Windows 2000 Server

Chapter 22 - Group Policy

Group Policy is one of the important Change and Configuration Management technologies provided in the Microsoft® Windows® 2000 operating system. Administrators use Group Policy to specify options for managed desktop configurations for groups of computers and users. Group Policy is flexible and includes options for registry-based policy settings, security settings, software installation, scripts, computer startup and shutdown, user logon and logoff, and folder redirection. Microsoft® Windows® 2000 Server includes hundreds of Group Policy settings you can configure. Group Policy allows an organization to reduce total cost of ownership by allowing administrators to enhance and control users' desktops.

In This Chapter

Related Information in the Resource Kit

- For more information about Active Directory™, see the chapters on Active Directory in this book.
- For more information about Change and Configuration Management see "Introduction to Desktop Management" in this book.
- For more information about Access Control see "Access Control" in this book.
- For more information about Group Policy backup see "Active Directory Backup and Restore" in this book.
- For information about the Software Installation snap-in, see "Software Installation and Maintenance" in this book.

Group Policy Overview

Group Policy allows you to stipulate users' environments only once, and to rely on the operating system to enforce them thereafter.

Group Policy objects are not profiles. A profile is a user environment setting that a user can change, such as: desktop settings, registry settings in NTUser.dat files, profiles directory, My Documents, or Favorites. You, as the administrator, manage and maintain Group Policy, an MMC hosted administrative tool used to set policy on groups of users and computers.

By default, Group Policy is inherited from site, to domain, and finally to the organizational unit level. The order and level in which you apply Group Policy objects (by linking them to their targets) determines the Group Policy settings that a user or computer actually receives. Furthermore, policy can be blocked at the Active Directory site, domain, or organizational unit level; or policy can be enforced on a per Group Policy object basis. This is done by linking the Group Policy object to its target and then setting the link to no override.

By default, Group Policy affects all computers and users in the site, domain, or organizational unit, and does not affect any other objects in that site, domain, or organizational unit.

Note In particular, Group Policy does not affect security groups.

Instead, you use security groups to filter Group Policy; that is, to alter its scope. This is done by adjusting the Apply Group Policy and the Read permissions on the Group Policy object for the relevant security groups, as explained later in this chapter.

Note The location of a security group in Active Directory is irrelevant to Group Policy.

Windows NT 4.0 and Windows 2000 Policy Comparison

Microsoft® Windows NT® 4.0 introduced the System Policy Editor (Poledit.exe), a tool that you use to specify user and computer configurations that it stores in the Windows NT registry. Using the System Policy Editor, you control the user work environment and enforce system configuration settings for all domain computers running Windows NT Workstation 4.0 or Windows NT Server 4.0. System Policy settings are registry settings that define the behavior of various components of the desktop environment.

In Windows 2000, you can create a specific desktop configuration for a particular group of users and computers by using the Group Policy snap-in. For Windows 2000 clients, the Group Policy snap-in almost entirely supersedes the System Policy Editor. It allows management of desktop configurations for large, possibly nested, and even overlapping, groups of computers and users. Non-local Group Policy objects exert their effect by being linked to any number of targets, which can be sites, domains, or organizational units in Active Directory.

System Policy in Windows NT 4.0, Windows 95, and Windows 98

The System Policy settings you specify with the System Policy Editor (Poledit.exe):

- Are applied to domains.
- Can be further controlled by user membership in security groups.
- Are not secure. They can be changed by a user with the registry editor (Regedit.exe).
- Persist in users' profiles, sometimes beyond their useful lives. After a registry setting is set using Windows NT 4.0 System Policy, the setting persists until the specified policy setting is reversed or the user edits the registry.
- Are limited to administratively mandated desktop behavior based on registry settings.

Note Windows NT 4.0 registry settings can be problematic when a user's security group membership changes. You might need to manually update or remove the registry settings.

The Group Policy snap-in provides built-in features for registry-based policy, security settings, software installation, scripts, and folder redirection. The Group Policy settings that you create are contained in a Group Policy object. Each Windows 2000–based computer has one local Group Policy object, and can also be subject to any number of non-local (that is, Active Directory–based) Group Policy objects.

The policy settings you specify using Group Policy represent the primary method for enabling centralized change and configuration management in Windows 2000.

Group Policy settings:

- Can be associated with sites, domains, and organizational units.
- Affect all users and computers in the site, domain, or organizational unit.
- Can be further controlled by user or computer membership in security groups.
- Are secure. Only an administrator can change the settings.
- Are removed and rewritten whenever policy changes.
- Can be used for finely tuned desktop control and to enhance the user's computing environment.

Note Windows NT 4.0 System Policy settings in the registry sometimes persisted past their useful life because these settings remained in effect until they were explicitly changed. Windows 2000 Group Policy settings do not persist past their useful life because Windows writes them to the following secure registry locations, and removes them when a Group Policy object no longer applies. The registry locations are \Software\Policies and \Software\Microsoft\Windows\CurrentVersion\Policies.

For a detailed comparison of Windows NT 4.0 System Policy as compared to Windows 2000 Group Policy, see "Applying Change and Configuration Management" in the *Microsoft® Windows® 2000 Server Resource Kit Deployment Planning Guide*.

Active Directory Structure and Group Policy

Group Policy implementation is one of the considerations in planning the Active Directory structure for your organization. The basic units of Group Policy are Group Policy objects. These are basic units in the sense that you link (or do not link, as the case might be) an entire Group Policy object at a time. It is not possible to link only a subset of a Group Policy object to a target. Using security groups to filter the scope of Group Policy also has the effect of turning the entire Group Policy object on or off; it does not function on only part of a Group Policy object. (Notwithstanding the fact that the Software Installation and Folder Redirection extensions of Group Policy exploit permissions to tailor the behavior of those particular extensions based on security group membership.)

There are two types of Group Policy objects: local Group Policy objects and non-local Group Policy objects.

Note Each Windows 2000–based computer has only one local Group Policy object.

In the rest of this section, all Group Policy objects are non-local unless otherwise specified.

Group Policy objects are stored in a Windows 2000 domain, and their effects are enabled on sites, domains, or organizational units to which they are linked.

- A Group Policy object linked to a site (using Active Directory Sites and Services) applies to all domains at the site.
- A Group Policy object applied to a domain applies directly to all users and computers in the domain and by inheritance to all users and computers in organizational units (and in generic Active Directory containers) farther down the Active Directory tree as seen in the Active Directory Users and Computers namespace.
- A Group Policy object applied to an organizational unit applies directly to all users and computers in the organizational unit and by inheritance to all users and computers in organizational units (and in generic

Active Directory containers) farther down the Active Directory tree as seen in the Active Directory Users and Computers namespace.

It is not possible to link a Group Policy object to a generic Active Directory container. (A generic Active Directory container is identifiable by its plain folder icon in the Active Directory Users and Computers console. The icon for an organizational unit is similar, except that a small book is superimposed on the folder.) However, users and computers in generic Active Directory containers do receive policy by inheritance from Group Policy objects linked at a higher level of Active Directory. For example, the **Users** and **Computers** containers you see in Active Directory Users and Computers cannot have Group Policy objects linked directly to them, but they do receive domain-linked Group Policy objects by means of inheritance.

The local Group Policy object is applied first. Then site-linked Group Policy objects are applied in administratively specified order, then domain-linked ones in specified order, and lastly organizational unit-linked Group Policy objects beginning at the highest (in Active Directory hierarchy) organizational unit containing the user or computer account and ending with the lowest (closest to the user or computer) organizational unit containing the user or computer. At each organizational unit, any Group Policy objects linked to it are applied in administratively specified order.

The order of application detailed in the previous paragraph (1. Local, 2.: Site, 3. Domain, 4. Organizational Unit) is significant to the architect of Active Directory, because by default, policy applied later overwrites policy applied earlier for each setting where the later applied policy was either **Enabled** or **Disabled**. Settings that are **Not Configured** don't overwrite anything — any **Enabled** or **Disabled** setting applied earlier is allowed to persist.

This is the default behavior. Mechanisms exist that let you either force or prevent Group Policy objects from affecting groups of users or computers. The most powerful mechanisms for avoiding the default behavior are the **No Override** and **Enforce Policy Inheritance** settings. It is best to minimize the use of these.

Managing Group Policy

It is important to understand the following topics as they relate to managing Group Policy:

Group Policy Infrastructure and Mechanics. How Group Policy works, including linking Group Policy objects and filtering the scope of Group Policy using security groups.

Administrative Requirements for Using Group Policy. The rights you must have to use Group Policy in an Active Directory environment.

Microsoft Management Console Snap-in Extension Model. An explanation of what you see in the MMC console with Group Policy and its extensions in place.

Group Policy Infrastructure and Mechanics

In this section you learn about Group Policy objects, links to make them exert their effects, the snap-in you use to edit them, and security groups to refine their scope.

Group Policy Objects and the Group Policy Snap-in

You can think of Group Policy objects as the documents associated with the Group Policy snap-in. This is somewhat analogous to the association of .doc files with Microsoft® Word, or .txt files with Notepad; however, the analogy is not perfect.

Changes to a Group Policy object are not deferred until an explicit Save is executed, but take place during the actual edit.

Note You cannot open Group Policy objects in read-only mode.

Links to Sites, Domains, and Organizational Units

You can link Group Policy objects to specific sites, domains, or organizational units, thus maximizing and extending the power of Active Directory. Data within Group Policy objects is evaluated by the affected clients, which exploit the hierarchical nature of Active Directory to determine precedence of Group Policy settings in cases of conflict.

Access to the Group Policy Snap-in

You create a non-local Group Policy object by using the Group Policy snap-in, either as an extension to Active Directory snap-ins, or as a stand-alone MMC console.

The most common route to the Group Policy snap-in is from Active Directory Users and Computers. This allows you to link Group Policy objects to domains or organizational units. You can also access Group Policy through Active Directory Sites and Services. This is how you link Group Policy objects to sites. From these two Active Directory consoles, Group Policy is accessible by means of a context menu. You right-click the site, domain, or organizational unit, point to Properties, and then click the **Group Policy** tab. For specific examples on how to create a Group Policy object, see Windows 2000 Help.

Filtering by Security Group Membership

You can filter the effects of Group Policy on computers and users by using membership in security groups and setting discretionary access control list (DACL) permissions. This implementation ensures faster processing of Group Policy objects than would otherwise be possible. Furthermore, by using security groups, you can limit who in your organization can create Active Directory links to Group Policy objects, as well as who has access to create and modify Group Policy objects.

For details, see "Using Security Groups to Filter and Delegate Group Policy" later in this chapter.

Administrative Requirements for Using Group Policy

To set Group Policy for a selected Active Directory site, domain, or organizational unit, you must have access to a Windows 2000 domain controller for that Active Directory, and you must have Read/Write permissions to access the system volume of domain controllers (that is, the Sysvol folder), and you must have Modify Rights to the selected directory site, domain, or organizational unit. The system volume folder is created when you install a Windows 2000 domain controller or promote a Windows 2000 server to domain controller.

By default, Group Policy affects all computers and users in an Active Directory site, domain, or organizational unit to which the Group Policy object is linked. However, you can filter the effects of Group Policy, based on users' or computers' membership in Windows 2000 security groups. To filter Group Policy, you use the **Security** tab on a Group Policy object's **Properties** page to set permissions. You also use permissions to delegate the use of the Group Policy snap-in.

Microsoft Management Console Snap-in Extension Model

The main nodes of the Group Policy snap-in are MMC snap-in extensions. These extensions include Administrative Templates, Scripts, Security Settings, Software Installation, Remote Installation Services, Internet Explorer Maintenance, and Folder Redirection.

By default, all the available Group Policy snap-in extensions load when you start the Group Policy snap-in. You can modify this default behavior by using the MMC method of creating custom consoles and by using policy settings to control the behavior of MMC.

See the settings under User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\ and its subfolders for Group Policy settings concerning MMC.

Developers can create an MMC extension to the Group Policy snap-in to expand its capability to provide additional settings. These snap-in extensions can, in turn, be extended. An example of such an extensible snap-in is the Security Settings snap-in, which includes several snap-in extensions.

For information about creating MMC consoles for delegating Group Policy and related tasks, see "Delegating Control of Group Policy" later in this chapter.

For information about the Group Policy snap-in extensions, see "Extensions to the Group Policy Snap-in" later in this chapter.

For more information about Microsoft Management Console and Group Policy, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Configuring Group Policy

To use Group Policy, you need to know the features of the Group Policy user interface and their roles in configuring Group Policy.

Group Policy Snap-in Namespace

The root node of the Group Policy snap-in displays as the name of the Group Policy object and the domain in which it is stored, in the following format:

<Group Policy object name> [*<server name>*] Policy

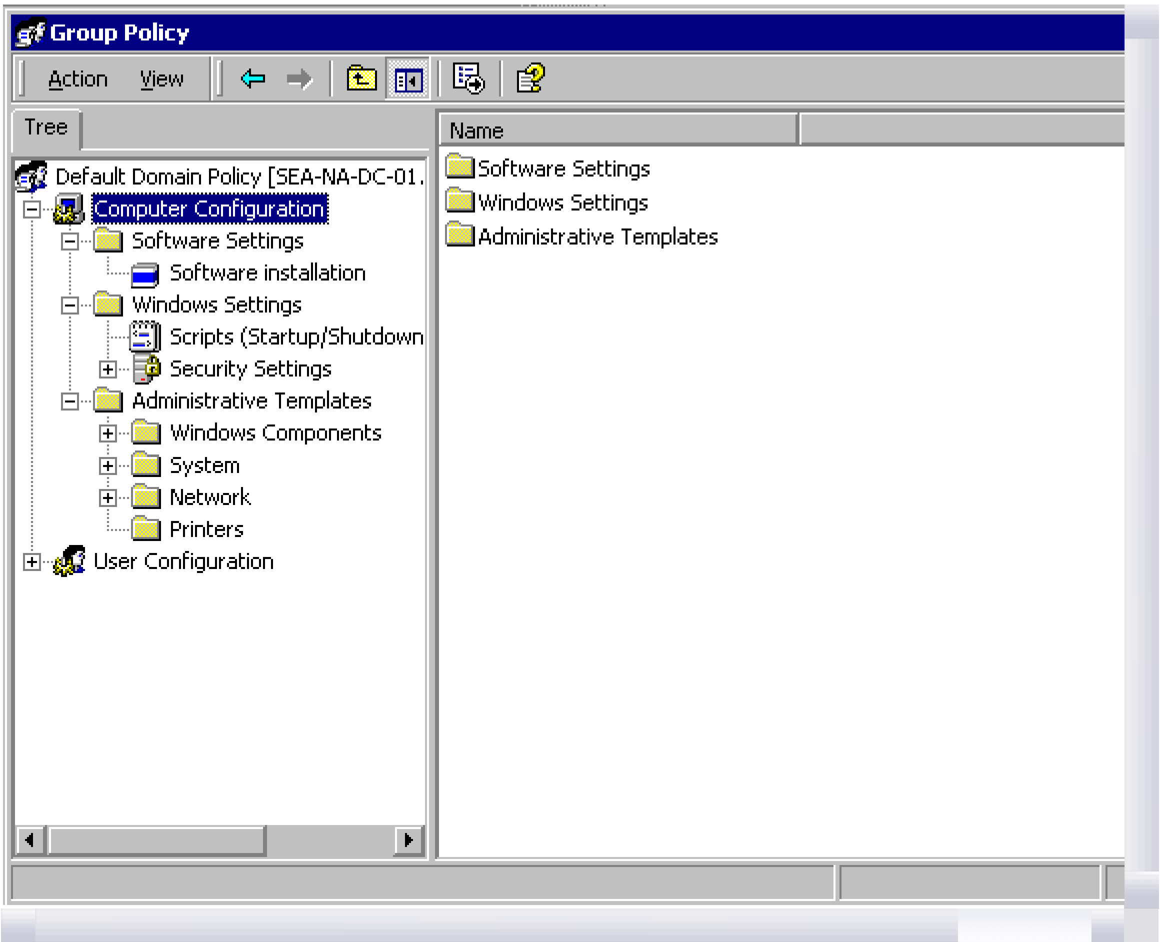
For example:

Default Domain Policy [MSMSRV01.Reskit.com] Policy

The next level of the namespace has two nodes: Computer Configuration and User Configuration. These are the parent folders that you use to configure specific desktop environments and to enforce Group Policy on groups of computers and users, respectively, on the network.

