



Operating System

Windows 2000 Group Policy

White Paper

Abstract

This paper describes Group Policy, one of the key IntelliMirror® management technologies provided for change and configuration management in Microsoft® Windows® 2000 operating system. Administrators use Group Policy to specify options for managed configurations for groups of computers and users. Group Policy includes options for registry-based policy settings, security settings, software installation, scripts, folder redirection, Remote Installation Services, and Internet Explorer maintenance.

This paper is intended for information technology managers and system administrators who are interested in using Group Policy to manage users' desktop environments.

© 2000 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Windows, IntelliMirror, Jscript, Active Directory, Visual C++, MS-DOS, Visual Basic, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0700

Contents

Introduction.....	1
Administrative Requirements for Using Group Policy	1
What this Paper Contains	1
Overview of Group Policy Infrastructure and Mechanics	3
Linking Group Policy Objects to Active Directory Containers	3
Group Policy Hierarchy	4
Using Security Groups to Filter the Scope of the Group Policy Object	5
MMC Snap-in Extension Model	8
Group Policy Snap-in Namespace	8
Delegating Group Policy.....	14
Using Security Groups to Delegate Group Policy	14
Specifying Group Policy to Control the Behavior of MMC extensions	17
Group Policy Extension Snap-ins	21
Administrative Templates	21
Security Settings	23
Software Installation	27
Scripts	27
Folder Redirection	31
Internet Explorer Maintenance	31
Remote Installation Services	33
Extending the Group Policy Functionality	35
Group Policy Processing.....	36
Initial Processing of Group Policy	36
Background refresh of Group Policy	37
Slow Links and Remote Access Issues	39
Client-side Processing of Group Policy	41
Server Processing	43
Specifying a Domain Controller for Setting Group Policy	45
Specifying a Domain Controller for Group Policy Editing by Using Preferences	45

Specifying a Domain Controller by Using Policy	46
Local Group Policy.....	48
Local Group Policy Object	48
Starting the Group Policy Snap-in on Windows 2000 Professional	49
Using the Group Policy Snap-in Focused on a Remote Computer	49
Local Group Policy Object Processing	50
Group Policy Loopback Support.....	51
Policy Settings for Group Policy	53
Specifying Policy Settings for Group Policy	53
Group Policy and Active Directory Sites	58
Setting up Group Policy on a Site	58
Design Considerations for Organizational Unit Structure and Use of Group Policy Objects.....	62
OU Structure	62
Design Principles	63
Design Examples	66
IntelliMirror Features without Active Directory.....	74
Roaming User Profiles and Logon Scripts	74
Folder Redirection	74
Internet Explorer Maintenance	74
Applying Administrative Templates (Registry-Based Policy)	74
Migrating Policy-Enabled Clients from Windows NT 4.0 to Windows 2000.....	79
Windows NT 4.0 and Windows 2000 Policy Comparison	79
Migrating to Windows 2000	80
Windows NT 4.0 Clients	83
Zero Administration Kit (ZAK) for Windows to Windows 2000 Upgrades	85

Appendix A: Security Settings and User Rights	90
Security Settings in the Default Domain Controllers Policy	91
Help for Windows NT 4.0 Administrators	94
Frequently Asked Questions about Security Settings	95
Appendix B: Group Policy Settings for Internet Explorer	97
Specifying Policy Settings for Internet Explorer Maintenance	97
Appendix C: Group Policy Storage	105
Group Policy Container	105
Group Policy Template	105
Registry.pol Files	108
Appendix D: Windows NT 4.0, Zero Administration Kit, and Windows 2000 Namespace Comparison	112
Appendix E: Frequently Asked questions	117
Infrastructure—Server side	117
Infrastructure—Client side	119
Group Policy Snap-in	121
General Issues	121
Glossary	124
For More Information	131
Management and Overview Papers	131
Technical Papers	132

Introduction

This paper is part of a series that describes Windows 2000 Group Policy. The first paper, "Introduction to Windows 2000 Group Policy," presented an overview of Group Policy. This paper provides more detailed technical information.

Group Policy provides directory-based desktop configuration management. In Windows 2000, you use Group Policy to define configurations for groups of users and computers. With Group Policy, you can specify settings for registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance. The Group Policy settings that you create are contained in a Group Policy object (GPO). By associating a GPO with selected Active Directory™ service system containers—sites, domains, and organizational units (OUs)—you can apply these settings to the users and computers in those Active Directory containers. To create GPOs, you use the Group Policy Microsoft Management Console¹ (MMC) snap-in.

Administrative Requirements for Using Group Policy

To make use of all of its features, Group Policy requires Active Directory and Windows 2000 clients. To set Group Policy for a selected Active Directory container, you must have a Windows 2000 domain controller installed, and you must have read and write permission to access the system volume of domain controllers (Sysvol folder) and modify rights to the currently selected directory container. The system volume folder is automatically created when you install a Windows 2000 domain controller (or promote a server to domain controller).

Note: Group Policy depends on Active Directory; therefore, it is crucial to understand Active Directory and its structure. It is highly recommended that you familiarize yourself with Active Directory concepts before implementing Group Policy.

To learn about Active Directory directory services, see the Active Directory white papers at <http://www.microsoft.com/windows2000/library/howitworks>. Information on planning and implementing Active Directory is available in the [Windows 2000 Server Resource Kit Deployment Planning Guide](http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp) at <http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp>.

What this Paper Contains

This paper presents information on the following topics:

[Overview of Group Policy Infrastructure and Mechanics](#)

[Delegating Group Policy](#)

[Group Policy Extension Snap-ins](#)

[Group Policy Processing](#)

¹ The Microsoft Management Console (MMC) provides an open, extensible, common console framework for management applications. MMC provides a unified user interface for hosting administrative tools, including snap-ins, to administer networks, computers, services, and other system components.

[Specifying a Domain Controller for Setting Group Policy](#)

[Local Group Policy](#)

[Group Policy Loopback Support](#)

[Policy Settings for Group Policy](#)

[Group Policy and Active Directory Sites](#)

[Design Considerations for Organizational Unit Structure and Use of Group Policy Objects](#)

[IntelliMirror Features without Active Directory](#)

[Migrating Policy-Enabled Clients from Windows NT 4.0 to Windows 2000](#)

[Security Settings and User Rights](#)

[Group Policy Settings for Internet Explorer](#)

[Group Policy Storage](#)

[Windows NT 4.0, Zero Administration Kit, and Windows 2000 Namespace Comparison](#)

[Frequently Asked Questions](#)

Overview of Group Policy Infrastructure and Mechanics

Group Policy uses a document-centric approach to creating, storing, and associating policy settings. Similar to the way in which Microsoft Word stores information in .doc files, Group Policy settings are contained in Group Policy objects (GPOs). By analogy, the Group Policy snap-in is to GPOs as Microsoft Word is to .doc files.

GPOs are associated with the following Active Directory containers: sites, domains, or OUs. The settings within the GPOs are then evaluated by the affected clients, using the hierarchical nature of the Active Directory.

To create Group Policy you use the Group Policy MMC snap-in, either as a stand-alone tool or as an extension to an Active Directory-related snap-in (such as the Active Directory Users and Computers snap-in or the Active Directory Sites and Services snap-in). The preferred method is to use the Group Policy snap-in as an extension to an Active Directory snap-in. This allows you to browse the Active Directory for the correct Active Directory container, and then define Group Policy based on the selected scope. To access Group Policy from either the Active Directory Users and Computers snap-in console or in the Active Directory Site and Services snap-in console, select the **Group Policy** tab from the **Properties** page of a site, domain, or organizational unit.

Linking Group Policy Objects to Active Directory Containers

Any site, domain, or OU may be associated with any Group Policy Object. As shorthand, we will use the acronym SDOU to mean a site, domain, or OU.

A given GPO can be associated (linked) to more than one site, domain, or OU. Conversely, a given site, domain, or OU can have multiple GPOs linked to it. In the case where multiple GPOs are linked to a particular site, domain, or OU, you can prioritize the order of precedence in which these GPOs are applied.

By linking GPOs to Active Directory sites, domains, and OUs, you can implement Group Policy settings for as broad or as narrow a portion of the organization as you want:

- A GPO linked to a site applies to all users and computers in the site.
- A GPO applied to a domain applies directly to all users and computers in the domain and by inheritance to all users and computers in child OUs. Note that policy is *not* inherited across domains.
- A GPO applied to an OU applies directly to all users and computers in the OU and by inheritance to all users and computers in child OUs.

GPOs are stored on a per-domain basis, however, you can link a site, domain, or OU to a GPO in another trusted domain, although this is not recommended in general for performance reasons.

To link a GPO to a site, use the Active Directory Sites and Services snap-in. To link a GPO to a domain or OU, use the Active Directory Users and Computers snap-in. In either tool, right-click the site, domain, or OU to which you want to link the GPO, and select **Properties**. Then select the **Group Policy** tab, which you use to create, edit, and manage GPOs.

The following illustration shows the Group Policy model of linking sites, domains, and OUs to Group Policy objects.

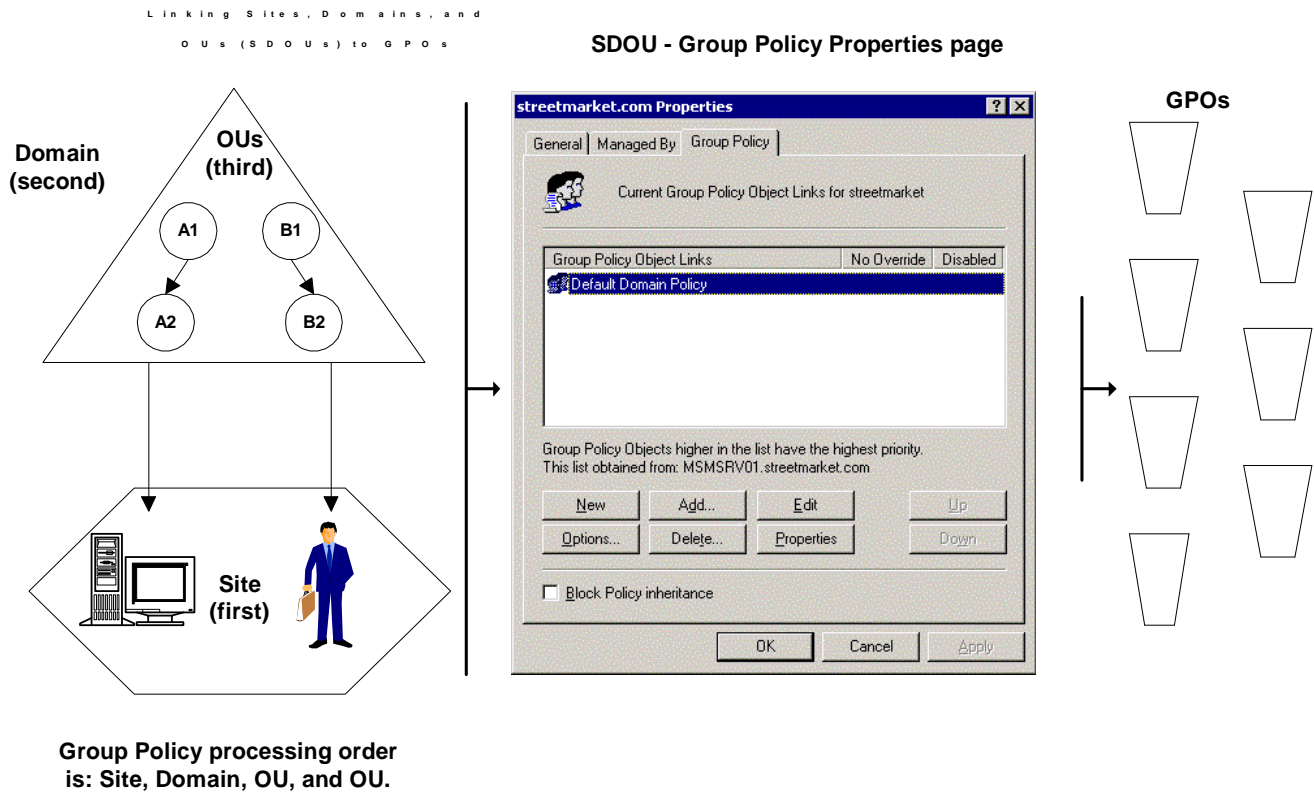


Figure 1. Linking Active Directory containers to Group Policy Objects

Group Policy Hierarchy

By default, Group Policy is inherited and cumulative, and it affects all computers and users in an Active Directory container. Group Policy objects are processed according to the following order:

1. The local Group Policy object (LPGO) is applied (See Local Group Policy section for details).
2. GPOs linked to sites.
3. GPOs linked to domains
4. GPOs linked to organizational units (OUs). In the case of nested OUs, GPOs associated with parent OUs are processed prior to GPOs associated with child OUs.

This order of GPO processing – local, site, domain, OU – is significant because policy applied later overwrites policy applied earlier.

No Override and Block Inheritance Policy Options

You can enforce the Group Policy settings in a specific Group Policy object by using the **No Override** option so that GPOs in lower-level Active Directory containers are prevented from overriding that policy. For example, if you have defined a specific GPO at the domain level and specified the **No Override** option, the policies that the GPO contains apply to all OUs under that domain; that is, the lower-level containers (OUs) cannot override that domain Group Policy.

You can also block inheritance of Group Policy from parent Active Directory containers by using the **Block policy inheritance** option. For example, if you specify the **Block policy inheritance** option for an OU, this prevents policy in higher-level Active Directory containers (such as a higher-level OU or domain) from applying. However, **No Override** policy options always take precedence.

Figure 1 below shows a sample domain structure to illustrate how Group Policy objects can be applied to containers in the Active Directory.

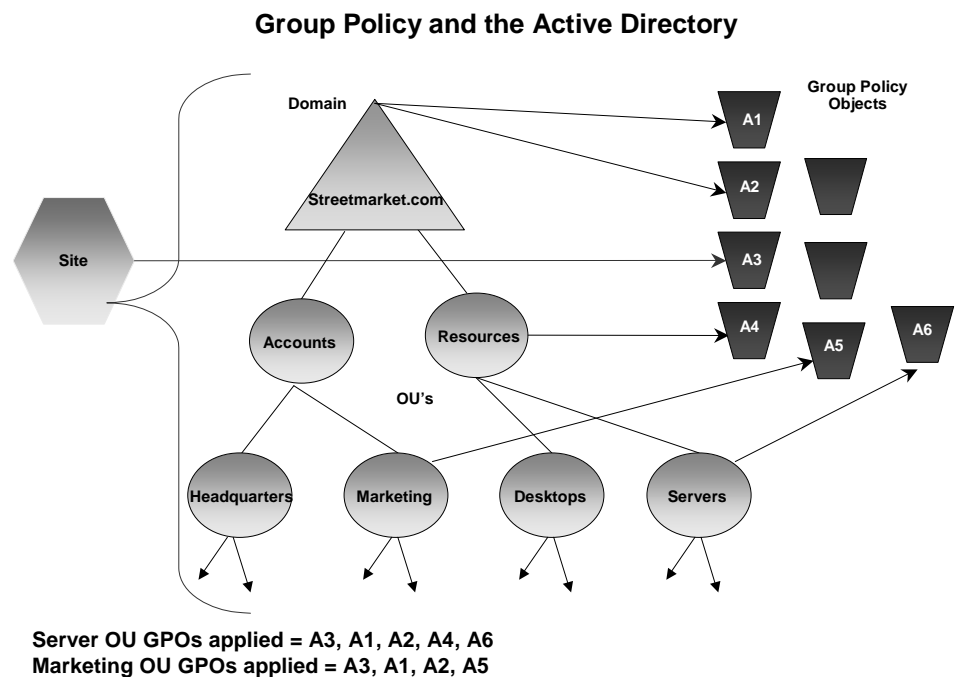


Figure 2. Group Policy and the Active Directory

Using Security Groups to Filter the Scope of the Group Policy Object

You can further refine which groups of computers and users a particular GPO influences by using Windows 2000 security groups. To do this, you use the

Security property page of a given GPO to set access permissions (discretionary access control lists², or DACLs) to allow or deny access to the GPO by specified groups.

You can view and modify the security settings from the **Security** tab on the **Properties** page of the specific GPO. The **Security** tab is accessible by right-clicking the root node in the Group Policy snap-in, clicking **Properties**, and then **Security**. Or from the **Properties** page of a given site domain, or OU, select the **Group Policy** tab, right-click the appropriate Group Policy object in the GPO list, select **Properties**, and then click **Security**.

By default, a GPO affects all users and computers that are contained in the linked site, domain, or OU. By changing the Access Control Entries (ACEs) within the DACL, the effect of any GPO can be modified to exclude or include the members of any security group.

Both Read and Allow Group Policy ACEs are required for a GPO to apply to a group. By default, authenticated users have both Apply Group Policy and Read ACE permissions set to **Allow**. Everyone in the organization is automatically an Authenticated User. Therefore, the default behavior is for every Group Policy object to apply to every Authenticated User. By default, domain administrators, enterprise administrators, and the local system have full control permissions, without the Apply Group Policy ACE. However, administrators are members of Authenticated Users, which means that they will receive the settings in the GPO by default.

To prevent GPO policy from applying to a specified group requires removal of the Apply Group Policy ACE from that group. If you remove the Apply Group Policy ACE (clear the **Allow checkbox**) for Authenticated Users, you can then explicitly grant this permission to individual security groups that should receive the policy settings. Alternatively, you could set Apply Group Policy to **Deny** for certain classes of users, such as administrators, that will never need that policy.

Note: Use the Deny ACE with caution. A Deny ACE setting for any group has precedence over any Allow ACE given to a user or computer because of membership in another group.

Best Practice: If you disallow Apply Group Policy for a GPO for some users, consider also disallowing Read access to those users. When the Read ACE is allowed and the Apply Group Policy is not, the GPO is still processed by the user even though it is not applied to the user. Therefore, to improve performance, you should remove the Read Access Control Entry to prevent the user from processing the GPO. In addition, removing Read access increases security. With Read access allowed, it is possible for an inquisitive user with considerable knowledge of the Active Directory to read the contents of that GPO, even if it's not applied to them. This may not be desirable in some cases, for example, a GPO for the Human Resources (HR) group. It might be advisable to limit Read access on GPOs that

² A discretionary access control list (DACL) is a list of permissions within a security descriptor.

affect the HR users to only those users.

Security groups and DACLs are also used to delegate control of Group Policy objects, as explained in [Delegating Group Policy](#).

MMC Snap-in Extension Model

The nodes of the Group Policy MMC snap-in are themselves MMC snap-in extensions. These extensions include Administrative Templates, Scripts, Security Settings, Software Installation, Folder Redirection, Remote Installation Services, and Internet Explorer maintenance. Extension snap-ins may in turn be extended. For example, the Security Settings snap-in includes several extension snap-ins. Developers can also create their own MMC extensions to the Group Policy snap-in to provide additional policies.

For more information on creating MMC extensions, see the Microsoft Management Console section of the Microsoft Platform SDK documentation at:

<http://msdn.microsoft.com/developer/sdk/platform.htm>.

By default, all the available Group Policy snap-in extensions are loaded when you start the Group Policy snap-in. You can modify this default behavior by creating a custom MMC console, or by using policy settings to control the behavior of MMC itself. The MMC options are accessed under the **User**

Configuration\Administrative Templates\Windows Components\Microsoft Management Console node. To find out more, see [Specifying Group Policy to Control the Behavior of MMC and Snap-ins](#), later in this document.

For further information on the Microsoft Management Console, see the "[Microsoft Management Console: Overview](#)" white paper at

<http://www.microsoft.com/windows2000/library/howitworks/management/mmcover.asp> and the "[Step-by-Step Guide to the Microsoft Management Console](#)" at <http://www.microsoft.com/windows2000/library/planning/mamagement/mmcsteps.asp>, both of which are available on the [Windows 2000 Web site](#), www.microsoft.com/windows2000.

Group Policy Snap-in Namespace

The root node of the Group Policy snap-in is displayed as the name of the GPO and the domain to which it belongs, in the following format:

GPO Name [DomainName.com] Policy

For example:

Default Domain Policy [HQ-RES-DC-01.reskit.com] Policy

Computer Configuration and User Configuration

Below the root node, the namespace is divided into two parent nodes: Computer Configuration and User Configuration. These are the parent folders that you use to configure Group Policy settings. Computer-related Group Policy is applied when the operating system boots and during the periodic refresh cycle, explained later in this document. User-related Group Policy is applied when users log on to the computer and during the periodic refresh cycle.

Extensions to the Group Policy Snap-in

Three nodes exist under the Computer Configuration and User Configuration parent nodes: Software Settings, Windows Settings, and Administrative Templates. The Software Settings and Windows Settings nodes contain extension snap-ins that extend either or both of the Computer Configuration or User Configuration nodes. Most of the extension snap-ins extend both of these nodes, but frequently with different options. The Administrative Templates node namespace contains all policy settings pertaining to the registry; it can be extended by using administrative template (.adm) files.

The Group Policy extension snap-ins include:

- **Administrative Templates.** This extension contains all registry-based policy settings, including those for the Windows 2000 operating system and its components, and any registry-based policy settings provided by applications. You use these policies to mandate registry settings that control the behavior and appearance of the desktop, the operating system components, and applications that provide registry-based policy. This node uses administrative template (.adm) files to specify the registry settings that can be modified through the Group Policy snap-in user interface. For more information on .adm files, see [Administrative Templates](#) later in this paper.
- **Security Settings.** The Security Settings extension is used 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. For more information on security settings, see [Security Settings](#) and [Appendix E: Security Settings](#), later in this paper, and the security white papers available on the [Windows 2000 Server Web site](http://www.microsoft.com/windows2000/library/technologies/security/default.asp) at <http://www.microsoft.com/windows2000/library/technologies/security/default.asp>.
- **Software Installation.** You can use the Software Installation snap-in to centrally manage software in your organization. You can assign and publish software to users and assign software to computers. For detailed information on software installation, see [Software Installation](#), later in this document, and the "[Software Installation and Maintenance](#)" white paper at <http://www.microsoft.com/windows2000/library/operations/management/siamwp.asp>.
- **Scripts.** Scripts are used to automate tasks at computer startup and shutdown, and at user logon and logoff. You can use any language supported by Windows Scripting Host. These include the Microsoft Visual Basic® development system, Scripting Edition (VBScript), JavaScript, PERL, and MS-DOS®-style batch files (.bat and .cmd). See [Scripts](#), later in this document, and the Microsoft Scripting Technologies website at <http://msdn.microsoft.com/scripting/default.htm> for more information.

-
- **Remote Installation Services.** Remote Installation Services (RIS) is used to control the behavior of the Remote Operating System Installation feature as displayed to client computers. See [Remote Installation Services](#), later in this document, and the "[Remote Operating System Installation](#)" white paper at <http://www.microsoft.com/windows2000/library/planning/management/remoteos.asp>.
 - **Internet Explorer Maintenance.** Internet Explorer Maintenance is used to manage and customize Internet Explorer on Windows 2000-based computers. You can also export settings for Windows 95, Windows 98, and Windows NT 4.0 clients (the settings are exported into an .ins and .cab file format for those platforms). Administrators can set options for Browser UI, connections, URLs, proxy settings, security zones, and Favorites and Channels. See [Internet Explorer Maintenance](#), later in this document, and the MS Internet Explorer 5.0 Resource Kit Tools and Utilities at <http://www.microsoft.com/TechNet/IE/reskit/ie5/tools.asp>.
 - **Folder Redirection.** You can use Folder Redirection to redirect Windows 2000 special folders from their default user profile location to an alternate location on the network. These special folders include My Documents, Application Data, Desktop, and the **Start** menu. See [Folder Redirection](#), later in this document, and the "[User Data and Settings Management](#)" white paper at <http://www.microsoft.com/windows2000/library/operations/management/settings.asp>.

Information on extending the functionality of the Group Policy snap-in can be found in a white paper called "Implementing Registry-Based Group Policy for Applications," which is being posted at <http://www.microsoft.com/windows2000/library/howitworks/default.asp>

Figure 3 below shows the Group Policy snap-in.

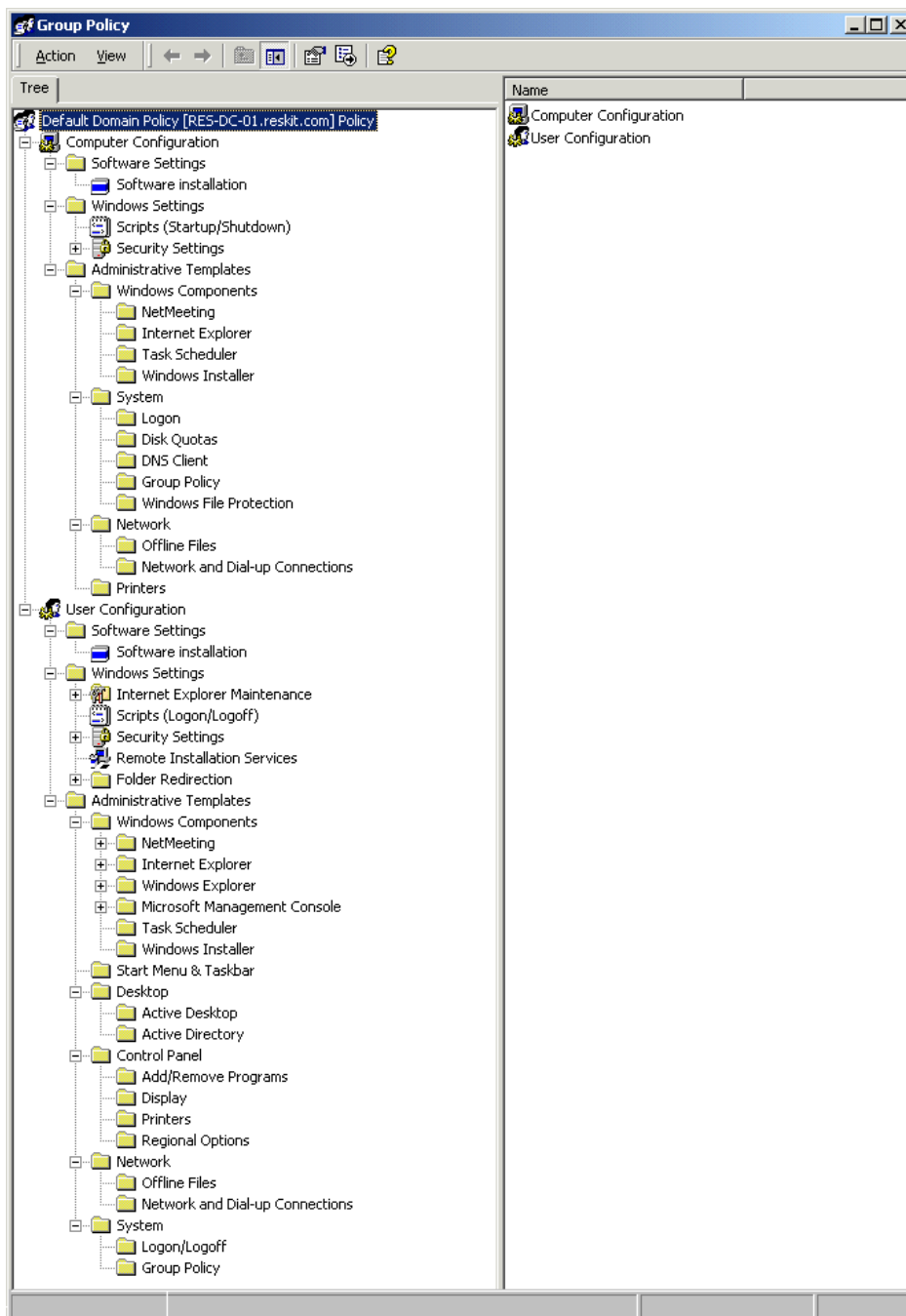


Figure 3. The Group Policy snap-in console

Client-side Extensions to Group Policy

Some 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.

For more information on the client-side extensions, see the [Client-side Processing of Group Policy](#) section later in this paper.

