on under another User account to test them. For more information on using Terminal Services, see *MCSE: Windows 2000 Server Study Guide* (Sybex, 2000).

Using Administrative Templates

There are many different options that can be modified by Group Policy settings. Microsoft has included some of the most common and useful items by default, and they're made available when you create new GPOs or when you edit existing ones. You can, however, create your own templates and include them in the list of settings.

By default, there are several templates that are included with Windows 2000. These are as follows:

Common.adm Contains the policy options that are common to both Windows 95/98 and Windows NT 4 computers.

Inetres.adm Contains the policy options for configuring Internet Explorer options on Windows 2000 client computers.

System.adm Includes common configuration options and settings for Windows 2000 client computers.