Computer Configuration

Computer configuration includes all computer-related policy settings that specify operating system behavior, desktop behavior, security settings, computer startup and shutdown scripts, computer-assigned application options, and application settings. Computer-related Group Policy is applied when the operating system initializes and during the periodic refresh cycle, explained later in this document. In general, computer policy takes precedence over conflicting user policy. Figure 22.1 shows the Group Policy Snap-in Console Computer Configuration.

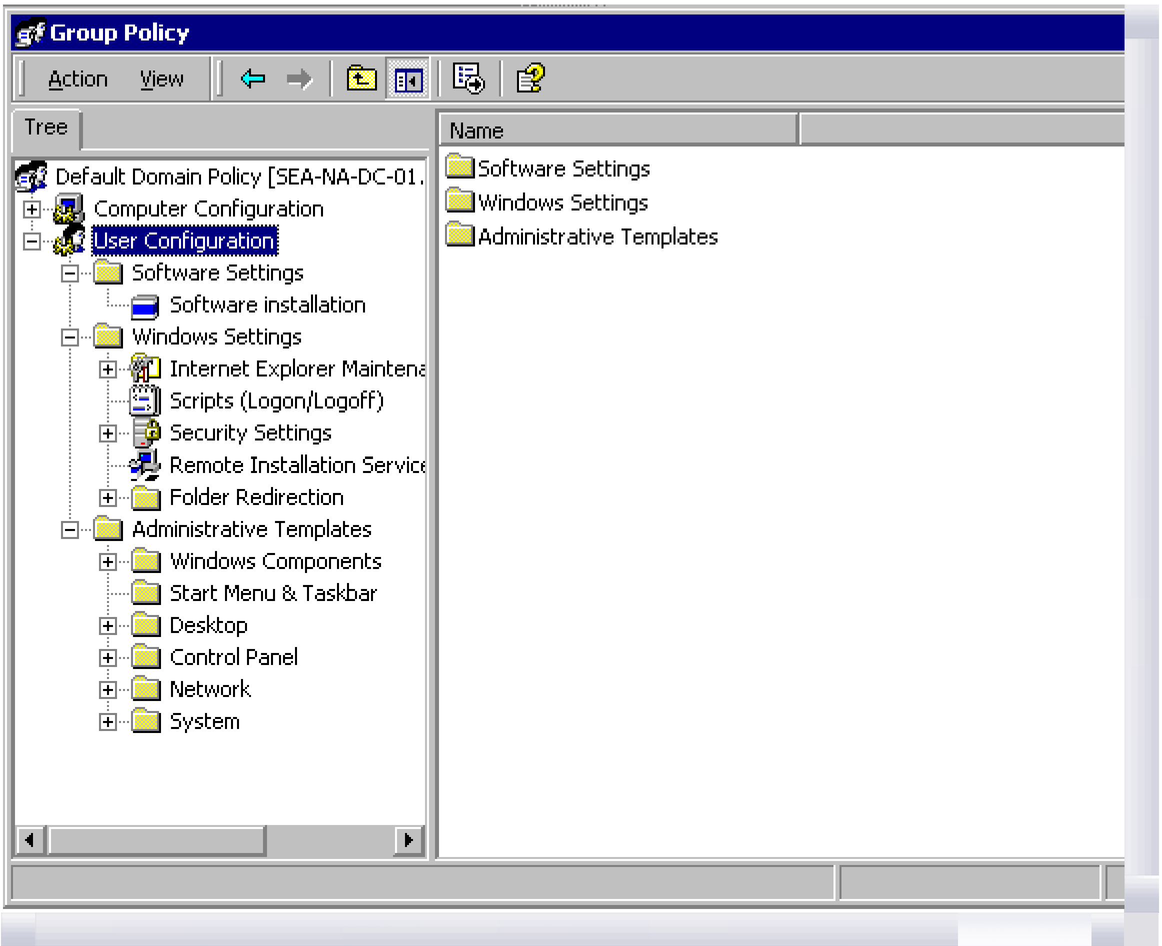


If your browser does not support inline frames, click here to view on a separate page.

Figure 22.1 The Group Policy Snap-in Console Computer Configuration

User Configuration

User configuration includes all user-related policy settings that specify operating system behavior, desktop settings, security settings, assigned and published application options, application settings, folder redirection options, and user logon and logoff scripts. User-related Group Policy is applied when users log on to the computer and during the periodic refresh cycle. Figure 22.2 shows the Group Policy Snap-in Console User Configuration.



If your browser does not support inline frames, click here to view on a separate page.

Figure 22.2 The Group Policy Snap-in Console User Configuration

In certain strictly managed computing environments, it is useful to mandate a specific desktop configuration regardless of which user logs on to the computer. Schools, libraries, public kiosks, some laboratories, and reception areas are candidates for policy of this sort. You implement this by appending (or, more severely, replacing) the User Configuration settings for the user account with the User Configuration settings for the computer account. This process is called loopback and it is explained in "Group Policy Loopback Support" later in this chapter.

There are several child nodes under the Computer Configuration and User Configuration parent nodes. These include:

- Software Settings, which is a location for independent software vendors (ISVs) to add further extensions. If no nodes have been added by ISVs, then Software Settings contains just the Software Installation extension included with Windows 2000.
- Windows Settings, which holds extensions provided by Microsoft.
- Administrative Templates, which shows namespace for registry-based policy settings. The Administrative Templates namespace is created by adding .adm files. You do this by right-clicking either of the Administrative Templates nodes, and then clicking "Add/Remove Templates."

Extensions to the Group Policy Snap-in

A Group Policy snap-in extension can extend the Group Policy namespace under the User Configuration or Computer Configuration nodes, or both. Most of the snap-in extensions extend both of these nodes, but frequently with different options. The Group Policy snap-in extensions included with Windows 2000 are listed below.

Administrative Templates These include registry-based Group Policy, which you use to mandate registry settings that govern the behavior and appearance of the desktop, including the operating system components and applications. There are over 450 of these settings available for you to configure, and you can add more using .adm files. To avoid undesirably persistent registry settings, any additional registry settings should be placed in \Software\Policies or \Software\Microsoft\Windows\CurrentVersion\Policies. See Group Policy Overview in this chapter about undesirably persistent registry settings.

Security Settings You use the Security Settings extension to set security options for computers and users within the scope of a Group Policy object. You can define local computer, domain, and network security settings.

Software Installation You use the Software Installation snap-in to centrally manage software in your organization. You can assign and publish software to users, and assign (but not publish) software to computers. You use Software Installation to install applications. The target computer needs to have the Windows 2000 operating system in place, as well as the client-side extension for Software Installation, Appmgmts.dll. To install Windows 2000 on a remote computer, use Remote Installation Services.

Scripts You can use scripts to automate computer startup and shutdown and user logon and logoff sessions. You can use any Windows Script Host–supported language you like. Your options include Microsoft® Visual Basic® Scripting Edition (VBScript), JavaScript, Perl, and MS-DOS®-style batch files (.bat and .cmd).

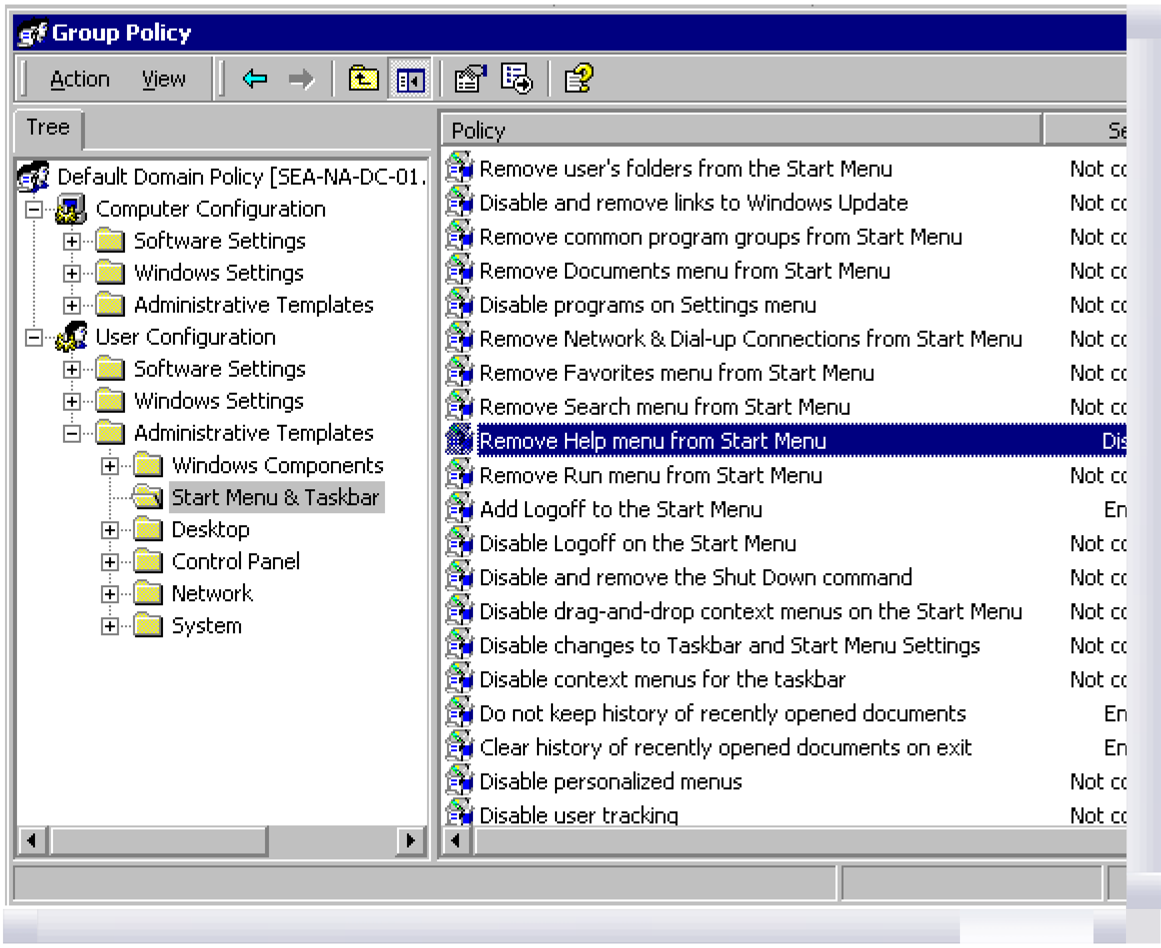
Remote Installation Services You use Remote Installation Services (RIS) to control the behavior of the Remote Operating System Installation feature as displayed to client computers. Group Policy requires a genuine Windows 2000 client, not merely a client of Active Directory running on a previous version of Windows.

Internet Explorer Maintenance You use Internet Explorer Maintenance to administer and customize Microsoft® Internet Explorer on Windows 2000–based computers.

Folder Redirection You use Folder Redirection to redirect Windows 2000 special folders from their default user profile location to an alternate location on the network, where you can centrally manage them. Windows 2000 special folders include My Documents, Application Data, Desktop, and **Start** Menu.

Administrative Templates

In Windows 2000, the Administrative Templates node of the Group Policy snap-in uses an administrative template (.adm) file to specify the registry settings you can modify through the Group Policy snap-in user interface Policy Group Policy object. Figure 22.3 shows some Administrative Template Group Policy settings. The Policy pane lists some policy settings that make up the User Configuration part of the Default Domain Policy of the Group Policy object.



Policy	Se
Remove user's folders from the Start Menu	Not cc
Disable and remove links to Windows Update	Not cc
Remove common program groups from Start Menu	Not cc
Remove Documents menu from Start Menu	Not cc
Disable programs on Settings menu	Not cc
Remove Network & Dial-up Connections from Start Menu	Not cc
Remove Favorites menu from Start Menu	Not cc
Remove Search menu from Start Menu	Not cc
Remove Help menu from Start Menu	Dis
Remove Run menu from Start Menu	Not cc
Add Logoff to the Start Menu	En
Disable Logoff on the Start Menu	Not cc
Disable and remove the Shut Down command	Not cc
Disable drag-and-drop context menus on the Start Menu	Not cc
Disable changes to Taskbar and Start Menu Settings	Not cc
Disable context menus for the taskbar	Not cc
Do not keep history of recently opened documents	En
Clear history of recently opened documents on exit	En
Disable personalized menus	Not cc
Disable user tracking	Not cc

If your browser does not support inline frames, click here to view on a separate page.

Figure 22.3 Administrative Template Group Policy Settings

Note The Windows NT 4.0 System Policy Editor uses files called administrative templates (.adm files) to determine which registry settings you can modify by presenting a namespace for those settings in the System Policy Editor. Windows 2000 .adm files have new features, such as Explain text. The Windows 2000 Resource Kit CD-ROM includes a searchable reference file, GP.chm, with details about the administrative templates settings included with Windows 2000 Server.

The Administrative Templates nodes of the Group Policy snap-in present registry-based Group Policy settings to the administrator. Administrative Templates govern a variety of behaviors for the Windows 2000 operating system and its components and applications. These settings are written to the HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE portion of the registry database, as appropriate.