Group Policy Storage

A Group Policy object is a virtual object. The policy setting information of a GPO is actually stored in two locations: the Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC is an Active Directory container that stores GPO properties, including information on version, GPO status, and a list of components that have settings in the GPO. The GPT is a folder structure within the file system that stores Administrative Template-based policies, security settings, script files, and information regarding applications that are available for Software Installation. The GPT is located in the system volume folder (Sysvol) in the \Policies sub-folder for its domain.

It is possible to store data related to policy information outside the GPO. However, this requires that at least a link to the data be stored either in the GPC or the GPT. This is *not* recommended because it could complicate back up and restore procedures. In addition, the information outside the GPO may not be deleted if you delete the GPO, whereas Windows 2000 will automatically delete the information from the GPC and GPT.

Replication of a GPO to other domain controllers happens through two different mechanisms. The GPC is replicated by using Active Directory replication, whereas the GPT is replicated using File Replication Service (FRS). The settings from a GPO are only applied when the GPC and GPT are synchronized. GPOs are identified by their globally unique identifiers (GUIDs) and stored at the domain level.

The following illustration shows the interaction between the Group Policy snap-in, a GPO, and the storage location of the data contained in the GPO.

The Group Policy Model Storage

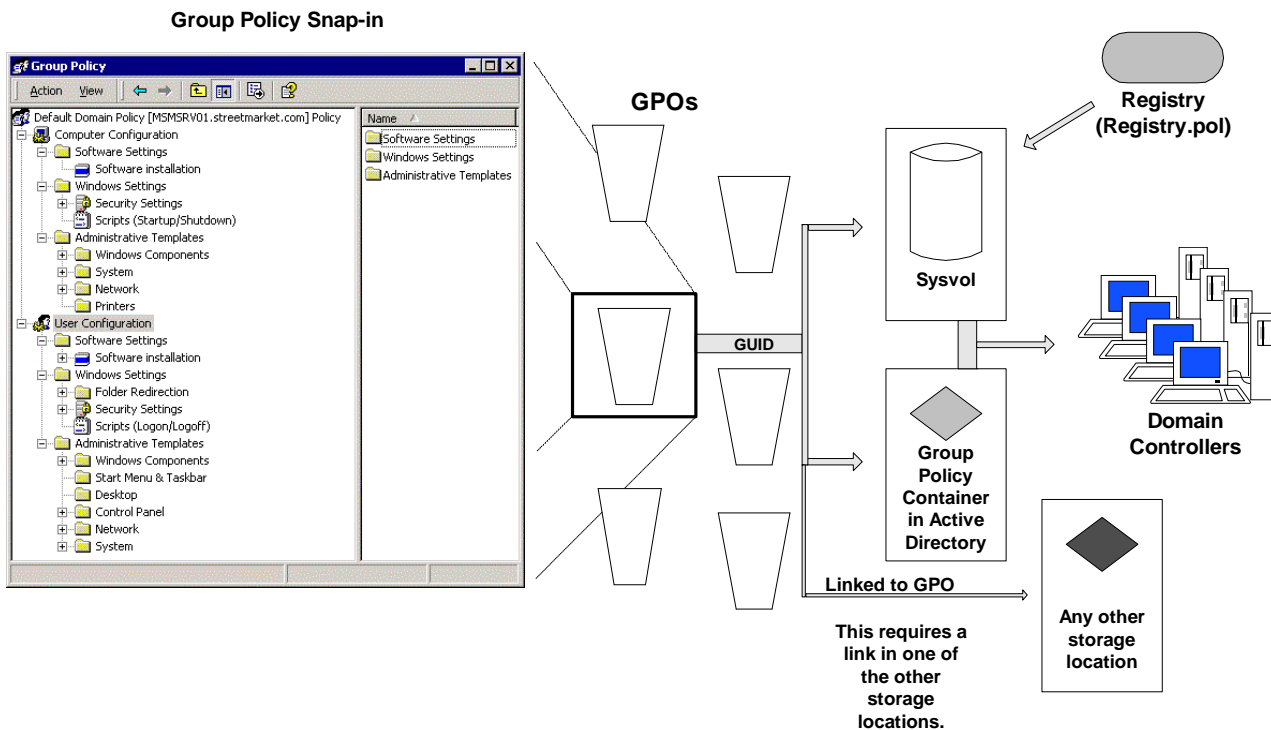


Figure 4. Group Policy and storage

For additional information on storage of Group Policy information, see [Appendix C: Group Policy Storage](#), later in this paper.

Delegating Group Policy

One of the features of the Active Directory is its ability to delegate control of portions of the directory service. This section explains how Group Policy fits in with the delegation of sites, domains, and organizational units.

The delegation of Group Policy consists of the following 4 aspects, which can be used together or separately, as a particular situation requires:

- Managing Group Policy links for a site, domain, or OU
- Editing Group Policy Objects
- Creating Group Policy Objects
- Specifying Group Policy to Control the Behavior of MMC extensions

The underlying mechanism for achieving delegation using the first three methods is the application of the appropriate DACLs to Group Policy objects and other objects in the Active Directory. This mechanism is identical to using security groups to filter the application of Group Policy objects to various users, as described earlier in this paper.

The fourth method of delegation relies on several policy settings within the Group Policy infrastructure that are designed to control the behavior of the MMC and MMC snap-ins. For example, you can use Group Policy to manage the rights to create, configure, and use MMC consoles, and to control access to individual snap-ins.

Using Security Groups to Delegate Group Policy

The following table lists the default 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, administrators are also authenticated users, which means that they have the **Apply Group Policy** attribute set. If this is not desired, administrators have two choices:

- Remove Authenticated Users from the list on the security tab of the GPO, and add a new security group with the Apply Group Policy and Read attributes set to **Allow**. This new group should contain all the users that 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 GPO from being applied to members of those groups. Remember that an ACE set to **Deny** always takes precedence over **Allow**. Therefore, if a given user is a member of another group that is set to explicitly **Allow** the Apply Group Policy attribute for this GPO, it will still be denied.

Managing Group Policy Links for a Site, Domain, or OU

The **Group Policy** tab in the **Properties** page for a site, domain, or OU allows the administrator to specify which Group Policy objects are linked to this site, domain, or OU. 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 objects and the **gPOptions** property contains the **Block Policy Inheritance** setting.

To manage GPO links to a site, domain, or OU, you must have read and write access to the **gPLink** and **gPOptions** properties. By default, domain administrators have this permission for domains and OUs, and only Enterprise Administrators and Domain Administrators of the forest root domain can manage links to sites.

The Active Directory supports security settings on a per-property basis. This means that a non-administrator can be given read and write access to specific properties. In this case, if non-administrators have read and write access to the **gPLink** and **gPOptions** properties, they can manage the list of GPOs linked to that site, domain, or OU. To give a user Read and Write access to these properties, use the **Delegation Wizard** and select the **Manage Group Policy links** predefined task.

Example 1

In this example, control of an organizational unit is delegated to a non-administrative user so that a user or group of users can select from existing Group Policy Objects and apply them to users, but not create new Group Policy Objects.

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

The user or the members of the group that you selected in step 4 will be able to change the list of Group Policy links for the OU selected in step 1.

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 GPOs, 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 GPO, that user becomes the creator and owner of the GPO; therefore, the user can edit the GPO. Being a member of the Group Policy Creator Owners group gives the non-administrator full control of *only* those GPOs that the user creates or those explicitly delegated to that user; it does not give the non-administrator any additional rights over other GPOs for the domain—these users are *not* granted rights over GPOs they didn't create.

Note that when an administrator creates a GPO, the Domain Administrators group becomes the Creator Owner of the Group Policy Object.

When delegating to non-administrators, you should also consider delegating the ability to manage the links for a specific OU. The reason is that by default, non-administrators cannot manage links, and this will prevent them from being able to use the Active Directory Users and Computers snap-in to even create a Group Policy object. There is a work-around whereby these users can create a custom MMC console, and they can create a GPO when they select the **All** tab.

Example 2

In this example, control of an organizational unit is delegated to a non-administrator user so that the user or group of users can select from existing Group Policy objects and also create new Group Policy objects.

1. First, complete all the steps in Example 1 above.
2. To allow for creation of new Group Policy objects, you need to add the user or group of users to the Group Policy Creator Owners group. In the Active Directory Users and Computers tools, navigate to the **Users** container in the root of the domain.
3. Double-click **Group Policy Creator Owners**.
4. In the **Properties** page, select the **Members** tab.
5. Press **Add**, and add the group of users (or user) selected above to the security group.

The user or group of users will be able to create new Group Policy objects. The user who creates each object becomes the Creator Owner of that GPO.

Editing Group Policy Objects

To edit a GPO, the user must have both read and write access to the GPO. For the current release of the product, read-only support for opening a GPO is *not* provided.

To edit a GPO, the user must be one of the following:

- An administrator.
- A Creator Owner.
- A user with delegated access to the GPO. That is, an administrator, or the Creator Owner, must have provided to this user both read and write access to the GPO by using the Security tab in the GPO Properties page.

By default, Domain Administrators, Enterprise Administrators, the operating system, and the GPO Creator Owner can edit GPOs because they have full control of GPOs without the **Apply Group Policy** attribute.

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 on the root node, select **Properties**, and click **Security**.
3. Press **Add** to add the user or group of users, and give them read and write access. At this point, decide whether the users should also have the policy applied to them or just be able to edit it. If they do not need the policy applied to them, clear the **Apply Group Policy** option.
4. Press **OK** to save the changes.

The user or group of users () will be able to edit the Group Policy object.

Specifying Group Policy to Control the Behavior of MMC extensions

Windows 2000 Group Policy includes several policy settings designed to control the behavior of MMC snap-ins. For example, you can use Group Policy to manage the rights to use MMC snap-ins.

Restricting Access to a List of Permitted Snap-ins

Administrators can specify which MMC snap-ins may be run by the affected user and which may not. This may be specified to be inclusive, which only allows a set of snap-ins to run, or it may be set as exclusive, which does not allow a set of snap-ins to run.

To create a list of permitted snap-ins for users, enable the **Restrict users to the explicitly permitted list of snap-ins** policy. When this policy is enabled, only permitted snap-ins can be run. If this policy is disabled or not configured, all snap-ins are permitted, except those you explicitly prohibit.

This policy is available in the Group Policy console under the **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console** node. For more information on this policy setting, double-click the policy in the details pane, and click the **Explain** tab.

Controlling Access to a Snap-in

To restrict or explicitly permit access to a particular snap-in, navigate to **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins\Group Policy** in the console tree. In the details pane, double-click the snap-in that you want to permit or restrict, and then select an option. For more information on these policy settings, double-click the desired policy in the details pane, and click the **Explain** tab, as shown in Figure 5, below.

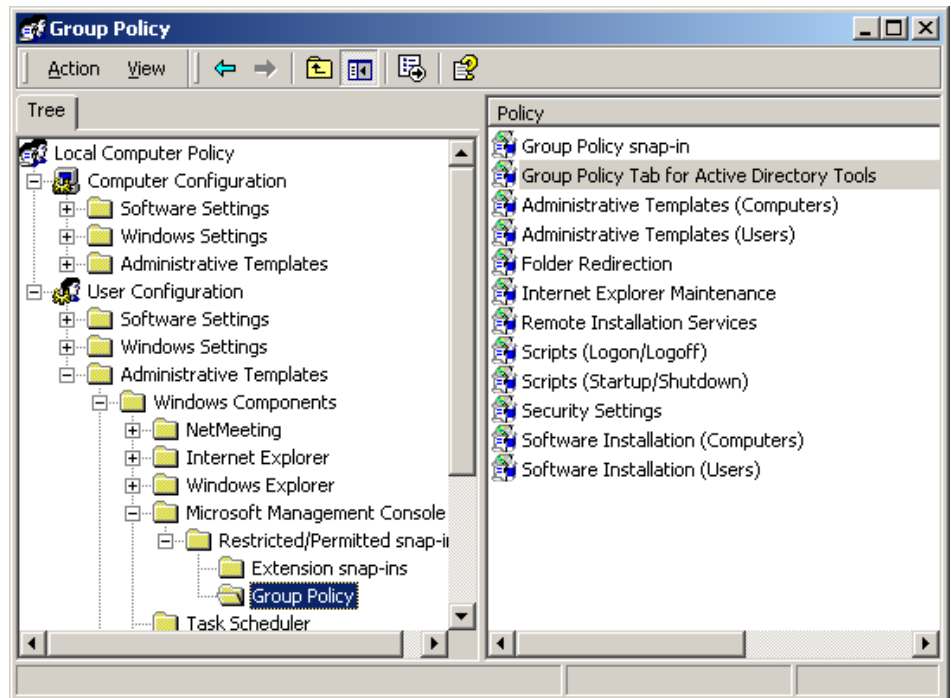


Figure 5. Controlling access to a snap-in

Preventing Use of MMC in Author Mode

Administrators can enable the **Restrict the user from entering author mode** policy in order to prevent users from using MMC in author mode. This policy is available in the Group Policy console under the **User Configuration\Administrative Templates\Windows Components\Microsoft Management Console** node.

For more information on these policy settings, double-click the policy in the details pane, and then click the **Explain** tab in the policy **Properties** dialog box.

Creating Custom Group Policy Snap-in Consoles

You can create custom Group Policy MMC consoles (.msc files), which include only a subset of the Group Policy snap-in extensions. You can combine this with the use of the policy settings above to provide a customized tool. For example, you could 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.

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

1. Click **Start**, click **Run**, type **MMC**, and then press **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 Standalone 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 GPO you want to manage, and then click **OK**.

-
6. Click **Finish** in the **Select Group Policy Object** dialog box, and then click **Close** in the **Add Standalone Snap-in** dialog box.
 7. Select the **Extensions** tab, and select the extension snap-ins you want to use.
 8. Click **OK**. The Group Policy snap-in opens with focus on the GPO you specified.
 9. After you specify the policies you want to use, click **Save As** on the **Console** menu to save your settings (in a .msc file).

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

Group Policy Extension Snap-ins

The Group Policy extension snap-ins constitute the main nodes in the Group Policy snap-in namespace; they are all loaded by default when the Group Policy snap-in is started. You can modify which extensions are loaded by creating custom consoles for Group Policy, and by specifying policy settings for MMC. For more information, see [Creating Custom Group Policy Snap-in Consoles](#) and [Specifying Group Policy to Control the Behavior of MMC and Snap-ins](#) in this document.

This section presents additional information on the following topics:

- [Administrative Templates](#)
- [Security Settings](#)
- [Software Installation](#)
- [Scripts \(Startup/Shutdown and Logon/Logoff\)](#)
- [Folder Redirection](#)
- [Internet Explorer Maintenance](#)
- [Remote Installation Services](#)

Administrative Templates

In Windows NT 4.0, the System Policy Editor uses files called *administrative templates* (.adm files) to determine which registry settings can be modified. These files define which settings are displayed by the System Policy Editor user interface.

In Windows 2000, the Administrative Templates node of the Group Policy snap-in uses administrative template (.adm) files to specify the registry settings that can be modified through the Group Policy snap-in user interface.

The Administrative Templates node includes all registry-based Group Policy information. This includes Group Policy for the Windows 2000 operating system and its components and for applications. Policy settings pertaining to a user who logs on to a given workstation or server are written to the **User** portion of the registry database under **HKEY_CURRENT_USER (HKCU)**. Computer-specific settings are written to the **Local Machine** portion of the registry under **HKEY_LOCAL_MACHINE (HKLM)**.

The .Adm File

.Adm files are Unicode files which consist of a hierarchy of categories and subcategories that define how the options are displayed through the Group Policy snap-in UI. They also indicate the registry locations where changes should be made if a particular selection is made, specify any options or restrictions (in values) that are associated with the selection, and in some cases, indicate a default value to use if a selection is activated. Windows 2000 includes three .adm files, System.adm, Inetres.adm, and Conf.adm, which contain all the settings initially displayed in the Administrative Templates node. It also includes .adm files for use with the Windows NT 4.0 System Policy Editor tool, as noted in the following table.

.Adm file	Use	Description
System.adm	Windows 2000	Loaded by default.
Inetres.adm	Windows 2000	Loaded by default.
Conf.adm	Windows 2000	Loaded by default.
Winnt.adm	Windows NT 4.0	Use with System Policy Editor, Poedit.exe.
Common.adm	Windows NT 4.0, Windows 95, and Windows 98	Use with System Policy Editor, Poedit.exe.
Windows.adm	Windows 95 and Windows 98	Use with System Policy Editor, Poedit.exe.

Distinguishing True Policies from Group Policy Preferences

In Windows 2000, all shipping policies set registry keys and values in either the **\Software\Policies** (the preferred location for all new policies) or **\Software\Microsoft\Windows\CurrentVersion\Policies** trees, in either **HKCU** or **HKLM**.

Policy settings that are stored in these specific locations of the registry are known as *true policies*. Storing settings here has the following advantages:

- These trees are secure and cannot be modified by a non-administrator.
- When Group Policy changes, for any reason, these trees are cleaned, and the new policies are then rewritten.

This prevents the behavior that was often present in Windows NT 4.0, whereby System Policies resulted in persistent settings in the user and computer registry. The policy remained in effect until the value was reversed, either by a counteracting policy or by editing the registry. These settings are stored outside the approved registry locations above and are known as *preferences*.

All the policy settings in the System.adm, Inetres.adm, and Conf.adm files use registry settings in the Policies trees of the registry. This means that they will *not* cause persistent settings in the registry when the GPO that applies them is no longer in effect.

By default, only true policies are displayed in the Group Policy snap-in. The following .adm files are loaded:

- System.adm: contains operating system settings
- Inetres.adm: contains Internet Explorer restrictions
- Conf.adm: contains NetMeeting settings

Note: Because of the persistent nature of non-policy settings, they should be avoided.

It is still possible for administrators to add an additional .adm file that sets registry values outside of the Windows 2000 Group Policy trees mentioned previously. These settings might be more appropriately referred to as preferences because the user, application, or other parts of the system can also change them. In this case, the administrator is ensuring that this registry key or value is set in a particular way. Although it is possible to add any .adm file to the namespace, if you use an .adm file from a previous version of Windows, the registry keys are unlikely to have an effect on Windows 2000, or they actually set preference settings and mark the registry with these settings; that is, the registry settings persist.

Viewing Group Policy Preferences

There is a user preference that allows preferences to be displayed in the Group Policy user interface; it is called **Show Policies Only** and is located in the **View** menu of the MMC. The ability to clear the checkbox for this setting and allow non-policy settings to be displayed may be prevented by using a policy setting located in **User Configuration\Administrative Templates\System\Group Policy**. If the preference (or policy) is not set to **Show Policies Only**, the icon for those settings is displayed in red. True policies are displayed in blue. Note that it is not possible for the selected state for this policy to persist; that is, there is no preference for this policy setting.

A Group Policy called **Enforce Show Policies Only** is available in **User Configuration\Administrative Templates**, under the **System\Group Policy** nodes. If you set this policy to **Enabled**, the **Show policies only** command is turned on and administrators cannot turn it off; in addition, the Group Policy snap-in displays only true policies. If you set this policy to **Disabled** or **Not configured**, the **Show policies only** command is turned on by default; however, you can view preferences by turning off the **Show policies only** command. To view preferences, you must turn off the **Show policies only** command, which you access by selecting the **Administrative Templates** node (under either the **User Configuration** or the **Computer Configuration** node), and then clicking the **View** menu on the Group Policy console and clearing the **Show policies only** check box.

In Group Policy, preferences are indicated by a red icon to distinguish them from true policies, which are indicated by a blue icon.

Use of non-policies within the Group Policy infrastructure is strongly discouraged because of the persistent registry settings behavior mentioned previously. To set registry policies on Windows NT 4.0, Windows 95, and Windows 98 clients, use the Windows NT 4.0 System Policy Editor tool, Poedit.exe.

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 the Group Policy application.

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 the following:

- **Account Policies.** These are computer security settings for password policy, lockout policy, and Kerberos policy in Windows 2000 domains.
- **Local Policies.** These include security settings for audit policy, user rights assignment, and security options. Local policy allows you to configure who has local or network access to the computer and whether or how local events are audited.
- **Event Log.** This controls security settings for the Application, Security, and System event logs. You can access these logs using the Event Viewer.
- **Restricted Groups.** Allows you to control who should and should not belong to a restricted group, as well as which groups a restricted group should belong to. This allows administrators to enforce security policies regarding sensitive groups, such as Enterprise Administrators or Payroll. For example, it may be decided that only Joe and Mary should be members of the Enterprise Administrators group. Restricted groups can be used to enforce that policy. If a third user is added to the group (for example, to accomplish some task in an emergency situation), the next time policy is enforced, that third user is automatically removed from the Enterprise Administrators group.
- **System Services.** These control startup mode and security options (security descriptors) for system services such as network services, file and print services, telephone and fax services, Internet and intranet services, and so on.
- **Registry.** This is used to configure security settings for registry keys including access control, audit, and ownership. When you apply security on registry keys, the Security Settings extension follows the same inheritance model as that used for all tree-structured hierarchies in Windows 2000 (such as the Active Directory and NTFS). Microsoft recommends that you use the inheritance capabilities to specify security only at top-level objects, and redefine security only for those child objects that require it. This approach greatly simplifies your security structure and reduces the administrative overhead that results from a needlessly complex access-control structure.
- **File System.** This is used to configure security settings for file-system objects, including access control, audit, and ownership.
- **Public Key Policies.** You use these settings to:
 - Specify that computers automatically submit a certificate request to an enterprise certification authority and install the issued certificate.
 - Create and distribute a certificate trust list.
 - Establish common trusted root certification authorities.
 - Add encrypted data recovery agents and change the encrypted data recovery policy settings.

-
- **IP Security Policies on Active Directory.** IP Security (IPSec) policy can be applied to the GPO of an Active Directory object. This propagates that IPSec policy to any computer accounts affected by that Group Policy object.

For more information on security settings and IPSec issues, refer to the [Windows 2000 Server Online Help](http://www.microsoft.com/windows2000/support/online/docs/default.asp) at <http://www.microsoft.com/windows2000/support/online/docs/default.asp>.

Windows 2000 Default Security Templates

Windows 2000 includes three default security templates called *Basic*. These new default security settings are applied to Windows 2000 systems that have been installed onto an NTFS partition. When Windows 2000 is installed onto a FAT file system, security cannot be applied.

The following Basic security templates are used:

- Basicwk.inf for workstations
- Basicsv.inf for servers
- Basicdc.inf for domain controllers

The Basic security templates specify default Windows 2000 security settings for all security areas, with the exception of User Rights and Groups. These templates can be applied to Windows 2000 systems using the Security Configuration and Analysis MMC snap-in or by using the Secedit.exe command-line tool.

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 were constructed based on the assumption that they would be applied to Windows 2000 computers that are configured with the new Windows 2000 default security settings. In other words, these templates *incrementally* modify the default security settings. They do not include the default security settings plus the modifications.

The following table lists the incremental security templates included in Windows 2000.

Security Configuration	Computer	Templates	Description
Compatible	Workstation, and server	Compatws.inf	For customers who do not want their users to run as Power Users (by default all users are Power Users on Windows 2000 professional), the Compatible configuration opens up the default permissions for the Users group so that legacy applications are more likely to run. Office 97 should run successfully when users are logged on as a User to a Windows 2000 computer that has had the Compatible security template applied over the default settings. Note that this is not considered a secure environment.
Secure	Workstation, server, and domain controller	Securews.inf and Securedc.inf	The Secure configuration provides increased security for areas of the operating system that are not covered by permissions. This 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 configurations because the secure configurations assume that default Windows 2000 security settings are in effect.
Highly Secure	Workstation, server, and domain controller	Hisecws.inf and Hisecdc.inf	The Highly Secure configuration is provided for Windows 2000 computers that operate in native (or pure) Windows 2000 environments <i>only</i> . In this configuration, it is required that all network communications be digitally signed and encrypted at a level that can only be provided by Windows 2000. Thus, a Windows 2000 highly secure computer cannot communicate with a Windows 95, Windows 98, or Windows NT client.

Security Levels

The following table describes the relative levels of security that can be associated with the operating system, based on the templates that have been applied and the type of user accessing the system. No inference should be made with respect to the security of applications running in this environment. The items are listed in the table in order of increasing security level.

Templates applied	User level
Default	Power User
Default + Compatible	User
Default	User
Default + Secure	User
Default + Secure + Highly Secure	User

Thus, logging in as a Power User to a Windows 2000 system that has been installed onto an NTFS system can be less secure than logging into that same system as a User.

For more information on security settings, see the ["Step-by-Step Guide to Configuring Enterprise Security Policies"](http://www.microsoft.com/windows2000/library/planning/security/entsecsteps.asp) at <http://www.microsoft.com/windows2000/library/planning/security/entsecsteps.asp>,

and the "[Step-by-Step Guide to Internet Protocol Security \(IPSec\)](#)" at <http://www.microsoft.com/windows2000/library/planning/security/ipsecsteps.asp>. For information on the default security settings contained in the Default Domain Policy GPO and Default Domain Controller Policy GPO, see [Appendix A: Security Settings and User Rights](#) later in this paper.

Software Installation

You 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 computers.

You *assign* applications to groups of users so that all users who require the applications automatically have the application on their desktops—without requiring the administrator or technical personnel to set up the application on each desktop. When you assign an application to a group of users, you are actually *advertising* the application on all the users' desktops. The next time a user logs on to Microsoft Windows 2000, the application is advertised. This means that 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 on the user's computer, the application is installed the first time the user activates the application.

When the user selects the application from the **Start** menu the first time, it sets up automatically, and then opens.

You can also *publish* applications to groups of users, making the application available for users to install should 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. Published applications store their advertisement information in the Active Directory.

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. Alternatively, if the administrator has configured this feature, users can open a document file associated with a published application (for example, an .xls file to install Microsoft Excel).

For more information, see the "[Software Installation and Maintenance](#)" white paper at <http://www.microsoft.com/windows2000/library/operations/management/siamwp.asp> and the [Step-by-Step Guide to Software Installation and Maintenance](#) at <http://www.microsoft.com/windows2000/library/planning/management/swinstall.asp>.

Scripts

With the Scripts extensions, you can assign scripts to run when the computer starts

or shuts down or when users log on or off their computers. For this purpose, you can use Windows Scripting Host to include both Visual Basic® Scripting Edition (VBScript) and Jscript® development software script types.

Windows 2000 includes Windows Scripting Host, a language-independent scripting host for 32-bit Windows platforms. Microsoft anticipates that other software companies will provide ActiveX® scripting engines for other languages, such as Perl, TCL, REXX, and Python.

For more information about Windows Scripting Host, see <http://www.microsoft.com/scripting>.

The names of scripts and their command lines (in the form of registry keys and values) are stored in the Registry.pol file, described later in this document.

Types of Scripts

The five script types are as follows:

- Group Policy logon scripts.
- Group Policy logoff scripts.
- Group Policy startup scripts.
- Group Policy shutdown scripts.
- Legacy logon scripts (those specified on the User object). This includes support for Windows Scripting Host³ scripts. Windows Script Host supports scripts written in VBScript or JavaScript. This means that you can now enter a command line like *sample.vbs* in the logon script path of the user object.

Note: Consider carefully how to use such scripts if you have a mixed environment that includes Windows NT 4.0, Windows 95, Windows 98, and Windows 2000 clients. The Windows 2000 and the Windows 98 clients will properly run .vbs and .js scripts. To run .vbs and .js scripts on Windows NT 4.0 and Windows 95 clients, you must embed the scripts in batch (.bat) files. The scripts continue to run in a normal window. There is a policy that allows for scripts to be run as hidden or minimized. You can also install Windows Scripting Host on Windows NT 4.0 and Windows 95 clients. For information on Windows Scripting Host, see <http://msdn.microsoft.com/scripting/windowshost/default.htm>.

By default, each of these script types runs asynchronously, and the window is

³ Windows Script Host serves as a controller of ActiveX scripting engines. With Windows Script Host, you can run scripts directly in Windows 2000 by clicking a script file on the desktop or by typing the name of a script file at the command prompt.

hidden. User logon and logoff scripts run as the user (not administrator), and computer logon and logoff scripts run as local system.

Specifying Policy Settings for Script Behavior

The following table lists the Group Policy options that are available to control the behavior of scripts.

Policy in Computer Configuration\Administrative Templates\System\Logon	Description
Run logon scripts synchronously	When this option is enabled, the system waits until the script finishes running before it starts Windows Explorer. Note that an equivalent option for this is available under the User Configuration node. The policy setting you specify in the Computer Configuration node has precedence over that set in the User Configuration node.
Run startup scripts asynchronously	By default, startup scripts run synchronously and hidden, which means the user cannot logon until the scripts complete. In some corporations, the administrator might want the scripts to run asynchronously since they could take a long time to complete. This policy allows the administrator to change the default behavior.
Run startup scripts visible	If this option is enabled, startup scripts run in a command window.
Run shutdown scripts visible	If this option is enabled, shutdown scripts run in a command window.
Maximum wait time for Group Policy scripts	This policy setting lets you change the default script timeout period. (By default, scripts will timeout after 600 seconds). The range is 0 to 32000 seconds.

Policy in User Configuration\Administrative Templates\System\Logon/Logoff	Description
Run logon scripts synchronously	When you enable this option, Windows waits for the scripts to finish running before it starts Windows Explorer. Note that an equivalent option for this is available under the Computer Configuration node. The policy setting you specify in the Computer Configuration node has precedence over that set in the User Configuration node.
Run legacy logon scripts hidden	If this option is enabled, legacy logon scripts will run in hidden mode.
Run logon scripts visible	If this option is enabled, logon scripts run in a command window.
Run logoff scripts visible	If this option is enabled, logoff scripts run in a command window.

Note: Scripts that run hidden (and to a lesser degree minimized) can cause an errant script or one that prompts for user input to wait for 600 seconds. This is the default wait-time value and may be changed using a Group Policy. During this time, the system appears to be hung up. In the case of a script running in a minimized window, if the user selects the window, its processing can be stopped.

Best Practice: For easier manageability, it is a good idea to use Group Policy scripts and to avoid using per-user scripts, if at all possible. Rather than using a single monolithic script with lots of internal logic branching, Group Policy-based logon scripts allow for use of tiered and modular scripts targeted to the desired set of users.

Folder Redirection

The Folder Redirection extension is used 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

For example, you could redirect a user's My Documents folder to \\Server\Share\%username%. By redirecting the My Documents folder, you can provide the following advantages:

- Ensure that users' documents are available when they roam from one computer to another.
- 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 (RUP). This means that the My Documents folder and its contents are copied back and forth between the client computer and the server when users log on and log off. Relocating the My Documents folder outside of the user profile can significantly decrease that time.
- Store user data on the network (rather than on the local computer). The data can then be managed and protected by the Information Technology department.
- Make users' network-based My Documents folder available to users when they are disconnected from the corporate network by using Offline Folder technologies.

More information on Folder Redirection will be available in a white paper called "User Data and Settings Management" at <http://www.microsoft.com/windows2000/library/operations/management/settings.asp>

Internet Explorer Maintenance

The Internet Explorer Maintenance extension snap-in includes policy settings to manage the following:

- **Browser User Interface**—You use these options to customize the browser's appearance. For example, you can specify settings for the browser title bar, toolbar button options, and so on.
- **Connection Settings**—You can preset and manage the connection settings, such as local area network (LAN) and dial-up options.
- **Custom Universal Resource Locators (URLs)** —You can specify which URLs are displayed by the browser, for example, for the Home page, those on the Favorites list, and for the Search page.
- **Security**—You can preset security settings such as security zones, content ratings, and Authenticode. (A browser can be configured to allow only signed

code to be downloaded. Authenticode is Microsoft's version of object signing; it provides a basis for verifying the origin and integrity of an object, as well as links to policies of a certificate authority).

- **Program Associations**—You can specify which Internet programs to use by default for Internet-related tasks such as reading e-mail or viewing newsgroups.

Exporting Internet Explorer Settings for Down-level Clients

Administrators can export Internet Explorer policy settings into an auto-configuration package (an .ins file and its associated .cab files) to be used to apply these settings to Windows 95, Windows 98, and Windows NT 4.0 clients. The exported packages are auto-configuration packages. Before the Windows 2000 Group Policy MMC snap-in extension was created, Internet Explorer settings were applied to Internet Explorer clients using auto-configuration packages after Internet Explorer installation. Using GPOs is the preferred method of applying Internet Explorer policy settings on Windows 2000 clients, although Windows 2000 does support auto-configuration packages.

Using the Internet Explorer Maintenance Preference Mode Option

Administrators can specify to use a **Preference Mode** option for Internet Explorer Maintenance. By default, the Internet Explorer Maintenance extension snap-in is in true policy mode; that is, the options apply and work like all other policies. Optionally, administrators can set the mode for a given GPO as a **Preference Mode**—this constitutes a one-time default mode. The **Preference Mode** option enforces the specified setting only once per GPO. When this mode is selected, this is tracked in the registry and it is checked the next time the GPO is applied.

By default, the **Preference Mode** option is hidden. The **Internet Explorer Maintenance** node has to have focus before this option can be accessed. You access this option by right-clicking **Internet Explorer Maintenance** node and selecting **Preference Mode** on the context menu. This adds an **Advanced** node to the results pane. This node contains settings for managing Temporary Internet files and other UI features. Note that switching to **Preference Mode** disables some of the Internet Explorer Maintenance nodes. If a setting name has **Preference Mode** appended to it, it can be used in that mode; otherwise, it means that setting is disabled. For example, the **Connection Settings (Preference Mode)** option under the **Connection** node can be used in **Preference Mode** as indicated by its labeling in the UI, whereas the **User Agent String** option (note the exclusion of **Preference Mode**) cannot be used in **Preference Mode** and this is reflected in its labeling.

A listing of Group Policy settings for Internet Explorer Maintenance is presented in [Appendix B: Group Policy Settings for Internet Explorer](#) later in this paper.

Using Internet Explorer Customization Wizard and Internet Explorer Profile Manager

Besides the Internet Explorer Maintenance Group Policy options mentioned above, it is also possible to customize Internet Explorer before deployment and to manage Internet Explorer on other operating systems by using the [Internet Explorer Customization Wizard](#), found at <http://www.microsoft.com/windows/ieak/en/corp/features/custwiz/default.asp>, and the [Internet Explorer Profile Manager](#), found at <http://www.microsoft.com/windows/ieak/en/corp/features/profmanager/default.asp>. They can also be found at <http://www.microsoft.com/windows/ieak/en/default.asp> ([Microsoft Internet Explorer Administration Kit](#)). These tools provide options for System Policies and restrictions that administrators can use to specify desktop, shell, and security settings, for example.

The **System Policies and Restrictions** folder of the Internet Explorer Profile Manager contains nine default policy template (.adm) files to specify policies and restrictions. These are saved to information (.inf) files, which are packaged into the automatic configuration companion cabinet (.cab) files for download to a user's system. When these .inf files are unpacked, they are used to change policies and restrictions on users' systems.

For detailed information on these tools, see the [Microsoft Internet Explorer 5 Corporate Deployment Guide](#) at <http://www.microsoft.com/windows/ieak/en/deploy/corp/default.asp>, available on the [Microsoft Internet Explorer Administration Kit](#) Web site.

Remote Installation Services

Remote Installation Services is an optional component that is included in the Windows 2000 Server operating system and works with other Windows 2000 technologies to implement the Remote Operating System Installation feature. Administrators use Remote Operating System Installation to remotely install a copy of the Windows 2000 Professional operating system on supported computers⁴. Administrators use the Remote Installation Services extension of Group Policy to specify which options are presented to users by the Client Installation Wizard, for example, Automatic Setup, Custom Setup, and Restart Setup.

Client computers that are enabled with Pre-boot Execution Environment (PXE) remote-boot technology access the RIS server to install the operating system, and then the Remote Installation Services server checks for Group Policy that affects 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

⁴ Computers that are PC98-compliant ship with a PXE Remote Boot ROM.

the Group Policy objects to determine the resulting policy. Based on the resulting policy, it determines which screens to send to the pre-boot RIS client code for display to the user.

For more information, see the "[Remote Operating System Installation](http://www.microsoft.com/windows2000/library/planning/management/remoteos.asp)" white paper at
<http://www.microsoft.com/windows2000/library/planning/management/remoteos.asp>

Extending the Group Policy Functionality

It is possible to extend the current functionality of the Group Policy snap-in by creating administrative template files (.adm), or by authoring a Group Policy extension snap-in.

For information on creating Group Policy extension snap-ins, see the Group Policy documentation in the [Microsoft Platform SDK](http://msdn.microsoft.com/downloads/sdks/platform/platform.asp) at <http://msdn.microsoft.com/downloads/sdks/platform/platform.asp>. Further information on creating registry-based Group Policy for applications can be found in a white paper called "Implementing Registry-Based Group Policy for Applications," which is being posted at <http://www.microsoft.com/windows2000/library/howitworks/default.asp>.

Group Policy Processing

Group Policy is processed in the following order: Local Group Policy Object (LGPO), then GPOs linked to containers in this order: site, domain, and OUs, including any nested OUs (starting with the OU further from the user or computer object). This means that the local Group Policy Object is processed first, and the OU to which the computer or user belongs (the one that it is a direct member of) is processed last. All of this is subject to the following conditions:

- Security group filtering that has been applied to GPOs
- Any domain-based Group Policy object (not local GPO) may be enforced by using the **No Override** option so that its policies cannot be overwritten. When more than one GPO has been marked as enforced, the GPO that is highest in the Active Directory hierarchy takes precedence.
- At any site, domain, or OU, Group Policy inheritance may be selectively designated as **Block Inheritance**. However, blocking inheritance does not prevent policy from **No Override** GPOs from applying; this is because enforced GPOs are always applied, and cannot be blocked.

Note: Every computer has a single local GPO that is always processed regardless of whether the computer is part of a domain or is stand-alone computer. The LGPO can't be blocked by domain-based GPOs. However, settings in domain GPOs always take precedence since they are processed after the LGPO.

Initial Processing of Group Policy

Group Policy for computers is applied at computer startup. For users, Group Policy is applied when they log on. By default, the processing of Group Policy is synchronous, which means that computer Group Policy is completed before the CTRL+ALT+DEL dialog box is presented, and user Group Policy is completed before the shell is active and available for the user to interact with it.

Synchronous Versus Asynchronous Processing

Synchronous processes can be described as a series of processes where one process must finish running before the next one begins. Asynchronous processes, on the other hand, can run on different threads simultaneously because their outcome is independent of other processes.

You can change the default processing behavior by using a policy setting for each so that processing is asynchronous instead of synchronous. However, this is not recommended because it can cause unpredictable or undesirable side effects. For example, if the policy has been set to remove the **Run** command from the **Start** menu, it is possible under asynchronous processing that a user could logon prior to this policy taking effect, so the user would initially have access to this functionality. To provide the most reliable operation, it is recommended that you leave the processing as synchronous.

Time Limit for Processing of Group Policy

Under synchronous processing, there is a time limit of 60 minutes for all of Group Policy to finish processing on the client. Any client-side extensions that are not finished after 60 minutes are signaled to stop, in which case the associated policy settings may not be fully applied. An errant extension may not be able to respond; in either case the Group Policy engine goes into asynchronous processing mode. This means that the Group Policy engine is no longer blocked while waiting for a running (likely errant) extension and continues to process; it leaves the extension(s) running and does not terminate it (them). There is no setting to control this time-out period or behavior.

Background refresh of Group Policy

In addition to the initial processing of Group Policy at startup and logon, Group Policy is applied subsequently in the background on a periodic basis, and can also be triggered on demand from the command line.

During a background refresh, a client side extension will by default only reapply the settings if it detects that a change was made on the server in any of its GPOs or its list of GPOs. This is done for performance reasons.

Not all Group Policy extensions are processed during a background refresh. Software Installation and Folder Redirection processing occurs only during computer startup or when the user logs on. This is because processing periodically could cause undesirable results. For example, for Software Installation, if an application is no longer assigned, it is removed. If a user is using the application while Group Policy tries to uninstall it or if an assigned application upgrade takes place while someone is using it, errors would occur.

Note: The script's extension is processed during background refresh, however the scripts themselves are only ran at startup, shutdown, logon, and logoff, as appropriate.

Periodic Refresh Processing

Group Policy is 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.

Note: Setting a short refresh interval in a production environment is not recommended; however this can be useful in test or demonstration scenarios. This is because a 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.

To change the policy refresh interval setting, edit the **Default Domain Controllers** Group Policy object, which is linked to the **Domain Controllers** organizational unit. The **Group Policy Refresh Interval for Computers** setting is located under **Computer Configuration/Administrative Templates/System/Group Policy** node.

For domain controllers, the default period is every five minutes. **Group Policy Refresh Interval for Domain Controllers** setting is available under **Computer Configuration/Administrative Templates/System/Group Policy** node.

On-Demand Processing

You can also trigger a background refresh of Group Policy on demand from the client. However, the application of Group Policy cannot be pushed to clients on demand from the server.

To refresh policy from the command line

1. Click **Start**, and click **Run**.
2. To refresh policies under the **Computer Configuration** node, type the following: **secedit /refreshpolicy MACHINE_POLICY [/enforce]**, then Click **OK**.
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 Encrypted File System (EFS) extensions to refresh regardless of whether or not there is a policy change. For other extensions, it has no effect.

Applications can request a policy refresh by calling the **RefreshPolicy** function.

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.

Registry Reads

Group Policy snap-in extensions can temporarily claim (or lock) a mutex (mutual exclusive) for policy, and then release that mutex. A function called **EnterCriticalPolicySection** pauses the background application of policy for the purpose of safe reading of the registry. Applications that read multiple policy entries and need to ensure that the values are not changed while they are being read should use this function.

If the critical section is not released in 10 minutes, the system forces the application to release it, and then policy can be applied again. This ensures that the background refresh of Group Policy does not occur during the read process.

For information on server-side details of Group Policy and related APIs, see the Microsoft Platform SDK at <http://msdn.microsoft.com/developer/sdk/platform.htm>.

Slow Links and Remote Access Issues

Special considerations apply when processing Group Policy over slow links or remote access.

NOTE: Note that while these issues are related, they are distinct, and the processing of Group Policy is different for each. In particular, *remote access* does not necessarily imply a slow link, nor does a LAN necessarily imply a fast link. A slow link is by default based on the algorithm described in the section below. Windows 2000 Server *remote access* is part of the integrated Routing and Remote Access Service; it connects remote or mobile users to corporate networks, allowing users to work as if their computers are physically connected to the network. Users run remote access software to connect to a remote access server, which is a computer running Windows 2000 Server and the Routing and Remote Access Service. The remote access server authenticates the user and services sessions until terminated by the user or network administrator. The remote access connection enables all services typically available to a LAN-connected client, such as file and print sharing, messaging, and Web server access.

Group Policy and Slow Links

When Group Policy detects a slow link, it sets the **GPO_INFO_FLAG_SLOWLINK** flag in the **GPO_INFO** structure to indicate that policy is being applied across a slow link. Individual client-side extensions can determine whether or not to apply policy over the slow link.

The default settings are as follows:

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

For all but the Administrative Templates snap-in and security settings snap-in, a policy is provided for toggling the slow link processing 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.

For Group Policy, Windows 2000 uses a new IP ping algorithm to ping the server, rather than measuring the file system performance method that was used in Windows NT 4.0.

A slow link is, by default, based on the following algorithm (where ms = milliseconds):

1. Ping the server with 0 bytes of data and time the number of milliseconds.

This value is time#1. If it is less than 10 ms, exit (assume a fast link).

2. Ping the server with 2 KB of uncompressible data, and time the number of milliseconds. This value is time#2. The algorithm uses a compressed .jpg file for this.
3. DELTA = time#2 - time#1. This removes the overhead of session setup, with the result being equal to the time to move 2 KB of data.
4. Calculate Delta three times, adding to TOTAL each DELTA value.
5. TOTAL/3 = Average of DELTA, in milliseconds.
6. $2 * (2 \text{ KB}) * (1000 \text{ millisecc/sec}) / \text{DELTA Average millisecc} = X$
7. $X = (4000 \text{ KBytes/sec}) / \text{DELTA Average}$
8. $Z \text{ Kilobits per second (Kbps)} = ((4000 \text{ KBytes/sec}) / \text{DELTA Average}) * (8 \text{ bits/byte})$
9. $Z \text{ Kbps} = 32000 \text{ kbps/Delta Avg.}$

Two KB of data have moved in each direction (this is represented by the leading factor two on the left side in step six above) through each modem, Ethernet card, or other device in the loop once.

The resulting Z value is evaluated against the policy setting. A default of less than 500 Kbps is considered a slow link; otherwise it is a fast link. This value may be set through Group Policy in the Administrative Templates node.

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. The connection speed is set for kilobits per second (Kbps).

For User Profiles, the **Slow network connection timeout for user profiles** policy is located in the **Computer Configuration\Administrative Templates\System\Logon** node. This policy has support for both pingging the server and checking the performance of the file system. This is because user profiles can be stored anywhere, and that server may or may not have IP support. Therefore, the user profile code first tries to ping the server. If the server does not have IP support, it falls back to measuring the file system's performance. You must specify connection speeds in both kilobytes per second (Kbps) and milliseconds (ms) when setting this policy.

Application of Group Policy During a Remote Access Connection

Group Policy is applied during a remote access connection as follows:

When using the **Logon using dial-up connection** checkbox on the logon prompt, both User and Computer Group Policy is applied, provided the computer is a member of the domain that the remote access server belongs to or trusts. However,

computer-based software installation settings are not processed. This is because normally computer policy would have been processed before the logon screen, but since no network connection is available until logon, the application of computer policy is done as background refresh at the time of logon.

When the logon is done with cached credentials, and then a remote access connection is established, Group Policy is not applied.

Group Policy is not applied to computers that are members of a foreign domain or a workgroup. Although the connection may still be made, access to domain resources may be affected (because of mismatched IPsec security).

Client-side Processing of Group Policy

Some of the Group Policy components include client-side extensions (.dlls) that are responsible for implementing Group Policy at the client computers. The client-side extensions are listed in the following table.

Client-side extension	DLL file name
Registry (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

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 **GetGPList** Win32 function. Each client-side extension processes the resulting list of GPOs.

The client-side extensions are loaded on an as-needed basis 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 GPOs. If a client-side extension has data in a GPO, 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 GPOs, it is not called.

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 (checkboxes). 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:

- **Allow processing across a slow network connection.** When a client-side extension registers itself with the operating system, it sets preferences in the registry, specifying whether it should be called when policy is being applied across a slow link. Some extensions move large amounts of data, so processing across a slow link can affect performance (for example, consider the time involved in installing a large application file across a 28.8 Kbps modem line). An administrator can set this policy to mandate that the client-side extension should run across a slow link, regardless of the amount of data.
- **Do not apply during periodic background processing.** Computer policy is applied at boot time, and then again in the background, approximately every 90 minutes thereafter. User policy is applied at user logon, and then approximately every 90 minutes after that. The **Do not apply during periodic background processing** option gives the administrator the ability to override this logic and force the extension to either run or not run in the background. **Note:** the Software Installation and Folder Redirection extensions process policy only during the initial run because it is risky to process policy in the background. For example, with Software Installation application upgrades, applications are installed during the initial run and not in the background. If it were done in the background, a user could be running an application, and then have it uninstalled and a new version installed. The application could also have a shared component that is in use by another application. This would prevent the installation from completing successfully.
- **Process even if the Group Policy Objects have not changed.** By default, if the GPOs on the server have not changed, it is not necessary to continually reapply them to the client, since the client should already have all the settings. However, local administrators may be able modify the parts of the registry where Group Policy settings are stored. In this case, it may make sense to reapply these settings during logon or during the periodic refresh cycle to get the computer back to the desired state.
For example, assume that you have used Group Policy to define a specific set of security options for a file. Then the user (with administrative privileges) logs on and changes it. The Group Policy administrator may want to set the policy to process Group Policy even if the GPOs have not changed so that the security is reapplied at every boot. This also applies to applications. Group Policy installs an application, but the end user can remove the application or delete the icon. The process gives the administrator the ability to restore the application at the next user logon, even if the Group Policy Objects have not changed option.

Note that, by default, security settings are applied every 16 hours (960 minutes) even if a GPO has not changed. It is possible to change this default period by using the following registry key:

```
HKLM\Software\Microsoft\Windows  
NT\CurrentVersion\Winlogon\GPExtensions\{82...}\MaxNoGPListChangesInterval, REG_DWORD, in number of minutes.
```

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

Client-side extension	Missing policy checkbox	Reason
Registry	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)	It is considered too risky to move users' files while they are logged on.
Software Installation	Background processing (Do not apply during periodic background processing)	It is considered too risky to install and uninstall an application when the user is logged on.

Server Processing

Group Policy Snap-in and the Operations Master

The Group Policy snap-in uses the Operations Master token for the primary domain controller (PDC) emulator when editing a GPO. This ensures that the Group Policy snap-in is always focused on the same domain controller (DC). User preference options and policy settings are available to modify this behavior. For more information on setting domain controller options, see the upcoming section on [Specifying a Domain Controller for Setting Group Policy](#).

Synchronization Between the Group Policy Template and the Group Policy Container

Lack of synchronization between the Group Policy Template (data stored on Sysvol) and Group Policy Container (data stored in the Active Directory) portions of the Group Policy Object can occur temporarily because of the differences in the replication schemes used by the Active Directory and the File Replica Set (FRS—for system volume data).

For those Group Policy extensions that store data in only one data store (either the Active Directory or Sysvol), this is not an issue, and Group Policy is applied as it can be read. Such extensions include Administrative Templates, Scripts, Folder Redirection, and most of the Security Settings.

For any Group Policy extension that stores data in both storage places (the Active Directory and Sysvol), the extension must properly handle the possibility that the data is unsynchronized. This is also true for extensions that need multiple objects in a single store to be atomic in nature, since neither storage location handles transactions.

An example of an extension that stores data in the Active Directory and Sysvol is Software Installation. The script files are stored on Sysvol and the Windows Installer package definition is in the Active Directory. If the script exists, but the corresponding Active Directory components are not present, then nothing is done. If the script file is missing, but the package is known in Active Directory, application installation fails gracefully and will be retried on the next processing of Group.

Specifying a Domain Controller for Setting Group Policy

In this version of Windows 2000, Group Policy writes data to the GPO immediately for each change. If two administrators are simultaneously editing the same GPO on different domain controllers, it is possible for the changes written by one administrator to be overwritten by another administrator, depending on replication latency.

To avoid this situation, the Group Policy snap-in by default uses the Operations Master token for the PDC emulator when editing a GPO. This forces the Group Policy snap-in to use the same domain controller and helps ensure that no data loss occurs.

However, it is possible to modify this default behavior by using either user-preference options or policy settings to set domain controller options for Group Policy, as described in the next sections. This will be useful in situations that require editing a GPO on a local domain controller. For example, if an administrator were delegated a GPO across a slow link, he or she would want to edit that GPO on the local domain controller for optimum performance. This functionality can be useful in some corporate scenarios, provided that more than one administrator does not typically administer a given GPO. For example, if you are an administrator in Japan and the PDC emulator is in New York, it may be problematic if you are forced to rely on a WAN link to access the New York PDC emulator. However, if no one else administers your GPOs, you could choose this option so that you could make your policy edits on a local domain controller so that performance is acceptable.

Specifying a Domain Controller for Group Policy Editing by Using Preferences

Administrators can use the Group Policy snap-in user interface to set domain controller options by selecting **DC Options** from the **View** menu. This option is available only when focus is on the root node of the Group Policy snap-in.

Selecting **DC Options** opens the **Options for domain controller selection** dialog box, where you can specify a domain controller (DC) to use for editing Group Policy:

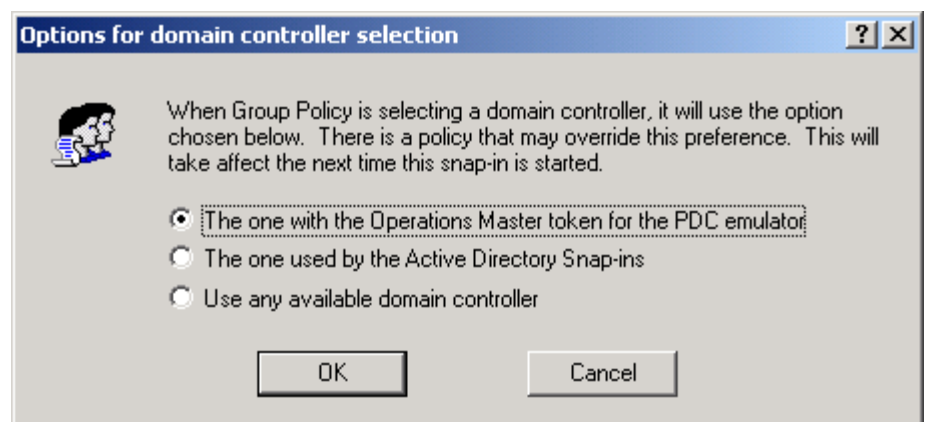


Figure 6. *Options for domain controller selection* dialog box

The available options for the **Options for domain controller selection** dialog box are:

- **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 could occur if two administrators were working on changes to the same GPO on different domain controllers within the replication cycle. In this version of Windows 2000, Group Policy writes data to the GPO for each change. If two administrators are editing a GPO on different domain controllers, it increases the possibility of changes being overwritten by replication. It is strongly recommended that the number of administrators be limited, that Group Policy use the PDC emulator Operations Master, and that the administrator be aware of other administrators who may be editing the same GPO.
- **The one used by the Active Directory Snap-ins.** Uses the domain controller that the Active Directory management snap-in tools are currently using. Each of these snap-ins includes an option for changing which domain controller is the focus of the current operations. When this option is selected, the Group Policy snap-in uses the same domain controller as the Active Directory snap-ins. For example, if the Active Directory Users and Computers snap-in is focused on DC3, Group Policy also uses DC3.
- **Use any available domain controller.** The third, and, in most cases, least desirable option 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.

All of these options may be overridden by a using policy setting, as described next. These settings are available in the **User Configuration\Administrative Templates\System\Group Policy** node of the Group Policy snap-in.

Specifying a Domain Controller by Using Policy

Domain administrators can use a policy to specify how Group Policy chooses a domain controller—that is, they can specify which domain controller option should be used. In such cases, the **DC Options** menu item is unavailable since a policy is in place that overrides any setting that the user chooses. This policy allows domain administrators to mandate that all administrators must use the PDC emulator, for example.

The DC options policy is available in the Administrative Templates node for User Configuration, in the System\Group Policy sub-container. The available DC options are the same as the preference settings listed above in the [Options for domain controller selection dialog](#) box description.

Error Handling on Failure to Reach a Domain Controller

If the Group Policy snap-in cannot reach the intended DC, the following error dialog box is displayed:

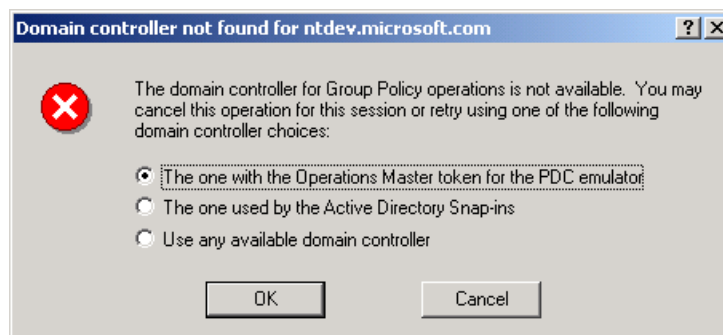


Figure 7. Domain controller not found dialog box

The default option for this dialog box is always the first option. However, if there is a policy in place, this error dialog box is not displayed. Instead, the following message is displayed: "Failed to find a domain controller. There may be a policy that prevents you from selecting another domain controller."

DC Selection Results

The following table indicates which DC the Group Policy snap-in will use, based on various combinations of conditions. Where:

PDC means use the DC with the Operations Master token for the PDC emulator.