The .adm file is a Unicode text file that specifies a hierarchy of categories and subcategories that together define how the options are displayed through the Group Policy snap-in user interface. Unicode support for .adm files is new in Windows 2000. It also indicates the registry locations where you need to make changes if a particular selection is made, specifies any options or restrictions in values that are associated with the selection, and in some cases, specifies a default value to use if a selection is activated. By default, three .adm files, System.adm, Inetres.adm, and Conf.adm, which together contain more than 450 settings appropriate to Windows 2000 operating system clients, are installed in the Group Policy console. Inetres.adm contains settings for Internet Explorer, and System.adm has a wide variety of settings. There is also a Conf.adm, containing Microsoft® NetMeeting® settings, which is not loaded by default.

Note See the **Explain** tab of each Group Policy setting's **Properties** page for more details on the policy settings within the .adm file.

The Administrative Templates nodes of the Group Policy snap-in can be extended by using custom .adm files. For more information about creating .adm files, see Windows 2000 Help.

Undesirably Persistent Registry Settings

Windows NT 4.0 registry settings remain in effect until they are explicitly reversed. Windows 2000 registry settings, by contrast, are removed and rewritten each time policy changes. Be aware of this possibly undesirable behavior if you consider using Windows NT 4.0–type registry settings on Windows 2000–based computers.

For more information, see "Using Windows NT 4.0 Administrative Templates in the Windows 2000 Group Policy Console" later in this chapter.

Other Group Policy Extensions That Use the Registry

Both Remote Installation Services (RIS) and Disk Quotas use the registry. RIS has a node in the Group Policy console, but no client-side extension; that is, no .dll on the client computer. This is not surprising, because the client typically won't have an operating system. Disk Quotas is an example of a component with a client-side extension (Dskquota.dll), but no node in the Group Policy console.

Remote Installation Services

Remote Installation Services (RIS) is an optional component included in the Windows 2000 Server operating system. You can use the RIS extension of Group Policy to control which screen options (such as Automatic Setup, Custom Setup, and Restart Setup) are available to users during the client installation wizard.

When a client computer enabled with Preboot Execution Environment (PXE) remote-boot technology accesses the remote installation server to install the operating system, the Remote Installation Services server checks for Group Policy pertaining to remote installation options defined for the user. The Boot Information Negotiation Layer (BINL) service running on the RIS server performs this work. It impersonates the user who logs on to the RIS client-side pre-boot user interface, and evaluates the Group Policy objects to calculate the resulting policy. Based on the resulting policy, it determines which screens are sent to the pre-boot RIS client code for display to the user.

RIS policies are stored in the Sysvol folder at the following location: Policies\{<*GUID of GPO*>}\User\Microsoft\RemoteInstall\oscfilter.ini. For detailed information about Remote Installation Services, see "Remote OS Installation" in this book.

Security Settings

You can define a security configuration within a Group Policy object. A security configuration consists of settings applied to one or more security areas supported on Windows 2000 Professional or Windows 2000 Server. The specified security configuration is then applied to computers as part of Group Policy enforcement.

The Security Settings extension of the Group Policy snap-in complements existing system security tools such as the **Security** tab on the **Properties** page (of an object, file, folder, and so on), and **Local Users and Groups** in **Computer Management**. You can continue to use existing tools to change specific settings whenever necessary.

The security areas that can be configured for computers include:

Account Policies These are computer security settings for password policy, lockout policy, and Kerberos policy in Windows 2000 domains.

Note These settings are only set at the domain level. If they are set at the organizational unit level, they are ignored.

Local Policies These include security settings for audit policy (Audit successful or failed logon attempts), user rights (who has network access to the computer) assignment, and security options (the ability to connect to a computer anonymously).

Event Log This controls settings such as size and retention method for the Application, Security, and System event logs. You can access these logs using Event Viewer.

Restricted Groups Allows you to control who needs to and who does not need to belong to security sensitive groups, as well as which other groups a security sensitive group needs to belong to. This allows administrators to enforce a membership policy regarding sensitive groups, such as Enterprise Administrators or Payroll. For example, it might be decided that only two users should be members of the Enterprise Administrators group. You can define the Enterprise Administrators group as a restricted group that contains only those two members. If a third user is added to the group (for example, to accomplish some task in an emergency situation), that user is automatically removed from the Enterprise Administrators group the next time policy is enforced. This mechanism can also be used to enforce group memberships on workstations in the domain (that is, enforcing that certain administrators from the domain are in the local Administrators groups on workstations).

System Services These control startup mode and access permissions for system services, such as who is allowed to stop and start the fax service.

Registry This is used to configure security settings for registry keys, including access control, audit, and ownership.

File System This is used to configure security settings for file-system objects, including access control, audit, and ownership.

Incremental Security Templates

Windows 2000 includes several incremental security templates. By default, these templates are stored in %systemroot%\Security\Templates. These predefined templates can be customized using the Security Templates MMC snap-in and can be imported into the Security Settings extension of the Group Policy snap-in.

These security templates are to be applied to Windows 2000–based computers that are configured with the Windows 2000 default security settings. They modify the default security settings incrementally, not cumulatively.

Note You should not apply these incremental templates to Windows 2000 systems that have been upgraded from Windows NT 4.0.

You should only apply these incremental templates onto Windows 2000 systems that have been clean-installed onto NTFS partitions. For NTFS computers that have been upgraded from Windows NT 4.0 or earlier, a Basic security template can be applied to configure the upgraded computer with the Windows 2000 default security settings. This is described in the following section. You cannot secure Windows 2000 systems that are installed on FAT file systems.

Security Configurations

Security configurations provide preconfigured sets of security settings that you can apply. You can configure them to Compatible, Secure, or High Secure Settings.

Compatible

The compatible template is provided in case you do not want to risk making end users into Power Users so that they can run older applications. This works on workstations and servers, and the template is called Compatws.inf.

Using this template, normal users — that is non-administrator and non-Power Users — cannot run most older applications on Windows 2000. This is because the default permissions granted to normal users are secure and most applications need to be rewritten to function properly in this environment. Applications that are Certified For Windows 2000 can be run successfully by a normal user. The Compatible configuration liberalizes the default permissions for the Users group so that older applications are more likely to run. Microsoft® Office 97 should run successfully when users are logged on as a User to a Windows 2000–based computer that has had the Compatible security template applied over the default settings. This is not considered a secure environment.

Secure

The Secure configuration provides increased security for areas of the operating system that are not secured by the default access control permissions. This works on workstations, servers, and domain controllers, and the templates are called Securews.inf and Securedc.inf

This configuration includes increased security settings for Account Policy, Auditing, and some well-known security-relevant registry keys. Access control lists are not modified by the secure configuration because this configuration assumes that default Windows 2000 security settings are in effect, and that users are members of the Users group. The Secure configuration removes all members of the Power Users group to enforce this assumption.

High Secure

The High Secure configuration provides increased security over the secure configuration. This works on workstations, servers, and domain controllers, and the templates are called Hisecws.inf and Hisecdc.inf.

The High Secure configuration requires that all network communications be digitally signed and encrypted. Because of these requirements, Windows 2000–based computers configured with the High Secure template might not be able to communicate with previous version clients such as Microsoft® Windows 98®–based (or earlier) computers that do not support the same network communication protections. The High Secure configuration also grants Power Users the same access to file system and registry keys as normal users. This allows users running Certified For Windows 2000 applications to offer inherent Power User capabilities such as the ability to create shares and change the system time without giving those same Power Users the lax permissions necessary to run noncertified applications. The High Secure template, when applied to servers, removes the Terminal Server user from all file system and registry ACLs, thus ensuring that users logging on to Terminal Server environments are also subject to the same secure access control policy as normal users.

Windows 2000 Default Security Templates

As noted earlier, the security templates described above (Compatible, Secure, and High Secure) incrementally modify the default Windows 2000 security settings that exist when Windows 2000 is clean-installed onto an NTFS partition. If you would like to apply these defaults to upgraded computers, or to clean-installed computers that have been subsequently modified, the following templates can be used:

- Basicwk.inf — applies default settings for Windows 2000 Professional–based computers for all areas except User Rights and Group Membership.
- Basicsv.inf — applies default settings for Windows 2000 Server–based computers for all areas except User Rights and Group Membership.
- Basicdc.inf — applies default settings for Windows 2000 Domain Controllers for all areas except User Rights and Group Membership. User Rights and Group Memberships are not modified by the basic templates because these templates are most often used for undoing file system or registry ACL changes, or to apply the default Windows 2000 ACLs to computers which have been upgraded from Windows NT 4.0. In these cases, customers usually want to maintain the existing User Rights and Group Memberships.

Software Installation

You can use the Software Installation snap-in to centrally manage software distribution in your organization. You can assign and publish software for groups of users, and you can assign software for groups of computers.

You assign applications to groups of users so that all users who require the applications have them on their desktops, without you or other technical personnel having to install the application on each desktop. When you assign an application to a group of users, you can be sure it is always available to them. When users log on to Windows 2000, the application shortcut appears on the **Start** menu, and the registry is updated with information about the application, including the location of the application package and the location of the source files for the installation. With this "advertisement" information about users' computers, the application is installed the first time users activate the application. When users select the application from the **Start** menu the first time, it installs and then opens. Users can remove assigned applications using Add/Remove Programs in Control Panel, but only for the duration of a logon session. The next time they start their computer, the application icon reappears.

You can also publish applications to groups of users, making the application available for users to install if they choose to do so. When you publish an application, no shortcuts to the application appear on users' desktops, and no local registry entries are made. That is, the application has no presence on the user's desktop. Information needed to published applications is stored in the Group Policy object.

To install a published application, users can use the Add/Remove Programs in Control Panel, which includes a list of all published applications that are available for them to use. Or, users can open a document file associated with a published application (for example, an .xls file to install Microsoft® Excel).

Scripts

Previously, the only native scripting language supported by the Windows operating system was the MS-DOS command language. In Windows 2000 this is expanded to include the Microsoft® ActiveX® scripting architecture. Windows 2000 includes Windows Script Host (WSH), a language-independent scripting host for 32-bit Windows platforms. WSH has low memory requirements and serves as a controller of ActiveX scripting engines. With WSH, you can run scripts directly in Windows 2000 by double-clicking a script file, or by typing the name of a script file at the command prompt. You can use any WSH scripting tool including VBScript programming system and Microsoft® JScript® programming system to create scripts. Independent software vendors provide WSH support for other popular scripting languages. You can use Windows Script Host to run .vbs and .js scripts directly on the Windows desktop or command console, without the need to embed the scripts in an HTML document. MS-DOS-type batch files (with .bat and .cmd extensions) also function using Windows 2000.

The Scripts node located under Computer Configuration allows you to specify startup and shutdown scripts, and to specify logon and logoff scripts.

In Windows 2000 the following five script types are supported:

- Legacy Logon scripts
- Group Policy Logon scripts
- Group Policy Logoff scripts
- Group Policy Startup scripts
- Group Policy Shutdown scripts

Table 22.1 shows some Group Policy settings that control how scripts are run.

Table 22.1 Group Policy Settings That Control Scripts

Location	Group Policy settings
Computer Configuration/Administrative Templates/System/Logon/	Run Logon Scripts Synchronously Run Startup Scripts Asynchronously Run Shutdown Scripts Visible Run Startup Scripts Visible
User Configuration/Administrative Templates/System/Logon/Logoff	Run Logon Scripts Synchronously Run Legacy Logon Scripts Hidden Run Logon Scripts Visible Run Logoff Scripts Visible

Scripts can cause the system to appear hung if an errant script (one that prompts the user for input) runs hidden. This occurs because the default wait time is 600 seconds. You can change this default using Group Policy. The setting is in the following location: Computer Configuration\Administrative Templates\System\Logon\Maximum wait time for Group Policy scripts.

If you run scripts in a minimized window, you can stop the scripts processing by normalizing the window.

You can also use the **Disable the Command Prompt** setting found under User Configuration\Administrative Templates\System. This prevents batch files from running (files with .cmd and .bat extensions). This optional setting should not be used for Terminal Services clients, because it prevents the Application Compatibility scripts from running. See Windows Explain text for details.

Legacy logon scripts are those scripts specified in the User object. You need to carefully consider these scripts if you have a mixed environment that includes Windows NT 4.0, Microsoft® Windows® 95, Windows 98, and Windows 2000 clients. The Windows 2000 and the Windows 98 clients properly run .vbs and .js scripts. However, to run .vbs and .js scripts on Windows NT 4.0 and Windows 95 clients, you need to embed the scripts in batch (.bat) files. The scripts continue to run in a normal window. Alternatively, you can install Windows Script Host to run unembedded scripts on Windows NT 4.0 and Windows 95 clients. The names of scripts and their command lines are stored in a .pol file in the form of registry keys and values.

For more information about Windows Script Host, see the Windows Script Technologies link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Folder Redirection

You use the Folder Redirection extension to redirect any of the following special folders in a user profile to an alternate location (such as a network share):

- Application Data
- Desktop
- My Documents
  - My Pictures
- Start Menu

You can redirect a user's My Documents folder to \\<*server name*>\<*share name*>\%username% and provide them with the following advantages:

- You can ensure that a user's documents are available when they roam from one computer to another, with or without roaming user profiles.
- When using roaming user profiles, you can reduce the time it takes to log on to and log off from the network. In Windows NT 4.0, the My Documents folder is part of the Roaming User Profile. This means that the My Documents folder and its contents are copied back and forth between the client computer and the server when the user logs on and logs off. By moving the My Documents folder out of the user profile, you can expedite user logon and logoff.
- You can store user data on the network rather than on the local computer, which allows you to manage and protect it.
- You can make a user's network-based folders available to them when they are disconnected from the corporate network by using Offline Folder technologies.

Analogous advantages apply to any redirected folder, not to only the My Documents folder. Redirecting to a DFS share provides a degree of safety in case of server failure. For more information about using offline folders, see "Remote OS Installation" in this book.

Extending the Group Policy Snap-in

Third-party application developers can extend the Group Policy snap-in to provide Group Policy specific to their applications. For this purpose, they can:

- Create an administrative template (.adm file). For more information, see Windows 2000 Help.
- Create a Group Policy MMC snap-in extension and provide the user interface for setting Group Policy specific to their application. For storing and distributing the policy, the following mechanisms are recommended:
  - The easiest is to use the API specific to the Group Policy MMC snap-in to write registry-based Group Policy to the Group Policy template. For more information about writing registry-based Group Policy to the Group Policy template, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
  - Use the **GetFileSysPath** function to store non-registry-based (file-based) policy information in a Group Policy template subfolder. You should use the <*company name*>\<*application name*>\<*version*> naming convention for this folder. Then place the required files in that Group Policy template subfolder. On the client side, Winlogon calls the client-side extension for the tool. This in turn processes the information stored in the directory in the Group Policy template. The application developer must use this mechanism appropriately. By storing the data in a Group Policy template subfolder, the application capitalizes on the built-in mechanisms of Group Policy (the Group Policy template and Winlogon) for applying special non-registry-based policy. For more information about the GetFile SysPath function, see the SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
  - You can store data in the Group Policy container. It is strongly recommended to use either the Group Policy container or the Group Policy template, not both.