Inherit means use the DC used by the Active Directory snap-ins.

Any DC means use any available DC.

1) and 2) means that 1) will be tried first, and then 2).

User preference	Policy	Results
Undefined	Undefined	1) PDC 2) Prompt
PDC	Undefined	1) PDC 2) Prompt
Inherit	Undefined	1) Inherit 2) Any DC
Any	Undefined	Any DC
N/A	PDC	PDC only
N/A	Inherit	1) Inherit 2) Any DC
N/A	Any	Any DC

Local Group Policy

You can set local Group Policy for any computer, whether or not it participates in a domain. To set local Group Policy, you use the Group Policy snap-in focused on the local computer. You can access the Group Policy snap-in tool 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. Group Policy is processed in this order: local GPO first, followed by Active Directory linked GPOs (site, domain, OU, and any nested OUs).

Local Group Policy Object

On all computers, a Local Group Policy Object (LGPO) exists—this is just the Group Policy Template portion. The location of the LGPO is

\\%SystemRoot%\System32\GroupPolicy. Each Group Policy extension snap-in queries the Group Policy engine to get the GPO type, and then decides if it should be displayed.

The following table indicates whether or not the Group Policy snap-in extensions open when the Group Policy snap-in is focused on an LGPO.

Group Policy snap-in extension	Loaded when Group Policy snap-in focused on LGPO
Security Settings	Yes
Administrative Templates	Yes
Software Installation	No
Scripts	Yes
Folder Redirection	No
Internet Explorer Maintenance	Yes

Local Group Policy Object and DACLs

In the current release, there is no **Apply Group Policy** ACE for the local GPO. If you have Read access to the LGPO, then the local GPO applies to you. The implication is that it's difficult to have to choose whom the LGPO should apply to (for example, the LGPO also applies to the administrator). Everyone with Read access to the LGPO who logs on gets the LGPO. If this is not what you want, a work-around exists. You can set the Read ACE to Deny for a specific user, and then the LGPO doesn't apply to that user. This is useful for administrators who don't want to be subject to the LGPO settings. However, without Read access, administrators cannot see the contents of the LGPO.

Viewing Policies When the Group Policy Snap-in is Focused on the Local Computer

When administrators run the Group Policy snap-in focused on a local computer, this shows the information in the local Group Policy object, not the cumulative effect of what has been applied to the computer or user. This feature is being investigated for the next release of the product. For Windows 2000, it shows the settings that a local administrator has set for that computer and all users of that computer. In the

evaluation process, when the computer is joined to a domain, all the policy settings are subject to being overwritten by domain-based policy (any policy set in the site, domain, or OU).

Starting the Group Policy Snap-in on Windows 2000 Professional
Windows 2000 Professional does not provide a user interface for accessing the Group Policy snap-in directly. However, you can access the Group Policy snap-in in the following manner.

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

1. Click **Start**, click **Run**, type **MMC**, and then press **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. The **Select Group Policy Object** dialog box appears. Click **Local Computer** to edit the Local Group Policy Object (LGPO), or **Browse** to find the GPO that you want to use.
6. Click **Finish**.
7. Click **OK**. The Group Policy snap-in opens with focus on the specified Group Policy object.

To use the Group Policy snap-in on a remote computer, you must have administrative rights on both computers, and the remote computer must be part of the namespace.

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

The Group Policy snap-in on a remote computer must be focused when the extension is added to an MMC console file, or as a command line option.

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 (like 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. Select **Browse**.
You may now select a GPO from the Active Directory or, as in this case, select the **Computer** tab.
6. Select **Another Computer**.

-
7. Either type in the computer name, or click **Browse** to locate it.
 8. You may use the **Look in** drop-down list box to select the domains to which you have access.

The supported computer name formats are:

- NetBIOS names, for example, *MachineName*.
- DNS-style, for example, *MachineName.Streetmarket.com*.

Starting the Group Policy Snap-in from the Command Line

The Group Policy snap-in (gpedit.msc) can be started with the following two command line switches:

- **/gpcomputer:"machinename"**

Where "machinename" can be either a NetBIOS or a DNS-style name. For example, "gpedit.msc /gpcomputer:"machinename"

or

"gpedit.msc /gpcomputer:"machinename.streetmarket.com"

- **/gpobject:"ADSI path"**

For example:

"LDAP://CN={GUID of the GPO},CN=Policies,CN=System,DC=Streetmarket,DC=com"

For these command line options to work with a saved console file, you must check the "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." checkbox. The shipping Gpedit.msc file is saved with this option on.

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

Local Group Policy Object Processing

When a computer is joined to a domain with the Active Directory and Group Policy implemented, a local Group Policy Object is processed. Note that LGPO policy is processed even when the **Block Policy Inheritance** option has been specified.

Local Group Policy Objects are always processed first, and then domain policy is processed. If a computer is participating in a domain and a conflict occurs between domain and local computer policy, domain policy prevails. However, if a computer is no longer participating in a domain, LGPO policy is applied.

Group Policy Loopback Support

Group Policy is applied to the user or computer, based upon where the user or computer object is located in the Active Directory. However, in some cases, users may need policy applied to them, based upon the location of the computer object, not the location of the user object. The Group Policy *loopback* feature gives the administrator the ability to apply user Group Policy, based upon the computer that the user is logging onto.

To describe the loopback feature, we'll use an example. In this scenario, you have full control over the computers and users in this domain because you have been granted domain administrator rights.

The following illustration shows the Reskit domain, which is used to work through this example.

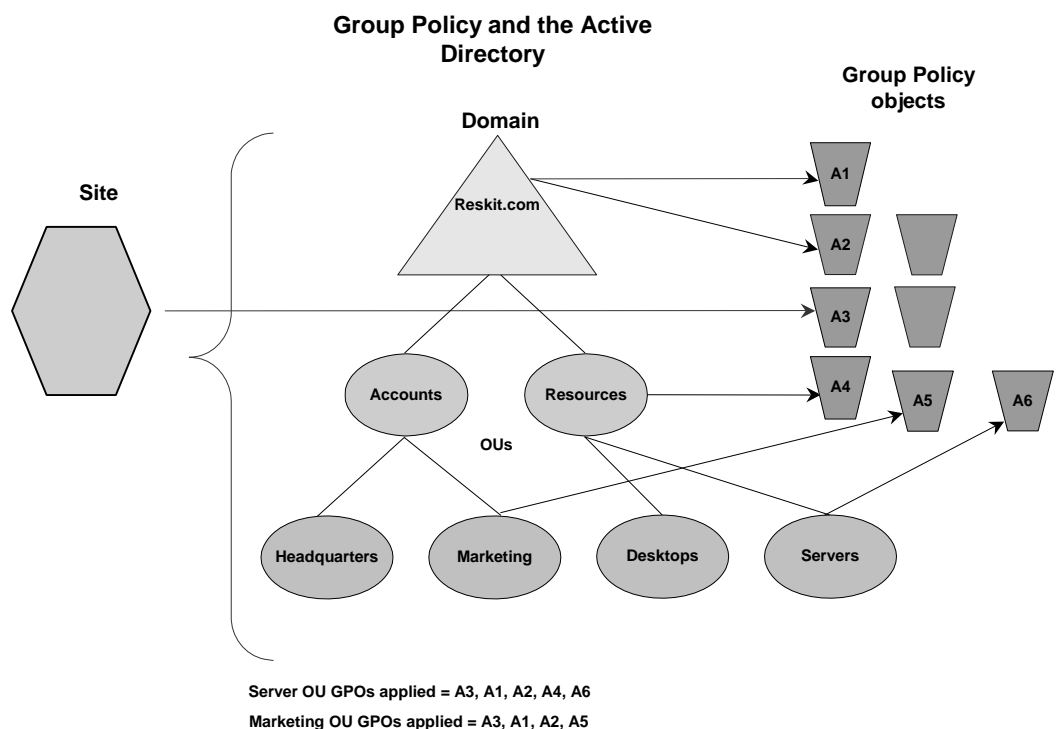


Figure 8. The Reskit domain

Normal user Group Policy processing specifies that computers located in the Servers OU have the GPOs A3, A1, A2, A4, A6 applied (in that order) during computer startup. Users of the Marketing OU have GPOs A3, A1, A2, A5 applied (in that order), regardless of which computer they log on to.

In some cases this processing order may not be what you want to do, for example, when you do not want applications that have been assigned or published to the users of the Marketing OU to be installed while they are logged on to the computers in the Servers OU. With the Group Policy loopback feature, you can specify two other ways to retrieve the list of GPOs for any user of the computers in the Servers

OU:

- **Merge mode.** In this mode, the user's list of GPOs is normally gathered during logon through the use of the **GetGPOList** function. Then **GetGPOList** is called again using the computer's location in the Active Directory. Next, the list of GPOs for the computer is added to the end of the GPOs for the user. This causes the computer's GPOs to have higher precedence than the user's GPOs. In this example, the list of GPOs for the computer is A3, A1, A2, A4, A6, which is added to the user's list of A3, A1, A2, A5, resulting 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 GPOs is not gathered. Only the list of GPOs based upon the computer object is used. In this example, the list is A3, A1, A2, A4, and A6.

You can set the loopback feature by using the **User Group Policy loopback processing mode** policy under Computer Settings\Administrative settings\System\Group Policy.

The processing of the loopback feature is implemented in the Group Policy engine⁵, not in the **GetGPOList** function. When the Group Policy engine is about to apply user policy, it looks 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.

⁵ The Group Policy engine is the part of Group Policy that runs in the Winlogon process.

Policy Settings for Group Policy

This section discusses the use of policy settings to specify the behavior of Group Policy.

Specifying Policy Settings for Group Policy

Administrators can specify policy settings that affect how Group Policy is applied and updated.

The following table lists the policy settings for Group Policy under the **Computer Configuration\Administrative Templates\System\Group Policy** nodes.

Policy	Description
Disable background refresh of Group Policy	Used to prevent Group Policy settings from being updated while the computer is in use. Applies to Group Policy for computers, users, and domain controllers.
Apply Group Policy for computers asynchronously during startup	Used to allow the system to display the logon prompt before it completes updates for computer Group Policy.
Apply Group Policy for users asynchronously during logon	Used to allow the system to display the Windows desktop before it completes updates for computer Group Policy.
Group Policy refresh interval for computers	<p>Used to specify how often Group Policy for computers is updated in the background while the computer is in use. Specifies a background update rate only for Group Policy settings under the Computer Configuration node. Computer Group Policy is updated in the background every 90 minutes by default, with a random offset of 0 to 30 minutes. Besides background updates, computer Group Policy is always updated when the system starts.</p> <p>Administrators can stipulate an update rate from zero to 64,800 minutes (45 days). When zero minutes is specified, the computer tries to update Group Policy every seven seconds. Such updates may interfere with users' work and increase network traffic; therefore, very short update intervals are not appropriate in most cases.</p>
Group Policy refresh interval for domain controllers	<p>Specifies how often Group Policy is updated, in the background, on domain controllers while they are running. The update rates that this policy specifies happen in addition to the updates processed when the system starts.</p> <p>By default, Group Policy on the domain controllers is updated every five minutes. Administrators can specify an update rate from zero to 64,800 minutes (45 days). When zero minutes is specified, the domain controller tries to update Group Policy every seven seconds. Such updates may interfere with users' work and increase network traffic; therefore, very short update intervals are not appropriate in most cases.</p>

Policy	Description
User Group Policy loopback processing mode	<p>Applies the set of Group Policy objects defined for the computer to any users who log on to a computer affected by this policy. This policy is intended for use in computers in public environments, such as those in classrooms and libraries, for example, where it is appropriate to define user Group Policy based on the computer being used.</p> <p>When this policy is enabled, Group Policy is applied to users logging on to this computer according to the Group Policy objects defined for the computer. Two options for the processing of this policy are available: merge mode and replace mode. See Group Policy Loopback Support for more information.</p>
Group Policy slow link detection	<p>Used to define a slow link for the purpose of Group Policy processing and updates. The system considers a connection to be slow if data that is transferred from the domain controller providing a Group Policy update to the computers in this group travels at a slower rate than that specified by this policy. See Group Policy and Network Connections (Slow Links) for more information.</p>
Registry policy processing	<p>Used to specify when Group Policy registry settings are applied. Affects all policies under the Administrative Templates node as well as policies that store values in the registry.</p> <p>Two options are available: Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
Internet Explorer Maintenance policy processing	<p>Used to specify when Internet Explorer Maintenance policy settings are processed. Affects all policy settings that use the Internet Explorer Maintenance extension of Group Policy, such as those under the User Configuration\Windows Settings\Internet Explorer Maintenance node, and overrides any customized settings set by the program implementing Internet Explorer Maintenance policy when it was installed.</p> <p>Three options are available: Allow processing across a slow network connection, Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
Software Installation policy processing	<p>Used to specify when Software Installation policy settings are processed. Affects all policy settings that use the Software Installation extension of Group Policy.</p> <p>Two options are available: Allow processing across a slow network connection, and Process even if the Group Policy objects have not changed.</p>
Folder Redirection policy processing	<p>Used to specify when Folder Redirection policy settings are processed. Affects all policies that use the Folder Redirection extension of Group Policy, such as those in the User Configuration\Windows Settings\Folder Redirection node.</p> <p>Two options are available: Allow processing across a slow network connection, and Process even if the Group Policy objects have not changed.</p>

Policy	Description
Scripts policy processing	<p>Used to specify when scripts policy settings are processed. Affects all policy settings that use the scripts extensions of Group Policy (for Startup/Shutdown, and Logon/Logoff).</p> <p>Three options are available: Allow processing across a slow network connection, Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
Security policy processing	<p>Used to specify when security settings policies are updated.</p> <p>Two options are available: Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
IP Security policy processing	<p>Used to specify when IP Security policies are updated.</p> <p>Three options are available: Allow processing across a slow network connection, Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
EFS recovery policy processing	<p>Used to specify when encryption policy settings are updated.</p> <p>Three options are available: Allow processing across a slow network connection, Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>
Disk Quota policy processing	<p>Used to specify when disk quota policies are updated. Affects all policies under the Computer Configuration\Administrative Templates\System\File System\Disk Quotas node. It also overrides any settings set by the program implementing the disk quota policy when it was installed.</p> <p>The following options are available: Allow processing across a slow network connection, Do not apply during periodic background processing, and Process even if the Group Policy objects have not changed.</p>

For more information on these policy settings, double-click the policy in the details pane, and then in the policy **Properties** dialog box, click the **Explain** tab.

The following table lists the policy settings for Group Policy for users. These are accessed under the **User Configuration\Administrative Templates\System\Group Policy** nodes.

Policy	Description
Group Policy refresh interval for users	<p>Used to specify how often Group Policy for users is updated in the background while the computer is in use. Affects the background update rate only for the Group Policy settings in the User Configuration node. Besides background updates, Group Policy for users is always updated when they log on.</p> <p>By default, user Group Policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes. Administrators can specify an update rate from 0 to 64,800 minutes (45 days). When 0 minutes is selected, the computer tries to update user Group Policy every 7 seconds. Such updates may interfere with users' work and increase network traffic; therefore, very short update intervals are not appropriate in most cases.</p>
Group Policy slow link detection	<p>Used to define a slow link for the purpose of Group Policy processing and updates. The system considers a connection to be slow if data that is transferred from the domain controller providing a Group Policy update to the computers in this group travels at a slower rate than that specified by this policy. See Group Policy and Network Connections (Slow Links) for more information.</p>
Group Policy domain controller selection	<p>Used to specify which domain controller to use for Group Policy.</p> <p>Three options are available: Use the Primary Domain Controller, Inherit from the Active Directory Snap-ins, Use any available domain controller. See Specifying a Domain Controller for Setting Group Policy for more information.</p>
Create new Group Policy Object links disabled by default	<p>Used to specify that Group Policy object links be created in a Disabled state. This allows administrators to configure and test such links before setting them to Enabled.</p>
Enforce Show Policies Only	<p>Used to prevent Group Policy <i>preferences</i> from being viewed. By default, only those policy settings defined in the loaded .Adm files that exist in the approved Group Policy trees are displayed; these settings are referred to as <i>true policies</i>. This means that the Group Policy snap-in does <i>not</i> display any items described in the .Adm file that set registry keys outside of the Group Policy trees; such items are referred to as Group Policy <i>preferences</i>.</p> <p>For more information, see Distinguishing True Policies from Group Policy Preferences, and Viewing Group Policy Preferences.</p>

Policy	Description
Disable automatic update of ADM files	<p>Used to prevent the system from updating the Administrative Templates source files automatically when the Group Policy snap-in is opened. When the Group Policy snap-in is started, the system loads the most recently updated copies of the Administrative Templates source files (.adm) that it finds in the <i>Systemroot\inf</i> directory. The .adm files create the list of policies that are displayed under the Administrative Templates node of the Group Policy snap-in.</p> <p>When this policy is enabled, the system loads the .adm files used the last time you ran Group Policy. Thereafter, the .adm files must be updated manually.</p>

For more information on these policy settings, double-click the policy in the details pane, and then in the policy **Properties** dialog box, click the **Explain** tab.

Group Policy and Active Directory Sites

Group Policy objects that are linked to site containers affect all computers in a forest of domains. Site information is replicated and available between all the domain controllers within a domain and all the domains in a forest. Therefore, any Group Policy object that is linked to a site container is applied to all computers in that site, regardless of the domain (in the forest) to which they belong. This has the following implications:

- It allows multiple domains (within a forest) to get the same Group Policy object (and included policies), although the Group Policy object only lives on a single domain and must be read from that domain when the affected clients read their site policy.
- If child domains are set up across wide area network (WAN) boundaries, the site setup should reflect this. If it does not, the computers in a child domain could be accessing a site Group Policy object across a WAN link.

To manage site GPOs, you need to be either Enterprise Administrator or domain administrator of the forest root domain.

You may want to consider using site-wide GPOs for specifying policy for proxy settings and network-related settings.

Setting up Group Policy on a Site

To define policy settings for a site you must start the Active Directory Site and Services Manager snap-in first.

To start the Active Directory Site and Services Manager tool

1. From the **Start** menu, click **Programs**.
2. Click **Administrative Tools**, and then click on **Active Directory Site and Services Manager**.

Next, add the site(s) you want to use.

To add new sites, use the Active Directory Site and Services Manager

1. Right-click **Sites** in the tree in the left pane of the console, and click **New**.
2. Click **Site**, and type in a name for the new site (for example, type **NewYork**), as shown in the following figure.

If presented with a Default Site Link, you may want to associate this site to a Site Link at this time.

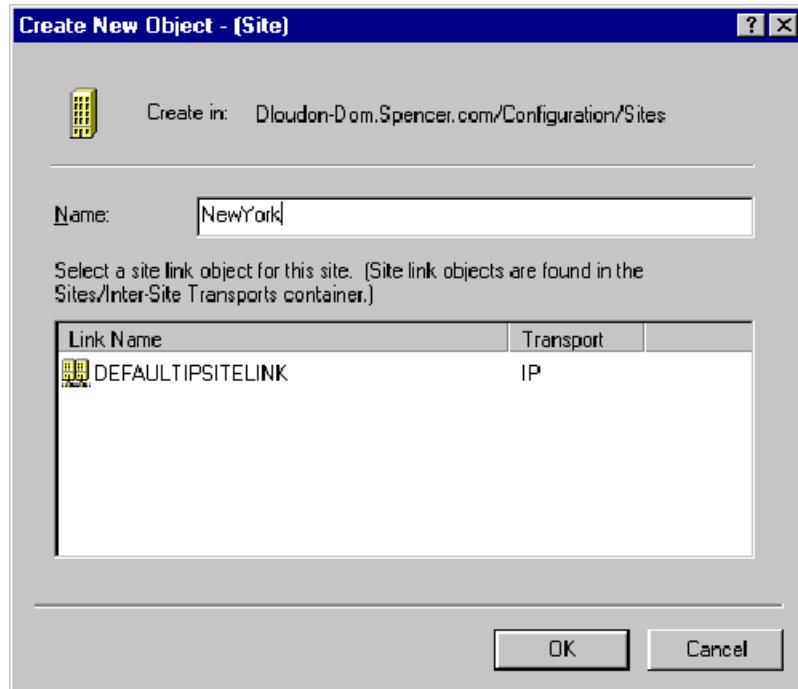


Figure 9. Creating a new site

You can now move computers from other sites into this site (under the NTDS Settings container).

Following the creation of site(s), you need to create the subnet(s) that are in a site. A site can span multiple subnets, but a subnet cannot span multiple sites.

To create a subnet

1. Right-click on **Subnet**.
2. Click **New Subnet**.
3. In the **Name** text box, type the network address of the subnet (that is, the base address of the subnet in dotted notation) and the number of bits to be masked, counting from the left to the right.
4. For example, type 164.110.30.0/24, which would translate to 164.110.30.0 with a mask of 255.255.255.0.
5. Click on the site that you want to associate with that subnet in the box below the **Name** text box.
6. Click **OK**.

After you have defined the site(s) and linked to a subnet(s), you can apply policy to the site by right clicking on the site name, choosing the **Properties** page, and then selecting the **Group Policy** tab. The rest of the GPO creation is exactly the same as for a domain or an OU.

The following are some issues surrounding Active Directory sites that may impact

Group Policy.

If you create the site(s) prior to DC promotion, your DCs are automatically placed in the correct sites.

- If you create the sites(s) after DC promotion, you must manually move the DC to the correct site. Do this by drilling down into the site to the server container. Inside the server container is a list of DCs thought to be in that site. To move a server to a different site, right-click on the server, and choose **Move**. Then click on the site to which you want to move the server.
- Replication between DCs in different sites occurs less frequently than replication between DCs in the same site, and during scheduled periods only. The replication schedule and frequency are properties of the site links that connect sites. The default inter-site replication frequency is three hours. To change it, go to the appropriate site link, into the IP link, and change the replication frequency or schedule as desired. This will have a major impact for policy, as explained next.

For example, assume that you leave replication set to three hours or change it to an even longer period. You then create a new OU in a domain spanning several sites. If the domain controller that the OU was created on is in a different site than the DC that holds the PDC emulator role, then you may have to wait three hours or longer for that new OU to replicate to the PDC. The OU must replicate to the PDC before you can associate a policy with that OU. If you want to create an OU and associate policy with that OU right away, you can work around inter-site replication latency by creating the OU on the PDC, or on a domain controller in the same site as the PDC.

You can also do this by specifically having Group Policy point to the same DC as the one the Active Directory snap-in tool is using. For information, see the [Specifying a Domain Controller for Group Policy Editing by Using Preferences](#) section. Remember that these preferences can be controlled by using a policy setting so you may not be able to do this, or you may only be able to read the policy settings. This means that if the administrator has previously set a policy to specify which DC to use, the **DC Options** menu item is unavailable since a policy is in place that overrides any setting that the user chooses. See the [Specifying a Domain Controller by Using Policy](#) section for more information.

An important issue to keep in mind if you are changing the default option for DC selection is that if two administrators are simultaneously editing the same GPO on different domain controllers, it is possible for the changes written by one administrator to be overwritten by another administrator, depending on replication latency. So care should be taken to ensure this does not happen.

Storage of a GPO Linked to a Site

By default, creating a new GPO for a site stores that GPO in the Forest Root domain.

To create a new GPO in a domain

1. Select **Add** (not **New**) from the **Group Policy** tab of the site that you want to use.
2. Select the **All** tab.
3. Select the appropriate domain in the **Look in** drop-down list.
4. Either right-click and select **New**, or click the **New GPO** toolbar button.
5. Give the new GPO a friendly name.
6. Select **OK**.

The GPO will be linked to the current site.

You can also select a GPO specifically created in another domain.

To select a GPO that already exists in another domain

1. From the **Group Policy** tab of the appropriate site, select **Add**.
2. Select the appropriate domain in the **Look in** drop-down list.
3. Select the GPO you want to use.
4. Click **OK**.

The GPO will be linked to the current site.

If the GPO does not yet exist, you can create one in the appropriate domain.

Design Considerations for Organizational Unit Structure and Use of Group Policy Objects

This section discusses issues you need to consider when planning and implementing your OU structure, and highlights recommendations for the use of GPOs.

OU Structure

The Group Policy architecture is flexible and allows for many types of design. The guiding principle as you design your OU structure should be to create a structure that is easy to manage and troubleshoot. There are two key reasons to create an OU:

- To enable delegation of administration.
- To scope the application of GPOs.

In general, do not try to model your OU structure based on your business organization. Rather, design your OU structure based on how you administer your business. Information on planning for Active Directory is available in the [Windows 2000 Server Resource Kit Deployment Planning Guide](http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp) at <http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp>, in *Chapter 9: Designing the Active Directory Structure*.

In most organizations, OU structure is likely to fall into one of the following categories:

- Flat OU structure: 1 or 2 levels
- Narrow OU structure: 3 to 5 levels
- Deep OU structure: more than 5 levels

For organizations with simple administration requirements, it is recommended that administrators use a simple model in which a flat OU structure is used and Group Policy objects are linked at the domain or OU level. Limited use of security groups to filter GPOs is recommended. If you need additional flexibility it suggested that you reconsider your OU structure.

For organizations with moderate administration requirements, it is recommended that administrators use a narrow OU structure and Group Policy objects are linked at the site, domain, or OU level as necessary. Limited use of the Block Policy Inheritance options, the Enforce Policy options, and security groups to filter GPOs is recommended.

For organizations with complex administration requirements, the Active Directory namespace may use flat, narrow, or deep OU structures. In such cases, administrators should consider the following issues:

- Flat OU model: use security groups and DACLs to filter effects of GPOs as a primary method, and Block Policy Inheritance and Enforce Policy options as secondary methods.
- Narrow OU model: link to GPOs at site, domain, and OU. As a secondary method, use Block Policy Inheritance and Enforce Policy options, and security groups and DACLs for filtering effects of GPOs.
- Deep OU model: link to GPOs at site, domain, and OU with security groups filtering and DACLs. As a secondary method, use Block Policy Inheritance and Enforce Policy options.

For more information on Active Directory infrastructure and planning and designing the Active Directory structure, see the [Windows 2000 Server Resource Kit Deployment Planning Guide](http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp) at <http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp>.

Design Principles

This section presents general guidelines for the use of Group Policy objects and policy features, and includes examples of GPO design.

Administration of Group Policy Objects

Delegation of authority, separation of administrative duties, central versus distributed administration, and design flexibility are important factors you'll need to consider when designing Group Policy and selecting which scenarios to use for your organization.

How you design your OU structure and GPOs will depend on the administrative requirements and roles in your corporation. For example, if administrators are organized according to their duties (such as security administrators, logon administrators, and so on), you may find it useful to define these policy settings in separate Group Policy Objects.

Delegation of authority will depend largely on whether you use centralized or distributed administration in your corporation. Based on their particular corporate requirements, network administrators can use security groups and Discretionary Access Control List permissions to determine which administrator groups can modify policies in Group Policy objects. Network administrators can define groups of administrators (for example, Software Installation administrators), and then provide them read and write access to selected Group Policy objects, allowing the network administrator to delegate control of the Group Policy object settings. Administrators who have read and write access to a Group Policy Object can by default control all of the contents of that Group Policy Object; however, you can restrict access by setting policy to control which MMC snap-ins can be loaded by that user, as previously described in the [Delegating Group Policy](#) section.

Separate Users and Computers into Different OUs

It's recommended that you separate users and computers into separate OUs. This is useful for these reasons:

- This simplifies GPO design because you need to focus on only configuration of either user or computers.
- Typically users and computers are administered differently, perhaps by different groups within your organization, which facilitates administration.
- You can reduce group policy processing time because you can disable the unused half of the GPO. It is possible to disable only the User or Computer portion of the GPO. To do this, right-click the GPO, click **Properties**, click either **Disable Computer Configuration settings** or **Disable User Configuration settings**, and then click **OK**. These options are available on the GPO **Properties** page, on the **General** tab.
- This type of design is required to enable loopback processing. See the [Group Policy Loopback Support](#) section for more information.

Functional versus Geographical OU Structure

When organizing OUs, there are two basic models to start with: functional and then geographical, or geographical and then functional. The key is never to implement a structure that forces an artificial layering, which means that the OU structure for computers may be very different than that for users—it all depends on how they are administered.

Minimize the Number of Group Policy Objects Associated with Users or Computers

You should note that the number of Group Policy objects that are applied to a user affects the logon processing time. (Similarly, the number of GPOs applied to a computer affects boot time). The greater the number of associated Group Policy objects, the longer logon will take to process them. During logon time, each GPO from the user's site, domain, and OU hierarchy is applied, provided the user has both the Read ACE and the Apply Group Policy ACE. Note that if the Apply Group Policy ACE is not set, but the Read ACE is, the GPO will still be processed (although not applied), thus impacting logon time. Therefore, if you implement filtering based on security groups, you should also clear Read Access for those users that you clear Apply Group Policy for.

Minimize the Use of the Block Policy Inheritance Feature

As mentioned previously, you can prevent Group Policy settings of parent Active Directory containers from affecting users and computers in lower-level parent Active Directory containers. This is a useful and powerful feature that you should use

judiciously only when a particular situation requires it. Blocking the inheritance of policy from parent Active Directory containers can complicate troubleshooting policy.

Minimize the Use of the No Override Feature

You can also ensure that the policy settings you specify in a given Group Policy object at a higher-level parent Active Directory container are enforced on lower-level parent Active Directory containers by using the No Override option. Only use this powerful feature when circumstances require it. Overuse of this feature with other related features, such as Block Policy Inheritance, can complicate troubleshooting policy.

Use Loopback Processing Only When Necessary

You can set User Configuration per computer and thus override user-specific policies with computer-specific policies. This is useful when you want to provide a specific desktop configuration regardless of which users log on to the computer. To set User Configuration per computer, you would use the Administrative Templates node under **Computer Configuration** in the Group Policy snap-in. For more information on this feature, see [Group Policy Loopback Support](#).

Avoid Using Cross-Domain GPO Assignments

Although you can assign Group Policy objects from different domains to a single Active Directory container if a particular situation requires it, you should note that in such cases Group Policy processing would be slower. This is because domain boundaries are crossed.

Design Examples

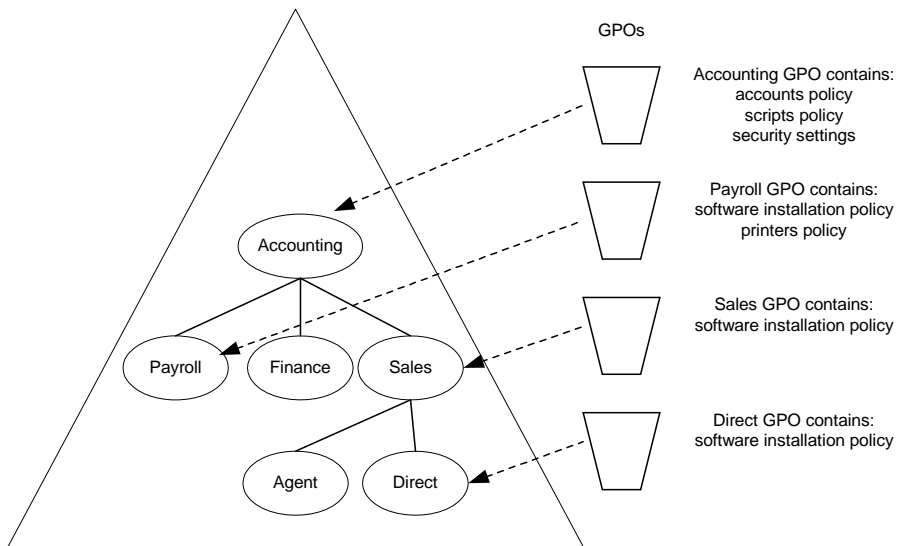
This section presents several models of GPO design. These examples are not intended as guidelines, but they do illustrate various ways to approach GPO design. In most corporate environments, administrators may use a combination of these or similar models, tailored to their business requirements.

The key overriding approaches are either functional or geographic models. The rest are usually variants of those.

Layered GPO Design Model

The objective of this design model is to create Group Policy objects based on a layered approach. This approach optimizes maintenance of Group Policy objects and facilitates delegation.

The following graphic illustrates an example of this model.

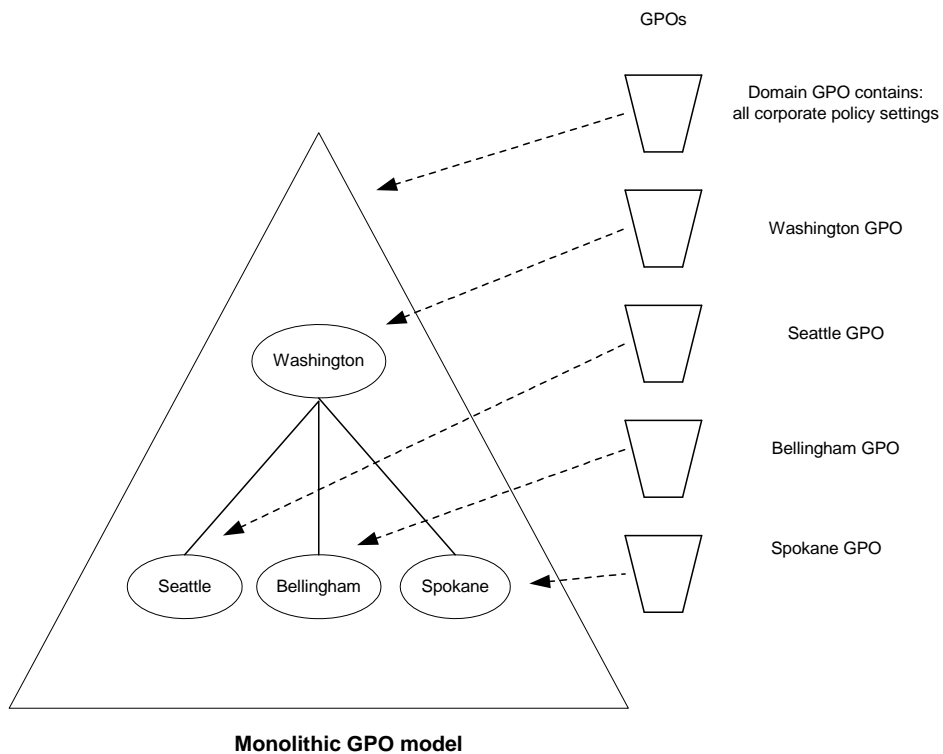


Layered GPO model

Monolithic GPO Design Model

The objective of this design is to create Group Policy objects based on a monolithic design—an approach that reduces the number of Group Policy objects that apply to a user and/or computer but may not be optimal for delegation.

The following graphic illustrates an example of the monolithic GPO model.

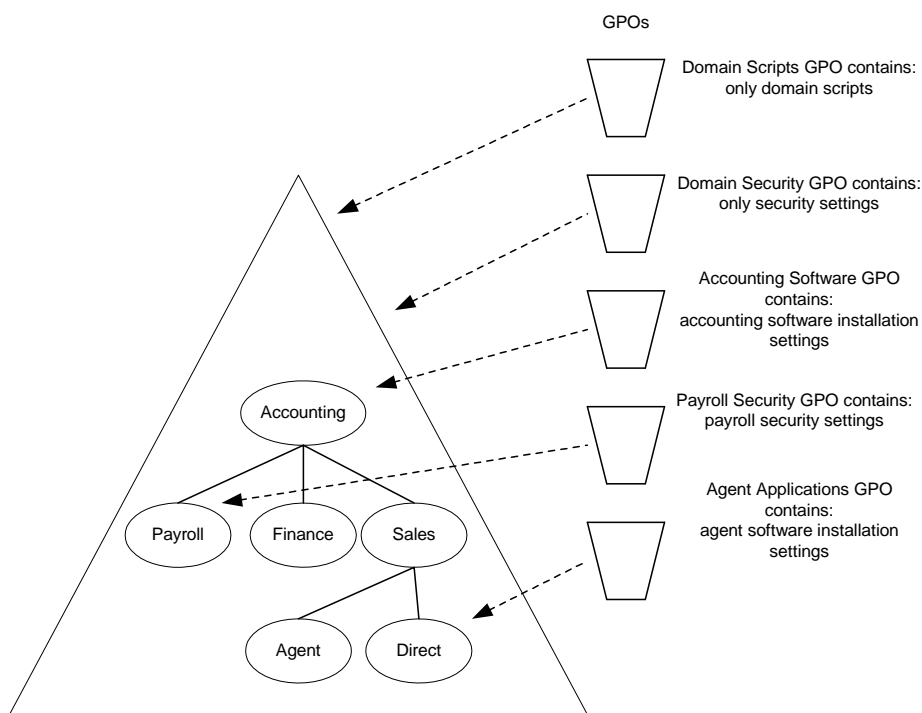


Single Policy Type GPO Design Model

The objective of this design is to create Group Policy objects that deliver a single type of Group Policy, for example, policy for security settings. Such a design optimizes separation of duties for administrators; however, it may increase the number of GPOs that are applied to a given user or computer.

Each Group Policy object delivers only one type of policy (security Group Policy objects are different from script Group Policy Objects, for example). Large corporations often create separate administrator groups based on administrative duties; this scenario would be useful in such corporate environments.

The following graphic illustrates an example of the single policy type GPO model.



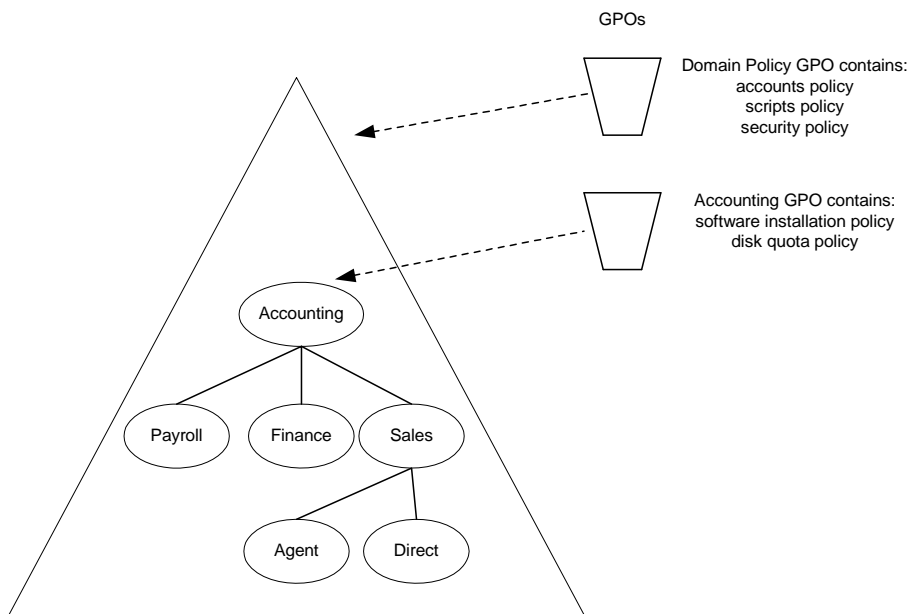
Single Policy GPO Model

Multiple Policy Types GPO Design Model

The objective of this design is to create Group Policy objects that deliver multiple types of policy. This is a hybrid of the single policy and monolithic models. Each Group Policy object delivers several types of policy settings.

For example, you can create a Group Policy object that includes Group Policy settings for software settings and application deployment and create another GPO that includes security and scripts settings, and so on. A Group Policy object design that supports multiple policy types is useful in delegating administration environments and can reduce the number of Group Policy objects that apply to a user and/or computer.

The following graphic illustrates an example of the multiple policy types GPO model.

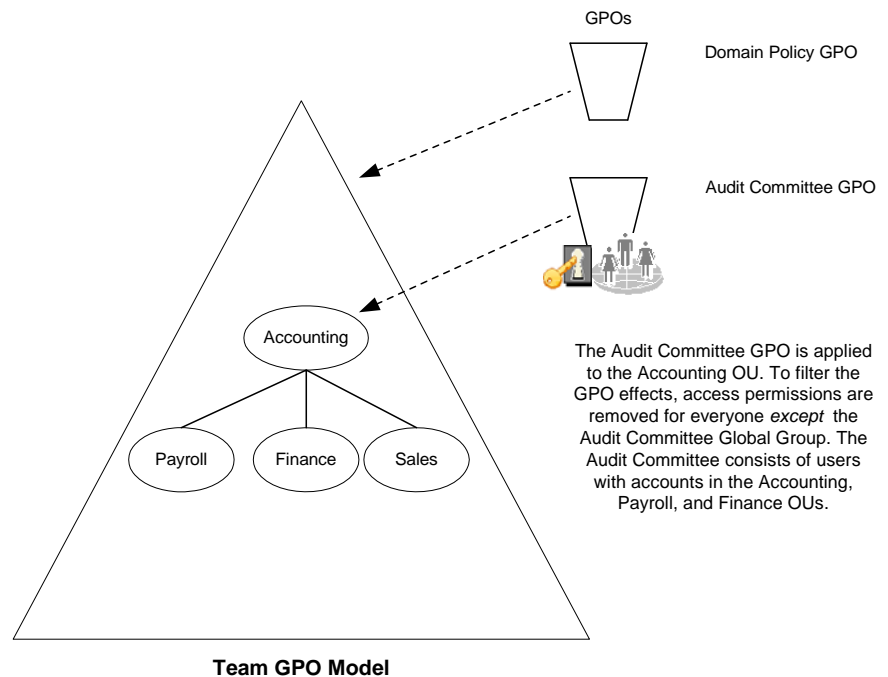


Multiple Policy Types GPO

Teams or Matrix Organizations GPO Model

This model applies to organizations that leverage the virtual team concept. Individuals within the organization form teams to perform a task or project and each individual is a member of multiple teams. Each team has specific Group Policy requirements. The OU architecture does not reflect the team structure. This model works by using security group filtering.

The following graphic illustrates an example of the team GPO design model.

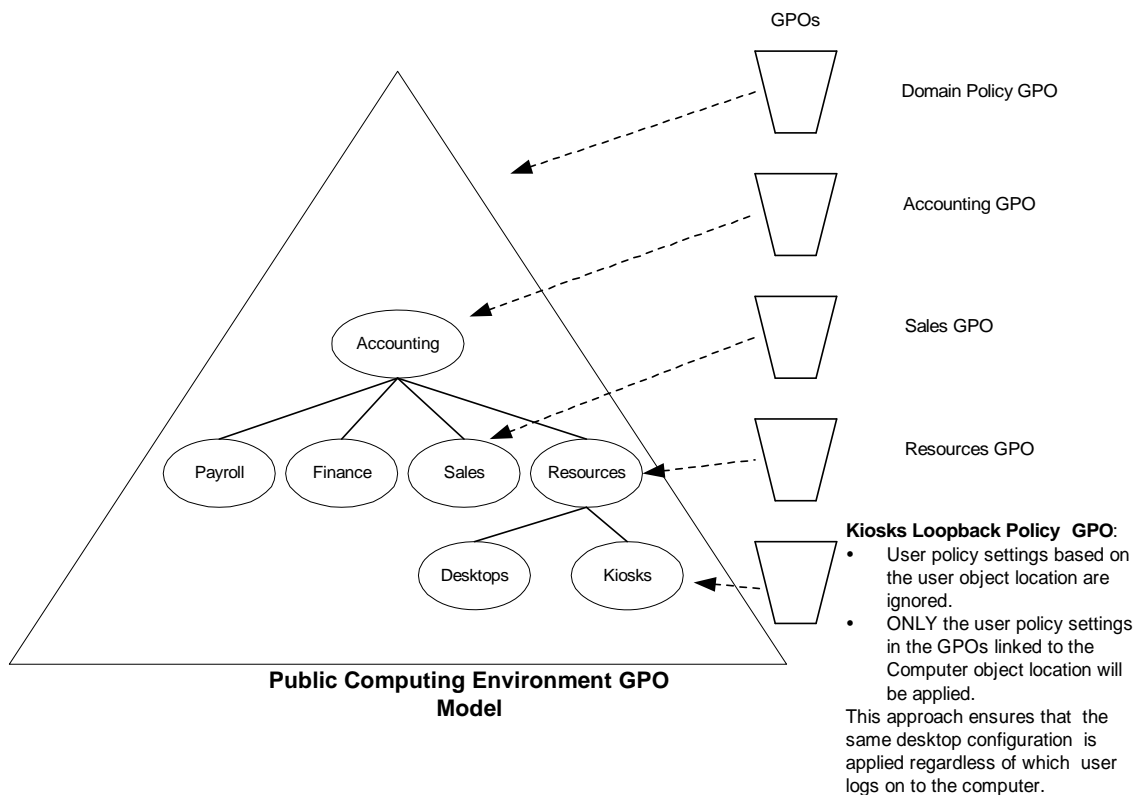


Public Computing Environment GPO Model

This scenario applies to environments where you want the computer Group Policy settings to always have precedence over the user Group Policy settings. This scenario is useful for training classes and kiosk-type environments in which you want to provide the same desktop environment regardless of which user logs on to the computer.

The following graphic illustrates an example of the GPO design for a public computing environment. The loopback policy feature with **Replace mode** is used in this example. See [Group Policy Loopback Support](#) for more information.

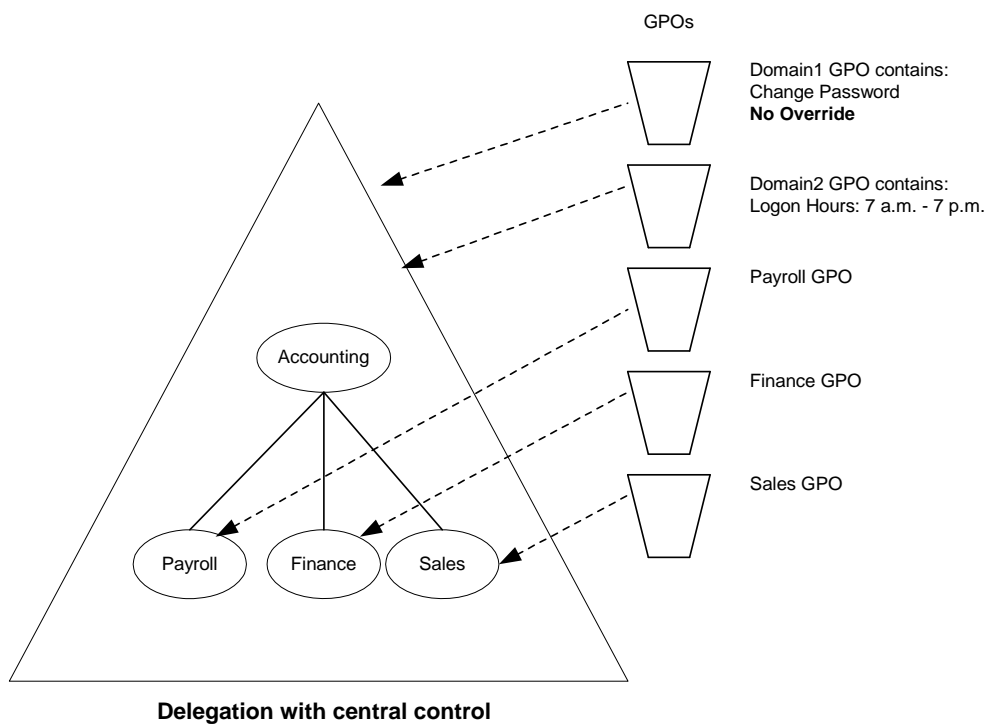
Normal Group Policy processing specifies that users in the Sales OU get these GPOs: Domain Policy GPO, Accounting GPO, and Sales GPO. With the loopback policy enabled in **Replace mode**, when users from the Sales OU log on to a computer in the Kiosks OU, the user will process *only* these GPOs: Domain Policy GPO, Accounting GPO, Resources GPO, and Kiosks Loopback Policy GPO—the users' list of GPOs is not gathered in this case. More specifically, the user settings specified in the Kiosks OU (and those inherited) are the *only* GPOs processed for the user logging onto computers in that OU. Those in the Users OU tree are not processed.



Delegation with Central Control

This model applies to organizations that choose to delegate administration of GPOs, but would like to enforce certain Group Policy settings throughout the domain (for example, specific security policies).

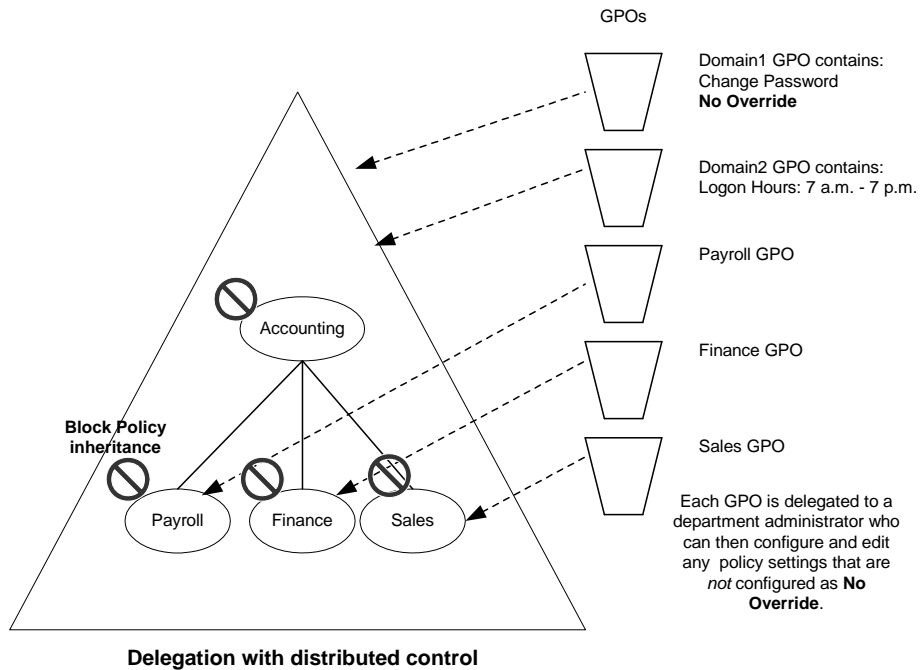
The following graphic illustrates an example of GPO delegation with centralized control, and use of the **No Override** option.



Delegation with Distributed Control

This scenario applies to organizations that want to allow administrators of organizational units to prevent Group Policy settings from being applied to their OU. The administrator of an OU can block Group Policies that have been assigned at higher levels in the hierarchy from applying to his or her OU. However, the administrator cannot block group policies that are marked as *No Override*.

This feature allows organizations to minimize the number of domains without sacrificing autonomy.



IntelliMirror Features without Active Directory

The full functionality of IntelliMirror requires Active Directory and Group Policy. However, in an environment without Active Directory and Group Policy, some of the capabilities are available. You can still implement the following IntelliMirror features to manage Windows 2000 clients:

- Roaming User Profiles and Logon Scripts
- Folder Redirection
- Internet Explorer Maintenance
- Administrative Templates (registry-based policy)

Roaming User Profiles and Logon Scripts

When using either a Windows NT 4.0 domain or Active Directory, both roaming user profiles and logon scripts are configured on the user object.

Folder Redirection

You can redirect special folders to alternate locations, either to a local or network location. You do this by modifying the values under the following registry key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Each value is of type **REG_SZ**, and the data is the redirected path (either local or UNC). The table below lists the folders that may be redirected and their associated value name.

Folder	Name
My Documents	Personal
My Pictures	My Pictures
Application Data	AppData
Desktop	Desktop
Start Menu	Start Menu

Internet Explorer Maintenance

Instead of using Group Policy to control Internet Explorer settings, administrators can use the Internet Explorer Administration Kit (IEAK) to apply settings to Internet Explorer clients using auto-configuration packages. The IEAK can be downloaded from <http://www.microsoft.com/windows/ieak>.

Applying Administrative Templates (Registry-Based Policy)

Domain-based Group Policy processing requires that the User and/or Computer objects be located in a Windows 2000 Active Directory. If the User or Computer objects are located in a Windows NT 4.0 domain, then Windows NT 4.0 System Policy will be processed for whichever of these objects is located in that domain—this could be the Computer or User object, or both. System Policy is defined as the

policy mechanism used natively in Windows NT 4.0; it is a set of registry settings that together define the computer resources available to a group of users or an individual. (Also be aware that the local GPO is always processed prior to any System policy.)

This section explains how to use System Policy to deliver the registry-based (Administrative Templates) policy settings that are available in Windows 2000. This may be needed for Windows 2000 clients that have either or both of the User or Computer objects located in Windows NT 4.0 domains. These procedures will also work for providing System policy from any Server Message Block (SMB)-enabled share or even from a local share.

Setting Registry-based Policy in a Windows NT 4.0 Domain

A Windows 2000 client will process System Policy if either the user and/or computer account are in a Windows NT 4.0 domain. (For exact details on processing behavior, see the section later in this document called [Migrating Policy-Enabled clients from Windows NT 4.0 to Windows 2000](#)). The client looks for the Ntconfig.pol file used by Windows NT 4.0-style System Policy. By default, it looks for this file in the NETLOGON share of the authenticating Windows NT 4.0 domain controller.

Setting Registry-based Policy in a Workgroup Environment

In the absence of a Windows NT 4.0 domain, the client can be configured to look for the NTconfig.pol file on the local computer or on any SMB share location, as explained in the section below, [Specifying a Manual Path to Retrieve the Policy File from a Specific Location](#).

Creating NTconfig.pol Files Based on Windows 2000 .Adm Files

Using the procedure below, you can create NTconfig.pol files based on the new Windows 2000 .Adm files, and apply these settings to Windows 2000 Server or Professional clients.

You will need the Windows NT 4.0 System Policy Editor tool, Poledit.exe. This tool is installed with Windows 2000 Server and Windows 2000 Advanced Server. You can install Poledit.exe on Windows 2000 Professional computers by installing the Windows 2000 Administration Tools that are included on the Windows 2000 Server and Windows 2000 Advanced Server CD-ROMs. To install Windows 2000 Administration Tools on a Windows 2000 Professional computer, open the i386 folder on the applicable Windows 2000 Server disc and then double-click the Adminpak.msi file. Follow the instructions that appear in the **Windows 2000 Administration Tools Setup** wizard.

Note: The System Policy Editor (Poledit.exe) from any previous operating system version cannot read the Unicode-formatted .adm files shipped in Windows 2000. You will need to use the version of System Policy Editor that ships in Windows 2000, which has been updated to support Unicode. Alternatively, you can use an

older version of Poedit.exe, if you resave the .adm files as .txt files without Unicode encoding.

1. Remove all **#if version** and **#endif** statements from the following .adm files: system.adm, inetres.adm, conf.adm, and then save the files. Do this to byprevent inadvertent loading of these files by poedit. (You can use Notepad or other text editor tool to edit these .adm files).

For example, in the Inetres.adm file, remove these lines:

```
#if version <= 2  
#endif
```

2. To open Poedit.exe from Windows 2000, click **Start**, click **Run**, and type **poedit.exe**.
3. In the **System Policy Editor** window, click **Policy Template** on the **Options** menu.
4. In the **Policy Template Options** dialog box, click **Add**, and then select one of the modified template files (the .adm files that you modified in step 1 above), and click **OK**.
5. Specify the appropriate policy settings based on groups (or not), as documented in the System Policy Editor online Help and below.
6. Save the file as NTconfig.pol to the Netlogon share of the Windows NT 4.0 domain controller. Alternatively, you can manually set a path for the policy file to use, as described in the [Specifying a Manual Path to Retrieve the Policy File from a Specific Location](#) section later in this document.

Note: The System Policy Editor is *not* included in Windows 2000 Professional, but is installed when you install the Windows 2000 Administrative Tools package on Windows 2000 Professional. The Windows 2000 Administration Tools can be installed from Adminpak.msi, located in the I386 folder of the Windows 2000 Server CD.

When you install the AdminPack, Poedit.exe and its supporting .adm files (Winnt.adm, Windows.adm, and Common.adm) are installed into the \System directory and the \Inf directory, as they were in Windows NT 4.0. Note that Poedit.exe is not added to the **Start** menu, but it is accessible from the command line.