Client-side Extensions to Group Policy

Most of the Group Policy snap-in extensions also include client-side extensions. These extensions are dynamic-link libraries (DLLs) that are responsible for implementing Group Policy at the client computers.

There are some client-side extensions, such as Disk Quotas, that don't correspond to a snap-in. For more information about the client-side extensions, see "Computer Policy for Client-Side Extensions" later in this chapter.

For information about Microsoft Management Console, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Group Policy Storage

There are two kinds of Group Policy objects: local and non-local. Only one local Group Policy object is stored on each Windows 2000–based computer. Non-local Group Policy objects are Active Directory–based.

Non-Local, Active Directory–Based Storage

Non-local Group Policy objects store Group Policy information in two locations: a Group Policy container and a Group Policy template. They are named with a globally unique identifier (GUID), which is used to keep them synchronized.

Figure 22.4 shows data storage locations which are typically contained in a Group Policy object.

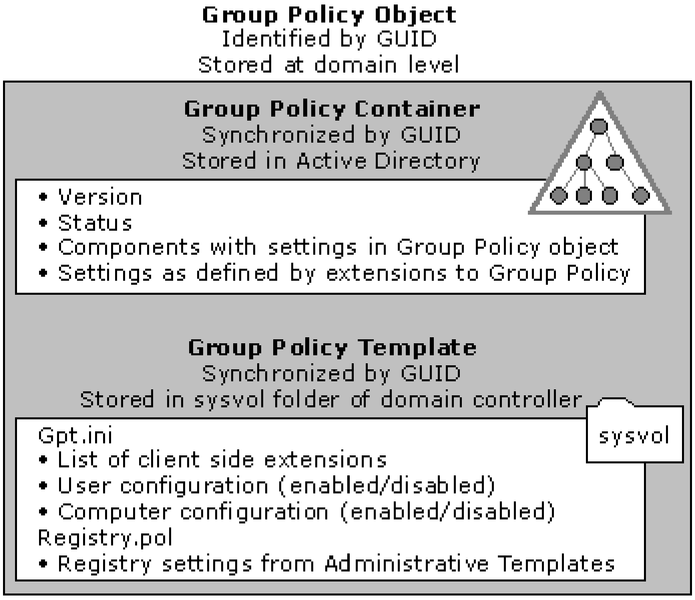

Group Policy Object
Identified by GUID
Stored at domain level
Group Policy Container
Synchronized by GUID
Stored in Active Directory
• Version
• Status
• Components with settings in Group Policy object
• Settings as defined by extensions to Group Policy
Group Policy Template
Synchronized by GUID
Stored in sysvol folder of domain controller
sysvol
Gpt.ini
• List of client side extensions
• User configuration (enabled/disabled)
• Computer configuration (enabled/disabled)
Registry.pol
• Registry settings from Administrative Templates

Figure 22.4 Group Policy Storage Model

Note This information about storage implementation is purely informational. As an administrator you don't interact with the Group Policy template and the Group Policy container directly, but through Active Directory tools such as the Group Policy console.

Group Policy Container

The Group Policy container is an Active Directory storage area for Group Policy object properties; it includes both computer and user Group Policy information. The Group Policy container has the following properties:

- Version information. This makes sure that the information is synchronized with the Group Policy template information.
- Status information. This indicates whether the Group Policy object is enabled or disabled.
- List of components (extensions) that have settings in the Group Policy object.
- Policy settings as defined by the extension snap-ins:

For example, the Group Policy container stores information used by the Software Installation snap-in to describe the status of the software available for installation. This data repository contains data for all applications, interfaces, and APIs that provide for application publishing and assigning.

Group Policy Template

Group Policy objects also store Group Policy information in a folder structure called the Group Policy template that is located in the System Volume folder of domain controllers (Sysvol) in the \Policies subfolder. The Group Policy template is the container where Administrative Template–based policy settings, Security Settings, applications available for Software Installation, and script files are stored.

When you modify a Group Policy object, the directory name given to the Group Policy template is the GUID of the Group Policy object that you modify. For example, a Group Policy template folder might be named as shown in the following example:

%systemroot%\sysvol\SYSVOL\www.Reskit.com\Policies\{47636445-af79-11d0-91fe-080036644603}

A Group Policy snap-in can store data outside the Group Policy object; however, this requires that at least a link to the Group Policy object be stored either in a Group Policy container (Active Directory data store) or in a Group Policy template (file-type data stored on the Sysvol folder).

Note Group Policy is not backed up separately from the rest of Active Directory. To back up Active Directory, you need to be a member of Backup Operators group. The required privilege is **Backup Files and Directories**. For instructions on backing up Active Directory, see "Active Directory Backup and Restore" in this book.

Gpt.ini File

At the root of each Group Policy template folder is a file called Gpt.ini. For local Group Policy objects, the Gpt.ini file stores information indicating:

- Which client-side extensions of the Group Policy snap-in contain User or Computer data in the Group Policy object.
- Whether the User or Computer portion is disabled.

- Version number of the Group Policy snap-in extension that created the Group Policy object.

Local Group Policy Objects

A local Group Policy object exists on every computer, and by default only nodes under Security Settings are configured. Settings in other parts of the local Group Policy object's namespace are not enabled or disabled. The local Group Policy object is stored in %systemroot%\System32\GroupPolicy, and it has the following permissions set through discretionary access control lists (DACLs):

- Administrators: full control
- Operating system: full control
- User: read

If Read permission is withdrawn from the Local Administrator group, Group Policy does not apply. This is a convenient way to exempt Local Administrators from a group Policy object even though they have the Apply Group Policy permissions set to **Allow**.

The local Group Policy object Gpt.ini file contains the following information:

GPCUserExtensionNames This Includes a list of GUIDs that tells the client side engine which client-side extensions have User data in the Group Policy object. The format is: [{<*GUID of client-side extension*>}{<*GUID of MMC extension*>}{<*GUID of second MMC extension if appropriate*>}][repeat first section as appropriate].

GPCMachineExtensionNames This includes a list of GUIDs that tells the client-side engine which client-side extensions have Computer data in the Group Policy object.

Options This refers to Group Policy object options such as User portion disabled or Computer portion disabled.

GPCFunctionalityVersion This is the version number of the Group Policy extension tool that created the Group Policy object.

Group Policy Template Subfolders

The Group Policy template folder contains a tree of subfolders. The number of subfolders that are present in the tree depends on the Group Policy object; however, at least two subfolders are always present. They are Machine and User. The following is a description of each folder:

Machine Includes a Registry.pol file that contains the registry settings that are applied to computers. When a computer initializes, this Registry.pol file is downloaded and applied to the **HKEY_LOCAL_MACHINE** portion of the registry.

User Includes a Registry.pol file that contains the registry settings that are applied to users. When a user logs on to a computer, this Registry.pol file is downloaded and applied to the **HKEY_CURRENT_USER** portion of the registry.

The Group Policy template folder also includes a Gpt.ini file which contains version information. For Active Directory–based Group Policy objects, this file contains the version number of the Group Policy object in a line of this form:

```
Version=<version number>
```

The version number is the decimal representation of an eight-digit hexadecimal number (a DWORD). The four least significant digits represent the Computer Settings version number, and the four most significant digits represent the User Settings version number. For example, if you see

```
Version=65539
```

then the Computer Settings version is 3, and the User Settings version is 1, because 65539 converted to hexadecimal is 0X00010003.

The Group Policy template folder can also include the following subfolders:

Adm Contains all of the .adm files for this Group Policy object.

Machine\Scripts\Shutdown Contains scripts that run when the computer shuts down.

Machine\Scripts\Startup Contains scripts that run when the computer starts.

Machine\Applications The contents depends on what applications are computer-assigned with a given Group Policy object.

Machine\Microsoft\Windows NT\Secedit Contains GptTmpl.inf, the default security configuration settings for a Windows 2000 domain controller.

User\Applications Contains the advertisement files (.aas files) used by the Windows installer.

User\Documents & Settings Contains Fdeploy.ini, which holds information about the Folder Redirection status of the current user's special folders.

User\Microsoft\RemoteInstall Contains OSCfilter.ini, which holds user choices for operating system installation through Remote Installation Services.

User\Microsoft\IEAK Contains settings for the Internet Explorer Maintenance Snap-in.

User\Scripts\Logoff Contains scripts that are run when the user logs off the computer.

User\Scripts\Logon Scripts to be run when the user logs on to the computer.

Note The User and Machine folders are created during installation, and other folders are created as needed when policy is set.

Registry.pol Files

The Administrative Templates extension of Group Policy saves information in the Group Policy template in text files with the name Registry.pol. These files contain the customized registry settings that are applied to the Machine or User portion of the registry which you specify using the Group Policy snap-in. The Windows 2000 Registry.pol file is analogous to the Windows 95 or Windows 98 Config.pol file and the Windows NT 4.0 NT Config.pol file.

Two Registry.pol files are created and stored in the Group Policy template, one for Computer Configuration, which is stored in the \Machine subdirectory, and one for User Configuration, which is stored in the \User subdirectory.

Note The format of the .pol files in the Group Policy template differs from that of the .pol files in previous versions of Windows.

The .pol files created by Windows NT 4.0 and Windows 95 can be applied only to the operating system on which they were created. The .pol file produced by the Windows NT 4.0 System Policy Editor was a binary file, whereas the Registry.pol file produced by Administrative Templates node of the Group Policy snap-in is a text file with embedded binary strings.

To view .pol files without applying them to the registry, use the Regview.exe tool located on the *Microsoft® Windows® 2000 Server Resource Kit* companion CD.

For additional information about Registry.pol files, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Group Policy Object Links

Group Policy objects are actually applied to a site, domain, or organizational unit by using a link. A non-local Group Policy object that is not linked to a site, domain, or organizational unit has no effect on any user or computer anywhere, even in the storage domain.

No Override as Compared to Block Policy Inheritance

You can set **No Override** on a specific Group Policy object link so that Group Policy objects linked at a lower-level of Active Directory — closer to the recipient user or computer account — cannot override that policy. If you do this, Group Policy objects linked at the same level, but not as **No Override**, are also prevented from overriding. If you have several links set to **No Override**, at the same level of Active Directory, then you need to prioritize them. Links higher in the list have priority on all Configured (that is, **Enabled** or **Disabled**) settings.

If you have linked a specific Group Policy object to a domain, and set the Group Policy object link to **No Override**, then the configured Group Policy settings that the Group Policy object contains apply to all organizational units under that domain. Group Policy objects linked to organizational units cannot override that domain-linked Group Policy object.

You can also block inheritance of Group Policy from above in Active Directory. This is done by checking **Block Policy inheritance** on the **Group Policy** tab of the **Properties** sheet of the domain or organizational unit. This option does not exist for a site.

Some important facts about **No Override** and Block Policy are listed below:

- **No Override** is set on a link, not on a site, domain, organizational unit, or Group Policy object.
- **Block Policy Inheritance** is set on a domain or organizational unit, and therefore applies to all Group Policy objects linked at that level or higher in Active Directory which can be overridden.
- **No Override** takes precedence over **Block Policy Inheritance** if the two are in conflict.

If you want to see what a Group Policy object is linked to, open it in the **Group Policy console**, right-click the root node, click **Properties**, and then click the **Links** tab. Click **Find Now** after setting the domain on the drop-down menu.

Multiple Group Policy Objects

Each non-local Group Policy object is stored in a specific domain, which we can call the storage domain. The storage domain should not be confused with a domain to which the Group Policy object is linked.

You can link multiple Group Policy objects to a single site, domain, or organizational unit. However, many sites, domains, and organizational units, can all obtain policy from a single Group Policy object by way of links to it, regardless of which domain the Group Policy object is stored in.

A Group Policy object can be linked to its storage domain, and if network connections to other domains are slow this is desirable. However, it doesn't have to be linked to its storage domain.

It is also possible to link a single Group Policy object more than once to a single site, domain, or organizational unit, though it is seldom useful to do so.

For performance reasons, it is best to avoid linking to a Group Policy object in a different domain.

Cross-Domain Editing of a Group Policy Object

Before you can edit a Group Policy object, the following two conditions must be met:

- You have Read/write permissions (or Full Control) of the Group Policy object.
- You are either logged on to the storage domain of the Group Policy object, or logged on to a domain that is trusted by the storage domain.

Using Security Groups to Filter and Delegate Group Policy

You use security groups in Group Policy for two purposes:

- To filter the scope of a Group Policy object
- To delegate control of Group Policy

Filtering the Scope of a Group Policy Object

You can refine which groups of computers and users a particular Group Policy object influences by using Windows 2000 security groups. To do this, use the **Security** tab on the **Properties** page of the Group Policy object.

Filtering affects the Group Policy object as a whole. That is, you cannot use security groups to apply (or prevent from applying) only some of the settings in a Group Policy object. However, this is not true in the cases of Folder Redirection and Software Installation, which have further ACLs set at the Group Policy object level to further refine behavior based on security group membership.

Setting Security Permissions for Receiving Group Policy

A discretionary access control list (DACL) is a list of permissions (such as Read, Apply Group Policy, and Full Control) on a Group Policy object or other object. You use the DACL on a Group Policy object to allow or deny access to the Group Policy object by users and computers according to their membership in security groups.

To use the **Security** tab on the **Properties** page for a Group Policy object, right-click the root node of the Group Policy snap-in, click **Properties**, and then click **Security**.

An alternative is to open the **Properties** page of a given site, domain, or organizational unit, then select the **Group Policy** tab, right-click a **Group Policy object** in the Group Policy object list, select **Properties**, and then click the **Security** tab. Group Policy objects that you can access this way are linked to the site, domain, or organizational unit.

You can specify which groups of users and computers have Apply Group Policy access control entries (ACEs) set to enable access to the Group Policy object. ACEs are permission entries within a discretionary access control list (DACL). Groups that have Apply Group Policy and Read access to the Group Policy object receive the configured Group Policy settings contained in it if they are subject to the Group Policy object through Active Directory. By default, authenticated users have both Apply Group Policy and Read permissions, but not Write or Full Control. This means that by default, users cannot modify the information in the Group Policy object. By default, domain administrators, enterprise administrators, and the local system have Full Control, without Apply Group Policy. By default, administrators are also authenticated users, which means that they also have the Apply Group Policy attribute set. For more information, see "Editing Group Policy Objects" later in this chapter.

Note It is recommended that you remove Read permission from groups whose members don't need to receive policy and contain users who are not administrators because this data can be viewed by any users with Read permission. Group Policy processes faster if both the Read and Apply Group Policy settings are disabled when the Apply Group Policy setting is not needed. In addition, Group Policy fails if a user has Read access to more than 1,000 Group Policy objects stored in one domain. For more information about Group Policy failing when more than 1,000 Group Policy objects are present, see "Troubleshooting Change and Configuration Management" in this book.