System Policy Files

Policies can define a specific user's settings or the settings for a group of users. The resulting policy file contains the registry settings for all users, groups, and computers that will be using the policy file. Separate policy files for each user, group, or computer are not necessary.

To create a policy that will be automatically downloaded from validating domain controllers, create a .pol file.

- For Windows NT 4.0 and Windows 2000, your .pol file should be named

NTconfig.pol and must be created using the System Policy Editor running on either of these platforms.

- For Windows 95, Windows 98, and Windows Millennium Edition, your .pol file should be named Config.pol and must be created using the System Policy Editor running on any of these platforms.
- As system administrator, you have the option of choosing an alternate name for the .pol file and directing the computer to update the policy from a path other than the NETLOGON share. You can do this either by manually changing the registry or by using System Policy, as described in the next section. This path can even be a local path such that each computer has its own policy file. However, if a change is necessary to all computers, this change must be made individually to each workstation.

When a user of a Windows 2000 client logs on to a Windows NT 4.0 domain, if the client is working in Automatic mode (which is the default), it checks the NETLOGON share on the validating domain controller for the NTconfig.pol file. If the client finds the file, it downloads it, parses it for the user, group, and computer policy data, and applies it if appropriate. If the client does not locate the policy file on its validating domain controller, it will not check any others. It is therefore critically important that replication of the NTconfig.pol file take place among the domain controllers performing authentication. The NETLOGON share for Windows NT 4.0 is in %SystemRoot%\repl\import\scripts. The NETLOGON share for Windows 2000 is in %SystemRoot%\Sysvol\Sysvol\

For more information on System Policy, refer to the “[Implementing Profiles and Policies for Windows NT 4.0](http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp)” white paper at http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp.

Specifying a Manual Path to Retrieve the Policy File from a Specific Location

You can change the default behavior so that a Windows 2000 client looks in a different location than the NETLOGON share. The **UpdateMode** registry setting forces the computer to retrieve the policy file from a specific location (expressed as a UNC path), regardless of which user logs in. You can set the **UpdateMode** setting using either the System Policy Editor in conjunction with the Common.adm file, or you can do this manually by editing the registry as described next.

In the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Update:

- Change the value of the **UpdateMode** to a hexadecimal value of 2 (Type = **REG_DWORD**).
- Create a string value called **NetworkPath**, and set the value to be the fully qualified file name of the .pol file to be loaded. (Type = **REG_SZ**).

To retrieve the policy file from a specific location

1. Open **System Policy Editor**, by clicking **Start**, clicking **Run**, and then typing **poledit**.
2. Ensure that the System.adm file is loaded. To do this, click **Options**, click **Policy Template**, and then in the **Policy Template Options** dialog box, make sure that System.adm is listed in the **Current Policy Template(s)** list box. If it is not listed, click **Add** to add this file.
3. To open the **Default Computer** policy, on the **File** menu, click **New Policy**, and double-click **Default Computer** from the **Policies for** list.
Or, to open the **Local Computer** policy, click **Open Registry** on the **File** menu, and then double-click **Local Computer**.
4. In the **Properties** dialog box (for either **Default Computer** or **Local Computer**), click the **Network** node, and click the **System policies update** node to display the **Remote update** option.
5. Check the **Remote update** box.
6. In the **Update mode** drop-down box, select **Manual (use specific path)**.
7. In the **Path for manual update** text box, type the UNC path and file name for the policy file to use.
8. Click **OK** to save your changes.

The first time the Windows 2000 client is modified locally using the System Policy Editor or receives a default System Policy file from the NETLOGON share of a domain controller, this location is written to the registry. Thereafter, all future policy updates use the location you specified manually. Note that this is a permanent change until the policy file resets the option to Automatic. The Windows 2000 client will *not* look at a domain controller again to find a policy file until you either change the instruction in the local registry, or modify the policy file in the location specified by the manual path to set the mode back to Automatic.

Migrating Policy-Enabled Clients from Windows NT 4.0 to Windows 2000

This section discusses behavior of Group Policy and System Policy in relation to migration to Windows 2000.

Windows NT 4.0 and Windows 2000 Policy Comparison

Group Policy is not System Policy from Windows NT 4.0. Although Group Policy does include the functionality from Windows NT 4.0 System Policy, it also provides policy settings for scripts, software installation, security settings, Internet Explorer maintenance, folder redirection, and Remote Installation Services.

In Windows NT 4.0 (and Windows 95 and Windows 98), the System Policies you specify with Poedit.exe:

- Are applied to domains.
- May be further controlled by user membership in security groups.
- Are not secure.
- Persist in users' profiles (this is sometimes referred to as *tattooing* the registry). This means that after a registry setting is set using Windows NT 4.0 System Policies, the setting persists until the specified policy is reversed or the user edits the registry.
- Are limited to desktop lockdown.

In Windows 2000, Group Policy:

- Represents the primary method for enabling centralized Change and Configuration Management. You can use Group Policy to manage registry-based policy, software installation options, security settings, scripts (for computer startup and shutdown, and for user logon and logoff), Internet Explorer maintenance, folder redirection, and Remote Installation Services.
- Can be associated with sites, domains, and organizational units.
- Affects all users and computers in the specified Active Directory container (site, domain, or OU) by default.
- May be further controlled by user or computer membership in security groups.
- Settings are secure.
- Default policy settings do not persist in the registry.
- Can be used for tightly managed desktop configurations and to enhance the user's computing environment.

The Windows NT 4.0 effect of persistent registry settings can be problematic when a user's group membership is changed. An advantage of Windows 2000 Group Policy is that this does not occur. When a Group Policy object no longer applies, registry settings written to the following two secure registry locations are cleaned up:

- \Software\Policies
- \Software\Microsoft\Windows\CurrentVersion\Policies

Migrating to Windows 2000

Migrating Windows NT 4.0-based clients and servers to Windows 2000 in various combinations causes different behavior for Group Policy. In a pure Windows 2000 environment where both the user and computer accounts are in a Windows 2000 domain, Windows 2000 clients process only Group Policy. System Policy is not processed. However, Windows 2000 clients can process System Policy in cases where either the user account and/or the computer account is not located in a Windows 2000 domain.

In many organizations it may be impractical to upgrade all Windows NT 4.0 servers and client computers simultaneously to Windows 2000. In this case, it is important that you know how Windows 2000 Group Policy and Windows NT 4.0 System Policy are affected during and after the migration process. This section presents information on the effects of migration on Group Policy.

Client Computers

Group Policy applies only to Windows 2000-based or later computers. There is no mechanism to process Group Policy on clients running Windows NT 4.0, Windows 95, Windows 98, and Windows Millennium Edition. Although Group Policy cannot be used on these clients, you can still use Windows NT 4.0-based System Policies. For more information, see the section called [Applying Administrative Templates \(Registry-Based Policy\)](#) earlier in this document.

Domain Controllers

For clients that are running Windows 2000, the processing of Group Policy varies depending on whether the user and computer accounts are located in a Windows NT 4.0 domain or in a Windows 2000 Active Directory domain.

The following table summarizes the behavior of the client with respect to policy, depending on whether the computer or user accounts (or both) are located on a Windows NT 4.0 Server-based server or on a Windows 2000 Server-based server with Active Directory.

In the table below, it is assumed that client computers are running Windows 2000. Clients that receive Windows NT 4.0 System Policy obtain it either from the NETLOGON share of the users' logon server or a redirected path.

Environment	Account Object Location	What Affects the Client
Pure Windows NT 4.0	Computer: Windows NT 4.0	At computer startup: Computer local Group Policy (only if changed). Every time the user logs on: Computer System Policy.
"	Computer refresh	Before Control-Alt-Delete: Computer local Group Policy only. After the user logs on: Computer local Group Policy and computer System Policy.
"	User: Windows NT 4.0	When the user logs on: User System Policy. If local Group Policy changes: User local Group Policy and user System Policy.
"	User refresh	User local Group Policy and user System Policy.
		(continued)

Environment	Account Object Location	What Affects the Client
Mixed (migration)	Computer: Windows NT 4.0	At computer startup: Computer local Group Policy (only if changed). Every time the user logs on: Computer System Policy.
	Computer refresh	Before Control-Alt-Delete: Computer local Group Policy only. After the user logs on: Computer local Group Policy and computer System Policy.
	User: Windows 2000	When the user logs on: Group Policy is processed after computer System Policy.
	User refresh	User Group Policy.
Mixed (migration)	Computer: Windows 2000	During system startup: Group Policy.
	Computer refresh	Computer Group Policy
	User: Windows NT 4.0	When the user logs on: User System Policy. If local Group Policy changes: User local Group Policy and user System Policy.
	User refresh	User local Group Policy and user System Policy.
Windows 2000	Computer: Windows 2000	During computer startup and when the user logs on: Group Policy.
	User: Windows 2000	
Windows 2000 in a workgroup (without Active Directory)	Local	Local Group Policy only.

Note: When the computer account object exists in a Windows NT 4.0 domain and the user account object exists in a Windows 2000 domain, computer System Policy is processed *when the user logs on*. It is recommended that you move out of this mixed processing mode and into a pure Windows 2000 mode as quickly as possible.

Upgrading Computer or User Accounts from Windows NT 4.0 to Windows 2000

While the user or computer accounts were managed by a Windows NT 4.0 domain controller, the registry on the client computers may have been altered outside the approved Group Policy trees. When a domain controller holding either the user or computer accounts is upgraded to Windows 2000, these settings remain on the

client computers unless the administrator undoes them by means of System Policy or by doing a clean install of Windows 2000 on the client computers.

For example, consider the following migration scenario:

1. Start with a Windows NT 4.0 domain with Windows NT 4.0 clients, and create and apply System Policies.
2. Upgrade one client to Windows 2000.
3. Verify that the System Policies are applied to the Windows 2000 client. The Windows 2000 client registry has now been *tattooed* with those System Policies. This is because System Policies have no mechanism for cleaning up registry entries that should no longer be applied. (This is referred to as *tattooing* the registry.)
4. Upgrade the Windows NT 4.0 PDC to Windows 2000 DC.
5. Make sure the user account and the computer are in a Windows 2000 domain.
6. Modify the System Policies NTconfig.pol and resave.

In this case, the System Policies changes made in step 6 will not apply to the client because Windows 2000 clients do not process System Policies when both the user and computer accounts are in a Windows 2000 domain.

Try to avoid this situation by performing a clean installation of Windows 2000. To facilitate a clean installation, you can use the User State Migration Tool to migrate the users' data and settings to the new installation. Note that this tool can be customized to make changes in the registry, allowing you to clean up tattooed System policy settings. The User State Migration Tool will be available in the Windows 2000 Server Resource Kit, Supplement One. See <http://www.reskit.com/> for details.

If a clean installation is not possible, consider using Regini.exe (available in the Resource Kit) to modify the registry settings.

For a comparison of the policy-related namespace in Windows NT 4.0, the Zero Administration Kit, and Windows 2000, see [Appendix D](#) in this document.

Windows NT 4.0 Clients

Windows 2000 has heightened security so that the local system of Windows NT 4.0 clients cannot read user security group information from the Active Directory. Prior to Service Pack 6, Windows NT 4.0 clients requested System Policies in the local system context, which means they will not get any System Policies based on security groups. Clients running Windows NT 4.0 Service Pack 6 (or later) or Windows 2000 impersonate the user rather than running in local system context when requesting System Policy. The most likely occurrence of this is in an upgrade of a Windows NT 4.0 Server to Windows 2000. The Windows NT 4.0 clients still get any user-specific or the default domain policies. If a user was previously getting

policies based on group membership, and default policies exist, the client now processes only the default policies.

For detailed information on Windows 2000 security, see the Security Services white papers at:

<http://www.microsoft.com/windows2000/library/technologies/security/default.asp>.

Zero Administration Kit (ZAK) for Windows to Windows 2000 Upgrades

This section presents information on upgrading ZAK-based servers and clients to Windows 2000.

Information on the [Zero Administration Kit for Windows](http://www.microsoft.com/windows/zak) is available at <http://www.microsoft.com/windows/zak>.

ZAK Upgrades

The following table highlights the results of upgrading domain controllers from Windows NT 4.0 to Windows 2000, or upgrading clients from Windows NT 4.0 ZAK and Windows 98 ZAK to Windows 2000, and Windows 2000 installations and upgrades in various combinations.

Domain Controller	Client	Results
Windows NT 4.0	Windows NT 4.0 ZAK upgrade to Windows 2000	The upgraded ZAK client functions in the same way as the pre-upgrade ZAK client. All System Policy is applied to the client.
Windows NT 4.0	Windows 98 ZAK upgrade to Windows 2000 ¹ .	In order to get policy, the client will require Windows NT 4.0-style System Policy.
Windows NT 4.0	Clean Windows 2000 install	Client setup will not correspond to that of a ZAK-style client ² .
Windows NT 4.0 upgrade to Windows 2000	Windows NT 4.0 ZAK	The client gets ZAK-style System Policy.
Windows NT 4.0 upgrade to Windows 2000	Windows 98 ZAK	The client gets ZAK-style System Policy.
Windows NT 4.0 upgrade to Windows 2000	Windows 2000 upgrade	In order to get policy, the client will require Group Policy.
Windows NT 4.0 upgrade to Windows 2000	Clean Windows 2000 install	The client gets Group Policy.
Windows NT 4.0 upgrade to Windows 2000	Install Windows NT 4.0 ZAK client	The client gets ZAK-style System Policy.
Windows NT 4.0 upgrade to Windows 2000	Install Windows 98 ZAK client	The client gets ZAK-style System Policy.

¹ Clients upgraded from Windows 98 ZAK to Windows 2000 require Windows NT 4.0-style System Policies. This is because the Windows 2000 client looks for Ntconfig.pol file in the Netlogon share. Installing ZAK support for Windows NT 4.0 is recommended. It is also possible to manually copy the policy file(s) using the [Zero Administration Kit for Windows](http://www.microsoft.com/windows/zak) instructions for Manual TaskStation or AppsStation setup.

² If administrators want to have ZAK-like functionality in a Group Policy environment, they can either install ZAK and then upgrade to Windows 2000, or use Group Policy and Folder Redirection to create a ZAK client. For more information, see the upcoming section called Adding New Windows 2000 Client Computers to a ZAK Environment.

The following section summarizes the results of upgrading Windows 98 ZAK clients and Windows NT 4.0 ZAK servers and clients to Windows 2000:

Windows NT 4.0 ZAK Client Upgrades

Windows 2000 upgrade clients that are managed by a Windows NT 4.0 domain controller continue to get System Policy. ZAK policies will work correctly; all functionality as a ZAK client is preserved.

Windows 98 ZAK Client Upgrades

Windows 2000 upgrade clients that are managed by a Windows NT 4.0 domain controller will not get their previous Windows 98 policy. Windows 2000 clients in a Windows NT 4.0 domain do not recognize the Config.pol file but instead look for the Ntconfig.pol file in the Netlogon share. You can ensure these clients continue to get System Policy by creating an NTconfig.pol file that has the same settings that were contained in the Config.pol file.

Primary Domain Controller Upgrade to Windows 2000 Domain Controller

The upgrade and promotion to domain controller processes work seamlessly, but because the domain is now Windows 2000, any Windows 2000 ZAK upgrade clients will cease processing System Policy and will need to have equivalent Group Policy applied. See the section called [ZAK in Group Policy](#) for the GPO-based policy settings required.

Adding New Windows 2000 Client Computers to a ZAK Environment

A clean installed Windows 2000 computer joined to a Windows NT 4.0 ZAK domain will not be set up correctly to be a ZAK-style client. If administrators want a Windows 2000 ZAK-style client, they can install Windows NT 4.0 ZAK client software first, and then upgrade the client to Windows 2000.

Alternatively, administrators can set up a clean install Windows 2000 computer as a ZAK client by redirecting the Start menu and Programs folders to point to the Netapps share on the ZAK server. It is also necessary to apply the Group Policy settings specified in the upcoming section called [ZAK in Group Policy](#). In addition, the user account for this new computer should be set up in accordance with the instructions given in the [Administrator's Guide for the Zero Administration Kit](#) (found at <http://www.microsoft.com/windows/zak/getzak.htm>), in the section called **Organizing Files, Shares and User Accounts on the Server. Finally, it is also necessary to redirect AppData to the Users account share.**

ZAK in Group Policy

In the case of a domain controller being upgraded to Windows 2000 with upgraded clients, it will be necessary to create a Group Policy object to specify policy settings.

To prevent all users in the domain from getting these policy settings, it is recommended that administrators create a security group for the targeted users and computers, and then use this group to filter the application of the GPO to the group members.

Group Policy Settings Required to Emulate a ZAK Installation

To emulate a ZAK installation, administrators must enable the Group Policy settings listed in this section.

Component and Group Policy snap-in namespace location	Policy settings to be enabled
Internet Explorer: Internet Control Panel Settings Located under User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel node	Disable the General Page Disable the Security Page Disable the Contents Page Disable the Connections Page Disable the Programs Page Disable the Advanced Page
Internet Explorer: Toolbars Settings Located under User Configuration\Administrative Templates\Windows Components\Internet Explorer\Toolbars node	Disable Customizing Browser Toolbar buttons Disable Customizing Browser Toolbars
Windows Explorer Settings Located under User Configuration\Administrative Templates\Windows Components\Windows Explorer node	Enable Classic Shell Remove Folder Options menu item from the Tools Menu Remove "Map Network Drive" and "Disconnect Network Drive" Disable Windows Explorer Default context menu Hide the manage item on the Windows Explorer context menu Hide these specified drives on My Computer [Hide all Drives] Hide hardware tab No "Computers near me" in My Network Places No "Entire Network" in My Network Places

Component and Group Policy snap-in namespace location	Policy settings to be enabled
<p>Task Scheduler Settings Located under User Configuration\Administrative Templates\Windows Components\Task Scheduler node</p>	Hide Property Pages Prevent Task Run or End Disable Drag-and-Drop Disable New Task Creation Disable Task Deletion Disable Advanced Menu Prohibit Browse
<p>Start Menu and Taskbar Settings Located under User Configuration\Administrative Templates\Start Menu & Taskbar node</p>	Remove Users folder from Start Menu Disable and Remove Links to Windows Update Remove Common Program Groups from Start Menu Disable Programs in Settings Menu Remove Network & Dialup Connections from Start Menu Remove Favorites from Start Menu Remove Search menu from Start Menu Remove Run menu from Start Menu Disable and Remove Shutdown Command Disable Drag-and-Drop context menus on the Start Menu Disable Changes to Taskbar & Start Menu Settings Disable Context menus for the Taskbar Disable Personalized Settings Disable User Tracking Disable Add "Run in separate memory space" checkbox to Run Dialog box
<p>Active Desktop Settings Located under User Configuration\Administrative Templates\Desktop\Active Desktop node</p>	Hide All Items
<p>Desktop Settings Located under User Configuration\Administrative Templates\Desktop node</p>	Hide all icons on Desktop Prohibit User from changing My Documents path Disable adding, dragging, dropping and closing the Taskbar Toolbars Don't save setting on exit
<p>Control Panel: Add/Remove Programs Settings Located under User Configuration\Administrative Templates\Control Panel\Add/Remove Programs node</p>	Disable Add/Remove Programs

Component and Group Policy snap-in namespace location	Policy settings to be enabled
Control Panel: Display Settings Located under User Configuration/Administrative Templates/Control Panel/Display node	Disable Display in Control Panel
Control Panel: Regional Options Settings Located under User Configuration/Administrative Templates/Control Panel/Regional Options node	Restrict Selection of Windows 2000 Menus and Dialogs Language
System: Logon/Logoff Settings Located under User Configuration/Administrative Templates/System/Logon/Logoff node	Disable Task Manager Run Logon Scripts Synchronously
Task Scheduler Settings Located under Computer Configuration/Administrative Templates/Windows Components/Task Scheduler node	Hide property page Prohibit Browse

Appendix A: Security Settings and User Rights

This appendix lists the Security Settings that are defined by default in the Default Domain Policy GPO. This GPO is created when the first domain controller in the domain is installed by DCPromo. If this first domain controller is upgraded from a Windows NT 4.0 domain controller, then the values defined for the Windows NT 4.0 domain are used instead.

These domain-wide account policy settings (Password Policy, Account Lockout Policy and Kerberos Policy) are enforced by the domain controller computers in the domain; therefore, all domain controllers always retrieve the values of these account policy settings from the Default Domain Policy GPO.

For a detailed description of each policy setting, refer to the Windows 2000 Server Resource Kit Online Help file for Group Policy, GP.CHM.

Policy	Default Value	Comment
Password Policy		
Enforce password history	1 password remembered	
Maximum password age	42 days	
Minimum password age	0 days	
Minimum password length	0 characters	
Passwords must meet complexity requirements	Disabled	
Store password using reversible encryption for all users in the domain	Disabled	
Account Lockout Policy		
Account Lockout Threshold	0	
Kerberos Policy		
Since Kerberos support was not available in previous versions of Windows NT, the following Kerberos policies are always defined for the first domain controller of a Windows 2000 domain, regardless of whether it was upgraded or not.		
Enforce user logon restrictions.	Enabled	
Maximum lifetime that a user ticket can be renewed	7 days	
Maximum user ticket lifetime	10 hours	
Maximum service ticket lifetime	60 minutes	
Maximum tolerance for synchronization of computer clocks	5 minutes	
Security Options		
Automatically logoff users when logon time expires	Disabled	This is a domain-wide setting even though it appears under the Security Options area.

Security Settings in the Default Domain Controllers Policy
 This section lists the Security Settings that are defined by default in the Default Domain Controller Policy GPO. This GPO is created when the first domain controller in the domain is installed via DCPromo. If this first domain controller is upgraded from a Windows NT 4.0 domain controller, then the values defined for the Windows NT 4.0 domain are used instead.

By default, these settings apply to all domain controllers in the domain. For a detailed description of each policy setting, refer to the Windows 2000 Server Resource Kit Online Help file for Group Policy, GP.CHM.

Policy	Default Value	Comment
Security Options		
Digitally sign server-side communication when possible	Enabled	
Audit Policy		
Audit Account Logon events	No Auditing	
Audit Account Management	No Auditing	
Audit Directory Service Access	No Auditing	
Audit Logon Events	No Auditing	
Audit Object Access	No Auditing	
Audit Policy Change	No Auditing	
Audit Privilege Use	No Auditing	
Audit Process Tracking	No Auditing	
Audit System Events	No Auditing	
User Rights Policy		
Access this computer from the network	Administrators, Authenticated Users, Everyone	If the following groups were given this right prior to running DCPromo, then they are removed: Backup Operators, Guests, Guest, and Users. If a Windows NT 4.0 domain controller is upgraded as the first Windows 2000 domain controller using a slipstreamed setup of Windows 2000 + Service Pack 1, then the Authenticated Users group is automatically given this right.
Act as part of the operating system		
Add workstations to the domain	Authenticated Users	This User Right is for the support of legacy APIs. You can also allow users to create computer accounts by using this User Right. Authenticated Users can only create 10 computer accounts using this User Right.

Back up files and directories	Administrators, Backup Operators, Server Operators	
Bypass traverse checking	Administrators, Authenticated Users, Everyone	If the following groups were given this right prior to running DCPromo, then they are removed: Backup Operators, Users.
Change the system time	Administrators, Server Operators	
Create a pagefile	Administrators	
Create a token object		
Create permanent shared objects		
Debug programs	Administrators	
Force shutdown from a remote system	Administrators, Server Operators	
Generate security audits		
Increase quotas	Administrators	
Increase scheduling priority	Administrators	
Load and unload device drivers	Administrators	
Lock pages in memory		
Log on as a batch job		
Log on as a service		
Log on locally	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	If the following groups were given this right prior to running DCPromo, then they are removed: Authenticated Users, Guests, Guest Users, and Everyone.
Manage auditing and security log	Administrators	
Modify firmware environment variables	Administrators	
Profile single process	Administrators	

Profile system performance	Administrators	
Replace a process-level token		
Restore files and directories	Administrators, Backup Operators, Server Operators	
Shut down the system	Account Operators, Administrators, Backup Operators, Server Operators, Print Operators	If the following groups were given this right prior to running DCPromo, then they are removed: Authenticated Users, Guests, Guest Users, and Everyone.
Take ownership of files or other objects	Administrators	
Deny Logon Locally		
Deny logon as a batch job		
Deny logon as a service		
Deny Access to this computer from network		
Remove Computer from Docking Station	Administrators	If the following groups were given this right prior to running DCPromo, then they are removed: Users.
Synchronize directory service data		
Enable computer and user accounts to be trusted for delegation	Administrators	If the following groups were given this right prior to running DCPromo, then they are removed: Users.

Help for Windows NT 4.0 Administrators

This section provides information to help administrators who have been using User Manager to configure security policies in the past move to the new model of Group Policy for editing and configuring security policies.

Changing Password Policy for the Domain

To change password policy for the domain, open the Default Domain GPO from the Administrative Tools menu:

1. Click **Start**, point to **Programs**, click **Administrative Tools**, and then click **Domain Security Policy**.
2. In the **Domain Security Policy** console, expand **Security Settings**, expand **Account Policies**, expand **Password Policy**, and then select the policy you want to modify in the results pane. You can then make changes.

Changing Auditing Policy or User Rights for Domain Controllers

To change the Audit policies or User Rights defined for domain controllers, open the Default Domain Controllers GPO from the Administrative Tools menu:

1. Click **Start**, point to **Programs**, click **Administrative Tools**, and then click **Domain Controller Security Policy**.
2. In the **Domain Controller Security Policy** console, expand **Security Settings**, expand **Local Policies**, click either **Audit Policy** or **User Rights Assignment**, and then select the policy you want to modify in the results pane.

Changing local Password Policy on member Workstations or Servers (Non-Domain Controllers)

Because the **Default Domain Policy GPO** applies to all computers in the domain and because domain-level policies override local policy settings, member workstations and servers apply the Default Domain password policy settings to their local account databases by default. If this does not meet your requirements, then the permissions on the **Default Domain GPO** have to be reconfigured so that member computers that you do not want to receive this policy do not have the **Apply Group Policy** permission on the **Default Domain GPO**. After the permissions are configured so that the member computer does not have access to the default domain policy, local policy settings will no longer be overridden by the password policy settings defined in the **Default Domain GPO**.

To modify Local Password Policy security settings using the Local Security Policy UI:

1. Click **Start**, point to **Programs**, click **Administrative Tools**, and then click **Local Security Policy**.
2. In the **Local Security Settings** console, expand **Security Settings**, expand **Account Policies**, click **Password Policy**, and then select in the results pane the policy you want to edit.

Frequently Asked Questions about Security Settings

Is it possible to define different account policies (Password, Lockout, or Kerberos Policies) for different OUs?

No. All domain controllers for a domain enforce the account policies that are defined in the Default Domain Policy. Domain controllers ignore password, lockout, or Kerberos policies defined at an OU or LGPO level.

After modifying a local security setting, the change does not take effect. What is happening?

The Group Policy model specifies that any policies configured locally may be overridden by like policies specified in the domain. The **Local Security Settings** UI lists the local security setting and the effective security setting for each policy item. (You can access the **Local Security Settings** UI by clicking **Start**, pointing to **Programs**, clicking **Administrative Tools**, and selecting **Local Security Policy**). If the effective security setting is different from the local security setting, it implies that there is a policy from the domain that is overriding your setting.

After modifying a domain-level-policy security setting, the change does not take effect. What is happening?