Network administrators (members of the Enterprise Administrators or Domain Administrators group) can also use the **Security** tab on the Group Policy object **Properties** page to determine which administrator groups can modify policy settings in Group Policy objects. To do this, the network administrator can define groups of administrators (for example, marketing administrators), and then provide them with Read/write access to selected Group Policy objects. This allows the network administrator to delegate control of Group Policy objects.

Having full control of a Group Policy object does not enable you to link it to a site, domain, or organizational unit. However, you can grant that ability using the Delegation of Control Wizard.

Delegating Control of Group Policy

Group Policy is one of the administrative tasks that can be delegated in Windows 2000. The following three Group Policy tasks can be independently delegated:

- Managing Group Policy links for a site, domain, or organizational unit.
- Creating Group Policy objects.
- Editing Group Policy objects.

Non-local Group Policy, like all Active Directory–based administrative tools, requires a Windows 2000 domain controller. Group Policy, like most other Windows 2000 administrative tools, is hosted in MMC consoles. The rights to create, configure, and use MMC consoles, therefore, have policy implications. You can control these rights through Group Policy under

<*Group Policy object name*>/User Configuration/Administrative Templates/Windows Components/Microsoft Management Console/

and its subfolders.

Table 22.2 lists the security permission settings for a Group Policy object.

Table 22.2 Security Permission Settings For A Group Policy Object.

Groups or Users	**Security permission**
Authenticated User	Read with Apply Group Policy ACE
Domain Administrators Enterprise Administrators Creator Owner Local System	Full Control without Apply Group Policy ACE

Note By default, if you are an administrator, you are also an authenticated user, which means that you have the **Apply Group Policy** attribute set. For more information, see "Editing Group Policy Objects" later in this chapter.

To administer Group Policy, you need to log on to a local or remote domain controller, which requires special permission. If you are a domain administrator or you are the built- in administrator on a domain controller, you have this permission.

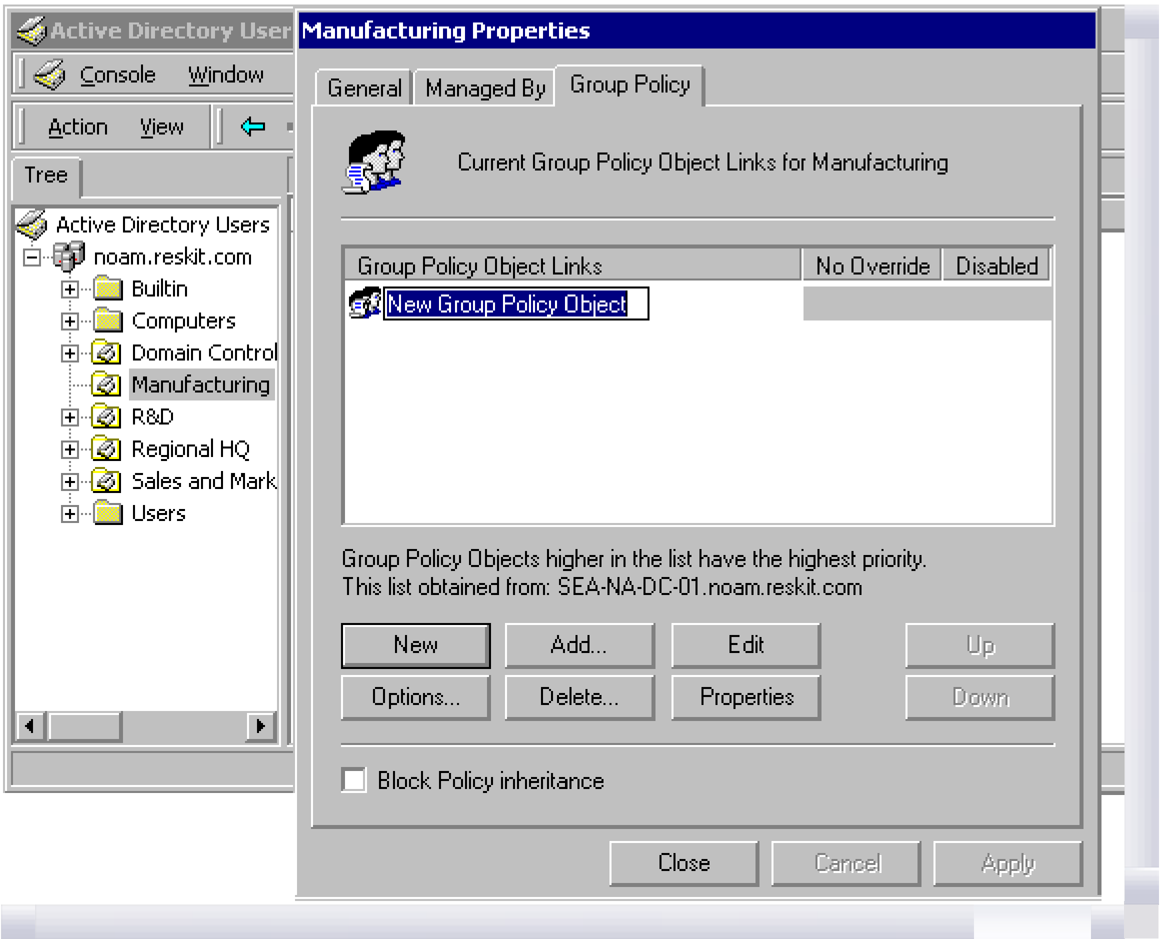
Non-administrators can log on to a domain controller only if they have Log On Locally permission. This is part of the Default Domain Controllers Group Policy object, linked to the Domain Controllers organizational unit in Active Directory Users and Computers. The setting is found under Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/Log on locally.

It is recommended that you create a security group containing those users who should be able to log on locally to the domain controller, and add them to the list of groups shown on the **Log On Locally** form. Remember that computer policy for the domain controller must refresh before the new permissions take effect.

Managing Group Policy Links for a Site, Domain, or Organizational Unit

The **Group Policy** tab in the site, domain, or organizational unit's **Properties** page allows you to specify which Group Policy objects are linked to this site, domain, or organizational unit. This property page stores the user's choices in two Active Directory properties called **gPLink** and **gPOptions**. The **gPLink** property contains the prioritized list of Group Policy object links and the **gPOptions** property contains the **Block Policy Inheritance** policy setting for domains or organizational units. The **Block Policy Inheritance** policy setting is not available for sites.

Figure 22.5 illustrates the creation of a new Group Policy object from within Active Directory Users and Computers. It has the default name **New Group Policy Object**, which you can change to something more descriptive. It will be stored in the noam.reskit.com domain, and it will automatically be linked to the Manufacturing organizational unit.



If your browser does not support inline frames, click here to view on a separate page.

Figure 22.5 Manufacturing Properties of New Group Policy Object

Active Directory supports security settings on individual properties. Thus, a non-administrator can be given Read and Write access to specific properties. If non-administrators have Read and Write access to the **gPLink** and **gPOptions** properties, they can manage the list of Group Policy objects linked to that site, domain, or organizational unit. To give a user Read and Write access to these properties, use the Delegation of Control Wizard and select the **Manage Group Policy links** predefined task.

Creating Group Policy Objects

By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and the operating system can create new Group Policy objects. If the domain administrator wants a non-administrator or group to be able to create Group Policy objects, that user or group can be added to the Group Policy Creator Owners security group. When a non-administrator who is a member of the Group Policy Creator Owners group creates a Group Policy object, that user becomes the Creator Owner of the Group Policy object. Then the user can edit the Group Policy object. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of only those Group Policy objects that the user creates or those explicitly delegated to that user. It does not give the user full control of any other Group Policy objects, and does not allow the user to link Group Policy objects to sites, domains, or organizational units.

Editing Group Policy Objects

By default, Group Policy objects give Domain Administrators, Enterprise Administrators, the operating system, and the Group Policy object Creator Owner full control without the **Apply Group Policy** attribute. They can edit the Group Policy object. But even if members of those groups have accounts in Active Directory sites, domains, or organizational units linked to the Group Policy object, the policy settings contained in that Group Policy object do not apply to them unless both of the following two conditions pertain:

- They have **Apply Group Policy** set to **Allow** as members of another security group.
- They don't have **Apply Group Policy** set to **Deny** as members of any security group.

By default, Authenticated Users have Read access to the Group Policy object with the **Apply Group Policy** attribute set.

Note By default, if you are an administrator, you are also an authenticated user, which means that you have the **Apply Group Policy** attribute set. If this is not what you intend, you have two choices:

- Remove authenticated users from the list, and add a security group with the **Apply Group Policy** attribute set to **Allow**. This new group should contain all the users who this Group Policy is intended to affect.
- Set the **Apply Group Policy** attribute to **Deny** for the Domain and Enterprise Administrators, and possibly the Creator Owner groups. This will prevent the Group Policy object from being applied to members of those groups. Remember that an ACE set to **Deny** always takes precedence over **Allow**. If a given user is a member of another group that is set to explicitly **Allow** the **Apply Group Policy** attribute for this Group Policy object, it will still be denied.

When a non-administrator creates a Group Policy object, he or she becomes the Creator Owner of the Group Policy object. When an administrator creates a Group Policy object, the Domain Administrators group becomes the Creator Owner of the Group Policy object.

To edit a Group Policy object, the user must have both Read and Write access to the Group Policy object. A Group Policy object cannot be opened in read-only mode. In other words, if you can open the Group Policy snap-in, you can edit the Group Policy object that appears in the namespace. Moreover, the changes occur during the edit. There is no "Save" or "Activate" step. As a precaution, you might want to unlink a Group Policy object from any site, domain, or organizational unit during the edit. Or you can leave it linked, but disable both the User and Computer nodes.

To edit a Group Policy object, the user must be one of the following:

- An administrator.
- A Creator Owner.
- A user with delegated access to the Group Policy object. That is, an administrator or the Creator Owner must have delegated access to this user by using the **Security** tab in the Group Policy object **Properties** page, and adding them to the Group Policy Creator Owners list.

Examples of Group Policy Delegation

Below are three examples of Group Policy delegation.

Example 1

In this example, control of an organizational unit is delegated to a non-administrative user so that a user can link existing Group Policy objects to the organizational unit but not create new Group Policy objects.

Throughout this example, a security group can take the place of the individual user.

1. In **Active Directory Users and Computers** snap-in, right-click the **Organizational Unit** that you want to delegate, and select **Delegate Control**.
2. In the **Delegation of Control Wizard**, click **Next** to go past the introduction page. You will be prompted for the names of the users and groups to which you want to delegate control.
3. Select a previously defined user, and click **Next**.
4. In the list of **Predefined Tasks**, select **Manage Group Policy links**, and then click **Next**.
5. Click **Finish** to complete the changes.

The user who you selected can add and delete Group Policy object links for the organizational unit whose control you delegated, to any Group Policy objects to which they have Read access.

If the Group Policy object is stored in another domain, the user's domain must be trusted by the storage domain.

Example 2

In this example, a user is given permission to create new Group Policy objects.

This permission is often useful in combination with the right to create links, as described in the previous example. To allow for creation of new Group Policy objects, you need to add the user to the **Group Policy Creator Owners** administrators group.

1. In **Active Directory Users and Computers**, navigate to the **Users** container in the root of the domain.
2. Double-click **Group Policy Creator Owners**.
3. In the **Properties** page, select the **Members** tab.
4. Click **Add**, and then add the user selected above to the security group.

The user can create new Group Policy objects, and the specific user who created each object becomes the Creator Owner of that Group Policy object.

You create Group Policy objects from within Active Directory Users and Computers by right-clicking the domain or organizational unit, clicking **Properties**, then the **Group Policy** tab, and then **New.** These objects are, by default, linked to the domain or organizational unit that has focus when they are created. Thus, a user with delegated rights, or you as an administrator, or any user who carries out the task of creating a Group Policy object in this way must have permission not only to create the Group Policy object, but also permission to link it to the domain or organizational unit. Otherwise the **New** button on the **Properties** sheet for the domain or organizational unit is shaded.

Example 3

In this example, control of a Group Policy object is delegated to a non-administrator user or group of users.

1. Open a **Group Policy object** in the **Group Policy** snap-in.
2. Right-click the root node, select **Properties**, and click **Security**.
3. Click **Add** to add the group of users or user, and then click **Full control**.
4. Clear the **Apply Group Policy** option or leave it checked depending on your purpose.

   This example shows how to delegate control of the Group Policy object. For this, you do not need the Apply Group Policy permission. If you clear the **Apply Group Policy** check box, the **Full Control** check box is also cleared, but the user still has Read/Write access to the Group Policy object.
5. Click **OK** to save the changes.

The user or group of users can edit the Group Policy object.

Creating MMC Consoles to Delegate Group Policy

You can delegate Group Policy administrative rights by creating and saving Group Policy MMC consoles, and then specifying which users and groups have access permissions to the Group Policy object, site, domain, or organizational unit. You define permissions for a Group Policy object by using the **Security** tab on the **Properties** page of the Group Policy object. These permissions grant or deny access to a Group Policy object to specified groups.

This type of delegation is augmented by the Group Policy settings available for MMC. Several settings are available in the Administrative Templates node, under Windows Components, Microsoft Management Console. These settings enable you to establish which MMC snap-ins the affected user can or cannot run. You can specify this as inclusive, which only allows a set of snap-ins to run, or as exclusive, which does not allow a set of snap-ins to run. See the **Explain** tab text of the individual policy setting for more information.

You can create custom consoles (.msc files) for Group Policy as for any other snap-in.

You can create and save custom Group Policy consoles that include only a subset of the Group Policy snap-in extensions. For example, you can create a custom Group Policy console that includes only the Security Settings extension. This allows you to define Group Policy settings in a modular fashion.

You can also create custom consoles that contain instances of Group Policy focused on different Group Policy objects or that contain snap-ins unrelated to Group Policy.

The computer on which the console runs must hold any DLLs used by the snap-ins. If the computer is a domain controller, the DLLs are probably present already. If not, their presence on the Windows 2000 member server or Windows 2000 Professional–based computer can be ensured by assigning or publishing the Windows 2000 Administration Tools. The package is called Adminpak.msi, and you can find it on the Windows 2000 Server companion CD.

There are several ways to start the Group Policy snap-in depending on your purpose. See Windows 2000 Help for more information. It is recommended that you delegate Group Policy using Custom Consoles. To do this, you should start Group Policy as a stand-alone snap-in:

To start Group Policy as a stand-alone snap-in

1. Click **Start**, click **Run**, type **MMC**, and then click **Enter**.
2. In the MMC window, on the **Console** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Add Snap-in** dialog box, click **Group Policy**, and then click **Add.**
5. In the **Select Group Policy object** dialog box, click **Browse** to find the Group Policy object you want to manage.
6. Click **Extensions**, and then select the extension snap-ins you want to use.
7. Click **Finish**.
8. Click **OK**. The Group Policy snap-in opens with focus on the Group Policy object you specified.
9. After you specify the policy settings you want to use, click **Save As** on the **Console** menu to save your settings in an .msc file.

To set access permissions, use the **Security** tab on the **Properties** page of the selected Group Policy object. These permissions allow or deny access to the Group Policy object by specified groups.

There are dozens of Group Policy settings that allow or deny access to various snap-ins and snap-in extensions. Check the following folders for settings that might be relevant for your organization:

- User Configuration/Administrative Templates/Microsoft Management Console
- User Configuration/Administrative Templates/Microsoft Management Console/Restricted/Permitted snap-ins
- User Configuration/Administrative Templates/Microsoft Management Console/Restricted/Permitted snap-ins/Extension Snap-ins
- User Configuration/Administrative Templates/Microsoft Management Console/Restricted/Permitted snap-ins/Group Policy

Group Policy Processing

Group Policy is processed in the following order:

The local Group Policy object. This is the only source of Group Policy for stand-alone computers or computers in workgroups. The local Group Policy object is always processed.

Active Directory linked Group Policy objects. Site first, domain next, and organizational unit last, including any nested organizational units, from parent to child. At each site, domain, or organizational unit, one, many, or no Group Policy objects can be linked. If more than one link is present, those links can be prioritized.

Note The **Block policy inheritance** or **No Override** options can affect the presence or absence of Group Policy objects in the list of Group Policy objects to be processed, but cannot change their order. The blockade occurs at the domain or organizational unit level, thus removing all non-local Group Policy objects that would otherwise be processed earlier, except those set to **No Override**. The local Group Policy object cannot be blocked. The **No Override** setting for Group Policy is an attribute of a link, and therefore applies to a *particular* Group Policy object, and only at the *particular* site, domain, or organizational unit to which it is linked.

Computer policy is processed at startup and then user policy is processed when the user logs on. Although computer policy is applied before user policy, if user and computer policy settings specify different behavior, the computer policy will generally prevail. This is not enforced by the Group Policy infrastructure, but is rather a convention that is followed by the operating system and by applications that exploit Group Policy unless there are specific reasons that the convention is not appropriate for a given policy setting.

Note There are policy processing issues that arise if you use Windows NT 4.0 and migrate to a Windows 2000 environment. For more information, see "Migration Issues Pertaining to Group Policy" later in this chapter.

Most Group Policy settings are implemented at the client computer by DLLs on the client. These DLLs are called client-side extensions. Remote Installation Services is an exception. RIS has no client-side extension because it is used to install an operating system remotely, and a DLL is useless without an operating system.

For each client-side extension, the Group Policy object processing order is obtained from a list of Group Policy objects, which is obtained from the **GetGPOList** Microsoft® Win32® function. Each client-side extension processes the resulting list of Group Policy objects.

In most cases policy settings specified in the Computer Configuration node have precedence over the same setting if one exists in the User Configuration node. There are a few exceptions and their behavior is set forth in the Explain text for those settings. An example is Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges, which requires the setting in both Computer and User Configuration to be enabled or it is not activated. See the Explain text for that policy setting for details.

Group Policy affects only users and computers contained in sites, domains, and organizational units. Specifically, Group Policy objects are not applied to Security Groups.

Synchronous and Asynchronous Processing

Asynchronous refers to processes that do not depend on each other's outcome, and can therefore occur on different threads simultaneously. The opposite is synchronous. Synchronous processes wait for one to complete before the next begins. For those Group Policy settings for which both types of processes are available as options, you choose between the faster asynchronous or the safer, more predictable synchronous processing.

By default, the processing of Group Policy is synchronous. Computer policy is completed before the CTRL+ALT+DEL dialog box is presented, and user policy is completed before the shell is active and available for the user to interact with it.

Note You can change this default behavior by using a policy setting for each so that processing is asynchronous. This is not recommended unless there are compelling performance reasons. To provide the most reliable operation, leave the processing as synchronous.

Group Policy for computers is applied at computer startup. For users, Group Policy is applied when they log on.

Periodic Refresh Processing

You can specify that Group Policy be processed periodically. By default, this is done every 90 minutes with a randomized offset of up to 30 minutes. You can change these default values by using a Group Policy setting in Administrative Templates. Setting the value to zero minutes causes the refresh rate to be set to seven seconds.

If you want to change this setting, edit the Default Domain Controllers Group Policy object. It is linked to the Domain Controllers organizational unit. The setting is located under Computer Configuration/Administrative Templates/System/Group Policy/Group Policy Refresh Interval for Computers.

Caution Short refresh intervals are intolerable in a production environment. Every policy refresh causes the Windows shell to be refreshed, which in turn causes all open context menus to close, a brief flicker of the screen, and so on. Such intervals are intended to be used only in test or demonstration scenarios.

The default period is every five minutes for domain controllers. There is a setting for this under Computer Configuration/Administrative Templates/System/Group Policy/Group Policy Refresh Interval for Domain Controllers.

Software Installation and Folder Redirection processing occurs only during computer startup or when the user logs on, not during the periodic refresh. For these extensions, periodic processing is inappropriate. For example, in the case of Software Installation, if an application is no longer assigned, it can be removed automatically, if you have used Group Policy to set it up that way. If a user is using the application while Group Policy tries to uninstall it, or if an assigned application upgrade takes place while a user is using it, the user will encounter an error.

Optional Processing of Group Policy Even If It Has Not Changed

To achieve the highest level of policy settings security, activate the **Process Even If The Group Policy Objects Have Not Changed** policy for each of the Group Policy client-side extensions that require it. These policy settings are located in the Computer Configuration node, under Administrative Templates, System, Group Policy. Each client-side extension has a policy setting for controlling the policy processing. By default, each Group Policy client-side extension updates its policy settings only when they have changed. Choosing this option ensures that the selected settings are applied at every logon session to Active Directory, but forgoes the performance optimization achieved by skipping the application of policy settings when they have not changed. For information about Windows 2000 security, see the chapters under "Distributed Security" in this book.

Group Policy and Network Bandwidth

When Group Policy detects a slow link, it sets a flag to indicate this to client-side extensions.

The default settings for whether policy is applied over a slow link are shown below. ON indicates that processing occurs even if the link is judged to be slow.

- Security Settings — ON (and cannot be turned off)
- Administrative Templates — ON (and cannot be turned off)
- Software Installation — OFF
- Scripts — OFF
- Folder Redirection — OFF
- Internet Explorer Maintenance — OFF

For all but the Administrative Templates and Security snap-ins, a policy is provided for toggling the settings.

Setting Policy for Slow-Link Definition

You can use Group Policy to set the definition of a slow link for computers and users, and for user profiles.

Note Windows 2000 adds an IP algorithm to ping the server, whereas Windows NT 4.0 just measures the file system performance.

The following algorithm is used to determine whether the link should be considered slow:

Ping the server with 0 bytes of data and time the number of milliseconds. Call this value time#1. If it is less than 10 milliseconds, then assume it is a fast link, and exit.

Ping the server with an uncompressible 2 kilobytes (KB) of data, and time the number of milliseconds. Call this value time#2. The algorithm uses an already compressed .jpg file. If it used a compressible file, the modem would compress it and make the network appear faster than it is.

DELTA = time#2 - time#1. This removes the overhead of session setup. DELTA is the time in milliseconds to move 2 KB.

DELTA is measured three times, and the average of the three values of DELTA obtained is called AVG.

Then the connection speed Z, measured in kilobits per second (Kbps), is:

Z = 32000/AVG.

The correctness of this formula is more apparent with the units in place:

(Z kilobits / second) = 2 * (2 KB) * (8 bits/ byte) * (1000 milliseconds / second) / (AVG milliseconds).

2 KB of data have moved through each modem, Ethernet card or other device in the loop once in each direction, so this equation for calculating the one-way bandwidth has a leading factor of 2 on the right side.

Note The speed Z used here is the average of the upload and download speeds. In most cases, this average is the same as the download speed itself. However, in some cases the upload and download speeds are different enough that you should take this into account. An example of this is Asymmetric Digital Subscriber Line (ADSL). Using ADSL you might have upload speeds of 128 Kbps and download speeds of 768 Kbps.

Z is compared with 500 Kbps (or an alternative threshold of your choice if you change from the default Group Policy setting of 500 Kbps).

If Z is less than 500 Kbps the connection is considered slow, otherwise it is considered fast.

You can set the default value of 500 Kbps in the Group Policy console under <*Group Policy object name*>/Computer Configuration/Administrative Templates/System/Group Policy/Group Policy slow link detection.

To specify policy settings for Group Policy slow link detection for computers, you use the Computer Configuration\Administrative Templates\System\Group Policy node. To set this policy for users, you use the User Configuration\Administrative Templates\System\Group Policy node.

For User Profiles, the Slow network connection time-out for user profiles policy is located in the Computer Configuration\Administrative Templates\System\Logon node. The user profile code first tries to contact (or ping) the server. If the server does not have IP support, it falls back to measuring the file system's performance. You specify a threshold connection speed in kilobits per seconds, and a threshold transit time in milliseconds, when configuring this policy setting.

Registry Reads

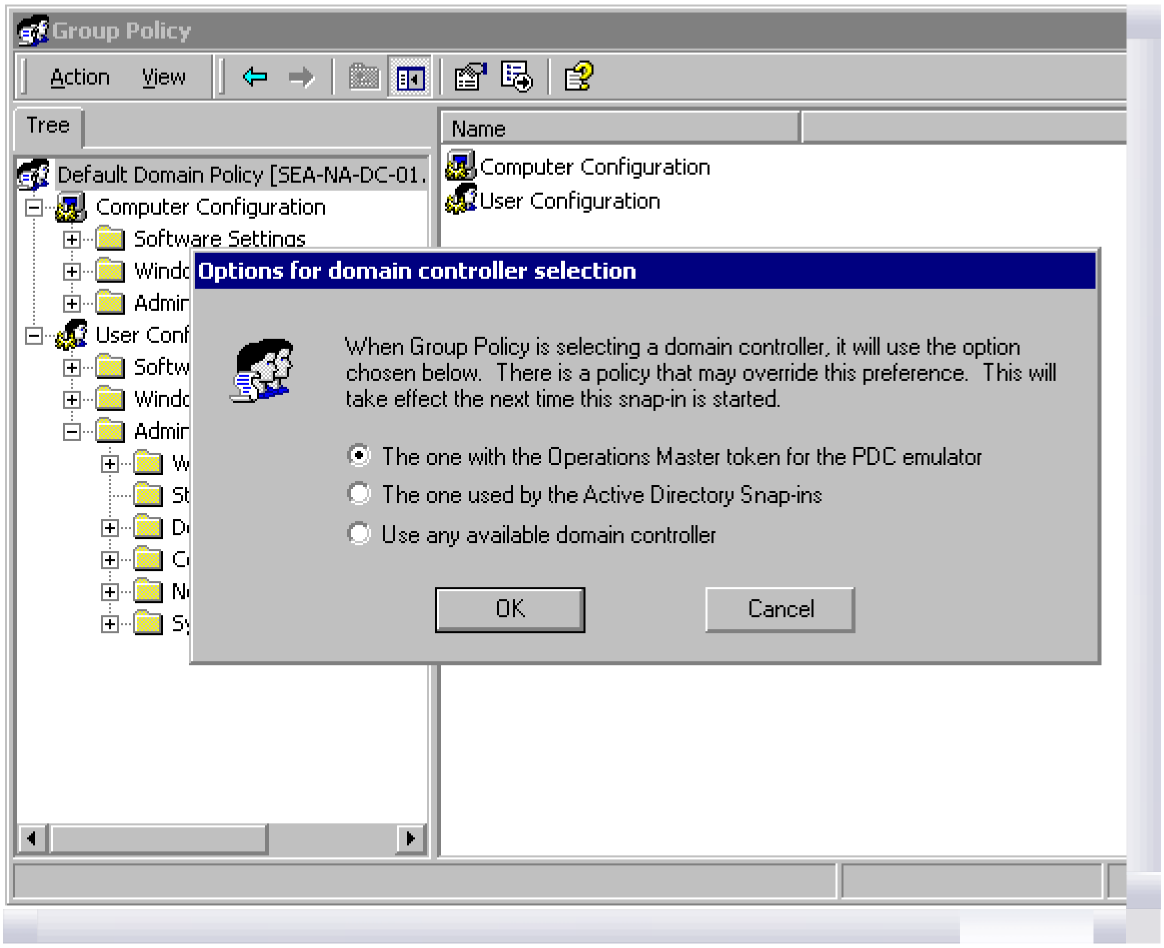
Group Policy snap-in extensions can temporarily claim (or lock) a mutex (mutual exclusive) for policy, and then release that mutex. APIs exist to allow a client-side extension to claim the mutex, read the required values, then release the critical section. If it is not released in 10 minutes, the client-side extension is forced to release it. This ensures that the background refresh of Group Policy does not occur during the read process.

For more information about the Windows 2000 Group Policy APIs, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Specifying a Domain Controller for Setting Group Policy

Two methods are available to set domain controller options for Group Policy. One method is to use the Group Policy snap-in user interface, where the user can set domain controller options by using the DC Options dialog box, as described next. The other method allows the primary domain administrators to set domain controller options by using a policy in the Administrative Templates node, as described in Specifying Policy for Domain Controller Options listed later.

The Group Policy snap-in **View** menu contains an entry called DC Options, which opens the Options for the domain controller selection dialog box, where you will be able to specify a preference for a domain controller to use for editing Group Policy. Figure 22.6 shows the **Options for domain controller selection** dialog box.



Options for domain controller selection

When Group Policy is selecting a domain controller, it will use the option chosen below. There is a policy that may override this preference. This will take effect the next time this snap-in is started.

● The one with the Operations Master token for the PDC emulator

○ The one used by the Active Directory Snap-ins

○ Use any available domain controller

If your browser does not support inline frames, click here to view on a separate page.

Figure 22.6 Options for Domain Controller Selection Dialog Box

In the **Options for domain controller selection** dialog box shown in Figure 22.6, you can choose the following options:

The one with the Operations Master token for the PDC emulator. This is the default and preferred option. Using this option helps ensure that no data loss occurs. This forces the Group Policy snap-in to use the same domain controller. Data loss can occur if two administrators are working on changes to the same Group Policy object on different domain controllers within the replication cycle. Group Policy writes data to the Group Policy object for each change. If two administrators are editing a Group Policy object on different domain controllers, it increases the possibility of changes being overwritten by replication. It is strongly recommended that you limit the number of administrators permitted to administer Group Policy, and that you make sure that Group Policy uses the primary domain controller emulator Operations Master. It is also recommended that administrators be aware of other administrators who might be editing the same Group Policy object.

The one used by Active Directory Snap-ins. Uses the domain controller that Active Directory management snap-ins are using. Each of these snap-ins includes an option for changing which domain controller is the focus of its current operations. When this option is selected, the Group Policy snap-in uses the same domain controller.

Use any available domain controller. The third, and least desirable option in most cases, allows the Group Policy snap-in to choose any available domain controller. When this option is used it is likely that a domain controller in the local site will be selected.