The Group Policy model applies domain-level policy changes periodically; therefore, it is likely that the policy changes made in the directory have not been made to your computer yet. To trigger a policy propagation on a local computer, type the following at the command line:

```
secedit /refreshpolicy MACHINE_POLICY
```

This will cause any changes made to domain-level policies to be applied to the local computer. To force a reapplication of policy to domain level policies, regardless of whether there has been a change or not, type the following at the command line:

```
secedit /refreshpolicy MACHINE_POLICY /enforce
```

You can determine whether or not security was applied successfully by viewing the Application Event Log. If an error occurred during the process of applying security policy, you can get detailed information by setting the following **REG_DWORD** to **0x02**:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-
00C04F79F83A}\ExtensionDebugLevel
```

When this value is set, the Security Configuration Engine (SCE) will log policy-processing information in the Winlogon.log file at
%windir%\Security\Logs\Winlogon.log.

What is the Add Workstation to Domain Logon right, and how does it relate to delegating similar permissions on the directory?

The **Add Workstation to Domain** user right is supported for applications that use downlevel SAM (Security Accounts Manager) NET APIs to create computer accounts. Users that have this right are allowed to create 10 computer accounts in the Active Directory **Computers** container using these down-level APIs. When a user creates a computer account using this user right, the Domain Administrators group becomes the owner of the computer object. Note that this right is *not* recognized when LDAP is used to create computer accounts.

In Windows 2000, the recommended way to allow a user or group to create computer accounts is by granting that user or group the permission to **Create Computer Objects** on the desired container. This can be accomplished in the Active Directory Users and Computers snap-in via the Delegation Wizard or through the **Security** tab on the **Properties** page of the container. When a computer account is created using access control permissions, the actual creator of the object becomes the owner of that object.

Note: The create-computer-object permission should not be granted indiscriminately. Allowing users to create computers in the domain is similar to allowing users to create user accounts in the domain. Unlike Windows NT 4.0, Windows 2000 computer objects can be used to do network authentication and, hence, to access resources over the network. Users that have access permissions to create computer objects are also not subject to any quota restrictions. That is, they can create any number of computer accounts.

The best security practice would be to grant only trusted users (by using a group) the permission to create computer objects. At the time the computer object is created, the creator can define which users are allowed to use that computer object to join their physical computer to the domain.

For more information on security, see the following:

- The Security white papers in the [Windows 2000 Technical Library Web site](http://www.microsoft.com/eindows2000/library/howitworks/default.asp) (at <http://www.microsoft.com/eindows2000/library/howitworks/default.asp>)
- The Planning Distributed Security section of the [Windows 2000 Server Resource Kit Deployment Planning Guide](http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp) at <http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp>
- [Windows 2000 Server online Help](http://windows.microsoft.com/windows2000/en/server/help) at <http://windows.microsoft.com/windows2000/en/server/help>.

Appendix B: Group Policy Settings for Internet Explorer

This section lists the Group Policy settings available for Internet Explorer Maintenance.

Specifying Policy Settings for Internet Explorer Maintenance
The following table lists the available policy settings for **Internet Explorer Maintenance** under **User Configuration\Windows Settings**.

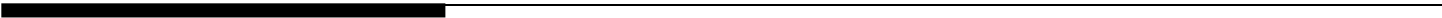
Policy settings under User Configuration\Windows Settings\Internet Explorer Maintenance	Description
\Browser User Interface	
Browser Title	Used to customize the text that appears in the title bar of the Internet Explorer Web browser and Outlook Express. The text that you type will be added after the text "Microsoft Internet Explorer Provided by" or "Outlook Express Provided by."
Animated Bitmaps	Used to customize the logo in the upper right corner of Internet Explorer. The logo appears in two states: animated when the browser is in use, and static when no action is taking place.
Custom Logo	Used to customize the Internet Explorer static logo. This bitmap appears when no action is taking place in the browser. To use a custom static logo, you must provide two bitmaps; one should be 22-by-22 pixels and the other 38-by-38 pixels.
Browser Toolbar Buttons	Used to customize the toolbar buttons in the user's browser. You can specify the script or program that the buttons launch, as well as their appearance.
\Connection	
Connection Settings	Used to preset connection settings for users by importing the connection settings from your computer (the administrator's).
Automatic Browser Configuration	Used to assign URLs to files that will automatically configure Internet Explorer. This feature is useful if you want to control the settings of several users from one central location. You can configure options by using .ins files, also known as IEAK profiles. Using .ins files, you can include standard proxy settings. You can also specify script files in .js, .jvs, or .pac format that enable you to configure and maintain advanced proxy settings.
Proxy Settings	Used to specify which proxy servers users can connect to.
User Agent String	Site statistics, such as how many times, and by which types of Web browsers, Web content is accessed, can be tracked with a user agent string, which provides information to the Web server about the users' Web browsers. You can use this policy setting to customize a portion of the user agent string.
\URLs	
Favorites and Links	Used to customize the Favorites folder and Links bar in Internet Explorer by adding links to sites related to your company or services.
Important URLs	Used to specify URLs for the home, search, and online support pages for Internet Explorer.
Channels	Used to add a custom channel or channel category (folder) to Internet Explorer.

Policy settings under User Configuration\Windows Settings\Internet Explorer Maintenance	Description
\Security	
Security Zones and Content Ratings	Used to manage security zones and content ratings for Internet Explorer. You can customize the settings for each security zone. Through content ratings, you can prevent users from viewing content that may be considered offensive.
Authenticode Settings	Authenticode® technology can be used to help manage Internet Explorer security. Authenticode is used to designate software publishers and credentials agencies as trustworthy.
\Programs	
Programs	Used to import the administrator's default program settings, such as which programs are the default for e-mail and for editing HTML files. These settings are located on the Programs tab of the Internet Options dialog box.

Specifying Policy Settings for Internet Explorer

The following table lists the policy settings available for **Internet Explorer** under **Computer Configuration\Administrative Templates\Windows Components**.

Policy setting under Computer Configuration\Administrative Templates\Windows Components\Internet Explorer	Description
Security Zones: Use only machine settings	Applies security zone settings to all users of the same computer. Security zones are groups of Web sites with the same level of security.
Security Zones: Do not allow users to change policies	Prevents users from changing security zone settings.
Security Zones: Do not allow users to add/delete sites	Prevents users from adding or removing sites from security zones. The Disable the Security page policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel) removes the Security tab from the interface, and takes precedence over this policy. If Disable the Security page is enabled, this policy is ignored.
Make proxy settings per-machine (rather than per-user)	Applies proxy settings to all users of the same computer.
Disable Automatic Install of Internet Explorer components	Prevents Internet Explorer from automatically installing components.
Disable Periodic Check for Internet Explorer software updates	Prevents Internet Explorer from determining if a new version of the browser is available.
Disable software update shell notifications on program launch	Specifies that programs using the Microsoft Software Distribution Channel will not notify users when they install new components. The Software Distribution Channel is a means of updating software dynamically on users' computers by using Open Software Distribution (.osd) technologies.
Disable showing the splash screen	Prevents the Internet Explorer splash screen from appearing when users start the browser.



The following table lists the policy settings available for **Internet Explorer** under **User Configuration\Administrative Templates\Windows Components**.

Policy setting under User Configuration\Administrative Templates\Windows Components\Internet Explorer	Description
Search: Disable Search Customization	Makes the Customize button in the Search Assistant page appear dimmed.
Search: Disable Find Files via F3 within the browser	Disables use of the F3 key to search in Internet Explorer and Windows Explorer.
Disable external branding of Internet Explorer	Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by a third party.
Disable importing and exporting of favorites	Prevents users from exporting or importing favorite links by using the Import/Export wizard.
Disable changing Advanced page settings	Prevents users from changing settings on the Advanced tab in the Internet Options dialog box.
Disable changing home page settings	Prevents users from changing the home page of the browser. The home page is the first page that is displayed when users start the browser.
Use Automatic Detection for dial-up connections	Specifies that Automatic Detection will be used to configure dial-up settings for users.
Disable caching of Auto-Proxy scripts	Prevents automatic proxy scripts, which interact with a server to automatically configure users' proxy settings, from being stored in the users' cache.
Display error message on proxy script download failure	Specifies that error messages be displayed if problems occur with the proxy script.
Disable changing Temporary Internet files settings	Prevents users from changing the browser cache settings, such as the location and amount of disk space to use for the Temporary Internet Files folder.
Disable changing history settings	Prevents users from changing the history settings for the browser
Disable changing color settings	Prevents users from changing the default Web page colors.
Disable changing link color settings	Prevents users from changing the colors of links on Web pages.
Disable changing font settings	Prevents users from changing font settings.
Disable changing language settings	Prevents users from changing settings for language.
Disable changing accessibility settings	Prevents users from changing accessibility settings.
Disable Internet Connection wizard	Prevents users from running the Internet Connection wizard.
Disable changing connection settings	Prevents users from changing settings for dial-up connections.
Disable changing proxy settings	Prevents users from changing proxy settings.
Disable changing Automatic Configuration settings	Prevents users from changing settings for automatic configuration, a process that administrators can use to update browser settings periodically.
Disable changing ratings settings	Prevents users from changing ratings, which help control the type of Internet content that can be viewed.
Disable changing certificate settings	Prevents users from changing certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers

Policy setting under User Configuration\Administrative Templates\Windows Components\Internet Explorer	Description
Disable changing Profile Assistant settings	Prevents users from changing settings for the Profile Assistant. (The My Profile button is accessed by clicking Internet Options on the Tools menu, and then clicking the Content tab in the Internet Options dialog box).
Disable AutoComplete for forms	Prevents Internet Explorer from automatically completing forms, such as filling in a name or a password that the user has entered previously on a Web page.
Do not allow AutoComplete to save passwords	Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.
Disable changing Messaging settings	Prevents users from changing the default programs for messaging tasks.
Disable changing Calendar and Contact settings	Prevents users from changing the default programs for managing schedules and contacts
Disable the Reset Web Settings feature	Prevents users from restoring default settings for home and search pages.
Disable changing default browser check	Prevents Internet Explorer from checking to determine if it is the default browser.
Identity Manager: Prevent users from using Identities	Prevents users from configuring unique identities by using Identity Manager , which enables users to create multiple accounts, such as e-mail accounts, on the same computer. Each user has a unique identity, with a different password and different program preferences.
Internet Control Panel	
Disable the General page	Removes the General tab from the interface in the Internet Options dialog box.
Disable the Security page	Removes the Security tab from the interface in the Internet Options dialog box.
Disable the Content page	Removes the Content tab from the interface in the Internet Options dialog box.
Disable the Connections page	Removes the Connections tab from the interface in the Internet Options dialog box.
Disable the Programs page	Removes the Programs tab from the interface in the Internet Options dialog box.
Disable the Advanced page	Removes the Advanced tab from the interface in the Internet Options dialog box.
Offline Pages	
Disable adding channels	Prevents users from adding channels to Internet Explorer.
Disable removing channels	Prevents users from disabling channel synchronization in Internet Explorer.
Disable adding schedules for offline pages	Prevents users from specifying that Web pages can be downloaded for viewing offline. Making Web pages available for offline viewing allows users to view the Web pages' content when their computer is not connected to the Internet.
Disable editing schedules for offline pages	Prevents users from editing an existing schedule for downloading Web pages for offline viewing.
Disable removing schedules for offline pages	Prevents users from clearing the pre-configured settings for Web pages to be downloaded for offline viewing.
Disable offline page hit logging	Prevents channel providers from recording information about when their channel pages are viewed by users who are working offline.
Disable all scheduled offline pages	Disables existing schedules for downloading Web pages for offline viewing.

Policy setting under User Configuration\Administrative Templates\Windows Components\Internet Explorer	Description
\Offline Pages	
Disable channel user interface completely	Prevents users from viewing the Channel bar interface. Channels are Web sites that are automatically updated on the users' computers according to a schedule specified by the channel provider.
Disable downloading of site subscription content	Prevents content from being downloaded from Web sites to which users have subscribed.
Disable editing and creating of schedule groups	Prevents users from adding, editing, or removing schedules for offline viewing of Web pages and groups of Web pages to which users have subscribed.
Subscription Limits	Restricts the amount of information downloaded for offline viewing. You can set limits for the size and number of pages that users can download.
\Browser menus	
File menu: Disable Save As...menu option	Prevents users from saving Web pages from the browser File menu to their hard disk or to a network share.
File menu: Disable New menu option	Prevents users from opening a new browser window from the File menu.
File menu: Disable Open menu option	Prevents users from opening a file or Web page from the File menu in Internet Explorer.
File menu: Disable Save As Web Page Complete	Prevents users from saving the entire contents that are displayed on or run from a Web page, including the graphics, scripts, linked files, and other elements. It does not prevent users from saving the text of a Web page.
File menu: Disable closing the browser and Explorer windows	Prevents users from closing Internet Explorer and Windows Explorer.
View menu: Disable Source menu option	Prevents users from viewing the HTML source of Web pages by clicking the Source command on the View menu.
View menu: Disable Full Screen menu option	Prevents users from displaying the browser in full-screen (kiosk) mode, without the standard toolbar.
Hide Favorites menu	Prevents users from adding, removing, or editing the list of Favorite links.
Tools menu: Disable Internet Options...menu option	Prevents users from opening the Internet Options dialog box from the Tools menu in Internet Explorer.
Help menu: Remove 'Tip of the Day' menu option	Prevents users from viewing or changing the Tip of the Day interface in Internet Explorer.
Help menu: Remove 'For Netscape Users' menu option	Prevents users from displaying tips for users who are switching from Netscape.
Help menu: Remove 'Tour' menu option	Prevents users from running the Internet Explorer Tour option from the Help menu in Internet Explorer.
Help menu: Remove 'Send Feedback' menu option	Prevents users from sending feedback to Microsoft by clicking the Send Feedback command on the Help menu.
Disable Context menu	Prevents the shortcut menu from appearing when users click the right mouse button while using the browser.

Policy setting under	Description
User Configuration\Administrative Templates\Windows Components\Internet Explorer	
\Browser	
Disable Open in New Window menu option	Prevents users from using the shortcut menu to open a link in a new browser window; users cannot point to a link, right-click, and select the Open in New Window command.
Disable Save this program to disk option	Prevents users from saving a program or file that Internet Explorer has downloaded to the hard disk.
\Toolbars	
Disable customizing browser toolbar buttons	Prevents users from specifying which buttons appear on the Internet Explorer and Windows Explorer standard toolbars.
Disable customizing browser toolbars	Prevents users from specifying which toolbars are displayed in Internet Explorer and Windows Explorer.
Configure Toolbar Buttons	Used to specify which buttons are displayed on the standard toolbar in Internet Explorer.
\Persistence Behavior	
File size limits for Local Machine zone	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Computer security zone.
File size limits for Intranet zone	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Local Intranet security zone.
File size limits for Trusted Sites zone	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Trusted Sites security zone.
File size limits for Internet zone	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Internet security zone.
File size limits for Restricted Sites zone	Limits the amount of storage that a page or site using the DHTML Persistence behavior can use for the Restricted Sites security zone.
\Administrator Approved Controls	
Media Player	Designates the Media Player ActiveX control as administrator approved. Media Player is used to play sounds, videos, and other media.
Menu Controls	Designates a set of Microsoft ActiveX controls used to manipulate pop-up menus in the browser as administrator approved.
Microsoft Agent	Designates the Microsoft Agent ActiveX control as administrator approved. Microsoft Agent is a set of software services that supports the presentation of software agents as interactive personalities within the Microsoft Windows interface.
Microsoft Chat	Designates the Microsoft Chat ActiveX control as administrator approved. Web authors use this control to build text- and graphical-based Chat communities for real-time conversations on the Web.
Microsoft Survey Control	
Shockwave Flash	
NetShow File Transfer Control	

Policy setting under User Configuration\Administrative Templates\Windows Components\Internet Explorer	Description
Administrator Approved Controls	
DHTML Edit Control	
Microsoft Scriptlet Component	
Carpoin	Designates the Microsoft Network (MSN) Carpoint automatic pricing control as administrator approved. This control enables pricing functionality on the Carpoint Web site, where users can shop for and obtain information about vehicles.
Investor	Designates a set of Microsoft Network (MSN) Investor controls as administrator approved. These controls allow users to view updated lists of stocks on their Web pages.
MSNBC	Designates a set of MSNBC controls as administrator approved. These controls enable enhanced browsing of news reports on the MSNBC Web site.

Appendix C: Group Policy Storage

Group Policy Objects store information in two locations: a Group Policy Container and a Group Policy Template.

Group Policy Container

The Group Policy Container (GPC) is an Active Directory container that stores Group Policy Object properties; it includes sub-containers for computer and user Group Policy information. The Group Policy Container has the following properties:

- **Version information.** This is used to ensure that the information is synchronized with the Group Policy Template information. Indicates the number of changes made to the GPO.
- **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.
- **File System path.** The UNC path to the Sysvol folder.
- **Functionality version.** This is the version of the tool that created the GPO. Currently, this is version 1.

For example, the Group Policy Container stores information used by the Software Installation snap-in to describe the state 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 (GPT) that is located in the System Volume folder of domain controllers (Sysvol) in the \Policies sub-folder. The Group Policy Template is the container where Security Settings, Administrative Template-based policies, applications available for Software Installation, and script files are stored.

When you modify a GPO, the directory name given to the Group Policy Template is the GUID of the Group Policy Object that you modified. For example, assume that you modified a GPO associated with a domain called Seattle. The resulting GPT folder would be named as follows (the GUID is an example):

```
%systemroot%\sysvol\
```

where the second *sysvol* is shared as SYSVOL. (The default location of the Sysvol folder is %systemroot%).

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 the following:

- 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.

For the local GPO, the Gpt.ini file contains the following information:

```
[General]
GPCUserExtensionNames //Includes a list of GUIDs that tells the client
                        side engine which Client Side Extensions have User
                        data in the GPO.
                        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 //Includes a list of GUIDs that tells the
                           client side engine which Client Side Extensions
                           have Machine data in the GPO.

Options..//Refers to GPO options such as User portion disabled or Machine
          portion disabled.

GPCFunctionalityVersion //The Version number of the Group Policy
                        extension tool that created the Group Policy
                        object.
```

Gpt.ini for Active Directory GPOs

The Gpt.ini file for Active Directory GPOs contains the following entries, which are stored in the Active Directory:

```
Version=0 //Version number of the Group Policy Object
DisplayName //Display name of the GPO
```

Local Group Policy Objects

A local Group Policy Object exists on every computer, and by default it contains only security policy (that is, other types of policy settings are not configured by default). The local GPO is stored in %systemroot%\System32\GroupPolicy, and it has the following ACL permissions:

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

Group Policy Template Subfolders

The Group Policy Template folder contains the following subfolders:

- **User.** Includes a Registry.pol file that contains the registry settings to be 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 **User** folder may contain the following subfolders (depending on the GPO contents):

- **Applications.** Contains the advertisement files (.aas files) used by the Windows installer. These are applied to users.
- **User Documents and Settings.** Contains the Fdeploy.ini file, which includes status information about the Folder Redirection options for the current user's special folders.
- **Microsoft\RemoteInstall.** Contains the OSCfilter.ini file, which holds user options for operating system installation through Remote Installation Services.
- **Microsoft\IEAK.** Contains settings for the Internet Explorer Maintenance Snap-in.
- **Scripts\Logon.** Contains all the user logon scripts and related files for this Group Policy object.
- **Scripts\Logoff.** Contains all the user logoff scripts and related files for this Group Policy object.
- **Machine.** Includes a Registry.pol file that contains the registry settings to be applied to computers. When a computer initializes, this Registry.pol file is downloaded and applied to the **HKEY_LOCAL_MACHINE** portion of the registry.

The **Machine** folder may contain the following subfolders (depending on the GPO):

- **Scripts\Startup.** Contains the scripts that are to run when the computer starts up.
- **Scripts\Shutdown.** Contains the scripts that are to run when the computer shuts down.
- **Applications.** Contains the advertisement files (.aas files) used by the Windows installer. These are applied to computers.
- **Microsoft\Windows NT\Secedit.** Contains the Gpttmpl.inf file, which includes the default security configuration settings for a Windows 2000 domain controller.
- **Adm.** Contains all of the .adm files for this Group Policy object.

The User and Machine folders are created at install time, and the other folders are created as needed when policy is set.

Registry.pol Files

The Administrative Templates snap-in extension of Group Policy saves information in the Group Policy Template in binary files referred to as Registry.pol files; they are stored in the Group Policy Template. These files contain the customized registry settings that you specify (by using the Group Policy snap-in) to be applied to the Machine (**HKLM**) or User (**HKLU**) portion of the registry.

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 Registry.pol files in the Group Policy Template differs from that of previous versions of Windows NT and Windows 95 operating systems. NTconfig.pol or Config.pol files created by Windows NT 4.0 and Windows 95 can be applied only to the operating system on which they were created.

When you use the Administrative Templates extension of the Group Policy snap-in to define customized registry settings to be applied to the Machine (HKLM) or User (HKLU) portion of the registry, two Registry.pol files are created and stored in the Group Policy Template. One Registry.pol file is for Computer Configuration-related registry settings and is stored in the **\Machine** sub-directory, and the other is for User Configuration settings and is stored in the **\User** sub-directory.

The Windows 2000 Registry.pol file consists of a header and registry values.

The header contains version information and signature data, both **DWORD** values:

```
REGFILE_SIGNATURE 0x67655250
REGISTRY_FILE_VERSION 00000001 (increments each time the file format
changes)
```

The registry values begin with an opening bracket ([]) and end with a closing bracket (]):

```
[key;value;type;size;data]
```

where:

Key is the path to the registry key to use for the category. Do not include **HKEY_LOCAL_MACHINE** or **HKEY_CURRENT_USER** in the registry path. The location of the file determines which of these keys is used.

The following value has special meaning for this field:

- ****DeleteKeys**—a semi-colon-delimited list of values to delete.
For example: ****DeleteKeys NoRun;NoFind**.

Value is the name of the registry value. The following values have special meaning for this field:

- ****DeleteValues**—a semi-colon-delimited list of values to delete. Use as a value of the associated key.
- ****Del.valuename**—deletes a single value. Use as a value of the associated key.
- ****DelVals**—deletes all values in a key. Use as a value of the associated key.

Type is a data type. The field can be any of the standard registry value types, for example:

- **REG_DWORD**
- **REG_EXPAND_SZ**
- **REG_SZ**

Note that although the file format supports all the registry data types (such as **REG_MULTI_SZ**), the Administrative Templates node does not support these registry types: **REG_BINARY**, **REG_MULTI_SZ**.

Size is the size of the data field in bytes. For example, 4.

Data is the raw information. For example, 4 bytes of data 0x00000001.

It is possible that the *valuename*, *type*, *data*, and *size* could be missing or 0. In this case, only the key should be created.

This pattern of [] entries continues until the end of the file.

The following special values are used for deleting keys and values:

- ****DeleteKeys //** Semi-colon-delimited list of keys to delete.
For example: ****DeleteKeys REG_SZ NoRun;NoFind**.
- ****DeleteValues //** Semi-colon-delimited list of values to delete.
Used as a value of the designated key.
- ****Del.valuename //** Deletes a single value name.
Used as a value of the designated key.
- ****DelVals //** Deletes all values in a key.
Used as a value of the designated key.

The Registry.pol file contains data to be written to the registry based on the settings specified with the Group Policy snap-in, and the names of any scripts and their

command lines (in the form of registry keys and values).

How Registry.pol Files Are Created

The following section outlines how to form Registry.pol files:

- When you start the Group Policy snap-in, a temporary registry tree is created that consists of two nodes: USER and MACHINE.
- As you navigate the Administrative Templates node of the Group Policy snap-in, .adm file nodes are displayed. The .adm files within the Group Policy snap-in nodes are loaded dynamically when a particular node is selected, and the .adm file is then cached.
- When a policy is selected in the details pane (the right side of the MMC console window), the temporary registry is queried to determine whether the selected policy already has registry values assigned to it; if it does, those values are displayed in the **Policy** dialog box.
If the selected policy does not have a registry value assigned to it, the default value from the .adm file or from the associated MMC snap-in extension is used.
- After you modify a policy, the registry values that you specify are written to the appropriate portion of the temporary registry (either **MACHINE** or **USER**).
- When you close the Group Policy snap-in, the temporary registry hives are exported to the Registry.pol files in the appropriate folders of the Group Policy Template.
- The next time you start the Group Policy snap-in for the same Group Policy Object for which you have previously set Group Policy settings, the registry information from the corresponding Registry.pol files is imported into the temporary registry tree. Therefore, when you view the policies, they reflect the current state.

Appendix D: Windows NT 4.0, Zero Administration Kit, and Windows 2000 Namespace Comparison

The following tables list comparisons of the Windows NT 4.0, the Zero Administration Kit (ZAK), and the Windows 2000 policy-related namespace.

The following notation is used in the tables:

P = Policy

SYS = not in Administrative Templates (system configured)

N/A = not available

Policy Option – Windows NT4.0 and ZAK namespace	Windows 2000 namespace		Notes
Default User			
Control Panel\Display\Restrict Display\	User Configuration\Administrative Templates\Control Panel\Display		
Deny access to display icon	Prohibit user from running Display control panel	P	
Hide Background Tab	Same	P	
Hide Screen Saver Tab	Same	P	
Hide Appearance Tab	Same	P	
Hide Settings Tab	Same	P	
Desktop\Wallpaper			
Wallpaper Name	N/A		
Tile Wallpaper	N/A		
Desktop\Color Scheme			
Scheme name	N/A		
Shell\Restrictions			
Remove Run command from Start menu	User Configuration\Administrative Templates\Start Menu & Task Bar	P	
Remove folders from Settings on Start menu	User Configuration\Administrative Templates\Start Menu & Task Bar	P	
Remove Taskbar from Settings on Start menu	User Configuration\Administrative Templates\Start Menu & Task Bar	P	Disable changes to Task Bar and Start menu settings.
Remove Find command from Start menu	User Configuration\Administrative Templates\Start Menu & Task Bar	P	Remove Search menu from Start menu.
Hide drives in My Computer	User Configuration\Administrative Templates\Windows Components\Explorer	P	Hide these specified drives in My Computer.
Hide Network Neighborhood	User Configuration\Administrative Templates\Desktop	P	My Network Places.
No Entire Network in Network Neighborhood	User Configuration\Administrative Templates\Windows Components\Explorer	P	My Network Places.
No Workgroup contents in Network	User Configuration\Administrative	P	My Network Places.

Policy Option – Windows NT4.0 and ZAK namespace	Windows 2000 namespace		Notes
Neighborhood	Templates\Windows Components\Explorer		
Hide all items on Desktop	User Configuration\Administrative Templates\Desktop	P	
Disable Shut Down command	User Configuration\Administrative Templates\Start Menu & Task Bar User Configuration\Administrative Templates\System\Logon/Logoff	P	Disable shutdown. Remove shutdown.
Don't save settings at exit	User Configuration\Administrative Templates\Desktop	P	
System\Restrictions	User Configuration\Administrative Templates\System		
Disable Registry editing tools	Same	P	
Run only allowed Windows applications	Same	P	
Windows NT Shell\Custom User Interface			
Custom Shell	N/A		Shell name.
Windows NT Shell\Custom Folders			
Custom Programs Folder	N/A		
Custom Desktop Icons	User Configuration\Windows Settings\Folder Redirection\Desktop	SYS	
Hide Start menu subfolders	N/A		
Custom Startup Folder	N/A		
Custom Network Neighborhood	N/A		Called "My Network Places folder" in Windows 2000.
Custom Start menu	User Configuration\Windows Settings\Folder Redirection\Start Menu	SYS	
Windows NT Shell Restrictions			
Only use approved Shell extensions	User Configuration\Administrative Templates\Windows Components\Windows Explorer	P	
Remove File menu from Explorer	User Configuration\Administrative Templates\Windows Components\Windows Explorer	P	Disable File menu in Shell folders.
Remove common program groups from Start menu	User Configuration\Administrative Templates\Start Menu & Task Bar	P	Hide versus Remove.
Disable Context Menus for the Taskbar	User Configuration\Administrative Templates\Start Menu & Task Bar	P	

Disable Explorer's default context menu	User Configuration\Administrative Templates\Windows Components\Explorer	P	Disable context menu in Shell folders.
Remove the Map Network Drive and Disconnect Network Drive options	User Configuration\Administrative Templates\Windows Components\Explorer	P	Disable net connections/disconnections.
Disable link file tracking	N/A User Configuration\Administrative Templates\Windows Components\Explorer	P	Do not involve the domain controller with distributed link tracking. Do not rack shell shortcuts during roaming.
Windows NT System	User Configuration\Administrative Templates\System\Logon/Logoff		
Parse Autoexec.bat	N/A		
Run logon scripts synchronously	Computer Configuration\Administrative Templates\System\Logon	P	Many others added for Windows 2000
Disable Task Manager	Same	P	
Show welcome tips at logon	N/A		
ZAK Policies\Windows NT\			
User Profiles through System Policies			
AppData Folder	User Configuration\Windows Settings\Folder Redirection.	SYS	Custom Application Folder.
Favorites Folder	N/A		.
NetHood Folder	User Configuration\Windows Settings\Folder Redirection\		
PrintHood Folder	N/A		
Recent Folder	N/A		
SendTo Folder	N/A		
Internet Explorer Security\Active Content	Many new Internet Explorer Policies in User Configuration\Administrative Templates\Windows Components\Internet Explorer		
Allow download of ActiveX content	N/A		
Enable ActiveX Controls and Plug-ins	N/A		
Run ActiveX scripts	N/A		
Enable Java Programs	N/A		
Internet Explorer Security\Active Content Security Level			

Select Security Level	N/A		
Drives\Restrictions\Show only selected drives			
Choose drives that will be shown	User Configuration\Administrative Templates\Windows Components\Windows Explorer	P	Hide these specified drives in My Computer.
ZAK Policies\Windows\Load			
Enter Program to be Run on Startup	N/A		

Default Computer			
Network\System policies update\Remote update			
Update mode	N/A		
Path for manual update	N/A		
Display error messages	N/A		
Load balancing	N/A		
System\SNMP			
Communities	N/A		
Permitted managers	N/A		
Traps for Public community	N/A		
System\RUN			
Items to run at startup	N/A		
Windows NT Network\Sharing			
Create hidden drive shares (workstation)	N/A		
Create hidden drive shares (server)	N/A		
Windows NT Printers			
Disable browse thread on this computer	N/A		
Scheduler priority	N/A		
Beep for error enabled	N/A		
Windows NT Remote Access			
Max number of unsuccessful authentication retries	N/A		
Max time limit for authentication	N/A		

Wait interval for callback	N/A		
Auto Disconnect	N/A		
Windows NT Shell\Custom shared folders			
Custom shared Programs folder	N/A		
Custom shared desktop icons	N/A		
Custom shared Start menu	N/A		
Custom shared Startup folder	N/A		
Windows NT System\Logon			
Logon banner—Caption, Text	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	SYS	Message text for users attempting to log on. Message title for users attempting to log on.
Enable shutdown from Authentication dialog box	User Configuration\Administrative Templates\Start Menu & Task Bar	P	Disable/Remove the Shutdown Command.
Do not display last logged on user name	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	SYS	Do not display last user name in logon screen.
Run logon scripts synchronously	Computer Configuration\Administrative Templates\System\Logon\	P	
Windows NT System\File System			
Do not create 8.3 file names for long file names	N/A		
Allow extended characters in 8.3 file names	N/A		
Do not update last access time	N/A		
Windows NT User Profiles			
Computer Configuration\Administrative Templates\Logon\			
Delete cached copies of roaming profiles	Same	P	
Automatically detect slow network connections	Automatically detect slow network connections for user profiles.	P	
Slow network connection time-out	Same	P	
Time-out for dialog boxes	Same	P	

Appendix E: Frequently Asked questions

This section presents frequently asked questions on Group Policy.

Infrastructure - Server side

Is it possible to set up individual computer or user policies?

You cannot set up any Group Policy directly on a computer or user object; a Group Policy object can *only* be associated with sites, domains, and organizational units. To apply a GPO to a subset of users or computers (or even a single user or computer) within a site, domain, or OU, you can use security filtering.

For information filtering Group Policy, see the section in this document on [Using Security Groups to Filter the Scope of the Group Policy Object](#).

What are the inheritance rules for Group Policy and the Active Directory?

Group Policy is processed in the following order: Local Group Policy object, site, domain, OU, and additional child OUs. This means that the local Group Policy object is processed first, and the OU to which the computer or user belongs (the one that it is a direct member of) is processed last. All of this is subject to the following exceptions:

- Any domain-based Group Policy object (not local GPO) may be enforced by using the **No Override** option so that its policies cannot be overwritten. When more than one GPO has been marked as enforced, the GPO that is highest in the Active Directory hierarchy takes precedence.
- At any site, domain, or OU, Group Policy inheritance may be selectively designated as **Block Inheritance**. However, blocking inheritance does not prevent policy from **No Override** GPOs from applying; this is because enforced GPOs are always applied, and cannot be blocked.

If you apply policies to an OU that contains only groups (of any kind) and no users, are the policies applied to the members of the group?

No, Group Policy Objects (GPOs) are applied only to the users and computers that are members of the organizational unit. A different mechanism is used to filter the effect of GPOs, based on membership in security groups. The preceding question addresses this issue.

Can you apply a GPO directly to a security group?

No, GPOs are applied only to the users and computers that are members of a site, domain, or organizational unit (SDOU). However, you can filter the scope of a GPO based on membership of those users in a security group, by adjusting the discretionary access control list (DACL) permissions for that group on the GPO. This design was chosen for performance reasons.

You can also filter the scope of a GPO on a site, domain, or OU by using the

Security tab on the **GPO Properties** page to set DACL permissions and selecting an access control entry called **Apply Group Policy**.

For more information, see [Using Security Groups to Filter the Scope of the Group Policy Object](#) at the beginning of this document.

Why can't I delete the default GPO (Default Domain Policy), no matter which administrative group I belong to?

By default, the Delete Access Control entry has not been allowed to the Administrators groups. Administrators do have all other rights. The reason for this is to prevent the accidental deletion of this GPO, which contains important and required settings for the domain. If it is truly required that the GPO be deleted because the settings have been set in other GPOs, the Delete access control entry must be given back to the appropriate group.

Why do I sometimes get the prompt "The Domain Controller for Group Policy operations is not available. You may cancel this operation for this session or retry using one of the Following domain controller choices."?

The Group Policy snap-in uses the primary domain controller emulator Operations Master token when editing a GPO. For information, see [Specifying a Domain Controller for Setting Group Policy](#), and [Group Policy Snap-in and the Operations Master](#) earlier in this paper.

What is the best method of copying or replicating policies between domains?

While no part of a GPO is replicated outside of a domain, it is possible to establish a link to a GPO in a domain other than your own. Use the **Add** button on the target site, domain, or OU **Group Policy Properties** page. Use the **Look in** list box to navigate to the domain in which the GPO exists; then browse to it, and select it. There are performance implications associated with linking GPOs across domains. All computers and users affected by the cross-domain linked GPO must access the other domain and pull the GPO information from it. It is, therefore, important to consider WAN issues before you establish such a link.

For a limited way to copy policies, see the section called Saving and Moving the Scenario GPOs to Another Domain in the "[Using Group Policy Scenarios](#)" white paper, which is found at <http://www.microsoft.com/windows2000/library/howitworks/management/grouppolicy.asp>.

The ability to have enterprise-wide GPOs and the ability to copy GPOs will be considered for the next release of Windows 2000 Server.

How can I get more information regarding the processing of Group Policy into the Event log of a client computer?

You can set the following registry key for this by using the Registry Editor tool (regedit.exe):

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics  
RunDiagnosticLoggingGroupPolicy REG_DWORD 1
```