You can override all of these options using a policy setting, as described in the following section.

Specifying Policy for Domain Controller Options

The Group Policy snap-in uses the primary domain controller emulator operations master token when editing a Group Policy object. This token makes sure that the Group Policy snap-in is always focused on the same domain controller. User preference options and policy settings are available to modify this behavior so that Group Policy can use a different domain controller.

If you are the primary domain administrator, you can use a policy to specify how Group Policy chooses a domain controller — that is, you can specify which domain controller option should be used. If the selected option is not available, the user receives an error message. When this occurs, the DC Options menu item is shaded (unavailable) because a policy is in place that overrides any setting that the user picks. This policy allows domain administrators to indicate that all administrators must use the primary domain controller, for example. The domain controller options settings are available in the **User Configuration, Administrative Templates, System, Group Policy** node of the Group Policy snap-in. The available domain controller options are the same as the preference settings listed above in the **Options for domain controller selection** dialog box description.

For example, if you are an administrator on one continent and the primary domain controller is on another, you can make your policy edits locally, so that the performance is acceptable. Remember, though, that if someone else edits the same Group Policy object simultaneously, the winner depends on the unpredictable actions of the network.

If the Group Policy snap-in cannot reach the intended domain controller, by default you receive the following error message: "Error Handling on Failure to Reach a Domain Controller." Then you are given the option to cancel the operation or make a selection to retry accessing a domain controller using the following choices:

- The one with the Operations Master token for the primary domain controller emulator.
- The one used by Active Directory Snap-ins.
- Use any available domain controller.

If instead of the error message just described, you get the message "Failed to find a domain controller. There may be a policy that prevents you from selecting another domain controller," then check to see whether the following Group Policy setting is in effect:

<*Group Policy object name*>/User Configuration/Administrative Templates/System/Group Policy/Group Policy domain controller selection

Domain Controller Selection Results

Table 22.3 shows the results of various combinations of domain controller conditions. The following terms are used in Table 22.3:

- **Primary Domain Controller**: is the domain controller with the Operations Master token for the primary domain controller emulator.
- **Inherit**: is the domain controller used by Active Directory snap-ins.
- **1) and 2)** : means that 1) is tried first then 2).

Table 22.3 Domain Controller Selection Results

User preference	Policy	Inherit domain controller	Results
Undefined	Undefined	N/A	1) Primary domain controller 2) Prompt
Primary domain controller	Undefined	N/A	1) Primary domain controller 2) Prompt
Inherit	Undefined	Yes	Inherit
Inherit	Undefined	No	Any domain controller
Any domain controller	Undefined	N/A	Any domain controller
N/A	Primary domain controller	N/A	Primary domain controller only
N/A	Inherit	Yes	Inherit
N/A	Inherit	No	Any domain controller
N/A	Any	N/A	Any domain controller

Client-side Processing of Group Policy

Some of the Group Policy components include client-side extensions (.dlls) that implement Group Policy at client computers. The client-side extensions are loaded as needed when a client computer is processing policy. The client computer first gets a list of Group Policy objects. Next, it loops through all the client-side extensions and determines whether each client-side extension has any data in any of the Group Policy objects. If a client-side extension has data in a Group Policy object, the client-side extension is called with the list of Group Policy objects that it should process. If the client-side extension does not have any settings in any of the Group Policy objects, it is not called.

Table 22.4 lists the client-side extensions.

Table 22.4 Client-side Extensions

Client-side extension	DLL file name
Registry (in Administrative Templates)	Userenv.dll

Disk Quota (in Administrative Templates)	Dskquota.dll
Folder Redirection	Fdeploy.dll
Scripts	Gptext.dll
Software Installation	Appmgmts.dll
Security	Scecli.dll
IP Security	Gptext.dll
EFS (Encrypting File System) Recovery	Scecli.dll
Internet Explorer Maintenance	iedkcs32.dll
Remote Installation Services	none

Client-side Extension Preferences

The values that the client-side extension puts in the registry are preferences as opposed to Group Policy settings. However, if you decide that the client-side extension should run across a slow link, regardless of the amount of data, you can enable these policies.

All MMC snap-ins register themselves in the following location in the registry:

HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \MMC \SnapIns{*Snap-in-GUID*}

Possible REG_SZ value names are as follows:

- About
- NameString
- NodeType
- Provider
- Version

In addition to the location mentioned earlier, Group Policy Client Side Extensions also register themselves in the following location in the registry:

HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion\Winlogon\GPExtensions\{CSE-GUID}

Possible REG_DWORD value names are as follows:

Important The REG_DWORD value names listed here are informational only. It is recommended that you do not change these.

- EnableAsynchronousProcessing
- LastPolicyTime
- MaxNoGPOListChangesInterval
- NoBackgroundPolicy
- NoGPOListChanges
- NoMachinePolicy
- NoSlowLink
- NoUserPolicy
- NotifyLinkTransition
- PerUserLocalSettings
- PrevSlowLink
- RequiresSucessfulRegistry
- Status
- This possible REG_SZ valuename
- ProcessGroupPolicy
- This REG_EXPAND_SZ valuename
- DllName

Note LastPolicyTime and Status are set automatically by the Group Policy engine, not by the client-side extensions.

Computer Policy for Client-side Extensions

A computer policy exists for each of the Group Policy client-side extensions. Each policy includes a maximum of three options. Some of the client-side extensions include only two computer policy options; in those cases, this is because the third option is not appropriate for that extension. The computer policy options are as follows:

Allow processing across a slow network connection. When a client-side extension registers itself with the operating system, it sets values in the registry, specifying whether it should be called when policy is applied across a slow link. Some extensions move large amounts of data, so processing across a slow link can hurt performance. Installing a large application across a 28.8 Kbps modem line is impractical.

Do not apply during periodic background processing. Computer policy is applied at startup, as well as periodically in the background, approximately every 90 minutes. User policy is applied at user logon, then every 90 minutes. Some extensions process policy only initially, not periodically, because processing that took place in the midst of a user's session would be disruptive. For example, with Software Installation, applications are installed or upgraded during the initial run and not in the background. If it were done in the background, a hapless user might be running an application even while having it uninstalled. Or the application might have a shared component that is in use by another application, preventing the installation from completing successfully. The **Do Not Apply During Periodic Background Processing** option gives you the ability to override this logic and force the extension to either run or not run in the background.

Process Even If The Group Policy Objects Have Not Changed. By default, if the Group Policy objects on the server have not changed, it is not necessary to continually reapply them to the client, because the client should already have all the settings. However, users might be able to change some settings if they are administrators of their computers. In this case, it might make sense to reapply these settings when the user logs on or during the periodic refresh cycle to get the computer back to the desired status.

For example, if you have used Group Policy to define a specific set of security options for a file, and the user with administrative privileges logs on and changes it, then, you might want to set the policy to process Group Policy even if the Group Policy objects have not changed. This makes sure that security is reapplied periodically and at every startup. This also applies to applications. Group Policy installs an application, but the end user can remove the application or delete the icon. The **Process Even If The Group Policy Objects Have Not Changed** option gives you the ability to restore the application at the next user logon session.

Table 22.5 lists the client-side extensions that include only two computer policy options, as well as the reason for this.

Table 22.5 Client-side Extension and Policy Options

Client-side extension	Missing policy checkbox	Reason
Administrative Templates	Slow link (Allow processing across a slow network connection)	Registry policy is always applied because it controls the other client-side extensions.
Security Settings	Slow link (Allow processing across a slow network connection)	To ensure that security settings are in effect, they must always be applied, even across a slow link.
Folder Redirection	Background processing (Do not apply during periodic background processing)	User might be using the folders or their contents.
Software Installation	Background processing (Do not apply during periodic background processing)	It would be disconcerting to the user to have an application uninstall while it is open.

The processing of policy is also affected by issues that are not governed by specific policy settings and not apparent in the user interface. The include the following:

Messages and Events When Group Policy is applied, a WM_SETTINGCHANGE message is sent, and an event is signaled. Applications that can receive window messages can use it to respond to a Group Policy change. Those applications that do not have a window to receive the message (as with most services) can wait for the event.

On-Demand Processing Group Policy can also be applied on demand. To do this, applications can call the RefreshPolicy function, which allows applications to request a policy refresh. The administrator can refresh policy from the command line as follows:

1. Click **Start,** and then click **Run**.
2. To refresh policies under the **Computer Configuration** node, type the following, and then click **OK**:

   secedit /refreshpolicy MACHINE_POLICY [/enforce]
3. To refresh policies under the **User Configuration** node, type the following, and then click **OK**:

   secedit /refreshpolicy USER_POLICY [/enforce]

The optional "/enforce" switch causes policy for the Security and EFS extensions to refresh whether or not there is a policy change. For other extensions it has no effect.

Time Limit for Processing of Group Policy There is a time limit of 60 minutes for all the client-side extensions to finish processing policy. An errant client-side extension that is not finished after 60 minutes will be stopped and the associated policy settings will not be processed. There is no Group Policy setting to change the default time limit.

Using Group Policy on Stand-alone Computers

You can set local Group Policy for computers that are not members of a domain. To set local Group Policy, you use the Group Policy snap-in focused on the local computer. You can gain access to the Group Policy snap-in by typing "MMC" at the command prompt, adding the Group Policy snap-in to the MMC console, and focusing the Group Policy snap-in on the local computer.

Local Group Policy Object

Local Group Policy objects exist on stand-alone computers, however it consists of only the Group Policy template portion of a Group Policy object. The location of the local Group Policy object is %SystemRoot%\System32\GroupPolicy. Each Group Policy extension snap-in queries Group Policy to receive the Group Policy object type (local or Active Directory–based), and then determines if it should be displayed in the console.

Table 22.6 indicates whether or not each Group Policy snap-in extension opens when the Group Policy snap-in is focused on a local Group Policy object.

Table 22.6 When Group Policy Snap-in Loads

Group Policy snap-in extension	Loads when Group Policy snap-in focused on local Group Policy object
Security Settings	Yes
Administrative Templates	Yes
Software Installation	No
Scripts	Yes
Internet Explorer Maintenance	Yes
Remote Installation Services	No
Folder Redirection	No

Starting Group Policy on Windows 2000 Professional

Windows 2000 Professional does not provide a preconfigured MMC console for accessing non-local Group Policy directly, except for Security Settings, which can be accessed from Control Panel. However, you can create your own custom Group Policy console by taking the following steps:

To start the Group Policy snap-in on Windows 2000 Professional

1. Click **Start**, click **Run**, type **MMC**, and then click **OK**.
2. In the MMC window, on the **Console** menu, click **Add/Remove Snap-in**.
3. On the **Standalone** tab, click **Add**.
4. In the **Add Snap-in** dialog box, click **Group Policy**, and then click **Add**. The **Select Group Policy object** dialog box appears.
5. Click **Local Computer** to edit the local Group Policy object, or **Browse** to find the Group Policy object that you want to use.
6. Click **Finish**.
7. Click **OK**. The Group Policy snap-in opens focused on the specified Group Policy object.

   Note To use the Group Policy snap-in focused on a remote computer, you must have administrative rights on the target computer in addition to appropriate permission to use the snap-in.

Using the Group Policy Snap-in Focused on a Remote Computer

The Group Policy object seen at the root node of the Group Policy console is said to have "focus." The console can be focused on any computer's local Group Policy object, or any Active Directory–based Group Policy object.

Note Focusing the Group Policy snap-in, whether on a remote computer or the local computer, or on an Active Directory–based Group Policy object, must be done when the extension is added to an MMC console file, or as a command line option. The focus cannot be changed while the Group Policy console is in use.

To add Group Policy to an MMC console focused on a specific remote computer

1. Click **Start**, click **Run**, and type **MMC**. Or you can open an existing saved console such as Console1.mmc.
2. In the **MMC** window, on the **Console** menu, click **Add/Remove** Snap-in.
3. On the **Standalone** tab, click **Add**.
4. In the **Add Snap-in** dialog box, click **Group Policy**, and then click **Add**. By default this is set to open on the local computer.
5. Click **Browse**.
6. You can now select a Group Policy object from Active Directory or, as in this case, select the **Computer** tab.
7. Select **Another Computer**.
8. Either type in the computer name or click **Browse** to locate it.
9. Select the domains to which you have access in the **Look in** drop-down list.

The supported computer name formats are:

- NetBIOS names; for example:

  ```
  ThisComputer
  ```

- DNS-style; for example:

  ```
  ThisComputer.Reskit.com
  ```

You can start the Group Policy snap-in with the following two command line switches:

- Specific computer

  ```
  /gpcomputer:<machinename>
  ```

  Where <machinename> can be either a NetBIOS or a DNS-style name.

  For example:

  ```
  gpedit.msc /gpcomputer:"ThisComputer"
  ```

  or

  ```
  gpedit.msc /gpcomputer:"ThisComputer.Reskit.com"
  ```

  Note that there is no space following:

  ```
  /gpcomputer:
  ```

  Also, the quotes are necessary, not optional.

- Specific ADSI path

  ```
  /gpobject:"<ADSI path>"
  ```

  For example:

  ```
  /gpobject:"LDAP://CN={31B2F340-016D-11D2-945F-
  00C04FB984F9},CN=Policies,CN=System,DC=Reskit,DC=com"
  ```

  in which the GUID for the Group Policy object is a made-up example.

For these command line options to function with a saved console file, you must select the check box titled "Allow the focus of the Group Policy snap-ins to be changed when launching from the command line." This only applies if you save the console. The Gpedit.msc file supplied with Windows 2000 has this option enabled.

Note The Security Settings extension does not support remote management for local policy in Windows 2000.

Local Group Policy Object Processing

The local Group Policy object is processed even when the **Block Policy Inheritance** option has been specified on a domain or organizational unit.

Local Group Policy objects are always processed first, and then non-local (that is, Active Directory–based) policy is processed. If a computer is participating in a domain, and a conflict occurs between non-local and local computer policy, then by default, non-local policy prevails by overwriting local policy. If a computer withdraws from a domain, local Group Policy object policy settings are still applied and assume greater importance because they can no longer be overwritten.

If the Computer Account object and User Account object are both managed by Windows NT 4.0 domain controllers and are therefore not in Active Directory, then no local Group Policy object will be processed. For details about other interoperability situations that can arise during migration, see "Migration Issues

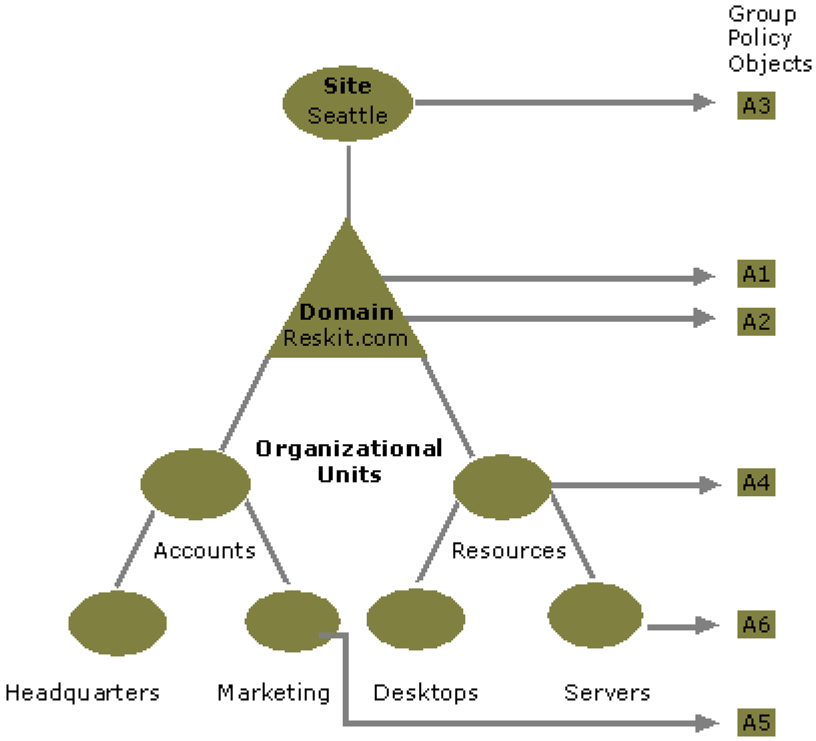
Pertaining to Group Policy" later in this chapter.

Group Policy Loopback Support

Group Policy applies to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. However, in some cases, users might need policy applied to them based on the location of the computer object alone. The Group Policy loopback feature gives you the ability to apply Group Policy objects that depend only on which computer the user logs on to.

Note Loopback is supported only in a purely Windows 2000–based environment. Both the computer account and the user account must be in Active Directory. If either account is managed by a Windows NT 4.0–based domain controller, loopback does not function. The client computer must be a Windows 2000–based computer.

The following scenario describes the loopback feature. In this scenario, you have full control over the computers and users in this domain because you have been granted domain administrator rights. Figure 22.7 shows the Reskit domain.



If your browser does not support inline frames, click here to view on a separate page.

Figure 22.7 The Reskit Domain

When users work in their own workstations, they should have Group Policy applied to them according to the policy settings defined, based on the location of the user object. However, when users log on to a computer whose computer object is in the server's organizational unit, they should receive user policy settings based on the computer object location, rather than the user object location.

In Figure 22.8, normal user Group Policy processing specifies that computers located in the server's organizational unit have the Group Policy objects A3, A1, A2, A4, and A6 applied in that order during computer startup. Users of the Marketing organizational unit have Group Policy objects A3, A1, A2, and A5 applied in that order, regardless of which computer they log on to.

In some cases this processing order might not be appropriate; for example, when you do not want applications that have been assigned or published to the users of the Marketing organizational unit to be installed while they are logged on to the computers in the Servers organizational unit. With the Group Policy loopback support feature, you can specify two other ways to retrieve the list of Group Policy objects for any user of the computers in the Servers organizational unit. You can use either the Merge Mode or the Replacement Mode.

Merge Mode. In this mode, when the user logs on, the user's list of Group Policy objects is gathered normally by using the **GetGPOList** function, and then **GetGPOList** is called again using the computer's location in Active Directory. Next, the list of Group Policy objects for the computer is added to the end of the Group Policy objects for the user. This causes the computer's Group Policy objects to have higher precedence than the user's Group Policy objects. In this example, the list of Group Policy objects for the computer is A3, A1, A2, A4, and A6, which is added to the user's list of A3, A1, A2, and A5, and thus results in A3, A1, A2, A5, A3, A1, A2, A4, and A6 (listed in lowest to highest priority).

Replace Mode. In this mode, the user's list of Group Policy objects is not gathered. Only the list of Group Policy objects based upon the computer object is used. In Figure 22.7, the list is A3, A1, A2, A4, and A6.

The loopback feature was implemented in the Group Policy engine, not in the **GetGPOList** function. When the Group Policy engine is about to apply user policy, it searches in the registry for a computer policy, which specifies which mode user policy should be applied in. Then, based upon this policy, it calls **GetGPOList**, as appropriate.

Supporting Windows NT 4.0, Windows 95, and Windows 98 Clients

The Windows 2000 Group Policy does not provide client support for Windows NT 4.0–based, Windows 95–based, or Windows 98–based computers, notwithstanding the availability of Active Directory client support for those earlier versions of Windows.

Policy support for Windows NT 4.0–based clients is provided by using Windows NT 4.0–style administrative templates (.adm files) and Windows NT 4.0 System Policy Editor (Poledit.exe) files.

Windows 95 and Windows 98 clients need to be managed with the System Policy Editor.

Client computers that are running Windows NT 4.0, Windows 95, or Windows 98 need to have the .pol file (Config.pol for Windows 98 or Windows 95, or Ntconfig.pol for Windows NT 4.0) created on the client computer's operating system copied to the domain's Netlogon share. This is: %systemroot%\SYSVOL\sysvol\<*domain name*>\SCRIPTS under Windows 2000, or %systemroot%\winnt\system32\Repl\Import\Scripts under Windows NT 4.0.

For information about installing the System Policy Editor, see Windows 2000 Server Help. The System Policy Editor is included with Windows 2000 Server but is not included with Windows 2000 Professional. The Windows 2000 Optional Administrative Tools package (Adminpak.msi), which includes the System Policy Editor, comes on the Windows 2000 Server companion CD for installation onto computers running Windows 2000 Professional.

Using Windows NT 4.0 Administrative Templates in the Windows 2000 Group Policy Console

On the menu bar of the Group Policy console, the **Show Policies Only** setting is under the **View** button. This is active (checked) by default. It prevents Windows NT 4.0 Administrative Templates, which are used to supply namespace for the System Policy Editor, from supplying that same namespace in the Group Policy console. This is safest, because Windows NT 4.0 registry-based policy is undesirably persistent from the Windows 2000 administrative perspective, and it is best to not use System Policy on Windows 2000 clients. However, it is possible to uncheck **Show Policies Only**, so that true Group Policy settings appear in blue, and System Policy settings appear in red. The next time you run the Group Policy snap-in, non-Group Policy settings are hidden again.

It is recommended that you use the **Enforce Show Policies Only** setting, in User Configuration/Administrative Templates/System/Group Policy if you delegate Group Policy administrative tasks using custom consoles. This prevents users of the console from unchecking **Show Policies Only**.

Migration Issues Pertaining to Group Policy

In organizations containing many networked Windows NT 4.0–based computers, including primary domain controllers, backup domain controllers, client workstations, and client stand-alone servers, it might not be practical to upgrade all computers simultaneously to Windows 2000. Therefore, when a network of Windows NT 4.0–based computers is upgraded to Windows 2000, you need to know what to expect during and after the migration process.

Before the migration is complete you might need to manage a domain in which all of the following types of computers participate:

- Windows 2000 Server domain controllers
- Windows NT 4.0 Server domain controllers
- Windows 2000 Professional clients
- Windows 2000 Server clients
- Windows NT 4.0 Workstation clients
- Windows NT 4.0 Server clients
- Computers running earlier versions of Windows, such as Windows 98

There are many interactions to consider. Fortunately, the conditions on the client side are not complicated.

The Client Side

The only computers that are subject to and are able to use Group Policy are Windows 2000–based computers. Client computers running Windows NT 4.0 receive System Policy as administered through the System Policy Editor (Poledit.exe). Client computers running Windows 98 or Windows 95 are also managed using System Policy compatible with those operating systems. You can only use the .pol files created using Poledit.exe on computers running the operating system on which the .pol file was created. Windows NT–based computers cannot use Config.pol (Windows 98 or Windows 95 System Policy), nor can Windows 98–based or Windows 95–based computers use NTConfig.pol (Windows NT System Policy).

The Domain Controller Side

The interaction of Windows NT 4.0 System Policy and Windows 2000 Group Policy during migration is described in this section. You can assume that the client computers, meaning all computers other than the domain controllers, run either Windows 2000 Professional or Windows 2000 Server unless the contrary is specifically stated.

For a user to log on to a domain successfully, both the user and the computer must be known to the domain. You need to know what behavior to expect when computer or user accounts, or both, have not yet been upgraded from Windows NT 4.0 to Windows 2000.

Computer and User Accounts Both on Windows NT 4.0 Domain Controllers.

These accounts might be on the same or different domain controllers. There might be Windows 2000 domain controllers on the intranet as well; however, they don't handle these particular accounts. The user and computer are not in Active Directory.

System Startup

Local Group Policy for the computer is applied when the computer starts up.

User Logon

Windows NT 4.0 System Policy for the computer is applied. Then, Windows NT 4.0 System Policy for the user is applied. Then, if local Group Policy has changed since it was last applied, the following policy settings are applied: Local Group Policy for the user, followed by Windows NT 4.0 System Policy for the user.

Computer and User Accounts Both on Windows 2000 Domain Controllers

The user account and computer account are both in Active Directory. There might be Windows NT 4.0 domain controllers on the intranet as well, but they are not involved in the startup/logon negotiation because Windows 2000 clients prefer Windows 2000 domain controllers.

System Startup

Windows 2000–based computer Group Policy is applied at boot time.

User Logon

Windows 2000 user Group Policy is applied when the user logs on.

Computer is Managed in a Windows NT 4.0 Account and User is Managed in a Windows 2000 Account

The user account is in Active Directory, and the computer account is not. The computer account is managed by a Windows NT 4.0 domain controller. This is a common scenario.

System Startup

Local Group Policy for the computer is applied when the computer starts up.

User Logon

When the user logs on, the computer receives System Policy, and then the user receives all Group Policy to which the user is entitled. The user does not receive System Policy.

Upgrading the Computer Accounts

Persistent registry settings can be an issue when upgrading the computer accounts from Windows NT 4.0 to Windows 2000. While the client computer was subject to System Policy, its registry received settings outside the approved Group Policy trees, and these are not removed on the client when the domain controller is upgraded. You should look for unwanted residual effects of System Policy and take corrective steps, such as using Regini.exe, found in %systemroot%/System32/, to remove the old settings.

For example, Windows NT 4.0 has a Logon Banner policy. In Windows 2000, Logon Banner policy is handled differently, in Security Settings rather than using an Administrative Template. If you observe after upgrading the computer account that the Windows NT 4.0 Logon Banner policy is still in force, then reverse that setting on a one-time basis.

It is recommended that you avoid issues such as these by giving the client computer a freshly installed Windows 2000 operating system, rather than an upgrade. If you do this, there are no holdover Windows NT 4.0 registry settings.

User is Managed in a Windows NT 4.0 Account and Computer is Managed in a Windows 2000 Account

The computer account is in Active Directory, and the user account is not. The user account is managed by a Windows NT 4.0 domain controller.

Windows NT 4.0 resource domains (often containing computer accounts, printers, shared folders, and so on.) are often made into Windows 2000 organizational units in Active Directory. In this way, what were several Windows NT 4.0 resource domains can be handled in just one Windows 2000 domain. Because fewer computers are typically needed when upgrading resource domains in this way than when upgrading all the user accounts, this migration status is less common than the previous one.

System Startup

All Group Policy to which the computer is subject is applied to the computer when it boots.

User Logon

System Policy is applied to the user when the user logs on. If the local Group Policy object has changed since it was last processed, the following policy settings are applied: Local Group Policy for the user, followed by Windows NT 4.0 System Policy for the user. Computer System Policy is not applied.

Upgrading the User Accounts

During the time that the user accounts were managed by a Windows NT 4.0 domain controller, the client computers might have had their registries altered outside the approved Group Policy trees. When the domain controller holding the user accounts is upgraded to Windows 2000, these settings remain on the client computers unless the administrator undoes them by means of System Policy or — easier for the administrator — the client computers get fresh installations of Windows 2000.

Trust Relationships with Previous Versions of Windows

There is a subtle migration issue you need to avoid related to how trusts are handled in Windows NT 4.0 and how this relates to Windows 2000 upgrades.

Suppose you have a Windows 2000 domain controller (call it A) with a previous version trust relationship to a Windows NT 4.0 domain controller (call it B). You upgrade B to Windows 2000 and then link an organizational unit managed by A to a Group Policy object stored in B's domain. A user in the organizational unit logs on to A expecting to receive policy from the Group Policy object stored in B's domain — but it doesn't work. The reason is that the upgrade of the domain controller does not automatically upgrade the trust relationship, and the user won't have access to the Sysvol share on B.

To solve this problem, you need to break the trust after upgrading B to Windows 2000. Then create a new Windows 2000–style trust and the user receives Group Policy as expected.

Best Practices

Use Group Policy in Preference to Windows NT 4.0 System Policy

System Policy is undesirably persistent from a Windows 2000 perspective. Group Policy is cleaned up and refreshed whenever policy changes.

Disable Unused Parts of a Group Policy Object

If you notice that under the User Configuration or Computer Configuration node of the console, a Group Policy object only has settings that are **Not Configured**, then you can avoid processing those settings by disabling the node. This expedites startup and the logon session for those users and computers subject to the Group Policy object.

Disabling both parts of a Group Policy object makes it behave as if it is not linked to any site, domain, or organizational unit, even though the links still exist.

Use the Block Policy Inheritance and No Override Features Sparingly

Routine use of these feature makes it difficult to troubleshoot policy.

Minimize the Number of Group Policy Objects Associated with Users in Domains or Organizational Units

The more Group Policy objects are applied to a user, the longer it takes to log on.

Filter Policy Based on Security Group Membership

Keep in mind that a Group Policy object will not apply to a user if the Read or Apply Group Policy access control entries (ACEs) are not set to **Allow** on security groups of which the user is a member. This is the mechanism by which policy can be prevented from applying to users (or computers) who would otherwise be subject to it either by links or by inheritance. It is a good, efficient mechanism, and the administrator can greatly expedite the logon and startup experiences of the users in his or her organization by exploiting it fully.

Override User-Based Group Policy with Computer-Based Group Policy Only When Necessary

Do this only if you need the desktop configuration to be the same regardless of which user logs on.

Avoid Cross-Domain Group Policy Object Assignments

The processing of Group Policy objects slows the logon session and startup if Group Policy is obtained from another domain.

Additional Resources

- For the most recent information about Group Policy in Windows 2000 Server, see the Microsoft Windows 2000 Server link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For information about the administrative templates settings that are included with Windows 2000 Server, see the searchable reference file GP.chm on the Windows 2000 Server Resource Kit CD-ROM.
- For more information about Group Policy in Windows 2000 Server, see the ResourceLink link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For more information about the Group Policy API, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For information about the Group Policy API see the *Microsoft® Windows® 2000 Platform Software Development Kit*.
- For information about Microsoft Management Consoles (MMC), see the *Microsoft® Windows® 2000 Platform Software Development Kit.*
- For Group Policy walk-throughs, see the Windows 2000 Management Services link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Send feedback to Microsoft