Setting this key causes additional information to be logged to the event log when Group Policy is running.

In what order are policies processed during computer startup and user logon?

The policy processing sequence is the following:

- The network starts—Remote Procedure Call System Service (RPCSS) and Multiple UNC (Universal Naming Convention) Provider (MUP) must be started.
- Apply computer Group Policy—this is done synchronously by default.
- Run startup scripts—these are run hidden and synchronously by default. This means that each script must complete or time out before the next one starts.
- CTRL+ALT+DEL is pressed.
- After the user is validated, the profile is loaded.
- Apply user Group Policy—this is done synchronously by default. Group Policy is processed in the following order: Windows NT 4.0, local, site domain, OU, and so on. UI is displayed while policies are being processed.

Note: Windows NT 4.0 style policies process both computer and user settings, potentially overwriting the Active Directory-based Group Policy settings that were applied at computer startup.

- Run logon scripts—Group Policy-based logon scripts are run hidden (unlike in Windows NT 4.0) and asynchronously by default. The user object script, which is run in a normal window (like Windows NT 4.0), is run last.
- Start the shell.

Notes: Policy settings exist for reversing the synchronous or asynchronous defaults for running scripts and applying policy. For more details on policy options for scripts see the Scripts section of this paper.

By default, scripts time out after 600 seconds. A policy setting exists that lets you change this

default.

Policy settings also exist for specifying whether scripts are run hidden, minimized, or in a normal window.

You can specify a Group Policy to disable Windows NT 4.0-style policies.

How often is Group Policy applied, and how do I change it?

For users and all computers (except domain controllers), policy is applied by default every 90 minutes with a variable offset of 30 minutes. For domain controllers, the default is every 5 minutes. You can change these defaults by setting a Group Policy within the Administrative Templates node of the Group Policy snap-in.

The application of Group Policy cannot be scheduled or pushed to clients. Exceptions to this include the Software Installation and Folder Redirection snap-ins. The Scripts extension runs during the background refresh, but the scripts are actually run by Winlogon at the appropriate time.

How long does it take to process Group Policies?

This depends on the number of GPOs being processed for a specified computer or user and on the number of policies set with each GPO.

A great deal of work on performance issues pertaining to Group Policy was done for the release of the product. This performance information has been published in an Microsoft Press book called "[Building Enterprise Active Directory™ Services: Notes from the Field.](#)" *Chapter Five: Active Directory Client Network Traffic* includes information pertaining to logon scripts, policy files, and the effects of Group Policy on logon traffic.

Which policies do I see when viewing the policies that are set when the Group Policy snap-in is run focused on a local computer?

This shows the information in the local Group Policy object, but not the cumulative effect of what has been applied to the computer or user. This feature will be investigated for the next release of the product. For Windows 2000, it shows the settings that a local administrator has set for that computer and all users of that computer. In the evaluation process, when the computer is joined to a domain, all the policy settings are subject to being overwritten by domain-based policy (any policy set in the site, domain, or OU).

Group Policy Snap-in

What happened to the policies such as Logon Banner or Disable CTRL+ALT+DEL that were available in Windows NT 4.0?

These and other policies that are security-related have been moved to the Security Settings node, under Local Policies\Security Options. This includes the following policies:

- Disable CTRL+ALT+DEL.
- Do not display last user name in logon screen.
- Message text, caption, title for users logging on (legal notice).
- Allow system to be shutdown without having to log on.

For more information, see [Appendix D: Windows NT 4.0, Zero Administration Kit, and Windows 2000 Namespace Comparison](#).

General Issues

Can I transfer System Policies to Group Policy Objects?

You cannot migrate Windows NT 4.0 System Policies *directly* to Windows 2000. In Windows NT 4.0, System Policies were stored in one .pol file with group information embedded. One way to extract policy settings from Windows NT 4.0 .pol files is by using the Gpolmig.exe tool included in the [Windows 2000 Server Resource Kit Tools](#). Gpolmig.exe is used to migrate settings from Windows NT policy files to the Windows 2000 Group Policy object structure.

Windows NT 4.0 clients on Windows 2000 Server and Windows 2000 Professional computers on Windows NT 4.0 server will continue to work as they did before, using the Netlogon share.

With Windows 2000 Server, when a Windows NT 4.0 client is upgraded to Windows 2000, it will get only Active Directory-based Group Policies and not Windows NT 4.0-style policies.

What is the plan for providing users with the ability to determine the resultant set of policies for a computer and user?

In the next release, we will provide an isolation layer that exposes all resultant Group Policy data by using a standard schema. The Windows Management Instrumentation (WMI)⁶ technology and schema will be used to implement this interface to the Group Policy Resultant Set of Policy (RSoP) data.

Using this approach provides a consistent data interface for developers to use when creating RSoP tools.

In addition, Microsoft will build a basic administrator's RSoP tool that uses the WMI-based infrastructure and provides the following capabilities:

- Generates the actual RSoP for a given target, for example, a particular computer or user. This addresses the question of which policies were applied.
- Views the potential state. This answers the question of which policies would be applied for a user, a computer, and a user on a specific computer, given a particular target.
- Indicates the source GPOs for each of the resultant policies.

Do Group Policies override User Profile settings?

Yes.

Where is the System Policy Editor (Poedit.exe) located, and why would I need to use it?

The Windows NT 4.0 System Policy Editor, Poedit.exe, is located in the %systemroot% directory. The Windows NT 4.0-style .adm files are located in the %systemroot%\inf directory (the same location as in Windows NT 4.0). The System Policy Editor user interface is not exposed in Windows 2000 server. Administrators still have to use Poedit.exe to create registry-based policies for all clients running Windows NT 4.0, Windows 95, and Windows 98.

To create a properly formatted .pol file for Windows 95 or Windows 98, Poedit.exe must be run on a Windows 95 or Windows 98 client. For more details about this process and Windows NT 4.0 System Policy, see the white paper called "[Implementing Profiles and Policies for Windows NT 4.0](http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp)," available at http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp.

⁶ The Windows Management Instrumentation is an implementation of the Desktop Management Task Force's (DMTF) Web-based Enterprise Management (WBEM) initiative, which provides standards for accessing and sharing management information in an enterprise environment.

For Windows NT 4.0 and Windows 2000, Poedit.exe may be run on either system. The resultant .pol file must then be copied to the domain controller's Netlogon share.

Is there a programmatic way to add, edit, or delete GPOs?

No process is available to *script* Group Policy Objects. However, you can programmatically add, edit, or delete GPOs by using the **IGroupPolicyObject** interface defined in the Gpedit.h file. For details on the Group Policy APIs, see the Microsoft Platform SDK at <http://msdn.microsoft.com/developer/sdk/platform.htm>.

Some of these functions can be performed with the Windows 2000 Server Resource Kit command line tool called GPOTool.exe. You can use GPOTool.exe to do the following:

- Perform Group Policy object checks for consistency, including reading directory services properties (version, friendly name, extension, SYSVOL data (Gpt.ini), and GUIDs), comparing directory services and SYSVOL version numbers, and performing other consistency checks.
- Check Group Policy object replication. The tool reads the Group Policy object instances from each domain controller and compares them (selected GPC properties and full recursive compare for GPT).
- View Group Policy object information, including such properties as functionality version and extension GUIDs.
- Browse Group Policy objects based on friendly name or GUID. A partial match is also supported for both name and GUID.
- Set options for preferred domain controllers. By default, all available domain controllers in the domain are used; this can be overwritten with the supplied list of domain controllers from the command line.
- Viewing policies in different domains by using a command-line option.
- Run in verbose mode. A command-line option can turn on verbose information about the policies being processed.

For more information about the GPOTool.exe and other Windows 2000 Resource Kit software tools, see <http://www.microsoft.com/windows2000/library/resources/reskit/tools/default.asp>.

Glossary

This section presents terminology used in this document.

Active Directory

The Windows 2000 directory service that stores information about all objects on the computer network and makes this information easy for administrators and users to find and apply. With the Active Directory, users can gain access to resources anywhere on the network with a single logon. Similarly, administrators have a single point of administration for all objects on the network, which can be viewed in a hierarchical structure.

administrative templates (.adm files)

Template files that provide settings pertaining to Windows 2000, Windows NT version 4.0, and Windows 95 and Windows 98 operating system and registry structure. The .adm file specifies the registry settings that can be modified through the Group Policy snap-in user interface. The .adm file consists of a hierarchy of categories and subcategories that together define how the options are displayed through the Group Policy snap-in user interface. It also indicates the registry locations where changes should be made 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.

Administrative Templates snap-in extension

A Group Policy snap-in extension that includes all registry-based Group Policy, which you use to define settings that control the behavior and appearance of the desktop, including the operating system and applications.

The Administrative Templates snap-in extension includes functionality for managing disk quotas.

application assignment

In Windows 2000, you can use the Software Installation snap-in extension of the Group Policy snap-in to *assign* applications to users so that the applications appear to be installed and available on the user's desktop whenever a user logs on.

You assign applications to a particular Group Policy Object (GPO), which is, in turn, associated with a selected directory container (site, domain, or organizational unit). When you assign applications, the application is *advertised* to every user managed by the GPO. This installs only enough information about the application to make application shortcuts appear on the Start menu and the necessary file associations appear in the registry. When users managed by the GPO log on to a computer running Windows 2000, the application appears on their Start menu. When users select the application from the Start menu for the first time, the application is installed. Advertised applications can also be installed by clicking on a document managed by the application (either by file extension or by COM-based activation).

application publishing

In Windows 2000, you can use the Software Installation snap-in extension of the Group Policy snap-in to *publish* applications to users. Published applications are those that the administrator makes available for on-demand use.

Published applications have no presence on the users' computers. That is, no shortcuts or Start menu references to the application are present on the desktop. A published application is advertised to the Active Directory. The advertised attributes are used to locate the application and all the information required for installing it. After the application is advertised in the Active Directory, users can activate it by document association, just as an assigned application. Users can also set up the program using the Add/Remove Programs Control Panel tool on their desktop.

.cab file

A .cab file contains one or more files, all of which are downloaded together in a single compressed cabinet file. Included in the cabinet is an .inf file that provides further installation information. The .inf file may refer to files in the .cab and to files at other uniform resource locators (URLs).

discretionary access control list (DACL)

A part of the security descriptor that specifies the groups or users that can access an object, as well as the types of access (permissions) granted to those groups or users. *See also* security descriptor.

disk quotas

Within the Administrative Templates node of the Group Policy snap-in are policy options for managing disk quotas, which administrators can use to monitor and limit disk space use for NTFS volumes formatted as NTFS version 5.0. After you enable disk quotas, you can set options for disk quota limits and warnings.

domain

A grouping of servers and other network objects under a single name. Domains provide the following benefits:

- You can group objects into domains to help reflect your company's organization in your computer network.
- Each domain stores only the information about the objects located in that domain. By partitioning the directory information this way, the Active Directory scales up to as many objects as you need to store information about on your network.
- Each domain is a security boundary—this means that security policies and settings (such as administrative rights, security policies, and ACLs) do not cross from one domain to another. The administrator of a domain has absolute rights to set policies within that domain only.

domain trees

You can combine multiple domains into structures called domain trees. The first domain in a tree is called the root of the tree, and additional domains in the same tree are called child domains. A domain immediately above another domain in the same tree is referred to as the parent of the child domain. All domains within a single domain tree share a hierarchical naming structure. Domains that share a common root share a contiguous namespace. Domains in a tree are joined together through two-way, transitive trust relationships. These trust relationships are two-way and transitive, therefore, a domain joining a tree immediately has trust relationships established with every domain in the tree.

Folder Redirection snap-in extension

A Group Policy snap-in extension that you use to place the Windows 2000 special folders in network locations other than their default location (%systemroot%/Documents and Settings) on the local computer.

globally unique identifier (GUID)

A 128-bit integer that identifies a particular object class and interface. GUIDs are virtually guaranteed to be unique. A GUID can be generated using either the uuidgen.exe utility from the Platform Software Development Kit, or the guidgen tool included in the Microsoft Visual C++® development system. For more information about GUIDs, see the OLE Programmer's Reference, Volume One; the Platform Software Development Kit documentation; and Inside OLE, 2d ed. by Kraig Brockschmidt, Redmond, Wash.: Microsoft Press, 1995.

Group Policy

A component used in Windows 2000 to define options for managed desktop configurations for groups of users and computers. To specify Group Policy options, you use the Group Policy MMC snap-in.

Group Policy engine

The part of Group Policy that runs in the Winlogon process.

Group Policy Object

The Group Policy settings that you create by using the Group Policy snap-in are contained in a Group Policy object (GPO), which is in turn associated with selected Active Directory containers: sites, domains, and organizational units (OUs).

Group Policy MMC snap-in

To create a specific desktop configuration for a particular group of users and computers, you use the Group Policy MMC snap-in.

You can specify Group Policy settings for the following:

- Registry-based policies—Includes Group Policy for the Windows 2000 operating system and its components and for applications. To manage these settings, use the Administrative Templates node of the Group Policy snap-in.

-
- Security settings—Includes options for local computer, domain, and network security settings.
 - Software Installation and Maintenance options—Used to centrally manage application installation, updates, and removal.
 - Script options—Includes scripts for computer startup and shutdown and user logon and logoff.
 - Folder Redirection options—Allows administrators to redirect users' special folders to the network.
 - Internet Explorer Maintenance—Used to manage and customize Internet Explorer on Windows 2000-based computers.
 - Remote Installation Services—Used to control the behavior of the Remote Operating System Installation feature as displayed to client computers

Internet Explorer Maintenance extension snap-in

Administrators use Internet Explorer Maintenance to manage and customize Microsoft Internet Explorer on Windows 2000-based computers.

Microsoft Management Console (MMC)

A common console framework for system-management applications. The primary goal of the Microsoft Management Console is to support simplified administration and lower cost of ownership through tool integration, task orientation, support for task delegation, and overall interface simplification. The MMC console hosts the administrative tools (these are called MMC snap-ins); the console itself provides no management functionality.

MMC snap-in

Tools that extend the MMC console and provide administrative functionality. A snap-in functions independently from other snap-ins.

MMC extension snap-in

A tool that enhances the functionality of a parent snap-in. An extension depends on a parent snap-in for contextual data.

organizational unit (OU)

A type of directory object contained within domains. OUs are logical containers into which you can place users, groups, computers, and even other organizational units.

registry

A database in which Windows NT internal configuration information and computer- and user-specific settings are stored.

registry hive

A section of the registry that is saved as a file. The registry subtree is divided

into hives (named for their resemblance to the cellular structure of a beehive). A hive is a discrete body of keys, subkeys, and values.

Remote Installation Services

A new optional component included in Windows 2000 Server that administrators can use to remotely install a local copy of the Windows 2000 Professional operating system on supported computers throughout their organization. Administrators can deploy a new version of an operating system upgrade to large numbers of clients at one time from a centralized location. Administrators can use Group Policy to specify the client installation options that groups of users can access. These options are determined by the specific Remote OS Installation Group Policy settings that administrators define for the site, domain, or OU to which the users belong, in conjunction with the specific security group or user account.

schema

The formal definition of all object classes, and the attributes that make up those object classes, that can be stored in the directory. The Active Directory includes a default schema, which defines many object classes, such as users, groups, computers, domains, organizational units, and security policies. The Active Directory schema is dynamically extensible; this means that you can modify the schema by defining new object types and their attributes and by defining new attributes for existing objects. You can do this either programmatically with the Schema Manager snap-in tool included with Windows NT Server.

scripts

Batch files (.bat) or executable (.exe) files that run when a computer starts up or shuts down or when a user logs on or off at any type of workstation on the network. Windows 2000 supports Windows Scripting Host Visual BasicScripting Edition (VBScript) and Jscript, while continuing to support MS-DOS command scripts and executable files.

security descriptor

A set of access-control information attached to every container and object on the network. A security descriptor controls the type of access allowed to users and groups. Administrators assign security descriptors to objects stored in the Active Directory in order to control access to resources or objects on the network.

A security descriptor lists the users and groups that are granted access to an object (a file, printer, or service, for example), and the specific permissions assigned to those users and groups. *See also* discretionary access control list *and* system access control list.

Security Settings extension snap-in

A Group Policy extension snap-in that you use to define security configuration for computers within a Group Policy object. A security configuration consists of settings applied to each security area supported for Windows 2000 Professional or Windows 2000 Server. This configuration is included within a GPO.

site

In Windows 2000 you register your network's physical topology by defining sites. A site is defined as one or more IP subnets. Windows 2000 uses site information to direct requests from one computer to be fulfilled by another computer at the same site. For example, when a workstation logs on, the Active Directory uses the TCP/IP address of the workstation, along with the site information you have entered, to locate a domain controller on the local site. This local controller is used to service the workstation's requests.

Scripts extension snap-in

A Group Policy extension snap-in that you use to assign scripts to run at computer startup or shutdown or upon user logon or logoff.

Software Installation extension snap-in

A Group Policy extension snap-in that you use to centrally manage software distribution in your organization.

system access control list (SACL)

Part of a security descriptor that specifies which user accounts or groups to audit when accessing an object, the access events to be audited for each group or user, and a Success or Failure attribute for each access event, based on the permissions granted in the object's DACL.

total cost of ownership (TCO)

Refers to the administrative costs associated with computer hardware and software purchases, deployment and configuration, hardware and software updates, training, maintenance, and technical support.

Windows Installer packages (.msi files)

Packages that contain all the information necessary to describe to the Windows Installer how to set up an application in every conceivable situation: various platforms, different sets of previously installed products, earlier versions of a product, and numerous default installation locations. The Software Installation extension snap-in to the Group Policy snap-in uses .msi packages.

Zero Administration Windows

Microsoft's solution for lowering the total cost of ownership is an initiative called Zero Administration Windows. The broad goals for Zero Administration Windows are to significantly lower the cost of initial configuration from today's levels and to decrease administrative overhead when the network is running in a steady state. After initial computer configuration, a combination of automatic application setup, scripting, and desktop policies significantly lowers the costs associated with managing workstations.

For More Information

For the latest information on Windows 2000 Server, Change and Configuration Management, and IntelliMirror, see the [Windows 2000 Server](http://www.microsoft.com/windows2000/guide/server/overview/default.asp) Web site at <http://www.microsoft.com/windows2000/guide/server/overview/default.asp>.

Management and Overview Papers

The following table lists a series of papers that introduce the Microsoft Windows management services and change and configuration management. These papers are intended for managers and technical decision-makers who need to understand the business requirements for, and the benefits of, management features, as well as the Microsoft management architecture, tools, and solutions. We recommend that you read these in the order listed below.

Title	Content	Point your browser to:
Introduction to Windows Management Services	An overview of the management roles and disciplines, as well as the architecture for management solutions that will be available, either as part of the operating system or as an add-on.	http://www.microsoft.com/windows2000/library/howitworks/management/managementintro.asp .
Windows 2000 Desktop Management Overview	An overview of change and configuration management and an introduction to how Microsoft products, such as Windows 2000 IntelliMirror, Remote OS Installation and Systems Management Server address this management discipline.	http://www.microsoft.com/windows2000/library/howitworks/management/ccmintro.asp .
Introduction to IntelliMirror	An overview of the features of Windows 2000 IntelliMirror and scenarios for how organizations can benefit from IntelliMirror.	http://www.microsoft.com/windows2000/library/howitworks/management/intellimirror.asp .
Remote Operating System Installation Overview	An overview of the features of Remote Operating System Installation and scenarios illustrating how organizations can benefit from Remote Operating System.	http://www.microsoft.com/windows2000/library/howitworks/management/remoteover.asp .
Systems Management Server: Executive Overview	An overview of the features of Systems Management Server, and discussion of its benefits.	http://www.microsoft.com/smsmgmt/exec/default.asp and http://www.microsoft.com/smsmgmt/default.asp .

Technical Papers

The following table lists additional technical papers that are or will be available for administrators and Information Technology (IT) managers who are interested in understanding the details of Windows management services features and technologies.

More information on	Is or will be available in this web site:
Active Directory	http://www.microsoft.com/windows2000/library/technologies/activedirectory/default.asp .
Step-by-Step Guide to Understanding the Group Policy Feature Set	http://www.microsoft.com/windows2000/library/planning/management/groupsteps.asp .
Using Group Policy Scenarios	http://www.microsoft.com/windows2000/library/howitworks/management/grouppolicy.asp .
Microsoft Windows Installer Service	http://www.microsoft.com/windows2000/library/howitworks/management/installer.asp .
Software Installation and Maintenance	http://www.microsoft.com/windows2000/library/operations/management/siamwp.asp .
Remote OS Installation Service	http://www.microsoft.com/windows2000/library/planning/management/remoteos.asp .
User Settings and User Data	http://www.microsoft.com/windows2000/library/operations/management/settings.asp .
Windows Management Instrumentation (WMI)	http://www.microsoft.com/windows2000/library/technologies/management .
Implementing Profiles and Policies for Windows NT 4.0	http://www.microsoft.com/ntserver/management/deployment/planguide/prof_policies.asp .